AccessData Forensic Toolkit 5.5 Release Notes

Document Date: 8/20/2014

Introduction

This document lists the new features, fixed issues, and known issues for Forensic Toolkit® (FTK®) 5.5. All known issues published under previous release notes still apply until they are listed under “Fixed Issues.”

Important Information

Latest Documentation

- 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*.

Known File Filter

- For information on installing and configuring KFF, see the *KFF Install Guide*, or go to: http://www.accessdata.com/support/product-downloads > *Known File Filter (KFF)*.

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.

5.5 New and Improved

For information about new features in previous releases, see:

- 5.4 New and Improved (page 9)

The following items are new and improved for this release:

Bookmarks

Bookmarks have been enhanced to improve their productivity and usefulness. With the new, enhanced bookmarks, you can:

- Set a bookmark for a video thumbnail. This feature allows you to:
  - Easily create a bookmark for a selection within a video.
  - Adjust the beginning and end of the video selection.
  - Generate a report that contains the actual video clip section that you bookmark.
- Create, edit, and display Bookmark comments in HTML format.
- Create empty bookmarks. You can create an empty bookmark as a placeholder and then add more information at a later time.

Mozilla Firefox

Enhanced Mozilla Firefox support. Features include the following:

- Two new processing options allow you to expand Mozilla Firefox cache and FireFox SQLite files into individual records.
- Mozilla Firefox Internet Artifacts are organized in the *Overview* and *Internet/Chat* tabs.
- Supported artifacts are Bookmarks, Browser History, Cookies, Downloads, Form History, Login Data, Keywords, and Favorites.
- Web pages are reconstructed from the Mozilla Firefox cache and history. When there is not enough data collected to reconstruct the web page, information about the history displays in place of the reconstructed web page.

Graphics

New support for extracting Windows 8/8.1 thumbcache files.

Review

You can now create video thumbnails while viewing videos in the *File Content Viewer*.

KFF

You can now use the right-click menu to close groups that were imported into KFF.

Document Content Analysis

The new Document Content Analysis feature analyzes and then organizes documents into “clusters” for quicker review. Clusters display as groups in the Evidence Explorer and are called *Cluster Topic Containers*. Each *Cluster Topic Container* holds a set of documents that have similar keywords and topics. Documents analyzed include Word documents, text documents, and PDFs.

Language Localization

The program is now available in the following additional languages:

- Portuguese
- Spanish
- Korean
- Chinese

Fixed Issues in 5.5

For information about fixed issues for previous releases, see the following:

- Fixed Issues in 5.4 (page 10)

The following issues have been fixed in this release:

Bookmarks

- Manual Timeline Comments no longer become inactive when changing Column Setting. (13084)
- After making changes to Timeline Bookmark Comments, the **Save Changes** button is now activated. (13172)
- After editing a saved bookmark comment, not saving the changes no longer deletes the entire bookmark comment. (15193)
- The *Save* dialog only appears once when clicking **No** after switching tabs within the bookmark. (15196)
- The **OK** button is now disabled until the Bookmark's required fields are completed. (15348)

Evidence Explorer

- Viewing certain Internet history entries no longer cause the application to close. (15367)

Search

- The *Limits Search Hits* dialog now shows the correct number of default hits to display in the **Hits to Display > First** field. (14559)

KFF

- Sorting by the source column in KFF no longer causes FTK to stop responding. (13109)
- After choosing groups in a KFF template, the **Save** button is now activated. (14687)

Decryption

- Drives encrypted with FileVault 2 are now properly detected. (13354)
- All versions of Lotus Notes NSF files are now properly decrypted. (13746)
- All Word 2000 files now decrypt and display correctly. (15970)

Cerberus

- Cerberus Stage 2 analysis now executes correctly when the threshold is configured to identify files with a Cerberus score that fits that criteria. (9207)

Known Issues in 5.5

For a list of known issues for previous 5.x releases, see the following:

- Known Issues in 5.4 (page 11)

The following items are known issues in this release:

Copy Case

- You cannot use Copy Previous Case from version 4.1 (Oracle Only) to version 5.5. (16829)
- When copying a case from a previous version of the application (Copy Previous Case) that was created with multiple users, the Copy Case process may, in certain situations, fail after assigning those users to the latest version. (12522)

Bookmarks

- Bookmark comments using HTML formatting do not display correctly in Timeline Reports. (16854)
- Deselecting a comment field in a *Timeline Bookmark* does not activate the **Save Changes** button. (16874)
- Bookmark and File Comments are removed when generating a report from the *Bookmark* tab.

  Workaround: Save your bookmark (**Save Changes**) before generating a report from the *Bookmark* tab. (15770)
- Bookmarking an index hit does not highlight the correct selection in the bookmark when processed with KFF. (15672)
- After bookmarking an attachment and choosing to include the Parent Email, when creating the report, the Parent Email will not display in the report or link the attachment. (13972)

Evidence Explorer

- BMP files extracted from Windows 8.1 Thumbcache files are not displaying in the *Natural View*. (14328)
- Attempting to view a file from an *Index Search* displays an error but does not view the file in the *Natural View*. (14566)

Search

- Using the arrow keys to expand and navigate through the *Results* pane may cause the application to stop responding. (16791)

Document Content Analysis

- The *Analysis Method* feature in the *Document Content Analysis Options* dialog does not function and is scheduled to be removed in the next release. (17577)

Other

- At times, working in large cases may cause the application to stop responding. (14392)

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 Under *Current Releases,* 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 5.4 Release Notes

Document Date: 6/6/2014

Introduction

This document lists the new features, fixed issues, and known issues for Forensic Toolkit® (FTK®) 5.4. Please be aware that all known issues published under previous release notes still apply until they are listed under "Fixed Issues."

Important Information

Latest Documentation

- 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
- 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.
- 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 the *Install Guide*.
- Offline versions of the maps used for Geolocation are available. Use the links **Geolocation Map for Offline Use** and **Geolocation Map for Offline ReadMe** on the FTK Product download page:
  http://www.accessdata.com/support/product-downloads/ftk-download-page

PostgreSQL

- 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.

Oracle

- Oracle 10g is not compatible with Windows 8.
- When you first launch FTK and add the database, change the Oracle SID from ADG to FTK2 after selecting Oracle as your database.
- Oracle 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.

Known File Filter

- For information on installing and configuring KFF, see the *KFF Install Guide*, available in the *User Guide* or at:

  http://www.accessdata.com/support/product-downloads > *Known File Filter (KFF)*.
- To install the KFF server, you must have Administrator privileges. Otherwise, you get the following error:

  Unhandled exception has occurred in your application.
- 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 ..."

  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.
- If you are installing KFF in a distributed processing environment, you must specify the KFF server by its IP address and not use 'localhost'. Otherwise you may get incorrect KFF counts.

Recommendations

- 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.

- 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.

Index Search

- Index Searches on ACSCII/UTF-8 files do not recognize any information included in tags. To search tags within ASCII/UTF-8 files, use the Live Search feature.

5.4 New and Improved

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

Administration

- You can now recover forgotten or lost passwords. Using a Password Reset File, you can reset your password. The Password Reset File is unique to your user name, password, and database. Create your Password Reset File and store it in a secure place. When you need to reset your password, simply access the Password Reset File in the Reset Password dialog. After resetting your password, create a new Password Reset File for the next time you need to reset your password.

Attaching/Restoring Cases

- You can now choose the path of the location to store the case's DB files, including a default option to save the DB files in the case folder. This is the same functionality that exists during a Case Creation.

Data Carving

- Added a new data carver for carving TIFF files.

Review

- You can now view Internet Explorer 10 and Internet Explorer 11 web pages in the *Natural Viewer*.

Case Review

- Added additional support that includes Outlook 2013 OST files.

Supported Operating Systems

- You can now install and run the application on Windows Server 2012.

Visualization

- Geolocation Visualization now includes a Geolocation Grid that displays information about each item on the map.
  - The grid has has column-level filters that let you filter the items in the grid.
  - You can view two different tabs:
    - Network Communication: If you launch Geolocation from the Volatile tab, you can view Volatile data.

- Exif: If you launch Geolocation from anywhere but the Volatile tab, you can view Exif data from photos

Fixed Issues in 5.4

The following issues have been fixed in this release:

Case Restore

- When restoring a case that had multiple users with different roles, you no longer get an error when mapping all users to the App Admin or Case Admin roles. (10986)

Bookmarks

- When changes are not made to a bookmark, you are no longer prompted to save your bookmark when exiting. (7601)

Export

- When using *Exporting Children*, the export now maintains the folder and file structure from the child case. (10479)

Language

- The Language Identification filter now works correctly with multiple selected languages. (8856)

Search

- Under *Index Search Options*, you can no longer configure the *Max words to return* option to be lower than the minimum default (16), regardless whether you click **OK** or press **Enter** after entering the new number. (9884)

Reporting

- *Time Zone for Display* now displays the correct time zone when you run a previous report with a different time zone selected. (10202)

KFF

- Fixed the issue where importing some *.csv files would return the status, “Import returned status of: 14.” (4197)
- Sorting by the *Source* column in the KFF dialog no longer cause the program to stop responding. (10570)

Other

- The opening splash screen now loads faster. (8314)

Known Issues in 5.4

The following items are known issues in this release:

Copy Case

- Copy Case does not retain Bookmark Comments and File Comments for the bookmark you copied. (10600)

Data Carving

- GIF carving produces inconsistent results. (9636)

Bookmarks

- When working with large images, using a custom filter delays Bookmark creation. The program stops responding after the Bookmarks are created. (10362)

Restore

- Restoring a case using the *Database Directory* path and selecting **In the case folder** creates two folders. One folder contains the database and the other folder contains the case. (11719)

KFF

- Closing User-Defined groups from imported KFF files generates an error and fails to close. (6930)
- You cannot open a User-Defined group that was previously closed. (10179)

Logging

- Existence of a folder called C:\LOGS causes the program to create large log files and store them in this folder. (9912)

Geolocation

- In the *Filters* dialog, clicking the drop-down fields does nothing.

  Workaround: Using the Up and Down arrows on the keyboard expands the drop-down fields correctly. (11322)
- When using *Quickpick* on a sub folder, the *Heatmap* dialog opens to the root folder. (11361)
- Switching between categories in Heatmap does not retain the category structure from the previous dialog and returns you to the root of the category. (11375)

Cerberus

- Cerberus Stage 2 analysis is missing some items that match the Stage 2 criteria. (9207)

ResolutionOne/FTK Compatibility

- You cannot Archive or Detach in FTK when ResolutionOne is installed on the same computer. (8383)

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 Under *Current Releases,* 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*.