

FORENSIC TOOLKIT® 2.1.0

Release Notes

The following sections present information on the new features, resolved issues, and known issues with the AccessData (AD) Forensic Toolkit (FTK) 2.1.0 release.

New Features

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

NEW USER INTERFACE FEATURES

- Users can use AD Network License Service (NLS) to get licenses for FTK sessions. Please refer to our website for more information about the NLS or to download it.
<http://www.accessdata.com/support.html>
- The UI layout now more closely resembles the FTK 1.x UI.
- dtSearch index hits can now display in Natural view as well as the filtered text view.
- Users can now specify a folder location for each case.
- Labels can now be used in the cases.
- While some options, like backup and restore, remain restricted to the Case Administrator, multiple users can now access the same case.
- A new role, Application Administrator, has been added.
- Application Administrator(s) can reset FTK user passwords.
- FTK now associates permissions for accessing evidence to the user running FTK rather than the services.
- Multiple images from the same folder can be added as evidence at the same time.
- In the advanced section of the AD Oracle 1.2 setup, the users can select the Oracle SYS password.
- Oracle Installer now supports multiple instances of Oracle.
- FTK now decrypts Office 2007 files.
- The user can now export selected files as an **.ad1** image.

- When exporting, the original directory structure can be recreated.
- Exporting is enhanced to allow the user to do the following:
 - Export files to .AD1 image.
 - Export whole-disk images.
- When exporting items, a summary file is created in the destination folder.
- Improved embedded OLE object handling.
- Encase .L01 image files are now supported.
- Users can now process and review Lotus Notes (NSF) files and encrypted data.
- Fuzzy Hashing has been added.
- When exporting files, users can now select to append the extension when it is bad or missing.
- Steganography support has been added for processing newly-added files, and for additional analysis.
- The KFF Library has been updated with 45 million new hashes.
- In the case folder there is a log file created called **ftkWorker.infolog.txt**. It contains the options selected when the case was processed.

NEW OPERATING SYSTEM SUPPORT

FTK now operates on the following additional operating systems:

- Microsoft* Windows* XP* x64
- Microsoft Windows Server 2003* x64
- Microsoft Windows Vista* x32 and x64
- Microsoft Windows Server 2008* x32 and x64

NEW REPORT OUTPUT OPTIONS

FTK can now generate reports in the following additional formats:

- .xml
- .rtf
- .wml
- .docx

- .odf
- Selected Text now displays in a report.
- The Extension list is no longer the default list.
- All Graphics in the case is no longer the default report setting.

NEW FILE SYSTEM SUPPORT

FTK now supports for the following additional file systems:

- UFS file system
- JFS file system
- LVM2 file system

NEW DECRYPTION TECHNOLOGIES

FTK now supports the following decryption technologies:

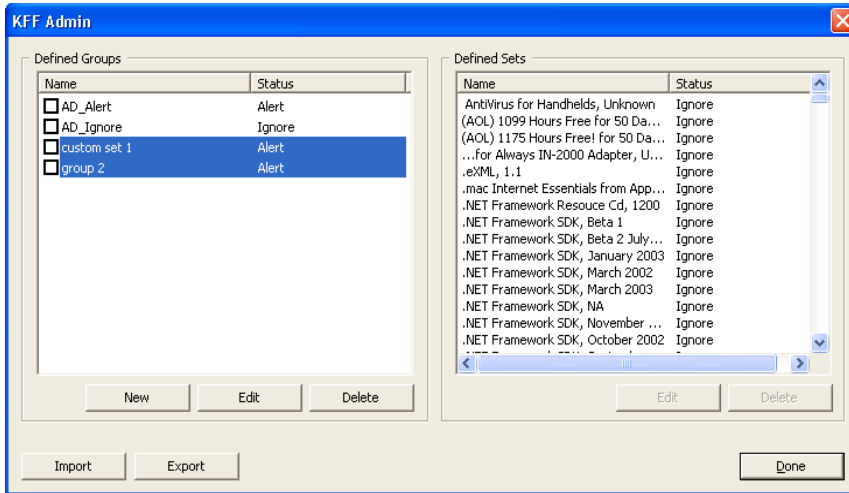
- Utimaco (SafeGuard)
- Credant
- SafeBoot

NEW KFF INFORMATION

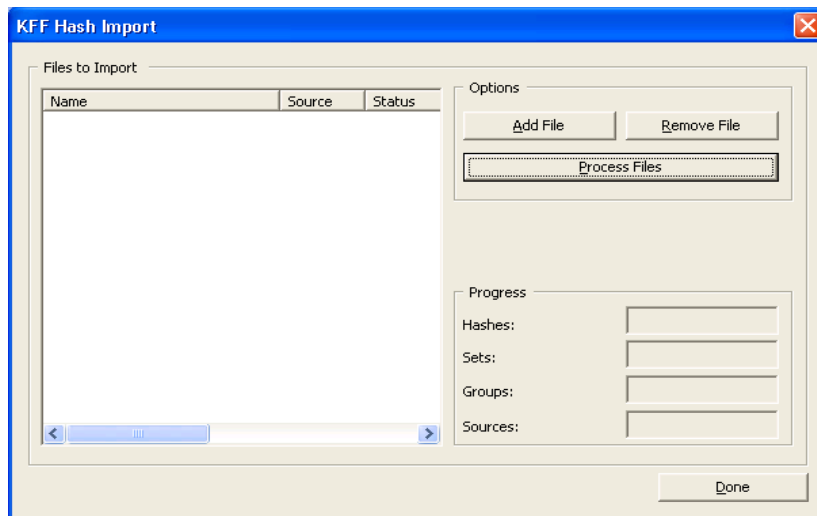
To save your custom groups:

Select *Tools->KFF->Manage*

In the defined Groups section, highlight the custom groups you want to export, and click the “Export” button. (Note: If your custom defined groups do not contain all you custom sets, you will need to create a new group that contains the sets you want to save).

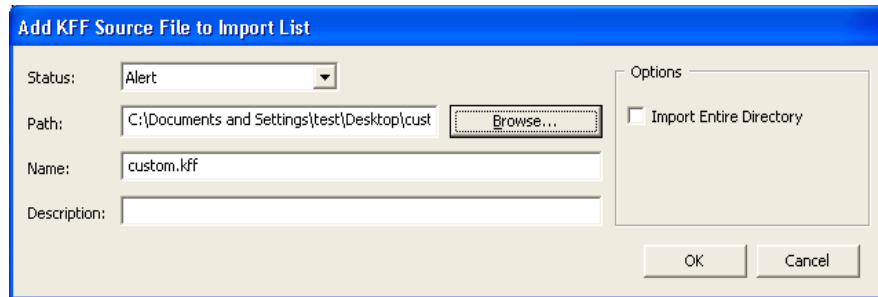


1. Enter the information necessary to save the file.
2. To Import the groups into the new KFF:
3. In an open case, select Tools->KFF->Manage
4. On the KFF admin dialog, click on the “Import” button
5. On the KFF hash import dialog, click on the “Add File” button.

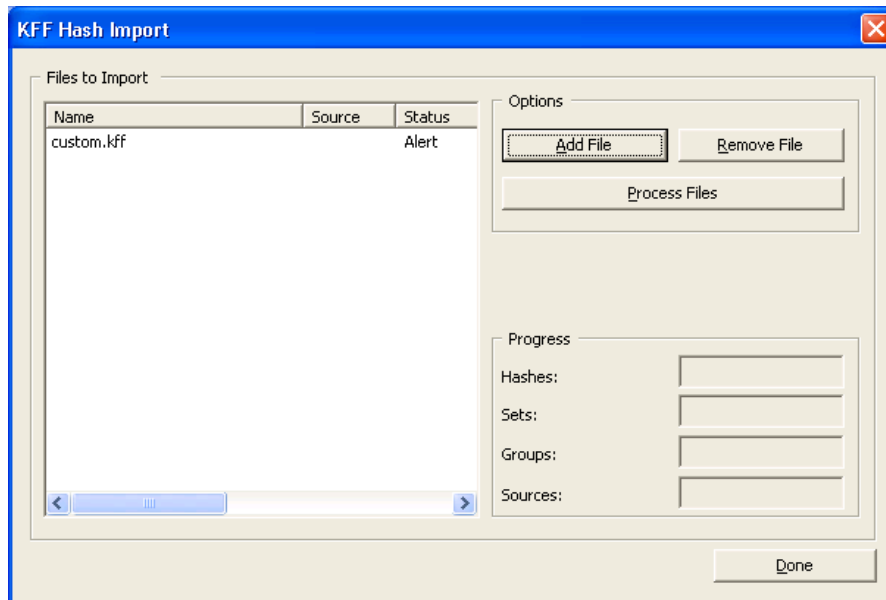


6. On the Add KFF Source File to Import List dialog, click *Browse* and navigate to the file you exported containing the custom KFF groups.

7. After you selected it, and the dialog is automatically populated,click **OK**.



8. Back in the KFF Hash Import dialog, click on the “Process Files” dialog, and then “Done” once the files are processed.



9. Click “Done” in the KFF Admin Dialog.

MODIFICATIONS AND ENHANCEMENTS

USER INTERFACE

Installation and the User Interface have been improved in the following ways:

- When installing Oracle, the installer now correctly lists available drives for the Oracle Home.
- FTK2.1 can now be installed on a Turkish OS.
- Flag Duplicates and HTML File Listing are now available in Additional Analysis.
- Registry Viewer Wordlist export now works correctly.
- Localized versions now manage and display the Column Settings dialog correctly.
- Manage Evidence dialogs in the German version are now corrected.
- Manage KFF dialogs in localized versions are now corrected.
- Copy Special dialogs in localized versions are now corrected.
- dtSearch dialog buttons in Additional Analysis have been corrected.
- FTK2 Logging is improved.
- Exported files retain MAC times on NTFS volumes.
- Restore – when restoring a case, the user can choose where the case files will be stored.
- Expand Compound Files is off by default. This means items inside archives will not be processed. To process the contents of archives, check *Expand Compound Files* in the Refinement Options or Detailed Options dialog of the New Case Wizard.
- The Search results pane no longer puts special characters around the search term:
<|word|>

PERFORMANCE IMPROVEMENTS

FTK 2.1.0 improved in performance in the following ways:

- Improved processing on multi core computers
- Quickly enumerates evidence items (FDS) before further processing
- Improved KFF processing
- Improved speed of dtSearch indexing

- Improved speed of QuickPicks queries
- Improved response when switching between tabs
- Improved UI response in trees and lists
- Improved speed of opening the “Overview” tab
- Added multi-thread database access to item list, counts, categories, status, and email, improving response times for those items.
- Reduced time required to expand large folders in the Explore tree.

KNOWN ISSUES

The following known issues exist with this current release:

Important: Make sure your Temporary File Path is set to a drive that has enough free space. Temporary files may require free space equal to the evidence image size. This path is set in the preferences menu in the Case Management window under Tools.

- FTK 2.1 does not coexist with previous versions of FTK 2. Users could consider setting up a dual-boot system if they need to run multiple versions of FTK 2.
- The @ symbol is no longer indexed. To search for an email address in an index search, enclose it in quotation marks, for example, “support@accessdata.com”.
- In Search, a hyphen (dash) is now treated as a space. To search for hyphenated words/phrases, use quotes at the beginning and end.
- Wait for Additional Analysis processing that requires indexing, such as indexing, data carving (with indexing turned on), decrypting (with indexing turned on), to complete before attempting to access the index. Running an index search while FTK is merging new files into the index may prevent the new data from being merged correctly.
- If you get a crash error while processing, that contains a dialog with an OK button, you can click OK, and the worker should resume processing.
- If the FTK2.1 system has .NET 1.1 installed, reports generated in the following formats result in an error message:
 - RTF
 - WML
 - DOCX
 - ODF

The following workarounds are available:

- Remove/uninstall .net framework 1.1 from the machine. FTK2 only needs .net 2.0 for ftk-2 to work and since 1.1 is out dated already, it should not have any issues removing 1.1.
- If the user chooses not to remove/uninstall .net framework 1.1 (because they need it), they can install "Microsoft Visual J# .Net Redistributable Package 1.1" on their system. This will solve the report generation problem.
- When using a Windows Vista or 2008 class machine and the NLS is installed on the same machine as the client, the client must not be pointed to the local host/loopback IP (127.0.0.1 or localhost) address of the machine. Instead, point to the network IP address.
- If your Worker is set to go into a hibernation, sleep, or suspend mode after a specified period of inactivity, and you leave the Worker processing, when the inactivity limit is reached, the hibernation mode will cause the Worker to lose connection with the remote Oracle DB. When the Worker is brought out of hibernation, processing will resume, and no data will be lost. However, the time that it was assumed that processing was taking place but was not will be lost.

To avoid this, set the Worker not to hibernate, sleep or suspend.

- Version Manager must be Run as Admin in Vista.
- Mobile Phone Examiner does not run in a 64-bit environment.
- FTK cannot be installed in a folder named with a right-to-left-reading language that uses unicode characters.
- When uninstalling FTK2.1, if the KFF is installed, it will be removed without prompting the user.
- FTK2.1 does not parse metadata from MS Office 2007 documents.
- The scroll bar on the file content pane is not adjusting for the size of the graphic being displayed.
- When processing a .cue file with multiple sessions (for a CD or DVD image), only the last session can be viewed correctly. The last session contains all information from the disc image, so previous sessions are irrelevant.
- When creating a report in .RTF format with export links - these links will not work when clicked-on in Microsoft Word
- Workaround: Open the .RTF in a different application.
- When a user changes the Network Security Device location, if the name and/or port are incorrect, the user will not receive notification.
- FTK cannot use a network dongle for local licenses. You must use the NLS for all network dongles. This is working as designed.

- If a case is locked, the Manage DB Sessions dialog can be used to kill the session and unlock the case. In the Case Management UI, click *Database > Session Management*.
- You can't delete evidence from a restored case that was created by a different user.
- FTK cannot decrypt Yahoo IM conversations if they were moved to another directory and then added as evidence without being renamed to the real account name.
- While viewing files in FTK, if you get a message that IE was trying to close the file, click No, or FTK will close.
- If booting a computer with a CodeMeter device in the USB port prevents the computer from booting properly, change the boot order in the BIOS or remove the CodeMeter device until the computer has booted.
- After running a search, if you create a bookmark containing data from the metadata section of the file in the index search view, you will not be able to see the selection in the bookmark tab. The metadata is only viewable in the search tab.

COMMENTS?

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