

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 3rd-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 unencrypted 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 FileTypes 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 Simple File Sharing to be disabled on XP target computers to be successful.
- If you hit 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.
- 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.
- When a user cancels decryption of a Credant image and then attempts again to decrypt the image the message “Server Busy” appears and will not go away until the user exits FTK.
- 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. If this happens, it is recommended that the case be started over or 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 FTK1, you may encounter an error message:
Application_is_running.exe has stopped running
Make sure FTK 1 is not running, select, close the program and continue with the installation.