
FTK 2.0.2 Readme

The following sections present information on the new features, resolved issues, and known issues with the FTK 2.0.2 release.

NEW FEATURES

The following features have been added to FTK with this release:

INTERFACE IMPROVEMENTS

The interface has been improved in the following ways:

- Cases open faster when selected in the Case Manager Window.
- The File Extension Tree in the Overview Tab expands and collapses more quickly.
- It is now easier and quicker to switch between tabs.
- Default filters apply faster.
- The full path of the currently selected file displays at the bottom of the FTK window.

OTHER FEATURES

These features have been added as well:

- **Windows Event Logs:** FTK identifies and renders readable views of Windows event log (.evt) files.

- **Windows Shortcut Files:** FTK carves and renders .lnk files.
- FTK 2.0.2 now includes improved PNG carving.
- The install has been separated into three separate install components (FTK Package, Oracle and KFF Library) to make updates to each of these pieces easier in the future.
- Added the User Guide to the Installer and to the Help menu within the product.

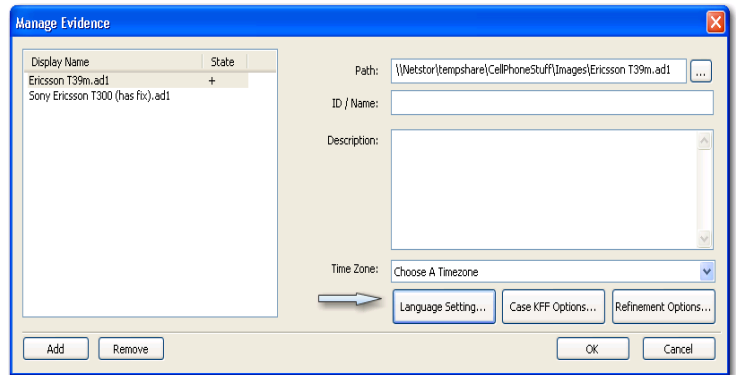
LANGUAGE SETTING SELECTION

FTK contains new functionality that allows the user to specify which language encoding to use when interpreting evidence. This user-selected language encoding is applied when FTK parses a binary file and presents a human-readable interpreted HTML view of that file.

By default, the language encoding used by FTK is the default encoding used by Windows on the computer on which FTK is running. A computer running the English-language version of Windows uses 'Windows ANSI 1252' language encoding, and FTK creates HTML interpreted views of evidence using that encoding. A computer running the Japanese-language version of Windows uses 'Windows ANSI 932' encoding, and FTK creates HTML interpreted views of evidence using that encoding.

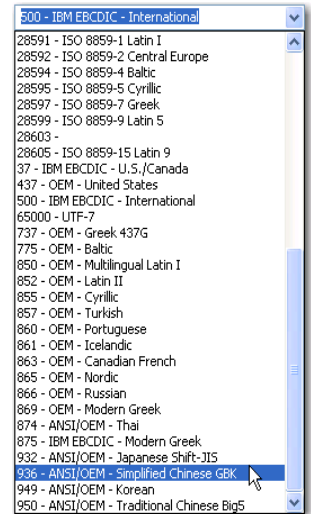
Use the Language Settings button in the Manage Evidence window to change the language encoding used by FTK to interpret the evidence as displayed in the following figure.

Figure 1-1. Manage Evidence Window with Language Selection Button



After browsing to the evidence you will add to the case, click *Language Setting* and select the appropriate code page from the drop-down list, as displayed in the following figure.

Figure 1-2. *Language Selection Drop-Down*



The selected language is the language used by FTK to create any human-readable interpreted HTML views of binary files.

EMAIL ARCHIVES

FTK creates interpreted HTML views for the following email archives:

- Outlook PST archives
- Outlook Express DBX archives
- Exchange Server EDB databases
- Email archives from Eudora, Thunderbird, Netscape mail, and other mail applications which use the mbox format.

WINDOWS SYSTEM FILES

FTK creates interpreted HTML views for the following Windows System Files:

- Recycle Bin (INFO2 and Vista Recycle bin files)
- Thumbnail archives (thumbs.db and thumbcache_nnn.db)

- EMF print spools (.spl)
- EFS Streams (\$EFS)
- Windows Event logs (.evt)
- Registry hive files (selected values from Sam, System, and Software files)

INTERNET AND CHAT FILES

FTK creates interpreted HTML views for the following types of internet and chat files:

- AOL History files (.arl)
- AOL Auto-complete Cache (.aut)
- AOL Address Book (.aby)
- AOL IM Buddy List (.bag)
- Netscape History (history.dat)
- Netscape Cookie index (cookies.txt)
- Netscape Form History (formhistory.dat)
- Netscape Address book (history.mab and abook.mab)
- Netscape Mail Folder cache (panacea.dat)
- Netscape Mail Databases (*.msf)
- Yahoo! Messenger Chat logs (*.dat)

RESOLVED ISSUES

The following lists the issues that have been resolved between the release of FTK 2.0 and FTK 2.0.2:

- AOL emails can now be exported with no errors.
- Attachments and parent email are now included with original email in bookmarks.
- Print Spool .spl files are being correctly categorized.
- Language Selector is now the same version on all of AccessData's shipping products.
- Selected items retain their selection after a refresh.
- Install now indicates the entire path for installation.
- The Disable Hyperlinks button has been redesigned for clarity.

-
- FTK no longer crashes on exit, as it would occasionally do before.
 - Mapped drives are now converted to UNC so that FTK will recognize the path and process evidence contained on a mapped drive.
 - .search-ms files and .rdf files are no longer listed in the Bad Extension category.
 - Ctrl+F search now works for non-English characters in UTF-8 encoded files.
 - KFF Alerts and Ignore numbers are now consistent when doing Additional Analysis.
 - FTK now processes cases where the computer name of the machine where the FTK Program is installed begins with a number or non-alphabetic character.
 - Zero length files no longer appear in the KFF Ignorable container.
 - Ability to change encoding in the Natural and Web view has been added.
 - Unnecessary database calls for refresh were eliminated.
 - Issues backing up multiple cases at the same time have been resolved.
 - Only checked graphics are included now in a report, instead of all graphics.
 - Processing begins more quickly when Additional Analysis is invoked.
 - Files added individually are now included when using the Actual Files filter.

RESOLVED CARVING ISSUES

The following issues with carving have been resolved with this release:

- Manual data carving and saving item as HTML had a sporadic hang, this issue has been fixed.
- Improved Metacarving on NTFS volumes.

LOCALIZATION AND NON-ENGLISH RESOLVED ISSUES

The following issues with non-English languages and characters have been resolved:

- Live search now finds non-ASCII characters.
- KFF search results for alert and ignore files can now be localized.
- Export word list now exports non-ASCII characters.
- Reports are now localized.

RESOLVED SEARCH ISSUES

The following issues have been resolved with Live and Indexed Searches:

- dtSearch results are now copied to the clipboard correctly.
- Indexed word list now includes non-ASCII characters.
- Sporadic hang when performing multiple live searches has been fixed.

KNOWN ISSUES

The following are known issues with FTK 2.0.2.

ADDITIONAL ANALYSIS ISSUES

The following must be performed during initial analysis and cannot be performed in Additional Analysis:

- Meta Carve
- Generate HTML File Listing

Also note, if indexing has been performed during pre-processing, indexing again with Additional Analysis causes the Total Hits column displays twice the number of actually available items that meet that hit criterion. The Index Search Results field still displays the correct available hits.

EXPORTING FILTERS

Filters with illegal Windows filename characters in their titles cannot be exported.

DTSEARCH FOR SYNONYMS

Typing an ampersand (&) does not enable synonym searching.

Workaround: Click *Options* in the Search Criteria section and select *Synonym* in the Search Options section.

CHANGED PASSWORD

If the user is unable to log into FTK because of a Windows password reset, the system credentials also need to be reset in the AccessData - Worker Monitor service to resynchronize the system password with FTK.

1. Right-click *My Computer*.
2. Select *Manage*.
3. In the Computer Management window expand *Services and Applications*.
4. Click on *Services* to display a list of running services.
5. Click on the AccessData - Worker Monitor service.
6. Click *Stop* to stop the service.
7. Agree to stop the AccessData - Database Monitor as well.
8. Right-click the stopped service and select *Properties*.
9. Click the *Log On* tab.
10. Select *This Account* and enter the domain log on information.
11. Click *OK*.
12. Restart AccessData - WorkerMonitor.
13. Restart AccessData - DatabaseMonitor.

YAHOO MESSENGER CHAT LOGS

FTK parses Yahoo Messenger Chat Logs showing the conversations between individuals, however the contents of the chat are not indexed in dtSearch* making the terms unfindable when running an Index Search

REPORT ISSUES

These following section list issues apply to reports and their outputs:

SELECTED BOOKMARK CONTENT

The Remember Selection option inside a bookmarked item, only puts its output into the report when the selection is smaller than 4,500–5,000 characters.

DUPLICATION OF LAST REPORT LINE

In the HTML version of a report, if a bookmark is listed in the last line of the first page, FTK reprints the same bookmark on the top of the subsequent page.

ILLEGAL FILENAME CHARACTER HANDLING

If a filename in a report contains illegal characters for a Windows filename, such as a file named for the subject line of an email, FTK replaces the illegal character with an underscore (_) character but leaves the filename the same in the report. The link to this filename, however, is dead and does not function.

INCLUDING NON-PRESENT FILE TYPES IN A REPORT

When generating a report, include desired file types. If a file type not present is chosen for inclusion in a report, FTK generates the report including all of the files in the case.

LARGE CASE SIZE REPORT GENERATION

When a PDF report length begins to approach 11,000 pages, the report fails to generate.

Workaround: Take information out of the report to make it smaller, or split the report into smaller reports.

Alternate Workaround: Use the HTML format for reporting instead of PDF for very large reports.

OUTPUT DISPLAY OF FILES

When HTML files are displayed in the FTK interface, they default to the Natural tab view in the File Content pane. When these files are output into a report they display in their unformatted form. This causes HTML files to be output in their raw HTML form instead of the interpreted form as they would display in a Web browser.

OTHER ISSUES

- FTK cannot import hashes from .csv files with Unicode anywhere in the path.
- FTK only runs on 32-bit systems.

-
- When importing a file containing hashes into the KFF, ensure that a blank line is inserted at the end of the last line to include the last line in the import.
 - When filtered text is viewed on a file that is not in the index, the viewer may slow down some other applications that are running. If this occurs, close FTK and restart the application.
 - There are performance issues with the QuickPicks feature.
 - On computers with the OS Environment variables for TMP and TEMP set to a different drive than where Windows is installed will result in the error message: “Local Oracle Unavailable.”

Workaround: (1) Change the system environment so that the Temp folder is on the same drive as Windows; or (2) Install the FTK Program to a folder on the drive where the Temp folder resides.

DEFAULT CASE FOLDER LOCATION

FTK currently defaults to a case folder of `C:\ftk2-data`. This can be changed to a location with more storage capacity. To change it, perform the following steps:

1. Click *Start > Run*
2. Enter `regedit`.
3. Click *OK*.
4. Open `HKEY_LOCAL_MACHINE\Software\AccessData\Products\SDS`
5. Double-click the `sp` value, change the directory to the new storage location.
6. Click *OK*.

Important: The new path must be in ASCII characters and cannot contain Unicode characters. This also applies to `TempDir`.

WARNING

If previous cases exist on the computer, they have to be moved to the new location or the cases will not function further. If the temp file directory is moved, any stored temp files must also be moved to the new temp folder.

If a UNC path or an invalid path is used for either the default case location or the temp directory, both keys will be reset to the default when FTK is launched.