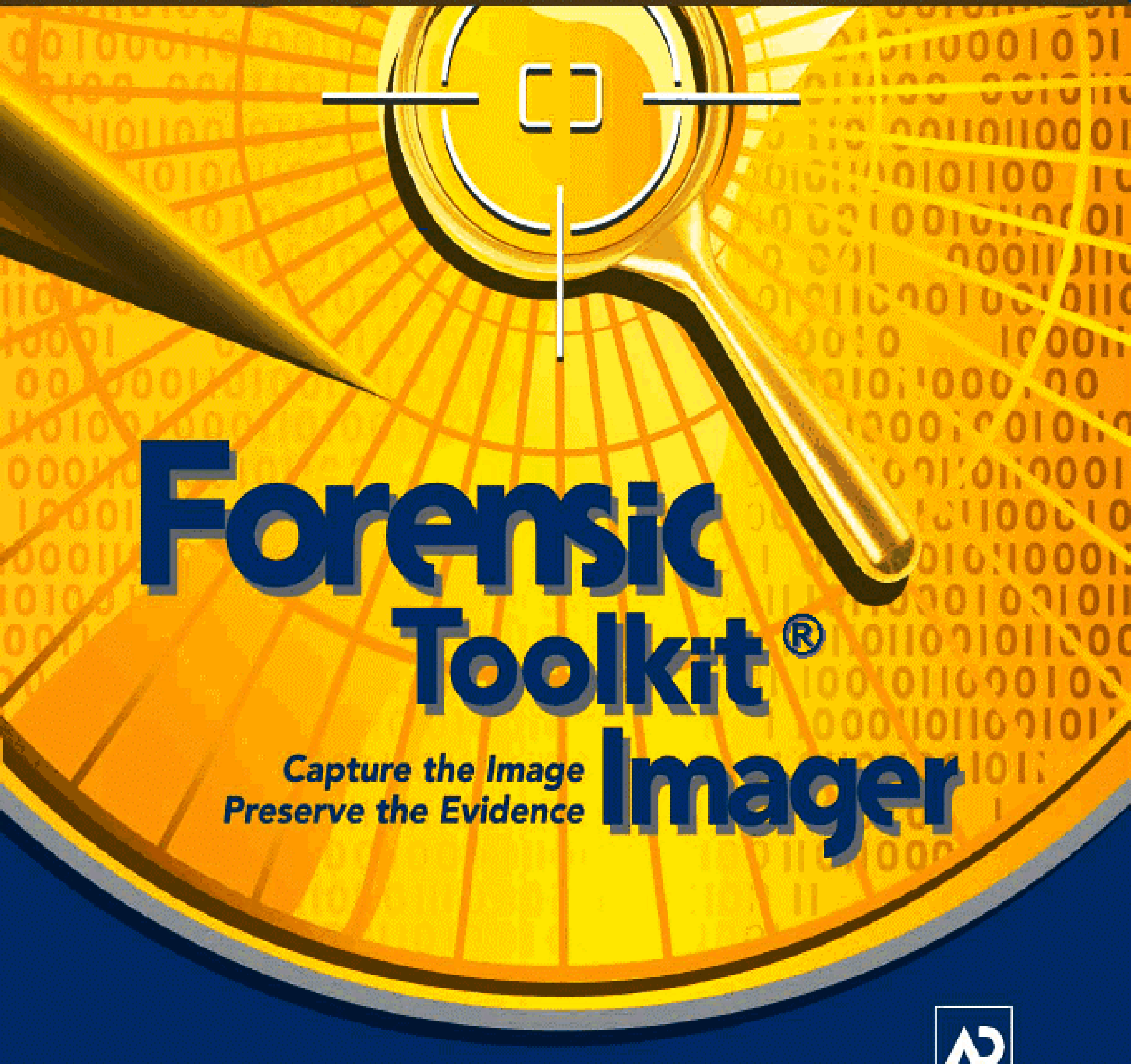
USER GUIDE

Find, Organize, & Analyze Computer Evidence



Forensic Toolkit® Imager

Capture the Image
Preserve the Evidence

AccessData

AccessData FTK Imager

LEGAL INFORMATION

AccessData Corp. makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, AccessData Corp. reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, AccessData Corp. makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, AccessData Corp. reserves the right to make changes to any and all parts of AccessData software, at any time, without any obligation to notify any person or entity of such changes.

You may not export or re-export this product in violation of any applicable laws or regulations including, without limitation, U.S. export regulations or the laws of the country in which you reside.

AccessData Corp.
384 South 400 West
Suite 200
Lindon, Utah 84042
U.S.A.

www.accessdata.com

AccessData Trademarks

AccessData® is a registered trademark of AccessData Corp.

Distributed Network Attack® is a registered trademark of AccessData Corp.

DNA® is a registered trademark of AccessData Corp.

Forensic Toolkit® is a registered trademark of AccessData Corp.

FTK® is a registered trademark of AccessData Corp.

Password Recovery Toolkit® is a registered trademark of AccessData Corp.

PRTK® is a registered trademark of AccessData Corp.

Registry Viewer® is a registered trademark of AccessData Corp.

Documentation Conventions

In AccessData documentation, a greater-than symbol (>) is used to separate actions within a step. Where an entry must be typed in using the keyboard, the variable data is set apart using [*variable_data*] format.

A trademark symbol (®, ™, etc.) denotes an AccessData trademark. All third-party trademarks and copyrights are the property of the trademark and copyright holders. AccessData claims no responsibility for the function or performance of third-party items.

We value all feedback from our customers. For technical and customer support issues, please email us at **support@accessdata.com**. For documentation issues, please email us at **documentation@accessdata.com**.

Registration

The AccessData product registration is tracked by the USB security device included with your purchase, and is managed by AccessData. Registration is done at AccessData, and when you purchase your product, no additional action on your part is necessary for initial registration.

SUBSCRIPTIONS

AccessData provides an annual licensing subscription with all new product purchases. The subscription allows you to download and install the latest product releases for your licensed products. Following the initial licensing period, a subscription renewal is required for updating your products. You can renew your subscriptions through your AccessData Sales Representative.

Use LicenseManager to view your current registration information, to check for product updates and to download the latest product versions, where they are available for download. You can also visit our website, www.accessdata.com anytime to find the latest releases of our products.

For more information, see Managing Licenses in your product manual or on the AccessData website.

ACCESSDATA CONTACT INFORMATION

MAILING ADDRESS AND GENERAL PHONE NUMBERS

You can contact AccessData in the following ways:

TABLE Front-1 Mailing Address, Hours, and Department Phone Numbers

Corporate Headquarters	AccessData Corp. 384 South 400 West Suite 200 Lindon, UT 84042 USA **Voice**: 801-377-5410 **Fax**: 801-377-5426
General Corporate Hours:	Monday through Friday, 8:00 AM – 5:00 PM (MST) AccessData is closed on US Federal Holidays
State and Local Law Enforcement Sales	**Voice**: 801-377-5410, option 1 **Fax**: 801-765-4370 **Email**: Sales@AccessData.com
Federal Sales	**Voice**: 800-574-5199, option 2 **Fax**: 801-765-4370) **Email**: Sales@AccessData.com

TABLE Front-1 Mailing Address, Hours, and Department Phone Numbers

Corporate Sales	**Voice**: 801-377-5410, option 3 **Fax**: 801-765-4370 **Email**: Sales@AccessData.com
Training	**Voice**: 801-377-5410, option 6 **Fax**: 801-765-4370 **Email**: Training@AccessData.com
Accounting	**Voice**: 801-377-5410, option 4

TECHNICAL SUPPORT

You can contact AccessData Customer and Technical Support in the following ways:

TABLE Front-2 AccessData Customer & Technical Support Contact Information

Customer Service Hours:	Monday through Friday, 7:00 AM – 6:00 PM (MST)
Customer/Technical Support Free technical support is available on all AccessData products.	**Voice**: 801-377-5410, option 5 **Voice**: 800-658-5199 (Toll-free North America) **Email**: Support@AccessData.com **Website**: http://www.AccessData.com/Support

The Support website allows access to Discussion Forums, Downloads, Previous Releases, our Knowledgebase, a way to submit and track your "trouble tickets", and in-depth contact information.

Note: All support inquiries are typically answered within one business day. If there is an urgent need for support, contact AccessData via phone during normal business hours.

DOCUMENTATION

Please e-mail any typos, inaccuracies, or other problems you find with the documentation to:
documentation@accessdata.com

Table of Contents

Chapter 1 Introduction and Installation of FTK Imager

FTK IMAGER

FTK® Imager is a data preview and imaging tool that lets you quickly assess electronic evidence to determine if further analysis with AccessData® Forensic Toolkit® (FTK) is warranted. FTK Imager can also create perfect copies (forensic images) of computer data without making changes to the original evidence. With FTK Imager, you can:

- Preview files and folders on local hard drives, network drives, floppy diskettes, Zip disks, CDs, and DVDs
- Create forensic images of local hard drives, floppy diskettes, Zip disks, CDs, and DVDs, entire folders, or individual files from various places within the media.
- Preview the contents of forensic images stored on the local machine or on a network drive
- Export files and folders from forensic images.

  Note: This feature comes in handy if your OS fails, but the drive still spins. Image your drive using a write-blocker, and export your data, photos, etc.
- Generate hash reports for regular files and disk images (including files inside disk images)

Important: When using FTK Imager to create a forensic image of a hard drive, be sure you are using a hardware-based write-blocking device. This ensures that your operating system does not alter the hard drive when you attach it to your computer.

FTK Imager is a data acquisition tool that can be used to quickly preview evidence and, if the evidence warrants further investigation, create a forensically sound image of the media.

To prevent accidental or intentional manipulation of the original evidence, FTK Imager makes a bit-for-bit duplicate image of the media. The forensic image is identical in every way to the original, including file slack and unallocated space or drive free space.

When you acquire computer evidence, you can use FTK Imager to create an image of the source drives or files. FTK Imager can also create a hash of the original image that you can later use as a benchmark to prove the integrity of your case evidence. A hash generated by FTK Imager can be used to verify that the image hash and the drive hash match after the image is created.

Two hash functions are available in FTK Imager: Message Digest 5 (MD5) and Secure Hash Algorithm (SHA-1). After you create an image of the data, you can then use AccessData Forensic Toolkit (FTK) to perform a complete and thorough forensic examination and create a report of your findings.

INSTALLING FTK IMAGER

FTK Imager can be installed to the computer where it will be used, or it can be run from a portable device such as a USB thumb drive on a machine in the field, so there is no need to install it on a suspect's computer.

INSTALLING LOCALLY

Install FTK Imager to a local hard drive when you intend to attach hardware-containing evidence to that computer for previewing and imaging evidence.

To install FTK Imager, do the following:

1. Browse to the FTK Imager setup file, either from an installation disc, or from the saved file downloaded from http://www.accessdata.com/downloads.html.
2. Under Utilities, look for FTK Imager. Click *Download* to download the latest released version.
3. Click *Save File.*
4. Browse to the location where you wish to save the install file, and click *Save.*
5. When the download is complete, browse to the location where it was saved.
6. Execute the setup file by double-clicking it.

7. Click *Run*.
8. Click *Next* to continue the installation.
9. Read and accept the License Agreement, then click *Next.*
10. Accept the default installation location, or browse to a different location, then click *Next*.
11. Mark *Run the FTK Imager* box to force Imager to run immediately after the install is complete.
12. Click *Finish* to complete the installation and close the wizard.

INSTALLING TO A PORTABLE DEVICE

There are two ways to use Imager on a portable device. One way is to copy the FTK Imager Lite files directly to the device, avoiding installing to a local computer first. The other is to run the installation on a local computer, then copy the FTK Imager folder from the [*Drive*]:\Program Files\AccessData\FTK Imager folder to the thumb drive or other portable device.

The two main differences you will notice between these methods are that a) the FTK Imager Lite program has fewer files (only the essentials), and b) the FTK Imager Lite program is not always as current as the latest full release of the product. This means you may not have a full feature set if you choose to copy the Lite file set instead of downloading and installing the latest version and copying all of those files to your portable media.

Once the FTK Imager program files are saved to the portable media, that media can be connected to any computer running a Windows OS, and the program can be executed from the portable media device.

With either method, you will need to make a target drive available for saving the imaged data.

RUNNING FTK IMAGER

FTK Imager can be run in a variety of ways:

- Double-click on the desktop icon .
- Execute the FTK Imager.exe file from a thumb drive.
- Click *Start* > *Run* > *Browse.* Browse to and select FTK Imager.exe from the location it was installed to, and add a command line switch as discussed below.

COMMAND LINE OPTIONS

FTK Imager supports three command line options:

- /CreateDirListing= creates a directory listing file in the folder where FTK Imager.exe is run from.
- /VerifyImage= verifies an image when you specify the image path and filename
- /EnableDebugLog= enables logging to the FTKImageDebug.log file created in the folder you run FTK Imager.exe from.

Note: If you fail to specify an image when using the /CreateDirListing= or /VerifyImage= options, an error message appears indicating no image was found.

To use these options, close FTK Imager, then from the Windows Start Menu, click *Run*. In the Run text box, browse to the path and folder containing FTK Imager.exe, then click *Open*. At the end of the resulting text line, add one space before the option you wish to use, then click *OK*.

Chapter 2 Using FTK Imager

FTK IMAGER INTERFACE

The FTK Imager interface window is divided into several panes: the Evidence Tree, File List, Properties, Hex Value Interpreter, Custom Content Sources, and the Viewer. All the panes (except the Viewer) can be undocked from the program window and repositioned on your screen. The Menu and Button tool bars can also be undocked.

To undock a pane or tool bar, select it and click and drag its title bar to the desired location.

To re-dock the pane, move the pane inside the FTK Imager window until an outline shape snaps into place in the desired position, then release the pane.

To return all panes to their original positions, select *View > Reset Docked Windows.*

MENU BAR

Use the menu bar to access all the features of FTK Imager. To show or hide the menu bar, click *View > Menu Bar.* You can also right-click the menu bar to access the menu.

FILE MENU

The File menu provides access to all the features you can use from the Toolbar. See "ToolBar" on page 6

View Menu

The View menu allows you to customize the appearance of FTK Imager, including showing or hiding panes and control bars.

Mode Menu

The Mode menu lets you select the preview mode of the Viewer. Finally, the Help menu gives you access to help and information about FTK Imager.

Help Menu

The Help menu provides access to the FTK Imager User Guide, and to information about the program version and so forth.

ToolBar

The Toolbar contains all the tools, or features, that can be accessed from the File menu, except Exit. The following table provides basic information on each feature.

TABLE 2-1 FTK Imager Toolbar Components

Button	Description
	Add Evidence Item
	Add All Attached Devices
	Remvoe Evidence Item
	Remove All Evidence Items
	Create Disk Image
	Export Disk Image
	Export Logical Image (AD1)
	Add to Custom Content Image (AD1)

TABLE 2-1 FTK Imager Toolbar Components

Button	Description
	Create Custom Content Image (AD1)
	Verify Drive/Image
	Capture Memory
	MetaCarve (Deep Scan)
	Obtain Protected Files
	Detect EFS Encryption
	Export Files
	Export File Hash List
DIR	Export Directory Listing

VIEW PANES

There are several basic view panes in FTK Imager. They are described here.

EVIDENCE TREE

The Evidence Tree (upper-left pane) displays added evidence items in a hierarchical tree. At the root of the tree are the selected evidence sources. Listed below each source are the folders and files it contains.

Click the plus sign next to a source or folder to expand the view to display its subfolders. Click the minus sign next to an expanded source or folder to hide its contents.

When you select an object in the Evidence Tree, its contents are displayed in the File List. The properties of the selected object, such as object type, location on the storage media, and size, are displayed in the Properties pane. Any data contained in the selected object is displayed in the Viewer pane.

File List

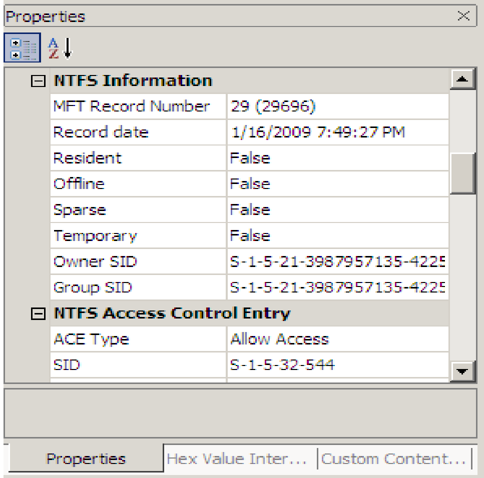
The File List shows the files and folders contained in whichever item is currently selected in the Evidence Tree. It changes as your selection changes.

Combination Pane

FTK Imager's lower-left pane has three tabs: Properties, Hex Value Interpreter, and Custom Content Sources. Each is described here.

Properties

The Properties tab displays a variety of information about the object currently selected in the Evidence Tree or File List.

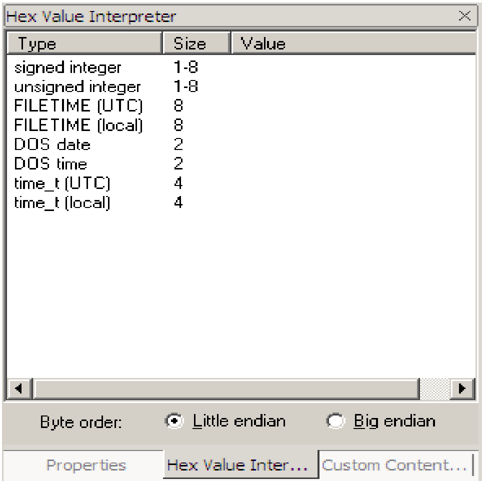


NTFS Information	
MFT Record Number	29 (29696)
Record date	1/16/2009 7:49:27 PM
Resident	False
Offline	False
Sparse	False
Temporary	False
Owner SID	S-1-5-21-3987957135-4225
Group SID	S-1-5-21-3987957135-4225
NTFS Access Control Entry	
ACE Type	Allow Access
SID	S-1-5-32-544

Properties include information such as object type, size, location on the storage media, flags, and timestamps.

HEX VALUE INTERPRETER

The Hex Value Interpreter tab converts hexadecimal values selected in the Viewer into decimal integers and possible time and date values.



Hex Value Interpreter

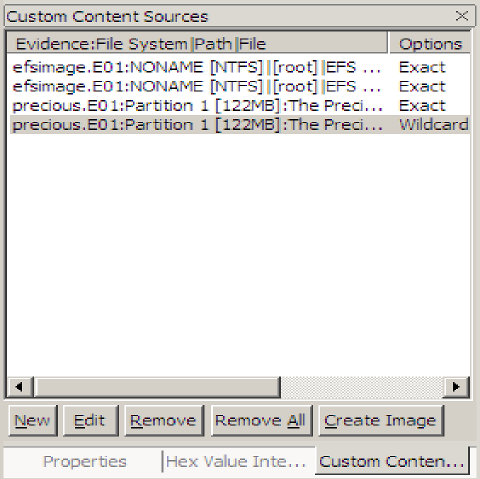
Type	Size	Value
signed integer	1-8	
unsigned integer	1-8	
FILETIME (UTC)	8	
FILETIME (local)	8	
DOS date	2	
DOS time	2	
time_t (UTC)	4	
time_t (local)	4	

Byte order: ● Little endian ○ Big endian

To convert hexadecimal values, highlight one to eight adjacent bytes of hexadecimal code in the Viewer. A variety of possible interpretations of the selected code are automatically displayed in the Hex Value Interpreter. This feature is most useful if you are familiar with the internal code structure of different file types and know exactly where to look for specific data patterns or time and date information.

Custom Content Sources

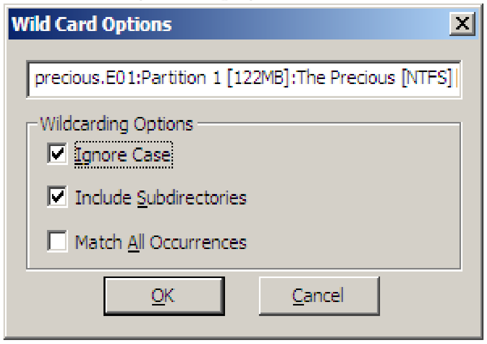
Each time you add an item to be included in a Custom Content image, it is listed here.



Custom Content Sources

Evidence:File System|Path|File	Options
efsimage.E01:NONAME [NTFS]|[root]|EFS ...	Exact
efsimage.E01:NONAME [NTFS]|[root]|EFS ...	Exact
precious.E01:Partition 1 [122MB]:The Preci...	Exact
precious.E01:Partition 1 [122MB]:The Preci...	Wildcard

You can add, edit, remove one or all sources, and create the image from here. Clicking *Edit* opens the Wild Card Options dialog. For more information, see “Creating Custom Content Images” on page 22.



Wild Card Options

precious.E01:Partition 1 [122MB]:The Precious [NTFS]

Wildcarding Options

☑ Ignore Case

☑ Include Subdirectories

☐ Match All Occurrences

Viewer

The Viewer shows a hex data view of the currently selected file. The content can be scrolled through so you can see the entire file content. In addition, with the Combo Pane Hex Value Interpreter open, hex interpretation of text selected in the Viewer pane can be viewed simultaneously.

PREVIEWING EVIDENCE

Evidence items can be previewed prior to deciding what should be included in an image.

Important: If the machine running imager has an active internet connection and you are using Imager to preview 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.

PREVIEW MODES

FTK Imager offers three modes for previewing electronic data: **Automatic mode, Text mode,** and **Hex mode.** These modes are selectable from the Mode menu, or from the Toolbar.

AUTOMATIC MODE

Automatic mode automatically chooses the best method for previewing a file's contents. For example:

- Webpages, Web-related graphics (JPEGs and GIFs), and any other media types for which Internet Explorer plug-ins have been installed are displayed by an embedded version of Internet Explorer in the Viewer.
- Text files are displayed in the Viewer as ASCII or Unicode characters.
- File types that cannot be viewed in Internet Explorer are displayed outside of FTK Imager in their native application provided those applications are installed locally, and the appropriate file associations have been configured in Windows.
- File types that cannot be viewed in Internet Explorer and that do not have a known native viewer are displayed as hexadecimal code in the Viewer.

TEXTMODE

Text mode allows you to preview a file's contents as ASCII or Unicode characters, even if the file is not a text file. This mode can be useful for viewing text and binary data that is not visible when a file is viewed in its native application.

Hex Mode

Hex mode allows you to view every byte of data in a file as hexadecimal code. You can use the Hex Value Interpreter to interpret hexadecimal values as decimal integers and possible time and date values.

Note: Preview modes apply only when displaying file data. The data contained in folders or other non-file objects is always displayed in hexadecimal format.

Adding Evidence Items

To add an evidence item to the Evidence Tree:

1. Click *File* > *Add Evidence Item*,

   OR

   Click the *Add Evidence Item* button on the Toolbar.
2. Select the source you want to preview, then click *Next.*
3. Select the drive or browse to the source you want to preview, then click *Finish.*

   The evidence item appears in the Evidence Tree.
4. Repeat these steps to add more evidence items.

Adding All Attached Devices

To add data from the devices attached to a machine,

1. Click *File* > *Add All Attached Devices*,

   OR

   Click the *Add All Attached Devices* button on the Toolbar.

The *Add All Attached Devices* function, also known as auto-mount, scans all connected physical and logical devices for media. If no media is present, the device is skipped.

Removing An Evidence Item

You can remove evidence items individually, or start over again by removing all evidence at once.

To remove an evidence item:

1. In the Evidence Tree, select the evidence item you want to remove.

Note: You must select the entire evidence item to remove it; you cannot remove only part of an item.

2. Click *File* **>** *Remove Evidence Item*,

   OR

   Click the *Remove Evidence Item* button on the tool bar.

   The evidence item is removed from the Evidence Tree.

Removing All Evidence Items

To remove all evidence items at once:

1. Click *File* > *Remove All Evidence Items,*

   OR

   Click the *Remove All Evidence Items* button on the tool bar.

   All evidence items are removed from the Evidence Tree.

Obtaining Protected Registry Files

The Windows operating system does not allow you to copy or save live Registry files. Without FTK Imager, users have had to image their hard drive and then extract the RegistryRegistry files, or boot their computer from a boot disk and copy the Registry files from the inactive operating system on the drive. FTK Imager provides a much easier solution. It bypasses the Windows operating system and allows you to copy Registry files in spite of the Windows file lock.

Accessing Protected Registry Files on a local machine

To obtain the Protected Registry Files using FTK Imager running on the machine whose Registry files you need:

1. Launch FTK Imager.
2. Click *File* > *Obtain Protected Files*,

   OR

   Click the *Obtain Protected Files* button on the toolbar.
3. Designate a destination directory and specify file options.
4. Select the option that suits your needs:

- **Minimum files for login recovery**: retrieves Users, System, and SAM files from which you can recover a user's account information.
- **Password recovery and all Registry files**: retrieves Users, System, SAM, NTUSER.DAT, Default, Security, Software, and Userdiff files from which you can recover account information and possible passwords to other files. This list can also be imported to the AccessData password recovery tools, such as Rainbow Tables, PRTK, and DNA.

5. Click *OK*.

   FTK Imager exports the selected files to the designated location.
6. Add the files to the case.
7. To open the Registry files, click File, and then Registry Viewer, or right-click a Registry file in the file list, and then select Registry Viewer.

   Note: These steps will not acquire Protected Files from a drive image; only from the live system running Imager. See the directions below to acquire Protected Files from a drive image.

ACCESSING REGISTRY FILES FROM A DRIVE IMAGE

To obtain the protected Registry files from a drive image using FTK Imager:

In XP

1. Navigate to [*Drive*]:\Documents and Settings\[username]\.
2. Export
   - ntuser.dat
3. Navigate to [*Drive*]:\Windows\System32\Config\.
4. Export
   - SAM
   - System
   - Software
   - Security

In Vista

1. Navigate to [*Drive*]:\Users\[username]\
2. jExport
   - ntuser.dat
3. Navigate to [*Drive*]:\Windows\System32\Config\
4. Export

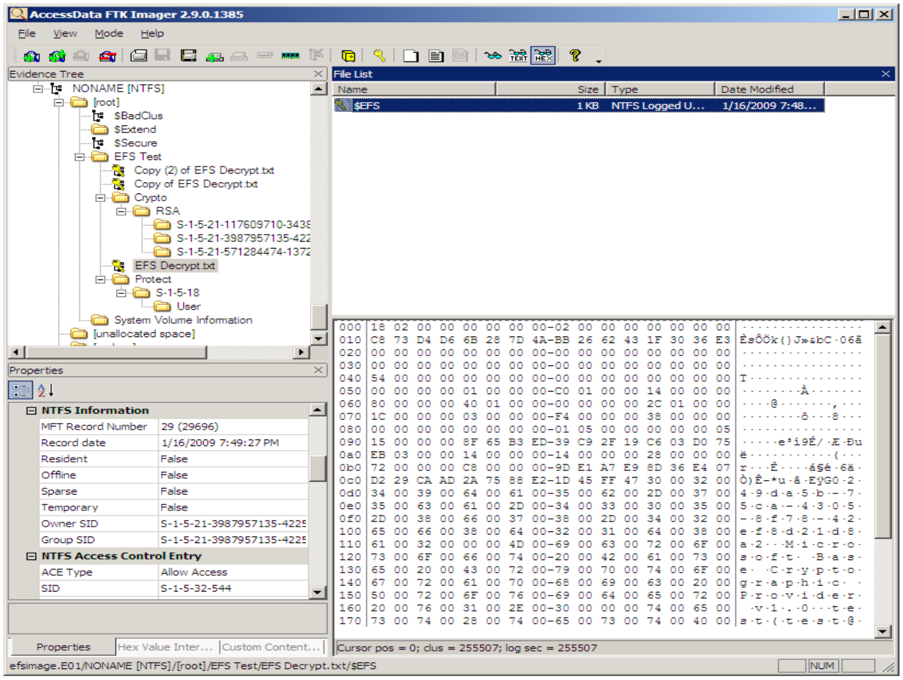
- SAM
- System
- Software
- Security

Regardless of the operating system, export the files to an accessible location (where you have rights and permissions), then add/open them one at a time in Registry Viewer.

DETECTING EFS ENCRYPTION

You can check for encrypted data on a physical drive or an image with FTK Imager. The following figure represents a view of detected EFS-Encrypted files:

Figure 2-1 Detected EFS Encrypted Files



Name	Size	Type	Date Modified
$EFS	1 KB	NTFS Logged U...	1/16/2009 7:48...

NTFS Information	
MFT Record Number	29 (29696)
Record date	1/16/2009 7:49:27 PM
Resident	False
Offline	False
Sparse	False
Temporary	False
Owner SID	S-1-5-21-3987957135-4225
Group SID	S-1-5-21-3987957135-4225
NTFS Access Control Entry	
ACE Type	Allow Access
SID	S-1-5-32-544

```
000 18 02 00 00 00 00 00 00-02 00 00 00 00 00 00 00  ················
010 C8 73 D4 D6 6B 28 7D 4A-BB 26 62 43 1F 30 36 E3  ÈsÔÖk(}J»&bC·06ã
020 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
030 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
040 54 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  T···············
050 00 00 00 00 01 00 00 00-C0 01 00 00 14 00 00 00  ········À·······
060 80 00 00 00 40 01 00 00-00 00 00 00 2C 01 00 00  ····@·······,···
070 1C 00 00 00 03 00 00 00-F4 00 00 00 38 00 00 00  ········ô···8···
080 00 00 00 00 00 00 00 00-01 05 00 00 00 00 00 05  ················
090 15 00 00 00 8F 65 B3 ED-39 C9 2F 19 C6 03 D0 75  ·····e³í9É/·Æ·Ðu
0a0 EB 03 00 00 14 00 00 00-14 00 00 00 28 00 00 00  ë···········(···
0b0 72 00 00 00 C8 00 00 00-9D E1 A7 E9 8D 36 E4 07  r···È····á§é·6ä·
0c0 D2 29 CA AD 2A 75 88 E2-1D 45 FF 47 30 00 32 00  Ò)Ê-*u·â·EÿG0·2·
0d0 34 00 39 00 64 00 61 00-35 00 62 00 2D 00 37 00  4·9·d·a·5·b·-·7·
0e0 35 00 63 00 61 00 2D 00-34 00 33 00 30 00 35 00  5·c·a·-·4·3·0·5·
0f0 2D 00 38 00 66 00 37 00-38 00 2D 00 34 00 32 00  -·8·f·7·8·-·4·2·
100 65 00 66 00 38 00 64 00-32 00 31 00 64 00 38 00  e·f·8·d·2·1·d·8·
110 61 00 32 00 00 00 4D 00-69 00 63 00 72 00 6F 00  a·2···M·i·c·r·o·
120 73 00 6F 00 66 00 74 00-20 00 42 00 61 00 73 00  s·o·f·t· ·B·a·s·
130 65 00 20 00 43 00 72 00-79 00 70 00 74 00 6F 00  e· ·C·r·y·p·t·o·
140 67 00 72 00 61 00 70 00-68 00 69 00 63 00 20 00  g·r·a·p·h·i·c· ·
150 50 00 72 00 6F 00 76 00-69 00 64 00 65 00 72 00  P·r·o·v·i·d·e·r·
160 20 00 76 00 31 00 2E 00-30 00 00 00 74 00 65 00   ·v·1·.·0···t·e·
170 73 00 74 00 28 00 74 00-65 00 73 00 74 00 40 00  s·t·(·t·e·s·t·@·
```

Cursor pos = 0; clus = 255507; log sec = 255507

efsimage.E01/NONAME [NTFS]/[root]/EFS Test/EFS Decrypt.txt/$EFS

NUM

To detect encrypted files:

1. Click *File > Detect Encryption*,

   OR

Click the *Detect Encryption* button 🔑 on the tool bar. The program will scan the evidence and notify you if encrypted files were located. As illustrated in the figure above, EFS Encrypted files are indicated by a key icon, 🔑, in the Evidence Tree.

AD Encryption

New in version 2.9 is the ability to encrypt data during export to an image. This feature is know as AD Encryption.

Supported image types are:

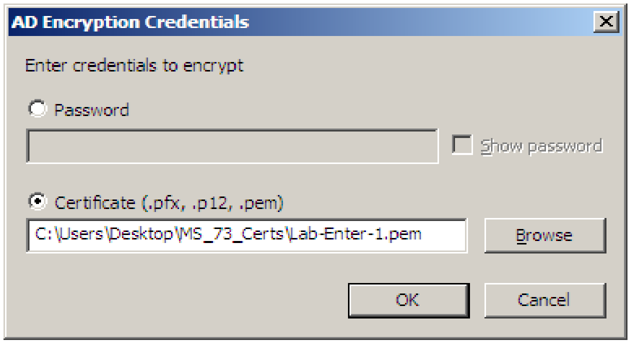
- AD1 (AD Custom Content)
- E01 (EnCase Compatible)
- S01 (Smart)
- 001 (RAW/DD)

AD Encryption also supports the following:

- Hash algorithm SHA-512.
- Crypto algorithms AES 128, 192, and 256.
- Key materials (for encrypting the AES key): pass phrases, raw key files, and certificates.

Note: A raw key file is any arbitrary file whose raw data will be treated as key material.

Figure 2-2 AD Encryption Credentials Options



AD Encryption Credentials

Enter credentials to encrypt

○ Password

□ Show password

● Certificate (.pfx, .p12, .pem)

C:\Users\Desktop\MS_73_Certs\Lab-Enter-1.pem

Certificates use public keys for encryption and corresponding private keys for decryption.

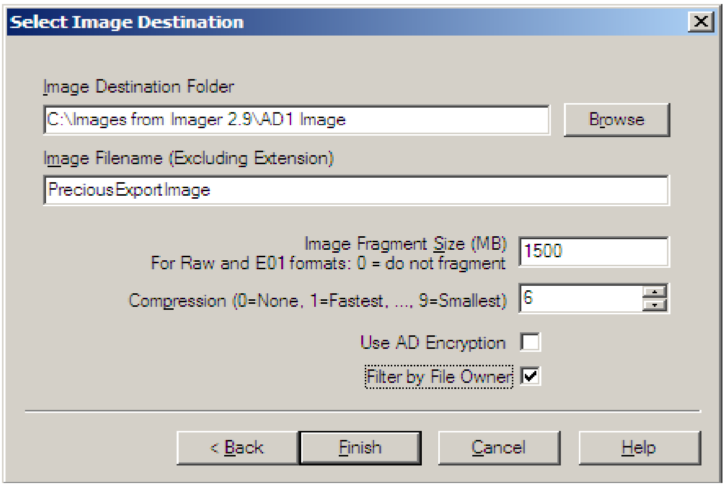
- To encrypt with a password, mark *Password*, then type and re-type the password to use.

- To encrypt with a certificate, mark *Certificate* then browse to the certificate you wish to use.

Export By SID

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.

Figure 2-3 Select Image Destination



Select Image Destination

Image Destination Folder: C:\Images from Imager 2.9\AD1 Image

Image Filename (Excluding Extension): PreciousExportImage

Image Fragment Size (MB)
For Raw and E01 formats: 0 = do not fragment: 1500

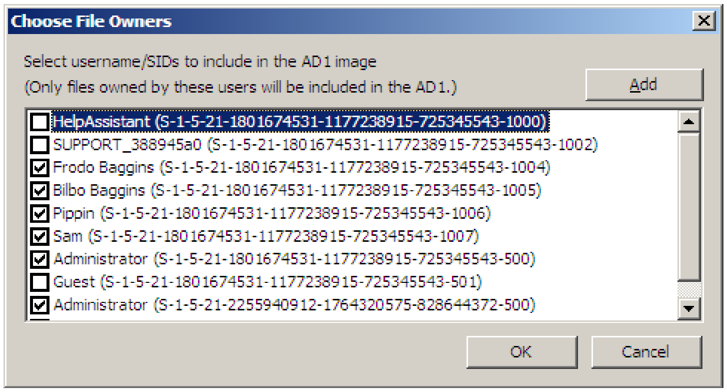
Compression (0=None, 1=Fastest, ..., 9=Smallest): 6

Use AD Encryption □

Filter by File Owner ☑

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.

Figure 2-4



Choose File Owners

Select username/SIDs to include in the AD1 image
(Only files owned by these users will be included in the AD1.)

□ HelpAssistant (S-1-5-21-1801674531-1177238915-725345543-1000)
□ SUPPORT_388945a0 (S-1-5-21-1801674531-1177238915-725345543-1002)
☑ Frodo Baggins (S-1-5-21-1801674531-1177238915-725345543-1004)
☑ Bilbo Baggins (S-1-5-21-1801674531-1177238915-725345543-1005)
☑ Pippin (S-1-5-21-1801674531-1177238915-725345543-1006)
☑ Sam (S-1-5-21-1801674531-1177238915-725345543-1007)
☑ Administrator (S-1-5-21-1801674531-1177238915-725345543-500)
□ Guest (S-1-5-21-1801674531-1177238915-725345543-501)
☑ Administrator (S-1-5-21-2255940912-1764320575-828644372-500)

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.

CREATING FORENSIC IMAGES

FTK Imager allows you to write an image file to a single destination or to simultaneously write multiple image files to multiple destinations.

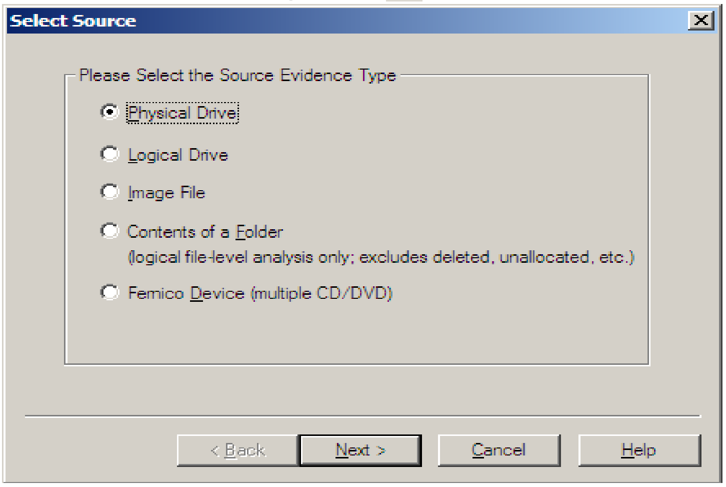
Important: When using FTK Imager to create a forensic image of a hard drive, be sure you are using a hardware-based write-blocking device. This ensures that your operating system does not alter the hard drive when you attach it to your imaging computer.

To create a forensic image:

1. Click *File* > *Create Disk Image*,

   OR

   Click the *Create Disk Image* button on the tool bar.


Select Source

Please Select the Source Evidence Type

● Physical Drive

○ Logical Drive

○ Image File

○ Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)

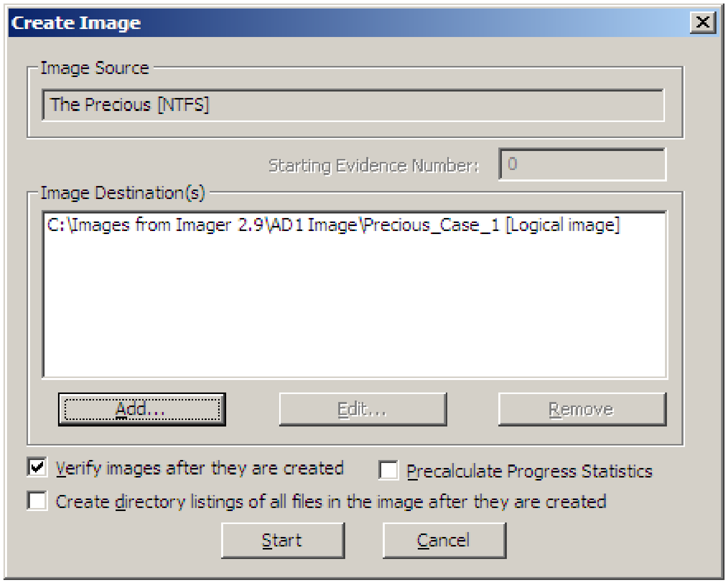
○ Fernico Device (multiple CD/DVD)

2. Select the source you want to make an image of and click *Next*.

   If you select Logical Drive to select a floppy or CD as a source, you can check the *Automate multiple removable media box* to create groups of images. Imager will automatically increment the case numbers with each image, and if something interrupts the process, you may assign case number manually.

3. Select the drive or browse to the source of the image you want, and then click *Finish*.

4. In the Create Image dialog, click *Add*.



Create Image

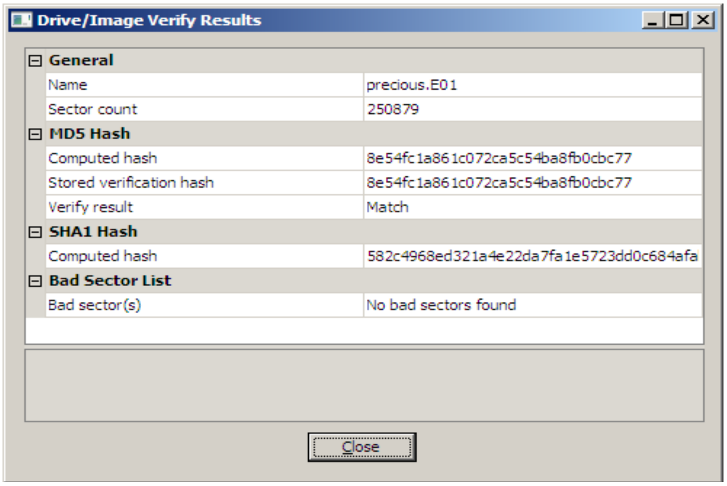
Image Source: The Precious [NTFS]

Starting Evidence Number: 0

Image Destination(s): C:\Images from Imager 2.9\AD1 Image\Precious_Case_1 [Logical image]

☑ Verify images after they are created
□ Precalculate Progress Statistics
□ Create directory listings of all files in the image after they are created

- You can compare the stored hashes of your image content by checking the Verify images after they are created box. If a file doesn't have a hash, this option will generate one



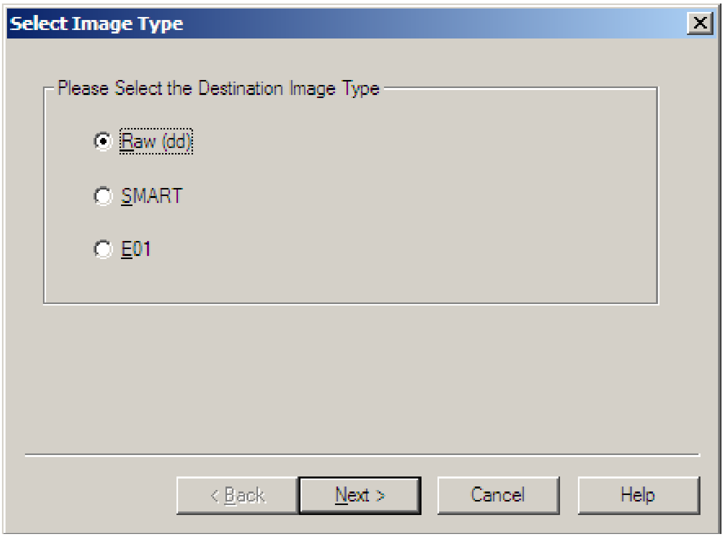
Drive/Image Verify Results

General	
Name	precious.E01
Sector count	250879
MD5 Hash	
Computed hash	8e54fc1a861c072ca5c54ba8fb0cbc77
Stored verification hash	8e54fc1a861c072ca5c54ba8fb0cbc77
Verify result	Match
SHA1 Hash	
Computed hash	582c4968ed321a4e22da7fa1e5723dd0c684afa
Bad Sector List	
Bad sector(s)	No bad sectors found

- You can list the entire contents of your images with path, creation dates, whether files were deleted, and other metadata. The list is saved in a tab-separated value format.

5. Select the type of image you want to create, then click *Next*.

Note: If you are creating an image of a CD or DVD, this step is skipped because all CD/DVD images are created in the IsoBuster CUE format.



Select Image Type

Please Select the Destination Image Type

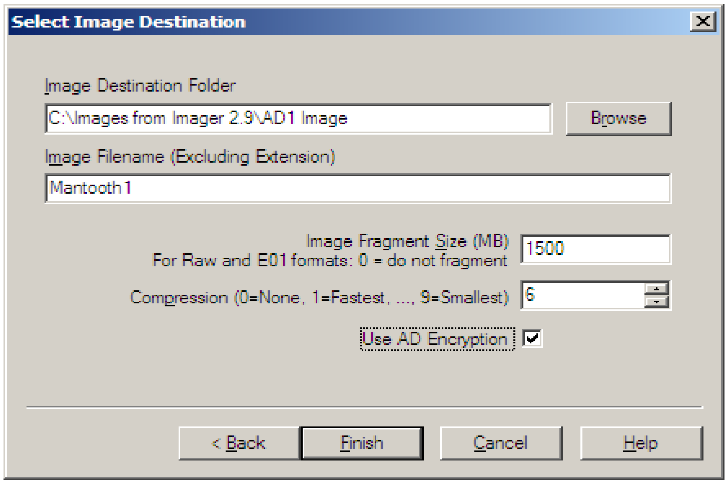
● Raw (dd)

○ SMART

○ E01

The raw image type is not compressed. If you select the Raw (dd) type, be sure to have adequate available drive space for the resulting image.

If you select SMART or E01 as the image type, complete the fields in the Evidence Item Information dialog, and click *Next*.



Select Image Destination

Image Destination Folder: C:\Images from Imager 2.9\AD1 Image

Image Filename (Excluding Extension): Mantooth1

Image Fragment Size (MB)
For Raw and E01 formats: 0 = do not fragment: 1500

Compression (0=None, 1=Fastest, ..., 9=Smallest): 6

Use AD Encryption ☑

6. In the Image Destination Folder field, type the location path where you want to save the image file, or click *Browse* to find and select the desired location.

Note: If the destination folder you select is on a drive that does not have sufficient free space to store the entire image file, FTK Imager prompts for a new destination folder when all available space has been used in the first location. However, all related image files must be saved together in the same folder prior to being added to a case.

7. In the Image Filename field, specify a name for the image file but do not specify a file extension.
8. In the Image Fragment Size field, specify the maximum size in MB for each fragment of the image file.

   The .S01 format is limited by design to sizes between 1 MB and 2047 MB (2 GB). Compressed block pointers are 31-bit numbers (the high bit is a compressed flag), which limits the size of any one segment to two gigabytes.

Note: If you want to transfer the image file(s) to CD, accept the default fragment size of 650 MB.

9. To encrypt the new image with AD Encryption, mark the *Use AD Encryption* box. For more information, see "AD Encryption" on page 16.

   When selected, you can choose between encrypting with a password, or encrypting with a certificate.

   When encryption selections are made, click *OK* to save selections and return to the Create Image dialog.
10. To add another image destination (i.e., a different saved location or image file type), click Add, and repeat steps 5-10.
    - To change an image destination, select the destination you want to change and click *Edit*.
    - To delete an image destination, select the destination and click *Remove*.
11. Click *Start* to begin the imaging process. A progress dialog appears that shows the following:
    - The source that is being imaged
    - The location where the image is being saved
    - The status of the imaging process
    - A graphical progress bar
    - The amount of data in MB that has been copied and the total amount to be copied
    - Elapsed time since the imaging process began
    - Estimated time remaining until the process is complete
12. After the images are successfully created, click Image Summary to view detailed file information, including MD5 and SHA1 checksums

    Note: This option is available only if you created an image file of a physical or logical drive.
13. When finished, click *Close*.

CREATING CUSTOM CONTENT IMAGES

FTK Imager allows you to customize your image to decrease the time and memory required to store important information and evidence. With the Custom Content Image feature, you can select specific files from a live file system or an existing image to make a smaller, more specific image. You can also search an existing image using a wild-card character to create a custom image having only those files that fit your criteria.

Custom Images serve investigators who must acquire evidence quickly, or who need only particular items of information to create evidence. Images can also be customized to fit on a thumb-drive or other portable media.

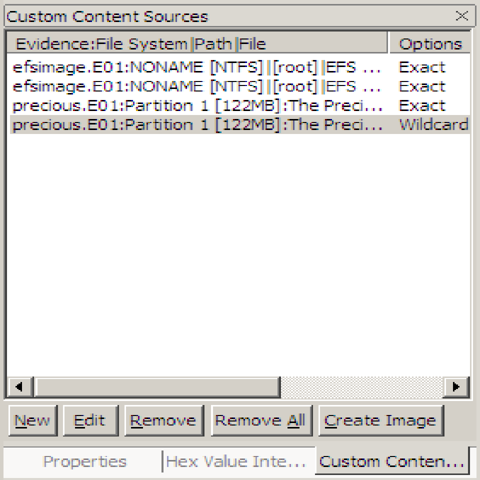
Note: When exporting the contents of a folder to a Custom Content Image (AD1), or Logical Image (AD1), if a file in the folder being exported is locked (in use by another process or program), an error message pops up showing the problem and the name of the file that is in use.

To create a custom image:

1. Add a drive or folder to Imager as an evidence item, and review the contents for the information you want to add to a custom image.
2. Click *File > Add to Custom Content Image*,

   OR

   Right-click each item to open the Export menu. Select *Add to Custom Content Image (AD1)*. The item is listed in the Custom Content Sources pane.

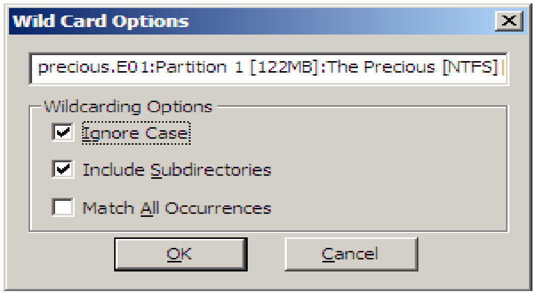


Evidence:File System|Path|File	Options
efsimage.E01:NONAME [NTFS]|[root]|EFS ...	Exact
efsimage.E01:NONAME [NTFS]|[root]|EFS ...	Exact
precious.E01:Partition 1 [122MB]:The Preci...	Exact
precious.E01:Partition 1 [122MB]:The Preci...	Wildcard

Note: The Custom Content Sources pane in dockable; that is, you can move it to any corner of the Imager window, or you can even undock it from the Imager window entirely, and drag it to a second monitor screen.

3. Continue adding content by repeating this step until you've specified or selected all the evidence you want to add to this Custom Content image.

   You can change the items in your custom image list. Use the *New* and *Remove* buttons to include or exclude items, and the *Edit* button to open the Wild Card Options dialog.



precious.E01:Partition 1 [122MB]:The Precious [NTFS]|

Wildcarding Options

☑ Ignore Case

☑ Include Subdirectories

□ Match All Occurrences

   The Wild Card Options dialog allows you to create filters to find specific files. In the path description field, you can type:

   - Use a question mark (?) to replace any single character in the file name and extension
   - Use an asterisk (*) to replace any series of characters in a file name and extension
   - Use the pipe character (|) to separate directories and files.

The following table shows examples of wild card filtering:

TABLE 2-2 Wild Card Naming Examples

Goal	Wild Card Description
Collect all files ending in .doc that reside in any folder named My Documents.	My Documents|*.doc
Collect all internet cookies on a system with multiple users.	Cookies|index.dat
Collect the Outlook e-mail archives on a multiple-user Windows XP system.	Application Data|Microsoft|Outlook|*.pst Application Data|Microsoft|Outlook|*.ost

The check box options can be used individually or in combination to filter unwanted files:

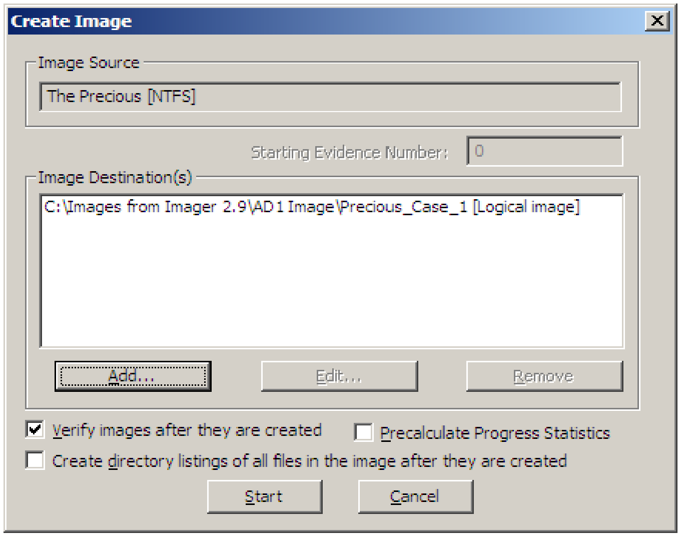
- **Ignore Case** allows all directories in the added evidence regardless of capitalization.
- **Include Subdirectories** includes all files and subdirectories in the added evidence below the specified folder.

- **Match All Occurrences** locates all directories in the added evidence that match the given expression. It eliminates the need to right-click each node in the evidence tree and selecting Add to Custom Content Image (AD1) one by one.

  For example, if you wanted to collect all files ending in .doc that reside in all folders named My Documents, FTK Imager would search all the added evidence for each occurrence of My Documents, and then collect all .doc files under that directory.

  Unchecking Include Subdirectories would find only the files in the root of the My Documents folder.

4. When all Custom Content Sources have been identified and added, click *Create Image*. The Create Image dialog opens and allows you to specify options for this AD1 image



Create Image

Image Source

The Precious [NTFS]

Starting Evidence Number: 0

Image Destination(s)

C:\Images from Imager 2.9\AD1 Image\Precious_Case_1 [Logical image]

☑ Verify images after they are created

□ Precalculate Progress Statistics

□ Create directory listings of all files in the image after they are created

5. Click *Add* to specify the location for the saved image file.
6. Enter optional Evidence Item Information such as Case Number, Evidence Number, Unique Description, Examiner, and Notes.
7. Click *Next* to continue.

8. The Select Image Destination dialog opens.

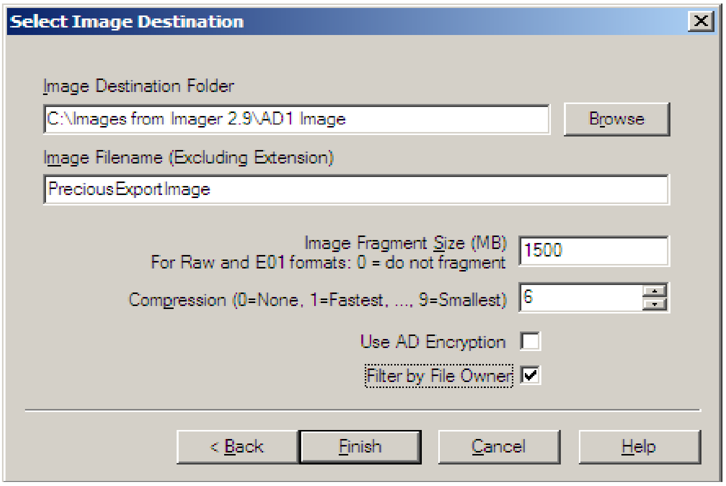


Image Destination Folder: C:\Images from Imager 2.9\AD1 Image

Image Filename (Excluding Extension): PreciousExportImage

Image Fragment Size (MB)
For Raw and E01 formats: 0 = do not fragment: 1500

Compression (0=None, 1=Fastest, ..., 9=Smallest): 6

Use AD Encryption ☐

Filter by File Owner ☑

9. Specify or click Browse to locate the destination folder for the new image.

10. Specify a filename for the new image, with no extension.

11. Specify the fragment size for the image. Default is 1500 MB. To save image segments that can be burned to a CD, specify 650 MB. To save image segments that can be burned to a DVD, specify 4GB. RAW and E01 format images can be set to 0 to produce a single file.

12. Select the compression level to use. Selecting 0 (zero) produces the largest file, with no compression. Selecting 9 (nine) produces the smallest file with the greatest compression, however it is the slowest image to produce. Compression level 1 (one) is the fastest image to create, with slight compression.

13. Choose whether to *Use AD Encryption*. For more information, see Step 9 under "Creating Forensic Images" on page 18.

14. Choose whether to Filter by File Owner. For more information, see "Export By SID" on page 17.

    To change a selected destination, highlight it in the Image Destination(s) box, then click *Edit*. Additional options include:

    - Verify images after they are created.
    - Precalculate Progress Statistics.
    - Create a list of the files contained in your image.

15. Click *Start* when you are ready to create the custom image, or *Cancel* to abandon the process.

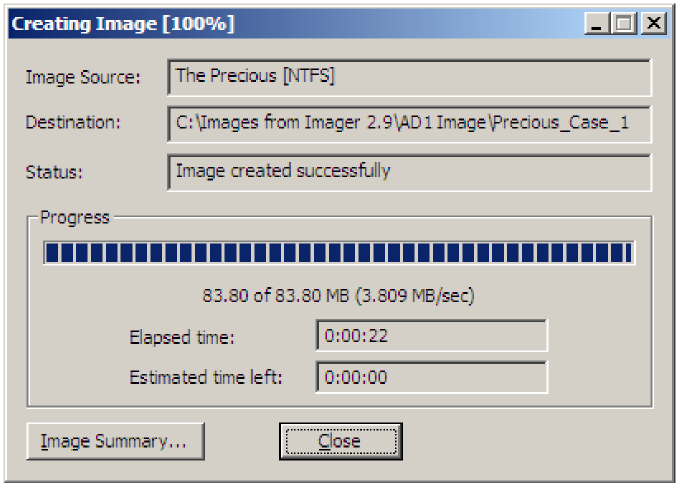


Image Source: The Precious [NTFS]

Destination: C:\Images from Imager 2.9\AD1 Image\Precious_Case_1

Status: Image created successfully

83.80 of 83.80 MB (3.809 MB/sec)

Elapsed time: 0:00:22

Estimated time left: 0:00:00

A progress dialog opens displaying destination, time, and status of the image file's creation.

Exporting Forensic Images

Convert an existing image file to a different format by exporting it, and choosing a different image format from the original. Export whole image files to convert them. Export selected contents of a drive or image to create a Custom Content Image (AD1).

Exporting Files

Exporting or copying files from an evidence item allows you to print, e-mail, salvage files, or organize files as needed, without altering the original evidence.

To export or copy files from an evidence item:

1. In the Evidence Tree, select the folder that contains the files you want to export. The folder's contents are displayed in the File List.
2. In the File List, select the files you want to export.

   Note: Click the first, then Shift-click the last to select a block of contiguous files. Click a file, then Ctrl-click individual files to select multiple non-contiguous files.
3. Click *File* > *Export Files*,

   OR

Click the *Export Files* button on the tool bar.

4. In the Browse for Folder dialog, browse to the location where you want to save the exported files.
5. Click *OK*. The files are copied to the specified location.

EXPORTING FILE HASH LISTS

Hashing is the process of generating a unique value based on a file's contents. This value can then be used to prove that a copy of a file has not been altered in any way from the original file. It is computationally infeasible for an altered file to generate the same hash number as the original version of that file. The Export File Hash List feature in FTK Imager uses the MD5 and SHA1 hash algorithms to generate hash numbers for files.

To generate and export hash values to a list:

1. In the Evidence Tree, select the folder that contains the objects you want to hash. The object's contents are displayed in the File List.
2. In the File List, select the folders or files you want to hash. If you select a folder, all the files contained in the folder and its subfolders are hashed.

   Note: Click the first, then Shift-click the last to select a block of contiguous files. Click, Ctrl-click individual files to select multiple non-contiguous files.
3. Click *File > Export File Hash List*,

   OR

   Click the *Export File Hash List* button on the tool bar.
4. In the Save As dialog, type a name for the file hash list in the File Name field.
5. Click *Save.*

   The hash list is saved as a file of comma-separated values (*.csv). You can view this file in a spreadsheet application, such as Microsoft Excel, or import it into FTK as a KFF database.

EVIDENCE ITEM INFORMATION

If you select the `.S01` (SMART) or `.E01` (Encase) image types when creating or exporting a forensic image, you can enter information and notes about the evidence item. This information is attached to the image file. You can enter the following information:

- The number of the case the evidence item is associated with

- The number assigned to the evidence item
- A unique description of the evidence item, for example, "System hard drive retrieved from suspect's personal home computer."
- The name of the examiner who is creating the image
- Notes about the evidence item that may be useful to the investigation

To export an AD1 logical image:

1. In the Evidence Tree, select the content you want to export as a logical image.
2. Click *File > Export AD1 Logical Image.*

   OR

   Right-click the folder and select *Export AD1 Logical Image* from the quick menu.
3. In the Create Image dialog, click *Add.*
4. In the Image Destination Folder field, type the path and filename for the new image file,

   OR

   Click Browse to select the desired location.

Note: If the destination folder you select is on a drive that does not have sufficient free space to store the entire image file, FTK Imager prompts for a new destination folder when all available space has been used in the first location. However, all related image files must be saved together in the same folder prior to being added to a case.

5. In the Image Filename field, specify a name for the new image file, but do not specify an extension.
6. In the Image Fragment Size field, specify the maximum size in MB for each fragment of the new image file. Image Fragment Size has nomaximum size limit, except available drive space.

Note: If you want to copy the image file(s) to CD, specify a fragment size of 650 MB. If a large image is split over multiple drives, it must be verified manually by placing all image segments in the same directory. For image file(s) that will fit on a DVD, specify a 4GB segment size.

7. Click *Finish* to return to the Create Image dialog.
8. Click *Add* to specify a destination for your custom image.
   - Check *Verify Images after they are created* to check the image hash signature. This detects whether the content of the original data has changed when it was copied to the image.
   - Check *Create directory listings of all files in the image* to record the file names and paths of the image contents. This record will be saved in Microsoft Excel format, and often functions as evidence.

- Check *Precalculate Progress Statistics* to see approximately how much time and storage space creating the custom image will require before you start, and as the imaging proceeds.

8a. To add another image destination (i.e., a different saved location), click *Add* and repeat steps 4-7.

8b. To change an image destination, select the destination to change and click *Edit.*

8c. To delete an image destination, select the destination and click *Remove.*

9. Click *Start* to begin the export process. A progress dialog appears that shows the following:

- The source image file that is being exported
- The location where the new image is being saved
- The status of the export process
- A graphical progress bar
- The amount of data in MB that has been copied and the total amount to be copied
- Elapsed time since the export process began
- Estimated time left until the process is complete

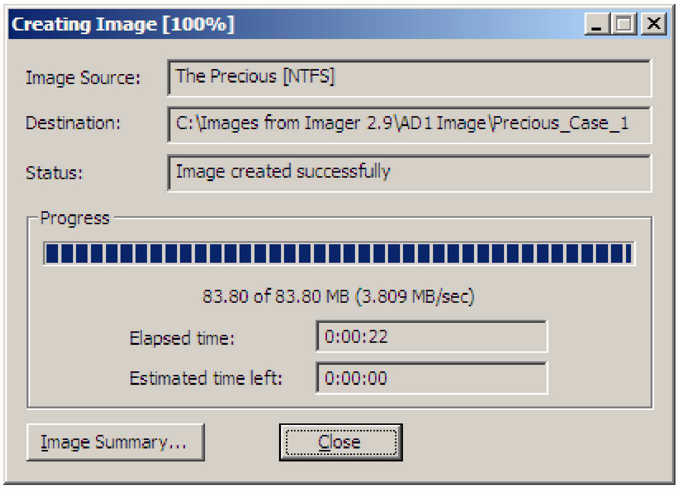


Image Source: The Precious [NTFS]

Destination: C:\Images from Imager 2.9\AD1 Image\Precious_Case_1

Status: Image created successfully

83.80 of 83.80 MB (3.809 MB/sec)

Elapsed time: 0:00:22

Estimated time left: 0:00:00

10. When the Status field reads “Image created successfully,” you can choose to do the following:

10a. View the files and the hashes (MD5 and SHA1) of your custom image by clicking the *Image Summary* button.

10b. Click *Close.*

Exporting Directory Listings

You can export a list of folders and their file content on the selected drive or partition.

To export a directory listing:

1. Select the directory you want to export.
2. Click *File* > *Export Directory Listing*,

   OR

   Click the *Export Directory Listing* button DIR.
3. Select the location for the saved file, and type in a file name.
4. Click *Save*.

Verifying Drives and Images

FTK Imager allows you to calculate MD5 and SHA1 hash values for entire drives and images to verify that copies of evidence items have not been altered in any way from the originals.

To verify a drive or image:

1. In the Evidence Tree, select the drive or image you want to verify.
2. Click *File* > *Verify Drive/Image*,

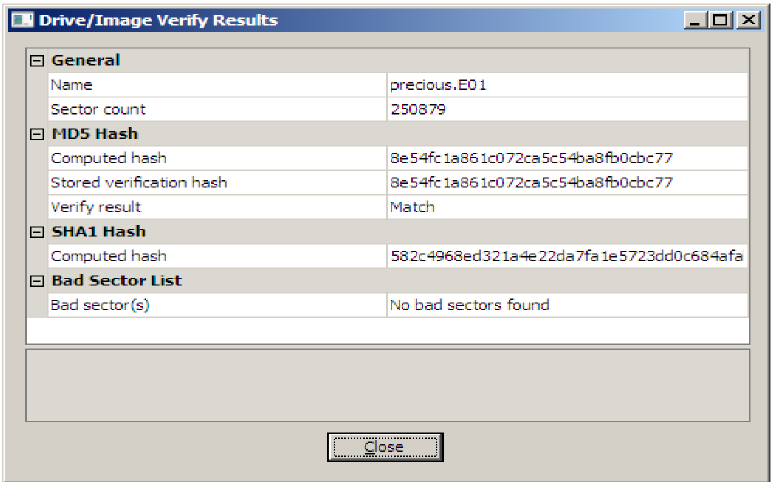
   OR

   Click the *Verify Drive/Image* button on the tool bar.

   A progress dialog appears, showing:

   - The name of the drive or image you are verifying
   - A graphical progress bar
   - The amount of data (in MB) that has been verified and the total amount to be verified
   - Elapsed time since the verification process began
   - Estimated time remaining until the process is complete

3. Once the verification process has successfully completed, the Drive/Image Verify Results summary screen appears, showing the following:



⊟ **General**	
Name	precious.E01
Sector count	250879
⊟ **MD5 Hash**	
Computed hash	8e54fc1a861c072ca5c54ba8fb0cbc77
Stored verification hash	8e54fc1a861c072ca5c54ba8fb0cbc77
Verify result	Match
⊟ **SHA1 Hash**	
Computed hash	582c4968ed321a4e22da7fa1e5723dd0c684afa
⊟ **Bad Sector List**	
Bad sector(s)	No bad sectors found

- Name of the drive or image that was verified
- Number of sectors in the drive or image
- MD5 hash computed for the drive or image
- If you verified an image that contains its own hash value, such as a .S01 (SMART) or .E01 (EnCase) image, the hash value stored inside the image is also displayed.
- Whether the hash value stored in the image matches the hash value computed by FTK Imager
- SHA1 hash computed for the drive or image
- Number of bad sectors found

Note: You can copy any of the results on the Verify Results screen (for example, the MD5 or SHA1 hash values). Simply click the result to highlight it, then right-click and select *Copy* from the quick menu. You can then paste the copied result into a text editor.

IMPORTING SETS OF FILES

You can save a set of folders and files to a directory, then create custom images of those folders and files from other drives.

For example, if you're tracking a folder of graphics throughout several drives, you would create a Custom Content image of those folders and files and export it to a drive. When creating an image of a new device, you would then import the folders and files from the drive, and Imager will make a Custom Content image of those folders and files as they occur on the next device you image.

To create a folder and file set to image:

1. List the files and folders to include with the Create Custom Content Image dialog.
2. Click *Export* to save the folders and files to a drive.
3. Start an image on a new device.
4. Open the *Create Custom Content Image* dialog, and click *Import*.
5. Navigate to the folders and files you exported.
6. Select the files you want to include in the new image, then click *Add*.
7. On the *Create Custom Content Image* dialog, click *Create Image*.

Chapter 3 Using a Logicube Device

INTEGRATING A LOGICUBE FORENSIC MD5

With FTK Imager, you can connect to and control a Logicube Forensic MD5 imaging device through the FTK Imager interface. For additional information on using the Logicube Forensic MD5 device, including explanations of specific options, see the Logicube Forensic MD5 documentation.

To integrate the Logicube Forensic MD5 with FTK Imager:

1. Connect the Logicube Forensic MD5 to your computer's parallel port and turn on the device.
2. Start FTK Imager. The Tools menu opens only if the Logicube Forensic MD5 is connected to your computer and turned on before you start FTK Imager.
3. From the menu, select Tools, and then Logicube Forensic MD5.
4. In the Logicube MD5 dialog, you can perform the following functions:
    - Create an image file of an external drive connected to the Logicube Forensic MD5
    - Format the Logicube Forensic MD5 internal destination drive
    - Access the Logicube Forensic MD5 internal drive as a USB drive
    - Access the Logicube Forensic MD5 compact flash drive as a USB drive
    - View hardware information about the Logicube Forensic MD5.
5. To exit the Logicube MD5 dialog, click *OK*.

Creating an Image File with the Logicube Forensic MD5

Using FTK Imager, you can create an image file of an external drive connected to the Logicube Forensic MD5. The image file is saved on the Forensic MD5 internal drive.

To create an image file of an external drive:

1. In the Logicube MD5 dialog, click *Image Source Drive*. The Image Parameters dialog appears.
2. In the File Size drop-down list, select the maximum size for each fragment of the image file.
3. In the Filename field, type a name for the image file, but do not specify a file extension. Filenames must be eight characters or fewer, and alphanumeric characters only.
4. From the *Verify Mode* drop-down list, select the type of data checking you want to use.
5. From the *Speed* drop-down list, select the data transfer speed.
6. Click *OK* to begin the imaging process. Progress information is displayed in the Image Parameters dialog and includes the following:
   - A graphical progress bar
   - The amount of data in MB copied per minute
   - Estimated time remaining until the process is complete
   - The number of sectors copied

Formatting the Logicube Forensic MD5 Internal Hard Drive

FTK Imager allows you to format the Logicube Forensic MD5's internal hard drive to erase previously-stored data and ensure there is enough room for a new image file to be stored.

To format the Forensic MD5 internal drive, click *Format Destination Drive* in the Logicube MD5 dialog. The drive is formatted using the FAT32 file system.

Using the Logicube Forensic MD5 Internal Drive as a USB Drive

Using FTK Imager, you can access information stored on the Logicube Forensic MD5 internal drive through a USB connection.

To access the Forensic internal drive as a USB drive:

1. In the Logicube MD5 dialog, click USB Internal Drive. The Logicube Forensic MD5 switches to USB mode.
2. Connect the USB cable from the Logicube Forensic MD5's dock to your USB port. Windows assigns a drive letter to the Forensic MD5's internal drive, allowing you to access it as a logical drive.
3. When finished, use Window's Safely Remove Hardware feature to disconnect the drive.
4. In the FTK Imager dialog, click *OK* to switch the Logicube Forensic MD5 out of USB mode.

ACCESSING THE LOGICUBE FORENSIC MD5 COMPACT FLASH DRIVE AS A USB DRIVE

FTK Imager also lets you access the Logicube Forensic MD5 compact flash drive through a USB connection.

To access the Forensic MD5's compact flash drive as a USB drive:

1. In the Logicube MD5 dialog, click USB Compact Flash. The Logicube Forensic MD5 switches to USB mode.
2. Connect the USB cable from the Logicube Forensic MD5's dock to your USB port. Windows assigns a drive letter to the Forensic MD5's compact flash drive, allowing you to access it as a logical drive.
3. When finished, use Window's Safely Remove Hardware feature to disconnect the drive.
4. In the FTK Imager dialog, click *OK* to switch the Logicube Forensic MD5 out of USB mode.

VIEWING THE LOGICUBE FORENSIC MD5 HARDWARE INFORMATION

To view the Logicube Forensic MD5's hardware information, click *Hardware Version Info* in the Logicube MD5 dialog.

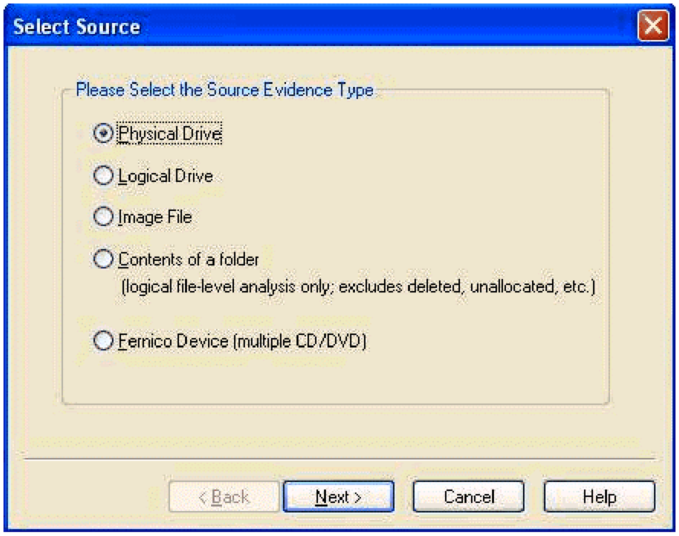
Chapter 4 Using a Fernico Device

INTEGRATING A FERNICO FAR SYSTEM

The Fernico FAR® system backs up forensic data from network locations or from locally attached hard drives, automatically spanning the content over a series of discs. Backups include integral MD5 verification and full chain-of-evidence reporting.

ACCESSING THE FERNICO FAR SYSTEM FROM IMAGER

If you have a Fernico FAR System installed, the source selection dialog will list the Fernico device as a source evidence type.



Select Source

Please Select the Source Evidence Type

● Physical Drive

○ Logical Drive

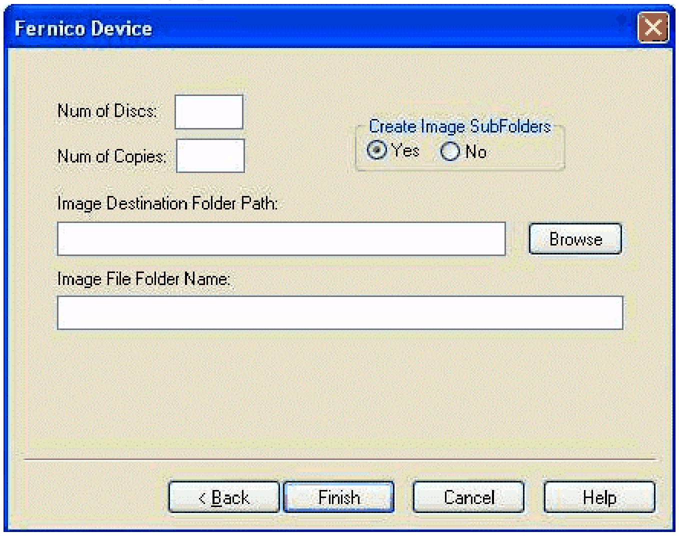
○ Image File

○ Contents of a folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)

○ Fernico Device (multiple CD/DVD)

To access the Fernico FAR system:

1. Select the Fernico Device (multiple CD/DVD), and then click *Next*. The Fernico Device dialog opens.



Create Image SubFolders ● Yes ○ No

2. In the Num of Discs field, type the number of discs loaded into the device.
3. In the Num of Copies field, type the number of copies to be placed on the discs.
4. The Fernico device will image all subfolders by default. Select the *No* radio button if you don't want subfolders imaged.
5. Type a destination for the image in the Image Folder Path field, or use the Browse button.
6. Type a name for the image folder in the Image File Folder Name field.
7. Click *Finish*. A DOS window will open showing the imaging progress.

For more information on the Fernico FAR System, see the Fernico documentation.

Appendix A Recognized Image Formats

FTK® Imager supports these file systems and image formats:

TABLE A-1 Recognized Image Types

Image Type	Recognized Format	
File Systems	• FAT 12	• Ext3
	• FAT 16	• HFS
	• FAT 32	• HFS+
	• NTFS	• Reiser
	• Ext2	
Hard Disk Image Formats	• Encase (.E01)	• ICS
	• SnapBack	• Ghost (forensic images only)
	• Safeback 2.0 and under	• SMART (.S01)
	• Expert Witness	• VMWare
	• Linux DD (.001)	
CD & DVD Image Formats	• Alcohol (*.mds)	• Pinnacle (*.pdi)
	• CloneCD (*.ccd)	• PlexTools (*.pxi)
	• ISO (*.iso)	• Roxio (*.cif)
	• IsoBuster CUE (*.cue)	• Virtual CD (*.vc4)
	• Nero (*.nrg)	
Logical Image Formats	• AD1 AccessData Custom Content Image (*.ad1)	
	• L01 EnCase Custom Content Image (*.L01)	