AccessData Forensic Toolkit 5.3.6 Release Notes

Document Date: 1/28/2015

Introduction

This document lists the new features, fixed issues, and known issues for Forensic Toolkit® (FTK®) 5.3.6. Please be aware that all known issues published under previous release notes still apply until they are listed under "Fixed Issues."

Fixed Issues in 5.3.6

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

- Fixed Issues in 5.3.5 (page 5)

The following issues have been fixed in this release:

- When attempting to assign additional roles to a user for a case, the assignment is made successfully and you no longer get the following error

  "An error occurred while attempting to connect to the database or the network. Please close and restart FTK ." (25110)
- When viewing thumbnails of graphics, the quality of the thumbnail remains the same regardless of the thumbnail size. (10505)

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 5.3.5 Release Notes

Document Date: 7/29/2014

Introduction

This document lists the new features, fixed issues, and known issues for Forensic Toolkit® (FTK®) 5.3.5. 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
- 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.

5.3.5 New and Improved

For information about new features in previous 5.x releases, see:

- 5.3.4 New and Improved (page 10)
- 5.3.3 New and Improved (page 15)
- 5.3.2 New and Improved (page 20)
- 5.3.1 New and Improved (page 25)
- 5.3 New and Improved (page 31)
- 5.2 New and Improved (page 41)

There are no new features for this release.

Fixed Issues in 5.3.5

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

- Fixed Issues in 5.3.4 (page 10)
- Fixed Issues in 5.3.3 (page 16)
- Fixed Issues in 5.3.2 (page 20)
- Fixed Issues in 5.3.1 (page 25)
- Fixed Issues in 5.3 (page 32)
- Fixed Issues in 5.2.1 (page 37)
- Fixed Issues in 5.2 (page 43)

The following issues have been fixed in this release:

Bookmarks

- When editing a new bookmark, the **Save Changes** button is now active after adding a bookmark or file comment. (15105)
- Creating a bookmark report now correctly labels *Bookmark Comments* in the report. (15106)
- A bookmark now recognizes saved changes to the *File Comment*. Previously, you were prompted to save the bookmark even though there were no changes to be saved. (15108)
- When creating a bookmark report, *Bookmark Comments* created for one bookmark no longer display in subsequent bookmarks. (15110)

Reporting

- Selecting a second-level child bookmark of Shared without selecting the first-level child bookmark now correctly includes the second-level child bookmark in the report. (14836)

KFF

- In the **Manage > KFF** menu, the **OK** button is now immediately available after creating a new group. (4252)
- Sorting by the *Source* column in the KFF dialog no longer cause the program to stop responding. (10570)

Decryption

- Drives encrypted with FileVault 2 are now properly detected. (13354)
- All versions of Lotus Notes NSF files are now properly decrypted. (13746)

Known Issues in 5.3.5

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

- Known Issues in 5.3.4 (page 11)
- Known Issues in 5.3.3 (page 16)
- Known Issues in 5.3.2 (page 21)
- Known Issues in 5.3.1 (page 27)
- Known Issues in 5.3 (page 33)
- Known Issues in 5.2 (page 45)

The following items are known issues:

KFF

- After processing a case with defaults and extra options, the *KFF Admin* window displays the *Case Specific* template. (13399)

Graphics

- The Thumbnail pane on the Graphics tab does not scroll vertically. (13256)

Case Review

- Individually parsed entries for Internet Explorer 9 Cache files do not display in Cool HTML. (3476)

Decryption

- When decrypting drives encrypted with FileVault 2, the decryption completes, but the files detected from the drive are not consistent. (13354)

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 5.3.4 Release Notes

Document Date: 6/19/2014

Introduction

This document lists the new features, fixed issues, and known issues for Forensic Toolkit® (FTK®) 5.3.4. 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 admin 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.

5.3.4 New and Improved

For information about new features in previous 5.x releases, see:

- 5.3.3 New and Improved (page 15)
- 5.3.2 New and Improved (page 20)
- 5.3.1 New and Improved (page 25)
- 5.3 New and Improved (page 31)
- 5.2 New and Improved (page 41)

There are no new features for this release.

Fixed Issues in 5.3.4

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

- Fixed Issues in 5.3.3 (page 16)
- Fixed Issues in 5.3.2 (page 20)
- Fixed Issues in 5.3.1 (page 25)
- Fixed Issues in 5.3 (page 32)
- Fixed Issues in 5.2.1 (page 37)
- Fixed Issues in 5.2 (page 43)

The following issues have been fixed in this release:

DBControl

- In DBControl, you can now assign multiple users to a single user when restoring a case from a previous version of FTK. (12875)

Case

- The *Case Created Date* now displays in Coordinated Universal Time (UTC). (12595)

Parsing

- Hard links parsed from an HFS+ system now display correctly. (9114)

Graphics

- Changes to thumbnail sizes now persist when switching between tabs. (12076)

Reporting

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

Known Issues in 5.3.4

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

- Known Issues in 5.3.3 (page 16)
- Known Issues in 5.3.2 (page 21)
- Known Issues in 5.3.1 (page 27)
- Known Issues in 5.3 (page 33)
- Known Issues in 5.2 (page 45)

The following items are known issues:

Search

- Selecting files in an Index Search may cause the program to stop responding. (13031)

Database

- At times, it may take twice as long to process large amounts of data on a PostgreSQL database than in earlier versions of FTK. (13141)

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 5.3.3 Release Notes

Document Date: 5/19/2014

Introduction

This document lists the new features, fixed issues, and known issues for Forensic Toolkit® (FTK®) 5.3.3. 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 admin 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.

5.3.3 New and Improved

For information about new features in previous 5.x releases, see:

- 5.3.2 New and Improved (page 20)
- 5.3.1 New and Improved (page 25)
- 5.3 New and Improved (page 31)
- 5.2 New and Improved (page 41)

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

Administration

- You can now recover forgotton 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. You can only use the Password Reset File once. 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.

Fixed Issues in 5.3.3

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

- Fixed Issues in 5.3.2 (page 20)
- Fixed Issues in 5.3.1 (page 25)
- Fixed Issues in 5.3 (page 32)
- Fixed Issues in 5.2.1 (page 37)
- Fixed Issues in 5.2 (page 43)

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)

Known Issues in 5.3.3

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

- Known Issues in 5.3.2 (page 21)
- Known Issues in 5.3.1 (page 27)
- Known Issues in 5.3 (page 33)
- Known Issues in 5.2 (page 45)

The following items are known issues:

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)

Cerberus

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

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 5.3.2 Release Notes

Document Date: 4/17/2014

Introduction

This document lists the new features, fixed issues, and known issues for Forensic Toolkit® (FTK®) 5.3.2. 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.
- 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.
- 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.

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 admin privileges. Otherwise, you get the following error:

  Unhandled exception has occurred in your application. (9092)
- 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.

5.3.2 New and Improved

For information about new features in previous 5.x releases, see:

- 5.3.1 New and Improved (page 25)
- 5.3 New and Improved (page 31)
- 5.2 New and Improved (page 41)

Database

- PostgreSQL 9.1.13
    - PostgreSQL 9.1.13 corrects the Heartbleed security issue. You are not required to upgrade from previous versions of PostgreSQL; however, upgrading will protect you from the Heartbleed security risk.
    - This version of PostgreSQL is now provided on the installation disc.
    - For new installations, PostgreSQL 9.1.13 is the default database.
    - For information about version 9.1.13, see http://www.postgresql.org/docs/9.1/static/index.html

  Important: Important PostgreSQL upgrade instructions are in the *FTK Installation Guide*.

Fixed Issues in 5.3.2

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

- (page 32)
- Fixed Issues in 5.2.1 (page 37)
- Fixed Issues in 5.2 (page 43)

The following issues have been fixed in this release:

Bookmarks

- You can now add a manual comment to a bookmark. Previously, the Add button was inactive when adding manual comments. (8432)
- Multi-line bookmark comments now appear correctly in reports. (8432)

Copy Case

- When a *Copy Previous Case* function now fails, all subsequent Copy Previous Case functions are not affected and execute correctly. (7677)

Known Issues in 5.3.2

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

- Known Issues in 5.3 (page 33)
- Known Issues in 5.2 (page 45)

The following items are known issues:

-

Agents

- Attempting to collect volatile data from a Windows XP, 64-bit machine displays an error and fails to collect the data. (9105)

Language

- The Language Identification filter only pulls the selected language if it is listed singlely. The filter excludes multiple selected languages. (8856)
- Languages within items are not being correctly identified. (8898)

Other

- File Categories in the file category returns a count of one fewer than the File Category node count. (8497)

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 5.3.1 Release Notes

Document Date: 4/7/2014

Introduction

This document lists the new features, fixed issues, and known issues for Forensic Toolkit® (FTK®) 5.3.1. 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.
- 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.
- 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.

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 admin privileges. Otherwise, you get the following error:

  Unhandled exception has occurred in your application. (9092)
- 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.

5.3.1 New and Improved

For information about new features in previous 5.x releases, see:

- 5.3.1 New and Improved (page 25)
- 5.2 New and Improved (page 41)

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

Common Video File Format

When converting videos to a common format, MP4 is now used.

ESE Support

- You can now parse and review data from generic ESE (Extensible Storage Engine) database formats. Some applications that use ESE format include: Windows Live Mail, Desktop Search for Vista and Windows 7, Windows Help Center, and more.

Data Carving

- Added a new data carver for carving ZIP files.

Fixed Issues in 5.3.1

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

- (page 32)
- Fixed Issues in 5.2.1 (page 37)
- Fixed Issues in 5.2 (page 43)

The following issues have been fixed in this release.

Summation/Insight Integration

- With Summation/Insight installed, creating a filter in FTK no longer causes FTK to close. (7089)

Database

- On a PostgreSQL database, restarting a machine while processing an image no longer corrupts the PostgreSQL database. (4714)

Review

- The **Download** category now displays correctly in the *Chrome* node of the *Internet/Chat* tab. (7345)
- Fixed the issue where counts in 5.3 are inconsistent from counts in 5.2.1 with Internet/Chat files. Sub-categories were also missing in 5.3. (6742)

Search

- Deleting a search query from an Index Search no longer causes the application to become unresponsive. (4536)
- The Search Index no longer displays incorrect counts during a search. This issue occurred infrequently. (6313)
- Attempting to export a live search query no longer causes FTK to stop responding. (7227)

KFF

- Deleting a KFF hash from the Hash dialog now correctly removes the hash so that is does not appear in future searches. (4964)
- All available sets are now displayed in the Templates tab when no group is selected. (4973)
- Corrected color display problems in the KFF Hashes dialog. This only occurred on Windows XP machines. (4450)
- The *OK* button in the KFF Library Set dialog is not active until there are changes to save. (4454)

Bookmarks

- Reports run on an Oracle or MSSQL database with large bookmarks (containing more than 1001 items) now correctly display all of the bookmarks in the report. (5603)

Copy Case

- On Server 2012, Windows 8.1, and MSSQL, Copy Case now correctly displays the Copy Source. (6726)

Agent

- Agents are now updating correctly from 4.9 to 5.3. (6012)

Language

- The Language Selector desktop icon no longer displays the .EXE extension in the name. (7172)

Known Issues in 5.3.1

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

- Known Issues in 5.3 (page 33)
- Known Issues in 5.2 (page 45)

The following items are known issues:

Database

- The FTK_log.txt is reporting errors after installing and adding PostgreSQL 9.16 to FTK. (5377)
- When the program runs queries against the database during database optimization on a PostgreSQL, processing may stop responding. This occurs intermittently. (3444)

Reports

- Any comments added to a Bookmark will display RTF formatting codes in Reports. (7554)

Language

- Changing the language and then accessing or creating a case causes the program to stop responding.
  Workaround: Set the language to English. (7234)

Review

- Deleted files with non-Latin characters (for example, Asian, Middle-Eastern, Russian, and so forth) are not displaying correctly in the Case Overview file list. (7448)

Case Manager

- When a Copy Previous Case function fails, all subsequent Copy Previous Case functions will fail even when there is no problem with the case being copied.
  Workaround: Restart the program and run Copy Previous Case again. (7677)

Visualization

- There are two file categories named “Other Known Types” in the Heatmap option. When both are selected, one supersedes the other and the selected results only come from the one category. (3489)

Other

- Some DOC files are not decrypting correctly. (3494)
- Adding multiple columns to the Column Settings causes the File List to refresh slowly. (3548)
- There are file count and index count inconsistencies between the FTK 4.2 and FTK 5.3 versions. (6728)

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 Release Notes

Document Date: 3/20/2014

Introduction

This document lists the new features, fixed issues, and known issues for Forensic Toolkit® (FTK®) 5.3. 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:
  - We recommend that you disable the "Enable write caching on the device" setting for the hard disk that PostgreSQL is installed on. We recommend this in order to avoid the possible corruption of PostgreSQL data if the computer is not shut down properly or if the disk is defragmented during evidence processing.(3276)
  - 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.
- 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.
- 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.

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 admin privileges. Otherwise, you get the following error:

  Unhandled exception has occurred in your application. (9092)
- 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.

5.3 New and Improved

For information about new features in previous 5.x releases, see:

- 5.2 New and Improved (page 41)

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

Database

- PostgreSQL 9.1.11
    - This updated version of PostgreSQL is now provided on the installation disc.
    - If you have a previous version of PostgreSQL, you can upgrade to 9.1.11 but it is not required.
    - For new installations, PostgreSQL 9.1.11 is the default database.
    - For information about version 9.1.11, see http://www.postgresql.org/docs/9.2/static/release-9-1-11.html

    Important: Important PostgreSQL upgrade instructions are in the *FTK Installation Guide*.

Graphics Thumbnails

- Adjustable thumbnail graphic sizing

Examiner Category Changes

- Event folder will now be titled Windows EVTX Events instead of Windows Vista/7 Event Logs
- SQLite history files will now be categorized in the Internet Artifacts bucket

Common Video File Format

MP4 is now the common video file format

Review

- You can now view both the MFT and Internal Metadata time stamp information for documents being investigated in FTK.

KFF

Updated KFF Server version 1.25Cerberus

- You can now change the scoring for **Security** in the *Manage Cerberus Weighting* window. (TFS 5744)
-

Fixed Issues in 5.3

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

- Fixed Issues in 5.2.1 (page 37)
- Fixed Issues in 5.2 (page 43)

The following issues have been fixed in this release.

Search

- The indexing option to include free space is now working correctly. (6039)

Evidence Explorer

- SQLite history files are now processed correctly to *Case Overview*. Google SQLite files are located under **Internet/Chat Files** and items parsed from the file urlclassifier3.sqlite are located under **Documents > HTML**. (3297)

KFF

- The Hash Window now opens after creating a new Library Set. (4451)
- You can now sort columns within the Hash window. (5622)
- Hash names now appear correctly in the hash list. Previously, the hash's path appeared in the *Name* column and the hash's name appeared in the *Description* column. (5621)
- When editing hashes in the *KFF Hashes* window, the **OK** button is enabled when there are changes to save and disabled when no changes were made. (4541)

Geolocation

- The Volatile Geolocation button now displays the description of the feature when hovering the mouse over the button. (3447)

Visualization

- The *Social Analyzer* now correctly displays all connections to each Domain. (5135)

Examiner

- Values in the Duplicate File column now display as "Primary" or "Secondary". Previously, the Duplicate File values displayed as numeric values. (4240)

- Increased the size of the Index pane for better usability. (5671)
- The program no longer stops responding when you view hits that are still retrieving. (3986)

Other

- Adding remote data using an existing agent no longer fails to retrieve the memory scan. (5241)

Known Issues in 5.3

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

- Known Issues in 5.2 (page 45)

The following items are known issues:

Database

- On a PostgreSQL database, restarting a machine while processing an image may corrupt the PostgreSQL database. (4714)

Reports

- In PDF Reports, the *Screen Capture* section does not display page numbers. (6593)

Search

- Attempting to alter the search while an Index Search is still running generates an error. **Workaround:** Wait for the Index Search to complete before making changes to the query. (5484)
- Attempting to access search results while an Index Search is still running generates an error. **Workaround:** Wait for the Index Search to complete before clicking the results. (6496)

KFF

- Deleting a hash in a KFF library containing multiple hashes does not remove the deleted hash from the KFF Alert Files. (5648)

Review

- There is no scroll bar in the File Content pane for the default Natural View. (6588)
- When creating a Bookmark, the Email Attachments section is not active when an email with attachments is being bookmarked. (6627)

Agent

- Running a Memory Analysis or a Memory Dump does not retrieve or display the Remote Address in the *Detail List* pane. (3993)

Other

- After processing an image of a file with a Stream File within the file, that file is not recorded anywhere in the FTK results. (3452)
- The *Custodian Duplicates* field is not populating after 8 million records are processed. (543)

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 5.2.1 Release Notes

Document Date: 2/21/2014

Introduction

This document lists the new features, fixed issues, and known issues for Forensic Toolkit® (FTK®) 5.2.1. 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 5.2 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.
- 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.
- 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.

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 admin privileges. Otherwise, you get the following error:

  Unhandled exception has occurred in your application. (9092)
- 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.

Exporting Emails to PST

- 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*.

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.

Fixed Issues in 5.2.1

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

- Fixed Issues in 5.2 (page 43)

The following issues have been fixed in this release.

Decryption

- Deleted Credant files are decrypted. (4849)

Search

- In 5.2, the Merge Case Index option was removed and the processing engine did this function automatically.

KFF

- Hashes in custom KFF libraries can be deleted.

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 5.2 Release Notes

Document Date: 2/18/2014

Introduction

This document lists the new features, fixed issues, and known issues for Forensic Toolkit® (FTK®) 5.2. 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 5.2 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.
- 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.
- 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.

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 admin privileges. Otherwise, you get the following error:

  Unhandled exception has occurred in your application. (9092)
- 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.

Exporting Emails to PST

- 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*.

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.

5.2 New and Improved

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

Evidence Processing

- Added support for ZIPX file format. You can now expand ZIPX archives and process the contents.
- On the *Additional Analysis* window, the *Target Items* now display on the bottom for each tab.
- During processing, the *Pause* button is no longer available on the processing status page.

Decryption

- The processing status page for Auto Decryption now has a *Cancel* option.

Internet Artifacts

- You can process and parse mail.ru agent history files (Mra.dbs) for email and chat files.

Visualization

- There is a new Heatmap Visualization feature. This feature provides a visual representation of the files being investigated within a case. You can view a representation of the files by their type, size, or count. With Heatmap Visualization, you can:
    - Select a file category, such as Documents, Spreadsheets, Graphics, Email, Executables, Archives, and so on.
    - View by file types, folders, or extensions. You can then view by file count or file size.
    - Explore each category and view data that is grouped into sub-categories. For example, you can open the Graphics category to see sub-categories of JPEG, Tiff, Bitmap, PNG, GIF, and so on.
- You can now view volatile network data in geolocation. This lets you see where a computer is communicating to visually.

- There are three new Column Templates to help you quickly display Geolocation-based columns in the File List:
  - *Geolocation* - Displays all available Geolocation columns.
  - *GeoEXIF* - Displays all columns that contain EXIF-related Geolocation data.
  - *GeoIP* - Displays all columns that contain IP-related Geolocation data.

Examiner

- When you highlight files in the File List, there is a new right-click option to **Check/Uncheck All Highlighted** items.
- You can now view NTFS ACL attributes in the Properties pane. This gives you the same functionality that is currently found in Imager. When there are multiple sets of ACL attributes present, they are now distinguished by number.

KFF

- **Updated KFF Server version 1.24**
  - New KFF Templates

    When you enable KFF, you now select a single KFF template for the case. When you create a template, you specify the groups of hash sets that you want to use in that template. You can manually create, edit, and delete templates.
  - Lockable KFF Libraries

    You can now lock a KFF library. You may have multiple applications that share the KFF Server and libraries. When you lock a library, another application cannot delete it, edit it, or modify the sets or hashes that are part of it. This is useful when using a product like Summation or InSight along with FTK. If you create a library in FTK and lock it, a user in InSight cannot delete or edit it.
  - Manually create and edit libraries

    You can manually view, add, edit, and delete libraries.
  - Manually create and edit hash sets

    You can manually view, add, edit, and delete hash values within a hash set.
  - KFF Hash Finder

    You can use the KFF Hash Finder to search for individual hash values within a hash set.
  - Expanded CSV Hash Import

    You can use an expanded CSV format to import hashes into more than one set at a time using a single CSV file. For example, you can add some hashes to one hash set with an Alert status, and add different hashes to another set with an Ignore status.
  - New KFF Import Log

    When you perform an import of hashes, a log file is created and records the hashes that were updated or if any errors occurred during the import.

Other

- The Merge Case Index option has been removed. The processing engine does this automatically.

Cerberus Add-on

Cerberus is an integrated add-on module for malware analysis that allows you to detect and triage suspect binaries. Cerberus requires an additional license. For more information, see http://accessdata.com/.

- Weighted Cerberus Scores - When you enable Cerberus Analysis, you can define the weight assigned to each Cerberus stage 1 score. These Stage 1 scores are designed to identify and score specific malware properties and traits. The user-defined weights can be saved per case as well as globally in the Evidence Processing templates.

Fixed Issues in 5.2

The following issues have been fixed in this release.

Installation and Upgrade

- The BlackIce temporary files that are installed as part of the Processing Engine are installed in the same folder as the temporary Processing Engine files. (31494)

Internet Artifacts

- In the *Properties* view of a Chrome internet artifact, the *Last Visited* and *This Visit* date attributes are displayed. (23628)
- The *URL has HTML* Internet History column now populates data. (33368)
- When viewing Gmail Offline Messages from the *Internet/Chat* tab, the counts are correct. (22810)

Processing

- When selecting *Registry Reports* in *Additional Analysis*, the *File Signature Analysis* option is now automatically selected so that the reports are created properly. (27001)
- When configuring the *Indexing Options* within *Processing Options*, if you use accented letters, you no longer get an error. (25944)
- OCR for PNG, BMP, and TIFF file types work properly in Additional Analysis. (32331)

Decryption

- Images with PGP encryption are recognized and processed correctly. (36155)
- Passwords are not removed from the Perform Automatic Decryption password list during processing. (31469)
- All Credant decryption is performed through the Processing Engine. The resolves any inconsistency with using *Tools* > *Credant Decryption*. (4489)

Reports

- In HTML reports, bookmarks which have special characters in their names now display correctly. (32291)

Labels

- Labels colors are now consistent when viewing them across all products. (3982)

Bookmarks

- When creating a report with a bookmark that has the '&' character in the name, the application will now complete the report. (28856)

KFF

- Changes made in KFF are now displayed properly after clicking Apply. (31400)

Examiner

- Prefetch files are now displayed properly in the File Content pane. (29590)
- The count of *Unknown Types* is correct after selecting *Expand Compound Files* in *Additional Analysis*. (31408)
- Unicode characters in the filename of 7-Zip files are now displayed correctly in the file list. (35269)

Volume Shadow Copy

- If "Full" restore option is selected, you are warned if more than one restore point is checked. You can add the evidence item again if you don't choose to add it as a restore point image originally. You can then choose restore points. (35734)

Agent

- Fixed the issue that 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). (27694)

Search

- If you press the Delete key while in the Search Results pane, you no longer get an error. (31847)
- Fixed the issue that when running an index search sometimes caused the application to close. (3963)

Imaging

- Imager can properly mount .dd images in Windows 8. (29712)

Photo DNA

- Adding more than 5,000 images to a Photo DNA Library no longer causes the application to hang. (30264)

Other

- Fixed the issue that when exporting emails to a PST and using the 'Preserve file structure' option selected, some emails may not display in Outlook. (19086)
- The correct MFT Record date for NTFS images is displayed in the properties tab. (30490)

Cerberus Add-on

- Cerberus now takes advantage of the Yara functionality (35363).

Known Issues in 5.2

The following items are known issues:

Administration

- If you only have one Admin account, and you change that user's role to something else, like a case reviewer, there is no way to access the application as an Admin without re-installing the application and the database. Make sure there is another Admin account before deleting or changing an Admin's account. (3486)

Case Management

- If you are logged in as a Case Administrator with the same user name as was used in a previous version, and attempt to use Copy Previous Case, the case will not copy. (4014)

Decryption

- Some documents are not being decrypted when the correct password is added in the Decrypt Files dialog. (3450)
- Quickbooks 2009 files may not be identified correctly for file decryption. (4328)
- After decrypting a Credant image, the Machine ID field is blank. (4319)
- Files in Safeboot images may not get decrypted. (4296)
- Some files may not be recognized as being encrypted (displayed in red) and cannot be decrypted using auto decryption. (4277)

Processing

- The Last Modified and Creation dates for a PDF may be different than those of the original source file, such as a Word file. (4542)
- Running Additional Analysis multiple times may cause the application to become unresponsive and create "Channel Faulted" errors in the ProcessingHost_error.log. (4394)

Internet Artifacts

- Internet Explorer cookies may not be parsed our correctly during processing. (3475)
- Clicking on a parsed Download item generates an "Unable to open the evidence" error. (4276)

Search

- When viewing the results of an index search and highlighting multiple hits, the focus of the source item in the File List is lost. (3470)
- Deleting a search query from an Index Search may cause the application to become unresponsive. (4536)
- The automatic index merge may not function properly. (4335)
- Setting a pre-filter in index search and trying to export or copy the file to the clipboard may not work. (4327)
- Index search file node shows more hits than what is listed underneath the node. (4303)

Summation/Insight Integration

- If you create a case in FTK and create labels, then open the case in InSight or Summation, you cannot see the labels. (4337)

Visualization

- Several Geolocation columns are not populated, including: Area Code. Metro Code, Postal Code, and Direction. (4306, 3490)
- When using Heatmap, if you drill down on an AD1 file, the view will go blank. (4321)

KFF

- If you have a previous version of the KFF Server, 1.2.2 or older, and click Manage > KFF, the application may close. Be sure to install the latest version of KFF Server (1.2.4). (4635)
- Some CSV files do not import properly. (3461)

Cerberus

- If you process data with Cerberus enabled, and then run Additional Analysis and change Cerberus scores, files that already have scores are not analyzed again. (4120)

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*.