AccessData Forensic Toolkit 5.3.13 Release Notes

Document Date: 9/1/2015

Introduction

This document lists the new features, fixed issues, and known issues for Forensic Toolkit® (FTK®) 5.3.13 that have been added since the release of 5.3.8. Please be aware that all known issues published under previous release notes still apply until they are listed under “Fixed Issues.”

For information about previous releases, see:

- AccessData Forensic Toolkit 5.3.8 Release Notes (page 5)

New and Improved

The following features have been added in this release:

Item List Row Limit

By default, if a case has over 1,000,000 items, the Item List will now display the first 1,000,000 rows and give you an option to display more rows. You can also configure the limit of how many rows are displayed at one time. (30882)

Natural Viewer

The INSO version for the Natural tab has been updated.

Fixed Issues

The following issues have been fixed in this release:

Processing

- If during processing you run our of disk space, the processing pauses. If you make more space available, you can click Resume. (33041, 33241,30620)
- Fixed an issue that caused the following processing error: “Post-Processing: RestoreObjectConstraints failed”. (30117)

Search, Labels, and Filters

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

Filters

- An imported filter successfully calculates the size of files in images. (25142)

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)

Reports

- The information in the Audit log is more concise. (30286)

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 changing tabs. (29975)

Management

- If you attempt to open the Database menu for a database that is not currently running, FTK no longer crashes. (31104)
- After assigning Evidence Groups, the evidence is displayed in the Evidence tree under the appropriate group, and not at the root level. (30714)
- The Database menu option, *Put each case in its own DB*, works properly with a when a new database is used.

Other

- 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)
- Queries do not lock the database. (30056)
- You can successfully cancel a query from within the application. (30468)

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*, available in the *User Guide* or at:
  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.

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 5.3.8 Release Notes

Document Date: 4/20/2015

Introduction

This document lists the new features, fixed issues, and known issues for Forensic Toolkit® (FTK®) 5.3.8. Please be aware that all known issues published under previous release notes still apply until they are listed under "Fixed Issues."

5.3.8 New and Improved

The following features have been added in 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 too 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.

BDControl

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

Fixed Issues in 5.3.8

For information about fixed issues for previous 5.x releases, see the following:

- Fixed Issues in 5.3.7 (page 11)
- Fixed Issues in 5.3.6 (page 14)
- Fixed Issues in 5.3.5 (page 19)

The following issues have been fixed in this release:

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)

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)

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*, available in the *User Guide* or at:
  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.

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*.