AccessData Forensic Toolkit 5.6.4 Release Notes

Document Date: 9/8/2015

Introduction

This document lists the new features, fixed issues, and known issues for Forensic Toolkit® (FTK®) 5.6. All known issues published under previous release notes still apply until they are listed under “Fixed Issues.”

For convenience, the Release Notes from previous versions are included at the end of this document.

Supported Platforms

For a list of supported platforms for FTK see the following:

http://accessdata.com/solutions/digital-forensics/forensic-toolkit-ftk/technical

Important: In future versions of FTK, it will no longer support running on Windows XP.

5.6.4 New and Improved

The following items are new and improved for this release:

System

Processing

- When processing evidence, you can now pause and resume the processing.
- When creating a case, there are two new pre-configured processing profiles:
  - eDiscovery Defaults
  - Summation Defaults

KFF

- After installing the KFF Import Utility and KFF Migration tools, there are now Start Menu entries for them.

Examiner

Load Files

- You can now create a load file which lets you export data from a case in FTK and then import it into litigation document management applications such as AccessData Summation and eDiscovery.

  You create the load file by creating a report and using a new *Load File* report format.

  Important: When selecting which files to include in the report, you must also enable those files to be exported in the report. Otherwise, the files are not included in the load file.

System Information

- You can now export the content in the System Information tab into an XML file.

XML File List Info Export

- When performing an *Export File List Info*, you can now select XML as an output type.

Data Carving

- Improvements have been made in supporting popular Chinese file types, such as EML.

Fixed Issues in 5.6.4

The following issues have been fixed in this release:

Upgrade/Migration

- Fixed an issue that caused “Key not found in mapping” errors during migration. (30846)

Management

- If you attempt to open the Database menu for a database that is not currently running, FTK no longer crashes. (31104)
- Using a password reset file no longer displays a *Token file does not match* error. (32432)

Processing

- Processing no longer hangs when processing certain zip files with dtSearch disabled. (26344)
- Fixed an issue that sometimes occurred when accessing the OCR menu in Additional Analysis. (33418, 33573)
- Re-indexing after manually removing the generated index completes properly. (30021)
- Evidence counts for deleted files are correct when the *Include Deleted Files* processing option is enabled and the *Meta Carve* option is not enabled. (27149)

Decryption

- Decrypting a CheckPoint image no longer displays an Unrecognized File System error. (15251)

Performance

Performance and stability has been improved in the following areas:

- When using a right-click mouse option on several selected files. (29927)
- When using the Overview tree Evidence group. (30285,30894)
- When using the Graphic tab. (31244, 31270)
- When performing an index search. (31231)

Examiner

Bookmarks

- Fixed an issue that sometimes caused bookmarks to not function properly with email attachments. (32431)

Reports

- The information in the Audit log is more concise. (30286)
- Fixed an issue that caused some label colors to be displayed incorrectly in the reports dialog. (33410)

Other

- Fixed an issue that sometimes caused PDF files to display incorrectly in the Natural Viewer. (13569)
- In the Graphics tab, you can properly select thumbnails after resizing the application window. (31180)
- The File List properly refreshes when creating labels while files are checked. (31113)
- Fixed an issue that may have caused the System Information tree to not populate. (32333)
- When importing a memory dump, data is no longer populated in Evidence tree, but only in the Volatile tab. (31393)
- Fixed an issue that could cause the UI to lock when multiple users were attached to the same case. (30692)
- When using German regional settings and location, Geolocation EXIF longitude and latitude data is displayed properly. (28518)
- When using German regional settings and language, you can successfully restore a case (28290)

Important Information

Latest Documentation

- The User Guide that is loaded from the Help menu may not be the latest available version.
  The latest FTK documentation is located at:
  http://www.accessdata.com/support/product-downloads/ftk-download-page

Installation and upgrade

- For FTK installation and upgrade instructions, see the *FTK Quick Install Guide* and the detailed *FTK Installation Guide* which are available at

  http://www.accessdata.com/support/product-downloads/ftk-download-page
- FTK supports Distributed Processing Engines (DPEs).

  Before installing Distributed Processing, see the *Install Guide*.

Upgrading CodeMeter

- FTK 5.6.1 and later include an updated version of CodeMeter Runtime Kit (5.21).
  - If this is a new installation of FTK you do not need to do anything and the latest version of CodeMeter is installed.
  - If you are upgrading to FTK 5.6.1, be aware that a security vulnerability has been detected in Codemeter 4.5. However, if you simply upgrade from CodeMeter 4.5 to 5.21, the vulnerability remains. To fix the vulnerability, you must manually uninstall 4.5 before installing 5.21.

    If you are upgrading to FTK 5.6.1, manually uninstall CodeMeter first and then install FTK 5.6.1 which will install a clean CodeMeter 5.21. Otherwise, after upgrading to FTK 5.6.1, manually uninstall CodeMeter 4.5 and then manually install CodeMeter 5.21.

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 get corrupted.

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

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.
- If you choose to have a case's database files placed in the case folder, do not move your case folder without first archiving and detaching the case.

Where to get more information

Use the following documentation resources to learn more about this product. Each document is available in PDF format in the download ISO file. The *User Guide* is also available through the *Help* menu in FTK.

The latest version of each document is available in the *Product Release* pane on the FTK product download page:

http://www.accessdata.com/support/product-downloads/ftk-download-page

Document	Description
Quick Installation Guide	Basic information about how to install and upgrade this and related products.
FTK Installation Guide	Information about how to install and upgrade this and related products.
User Guide	Information about how to use this product, including detailed technical information and instructions for performing tasks.
Upgrading, Migrating, and Moving Cases	Information about upgrading and migrating cases from 4.1 to 4.2, and moving cases from one database to another.
Upgrading Cases	Information about upgrading cases from 4.1 to 4.2.
Migrating Archived Cases	Information about upgrading or migrating cases that you have archived in a previous release.
KFF Quick Install Guide and KFF installation files	For the most current KFF Server and KFF data installation files, as well as the *KFF Quick Install Guide*, visit the AccessData Product Downloads page: http://www.accessdata.com/support/product-downloads Expand the *Known File Filter (KFF)* section and then the *KFF Server* section.

Comments?

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

AccessData Forensic Toolkit 5.6.3 Release Notes

Document Date: 8/24/2015

Introduction

This document lists the new features, fixed issues, and known issues for Forensic Toolkit® (FTK®) 5.6. All known issues published under previous release notes still apply until they are listed under “Fixed Issues.”

Supported Platforms

For a list of supported platforms for Forensic Toolkit® (FTK®), see the following:

http://accessdata.com/solutions/digital-forensics/forensic-toolkit-ftk/technical

Important: In future versions of Forensic Toolkit® (FTK®), it will no longer support running on Windows XP.

5.6.3 New and Improved

The following items are new and improved for this release:

Processing and Displaying Evidence Counts

Registry Setting to Restrict Count Updates

When you open the *Examiner* > *Overview* tab, queries are run to calculate the evidence counts in multiple categories: *Evidence Groups*, *File Extension*, *File Category,* and *Labels*. If you have a large case, you can speed up performance by calculating counts in only one category. You can now configure a registry setting that will let you specify one category to calculate.

You can restrict this in one of two ways:

- Through a registry setting
- In the Examiner interface

You can restrict calculation to a single evidence category by adding a settings entry in the registry. Use the following path in the registry to add the settings value:

HKEY_CURRENT_USER/Software/AccessData/Products/Forensic Toolkit/5.3/Settings/Tabs/Tab7

Add value:

OverviewUpdateType REG_DWORD *2*

You can use the following data values:

FILE CATEGORY	2
FILE EXTENSION	3
LABELS	6
EVIDENCE GROUPS	7

As an alternative, in the Examiner interface, you can click on an item within one of these evidence categories and press the *Home* key on the keyboard to reduce the case overview tree to only that item and it's children. For example, you can reduce the case overview tree to showing only *Documents*. This choice is stored in the settings for the Overview tab. You can click on an item in the reduced tree and press the *End* key on the keyboard to restore the full case overview tree.

Hiding the Total Logical Size

When viewing evidence in the Examiner, the Total Logical Size (Total LSize) is calculated for different categories of evidence. To speed up the interface for large cases, you can disable the calculation and display of this value by adding a registry value:

HKLM\SOFTWARE\AccessData\Products\Forensic Toolkit\version

Add value:

hide_total_logical_size DWORD value *1*

Use 0 to display the value.

Examiner

Search

- If a case was originally processed using distributed processing, when a reviewer conducts a live search, the system will first attempt to use the computer with the distributed processing engine, but if it is not available, it will use the reviewer’s local computer to conduct the search.

Memory Allocation

- Previously, when entering the Examiner, whenever you clicked any tab for the first time, memory was allocated for displaying graphic and video thumbnails. Now, memory is only allocated if the tab uses the Thumbnail pane.

Filters

- The Cache Common Filters feature has been removed.

Natural Viewer

- The INSO version for the Natural tab has been updated.

DBControl

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

Fixed Issues in 5.6.2 and 5.6.3

The following issues have been fixed in this release:

System

System Users

- If you create a new user, but do not assign a role at that time, that user's name will now appear in the list when assigning users to a case. (27448)

Processing

- Evidence counts for deleted files are correct when the *Include Deleted Files* processing option is enabled and the *Meta Carve* option is not enabled. (27149)
- When an index merge is occurring in one case, adding evidence to another case can complete without delays. (29803)'If multiple people are working in the same case, one user performing Additional Analysis does no lock the interface for other users. (30083)
- Fixed an issue that caused the following processing error: "Post-Processing: RestoreObjectConstraints failed". (30117)
-

Distributed Processing

- You can successfully decrypt files when using Distributed Processing Manager. (17083)
- Files are exported successfully when using Distributed Processing Manager. (24867)
- When using distributed processing, you can successfully "Process Manually Carved Items". (27563)
- When using distributed processing, you can successfully process large sets of data with meta carving. (29563)

Regional Settings

- When using German (non-U.S) regional settings and language, you can successfully restore a case (28290)
- When using German (non-U.S) regional settings and location, Geolocation EXIF longitude and latitude data is displayed properly. (28518)

PostgreSQL

- When using PostgreSQL and when deleting a case, the case schema is no longer orphaned in the database. (7148)
- A large case on PostgreSQL opens quicker. (28759)

Examiner

Geolocation

- If you create a case in one language and then back it up and the try to restore it to a different language, it no longer causes problems in Geolocation. (29449)

Search, Labels, and Filters

- Running an index search in a large case no longer blocks other activities. (29818)

Decryption

- Fixed some issues decrypting files with GuardianEdge. (31119)

Other

- Queries do not lock the database. (30056)
- You can successfully cancel a query from within the application. (30468)
- Enhanced performance when trying to view many objects in a large case. (30219)
- Performance has been enhanced when changing tabs. (29975)
- Performance has been increased in the Thumbnail view. (30365)
- When opening File Content > Properties, it opens at the top. (30325)

Important Information

Latest Documentation

- The User Guide that is loaded from the Help menu may not be the latest available version.
  The latest FTK documentation is located at:
  http://www.accessdata.com/support/product-downloads/ftk-download-page

Installation and upgrade

- For FTK installation and upgrade instructions, see the *FTK Quick Install Guide* and the detailed *FTK Installation Guide* which are available at
  http://www.accessdata.com/support/product-downloads/ftk-download-page
- FTK supports Distributed Processing Engines (DPEs).
  Before installing Distributed Processing, see the *Install Guide*.

Upgrading CodeMeter

- FTK 5.6.1 and later include an updated version of CodeMeter Runtime Kit (5.21).

- If this is a new installation of FTK you do not need to do anything and the latest version of CodeMeter is installed.
- If you are upgrading to FTK 5.6.1, be aware that a security vulnerability has been detected in Codemeter 4.5. However, if you simply upgrade from CodeMeter 4.5 to 5.21, the vulnerability remains. To fix the vulnerability, you must manually uninstall 4.5 before installing 5.21.

  If you are upgrading to FTK 5.6.1, manually uninstall CodeMeter first and then install FTK 5.6.1 which will install a clean CodeMeter 5.21. Otherwise, after upgrading to FTK 5.6.1, manually uninstall CodeMeter 4.5 and then manually install CodeMeter 5.21.

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 get corrupted.

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

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.
- If you choose to have a case's database files placed in the case folder, do not move your case folder without first archiving and detaching the case.

Where to get more information

Use the following documentation resources to learn more about this product. Each document is available in PDF format in the download ISO file. The *User Guide* is also available through the *Help* menu in FTK.

The latest version of each document is available in the *Product Release* pane on the FTK product download page:

http://www.accessdata.com/support/product-downloads/ftk-download-page

Document	Description
Quick Installation Guide	Basic information about how to install and upgrade this and related products.
FTK Installation Guide	Information about how to install and upgrade this and related products.
User Guide	Information about how to use this product, including detailed technical information and instructions for performing tasks.
Upgrading, Migrating, and Moving Cases	Information about upgrading and migrating cases from 4.1 to 4.2, and moving cases from one database to another.
Upgrading Cases	Information about upgrading cases from 4.1 to 4.2.
Migrating Archived Cases	Information about upgrading or migrating cases that you have archived in a previous release.
KFF Quick Install Guide and KFF installation files	For the most current KFF Server and KFF data installation files, as well as the *KFF Quick Install Guide*, visit the AccessData Product Downloads page: http://www.accessdata.com/support/product-downloads Expand the *Known File Filter (KFF)* section and then the *KFF Server* section.

Comments?

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

AccessData Forensic Toolkit 5.6.1 Release Notes

Document Date: 3/09/2015

Introduction

This document lists the new features, fixed issues, and known issues for Forensic Toolkit® (FTK®) 5.6. All known issues published under previous release notes still apply until they are listed under “Fixed Issues.”

Supported Platforms

For a list of supported platforms for Forensic Toolkit® (FTK®), see the following:

http://accessdata.com/solutions/digital-forensics/forensic-toolkit-ftk/technical

Important: In future versions of Forensic Toolkit® (FTK®), it will no longer support running on Windows XP.

5.6.1 New and Improved

The following items are new and improved for this release:

Filters

- In the Filter Definition dialog, there is now a option to select all of the listed properties.
- The Cache Common Filters feature has been removed.

Search

- When performing a live search, and selecting a file in the search results, the appropriate File Content viewer will be used based on the Code Page of the term. For example, if searching a term using Chinese characters, the appropriate Code Page will be detected and the term will be displayed in the Text view.

File List

- To provide more context for column names in the File List, the tooltip now displays the long column name which provides additional information about he column.

Other

- When performing a search using Chinese characters, if the characters are together without spaces, they are treated as a phrase rather than as two separate items.

Fixed Issues in 5.6.1

The following issues have been fixed in this release:

Installation

- The Processing Engine installer in the FTK Suite installation properly recognizes if the Processing Engine was previously installed with Summation. (27056, 27150)

Processing

- You can successfully decrypt files when using a distributed Processing Manager. (17083)
- Reports generate successfully when using a distributed Processing Manager. (24866)
- Files are exported successfully when using a distributed Processing Manager. (24867)
- File count and index count inconsistencies have been resolved. (6728)

KFF

- When creating a new case or running Additional Analysis, the drop-down list of KFF groups automatically refreshes to show newly created groups. (25031)
- The Edit Group pane automatically refreshes after making changes. (23637)

Filters

- An imported filter successfully calculates the size of files in images. (25142)
- An imported custom filter that has over 600 properties returns results quickly. (25150)

Other

- When looking at recovered deleted files that use Chinese characters in the file name, the files names display correctly. (23741)

Important Information

Latest Documentation

- The User Guide that is loaded from the Help menu may not be the latest available version.
  The latest FTK documentation is located at:
  http://www.accessdata.com/support/product-downloads/ftk-download-page

Installation and upgrade

- For FTK installation and upgrade instructions, see the *FTK Quick Install Guide* and the detailed *FTK Installation Guide* which are available at
  http://www.accessdata.com/support/product-downloads/ftk-download-page
- FTK supports Distributed Processing Engines (DPEs).
  Before installing Distributed Processing, see the *Install Guide*.

Upgrading CodeMeter

- FTK 5.6.1 and later include an updated version of CodeMeter Runtime Kit (5.21).
  - If this is a new installation of FTK you do not need to do anything and the latest version of CodeMeter is installed.
  - If you are upgrading to FTK 5.6.1, be aware that a security vulnerability has been detected in Codemeter 4.5. However, if you simply upgrade from CodeMeter 4.5 to 5.21, the vulnerability remains. To fix the vulnerability, you must manually uninstall 4.5 before installing 5.21.
    If you are upgrading to FTK 5.6.1, manually uninstall CodeMeter first and then install FTK 5.6.1 which will install a clean CodeMeter 5.21. Otherwise, after upgrading to FTK 5.6.1, manually uninstall CodeMeter 4.5 and then manually install CodeMeter 5.21.

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

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.
- If you choose to have a case's database files placed in the case folder, do not move your case folder without first archiving and detaching the case.

Known Issues in 5.6.1

The following items are known issues in this release:

Processing

- During processing, if you enable *Expand Compound Files*, and enable the MS Office, OLE and OPC documents option, the processed file counts may be incorrect. (27149)
- Image files may not have a thumbnail created for them if KFF is enable while processing. The job log lists any failures. (26954)

Filters

- When applying a time-based filter, such as having a rule Created Date Is Before 1/1/2008, files may not be filtered correctly. (26649)

Decryption

- When exporting emails with attachments to MSG that were encrypted with Credant, the attachments are not decrypted making them unreadable. (24800)
- An image from Windows 7 with TPM and BitLocker may show as an Unrecognized File System. (27171)

KFF

- Running KFF on a Windows 7 32 bit computer may not flag all the files it should. (26896)
- Archiving .HKE data may not save any data. (28007)

Search

- On 32-bit computers, when Expanding Terms, the Wordnet dictionary may fail to initialize or function properly. (25233)

Processed Data Display

- After enabling the *IE Recovery* and *IE Web Cache* expansion options and looking at the data, data from IE 11 is contained folders that are named differently (includes a *IE Web Cache* prefix) than data from IE 9 and 10.

Imager

- AccessData Imager 3.x may fail when detecting an EX01 image. (22929)
- AccessData Imager 3.3 may not recognize all partitions for EnCase 7 E0. (26307)

Where to get more information

Use the following documentation resources to learn more about this product. Each document is available in PDF format in the download ISO file. The *User Guide* is also available through the *Help* menu in FTK.

The latest version of each document is available in the *Product Release* pane on the FTK product download page:

http://www.accessdata.com/support/product-downloads/ftk-download-page

Document	Description
Quick Installation Guide	Basic information about how to install and upgrade this and related products.
FTK Installation Guide	Information about how to install and upgrade this and related products.
User Guide	Information about how to use this product, including detailed technical information and instructions for performing tasks.
Upgrading, Migrating, and Moving Cases	Information about upgrading and migrating cases from 4.1 to 4.2, and moving cases from one database to another.
Upgrading Cases	Information about upgrading cases from 4.1 to 4.2.
Migrating Archived Cases	Information about upgrading or migrating cases that you have archived in a previous release.
KFF Quick Install Guide and KFF installation files	For the most current KFF Server and KFF data installation files, as well as the *KFF Quick Install Guide*, visit the AccessData Product Downloads page: http://www.accessdata.com/support/product-downloads Expand the *Known File Filter (KFF)* section and then the *KFF Server* section.

Comments?

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

AccessData Forensic Toolkit 5.6 Release Notes

Document Date: 12/08/2014

Introduction

This document lists the new features, fixed issues, and known issues for Forensic Toolkit® (FTK®) 5.6. All known issues published under previous release notes still apply until they are listed under “Fixed Issues.”

Supported Platforms

For a list of supported platforms for Forensic Toolkit® (FTK®), see the following:

http://accessdata.com/solutions/digital-forensics/forensic-toolkit-ftk/technical

Important: In future versions of Forensic Toolkit® (FTK®), it will no longer support running on Windows XP.

5.6 New and Improved

The following items are new and improved for this release:

Installation

- There is a simplified FTK installer that makes it easier to install all of the FTK components.

System Information Tab

There is a new *System Information* tab. This tab lets you view system information that contains detailed information about disk images in an easy to read format. You can view several important pieces of information about the target computer and the users of that computer.

Not all attributes are available for all disk images, however, the possible attributes that you can see are:

- Applications
  - Prefetch
  - User Assist
  - Installed

- Network Information
  - Network Shares
  - Network Connections
  - Wireless Profiles
- Owner Information
- Recent Files
  - LNK
  - NT User
  - Shortcuts
- SAM Users
- USB Devices

Processing

- Entity Extraction

  There are new *Entity Extraction* processing options that identify and extract specific types of data in your evidence. You can process and view each of the following types of entity data:

  - Credit Card Numbers
  - Phone Numbers
  - Social Security Numbers

  In the *Examiner*, under the *Document Content* node in the *Overview* tab, you can view the extracted data.

- Exchange 2013 Support

  You can now collect and process data from Exchange 2013 .

- New *Enable Standard Viewer* processing option

  There is a new processing option called *Enable Standard Viewer*, which is intended for functionality when viewing data in *Resolution1 eDiscovery* or *Summation*. This option does the following:

  - During processing, for document files (such as .TXT, .DOC, .PPT, .MSG, and so forth), a file is created in SWF format that you can annotate and redact.

    This is done for files that are 1 MB or larger. For smaller files, they are generated on-the-fly when you select them in *Review*.

    The new files are saved in the case folder as .DAT files in SWF format.

  - When opening *Review* in *Resolution1 eDiscovery* or *Summation*, the default viewer is the *Standard Viewer*.

    When the *Standard Viewer* is used, the converted SWF file is displayed rather than the original native file. This enables you to work on a file, such as doing redactions, without having to manually create the SWF file first.

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

- *Create HTML for Email* processing option

  The *Create HTML for Email* option has been removed from the *Lab/eDiscovery Options* evidence processing page.

KFF

The KFF feature has a new architecture and has the following enhancements:

- KFF Server includes an enhanced lookup service
- Supports importing billions of hash sets
- Faster performance
- Simpler implementation by using only KFF Groups and Sets (KFF Libraries and Templates are no longer used)
- Enhanced import functionality
- You can create an archive of all KFF data on one server for backup or sharing across multiple servers.
- New utility for migrating legacy KFF data to the new architecture.

KFF Notes:

- The same import and export formats from previous versions of KFF are supported.
- The method of installing NSRL, NDIC, and DHS data has been updated.
- NSRL updates for the legacy KFF format will end in the 2nd quarter of 2015. From that time, NSRL updates will only be provided in the new format.
- Geolocation uses the new KFF Server to process the location data for Geolocation maps and there are new installation files for Geolocation data.

Decryption

- Credant version 7.7 is now supported in both online and offline key bundle modes.

Volume Shadow Copy

- Support for encrypted drives to detect and find restore points with Volume Shadow Copy has been added.

Bookmarks

- The following Improvements have been made in the usability of the Bookmarks HTML editor:
  - New descriptive icons and tool tips
  - A new color picker for text and background colors

Search

- Search results are displayed faster.

Case Management

- If you have a licence for Summation or Resolution1, when you back up a case, you can also select to backup the Summation or Resolution1 application database.

IPv6 Support

- The AD Enterprise Management Server and the Enterprise agents now support IPv6.

Agent

- McAfee ePO packages are no longer supported.

Fixed Issues in 5.6

The following issues have been fixed in this release:

Administration

- When you create a new user with the Application Administration role, you are prompted to create a password reset file. (11311)
- When using Copy Previous Case, all files and folders are properly copied. (20585)
- When installing the Processing Engine in Windows 8.1, if the logged in user name has a space in it, the installer no longer fails. (21399, 21894)

Processing

- When processing data from a FileVault2 image, the *Discovered Items* count is now correct. (14530)
- When processing data from a FileVault2 image, JPG images are now processed correctly. (14488)
- You no longer get the error "No restore points were detected on the given source" when configuring the processing options for a PGP image and clicking the *Choose Restore Points* button. (13480)
- When expanding PST and OST files, emails are expanded properly. (20568)
- When processing with Restore Points" enabled, processing no longer hangs. (11899)
- When processing with the Meta Carve enabled, items are carved properly. (16316)

Bookmarks

- After playing a media file from a bookmark, such a video, and then selecting a different bookmark or file in another tab, the media playback is now stopped. (15664, 16992)
- Selections added to a bookmark from an Index search are now being selected properly in the Bookmark tab. (14713)
- Bookmark comments using HTML formatting now display correctly in Timeline Reports. (16854)
- File comments are saved correctly in bookmarks. (13266)
- The option to bookmark selected text works properly. (13959)

Columns

- The following new Filename columns have been added:
  - *Filename Access Date*
  - *Filename Create Date*
  - *Filename MFT Change Date*
  - *Filename Modify Date*
- In the *Manage Columns* dialog, many column short names have been updated. (23361)

Import

- Importing a file that is in use by another program no longer causes a fatal error. (14371)

Export

- When exporting File List Info, the local time is now kept as well as the UTC time. (21109)
- When exporting File List Info, the Deleted column is no longer blank. (23253)

Indexing

- The *Indexed* filter no longer displays data that was not actually indexed during processing. (13383)

Search

- Selecting files in an Index Search no longer causes the program to stop responding. (13031)
- After deleting an expanded search, and re-searching for the same term, the search performs correctly and the application doesn't hang. (16783)
- Using the arrow keys to expand and navigate through the *Results* pane no longer causes the application to stop responding. (16791)

Evidence Explorer

- Attempting to view a file from an *Index Search* no longer displays an error and now views the file in the *Natural View*. (14566)

Geolocation

- Filtering *Latitude* & *Longitude* columns in *File List* now works correctly. (17531)
- Geotagged *Latitude* & *Longitude* columns in *File List* are populated correctly when the KFF server is not installed. (17368)

Decryption

- Word 97 files are now decrypted correctly. (3450)
- When processing a FileVault 2 image, you are now prompted for credentials. (14699)

Visualization

- PST and OST files properly appear in the Timeline view. (18865)

Other

- Filename filters now properly filter files with Chinese characters in the name. (18682)
- When working with time-based filters, the case time zone is used for date and times offsets. (23894)
- When selecting time-based filters, the application does not crash. (22892)

Cerberus

- Processing no longer fails when enabling Cerberus. (10313)

Important Information

Latest Documentation

- The User Guide that is loaded from the Help menu may not be the latest available version.
  The latest FTK documentation is located at:
  http://www.accessdata.com/support/product-downloads/ftk-download-page

Installation and upgrade

- For FTK installation and upgrade instructions, see the *FTK Quick Install Guide* and the detailed *FTK Installation Guide* which are available at
  http://www.accessdata.com/support/product-downloads/ftk-download-page
- FTK supports Distributed Processing Engines (DPEs).
  Before installing Distributed Processing, see the *Install Guide*.

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

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.
- If you choose to have a case's database files placed in the case folder, do not move your case folder without first archiving and detaching the case.

Known Issues in 5.6

The following items are known issues in this release:

Filters

- If you create a filters using the "TO" email field, it does not return any results if the Operators is set to "Is". (13489)

Decryption

- PGP decrypted partitions are not decrypted properly and return an "Unrecognized file System" error. (14069)

OCR

- Chinese characters may not be indexed correctly when performing OCR. (18753)

Search

- On 32-bit computers, you may get an Out of Memory error when viewing index search results. (17764, 18623)

Entity Extraction

- Some phone number formatting does not generate entity nodes with the whole 10 digit number. (21517)

Compatibility with Summation and Resolution1

- Case created in FTK that have been Archive and Detached and then Attached in FTK won't be displayed or accessible in Resolution1 or Summation. The FTK Archive feature doesn't save the App DB information that Resolution1 and Summation requires. Please use the Backup/Restore feature instead. (22221)
- If you create a project in Resolution1 or Summation, then open it in FTK, delete an evidence item, then go back to Resolution1 or Summation, the evidence is still included in the Project's evidence list. However, when you view the project in Review, the deleted evidence is not displayed. (22012)
- When using the *Enable the Standard Viewer* processing option, the following files cannot be converted to SWF and the processing report reports errors: unallocated space, restore files, config files, and .DAT files. (21975)
- When sharing the same database with Resolution1 or Summation, you may not be able to delete a case using FTK, but can using Resolution1 or Summation. (20971)
- When you add Data Sources in Resolution1 or Summation, they displayed as Evidence Groups in FTK cases. However, Data Sources are not project specific, so in FTK, all Data Sources are shown in a single FTK case. (23426)

Other

- You cannot have two different CodeMeter dongles at the same time. Either remove one dongle or combine all licenses on one dongle. (12043)
- Recovered deleted files with Chinese characters may have garbage characters. (23741)
- .INK files that have Russian characters report "Invalid Shortcut File". (23447)

Where to get more information

Use the following documentation resources to learn more about this product. Each document is available in PDF format in the download ISO file. The *User Guide* is also available through the *Help* menu in FTK.

The latest version of each document is available in the *Product Release* pane on the FTK product download page:

http://www.accessdata.com/support/product-downloads/ftk-download-page

Document	Description
Quick Installation Guide	Basic information about how to install and upgrade this and related products.
FTK Installation Guide	Information about how to install and upgrade this and related products.
User Guide	Information about how to use this product, including detailed technical information and instructions for performing tasks.
Upgrading, Migrating, and Moving Cases	Information about upgrading and migrating cases from 4.1 to 4.2, and moving cases from one database to another.
Upgrading Cases	Information about upgrading cases from 4.1 to 4.2.
Migrating Archived Cases	Information about upgrading or migrating cases that you have archived in a previous release.
KFF Quick Install Guide and KFF installation files	For the most current KFF Server and KFF data installation files, as well as the *KFF Quick Install Guide*, visit the AccessData Product Downloads page: http://www.accessdata.com/support/product-downloads Expand the *Known File Filter (KFF)* section and then the *KFF Server* section.

Comments?

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