AccessData Forensic Toolkit 4.1
Release Notes

Document Date: October 16, 2012

Introduction

This document includes information about the AccessData® Forensic Toolkit® (FTK®) 4.1 release. Please be aware that all known issues that have been published under previous release notes, still apply until they are listed under a "Fixed Issues" section.

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

See the following:

- AccessData Forensic Toolkit 4.0.2 Release Notes (page 9)
- AccessData Forensic Toolkit 4.0.1 Release Notes (page 14)
- AccessData Forensic Toolkit 4.0 Release Notes (page 19)

For information about additional previous releases, see the AccessData web site at http://accessdata.com/.

Important Information

The following are important considerations to be aware of:

Installation and upgrade:

- FTK does not support skipping versions when you upgrade cases. You must upgrade in the order of the released versions. For example, you cannot upgrade cases from FTK 3.1 to FTK 4.0. In this example, you would need to upgrade first from FTK 3.1 > FTK 3.2 > FTK 3.3 > FTK 3.4 > FTK 4.0. (63494) (57461)
- Whenever possible, install the database software to a physical system. AccessData does not recommend configurations where the database or the Evidence Processing Engine is running on a virtual machine.
- The Exporting Emails to PST feature requires that you have Microsoft Outlook and the Microsoft Collaboration Data Objects (CDO) installed on the same computer as the processing engine. The Processing Engine installer will attempt to download and install CDO automatically. However, if the computer does not have an internet connection, you will need to install CDO manually.

  See http://www.microsoft.com/en-us/download/details.aspx?id=3671

Data and Database Management

- AccessData recommends that, whenever possible, users 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 or web pages, 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 to configure antivirus to exclude the database (PostgreSQL, Oracle database, MS 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 antivirus deletes/Quarantines the binary from the temp Cerberus analysis will not be performed.
- When using an Oracle database, it must be installed on a computer with a name that begins with a letter (a-z and A-Z). Due to a restriction on domain names in RFC 1035, applications cannot connect to Oracle if the computer’s name begins with a number. If the Oracle computer has a name that begins with a number, you must change the machine name before you install Oracle.
- You can download the Oracle Critical Patch Update for this release from the AccessData Support Downloads web site. First back up the database, and then close all programs before you install the patch. (58583, 58248)
- If you choose to have a case’s database files placed in the case folder, do not move your case folder without first archiving and detaching the case. (64450)
- If you bookmark a manually carved item that has not been processed, the file does not display in a bookmark or in a report until you process it. You can use the “Process Manually Carved Items” option in the *Evidence* drop-down menu, to processes the manually carved item. (57812)

4.1 New, Improved, and Enhanced Features

The following items are new and improved features, or feature enhancements for the 4.1 release.

For enhancements in the previous 4.x releases, see the following:

- 4.0.2 New, Improved, and Enhanced Features (page 10)
- 4.0.1 New, Improved, and Enhanced Features (page 15)
- 4.0 New, Improved, and Enhanced Features (page 20)

Media Analysis Enhancements

- New Video Tab

  You can generate thumbnails from video files and display them in the *Video Thumbnail* pane. This functionality lets you quickly examine a portion of the contents within video files without having to watch the full content of each media file.

  You can define the thumbnail generation interval based on one of the following:

    - Percent (1 thumbnail every “n”% of the video)
    - Interval (1 thumbnail every “nonskeds)
- Generate Common Video File

  You can convert all supported video types into a format that Windows Media Player supports. All converted videos are stored in the case folder and when a user selects a video, it is playable within FTK.

  You can define the lines of resolution and the bit rate.

Exporting Enhancements

- Improved handling of Outlook 2010 email drafts when exporting. (67505)
- Exporting Emails to PST

  You can export email messages to a PST file, even if they didn't come from a PST file originally. This lets you accomplish the following:

  - Export messages from RFC822, NSF, PST, Exchange, and so on to a PST.
  - As the opposite of reduction, you can create a new PST file with responsive messages in it. This creates a new PST rather than exporting the whole source PST and running reduction to remove anything non-responsive.
  - Convert email archives, such as NSF, to a PST with the same folder and message structure.

  Note: This export feature requires that you have Microsoft Outlook and the Microsoft Collaboration Data Objects (CDO) installed on the same computer as the processing engine. The Processing Engine installer will attempt to download and install CDO automatically. However, if the computer does not have an internet connection, you will need to install CDO manually.

  See http://www.microsoft.com/en-us/download/details.aspx?id=3671

- Header info has been added to the export manifest file. (69056)

Processing Enhancements

- The handling of NSF Emails with compressed email bodies has been improved. (66674)
- The following new carvers have been added. These new carvers are not enabled by default:

AIM Chat Logs	Firefox Form History	Windows Messenger Plus w/ chat logging
Facebook Status Updates	Firefox Places	MSN/WLM Chat
Facebook Chat	Firefox Session Store	Yahoo Diagnostic
Facebook Email Artifact	Frostwire Props Files	Yahoo Webmail Chat
Facebook Mail Snippets	GigaTribe Chat	Yahoo Mail
Facebook Fragment	IE8 Recovery URL	Yahoo Group Chat Recvd
Gmail Email Message	Limewire Props	Yahoo Group Chat Sent
Gmail Parsed Email	Limewire/Frostwire Keyword Search	Yahoo Chat
Google Talk Chats	mIRC Chat Log	Yahoo Chat UnAllocated
Hotmail Email Artifact	MySpace Chat	Yahoo Unencrypted Active
Bebo Chat	Twitter Status	

File Content Viewing Enhancements

- You can now easily view data about Windows prefetch (.pf) files.

  When you select a prefetch file in the file list, the following application data is displayed in HTML format in the *Natural* tab of the *File Content* pane:

  - The file path of the application executable file
  - The number of times the application has been run
  - The last time the application was run

Support for Windows EVTX log files

- You can now view data that is contained in Microsoft EVTX log files in HTML format in the *Natural* tab of the *File Contents Pane*. (T6636)
- There is a new option in Expand Compound Files for EVTX. When EVTX is selected, it will create a separate object for each event. This allows a user to view EVTX events interspersed with file data.
- You can also use the following new EVTX-related columns in the *File List*:
  - EVTX Event Channel
  - EVTX Event Computer
  - EVTX Event Data
  - EVTX Event ID
  - EVTX Event Level
  - EVTX Event Source
  - EVTX Event Source Name
  - EVTX Event User ID

Decryption Enhancements

- **Decrypting Microsoft Office and Outlook Digital Rights Management (DRM) Protected Files**

  If your organization uses Windows Rights Management (RMS) to protect your Microsoft Office files and Outlook email files, you can use the Examiner to decrypt them. If you are investigating Microsoft Office files and Outlook email files from within your organization, this saves you time by decrypting and indexing DRM protected files in batch. By using this feature you no longer have to first export each document and then decrypt them individually with the RMS server.

  Important: This feature only applies to files that are DRM protected from within your Domain. You cannot use this feature to decrypt files that are protected by other organization's RMS systems.

  To decrypt DRM protected files, the following prerequisites must exist:
  - Your Examiner computer and the Microsoft RMS server must be in the same domain.
  - The Examiner computer must be able to authenticate with the RMS server. The machine activation happens when you first attempt to open or to protect a document for the first time.
  - You must be logged into the Examiner computer with a Domain account that has Super User access to the Microsoft RMS server.
  - You must have Microsoft Office installed on the Examiner computer. To decrypt DRM protected PST files, Outlook must be installed on the Examiner computer. It must be configured to work with your organization's Microsoft Exchange Server system.
  - When you attempt to decrypt, the system will prompt with a Security Alert, select View Certificate and then click Install Certificate.
- You can now configure Credant server settings in two separate ways:
  - Globally, for all cases, in the *Case Manager* interface under the *Tools* menu.
  - For a specific case on the *Additional Analysis* page.

    From the *Additional Analysis* page, you can select to decrypt Credant files. If you select to decrypt Credant files, the *File Signature Analysis* option will automatically be selected as well. (68848, 69165)
- You can now do a Live Search on Credant files on the fly after performing a drive preview. (70081)

Database Optimization for Large Cases

- If you are using PostrgreSQL, you can now select an option to optimize your database for large cases. (68733)

Installation and Upgrade Enhancements

- You can now migrate users, shared roles, filters, columns, and so on from the previous version when the database is initialized. (68535)

Other Enhancements

- RSR (Registry) reports that were available on the website to add to FTK have now been incorporated into the product. (67649)

Add on Module Enhancements

- This release includes enhancements to the FTK Cerberus and Visualization add-on modules.

  For information, see 4.1 Release Notes for Add-on Modules (page 6).

4.1 Fixed Issues

The following items are resolved issues in the 4.1 release.

For resolved issues in the previous 4.x, releases, see the following:

- 4.0.2 Fixed Issues (page 11)
- 4.0.1 Fixed Issues (page 16)
- 4.0 Fixed Issues (page 21)

Processing Fixes

- The handling of NSF Emails with compressed email bodies has been improved. (66674)
- Fixed an issue that if processing was done with both 'KFF' and 'Optical Character Recognition' selected, two OCR files were generated for each file that had OCR done in it. (67248)
- Fixed an issue where, in certain cases, FTK took a long time to render SQLite database files. (68246)

Miscellaneous Fixes

- Fixed an issue where, in certain cases, FTK was showing address book GUIDs instead of email addresses in the “To” and “From” fields. (68228)
- Fixed an issue in the HTML file listing where Local and UTC times were backwards. (63082)
- The Auto Commit default value is now displayed in the case indexing options instead of 0. (58701)
- The visible area in the Social Analyzer when the radius is zoomed in has been improved. (66495)
- Fixed an issue where when using certain reporting options, case reviewers were able to export certain items that had been marked as privileged. (68202)
- Added support for index search hit highlighting for PDF files in the natural view. Previously, only the filtered text view supported index search hit highlighting for PDF files. (68336)
- PDF files are now identified through the PDF file system and will no longer be identified through *Custom File Identification*. (67866)
- Fixed an issue where certain IMG files were causing a crash. (69663)
- Fixed an issue where some SHA1 hashes were being truncated in the Export Manifest file. (69155)
- Fixed filter issue in UI when using file hashes (MD5, SHA1, etc.). (69273)

- Improved handling of EML files. (69910)
- Fixed an issue with duplicate email counts. (70078)
- Fixed an issue when importing user defined KFF groups. (70086)

4.1 Known Issues

The following items are known issues found in the 4.1 release.

For known issues found in previous 4.x releases, see the following:

- 4.0.2 Known Issues (page 12)
- 4.0.1 Known Issues (page 17)
- 4.0 Known Issues (page 23)

Installation

- The KFF installation on PostgreSQL can take quite a bit of time to complete. (68237)
- The KFF install will not work on Postgres if the dbname has been changed from FTK2. (70629)

Graphics and Video

- The Video tab has a tab filter set to only show media that has had a thumbnail or video file rendered from it during processing. If the video options were not selected for processing, the video tab will be blank. (67871)
- SWF video files are not supported. (67958)

Other Known Issues:

- When viewing files after performing a dtSearch, when you click through the search results, you may not see the results in the expected order. If the file contains headers and footers, such as PDF files, the results from the main body of the text in the page will be shown in order. It will then show any results in the header and then footer on that page. It will then proceed to the body of the next page, followed by the header and footer, and so on. (68556)
- When exporting from 7-Zip files, some EXE files may become corrupted. (70071)
- In the FTK product shortcut, the Target field includes the following parameter:

  -product=*productname*

  with a product name, such as, FTK, Lab, and so on. If this parameter is not set, AccessData Enterprise will open by default.

4.1 Release Notes for Add-on Modules

4.1 Release Notes for the Cerberus Add-on

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

For Cerberus Release notes from previous 4.x releases, see the following:

- 4.0.2 Release Notes for the Cerberus Add-on (page 12)
- 4.0.1 Release Notes for the Cerberus Add-on (page 17)
- 4.0 Release Notes for the Cerberus Add-on (page 23)

Please note the following enhancements:

Cerberus Add-on Enhancement

- Stage 1 Cerbrus Analylsis now includes the following additional information:
  - Entropy Score: Displays a score of the binaries entropy used for suspected packing or encrypting
  - Modules Section: Displays the DLLs loaded with the binary
  - Packer & Encryptor Identification: Attempts to display a list of identified packers and encryptors whose signagture matches known malware packages.
- Integrated Unpacker for certain family of packers. Cerbrus Analylsis attempts to unpack the binary and analyze the contents and displays the results of unpacking efforts.

4.1 Release Notes for the Visualization Add-on

There is an add-on module called Visualization. The visualization module lets you view data in multiple display formats, including time lines, cluster graphs, pie charts and more. This functionality lets you quickly determine relationships in the data and find key pieces of information. Visualization requires an additional license. For more information, see http://accessdata.com/.

For Visualization Release Notes for the previous 4.x releases, see the following:

- 4.0.2 Release Notes for the Visualization Add-on (page 13)
- 4.0.1 Release Notes for the Visualization Add-on (page 18)
- 4.0 Release Notes for the Visualization Add-on (page 23)

Please note the following enhancements:

- New Detailed View in Visualization

  You can use the *Detailed* view of the visualization time line to get a more granular view of the files and emails in your data set. This helps you use the time line to identify the files and emails that are important in your investigation. The detailed view provides the following time bands that you can turn on or off to get a more or less granular view of the files:
  - Years
  - Months
  - Days
  - Hours
  - Minutes
  - Seconds
  - Milliseconds

  Different file types are represented by different colors to assist in identifying relevant files.
- **Select All** and **Select None** options have been added to the Basic Time line View in Email Visualization. (68170)
- The Visualization demo time remaining information has been removed from the message box that appeared when logging in and is now displayed in the **Help >About** dialog. (67738)

- Fixed an issue that caused the warning Info box to continue showing after clicking “No” to not continue with Visualization. (66792)
- Fixed an issue on the extensions bar where the selection was cleared after moving the scroll bar in the Extensions Distribution pane. (66843)
- Fixed an issue that when making a selection from the File Extensions Distribution pane, it did not refresh the Categories Distribution Chart pane. (66893)
- Fixed an issue where legend names were not sorted alphabetically in the File Visualization window. (68304)
- Fixed an issue in visualization where 0 length files were sometimes showing a size of -1 bytes. (68992)

Please note the following issues:

- When viewing the visualization *Categories Distribution Chart*, the percentages are rounded to the nearest one-hundredth percent. If a certain category has a percentage lower that one-hundredth of a percent, such as 0.008 %, it will display as 0%, even though there are a limited number of actual files. (68508)
- When viewing the detailed time line, and files are grouped by *Selected Time*, if you click a group, the total *File Count* for that group is displayed in the flag and next to the file list. If the files are grouped by *Fixed Number*, the File Count number is not shown next to the file list. (68530)

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 4.0.2 Release Notes

Document Date: June 13, 2012

Introduction

This document includes information about the AccessData® Forensic Toolkit® (FTK®) 4.0.2 release. Please be aware that all known issues that have been published under previous release notes, still apply until they are listed under a “Fixed Issues” section.

For your convenience, both the version 4.0.1 and the version 4.0 release notes are included at the end of this document. See the following:

- AccessData Forensic Toolkit 4.0.1 Release Notes (page 14)
- AccessData Forensic Toolkit 4.0 Release Notes (page 19)

For information about additional previous releases, see the AccessData web site at http://accessdata.com/.

Important Information

The following are important considerations to be aware of:

- You can download the Oracle Critical Patch Update for this release from the AccessData Support Downloads web site. First back up the database, and then close all programs before you install the patch. (58583, 58248)
- AccessData recommends that, whenever possible, users 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 or web pages, 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.
- 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 has a name that begins with a number, you must change the machine name before you install Oracle.
- Whenever possible, install the database software to a physical system. AccessData does not recommend configurations where the database or the Evidence Processing Engine is running on a virtual machine.
- If you choose to have a case’s database files placed in the case folder, do not move your case folder without first archiving and detaching the case. (64450)

- FTK does not support skipping versions when you upgrade cases. You must upgrade in the order of the released versions. For example, you cannot upgrade cases from FTK 3.1 to FTK 4.0. In this example, you would need to upgrade first from FTK 3.1 > FTK 3.2 > FTK 3.3 > FTK 3.4 > FTK 4.0. (63494) (57461)
- If you bookmark a manually carved item that has not been processed, the file does not display in a bookmark or in a report until you process it. You can use the "Process Manually Carved Items" option in the *Evidence* drop-down menu, to processes the manually carved item. (57812)

4.0.2 New, Improved, and Enhanced Features

The following items are new and improved features, or feature enhancements for the 4.0.2 release.

For enhancements in the previous 4.0.1 or 4.0 releases, see the following:

- 4.0.1 New, Improved, and Enhanced Features (page 15)
- 4.0 New, Improved, and Enhanced Features (page 20)

File System Enhancements

- FTK now supports the EX01 Evidence Format. (66024) (66389)
- This release improves the handling of unallocated space for Android EXT4 partitions. (65613)
- This release improves the handling of unallocated space in YAFFS partitions. (65601)

Processing Enhancements

- When you choose to index or expand in *Additional Analysis*, file slack and drive free space is included by default. (63473)
- A new option has been added to not process embedded graphics from email items. The default behavior has not changed. The option only applies if you select it in the processing options. (65912)
- You can now run an *Entropy Test* on files without performing indexing.

Backup Enhancements

- You can now select multiple cases in the *Case List* pane and back up/detach them at the same time. (66503) (66503)

Bookmarking Enhancements

- The user interface now lets you bookmark more than 9,999 items at a time. (65840)

Decryption Enhancements

- This release adds new decryption support for YAFFS 1 and YAFFS 2.
- This release adds new decryption support for IOS.
- Transparently decrypted files have the *Decrypted* flag set instead of the *Encrypted* flag. You can search for these files by sorting or filtering on the *Decrypted* column. If you need to view the original encrypted data, right-click on the file and select *Find on Disk*. (65314)

Filtering Enhancements

- This release improves the user interface’s tab order in the *Filter Definition* dialog. (65805)

Optical Character Recognition (OCR) Enhancements

- FTK now has support for a new OCR engine. Existing Glyph Reader customers will be switched to the new OCR engine.

Registry File Enhancements

- You can now send registry files to Registry Viewer from FTK even if the files have not yet been identified.

Searching Enhancements

- When you do a *Live Search* with a filter selected, the *Search Results* tree now shows the type of filter option that you used for that particular search. (65961)

Known File Filter Enhancements

- For user-defined KFF sets, the *Source Vender* column is now populated. (57244)

Add on Module Enhancements

- This release includes enhancements to the FTK Cerberus and Visualization add-on modules.

  For information, see 4.0.2 Release Notes for Add-on Modules (page 12).

4.0.2 Fixed Issues

The following items are resolved issues in the 4.0.2 release.

For resolved issues in the previous 4.0.1 or 4.0, releases see the following:

- 4.0.1 Fixed Issues (page 16)
- 4.0 Fixed Issues (page 21)

Installation and Configuration Fixes

- Fixed an issue where when a user installed the product to a Unicode folder, the indexing options in the *New Case Wizard* were not populated. (65582)

Backup and Restore Fixes

- Fixed an issue where if the case folder path contained the ampersand "&" character, and if the case was detached and then attached again, the attachment failed. (65385)

Decryption Fixes

- Fixed an issue where FTK was showing "*Document is encrypted*" for certain protected XLS files instead of the contents of the file. (65839)

Exporting Fixes

- This release fixes an issue where you could not open evidence from an *Export to Image* file action. (66122)

- This release fixes an issue where, in certain instances, blank fields in the *File List* pane were filled in with duplicate data when they were exported to a CSV file. (66129)

Filtering Fixes

- Fixed an issue where some filters displayed the operator "*attribute does not exis*t" 3 times in the operators list. (65237)

Miscellaneous Fixes

- Fixed an issue where when you un-docked the *File Content* pane, it remained open in the other tabs. (57321) (65248)
- Fixed an issue where the product was sometimes not able to connect to the database. (65906)
- This release fixes an issue with the vertical scroll bar of the *Properties* window. It was previously covering the data in the view. (57582)
- This release fixes an issue where the column sort indicator arrow, did not update properly in the *File List* pane. (65997)
- Improved the handling of MSG items that are attached to emails, when exporting to MSG. (66216)

4.0.2 Known Issues

The following items are known issues found in the 4.0.2 release.

For known issues found in the 4.0.1 or 4.0 releases, see the following:

- 4.0.1 Known Issues (page 17)
- 4.0 Known Issues (page 23)

Known Issues:

- Viewing search hits in large files is a very resource intensive action. It can slow down the product's performance. (65382)
- Distributed Processing, with PostgreSQL as the database, does not work with multiple network interface cards that are teamed together or that are using Link Aggregation Control Protocol (LACP). It does work with a single network interface card. (64286)
- Certain PDF files, that are processed as evidence from a network location, can cause processing to slow down.

4.0.2 Release Notes for Add-on Modules

4.0.2 Release Notes for the Cerberus Add-on

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

For Cerberus Release notes from the previous 4.0.1 and 4.0 releases, see the following:

- 4.0.1 Release Notes for the Cerberus Add-on (page 17)

- 4.0 Release Notes for the Cerberus Add-on (page 23)

Please note the following:

- Cerberus stage 1 analysis has been enhanced to include several additional details. The report now includes details about a file's size, the examined functions, any potentially threatening functions, detailed versioning information, and detailed signature information.

4.0.2 Release Notes for the Visualization Add-on

FTK supports an add-on module called Visualization. The visualization module lets you view data in multiple display formats, including time lines, cluster graphs, pie charts and more. This functionality lets you quickly determine relationships in the data and find key pieces of information. Visualization requires an additional license. For more information, see http://accessdata.com/.

For Visualization Release Notes for the previous 4.0.1 and 4.0 releases see the following:

- 4.0.2 Release Notes for the Visualization Add-on (page 13)
- 4.0 Release Notes for the Visualization Add-on (page 23)

Please note the following Enhancements:

- Beginning with this version, the product now includes a free 30-day evaluation license for the Visualization add-on Module. This functionality will be in effect until the promotion expires.
- You can now select objects to *Label*, *Create Bookmarks*, *Clear a checked item*, or *add it to other checked items*, directly from the Visualization window.
- This release improves the performance in Visualization when you change the time-span from the *Created Date* to the *Modified Date*. (65809)
- The communication volume graph in the *Social Analyzer* tool has been enhanced to more accurately represent the volume of communication. (65816)

Please note the following issues:

- The time line's current date selection does not match the *Current Selection* information that is displayed on the time line's status bar. An additional day is added to the time line status bar. (66296)

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 4.0.1 Release Notes

Introduction

This document includes information about the AccessData® Forensic Toolkit® (FTK®) 4.0.1 release. Please be aware that all known issues that have been published under previous release notes, still apply until they are listed under a “Fixed Issues” section.

For your convenience, the version 4.0 Release Notes are included at the end of this document.

See AccessData Forensic Toolkit 4.0 Release Notes (page 19)

For information about previous releases, see the AccessData web site at http://accessdata.com/.

Important Information

The following are important considerations to be aware of:

- You can download the Oracle Critical Patch Update for this release from the AccessData Support Downloads web site. First back up the database, and then close all programs before you install the patch. (58583, 58248)
- AccessData recommends that, whenever possible, users not have an active internet connection when they run Imager or FTK. If the computer running Imager or FTK has an active internet connection and you are viewing certain types of HTML or Web pages, 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.
- 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 has a name that begins with a number, you must change the machine name before you install Oracle.
- Whenever possible, install the database software to a physical system drive. AccessData does not support configurations where the database or the Evidence Processing Engine is running on a virtual machine. Additionally, installing the CodeMeter software on a virtual machine is not recommended. (56262)
- If you choose to have a case’s database files placed in the case folder, do not move your case folder without first archiving and detaching the case. (64450)
- FTK does not support skipping versions when you upgrade cases. You must upgrade in the order of the released versions. For example, you cannot upgrade cases from FTK 3.1 to FTK 4.0. In this example, you would need to upgrade first from FTK 3.1 > FTK 3.2 > FTK 3.3 > FTK 3.4 > FTK 4.0. (63494) (57461)
- If you bookmark a manually carved item that has not been processed, the file does not display in a bookmark or in a report until you process it. You can use the "Process Manually Carved Items" option in the *Evidence* drop-down menu, to proceses the manually carved item. (57812)

4.0.1 New, Improved, and Enhanced Features

The following items are new and improved features, or feature enhancements for the 4.0.1 release.

For enhancements in the 4.0 release, See 4.0 New, Improved, and Enhanced Features on page 20.

Processing Enhancements

- You can now obtain metadata from PDFs, including “Title”, “Author”, “Subject”, “Keywords”, “Creator”, “Producer”, “Creation Date”, and “Modification Date”. This feature also lets you extract attachments (but not embedded graphics) from PDFs. To extract the attachments, you can choose to expand PDFs as compound files. PDF Attachments are the files in Adobe Reader’s bottom window that open with Adobe’s paperclip feature.
- There are new processing options for additional registry data that is gathered from a memory analysis. (64873)
- There is a new index processing option called *Do Not include document metadata in filtered text*. This option lets you prevent the collection of internal metadata properties for indexed filtered text. The fields for these metadata properties are still populated for field-level review. However, if selected you do not see information such as “Author”, “Title”, “Keywords”, “Comments”, etc in the *Filtered* text pane of the *Examiner*. The exclude office metadata option only excludes it from filtered text and not from attributes. If you export using another utility, such as ECA or eDiscovery, and include the filtered text of the file with the export, the metadata is filtered from the exported file. (64514) (65560)
- The identification and processing of PDF files is improved. (65101)
- The processing speed for the Optical Character Recognition (OCR) feature is improved. (64237)
- The processing speed is improved when you use KFF processing options and a PostgreSQL database. (62400)
- The reporting of processing times for the log file and the progress window is improved. (64522)

Bookmarking Enhancements

- When you bookmark an index.dat entry, the *Create Bookmark* dialog provides an option to include the entry’s parent index.dat file in the bookmark. (58750)

Exporting Enhancements

- The exporting of metadata from NSF emails into MSG format is improved. (64515)
- When you export a manifest file, the file name of the manifest file is renamed from FTKExportSUmmary&Errors.TXT to FTKExportSummary.TXT (60733)

Searching Enhancements

- Live Search’s text information has been updated to be more clear about the options that you have selected. (61526)

Miscellaneous Enhancements

- The option to *Manage KFF* is located under the *Database* menu in the *Case Manager,* as well as from the *Examiner*. (57441)
- Improved support for finding hidden processes, when the option is selected in the "Add Remote Data" feature. (65264)

Add on Module Enhancements

- This release includes several enhancements to the FTK Cerberus and Visualization add-on modules For information, see 4.0.1 Release Notes for Add-on Modules (page 17).

4.0.1 Fixed Issues

The following items are resolved issues in the 4.0.1 release.

For resolved issues in the 4.0 release, See 4.0 Fixed Issues on page 21.

Installation and Configuration Fixes

- When you create a trusted user, the Application Administrator’s account is validated if you select *Trusted User.* (64335)
- This release fixes an issue in the *Copy Previous Case* dialog where the user assignment window was blank if you used a PostgreSQL database. (64524)
- This release fixes an issue where FTK 3.4.1 could not open cases after you selected a time zone for processing in FTK 4.0. (64559)

Searching Fixes

- This release fixes an issue where certain custom file carvers were causing *Other known Types*, in the *dtSearch* window to not expand. (64822)
- This release fixes a hang in the *Index Search* tab that occurred when searching through custom carved MPEG files. (57740)

Exporting Fixes

- This release fixes an issue with exporting HTML views for carved files. (58520)

Email Fixes

- This release fixes an issue where FTK was rendering some emails with white text on a white background. This previously made text not viewable in the window. (63384)

Reporting Fixes

- This release fixes an issue in user-generated reports where non-English characters were displayed instead of the words "Time Zone for display." (65009)

Miscellaneous Fixes

- This release fixes an issue that occurred when you viewed drivers in the *Detailed Information* pane. The pane did not update when switching between the entries in the list unless the selected item contained data. (64207)
- This release fixes an issue with a crash that sometimes happened when you moved the *File List* pane and then quickly closed the *Examiner.* (62976)
- The *write cache* field in the *Drive Mounting* dialog has been fixed to automatically populate with a valid path. (64821)

4.0.1 Known Issues

The following items are known issues found in the 4.0.1 release.

For known issues found in the 4.0 release, see 4.0 Known Issues (page 23)

Known Issues:

- When exporting an email message that has an embedded message, the exported embedded message may have blank header information (To, From, CC, BBB, Subject). To work around this isssue, export the embedded message separate from the embedded email. (65744)
- Image mounting does not work in FTK or Imager if the agent is installed on that machine. (58791)
- Distributed Processing, with PostgreSQL as the database, does not work with multiple network interface cards that are teamed together or that are using Link Aggregation Control Protocol (LACP). It does work with a single network interface card. (64286)
- The *SafeGuard Enterprise decryption* dialog displays an error message when you click the *Cancel* button. (19975)
- The “Key” icon that is displayed next to files for the category *Other Encryption Files* in the *File List* pane is distorted. (18628)
- Certain antivirus programs have been known to flag jam.dll as malware. This is a false positive and can be ignored.

4.0.1 Release Notes for Add-on Modules

4.0.1 Release Notes for the Cerberus Add-on

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

See also 4.0 Release Notes for the Cerberus Add-on (page 23)

Please note the following:

- The HTML results of a Cerberus Malware analysis can now be indexed so that you can run a search for them.
- Cerberus malware triage includes a new filter called *Cerberus Static Analysis*. This filter limits the display of files in the *File List Pane* to only the files that have had Cerberus Stage 2 run against them.
- Cerberus malware triage includes a new column called *Cerberus Static Analysis*. This column displays the letter “*Y*” next to files that have had Cerberus Stage 2 analysis run on them.

Filtering Enhancements

- FiltersA new default filter called *Cerberus Static Analysis* is added. This filter lets you see the files that have had Cerberus Stage 2 Analysis run against them. (63176)

4.0.1 Release Notes for the Visualization Add-on

FTK supports an add-on module called Visualization. The visualization module lets you view data in multiple display formats, including time lines, cluster graphs, pie charts and more. This functionality lets you quickly determine relationships in the data and find key pieces of information. Visualization does require an additional license. For more information, see http://accessdata.com/.

See also 4.0 Release Notes for the Visualization Add-on (page 23)

Please note the following:

- The visualization module is not available on new tabs that are created by users. It is only available from the *Explore*, *Overview,* and *Email* tabs. (62810) (64420)
- Email visualization includes history items called breadcrumbs. If you select a breadcrumb in the email visualization time line, the time line is reset to the view that was displayed when the breadcrumb was created. (64547)
- Visualization has been updated to let you modify the appearance of the Visualization windows. You can choose from nine different color schemes.
- Visualization now supports showing FAT last accessed times. (64243)
- A new extension column has been added to the file data list in visualization. This column lets you sort items by extension. (64439)
- You can now minimize and maximize the windows in Visualization. (64160)
- Visualization now launches separate from the Examiner window, and each window shows up separately in the task bar. (64162)
- Visualization has been updated so that if a file’s “Created date”, “Modified date”, or “Last Accessed date” is prior to the year 1985, then visualization displays a dialog box. The dialog box asks you if you want to include the files with these dates in the visualization display. If you select the option, *Do not ask me again*, Visualization remembers your preference the next time the dates precede 1985.
- In Visualization, you can now view the file extension graph in linear or log mode. This provides easier selection of items in the interface. (64448)
- You can now type in the filter dialog box in Visualization. Previously, you could only copy and paste into it. (63920)
- This release fixes a refresh issue in Visualization's file details list pane that occurred when you changed Visualization metrics. (64931)
- Various display issues with Visualization views and behaviors have been improved. (64958)
- The *Total File Count* field in Visualization has been removed. (63991) (64231)

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 4.0
Release Notes

Introduction

This document includes information about the AccessData® Forensic Toolkit® (FTK®) 4.0 release. Please be aware that all known issues published under previous release notes still apply until they are listed under a “Fixed Issues” section.

For information about previous releases, see the AccessData web site at http://accessdata.com/.

Important Information

The following are important considerations to be aware of:

- You can download the Oracle Critical Patch Update for this release from the AccessData Support Downloads web site. Close all programs before installing the patch. (58583, 58248)
- If the computer running Imager or FTK has an active internet connection and you are viewing certain types of HTML or Web pages, there is a potential risk associated with specially crafted pages or binaries. These pages or binaries can trigger unintended consequences such as running malicious code or scripts.

  AccessData recommends that, wherever possible, users not have an active internet connection while running Imager or FTK. If the computer running Imager or FTK has an active internet connection and you are viewing certain files/binaries (for example, HTML), there is a potential risk associated with specially crafted pages. These pages or binaries can trigger unintended consequences, such as running malicious code or scripts.
- The Oracle database must be installed on a machine with a name that begins with a letter (a-z and A-Z). Applications cannot connect to Oracle if the machine name begins with a number.

  This is because of a restriction on domain names in RFC 1035.

  If the Oracle computer has a name that begins with a number, you must change the machine name prior to installing Oracle.
- The database software should be installed to a physical system drive whenever possible. AccessData does not support configurations where the database is running on a virtual machine. Additionally, installing the CodeMeter software on a virtual machine is not recommended. (56262)
- FTK does not support skipping versions when upgrading cases. You must upgrade in the order of released versions. For example: you cannot upgrade cases from FTK 3.1 to FTK 4.0. In this example you would need to upgrade first from FTK 3.1 > FTK 3.2 > FTK 3.3 > FTK3.4 > FTK 4.0. (63494) (57461)
- If you bookmark a manually carved item that has not been processed, the file will not show up in the bookmark or report until you process the manually carved item using the "Process Manually Carved Items" option in the *Evidence* drop-down menu. (57812)

4.0 New, Improved, and Enhanced Features

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

Remote Analysis Enhancements

- This version introduces enterprise-class remote analysis capabilities. It now includes the incident response and remote digital investigation capabilities of the Enterprise agent on a single node at a time. For more information, see the topics in the chapter, Working with live Evidence, in the user guide.

Additional Functionality

- FTK now supports processing Exchange 2010 EDB files. You can drill down and get all the emails in all the mailboxes in the EDB. (59391)
- Index searching now supports Microsoft TR1 regular expression operands for pattern searches within individual terms (not across words or terms). (54594) For Microsoft TR1 Regular Expressions support information see http://msdn.microsoft.com/en-us/library/bb982727.aspx
- Processing support for 7-Zip files has been added to this release. However; to decrypt them you must use PRTK. They cannot be decrypted within FTK. Also note that they may take more time to expand than WinZip files. (59828) (60015) (58907) (60093)
- FTK supports additional memory analysis capabilities including the ability to parse and display handle information, as well as support for viewing data from the Virtual Address Descriptor (VAD) tree. You can view the resources that allocated by programs by viewing the information that is contained in the VAD tree.
- FTK can now read images containing more than 1,000 segments. (63302)
- Optical Character Recognition (OCR) is now supported when running FTK on XP Operating systems. (57776)
- Added Checkpoint/PointSec R73 7.4.5 decryption support.
- Added YAFFs phone file system support to FTK 4.0 (64090)
- Added support for SafeGuard Enterprise 5.6 image files (62450)
- Indexing support of Visio 2010 .VSDs.
- Indexing support of .DOTMs.
- Indexing support of .DOTXs.

Processing and Performance Enhancements

- Processing enhancements to process evidence concurrently and use memory more efficiently.
- Optimized DB threading for improved processing performance.
- Improved memory handling for processing large cases (61423)
- New option to OCR only PDF files that have small extracted text according to a settable threshold. Has yielded 34% - 47% observed speedup.
- Omitting Office Metadata (e.g. creator, reviewer comments) and only expand office docs with actual embedded objects (e.g. Not OLE streams)
- Only expanding real attachments of RFC822 Emails
- Improved the processing and the indexing of Visio 2003 (.vsd) files. (62451)
- Improved FTK's parsing of index.dat files to better handle the *Checked Time* and the *Expired TIme* timestamps. (59480)

- FTK no longer indexes KFF ignorable files by default. This change improves processing. If you need to index KFF ignorable files you can select them in the pre-processing screen, under *Index Refinement (Advanced)* options. (62914) (62915)
- Word lists now import faster. (59040)
- Improved UI performance when expanding email trees in the *Email* tab. (58453)
- When processing internet emails, extraneous folders and other mime parts are no longer added as separate items. (62257)
- The *Apply label* drop down has been enhanced to let you click the displayed label to apply it to a file instead of being forced to choose it from the drop down each time that you want to apply the same label. (55166)
- The *Decryption* dialog has been enhanced to allow users to enter multiple passwords by pressing the “Enter” key between each one instead of having to click the **Save password** button. (59127)

Miscellaneous Enhancements

- An SMS text message column is now available in reports on mobile phone images. (60032)
- A warning message is now displayed when you attempt to switch an application administrator to a case administrator or case reviewer (59565)
- Within the *Live Search* module the tabs for *Text*, *Pattern* and *Hex* now remain docked when selected. (59671)

4.0 Fixed Issues

The following items are resolved issues in this release:

Backup/Restore

- You can now use cancel buttons (“X icons”) in the interfaces to back-up, restore, and archive cases. (56287) (59012)

Decryption Fixes

- FTK now shows/decrypts from multiple IDs setup by SEE. In previous versions it only supported one. (60839)
- When adding a recovery file for CheckPoint encryption, when you click the browse button, the *Open* dialog now appears in front of the *Credentials* dialog as expected, instead of behind it. (62797)
- Improved processing of Base64 encoded attachments in sent email messages. (61605)
- Improved the handling of XLS files that are level 1 encrypted (protected cells). These files should be able to be viewed without the password. (61200)

Email Fixes

- Improved the algorithm for finding an email’s logical/physical size. More emails now have a logical/physical size than in previous versions. (61252)
- Improved Lotus Notes email processing so that embedded icons do not show as attachments in FTK. (61451)

Export Fixes

- Improved interface responsiveness when doing multiple export jobs. (57378)
- Improved handling of email export for the subject line of an Outlook 2010 email. (60335)
- Improved the file export feature to better handle long file paths. (58893)

Install Fixes

- Oradjuster has been added back into the FTK installation wizard. (61858)

Known File Filter (KFF) Fixes

- After a KFF import completes, the defined sets now show up in the list. (60061)

Processing Fixes

- Improved RFC822 email handling for the delivery time field. (61800)
- Improved processing. Fixed an issue where in certain instances the processing engine would hang. (59689)
- The Distributed Processing Engine installer now includes a prerequisite check for .NET 4 availability.(59285)
- Improved the processing and indexing of certain PDF files. (61408)

Searching Fixes

- The *Indexed* column does not display an *N* for non-indexed item. Instead; if an item has not been indexed, the column is displayed as blank. If the item has been indexed, a *Y* is displayed in the column. (59347)
- In previous versions, creating a bookmark from an index search failed if the search term was over 2000 characters. This has been fixed, and the search term that is saved in the bookmark comment is now truncated at 2000 characters. (58798)
- Improved indexing functionality on decrypted files that are processed after the initial processing operation has been run. (63547)
- The time stamps for Live Search in the PostgreSQL Database are now in UTC time instead of the local machine time. (60102) (63360)

Miscellaneous Fixes

- FTK loads more than the first page of documents (PPT, DOC, PDF, etc.) in the natural file content view. Note: Large documents may take a long time to load. (59256)
- Fixed an issue with sector size information when restoring an image to a drive. (60202)
- Fixed an issue where in certain situations "Execute SQL" was failing. (59476)
- When doing a *Copy Special/Paste* into a spreadsheet, the *Accessed Date* column is now populated with available dates instead of N/A. (60187)
- The default setting for the *Auto Commit* interval is now displayed in the FTK UI. (61933)
- In the *Filter Manager*, the images for the VENN diagrams have been updated to more accurately represent the functions of the operators that they represent. (57652)
- Fixed an issue with mounting Logical evidence files in Imager if they were created with FTK.

4.0 Known Issues

Known Issues:

- The IRP and Layering information in the *Detailed Information* pane will only update when you click on an item that has the additional data. Information may still be displayed from a prior item when you have clicked on a different entry that did not have any additional detailed information. (64207)
- If you create a case that has a space at the end of the name, add live evidence, and then choose to create an AD1, the program will crash. To workaround this issue do not put a space at the end of the case name. (62386)
- The PostgreSQL database may fail to initialize if the locale of the computer contains an apostrophe character. For example, the locale “People’s Republic of China.”

  To work around this issue, you must initialize the database manually by running the following command:

  ```
  C:\Program Files\AccessData\PostgreSQL\bin>initdb -U postgres --pwprompt -E UTF8 -A md5 --no-locale -D d:\pgData
  ```
- FTK does not prevent you from creating two or more *Column Settings* profiles with the same name but with different character case. For example, although not recommended, you could create two different profiles named “Email” and named “EMAIL."(55732, 52510, 58961)

4.0 Release Notes for Add-on Modules

4.0 Release Notes for the Cerberus Add-on

FTK now supports a new add-on module for malware analysis called Cerberus. Cerberus integrates with FTK to let you detect and triage suspect binaries. In minutes, you can determine the behavior and intent of binaries, as well as the potential threat they pose, without waiting for a malware team to perform weeks of analysis. Cerberus requires an additional license. For more information, see http://accessdata.com/.

Please note the following:

- Additional analysis can be run to include files that have not had the *Cerberus Stage 2* done if the threshold value is lowered. In this case, if the threshold is raised FTK does not delete the Cerberus stage 2 results that have already been created. (62993)

4.0 Release Notes for the Visualization Add-on

FTK now supports a new add-on module called Visualization. The visualization module lets you view data in seconds in multiple display formats, including time lines, cluster graphs, pie charts and more. This functionality lets you quickly determine relationships in the data and find key pieces of information. Visualization requires an additional license. For more information, see http://accessdata.com/.

Please note the following:

- Visualization can only display data that has an associated date. If a file or an email does not contain a valid Created, Modified, Last Accessed, Sent or Received date, it is not displayed in the visualization module. For example, carved files do not have an associated date so they are not displayed in the visualization module. If you attempt to visualize a data set that does not have dates, the time line pane displays the text *No data Series*. If a file contains a Created date but not a Modified date, and you change the pane to display the file by Modified date, the file is no longer displayed in the visualization module. (61524)