# Table of Contents

## INTRODUCING AD ENTERPRISE

- Overview of Investigating Digital Evidence .............................................................. 9
- About Examining Digital Evidence ............................................................................. 13
- About Managing Cases and Evidence ....................................................................... 13
- What You Can Do With the Examiner ........................................................................ 14

## ADMINISTRATING AD ENTERPRISE

- Initializing the Database and Creating an Application Administrator Account ............... 21
- Changing Your Password ......................................................................................... 23
- Recovering a Password ............................................................................................. 23
- Managing Database Sessions ..................................................................................... 27
- Managing KFF Settings ............................................................................................. 28
- Restoring an Image to a Disk ..................................................................................... 29
- Adding New Users to a Database .............................................................................. 29
- Managing Roles ......................................................................................................... 30
- About Assigning Roles to Users ................................................................................ 30
- Email Notifications for Case-Level Permissions ...................................................... 39
- Assigning Users Shared Label Visibility .................................................................... 40
- Setting Additional Preferences .................................................................................. 40
- Managing Global Features ....................................................................................... 42

## USING THE AUDIT LOG

- About the Audit Log .................................................................................................. 48
- Exporting an Event Audit Log .................................................................................... 48

## CASE MANAGEMENT

- About Case Management ............................................................................................ 60
- The User Interfaces ...................................................................................................... 60
- Menus of the Case Manager ........................................................................................ 61
- Opening an Existing Case ........................................................................................... 68
- Evidence Processing Options ..................................................................................... 85
- Converting a Case ........................................................................................................ 121
- Migrating Cases Between Database Types .................................................................. 123
- Creating and Using Tasks ........................................................................................... 131

## WORKING WITH EVIDENCE IMAGE FILES

- Verifying Drive Image Integrity .................................................................................. 138
- Mounting an Image to a Drive .................................................................................... 139
- Benefits of Image Mounting ...................................................................................... 140
- Characteristics of a Logically Mounted Image .......................................................... 141
- Characteristics of a Physically Mounted Image ......................................................... 141
- Mounting an Image as Read-Only .............................................................................. 141
- Mounting a Drive Image as Writable ......................................................................... 143
- Unmounting an Image ............................................................................................... 144
- Restoring an Image to a Disk .................................................................................... 144
- Performing Final Carve Processing .......................................................................... 145
Installing The Enterprise Agent on Linux ................................................................. 773
Installing the macOS Managed Agent .................................................................. 778
Installing the Legacy MacAgent ........................................................................... 795
Part I

Introducing AD Enterprise

This part contains introductory information about AccessData® AD Enterprise and contains the following chapters:

Introducing AccessData® AD Enterprise
Getting Started with the User Interface
Introducing AccessData® AD Enterprise

AccessData® AD Enterprise lets you do thorough computer forensic examinations. It includes powerful file filtering and search functionality, and access to remote systems on your network.

AccessData forensic investigation software tools help law enforcement officials, corporate security, and IT professionals access and evaluate the evidentiary value of files, folders, and computers.

This chapter includes the following topics

About Acquiring Digital Evidence
About Examining Digital Evidence
About Managing Cases and Evidence
What You Can Do With the Examiner
Overview of Investigating Digital Evidence

This section describes acquiring, preserving, analyzing, presenting, and managing digital evidence and cases. Forensic digital investigations include the following process:

1. Acquisition

   Acquisition involves identifying relevant evidence, securing the evidence, and creating and storing a forensic image of it. 
   About Acquiring Digital Evidence (page 29)

2. Analysis

   Analysis involves creating a case and processing the evidence with tools to properly investigate the evidence. 
   About Examining Digital Evidence (page 31)

3. Presentation

   Presentation involves creating a case report that documents and synthesizes the investigation. About Presenting Evidence (page 33)

4. Management

   Management involves maintenance tasks such as backing up, archiving, detaching, attaching, restoring, and deleting cases and evidence. 
   About Managing Cases and Evidence (page 31)

   The admissibility of digital evidence in a court of law, can be dependent on preserving the integrity of the source data when it is acquired.

   When digital evidence is acquired, forensic examiners create clones of the digital evidence to prevent any possibility of the digital evidence being changed or modified in any way. This acquired duplication is called a forensic image. If there is question to the authenticity of the evidence, the image can be compared to the original source data to prove or to disprove its reliability.

   To create a forensic image, the data must be acquired in such a way that ensures that no changes are made to the original data or to the cloned data. The acquired data must be an exact “bit-by-bit” duplication of the sourcedata. You can use AccessData’s Imager tool to acquire exact duplicates of digital evidence.

   Preserving the evidence is accomplished both in the method of acquisition and the storage of the acquired data. Creating an exact replica of the original source is critical in forensic investigations. Keeping that replica safe from any source of corruption or unauthorized access involves both physical and electronic security. Once a case is
created and the evidence is added to it, the case becomes just as critical. Acquired 001, E01, S01, and AD1 images can be encrypted using AD Encryption.

**Types of Digital Evidence**

Digital evidence is data such as documents and emails that can be transmitted and stored on electronic media, such as computer hard drives, mobile phones, and USB devices.

The following are types of digital evidence

5. **Static evidence**

The data that is imaged before it is added to a case is known as static evidence because it stays the same. Images can be stored and remain available to the case at all times because the image is an exact replica of evidence data in a file format.

6. **Live evidence**

Live evidence can be data that is acquired from a machine while it is running. It is often saved to an image as it is acquired. Sometimes, this is necessary in a field acquisition. Other times, it can be an original drive or other electronic data source that is attached to the investigation computer.

7. **Local live evidence**

An example of local live evidence is an original drive or other electronic data source that is attached to the investigation computer. It can also be data acquired from a device on a remote computer while the device is mounted to the system as Read/Write. All connections to the evidence should be made through a hardware write-blocking device. Live evidence that is attached to the investigation computer must remain connected throughout the entire investigation. It is best to create an image of any evidence source outside of your network, rather than risk having the source removed during the course of the investigation.

8. **Remote live evidence**

Another type of live evidence is data acquired directly from machines that are connected to your corporate network. This live evidence is referred to as remote evidence. The process of adding it to your case for investigation is known as Remote Data Acquisition. To acquire remote live evidence, you must use AccessData Enterprise.
Acquiring Evidence

Some aspects of acquiring evidence are dependent on local or federal law. Be aware of those requirements before you acquire the evidence. You can utilize static evidence as well as acquire and use live and remote evidence from computers on your network.

About Acquiring Static Evidence

For digital evidence to be valid, it must be preserved in its original form. The evidence image must be forensically sound, in other words, identical in every way to the original. The data cannot be modified by the acquisition method used. The following tools can do such an acquisition

9. Hardware Acquisition Tools

Duplicate, or clone, disk drives and allow read-only access to the hard drive. They do not necessarily use a CPU, are self-contained, and are often hand-held.

10. Software Acquisition Tools

Create a software duplication of the evidence called a disk image. Imager lets you choose the image file format, the compression level, and the size of the data segments to use.

AccessData Imager is a software acquisition tool. It can quickly preview evidence. If the evidence warrants further investigation, you can create a forensically sound disk image of the evidence drive or source. It makes a bit-by-bit duplicate of the media, rendering a forensic disk image identical in every way to the original, including file slack and allocated or free space.

You should use a write-blocking device when using software acquisition tools. Some operating systems, such as Windows, make changes to the drive data as it reads the data to be imaged. You can process static evidence, and acquire live data from local network machines for processing. You can also view and preview evidence on remote drives, including CDs and DVDs.

See Working with Static Evidence on page 135.

About Acquiring Live Evidence

You can collect evidence from a live machine when you must. For criminal investigations, it is especially important to be aware of the data compromises you will face in such a situation, however sometimes there is no other choice. One such example is when the suspect drive is encrypted and you must acquire the image in-place while the
machine is running. Another example is when imaging a RAID array; it must be live to be properly acquired.
See Adding Local Live Evidence on page 169.
About Acquiring Remote Evidence

With the AccessData Enterprise license, you can acquire live evidence from your active networked computers, including information in RAM, and drive data. In addition, using Remote Drive Management System (RDMS), you can mount any drive through a mapping and browse its contents, then make a custom image of what you find. This type of evidence is known as remote evidence because it is not stored on the examiner computer but is within your network.

See Acquiring Live Evidence on page 158.

About Examining Digital Evidence

Analyzing evidence is a process to locate and identify meaningful data to make it available to the appropriate parties in an easy-to-understand medium.

After you have completed installation and created a case, you can add evidence for analysis. Evidence can include images of hard drives, floppy drives, CDs and DVDs, portable media such as USB drives, and/or live (un-imaged) data from any common electronic source.

The data can be hashed and indexed. You can run searches in the index for specific words like names and email addresses, or you can run live searches.

You can use the Known File Filter (KFF) library to categorize specific information during evidence analysis. The KFF lets you automatically assign files a status of Alert, Ignore, or Disregard.

About Managing Cases and Evidence

As you work with cases, it is a best practice to back up the cases and the evidence. Back up of evidence files is as easy as copying them to a secure location on a secure media. Back up of cases can be more complicated, but is equally important in the event of a crash or other catastrophic data loss.

Back up of a case requires the same amount of drive space as the case itself. This is an important consideration when planning your network resources for investigations.

Some of the case management features include: Archive, Archive and Detach, and Attach. These features give you control over your cases.

See Managing Global Features (page 54).
What You Can Do With the Examiner

You can use tab views to locate data such as the following:

The **Overview** tab lets you narrow your search to look through specific document types, or to look for items by status or file extension.

The **Graphics** tab lets you quickly scan through thumbnails of the graphics in the case.

The **Email** tab lets you view emails and attachments. As you find items of interest, you can do the following:

- Create, assign, and view labels in a sorted file list view.
- Use searches and filters to find relevant evidence.
- Create bookmarks to easily group the items by topic or keyword, find those items again, and make the bookmarked items easy to add to reports.
- Export files as necessary for password cracking or decryption, then add the decrypted files back as evidence.
- Add external, supplemental files to bookmarks that are not otherwise part of the case.

**About Indexing and Hashing**

During case creation and evidence import, you have the option to create an index of the data and to create hash numbers of all the files contained in the data.

Indexing is the process of creating an index with a searchable list of the words or strings of characters in a case. The index instantaneously provides results. However, it is sometimes necessary to use a live search to find things not contained in the index.

Hashing a file or files refers to the process of using an algorithm to generate a unique value based on a file's contents. Hash values are used to verify file integrity and identify duplicate and known files. Known files can be standard system files that can be ignored in the investigation or they can be files known to contain illicit or dangerous materials. Ignore and alert statuses provide the investigator with valuable information at a glance.

Three hash functions are available: Message Digest 5 (MD5), Secure Hash Algorithms 1 (SHA-1), and Secure Hash Algorithms 256 (SHA-256).

Typically, individual file hashes (each file is hashed as it is indexed and added to a case) compare the results with a known database of hashes, such as the KFF. However, you can also hash multiple files or a disk image to verify that the working copy is identical to the original.
About the Known File Filter Database
The Known File Filter (KFF) is an AccessData utility used to compare file hashes in a case against a database of hashes from files known to be ignorable (such as known system and program files) or with alert status (such as known contraband or illicit material), or those designated as disregard status (such as when a search warrant does not allow inspection of certain files within the image that have been previously identified). The KFF allows quick elimination or pinpointing of these files during an investigation. Files which contain other files, such as ZIP, CAB, and email files with attachments are called container files. When KFF identifies a container file as either ignorable or alert, the component files are not extracted. If extraction is desired, the files must be manually extracted and added to the case.
See Using the Known File Filter (KFF) on page 362.

About Searching
You can conduct live searches or index searches of acquired images. A live search is a bit-by-bit comparison of the entire evidence set with the search term and takes slightly more time than an Index search. Live searches allow you to search non-alphanumeric characters and to perform pattern searches, such as regular expressions and hex values.
See Searching Evidence with Live Search (page 510)
The Index search compares search terms to an index file containing discrete words or number strings found in both the allocated and unallocated space in the case evidence. The investigator can choose to generate an index file during preprocessing.
See Searching Evidence with Index Search (page 521)
AccessData products use dtSearch, one of the leading search tools available, in the index search engine. dtSearch can quickly search gigabytes of text.

About Bookmarking
As important data is identified from the evidence in the case, bookmarking that data enables you to quickly find and refer to it, add to it, and attach related files, even files that are not processed into the case. These files are called “supplementary files.” Bookmarks can be included in reports at any stage of the investigation and analysis.
See Bookmarking Evidence (page 498)
About Presenting Evidence

You can present digital evidence by creating a case report containing the evidence and investigation results in a readable, accessible format.

Use the report wizard to create and modify reports. A report can include bookmarks (information selected during the examination), customized graphic references, and selected file listings. Selected files, such as bookmarked files and graphics, can be exported to make them available with the report. The report can be generated in several file formats, including HTML and PDF and can be generated in multiple formats simultaneously.

See Working with Evidence Reports (page 618).

About Cloud Based and Virtualization Support

Cloud Based Relational Database Services (RDS) Support

The AccessData Suite can now be run on Amazon Web Services (AWS) using the new Cloud Based option. Users will log in using a link to the web service and all services and processing will be located online. Users have the option to use the AWS™ provided PostgreSQL engine or the AWS Aurora™ service. AWS PostgreSQL RDS is wire-compatible with PostgreSQL 9.6.x.

For information, see the Release Notes.

Virtualization Support

AccessData will support its products in a virtual environment running on operating systems and environments supported by both the Vendor/manufacturer and AccessData.

For more information, see the Release Notes.
You can use two primary interfaces to work with cases and evidence:
- Case Manager
- Examiner

The Case Manager

You can use the Case Manager to manage application settings that apply to multiple cases. The following is an example of the Case Manager:

![Case Manager Example](image-url)
The Examiner

You can use the Examiner to locate and interpret case data. The following is an example of the Examiner:

The Examiner

For more information, see the following
See Using the AD Enterprise Examiner Interface
Part II

Administrating AD Enterprise

This part contains information about administrating and configuring AD Enterprise and contains the following chapters:

AD Enterprise Application Administration (page 38)
Using the Audit Log (page 59)
Chapter 3
AD Enterprise Application Administration

This chapter includes topics that discuss administration tasks that you can do within the Case Manager interface.

See the following

See Initializing the Database and Creating an Application Administrator Account on page 39.
See Changing Your Password on page 40.
See Recovering a Password on page 40.
See Setting Database Preferences on page 42.
See Managing Database Sessions on page 42.
See Creating Databases for Individual Cases on page 43.
See Creating Databases for Individual Cases on page 43.
See Managing KFF Settings on page 43.
See Recovering and Deleting Processing Jobs on page 44.
See Restoring an Image to a Disk on page 44.
See Adding New Users to a Database on page 45.
See About Assigning Roles to Users on page 45.
See Email Notifications for Case-Level Permissions on page 52.
See Assigning Users Shared Label Visibility on page 52.
See Setting Additional Preferences on page 53.
See Managing Global Features on page 54.

**Important:** It is strongly recommended to configure anti-virus to exclude the database (PostgreSQL, MS SQL)AD temp, source images/loose files, and case folders for performance and data integrity.
Initializing the Database and Creating an Application Administrator Account

The database and application must already be installed prior to this step. The first time you launch the application, you specify the database to use. The application then creates the database schema which is required before any case data can be loaded into the database. You will be prompted to give the location of the database. This option allows a non-local database to be specified even if a local database is present.

After initializing the database, you are prompted to create an Application Administrator account. This account lets you create other user accounts and perform other administrative tasks.

To initialize the database and create an Application Administrator account
1. Click the shortcut icon to open the application
2. If it does not detect a configured database connection for this version, you will be prompted to Add Database.
3. In the RDBMS drop-down menu, select the brand of database that you are connecting to.
4. Specify the server hosting the database in the Host field.

If the database is on the same computer as FTK, you can leave this field empty.
5. (Optional) Give the database connection a nickname in the Display name field.
6. Specify the database name by doing one of the following:
   - If you are using PostgreSQL or MS SQL Server, for the PostgreSQL dbname or mssql sa, you can use the default values or enter your own value. If you enter your own value, make sure that you record it so that you know the database name.
7. Do not change the Port number fields unless you have a custom database configuration.
8. If you are using MS SQL Server, you can check Use Integrated Security to use your Windows authentication credentials.
9. Click OK.

If the connection attempt to the database was successful, the database will be initialized.
10. In the *Please Authenticate* dialog, log into the database using your database administrator account credentials.
   - If you used the default installation, enter the following credentials:
     Username: postgres
     Password: AD@Password
   - If you used the advanced installation or installed a different database, enter your credentials. A successful login initializes the database and opens the *Case Manager* window.

11. In the *Add New User* dialog, create an Application Administrator account for this version of the database schema.
   - Enter a name and password.
   - Record this information in a secure place.

12. Click **OK**.
Changing Your Password
Once logged into the system, you can change your password.

To change your password
1. In Case Manager, click Database > Change Password.
2. In the Change Password dialog box, enter your current password.
3. Enter your new password in the New Password text box.
4. Verify your new password by entering it again in the Re-enter text box.
5. Click OK.

Recovering a Password
You can recover an Administrator database password using a Password Reset File. Only the Administrator logged into the program can create the reset file and only the Administrator that created the reset file can use the file to reset the password. Before recovering your Administrator password, you will create a Password Reset File. Once you reset a password, the Password Reset File you used is no longer valid.

There are two main components to recover an Administrator’s password:
See Creating a Password Reset File on page 40.
See Resetting your Password on page 41.
Creating a Password Reset File

You can use one of the following methods to create a Password Reset file:
When creating a user with the Application Administration role and assigning a new password
When changing the password for a user with the Application Administration role
Accessing the Create Password Reset File option in the Administer Users dialog.

When creating/changing a password
1. After entering the new password, click OK.
2. A prompt appears that asks you to create a Password Reset File. Click Yes.
3. Navigate to a secure location and enter the name of the Password Reset File.

**Important:** Choose a location for the Password Reset File that only you know and to which others do not have immediate access. Keep its location confidential.
4. Click OK.

From the Administer Users dialog
1. In Case Manager, click Database > Administer Users.
2. Highlight your User Name (that is, the User Name under which you are logged in).
3. Click Create Password Reset File.
4. Navigate to a secure location and enter the name of the Password Reset File.

**Important:** Choose a location for the Password Reset File that only you know and to which others do not have immediate access. Keep its location confidential.
5. Click OK.
Resetting your Password
To reset your password, enter the Password Reset File you created previously.

Note: Any Password Reset Files that have already been used to reset passwords are no longer valid and will not work. Password Reset Files from other users or other databases also will not work. Only the Password Reset File that you created previously with your User Name and Password will work.

To enter the Password Reset File
1. When prompted for your password, enter your User Name.
2. Click OK.

   The Reset Password button appears in the Please Authenticate dialog.
3. Click Reset Password.
4. Locate the Password Reset File, highlight it, and click OK.
5. Enter a new password, verify the new password, and click OK.
Recovering and Deleting Processing Jobs

The Preferences dialog lets you specify where to store the temporary file, the location of a network license and whether you want to optimize the database after you process evidence.

To set database preferences
1. In the Case Manager, click **Tools > Preferences**. Type in or browse to the folder you want temporary files to be written to.
2. Select a location for the temporary file folder.

The Temporary File Folder stores temporary files, including files extracted from ZIP and email archives. The folder is also used as scratch space during text filtering and indexing. The Temporary File Folder is used frequently and should be on a drive with plenty of free space, and should not be subject to drive space allocation limits.
3. If your network uses AccessData Network License Service (NLS), you must provide the IP address and port for accessing the License Server.
4. Specify if you want to optimize the case database.

This is set to optimize by default. Unmark the check box to turn off automatic optimization. This causes the option to be available in Additional Analysis for those cases that were processed with Optimize Database turned off initially. The Restore Optimization option in Additional Analysis does not appear if Database Optimization is set in the New Case Wizard to be performed following processing, or if it has been performed already on the current case from either place.
5. In the **Preferences** dialog, click **OK**.
Recovering and Deleting Processing Jobs

Managing Database Sessions

You can use the Sessions Management dialog to manage and track database sessions from within the CaseManager. You can also use the Manage DB Sessions dialog to terminate cases that are open and consuming sessions, but are inactive. This lets open file handles close so that processing can be restarted.

To open the Manage DB Sessions dialog, in the Case Manager, click Database > Session Management.

Note: This feature only applies to MS SQL and PostgreSQL databases.

To improve performance, when you create new cases in FTK 6.0 or newer, a new database is created for each new case.

In addition to improved performance, if you configured the database location to be in the case folder, the database files are located under the case folder. This allows you to easily back up a case at the folder level as the case data and the database for the case are all under one case folder.

For example, if you create a case called Investigation, select the In the case folder option for the database location, and want to find the database files for that case, you could go to your FTK Cases folder (this is the fileyou listed as the case folder directory), click on the Investigation folder (this is the individual case folder), and open the DB folder, which contains all the database files for this case. If the In the case folder option is not selected, the database will be found in the appropriate Case folder located within the main MS SQL or PostgreSQL database files.

Important: Previous to FTK 6.0, all database files were stored within the main database and must be accessed through either the MS SQL or PostgreSQL database folder. This feature is enabled by default.

To disable the individual case database feature

- In the Case Manager, click Database > Put each case in its own DB

This will deselect the option and cases will be stored within the main database.
Recovering and Deleting Processing Jobs

Managing KFF Settings

The AccessData Known File Filter (KFF) can be managed from the Case Manager > Manage menu. Click KFF to open the KFF Admin dialog box.

This functionality is also found in the Examiner main window under Manage > KFF. The functionality is the same regardless of how you launch KFF Admin. This shows the KFF Server Type and Server Address. You can test communication with the KFF Server.

For information about configuring a KFF Server, see Getting Started with KFF (Known File Filter) (page 328).

Jobs that are started but unable to finish can be restarted or deleted.

To recover and delete processing jobs

1. Click Tools > Recover Processing Jobs. If no jobs remain unfinished, an error message pops up. Click Continue to see the Recover Processing Jobs dialog. If it is empty, you can choose whether to Restart or Delete those jobs.

2. Click Select All, Unselect All, or mark the check box for each job to be recovered.

3. Do one of the following:
   - Click Restart. In the Recovery Type dialog, choose the recovery type that suits your needs.
   - Click Delete. Click Yes to confirm that you want to delete the job permanently.

4. Click Close.
Recovering and Deleting Processing Jobs

Restoring an Image to a Disk

You can restore a disk image (001 (RAW/dd), E01, or S01) to a physical disk. The target disk must be the same size or larger than the original, uncompressed disk.

**To restore an image to a disk**

1. In the *Case Manager* or in the *Examiner*, click **Tools > Restore Image to Disk**. The *Restore Image to Disk* dialog opens.
2. Browse to and select the source image (must be RAW-dd/001, E01, or S01).
3. Click the *Destination drive* drop-down to choose the drive to restore the image to.

If you have connected an additional target drive and it does not appear in the list, click **Refresh** to update the list.

4. If the target (destination) drive is larger than the original, uncompressed data, and you don’t want the image data to share the drive space with old data, mark the **Zero-fill remainder of destination drive** check box.
5. If you need the operating system to see the target drive by drive letter, mark the **Notify operating system to rescan partition table when complete** check box.
6. Click **Restore Image**.

Adding New Users to a Database

The Application Administrator can add new users to a database. The Add New User dialog lets you add users, disable users, change a user’s password, set roles, and show disabled users.

**To add a new user**

1. Click **Database > Administer Users > Create User**.
2. In the *Add New User* dialog, enter information for the following:

| **User Name** | Enter the name that the user is known as in program logs and other system information. |

--
### Full Name
Enter the full name of the user as it is to appear on case reports.

### Password
Enter and verify a password for this user.

### Email Address
Enter a valid email address; this will be used for any notifications.

### Role
Assign rights to the selected user name using roles. The default roles are:

- **Application Administrator**: Can perform all types of tasks, including adding and managing users.
- **Case/Project Administrator**: Can perform all of the tasks an Application Administrator can perform, with the exception of creating and managing users.
- **Case Reviewer**: Cannot create cases; can only process cases.

3. Click **OK** to apply the selected role to the new user.

4. Click **OK** to exit the Add New User dialog.

### Managing Roles
A role is a user group with a specific set of permissions to perform defined investigative tasks. The Administrator can add new roles, modify existing roles, and view a role’s permissions.

### About Assigning Roles to Users
A user can have two levels of roles assigned to him or her. A user can have initial roles granted that apply globally across all cases in a database, and a user can also have specific roles granted for a specific case.

Roles can be granted as follows:

11. Roles that apply to all cases in a database are granted from the Database > Administer Users dialog.

12. Roles that apply to a specific case are granted from the Case > Assign Users dialog.

The permissions that are applied through roles are cumulative, meaning that if you apply more than one, the greatest amount of rights and permissions become available. When you assign roles that apply globally across the database, you cannot reduce the
rights on a case-by-case basis.
AccessData recommends that when you first create a user account, save the account and close the dialog without setting a role. Then click **Case > Assign Users** to assign roles on a case-by-case basis. You can also assign all new users the Case Reviewer role for the database and, then selectively add additional roles as needed on a case-by-case basis.
There are pre-defined roles and you can create your own.

**About Permissions**
Permissions are like user rights on a network. They define what types of information and which machines a user in a specific role can access, and what tasks can be performed by users with that Role.
Tips for Assigning Permissions to Users

It is important to understand that when you create user accounts (Database > Administer Users) and assign roles to users from that dialog, the roles you assign are global for this database; you cannot reduce their rights on a case-by-case basis. If you decide to limit a user’s rights by assigning a different role, you must return to the Database > Administer Users dialog, select a user and choose Set Roles. Unmark the current role and click OK with no role assigned here, or choose a different role that limits access, then click OK to save the new setting.

AccessData recommends that you first create the user account, save the account and close the dialog without setting a role. Then, click Case > Assign Users to assign roles on a case-by-case basis. Or you could assign all new users the global Case Reviewer role, then selectively add the Case/Project Administrator or Application Administrator role as needed. The permissions that are applied through roles are cumulative, meaning that if you apply more than one, the greatest amount of rights and permissions become available.

About Additional Roles

You can use the Case Manager to assign specific roles to users on a case-by-case basis. You can do this by using the Additional Roles feature.

For example, you may have a user who has a general role of Case Reviewer. However, you may want to give that user additional rights to a specific case. You can assign that user an Additional Role for that specific case. You could assign them a Project/Case Administrator role to grant some management rights, or you could assign them the Application Administrator role to grant them all rights for the case.

It is important to note that the rights granted through an Additional Role only apply once the user has opened the case in the Examiner. It does not grant them rights to the case using the Case or Management menus in the Case Manager. For example, this user cannot backup the case. To grant them rights at the Case Manager level, you would need assign them the regular Project/Case Administrator role, not as an Additional Role.
About Predefined Roles

The following roles are predefined and can easily be used:

Application Administrator - has all rights
Project/Case Administrator - has most rights to manage assigned cases and to create and manage new cases. (This role can only manage cases that the user is assigned to or has created themselves.)
Case Reviewer - has rights to view data in assigned cases. You can manage the rights that any role has.

**Important:** The Administrator role overrides all other permissions granted to a user.

The following tables display the default rights that the roles have or don't have.

Restrictions to the Case Reviewer Role

The case reviewer role does not have all of the permissions as the application administrator and the database administrator.

Permissions Denied to Case Reviewer Users

<table>
<thead>
<tr>
<th>Permission</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create, Add, or Delete cases</td>
<td>Use Imager</td>
</tr>
<tr>
<td>Administer Users</td>
<td>Use Registry Viewer</td>
</tr>
<tr>
<td>Data Carve</td>
<td>Use PRTK</td>
</tr>
<tr>
<td>Manually Data Carve</td>
<td>Use Find on Disk</td>
</tr>
<tr>
<td>Assign Users to Cases</td>
<td>Use the Disk Viewer</td>
</tr>
<tr>
<td>Add Evidence</td>
<td>View File Sectors</td>
</tr>
<tr>
<td>Access Dell Encryption Decryption from the Tools Menu</td>
<td>Define, Edit, Delete, Copy, Export, or Import Filters</td>
</tr>
<tr>
<td>Decrypt Files from the Tools Menu</td>
<td>Export Files or Folders</td>
</tr>
<tr>
<td>Mark or View Items Flagged as &quot;Ignorable&quot; or &quot;Privileged&quot;</td>
<td>Access the Additional Analysis Menu</td>
</tr>
<tr>
<td>Manage the KFF</td>
<td>Backup or Restore Cases</td>
</tr>
<tr>
<td>Enter Session Management</td>
<td>Create Custom Data Views</td>
</tr>
</tbody>
</table>
Differences Between the Case Administrator and Application Administrator Roles in the Examiner

Default Case Administrator and Application Administrator Role Comparison (In the Examiner)

<table>
<thead>
<tr>
<th>Examiner Menu</th>
<th>Feature</th>
<th>Project/Case Administrator</th>
<th>Application Administrator</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>File</strong></td>
<td>Export</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td>Export to Image</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td>Export Word List</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td>Reports</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td>Timeline Report</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td>Job Summary Report</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td>Export Event Audit Log</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td><strong>Evidence</strong></td>
<td>Add/Remove</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td>Add Remote Data</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td>Additional Analysis</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td>Process Manually Carved Items</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td></td>
<td>Manage Evidence Group</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td>Import Memory Dump</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td>Import Custom Column File</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Import Custom Column Data</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Delete Custom Column Data</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Merge Case Index</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td><strong>Filter</strong></td>
<td>New</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td>On</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td>Import</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td>Tab Filter</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td><strong>Tools</strong></td>
<td>Decrypt Files</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td>Verify Image Integrity</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Restore Image to Drive</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Mount Image to Drive</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Examiner Menu</td>
<td>Feature</td>
<td>Project/Case Administrator</td>
<td>Application Administrator</td>
</tr>
<tr>
<td>-----------------</td>
<td>----------------------------------</td>
<td>----------------------------</td>
<td>----------------------------</td>
</tr>
<tr>
<td>Disk Viewer</td>
<td></td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Other Applications &gt;</td>
<td>Imager, PRTK, Registry Viewer</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Configure Agent Push</td>
<td></td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Push Agents</td>
<td></td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Manage Remote Acquisition</td>
<td></td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Unmount Agent Drive</td>
<td></td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Disconnect Agents</td>
<td></td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Recover Processing Jobs</td>
<td></td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Execute SQL</td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Select Audit Events</td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Manage</td>
<td>KFF</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>PhotoDNA</td>
<td></td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Labels &gt; Manage Shared Labels</td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Carvers &gt; Manage Carvers</td>
<td></td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Carvers &gt; Manage Shared Carvers</td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Filters &gt; Manage Filters</td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Filters &gt; Manage Shared Filters</td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Columns &gt; Manage Columns</td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Columns &gt; Manage Shared Columns</td>
<td></td>
<td></td>
<td>x</td>
</tr>
</tbody>
</table>
**Assigning Initial Database-level Roles to Users**

You can use the case manager to assign roles to users. Although the default roles can all be selected concurrently, AccessData recommends that only one of these be selected for any user to avoid granting either redundant or excessive permissions.

**To assign initial database-level roles to users**

1. In the *Case Manager*, click **Database > Administer Users**.

2. Do one of the following:
   - If the user does not yet exist in the system click **Create User** to create the user.
   - If the user does exist in the system, select the user’s name and click **Set Roles**.

3. Click **Set Roles** to assign a role that limits or increases database and administrative access.

4. To assign a default role, mark the check box next to that role. The default roles are as follows:
   - **Application Administrator**: Can perform all types of tasks, including adding and managing users.
   - **Case/Project Administrator**: Can perform all of the tasks an Application Administrator can perform, with the exception of creating and managing users.
   - **Case Reviewer**: Cannot create cases; can only process cases.

5. Click **OK** to apply the selected role to the new user, save the settings, and return to the *Add New User* dialog.
Assigning Additional Case-level Roles to Users

You can use the Case Manager to assign specific roles to users on a case-by-case basis. You can do this by using the Additional Roles feature.

To assign additional case-level roles to users
1. In the Case Manager, select the case for which you want to grant additional roles to a user.
2. Click Case > Assign Users.
3. In the Assigned Users pane, select the user that you want to grant additional roles to.
4. Click Additional Roles.
5. In the Additional Roles dialog, under Additional Roles for this Case, select the roles that you want to grant.
6. Click OK.
7. Click Done.

Adding New Roles
You can add new, customized roles to your system.

To add a new role
1. Click Database > Administer Roles.
2. Click New Role at the bottom of the Define Roles window.
3. Enter a name for the role in the Role name field at the top of the window. Enter a description if desired.
4. Click OK.
5. Select the Rights check boxes that you want to associate with this role. When satisfied with the settings you have selected, click Save.

Important: Be sure to view all pages of the Rights field by using the drop down menu to toggle between pages.
Modifying Roles
You can modify a role to meet your needs.

To modify (edit) an existing role
1. Locate the role to modify in the Define Roles window.
2. In the Roles field, highlight the role you would like to edit.
3. Select or deselect the appropriate rights associated with the role.
4. Click Save.

Viewing a Role’s Permissions
You can view the permissions assigned to a particular role.

To view the Permissions assigned to a role
1. Locate the role to view in the Define Roles window.
2. In the Roles field, highlight the role you would like to view. All assigned permissions will be checked in the Rights field.

Note: Be sure to view all pages of the Rights field. Use the drop down menu to toggle between pages.
Email Notifications for Case-Level Permissions

You can send email notifications to alert a user when they have been granted permissions to a case. This feature will use the email entered into the user profile to send a message alert for each case they have been allowed to access. You may also add a message to the standard email alert if desired. These notifications can be sent to multiple email addresses at the same time.

**Important:** A functional email address must be associated with each user being added to the case or the notification will not be sent.

**To send a notification email when adding a user(s) to a case**

1. In the Case Manager, select the case for which you want to add and notify a user.
2. Click **Case > Add Users/Groups** and add users or groups, being sure to include a functional email address for each user. For more information, see *Adding New Users to a Database* (page 45).
3. Check the box next to **Notify users**.
4. If you wish to include additional information other than the default notification that the user has been added to the selected case, you may type your text into the **Message** box. This information will then appear in the body of the email notification.
5. Click **Done**. This will automatically send an email to each user’s associated email address alerting them of his or her addition to the case.

**To set up email notification information**

1. In the Case Manager, select a database and log in.
2. Navigate to **Manage > Email notification settings**. The Manage Email Alert Settings dialog will open.
3. Fill in the **Manage Email Alert Settings** dialog with the appropriate information.
4. If you choose to send a Test Alert, enter the appropriate addresses into the **Send Test Alert** box and press **Send**.
5. Click **OK**.

**Note:** Outgoing TCP traffic must be allowed on port 25.
Assigning Users Shared Label Visibility

Shared Labels give Application Administrators the added benefit of assigning visibility to only specific users on a case-by-case basis.

To assign Label Visibility
1. In Case Manager, click Case > Assign Users. The Assign Users for Case dialog opens, and a list of users that have permissions in the currently selected case appears.
2. Highlight a User.
3. Click Label Visibility to open the Manage Label Visibility dialog.

To show or hide Labels
1. Select a user in the User List pane. The Shared Labels dialog opens. Initially all are set as Visible.
2. Move labels as needed, based on the following:
   - Select a label you want that user not to see in any case, and click the > button.
   - To move a hidden label into the Visible Labels pane, select it, and click the < button.

Setting Additional Preferences

Choosing a Temporary File Path
The Temporary File Folder stores temporary files, including files extracted from ZIP and email archives. The folder is also used as scratch space during text filtering and indexing. The Temporary File Folder is used frequently and should be on a drive with plenty of free space, and should not be subject to drive space allocation limits.

To specify a location for the Temporary File Folder
1. In the Case Manager, click Tools > Preferences. Type in or browse to the folder you want temporary files to be written to.
2. Select the folder, then click OK.
3. In the Preferences dialog, verify the path is what you wanted.
4. In the Theme to use for Visualization section, you can also choose a color scheme to apply to the visualization windows.
5. Click OK.

Providing a Network Security Device Location
If your network uses AccessData Network License Service (NLS), provide the IP address and port for accessing the License Server.

**Setting Theme Preferences for the Visualization Add on**

**To change the appearance of the Visualization window**
1. In the Case Manager, click **Tools > Preferences**.
2. In the *Theme to use for Visualization* section, select a color scheme to apply to the Visualization windows.
3. Click **OK**.

**Private and Public Keys**

You can configure the private and public key for agents.
For information about Agent certs, see Using Agent Certs in Forensics Products (page 680).

**Agent List**

You can also configure a list of Agents. See Using the Windows Agent List on page 169.

**Optimizing the Case Database**

This is set to optimize by default. Unmark the check box to turn off automatic optimization. This causes the option to be available in Additional Analysis for those cases that were processed with Optimize Database turned off initially.

---

**Note:** The Restore Optimization option in Additional Analysis will not appear if Database Optimization was set in the New Case Wizard to be performed following processing, or if it has been performed already on the current case from either place.

---

**Configuring KFF**

To use the Known File Filter feature (KFF), you must configure a KFF Server. In this dialog, you specify the type of KFF Server and its location.
For information on configuring the KFF Server, see Getting Started with KFF (Known File Filter) (page 328).
After the KFF server has been configured, you can click Test Server to test the communication with the KFF Server.

Managing Global Features
Several features that were previously available only in a case are now fully implemented for global application, and are known as “Shared.” Since they are available globally, they are managed from the Case Manager interface, under the Tools menu.
The Application Administrators manage all Shared features. It is a good practice to set these up to the extent you are able, before you create your first case. Of course, new ones can be added at any time and copied to existing cases. Shared features can be created within cases by both Application and Case Administrators, and Shared (added to the global list).
Since each Shared feature has been documented to some extent in other chapters of the User Guide, only the parts of the features that apply specifically to Application Administrators are explained here. Cross-references are added to provide quick access to more complete information.
Managing Shared Custom Carvers

Carvers provide a comprehensive tool that allows you to customize the carving process to access hidden data exactly the way you need it. You can create new, and edit or delete existing shared carvers. In addition, you can import and export carvers, and copy carvers to cases that were previously processed without a particular custom carver.

There are no default carvers listed in the Manage Shared Custom Carvers dialog. It contains only custom-designed carvers that are shared.

See also Custom Carvers (page 101)

To create a Shared Custom Carver
1. In the Case Manager, click Manage > Carvers.
2. From the Manage Shared Custom Carvers dialog, click New.
3. Set the data carving options that you want to use.
4. Click Save when the new carver has been defined to meet your needs. You will see the new carver in this list and when you mark the Carving option in the New Case Wizard.
5. In the Manage Shared Carvers dialog, click the appropriate button to:
   - Create **New** shared custom carvers
   - **Edit** existing shared custom carvers
   - **Delete** shared custom carvers
   - **Import** shared custom carvers that have been exported from cases
   - **Export** shared custom carvers
   - **Copy** shared custom carvers to a case
6. Click **OK** to close the Carving Options dialog.
Managing Custom Identifiers

Custom File Identifiers let you specify which file category or extension should be assigned to files with a certain signature. While Custom Identifiers can be created and/or selected by a Case Administrator in the New Case Wizard, Shared Custom Identifiers are created and managed from a separate menu.

See also Creating Custom File Identifiers (page 107).

To Create a Shared Custom Identifier
1. In the Case Manager, click Manage > Custom Identifiers.

Initially, the Custom Identifiers List pane is empty, and the rest of the window is grayed-out.
2. Click Create New. The window activates.
3. Enter a name for the new Custom Identifier. The name you enter is added into the Custom Identifiers List.
4. Enter a description to help define the identifier's purpose.
5. Create the Custom Identifier by defining Operations and using the AND and OR buttons.
6. When you are done defining this Custom Identifier, click Apply. You can also do the following
   - Click Delete to delete an unwanted or outdated identifier.
   - Click Export to save the selected identifier as a TXT file.
   - Click Import to add an external identifier file.
   - Click Close to close the Custom Identifiers dialog.
Managing Columns

Shared Columns use the same windows and dialogs that Local Columns use.

To create a Shared Column Template
1. In Case Manager, click Manage > Columns.

   The Manage Shared Column Settings dialog opens.
2. Highlight a default Column Template to use as a basis for a Custom Column Template.
3. Click New.
4. Enter a new name in the Column Template Name field.
5. Select the Columns to add from the Available Columns pane, and click Add >> to move them to the Selected Columns pane.
6. Select from the Selected Columns pane and click Remove to clear an unwanted column from the Selected Columns.
7. When you have the new column template defined, click OK. See also Customizing File List Columns (page 613).

Managing File Extension Maps

Extension Maps can be used to define or change the category associated to any file with a certain file extension. For example, files with BAG extension which would normally be categorized as “Unknown Type” can be categorized as an AOL Bag File, or a files with a MOV extension that would normally be categorized as Apple QuickTime video files can be changed to show up under a more appropriate category since they can sometimes contain still images.
To create a Shared Custom Extension Mapping

1. In the Case Manager, click Manage > File Extension Maps.
2. In the Custom Extension Mapping dialog, click Create New.
3. Enter a name for the new mapping.
4. Enter a description for easier identification.
5. In the Category pane, select a file type you want to map an extension to.
6. Click Add Extension.

   The Add New Extension dialog box opens.
7. Enter the new extension to add.
8. Click OK.

You can also do the following:

- Click Delete to remove an unwanted or outdated mapping.
- Click Import to add an external Custom Extension Mapping file for Shared use.
- Click Export to save a Custom Extension Mapping file.
- Click Close to close the Custom Extension Mapping dialog. See also Custom Case Extension Maps (page 108).
Managing Filters

Filters consist of a name, a description, and as many rules as you need. A filter rule consists of a property, an operator, and one or two criteria. (You may have two criteria in a date range.)

To create a new Shared filter
1. From Case Manager, click Manage > Filters.

   The Manage Shared Filters dialog opens.
2. Do one of the following:
   ● If there is an existing filter in the Filters list that you want to use as a pattern, or template, highlight that filter and click Copy.
   ● If there is no filter that will work as a pattern, Click New.
3. Enter a name and a short description of the new filter.
4. Select a property from the drop-down menu.
5. Select an operator from the Properties drop-down menu.
6. Select the applicable criteria from the Properties drop-down menu.
7. Each property has its own set of operators, and each operator has its own set of criteria. The possible combinations are vast.
8. Select the Match Any operator to filter out data that satisfies any one of the filter rules or the Match All operator to filter out data that satisfies all rules of the filter.

You can test the filter without having to save it first. Check the Live Preview box to test the filter as you create it.
Using the Audit Log

About the Audit Log
The audit log preserves an explicit record of user activity during an logged-in session of the application. These records are useful for management oversight as well as case history record keeping. You can use audit logging which logs the following agent actions:

- You connected to a specific computer
- You performed a preview
- You performed a full disk image

Exporting an Event Audit Log
Events are logged for each database and for each case in a database. Logged events can be exported to a file containing selected events. Application Administrators can define the specific events to be logged for all new cases, with the exception of some events that are always logged by default.

The Case Reviewer cannot see any Export Event Audit Log features or menus. Case Administrators can set up their own log preferences within a case. Case Admin-defined settings do not affect those defined by the Application Administrator.

Event Audit Logs are exported and saved in CSV format, so they can be opened into a spreadsheet application such as Excel or QuattroPro where they can be sorted according to the data type you want to evaluate.

Event Audit Logs are useful for evaluating what users are doing, how long it takes to complete a task, the balance of work for each user and administrator, how the program is being used, and many other events that take place within the AD Lab environment.

The Event Audit log files can be exported from the current case by either an Application Administrator or a Case Administrator from within that case. Note that the list of available events for export from within a case is only about half the number of events that can be exported from Case Manager.
The Case Manager Export Event Audit Log feature allows the Application Administrator to export from multiple cases simultaneously. Whether from the Case Manager, or the Examiner, the Export Event Audit Log dialog box allows the Administrator to filter the exported log data to get the exact data set needed. The filters that can be applied areas follows:

**Case:** (Applies to Application Administrators global Case Administrators only)
From *Case Manager*, choose **None** instead of a single case, or all cases, to export a global Event Audit Log.

**User(s):**
Application Administrators from *Case Manager*.
Case Administrators assigned globally from *Examiner*.

**Event(s):**
Application Administrators from *Case Manager*, choosing one or all cases.
Application or Case Administrators from *Examiner* choosing from *Case Events* only.

**Date Range:**
Set a *Date* and *Time* range for events to export.
 When selecting Users, a list of AD Lab defined Users displays the Usernames and Full Names. Roles are not listed here. Mark the check box next to each user who has rights to the case or cases from which Event Audit Logs are being exported.

Defining the events to export is done differently for a new case than it is from an existing, open case.
Exporting Global Event Audit Logs

Global events are automatically logged at all times. They cannot be set to log or not log. The Application or Case Administrator role is the only one that can be assigned that has the permissions to export reports of the logged global events.

Global Audit Events

<table>
<thead>
<tr>
<th>Event</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log on</td>
<td>Log off</td>
</tr>
<tr>
<td>Time logged on</td>
<td>Changed own password</td>
</tr>
<tr>
<td>Rights at login</td>
<td>Roles at login</td>
</tr>
<tr>
<td>New user</td>
<td>Disable user</td>
</tr>
<tr>
<td>Create role</td>
<td>Copy role</td>
</tr>
<tr>
<td>Copy role</td>
<td>Change rights to role</td>
</tr>
<tr>
<td>Import role</td>
<td>Export role</td>
</tr>
<tr>
<td>Create shared label</td>
<td>Remove shared label</td>
</tr>
<tr>
<td>Rename shared label</td>
<td>Change color of shared label</td>
</tr>
<tr>
<td>Copy labels to shared</td>
<td>Import shared label</td>
</tr>
<tr>
<td>Export shared label</td>
<td>Create a shared label group</td>
</tr>
<tr>
<td>Delete a shared label group</td>
<td>Rename a shared label group</td>
</tr>
<tr>
<td>Add label(s) to shared group</td>
<td>Remove label from sharedgroup</td>
</tr>
</tbody>
</table>
Global Audit Events (Continued)

<table>
<thead>
<tr>
<th>Event</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit report</td>
<td>Create case</td>
</tr>
<tr>
<td>Delete case</td>
<td>Administer case</td>
</tr>
<tr>
<td>Archive case</td>
<td>Detach case</td>
</tr>
<tr>
<td>Copy case</td>
<td>Restore case</td>
</tr>
<tr>
<td>Attach case</td>
<td>Replace attached case file</td>
</tr>
<tr>
<td>Add attached case file</td>
<td>Remove attached case file</td>
</tr>
</tbody>
</table>

To export a Global Event Audit Log

1. Log in to AD Lab as a user with the Application Administrator role.

2. Click Database > Export Event Audit Log.
3. In the Case drop-down, select None.
4. Click User(s).
5. In the Select User(s) dialog box, mark the check box next to each user whose activities you want to include.
6. Click OK.
7. Click Event(s).
8. In the Select Event(s) dialog box, mark the check box next to each event type you want to include.

When you mark an item, you may notice that the Select Associated ID(s) or the Select Associated Target ID(s) buttons activate. The active button indicates that you can select more specific information for that event.
A good example of the difference between the two is as follows:

- Mark **Create Bookmark**, and the **Select Associated ID(s)** button activates. Click **Select Associated ID(s)** and you see the list of bookmarks, both shared and individual, within a case.

- Mark **Add files to bookmark**, and both the **Select Associated ID(s)** and the **Select Associated Target ID(s)** button also activates. Click **Select Associated ID(s)** and you see the list of Bookmarks, both shared and individual, within a case. Click **Select Associated Target ID(s)** to see the files that are contained in the selected bookmark(s).

- The following are indications in the **Select Events** dialog box of whether additional ID(s) have been selected:

  After you have selected **Associated ID(s)**, an asterisk (*) follows the **Event Name** in the **Select Event(s)** list.

  After you have selected **Associated Target ID(s)**, a dagger (†) follows the **Event Name** in the **Select Event(s)** list.

9. After you have finished selecting the **Associated IDs** and **Associated Target IDs** for the events to be audited in the case, click **OK**.

10. In the **Export Event Audit log** dialog box, to filter events by date, mark the **Date Range** check box, and specify the beginning date and time and the ending date and time to include events within.

11. When you are done setting the filters for the events to include in the log, click **Generate**.
Exporting Case Event Audit Logs

The available case events that can be selected for audit from Case Manager are defined in the New Case wizard (only available to application administrators). If all events are selected from the list when the case is created, they will be available for selection in the Examiner by either the Application Administrator or the Case Administrator.

**Note:** The events marked with asterisk (*) apply to AD Enterprise only

### Case Audit Events

<table>
<thead>
<tr>
<th>Event</th>
<th>Event</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open case</td>
<td>Label files</td>
<td>Copy special</td>
</tr>
<tr>
<td>Close case</td>
<td>Remove label from an object</td>
<td>Create report</td>
</tr>
<tr>
<td>Restore an image to disk</td>
<td>Change color of label</td>
<td>Rights in the case</td>
</tr>
<tr>
<td>Has viewed objects</td>
<td>Copy shared labels to the case</td>
<td>Created a group</td>
</tr>
<tr>
<td>Export data from case</td>
<td>Import label</td>
<td>Updated group information and or associations</td>
</tr>
<tr>
<td>Assign file category</td>
<td>Export label</td>
<td>Deleted the group</td>
</tr>
<tr>
<td>Ignorable: set</td>
<td>Create a label group</td>
<td>Updated/Inserted/Deleted LDAP group information*</td>
</tr>
<tr>
<td>Ignorable: unset</td>
<td>Delete a label group</td>
<td>Connected to a remote agent*</td>
</tr>
<tr>
<td>Privileged: set</td>
<td>Rename a label group</td>
<td>Preview a drive on an agent computer*</td>
</tr>
<tr>
<td>Privileged: unset</td>
<td>Add label(s) to group</td>
<td>Image a drive on an agent computer*</td>
</tr>
<tr>
<td>Start viewing objects</td>
<td>Remove label(s) from group</td>
<td>Create agent*</td>
</tr>
<tr>
<td>Index search</td>
<td>Process evidence</td>
<td>Push agent*</td>
</tr>
<tr>
<td>Live search</td>
<td>Additional analysis</td>
<td>Open memory stream*</td>
</tr>
<tr>
<td>Create bookmark</td>
<td>Add evidence</td>
<td>Search memory*</td>
</tr>
<tr>
<td>Add files to bookmark</td>
<td>Remove evidence</td>
<td>Remediation job run*</td>
</tr>
<tr>
<td>Remove a file from bookmark</td>
<td>Merge case index</td>
<td>Wipe remote file*</td>
</tr>
<tr>
<td>Modify bookmark</td>
<td>Map an image to disk</td>
<td>Kill remote processes*</td>
</tr>
<tr>
<td>Remove bookmark</td>
<td>Total of all viewed objects</td>
<td>Get remote file*</td>
</tr>
<tr>
<td>Define label</td>
<td>Role(s) upon opening case</td>
<td>Copy remote file*</td>
</tr>
<tr>
<td>Remove label</td>
<td>Export word list</td>
<td>Execute remote command*</td>
</tr>
<tr>
<td>Rename label</td>
<td>Export file list</td>
<td></td>
</tr>
</tbody>
</table>
To define the list of available case events in a new case
1. Log in as a user with application administrator privileges.
2. In Case Manager click Case > New.
3. In New Case Options, click Customize.
4. In Detailed Options, click Event Audit Log.
5. Do any combination of the following:
   - Click Select All to mark all available events.
   - Click Clear All to unmark all available events.
   - Mark individual check boxes to mark or unmark events to customize the list.
6. Click Save as Defaults to preserve the customized list as the default.

Any user with Administrative privileges can modify this default list, or simply make changes to the list for a single case.

To Export a Case Event Audit Log
1. Log in to AD Lab as a user with the Application Administrator or Case Administrator role.
2. Open the case from which you want to export an Event Audit Log.
3. Click Tools > Select Audit Events.
4. Click Select All or Clear All, and select or unselect individual items as needed.
5. Click OK.
6. From the Examiner window, click File > Export Event Audit Log.

The Case drop-down displays the name of the case you currently have open, and cannot be changed.
7. Click User(s).
8. In the Select User(s) dialog box, mark the check box next to each user whose activities you want to include.
9. Click OK.
10. Click Event(s).
11. In the Select Event(s) dialog box, mark the check box next to each event type you want to include.

When you mark an item, you may notice that the Select Associated ID(s) or the Select Associated Target ID(s) buttons activate. The active button indicates that you can select more specific information for that event. For example:

- **Mark Create Bookmark**, and the Select Associated ID(s) button activates. Click Select Associated ID(s) and you see the list of bookmarks, both shared and individual, within a case.

- **Mark Add files to bookmark**, and both the Select Associated ID(s) and the Select Associated Target ID(s) button also activates. Click Select Associated ID(s) and you see the list of bookmarks, both shared and individual, within a case. Click Select Associated Target ID(s) to see the files that are contained in the selected bookmark(s).

The following are indications in the Select Events dialog box of whether additional ID(s) have been selected:

- After you have selected Associated ID(s), an asterisk follows the Event Name in the Select Event(s) list.

- After you have selected Associated Target ID(s), a dagger follows the Event Name in the Select Event(s) list.

12. After you have finished selecting the Associated IDs and Associated Target IDs for the events to be audited in the case, click OK.

13. In the Export Event Audit Log dialog box, to filter events by date, mark the Date Range check box, and specify the beginning date and time and the ending date and time to include events within.

14. When you are done setting the filters for the events to include in the log, click Generate.
**Viewing Permissions Changes in the Audit Log**

It is possible to view permissions changes in the Audit Log. Information recorded includes such items as when a user has been added to a new role as well as the administrator who made the change. To view permissions logs you must include all cases in the database within the parameters of the exported log. This will allow the log to show non-case specific changes.

**To view permissions changes in the Audit Log**

1. Access the current Audit Log in the Case Manager by selecting **Database > Export Event Audit Log**.
2. Set the **Cases** value to `<none>`. This will allow the log to show all case and non-case specific log items.

---

**Note:** If you select All Cases, the log will omit the rights and roles logging because this data is external to individual cases. You must set the Cases value to `<none>` to get the full Audit Log, including permissions changes.

3. Click **Generate**. Name and **Save** the file, then open the file. You will see all Audit Log data.

---

**Note:** When the Case column shows a value of -1, this indicates that all cases are included in the log.

---

**Viewing Exported Event Audit Logs**

Event Audit Logs are exported in CSV format, so they can be opened in Microsoft Excel, Corel QuattroPro, OpenOffice Calc, or any other spreadsheet-type program.

**To view an exported Event Audit Log**

1. Open the spreadsheet program you normally use.
2. Choose to open a file and navigate to the audit log file you exported.
3. Click **Open**.
4. In the **Text Import** dialog box, select the comma, and tab separators.
5. If available, click the quotation mark (") text delimiter.
6. Click **OK**.
Including Event Audit Log Data in a Report

You can now include the Event Audit Log data in a report. To do so, you must set the criteria as you normally would, but it is done from the Report Options dialog box.

To create a Report that includes Event Audit Log data
1. In the Examiner, click Tools > Select Audit Events.
2. Do any combination of the following:
   • Click Select All to mark all available events.
   • Click Clear All to unmark all available events.
   • Mark individual check boxes to mark or unmark events to customize the list.
3. Click OK when the events you want included in the Report are selected.
5. In the Report Options dialog box, mark the check box next to Event Audit Log.
6. Select the Event Audit Log label next to the check box to open the Event Audit Log filter options dialog box.
7. Click User(s).
8. In the Select User(s) dialog box, mark the check box next to each user whose activities you want to include.
9. Click OK.
10. Click Event(s).
11. In the Select Event(s) dialog box, mark the check box next to each event type you want to include.

When you mark an item, you may notice that the Select Associated ID(s) or the Select Associated Target ID(s) buttons activate. The active button indicates that you can select more specific information for that event.
A good example of the difference between the two is as follows:

- Mark Create Bookmark, and the Select Associated ID(s) button activates. Click Select Associated ID(s) and you see the list of Bookmarks, both shared and individual, within a case.
- Mark Add files to bookmark, and both the Select Associated ID(s) and the Select Associated TargetID(s) button also activates. Click Select Associated ID(s) and you see the list of bookmarks, both shared and individual, within a case. Click Select Associated Target ID(s) to see the files that are contained in the selected bookmark(s).

The following are indications in the Select Events dialog box of whether additional ID(s) have been selected:

- After you have selected Associated ID(s), an asterisk follows the Event Name in the Select Event(s) list.
- After you have selected Associated Target ID(s), a dagger follows the Event Name in the SelectEvent(s) list.

12. After you have finished selecting the Associated IDs and Associated target IDs for the events to be audited in the case, click OK.
13. In the Export Event Audit log dialog box, to filter events by date, mark the Date Range check box, and specify the beginning date and time and the ending date and time to include events within.
14. When you are done setting the filters for the events to include in the log, click OK.
15. In the Report Output dialog box, specify the destination folder, make your Language, output Formats, Export Options, and other selections.
16. Click OK to generate the Report.
Part III

Case Management

This part contains information about managing cases. It contains the following chapters:

Introducing AD Enterprise Case Management (page 68)
Creating and Configuring New Cases (page 76)
Managing Case Data (page 115)
Working with Evidence Image Files (page 129)
Working with Static Evidence (page 135)
Filtering Data to Locate Evidence (page 241)
Working with Labels (page 261)
Decryption (page 265)
Exporting Data from the Examiner (page 288)
Getting Started with KFF (Known File Filter) (page 328)
About Cerberus Malware Analysis (page 303)
Running Cerberus Malware Analysis (page 321)
Chapter 5
Introducing AD Enterprise Case Management

This chapter includes the following topics

About Case Management (page 68)
The User Interfaces (page 68)
About the Cases List (page 69)
Menus of the Case Manager (page 69)

About Case Management
Case management includes creating new cases, as well as backing up, archiving, detaching, restoring, attaching, deleting cases from the database, and managing case and evidence files.

Case management tasks are performed from the Case Manager.

Note: Multiple user names in a case are automatically assigned to Original User Names when a case is Archived, or Archived and Detached, and then restored. They can also be reassigned if necessary.

See Creating a Case (page 78)
See Managing Case Data (page 115)

The User Interfaces
The Case Manager lets you add and manage cases, users, roles and permissions, and do other management tasks. You can use the Case Manager to apply settings globally to all cases in the system.

Menus of the Case Manager (page 69)
You can use the Examiner to locate, bookmark, and report on evidence. Menus of the Examiner (page 390)
About the Cases List

The Cases List shows all of the cases that are available to the currently logged in user. The right pane displays information about the cases. The information that is shown for Case File, Description File, and Description are determined by the either the Application Administrator or the Case Administrator.

Menus of the Case Manager

Case Manager Menus

<table>
<thead>
<tr>
<th>Menu</th>
<th>More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>File</td>
<td>The File menu lets you exit the Case Manager.</td>
</tr>
<tr>
<td></td>
<td>See Options of the Case Manager File Menu (page 70)</td>
</tr>
<tr>
<td>Database</td>
<td>The Database menu lets you administer users and roles.</td>
</tr>
<tr>
<td></td>
<td>See Options of the Case Manager Database Menu (page 70)</td>
</tr>
<tr>
<td>Case</td>
<td>The Case menu lets you create, backup, and delete cases. You can also assign usersto roles.</td>
</tr>
<tr>
<td></td>
<td>See Options of the Case Manager Case Menu (page 72)</td>
</tr>
<tr>
<td>Tools</td>
<td>The Tools menu lets you configure the processing engine, recover interrupted jobs and restore images to a disk.</td>
</tr>
<tr>
<td></td>
<td>See Options of the Case Manager Tools Menu (page 73)</td>
</tr>
<tr>
<td>Manage</td>
<td>The Manage menu lets you administrate shared objects such as columns, labels and carvers.</td>
</tr>
<tr>
<td></td>
<td>See Options of the Case Manager Manage Menu (page 74)</td>
</tr>
<tr>
<td>Help</td>
<td>The Help menu lets you access the user guide as well as view version and copyright information.</td>
</tr>
<tr>
<td></td>
<td>See Options of the Case Manager Help Menu (page 75)</td>
</tr>
</tbody>
</table>
Options of the Case Manager File Menu

**Options of the Case Manager File Menu**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exit</td>
<td>Exits and closes the program.</td>
</tr>
</tbody>
</table>

Options of the Case Manager Database Menu

**Options of the Case Manager Database Menu**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log In/ Log Out</td>
<td>Opens the authentication dialog for users to log into the database. You can log out the currently authenticated user without closing the program.</td>
</tr>
<tr>
<td>Add Database</td>
<td>Makes an additional database available for the system to utilize.</td>
</tr>
<tr>
<td>Remove Database</td>
<td>Removes a database from the list of those available to the system.</td>
</tr>
<tr>
<td>Set as Default</td>
<td>Sets the selected database as the default for the system.</td>
</tr>
<tr>
<td>Put each case in</td>
<td>Creates a new database for each new case. This is enabled by default.</td>
</tr>
<tr>
<td>its own DB</td>
<td></td>
</tr>
<tr>
<td>Change password</td>
<td>Opens the Change Password dialog. The currently authenticated user can change their own password by providing the current password, then typing and re-typing the new password.</td>
</tr>
<tr>
<td></td>
<td>See Changing Your Password on page 40.</td>
</tr>
<tr>
<td>Administer Users</td>
<td>Lets you manage user accounts. The Application Administrator can change users' roles.</td>
</tr>
<tr>
<td></td>
<td>See Adding New Users to a Database on page 45.</td>
</tr>
<tr>
<td>Administer Groups</td>
<td>Creates and customizes groups that can be assigned to users globally, or on a case-by-case basis.</td>
</tr>
<tr>
<td></td>
<td>See Managing Groups on page 57.</td>
</tr>
<tr>
<td>Administer Roles</td>
<td>Creates and customizes roles that can be assigned to users globally, or on a case-by-case basis.</td>
</tr>
<tr>
<td></td>
<td>See Managing Roles on page 60.</td>
</tr>
<tr>
<td>Session Management</td>
<td>Opens the Manage Database Sessions dialog. Click Refresh to update the view of current sessions. Click Terminate to end sessions that are no longer active.</td>
</tr>
<tr>
<td></td>
<td>See Managing Database Sessions on page 42.</td>
</tr>
</tbody>
</table>
## Options of the Case Manager Database Menu

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Export Event Audit Log</td>
<td>Opens the <em>Export Event Audit Log</em> dialog to export event logs filtered by Case, User, Event, and Data Ranges. See <em>Using the Audit Log</em></td>
</tr>
<tr>
<td>Configure</td>
<td>Opens the Configure Database dialog. See <em>Creating Databases for Individual Cases</em> on page 43.</td>
</tr>
</tbody>
</table>

## Options of the Case Manager Case Menu

### Options of the Case Manager Case Menu

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New</td>
<td>Start a new case with the currently authenticated user as the Case Administrator. Case Reviewers cannot create a new case. See <em>Creating a Case</em> (page 78)</td>
</tr>
<tr>
<td>Open</td>
<td>Opens the highlighted case with its included evidence.</td>
</tr>
<tr>
<td>Assign Users</td>
<td>Allows the Application Administrator or the Case Administrator to adjust or control the rights of other users to access a particular case. Also allows the Administrator to control which users can see which of the Shared Labels that are available. See <em>What You Can Do With Labels</em> (page 261)</td>
</tr>
<tr>
<td>Backup</td>
<td>Opens a dialog for specifying names and locations for backup of selected cases. You can select multiple cases in the <em>Case Manager</em> to backup. Options are: <em>Backup</em>, <em>Archive</em>, <em>Archive and Detach</em>. See <em>Managing Case Data</em> on page 115.</td>
</tr>
<tr>
<td>Restore</td>
<td>Opens a Windows Explorer instance for locating and restoring a selected, saved case. Options are: <em>Restore an archived case</em> <em>Attach an archived and detached case</em>. See <em>Managing Case Data</em> on page 115.</td>
</tr>
<tr>
<td>Delete</td>
<td>Deletes the selected case. Pop-up appears to confirm deletion. See <em>Deleting a Case</em> on page 122.</td>
</tr>
</tbody>
</table>
Introducing AD Enterprise Case Management

### Menus of the Case Manager

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create Task</td>
<td>You can create new tasks.</td>
</tr>
<tr>
<td></td>
<td>See Creating and Using Tasks on page 123.</td>
</tr>
<tr>
<td>Refresh Case List</td>
<td>Right-click in the Case List area and select Refresh Case List, or click F5 to refresh the case list with any new information.</td>
</tr>
<tr>
<td>Remove Generated Index</td>
<td>This option lets you select a case and delete its index. If you remove a case’s index, you cannot use index searches until you create a new index. To create a new index, in the Examiner, click Evidence &gt; Additional Analysis. Select dtSearch® Text Index and click OK.</td>
</tr>
<tr>
<td>iSubmit Forms</td>
<td>Users have the ability to pull pertinent information from iSubmit and auto-create a casewith that information, allowing investigators to track a case from start to completion within the iSubmit program. See Opening a Case in iSubmit on page 77.</td>
</tr>
<tr>
<td>Copy Previous Case</td>
<td>Copy a case from a previous version (4.2 or later) into the database. The use of a UNC folder path is no longer required beginning with version 4.2 and newer. To use copy from previous case you don’t backup the case in the previous version, you simply use the “Copy Previous Case” feature. If you want to use Backup, you can backup the case in a previous version, such as 4.2 then restore it to the new version. Copy Previous Case doesn’t recognize backed-up cases.</td>
</tr>
<tr>
<td>Options</td>
<td>Description</td>
</tr>
<tr>
<td>Copy Previous Case</td>
<td>Copy a case from a previous version (4.2 or later) into the database. The use of a UNC folder path is no longer required beginning with version 4.2 and newer. To use copy from previous case you don’t backup the case in the previous version, you simply use the “Copy Previous Case” feature. If you want to use Backup, you can backup the case in a previous version, such as 4.2 then restore it to the new version. Copy Previous Case doesn’t recognize backed-up cases.</td>
</tr>
</tbody>
</table>

See Creating and Using Tasks on page 123.
### Options of the Case Manager Tools Menu

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recover Processing Jobs</td>
<td>Allows you to recover jobs that were interrupted during processing so the processing can be completed.</td>
</tr>
<tr>
<td>Show Progress Window</td>
<td>Opens the <em>Progress</em> window so you can check the Processing Status.</td>
</tr>
<tr>
<td>Restore Image to Disk</td>
<td>Copies a disk image to a disk other than the original.</td>
</tr>
<tr>
<td>Set LDAP Authentication</td>
<td>Allows you to enable and disable LDAP Authentication.</td>
</tr>
</tbody>
</table>
| Dell Encryption Server Settings | Lets you configure Dell Encryption server settings.  
See Decrypting Dell Encryption Files (Dell Data Protection | Encryption Server) on page 278.  
See Setting Additional Preferences on page 53. |
## Options of the Case Manager Manage Menu

### Options of the Case Manager Manage Menu

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Carvers</td>
<td>Manage Shared Custom Carvers. Custom Carvers created here can be copied to cases. See <a href="#">Managing Shared Custom Carvers</a> on page 55.</td>
</tr>
<tr>
<td>Custom Identifiers</td>
<td>Manage Shared Custom Identifiers. Custom Identifiers created here are automatically made available to all new cases, but cannot be copied directly to earlier cases. They must be exported and then imported into such cases. See <a href="#">Managing Custom Identifiers</a> on page 56.</td>
</tr>
<tr>
<td>Columns</td>
<td>Manage Shared Column Settings. Custom Columns created here can be copied to cases. See <a href="#">Managing Columns</a> on page 57.</td>
</tr>
<tr>
<td>File Extension Maps</td>
<td>Manage Shared File Extension Mappings. File Extension Maps created here are automatically made available to all new cases, but cannot be copied directly to earlier cases. They must be exported and then imported into such cases. See <a href="#">Managing File Extension Maps</a> on page 57.</td>
</tr>
<tr>
<td>Filters</td>
<td>Manage Shared Filters. Custom Filters created here can be copied to cases. See <a href="#">Managing Filters</a> on page 58.</td>
</tr>
<tr>
<td>Labels</td>
<td>Manage Shared Labels. Custom Labels created here can be copied to cases. See <a href="#">Working with Labels</a> on page 261.</td>
</tr>
<tr>
<td>KFF</td>
<td>To use the Known File Filter feature (KFF), you must configure a KFF Server. In this dialog, you specify the type of KFF Server and its location.</td>
</tr>
<tr>
<td></td>
<td>For information on configuring the KFF Server, see <a href="#">Getting Started with KFF (Known File Filter)</a> (page 328).</td>
</tr>
<tr>
<td></td>
<td>After the KFF server has been configured, you can click <strong>Test Server</strong> to test the communication with the KFF Server.</td>
</tr>
<tr>
<td>Evidence Processing Profiles</td>
<td>Lets you configure Evidence Processing Profiles. See <a href="#">Using Processing Profiles</a> on page 81.</td>
</tr>
<tr>
<td>Email Notification Settings</td>
<td>See <a href="#">Email Notifications for Case-Level Permissions</a> on page 52.</td>
</tr>
<tr>
<td>Indexed Search Term Weights</td>
<td>See <a href="#">Adjusting the Weighting Criteria for an Index Search Term</a> on page 524.</td>
</tr>
</tbody>
</table>
Opening a Case in iSubmit

Options of the Case Manager Help Menu

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Guide</td>
<td>To access the latest documentation, download the zip file from <a href="http://www.accessdata.com/productdocs/adenterprise/adenterprise.zip">www.accessdata.com/productdocs/adenterprise/adenterprise.zip</a>.</td>
</tr>
<tr>
<td>About</td>
<td>Provides version and build information, copyright and trademark information, and other copyright and trade acknowledgements.</td>
</tr>
</tbody>
</table>

Creating and Configuring New Cases

This chapter explains how to create a new case and configure the case options. If you have cases that were created in version 2.2 or later, you can convert them to the latest version.

This chapter includes the following topics

- Opening an Existing Case (page 76)
- Opening a Case in iSubmit (page 77)
- Creating a Case (page 78)
- Configuring Detailed Options for a Case (page 79)
- Evidence Processing Options (page 88)
- Adding Evidence to a New Case (page 114)
- Converting a Case (page 114)
Opening a Case in iSubmit

Opening an Existing Case

You can open a case that has previously been created and closed.

To open an existing case

1. Open the Case Manager.
2. In the Case Manager, highlight and double-click a case to open it.

Note: If you attempt to open a case you have not been assigned to, you will receive a message saying, “You have not been assigned to work on this case.” This is because you must be authenticated to open the case.

Users have the ability to pull pertinent information from iSubmit and auto-create a case with that information, allowing investigators to track a case from start to completion within the iSubmit program.

This feature requires an add-on license for iSubmit. Please see your sales representative for details. A key will need to be created before you can connect to the iSubmit database.

To create an iSubmit key in the registry

- Create the following REG_SZ key: [HKEY_LOCAL_MACHINE\SOFTWARE\AccessData\Products\Forensic Toolkit\6.3]“iSubmitLicense“=[The iSubmit license number you have obtained from iSubmit]

Note: The version of AccessData software must match the current version you are using. For example FTK 6.3 and 6.3.1 will both use 6.3.
Opening a Case in iSubmit

To connect to an iSubmit database
1. In the Case Manager, navigate to Case > iSubmit Forms.

The iSubmit Forms dialog will open, allowing you to search for an existing form by entering the Form Type and Date Range.
2. Click Update Forms List and select the desired iSubmit form. Click Create.
3. Select the proper Form ID and click Create.

The New Case dialog will open and the new case will then be tracked within iSubmit. The form number is shown in the Reference Field and is automatically populated from the iSubmit database.

Note: You will need to put the iSubmit key in the registry for this to work.
Creating a Case

Case information is stored in a database, and allows case administration as each new case is created.

To start a new case
1. Open the Case Manager.
2. Click Case > New. The New Case Options dialog opens.
3. Enter a name for the case in the Case Name field.
4. (Optional) Enter any specific reference information in the Reference field.
5. (Optional) Enter a short description of the case in the Description field.
6. You can use the Description File option to attach a file to the case. For example you can use this field to attach a work request document or a warrant to the case.
7. In the Case Folder Directory field specify where to store the case files. If you wish to specify a different location for the case, click the Browse button.

Note: If the case folder directory is not shared, an error occurs during case creation.

8. (Optional) In the Database Directory field you can specify a location for where to store database directory files. You can check the In the case folder option to save the database directory in the case folder. If you do not specify these options, the database directory is saved to the default location of the database.

Note: The location that you specify for Database Directory is relative to your database computer. If you intend to specify a location that is on a different computer than your database, for example in a multi-box scenario, then you must enter a network path.

Important: If using a UNC path for the case folder, and selecting the In the case folder option for the database directory, and if the database process isn’t running as a network user, it will not be able to access the UNC path and will therefore fail to create the database files.
9. Configure the default processing options for the case by either using a processing profile or using custom settings.

See Configuring Detailed Options for a Case on page 79.
10. If you wish to open the case as soon as it is created, mark Open the case.
11. Click OK to create the new case.
When you configure Detailed Options for a case, there are options for doing the following:

13. Configuring Default Processing Options for a Case (page 80)
14. Configuring Evidence Refinement (Advanced) Options (page 109)
15. Selecting Index Refinement (Advanced) Options (page 111)
16. Selecting Lab/eDiscovery Options.
17. Managing Custom Identifiers (page 56)

About Processing Options
To help you in investigating the evidence in a case, the evidence data is processed. When evidence is processed, data about the evidence is created and stored in the database. You can view the processed data in the Examiner.

Evidence is processed at the following times:
When adding evidence to a case
After the initial processing, when performing an additional analysis

There are many different types of processing options. You can choose which processing options are relevant to your case.

The following are some examples of how your data can be processed:
Generate hash values for all of the files in the evidence.
Categorize the types of files in your evidence, such as graphics, office documents, encrypted files, and so on.
Expand the contents of compound files, such as ZIP or TAR files.
Create an index of the words that are in the evidence files for quick searches and retrieval.
Create thumbnails for the graphics and videos in the evidence.
Decrypt encrypted files.
Compare files in your evidence against a list of known files that you may want to be alerted about (such as contraband images) or files that you want to ignore (such as Windows system files).
You can select processing options at the following times:
When you create a case (Detailed Options) -- these become the default options for the case. See Evidence Processing Options (page 88)
When you add evidence to an existing case (Refinement Options) -- you can either use or override the case defaults.
See Configuring Evidence Refinement (Advanced) Options (page 109)
When you perform an Additional Analysis on a case. See Using Additional Analysis (page 147)

Each processing option that you enable increases the time that it take to process the evidence. Depending on your situation, you may want to select more or fewer options.
For example, in one scenario, you may want to process the evidence as quickly as possible. In this case, you can use a pre-defined “Field Mode” that deselects almost all processing options and therefore takes the shortest amount of time. After the initial processing, you can perform an Additional Analysis and enable additional processing options.
In another scenario, you may want to take the time to categorize and index files during the initial processing, so you can enable those options. This will take a significant amount of time for a large evidence set.
There is a Pause button available in the Data Processing Status window for situations where you need to interrupt evidence processing. Once you are ready to continue, select the Resume option.

Configuring Default Processing Options for a Case
When you create a case, you define the default processing options that are used whenever evidence is added to that case. By specifying default processing options for a case, you do not have to manually configure the processing options each time you add new evidence. The case-level defaults can be overridden and customized when you add new evidence or when you perform an additional analysis.
You configure the default processing options for a case in one of the following ways:
Using Processing Profiles (page 81)
Customizing the Processing Profile Buttons (page 86)

Note: One factor that may influence which processing options to select is your schedule. If you disable indexing, it shortens case processing time. The case administrator can return at a later time and index the case if needed. The fastest way to create a case and add evidence is to use Field Mode.
Using Processing Profiles

About Processing Profiles

As an investigator, you may want to be able to save a set of processing options as a profile so that they can be easily reused. Processing profiles are a saved list of processing options that are stored in the database.

Processing profiles are created at the global level and are available anytime you create a case. For example, you may need to focus on certain types of data in a case, such as images and videos. In this example, you can create a processing profile that enables the following processing options:

- KFF
- Expand Compound Files
- Flag Bad Extensions
- Create Thumbnails for Graphics
- Create Thumbnails for Video
- Generate Common Video File
- Explicit Image Detection
- PhotoDNA

Each time you create this kind of case, you can use a profile with these options set as default and you won’t need to manually specify them again.

Processing profiles are used at the case level. Specifically, when you create a case, you can select a processing profile from a drop-down list as the default processing options for that case. Any time that you add evidence to that case, the profile's setting will be the default "Refinement Options". This saves you time by not having to reconfigure processing options each time you add evidence to the case. However, when you add evidence to a case, you can modify the processing options for that evidence set. The profile is simply a set of default settings for the case.

Processing profiles are stored in the database. It is important to note that the profile itself does not get saved with the case but only the processing options that are in the profile.

There are five pre-defined, one-click processing profiles:

- Forensic processing (these were the Factory Defaults in version 4.x and earlier)
- eDiscovery processing
- Summation processing
- Basic assessment
- Field mode

See About Pre-configured Processing Profiles on page 82.

When you create a case, you can use one of the pre-configured profiles or create/select a custom profile. If you create a custom profile, you can save it with a unique name so that you can re-use it in a different case.

See Creating a Custom Processing Profile (page 84)
**Important:** When you create a custom profile, the settings for *Custom File Identification* are not stored in the processing profile. The *Send Email Alert* and *Decrypt Dell Encryption Files* settings on the Evidence Processing tab are also not stored in the processing profile.

You can choose which profiles populate in the five one-click processing profile buttons for ease of use. The pre-configured profile options and your other custom profiles will still be available in the drop down menu. You can also edit, delete, import, or export custom processing profiles. See *Managing Processing Profiles* (page 86)

You can also set custom processing options for a case without saving them to a profile. See *Customizing the Processing Profile Buttons* on page 86.

About Pre-configured Processing Profiles

There are five pre-defined, one-click processing profiles. You cannot edit, delete, or export these profiles. However, you can use them as a template for a new custom profile.

The following are the pre-configured profiles.
**Forensic processing**

This profile includes the following processing options:

- MD5 Hash
- SHA-1 Hash
- Expand common compound files
  - This will expand many types of compound files. See Expanding Compound Files (page 91)
- File Signature Analysis
- Flag Bad Extensions
- Search Text Index
  - This processing profile will not index unallocated space or slack space. Unindexed areas such as the unallocated space/file slack can be indexed by utilizing Additional Analysis.
- Create Thumbnails for Graphics
- Include Deleted Files
- Include File Slack
- Include Free Space

For a description of processing options, see Evidence Processing Options (page 88)
eDiscovery processing

The eDiscovery profile allows the processed evidence to be easily imported into AD eDiscovery. These options include:

- MD5 Hash
- Flag Duplicate Files
- Expand Compound Files
- File Signature Analysis
- Search Text Index

This processing profile will not index unallocated space or slack space. Unindexed areas such as the unallocated space/file slack can be indexed by utilizing Additional Analysis.

- Document Content Analysis
- Don’t Expand Embedded Graphics
- Do not include document metadata in filtered text
- Enable Advanced De-duplication Analysis
- Propagate Email Attributes
- Create Email Threads
- Cluster Analysis
- Include Extended Information in the Index
**Summation processing**
The Summation profile allows the processed evidence to be easily imported into AD Summation.

These options include:
- MD5 Hash
- Flag Duplicate Files
- Expand Compound Files
- File Signature Analysis
- Flag Bad Extensions
- Search Text Index

This processing profile will not index unallocated space or slack space. Unindexed areas such as the unallocated space/file slack can be indexed by utilizing Additional Analysis.

- Create Thumbnails for Graphics
- Create Thumbnails for Videos
- Generate Common Video File
- Document Content Analysis
- Do not include document metadata in filtered text
- Enable Advanced De-duplication Analysis
- Propagate Email Attributes
- Create Email Threads
- Cluster Analysis
- Include Extended Information in the Index

**Basic assessment**
This profile includes the following processing options:
- Expand Compound Files
- Include Deleted Files
- Include File Slack
- Include Free Space
- Include Message Headers

**Field mode**
FTK Field Mode disables the standard processing options when processing evidence. This speeds up processing. You can then re-enable processing options through Additional Analysis.

See [Using Additional Analysis](#) (page 147)

The Job Processing screen always shows 0 for Queued when Field Mode is enabled, because items move directly from Active Tasks to Completed.

**Image Processing**
This profile includes the following processing options:

- MD5 Hash
- SHA-1 Hash
- Expand common compound files
  This will expand many types of compound files. See Expanding Compound Files (page 91)
- File Signature Analysis
- Flag Bad Extensions
- Search Text Index
  This processing profile will not index unallocated space or slack space. Unindexed areas such as the unallocated space/file slack can be indexed by utilizing Additional Analysis.
- Create Thumbnails for Graphics
- Create Thumbnails for Videos
- Generate Common Video File
- Explicit Image Detection
- Include Deleted Files
- Include File Slack
- Include Free Space

For a description of processing options, see Evidence Processing Options (page 88)
Video Processing
This profile includes the following processing options:

- MD5 Hash
- SHA-1 Hash
- Expand common compound files

This will expand many types of compound files. See Expanding Compound Files (page 91)

- File Signature Analysis
- Flag Bad Extensions
- Search Text Index
  - This processing profile will not index unallocated space or slack space. Unindexed areas such as the unallocated space/file slack can be indexed by utilizing Additional Analysis.
  - Create Thumbnails for Videos
  - Generate Common Video File
  - Explicit Image Detection
  - Include Deleted Files
  - Include File Slack
  - Include Free Space
**All Communication**

- MD5 Hash
- SHA-1 Hash
- Expand common compound files

  This will expand many types of compound files. See *Expanding Compound Files* (page 91)

- File Signature Analysis
- Flag Bad Extensions
- Search Text Index
  
  - This processing profile will not index unallocated space or slack space. Unindexed areas such as the unallocated space/file slack can be indexed by utilizing Additional Analysis.

- Include Deleted Files
- Include File Slack
- Include Free Space

For a description of processing options, see *Evidence Processing Options* (page 88)
Creating a Custom Processing Profile
You can create a processing profile by selecting a set of processing options and then saving them as a profile. You can create a processing profile at one of the following times:
- Before creating a case
- While configuring processing options for a new case

To create a custom processing profile
1. From the Case Manager do one of the following:
   - To create a profile before creating a case, do the following:
     1a. Click Manage > Evidence Processing Profiles.
     1b. Click New Profile.
     You can use the Profile dropdown to select an existing profile as a template.
     - To create a profile while creating a new case, do the following:
     1a. Click Case > New.
     1b. In the Processing profile field, select one of the built-in options and click Customize.
2. Do the following:

   2a. Click the Evidence Processing icon in the left pane, and select the processing options to be the default options for the case. For more information, see Evidence Processing Options (page 88).

   2b. Click the Evidence Refinement (Advanced) icon to select the evidence refinement options to use on this case. For more information, see Configuring Evidence Refinement (Advanced) Options (page 109).

   2c. Click the Index Refinement (Advanced) icon to select the index refinement options to use on this case. For more information, see Selecting Index Refinement (Advanced) Options (page 111).

   2d. Click the Evidence Lab/eDiscovery icon to select the advanced options to use on this case. For more information, see Selecting Lab/eDiscovery Options.

Important: When you create a custom profile, the settings for Custom File Identification are not stored in the processing profile. When you configure these options, the Save As... profile button is grayed out to signify that they are not saved as part of a profile.
See Managing Custom Identifiers (page 56).
3. When you are satisfied with your options, click **Save As...** or **Save user Profile...** to create the profile.

4. Enter a name for the profile.
   - To create a new profile, enter a unique name.
     
     You cannot use **AD Standard**, **AD Field Mode**, or **Custom**.
   - To update an existing custom profile, enter the profile name.

5. (Optional) Enter a description of the profile.

6. Click **Save**.

---

**Managing Processing Profiles**

You can do the following to manage processing profiles.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Edit</strong></td>
<td>You can edit an existing custom profile. You cannot edit the five pre-configured profiles. To edit a profile, you select an existing profile, make the desired changes, save the profile, and confirm that you want to replace the existing profile.</td>
</tr>
<tr>
<td><strong>Set as Default</strong></td>
<td>You can set a processing profile as the global default. Whenever you create a new case, the default profile is listed. If a profile not associated with a button has been set as the default, none of the buttons will appear greyed out and the default profile name will appear in the Profiles drop down. The default profile is denoted by a green check mark.</td>
</tr>
<tr>
<td><strong>Delete</strong></td>
<td>You can delete an existing custom profile. You cannot delete the five pre-configured profiles. If you delete a custom profile that has been selected as the default, the profile is deleted and the Forensic processing profile becomes the default.</td>
</tr>
<tr>
<td><strong>Lock/Unlock</strong></td>
<td>You can lock a profile so that others cannot edit or delete it. Any pre-defined profiles cannot be unlocked.</td>
</tr>
<tr>
<td><strong>Export</strong></td>
<td>You can export a custom profile so that you can archive it or use it on a different computer. The exported settings are saved in xml format.</td>
</tr>
<tr>
<td><strong>Import</strong></td>
<td>You can import a profile that has been previously exported.</td>
</tr>
</tbody>
</table>
**To manage processing profiles**
1. In the *Case Manager*, click Manage > Evidence Processing Profiles.
2. In the *Manage Evidence Processing Profiles* dialog, select a profile to manage.
3. Select an action to perform on the profile.
4. Click Close.

**Customizing the Processing Profile Buttons**
It is possible to customize the profiles that appear on the quick-start profile buttons in the New Case Options dialog. This will allow you to access your most commonly used processing profiles with one click. You will need to have already created your custom profiles before associating them with a button. For more information, see *Creating a Custom Processing Profile* (page 84). These changes are global and will be seen by all users.

**Note:** These changes can only be made by an Application Administrator.

**To customize the quick-start profile buttons**
1. In the *Case Manager*, select Manage > Evidence Processing Profiles.

   In the Manage Evidence Processing Profiles dialog you will see a list of all the current profiles along with a short description, if added; a locked indicator; and the button number assigned, if any. The green check mark indicates the default profile.
2. Highlight a profile in the grid and click *Set Button*.

   A window will appear allowing you to choose a number for that button. The numbers correspond to the button location, 1 being all the way to the left and 5 being all the way to the right.
3. Once you have selected a position, click *Save*.

   The new option will now be shown on the selected button. The profile option formerly in that position will no longer be associated with a button, but will still be shown in the Profile drop down list.
Manually Customizing a set of Detailed Options
You can configure default processing options for a case without saving it as a profile.

To manually customize the evidence processing options
1. From the New Case Options dialog, click Custom.

1a. Click the Evidence Processing icon in the left pane, and select the processing options to be the default options for the case. For more information, see Evidence Processing Options (page 88).
1b. Click the Evidence Refinement (Advanced) icon to select the evidence refinement options to use on this case. For more information, see Configuring Evidence Refinement (Advanced) Options (page 109).
1c. Click the Index Refinement (Advanced) icon to select the index refinement options to use on this case. For more information, see Selecting Index Refinement (Advanced) Options (page 111).
1d. Click Custom File Identification to configure Custom Identifiers. For more information, see Managing Custom Identifiers (page 56).
2. Click OK.

In the Processing Profile field, it will display Custom to show that you did not save the options as a profile.
3. When you are satisfied with your evidence refinement options, click OK to create the case and continue to the Evidence Processing screen.
Evidence Processing Options

The following table outlines the Evidence Processing options.

**Evidence Processing Options**

<table>
<thead>
<tr>
<th>Process</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MD5 Hash</td>
<td>Creates a digital fingerprint using the Message Digest 5 algorithm, based on the contents of the file. This fingerprint can be used to verify file integrity and to identify duplicate files.</td>
</tr>
<tr>
<td>SHA-1 Hash</td>
<td>Creates a digital fingerprint using the Secure Hash Algorithm-1, based on the contents of the file. This fingerprint can be used to verify file integrity and to identify duplicate files.</td>
</tr>
<tr>
<td>SHA-256 Hash</td>
<td>Creates a digital fingerprint using the Secure Hash Algorithm-256, based on the contents of the file. This fingerprint can be used to verify file integrity and to identify duplicate files. SHA-256 is a hash function computed with 32-bit words, giving it a longer digest than SHA-1.</td>
</tr>
<tr>
<td>PHash</td>
<td>Creates a Perpetual Hash for a multimedia file derived from a feature of its contents.</td>
</tr>
<tr>
<td>Flag Duplicate Files</td>
<td>Identifies files that are found more than once in the evidence. This is done by comparing file hashes.</td>
</tr>
<tr>
<td>KFF</td>
<td>Enables the Known File Filter (KFF) that lets you identify either known insignificant files that you can ignore or known illicit or dangerous files that you want to be alerted to.</td>
</tr>
<tr>
<td></td>
<td>When you enable KFF, you must select a KFF Template to use. You can select an existing KFF Template from the drop-down menu or click ... to create a new one.</td>
</tr>
<tr>
<td></td>
<td>See Using the Known File Filter (KFF) on page 362.</td>
</tr>
<tr>
<td>Expand Compound Files</td>
<td>Automatically opens and processes the contents of compound files such as ZIP, email, and OLE files.</td>
</tr>
<tr>
<td></td>
<td>See Expanding Compound Files on page 91.</td>
</tr>
<tr>
<td></td>
<td>The option File Signature Analysis is not forced to be selected. This lets you initially see the contents of compound files without necessarily having to process them. Processing can be done later, if it is deemed necessary or beneficial to the case by selecting File Signature Analysis.</td>
</tr>
<tr>
<td>File Signature Analysis</td>
<td>Analyzes files to indicate whether their headers or signatures match their extensions. This option must be selected if you choose Registry Summary Reports.</td>
</tr>
<tr>
<td>Flag Bad Extensions</td>
<td>Identifies files whose types do not match their extensions, based on the file header information. This option forces the File Signature Analysis option to be checked.</td>
</tr>
<tr>
<td>Entropy Test</td>
<td>Identifies files that are compressed or encrypted. Compressed and encrypted files identified in the entropy test are not indexed.</td>
</tr>
<tr>
<td><strong>Process</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Search Text Index</td>
<td>Stores the words from evidence in an index for quick retrieval. Additional space requirement is approximately 25% of the space required for all evidence in the case.</td>
</tr>
<tr>
<td></td>
<td>Indexing Options...</td>
</tr>
<tr>
<td></td>
<td>See Using dtSearch Text Indexing (page 96) for extensive options for indexing the contents of the case.</td>
</tr>
<tr>
<td></td>
<td>Generated text that is the result of a formula in a document or spreadsheet is indexed, and can be filtered.</td>
</tr>
<tr>
<td>Create Thumbnails for Graphics</td>
<td>Creates thumbnails for all graphics in a case.</td>
</tr>
<tr>
<td></td>
<td>Thumbnails are always created in JPG format, regardless of the original graphic file type.</td>
</tr>
<tr>
<td></td>
<td>See Examining Graphics on page 430.</td>
</tr>
<tr>
<td>Create Thumbnails for Videos</td>
<td>Creates thumbnails for all videos in a case.</td>
</tr>
<tr>
<td></td>
<td>You can also set the frequency for which video thumbnails are created, either by a percent (1 thumbnail every “n”% of the video) or by interval (1 thumbnail every “n” seconds).</td>
</tr>
<tr>
<td></td>
<td>See Examining Videos on page 445.</td>
</tr>
<tr>
<td>Generate Common Video File</td>
<td>When you process the evidence in your case, you can choose to create a common video type for videos in your case. These common video types are not the actual video files from the evidence, but a copied conversion of the media that is generated and saved as an MP4 file that can be previewed on the video tab.</td>
</tr>
<tr>
<td></td>
<td>See Examining Videos on page 445.</td>
</tr>
<tr>
<td>EXIF for Videos</td>
<td>Parses XMP metadata (similar to EXIF data) from processed MP4 and most all other modern video file formats. When parsed from a video file, the metadata values are displayed on the Properties tab of the file viewer pane.</td>
</tr>
<tr>
<td>HEIC Conversion</td>
<td>Converts HEIC formats to be viewed in the Native viewer.</td>
</tr>
<tr>
<td>Enable File Encryption</td>
<td>Enables the detection of encrypted files within an image. Turning this off will allow for faster processing.</td>
</tr>
<tr>
<td>Detection</td>
<td></td>
</tr>
<tr>
<td>HTML File Listing</td>
<td>Creates an HTML version of the File Listing in the case folder.</td>
</tr>
<tr>
<td>CSV File Listing</td>
<td>The File Listing Database is now created in CSV format instead of an MDB file and can be added to Microsoft Access.</td>
</tr>
</tbody>
</table>
### Data Carve

Carves data immediately after pre-processing. Click **Carving Options**, then select the file types to carve. Uses file signatures to identify deleted files contained in the evidence. All available file types are selected by default.

For more information on Data Carving, see [Data Carving](#) (page 99).

### Meta Carve

Carves deleted directory entries and other metadata. The deleted directory entries often lead to data and file fragments that can prove useful to the case, that could not be found otherwise.

### Optical Character Recognition (OCR)

Scans graphics files for text and converts graphics-text into actual text. That text can then be indexed, searched and treated as any other text in the case.

For more detailed information regarding OCR settings and options, see [Optical Character Recognition (OCR)](#) (page 102).

### Process | Description
---|---
Explicit Image Detection | Click **EID Options** to specify the EID threshold for suspected explicit material found in the case.
See [Evaluating Explicit Material](#) on page 436.
EID is an add-on feature. Contact your sales representative for more information.

Registry Reports | Creates Registry Summary Reports (RSR) from case content automatically. Click RSR Directory to specify the location of the RSR Templates. When creating a report, click the RSR option in the Report Wizard to include the RSR reports requested here. RSR requires that File Signature Analysis also be selected. If you try to select RSR first, an error will pop up to remind you to mark File Signature Analysis before selecting RSR.

Include Deleted Files | Excludes deleted files from the case.

Send Email Alert on Job Completion | Opens a text box that allows you to specify an email address where job completion alerts will be sent.

**Note:** Outgoing TCP traffic must be allowed on port 25.

**Important:** These Emails are often filtered into Spam folders.

Decrypt Dell Encryption Files | See [Decrypting Dell Encryption Files (Dell Data Protection | Encryption Server)](#) on page 278.
If you select to decrypt Dell Encryption files, the File Signature Analysis option will automatically be selected as well.

Process Internet Browser History for Visualization | Processes internet browser history files so that you can see them in the detailed visualization timeline.
See [Visualizing Internet Browser History Data](#) on page 588.

Perform Automatic Decryption | Disabled by default. Attempts to decrypt files using a list of passwords that you provide.
<table>
<thead>
<tr>
<th>Process</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Language Translation</td>
<td><strong>DISABLED BY DEFAULT. ANALYZES DOCUMENTS USING SDL MACHINE LEARNING TECHNOLOGIES (USING LANGUAGE KEY PAIRS). LICENSING REQUIRED FOR THIS FEATURE TO FUNCTION.</strong> See Language Translation.</td>
</tr>
<tr>
<td>Language Identification</td>
<td>Disabled by default. Analyzes the first two pages of every document to identify the languages contained within. The user will be able to filter by a Language field within review and determine who needs to review which documents based on the language contained within the document. See Identifying Document Languages on page 462.</td>
</tr>
<tr>
<td>Document Content Analysis</td>
<td>Disabled by default. Analyzes the content and groups it according to topic in the Overview tab. When selected, the DCA Options button is also activated and opens the Document Content Analysis Options. See Analyzing Document Content on page 554.</td>
</tr>
</tbody>
</table>
| Entity Extraction (Document Content) | Disabled by default. Identifies and extracts specific types of data in your evidence. You can select to process one or all of the following types of entity data:  
  - Credit Card Numbers  
  - Phone Numbers  
  - Social Security Numbers  
  In the Examiner, under the Document Content node in the Overview tab, you can view the extracted data. See Using Entity Extraction on page 554.                                                                                                                                                                                                 |
| Generate System Information | Extracts data and populates the System Information tab. See Viewing System Information on page 547.                                                                                                                                                                                                                                                                                                                                                                                   |
| Persons of Interest         | Scraps contact information from email signatures for use in conjunction with the “Communication Participants” list.                                                                                                                                                                                                                                                                                                                                                                                             |

If you expand data, you will have files that are generated when the data was processed and was not part of the original data. There are tools to help you identify generated data. See Identifying Processing-Generated Data on page 452. See Relating Generated Files to Original Files on page 452.
Expanding Compound Files

About Expanding Compound Files

You can expand individual compound file types. This lets you see child files that are contained within a container such as ZIP files. You can access this feature from the Case Manager’s new case wizard, or from the Add Evidence or Additional Analysis dialogs.

See Evidence Processing Options on page 88. You can filter the list of file types. See Filtering the Compound File Expansion Options List on page 95. Some file types are selected to be expanded by default.

Important: If you expand data, you will have files that are generated when the data was processed and were not part of the original data. There are tools to help you identify generated data.


See Relating Generated Files to Original Files on page 452.
You can expand the following compound files:

**Compound File Types**

<table>
<thead>
<tr>
<th>Type</th>
<th>Expansion Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>7-ZIP</td>
<td>Expanded by default</td>
</tr>
<tr>
<td>Active Directory</td>
<td>Not expanded by default</td>
</tr>
<tr>
<td>AFF4</td>
<td>Not expanded by default</td>
</tr>
<tr>
<td>Android APK</td>
<td>Not expanded by default</td>
</tr>
<tr>
<td>BZIP2</td>
<td>Expanded by default</td>
</tr>
<tr>
<td>Cellebrite UFDR</td>
<td>Not expanded by default</td>
</tr>
<tr>
<td>ESE DB</td>
<td>Expands ESE (Extensible Storage Engine) databases. See About Extensible Storage Engine (ESE) Databases on page 465.</td>
</tr>
<tr>
<td>EVT</td>
<td>Not expanded by default</td>
</tr>
<tr>
<td>EVTX</td>
<td>Not expanded by default</td>
</tr>
<tr>
<td>EXIF</td>
<td>Not expanded by default</td>
</tr>
</tbody>
</table>

Exterro Mobile Parsers Not expanded by default – This processing option has replaced previously available mobile options. Utilizing this option will attempt to parse mobile applications if available.

<table>
<thead>
<tr>
<th>Type</th>
<th>Expansion Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>AOL Files</td>
<td>Not expanded by default</td>
</tr>
<tr>
<td>Blackberry IPD backup file</td>
<td>Not expanded by default.</td>
</tr>
<tr>
<td>Chrome Bookmarks</td>
<td>Not expanded by default</td>
</tr>
<tr>
<td>Chrome Cache</td>
<td>Not expanded by default</td>
</tr>
<tr>
<td>Chrome SQLite</td>
<td>Not expanded by default</td>
</tr>
<tr>
<td>DBX</td>
<td>Expanded by default</td>
</tr>
<tr>
<td>EMFSPOOL</td>
<td>Not expanded by default</td>
</tr>
<tr>
<td>EVTX</td>
<td>Not expanded by default</td>
</tr>
<tr>
<td>EXIF</td>
<td>Not expanded by default</td>
</tr>
<tr>
<td>Evidence Processing Options</td>
<td></td>
</tr>
<tr>
<td>----------------------------</td>
<td></td>
</tr>
<tr>
<td>Creating and Configuring New Cases</td>
<td></td>
</tr>
</tbody>
</table>

Firefox Cache  Not expanded by default. See About Expanding Google Chrome, Firefox, and IE 9 Data on page 466.

Firefox JSON  Not expanded by default. See About Expanding Google Chrome, Firefox, and IE 9 Data on page 466.

Firefox SQLite  Not expanded by default. See About Expanding Google Chrome, Firefox, and IE 9 Data on page 466.

GZIP  Expanded by default

IE Cookie Text (IE 10 and newer)  Not expanded by default. See About Expanding Data from Internet Explorer (IE) Version 10 or Later on page 467.

IE Recovery (IE 10 and newer)  Not expanded by default. Expands IE Recovery data that was stored when access to a Web site was lost.

See Expanding Internet Artifact Data on page 469.

IE WebCache (IE 10 and newer)  Not expanded by default. Expands the Web cache data for IE 10 and later IE versions. See About Expanding Data from Internet Explorer (IE) Version 10 or Later on page 467.

IIS Log  Not expanded by default. See Viewing IIS Log File Data on page 455.

Internet Explorer Files (IE 9)  Not expanded by default.

Expands Internet Explorer internet artifact data. See Expanding Internet Artifact Data on page 469.

iOS Backup  Not expanded by default. See Working with iOS Backup on page 479.

iOS WeChat  Not expanded by default.

iOS WhatsApp  Not expanded by default.

Log2t CSV  Not expanded by default. This processing option will recognize CSV filesthat are in the Log2timeline format and parses the data within the singleCSV into individual records within the case. The individual records from the CSV will be interspersed with other data, giving you the ability to perform more advanced timeline analysis across a very broad set of data. In addition you can leverage the visualization engine to perform more advanced timeline based visual analysis.

See Log2timeline CSV fields on page 461.

Lotus Notes (NSF)  Not expanded by default.
<table>
<thead>
<tr>
<th>File Type</th>
<th>Expansion Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mail.ru Chat</td>
<td>Expanded by default. Parses Mail.RU Agent chat history files and email(mra.dbs). See <a href="#">Expanding Internet Artifact Data</a> on page 469.</td>
</tr>
<tr>
<td>MBOX</td>
<td>Expanded by default</td>
</tr>
<tr>
<td>McAfee Log</td>
<td>Not expanded by default.</td>
</tr>
<tr>
<td>Microsoft Exchange (EDB)</td>
<td>Expanded by default. Exchange 2013 and previous onlyMS Office, OLE and OPC documents Not expanded by default.</td>
</tr>
<tr>
<td>MSG</td>
<td>Expanded by default</td>
</tr>
<tr>
<td>OpenSSH known_hosts File</td>
<td>Not expanded by default. Outlook for Mac OLM Not expanded by default.</td>
</tr>
<tr>
<td>PDF</td>
<td>Expanded by default</td>
</tr>
<tr>
<td>Pidgin Chat Log</td>
<td>Not expanded by default.</td>
</tr>
<tr>
<td>PKCS7 and S/MIME Files</td>
<td>Expanded by default</td>
</tr>
<tr>
<td>PST</td>
<td>Expanded by default</td>
</tr>
<tr>
<td>RAR</td>
<td>Expanded by default</td>
</tr>
<tr>
<td>Registry (full)</td>
<td>Not expanded by default.</td>
</tr>
<tr>
<td>Registry (timeline)</td>
<td>Not expanded by default. See <a href="#">Viewing Registry Timeline Data</a> on page 457.</td>
</tr>
<tr>
<td>RFC822 Internet Email</td>
<td>Expanded by default</td>
</tr>
<tr>
<td>Skype SQLite</td>
<td>Not expanded by default. See <a href="#">Expanding Internet Artifact Data</a> on page 469.</td>
</tr>
<tr>
<td>SQLite Databases</td>
<td>Not expanded by default.</td>
</tr>
<tr>
<td>TAR</td>
<td>Expanded by default</td>
</tr>
<tr>
<td>Unistore Database (Windows 10 Mail)</td>
<td>Not expanded by default. See <a href="#">Processing Windows 10 Email and Contacts</a> on page 428.</td>
</tr>
<tr>
<td>Windows Firewall Log</td>
<td>Not expanded by default.</td>
</tr>
<tr>
<td>Windows Registry.pol</td>
<td>Not expanded by default.</td>
</tr>
<tr>
<td>Evidence Processing Options</td>
<td></td>
</tr>
<tr>
<td>-----------------------------</td>
<td></td>
</tr>
<tr>
<td>Windows Thumbnails Not expanded by default.</td>
<td></td>
</tr>
<tr>
<td>XRY Not expanded by default.</td>
<td></td>
</tr>
<tr>
<td>X-Ways Not expanded by default.</td>
<td></td>
</tr>
<tr>
<td>ZIP, including ZIPX Expanded by default</td>
<td></td>
</tr>
</tbody>
</table>
Be aware of the following before you expand compound files:

- If you have labeled or hashed a family of files, then later choose to expand a compound file type that is contained within that label or family, the newly expanded files do not inherit the labeling from the parent, and the family hashes are not automatically regenerated.

- Many Lotus Notes emails, *.NSF, are being placed in the wrong folders in the Examiner.

This is a known issue wherein Lotus Notes routinely deletes the collection indexes. Lotus Notes client has the ability to rebuild the collections from the formulas, but Examiner cannot. So if Lotus Notes data is acquired shortly after the collections have been cleared, then the Examiner does not know where to put the emails. These emails are all placed in a folder named ",[other1]."

To work around: Open the NSF file in the Lotus Notes client, and then close (you may need to save), then acquire the data and process it. The emails will all be in the right folder because the view collections are recreated.

- Compound file types such as AOL, Blackberry IPD Backup, EMFSpool, EXIF, MSG, PST, RAR, and ZIP can be selected individually for expansion. This feature is available from the Case Manager new case wizard, or from the Add Evidence or Additional Analysis dialogs.

- Only the file types selected are expanded. For example, if you select ZIP, and a RAR file is found within the ZIP file, the RAR is not expanded.
Filtering the Compound File Expansion Options List

It is possible to filter the Compound File Expansion Options list by category. Use the Categories dropdown at the top of the list to select a category. Use the Select All and Clear All buttons to select or clear all options within the selected category.

The following categories can be used to filter:

### Compound File Expansion Options Category List

<table>
<thead>
<tr>
<th>Category</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>All</td>
<td>This is the full list of supported Compound File Expansion Options.</td>
</tr>
<tr>
<td>All Communications</td>
<td>This option includes all supported file types that are used for communication.</td>
</tr>
<tr>
<td>All Mobile</td>
<td>This option includes all supported file types found on any mobile device.</td>
</tr>
<tr>
<td>Android</td>
<td>This option includes all supported file types found on Android devices.</td>
</tr>
<tr>
<td>Archives</td>
<td>This option includes all supported archive file types.</td>
</tr>
<tr>
<td>Browsers</td>
<td>This option includes all supported file types used within a browser.</td>
</tr>
<tr>
<td>Email</td>
<td>This option includes all supported email file types.</td>
</tr>
<tr>
<td>Other Forensic Tools</td>
<td>This option includes all supported (third-party) evidence filetypes.</td>
</tr>
<tr>
<td>Logs</td>
<td>This option includes all supported log file types.</td>
</tr>
<tr>
<td>Windows</td>
<td>This option includes all supported file types used within a Windows system.</td>
</tr>
</tbody>
</table>

Selecting the Cancel button will erase all changes and the default options will populate if the dialog is re-opened.
Selecting File Type to Expand

**To expand compound files**
1. Do one of the following:
   - For new cases, in the New Case Options dialog click Detailed Options.
   - For existing cases, in the Examiner, click Evidence > Additional Analysis.
2. Select Expand Compound Files.

The option File Signature Analysis is no longer forced to be checked when you select **Expand Compound Files**. This lets you see the contents of compound files without necessarily having to process them. You can choose to process them later, if it is deemed necessary or beneficial to the case.
3. Select **Include Deleted Files** if you also want to expand deleted compound files.
4. Click Expansion Options.
5. In the Compound File Expansions Options dialog do the following:
   - If you do not want to expand office documents that do not have embedded items, select **Only expand office documents with embedded items**.
   - Select the types of compound files that you want expand.

Only the file types that you select are expanded. For example, if you select ZIP, and a RAR file is contained within the ZIP file, then the RAR is not expanded.

**Note:** The option File Signature Analysis is not forced to be selected. This lets you initially see the contents of compound files without necessarily having to process them. Processing can be done later, if it is deemed necessary or beneficial to the case by selecting File Signature Analysis.

6. In the Compound File Expansions Options dialog, click **OK**.
7. Click **OK**.
Using dtSearch Text Indexing
You can use the following indexing options to choose from when creating a new case.

Indexing a Case
All evidence should be indexed to aid in searches. Index evidence when it is added to the case by checking the dtSearch Text Index box on the Evidence Processing Options dialog, or index after the fact by clicking and specifying indexing options.
Scheduling is another factor in determining which process to select. Time restraints may not allow for all tasks to be performed initially. For example, if you disable indexing, it shortens the time needed to process a case. You can return at a later time and index the case if needed.

dtSearch Indexing Space Requirements
To estimate the space required for a dtSearch Text index, plan on approximately 25% of the space needed for each case's evidence.

Configuring Case Indexing Options
Case Indexing gives you almost complete control over what goes in your case index. These options can be applied globally from Case Manager. These options must be set prior to generating the index.

Note: Search terms for pre-processing options support only ASCII characters.
To set Indexing Options as the global default

1. In Case Manager, click Case > New > Detailed Options.
2. In the Evidence Processing window, mark the dtSearch Text Index check box.
3. Click Indexing Options to bring up the Indexing Options dialog box.
4. Set the options using the information in the following table:

### dtSearch Indexing Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Letters</td>
<td>Specifies the letters and numbers to index. Specifies Original, Lowercase, Uppercase, and Unaccented. Choose Add or Remove to customize the list. By default, the @ symbol is treated as a letter and is included in the search index.</td>
</tr>
<tr>
<td>Noise Words</td>
<td>A list of words to be considered “noise” and ignored during indexing. Choose Add or Remove to customize the list.</td>
</tr>
<tr>
<td>Hyphens</td>
<td>Specifies which characters are to be treated as hyphens. You can add standard keyboard characters, or control characters. You can remove items as well. By default, underscore characters (“_”) are listed in the Hyphens box and are therefore subject to the option selected under Hyphen Treatment.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hyphen Treatment</td>
<td>Specifies how hyphens are to be treated in the index. Options are:</td>
</tr>
<tr>
<td></td>
<td>• Ignore</td>
</tr>
<tr>
<td></td>
<td>Hyphens will be treated as if they never existed. For example, the term “counter-culture” would be indexed as “counterculture.”</td>
</tr>
<tr>
<td></td>
<td>• Hyphen</td>
</tr>
<tr>
<td></td>
<td>Hyphens will be treated literally. For example, the term “counter-culture” would be indexed as “counter-culture.”</td>
</tr>
<tr>
<td></td>
<td>• Space</td>
</tr>
<tr>
<td></td>
<td>Hyphens will be replaced by a non-breaking space. For example the term “counter-culture” would be indexed as two separate entries in the index being “counter” and “culture.”</td>
</tr>
<tr>
<td></td>
<td>• All</td>
</tr>
<tr>
<td></td>
<td>Terms with hyphens will be indexed using all three hyphen treatments. For example the term “counter-culture” will be indexed as “counterculture”, “counter-culture”, and as two separate entries in the index being “counter” and “culture.”</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Spaces</td>
<td>Specifies which special characters should be treated as spaces. Remove characters from this list to have them indexed as any other text. Choose Add or Remove to customize the list.</td>
</tr>
<tr>
<td></td>
<td>For example, to have the @ symbol not included in the index, you would need to do two things:</td>
</tr>
<tr>
<td></td>
<td>● Remove the @ from the Letters list.</td>
</tr>
<tr>
<td></td>
<td>● Add the @ to the Spaces list.</td>
</tr>
<tr>
<td>Ignore</td>
<td>Specifies which control characters or other characters to ignore. Choose Add or Remove to customize the list.</td>
</tr>
<tr>
<td>Max Word Length</td>
<td>Allows you to set a maximum word length to be indexed.</td>
</tr>
<tr>
<td>Index Binary Files</td>
<td>Specify how binary files will be indexed. Options are:</td>
</tr>
<tr>
<td></td>
<td>● Index all</td>
</tr>
<tr>
<td></td>
<td>● Skip</td>
</tr>
<tr>
<td></td>
<td>● Index all (Unicode)</td>
</tr>
<tr>
<td>Enable Date Recognition</td>
<td>Choose to enable or disable this option</td>
</tr>
<tr>
<td></td>
<td>Presumed Date Format For Ambiguous Dates</td>
</tr>
<tr>
<td></td>
<td>If date recognition is enabled, specify how ambiguous dates should be formatted when encountered during indexing. Options are:</td>
</tr>
<tr>
<td></td>
<td>● MM/DD/YY</td>
</tr>
<tr>
<td></td>
<td>● DD/MM/YY</td>
</tr>
<tr>
<td></td>
<td>● YY/MM/DD</td>
</tr>
<tr>
<td>Set Max Memory</td>
<td>Allows you to set a maximum size for the index.</td>
</tr>
<tr>
<td>Auto-Commit Interval(MB)</td>
<td>Allows you to specify an Auto-Commit Interval while indexing the case. When the index reaches the specified size, the indexed data is saved to the index. The size resets, and indexing continues until it reaches the maximum size, and saves again, and so forth.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Cache Filtered Text in the index</td>
<td>Filtered Text is being cached in the dtSearch index by default, however it can be toggled on or off. The advantage to caching filtered text is that it produces more reliable search hit highlighting and it reduces the time to return index search results. However, NOT caching filtered text will result in a smaller index and shorter time to complete the indexing process.</td>
</tr>
<tr>
<td>Modify for TR1 expressions</td>
<td>Configures the indexing engine to index TR1 regular expressions. See Using dtSearch Regular Expressions on page 529.</td>
</tr>
</tbody>
</table>
| Create optional accent sensitive index | Generates the index in such a way that, when the “Accents are Significant” option is enabled for index searching, the investigator can optionally control whether characters with accent marks are distinguished from those without. For example “abc” versus “äbc”.  
FTK has always and still does default to an Accent Sensitive Index. This means that "abc" will only find "abc" and "äbc" will only find "åbc". In Examiner, the "Index Search" tab’s “Options...” dialog an option called “Accents are significant” will appear in cases where an Accent Sensitive Index has been generated and can be selected to control how accents are treated.  
See Selecting Index Search Options (page 526) for more information on the “Accents are Significant” search option.                                                                                                                                                                                                                                           |

**Note:** The Indexing Options dialog does not support some Turkish characters.

5. When finished setting Indexing Options, click **OK** to close the dialog.
6. Complete the **Detailed Options** dialog.
7. Click **OK** to close the **Detailed Options** dialog.
8. Specify the path and filename for the **Default Options** settings file.
9. **Click Save.**
10. In the **Case Manager**, click **Case > New**.
11. Proceed with case creation as usual. There is no need to click **Detailed Options** again in creating the case to select options, unless you wish to use different settings for this case.
In addition to performing searches within the case, you can also use the Index to export a word list to use as a source file for custom dictionaries to improve the likelihood and speed of password recovery related to case files when using the Password Recovery Toolkit (PRTK). You can export the index by selecting File > Export Word List. See also Searching Evidence with Index Search (page 521).

**Data Carving**

Data carving is the process of looking for data on media that was deleted or lost from the file system. Often this is done by identifying file headers and/or footers, and then "carving out" the blocks between these two boundaries.

AccessData provides several specific pre-defined carvers that you can select when adding evidence to a case. In addition, Custom Carvers allow you to create specific carvers to meet your exact needs.

Data carving can be selected in the New Case Wizard as explained below, or from within the Examiner. In addition, because Custom Carvers are now a Shared feature, they can be accessed through the Manage menu. These are explained below.

### Pre-defined Carvers

The following pre-defined carvers are available. Some carvers are enabled by default.

<table>
<thead>
<tr>
<th>Carver</th>
<th>Enabled by default?</th>
</tr>
</thead>
<tbody>
<tr>
<td>AOL bag files</td>
<td>No</td>
</tr>
<tr>
<td>BMP files</td>
<td>No</td>
</tr>
<tr>
<td>EMF files</td>
<td>No</td>
</tr>
<tr>
<td>GIF files</td>
<td>No</td>
</tr>
<tr>
<td>HTML files</td>
<td>No</td>
</tr>
<tr>
<td>JPEG files</td>
<td>No</td>
</tr>
<tr>
<td>LNK files</td>
<td>No</td>
</tr>
<tr>
<td>OLE files (MS Office)</td>
<td>No</td>
</tr>
<tr>
<td>PDF files</td>
<td>No</td>
</tr>
<tr>
<td>PNG files</td>
<td>No</td>
</tr>
<tr>
<td>SQLite DB Files</td>
<td>No</td>
</tr>
<tr>
<td>TIFF files</td>
<td>No</td>
</tr>
<tr>
<td>ZIP files</td>
<td>No</td>
</tr>
</tbody>
</table>
Selecting Data Carving Options

If you are unfamiliar, please review Creating a Case (page 78) and Configuring Detailed Options for a Case (page 79) before beginning this section.

When you are in the New Case Wizard in Detailed Options > Evidence Processing, click Data Carve > Carving Options to open the dialog shown below.

If you already have a case open with evidence added and processed, click the following:

- Evidence > Additional Analysis > Data Carve > Carving Options

Standard Data Carving gives you a limited choice of which file types to carve. Choose which types of data to carve according to the information below.

To set Data Carving options
1. Select Data Carve.
2. Click Carving Options.
3. Select the types of files you want carved.
   - Click Select All to select all file types to be carved.
   - Click Clear All to unselect all file types.
   - Click on individual file types to toggle either selected or unselected.

**Note:** It may help to be aware of the duplicate files and the number of times they appear in an evidence set to determine intent.

4. Depending on the file type highlighted, the Selected Carver Options may change. Define the optional limiting factors to be applied to each file:
   - Define the minimum byte file size for the selected type.
   - Define the minimum pixel height for graphic files.
   - Define the minimum pixel width for graphic files
5. Mark the box, Exclude KFF Ignorable files if needed.
6. If you want to define Custom Carvers, click Custom Carvers. (Custom Carvers are explained in the next section.) When you are done with Custom Carvers, click Close.
7. In the Carving Options dialog, click OK.
Custom Carvers

The Custom Carvers dialog allows you to create your own data carvers in addition to the built-in carvers. Custom Carvers can be created and shared from within a case, or from the Case Manager. Application Administrators have the necessary permissions to access the Manage Shared Carvers dialog. Case Administrators can manage the Custom Carvers in the cases they administer. Case Reviewers are not allowed to manage Custom Carvers.

Shared Custom Carvers are automatically available globally; but can be copied to a case when needed. Carvers created within a case are automatically available to the case, but can be shared and thus made available globally.

To access Manage Custom Carvers dialogs, click Manage > Carvers > Manage Custom Carvers (or Manage Shared Carvers if you are an Application Administrator).

The Manage Shared Custom Carvers and Manage Custom Carvers dialogs are very similar. The difference is whether you can copy the carvers to a case or make the carvers shared.

The Custom Carvers dialog allows you to define carving options for specific file types or information beyond what is built-in. Once defined, these carving options files can be Shared with the database as well as exported and imported for use in other cases. The original, local copy, remains in the case where it was created, for local management.

Additional Multimedia Carvers have been created by Exterro. Refer to the Multimedia Carvers KB article.

To create a Custom Data Carver

1. Click New.
2. Complete the data fields for the Custom Carver you are creating. Options are as follows:

   - Name: Name of the Carver
   - Author: Name of the Creator
   - Description: Summarizes the intended use of the carver
   - Minimum File Size in bytes (Optional)
   - Maximum File Size (Optional) in bytes

The default Custom Carver Maximum File Size is 2147483647 bytes.

The carver Max File Size in bytes must be populated with any size larger than the defined Minimum File Size in bytes (default is 0). A Maximum File Size equal to or less than the minimum size, or <no entry>, results in an error prompting for a valid number to be entered.
• File extension:
  Defining the extension of the carved file helps with categorization, sorting, and filtering carved files along with other files in the case.

• Key Signature(s) and Other Signature(s):
  Enter the ASCII text interpretation of the file signature as seen in a hex viewer. Many can be defined, but at least one key signature must be present in the file inorder to be carved.

  Click the + icon to begin defining a new Key Signature or Other Signature. Click the - icon to remove a defined Key Signature or Other Signature.

• File Category:
  The File Category the carved item will belong to once it is carved. The specified category must be a leaf node in the Overview tab.

  • Offset: Use decimal value.
  • Length: The length in bytes.
  • Little Endian: If not marked, indicates Big Endian.
  • Signature: Enter the ASCII text interpretation of the file signature as seen in a hex viewer.
  • Case Insensitive: Default is case sensitive. Mark to make the end File Tag Signature not case sensitive.

3. When done defining the Custom Carver, click **Close**.

**Note:** When adding signatures to a carver, the **Signature is case sensitive** check box is used when carving for signatures that can be both upper or lower case. For example, `<HTML>` and `<html>` are both acceptable headers for HTML files, but each of these would have a different signature in hex, so therefore they are case sensitive.

  • The objects and files carved from default file types are automatically added to the case, and can be searched, bookmarked, and organized along with the existing files.

However, custom carved data items are not added to the case until they are processed, and they may not sort properly in the File List view. They are added to the bottom of the list, or at the top for a Z-to-A search, regardless of the filename.
**Optical Character Recognition (OCR)**

Optical Character Recognition (OCR) processing identifies text contained in graphic image files. The text is then indexed so that it can be searched, and bookmarked. Two separate OCR engines are available within the application. The “LeadTools” OCR engine can be selected in the Case Processing and Additional Analysis areas LeadTools of the application interface. The ABBYY FineReader OCR engine integration is available as a separate add-on tool (with separate license from ABBYY).

See ABBYY FineReader Integration on page 103. See LeadTools OCR Analysis on page 104. See LeadTools Optical Character Recognition (OCR) Confidence Score on page 104.

**Important:** Before running OCR analysis, be aware of the following:
- OCR is only a helpful tool for the investigator to locate images from index searches. OCR results should not be considered evidence without further review.
- OCR can have inconsistent results. OCR engines by nature have error rates. This means that it is possible to have results that differ between processing jobs on the same machine with the same piece of evidence.
- Some large images can cause OCR to take a very long time to complete. Under some circumstances, they may not generate any output.
- Graphical images that have no text or pictures with unaligned text can generate bad output.
- OCR works best on typewritten text that is cleanly scanned or similarly generated. Text from other graphic files can generate unreliable output that can vary from run to run.
- Once a graphic image object from a case has been processed by one of the two OCR engines, it is flagged as having completed OCR and will therefore not be submitted for further OCR processing on subsequent runs of either OCR engine jobs.
- ABBYY OCR processing does not calculate an OCR confidence score for processed graphics.
ABBYY FineReader Integration

FTK can leverage the AccessData Quin-C API to access the ABBYY FineReader OCR engine integration which provides a robust alternative OCR engine for indexing graphic image files. In addition to an AccessData Quin-C installation, the ABBYY product integration requires an add-on component installation and a license sold separately from ABBYY (not included with AccessData licensing). For more information on the steps to integrate and configure ABBYY for use with FTK, please refer to the AccessData KB article regarding ABBYY FTK / Quin-C integration. The option to “Run ABBYY OCR Processing” in the examiner interface will be grayed out until properly installed and configured.

When run, the ABBYY OCR Processing option will automatically OCR all graphic image files within the case that have not already been submitted for OCR analysis.

To Run ABBYY OCR Processing
1. Open the case into the examiner interface.
2. Select Tools >> Run ABBYY OCR Processing... to start the OCR job.
3. The Data Processing Status window appears.
4. Wait until the processing job completes.
5. At this point, the text in the graphics submitted for OCR processing should be search-able via the index search tab.
Running LeadTools OCR engine against a file type creates a new child file item. The graphic files are processed normally, and another file with the parsed text from the graphic is created. The new OCR file is named the same as the parent graphic, [graphicname.ext], but with the extension OCR, for example, graphicname.ext.ocr.

You can view the graphic files in the File Content View when it is selected in the File List View. The Natural tab shows the graphic in its original form. The Filtered tab shows the OCR text that was added to the index.

To run LeadTools Optical Character Recognition
1. Do one of the following:
   - For new cases, in the New Case Options dialog click Detailed Options.
   - For existing cases, in the Examiner, click Evidence > Additional Analysis.
2. Select Optical Character Recognition. OCR requires File Signature Analysis and dtSearch Indexing to be selected. When Optical Character Recognition is marked, the other two options are automatically marked and grayed-out to prevent inadvertent mistakes, and ensure successful processing.
3. Click OCR Options.
4. In the OCR Options dialog, select from the following options:

<table>
<thead>
<tr>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>File Types</td>
<td>Lets you specify which file types to include in the OCR process during case processing. For PDF files, you can also control the maximum filtered text size for which to run OCR against.</td>
</tr>
<tr>
<td>Filtering Options</td>
<td>Lets you specify a range in file size to include in the OCR process. You can also specify whether or not to only run OCR against black and white, and grayscale. The Restrict File Size option is selected by default. By default, OCR file generation is restricted to files larger than 5K. If you do not want to limit the size of OCR files, you must disable this option.</td>
</tr>
<tr>
<td>Engine</td>
<td>Lets you choose the OCR engine to use.</td>
</tr>
</tbody>
</table>

5. In the OCR Options dialog, click OK.
6. In the Evidence Processing dialog, click OK.
LeadTools Optical Character Recognition (OCR) Confidence Score

There is an option to show the confidence score for each file that has been processed with OCR. It is recommended to use this feature to sort documents processed using OCR to determine which files may need to be manually reviewed for the desired keywords. The OCR Confidence Score value may be one of the following:

<table>
<thead>
<tr>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-100%</td>
<td>The OCR confidence % score for a document that had a successful OCR process; the higher the score, the higher the confidence.</td>
</tr>
<tr>
<td>No Score Available (2)</td>
<td>The OCR results are from a previous version.</td>
</tr>
<tr>
<td>Minimal Confidence (1)</td>
<td>The OCR extraction is not in a supported language or is not clear.</td>
</tr>
<tr>
<td>No Text Found (0)</td>
<td>The OCR process did not identify any text to extract.</td>
</tr>
<tr>
<td>OCR Skipped (-1)</td>
<td>The OCR process was skipped due to some condition.</td>
</tr>
<tr>
<td>OCR Extraction Error (-2)</td>
<td>The OCR process failed for that file.</td>
</tr>
<tr>
<td>Blank</td>
<td>The file does not need the OCR process; for example, a .DOC file or email.</td>
</tr>
</tbody>
</table>

**Note:** For data that is upgraded from a previous version, if a file has been previously processed with OCR, it will show a value of 2. You can use the Additional Analysis tool, found in the Evidence menu, to re-OCR the document and you will get the new OCR confidence score.

**To use the OCR Confidence Score**

1. Process your data using the Optical Character Recognition option. See Optical Character Recognition (OCR) on page 102.
2. Add the OCR Graphic column to the File List.

See Managing Columns on page 613.
3. Sort the File List using the OCR Graphic column

Use the scores shown in the File List to determine which items should be reviewed for keywords.
Using Explicit Image Detection

About Explicit Image Detection
Explicit Image Detection (EID) is an add-on feature. Contact your sales representative for more information. EID reads all graphics in a case and assigns both the files and the folders they are contained within a score according to what it interprets as being possibly illicit content. The score ranges are explained later in this section.

To add EID evidence to a case
1. Click Evidence > Add/Remove.
2. In the Detailed Options > Evidence Processing dialog, ensure that File Signature Analysis is marked.
3. Select Explicit Image Detection
4. Click EID Options. The three EID options are profiles that indicate the type of filtering that each one does. You can choose between any combination of the following profiles depending on your needs:

<table>
<thead>
<tr>
<th>Profile Name</th>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>X-DFT</td>
<td>Default (XS1)</td>
<td>This is the most generally accurate. It is always selected.</td>
</tr>
<tr>
<td>X-FST</td>
<td>Fast (XTB)</td>
<td>This is the fastest. It scores a folder by the number of files it contains that meet the criteria for a high likelihood of explicit material. It is built on a different technology than X-DFT and does not use &quot;regular&quot; DNAs. It is designed for very high volumes, or real-time page scoring. Its purpose is to quickly reduce, or filter, the volume of data to a meaningful set.</td>
</tr>
<tr>
<td>X-ZFN</td>
<td>Less False Negatives (XT2)</td>
<td>This is a profile similar to X-FST but with more features and with fewer false negatives than X-DFT. You can apply this filter after initial processing to all evidence, or to only the folders that score highly using the X-FST option. Check-mark or highlight those folders to isolate them for Additional Analysis. In Additional Analysis, File Signature Analysis must be selected for EID options to work correctly.</td>
</tr>
</tbody>
</table>

5. When the profile is selected, click OK to return to the Evidence Processing dialog and complete your selections.

AccessData recommends that you run Fast (X-FST) for folder scoring, and then follow with Less FalseNegatives
(X-ZFN) on high-scoring folders to achieve the fastest, most accurate results.

After you select EID in Evidence Processing or Additional Analysis, and the processing is complete, you must select or modify a filter to include the EID related columns in the File List View.

Including Registry Reports
   The Registry Viewer supports Registry Summary Report (RSR) generation as part of case processing.

To generate Registry Summary Reports and make them available for the case report
1. Ensure that File Signature Analysis is marked.
2. Mark Registry Reports.
3. Click RSR Directory.
4. Browse to the location where your RSR templates are stored.
5. Click OK.

Send Email Alert on Job Completion
   You can choose to send an email notification when a job completes. This encompasses both evidence being added to or removed from a case.

   This option is also available from Evidence > Additional Analysis. Select Send Email Alert on Job Completion, click on the Email Alert Options button, and enter the email address of the recipient(s) in the Job Completion Alert Address box, then click OK. To alert all case users, check the Email notification to all case users box.

To set up email notification information
1. In the Case Manager, select a database and log in.
2. Navigate to Manage > Email notification settings. The Manage Email Alert Settings dialog will open.
3. Fill in the Manage Email Alert Settings dialog with the appropriate information.
4. If you choose to send a Test Alert, enter the appropriate addresses into the Send Test Alert box and press Send.
5. Click OK.

   Note: Outgoing TCP traffic must be allowed on port 25.

Custom File Identification Options
   Custom File Identification provides the examiner a way to specify which file category or extension
should be assigned to files with a certain signature. These dialogs are used to manage custom identifiers and extension maps specific to the case.

In Detailed Options, the Custom File Identification dialog lets you select the Custom Identifier file to apply to the new case. This file is stored on the system in a user-specified location. The location can be browsed to, by clicking Browse, or reset to the root drive folder by clicking Reset.

**Creating Custom File Identifiers**

Custom File Identifiers are used to assign categories to files that may or may not already be automatically categorized in a way that is appropriate for the case. For example, a file that is discovered, but not categorized, will be found under the “Unknown Types” category. You can prevent this categorization before the evidence is processed by selecting a different category and sub-category.

Custom Identifiers provide a way for you to create and manage identifiers, and categorize the resulting files into any part of the category tree on the Overview tab. You can select from an existing category, or create a new one to fit your needs.

You can define identifiers using header information expected at a specific offset inside a file, as is now the case, but in addition, you can categorize files based on extension.

**Note:** PDF files are now identified through the PDF file system and will no longer be identified through Custom File Identification.

**To create a Custom Identifier file**

1. In the Case Manager, click Case > New > Detailed Options.
2. Click Custom File Identification.
4. Fill in the fields with the appropriate values. The following table describes the parameters for Custom File Identifiers:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The value of this field defines the name of the sub-category that will appear below the selected Overview Tree category and the category column.</td>
</tr>
<tr>
<td>Description</td>
<td>Accompanies the Overview Container’s tree branch name.</td>
</tr>
</tbody>
</table>
Creating and Configuring New Cases

<table>
<thead>
<tr>
<th>Category</th>
<th>The general file category to which all files with a matching file signature should be associated.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Offset</td>
<td>The decimal offset of where the unique signature (see Value) can be found within the file given that the beginning of the file is offset 0.</td>
</tr>
<tr>
<td>Value</td>
<td>Any unique signature of the file expressed in hexadecimal bytes.</td>
</tr>
</tbody>
</table>

**Note:** The Offset must be in decimal format. The Value must be in hexadecimal bytes. Otherwise, you will see the following error: Hex strings in the Offset field cause an exception error.

"Exception: string_to_int: conversion failed was thrown."

**Important:** After creating a Case Custom File Identifier, you must apply it, or it will not be saved.

5. When you are done defining the Custom File Identifier, click **Make Shared** to share it to the database. This action saves it so the Application Administrator can manage it.

6. Click **OK** to close the dialog. Select the identifier you just created and apply it to the case you are creating. Otherwise it will not be available locally in the future.

Custom Case Extension Maps

Extension Maps can be used to define or change the category associated to any file with a certain file extension. For example, files with BAG extension, which would normally be categorized as “Unknown Type,” can be categorized as an AOL BAG file, or files with a MOV extension, that would normally be categorized as Apple QuickTime video files, can be changed to show up under a more appropriate category since they can sometimes contain still images.

**To create a Case Custom Extension Mapping**

1. Within the **Detailed Options** dialog of the **New Case** wizard, select **Custom File Identification** on the left hand side.

2. Under the **Extension Maps** column, click **New**.

3. Fill in the fields with the appropriate values.

4. Mark **Make Shared** to share this Custom Extension Mapping with the database.

Shared features such as Custom Extension Mappings are managed by the Application Administrator. Your copy remains in the case for you to manage as needed.

The following table describes the parameters for Custom Extension Mappings:
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The value of this field defines the name of the sub-category that will appear below the selected Overview Tree category and the category column.</td>
</tr>
<tr>
<td>Category</td>
<td>The general file category to which all files with a matching file signature should be associated.</td>
</tr>
<tr>
<td>Description</td>
<td>Accompanies the Overview Container's tree branch name.</td>
</tr>
<tr>
<td>Extensions:</td>
<td>Any file extension that should be associated to the selected Category.</td>
</tr>
</tbody>
</table>

**Note:** You must use at least one offset:value pair (hence the [...]+), and use zero or more OR-ed offset:value pairs (the [...]*). All of the offset:value conditions in an OR-ed group are OR-ed together, then all of those groups are AND-ed together.
Configuring Evidence Refinement (Advanced) Options

The Evidence Refinement Options dialogs allow you to specify how the evidence is sorted and displayed. The Evidence Refinement (Advanced) option allows you to exclude specific data from being added to the case when found in an individual evidence item type.

Many factors can affect which processes to select. For example, if you have specific information otherwise available, you may not need to perform a full text index. Or, if it is known that compression or encryption are not used, an entropy test may not be needed.

**Important:** After data is excluded from an evidence item in a case, the same evidence cannot be added back into the case to include the previously excluded evidence. If data that was previously excluded is found necessary, the user must remove the related evidence item from the case, and then add the evidence again, using options that will include the desired data.

To set case evidence refining options

1. Click the Evidence Refinement (Advanced) icon in the left pane.

The Evidence Refinement (Advanced) menu is organized into two dialog tabs:

- Refine Evidence by File Status/Type
- Refine Evidence by File Date/Size

2. Click the corresponding tab to access each dialog.

3. Set the needed refinements for the current evidence item.

4. To reset the menu to the default settings, click Reset.

5. To accept the refinement options you have selected and specified, click OK.
Refining Evidence by File Status/Type

Refining evidence by file status and type allows you to focus on specific files needed for a case.

**Refine by File Status/Type Options**

<table>
<thead>
<tr>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Include File Slack</td>
<td>Mark to include file slack space in which evidence may be found.</td>
</tr>
<tr>
<td>Include Free Space</td>
<td>Mark to include unallocated space in which evidence may be found.</td>
</tr>
<tr>
<td>Include KFF Ignorable Files</td>
<td>(Recommended) Mark to include files flagged as ignorable in the KFF for analysis.</td>
</tr>
<tr>
<td>Don’t Expand Embedded Graphics</td>
<td>Mark to include embedded graphics within emails.</td>
</tr>
<tr>
<td>Include OLE Streams and Office 2007 package contents</td>
<td>Mark to include Object Linked and Embedded (OLE) data streams, and Office 2007 (DOCX, and XLSX) file contents that are layered, linked, or embedded.</td>
</tr>
</tbody>
</table>
| Deleted | Specifies the way to treat deleted files. Options are:  
- Ignore Status  
- Include Only  
- Exclude  
Defaults to “Ignore Status.” |
| Encrypted | Specifies the way to treat encrypted files. Options are:  
- Ignore Status  
- Include Only  
- Exclude  
Defaults to “Ignore Status.” |
| From Email | Specifies the way to treat email files. Options are:  
- Ignore Status  
- Include Only  
- Exclude  
Defaults to “Ignore Status.” |
| File Types | Specifies which types of files to include and exclude. |
| Only add items to the case that match both File Status and File Type criteria | Applies selected criteria from both File Status and File Types tabs to the refinement. Will not add items that do not meet all criteria from both pages. If this option is not checked, and if you set a File Status, such as From Email > Include Only, then only the File Status value will be used and the File Type will be ignored. |
Adding Evidence to a New Case

Refining Evidence by File Date/Size
Refine evidence further by making the addition of evidence items dependent on a date range or file size that you specify. However, once in the case, filters can also be applied to accomplish this.

Refine by File Date/Size Options

<table>
<thead>
<tr>
<th>Exclusion</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Refine Evidence by File Date</td>
<td>To refine evidence by file date:</td>
</tr>
<tr>
<td></td>
<td>1. Check Created, Last Modified, and/or Last Accessed.</td>
</tr>
<tr>
<td></td>
<td>2. In the two date fields for each date type selected, enter beginning and ending date ranges.</td>
</tr>
<tr>
<td>Refine Evidence by File Size</td>
<td>To refine evidence by file size:</td>
</tr>
<tr>
<td></td>
<td>1. Check At Least and/or At Most (these are optional settings).</td>
</tr>
<tr>
<td></td>
<td>2. In the corresponding size boxes, specify the applicable file size.</td>
</tr>
<tr>
<td></td>
<td>3. In the drop-down lists, to the right of each, select Bytes, KB, or MB.</td>
</tr>
</tbody>
</table>

Selecting Index Refinement (Advanced) Options
The Index Refinement (Advanced) feature allows you to specify types of data that you do not want to index. You may choose to exclude data to save time and resources, or to increase searching efficiency.

Note: AccessData strongly recommends that you use the default index settings.

To refine an index
1. Within the Detailed Options dialog of the New Case wizard, click Index Refinement (Advanced) in the left pane.

The Index Refinement (Advanced) menu is organized into two dialog tabs:

- Refine Index by File Status/Type
- Refine Index by File Date/Size

2. Click the corresponding tab to access each dialog.
3. Define the refinements you want for the current evidence item.
4. Click Reset to reset the menu to the default settings.
5. Click OK when you are satisfied with the selections you have made.
Adding Evidence to a New Case

Refining an Index by File Status/Type

Refining an index by file status and type allows the investigator to focus attention on specific files needed for a case through a refined index defined in a dialog.

At the bottom of the two Index Refinement tabs you can choose to mark the box for **Only index items that match both File Status AND File Types criteria**, if that suits your needs.

**Refine Index by File Status/Type Options**

<table>
<thead>
<tr>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Include File Slack</td>
<td>Mark to include free space between the end of the file footer, and the end of a sector, in which evidence may be found.</td>
</tr>
<tr>
<td>Include Free Space</td>
<td>Mark to include both allocated (partitioned) and unallocated (unpartitioned) space in which evidence may be found.</td>
</tr>
<tr>
<td>Include KFF Ignorable Files</td>
<td>Mark to include files flagged as ignorable in the KFF for analysis.</td>
</tr>
<tr>
<td>Include Message Headers</td>
<td>Marked by default. Includes the headers of messages in filtered text. Unmark this option to exclude message headers from filtered text.</td>
</tr>
<tr>
<td>Do not include document metadata in filtered text</td>
<td>Not marked by default. This option lets you turn off the collection of internal metadata properties for the indexed filtered text. The fields for these metadata properties are still populated to allow for field level review, but the you will no longer see information such as Author, Title, Keywords, Comments, etc in the Filtered text panel of the review screen. If you use an export utility such as ECA or eDiscovery and include the filtered text file with the export, you will also not see this metadata in the exported file.</td>
</tr>
<tr>
<td>Include OLE Streams</td>
<td>Includes Object Linked or Embedded (OLE) data streams that are part of files that meet the other criteria.</td>
</tr>
<tr>
<td>Deleted</td>
<td>Specifies the way to treat deleted files. Options are:</td>
</tr>
<tr>
<td></td>
<td>• Ignore status</td>
</tr>
<tr>
<td></td>
<td>• Include only</td>
</tr>
<tr>
<td></td>
<td>• Exclude</td>
</tr>
<tr>
<td>Encrypted</td>
<td>Specifies the way to treat encrypted files. Options are:</td>
</tr>
<tr>
<td></td>
<td>• Ignore status</td>
</tr>
<tr>
<td></td>
<td>• Include only</td>
</tr>
<tr>
<td></td>
<td>• Exclude</td>
</tr>
</tbody>
</table>
## Adding Evidence to a New Case

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>From Email</td>
<td>Specifies the way to treat email files. Options are:</td>
</tr>
<tr>
<td></td>
<td>● Ignore status</td>
</tr>
<tr>
<td></td>
<td>● Include only</td>
</tr>
<tr>
<td></td>
<td>● Exclude</td>
</tr>
<tr>
<td>Include OLE Streams</td>
<td>Includes Object Linked or Embedded (OLE) files found within the evidence.</td>
</tr>
<tr>
<td>File Types</td>
<td>Specifies types of files to include and exclude.</td>
</tr>
<tr>
<td>Exclude by Category</td>
<td>Specified categories to include and exclude. Additionally allows specific types to be included/excluded within the group while selected.</td>
</tr>
<tr>
<td>Only add items to the Index</td>
<td>Applies selected criteria from both File Status and File Types tabs to the</td>
</tr>
<tr>
<td>that match both File Status</td>
<td>refinement. Will not add items that do not meet all criteria from both pages.</td>
</tr>
<tr>
<td>and File Type criteria</td>
<td></td>
</tr>
</tbody>
</table>

### Refining an Index by File Date/Size

Refine index items dependent on a date range or file size you specify.

#### Refine Index by File Date/Size Options

<table>
<thead>
<tr>
<th>Exclusion</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Refine Index by File Date</td>
<td>To refine index content by file date:</td>
</tr>
<tr>
<td></td>
<td>1. Select <strong>Created</strong>, <strong>Last Modified</strong>, or <strong>Last Accessed</strong>.</td>
</tr>
<tr>
<td></td>
<td>2. In the date fields, enter beginning and ending dates within which to include files.</td>
</tr>
<tr>
<td>Refine Index by File Size</td>
<td>To refine evidence by file size:</td>
</tr>
<tr>
<td></td>
<td>1. Click in either or both of the size selection boxes.</td>
</tr>
<tr>
<td></td>
<td>2. In the two size fields for each selection, enter minimum and maximum file sizes to include.</td>
</tr>
<tr>
<td></td>
<td>3. In the drop-down lists, select whether the specified minimum and maximum file sizes refer to <strong>Bytes</strong>, <strong>KB</strong>, or <strong>MB</strong>.</td>
</tr>
</tbody>
</table>

### Selecting Lab/eDiscovery Options

AD Lab and eDiscovery have additional options available for advanced de-duplication analysis.

De-duplication is separated by email items and non-email items. Within each group, the available options can be applied by case or by Custodian.

**Note:** This option is not enabled by default when using the eDiscovery Default processing profile.
Adding Evidence to a New Case

The following table provides more information regarding each option and its description.

**AD Lab/eDiscovery Detailed Options**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Advanced De-duplication Analysis</td>
<td></td>
</tr>
</tbody>
</table>
| Email Items De-duplication Scope | Choose whether you want this de-duplication process to be applied at the Case level, or at the Custodian level.  
  - Case Level  
  - People (Custodian) Level |

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| De-duplication Options | For each item type you check, AD Lab eliminates duplicates from the case as it processes through the collected evidence. Uncheck an item type to keep all duplicate instances in your case.  
  Available item types  
  - Email To  
  - Email From  
  - Email CC  
  - Email BCC  
  - Email Subject  
  - Email Submit Time  
  - Email Delivery Time  
  - Email Attachment Time  
  - Email Attachment Count  
  - Email Hash  
    - Body Only  
    - Body and Attachments |
| Non-email Items De-duplication Scope | Choose whether you want this de-duplication process to be applied to the entire case or at the custodian level.  
  - Case Level  
  - People (Custodian) Level |
## Adding Evidence to a New Case

### De-duplication Option

There is only one option available for non-email items; either you are going to de-duplicate just the actual files, or if unmarked, you will de-duplicate actual files only, or all files, including children, zipped, OLE, and carved files.

- **Actual Files Only**

### Propagate Email

When an email has attachments or OLE items, marking this option causes the Attributes email's attributes to be copied and applied to all “child” files of the email “parent.”

### Cluster Analysis

Invokes the extended analysis of documents to determine related, near duplicates, and email threads.

See [Viewing Data in Volume Shadow Copies](#) on page 421. Configure the details by clicking **NDA Options**.

### Cluster Analysis Options

This lets you specify the options for Cluster Analysis. You can specify which document types to process:

- Documents
- Presentations
- Spreadsheets
- Email

You can also specify the similarity threshold, which determines the level of similarity required for documents to be considered related or near duplicates.

### Option Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Include Extended</td>
<td>If you create a case in FTK and are going to review it in Summation or eDiscovery, Information in the select this option to make the index data fully compatible with Summation/ Index eDiscovery.</td>
</tr>
</tbody>
</table>
Adding Evidence to a New Case

Enable ‘Standard’ viewer.

If you create a case in FTK and are going to review it in Summation or eDiscovery, select this option to automatically create a set of SWF files for all document files found during processing. These SWF files will be used as the default file rather than the original file when annotating and redacting within the case and will be created during processing for any file 1 MB or larger. Smaller files will be created on-the-fly when selected in Review.

When opened in the Standard Viewer in eDiscovery or Summation, the converted SWF file is displayed by default, rather than the original file. This enables users to work on a file without first having to manually create a SWF file.

Note: This option is disabled by default, and when enabled, slows processing speeds.

Create Email Threads Sorts and groups emails by conversation threads.

If you marked Open the Case before clicking OK in the New Case Options dialog, when case creation is complete, the Examiner opens. Evidence items added here will be processed using the options you selected in pre-processing, unless you click Refinement Options to make changes to the original settings.

Working with Volume Shadow Copies

You can examine data that is contained in NTFS Volume Shadow Copies. See Examining Data in Volume Shadow Copies on page 143.

Converting a Case

If you have cases that were created in version 2.2 or later, you can convert them to the latest version. Refer to the following guidelines for migrating 2.x cases.

Important: Consider the following information:

- Any case created with a version prior to 2.2 must be re-processed completely in the latest version.
- AccessData recommends reprocessing active cases instead of attempting to convert them, to maximize the features and capabilities of the new release.
Adding Evidence to a New Case

- AccessData recommends that no new evidence be added to any case that has been converted from an earlier version. This is because newer versions of processing gathers more information than was done in versions prior to 2.x.

Therefore, if evidence is added to a converted 2.2 case, the new evidence will have all the info gathered by the newest version; however, the data from the converted 2.2 case will not have this additional information. This may cause confusion and bring forensic integrity into question in a court of law.

For more information, see the webinar that explains Case Portability in detail. This webinar can be found under the Core Forensic Analysis portion of the webpage: http://www.accessdata.com/Webinars.

The AccessData website works best using Microsoft Windows Explorer. You will be required to create a username and password if you have not done so in the past. If you have used this website previously, you will need to verify your email address. The website normally remembers the rest of the information you enter.

For instructions on converting cases, see the Migrating Cases document located at http://www.accessdata.com/support/product-downloads/ftk-download-page.
Managing Case Data

This chapter includes the following topics
- Backing Up a Case (page 116)
- Archiving and Detaching a Case (page 119)
- Attaching a Case (page 120)
- Restoring a Case (page 121)
- Migrating Cases Between Database Types (page 122)

About Performing a Backup and Restore on a Multi-Box Installation

If you have installed the Examiner and the database on separate boxes, or if you have case folders on a different box than the application, there are special considerations you must take into account. For instructions on how to back up and restore in this environment, see Configuring a Multi-box Setup in the User Guide.

Performing a Backup of a Case

At certain milestones of an investigation, you should back up your case to mitigate the risk of an irreversible processing mistake or perhaps case corruption.

Case backup can also be used when migrating or moving cases from one database type to another. For example, if you have created cases using 4.1 in an Oracle database and you want to upgrade to 5.0.x and migrate the case(s) to a PostgreSQL database. Another example is if you have created cases using 5.0.x in an Oracle database and you want to move the case(s) to the same version that is running a PostgreSQL database.

When you back up a case, the case information and database files (but not evidence) are copied to the selected destination folder. AccessData recommends that you store copies of your drive images and other evidence separate from the backed-up case.

Important: Case Administrators back up cases and must maintain and protect the library of backups against unauthorized restoration, because the user who restores an archive becomes that case’s administrator.

Note: Backup files are not compressed. A backed-up case requires the same amount of space as that case’s database table space and the case folder together.
Starting in 4.2, all backups are performed using the database independent format rather than a native format. The database independent format facilitates migrating and moving cases to a different database application or version. You can perform a backup using a native format using the dbcontrol utility. For more information, contact AccessData Technical Support.

**Important:** Do not perform a backup of a case while any data in that case is being processed.

**To back up a case**

1. In the *Case Manager* window, select the case to back up. You can use Shift + Click, or Ctrl + Click to select multiple cases to backup.
2. Do one of the following:
   - Click Case > Backup > Backup.
   - Right-click on the case in the *Cases* list, and click **Backup**.
3. In the field labeled *Backup folder*, enter a destination path for the backup files.

**Important:** Choose a folder that does not already exist. The backup will be saved as a folder, and when restoring a backup, point to this folder (not the files it contains) in order to restore the case.

4. *(Option)* Use database independent format.

   All backups are performed using the database independent format. You cannot change this option.

5. *(Optional)* Back up the Summation or Resolution1 application database.

   If you have a license for Summation or Resolution1, when you back up a case, you can also select to backup the Summation or Resolution1 application database by doing the following:
   
   5a. Click **App DB**...
   
   5b. Specify the App DB properties and credentials.

6. **Click OK**.

**Note:** The following information may be useful:

- Each case you back up should have its own backup folder to ensure all data is kept together and cannot be overwritten by another case backup. In addition, AccessData recommends that backups be stored on a separate drive or system from the case, to reduce space consumption and to reduce the risk of total loss in the case of catastrophic failure (drive crash, etc.).
- The absolute path of the case folder is recorded. When restoring a case, the default path is the original path. You can choose the default path, or enter a different path for the case restore.
Performing a Database-only Backup

There is a new -backuponly switch that you can use with DBControl.exe that will only backup the database portion of the case, but does not backup the case folder.

To perform a database-only backup
1. Open a Command Prompt in Windows.
2. Go to the following path:

   C:\Program Files\AccessData\Forensic Toolkit\version\bin
3. Enter the following:

   dbcontrol.exe pgdb=adg port=<port#> -backuponly caseid=<case#> backuppath=<path to backup thedb>

**Note:** You will need to have the port number, case ID, and backup path before you begin the database-only backup process.
Archiving a Case

When work on a case is completed and immediate access to it is no longer necessary, that case can be archived.

The Archive and Detach function copies that case’s database table space file to the case folder, then deletes it from the database. This prevents two people from making changes to the same case at the same time, preserving the integrity of the case, and the work that has been done on it. Look for filename DB fn. Archive keeps up to four backups, DB f0, DB f1, DB f2, and DB f3.

To archive a case
1. In the Case Manager, select the case to archive.
2. Click Case > Backup > Archive.
3. A prompt asks if you want to use an intermediate folder.

The processing status dialog appears, showing the progress of the archive. When the archive completes, close the dialog.

To view the resulting list of backup files
1. Open the cases folder.

---

**Note:** The cases folder is no longer placed in a default path; instead it is user-defined.

2. Find and open the sub-folder for the archived case.
3. Find and open the sub-folder for the archive (DB fn).
4. You may view the file names as well as Date modified, Type, and Size.
Archiving and Detaching a Case

When work on a case is not complete, but it must be accessible from a different computer, archive and detach that case.

The Archive and Detach function copies that case’s database table space file to the case folder, then deletes it from the database. This prevents two people from making changes to the same case at the same time, preserving the integrity of the case, and the work that has been done on it.

To archive and detach a case
1. In the Case Manager, click Case > Backup > Archive and Detach. The case is archived.
2. You will see a notice informing you that the specified case will be removed from the database. Click OK to continue, or Cancel to abandon the removal and close the message box.
3. A prompt asks if you want to use an intermediate folder.

The processing status dialog appears, showing the progress of the archive. When the archive completes, close the dialog.

To view the resulting list of files
1. Open the folder for the archived and detached cases.
2. Find and open the sub-folder for the archived case.

---

Note: The cases folder is no longer placed in a default path; instead it is user-defined.
3. Find and open the sub-folder for the archive (DB fn).

You may view the file names as well as Date Modified, Type, and Size.
Attaching a Case

Attaching a case is different from restoring a case. You would restore a case from a backup to its original location in the event of corruption or other data loss. You would attach a case to the same or a different machine/database than the one where it was archived and detached from. The Attach feature copies that case’s database table space file into the database on the local machine.

**Note:** The database must be compatible and must contain the AccessData schema.

To attach a detached case
1. Click Case > Restore > Attach.

**Important:** Do NOT use “Restore” to re-attach a case that was detached with “Archive.” Instead, use “Attach.” Otherwise, your case folder may be deleted.
2. Browse to and select the case folder to be attached.
3. (Optional) Select **Specify the location of the DB files** and browse to the path to store the database files for this case.
   3a. Select **In the case folder** to place the database files in subfolder of the case folder.
4. Click **OK**.
Restoring a Case

When your case was backed up, it was saved as a folder. The folder selected for the backup is the folder you must select when restoring the backup.

**Note:** Do not use the *Restore...* function to attach an archive (instead use *Attach...*).

To restore a case
1. Open the Case Manager window.
2. Do either of these:
   - Click Case > Restore > Restore.
   - Right-click on the Case Manager case list, and click **Restore > Restore**.
3. Browse to and select the backup folder to be restored.
4. (Optional) Select **Specify the location of the DB files** and browse to the path to store the database files for this case.
   4a. Select **In the case folder** to place the database files in subfolder of the case folder.
5. You are prompted if you would like to specify a different location for the case folder. The processing status dialog appears, showing the progress of the archive. When the archive completes, close the dialog.
Deleting a Case

To delete a case from the database
1. In the Case Manager window, highlight the name of the case to be deleted from the database.
2. Do either of these:
   - Click Case > Delete.
   - Right-click on the name of the case to deleted, and click Delete
3. Click Yes to confirm deletion.

WARNING: This procedure also deletes the case folder. It is recommended that you make sure you have a backup of your case before you delete the case or else the case is not recoverable.

Storing Case Files
Storing case files and evidence on the same drive substantially taxes the processors' throughput. The system slows as it saves and reads huge files. For desktop systems in laboratories, you can increase the processing speed by saving evidence files to a separate server. For more information, see the separate installation guide.
If taking the case off-site, you can choose to compromise some processor speed for the convenience of having your evidence and case on the same drive, such as a laptop.

Migrating Cases Between Database Types
You can migrate or move cases from one database to another. For more information, see the Quick Install Guide
and the Upgrading Cases guide.
Collaboration

Creating and Using Tasks

About Tasks
Administrators and users can create tasks and assign them to users associated with a case. Each task is associated to a single case and can be assigned to a single user. Those that have been assigned a task can report the status and progress of the task.

When a user logs in, if they have new tasks that have been assigned to them since the last time they logged in, that user is prompted if they want to see the list of tasks assigned to them. From the list of tasks, they can open the case in Examiner.

As users examine case data as part of a task, they can assign evidence items to the task. An administrator or user can then easily see the files that have been assigned during the work of the task. Files in the File List that have been assigned to a task are displayed in aqua color.

For example, a user may be given a task to review a set of evidence to find any emails sent from or to a certain person. As the user reviews the evidence and finds relevant emails, they can assign them to the task. The user can also add comments regarding the emails that may be helpful. An administrator or user can view the task and monitor the progress of the task and view any files that have been assigned to it, with any accompanying comments.

The following tables describe the properties of tasks.

When you create (and later edit) a task, you can set the following properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Task name</td>
<td>The name of the task. Required.</td>
</tr>
<tr>
<td>The user that the task is assigned to</td>
<td>You can select from any user that is associated to the case.</td>
</tr>
<tr>
<td>A priority</td>
<td>• Extreme&lt;br&gt;• High&lt;br&gt;• Medium&lt;br&gt;• Low&lt;br&gt;• Unimportant</td>
</tr>
<tr>
<td>A due date</td>
<td>Selectable using a calendar</td>
</tr>
<tr>
<td>Alert status</td>
<td>You can check an Alert field. The Alert status is displayed as Yes or No in a sortable Alert column in the Tasks list. This can designate a task that has immediate priority.</td>
</tr>
<tr>
<td>Task notes</td>
<td>You can use the text editor to add a note to the task. For example, an administrator can add specific instructions about the task.</td>
</tr>
</tbody>
</table>
After tasks are created, users can select and update tasks using the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name, Assigned to, Priority, and Due date</td>
<td>A user can modify these fields.</td>
</tr>
<tr>
<td>Task status</td>
<td>- Created</td>
</tr>
<tr>
<td></td>
<td>- Assigned</td>
</tr>
<tr>
<td></td>
<td>- Started</td>
</tr>
<tr>
<td></td>
<td>- Completed</td>
</tr>
<tr>
<td></td>
<td>- Rejected</td>
</tr>
<tr>
<td></td>
<td>- Closed Incomplete</td>
</tr>
<tr>
<td></td>
<td>When a task is first created, and if it is assigned to a user, when the task is saved, the status is automatically changed to Assigned.</td>
</tr>
<tr>
<td>Progress</td>
<td>The progress by % completed, from 0 - 100 with intervals of 20.</td>
</tr>
<tr>
<td>Task notes</td>
<td>You can view notes that have been added to a task. You can use the text editor to add a note to the task. For example, a user can add notes about their work on the task.</td>
</tr>
<tr>
<td>File Comments</td>
<td>A user can view or add comments to files that have been assigned to the task.</td>
</tr>
<tr>
<td>The files assigned to the task</td>
<td>In the Examiner File List, users can assign evidence files to tasks. Those files are shown in the task’s Files list. You can remove files from the task.</td>
</tr>
<tr>
<td>File Comments added to files</td>
<td>In the Examiner File List, when users assign evidence files to tasks, they can add a comment to the file. If you assigned multiple files, the comment is added to all files. Those comments are shown in the task’s File Comment list after selecting a file. Comments can be added or edited.</td>
</tr>
</tbody>
</table>
Users can select a task and view the following un-editable fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>The case name and case id the task is associated with</td>
<td>A task can only be assigned to one case. The case that the task has been assigned to is displayed.</td>
</tr>
<tr>
<td>Created</td>
<td>The date and time the task was created.</td>
</tr>
<tr>
<td>Date and time last updated</td>
<td>The date and time the task was last updated.</td>
</tr>
<tr>
<td>Last updated by</td>
<td>The user who last updated the task.</td>
</tr>
<tr>
<td>The task history</td>
<td>Click <strong>Show history</strong> to display or hide the history of the task. This shows certain modifications that have been made to the task. For example, when it was modified and which properties were modified (progress, status, and so forth).</td>
</tr>
</tbody>
</table>

About Permissions and Tasks

**Important:** The only restriction on using tasks in relation to permissions is that users can create a task only in the cases that they have permissions to. However, any user can view, modify, and delete any task.

**Using Tasks**

**To create a new Task**

1. Do one of the following:
   - In the **Case Manager** through the **Case** menu:
     1a. In the Cases list, click (and highlight) the case that you want to create a task within.
     1b. Click **Case > Create Task**.
     - In the **Case Manager** through the **Cases** list:
     1a. In the Cases list, right-click the case that you want to create a task within.
     1b. Click **Create Task**.
     - Through the Case Examiner:
       1a. In the View menu, click **Create Task**.
       1b. Through the Case Examiner **File List**:
       1a. In the File List, check or highlight one or more files that you want to add to a new task.
       1b. Right-click.
       1c. Click **Create Task**.
       1d. Specify which file to add to the task.
       1e. Add a comment if desired.
2. In the Task dialog and in the Case name field, verify that the case is correct.

3. In the Task name field, give the task a name.

4. Optional:
   4a. In the Assigned to field, select a user.

   **Note:** You can only select users that are associated with this case.

   **Note:** If you assign a user, when the task is saved, the status will automatically be changed to Assigned.

4b. In the Priority field, assign a priority.

4c. In the Due field, enter a due date.

4d. To enter text notes for the task, double click the Notes pad.

   4e. You can enable the Alert setting to display a Yes or No value in the Alert column.

   4f. Click Create.

**To view and filter the Task list**

1. Open the Tasks list by doing one of the following:
   • In the Case Manager through the Case menu:
     1a. Click Case > Tasks.
   • In the Case Manager through the Cases list:
     1a. In the Cases list, right-click the case that you want to views tasks within.
      1b. Click Tasks.
      • Through the Examiner:
        1a. In the View menu, click Tasks.

2. You can view the tasks in the Tasks list.

3. You can filter the Tasks list by doing the following (if you select multiple filters, the results are combined):
   • Check Current Case to view only the tasks associated to the current case.
   • Clear Current Case to view the tasks associated with any case.
   • Check All Users to view the tasks assigned to all users.
   • Clear All Users to view only the tasks associated with the logged-in user.
• Check *Unassigned* to view any tasks that are not assigned to a user.
• Clear *Unassigned* to view only the tasks that are assigned to a user.
• Specify a Status. In the drop-down, you can select one or more options. Click an item to toggle it on or off.
• Specify a Progress %. In the drop-down, you can select one or more options. Click an item to toggle it on or off.
• Specify a Priority. In the drop-down, you can select one or more options. Click an item to toggle it on or off.
To view tasks assigned to you
1. Log in using your account credentials.

If a task has been assigned to you since the last time you logged in, you will see the message: New tasks have been assigned to you since your last login. Open the task list now?
2. To open the task list, click Yes.

To view and modify tasks
1. Open the Tasks list.
2. Filter the Tasks list as desired.
3. Click a task.

The task properties are displayed.
4. View and modify any editable property.
5. To view or add comments for a task, view or double-click in the Notes field.
6. To view the history of a task, check Show History.
7. To view any files assigned to a task, view the Files list.
8. To view comments that have been previously added to a file, click a file in the Files list and view the File Comment.
9. To add or modify a comment to a file, click a file in the Files list and click in File Comment, add the text, and click Save Changes.

Note: You can only add a comment to one file at a time and you must click Save Changes before switching to a different file.
10. To save any changes, click Save Changes.

To open the Examiner of the relevant case of a task
1. In the Tasks list, click (highlight) a case.
2. Click Open Case.

To assign evidence files to an existing task
1. Open the Examiner.

2. In the File List, check or select (highlight) one or more files that you want to add to an existing task.

3. Right-click.

4. Click Add to Task.

5. Select whether to add highlighted, checked, or all listed items.

6. (Optional) Enter a comment for the files being added. (It will be added to all selected files.)

7. Select the existing task that you want to add the files to.

8. Click OK.

9. Files that have been assigned to a task are displayed in the Tasks list in aqua color.

To delete a task

1. Open the Tasks list.

2. Filter the Tasks list as desired.

3. Click a task.

The task properties are displayed.

4. Click Delete Task.

5. Confirm the deletion by clicking Yes.

Any files assigned to a deleted task are no longer associated with the task.
Chapter 9
Working with Evidence Image Files

This chapter contains the following topics
- Verifying Drive Image Integrity (page 129)
- Mounting an Image to a Drive (page 130)
- Benefits of Image Mounting (page 130)
- Characteristics of a Logically Mounted Image (page 131)
- Characteristics of a Physically Mounted Image (page 131)
- Mounting an Image as Read-Only (page 131)
- Mounting a Drive Image as Writable (page 132)
- Unmounting an Image (page 133)
- Restoring an Image to a Disk (page 133)
- Performing Final Carve Processing (page 133)
- Recovering Processing Jobs (page 134)

Verifying Drive Image Integrity
A drive image can be altered or corrupted due to bad media, bad connectivity during image creation, or by deliberate tampering. This feature works with file types that store the hash within the drive image itself, such as EnCase (E01) and SMART (S01) images.
To verify an evidence image’s integrity, a hash of the current file is generated and allows you to compare that to the hash of the originally acquired drive image.
To verify that a drive image has not changed

1. Select Tools > Verify Image Integrity.

In case the image file does not contain a stored hash, one can be calculated. The Verify Image Integrity dialog provides the following information:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Image Name</td>
<td>Displays the filename of the evidence image to be verified.</td>
</tr>
<tr>
<td>Path</td>
<td>Displays the path to the location of the evidence image file.</td>
</tr>
<tr>
<td>Command</td>
<td>Click <strong>Verify</strong> or <strong>Calculate</strong> to begin hashing the evidence image file.</td>
</tr>
</tbody>
</table>

2. Click either **Calculate**, or **Verify** according to what displays in the Command column, to begin hashing the evidence file.

The Progress dialog appears and displays the status of the verification. If the image file has a stored hash, when the verification is complete, the dialog shows and compares both hashes. Completing these processes may take some time, depending on the size of the evidence, the processor type, and the amount of available RAM.

Mounting an Image to a Drive

Image Mounting allows forensic images to be mounted as a drive or physical device, for read-only viewing. This action opens the image as a drive and allows you to browse the content in Windows and other applications.

Supported types are RAW/dd images, E01, S01, AD1, and L01.

Full disk images RAW/dd, E01, and S01 can be mounted Physically. Partitions contained within full disk images, as well as Custom Content Images of AD1 and L01 formats can be mounted Logically. The differences are explained in this section.

**Note:** Encrypted images cannot be mounted as either a drive or physical device.
Benefits of Image Mounting

The ability to mount an image with AccessData forensic products provides the following benefits:

- Mount a full disk image with its partitions all at once; the disk is assigned a Physical Drive name and the partitions are automatically assigned a drive letter beginning with either the first available, or any available drive letter of your choice.
- A full disk image mounted physically, and assigned a Physical Drive name that can be read using Imager or with any Windows application that performs Physical Name Querying.
- Mount images of multiple drives and/or partitions. The mounted images remain mounted until unmounted or until Imager is closed.
- Mounted images can be easily unmounted in any order, individually, or all at once.
- A logically mounted image may be viewed in Windows Explorer as though it were a drive attached to the computer, providing the following benefits:
  - File types with Windows associations can be viewed in their native or associated application, when that application is installed locally.
  - Anti-virus applications can be run on the mounted image.
  - Because the logically mounted image is seen as a drive in Windows Explorer, it can be shared, and viewed from remote computers when Remote Access has been configured correctly.
  - Files can be copied from the mounted image to another location.
- Mount NTFS / FAT partitions contained within images as writable block devices. This feature caches sections of a read-only image to a temporary location allowing the user to “write” to the image without compromising the integrity of the original image.

Once mounted via the write cache mount method, the data can then be leveraged by any 3rd party tools which require write access.
Characteristics of a Logically Mounted Image

AD1 and L01 are both custom content images, and contain full file structure, but do not contain any drive geometry or other physical drive data. Thus, these images do not have the option of being mounted Physically.

Note: When Logically mounting an image, the drive or partition size displays incorrectly in the Windows Start > Computer view. However, when you open the “drive” from there, the folders and files contained within themounted image do display correctly.

Characteristics of a Physically Mounted Image

When you mount an image physically, while it cannot be viewed by Windows Explorer, it can be viewed outside of Imager using any Windows application that performs Physical Name Querying. E01, S01, and RAW/dd images are drive images that have the disk, partition, and file structure as well as driven data. A physical disk image can be mounted Physically; the disk image partitions can be mounted Logically.

Mounting an Image as Read-Only

To mount an image

1. If you already have the desired image added as evidence in the case, select that item, then do Step 2 to auto-populate the Source box with the image file to be mounted, as shown in Step 3.

If you do not already have the desired image added as evidence, begin with Step 2.

2. Do one of the following:

   - Right-click and choose Mount Image to Drive.
   - Select the image from the Evidence tree. Right-click and choose Mount Image to Drive.
   - Click Tools > Mount Image to Drive, then browse to the image on your local drive or on a network drive you have access to.

3. Enter the path and filename, or click Browse to populate the Source box with the path and filename of the image to be mounted.

After selecting an image, the Mount Type will default to the supported mapping based on the image type selected. Click the drop-down to display other available mount types. After selecting an image, the MapType will default to the supported mapping based on the image type selected.
Click the drop-down to display other available map types.

4. Select the Mount Type to use for mounting.

Available Mount Types are Physical & Logical, Physical Only, and Logical Only. If the Mount Type selected includes Logical, you can select the Drive Letter to assign as the mount point.

5. Click the Drive Letter drop-down to see all drive letters that are available for assignment to the mounted image.

6. Click the Mount Method drop-down to select **Block Device / Read Only** or **File System / Read Only**.

**Note:** If you are mounting an HFS image of a Mac drive, you must choose **File System / Read Only** to view contents of the drive. Otherwise, it will appear empty, and may prompt you to format the drive.

7. Click **Mount**.

All the related mount information will be displayed in the Mapped Image List. To mount another image, repeat the process. You can continue to mount images as needed, until you run out of evidence to add, or mount points to use. Mounted images remain available until unmounted, or until the program is closed.

8. Click **Close** to return to the main window.
Mounting a Drive Image as Writable

When mounting an image as writable, you must be working with a physical image, and the mount type you select must be Physical & Logical. This is the only option that provides the **Block Device /Writable** Mount Method.

**To mount a drive image as writable**
1. In the *Examiner*, click Tools > Mount Image to Drive.
2. Select a full disk image such as 001/Raw dd, E01, or S01 file type.
3. In the *Mount Type* drop-down, select **Physical & Logical**.
4. In the *Drive Letter* drop-down, select **Next Available** (default), or select a different drive letter.

---

**Note:** Check your existing mappings. If you map to a drive letter that is already in use, the original will prevail and you will not be able to see the mapped image contents.

5. In the *Mount Method* drop-down, select **Block Device / Writable**.
6. In the *Write Cache Folder* text box, type or click **Browse** to navigate to the folder where you want the Write Cache files to be created and saved.
7. Click **Mount**.

You will see the mapped images in the Mapped Image List.

**To view or add to the writable mapped drive image**
1. On your Windows desktop, click **Start > Computer** (or **My Computer**).
2. Find the mapped drive letter in your Hard Disk Drives list. It should be listed by the name of the Image that was mounted, then the drive letter.
3. Double-click on it as you would any other drive.
4. As a test, right-click and choose **New > Folder**.
5. Enter a name for the folder and press **Enter**.
6. The folder you created is displayed in the Folder view.
7. Mapped images remain mapped until unmapped, or until the application is shut down.
Recovering Processing Jobs  
Unmounting an Image

To unmount a mounted image
1. Click File > Image Mounting. The Map Image to Drive dialog opens.
2. Highlight the images to unmount, click Unmount. To unmount multiple mappings, click the first, then Shift-click the last to select a block of contiguous mappings. Click a file, then Ctrl-click individual files to select multiple non-contiguous mappings.)
3. Click Done to close the Map Image to Drive dialog.

Restoring an Image to a Disk
A physical image such as 001 (RAW/dd), E01, or S01, can be restored to a drive of equal or greater size to the original, un-compressed drive.

To restore an image to a disk
1. Connect a target drive to your computer.
2. In the Examiner, click Tools > Restore Image to Disk.
3. Click Browse to locate and select the source image. It must be a full-disk image such as 001 (Raw/dd), E01, or S01.

The source image must be a disk image. A logical image such as AD1 will not work for this feature.
4. Click the Destination Drive drop-down, select the target drive you connected in Step 1. If you do not see that drive in the list, click Refresh.
5. Mark the Zero-fill remainder of destination drive check box if the drive is larger than the original un-compressed drive.
6. Mark the Notify operating system to rescan partition table when complete check box to allow the new drive to be seen by the OS. If you plan to connect the drive in a different computer there is no need to do this step.

When you are finished selecting options, click Restore Image to continue.
Recovering Processing Jobs
Performing Final Carve Processing

When you have selections saved as carved files from any file in the Hex viewer, performing Final Carve Processing carves the files, saves them, adds them to the case, and even creates or assigns them to bookmarks you specified when the data was selected.

Final Carve Processing jobs can be monitored in the Progress Window as Additional Analysis Jobs.

Jobs that are started but unable to finish for whatever reason can be deleted or restarted. Click **Tools > Recover Processing Jobs**. If no jobs remain unfinished, the Recover Processing Jobs dialog box is empty. Click **Close**. If there are jobs in the list, you can choose whether to Restart or Delete those jobs.

**To recover incomplete processing jobs**

1. Click **Select All, Unselect All**, or mark the check box for each job to be recovered.
2. Click **Restart**.
3. In the **Recovery Type** dialog, choose the recovery type that suits your needs:
   - **Continue processing** from where the job ended.
   - **Restart** the job from the beginning.
4. Click **Close**.
5. To verify the progress of a restarted or continued job, click **Tools > Show Progress Window**.

**To remove incomplete processing jobs**

1. Click **Select All, Unselect All**, or mark the check box for each job to discard.
2. Click **Delete**.
3. Click **Yes** to confirm that you want to delete the job permanently.
4. Click **Close**.
Chapter 10
Working with Static Evidence

This chapter includes the following topics

- Static Evidence Compared to Remote Evidence (page 135)
- Acquiring and Preserving Static Evidence (page 136)
- Adding Evidence (page 136)
- Working with Evidence Groups (page 140)
- Selecting Evidence Processing Options (page 141)
- Selecting a Language (page 142)
- Examining Data in Volume Shadow Copies (page 143)
- Using Additional Analysis (page 147)
- Data Carving (page 152)
- Hashing (page 152)
- Viewing the Status and Progress of Data Processing and Analysis (page 154)
- Viewing Processed Items (page 155)
- Editing the Processing Management Queue (page 155)
- Viewing Evidence Information (page 156)

Static Evidence Compared to Remote Evidence

Static evidence describes evidence that has been captured to an image before being added to the case.
Live evidence describes any data that is not saved to an image prior to being added to a case. Such evidence is always subject to change, and presents risk of data loss or corruption during examination. For example, a suspect’s computer, whether because a password is not known, or to avoid the suspect’s knowing that he or she is under suspicion, may be imaged live if the computer has not yet been or will not be confiscated.

Remote evidence describes data that is acquired from remote live computers in the network after the case has been created.

This chapter covers working with static evidence. For more information regarding acquisition and utilization of remote evidence, see Working with Live Evidence (page 169).
Acquiring and Preserving Static Evidence

For digital evidence to be valid, it must be preserved in its original form. The evidence image must forensically sound, in other words, identical in every way to the original.

See also About Acquiring Digital Evidence (page 29)

Adding Evidence

When case creation is complete, the Manage Evidence dialog appears. Evidence items added here will be processed using the options you selected in pre-processing. Please note the following information as you add evidence to your case:

- You can now drag and drop evidence files from a Windows Explorer view into the Manage Evidence dialog.
- You can repeat this process as many times as you need to, for the number of evidence items and types you want to add.
- DMG (Mac) images are sometimes displayed as “Unrecognized File System.” This happens only when the files are not “Read/Write” enabled.

If the DMG is a full disk image or an image that is created with the read/write option, then it is identified properly. Otherwise the contents will not be recognized properly.

- After processing, the Evidence Processing selected options can be found in the case log. You can also view them by clicking Evidence > Add/Remove. Double-click on any of the evidence items to open the Refinement Options dialog.
- Popular mobile phone formats (found in many MPE images) such as M4A, MP4, AMR, and 3GP can be recognized. These file types will play inside the Media tab as long as the proper codecs are installed that would also allow those files to play in Windows Media Player.

To add static evidence (an exact image, or “snapshot” of electronic data found on a hard disk or other data storage device) to an existing case, select Evidence > Add/Remove from the menu bar and continue.

**Note:** Use Universal Naming Convention (UNC) syntax in your evidence path for best results.

Click Refinement Options to override settings that were previously selected for evidence added to this case. If you do not click Refinement Options here, the options that were specified when you created the case will be used.

Configuring Default Processing Options for a Case (page 80)
After evidence has been added, you can perform many processing tasks that were not performed initially. Additional evidence files and images can be added and processed later, if needed.

Manage Evidence Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add</td>
<td>Opens the Select Evidence Type dialog. Click to select the evidence type, and a Windows Explorer instance will open, allowing you to navigate to and select the evidence you choose.</td>
</tr>
<tr>
<td>Remove</td>
<td>Displays a caution box and asks if you are sure you want to remove the selected evidence item from the case. Removing evidence items that are referenced in bookmarks and reports will remove references to that evidence and they will no longer be available. Click Yes to remove the evidence, or click No to cancel the operation.</td>
</tr>
<tr>
<td>Path</td>
<td>The full pathname of the evidence file.</td>
</tr>
<tr>
<td>ID/Name</td>
<td>The optional ID/Name of the evidence being added.</td>
</tr>
<tr>
<td>Description</td>
<td>The options description of the evidence being added. This can be the source of the data, or other description that may prove helpful later.</td>
</tr>
<tr>
<td>Evidence Group</td>
<td>Click the drop-down to assign this evidence item to an Evidence Group. For more information regarding Evidence Groups, see Working with Evidence Groups (page 140).</td>
</tr>
<tr>
<td>Evidence Category</td>
<td>Click the drop-down to assign a system category to this evidence item. Users can select from iOS, Android, Windows, MAC OS, Linux and auto detect. If unsure please select the auto option.</td>
</tr>
<tr>
<td>Time Zone</td>
<td>The time zone of the original evidence. Select a time zone from the drop-down list.</td>
</tr>
</tbody>
</table>
### Merge Case Index

Merges fragmented index segments to improve performance of index-related commands, such as Index Searching.

**Note:** The application automatically merges the case index when system resources allow whether or not Merge Case Index is selected. Selecting this option forces the merge to execute regardless of system resources.

| Language Setting | Select the code page for the language to view the case in. The Language Selection dialog contains a drop-down list of available code pages. Select a code page and click **OK**. |
| Case KFF Options | Opens the KFF Admin box for managing KFF libraries, groups, and sets for this case. |

### Manage Evidence Options (Continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Refinement Options</td>
<td>Displays the Refinement Options for Evidence Processing. This dialog has limited options compared to the Refinement Options selectable prior to case creation. Select the options to apply to the evidence being added, then click <strong>OK</strong> to close the dialog.</td>
</tr>
</tbody>
</table>

When you are satisfied with the evidence options selected, click **OK**.

**Note:** To remove evidence from the list either before processing, or after it has been added to the case, select the evidence item in the list, then click **Remove**.

**Note:** When you export data from a case as an image, and then add that image as evidence in either the same case or a different case, the name of the image is renamed using a generic term. This prevents a user generated image name from being indexed with evidence.
To add a Mobile Phone Image

To add a Mobile Phone Image with FTK 7.6, Exterro has introduced native mobile image ingestion, processing and parsing. While ingestion follows the same workflow as typical image formats such as .AD1, .E01 etc., there are some caveats which are listed below.

**Supported Mobile Images**

- **Physical Extractions**
  - .Bin

- **Full File System with Keychain**
  - .Zip with Keychain.plist/Android Keystore

- **File System**
  - .Zip
  - .Tar

- **Android Backups**
  - .Ab

**Recommended Processing Options**

- **Exterro Mobile Parser**: To parse supported mobile applications. *Available in Expansion Options, expanded in Refinement Options.*

- **Generate System Summary**: To automatically generate a system related summary. *Available in Refinement Options.*

- **Android Backup**: To parse Android Backups. *Available in Expansion Options, expanded in Refinement Options.*
Processing Cellebrite UFD: File system, Full File system (Android and iOS), GrayShift Images (Android and iOS) and .TAR containers

1. Navigate to **Manage Evidence**.
2. Click on **Add** to add an evidence image.

3. Select **Individual File(s)**.
4. Select the Mobile Image (UFD or ZIP + Plist/Android Keystore):
   a. **UFD** – Select the UFD file and associated ZIP file. If the associated ZIP file is not selected, FTK will automatically select the ZIP file within the same directory.
   
   ![Image of Manage Evidence window]

   b. **ZIP** – Select the ZIP file. The associated .plist/Android Keystore file will be automatically selected by FTK.

   **Important:** Consider the following:
   - Evidence taken from any physical source that is removable, whether it is a “live” drive or an image, will become inaccessible to the case if the drive letters change or the evidence-bearing source is moved. Instead, create a disk image of this drive, save it either locally, or to the drive you specified during installation, then add the disk image to the case. Otherwise, be sure the drive will be available whenever working on the case.
5. Open **Refinement Options**.
6. Ensure the following options are selected:
   a. **Exterro Mobile Parser**: To parse supported mobile applications. **Available in Expansion Options**, expanded in **Refinement Options**.
   b. **Generate System Summary**: To automatically generate a system related summary. **Available in Refinement Options**.
7. Fill in the **ID/Name** field with any specific ID or Name data applied to this evidence for this case.
8. Use the **Description** field to enter an optional description of the evidence being added.
9. Select the **Evidence Group** that this evidence item belongs to. Click Manage to create and manage evidence groups.
10. Select the **Evidence Category** that this evidence item is associated to.
11. Select the **Time Zone** of the evidence where it was seized from the drop-down list in the Time Zone field. This is required to save the added evidence.
12. After selecting an Evidence Type, and browsing to and selecting the evidence item, the selected evidence displays under Display Name. The Status column shows a plus (+) symbol to indicate that the file is being added to the case.
13. Click **OK** to begin processing.

Processing Physical Extractions (.Bin)

1. Navigate to **Manage Evidence**.
2. Click on **Add** to add an evidence image.
3. Select **Acquired Image(s)**.

4. Select the Mobile Image (.bin).

**Important:** Consider the following:
Evidence taken from any physical source that is removable, whether it is a “live” drive or an image, will become inaccessible to the case if the drive letters change or the evidence-bearing source is moved. Instead, create a disk image of this drive, save it either locally, or to the drive you specified during installation, then add the disk image to the case. Otherwise, be sure the drive will be available whenever working on the case.

5. Open **Refinement Options**.
6. Ensure the following options are selected:
   a. **Exterro Mobile Parser**: To parse supported mobile applications. *Available in Expansion Options, expanded in Refinement Options.*
b. **Generate System Summary:** To automatically generate a system related summary. *Available in Refinement Options.*

7. Fill in the **ID/Name** field with any specific ID or Name data applied to this evidence for this case.
8. Use the **Description** field to enter an optional description of the evidence being added.
9. Select the **Evidence Group** that this evidence item belongs to. Click Manage to create and manage evidence groups.
10. Select the **Evidence Category** that this evidence item is associated to.
11. Select the **Time Zone** of the evidence where it was seized from the drop-down list in the Time Zone field. This is required to save the added evidence.
12. After selecting an Evidence Type, and browsing to and selecting the evidence item, the selected evidence displays under Display Name. The Status column shows a plus (+) symbol to indicate that the file is being added to the case.
13. Click **OK** to begin processing.

**Processing Android Backups**

1. Navigate to **Manage Evidence.**
2. Click on **Add** to add an evidence image.

![Manage Evidence Window](image)
3. Select **Individual File(s)**.

![](image1.png)

4. Select the Mobile Image (.bin).

![](image2.png)

**Important:** Consider the following:
Evidence taken from any physical source that is removable, whether it is a “live” drive or an image, will become inaccessible to the case if the drive letters change or the evidence-bearing source is moved. Instead, create a disk image of this drive, save it either locally, or to the drive you specified during installation, then add the disk image to the case. Otherwise, be sure the drive will be available whenever working on the case.

5. Open **Refinement Options**.
6. Ensure the following options are selected:
   a. **Android Backup**: To parse Android Backups. Available in Expansion Options, expanded in Refinement Options.
   b. **Exterro Mobile Parser**: To parse supported mobile applications. Available in Expansion Options, expanded in Refinement Options.
   c. **Generate System Summary**: To automatically generate a system related summary. Available in Refinement Options.

7. Fill in the ID/Name field with any specific ID or Name data applied to this evidence for this case.
8. Use the Description field to enter an optional description of the evidence being added.
9. Select the **Evidence Group** that this evidence item belongs to. Click Manage to create and manage evidence groups.
10. Select the **Evidence Category** that this evidence item is associated to.
11. Select the **Time Zone** of the evidence where it was seized from the drop-down list in the Time Zone field. This is required to save the added evidence.
12. After selecting an Evidence Type, and browsing to and selecting the evidence item, the selected evidence displays under Display Name. The Status column shows a plus (+) symbol to indicate that the file is being added to the case.
13. Click **OK** to begin processing.
To add new evidence to the case

1. Do one of the following:
   - Drag and drop the evidence file into the Manage Evidence > Evidence Name list field.
   - Click Add to choose the type of evidence items to add into a new case.

   **Important:** Consider the following:
   - Evidence taken from any physical source that is removable, whether it is a “live” drive or an image, will become inaccessible to the case if the drive letters change or the evidence-bearing source is moved. Instead, create a disk image of this drive, save it either locally, or to the drive you specified during installation, then add the disk image to the case. Otherwise, be sure the drive will be available whenever working on the case.
   - To add physical or logical drives as evidence on any 64-bit Windows system you must run the application as an Administrator. Otherwise, an empty drive list displays. If you encounter this problem on a 64-bit system, log out, then run again as Administrator.
   - While it is possible to add a CUE file as a valid image type, when adding a CUE file as “All images in a directory”, although adding the BIN and the CUE are actually the same thing the user gets double of everything.

   **Workaround:** Remove duplicates before processing.

2. Mark the type of evidence to add, and then click **OK**.

3. Click the **Browse** button at the end of the Path field to browse to the evidence folder. Select the evidence item from the stored location.

4. Click **OK**.

---

**Note:** Folders and files not already contained in an image when added to the case will be imaged in the AD1 format and stored in the case folder. If you select AD1 as the image type, you can add these without creating an image from the data.

5. Fill in the ID/Name field with any specific ID or Name data applied to this evidence for this case.

6. Use the Description field to enter an optional description of the evidence being added.

7. Select the **Evidence Group** that this evidence item belongs to. Click **Manage** to create and manage evidence groups.
8. Select the **Evidence Category** that this evidence item is associated to.

9. Select the **Time Zone** of the evidence where it was seized from the drop-down list in the **Time Zone** field. This is required to save the added evidence.

   After selecting an Evidence Type, and browsing to and selecting the evidence item, the selected evidence displays under Display Name. The Status column shows a plus (+) symbol to indicate that the file is being added to the case.

**To pause evidence processing**
- In the Data Processing Status window, select the **Pause** button.

   An entry will appear in the Messages box stating that the processing has been paused and listing the date and time it was paused.

**To resume evidence processing**
- In the Data Processing Status window, select the **Resume** button.

   An entry will appear in the Messages box stating that the processing has resumed and listing the date and time it resumed.
Working with Evidence Groups

Evidence Groups let you create and modify groups of evidence. You can share groups of evidence with other cases, or make them specific to a single case.

To create an evidence group
1. In Examiner, click Evidence > Add/Remove.
2. With an evidence item selected in the Display Name box, click Manage to the right of Evidence Group.
3. In the Manage Evidence Group dialog, click Create New to create a new Evidence Group.
4. Provide a name for the new evidence group, and mark the Share With Other Cases box to make this group available to other cases you may be working on.
5. Click Create to create and save this new group.
6. Click Close.

To modify an evidence group
1. In Examiner, click Evidence > Add/Remove.
2. With an evidence item selected in the Display Name box, click Manage to the right of Evidence Group.
3. To modify a group, highlight it in the list, and click Modify.
4. Make the changes to the group, then click Update.
5. Click Close.

To delete an evidence group
1. In Examiner, click Evidence > Add/Remove.
2. With an evidence item selected in the Display Name box, click Manage to the right of Evidence Group.
3. To delete a group, highlight it in the list, and click Delete.
4. Click Close.
Selecting Evidence Processing Options
The Evidence Processing options allow selection of processing tasks to perform on the current evidence. Select only those tasks that are relevant to the evidence being added to the case. See Configuring Default Processing Options for a Case on page 80.
After processing, the Evidence Processing options selected for this case can be found in the case log. You can also view them by clicking Evidence > Add/Remove. Double-click on any of the evidence items to open the Refinement Options dialog.
Some pre-processing options require others to be selected. For example:
- Data Carving depends on Expand
- KFF depends on MD5 hashing
- Flag Duplicates depends on MD5 hashing
- Indexing depends on Identification
- Flag bad extension depends on File Signature Analysis.

Different processing options can be selected and unselected depending on the specific requirements of the case.
At the bottom of every Refinement Options selection screen are the following options:
- OK: accepts current settings without saving for future use.
- Cancel: cancels the entire Detailed Options dialog without saving settings or changes, and returns to the New Case Options dialog.

If you choose not to index in the Processing Options page, but later find a need to index the case, click Evidence > Additional Analysis. Choose All Items, and check dtSearch * Index.

To set Evidence Refinement Options for this case
1. Click Refinement Options to open the Refinement Options dialog. Refinement Options are much the same as Detailed Options.

The sections available are:
- Evidence Processing: For more information on Evidence Processing options, see Selecting Evidence Processing Options (page 141).
- Evidence Refinement (Advanced): For more information on Evidence Refinement (Advanced) options, see Configuring Evidence Refinement (Advanced) Options (page 109).
- Index Refinement (Advanced): For more information on Index Refinement (Advanced), see Selecting Index Refinement (Advanced) Options (page 111).
2. Click **OK** to accept the settings and to exit the *Manage Evidence* dialog.
3. Select the **KFF Options** button to display the *KFF Admin* dialog.

---

**Note:** The AD Alert and the AD Ignore Groups are selected by default.

4. Click **Done** to accept settings and return to the *Manage Evidence* dialog.
5. Click **Language Settings** to select the code page for the language to be used for viewing the evidence.

   More detail is given in the following section.

6. Click **OK** to add and process the evidence.

---

### Selecting a Language

If you are working with a case including evidence in another language, or you are working with a different language Operating System, click **Language Settings** from the Manage Evidence dialog.

The Language Setting dialog appears, allowing you to select a code page from a drop-down list. When the setting is made, click **OK**.
Examining Data in Volume Shadow Copies

You can examine data that is contained in NTFS Volume Shadow Copies. In NTFS partitions, the Volume Shadow Copy Service (VSS) maintains a copy of every 16 KB block that is changed. These blocks are packaged up at predetermined times (which differ depending on the operating system being run) as a Volume Shadow Copy (VSC) or restore point. These restore points can contain data that has been renamed or deleted. They can also contain hidden malware, especially persistent code.

Encrypted drives are supported.

You can mount and process restore points as a separate evidence items within a case. When restore points are processed, a unique file system image for each restore point is created under the source NTFS partition.

You can view the files in the different file system images to analyze the difference between each restore point and the files that are unique to each one. This helps you see how a system has changed over a period of time. You can identify and parse files within the restore points and can search for evidence or malware hidden there.

You configure the processing of restore points when you add new evidence to a case. You can do this for a new case or an existing case. If the evidence that you are adding contains an NTFS partition with Volume Shadow Copy restore points, a Select Restore Points option is available. You can view all of the available restore points and select the ones that you want to process.

When viewing the restore point data, you can use the following VSC-related columns the provides details about the data.
VSC-related Columns

<table>
<thead>
<tr>
<th>VSC-Delta Restore Point End</th>
<th>Date of second restore point of a delta file</th>
</tr>
</thead>
<tbody>
<tr>
<td>VSC-Delta Restore Point Start</td>
<td>Date of first restore point of a delta file</td>
</tr>
<tr>
<td>VSC-Delta State</td>
<td>The state of a delta file as compared in two restore points</td>
</tr>
<tr>
<td>VSC-Renamed From</td>
<td>The name this file was renamed from</td>
</tr>
<tr>
<td>VSC-related Columns</td>
<td></td>
</tr>
<tr>
<td>VSC-Renamed To</td>
<td>The name this file was renamed to</td>
</tr>
<tr>
<td>VSC-Restore Point Date</td>
<td>Date of restore point this file came from</td>
</tr>
</tbody>
</table>

See Managing Columns on page 613.

About Restore Point Processing Options

When you select restore points to process, you select the following options:

- Which restore points to include
- The restore point expansion options (Delta/Full)

Restore Points Selection

If an NTFS partition has restore points, you can select which restore points to expand as file system images. Each restore point that you select is represented by a unique file system. You can select the Current files as well as any previous restore points.

Important: You can select to process one or more restore point. If you do not select a restore point, you cannot add it later within the same evidence item. You must re-add the NTFS partition.
as a new evidence item and then select the desired restore points.
Restore Point Expansion Options

You choose from the following expansion options.

Full    All restore points are added as full file systems. The benefit of this option is that you can view all of the files in all of the restore points. However, you will potentially have duplicate files, making the data set large. It can also make it more difficult to find the files that have been deleted or modified.

If “Full” restore option is selected, you are warned if more than one restore point is checked.

You can add the evidence item again if you don’t choose to add it as a restore point image originally. You can then choose restore points.

• Delta - Oldest to latest
• Delta - Latest to Oldest

Instead of creating a full partition for each restore point, one full partition is created for the oldest restore point selected while all newer restore points are created as deltas. The advantage of this option is that you do not have duplicate files and the contents of the other restore points are smaller, making it easier to find the files or folders that have been deleted or modified.

The latest restore point selected is created as a full image while all older restore points are created as deltas.
Managing Restore Points

**To process restore point file systems**
1. In either a new or an existing case, add new evidence, and select evidence that has an NTFS partition.
2. On the *Manage Evidence* page, click **Choose Restore Points**. If the button is active, then the evidence has an NTFS partition.

If the button is grayed out, the evidence does not have an NTFS partition.

When you click the button, if the NTFS partition does not have any restore points, a message is displayed.

3. Select the restore points that you want to process as file systems. See *About Restore Point Processing Options* on page 144.
4. Select the expansion option.
5. Click **OK**.
**Viewing Restore Point Data**

After the evidence with the restore points has been processed, you can view the data. You can view the created file systems for the restore points that you selected.

You can also add columns to the File List to display

**To view restore point file systems**
1. In the Examiner, click the **Explore** tab.
2. Select the evidence item and the NTFS partition.
3. You can view a file system image for each restore point.
4. You can view the content of each restore point to compare folders and files.
5. You can use VSC-related columns to view detailed data. See **VSC-related Columns** on page 143.
6. You can also use searches, filters, and so on to find and analyze the files in the share points.

**Note:** If you selected "Latest to Oldest", the tree will show Current first, but then the deltas are sorted by the oldest to the newest. If you selected "Oldest to Latest" the folders are sorted in the correct order.
Using Additional Analysis

After evidence has been added to a case and processed, you may wish to perform other analysis tasks. To further analyze selected evidence, click Evidence > Additional Analysis.

Most of the tasks available during the initial evidence processing remain available with Additional Analysis. See Evidence Processing Options on page 88.

Specific items can also be targeted. Multiple processing tasks can be performed at the same time. Make your selections based on the information in the table below. Click OK when you are ready to continue.

Additional Analysis Options

<table>
<thead>
<tr>
<th>Field Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hashing / Job Options Tab</td>
<td></td>
</tr>
<tr>
<td>File Hashes</td>
<td>These options create file hashes for the evidence. The Options are:</td>
</tr>
<tr>
<td>MD5 Hash</td>
<td>This hash option creates a digital fingerprint based on the contents of the file. This fingerprint can be used to verify file integrity and to identify duplicate files.</td>
</tr>
<tr>
<td>SHA-1 Hash</td>
<td>This hash option creates a digital fingerprint based on the contents of the file. This fingerprint can be used to verify file integrity and to identify duplicate files.</td>
</tr>
<tr>
<td>SHA-256</td>
<td>This hash option creates a digital fingerprint based on the contents of the file. This fingerprint can be used to verify file integrity and to identify duplicate files.</td>
</tr>
<tr>
<td>Flag Duplicates</td>
<td>Mark to flag duplicate files. This applies to all files in the case, regardless of the Target Items selected.</td>
</tr>
</tbody>
</table>

**Note:** A blank hash field appears for unallocated space files, the same as if the files had not been hashed at all. To notate in the hash field the reason for it being blank would slow the processing of the evidence into the case.

| KFF | Enables the Known File Filter (KFF) that lets you identify either known insignificant files that you can ignore or known illicit or dangerous files that you want to be alerted to. When you enable KFF, you must select a KFF Template to use. You can select an existing KFF Template from the drop-down menu or click ... to create a new one. See Getting Started with KFF (Known File Filter) on page 328. You can select to Recheck previously processed items when searching for new information, or when a KFF group is added or changed. Mark Recheck previously processed items if changes have been made to the KFF since the last check. |

<p>| Target Items | Select the items on which to perform the additional analysis. Highlighted, and Checked items will be unavailable if no items in the case are highlighted or checked. The following list shows |</p>
<table>
<thead>
<tr>
<th>Field Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>the available options:</td>
<td></td>
</tr>
<tr>
<td><strong>Highlighted Items:</strong></td>
<td>Performs the additional analysis on the items highlighted in the File List pane when you select Additional Analysis.</td>
</tr>
<tr>
<td><strong>Checked Items:</strong></td>
<td>Performs the additional analysis on the checked evidence items in the File List pane when you select Additional Analysis.</td>
</tr>
<tr>
<td><strong>Currently Listed Items:</strong></td>
<td>Performs the additional analysis on all the evidence items currently listed in the File List pane when you select Additional Analysis.</td>
</tr>
<tr>
<td><strong>All Items:</strong></td>
<td>Performs the additional analysis on all evidence items in the case.</td>
</tr>
<tr>
<td>PHash/Photo DNA</td>
<td>Enables PhotoDNA which lets you compare images in your evidence against known images in a library.</td>
</tr>
<tr>
<td></td>
<td>See About PhotoDNA on page 378.</td>
</tr>
<tr>
<td>Additional Indexing Options:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Opens the Indexing Options dialog.</td>
</tr>
<tr>
<td></td>
<td>See Configuring Case Indexing Options (page 96) for more information.</td>
</tr>
<tr>
<td>Additional Indexing Options:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Opens the Index Refinement (Advanced) dialog.</td>
</tr>
<tr>
<td></td>
<td>See Selecting Index Refinement (Advanced) Options (page 111) for more information.</td>
</tr>
<tr>
<td>Indexing / Tools tab</td>
<td></td>
</tr>
<tr>
<td>Indexed Search</td>
<td><strong>dtSearch® Index</strong></td>
</tr>
<tr>
<td></td>
<td>Choose dtSearch® Index to create a dtSearch index that enables instantaneous index searches. Marking dtSearch Index activates the Entropy Test check box.</td>
</tr>
<tr>
<td></td>
<td><strong>Entropy Test</strong></td>
</tr>
<tr>
<td></td>
<td>Select Entropy Test to exclude compressed or encrypted items from the indexing process.</td>
</tr>
<tr>
<td>Decryption</td>
<td><strong>Decrypt Dell Encryption Files:</strong></td>
</tr>
<tr>
<td></td>
<td>See Decrypting Dell Encryption Files (Dell Data Protection</td>
</tr>
<tr>
<td></td>
<td>If you select to decrypt Dell Encryption files, the File Signature Analysis option will automatically be selected as well.</td>
</tr>
<tr>
<td></td>
<td><strong>Perform Automatic Decryption:</strong></td>
</tr>
<tr>
<td></td>
<td>Attempts to decrypt files using a list of passwords that you provide.</td>
</tr>
</tbody>
</table>
Other Tools:

<table>
<thead>
<tr>
<th>Field Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Optical Character Recognition:</strong></td>
<td>Parses text from graphics images and adds them to the Index. Creates an additional file with the OCR extension. Click <strong>OCR Options</strong> to select specific graphics files to run the OCR process on, or to set limiting factors such as size, or grayscale. For more detailed information regarding OCR settings and options, see <strong>Optical Character Recognition (OCR)</strong> (page 102).</td>
</tr>
<tr>
<td><strong>Explicit Image Detection:</strong></td>
<td>Enables EID Options button. The EID license is purchased separately. This item will be disabled unless the license is detected on your CmStick. Click <strong>EID Options</strong> to select the processes to run. Choose default, speed, or accuracy settings. See <strong>Evaluating Explicit Material</strong> on page 436.</td>
</tr>
<tr>
<td><strong>Registry Reports:</strong></td>
<td>Enables Registry Summary Reports (RSRs) to be used directly from Registry Viewer if it is installed. Click RSR Directory to specify the location of any RSR templates you have saved or downloaded from the AccessData web site.</td>
</tr>
<tr>
<td><strong>Cerberus Analysis</strong></td>
<td>Performs a malware analysis on executable binaries. See <strong>About Cerberus Malware Analysis</strong> on page 303. See <strong>Running Cerberus Malware Analysis</strong> on page 321.</td>
</tr>
<tr>
<td><strong>Language Identification</strong></td>
<td>Analyzes the first two pages of every document to identify the languages contained within. The user will be able to filter by a Language field within review and determine who needs to review which documents based on the language contained within the document. See <strong>Identifying Document Languages</strong> on page 462.</td>
</tr>
<tr>
<td><strong>Document Content Analysis</strong></td>
<td>Analyzes the content and groups it according to topic in the Overview tab. When selected, the DCA Options button is also activated and opens the Document Content Analysis Options. See <strong>Using Document Content Analysis</strong> on page 558.</td>
</tr>
<tr>
<td><strong>Entity Extraction (Document Content)</strong></td>
<td>Identifies and extracts specific types of data in your evidence. You can select to process one or all of the following types of entity data:</td>
</tr>
<tr>
<td>****</td>
<td></td>
</tr>
<tr>
<td>****</td>
<td>● Credit Card Numbers</td>
</tr>
<tr>
<td>****</td>
<td>● Phone Numbers</td>
</tr>
<tr>
<td>****</td>
<td>● Social Security Numbers</td>
</tr>
<tr>
<td>****</td>
<td>In the Examiner, under the Document Content node in the Overview tab, you can view the extracted data. See</td>
</tr>
</tbody>
</table>
Cluster Analysis  
(AD Lab and Summation license only)
Invokes the extended analysis of documents to determine related, near duplicates, and email threads. 
See Performing Cluster Analysis on page 560. Configure the details by clicking Analysis Options.

<table>
<thead>
<tr>
<th>Field Item</th>
<th>Description</th>
</tr>
</thead>
</table>
| Cluster Analysis Options | (AD Lab and Summation license only) This lets you specify the options for Cluster Analysis. You can specify which document types to process:  
- Documents  
- Presentations  
- Spreadsheets  
- Email  
You can also specify the similarity threshold, which determines the level of similarity required for documents to be considered related or near duplicates. |
| Generate System Summary | Extracts data and populates the System Information tab. See Viewing System Information on page 547. |
| Persons of Interest | Scraps contact information from email signatures for use in conjunction with the “Communication Participants” list. |

**Miscellaneous tab**

**File Type Identification**  
*File Signature Analysis:* Analyzes files to indicate whether their headers or signatures match their extensions.  
If you select one of those options, the File Signature Analysis option is still automatically selected, but the option is not disabled and you can manually deselect it. Disable this option with care.  
This does not apply to the initial processing options.

**Carving**  
Carves data immediately after pre-processing. Click Carving Options, then select the file types to carve. Uses file signatures to identify deleted files contained in the evidence. All available file types are selected by default.  
For more information on Data Carving, see Data Carving (page 99).
The Carving option relies on the Expand Compound Files option to be enabled.

### Miscellaneous

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Expand Compound Files</strong></td>
<td>Expands and indexes files that contain other files. <strong>Include Deleted Files.</strong> Checked by default. Uncheck to exclude deleted files from the case.</td>
</tr>
<tr>
<td><strong>Meta Carve</strong></td>
<td>Carves deleted directory entries and other metadata. The deleted directory entries often lead to data and file fragments that can prove useful to the case, that could not be found otherwise.</td>
</tr>
<tr>
<td><strong>Create Thumbnails for Graphics:</strong></td>
<td>Generates thumbnails for graphic files found in the evidence. Thumbnails are always JPG format, regardless of the original graphic format.</td>
</tr>
</tbody>
</table>

### Field Item | Description

<table>
<thead>
<tr>
<th>Field Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create Thumbnails for Videos</td>
<td>Creates thumbnails for all videos in a case. You can also set the frequency for which video thumbnails are created, either by a percent (1 thumbnail every &quot;n&quot;% of the video) or by interval (1 thumbnail every &quot;n&quot; seconds). See Examining Videos on page 445.</td>
</tr>
<tr>
<td>Create Common Video File</td>
<td>When you process the evidence in your case, you can choose to create a common video type for videos in your case. These common video types are not the actual video files from the evidence, but a copied conversion of the media that is generated and saved as an MP4 file that can be previewed on the video tab. See Examining Videos on page 445.</td>
</tr>
<tr>
<td>EXIF for Videos</td>
<td>Parses XMP metadata (similar to EXIF data) from processed MP4 and most all other modern video file formats. When parsed from a video file, the metadata values are displayed on the Properties tab of the file viewer pane.</td>
</tr>
<tr>
<td>HEIC Conversion</td>
<td>Convert HEIC files to be viewed in the Native viewer.</td>
</tr>
</tbody>
</table>
### Hashing

When the MD5 Hash option is chosen for evidence processing, the MD5 hash value for every file item discovered within the evidence is computed. The same is true for SHA-1 Hash and SHA-256 options. In general, a hash value can be used (in most situations) to uniquely identify a digital file - much like a fingerprint can uniquely identify the person to whom it belongs.

Several specific purposes are served by enabling hashing during processing. First and foremost, when the MD5 Hash and/or SHA-1 Hash options are chosen along with the KFF option, each file item’s MD5 (and/or SHA-1) value can be found within the KFF Library. The KFF Library does not contain any SHA-256 values. All of the file items within the evidence that have been encountered and reliably cataloged by other investigators or US Federal Government archivists can be identified. This feature lets you find the “known” files within the evidence, which brings some intriguing advantages to the investigator.

These are described in Using the Known File Filter (KFF) (page 362).
Data Carving

Data carving is the process of locating files and objects that have been deleted or that are embedded in other files.
You can recover and add embedded items and deleted files that contain information that may be helpful in forensic investigations.
The data carving feature allows the recovery of previously deleted files located in unallocated space. Users can also carve directory entries to find information about data or metadata.

**Note:** You can create custom carvers. In addition, you can manually carve for any file type for which you have the correct header/footer/file length information, then save that file and add it to the case. In addition, you can carve any data from any file, and save the selected data as a separate file and add it to the case.

See also Custom Carvers (page 101).
To recover embedded or deleted files, the case evidence is searched for specific file headers. Using the data from a file header for a recognized file type the length of that file is determined, or the file footer is found, and “carves” the associated data, then saves it as a distinct file. A child object is created with a name reflecting the type of object carved and its offset into the parent object’s data stream. Embedded or deleted items can be found as long as the file header still exists.

Data carving can be done when adding evidence to a case, or by clicking Evidence > Additional Analysis > Data Carve from within a case.

**Recognized File Types for Data Carving**
- AOL Bag Files . LNK Files
- BMP Files . OLE Archive Files (Office Documents)
- EMF Files . PDF Files
- EML Files . PNG Files
- GIF Files . TIFF Files

Working with Static Evidence  Hashing | 175
Chapter 11

Recognized File Types for Data Carving (Continued)

- HTML Files
- Zip Files
- JPEG Files

You can set additional options to refine the data carving process for the selected file types.

Data Carving Files When Processing a New Case

Data Carving can be done during initial case creation by setting preprocessing options, or later, as an Additional Analysis task.

Viewing the Status and Progress of Data Processing and Analysis

The Data Processing Status screen lets you view the status of any processing, analysis, or searching that is being done on evidence in a case. This screen is also called the Progress Window.

To view the status and progress of data processing and analysis

1. In the Examiner, click View > Progress Window to open the Data Processing Status screen. Processing is categorized according to the following job types:
   - Add Evidence
   - Additional Analysis
   - Live Search
   - Other
2. Click on a job type in the left pane, to view aggregate progress statistics for all of the items in a job type.
3. Click the expand icon to the left of a job type and then select an individual job or task to view the status of jobs and tasks.

Details about each task in a job are displayed in the right hand pane under Messages. You can also view the following status information about job processing:
# Chapter 11

**Information** | **Description**
--- | ---
Overall | The percentage complete as each task progresses.
**Discovered** | The number of items that have been discovered.
**Processed** | The number of items that have been processed. If you compare the numbers in the *Data Processing Status* screen with the numbers shown in **Overview tab > Case Overview > File Category**, for example, you may notice that the numbers are not the same. If there is a difference, the numbers in the case are accurate; the numbers in the *Data Processing screen on the progress bar items* are not.
**Indexed** | The number of items that have been indexed.
**Process State** | The current status of a job's processing. When the job is complete, this field displays Finished, and the Message box in the right pane also displays Job Finished.
**Name** | The file name of the evidence item that is processing in a task.
**Path** | The path to where the evidence item is stored.
**Process Manager** | The Process Manager computer is listed by its name or by its IP Address. If your Evidence Processing Engine runs on the same computer as the *Examiner* and the database, then "localhost" is the default Process Manager. If you are using Distributed Processing, the Process Manager or the Remote Processing computer is listed.

4. You can select from the following options:

- **Job Folder** lets you open the location where the JobInformation.log for this job is stored. You can view detailed information about the processing tasks and any errors or failures in the JobInformation.log file.
- **Remove when finished** lets you remove a task or job from the job list when it has completed processing.
- **Pause** lets you pause the current evidence processing task and adds an entry in the Messages box listing the date and time it was paused.
- **Resume** lets you resume the current processing task after having paused it and adds an entry in the Messages box listing the date and time processing was resumed. This option only appears after the **Pause** option has been enabled.
Chapter 11

- **Cancel** lets you stop the current task from running.

5. Click **Close** to close the display but not cancel any current tasks.

Viewing Processed Items

It is not necessary to wait for the program to finish processing the case to begin viewing data. The metadata— the information about the evidence—can be viewed in several modes before the evidence image has completed processing.

**Important:** Do not attempt to do any search prior to processing completion. You can view processed items from the tabbed views, but searching during indexing may corrupt the index and render the case useless.

Editing the Processing Management Queue

It is possible to adjust the processing queue in order to move high priority evidence items to the top of the list. This can be done by the Application Administrator.

**To edit the evidence processing queue**

1. Add evidence items to the processing queue as normal. For more information, see [Adding Evidence](page 136).
2. Once the items are in line for processing, navigate to **Evidence > Manage Processing**.
3. In the *Manage Evidence Processing* window, select the desired evidence items and click either the **Move Up** or **Move Down** buttons, depending on how you’d like to arrange the items in the processing queue.

**Note:** Processing will have already begun by the time you change the processing priorities and your desired item may not be first on the list. It will be the first priority once the item(s) currently processing complete.
Chapter 11
Viewing Evidence Information

Evidence Tracking
Evidence information for all evidence items created using Imager, MPE+, or Cellebrite are available for export. This allows for proper tracking of evidence.

To view Imager or MPE+ processed evidence information
1. In the Manage Evidence dialog, click on the desired evidence item in the list on the left to highlight it.
2. Click the View Evidence Info button.

A text file will open displaying the following information for the selected evidence item.

Evidence Tracking Data
General Information
Name of the evidence item
Case information
Product and version of the software used to acquire the evidence image
Case number
Evidence number Unique description
Examiner who processed the case
Any notes entered when the case was acquired

Physical Evidentiary Item(Source) Information
Device Information Source type
Drive Geometry Bytes per sector Sector count
Image Image type
Source data size Sector count
Computed Hashes MD5 checksum SHA1 checksum
Image Information Acquisition started Acquisition finished
General Information
Segment list
Image Verification Results Verification started
Verification finished MD5 checksum SHA1 checksum

To view Cellebrite-processed evidence information
1. Select the Cellebrite image (UFDR) from the Evidence Items panel on the Explore Tab.
2. In the File List, select the file named Extraction Summary.
3. The evidence tracking information for the selected file will appear in the File Content pane, in Cool HTML. It is also contained in the report.xml file, found in the File List, which can be exported.
Chapter 11
Acquiring Live Evidence

Using AD Enterprise, you can acquire live evidence from local and remote network computers. See also About Acquiring Digital Evidence (page 29) for details on the ways that evidence can be acquired, and precautions to take before acquiring evidence.

This chapter includes the following topics

- **About Live Evidence** (page 159)

- **Local Live Evidence**
  - Acquiring Local Live Evidence (page 160)
    - About Local Live Evidence (page 160)
    - Adding Local Live Evidence (page 160)

- **Remote Live Evidence**
  - About Acquiring Remote Live Evidence (page 161)
  - About the AccessData Enterprise Agent (page 163)
  - Adding Remote Data (page 167)
    - Browsing and Selecting Nodes (page 168)
    - Acquiring Volatile Data (page 175)
    - Acquiring Memory Data (page 177)
    - Acquiring Drive Data (page 180)
    - Mounting a Device (page 182)
    - Collecting Filesystem Data (page 184)
    - Acquiring Remote Data from macOS Managed Agents (page 196)
  - Site Server Data Collections (page 201)
  - Data Sources (page 204)
  - Collections (page 224)
Acquiring Local Live Evidence

Data that you gather and process from an active data source is called live evidence.

_Types of Live Evidence_

Live evidence is data that you gather and process from an active data source. It is important to understand any implications of acquiring data live. See _About Acquiring Digital Evidence_ on page 29.

You can acquire and investigate the following types of live evidence:

- Local - Live evidence from an original drive or other electronic data source that is attached to the investigation computer

See _Acquiring Local Live Evidence_ on page 160.

- Remote - Evidence from one or many Agents installed on workstations within the network. See _About Acquiring Remote Live Evidence_ on page 161.

_About Local Live Evidence_

An example of local live evidence is an original drive or other electronic data source that is attached to the investigation computer. It can also be data acquired from a device on a remote computer while the device is mounted to the system as Read/Write.

When adding live evidence you can select from the following evidence types:

- The contents of a directory (local or network share)
- An individual file
- A Physical drive
- A Logical drive
Acquiring Local Live Evidence

Adding Local Live Evidence
You can add live evidence and then create a static image of that data. You can also add the data without creating an image, but realize that as the files are read, the operating system makes changes to the file statuses, the Read date and time stamps, and the Accessed time and date stamps. You can add the entire contents of a folder or a single file from a device that is attached to the Examiner machine.

To add local live evidence to a case
1. In Examiner, click Evidence > Add/Remove.
2. In the Manage Evidence dialog box, click Add.
3. Do one of the following:
   - Click Contents of a Directory, then click OK. Browse to and select the directory. Read the warning. To continue click Yes.
   - Click Individual Files, then click OK. Browse to the location, select one or more files. You can use Shift-Click or use Ctrl-Click to select multiple files. Read the warning. To continue click Yes.
   - Click Physical Drive, then click OK. Read the warning. To continue, click Yes. Select a drive. The drives are listed in UNC format and are pre-pended with the string: PHYSICALDRIVE. Click OK.
   - Click Logical Drive, then click OK. Read the warning. To continue, click Yes. Select a drive. The drives are listed by drive letter. Click OK.
4. A job is created and the Data Processing Status window opens. Live Evidence Jobs are displayed under Add Evidence Jobs.
5. Click Close.
Enterprise lets you run jobs that provides for the real-time acquisition of live remote evidence from one or many Agents installed on workstations within the network. Using Enterprise Examiner, you can gather many types of active information from your firm’s network computers, including information in RAM, processes being run, and much more. This type of evidence is known as remote live evidence.

Types of Remote Data
You can acquire data directly from computers on your network. This data is called remote live evidence. The process of adding the data into a case is called remote data acquisition. Enterprise allows you (depending on your rights and permissions) to remotely and discretely acquire forensic snapshots of the following information.

Types of Remote Data to Acquire

- Process Info
- Services Info
- DLL Info
- Driver Info
- User Info
- Open Handles
- Network Sockets
- Network Devices
- Registry Info

- RAM
- Memory Search
- Physical Drives Logical Drives Mounted Devices Filtered File Systems

Administrative rights and permissions are required on the remote computer to collect remote live evidence. See Requirements for Adding Remote Data on page 162.

**Note:** If the Mozilla Firefox directory is added as evidence while in use, the history, downloads, and so forth that are normally acquired, are identified as zero-length files.
Volatile Data

Some live evidence like processes and services information may fluctuate and change frequently. This evidence is called volatile data. Volatile data is different than memory data and does not contain the same information as a Memory Data (RAM) acquisition. A RAM acquisition downloads all the RAM data into a memory dump, and then it is read and processed when you add it to a case.

Volatile Data is different from Memory Data. Volatile data is acquired quickly through OS API calls, and does not get all of the information a Memory Data (RAM) acquisition gets on its own. The RAM acquisition downloads all the RAM data first in a memory dump, then reads and processes it when it is added to the case.

Drive Data

Drive Data includes both physical (including USB flash drives, memory sticks, external hard drives, etc.) and logical drives (normally accessed by local drive letter), as well as mounted devices that are available on a selected Agent Source node.

Memory Dump

Another type of evidence that you can add is a memory dump from a computer on your network.

Requirements for Adding Remote Data

To add remote data in Enterprise, you must meet the following requirements:

- Enterprise must have a current license.
- Your user account must have role assignment with adequate permissions to be able to access the Add Remote Evidence dialog.
- The Enterprise System Administrator assigns roles to examiners. These roles determine which nodes, or network user machines an examiner is authorized to investigate and what types of information the Examiner can access.
- The agent must be installed on the target computer(s). For more information on available Agents and their installation. See About the AccessData Enterprise Agent on page 163.
- Ensure that the system date and time on all machines are synchronized, or at least close. If the target machine is behind by more than 24 hours, the Agent connection will work, but you will not be able to acquire data.
- Enterprise must be run As Administrator in order to push agents to remote machines.
About the AccessData Enterprise Agent

In order to add remote data from computer nodes, you must install the AccessData Enterprise Agent on them. The following agents are supported:

- **Windows Agent** - See [Installing and Using the Windows Agent](#) on page 164.
- **Linux Agent** - Must be installed manually. See [Installing the Linux Agent](#) on page 688.
- **Mac Agent** - Must be installed manually. See [Installing the Mac Agent](#) on page 691.

The Enterprise Windows Agent is made up of the following components:

- **agentcore.exe** - This is the main service executable that runs as the service named AgentService. This is the service which is always running.
- **agent modules** - depending on the type of data you are collecting, the core uses different modules. For example, there are modules for collecting memory data, volatile data, drive data, etc. Each module is an exe which gets run when that kind of task is initiated. When the task is complete, the module will close. The modules that can run are addm, diskpreview, memory, netfs, remediate, rim, volatile.

Agent files are commonly updated with Enterprise releases.
Communication to and from the Enterprise agent is encrypted and authenticated using the asymmetric key in the SSL certificate configured in the Enterprise system.

Certificates

Whichever type of certificate you use, a copy of the certificate files must be stored in a place where AD Enterprise will always have access and permissions to read them. During installation or configuration changes, you will need to enter the file path to your certificates in the following places:

- **Agent Configuration**
  
  This is found in the Case Manager at the following path: **Tools > Preferences**.

- **Configure Agent Push**

  This is found in the Examiner at the following path: **Tools > Configure Agent Push**.

See [Configuring Windows Agent Cert Settings](#) (page 164) for more information on creating these settings.

**Note:** You need to create only one set of certificate keys. (where the public key certificate is exported from the private key container). All deployment methods can use the same certificate pair.
Configuring the Agent Push

Installing and Using the Windows Agent

About the Windows Agent

- Memory Analysis
- Import Memory Dump
- Volatile Memory

Methods of deploying the Enterprise Agent

You can use the following methods to deploy the Enterprise Agent:

- **Auto Deployment**: You can push the Agent using the Enterprise application. See Installing the Windows Agent through Enterprise on page 164.

- **Manual Deployment**: Using the agent binary (FTKagent.exe) and pre-created certificate running on the target machine.

See Manually Installing the Windows Agent on page 674.

- **Network Deployment**: Agents can be deployed using Active Directory, SMS, SCCM, or other means of package deployment available to you using the same command line options described in “Manually Installing the Windows Agent” on page 674. Policies can be set for auto-renewal and for updating.

When the agent is installed, the default path is Program Files > AccessData > Agent. The modules are installed in the Modules subfolder.
Configuring the Agent Push

Installing the Windows Agent through Enterprise

Configuring Windows Agent Cert Settings

In order to push and use the Windows Agent, you must provide private and public keys of your certificates. You can also configure an Agent List which allows you to select which agents to run jobs on.

**To configure**

1. In the Case Manager, click **Tools > Preferences**.
2. In the Agent Configuration box, enter the paths for your certs.

For more information about agent certs, see Using Agent Certs in Forensics Products (page 680). The default port value that is used to communicate with the agent is 3999. The configured port is also added to a rule in the firewall on the agent computers. The certs are installed in the Program Files > AccessData > Agent > Config folder. The private cert is names a unique GUID ID number.

Before pushing the agent, you must verify that all file paths are configured correctly.

**To configure the Agent Push**

1. Open the case where you want to add remote data.
2. Click Tools > Configure Agent Push...
3. Verify that all settings are configured. They should be populated by default based on your installation paths and the key folders you previously configured.

Pushing the Windows Agent to Remote Computers

You can use Enterprise to install the Windows Agent on remote computers. The Agent software will be installed on multiple nodes using different jobs simultaneously.

**Note:** After installing the agent, there is no list in Enterprise that shows you the computers with the agent installed.
Configuring the Agent Push

To remotely push the Windows Agents to remote computers
1. Open the case where you want to add remote data.
2. Click Tools > Push Agents....
3. You can use one of the following methods to specify which computer nodes to install the Windows Agent on:
   - Using Add to manually specify the computers. If you don’t have many computers to specify at the time, you can add a computer to the list one at a time. You can enter the full computer name or IP address and then click Add. You can repeat as often as desired.
   - Importing a list of computers. Click Import and select a valid TSV file. Importing Computers from a TSV File (page 166)
4. (Optional) Use custom agent name. You can change the default name of the service or executable name. This is available so that you can mask the type and purpose of the agent on the computers.
5. (Optional) Update the agent if it is present. Select this option to update any previous versions of the Enterprise agent that may be installed on the selected computers. This action will uninstall the old agent and pushes out the new agent.
6. (Optional) Allow manual install. This option lets a user uninstall the Windows Agent using the local computer’s Control Panel > Uninstall a program list. If this option is not selected, the user does not have permissions to uninstall it.
7. (Optional) Use WMI Push only. By default, Enterprise uses remcom to push the agent. You can select this option to use WMI. You may need to select this option if your environment requires WMI.
8. Click OK.
9. In the Credentials dialog, enter the credentials required to install the agent and click Add.

You can add multiple credentials that can be tried, for example the domain Administrator’s credentials. Note: These credentials are not stored when you close Enterprise.
10. Click OK.
Importing Computers from a TSV File

You can import a list of multiple computers from a TSV file. You can import a TSV file for either of the following tasks:

- Configuring the list of computers to push the Windows Agent to.
- Configuring the list of computers in the Agent List for selecting which computers to run jobs on.

Note: Pushing the Windows Agent to a computer does NOT automatically add the computer to the Agent List.

To create a valid TSV file

1. Start by creating a CSV file, such as using a spreadsheet.
2. You must have at least two columns:

The first column is a friendly name (of your choosing) of the computer.
The second column is the node host name (fully qualified domain, IP address, or IP Range) of the computer.
For example:

Node1    123.22.24.35
Node2    test.data.com
Group1   123.23.3.0-123.23.3.55

3. (Optional) You can have optional third and/or fourth columns. The third column is a textual description of the computer.

The fourth column is the IP address (for example, if you used the FQDN). For example:

Node1    123.22.24.35    George’s computer    123.22.24.35
Node2    test.data.com    John’s computer    123.22.24.65
Group1   123.23.3.0-123.23.3.55    Dev group

4. Save the list as a TSV file (in Excel “Save as Type: Text (Tab delimited) (*.txt)”)
5. Rename file extension to *.TSV
Importing Computers from a TSV File

Uninstalling the Windows Agent Remotely

You can uninstall the Windows Agent from one or more computers remotely.

To remotely uninstall the Windows Agents from remote computers
1. Open the case where you added remote data.
2. Click Tools > Push Agents....
3. You can do one of the following to select which computer nodes to uninstall the Windows Agent from:
   - Using Add to manually specify the computers. If you don’t have many computers to specify at the time, you can add a computer to the list one at a time. You can enter the full computer name or IP address and then click Add. You can repeat as often as desired.
   - Importing a list of computers. Click Import and select as valid TSV file. Importing Computers from a TSV File (page 166)
4. Select Uninstall agent.
5. Click OK.
Adding Remote Data

Although your primary role might be to acquire forensic evidence from a user’s machine, you can also use Enterprise to detect malware, viruses, or other software that might jeopardize your organization. To acquire remote data from a user’s computer, the Enterprise Agent must be running on the remote computer and you must be granted the appropriate rights by the Enterprise System Administrator.

There are two distinct interfaces for acquiring remote workstation data via the Enterprise agent depending on what OS is running on the endpoint. For macOS acquisitions, “How to acquire data from macOS managed agents:” on page 167.

How to acquire data from Windows, Linux/Unix, or legacy Mac OS X agents:

1. Open your case in Enterprise Examiner and click Evidence > Add Remote Data...

The Add Remote Data window enables you to select the Agents and the types of data you want to collect.

2. Configure the acquisition job by doing the following:

2a. Select the nodes that you want to collect from.
See Browsing and Selecting Nodes on page 168.
2b. Select the information that you want to gather. See Selecting which Data to Add on page 173.
2c. Configure acquisition options.
See Selecting Acquisition Options on page 173.
2d. Configure Agent options.
See Installing and Updating Windows Agents during a Job on page 174.
2e. Configure Resource Usage.
See Indicating the Level of Resource Usage on page 174.
2f. Configure job preferences.
See Configuring Job Preferences on page 174.
3. Click OK to start the job.

How to acquire data from macOS managed agents:

1. Ensure FTK Plus is installed locally to the system hosting AD Enterprise.
2. Ensure the ExterroSelfHostService is running.
3. Open your case in Enterprise Examiner and click Evidence > Add Remote Mac Data...
4. Depending on the type of investigation, you might configure the acquisition job based on one or more of the following sample workflows:

4a. Standard User Data Collection Workflow (page 198)
4b. macOS Agent Logical Disk Acquisition Workflow (page 199)
**To add a network node or branch**

**Browsing and Selecting Nodes**

The *Browse and Select Nodes* panel lets you select the Agents that you want to run an acquisition job on. When the *Add Remote Data* window is first launched, this panel is empty.

To populate the *Browse and Select Nodes* panel, you can use multiple methods.

### Browse and Select Nodes

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Browse and Select Nodes box</strong></td>
<td><img src="image" alt="Browse and Select Nodes box" /></td>
</tr>
<tr>
<td><strong>Red text:</strong></td>
<td>Current user does not have rights to access the agent.</td>
</tr>
<tr>
<td><strong>Black text:</strong></td>
<td>Current user has rights to access the agent.</td>
</tr>
<tr>
<td><strong>Grayed out:</strong></td>
<td>Enterprise is unable to communicate with the agent.</td>
</tr>
</tbody>
</table>

**Agent Source buttons**

- **Load Available Agents from Active Directory.**
  - This button is hidden (disabled) by default. For more information, see below.
  - If you load an Agent from Active Directory, ensure the node was defined by hostname. To enable this option, the following string values would need to be deleted:
    - **x64 Key**
      - `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\AccessData\Enterprise | DisableAD(String value)`
    - **x32 Key**
      - `HKEY_LOCAL_MACHINE\SOFTWARE\AccessData\Enterprise | DisableAD (String value)`
  - See *Check Agent Connections* on page 171.

- **Load Available Agents from the Agent List.**
  - This will load the list of Agents that is configured in the Agent List.
  - See *Using the Windows Agent List* on page 169.
  - You can test the agent connection nodes in the list. See *Check Agent Connections* on page 171.
To add a network node or branch

Load Available Agents from Text Box.

If you know the Node Names or IP Addresses of the Agents you want to examine, click this icon to enable the Manual Entry group box. Enter the information and click Add.

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Show all Loaded Agents from all Sources.</td>
</tr>
<tr>
<td></td>
<td>Show all Checked Agents from Any Source.</td>
</tr>
</tbody>
</table>

**Check Agent Connection**

You can verify whether the selected nodes can connect to Enterprise. See Check Agent Connections on page 171.

**Manual Entry**

You can manually add a node by entering its name or IP address and then click Add.

**Load from file...**

You can load agents from a saved Agents file. To load agents from multiple files, use commas to separate the agent names (e.g., agent1, agent2, etc.).

**Agent Filter**

Narrow the list of agents to view in the Browse and Select Nodes pane. See Filtering Agents on page 172.

**Hide unauthorized agents**

Hide agents from the list that are not authorized.

**Import**

See Exporting and Importing AccessData Agent Lists (ADAL) on page 172.

**Export**

See Exporting and Importing AccessData Agent Lists (ADAL) on page 172.
To add a network node or branch

Using the Windows Agent List

The Agent List allows you to add, import, and delete individual nodes from the list of agents. When you Add Remote Data, you can select computers based on this Agent List.

It is also possible to Select All or Select None of the nodes in the list using the corresponding buttons found beneath the Agent List.

See Browsing and Selecting Nodes on page 168.

---

**Note:** Pushing the Windows Agent to a computer does NOT automatically add the computer to the Agent List.

---

Adding Nodes to the Agent List

You can add a network node or branch to the Enterprise agent list.

1. In the Case Manager, click **Tools > Preferences**.
2. In the Agent Configuration box, click **Agent List**.
3. In the Agent List window, Click **Add**.
4. Enter a **Friendly Name** for the network node or branch.
5. Use any of the following to identify the branch’s nodes:
   - IP Address
   - FDQN or Hostname
   - IP Range (not supported when acquiring macOS agents)
   - From File... Upload a TSV file containing a range or class of IP addresses. For details, see Importing Computers from a TSV File (page 166)
6. The From AD... button is available to import computer records from Active Directory on systems where that has been configured.
7. Select the **is Mac** checkbox to define which agent nodes are running the macOS managed agent. See About macOS Managed Agent on page 692.
8. Click **OK**.
To add a network node or branch

Modifying Nodes

You can modify the attributes of an existing node.

To modify an existing node’s attributes
1. Locate the node in the Agent List table.
2. Select the information you wish to modify.

If you wish to modify the IP address, you will need to delete the node and add a new one.
3. Make the desired changes.
4. Click OK.

Note: When you edit a node that has been selected in a role, that node will no longer be selected in that role. It must be re-assigned.

Assigning Nodes to Roles

You can assign specific nodes to an existing Role.

To assign a node (or nodes) to a Role
1. Navigate to the Agent List panel.
2. Click the Roles button.
3. In the Manage Agent Roles window, select the Role for which you want to assign nodes.
4. Check the boxes next to the Agents you wish to assign to that Role.
5. Click OK.
Check Agent Connections

You can select nodes (individual or click All) and then click **Check Agent Connections** to verify that Enterprise can communicate with the Agent on those nodes. Agents displayed in the Browse and Select Nodes pane are color-coded to indicate their type and status.

**Agent Status Color Codes**

<table>
<thead>
<tr>
<th>Agent Color</th>
<th>Agent Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red</td>
<td>You do not have rights to access the Agent.</td>
</tr>
<tr>
<td>Black</td>
<td>You have rights to access the Agent. Click the Agent to select it.</td>
</tr>
<tr>
<td>Green</td>
<td>The Agent you selected is available and that Enterprise can communicate with it. The box next to the Agent is checked.</td>
</tr>
</tbody>
</table>
| Grey        | Enterprise cannot communicate with the Agent you selected. The following conditions may exist:  
  ● The computer may be offline or shut down.  
  ● The Agent software may not be running properly.  
  ● The Agents certs may not be configured correctly. |
| Purple      | Selectable range of Agents. |
Filtering Agents enables you to narrow the list of agents to view in the Browse and Select Nodes pane.

**To filter the Agents list**
1. In the Agent Filter text field below the Agent Source box, type the node name or the IP addresses of the machines to include. If manually adding multiple Agents, separate each with a comma and a space.
2. Mark *Hide Unauthorized Agents* to filter the list to show only the agents that you are authorized to access.

Exporting and Importing AccessData Agent Lists (ADAL)
You can export and import Agent lists that you have created. This is a convenient way of grouping and accessing Agent lists that you use frequently.

**Exporting an AccessData Agent List (ADAL)**

After you have selected a common list of Agents, you can save them to a file to use later.

**To export an Agent list**
1. Open Evidence Explorer and navigate to the Evidence >> Add Remote Data dialog
2. When all needed Agents are added to the **Browse and Select Nodes** pane, mark the check boxes for the nodes to include in the exported list.
3. Select the Agents you want to add to the export list.
4. Click **Export**
5. In the **Export Agent List** dialog, choose **Selected Agents Only** to export only the Agents selected in the **Browse and Select Nodes** pane, or choose **All Agents** to export the entire list of Agents.

*Important:* When exporting lists, be cautious when selecting “All Agents” (especially with large lists such as Active Directory listings) as it may take a very long time to import these lists.
6. Enter or browse to a file path and provide a filename (all export files have the .adal extension).
7. Click **Save** to save the export list and return to the **Export Agent List** dialog.
8. Click **OK**.
Importing an AccessData Agent List (ADAL)

1. Open Evidence Explorer and navigate to the Evidence >> Add Remote Data dialog
2. Click Import.
3. Select the Agent List [agentlist.adal] to import.
4. Click Open.

Selecting which Data to Add

Once you select a Node in the Browse and Select Nodes pane, the Selection Information panel will activate. In this panel, you will select the information you wish to add to your case.

Important: The Selection Information will only apply to the highlighted agent.

To apply a Selection Information option to ALL checked agents:

1. Click the Preferences button. Select the items you want to collect for all agents.
2. Check the Apply to Selected box.
3. Click OK.

Note: If you do not check the Apply to Selected box, nothing will be added to the Selection Information.

You can do the following:

- Acquiring Volatile Data (page 175)
- Acquiring Memory Data (page 177)
- Acquiring Drive Data (page 180)
- Mounting a Device (page 182)
- Collecting Filesystem Data (page 184)
**Selecting Acquisition Options**
Select the Acquisition Options to use. Choices are:
- Include Hidden Processes
- Include Injected DLLs

**Installing and Updating WindowsAgents during a Job**
When running a Add Remote Data job on selected nodes, you can specify to install or update the Windows agents on nodes if needed.
However, it is recommended that you install the Agent using the Tools > Push Agents option. See Pushing the WindowsAgent to Remote Computers on page 165.

**To install or update Windows Agents**
1. Select one or more nodes.
2. Select the information you want to collect.
3. Check the box next to Install or Update Agent Modules. Mark one of the following:
   - Agent and Modules
   - Modules only

**Note:** The newer Agent and Agent Module files must be available if you want to install them to themachine with an older Agent.

**Important:** Earlier Agents do not need to be updated to work with the Enterprise.
4. Click OK.

**Indicating the Level of Resource Usage**
You can control the level of resource usage on remote target machines. Choose from High, Medium, or Low.
High resource usage may slow the agent machine’s performance, and may arise suspicions about the source of disk activity. Low resource usage makes the acquisition take longer, but it is easier to maintain the stealth of the acquisition.
Select the level of resource usage that will cause the user of the Agent system the least amount of inconvenience or suspicion of being monitored.
Configuring Job Preferences

In the Add Remote Data >> Preferences dialog, you can define which acquisition data types you want preselected by default for each acquisition job.

Mark the Apply to Selected checkbox to associate the currently selected data types to each of the nodes listed for the acquisition job.

Acquiring Volatile Data

To open the Add Remote Data dialog, from the Enterprise Examiner UI, click Evidence > Add Remote Data.

Once the remote data is added to the case, it is stored as xml data and in the database and will appear in the Volatile tab.

See Examining Volatile Data on page 538.

To acquire Volatile data

1. Use the Agent Source Selection Box to select Agents for examination.

For more information about selecting Agents, see Browsing and Selecting Nodes (page 168).

2. Select an Agent by marking the check box next to it.

3. Select the type of remote information to include in the Selection Information pane:
   - Process Info (on a Linux based machine, some processes may return a hash value of 0 as these are forked processes, drivers or routines from a parent process.)
   - Services Info
   - DLL Info
   - User Info
   - Open Handles
   - Network Sockets
   - Network Devices
   - Registry Info (this takes more time to collect and should be excluded if acquiring from a Linux based machine)

Mark Include Volatile Data to automatically mark all Volatile Data types, or mark each type individually.

4. When selecting Include Volatile Data > Registry Info, the Acquire Registry Keys dialog will open once you click OK. You must select the root key and at least one subkey, or no data will be acquired for that selection.

4a. Enter in the specific subkey to be included, such as HKEY_LOCAL_MACHINE > SOFTWARE, or mark the Include Subkeys box.

4b. Retrieving large numbers of Registry keys from large numbers of Agents, such as from a range
of Agent IP Addresses, is very memory-intensive. AccessData recommends that you limit the number of Agents, the number or Registry keys, or both to maximize efficiency.

5. If selecting multiple agents, each one can collect different data. The chosen Selection Information items will apply only to the highlighted node. To apply a Selection Information option to all the checked agents, click the Preferences button, select the options you want to collect for all agents, and check the Apply to Selected box. Click OK to close the Selection Preferences box.

**Note:** If you do not check the Apply to Selected box, nothing will be added to the Selection Information.

6. Click OK.

**Saving Volatile Data to a Static File**
Once you collect the volatile data, you will want to save it before you begin your examination. This prevents the live data from changing or disappearing as you examine the evidence.

**To save live data to a static file:**
1. Once the live data has populated in the Explore tab, use quickpicks to select the top item in the file tree and select File > Export to Image.
2. In the Create Custom Content dialog, select All Listed Items. Click OK.
3. In the Create Image dialog, select an image destination by clicking Add.
4. In the Select Image Destination dialog, enter the desired Image Destination Folder and Image Filename. Click OK.

It is possible to enter additional information in this dialog, but not required.

5. In the Create Image dialog, select any desired options and click Start.

**Important:** Do not select the Add image to case when completed option. You will need to open a new case in order to avoid duplicate data. If you are required to keep the evidence in the same case, remove the Live Preview data by going to Evidence > Add/Remove and removing the original evidence file before adding the newly-created AD1.
Acquiring Memory Data

Memory dumps can be a good source of forensic artifacts. When you acquire live RAM for analysis, you can save the memory data to a dump file for use later in this or another case, or you can download the contents of the RAM and add it to the current case.

Acquiring Live Memory for Analysis

When you select Memory Data to acquire you can choose to acquire live RAM data, do a Memory search on the data, or both.

When performing a Memory Search, you can search for items in memory, such as services and associated DLLs.

AccessData currently recommends that RAM acquisitions be done as a separate action from Volatile Data acquisitions. The Volatile acquisition pulls data through the API, where it is readily available, but may override the RAM acquisition settings, thus preventing the proper acquisition of data such as the System Descriptor Tables.

To acquire RAM Data

1. In Add Remote Data > Browse and Select Nodes pane, mark the Agent(s) to acquire RAM from.
2. In the Selection Information pane, click Include Memory Data if you want to acquire the RAM data and perform a memory search at the same time. If not, choose the option that suits your needs.
3. Make selections for Acquisition Options.
4. Make selections for Update Agent.
5. Make selections for Resource Usage.
6. Click OK.
7. Do one of the following:
   - Choose Memory Analysis to add the RAM data directly to the case you are working on.
   - Choose Memory dump to save the dump file to a destination folder and name of your choosing.
8. Click OK.
9. If you chose Memory Analysis, the Data Processing Status dialog opens to display the memory acquisition jobs you requested.
10. If you chose Memory dump, the Memory Dump dialog opens and you can continue to specify the options for the memory dump file.

10a. Specify a Memory Dump Location. This can be a destination local to your Examiner machine, or on the remote Agent machine, but must be a location where you have full access permissions.
10b. Choose a file type for the memory dump file. Options are RAW and AD1.

10c. Mark the box labeled Add memory analysis to case if you want to do so.

10d. Mark the box labeled Get memory page file to make the memory page file available to the case.

10e. Click OK to save settings and continue.

11. If you chose Memory Search, the Memory Search dialog opens to allow you to specify the following:

11a. In the Search Hit options, choose one of the following:
   ■ Return the process only
   ■ Return the process with associated DLLs

11b. In the DLL Hit options, choose one of the following:
   ■ Return the DLL only
   ■ Return the DLL with associated process

11c. In the Search Term type, choose one of the following:
   ■ Text
   ■ Pattern
   ■ Hex

11d. In the CodePages, choose any or all of the following:
   ■ ANSI
   ■ UTF 16 BE
   ■ Case insensitive
   ■ UTF 16 LE
   ■ UTF8

11e. Search terms, type one term at a time, and click Add.

12. When you are finished specifying the memory search options, click OK.

The processing requests are added, the memory is acquired, and the search is performed as three separate jobs in the Data Processing Status window.
Importing Memory Dumps
The Import Memory Dump feature allow you to import memory dump files from this or other case file in to the current case.

**Note:** Using Enterprise Examiner it is possible to compare a set of previously imported fuzzy hash values against a process list in a memory dump.

**To import a memory dump**
1. From the Enterprise Examiner, click **Evidence > Import Memory Dump**.
2. Select the Agent system from the drop down list. If the Agent is not listed, select the **<Add new Agent>** item from the list, and enter an Agent name or IP Address.
3. Click the **Browse** button to locate the memory dump file you want to add to your case and click **Open**.

**Note:** For OS system profiles that are not included in list of Volatility 2 profile drop-down list, mark the "Don't see your profile? Try Volatility 3." checkbox
4. Click **OK** to add the memory dump to your case.
5. The memory dump data appears in the Volatile tab in the Examiner window under the Agent name and acquisition date and time. Each acquisition is displayed separately under its data and time stamp, grouped by Agent, Acquisition Time, or Operation Type.

See also **Using the Volatile Tab** (page 539).
Acquiring Drive Data

When examining drive data, you can acquire data from the following types of drives:

- Physical Drives
- Logical Drives

You can also acquire information in the following ways:

- Previewing data only
- Acquiring complete disc image

A separate job is created for each selected data source associated with the machine, but does not include memory. These jobs can be monitored in View > Progress Window > Data Processing Status > Other Jobs.

To include drive data in an acquisition

1. In the Examiner, click Evidence > Add Remote Data.
2. Select the nodes you want to acquire from.
3. In the Selection Information pane, select Include Drive Data.
4. Select one or more from the following:
   - Physical Drive (Preview/Acquire)
   - Logical Drive (Preview/Acquire)
   - Filtered File System (Preview only)

   To use the Filtered File System option, see Collecting Filesystem Data (page 184)
5. Make selections for other job options.

See Browsing and Selecting Nodes on page 168.
6. Click OK.
7. In the Select Drives pane, expand the drive list for that Agent machine and select a drive to view that drive’s information in the Details pane.
8. Select the type of drive data to be examined on the Drive Data group box:
9. (Optional) **Preview Information Only**: Provides a list of the files in the drives, not the actual files themselves. After this information is processed, click Evidence > Additional Analysis and select MD5, SHA1, or KFF Lookup to Flag Duplicate Files.
**Note:** Choose Preview Information Only to open the data into Enterprise. You will see it in the Evidencetab. Click **File > Export to Image** to create an AD Encryption-encrypted image. For more information see **Exporting an Image to an Image** (page 294).

9a. Select **Include Slack** to detect fragments of files that have not been completely overwritten and/or **Recover Deleted Files** to recover deleted files that have not been overwritten.

9b. Check **Include Hidden Processes** in the **Acquisition Option** group box to include processes designed to remain invisible to the Task Manager.

10. (Optional) **Complete Disc Image:** Creates an actual image of the drives. This process can take a long time and can significantly impact the CPU usage of the Agent system.

10a. Specify the Disk Image Path information relative to **This (local) machine** or **Remote source machine**.

10b. Enter or browse to locate the **File Path** for the Disk Image destination.

10c. If you chose **Remote source machine**, enter the Username and Password where you have permissions to write the image.

10d. For security, you can add a password.

10e. Mark **Add image to case when complete** to add the data to the case as soon as the acquisition is complete.

10f. Click **Image Details** if any Evidence Item Information is required. This includes Case Number, Evidence Number, Unique Description, Examiner and Notes. Additionally, you can include a Fragment Size and Compression value. This option is only available for Physical and Logical collections.

11. Click **OK** to begin the Drive Data acquisition.

**Note:** If the Firefox directory is added as evidence while in use, the history, downloads, and other files are identified as zero-length files.
Mounting a Device
Mounting a device allows you to mount an Agent’s drive or device and view it in Windows Explorer as if it were attached to your drive.

To Mount a Remote Data Device
1. In the Add Remote Data dialog, under Selection Information, click Mount a device.
2. Select the drive(s) to mount, then click OK to open the Map remote drives dialog.
3. In the Select drive dialog, click the to select the drive letter to map the remote device to on your machine.

The device remains mounted until you unmount it or until you close Enterprise Examiner.

Unmounting a Device
There are two ways to unmount, or un-map a mounted Agent device. Choose one of the following methods to unmount a mounted Agent device.

To Unmount a Device, Method 1
1. Click Tools > Unmount Agent Drive.
2. In the Unmount Agent Drive dialog, do one of the following:
   - Select a drive to unmount
   - Select All Agents to unmount all drives on all Agents at the same time.
3. Click OK.

To Unmount a Device, Method 2
1. Click Evidence > Add Remote Data.
2. Add and select the Agent that owns the mounted drive that is to be unmounted.
3. Click Mount a device. No other options need to be selected.
4. Click OK.
5. In the Map remote drives list, any mounted devices will be bolded, and will display their mapped drive letter. Select the one that is to be unmounted.
6. Click Unmap drive.
7. Click Done, to close the dialog, or you can select a different drive to mount without starting over.
Specifying Additional Requirements and Initiating the Acquisition

To continue specifying requirements

1. Click OK to advance to the various screens that are required to supply the additional path, credential, or other information necessary to accomplish the acquisition based on the selection information you have chosen.

For example, if one of your choices were to acquire Registry Information, a dialog appears that prompts you to supply the Registry Key Path and Root Key, and mark whether to include any subkeys.

Note: When selecting to acquire Registry Info, you must also select at least one subkey after the root key from the drop-down, or you will not get any Registry results.

If you had also selected drive information, the next screen would prompt you to indicate whether to Preview Information Only, or to make a complete Disc Image, and whether to Include Slack and/or Recover Deleted Files.

2. When all of the requirements have been met and your selections are complete, click OK to begin the data acquisition.

The Data Processing Status screen opens and the Other Jobs group is open, showing progress on each of the tasks you have requested. This is illustrated in the following figure:

Close the Data Processing Status window at any time. Click View > Progress Window to check job processing status. When the status indicates that all data has been collected, close the window and click the Evidence tab to view acquired physical and logical drives or drive images. Click the Volatile tab in the Enterprise Examiner to view the Volatile information.
Collecting Filesystem Data

You can acquire different types of drive data. See Acquiring Drive Data on page 180. One option is to collect filesystem data. This option lets you preview common areas of interest to determine the severity of a breach, determine the scope of the incident and what was impacted in the system.

For example, you can do the following:

- Investigate suspected systems to determine the scope and root cause of an incident.
- Determine whether a machine has been compromised or has compromised others.
- Use predefined or personalized filters to create targeted data collections for up to 50 nodes. When collecting filesystem data, you use filters to select the data that you want to preview.

You can use the following filters:

- The pre-built filter (AD_Cyber_Forensics_Initial_Triage_Filter.xml) Using the AD Cyber Forensics Initial Triage Filter (page 186)
- Your own custom filters

Using Custom Filters (page 189)
In order to fully process the data before analysis, it is important to follow the complete workflow below.

To collect filesystem data

1. Before you can collect the filesystem data, you must be sure the agent has been installed. To review information on the agent, see About the AccessData Enterprise Agent (page 163).
2. In the Examiner, click Evidence > Add Remote Data.
3. Select the nodes you want to acquire from.
4. In the Selection Information pane, select Include Drive Data.
5. Select Filtered File System (Preview only)

Note: If you are selecting multiple nodes, be sure this option is checked for each node by selecting the Preferences button, selecting the Filtered File System option, checking Apply to Selected, and clicking OK.
6. Make selections for other job options.

See Browsing and Selecting Nodes on page 168.
7. Click OK. Enter your credentials when prompted.

8. In the Select Filesystems dialog, select the filesystem you want to acquire data from.

9. Configure a filter to use to acquire data by doing one of the following:

   - Using the AD Cyber Forensics Initial Triage Filter (page 186)
   - Using Custom Filters (page 189)

10. Once you have configured the filter, select whether or not to include deleted files.

11. (Optional) Once you have configured the filter, save the contents of the filter.

   **Note:** When you click OK, any text in the Filter dialog will be cleared. If you want to save the filter, click Save As and save to a file. If you make additional changes to a saved file, you can click Save.

   The Filters are also saved in the case folder as an external stream cache. They are stored under “case name\evidence_filters. The filters are saved as .dat files that can be opened in an editor. The name of the .dat file is the same as the “Evidence ID”.

12. To collect data, click OK.

   The Data Processing Status dialog displays the progress.

13. **Important:** After acquiring data, do the following:

   13a. Converting Live Preview Data to an AD1 (page 192)
   13b. Run Additional Analysis (page 193)

14. View the acquired and processed data.

   See Examples of Collecting and Viewing Data on page 193.
Using the AD Cyber Forensics Initial Triage Filter

About the AD Cyber Forensics Initial Triage Filter

To assist you in collecting filesystem data, you can use a targeted, pre-built filter (AD_Cyber_Forensics_Initial_Triage_Filter.xml).

Using the predefined filter settings, you can investigate the following items:

- System files
- Installed programs
- Registry information

This filter includes data collection for the following items.

**AD Cyber Forensics Initial Triage Filter Options**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logon Data</td>
<td>This filter shows users who have logged on to a Windows system.</td>
</tr>
<tr>
<td>Network Shares</td>
<td>This filter shows network share connections, including network paths typed into the Run command.</td>
</tr>
<tr>
<td>SSH Data</td>
<td>This filter shows whether a computer has been in communication with other computers, and which computers they have connected to.</td>
</tr>
<tr>
<td>Capturing Windows Registry Modification Logs</td>
<td>Note: This filter requires IT to enable security policies on the target node(s). Please see the Enabling Security Policies - IT Settings for AgentMachines document for more details.</td>
</tr>
<tr>
<td>Windows Firewall Log</td>
<td>This filter can show malicious activity that is not revealed by inspecting the registry directly, as a malicious user could restore an old value of an exploited registry key used to cover their tracks. Showing the changes to the registry as well as the registry prevents this scenario.</td>
</tr>
</tbody>
</table>

**Note:** This filter requires IT to enable security policies on the target node(s). Please see the Enabling Security Policies - IT Settings for AgentMachines document for more details.

This filter is for monitoring outgoing communications in the network traffic. It specifically shows what has been allowed through the firewall. This can show whether a compromised machine has been communicating with other machines.
### AD Cyber Forensics Initial Triage Filter Options (Continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Windows Group Policy Configurations** | This filter includes the group policy configurations that have been synchronized from the organizational policies (Active Directory) and local changes that have been made to group policies (regardless of whether or not these local changes have actually been applied).  
This filter has two purposes. It shows whether group policy files that are queued to sync to the registry are different from what is actually in the registry; which could indicate malicious modification in order to circumvent the group policy system. It also shows what has not synced to the group policy system yet, in case the failure to sync allowed a security breach.  
**Important:** None of the configuration values in this filter are guaranteed to be synchronized with the registry. |
| **Windows Group Policies (GPOs) in the Registry** | This filter is for the policy configuration that exists in the registry. This shows how the software will behave when interacting with all related policies. It includes a full list of the registry group policies that come with Windows out-of-the-box.  
**Important:** The AD Cyber Forensics Initial Triage Filter is a little generous with the GPO data it includes, so note that despite the path the data in it may not be officially associated with a policy. You’ll need to confirm before marking an item as a policy change.  
**Note:** This filter requires IT to enable security policies on the target node(s) Please see the Enabling Security Policies - IT Settings for AgentMachines document for more details. |
| **Windows Account Modifications** | This filter shows any changes made to local user accounts. It is used to determine if any local accounts have been created, particularly with administrative privileges. |
Accessing the AD Cyber Forensics Initial Triage Filter

**To access the AD Cyber Forensics Initial Triage Filter**
1. In the Select Filesystems dialog, click **Open**.
2. Browse to the filter file.

The AD_Cyber_Forensics_Initial_Triage_Filter.xml file can be found at the following path:

```
ProgramData > AccessData > Products > Forensic Toolkit > 6.x > AD_Cyber_Forensics_Initial_Triage_Filter.xml
```

**Note:** This filter is designed as an “all-in-one” filter. It is possible to run one portion of the AD Cyber Forensics Initial Triage Filter at a time in order to break the data into manageable chunks. Copy/paste the portion(s) you want to run into the Filter text box.

**Note:** When you click OK, any text in the Filter dialog will be cleared. If you want to save the filter, click Save As and save to a file. If you make additional changes to a saved file, you can click Save.

The Filters are also saved in the case folder as an external stream cache. They are stored under “case name”\evidence\filters. The filters are saved as .dat files that can be opened in an editor. The name of the .dat file is the same as the “Evidence ID”.

3. Once you have configured the filter, select whether or not to **Include deleted files**.
4. (Optional) Once you have configured the filter, save the contents of the filter.

**Note:** When you click OK, any text in the Filter dialog will be cleared. If you want to save the filter, click Save As and save to a file. If you make additional changes to a saved file, you can click Save.

The Filters are also saved in the case folder as an external stream cache. They are stored under “case name”\evidence\filters. The filters are saved as .dat files that can be opened in an editor. The name of the .dat file is the same as the “Evidence ID”.

5. To collect data, click **OK**.

The Data Processing Status dialog displays the progress.
6. **Important:** After acquiring data, do the following:

6a. Converting Live Preview Data to an AD1 (page 192)
6b. Run Additional Analysis (page 193)
7. View the acquired and processed data.
See Examples of Collecting and Viewing Data on page 193.
Using Custom Filters

You can create a custom filter. To create a custom filter, you use the Filter Builder. The filter builder tool allows you to create complex filters for use within the Select Filesystems collection dialog. There are three main tabs:

- **General Filters** (page 190)
- **Advanced Options** (page 192)
- **Xml Preview** (page 192)

After creating a custom filter you can save it and re-use it in a future job.

To use a custom filter

1. In the *Select Filesystems* dialog, do one of the following:
2. Enter a filter using one of the methods below:
   - To create your own custom filter, click the **Create Filter** button to launch the *Filter Builder* tool. See *Using the Filter Builder* on page 189.
   - To use a filter that you have previously created and saved, click **Open** and browse to an existing filter file.
   - Type or paste a filter into the *Filter* text box.
3. Once you have configured the filter, select whether or not to *Include deleted files*.
4. (Optional) Once you have configured the filter, save the contents of the filter.

**Note:** When you click OK, any text in the Filter dialog will be cleared. If you want to save the filter, click **Save As** and save to a file. If you make additional changes to a saved file, you can click **Save**.

The filters are also saved in the case folder as an external stream cache. They are stored under “case name”\evidence_filters. The filters are saved as .dat files that can be opened in an editor. The name of the .dat file is the same as the “Evidence ID”.

5. To collect data, click **OK**.

   The *Data Processing Status* dialog displays the progress.

6. **Important:** After acquiring data, do the following:

6a. **Converting Live Preview Data to an AD1** (page 192)
6b. **Run Additional Analysis** (page 193)
7. View the acquired and processed data.

See **Examples of Collecting and Viewing Data** on page 193.
Using the Filter Builder

**To build a custom filter**

1. In the Filtered File System (Preview Only), click Create Filter. The *Filter Builder* dialog opens.

2. Configure the filter using the following tabs.
   - General Filters (page 190)
   - Advanced Options (page 192)
   - Xml Preview (page 192)

3. Verify the contents of the filter using the *Xml Preview* tab.

4. To close the Filter Builder and copy the data, click **OK**.

General Filters

In this tab you have the option to use both *Include and Exclude Filters*. Click **Add** in either section to open the File Filter dialog. Here you can filter for attributes using the following tabs:

- Common File Attributes (page 190)
- Common Email Attributes (page 190)
- All Attributes (page 190)
- File Content (page 191)
- Hashes (page 191)

You can also **Edit** or **Delete** any of the listed attributes, in either the *Include or Exclude Filters*. 
Common File Attributes

This tab allows you to select the following attributes:
- Creation Date/Time
- Modified Date/Time
- Last Accessed Date/Time
- File Size
- File Extensions
- File Paths

Note: If using a Regular Expression operator, the path you enter must fully match. To use as a subset of a path, place .* before and after to make it function as a wildcard.

Common Email Attributes

This tab allows you to select the following attributes:
- Email Submit Date/Time
- Email Delivery Date/Time
- Email Subject
- Email From
- Email To
- Email CC
- Email BCC
All Attributes

This tab allows you to search through a full list of individual attributes and customize each one individually. Select Add to view the full list or select the Favorites option, which shows the most commonly-used attributes.

For each attribute you may select the following:

- Operator

The Operator options that you have are dependant on the type of attribute you selected. For example, for some attributes you can select Exists or Equals, for others you may also have Less Than, Greater Than, or Between.

- Value
- Second Value (For example, a second date when using a Between operator)
- Ignore Case
- Match if Attribute Missing

You can also Edit or Delete items in the All Attributes tab.

---

**Note:** If using a Regular Expression operator, it does a regex_search and not a regex_match. As a result, only a subset has to match, not the entire attribute. It is treated as if there is a * (wildcard) at both ends. To require the entire attribute to match, surround it with ^ and $.
**File Content**

This tab allows you to search file content using the following options:
- **Search Type**

This dropdown includes the following options:
- All
- Any
- Regular Expression
- Nested - This lets you build a tree-type control with children using And and Or operators.

**Note:** Whenever you add a child, you must click Apply Changes for that node.

- Nested Regular Expression
- Keyword Threshold

Set this to the minimum number of hits required per document
- Keywords
- Luhn Options

This allows you to apply the Luhn Filter and to select the following options:
- Default Credit Card Numbers
- Custom Regular Expression
- Luhn Threshold

**Note:** File Content searches use the ECMA script.

**Hashes**

This tab allows you to enter a hash number(s) to search for, using equals or does not equal as the operator. To add a hash, type the data into the highlighted line. To delete, highlight a line and press the delete key on your keyboard.
Advanced Options
This tab allows you to apply the following options:
- Collect Encrypted Files
- Collect No Extension Files
- Smart File Identification
- Volume Slack
- Unused Disk Area
- System Files
- Include Deleted Files in Archives
- Enable I30 Parsing
- Auto Drill Down

When selected, you can enter in all desired drill down options. This also enables the Collect Archive Content Only option. Check if desired.

Xml Preview
This tab shows a preview of the filter xml for all the selections you have made using the Filter Builder. You can copy/paste this into the Filter box in order to save or edit for use in later cases by clicking OK.

**Note:** You can save a filter created using the Filter Builder tool. Once you click OK the xml will populate in the Filter text box in the Select Filesystems window. Be sure to select Save As and follow the prompts before you click OK and start the collection.
Converting Live Preview Data to an AD1

It is important to convert the preview data to an AD1 or static file as quickly as possible. Live data is constantly changing and you may lose access to information as the target computer continues to run, or even turns off.

To convert the live preview data into an AD1:

1. Once the live data has populated in the Explore tab, use quickpicks to select the top item in the file tree and select File > Export to Image.
2. In the Create Custom Content dialog, select All Listed Items. Click OK.
3. In the Create Image dialog, select an image destination by clicking Add.
4. In the Select Image Destination dialog, enter the desired Image Destination Folder and Image Filename. Click OK.

It is possible to enter additional information in this dialog, but not required.

5. In the Create Image dialog, select any desired options and click Start.

Important: Do not select the Add image to case when completed option. You will need to open a new case in order to avoid duplicate data. If you are required to keep the evidence in the same case, remove the Live Preview data by going to Evidence > Add/Remove and removing the original evidence file before adding the newly-created AD1.
Run Additional Analysis
In order for the collected data to be parsed into the correct files and categories, it is necessary to run Additional Analysis on the AD1 file you have just created.

To add the new AD1 file and run an additional analysis job:
1. Open a new case or remove the live preview data in the existing case to avoid duplicate data.

To remove the live preview data navigate to Evidence > Add/Remove and removing the original evidence file before adding the newly-created AD1.
2. In the case, navigate to Evidence > Add/Remove. Click the Add button. Select Acquired Image(s) and click OK.
3. Navigate to the folder where you saved the AD1 file. Select the file and click Open.
4. Click the Refinement Options button.
5. Select the Expand Compound Files option and click the Expansion Options button. In the Compound File Expansion Options window, select the following:
   - McAfee Log
   - OpenSSH known_hosts File
   - Windows Firewall Log
   - Windows Registry.pol
   - Any additional options that may apply
6. Click OK to add the evidence and open the case.

Examples of Collecting and Viewing Data
The following steps outline how to collect and view examples of the data that you may collect.

Viewing Preview Data Acquired using the AD_Cyber_Forensics_Initial_Triage_Filter.xml
After processing the remote data, you can see it in the Examiner. Drive data will appear as a new node on the Evidence tab.
Viewing Net Logon Data

Using the pre-built filter, you can collect Windows Net Logon data. By default, the Logon data that is captured are events when users log in to Windows. These Logon events are stored in the registry as event type 4624. What is not captured are when service accounts start and stop which Windows records as a Logon type 5.

You can view the Logon events.

To view Net Logon data
1. In the Examiner, do one of the following:
   • Using the Explorer tab:
     1a. Click Evidence.
     1b. Expand the target you acquired data from.
   • Using the Overview tab:
2. The File List displays the list of Logon events.
3. You can click an event in the File List and view the properties in the File Content > Properties pane.
4. You can also right-click the File List > column headers > All Features and add the EVTX columns to the File List to display detailed data in the columns rather than having to look at each one individually.
Viewing Registry Data

Using the pre-built filter, you can collect and view Windows Registry data. The NTUSER.DAT is stored as a folder that you can browse.

To view Registry data
1. Click Evidence.
2. Expand the target you acquired data from.
3. Expand **Root > Users**.
4. Expand a user.
5. Expand NTUSER.DAT.
6. Expand and view data.

Specific details are listed below.

Viewing Network Shares

Using the pre-built filter, you can collect a user’s network shares information that is in the registry. By default the shares data is stored in two different locations.

To view network shares data
1. Click Evidence.
2. Expand the target you acquired data from.
3. Expand **Root > Users**.
4. Expand a user.
6. Click MountPoints2.

The items displayed in the File List beginning with ## are shares the user had connected to. The # represents a \.
7. Click RunMRU.

The items displayed in the File List are the text that the user has entered in the Windows Run dialog, such as a path. They are stored in items labeled as letters. You can click a letter and view the content in the File Content pane.
Viewing SSH Known Hosts

Using the pre-built filter, you can collect a user’s ssh host information that is stored in cygwin, Windows 10 Windows client, or Linux computer. To view cygwin .ssh hosts data
1. Click Evidence.
2. Expand the target you acquired data from.
3. Expand cygwin64 > home > user > .ssh.
4. In the File List, click known_hosts.
5. In the File Content pane, you can see the list of host names that the computer has connected to.
6. To view additional information, you can run Additional Analysis, select to Expand Compound Files, and in the Expansion Options, select the option to OpenSSH known_hosts file.

This will open information for each host and the File List will shown an item for each host connection.

When viewing the properties of each host, you can view the Destination IP Address and DestinationHostname

7. To view SECSH host keys data in the registry
   7a. Click Evidence.
   7b. Expand the target you acquired data from.
   7c. Expand Root > Users.
   7d. Expand a user.
   7e. Expand Documents > NetSarang > SECSH > Hostkeys. In the properties, you can view the Destination Hostname.

8. To view MobaXterm host keys data in the registry
   8a. Click Evidence.
   8b. Expand the target you acquired data from.
   8c. Expand Root > Users.
   8d. Expand a user.
   8e. Expand Documents > MobaXterm > slash > tmp > sessions. In the properties, you can view the Destination Hostname.
9. To view PuTTY and KiTTY host keys data in the registry

9a. Click Evidence.
9b. Expand the target you acquired data from.
9c. Expand Root > Users.
9d. Expand a user.
9e. Expand NTUSER.DAT > Software.
9f. Expand 9bis.com > PuTTY > SshHostKeys.
9g. Expand SimonTatham > KiTTY > SshHostKeys.

Acquiring Remote Data from macOS Managed Agents

Data acquisitions from macOS agent nodes are very different from all other supported Enterprise agent acquisitions and therefore are done via the Mac Agent Collection interface which is specially designed for macOS collections.

To assist you in familiarizing yourself with the unique macOS data acquisition options available, some example acquisition workflows are provided below and are designed to give you a general idea of what is possible for your own macOS investigations.

Generally speaking, a macOS acquisition follows this procedure:

1. Add node(s) to Agent List
2. Connect to agent and select data to acquire
3. Review and acquire select files and folder
4. Monitor job progress
**Configuring Mac Agent Collection Interface**

Mac Agent Collections will use the selected case and its storage location to store the data collected from macOS systems during a collection.

**Mac Agent Collection Configuration**

<table>
<thead>
<tr>
<th>Element</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process Image to Case when complete</td>
<td>Mark this option to have the evidence image automatically attached to the corresponding case and processed with default processing settings.</td>
</tr>
<tr>
<td>NOTE: You may have to close the case examiner in order for the macOS data that was ingested automatically to be displayed.</td>
<td></td>
</tr>
<tr>
<td>Cancel All Agent Jobs</td>
<td>This button will terminate all active jobs.</td>
</tr>
</tbody>
</table>

![Settings](image)
To configure Mac Agent Collection interface

1. From the case examiner interface, navigate to Evidence >> Add Remote Mac Data
2. The Mac Agent Collection interface appears
3. Select an available macOS agent endpoint and click Connect to Agent
4. Click the configure button.
5. Define the settings as desired. See Mac Agent Collection Configuration (page 196) for reference.
6. Click OK to save your changes.

Building macOS Agent List

Prior to running any data acquisition jobs against macOS agent nodes, the nodes must first be added to the Enterprise global Agent List and marked with the is Mac flag. See Adding Nodes to the Agent List on page 169.

About Mac Agent Collection Search and Culling Options

The following table defines the supported range and syntax of the available macOS agent data culling options.

Mac Agent Collection Search and Culling Options

<table>
<thead>
<tr>
<th>Field</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search Files</td>
<td>The Search Files field runs a quick search against the macOS system index and accepts text strings connected by boolean operators AND and OR.</td>
</tr>
<tr>
<td>Advanced Search Options</td>
<td>When marked, the Index Search option will run the search terms against the macOS system index. When unmarked, the agent will perform a live search of the file system.</td>
</tr>
<tr>
<td>Keywords</td>
<td>The keywords field accepts text strings connected by boolean operators AND and OR.</td>
</tr>
</tbody>
</table>
### Mac Agent Collection Search and Culling Options

<table>
<thead>
<tr>
<th>Field</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ex: .txt,.pdf,.docx,.xlsx,.pptx</td>
<td>The file extension field accepts text string values and uses an asterisk (*) as a wildcard character anywhere in the string.</td>
</tr>
<tr>
<td>Date</td>
<td>The date field defines whether the range being search represents the Date Created or the Date Modified metadata timestamps from the file system.</td>
</tr>
<tr>
<td>From: To:</td>
<td>From: To: fields use the calendar pop-out to define the date range of the date field in MM/DD/YYYY format.</td>
</tr>
<tr>
<td>🗄️</td>
<td>In the file system tree, all subfolders are automatically checked whenever you select a parent directory. Each box checked will result in a separate entry on the Review screen when added.</td>
</tr>
<tr>
<td>Uncheck All</td>
<td>Removes marks from all selected check boxes in the tree view pane.</td>
</tr>
<tr>
<td><img src="image" alt="Uncheck All" /></td>
<td>Column filter appears blue when applied.</td>
</tr>
</tbody>
</table>
Standard User Data Collection Workflow

This example targets a standard list of user generated data files by list of common file extensions. For detailed information on supported syntax, see About Mac Agent Collection Search and Culling Options (page 197).

How to collect a standard set of user data files by file extension

1. In the Mac Agent Collection interface, select the target macOS node populated from the Agent List drop-down list and click Connect to Agent.

2. Select Live Preview

3. Open the Advanced Search dialog

4. Choose one or more of the following culling options (populating more than one field will AND the criteria):
   4a. Keywords (searches dtSearch index) See Searching Evidence with Index Search (page 521)
   4b. Live search
   4c. File Extensions
   4d. Date Range

5. Click Search

6. When the results have loaded, mark the Select All checkbox at the top-left of the file grid.

7. Click Add Checked Files

8. Click Review

9. Refer to Acquiring Checked Files From Mac Agent Collection Review (page 199) to complete the data acquisition.
macOS Agent Logical Disk Acquisition Workflow

This workflow simply acquires all files from one or more of the logical partition “slices” selected for the acquisition.

How to collect a standard set of user data files by file extension

1. In the Mac Agent Collection interface, select the target macOS node populated from the Agent List drop-down list and click Connect to Agent.

2. Select Acquire Logical Drive

3. A list of all attached internal and external drives is displayed

4. Mark the checkboxes for one or more slices you wish to acquire.

5. Click Acquire Selected

6. Check the progress of all acquisition jobs via the Jobs Monitor. See Managing Jobs in the Mac Agent Collection Jobs Monitor on page 200.

Acquiring Checked Files From Mac Agent Collection Review

On the Review screen, you can review and refine which files / folders you want included in the evidence image acquired from the macOS system.

How to acquire checked files from mac agent collection review

1. Use the file grid column filters and checkboxes to select which items should be included in the acquisition.

2. A preview panel is available to review the contents of selected files.

3. When your list is finalized, click Acquire Files/Folder

4. Check the progress of all acquisition jobs via the Jobs Monitor. See Managing Jobs in the Mac Agent Collection Jobs Monitor on page 200.
**Managing Jobs in the Mac Agent Collection Jobs Monitor**

The Mac Agent Collection Job Monitor tracks the active acquisition jobs status, start time, and other statistics about the current job. Records for job history can also be displayed.

### Elements of the Jobs Monitor

<table>
<thead>
<tr>
<th>Element</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Show Only Active Jobs</td>
<td>When enabled, it filters the list to only show active jobs. Unmark this box to display job acquisition record history.</td>
</tr>
<tr>
<td>Poll Job Status</td>
<td>When marked, the Job Monitor interface will automatically refresh the latest information about the job status records displayed.</td>
</tr>
<tr>
<td>Refresh</td>
<td>Manually refreshes the latest information about the job status records displayed.</td>
</tr>
<tr>
<td>Job ID</td>
<td>Unique numerical value assigned to each job. Sort by this column to see latest to oldest jobs submitted.</td>
</tr>
<tr>
<td>Machine</td>
<td>Hostname of the system that initiated the job.</td>
</tr>
<tr>
<td>Type</td>
<td>Lists the type of job such as “ManagedAgentJob” or “FTK PlusCloudProcessorJob”</td>
</tr>
<tr>
<td>Status</td>
<td>Tracks the current status of the job such as Active, Completed, or Failed</td>
</tr>
<tr>
<td>Processed</td>
<td>Records the number of items successfully acquired by the agent or processed by the engine.</td>
</tr>
<tr>
<td>Error</td>
<td>Total number of errors reported.</td>
</tr>
<tr>
<td>Total</td>
<td>Sum of objects reported as “Processed” or “Error”</td>
</tr>
<tr>
<td>User</td>
<td>Application username of the user who initiated the job.</td>
</tr>
<tr>
<td>Start</td>
<td>Timestamp of when the job was submitted (Displayed in GMT timezone).</td>
</tr>
<tr>
<td>End</td>
<td>Timestamp of when the job was marked as completed (Displayed in GMT timezone).</td>
</tr>
</tbody>
</table>

Column filter appears blue when applied. Columns can be filtered based on exact strings, contains, starts with, etc.

- [ ] Select All
- [ ] [null]
- [ ] WIN2016

Show rows with value that

- Is equal to
- And
- Is equal to

Filter  Clear Filter

- Pause | Resume | Kill  Jobs in a highlighted row can be paused, resumed, or terminated one at a time.                                                                                                              |
- Close   Close the Job Monitor interface and returns to Mac Agent Collection.                                                                                                                          |
Site Server Data Collections

AccessData Enterprise integrates with the AccessData Site Server for the purpose of local and remote network collections as well as off-network device acquisition. The AccessData Site Server is has the ability to collect custodians’ data from “On-prem” and cloud-based structured data repositories such as Gmail, OneDrive, MS Exchange, Sharepoint, etc as well as acquire data from users' network shares and workstations. The AccessData Enterprise Agent can be configured to “phone home” over the public Internet to an instance of a Site Server on a public IP address to facilitate off-network data acquisition where it does not matter to what network the workstation endpoint is connected. This functionality serves to acquire data from the growing number of workstations of employees working-from-home.

**Note:** Structured Data Connector integration features are licensed separately in addition to the AD Enterprises license.

**About Structured Data Repository Collections**

The user interface within which you configure the structured data connectors is a web page hosted by the Forensic Tools Suite of applications.

**To Configure Structured Data Repository Collections**

1. Launch AD Enterprise and login
2. Open a case to the Examiner interface.
3. Navigate to Evidence >> Add Off-Network/Cloud Data

(Web page opens)

4. In the web browser, navigate to Home >> Data Sources
5. Configure any of the connectors listed below as appropriate:

About Data Custodians

The user interface within which you manage the data custodians’ records is a web page hosted by the Forensic Tools Suite of applications.

To Configure Data Custodian Records

1. Launch AD Enterprise and login
2. Open a case to the Examiner interface.
3. Navigate to Evidence >> Add Off-Network/Cloud Data (Web page opens)
4. In the web browser, navigate to Home >> Data Sources >> Manage Custodian tab.
5. For more information on this topic, See Custodians on page 204.

About Off-Network Data Acquisitions

In order to acquire data from an “off-network” agent workstation connected to the public Internet, the agent must be installed with a specific configuration. The agent installation command must define the IP address of the Public Site Server to which the agent should check-in with on a regular time interval.

The command used to install the agent should therefore include the following command line options:

<table>
<thead>
<tr>
<th>Command Line Options</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>PUBSS</td>
<td>Public IP address of the Public Site Server service.</td>
</tr>
<tr>
<td>PORT</td>
<td>Network port of the Site Server Service.</td>
</tr>
</tbody>
</table>

For more information on manually installing the AccessData Enterprise Agent, see Manually Installing the Agent(page 675) and more specifically the Command Line Options (page 675)

About Managing Target Computer Records

Similar to the Agent List in the desktop interface, the details of the agent workstations can be managed via a webuser interface hosted by the Forensic Tools Suite of applications.
To Manage Target Computer Records
1. Launch AD Enterprise and login
2. Open a case to the Examiner interface.
3. Navigate to Evidence >> Add Off-Network/Cloud Data (Web page opens)
4. In the web browser, navigate to Home >> Data Sources >> Computers
5. For more information on this topic, See Managing Computers on page 208.

Integrating Enterprise with a Site Server
Prior to executing collection / acquisition jobs against the Site Server, the Enterprise interface must first be configured to talk to AccessData Site Server.

Note: For detail on installing and configuring the AccessData Site Server component, please reference the ADEnterprise Install documentation.

To Connect AD Enterprise to Site Server
1. Login to AD Enterprise.
2. In the Case Management interface, navigate to Tools >> Preferences >> Configure AccessData Servers
3. Configure the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site Server Host</td>
<td>The IP Address of the server hosting the Site Server service.</td>
</tr>
<tr>
<td>Site Server Port</td>
<td>The network port of the Site Server service.</td>
</tr>
</tbody>
</table>

4. Click Save.
5. On the preferences dialog, click OK.

To Configure Site Server Settings
1. See https://support.accessdata.com/hc/en-us/articles/115001615088
Data Sources

Data Sources are the sources of data relevant to a case during electronic discovery or security investigation. The data can include electronically stored information on employees, system management computers, and can refer to people, Network shares, Domino or Exchange email accounts, or other public repositories associated with the person. The Data Sources module allows you to add, define, delete and edit data sources. Once data sources have been configured, data can be collected remotely and then processed.
Managing Data Sources

FTK Central supports data management and collection from 11 different data sources and the details to manage the data sources are provided in the upcoming sections.

*Elements of Managing Data Sources*

| Network Share | • Adding Network Share data sources  
| • Importing Network Shares data sources from CSV  
| • Mapping Network Share to custodians  
| • Editing Network Share data sources  
| • Deleting Network Share data sources |

| Computer | • Adding Computer data sources  
| • Importing Computer data sources from CSV  
| • Mapping Computer to custodians  
| • Editing Computer data sources  
| • Deleting Computer data sources  
| • Creating Endpoint Reports |

| Gmail | • Adding Gmail data sources  
| • Mapping Gmail data sources to custodians  
| • Editing Gmail data sources  
| • Deleting Gmail sources |

| Google Drive | • Adding Google Drive sources  
| • Mapping Google Drive data sources to custodians  
| • Editing Google Drive data sources  
| • Deleting Google Drive sources |

| OneDrive | • Adding OneDrive sources  
| • Mapping OneDrive data sources to Custodians  
| • Editing OneDrive data sources  
| • Deleting OneDrive sources |

| Microsoft Teams | • Adding Microsoft Teams sources |
| Slack | • Adding Slack data sources  
• Editing Slack data sources  
• Deleting Slack data sources |
|---|---|
| SharePoint | • Adding SharePoint data sources  
• Editing SharePoint data sources  
• Deleting SharePoint data sources |
| Exchange | • Adding Online/Office 365 data sources  
• Adding Exchange data sources  
• Mapping Exchange data sources to custodians  
• Editing Exchange data sources  
• Deleting Exchange data sources |
| Box | • Adding Box data sources  
• Editing Box data source  
• Deleting Box data source |

**Tip:** To filter the grid efficiently, you can simply enter a keyword into the search box located at the top of any grid and click the search button or press enter.
Network Share
Shares are network folders on which the person may possess read and write access permissions. You can add or remove shares from this page, edit a share path, or add and edit a share’s locality and description.

Adding Network Share data sources

To add a Network Share data source:

1. From the home page, click Data Sources.
2. Navigate to Network Share.

3. Click Add Network Share.
   - The Add Network Share Details pop-up is displayed.

4. Enter the Path of a network share.
5. Provide a Description.
6. Choose No Credentials if you don’t want any authentication to access it or New Credentials to set a username and password for it.

Note: The below steps are to be performed for configuring new credentials.
i. Provide a **Domain/Username** for the network share.

ii. Provide a **Password**.

iii. Repeat the same password in **Confirm Password** field.

7. **Click Save.**
Importing Network Share from CSV

*To add a Network Share data source from CSV:*

1. From the home page, click **Data Sources**.
2. Navigate to **Network Share**.
3. Click **Import Network Share(s) from CSV**.
   - The **Import Network Share(s) from CSV** pop-up is displayed.

   ![Import Network Share(s) from CSV](image)

4. Click **Select files**.
5. Select the required file or drag and drop the file to be uploaded.
6. Click **Import**.

**Note:** You can click on **Download Template** fill in the details of the network share and upload it for the application to read the network shares to be imported.
Mapping Network Shares data sources to Custodians

To map a Network Share data source to custodians:

1. From the home page, click Data Sources.
2. Navigate to Network Share.
3. Click Map Custodian against the data source to be mapped.
   - The Map Custodians pop-up is displayed.

4. Select the required custodians by enabling the checkbox against it.
5. Click Save.
Editing Network Share data sources

To edit a Network Share data source:

1. From the home page, click **Data Sources**.
2. Navigate to **Network Share**.
3. Click **Edit** against the data source to be edited. ▪ The **Edit Network Share Details** pop-up is displayed.

4. Make the necessary changes.
5. Click **Save**.
Deleting Network Share data sources

To delete a Network Share data source:

1. From the home page, click Data Sources.
2. Navigate to Network Share.
3. Click Delete against the data source to be deleted.
   - The Please confirm pop-up is displayed.
4. Click Yes.

Note: You can also perform bulk deletion of the data source by enabling the checkbox against it and clicking on Delete.
Computer

One of the primary sources of evidence used in a case originates on workstations (or nodes) managed by a person. You can add or remove computers from this page, edit a share path, or add and edit a computer’s information and description.

Adding Computer data sources

*To add a computer data source:*

1. From the home page, click *Data Sources*.
2. Navigate to *Computer*.
3. Click *Add Computer*.
   - The *Add Computer* pop-up is displayed.
4. Provide a name for the computer in *Computer Name* field.
5. Provide a description for the computer in *Description* field.
6. Click *Save*. 
Importing Computer data sources from CSV

To import computer data sources from CSV:

1. From the home page, click **Data Sources**.
2. Navigate to **Computer**.
3. Click **Import Computer(s) from CSV**.
   - The **Import Computer(s) from CSV** pop-up is displayed.
4. Click **Select files**.
5. Select the required file or drag and drop the file to be uploaded.
6. Enable the checkbox against **Associate to Groups** to associate groups to computers.
7. Enable the checkbox against **Merge new groups to existing computers** to associate new groups to computers that were previously added by CSV import.
8. Click **Import**.

**Note:** You can click on **Download Template** fill in the details of the network share and upload it for the application to read the network shares to be imported.
Mapping Computer data sources to Custodians

To map a computer data source to custodians:

1. From the home page, click **Data Sources**.
2. Navigate to **Computer**.
3. Click **Map Custodian** against the data source to be mapped.
   - The **Map Custodians** pop-up is displayed.

4. Select the required custodians by enabling the checkbox against it.
5. Click **Save**.
Editing Computer data sources

To edit a computer data source:

1. From the home page, click Data Sources.
2. Navigate to Computer.
3. Click Edit against the data source to be edited.
   - The Edit Computer pop-up is displayed.

4. Make the necessary changes.
5. Click Save.
Deleting Computer data sources

To delete a computer data source:

1. From the home page, click Data Sources.
2. Navigate to Computer.
3. Click Delete against the data source to be deleted.
   - The Please confirm pop-up is displayed.

```
Please confirm

Are you sure to delete this computer?

No     Yes
```

4. Click Yes.

Note: You can also perform bulk deletion of the data source by enabling the checkbox against it and clicking on Delete.
Creating Endpoint Reports

To create an endpoint report from data sources:

1. From the homepage, click **Data Sources**.
2. Click Computer.
3. Click Export.
4. Select any of the following report types:
   - HTML
   - CSV
   - PDF

The report will be created, listing the computers and their associated columns.

**Tip:** To create a report of specific endpoints, ensure computers have been filtered using the columns available. If this is not followed, a report will feature all computers listed in Data Sources.
Gmail
You can configure the application to collect data from Gmail at a domain (administrative) level. Administrators can collect from individual accounts without needing individual credentials. The service account must be used for collections.

Tip: If you have updated your FTK Central environment with an existing Data Source, ensure they are removed and reconfigured.

Adding Gmail data sources

To add a Gmail data source:

1. From the home page, click Data Sources.
2. Navigate to Gmail.
3. Click Add Gmail.

- The Add Gmail Details pop-up is displayed.

4. Provide a Name for the Gmail.
5. Enter the Domain Name.
6. Enter the Service account API key.
7. Select the Associated to all custodians to associate all the custodians to the server.
8. Click Save.
Mapping Gmail data sources to Custodians

*To map a Gmail data source to custodians:*

1. From the home page, click **Data Sources**.
2. Navigate to **Gmail**.
3. Click **Map Custodian** against the data source to be mapped.
   - The **Map Custodians** pop-up is displayed.

4. Select the required custodians by enabling the checkbox against it.
5. Click **Save**.
Editing Gmail data sources

To edit a Gmail data source:

1. From the home page, click Data Sources.
2. Navigate to Gmail.
3. Click Edit against the data source to be edited.
   ▪ The Edit Gmail Details pop-up is displayed.
   ▪ Make the necessary changes.
   ▪ Click Save.
Deleting Gmail data sources

To delete a Gmail data source:
1. From the home page, click Data Sources.
2. Navigate to Gmail.
3. Click Delete against the data source to be deleted.
   ▪ The Please confirm pop-up is displayed.
4. Click Yes.

Note: You can also perform bulk deletion of the data source by enabling the checkbox against it and clicking on Delete.

Google Drive

You can configure the application to collect files from a Google Drive. Once you have configured the application to collect from your Google Drive, you can choose to collect from this source with a collection job. The service account must be used for collections.

Tip: If you have updated your FTK Central environment with an existing Data Source, ensure they are removed and reconfigured.

Notes:
- When the user runs a Report only collection for Google Drive, native Google files (Docs, Spreadsheets, Slides, and Forms) do not count against a user’s storage quota and show as zero bytes.
- Google does not expose the size of the native files from Google Drive and hence only the file size is downloaded when file is downloaded (File Scan Collection/Non report only scenario).
Adding Google Drive data sources

To add a Google Drive data source:
1. From the home page, click **Data Sources**.
2. Navigate to **Google Drive**.
3. Click **Add Google Drive**.
   - The **Add Google Drive Details** pop-up is displayed.
4. Provide a **Name** for the Google Drive.
5. Enter the **Service account API key**.
6. Select the **Associated to all custodians** to associate all the custodians to the server.
7. Click **Save**.
Mapping Google Drive data sources to Custodians

To map a Google Drive data source to custodians:

1. From the home page, click Data Sources.
2. Navigate to Google Drive.
3. Click Map Custodian against the data source to be mapped.

The Map Custodians pop-up is displayed.

4. Select the required custodians by enabling the checkbox against it.
5. Click Save.
Editing Google Drive data sources

To edit a Google Drive data source:

1. From the home page, click Data Sources.
2. Navigate to Google Drive.
3. Click Edit against the data source to be edited.
   - The Edit Google Drive Details pop-up is displayed.

   - Make the necessary changes.
4. Click Save.
Deleting Google Drive data sources

To delete a Google Drive data source:

1. From the home page, click Data Sources.
2. Navigate to Google Drive.
3. Click Delete against the data source to be deleted.
   - The Please confirm pop-up is displayed.
4. Click Yes.

Note: You can also perform bulk deletion of the data source by enabling the checkbox against it and clicking on Delete.
OneDrive
You can configure the application to collect all files from a OneDrive. Once you have configured the application to collect from your OneDrive, you can choose to collect from this source with a collection job. If attempting to collect from GCC environments please refer to the Office 365 Credentials section.

Tip: If you have updated your FTK Central environment with an existing Data Source, ensure they are removed and reconfigured.

Adding OneDrive data sources

To add a OneDrive data source:

1. From the home page, click Data Sources.
2. Navigate to OneDrive.
3. Click Add OneDrive.
- The **Add OneDrive Details** pop-up is displayed.

4. Enter a OneDrive Name.
5. Choose the API Method.
   a) Graph API:
      i. Enter the **Tenant Active Directory Name**.
      ii. Enter the **Application (client ID)**.
      iii. Enter the **Secret Value**.
   b) Export API:
      i. Choose the **User Credentials**.
         - No Credentials – This will fetch the credentials configured in the System Management > Manage Credentials page.
         - New Credentials – Select this to configure users with new credentials.
6. Click **Save**.
Mapping OneDrive data sources to Custodians

To map a OneDrive data source to custodians:

1. From the home page, click Data Sources.
2. Navigate to OneDrive.
3. Click Map Custodian against the data source to be mapped.
   - The Map Custodians pop-up is displayed.

4. Select the required custodians by enabling the checkbox against it.
5. Click Save.
Editing OneDrive data sources

To edit a OneDrive data source:

1. From the home page, click Data Sources.
2. Navigate to OneDrive.
3. Click Edit against the data source to be edited.
   ▪ The Edit OneDrive Details pop-up is displayed.
4. Make the necessary changes.
5. Click Save.
Deleting OneDrive data sources

To delete a OneDrive data source:

1. From the home page, click Data Sources.
2. Navigate to OneDrive.
3. Click Delete against the data source to be deleted.
   ▪ The Please confirm pop-up is displayed.
4. Click Yes.

Note: You can also perform bulk deletion of the data source by enabling the checkbox against it and clicking on Delete.
Microsoft Teams

You can configure the application to collect files Microsoft Teams business user accounts. You can add, edit, or delete multiple accounts from this page. If attempting to collect from GCC environments please refer to the Office 365 Credentials section.

Adding Microsoft Teams data sources

To add a Microsoft Teams data source:

1. From the home page, click Data Sources.
2. Navigate to Microsoft Teams.
3. Click Add Microsoft Teams.

   - The Add Microsoft Teams Details pop-up is displayed.

4. Enter a Microsoft Teams Name.
5. Select the API Method.
   a) Graph API:
      i. Enter the Application (client ID) of the Microsoft Teams.
      ii. Enter the Secret Value of the Microsoft Teams.
iii. Enter the **Redirect URL** of the Microsoft Teams.

b) Export API:
   i. Choose the **User Credentials**.
      - No Credentials – This will fetch the credentials configured in the System Management > Manage Credentials page.
      - New Credentials – Select this to configure users with new credentials.

6. Click **Save**.
Editing Microsoft Teams data sources

To edit a Microsoft Teams data source:

1. From the home page, click **Data Sources**.
2. Navigate to **Microsoft Teams**.
3. Click **Edit** against the data source to be edited.
   - The **Edit Microsoft Teams Details** pop-up is displayed.
   - Make the necessary changes.
   - Click **Save**.

4. Make the necessary changes.
5. Click **Save**.
Deleting Microsoft Teams data sources

To delete a Microsoft Teams data source:

1. From the home page, click Data Sources.
2. Navigate to Microsoft Teams.
3. Click Delete against the data source to be deleted.
   - The Please confirm pop-up is displayed.
4. Click Yes.

Note: You can also perform bulk deletion of the data source by enabling the checkbox against it and clicking on Delete.
Slack
You can configure the application to collect files from Slack business user accounts. You can add, edit, or delete multiple accounts from this page.

Adding Slack data sources

*To add a Slack data source:*

1. From the home page, click **Data Sources**.
2. Navigate to **Slack**.
3. Click **Add Slack**.
   - The **Add Slack Details** pop-up is displayed.
4. Enter a Slack Name.
5. Enter the **Client ID** of the Slack.
6. Enter the **Client Secret** of the Slack.
7. Enter the **Redirect Url** of the Slack.
8. Click **Save**.
Editing Slack data sources

To edit a Slack data source:

1. From the home page, click Data Sources.
2. Navigate to Slack.
3. Click Edit against the data source to be edited.
   - The Edit Slack Details pop-up is displayed.
4. Make the necessary changes.
5. Click Slack and authorize the account and to establish a successful connection.
6. Click Save.
Deleting Slack data sources

To delete a Slack data source:
1. From the home page, click Data Sources.
2. Navigate to Slack.
3. Click Delete against the data source to be deleted. ▪ The Please confirm pop-up is displayed.
4. Click Yes.

Note: You can also perform bulk deletion of the data source by enabling the checkbox against it and clicking on Delete.
SharePoint
You can configure the application to collect from document libraries, wikis, blogs, calendars, contacts, announcements, surveys, and discussion boards on team and individual sites of SharePoint. The following are the versions supported:

- Microsoft SharePoint 2010
- Microsoft SharePoint 2013
- Microsoft SharePoint 2016
- Office 365
- OneDrive for Business (Collection of personal OneDrive accounts is not supported.)

If attempting to collect from GCC environments please refer to the Office 365 Credentials section.

Adding SharePoint data sources

To add a SharePoint data source:
1. From the home page, click Data Sources.
2. Navigate to SharePoint.
3. Click Add SharePoint.
- The **Add SharePoint Details** pop-up is displayed.

![Add SharePoint Details](image)

4. Enter the **Web Application URL**.
   - The value of this field is typically be formatted as the following: http://[Address]:[Port]

   where [Address] is the host name or IP address of the system hosting the SharePoint Web Application. You can optionally use the [Port] address if you are connecting to a specific SharePoint web application. If you provide a URL that does not specify the port, port 80 is used.

   If you specify a root path, such as http://server_name/, when you run the Collection, you can select SharePoint site URLs that may exist within sub sites off of the root path.

   For example, you could include URLs of any blogs, discussion boards, document libraries, or wikis within the specified root path.

   If you specify a SharePoint path to a particular organization’s department, you can include the blogs, discussion boards, document libraries, or wikis just within that department site. For example, the path may look like http://server_name/sites/marketing
5. Choose the **API Method**.

c) Graph API:

   i. Enter the **Locality**.

      - (Optional). Lets you type the name of the desired locality to associate this server to a specific location or IP range of nodes.

   ii. Enter the **Domain**.

      - (Optional) If the user account entered in the Username field is a domain user account, the domain must be specified; otherwise leave this field blank.

   iii. Enter the **Username**.

      - Lets you specify the username of an account that is granted Full Read access to SharePoint.

   iv. Enter the **Password**.

   v. Repeat the same password in **Confirm Password** field.
d) Export API:

i. Choose the **User Credentials**.

- No Credentials – This will fetch the credentials configured in the System Management > Manage Credentials page.
- New Credentials – Select this to configure users with new credentials.

![Add SharePoint Details Form](image)
Editing SharePoint data sources

To edit a SharePoint data source:

1. From the home page, click **Data Sources**.
2. Navigate to **SharePoint**.
3. Click **Edit** against the data source to be edited.
   - The **Edit SharePoint Details** pop-up is displayed.
4. Make the necessary changes.
5. Click **Save**.
Deleting SharePoint data sources  

To delete a SharePoint data source:

1. From the home page, click Data Sources.
2. Navigate to SharePoint.
3. Click Delete against the data source to be deleted.
   - The Please confirm pop-up is displayed.
4. Click Yes.

Notes: You can also perform bulk deletion of the data source by enabling the checkbox against it and clicking on Delete.
Exchange

You can configure the application to collect data from your Microsoft Exchange server which includes email, calendars, contacts, faxes, and voice mail. The following are the versions supported:

- Exchange 2010 SP1
- Exchange 2013
- Exchange 2016
- Exchange EAC (2019)
- Office 365

**Notes:** Exchange Online Basic Authentication deprecation is in progress (31st December 2022) and if already disabled will need to be enabled here: https://portal.office.com/adminportal/home/ to continue with any collections.

If attempting to collect from GCC environments please refer to the [Office 365 Credentials](#) section.
Adding Online/Office 365 data sources

EWS API Method

To add an Online/Office 365 data source (EWS API Method):

1. From the home page, click Data Sources.
2. Navigate to Exchange.

3. Click Add Exchange.
   - The Add Exchange Mail Server Details pop-up is displayed.
4. Select **Online/Office 365** as the **Version** from the drop-down.
5. Enter a **Name** for the Exchange Server.
6. Select the **EWS** option for **API Method** field.

7. Enter the IP address of the Exchange Server in **Address**.
8. Enter the **Tenant ID** in the **Admin Tenant** field.
9. Enter the **Microsoft Exchange Client ID**.
10. Enter the **Microsoft Exchange Client Secret**.
11. Select the **Associated to all custodian** checkbox to associate all the custodians to the server.

   **Note:** If you have previously associated individual custodian to a server, this action will overwrite the associations of the individual custodian.

12. Click **Save**.
Graph API Method

To add an Online/Office 365 data source (Graph API Method):

1. From the home page, click Data Sources.
2. Navigate to Exchange.

3. Click Add Exchange.
   - The Add Exchange Mail Server Details pop-up is displayed.
4. Select **Online/Office 365** as the **Version** from the drop-down.
5. Enter a **Name** for the Exchange Server.
6. Select the **Graph API** option for the **API Method** field.

7. Enter the **Tenant ID** in the **Admin Tenant** field.
8. Enter the **Microsoft Exchange Client ID**.
9. Enter the **Microsoft Exchange Client Secret**.
10. Select the **Associated to all custodian** checkbox to associate all the custodians to the server.

   **Note:** If you have previously associated individual custodian to a server, this action will overwrite the associations of the individual custodian.

11. Click **Save**.
**Export API Method**

*To add an Online/Office 365 data source (Export API Method):*

1. From the home page, click **Data Sources**.
2. Navigate to **Exchange**.

3. Click **Add Exchange**.
   - The **Add Exchange Mail Server Details** pop-up is displayed.

4. Select **Online/Office 365** as the **Version** from the drop-down.
5. Enter a **Name** for the Exchange Server.
6. Select the **Export API** option for the **API Method** field.
7. Select the any one of the below options for **User Credentials** field:
   - **No Credentials** – Select this option to create the data source without specific account credentials.
   - **New Credentials** – Select this option to create the data source for a specific user account. Upon enabling this option, the following fields will be displayed.

   - **Admin user account** – Provide the admin user account’s email address.
   - **Refresh Token** – Provide the corresponding accounts Refresh Token.

8. Click **Save**.
Adding Exchange data sources

*To add an Exchange data source:*

1. From the home page, click **Data Sources**.
2. Navigate to **Exchange**.

3. Click **Add Exchange**.
   - The **Add Exchange Mail Server Details** pop-up is displayed.

5. Enter a **Name** of the Exchange Server.
6. Enter the **Address**.
7. Enter the **Username**.
8. Enter the **Password**.
9. Repeat the same password in **Confirm Password** field.
10. You can select the **Exchange Server-side Mail Box Indexing Enabled?** checkbox if you have indexing enabled on the server.

   **Warning:** If you want to use filters on the data collected, you must have this action checked.

11. Enable the **Use Custom AD Settings** checkbox to use a custom active directory instead of the local active directory server.

   **Note:** By default, the application uses the local Active Directory server. If you have an advanced scenario, such as a cross-domain scenario, you can select to this option and specify the AD Server, AD Port, AD BaseDN settings.

12. Select the **Associated to all custodians** to associate all the custodians to the server.

   **Note:** If you have previously associated individual custodian to a server, this action will overwrite the associations of the individual custodian.

13. Click **Save**.
Adding On-Premise Exchange data sources (EAC)

**Notes:**
- FTK Central supports collection for the Exchange 2019 version.
- Refer to the Exterro Exchange Admin Center (EAC) - Configuration Guide.

**To add an On-Premise Exchange data source (EAC):**

1. From the home page, click **Data Sources**.
2. Navigate to **Exchange**.
3. Click **Add Exchange**.
   - The **Add Exchange Mail Server Details** pop-up is displayed.

![Exchange List](image)
4. Select Exchange EAC as the **Version** from the drop-down.

5. Enter a **Name** of the Exchange Server.
6. Enter the **Address**.
7. Enter the **Username**.
8. Enter the **Password**.
9. Repeat the same password in **Confirm Password** field.
10. Select the **Associated to all custodians** to associate all the custodians to the server.

   **Note:** If you have previously associated individual custodian to a server, this action will overwrite the associations of the individual custodian.

11. Click **Save**.
Mapping Exchange data sources to Custodians

To map an Exchange data source to custodians:

1. From the home page, click **Data Sources**.
2. Navigate to **Exchange**.
3. Click **Map Custodian** against the data source to be mapped.
   - The **Map Custodians** pop-up is displayed.
4. Select the required custodians by enabling the checkbox against it.
5. Click **Save**.
Editing Exchange data sources

To edit an Exchange data source:

1. From the home page, click **Data Sources**.
2. Navigate to **Exchange**.
3. Click **Edit** against the data source to be edited.
   - The **Edit Exchange Mail Server Details** pop-up is displayed.

4. Make the necessary changes.
5. Click **Save**.

**Note:** The fields displayed may vary based on the Exchange data source type.
Deleting Exchange data sources

*To delete an Exchange data source:*

1. From the home page, click **Data Sources**.
2. Navigate to **Exchange**.
3. Click **Delete** against the data source to be deleted.
   - The **Please confirm** pop-up is displayed.
4. Click **Yes**.

**Note:** You can also perform bulk deletion of data sources by clicking the checkbox against it and clicking on **Delete**.
Box
You can configure the application to collect structured and unstructured data from Box. You can add, edit, or delete multiple accounts from this page.

Adding Box data sources

*To add a Box data source:*

1. From the home page, click Data Sources.
2. Navigate to Box.

3. Click Add Box.
   - The Add Box Details pop-up is displayed.

4. Provide a Name for Box.
5. Enter the User Name.
6. Enter the Client ID.
7. Enter the Client Secret.
8. Enter the Public Key ID.
9. Enter the Private Key.
10. Enter the Private Key Password.
11. Click Save.
Editing Box data sources

To edit a Box data source:

1. From the home page, click **Data Sources**.
2. Navigate to **Box**.
3. Click **Edit** against the data source to be edited.
   - The **Edit Box Details** pop-up is displayed.

4. Make the necessary changes.
5. Click **Save**.
Deleting Box data sources

To delete a Box data source:

1. From the home page, click **Data Sources**.
2. Navigate to **Box**.
3. Click **Delete** against the data source to be deleted.
   - The **Please confirm** pop-up is displayed.
4. Click **Yes**.

**Note:** You can also perform bulk deletion of the data source by enabling the checkbox against it and clicking on **Delete**.
Office 365 Credentials

You can define the URLs to allow collections from Office 365 GCC environments such as Exchange, OneDrive, Teams and SharePoint. You can also choose the API method to be Graph API or Export API.

**Note:** When the required URLs are configured, they will only allow GCC high collections. Users must remove GCC URLs and replace them with non-GCC URLs to allow collections from non-GCC environments.

**GCC URLs**
Azure AD Authentication URL: [https://login.microsoftonline.us](https://login.microsoftonline.us)
Microsoft Graph URL: [https://graph.microsoft.us](https://graph.microsoft.us)

**Non-GCC URLs**
Azure AD Authentication URL: [https://login.microsoftonline.com](https://login.microsoftonline.com)
Microsoft Graph URL: [https://graph.microsoft.com](https://graph.microsoft.com)

**To define Office 365 credentials:**

1. From the home page, click **Settings** from the top-right corner.
2. Navigate to the **System Management** tab.
3. Click **Manage Credentials**.
4. Navigate to **Office 365 Credentials**.
5. Enter the **Azure AD Authentication URL**.
6. Enter the **Microsoft Sharepoint Locality**.
7. Enter the **Microsoft Sharepoint Domain**.
8. Choose the **API Method**.
   a) Graph API - Selecting this will collect data using the Graph API method.
   b) Export API (SCC) – Selecting this will collect data using the PowerShell script.
i. Enter the **Refresh Token**.

ii. Enter the **Admin User Account**.

iii. Enter the **Microsoft Teams Redirect URL**.

iv. Enter the **Microsoft Client ID (Teams & OneDrive)**.

v. Enter the **Microsoft Client Secret (Teams & OneDrive)**.

vi. Enter the **Microsoft Sharepoint Username**.

vii. Enter the **Microsoft Sharepoint Password**.

viii. Enter the **Tenant Active Directory Name**.

ix. Choose the **O365 Export Scope**.

   a. Indexed Only - All items, excluding the one that have unrecognized format are encrypted, or not indexed for other reasons.

   b. Unindexed only - Only the items that have an unrecognized format are encrypted, or not indexed for other reasons.

   c. Both Indexed and Unindexed - All the items, including the one that have unrecognized format are encrypted, or not indexed for other reasons.

9. Select the **Office 365 Environment** type.

   a) Standard - Select this to collect data for Standard Method where the URL of O365 will end with `.com`.

   b) GCC High - Select this to Collect data specific to GCC where the URL ends with `.us`.

10. Click **Save**.
Collections

Collections is a process that gathers, filters, and archives information from a wide variety of data sources. You can create a collection to collect data on a computer, network share, public data repository, email account, or all of the above within the application. The collection can be set up with filters to find only the files that are needed for the case. After collection, the data is processed and reviewed for relevance and transferred to the legal counsel.
**Elements of Collection**

<table>
<thead>
<tr>
<th>Managing Collections</th>
<th>Configuring data sources for collection</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Creating Collections</td>
<td>• Custodian (specific data sources)</td>
</tr>
<tr>
<td>• Approving Collections</td>
<td>• Data Sources</td>
</tr>
<tr>
<td>• Executing Collections</td>
<td>• Collection Filters for data source</td>
</tr>
<tr>
<td>• Processing Collections</td>
<td>• Viewing Collection Details</td>
</tr>
<tr>
<td>• Cancelling Collection Process</td>
<td>• Generating Reports for Collections</td>
</tr>
<tr>
<td>• Resubmitting Collections</td>
<td>• Editing Collections</td>
</tr>
<tr>
<td>• Viewing Collection Details</td>
<td>• Deleting Collections</td>
</tr>
<tr>
<td>• Generating Reports for Collections</td>
<td>• Editing Collections</td>
</tr>
<tr>
<td>• Editing Collections</td>
<td>• Deleting Collections</td>
</tr>
<tr>
<td>• Deleting Collections</td>
<td>• Configuring data sources for collection</td>
</tr>
</tbody>
</table>
Creating Collections

To create a collection:

1. From the home page, click **Collection**.
   - The Manage page of Collection is displayed.

2. Click **Create New Collection**.
   - The collection creation page is displayed.
3. Select the **Collection Type** based on the below description:
   - **File Scan** – To collect all the target files.
   - **Agent Scan** - To run collection jobs related to RAM/Volatile analysis, Software Inventory, Agent Remediation and IOC jobs. *(Refer the Agent Scan Collections section for more details)*
   - **Report Only** – To collect a list of endpoint files. This is used primarily to help you identify the data that can be collected by giving you a report collection in the file list.

4. Provide a **Name** for the collection.
5. Provide a **Description** for the collection.
6. Select the case associated to the collection from the **Case** drop-down field.
**Note:** The location for **Results Path** will be automatically populated based on the case selected in which the collected files will be stored. However, you can change the path if required. To do so,

i. Click **Folder** against the Results Path field.
   - The below page appears.

   ![Directory Browser](image)

   i. Enter the **Server Path**.
   
   ii. Click **Go** to view the directories available on the server.
   
   iii. Select the folder to be where the results are to be saved.

   ![Path Selection](image)

   iv. Click **Select**.
7. Select either of the **Target Options** section as stated below:

**Note:** Selecting **Custodian’s** with the **Custom** option will collect only the data from the data sources selected for a particular Custodian and selecting one from the **Data Sources** section will collect all the data from the particular data source, both associated and unassociated to custodians.

Alternatively, using the **Group** option will allow collection of all custodian associated data sources within an assigned group.
a. Enable the required **Custodian's** option and select any or all of the below data sources:
   - Select Custodian's Computers
   - Select Custodian's Shares
   - Select Custodian's Exchange
   - Select Custodian's Gmail
   - Select Custodian's OneDrive
   - Select Custodian's Box
   - Select Person's Google Drive

   (OR)

b. Select any or all of the following **Data Sources**:
   - Computers
   - Network Shares
   - SharePoint
   - Microsoft Teams
   - Slack
   - Box
8. Enable the **Advanced Options Activated** checkbox to configure the following advanced collection functionalities:

i. Select any of the following options for **AD1 Encryption** field:
   - **Disabled** – To turn off encryption of an AD1 evidence image file.
   - **Certificate** – To encrypt an AD1 evidence image file with a certificate. Certificates use public keys for encryption and corresponding private keys for decryption. You can configure the certificates that appear in the drop-down menu.
   - **Password** - To encrypt an AD1 evidence image file with a password that you specify.

ii. Enable **Create AD1 Files on Agent** to create a AD1 image on the machine.

iii. Enable **Skip PST Creation** checkbox to avoid creating a PST file while collecting email files.

iv. Enable **Maximum Concurrent Agent(s)** toggle to limit the amount of active agent jobs running concurrently.
9. Select any one of the below provided options to define the time the system (site servers) should try and contact data sources within a job from the Job Expiration field:

- **Single Attempt** – To try only one once and terminate the unsuccessful attempt.
- **Cancel Pending** – To define the time after which a pending job should be terminated. Agents that have already contacted the server will continue to run until the task is complete regardless of the expiration date.
- **Cancel Incomplete** - To define the time after which an incomplete job should be terminated.

**Warning:** When cancelling a recurring job, only the job that is currently running in Site Server will cancel. The next occurrence of the job will start at its appointed time.
10. Enable the **Auto Process Collection** option to process the evidence automatically.

    **Note:** If this option is disabled, you will have to manually trigger the processing.

11. Select the required processing profile from the **Processing Option** drop-down field.

12. Enable the **Auto Deploy Agents** option if you want to deploy agents to computers included in the collection. Refer to the **Agent Credentials** section.
13. While multiple collections can run simultaneously, Batching Options allow jobs to run in groups. I.e., A selection of 3 Maximum Concurrent Agents will only allow 3 concurrent jobs to be run at once until finished, which would then allow the next batch of jobs to be started.

**Warnings:**
- The Auto Deploy is applicable only when the Target Option is selected as Computer against the Custodians or the Data Sources.
- The Auto Deploy option will not be applicable if multiple options are selected against the Custodians or Data Sources.

(OR)
14. Click **Save and Next**.

**Data Sources**

Based on the data sources selected in the Target Options, the corresponding data source configuration sections will be displayed for you. Detailed steps to configure the required data source is provided in the [Data Source Configuration](#) section.
15. Select the **Execution Mode** for the Collection based as required:

- **Manual** – You should initiate the collection process manually.
- **Scheduled** – You can configure the **Collection Start Date** during when the collection will be initiated.
- **Automatic** – The collection is automatically initiated based on the approval mode selected.

16. Select the **Approval Mode** based on the below description:

- **None** – No approvals required for the collection.
- **By Role** – Only users with selected roles assigned to them can approve this collection. After the collection is created, the job must first be approved and then it must be executed.
- **By User List** – Only the users selected in the corresponding list can approve this collection. After the collection is created, the job must first be approved (by all the selected users) and then it must be executed.
17. Review and ensure all the configurations made for the collection are correct.

**Note:** You can click Back to navigate back to the previous page to make any changes.

18. Click Submit Collection.

The collection will be created and the process will be initiated based on the selected **Execution Mode**.
Agent Scan Collections

You are able to run agent jobs that range from remediation, software inventory to threat scans:

- Software Inventory
- Agent Remediation
- Volatile Job
- Threat Scan
- Memory Acquisition
- Memory Analysis

Setting up Agent Scan Jobs

To set up agent scan job:

1. From the homepage, click Collection.
2. Click Create New Collection.
   - The Create New Collection page will be displayed.
3. Select the Collection Type as Agent Scan.
4. Provide the collection’s Name.
5. Provide a brief description of the collection in the Description field.
6. Select the case associated to the collection from the **Case** drop-down field.

**Note:** The location for **Results Path** will be automatically populated based on the **Case** selected in which the collected files will be stored. You can modify the path if required.

7. Select the **Computers** options from the **Data Sources** column for the **Target Options** field.

**Note:** Alternatively, you can enable the **Custodians** option > **Select Person’s Computers**.

8. Enable the **Auto Process Collection** option to process the evidence automatically.
9. Enable the **Auto Deploy Agents** option if you want to deploy agents to computers included in the job.
10. Customize the **Batching Options** to run collection jobs on computers in batches.
11. Click **Save and Next**.
12. If **Auto Deploy Agents** was selected, you will be navigated to the **Agent Operations** section where the following information should be configured:
   13. **Install** – Select to push an agent to the endpoint. This can cause the machine to restart without warning.
   o **Make Public Instance** - Configure the agent to check a public instance after the agent is installed.
   o **Agent Type**: Local Storage
   o **Use Site Server Default Port** – Configure the default port the site server is using.
   o **Use Custom Port** – Configure the custom port for agent usage.
   o **Service Name** – Configure the name of the agent service.
   o **Executable Name** – Configure the name of the agent executable.

   (OR)
   • **Uninstall** – Select to remove an agent from the endpoint.

14. Click **Save and Next**.
15. Select the required **Computers**.
16. Select any one of the below provided **Agent Scan Type**.

   • **Software Inventory**
   • **Agent Remediation**
   • **Volatile Job**
   • **Threat Scan**
   • **Memory Acquisition**
   • **Memory Analysis**

Follow the sections below to configure Agent Scan types.
Scheduling an Agent Scan Job

To schedule agent scan job:

1. From the Scheduling & Approvers section, select the Execution Mode as Scheduled.
2. Check Enable Recurrence.
   a. Configure the Recurrence Pattern based on your requirement.
   b. Configure the End Recurrence based on your requirement.
   c. If required, select the Incremental Collection option for the Collection Options field. This allows you to view data as soon as it becomes available rather than having to wait for the whole collection to be completed.
Software Inventory

The Software Inventory collection job will retrieve data relating to the software installed on the machine as well as any hardware utilization data. The installedsoftware.xml associated with this collection will be stored in the job data path related to the job named during the collection.

*To set up the software inventory job:*

1. Select **Software Inventory** as the **Agent Scan Type**.
2. Click **Save and Next**.
3. Configure the **Scheduling & Approvers** section based on your requirements.
4. Click **Save and Next**.
5. Click **Submit Collection**.

**Tip:** The **System Inventory** column set in review mode can be utilized to efficiently review the system data.
Agent Remediation

The Agent Remediation job allows processes to be stopped, scripts to be sent and executed and file deletion.

**Note:** When Executing or Sending Files, ensure paths provided are absolute. Additionally, ensure they are not UNC paths.

**To setup the agent remediation:**

1. Select **Agent Remediation** as the **Agent Scan Type**.
2. Click **Add New Row** in the **Agent Remediation** section.
3. Select any one of the below provided options for the **Remediation Command** field.
   - Kill process by process ID.
   - Kill all process by name.
   - Delete file.
   - Execute.
   - Send file.

**Tip:** Multiple options can be run by clicking **Add New Row** consecutively.
Kill process by process ID

To kill processes by process ID on an endpoint:

4. Ensure the **Kill process by process ID** option has been selected for the **Remediation Command** field.
5. Enter the Process ID in the **Remediation Data** field.
6. Click **Save**.
7. Click **Save and Next**.
8. Configure the **Scheduling & Approvers** section based on your requirements.
9. Click **Save and Next**.
10. Click **Submit Collection**.
**Kill process by name**

To kill processes by name on an endpoint:

11. Ensure the **Kill all process by name** option has been selected for the **Remediation Command** field.
12. Enter the process name in the **Remediation Data** field.
13. Click **Save**.
14. Click **Save and Next**.
15. Configure the **Scheduling & Approvers** section based on your requirements.
16. Click **Save and Next**.
17. Click **Submit Collection**.
Delete File

To delete files on an endpoint:

18. Ensure the **Delete file** option has been selected for the **Remediation Command** field.
19. Provide the **Description**.
20. Enter the Target File Path (for the file to be deleted).
21. Click **Save**.
22. Click **Save and Next**.
23. Configure the **Scheduling & Approvers** section based on your requirements.
24. Click **Save and Next**.
25. Click **Submit Collection**.
**Execute**

*To execute files on an endpoint:*

26. Ensure the **Execute** option has been selected for the **Remediation Command** field.
27. Provide a **Description**.
28. Enter the **Target File Path** (for the file to be executed) – this is the file located on the local machine. **Example**: `Powershell.exe`.
29. Enter any **Command Arguments** if required.
30. Enable the **Spawn the process** option to automatically start any processes during execution.
31. Click **Save**.
32. Click **Save and Next**.
33. Configure the **Scheduling & Approvers** section based on your requirements.
34. Click **Save and Next**.
35. Click **Submit Collection**.
Send File
To send a file to an endpoint:

36. Ensure the Send File option has been selected for the Remediation Command field.
37. Provide a Description.
38. Enter or browse & select the Source File Path (the file being sent).
39. Enter the Destination File Path (where the file will be stored).
40. Select any one of the following operation commands if required:
   - Delete File
   - Execute
     - Arguments

41. Click Save.
42. Click Save and Next.
43. Configure the Scheduling & Approvers section based on your requirements.
44. Click Save and Next.
45. Click Submit Collection.
Volatile Job

Volatile job performs an analysis of the processes, connections, services running on the operating system as well as any (customizable) registry files using Volatility. The subsequent XML files generated from Volatility can be found within the case folder. This data can be processed through Cerberus if required.
To set up the volatile job for agent scan collections:

1. Select **Volatile Job** for the **Agent Scan Type** field.
2. Check the required **Volatile Options**.

   **Note:** If required, you can enable the **Select All** option to select all **Volatile Options**.

3. Select any one of the below provided **Registry** options:
   - **None**
   - **Include Registry** – To include information relating to the selected registry key.
   - **Include Registry On Disk** – To include information relating to the selected registry key as well as any hidden values.

4. Upon selecting a **Registry** option, select any one of the below provided pre-defined templates from the drop-down and click on **Add Rows From Template**.
   - AutoStart
   - General
   - Hardware
   - UserActivity

   **Warning:** The above field will be disabled if **None** is selected as the **Registry** option.

5. Click **Save and Next**.
6. Configure the **Scheduling & Approvers** section based on your requirements and click **Save and Next**.
7. Click **Submit Collection**.

   **Note:** When collecting processes from a Linux endpoint, some processes may return a hash value of 0. This is correct as these particular items are forked processes, drivers or routines from a parent process.

   **Tip:** To classify volatile jobs efficiently, the **Object Type** and **Object Sub Type** columns can be used during review.
Threat Scan

Threat Scan jobs are jobs that search for threats in the data. Threat Scan jobs apply filters from the IOCs and YARA rules to the data and alert you to suspicious files.

IOCs are XML documents that allow you to capture information about threats to your enterprise, including malware, registry changes, and memory artifacts. YARA rules are custom rules that you import that allow you to hunt for malware by values found in the binary or in physical memory.

Note: When creating or locating a YARA rule, make sure that the YARA rule identifier (the first line of the YARA rule) contains only alphanumeric characters and the underscore ‘_’ character. For more information about writing YARA rules, see the YARA user manual at http://plusvic.github.io/yara/.

Criteria for Successful IOCs

When either creating or examining an IOC, make sure that IOC contains the following criteria:

- The focus of the IOC should be narrow. Rules specified in the IOC should focus on one particular aspect instead of casting a wide net in the data. For example, instead of an IOC rule specifying the examination of an entire system, the rule should specify a file path within the system. Or if a registry is to be examined, the IOC should examine a hive in the registry, not the full registry.

- The IOC should not consume massive system resources. Rules specified in the IOC should avoid taxing system resources. For example, if you are searching for a specific item, you should specify that the IOC examines the metadata, which can be restricted by filter. If you specify that the IOC examines the inner details, the system must open and examine every file. This consumes more system resources and taxes the system.

- An IOC with more indicator items is better than an IOC with fewer indicator items. Rules specified in the IOC should have as many indicator items as necessary. This allows the IOC to filter the data to a more manageable subset. For example, an IOC that searches for a file that is smaller than 10MB and is larger than 5MB (5<x>10) will be more successful than an IOC that only searches for a file that is smaller than 10MB (10<x).
To perform an IOC threat scan on an endpoint:

1. Select **Threat Scan** as the **Agent Scan Type**.
2. Click **Import**.
   - The **Threat Filter Import Wizard** prompt is displayed.
3. Select **IOC** for the **Threat Filter Type** field.
4. Click **Next**.
5. Click **Add Files** or **Add Folder** to browse and import the required set of rules.

   **Note:** You can enable the **Directory processing is recursive** option in order to process the child folders and files.
6. Click **Save and Next**.
7. If required, enter a **Source**, **Category**, **Tag** and **Group**.
8. Click **Submit**.
9. Check the imported rules.
10. If required, select and configure the required **Advanced Options** provided below:
    - Perform String Content Search
    - Disable File Hashing
      - Disable only for files larger than
    - Disable YARA for files larger than
    - Archive Drill Down
11. Click **Save and Next**.
12. Configure the **Scheduling & Approvers** section based on your requirement.
13. Click **Save and Next**.
14. Click **Submit Collection**.
YARA

To perform YARA threat scans on an endpoint:

1. Select **Threat Scan** as the **Agent Scan Type**.
2. Click **Import**.
   - The **Threat Filter Import Wizard** prompt is displayed.
3. Select **YARA** for the **Threat Filter Type** field.
4. Click **Next**.
5. Click **Add Files** or **Add Folder** to import the required set of rules.

**Note:** You can enable the **Directory processing is recursive** option in order to process the child folders and files.

6. Click **Save and Next**.
7. Select any of the below provided *Yara Advanced Filtering* options.

10. **Target Process** - Allows the YARA rule to target memory and other processes.

11. **Target Files** - Allows the YARA rule to target files. You can filter the files by the following:

12. **Extension** - Allows you to filter files by extension. List multiple extensions in a comma separated list. You can filter the extensions by either an equal or not equal operator. You can use a star (*) as a wildcard.

13. **Path Contains** - Allows you to filter files by the path contains. You can enter a partial path in the field as well as enter a fully qualified path.

14. **File Size (Bytes)** - Allows you to filter files by file size. You can filter file size by the following operators: any, equal, greater than, or less than. Specify the file size by bytes, kilobytes, or megabytes.

15. **File Creation Date** - Allows you to filter files by file creation date. You can filter the file creation date by the following operators: any, range, or single. For range, you can specify either outside of the range or between the range.

16. **File Modified Date** - Allows you to filter files by file modification date. You can filter the file modification date by the following operators: any, range, or single. For range, you can specify either outside of the range or between the range.

17. **File Last Accessed Date** - Allows you to filter files by file last accessed date. You can filter the file last accessed date by the following operators: any, range, or single. For range, you can specify either outside of the range or between the range.

18. **Target Both** - Allows the YARA rule to target both memory and other processes.
8. Click **Save and Next**.
9. If required, enter the information for Source, Category, Tag and Group fields.
10. Click **Submit**.
11. Check the imported rules.
12. If required, select any of the below provided **Advanced Options**:
   - Perform String Content Search
   - Disable File Hashing
     - Disable only for files larger than
   - Disable YARA for files larger than
   - Archive Drill Down
13. Click **Save and Next**.
14. Configure the **Scheduling & Approvers** section based on your requirements.
15. Click **Save and Next**.
16. Click **Submit Collection**.
Collecting Matched Files

When a Threat Scan is complete and has found matches on an endpoint, FTK Central will create a Threat Scan Filter which can be found in the case. The item will be listed in the review grid as Threat Scan Filter. While the threat scan filter will list the name of the matched files, it will further include the path, created date, modified date, accessed data, MD5 hash as well as the size.

To collect the matched files:

1. From the homepage, click Case.
2. Select a case that has had a successful threat scan job completed.
3. Click on the case name.
4. Click Enter Review.
5. Locate the Threat Scan Filter in the grid.
6. Check the required files to be collected.
7. Click Collect Files.

This will automatically collect the matched items and the processed files will be displayed in the case Review.
Memory Acquisition
Executes a memory acquisition job that includes a page file and creates an archive file. The file can be found in the jobs folder associated to the case configured during collection.

To acquire memory from an endpoint:
1. Select Memory Acquisition as the Agent Scan Type.
2. Select the required Memory Acquisition options.
3. Include a page file
4. Include Archive file
5. Click Save and Next.
6. Configure the Scheduling & Approvers section based on your requirement.
7. Click Save and Next.
8. Click Submit Collection.
Memory Analysis
Executes a memory analysis job collecting DLLs, Drivers, Handles, Registry, Sockets, and VAD information.

To configure the memory analysis job:
1. Select Memory Analysis as the Agent Scan Type.
2. Select the required Memory Analysis options:
   - Include Interrupt Descriptor Table Analysis
   - Include Service Descriptor Table Analysis
   - Include Driver Analysis
   - Include DLLs
   - Include Handles
   - Include Sockets
   - Include VAD
   - Include Crypto
   - Include Registry
3. Click Save and Next.
4. Configure the Scheduling & Approvers section based on your requirement.
5. Click Save and Next.
6. Click Submit Collection.

Tip: The Memory Analysis column set in review mode can be utilized to efficiently review memory data.

Job Template
Creating a Job Template
The job templates can be utilized to create a pre-configured collection intended to assist you during collection creation. Templates can be edited during execution, if required.
To create a job template:

1. From the homepage, click **Collections**.
2. Click **Create New Collection**.
   - The **Create New Collection** page will be displayed.
3. Configure the **Collection Options**.
4. Enable the **Save As Job Template ONLY** option in order to save the configured information as a template to be used later.

   **Note:** You can enable the **Include Target Options in Template** option to also save the **Target Options** configuration to the template.

5. Select further collection options.

   **Note:** These changes made to the collection plan after enabling the **Save As Job Template ONLY** option will also be saved to the template.

6. Click **Submit Template**.
Selecting a Job Template

**To select a job template:**

1. From the homepage, click **Collections**.
2. Click **Create New Collection**.
   - The **Create New Collection** page will be displayed.
3. Configure the Collection Options.
4. Enable the Use Job Template option.
5. Select the required template from the drop-down list.
6. Upon selecting the template, corresponding information will be auto-populated to the relevant fields.
Note:

- You can choose to delete the selected job template by clicking on the **Delete Job Template** icon displayed against the selected template.

- If the **Include Target Options in Template** option is enabled while creating a template, the corresponding targets information will also be selected during collection creation.
Managing Collections

After creating a collection, based on the approval, execution, and processing options, you will have to manage the collection to complete it. This section helps you in managing the collection at various statuses. Depending on the stage on which the collection is at a moment, there are 8 statuses for a collection as listed below:

<table>
<thead>
<tr>
<th>Collection Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not Started</td>
<td>Collection has been created but no collection data has been retrieved.</td>
</tr>
<tr>
<td>Collecting</td>
<td>Collection process has started and data is being collected.</td>
</tr>
<tr>
<td>Completed</td>
<td>Collection is completed and data has been retrieved.</td>
</tr>
<tr>
<td>Cancelled</td>
<td>Collection has been cancelled.</td>
</tr>
<tr>
<td>Terminated</td>
<td>Collection has been terminated by a user.</td>
</tr>
<tr>
<td>Failed</td>
<td>Collection has failed.</td>
</tr>
<tr>
<td>Completed with Errors</td>
<td>Collection is completed but with some errors during collection.</td>
</tr>
<tr>
<td>Pending</td>
<td>Collection is yet to start, pending approval.</td>
</tr>
</tbody>
</table>

**Tip:** To filter the grid efficiently, you can simply enter a keyword into the search box located at the top of any grid and click the search button or press enter.
Approving Collections

Depending upon the Approval Mode selected, the collection has to be approved before it can be executed.

Warning: If multiple approvers were selected during the collection creation, all the selected users must approve the collection.

To approve a collection:

1. From the home page, click Collection.
2. Click on the Context menu against the required collection.
3. Click on Approve Collection.
   - The Job Approve prompt is displayed.
4. Click Approve.

Notes:
- You can click on Approve & Execute to concurrently approve and execute the collection process.
- The collection will be approved for processing and the process will be initiated based on the Execution Mode configured for the collection.
Executing Collections

Executing a collection initiates the process of collecting the data from the target data sources. Based on the execution mode selected, you may have to manually trigger the execution for a collection. It is to be noted that you can execute a collection only after it is approved.

To execute a collection:

1. From the home page, click Collection.
2. Click on the Context menu against the required collection.
3. Click on Execute Collection.
4. The Job Execution prompt is displayed.

4. Click Yes.
Processing Collections

If you automatically process a collection, the full collection is processed each time. For example, for the first collection, 100 files are processed. The second collection, 105 files are processed. The third collection, 145 files are processed. During the review process you will see 350 files. If the same file occurs during all three collections, then the object names will remain identical, but the objectids will be unique.

To process a collection:

1. From the home page, click **Collection**.
2. Click on the **Context menu** against the required collection.
3. Click on **Process Collection**.
4. The **Job Process** prompt is displayed.
5. Click **Yes**.
Cancelling Collection Process

To cancel a collection process:

1. From the home page, click **Collection**.
2. Click on the **Context menu** against the required collection.
3. Click on **Cancel Collection**.
4. The **Job Cancellation** prompt is displayed.

   *Computer Collection*: The job will be cancelled. Press Yes to proceed

   - Click **Yes**.
Resubmitting Collections

There may be situations where collection jobs have been stopped or failed due to your circumstances. Resubmitting a collection will allow you to run a collection job against the target again.

**To resubmit a collection job:**

1. From the home page, click **Collection**.
2. Click on the **Context menu** against the required collection.
3. Click on **Resubmit Collection**.
   - The **Resubmit Job** prompt is displayed.
4. Provide a name for the resubmitted collection in **New Job Name**.
5. Select any one of the following **Resubmit Types** based on their descriptions:
   - **Include Failed Items Only** – To collect only the failed files.
   - **Include all Incomplete Items Only** – To collect all the files that were not collected in the previous iteration.
   - **Include all Failed Files (Shares Only)** – To collect all the files that were not collected in the previous iteration from just the Network Shares data source.
   - **Copy Job** – To duplicate the collection process and re execute the collection based on the **Collection Option**.
6. Select any one of the following Collection Options based on their descriptions:
   - **Full** – To collect all the files present in the data sources associated to the collection.
   - **Incremental** – To collect only the files newly added to associated data sources after completing the collection process.

7. Click **Resubmit**.
Viewing Collection Details

You can view a snapshot of collection which includes information about the name of the collection, collection progress (in terms of percentage), total volume of files collected, time taken to collect the files, number of data sources targeted, last collected file, etc.

To view the collection details:

1. From the home page, click **Collection**.
2. Click on the **Context menu** against the required collection.
3. Click on **Collection Details**.

- The **Collection Progress** prompt is displayed.

Note: You can click on **Responsive File Path** button against the required data source to view the location path where the collected files are stored.
Generating Reports for Collections
You can generate detailed information reports on collected files, emails, file statistics, remediated files, etc. of a collection.

⚠️ **Warning:** You can generate a report only after the collection is processed.

**To generate the reports specific to a collection:**
1. From the home page, click **Collection**.
2. Click on the **Context menu** against the required collection.
3. Click on **Collection Details**.
4. Click on the **Download Reports** button and select any of the below mentioned reports to download it in .xlsx format.

<table>
<thead>
<tr>
<th>Report Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Details Report</td>
<td>Provides a detailed snapshot of the collection which includes the Collection options, data sources, collection results (success/failure) for nodes.</td>
</tr>
<tr>
<td>Results Report</td>
<td>Displays information on collection results for the job. When using a collection job to collect emails, an EmailID is generated for each email by FTK Central. This EmailID is displayed in a column in the collected email and failed email tabs of the jobs results report.</td>
</tr>
<tr>
<td>Errors Report</td>
<td>Displays a breakdown of failed targets and the errors associated to the collection.</td>
</tr>
</tbody>
</table>

**Tip:** The downloaded reports will also be available in the Case Folder Path.
Editing Collections

To edit a collection:

1. From the home page, click **Collection**.
2. Click on the **Context menu** against the required collection.
3. Click on **Edit Collection**.
   - The **Edit Collection** page is displayed.
4. Make the necessary changes.
5. Click **Submit Collection**.
Deleting Collections

To delete a collection:

1. From the home page, click Collection.
2. Click on the Context menu against the required collection.
3. Click on Delete Collection.
   - The Please confirm prompt is displayed.
4. Click Delete.
Reviewing Collections

To review a collection:

Users can access an associated case to a collection efficiently by using the review icon. This icon will navigate users to the review mode.

1. From the home page, click **Collection**.
2. Click on the **Review icon** against the required collection.
   - The associated case will open in review mode.
Data Source Configuration for Collection

In order to collect information from the required data sources, you should select the required options from the Target Options field while creating a collection. Here, the options in Custodian's and Data Sources are mutually exclusive i.e., you can select either Custodian's or Data Sources.

Notes:
- Only upon enabling the Custodian's checkbox, the corresponding options will be enabled.
- You can select more than one options for Custodian's and Data Sources fields.

Note: Ensure the Creating Collections Section has been reviewed before attempting a Data Source collection.
Custodian-based Collections

To configure the custodian data source for collection:

Upon selecting the required data sources under the Custodian’s section,

1. Select the required custodians from the list

2. Click Save and Next.

Based on the selected data sources, any or all of the following data sources are to be configured:
Computers
Computer-based collections allow endpoint collections with exclusive configuration options as listed below.

**Auto Deploy Agents**
The Auto Deploy option will be applicable only when the computer is selected in the target options, either against the Custodians or Data Sources.

1. Upon enabling the **Auto Deploy Agents** checkbox and clicking on **Save and Next**, the below **Agent Operations** section will be displayed.
On the Agent Operations page, select from the following options:

<table>
<thead>
<tr>
<th><strong>Option</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Uninstall</td>
<td>Select to remove the agent from the machine</td>
</tr>
<tr>
<td>Install</td>
<td>Select to push the agent to the machine. Remember that the agent install may cause the machine to restart without a warning.</td>
</tr>
<tr>
<td>Make Public Instance</td>
<td>Configure the agent to check a public instance after the agent is installed.</td>
</tr>
<tr>
<td>Configure Periodic Check-In</td>
<td>Configure the agent to communicate back to the server.</td>
</tr>
<tr>
<td>Agent Type – Local Storage</td>
<td>Agent uses local files for configuration and data. Agent is installed (persists after reboot).</td>
</tr>
<tr>
<td>Use Site Server Default Port</td>
<td>Enabling this will force the agent to use Port:54545</td>
</tr>
<tr>
<td>Use Custom Port</td>
<td>Enter the port designated to communicate with the agent.</td>
</tr>
<tr>
<td>Service Name</td>
<td>Enter the name that you want the agent to be displayed as.</td>
</tr>
<tr>
<td>Executable Name</td>
<td>Enter the name of the file that is being run.</td>
</tr>
</tbody>
</table>

Upon selecting the required agent operations and clicking on Save and Next, you will be navigated to the Custodians section.

(OR)

If the Agent Deploy option is not selected in the Collection Options section, the Agent Operations section will be skipped and you will be navigated to the Custodians section.

Upon selecting the required custodians and clicking on Save and Next from the Custodians section, you will be
navigated to the **Computers** section.

2. Select the required computers from the list.

   **Warning:** You cannot proceed to collect all the data from the computer. You must include at least one among the Extension, Size, Date, Path, Luhn, Keyword, or MD5 Hash filter properties within the Include/Exclude filters to perform a targeted collection.

3. Click **Save and Next**.
**Batching Options**

While multiple collections can run simultaneously, Batching Options allow jobs to run in groups. I.e. A selection of 3 Maximum Concurrent Agents will only allow 3 concurrent jobs to be run at once until finished, which would then allow the next batch of jobs to be started.

**Advanced Filter Options**

You can configure the **Advanced Filters** section in the right pane to filter and collect only the required information based on the type of Collection. The applicable filters for the collection types are listed below:

i. **For Filtered Collection:**

<table>
<thead>
<tr>
<th>Type</th>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Source Type</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>File System</td>
<td>To collect the drives from the target's file system.</td>
<td></td>
</tr>
<tr>
<td>Logical Disk</td>
<td>To collect only the target's logical drive space.</td>
<td></td>
</tr>
<tr>
<td>Physical Disk</td>
<td>To collect the target's entire physical drive.</td>
<td></td>
</tr>
<tr>
<td><strong>Search Type</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Site Server</td>
<td>To search using the Site Server.</td>
<td></td>
</tr>
<tr>
<td>Agent &amp; Site Server</td>
<td>To search first with the agent and then with the Site Server.</td>
<td></td>
</tr>
<tr>
<td>Agent</td>
<td>To search files using the agent.</td>
<td></td>
</tr>
<tr>
<td>Collect System Files</td>
<td>To search system files that are normally hidden from view. Files with “$” contain system meta data and in NTFS, the $MFT contains the file system pointers to all files.</td>
<td></td>
</tr>
<tr>
<td>Scan Deleted Files</td>
<td>To scan free space of a partition for files matching the filter criteria.</td>
<td></td>
</tr>
<tr>
<td>Scan Unused Disk Area</td>
<td>To scan unallocated disk space for files matching filter criteria.</td>
<td></td>
</tr>
<tr>
<td>Archive Drill Down</td>
<td>If archive files exist in any of the available data sources that contain compressed files of interest, this option lets you open the archive</td>
<td></td>
</tr>
<tr>
<td>Type</td>
<td>Options</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>----------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>Collect Responsive Archives</td>
<td>Collects any archive that contains files that match filter criteria.</td>
</tr>
<tr>
<td></td>
<td>Custom Drill Down Extensions</td>
<td>Allows you to specify the extension for the archive drill down. If you do not specify the extension, the default will be used.</td>
</tr>
<tr>
<td></td>
<td>Include Deleted Files</td>
<td>Will scan free space of a partition for files matching filter criteria.</td>
</tr>
<tr>
<td></td>
<td>Use Internal File Identification</td>
<td>Sees the software’s file identification when checking file extensions.</td>
</tr>
<tr>
<td></td>
<td>Collect Non-Extension Files</td>
<td>Collects all files that do not have an extension.</td>
</tr>
<tr>
<td></td>
<td>Collect Unsearchable Encrypted Files</td>
<td>Will collect encrypted files that cannot be accessed to search for keyword filter criteria.</td>
</tr>
<tr>
<td></td>
<td>Enable PreScan</td>
<td>Will scan the collection target before collecting. Enables accurate completion percentage, file counts, and size predictions for Real Time Status screen.</td>
</tr>
<tr>
<td></td>
<td>Parse $130 INDX Records</td>
<td>Gets additional information about deleted files.</td>
</tr>
<tr>
<td></td>
<td>Exclude Removable Drives/Media</td>
<td>Excludes removable drives that are recognized by Site Server from the collection. This option is only available for collection jobs. Not all removable drives are recognized</td>
</tr>
</tbody>
</table>
Type | Options | Description
--- | --- | ---

as such so this option may not exclude ALL removable drives

ii. For Full Disk Acquisition

A Full Disk Acquisition job would collect the entire contents of a computer’s hard drive, so the advanced options will include fewer choices as listed below:

- Collect from Target Options
  - **Logical Disk**: To collect only the target’s logical drive space.
  - **Physical Disk**: To collect the target’s entire physical drive. You can choose the sectors required.

- **Use Redirected Acquisition**: Uses the agent to push the collected data directly to the Job Data path given in the Job Options screen instead of moving it to the temporary storage location and then to the Job Data path.
**Include/Exclude Filter Options**

When creating a filtered collection, Include/Exclude filters will be available. The table below lists all available options when creating a File Scan/Report Only collections.

<table>
<thead>
<tr>
<th>Options</th>
<th>Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter Name</td>
<td>Allows you to name a filter when attempting to save it as a template.</td>
</tr>
<tr>
<td>Extensions</td>
<td>Allows you to filter files by extension. List multiple extensions in a comma separated list. You can filter the extensions by either an equal or not equal operator. You can use a star (*) as a wildcard.</td>
</tr>
<tr>
<td>Path</td>
<td>Allows you to filter files by the path contains. You can enter a partial path in the field as well as enter a fully qualified path. For example, if you added “confidential”, it would include all folders with “confidential” in the path.</td>
</tr>
<tr>
<td>File Size (bytes)</td>
<td>Allows you to filter files by file size. You can filter file size by the following operators: any, equal, greater than, or less than. Specify the file size by bytes, kilobytes, or megabytes.</td>
</tr>
<tr>
<td>File Creation Date</td>
<td>Allows you to filter files by file creation date. You can filter the file creation date by the following operators: any, range, or single. For range, you can specify either outside of the range or between the range.</td>
</tr>
<tr>
<td>File Modified Date</td>
<td>Allows you to filter files by file modification date. You can filter the file modification date by the following operators: any, range, or single. For range, you can specify either outside of the range or between the range.</td>
</tr>
<tr>
<td>File Last Accessed</td>
<td>Allows you to filter files by file last accessed date. You can filter the file last accessed date by the following operators: any, range, or single. For range, you can specify either outside of the range or between the range.</td>
</tr>
</tbody>
</table>
| Keywords              | Allows you to include files that match any or all regular expressions/keywords entered into the text field. When writing queries for the Keyword(s) field, use the terms AND or OR to help refine your search. For example:  
  - Apple AND orange returns files with both terms apple and orange.  
  - Apple OR orange returns files with either the term apple or orange.  
  - (Apple AND orange) OR (banana) returns files with either the terms apple and orange or files with the term banana.  
  - ‘Apple and orange’ OR banana returns files with either the term apple and orange or files with the term banana. |
<p>| Credit Card Numbers   | Used in conjunction with the Keyword option, the credit card option allows you to include credit card numbers using Luhn testing. Luhn testing distinguishes valid credit card numbers from what could be a random selection of digits. |</p>
<table>
<thead>
<tr>
<th>Options</th>
<th>Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search File Name Only</td>
<td>Used in conjunction with the Keyword option, this forces the keyword search to only apply to file names.</td>
</tr>
<tr>
<td>Custom</td>
<td>Allows you to include a custom regex expression. To filter by regular expressions, enter the regular expression delimiters. For example: <code>\d\d\d\d</code>. You are not able to use dashes when creating a custom regex expression. For example: <code>\d\d\d\d\d\d\d\d\d\d\d\d\d</code></td>
</tr>
<tr>
<td>MD5 Hash</td>
<td>Allows you to add specific MD5 hash values to be included in the job.</td>
</tr>
</tbody>
</table>
Network Shares

Upon selecting the required custodians and clicking on **Save and Next** from the **Custodians** section, you will be navigated to the **Network Shares** section.

1. Select the required network share locations from the list.

   **Note:** You can filter the files from the data source by using the Include/Exclude filters.

2. Click **Save and Next**.
**Advanced Filter Options**

You can configure the **Advanced Filters** section in the right pane to filter and collect only the required information by using any of the filters provided below:

<table>
<thead>
<tr>
<th>Filter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collect System Files</td>
<td>To search system files that are normally hidden from view. Files with “$” contain system meta data and in NTFS, the $MFT contains the file system pointers to all files.</td>
</tr>
<tr>
<td>Archive Drill Down</td>
<td>If archive files exist in any of the available data sources that contain compressed files of interest, this option allows you to open the archive files as part of the job and checks them against keywords supplied in the keyword filter.</td>
</tr>
<tr>
<td>Collect Responsive Archives</td>
<td>Collects the archive/container files (ZIP, RAR and so forth) of any responsive file when using the drill-down option.</td>
</tr>
<tr>
<td>Custom Drill Down Extensions</td>
<td>Allows you to specify the extension for the archive drill down. If you do not specify the extension, the default will be used.</td>
</tr>
<tr>
<td>Collect Non-Extension Files</td>
<td>Collect all files that do not have an extension.</td>
</tr>
<tr>
<td>Use Internal File Identification</td>
<td>Sees the software’s file identification when checking file extensions.</td>
</tr>
<tr>
<td>Collect Unsearchable Encrypted Files</td>
<td>Collects files that cannot be accessed to search for keyword filter criteria.</td>
</tr>
<tr>
<td>Enable PreScan</td>
<td>Will scan the collection target before collecting. Enables accurate completion percentage, file counts, and size predictions for Real Time Status screen.</td>
</tr>
</tbody>
</table>
Exchange

Upon selecting the required custodians and clicking on Save and Next from the Custodians section, you will be navigated to the Exchange section.

1. Select the required Exchange mailbox connectors from the list. Ensure the Connector Type is appropriately selected. Exchange Admin Center (EAC), Exchange Web Services (EWS), Export API, and Graph API options will be listed in the drop-down list if configured.

   **Note:** You can filter the files from the data source by using the Include/Exclude filters.

2. Select additional collection options if required. Applicable to EWS/Graph API collections only.

<table>
<thead>
<tr>
<th>Collection Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Include Recoverable Deletes</td>
<td>Allows you to collect deletions. Deletions are enabled by default in Exchange. There’s no need to specify a folder path because there is no folder structure retained for those items.</td>
</tr>
<tr>
<td>Include Recoverable Purges</td>
<td>Allows you to collect purges (hard deletes) of data. In order to collect purges from an Exchange server, enable purges in the Exchange server. There is no need to specify a folder path because there is no folder structure retained for those items.</td>
</tr>
<tr>
<td>Collection Option</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Include Recoverable Versions</td>
<td>Allows you to collect versions of data that have been saved. In order to collect versions from an Exchange server, enable versions in the Exchange server. There is no need to specify a folder path because there is no folder structure retained for those items.</td>
</tr>
<tr>
<td>Include Archive MailBox</td>
<td>Allows you to collect from an archive mailbox.</td>
</tr>
</tbody>
</table>

3. Provide the required folder’s name in the **Mailbox Folder Path(s)** field to collect the data present in the folder.

**Note:** You can also provide multiple folder names separated with commas (,) to collect the data present in all the specified folders.

4. Click **Save and Next**.
Gmail

Upon selecting the required custodians and clicking on **Save and Next** from the **Custodians** section, you will be navigated to the **Gmail** section.

1. Select the required Gmail mailbox connectors from the list.

   **Note:** You can filter the files from the data source by using the Include/Exclude filters.

2. Click **Save and Next**.
OneDrive
Upon selecting the required custodians and clicking on **Save and Next** from the **Custodians** section, you will be navigated to the **OneDrive** section.

1. Select the required OneDrive connectors from the list.

   **Note:** You can filter the files from the data source by using the Include/Exclude filters.

2. Click **Save and Next**.
Google Drive
Upon selecting the required custodians and clicking on **Save and Next** from the **Custodians** section, you will be navigated to the **Google Drive** section.

1. Select the required Google Drive connectors from the list.

   **Note:** You can filter the files from the data source by using the Include/Exclude filters.

2. Click **Save and Next**.
Box

Upon selecting the required custodians and clicking on **Save and Next** from the **Custodians** section, you will be navigated to the **Box** section.

1. Select the required Box connectors from the list.

   **Note:** You can filter the files from the data source by using the Include/Exclude filters.

2. Click **Save and Next**.
Data Sources

To configure the data sources for collection:
Upon selecting the required options for Data Sources field, any or all of the following data source are to be configured:

Note: Ensure the Creating Collections Section has been reviewed before attempting a Data Source collection.

Additionally, if attempting a collection of GCC environment, refer to the Office 365 Credentials section.
Computers

*Auto Deploy Agents*

The Auto Deploy option will be applicable only when the Computer is selected in the target options, either against the Custodians or Data Sources.

<table>
<thead>
<tr>
<th>Target Options</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Custom</strong></td>
</tr>
<tr>
<td><strong>Custodians</strong></td>
</tr>
<tr>
<td><strong>Select Person's Computers</strong></td>
</tr>
<tr>
<td>Select Person's Shares</td>
</tr>
<tr>
<td>Select Person's Exchange</td>
</tr>
<tr>
<td>Select Person's Gmail</td>
</tr>
<tr>
<td>Select Person's OneDrive</td>
</tr>
<tr>
<td>Select Person's Google Drive</td>
</tr>
</tbody>
</table>

(OR)

<table>
<thead>
<tr>
<th>Target Options</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Custom</strong></td>
</tr>
<tr>
<td><strong>Custodians</strong></td>
</tr>
<tr>
<td><strong>Computers</strong></td>
</tr>
<tr>
<td>Network Shares</td>
</tr>
<tr>
<td>SharePoint</td>
</tr>
<tr>
<td>Microsoft Teams</td>
</tr>
<tr>
<td>Slack</td>
</tr>
</tbody>
</table>
1. And upon enabling the **Auto Deploy Agents** checkbox and clicking on **Save and Next**, the below **Agent Operations** section will be displayed.

On the Agent Operations page, select from the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Uninstall</td>
<td>Select to remove the agent from the machine</td>
</tr>
<tr>
<td>Install</td>
<td>Select to push the agent to the machine. Remember that the agent install may cause the machine to restart without a warning.</td>
</tr>
<tr>
<td>Make Public Instance</td>
<td>Configure the agent to check a public instance after the agent is installed.</td>
</tr>
<tr>
<td>Configure Periodic Check-In</td>
<td>Configure the agent to communicate back to the server.</td>
</tr>
<tr>
<td>Agent Type – Local Storage</td>
<td>Agent uses local files for configuration and data. Agent is installed (persists after reboot).</td>
</tr>
<tr>
<td>Use Site Server Default Port</td>
<td>Enabling this will force the agent to use Port:54545</td>
</tr>
<tr>
<td>Use Custom Port</td>
<td>Enter the port designated to communicate with the agent.</td>
</tr>
<tr>
<td>Service Name</td>
<td>Enter the name that you want the agent to be displayed as.</td>
</tr>
<tr>
<td>Executable Name</td>
<td>Enter the name of the file that is being run.</td>
</tr>
</tbody>
</table>

Upon selecting the required agent operations and clicking on Save and Next, you will be navigated to the **Custodians** section.

(OR)
If the **Agent Deploy** option is not selected in the **Collection Options** section, the Agent Operations section will be skipped and you will be navigated to the **Custodians** section.

Upon selecting the required options for **Data Sources** field and clicking on **Save and Next** from the **Collection Options** section, you will be navigated to the **Computers** section.

3. **Select the required computers from the list.**

   **Warning**: You cannot proceed to collect all the data from the computer. You must include at least one among the Extension, Size, Date, Path, Luhn, Keyword, or MD5 Hash filter properties within the Include/Exclude filters to perform a targeted collection.

4. **Click **Save and Next**.
**Advanced Filter Options**

You can configure the **Advanced Filters** section in the right pane to filter and collect only the required information based on the type of Collection. The applicable filters for the collection types are listed below:

i. For Filtered Collection:

<table>
<thead>
<tr>
<th>Source Type</th>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>File System</strong></td>
<td></td>
<td>To collect the drives from the target’s file system.</td>
</tr>
<tr>
<td><strong>Logical Disk</strong></td>
<td></td>
<td>To collect only the target’s logical drive space.</td>
</tr>
<tr>
<td><strong>Physical Disk</strong></td>
<td></td>
<td>To collect the target’s entire physical drive.</td>
</tr>
<tr>
<td><strong>Siteserver</strong></td>
<td></td>
<td>To search using the Site Server.</td>
</tr>
<tr>
<td><strong>Agent &amp;</strong></td>
<td><strong>Siteserver</strong></td>
<td>To search first with the agent and then with the Site Server.</td>
</tr>
<tr>
<td><strong>Agent</strong></td>
<td></td>
<td>To search files using the agent.</td>
</tr>
<tr>
<td><strong>Collect System</strong></td>
<td><strong>Files</strong></td>
<td>To search system files that are normally hidden from view. Files with “$” contain system meta data and in NTFS, the $MFT contains the file system pointers to all files.</td>
</tr>
<tr>
<td><strong>Scan Deleted</strong></td>
<td><strong>Files</strong></td>
<td>To scan free space of a partition for files matching the filter criteria.</td>
</tr>
<tr>
<td><strong>Scan Unused</strong></td>
<td><strong>Disk Area</strong></td>
<td>To scan unallocated disk space for files matching filter criteria.</td>
</tr>
<tr>
<td><strong>Archive Drill</strong></td>
<td><strong>Down</strong></td>
<td>If archive files exist in any of the available data sources that contain compressed files of interest, this option lets you open the archive files as part of the job and checks them against keywords supplied in the keyword filter.</td>
</tr>
<tr>
<td><strong>Collect</strong></td>
<td><strong>Responsive</strong></td>
<td><strong>Archives</strong> Collects any archive that contains files that match filter criteria.</td>
</tr>
</tbody>
</table>

---

*Reviewing Cases* | 373
<table>
<thead>
<tr>
<th>Type</th>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Custom Drill Down Extensions</td>
<td>Allows you to specify the extension for the archive drill down. If you do not specify the extension, the default will be used.</td>
</tr>
<tr>
<td></td>
<td>Include Deleted Files</td>
<td>To scan the free space of a partition for files matching the filter criteria.</td>
</tr>
<tr>
<td></td>
<td>Use Internal File Identification</td>
<td>To view the software’s file identification when checking file extensions.</td>
</tr>
<tr>
<td></td>
<td>Collect Non-Extension Files</td>
<td>Collects all files that do not have an extension.</td>
</tr>
<tr>
<td></td>
<td>Collect Unsearchable Encrypted Files</td>
<td>Collects files that cannot be accessed via search by keyword filter criteria.</td>
</tr>
<tr>
<td></td>
<td>Enable PreScan</td>
<td>Will scan the collection target before collecting. Enables accurate completion percentage, file counts, and size predictions for Real Time Status screen.</td>
</tr>
<tr>
<td></td>
<td>Parse $130 INDX Records</td>
<td>Parses $130 INDX Records.</td>
</tr>
<tr>
<td></td>
<td>Exclude Removable Drives/Media</td>
<td>Excludes removable drives that are recognized by Site Server from the collection. This option is only available for collection jobs. Not all removable drives are recognized as such so this option may not exclude ALL removable drives</td>
</tr>
</tbody>
</table>

**Note:** $I30 INDX records are the names given to NTFS MFT attributes containing file name indexes for directories.

---

**ii. For Full Disk Acquisition:**

A Full Disk Acquisition job would collect the entire contents of a computer’s hard drive, so the advanced options will
include fewer choices as listed below:

- **Collect from Target Options**
  - **Logical Disk**: To collect only the target’s logical drive space.
  - **Physical Disk**: To collect the target’s entire physical drive. You can choose the sectors required.

- **Use Redirected Acquisition**: Uses the agent to push the collected data directly to the Job Data path given in the Job Options screen instead of moving it to the temporary storage location and then to the Job Data path.

**Batching Options**

While multiple collections can run simultaneously, Batching Options allow jobs to run in groups. I.e. A selection of 3 Maximum Concurrent Agents will only allow 3 concurrent jobs to be run at once until finished, which would then allow the next batch of jobs to be started.

![Batching options](image)
Network Shares
Upon selecting the required options for **Data Sources** field and clicking on **Save and Next** from the **Collection Options** section, you will be navigated to the **Network Shares** section.

1. Select the required network share locations from the list.

   **Note:** You can filter the files from the data source by using the Include/Exclude filters.

2. Click **Save and Next**.
**Advanced Filter Options**
You can configure the **Advanced Filters** section in the right pane to filter and collect only the required information based on the below provided filters options:

<table>
<thead>
<tr>
<th>Filter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collect System Files</td>
<td>To search system files that are normally hidden from view. Files with “$” contain system meta data and in NTFS, the $MFT contains the file system pointers to all files.</td>
</tr>
<tr>
<td>Archive Drill Down</td>
<td>If archive files exist in any of the available data sources that contain compressed files of interest, this option allows you to open the archive files as part of the job and checks them against keywords supplied in the keyword filter.</td>
</tr>
<tr>
<td>Collect Responsive Archives</td>
<td>Collects the archive/container files (ZIP, RAR and so forth) of any responsive file when using the drill-down option.</td>
</tr>
<tr>
<td>Custom Drill Down Extensions</td>
<td>Allows you to specify the extension for the archive drill down. If you do not specify the extension, the default will be used.</td>
</tr>
<tr>
<td>Collect Non-Extension Files</td>
<td>Collect all files that do not have an extension.</td>
</tr>
<tr>
<td>Use Internal File Identification</td>
<td>Sees the software’s file identification when checking file extensions.</td>
</tr>
<tr>
<td>Collect Unsearchable Encrypted Files</td>
<td>Collects files that cannot be accessed to search for keyword filter criteria.</td>
</tr>
<tr>
<td>Enable PreScan</td>
<td>Will scan the collection target before collecting. Enables accurate completion percentage, file counts, and size predictions for Real Time Status screen.</td>
</tr>
</tbody>
</table>
SharePoint

Upon selecting the required options for **Data Sources** field and clicking on **Save and Next** from the **Collection Options** section, you will be navigated to the **SharePoint** section.

1. Select the required SharePoint locations from the list.

   **Note:** You can filter the files from the data source by using the Include/Exclude filters.

2. Click **Save and Next**.
Microsoft Teams

Upon selecting the required options for **Data Sources** field and clicking on **Save and Next** from the **Collection Options** section, you will be navigated to the **Microsoft Teams** section.

1. Select the required Microsoft Teams accounts from the list.

   **Note:** You can filter the files from the data source by using the Include/Exclude filters.

2. Click **Save and Next**.
Slack

Upon selecting the required options for Data Sources field and clicking on Save and Next from the Collection Options section, you will be navigated to the Slack section.

1. Select the required Slack accounts from the list.

   **Note:** You can filter the files from the data source by using the Include/Exclude filters.

2. Click Save and Next.
Collection Filters for Data Sources

To configure the collection filters for data sources:

Filter behaviors

The following are the fundamentals of using filters:

• When writing queries for the Keyword(s) field, use the terms AND or OR to help refine your search. For example:
  “Apple AND Oranges” will return only the files with both terms “apple” and “oranges”.

• In the extension field, you can use an asterisk (*) as a wildcard. For example, doc* which will include .DOC and .DOCX.

  Note: You can specify multiple extensions by separating with a comma.

• In the Path, you can include or exclude files based on folders/sub-folders in the share or on the computer. You can specify folders by doing the following:
  o Include or exclude a complete folder name. Example: \documents\my_Work_files\
  o Include or exclude a folder name using wildcards. e.g. *work*
  o Spaces within a folder name are allowed. e.g. shared files

  Note: You can specify multiple paths by separating with a comma.

• Multiple properties are treated with AND: When you add a filter, you can configure one or more properties within the filter and the properties are combined as an AND function. For example, if you add an inclusion filter, and in that one filter specify an extension of PDF and also a file size of greater than 2MB, the logic is “PDF” AND “>2MB”. The results will include only PDF files that have a file size greater than 2 MB.

• Multiple values in same property are treated with OR: When more than one values are provided for a same property, the values are treated with OR function. As another example, if you add an inclusion filter with two extensions “DOCX, XLSX” then the results will include both DOCX and XLSX files.

• Path always takes precedence: If you include a path as a property in a filter, any other properties specified in the same filter will only apply to the specified path. Suppose you target a network share \documents and you create an inclusion filter and specify the folder my_Work_files. Additionally, in the same filter you specify a file extension as PDF. In this example, only the PDF files in the my_Work_files folder is included.

• Inclusion and Exclusion filters are treated with AND: You can add both Inclusion filter and Exclusion filter to get the required data. For example, specify an Inclusion filter with extension as PDF and an Exclusion filter, file size greater than 3MB. The result will include only PDF files that are less than 3MB.
1. From the data source section, click **Include/Exclude**.
   - The **Apply Filter** prompt is displayed.

2. Provide a name for the filter in **Filter Name**.
3. Select if you want to **Include** or **Exclude** the filtered files by enabling the required option in the top right corner of the prompt.
4. Configure the required filters as instructed in **Filter Behaviors**.

   **Note:** You can enable the **Save Filter as Template** checkbox to save the configured filter as a template.

5. Click **Apply**.
Load Saved Filters

To load a saved filter:

1. From the required data source section, click **Load Saved Filter**.
   - The **Load Saved Filter** prompt is displayed.

   ![Load Saved Filter Prompt]

<table>
<thead>
<tr>
<th>Filter Name</th>
<th>Filter Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter 1</td>
<td>Include</td>
</tr>
<tr>
<td>Filter 2</td>
<td>Include</td>
</tr>
</tbody>
</table>

   ![Filter List]

**Note:** You can click on **Delete** against the required filter template to delete it.
2. Select the required filters.
3. Click **Submit**.
   - The selected filter will be applied to the data source.

![Filters Panel]

**Note:** You can click on **View**, **Edit**, or **Delete** to view, edit, or delete the filter.
Reviewing Cases

This part contains information about reviewing cases and contains the following chapters:

- Using the AD Enterprise Examiner Interface (page 388)
- Exploring Evidence (page 402)
- Examining Evidence in the Overview Tab (page 421)
- Examining Email (page 426)
- Examining Graphics (page 430)
- Examining Videos (page 445)
- Examining Miscellaneous Evidence (page 451)
- Bookmarking Evidence (page 498)
- Searching Evidence with Live Search (page 510)
- Searching Evidence with Index Search (page 521)
- Using the Known File Filter (KFF) (page 362)
- Using Project VIC (page 378)
- Viewing System Information (page 547)
- Using Visualization (page 562)
- Customizing the Examiner Interface (page 608)
- Working with Evidence Reports (page 618)
- Using the Sawmill Log Tab (page 636)
Chapter 21
Using the AD Enterprise Examiner Interface

About the Examiner
You can use the examiner to locate, organize, and export data. The Examiner interface contains tabs, each with a specific focus. Most tabs also contain a common toolbar and file list with customizable columns. Additional tabs can be user-defined. For example, you can use the following tabs to perform a specific task:

- The *Overview* tab lets you narrow your search to look through specific document types, or to look for items by status or file extension.
- The *Graphics* tab lets you quickly scan through thumbnails of the graphics in the case.
- The *Email* tab lets you view emails and attachments. As you find items of interest, you can do the following:
  - Create, assign, and view labels in a sorted file list view.
  - Use searches and filters to find relevant evidence.
  - Create bookmarks to easily group the items by topic or keyword, find those items again, and make the bookmarked items easy to add to reports.
  - Export files as necessary for password cracking or decryption, then add the decrypted files back as evidence.
  - Add external, supplemental files to bookmarks that are not otherwise part of the case.

Tabs of the Examiner

*Note:* When entering the Examiner and clicking on a tab for the first time, if that tab uses the Thumbnail pane memory is allocated for displaying graphics and video thumbnails if they are present in the case.
Tabs of the Examiner

<table>
<thead>
<tr>
<th>Tab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Explore</td>
<td>See Explorer Tree Pane (page 402)</td>
</tr>
<tr>
<td>Overview</td>
<td>See Using the Overview Tab (page 421)</td>
</tr>
<tr>
<td>Email Tab</td>
<td>See Using the Email Tab (page 426)</td>
</tr>
<tr>
<td>Graphics</td>
<td>See Using the Graphics Tab (page 430)</td>
</tr>
<tr>
<td>Video</td>
<td>See Examining Videos (page 445)</td>
</tr>
<tr>
<td>Internet/Chat</td>
<td>See Examining Internet Artifact Data (page 464)</td>
</tr>
<tr>
<td>Bookmarks</td>
<td>See Using the Bookmarks Tab (page 505)</td>
</tr>
<tr>
<td>Live Search</td>
<td>See Conducting a Live Search (page 510)</td>
</tr>
<tr>
<td>Index</td>
<td>See Conducting an Index Search (page 522)</td>
</tr>
<tr>
<td>System Information</td>
<td>See Viewing System Information (page 547)</td>
</tr>
<tr>
<td>Volatile</td>
<td>See Viewing System Information (page 547)</td>
</tr>
<tr>
<td>Mobile</td>
<td>See Examining Mobile Phone Data (page 471)</td>
</tr>
<tr>
<td>Volatile Tab</td>
<td>See Using the Volatile Tab (page 539)</td>
</tr>
<tr>
<td>Sawmill Tab (when installed)</td>
<td>See The Sawmill Log Tab (page 636)</td>
</tr>
</tbody>
</table>

Also, see Menus of the Examiner (page 390)

Miscellaneous types of evidence

See Examining Miscellaneous Evidence on page 451.

Creating Screen Captures in the Examiner

You can capture screen shots within the Examiner interface. You can include the screen captures when creating reports. You can use screen captures to include information that is not easy to export or include in reports.

See Adding Screen Captures from Examiner on page 628.
Menus of the Examiner

When a case is created and assigned a user, the Examiner window opens with the following menus:

Examiner Menus

<table>
<thead>
<tr>
<th>Menu</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>File</td>
<td>See Options of the Examiner File Menu (page 391)</td>
<td></td>
</tr>
<tr>
<td>Edit</td>
<td>See Options of the Examiner Edit Menu (page 392)</td>
<td></td>
</tr>
<tr>
<td>View</td>
<td>See Options of the Examiner View Menu (page 393)</td>
<td></td>
</tr>
<tr>
<td>Evidence</td>
<td>See Options of the Examiner Evidence Menu (page 395)</td>
<td></td>
</tr>
<tr>
<td>Filter</td>
<td>See Options of the Examiner Filter Menu (page 397)</td>
<td></td>
</tr>
<tr>
<td>Tools</td>
<td>See Options of the Examiner Tools Menu (page 398)</td>
<td></td>
</tr>
<tr>
<td>Manage</td>
<td>See Options of the Examiner Manage Menu (page 400)</td>
<td></td>
</tr>
<tr>
<td>Help</td>
<td>See Options of the Examiner Help Menu (page 401)</td>
<td></td>
</tr>
</tbody>
</table>
Options of the Examiner Filter Menu

Options of the Examiner File Menu

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Export</td>
<td>Exports selected files and associated evidence to a designated folder.</td>
</tr>
<tr>
<td>Export to Image</td>
<td>Exports one or more files as an AD1 image to a storage destination.</td>
</tr>
<tr>
<td></td>
<td>When exporting to AD1 the image's file path is added under a root directory. This speeds the process of gathering data for the AD1, and for shortening the path to AD1 content.</td>
</tr>
<tr>
<td>Export File List Info</td>
<td>Exports selected file information to files formatted as the Column List in CSV, TSV, and TXT formats.</td>
</tr>
<tr>
<td>Export Word List</td>
<td>Exports the words from the cases index as a text file. You can use this word list to create a dictionary in the AccessData PRTK and DNA products.</td>
</tr>
<tr>
<td></td>
<td>See Exporting a Word List (page 297)</td>
</tr>
<tr>
<td>Create Portable Case</td>
<td>Exports case data for “offline” review in FTK Plus Offline interface.</td>
</tr>
<tr>
<td></td>
<td>See Reviewing Portable Case Data in FTK Plus (page 496)</td>
</tr>
<tr>
<td>Report</td>
<td>Opens the Report Options dialog for creating a case report.</td>
</tr>
<tr>
<td></td>
<td>See Creating a Case Report (page 619)</td>
</tr>
<tr>
<td>Timeline Report</td>
<td>Opens the Timeline Report dialog for creating a Timeline bookmark report.</td>
</tr>
<tr>
<td>Volatile Data Report</td>
<td>Opens a Volatile Data Report created from live data collected remotely and added to this case. This option is grayed out unless Volatile Data has been added to the case.</td>
</tr>
<tr>
<td>Job Summary Report</td>
<td>Opens an Evidence History.log report showing a job summary for all processing done within the case.</td>
</tr>
<tr>
<td>Export Event Audit Log...</td>
<td></td>
</tr>
<tr>
<td>Close</td>
<td>Closes the Examiner and returns to the Case Manager window.</td>
</tr>
<tr>
<td>Exit</td>
<td>Closes both the Examiner and Case Manager windows.</td>
</tr>
</tbody>
</table>
## Options of the Examiner Filter Menu

## Options of the Examiner Edit Menu

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Copy Special</td>
<td>Duplicates information about the object copied as well as the object itself, and places the copy in the clipboard. See Copying Information from the Examiner (page 288)</td>
</tr>
</tbody>
</table>

## Options of the Examiner View Menu

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Refresh</td>
<td>Reloads the current view with the latest information.</td>
</tr>
<tr>
<td>Filter Bar</td>
<td>Inserts the filter toolbar into the current tab. These features are also available from the Filter menu.</td>
</tr>
<tr>
<td>Time Zone Display</td>
<td>Opens the Time Zone Display dialog.</td>
</tr>
<tr>
<td>Thumbnail Size</td>
<td>Selects the size of the thumbnails displayed from the Graphics tab. Select from the following:</td>
</tr>
<tr>
<td></td>
<td>• Extra Large - default</td>
</tr>
<tr>
<td></td>
<td>• Large-default</td>
</tr>
<tr>
<td></td>
<td>• Medium</td>
</tr>
<tr>
<td></td>
<td>• Small</td>
</tr>
<tr>
<td>Tab Layout</td>
<td>Manages tab settings. The user can lock an existing setting, add and remove settings, and save settings one tab at a time or all at once. The user can also restore previous settings or reset them to the default settings. These options are in the following list:</td>
</tr>
<tr>
<td></td>
<td>• Save</td>
</tr>
<tr>
<td></td>
<td>• Restore</td>
</tr>
<tr>
<td></td>
<td>• Reset to Default</td>
</tr>
<tr>
<td></td>
<td>• Remove</td>
</tr>
<tr>
<td></td>
<td>• Save All Tab Layouts</td>
</tr>
<tr>
<td></td>
<td>• Lock Panes</td>
</tr>
<tr>
<td></td>
<td>• Add New Tab Layout</td>
</tr>
</tbody>
</table>
## Options of the Examiner Filter Menu

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>File List Columns</strong></td>
<td>Specifies how to treat the file list column setting for the currently active tab. See Managing Columns (page 613) for more information. Options are:</td>
</tr>
<tr>
<td></td>
<td>• Save As Case Default</td>
</tr>
<tr>
<td></td>
<td>• Save All as Case Default</td>
</tr>
<tr>
<td></td>
<td>• Save As Global Default</td>
</tr>
<tr>
<td></td>
<td>• Save All as Global Default</td>
</tr>
<tr>
<td></td>
<td>• Reset to Factory Default</td>
</tr>
<tr>
<td></td>
<td>• Reset All To Factory Default</td>
</tr>
<tr>
<td><strong>File Content Tabs</strong></td>
<td>Specifies the behavior of file content when a different tab is selected. Options are:</td>
</tr>
<tr>
<td><strong>Switching</strong></td>
<td>• Auto</td>
</tr>
<tr>
<td></td>
<td>• Manual</td>
</tr>
<tr>
<td><strong>Explore Tree</strong></td>
<td>Displays the Explore Tree in the upper-left pane.</td>
</tr>
<tr>
<td><strong>Graphics Tree</strong></td>
<td>Displays the Graphics Tree in the upper-left pane.</td>
</tr>
<tr>
<td><strong>Overview Tree</strong></td>
<td>Displays the Overview Tree in the upper-left pane.</td>
</tr>
<tr>
<td><strong>Email Tree</strong></td>
<td>Displays the Email Tree in the upper-left pane.</td>
</tr>
<tr>
<td><strong>Bookmark Tree</strong></td>
<td>Displays the Bookmark Tree in the upper-left pane.</td>
</tr>
<tr>
<td><strong>Index Searches</strong></td>
<td>Displays the Index Search Results pane in the upper-left pane.</td>
</tr>
<tr>
<td><strong>Live Searches</strong></td>
<td>Displays the Live Search Results pane in the upper-left pane.</td>
</tr>
<tr>
<td><strong>Bookmark Information</strong></td>
<td>Adds the Bookmark Information pane into the current tab.</td>
</tr>
<tr>
<td><strong>File List</strong></td>
<td>Adds the File List pane into the current tab.</td>
</tr>
<tr>
<td><strong>File Content</strong></td>
<td>Adds the File Content pane into the current tab.</td>
</tr>
<tr>
<td><strong>Email Attachments</strong></td>
<td>Displays the attachments to email objects found in the case. Available only in the Email and Overview tabs.</td>
</tr>
<tr>
<td><strong>Email Conversation</strong></td>
<td>Displays the Email Conversation pane.</td>
</tr>
<tr>
<td><strong>Properties</strong></td>
<td>Inserts the Object Properties pane into the current tab view.</td>
</tr>
<tr>
<td><strong>Hex Value Interpreter</strong></td>
<td>Displays a pane that provides an interpretation of Hex values selected from the Hex View pane.</td>
</tr>
<tr>
<td><strong>Thumbnails</strong></td>
<td>Displays a pane containing thumbnails of all graphics found in the case.</td>
</tr>
<tr>
<td><strong>Video View</strong></td>
<td>Displays a pane containing thumbnails of all videos found in the case.</td>
</tr>
<tr>
<td><strong>Tasks</strong></td>
<td>Views the Tasks list.</td>
</tr>
<tr>
<td></td>
<td>See Creating and Using Tasks on page 123.</td>
</tr>
<tr>
<td><strong>Create Task</strong></td>
<td>Creates a new Task.</td>
</tr>
<tr>
<td></td>
<td>See Creating and Using Tasks on page 123.</td>
</tr>
</tbody>
</table>
Options of the Examiner Filter Menu

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Show Bounding Box Images</td>
<td>None - Disables bounding box display</td>
</tr>
<tr>
<td></td>
<td>Facial - Displays bounding boxes for images that have been processed for facial recognition.</td>
</tr>
<tr>
<td></td>
<td>Image Items - Displays bounding boxes for graphic images that have been processed for image recognition.</td>
</tr>
<tr>
<td>Progress Window</td>
<td>Opens the Progress dialog, from which you can monitor tasks and/or cancel them.</td>
</tr>
</tbody>
</table>

Options of the Examiner Evidence Menu

**Options of the Examiner Evidence Menu**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add/Remove</td>
<td>Opens the Manage Evidence dialog, used to add and remove evidence. From Manage Evidence, choose from the following:</td>
</tr>
<tr>
<td></td>
<td>Time Zone — Choose Time Zone for evidence item Refinement</td>
</tr>
<tr>
<td></td>
<td>Options — Select Evidence Refinement Options</td>
</tr>
<tr>
<td></td>
<td>Language Setting — Choose the language of the evidence item</td>
</tr>
<tr>
<td></td>
<td>Define and Manage Evidence Groups</td>
</tr>
<tr>
<td></td>
<td>Select Case KFF Options</td>
</tr>
<tr>
<td>Add Remote Data</td>
<td>Opens the Add Remote Data dialog from which you can remotely access volatile, memory, and/or drive data and add it to the case. To Collect remote data from another computer on the network, provide the following:</td>
</tr>
<tr>
<td></td>
<td>Remote IP Address</td>
</tr>
<tr>
<td></td>
<td>Remote Port</td>
</tr>
<tr>
<td></td>
<td>Select any or all of the following:</td>
</tr>
<tr>
<td></td>
<td>Physical Drives (Can be mapped using RDMS) Logical Drives (Can be mapped using RDMS) Memory Analysis</td>
</tr>
<tr>
<td></td>
<td>Click OK or Cancel.</td>
</tr>
<tr>
<td>Add Remote Mac Data...</td>
<td>Launches the Mac Agent Collection interface.</td>
</tr>
<tr>
<td></td>
<td>See Acquiring Remote Data from macOS Managed Agents (page 196)</td>
</tr>
<tr>
<td>Add Off-Network/Cloud Data...</td>
<td>Launches the web-based Site Server collections interface.</td>
</tr>
<tr>
<td></td>
<td>Site Server Data Collections (page 201)</td>
</tr>
</tbody>
</table>
### Options of the Examiner Filter Menu

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Additional Analysis</td>
<td>Opens the Additional Analysis dialog with many of the same processing options available when the evidence was added. Allows the user to reprocess using available options not selected previously.</td>
</tr>
<tr>
<td></td>
<td>See Using Additional Analysis (page 147).</td>
</tr>
<tr>
<td>Process Manually Carved Items</td>
<td>Initiates the processing of items that have been manually carved, using the selected options.</td>
</tr>
<tr>
<td>Manage Evidence Groups</td>
<td>Opens the dialog where you can create and manage Evidence Groups.</td>
</tr>
<tr>
<td>Import Memory Dump</td>
<td>Opens the Import Memory Dump File dialog which allows you to select memory dumps from other case files or remote data acquisitions, and import them into the current case. The memory dump file must have been previously created.</td>
</tr>
<tr>
<td></td>
<td>See Working with Live Evidence (page 169)</td>
</tr>
<tr>
<td>Import Custom Column File</td>
<td>When a Custom Column Settings file has been created, import it into your case using this tool.</td>
</tr>
<tr>
<td>Delete Custom Column Data</td>
<td>If you have imported or created a Custom Column Settings file, use this tool to delete the associated column and its data from the view.</td>
</tr>
<tr>
<td>Merge Case Index</td>
<td>The processing engine does this automatically and no longer needs user interaction to select the merge.</td>
</tr>
<tr>
<td>Manage Processing</td>
<td>Opens the Manage Evidence Processing Processes dialog.</td>
</tr>
</tbody>
</table>
## Options of the Examiner Filter Menu

### Options of the Examiner Filter Menu

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New</td>
<td>Opens the <em>Filter Definition</em> dialog to define a temporary filter.</td>
</tr>
<tr>
<td>Duplicate</td>
<td>Duplicates a selected filter. A duplicated filter serves as a starting point for customizing a new filter.</td>
</tr>
<tr>
<td>Delete</td>
<td>Deletes a selected filter.</td>
</tr>
<tr>
<td>On</td>
<td>Applies the selected filter globally in the application. The File List changes color to indicate that the filter is applied.</td>
</tr>
<tr>
<td>Import</td>
<td>Opens the Windows file manager allowing the user to import a pre-existing filter.</td>
</tr>
<tr>
<td>Export</td>
<td>Opens the Windows File Manager allowing the user to save a filter. The name of the filter cannot have any special or invalid characters or the export will not work.</td>
</tr>
<tr>
<td>Tab Filter</td>
<td>Allows the selection of a filter to apply in the current tab.</td>
</tr>
</tbody>
</table>
### Options of the Examiner Tools Menu

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Decrypt Files</td>
<td>Decrypts EFS and Office files using passwords you enter.</td>
</tr>
<tr>
<td></td>
<td>See <a href="#">Decryption</a> (page 265)</td>
</tr>
<tr>
<td>Dell Encryption Decryption</td>
<td>Opens the <em>Dell Encryption Decryption</em> dialog where you enter the decryption information.</td>
</tr>
<tr>
<td></td>
<td>See [Decrypting Dell Encryption Files (Dell Data Protection</td>
</tr>
<tr>
<td>Send to DNA/PRTK for password recovery</td>
<td>Uses the integrated DNA/PRTK capabilities to decrypt several types of encrypted files.</td>
</tr>
<tr>
<td></td>
<td>See <a href="#">Recovering Passwords using the PRTK/DNA Integrated Tool</a> on page 272.</td>
</tr>
<tr>
<td>Verify Image Integrity</td>
<td>Generates hash values of the disk image file for comparison.</td>
</tr>
<tr>
<td></td>
<td>See <a href="#">Verifying Drive Image Integrity</a> (page 129)</td>
</tr>
<tr>
<td>Restore Image to Disk</td>
<td>Restores a physical image to a disk. If the original drive was on a bootable partition, the restored image may also be bootable. This feature is disabled for Case Reviewers.</td>
</tr>
<tr>
<td>Mount Image to Drive</td>
<td>Allows the mounting of a physical or logical image for read-only viewing. Logically mounting images allows them to be viewed as a drive-letter in Windows Explorer. Mounted logical drives now show the user the correct file, even when a deleted file with the same name exists in the same directory.</td>
</tr>
<tr>
<td></td>
<td>See <a href="#">Mounting an Image to a Drive</a> (page 130)</td>
</tr>
<tr>
<td>Disk Viewer</td>
<td>Opens a hex viewer that allows you to see and search contents of evidence items.</td>
</tr>
<tr>
<td></td>
<td>Search Text for a term using Match Case, ANSI, Unicode, Regular Expression or Search Up instead of down; Search Hex using Search Up. Specify a logical sector or a cluster.</td>
</tr>
<tr>
<td>Other Applications</td>
<td>Opens other AccessData tools to complement the investigational analysis.</td>
</tr>
<tr>
<td>Configure Agent Push</td>
<td>Opens configuration dialog for pushing the agent to remote machines for data acquisition.</td>
</tr>
<tr>
<td>Push Agents</td>
<td>Push, or install, an Agent to a remote machine. You can Add, Remove, Import, or Export a single machine or a list of machines here.</td>
</tr>
<tr>
<td>Batch Remediation</td>
<td>Opens the <em>Batch Remediation</em> dialog for performing tasks such as wiping files, killing processes, executing commands and updating proxies.</td>
</tr>
<tr>
<td>Manage Remote Acquisition</td>
<td>Opens the <em>Remote Acquisition</em> dialog. Set the drive acquisition retry options here to set compression levels, balance speed of transfers with the amount of bandwidth usage, and set compression levels for remote data transfers.</td>
</tr>
</tbody>
</table>

---

### Options of the Examiner Tools Menu (Continued)
<table>
<thead>
<tr>
<th><strong>Option</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Sawmill</td>
<td>Configure Sawmill usage or remove it from the Enterprise Examiner system. Sawmill is a third-party program for logging activity. See Using the Sawmill Log Tab on page 636.</td>
</tr>
<tr>
<td>Unmount Agent Drive</td>
<td>Unmount a remote drive that is mounted through RDMS.</td>
</tr>
<tr>
<td>Recover Processing Jobs</td>
<td>Restarts processing so jobs that were interrupted can be completed.</td>
</tr>
<tr>
<td>Visualization</td>
<td>Lets you launch the Visualization add on module for the data that you currently have displayed in the File List Pane. Visualization is only available from the Explore, Overview, and Email Tabs. See Using Visualization on page 562.</td>
</tr>
<tr>
<td>Execute SQL</td>
<td>Executes a user-defined SQL script from within the interface.</td>
</tr>
<tr>
<td>Select Audit Events</td>
<td>Opens the Audit Events dialog where you can choose from several events to audit.</td>
</tr>
<tr>
<td>Run Python Script</td>
<td>Allows you to run any Python script on selected evidence files within a case. See Python Scripting on page 489.</td>
</tr>
<tr>
<td>Image Analysis</td>
<td>Multiple tools to perform A.I. assisted image recognition and facial recognition. See Image Analysis on page 439.</td>
</tr>
<tr>
<td>Enhanced Internet Artifact Analysis</td>
<td>Deep scans browser archives and their corresponding artifacts. See Using the Enhanced Internet Artifact Parser on page 464.</td>
</tr>
<tr>
<td>Run Abbyy OCR Processing</td>
<td>3rd party integrated OCR engine (optional add-on)</td>
</tr>
<tr>
<td></td>
<td>See To Run ABBYY OCR Processing on page 103.</td>
</tr>
</tbody>
</table>
Options of the Examiner Help Menu

Options of the Examiner Manage Menu

<table>
<thead>
<tr>
<th>Tool Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>KFF</td>
<td>Manage Known File Filter (KFF) Library, sets, and groups.</td>
</tr>
<tr>
<td></td>
<td>See Using the Known File Filter (KFF) (page 362).</td>
</tr>
<tr>
<td>Labels</td>
<td>Manage Local and Shared Labels as well as Label Groups.</td>
</tr>
<tr>
<td></td>
<td>See What You Can Do With Labels (page 261).</td>
</tr>
<tr>
<td>Carvers</td>
<td>Manage Local and Shared Custom Carvers.</td>
</tr>
<tr>
<td></td>
<td>See Data Carving (page 99).</td>
</tr>
<tr>
<td>Filters</td>
<td>Manage Local and Shared Filters.</td>
</tr>
<tr>
<td></td>
<td>See Filtering Data to Locate Evidence (page 241).</td>
</tr>
<tr>
<td>Columns</td>
<td>Manage Local and Shared Columns.</td>
</tr>
<tr>
<td></td>
<td>See Customizing File List Columns (page 613).</td>
</tr>
<tr>
<td>Indexed Search Term Weights</td>
<td>See Adjusting the Weighting Criteria for an Index Search Term on page 524.</td>
</tr>
</tbody>
</table>

Options of the Examiner Help Menu

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Case Folder</td>
<td>Opens the folder that contains the case data.</td>
</tr>
<tr>
<td>About</td>
<td>Provides version and build information, copyright and trademark information, and other copyright and trade acknowledgments.</td>
</tr>
</tbody>
</table>
Chapter 22
Exploring Evidence

The Explore tab displays all the contents of the case evidence files and drives as the original user would have seen them.

This chapter includes the following topics:

- Explorer Tree Pane (page 402)
- File List Pane (page 403)
- The File Content Viewer Pane (page 410)
- The Filter Toolbar (page 419)
- Using QuickPicks (page 420)

Explorer Tree Pane

Lists directory structure of each evidence item, similar to the way one would view directory structure in Windows Explorer. An evidence item is a physical drive, a logical drive or partition, or drive space not included in any partitioned drive, as well as any file, folder, or image of a drive, or mounted image.

The Explorer Tree Pane
File List Pane

About the File List

Displays case files and pertinent information about files, such as filename, file path, file type and many more properties as defined in the current filter. The files here may display in a variety of colors.

They are as follows:

- Black = Default
- Grey = Deleted
- Pink = Bookmarked or added to a task.

See Bookmarking Evidence on page 498. See on page 114.

- Red = Encrypted

See Identifying the Encrypted Files in a Case on page 269.

The File List view reflects the files available for the current tabbed view and the properties that meet selected Column templates, limited by any filters that may be applied. In this pane, you can choose which columns to display, as well as the order of those columns, create Bookmarks, create Labels, Copy or Export File Lists. The File List pane is included in all default tab views.

The File List Pane

![File List Pane Screenshot]
Customizing the Colors of the File List

It is possible to customize the colors in the File List. In the File List, lines have alternating colors for ease of use. It is possible to change both the odd and even lines in the list separately. Colors can be set for the following states:

**Customizable Color Options for the File List**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Entry</th>
</tr>
</thead>
<tbody>
<tr>
<td>Color</td>
<td>The color of the odd lines in a default state</td>
<td>&lt;BgColor&gt;255, 255, 255&lt;/BgColor&gt;</td>
</tr>
<tr>
<td>Alt Color</td>
<td>The color of the even lines in a default state</td>
<td>&lt;BgAltColor&gt;248, 248, 248&lt;/BgAltColor&gt;</td>
</tr>
<tr>
<td>Color Filtered</td>
<td>The color of a filtered item in an odd numbered line</td>
<td>&lt;BgColor_Filtered&gt;255, 255, 200&lt;/BgColor_Filtered&gt;</td>
</tr>
<tr>
<td>Alt Color Filtered</td>
<td>The color of a filtered item in an even numbered line</td>
<td>&lt;BgAltColor_Filtered&gt;248, 248, 200&lt;/BgAltColor_Filtered&gt;</td>
</tr>
<tr>
<td>Color Quick Pick</td>
<td>The color applied to a quick pick item in an odd numbered line</td>
<td>&lt;BgColor_QuickPick&gt;248, 255, 248&lt;/BgColor_QuickPick&gt;</td>
</tr>
<tr>
<td>Alt Color Quick Pick</td>
<td>The color applied to a quick pick item in an even numbered line</td>
<td>&lt;BgAltColor_QuickPick&gt;228, 244, 228&lt;/BgAltColor_QuickPick&gt;</td>
</tr>
<tr>
<td>Alt Color Filtered Quick Pick</td>
<td>The color applied to a filtered quick pick item</td>
<td>&lt;BgAltColor_Filtered_QuickPick&gt;240, 248, 216&lt;/BgAltColor_Filtered_QuickPick&gt;</td>
</tr>
</tbody>
</table>

In order to change the colors, you must add the Entry value to the Preferences.xml file. The colors are based on RGB values, with the three numbers representing the Red, Green, Blue values in that order.

**Note:** If you need help knowing what values equal which colors, you can search for RGB values online to find the information you need. There are over 16 million color combinations, so they are not listed here.

The Entries listed in the table above, once added to the Preferences.xml file, will allow you to customize the colors in the File List.

**To customize the colors in the File List**
1. Navigate to the `Preferences.xml` file at the following path:

   `%ProgramData%\AccessData\Products\Forensic Toolkit\[x.x]\Preferences.xml`

2. Type the desired Entry line from the table above into the `Preferences.xml` file, replacing the default RGB value (shown) with your desired RGB value.

3. Save and close the `Preferences.xml` file and restart the program. The File List will now display the customized color(s).

**Using the File List’s Columns**

For each evidence item, you can display multiple columns of information about that item.

You can hover over a column’s short name to display a tooltip that shows a more descriptive column long name.

You can sort the list using any column. Click on a column heading in the File List view to sort on that column. Hold down the Shift key while clicking a different column header to make the newly selected column the primary-sorted column, while the previous primary-sorted column becomes the secondary-sorted column. There are only two levels of column sorting, primary and secondary. To undo a secondary sort, click on a different column header to make it the primary-sorted column.

Column widths in most view panes can be adjusted by hovering the cursor over the column heading borders, and dragging the column borders wider or narrower.

See **Customizing File List Columns** (page 613).

A data box displays in the lower-right of the File List View that indicates the total logical size of the currently listed files.
Using the File List’s Type-Down Control Feature

When you view data in the File List, use can use a type-down control feature to locate information. To use the type-down control feature, select any file in the file list and then type the first letters of a file. As you continue to type, the file selector moves to the file list to the closest match to what you type.

**Icons of the File List Tool Bar**

### File List Tool Bar

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="icon" alt="Check All" /></td>
<td>Checks all of the files in the current list.</td>
</tr>
<tr>
<td><img src="icon" alt="Uncheck All" /></td>
<td>Unchecks all of the files in the current list.</td>
</tr>
<tr>
<td><img src="icon" alt="Uncheck All" /></td>
<td>Unchecks all of the files in the current case.</td>
</tr>
<tr>
<td><img src="icon" alt="Create New Bookmark" /></td>
<td>Opens the <em>Create New Bookmark</em> dialog.</td>
</tr>
<tr>
<td><img src="icon" alt="Bookmark Color" /></td>
<td>Enables / disables bookmark color association.</td>
</tr>
<tr>
<td><img src="icon" alt="Manage Labels" /></td>
<td>Opens the <em>Manage Labels</em> dialog.</td>
</tr>
<tr>
<td><img src="icon" alt="Apply Label" /></td>
<td><strong>Apply Label</strong> drop-down allows you to select from the list of defined labels and apply it to a single selected file or a group of files as selected in the <strong>Apply Label To</strong> drop-down.</td>
</tr>
<tr>
<td><img src="icon" alt="Select Label Target" /></td>
<td><strong>Select Label Target</strong> drop-down allows you to specify currently Highlighted, Checked, or Listed files for the Label you choose from the <strong>Apply Label</strong> drop-down.</td>
</tr>
<tr>
<td><img src="icon" alt="Export File List" /></td>
<td><strong>Export File List</strong> lets you save selected files to another folder.</td>
</tr>
<tr>
<td><img src="icon" alt="Copy Special" /></td>
<td>Opens the <em>Copy Special</em> dialog.</td>
</tr>
<tr>
<td><img src="icon" alt="Column Settings" /></td>
<td>Opens the <em>Column Settings</em> dialog.</td>
</tr>
</tbody>
</table>
### File List Tool Bar (Continued)

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email</td>
<td><strong>Column Templates</strong>&lt;br&gt;Sets the columns to a specific selection from the list of defined column sets.&lt;br&gt;See Managing Columns on page 613. Some Default Column Templates are:&lt;br&gt;• Cerberus Results&lt;br&gt;  See Cerberus Columns on page 323.&lt;br&gt;• eDiscovery&lt;br&gt;• eDiscovery Mail&lt;br&gt;• Email&lt;br&gt;• Explicit Image Detection (EID)&lt;br&gt;• File Listing&lt;br&gt;• GeoEXIF, GeoIP, Geolocation - Shows Geolocation-related columns&lt;br&gt;  See Using Geolocation Columns in the Item List on page 604.&lt;br&gt;• Internet History&lt;br&gt;  See Examining Internet Artifact Data on page 464.&lt;br&gt;• Normal (default)&lt;br&gt;• Reports: File Path Section&lt;br&gt;• Reports: Standard&lt;br&gt;Displays the selected Time Zone from the local machine.</td>
</tr>
<tr>
<td></td>
<td>Opens the Heatmap page.&lt;br&gt;See Using Visualization Heatmap on page 595.</td>
</tr>
<tr>
<td></td>
<td>Opens the Geolocation page.&lt;br&gt;See Using Visualization Geolocation on page 597.</td>
</tr>
<tr>
<td></td>
<td>Opens the Visualization page.&lt;br&gt;See Using Visualization on page 562.</td>
</tr>
<tr>
<td></td>
<td>Leave query running when switching tabs (this may affect the performance of other tabs).</td>
</tr>
<tr>
<td></td>
<td>Cancel retrieving row data. This is not a pause button. To retrieve row data after clicking <strong>Cancel</strong>, you must begin again. There is no way to pause and restart the retrieval of row data.</td>
</tr>
<tr>
<td></td>
<td>Active spinner indicates Processing activity.</td>
</tr>
</tbody>
</table>
**Note:** When checking files in a case, these two rules apply:

- Checked files are persistent and remain checked until the user unchecks them.
- Checked files are per-user; another user or an Administrator will not see your checked files as checked when viewing the same case.

**File List View Right-Click Menu**

When you right-click on any item in the File List view, a menu with the following options appears. Some options are enabled or disabled, depending on the tab you are in, the evidence that exists in the case, the item you have selected, or whether bookmarks have been created.

**File List View Right-Click Menu Options**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open</td>
<td>Opens the selected file.</td>
</tr>
<tr>
<td>Launch in Content Viewer</td>
<td>Launches the file in the Content Viewer, formerly known as Detached Viewer.</td>
</tr>
<tr>
<td>Open With</td>
<td>Opens the file. Choose either Internet Explorer or an External Program.</td>
</tr>
<tr>
<td>Create Bookmark</td>
<td>Opens the Create New Bookmark dialog for creating a new bookmark. See Bookmarking Evidence on page 498.</td>
</tr>
<tr>
<td>Create Project VIC</td>
<td>See Using Project VIC on page 378.</td>
</tr>
<tr>
<td></td>
<td>Bookmark.</td>
</tr>
<tr>
<td>Add to Bookmark</td>
<td>Opens the Add to Bookmark dialog for adding selected files to an existing bookmark. See Bookmarking Evidence on page 498.</td>
</tr>
<tr>
<td>Remove from Bookmark</td>
<td>Removes a file from a bookmark. From the Bookmarks tab, open the bookmark containing the file to be removed, then select the file. Right-click and select Remove from Bookmark. See Bookmarking Evidence on page 498.</td>
</tr>
<tr>
<td>Labels</td>
<td>Opens the Labels dialog. View assigned Labels, create or delete a Label, Apply a Labels to file, or Manage Local or Manage Global Labels. See Working with Labels on page 261.</td>
</tr>
<tr>
<td>Review Labels</td>
<td>Opens the Label Information dialog to display all labels assigned to the selected file or files. See Working with Labels on page 261.</td>
</tr>
<tr>
<td>Mount Image to Drive</td>
<td>Allows you to mount an image logically to see it in Windows Explorer, or physically to view. See Mounting an Image to a Drive on page 130.</td>
</tr>
<tr>
<td>Add Decrypted File</td>
<td>Right-click and select <strong>Add Decrypted File</strong>. Opens the Add Decrypted File dialog. Browse to and select the file to add to the case, click <strong>Add</strong>.</td>
</tr>
<tr>
<td>--------------------</td>
<td>-------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>View File Sectors</td>
<td>Opens a hex view of the selected file. Type in the file sector to view and click <strong>GoTo</strong>.</td>
</tr>
<tr>
<td>Find on Disk</td>
<td>Opens the Disk Viewer and shows where the file is found in the disk/file structure. <strong>Note</strong>: Find on disk feature won’t find anything under 512 B physical size. Files smaller than 1500 bytes may reside in the MFT and do not have a start cluster. Find on disk depends on that to work.</td>
</tr>
<tr>
<td>Find Similar Files</td>
<td>Opens the <strong>Search for Similar Files</strong> dialog. The selected file’s hash value is displayed. Click <strong>From File</strong> to see the filename the hash is from. The Evidence Items to Search box shows all evidence items in the case. Mark which ones to include in the search. Select the Minimum Match Similarity you prefer, and click <strong>Search</strong> or <strong>Cancel</strong>.</td>
</tr>
<tr>
<td>Open in Registry Viewer</td>
<td>Opens a registry file in AccessData’s Registry Viewer. Choose SAM, SOFTWARE, SYSTEM, SECURITY, or NTUSER.dat.</td>
</tr>
<tr>
<td>Export</td>
<td>Opens the <strong>Export</strong> dialog with all options for file export, and a destination path selection. See <strong>Exporting Data from the Examiner</strong> on page 288.</td>
</tr>
<tr>
<td>Export to Image</td>
<td>Opens the <strong>Create Custom Content</strong> Image dialog. See <strong>Exporting Data from the Examiner</strong> on page 288.</td>
</tr>
<tr>
<td>Acquire to Disk Image</td>
<td>Allows you to create a new disk image (001, AFF, E01, or S01) from a disk image in the case.</td>
</tr>
<tr>
<td>Export File List Info</td>
<td>Opens the <strong>Save As</strong> dialog. Choose TXT, TSV, or CSV. The default name is FileList.TXT.</td>
</tr>
<tr>
<td>Copy Special</td>
<td>Opens the <strong>Copy Special</strong> dialog.</td>
</tr>
<tr>
<td>Check All Files in Current List</td>
<td>Check-marks all files in the current list.</td>
</tr>
<tr>
<td>Uncheck all Files in Current List</td>
<td>Unchecks all files in the current list.</td>
</tr>
<tr>
<td>Uncheck All Files in Case</td>
<td>Unchecks all files in the case.</td>
</tr>
<tr>
<td>Check/Uncheck All Highlighted</td>
<td>Checks or unchecks all files that are currently highlighted in the list. (Pressing the space bar does the same thing.)</td>
</tr>
<tr>
<td>Change “Flag as Ignorable” Status</td>
<td>Change Flag Status of all files as either Ignorable or Not Ignorable according to Selection Options.</td>
</tr>
<tr>
<td>Change “Flag as Privileged” Status</td>
<td>Change Flag Status of all files as either Privileged or Not Privileged according to Selection Options.</td>
</tr>
<tr>
<td>Re-assign File Category</td>
<td>Change File Category assignment.</td>
</tr>
<tr>
<td>View This Item In a Different List</td>
<td>Changes the File List view from the current tab to that of the selected tab from the pop-out.</td>
</tr>
</tbody>
</table>
The File Content Viewer Pane

Displays the contents of the currently selected file from the File List. The Viewer toolbar allows the choice of different view formats.

You can use CTRL+F to search within the File Content pane. The File Content pane tab offers a variety of tabs that enable the user to manipulate how the selected object's contents are to be displayed on the screen. Each of these tabs will be discussed in detail below.

Tabs of the File Content Pane

**Note:** The Find on Disk feature (in File List view, right-click an item) won't find anything under 512 Bytes physical size. Also, files smaller than 1500 bytes may reside in the MFT and thus do not have a start cluster. Find on Disk depends on the start cluster information to work.

**Note:** In the File List view of any tab, a much-greater-than symbol (>>>) denotes that the path is not an actual path, but that the file came from another file or source, such as a zipped, compressed, or linked (OLE) file, or that it was carved.
The File Content pane title changes depending on which tab is selected at the bottom of the window. The available tabs are File Content, Properties, and Hex Interpreter. These three tabs default to the bottom left of the File Content pane in any program tab where it is used. The three tabs can be re-ordered by clicking on a tab and dragging-and-dropping it to the position in the linear list where you want it. Click any of these tabs to switch between them. The information displayed applies to the currently selected file in the Viewer pane.

The Natural Tab

The Natural view tab attempts to emulate what a file might look like in its native application. This viewer uses INSO filters for viewing hundreds of file formats without the native application being installed.

File Content Pane: Natural Tab

![File Content Pane: Natural Tab Image]

**Note:** When highlighting terms in Natural View, each term throughout the document is highlighted, one term at a time. When it reaches the limit of highlighting in that window, regardless of which term it is on (first, second, third, etc.) it stops highlighting. There is no workaround.

**Note:** Viewing large items in their native applications may be faster than waiting for them to be rendered in the

*Examiner* viewer.

The Natural View top tab is the only one of the four that has additional tabs that provide for the viewing of Text, Media, and Web files, in their native application environment.
File Content Pane: Default, Media, and Web Tabs

- **Natural Tab: Default**

The Default tab displays documents or files in a viewer that uses INSO (Inside-Out) Technology, according to their file type.

- **Natural Tab: Media**

Case audio and video files play using an embedded Windows Media Player. The Examiner has the functionality to recognize popular mobile phone formats (found in many MPE images) such as M4A, MP4, AMR, and 3GP. These file types play inside the Media tab as long as the proper codecs are installed that would also allow those files to play in Windows Media Player.

- **Natural Tab: Web**

The Web view uses an embedded Internet Explorer instance to display the contents of the selected HTML file. In the Web view, the top-left border of the pane holds two toggle buttons for enabling or disabling HTML content.

- **Natural Tab: Web (HTML5)**

The Web (HTML5) view uses an embedded Internet Explorer instance to display the contents of the selected HTML file.
Enable or Disable CSS Formatting. CSS formatting displays any fonts, colors, and layout from cascading style sheets. HTML formatting not part of a cascading style sheet might remain. Enabled feature is indicated by a blue background; disabled feature is indicated by a gray background.

Enable or Disable External Hyperlinks. Enabled hyperlinks in the file will link to active internet pages. They may not accurately provide data that was available using that link at the time the image was made, or the evidence was acquired. Enabled feature is indicated by a blue background; disabled feature is indicated by a gray background.

The Properties Tab

The Properties tab is found in the File Content View, and displays a pane, or window of information about a selected file. The following figure displays the information contained in the Properties pane. This information corresponds to the file selected in the File List pane.

The Properties Tab
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The filename of the selected file.</td>
</tr>
<tr>
<td>Item Number</td>
<td>A number assigned to the item during evidence processing.</td>
</tr>
<tr>
<td>File Type</td>
<td>The type of a file, such as an HTML file or a Microsoft Word 98 document. The file header is used to identify each item's file type.</td>
</tr>
<tr>
<td>Path</td>
<td>The path from the evidence source down to the selected file.</td>
</tr>
<tr>
<td>General Info</td>
<td>General information about the selected file:</td>
</tr>
<tr>
<td></td>
<td><em>File Size:</em> Lists the size attributes of the selected file as follows:</td>
</tr>
<tr>
<td></td>
<td>- Physical size of the file, including file slack</td>
</tr>
<tr>
<td></td>
<td>- Logical size of the file, excluding file slack</td>
</tr>
<tr>
<td></td>
<td><em>File Dates:</em> Lists the Dates and Times of the following activities for that file on the imaged source:</td>
</tr>
<tr>
<td></td>
<td>- Created</td>
</tr>
<tr>
<td></td>
<td>- Last accessed</td>
</tr>
<tr>
<td></td>
<td>- Last modified</td>
</tr>
<tr>
<td></td>
<td>All dates with times are listed in UTC and local times.</td>
</tr>
<tr>
<td>File Attributes</td>
<td>The attributes of the file:</td>
</tr>
<tr>
<td></td>
<td>General:</td>
</tr>
<tr>
<td></td>
<td>- <em>Actual File:</em> True if an actual file. False if derived from an actual file.</td>
</tr>
<tr>
<td></td>
<td>- <em>From Recycle Bin:</em> True if the file was found in the Recycle Bin. False otherwise.</td>
</tr>
<tr>
<td></td>
<td>- <em>Start Cluster:</em> Start cluster of the file on the disk.</td>
</tr>
<tr>
<td></td>
<td>- <em>Compressed:</em> True if compressed. False otherwise.</td>
</tr>
<tr>
<td></td>
<td>- <em>Original Name:</em> Path and filename of the original file.</td>
</tr>
<tr>
<td></td>
<td>- <em>Start Sector:</em> Start sector of the file on the disk.</td>
</tr>
<tr>
<td></td>
<td>- <em>File has been examined for slack:</em> True if the file has been examined for slack. False otherwise.</td>
</tr>
<tr>
<td></td>
<td>DOS Attributes:</td>
</tr>
<tr>
<td></td>
<td>- <em>Hidden:</em> True if Hidden attribute was set on the file. False otherwise.</td>
</tr>
<tr>
<td></td>
<td>- <em>System:</em> True if this is a DOS system file. False otherwise.</td>
</tr>
<tr>
<td></td>
<td>- <em>Read Only:</em> True or False value.</td>
</tr>
<tr>
<td></td>
<td>- <em>Archive:</em> True if Read Only attribute was set on the file. False otherwise.</td>
</tr>
<tr>
<td></td>
<td>- <em>8.3 Name:</em> Name of the file in the DOS 8.3 naming convention, such as [filename.ext].</td>
</tr>
<tr>
<td></td>
<td><em>Verification Hashes:</em> True if verification hashes exist. False otherwise.</td>
</tr>
</tbody>
</table>

Exploring Evidence The File Content Viewer Pane | 411
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>NTFS Information:</strong></td>
<td></td>
</tr>
<tr>
<td>● <em>NTFS Record Number:</em> The number of the file in the NTFS MFT record.</td>
<td></td>
</tr>
<tr>
<td>● <em>Record Date:</em> UTC time and date record was last modified.</td>
<td></td>
</tr>
<tr>
<td>● <em>Resident:</em> True if the item was Resident, meaning it was stored in the MFT and the entire file fit in the available space. False otherwise. (If false, the file would be stored FAT fashion, and its record would be in the $I30 file in the folder where it was saved.)</td>
<td></td>
</tr>
<tr>
<td>● <em>Offline:</em> True or False value.</td>
<td></td>
</tr>
<tr>
<td>● <em>Sparse:</em> True or False value.</td>
<td></td>
</tr>
<tr>
<td>● <em>Temporary:</em> True if the item was a temporary file. False otherwise.</td>
<td></td>
</tr>
<tr>
<td>● <em>Owner SID:</em> The Windows-assigned security identifier of the owner of the object.</td>
<td></td>
</tr>
<tr>
<td>● <em>Owner Name:</em> Name of the owner of that file on the source system.</td>
<td></td>
</tr>
<tr>
<td>● <em>Group SID:</em> The Windows-assigned security identifier of the group that the owner of the object belongs to.</td>
<td></td>
</tr>
<tr>
<td>● <em>Group Name:</em> The name of the group the owner of the file belongs to.</td>
<td></td>
</tr>
<tr>
<td><strong>NTFS ACL attributes. This is the same functionality that is currently found in Imager. When there are multiple sets of ACL attributes present, they are now distinguished by number.</strong></td>
<td></td>
</tr>
<tr>
<td><strong>File Content Info</strong></td>
<td>The content information and verification information of the file.</td>
</tr>
<tr>
<td>● <em>MD5 Hash:</em> The MD5 (16 bytes) hash of the file (default).</td>
<td></td>
</tr>
<tr>
<td>● <em>SHA-1 Hash:</em> The SHA-1 (20 bytes) hash of the file (default).</td>
<td></td>
</tr>
<tr>
<td>● <em>SHA-256 Hash:</em> the SHA-256 (32 bytes) hash of the file (default).</td>
<td></td>
</tr>
</tbody>
</table>

The information displayed in the Properties tab is file-type-dependent, so the selected file determines what displays.
The Hex Tab

The Hex tab shows the file content in hexadecimal. It is different from the Hex Interpreter tab at the bottom of the screen.

The Hex Tab

The bar symbol indicates that the character font is not available, or that an unassigned space is not filled.

File Content Hex View Right-click Menu Options

<table>
<thead>
<tr>
<th>Select all</th>
<th>Show decimal offsets</th>
</tr>
</thead>
</table>

| Copy text | Show text only |
| Copy hex | Fit to window |
| Copy Unicode | Save current settings |
| Copy raw data | Go to Offset takes you to a desired offset. You can select the Hex data to save as a separate file. |
| Save selection | Save selection as carved file lets you manually carve data from files. |

The Hex Interpreter Tab

The Hex Interpreter tab shows interpreted hexadecimal values selected in the Hex tab viewer on the File Content tab in the Viewer pane into decimal integers and possible time and date values as well as Unicode strings.
The Hex Interpreter Tab

The Hex Value Interpreter reads date/time stamp values, including AOL date/time, GPS date/time, Mac date/time, BCD, BCD Hex, and BitDate.

The Hex tab displays file contents in hexadecimal format. Use this view together with the Hex Interpreter pane. The Hex View tab is also found in the File Content View. This feature helps if you are familiar with the internal code structure of different file types, and know where to look for specific data patterns or for time and date information.

To convert hexadecimal values

1. Highlight one to eight continuous bytes of hexadecimal code in the File Content pane > File Content tab viewer > Hex tab. (Select two or more bytes for the Unicode string, depending on the type of data you want to interpret and view.)
2. Switch to the Hex Interpreter tab at the bottom of the File Content Viewer > Hex tab, or open it next to, or below the File Content tab > Hex tab view to see both concurrently.
3. The possible valid representations, or interpretations, of the selected code automatically display in the Hex Value Interpreter.

Little-endian and big-endian refers to which bits are most significant in multi-byte data types, and describes the order in which a sequence of bytes is stored in a computer’s memory. Microsoft Windows generally runs as LittleEndian, because it was developed on and mostly runs on Intel-based, or Intel-compatible machines.

In a big-endian system, the most significant bit value in the sequence is stored first (at the lowest storage address). In a little-endian system, the least significant value in the sequence is stored first. These rules apply when reading from left to right, as we do in the English language.

As a rule, Intel based computers store data in a little-endian fashion, where RISC-based systems such as Macintosh, store data in a big-endian fashion. This would be fine, except that a) AccessData’s products image and process data from both types of machines, and b) there are many applications that were developed on one type of system, and are now “ported” to the other system type. You can’t necessarily apply one rule and automatically know which it is.

Little-endian is used as the default setting. If you view a data selection in the Hex Interpreter and
it does not seem correct, you can try choosing the big-endian setting to see if the data displayed makes more sense.

The Text Tab

The Text tab displays the file’s content as text using the code page selected from the View Text As drop-down menu.

The File Content pane currently provides many code pages from which to choose. When the desired code page is selected, the Text tab will present the view of the selected file in text using the selected code page language.

The Filtered Tab

The Filtered tab shows the file’s text created during indexing. The following figure represents content displayed in the filtered tab. The text is taken from an index created for the current session if indexing was not previously selected.
The Filter Toolbar

The interface provides a tool bar for applying QuickPicks and Filters to the case. See also Filtering Data to Locate Evidence (page 241)

The Filter Toolbar

Filter Toolbar Components

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Filter on/off icon]</td>
<td>Turns the filter on or off. Filtered data is shown in a colored pane to indicate that it is filtered. In addition, if no filter is applied, the icon is grayed out. When active, or ON, the Filter button has a light blue background. When inactive, or OFF, the background is gray.</td>
</tr>
<tr>
<td>![Filter drop-down menu]</td>
<td>Opens the drop-down menu listing defined filters. Applies the selected filter.</td>
</tr>
<tr>
<td>![Filter Manager icon]</td>
<td>Opens the Filter Manager. The Filter Manager allows multiple filters to be selected and applied concurrently. These are known as Compound filters.</td>
</tr>
<tr>
<td>![QuickPicks on/off icon]</td>
<td>Turns the QuickPicks filter on or off. The QuickPicks filter is used in the Explore tab to populate the file list with only items the investigator wishes to analyze. When active, or ON, the QuickPicks button is light blue. When inactive, or OFF, the background is gray.</td>
</tr>
<tr>
<td>![Lock/Unlock icon]</td>
<td>Locks or unlocks the movable panes in the application. When the lock is applied, the box turns grey, and the panes are locked. When unlocked, the box has a light blue background and blue outline, indicating the panes can be moved.</td>
</tr>
</tbody>
</table>
Using QuickPicks

QuickPicks is a type of filter that allows the selection of multiple folders and files in order to focus analysis on specific content. The following figure represents the Explore Evidence Items tree with a partially selected set of folders and sub-folders using the QuickPicks feature. The QuickPicks filter simultaneously displays open and unopened descendent containers of all selected tree branches in the File List at once. The colors of the compound icons indicate whether descendants are selected. The icons are a combination of an arrow, representing the current tree level, and a folder, representing any descendants.

QuickPicks Icons

A dark green arrow behind a yellow folder means that although the folder itself is not selected, some of its descendents are selected.

A white arrow with no folder means neither that folder, nor any of its descendents is selected.

The File List view reflects the current QuickPicks selections. When QuickPicks is active, or on, if no folders are selected, the File List view shows the currently selected item in the Tree view, including first-level child objects. When any item is selected, that selection is reflected in the File List view. When QuickPicks is not active, or off, the File List view displays only items at the selected level in the tree view, with no children.
Chapter 23
Examining Evidence in the Overview Tab

This chapter includes the following topics
- Using the Overview Tab (page 421)

Using the Overview Tab
The Overview tab provides a general view of a case. You can find the number of items in various categories, view lists of items and lists of individual files by category, status, and extension. Evidence categories are represented by trees in the upper-left Case Overview pane of the application.

The Overview Tab

Evidence Groups Container
Evidence items can be assigned to a group when they are added to a case. The Evidence Groups Container shows at-a-glance which Evidence Groups are in use in a case, and the number of items associated with each.

File Items Container
The File Items container itemizes files by whether they have been checked and lists in an expandable tree view the evidence files added to the case.
File Categories (Continued)

File Extension Container
The File Extension container itemizes files by their extensions, such as TXT, MAPIMAIL, and DOC and lists them in a tree view.

The File Extension Container content numbers do not synchronize or match up with the overall number of case items. This is because case items, such as file folders, do not have extensions and, therefore, are not listed in the File Extension Container.

File Category Container
File Category container itemizes files by type, such as a word processing document, graphic, email, executable (program file), or folder, and lists them in a tree view.

The statistics for each category are automatically listed. Expand the category tree view to see the file list associated with it.

BlackBerry IPD files (the files created on your PC when you back up your BlackBerry device) are recognized and categorized. Not every BlackBerry device has the same features as all the others, and everyone uses their device differently so there is no guarantee that every type of data will be available from every set of backup IPD files. You will most likely see HTML and XML files, Messages, and Pictures/Photos. Address Books, Tasks, and Calendars will be extracted if available.

File Categories

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Archives</td>
<td>Archive files include email archive files, ZIP, STUFFIT, THUMBS.DB thumbnail graphics, and other archive formats.</td>
</tr>
<tr>
<td>Databases</td>
<td>Database files such as those from MS Access, Lotus Notes NSF, and other database programs.</td>
</tr>
<tr>
<td>Documents</td>
<td>Includes recognized word processing, HTML, WML, XML, TXT, or other document-type files.</td>
</tr>
<tr>
<td>Email</td>
<td>Includes email messages from Outlook, Outlook Express, AOL, Endoscope, Yahoo, Rethink, Udder, Hotmail, Lotus Notes, and MSN.</td>
</tr>
<tr>
<td>Executables</td>
<td>Includes Win32 executable files and DLLs, OS/2, Windows VxD, Windows NT, Java Script, and other executable formats.</td>
</tr>
<tr>
<td>Folders</td>
<td>Folders or directories that are located in the evidence.</td>
</tr>
<tr>
<td>Graphics</td>
<td>Lists files having the standard recognized graphic formats such as TIF, GIF, JPEG, HEIC, HEVC, and BMP, as found in the evidence.</td>
</tr>
</tbody>
</table>
### File Categories (Continued)

- **Internet/Chat Files** Lists Microsoft Internet Explorer cache and history indexes.
- **Mobile Phone** Lists data acquired from recognized mobile phone devices.
- **Multimedia** Lists AIF, WAV, ASF, and other audio and video files as found in the evidence.
- **OS/File System Files** Lists partitions, file systems, registry files, and so forth.
- **Other Encryption Files** Lists found encrypted files, as well as files needed for decryption such as EFS searchstrings, Public Keys, Private Keys, and other RSA Keys.
  For more information on Decrypting Encrypted Files, See [Decryption](page 265).
- **Other Known Types** A miscellaneous category that includes audio files, help files, dictionaries, clipboard files, link files, and alternate data stream files such as those found in Word DOC files, etc.
  **Note:** Other Known Types includes NSF Misc. Note (Calendar, $profile data, and other miscellaneous files that in the past were shown as HTML), and NSF Stub Note (a link to the same email or calendar item in another view) sub categories.
- **Presentations** Lists multimedia file types such as MS PowerPoint or Corel Presentation files.
- **Slack/Free Space** Lists files, or fragments of files that are no longer seen by the file system, but that havenot been completely overwritten.
- **Spreadsheets** Lists spreadsheets from Lotus, Microsoft Excel, Quattro Pro, and others, as found in the evidence.
- **System Summary** Detailed metadata parsed from the evidence data regarding the attributes of the system hardware and software. Use the Generate System Summary processing option to parse data into these categories. **System Summary is not indexed if selected.** See [Evidence Processing Options](page 88).
- **Unknown Types** Lists files whose types are not identified.
- **User Types** Lists user-defined file types such as those defined in a Custom File Identification File.
**File Categories (Continued)**

*File Status Container*

File Status covers a number of file categories that can alert the investigator to problem files or help narrow down a search.

The statistics for each category are automatically listed. Click the category button to see the file list associated with it. The following table displays the file status categories.

**File Status Categories**

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bad Extensions</td>
<td>Files with an extension that does not match the file type identified in the</td>
</tr>
<tr>
<td></td>
<td>file header, for example, a GIF image renamed as [graphic].txt.</td>
</tr>
<tr>
<td>Data Carved Files</td>
<td>The results of data carving when the option was chosen for preprocessing.</td>
</tr>
<tr>
<td>Decrypted Files</td>
<td>The files decrypted by applying the option in the Tools menu.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: Decrypted status means the file was decrypted from evidence added to the case in its original form. The software has had control of the file and knows it was originally encrypted, that it was contained in the original evidence, and thus, is relevant to the case.</td>
</tr>
<tr>
<td>Deleted Files</td>
<td>Complete files or folders recovered from slack or free space that were deleted by the owner of the image, but not yet written over by new data.</td>
</tr>
<tr>
<td>Duplicate Items</td>
<td>Any items that have an identical hash.</td>
</tr>
<tr>
<td></td>
<td>Because the hash is independent of the filename, identical files may actually have different filenames.</td>
</tr>
<tr>
<td></td>
<td>The first instance of a file found during processing is the primary item. Any subsequently found files, whose hash is identical, is considered a secondary item, regardless of how many duplications of the same file are found.</td>
</tr>
<tr>
<td>Email Attachments</td>
<td>Files attached to the email in the evidence.</td>
</tr>
</tbody>
</table>

**Email Related Items (From Email)**

All email-related files including email messages, archives, and attachments.
To Restrict Count Updates by Adding a Settings Entry in the Registry

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encrypted Files</td>
<td>Files that are encrypted or have a password. This includes files that have a</td>
</tr>
<tr>
<td></td>
<td>read-only-password; that is, they may be opened and viewed, but not modified</td>
</tr>
<tr>
<td></td>
<td>by the reader. If the files have been decrypted with EFS, and you have access</td>
</tr>
<tr>
<td></td>
<td>to the user’s login password, you can decrypt these files.</td>
</tr>
<tr>
<td>Flagged Ignore</td>
<td>Files that are flagged to be ignored are probably not important to the case.</td>
</tr>
<tr>
<td>Flagged Privileged</td>
<td>Files that are flagged as privileged cannot be viewed by the Case Reviewer.</td>
</tr>
<tr>
<td>From Recycle Bin</td>
<td>Files retrieved from the Windows Recycle Bin.</td>
</tr>
<tr>
<td>KFF Alert Files</td>
<td>Files identified as likely to be contraband or illicit in nature.</td>
</tr>
<tr>
<td>KFF Ignorable</td>
<td>Files identified as likely to be forensically benign.</td>
</tr>
<tr>
<td>OCR Graphics</td>
<td>Files with graphic text that have been interpreted by the Optical Character</td>
</tr>
<tr>
<td></td>
<td>Recognition engine.</td>
</tr>
<tr>
<td>OLE Sub-items</td>
<td>Items or pieces of information that are embedded in a file, such as text,</td>
</tr>
<tr>
<td></td>
<td>graphics, or an entire file. This includes file summary information (also</td>
</tr>
<tr>
<td></td>
<td>known as metadata) included in documents, spreadsheets, and presentations.</td>
</tr>
<tr>
<td>Project VIC Matches</td>
<td>Files flagged as matches according to Project VIC analysis.</td>
</tr>
<tr>
<td>User Decrypted</td>
<td>Files you’ve previously decrypted, and then added to the case.</td>
</tr>
</tbody>
</table>

**Note:** A user can add any file using Add Decrypted File, and it will be set as decrypted by user. This status indicates that AccessData did not decrypt this file, and cannot guarantee its validity or that such a file has anything to do with the case.

**Cluster Topic Container**

Cluster Topic are groups of files created through Document Content Analysis. This feature allows you to group Email Threaded data and Near Duplicate data together for quicker review. After the application completes the analysis, the content appears in the Cluster Topic container. The content is organized by the keywords in which the documents were analyzed and grouped. Documents that do not fit into a Content Topic category are placed in the UNCLUSTERED category.

**Using Document Content Analysis** (page 558)
To Restrict Count Updates by Adding a Settings Entry in the Registry

Processing and Displaying Evidence Counts

When you open the Examiner > Overview tab, queries are run to calculate the evidence counts in multiple categories: Evidence Groups, File Extension, File Category, and Labels. If you have a large case, you can speed up performance by calculating counts in only one category. You can restrict this in one of two ways:

- Through a registry setting
- In the Examiner interface

1. Navigate to the following path in the registry to add the settings value:
   - HKEY_CURRENT_USER\Software\AccessData\Products\Forensic Toolkit\[x.x]\Settings\Tabs\Tab7
2. Add the following value: OverviewUpdateType REG_DWORD 2

Use the data values in the following table to select which category you would like to specify.

<table>
<thead>
<tr>
<th>Registry Data Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>FILE CATEGORY</td>
</tr>
<tr>
<td>FILE EXTENSION</td>
</tr>
<tr>
<td>LABELS</td>
</tr>
<tr>
<td>EVIDENCE GROUPS</td>
</tr>
</tbody>
</table>

To Restrict Count Updates in the Examiner Interface

1. Click on an item within one of the evidence categories that contain evidence counts.
2. Press the Home key on the keyboard.

This will reduce the case overview tree to only the selected item and it’s children. For example, if you select the Documents category, this will reduce the case overview tree to showing only Documents. This choice is stored in the settings for the Overview tab.

To Restore Full Count Updates in the Examiner Interface

- Click an item in the reduced tree and press the End key on the keyboard to restore the full case overview tree.
To Restrict Count Updates by Adding a Settings Entry in the Registry

Disabling the Calculation and Display of the Total Logical Size
When viewing evidence in the Examiner, the Total Logical Size (Total LSize) is calculated for different categories of evidence. To speed up the interface for large cases, you can disable the calculation and display of this value by adding a registry value.

To Hide the Total Logical Size
1. Navigate to the following path in the registry: HKLM\SOFTWARE\AccessData\Products\Forensic Toolkit\version
2. Add the following value: hide_total_logical_size DWORD value 1

To Restore the Total Logical Size
❖ Use the following value: hide_total_logical_size DWORD value 0
Chapter 24
Examining Email

Using the Email Tab
The Email tab displays email mailboxes and their associated messages and attachments. The display is a coded HTML format.

The Email Tab

**Email Status Tree**
The Email Status tree lists information such as the sender of the email, and whether an email has attachments. They are listed according to the groups they belong to.

**Email Archives Tree**
The Email Archives tree lists Email related files that are considered containers. Item types include DBX, MBX,PST/OST, Saved Mail, Sent Mail, Trash, and so forth. The tree is limited to archive types found within the evidence during processing.
**Email Tree**

The Email tree lists message counts, AOL DBX counts, PST counts, NSF counts, MBOX counts, and other such counts. Exchange and PST Emails can be exported to MSG format. In addition, MSG files resulting from an export of internet email look the way they should.

The **Email Tab > Email** Items tree view contains two new groups: Email By Date (organized by Year, then byMonth, then by Date, for both Submitted and Delivered); and Email Addresses (organized by Senders and Recipients, and subcategorized by Email Domain, Display Name, and Email Addresses).

You can also export Tasks, Contacts, Appointments, Sticky Notes, and Journal Entries to MSG files.

**Important:** If the Mozilla Firefox directory is added as evidence while in use, history, downloads, etc. are identified as zero-length files.

When an email-related item is selected in the File List, right-click and choose **View this item in a different list > Email** to see the file in Email context.

**Note:** Email data parsed into the new nodes in the Email tree view will only be populated in new cases. Converted cases will not have this data. To make this data available in older cases, re-process the case in the new version.
It is possible to process and view Email and Contacts for Windows 10 Email.

**Note:** This software does not parse anything other than Email and Contacts for Windows 10 Email at this time.

### Processing Windows 10 Email and Contacts

**To Process Windows 10 Email and Contacts:**
1. In the Evidence Processing window, select **Expand Compound Files**.
2. Click on the **Expansion Options** button. Scroll down and select the **Unistore Database (Windows 10 Mail)** option.
3. Click **Ok** and process the evidence.

### Viewing Windows 10 Email and Contacts

In the Windows File System, the ESE database is found in the store.vol file within the Unistore DB. This is where the logical structure for emails, contacts, and other important information is kept. There are two ways to view Windows 10 Email and Contacts. If you choose to see the full file structure of the store.vol file, you will need to use the Explore Tab. If you only want to view emails, the Email Tab contains all emails in the case, including Windows 10 Email.

**To View Windows 10 Contacts in the Explore Tab:**
1. Process the evidence as described above.
2. Navigate to the **Explore Tab**.
3. In the Evidence Items pane, navigate to the user’s **EmailComms > Comms > UnistoreDB > store.vol** file. Drill down until you see the email folders.
4. To view contacts, open the folder for the email program you are looking for. Expand the IPM.root folder, then select the Contacts folder. The Contacts will then populate in the File List pane. Select a Contact from the list to see the information associated with that contact in the File Content pane. Select the Properties tab to view the various properties associated with the selected contact in Cool HTML.
To View Windows 10 Email in the Explore Tab:
1. Process the evidence as described above.
2. Navigate to the Explore Tab.
3. In the Evidence Items pane, navigate to the user’s EmailComms > Comms > UnistoreDB > store.vol file. Inside this file will be the various email folders.
4. To view emails, expand the IPM.root folder for the email program you are looking for and select the Inbox folder. The list of emails will then populate in the File List pane. Select an email to view it in the File Content pane. Select the Properties tab to view the various properties associated with the selected email.

**Note:** If you’d like to see an email in the Email Tab instead of the Explore Tab, right-click on the email and select View This Item In a Different List > Email.

To View Windows 10 Email in the Email Tab:
❖ Windows 10 Email is automatically populated in the existing folders in the email tab.

**Exporting Windows 10 Email**
Individual emails can be exported as MSG files. When exported, all existing attachments will be included.

**Note:** If the user has not downloaded the attachment, the content will not be available.

To Export a Windows 10 Email:
1. Right-click on the item you’d like to export and select Export.
2. In the Export window, select the Export emails as MSG option and set a Destination path.
3. Click Ok.

Your email(s) will be exported to the selected destination folder.
Chapter 25
Examining Graphics

This chapter includes the following topics

- Using the Graphics Tab (page 430)
- Evaluating Explicit Material (page 436)
- Image Analysis (page 439)
- Image Recognition Analysis (page 439)
- Facial Recognition (page 441)

Using the Graphics Tab
The Graphics tab displays the graphics in a case like a photo-album.

The Graphics Tab
Each graphic file is shown in a thumbnail view. A graphic displays in the Thumbnail view when its thumbnail is checked in the File Contents pane.

**Graphics tab Thumbnails**

In the thumbnail viewer, if a graphic is not fully loaded, the following icon is displayed:

![Icon for partially loaded graphic](image1)

In the thumbnail viewer, if a graphic cannot be displayed, the following icon is displayed:

![Icon for unresolvable graphic](image2)

Beneath each thumbnail image is a check box. When creating a report, choose to include all of the graphics in the case or only those graphics that are checked.

![Check box for including graphics](image3)

The Evidence Items pane shows the Overview tree by default. Use the View menu to change what displays here.
About the Graphics Tab Filter

The graphics files that appear on the Graphics Tab are the ones that meet the criteria of the Graphics tab filter that is applied. You can change the tab filter to view different sets of files. The Graphics tab has its own tab filter. See Using Tab Filters (page 245) for more information.

In a new installation, the Graphics tab filter is set to the Graphic Files w/o Dup+Ignore filter by default.

This eliminates the need to sort through a high volume of unrelated images. File types not shown when this filter is applied include duplicate items, flagged ignore, and KFF ignorable.

See Ignore Highlighted on page 435.

In an upgrade environment, the current tab filter will be the filter that was previously used. You can apply the Graphics Files w/o Dup+Ignore filter as the default Graphics Tab Filter.

To change the tab filter

1. In the Examiner, navigate to Filter > Tab Filter.
2. In the drop down menu, select a filter to apply to the current tab. See Using Tab Filters (page 245) for more information.

Stacking Filters in the Graphics Tab

There is a default filter on the graphics tab that filters out duplicates and KFF ignorable files. This filter can be changed depending on what items you are searching for. See Using Simple Filtering (page 245) for instructions on how to change and apply tab filters.

You can also add standard filters (such as a Not Bookmarked filter) to pare down the images in the panel to view only things you haven’t seen or that haven’t been processed already. This can be ideal for investigating large batches of images. See Using Compound Filters (page 249) for instructions on how to create and apply multiple filters simultaneously.

See Filtering Data to Locate Evidence (page 241) for more information on using filters.
The Thumbnails Size Setting

The thumbnail settings allow large amounts of graphic data to be displayed for evidence investigation, or larger thumbnails to show more detail quickly. The investigator does not always need to see details to pick out evidence; scan the thumbnails for flesh tones, photographic-type graphics, and perhaps particular shapes. Once found, the graphics can be inspected more closely in the Content Viewer. There are two ways to change the thumbnails size setting, in the Examiner View menu or with the Thumbnail Size Selector ( ).

- To change the Thumbnail Size in the View menu, click View > Thumbnail Size and select a size.
- To change the Thumbnail Size with the Thumbnail Size Selector, click and select a size.

Note: The thumbnail pane needs to be sized at least one thumbnail in height for the scrolling feature to work properly.

Changing the Thumbnail Size
The detachable pane feature is especially useful when you undock the thumbnails graphics pane and move it to a second monitor, thus freeing your first monitor to display the entire data set for the graphics files being analyzed. You can undock the Thumbnails pane, and expand it across the screen. Then you can open the Thumbnails Settings sub-menu, and scale the thumbnails down to fit as many as possible in the pane.

**Moving the Thumbnails Pane**

![Image of Thumbnails Pane]

**Using the Thumbnails Pane**

The Graphics tab will automatically load all images in the case. It can load over ten million images for review. There are three actions available within the Thumbnail pane:

- Show Tooltip checkbox
- Ignore Highlighted button
- Thumbnail Size Selector dropdown
Show Tooltip
When the Show Tooltip checkbox is selected, information about an image is displayed as the mouse hovers over it. The tooltip displays the following information for the image:

- Name
- Logical Size
- Physical Size
- Created

Ignore Highlighted
You can remove unrelated images from the Thumbnails Pane using the Ignore Highlighted button.
Selecting one or more files in the Thumbnails Pane and clicking the Ignore Highlighted button will give the file(s) a Flagged Ignore status. If the default Graphic Files w/o Dup+Ignore filter is applied, the selected files will no longer be visible in the Graphics tab. This allows graphics files that are not applicable to the case to be removed from the Thumbnail Pane.
See About the Graphics Tab Filter on page 432.

To review the files that have been flagged with an ignore marker, navigate to Overview > File Status > Flagged Ignore.

Thumbnail Size Selector
There is a dropdown box in the Thumbnail Pane that will quickly change the size of the displayed thumbnails. The following size options are available:

- Extra Large
- Large
- Medium
- Small
Evaluating Explicit Material

When explicit material is suspected in a case, the Explicit Image Detection (AID) feature allows for easier location and identification of those files. When creating the case, there are options for identifying explicit material.

See Using Explicit Image Detection (page 105) for more information on setting the EID pre-processing options prior to case creation.

When the pre-processing options are set and applied to evidence as it is processed, in the case you can easily identify files that fit the criteria you set.

Note: You can also use the Project VIC feature to identify known explicit images. See Using Project VIC on page 378.

Filtering EID Material

The following tasks can help you use the EID feature.

Create an EID Tab Filter

A Tab Filter must be used here to filter the folders from the Explore tab, but not filter out the Folders’ content from the Graphics Tab. However, the filter itself must be created first, then the filter must be applied as a Tab Filter.

To create a filter for the EID folders in your case

1. Click the Explore tab.
2. Ensure that Filters are turned off, and the Filter drop-down displays "-unfiltered-".
4. Create a Filter to include EID Folders that have high scores.

4a. Give the Filter a name that reflects its purpose.
4b. Provide a description with enough information to be helpful at a glance.
4c. Set up rules. Check each rule to include it in the filter.
   4d. Mark Live Preview to see the effects of the filter on the current File List.
   4e. Choose Match Any, or Match All, to fit your needs, according to the preview.
   4f. Click Save > Close.

If you choose to, repeat Steps 3 and 4 for Medium folders with a criteria of 40, then move to Step 5.

5. From the Filter Manager, copy the new filters to the Include list on the top-right side of the view.
6. At the bottom of the dialog, click Apply and Close.
To apply the new filter as a Tab filter
1. Click the Explore tab.
2. Ensure that Filters are turned off, and the Filter drop-down displays “-unfiltered-”.
3. Click Filter > Tab Filter.
4. In the Tab Filter Selection dialog, click the drop-down to select Explicit images folder (high score) as created earlier.
5. Click OK.

Change the Column List Settings
To view the Explicit Image Detection (EID) statistics for your case in the File List, do the following:
1. Click the Graphics tab.
2. In the File List, select the default EID column template from the drop-down list, or add the EID columns to the column template you choose. To customize a Columns Template for EID content, do the following:
   2a. Click Column Settings in the File List toolbar.
   2b. In the Manage Column Settings dialog, click New, or highlight an existing template and click Copy Selected.
   2c. In the Column Settings dialog, select the EID-related column headings to add to the template, and click Add
   2d. Make your selections.
   2e. Move the selected columns up in the list to make them display closer to the left-most column in the view, as it best works for you.
3. Click OK
4. From the Manage Column Settings, select the New Column template, and click Apply. Later, to re-apply this column template, select it from the Column Setting drop-down. The resulting columns are displayed in the File List view
5. In the File List view, arrange the column headings so you can see the EID data.
6. Click any column heading to sort on that column, to more easily see and evaluate the relevant data.
**EID Scoring**

Each folder is given a score that indicates the percentage of files within the folder that have an EID score above 50. For example, if the folder contains 8 files and three of them score over 50, the folder score will be 38 (3 is 37.5% of 8). Now, a folder score of 38 does not mean there is no objectionable material in that folder, it only means that there is not a high concentration of objectionable material found there.

Explicit Image Detection filtering rates pictures according to the presence or absence of skin tones in graphic files. In addition, it not only looks for flesh tone colors, but it has been trained on a library of approximately 30,000 pornographic images. It assesses actual visual content. This capability increases the speed with which investigators can handle cases that involve pornography.

Successfully filtered pictures are issued a score between 0 and 100 (0 being complete absence of skin tones, and 100 being heavy presence of skin tones). A score above 100 indicates that no detection could be made. When you set filters for analyzing the scored data, you specify your own acceptance threshold limit for images you may consider inappropriate. Negative scores indicate a black and white, or grayscale image where no determination can be made, or that some error occurred in processing the file.

### Descriptions of EID Scoring Values

<table>
<thead>
<tr>
<th>Score</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 to 100</td>
<td>The amount of skin tones detected. 0 = few skin tones detected, 100 heavy skin tones detected</td>
</tr>
<tr>
<td>-1</td>
<td>File not found</td>
</tr>
<tr>
<td>-2</td>
<td>License error</td>
</tr>
<tr>
<td>-3</td>
<td>Wrong file format</td>
</tr>
<tr>
<td>-4</td>
<td>No match found</td>
</tr>
<tr>
<td>-5</td>
<td>Folder not found</td>
</tr>
<tr>
<td>-6</td>
<td>Unknown error</td>
</tr>
<tr>
<td>-7</td>
<td>Cannot load image (e.g., corrupt image)</td>
</tr>
<tr>
<td>-8</td>
<td>Not enough information</td>
</tr>
</tbody>
</table>
-9  Face detection profile path is null

-10  Can't open face detection directory
-11  Face detection file not found

-12  Input classifier not initialized

-13  Init profile failed

-14  File path is empty

-16  Image data is empty

-17  Null matching handle

-18  Missing retrieval result
-100  An unsupported file format

-101  An unsupported black & white image

-102  An unsupported grayscale image
-103  An unsupported monochrome image

-1000  An unknown error
-1001  The EID score function threw an exception
-1002  The EID score function threw an exception
Image Analysis

About Image Analysis

The Image Analysis tools automatically recognize specific objects or facial profiles by leveraging the power of TensorFlow and the Quin-C Server.

Image Recognition relies on built-in training models for common illicit activity patterns. Categories include money, guns, child exploitation, syringes, etc. Users can automatically search the case data for images that fall into any of the selected categories.

The Facial Recognition tools can be custom trained to detect and flag facial profile patterns within a given data set.
**Image Recognition Analysis**

Image Recognition Analysis is the process that utilizes the power of the TensorFlow A.I. engine to automatically identify and tag images that match models found within a evidence data set.

**Prerequisites**

- The following components running on a Windows Server 2016 platform or newer:
  - FTK Central Server (Process name: Weblabselfhost Servicename: ExterroSelfHostService)
  - AccessData.AI_Server
  - Python 3.7.x (automatically installed with AI server)

**Notes:**

- Windows system PATH environment variables need to include entries for the following two Python directories:
  
  `C:\Program Files\Python37; C:\Program Files\Python37\Scripts;`

- Lots of space is required on the drive where the following Tensorflow temp directory is hosted:
  
  `C:\Program Files\AccessData\tensorflow\tensorflowstorage\temp`
How to Perform Image Recognition Analysis

1. Ensure the A.I. Server is running
2. Launch Enterprise and open the case examiner interface.
3. In the case examiner interface, select **Tools >> Image Analysis >> Image Recognition**
4. Select a provided model from the Identified Categories list.
5. Select Highlighted/Checked/Listed files to run this process against.
6. Select a Minimum Threshold Score (Confidence). The default value will retain the best results.

7. Click OK.
8. The Data Processing Status window appears.
9. On the Other Jobs view, wait for the facial recognition data processing jobs to complete.
10. When complete, the images within the processed dataset that are flagged as a match will be automatically added to a label named “FacialRecognitionResults.”
Facial Recognition

About Facial Recognition Training

The Facial Recognition feature trains the application to recognize a specific face by leveraging the power of TensorFlow and the Quin-C Server.

Facial Recognition training is performed by using a bounding box on either a single image or set of images. Once trained, users can search the case data for similar images. Filters for each set of results are created based on the training data file name. These filters are automatically applied to responsive images, allowing investigators to use a single filter to quickly view results.

Prerequisites

- The following components running on a Windows Server 2016 platform:
  - Quin-C Server (Process name: Weblabsselfhost Servicename: ExterroSelfHostService)
  - AccessData_AI_Server
  - Python 3.7.x (automatically installed with AI server).

  Note: Windows system PATH environment variables need to include entries for the following two Python directories:
C:\Program Files\Python37; C:\Program Files\Python37\Scripts;
Lots of space is required on the drive where the following Tensorflow temp directory is hosted:

C:\Program Files\AccessData\tensorflow\tensorflowstorage\temp

How to train A.I. engine to do facial recognition
1. Ensure the A.I. Server is running
   1a. Right-click the Start_AI_Server.bat script (located on the desktop where the AccessData_AI_Server component is installed) and select “Run As Administrator” to start the A.I. server engine.
2. Launch Enterprise and open the case examiner interface.
3. Locate the graphics of “known” faces to be used to train the A.I. engine (it is recommended to submit at least 100 graphics per face profile for best results).
4. In the Natural Viewer tab, use the mouse cursor to draw a box around the face to be submitted.
5. Right-click within the box drawn, select Save for Facial Recognition...
6. In the Save Suspect Face window, do one of the following:
   6a. Select a face profile from the list and click Save.
   6b. Click the Name column header and type in a label for a new face profile

Note: All facial recognition profile directories are automatically saved to a subfolder named facialrecognition under the main case folder.

7. Click Save
8. Repeat steps 3-7 until the desired facial profile(s) has sufficient samples.
9. In the case examiner interface, select Tools >> Image Analysis >> Facial Training...
10. The Facial Training window appears displaying a list of current facial profiles. Click OK to start a facial training job.
11. The Data Processing Status window appears

Note: In the background a new label is created for any new facial profiles that don’t already have labels.

12. On the Other Jobs view, wait for the facial recognition training data processing job to complete.
13. Once facial recognition training is complete, the system is ready to perform Facial Recognition Analysis on the facial profiles that have been trained.
Facial Recognition Profiles

As a result of facial recognition training, each facial recognition profile will have a directory automatically saved to a subfolder named `facialrecognition` under the main case folder. The names of the subfolders within the `facialrecognition` directory correspond to each of the profiles created on the examiner system.

**How to Rename a Facial Recognition Profile**

1. Make sure no current facial recognition jobs are running for the profile to be renamed.
2. In Windows Explorer, browse to the folder named “FacialRecognition” located at the root of your system’s main case folder.

```
- CaseData
  - AnnotatedImages
  - FacialRecognition
  - ImageRecognition
  - imagetrainer
```

3. Simply rename the subfolder to rename the list of profiles displayed in the “Save Suspect Face” dialog.

Facial Recognition Analysis

Facial Recognition Analysis is the process that utilizes the power of the TensorFlow A.I. engine to automatically identify and tag facial images that match models found within a evidence data set. Matching faces within a data set will have a bounding box automatically drawn around the face and will display that tag associated to the profile for easy identification of individuals or suspects.
How to perform facial recognition analysis

1. At least one round of Facial Recognition training must have already been completed prior to performing the following steps. See About Facial Recognition Training on page 441.

2. Ensure the A.I. Server is running

   2a. Right-click the “Start_AI_Server.bat” script (located on the desktop where the AccessData_AI_Server” component is installed) and select “Run As Administrator” to start the A.I. server engine.

3. Launch Enterprise and open the case examiner interface.

4. In the case examiner interface, select **Tools >> Image Analysis >> Facial Recognition**

5. The Data Processing Status window appears.

6. On the *Other Jobs* view, wait for the facial recognition data processing jobs to complete.

7. When complete, the images within the processed dataset that are flagged as a match will be automatically added to a label named “FacialRecognitionResults.”

Image Training Data Distribution

Upon completion of facial recognition training, a “model” file is created. Modeling data is stored in a file with a *.pb file extension. These modeling files can be distributed (copied) from one A.I. server installation to another in order to avoid redundant facial recognition training work on each system.

How to Distribute Image Training Models

1. Locate the training model files (*.pb) within the following directory:

   [DRIVE]\Program Files\AccessData\tensorflow\tensorflowstorage\exported_models\n
2. Make copies of the .pb files for the models you wish to transfer.

3. Paste the .pb files into the following directory on the destination system.

   [DRIVE]\Program Files\AccessData\tensorflow\tensorflowstorage\exported_models\n
4. The destination system will automatically pickup the training models when launched.
Similar Face Detection

To quickly identify graphic images containing faces of persons with matching or similar facial features, use the Similar Face Detection analysis. This option will launch an analysis, and then when complete, the results can be reviewed in FTK Plus. Similar Face Detection uses the power of the Tensorflow AI engine to perform the analysis.

How to run similar face detection

1. Ensure the AccessData AI service is running.
2. In Case Examiner, select Similar Face Detection from the Tools >> Image Analysis menu.
3. The processing status window appears and the Similar Face Detection job starts automatically.
4. When complete, navigate to Tools >> Other Applications >> FTK Plus to review the results.

Similar Object Detection

To quickly identify graphic images containing objects with similar attributes, use the Similar Object Detection analysis. This option will launch an analysis job, and then when complete, the results can be reviewed in FTK Plus.

How to run similar object detection

1. Ensure the AccessData AI service is running.
2. In Case Examiner, select Similar Object Detection from the Tools >> Image Analysis menu.
3. The processing status window appears and the Similar Object Detection job starts automatically.
4. When complete, navigate to Tools >> Other Applications >> FTK Plus to review the results.
Chapter 26
Examining Videos

The Video tab lets you view detailed information about the video files in your cases. You can generate thumbnails from video files and display them in the Video Thumbnail pane. This functionality lets you quickly examine a portion of the contents within video files without having to watch each media file individually.

See Generating Thumbnails for Video Files (page 446)

The Video tab also includes an embedded media player that lets you view the contents of video files. When you process the evidence in your case, you can choose to create a common video type for each of the various videos in your case. These common video types are not the actual video files from the evidence, but a copied conversion of the media that is generated by AccessData. These features let you view the contents of multiple video types, in a common resolution, and sampling rate, from within the Examiner’s embedded media player.

See Creating Common Video Files (page 447)

When you process evidence, video thumbnails are created by default. To disable the creation of video thumbnails, turn off the Create Thumbnails for Videos option in the Evidence Processing options.

See Evidence Processing Options on page 88.
Generating Thumbnails for Video Files

You can generate thumbnail graphics based on the content that exists within video files in your case. Video thumbnail generation is accomplished during processing. You can either set up video thumbnail generation when you create a new case, or you can run the processing against an existing case by using the Additional Analysis dialog.

To generate thumbnails for video files

1. Do one of the following:
   - In the Case Manager, click Case > New. Then, click Detailed Options.
   - In the Examiner, click Evidence > Additional Analysis > Hashing/Job Options.

2. Check Create Thumbnails for Videos.
3. Click Thumbnail Options.
4. In the Video Thumbnail Options dialog, set from the following:

   Percent This option generates thumbnails against videos based on the percentage of a video's total content. For example, if you set this value to 5, then at every 5% of the video a thumbnail is generated.

   Interval This option generates thumbnails against videos based on seconds. For example, if you set this value to 5, then at every 5 seconds within a video, a thumbnail is generated.

5. Click OK.
Generating Thumbnails for Video Files

Generating Video Thumbnails from the Natural Viewer
You can also capture video thumbnails directly from a video viewed in the Natural Viewer. This feature allows you to find and capture specific information from video you are reviewing. After capturing a video thumbnail, you can then bookmark that thumbnail for future review.

To capture a video thumbnail from the Natural Viewer
1. From Evidence Explorer, click the Video tab.
2. Highlight the video and click the Natural tab in the File Content pane.
3. Click the Play button (▶).
4. Click the Pause button when you are ready to capture a video thumbnail.

Note: You can navigate through the video using the Rewind and Fast Forward
5. Click Add in the bottom right corner of the Video Thumbnails pane.

The application creates a video thumbnail of the paused frame and places that thumbnail in the VideoThumbnail pane.
Creating Common Video Files

When you process the evidence in your case or during Additional Analysis, you can choose to create a common video type for videos in your case. These common video types are not the actual video files from the evidence, but a copied conversion of the media that is generated and saved as an MP4 file that can be previewed on the video tab. Common video files are not created by default. See Evidence Processing Options on page 88.

To create common video files

1. Do one of the following:
   - In the Case Manager, Click Case > New. Then, click Detailed Options.
   - In the Examiner, click Evidence > Additional Analysis.

2. Check Create Common Video Files.

3. Process or analyze evidence.

Video Formatting Options

4. In the Video Formatting Options dialog, set the following:
   - **Lines of Resolution**: Sets the number of vertical lines in the video. The higher it is, the better the resolution.
   - **Bit Rate**: Sets the rate of bits in Kbps measurements. The higher it is, the better the resolution.

5. Click OK.
Using the Video Tree Pane

The Video tree pane lets you see the multimedia content in a tree view. The content that is displayed in the Video tab is dependent on a default Tab Filter called Video Tab Filter: Video Thumbnails.

The contents in the Video tree displays the multimedia contents in your case and information about the content that applies to the requirements of the Tab filter.

For example, in the graphic below, you can see that the case has 46 total multimedia files. 12 of those multimedia files meet the requirements of the Tab filter and therefore have had video thumbnails generated for them.

**Video Tab: Video Tree Pane**

![Video Tree Pane Graphic]

You can use the Video tree pane to navigate and drill down to specific multimedia containers and files. If you select a file in the tree pane, The Video Thumbnails pane and the File List pane display the content that is contained in your selection.
The Thumbnail Size Setting

The Video Thumbnails pane displays any video thumbnails that you have generated based on your selection in either the Video tree view or in the File List Pane.

Video Tab: Video Thumbnail Pane

You can use the Video Thumbnail pane to rapidly scan through the visual contents in a video file, without having to launch and watch the entire video.

In the Video Thumbnails pane, if a thumbnail could not be generated the following icon is displayed:

![AccessData](image)

In the Video Thumbnails pane, beneath the first thumbnail image for a set of videos is a check box. You can select this check box to check the video file in the Examiner.
The Thumbnail Size Setting

Playing a Video from a Video Thumbnail

You can play a video in the File Content Viewer starting from a selection in the Video Thumbnail pane. For example, if you visually scan the contents of the video thumbnails pane and discover something you need to investigate in the File Content viewer, rather than watching the entirety of the video, you can select the location you want to start the video by selecting that thumbnail.

To Play a Video from the Location of a Video Thumbnail

1. In the Video Thumbnails pane, click the thumbnail from which you want to start the video.

2. In the File Content Pane, in the Natural tab, click the **Play** icon.

The video begins to play from the location that you selected in the Video Thumbnails pane.

You can change the size of the thumbnails that are displayed in the Video tab of the Examiner. See The Thumbnails Size Setting (page 433) for information on how to do this.

Moving the Thumbnails Pane

You can move, float, and dock the thumbnails pane in the Video tab of the Examiner. See Moving the Thumbnails Pane (page 434) for information on how to do this.
Chapter 27
Examining Miscellaneous Evidence

This chapter contains information on the following ways to view evidence:

- Identifying Processing-Generated Data (page 452)
- Relating Generated Files to Original Files (page 452)
- Viewing Windows Prefetch Data (page 453)
- Viewing Data in Windows XML Event Log (EVTX) Files (page 453)
- Viewing IIS Log File Data (page 455)
- Viewing Registry Timeline Data (page 457)
- Viewing Log2Timeline CSV File Data (page 459)
- Identifying Document Languages (page 462)
- Examining Internet Artifact Data (page 464)
- Examining Mobile Phone Data (page 471)
- The asterisk (*) indicates that a particular item is not included for system messages.
- Android Parsers (page 487)
- Python Scripting (page 489)
- Viewing Data in Volume Shadow Copies (page 492)
- Viewing Microsoft Office and Adobe Metadata (page 492)
- About Windows 8 and 10 Keyword Searches (page 493)
- SQLite Query Builder (page 494)
- SQLite Query Builder (page 494)
- Reviewing Portable Case Data in FTK Plus (page 496)
Identifying Processing-Generated Data

There are some files that get generated during processing. Examples of these files include data broken out from compound files, EXIF data from graphic images, file metadata, and so on. There is a column called Actual File which can be used in the File List to designate if the file was in the original data (True) or if it was generated during processing (False).

See Managing Columns on page 613.

Also, when looking at the file name at the bottom of the File List, if the file was generated by FTK, there is an >> after the parent file name and before the generated file name.

For example, photo.jpg>>photo.exif.html, or mystuff.zip>>pass.doc See File List Pane on page 403.

You can also use bookmarks to relate generated files with the actual source file in the evidence. See Identifying Processing-Generated Data on page 452.

Relating Generated Files to Original Files

Some files in your evidence may not be original files but may have been generated during processing. Examples of these files include data broken out from compound files, EXIF data from images, file metadata, and so on.

You can use bookmarks to quickly relate generated files with the actual source file in the evidence. By selecting the Actual Source File option, the source file will be listed and bookmarked as well. All parent items are recursively related within the bookmark from the generated item to the actual source file and not just a parent folder.

See Creating a Bookmark on page 499.

For example, during processing, a DOC file may be generated from a ZIP file. If you bookmark the DOC file and select the Actual Source File option, the original ZIP file is included in the bookmark as well.

The related items are also shown in the bookmark section of reports.

You can also view information in the File List to identify processing-generated files. See Identifying Processing-Generated Data on page 452.

To relate generated files to the original files in bookmarks

1. Right-click a file that was generated during processing.
2. Click either Create Bookmark or Add to Bookmark.
3. On the bookmark dialog, select Actual Source File.
Viewing Windows Prefetch Data

You can easily view data about Windows prefetch (PF) files. When you select a prefetch file in the File List, the following application data is displayed in HTML format in the Natural tab of the File Content pane:

- The file path of the application executable file
- The number of times the application has been run
- The last time the application was run

Viewing Data in Windows XML Event Log (EVTX) Files

About Viewing EVTX Log Files

You can view Microsoft Windows XML event log data. You can view event data in HTML format in the Natural tab of the File Content pane.

You can view event data in one of two ways:

- View event data that is contained in Microsoft Windows XML event log (EVTX) files
- Expand EVTX log files into separate objects for every event record

In the File List, you can see a list of all of the EVTX files. When you view an EVTX log file, in the File Content pane, you can view the information about all of the events that are contained in that one file. There can be a lot of data contained in one file.

When you expand EVTX log files, each event is extracted as its own record. As a result, in the File List, each event is shown as its own item. Each item has a small amount of data in it but there can be many individual event records. For example, you may have 100 EVTX log files, and if you expand them, you can have over 100,000 individual event records.

When you process evidence, you have the option of expanding EVTX log files. The options are turned off by default. See Evidence Processing Options on page 88. See Using Additional Analysis on page 147.

If you expand EVTX files into separate event objects, you can also use the following columns in the File List:

- EVTX Event Channel
- EVTX Event Computer
- EVTX Event Data
- EVTX Event ID
- EVTX Event Level
- EVTX Event Source
- EVTX Event Source Name
- EVTX Event User ID

If you expand data, you will have files are generated when the data was processed and was not part of the original data. There are tools to help you identify generated data.
See Identifying Processing-Generated Data on page 452.
See Relating Generated Files to Original Files on page 452.

To view EVTX log files
1. In the Examiner, click Overview.
2. In Case Overview, do one of the following:
   - View by file extension:
     - Click File Extension.
     - If present, click evtx.
   - View by file category:
     - Click File Category.
     - If present, click Windows EVTX Event Log.
3. If your case has any EVTX files, they are displayed in the File List.
4. Click an EVTX file to view the data in the Natural tab.

Some log files may not contain any events and you will only see the heading EVTX Events.

To expand EVTX log files into individual event records
1. In the Examiner, click Evidence > Additional Analysis.

See Using Additional Analysis on page 147.
2. Under Miscellany, select Expand Compound Files.
3. Click Expansion Options.
4. Select EVTX.
5. Click OK to save the expansion settings.
6. Click OK to process the evidence to expand EVTX files.

To view individual event records
1. In the Examiner, click Overview.
2. In Case Overview, Click File Category.
3. If present, click Windows EVTX Event.
4. If your case has any event records, they are displayed in the File List.
5. Click an event record to view the data in the Natural tab.

**To add EVTX-related columns in the File List**

- To add EVTX-related columns in the File List, add the EVTX-related columns to a new or existing column template.

See [Managing Columns](#) on page 613.
These columns will display data only for the expanded individual events, not for the EVTX log files.

**Viewing IIS Log File Data**

You can view data that is contained in IIS log files in HTML format in the Natural tab of the File Contents Pane.
You can also process IIS log files so that they are broken into individual records and interspersed with other items to support timeline analysis. To process IIS log files, there is a new IIS LOG check box in Evidence Processing Options > Expansion Options. This option is not enabled by default.

You can view IIS log data in one of two ways:

---

**View the log file data**

In the File List, you can see a list of IIS log files. When you view a log file, in the File Content pane, you can view the information that are contained in that one file. There can be a lot of data contained in one file.

**Expand log file data out as individual records**

When you expand IIS log files, each record is extracted. As a result, in the File List, each record is shown as its own item.
When you process evidence, you have the option of expanding IIS log files. The options is turned off by default.
See [Evidence Processing Options](#) on page 88.
See [Using Additional Analysis](#) on page 147.

If you expand IIS log files into separate records, you can also use the following columns in the File List:

- c-ip
- cs(Cookie)
- cs(Referer)
- cs(User-Agent)
- cs-bytes
- cs-host
- cs-method
- cs-uri-query
- cs-uri-stem
- cs-username
- s-computername
- s-ip
- s-port
- s-sitename
- sc-bytes
- sc-status

If you expand data, you will have files are are generated when the data was processed and was not part of the original data. There are tools to help you identify generated data. See Identifying Processing-Generated Data on page 452. See Relating Generated Files to Original Files on page 452.

**To expand IIS log files into individual records**

1. In the Examiner, click Evidence > Additional Analysis.

See Using Additional Analysis on page 147.

2. Under Miscellany, select Expand Compound Files.

3. Click Expansion Options.

4. Select IIS Log.

5. Click OK to save the expansion settings.

6. Click OK to process the evidence to expand the files.

**To add IIS log-related columns in the File List**

- To add IIS log-related columns in the File List, add the IIS log-related columns to a new or existing column template.

See Managing Columns on page 613.

These columns will display data only for the expanded individual records, not for the IIS log files.
Viewing Registry Timeline Data

You can view registry additional data in HTML format in the Natural tab of the File Contents Pane to support timeline analysis.

You can process Registry data files so that they are broken into individual records so they are interspersed with other items to support timeline analysis. To process Registry data, there is a new Registry check box in Evidence Processing Options > Expansion Options. This option is not enabled by default.

The following registry areas are supported:

- **SAM:**
  - SAM\Domains\Account\Users

- **NTUSER.DAT:**
  - Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count
  - Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{5E6AB780-7743-11CF-A12B-00AA004AE837}\Count
  - Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count
  - Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F\Count
  - Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\CIDSizeMRU
  - Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\FirstFolder
  - Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedPidlMRU
  - Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedPidlMRULegacy
Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidlMRU

You can view Registry data in one of two ways:

<table>
<thead>
<tr>
<th>View the Registry data</th>
<th>In the File List, you can view Registry files.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expand Registry data out as individual records</td>
<td>When you expand Registry data, each record is extracted. As a result, in the File List, each record is shown as its own item. When you process evidence, you have the option of expanding Registry data. The options is turned off by default. See Evidence Processing Options on page 88. See Using Additional Analysis on page 147.</td>
</tr>
</tbody>
</table>

If you expand Registry data into separate records, you can also use the following columns in the File List:

- Registry Action Description
- Registry Action Name
- Registry Action Type
- Registry File

If you expand data, you will have files are generated when the data was processed and was not part of the original data. There are tools to help you identify generated data. See Identifying Processing-Generated Data on page 452. See Relating Generated Files to Original Files on page 452.

**To expand Registry data into individual records**

1. In the Examiner, click Evidence > Additional Analysis.

2. Under Miscellany, select Expand Compound Files.

3. Click Expansion Options.

4. Select Registry.

5. Click OK to save the expansion settings.

6. Click OK to process the evidence to expand the files.
To add Registry-related columns in the File List

- To add Registry-related columns in the File List, add the Registry-related columns to a new or existing column template.

See Managing Columns on page 613.
These columns will display data only for the expanded individual records.

Viewing Log2Timeline CSV File Data

You can view data that is contained in CSV files that are in the Log2timeline format. You can view the data in the
Natural view of the File Content pane.
The individual records from the CSV will be interspersed with other data, giving you the ability to perform more advanced timeline analysis across a very broad set of data. In addition you can leverage the visualization engine to perform more advanced timeline based visual analysis.

To process CSV files, there is a new Log2tCSV check box in Evidence Processing Options > ExpansionOptions. This option is not enabled by default.
You can view CSV data in one of two ways:

<table>
<thead>
<tr>
<th>View the original CSV files</th>
<th>In the File List, you can see a list CSV files. When you select a file, you can view the information that is contained in each file in the File Content pane.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expand log file data out as individual records</td>
<td>When you expand CSV files, each record is extracted. As a result, in the File List, each record is shown as its own item.</td>
</tr>
<tr>
<td></td>
<td>When you process evidence, you have the option of expanding CSV files. The options is turned off by default.</td>
</tr>
<tr>
<td></td>
<td>See Evidence Processing Options on page 88. See Using Additional Analysis on page 147.</td>
</tr>
<tr>
<td></td>
<td>If you expand CSV files into separate records, you can also use columns to view each CSV field.</td>
</tr>
<tr>
<td></td>
<td>See the table Log2timeline CSV fields (page 461)</td>
</tr>
</tbody>
</table>
If you expand data, you will have files are are generated when the data was processed and was not part of the original data. There are tools to help you identify generated data. See Identifying Processing-Generated Data on page 452. See Relating Generated Files to Original Files on page 452.

To view the un-expanded CSV files
1. In the Examiner, click the Overview tab.
2. Expand File Category.
3. If CSV files exist in your evidence, you can expand Other Known Types > Log2t CSV logs. A list of Log2t CSV files is displayed in the File List.
4. Click a file to view the un-expanded data.

To expand CSV files into individual records
1. In the Examiner, click Evidence > Additional Analysis.

See Using Additional Analysis on page 147.
2. Click Miscellaneous
3. Under Miscellany, select Expand Compound Files.
4. Select Expand Compound Files.
5. Click Expansion Options.
6. Select Log2t CSV.
7. Click OK to save the expansion settings.
8. Click OK to process the evidence to expand the files.

To add CSV-related columns in the File List
1. In the Examiner, click the Column Settings icon. See Managing Columns on page 613.
2. Either create a new column template or edit an existing one.
3. In the Available Columns list, expand Log2T.
4. Add the desired columns to the template.
5. Click OK.
6. Select the template name you just configured.
7. Click Apply.
This applies the template to the File List.

8. Click Close.

9. In the Overview tab, expand **File Category > Other Known Types > Log2t CSV log entry**. A list of Log2t entries is displayed in the **File List**.

You will see the data in the columns for each record.
These columns will display data only for the expanded individual records, not for the original CSV files.
**Log2timeline CSV fields**

- **Log2t Desc**  
  A description field, this is where most of the information is stored. This field is the full description of the field, the interpreted results or the content of the actual log line.

- **Log2t Extra**  
  Additional information parsed is joined together and put here. This 'extra' field may contain various information that further describe the event. Some input modules contain additional information about events, such as further divide the event into source IP's, etc. These fields may not fit directly into any other field in the CSV file and are thus combined into this 'extra' field.

- **Log2t Filename**  
  The full path of the filename that contained the entry. In most input modules this is the name of the log file or file being parsed, but in some cases it is a value extracted from it, in the instance of $MFT this field is populated as the name of the file in question, not the $MFT itself.

- **Log2t Format**  
  The name of the input module that was used to parse the file. If this is a log2timeline input module that produced the output it should be of the format `Log2t::input::NAME` where name is the name of the module. However other tools that produce l2t_csv output may put their name here.

- **Log2t Host**  
  The hostname associated with the entry, if one is available.

- **Log2t Inode**  
  The inode number of the file being parsed, or in the case of $MFT parsing and possibly some other input modules the inode number of each file inside the $MFT file.

- **Log2t MACB**  
  The MACB or legacy meaning of the fields, mostly for compatibility with the `mactime` format.

- **Log2t Notes**  
  Some input modules insert additional information in the form of a note, which comes here. This might be some hints on analysis, indications that might be useful, etc. This field might also contain URL's that point to additional information, such as information about the meaning of events inside the EventLog, etc.

- **Log2t Short**  
  The short description of the entry, usually contains less text than the full description field. This is created to assist with tools that try to visualize the event. In those output the short description is used as the default text, and further information or the full description can be seen by either hovering over the text or clicking on further details about the event.

- **Log2t Source**  
  The short name for the source. This may be something like LOG, WEBHIST, REG, etc. This field name should correspond to the type field in the TLN output format and describe the nature of the log format on a high level (all log files are marked as LOG, all registry as REG, etc.)

- **Log2t SourceType**  
  A more comprehensive description of the source. This field further describes the format, such as "Syslog" instead of simply "LOG", "NTUSER.DAT Registry" instead of "REG", etc.
• **Log2t User**  The username associated with the entry, if one is available.

• **Log2t Version**  The version number of the timestamp object.
Identifying Document Languages

When processing evidence, you can perform automatic language identification. This will analyze the first two pages of every document to identify the language that is contained within.

To identify languages, you enable the Language Identification processing option.

See Evidence Processing Options on page 88. See Using Additional Analysis on page 147.

After processing is complete, you can add the Language column in the File List in the Examiner. See Managing Columns on page 613.

You can filter by the Language field within review and determine who needs to review which documents based on the language contained within the document.

If there are multiple languages in a document, the first language will be identified.

This feature is enabled by selecting a new Language Identification processing option. When you enable Language Identification, you have the following options:

- **Document Types to process** - You can select to process the following file types:
  - Documents
  - Presentation
  - Spreadsheets
  - Email
- **The languages to identify** - You can select to identify the following:
  - Basic languages that include English, Chinese, Spanish, Japanese, Portuguese, Arabic, French, Russian, and Korean.
  - Extended languages. Performs language identification for 67 different languages. This is the slowest processing option.

**Note:** The Language Identification processing option is disabled by default. If you enable it, the basic languages setting and all four document types are enabled by default.
Basic Languages

The system will perform language identification for the following languages:

- Arabic
- Chinese
- English
- French
- German
- Japanese
- Korean
- Portuguese
- Russian
- Spanish

If the language to identify is one of the ten basic languages (except for English), select Basic when choosing Language Identification. The Extended option also identifies the basic ten languages, but the processing time is significantly greater.
The system will perform language identification for 67 different languages. This is the slowest processing option. The following languages can be identified:

<table>
<thead>
<tr>
<th>Afrikaans</th>
<th>Albanian</th>
<th>Amharic</th>
<th>Arabic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Armenian</td>
<td>Basque</td>
<td>Belarusian</td>
<td>Bosnian</td>
</tr>
<tr>
<td>Breton</td>
<td>Bulgarian</td>
<td>Catalan</td>
<td>Chinese</td>
</tr>
<tr>
<td>Croatian</td>
<td>Czech</td>
<td>Danish</td>
<td>Dutch</td>
</tr>
<tr>
<td>English</td>
<td>Esperanto</td>
<td>Estonian</td>
<td>Finnish</td>
</tr>
<tr>
<td>French</td>
<td>Georgian</td>
<td>German</td>
<td>Greek</td>
</tr>
<tr>
<td>Hawaiian</td>
<td>Hebrew</td>
<td>Hindi</td>
<td>Hungarian</td>
</tr>
<tr>
<td>Icelandic</td>
<td>Indonesian</td>
<td>Irish</td>
<td>Italian</td>
</tr>
<tr>
<td>Japanese</td>
<td>Korean</td>
<td>Latin</td>
<td>Latvian</td>
</tr>
<tr>
<td>Lithuanian</td>
<td>Malay</td>
<td>Manx</td>
<td>Marathi</td>
</tr>
<tr>
<td>Nepali</td>
<td>Norwegian</td>
<td>Persian</td>
<td>Polish</td>
</tr>
<tr>
<td>Portuguese</td>
<td>Quechua</td>
<td>Romanian</td>
<td>Rumantsch</td>
</tr>
<tr>
<td>Russian</td>
<td>Sanskrit</td>
<td>Scots</td>
<td>Scottish Gaelic</td>
</tr>
<tr>
<td>Serbian</td>
<td>Slovak</td>
<td>Slovenian</td>
<td>Spanish</td>
</tr>
<tr>
<td>Swahili</td>
<td>Swedish</td>
<td>Tagalong</td>
<td>Tamil</td>
</tr>
<tr>
<td>Thai</td>
<td>Turkish</td>
<td>Ukrainian</td>
<td>Vietnamese</td>
</tr>
<tr>
<td>Welsh</td>
<td>Yiddish</td>
<td>West Frisian</td>
<td></td>
</tr>
</tbody>
</table>
Language Translation

When processing evidence, you can perform automatic language translation. This will analyze documents using SDL machine learning technologies. The supported languages will depend on the license you have, and will depend on the key pairs supported.

Prerequisites
1. SDL Language Translation must be installed.
   - Refer to the KB article: RWS Translation – Installation & Configuration Guide.
2. A valid SDL license is required.

How to Configure and use the Language Translation processing option
1. Do one of the following:
   - For new cases, in the New Case Options dialog click Customize.
   - For existing cases, in the Examiner, click Evidence > Additional Analysis.
2. Check Language Translation.
3. Click Language Translation Options.
4. Click Configure.
5. Enter the following:
   - Server URL
   - Port Number
   - API Key
6. Click OK.
Examining Miscellaneous Evidence

Examining Internet Artifact Data

You can examine detailed information about the internet artifact data in your case. At a basic level, when evidence is processed, internet artifact files from across all parsed browser archives in the data set are categorized and organized into one examiner tab so that you can easily review them.

Using the Enhanced Internet Artifact Parser

Prerequisites

1. The ExterroSelfHostService must be running.
2. During processing, Expand Compound Files >> Expansion Options >> Categories: Browsers needs to have all applicable browser data types selected.

How to use the Enhanced Internet Artifact Parser

1. After checking prerequisites above, open your case in the Case Examiner interface.
2. Navigate to Tools >> Enhanced Internet Artifact Parser
3. The Data Processing Status window appears.
4. On the Other Jobs view, wait for the internet data parser processing jobs to complete.
5. Once complete, the Internet tab will be populated with additional web artifact insights.
**Internet Artifact Reference List**

For example, using these views, you can quickly see the following files:

- **AOL**:
  - AOL ABY files
  - AOL Buddy List
  - AOL User History
- **Chrome Browser**:
  - Bookmark files
  - Cookies files
  - History files
- **Internet Explorer**:
  - MSIE Cookie Index files
  - MSIE History files
- **Microsoft Live Messenger Log files**
- **Mozilla**
  - Address Book files
  - Cookie Index files
  - History files
  - Mozilla Thunderbird email files
- **Skype**
  - Skype Data
  - Skype Files
- **Web-based email providers**
  - Flashmail
  - Foxmail
- **Yahoo IM conversation files**
- **mail.ru agent history files (Mra.dbs)**:
  - User account information and encrypted account password

From the registry at HKCU\Software\Mail.Ru\Agent\magent_logins3\*

- Parsed contacts and messages from mra.dbs files
Each message contains a plain-text and an RTF version, both UTF16LE.

- Contact list from the inbox.ru.xml.

For many of these files, you can view information from the files in the Natural view. For example, you can see an AOL Buddy List or the contents of a Yahoo IM conversation. Some internet artifact information is stored in SQLite tables. Most of these tables are viewable in the Natural view.

**About Extensible Storage Engine (ESE) Databases**

Extensible Storage Engine (ESE) databases are used by many Microsoft components as well as other programs to store and retrieve data. Some of these components include:

- MS Exchange Server (2007)
- MS Exchange Server (2010)
- Active Directory
- Windows Live Server
- Desktop Search (Vista and Windows 7)
- IE 10 Web Data (for example, history, cookies, cache, and so forth)
- SRS (Site Replication Service) Template
- Windows Help Center
- Windows Update
- Windows System Update
- Windows Server Security
- Windows Server WINS
- Windows Server DHCP
- NT File Replication Service

These ESE databases are expanded when processing evidence (if selected in the Expansion Options) and displayed in Evidence Groups. Most of the ESE databases appear in File Category > Databases. The exception is Exchange ESE databases, which appear in File Category > Email. Internet Explorer version 10 or later also use ESE databases to store data like the internet history, cookies, cache, and so forth. (See About Expanding Data from Internet Explorer (IE) Version 10 or Later on page 467.)
To expand the ESE Databases into individual records
1. In the Examiner, click Evidence > Additional Analysis.

See Using Additional Analysis on page 147.
2. Click Miscellaneous
3. Under Miscellany, select Expand Compound Files.
4. Select Expand Compound Files.
5. Click Expansion Options.
6. Verify that ESE DB is selected.
7. Click OK to save the expansion settings.
8. Click OK to process the evidence to expand the files.

About Expanding Google Chrome, Firefox, and IE 9 Data
There are advanced processing options that will expand the basic Google Chrome, Mozilla Firefox, and Internet Explorer data. You can do the following:
- Expand Google Chrome and Mozilla Firefox SQLite tables and IE 9 IE.DAT files to create individual records.

This provides investigators the ability to bookmark specific records from within the tables. For example, if you are looking for a specific Top Site record, you can more easily find and bookmark the record you need.
- Reconstruct web pages.

When viewing either Cache or History entries, if enough data is stored in the cache, you can see the reconstructed web page that was cached when the user was browsing the respective web site.
The following table lists the expanded data that you can view:
### Internet Artifact Expanded Data

<table>
<thead>
<tr>
<th>Browser</th>
<th>Data Components</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chrome</td>
<td>Cache Index Data</td>
</tr>
<tr>
<td></td>
<td>• Cookies</td>
</tr>
<tr>
<td></td>
<td>• Downloads</td>
</tr>
<tr>
<td></td>
<td>• History</td>
</tr>
<tr>
<td></td>
<td>• Top Sites</td>
</tr>
<tr>
<td></td>
<td>• Key Words</td>
</tr>
<tr>
<td></td>
<td>• Web Autofill Data</td>
</tr>
<tr>
<td>Firefox</td>
<td>Bookmarks</td>
</tr>
<tr>
<td></td>
<td>• Cache Index Data</td>
</tr>
<tr>
<td></td>
<td>• Cookies</td>
</tr>
<tr>
<td></td>
<td>• Favorites</td>
</tr>
<tr>
<td></td>
<td>• Form History</td>
</tr>
<tr>
<td></td>
<td>• History</td>
</tr>
<tr>
<td>Internet Explorer 9</td>
<td>IE Cache Entries</td>
</tr>
<tr>
<td></td>
<td>• IE Cookies Entries</td>
</tr>
<tr>
<td></td>
<td>• IE History Entries</td>
</tr>
<tr>
<td></td>
<td>• IE Download Entries</td>
</tr>
</tbody>
</table>

• MSIE Recovery dat Entries
When viewing the expanded data, you can use the following columns in the File List to display detailed data.

**Internet History Columns**

<table>
<thead>
<tr>
<th>Action URL</th>
<th>Autofill Name</th>
<th>Autofill Value</th>
<th>Bytes Downloaded</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cookie Name</td>
<td>Cookie Path</td>
<td>Cookie Value</td>
<td>Count</td>
</tr>
<tr>
<td>Duration</td>
<td>Encrypted Card Number</td>
<td>End Time</td>
<td>Expiration Month</td>
</tr>
<tr>
<td>Expiration Time</td>
<td>Expiration Year</td>
<td>File Path</td>
<td>Google Profile Address</td>
</tr>
<tr>
<td>Google Profile City</td>
<td>Google Profile Company Name</td>
<td>Google Profile Country</td>
<td>Google Profile Country Code</td>
</tr>
<tr>
<td>Google Profile Email Address</td>
<td>Google Profile First Name</td>
<td>Google Profile Last Name</td>
<td>Google Profile Middle Name</td>
</tr>
<tr>
<td>Google Profile Phone Number</td>
<td>Google Profile State</td>
<td>Host Key</td>
<td>Last Updated Time</td>
</tr>
<tr>
<td>Last Visit Time</td>
<td>Name on Card</td>
<td>Offline User Email</td>
<td>Opened</td>
</tr>
<tr>
<td>Origin URL</td>
<td>Password Element</td>
<td>Password Value</td>
<td>Rank</td>
</tr>
<tr>
<td>Redirects to</td>
<td>Start Time</td>
<td>Terms</td>
<td>This Visit Time</td>
</tr>
<tr>
<td>Types Times</td>
<td>URL</td>
<td>URL has HTML</td>
<td>Username Element</td>
</tr>
<tr>
<td>Username Value</td>
<td>Visit Times</td>
<td>Zip Code</td>
<td></td>
</tr>
</tbody>
</table>

See **Managing Columns** on page 613.
See **Icons of the File List Tool Bar** on page 406.

If you expand internet artifact data, you will have files are are generated when the data was processed and was not part of the original data. There are tools to help you identify generated data.

See **Identifying Processing-Generated Data** on page 452. See **Relating Generated Files to Original Files** on page 452.
About Expanding Data from Internet Explorer (IE) Version 10 or Later

Data from Internet Explorer (IE) 10 is stored in a database called WebCacheV01.dat. This file is an ESE (Extensible Storage Engine) database that points to IE 10's cached files. When expanded in Examiner, you can view the following data:

**Internet Artifact Expanded Data**

- Internet Explorer 10
- IE Web Cache Compatibility Entries
  - IE Web Cache Content Entries
  - IE Web Cache Cookie Entries
  - IE Web Cache DOM Store Entries
  - IE Web Cache Download Entries
  - IE Web Cache RSS Feed Entries
  - IE Web Cache History Entries
  - Other Web Cache Entries

This data displays in the Overview tab under Internet/Chat Files or in the Internet tab.

IE 10 (and later) WebCache Data on a Live System

You cannot expand or display Internet Explorer 10 (or later) WebCache data from a live system. WebCache data is locked by the Windows operating system and does not display correctly in the Examiner.

About Internet Artifact Processing Options

To expand internet artifact data, you enable processing options either when you add the evidence or later by using Additional Analysis.

---

**Note:** The IE WebCache contains many files and can take additional time to expand. Therefore, IE WebCache is not selected by default.

**Important:** Expanding internet artifact data can add a significant amount of data to your evidence.

See Evidence Processing Options on page 88. See Using Additional Analysis on page 147.
### Internet Artifact Processing Options

<table>
<thead>
<tr>
<th>Browser</th>
<th>Expand Compound Files</th>
<th>Additional Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chrome</td>
<td>• Expand Compound Files &gt; Chrome Bookmarks  &lt;br&gt;• Expand Compound Files &gt; Chrome Cache  &lt;br&gt;• Expand Compound Files &gt; Chrome SQLite  &lt;br&gt;• Expand Compound Files &gt; Chrome JSON  &lt;br&gt;• Expand Compound Files &gt; Chrome LevelDB  &lt;br&gt;• Expand Compound Files &gt; Chrome SNSS</td>
<td>• Unselected by default</td>
</tr>
<tr>
<td>Firefox</td>
<td>• Expand Compound Files &gt; Firefox Cache  &lt;br&gt;• Expand Compound Files &gt; Firefox SQLite  &lt;br&gt;• Expand Compound Files &gt; Firefox JSON</td>
<td>• Unselected by default</td>
</tr>
<tr>
<td>Internet Explorer Files (IE 9)</td>
<td>• Expand Compound Files &gt; Internet Explorer Files (IE 9)</td>
<td>• Unselected by default</td>
</tr>
<tr>
<td>Internet Explorer 10 or later</td>
<td>• Expand Compound Files &gt; Internet Explorer  &lt;br&gt;• Expand Compound Files &gt; IE Recovery  &lt;br&gt;• Expand Compound Files &gt; IE WebCache</td>
<td>• Selected by default  &lt;br&gt;• Unselected by default. This lets you expand IE Recovery data that was stored when access to a Web site was lost.  &lt;br&gt;• Unselected by default.</td>
</tr>
<tr>
<td>Edge</td>
<td>• Expand Compound Files &gt; Edge Bookmarks  &lt;br&gt;• Expand Compound Files &gt; Edge Cache  &lt;br&gt;• Expand Compound Files &gt; Edge SQLite</td>
<td>• Unselected by default</td>
</tr>
<tr>
<td>Safari</td>
<td>• Expand Compound Files &gt; Safari Plist  &lt;br&gt;• Expand Compound Files &gt; Safari  &lt;br&gt;• Expand Compound Files &gt; SQLite</td>
<td>• Unselected by default</td>
</tr>
</tbody>
</table>
About Viewing Internet Artifact Data

After you have expanded the artifact data, you can view the data in the Examiner. You can view expanded data in one of the following ways:

- Clicking an individual file and viewing the contents in the Natural view. For most items, you will see the data displayed in a table.
  - Viewing Reconstructed web pages

For history and cache entries, if enough data exists, the reconstructed web page appears. If enough data is not available, informational data appears instead. You can use the URL has HTML column to help you determine which files can be reconstructed.

- Adding columns to the File List that displays expanded data.

You can add columns for all of the expanded items that is generated. A sample is listed in the InternetHistory Columns table above.

You can view a list of all of the Internet History columns by looking at the Internet History column group in the column manager.

See Managing Columns on page 613.

In the Internet/Chat files folder, the files are organized as follows:

- Chrome:
  - Original Chrome artifact files are stored under the Chrome Browser Files folder
  - The expanded data is stored under the Chrome Browser Data folder.
- Firefox:
  - Original Firefox artifact files are stored under the Firefox Files folder
  - The expanded data is stored under the Firefox Browser Data folder.
- IE
  - Original IE artifact files are stored under the Internet Explorer Browser Files folder
  - The expanded data is stored under the Internet Explorer Browser Data folder.
Expanding Internet Artifact Data

To expand internet artifact data

1. When either adding evidence to a case or performing Additional Analysis, access the processing options.

See Evidence Processing Options on page 88.

See Using Additional Analysis on page 147.

2. Select the option to Expand Compound Files.

3. Click Expansion Options.

4. Select one or more of the following options:
   - Chrome:
     - Chrome Bookmarks
     - Chrome Cache
     - Chrome SQLite
   - Firefox:
     - Firefox Cache
     - Firefox SQLite
   - IE:
     - IE Cookie Text
     - IE Recovery
     - IE WebCache
     - Internet Explorer Files
   - Skype SQLite

See About Internet Artifact Processing Options on page 468.

5. Process your data.
Mobile Phone Columns

Viewing Internet Artifact Data

To view expanded internet data in the Natural view

1. In the examiner, open one of the following: (Both tabs display the same data.)
   - The Overview tab > File Category > Internet/Chat Files

---

Note: Chrome and Firefox SQLite files are also located in Internet/Chat Files.

- The Internet tab

2. For Chrome files, expand Chrome Browser > Chrome Browser Data.
3. For Firefox files, expand Mozilla Files > Firefox Browser > Firefox Browser Data.
4. For IE files, expand Internet Explorer Browser > Internet Explorer Browser Data.
5. Select a folder, such as Cookies.
6. Click an item in the File List.

The cookie’s data is displayed in the Natural view.

7. Click History.
8. Click an item in the File List.

If possible, the reconstructed web page will be shown. If insufficient data exists, informational data will be shown instead.

9. You can perform a search for a specific value in the Natural view by clicking CTRL-F.

To view expanded internet data using columns

1. In the examiner, open one of the following: (Both tabs display the same data.)
   - The Overview tab > File Category > Internet/Chat Files
   - The Internet tab

2. Click the Column Settings icon.

See Managing Columns on page 613.

3. Either create a new column template or edit an existing one.
4. In the Available Columns list, expand Data.
5. Add the desired columns to the template.
Mobile Phone Columns
For example, to add columns for Chrome or Firefox browser history data, use the following:

- URL
- Visit Times
- Typed Times
- Last Visit Time
- This Visit Time
- Duration
Mobile Phone Columns

6. Click OK.
7. Select the template name you just configured and click Apply. This applies the template to the File List.
8. Click Close.
9. Expand Browser > Browser Data for either Chrome or Firefox.
10. Click History.

In this example, you will see the history data in the columns for each record.

Examining Mobile Phone Data

You can examine detailed information about the mobile phone data in your case using the dedicated Mobile Data tab.

The mobile phone data that you can see comes from the following sources:

- AD1 files from AccessData Mobile Phone Examiner
- Cellebrite UFDR report files
- Cellebrite UFD files

See Working with Cellebrite UFDR Images on page 479.
- XRY data extraction archives.

At a basic level, when evidence is processed, mobile phone files are categorized and organized so that you can easily see them. You can use the Mobile Data or Overview tabs to quickly view data specific to mobile phones:
- The Mobile Data tab
- The Overview tab > File Category > Mobile Phone
Mobile Phone Columns
For example, using these views, you can quickly see the following files:

- Mobile Phone Data
  - Bookmark
  - Call History
  - Cookie
  - Powering Event
  - SMS Messages
  - Web History
- Mobile Phone Files
  - Cellebrite Files

For many of these files, you can view information from the files in the Natural view. For example, you can see artifacts for the Call History or the contents of an SMS Message. Some mobile phone information is stored in SQLite tables. Most of these tables are viewable in the Natural view.

Note: The files listed in the Mobile Phone Data section are specific to the particular mobile phone image you have processed, and will be different for each mobile phone image.

There are many files found on mobile phones that are not specific to the Mobile Phone file category. This data could include, but is not limited to, the following file categories:

- Archives
- Databases
- Documents
- Folders
- Graphics

These files can also be viewed by using the Overview tab.
Mobile Phone Columns

Requirements for Mobile Image Ingestion:

- Mobile Image formats such as UFD, Grayshift Images, ZIP, TAR, AB require users to ingest them as Individual Files. Prompts to create an AD1 image of the mobile data is not required, users can dismiss this prompt.

- Mobile Image formats such as BIN or UFD, Grayshift Images, ZIP, TAR, AB stored within an AD1 or E01 image, require users to ingest them as Acquired Images.

- Grayshift images must be located in the same directory as the associated .plist file.
  - Grayshift images and associated .plist files must have the same file name.

- To populate mobile data within the System Summary tab, users must ensure the Generate System Summary option is selected during processing.
Using the Exterro Mobile Parser

The Exterro Mobile Parser succeeds the Chat Application Parser and now supports a number of chat applications on mobile devices. The list below shows the currently supported applications:

<table>
<thead>
<tr>
<th>Application</th>
<th>Android</th>
<th>iOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Android Messages</td>
<td>Latest</td>
<td>Not Applicable</td>
</tr>
<tr>
<td>Discord</td>
<td>Not Applicable</td>
<td>Latest</td>
</tr>
<tr>
<td>Facebook messenger</td>
<td>386.2.0.22.106</td>
<td>Latest</td>
</tr>
<tr>
<td>Google Chat / Hangouts</td>
<td>Latest</td>
<td>Latest</td>
</tr>
<tr>
<td>IMOPlus</td>
<td>2022.11.1051</td>
<td>Latest</td>
</tr>
<tr>
<td>Instagram</td>
<td>261.0.0.21.111</td>
<td>Latest</td>
</tr>
<tr>
<td>iOS Messages (iOS)</td>
<td>Not Applicable</td>
<td>Latest</td>
</tr>
<tr>
<td>KakaoTalk</td>
<td>9.9.7</td>
<td>Latest</td>
</tr>
<tr>
<td>Kik</td>
<td>15.48.1.27323</td>
<td>Latest</td>
</tr>
<tr>
<td>Line</td>
<td>12.19.1</td>
<td>Latest</td>
</tr>
<tr>
<td>Signal</td>
<td>Latest</td>
<td>Latest</td>
</tr>
<tr>
<td>Skype</td>
<td>8.89.0.403</td>
<td>Latest</td>
</tr>
<tr>
<td>Slack</td>
<td>22.11.30.0</td>
<td>Latest</td>
</tr>
<tr>
<td>Snapchat</td>
<td>12.08.0.29</td>
<td>Latest</td>
</tr>
<tr>
<td>Telegram</td>
<td>916</td>
<td>Latest</td>
</tr>
<tr>
<td>Threema</td>
<td>4.84</td>
<td>Latest</td>
</tr>
<tr>
<td>Tinder (Partial Support)</td>
<td>Latest</td>
<td>Latest</td>
</tr>
<tr>
<td>Twitter</td>
<td>9.65.6-release.0</td>
<td>Latest</td>
</tr>
<tr>
<td>Viber</td>
<td>18.9.2.0</td>
<td>Latest</td>
</tr>
<tr>
<td>WeChat (Partial Support)</td>
<td>Latest</td>
<td>Latest</td>
</tr>
<tr>
<td>WhatsApp</td>
<td>2.22.23.84</td>
<td>Latest</td>
</tr>
</tbody>
</table>

While FTK supports parsing of mobile images, the file counts may slightly differ to third party solutions.

How to use the Exterro Mobile Parser

1. The ExterroSelfHostService must be running.
2. During processing, Expand Compound Files >> Expansion Options >> Exterro Mobile Parser selected.
3. The Data Processing Status window appears.
4. On the Other Jobs view, wait for the chat application data processing job to complete.
5. Once complete, the Mobile tab will be populated with additional mobile phone data insights.
Mobile Phone Columns

About Expanding Mobile Phone Data
When viewing the expanded mobile phone data, you can use the following columns in the File List to display detailed data.

Mobile Phone Columns

Android Columns Groups

- Mobile Application Icon Layout(Android)
- Mobile Calendar Event List(Android)
- Mobile Device Account Information(Android)
- Mobile Device Application Permission(Android)
- Mobile Device Application Usage(Android)
- Mobile Device Avatar(Android)
- Mobile Device Bluetooth Information(Android)
- Mobile Device Calendar Information
- Mobile Device Call Information(Android)
- Mobile Device Contact Information(Android)
- Mobile Device Contact Number(Android)
- Mobile Device Contact Organisation(Android)
- Mobile Device Contact Website (Android)
- Mobile Device Contact(Android)
- Mobile Device ContactGroup(Android)
- Mobile Device Email Address(Android)
- Mobile Device Email Attachment(Android)
- Mobile Device File System Entry(Android)
- Mobile Device GMap Direction(Android)
- Mobile Device GMap Location(Android)
- Mobile Device Information(Android)
- Mobile Device Journey Step(Android)
- Mobile Device SMS/ MMS(Android)
- Mobile Device WiFi Information(Android)
- Mobile File Download(Android)
Mobile Phone Columns

- Mobile Google Assistant(Android)
- Mobile Google Cello(Android)
- Mobile Google Document(Android)
- Mobile Google Photo Local(Android)
- Mobile Google Photo Media (Android)
- Mobile Google Playstore Installed Application(Android)
- Mobile Google Playstore (Android)
- Mobile Nearby Share(Android)
- Mobile Secure Setting(Android)
- Mobile SIM Card(Android)

Ios Column Groups

- Mobile Activity Level(iOS)
- Mobile Address Book Contact(iOS)
- Mobile Airdrop Background Activity(iOS)
- Mobile Airdrop Discoverability(iOS)
- Mobile App Installation Activities(iOS)
- Mobile Apple Maps(iOS)
- Mobile Application Activities(iOS)
- Mobile Application Permission(iOS)
- Mobile Application Usage(iOS)
- Mobile Audio Notes(iOS)
- Mobile Battery Level(iOS)
- Mobile Bluetooth Paired Devices(iOS)
- Mobile Cached Locations(iOS)
- Mobile Calendar Entry(iOS)
- Mobile Call Information(iOS)
- Mobile Cell Tower Location(iOS)
- Mobile Connected Account(iOS)
- Mobile Contact(iOS)
Mobile Phone Columns

- Mobile Credit Card Records(iOS)
- Mobile DataUsage SQLite(iOS)
- Mobile Device Audio Playback(iOS)
- Mobile Device Autolock State(iOS)
- Mobile Device Backlight(iOS)
- Mobile Device Camera State(iOS)
- Mobile Device External Power Connected States(iOS)
- Mobile Device Information(iOS)
- Mobile Device Lock State(iOS)
- Mobile Do Not Disturb Settings(iOS)
- Mobile OS Store Records(iOS)
- Mobile Email Application Data(iOS)
- Mobile Generic Password Records(iOS)
- Mobile Health Heart Rate(iOS)
- Mobile Home Screen Layout(iOS)
- Mobile Installed Application(iOS)
- Mobile Intents(iOS)
- Mobile Interaction(iOS)
- Mobile Internet Password Records(iOS)
- Mobile Know-Lock States(iOS)
- Mobile Learned Locations(iOS)
- Mobile Map Route(iOS)
- Mobile NetUsage SQLite(iOS)
- Mobile Network Connectivity(iOS)
- Mobile Parked Vehicle Locations(iOS)
- Mobile Payment Cards(iOS)
- Mobile Payment Transaction List(iOS)
- Mobile Powerlog Application Usage(iOS)
- Mobile Powerlog Timezone Information(iOS)
- Mobile Process Data Usage(iOS)
Mobile Phone Columns

- Mobile Safari History(iOS)
- Mobile Screen Time Application Usage(iOS)
- Mobile Screen Time Synced Application(iOS)
- Mobile Sim Card Information(iOS)
- Mobile Stairs Climbed(iOS)
- Mobile Steps Taken(iOS - pedometer)
- Mobile System Version Information(iOS)
- Mobile Text Notes(iOS)
- Mobile Siri Usage(iOS)
- Mobile Visited Locations(iOS)
- Mobile Voice Mail(iOS)
- Mobile Walk Travel Distance(iOS)
- Mobile Web Usage(iOS)
- Mobile Wifi Connection Location(iOS)
- Mobile Wifi Information(iOS)
- Mobile Device Information(iOS)
- Mobile Device Orientation(iOS)

Message Column Groups

- Chat Conversations (Old)
- Messages
- Messages (Old)
- Messages - MMS Details
- Messages - SMS Details
- Mobile Chat Conversations
- Mobile Messages MMS

Other Column Groups

- Mobile Android Keystore
- Mobile App Usage
- Mobile App Usage (Old)
Mobile Phone Columns

- Mobile Browser Autofill
- Mobile Browser Bookmarks
- Mobile Browser Cloud Device
- Mobile Browser Favourite Icon
- Mobile Browser History
- Mobile Browser Payment Card
- Mobile Browser Session
- Mobile Browser Tab
- Mobile Browser Topsite
- Mobile Calendar
- Mobile Calls
- Mobile Cards
- Mobile Contacts
- Mobile Device
- Mobile Device Apps
- Mobile Device Call Log
- Mobile Device Contacts (Old)
- Mobile Device Event Attendee
- Mobile Device Events
- Mobile Device Notes
- Mobile Google Calendar
- Mobile Google Calendar Event
- Mobile Installed Apps
- Mobile Other Items
- Mobile Password Info
- Mobile Searched Items
- Mobile Searches
- Mobile User Accounts
- Mobile User Dictionary
- Mobile Wireless Network
Mobile Phone Columns

- SIM Cards
- WiFi History

<table>
<thead>
<tr>
<th>Note Summary</th>
<th>Note Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Task</td>
<td>Time</td>
</tr>
</tbody>
</table>

Viewing Mobile Phone Data

To view expanded mobile phone data in the Natural view

1. In the examiner, open the Mobile Data tab

2. Select a node, such as SMS Messages.

3. Click an item in the File List.

The data is displayed in the Natural view.

4. Click Mobile Phone Files.

5. Click Extraction Summary in the File List.

Details of the original mobile phone extraction will be shown.

6. You can perform a search for a specific value in the Natural view by clicking CTRL-F.
1. In the examiner, open the **Mobile Data** tab.

2. Click the Column Settings templates drop-down. There are six mobile phone templates available:
   - Mobile Device Apps
   - Mobile Device Call Log
   - Mobile Device Contacts
   - Mobile Device Events
   - Mobile Device MMS
   - Mobile Device SMS

3. Either create a new column template or edit an existing one. See *Managing Columns* on page 613.

4. In the Available Columns list, expand Mobile Phones.

5. Add the desired columns to the template.

   For example, to add columns for SMS Messages data, use the following:
   - SMS From
   - SMS From Number
   - SMS Service Center
   - SMS State
   - SMS Text
   - SMS Time Received
   - SMS Time Sent
   - SMS Time Zone of Sender
   - SMS To
   - SMS To Number
   - SMS Type

6. Click **OK**.

7. Select the template name you just configured and click **Apply**. This applies the template to the File List.

8. Click **Close**.

9. Apply the **Mobile Device SMS** column template.

10. Expand Mobile Phone > Mobile Phone Data.

11. Click SMS Messages.

   In this example, you will see the SMS data in the columns for each record.
To view expanded mobile phone data using filters

1. In the examiner, open the Mobile Data tab

2. Click the Filter dropdown. There are five mobile phone templates available:
   - Mobile Phone: Calendar
   - Mobile Phone: Call History
   - Mobile Phone: Messages
   - Mobile Phone: Phonebook
   - Mobile Phone Files

3. Either apply an existing filter or create a new one. See Managing Filters on page 58.

4. Once applied, you will see only those items allowable by the selected filter. The File List contents will also be highlighted yellow, showing a filter is applied.

**Standard Messaging Format**

The Web (HTML5) tab shows a realistic view of chat conversations. Conversations look more like they do on the original device, making it easier to view and to export information to third parties without having to append an explanation for the data.

During processing, be sure to select the All Communications option. This will mark any mobile conversations by default.

You can find the Web (HTML5) tab in the File Content panel, in the Natural view side tabs. The Web (HTML5) view is also available on the Index Search Tab.

**Important:** If a non-text item from a chat was not included in the evidence file, the unavailable item will be listed along with any relevant information. These could include items such as images, videos, voice recordings, locations, stickers, emojis, or other attachments.

The viewer has been implemented for the following chat conversations:

<table>
<thead>
<tr>
<th>Android SMS</th>
<th>Android MMS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cellebrite Chat</td>
<td>FB Messenger (Android)</td>
</tr>
<tr>
<td>Hangouts</td>
<td>Instagram (Android)</td>
</tr>
<tr>
<td>Kik (Android)</td>
<td>pidgin</td>
</tr>
<tr>
<td>Skype</td>
<td>Viber (Android)</td>
</tr>
</tbody>
</table>
WeChat (Android) • WeChat (iOS)
WhatsApp (Android) • WhatsApp (iOS)
• XRY Chat

Use the Chat Conversations column setting in the File List to see the most relevant data for these files. The type of chat will be listed in the Src (Source) column. It is possible to sort using this column to find data from a particular source.

**Applying the Standard Messaging Format**

**To view the data in Standard Messaging Format**
1. Navigate to the Internet tab.
2. Navigate to the desired folder in the evidence tree. Select a message in the File List.
3. In the File Content panel, select the Natural Tab at the top. Select the Web (HTML5) Tab on the right side.

The data will display in a similar format to the one used on the original device.

**Note:** It may be easier to use a different tab for certain types of mobile phone data.

**Working with Cellebrite UFDR Images**

About Expanding Cellebrite Data
To expand Cellebrite mobile phone data, you enable processing options either when you add the evidence or later by using Additional Analysis.

See Evidence Processing Options on page 88. See Using Additional Analysis on page 147.

Expanding Cellebrite Data

**To expand Cellebrite data**
1. When either adding evidence to a case or performing Additional Analysis, access the processing options.
See Evidence Processing Options on page 88.
See Using Additional Analysis on page 147.

2. Select the option to Expand Compound Files.

3. Click Expansion Options.

4. Click Clear All.

5. Select the Cellebrite UFDR option.

6. Process your data.

Expanding Cellebrite UFD Data

To expand Cellebrite data

1. When either adding evidence to a case or performing Additional Analysis, access the processing options.
   See Evidence Processing Options.
   See Using Additional Analysis.
2. Select the option to Expand Compound Files.
3. Click Expansion Options.
4. Click Clear All.
5. Select the Exterro Mobile Parser option.
   • In addition, System Summary can be selected to populate system information.
6. Process your data.
**Working with iOS Backup**

About Expanding iOS Backup Data
To expand iOS Backup data, you will need to enable the appropriate processing option either when you add the evidence or later by using Additional Analysis.

---

**Note:** You will need the user’s password in order to open any encrypted backup files. We currently do not decrypt iOS Backup files.

---

Expanding iOS Backup Data

**To Expand iOS Backup Data:**
1. During processing, or in Additional Analysis, open the Evidence Processing window.
2. Check the Expand Compound Files option.
3. Click on the Expansion Options box and check the box for iOS Backup.
4. Click Ok and process the evidence.

Locating iOS Backup Data

**To Locate iOS Backup Data:**
1. In the Explore Tab, open the evidence and navigate to the Manifest.db file.
2. Select any folder to view iOS Backup evidence.

**Important:** When looking at iOS Backup files in the Overview Tab, these files will not be classified as MobilePhone files. They will be classified as the standard file category for each type of file found on the phone.

*Working with Facebook Messenger (Android)*

To expand Facebook Messenger App data on an Android phone, you will need to enable the appropriate processing option either when you add the evidence or later by using Additional Analysis.
Expanding Facebook Messenger (Android) Data

**To Expand Facebook Messenger (Android) Data:**
1. During processing, or in *Additional Analysis*, open the *Evidence Processing* window.
2. Check the Expand Compound Files option.
3. Click on the Expansion Options box and check the box for Facebook Messenger (Android).
4. Click *Ok* and process the evidence.

**Note:** There is a known issue within Facebook that deletes the last names of contacts and substitutes the firstname for the last name. This is a bug within Facebook, but the behavior will persist when exploring evidence within the Examiner.

Locating Facebook Messenger (Android) Data

**To Locate Facebook Messenger (Android) Data:**
1. In the *Explore Tab*, open the phone evidence and navigate to the following path:

   [root] > data > com.facebook.orca > databases > threads_db2
2. Open the *threads_db2* folder. Select either the *Contacts*, *inbox*, or *pending* folder to view the data.

   **Important:** The *pending* folder will not always have data in it.

**To View Facebook Messenger (Android) Contacts:**
1. Navigate to and highlight the *Contacts* folder, as described above.
2. The *File List* will show the available contacts. Select a contact, and the associated information for that contact will appear in the *File Content* pane.

**Note:** The Profile URLs shown for Facebook Messenger (Android) contacts are external and unusable because they require Facebook cookies to work.
To View Facebook Messenger (Android) Conversations:

1. Navigate to the inbox folder, as described above.

2. Select a conversation. It will populate as individual messages in the File List. The entire conversation will appear in Cool HTML in the File Content pane.

Note: The Attachments Column will contain links, not actual items. These links are external (stored in the cloud) and will need the Facebook cookies to work, meaning you must be logged in under the proper Facebook account to view them. The Pending Send Media Attachment Column will also have a link to the image. But since this image was pending, it might be available somewhere in the evidence.

Facebook Messenger Data Types
The following data types can be extracted from Facebook Messenger on Android:

Contacts
- User
- First Name
- Last Name
- Last Update Time
- Profile URLs

Message Threads
- Timestamp
- User
- Message
- Attachment URLs
- Attachments (if the data is present in the image)
It is possible to extract the following mobile chat applications:

- WeChat for Android
- WeChat for iOS
- WhatsApp for Android
- WhatsApp for iOS

WeChat for Android Data Types

The following data types can be extracted from WeChat Apps on Android. Unless specified otherwise, the data shows in both the Content Viewer (in CoolHTML) and in the Property Window (attributes).

**Device Owner Info**
- Display Name
- Username
- Phone
- Description (CoolHTML only)
- Comment (CoolHTML only)
- City
- State
- Country

**Contact Items**
- Display Name
- Username
- Note
- Country
- City

**Conversation Items**
- Create Date
- Modify Date
- Message Count
- Participants
- CoolHTML List of all messages

This includes Sent, To, and Message Data (including thumbnails of sticker, picture, and video clip messages)
Message Items
- Create Date
- From
- To
- Message

Displays a thumbnail image in CoolHTML if it is a sticker, picture, or video clip.
- Attachment Count

Attachment Items

Attachment items include pictures, video clips, and voice recordings. The picture, audio, or video clip is shown in the Content Viewer when available.

Note: Audio is compressed and not directly playable.

- Original Path (attribute only)

Viber for Android Data Types

The following data types can be extracted from Viber on Android. Unless specified otherwise, the data shows in both the Content Viewer (in CoolHTML) and in the Property Window (attributes).
- Chat Text
- Chat Attendees
- Shared Location
- Shared Location Date and Time
- Money Sent
- Files Transferred in Chat
- Joined Groups and Attendees
- Images Shared in Chat
- Voice Recording Shared in Chat
- Video Recording Shared in Chat
- Video Call Duration
- Voice Call Duration
- Contact List
WeChat for iOS Data Types
The following data types can be extracted from WeChat Apps on iOS. Unless specified otherwise, the data shows in both the Content Viewer (in CoolHTML) and in the Property Window (attributes).
- Contact Names (when available)
- Contact Phone Number (when device owner)
- Video Thumbnails
- Picture Files
- Message Contents
- Message Dates
- Message Sender
- Message Recipients

WhatsApp for Android Data Types
The following data types can be extracted from WhatsApp on Android. Unless specified otherwise, the data shows in both the Content Viewer (in CoolHTML) and in the Property Window (attributes).

Contacts
- Display Name
- Phone Number
- Status
- Given Name
- Family Name
- Nickname
- Company

Conversation
- Message Count
- Participants
- Thread ID
- Item Description
- Sent Date
- From
- To
- Message
- Date Created
- Date Modified

**Message**
- From
- To
- Item Description
- Date Created
- Date Modified
- Sent Date
- Message

**Attachment**
- Name
- File Class
- File Size

**WhatsApp for iOS Data Types**
The following data types can be extracted from WhatsApp on iOS. Unless specified otherwise, the data shows only in the Content Viewer (in CoolHTML) and not in the Property Window (attributes).

**Device Owner Information**
- App Version (CoolHTML only)
- Number of Times Launched (CoolHTML only)
- Date of Last Auto Backup (CoolHTML only)
- Full Name
- Username
- User’s What’s App JabberID (CoolHTML only)
- Call Sound (CoolHTML only)
- Blacklist in Sync (CoolHTML only)
- Number of System Bytes Received (CoolHTML only)
- Number of System Bytes Sent (CoolHTML only)
- Number of VoIP Bytes Received (CoolHTML only)
- Number of VoIP Bytes Sent (CoolHTML only)
- Number of VoIP Calls Received (CoolHTML only)
- Number of VoIP Calls Sent (CoolHTML only)
- Date modified (attributes only)

**Contact Items**
- ID (CoolHTML only)
- Full Name
- First Name
- Last name (attributes only)
- Nickname
- Account (CoolHTML only)
- JabberID (CoolHTML only)
- Mobile Number
- Home Phone
- Is Starred
- Description (attributes only)
- File Class (attributes only)

**Group Items**
- ID (CoolHTML only)
- Group Name (CoolHTML only)
- Group JabberID (CoolHTML only)
• Date Created
• Date Modified (attributes only)
• Member List (CoolHTML only)
• Created By Member (CoolHTML only)
• Description (attributes only)
• File Class (attributes only)

Conversation Items
• ID (CoolHTML only)
• Conversation Name (CoolHTML only)
• Create Date
• Message Count
• Modify Date

last message time
• Participants
  • Partner (CoolHTML only)
  • Description (attributes only)
  • File Class (attributes only)

Message Items
• Date Sent Creation Date
• Date Modified (attributes only)
• From*
• To*
• Is Outgoing* (CoolHTML only)
• Is Starred* (CoolHTML only)
• Message Type (CoolHTML only)

Includes Text, Image, File, Audio, Video, VCard, Shared Location, System Message.
• Text (CoolHTML only)
Includes audio_file_location, picture_thumbnail, video_thumbnail, shared_map_location_thumbnail, lat, long, vcard, file*

- Description (attributes only)
- File Class (attributes only)
- Message Text (attributes only) Text Messages Only
- Image Width and Height (attributes only)
- Longitude and Latitude (attributes only) Shared Location

**Note:** The asterisk (*) indicates that a particular item is not included for system messages. Android Parsers

---

**Android Phone Contacts**

**To view Android Contacts files:**

1. When importing evidence, select the **Android Contacts Database** option in the **Compound File Expansion Options** list.

2. Do one of the following:

2a. In the Evidence Tree, drill down to the phone databases and select the contacts database. A list of all contacts will populate in the File List.

2b. In the **Mobile Data** tab, navigate to Mobile Phone > Mobile Phone Items and highlight **Mobile Phone Items**.

3. Select an item in the **File List** and the **File Content** panel will display all associated contact information.
Android Calendar

To view Android Calendar data:
1. When importing evidence, select the Android Calendar Database option in the Compound File Expansion Options list.
2. In the Overview Tab, drill down to File Category > Mobile Phone > Mobile Phone Items and highlight Mobile Phone Items.
3. Select an item in the File List and the File Content panel will display all associated information.

Android Call Log

To view Android Call Log data:
1. When importing evidence, select the Android Call History Log option in the Compound File Expansion Options list.
2. In the Overview Tab, drill down to File Category > Mobile Phone > Mobile Phone Items > Call and highlight Call.
3. Select an item in the File List and the File Content panel will display all associated information.

Android SMS/MMS

To view Android SMS/MMS data:
1. When importing evidence, select the Android SMS/MMS Database option in the Compound File Expansion Options list.
2. In the Overview Tab, drill down to File Category > Mobile Phone > Mobile Phone Items and highlight Mobile Phone Items.
3. Select an item in the File List and the File Content panel will display all associated information.
Support for Gmail on Android

To view Android Gmail data:
1. When importing evidence, select the **Android Gmail Database** option in the **Compound File Expansion Options** list.
2. In the **Overview Tab**, drill down to **File Category > Mobile Phone > Mobile Phone Items** and highlight **Mobile Phone Items**.
3. Select an item in the **File List** and the **File Content** panel will display all associated information.

Support for Kik Files on Android

To view Android Kik data:
1. When importing evidence, select the **Kik (Android)** option in the **Compound File Expansion Options** list.
2. In the **Overview Tab**, drill down to **File Category > Mobile Phone > Mobile Phone Items** and highlight **Mobile Phone Items**. If you do not want to see all items together in the **File List**, you can select from **Chat Conversation**, **Chat Messenger**, or **Contact**.
3. Select an item in the **File List** and the **File Content** panel will display all associated information.

**Note:** Kik items (contacts, messages) will display a title beginning with Kik at the top of the table shown in the File Content panel. They will also have a Path entry that begins with Kik.
Support for Google Hangouts on Android

Note: Google Hangout databases are named babel#, where # represents a number.

To view the Google Hangout database files:

1. When importing evidence, select the Hangouts (Android) option in the Compound File Expansion Options list.
2. Do one of the following:

2a. In the Evidence Tree, navigate to the databases folder and select a babel database. Select the database file to see the properties of the database.

2b. In the Overview Tab, drill down to File Category > Mobile Phone > Mobile Phone Items and highlight Mobile Phone Items. If you do not want to see all items together in the File List, you can select from Chat Conversation or Chat Message.
3. Select an item in the File List and the File Content panel will display all associated information.

Note: Hangouts Items (contacts, messages) will display a title beginning with Hangouts at the top of the table shown in the File Content panel. They will also have a Path entry that begins with Hangouts.
Python Scripting
The Python Scripting tool allows investigators to run any Python script against evidence and generate results which can then be added back to the case. For example, Python scripts can be used to parse SQLite databases that are not currently parsed within the Examiner. Both pre-defined and individually-created parsers can be run on the evidence files. These parsers, written using Python scripting, are applied to exported evidence files by using the Python Scripting user interface. The data must be processed externally, but can be included in reports as if it was parsed within the Examiner.

About the Python Script User Interface
The Python Script user interface facilitates the following actions:

- Select which evidence files to parse through the Python script.
- Export the selected files to a folder outside of the Examiner.
- Select the Python script(s) to run on the selected files.
- Execute the Python script(s) on the files in the exported folder.
- (Optional) Create a bookmark inside the Examiner to relate the results to the case and to include the new data in any reports.

Pre-defined Python Scripts
The following pre-defined Python scripts are included in the Python Script user interface:

- EventBasedLogin
- Exif2Kmz
- SQLiteWizard
- SQLite_Data_Carver

Each pre-defined script has a corresponding executable option, for those who prefer to run the EXE file.

Python Processing Options
There are two different options when processing case data using an external Python Script. If the files have not been exported previously, the Python Script user interface will walk through all of the steps, including the step to automatically create a bookmark and attach the Python results as supplementary files. If the files have already been exported, there is an option to run the Python
Script on the existing folder containing the exported files; however, his option does not allow the files to be automatically associated with the bookmark created by the wizard. They can be attached manually once the bookmark has been created, if desired. This option should not be used if the files must be related in the final report.

Using the Python Scripting User Interface

The Python Script user interface allows any Python script to be run on selected evidence files within a case, enabling the custom parsing and processing of evidence not yet supported by the tool. The Python Script user interface allows results to be attached to case reports by using bookmarks. Multiple scripts can be run consecutively within the wizard.

To use the Python Script User Interface

1. In the File List, select the desired evidence items to be searched.

2. Perform one of the following steps to open the Python Script Wizard:
   - Right click on one of the evidence items and select the Run Python Script option.
   - Open the Tools menu and select the Run Python Script option.

3. In the Export Files portion of the wizard, perform the following actions:
   3a. Choose which selected items to include.
   3b. Enter a destination folder and confirm the processing manager.
   3c. Optionally, select any necessary advanced options.
   3d. Click Next. The files will be exported to the chosen folder.

Note: If you have already exported the desired files from FTK, you may select Option 2 and run the script on the existing folder without exporting the files again. However, this option will not allow you to automatically associate the evidence files with the bookmark created within the Python wizard. Report result files can still be attached to a bookmark as supplementary files. It is recommended that you not use Option 2 unless you do not plan to associate evidence files to the bookmark.

4. Once the Export has completed, the Export Progress portion of the wizard will appear. This window will show the Export Log, as well as the number of items exported and the error count. If any errors occurred, a button will appear allowing the user to view the error log. There is also a View Export Folder button in order to quickly access the exported file(s).

5. The Script Execution portion of the wizard will appear. Perform the following actions:
   5a. Select any Python script file to run. There is a drop down option that will automatically populate with the pre-defined scripts included with the product. The pre-defined scripts will offer...
both the compiled executable version as well as the Python script source version (which requires the Python environment).

5b. Add additional scripts using the Add New button. Once selected, this option will allow users to browse to the file containing the new Python script and apply it. New scripts will be added automatically to the drop down list for future use.

5c. To view the selected script in a text editor, click the View Script button.

5d. Enter the Input and Output folders. If the files have been exported using the wizard, the Input folder will be entered automatically and cannot be changed.

5e. Additional parameters may be added into the appropriate box.

5f. Verify the content in the Final Script Command box. This shows the actual command that will be executed.

5g. The Python environment verification will run automatically and the results will be displayed. If desired, use the Re-verify environment button to be sure the right version of Python is installed on the system.

5h. Click Next to execute the script.

Note: Python must be installed and working prior to beginning this step if a script file (.py) is selected. Visit www.python.org to install the python environment. If the compiled executable (.exe) version is selected, the Python environment is not required.

6. This will take you to the Script Progress portion of the wizard. A progress bar with a Pause/Cancel button will appear while the script is running. Any warnings or errors will appear in the Warnings/Errors box. If additional input is needed for the script, there is a text box. When prompted, enter the input and click the Enter button to allow the script to complete. Once the script has completed, click Next.

Note: If you are running scripts in a Python 2 environment you will not be able to interact with the script using the standard input prompts from the user interface. However, the user interface will allow you to enter values when prompted in a Python 3 environment.

7. In the Bookmark Creation portion of the wizard, it is possible to create a bookmark in order to include the Python results in a report. If a bookmark is desired, complete the following steps:

7a. Select the Create Bookmark option.

7b. Enter the desired Name for the bookmark.

7c. Enter any necessary Comments related to the bookmark.

7d. Select a location for the bookmark by choosing a parent folder.

7e. Click the Attach button to attach the Python results as supplementary files in the bookmark.
7f. Select the *Associate exported items to this bookmark* option to include the original evidence files in the bookmark. These files will auto-populate using the output file from the script execution step.

7g. If no bookmark is required, select the *Do not create a Bookmark* option.

7h. Click **Next**.

8. If the option to create a bookmark was selected, the *Bookmark Progress* portion of the wizard will appear. The bookmark creation status will be displayed. When finished, click **Next**.

9. The *Summary* portion of the wizard will appear. This will include three sections of data: Export, Script Execution, and Bookmark. Click **Finish**.

The bookmark will now be visible in the Bookmarks tab of the Examiner. The Python output files will be listed in the Supplementary Files panel of the bookmark.
Viewing Data in Volume Shadow Copies
You can examine data that is contained in NTFS Volume Shadow Copies. See Examining Data in Volume Shadow Copies on page 143.

Viewing Microsoft Office and Adobe Metadata
You can examine metadata from Microsoft Office and Adobe documents. This data is processed by default, but you must use the following method to view it.

To view Microsoft Office and Adobe Metadata
1. In the examiner, open one of the following:
   - The Overview tab > File Category > Documents > Adobe Documents
   - The Overview tab > File Category > Documents > Microsoft Documents
2. In the File List, click the Check all files in the current list icon.
3. Click on the Column Settings icon. See Managing Columns on page 613.
4. Either create a new column template or edit an existing one.
5. In the Available Columns list, expand Office-specific Features or All Features.
6. Add the desired columns to the template.

For example, to add columns for Adobe metadata, use the following:
   - All Features
     - Meta-data - Date Created
     - Meta-data - Date Modified
7. Click OK.
8. Select the template name you just configured and click Apply. This applies the template to the File List.
9. Click Close.
10. You will now see the meta-data information in the columns for each record.

When viewing the expanded files, you can use the following columns in the File List to display detailed data.
Microsoft Office and Adobe Metadata Columns

- Microsoft Office documents
- CreateTime (Content created)
- EmbeddedComments (PPT files)
- HiddenColumnsRows (Excel files)
- HiddenWorkSheets (Excel files)
- LastPrinted
- LastSavedTime (Date last saved)
- RevisionNumber
- TotalEditingTime (Word and PPT)
- TrackChanges
- From file Origin properties

Adobe files
- Meta-data - DateCreated
  - Meta-data - DateModified

About Windows 8 and 10 Keyword Searches

Windows 8 and Windows 10 have added the ability to perform an advanced search query. These advanced search query files are now parsed automatically during forensic processing. Advanced Query Searches are saved by Windows in the Admin > Searches folder. There are two default searches found in Windows 10. These are the Indexed Locations and Everywhere files.
SQLite Query Builder

Users can create and incorporate SQLite Queries from within the user interface. This allows investigators to produce an HTML report of an unsupported SQLite database.

Expanding Unsupported SQLite Databases

Investigators can expand unsupported SQLite databases within their evidence files using the SQLite QueryBuilder.

Important: To use this feature, the SQLite Databases option must be selected in the Expand Compound Files portion of the Evidence Processing Options when processing evidence.

To expand SQLite database files

1. Locate the SQLite database files within your evidence files. To do this, filter on the Categories column using SQLite database as the content.

Note: Some of these files may not have information to query.

2. Determine the number of columns and tables used within the files you would like to expand.

3. Create and save a query for each file to be expanded. For more information, see Creating Queries.

Note: Queries are specific to the file for which they are created. Be sure to name the query something similar to the name of the original file to make it easy for users to know which query applies to which file.

4. In FTK, return to the list of SQLite database files. Right click on the file you would like to expand and select the Run SQLite Query option. The Run Query dialog will open. Enter a Report Name and select a destination for the report.

5. Select the proper query from the list you have created and saved, and click OK.

6. Navigate to the destination folder and you will see three new files: XHTML, XML, and XSLT. Open the XHTML file and you will see the contents of the selected SQLite database in table form.
Creating Queries

You can use the following information to create a basic query template. Be sure to replace the information within brackets with data for the specific SQLite database files you would like to expand.

**Note:** Queries will only run on a single file and all fields are output as strings, not binary values.

To create a query for expanding SQLite files
1. Open Notepad.
2. Write a simple query: “Select [column(s)] from [table]”
3. Save the query.

Query Options
You can write queries to perform multiple tasks; including, but not limited to, the following functions:
- To select all columns in a table
- To select specific columns in a table
- To include information from two or more tables within the same file

To select all columns in a table
❖ Use the following query:

```
Select * from [tablename]
```

To select specific columns in a table
❖ Use the following query:

```
Select [colname1], [colname2], [colname5] from [tablename]
```

To include information from two or more tables within the same file
❖ Use the following query:

```
Select 'table 1' as [column(s)] from [table 1] union Select 'table 2' [column(s)] from [table 2]
```
Viewing SQLite Database Schema Information

It is possible to view the schema HTML file for a SQLite database. When viewed in the File Content panel, tables showing which data is contained within the selected database will be visible. This can provide insight into whether a particular Python script should be applied in order to locate more specific data of interest.

To view SQLite database schema.html files:
1. When processing the evidence, select only the SQLite Databases option in the Compound File Expansion Options.

2. Once the evidence is processed, locate the SQLite database for which you would like to view the schema.html file. If the path for the database is unknown, perform the following steps:

2a. On the Overview tab, drill down the following path: File Category > Databases > Other Databases > SQLite Databases.

2b. Select SQLite Databases.

2c. In the File List you will be able to view the path for the desired SQLite database.

3. In the Explore tab, locate and select the SQLite database for which you would like to view the schema.html file.

4. In the File List, select the appropriate schema.html file.

5. In the File Content pane, the Table Schema information will appear in HTML.
Reviewing Portable Case Data in FTK Plus

About Portable Case Review
Portable Cases enable the investigator to export or share specific items from FTK for review in a “portable” FTK Plus instance running on a system without any licensing restrictions. When Portable Case data is opened, the interface will look similar to FTK Plus, however only consisting of a limited feature set. For example, quick searches will be available, but advanced search is not.

Prerequisites
1. The system that will host the “portable” FTK Plus Offline must have Microsoft .NET Framework 4.7.2 and Visual C++ 2013 Redistributable already installed.
2. The FTK Plus Offline system does not need to have full version of FTK Plus installed. The FTK Plus Offline binaries come bundled with the exported data by default.

Note: When a Portable Case is being opened, it will install both VLC and OutsideX if they are not already present.
How to Create Portable Case data
1. In the Examiner, do one of the following:
   - Highlight the items that you want to export to the portable case..
   - Check the items that you want to export to the portable case..
   - Make the File List pane display the items that you want to export to the portable case.
   - If you wish to export ALL objects, simply proceed to the next step.
2. Go to File >> Create Portable Case
3. In the Create Portable Case dialog, if you wish to export a copy of the FTK Plus installer with the portable case data, mark the “Include FTK Plus” checkbox.
4. Do one of the following:
   4a. Mark the box labeled “Export to case folder” in order to have the portable case data automatically written to the case folder that corresponds to the current FTK case.
   OR
   4b. Unmark the box labeled “Export to case folder” in order to write the portable case data to the directory of your choice.
5. In the Export Name field, provide a name for the portable case data export.
6. In the Target Items section, select the option that applies to the list of files you wish to the portable case.
7. Set a ‘Max Single File Export Size (MB)’ to limit single file export sizes.
8. Select ‘Include Email Attachments’ if required.
9. Click OK when ready.
10. The Data Processing Status window appears and displays the progress of the export job to the chosen directory.

How to use portable case data
1. Locate the portable case data exported from your case previously.
   By default the data will be written to:
   ...
   \[CASE_FOLDER]\Jobs\job_[X]_[X]\...
2. Launch the BAT file
This batch file checks prerequisites, installs OutsideInx64 viewer, and FTK Plus if not already installed

3. In FTK Plus Offline interface, click the Explore Offline Data File button.

4. Browse to the data.db file found at the root of the portable case data folder and open it.

5. The portable case data now loads into the FTK Plus Offline interface.

How to sync portable case data back to FTK

1. Copy the portable case database file (*.db) to a location where FTK can read it (such as a local drive or network share).

2. Launch FTK and open the case into the Case Examiner interface.

3. Click File >> Portable Case Sync

4. Click the ellipse button “...” to browse to the location of the database file (*.db).

5. Select the DB file and click Open.

6. The portable case data is imported and synchronized with the labels, bookmarks, bookmark comments, and notes that exist in the FTK case data.
Chapter 28
Bookmarking Evidence

This chapter includes the following topics
- About Bookmarks (page 498)
- About Timeline Bookmarks (page 498)
- Using the Bookmarks Tab (page 505)
- Creating a Bookmark (page 499)
- Viewing Bookmark Information (page 505)
- Bookmarking Selected Text (page 506)
- Adding to an Existing Bookmark (page 507)
- Creating Email or Email Attachment Bookmarks (page 508)
- Adding Email and Email Attachments to Existing Bookmarks (page 508)
- Moving a Bookmark (page 509)
- Copying a Bookmark (page 509)
- Deleting a Bookmark (page 509)
- Deleting Files from a Bookmark (page 509)

About Bookmarks
A bookmark is a group of files that you want to reference in your case. These are user-created and the list is stored for later reference, and for use in the report output. You can create as many bookmarks as needed in a case. Bookmarks can be nested within other bookmarks for convenience and categorization purposes.

Bookmarks help organize the case evidence by grouping related or similar files. For example, you can create a bookmark of graphics that contain similar or related graphic images. The Bookmarks tab lists all bookmarks that have been created in the current case.

Bookmarks only apply to the case they are created in.
**About Timeline Bookmarks**

When creating bookmarks, you can also create a Timeline type of bookmark. A Timeline bookmark lets you show the chronological relationships of the files in your case. When you create a Timeline bookmark, you can record the Create Date, Accessed Date, and Modified Date for files as individual items. You can then export that data to a CSV report file. Each action (create, accessed, modified) for each file is a separate item in the report.

When sorted by the date and time, the CSV report file presents a chronological timeline of the actions of the evidence files in your case.

For example, you can create a bookmark of files that were downloaded from the internet. The report shows when the files were downloaded (created) and the time interval between then and when they were last accessed. You can also see if and when the files were modified.

You can also add manual timeline data. Manual timeline data lets you add items to your timeline that may not be represented by the files in your case. For example, you may have phone logs that show when relevant phone calls were placed. You can add those phone calls as manual timeline items so that they appear in your report along with the file information in the case.

You can use the exported CSV file to produce your own chronological timeline of the evidence in the case. This can present a clearer view of how certain events happened which can help investigators communicate to the jurors and judge on their case.

The CSV report file includes the following data as columns:

- The date/time stamp of the file action
- The type of file action (Modified, Accessed, Created, or Other). The Other category is used for manual timeline entries.
- The bookmark name
- The filename
- Any comments that you manually entered for each item

A bookmark can either be a timeline bookmark or a regular bookmark, but not both.
Creating a Bookmark

To create a bookmark

1. In the File List view, select the files that you want to add to the bookmark.

You can either highlight the files that you want to include, check the boxes of the files that you want to include, or do nothing to include all files.

2. Right-click on a selected file in the File List view and click Create Bookmark.

3. Enter the information about the bookmark. See Bookmarks Dialog Options on page 501.

4. Click OK.

Note: Applying filters to a group of listed files for bookmarking can speed the process. The All Highlighted setting does not work in this instance. Enabling this feature would significantly slow the response of the program. Instead, use either the Checked Files filter, or the All Files Listed filter.
About Empty Bookmarks

You can create bookmarks that contain only the name and location of the bookmark. These are called Empty Bookmarks. Empty Bookmarks allow you to add “placeholders” while investigating a case. This feature makes it easy to mark your place and come back to it later. For example, while investigating a fraud case, you notice an email that may or may not be pertinent to your investigation. Creating an Empty Bookmark allows you to quickly “save your place” and come back later when you have more time to delve into that evidence.

You can also use Empty Bookmarks to format your Bookmarks tree. This allows you to better organize your bookmarks. For example, you may be investigating documents, video, graphics, and emails. You could create an Empty Bookmark called Documents, under which you would place all of your document-related bookmarks.

Then, you would create an Empty Bookmark called Video, under which you would place all of your video-related bookmarks. Continue creating Empty Bookmarks until you have a manageable Bookmark tree.

There are two ways to create Empty Bookmarks, creating the Empty Bookmark from the Bookmarks tab or in the Create New Bookmark dialog.

To create an Empty Bookmark from the Bookmarks tab

1. In Evidence Explorer, click the Bookmarks tab.
2. Right-click the bookmark under which to create the Empty Bookmark.
3. Click Create Empty Bookmark.
4. Enter a name for the Empty Bookmark and click OK.

You add and save additional bookmark information to an Empty Bookmark at anytime by using the Bookmark Information pane.

To create an Empty Bookmark in the Create New Bookmark dialog

2. In Files to Include, select None.
3. Save the bookmark.
# Bookmarks Dialog Options

## Options of the Bookmark Information Pane

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bookmark Name</td>
<td>The name of the bookmark.</td>
</tr>
<tr>
<td>Bookmark Comment</td>
<td>Comments about the bookmark or its contents. Bookmark Comments are created in an HTML editor. HTML allows you to format your comments within the bookmark and for any subsequent reports. See <a href="#">Bookmark Comments HTML Editor</a> on page 503.</td>
</tr>
<tr>
<td>Files to Include</td>
<td>Specify which files in the File List to include in this bookmark. You can select one of the following:</td>
</tr>
<tr>
<td></td>
<td>- All Highlighted - Includes only the highlighted items.</td>
</tr>
<tr>
<td></td>
<td>- All Checked - Includes only the checked items.</td>
</tr>
<tr>
<td></td>
<td>- All Listed - Includes all items in the File List.</td>
</tr>
<tr>
<td></td>
<td>- None - Creates an Empty Bookmark.</td>
</tr>
<tr>
<td>Timeline Bookmark</td>
<td>Select this option to make this a Timeline bookmark. If you select the Timeline tab, this option is selected automatically. A bookmark can either be a Timeline Bookmark or a regular bookmark, but not both.</td>
</tr>
<tr>
<td>Select Existing Bookmark</td>
<td>Select the parent bookmark under which you would like to save the bookmark. A default shared tree for bookmarks available to all investigators is created, and a bookmark tree specific to the case owner is created. If the bookmark is related to an older bookmark it can be added under the older bookmark, with the older bookmark being the parent, or it can be saved as a peer.</td>
</tr>
<tr>
<td>Comments tab</td>
<td>This lets you configure elements of a standard bookmark.</td>
</tr>
<tr>
<td>File Comments</td>
<td>You can assign a comment to each file in the bookmark. Comments are created in an HTML editor. HTML allows you to format your comments within the bookmark and for any subsequent reports. See <a href="#">Bookmark Comments HTML Editor</a> on page 503.</td>
</tr>
<tr>
<td>Supplementary Files</td>
<td>You can add external, supplementary files associated with the bookmark. Options are:</td>
</tr>
<tr>
<td></td>
<td>- Attach: Allows the investigator to add external supplementary files to the bookmark. The attached files appear in the Supplementary Files pane and are copied to the case folder.</td>
</tr>
<tr>
<td></td>
<td>- Remove: Removes a selected supplementary file from the bookmark.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Also include</td>
<td>If applicable, you can include the following:</td>
</tr>
<tr>
<td></td>
<td>- Parent index.dat</td>
</tr>
<tr>
<td></td>
<td>The option to include Parent index.dat is only available if you have selected to bookmark an index entry, for example a cookie. This option includes the entry’s parent index.DAT file in the bookmark.</td>
</tr>
<tr>
<td></td>
<td>- Email Attachments - If one of the items selected is an email with attachments, this will include all of the attachments that the email has.</td>
</tr>
<tr>
<td></td>
<td>- Parent Email - If one of the items selected is an email attachment object, selecting this option will include the parent email.</td>
</tr>
<tr>
<td></td>
<td>- Exclude Selected OCR Extractions</td>
</tr>
<tr>
<td></td>
<td>The Exclude Selected OCR Extractions check box appears only when OCR- extracted files have been selected when creating a new or adding to an existing bookmark. If, instead, you have selected graphic files, and have not selected their OCR counterparts, the check box for OCR Extractions of selected Graphics will be active and available.</td>
</tr>
<tr>
<td></td>
<td>- Actual Source File</td>
</tr>
<tr>
<td></td>
<td>This option lets you include the parent child of a processing-generated file.</td>
</tr>
<tr>
<td></td>
<td>See Relating Generated Files to Original Files on page 452.</td>
</tr>
<tr>
<td>Bookmark Selection in File also</td>
<td>Check this item to have the highlighted text in a file automatically highlighted when the bookmark is re-opened. The highlighted text prints in the report.</td>
</tr>
<tr>
<td></td>
<td>The selected text that will be included displays in the text box below the check box.</td>
</tr>
</tbody>
</table>

**Timeline tab**

This lets you configure elements of a Timeline bookmark.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create Date</td>
<td>Select this option to record the date and time that the file was created.</td>
</tr>
<tr>
<td>Accessed Date</td>
<td>Select this option to record the date and time that the file was last accessed.</td>
</tr>
<tr>
<td>Modified Date</td>
<td>Select this option to record the date and time that the file was last modified.</td>
</tr>
<tr>
<td>Object Timeline Comments</td>
<td>You can assign a comment to each file timestamp in the bookmark. Comments are created in an HTML editor. HTML allows you to format your comments within the bookmark and for any subsequent reports. See Bookmark Comments HTML Editor on page 503. The timeline comments are shown in the timeline report anchored to each date, and each date being used will create a new row in the text report.</td>
</tr>
<tr>
<td>Manual Timeline Data</td>
<td>In this section, you can add manual timeline entries that are not available as items in the File List. For example, you may have access to phone records and you can add call histories as individual manual entries. You enter the date and time of the items and then in the CSV, they are displayed chronologically with the other items in your bookmark. <strong>Note:</strong> Manual items are listed as Other in the report.</td>
</tr>
<tr>
<td>Manual Timeline Comments</td>
<td>(Optional) Enter a comment or description to enter a Manual Timeline item. Comments are created in an HTML editor. HTML allows you to format your comments within the bookmark and for any subsequent reports. See Bookmark Comments HTML Editor on page 503.</td>
</tr>
<tr>
<td>Manual Date</td>
<td>Enter the date of the Manual Timeline item. You can click the arrow to open a calendar.</td>
</tr>
<tr>
<td>Manual Time</td>
<td>Enter the time of the Manual Timeline item.</td>
</tr>
<tr>
<td>Add</td>
<td>Click Add to save the Manual Timeline item. The item is added to the Manual Timeline Entries list.</td>
</tr>
<tr>
<td>Remove</td>
<td>Highlight a Manual Timeline entry and click Delete to remove it from the list.</td>
</tr>
<tr>
<td>Manual Timeline Entries</td>
<td>The list Manual Timeline items that you have added.</td>
</tr>
<tr>
<td>Select Bookmark Parent</td>
<td>Select the parent bookmark under which you would like to save the bookmark. There are two default bookmark parents: • A Shared tree that is available to all investigators • A bookmark tree specific to the logged-in-user Administrators and Case Administrators can see and use all bookmarks in a case. If the bookmark is related to an older bookmark it can be added under the older bookmark, with the older bookmark being the parent, or it can be saved as a peer.</td>
</tr>
</tbody>
</table>

**Bookmark Comments HTML Editor**
The HTML Editor for Bookmark Comments allows you to format Bookmark Comments using HTML.

**Important:** You are required to use the HTML Editor when entering Bookmark Comments, with or without formatting.

**To enter Bookmark Comments**

1. In *Evidence Explorer*, click the **Bookmarks** tab.
2. Highlight (click) a bookmark from the **Bookmarks** pane.
3. Click the **Edit** button next to the Comment field. The HTML Editor appears.
4. Enter and/or format your comments using formatting options. You can also format your comments directly in HTML by clicking **Source**. For a brief description of each HTML formatting option, click **Help** in the HTML Editor.
5. Click **Done** in the HTML Editor when finished.

**Note:** ALWAYS click **Done** in the HTML Editor to exit the editor and keep your comments. You still need to save the Bookmark (**Save Changes**) to keep the comment in the Bookmark.
**Viewing Bookmark Information**

The Bookmark Information pane displays information about the selected bookmark and the selected bookmark file. The data in this pane is editable by anyone with sufficient rights.

Select a bookmark in the Bookmarks tree view of the Bookmarks tab, or in the Bookmarks node in the tree of the Overview tab to view information about a bookmark. The Overview tab view provides limited information about the bookmarks in the case. The Bookmark tab provides all information about all bookmarks in the case. In the Bookmark tab, the Bookmark Information pane displays the Bookmark Name, Creator Name, Bookmark Comment, and Supplementary files. When selected, a list of files contained in the bookmark displays in the File List. If you select a file from the File List, the comment and selection information pertaining to that file displays in the Bookmark Information pane.

Bookmarked files display in a different color in the File List pane than non-bookmarked files for easy identification. The colored text for bookmarks feature can be toggled on or off using the button in the file list toolbar.

Change any of the information displayed from this pane. Changes are automatically saved when you change the bookmark selection.

In the File List, bookmarked items display in a different color for easy identification. You may need to refresh the view to force a rewrite of the screen for the different color to display. Forcing a rewrite would impact the overall performance of the program.

**Creating a Timeline Bookmark Report**

After you have created Timeline Bookmarks, you can create Timeline Bookmark Reports. The reports are in CSV format. You can specify one or more Timeline Bookmarks for each report. You specify one or more Timeline Bookmarks for each report. You specify the location and name of the saved CSV report.

See About Timeline Bookmarks on page 498.
To create a timeline Bookmark Report
1. In the Examiner, click File > Timeline > Report.
2. Select one or more Timeline Bookmarks to use for the report.
3. (Optional) Select one of the following
   - Select All Children - This selects all of the children of the selected bookmarks in the bookmark tree.
   - Clear All Children - This clears all of the children of the selected bookmarks in the bookmark tree.
4. Click Select to select an output folder.
4a. Select the folder to save the report in.
4b. Specify the name of the report or use the default Timeline Report name.
5. Click Generate to save the report.

Using the Bookmarks Tab
You can use the Bookmark tab to view, create, and edit bookmarks.

Bookmarking Selected Text
Bookmarked selections are independent of the view in which they were made. Select hex data in the Hex view of a bookmarked file and save it; bookmark different text in the Filtered view of the same file and save that selection as well.

To add selected text in a bookmark
1. Open the file containing the text you want to select.
2. From the Natural, Text, Filtered or Hex views, make your selection.

Note: If the file is a graphic file, you will not see, nor be able to make selections in the Text or the Natural views.
3. Click Create Bookmark in the File List toolbar to open the Create New Bookmark dialog.
4. When creating your bookmark, check Bookmark Selection in File.
5. To save selected content, choose the view that shows what you want to save, then highlight the content to save.
6. Right-click the selected content. Click Save As.
7. In the Save As dialog, provide a name for the selection and click Save. The selection remains in the bookmark.

Bookmarking Video Thumbnails

You can bookmark Video Thumbnails by creating a new bookmark or adding to an existing bookmark. By default, Video Thumbnails that are added to Bookmarks play from the location thumbnail to end of the video. You can update, change the start/end times, or remove the thumbnail from within the bookmark. You can also export your video thumbnails to your report.

See Using the Video Thumbnails Pane on page 449. See About Bookmarks on page 498. See Adding Bookmarks to a Report on page 621.

Adding a Video Thumbnail to a New or Existing Bookmark

To add a Video Thumbnail to a new or existing Bookmark

1. From the Evidence Explorer, click the Video tab.
2. Right-click the video thumbnail for the Bookmark.
3. Click either:
   - Create Bookmark. See Creating a Bookmark on page 499.
   - Add to Bookmark. See Adding to an Existing Bookmark on page 507.
4. Follow the instructions for creating and/or adding to a Bookmark.

About Updating/Removing Bookmarked Video Thumbnails

Once there are Video Thumbnails in a Bookmark, you can update (change) the Video Thumbnail or remove it.

Note: You cannot add a selection of a video from the Bookmark's Natural Viewer using the Add Selection button. To add a video thumbnail to a bookmark, see Adding a Video Thumbnail to a New or Existing Bookmark (page 506).

To update a Video Thumbnail in a Bookmark

1. From the Evidence Explorer, click the Bookmarks tab.
2. In the Bookmarks pane, navigate to and highlight the Bookmark containing the Video Thumbnail(s).
3. In the File List pane, highlight the video from which the thumbnails were created.

4. In the Bookmark Information > Selections pane, click (highlight) the thumbnail (selection).

5. In the File Content > Natural Viewer, click Play ( ) and then Pause.

6. Click Update Section.

7. Enter a Start and/or End Time.

8. Click OK.

To remove a Video Thumbnail from a Bookmark

1. From the Evidence Explorer, click the Bookmarks tab.

2. In the Bookmarks pane, navigate to and highlight the Bookmark containing the Video Thumbnail(s).

3. In the File List pane, click (highlight) the video from which the thumbnails were created.

4. In the Bookmark Information > Selections pane, click (highlight) the thumbnail (selection).

5. Click Remove Selection.

6. Confirm the change.

Adding to an Existing Bookmark

Sometimes additional information or files are desired in a bookmark.

To add to an existing bookmark

1. Select the files to be added to the existing bookmark.

2. Right-click the new files.

3. Click Add to Bookmark.

4. When available (depending on the type of files you are adding), make selections for Files to Add, Also Include, OCR Extractions of Selected Graphics, and Bookmark Selection in File.

5. Open the parent bookmark tree.

6. Select the child bookmark to add the file or information to.

7. Click OK.
When bookmarking an email, you can also add and bookmark any attachments. You can also include a parent email when you bookmark an email attachment.

To create a bookmark for an email, follow the steps for creating a bookmark. Select the email to include in the bookmark. Right-click and choose **Create Bookmark**. Note that by default, the **Email Attachments** box is active, but unmarked. If only the parent email is needed, the **Email Attachments** box should remain unselected.

Complete the bookmark creation normally by naming the bookmark, selecting the bookmark parent, then clicking **OK**.

If you need to bookmark only an attachment of the email, select and right-click on the attachment. Choose **Create Bookmark**. For more information on creating bookmarks, see, *Creating a Bookmark* (page 499).

Notice that the Parent Email box is automatically active, allowing you to include the parent email if it is not part of the selection you have already made. If the Parent Email box is checked, and there is more than one attachment, the Email Attachments box becomes active as well, allowing you to also include all attachments to the parent email. To add only the originally selected attachment to the bookmark, do not check the Parent Email box.

**Adding Email and Email Attachments to ExistingBookmarks**

To add an email to a bookmark, select the email to add, then right-click on the email and choose **Add To Bookmark**. Note that if emails are selected, but their attachments are not selected, the **Email Attachments** box is active, but not marked. If only the parent email is needed, the **Email Attachments** box can remain unselected. If you have selected only the attachment, include the attachment’s parent email by marking the **Parent Email** box.

One way to be sure to find the exact items you want is to highlight an interesting item in the File List view in one tab, then right-click on it and select **View This Item in a Different List**. Click on **Email** and you are taken to the Email tab with the selected email highlighted in the File List view, and displayed in the Natural tab in the File Content pane. In the Email Attachments pane on the right that file is displayed, along with its role; whether it is a parent email, part of the email thread, or an attachment.

If only an attachment of an email is needed to be added to the bookmark, select the attachment and follow the instructions for adding to a bookmark.
To move a bookmark
1. From either the Bookmark tab or the Overview tab, select the bookmark you want to move.
2. Drag the bookmark to the desired location and then release the mouse button.

Copying a Bookmark

To copy a bookmark
1. From either the Bookmark tab or the Overview tab, select the bookmark you want to copy.
2. Using the right mouse button, drag the bookmark to the desired location and release the mouse button.

Deleting a Bookmark

To delete a bookmark
1. In the Bookmark tab, expand the bookmark list and highlight the bookmark to be removed.
2. Do one of the following:
   - Press the Delete key.
   - Right-click on the bookmark to delete, and click Delete Bookmark.

Deleting Files from a Bookmark

To delete files from a bookmark
1. From either the Overview tab or the Bookmarks tab, open the bookmark containing the file you want to delete.
2. Right-click the file in the Bookmark File List pane.
3. Do one of the following:
   - Select Remove from Bookmark.
• Press the Delete key on your keyboard. You will be prompted, “Are you sure you want to delete files from this bookmark?” Click Yes.

• Deleting a file from a bookmark does not delete the file from the case.
Searching Evidence with Live Search

Searching evidence for information pertaining to a case can be one of the most crucial steps in the examination. An index search gives rapid results, and a live search includes options such as text searching and hexadecimal searching. You can view search results from the File List and File Contents views of the Search tab.

The Live Search is a process involving a bit-by-bit comparison of the entire evidence set with the search term. This chapter includes the following topics

- Conducting a Live Search (page 510)
- Live Text Search (page 511)
- Live Hex Search (page 513)
- Live Pattern Search (page 514)
- Using Pattern Searches (page 514)
- Predefined Regular Expressions (page 517)
- Creating Custom Regular Expressions (page 519)

Conducting a Live Search

The live search takes slightly more time than an index search because it involves a bit-by-bit comparison of the search term to the evidence. A live search is flexible because it can find patterns of non-alphanumeric characters, including those that are not generally indexed. It is powerful because you can define those patterns to meet your needs in an investigation.

**Note:** If a case was originally processed using distributed processing, when a reviewer conducts a live search, the system will first attempt to use the computer with the distributed processing engine, but if it is not available, it will use the reviewer’s local computer to conduct the search.
A Text search finds all strings that match an exact entry, such as a specific phone number (801-377-5410). When conducting a Live Text Search, there are no arrows to click for operand selection. A Live Text Search gives you options such as ANSI, Unicode with UTF-16 Little Endian, UTF-16 Big Endian, and UTF-8. The latter two are always case-sensitive. You can also choose from a list of other Code Pages to apply to the current search. In addition, you can select Case Sensitivity for any Live Text Search.

**Note:** When entering Chinese characters into search, you must have both ANSI and Unicode options selected.

The difference between a Pattern search and a Text search is that a text search searches for the exact typed text, there are no operands so the results return exactly as typed. For example, a simple Pattern search allows you to find all strings that match a certain pattern, such as for any 10-digit phone number (nnn-nnn-nnnn), or nine-digit social security number (nnn-nn-nnnn). More complex Pattern searches ("regex") require specific syntax. See Live Pattern Search (page 514).

Search terms can be entered then exported as XML files, then imported at any time, or with any case. Text files can be imported and used in Live Search, however the Live Search Export feature supports only XML format.

**Note:** When importing TXT files that the search of those terms depend on the specific tab your in. (ie If I have a few hex terms and import the TXT list into Live Search in the Patterns tab), the search is run as a pattern search and not hex.
To Conduct a Live Text search

1. In the Live Search tab, click the Text tab.

In the Text or Pattern tabs, you can check the character sets to include in the search.
2. If you want to include sets other than ANSI and Unicode, check Other Code Pages and click Select.
3. Select the needed sets.
4. Click to include EBCDIC, Mac, and Multibyte as needed.
5. Click OK to close the dialog.
6. Check Case Sensitive if you want to search specifically uppercase or lowercase letters as entered. Case is ignored if this box is not checked.
7. Enter the term in the Search Term field.
8. Click Add to add the term to the Search Terms window.
9. Click Clear to remove all terms from the Search Terms window.
10. Repeat Steps 7, 8, and 9 as needed until you have your search list complete.

When you have added the search terms for this search, it is a good idea to export the search terms to a file that can be imported later, saving the time of re-entering every item, and the risk of errors. This is particularly helpful for customized pattern searches.

11. In the Max Hits Per File field, enter the maximum number of search hits you want listed per file. The default is 200. The range is 1 to 65,535. If you want to apply a filter, do so from the Filter drop-down list in the bar below the Search Terms list. Applying a filter speeds up searching by eliminating items that do not match the filter. The tab filter menu has no effect on filtering for searches.
12. Select a Processing Manager if required.
13. Click Search.
14. Select the results to view from the Live Search Results pane. Click the plus icon (+) next to a search line to expand the branch. Individual search results are listed in the Live Search Results pane, and the corresponding files are listed in the File List. To view a specific item, select the hit in the search results. Selected hits are highlighted in the Hex View tab.
15. When a search is running you can click View > Progress Window to see how the job is progressing.

Note: In the progress window, you can Pause, Resume, and Cancel jobs, in addition to closing the window. (Pause and Resume are the same button, but the label changes depending on
processing activity.)

**Note:** Mark the *Remove when finished* check box to take completed jobs off the list for housekeeping purposes.
16. When processing is complete, return to the Live Search tab to review the results.

Right-click on a search result in the Live Search Results pane to display more options. The available right-click options are as follows:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create Bookmark</td>
<td>Opens the <em>Create New Bookmark</em> dialog.</td>
</tr>
<tr>
<td>Copy to Clipboard</td>
<td>Opens a new context-sensitive menu. Options are:</td>
</tr>
<tr>
<td></td>
<td>- All Hits In Case</td>
</tr>
<tr>
<td></td>
<td>- All Hits In Search</td>
</tr>
<tr>
<td></td>
<td>- All Hits In Term</td>
</tr>
<tr>
<td></td>
<td>- All Hits In File</td>
</tr>
<tr>
<td></td>
<td>- All File Stats In Case</td>
</tr>
<tr>
<td></td>
<td>- All File Stats In Search</td>
</tr>
<tr>
<td></td>
<td>- All File Stats In Term</td>
</tr>
<tr>
<td>Export to File</td>
<td>Opens a new context-sensitive menu. Options are:</td>
</tr>
<tr>
<td></td>
<td>- All Hits In Case</td>
</tr>
<tr>
<td></td>
<td>- All Hits In Search</td>
</tr>
<tr>
<td></td>
<td>- All Hits In Term</td>
</tr>
<tr>
<td></td>
<td>- All Hits In File</td>
</tr>
<tr>
<td></td>
<td>- All File Stats In Case</td>
</tr>
<tr>
<td></td>
<td>- All File Stats In Search</td>
</tr>
<tr>
<td></td>
<td>- All File Stats In Term</td>
</tr>
<tr>
<td>Set Context Data Width</td>
<td>Opens the <em>Data Export Options</em> window. Allows you to set a context width</td>
</tr>
<tr>
<td></td>
<td>from 32 to 2000 characters within which it can find and display the search</td>
</tr>
<tr>
<td></td>
<td>hit.</td>
</tr>
<tr>
<td>Export Search Term</td>
<td>Select to export a search term list that can be imported into this or other</td>
</tr>
<tr>
<td></td>
<td>cases.</td>
</tr>
<tr>
<td>Delete All Search</td>
<td>Deletes all search results from the Live Search Results pane.</td>
</tr>
<tr>
<td>Results</td>
<td></td>
</tr>
<tr>
<td>Delete this Line</td>
<td>Deletes only the highlighted search results line from the Live Search Results</td>
</tr>
<tr>
<td></td>
<td>pane.</td>
</tr>
</tbody>
</table>

Searching before the case has finished processing will return incomplete results. Wait to search until the case has finished processing and the entire body of data is available.

**Note:** Search terms for pre-processing options support only ASCII characters.
Live Hex Search

Hexadecimal (Hex) format includes pairs of characters in a base 16 numeric scheme, 0-9 and a-f. Hex searching allows you to search for repeating instances of data in Hex-format, and to save Hex-format data search strings to an XML file and re-use it in this or other cases.

Click the Hex (Hexadecimal) tab to enter a term by typing it directly into the search field, by clicking the Hexadecimal character buttons provided, or by copying hex content from the hex viewer of another file and pasting it into the search box. Click Add to add the hex string to the search terms list.

The instructions for conducting a live search on the hex tab are similar to conducting searches on the Pattern tab. Remember, when searching for hexadecimal values, a single alphabetic or numeric text character is represented by hex characters in pairs.

**To do a Hex search**

1. In the Live Search tab, click the Hex tab.
2. Add Hex search strings using the keyboard or using the Alpha-numeric bar above the Search Terms box.
3. Click Add to add the term to the Search Terms window.
4. Click Clear to remove all terms from the Search Terms window.
5. Repeat Steps 2, 3, and 4 as needed until you have your search list complete.
6. When you have added the search terms for this search, it is a good idea to export the search terms to a file that can be imported later, saving the time of re-entering every item, and reduces the risk of errors.
   This is particularly helpful for customized pattern searches.
7. In the Max Hits Per File field, enter the maximum number of search hits you want listed per file. The default is 200. The range is 1 to 65,535. If you want to apply a filter, do so from the Filter drop-down list in the bar below the Search Terms list. Applying a filter speeds up searching by eliminating items that do not match the filter. The tab filter menu has no effect on filtering for searches.
8. Select a Processing Manager if required.
9. Click Search.
10. Select the results to view from the Live Search Results pane. Click the plus icon (+) next to a search line to expand the branch. Individual search results are listed in the Live Search Results pane, and the corresponding files are listed in the File List. To view a specific item, select the file in the search results. All search results are highlighted in the Hex View tab.
The more complex Live Pattern “Regex” style search can be used to create pattern searches, allowing forensics analysts to search through large quantities of text information for repeating strings of data such as:

- Telephone Numbers
- Social Security Numbers
- Computer IP Addresses
- Credit Card Numbers

In the Live Search tab, click the **Pattern** tab. Each has different options. The patterns consist of precise character strings formatted as mathematical-style statements that describe a data pattern such as a credit card or social security number. Pattern searches allow the discovery of data items that conform to the pattern described by the expression, rather than what a known and explicitly entered string looks for.

These pattern searches are similar to arithmetic expressions that have operands, operators, subexpressions, and a value. For example, the following table identifies the mathematical components in the arithmetic expression, $5/((1+2)*3)$.

### Regex Pattern Search Components

<table>
<thead>
<tr>
<th>Component</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operands</td>
<td>5, 1, 2, 3</td>
</tr>
<tr>
<td>Operators</td>
<td>/, ( ), +, *</td>
</tr>
<tr>
<td>Sub-Expressions</td>
<td>(1+2), ((1+2)*3)</td>
</tr>
<tr>
<td>Value</td>
<td>Approximately 0.556</td>
</tr>
</tbody>
</table>

Like the arithmetic expression in this example, pattern searches have operands, operators, subexpressions, and a value.

**Note:** Unlike arithmetic expressions, which can only have numeric operands, operands in pattern searches can be any characters that can be typed on a keyboard, such as alphabetic, numeric, and symbol characters.
**Using Pattern Searches**

A pattern search can consist of operands. The search engine searches left to right. Operators let regular expressions search patterns of data rather than for specific values. For example, the operators in the following expression enable the search engine to find all Visa and MasterCard credit card numbers in case evidence files:

\(<(\(d\)\(\|\)\(d\)\(\|\)\(d\)[\- ]\)\)\)\(d\)\(\|\)\(d\)\(\|\)\(d\)\>

Without the use of operators, the search engine could look for only one credit card number at a time.

**Visa and MasterCard Regular Expressions**

<table>
<thead>
<tr>
<th>Operands</th>
<th>-, spacebar space</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operators</td>
<td>\ ,&lt;, ( ), [ ], (3), &gt;</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Sub-expressions</th>
<th>((d)(d)(d)), (((d)(d)(d)|-)))</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value</td>
<td>Any sequence of sixteen decimal digits that is delimited by three hyphens and bound on both sides by non-word characters (xxxx–xxxx–xxxx–xxxx).</td>
</tr>
</tbody>
</table>

As the pattern search engine evaluates an expression in left-to-right order, the first operand it encounters is the backslash less-than combination (\<). This combination is also known as the begin-a-word operator. This operator tells the search engine that the first character in any search hit immediately follows a non-word character such as white space or other word delimiter.

**Note:** A precise definition of non-word characters and constituent-word characters in regular expressions is difficult to find. Consequently, experimentation may be the best way to determine if the forward slash less-than (\<) and forward slash greater-than (\>) operators help find the data patterns relevant to a specific searching task. The hyphen and the period are examples of valid delimiters or non-word characters.
The begin-a-word operator illustrates one of two uses of the backslash or escape character (\), used for the modification of operands and operators. On its own, the left angle bracket (<) would be evaluated as an operand, requiring the search engine to look next for a left angle bracket character. However, when the escape character immediately precedes the (<), the two characters are interpreted together as the begin-a-word operator by the search engine. When an escape character precedes a hyphen (-) character, which is normally considered to be an operator, the two characters (\-) require the search engine to look next for a hyphen character and not apply the hyphen operator (the meaning of the hyphen operator is discussed below).

The parentheses operator ( ) groups together a sub-expression, that is, a sequence of characters that must be treated as a group and not as individual operands.

The \d operator, which is another instance of an operand being modified by the escape character, is interpreted by the search engine to mean that the next character in search hits found may be any decimal digit character from 0-9.

The square brackets ([ ]) indicate that the next character in the sequence must be one of the characters listed between the brackets or escaped characters. In the case of the credit card expression, the backslash-hyphen- spacebar space ([\-spacebar space]) means that the four decimal digits must be followed by either a hyphen or spacebar space.

The {3} means that the preceding sub-expression must repeat three times, back to back. The number in the curly brackets ({ }) can be any positive number.

Finally, the backslash greater-than combination (\>), also known as the end-a-word operator, means that the preceding expression must be followed by a non-word character.

Sometimes there are ways to search for the same data using different expressions. It should be noted that there is no one-to-one correspondence between the expression and the pattern it is supposed to find. Thus the preceding credit card pattern search is not the only way to search for Visa or MasterCard credit card numbers.
Because some pattern search operators have related meanings, there is more than one way to compose a pattern search to find a specific pattern of text. For instance, the following pattern search has the same meaning as the preceding credit card expression:

```
\<\((\d\d\d\d)(\-\-\ ))\{3\}\d\d\d\d\d\>  
```

The difference here is the use of the pipe (|) or union operator. The union operator means that the next character to match is either the left operand (the hyphen) or the right operand (the spacebar space). The similar meaning of the pipe (|) and square bracket ([ ]) operators give both expressions equivalent functions.

In addition to the previous two examples, the credit card pattern search could be composed as follows:

```
\<\d\d\d\d\d\d\\-\-\d\>  
```

This expression explicitly states each element of the data pattern, whereas the \{3\} operator in the first two examples provides a type of mathematical shorthand for more succinct regular expressions.

### Predefined Regular Expressions

Many predefined regular expressions are provided for pattern searching.

**Examples of Predefined Regular Expressions**

- U.S. Social Security Numbers
- U.S. Phone Numbers
- U.K. Phone Numbers
- IP Addresses
- Visa and MasterCard Numbers
- Computer Hardware
- MAC Addresses

---

**Social Security Number**

The pattern search for Social Security numbers follows a relatively simple model:

```
\<\d\d\d\d\d\d\-\-\d\d\d\d\d\d\>  
```

This expression reads as follows: find a sequence of text that begins with three decimal digits, followed by a hyphen or spacebar space. This sequence is followed by two more decimal digits and a hyphen or spacebar space, followed by four more decimal digits. This entire sequence must be bounded on both ends by non-word characters.
**U.S. Phone Number**

The pattern search for U.S. phone numbers is more complex:

```
((\<1\[-\ ]\(?\(\(\<\)\d\d\d\d\(\d\[-\ ]\)?\<\d\d\d\d\d\d\d\d\>)
```

The first part of the above expression,

```
((\<1\[-\ ]\(?\(\(\<\)\d\d\d\d\(\d\[-\ ]\)?\<\d\d\d\d\d\d\d\>)
```

means that an area code may or may not precede the seven digit phone number. This meaning is achieved through the use of the question mark (?) operator. This operator requires that the sub-expression immediately to its left appear exactly zero or one times in any search hits. This U.S. Phone Number expression finds telephone numbers with or without area codes.

This expression also indicates that if an area code is present, a number one (1) may or may not precede the area code. This meaning is achieved through the sub-expression \(\<1\[-\ ]\)?, which says that if there is a “1” before the area code, it will follow a non-word character and be separated from the area code by a delimiter (period, hyphen, or spacebar space).

The next sub-expression, \(\(\(\<\)\d\d\d\d\(\d\[-\ ]\)?\), specifies how the area code must appear in any search hits. The \(\(\<\)\) requires that the area code begin with a left parenthesis or other delimiter. The left parenthesis is, of necessity, escaped. The initial delimiter is followed by three decimal digits, then another delimiter, a right parenthesis, a period, a hyphen, a forward slash, or a spacebar space. Lastly, the question mark (?) means that there may or may not be one spacebar space after the final delimiter.

The latter portion of this expression, \(<\d\d\d\d\d\d\(\d\[-\ ]\)?\d\d\d\d\d\d\>, requests a seven-digit phone number with a delimiter (period, hyphen, or spacebar space) between the third and fourth decimal digit characters. Note that typically, the period is an operator. It means that the next character in the pattern can be any valid character. To specify an actual period (.), the character must be escaped (\ .). The backslash period combination is included in the expression to catch phone numbers delimited by a period character.
**IP Address**

An IP address is a 32-bit value that uniquely identifies a computer on a TCP/IP network, including the Internet. Currently, all IP addresses are represented by a numeric sequence of four fields separated by the period character. Each field can contain any number from 0 to 255. The following pattern search locates IP addresses:

\<[1-2]?[0-9]?[0-9]\.[1-2]?[0-9]?[0-9]\.[1-2]?[0-9]?[0-9]\>

The IP Address expression requires the search engine to find a sequence of data with four fields separated by periods (\.). The data sequence must also be bound on both sides by non-word characters.

Note that the square brackets ([ ]) still behave as a set operator, meaning that the next character in the sequence can be any one of the values specified in the square brackets ([ ]). Also note that the hyphen (-) is not escaped; it is an operator that expresses ranges of characters.

Each field in an IP address can contain up to three characters. Reading the expression left to right, the first character, if present, must be a 1 or a 2. The second character, if present, can be any value 0–9. The square brackets ([ ]) indicate the possible range of characters and the question mark (?) indicates that the value is optional; that is, it may or may not be present. The third character is required; therefore, there is no questionmark. However, the value can still be any number 0–9.

You can build your own regular expressions by experimenting with the default expressions. You can modify the default expressions to fine-tune your data searches or to create your own expressions.

Visit the AccessData website, www.accessdata.com, to find a technical document on Regular Expressions.
Creating Custom Regular Expressions
Create your own customized regular expressions using the following list of common operators

### Common Regular Expression Operators

<table>
<thead>
<tr>
<th>Operator</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>.</td>
<td>A period matches any character.</td>
</tr>
<tr>
<td>+</td>
<td>Matches the preceding sub-expression one or more times. For example, “ba+” will find all instances of “ba,” “baa,” “baaa,” and so forth; but it will not find “b.”</td>
</tr>
<tr>
<td>$</td>
<td>Matches the end of a line.</td>
</tr>
<tr>
<td>*</td>
<td>Matches the preceding sub-expression zero or more times. For example, “ba*” will find all instances of “b,” “ba,” “baa,” “baaa,” and so forth.</td>
</tr>
<tr>
<td>?</td>
<td>Matches the preceding sub-expression zero or one times.</td>
</tr>
<tr>
<td>[ ]</td>
<td>Matches any single value within the square brackets. For example, “ab[xyz]” will find “abx,” “aby,” and “abz.”</td>
</tr>
<tr>
<td>-</td>
<td>A hyphen (-) specifies ranges of characters within the brackets. For example, “ab[0-3]” will find “ab0,” “ab1,” “ab2,” and “ab3.” You can also specify case specific ranges such as [a-r],or [B-M].</td>
</tr>
<tr>
<td>&quot;</td>
<td>(Back quote) Starts the search at the beginning of a file.</td>
</tr>
<tr>
<td>'</td>
<td>(Single quote or apostrophe) Starts the search at the end of a file.</td>
</tr>
<tr>
<td>&lt;</td>
<td>Matches the beginning of a word. In other words, the next character in any search hit must immediately follow a non-word character.</td>
</tr>
<tr>
<td>&gt;</td>
<td>Matches the end of a word. In other words, the last character in any search hit must be immediately followed by a non-word character.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>\b</td>
<td>Positions the cursor between characters and spaces.</td>
</tr>
<tr>
<td>\B</td>
<td>Matches anything not at a word boundary. For example, will find Bob in the name Bobby.</td>
</tr>
<tr>
<td>\d</td>
<td>Matches any single decimal digit.</td>
</tr>
<tr>
<td>\l</td>
<td>Matches any lowercase letter.</td>
</tr>
<tr>
<td>\n</td>
<td>Matches a new line.</td>
</tr>
<tr>
<td>\r</td>
<td>Matches a return.</td>
</tr>
<tr>
<td>\s</td>
<td>Matches any whitespace character such as a space or a tab.</td>
</tr>
<tr>
<td>\t</td>
<td>Matches a tab.</td>
</tr>
<tr>
<td>\u</td>
<td>Matches any uppercase letter.</td>
</tr>
<tr>
<td>\w</td>
<td>Matches any whole character [a-zA-Z 0-9].</td>
</tr>
<tr>
<td>^</td>
<td>Matches the start of a line.</td>
</tr>
</tbody>
</table>
Common Regular Expression Operators (Continued)

<table>
<thead>
<tr>
<th>Operator</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[:alpha:]</td>
<td>Matches any alpha character (short for the [a-z A-Z] operator).</td>
</tr>
<tr>
<td>[:alnum:]</td>
<td>Matches any alpha numerical character (short for the [a-z A-Z 0-9] operator).</td>
</tr>
<tr>
<td>[:blank:]</td>
<td>Matches any whitespace, except for line separators.</td>
</tr>
<tr>
<td>(n,m)</td>
<td>Matches the preceding sub-expression at least (n) (number) times, but no more than (m) (maximum) times.</td>
</tr>
</tbody>
</table>

Searching Evidence with Index Search

Searching evidence for information pertaining to a case can be one of the most crucial steps in the examination. Index Search gives instantaneous results, and Live Search supports modes like text and hexadecimal. Search results are viewed from the File List and File Contents views in the Search tab.

This chapter details the use of the Index Search feature. It includes the following topics:

- Conducting an Index Search (page 522)
- Using Search Terms (page 523)
- Expanding Search Terms (page 523)
- Adjusting the Weighting Criteria for an Index Search Term (page 524)
- Defining Search Criteria (page 525)
- Exporting and Importing Index Search Terms (page 525)
- Selecting Index Search Options (page 526)
- Viewing Index Search Results (page 528)
- Using dtSearch Regular Expressions (page 529)
- Documenting Search Results (page 535)
- Using Copy Special to Document Search Results (page 536)
• Bookmarking Search Results (page 537)
The Index Search uses the index to find the search term. Evidence items may be indexed when they are first added to the case or at a later time. Whenever possible, AccessData recommends indexing a case before beginning analysis.

Index searches are instantaneous. In addition, in the Index Search Results List, the offset of the data in the hit is no longer listed in the hit. You will see it when you look at the hit file in Hex view.

Running an Index search on large files or Index Searches resulting in a large number of hits may make the scrollbar appear not to work. However, it will return when the search is complete. For more information about indexing an evidence item, see Indexing a Case (page 96).

The Search Criteria pane shows a cumulative total of all listed or all selected terms, based on the And or the Or operator. The cumulative total displays at the bottom of the Search Terms list. This functionality has been added to match the way the Search Terms list functioned in previous versions.

Select none, one, several, or all search terms from the list, click either And or Or, then click either All or Selected to see cumulative results. You can see this feature at work in the figure below.

Important: If you start an index search and then refresh the interface before the search finishes, the search will cancel and restart. This will cause a sizable delay when searching in large or very large cases.

The Index contains all discrete words or number strings found in both the allocated and unallocated space in the case evidence.

You can configure how special characters, spaces and symbols are indexed. This is not done by default, however. One benefit is that you can easily search on an exact email address using username@isp (the extension, such as COM or NET, is not included automatically because a period (.) is not indexed.

In addition to performing searches within the case, you can also use the index to export a word list to use as a source file for custom dictionaries to improve the likelihood of and speed of password recovery related to case files when using the Password Recovery Toolkit (PRTK). You can export the index by selecting File > Export Word List.

Note: Performing a search using Unicode only works with Live Search, not Index Search. UTF encoded documents can be searched using dtSearch.

Note: dtSearch has been updated which changes some of the search functionality and results. The search is now filtering Windows and Linux executables (EXE, BIN, OCF, and ELF). This may reduce the number of search results and reduce certain items from being shown in the filtered text. For example, the text in a header of an application may include “This program cannot be run in DOS mode”. Because it is now filtered it will not longer show in Filtered text.

Using Search Terms
Type the word or term in the Search Term field. The term and terms like it appear in the Indexed Words column displaying the number of times that particular term was found in the data. Click Add or press Enter to place the term in the Search Terms list, or double-click the term in the indexed words column to add it to the Search Terms list.

**Using Unicode Characters in Search Terms**
You can search for Unicode characters when performing a search. For example, you can search for the ö character.

**To add Unicode characters**
1. Turn on your keyboard’s Num Lock.
2. In the Terms field, enter the Unicode. For example, do the following:

   2a. Press and hold down the ALT key.
   2b. Using the numeric keypad only, type 148.
   2c. Release the ALT key and the character is entered.

**Note:** For Windows 7 and earlier you can use a 3-digit unicode number. For Windows 8 and higher you must use a 4-digit number. See [http://support.microsoft.com/kb/315684/en-us](http://support.microsoft.com/kb/315684/en-us).

**Expanding Search Terms**
When performing an Index Search, you can use the Term Browser to build a search using terms that are related to one or more keywords. You then select which words you want to include in the search.

To expand terms, a third-party lexical database called WordNet ® is used. When you expand terms, you can use the following lists: Synonyms, Related, Specific, General.

For example, you may start with a keyword of “delete.” By using the Term Browser, it will suggest synonyms, such as “erase” and “cancel”. It will also suggest related terms, such as “cut,” “deletion,” and “excision”. It will also suggest general related terms, such as “censor,” “remove,” “take,” and “withdraw.” It will also suggest specific related terms, such as “strike,” “excise,” “scratch,” and “expunge”. You can select which of those words to include in your search.

The first time that you use this feature, the WordNet dictionary must be initialized. This is a one-time event and can take 5-15 minutes for it to complete. You are prompted before the initialization begins.
To search for terms using related words
1. In the Examiner, click Index Search.
2. Enter one or more keywords to the search terms.
3. Select one or more search terms that you want to expand.
4. Click Expand Terms.

A list of synonyms is generated.
To add other related words, select the Include Related, Include Specific, and Include General check boxes.
5. You can add terms to the term list, separated by a comma, and click Expand.
6. Select the words that you want to include in the search.
7. To build a search including the words that you selected, click Add to Search.

Adjusting the Weighting Criteria for an Index Search Term
It is possible to add a weight to index search terms. This allows for an accurate, weighted percentage when the index search results populate. These terms can be either global or case-specific.

To adjust the weight of an index search term
1. Open the desired case. Navigate to Manage > Indexed Search Term Weights.
2. In the Default Indexed Search Term Weights dialog, add a search term by clicking on the Plus button, then double-clicking the Term box and typing in your term.
3. Add a weight by double-clicking the Weight box for the desired term and typing in the desired weight.
4. Click OK. The term will now be indexed using the entered weight.

Note: It is possible to add a weight while typing in the search term on the Index Tab. To do this, add :## to the end of the term. For example, to weight the word Crime at a 15, type in the term as Crime:15. If you prefer not to use the saved weight for a particular search, type in the term with a :00 at the end. For example, you would type Crime:00.

To make weighted terms global
Select the **Shared** option at the top of the *Default Indexed Search Term Weights* dialog.
To make weighted terms case-specific

- Select the Local option at the top of the Default Indexed Search Term Weights dialog.

Refine a search even more by using the Boolean operators AND and OR. You can specify the terms to use in an index search by selecting specific entries, or by searching against all entries.

You can also use the NOT operator to force the search criteria to exclude terms. To do this, in the Index Search tab, in the Terms field, type NOT before the term that you want to exclude from the search criteria and then click Add.

For example, if you do not want to include files with the term “apple” in your search, enter NOT apple into the search criteria.

The Search Terms list now shows you a cumulative total for the search terms, individually, combined, or total. You can use the operators All and Selected to see more specific results. This is helpful when refining lists and terms to limit the results to a manageable number.

You can import a list of search terms to save having to type them multiple times. This is especially helpful when the list is long, or the terms are complex. When you create a search terms document, each term begins on a newline, and is followed immediately by a hard return. Save the file in TXT format in any text editor and save it for future use.

**Important:** When creating your search criteria, try to focus your search to bring up the smallest number of meaningful hits per search.

### Exporting and Importing Index Search Terms

You can export a list of search terms you have added to the list of search terms to save for later use.

**To export a set of search terms**

1. Highlight the search terms to export to a file.
2. Click Export.
3. Provide a filename and location for the file (the TXT extension is added automatically).
4. Click Save.

**To import a saved search terms file**

1. Click Import to import a set of search terms.
2. Select the search terms file you previously saved.
3. Click Open.
Note: An imported term cannot be edited, except to delete a term and re-add it to your satisfaction.

To refine an index search, from the Index Search tab, in the Search Criteria area click Options.

Important: The Search Options, Stemming, Phonic, and Synonym and Fuzzy cannot be combined. You may enable only one at a time.

Index Search Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stemming</td>
<td>Words that contain the same root, such as <em>raise</em> and <em>raising</em>.</td>
</tr>
<tr>
<td>Phonic</td>
<td>Words that sound the same, such as <em>raise</em> and <em>raze</em>.</td>
</tr>
<tr>
<td>Synonym</td>
<td>Words that have similar meanings, such as <em>raise</em> and <em>lift</em>.</td>
</tr>
<tr>
<td>Fuzzy</td>
<td>Finds words that have similar spellings, such as &quot;raise&quot; and &quot;raize.&quot; You can enable this option for all words in a request. The level of fuzziness that you can set is 1-10. The higher the level of fuzziness, the more differences are allowed when matching words, and the closer these differences can be to the start of the word. Setting too many letter differences may make the search less useful. Incrementing the fuzzy value increases the number of letters in a word that can be different from the original search term. You can also add fuzziness directly in the search term you enter using the &quot;%&quot; character. The number of % characters that you add determines the number of differences that are ignored when you search for a word. The position of the % characters determines how many letters at the start of the word have to match exactly. For example, &quot;ca%nada&quot; must begin with &quot;ca&quot; and have just one letter difference between it and &quot;canada.&quot; Whereas, &quot;c%%anada&quot; must begin with &quot;c&quot; and have only two letter differences between it and &quot;canada.&quot; In another example, marijuana can be spelled &quot;marihuana&quot; or &quot;maryjuana.&quot; In this case, your search expression could be &quot;mar%%uana.&quot; As with the fuzzy slider bar setting, you should exercise care when you use multiple % symbols because the number of junk hits rises quickly with each added error.</td>
</tr>
</tbody>
</table>

Searching Evidence with Index Search | Using dtSearch Regular Expressions | 561
| Accents are Significant | This checkbox only appears in projects where the option to “Create an Accent Sensitive Index” option was selected prior to generating the search index.

When selected, index searches for “abc” will still return hits for all instances of “abc” whether accented or not, but in a search for “äbc”, the accent sensitivity will be strictly enforced and therefore would only return hits for “äbc”.

If this box is unchecked (which is the default setting), a search for “abc” would return hits for all instances of abc whether accented or not whereas a search for “äbc” would return hits for both “äbc” and “abc”.

See Configuring Case Indexing Options on page 96. for information on creating an Accent Sensitive Index. |
| Max Files to List | Maximum number of files with hits that are to be listed in the results field. You can change this maximum number in the field. Searches limited in this way will be indicated by an asterisk (*) and the text “(files may be limited by “Max files to list” option)” which may be cut off if the file name exceeds the allowed line length. The maximum number of possible files with hits per search is 65,535. If you exceed this limit, the remaining hits will be truncated, and your search results will be unreliable. Narrow your search to limit the number of files with hits.

**Note:** Limiting the number of files to display does not work with some images. This is caused by dtSearch counting the chunks of files as individual files that are coming from the breaking of large unallocated space files into 10MB chunks. Since Those chunks are combined back into single files, the resulting file count will be less. |
| Max Hits per File | Maximum number of hits per file. You can change the maximum number in this field. Searches limited in this way will be indicated by an asterisk (*) and the text “(files may be limited by “Max hits per file” option)” which may be cut off if the file name and this text together exceed the allowed line length. The maximum number of possible hits per file is 10,000. |
| Max Words to Return | The maximum number of words to be returned by the search. |
### Files to Search

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Files</td>
<td>Searches all the files in the case.</td>
</tr>
<tr>
<td>File Name Pattern</td>
<td>Limits the search to files that match the filename pattern.</td>
</tr>
<tr>
<td></td>
<td>Operand characters can be used to fill-in for unknown characters. The asterisk (<em>) and question-mark (?) operands are the only special characters allowed in an index search. The pattern can include “?” to match any single character or “</em>” to match an unknown number of continuous characters. For example, if you set the filename pattern to “d?ugl*”, the search could return results from files named douglas, douglass, or druglord.</td>
</tr>
<tr>
<td></td>
<td>To enter a filename pattern:</td>
</tr>
<tr>
<td></td>
<td>• Check the <strong>File Name Pattern</strong> box.</td>
</tr>
<tr>
<td></td>
<td>• In the field, enter the filename pattern.</td>
</tr>
<tr>
<td><strong>Note:</strong> Search by date range is now limited to be between Jan 1, 1970 and Dec 31, 2000.</td>
<td></td>
</tr>
<tr>
<td>Files Saved Between</td>
<td>Beginning and ending dates for the time frame of the last time a file was saved.</td>
</tr>
<tr>
<td></td>
<td>• Check the <strong>Files Saved Between</strong> box.</td>
</tr>
<tr>
<td></td>
<td>• In the date fields, type the beginning and ending dates that you want to search between.</td>
</tr>
<tr>
<td><strong>Note:</strong> Search by date range is limited to be between Jan 1, 1970 and Dec 31, 2000.</td>
<td></td>
</tr>
<tr>
<td>Files Created Between</td>
<td>Beginning and ending dates for the time frame of the creation of a file on the suspect's system.</td>
</tr>
<tr>
<td></td>
<td>• Check the <strong>Files Created Between</strong> box.</td>
</tr>
<tr>
<td></td>
<td>• In the date fields, enter the beginning and ending dates that you want to search between.</td>
</tr>
<tr>
<td><strong>Note:</strong> Search by date range is now limited to be between Jan 1, 1970 and Dec 31, 2000.</td>
<td></td>
</tr>
<tr>
<td>File Size Between</td>
<td>Minimum and maximum file sizes, specified in bytes.</td>
</tr>
<tr>
<td></td>
<td>• Check the <strong>File Size Between</strong> box.</td>
</tr>
<tr>
<td></td>
<td>• In the size fields, enter the minimum and maximum file size in bytes that you want to search between.</td>
</tr>
<tr>
<td>Save as Default</td>
<td>Check this box to make your settings apply to all index searches.</td>
</tr>
</tbody>
</table>

Click Search Now when search criteria are prepared and you are ready to perform the search.
Viewing Index Search Results

Index Search results are returned instantaneously. The Index Search Results pane displays the results of your query in a tree-type view. The tree expands to show whether the resulting items were found in allocated or unallocated space. Further, when found in allocated space, the results are separated by file category. They are then sorted by relevancy, a percentage of the hits found per search term.

Using dtSearch Regular Expressions

You can use regular expression searching capabilities in the dtSearch index search tab. This functionality does not use RegEx++ that is used in the Live Search tab. dtSearch utilizes the TR1 (Technical Report 1) regular expressions.

Regular expressions in dtSearch provide a powerful syntax for searching for complicated patterns in text, such as one of several possible sequences of letters followed by a sequence of numbers. Regular expressions can also be used to express spelling variations of individual words. Regular expression patterns are arbitrary (i.e., supplied by the user dynamically) and cannot be pre-indexed.

Regular expression searching in dtSearch is limited to a single whole word. A regular expression included in the dtSearch box must be quoted and must begin with ##. An example of this is:

Apple and "##199[0-9]" - will find Apple and 1990 through 1999 Apple and "##19[0-9]+" - will find Apple and 190 through 199

However, if you want to look for Apple Pie, you cannot use "##app.*ie" since this is two words. Only letters and numbers are searchable. You cannot search for any of the non-indexed characters as defined in the Index Search Settings in the Detailed Options section of a case creation. Also, dtSearch does not store information about line breaks so any searches that are made that include the beginning of a line or the end of a line will not work.

Search considerations using the wildcard character "*" in a regular expression does have an effect on search speed: the closer to the front of a word the expression is, the more it will slow searching. "Appl.*" will be nearly as fast as "Apple", while ".*pple" will be much slower.

Note: Advanced searching for Social Security Numbers and Credit Card Numbers and other number patterns can be achieved, however modifications to the dtSearch engine must be made before processing the case. For more details, see Advanced Searching on page 7 of this paper.

For more information, see:

TR1 Regular Expressions For Text Patterns

Element Terms

Characters and target sequences are referred to as an Element and can be one of the following:

- A literal character typed as the actual letter or number (a or 1).
- A '.' (period) is any single character.
- An '*' (asterisk) is a wildcard character.
- (a) is a capture group.
- \d is a decimal character.
- For hex searches, \xh matches a hex entry (ie - \x0f).
- {2} is a repetition character.
- A ';' (comma) is a minimum character.
- (aa?) is a target sequence.
- An alternation character search is ‘this|that’.
- A concatenation sequence is ‘(a){2,3}(b){2,3}(c)’.
- A back reference is ‘((a+)(b+))(c+)\3’.
- (?:subexpression) matches the sequence of characters in the target sequence that is matched by the pattern between the delimiters.
- (?!:subexpression) matches any sequence of characters in the target sequence that does not match the pattern listed in the subexpression.
- A bracket or range expression of the form “[expr]”, which matches a value or a range, similar to a “set” in the Live Pattern Search.

Examples:

- “##a” matches the target sequence “a” but does not match the target sequences “b”, or “c”, and so on.
- “##.” matches a single character such as “a”, “b”, and “c”, and so on.
- “##sal*” matches the target ’sale’ and the target “salt” and so on.
- “##(a)” capture group, matches the target sequence “a” but does not match the target sequences “b”, or “c”, and so on.
- “##\d\d\d\d” matches the target sequence of four digits “1234”.
- “##aa?” or (0,1) matches the target sequence of “aa” and the target sequence of “aaa”.
- “##ab” matches the target sequence “ab.”
• "##[b-z]" or range, matches the target sequences "b" and "c" but does not match the target sequences "a".
• "##tom|jerry" matches the target sequence of 'tom' or 'jerry'.
• "##\d{4}" or repetition, matches the target sequence of four digits "1234".
• "##(?:aa)" or target sequence, matches the target sequence of "aa" and the target sequence of "aaa", and so on.

Ordinary Character

By entering actual ASCII characters, the search will return that set of characters after the element(s) are entered. By entering ordinary characters, "##nick", you would find said characters. However, if you wanted to look for Nick Davis, you could not use "##nick davis" since this is two words.

Single "Any" Character and Wildcard

The use of the any character element can be used if a letter or letters may be different, such as difference in spelling (example 'marijuana' and 'marihuana'). The wildcard is used to find any combination of characters after an element is entered.

Examples:
• "##(a*)" matches the target sequence "a", the target sequence "aa", and so on.
• "##a*" matches the target sequence "a", the target sequence "aa", and so on.
• "##(a.)" matches the target sequence "aa", the target sequence "ab", but will not find the target sequence the target sequence "aaa".
• "##a." matches the target sequence "aa", the target sequence "ab", but will not find the target sequence the target sequence "aaa".
• "##.*ick" matches the target sequence "nick", the target sequence "click", and so on.
• "##mari.uana" matches the target sequence "marijuana" and the target sequence "marihuana".

Capture Group

A capture group marks its contents as a single unit in the regular expression and labels the target text that matches its contents. The label that is associated with each capture group is a number, which is determined by counting the opening parentheses that mark capture groups up to and including the opening parenthesis.

Examples:
• "##(ab)*" matches the target sequence "ab", the target sequence 'abab", and so on.
• "##(a+)\(b+)\) matches the target sequence "ab, the target sequence "aab", the target sequence "abb", and so on.
• "##ab+" matches the target sequence "abb" but does not match the target sequence "abab."
• "##(ab)+" matches the target sequence "abab" but does not match the target sequence "abb."
• "##((a+)\(b+)\)(c+)" matches the target sequence "aabbbc" and associates capture group 1 with the subsequence "aabb", capture group 2 with the subsequence "aa", capture group 3 with "bbb", and capture group 4 with the subsequence "c".

Repetition
Any element can be followed by a repetition count. Examples:
• "##(a\{2\})" matches the target sequence "aa" but not the target sequence "a" or the target sequence "aaa".
• "##(a\{2,\})" matches the target sequence "aa", the target sequence "aaa", and so on, but does not match the target sequence "a".

A repetition count can also take the following form:
• "?" - Equivalent to "\{0,1\}". Examples:
• "a?" matches the target sequence "" and the target sequence "a", but not the target sequence "aa".
• "##(a\{a?\})(bbbb?)(c)" matches the target sequence "aabbbbc" and the target sequence "abbbc".

Decimal Character
You can locate any set of decimals by using the \d character element in the expression. Examples:
• "##\d\d\d\d" matches the target sequence "1234".
• "##\d[3]" matches the target sequence "123".
• "##\d\{3\}\d\d\d\d" matches the target sequence "1234567".
• Visa and "##\d\{4\}" will match any files that contain the word 'visa' and any four digits.
Alternation
A concatenated regular expression can be followed by the character '|' and another concatenated regular expression. Any number of concatenated regular expressions can be combined in this manner. The resulting expression matches any target sequence that matches one or more of the concatenated regular expressions.
Example:
- "##(nick|houston)" matches the target sequence "nick", or the target sequence "houston".

Concatenation
Regular expression elements, with or without repetition counts, can be concatenated to form longer regular expressions. The resulting expression matches a target sequence that is a concatenation of the sequences that are matched by the individual elements.
Examples:
- "##(a){2,3}(b){2,3}(c)" matches the target sequence "aabbc", the target sequence "aabbbbc".
- "##\d{4}{4}" matches the target sequence of "1234123412341234" (16 digits - no spaces).

Back Reference
A back reference marks its contents as a single unit in the regular expression grammar and labels the target text that matches its contents. The label that is associated with each capture group is a number, which is determined by counting the opening parentheses that mark capture groups up to and including the opening parenthesis that marks the current capture group. A back reference is a backslash that is followed by a decimal value N. It matches the contents of the Nth capture group. The value of N must not be more than the number of capture groups that precede the back reference.
Example:
- "((a+)(b+))(c+)\3" matches the target sequence "aabbccbb". The back reference "\3" matches the text in the third capture group, that is, the "(b+)". It does not match the target sequence "aabbccbb".
  - The first capture group is ((a+)(b+))
  - The second capture group is (a+)
  - The third capture group is (b+)
  - The fourth capture group is (c+)

Bracket or Character Range
A character range in a bracket expression adds all the characters in the range to the character set that is defined by the bracket expression. To create a character range, put the character '-' between...
the first and last characters in the range. Doing this puts into the set all characters that have a numeric value that is more than or equal to the numeric value of the first character, and less than or equal to the numeric value of the last character.

Examples:
- 
  • "[0-7]" represents the set of characters \{ '0', '1', '2', '3', '4', '5', '6', '7' \}. It matches the target sequences "0", "1", and so on, but not "a".
  • "[h-k]\) represents the set of characters \{ 'h', 'i', 'j', 'k' \}.
  • "[0-24]\) represents the set of characters \{ '0', '1', '2', '4' \}.
  • "[0-2]\) represents the set of characters \{ '0', '1', '2' \}.

An individual character in a bracket expression adds that character to the character set that is defined by the expression. If the bracket expression begins with a "\^" then this defines that the expression will consider all characters except for those listed.

Examples:
  • "[abc]\) matches the target sequences "a", "b", or "c", but not the sequence "d".
  • "[\^abc]\) matches the target sequence "d", but not the target sequences "a", "b", or "c".
  • "[\^a\^bc]\) matches the target sequences "a", "b", "c", or "\^", but not the target sequence "d".

**TR1 Regular Expressions For Number Patterns**
If order to achieve dtSearch capability in FTK for search strings such as Social Security Numbers, Credit Card Numbers, Employee Identification Numbers, Telephone Numbers, and so on, where a period or hyphen is present, certain steps must be done during the pre-processing phase of the case.

**Note:** NOTE: Currently, you cannot include search patterns with spaces.

Normal dtSearch strings for credit card numbers or social security numbers
The normal dtSearch wildcard string can be utilized as long as the hyphen is set to be indexed as a space:
  • Social Security Numbers - ==== ===
    ▪ Returns "123-45-6789"
    ▪ Will not return "123 45 6789"
  • Credit Card Numbers (16 digits) - ==== ===
    ▪ Returns "1234567890123456"
    ▪ Will not return "123 45 67890123 45 67890123 45 67890"
- Returns "1234-1234-1234-1234"
- Will not return "1234 1234 1234 1234"

Number Patterns
You can use dtSearch TR1 Regular Expression to find number patterns as you can in Live Searches for such things as Credit Card Numbers, Social Security Numbers, xxxxxxxx. Certain pre-processing options MUST be completed before this function will work.
Configuring Pre-Processing Options
If you to utilize the dtSearch TR1 Regular Expression functions for looking for number patterns, you must complete the following pre-processing options:

1. Start a new case.
2. Click Custom processing profile.
3. Click Indexing Options next to dtSearch Text Index.
4. On the Indexing Options dialog window set the following:
   - For Hyphen Treatments - set to Hyphen
   - In the Spaces section - remove the period
   - In the Spaces section - remove the left and right parenthesis
   - In the Letters section - click Add and in all 4 spaces, type a "." period and repeat for the left and right parenthesis, then click OK.
5. Process the case.

Examples of TR1 Regular Expressions for Number Patterns
- For Credit Card Numbers:
  - "##(\d{4}[\-\.)](\d{4}[\-\.)](\d{4}[\-\.)](\d{4}))"

  The first three groups are composed of - (\d{4}[\-\.)]. The expression is looking for four digits followed by a period, or hyphen. This group is repeated three times and followed by the group looking for the ending 4 digits.
  We can shorten that expression by writing it "##((\d{4}[\-\.)]{3})(\d{4}))". This will find 1234-5678-1234-5678 or 1234.5678.1234.5678

- For Social Security Numbers -
  - "##(\d{3}[\-\.)](\d{2}[\-\.)](\d{4}))".
  - This will find 123-45-6789 or 123.45.6789

- For U.S. Telephone Numbers -
  - "##(\d{4}[\-\.)]?((?\d{3}[\-\.)]?([\-\.)]?\d{3}[\-\.)]?([\-\.)]?\d{4}))" This will find:

567-8901
234-567-8901
1-234-567-8901
(234)567-8901
(234)-567-8901
567.8901
234.567.8901
1.234.567.8901
(234)567.8901
(234).567.8901
Using Copy Special to Document Search Results

Once a search is refined and complete, it is often useful to document the results. Right-click an item in the Search Results list to open the quick menu with the following options:

- **Create Bookmark:** Opens the Create Bookmark dialog. For more information on creating and using Bookmarks, see Using the Bookmarks Tab (page 505).

- **Copy to Clipboard:** Copies the selected data to the clipboard (buffer) where it can be copied to another Windows application, such as an Excel (2003 or earlier) spreadsheet.

---

**Note:** The maximum number of lines of data that can be copied to the clipboard is 10,000.

- **Export to File:** Copies information to a file. Select the name and destination folder for the information file. Uses the same criteria as Copy to Clipboard.

- **Set Context Data Width:** Context data width is the number of characters that come before and after the search hit.

- **Delete All Search Results:** Use this to clear all search results from the Index Search Results pane.

### Copy or Export Search Results

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Hits in Case</td>
<td>Saves all the current search terms' hits found from the entire case.</td>
</tr>
<tr>
<td>All Hits in Search</td>
<td>Saves all the search hits found in each search branch.</td>
</tr>
<tr>
<td>All Hits in Term</td>
<td>(Live search only) saves the instances of individual terms found from the list of search terms. For example, if a live search consisted of the list “black,” “hole,” “advent,” and “horizon,” this option would copy information on each of the terms individually.</td>
</tr>
<tr>
<td>All Hits in File</td>
<td>Records the instances of the search term in the selected file only.</td>
</tr>
<tr>
<td>All File Stats in Case</td>
<td>Creates a CSV file of all information requested in the case.</td>
</tr>
<tr>
<td>All File Stats in Search</td>
<td>Creates a CSV file of the information requested in the search.</td>
</tr>
<tr>
<td>All File Stats in Term</td>
<td>(Live search only) Creates a CSV file of the instances of individual terms found from the list of search terms.</td>
</tr>
</tbody>
</table>
Using Copy Special to Document Search Results
Using Copy Special to Document Search Results

After the information is copied to the clipboard, it can be pasted into a text editor or spreadsheet and saved. Choose Export to File to save the information directly to a file. Specify a filename and destination folder for the file, and then click OK. Search results can then be added to the case report as supplementary files.

Important: When exporting Index Search result hits to a spreadsheet file, the hits are exported as a CSV file in UTF-16LE data format. When opening in Excel, use the Text to Columns function to separate the Index Search hit values into columns.

The Copy Special feature copies specific information about files to the clipboard.

**Method 1 to copy information about the files in your search results**
1. Click in the search results list.
2. From the menu bar, select Edit > Copy Special.

**Method 2 to copy information about the files in your search results**
1. Find that file highlighted in the File List view.
2. Right-click on the desired file.
3. Select Copy Special.
4. Choose the column settings template to use from the drop-down list. Click Column Settings to define a new column settings template.

4a. Modify the column template in the Column Settings Manager. For more information on customizing column templates, see Customizing File List Columns (page 613).

   4b. Click Apply to return to the Copy Special dialog.
5. Select the customized column template if you created one.
6. Choose whether you want to include the header row in the file.
7. Under File List Items to Copy, select the option that best fits your needs:

   - **All Highlighted** to copy only the items currently highlighted in the list.
   - **All Checked** to copy all the checked files in the case.
   - **Currently Listed** to copy all currently listed items, but no others.
   - **All** to copy all items in the case.
8. The dialog states the number of files that your selection contains.
9. Click OK.
To keep track of particular search results, add them to new or existing bookmarks. Search results in the file list can be selected and added to a newly-created bookmark, or added to an existing bookmark as with any other data.

**To create a bookmark from the file list**

1. Select the files you want to include in the bookmark.
2. Right-click any of the selected files and select **Create Bookmark**.
3. Complete the **Create New Bookmark** dialog.
4. Click **OK**.

The bookmark appears in the **Bookmark** tab.

**Examining Volatile Data**

This chapter includes the following topics

- **Using the Volatile Tab** (page 539)
- **Understanding Memory** (page 541)
- **Viewing Memory Dump Data** (page 542)
- Performing File Remediation from the Volatile Tab (page 544)
- **Killing a Process** (page 544)
- **Wiping a File** (page 545)
- Adding Hashes to KFF Library from the Volatile Tab (page 545)
- Adding Hashes to Fuzzy Hash Library from the Volatile Tab (page 546)
- **Creating a Memory Dump File** (page 546)
The Volatile tab provides tools for viewing, finding, and comparing data gathered from the memory of live agent systems in your network. Other data acquired remotely, such as from a Mounted Image Drive or a Mounted Device is viewable from other tabs. The Volatile tab is specifically for remote memory data acquired as a memory dump. It can be added directly to a case upon acquisition, or saved as a dump file to be added to any case at a later time. See Acquiring Live Evidence (page 158).

When you have acquired volatile (Memory) data as a dump file the resulting acquisition data is displayed in the Volatile tab.

There are three main areas in the Volatile tab:
1. Tabbed Data View
2. Detail List View
3. Detailed Information View

It is important to remember that the views relate clockwise. When an item is selected in the Tabbed Data view, the related information is displayed in the Detail List view. An item selected in the Detail List view will display relevant information in the Detailed Information view, within the data tab that relates to the type of item that is selected.
The *Tabbed Data view* has three tabs:

- Snapshot
- Find
- Difference

Each *Tabbed Data View* displays a summary of acquired volatile data. You can sort the data in the following ways:

**Data View Sort Options**

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Image]</td>
<td>Sort acquired volatile data by <em>Operation Type</em>, such as those selectable from the <strong>Evidence &gt; Add Remote Evidence &gt; Selection Information</strong> dialog box. Found on Snapshot, Find, and Difference tabs.</td>
</tr>
<tr>
<td>![Image]</td>
<td>Sort acquired volatile data by the <em>Time of Acquisition</em>, displayed in the local machine’s time. Found on Snapshot, Find, and Difference tabs.</td>
</tr>
<tr>
<td>![Image]</td>
<td>Sort acquired volatile data by the <em>Source Machine or Agent</em>. Found on Snapshot, Find, and Difference tabs.</td>
</tr>
<tr>
<td>![Image]</td>
<td><em>Display saved comparisons</em>. When a comparison of found data is done, the results can be saved and viewed later. Found only on the Difference tab.</td>
</tr>
</tbody>
</table>

*Geolocation*. This button on the Volatile tab that will launch Geolocation for volatile data. See *Using Geolocation Tools* on page 600.

You can select from the following categories to view the data that you selected to collect:

- Process List
- Dll List
- Sockets
- Network Devices
- Driver List
- Service List
- User List
- Open Handles

The Detail List View provides information specific to the item currently selected in the Data View.
The content of the Detail List changes as different items are selected.

The Detailed Information View shows more specific information about the item in the Data View, and its selected component in the Detail List view.
Understanding Memory

Memory can include the physical “sticks” of memory that we put into the machine, commonly referred to as physical memory. However, video cards, network cards, and various other devices use memory that the Operating System (OS) must be able to access in order for the devices to work properly. Both physical memory and device memory are organized by the OS in a linear address map. For 32-bit operating systems, the linear address map is naturally 4GB. Traditionally the OS will put physical memory at the bottom of this map and the device memory at the top.

When a system has a full 4GB of physical memory, using all 4GB wouldn’t leave any room to address the device memory. Since the OS can’t function without access to the device memory, it simply doesn’t use all 4GB of physical memory. Evidence of this fact can be seen on the main Properties window of My Computer. If you have a 32-bit Windows XP system with 4GB of physical memory, you may notice that the Properties window will show that you have only 3.25GB of physical RAM. That limitation allows for addressing of devices within the 4GB address space.

Most acquisition products check how much physical memory is available (4GB using our example above), open a handle to the OS’s memory map (referred to as \Device\PhysicalMemory) and start reading, one page at a time. Thus, in an attempt to read all of the physical memory, what they are actually reading is the OS’s linear address map of both physical and device memory. However, some device memory is not meant to be read and the simple act of reading it could cause system instability. In fact, if the OS is 64-bit, this algorithm would miss the physical memory that was placed beyond the 4GB range.

The approach AccessData takes is to query the OS’s memory map for the regions that correspond to physical memory and only acquire those regions – filling the other regions with zeros. This method not only avoids any issue with system instability but also guarantees that it acquires all the physical memory that the OS is able to use — the memory that anyone would normally be interested in.
Viewing Memory Dump Data

A Memory Dump file includes all the Processes, DLLs, Sockets, Drivers, Open Handles, Processors, System Descriptor Tables and Devices in use at the time of the acquisition. The Volatile tab provides a view of all this data by type.

Right-click on any dump file in the Snapshot view to choose View Memory or Search Memory.

Viewing Hidden Processes

Hidden processes are automatically detected. There is no way to disable or turn off this feature. The detection compares a list of processes in memory to the operating systems's processes list to determine whether any running processes do not belong. These are the processes that are highlighted in yellow.

Hidden processes, when detected in a Memory Dump file, and found only in the Process List. Click on a dump file in the Process List, then scroll down the Detail List to locate any lines highlighted in yellow.

Click on a yellow-highlighted line in the Detail List to display related information in the Detailed Information list. Scroll across the columns list to see all the data.

Viewing Input/Output Request Packet Data

Input/Output Request Packet (IRP) data, also known as memory hooks, when detected in a memory dump file, are indicated in the Snapshot view by a yellow warning indicator. Memory hooks can be used for both legitimate and non-legitimate purposes.

In the Detail list, the items that contain memory hooks are highlighted in pink. Click on a pink-highlighted item to open that item in the Detailed Information view. The IRP tab shows the items and properties that are related to the IRP data that was detected. This data does not identify whether the IRP was bad or good, only that it was there, so you can determine its nature.

Tabs in the Detailed Information list provide additional related data for the selected data type. Some data types have several tabbed pages, and some have only a few. Each tabbed page contains different information related to the selected item, and each displays properties specific to the tabbed page for that information type. The property column headings are sortable to make it easier to locate critical information.

In addition to the IRP data view, access is provided to Service Descriptor Tables (SDT), and System ServiceDescriptor Tables (SSDT).

Up to four SSDT tables are available. The four tabs are placeholders only; their existence does not indicate no guarantee they will be populated. Notice that the names of the populated tables’ tabs are longer than those that are not populated. Only the data that is found in the evidence can be displayed.

Viewing Virtual Address Descriptor (VAD) Data
In the Windows operating system, every object opened by a program (example files, screens, sections of memory, etc.) is assigned a handle that the process in which the program is running can use. These handles are stored in a table that is managed by the process. This table is called the virtual address descriptor table (VAD).

A single process normally contains many VADs. Each VAD describes a range of virtual pages and tells the Memory Manager what those virtual pages represent. For example, a typical process will consist of an executable image (the program) and a set of dynamic link libraries (DLLs) that are used within that process, as well as data that is unique to the program. Each of these separate items exists somewhere within the address space of the program.

When each component is first loaded into the address space, the Memory Manager creates a new VAD entry for each such range of addresses. These VAD entries are in turn linked together in a binary tree that optimizes access to the most recently accessed VAD. This representation makes it easy to describe a sparse address space using a tree of VADs, it is fast to find entries within the VAD tree, and it is easy to reorganize VAD entries as necessary.

Investigating the VAD tree lets you view resources allocated by a program. The VAD tree constantly changes during execution of a program. Each time the VAD tree is read, the results are different.

**To view Virtual Address Descriptor (VAD) Data**

1. In the *Examiner*, select the *Volatile* tab.
2. In the *Snapshot* tab, expand **Process List**.
3. Expand the date of the snapshot.
4. Select the computer name.
5. In the upper-right pane, under *Detail List*, select a process.
6. In the lower-right pane, under *Detailed Information*, click the *VAD* tab.
7. The Virtual Address Descriptor (VAD) information is displayed in the *Detailed Information* pane.
Certain file remediation tasks are available for specific data types in the Volatile tab. After a remote volatile data acquisition is completed, click to expand the data type in the Snapshot tabbed view, then right-click on the item in the Detail List to choose from the available file remediation options.

**Volatile Tab File Remediation Options**

<table>
<thead>
<tr>
<th>Volatile Data Type</th>
<th>Kill Process</th>
<th>Wipe File</th>
<th>Add Hashes to KFF Lib</th>
<th>Add Hashes to Fuzzy Lib</th>
<th>Dump</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process List</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>DLL List</td>
<td>--</td>
<td>--</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Sockets</td>
<td>--</td>
<td>--</td>
<td>--</td>
<td>--</td>
<td>--</td>
</tr>
<tr>
<td>Driver List</td>
<td>--</td>
<td>--</td>
<td>X</td>
<td>X</td>
<td>--</td>
</tr>
<tr>
<td>Open Handles</td>
<td>--</td>
<td>--</td>
<td>--</td>
<td>--</td>
<td>--</td>
</tr>
<tr>
<td>Processors</td>
<td>--</td>
<td>--</td>
<td>--</td>
<td>--</td>
<td>--</td>
</tr>
<tr>
<td>System Descriptor Table</td>
<td>--</td>
<td>--</td>
<td>--</td>
<td>--</td>
<td>--</td>
</tr>
<tr>
<td>Devices</td>
<td>--</td>
<td>--</td>
<td>--</td>
<td>--</td>
<td>--</td>
</tr>
</tbody>
</table>

**Killing a Process**

Kill Process ends a process running on the remote computer the data was acquired from.

**To kill a process**

1. In the *Snapshot* view, click and expand the *Process List*.
2. In the *Detail List*, highlight or mark the check boxes of the processes to be killed.
3. Right-click in the Detail List and select *Kill Process*.
4. In the *Select Source* dialog box, select either *Highlighted Detail List items*, or *Checked items*.
5. Click *OK*. 
Wipe File completely removes a file from the remote computer the file was acquired from.

To wipe a file
1. In the Snapshot view, click and expand the Process List.
2. In the Detail List, highlight or mark the check boxes of the file to be wiped.
3. Right-click in the Detail List and select **Wipe File**.
4. In the Select Source dialog box, select either Highlighted Detail List items, or Checked items.
5. Click **OK**.

Adding Hashes to KFF Library from the Volatile Tab
Hashes can be added directly to the KFF Library directly from the Volatile tab.

To add hashes to the KFF Library
1. In the Detail List, highlight or mark the check boxes of the hashes to add to the KFF Library.
2. Right-click in the Detail List, and click **Add Hashes to KFF**.
3. Provide a name for the set.
4. Click **Add all hashes** to add the hashes of all displayed items, or **Add only checked hashes** in the current Detail List.
5. Select either **Alert** or **Ignore**.
6. Choose whether or not to Activate in [the current] case.
7. Click **OK**.
Hashes can be added directly to the Fuzzy Hash Library directly from the Volatile tab.

**To add hashes to the Fuzzy Hash Library**
1. In the Detail List, highlight or mark the check boxes of the file(s) hashes to add to the Fuzzy Hash Library.
2. Right-click in the Detail List, and click **Add Hashes to Fuzzy**.
3. Provide a name for the set.
4. Click **Add all hashes** to add the hashes of all displayed items, or **Add only checked hashes** in the current Detail List.
5. Select either **Alert** or **Ignore**.
6. Assign a Threshold Value.
7. Choose whether or not to Activate in [the current] case.
8. Click **OK**.

**Creating a Memory Dump File**
A dump file can be created and added to the case directly from the Volatile tab.

**To create a Dump file**
1. In the *Snapshot* view, click and expand the *Process List* or the DLL List.
2. In the *Detail List*, highlight or mark the check boxes of the files to be dumped.
3. Right-click in the Detail List and select **Dump to file**.
4. In the *Dump a file* dialog box, mark Include DLLs with processes, and/or Include parent process with DLLs.
5. Browse to and select a destination path for the dump file.
6. Click **OK**.
Viewing System Information

About Viewing System Information

You can view system information that contains detailed information about disk images in an easy to read format. You can view several important pieces of information about the target computer and the users of that computer. **System Summary is not indexed.**

You can view this information in the System Summary tab.

Not all attributes are available for all disk images, however, the possible attributes that you can see are:

- Applications
  - Prefetch
  - User Assist
  - Installed
- Browser
  - Cookies
  - URLs
- Network Information
  - Network Shares
  - Network Connections
  - Wireless Profiles
- Owner Information
- Recent Files
  - LNK
  - NT User
  - Shortcuts (LNK)
- SAM Users
- Shell Bags
- USB Devices

For details about the attributes, see Available System Information Data (page 439).
OSX System Information

Additionally, FTK now supports OSX system summary parsing. The options may differ on the version of OSX being processed.

- Applications
  - Installed
  - Application Permissions - MAC
  - Resumed Apps - MAC
  - StartUp Items - MAC
  - Menu Bar Apps - MAC
  - Dock Items - MAC
  - Core Analytics - MAC
  - KnowledgeC Application Activities
  - KnowledgeC Application Focus
  - KnowledgeC Application Usage

- Device Interaction
  - USB Devices
  - USB Connections History
  - AirDrop Discoverability
  - AirDrop Background Activity
  - Bluetooth Devices
  - Peripheral Device Information
  - KnowledgeC Device Plugged-In State

- Browsers
  - iCloud Downloads
  - iCloud Local Files
  - iCloud Uploads
  - KnowledgeC Safari History
  - Keyword Searches
  - Credentials
  - Downloads
  - Cookies
  - Rebuilt webpages
  - Social Media URLs
  - Darknet URLs
- Cryptocurrency URLs
- Tax Site URLs
- Google Searches
- Google MAPS Queries
- Phishing URLs
- Pornography URLs

- Networks
  - Network Utilities - MAC
  - Network Usage - Application Data
  - Network Usage Connections - MAC
  - Network Profiles - MAC
  - Network Interfaces - MAC
  - Daily Logs - Network Interface Status - MAC

- Recent Files/Folders
  - Bash/ZSH Sessions
  - Finder MRU - MAC
  - Recently Used Items
  - Spotlight Shortcuts

- File System Information
  - Volume Information
  - File System Information - APFS
  - File System Events

- Operating SDYstem Information
  - Timezone Information - MAC - Duplicate of (PowerLog Timezone Information)
  - Apple Accounts
  - User Accounts - MAC
  - Recovery Account Information
  - Deleted Accounts
  - Rebuilt Desktops
• Other KnowledgeC, PowerLog & Log Data
  ▪ PowerLog Timezone Information
  ▪ PowerLog Process Data Usage
  ▪ PowerLog Battery Level
  ▪ KnowledgeC Activity Level
  ▪ KnowledgeC Notification Usage
  ▪ KnowledgeC Screen Backlight States
  ▪ Daily Logs - Disk Status
  ▪ Daily Logs - Local System Status

The System Information tab is not populated with data by default. You must extract data during processing.

To extract data and have it populated in the System Information tab
  ❖ You must do one of the following:
    ● When adding disk images to a case, select the Generate System Information processing option. See Evidence Processing Options on page 88.
    ● For an existing case, use the Generate System Information option in Additional Analysis. See Using Additional Analysis on page 147.
Viewing System Information

After you have processed a disk image, you can view the system information.

To view system information data
1. Open the Examiner and click the System Information tab.

You can choose one image at a time to review in further detail. On the left hand side, there is a dropdown list of all of the images that have been processed into the case.
2. Select the disk image that you want to view.
3. Select the nodes that you want to view.

A tree of available attributes from the disk appears in the Categories panel.
On the right side of the tab, there are two panels which display additional information about the node you select on the left. The upper panel is titled Items and the lower panel is titled Provenance.

The Items panel displays lists of the attributes found within the selected node. For example, when looking at the Applications node, you may want to review a list of applications frequently used by the users of the target machine. You can select the node User Assist under the Applications node. Once you select this node from the tree on the left, in the Items panel you see a list of all of the applications frequently used by the users of the target machine along with the user that used that application, the number of times that application had been run, and the last time the application was run.

The Item list allows you to sort any column in either ascending or descending order to assist you in finding the information you need quickly.

In the Provenance panel, you can find the location of the data selected from the Items panel. Using the previous example of frequently used applications, you may want to review an application used by a specific user. From the Items list, you select the application you are interested in, and in the Provenance panel, you see the location from the target machine from which this information was obtained.
4. (Optional) In the Provenance panel, you can select the object, right-click, and set a bookmark.
Available System Information Data

This section contains information about the possible data available in the System Information tab. All of the data is collected from one or more sources, where a source can be a single file or a location within the file. Where possible, the complete source path is shown in the Provenance pane. Below are the details of the data available for each category and sub-category.

Possible data available in the System Information tab

<table>
<thead>
<tr>
<th>Category</th>
<th>Sub-Category</th>
<th>Description</th>
</tr>
</thead>
</table>
| Application Data | **Prefetch** | Each time you turn on your computer, Windows keeps track of the way your computer starts and which programs you commonly open. Windows saves this information as a number of small files in the prefetch folder. The next time you turn on your computer, Windows refers to these files to help speed the start process.

The prefetch folder is a subfolder of the Windows system folder. The prefetch folder is self-maintaining, and there's no need to delete it or empty its contents. If you empty the folder, Windows and your programs will take longer to open the next time you turn on your computer.

For each prefetch (.PF) file, in the System Information tab displays the following information:
- Complete path to the application executable
- Number of times the application was run
- Last time the application was run |
| User Assist     | **UserAssist** | UserAssist is a method used to populate a user’s start menu with frequently used applications. This is achieved by maintaining a count of application use in each user’s NTUSER.DAT registry file at sub key:

Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist

For each UserAssist entry in the registry, the System Information tab displays the following information:
- Complete path to the application executable
- Number of times the application was run
- Last time the application was run |
Possible data available in the System Information tab (Continued)

<table>
<thead>
<tr>
<th>Category</th>
<th>Sub-Category</th>
<th>Description</th>
</tr>
</thead>
</table>
| Installed    |              | Applications installed on the Windows system are viewable via the Control Panel -> Programs and Features. By default the list doesn’t show updates or system components unless the user selects to see them. The information can come from various places in the registry but the feature uses the HKLM\SOFTWARE registry file under the sub keys:  
  • Microsoft\Windows\CurrentVersion\Uninstall\  
  • Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\  
  Service packs, hot fixes, updates, or system components are not reported. For each installed application, the System Information tab displays the following information:  
  • Application name  
  • Application publisher (if available)  
  • Path to installed application (if available)  
  • Date application was installed (if available)  
  • Size of application install base (if available)  
  • Application version (if available) |
| Browser      | Cookies      | Represents an aggregation of cookies (listed with their corresponding attribute “Names” and their “Values”) cached by all supported web browsers installed to the system being investigated. |
|              | URLs         | An aggregation of URLs cached by the browsers installed to the system being investigated and the user profiles to which they belong. |
| Network Data | Network Shares | A network share is a computer resource made available from one host to other hosts on a computer network. In this feature, it is specifically the networks that were accessed using the Universal Naming Convention (UNC). This information is stored in each user’s NTUSER.DAT registry file at sub keys:  
  • Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoint s2  
  For each installed application, the System Information tab displays the following information:  
  • UNC Path  
  • Last connection time |
Possible data available in the System Information tab (Continued)

<table>
<thead>
<tr>
<th>Category</th>
<th>Sub-Category</th>
<th>Description</th>
</tr>
</thead>
</table>
| Network Connections |                   | A network connection provides connectivity between one computer and the Internet, a network, or another computer. In every case the connected to network has an identifying name. Network connections managed by Windows are stored in the HKLM\SOFTWARE registry file under the sub key:  
  • Microsoft\Windows NT\CurrentVersion\NetworkList  
For each network connection, the System Information tab displays the following information:  
  • Profile name  
  • First time connecting to the network  
  • Most recent time connecting to the network  
  • Network name  
  • Network category (e.g. Domain, Private, Public)  
  • Gateway MAC address  
  • Whether it is a wireless network (This is only set if for sure it is a wireless network) |
| Wireless Profiles  |                   | A wireless profile is a set of configuration parameters that allow a system to connect to a wireless access point. The profiles managed by Windows are stored in the file C:\ProgramData\Microsoft\Wlansvc\Profiles\Interfaces  
For each wireless profile, the System Information tab displays the following information:  
  • Profile name  
  • SSID  
  • Authentication (e.g. WPA2PSK, WPAPS K, etc.)  
  • Encryption (e.g. TKIP, AES, none, etc.) |
| Owner Information Data |       | This is basic data about the installed operating system and comes from the HKLM\SOFTWARE registry file under the sub key:  
  • Microsoft\Windows NT\CurrentVersion  
For each registry value, the System Information tab displays the following information:  
  • Name of the registry value  
  • The contents of the registry value |

Recent Files Data
Possible data available in the System Information tab (Continued)

<table>
<thead>
<tr>
<th>Category</th>
<th>Sub-Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>NTUser</strong></td>
<td></td>
<td>Many applications store recently used files in the user's NTUSER.DAT registry file. The specific applications that are extracted are from Microsoft Office and Adobe Acrobat. The following sub keys are examined:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Software\Microsoft\Office</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Software\Adobe</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Software\Microsoft\Windows\CurrentVersion\Explorer\MapNetworkDrive MRU</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2 For each recently used file, the System Information tab displays the following information:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Application name (i.e. Acrobat, Excel, PowerPoint, Word)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Absolute path to the recent file</td>
</tr>
<tr>
<td><strong>LNK Files</strong></td>
<td></td>
<td>LNK is a file extension for a shortcut file used by Microsoft Windows to point to an executable file. LNK stands for LiNK. Shortcut files are used as a direct link to an executable file, instead of having to navigate to the executable, LNK files are stored in each users' AppData\Roaming\Microsoft\Windows\Recent or Recent directory. For each LNK file, the System Information tab displays the following information:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Absolute path to target file</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Date/Time the target file was created</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Date/Time the target file was last written to</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Date/Time the target file was last accessed</td>
</tr>
<tr>
<td><strong>Jump Lists</strong></td>
<td></td>
<td>Jump Lists, new in Windows 7, take you right to the documents, pictures, songs, or web sites you turn to each day. To open a Jump List, just right-click a program button on the Windows 7 taskbar. (You can also get to Jump Lists by clicking the arrow next to the program name on the Start menu.) The files that support this feature are located in each users' AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations folder. For each LNK file inside each Jump List, the System Information tab displays the following information:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Absolute path to target file</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Date/Time the target file was created</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Date/Time the target file was last written to</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Date/Time the target file was last accessed</td>
</tr>
</tbody>
</table>
### Possible data available in the System Information tab (Continued)

<table>
<thead>
<tr>
<th>Category</th>
<th>Sub-Category</th>
<th>Description</th>
</tr>
</thead>
</table>
| SAM Users     | Data         | The Security Accounts Manager (SAM) HKLM\SAM registry file stores users' passwords in a hashed format either as a LAN hash or NT hash. To protect the file, Microsoft introduced the SYSKEY function so the on-disk copy of the SAM is partially encrypted with a key (usually referred to as the "SYSKEY"). For each user stored in the SAM registry, the System Information tab displays the following information:  
  - Name of the user  
  - SID  
  - Unencrypted current LAN hash  
  - Unencrypted previous LAN hash  
  - Unencrypted current NT hash  
  - Unencrypted previous NT hash |
| Shell Bags    |              | Shell bags help track views, sizes and positions of a folder window when viewed through Windows Explorer; this includes network folders and removable devices. |
| Mobile Data   |              | The Artifacts guide found on the Exterro website lists all supported artifacts both computers and mobile devices.  
  **Mobile Data** artifacts shown in the System Summary pane can be found in the specified document. |
Possible data available in the System Information tab (Continued)

USB Devices

When USB devices are plugged into a computer for the first time, the Windows operating system installs an appropriate driver and stores information about the device in the registry and the setupapi log file. On subsequent device connections, various registry keys are updated to reflect the last connection time. Details about each USB device are stored in the following registry locations:

- HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\EMDMgmt
- HKLM\SYSTEM\CurrentControlSet\Enum\USBSTOR
- HKLM\SYSTEM\CurrentControlSet\Enum\USB
- HKLM\SYSTEM\CurrentControlSet\Control\DeviceClasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b}
- HKLM\SYSTEM\CurrentControlSet\Control\DeviceClasses\{53f56308-b6bf-11d0-94f2-00a0c91efb8b}
- HKLM\SYSTEM\MountedDevices
- HKU\<user sid>\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2

For each USB device, the System Information tab displays the following information:

- Vendor name
- Vendor id
- Product name
- Product id
- Instance id (very similar to serial number)
- Revision
- First time device was connected
- Last time device was connected
- Last time a user mounted the device
- Drives the device was mounted to
- Volume labels
Possible data available in the System Information tab (Continued)

EVTX .................................................................

Windows records logs during use. They are stored as EVTX files which are parsed by FTK to display useful information in System Summary.

- Remote Desktop Protocol
- Power Events
- Account Management Events
- Login/Logout Events
- Shared Objects Events
- Scheduled Task Events
- Audit Policy Change Events
- Windows Service Events
- PowerShell Events
- Wireless LAN Auditing Events
- Process Tracking
- USB Mass Storage Events
- Other Events
Chapter 33
Analyzing Document Content

Depending on your license, you can analyze the content of documents in your evidence in the following ways:

- Using Document Content Analysis (page 558)
- Performing Cluster Analysis (page 560)
- Using Entity Extraction (page 554)

Using Entity Extraction

*About Entity Extraction*

You can extract entity data from the content of files in your evidence and then view those entities. You can extract the following types of entity data:

- Credit Card Numbers
- Phone Numbers
- Social Security Numbers

The data that is extracted is from the body of documents, not the meta data. Using entity extraction is a two-step process:

1. Process the data with the Entity Extraction processing options enabled. You can select which types of data to extract.
2. View the extracted entities in the Examiner.

The following table provides details of the type of data that is identified and extracted:

**Entity Extraction Details**

<table>
<thead>
<tr>
<th>Type</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credit Card Numbers</td>
<td>Numbers in the following formats will be extracted as credit card numbers:</td>
</tr>
</tbody>
</table>
## Entity Extraction Details

<table>
<thead>
<tr>
<th>Type</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>16-digit numbers</strong></td>
<td>For example,</td>
</tr>
<tr>
<td>used by VISA, MasterCard, and Discover in the following formats.</td>
<td>1234-5678-9012-3456 (segmented by dashes)</td>
</tr>
<tr>
<td></td>
<td>1234 5678 9012 3456 (segmented by spaces)</td>
</tr>
<tr>
<td></td>
<td><strong>Not:</strong></td>
</tr>
<tr>
<td></td>
<td>1234567890123456 (no segments)</td>
</tr>
<tr>
<td></td>
<td>12345678-90123456 (other segments)</td>
</tr>
<tr>
<td><strong>15-digit numbers</strong></td>
<td>For example,</td>
</tr>
<tr>
<td>used by American Express in the following formats.</td>
<td>1234-5678-9012-345 (segmented by dashes)</td>
</tr>
<tr>
<td></td>
<td>1234 5678 9012 345 (segmented by spaces)</td>
</tr>
<tr>
<td></td>
<td><strong>Notes:</strong></td>
</tr>
<tr>
<td></td>
<td>Other formats, such as 14-digit Diners Club numbers, will not be extracted as credit card numbers</td>
</tr>
</tbody>
</table>

### Phone Numbers

Numbers in the following formats will be extracted as phone numbers:

<table>
<thead>
<tr>
<th>Format</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Standard 7-digit</strong></td>
<td>For example:</td>
</tr>
<tr>
<td></td>
<td>123-4567</td>
</tr>
<tr>
<td></td>
<td>123.4567</td>
</tr>
<tr>
<td></td>
<td>123 4567</td>
</tr>
<tr>
<td></td>
<td><strong>Not:</strong> 1234567 (not segmented)</td>
</tr>
<tr>
<td><strong>Standard 10-digit</strong></td>
<td>For example:</td>
</tr>
<tr>
<td></td>
<td>(123)456-7890</td>
</tr>
<tr>
<td></td>
<td>(123)456 7890</td>
</tr>
<tr>
<td></td>
<td>(123) 456-7809</td>
</tr>
<tr>
<td></td>
<td>(123) 456.7809</td>
</tr>
<tr>
<td></td>
<td>+1 (123) 456.7809</td>
</tr>
<tr>
<td></td>
<td>123 456 7809</td>
</tr>
<tr>
<td></td>
<td><strong>Not</strong> 1234567890 (not segmented)</td>
</tr>
</tbody>
</table>
|               | **Note:** A leading 1, for long-distance or 001 for international, is not included in the extraction, however, a +1 is.
**Entity Extraction Details**

<table>
<thead>
<tr>
<th>Type</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>International</td>
<td>Some international formats are extracted, for example,</td>
</tr>
<tr>
<td></td>
<td>• +12-34-567-8901</td>
</tr>
<tr>
<td></td>
<td>• +12 34 567 8901</td>
</tr>
<tr>
<td></td>
<td>• +12-34-5678-9012</td>
</tr>
<tr>
<td></td>
<td>• +12 34 5678 9012</td>
</tr>
<tr>
<td></td>
<td>Not 12345678901 (not segmented)</td>
</tr>
<tr>
<td></td>
<td>Other international formats are not extracted, for example,</td>
</tr>
<tr>
<td></td>
<td>• 123-45678</td>
</tr>
<tr>
<td></td>
<td>• (10) 69445464</td>
</tr>
<tr>
<td></td>
<td>• 07700 954 321</td>
</tr>
<tr>
<td></td>
<td>• (0295) 416,72,16</td>
</tr>
</tbody>
</table>

Notes:  
Be aware that you may get some false positives.  
For example, a credit number 5105-1051-051-5100 may also be extracted as the phone number 510-5100.

<table>
<thead>
<tr>
<th>Social Security Numbers</th>
<th>Numbers in the following formats will be extracted as Social Security Numbers:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• 123-45-6789 (segmented by dashes)</td>
</tr>
<tr>
<td></td>
<td>• 123 45 6789 (segmented by spaces)</td>
</tr>
</tbody>
</table>

The following will not be extracted as Social Security Numbers:  
• 123456789 (not segmented)  
• 12345-6789 (other segments)
Enabling Entity Extraction

To enable entity extracting processing options:

1. You can enable entity extracting processing options at one of two times:
   - When creating a case or adding new evidence and configuring processing options. See Evidence Processing Options on page 88.
   - When running Additional Analysis on existing evidence. See Using Additional Analysis on page 147.

Viewing Entity Extraction Data

To view extracted entity data

1. In the Examiner, click the Overview tab.
2. Expand the Document Content node.
3. Expand a Document Content type, such as Credit Card Numbers or Phone Numbers.
4. Click an item to show the file in the File List that contains the extracted data.

Using Document Content Analysis

You can use Document Content Analysis to group document data together for quicker review.

---

Note: If you activated Document Content Analysis as an Evidence Processing option when you created the project, Document Content Analysis will automatically run after processing data and will not need to be run manually.

---

To perform Document Content Analysis on a new case

1. From Case Manager, click Manage > Evidence Processing Profiles.
2. In the Manage Evidence Processing Profiles dialog, create a new profile or edit an existing profile. See Configuring Default Processing Options for a Case on page 80.

See Using Processing Profiles on page 81.
3. From the Detailed Options dialog, click the Evidence Processing tab from the left menu and select Document Content Analysis.
4. (Optional) Click DCA Options and change the Analysis Threshold, if needed, and click OK.
• **Analysis Threshold** — Sets the level of similarity (in a percentage) that is required for documents to be considered related or near duplicates. The higher the percentage, the more similar the documents need to be in order to be considered similar.

5. Click **Save As** and follow the screens to save and/or replace the profile.

**To perform Document Content Analysis on an existing case**

1. In **Evidence Explorer**, click **Evidence > Add/Remove**.
2. From the **Manage Evidence** dialog, highlight the evidence you want to process using Document Content Analysis.
3. Click **Refinement Options**.
4. Select **Document Content Analysis** and change the DCA options, if needed. See **Evidence Processing Options** on page 88.

**Filtering Documents by Document Content Analysis**

Documents processed with Document Content Analysis can be filtered by the content of the documents in the evidence. The Cluster Topic container is created in Evidence Explorer in the Overview > Case Overview tab and is created from data processed with Document Content Analysis. Data included in the Cluster Topic container is taken from documents, including Word documents, text documents, and PDF documents.

In order for the application to filter the data and display the Cluster Topic container, the following must occur:

- **Prerequisites for Cluster Topic** (page 559)
- **How Document Content Analysis Works** (page 559)
- **Filtering with Cluster Topic** (page 559)
- **Considerations of Cluster Topic** (page 559)
Prerequisites for Cluster Topic

Before the Cluster Topic container can be created, the data in the project must be processed by Document Content Analysis. The data is processed automatically when Document Content Analysis is selected in the Evidence Processing options or you can process the data manually by selecting Document Content Analysis in the Refinement Options > Evidence Processing dialog.

Evidence Processing Options (page 88)
Configuring Evidence Refinement (Advanced) Options (page 109)

How Document Content Analysis Works

The application uses an algorithm to cluster the data. The algorithm accomplishes this by creating an initial set of cluster centers called pivots. The pivots are created by sampling documents that are dissimilar in content. For example, a pivot may be created by sampling one document that may contain information about children’s books and sampling another document that may contain information about an oil drilling operation in the Arctic. Once this initial set of pivots is created, the algorithm examines the entire data set to locate documents that contain content that might match the pivot’s perimeters. The algorithm continues to create pivots and clusters documents around the pivots. As more data is added to the project and processed, the algorithm uses the additional data to create more clusters.

Word frequency or occurrence count is used by the algorithm to determine the importance of content within the data set. Noise words that are excluded from Document Content Analysis are also not included in the Cluster Topic pivots or clusters.

Filtering with Cluster Topic

Once data has been processed by Document Content Analysis and categories are created under the Cluster Topic container, you can view the data in the Overview > File List.

Using the Overview Tab (page 421) Cluster Topic Container (page 424)

The topics of the categories available are terms created during the Document Content Analysis. Documents containing these terms are included in the category and are displayed in the File List when selected. Categories are comprised of two word phrases that occur in the documents. This is to make the category more legible.

The UNCLUSTERED category contains any documents that are not included under a Cluster Topic Container.
Considerations of Cluster Topic

You need to aware the following considerations when examining the Cluster Topic categories:

• Not all data will be grouped into categories at once. The application creates categories in an incremental fashion in order to return results as quickly as possible. Since the application is continually creating categories, the Cluster Topic container is continually updated.

• Duplicate documents are grouped together as they match a specific category. However, if a category is particularly large, duplicate documents may not be included as part of any category. This is to avoid performance issues. You can examine any duplicate documents or any documents not included in a category by highlighting the UNCLUSTERED category of the Cluster Topic container.

• Cluster Topic results can vary when performed on different databases and/or different computers. This is due to the analytic behavior of the Document Content Analysis process. Since limits have been set on the algorithm to allow for efficient collection of data, large amounts of content can thus produce varying results.

Performing Cluster Analysis

Depending on the license you own (an AD Lab license or a AD Summation license), you can perform an analysis of files to determine related documents and email threads. If there are files that are similar, one document is identified as the pivot, and then the other related files are given a score that shows how closely they are related to the Pivot. If a score is 100, it is a perfect match.

Note: With an FTK, FTK PRO, or AD Enterprise license, you can perform Cluster Analysis on a documents only using the Document Content Analysis feature.

See Using Document Content Analysis on page 558.

You perform the Cluster Analysis by enabling the Cluster Analysis processing option. See Identifying Processing-Generated Data on page 452.

See Relating Generated Files to Original Files on page 452.

When you enable Cluster Analysis, you have the following options:

• Document Types to process - You can select to process the following file types:
  • Documents
  • Presentation
  • Spreadsheets
  • Email
• Similarity Threshold - Determines the level of similarity required for documents to be considered related or near duplicates.
After processing is complete, you can add the **Review Set Pivot** and the **Distance to Pivot** columns in the File List in the Examiner. You will also use the standard **Item #** column to identify the Pivot file.

See **Managing Columns** on page 613.

**To Perform Cluster Analysis**
1. When either adding evidence to a case or performing Additional Analysis, access the processing options.

See **Adding Evidence to a New Case** on page 114. See **Using Additional Analysis** on page 147.
2. Select the option for **Cluster Analysis**.
3. Click NDA Options.
4. Select the document types to process and the similarity threshold.
5. Process your data.

**To view Cluster Analysis data using columns**
1. In the examiner, view the file types that you selected.
2. Click the Column Settings icon.

See **Managing Columns** on page 613.
3. Either create a new column template or edit an existing one.
4. Add the following columns to the template.
   - **Item #**
   - **Review Set Pivot**
   - **Distance to Pivot**
5. Click **OK**.
6. Select the template name you just configured.
7. Click **Apply**.

This applies the template to the File List.
8. Click **Close**.

The Review Set Pivot shows the Item # of the Pivot file, or the file that other files are compared to. If a file was identified as being a near duplicate, it will show a Distance to Pivot score. A perfect match has a score of 100.
Words Excluded from Cluster Analysis Processing

Noise words, such as if and or, are excluded from Cluster Analysis processing. The following words are excluded in the processing:

a, able, about, across, after, ain’t, all, almost, also, am, among, an, and, any, are, aren’t, as, at, be, because, been, but, by, can, can’t, cannot, could, could’ve, couldn’t, dear, did, didn’t, do, does, doesn’t, don’t, either, else, ever, every, for, from, get, got, had, hadn’t, has, hasn’t, have, haven’t, he, her, hers, him, his, how, however, i, if, in, into, is, isn’t, it, it’s, its, just, least, let, like, likely, may, me, might, most, must, my, neither, no, nor, not, of, off, often, on, only, or, other, our, own, rather, said, say, says, she, should, shouldn’t, since, so, some, than, that, the, their, them, then, there, these, they, they’re, this, tis, to, too, twas, us, wants, was, wasn’t, we, we’re, we’ve, were, weren’t, what, when, where, which, while, who, whom, why, will, with, would, would’ve, wouldn’t, yet, you, you’d, you’ll, you’re, you’ve, your.
Using Visualization

About Visualization

Visualization is a component that provides a graphical interface to enhance understanding and analysis of files and emails in a case. You view data based on file and email dates. Visualization provides dashboards with chats and lists that quickly show information about the data in the specified date range. Visualization helps you identify files and emails that you label and bookmark as part of your investigation.

Note: The Visualization feature is available as an add-on license. Please contact your AccessData sales representative for more information.

Visualization can only display data that has an associated date. If a file or an email does not contain a valid Created, Modified, Last Accessed, Sent or Received date, it is not displayed. For example, carved files do not have an associated date so they are not displayed in Visualization.

You can also take screen captures of the Visualization pages to have a record of the data.

Visualization supports the following data types:

- **File Data:** You can view file data from either the *Explore* tab or the *Overview* tab in the *Examiner* interface.
- **Email Data:** You can view email data from the *Email* tab in the *Examiner* interface. For more information see Visualizing Email Data (page 576).
- **Internet Browser History:** You can view internet browser history data.

For more information see Visualizing Internet Browser History Data (page 588).

Visualization also has the following components:

- **Using Visualization Heatmap** (page 595)
- **Using Visualization Social Analyzer** (page 589)
- **Using Visualization Geolocation** (page 597)
Launching Visualization

To launch visualization

1. Use the Explore, Overview, or Email tabs to specify a set of data.

   For example, in the Overview tab, you can view everything under File Extension or drill down to just DOC files.

2. When you have specified the data that you want to view in the Visualization pane, click the following pie chart icon:

   ![Pie Chart Icon]

   File List

<table>
<thead>
<tr>
<th>Name</th>
<th>Label</th>
<th>Item #</th>
<th>Ext</th>
<th>Path</th>
<th>Category</th>
<th>P-Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>Form1.doc</td>
<td></td>
<td>3023</td>
<td>doc</td>
<td>pr...</td>
<td>Microsoft Word</td>
<td>60.00 KB</td>
</tr>
<tr>
<td>My Buddies.doc</td>
<td></td>
<td>3727</td>
<td>doc</td>
<td>pr...</td>
<td>Microsoft Word</td>
<td>20.50 KB</td>
</tr>
<tr>
<td>Options.doc</td>
<td></td>
<td>3:00</td>
<td>doc</td>
<td>pr...</td>
<td>Microsoft Word</td>
<td>19.00 KB</td>
</tr>
</tbody>
</table>

   The data that you have displayed in the File List pane is the data that you can send to the visualization module.

   The visualization module opens in a separate window from the Examiner that you can minimize, maximize, and select in the Windows task bar.

3. On the time line, specify the date range for the base time line that you want to view data for. See Setting the Base Time Line on page 567.

   Important: The dashboard and data list displays information only for the data that exists in the base time line. If specified dates have no files, the dashboard displays the text “No Data Series.”

To properly use Visualization, you must specify the base time line that you want to view data for.
About the Visualization page

The Visualization page includes three main components:

- **Time line pane** - Provides a time line pane with graphics representing the available data. This is the top part of the page.
- **Dashboard** - Provides graphical chart panes about the data. This is the middle part of the page.
- **Data list pane** - Provides a list of the data items. The is the lower part of the page. You can resize each pane.

![Visualization page screenshot](image-url)
You can use one of the following two time line views:

- **Basic** - The basic view lets you specify a base time line that you want to view data for. For example, you can select a specific year or month, or you can specify a custom date range. Any data that falls in that date range will be represented in the charts and data list.

See [About the Base Time Line](#) on page 565.

- **Detailed** - The detailed time line view shows a graphical representation of each file or email message. If you have a lot of data in a given date range, you can narrow your view to days, hours, minutes, and milliseconds.

See [About the Detailed Visualization Time Line](#) on page 582.

**About the Base Time Line**

The top portion of the visualization page is the time line. The time line displays a graph with a representation of that data that is visualized. The data is displayed from the oldest date on the left to the most current date on the right.

The span of the time line is automatically configured based on the dates of the data that you specified for visualization. For example, if the data that you specified has creation dates that range from 8/15/2003 to 9/11/2003, it will build a time line with those dates as the start and end.
The vertical gray bars represent where the data files are on the time line. The gold text in the lower left corner of the time line details the full timespan.

In the Basic time line view, you configure the base time line. The base time line is the specific range of dates that you want to work with. This may be a smaller date range than the full timespan (dates in yellow).

The base time line is represented by the blue selection box with sliding vertical bars. You can modify the base time line to be any range within the full timespan.

**Important:** The dashboard and data list displays information only for the data that exists in the base time line. If specified dates have no files, the dashboard displays the text “No Data Series.” To properly use visualization, you must specify the base time line that you want to view data for.

When you first launch visualization, a limited default base time line is specified, starting with the oldest data that is in the data set. For example, if you are viewing files, the default base time line is the first month starting with the creation date of the oldest file.
In the example in the graphic shown above, there are four files in the default base time line of one month and those four files are shown in the list and represented in the dashboard. In the email visualization, the time line is displayed in weeks, with vertical gray bars representing the emails.

**Time Line Selection Tools**

<table>
<thead>
<tr>
<th></th>
<th>Week 52</th>
<th>Week 1</th>
<th>Week 2</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Setting the Base Time Line

You adjust the range and the location of the base time line by adjusting the blue selection box. The information in the visualization dashboard and data list change when you adjust the selection box.

See [About the Base Time Line](#) on page 565.

**To adjust the full timespan**

1. Below the time line, you can zoom in on the view of the total timespan (yellow full timespan bar) by clicking and dragging the end of the bar.
2. You can also slide the yellow bar left or right to adjust the range.

**To adjust the base time line**

1. You change the base time line of the data set by adjusting the blue selection box.
2. You can do one of the following options:
   - Select a period that is on the top of the time line, for example, a specific month like June.
   - Drag the sliders of the blue selection box to make it bigger or smaller.
   - Drag the selection box to a different position.
   - Use the mouse scroll wheel to move the selection box left or right.
Changing the View of Visualization

You can change the way that visualization looks. You can modify the way that bar charts in visualization appear. You can also change the color scheme of the visualization windows.

Modifying the Bar Chart Displays

You can use the radio buttons below the time line to change the appearance of bar charts in visualization.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log (default)</td>
<td>The Log (logarithmic) view makes visualization adjust the bars or lines to</td>
</tr>
<tr>
<td></td>
<td>raise the low points and lower the highs so that both are easier to view</td>
</tr>
<tr>
<td></td>
<td>on a chart. This view smooths the peaks and valleys in the chart.</td>
</tr>
<tr>
<td>Linear</td>
<td>The Linear view returns the view from Log to an unadjusted representation</td>
</tr>
<tr>
<td></td>
<td>of the data. Changing from the Log view to the Linear view shows more of</td>
</tr>
<tr>
<td></td>
<td>the variance and spikes in the data.</td>
</tr>
<tr>
<td>Bars (default)</td>
<td>The Bars option makes Visualization show evenly-spaced bars to represent</td>
</tr>
<tr>
<td></td>
<td>the data.</td>
</tr>
<tr>
<td>Line</td>
<td>The Line view makes Visualization show the data as an unbroken line with</td>
</tr>
<tr>
<td></td>
<td>peaks and valleys, representing increases and decreases in the amount of</td>
</tr>
<tr>
<td></td>
<td>data over time.</td>
</tr>
</tbody>
</table>

Changing the Theme of Visualization

You can modify the appearance of the Visualization windows. You can choose from nine different color schemes.

To change the theme of Visualization

1. In the Case Manager, click **Tools > Preferences**.
2. In the Preferences dialog, under *Theme to use for Visualization*, choose from the following:
   - Office Blue (default)
   - Metro
   - Office Black
   - Office Silver
   - Vista
   - Windows 7
   - Summer
   - Expression Dark
   - Transparent
Visualizing File Data

The file data dashboard lets you view bar graphs, pie charts, and details about the files in the data set.

When visualizing files data, you can do the following:

- Configuring Visualization File Dates (page 569)
- Visualizing File Extension Distribution (page 570)
- Visualizing File Category Distribution (page 571)
- Using the File Data List (page 572)
Configuring Visualization File Dates
When you view file data in the Visualization page, you can view data based on the following file data:

- Created date
- Modified date
- Last accessed date

If a file contains a Created date but not a Modified date, and you change the pane to display the file by Modified date, the file is no longer displayed in the visualization pane.

If a file’s Created date, Modified date, or Last Accessed date is prior to the year 1985, visualization displays a dialog box. The dialog box asks you if you want to include the files with these dates in the visualization display. If you select the option to Do not ask me again, Visualization will remember your preference the next time the dates precede 1985.

Configuring the file date type
1. On the Visualization page, click the file date type drop-down menu.
2. By default, it displays the Created setting.
3. Select Created, Modified, or Last Accessed.

Visualizing File Extension Distribution
The extension distribution chart lets you view the data for the selected date range. You can view selected data by the following ways:

- File extension counts
- File sizes

File counts and sizes are rounded to two decimal places. You can select a bar in the extension distribution chart to further refine the data that is displayed in the file data list. You can select an extension in the legend to select or un-select extensions.
**File Extension Distribution Pane**

The category distribution chart displays a pie chart of the data set. It is organized according to the categories of the Overview tab and displays the percentages of each category in the data set. The percentages are displayed as the nearest whole number. For example: 10%. However, if a section in a category represents less than 1 whole number, then the percentage is displayed to the hundredth percent. For example, 56%.

**Visualizing File Category Distribution**

The category distribution chart displays a pie chart of the data set. It is organized according to the categories of the Overview tab and displays the percentages of each category in the data set. The percentages are displayed as the nearest whole number. For example: 10%. However, if a section in a category represents less than 1 whole number, then the percentage is displayed to the hundredth percent. For example, 56%.

**Visualization Category Distribution Chart**
If several categories are displayed very closely together, they may overlap and it can be difficult to read the percentages. You can click the **Show Connectors** option to expand the percentages further from the pie chart and include a connecting line to the pie section that correlates to the percentage.

You can select a category in the pie chart to further refine that data that is displayed in the file data list.

---

**Using the File Data List**

The file data list displays detail about the files in the data set. The pane is similar to the File List pane in the Examiner interface. The information that is displayed in the file data list is generated based on the data that you refine through the use of the time line pane, the file extension distribution chart, and the categories distribution chart.
Within the file data list you can sort, group, and sub-group, items according to columns including; ID, Name, Category, Date, and Size. To sort, drag and drop the desired column heading onto the blue bar. Any column heading that includes a filter icon can be used to sort the file list data set.

**Important:** If you want to filter for a specific date, include the day of and the day after. The filter uses midnight as the time frame. So if you only want files with a date of January 27, 2013, include January 27 and January 28. That will include files from midnight on the 27th to midnight on the 28th.
You can perform several actions on selecting the files and then clicking the **Mark Selected Items** button. You can do the following:

- Label the item
- Create a bookmark from the item
- Clear a check mark if you have checked it.
- Check the item.

You can use the Filter icon on any of the column headings to create custom filters in the file details list.

When you select the filter icon, a filter dialog is displayed that lets you select items that apply to the column where you add filtering expressions. There are many various ways in which you can filter to refine the data that is displayed.

**Note:** You can filter and sort by file sizes such as bytes, KB, and MB. However, note that when you enter an operator to filter by size, you must enter the size according to its byte value. You cannot enter the value in KB or MB. For example, instead of entering 100 KB, you must enter 102400 for the filter to work properly.
File Data List Filtering Tool

- Frobagg.1.rdf
- Frodbagg.1vite.rdf
- frodo boggins@207[2].txt
- frodo boggins@ads.monster[1].txt
- frodo boggins@ads.pointroll[2].txt
- frodo boggins@adserver.theonering[2].txt
- frodo boggins@advertising[1].txt
- frodo boggins@aim[1].txt
- frodo boggins@aimtoday.aol[1].txt
- frodo boggins@amazon[2].txt
- frodo boggins@aol[1].txt
- frodo boggins@nmsbbl[1].txt

Show rows with value that

Is equal to

And

Is equal to

Filter  Clear Filter
Visualizing Email Data

The email visualization dashboard consists of the following items:

- **Email Time Line**

  See *Narrowing the Scope with the Email Time Line* on page 576.

- **Mail Statistics Graph**

  See *Viewing Mail Statistics* on page 578.

- **Email Details List**

  See *Using the Email Details List* on page 578.

- **Social Analyzer Chart**

  See *Using Visualization Social Analyzer* on page 589.

*Narrowing the Scope with the Email Time Line*

The time line provides an aggregate view of email items sent and received in the data set. You can scale and refocus the scope of the time line to a specific data range. You can change the scope and scale of the data set by adjusting the gray slider tool. You can change the focus of the data set by adjusting the blue slider tool.
Using History Items in the Email Time Line

In the Email Visualization pane, when you alter the selection in the time line, a history item, also called a “breadcrumb,” is added to the top of the time line. Each history item is labeled according to the date range that you have selected in the time line. You can use these history items to move forward or backward through different views that you have created.
**Viewing Mail Statistics**

The mail statistics graph displays the sent and received mail statistics in a bar chart. The data contained within the date range, in the email time line, determines the data that is displayed in the mail statistics graph.

You can select a bar in the statistics graph to further refine the data that is displayed below in the Email details list.

**Visualization Mail Statistics Chart**

![Mail Statistics Chart](image)

**Using the Email Details List**

The email details list displays custodian-level sent and received statistics for email items. The list contains a column for the custodian's name, a column for the custodian's sent mail, and a column for the custodian's received mail.

You can sort group and subgroup the emails according to the columns including: Sender, Address, Traffic Count, Sent Mail, and Received Mail. To group the list of emails, you can drag and drop the column headers onto the table heading of the details list. The list sorts first by the first columns that you drop, and then in the order of any preceding columns that you drop into the table heading.
Visualization Email Details List

You can use the Filter icon on any of the column headings to create filters in the Email Details List.

When you select the Filter icon, a filter dialog is displayed that lets you select items that apply to the column and add filtering expressions.

Email Details List Filtering Tool
In visualization, Email addresses that are similar but not exactly the same are displayed as two different addresses, even though they may be the same address. For example, the quotation marks for 'John Doe' and "John Doe" are not the same. These slight changes in text can happen from different email servers/software during email transit, and the program cannot discern duplicate email addresses.

If an email item is sent to multiple recipients, it is counted as a single item in the email details pane. In the TrafficDetails chart, you can see when the same email was sent to multiple recipients. To view specific information about the recipients of that email item, you can click the **Traffic Details** button.

You can check specific emails in the examiner from the email details list by selecting the emails and then choosing one of the Check Selected Items options, Sent, Received, or Both.

When you expand a specific email item, you can run additional functionality. This functionality includes the SocialAnalyzer chart. The buttons to open the Social Analyzer chart are located on the right side of a custodian’s email item in the list.

For more information see the following:
**Using Visualization Social Analyzer** (page 589)
Analyzing Email Domains in Visualization

Once you have opened the Social Analyzer pane, you can isolate and examine individual email domains.

**Note:** Social Analyzer is very graphics-intensive. In order to avoid server issues, you should cull the data with facets and other filters to isolate the information that you want to examine before viewing it in Social Analyzer.

**To analyze email domains in Visualization mode**

1. Open Social Analyzer.
2. Click the domain bubbles to select the domain(s) that you want to view.
3. (optional) If you want to view the top ten domains in terms of received emails. click 🌞. Each time you click this icon, the next top ten bubbles will be selected, and so forth.
4. (optional) You can zoom in and zoom out of the Social Analyzer panel. If you hover over a domain bubble, the full display name and address, as well as the count, is displayed in the tool tip.
5. You can expand selected email domains and examine individual emails in a domain. See Analyzing Individual Emails in Visualization on page 580.

Analyzing Individual Emails in Visualization

You can expand email domains to display individual emails and the traffic between those emails.

**To analyze individual emails within selected email domains**

1. Open Social Analyzer.
2. Click the domain bubbles to select the domain(s) that you want to view.
3. (optional) If you want to view the top ten domains in terms of received emails. click 🌞. Each time you click this icon, the next top ten bubbles will be selected, and so forth.
4. (optional) You can zoom in and zoom out of the Social Analyzer panel. If you hover over a domain bubble, the full Display Name and address, as well as the count, will be displayed in the tool tip.
5. Click ⬇️ to expand the domain names to display the individual emails.
Posting Email Results Back to the Examiner

After you have identified emails that are relevant to your investigation, you can post them back to the Examiner for further review. For example, you may drill down to an certain individual that had sent 25 emails to various domains. You can do the following:

- Add the 25 emails to a Label
- Add the 25 emails to a Bookmark
- Check the 25 emails in the File List
- Clear all other checked emails in the File List and check only these 25 emails.

To post email results
1. In the Social Analyzer, identify emails that you want to post.
2. Click Post Results Back.
3. Select the desired option.

About the Detailed Visualization Time Line

You can use the Detailed view of the visualization time line to get a more granular view of the files and emails in your data set. This helps you use the time line to identify the files and emails that are important in your investigation. The detailed view provides the following time bands that you can turn on or off to get a more or less granular view of the files:

- Years
- Months
- Days
- Hours
- Minutes
- Seconds
- Milliseconds

Different file types are represented by different colors to assist in identifying relevant files.
Using the Detailed Visualization Time Line

You can use the Detailed view of the time line to get a more granular view of the files and emails in your specified time line. You can change the Time Line View option to switch between the Basic view and the Detailed view.

**Important:** Before you launch the Detailed time line view, you must specify a base time line in the basic view that includes the data that you want to look at. Otherwise, you will only be able to see the files that are in the default base time line.

See [About the Base Time Line](#) on page 565.

**To use the detailed visualization time line**

1. Select a data set that you want to view.
2. Launch the visualization panel.

See [Launching Visualization](#) on page 563.

3. Specify the base time line for the data that you want to view. See [Setting the Base Time Line](#) on page 567.
4. For the Time Line View, click **Detailed**.

**Understanding How Data is Represented in the Detailed Time Line**

In the detailed view, each file, or group of files, is represented with a flag with a circle. Each flag displays the file’s name, item number, category, size, and date. If you click a flag, the item it represents is selected in the file list pane at the bottom of the visualization interface.

The color of each flag and circle represents the type of data. For example, the color blue represents Graphics files. To the right of the time line, there is a Legend that displays what each color represents.

The span of the files depends on the base time line that you selected previously in the basic view. See [Setting the Base Time Line](#) on page 567.
About Time Bands

If several items fall within a particular time frame, it can be difficult to see all of them. This is because their flags can overlap in the limited amount of interface space that is available.

You can manipulate the time line by giving the time line a greater or less granular view by using different time bands. You can use one or more of the following time bands to change your view:

- Years
- Months
- Days
- Hours
- Minutes
- Seconds
- Milliseconds

When you first open visualization, it will determine which time bands to enable based on the date range of the base time line.

You can choose to display or hide a time band. The bands are displayed at the bottom of the time line. The more time bands that you turn on, the more granular the data becomes.
For example, suppose you turn on the Year, Month, and Day time bands.

The Year time band is on the bottom, with the Month time band above that, and the Days time band (1-31) is above that. There are green dots in the bands. The green dots represent files or groups of files. Also in the example, there is a box in the center of the bands. That box is the view window. The view window is always in the center of the time line. You will only see the files that are in the view window. You can slide the time line to the left and right to place files into the view window.

If there are large clusters of files, you can turn on more time bands to get a more granular view of the files.
Modifying the Time Line Using Time Bands and Zoom
You can select different time bands to get a greater or less granular view of your data.

To change the time bands of the detailed time line
1. To display or hide a time band, in the top left corner, click a band to toggle it on or off. When a band is on, it is shadowed with a dark box.

Be aware that when you change time bands, the focus box of that time band will be centered in the timeline, and there may not be any files in the focus area. You will need to slide the time line to put the greendots back into the focus area.

2. Slide the time line to place the data in the view window. You can do one of the following options:
   - Click the right or left arrows in the upper-right corner.
   - Click the time line and drag it left or right.
   - Use the mouse scroll wheel to move it left or right.

3. You can also use the Zoom In and Zoom Out buttons (top-right corner) to modify the view.

The zoom feature does not change the time bands or the selected date range. It simply displays more or less of the data.

Understanding How Grouping Works in the Detailed Visualization TimeLine
If there are more than 500 items that all within a particular time period, the items are grouped together under a single grouped flag that represents all of the items. Grouping helps you to still use the detailed time line without having to view an overwhelming amount of data flags in a small amount of space.

You can have the data grouped by the following two methods:
   - Selected Time - (Default) Items are grouped by a specific time period, for example Days. For example, you could have 25 items on the 5th, 200 items on the 6th, and 1100 items on the 7th. There would be a single group for each day.
   - Fixed Number - Items are grouped into by a maximum group size of 500. Using the previous example, if there were 1325 total items, they would displayed in three groups of 441 files.

The group flag includes a Details button. Click the Details button to display a list of all of the items that are grouped under that flag.

You can also click a group to get a more granular view of the files in the group. When you click a group additional time bands are enabled to give you a more detailed view.
Be aware that multiple flags may be staked vertically. You may need to make the time line pane taller by dragging the bottom border of the pane down.

Example of grouping
You can view internet browser history files in the detailed visualization timeline. You can view browser history from the following browsers:

- Internet Explorer
- Firefox
- Chrome
- Safari
- Opera

In order to view internet browsing history files in the detailed visualization timeline, you must first process the browser history files. By default, the option to process browser history files is disabled. You must enable the Process Internet Browser History for Visualization option in either the processing options or additional analysis options.

See Evidence Processing Options on page 88. See Using Additional Analysis on page 147.

To view internet browser history files in the detailed visualization timeline

1. If you have browser history files, in the File List Overview tab, browse to File Category > Internet Chat Files > browser name > History.

2. Right-click one or more browser history files and select Visualize Browser History...

View browser history files from only one manufacturer at a time.

If the Visualize Browser History... option is grayed-out, then either the file has not been processed with the Process Internet Browser History for Visualization option enabled, or the file type is not supported.

If it is a supported file, the detailed visualization timeline is opened.

You may need to adjust the blue selection box to include the data that you want to see.

For information on viewing the visualization timeline, see About the Visualization page (page 564).

Visualizing Other Data

You can process specific file types so that they can be viewed in the visualization timeline.

- EVTX files - See Viewing Data in Windows XML Event Log (EVTX) Files (page 453)
- IIS Log files - See Viewing IIS Log File Data (page 455)
- Registry data files - See Viewing Registry Timeline Data (page 457)
- CSV files that are in the Log2Timeline format - See Log2timeline CSV fields (page 461)
Using Visualization Social Analyzer

About Social Analyzer

The Social Analyzer shows a visual representation of email volume contained in the data set. Social Analyzer will display all of the email domains in a project, as well as individual email addresses within the email domains.

Social Analyzer Map

The Social Analyzer map displays emails in the data set group by domain name. These domain names appear on the map in circles called “bubbles.” The larger the bubble, the more emails are contained within that domain. The bubbles in the map are arranged in a larger sphere according to how many emails were sent to that domain. The center bubble in the sphere will have the most emails sent from this domain, while domains radiating clockwise from the center will have fewer and fewer emails in their domain bubble. If you want to examine email domains with the most sent emails, concentrate on examining the bubbles in the center of the map.

Email data in the Social Analyzer map can be examined on two different levels. On the first level, you can get an overall view of communications between domains. You can then select domains that you want to examine in a
more detailed view and expand those domains to view communications between specific email addresses from the domain. For example, if you search for high email traffic between two domains, you can see which two domains have the highest amount of traffic between them. Select the two domains, and expand them to view the email traffic between individual users from those two selected domains.

See Analyzing Email Domains in Visualization on page 593. See Analyzing Individual Emails in Visualization on page 593.

Elements of the Social Analyzer Map

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Map" /></td>
<td>This map presents the overall view of the social analyzer data. The orange rectangle indicates the area displayed in the main social analyzer map. Black dots in the overall view show domains that are either selected or communicating. You can either expand or collapse the overall view by clicking on the triangle in the upper right corner.</td>
</tr>
<tr>
<td><img src="image" alt="Domain" /></td>
<td>When you select a domain bubble, it is surrounded by a colored double ring. The ring may be colored blue, black, purple, or red. The different colors allow you to distinguish between different selected domains, but they do not have any significant meaning.</td>
</tr>
<tr>
<td><img src="image" alt="Connection" /></td>
<td>Domain bubbles that are not selected, but have sent emails to the selected domain bubble, are surrounded by a single colored ring that is the same color as the selected domain bubble. This allows you to easily tell which domains have been communicating with the selected domain bubble. Domain bubbles that do not connect to any selected domains are greyed out.</td>
</tr>
<tr>
<td><img src="image" alt="Reverse" /></td>
<td>Lines connect other domain bubbles to the selected domain bubble. These lines represent emails sent to the selected domain from other domains. The more emails that have been sent to the domain, the thicker the line between domain bubbles are. You can also see emails sent from the selected domain. Select Show Reversed Connections in the Social Analyzer panel to show visual representations of emails sent from the selected domain.</td>
</tr>
<tr>
<td><img src="image" alt="Orange" /></td>
<td>A domain bubble with an orange ring indicates that a domain has been connected to from another domain multiple times. This allows you to pinpoint domains that have heavy communication between them.</td>
</tr>
</tbody>
</table>
**Accessing Social Analyzer**

To navigate throughout the **Social Analyzer** pane, click and drag inside the pane. Hover over an email domain bubble to view the total number of emails that were sent from the domain.

**Note:** Expansion of large datasets may result in slow server speeds and slow rendering the Social Analyzer visualization data.

**To access Social Analyzer**

1. Click Project Review.
2. In the *Item List* panel, click Options > Visualization > Social Analyzer.

**Social Analyzer Options Panel**

![Social Analyzer Options Panel](image)
**Social Analyzer Options**

The following table identifies the tasks that you can perform from the **Social Analyzer** panel.

### Social Analyzer Options

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Apply Visualization" /></td>
<td>Applies the visualization graph filters to the <em>Item List</em> grid. Once applied, only those items filtered with visualization will appear in the <em>Item List</em> grid.</td>
</tr>
<tr>
<td><img src="image" alt="Cancel Visualization" /></td>
<td>Cancels the visualization graph filters and exits out of Visualization.</td>
</tr>
<tr>
<td><img src="image" alt="Refresh" /></td>
<td>Refreshes the <strong>Social Analyzer</strong> pane.</td>
</tr>
<tr>
<td><img src="image" alt="Clear Selections" /></td>
<td>Clears the selected bubbles in the <strong>Social Analyzer</strong> pane.</td>
</tr>
<tr>
<td><img src="image" alt="Select Most Connected Items" /></td>
<td>Selects the ten bubbles that have been most connected to in the <strong>Social Analyzer</strong> pane. Each time you click this icon, the next top ten bubbles will be selected, and so forth.</td>
</tr>
<tr>
<td><img src="image" alt="Expand Selected Domains" /></td>
<td>Expands selected domains in the <strong>Social Analyzer</strong> pane. You can drill down to a second level to examine the email data. See Analyzing Individual Emails in Visualization on page 593.</td>
</tr>
<tr>
<td><img src="image" alt="Zoom In" /></td>
<td>Zooms into the <strong>Social Analyzer</strong> pane. If you are unable to view the social analyzer data, click <strong>Zoom In</strong> to locate the data. You can also zoom in by expanding the slider bar located at the bottom of the <strong>Social Analyzer</strong> pane, by using the + key on the keyboard, or by scrolling the mouse wheel up.</td>
</tr>
<tr>
<td><img src="image" alt="Zoom Out" /></td>
<td>Zooms out of the <strong>Social Analyzer</strong> pane. You can also zoom out by expanding the slider bar located at the bottom of the <strong>Social Analyzer</strong> pane, by using the - key on the keyboard, or by scrolling the mouse wheel down.</td>
</tr>
<tr>
<td><img src="image" alt="Expands and Collapses" /></td>
<td>Expands and collapses the overall map of the data set. Dots that appear in black in the overall map are domains/emails that are connected to the selected domain/email. The orange rectangle on the map shows where the expanded location is on the map.</td>
</tr>
</tbody>
</table>
## Social Analyzer Options

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
</table>
| **View** | - Show Reversed Connections - Select to show all reversed connections in the pane. Reversed connections are emails sent from a particular email or email domain.  
- Show Connections - Select to show the connections between domains in the pane. Connections are emails sent to a particular email or email domain.  
- Preview Connections on Hover - Select to view connections between domains when you hover over them. This option is not selected by default to speed rendering of the map.  
- Email Display - Display email domains either by the display name or address.  
- Bubble Limit - You can choose a display limit of either 2,500, 5,000, or 10,000 domains. Server issues may occur with larger display limits. |
| **Stats** | Displays the statistics of either the first or second level of the email domain data. You can view:  
- The total number of domains, emails, and bubbles in the pane.  
- The total number of selected domains, emails, and bubbles in the pane.  
- The total number of domains, emails, and bubbles that have been expanded.  
You can access the second level of data by clicking **Expand Selected Data**. |
Analyzing Email Domains in Visualization

Once you have opened the Social Analyzer pane, you can isolate and examine individual email domains.

**Note:** Social Analyzer is very graphics-intensive. In order to avoid server issues, you should cull the data with facets and other filters to isolate the information that you want to examine before viewing it in Social Analyzer.

To analyze email domains in Visualization mode

1. Click Project Review.
2. In the *Item List* panel, click Options > Visualization > Social Analyzer.
3. Click the domain bubbles to select the domain(s) that you want to view.
4. (optional) If you want to view the top ten domains in terms of received emails. click . Each time you click this icon, the next top ten bubbles will be selected, and so forth.
5. (optional) You can zoom in and zoom out of the Social Analyzer panel. If you hover over a domain bubble, the full display name and address, as well as the count, is displayed in the tool tip.
6. You can expand selected email domains and examine individual emails in a domain. See Analyzing Individual Emails in Visualization on page 593.

Analyzing Individual Emails in Visualization

You can expand email domains to display individual emails and the traffic between those emails.

To analyze individual emails within selected email domains

1. Click Project Review.
2. In the *Item List* panel, select Options > Visualization > Social Analyzer.
3. Click the domain bubbles to select the domain(s) that you want to view.
4. (optional) If you want to view the top ten domains in terms of received emails. click . Each time you click this icon, the next top ten bubbles will be selected, and so forth.
5. (optional) You can zoom in and zoom out of the Social Analyzer panel. If you hover over a domain bubble, the full Display Name and address, as well as the count, will be displayed in the tool tip.
6. Click to expand the domain names to display the individual emails.
Chapter 36

Using Visualization Heatmap

Heatmap allows you to view a visual representation of file categories and file volume within a project. Information displays in a grid comprised of squares of different colors and sizes. Each color represents a different file category, and the relative size of the square represents the file volume within the category. You can view each file category for more details about the files within that category (similar to a file tree) and navigate between file categories.

You can also switch between viewing the file volume by the physical size of each file and the file count. This allows you to see any discrepancies in the size of the files. For example, if someone were trying to hide a file by renaming the file extension, you could easily see the size discrepancy in the heatmap, and then investigate that particular file further.

To access Heatmap

1. In Forensics products, do the following:
   1a. Open the Examiner.
   1b. In the File List panel, click (Heatmap).

2. In other products, do the following:
   2a. Click Project Review.
   2b. In the Item List panel, click Options > Visualization > (Heatmap).

Heatmap Panel
Heatmap Options Panel
The following table defines the tasks from the Heatmap panel.

Heatmap Panel Options

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>Cancels the heatmap filters and exits out of Visualization.</td>
</tr>
<tr>
<td>✓</td>
<td>Apply the visualization graph filters to the Item List grid. Once applied, only those items filtered with visualization appear in the Item List grid.</td>
</tr>
</tbody>
</table>

Options

Category
- Files - Allows you to view files by the file category. You can view the files in each category:
  - By double-clicking that particular file category's square, or
  - By clicking the menu from the upper left side and choosing the file category that you want to view in the heatmap.
- Folders - Allows you to view files by the folders contained within the project. You can view the files in each folder:
  - By double-clicking that particular folder's square.
  - By clicking the menu from the upper left side and choosing the folder that you want to view in the heatmap.
- Extensions - Allows you to view files by the file extension.

Metric
- By Size - Allows you to view file types by size of the files. The larger the files, the larger the represented square in the heatmap.
- By Count - Allows you to view file types by quantity. The more files of a particular type that are in the project, the larger the represented square in the heatmap.
Chapter 37
Using Visualization Geolocation

About Geolocation Visualization
Geolocation allows you to view a map with real-world geographic location of evidence items that have geolocation information associated with them. This lets you understand where certain activities/actions took place.

See Using Visualization on page 145. Geolocation supports the following data types:
- Photos with GPS information in the EXIF data. If you have photos in the evidence that have GPS data in the EXIF data, you can see where those photos were taken.
- IP location data after gathering Volatile data (Enterprise license only). When using Forensic products and processing volatile/RAM data, you can see the lines of communication (both sent and received) between addresses, showing the location of all parties involved.

Using Geolocation Visualization with Forensics Products to View Security Data (page 605)

Note: When using Forensic products, Geolocation IP address data may take up to eight minutes to generate, depending upon other jobs currently running in the application.

About Viewing Geolocation Data
When viewing Geolocation data, you can use the following components in Review:
- Maps

When viewing geolocation data, you can use any of the following maps:
- OpenStreetMaps
- Offline Maps (See General Geolocation System Requirements (page 598) and Using Offline Maps (page 598))
- Geolocation Grid

Below the map, you can view a grid that shows details about the items in the map. See Using the Geolocation Grid on page 603.
- Geolocation Data in columns in the Item List

You can view geolocation data for files in the Item List.
See Using Geolocation Columns in the Item List on page 604. You can cull the data using filters and other tools in the item list to limit the data that is displayed in Geolocation.

General Geolocation System Requirements
As a minimum prerequisite, you must have the following:
- Internet access to view web-based maps.

By default, online maps are used to display map data for the Geolocation view. If you do not have internet access, you can download and use offline maps. See Using Offline Maps on page 598.

Using Offline Maps
If you do not have internet access, you will not have access to the default online maps. You can download and use offline maps for Geolocation. You can use the offline maps with either FTK, Lab, or Enterprise.
For more information, see:

Processing Geolocation Data
- For Forensic products (FTK, FTK Pro, Lab, and Enterprise)
  - The File Signature Analysis option must be selected when processing the evidence.
  - The geolocation data is automatically processed, there is not processing option to select.
- For , when you create a project, on the Processing Options tab, under Miscellaneous Options, you must select the Geolocation option.

See “Evidence Processing and Deduplication Options” in the Admin Guide.

Viewing Geolocation EXIF Data
When your evidence has photos with GPS information in the EXIF data, you can view photo locations.

To view EXIF data in Forensic products (FTK, FTK Pro, Lab, and Enterprise):
1. In FTK, open the Examiner.
2. In the *File List* panel, click ![Geolocation](Geolocation).

3. You can filter the items displayed and see item details. See *Using the Geolocation Grid* on page 603.
To view EXIF data in
1. Click Project Review.
2. In the Item List panel, click Options > Visualization > Geolocation.
3. You can filter the items displayed and see item details. See Using the Geolocation Grid on page 603.

Geolocation Panel - EXIF data
Using Geolocation Tools

The Geolocation Map Panel

Points of data in a particular area on the map are represented by large dots called clusters. The number on each cluster show how many points of data (known as pins) are represented by the cluster. Clicking a particular cluster on the map zooms in on a group of pins.

The general location of the clusters are determined by a central point on the map. The clusters radiate from this central point. When you zoom in and out of the map, your central point on the map moves as well, and clusters will shift position on the map. However, as you zoom into a cluster, the cluster rendered will more closely align itself with the location of the individual pins.

When viewing IP data, the connections between two pins display on the map as lines between clusters/pins. The width of the lines represent the amount of traffic between two IP address. The thicker the lines, the more traffic has occurred. Green lines represent traffic originating from the pin and red lines represent traffic entering the pin.

When you select a cluster and zoom in on a particular pin, you can select one or more pins. When a pin is selected, the outline and shadow of the selected pin turns orange. If you zoom out of the map, the cluster with one or more selected pins has an orange ring.

Hovering over the cluster displays the following icons:

- Selects all of the pins in a cluster.
- Clears all of the selected pins in a cluster.

The following table describes the Geolocation panel options.

<table>
<thead>
<tr>
<th>Geolocation Panel</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Checkmark]</td>
<td>After filtering data by selecting one or more pins, this applies the selected geolocations to the Item List grid. Once applied, only those geolocations filtered with visualization appear in the Item List grid. For network data, you will see any communication from those pins to any other location. This may include one or more items. If you enter the Geolocation view again, only those geolocation will be displayed in the map. To reset the items in the Item List, click the Project Explorer's Reset and Apply icons.</td>
</tr>
<tr>
<td>![X]</td>
<td>Cancels any new geolocation filters and exits out of Visualization. If you previously saved a filter, this will not clear the filter. You must clear filters in the Item List.</td>
</tr>
<tr>
<td>Pins displayed</td>
<td>Shows the number of pins that are displayed and the number selected.</td>
</tr>
<tr>
<td>Clear</td>
<td>Clears and selected pins.</td>
</tr>
<tr>
<td>Element</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Displays the number of pins selected in the map versus the number of pins available in the data.</td>
<td>Expands or collapses the overall view map.</td>
</tr>
<tr>
<td>Displays the latitude and longitude where the mouse pointer resides. To view the position of a particular pin, hover the mouse over the pin. To view the exact coordinates of the pin, select the pin and right-click.</td>
<td>Turns the connections between the pins/clusters either on or off.</td>
</tr>
<tr>
<td>Displays all of the pins on the map.</td>
<td>Zooms in or out on the map. A slide bar displays, allowing you to control the zoom feature.</td>
</tr>
<tr>
<td>View All/View Selected</td>
<td>Displays either EXIF data or network connection data. You can also view both types of data at the same time.</td>
</tr>
<tr>
<td>Right-clicking a pin displays more information about the pin.</td>
<td>Filter</td>
</tr>
</tbody>
</table>

**Detail of Pin**

![Image of a map with a pin and detailed information dialog box]

- **Broad Street**
- **Coordinate:** 40.706666666, -74.010666666
- **Status:**
- **Details:**
- **Color:** [Color choices]
- **Icon:** [Icon choices]
In the pin dialog, you can:

- Add any notes
- View the exact coordinates and status of the pin
- View the IP Address of the pin

**Note:** To save processing time and to ensure data accuracy, the host name does not populate in the Geolocation pin. However, the host name does populate in the Item List.

- Change the color and shape of the pin

If you make any changes to the pin, a warning icon displays that notifies you that changes were made to the pin and need to be saved. You can do the following in the pin dialog:

- Click to save the changes that you have made to the pin
- Click to reset the pin. If changes have been saved previously to the pin, this action resets the pin to the saved version

- Click to close the dialog
Using the Geolocation Grid

When you open Geolocation, you can view a grid that shows details of the items on the map. The Geolocation Grid shows the following:

- **Exif:** This shows the following Exif data from photos
  - Capture Data column
  - File Name column
  - File Size Coordinate column

When you click an item in the grid, the map will be centered to reflect the location of the selected item. You can minimize the grid so that the whole map is visible.

**Filtering Items in the Geolocation Grid**

When you first launch Geolocation, all of the items on the map are shown in the grid. You can filter the contents of the grid in the following ways.

- In the map, if you select a pin, only that item is displayed. You can click (and select) multiple pins.
- In the map, if you right-click a cluster and click [ ], that selects all of the pins in a cluster. This will filter the grid to those clustered pins. You can add multiple clusters to the grid.
- In the grid, the columns in the Geolocation Grid can be filtered to cull the items in the grid. For Network Communication data, the data in the bar chart is filtered as well when columns are filtered.
The data that the Geolocation filter uses to render the information is also available in columns in the Item List. You can find the following columns in the Item List, depending upon the data that has been collected. These columns can be sorted and filtered. See General Geolocation System Requirements on page 598.

Geolocation EXIF Data Columns
When your evidence has photos with GPS information in the EXIF data, you can view data using the following columns.

Geolocation Columns: EXIF data

<table>
<thead>
<tr>
<th>Column</th>
<th>Display name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Geotagged Area Code:</td>
<td>Area Code</td>
<td>Area code location of geotagged photo or object.</td>
</tr>
<tr>
<td>Geotagged City:</td>
<td>City</td>
<td>City location of geotagged photo or object.</td>
</tr>
<tr>
<td>Geotagged Country Code:</td>
<td>Country Code:</td>
<td>ISO country code location of geotagged photo or object, such as USA, FRA, MEX, HKG, and EST.</td>
</tr>
<tr>
<td>Geotagged Direction:</td>
<td>Direction</td>
<td>Direction geotagged photo or object.</td>
</tr>
<tr>
<td>Geotagged Latitude:</td>
<td>Latitude</td>
<td>Latitude of geotagged photo or object.</td>
</tr>
<tr>
<td>Geotagged Longitude:</td>
<td>Longitude</td>
<td>Longitude of geotagged photo or object.</td>
</tr>
<tr>
<td>Geotagged Postal Code:</td>
<td>Postal Code</td>
<td>Postal code of geotagged photo or object.</td>
</tr>
<tr>
<td>Geotagged Region:</td>
<td>Region</td>
<td>Regional or State location of geotagged photo or object, such as NY, DC, IL, FL, and UT.</td>
</tr>
<tr>
<td>Geotagged Source:</td>
<td>Source</td>
<td>Source used to resolve geotagged GPS location to locality information.</td>
</tr>
</tbody>
</table>

**Note:** The following columns are not used with exif data: GeoTagAreaCode, MetroCode, or Postal Code.
Using Geolocation Column Templates

When using AD Forensics products, you can use the following Column Templates to help you quickly display Geolocation-based columns in the File List:

- **Geolocation** - Displays all available Geolocation columns.
- **GeoEXIF** - Displays all columns that contain EXIF-related Geolocation data.
- **GeoIP** - Displays all columns that contain IP-related Geolocation data.

View Security Data

**Note:** This feature is only available with AD forensics products combined with a Memory Analysis license,

After gathering Volatile data, you can use geolocation to view IP location data to discover where in the world a computer is communicating. You can view IP locations data when using the following products:

The Geolocation view will display lines that trace internet traffic sent and received between IP addresses, indicating the physical location of all parties involved. You can drill into geographic regions to see multiple evidence items. You can then select specific data to post back to the case, where they can view information in the examiner or include it in reports.

**Note:** For data collected by Geolocation Visualization, the *To Domain Name*, *To ISP*, *To Netspeed*, and *To Organization* columns do not populate in the Item Grid. If you require this data, you need to purchase a MaxMind Premier database license.

**Geolocation Panel - IP Locations To view IP data in Geolocation viewer**
Prerequisites for Using Geolocation Visualization to View Security Data

- For examining network acquisition and volatile data, enable the Geolocation option in the Web Config file. To enable this option, contact AccessData’s support.
- Also for examining network acquisition and volatile data, you need to generate a text file of your IP locations and place the text file in the GeoData directory. For more information, contact AccessData’s support.

Configuring the Geolocation Location Configuration File

When using AD Forensics products, and when working with network acquisition and volatile data, some data may come from a private network where the physical location of the IP address is not known. For example, you may need to provide the location of your own network and any satellite offices that you interact with. Normally you would start with block of IPs in your local network.

To set this information, you need to populate a configuration file for the KFF server. The filename is iplocations.txt.

Geolocation Configuration Page Options

The table below lists the various Geolocation Configuration Page options.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ip Address</td>
<td>The IP address. The IP addresses must be written in CIDR format and need to be IPv4 addresses.</td>
</tr>
<tr>
<td>ID</td>
<td></td>
</tr>
<tr>
<td>Country Code</td>
<td>The two letter country code for a country, such as HK for Hong Kong or US for the United States.</td>
</tr>
<tr>
<td>Country Code 3</td>
<td>The three letter country code for a country, such as RUS for Russia or DEU for Germany.</td>
</tr>
<tr>
<td>Country</td>
<td>The full country name, such as United States or Argentina.</td>
</tr>
<tr>
<td>Region</td>
<td>The state or province of the geolocation data, such as NY for New York or ON for Ontario.</td>
</tr>
<tr>
<td>City</td>
<td>The city of the geolocation data, such as Beijing or San Francisco.</td>
</tr>
<tr>
<td>Postal Code</td>
<td>The postal code or zip code of the geolocation data.</td>
</tr>
<tr>
<td>Latitude</td>
<td>The latitude of the geolocation data.</td>
</tr>
<tr>
<td>Longitude</td>
<td>The longitude of the geolocation data.</td>
</tr>
</tbody>
</table>
Using Visualization Geolocation

<table>
<thead>
<tr>
<th>Metro Code</th>
<th>The metro code of the geolocation data.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Area Code</td>
<td>The area code of the geolocation data.</td>
</tr>
<tr>
<td>Continent Code</td>
<td>The continent code of the geolocation data. For example, NA for North America and AS for Asia.</td>
</tr>
<tr>
<td>Source</td>
<td>The source of the geolocation information. This field is optional.</td>
</tr>
</tbody>
</table>

Configuring the Location Configuration File Manually

You can manually create and edit the iplocations.txt text file for the KFF server. It has the following requirements:

- The text file needs to be saved with the filename iplocations.txt.
- The IP addresses must be written in CIDR format and need to be IPv4 addresses.
- Each comment line in the file must start with the character #. List only one address/network per line.
- The network line must contain the following information in the following order: address (in CIDR format), Id, CountryCode, CountryCode3, CountryName, Region, City, PostalCode, Latitude, Longitude, MetroCode, AreaCode, ContinentCode, Source.
- The iplocations.txt file must be placed in the Geodata folder of the kffdata folder on the server.

The following is an example of an iplocations.txt file:

```plaintext
#this file goes in the <kffdata>\GeoData directory
#address (in cidr form),Id,CountryCode,CountryCode3,CountryName,Region,City,PostalCode,Latitude,Longitude,MetroCode,AreaCode,ContinentCode,Source
#192.168.0.0/24,1,,USA,United States,Utah,Taylorsville,84129,40.6677,-111.9388,,801,,
#10.10.200.252/30,1,,USA,United States,Utah,Orem,84042,40.2969,-111.6946,,801,NA,
#10.10.200.48/32,1,,USA,United States,Utah,Orem,84042,40.2969,-111.6946,,801,NA, 10.10.200.0/24,1,,USA,United States,Utah,Orem,84042,40.2969,-111.6946,,801,NA,
```
Viewing Geolocation IP Locations Data

To view IP location data in FTK
1. Open the Examiner.
2. Click the Volatile tab.
3. In the Volatile tab, click (Geolocation).
4. You can filter the items displayed and see item details. See Using the Geolocation Grid on page 603.

Using the Geolocation Network Information Grid
- When viewing network acquisition and volatile data connection information, you can now view a grid that displays the following information:
  - Process Start Time
  - Machine
  - User Name
  - Process Name
  - Path
  - Host Name
  - IP Address
  - Coordinates
  - Ports

You can show the communication between multiple pins.
Customizing the Examiner Interface

This chapter includes the following topics

- About Customizing the Examiner User Interface (page 608)
- The Tab Layout Menu (page 609)
- Moving View Panels (page 610)
- Creating Custom Tabs (page 612)
- Managing Columns (page 613)
- Customizing File List Columns (page 613)
- Creating User-Defined Custom Columns for the File List view (page 615)
- Deleting Custom Columns (page 616)
- Navigating the Available Column Groups (page 616)

About Customizing the Examiner User Interface

You can use the View menu to control the pane views displayed in each tab. There are several tabs by default, but you can create an interface view that best suits your needs. Add or remove panes from the current tab using the View menu. Click View and click the unchecked pane to add it to the current view, or click a checked item on the list to remove that pane from the current view.

To save the new arrangement

- Click View > Tab Layout > Save.

The View menu lets you do the following:

- Refresh the current view's data.
- View the Filter Bar
- Display the Time Zone for the evidence.
- Choose the display size for graphic thumbnails.
- Manage Tabs.
- Select Trees and viewing panes to include in various tabs.
- Open the Progress Window.
The Tab Layout Menu

Use the options in the Tab Layout menu to save changes to tabs, restore original settings, and lock settings to prevent changes.

The following table describes the options in the Tab Layout menu.

Tab Layout Menu Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Save</td>
<td>Saves the changes made to the current tab.</td>
</tr>
<tr>
<td>Restore</td>
<td>Restores the Examiner window to the settings from the last saved layout. Custom settings can be restored.</td>
</tr>
<tr>
<td>Reset to Default</td>
<td>Sets the window to the setting that came with the program. Custom settings will be lost.</td>
</tr>
<tr>
<td>Remove</td>
<td>Removes the selected tab from the window.</td>
</tr>
<tr>
<td>Save All Layouts</td>
<td>Saves the changes made to all tabs.</td>
</tr>
<tr>
<td>Lock Panes</td>
<td>Locks the panes in place so that they cannot be moved until they are unlocked.</td>
</tr>
<tr>
<td>Add New Tab</td>
<td>Adds a new tab to the window. The new tab will be like the one selected when this option is used. Customize the tab as needed and save it for future use.</td>
</tr>
</tbody>
</table>
Moving View Panels
Move view panes on the interface by placing the cursor on the title of the pane, clicking, dragging, and dropping the pane on the location desired. Holding down the mouse button undocks the pane. Use the guide icons to dock the pane in a pre-set location. The pane can be moved outside of the interface frame.

To place the view panel at a specific location on the application
1. Place the mouse (while dragging a view pane) onto a docking icon. The icon changes color.
2. Release the mouse button and the panel seats in its new position. The following table indicates the docking options available:

Docking Icons

<table>
<thead>
<tr>
<th>Docking Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Docks the view panel to the top half of the tab.</td>
</tr>
<tr>
<td></td>
<td>Docks the view panel to the right half of the tab.</td>
</tr>
<tr>
<td></td>
<td>Docks the view panel to the left half of the tab.</td>
</tr>
</tbody>
</table>

Customizing the Examiner Interface
Moving View Panels
Docking Icons (Continued)

<table>
<thead>
<tr>
<th>Docking Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Docks the view panel to the bottom half of the tab.</td>
</tr>
<tr>
<td></td>
<td>Docks the view panel to the top, right, left, bottom, or center of the pane. When docked to the center, the new pane overlaps the original pane, and both are indicated by tabs on the perimeter of the pane.</td>
</tr>
<tr>
<td></td>
<td>Docks the view panel to the top, right, left, or bottom of the tree pane. The tree panes cannot be overlapped.</td>
</tr>
<tr>
<td></td>
<td>Locks the panels in place, making them immovable. When the lock is applied, the blue box turns grey. This button is found on the toolbar.</td>
</tr>
</tbody>
</table>

Creating Custom Tabs
Create a custom tab to specialize an aspect of an investigation, add desired features, and apply filters as needed to accommodate conditions specific to a case.

To create a custom tab
1. Click on the tab that is most like the tab you want to create.
2. Click View > Tab Layout > Add New Tab Layout.
3. Enter a name for the new tab and click OK. The resulting tab is a copy of the tab you were on when you created the new one.
4. From the View menu, select the features you need in your new tab.

Note: Features marked with diamonds are mutually exclusive; only one can exist on a tab at a time. Features with check marks can coexist in more than one instance on a tab.

5. Choose from the following:
   - Click Save to save this new tab’s settings
   - Click View > Tab Layout > Save.
   - Click View > Tab Layout > Save All to save all changes and added features on all tabs.
To remove tabs
1. Highlight the tab to be removed
2. Click View > Tab Layout > Remove.

Managing Columns
Shared Columns use the same familiar windows and dialogs that Local Columns use.

To create a Shared Column Template
1. In Case Manager, click Manage > Columns.

   The Manage Shared Column Settings dialog opens.
2. Highlight a default Column Template to use as a basis for a Custom Column Template.
3. Click New.
4. Enter a new name in the Column Template Name field.
5. Select the Columns to add from the Available Columns pane, and click Add >> to move them to the Selected Columns pane.
6. Select from the Selected Columns pane and click Remove to clear an unwanted column from the Selected Columns.
7. When you have the new column template defined, click OK.

Additionally, column settings can be set as default per tab and case or per tab for all cases. Reset to factory options are also available to easily reverse changes to any of these settings.

To save this tab’s current column setting as default for this case
1. On the appropriate tab and in the File List pane, select the preferred column setting from the column settings drop down menu.
2. Navigate to View >> File List Columns >> Save As Case Default

To save each tab’s current column setting as default for this case
1. On the each tab of the examiner interface, select the preferred column setting from the column settings drop down menu.
2. Navigate to View >> File List Columns >> Save All As Case Default
To save this tab’s current column setting as default for ALL cases
1. On the appropriate tab and in the File List pane, select the preferred column setting from the column settings drop down menu.
2. Navigate to View >> File List Columns >> Save As Global Default

To save each tab’s current column setting as default for ALL cases
1. On the each tab of the examiner interface, select the preferred column setting from the column settings drop down menu.
2. Navigate to View >> File List Columns >> Save All As Global Default

Customizing File List Columns
The Column Settings dialog box allows the modification or creation of new definitions for the file properties and related information that display in the File List, and in what order. Columns display specific information about, or properties of, the displayed files.

Column settings are also used to define which file information appears in case reports. Use custom column settings in defining reports to narrow the File List Properties information provided in the Bookmark and File List sections.

Additional states have been added to keep track of users’ Label selections. For example, if the user has already checked a Label name, that filename and path will turn red, and it remains red as long as it remains different from the original status. Clicking it again will cycle it back to its original status and its color will return to black.

Note: Checking the Label name before choosing Apply Labels To, unchecks the Label name. Choose Apply Labels To first, then check or select the files to apply the Label to.

Column Settings can be customized and shared.
To define or customize Column Settings

1. From the File List, click **Column Settings** button to open the Manage Column Settings dialog. From the Manage Column Settings dialog you can do any of the following tasks:

<table>
<thead>
<tr>
<th>Button</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>New</td>
<td>Create a new column template. This option opens a blank template you can use to create a new template from scratch.</td>
</tr>
<tr>
<td>Edit</td>
<td>Edit existing custom column templates. Use this option to make changes to an existing custom column template. You cannot edit default templates.</td>
</tr>
<tr>
<td>Copy Selected</td>
<td>Copy existing default or custom column templates. Start with the settings in an existing template to customize it to your exact needs without starting from scratch.</td>
</tr>
<tr>
<td>Delete</td>
<td>Delete existing custom column templates. You cannot delete default templates</td>
</tr>
<tr>
<td>Import</td>
<td>Import custom column templates XML files from other cases. Use Import to utilize a template from another source or that was created after you created your case.</td>
</tr>
<tr>
<td>Export</td>
<td>Export custom column templates to XML files for others to use. Export a custom column to use in another system.</td>
</tr>
<tr>
<td>Make Shared</td>
<td>Case Administrators can Share custom column templates to the database so they are available to all new cases. Once custom columns are Shared, the Application Administrator manages them. However, the original remains in the case so the Case Administrator has full control of it. Case Reviewers do not have sufficient permissions to create custom column templates.</td>
</tr>
<tr>
<td>Apply</td>
<td>Apply the selected column template</td>
</tr>
</tbody>
</table>

2. To define column settings using a new or copied template, click **New, Edit, or Copy Selected** to open the familiar Column Settings dialog.

3. In the Column Template Name field, type a name for the template.

4. In the Available Columns list, select a category from which you want to utilize a column heading.
   - You can add the entire contents of a category or expand the category to select individual headings.
   - You can move any item in the list up or down to position that column in the File List view. The top position is the first column from left to right.

5. When you are finished defining the column setting template, click **OK** to save the template and return to the Manage Column Settings dialog.

6. Highlight the template you just defined, and click **Apply** to apply those settings to the current File List view.
Creating User-Defined Custom Columns for the File List view

You can define your own custom columns for use in the File List view. You must first export a file list to a TSV or a CSV file from a case, then populate the spreadsheet with custom column names and your own data as it relates to items that are listed by the ObjectID. To add the resulting custom columns to the File List view, you simply import the TSV or CSV file that you created, add the custom columns to the template, and apply the template.

If you import a custom column sheet that contains a column that you do not want to import, but you do not want to delete the column, you can type IGNORE in the first row of the column.

Files saved as TSV or CSV are encoded UTF-8.

To define custom columns for the File List view

1. Open CCExample.CSV in a spreadsheet program. The default path to the file is

   C:\Program Files\AccessData\Forensic Toolkit\[version_number]

Use this example file to help you create your own custom columns.
2. In the File List, select the files that you want to add to your custom columns settings template.
3. From the File List, click Export File List.
4. In the Save in text box, browse to and select the destination folder for the exported file.
5. In the File name text box, type the first name of the file, but do not specify the extension.

Note: You can overwrite user created column setting files by giving the column template the same name as an existing user created template. Be sure you provide a file name that is unique if you don’t want to overwrite the original or existing column template file.

6. In the Save As type text box, click the drop-down and choose CSV (Comma delimited) (*.CSV)
7. In the File List items to export group box, click All Highlighted.
8. Click Column Settings.
9. In the Column Settings dialog box, ensure that Item Number is in the Selected Columns list. If desired, you can move it to the top of the list, or remove all other columns headings that are listed in the

   Selected Columns list.
10. Click OK.
11. In the Choose Columns drop-down, select the Column Setting you just created or modified.
12. Click Save.
13. Open the CSV file that you just created with the Export File List.
14. Copy the item numbers in the Item Number column.
15. In the opened CCexample.CSV file, paste the item numbers in the OBJECTID column.
16. Edit the column headings the way you want them.

For example, the spreadsheet column, “MyCustomInt:INT” displays as the column heading “MyCustomInt” in the File List view.
- Edit “MyCustomInt” to be whatever you want:
- The INT portion allows integer values in the column
- MyCustomBool:BOOL column allows true or false values
- CustomStr:STRING heading allows text values.

17. Save the CCExample.CSV file with a new name, and in a place where you have rights to save and access the file as needed.

18. Close the FileList.CSV (or whatever name you gave the Export File List file).

19. On the Evidence menu, click **Import Custom Column File**.

20. Navigate to the CSV file that you just saved, then click **Open**.

21. In the “Custom column data imported” dialog box, click **OK**.

22. On the **Manage** menu, click **Column > Manage Columns**, or click Column Settings on the File List toolbar.

23. Choose a column template to copy, or create a new one.

24. Add the custom column headings to a new or existing template.

25. In the Column Settings dialog box, click **OK**.

26. In the Manage Column Settings dialog box, select the template that contains the custom headings, and then click **Apply**.

---

**Deleting Custom Columns**

You can remove and delete custom columns that you have added to any column templates. You can delete custom columns even if the File List view is turned off.

---

**Note:** The data is not deleted; only the custom columns that allowed you to see that specific data are deleted.

---

**To delete custom column data**

1. On the Evidence menu, click **Delete Custom Column Data**.
2. Click **Yes** to confirm the deletion.
Customizing the Examiner Interface

Managing Columns | 673
Navigating the Available Column Groups

The Column Settings dialog box groups column settings according to the following:

Available Column Groups

19. Common Features
20. Disk Image Features
21. Email Features
22. Entropy Stats
23. File Status Features
24. File System Features
25. Images (Photos, etc.)
26. Messages
27. Mobile Phones
28. Zip Specific Features
29. Office Specific Features
30. Cerberus Static Analysis Features
31. Microsoft IIS Internet Server
32. Log2t
33. Internet Data
34. Geolocation
35. System Summary Information
36. Contacts Information
37. All Features

Within each grouping, you can choose from a list of various column headings that you want to add. You can also delete selected columns or arrange them in the order you want them to appear in the File List view.
To view the name, short name, and description of each available column
1. On the Manage menu, click Columns > Managed Shared Columns.
2. Do one of the following:
   - Select a category.
   - Open a category and select an individual column setting name.
3. Do either of the following:
   - Click Add >> to move your selection to the Selected Columns list.
   - Double-click your selection to add it to the Selected Columns list.
4. Do either of the following.
   - Use standard Windows column sizing methods to resize the column margins, thereby allowing you to read each description.
   - Click anywhere in the Select Columns list box, and then hover over a column description to see the entire description.
5. Click **OK**.

**Note:** The following information may be useful when navigating or viewing Available Columns and Groups.

- When you view data in the File List view, use the type-down control feature to locate the information you are looking for. Sort on the Filename column, then select the first item in the list.

Type the first letter of the filename you are searching for. As you continue to type, next filename that matches the letters you have typed will be highlighted in the list.

If at some point you see the file you are looking for displayed in the list, simply click on it. You may type the entire file name for the exact name to be fully highlighted in the list.

- A new column has been added, “Included by Filters” within the All Features group. This column tells you which filter caused a file to display in the File List pane. The Included by Filters column is not sortable.

- In the past, the “Processed” column was able to display only two states, Yes, and No. It has been changed to display different states, such as the following:

  P = Default (may be a null value)
  C = Complete
**Note:** \( M = \) User’s manually carved items
Automatic Column Switching

This option when enabled will switch to a relevant column set automatically, depending on the evidence type selected.
Working with Evidence Reports

You can create a case report about the relevant information of a case any time during or after the investigation and analysis of a case. Reports can be generated in different formats, including HTML and PDF. The PDF report is designed specifically for printing hard copies with preserved formatting and correct organization. The HTML report is better for electronic distribution. This chapter includes the following topics:

- Creating a Case Report (page 619)
- Adding Case Information to a Report (page 620)
- Adding Bookmarks to a Report (page 621)
- Adding Graphics Thumbnails and Files to a Report (page 623)
- Adding a File Path List to a Report (page 625)
- Adding a File Properties List to a Report (page 626)
- Adding Registry Selections to a Report (page 627)
- Adding Screen Captures from Examiner (page 628)
- Selecting the Report Output Options (page 629)
- Creating a Load File (page 630)
- Viewing and Distributing a Report (page 633)
- Modifying a Report (page 634)
- Exporting and Importing Report Settings (page 634)
- Writing a Report to CD or DVD (page 635)
Creating a Case Report

You can use the Report Wizard to create a report. The settings that you specify in the Report Wizard are persistent, and remain until they are changed by the user. You do not need to click OK until all the report creation information is entered or selected. If you inadvertently close the Report Wizard, you can re-open it by clicking File > Report.

To Create a Case Report

1. In the Examiner, click File > Report to run the Report Wizard.
2. Define your requirements for the following:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Case Information</td>
<td>See Adding Case Information to a Report (page 620)</td>
</tr>
<tr>
<td>Bookmarks</td>
<td>See Adding Bookmarks to a Report (page 621)</td>
</tr>
<tr>
<td>Graphics</td>
<td>See Adding Graphics Thumbnails and Files to a Report (page 623)</td>
</tr>
<tr>
<td>Videos</td>
<td>See Adding a Video to a Report (page 624)</td>
</tr>
<tr>
<td>File Path List</td>
<td>See Adding a File Path List to a Report (page 625)</td>
</tr>
<tr>
<td>File Properties</td>
<td>See Adding a File Properties List to a Report (page 626)</td>
</tr>
<tr>
<td>Registry Selections</td>
<td>See Adding Registry Selections to a Report (page 627)</td>
</tr>
</tbody>
</table>

3. When you have completed defining the report, click OK to open the Report Output options dialog. See Selecting the Report Output Options (page 629)
Adding Case Information to a Report
The Case Information dialog lets you add basic case information to a report, such as the investigator and the organization that analyzed the case.
For information about other items you can define for a report, see Creating a Case Report (page 619).

To Add Case Information to a Report
1. In the Examiner, click File > Report.
2. In the left pane, under Report Outline, highlight Case Information to display the Case Information options in the right pane.
You can select the Case Information check box to include a case information section in the report. You can deselect the Case Information check box to exclude a case information section from the report.
3. In the Default Entries pane, deselect any entries that you do not want to include in the report.

If you inadvertently remove a default entry that you require, close and reopen the case to have the default entries displayed again.
4. Double-click the Value field to enter information.
5. Add and remove entries with the Add and Remove buttons under the Default Entries section.
6. Provide a label (Name) and a value (Information) for the included entries.
7. (Optional) Select the Include File Extensions option to include a file extensions list and count in the File Overview portion of the report.

The list of file extensions appears in the report under Case Information, after File Items and File Category, and before File Status. The File Extensions List can be very long and may span many pages. If you intend to print the report, this may not be desirable.
Adding Bookmarks to a Report

The Bookmarks dialog lets you create a section in the report that lists the bookmarks that were created during the case investigation. Each bookmark can have a unique sorting option and a unique column setting.

For information about other items you can define for a report, see Creating a Case Report (page 619).

To add Bookmarks to a Report

1. In the Examiner, click File > Report.
2. In the left pane, under Report Outline, highlight Bookmarks to display the Bookmarks options in the right pane.

You can select the Bookmarks check box to include bookmarks in the report. You can deselect the Bookmarks check box to exclude bookmarks from the report.

3. In the right pane, click Filter to open the filters list.
4. Select one the filters from the list. The empty line at the top of the list lets you apply no filter to the bookmarks.
5. Select the options to indicate which bookmarks you want to include. Choose Shared and/or User bookmarks by group, or individually.
6. For each bookmark you choose to include, you can choose options from the Bookmark section on the right. Options include:
   - Include email attachments
     - This setting applies to all email children, not only common attachments.
     - Selecting this setting activates the Export Options button.
   - Export files & include links
     - Selecting this setting activates the Export Options button.
   - Export Cerberus analysis html files
   - Include thumbnail for each object
7. Choose a Thumbnail Arrangement option for each bookmark or bookmark group as follows:
   - Number of thumbnails per row
   - Include all thumbnails at end of each bookmark section
   - Group all file paths at the end of thumbnails
8. Specify if you want to export the bookmarked files and include links to them in the report when it is generated.

9. Specify if you want to include graphic and video thumbnails that may be part of any bookmarks. If you want to create links to original files in the report, choose both to export the original files and to include graphic and video thumbnails when the report is generated.

10. In the Report Options dialog, click Bookmarks.

11. Click Sort Options and do the following:
   - Click the plus (+) to add a criterion, or click minus (-) to delete a criterion.
   - Click the down arrow button on the right side of each line to open the drop down of available sort columns.
   - Click OK to save the selected Sort Options and close the dialog.

Note: The sort options you see are determined by the Columns Template you have selected. For more information on customizing columns, see Customizing File List Columns (page 613).

12. Specify if you want to apply all settings for this bookmark to child files.

Bookmark Export Options

The Bookmark Export Options dialog contains the following three options:
- Link to exported email attachments and filter out attachments in bookmark
  - When selected, this option creates links to exported email attachments and filters out the attachments in the bookmark.
- Include re-constructed web pages
  - When selected, this option exports all of the files necessary to view re-constructed web pages. The files are stored in the Report_Files folder in a sub folder called reconstructedpage.
- Export selections as their own file
  - When selected, this option saves each bookmark selection as an individual file.
Adding Graphics Thumbnails and Files to a Report

The Graphics section in the Report Options dialog lets you define whether-or-not to create a section in the report that displays thumbnail images of the case graphics. You can also link the thumbnails to a full sized version of the original graphics if desired.

For information about other items you can define for a report, See Creating a Case Report (page 619).

To add graphics thumbnails and files to a report

1. In the Examiner, click File > Report.
2. In the left pane, under Report Outline, highlight Graphics to display the Graphics options in the right pane.

You can select the Graphics check box to include graphics in the report. You can deselect the Graphics check box to exclude graphics from the report.

3. To apply a filter to any included graphics files in a report, click Filter and select a filter to apply to the graphics.
4. To export and link full-sized graphics in the report, click the Export and link full-size graphics to thumbnails option.
5. Select one of the following options

   • Include checked graphics only
   • Include all graphics in the case

6. To sort the graphics by name or by path, click Sort Options. In the Sort Options dialog, use the Plus (+) and Minus (-) buttons to add and remove sort options. Click the drop-down arrow on the right side of the line to select either Name or Path.
7. Specify the number of graphics thumbnails to display per row and choose whether-or-not to Group all filenames at end of report.
Adding a Video to a Report

The Video section in the Report Options dialog lets you define whether or not to create a section in the report that displays the thumbnail images and/or the rendered MP4 files of the case videos. You can also choose to include a link to the original full sized version of the video. These thumbnails and MP4 videos are created during evidence processing or during additional analysis.

See Generating Thumbnails for Video Files (page 446). See Creating Common Video Files (page 447).

To add video thumbnails and files to a report
1. In the Examiner, click File > Report.
2. In the left pane, under Report Outline, highlight Videos to display the Video options in the right pane.

You can select the Videos check box to include videos in the report. You can deselect the Videos checkbox to exclude videos from the report.
3. To apply a filter to any included video files in a report, click Filter and select a filter to apply to the videos.
4. To export and link the original videos in the report, click the Export and link original videos option.
5. To include a link to the rendered MP4 videos that were created during evidence processing or during additional analysis, check Export rendered videos.
6. To include the thumbnails of the videos in the report that were created during evidence processing or during additional analysis, check Export rendered thumbnails.
7. Select one of the following options
   - Include checked videos only
   - Include all videos in the case
8. To sort the videos by name or by path, click Sort Options. In the Sort Options dialog, use the Plus (+) and Minus (-) buttons to add and remove sort options. Click the drop-down arrow on the right side of the line to select either Name or Path.
9. Specify the number of video thumbnails to display per row in the Rendered Thumbnail Arrangement group box.
10. Click Columns. In the Manage Column Settings dialog, select the Settings Template to copy or edit.

For detailed information on creating and modifying Columns Templates, see Customizing File List Columns (page 613).
Adding a File Path List to a Report

The File Paths dialog lets you create a section in the report that lists the file paths of files in selected categories. The File Paths section displays the files and their file paths; it does not contain any additional information.

For information about other items you can define for a report, See Creating a Case Report (page 619).

**To add a File Path List to a Report**

1. In the Examiner, click **File > Report**.
2. In the left pane, under **Report Outline**, highlight **File Path** to display the **File Path** options in the right pane.

You can select the **File Path** check box to include a file path section in the report. You can deselect the **File Path** check box to exclude a file path section from the report.

3. Select a filter from the **Filter** drop-down, to apply a filter to the items you want to include a file path list.
   
   You can leave the filter option empty to not apply a filter.

4. Select from the **Available Categories** list to include the category or categories in the report by dragging the category to the **Selected Categories** list.

5. To also export and link to the selected files in the File Path list, select the check-boxes box next to the items in the **Selected Categories** box.

If you do not select a check-box **Selected Categories** list, the File Path is included in the report, but the files themselves are not exported and linked to the File Path in the report.
Adding Registry Selections to a Report

The File Properties dialog lets you create a section in the report that lists the file properties of files in selected categories. Several options let you make the File Properties List in the report as specific or as general as you want it to be. For information about other items you can define for a report, see Creating a Case Report (page 619).

To Add a File Properties List to a Report

1. In the Examiner, click File > Report.

   In the left pane, under Report Outline, highlight File Properties to display the File Properties options in the right pane.

   You can select the File Properties check box to include a file properties section in the report. You can deselect the File Properties check box to exclude a file properties section from the report.

2. Either click the Filter drop-down arrow and selecting the desired filter, or choose no filter by selecting the blank entry at the top of the filter drop-down list.

3. Drag and drop the categories that you want to include from the Available Categories window into the Selected Categories window.

4. Check a category in the Selected Categories window to export related files and link them to the File Properties list in the report.

   Checking an item automatically selects the files and folders under it. If you do not want to include all sub-items, expand the list and select and deselect each item individually.

5. In the Report Options dialog, click File Properties.

6. In the File Properties options area, click Columns.

7. In the Manage Column Settings dialog, select the Settings Template to copy or edit.

   For detailed information on creating and modifying Columns Templates, see Customizing File List Columns (page 613).

8. When you are done defining the columns settings, click OK.

   You might want to define how the data is sorted, according to column heading. In the File List view you are limited to a primary and secondary search. In the Report wizard, you can define many levels of sorting.


10. In the File Properties options area, click Sort Options and do the following:
Adding Registry Selections to a Report

- Click the plus (+) to add a criterion, or click minus (-) to delete a criterion.
- Click the down arrow button on the right side of each line to open the drop down of available sort columns.
- Click OK to save the selected Sort Options and close the dialog.

**Note:** The sort options you see are determined by the Columns Template you have selected

For more information on customizing columns, see Customizing File List Columns (page 613).

If your drive image contains Registry files, you can include them in your report. When creating a Report that includes Registry files, a DAT extension is being added to the link. If the link does not open in the report, it can be exported and opened in Notepad.

For information about other items you can define for a report, see Creating a Case Report (page 619).

**To Add Registry Selections to a Report**

1. In the *Examiner*, click File > Report.

   In the left pane, under Report Outline, highlight Registry Selections to display the registry selections options in the right pane.

   You can select the Registry Selections check box to include a Registry Selections section in the report. You can deselect the Registry Selections check box to exclude a Registry Selections section from the report.

2. In the Registry File Types window, check the file types for which you want to include headings for in your report.

3. In the right window, check the registry file paths that you want included in your report.

4. Mark the box Include user generated reports (if any) if you have generated Registry Reports using Registry Viewer, and you want to include them in this report.

**Note:** User-generated reports must exist in the case before generating the report, otherwise, this option is disabled. These reports are generated in Registry Viewer and can be collected from the Registry data found on the source drive.

5. Mark the box Select Auto Reports, to view and select which registry reports to include in the report from those that were generated automatically based on the registry reports selection in Case Manager.
Adding Registry Selections to a Report
> Case > New > Detailed Options > Evidence Refinement.

**Note:** If you did not select this option during pre-processing, this option is disabled in the Report Options dialog.
Adding Screen Captures from Examiner

You can now capture screen shots within the Examiner interface. You can include the screen captures when creating reports. You can use screen captures to include information that is not easy to export or include in reports, such as:

- The contents of the Natural view (File Content pane)
- The contents and information in the File List
- The contents of visualization pages

These UI elements can include information that is useful as evidence, but there is no way to present it outside of the UI.

When you create a screen capture, the following occurs:

- The file is saved in the case folder under a Screenshots sub-folder. (Do not manually rename the captured files, otherwise the Report dialog will not find them.)
- The file is saved in the original size and in a smaller size that may be needed to fit in a report.
- The name and description of the file is saved in the database so that they can be displayed in the Report Options dialog.

To create a screen capture

1. In the Examiner, click the screen capture icon.

2. Click and drag the + cursor to select the area that you want to capture.

3. In the Screen Capture Info dialog, give the screen capture file a name.

4. Enter a description.

This is recorded with the filename in the database.

5. Click Save.

6. To cancel a screen capture, click Esc.

To include a screen capture in a report

1. In the Examiner, click File > Report.

2. In the Report Options, click Screen Capture.
3. Select the screen captures that you want to include in the report.

4. (Optional) You can edit the description of the files, but not the filename.

5. Configure the other options for the report.

When the report is created, the image files are copied to the report folder.
Writing a Report to CD or DVD
Selecting the Report Output Options

The Report Output dialog lets you select the location, language, report formats, and other details of the report. You can also recreate the directory structure of exported items.

For information about other items you can define for a report, See Creating a Case Report (page 619).

To select the report output options
1. When you have completed defining the report, from the Report Options dialog, click OK to open the Report Output options dialog.
2. Type the destination folder name for the saved report, or use the Browse button to locate and select a location.
3. Use the drop-down arrow to select the language for the written report. Available languages are as follows:

   Arabic (Saudi Arabia)  Chinese (Simplified, PRC)
   English (United States)  German (Germany)
   Japanese (Japan)  Korean (Korea)
   Portuguese (Brazil)  Russian (Russia)  Spanish (Spain, Traditional Sort)  Swedish (Sweden)
   Turkish (Turkey)

4. Indicate the formats for publishing the report. You can choose any or all of the output formats.

To view a report made in any of the supported formats, you must have the appropriate application installed on your computer. Options are as follows:

PDF (Adobe Reader)  HTML (Windows Web Browser)  XML (Windows Web Browser)  RTF (Rich Text Format: Most Text Editors)
WML (Unix Web Browser)  DOCX (MS Office Word 2007)
ODT (Open Document Interchange: Sun Microsystems OpenOffice Documents)  Load File
Writing a Report to CD or DVD

Note: Some report output formats require J#, either 1.1 or 2.0. If you select RTF format, for example, and J# is not installed, you will see an error.

5. Under Export Options do the following:
   - Check the *Use object identification number for filename* to shorten the paths to data in the report. Links are still created for proper viewing of the files.
   - The unique File ID numbers, when used in a report, keep the pathnames shorter. This makes burning the report to a CD or DVD more reliable.
   - Check the *Append extension to filename if bad/absent* box to add the correct extension where it is not correct, or is missing.

6. Under HTML Report Customization, choose from the following:
   - If you wish to use your own custom graphic or logo, mark the *Use custom logo graphic* box, then browse to the file and select it. Use GIF, JPG, JPEG, PNG, or BMP file types.
   - If you wish to use a custom CSS file, mark the *Use custom CSS* box. Select the folder where the custom CSS files have been saved. Click **OK**. The folder you selected displays in the “Use CustomCSS” text box.

7. Click **OK** to run the report.

If the report folder you selected is not empty, you will see the following error message: Choose to **Delete** or **Archive** the contents of the folder, or to **Cancel** the report. Delete the contents of the current destination folder, or change to a different destination folder, then recreate the report or import it if you saved it during creation.

Creating a Load File
It is possible to create a load file, which enables you to export data from an existing or new case and import it into litigation document management applications such as AccessData Summation and eDiscovery.

To Create a Load File
1. In the *Examiner*, click **File > Report**.
Writing a Report to CD or DVD

2. In the left pane, under the Report Outline, select the check boxes for the options you would like to include in your load file. Be sure to highlight each item selected and fill out the appropriate information. You can add information to these areas using the methods described in the previous segments. When finished, press OK.

3. In the Report Output dialog, enter the path to the Report Folder. This is where your report will be located.

4. Select the appropriate Language and Time Zone.
Writing a Report to CD or DVD

5. Select the correct Export Option. Options include:
   - Use object identification number for filename
     - This setting makes it so the object identification number used in the existing or new case is also used as the filename in the load file.
   - Append extension to filename if bad/absent
     - Selecting this setting will append the correct or assigned filename to a file if none is present or if the current one is bad.

6. In the Formats area, check the box next to Load File and click the Options button.

7. In the Load File Export Options dialog, enter a Load File Name.

8. Select a Format for your load file. Options include:
   - Browser Briefcase
     - This option generates an HTML format that provides links to the native documents, images, and text files. You can have multiple links for image, native, and text documents. You can also work with production sets exported previously in iBlaze Browser Briefcase format. This allows you to have greater control over the production set.
   - CaseVantage
     - This option generates a DII file specifically formatted for use with the AD Summation CaseVantage program.
   - Concordance
     - This option generates a DAT file that can be used in Concordance.
   - EDRM
     - This option generates an XML file that meets the EDRM v1.2 standard.
   - Generic
     - This option generates a standard delimited text file.
   - iCONECT
     - This option generates an XML file formatted for use with the iConect program.
   - Introspect
     - This option generates an IDX file specifically formatted for use with the Introspect program.
   - Relativity
Writing a Report to CD or DVD

- This option generates a DAT file that can be used in Relativity.

- Ringtail (MDB)
  - This option generates a delimited text file that can be converted to be used in Ringtail.
Writing a Report to CD or DVD

- Summation eDII
  - This option generates a DII file specifically formatted for use with the AD Summation iBlaze or Enterprise programs.

**Note:** If you are outputting a Concordance, Relativity, or Generic load file, and include rendered images, you will also get an OPT and LFP file in the export directory.

9. Choose an *Encoding* option for your load file from the following:
   - ANSI
   - UTF-8
   - UTF-16

10. If you are creating a Concordance, Generic, Introspect, or Relativity load file, you need to specify the following options:
   - Choose whether to *Include a Header Row* by clicking on the checkbox.
   - Select the Multi-Entry Separator.
   - Select the Field Mapping.
   - Select the Text Identifier.
   - Select the *Newline*.

11. For the Browser Briefcase, CaseVantage, EDRM, iConect, Ringtail, or Summation eDII options, select only the Multi-Entry Separator.

12. In the *Available Fields* pane, select the options you want to appear in your report. Highlight each field you would like to include and click the >> button to move it to the *Selected Fields* pane. If you would like to change the order of appearance for these items in the report, highlight the item you would like to move in the *Selected Fields* pane and click on the Up or Down button until it is in the right place.

13. The *Files To Include* tab contains the following three options:
   - Export Native Files

When selected, this option allows you to export the emails contained in PST/NSF in one of three different ways:
   - Output a reduced version of the original PST/NSF file
Writing a Report to CD or DVD

- Output messages as individual HTML/RTF files
- Output messages as individual MSG files
Writing a Report to CD or DVD

- Export Rendered Images

When selected, this option allows you to select how rendered images appear in the load file. You can export using one or both of the following options:
  - Use existing image
  - Use SWF image

You can also select the File Format and Page Size for displaying these images.

- Export Text

When selected, this option allows you to choose the Export Priority from the following options:
  - Export extracted text over OCR text
  - Export OCR text over extracted text
  - Export both extracted text and OCR text

14. When finished selecting these options, click OK in both the Load File Export Options and Report Output dialogs.

15. The progress of load file generation will appear in the Data Processing Status dialog. Once the load file is generated, you can find it in the folder entered in Step 3. This folder will contain the load file as well as the original files for any items included in the report.

Note: Best results occur when you select the Summation defaults and the Enable Standard Viewing feature during processing when creating the case.

Customizing the Report Graphic

When you select HTML as an output format, you can add your own graphic or logo to the report.

To add your own graphic or logo
1. In the Examiner, click File > Report to open the Report wizard.
2. From the Report Options dialog, after you are done making selections for the Report Outline, click OK.
3. In the Report Output dialog, under Formats, mark HTML. This activates the HTML Report Customization options.
Writing a Report to CD or DVD

5. Click the **Browse** button to open the Windows Explorer view and browse to the graphic file to use for the report. The file format can be JIF, JPG, JPEG, PNG, or BMP.

6. Click **Open**.

7. When all Report options have been selected, click **OK**.

The progress bar dialog indicates the progress of the report.

---

**Note:** When selected, the finished HTML and/or PDF reports open automatically.

You can process only one set of reports at a time. If you select the options to create several different report formats before clicking **OK** to generate the report, all will process concurrently. However, if you start that process and then decide to create a new report, you will not be able to until the current report is finished generating.

If you start another report too soon, you will be prompted to wait, if you chose to create either HTML or PDF format for the report, it will automatically open when creation is complete. Otherwise, to view the report, click **Yes** when prompted.

---

**Using Cascading Style Sheets**

The formatting of reports can be customized with Cascading Style Sheets (CSS). Reports stores a file path you select (default or custom) to the folder containing the custom CSS files. When CSS is not selected, Reports use the default settings.

For reports to utilize the cascading style sheets, three CSS files are necessary, and must all be located in the specified CSS folder:

- Common.CSS
- Bookmarks.CSS
- Navigation.CSS

The original CSS files are found in the following path if no changes were made to the default:

C:\Program Files\AccessData\Forensic Toolkit\<version>\bin\ReportResources

Copy the *CSS files to a different directory before making changes to any of these files. Do not make changes to the original files.

To utilize the custom CSS files, click **Use custom CSS**, and select the path to the folder where the custom CSS files are stored.

When CSS is selected, Reports checks for those files in the specified directory. If any of the three files is missing you are notified and the report does not proceed.
Writing a Report to CD or DVD

**Note:** The UI option consists of a check box and a text path string. The path string points to the path directory that contains the three needed CSS files.

**Note:** The UI options settings are persistent per Windows login user. Thus, your selections will be persistent across the Case List for the currently authenticated user.

**Important:** In versions, the cascading style sheets have been updated for a better user experience. Updates include persistent highlighting on the navigation tree (so examiners know which item they are viewing) and better organization of data within the report.

However, if you have created personalized templates in previous versions, you will need to re-create them for 5.1.

Viewing and Distributing a Report

The report contains the information that you selected in the Report Wizard. When included in the report, files appear in both raw data and in the report format.

**To view the report outside of Examiner**

1. Browse to the report file
2. Click on the report file:
   - Click on index.htm to open an HTML document in your Web browser.
   - Click on the file [report].PDF to open the report in a PDF viewer.

Modifying a Report

Modify the report by changing the report settings, and recreating it. Add the new evidence or change report settings to modify the report to meet your needs.

Change the report settings for each report as needed.

All previously distributed reports should be retracted to keep all recipients current.

**Note:** If you want to keep a previous report, save the new report to a different folder that is empty.
Writing a Report to CD or DVD

Exporting and Importing Report Settings

Report settings are automatically saved whenever you generate a report. You can export the settings that you used as an XML file. You can then later import and reapply those same settings to use with new reports that you generate.

**To export report settings**

1. In the *Examiner*, click **File > Report**.
2. In the *Report Options* dialog box, click **Export**.
3. In the *Export Sections* dialog, select the sections that you want to export.
4. Click **OK**.
5. Click **Browse** to select a folder to save the settings.
6. You can accept the default name for the report settings file, or you can type a name for the settings file. An XML extension is automatically added when the report is created.
7. Click **Save** for each item you have selected in the Report Outline list.
8. Click **OK**.

**To import saved settings for a new report**

1. In the *Examiner*, click **File > Report**.
2. In the *Report Options* dialog, click **Import**.
3. Browse to a settings XML file that you want to apply, and select it.
4. Click **Open** to import and apply the settings file to your current report.
Writing a Report to CD or DVD

You can write a report to a CD or DVD, depending on the report’s size. It is recommended that you select **Use object identification number for filename**, in the Report Output options dialog. This option keeps paths shorter, so they do not exceed the limits of the media format.

After you create the report, write only the contents from the root of the report folder, and not the report folder itself. The autorun automatically launches the report’s main page (index.htm) using the default browser when the CD is read on a Windows computer.

**Note:** The following information pertains to burning reports to a CD or DVD.

- When burning some reports to a CD, some Registry Viewer Auto Reports links may be broken, where they work when viewing on the computer. To avoid this issue, make sure that longer Joliet filenames are enabled when burning report to a CD.
- To launch the report, the computer must be configured to automatically execute autorun files.
- If you burn the folder that contains the report to the CD or DVD, the autorun will not be at the root of the disk, and will not work properly.
- To prevent broken links to report files, use File Item numbers instead of names to keep paths short, and / or use the Joliet file naming to allow longer file paths.
Using the Sawmill Log Tab

This chapter includes the following topics
- The Sawmill Log Tab (page 636)

The Sawmill Log Tab

The Sawmill Log tab is optional and although you can choose to select it during installation, if Sawmill is not installed, you will get web page errors when you try to view the tab. When you purchase the Sawmill Log product, follow the installation instructions provided to activate this tab.
Part V

Reference

This part contains additional reference information and contains the following appendices

- Working with Windows Registry Evidence (page 638)
- Supported File Systems and Drive Image Formats (page 647)
- Recovering Deleted Material (page 650)
- Managing Security Devices and Licenses (page 653)

Chapter 41

Working with Windows Registry Evidence

This appendix contains information about the Windows Registry and what information can be gathered from it for evidence. It includes the following topics:

- Understanding the Windows Registry (page 638)
- Windows XP Registry Quick Find Chart (page 643)

Understanding the Windows Registry

For forensic work, registry files are particularly useful because they can contain important information such as the following:

- Usernames and passwords for programs, email, and Internet sites
- A history of Internet sites accessed, including dates and times
- A record of Internet queries (i.e., searches performed on Internet search engines like Google, Yahoo, etc.)
- Lists of recently accessed files (e.g., documents, images, etc.)
- A list of all programs installed on the system

AccessData Registry Viewer allows you to view the contents of Windows operating system registries. Unlike the standard Windows Registry Editor, which only displays the current system’s registry, Registry Viewer lets you examine registry files from any Windows system or user. Registry Viewer also provides access to a registry’s protected storage, which contains passwords, usernames, and other information not accessible from within Windows Registry Editor.
The files that make up the registry differ depending on the version of Windows. The tables below list the registry files for each version of Windows, along with their locations and the information they contain.
### Windows 9x Registry Files

The following table describes each item on the Windows 9x registry files.

<table>
<thead>
<tr>
<th>File</th>
<th>Location</th>
<th>Description</th>
</tr>
</thead>
</table>
| system.dat       | \Windows     | - Protected storage for all users on the system. Protected Storage is an access-restricted area of the registry that stores confidential user information including usernames and passwords for Internet web sites, email passwords for Microsoft Outlook or Outlook Express, and a record of queries (i.e., searches performed on Internet search engines like Google, Yahoo, etc.), including the time and date when they were performed.  
- Lists installed programs, their settings, and any usernames and passwords associated with them.  
- Contains the System settings. |
| user.dat         | \Windows     | - MRU (Most Recently Used) list of files. MRU Lists maintain a list of files so users can quickly re-access files. Registry Viewer allows you to examine these lists to see what files have been recently used and where they are located. Registry Viewer lists each program’s MRU files in order from most recently accessed to least recently accessed.  
- User preference settings (desktop configuration, etc.). |
|                  | profiles\user account |                                                                                                                                         |
Windows 9x Registry Files

Windows NT and Windows 2000 Registry Files

The following table describes each item in the Windows NT and Windows 2000 registry files.

<table>
<thead>
<tr>
<th>Windows NT and Windows 2000 Registry Files</th>
</tr>
</thead>
<tbody>
<tr>
<td>NTUSER.DAT</td>
</tr>
</tbody>
</table>

\Documents and Settings\[user account]

If there are multiple user accounts on the system, each user has an ntuser.dat file.

- Protected storage for all users on the system. Protected Storage is an access-restricted area of the registry that stores confidential user information including usernames and passwords for Internet web sites, email passwords for Microsoft Outlook or Outlook Express, and a record of Internet queries (i.e., searches performed on Internet search engines like Google, Yahoo, etc.), including the time and date when they were performed.

- All installed programs, their settings, and any usernames and passwords associated with them.

- User preference settings (desktop configuration, etc.).

---

<table>
<thead>
<tr>
<th>default</th>
<th>\Winnt\system32\config</th>
<th>System settings.</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAM</td>
<td>\Winnt\system32\config</td>
<td>User account management and security settings.</td>
</tr>
<tr>
<td>SECURITY</td>
<td>\Winnt\system32\config</td>
<td>Security settings.</td>
</tr>
<tr>
<td>software</td>
<td>\Winnt\system32\config</td>
<td>All installed programs, their settings, and any usernames and passwords associated with them.</td>
</tr>
<tr>
<td>system</td>
<td>\Winnt\system32\config</td>
<td>System settings.</td>
</tr>
</tbody>
</table>
## Windows XP Registry Files

The following table describes each item in the Windows XP registry files.

<table>
<thead>
<tr>
<th>Windows XP Registry Files</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>NTUSER.DAT</th>
<th>\Documents and Settings[user account]</th>
</tr>
</thead>
<tbody>
<tr>
<td>If there are multiple user accounts on the system, each user has an ntuser.dat file.</td>
<td></td>
</tr>
<tr>
<td>Protected storage for all users on the system. Protected Storage is an access-restricted area of the registry that stores confidential user information including usernames and passwords for Internet web sites, email passwords for Microsoft Outlook or Outlook Express, and a record of Internet queries (i.e., searches performed on Internet search engines like Google, Yahoo, etc.), including the time and date when they were performed.</td>
<td></td>
</tr>
<tr>
<td>All installed programs, their settings, and any usernames and passwords associated with them.</td>
<td></td>
</tr>
</tbody>
</table>
The logical registry is organized into the following tree structure:

The top level of the tree is divided into hives. A hive is a discrete body of keys, subkeys, and values that is rooted at the top of the registry hierarchy. On Windows XP systems, the registry hives are as follows:

- **HKEY_CLASSES_ROOT (HKCR)**
- **HKEY_CURRENT_USER (HKCU)**
- **HKEY_LOCAL_MACHINE (HKLM)**
- **HKEY_USERS (HKU)**
- **HKEY_CURRENT_CONFIG (HKCC)**
- **HKEY_DYN_DATA (HKDD)**

**HKEY_LOCAL_MACHINE** and **HKEY_USERS** are the root hives. They contain information that is used to create the **HKEY_CLASSES_ROOT**, **HKEY_CURRENT_USER**, and **HKEY_CURRENT_CONFIG** hives.

**HKEY_LOCAL_MACHINE** is generated at startup from the system.dat file and contains all the configuration information for the local machine. For example, it might have one configuration if the computer is docked, and another if the computer is not docked. Based on the computer state at startup, the information in **HKEY_LOCAL_MACHINE** is used to generate **HKEY_CURRENT_CONFIG** and **HKEY_CLASSES_ROOT**.

**HKEY_USERS** is generated at startup from the system User.dat files and contains information for every user on the system.

Based on who logs in to the system, the information in **HKEY_USERS** is used to generate **HKEY_CURRENT_USER**, **HKEY_CURRENT_CONFIG**, and **HKEY_CLASSES_ROOT**.

Keys and subkeys are used to divide the registry tree into logical units off the root.

When you select a key, Registry Editor displays the key's values; that is, the information associated with that key. Each value has a name and a data type, followed by a representation of the value's data. The data type tells you what kind of data the value contains as well as how it is represented. For example, values of the **REG_BINARY** type contain raw binary data and are displayed in hexadecimal format.
**Possible Data Types**

The following table lists the Registry's possible data types.

### Registry Data Types

<table>
<thead>
<tr>
<th>REG_BINARY</th>
<th>Binary Value</th>
<th>Raw binary data. Most hardware component information is stored as binary data and is displayed in hexadecimal format.</th>
</tr>
</thead>
<tbody>
<tr>
<td>REG_DWORD</td>
<td>DWORD Value</td>
<td>Data represented by a number that is 4 bytes long (a 32-bit integer). Many parameters for device drivers and services are this type and are displayed in binary, hexadecimal, or decimal format. Related values are REG_DWORD_LITTLE_ENDIAN (least significant byte is at the lowest address) and REG_DWORD_BIG_ENDIAN (least significant byte is at the highest address).</td>
</tr>
<tr>
<td>REG_EXPAND_SZ</td>
<td>Expandable String Value</td>
<td>A variable-length data string. This data type includes variables that are resolved when a program or service uses the data.</td>
</tr>
<tr>
<td>REG_MULTI_SZ</td>
<td>Multi-String Value</td>
<td>A multiple string. Values that contain lists or multiple values in a format that people can read are usually this type. Entries are separated by spaces, commas, or other marks.</td>
</tr>
<tr>
<td>REG_SZ</td>
<td>String Value</td>
<td>A text string of any length.</td>
</tr>
<tr>
<td>REG_RESOURCE_LIST</td>
<td>Binary Value</td>
<td>A series of nested arrays designed to store a resource list used by a hardware device driver or one of the physical devices it controls. This data is detected by the system and is displayed in hexadecimal format as a Binary Value.</td>
</tr>
<tr>
<td>REG_RESOURCE_REQUIREMENTS_LIST</td>
<td>Binary Value</td>
<td>A series of nested arrays designed to store a device driver's list of possible hardware resources that it, or one of the physical devices it controls, can use. This data is detected by the system and is displayed in hexadecimal format as a Binary Value.</td>
</tr>
<tr>
<td>REG_FULL_RESOURCE_DESCRIPTOR</td>
<td>Binary Value</td>
<td>A series of nested arrays designed to store a resource list used by a physical hardware device. This data is displayed in hexadecimal format as a Binary Value.</td>
</tr>
<tr>
<td>REG_NONE</td>
<td>None</td>
<td>Data with no particular type. This data is written to the registry by the system or applications and is displayed in hexadecimal format as a Binary Value.</td>
</tr>
<tr>
<td>REG_LINK</td>
<td>Link</td>
<td>A Unicode string naming a symbolic link.</td>
</tr>
<tr>
<td>REG_QWORD</td>
<td>QWORD Value</td>
<td>Data represented by a number that is a 64-bit integer.</td>
</tr>
</tbody>
</table>
Additional Considerations

If there are multiple users on a single machine, you must be aware of the following issues when conducting a forensic investigation:

- If there are individual profiles for each user on the system, you need to locate the USER.DAT file for the suspects.
- If all the users on the system are using the same profile, everyone’s information is stored in the same USER.DAT file. Therefore, you will have to find other corroborating evidence because you cannot associate evidence in the USER.DAT file with a specific user profile.
- On Windows 9x systems, the USER.DAT file for the default user is used to create the USER.DAT files for new user profiles. Consequently, the USER.DAT files for new profiles can inherit a lot of junk.

To access the Windows registry from an image of the suspect’s drive, you can do any of the following:

- Load the suspect’s drive image and export his or her registry files to view them in Registry Editor.
- Mount a restored image as a drive, launch Registry Editor at the command line from your processing machine, export the registry files from the restored image, then view them in a third-party tool.

Note: The problem with this method is that you can only view the registry as text. Registry Editor displays everything in ASCII so you can’t see hex or binary values in the registry.

- Use Registry Viewer. Registry Viewer integrates seamlessly with the Examiner to display registry files within the image and create reports.

Important: Registry Viewer shows everything you normally see in live systems using the Windows Registry Editor. However, unlike Registry Editor and other tools that use the Windows API, Registry Viewer decrypts protected storage information so it displays values in the Protected Storage System Provider key (PSSP). Registry Viewer also shows information that is normally hidden in null-terminated keys.
Seizing Windows Systems

Information stored in the registry—Internet Messenger sessions, Microsoft Office MRU lists, usernames and passwords for internet Web sites accessed through Internet Explorer, and so forth—are temporarily stored in HKEY_CURRENT_USER. When the user closes an application or logs out, the hive’s cached information is pulled out of memory and written to the user’s corresponding USER.DAT.

**Note:** Passwords and MRU lists are not saved unless these options are enabled.

**Important:** Because normal seizure procedures require that there be no alteration of the suspect’s computer in any way, you must be able to articulate why you closed any active applications before pulling the plug on the suspect’s computer. Sometimes it is better to simply pull the plug on the computer; other times, it makes more sense to image the computer in place while it is on. It may depend on what is the most important type of data expected to be found on the computer.

For example, Windows updates some program information in the registry when the changes are made. Other information is not updated until a program is closed. Also, if the computer’s drive is encrypted and you cannot decrypt it or don’t have the Key or password, you may have no choice except to image the live drive.

The Registry Quick Find Chart shown below gives more information.

**Windows XP Registry Quick Find Chart**

The following charts describe common locations where you can find data of forensic interest in the Windows Registry.

### System Information

**Windows XP Registry System Information**

<table>
<thead>
<tr>
<th>Registered Owner</th>
<th>Software</th>
<th>Microsoft\Windows NT\CurrentVersion</th>
<th>This information is entered during installation, but can be modified later.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registered Organization</td>
<td>Software</td>
<td>Microsoft\Windows NT\CurrentVersion</td>
<td>This information is entered during installation, but can be modified later.</td>
</tr>
<tr>
<td>Run</td>
<td>Software</td>
<td>Microsoft\Windows\Current Version\Run</td>
<td>Programs that appear in this key run automatically when the system boots.</td>
</tr>
<tr>
<td>Logon Banner Message</td>
<td>Software</td>
<td>Microsoft\Windows\Current Version\Policies\System\Legal NoticeText</td>
<td>This is a banner that users must click through to log on to a system.</td>
</tr>
<tr>
<td>Mounted Devices</td>
<td>System</td>
<td>MountedDevices</td>
<td>Database of current and prior mounted devices that received a drive letter.</td>
</tr>
<tr>
<td>Current Control Set</td>
<td>System</td>
<td>Select</td>
<td>Identifies which control set is current.</td>
</tr>
<tr>
<td>Shutdown Time</td>
<td>System</td>
<td>ControlSetXXX\Control\Windows</td>
<td>System shutdown time.</td>
</tr>
<tr>
<td>Event Logs</td>
<td>System</td>
<td>ControlSetXXX\Services\Eventlog</td>
<td>Location of Event logs.</td>
</tr>
<tr>
<td>Dynamic Disk</td>
<td>System</td>
<td>ControlSetXXX\Services\DMIO\Boot Info\Primary Disk Group</td>
<td>Identifies the most recent dynamic disk mounted in the system.</td>
</tr>
<tr>
<td>Pagefile</td>
<td>System</td>
<td>ControlSetXXX\Control\Session Manager\Memory Management</td>
<td>Location, size, set to wipe, etc.</td>
</tr>
<tr>
<td>Last User Logged In</td>
<td>Software</td>
<td>Microsoft\Windows NT\CurrentVersion\Winlogon</td>
<td>Last user logged in - can be a local or domain account.</td>
</tr>
<tr>
<td>Product ID</td>
<td>Software</td>
<td>Microsoft\Windows NT\CurrentVersion</td>
<td></td>
</tr>
<tr>
<td>OS Version</td>
<td>Software</td>
<td>Microsoft\Windows NT\CurrentVersion</td>
<td></td>
</tr>
<tr>
<td>Logon Banner Title</td>
<td>Software</td>
<td>Microsoft\Windows\Current Version\Policies\System\Legal NoticeCaption</td>
<td>User-defined data.</td>
</tr>
<tr>
<td>Logon Banner Message</td>
<td>Software</td>
<td>Microsoft\Windows\Current Version\Policies\System\Legal NoticeCaption</td>
<td>User-defined data.</td>
</tr>
<tr>
<td>Time Zone</td>
<td>System</td>
<td>ControlSet001(or002)\Control\TimeZoneInformation\Standard Name</td>
<td>This information is entered during installation, but can be modified later.</td>
</tr>
</tbody>
</table>
### Networking

<table>
<thead>
<tr>
<th>Windows XP Registry Networking Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Map Network Drive MRU</strong></td>
</tr>
<tr>
<td>NTUSER.DAT</td>
</tr>
<tr>
<td>Software\Microsoft\Windows\CurrentVersion\Explorer\Map Network Drive MRU</td>
</tr>
<tr>
<td><strong>TCP/IP data</strong></td>
</tr>
<tr>
<td>System</td>
</tr>
<tr>
<td>ControlSet\XXX\Services\TCPIP\Parameters</td>
</tr>
<tr>
<td><strong>TCP/IP Settings of a Network Adapter</strong></td>
</tr>
<tr>
<td>System</td>
</tr>
<tr>
<td>ControlSet\XXX\Services\adapter\Parameters\TCPIP</td>
</tr>
<tr>
<td><strong>Default Printer</strong></td>
</tr>
<tr>
<td>NTUSER.DAT</td>
</tr>
<tr>
<td>Software\Microsoft\Windows NT\CurrentVersion\Windows</td>
</tr>
<tr>
<td><strong>Default Printer</strong></td>
</tr>
<tr>
<td>NTUSER.DAT</td>
</tr>
<tr>
<td>\printers</td>
</tr>
<tr>
<td><strong>Local Users</strong></td>
</tr>
<tr>
<td>SAM</td>
</tr>
<tr>
<td>Domains\Account\Users\Names</td>
</tr>
<tr>
<td><strong>Local Groups</strong></td>
</tr>
<tr>
<td>SAM</td>
</tr>
<tr>
<td>Domains\Builtin\Aliases\Names</td>
</tr>
<tr>
<td><strong>Profile list</strong></td>
</tr>
<tr>
<td>Software</td>
</tr>
<tr>
<td>Microsoft\Windows NT\CurrentVersion\ProfileList</td>
</tr>
<tr>
<td><strong>Network Map</strong></td>
</tr>
<tr>
<td>NTUSER.DAT</td>
</tr>
<tr>
<td>Documents and Settings\username</td>
</tr>
</tbody>
</table>

### User Data

<table>
<thead>
<tr>
<th>Windows XP Registry User Data</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Run</strong></td>
</tr>
<tr>
<td>NTUSER.DAT</td>
</tr>
<tr>
<td>Software\Microsoft\Windows\CurrentVersion\Run</td>
</tr>
<tr>
<td><strong>Media Player Recent List</strong></td>
</tr>
<tr>
<td>NTUSER.DAT</td>
</tr>
<tr>
<td>Software\Microsoft\Media Player\Player\RecentFileList</td>
</tr>
<tr>
<td><strong>O:\S Recent Docs</strong></td>
</tr>
<tr>
<td>NTUSER.DAT</td>
</tr>
<tr>
<td>Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs</td>
</tr>
<tr>
<td><strong>Run MRU</strong></td>
</tr>
<tr>
<td>NTUSER.DAT</td>
</tr>
<tr>
<td>\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU</td>
</tr>
<tr>
<td><strong>Open And Save As Dialog Boxes MRU</strong></td>
</tr>
<tr>
<td>NTUSER.DAT</td>
</tr>
<tr>
<td>\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32</td>
</tr>
<tr>
<td><strong>Current Theme</strong></td>
</tr>
<tr>
<td>NTUSER.DAT</td>
</tr>
<tr>
<td>Software\Microsoft\Windows\CurrentVersion\Themes</td>
</tr>
</tbody>
</table>
Windows XP Registry User Data (Continued)

Last Theme NTUSER.DAT
Software\Microsoft\Windows\ and CurrentVersion\Themes\Last Theme Desktop theme\wallpaper.

File Extensions\ Program Association NTUSER.DAT
Software\Microsoft\Windows\ and CurrentVersion\Explorer\ FileExts Identifies associated programs with fileextensions.

User Application Data

Windows XP Registry User Application Data

<table>
<thead>
<tr>
<th>Word User Info</th>
<th>NTUSER.DAT</th>
<th>Software\Microsoft\office\ Version\Common\UserInfo</th>
</tr>
</thead>
<tbody>
<tr>
<td>Word Recent</td>
<td>NTUSE</td>
<td>This information is entered during installation, but can be modified later.</td>
</tr>
<tr>
<td>Docs IE Typed URLs</td>
<td>R.DAT</td>
<td>Microsoft word recent documents. Data entered into the URL address bar.</td>
</tr>
<tr>
<td>IE Auto-Complete</td>
<td>R.DAT</td>
<td>Web page auto complete password-</td>
</tr>
<tr>
<td></td>
<td>NTUSE</td>
<td>Software\Microsoft\Explorer\TypedURLs</td>
</tr>
<tr>
<td></td>
<td>R.DAT</td>
<td>\Software\Microsoft\Internet Explorer \Users\username</td>
</tr>
<tr>
<td>Passwords</td>
<td>NTUSER.DAT</td>
<td>NTUSER.DAT Internet Explorer\IntelliForms</td>
</tr>
<tr>
<td>IE Auto-Complete</td>
<td>ICQ</td>
<td>\Software\Microsoft\Protected Storage System Provider</td>
</tr>
<tr>
<td>Web Addresses</td>
<td>NTUSER.DAT</td>
<td>Software\Microsoft\Internet Explorer</td>
</tr>
<tr>
<td>Outlook Temporary</td>
<td>NTUSER.DAT</td>
<td>Software\Microsoft\office\Version\Outlook\Security</td>
</tr>
<tr>
<td>AIM</td>
<td>NTUSER.DAT</td>
<td>Software\America Online\AOL Instant Messenger\CurrentVersion\Users\username</td>
</tr>
<tr>
<td>Software\Microsoft\office\version\Common\UserInfo</td>
<td>encrypted values. Lists Web pages where auto complete was used. Default download directory when utilizing Internet Explorer. Location where attachments are stored when opened from Outlook. IM contacts, file transfer information, etc. This information is entered during installation, but can be modified later. IM contacts, file transfer information, etc.</td>
<td></td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>NTUSER.DAT</td>
<td>MSN Messenger \Software\Mirabilis</td>
<td>ICQ</td>
</tr>
<tr>
<td></td>
<td>Software\Microsoft\MSN Messenger\ListCache.NET</td>
<td>IM contacts, file transfer information, etc.</td>
</tr>
<tr>
<td>Kazaa NTUSER.DAT</td>
<td>MessengerService*</td>
<td>Configuration, search, download, IM data, etc.</td>
</tr>
<tr>
<td></td>
<td>Software\Kazaa</td>
<td>*</td>
</tr>
<tr>
<td>Yahoo NTUSER.DAT</td>
<td>Software\Yahoo\Pager\Profiles</td>
<td>* etc.</td>
</tr>
<tr>
<td>Google Client</td>
<td>Software\Google\NavClient\ History NTUSER.DAT</td>
<td>Acrobat, Photo deluxe, etc.</td>
</tr>
<tr>
<td>History NTUSER.DAT</td>
<td>Software\Adobe</td>
<td>*</td>
</tr>
</tbody>
</table>
Supported File Systems and Drive Image Formats

This appendix lists the file systems and image formats that are analyzed. It includes the following topics:

- File Systems (page 647)
- Whole Disk Encrypted Products (page 648)
- Hard Disk Image Formats (page 648)
- CD and DVD Image Formats (page 649)

File Systems

The following table lists AccessData identified and analyzed file systems.

Identified and Analyzed File Systems

- APFS
- AFF4 • HFS, HFS+
- CDFS • JFS
- EFS • NTFS
- exFAT • ReiserFS 3
- Ext2FS • UFS1, UFS2
- Ext3FS • VxFS (Veritas File System)
- Ext4FS • Windows 8 and Server 2012 ReFS
- FAT 12, FAT 16, FAT 32 • XFS
- Android: Physical Images, File System Images, Android Backups (.adb) encrypted/unencrypted, UFD.
- iOS: Full File System Images.
Whole Disk Encrypted Products

The following table lists identified and analyzed Whole Disk Encryption (WDE) decryption products (these all require the investigator to enter the password, AccessData forensic products don’t “crack” these).

Recognized and Analyzed Whole Disk Encryption Formats

- APFS Encrypted  •  McAfee Drive Encryption
- Apple FileVault  •  Microsoft Windows Bitlocker
- Apple FileVault 2  •  PGP Disk®
- Checkpoint / PointSec R73 7.4.5  •  SecureDoc WinMagic AES
- Checkpoint 7.6.150 with token challenge  •  Symantec Endpoint Encryption (formerly Guardian Edge)
- Dell Encryption  •  Symantec Drive Encryption (PGP WDE)
- 10.0 (only)
- Guardian Edge  •  Utimaco Safeguard Easy
- McAfee Endpoint Encryption  •  Utimaco SafeGuard Enterprise
  (Safeboot 5.x / 6.0)
Whole Disk Encrypted Products

Hard Disk Image Formats

The following table lists identified and analyzed hard disk image formats.

**Supported Hard Disk Image Formats**

- AccessData Logical Image (AD1) • Lx0, Lx01
- AFF (Advanced Forensic Format) • LVM, LVM2
- Apple Disk Image Files (*.dmg) • LVM2
- CTR (X-Ways) • MSVHD (MS Virtual Hard Disk)
- Encase E01, including ‘incomplete’ Tab-leau- created files
  - Nero Image Files (*.nrg)
- Encase EX01 • Raw
  - Encase L01 Logical Image • Safeback 2.0 and under
- Expert Witness • SMART Image Files (*.s01)
- Ghost (forensic images only) • SnapBack
- ICS • Virtual Box Images (*.vdi)
- Image Files *.img *.ima • VMWare (*.vmdk)
- Linux DD • YAFFS Images (*.yaffs1,*.yaffs2)
  - Virtual Hard Disk (*.vhd, *.vhdx)
The following table lists identified and analyzed CD and DVD image formats.

**Supported CD and DVD Formats**

<table>
<thead>
<tr>
<th>Format</th>
<th>Tool</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alcohol (*.mds)</td>
<td>PlexTools (*.pxi)</td>
</tr>
<tr>
<td>BDAV</td>
<td>Roxio (*.cif)</td>
</tr>
<tr>
<td>CloneCD (*.ccd)</td>
<td>SACD</td>
</tr>
<tr>
<td>ISO</td>
<td>SVCD</td>
</tr>
<tr>
<td>IsoBuster CUE</td>
<td>VCD</td>
</tr>
<tr>
<td>Nero (*.nrg)</td>
<td>Virtual CD (*.vc4)</td>
</tr>
<tr>
<td>Pinnacle (*.pdi)</td>
<td>Virtual CD (*.vc4)</td>
</tr>
</tbody>
</table>
Recovering Deleted Material

You can find deleted files on supported file systems by their file header. This appendix includes the following topics:

- **FAT 12, 16, and 32** (page 650)
- **NTFS** (page 651)
- **Ext2** (page 651)
- **Ext3** (page 651)
- **HFS / HFS+** (page 651)
- **APFS** (page 651)

**FAT 12, 16, and 32**

When parsing FAT directories, deleted files are identified by their names. In a deleted file, the first character of the 8.3 filename is replaced by the hex character 0xE5.

The file’s directory entry provides the file’s starting cluster (C) and size. From the size of the file and the starting cluster, the total number of clusters (N) occupied by the file are computed.

The File Allocation Table (FAT) is examined and the number of unallocated clusters are counted, starting at C (U). The recovered file \([\min(N, U)]\) clusters starting at C are then assigned.

If the deleted file was fragmented, the recovered file is likely to be incorrect and incomplete because the information that is needed to find subsequent fragments was wiped from the FAT system when the file was deleted.

If present, the long filename (LFN) entries are used to recover the first letter of the deleted file’s short filename. If the LFN entries are incomplete or absent, it uses an exclamation mark (“!”) as the first letter of the filename.

The volume free space for deleted directories that have been orphaned are searched with a meta-carve process. An orphaned directory is a directory whose parent directory or whose entry in its parent directory has been overwritten.
The Master File Table (MFT) is examined to find files that are marked deleted because the allocation byte in a record header indicates a deleted file or folder. It then recovers the file’s data using the MFT record’s data attribute extent list if the data is non-resident.

If the deleted file’s parent directory exists, the recovered file is shown in the directory where it originally existed. Deleted files whose parent directories were deleted are shown in their proper place as long as their parent directory’s MFT entry has not been recycled.

**Ext2**

Nodes that are marked deleted are searched for. The link count is zero and the deletion timestamp is nonzero.

For each deleted inode, the block pointers are processed and blocks are added to the deleted file. However, if an indirect block is marked allocated or references an invalid block number, the recovered file is truncated at that point because the block no longer contains a list of blocks for the file that the application is attempting to recover.

The filenames for files deleted on ext2 systems are not recovered. Instead, deleted files are identified by inode number because ext2 uses variable-length directory entries organized in a linked list structure. When a file is deleted, its directory entry is unlinked from the list, and the space it occupied becomes free to be partially or completely overwritten by new directory entries. There is no reliable way to identify and extract completely deleted directory entries.

**Ext3**

Deleted files from ext3 volumes are not recovered because ext3 zeroes out a file’s indirect block pointers when it is deleted.

**HFS / HFS+**

Deleted files from HFS are not recovered by default. Selecting the Data carving or Meta carving options as part of the evidence processing profile may be able to recover deleted files from HFS and HFS+ file systems.
APFS

Deleted files in APFS file systems are able to be recovered during processing by selecting the “Meta Carve” option. It is recommended to exclude duplicates from your case as this process will likely create numerous duplicate files. The following illustration attempts to describe the relationship between the read-only and the read/write partitions on a macOS Catalina system and the APFS “firmlinks” that act similar to symbolic links, but during examination can also cause logical loops and duplicate data to be acquired.
Chapter 44
Managing Security Devices and Licenses

This appendix includes information AccessData product licenses, Virtual CodeMeter activation, Network License Server, and API Key configurations.

Installing and Managing Security Devices
AccessData products require a licensing security device that communicates with the program to verify the existence of a current license.
You must install the security device software and drivers before you can manage licenses with LicenseManager. This section explains installing and using the CodeMeter Runtime software and the License Manager.

Installing the Security Device
AccessData products require a licensing security device that communicates with the program to verify the existence of a current license. The device is a WIBU-SYSTEMS (Wibu) CodeMeter (CmStick). This USB device requires specific software to be installed prior to connecting the devices and running your AccessData products. You will need the WIBU-SYSTEMS CodeMeter Runtime software with a WIBU-SYSTEMS CodeMeter (CmStick), either the physical USB device, or the Virtual device.
Store the CmStick or dongle in a secure location when it is not in use.

Installing the CodeMeter Runtime Software
When you purchase a product, AccessData provides a USB CmStick with the product package. To use the CmStick, you must first install the CodeMeter Runtime software, either from the shipping disc or from the setup file downloaded from the AccessData Web site.

Note: The CodeMeter software is automatically installed as part of the FTK suite.
To download the CodeMeter installer from the AccessData web site
2. On the download page, click CodeMeter.
3. Click Download Page.
4. Click Download Now.
5. Save the installation file to your download directory or other temporary directory on your drive.

To install CodeMeter
1. Do one of the following:
   ■ Launch the installer from the FTK installer by doing the following:
     1a. Launch the FTK installer Autorun.exe file.
     1b. Click Other Products.
     1c. Click Install License Manager.
        ■ Launch the installer from the download by doing the following:
        1a. Navigate to, and double-click the installation file.
        2. Wait for the Preparing to Install processes to complete.
        3. In the Welcome dialog, click Next.
        4. Read and accept the License Agreement
        5. Enter User Information.
        6. Click Next.
        7. Select the features you want to install.
        8. Click Next.
        9. Click Install.
        10. Click Finish.
        11. Click OK.

CodeMeter Error
If you are not using NLS for your security device configuration, after clicking No, you will see the following additional message.

Security Device Not Found
To remedy, click OK, then install the correct CodeMeter Runtime software, and connect the
CmStick or run License Manager to generate your Virtual CmStick. Then, restart FTK.
Installing LicenseManager

LicenseManager lets you manage product and license subscriptions using a security device or device packet file.

You can access the LicenseManager installer from the Web or from the FTK installer.

**To download the LicenseManager installer from the AccessData web site**

2. On the download page, click **LicenseManager**.
3. Click **Download Page**.
4. Click **Download Now**.
5. Save the installation file to your download directory or other temporary directory on your drive.

**To install LicenseManager**

1. Do one of the following:
   - Launch the installer from the FTK installer by doing the following:
     1a. Launch the FTK installer Autorun.exe file.
     1b. Click **Other Products**.
   1c. Click Install License Manager.
     - Launch the installer from the download by doing the following:
     1a. Navigate to, and double-click the installation file.
   2. Wait for the *Preparing to Install* processes to complete.
   3. Click **Next** on the Welcome screen
   4. Read and accept the License Agreement.
   5. Click **Next**.
   6. Accept the default destination folder, or select a different one.
   7. Click **Next**.
   8. In the Ready to Install the Program dialog, click **Back** to review or change any of the installation settings. When you are ready to continue, click **Install**.
   9. Wait while the installation completes.
   10. If you want to launch LicenseManager after completing the installation, mark the **Launch AccessData LicenseManager** check box.
11. Select the **Launch AccessData LicenseManager** check box to run the program upon finishing the setup. The next section describes how to run LicenseManager later.

12. Click **Finish** to finalize the installation and close the wizard.
To launch LicenseManager

1. Launch LicenseManager by clicking the LicenseManager icon on your desktop.

When starting, LicenseManager reads licensing and subscription information from the installed and connected WIBU-SYSTEMS CodeMeter Stick, or Keylok dongle.

**Note:** If using a Keylok dongle, and LicenseManager either does not open or displays the message, “Device Not Found”

2. Verify the correct dongle driver is installed on your computer.
3. With the dongle connected, check in Windows Device Manager to make sure the device is recognized. If it has an error indicator, right click on the device and choose Uninstall.
4. Remove the dongle after the device has been uninstalled.
5. Reboot your computer.
6. After the reboot is complete, and all startup processes have finished running, connect the dongle.
7. Wait for Windows to run the Add New Hardware wizard. If you already have the right dongle drivers installed, do not browse the internet, choose, “No, not this time.”
8. Click Next to continue.
9. On the next options screen, choose, “Install the software automatically (Recommended)
10. Click Next to continue.
11. When the installation of the dongle device is complete, click Finish to close the wizard.
12. You still need the CodeMeter software installed, but will not need a CodeMeter Stick to run LicenseManager.

**Note:** If using a CodeMeter Stick, and LicenseManager either does not open or displays the message, “Device Not Found”

13. Make sure the CodeMeter Runtime 4.20b software is installed. It is available at www.accessdata.com/support. Click Downloads and browse to the product. Click on the download link. You can Run the product from the Website, or Save the file locally and run it from your PC. Once the CodeMeter Runtime software is installed and running, you will see a gray icon in your system tray.
License Management Options (Continued)

14. Make sure the CodeMeter Stick is connected to the USB port.

If the CodeMeter Stick is not connected, LicenseManager still lets you to manage licenses using a security device packet file if you have exported and saved the file previously.

To open LicenseManager without a CodeMeter Stick installed

1. Click Tools > LicenseManager.

LicenseManager displays the message, “Device not Found”.

2. Click OK, then browse for a security device packet file to open.

Note: Although you can run LicenseManager using a packet file, AccessData products will not run with a packet file alone. You must have the CmStick or dongle connected to the computer to run AccessData productsthat require a license.

LicenseManager provides the tools necessary for managing AccessData product licenses on a WIBU- SYSTEMS CodeMeter Stick security device, a Keylok dongle, a Virtual Dongle, or in a security device packet file.

LicenseManager displays license information, allows you to add licenses to or remove existing licenses from a dongle or CmStick. LicenseManager, and can also be used to export a security device packet file. Packet files can be saved and reloaded into LicenseManager, or sent via email to AccessData support.

In addition, you can use LicenseManager to check for product updates and in some cases download the latest product versions.

LicenseManager displays CodeMeter Stick information (including packet version and serial number) and licensing information for all AccessData products. The Purchase Licenses button connects directly to the AccessData website and allows you to browse the site for information about products you may wish to purchase. Contact AccessData by phone to speak with a Sales Representative for answers to product questions, and to purchase products and renew licenses and subscriptions.

The LicenseManager Interface

The LicenseManager interface consists of two tabs that organize the options in the LicenseManager window: the Installed Components tab and the Licenses tab.
License Management Options (Continued)

The Installed Components Tab

The Installed Components tab lists the AccessData programs installed on the machine. The InstalledComponents tab is displayed in the following figure.

The following information is displayed on the Installed Components tab:

**LicenseManager Installed Components Tab Features**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Program</td>
<td>Lists all AccessData products installed on the host.</td>
</tr>
<tr>
<td>Installed Version</td>
<td>Displays the version of each AccessData product installed on the host.</td>
</tr>
<tr>
<td>Newest Version</td>
<td>Displays the latest version available of each AccessData product installed on the host.</td>
</tr>
</tbody>
</table>

Click **Newest** to refresh this list.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product Notes</td>
<td>Displays notes and information about the product selected in the program list.</td>
</tr>
<tr>
<td>AccessData Link</td>
<td>Links to the AccessData product page where you can learn more about AccessData products.</td>
</tr>
</tbody>
</table>

The following buttons provide additional functionality from the Installed Components tab:

**LicenseManager Installed Components Buttons**

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Help</td>
<td>Opens the LicenseManager Help web page.</td>
</tr>
<tr>
<td>Install Newest</td>
<td>Installs the newest version of the programs checked in the product window, if that program is available for download. You can also get the latest versions from our website using your Internet browser.</td>
</tr>
<tr>
<td>Newest</td>
<td>Updates the latest version information for your installed products.</td>
</tr>
<tr>
<td>About</td>
<td>Displays the About LicenseManager screen. Provides version, copyright, and trademark information for LicenseManager.</td>
</tr>
<tr>
<td>Done</td>
<td>Closes LicenseManager.</td>
</tr>
</tbody>
</table>
License Management Options (Continued)

Use the Installed Components tab to manage your AccessData products and stay up to date on new releases.
License Management Options (Continued)

The Licenses Tab

The Licenses tab displays CodeMeter Stick information for the current security device packet file and licensing information for AccessData products available to the owner of the CodeMeter Stick, as displayed in the following figure.

The Licenses tab provides the following information:

**LicenseManager Licenses Tab Features**

<table>
<thead>
<tr>
<th>Program</th>
<th>Shows the owned licenses for AccessData products.</th>
<th>Expiration Date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Shows the date on which your current license expires.</td>
<td>Status Shows these status of that product's license:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>None</strong>: the product license is not currently owned</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Days Left</strong>: displays when less than 31 days remain on the license.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Never</strong>: the license is permanently owned. This generally applies to Hash Tables and Portable Office Rainbow Tables.</td>
</tr>
<tr>
<td></td>
<td>Name Shows the name of additional parameters or information a product requires for its license.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Value Shows the values of additional parameters or information a product contained in or required for its license.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Show Unlicensed When checked, the License window displays all products, whether licensed or not.</td>
<td></td>
</tr>
</tbody>
</table>

The following license management actions can be performed using buttons found on the License tab:
License Management Options (Continued)

License Management Options

Remove License  Removes a selected license from the Licenses window and from the CodeMeter Stick or dongle. Opens the AccessData License Server web page to confirm success.

Refresh Device  Connects to the AccessData License Server. Downloads and overwrites the info on the CodeMeter Stick or dongle with the latest information on the server. Reload from Device Begins or restarts the service to read the licenses stored on the CodeMeter Stick or dongle.

Release Device  Click to stop the program reading the dongle attached to your machine, much like Windows' Safely Remove Hardware feature. Click this button before removing a dongle. This option is disabled for the CodeMeter Stick.

Open Packet File  Opens Windows Explorer, allowing you to navigate to a .PKT file containing your license information.

Save to File  Opens Windows Explorer, allowing you to save a .PKT file containing your license information. The default location is My Documents.

Finalize Removal  Finishes the removal of licenses in the unbound state. Licenses must be unbound from the CmStick or dongle before this button takes effect.
View RegistrationInfo
Displays an HTML page with your CodeMeter Stick number and other license information.

Add Existing License Allows you to bind an existing unbound license to your CodeMeter Stick, through an internet connection to the AccessData License Server.

Purchase License Brings up the AccessData product page from which you can learn more about AccessData products.

About Displays the About LicenseManager screen. Provides version, copyright, and trademark information for LicenseManager.

Done Closes LicenseManager.

Opening and Saving Dongle Packet Files
You can open or save dongle packet files using LicenseManager. When started, LicenseManager attempts to read licensing and subscription information from the dongle. If you do not have a dongle installed, LicenseManager lets you browse to open a dongle packet file. You must have already created and saved a dongle packet file to be able to browse to and open it.

To save a security device packet file
1. Click the Licenses tab, then under License Packets, click Save to File.
2. Browse to the desired folder and accept the default name of the .PKT file; then click Save.

Note: In general, the best place to save the .PKT files is in the AccessData LicenseManager folder. The default path is C:\Program Files\AccessData\Common Files\AccessData LicenseManager\.

To open a security device packet file
1. Select the Licenses tab.
2. Under License Packets, click Open Packet File.
3. Browse for a dongle packet file to open. Select the file and click Open.
Adding and Removing Product Licenses

On a computer with an Internet connection, LicenseManager lets you add available product licenses to, or remove them from, a dongle.

To move a product license from one dongle to another dongle, first remove the product license from the first dongle. You must release that dongle, and connect the second dongle before continuing. When the second dongle is connected and recognized by Windows and LicenseManager, click on the Licenses tab to add the product license to the second dongle.

Removing a License

To remove (unassociate, or unbind) a product license

1. From the Licenses tab, mark the program license to remove.

This action activates the Remove License button below the Program list box.

2. Click Remove License to connect your machine to the AccessData License Server through the internet.

3. When you are prompted to confirm the removal of the selected licenses from the device, click Yes to continue, or No to cancel.

4. Several screens appear indicating the connection and activity on the License Server, and when the license removal is complete, the following screen appears.

5. Click OK to close the message box.

Another internet browser screen appears from LicenseManager with a message that says, “The removal of your licenses from Security Device was successful!” You may close this box at any time.
Adding a License

To add a new or released license

1. From the Licenses tab, under Browser Options, click **Add Existing License**.

The AccessData LicenseManager Web page opens, listing the licenses currently bound to the connected security device, and below that list, you will see the licenses that currently are not bound to any security device. Mark the box in the Bind column for the product you wish to add to the connected device, then click **Submit**.

2. An AccessData LicenseManager Web page will open, displaying the following message, “The AccessData products that you selected has been bound to the record for Security Device nnnnnnnn within the Security Device Database.

“Please run LicenseManager’s “Refresh Device” feature in order to complete the process of binding these product licenses to this Security Device.” You may close this window at any time.

3. Click **Yes** if LicenseManager prompts, “Were you able to associate a new product with this device?”

4. Click **Refresh Device** in the Licenses tab of LicenseManager. Click Yes when prompted. You will see the newly added license in the License Options list.

Adding and Removing Product Licenses Remotely

While LicenseManager requires an Internet connection to use some features, you can add or remove licenses from a dongle packet file for a dongle that resides on a computer, such as a forensic lab computer, that does not have an Internet connection.

If you cannot connect to the Internet, the easiest way to move licenses from one dongle to another is to physically move the dongle to a computer with an Internet connection, add or remove product licenses as necessary using LicenseManager, and then physically move the dongle back to the original computer. However,
if you cannot move the dongle—due to organization policies or a need for forensic soundness—then transfer the packet files and update files remotely.

Adding a License Remotely

To remotely add (associate or bind) a product license
1. On the computer where the security device resides:
   1a. Run LicenseManager.
   1b. From the Licenses tab, click **Reload from Device** to read the dongle license information.
   1c. Click **Save to File** to save the dongle packet file to the local machine.
2. Copy the dongle packet file to a computer with an Internet connection.
3. On the computer with an Internet connection:
   3a. Remove any attached security device.
   3b. Launch LicenseManager. You will see a notification, “No security device found”.
   3c. Click OK.
   3d. An “Open” dialog box will display. Highlight the .PKT file, and click **Open**.
   3e. Click on the Licenses tab.
   3f. Click **Add Existing License**.
3g. Complete the process to add a product license on the Website page.
3h. Click **Yes** when the LicenseManager prompts, “Were you able to associate a new product with this dongle?”
   3i. When LicenseManager does not detect a dongle or the serial number of the dongle does not match the serial number in the dongle packet file, you are prompted to save the update file, [serial#].wibuCmRaU.
   3j. Save the update file to the local machine.
4. After the update file is downloaded, copy the update file to the computer where the dongle resides:
5. On the computer where the dongle resides:
   5a. Run the update file by double-clicking it. ([serial#].wibuCmRaU is an executable file.)
   5b. After an update file downloads and installs, click **OK**.
5c. Run LicenseManager.
   5d. From the Licenses tab, click **Reload from Device** to verify the product license has been added to the dongle.
Removing a License Remotely

To remotely remove (unassociate, or unbind) a product license
1. On the computer where the dongle resides:

1a. Run LicenseManager.
   1b. From the Licenses tab, click **Reload from Device** to read the dongle license information.
   1c. Click **Save to File** to save the dongle packet file to the local machine.
2. Copy the file to a computer with an Internet connection.
3. On the computer with an Internet connection:

3a. Launch LicenseManager. You will see a notification, “No security device found”.
   3b. Click **OK**.
   3c. An “Open” dialog box will display. Highlight the .PKT file, and click **Open**.
   3d. Click on the Licenses tab.
   3e. Mark the box for the product license you want to unassociate; then click **Remove License**.
   3f. When prompted to confirm the removal of the selected license from the dongle, click **Yes**. 3g. When LicenseManager does not detect a dongle or the serial number of the dongle does not match the serial number in the dongle packet file, you are prompted save the update file.
   3h. Click **Yes** to save the update file to the local computer.
   3i. The Step 1 of 2 dialog details how to use the dongle packet file to remove the license from a dongle on another computer.
   3j. Save the update file to the local machine.
4. After the update file is downloaded, copy the update file to the computer where the dongle resides.
5. On the computer where the dongle resides:

5a. Run the update file by double-clicking it. This runs the executable update file and copies the new information to the security device.
   5b. Run LicenseManager
   5c. On the Licenses tab, click **Reload from Device** in LicenseManager to read the security device and allow you to verify the product license is removed from the dongle.
   5d. Click **Save to File** to save the updated dongle packet file to the local machine.
6. Copy the file to a computer with an Internet connection.
**Updating Products**

You can use LicenseManager to check for product updates and download the latest product versions.

Checking for Product Updates

To check for product updates, on the Installed Components tab, click **Newest**. This refreshes the list to display what version you have installed, and the newest version available.

Downloading Product Updates

To install the newest version, mark the box next to the product to install, then click **Install Newest**.

---

**Note:** Some products are too large to download, and are not available. A notification displays if this is the case.

---

**To download a product update**

1. Ensure that LicenseManager displays the latest product information by clicking the Installed Components tab. Click **Newest** to refresh the list showing the latest releases, then compare your installed version to the latest release.

2. If the latest release is newer than your installed version, you may be able to install the latest release from our Website.

3. Ensure that the program you want to install is not running.

4. Mark the box next to the program you want to download; then click **Install Newest**.

5. When prompted, click **Yes** to download the latest install version of the product.

4a. If installing the update on a remote computer, copy the product update file to another computer.

5. Install the product update. You may need to restart your computer after the update is installed.
Purchasing Product Licenses

Use LicenseManager to link to the AccessData Web site to find information about all our products.

Purchase product licenses through your AccessData Sales Representative. Call 801-377-5410 and follow the prompt for Sales, or send an email to sales@accessdata.com.

Note: Once a product has been purchased and appears in the AccessData License Server, add the product license to a CodeMeter Stick, dongle, or security device packet file by clicking **Refresh Device**.

Sending a Dongle Packet File to Support

Send a security device packet file **only** when specifically directed to do so by AccessData support.

To create a dongle packet file

1. Run LicenseManager
2. Click on the Licenses tab.
3. Click Load from Device.
4. Click **Refresh Device** if you need to get the latest info from AD’s license server.
5. Click **Save to File**, and note or specify the location for the saved file.
6. Attach the dongle packet file to an e-mail and send it to:

   support@accessdata.com.
Virtual CodeMeter Activation Guide

Introduction
A Virtual CodeMeter (VCM) allows the user to run licensed AccessData products without a physical CodeMeter device. A VCM can be created using AccessData License Manager, but requires the user to enter a Confirmation Code during the creation process.

The latest revision of this guide can be found at: http://accessdata.com/downloads/media/VCM_Activation_Guide.pdf

Preparation
● Contact your AccessData sales rep to order a VCM confirmation code.
● Install CodeMeter Runtime 4.10b or newer (available on the AccessData download page).
● Install the latest release of License Manager (available on the AccessData download page).
● The following steps are to be run on the system where you want to permanently attach the VCM.

Note: Once created, the VCM cannot be moved to any other system.

Setup for Online Systems

To setup a Virtual CodeMeter
1. Unplug any AccessData dongles you currently have connected.
2. Launch License Manager.


3. Select Create A Local Virtual CMStick
4. Click OK.

The Confirmation Code Required dialog appears.
5. Enter your confirmation code.
6. Click OK, AccessData License Manager will automatically synchronize with the License Server over the Internet.
7. Click OK when the update completes. License Manager will then create the VCM on your system.
8. At this point, AccessData License Manager now displays a serial number for the VCM on the Licenses tab and the VCM can now operate in a similar way to a hardware CodeMeter device.
Setting up VCM for Offline Systems

You can setup a Virtual CodeMeter on a system that is not connected to the internet (offline). You must also have one machine that connects to the internet to perform certain steps. This section details what to do on which machine.

Perform these steps on the Online system
1. Unplug any AccessData dongles you currently have connected.
2. Launch License Manager.


3. Select Create Empty Virtual CMStick (offline).
4. Click OK.
5. The resulting dialog prompts you to save the *.wibucmrau file. Enter a name and path for the file, then click Save.
6. Transfer the *.wibucmrau to the Online system.

Perform these steps on the Online system
7. Unplug any AccessData dongles you currently have connected.
8. Launch License Manager.
9. Select Create Activation File (online).
10. Click OK.
11. In the Confirmation Code Required dialog, enter your confirmation code and click OK.
12. AccessData License Manager will automatically synchronize with the License Server over the internet. Data synchronized from the server will be written to the *.wibucmrau file. Click OK when the update completes.
13. Transfer *.wibucmrau back to the offline system.

Perform these steps on the Offline system
14. Unplug any AccessData dongles you currently have connected.
15. Launch License Manager.

16. Select Create Activate Virtual CMStick (offline).
17. Click OK.
18. The resulting dialog prompts you to browse to the location of the newly updated *.wibucmrau file. Locate the file, then click **Open**. License Manager creates the VCM on your system.

19. At this point, AccessData License Manager should now display a serial number for the VCM on the “Licenses” tab and the VCM can now operate in a similar way to a hardware CodeMeter device.

---

**Creating a Virtual CM-Stick with Server 2003/2008 Enterprise Editions**

This section contains special instructions for using a VCM with Windows Server 2003 or 2008 EnterpriseEditions. Complete each section in order.

**To Create an Empty CodeMeter License Container**

2. Open the CodeMeter Control Center. Make sure the window on the License tab is, empty indicating that no licenses are currently loaded.
3. Select File > Import License.
4. Browse to the License Manager program files directory.
   - 32 bit systems: C:\Program Files\AccessData\LicenseManager\**
   - 64 bit systems: C:\Program Files (x86)\ AccessData\LicenseManager\**
5. Highlight the TemplateDisc5010.wbb file, then click **Import**.
6. Click the **Activate License** button.
7. When the CmFAS Assistant opens, click **Next**.
8. Select Create license request, and click Next.
9. Confirm the desired directory and filename to save.WibuCmRaC. (Example: Test1.WibuCmRaC)
10. Click **Commit**.
11. Click **Finish**.

**To Copy to another machine**

1. Copy the new.WibuCmRaC to another machine that is not running Windows Server 2003/2008Enterprise.

---

**Note:** The destination system must have an active internet connection.
2. Unplug any AccessData dongles you currently have connected.
3. Launch License Manager.
4. Select Create Activation File (online).
5. Click OK.
6. In the Confirmation Code Required dialog enter your confirmation code and click OK.
7. AccessData License Manager will automatically synchronize with the License Server over the internet.
   Data synchronized from the server will be written to the *.wibucmrau file. Click OK when the update completes.

**To Finish the activation on the Windows Server 2003/2008 Enterprise system**
3. Open the CodeMeter Control Center. Make sure the window on the License tab empty indicating that no licenses are currently loaded.
4. Select File > Import License.
5. Browse to the location where the activated .WibuCmRaC is stored. Click Import.
6. AccessData License Manager now displays a serial number for the VCM on the Licenses tab and the VCM can now operate in a similar way to a hardware CodeMeter device.

**Virtual CodeMeter FAQs**
Q: How do I get a Virtual CodeMeter (VCM)?
A: Contact your AccessData product sales representative. They will provide you with a VCM confirmation code.

Q: How do VCMs work?
A: A VCM operates in almost exactly the same way as a hardware CodeMeter device, except that they exist as a file stored on the hard disk. During activation, the VCM file (named with a WBB extension) is tied to the hardware of the system using unique hardware identifiers. Those unique identifiers make VCMs non-portable. When AccessData License Manager is launched, it will automatically load the VCM and display its license information. From there, you can refresh,
remove, add existing licenses, etc just the same you would with a hardware security device.

Q: Are VCMs supported on virtual machines (VM)?
A: No. Due to the fact that virtual machines are portable and VCMs are not, VCMs are not supported on virtual machines. Currently it is recommended to use AccessData Network License Service (NLS) to license systems running as virtual machines. CLICK HERE for more information.

Q: Does the AccessData Network License Service (NLS) support VCMs?
A: The current release of NLS does not support using VCM as a network dongle. AccessData is considering this support for a future release.

Q: How can I “unplug” a VCM?
A: If you want to prevent License Manager from automatically loading the VCM you can "unplug" it by stopping the CodeMeter Runtime Service server and then moving (cut and paste) the WBB file to a new location (renaming the file does not suffice). By default the WBB file is located at:

32 bit systems:
C:\Program Files\CodeMeter\CmAct\n
64 bit systems:
C:\Program Files (x86)\CodeMeter\CmAct\n
Q: I have activated a VCM on my system, but now I need to activate it on a different system. What should I do?
A: Since a VCM is uniquely tied to the system on which it is activated, it cannot be moved to any other system. If you need to activate a VCM on a different system, you need to contact your AccessData Sales Representative.

Q: What if I need to reinstall Windows, format my drive, change my system’s hardware, or back up my VCM in case of a disaster? Will the VCM still work?
A: The VCM can be backed up by simply copying the WBB file to a safe location. It can be restored by copying the WBB file to the CmAct folder. The VCM cannot be restored without a WBB file. If you do not have a backup of your WBB file, you will need to get a new confirmation code from your AccessData Sales Representative.
Q: My AccessData product does not seem to recognize the license stored on a VCM. What am I doing wrong?

A: VCMs are supported by the following versions of AccessData products:
   - FTK 1.81.6 and newer
   - FTK 3.1.0 and newer
   - PRTK 6.5.0 and newer
   - DNA 3.5.0 and newer
   - RV 1.6.0 and newer
   - eDiscovery 3.1.2 and newer
   - AD Lab 3.1.2 and newer
   - AD Enterprise 3.1.0 and newer
   - MPE+ 4.0.0.1 and newer

Ensure that the version of the product you are running support VCMs. If the version you are running is listed as supported, verify that according to License Manager, the release date of the version you are running falls before the expiration date of the license.
Network License Server (NLS) Setup Guide

Introduction
This section discusses the installation steps and configuration notes needed to successfully setup an AccessData Network License Server (NLS).

Note: Click on this link to access the latest version of this guide: Network License Server (NLS) Setup Guide

Preparation Notes
- CodeMeter Runtime 3.30a or newer must be installed on all Client and Server systems
- AccessData License Manager must be used to prepare the network dongle. The system running License Manager must have internet access and have CodeMeter Runtime installed.

Setup Overview

To setup NLS
1. Download the latest release of NLS located in the utilities section of the AccessData download page.
2. Extract contents of ZIP to a folder of your choice.
3. On the NLS server system, run through the NLS Installation MSI and accept all defaults.
4. Prepare network dongle:
   4a. Provide the serial number to AD Support and request to have the “Network Dongle Flag” applied.
   4b. Migrate any additional licenses to the network dongle
   4c. Refresh the network dongle device using AccessData License Manager.
4. Prepare network dongle:
5. Launch the AccessData product on the NLS client system.
6. Enter the NLS server configuration information:
   - IP address or hostname of NLS server system
   - Port 6921
7. Click, OK.

If you encounter any problems, please read the notes below for troubleshooting information.
**Network Dongle Notes**

- AccessData License Manager 2.2.6 or newer should be installed in order to manage licenses on the network dongle.
- Network dongles can hold up to 120 physical licenses. Each License has a capacity to hold thousands of sub licenses (i.e. Client count or worker count).
- Contact AccessData Technical Support to have your CodeMeter device flagged as a Network Dongle (required for NLS).

**NLS Server System Notes**

- Make sure the CodeMeter device is flagged as Network Dongle (i.e. License Manager will show the serial as “1181234N”. To have this flag set on your CodeMeter device, please contact AccessData Technical Support).
- Server system must be configured to allow incoming and outgoing traffic on TCP port 6921.
- A web interface to view and revoke licenses all licenses is accessible at
  
  http://localhost:5555

  This page can be reached only from a web browser running locally on the NLS server system.
- A Network Dongle cannot be used to run AccessData products locally unless the NLS server is running locally.
- Some versions of Windows may not find a local NLS server when the DNS hostname of the server is provided. In those cases, it is recommended to use a static IP address.
- When using the NLS across domains, users must have permissions to access resources on both domains (either by dual-domain membership or cross-domain trust).
- When running NLS on Windows Server 2008, Terminal Services must be installed and accepting connections. If Terminal Services is not configured it will not open the port and share out the licenses correctly.
- The name of the service according to Windows is “AccessData Network License Service.”
**NLS Client System Notes**

- When launched, any NLS client application that needs to lease a license from the NLS server will automatically check for the following values within the Windows Registry.
  
  - **NetDonglePath**: The IP address or DNS hostname of the system hosting the Network License Server service which is found in the following registry key on the client system:
    
    HKEY_LOCAL_MACHINE\SOFTWARE\AccessData\Products\Common
  
  - **NetDonglePort**: The TCP port number through which the client and server systems have been configured to use. This value is located in the same key as NetDonglePath.
  
  - **uniqeild**: In order to lease a license from the server, the client system must first possess a unique identification value. This value is automatically generated by applications such as FTK, PRTK, or DNA. (Registry Viewer and FTK 1.x cannot be used setup initial client NLS configuration at this time.)

You can find the each client system’s uniqeild by inspecting the following registry key:

HKEY_LOCAL_MACHINE\SOFTWARE\AccessData\Shared

- The Client system must be configured to allow all incoming and outgoing traffic on TCP port 6921.

- The following products support the ability to lease a license from a NLS server:
  
  - FTK 2.2.1 and newer
  - FTK 1.81.2 and newer
  - FTK Pro 3.2 and newer
  - PRTK 6.4.2 and newer
  - DNA 3.4.2 and newer
  - Registry Viewer 1.5.4 and newer
  - AD Enterprise 3.0.3 and newer
  - AD Lab 3.0.4 and newer
  - AD Lab Lite 3.1.2 and previous
  - Mobile Phone Examiner 3.0 and newer
  - Explicit Image Detection (EID) Add-on
  - Glyph Add-on

- Use AccessData License Manager (ver. 2.2.4 or newer) to migrate licenses off other devices and onto a network device.

- When running AccessData products on Windows Vista, 7, or Server 2008 you must choose **Run as administrator** at least once in order to lease a license from a NLS server.
- If the NLS client application is having trouble leasing a license either from the NLS server, AccessData recommends that you reset the licensing configuration to default.
- To reset the licensing configuration, delete and recreate the NLS registry key located at:

  HKEY_LOCAL_MACHINE\SOFTWARE\AccessData\Products\Common
About API Key Generation

To generate an API authentication key, your CodeMeter License dongle must have the ADAPI sub-license (with current expiration date) applied as a license attribute of your AD FTK / Lab / Enterprise license. As long as this dongle is plugged into the machine when you launch the FTK.exe program, you will be able to generate API keys through the application. Typically you will want to bind this key to the application administrator account so that the API key has access to all of the REST API calls.
How to generate an API key

1. Insert the CodeMeter licensed for ADAPI to the Examiner system.
2. Launch FTK / Lab / Enterprise
3. In the Case Management interface, select the Access API Key option from the Tools menu.
4. In the Access Api Key Manager window, select the user account for whom you wish to generate an API key.

![Access Api Key Manager](image)

**Note:** Appropriate API related permissions will be granted to the selected user account once the API key is generated.

5. Click the Generate Key button.
6. The generated API key will populate in the key field.
Chapter 45
Manually Installing the Windows Agent

This chapter covers the manual installation of the agent in a Windows environment. This chapter includes the following topics:

- See Agent Certificate Requirements on page 674.
- See Manually Installing the Windows Agent on page 674.
- See Controlling Consumption of the CPU on page 679.
- See Important Information on page 679.

Agent Certificate Requirements
The certificates used by agent and site server can use either the SHA-1 or SHA-256 hashing algorithm. These do not require any “Key Usage” or other special fields.

Manually Installing the Windows Agent
Perform the following steps to manually install the Enterprise Agent in Windows:

- Specific Instructions for eDiscovery (page 674)
- Specific Instructions for Forensics Products (page 674)
- Manually Installing the Agent (page 675)
- Configuring Execname and Servicename Values (page 677)

Specific Instructions for eDiscovery
Follow these instructions if installing the Windows agent for use in eDiscovery: Using Agent Certs (page 567)
See Manually Installing the Agent on page 675.

Specific Instructions for Forensics Products
Follow these instructions if installing the Windows agent for use in FTK, AD Lab, or AD Enterprise:

Using Agent Certs in Forensics Products (page 680) See Manually Installing the Agent on page 675.
Manually Installing the Agent

To manually install the Agent

1. Run AccessDataAgent.msi or AccessDataAgent(64bit) using msiexec.

Note: These .msi files are located in the Program Files\AccessData\Forensic Toolkit\5.1\Bin\Agent\<x32 or x64> folder after installation.

There are several command line parameters available to use with this .msi as documented below. Here is an example command line that will install with the defaults:

If AccessDataAgent.msi resides in the folder C:\enterprise and ManagementServer.crt resides in [Drive]\certificates, type the following command line to install the agent with defaults:

msiexec /i [Drive]:\enterprise\AccessDataAgent.msi
CER=[Drive]\certificates\ManagementServer.crt.

The following table lists the command line options available for use with this AccessDataAgent.msi:

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>/i (i or x required)</td>
<td>Specifies install.</td>
</tr>
<tr>
<td>/x (i or x required)</td>
<td>Specifies un-install.</td>
</tr>
<tr>
<td>/qn (optional)</td>
<td>Allows you to install in quiet mode with no user interaction.</td>
</tr>
<tr>
<td>&lt;path and msi file name&gt; (required)</td>
<td>If running from the folder where the .msi is located you do not have to include path, only the filename.</td>
</tr>
<tr>
<td>CER=&lt;path and certificate file name&gt; (required)</td>
<td>Specifies the certificate the agent uses. Always include the path, regardless of location.</td>
</tr>
<tr>
<td>ALLUSERS=&lt;n&gt;</td>
<td>Configures the installer to be available to all users. The default option varies per operating system. The options are: allusers=1 configures the installer to be available to all users. allusers=0 configures the installer to be available to only the user who is installing the agent.</td>
</tr>
<tr>
<td>INSTALLDIR=&lt;custom install path&gt; (optional)</td>
<td>Allows you to change the install location from the default folder: (C:\Program Files\AccessData\Agent).</td>
</tr>
<tr>
<td>PORT=&lt;xxxx&gt; (optional)</td>
<td>Allows you to change the port from the default port (3999).</td>
</tr>
<tr>
<td>LIFETIME=$&lt;$d$&gt;$ (optional)</td>
<td>Allows you to configure the life cycle of the agent. The “$d$” value equals the Time To Live (TTL) measured in days. Adding a number preceded by a dash measures the TTL in minutes. For example: $&lt;$-$d$ $&gt;$.</td>
</tr>
</tbody>
</table>
## Command Line Options (Continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>CONN=&lt;n&gt;</td>
<td>Allows you to configure the number of maximum connections for the agent.</td>
</tr>
<tr>
<td>STORESIZE=&lt;n&gt;</td>
<td>Allows you to configure the size of the data store.</td>
</tr>
<tr>
<td>TRANSIENT=1</td>
<td>Allows you to configure the agent as a <em>Transient Agent</em>. Transient Agents have no protected storage and remove themselves when the agent machine is restarted.</td>
</tr>
<tr>
<td>FOLDER_STORAGE=1</td>
<td>Allows you to configure the agent as a <em>Persistent Agent</em>. Persistent Agents use a “local” file system based storage and not protected storage. Persistent Agents also remain on the agent machine after the machine is restarted. This allows for local logical disc space to store the results of Public Site Server jobs operating while the Agent is not on the WAN or can get to the Public Site Server.</td>
</tr>
<tr>
<td>SERVICELESS=1</td>
<td>Allows you to configure the agent to install with no protected storage and no installed service. The agent removes itself when the agent machine restarts or when the lifetime option expires, whichever comes first.</td>
</tr>
<tr>
<td>MAMA=&lt;Site Server IP address:port&gt;</td>
<td>Allows you to configure the IP Address of the Site Server to which the agent reports. For example, 10.32.41.113:54545 This parameter is used so that the Agents know which Site Server to check into for the first time. Additionally, after that first check-in, the Agents will learn the Site Servers that has its CIDR and check there next time. It will update based on movement of the physical IP of the node.</td>
</tr>
</tbody>
</table>
Command Line Options (Continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PUBSS=&lt;public instance IP&gt;</td>
<td>Allows you to configure the agent to connect to a Public Site Server (PUBSS). See About Site Servers on page 562. For example, pubss=192.192.192.192:5432. The Agent in Public Site Server (PUBSS) mode will check-in to the original PUBSS value that was part of the install. After that first check-in, it will receive a list of other Public Site Servers in the DMZ and then ping around to find the closest/fastest connection. For example, if the user is in New York and a job starts there, and then the user goes to Los Angeles, the user will go from the NYC PUBSS to the LA PUBSS and the collection should resume and support interruption. This is all completed based on the resolution of the IP address for the target and assignment in a proper CIDR range on Site Server config. See Site Server Configuration on page 565. This list will also get updated whenever it might change. This list comes from the Site Server configuration parameters you setup on your internal servers and not specifically some additional data entry. It comes from the virtue of having any Public Site Servers deployed. See MAMA=&lt;Site Server IP address:port&gt; on page 676.</td>
</tr>
<tr>
<td>PUBSS_DELAY=&lt;seconds&gt;</td>
<td><em>eDiscovery Only:</em> This can be used to delay the default check-in interval (30 minutes). You may want to alter this value if you have a lot of Agents on the PUBSS system.</td>
</tr>
</tbody>
</table>

Example Command Line Install

msiexec /i "C:\AgentInstall\AccessData Agent (64-bit).msi" cer="C:\AgentInstall\AccessData E1.crt" mama=10.10.35.32:54545 TRANSIENT=1 Persistent=1 Serviceless=1 lifetime=1 or lifetime=-5 pubss=192.192.192.192 5432

Configuring Execname and Servicename Values

The Execname and Servicename values change the names of the agent executable and agent service respectively. These values are added to the MSI using an MSI editor (such as ORCA.exe — a free MSI editor).
Command Line Options (Continued)

Changing the Execname Value

To make changes to the execname value
1. Run Orca.EXE.
2. Click File > Open.
3. Browse to the folder containing the “AccessData Agent.msi” or “AccessData Agent (64-bit).msi” file and open the file. The default path is:

   \[Drive]\Program Files\AccessData\Forensic Toolkit\3.2\Bin\Agent\x32 (or x64)\n
4. In the Tables list, select File...
5. In the FileName column, double-click “u4jwdc7h.exe|agentcore.exe”.

5a. Enter the filename to use for the agent core executable.

   Note: Replace the entire string with the filename.
6. Press Enter.
7. Click File > Save.

   Note: Do not close Orca if you are also changing the service name.
Changing the Servicename Value

**To make changes to the Servicename value**

*If you closed Orca, begin with Step 1. Otherwise, skip to Step 4.*

1. Run Orca.EXE.
2. Click File > Open.
3. Browse to the folder containing the “AccessData Agent.msi” or “AccessData Agent (64-bit).msi” file and open the file. The default path is:

   \[Drive]\Program Files\AccessData\Forensic Toolkit\3.2\Bin\Agent\x32 (or x64)\n
4. In the *Tables* list, select “ServiceControl”.
5. In the *Name* column, double-click “AgentService”.

   5a. Enter the name to use for the AgentService and press **Enter**.

   **Note:** Use the same value in steps 5a, 7a and 8a.

6. In the *Tables* list, select “ServiceInstall”.
7. In the *Name* column, double-click “AgentService”.

   7a. Enter the name to use for the AgentService (use the same value entered in step 5a) and press **Enter**.
8. In the *DisplayName* column, double-click “AgentService”.

   8a. Enter the name to use for the AgentService (use the same value entered in steps 5a and 7a) and press **Enter**.

9. Click File > Save.
10. Click File > Close.
You can edit a registry key that allows you to control what percentage of the CPU is used for the agent. This gives you the ability to throttle the CPU and insure that the agent does not consume all of the CPU available.

**To add a throttling registry key**

1. In the Registry Editor, expand the HKEY_LOCAL_MACHINE hive and locate the HKEY_LOCAL_MACHINE\SOFTWARE\AccessData\Shared folder.
2. Add a new DWORD (32-bit) value to the Shared folder. (HKEY_LOCAL_MACHINE\SOFTWARE\AccessData\Shared\throttling)
3. The data value of the DWORD should be the maximum percentage of the CPU allowed to be used by the module. For example, if you want the maximum percentage of the CPU used to be 25 percent, modify the DWORD data value and enter 25 in the Edit DWORD dialog. The value should be from 0-100. If the data value is left at 0, the CPU will not be throttled when the agent is started.
4. In the Edit DWORD dialog, select the Decimal radio button and click OK.
5. After applying the registry key changes, restart the agent service.

For more information on adding and editing registry keys, see Microsoft’s documentation.

**Important Information**

The following information is important to know about installing and executing an agent:

- In version 7.2 and newer, agent modules are automatically deployed to the agent as part of the Windows agent installation process.
- The ADMON module does not run on low resource priority. The ADMON module must run on Normal priority or higher in order to maintain connection to the system drivers.
Using Agent Certs in Forensics Products

About Certs

Definitions

- Agent - A service running on a target machine that will allow for remote collection of volatile, drive, and other data.
- Client - The program that submits jobs to and collects results from Agents. An example is AD Enterprise.
- Public Cert - A file with an X.509 certificate or cert chain and must include the root CA X.509.
- Private Cert - A file with a private key and X.509 certificate signed by root CA.

Where Certs are Used

Certs are used for secure communication in the following instances:

- Between the Client program and Agents.

Cert requirements

- Must be in a supported format (see sections below).
- SHA-1 or SHA-256 hashing algorithm both supported.
- Public Certs must include the root CA cert.
- Neither Key Usage nor Extended Key Usage cert extensions are required; ignored if present.

Supported formats for Public Certs

- Base64 encoded CER/CRT.
- Binary DER encoded P7B.
Supported formats for Private Certs
- Unencrypted PEM (Base64)
- ADP12
- PFX*

*The PFX/PKCS#12 format is not supported directly by Clients. It must be converted to ADP12 or PEM before it can be used. See instructions in the Cert Conversion sections for more details.

About Using Certs
The following table lists which certs are used and when:

<table>
<thead>
<tr>
<th>Agents:</th>
<th>Agents only use a Public Cert. It must be provided at install time.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client:</td>
<td>Client programs use a Private Cert to communicate with an Agent. For AD Enterprise, the path to the Private Cert must be entered into Agent settings. See Setting Agent Configuration Settings on page 54.</td>
</tr>
</tbody>
</table>
Creating Certs

Examples will be given in following sections for how to create your own certs. These are just examples and your situation and needs may be different. The examples show how to create certs using OpenSSL, so first you must obtain OpenSSL.

Install OpenSSL

Installing OpenSSL on Windows

The OpenSSL project does not distribute binaries for Windows, and does not officially recommend any specific binary distributions. Therefore, it is usually safer to use OpenSSL on Linux, obtaining it from your official distro repository. If you still would like to use Windows, an informal list of third party binary distributions can be found here: https://wiki.openssl.org/index.php/Binaries

- Download and extract files or run installer. (Use at your own risk.)
- After installing you should have a folder that contains at least openssl.exe, libeay32.dll, and ssleay32.dll.
- Follow steps below to configure OpenSSL (openssl.cnf)

Installing OpenSSL on Debian Linux

- Run this command from a terminal window: sudo apt-get install openssl

Installing OpenSSL on RedHat Linux

- Run this command from a terminal window: sudo yum install openssl
Configure OpenSSL

This step is required if you wish to establish yourself as a Root CA, which you will want to do unless someone else is performing the role of CA.

Download the example openssl.cnf from here and modify as desired:

Alternatively, especially on Linux, you may have an existing openssl.cnf (e.g., at /etc/ssl/openssl.cnf) that already suits your needs or you would like to use as a starting point. Take special note of the “dir” variable in your openssl.cnf. It may be something like “./demoCA”. You may need to adjust your commands below slightly depending on this variable.

Change to a directory where you want to store files associated with your CA and run these commands:

mkdir CA
cd CA
mkdir newcerts
mkdir private
echo 01 > serial
touch index.txt (on Windows, create an empty file named index.txt)

Windows: Place the openssl.cnf inside the CA folder and set the environment variable OPENSSL_CONF to “\openssl.cnf”. Alternatively, place the openssl.cnf in C:\usr\local\ssl\openssl.cnf.

This link may provide some additional help for configuring OpenSSL and establishing yourself as a Root CA: http://www.eclectica.ca/howto/ssl-cert-howto.php/
Generating the Root CA Self-signed Public Cert and Private Key
To generate the Root CA Self-signed Public Cert and Private Key, run this command:

```
openssl req -x509 -sha256 -newkey rsa:2048 -out ca.crt -keyout ca.key -days 3650
```

- Leave off `-sha256` if you want to use SHA-1 hashing algorithm.
- The `-days 3650` will make the cert valid for 10 years; change to another value if desired.
- Add `-nodes` if you don’t want to encrypt the ca private key (bad idea)

When prompted, enter desired passphrase (twice). Then follow the prompts to enter the Country Name, State, Organization, etc. You will probably want to include “Root” or “CA” somewhere in the Common Name.

The resulting ca.crt is the Public Cert that needs to be provided to agents during install. The resulting ca.key should be kept private and secure.

You may run this command to combine private key with X.509 to create a Private Cert for the CA:

- Linux: `cat ca.crt ca.key > ca.pem`
- Windows: `copy /b ca.crt + ca.key ca.pem`

However, this step is not necessary unless you are taking shortcuts and want to use the CA certs for everything (less secure; NOT recommended!). Also, this pem file cannot be be used directly unless you added `-nodes` above for no encryption, or you convert this PEM to ADP12 format.

Generating a Public/Private Cert Pair
You can generate a Public/Private Cert Pair for use by a Client.

Every Client can and should use its own unique keypair. But all certs need to be signed by the root CA, and public certs need to include the CA X.509.

1. Create a CSR (certificate signing request).

   ```
   openssl req -new -nodes -out client_1.csr -keyout client_1.key
   ```

   The `-nodes` makes the PEM unencrypted; you may leave it off, but encrypted PEMs are not supported directly by Client programs, so you will need to convert it to ADP12 format after.

   Follow the prompts to enter the Country Name, State, Organization, and so on. Use a Common Name that uniquely describes the specific Client instance.

2. Sign the CSR to create X.509 CRT.

   (Depending on your openssl.cnf, you may need to run this command from the CA directory, or...
demoCAdirectory, or a parent directory).

openssl ca -md sha256 -days 3650 -policy policy_match -keyfile ca.key -cert ca.crt -out client_1.crt -infiles client_1.csr

- Leave off -sha256 if you want to use SHA-1 hashing algorithm.
- The -days 3650 will make the cert valid for 10 years; change it to some other value if desired. Answer y when prompted to sign y/n.

Edit the resulting client_1.crt and remove all the lines before the

-----BEGIN CERTIFICATE-----.

3. Combine CA's X.509 with newly signed X.509 CRT to create a usable Public Cert.

openssl crl2pkcs7 -nocrl -outform DER -certfile client_1.crt -certfile ca.crt -out client_1.p7b

The -outform DER is very important; only P7B files in binary DER format are supported.

4. Combine private key and X.509 to create Private Cert:

- Linux: cat client_1.crt client_1.key > client_1.pem
- Windows: copy /b client_1.crt + client_1.key client_1.pem

5. At this point you may want to delete the CRT file (client_1.crt). You may also delete the CSR and KEY files.

Important: This CRT file is not usable as a Public Cert because it does not contain the CA cert. Only the client_1.p7b or the ca.crt (usually just ca.crt) are usable because they contain the CA cert. There is still a copy of the X.509 inside the client_1.p7b and the client_1.pem, so it is not lost. The resulting client_1.pem is the Private Cert to be entered into the Agent configuration in the Client. The client_1.p7b may be used for the Public Cert but generally only the ca.crt is used. See Setting Agent Configuration Settings on page 54.

Converting Certs using OpenSSL

Converting a Private Cert from PFX to PEM (unencrypted) using openssl

openssl pkcs12 -in cert.pfx -out test.pem -nodes

When prompted, enter the password of the PFX file; you may have to enter it more than once. Then, using a text editor, edit the file and remove all lines outside of

-----BEGIN CERTIFICATE----- and -----END CERTIFICATE-----.

For example, remove all lines such as Bag Attributes, Key Attributes, subject=, issuer=, and so on.

Converting a Private Cert from PEM to PFX using openssl

openssl pkcs12 -export -out cert.pfx -in cert.pem

When prompted for an export password, enter a chosen password; you may need to enter it
twice. Do not leave the password empty; although this may appear to work, PKCS#12 requires private keys in the PKCS#12 container to be encrypted, so a PFX that does not conform to this is invalid and may not be supported.
Examing Certs using OpenSSL

**Print human-readable contents of a CRT/CER file**
openssl x509 -in cert.crt -noout -text (to view X.509)

**Print human-readable contents of a P7B file**
openssl pkcs7 -in client_1.p7b -inform DER -noout -print_certs -text

**Print human-readable contents of a PEM file**
openssl x509 -in cert.pem -noout -text (to view X.509)
openssl rsa -in cert.pem -noout -text (to view private key)

**Print human-readable contents of a PFX/PKCS12 file**
Follow steps in previous section to convert PFX to PEM format, then print out contents of PEM using commands above.
Cert verification checklist

- Print out the human-readable contents of Public and Private certs using OpenSSL.

  You may also be able to verify some items by just double-clicking to view them in Windows. This works fine for CER and P7B; unfortunately, with PFX it wants to do an import, so you may not want to do that.

- For the Public Cert (CER or P7B): Verify that it contains the Root CA cert in there.

  It may have up to 3 certs in here (root CA, intermediate, and the leaf one). For each one, you are looking for the "CN=" part of the Subject to tell which cert it is.

  Also, verify that this file is in binary format by opening with notepad and noticing that it looks like random garbage. If you see a "-----BEGIN CERTIFICATE-----" in the P7B, then it was exported incorrectly and will not work with our products.

- For the Private Cert (PFX or PEM): Convert to PEM following instructions in this document.

  Verify that it contains the correct public cert with the common name (look for CN= on Subject line) you chose. This cert doesn't need to have the full chain of certs; usually just the one cert.

  Also, run the command to print out the private key to verify the PEM contains a private key.

- For the Cert to use while pushing agents (CER): This should be a CER file containing the Root CA (a P7B is also ok, but no need to be a P7B since only one cert in here). Use openssl to print it out in human-readable format and verify it contains just the Root CA cert.

- If still not working, try restarting WM and SS services one more time.
Installing the Linux Agent

This chapter discusses the Linux Agent Installer. It includes the following topics:
- See Installing The Enterprise Agent on Linux on page 688.

Installing The Enterprise Agent on Linux

The AccessData Agent is available for Unix-, Linux-, and Mac-based operating systems as well as for Windows. This chapter discusses the specific installation files to use for supported Linux platforms. The following chapter discusses installing the Mac Agent.

Supported Platforms

The Linux Agent Installer supports the following platforms:

Linux Agent Supported Platforms

<table>
<thead>
<tr>
<th>Installer</th>
<th>OS</th>
</tr>
</thead>
<tbody>
<tr>
<td>agent-linux32.sh</td>
<td>Amazon Linux v1</td>
</tr>
<tr>
<td></td>
<td>Amazon Linux v2</td>
</tr>
<tr>
<td>agent-linux64.sh</td>
<td>Red Hat Linux 7.x</td>
</tr>
<tr>
<td></td>
<td>CentOS_5.11_x64</td>
</tr>
<tr>
<td></td>
<td>CentOS 7.x</td>
</tr>
<tr>
<td></td>
<td>CentOS 8.x</td>
</tr>
<tr>
<td></td>
<td>Ubuntu 14 and newer</td>
</tr>
<tr>
<td></td>
<td>Debian 8.7 and newer</td>
</tr>
<tr>
<td></td>
<td>Fedora 33</td>
</tr>
</tbody>
</table>

The 6.2 or newer Linux Agent requires GLIBC 2.17. Collection from a system running an older GLIBC version can be attempted using the 6.1 version of the Agent, which can be obtained by contacting AccessData Support. A system's GLIBC version can be determined by running the following command: ldd --version.
Linux Agent Supported Platforms

<table>
<thead>
<tr>
<th>Installer</th>
<th>OS</th>
</tr>
</thead>
<tbody>
<tr>
<td>agent-rh5.sh</td>
<td>CentOS Enterprise 5 (32- &amp; 64-bit)</td>
</tr>
<tr>
<td>agent-rh5x64.sh</td>
<td>CentOS 7.1 64-bit</td>
</tr>
<tr>
<td>(older 6.1 agent; available on request)</td>
<td>Debian 8.7 64-bit</td>
</tr>
<tr>
<td></td>
<td>RedHat 5 (32- &amp; 64-bit)</td>
</tr>
<tr>
<td></td>
<td>Red Hat Enterprise Linux 7.1 64-bit</td>
</tr>
<tr>
<td></td>
<td>Red Hat Enterprise Linux 7.3 64-bit</td>
</tr>
<tr>
<td></td>
<td>SLED 11 (Suse Linux Enterprise Desktop) (32- &amp; 64-bit)</td>
</tr>
<tr>
<td></td>
<td>Ubuntu 9 (and newer) (64-bit)</td>
</tr>
<tr>
<td>agent-rh3.sh or agent-rh3x64.sh</td>
<td>RedHat 3 (32- &amp; 64-bit)</td>
</tr>
<tr>
<td>(older 6.1 agent; available on request)</td>
<td>Novell Linux Desktop (NLD) 9 (32-bit)</td>
</tr>
<tr>
<td></td>
<td>SLED 10 (Suse Linux Enterprise Desktop) (32- &amp; 64-bit)</td>
</tr>
</tbody>
</table>

Be sure to use the correct installer file for your 32- or 64-bit architecture/OS.

To install the Linux Agent

Execute the following command as root, and provide the appropriate information:

```
./agent-linux<bits>.sh <certpath> [-i <installpath>]
```

where <bits> is 32 or 64 depending on the operating system agent that is being used, and where <certpath> is the location of the public certificate to be used for identification, and where [-i <installpath>] indicates the directory to install the agent in. This defaults to:

```
/usr/AccessData/agent
```

To install the Linux Agent on Fedora Based OS's

Execute the following commands as root/sudo:

1. Open Terminal within the agent location path.
2. Enter the following command to give executable rights:
   ```
   chmod +x agent-linux64.sh
   ```
3. Follow the installation steps in the To Install Linux Agent section above.
   ```
   If the agent service fails to start, the steps below must be followed.
   ```
4. Enter the following command to set the security context of the Agent Core daemon:
   ```
   sudo /sbin/restorecon -v /etc/rc.d/init.d/agentcored
   ```
5. Enter the following command to search the Audit log and then update the allow/dontaudit policy for the Agent Core daemon:
   ```
   sudo ausearch -c '(entcored)' --raw | audit2allow -M my-entcored
   ```
6. Enter the following command to update the SELinux policy module:
   • sudo semodule -X 300 -i my-entcored.pp

7. Enter the following commands to restart the agent:
   • sudo /etc/init.d/agentcored stop
   • sudo /etc/init.d/agentcored start

8. Enter the following command to check the status of the agent:
   • sudo /etc/init.d/agentcored status

---

**Enterprise Linux Agent Install Parameters and Options**

<table>
<thead>
<tr>
<th><strong>Option</strong></th>
<th><strong>Result</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>-installpath, -i &lt;installpath&gt;</td>
<td>The destination path for installing the agent. Default: /usr/AccessData/agent/.</td>
</tr>
<tr>
<td>-lifetime, -l &lt;lifetime&gt;</td>
<td>The lifetime of the agent. Default: 0.</td>
</tr>
<tr>
<td></td>
<td>If &lt;lifetime&gt; == 0, it will never uninstall itself. If &lt;lifetime&gt; &gt; 0 it is days before uninstall.</td>
</tr>
<tr>
<td></td>
<td>If &lt;lifetime&gt; &lt; 0 it is in minutes before uninstall.</td>
</tr>
<tr>
<td>-port, -p &lt;port&gt;</td>
<td>The port the agent listens on. Default: 3999.</td>
</tr>
<tr>
<td>-connections, -c &lt;connections&gt;</td>
<td>The maximum number of concurrent connections allowed by the agent. Default is 10.</td>
</tr>
<tr>
<td>-size, -s &lt;storagesize&gt;</td>
<td>The protected storage area size. Default is 16777216 (16 MB)</td>
</tr>
</tbody>
</table>
**Uninstallation**
To uninstall the Linux Agent, execute the following command as root:

```
# ./agent-linux64.sh -rf
```

**Starting/Stopping the Service**
The Linux Agent service is started automatically on system startup, but can be stopped, started, and restarted anytime manually by executing commands such as the following (as root)

```
/etc/init.d/agentcored stop
/etc/init.d/agentcored start
/etc/init.d/agentcored restart
```
Chapter 48
Installing the Mac Agent

This chapter discusses the Agent Installer for Apple Macintosh. It includes the following topics:
- See Comparing the Mac OS X Agent to the macOS Agent on page 691.
- See Installing the macOS Managed Agent on page 692.
- See Pushing the macOS Agent on page 701.
- See Installing the Legacy Mac Agent on page 706.

Comparing the Mac OS X Agent to the macOS Agent
In keeping up with architecture and security enhancements in macOS (starting with High Sierra 10.13 and including subsequent releases Mojave 10.14 and Catalina 10.15), AccessData has developed an entirely new agent architecture known internally as the “managed agent”. Documentation that refers to the agent for Mac OS X only applies to the agent designed for macOS Sierra 10.12 and older. Any mentions of macOS agent only apply to the managed agent that supports macOS High Sierra 10.13 and the newer versions of macOS. See See Apple Macintosh OS Agent Reference on page 691.

Apple Macintosh OS Agent Reference

<table>
<thead>
<tr>
<th>Version</th>
<th>Code Name</th>
<th>AccessData Agent Type</th>
<th>Agent Installer Package</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mac OS X 10.9</td>
<td>Mavericks</td>
<td>Legacy Mac OS X agent</td>
<td>agent-mac10.6.mpkg</td>
</tr>
<tr>
<td>Mac OS X 10.10</td>
<td>Yosemite</td>
<td>Legacy Mac OS X agent</td>
<td>agent-mac10.6.mpkg</td>
</tr>
<tr>
<td>Mac OS X 10.11</td>
<td>El Capitan</td>
<td>Legacy Mac OS X agent</td>
<td>agent-mac10.6.mpkg</td>
</tr>
<tr>
<td>macOS 10.12</td>
<td>Sierra</td>
<td>Legacy Mac OS X agent</td>
<td>agent-mac10.6.mpkg</td>
</tr>
<tr>
<td>macOS 10.13</td>
<td>High Sierra</td>
<td>AccessData Managed Agent</td>
<td>AccessDataAgent-macos-installer-x64-1.X.XX.pkg</td>
</tr>
</tbody>
</table>
### Apple Macintosh OS Agent Reference

<table>
<thead>
<tr>
<th>Version</th>
<th>Code Name</th>
<th>AccessData Agent Type</th>
<th>Agent Installer Package</th>
</tr>
</thead>
<tbody>
<tr>
<td>macOS 10.14</td>
<td>Mojave</td>
<td>AccessData Managed Agent</td>
<td>AccessDataAgent-macos-installer-x64-1.XXX.pkg</td>
</tr>
<tr>
<td>macOS 10.15</td>
<td>Catalina</td>
<td>AccessData Managed Agent</td>
<td>AccessDataAgent-macos-installer-x64-1.XXX.pkg</td>
</tr>
<tr>
<td>macOS 11.0</td>
<td>Big Sur</td>
<td>AccessData Managed Agent</td>
<td>AccessDataAgent-macos-installer-x64-1.XXX.pkg</td>
</tr>
</tbody>
</table>

### Installing the macOS Managed Agent

The following sections relate only to the macOS Managed agent (High Sierra 10.13 and newer). See Comparing the Mac OS X Agent to the macOS Agent on page 691. This section covers the following topics:

- About macOS Managed Agent (page 692)
- Installing the macOS Agent Manually (page 693)
- macOS Agent Troubleshooting and Maintenance (page 700)
- Pushing the macOS Agent (page 701)

### About macOS Managed Agent

The macOS managed agent represents an entirely new agent architecture for AccessData. Below are some of the key features and system requirements.

#### Product Features

- Acquires one or more logical disk slices over-the-wire to specified network share.
- Acquires targeted files or contents of entire folder trees selected from live disk preview.
- Creates an index of all files on all attached drives
- Agent can be configured to index file system metadata (file name, path, date created etc.) and optionally index file content based on a list of file extensions.
- Search the index by file name, mask, or keywords by content using dtSearch free form query.
LiveSearch: Reindexing some folder on-the-fly and making a search over newly created index

Agent Endpoint System Requirements

Operation system:
- macOS High Sierra 10.13 or newer
- Network access enabled
- FullDiskAccess permissions (See Configuring macOS Agent Full Disk Access on page 697.)

Note: The Windows system hosting AD Enterprise needs “Enable NTFS long paths” enabled to prevent APFS long filenames / paths causing the acquisition to fail when written to the Windows system.

Hardware
- 6th gen Intel Core processor or better
- 2GB RAM
- 20GB hard drive with at least 15GB of available space

Software requirements:
- .NET Core Runtime 2.2.6 x64

Installing the macOS Agent Manually

Compared to the other AccessData agents, the macOS agent is much more complicated to install manually. It is recommended that you read through the following sections and assemble copies of the installer, configuration files, and certificates into a directory on systems administrators workspace or server so as to build a deployment package and streamline the entire process.
How to install the macOS agent manually

1. Transfer a copy of the macOS agent PKG (and cert and index / port configuration files) to target macOS system.

   **Important:** Do not modify PKG contents

2. Uninstall any existing macOS agent packages before proceeding. See macOS Agent Troubleshooting and Maintenance on page 700.

3. Do one of the following:

   3a. Double-click on agent installer and follow install wizard:

   ```
   AccessDataAgent-macos-installer-x64-$(Version).pkg
   ```

   3b. Using ssh:

   ```
   sudo installer -pkg /path/to/package.pkg -target /
   ```

4. When complete, the agent service (daemon) should be listed as running. See macOS Agent Troubleshooting and Maintenance on page 700.

5. Once installed properly, you will likely want to configure the following in order to enable all features that apply to your investigation:

   5a. Configuring macOS Agent Index Search Settings for configuring the search indexing settings.
   5b. Configuring macOS Agent Full Disk Access to grant Full Disk Access to the agent
   5c. Configuring Custom Network Port and Agent Certificate to configure a custom network port or agent certificate.
Configuring macOS Agent Index Search Settings

The macOS agent can be configured to build a search index of the metadata and file contents of the system. The indexing is enabled by default, but for best results, you should configure the Agent Settings file to meet the requirements of your investigation. The following procedures assume you will copy a pre-configured agentsetting.json file to the target system where the macOS agent has already been deployed. Refer to macOS Agent Troubleshooting and Maintenance for commands such as stopping and starting the agent service.

Configuring the Agent Index Setting File

1. Using a text editor, open the agentsetting.json file located at:

/usr/local/share/AccessData/ManagedAgent/AgentData/agentsetting.json

2. The JSON has separate configurations for each aspect of the system that could be indexed which are categorized by the DataName value.

Note: At this time, only the File and BrowserHistory DataName is supported in this version. OtherDataName values are placeholders for future functionality.

3. For the File Datename group of values, configure the following:
   - EnableIndexing to true
   - For FileMaskForContentsIndexing, define a list of file extensions you wish to have indexed.
   - For FoldersForContentsIndexing define a list of directories whose contents you wish to have indexed.
   - Configure other values as appropriate based on notes in the AgentSetting.json Reference Table

4. Save your changes when you are done.

How to update a macOS agent’s index search settings

1. Edit the agentsetting.json if you haven’t already. See Configuring the Agent Index Setting File on page 694.
2. Deploy the macOS agent package to the endpoint if not already deployed.
3. Stop the agent service.
4. Copy the agentsetting.json (overwrite) to:

   /usr/local/share/AccessData/ManagedAgent/AgentData/agentsetting.json

5. Start the agent service.
**Note:** Indexing the entire system can take one to several hours to complete.

### Agent Settings Reference Table

The following table describes the configurable fields of the agentsetting.json configuration file, the default values, and notes on appropriate usage.

### AgentSetting.json Reference Table

<table>
<thead>
<tr>
<th>Agent Settings Fields</th>
<th>Default Value</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>IndexingDirectory</td>
<td>/usr/local/share/AccessData/ManagedAgent/AgentData/Indices</td>
<td>Default location of search index.</td>
</tr>
<tr>
<td>DataType</td>
<td>0</td>
<td>DO NOT EDIT Built-in values range 0-16.</td>
</tr>
<tr>
<td>IndexLastCompleteTime</td>
<td>n/a</td>
<td>YYYY-MM-DD</td>
</tr>
<tr>
<td>DocumentsIndexed</td>
<td>n/a</td>
<td>Number of documents indexed.</td>
</tr>
<tr>
<td>IndexRefreshIntervalinMins</td>
<td>60</td>
<td>Time interval (minutes) between indexing updates.</td>
</tr>
<tr>
<td>MaxIndexSizeInMB</td>
<td>0</td>
<td><em>FUTURE FEATURE</em> Max index size in megabytes (MB). A value of &quot;0&quot; disables any limit on max index size.</td>
</tr>
<tr>
<td>IndexAllowedHours</td>
<td>&quot;0~24&quot;</td>
<td>Values in range 0<del>23 hours. A value of &quot;0</del>24&quot; allows indexing to occur at any hour of the day. Syntax is: HH~HH</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note: Start and end hours are delimited by a tilde (~) character.</td>
</tr>
</tbody>
</table>
### Agent Settings Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Default Value</th>
<th>Notes</th>
</tr>
</thead>
</table>
| FileMaskForContentsIndexing         | "pages", "numbers", "key", "kth", "emlx", "emix", "emlxpart", "ewsmbbox", "imapmbbox", "emlxpart", "txt", "ewsmbbox", "pdf", "imapmbbox", "docx" | File extensions to be indexed. When used in conjunction with FoldersForContentsIndexing, the filters use OR logic and so files meeting either criteria will be included in the index. Sample syntax is: 
```
[ "emlxpart", "txt", "ewsmbbox", "pdf", "imapmbbox", "docx"
 ]
```

| FoldersForContentsIndexing          | "*"           | List of directories whose contents will be indexed. When used in conjunction with FileMaskForContentsIndexing, the filters use OR logic and so files / folders meeting either criteria will be included in the index. Path must be fully qualified. Sub-strings of folder paths are not currently supported. Example: 
```
[ 
  "/Users/jsmith/Documents/pdf/", 
  "/Users/jdoe/notes/
]
```

<table>
<thead>
<tr>
<th>SearchHiddenFiles</th>
<th>false</th>
<th>true</th>
<th>false</th>
<th>Allow indexing of hidden files in the file system.</th>
</tr>
</thead>
<tbody>
<tr>
<td>SearchSystemFiles</td>
<td>false</td>
<td>true</td>
<td>false</td>
<td>Allow indexing of macOS System files.</td>
</tr>
</tbody>
</table>
Configuring macOS Agent Full Disk Access

The macOS agent requires Full Disk Access in order to acquire data and send it back to Enterprise. Prior to collecting from the macOS agent, the following configurations must be applied. Unfortunately due to increased security in macOS systems, these security configurations cannot be scripted with a standard bash script.

However thanks to Jamf’s partnership with Apple, this configuration can be done automatically when pushing the macOS agent.

For more information on macOS agent push via jamf see “Pushing the macOS Agent” on page 701
How to grant Full Disk Access to the macOS agent application

1. On the macOS endpoint, open System Preferences >> Security & Privacy
2. Select the Privacy tab.

3. From menu on the left, select Full Disk Access, then click the lock icon.
4. Use your Touch ID or enter your system administrator credentials and click Unlock.
5. Click +
6. Click Applications, then click the Utilities folder
7. Select Console and then click Open.
8. Repeat steps 5-7 to also add the **Terminal** app.

9. Launch Finder

10. From the menu bar, navigate to Go >> Go to Folder >> /Library/AccessDataAgent/$(Version)/

11. From that directory, drag the following files to the Security and Privacy window Full Disk Access:

   - ADG.ManagedAgentSvc
   - ADG.Agent.IndexingService

12. If for some reason `/bin/sh` is not already in the list with **Full Disk Access**, use Go to Folder navigate to it and add it.

13. The Full Disk Access list should now list:

   - ADG.ManagedAgentSvc
   - ADG.Agent.IndexingService
   - sh
   - Console
   - Terminal

14. Close the **Security and Privacy** window when the list is configured correctly.
Configuring Custom Network Port and Agent Certificate

Upon completing the install the macOS agent is, by default, configured to use the default network port and the default agent communication certificate built into AccessData Enterprise. The agent service listens for incoming connections on TCP 4999, by default. The default agent certificate is signed and issued by AccessData. Both the agent network port and the certificate file can be customized to meet the needs of your organization.

**How to configure the macOS agent to use a custom certificate**

1. Transfer a copy of your Enterprise public agent certificate to the macOS system.
2. Rename the public key cert file to `client.cer`
3. **Stop** the agent service.
4. Copy (overwrite) client.cer to:

   ```sh
   /usr/local/share/AccessData/ManagedAgent/AgentData/client.cer
   ```
5. **Start** the agent service.

**How to configure the macOS agent to listen on custom network port**

1. If you are editing the configuration of a live macOS endpoint, **stop** the agent service before proceeding.
2. Using a text editor, open the appsettings.json file located at:

   ```sh
   /Library/AccessDataAgent/<AgentVersion>/appsettings.json
   ```
3. Locate the “port”: 4999, setting and replace the 4999 with the desired port number.
4. Save your changes and **start** the agent service (if applicable) when you are done.
### macOS Agent Troubleshooting and Maintenance

The following table contains useful commands to help you troubleshoot and maintain the macOS agent.

**macOS Agent Resource Reference**

<table>
<thead>
<tr>
<th>Resource</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stop agent service</td>
<td><code>sudo launchctl unload /Library/LaunchDaemons/com.adg.managedagent.plist</code></td>
</tr>
<tr>
<td>Start agent service</td>
<td><code>sudo launchctl load /Library/LaunchDaemons/com.adg.managedagent.plist</code></td>
</tr>
</tbody>
</table>
| Agent Log                 | Enterprise Examiner: C:\Users\Public\Documents\AccessData\AccessDataLogs\adgselfhost.txt  
                           | macOS Endpoint: /Library/AccesdataAgent/${Version}/Logs/agentlog.txt  
                           | /Library/AccesdataAgent/${Version}/Logs/ADG.Agent.IndexingService.log |
| Check if agent process is running | `sudo ps -x | grep ADG`                                             |
| Kill agent process        | `sudo kill -9 <PID>`                                                |
| Lookup agent version      | Directory at this path lists version:  
                           | /Library/AccesdataAgent/${Version}                                    |
| Uninstall macOS agent     | `sudo bash /Library/AccesdataAgent/${Version}/uninstall.sh`          |
|                           | Answer yes (y), when prompted, if you wish to delete all saved agent settings as well. |
**Pushing the macOS Agent**

The macOS agent can be pushed to Mac systems using jamf PRO based on configured Jamf policies. Once a macOS device has been enrolled to jamf and the agent has been pushed, enrolled devices will check in with jamf PRO every 5 minutes by default to pull down any updated policies. For this documentation, it is assumed that your organization’s jamf PRO installation meets the following prerequisites.

**Jamf PRO Prerequisites**

1. jamf PRO version 10.19 (with active license) should be installed per the following guidelines:
   - [jamf PRO System Requirements](#)
   - [jamf PRO Documentation](#) (Administrator's Guide and Install Guides for Windows, Mac, and Linux)

   __Note:__ jamf Cloud and jamf Now are not currently supported

2. System hosting jamf PRO server must have network access to connect to the following web application URL:

   gateway.push.apple.com:2195

3. [Jamf PRO push certificates](#) are configured

4. Device enrollment has been configured and devices have been enrolled. macOS managed agent target endpoints are limited to these versions of macOS:
   - High Sierra (10.13)
   - Mojave (10.14)
   - Catalina (10.15)

5. A [jamf PRO "File Share Distribution Point"](#) has been created and configured.

6. The following files have been extracted from the Enterprise installation media and readily available to the Jamf PRO server system:
   - `agentsetting.json` (based on agentsetting_template.json. See [Configuring macOS Agent IndexSearch Settings](#) on page 694.)
   - `ConsoleProfiles.mobileconfig`
   - OPTIONAL-- Enterprise agent public key certificate file renamed to `client.cer` (See [Using Agent Certs in Forensics Products](#) on page 680.)
Configuring Jamf PRO to Push macOS Agents

Use the following procedure to add the macOS agent package to jamf PRO

How to configure Jamf PRO to push macOS agents

1. Upload macOS agent package to the jamf PRO File Share Distribution Point folder.

2. Under the Distribution Point folder, create subfolder named AgentConfiguration.

3. Transfer pre-configured copy of agentsetting.json to AgentConfiguration directory. See Configuring macOS Agent Index Search Settings on page 694.

4. Add two rules to the File Share Distribution Point’s web.config (located at the root level of the File ShareDistribution Point shared folder) to add mimeType entries for pushing .cer and .json files to endpoints.

```xml
<?xml version="1.0" encoding="UTF-8"?>
<configuration>
    <system.webServer>
        <staticContent>
            <mimeMap mimeType="file/download" fileExtension=".dmg"/>
            <mimeMap mimeType="application/octet-stream" fileExtension=".pkg"/>
            <mimeMap mimeType="application/octet-stream" fileExtension=".cer"/>
        </staticContent>
    </system.webServer>
</configuration>
```

5. In Jamf PRO, navigate to Computers >> Configuration Profiles >> Upload

See Jamf PRO Configuration Profiles for additional guidance

5a. Browse to ConsoleProfiles.mobileconfig and then click Upload.

5b. Click ConsoleProfiles to review the new profile entry.

5c. Click Edit button and configure these attributes:
   - Options | Privacy Preferences Policy Control | *These settings have already been pre-configured*
   - Scope | Targets | Target Computers | All Computers
   - Scope | Targets | Target Users | All Users

5d. Click Save and then Done
6. Add the following agent management scripts to Jamf PRO:

6a. Settings ➔ Computer Management ➔ Scripts ➔ +New

- Display Name | Update AccessData Agent settings

Script | Script Contents:
launchctl unload /Library/LaunchDaemons/com.adg.managedagent.plist
curl -k -o /usr/local/share/AccessData/ManagedAgent/AgentData/agentsetting.json "http://jamf.mycompany.com/jamf_share/AgentConfiguration/$4"
lanchorctl load /Library/LaunchDaemons/com.adg.managedagent.plist

**Note:** The above is a sample script. Jamf PRO URL value must be configured per environment

- Display Name | Start managed agent service

Script | Script Contents:
lanchorctl load /Library/LaunchDaemons/com.adg.managedagent.plist

- Display Name | Stop managed agent service

Script | Script Contents:
lanchorctl unload /Library/LaunchDaemons/com.adg.managedagent.plist

- Display Name | Update AccessData agent client certificate

Script | Script Contents:
lanchorctl unload /Library/LaunchDaemons/com.adg.managedagent.plist
curl -k -o /usr/local/share/AccessData/ManagedAgent/AgentData/client.cer "http://jamf.mycompany.com/jamf_share/AgentConfiguration/$4"
lanchorctl load /Library/LaunchDaemons/com.adg.managedagent.plist

**Note:** The above is a sample script. Jamf PRO URL value must be configured per environment

- Display Name | Update macOS Agent Network Port

Script | Script Contents:
lanchorctl unload /Library/LaunchDaemons/com.adg.managedagent.plist
ADG.ManagedAgentConfigurator --file app --transformer port:$4
lanchorctl load /Library/LaunchDaemons/com.adg.managedagent.plist
Installing the Mac Agent

Installing the Legacy Mac Agent | 793

- Display Name | Remove managed agents

Script | Script Contents:
- `launchctl unload /Library/LaunchDaemons/com.adg.managedagent.plist`
- `sleep 6`
- `rm -rf /Library/AccessDataAgent/*`

7. **Add new package entry to Jamf PRO** based on the attributes listed below.

7a. **Settings** >> **Computer Management** >> **Packages** >> +New
- **General** | Display Name: AccessData macOS Agent [version]
- **General** | Filename: AccessDataAgent-macos-installer-x64-[x].[x].[xx].pkg
- **Options** | Priority: 10

7b. Click **Save**

8. **Create an Agent Deployment Jamf PRO policy** based on the attributes listed below.

8a. **Computers** >> **Policies** >> +New
- **Options** | **General** | Display Name: Deploy AccessData macOS Agent
- **Options** | **General** | Trigger: Recurring Check-in
- **Options** | **General** | Frequency: Once per computer
- **Options** | **Packages** | Add the appropriate AccessData macOS Agent package
- **Options** | **Scripts (Before)** | Remove managed agents
- **Options** | **Scripts (After)** | Start managed agent service
- **Scope** | **Targets** | All Computers OR
- **Scope** | **Targets** | Specific Computers (via Selected Deployment Targets)
- **User Interaction** | **Start Message** | “Update AccessData agent to version x.x.xx”
- **User Interaction** | **Complete Message** | “Update AccessData agent to version x.x.xx”
- **User Interaction** | **Restart Message** | “This computer will restart in 5 minutes. Please save your work and log out”?

8b. Click **Save**
9. **Create an AccessData Agent Setting policy** based on the attributes listed below.

9a. **Computers >> Policies >> +New**
   - Options | General | Display Name: Update AccessData Agent settings
   - Options | General | Trigger: Recurring Check-in
   - Options | General | Frequency: Once per computer
   - Options | Scripts (Before) | **Add** Update AccessData Agent settings
   - Scope | Targets | All Computers OR
   - Scope | Targets | Specific Computers (by Selected Deployment Targets)

9b. Click **Save**

10. Jamf PRO is now configured to push the macOS agent. See **Configuring Optional JamfPRO Policies** to configure a custom agent certificate and custom network port.

### Configuring Optional Jamf PRO Policies

Upon completing the install the macOS agent is, by default, configured to use the default network port and the default agent communication certificate built into AccessData Enterprise. The agent service listens for incoming connections on TCP 4999, by default. The default agent certificate is signed and issued by AccessData. You can define Jamf PRO policies to configure a custom agent network port and / or agent certificate file to meet the needs of your organization.

**How to configure JAMF Pro to update AccessData Agent client certificate**

1. Upload new client certificate (client.cer) to **AgentConfiguration** folder in the jamf PRO File Share Distribution Point. See **Jamf PRO Prerequisites** on page 701.
2. In Jamf PRO, **create an AccessData Agent Certificate Deployment policy**

2a. **Computers >> Policies >> +New**
   - Options | General | Display Name: Update AccessData Agent Certificate
   - Options | General | Trigger: Recurring Check-in
   - Options | General | Frequency: Once per computer
   - Options | Scripts (Before) | **Add** Update AccessData agent client certificate
   - Scope | Targets | All Computers OR

   - Scope | Targets | Specific Computers (via Selected Deployment Targets)

2b. Click **Save**
How to configure JAMF Pro to change AccessData Agent port

1. In Jamf PRO, create a new AccessData Agent Port policy

   1a. Computers >> Policies >> +New
       - Options | General | Display Name: Update AccessData Agent Certificate
       - Options | General | Trigger: Recurring Check-in
       - Options | General | Frequency: Once per computer
       - Options | Scripts | Add Change AccessData agent port
       - Options | Scripts (Before) | Parameter Values | Port | [PORT VALUE 0-65535]
       - Scope | Targets | All Computers

1b. Click Save

Installing the Legacy Mac Agent

The following sections relate only to the legacy Mac agent (Sierra 10.12 and older). See Comparing the Mac OSX Agent to the macOS Agent on page 691. This section covers the following tasks:

- See Installing the macOS Managed Agent on page 692.
- See Building the Mac OS X Agent Package on page 706.
- See Configuring the Mac OS X Agent's Network Port on page 706.
- See Installing the Mac OS X Agent on page 707.
- See Uninstalling the Mac OS X Agent on page 708.
Configuring the AccessData Mac OS X Agent Install Package

The AccessData Agent requires an X.509 certificate in order to establish a secure network connection to the server or for AD Enterprise, the computer running Examiner. The package installer has been provided to aid in the distribution efforts of these certificates by allowing an Administrator to modify the AccessDataAgent package installer prior to installation of AccessData Agent software for Apple Macintosh. In addition to certificate distribution, the port used by the Agent can be configured.

The following instructions allow an Administrator to configure the AccessData Agent package installer.

Building the Mac OS X Agent Package

The AccessData Mac Agent installer requires that a certificate (or certificate tree) is bundled with the installer. The following is the sequence of steps that must be followed to bundle a certificate file into the installer.

2. Make a copy of your AccessData Enterprise agent public certificate available to your system.
3. Locate the Mac Agent installer MPKG file.

Note: Agent packages are found under "\Enterprise\Agents" folder on the AD Enterprise installation media.

4. Using a package manager (or right-click Show Package Contents on a Mac system), open the MPKG to display the package contents.
5. Within the MPKG, create a new folder, called Configure
6. Copy the public certificate file to the Configure folder.
7. Rename the public certificate file to adagent.cert
8. (Optional) If you wish to change the default port that the agent listens on, create a new text file within the Configure folder containing nothing but the desired port number, and name the file adagent.port.
9. The Mac agent package is now ready for deployment to target systems.
Configuring the Mac OS X Agent’s Network Port

The AccessDataAgent installer allows an Administrator to (optionally) configure the port the Agent will use to communicate with an Examiner when installed. This is done by adding a file containing the port number to the AccessDataAgent package installer. The following is a set of instructions an Administrator will use to configure the AccessData Agent package installer. To do so, complete Steps 1-5 under Bundling a Certificate, then continue with Step 1 here. If you do not need to do a custom configuration of the port, skip to Step 6 below.

1. Create a text file named adagent.port that contains the port number the Agent is to use; this file is to be distributed to each installation of the Agent.
2. Place the adagent.port file into the Configure folder (previously created to contain the X.509 certificate).
3. Right-click the AccessDataAgent package installer file.
4. Select Show Package Contents popup menu item.
5. Ensure that the Configure folder is located in the same folder opened in Step 4 (alongside the Contents folder).
6. Close the window.

Note: The installer will not run successfully if all of the above steps are not already completed. The folder and file names must be exactly as documented.
Mac OS X Agent Additional Configuration Options

The Mac installer supports the same settings as the Linux installer. Each setting should be added as a file inside a Configure directory inside the mpkg folder.

Enterprise Mac Agent Configuration Options

<table>
<thead>
<tr>
<th>Option (filename)</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>adagent.cert</td>
<td>Specifies the certificate file used for communication</td>
</tr>
<tr>
<td>adagent.port</td>
<td>Specifies the port the agent will listen on. The setting should contain nothing more than a number. The default port number is 4999</td>
</tr>
<tr>
<td>adagent.lifetime</td>
<td>Specifies the amount of time before the agent dissolves. Again the file should contain nothing more than a number. Same rules as for the Linux agent about sign and value. The default is 0.</td>
</tr>
<tr>
<td>adagent.connections</td>
<td>Sets the maximum number of concurrent connections allowed by the agent. The file should contain only a number. The default is 10.</td>
</tr>
<tr>
<td>adagent.size</td>
<td>Sets the protected storage area size. The file should contain only the number. The default is 16777216. (16 MB).</td>
</tr>
</tbody>
</table>

Installing the Mac OS X Agent

When the certificate is bundled and the port configuration file is complete and saved, distribute the

AccessDataAgent package installer to each target computer and run it locally.

1. Copy the MPKG to the root of the drive / authenticating if prompted
2. Double-click the MPKG file to install the Enterprise Agent

Uninstalling the Mac OS X Agent

The AccessData Mac Agent can be uninstalled via the provided utility.

1. Log in to the Mac system as a system administrator account.
2. Browse to the following directory: /Library/Application Support/AccessData
3. Double-click the uninstall utility
4. Enter the current user password.

Note: If the system administrator account does not have a password associated to it, a password must be assigned in order to run the uninstall utility.
We’d love to hear from you

Our team will be happy to help you on any questions. Write to us!

support@exterro.com

Copyright © 2022 Exterro, Inc.