

---

---

# *AccessData FTK 3.0.4*

## *Release Notes*

## INTRODUCTION

These Release Notes cover 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 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.

---

---

# *AccessData FTK 3.0.2*

## *Release Notes*

## **INTRODUCTION**

These Release Notes cover 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

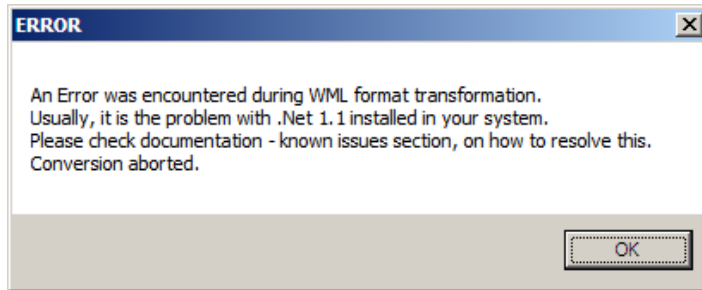
- Field Mode slow processing has been corrected.
- ”Bookmark selection in File” is no longer grayed out when creating a bookmark from an Index search result. (8768)
- When importing hash sets, cancelling the process no longer produces an error. (8781)
- “Open in Registry Viewer” now works properly when 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.

---

---

# *AccessData FTK 3.0*

## *Release Notes*

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 Material Identification has been integrated into this release of FTK. Look for the functionality in the Detailed Options dialog as Explicit Material Identification. 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 Material Identification (EMI) causes the processing to take much longer than without EMI 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`