
FTK Imager 2.9 Release Notes

These release notes apply to AccessData FTK Imager 2.9

IMPORTANT INFORMATION

- If the machine running imager has an active internet connection and you are viewing HTML from the systems cache, there is a potential risk associated with Microsoft Security Bulletin MS-09-054.

AccessData recommends that, wherever possible, users not have an active internet connection while Imager is running. In addition, please be aware that viewing HTML content in the Imager preview pane when connected to the internet has potential risk.

NEW AND IMPROVED

- Export to Logical Image (AD1) and Add to Custom Content Image (AD1) now allow the user to select and export files owned by particular SID(s), or add them to the image. (17456)
- A list of usernames and their SIDs allows one or more to be selected. The export then contains only those files owned by the selected SIDs/Users.
- If the desired SID does not appear on the list, click *Add* to manually enter one. This allows a user to create an image containing files owned by the SID of a domain account. Copy and paste the SID from another location, or type it in manually. User-entered SID(s)/Name(s) persist as long as Imager is open. (17900)

BUG FIXES

- Fixed a problem where, if a user chooses Add to Custom Content Image (AD1), or Export Logical Image (AD1), if a file in the folder being exported is locked (in use by another process or program), the export would appear successful, but the locked file would have a file size of 0 bytes. Imager exports an empty file. Now an error message pops up showing the problem and the name of the file that is in use. (17928)



The process cannot access the file because it is being used by another process. (32). Filename = "C:\pagefile.sys"

FTK Imager 2.8 Release Notes

These release notes apply to AccessData FTK Imager 2.8

NEW AND IMPROVED

- FTK Imager now has the ability to encrypt images it creates or exports. Full disk and partition images can be exported to E01, S01, 001 (RAW/DD), and Custom Content images (AD1) can also be created.

All these image types can be encrypted with AD Encryption that uses AES-256 encryption.

FIXES

- Imager now pops up a warning before overwriting a previous memory capture.
- Obtain Protected Files in Windows 7 OS now works correctly.

COMMENTS?

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

FTK Imager 2.7 Release Notes

These release notes apply to AccessData FTK Imager 2.7

NEW AND IMPROVED

- FTK Imager can now capture RAM contents on 32-bit and 64-bit computers. Previously, only 32-bit RAM capture was supported.
- RAM Capture files are now saved as **.MEM** files for better compatibility with FTK.

COMMENTS?

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

AccessData FTK Imager 2.6.1

Release Notes

These Release Notes cover fixes for AccessData FTK Imager 2.6.1.

FIXES

- Fixed a hang/error when trying to create an image of certain CDs.
- Corrected a problem that caused the application to fail to start. The related error message was: “The application failed to initialize properly (0xc0150002). Click on OK to terminate the application.”
- Fixed an issue where some characters in the filename of an HFS image caused an error when attempting to export the file.
- Fixed a crash that could occur when trying to Image a defective drive.

KNOWN ISSUES

- The new RAM Acquisition feature is available only for 32-bit operating systems.

COMMENTS?

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

AccessData FTK Imager 2.6

Release Notes

These Release Notes cover new features, enhancements, and known issues for AccessData FTK Imager 2.6.

IMPROVEMENTS

- FTK Imager now supports the latest E01 image format with SHA1 hashing.
- FTK Imager can now export folders and files from image files that contain “:” and “\” in the name.
- Logical Partition acquisition now includes sectors at the end of the partition that lie outside the file system boundary. This data was previously gathered only during Physical Partition acquisition.
- When verifying images, Imager now reports the location (when possible) of any corrupted data in the image.
- FTK Imager now contains the latest ISO Buster support for HD DVD and Blu-Ray disks.
- FTK Imager now has improved support for LVM 2 partitions within disk images.
- FTK Imager has added new file system support for JFS/UFS support.
- FTK Imager now supports RAM Acquisition. See Additional Information below for instructions.

FIXES

- FTK Imager 2.5.x images can now be successfully added to EnCase using drag-and-drop.

KNOWN ISSUES

- MetaCarve (Deep Scan) menu item and button do not work. This feature is not available.

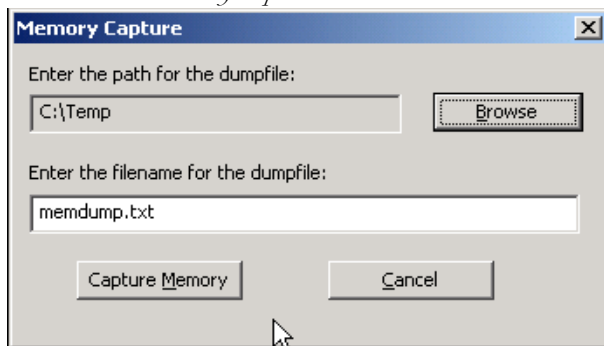
ADDITIONAL INFORMATION

FTK Imager now supports RAM Acquisition. Capture the contents of the local machine's RAM to a file in a user-specified location. A summary file containing information about what was captured is also created and stored in the same location as the Memory Capture. This feature requires Imager to be run with administrator rights.

Note: RAM acquisitions are not currently supported on operating systems that require signed drivers.

To capture the contents of RAM on the local machine to a dumpfile, do the following:

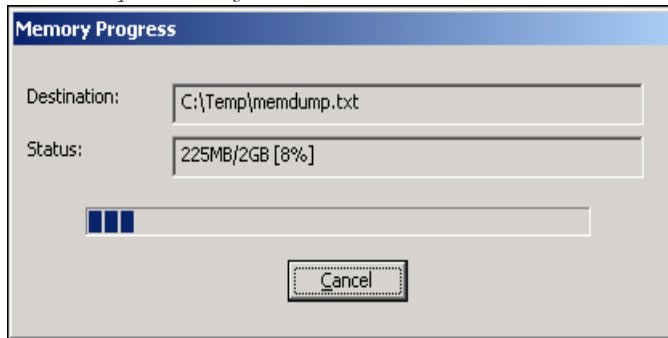
1. Click *File > Memory Capture*.



2. Enter a path for the dumpfile
OR
Click *Browse* to select a location.
3. Enter a name for the dumpfile
OR

Accept the default name, memdump.txt.

4. Click *Capture Memory*.



5. Wait while the memory capture progresses. If there is an existing dumpfile in the same location by the same name, you will receive an error saying the driver could not be started. Delete or move the file, then shut down and restart Imager to create a new dump file.
6. If you wish to abandon the RAM dump before it is complete, click *Cancel*.
7. When the RAM dump is complete, click *Close*. The Memory Capture dialog closes, and the RAM dump file is available for processing in AccessData Enterprise.

COMMENTS?

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

FTK Imager 2.5.5 Release Notes

INTRODUCTION

This document lists important information necessary for the use of AD FTK Imager 2.5.5.

FIXES

The following known issues have been fixed with this release of AD FTK Imager 2.5.5:

- • Compatibility issues with E01 files and EnCase have been resolved.
- *.E01 images created with FTK Imager would not load properly in EnCase if dragged and dropped. When dragging and dropping the image into EnCase an error would result: "Error: Error in "Header": String cannot be longer than 12 characters". This issue has been fixed.

COMMENTS?

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

FTK Imager 2.5.4 Release Notes

These release notes apply to AccessData FTK Imager 2.5.4.

NEW FEATURES

This version contains these new features:

AUTO MOUNT

You can now choose to add as evidence all devices that are accessible to your machine. You can also remove any or all listed devices from your evidence tree.

AD1 IMAGE VERIFICATION

Imager can now verify AD1 image files.

Note: Always check your logs after verification is finished.

EXPORT AD1 DIRECTORY

You can now export a directory listing from an existing AD1 image.

UNSEGMENTED E01 FILES

Imager can now create and read large unsegmented E01 files.

MODIFICATIONS AND ENHANCEMENTS

MFT RECORD OFFSETS

- Imager now shows the offsets of \$MFT records next to the record number.

WILDCARD ABILITIES

- You can now use both (*) and (?) for wildcard searching. Use (*) for searching an undefined number of characters, or (?) for searching a single character. For example, if you want to create an image of a folder that contains all the files that begin with the letter d, you type in **d*** to find them. If instead you want to search for all filenames that contain the words run or ran, you type **r?n** to find both in one search. You can then make an image of the files located.

Note: “Wildcarding Options” has become “Wild Card Options,” and “Match Parent Directories” has become “Match All Occurrences.”

IMPROVED IMAGE SUMMARY

- The image creation start and finish date and time are now found in the Image Summary.
- The image verification start and end times are also now found in the Image Summary.
- Find the Image Summary information in:
imagepath\imagefolder\imagename.imagetype.txt.

DOMAIN USER FILES

- When a user logs onto a domain instead of the local workstation, his password is not stored in the local SAM file, but in the **ntds.dit** file on the Active Directory* domain controller. When Imager is run on an Active Directory domain controller, the Obtain Protected Files function now also attempts to capture the `\Windows\ntds\ntds.dit`. This allows the investigator to obtain logon information without shutting down the domain controller system.

PATH INFORMATION DISPLAY

The full path of files now displays both when user clicks on a file in the file list, and when the user clicks on a file in the evidence tree.

DEFAULT IMAGE SEGMENT SIZE

Default Image Segment size has changed from 650MB to 1500MB.

BUG FIXES

- **Image.txt** file now contains information about the version of Imager used to create the image.
- Fixed the error “Failure: The system cannot find the file specified. (2)OO” when creating AD1 custom content images.
- Imager successfully images filenames/pathnames that exceed 260 characters.
- All CD/DVD sessions now display in file listing. Naming convention is changed from **.iso.csv** to **.cue.csv**.
- Export Directory Listing is now available for AD1 images.
- You can now edit the “Evidence Item Information” for an already defined AD1 image in Imager.
- Imaging multiple diskettes now completes successfully.

COMMENTS?

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