

---

---

# *AccessData FTK 3.1.2*

## *Release Notes*

### **CONTENTS**

- *AccessData FTK 3.1.2 Release Notes..... 1*
- *AccessData FTK 3.1.1 Release Notes..... 3*
- *AccessData FTK 3.1 Release Notes..... 5*
- *AccessData FTK 3.0.4 Release Notes..... 15*
- *AccessData FTK 3.0.2 Release Notes..... 19*
- *AccessData FTK 3.0 Release Notes..... 23*

### **INTRODUCTION**

These Release Notes cover improvements and bug fixes for AccessData FTK 3.1.2.

### **NEW AND IMPROVED**

- The “View This Item in a Different List” feature has been improved to allow the user to right click on a folder, then go to that folder in the Graphics tab and see the files inside. This change accommodates the need for users to select a folder with an EID score and then to be taken to that same folder in the tree on the Graphics tab. The File List view is then populated with the graphics contained in that folder. (17073)

- 
- In the Index Search tab, a check box, *Accumulate Results*, has been added that tells FTK to calculate cumulative results for indexed searches when requested by the user. If not marked, the cumulative results will not automatically display. (18154)
  - Improved identification support for JavaScript Object Notation (JSON) files such as those found in programs like FaceBook. When found in a case, they are categorized as JSON files. (15557)

## BUG FIXES

- Fixed the Registry Viewer to correctly report in the Key Properties window the UserAssist values whose offsets were changed in Windows 7. (18202)
- Reformatted the RSR report file names to be shorter, and thus enable them to be burned to a CD. (18198)
- “View item in a different list” now works, even if the evidence item was in a group. (18188)
- Importing a .KFF file into the KFF Manager no longer causes FTK to crash. (18111)
- FTK & Imager now properly identify files in NTFS, even when the \$MFT \$Bitmap is corrupted. (18096)
- The body of an e-mail from an .OST, when exported in .MSG format, is now properly displaying when viewed in Outlook. (18069)
- FTK now displays Firefox columns and data correctly even when columns have been added. (15175)
- FTK 3.0.4 cases now successfully copy to FTK 3.1 even if a case has been backed up and restored, or has been archived and detached and then attached.
- If you were using NLS previously, and had a problem with licenses not immediately releasing licenses when the program is exited, you must install the latest version of NLS that is provided with the FTK 3.1.2 release to correct the problem. (18133)
- If you carve any single one type of file, Additional Analysis now allows you to carve other files as well. (17983)
- Illegal characters in Email Subject Line are now replaced with underscore(s) when the email message is exported to MSG. (16812)
- Manually carved items can now successfully be added to a bookmark on creation. (18154)

---

## KNOWN ISSUES

- If the user starts building a Custom Data View (CDV) and then closes the dialog, the menu option is greyed out and it cannot be reopened until all CDV(s) being built are complete. (18386)

---

---

# *AccessData FTK 3.1.1*

## *Release Notes*

### **CONTENTS**

- *AccessData FTK 3.1.2 Release Notes..... 1*
- *AccessData FTK 3.1.1 Release Notes..... 3*
- *AccessData FTK 3.1 Release Notes..... 5*
- *AccessData FTK 3.0.4 Release Notes..... 15*
- *AccessData FTK 3.0.2 Release Notes..... 19*
- *AccessData FTK 3.0 Release Notes..... 23*

### **INTRODUCTION**

These Release Notes cover improvements and bug fixes for AccessData FTK 3.1.1.

### **NEW AND IMPROVED**

- Added support for carving FAT Lost File Chains. (17826)
- The “Manage Labels” dialog has been improved to allow the user to Extend Labels to “family” associated items. (17936)

In this context, “Family” means to apply the same label to the parent item and all sibling and child items, as follows:

- 
- Family for email and attachments means the entire email node and descendents. For example, if you label an attachment, extending that Label will include the email (actual email in the archive, not embedded) and all descendents.
  - Family for non-email related items (eDocs) means the actual file on the filesystem. For example, labeling an item in a .ZIP file will label the top level .ZIP and all the descendents of it.
  - The Extend Labels feature includes two options: (17193)
    - One for children of the selected item including the selected item.
    - One for parents not including the source archive. These options would travel the archive the item is contained in, and label all related items down the tree and up the tree to (but not including) the archive itself.

## BUG FIXES

- Fixed a problem where cases copied from FTK 3.0.4 would fail to copy to FTK 3.1 if the case has been restored in any way. The fix applies to cases that have been backed up and restored, as well as those that were archived and detached and then attached. (17808)
- Fixed a problem with Backup and Restore when using UNC paths.

## KNOWN ISSUES

- RSR generated files are named in a manner that allows the user to see what Registry file was used to create the report, as well as the template used. Because of this, the file name can become quite long, and may result in path length issues in certain circumstances, such as when burning a report to disc.

## COMMENTS?

We value all feedback from our customers. Please contact us at [support@accessdata.com](mailto:support@accessdata.com), or send documentation issues to [documentation@accessdata.com](mailto:documentation@accessdata.com).

---

---

# *AccessData FTK 3.1*

## *Release Notes*

### **CONTENTS**

- *AccessData FTK 3.1.2 Release Notes..... 1*
- *AccessData FTK 3.1.1 Release Notes..... 3*
- *AccessData FTK 3.1 Release Notes..... 5*
- *AccessData FTK 3.0.4 Release Notes..... 15*
- *AccessData FTK 3.0.2 Release Notes..... 19*
- *AccessData FTK 3.0 Release Notes..... 23*

### **INTRODUCTION**

These Release Notes cover new features and enhancements, as well as bug fixes and known issues for AccessData FTK 3.1.

### **IMPORTANT INFORMATION**

- AccessData recommends that the amount of RAM be 2 GB per processing core (e.g. an 8 core machine should have at least 16 GB of RAM). The minimum RAM must not be less than 1 GB per core.
- As a rule of thumb, remember that Distributed Processing may not help reduce processing times unless the number of objects to be processed exceeds 1,000 times the number of cores. For example, on a system with eight cores, the additional

---

distributed processing engine machines may not assist in the processing unless the evidence contains greater than 8,000 items.

- If you want to change the Temporary Files folder, you must run FTK as Administrator. (17147)

**Important:** AccessData has changed the way jobs are allocated to each engine based upon available resources. The new approach works by calculating the Number of Cores or hyper threading time two (2), which determines the total number of processing threads the engine will use. Each job requires minimum of two threads plus one GB of FREE physical memory to start. So when the engine gets a request to process something, it looks at the total number of jobs it is already working on. If it has at least two threads it can use on the new job then it looks at free physical memory. If it also finds one GB free RAM available, then it will start up an `adprocessor.exe` to process the job.

## NEW AND IMPROVED

- FTK can now be configured to send an email when processing is complete.  
**Note:** The FTK computer must be able to connect directly to the recipient's SMTP server.
- FTK 3.1 and FTK Imager 2.8 now have the ability to encrypt images. E01, S01, 001 (RAW/DD), and AD1 can be encrypted with AD Encryption, which supports the following:
  - Hash algorithm SHA-512.
  - Crypto algorithm AES-256.
  - Key materials (for encrypting the AES key): pass phrases, raw key files, and certificates.
- A user account having Admin rights is no longer required for running FTK. However, Admin rights are required the first time FTK 3.1 is run. (16209)
- Case folders are now automatically given the user-defined case name for easier identification. Duplicate case names will cause a number to be appended to the end of the folder name. (996)
- H.264 formatted videos are now properly recognized and played in FTK 3.1 if the correct codecs are installed. (13044)
- FTK now supports EFS decryption of EFS files encrypted on Windows 7 systems, using default Windows 7 EFS settings. (14634)
- Added support for Vista Bitlocker image processing. (14948)
- Live Search is now significantly faster. (16315)

- 
- New Filter Manager feature allows advanced user control and manipulation of filters. You can now create and apply compound filters, and can both Include and Exclude file types using the Filter Manager. (15084)
  - New in version 3.1 both the Online and Offline Credant Decryption dialog boxes have a Decryption Threads dropdown box. This dictates the total number of threads assigned to decryption, not the number of decryption threads per core. Generally the default value can be used, but higher or lower values can be selected if necessary. (17543)
  - A new File Property Column has been added called “Included by Filter(s)”. It displays the filters that are active that caused this file to display in the File List View. If a compound filter is selected (uses multiple filters), each filter is listed, and is separated by a comma from the next one. This column is not sortable. (16637)
  - FTK 3.1 now provides Cumulative Results for all files when multiple search terms are entered. The Cumulative Results feature works for both “And” and “Or”, which is indicated at the bottom of the cumulative results display. (14953)
  - Evidence items can now be organized into user-created groups called Evidence Groups, which can be specific to a single case, or shared between cases. There is a new level in the Evidence tree for these groups. If an evidence item is not assigned to a group, that item will be listed at the root of the Evidence tree node instead of under an Evidence group. (15173)
  - Explicit Image Detection now populates the EID scores for folders, as well as files, so the user can quickly see where to focus the investigation. (15270)
  - Optical Character Recognition (OCR) has been added to the processing options for FTK 3.1. The OCR process extracts text in graphics files and then indexes the content so extracted text can be, searched, bookmarked, and so forth. (15285)

Selecting OCR in Evidence Options activates the OCR Options button. Clicking the OCR Options button opens a dialog with the list of supported file types and a check box for the selection of each.

Selecting a file type in this dialog will result in a new (child) file item. The new OCR file is named the same as the parent graphic, [*graphicname.ext*], but with the extension .OCR, for example, *graphicname.ext.ocr*. When viewing this additional child OCR item, the OCR text output will be seen in the Filtered View tab. If the Natural View tab is selected, the parent graphic is displayed.

**Important:** It is important to understand the limitations and variability of the OCR process. Therefore, the following information may prove useful as you incorporate the use of OCR in the processing of your cases:

- OCR can have inconsistent results. OCR engines by nature have error rates which means that it is possible to have results that differ between processing jobs on the same machine with the same piece of evidence.

- 
- The Tesseract engine that FTK uses for OCR is a learning engine and can generate different results on different computers.
  - Some large images can cause OCR to take an extraordinarily long time to complete and under some circumstances not generate any output for a given file.
  - Graphical images that have no text or pictures with unaligned text can generate garbage output.
  - OCR is best on typewritten text that is cleanly scanned or similarly generated. All other picture files can generate unreliable output that can vary from run to run.
  - OCR is only a helpful tool for the investigator to locate images from index searches and OCR results should not be considered evidence without further review.
  - The default Optical Character Recognition engine FTK ships with is Tesseract. AccessData also provides an option to upgrade the OCR engine to one which has better performance and a higher accuracy rate based on testing. To obtain the Glyph Reader OCR engine that has an additional cost please contact [sales@accessdata.com](mailto:sales@accessdata.com).
  - By default, OCR file generation is restricted to files larger than 5K. This can be adjusted by the user in the OCR options dialog. (17187)
  - A new user interface has been added in Detailed Options when creating a new case. The File Identification Options dialog for Custom File Identification now allows you to create and manage custom identifiers and map extensions to specific file types. Files are created in .TXT format and can be saved and reloaded. (15445)
  - FTK can now import a list of search terms for Live Search. (14826)
  - Data Carving has been improved. A new interface allows for the creation and modification of Custom Carvers. (15483)
  - Improved handling of Windows 7 `Thumbcache.db` files (16509)
  - AccessData now offers a WIBU-SYSTEMS Virtual CmStick (soft license dongle). The Virtual CmStick is a file that allows full use of the program without worry that the USB CmStick could be lost or stolen.

Licenses can be bound and un-bound from one USB or Virtual CmStick to another just as with the original USB CmStick. The Virtual CmStick itself, however, is not transferable from one machine to another. (15228)

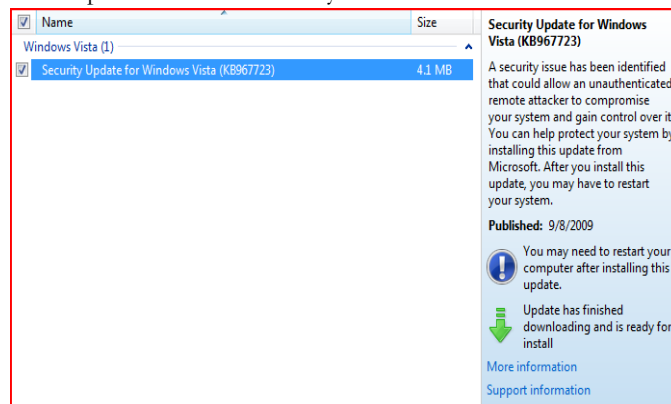
- Please contact Support if you are interested in migrating from a physical USB CmStick to a Virtual CmStick Soft License (virtual dongle).

**Note:** The Virtual CmStick is not supported in Virtual Machine environments or for NLS systems.

---

## BUG FIXES

- NSF container files are identified as one of 2 file types: “Lotus Notes Database” and “Lotus Notes Mailbox”. The exclusion list has been adjusted, and in the 3.1 release, the Lotus Notes Mailbox container will not be indexed, but the children will be.
- File List for Checked Items now loads faster and displays any counts in the File List Status bar for Loaded, Filtered, and Total. (10391)
- Improved handling of MBX files. (11850)
- HTML files that contain java script no longer run the java script when viewed. (16416)
- FTK can now decrypt EFS files with a user account that had no password. (16502)
- On the Index Search tab, under *Options*, the Search Options *Stemming*, *Phonic*, *Synonym*, and *Fuzzy Search* functions have been changed. Only one can be selected at a time, based on recommendations from DtSearch.
- The “Security Update for Windows Vista (KB967723)” published in 9/8/2009 fixed a Windows security issue, but when installed, RAM data acquired by FTK from that computer could not be analyzed in FTK 3.0.4



- That same data can now be analyzed in FTK 3.1. (16035)

## KNOWN ISSUES

- Important:** OCR (Optical Character Recognition) can have inconsistent results. OCR engines by nature have error rates which means that it is possible to have results that differ between processing jobs. For additional information see “New and Improved” on page 6 of this document.
- If your machine has less than 1 GB per core when processing multiple pieces of evidence under certain circumstances processing will fail and not recover. We

---

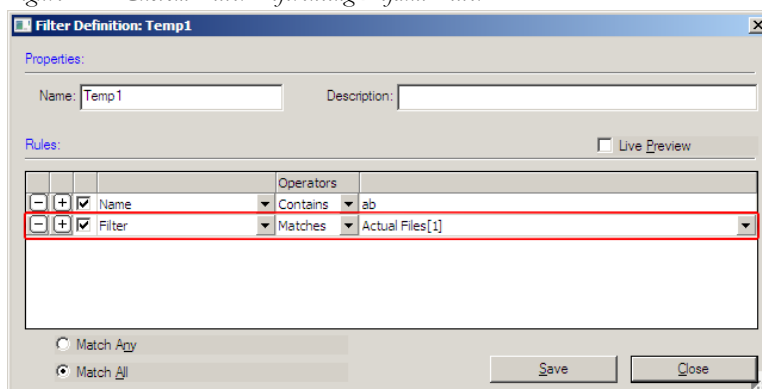
recommend that the amount of RAM be 2 GB per processing core (e.g. an 8 core machine should have at least 16 GB of RAM).

- When upgrading a case having live search hits from version 2.2.1 to version 3.1, the Live Search hits are not always correctly highlighted in the converted case. (17421)
- After right-clicking on a file and reassigning it as a different file type, the file continues to be filtered by both the original file type and the newly assigned file type. This is because manually reassigning a category does not change other file attributes (such as To:, From:, BCC:, etc) and thus that file may still show up as its original file type, or with different filters. (14083)
- Processing UDF logical drive appears to hang in processing during indexing. (16918)

**Workaround:** Image the UDF drive and add the image to the case.

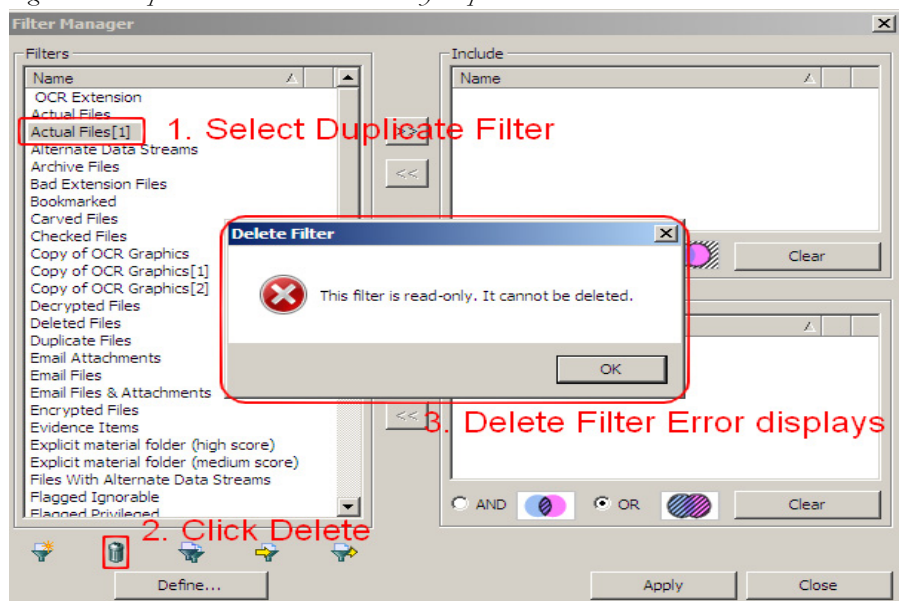
- Custom identification will not change file category for any compound or archive file (zip, pst, etc). (17119)
- Custom carved items are assigned the category chosen by the user in the carver definition, and are not run through file identification for category assignment.
- If a custom filter that references a default filter is imported, all default filters referenced within the custom filter will have a read-only duplicate with a [n] appended to its name. Such a filter is illustrated in the following figure (17478):

*Figure 1-1 Custom Filter Referencing Default Filter*



After the custom filter is created, saved, and exported, and the original deleted, importing the custom filter creates the following scenario:

Figure 1-2 Imported Filter Causes Read-Only Duplicate Filter That Cannot Be Deleted



- When running FTK 3.1 on a 64-bit system, if adding physical or logical drives as evidence, the drives list may be empty. This is an OS security issue, and applies only to 64-bit Windows operating systems as follows:

TABLE 1-1 64-bit Windows Operating Systems

- |                  |             |
|------------------|-------------|
| • XP             | • Vista     |
| • Server 2008    | • Windows 7 |
| • Server 2008 R2 |             |

**Workaround:** Logout of FTK, then run FTK again as Admin. Open the case and add the physical or logical drives.

- Plaintext/RFC822 emails (from Outlook Express, Eudora, MBox, etc.), may have duplicate hits. This is because the email itself and its preamble, epilog, mime parts, and so forth are being indexed. (17064)
- Generally, carvers in FTK are designed not to carve a file type from within a file of the same type. However, if using custom identifiers to change a file category for known file types, the built-in carvers will not know to skip carving and will carve out

---

a duplicate file of the original file type. For example, if a custom identifier is used to classify a PDF as a XYZ file, the carvers will carve out a PDF (the original file) and add it as a sub item of the custom identified file. (17103)

- In Windows, if the user has defined a TEMP\TMP path different from the system default TEMP\TMP path, the agent will push successfully to the machine, but may not run properly. Once the Temporary Agent is pushed to the remote machine, if FTK has trouble, login on the remote machine as Administrator, then follow Workaround instructions.

**Workaround:** On the Agent machine, click *Start* > right-click *Computer* > click *Properties* > *Advanced* > *Environment Variables*. Delete the User Variables or change them for TEMP\TMP to match the system variable TEMP\TMP path and restart the computer.

- When binary files are indexed (i.e searched for real words in a stream of binary data), by default, a “word” is added to the index only if it is detected that there are 6 characters in a row that are letters or numbers. If the user wants to reduce this level, they can change the value from 6 to 5, or 4, or 3 (3 is the minimum setting, 32 is the maximum). The benefit is that it will index shorter words that are currently ignored. However, significantly more irrelevant data will then be added to the index from binary files and processing will be slowed.

To change the default setting, add a key to the registry on all processing computers and set the value as follows:

- Key:

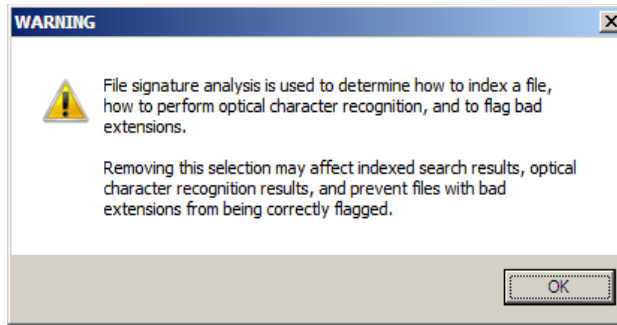
HKEY\_LOCAL\_MACHINE\SOFTWARE\AccessData\Products\Evidence Processing Engine\3.1\Indexer

- Value:

“UnicodeFilterMinTextSize”=dword:00000005

The last number in the value string is the number of characters the string should contain.

- Registry Summary Reports (RSR) requires File Signature Analysis as a dependency. File Signature Analysis is selected by default. Unmarking the File Signature Analysis option produces the following message:



Running RSR without Field Signature Analysis will result in no automatic RSRs being generated. (16666)

- System I/O Cache Registry: The System I/O Cache is a cache maintained by the OS. Windows caches all read I/O bytes - network and disk. So if the same thing is read again, and it hasn't changed, it comes straight from memory rather than going out to disk again. The Windows Operating System lets the System I/O Cache use as much memory as it wants. This works well provided there is free physical memory. If you have programs running that are doing a lot of I/O reads (like **adprocessor.exe** or **adindexer.exe**) that run for a long time, then the System I/O Cache swells up and uses all the available memory. When there is no RAM available for the system I/O cache, the OS gets more by going through all the user programs and taking memory from them. The result is that the user programs page out to virtual memory. This results in all user programs slowing down (because they have to read memory out of the swap file) which can ultimately lead to processing jobs failing because the ADProcessor times out. We have added a registry option in 3.1 that allows FTK to manage the system cache to prevent this type of situation.

If you notice that your system is slowing or you are getting errors in processing, you can limit the cache size by creating a specific Registry key.

To create the Registry key necessary to limit the system cache, do the following:

1. Run Regedit.
2. Navigate to:  
`HKEY_LOCAL_MACHINE\SOFTWARE\AccessData\Products\Evidence Processing Engine\3.1\`
3. Right-click on 3.1 and choose *New > DWORD*.
4. Name the new DWORD "SetSystemCache".

- 
5. Right-click on the new DWORD, *SetSystemCache*, and choose *Modify* (not Modify Binary Data).
  6. Change the Value Data to 1, with a Hexadecimal Base.
    - With this setting the engine will tell the OS not to use more than 1/3 of the physical RAM (or 1GB, whichever is more) for the System I/O Cache.
  7. Exit Regedit.
  8. Run FTK as Administrator to use the newly created key.

## COMMENTS?

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

---

---

# *AccessData FTK 3.0.4*

## *Release Notes*

### CONTENTS

- *AccessData FTK 3.1.2 Release Notes..... 1*
- *AccessData FTK 3.1.1 Release Notes..... 3*
- *AccessData FTK 3.1 Release Notes..... 5*
- *AccessData FTK 3.0.4 Release Notes..... 15*
- *AccessData FTK 3.0.2 Release Notes..... 19*
- *AccessData FTK 3.0 Release Notes..... 23*

### INTRODUCTION

These Release Notes cover installation prerequisites, bug fixes, and known issues for AccessData FTK 3.0.4.

### INSTALLATION PREREQUISITES

**Important:** If you are running eDiscovery, please call AccessData Customer Support before upgrading to the FTK 3.0.4 processing component. There are specific instructions you will need.

- You must have either an Administrator account or Administrator privileges for installing the CodeMeter software and managing licenses.

- 
- The Distributed Processing Engines must be installed (or configured) so that the process has administrator rights on the computer where the distributed engine is running (Domain Admin user rights are not sufficient). Refer to the Install chapter of the User Guide for more information.
  - If FTK 3.0.4 is being installed on Windows Server 2008 R2 .NET Framework 3.5.1 must be installed first. This can be done from the Server Manager Add Features Wizard.
  - By default, FTK is configured to optimize processing speed by creating indexes later in the process. This can cause searching for items while the case is still processing to be slow or unresponsive.

You can change this under *Tools > Processing Engine Config*, with the check box at the bottom. If you are using distributed processing, a registry change needs to be made on those computers as well.

A .REG file called **ProcessWithIndexes.reg** has been provided that can be run on the distributed processing computers that will make these registry changes for you. This is located in the FTK folder on the Application disk. Alternatively, the following two registry keys can be added to the distributed processing computers (remove these to undo the modification).

HKEY\_LOCAL\_MACHINE\SOFTWARE\AccessData\Products\Forensic Toolkit\3.0\ProcessWithIndexes (dword = 00000001)

HKEY\_LOCAL\_MACHINE\SOFTWARE\AccessData\Products\Forensic Toolkit\3.0\UsePlainBuffers (value = ON)

## NEW AND IMPROVED

- FTK 3.0.4 now supports distributed processing. Use up to 3 additional remote processing engines to improve processing time.
- There is a three (3) character minimum now for Live Search. This change was necessary to better utilize memory and provide faster performance. (15099)

## BUG FIXES

- Adobe Reader 9 files are now displayed in the Web view instead of Default view. (14570)
- Better handling of SQLite files (15376)
- Improved rendering of .NSF messages (15786)
- Improved processing speed of e-mail archives (6727)

- 
- Improved Progress Dialog information when processing multiple images (14261)
  - Metacarved files are no longer showing up in the file list when the “Actual files” filter is applied. (14579)
  - Recover Processing Jobs window no longer lists currently running jobs. (14941)
  - Improved MBX mailbox summary display (15307)
  - Improved agent connection performance (15706)
  - Kodak DCR files are now handled correctly in field mode (15744)
  - Improved EID options for faster processing (15899)

## KNOWN ISSUES

- DMG (Mac) images are displayed as “Unrecognized File System” in FTK. This happens only when the files are not “read/write” enabled. (15513, 15523)
- If the DMG is a full disk image or an image that is created with the read/write option, FTK will identify it properly. Otherwise the contents will not be recognized properly.
- If a distributed processing engine has been disabled, but not removed, the processing log will show errors trying to communicate with the disabled engine. Removing the engine from the list will eliminate these errors. (15733)
- Remote device mounting does not work on Windows 7 when mounting an NTFS drive. (15823)
- After processing a large case and then running an index search on terms that have a large number of hits, the results can sit in retrieving for several minutes. (15966)
- If a job is canceled during processing, the log may include a line that says the job finished, underneath the line that says the job was cancelled. (15721)
- After you cancel a remote acquisition with the agent, you must close the case to disconnect the agent. (15968)
- When a user adds a Safeboot image to a case for processing, the prompt to enter credentials will also notify the user of which partitions are encrypted in the image and lets the user choose which ones to decrypt. (15734)
- When a user selects to decrypt only one partition, the other encrypted partitions will not get added to the case as evidence.  
**Workaround:** decrypt all partitions at the time they are added.
- It is now possible to add a .CUE file as a valid image type. If the user selects add “All images in a directory”, FTK does distinguish between the .BIN and the .CUE files and the user gets double of everything. (15159)

---

**Workaround:** Remove the duplicate items before processing.

- If a user does a memory acquisition without selecting a destination, the dump file is saved to the root. (16033)
- On certain 64-bit operating systems, LicenseManager may not launch from within FTK. If this is the case, launch LicenseManager from the desktop shortcut or from the start menu.

## COMMENTS?

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

---

---

# *AccessData FTK 3.0.2*

## *Release Notes*

### **CONTENTS**

- *AccessData FTK 3.1.2 Release Notes..... 1*
- *AccessData FTK 3.1.1 Release Notes..... 3*
- *AccessData FTK 3.1 Release Notes..... 5*
- *AccessData FTK 3.0.4 Release Notes..... 15*
- *AccessData FTK 3.0.2 Release Notes..... 19*
- *AccessData FTK 3.0 Release Notes..... 23*

### **INTRODUCTION**

These Release Notes cover improvements, bug fixes, and known issues for AccessData FTK 3.0.2.

### **FYI**

- You must have either an Administrator account or Administrator privileges for installing the CodeMeter software and managing licenses.

---

## NEW AND IMPROVED

- FTK now supports distributed processing. Up to three additional processing engines can be employed to speed up case processing.
- FTK UI now supports Swedish and Turkish.
- New Memory Acquisition Features:
  - Process and DLL Dumping - option to dump processes and DLLs directly from memory dump or live memory to files.
  - Page File Support - option to dump the page (swap) file with a memory dump.
  - Create .AD1 Image file from memory - option to combine the memory dump and page file into an .AD1 image.
- Cases can now be sorted in the Case Manager by either Name or Date Modified. (3645)
- The Live Search tab, *Other Code Pages > Select Other CodePages to Search* dialog now has “Select All” and “Unselect All” buttons. (14385)
- EMLX files are now supported in FTK 3. (14439)
- The Label column in the File List View now can be sorted to place all files with Labels together at the top or the bottom of the File List (sorted by first character of the first label applied). (14595)
- Enhanced AOL address book support. (14791)
- KFF Admin dialog will now delete all selected defined sets at one time. (8282)

## BUG FIXES

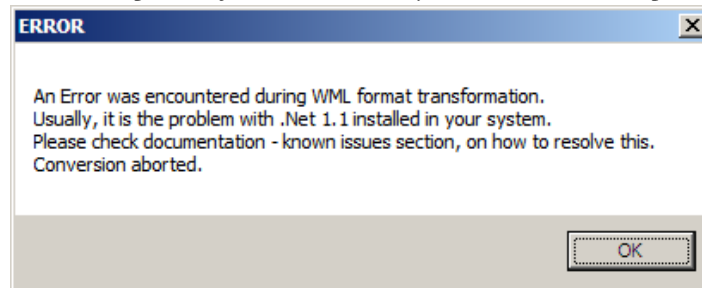
- Field Mode slow processing has been corrected.
- ”Bookmark selection in File” is no longer grayed out when creating a bookmark from an Index search result. (8768)
- When importing hash sets, cancelling the process no longer produces an error. (8781)
- “Open in Registry Viewer” now works properly when chosen from the right-click menu on a selected registry file in a case. (14373)
- Registry report “System - Time Zone Settings.rsr” is now being generated correctly. (14374)
- A new Cancel button allows cancelling out of the Map Users dialog instead of continuing with possibly the wrong settings or user mappings. (11697)
- Deleting a hit in the Index Search tab now works properly. (12024)

- 
- Statuses for all images being concurrently processed now display properly. (14261)
  - Specifying a report output folder with double-byte characters in the name or path no longer causes report generation to fail. (14288)
  - Credant .CEF files are now being correctly categorized. (14547)
  - Evidence Processing Options are now displayed properly for evidence items in the Add/Remove Evidence window. (14389)
  - Resolved the processing issue causing the error “Inso\_pipe\_helper.exe - Entry Point Not Found”. (14517)
  - Clicking *View->Tab Layout->Reset to default* no longer causes the File List in the Index Search tab to go blank. (14578)
  - Metacarved files no longer show up in the File List when the “Actual Files” filter is applied. (14579)
  - FTK now converts %20 to a space in the URL field for **index.dat** files. (14596)
  - The down arrow now works in the Supplementary File List for a Bookmark. (14449)
  - Fixed a bug where, if processing crashed while the initial enumeration was running, the same evidence item was added multiple times to the case. (14507)
  - PostScript graphic files are now processed correctly. (14397)
  - Viewing hits in filtered view no longer produces an error. (14400)
  - Improved handling of Index.dat files. (14571)
    - In the UI, File List view, URL items list in the header (left side) as “URL”; Leak items list as “URL - LEAK”, and Redirect items list as “URL - REDR”, so they can be distinguished easily by investigators.
    - In delimited output such as .CSV or a Copy Special, a new column has been added as the first column output. It is labeled “Type” and will contain the type of item “URL”, “LEAK”, or “REDR” to identify the type of item and to allow investigators to sort by type.

## KNOWN ISSUES

- FTK can crash when moving to a tab that was created with a UI-language setting other than the current one. (1926)

- 
- Some report output formats require J#, either 1.1 or 2.0. If you select .RTF format, for example, and J# is not installed, you will see an error reporting the following:



This happens when creating a report in any or all of the following formats: RTF, WML, DOCX and ODF. To resolve this error, install the J# version, either 1.1 or 2.0, that matches your .NET installation.

- “Copy Case from 2.2.” function cannot copy fuzzy hash groups and they will be removed from the copied case (although still present in the original). (14640)
- Processing a live DVD can take an extremely long time to process. AccessData recommends creating an image of the DVD first and then processing the image.
- Report settings cannot be imported from earlier versions into 3.0.2. Report settings must be recreated after installing the 3.0.2 Patch. (14563)
- Configuring Distributed Processing (*Case Manager > Tools > Processing Engine Configuration*) is slow, but it is working. Once selected, please allow it to finish.
- You must expand the search hits at least one level (Allocated/Unallocated) to be able to highlight a search query, then click on a file in the file list pane and view the file in the File Content pane.
- The Pause, Resume, and Cancel buttons on the Processing Window are not working at this time.

## USEFUL INFORMATION

- When employing distributed processing, there are operations that will only utilize a single engine. When an archive or compound file is being opened/expanded the operation must complete before the discovered items are sent to the distributed processing engines.

---

## COMMENTS?

We value all feedback from our customers. Please contact us at [support@accessdata.com](mailto:support@accessdata.com), or send documentation issues to [documentation@accessdata.com](mailto:documentation@accessdata.com).

---

---

# *AccessData FTK 3.0*

## *Release Notes*

### **CONTENTS**

- *AccessData FTK 3.1.2 Release Notes..... 1*
- *AccessData FTK 3.1.1 Release Notes..... 3*
- *AccessData FTK 3.1 Release Notes..... 5*
- *AccessData FTK 3.0.4 Release Notes..... 15*
- *AccessData FTK 3.0.2 Release Notes..... 19*
- *AccessData FTK 3.0 Release Notes..... 23*

### **INTRODUCTION**

These Release Notes cover new features, enhancements, and known issues for AccessData Forensic Toolkit 3.0.

### **NEW AND IMPROVED**

- FTK now features Remote Drive capture and mounting capabilities. This enables examiners to use FTK, Imager, or a 3<sup>rd</sup>-party application to forensically analyze live data (system memory, logical volumes, physical devices) on a remote device from the examiner system.
- RAM Dump Analysis can enumerate running processes, associated DLLs, network sockets, etc. from 32-bit Windows computers.

- 
- Index search results are now grouped by category.
  - Redesigned Processing Engine with Cancel/Pause/Resume functionality.
  - File List is much more responsive.
  - Support has been added for decryption of PGP® Whole Disk Encryption.
  - Support for Guardian Edge disk decryption has been added.
  - Improved Macintosh support including processing of B-Trees, PLIST support, SQLite support, Apple DMG and DD\_DMG disk image support, and JSON file support.
  - FTK 3 now offers automatic Registry Viewer Summary Report (RSRs) generation during processing.
  - EXIF data for JPG files now display as sub-items when Expand Compound Files is selected.
  - Enhanced Graphics Tab has faster image retrieval and backup time, new icons to represent corrupted images and images still loading.
  - New Progress window shows detailed processing information.
  - File times shown in the file listing window now include the time zone info (using the +/- offset from GMT format - i.e. +7) after the time.
  - Improved CD File System support.
  - Index Search Tab Results List loads faster.
  - Items including thumbnails, decrypted files, and supplementary files from bookmarks are no longer stored in the database. They are now put in the case folder.
  - In FTK 3.0, when exporting Index search result hits to a spreadsheet file, the hits are exported as a .CSV file in UTF-16LE data format. When opening in Excel, use the Text to Columns function to separate out the Index Search hit values into columns.
  - Generated text that is the result of a formula in a document or spreadsheet is indexed, and can be filtered.
  - The Oradjuster utility has been integrated into the FTK interface under the case Tools menu. This allows memory allocation to be quickly adjusted depending on what tasks are being performed.

**Note:** The integrated utility will only work if FTK and Oracle are on the same computer and Oradjuster has already been run once outside of FTK.
  - LTU Explicit Image Detection has been integrated into this release of FTK. Look for the functionality in the Detailed Options dialog as Explicit Image Detection. A separate LTU license is required to enable this capability.

- 
- Decrypted filenames are now patterned as “*filename - decrypted.ext*” instead of “Decrypted copy of *filename.ext*”. This allows them to be sorted by file name so they are next to the source item.
  - The email attachment pane is now available on any tab except Volatile, and does not require the email tree to be present.
  - In the File List, bookmarked items display in a different color for easy identification. You may need to refresh the view to force a rewrite of the screen for the different color to display.
  - Users can select a unique column setting per bookmark for report generation.
  - Improved support for Cascading Style Sheets (CSS) for HTML report generation.
  - Enhanced support for exporting Exchange emails to MSG.
  - The symbol “»” is used in the File List to denote that the path for files found inside archives is not a path to actual files.
  - Application Administrators can now update user account settings such as User Name, Role, and Password.
  - Session Management window now has a refresh option to enable the user to view updated status.
  - Detached Viewer can now be launched from a right-click menu.
  - The SAM registry report now shows the Relative Identifier (RID) in decimal format.
  - FTK now lets you attach and detach cases from the Case Management window.
  - FTK 3.0 now supports new Encase 6.12 image format (SHA1).
  - To overcome the file size limitations of .MDB files, the File Listing Database is now created in .CSV format and can be added to Microsoft Access, Excel, etc.
  - When importing an archived case, the users can be remapped to different users if needed.
  - The Case Processing Report now includes items that could not be processed per evidence.

## BUG FIXES

- Users now have the option when FTK is first run, to connect to a remote Oracle database even when a local database exists.
- The install now fully supports installing to a folder named with Unicode characters.
- When importing hashes from a CSV file to the KFF library, the last hash is no longer dropped if it is not specifically followed by a hard return; program also checks for

---

proper length of last MD5 and SHA1. If MD5 is too short neither will be written, if the SHA1 is too short, only the MD5 will be written.

- .LST File types have been moved to the Unknown category and their text content will now display.
- In the Case Management window, certain options that were available can no longer be accessed without user authentication.
- Better handling of HTML tags in emails added to reports.
- Faster response opening large cases.
- Ascending sort order Type-down for the following columns now work properly: Sent Representing Email Address, Sender Email Address, and Sent Representing Name.
- FTK now correctly identifies non-encrypted EXT3 partitions within an image or drive with SafeGuard encryption information in the boot sector.
- Improved OLE Stream identification.
- .BIN images are now included in the default list of image types when adding images to a case.
- User-Defined File Types now display properly in the File Types List.
- The message body of Internet mail exported to .MSG now displays correctly.
- HKE hash sets can now be imported into the KFF.

## KNOWN ISSUES

- On a 32-bit OS, if you switch to the Debug Logs in the View Menu in the Progress Window, and then back to Job Status, FTK UI will crash.
- The Remote Drive Mounting feature (RDMS) agent push requires that Simple File Sharing be disabled on XP target computers to be successful.
- If you click *Cancel* on the Data Processing Status window, you must manually end processinghost.exe before processing additional evidence.
- There are two predefined filters that do not work correctly:
  - KFF Ignore or OLE Subitems
  - KFF Ignore or OLE Subitems, or Duplicates
- Installing 32-bit FTK on a 64-bit system will not work with NLS.
- Running an Index search on large files or running Index Searches resulting in a large number of hits may make the scroll bar appear not to work. (TEAM 5474)
- Potential problem if restoring the same case multiple times simultaneously. When a user restores a case to FTK, they correctly receive an error when trying to add or

---

restore the same case again. However, when the user restores the case while the first attempt is still in the process of restoring, no error is received and the same case can be restored many times before the first attempt has time to complete. The result is a list of cases with unique case IDs but the same file path. If one case is then deleted, all of them have the file paths deleted that are in common.

- In the Index Search Results List, the offset of the data in the hit is no longer listed in the hit. You will see it when you look at the hit file in Hex view.
- If you add a description file to a case and then remove it and add the same file again, the file will not add the second time or any other time thereafter. **Workaround:** add some other file and remove it and then add the first file again.
- Bookmarks not in alphabetical order or numeric order. They are listed in order of creation.
- Find on disk feature won't find anything under 512b physical size. Files smaller than 1500 bytes may reside in the MFT and do not have a start cluster. Find on disk depends on that to work. This is working as designed.
- The color of bookmarked files in the file list will not change until the list is refreshed.
- Highlighted files in a file list are lost after applying a filter.
- While a file list is loading, if you click the cancel button on the tool menu, the File List must be refreshed in order to display the full list.
- When .DOCX and .XLSX files have formulas that generate text, that generated text can be searched on in those file types. Formulas in .XLS files cannot be generated, and thus the text cannot be searched.
- Currently the Oradjuster utility will only install to computers with English language operating system (or at least the Program Files path is in English so it can find the Oracle install location). When archiving a case, only the last 4 archives of that case are kept. Four file names are used for a case archive. It rotates thru from 0 to 3, and then overwrites the oldest. There is no prompt to remind you of the overwrite action.
- Processing a case using the Explicit Image Detection (EID) causes the processing to take much longer than without EID selected. This is normal due to the type of processing that is required.
- If the same evidence item appears multiple times in a case, the evidence item enumeration may have experienced a crash. Item enumeration occurs at the beginning of processing.  
**Workaround:** If this happens, it is recommended that the case be started over or that the failed evidence item be removed from the case.
- Any item that contains a “/” in the name will display “»” in place of the / (e.g. 10/21/2009 in an email name will display as 10»21»2009).

- 
- When viewing search hit results for binary file types the Natural view will not highlight the hits. Use filtered text.
  - Under certain circumstances, metacarving may find files with no name. Metadata for these files cannot currently reside in the database and will cause the discovered and processed counts to increment beyond the indexed count.
  - When installing KFF for FTK 1, you may encounter an error message:  
**Application\_is\_running.exe** has stopped running.

**Workaround:** Make sure FTK 1 is not running, select, close the program and continue with the installation.

- OrAdjuster does not work on German XP. (TEAM 14111 Bug)

Here's the background: **Oradjuster.exe** needs to find the **ORACLE\_HOME** folder, the folder structure where the database lives. Why? First, **Oradjuster.exe** calls **sqlplus.exe** to do its DB interaction, and it needs to know where to find **sqlplus.exe**. Second, **Oradjuster.exe** must shutdown and restart the DB (at least on its first run), and these operations must be done locally. Therefore, **Oradjuster.exe** must verify that the DB is present on the local host. How does **Oradjuster.exe** find the **ORACLE\_HOME** folder? By consulting a file created and left behind by the Oracle Universal Installer. The file is:

`%SystemDrive%\Program Files\Oracle\Inventory\ContentsXML\inventory.xml`

## COMMENTS?

We value all feedback from our customers. Please contact us at [support@accessdata.com](mailto:support@accessdata.com), or send documentation issues to [documentation@accessdata.com](mailto:documentation@accessdata.com).