

# *FTK 2.2 Release Notes*

These Release Notes cover new features, enhancements, and known issues for AccessData Forensic Toolkit 2.2.

## **NEW AND IMPROVED**

- This release allows 2.1.x and 2.2 (and future) versions of FTK 2 to be installed on the same machine, at the same time, using a single installation of the Oracle database. There is no requirement to uninstall the existing version of FTK 2.1.x or to convert existing cases. This allows cases to remain in the version of FTK in which they were created. If you prefer to convert cases to be compatible with FTK 2.2.0, there is a utility to do the conversion (see instructions below).
- New indexing options are available to create more targeted indexes to help locate data faster.
- Field Mode quickly enumerates the contents of evidence items without pre-processing options (no hashing, indexing, etc.). File categorization is based on extension only. File Signature Analysis can be performed in Additional Analysis to refine categorization based on file header/signature content.
- Searches can now be done while indexing is still running without interfering with the indexing process.
- Export email messages from PST format to MSG files

- Support for LZ1 compression in Lotus Notes
- Improved options for refining OLE streams
- Improved parsing of AOL/AIM buddy lists
- Custom graphic/logo can now be added to reports
- Users can now filter by evidence ID
- Improved handling of CD/DVD images
- Faster display of search hit results
- File exporting speed is faster
- User interface working with Labels is faster
- Other UI and database performance improvements

## BUG FIXES

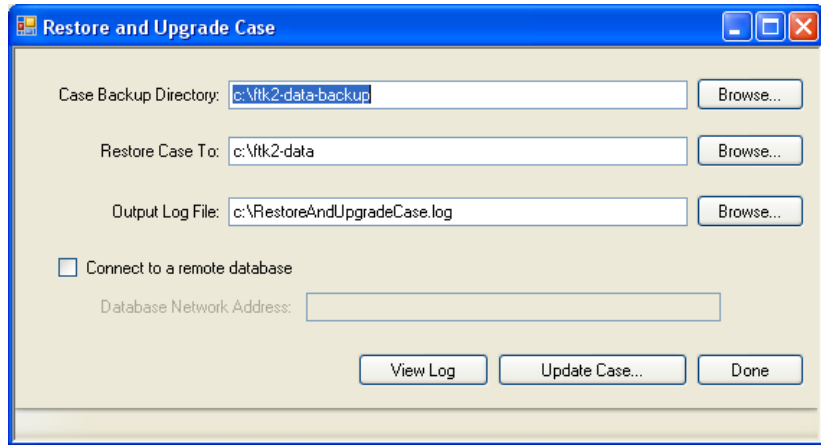
- Fixed several reported crashes during indexing
- WMV video files were being categorized as Multimedia Audio files. They are now properly categorized as Multimedia Video files.
- Decrypting EFS or Credant files now takes advantage of multi-processor machines for faster performance.
- Fixed a crash when right-clicking on a graphic and selecting Open with Content Viewer
- BMP files contained in some Notes NSF files were not viewable. This has been fixed.
- Fixed a memory leak associated with Live Search
- Fixed a bug that caused a crash when launching multiple Registry Viewers after running a report
- Fixed a bug where NSF evidence could not be decrypted after going through a backup and restore process.

- Some NSF files were not being recognized as mailboxes
- Some NSF imbedded graphics were not showing up
- Fixed a crash when running dtSearch in Additional Analysis on large cases.
- Fixed an issue where DBX inbox emails were not being added if the emails were empty.

## UPGRADING CASES

AccessData has created an upgrade tool that will allow users to restore archived 2.1.x cases into 2.2.0. Launch the upgrade tool from the Start Menu under AccessData, Forensic Toolkit.

1. For the 'Case Backup Directory' path, enter the folder of the archived case to be restored. The original archived case will remain unaltered.
  - **Important:** Make sure the database patch has been applied to Oracle databases running on Vista x64 and Server 2008 x64 prior to backing up cases in FTK 2.1.x. If the patch is not applied cases will not backup properly and cannot be restored into any version of FTK. The database patch is contained in the FTK 2.1.1 patch download available from the AccessData web site.
  - On a two computer install, the Oracle services and the 'Restore and Upgrade Cases' application must have access rights to the archive (source) folder and the Upgrade application must have write access to the case destination folder and the log folder.



2. In the 'Restore Case To' path, enter the path to FTK 2.2 case folder. AccessData recommends using a different case folder than 2.1.1 is using.
3. In the 'Output Log File', enter the path and file name for the Upgrade log file. This log contains information on the conversion/restore process.
4. If the case is being restored to an Oracle database on a different computer, check the 'Connect to a remote database' box, and enter the IP address of that computer.
5. Click the 'Update Case' button. Watch for status in the bottom left corner of the dialog. The successfully converted/restored case will show up in the Case Management window in FTK 2.2.

## KNOWN ISSUES

- Oracle will not function properly if installed to a machine with a name that starts with a number.

- Deleting results from a previous Live Search while a new search is running causes the new search return zero hits. Running the search again will return results.
- The binary files setting of dtSearch will not have the exact same behavior in FTK as it does in dtSearch's products. FTK processing may take binary data and convert it to text as a separate step, then the text will get indexed. This may include files such as JPGs, OLE archives and streams, Access files, .DBF files, and huge binary data files (including unallocated space).
- If Field Mode is used to process the first evidence item added to a case, any additional evidence items added to that case will be processed in field mode. Additional Analysis can be used for further processing and indexing. If Field Mode is not used on the first evidence item in the case, the Field Mode option will not be available for additional evidence items added to the case.
- If the Field Mode box is checked and then unchecked in New Case Options, it will uncheck all the Detailed Options for Evidence Processing. Clicking the Reset to Factory Defaults button on the Detailed Options window will restore the default settings.
- When doing a “Find Similar Files” search multiple times, the results from the previous search may be cached and show up. To prevent this, use the “Clear the cache” checkbox.
- Choosing a max word length and then running a search may highlight the whole word instead of the portion of the word.
- The option for the Max Words to return may not limit the search results returned.
- Disk encryption is not supported for encrypted VMWare images.
- An unencrypted image of an encrypted drive may be incorrectly identified as being encrypted if there are non-NTFS, non-FAT partitions. The work around for these situations is to click the Cancel button when asked for decryption credentials
- When using a Checked Filter, the File Category treenode count does not update when unchecking some of the files that are filtered. A manual refresh will update the counts.
- Category item counts may not match Filtered item counts under certain circumstances. Files are first categorized by extension, and then later by file analysis. As a result, certain file types may contain

two category IDs for filtering, causing them to show up when either filter category is used.

- Using Voom to create a dd/001 image of a drive, may causing an "error without options" error/crash with the image. If you use Voom or some other program which puts a .bin extension on raw images, you must rename the image to .dd or .001 before processing it.
- Attempting to process CodeMeter as a physical drive will cause FTK2 to hang.
- The max word length has a minimum length of 4 even though the UI allows numbers lower than 4.
- If files are highlighted in the file list and then a filter is applied, the highlighting will be lost
- If more than 1000 labels are created for a case, labels will not work properly.
- If Field Mode is used, no index is created. If an Index Search term is entered, the hit count will appear as -1 in the Search Criteria list.

# *FTK 2.1.1 Patch Release*

## *Notes*

This patch will update FTK 2.1.0 to FTK 2.1.1.

## **NEW AND IMPROVED**

This patch contains the following fixes and updates:

- When Registry Viewer is launched from within FTK, it now displays on top of the FTK application instead of behind it.
- Issues with Backup/Restore/Deleting of cases has been resolved.
- Spreadsheet tabs, PDF, PPT, AUT files will now display properly in the viewer.
- Accuracy of the progress bar has been improved, including the reporting of 100% while the case is still being processed.
- Searching /viewing indexed search hits in large files has been improved.
- In Windows Vista and 2008 exporting filters now works properly.
- Issues with saving indexed search hits have been resolved.

- Customer reported crashes during processing and viewing cases have been resolved.

## **KNOWN ISSUES**

- The media tab is unavailable in XP 64-bit and server 2003 64-bit because Windows does not put a 64-bit version of media player on those operating systems.