FTK 7.4.2
Release Notes

Document Date: 2/1/2021

Introduction

This document lists the new features, fixed issues, and known issues for this version. All known issues published under previous release notes still apply until they are listed under "Fixed Issues."

What’s New in 7.4.2

The following items are new in this release:

Database

- FTK now references the databaseConfig.xml (as opposed to FTKDatabases.xml) to connect to the evidence database instance. (FCR-130)

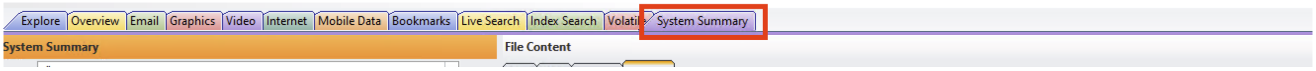
  Current database connection file:
  `[DRIVE]\ProgramData\AccessData\Shared\DatabaseConfig.xml`

  Deprecated database connection file:
  `[DRIVE]\ProgramData\AccessData\Products\Forensic Toolkit\FTK Databases.xml`

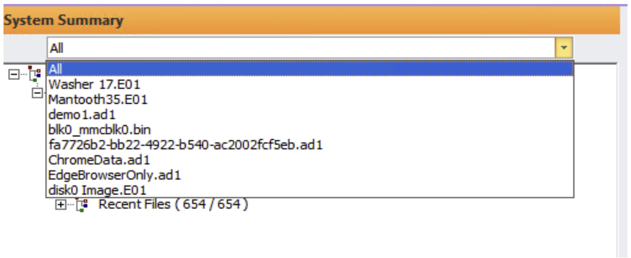
- The “dbvalidate” function of the DBCONTROL utility has been updated to be compatible with the database schema used by version 7.4. (FCR-616)

Data Review

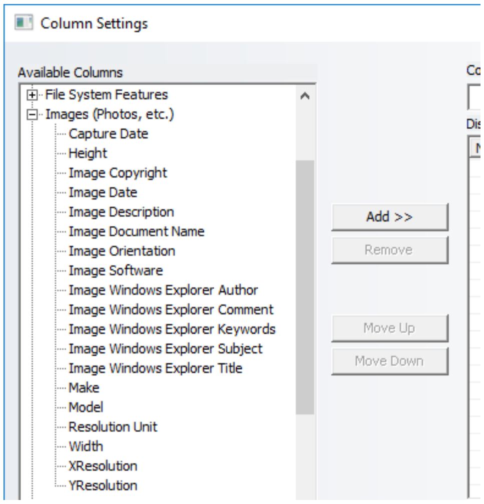
- System Information Tab has been replaced with new “System Summary” Tab. (FCR-805)



- Ability to switch between evidences in System Summary Tab. (FCR-805)



- EXIF metadata parsed from graphic images is now available as columns in file grid. (FCR-414) Many of the EXIF column fields are available under the *Images* category in the Column Settings manager.

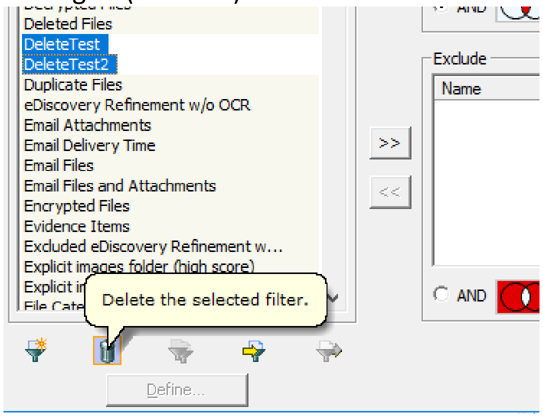


Column Settings

Available Columns

- File System Features
- Images (Photos, etc.)
  - Capture Date
  - Height
  - Image Copyright
  - Image Date
  - Image Description
  - Image Document Name
  - Image Orientation
  - Image Software
  - Image Windows Explorer Author
  - Image Windows Explorer Comment
  - Image Windows Explorer Keywords
  - Image Windows Explorer Subject
  - Image Windows Explorer Title
  - Make
  - Model
  - Resolution Unit
  - Width
  - XResolution
  - YResolution

- An option to bulk delete (CTRL-click) user-created filter records is now available in the Filter Manager. (FCR-419)



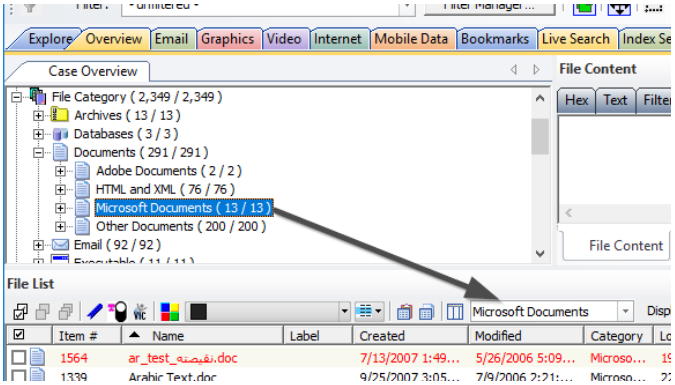
Deleted Files
DeleteTest
DeleteTest2
Duplicate Files
eDiscovery Refinement w/o OCR
Email Attachments
Email Delivery Time
Email Files
Email Files and Attachments
Encrypted Files
Evidence Items
Excluded eDiscovery Refinement w...
Explicit images folder (high score)
Explicit i
File Cate

Delete the selected filter.

- Improved column data for better handling metadata parsed from Microsoft Office files (FCR-421)

Metadata Columns Parsed from Microsoft Office Files	
Author	Last Saved By
Total Editing Time	Create Time
Last Saved Time	Number of Pages
Revision Number	Title

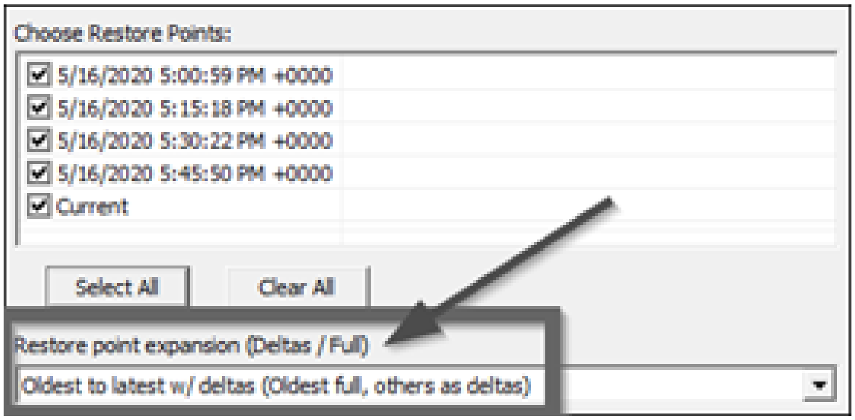
- When certain category notes are selected (from the Overview tab for example), the application will now automatically select a corresponding column setting profile for you in the grid. (See ***Appendix A*** for the mapping of filters to columns.) (FCR-428 / FCR-429)



File Category (2,349 / 2,349)
Archives (13 / 13)
Databases (3 / 3)
Documents (291 / 291)
Adobe Documents (2 / 2)
HTML and XML (76 / 76)
Microsoft Documents (13 / 13)
Other Documents (200 / 200)
Email (92 / 92)

Item #	Name	Label	Created	Modified	Category
1564	ar_test_نقيضة.doc		7/13/2007 1:49…	5/26/2006 5:09…	Microso…
1339	Arabic Text.doc		9/25/2007 3:05…	7/9/2006 2:21:…	Microso…

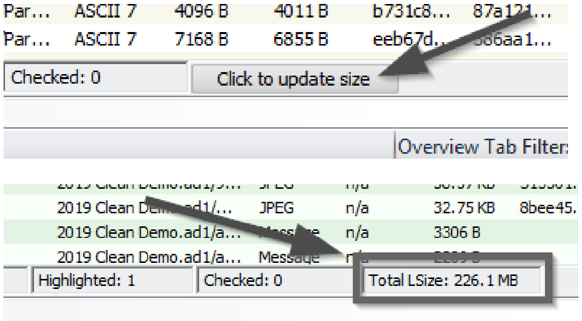
- The descriptor used to identify restore point images in the Explore tab tree view pane has been ordered “Oldest to latest…” by default to clearly indicate the point in time the snapshot was taken. (FCR-77)


Choose Restore Points:

☑ 5/16/2020 5:00:59 PM +0000
☑ 5/16/2020 5:15:18 PM +0000
☑ 5/16/2020 5:30:22 PM +0000
☑ 5/16/2020 5:45:50 PM +0000
☑ Current

Restore point expansion (Deltas / Full)
Oldest to latest w/ deltas (Oldest full, others as deltas)

- The *Total LSize* grid pane statistic is now calculated on-demand via the “Click to update size” button. (FCR-105)



Par…	ASCII 7	4096 B	4011 B	b731c8…	87a121…
Par…	ASCII 7	7168 B	6855 B	eeb67d…	386aa1…

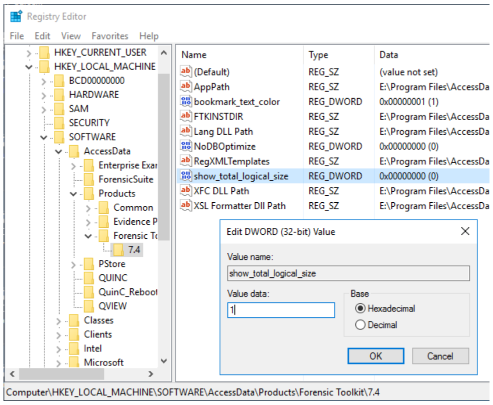
Checked: 0 | Click to update size

Overview Tab Filter:

2019 Clean Demo.ad1/a…	JPEG	n/a	32.75 KB	8bee45.
2019 Clean Demo.ad1/a…	Message	n/a	3306 B	
2019 Clean Demo.ad1/a…	Message	n/a		

Highlighted: 1 | Checked: 0 | Total LSize: 226.1 MB

To control the behavior of the *TotalLSize* calculation, create the following DWORD 32bit registry key value:
HKEY_LOCAL_MACHINE\SOFTWARE\AccessData\Products\Forensic Toolkit\[version] | show_total_logical_size



Name	Type	Data
(Default)	REG_SZ	(value not set)
AppPath	REG_SZ	E:\Program Files\AccessDa
bookmark_text_color	REG_DWORD	0x00000001 (1)
FTKINSTDIR	REG_SZ	E:\Program Files\AccessDa
Lang DLL Path	REG_SZ	E:\Program Files\AccessDa
NoDBOptimize	REG_DWORD	0x00000000 (0)
RegXMLTemplates	REG_SZ	E:\Program Files\AccessDa
show_total_logical_size	REG_DWORD	0x00000000 (0)
XFC DLL Path	REG_SZ	E:\Program Files\AccessDa
XSL Formatter Dll Path	REG_SZ	E:\Program Files\AccessDa

Edit DWORD (32-bit) Value

Value name: show_total_logical_size

Value data: 1

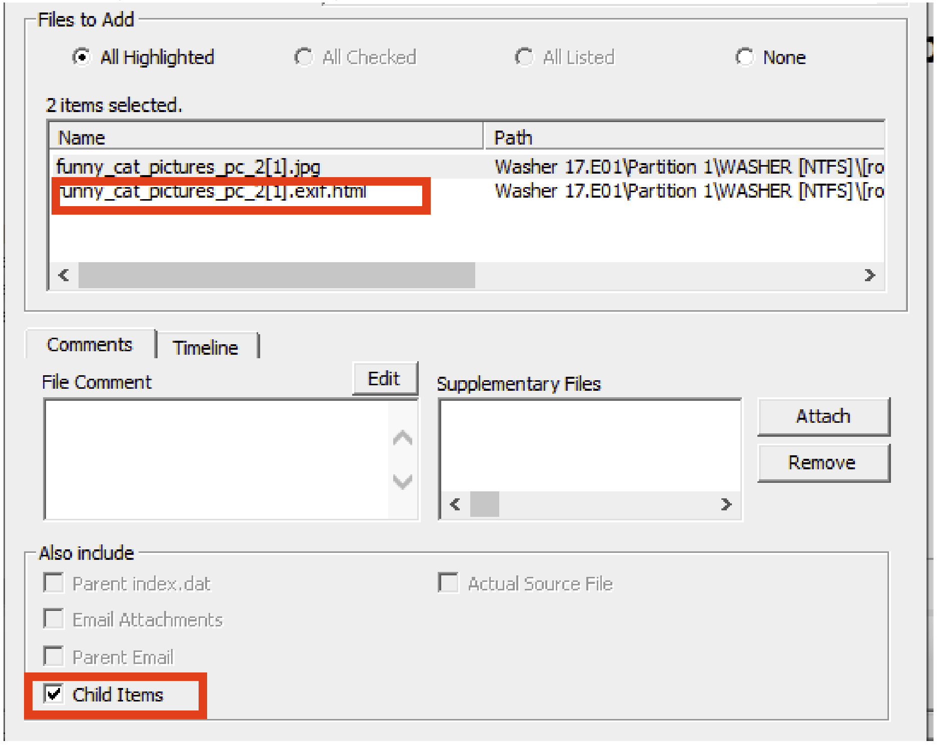
Base: ● Hexadecimal ○ Decimal

OK Cancel

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\AccessData\Products\Forensic Toolkit\7.4

Value of: show_total_logical_size	**Notes**
2	Displays "Click to update size" button. Total LSize displayed and calculated on-demand. This is the application default setting.
1	Total LSize Enabled
0	Total LSize Disabled

- A graphic image record, from which an EXIF database record was parsed, can now be associated as a child object to the EXIF object in a bookmark. (FCR-586)



Files to Add

● All Highlighted ○ All Checked ○ All Listed ○ None

2 items selected.

Name	Path
funny_cat_pictures_pc_2[1].jpg	Washer 17.E01\Partition 1\WASHER [NTFS]\[ro
unny_cat_pictures_pc_2[1].exif.html	Washer 17.E01\Partition 1\WASHER [NTFS]\[ro

Also include

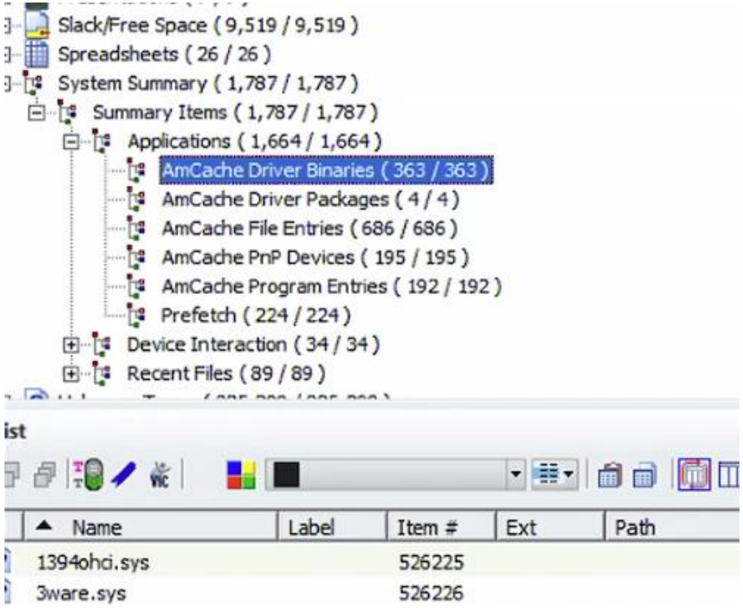
☐ Parent index.dat ☐ Actual Source File

☐ Email Attachments

☐ Parent Email

☑ Child Items

- Overview tab now includes node for a breakout of *System Summary* information parsed from evidence. (FCR-577)



```
Slack/Free Space ( 9,519 / 9,519 )
Spreadsheets ( 26 / 26 )
System Summary ( 1,787 / 1,787 )
  Summary Items ( 1,787 / 1,787 )
    Applications ( 1,664 / 1,664 )
      AmCache Driver Binaries ( 363 / 363 )
      AmCache Driver Packages ( 4 / 4 )
      AmCache File Entries ( 686 / 686 )
      AmCache PnP Devices ( 195 / 195 )
      AmCache Program Entries ( 192 / 192 )
      Prefetch ( 224 / 224 )
    Device Interaction ( 34 / 34 )
    Recent Files ( 89 / 89 )
```

Name	Label	Item #	Ext	Path
1394ohci.sys		526225		
3ware.sys		526226		

- System summary items can now be reported as normal objects using labelling, bookmarking etc. or can also be exported as “Export File List Info”.

Exports

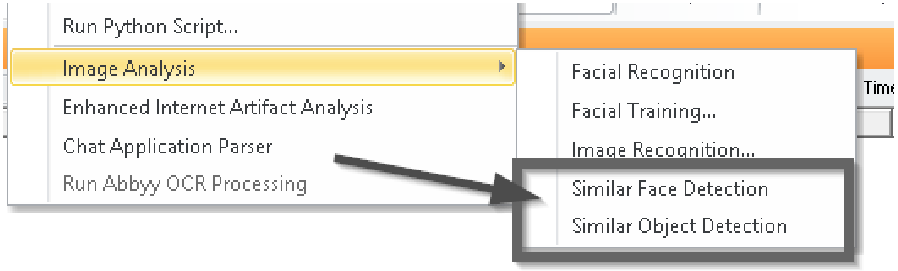
- Load file exports are now configurable to support native files greater than 50MB in size. (FCR-25)
- Control the maximum size of files included in a portable case export.

  To configure this, edit the value argument in the following key of the ADG.WeblabSelfHost.exe.config file:

  ```
  <add key="MaxFileSizeForBreadViewerInMB" value="2000" />
  ```

Image Recognition

- Image Analysis tools now include automatic Similar Face and Similar Object detection parsing. (FCR-449)



Installation

- The option to install Compelson components is now available as part of the “Advanced” install path in the Forensic Tools Suite installation wizard. (FCR-438)

  NOTE: Compelson components are not installed by default

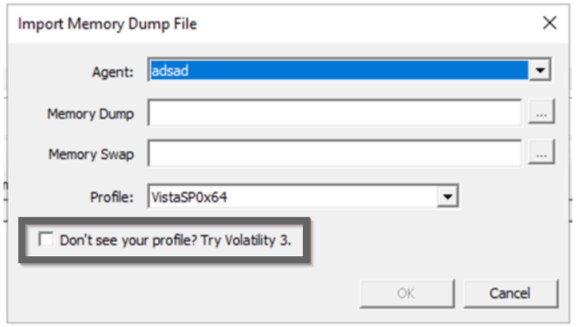
- The Forensic Tools Installer has been refined and simplified to help install all the appropriate components depending on the product being installed. Additionally, the Quin-C service can now be installed on a central server as appropriate. (FCR-439)
- The Quin-C service can now be configured to run as a specified Windows user’s credentials. (FCR-809)

Memory Dump Analysis

- The Volatility framework integration has been updated to version 3. (FCR-48 / FCR-506)

  Volatility Analysis of Imported Memory Dump Files
  The new check box shown below allows you to enable Volatility 3 as appropriate.

For system profiles that are not listed, mark the “Don’t see your profile? Try Volatility 3.” checkbox:



Import Memory Dump File

Agent: adsad

Memory Dump

Memory Swap

Profile: VistaSP0x64

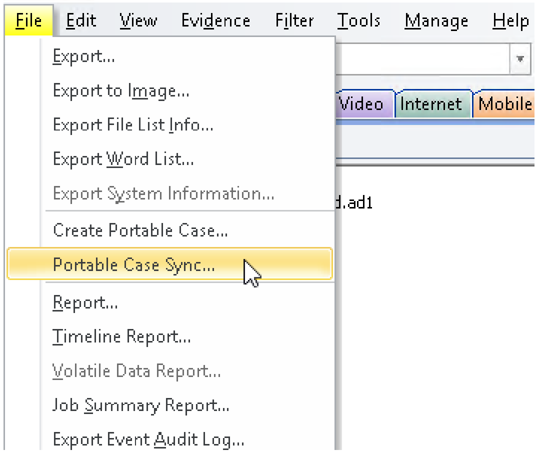
☐ Don't see your profile? Try Volatility 3.

Mobile

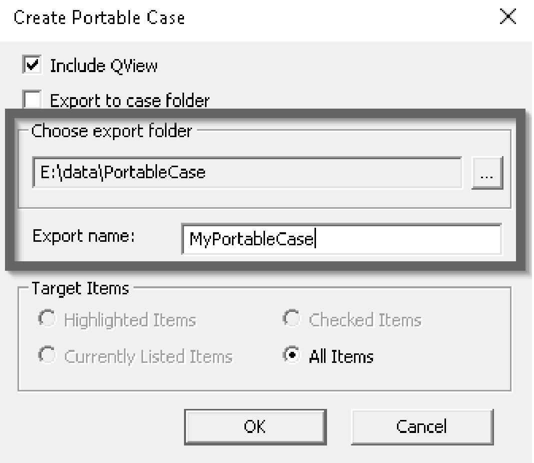
- Updated support for parsing Cellebrite UFDR version 7.34 and above. (FCR-411)

Portable Case (QView Offline)

- The changes made to labels, bookmarks, bookmark comments, and notes made in the Portable Case interface can now be synchronized back to the case in FTK. (FCR-85)



- When exporting case data for review in QView Offline interface, you now have the option to define a custom path and the name of the portable case data archive file. (FCR-303 / FCR-313)


Create Portable Case

☑ Include QView

□ Export to case folder

Choose export folder: E:\data\PortableCase

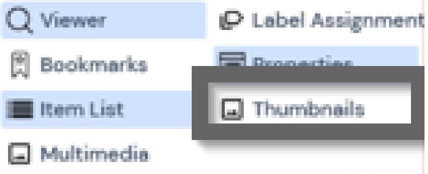
Export name: MyPortableCase

Target Items

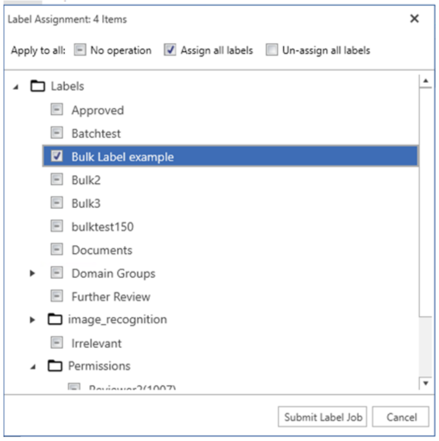
○ Highlighted Items ○ Checked Items

○ Currently Listed Items ● All Items

- QView Offline interface now features:
  - Graphic thumbnail panel. (FCR-307)



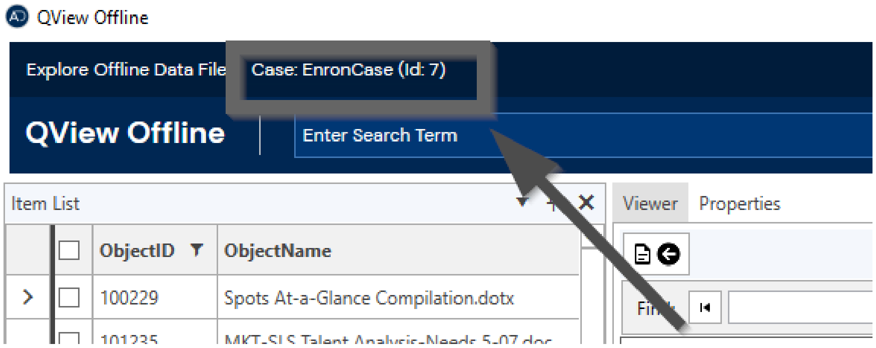
  - Options to Create / Delete Labels and Bookmarks. (FCR-309)
  - Bulk Bookmark and bulk labeling options are now available via the right-click context menu in grid. (FCR-308)


Label Assignment: 4 Items

Apply to all: ⊟ No operation ☑ Assign all labels □ Un-assign all labels

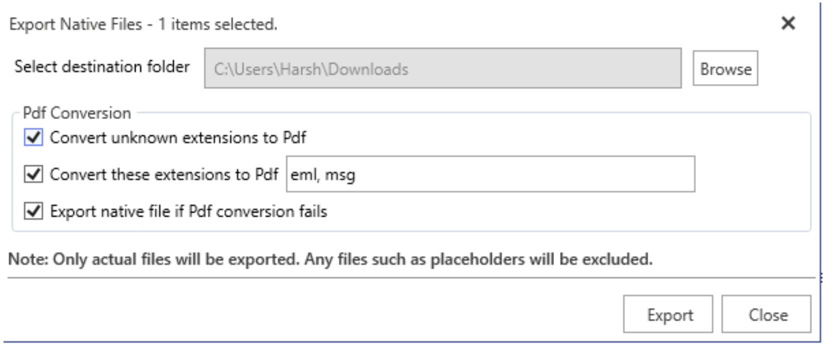
- Labels
  - ⊟ Approved
  - ⊟ Batchtest
  - ☑ Bulk Label example
  - ⊟ Bulk2
  - ⊟ Bulk3
  - ⊟ bulktest150
  - ⊟ Documents
  - ⊟ Domain Groups
  - ⊟ Further Review
  - image_recognition
  - ⊟ Irrelevant
  - Permissions
    - ⊟ Reviewer2(1007)

- ○ The name of the case from which the data was loaded into the interface. (FCR-629)



	ObjectID	ObjectName
> □	100229	Spots At-a-Glance Compilation.dotx
□	101235	MKT-SLS Talent Analysis-Needs 5-07.doc

- ○ You can now save your preferred layout(s) for use in the QView Offline interface. (FCR-631)
- ○ Ability to convert files to “pdf” when exporting from QView Offline.


Export Native Files - 1 items selected.

Select destination folder: C:\Users\Harsh\Downloads   Browse

Pdf Conversion

☑ Convert unknown extensions to Pdf

☑ Convert these extensions to Pdf: eml, msg

☑ Export native file if Pdf conversion fails

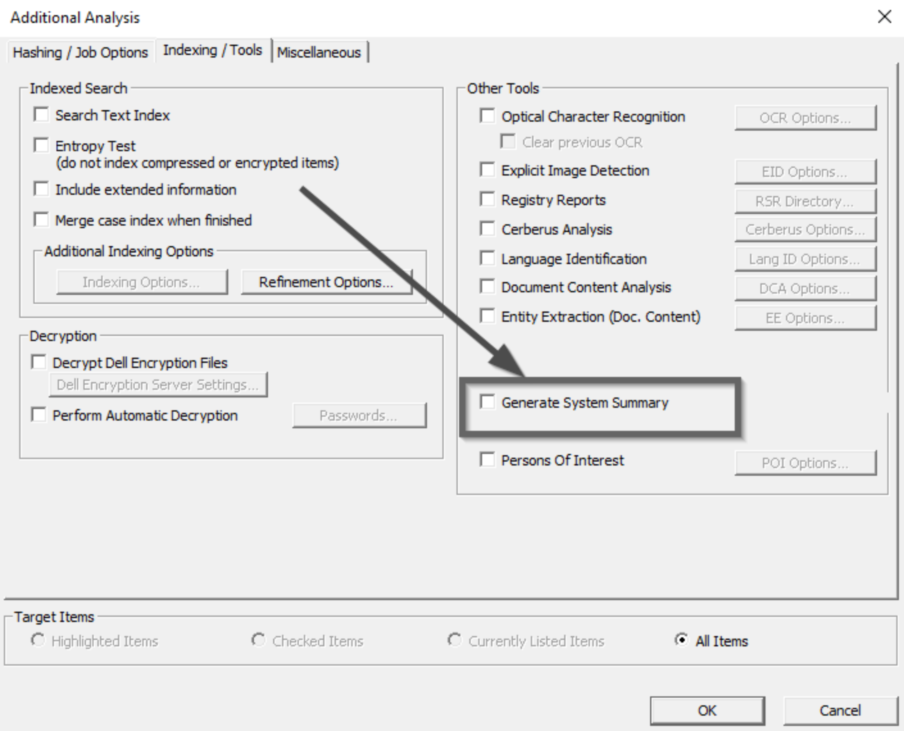
Note: Only actual files will be exported. Any files such as placeholders will be excluded.

Processing

- Greatly enhanced Windows System Summary information parsing. (FCR-578)

  See ***Appendix B*** for detail on supported artifact categories.

  Important: In order to index search the parsed Windows System Summary Information data, you must run a separate indexing job via Additional Analysis in addition to the index created when the data was ingested. (FCR-807 / FCR-1010)



Additional Analysis

Hashing / Job Options | Indexing / Tools | Miscellaneous

Indexed Search
□ Search Text Index
□ Entropy Test
(do not index compressed or encrypted items)
□ Include extended information
□ Merge case index when finished

Additional Indexing Options
Indexing Options... | Refinement Options...

Decryption
□ Decrypt Dell Encryption Files
Dell Encryption Server Settings...
□ Perform Automatic Decryption | Passwords...

Other Tools
□ Optical Character Recognition | OCR Options...
□ Clear previous OCR
□ Explicit Image Detection | EID Options...
□ Registry Reports | RSR Directory...
□ Cerberus Analysis | Cerberus Options...
□ Language Identification | Lang ID Options...
□ Document Content Analysis | DCA Options...
□ Entity Extraction (Doc. Content) | EE Options...
□ Generate System Summary
□ Persons Of Interest | POI Options...

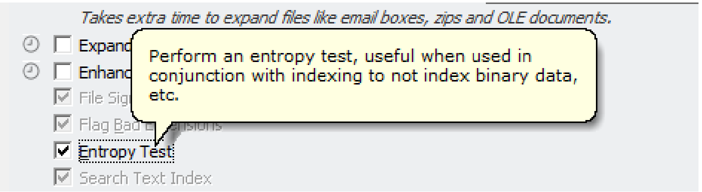
Target Items
○ Highlighted Items ○ Checked Items ○ Currently Listed Items ● All Items

OK | Cancel

- EXIF data is now parsed into metadata columns for use in the grid to sort, filter, tag, report, etc. (FCR-26 / FCR-154)

EXIF Metadata Columns Parsed	
Name	Exif datetimedigitized
Exif datetime	Exif Make
Exif Model	Lat.
Long	L-Size
Path	Duplicate File
Created	Modified

- Improved tooltips for evidence processing options (hover your mouse over the option. (FCR-102)



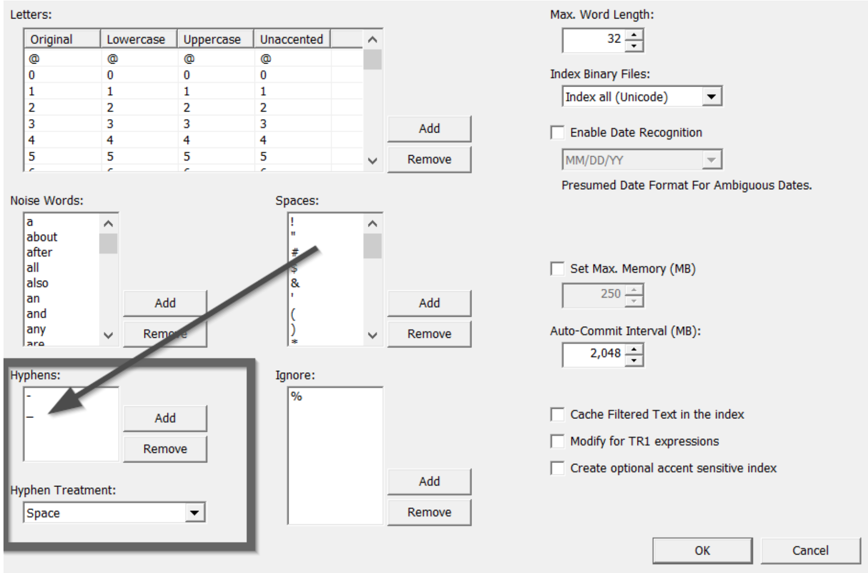
Takes extra time to expand files like email boxes, zips and OLE documents.

□ Expand
□ Enhanc
☑ File Sig
☑ Flag Bad ... ensions
☑ Entropy Test
☑ Search Text Index

Perform an entropy test, useful when used in conjunction with indexing to not index binary data, etc.

- The Evidence Processing Profile manager's Indexing Options dialog now lists the underscore character ("_") in the *Hyphens* character box. Therefore underscore characters are now indexed as a space character (" ") by default. (FCR-103)

  Note: Words in text that are joined by an underscore will be indexed as two separate words by default. The way hyphen characters are treated can be overridden by selecting an option from the *Hyphen Treatment* drop-down.



Letters:

Original	Lowercase	Uppercase	Unaccented
@	@	@	@
0	0	0	0
1	1	1	1
2	2	2	2
3	3	3	3
4	4	4	4
5	5	5	5

Noise Words: a, about, after, all, also, an, and, any

Spaces: ! " # $ & ' ( )

Hyphens: - –

Hyphen Treatment: Space

Ignore: %

Max. Word Length: 32

Index Binary Files: Index all (Unicode)

□ Enable Date Recognition

MM/DD/YY

Presumed Date Format For Ambiguous Dates.

□ Set Max. Memory (MB)

250

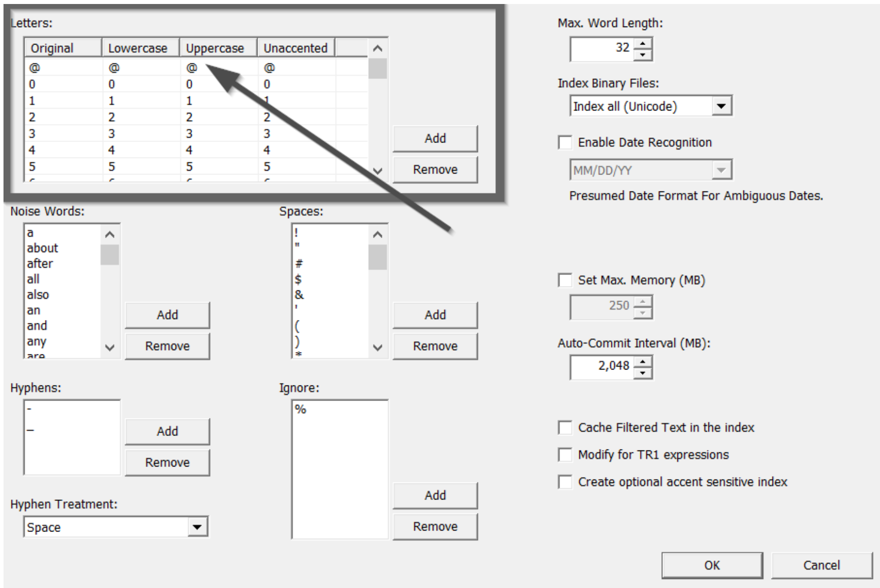
Auto-Commit Interval (MB): 2,048

□ Cache Filtered Text in the index

□ Modify for TR1 expressions

□ Create optional accent sensitive index

- The at ("@") symbol is now indexed by default and is listed among the *Letters* characters in the processing profile *Indexing Options* dialog. (FCR-160)



Letters:

Original	Lowercase	Uppercase	Unaccented
@	@	@	@
0	0	0	0
1	1	1	1
2	2	2	2
3	3	3	3
4	4	4	4
5	5	5	5

Noise Words: a, about, after, all, also, an, and, any

Spaces: ! " # $ & ' ( )

Hyphens: - –

Hyphen Treatment: Space

Ignore: %

Max. Word Length: 32

Index Binary Files: Index all (Unicode)

□ Enable Date Recognition

MM/DD/YY

Presumed Date Format For Ambiguous Dates.

□ Set Max. Memory (MB)

250

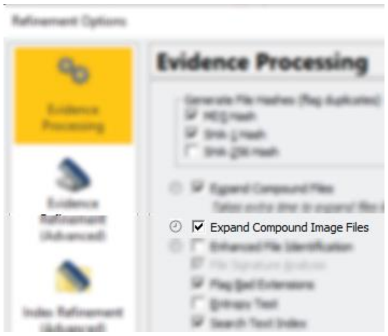
Auto-Commit Interval (MB): 2,048

□ Cache Filtered Text in the index

□ Modify for TR1 expressions

□ Create optional accent sensitive index

- "Expand Compound Image Files" option is now automatically selected when the option to expand AFF4 is selected from the "Expand Compound Files" menu. [FCR-361)



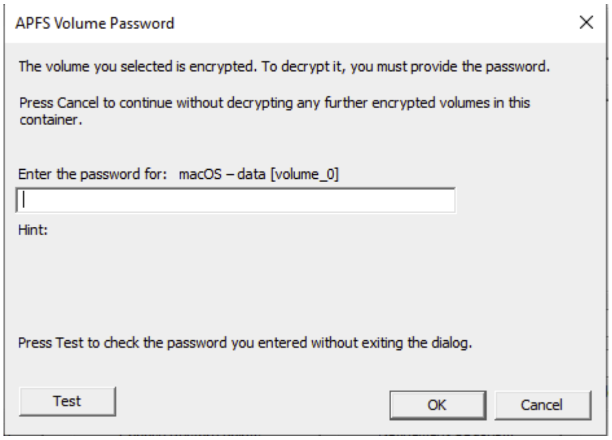
Refinement Options

Evidence Processing

Generate File Hashes (Flag duplicates)
☑ MD5 Hash
☑ SHA-1 Hash
☐ SHA-256 Hash

☑ Expand Compound Files
Takes extra time to expand files
☑ Expand Compound Image Files
☐ Enhanced File Identification
☑ File Signature Analysis
☑ Flag Bad Extensions
☐ Entropy Test
☑ Search Text Index

- HTML styling for System Summary items has been redesigned to be consistent with other HTML pages within the application. (FCR-852)
- FileVault 2 Decryption (APFS) support. Users can now import non-T2 MAC based images and FTK will prompt for FileVault2 encryption. (FCR-596)



APFS Volume Password

The volume you selected is encrypted. To decrypt it, you must provide the password.

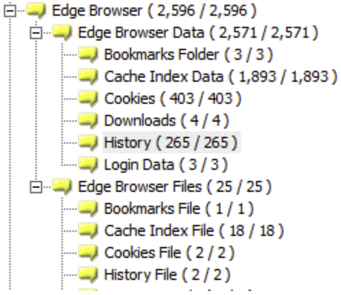
Press Cancel to continue without decrypting any further encrypted volumes in this container.

Enter the password for: macOS – data [volume_0]

Hint:

Press Test to check the password you entered without exiting the dialog.

- Faster processing of AFF4 image files. (FCR-796)
- New column displays number of words OCR'ed for each file object. (FCR-853)
- Support for parsing Microsoft Edge (Chromium platform) data. (FCR-481)



- Edge Browser (2,596 / 2,596)
  - Edge Browser Data (2,571 / 2,571)
    - Bookmarks Folder (3 / 3)
    - Cache Index Data (1,893 / 1,893)
    - Cookies (403 / 403)
    - Downloads (4 / 4)
    - History (265 / 265)
    - Login Data (3 / 3)
  - Edge Browser Files (25 / 25)
    - Bookmarks File (1 / 1)
    - Cache Index File (18 / 18)
    - Cookies File (2 / 2)
    - History File (2 / 2)

- The functionality of the "Generate System Information" processing options are now known as "Generate System Summary".

Reports

- The file name of screen captures included in a report can now be renamed as part of the Report Options. (FCR-589)

Viewer

- Video files now default to 720 lines of resolution in the multimedia viewer. (FCR-581)

Fixed Issues in 7.4.2

The following items have been fixed in this release:

Case Examiner

- Fixed the issue where the column setting you selected would revert to a previous value when you click to open a different node on the Overview Tab. (FCR-598 / FCR-599)

Database

- Case backups taken from an FTK system connected to PostgreSQL, can now be successfully restored to a FTK system connected to MSSQL. (FCR-111)

  NOTE: Any strings that exceed the maximum length supported by MSSQL for that field, will be truncated as part of the restore process.
- Resolved the issue where case Attach / Restore would fail when mapping multiple users to a single user due to the multiple users having made selections on the same objects. (FCR-113 / FCR-476)
- The issue that caused "Copy Previous Case" to not list cases created in an older version to be listed has been addressed. (FCR-184)
- The "Archive and Detach" function will no longer detach a case from the database if the creation of the case archive fails. (FCR-286)
- Fixed issue that would break new case creation in FTK after upgrading to MSSQL 2012 to MSSQL 2019. (FCR-452)
- The “ValidatePermissionsAndVersion” function of the DBconfig utility has been updated to properly validate the database user permissions and schema versions. (FCR-472)

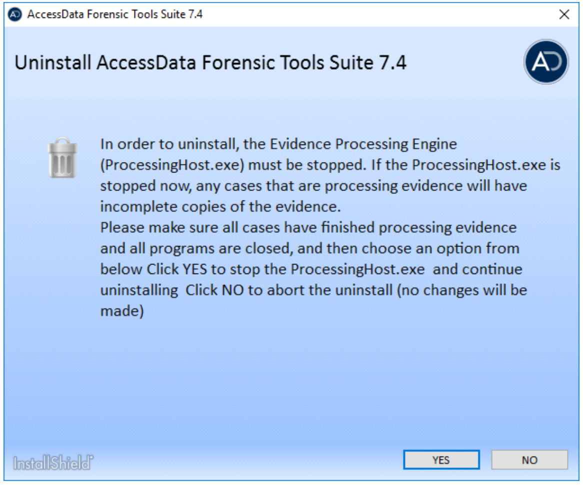
Export

- Fixed the issue causing load files to export with incorrect DocID and missing the metadata for the selected fields. (FCR-91 / ER-70)
- The “All Highlighted” option is now available when exporting graphic thumbnails from the right-click context menu. (FCR-99)
- Fixed the Load file export failure caused by systems with a database configuration XML that did not have any of the database connection records flagged as the default. (FCR-112)
- The Live Search results pane export option *Export to File >> All Hits to Term* now successfully exports the data as expected. (FCR-114)

Installation

- Forensic Tools Suite Installation wizard no longer allows the user to skip the validation of the service account credentials (invalid credentials would cause the Quin-C service to fail to start). (FCR-115)
- If ProcessingHost.exe is still running at the time that the FTK Tools Suite v7.4 is being uninstalled, the following message will appear and the user can choose whether to force the process to

terminate or let it run to completion before completing the uninstall process. (FCR-126)



AccessData Forensic Tools Suite 7.4

Uninstall AccessData Forensic Tools Suite 7.4

In order to uninstall, the Evidence Processing Engine (ProcessingHost.exe) must be stopped. If the ProcessingHost.exe is stopped now, any cases that are processing evidence will have incomplete copies of the evidence.
Please make sure all cases have finished processing evidence and all programs are closed, and then choose an option from below Click YES to stop the ProcessingHost.exe and continue uninstalling Click NO to abort the uninstall (no changes will be made)

KFF

- When importing ProjectVIC 2.0 hashes to the KFF, the hash values now appear as expected. (FCR-97)
- Fixed the issue that caused certain hash file formats from successfully importing to the KFF. Supported KFF formats include:

Format	File Extension	Notes
XML	.xml	
KFF	.kff	
HKE	.hke	
HDB	.hdb	
HASH	.hash	Sometimes ends with "hash.txt"
CSV	.csv	
TSV	.tsv	
NSRL	nsrl.txt	NSRL files must be imported via the KFF Import Utility

Mount Image to Drive

- The issue that caused the Mount Image to Drive function to fail with error “Installation of drive mapping drivers failed.” when mounting certain images, has been resolved. (FCR-104)

Portable Case (QView Offline)

- The issue preventing certain media files from displaying in the *QView Offline* viewer has been resolved. (FCR-246)
- Selected object from Item List is now being highlighted in the Thumbnails panel (FCR-367)
- Export option "All Selected" has been replaced with "All Highlighted" (FCR-398)

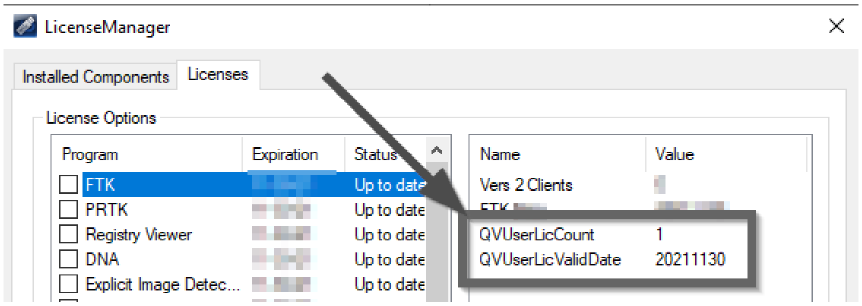
Processing

- Faster UFDR processing – Evidence processor has been updated to parse UFDR files 40% faster than earlier versions. (QC2-21)
- Improved the tooltip description for the *Metacarve* processing option (FCR-107)
- Significant speed improvement to the processing of AFF4 images. (FCR-123 / FCR-597)
- Updated user guide documentation on the use of Yara rules in Cerberus analysis. (FCR-138)
- RestorePoints/VSC now processing correctly whenever three or more submitted for processing at the same time. (FCR-451)
- System Information section now populates data properly when evidence processed into case includes Volume Shadow Copy (VSC) data. (FCR-453)
- Improved handling for parsing System Information data from evidence images. (FCR-454)
- Volumes with an exFAT file system and formatted with the following cluster sizes can now be parsed correctly. (FCR-473 / FCR-538)
    - 64KB
    - 128KB
    - 512KB
    - 1024KB
    - 2048KB
    - 4096KB
    - 8192KB
    - 16384KB
    - 32768KB
- Fixed the issue that prevented DPEs from processing data when added to the DPM configuration on-the-fly (meaning without having to restart the DPM service). (FCR-522)
- Resolved the issue where the Languages box would be empty in the OCR Options dialog. (FCR-524)

  The user will now be prompted with a message whenever an OCR engine is not detected or if the OCR engine does not have any languages to populate in the list.

Quin-C / QView Integration

- One QView license included with every FTK license. (FCR-64 / FCR-391)
    - Notes Per License Dongle:
        - **New Dongle:** 1 free QView license automatically included per FTK license
        - **Existing Dongle:** Free QView license already added to dongle.
          NOTE: You must refresh the dongle to receive the updated license.
    - Notes Per Product:
        - **FTK Environments (Just 1 license on dongle):** QView will only work on the machines where FTK is running.
        - **Lab / Enterprise Environments (more than 1 FTK licenses)**: QView will look at the number of users licensed and then provide the ability to users to run it from multiple machines.
            - For example, if there are 5 users licensed to a dongle, there can be only 5 running instances of QView at one time.
                - If a user opens QView with same username on different machines, QView will terminate the first user session after 10 minutes.
    - Example of QView License

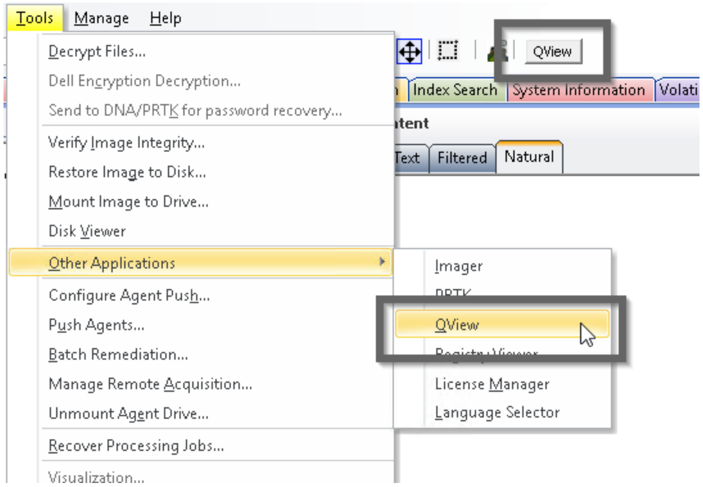


Program	Expiration	Status
□ FTK	[redacted]	Up to date
□ PRTK	[redacted]	Up to date
□ Registry Viewer	[redacted]	Up to date
□ DNA	[redacted]	Up to date
□ Explicit Image Detec...	[redacted]	Up to date

Name	Value
Vers 2 Clients	[redacted]
FTK [redacted]	[redacted]
QVUserLicCount	1
QVUserLicValidDate	20211130

- QView can be launched either via the toolbar button or via the **Tools** >> **Other Applications** list. (FCR-109 / FCR-304)

  Note: The Tools menu option to launch QView now appears greyed out and the launch QView button does not appear if QView is not installed.



- FTK features that depend on QView or the Quin-C service will now present an error and notify the user whenever the dependency is unavailable. (FC-782 / FCR-248 / FC-833)

Search

- Resolved the issue causing a SQL deadlock error related to concurrent index searches. (FCR-90)

Processing

- APFS encrypted AFF4 images now process correctly. (FCR-89)
- Restore points are now properly detected from within Bitlocker encrypted volumes. (FCR-240)
- For searches that detect more than 250k hits in a single file, FTK will display a prompt recommending to instead use the dtSearch “xfilter syntax” for those search terms. (FCR-570)

  See: https://support.dtsearch.com/webhelp/dtsearchcppapi/File_Conditions.html

- Fixed an issue that returned a "The local processing engine is disabled" error when using the “Expand Compound Image Files” additional analysis processing option. (FCR-846)
- The issue that caused embedded PDF files to be parsed with BIN file extension has been resolved. (FCR-733)
- Fixed an issue that caused processing to stall during “Database Optimization” phase. (FCR-819)
- The issue that would cause “Error: The local processing engine is disabled” when processing AFF4 images has been resolved. (FCR-846)

Upgrades

- When connecting 7.4 to an existing evidence database, the user is notified if the database account credentials, they entered are invalid. (CRI-254)

User Interface

- Tab Filters are now persistent across opened case sessions. (FCR-254)
- Fixed issue related to launching QView from the desktop shortcut. (FCR-674)
- Column template drop-down has been resized to accommodate longer template names. (FCR-792)

- Windows System Information Parser now writes log to the following file path. (FCR-787)

  ```
  {ALLUSERSPROFILE}\Documents\AccessData\AccessDataLogs\WindowsParser.txt
  ```

- Users without permission to launch QView are not able to launch QView from toolbar button. (FCR-842)

Important Information

Supported Platforms

Operating Systems Support

The following Windows operating systems are supported:

Operating System Version	FTK Tools Suite Platform	AccessData Agent Endpoint	Volatile Data Target
Windows 7 (x64)	Not Supported	Supported	Supported
Windows 8 (x64)	Not Supported	Supported	Supported
Windows 8.1 (x64)	Not Supported	Supported	Supported
Windows 8.1 Update 1 (x64)	Not Supported	Supported	Supported
Windows 10 v1709 (x64)	Supported	Supported	Supported
Windows 10 v1809 (x64)	Supported	Supported	Supported
Windows 10 v1909 (x64)	Supported	Supported	Supported‡
Windows 10 v2004 (x64)	Supported	Supported	Supported‡
Windows 10 v20H2 (x64)	Supported	Supported	Supported‡
Windows Server 2008 and 2008R2	Not Supported	Supported	Supported
Windows Server 2012	Not Supported	Supported	Supported
Windows Server 2012R2	Supported	Supported	Supported
Windows Server 2016	Supported	Supported	Supported
Windows Server 2019	Supported	Supported	Supported
Windows Crash Dump (x64)	n/a	n/a	Supported
Linux Ubuntu 17	Not Supported	Supported	Supported
Linux Ubuntu 18	Not Supported	Supported	Supported
Linux Ubuntu 19	Not Supported	Supported	Supported
Linux Ubuntu 20	Not Supported	Supported	Not Supported
Red Hat Enterprise Linux 7.0	Not Supported	Supported	Supported
Red Hat Enterprise Linux 7.2	Not Supported	Supported	Supported
Red Hat Enterprise Linux 7.3	Not Supported	Supported	Supported
Red Hat Enterprise Linux 7.6	Not Supported	Supported	Supported
Red Hat Enterprise Linux 7.7	Not Supported	Supported	Supported
Red Hat Enterprise Linux 8.2	Not Supported	Supported*	Supported
Mac OS X 10.9 (Mavericks)	Not Supported	Supported	Supported
Mac OS X 10.10 (Yosemite)	Not Supported	Supported	Supported
Mac OS X 10.11 (El Capitan)	Not Supported	Supported	Supported
Mac OS X 10.12 (Sierra)	Not Supported	Supported	Supported
macOS 10.13 (High Sierra)	Not Supported	Supported	Not Supported
macOS 10.14 (Mojave)	Not Supported	Supported	Not Supported
macOS 10.15 (Catalina)	Not Supported	Supported	Not Supported
macOS 11.0 (Big Sur)	Not Supported	Supported	Not Supported

* = See ***Known Issues in 7.4*** ‡ = Requires Volatility 3

See the AD System Implementation Guide at

https://support.accessdata.com/hc/en-us/sections/200667399-System-Specification-Guides

Microsoft SQL Server Support

The following SQL databases are supported:

- SQL Server 2012
- SQL Server 2014
- SQL Server 2016
- SQL Server 2019

PostgreSQL Support

The following versions of PostgreSQL are supported:

- 9.6.3.5
- 11.2 (this is the version provided with the installation files)

For Additional Information

Latest Documentation

The documentation is sometimes updated. For the latest documentation, see the product download page:

http://accessdata.com/product-download

or download the zip file from

http://www.accessdata.com/productdocs/ftk/ftk.zip

Installation and Upgrade

- The FTK Suite (FTK, AD Lab, AD Enterprise) no longer supports multiple products of the same version running on the same machine at the same time. The user can only install one of the three products of a specific version on a single machine. (29786, 30927)
- All licensed AccessData applications require CodeMeter Runtime to be installed local to the system where the license information will be retrieved (this includes NLS client systems).

Cloud Based Relational Database Services (RDS) Support

The AccessData Suite can utilize the power and scale of the Amazon Aurora PostgreSQL Compatible Cloud Database Service

AWS Aurora is an Amazon proprietary service that is wire compatible with PostgreSQL offering up to 5x faster than a traditional PostgreSQL instance.

To use the amazon RDS Instance, you will need to set up your instance in your AWS console prior to installing the AccessData Suite. When configuring your RDS instance, make sure that the DB engine version for your instance is PostgreSQL 11.4 or higher.

You will have two options: set a password for the “postgres” user, or to use IAM Authentication. AccessData’s Forensic Tools Suite will not work with IAM Authentication. So make sure you keep track of the password set for your “postgres” user for future reference.

Important: AccessData recommends not making the Database "Publicly accessible" for security reasons. If using a VPN to connect to your cloud provider, you will need to update the rules for your security group to allow connections over your VPN.

AD Product Virtualization and Cloud Guidelines

Overview

This support KB article contains a document that outlines the support boundaries and procedures for supporting virtualized and cloud environments for AccessData software:

https://support.accessdata.com/hc/en-us/articles/360009043514-Virtualization-and-AD-Products

Running PostgreSQL on a Virtual Machine

If you run PostgreSQL on a virtual machine with a dynamically allocated virtual hard drive, you must manually stop the PostgreSQL service before rebooting the virtual machine. Otherwise, PostgreSQL will become corrupted.

If you run PostgreSQL on a virtual machine with a fixed size virtual hard drive, then PostgreSQL will not become corrupted when rebooting.

This does not apply to PostgreSQL instances hosted in a managed database service such as AWS Relational Database Service™.

Linux Agent Support

- Official Support for Red Hat Linux 6.x and 7.x
  The 6.2 Linux Agent requires GLIBC 2.17 or newer. Collection from a system running on 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: Idd -version.

KFF

- The KFF Server uses the Apache Cassandra database. The version of Cassandra being used requires 64-bit Java 8. No other version of Java (7 or 9) is currently supported.
  - To install Java, go to: https://java.com/en/download/windows-64bit.jsp

    - If you are using a 32-bit browser, your browser may automatically download the 32-bit version. You must use the 64-bit version.
- Make sure that you use the latest version of the KFF Server.
  See https://accessdata.com/product-download > Known File Filter 5.6 and up.
- When importing data using the KFF Import Utility, make sure that you get a confirmation that the import is complete before processing data using that KFF data. This is particularly important when importing NSRL data that takes several hours to import.
- Only the Project VIC and NSRL sets are locked/protected. All other sets in the KFF can be modified and archived.

Recommendations

- Cerberus writes binaries to the AD Temp folder momentarily in order to perform the malware analysis. Upon completion, it will quickly delete the binary. It is important to ensure that your antivirus is not scanning the AD Temp folder. If the antivirus deletes/quarantines the binary from the temp, Cerberus analysis will not be performed.
- When creating a Custom Data View, the available filter list should not include: Checked Files, Unchecked Files (checked status is not available across users), Bookmarked Files, Labeled Files (too broad and will include all bookmarks or labels). These filters have been removed from the list. (6533)

Known Issues in 7.4.2

Case Examiner

- Importing a memory dump from a Windows 10 v1709 system can cause FTK to crash. (FCR-604)
- The Column Template drop-down field does not always display correctly when the list of columns is exceedingly large. (FCR-792)

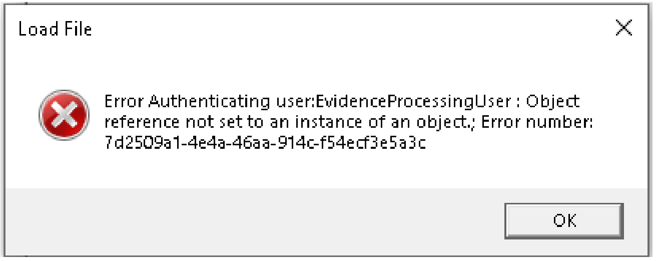
Database

- In the DBconfig.exe utility, marking the *Default* check box does not actually update the corresponding fields in the XML configuration file. (CRI-610)

Export

- Load file exports from systems with connections to more than one database instance may result in the following error message. (FCR-353)

  Load File
  Error Authenticating userEvidenceProcessingUser : Object reference not set to an instance of an object…

  Load File

  Error Authenticating user:EvidenceProcessingUser : Object reference not set to an instance of an object.; Error number: 7d2509a1-4e4a-46aa-914c-f54ecf3e5a3c

  Workaround: Close FTK application completely and try again after relaunching FTK.
- When exporting item parsed from a PST archive into AD1 format, the exported data may be unreadable. (FCR-799)

  Workaround: Export the data to AD1 using QView.

Installation

- The Distributed Processing Manager (DPM) and Distributed Processing Engine (DPE) installers don't automatically install the Microsoft .NET Framework 4.7.2. However, the Microsoft .NET 4.7.2 Framework is required in order to run distributed processing. (CRI-611)

Portable Case (QView Offline)

- QView Offline will fail to launch if the name of the portable case data name includes certain special characters. (FCR-611)

  Workaround: Rename the portable case data using a name that does not contain special characters.

Processing

- NTFS volumes formatted with 128 KB, 256 KB, 512 KB, 1024 KB, or 2048 KB cluster sizes are not supported. (FCR-473)
- HTML tags are not properly indexed. (FCR-630)

Search

- For email headers fields that contain custom fields key/value pairs, the way the data is stored has been updated to accommodate long length strings. (FCR-263)

  Note: The email header key/value pair metadata is included in the search index using FTK. However, to export the metadata, AccessData recommends to use Quin-C.

Upgrades

- Connecting a version 7.3 (or newer) Forensic Tools application to a database in use by eDiscovery 7.1.1 will cause the 7.3 application to attempt to automatically upgrade case schemas. AccessData eDiscovery 7.1.1 can only be integrated with applications that shipped with Forensic Tools 7.1.

Appendix A

The following is a list of mappings between built-in FTK filters and automatic column settings.

Here are the mappings:

Filters	Columns
Documents	Documents
Email	Email
Chat Messages	Messages
Chat Conversations	Mobile Chats/Conversations
Media	General
Graphics	Graphics
Video	Video
Audio	Audio
Geo-Location (Country & City)	Location
OS/System/Apps	General
Encryption Files	General
Others	General
KFF	KFF
Mobile	General
Mobile Phone Files	General
Mobile App Usage	Mobile App Usage
Bluetooth Device	Bluetooth
Calendar Item	Calendar
Calls	Calls
Contact	Contact
Cookies	Cookie
Device Location	Device Location
Installed App	Installed App
MMS Message	MMS
Notes	Notes
Other Phone Items	Other Phone Item
Password	Password
Searches	Search
User Account	User Account
User Dictionary	User Dictionary
VoiceMail	Voicemail
Web History	Web History
Wireless Network	Wireless Network

Appendix B

The following tables lists the categories and sub-categories of the Extended System Information parsing processing option.

Category	Sub Categories
Applications	Installed
	Prefetch
	User Assist
	AmCache Driver Binaries
	AmCache Driver Packages
	AmCache File Entries
	AmCache PnP Devices
	AmCache Program Entries
	AutoRun Items
	StartUp Items
	System Services
	Shim Cache
Device Interaction	USB Devices
	AmCache Device Containers
Browsers	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 Shares
	Network Connections
	Wireless Profiles
	Network Interfaces
Recent Files/Folders	Keyword Searches
	Shortcuts (LNK)
	Jump List

	AmCache Shortcuts
	MRU Run Commands
	MRU Recent Files & Folders
	MRU Recent Open/Saved Files
	MRU Folder Access
	Shell Bags
File System Information	Volumes
	Disk List
Operating System Information	Owner Information
	Timezone Information
	User Accounts
	Group Accounts
	Windows Notifications Center
	Windows Timeline Activity
	Rebuilt Desktops
SRUM	SRUM Network Connections
	SRUM Network Usage
	SRUM Push Notifications

Comments?

We value all feedback from our customers. Please contact us at support@accessdata.com, or send documentation issues to documentation@accessdata.com.

AccessData Legal Information

Document date: February 1, 2021

Legal Information

©2020 AccessData Group, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

AccessData Group, Inc. makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, AccessData Group, Inc. reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, AccessData Group, Inc. makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, AccessData Group, Inc. reserves the right to make changes to any and all parts of AccessData software, at any time, without any obligation to notify any person or entity of such changes.

You may not export or re-export this product in violation of any applicable laws or regulations including, without limitation, U.S. export regulations or the laws of the country in which you reside.

AccessData Group, Inc.
603 E. Timpanogos Circle
Building H
Orem, UT 84097 USA

AccessData Trademarks and Copyright Information

The following are either registered trademarks or trademarks of AccessData Group, Inc. All other trademarks are the property of their respective owners

.

AccessData®

AccessData Certified Examiner® (ACE®)

AD AccessData™

AD eDiscovery®

AD RTK™

LawDrop®

AD Summation®

Discovery Cracker®

Distributed Network Attack®

DNA®

Forensic Toolkit® (FTK®)

Summation®

Mobile Phone Examiner Plus®

MPE+ Velocitor™

Password Recovery Toolkit®

PRTK®

Registry Viewer®

A trademark symbol (®, ™, etc.) denotes an AccessData Group, Inc. trademark. With few exceptions, and unless otherwise notated, all third-party product names are spelled and capitalized the same way the owner spells and capitalizes its product name. Third-party trademarks and copyrights are the property of the trademark and copyright holders. AccessData claims no responsibility for the function or performance of third-party products.

Third party acknowledgements:

- AFF® and AFFLIB®   Copyright® 2005, 2006, 2007, 2008 Simson L. Garfinkel and Basis Technology Corp. All rights reserved.
  Copyright © 2005 - 2009 Ayende Rahien
- FreeBSD ® Copyright 1992-2011. The FreeBSD Project.
- BSD License:
  Copyright (c) 2009-2011, Andriy Syrov. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer; Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution; Neither the name of Andriy Syrov nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
- WordNet License:
  This license is available as the file LICENSE in any downloaded version of WordNet.
- WordNet 3.0 license: (Download)
  WordNet Release 3.0 This software and database is being provided to you, the LICENSEE, by Princeton University under the following license. By obtaining, using and/or copying this software and database, you agree that you have read, understood, and will comply with these terms and conditions.: Permission to use, copy, modify and distribute this software and database and its documentation for any purpose and without fee or royalty is hereby granted, provided that you agree to comply with the following copyright notice and statements, including the disclaimer, and that the same appear on ALL copies of the software, database and documentation, including modifications that you make for internal use or for distribution. WordNet 3.0 Copyright 2006 by Princeton University. All rights reserved. THIS SOFTWARE AND DATABASE IS PROVIDED "AS IS" AND PRINCETON UNIVERSITY MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED. BY WAY OF EXAMPLE, BUT NOT LIMITATION, PRINCETON UNIVERSITY MAKES NO REPRESENTATIONS OR WARRANTIES OF MERCHANT- ABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR THAT THE USE OF THE LICENSED SOFTWARE, DATABASE OR DOCUMENTATION WILL NOT INFRINGE ANY THIRD PARTY PATENTS, COPYRIGHTS, TRADEMARKS OR OTHER RIGHTS. The name of Princeton University or Princeton may not be used in advertising or publicity pertaining to distribution of the software and/or database.

Title to copyright in this software, database and any associated documentation shall at all times remain with Princeton University and LICENSEE agrees to preserve same.

- XMLmind XSL-FO Converter Professional Edition Developer License Agreement:
  Distribution
  Licensee may not distribute with the Application any component of the Software other than the binary class library (xfc.jar) for the JavaTM version and the Dynamic Link Library file (xfc.dll) for the .NET version.
  Licensee shall include the following copyright notice: "XMLmind XSL-FO Converter Copyright © 2002-2009 Pixware SARL", with every copy of the Application. This copyright notice may be placed together with Licensee's own copyright notices, or in any reasonably visible location in the packaging or documentation of the Application.
  Licensee may use, distribute, license and sell the Application without additional fees due to Licensor, subject to all the conditions of this License Agreement.
- "Amazon Web Services", "AWS" "AWS Aurora" "AWS Relational Database Service" are trademarks of Amazon.com, Inc. or its affiliates in the United States and/or other countries and is used with permission https://aws.amazon.com/aispl/trademark-guidelines/.
- Apache(r), Apache Cassandra and the flame logo is a registered trademark of the Apache Software Foundation in the United States and/or other countries. No endorsement by the Apache Software Foundation is implied by the use of these marks.