Known File Filter (KFF)

Installation Guide

Version 6.3.x

ACCESSDATA®

AccessData Legal and Contact Information

Document date: November 7, 2017

Legal Information

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.
588 West 400 South Suite 350
Lindon, UT 84042
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®	AD Summation®	Mobile Phone Examiner Plus®
AccessData Certified Examiner® (ACE®)	Discovery Cracker®	MPE+ Velocitor™
AD AccessData™	Distributed Network Attack®	Password Recovery Toolkit®
AD eDiscovery®	DNA®	PRTK®
AD RTK™	Forensic Toolkit® (FTK®)	Registry Viewer®
	LawDrop®	Summation®

Contents

Chapter 1

Getting Started with KFF (Known File Filter)

Introducing KFF

This document contains the following information about understanding and getting started using KFF (Known File Filter) with products 6.3 and later. If you are using products version 6.2 and earlier, refer to that version's documentation.

Important: AccessData applications versions 6.3 and later use a new KFF architecture. If you are using one of the following applications version 6.3 or later, you must install and implement the new KFF architecture:

- Forensics products (FTK, FTK Pro, AD Lab, AD Enterprise)
- Summation
- eDiscovery

See What has Changed in Version 6.3 on page 36.

About the KFF Server and Geolocation

Geolocation (GeoIP) data is used for the Geolocation Visualization feature of several AccessData products.

Important: In versions 6.3 and later, Geolocation data is installed automatically and independently and is no longer tied to KFF.

About KFF

KFF (Known File Filter) is a utility that compares the file hash values of known files against the files in your project. The known files that you compare against may be the following:

- Files that you want to ignore, such as operating system or application files
- Files that you want to be alerted about, such as malware or other contraband files

The hash values of files, such as MD5, are based on the file's content, not on the file name or extension. This helps you identify files even if they are renamed.

Using KFF during your analysis can provide the following benefits:

- Immediately identify and ignore 40-70% of files irrelevant to the project.
- Immediately identify known contraband files.

Introduction to the KFF Architecture

There are two distinct components of the KFF architecture:

- KFF Server - The KFF Server is the component that is used to store and process the KFF data against your evidence. After you install the KFF Server, you import your KFF data into it.

  See Installing the KFF Server on page 9.
- KFF Data - The KFF data are the hashes of the known files that are compared against the files in your project. The KFF data is organized in KFF Hash Sets and KFF Groups. The KFF data can be comprised of hashes obtained from pre-configured libraries (such as NSRL) or custom hashes that you configure yourself.

  See Components of KFF Data on page 5.

Components of KFF Data

Item	Description
Hash	The unique MD5 or SHA-1 hash value of a file. This is the value that is compared between known files and the files in your project.
Hash Set	A collection of hashes that are related somehow. The hash set has an ID, status, name, vendor, package, and version. In most cases, a set corresponds to a collection of hashes from a single source that have the same status.
Group	KFF Groups are containers that are used for managing the Hash Sets that are used in a project. KFF Groups can contains Hash Sets as well as other groups. Projects can only use a single KFF Group. However, when configuring your project you can select a single KFF Group which can contains nested groups.
Status	The specified status of a hash set of the known files which can be either Ignore or Alert. When a file in a project matches a known file, this is the reported status of the file in the project.

Item	Description
Library	A pre-defined collection of hashes that you can import into the KFF Server. You can use the following pre-defined libraries: • NSRL • NDIC HashKeeper • DHS • For law enforcement users, you can also use Project Vic libraries. See About Pre-defined KFF Hash Libraries on page 6.

About the Organization of Hashes, Hash Sets, and KFF Groups

Hashes, such as MD5, SHA-1, etc., are based on the file's content, not on the file name or extension.

You can also import hashes into the KFF Server in **.CSV** format.

For FTK-based products, you can also import hashes into the KFF Server that are contained in **.TSV**, **.HKE**, .**HKE.TXT**, .**HDI**, .**HDB**, .**hash**, **.NSRL**, or .**KFF** file formats.

You can also manually add hashes.

Hashes are organized into Hash Sets. Hash Sets usually include hashes that have a common status, such as Alert or Ignore.

Hash Sets must be organized into to KFF Groups before they can be utilized in a case or project.

About Pre-defined KFF Hash Libraries

There are pre-configured hash sets currently available for KFF that come from federal government agencies and are available in KFF libraries.

See About KFF Pre-Defined Hash Libraries on page 31.

You can use the following KFF libraries:

- NIST NSRL
  See Importing the NIST NSRL Library on page 24.
- NDIC HashKeeper (Sept 2008)
  See Importing the NDIC Hashkeeper Library on page 28.
- DHS (Jan 2008)
  See Importing the DHS Library on page 28.
- For law enforcement users using forensic products, you can also use Project Vic libraries.
  See Using Project VIC on page 286.

It is not required to use a pre-configured KFF library in order to use KFF. You can configure or import custom hash sets. See your application's *Admin Guide* for more information.

How KFF Works

The Known File Filter (KFF) is a body of MD5 and SHA1 hash values computed from electronic files. Some pre-defined data is gathered and cataloged by several US federal government agencies or you can configure you own. KFF is used to locate files residing within project evidence that have been previously encountered by other investigators or archivists. Identifying previously cataloged (known) files within a project can expedite its investigation.

When evidence is processed with the MD5 Hash (and/or SHA-1 Hash) and KFF options, a hash value for each file item within the evidence is computed, and that newly computed hash value is searched for within the KFF data. Every file item whose hash value is found in the KFF is considered to be a known file.

Note: If two hash sets in the same group have the same MD5 hash value, they must have the same metadata. If you change the metadata of one hash set, all hash sets in the group with the same MD5 hash file will be updated to the same metadata.

The KFF data is organized into Groups and stored in the KFF Server. The KFF Server service performs lookup functions.

Status Values

In order to accelerate an investigation, each known file can labeled as either Alert or Ignore, meaning that the file is likely to be forensically interesting (Alert) or uninteresting (Ignore). Other files have a status of Unknown.

The Alert/Ignore designation can assist the investigator to hone in on files that are relevant, and avoid spending inordinate time on files that are not relevant. Known files are presented in the Overview Tab's File Status Container, under "KFF Alert files" and "KFF Ignorable."

Hash Sets

The hash values comprising the KFF are organized into hash sets. Each hash set has a name, a status, and a listing of hash values. Consider two examples. The hash set "ZZ00001 Suspected child porn" has a status of Alert and contains 12 hash values. The hash set "BitDefender Total Security 2008 9843" has a status of Ignore and contains 69 hash values. If, during the course of evidence processing, a file item's hash value were found to belong to the "ZZ00001 Suspected child porn" set, then that file item would be presented in the KFF Alert files list. Likewise, if another file item's hash value were found to belong to the "BitDefender Total Security 2008 9843" set, then that file would be presented in the KFF Ignorable list.

In order to determine whether any Alert file is truly relevant to a given project, and whether any Ignore file is truly irrelevant to a project, the investigator must understand the origins of the KFF's hash sets, and the methods used to determine their Alert and Ignore status assignments.

You can install libraries of pre-defined hash sets or you can import custom hash sets. The pre-defined hash sets contain a body of MD5 and SHA1 hash values computed from electronic files that are gathered and cataloged by several US federal government agencies.

See About KFF Pre-Defined Hash Libraries on page 31.

Higher Level Structure and Usage

Because hash set groups have the properties just described, and because custom hash sets and groups can be defined by the investigator, the KFF mechanism can be leveraged in creative ways. For example, the investigator may define a group of hash sets created from encryption software and another group of hash sets created from child pornography files and then apply only those groups while processing.

About KFF Data Formats

When importing KFF data, you can import the following file formats:

- CSV file format
- Forensics products: .HDB, .HKE, .KFF, .XML, .HASH file formats
- Forensics products used by law enforcement: Project VIC JSON file format

About the CSV Format

When you import or export KFF data, you can import from or export to a CSV format. When you use the .CSV format, you use a single .CSV file at a time. The .CSV file can contain hashes, Hash Sets and KFF Groups that you import or export.

See Components of KFF Data on page 5.

Using the CSV format	
Exporting to CSV format	When you export KFF data using the CSV format, you can export specific pieces of KFF data, such as one or more Hash Sets or one or more KFF Groups. The exported CSV contains the hashes as well as all of the information about any associated Hash Sets and KFF Groups. Each export is contained in one .CSV file. CSV files can be easily viewed and can be manually edited.
Importing from CSV format	When you import a CSV file, the data in the file is data is added to your existing KFF data. The CSV file can be a simple file containing only the hashes of files, or it can contain additional information about Hash Sets and KFF Groups. For example, suppose you manually created four Hash Sets and one KFF Group. That would be the only contents in your *KFF Server*. Suppose you import a .CSV file that contains five hash sets and two KFF Groups. They will be added together for a total of nine Hash Sets and three KFF Groups. To import .CSV files, you can do either of the following: • Use the KFF Import feature in your application. See *Using the Known File Feature* chapter. • Use the stand-alone KFF Import Utility. See Importing KFF Data on page 20.

To view a sample of a .CSV file that contains binaries and Hash Sets and KFF Groups, perform a CSV export and view the file in Excel. You can also use the format of CSV files that were exported in previous versions.

Installing the KFF Server

About Installing the KFF Server

In order to use KFF, you must first install and configure a KFF Server.

- For product versions 6.3 and later, you install a KFF Server by installing Apache Cassandra.
- For product versions 5.6 - 6.2, you install a KFF Server by installing the AccessData Elasticsearch.

Where you install the KFF Server depends on the product you are using with KFF.

See Determining Where to Install the KFF Server on page 11.

About KFF Server Versions

The KFF Server (AccessData Elasticsearch Windows Service) may be updated from time to time. It is best to use the latest version.

Product Version	KFF Server	Released	Installation Instructions
6.3	Apache Cassandra Version 3.11	• October 2017 with 6.3 versions of ▪ FTK-based products ▪ Summation ▪ eDiscovery	See Determining Where to Install the KFF Server on page 11.

About Upgrading from Earlier Versions

If you have used KFF with applications with a previous KFF Server architecture, you can migrate your legacy KFF data to the new architecture.

See Migrating Legacy KFF Data from Previous Versions on page 18.

Process for Installing KFF

The process for installing KFF is as follows:

1. Downloading the Latest KFF Installation Files (page 10)
2. Determining Where to Install the KFF Server (page 11)
3. Installing the KFF Server (page 13)
4. Configuring the KFF Server location:
   - Configuring the KFF Server Location on AD Lab and AD Enterprise (page 15)
   - Configuring the KFF Server Location on Summation or eDiscovery (page 16)
5. (Optional) Upgrading or importing KFF data.
   - See Migrating Legacy KFF Data from versions 5.5 and earlier on page 19.
   - About Importing KFF Data (page 20)
   - Importing Pre-defined KFF Data Libraries (page 23)

Downloading the Latest KFF Installation Files

You can download ISO files which has the latest KFF files. Files may be updated from time to time.

To download the latest KFF Installation Files

1. Go to the AccessData Current Releases - Digital Forensics product download page.
   You can also download the file from the FTK or AD Lab product download pages.
2. Click the following:
   - **Known File Filter (KFF) Compatible with 6.3 and above**.
3. Do one of the following:
   - To download the KFF Server files, and utilities, click **KFF for all 6.3 products**.
   - To download the DHS library, click **KFF DHS**.
   - To download the NDIC library, click **KFF NDIC**.
   - To download the NSRL, you can use files from AccessData or you can access them from www.nist.gov.
     See Importing the NIST NSRL Library Files from AccessData on page 26.
4. Click **Download Now.**

Determining Where to Install the KFF Server

Where you install the KFF Server depends on the application and environment you are running.

- For FTK and FTK Pro applications, the KFF Server **must** be installed on the same computer that runs the FTK Examiner application.
- For AD Lab and AD Enterprise, applications, the KFF Server is generally installed on a different computer that runs the Examiner application.
- For Summation or eDiscovery, the KFF Server may be installed on either the same computer as the application or on a remote computer. For large environments, it is recommended that the KFF Server be installed on a dedicated computer.

After installing the KFF Server, you configure the application with the location of the KFF Server.

See Configuring the Location of the KFF Server on page 15.

AD Lab and AD Enterprise

With AD Lab and Enterprise, you generally install the KFF Server on a different computer than the application.

Special Configuration Steps for KFF

When you install the KFF Server on a different computer than the application you perform special configuration steps by doing the following:

- Configure the KFF Sever location.
  See Configuring the KFF Server Location on AD Lab and AD Enterprise on page 15.
- Application version 6.3 and later:
  - During the installation of Cassandra, you must enable and configure Remote Access.
    See Installing the KFF Server on page 13.
  - If you installed Cassandra without enabling remote access, you can manually configure Cassandra.
    See Manually Configuring Remote Setting for Cassandra on page 17.

Summation or eDiscovery

With Summation or eDiscovery, you may have one of the following environments. The type of environment determines where and how to configure the KFF Server.

Environment	KFF Server Location and Configuration
Single Server	All components of the application are installed on a single server. ● You can install the KFF Server on this server or a different remote computer. ● If you install the KFF Server on the same server, no special configuration for KFF is needed. ● If you install the KFF Server on a remote computer, you must perform special configuration steps for KFF.
Distributed Components with Local Processing	Components of the application are installed on multiple servers. For example, the MAP component is on one server and other application components, such as WCF Services and Local Processing are installed on a separate computer. ● You can install the KFF Server on the same server as WCF Services and Local Processing or on a different remote computer. ● If you install the KFF Server on the same server, no special configuration for KFF is needed. ● If you install the KFF Server on a remote computer, you must perform special configuration steps for KFF.
Distributed Processing Manager and Engines	You have installed the Distributed Processing Manager and Distributed Processing Engines. ● You can install the KFF Server on any computer. ● You must perform special configuration steps for KFF.
Dedicated KFF Server	For performance, you can install the KFF Server on a dedicated computer. ● You must perform special configuration steps for KFF.

If you do not need to perform special configuration steps, you can use default settings.

Special Configuration Steps for KFF

If needed, when you perform special configuration steps, you must do the following:

- Configure the KFF Sever location by editing two application configuration files.
  See Configuring the KFF Server Location on Summation or eDiscovery on page 16.
- Application version 6.3 and later:
  - During the installation of Cassandra, you must enable and configure remote access.
    See Installing the KFF Server on page 13.
  - If you installed Cassandra without enabling remote access, you can manually configure Cassandra.
    See Manually Configuring Remote Setting for Cassandra on page 17.

Installing the KFF Server

How you install the KFF Server depends on version of the product you are running.

For product versions 6.3 and later, you install the KFF Server by installing Apache Cassandra 3.11.

About Installing Cassandra

For product versions 6.3 and later, you install the KFF Server by installing Apache Cassandra 3.11.

Cassandra Prerequisites

When you install Cassandra, it will also install Python 2.7.13 if needed.

Important: In order to install Cassandra, you must have 64-bit Java for Windows version 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, you may automatically download the 32-bit version. You must use the 64-bit version.

Cassandra and Firewalls

During the installation, if you check the box to *Enable Remote Access*, the installer creates an inbound exception rule for the port entered in the Cassandra installer (if the rule has not already been created).

The rule has the following attributes:

- name = AccessData Cassandra Remote Access Port
- direction = in
- program = “<install directory>\Cassandra\bin\daemon\prunsrv.exe”
- local port = 9042 (or whatever the user entered)
- protocol = tcp

If you uninstall Cassandra, the installer checks to see if Enable Remote Access was checked during install, and if it was, the installer looks for the above firewall rule using the 5 listed attributes, and if it finds the rule, it removes it from the firewall.

Installing Cassandra

To install Cassandra

1. Select the computer that you want to install Cassandra on.
   See Determining Where to Install the KFF Server on page 11.
2. If needed, install 64-bit Java 8.
3. Do one of the following to access AccessData_Cassandra_Installer.exe:
   - Disk
   - Download
4. Launch AccessData_Cassandra_Installer.exe.
5. If needed, install Python 2.7.
6. On the *Welcome* page, click **Next**.
7. Accept the license terms and click **Next**.
8. Verify or change the the *Destination Folder* and click **Next**.
9. If needed, configure Remote Access.
   See Determining Where to Install the KFF Server on page 11.

Important: If installing for FTK, do not enable Remote Access. FTK requires a setting of localhost.

9a. Select *Enable Remote Access*.

9b. In the *RPC_Address* field, enter the IP address of the computer you are installing on. For example, 10.10.10.10.

9c. In the *Native Transport Port Number* field, leave the default 9042.

9d. Click **Next**.

If you do not enable Remote Access during installation, you can manually configure it later.
See Manually Configuring Remote Setting for Cassandra on page 17.

10. If you enabled Remote Access, set the User Credentials for the service and click **Next**.
11. Click **Install** to perform the installation.
12. Click **Finish**.
13. If your AccessData application is already open, restart it.

Configuring the Location of the KFF Server

After installing the KFF Server, on the computer running the application, such as Summation, eDiscovery, FTK, or AD Lab, you configure the location of the KFF Server.

Do one of the following:

- Configuring the KFF Server Location on AD Lab and AD Enterprise (page 15)
- Configuring the KFF Server Location on Summation or eDiscovery (page 16)
- Manually Configuring Remote Setting for Cassandra (page 17)

Configuring the KFF Server Location on AD Lab and AD Enterprise

If running FTK, you use default settings.

If running with AD Lab or AD Enterprise, and if not using default settings, before using KFF, you must configure the location of the KFF Server.

Important: To configure KFF, you must be logged in with Admin privileges.

To view or edit KFF configuration settings

1. In the *Case Manager*, click **Tools > Preferences > Configure KFF**.
2. You can set or view the address of the KFF Server.
   - If you installed the KFF Server on the same computer as the application, this value will be localhost.
   - If you installed the KFF Server on a different computer, identify the KFF server.
3. Click **Test** to validate communication with the KFF Server.
4. Click **Save**.
5. Click **OK**.

Configuring the KFF Server Location on Summation or eDiscovery

When using the KFF Server with Summation or eDiscovery, two configuration files must point to the KFF Server location.

Important: If you are upgrading to 6.3 or later from 6.2 or earlier, the syntax of and the port values for the KFF Server have changed. If the KFF Server is not being recognized, make sure that the two config files are correct.

See What has Changed in Version 6.3 on page 36.

KFF Server Location scenarios
If one of the following is true, you can use the default settings and the KFF Server location is configured as "localhost". ● Your Summation or eDiscovery installation is on a single server ● Your Summation or eDiscovery installation is on multiple servers, and you install the KFF Server on the same server that is running WorkManager If needed, you can verify the settings without changing them.
If one of the following is true, you must manually specify the location of the KFF Server: ● If you change the location of your KFF Server ● If you install the KFF Server on a different computer than is running WorkManager ● If you are using distributed processing For KFF processing to work correctly in this situation, change the the **KFFServerURL** setting from "localhost" to the actual IP address.

Manually Verifying or Configuring the KFF Server Location on products 6.3 and later

1. Configure **AdgWindowsServiceHost.exe.config:**
   - 1a. On the computer running the work manger service, go to **C:\Program Files\AccessData\Common\FTK Business Services**.
   - 1b. Open **AdgWindowsServiceHost.exe.config**.
   - 1c. Find the line **<add key="KFFServerUrl" value="localhost:9042" />**.
     Note: 9042 is the default port for Cassandra.
   - 1d. If needed, change *localhost* to be the location IP address of your KFF server.
     For example, value="10.10.10.10:9042"
     Otherwise, leave as localhost.
   - 1e. Leave the following line unchanged:
     <add key="KFFServerDBType" value="Cassandra" />
   - 1f. Save and close the file.
   - 1g. If you changed the file, restart the *AccessData Business Services Common* service.

2. Configure **Infrastructure.WorkExecutionServices.Host.exe.config**:
   2a. On the computer running the work manger service, go to **C:\Program Files\AccessData\eDiscovery\WorkManager**.
   2b. Open **Infrastructure.WorkExecutionServices.Host.exe.config**.
   2c. Find the line **<add key="KFFServerUrl" value="localhost:9042" />**.
   Note: 9042 is the default port for Cassandra.
   2d. If needed, change *localhost* to be the location IP address of your KFF server.
   For example, value="10.10.10.10:9042"
   Otherwise, leave as localhost.
   2e. Leave the following line unchanged:
   <add key="KFFServerDBType" value="Cassandra" />
   2f. Save and close the file.
   2g. If you changed the file, restart the *AccessData Work Manager* service.
3. Migrate or Import your KFF Hash Data.
   See About Importing KFF Data on page 20.

Manually Configuring Remote Setting for Cassandra

In some situations Cassandra needs be to configured to enable Remote Access.

See Determining Where to Install the KFF Server on page 11.

During the installation of Cassandra there is the option to *Enable Remote Access* and then set the *RPC_Address* (the IP address of the computer that Cassandra is installed on).

If you set these settings correctly during the installation, no further configuration is needed.

However, if you did not enable remote access or make a change, you can manually configure the remote settings for Cassandra.

Note: Use an editor that supports YAML files.

To manually configuring remote settings for Cassandra

1. Go to the location that you installed Cassandra.
   By default, it is C:\Program Files\AccessData\Cassandra.
2. Open the \conf folder.
3. Edit the cassandra.yaml file.
4. Search for rpc_address:
5. Change the address from local host to the IP or DNS name of the computer running Cassandra.
   For example change **rpc_address: localhost** to **rpc_address: 10.10.10.10**
6. Search for native_transport_port:
7. Verify that the setting is:
   native_transport_port: 9042 (or the port you are using)
8. Save and exit the file.
9. Restart the AccessData Cassandra service.

Migrating Legacy KFF Data from Previous Versions

You can migrate KFF Data from a previous KFF Server architecture to a newer one.

- See Migrating Legacy KFF Data from versions 5.6 - 6.2 to 6.3 on page 18.
- See Migrating Legacy KFF Data from versions 5.5 and earlier on page 19.

Migrating Legacy KFF Data from versions 5.6 - 6.2 to 6.3

If you have are using applications version 6.3 and later and you previously used KFF with applications versions 5.5 - 6.2, you can migrate the older data from the Elasticsearch KFF Server to the new KFF Server architecture used in 6.3 and later. To migrate the KFF data, you use the *AccessData Has Manager Migration Tool*. This tool is a separate Windows-based application.

Important: Please note the following:

- Applications version 6.3 and later can only use the new KFF architecture that was introduced in versions 6.3. If you want to use KFF data from previous versions, you must migrate the data.
- If you have NSRL, NDIC, or DHS data in your legacy data, those sets will not be migrated. You must re-import them using the 6.3 versions or later of those libraries. Only legacy custom KFF data will be migrated.
- You cannot migrate data from 5.5 and earlier directly to 6.3 or later. You must do a two-step migration process and migrate first to the 5.6-6.2 format.
- If you already have data in Cassandra and you migrate from Elasticsearch, if the same hash exists on bother servers, and one if either one of them has an Alert status, it will be given an Alert status. Otherwise, data will be migrated with the same values.

Legacy KFF data is migrated to KFF Groups and Hash Sets on the new KFF Server.

You migrate data using the KFF Migration Tool. To use the KFF Migration Tool, you identify the following:

- The server where the legacy Elasticsearch KFF data is located.
- The server where the legacy Elasticsearch KFF data will be located to (the Cassandra location).

To install the KFF Migration Tool

1. You can install the KFF Migration Tool onto any computer as long as it can access the servers running Elasticsearch and Cassandra.
2. Access the KFF Installation disc, and run the autorun.exe.
3. Click the **Hash Manager Migration Tool**.
4. Complete the installation wizard.
   The default path is Program Files (x86)\AccessData\HashManagerMigration.
   You can use the default or enter a new path.
5. The tool is automatically opened after installation.

To migrate legacy KFF data

1. Launch the KFF Hash Manager Migration Tool.
2. Enter the location and port of the legacy ElasticSearch KFF data.
   For example, if ElasticSearch is on the same computer, you can use the default location of http://localhost:9200.
   If it is on a different computer, enter the IP address and port of the computer. For example, http://10.10.10.10:9200.

3. Enter the location of the new KFF server (Cassandra database).
   For example, if Cassandra is on the same computer, you can use the default location of localhost. If it is on a different computer, enter the IP address, for example, 10.10.10.10.
4. Click **Start Migration**.

Migrating Legacy KFF Data from versions 5.5 and earlier

If you have used KFF with applications versions 5.5 and earlier, you can migrate that data from the legacy KFF Server to the Elasticsearch KFF Server architecture that was used in version 5.6 - 6.2. You cannot migrate data from 5.5 directly to 6.3 or later. Instead, you must upgrade the legacy to a 5.6 - 6.2 format, then migrate that to 6.3.

Important: Applications version 5.6 - 6.2 can only use the Elasticsearch KFF architecture. If you want to use KFF data from previous versions, you must migrate the data.

Important: If you have NSRL, NDIC, or DHS data in your legacy data, those sets will not be migrated. You must re-import them using the 5.6 - 6.2 versions of those libraries. Only legacy custom KFF data will be migrated.

Legacy KFF data is migrated to KFF Groups and Hash Sets on the new KFF Server.

Because KFF Templates are no longer used, they will be migrated as KFF Groups, and the groups that were under the template will be added as sub-groups.

You migrate data using the KFF Migration Tool. To use the KFF Migration Tool, you identify the following:

- The Storage Directory folder where the legacy KFF data is located.
  This was folder was configured using the KFF Server Configuration utility when you installed the legacy KFF Server. If needed, you can use this utility to view the KFF Storage Directory. The default location of the KFF_Config.exe file is Program Files\AccessData\KFF.
- The URL of the new KFF Server (the computer running the AccessData Elastic Search Windows Service)
  This is populated automatically if the new KFF Server has been installed.

To install the KFF Migration Tool

1. On the computer where you have installed the KFF Server, access the KFF Installation disc, and run the **autorun.exe**.
2. Click the *64 bit* or *32 bit* **Install KFF Migration Utility**.
3. Complete the installation wizard.

To migrate legacy KFF data

1. On the legacy KFF Server, you must stop the KFF Service.
   You can stop the service manually or use the legacy KFF Config.exe utility.
2. On the new KFF Server, launch the KFF Migration Tool.
3. Enter the directory of the legacy KFF data.
4. The URL of Elasticsearch should be listed.
5. Click **Start**.
6. When completed, review the summary data.

Importing KFF Data

About Importing KFF Data

You can import hashes and KFF Groups that have been previous configured.

You can import KFF data in one of the following formats:

KFF Data sources that you can import

Source	Description
Pre-configured KFF libraries	You can import KFF data from the following pre-configured libraries ● NIST NSRL ● NDIC HashKeeper ● DHS ● Law enforcement users: Project VIC To import large KFF libraries, use the KFF Import Utility. See About KFF Data Import Tools on page 21. See Importing Pre-defined KFF Data Libraries on page 23. See KFF Library Reference Information on page 31.
Custom Hash Sets and KFF Groups	You can import custom hashes from CSV and other file types. See About the CSV Format on page 8. You can import custom CSV files either through the application or the KFF Import Utility. Other files types can be imported in FTK. See About KFF Data Import Tools on page 21.

About KFF Data Import Tools

When you import KFF data, you can use one of two tools:

KFF Data Import Tools

The application's Import feature	The KFF management feature in the application lets you import .CSV files (especially files that only have one KFF status). For FTK-based forensics products, you can also import custom hashes from the following file types: ● Delimited files (CSV or TSV) ● Hash Database files (HDB) ● Hashkeeper files (HKE) ● FTK Exported KFF files (KFF) ● FTK Supported XML files (XML) ● FTK Exported Hash files (HASH) ● Project VIC JSON files To import these kinds of files, use the KFF Import feature in your application. See *Using the Known File Feature* chapter. You can also manually create your own KFF hash set data.

KFF Import Utility	You can import files using the KFF Import Utility.
	It is recommended that you use the KFF Import Utility to import files in the following situations:
	● A CSV file that has a mixture of Alert and Ignore statuses.
	● Large pre-configured libraries:
	  ■ NIST NSRL
	  ■ NDIC HashKeeper
	  ■ DHS
	See Using the KFF Import Utility on page 22.

About Default Status Values

When you import KFF data, you configure a default status value of Alert or Ignore. When adding Hash Sets to KFF Groups, you can configure the KFF Groups to use the default status values of the Hash Set or you can configure the KFF Group with a status that will override the default Hash Set values.

See Components of KFF Data on page 5.

About Duplicate Hashes

If multiple Hash Set files containing the same Hash identifier are imported into a single KFF Group, the group keeps the last Hash Set's metadata information, overwriting the previous Hash Sets' metadata. This only happens within an individual group and not across multiple groups.

Using the KFF Import Utility

It is important that you use the correct version of the KFF Import Utility with the version of the application you are using. The KFF Import Utility was modified significantly for 6.3.

Using the KFF Import Utility versions 6.3 *and* later

About the KFF Import Utility

Due to the large size of some KFF data, a stand-alone KFF Import utility is available to use to import the data. This KFF Import utility can import large amounts of data faster then using the import feature in the application.

It is recommend that you install and use the KFF Import utility to import the following pre-configured libraries:

- NIST NSRL
- NDIC HashKeeper
- DHS

After importing NSRL, NDIC, or DHS libraries, these libraries are displayed in the *Currently Installed Sets* list.

See Components of KFF Data on page 5.

You can also use the KFF Import Utility to remove the NSRL, NDIC, or DHS indexes that you have imported.

Installing the KFF Import Utility versions 6.3 and later

You must use the matching version of the KFF Import Utility with your application, for example, 6.3.

To install the KFF Import Utility

1. On the computer where you have installed the KFF Server, access the KFF Installation disc, and run the **autorun.exe**.
2. Click the **Install KFF Import Utility**.
3. Complete the installation wizard.
4. To import libraries, see See About Importing Pre-defined KFF Data Libraries on page 23.

Importing a CSV Using the KFF Import Utility versions 6.3 and later

You can import Hash Sets and KFF Groups by importing a custom CSV file.

See About the CSV Format on page 8.

To import a CSV using the KFF Import Utility

1. Open the KFF Import Utility.
2. Click the *Browse ..* button and locate the CSV that you want to import.
3. Click **Open**.
4. (Optional) - Enter package, vendor, version, etc.

5. If you installed Cassandra enabling Remote Access, in the *Server address* field, you must enter the computer's IP that has Cassandra installed on it, even if it is on the same computer as the import utility. Otherwise, leave it as localhost.
6. Click **Import**.
7. When complete, click **OK**.

Removing Pre-defined KFF Libraries Using the KFF Import Utility version 6.3 and later

You can remove a pre-defined KFF Library that you have previously imported.

You cannot see or remove existing custom KFF data (your own CSVs or manually entered data).

Important: Removing files using this method takes a very long time (up to a couple of hour for NIST and DHS, and many hours for NSRL). You may want to manually deletes sets and groups using the application instead.

To remove pre-defined KFF Libraries

1. On the KFF Server, open the KFF Import Utility.
2. Select the library that you want to remove.
3. Click **Remove**.

Importing Pre-defined KFF Data Libraries

About Importing Pre-defined KFF Data Libraries

After you install the KFF Server, you can import pre-defined NIST NSRL, NDIC HashKeeper, and DHS data libraries.

See About KFF Pre-Defined Hash Libraries on page 31.

Important: In versions 6.3, you must import specific files for these versions. It is recommend that you use the KFF Import Utility.

After importing pre-defined KFF Libraries, you can remove them from the KFF Server.

- Removing Pre-defined KFF Libraries Using the KFF Import Utility version 6.3 and later (page 23)

See the following sections:

- Importing the NIST NSRL Library (page 24)
- Importing the NDIC Hashkeeper Library (page 28)
- Importing the DHS Library (page 28)

Importing the NIST NSRL Library

To import NSRL data in applications version 6.3 and later, you can do one of the following:

- Download version 2.58 or later RDS files from nist.gov and import them.
  See Downloading and Importing the NIST NSRL Files from NIST.ORG on page 24.
- Download version 2.54 files from AccessData and import them.
  See Downloading and Importing the NIST NSRL Files from NIST.ORG on page 24.

Downloading and Importing the NIST NSRL Files from NIST.ORG

You can download the latest ISO files directly from the NIST.GOV.

After you have downloaded the files, you import them into the KFF Server.

Before importing NSRL data, we recommend that you verify the hashes of the iso files that you downloaded from NIST. This assures that the data has not been corrupted.

Important: Please note the following:

- The complete NSRL library data is contained in a large (3 GB) .ZIP file in the image file. When expanded, the data is about 14 GB.
- Due to the large amount of NSRL data, it will take 6-8 hours to import the NSRL data using the KFF Import Utility. If you import from within an application, it will take even longer.
- You must not have a previous version version of the NSRL library installed. If needed, uninstall the previous version first.

To download NSRL files from NIST.ORG

1. Go to https://www.nist.gov/software-quality-group/national-software-reference-library-nsrl
2. Click **NSRL Download**.
3. Click **Current RDS Hash Sets**.
4. Click and download **Modern RDS**.
5. Compare and the hashes of your downloaded iso files with the hashes listed at:
   https://s3.amazonaws.com/rds.nsrl.nist.gov/RDS/current/version.txt
   (This address is case-sensitive)

To prepare NSRL files for importing

1. Mount the RDS ISO file.
2. Create a folder that you can browse to from the Import Utility (for example, **RDS_258_modern**).
3. Extract the NSRLFile.txt.zip file into that RDS folder.
4. Copy the following files from the ISO image to that same RDS folder:
   - NSRLProd.txt
   - NSRLOS.txt
   - NSRLMfg.txt
5. Create an **AppTypes.txt** file.

   In this file, you can specify application files that you may want to flag as Alert rather than Ignore.

   5a. In the same folder as the NSRLFile.txt.zip file, create a text file named **AppTypes.txt**.

   5b. In the file, include the following text:

   This is a text file listing the application types (one per line) which should have "Alert" status set:

   Anti-KeyLogger

   Computer Investigation

   Data Encryption

   Disk Wiper

   Encryption

   Forensic

   Forensic Toolkit

   Hacker Tool

   Keyboard Logger

   Steganography

   5c. Save and exit the file.
6. Verify that the folder has the following files:
   - NSRLProd.txt
   - NSRLOS.txt
   - NSRLMfg.txt
   - NSRLFile.txt
   - AppTypes.txt

To import the NIST NSRL library

1. On the KFF Server, launch the 6.3 or later version of the *KFF Import Utility*.

   See About Importing KFF Data on page 20.
2. Do the following:

   2a. In the *File to Import* field, browse to and select the **NSRLFile.txt** file that you previously extracted.

   2b. If you installed Cassandra enabling Remote Access, in the *Server address* field, you must enter the computer's IP that has Cassandra installed on it, even if it is on the same computer as the import utility. Otherwise, use localhost.

   2c. Click **Import**.

   2d. The import will take several hours.

   2e. When the import is complete, click **OK**.

   2f. The NSRL library will be listed in the *Currently Installed Sets*.

Importing the NIST NSRL Library Files from AccessData

You can download version 2.54 files from AccessData and import them.

See About NSRL Library Files Provided by AccessData on page 27.

Important: The NSRL library data is contained in a large (3.75 GB) .ZIP file. When expanded, the data is about 21.7 GB. Make sure that your file system can support files of this size.

Important: Due to the large amount of NSRL data, it will take approximately 8 hours to import the NSRL data using the KFF Import Utility.

To install the NSRL library

1. On the computer that you want to be the KFF Server, extract the nsrlsource_2.54.zip file that is at the root of the ISO.
2. On the computer that you want to be the KFF Server, install the AccessData Cassandra Service.
3. Install the *KFF Import Utility* version 6.3.
4. Use the *KFF Import Utility* to import the NSRL library by doing the following:
   - 4a. Launch the *KFF Import Utility*.
   - 4b. Browse to the NSRLFile.txt that is contained in the nsrlsource_2.54 folder.
   - 4c. Click **Open**.
   - 4d. Click **Import**.
   - 4e. When the import is complete, a finished window pops up, click OK.

About NSRL Library Files Provided by AccessData

You can import the NSRL library into your KFF Server. During the import, two KFF Groups are created: NSRL_Alert and NSRL_Ignore. In FTK-based products, these two groups are automatically added to the Default KFF Group.

The NSRL libraries are updated from time to time. The NSRL import feature supports appending new data and updating existing data when importing a newer version. To import and maintain the NSRL data, you do the following:

Process for Importing and Maintaining the NIST NSRL Library

1. Import the complete NSRL library.	You must first install the most current complete NSRL library. You can later add updates to it. To access and import the complete NSRL library, see Importing the NIST NSRL Library (page 24)
2. Import updates to the library	When updates are made available, import the updates to bring the data up-to date. See Installing KFF Updates on page 30. **Important:** In order to use the NSRL updates, you must first import the complete library. When you install an NSRL update, you must keep the previous NSRL versions installed in order to maintain the complete set of NSRL data.

Available NRSL library files (new format)

NSRL Library Release	Released	Information
Complete library version 2.54 (source .ZIP file)	Mar 2017	For use only with applications version 5.6 and later. Contains the full NSRL library up through update 2.54.
Complete library version 2.45 (source .ZIP file)	Nov 2014	For use only with applications version 5.6 and later. Contains the full NSRL library up through update 2.45.

Importing the NDIC Hashkeeper Library

You can import the Hashkeeper 9.08 library.

For application versions 6.3 and later, these files are stored in CSV format.

To import the Hashkeeper library

1. Have access to the NDIC source files by download the ZIP file from the web:
   See Downloading the Latest KFF Installation Files on page 10.
2. Extract the ZIP file.
3. On the KFF Server, launch the 6.3 or later version of the *KFF Import Utility.*
   See About Importing KFF Data on page 20.
4. Do the following:
   4a. In the *File to Import* field, browse to and select the **ndic.csv** file.
   4b. If you installed Cassandra enabling Remote Access, in the *Server address* field, you must enter the computer's IP that has Cassandra installed on it, even if it is on the same computer as the import utility. Otherwise, use localhost.
   4c. Click Import.
   4d. The import may take a few minutes.
   4e. When the import is complete, click **OK**.
   4f. The NDIC library will be listed in the *Currently Installed Sets*.

Importing the DHS Library

You can import the DHS 1.08 library.

For application versions 6.3 and later, these files are stored in CSV format.

To import the DHS library

1. Have access to the DHS source files by download the ZIP file from the web:
   See Downloading the Latest KFF Installation Files on page 10.
2. Extract the ZIP file.
3. On the KFF Server, launch the 6.3 or later version of the *KFF Import Utility.*
   See About Importing KFF Data on page 20.
4. Do the following:
   4a. In the *File to Import* field, browse to and select the **dhs.csv** file.
   4b. If you installed Cassandra enabling Remote Access, in the *Server address* field, you must enter the computer's IP that has Cassandra installed on it, even if it is on the same computer as the import utility. Otherwise, use localhost.
   4c. Click Import.
   4d. The import may take a few minutes.
   4e. When the import is complete, click **OK**.
   4f. Do not process with NSRL data untill there is confirmation that the import is done.
   4g. The DHS library will be listed in the *Currently Installed Sets*.

Uninstalling KFF

You can uninstall KFF application components independently of the KFF Data.

Main version	Description
Applications 5.6 to 6.2	For applications version 5.6 and later, you uninstall the following components: ● *AccessData Elasticsearch Windows Service* (KFF Server) v1.2.7 and later Note: Elasticsearch is used by multiple features in various applications, use caution when uninstalling this service or the related data. ● *AccessData KFF Import Utility* (v5.6 and later) ● *AccessData KFF Migration Tool* (v1.0 and later) ● *AccessData Geo Location Data* (v2014.10 and later) Note: This component is not used by the KFF feature, but with the KFF Server for the geolocation visualization feature. The location of the KFF data is configured when the *AccessData Elasticsearch Windows Service* was installed. By default, it is located at C:\Program Files\AccessData\Elacticsearch\Data.
Applications 5.5 and earlier	For applications version 5.5 and earlier, you can uninstall the following components: ● KFF Server (v1.2.7 and earlier) Note: The KFF Server is also used by the geolocation visualization feature. ● AccessData Geo Location Data (1.0.1 and earlier) This component is not used by the KFF feature, but with the KFF Server for the geolocation visualization feature. The location of the KFF data was configured when the *KFF Server* was installed. You can view the location of the data by running the *KFF.Config.exe* on the KFF Server. If you are upgrading from 5.5 to 5.6, you can migrate your KFF data before uninstalling the KFF Server.

Installing KFF Updates

From time to time, AccessData will release updates to the KFF Server and the KFF data libraries.

Some of the KFF data updates may require you to update the version of the KFF Server.

To check for updates, do the following:

1. Go to the KFF product download page.
   See Downloading the Latest KFF Installation Files on page 10.
2. Check for updates.
   - See About KFF Server Versions on page 9.
   - See Importing the NIST NSRL Library on page 24.
3. If there are updates, download them.
4. Install or import the updates.

KFF Library Reference Information

About KFF Pre-Defined Hash Libraries

This section includes a description of pre-defined hash collections that can be added as AccessData KFF data.

The following pre-defined libraries are currently available for KFF and come from federal government agencies:

- NIST NSRL (The default library installed with KFF)
- NDIC HashKeeper (An optional library that can be downloaded from the AccessData Downloads page)
- DHS (An optional library that can be downloaded from the AccessData Downloads page)

For law enforcement users, you can also use Project Vic libraries.

See Using Project VIC on page 286.

Use the following information to help identify the origin of any hash set within the KFF

- The NSRL hash sets do not begin with “ZZN” or “ZN”. In addition, in the AD Lab KFF, all the NSRL hash set names are appended (post-fixed) with multi-digit numeric identifier. For example: “Password Manager & Form Filler 9722.”
- All HashKeeper Alert sets begin with “ZZ”, and all HashKeeper Ignore sets begin with “Z”. (There are a few exceptions. See below.) These prefixes are often followed by numeric characters (“ZZN” or “ZN” where N is any single digit, or group of digits, 0-9), and then the rest of the hash set name. Two examples of HashKeeper Alert sets are:
  - “ZZ00001 Suspected child porn”
  - “ZZ14W”

  An example of a HashKeeper Ignore set is:
  - “Z00048 Corel Draw 6”
- The DHS collection is broken down as follows:
  - In 1.81.4 and later there are two sets named “DHS-ICE Child Exploitation JAN-1-08 CSV” and “DHS-ICE Child Exploitation JAN-1-08 HASH”.
  - In AD Lab there is just one such set, and it is named “DHS-ICE Child Exploitation JAN-1-08”.

Once an investigator has identified the vendor from which a hash set has come, he/she may need to consider the vendor’s philosophy on collecting and categorizing hash sets, and the methods used by the vendor to gather hash values into sets, in order to determine the relevance of Alert (and Ignore) hits to his/her project. The following descriptions may be useful in assessing hits.

NIST NSRL

The NIST NSRL collection is described at: http://www.nsrl.nist.gov/index.html. This collection is much larger than HashKeeper in terms of the number of sets and the total number of hashes. It is composed entirely of hash sets being generated from application software. So, all of its hash sets are given Ignore status by AccessData staff except for those whose names make them sound as though they could be used for illicit purposes.

The NSRL collection divides itself into many sub-collections of hash sets with similar names. In addition, many of these hash sets are “empty”, that is, they are not accompanied by any hash values. The size of the NSRL collection, combined with the similarity in set naming and the problem of empty sets, allows AccessData to modify (or selectively alter) NSRL’s own set names to remove ambiguity and redundancy.

Find contact info at http://www.nsrl.nist.gov/Contacts.htm.

NDIC HashKeeper

NDIC’s HashKeeper collection uses the Alert/Ignore designation. The Alert sets are hash values contributed by law enforcement agents working in various jurisdictions within the US - and a few that apparently come from Luxemburg. All of the Alert sets were contributed because they were believed by the contributor to be connected to child pornography. The Ignore sets within HashKeeper are computed from files belonging to application software.

During the creation of KFF, AccessData staff retains the Alert and Ignore designations given by the NDIC, with the following exceptions. AccessData labels the following sets Alert even though HashKeeper had assigned them as Ignore: “Z00045 PGP files”, “Z00046 Steganos”, “Z00065 Cyber Lock”, “Z00136 PGP Shareware”, “Z00186 Misc Steganography Programs”, “Z00188 Wiping Programs”. The names of these sets may suggest the intent to conceal data on the part of the suspect, and AccessData marks them Alert with the assumption that investigators would want to be “alerted” to the presence of data obfuscation or elimination software that had been installed by the suspect.

The following table lists actual HashKeeper Alert Set origins:

A Sample of HashKeeper KFF Contributions

Hash	Contributor	Location	Contact Information	Case/Source
ZZ00001 Suspected child porn	Det. Mike McNown & Randy Stone	Wichita PD		
ZZ00002 Identified Child Porn	Det. Banks	Union County (NJ) Prosecutor's Office	(908) 527-4508	case 2000S-0102
ZZ00003 Suspected child porn	Illinois State Police			
ZZ00004 Identified Child Porn	SA Brad Kropp, AFOSI, Det 307		(609) 754-3354	Case # 00307D7-S934831

A Sample of HashKeeper KFF Contributions (Continued)

Hash	Contributor	Location	Contact Information	Case/Source
ZZ00000, suspected child porn	NDIC			
ZZ00005 Suspected Child Porn	Rene Moes, Luxembourg Police		rene.moes@police.etat.lu	
ZZ00006 Suspected Child Porn	Illinois State Police			
ZZ00007b Suspected KP (US Federal)				
ZZ00007a Suspected KP Movies				
ZZ00007c Suspected KP (Alabama 13A-12-192)				
ZZ00008 Suspected Child Pornography or Erotica	Sergeant Purcell	Seminole County Sheriff's Office (Orlando, FL, USA)	(407) 665-6948, dpurcell@seminolesheriff.org	suspected child pornogrpahy from 20010000850
ZZ00009 Known Child Pornography	Sergeant Purcell	Seminole County Sheriff's Office (Orlando, FL, USA)	(407) 665-6948, dpurcell@seminolesheriff.org	200100004750
ZZ10 Known Child Porn	Detective Richard Voce CFCE	Tacoma Police Department	(253)594-7906, rvoce@ci.tacoma.wa.us	
ZZ00011 Identified CP images	Detective Michael Forsyth	Baltimore County Police Department	(410)887-1866, mick410@hotmail.com	
ZZ00012 Suspected CP images	Sergeant Purcell	Seminole County Sheriff's Office (Orlando, FL, USA)	(407) 665-6948, dpurcell@seminolesheriff.org	
ZZ0013 Identified CP images	Det. J. Hohl	Yuma Police Department	928-373-4694	YPD02-70707

A Sample of HashKeeper KFF Contributions (Continued)

Hash	Contributor	Location	Contact Information	Case/Source
ZZ14W	Sgt Stephen May		Tamara.Chandler@oag.state.tx.us, (512)936-2898	TXOAG 41929134
ZZ14U	Sgt Chris Walling		Tamara.Chandler@oag.state.tx.us, (512)936-2898	TXOAG 41919887
ZZ14X	Sgt Jeff Eckert		Tamara.Chandler@oag.state.tx.us, (512)936-2898	TXOAG Internal
ZZ14I	Sgt Stephen May		Tamara.Chandler@oag.state.tx.us, (512)936-2898	TXOAG 041908476
ZZ14B	Robert Britt, SA, FBI		Tamara.Chandler@oag.state.tx.us, (512)936-2898	TXOAG 031870678
ZZ14S	Sgt Stephen May		Tamara.Chandler@oag.state.tx.us, (512)936-2898	TXOAG 041962689
ZZ14Q	Sgt Cody Smirl		Tamara.Chandler@oag.state.tx.us, (512)936-2898	TXOAG 041952839
ZZ14V	Sgt Karen McKay		Tamara.Chandler@oag.state.tx.us, (512)936-2898	TXOAG 41924143
ZZ00015 Known CP Images	Det. J. Hohl	Yuma Police Department	928-373-4694	YPD04-38144
ZZ00016	Marion County Sheriff's Department		(317) 231-8506	MP04-0216808

The basic rule is to always consider the source when using KFF in your investigations. You should consider the origin of the hash set to which the hit belongs. In addition, you should consider the underlying nature of hash values in order to evaluate a hit's authenticity.

Higher Level KFF Structure and Usage

Since hash set groups have the properties just described (and because custom hash sets and groups can be defined by the investigator) the KFF mechanism can be leveraged in creative ways. For example:

- You could define a group of hash sets created from encryption software and another group of hash sets created from child pornography files. Then, you would apply only those groups while processing.
- You could also use the Ignore status. You are about to process a hard drive image, but your search warrant does not allow inspection of certain files within the image that have been previously identified. You could do the following and still observe the warrant:
  - 4a. Open the image in Imager, navigate to each of the prohibited files, and cause an MD5 hash value to be computed for each.
  - 4b. Import these hash values into custom hash sets (one or more), add those sets to a custom group, and give the group Ignore status.
  - 4c. Process the image with the MD5 and KFF options, and with AD_Alert, AD_Ignore, and the new, custom group selected.
  - 4d. During post-processing analysis, filter file lists to eliminate rows representing files with Ignore status.

Hash Set Categories

The highest level of the KFF's logical structure is the categorizing of hash sets by owner and scope. The categories are AccessData, Project Specific, and Shared.

Hash Set Categories

Category	Description
AccessData	The sets shipped with as the Library. Custom groups can be created from these sets, but the sets and their status values are read only.
Project Specific	Sets and groups created by the investigator to be applied only within an individual project.
Shared	Sets and groups created by the investigator for use within multiple projects all stored in the same database, and within the same application schema.

Important: Coordination among other investigators is essential when altering Shared groups in a lab deployment. Each investigator must consider how other investigators will be affected when Shared groups are modified.

What has Changed in Version 6.3

With the 6.3 release of eDiscovery, Summation, and FTK-based forensics products, the KFF architecture and features have been updated. This architecture is used in versions 6.3 and later.

If you used KFF with applications version 6.2 or earlier, be aware of the following changes in the KFF functionality.

KFF Changes from version 6.2 to 6.3

Item	Description
KFF Server	KFF Server now runs as a different service. • In versions 5.6 through 6.2, the KFF Server ran as the *AccessData Elastic-search Windows Service*. • In 6.3 and later, the KFF Server uses the *AccessData Cassandra* service. **Important:** If you are upgrading from 6.2 or earlier, all KFF data must be created in or migrated into the new KFF Server. See Migrating Legacy KFF Data from versions 5.6 - 6.2 to 6.3 on page 18.

eDiscovery or Summation KFF Server Configuration Files	In eDiscovery or Summation, there are two configuration files that configure the location of the KFF server.
	See Configuring the KFF Server Location on Summation or eDiscovery on page 16.
	The location format and port value in those files have changed.
	In 5.6 - 6.2, the following was used:
	`<add key="KffElasticSearchUrl" value="http://localhost:9200" />`
	In 6.3 it was changed to:
	`<add key="KFFServerUrl" value="localhost:9042" />`
	Note: The "http://" text is no longer used and Cassandra uses port 9042 instead of 9200.
	There is also a new line:
	`<add key="KFFServerDBType" value="Cassandra" />`

Hash Manager Migration Tool	If you are upgrading from 5.6 through 6.2, there is a new tool that lets you migrate custom KFF data to the new KFF Server on 6.3. See Migrating Legacy KFF Data from versions 5.6 - 6.2 to 6.3 on page 18. **Important:** NIST NSRL, NDIC HashKeeper, or DHS library data from 6.2 and earlier will not be migrated when using the Migration Tool. You must re-import those using the 6.3 KFF Import Tool. See About Importing Pre-defined KFF Data Libraries on page 23.
KFF Import Utility	This utility has been updated to use the new KFF Server. If you are upgrading from 5.6 - 6.2, make sure to install and use the new 6.3 version. See Using the KFF Import Utility on page 22.

KFF Changes from version 6.2 to 6.3

Item	Description
NDIC HashKeeper and DHS libraries	To use these libraries, you must import new versions of the files using the 6.3 version of the KFF Import Utility. NDIC HashKeeper and DHS libraries are now downloaded from AccessData and imported as CSV files. See About Importing Pre-defined KFF Data Libraries on page 23.
NIST NSRL	To import NSRL data, you can do either of the following: ● Download version 2.54 files from AccessData and import them. ● Download version 2.58 or later RDS files from nist.gov and import them. See Importing the NIST NSRL Library on page 24.
Export/Import	When you export and import KFF data, the Binary format (Entire Library) is no longer available. CSV is the only export format supported.
Geolocation data	Geolocation data is installed independently and is no longer linked to KFF.