AccessData Forensic Toolkit 5.0.1 Release Notes

Document Date: 08/21/2013

Introduction

This document lists the new features, fixed issues, and known issues for Forensic Toolkit® (FTK®) 5.0.1. Please be aware that all known issues published under previous release notes still apply until they are listed under "Fixed Issues."

Important Information

Installation and upgrade:

- For installation instructions, see the *Quick Install Guide* or the *Detailed Install Guide*. You can access these guides at http://www.accessdata.com/support/product-downloads/ftk-download-page.
- FTK supports Distributed Processing Engines (DPEs). Distributed Processing allows the installation of up to three additional processing engines to share the work load of processing evidence in a case.
  Before installing Distributed Processing, see either the *Quick Install Guide* or the *Detailed Install Guide*.
- FTK does not support skipping versions when you upgrade cases from previous major or minor versions. You must upgrade in the order of the released versions. For example, you cannot upgrade cases from FTK 4.1 or earlier directly to FTK 5.x. You must first upgrade 4.1 to FTK4.2.x and then upgrade from FTK 4.2.x to FTK 5.x.
- Whenever possible, install FTK on a physical system. Due to performance, AccessData does not recommend configurations where the database or the Evidence Processing Engine is running on a virtual machine.
- Oracle 10g is not compatible with Windows 8.
- If you are using Oracle, when you first launch FTK and add the database, when you select to use Oracle, you must change the Oracle SID from ADG to FTK2.
- To install the KFF server, you must have admin privileges. Otherwise, you get the following error:
  Unhandled exception has occurred in your application. (9092)

- You may need to adjust the KFF Server thread counts in order for KFF to complete processing.

  If you have too few KFF Lookup Interface threads configured, it can result in KFF not completing and generating the following error in the error log:

  [Date] Failure on item ... Could not connect to KFF Server ..., token ...

  For a computer with a quad core, the default amount of 300 threads should be adequate. If you have a computer with fewer cores, the thread count can be increased. If you get the error, increase the thread count.

  For instructions on configuring KFF, see the *Working with the KFF Library* chapter in the FTK User Guide.

- The Exporting Emails to PST feature requires that you have either Microsoft Outlook or the Microsoft Collaboration Data Objects (CDO) installed on the same computer as the processing engine.

  CDO does not support exporting Unicode email messages. Attempting to export Unicode messages to PST with CDO installed will result in errors and the resulting PST will be missing any Unicode email messages. To export Unicode email messages, install Outlook.

  For more information, see the *Quick Installation Guide*.

  See Where to get more information on page 21.

Data and Database Management

- AccessData recommends that, whenever possible, you not have an active internet connection when running Imager or FTK. If the computer running Imager or FTK has an active internet connection and you are viewing certain types of HTML web pages or binaries, there is a potential risk that is associated with specially crafted pages or binaries. These pages or binaries can trigger unintended consequences, such as running malicious code or scripts.
- If using PostgreSQL, please note the following:
  - If the computer has fewer than 16 cores (< 16), then in the PostgreSQL configuration file, set the max_connections to 60 per computer.

    For example, if there are 4 computers in the Distributed Processing Model in which every computer has fewer than 16 cores, then set max_connections to 240 (60*4).
  - If the computer has 16 or more cores (>= 16), then in the PostgreSQL configuration file, set the max_connections to 125 per computer.
  - For example, if there are 4 computers in the Distributed Processing Model in which 3 computers are 8 core (<16) and 1 computer is 16 core (>=16), then set max_connections to 245 (60*3 + 125*1).
  - If there is just one computer in the Distributed Processing Model, the max_connections should be no less than 100.
- It is strongly recommended that you configure your antivirus to exclude the database (PostgreSQL, Oracle database, Microsoft SQL) AD temp, source images/loose files, and case folders for performance and data integrity.
  - Cerberus writes binaries to the AD Temp folder momentarily in order to perform the malware analysis. Upon completion, it will quickly delete the binary. It is important to ensure that your antivirus is not scanning the AD Temp folder. If the antivirus deletes/quarantines the binary from the temp, Cerberus analysis will not be performed.
- When using an Oracle database, it must be installed on a computer with a name that begins with a letter (a-z and A-Z). Due to a restriction on domain names in RFC 1035, applications cannot connect to Oracle if the computer's name begins with a number. If the Oracle computer name begins with a number, you must change the machine name before installing Oracle.
- 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. (64450)
- If you bookmark a manually carved item that has not been processed, the file does not display in a bookmark or in a report until you process it. You can use the "Process Manually Carved Items" option in the Evidence drop-down menu to process the manually carved item. (57812)

5.0.1 New and Improved

For a list of new and improved features for 5.0, see 5.0 New and Improved (page 12).

The following items are new and improved features and feature enhancements for this release:

Evidence Processing

- The time to perform Static Ram and Memory analysis has been improved.
- The time to perform Field Mode processing jobs has been improved.
- The time to perform Remote Preview jobs has been improved.

Internet Artifacts

- After expanding compound SQLITE files, such as Google Chrome internet history, you can now view the HTML-rendered index within the table. You can also view the structure of the database itself on the Explore tab.

KFF

- **Updated KFF Server**

  The KFF Server has been updated to version 1.2.1.x.

  You can install these updates from one of the following locations:

  - The physical *KFF Installation Disc*
  - The *KFF Installation Disc* ISO
  - Individual installation files

    Both the ISO and the individual files are available in the KFF or the FTK sections on the AccessData product download page:

    http://www.accessdata.com/support/product-downloads

DNA

- There is a new module for DNA (Distributed Network Attack) 7.2 that provides support for RAR 5.0 files.

  The RAR update file is available in the Decryption section on the AccessData product download page:

  http://www.accessdata.com/support/product-downloads

Add on Module Enhancements

This release includes enhancements to the Cerberus add-on module.

For information, see Release Notes for Add-on Modules (page 20).

Fixed Issues in 5.0.1

For a list of issues that were fixed 5.0, see Fixed Issues in 5.0 (page 16).

The following issues have been fixed for FTK 5.0.1:

Decryption

- Fixed an issue that prevented the decryption of S/MIME encrypted messages from a PST. The option to decrypt S/MIME files under *Tools* > *Decrypt Files* is now available. (21684)
- Fixed an issue that prevented the decryption of Credant files and not displaying an error. (26316)

Search

- Fixed an issue that sometimes caused slow results when running an indexed search. (25584).
- Fixed an issue that caused the item numbers in exported search results (CSV file) to not match the object numbers in the application. (26304)
- Fixed an issue that sometimes caused a slow response when expanding and retracting search options. (15156)

Processing

- When running Additional Analysis and selecting *Explicit Image Detection*, the required option of *File Signature Analysis* is now automatically selected as well. (26749)
- Fixed an issued that caused Facebook JSON files from being listed in the *Overview* tab under *Unknown Types\Unknown*. They are now listed under *Other Known Type*s in a *JSON* file category. (26824)

Reports

- Fixed an issue that when generating a Timeline Report, the forward slashes did not appear correctly in Excel (25596).

Filters

- Fixed an issue that caused an error *[Missing string: 11611]* when creating a filter using the *Language* filter. (24992).
- Fixed an issue that caused filtering to sometimes not work properly when attempting to exclude non-English files. (24942)
- Fixed an issue that caused an edited custom filter to not save when the filter referred to other filters. (26747)
- Fixed an issue that caused a Label filter to filter out all files rather than the ones that were labeled. (27793)
- Fixed an issue that caused rules to sometimes not work properly in filters causing files to be listed that were not expected. (29505)

KFF

- Fixed an issue that caused KFF groups to sometimes not function properly after uninstalling and re-installing KFF data. (23522)
- Fixed an issue that caused FTK to become unresponsive if the KFF server was stopped and Additional Analysis was run with *KFF* selected. (24027)
- Fixed an issue that sometimes caused an Error 22 to be returned when importing a KFF or XML file. (24129)
- Fixed an issue that sometimes caused the following error when installing the KFF Server on XP computers: "Error 1920. Service AccessData KFF Server (ad_kff) failed to start. Verify that you have sufficient privileges to start system services." (25290)
- Fixed an issue that sometimes caused the default KFF group from being used when processing rather than the selected group. (28434)
- Fixed an issue that sometimes caused a “Failure on item...Could not perform KFF lookup on object” error. (26645)

Agent

- Fixed an issue that when adding remote data (Image Drive) using the Temporary Agent, the agent sometimes failed. (27692)

Other

- Fixed an issue that caused the UI to be very slow when expanding the Explore tab when there are many disk images in the case. (28891)
- When managing column settings, fixed an error that sometimes caused duplicate column names to appear. (23820)
- In the column settings dialog, the columns associated with PhotoDNA now have descriptions (23719).
- Fixed an issue that prevented the scroll bar to appear in the Administer User page. (24154)
- Fixed an issue that sometimes caused errors when importing multiple carvers files. (23720)
- Fixed an issue that if the case folder was manually deleted or moved during the time that the case was created, it caused the interface to hang. (21587)
- Fixed an issue that sometimes an occurred when closing FTK on Windows XP computers and getting a message that ‘it encountered a problem and needs to close’. (25739)
- When running in evaluation mode, the product title bar now displays “Evaluation Version” at the end of the title. (26997)
- All items assigned to the OLE Storage category now have a folder icon instead of a light bulb icon. (26626)
- In the column settings dialog, the columns associated with PhotoDNA now have descriptions (23719).
- Fixed an issue that caused inconsistent counts when enumerating NTFS file systems with additional threading (24868)

Known Issues in 5.0.1

For a list of known issues that existed in 5.0, see Known Issues in 5.0 (page 18).

The following items are known issues:

Rights and Permissions

- If you only have one user account with the Application Administrator role, and you change that user's role, you no longer have a user with Application Administrator rights. The application does not prevent or warn you that there is not another admin. You must re-install the application and the database. (25369)

Decryption

- When running an environment that has Microsoft RMS and that has Outlook on it, and you restrict emails, Outlook emails cannot be decrypted. (25505)
- When running an environment that has Microsoft RMS, and you restrict Office documents, they cannot be decrypted. (25608)
- When using the *Decrypt Credant Files* processing option, Credant files may not get decrypted. If using the *Tools* > *Credant Decryption* option in the Examiner, decryption works properly. (24443)
- Clicking on a file in the Examiner that is encrypted with Credant may cause the Examiner to crash. (26492)
- When using Distributed Network Attack (DNA), if more than one job is running, and if you delete one job and then re-add it, the job that was not deleted and re-added is placed in a queued status and you must manually pause and resume the job for it to continue. (26201)
- The following encrypted files cannot be decrypted using the Perform Automatic Decryption option during processing. Instead, you must use the *Tools* > *Decrypt Files* option in the Examiner. (26665)
  - EFS, Lotus Notes (whole), Lotus Notes/emails, SMIME, and Credant.

Processing

- Selecting the *Expand Compound Files* > *RFC822 Internet Email* option does not expand internet mail files. (25606)
- The Fuzzy Hash feature is not reporting correct data. (24883)
- When performing Additional Analysis, the *Registry Reports* option requires that *File Signature Analysis* also be selected. It is not automatically selected and you must select manually in order to generate the reports. (27001)

Search

- If using Oracle as the database, and if you apply over 100 individual index searches, additional files are not displayed in the list. Then if you apply any filter and then attempt to export all the hits in file, the dialogue box will not appear for the export. (26136)

Internet Artifacts

- If the full_path column is missing in the Chrome History SQLite file, you are unable to view data in the Natural view or drill down into the History file. (26433)

Reports

- When creating reports using the File Category, File Extension, or File Status categories, you are unable to generate the report in the following formats: RTF, WML, DOCX, and ODT. You will get a Format Transformation error. (26294)

Agent

- When adding remote data (Image Drive) using the Temporary Agent, and then trying to cancel the job, the cancel buttons turn inactive (for both the Creating Image and the Verifying Image tasks). Then when trying to exit FTK, you may get the error message "Cannot disconnect agent while there are active acquisitions." You must end FTK.exe in task manager. (27694)
- If you attempt to install the FTK Temporary Agent and you specify an invalid IP address, you get a Server Busy error and you cannot cancel it. You must restart FTK. (27648)

KFF

- When a connection with the KFF Server is lost, and then trying to add evidence to a case, you may get an error that the evidence cannot be processed. (27909)

Internet Carvers

- The following carvers that were added in FTK 5.0 are not available in the Processing Options. (28169)

  - Ares P2P
  - Chrome History
  - Dropbox
  - eMule
  - Facebook
  - Flickr
  - Google Docs
  - Google Drive
  - Google Plus
  - Google Plus Chat
  - Hotmail
  - ICQ 7M Chat History
  - Internet Explorer 10
  - Safari
  - Shareaza
  - SkyDrive
  - Skype\Skype 3
  - Torrent
  - Twitter
  - World of Warcraft
  - Yahoo

Other

- The language identification feature may sometimes mis-identify languages when they are similar. For example, Italian may be mistaken for Spanish and Dutch for German. (21872).
- When configuring Additional Analysis, if you select a tab, then press escape, the tap display goes blank. Click another tab and the view is restored. (27688)
- From the File > Reports page, if you click a tree item and then press escape, the tree view goes blank. You must restart Examiner. (27689)

- When creating a new filter, the Zip Code property is not recognized. (26278)

Release Notes for Add-on Modules

5.0.1 Release Notes for the Cerberus Add-on

There is an add-on module for malware analysis that is called Cerberus. Cerberus is integrated to allow you to detect and triage suspect binaries. You can determine the behavior, intent, and potential threat of suspect binaries without waiting for a malware team to perform weeks of analysis. Cerberus requires an additional license. For more information, see http://accessdata.com/.

For the Release Notes for Cerberus for previous versions, see the following:

- 5.0 Release Notes for the Cerberus Add-on (page 20)

Known Issues:

- Avast Antivirus is flagged as a threat. (20938)

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	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.

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 5.0 Release Notes

Document Date: 06/04/2013

Introduction

This document lists the new features, fixed issues, and known issues for Forensic Toolkit® (FTK®) 5.0. Please be aware that all known issues published under previous release notes still apply until they are listed under "Fixed Issues."

Important Information

Installation and upgrade:

- FTK does not support skipping versions when you upgrade cases from previous major or minor versions. You must upgrade in the order of the released versions. For example, you cannot upgrade cases from FTK 4.1 or earlier directly to FTK 5.0. You must first upgrade 4.1 to FTK 4.2.x and then upgrade from FTK 4.2.x to FTK 5.0.
- Whenever possible, install FTK on a physical system. Due to performance, AccessData does not recommend configurations where the database or the Evidence Processing Engine is running on a virtual machine.
- If you are using Oracle, when you first launch FTK and add the database, when you select to use Oracle, you must change the Oracle SID from ADG to FTK2.
- To install the KFF server, you must have admin privileges. Otherwise, you get the following error:

  Unhandled exception has occurred in your application. (9092)
- You may need to adjust the KFF Server thread counts in order for KFF to complete processing.

  If you have too few KFF Lookup Interface threads configured, it can result in KFF not completing and generating the following error in the error log:

  [Date] Failure on item ... Could not connect to KFF Server ..., token ...

  For a computer with a quad core, the default amount of 50 threads should be adequate. If you have a computer with less cores, the thread count should be at least 150. If you get the error, increase the thread count.

  For instructions on configuring KFF, see the *Working with the KFF Library* chapter in the FTK User Guide.

- The Exporting Emails to PST feature requires that you have either Microsoft Outlook or the Microsoft Collaboration Data Objects (CDO) installed on the same computer as the processing engine.

  CDO does not support exporting Unicode email messages. Attempting to export Unicode messages to PST with CDO installed will result in errors and the resulting PST will be missing any Unicode email messages. To export Unicode email messages, install Outlook.

  For more information, see the *Quick Installation Guide*.

  See Where to get more information on page 21.

Data and Database Management

- AccessData recommends that, whenever possible, you not have an active internet connection when running Imager or FTK. If the computer running Imager or FTK has an active internet connection and you are viewing certain types of HTML web pages or binaries, there is a potential risk that is associated with specially crafted pages or binaries. These pages or binaries can trigger unintended consequences, such as running malicious code or scripts.
- It is strongly recommended that you configure your antivirus to exclude the database (PostgreSQL, Oracle database, Microsoft SQL) AD temp, source images/loose files, and case folders for performance and data integrity.
  - Cerberus writes binaries to the AD Temp folder momentarily in order to perform the malware analysis. Upon completion, it will quickly delete the binary. It is important to ensure that your antivirus is not scanning the AD Temp folder. If the antivirus deletes/quarantines the binary from the temp, Cerberus analysis will not be performed.
- When using an Oracle database, it must be installed on a computer with a name that begins with a letter (a-z and A-Z). Due to a restriction on domain names in RFC 1035, applications cannot connect to Oracle if the computer's name begins with a number. If the Oracle computer name begins with a number, you must change the machine name before installing Oracle.
- 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. (64450)
- If you bookmark a manually carved item that has not been processed, the file does not display in a bookmark or in a report until you process it. You can use the "Process Manually Carved Items" option in the Evidence drop-down menu to process the manually carved item. (57812)

5.0 New and Improved

The following items are new and improved features and feature enhancements for this release:

Evidence Processing

- **Processing Profiles**

  When you create a case, you can configure and re-use profiles, like templates, of processing options. You can create different profiles for different investigative needs. For example you can create one profile for email investigations and another for media investigations. You can then choose from these profiles prior to processing data in a case. This provides processing consistency and saves time by not requiring you to define the exact processing settings for each case. There are two pre-configured profiles: a standard default and a field mode. You can also export and import processing profiles so that they can be shared.

  Processing profiles replace the *Save As My Default* and the *Reset to Factory Defaults* options.

  The *Field Mode* check box has been removed and is replaced by a Field Mode processing profile.

- **New internet artifact carvers**

  Several new internet carvers have been added to the processing options. These provide additional carving capability for more internet artifacts. The following is a list of programs identified by the new carvers:

  - Ares P2P
  - Chrome History
  - Dropbox
  - eMule
  - Facebook
  - Flickr
  - Google Docs
  - Google Drive
  - Google Plus
  - Google Plus Chat
  - Hotmail
  - ICQ 7M Chat History
  - Internet Explorer 10
  - Safari
  - Shareaza
  - SkyDrive
  - Skype\Skype 3
  - Torrent
  - Twitter
  - World of Warcraft
  - Yahoo

- **Ability to add CSV as individual records to support timeline analysis**

  There is a new processing option that will recognize CSV files that are in the Log2timeline format and parses the data within the single CSV into individual records within the case. The individual records from the CSV will be interspersed with other data, giving you the ability to perform more advanced timeline analysis across a very broad set of data. In addition you can leverage the visualization engine to perform more advanced timeline based visual analysis. When you expand CSV files into separate records, you can use several new columns in the File List to view each CSV Log2timeline field.

Visualization

- **Visualization is now a standard feature**

  The visualization module lets you view file, email, and internet browser history data in multiple display formats, including time lines, cluster graphs, pie charts and more. This functionality lets you quickly determine relationships in the data and find key pieces of information.

- **New Social Analyzer II Visualization**

  Email Social Analyzer has been improved and now supports case wide visual analytics. The Social Analyzer Visualization function lets you see the big picture of email domain clusters talking to each other.

You can multi-select and drill-down into specific domains to see individual email addresses and who the communicated with in other domains. This feature provides a more interactive way to view email communication and cull data based off of domain and emails of interest.

- **Screenshot support for Visualization**

  A method for taking a screenshot of a Visualization filter and including it as part of a report has been added. While working within the Visualization screen, you may want to capture the graphic representation of the data you are viewing for reporting purposes. There is now an option to take this screenshot, add a note, and include them as part of the final report.

Mobile Phone Examiner Plus (MPE+)

FTK 5.0 ships with the following features:

- **30-day evaluation license of MPE+**

  MPE+ is a stand-alone mobile forensics software solution that supports 6800+ devices, Including iOS®, Android™, and Blackberry® devices. MPE+ images integrate seamlessly with FTK software, allowing you to correlate evidence from multiple mobile devices with evidence from multiple computers within a single interface.

- **One year of MPE+ Essentials**

  MPE+ Essentials is a modified version of MPE+ that allows you to analyze data from only iOS and Android devices.

Explicit Image Detection

- **Explicit Image Detection is now a standard feature**

  Much more than just a flesh tone detector, the Explicit Image Detection (EID) feature allows for easier location and identification of potentially explicit material. This option is available when creating a new case.

File Decryption

- **Decrypt files during processing with a password list**

  A new processing option allows you to automatically decrypt encrypted files during processing by pre-defining a password list. As files are identified as encrypted, the passwords are used to try to decrypt them and the contents become available. After processing, you can use the Decrypted Files filter to view a list of the decrypted files.

- **Integration with Password Recovery Toolkit (PRTK) and Distributed Network Attack (DNA) for password recovery**

  You can select encrypted files from the file list and submit them directly to PRTK or DNA for password recovery. Once the passwords have been recovered they can be used in FTK to decrypt the respective files. To use this integration, either PRTK or the DNA host must be installed on the same computer as the Examiner.

- **Integration with Password Recovery Toolkit (PRTK) for enhanced file decryption**

  With the appropriate passwords, you can now decrypt most all of the same file formats that AccessData PRTK and DNA can decrypt.

  File families now supported include the following:

  - ABICoder
  - AdvancedFileLock
  - Apple DMG
  - Apple FileVault
  - Apple FileVault 2
  - AShampoo
  - CryptoForge
  - Cypherus
  - iOS backup files
  - OpenOffice
  - PDF
  - PGP password file
  - RAR
  - WinZip adv.encryption
  - ZIP
  - 7-Zip

- **Enhanced Bitlocker Support**
  - You can now decrypt partitions from Windows 8 Bitlocker.
  - You can now enter credentials for and decrypt multiple Bitlocker partitions.

Reports

- **Timeline support for bookmarked items in reports**

  A new bookmark feature lets you send specific bookmarks to a timeline report based on the Created, Accessed, and Modified date of the document. Additionally you can create manual timeline items for notes or other items that are not an actual document in the case. From these bookmarked items, you can generate a CSV formatted timeline report that will put the bookmarked items in chronological order. This provides you a way of putting documents in chronological order for easier visibility into the events that took place for the case.

Internet Artifacts

- **Google Chrome internet artifacts enhancements**
  - *Better organization and support for Google Chrome*

    Google Chrome internet artifacts are now more granularly organized in the Overview Tab (Bookmarks, Cookies, Credit Card Data, Data Profile, Downloads, History, Key Words, Login Data, Top Sites, and Web AutoFill Data) so that you can look for specific artifacts in an easier manner.
  - *Reconstruction of web pages for Chrome*

    You can now see a reconstruction of the web page that was cached when the user was browsing the respective web site.

    Note: If there is not enough data in the cache, the web page will not be reconstructed. Informational data about the history will be displayed instead.
  - *Deeper drill down into Google Chrome artifacts*

    A new processing option enables you to create individual records from a Google Chrome artifact SQLite Database. This provides investigators the ability to bookmark specific records from within the database. For example, if you are looking for a specific Top Site record, you can more easily find and bookmark the record you need.
- **New Internet/Chat Tab**

  A new Internet/Chat tab has been added to the Examiner interface to help you quickly view internet artifacts data. This displays the same data that is shown in the Overview tab under the Internet/Chat section.

- **Renamed Mozilla folder**
  In the Internet/Chat folder, the Netscape folder has been renamed to Mozilla Files.

KFF

- **Updated KFF NSRL 2.40 library**
  The NSRL library has been updated to NSRL 2.40.
  When you install an NSRL update, you must keep the previous NSRL versions installed in order to maintain the complete set of NSRL data.
- **Updated KFF Server**
  The KFF Server has been updated to version 1.2.0.
  You can install these updates from one of the following locations:
  - The *Database (PostgreSQL) and KFF Installation Disc* ISO
  - Individual installation files
    Both are available on the AccessData product download page:
    http://www.accessdata.com/support/product-downloads

Media Investigation

- **Microsoft PhotoDNA Integration**
  A new processing option has been added to provide integration with the PhotoDNA algorithm. PhotoDNA is an image-matching technology developed by Microsoft Research in collaboration with Dartmouth College. It creates a unique signature for a digital image, something like a fingerprint, which can be compared with the signatures of other images to find copies of that image. Like the Known File Filter (KFF), this algorithm can be used to filter images in a case to reduce review time.
  When an image is compared to a PhotoDNA library, the software generates a score between the image and the closest match in the library. The score represents the distance between the two images. If the score is 0 then it means it is an identical or near-identical visual match. If the score is greater than 41943.04 then it is not a match and FTK will not record the match and the field will be blank.
  This feature allows you to:
  - Create a library of DNA values
  - Import and export your DNA libraries
  - View the calculated distance between the values of known images in the library and the images in your case

  Three new columns have been added to allow you to use this feature:
  - PhotoDNA Data
  - PhotoDNA Distance
  - PhotoDNA File ID

Imager

- **Destination Spanning**
  When creating an image, you can now specify secondary locations to be used if the first location fills up.
- **Enhanced Features for Command-line Imager**
  - You can now capture the RAM of a target computer
  - You can now capture the Pagefile contents of the target computer

Database Compatibility with Summation 5.0 and eDiscovery 5.0

Now FTK and Summation or eDiscovery users can work collaboratively -- accessing the same case data on the same database to perform legal review and forensic examination simultaneously.

You can do the following with Summation or eDiscovery cases:

- Open a case
- Backup and restore a case
- Add and remove evidence
- Perform Additional Analysis
- Search and Index data
- Export data

Other

- **Enhanced Vista /Windows 7 Recycle bin parsing**

  Previously, when data was analyzed from the recycle bin, attributes of a file were parsed into different records making it difficult to reconcile the attributes of a single file because they were listed as multiple records within the case. With this enhancement, all of the attributes of a single file are consolidated into a single record for that file. This feature provides an easier way to view and export the data for files within the recycle bin.
- **Automated Language Identification**

  A new processing option has been added that will analyze the first two pages of every document to identify the languages contained within. The user will be able to filter by a Language field within review and determine who needs to review which documents based on the language contained within the document.
- **Modified Additional Analysis page**

  The Additional Analysis page has been separated into three function-based tabs to provide faster identification of processing options.
- **Agent Data Acquisition**

  The speed of acquiring data through an agent has been improved.

Add on Module Enhancements

This release includes enhancements to the Cerberus add-on module.

For information, see Release Notes for Add-on Modules (page 20).

Fixed Issues in 5.0

The following issues have been fixed for FTK 5.0:

Export

- Fixed an issue that caused the "'Export messages from email archives to PST" feature to fail. (15196)
- Fixed an issue that when you decrypted a file, and then exported it to an image, if you processed that image, the file was not decrypted. The exported file is now viewable. (17319)
- Fixed an issue that prevented an NSF file from being exported to a PST file. (11580)
- Fixed an issue that when exporting an AOL Email Archive (PFC) file, either as individual emails (MSG) or the entire archive (PST) the resulting emails did not contain the FROM: field data. (20340)

Processing

- Fixed an issue that caused some processing information to not be stored in the jobinformation.log. (17532)
- Fixed an issue that caused processing to sometimes fail when the Indexing processing option was enabled and you added data with SWF files. (15746)
- Fixed an issue that if using OCR and selecting the B&W and Grayscale option, and then setting the Filter to OCR Graphics, the File List pane may display graphics with color. (13140)

Visualization

- Fixed an issue that caused the *Traffic Details* in Email Visualization to sometimes show all *Sent* and *Received* mail as the total count for *Received Mail*. (17657)
- Fixed an issue that sometimes caused the Visualization pane to be become unresponsive when changing the Timeline date from *Created* to *Modified*. (15171, 21964)
- Fixed an issue that may cause the Visualization pane to be become unresponsive when launching the Social Analyzer if there was no data in the Timespan bar. Now, if no data is available, the Social Analyzer button is deactivated. (22174)
- Fixed an issue that caused the Timeline to change when switching from the Created to Modified file values. (22598)
- Fixed an issue that caused the Row Highlighting to not work correctly in some circumstances. (11589)
- Fixed an issue that caused the email traffic details to sometimes not display properly. (22504)

Bookmarks

- Fixed an issue that when deleting a file from a bookmark, you were prompted to confirm the deletion a second time, and regardless of your response, the file was deleted. This issue only occurred when using Microsoft SQL Server for the database. (18215)

Search

- Fixed an issue that prevented the "Limit Search Hits" from working correctly when doing an Index Search. (14619)
- Fixed an issue that when performing a Live Search, if you clicked Remove more than once, it would clear the whole list. (14896)

KFF

- Fixed an issue that caused an “Error 1721” when uninstalling NSRL data after stopping or uninstalling the KFF Server. (17617)
- Fixed an issue that caused the KFF Server to not restart after uninstalling NDIC data. (18122)
- Fixed an issue that when the 64-bit KFF Server was installed, it was installed to the Program Files (x86). instead of the normal Program Files folder. (22022)
- Fixed an issue that after uninstalling the KFF Server and trying to uninstall the KFF Data, an Error 1721 was returned and you could not uninstall the data. (13920)
- You no longer need to perform a manual reboot of the computer after installing the KFF Server on 64-bit computers. (15000)
- Fixed an issue that when uninstalling the KFF server, the service was not removed. (7279)

Other

- Fixed an issue that caused the Codemeter installation to fail on Windows 8 computers. (68531)
- Fixed an issue that prevented you from viewing deleted emails in a PST. (21582)
- When adding live evidence (files or folders) through Evidence Processing, if it encountered a file that it could not open, there was no error recorded in a log and a 0-byte file was added to the case. An error is now displayed and the error gets reported in the JobInformation.log. (18458)
- Fixed an issue that caused the tree view to not work correctly if graphic thumbnails were dragged off the dock of the Graphics tab. (23359)

Known Issues in 5.0

The following items are known issues:

Search

- When doing a live search with multiple Chinese characters, no results are found. (9471)
- You can only get unicode search results when using Live Search and not dtSearch. (15338)

Reports

- Links to files in a PDF report do not open if Japanese characters are in the file name. The link does work in HTML reports. (22936)
- When creating a report in ODT format, the page numbers display as 0. If you do a page preview, the page numbers will be generated. (22952)

Processing

- Some information is not saved in processing profiles. (21000)

  When you create a custom profile, the settings for *Custom File Identification* or *Event Audit Log* options are not stored in the processing profile. The *Send Email Alert* and *Decrypt Credant Files* settings on the Evidence Processing tab are also not stored in the processing profile.

- When performing data carving, you may get different results when done during Additional Analysis versus processing when adding evidence. This is because during processing when adding evidence, the thumb.db files are included whereas when using Additional Analysis, they are not. (23693)

KFF

- You cannot import .HASH files. (16520, 21671)
- When you import an XML or KFF file, the import will be successful but you may see the following error:

  "Import returned error of: 22"

  You can ignore the error. (24129)
- The version numbers of installed KFF libraries are not displayed in the KFF Manager. (13650)

Decryption

- When decrypting files from the Tools > Decrypt Files page, the decryption progress dialog appears briefly then closes. (23234)

Visualization

- When viewing large amounts of email data in Visualization and adjusting the range of data, the display may take some time to refresh the data. (21881)

Other

- FTK may not launch correctly if installed on Windows Server 2008 R2 or Server 2003 R2 if you also have Adobe Acrobat installed. You may get an error: "The application failed to initialize properly (0xc00000142)". (19148)
- When exporting emails to a PST and using the 'Preserve file structure' option selected, some emails may not display in Outlook. (19086)

CIRT Compatibility

- CIRT job names are only viewable in FTK by node.

  For example, if a job in CIRT is called Collection One, in FTK you only see the IP address of the node it ran against and not the name. (16161)
- Computer software inventory data from a CIRT job does not display when the case is viewed in FTK. (15818)
- FTK does not recognize CIRT users who log into CIRT using Windows authentication. To use a CIRT user in FTK, you must create the user account in CIRT and grant the user the permissions that you want them to have in FTK. (15813)

Summation and eDiscovery Compatibility

- The same documents may be displayed differently in the Natural Views of each product. (23084)
- The search results counts for the same case may be different when viewed in the different products due to the way search options are executed in the respective products. (23005)
- If using Summation or eDiscovery to add evidence to a case that was created in FTK, search does not return results from the new data. (23006) You can do one of the following as a workaround for this issue:
  - Add new evidence to a case using the same application that was used to add the original evidence.

    - After adding the new evidence using eDiscovery or Summation, add either a label or a code to the new data which will cause the new data to be re-indexed.
- If using Summation or eDiscovery to add evidence to a case that was created in FTK, the Processing and Indexing counts may be different due to different processing options. (22945)
- Attempting to view an FTK case in Summation or eDiscovery may sometimes cause an exception error message. (22947)
- The processing options applied to a case are different from which ever product the case is created in. For example, you may create a case in eDiscovery, process the evidence, and then add more evidence using FTK. If you compare the JobInformation.log files, the processing options applied by FTK are different from eDiscovery. (17186)

Enterprise

- If you create a case and include a period at the end of the case name, and then add remote data, no data is shown in the Volatile tab. (17838)

Release Notes for Add-on Modules

5.0 Release Notes for the Cerberus Add-on

There is an add-on module for malware analysis that is called Cerberus. Cerberus is integrated to allow you to detect and triage suspect binaries. You can determine the behavior, intent, and potential threat of suspect binaries without waiting for a malware team to perform weeks of analysis. Cerberus requires an additional license. For more information, see http://accessdata.com/.

Known Issues:

- Avast Antivirus is flagged as a threat. (20938)

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	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.

Comments?

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