Imager
User Guide

AD ACCESSDATA®

AccessData Legal and Company Information

AccessData Legal Information

Document date: January 28, 2020

Legal Information

AccessData Group, Inc.
603 E. Timpanogos Circle
Building H
Orem, UT 84097 USA

AccessData Trademarks and Copyright Information

The following are either registered trademarks or trademarks of AccessData Group, Inc. All other trademarks are the property of their respective owners

.

AccessData®	AD Summation®	Mobile Phone Examiner Plus®
AccessData Certified Examiner® (ACE®)	Discovery Cracker®	MPE+ Velocitor™
AD AccessData™	Distributed Network Attack®	Password Recovery Toolkit®
AD eDiscovery®	DNA®	PRTK®
AD RTK™	Forensic Toolkit® (FTK®)	Registry Viewer®
	LawDrop®	Summation®

A trademark symbol (®, ™, etc.) denotes an AccessData Group, Inc. trademark. With few exceptions, and unless otherwise notated, all third-party product names are spelled and capitalized the same way the owner spells and capitalizes its product name. 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 products.

Third party acknowledgements:

- AFF® and AFFLIB® Copyright® 2005, 2006, 2007, 2008 Simson L. Garfinkel and Basis Technology Corp. All rights reserved.
  Copyright © 2005 - 2009 Ayende Rahien

- FreeBSD ® Copyright 1992-2011. The FreeBSD Project.

- BSD License:
  Copyright (c) 2009-2011, Andriy Syrov. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer; Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution; Neither the name of Andriy Syrov nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

- WordNet License:
  This license is available as the file LICENSE in any downloaded version of WordNet.
  WordNet 3.0 license: (Download)
  WordNet Release 3.0 This software and database is being provided to you, the LICENSEE, by Princeton University under the following license. By obtaining, using and/or copying this software and database, you agree that you have read, understood, and will comply with these terms and conditions.: Permission to use, copy, modify and distribute this software and database and its documentation for any purpose and without fee or royalty is hereby granted, provided that you agree to comply with the following copyright notice and statements, including the disclaimer, and that the same appear on ALL copies of the software, database and documentation, including modifications that you make for internal use or for distribution. WordNet 3.0 Copyright 2006 by Princeton University. All rights reserved. THIS SOFTWARE AND DATABASE IS PROVIDED "AS IS" AND PRINCETON UNIVERSITY MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED. BY WAY OF EXAMPLE, BUT NOT LIMITATION, PRINCETON UNIVERSITY MAKES NO REPRESENTATIONS OR WARRANTIES OF MERCHANT-ABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR THAT THE USE OF THE LICENSED SOFTWARE, DATABASE OR DOCUMENTATION WILL NOT INFRINGE ANY THIRD PARTY PATENTS, COPYRIGHTS, TRADEMARKS OR OTHER RIGHTS. The name of Princeton University or Princeton may not be used in advertising or publicity pertaining to distribution of the software and/or database. Title to copyright in this software, database and any associated documentation shall at all times remain with Princeton University and LICENSEE agrees to preserve same.

- XMLmind XSL-FO Converter Professional Edition Developer License Agreement:
  Distribution
  Licensee may not distribute with the Application any component of the Software other than the binary class library (xfc.jar) for the JavaTM version and the Dynamic Link Library file (xfc.dll) for the .NET version.
  Licensee shall include the following copyright notice: "XMLmind XSL-FO Converter Copyright © 2002-

2009 Pixware SARL", with every copy of the Application. This copyright notice may be placed together with Licensee's own copyright notices, or in any reasonably visible location in the packaging or documentation of the Application.
Licensee may use, distribute, license and sell the Application without additional fees due to Licensor, subject to all the conditions of this License Agreement.

- "Amazon Web Services", "AWS" "AWS Aurora" "AWS Relational Database Service" are trademarks of Amazon.com, Inc. or its affiliates in the United States and/or other countries and is used with permission https://aws.amazon.com/aispl/trademark-guidelines/.

- Apache(r), Apache Cassandra and the flame logo is a registered trademark of the Apache Software Foundation in the United States and/or other countries. No endorsement by the Apache Software Foundation is implied by the use of these marks.

Company Information

Documentation Conventions

In AccessData documentation, a number of text variations are used to indicate meanings or actions. For example, 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. Steps that require the user to click on a button or icon are indicated by **Bolded text**. This *Italic* font indicates a label or non-interactive item in the user interface.

A trademark symbol (®, ™, etc.) denotes an AccessData Group, Inc. trademark. Unless otherwise notated, all third-party product names are spelled and capitalized the same way the owner spells and capitalizes its product name. 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 products.

Registration

The AccessData product registration is done at AccessData after a purchase is made, and before the product is shipped. The licenses are bound to either a USB security device, or a Virtual CmStick, according to your purchase.

Subscriptions

AccessData provides a one-year licensing subscription with all new product purchases. The subscription allows you to access technical support, and to download and install the latest releases for your licensed products during the active license period.

Following the initial licensing period, a subscription renewal is required annually for continued support and for updating your products. You can renew your subscriptions through your AccessData Sales Representative.

Use License Manager 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 web site,

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

Your AccessData Sales Representative is your main contact with AccessData. Also, listed below are the general AccessData telephone number and mailing address, and telephone numbers for contacting individual departments

Mailing Address and General Phone Numbers

You can contact AccessData in the following ways:

AccessData Mailing Address, Hours, and Department Phone Numbers

Corporate Headquarters:	AccessData Group, Inc. 603 E. Timpanogos Circle Building H Orem, UT 84097 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*: 800.574.5199, 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
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

Technical support is available on all currently licensed AccessData solutions.
You can contact AccessData Customer and Technical Support in the following ways:

AccessData Support Portal

You can access the Chat, Knowledge Base, Discussion Boards, White Papers and more through the AccessData Support Portal:

https://support.accessdata.com

E-Mail Support:

support@accessdata.com

Telephone:

Americas/Asia-Pacific:

800-658-5199 (North America)

Support Hours: Mon-Fri, 7:00 AM – 6:00 PM (MST), except corporate holidays.

NOTE: Emergency support is available on weekends:

Saturday and Sunday 8:00am – 6:00pm MST via support@accessdata.com

Documentation

Please email AccessData regarding any typos, inaccuracies, or other problems you find with the documentation: *documentation@accessdata.com*

Professional Services

The AccessData Professional Services staff comes with a varied and extensive background in digital investigations including law enforcement, counter-intelligence, and corporate security. Their collective experience in working with both government and commercial entities, as well as in providing expert testimony, enables them to provide a full range of computer forensic and eDiscovery services.

At this time, Professional Services provides support for sales, installation, training, and utilization of Summation, eDiscovery, FTK, FTK Pro, Enterprise, and Lab. They can help you resolve any questions or problems you may have regarding these solutions.

Contact Information for Professional Services

Contact AccessData Professional Services in the following ways:

AccessData Professional Services Contact Information

Contact Method	Number or Address
Phone	North America Toll Free: 800-489-5199, option 7
	International: +1.801.377.5410, option 7
Email	*services@accessdata.com*

Table of Contents

Chapter 1 Overview

About FTK Imager

FTK® Imager is a data preview and imaging tool that lets you quickly assess electronic evidence to determine if further analysis with a forensic tool such as 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:

- 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 files and folders on local hard drives, network drives, floppy diskettes, Zip disks, CDs, and DVDs

- Preview the contents of forensic images stored on the local machine or on a network drive

- Mount an image for a read-only view that leverages Windows Explorer to see the content of the image exactly as the user saw it on the original drive.

- Export files and folders from forensic images.

- See and recover files that have been deleted from the Recycle Bin, but have not yet been overwritten on thedrive.

- Create hashes of files using either of the two hash functions available in FTK Imager: Message Digest 5 (MD5) and Secure Hash Algorithm (SHA-1).

- Generate hash reports for regular files and disk images (including files inside disk images) that you can later use as a benchmark to prove the integrity of your case evidence. When a full drive is imaged, 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, and that the image has remained unchanged since acquisition.

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

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. This allows you to store the original media away, safe from harm while the investigation proceeds using the image.

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.

Understanding AD1 Image File Version Compatibility

About Image V3 and V4 Files

AccessData has produced a new AD1v4 image format that is different than the previous AD1v3 format. Older versions of AccessData products cannot recognize the new v4 format.

As a result, two versions of Imager are available to download and use:

- Imager 3.4.0
- Imager 3.4.2 (and later)

Use the following table to understand which products can use which AD1 format.

AD1 Image versions and supported applications

- Imager 3.4.1 and later - FTK 6.0 and later - Summation 6.0 and later - eDiscovery 6.0 and later	- If you create an AD1 using one of these products, it is created only in the new v4 format. - These products can read either AD1v3 or AD1v4 image files.
Imager 3.4.0	- This version can read either AD1v3 or AD1v4 files but creates only AD1v3 files. - Use this version when working with AD1 files for 5.x versions of FTK, Summation, or eDiscovery - You can use this version to open an AD1v4 file and save it as an AD1v3 file. (See below)
- FTK 5.x and earlier - Summation 5.x and earlier - eDiscovery 5.x and earlier - Imager 3.3.x and earlier	- These products can read only AD1v3 files. - These products can create only AD1v3 files.

Converting v4 image files to v3

It is important to note that AD1 files created in 6.x versions of FTK, Summation, or eDiscovery are the v4 format and cannot be read by 5.x versions and earlier of those products as well as Imager 3.3.x and earlier. Using an older version of Imager will result in an "Image detection failed" error.

However, you can open a v4 file in Imager 3.4.0 (only) and save it as a v3 file.

To use Imager 3.4.0 to convert a v4 file to a v3 file, note the following:

- The verification hashes will be different because a v4 AD1 includes GUID tables that get hashed.
- To avoid having the top-level (filesystem) node's name changed, the AD1 should be created by doing the following:
  - Correct: **File** > **Create Disk Image** (follow wizard)
  - Incorrect: Add AD1, expand, right click on filesystem node in tree, Export Logical Image (AD1)

  > **Note:** Note: An AD1 image is not really a disk image even though the option you use is *Create Disk Image*.

Determining the Version of an Image File

A hex editor can be used to quickly determine if your AD1 is v3 or v4.
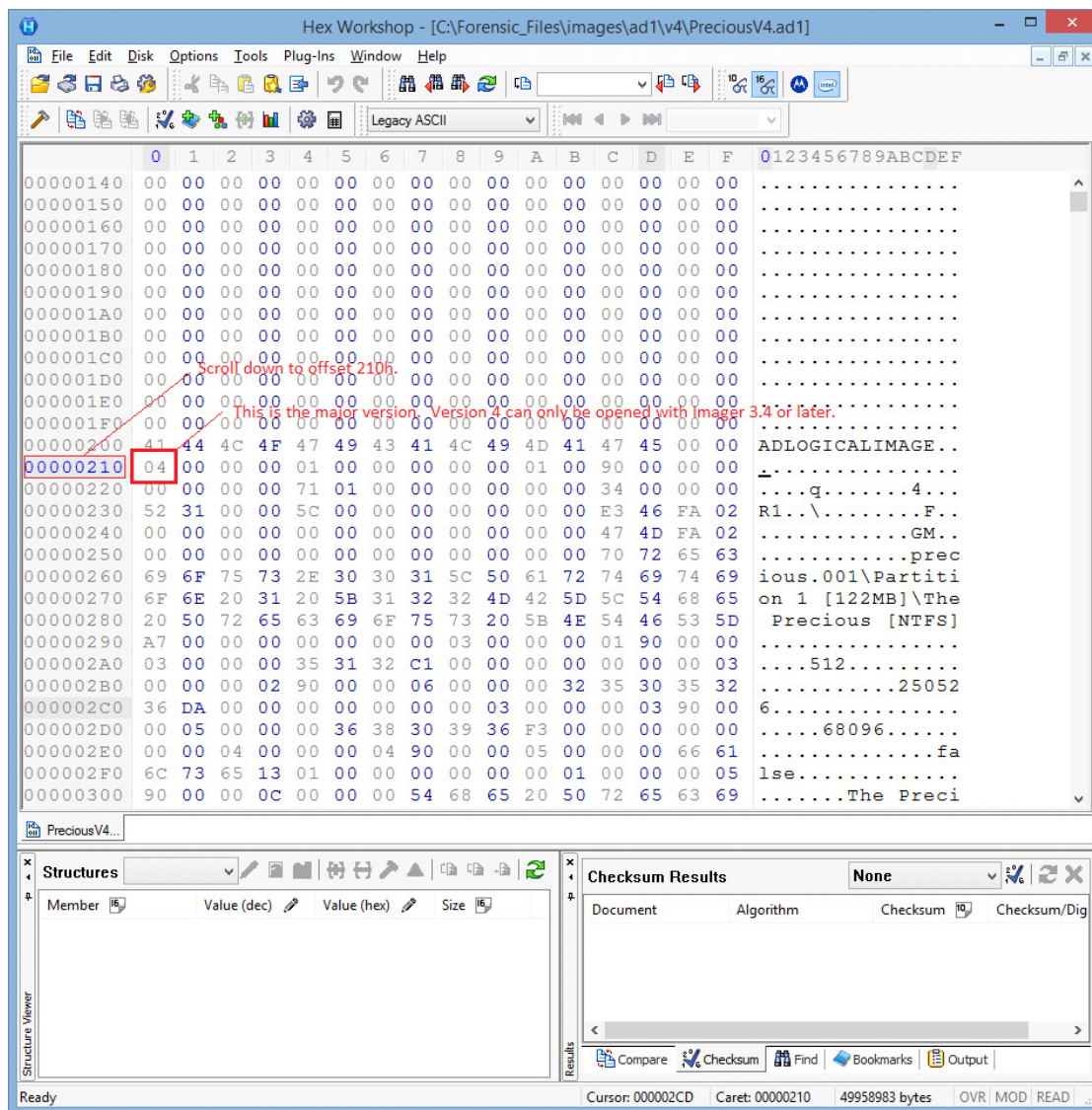
Chapter 2 Installation

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 connected to a machine in the field, so there is no need to install it on a suspect's computer in order to capture its image.

Starting with version 3.4.2, Imager is a 64-bit application.

Installing Locally

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

To install FTK Imager

1. Browse to the FTK Imager setup file, either from an installation disc, or from the saved file downloaded from http://accessdata.com/support/adownloads. The following is an example of what you will find on the web site, however, the version number and its MD5 hash number will change**.**

AccessData Web Site: Imager Downloads

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. On the *Welcome* screen, click **Next**.

8. Read and accept the *License Agreement*, then click **Next.**

9. Do one of the following:

    ● Accept the default installation location.

    ● Browse to a different destination folder.

10. Click **Next**.

11. In the *Ready to Install* screen, click **Next**.

12. Do one of the following:

    ● Mark the **Launch AccessData FTK Imager** box to force Imager to run immediately after the install is complete.

    ● Leave the box unmarked to run the newly installed program at a later time.

Note: On MS Windows Server 2008R2 running User Account Control (UAC), marking the **Launch** box does nothing. You must manually run FTK Imager after installation.

---

13. 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:

● Copy the FTK Imager Lite files directly to the device, avoiding installing to a local computer first.
  Unzip the downloaded files to the portable drive and execute the file from there.
  The FTK Imager Lite program has fewer files (only the essentials) and does not require a separate installation, although you must unzip the downloaded file to extract its contents into a folder before use.

● Run the installation on a local computer, then copy the FTK Imager folder from the [*Drive*]:\Program Files\AccessData\FTK Imager to the thumb drive or other portable device.

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 file,

FTK Imager.exe 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, and a reliable write-blocker must still be used.

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.
  Sample:
  "ftk imager.exe" /CreateDirListing e:\precious.E01
- **/VerifyImage**
  Verifies an image when you specify the image path and filename.
  Sample:
  "FTK Imager.exe" /VerifyImage E:\precious.E01
- **/EnableDebugLog**
  Enables logging to the **FTKImageDebug.log** file created in the folder you run **FTK Imager.exe** from.
  Sample:
  "FTK Imager.exe" /EnableDebugLog

> **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 run FTK Imager using the Command Line Options

1. Close FTK Imager, then from the *Windows Start Menu*, click **Run**.

2. In the *Run* text box, browse to the path and folder containing **FTK Imager.exe**, then click **Open**.

3. At the end of the resulting text line:

   3a. Add one space before the option you wish to use

   3b. Type the option to use.

   3c. Add another space and any corresponding data.

   3d. Click **OK**.

Chapter 3 The FTK Imager User Interface

This chapter discusses the FTK Imager User Interface and options.

The FTK Imager UI

The FTK Imager User Interface is divided into several panes; each is dockable. The *Evidence Tree*, *File List*, *Properties*, *Hex Value Interpreter*, *Custom Content Sources* panes, *Menu*, and *Toolbar* can all be undocked and resized to best fit your needs. Each can be re-docked individually, or you can reset the entire view for the next investigation.

To undock a pane or toolbar

> ❖ Select it and click and drag its title bar to the desired location.

To re-dock a pane or toolbar

> ❖ Drag 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

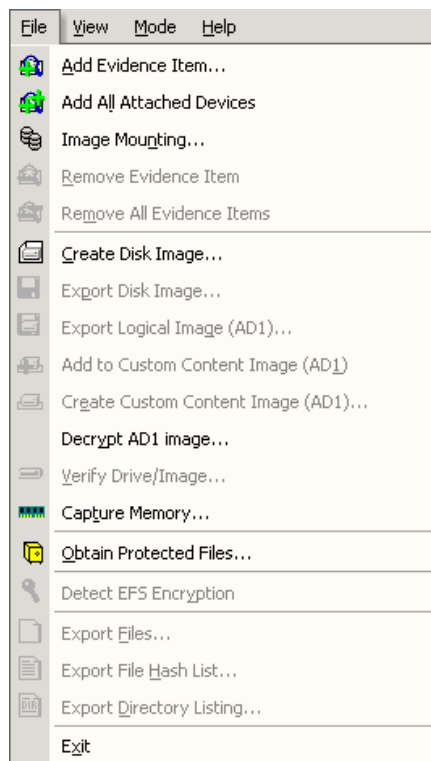> ❖ Select **View > Reset Docked Windows**.

Menu Bar

Use the *Menu* Bar to access all the features of FTK Imager. The Menu Bar is always visible and accessible. There are four items on the Menu Bar. They are discussed in detail in this section.

File Menu

The *File* menu provides access to all the features you can use from the *Toolbar*.
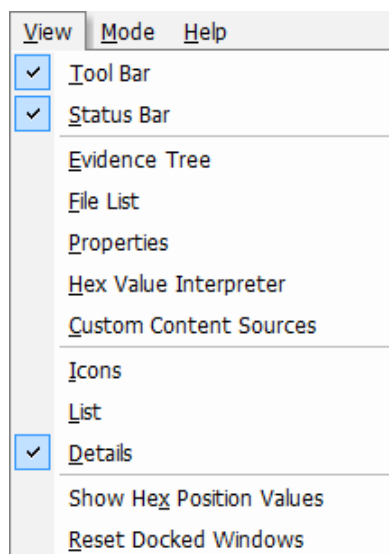
The File Menu

See Toolbar (page 18).

View Menu

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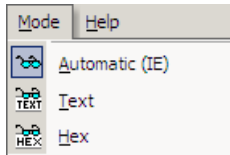
The View Menu

Mode Menu

The *Mode* menu lets you select the preview mode of the *Viewer*. Each of the viewing modes is discussed in more detail in Chapter 3. See Preview Modes (page 23).
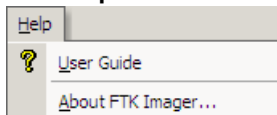
The Mode Menu

Help Menu

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

The Help Menu

Toolbar

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

FTK Imager Toolbar Components

Button	Description
	Add Evidence Item
	Add All Attached Devices
	Image Mounting. Opens the Map Image to Drive dialog.
	Remove Evidence Item
	Remove All Evidence Items
	Create Disk Image
	Export Disk Image

FTK Imager Toolbar Components (Continued)

Button	Description
	Export Logical Image (AD1)
	Add to Custom Content Image (AD1)
	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
	Export Directory Listing
	Choose IE, text, or hex viewer automatically
	View files in plain text
	View files in hex format
	Open FTK Imager User Guide
	Show or Hide Panels. Choose to show or hide the *Toolbar*, *Evidence Tree*, *File List*, *Properties*, *Hex Value Interpreter*, and/or *Custom Content Sources Pane*s.

View Panes

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

Evidence Tree Pane

The Evidence Tree pane (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 sub folders.

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 Pane

The *File List* pane 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 either the *Evidence Tree* or the *File List*.

The Properties Tab
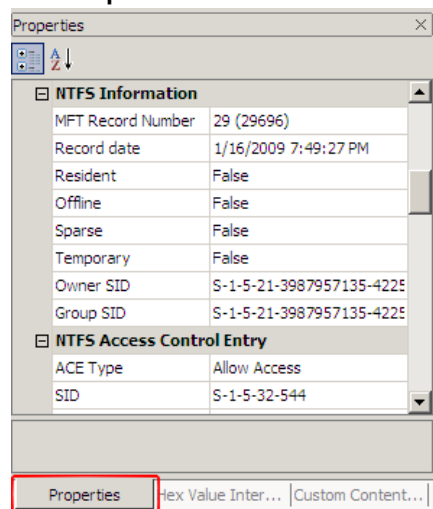
Properties include information such as object type, size, location on the storage media, flags, and time stamps.

Hex Value Interpreter

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

The Hex Value Interpreter Tab
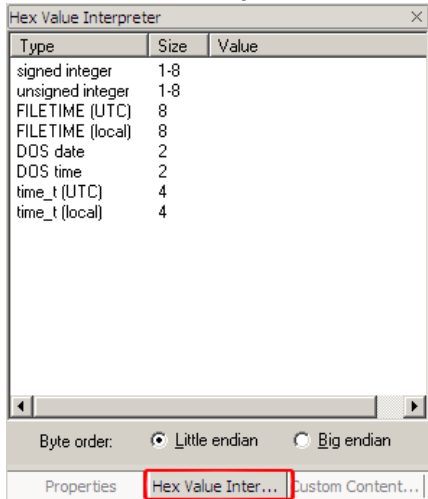
To convert hexadecimal values, highlight one to eight adjacent bytes of hexadecimal code in the *Viewer*. A variety of possible interpretations of the selected code are automatically displayed in the *Hex Value Interpreter*. This feature is most useful if you are familiar with the internal code structure 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.

The Custom Content Sources Tab
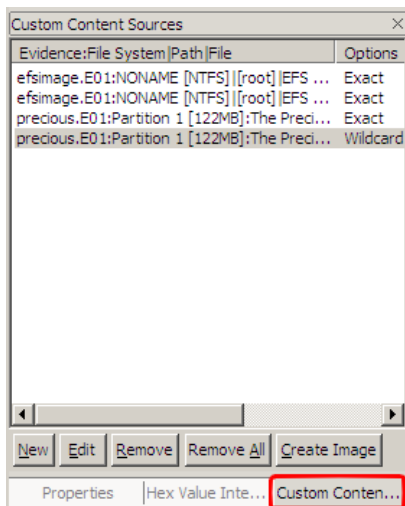
You can add, edit, and remove one or all sources, and create the image from here.

Click **Edit** to open the *Wild Card Options* dialog box.

Wild Card Options
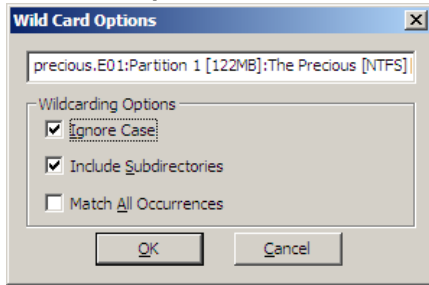
For more information, see Creating Custom Content Images (page 43).

Viewer

The *Viewer* shows the content of the currently selected file, based on the Preview Mode selected: Natural, Text, or Hex. See Preview Modes (page 23) for more information.

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

Chapter 4 Working With Evidence

Use FTK Imager to preview evidence prior to creating the image file(s). You can then choose to image the entire evidence object, or choose specific items to add to a Custom Content (AD1) image. This chapter discusses working with evidence and using FTK Imager to accomplish the creation of forensic images that meet your exact needs.

Previewing Evidence

Evidence items can be previewed prior to deciding what should be included in an image. Beginning with FTK Imager 3.0 support is included for VXFS, exFAT, and Ext4 file systems.

W A R N I N G: If the machine running FTK Imager has an active Internet connection and you are using Imager to preview HTML content 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.

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*, as introduced in Chapter 2. Each is described in more detail here.

Automatic Mode

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

- Web pages, 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 by default in Hexadecimal Mode in the Viewer.

Text Mode

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

You can add a single evidence item, or several at one time. These procedures are explained in this section.

Adding a Single Evidence Item

To add an evidence item to the Evidence Tree

1. Do one o f the following:

    ● Click **File > Add Evidence Item.**

    ● Click the **Add Evidence Item** button on the *Toolbar*.

2. Select the source type 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 all of the devices attached to a machine

❖   Do one of the following:

    ● Click **File > Add All Attached Devices.**

    ● 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 in an attached device such as a CD- or DVD-ROM or a DVD-RW, the device is skipped.

Image Mounting

New beginning in version 3.0 of FTK Imager, Image Mounting allows forensic images to be mounted as a drive or physical device, for read-only viewing. This action opens the image as a drive and allows you to browse the content in Windows and other applications. Supported types are RAW/dd images, E01, S01, AFF, AD1, and L01. Full disk images RAW/dd, E01, and S01 can be mounted Physically. Partitions contained within full disk images, as well as Custom Content Images of AD1 and L01 formats can be mounted Logically. The differences are explained in this section.

Note: AD encrypted images can now be mounted as either a drive or a physical device. Other types of encrypted images are not supported for mounting as either a drive or physical device.

Benefits of Image Mounting

The ability to mount an image with FTK Imager provides the following benefits, and you may find others as you use the feature:

- Mount a full disk image with its partitions all at once; the disk is assigned a PhysicalDrive*n* name and the partitions are automatically assigned a drive letter beginning with either the first available, or any available drive letter of your choice.

- Read a full disk image mounted physically, and assigned a Physical Drive *n* name using Imager or using any Windows application that performs Physical Name Querying.

- Read and write to the mounted image using a cache file. The original content is not altered.

- Mount images of multiple drives and/or partitions. The mounted images remain mounted until unmounted or until Imager is closed.

- Easily unmount mounted images in any order, individually or all at once.

- View a logically mounted image in Windows Explorer as though it were a drive attached to the computer, providing the following benefits:

  - View file types with Windows associations in their native or associated application, when that application is installed locally.

  - Run anti-virus applications on the mounted image.

  - Share and view the logically mounted image as a drive in Windows Explorer from remote computers when Remote Access has been configured correctly.

  - Copy files from the mounted image to another location.

  - Prevent files from being copied into the mounted image from another location. (Because the image is read-only, there is no worry that a remote user, or any user, viewing the image will make a change that would render the data invalid.)

Characteristics of a Logically Mounted Image

AD1 and L01 are both custom content images, and contain full file structure, but do not contain any drive geometry other other physical drive data. Thus, these images do not have the option of being mounted Physically.

Note: When Logically mounting an image, the drive or partition size displays incorrectly in the Windows **Start > Computer** view. However, when you open the "drive" from there, the folders and files contained within the mounted image do display correctly.

Characteristics of a Physically Mounted Image

When you mount an image physically, while it cannot be viewed by Windows Explorer, it can be viewed outside of Imager using any Windows application that performs Physical Name Querying.

E01, S01, AFF, and 001 (RAW/dd) images are drive images that have the disk, partition, and file structure as well as drive data. A physical disk image can be mounted Physically; and its disk image partition(s) can be mounted Logically.

Mounting an Image

To mount an image

1. If you already have the desired image added as evidence in the Imager Evidence List, select that item, then do Step 2 to auto-populate the Source box with the image file to be mounted, as shown in Step 3.

   If you do not already have the desired image added as evidence, begin with Step 2.

---

2. Do one of the following:

    - Click **File >Image Mounting.**

    - Click the **Image Mounting** button on the *Toolbar*.

3. Type in the path and filename, or click **Browse** to populate the *Source* box with the path and filename of the image to be mounted.

    After selecting an image, the Mount Type will default to the supported mapping based on the image type selected. Click the drop-down to display other available Mount Types.

Mount Image to Drive
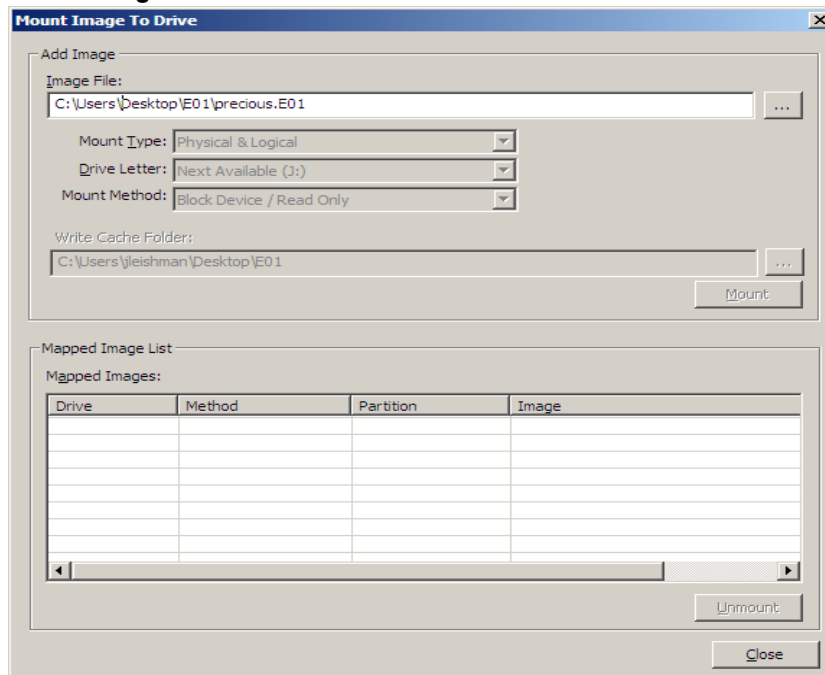
4. Select the *Mount Type* to use for mounting.
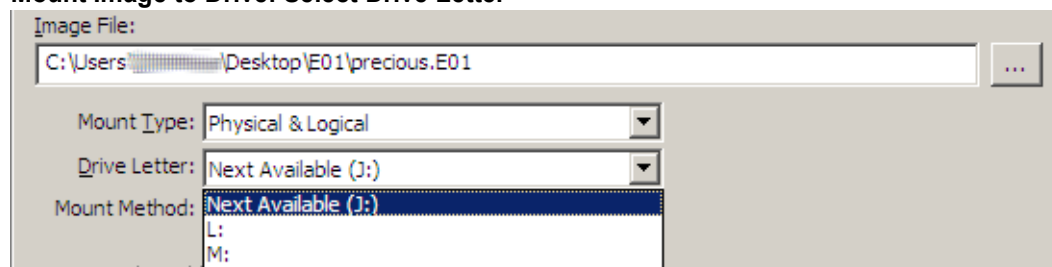
Mount Image to Drive: Select Mount Type
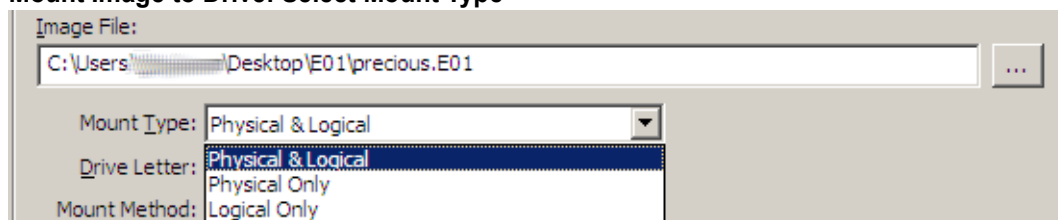
Available Mount Types are *Physical & Logical*, *Physical Only*, and *Logical Only*.

If the *Mount Type* selected includes *Logical*, you can select the Drive Letter to assign as the mount point.
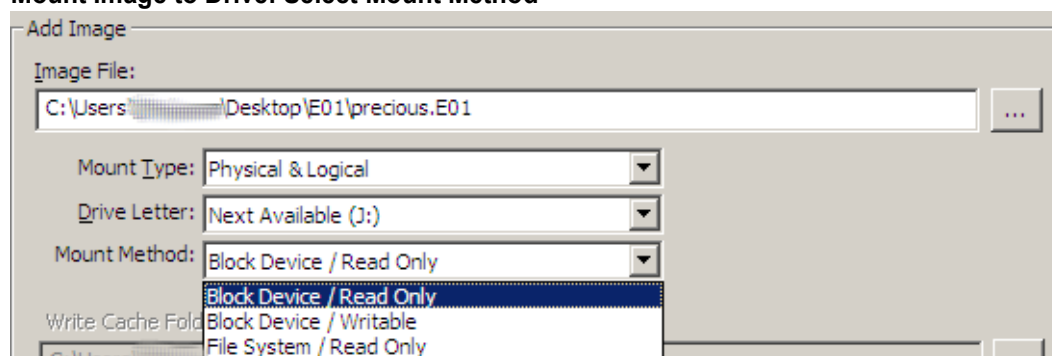
5. Click the Drive Letter drop-down to see all drive letters that are available for assignment to the mounted image

Mount Image to Drive: Select Drive Letter

Image File:

C:\Users▓▓▓▓▓▓▓▓▓▓\Desktop\E01\precious.E01 [...]

Mount Type: Physical & Logical

Drive Letter: Next Available (J:)

Mount Method: Next Available (J:)
L:
M:

6. Select the drive letter to use for this mounting.

7. Click the *Mount Method* drop-down to select from the available Mount Methods.
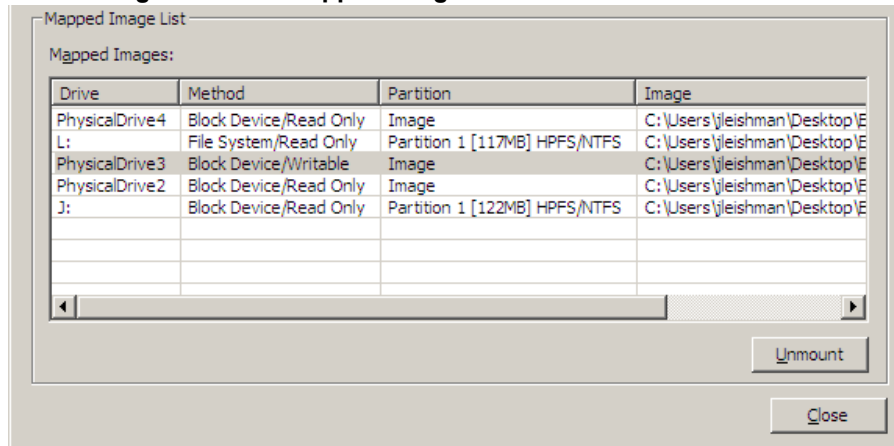
Mount Image to Drive: Select Mount Method

Add Image

Image File:

C:\Users▓▓▓▓▓▓▓▓▓▓\Desktop\E01\precious.E01 [...]

Mount Type: Physical & Logical

Drive Letter: Next Available (J:)

Mount Method: Block Device / Read Only

Block Device / Read Only
Write Cache Fold Block Device / Writable
File System / Read Only

Available Mount Methods are shown and described in the following table:

Mount Image: Mount Methods

Block Device/Read Only	Reads the device as a block device, meaning that the mounted device must be viewed using any Windows application that performs Physical Name Querying
Block Device/Writable	Allows you to write to the evidence, make notes, and so forth. the changes and notations are saved in a cache file, but no changes are made to the original. If selected, provide path information for the cache file in the Write Cache Folder field.
File System/Read Only	Reads the device as a read-only device that you can view using Windows Explorer.

8. Select the *Mount Method* to use for this mounting.

9. When all mount options are selected, click **Mount**.

All the related mount information will be displayed in the *Mapped Image List*.

Mount Image To Drive: Mapped Image List

Drive	Method	Partition	Image
PhysicalDrive4	Block Device/Read Only	Image	C:\Users\jleishman\Desktop\E
L:	File System/Read Only	Partition 1 [117MB] HPFS/NTFS	C:\Users\jleishman\Desktop\E
PhysicalDrive3	Block Device/Writable	Image	C:\Users\jleishman\Desktop\E
PhysicalDrive2	Block Device/Read Only	Image	C:\Users\jleishman\Desktop\E
J:	Block Device/Read Only	Partition 1 [122MB] HPFS/NTFS	C:\Users\jleishman\Desktop\E

Mapped Image List
Mapped Images:

Unmount

Close

> To mount another image, repeat the process. You can continue to mount images as needed, until you run out of evidence to add, or mount points to use. Mounted images remain available until unmounted, or until Imager is closed.

10. Click **Close** to return to FTK Imager.

Unmounting an Image

To unmount a mounted image

1. Click **File > Image Mounting.**

2. In the *Mount Image to Drive* dialog box, highlight the image to unmount.

3. Click **Unmount.**

4. Click **Done** to close the *Mount Image to Drive* dialog and return to FTK Imager.

To unmount multiple mappings

1. Choose one of the following:

   ● Click the first, then Shift-click the last to select a block of contiguous mappings.

   ● Click a mapping in the list, then Ctrl-click individual mappings to select multiple non-contiguous mappings.

   ● Click and drag to select multiple Mounted Images.

2. Click **Done** to close the *Mount Image to Drive* dialog and return to FTK Imager.

Removing Evidence

When required, evidence items can be removed individually, or altogether. Both methods are discussed in this section.

Removing a Single 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. Do one of the following:

   - Click **File > Remove Evidence Item**

   - Click the **Remove Evidence Item** button on the *Toolbar*.

The evidence item is removed from the Evidence Tree.

Removing All Evidence Items

To remove all evidence items at once

   ❖ Do one of the following:

   - Click **File > Remove All Evidence Items**

   - Click the **Remove All Evidence Items** button on the *Toolbar*.

   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 Registry 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 circumvents the Windows operating system and its file locks, thus allowing you to copy the live Registry files.

Acquiring Protected Registry Files on a Local Machine

You can acquire the Protected Registry Files using FTK Imager running on the machine whose Registry files you need.

To acquire Protected Registry Files on a local machine

1. Launch FTK Imager.
2. Do one of the following:
   - Click **File > Obtain Protected Files.**
   - Click the **Obtain Protected Files** button on the *Toolbar*.
3. Specify a destination directory.
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 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, do one of the following:
   - Click **File > Registry Viewer.**
   - Right-click a Registry file in the file list, 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 access 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 the following files:

- SAM

- System

- Software

- Security

In Vista

1. Navigate to [*Drive*]:\Users\[*username*]\

2. Export

- ntuser.dat

3. Navigate to [*Drive*]:\Windows\System32\Config\

4. Export the following files:

- 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.

Using Encrypted Images

FTK Imager can work with images that are encrypted with either EFS or AD Encryption.

The use of encrypted images is discussed below.

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:

Detected EFS Encrypted Files
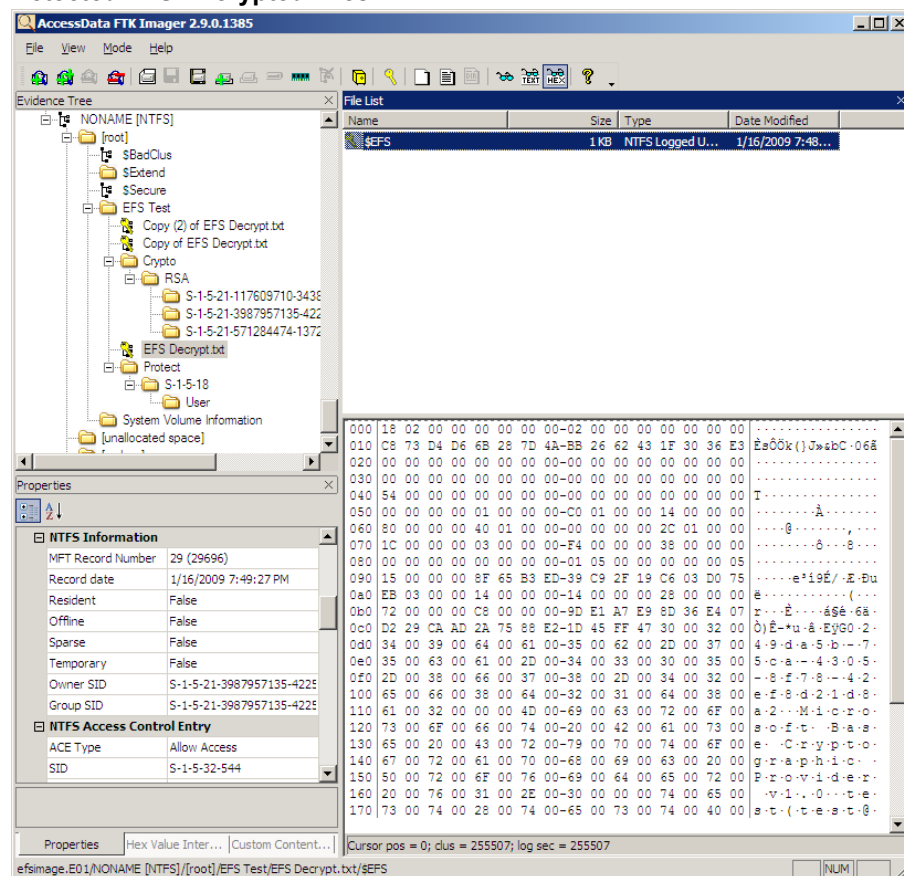
To detect encrypted files

1. Do one of the following:

   - Click **File > Detect Encryption**.

   - Click the **Detect Encryption** button on the *Toolbar*.

   The program scans the evidence and notifies you if encrypted files are located. As illustrated in the figure above, EFS Encrypted files are indicated by a key icon, in the Evidence Tree.

AD Encryption

FTK Imager 3.0 and later has 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 Logical Image)
- E01 (EnCase Compatible)
- S01 (Smart)
- AFF (Advanced Forensic Format)
- 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.

AD Encryption Credentials Options
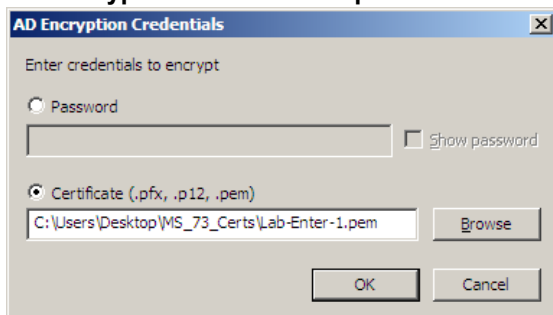
Certificates use public keys for encryption and corresponding private keys for decryption.

- 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 to use.

AFF Encryption

New beginning in FTK Imager 3.0 is the ability to create images using AFF Encryption. When you create an AFF encrypted image, a password is required. If you wish to open that encrypted image later, you will need to supply the password that was used when it was created.

The AFF Encryption Dialog Box

AFF Encryption

Enter password to decrypt : Mantooth29.aff

Password

`********` ☐ Show password

OK   Cancel
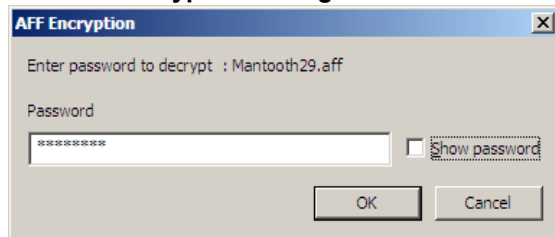
Chapter 5 FTK Imager Output Files

FTK Imager allows you to make several different types of forensic images. In addition, drive content and hash lists can be exported. This chapter discusses the available options.

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 using the same source data or drive.

### *Imaging Complete Drives or Partitions*

Important: The following important information should be reviewed and understood prior to imaging complete drives or complete partitions on drives:

- 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.

- When exporting data to an image from an encrypted drive, create the image physically, not logically. A physical image is often required for decrypting full disk encryption.

To create a forensic image

1. Do one of the following:
   - Click **File > Create Disk Image**.
   - Click the **Create Disk Image** button 🖫 on the *Toolbar*.

Select Source
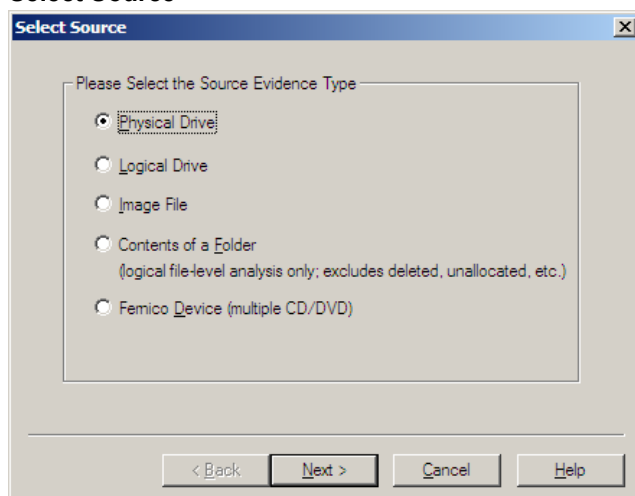
2. In the Select Source dialog box, select the source you want to make an image of.

3. Click **Next**.

4. If you select Logical Drive and need 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.

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

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

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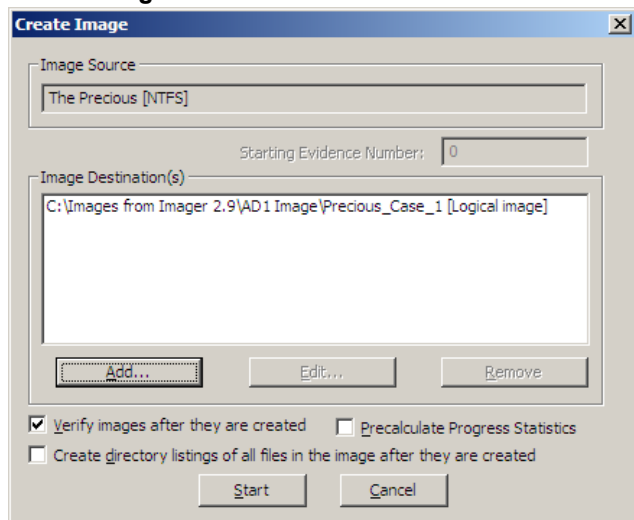
- Compare the stored hashes of your image content by checking the **Verify images after they are created** box. If a file doesn't have a hash, this option will generate one.

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

7. Select the type of image you want to create.

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. Hashes are not generated for CD and DVD images so they will not be verified, as well.

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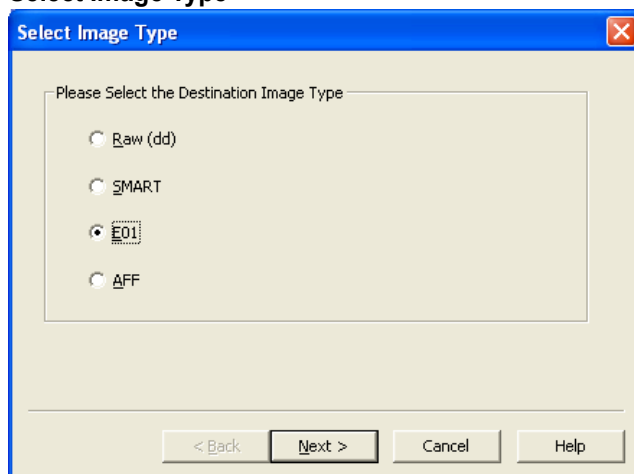
Important: The raw image type is not compressed. If you select the Raw (dd) type, be sure to have adequate available drive space for the resulting image.

7a. If you are creating an AFF image type, choose **AFF**.

The *Image Destination Folder* dialog box you see will be different than that seen when selecting ay other image type

Select Image Type with AFF Selected.
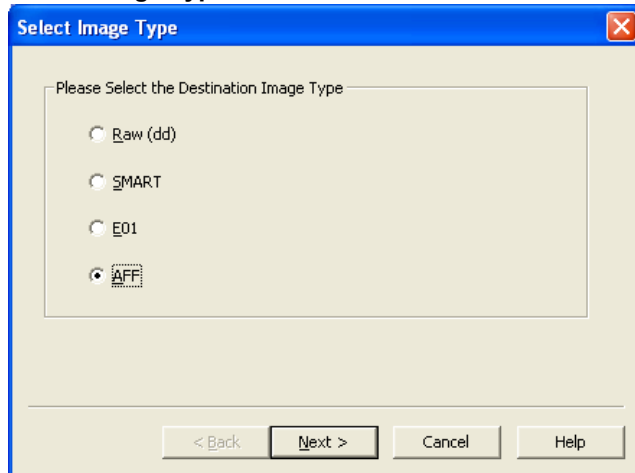
7b. Click **Next**.

8. Specify Evidence Item Information. All Evidence Item Information is optional, but it is helpful to have the information easily accessible in case it is called into question at any time after creation

Evidence Item Information

9. Complete the fields in the Evidence Item Information dialog.

Select Image Destination
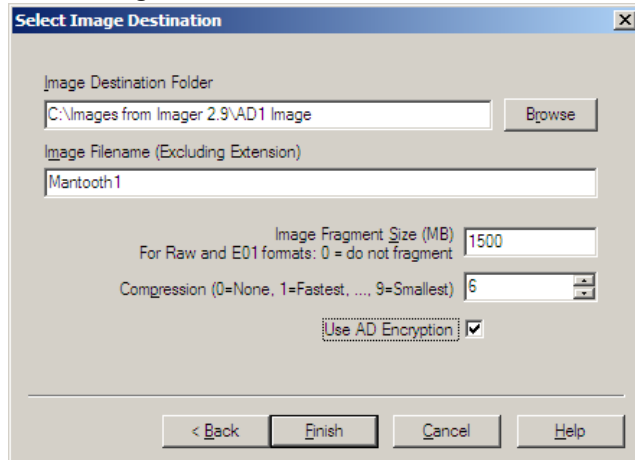
10. Click **Next**.

11. In the Image Destination Folder field, do one of the following:

    - Type the location path where you want to save the image file.

    - 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.

12. In the Image Filename field, specify a name for the image file but do not specify a file extension.

13. Specify the Image fragment Size:

    - Default Image Fragment Size = 1500 MB

    - To save images segments that can be burned to a CD, specify 650 MB.

    - To save image segments that can be burned to a DVD, specify 4000 MB.

    - 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.

        13a. Select the compression level to use.

        - 0=No Compression
        - 1=Fastest, Least Compression (faster, and also slightly smaller than a 0-compression file)
        - 9=Slowest, Most Compression (smallest file, slowest to create).
        - Numbers between 1 and 9 produce an image with varying levels of compression to speed ratio.

14. To encrypt the image, choose the correct encryption box as explained below:

    14a. To encrypt the new image with AD Encryption, mark the **Use AD Encryption** box.

    14b. To encrypt the new image with AFF Encryption, mark the **Use AFF Encryption** box.
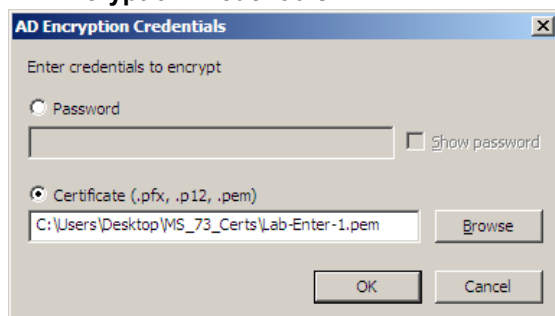
Select Image Destination
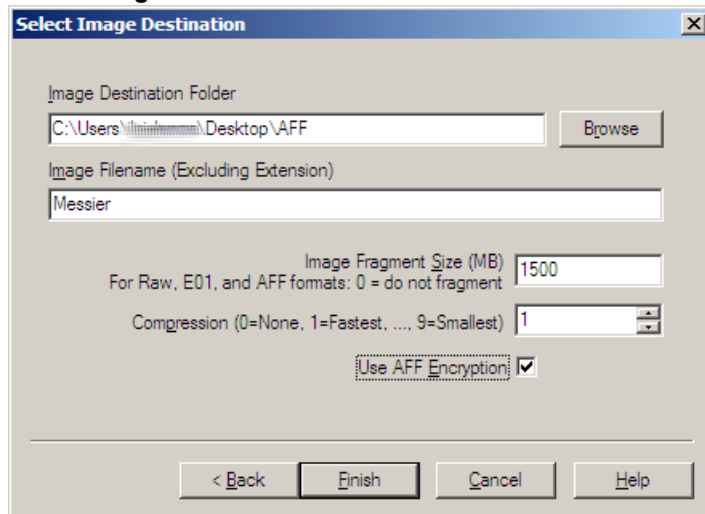
15. Click **Finish**.

    For more information, see Detecting EFS Encryption (page 33).

16. When AD Encryption is selected, you can choose between encrypting with a password, or encrypting with a certificate.

AD Encryption Credentials

If you use a password, you must type, then retype that password to confirm.

● Click **Show Password** to display the password in plain text as you type it the first time, to verify you are typing it correctly.

● Uncheck **Show Password** to replace the characters with asterisks.

16a. When AFF Encryption is selected, type the password, and retype the password to confirm.

AFF Encryption

16b. Click **Show Password** to see that you have typed it correctly the first time.

17. When encryption selections are made, click **OK** to save selections and return to the Create Image dialog.

18. To add another image destination (i.e., a different saved location or image file type), click **Add**, and repeat steps 4-14.

    - 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**.

19. Click **Start** to begin the imaging process.

20. After the images are successfully created, the *Drive/Image Verify Results* box shows detailed image information, including MD5 and SHA1 check sums, and bad sectors.
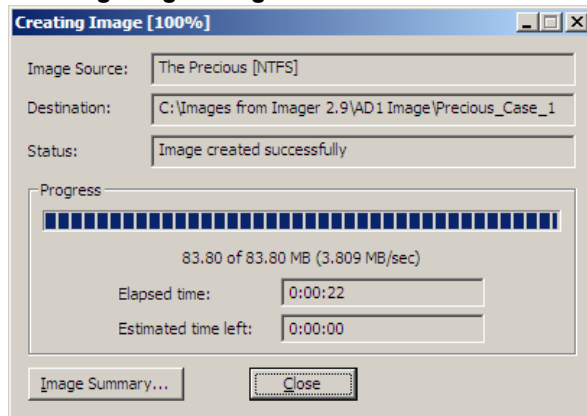
Drive/Image Verify Results
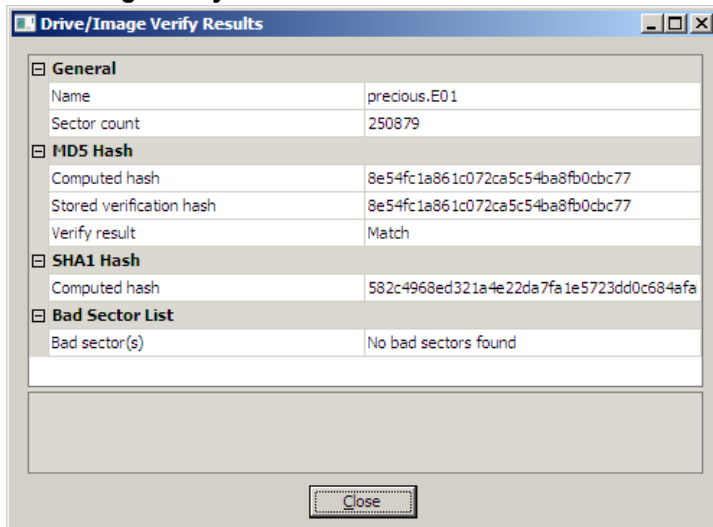
Note: The data displayed in the results box vary, according to the type of image created.

21. A progress dialog appears that shows the following:

Creating Image: Image

- 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
- Image Summary button. Click it to open the *Image Summary* window as shown below:

Image Summary
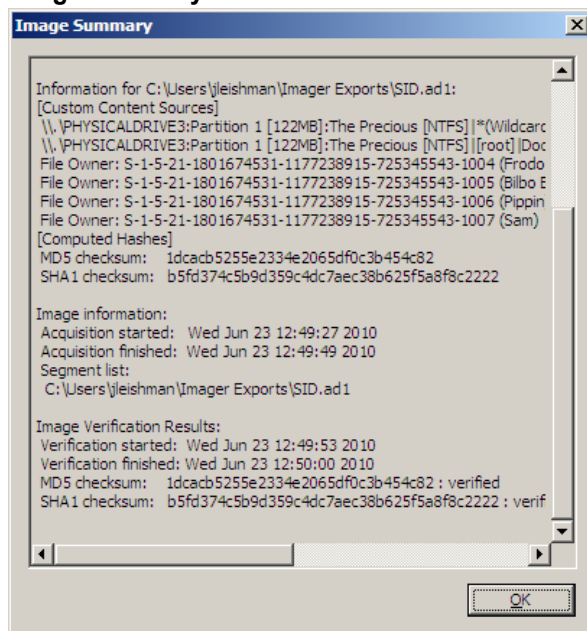
The Image Summary also includes the data you entered in the Evidence Item Information dialog.

22. Click **OK** to close the *Image Summary*.

23. Click **OK** to return to the *Creating Image* dialog.

24. Click **Close** to exit back to Imager.

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 exact 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 Content 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. Do one of the following:

   ● Click **File > Add to Custom Content Image**.

   ● 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.

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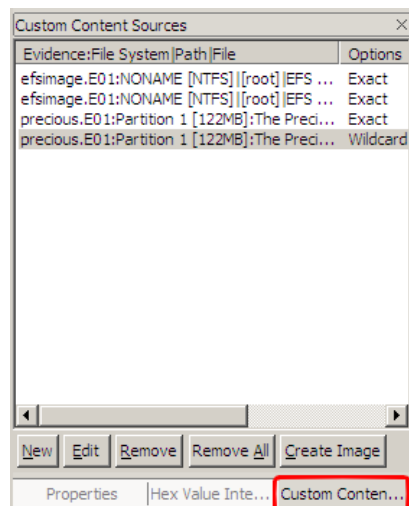
Note: The *Custom Content Sources* pane is dockable; that is, you can move it to any corner of the Imager window, or you can even undock it from the Imager window entirely, and drag it to a second monitor screen.

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.

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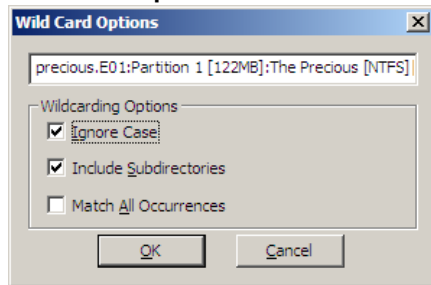
The *Wild Card Options* dialog box allows you to create filters to find specific files. In the path description field, you can type:

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

The following table shows examples of wild card filtering:

Wild Card Naming Examples

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** causes Imager to 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**.

Create Image
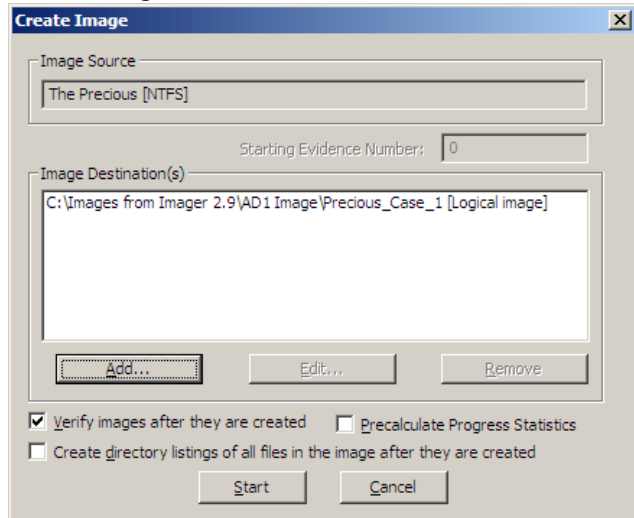
5. In the *Create Image* dialog box, specify options for this AD1 image.

6. Click **Add** to add a destination for the new Image.

7. Specify *Evidence Item Information.*
    All evidence item information is optional, but it is helpful to have the information easily accessible in case it is called into question at any time after creation.

The Evidence Item Information Dialog Box
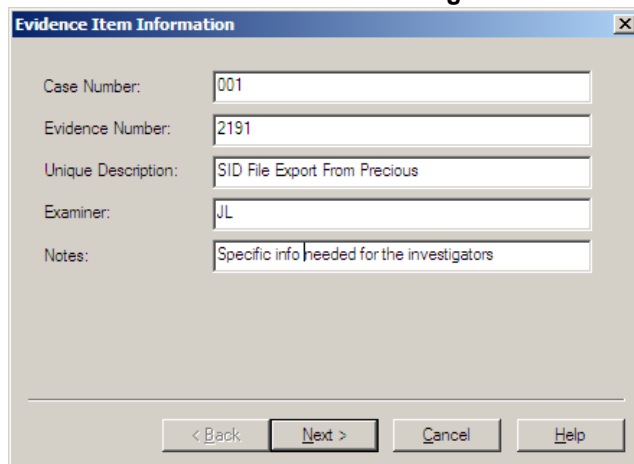
8. Click **Next**.

The Select Image Destination Dialog Box
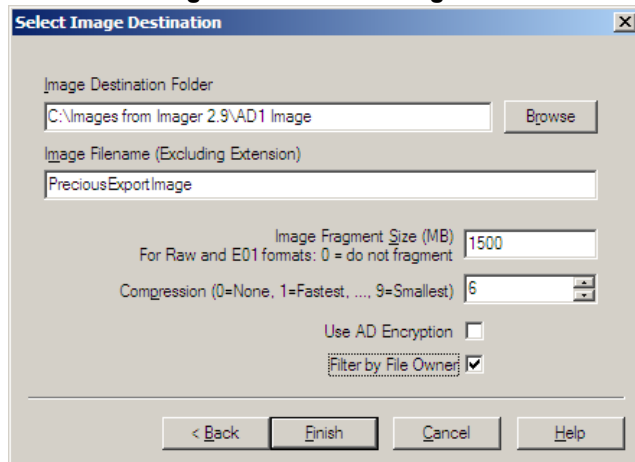
9. Complete the *Select Image Destination* dialog as follows:

   9a. Specify or browse to the destination folder.

   9b. Type the filename for the new Image, without an extension; the extension is determined by the image type selected and is added automatically.

   9c. Specify the Image fragment Size:

   - Default Image Fragment Size = 1500 MB
   - To save images segments that can be burned to a CD, specify 650 MB.
   - To save image segments that can be burned to a DVD, specify 4000 MB.
   - 0 creates a single-file (non-fragmented) image. Use this if you will never need to use smaller media for storage or transport of the image data.

     9d. Select the compression level to use.

   - 0=No Compression
   - 1=Fastest, Least Compression (faster, and also slightly smaller than a 0-compression file)
   - 9=Slowest, Most Compression (smallest file, slowest to create).
   - Numbers between 1 and 9 produce an image with varying levels of compression to speed ratio.

   9e. Choose whether to **Use AD Encryption.** For more information, see Step 9 under "Creating Forensic Images" beginning on page 36.

   9f. Choose whether to **Filter by File Owner**. For more information, see Exporting By SID (page 48).

10. Click **Finish** in the Select Image Destination dialog to save these settings and return to the Create Image dialog.

11. To add another image destination (i.e., a different, additional saved location), click **Add** and repeat steps 5 through 8.

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

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

14. Mark the additional options as desired:

   - Check **Verify Images after they are created** to check the image hash signature. This detects whether the content of the original data has changed since it was copied to the image.

   - Check **Create directory listings of all files in the image t**o 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.

15. Click **Start** to begin the export process. A progress dialog appears showing 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

Creating Image (Progress Window)
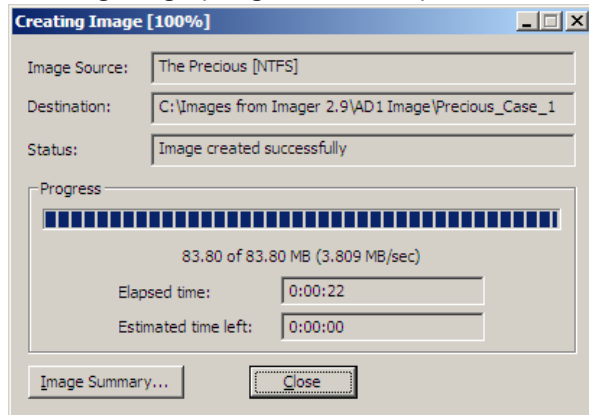
16. By default, when the image creation is complete, a status box opens to display a window showing the files and the hashes (MD5 and SHA1) of your custom image.

16a. Click **Close** when you are done viewing the hash information.

16b. Click **Close** again to return to the Creating Image dialog. At this point, the Status window will say Image Created Successfully.

17. Click **Image Summary** to open the Image Summary window that displays the Image Creation Log Evidence Item Information you entered at the beginning.

18. Click **OK** to return to the Creating Image dialog.

19. Click **Close** to exit back to Imager.

Exporting From FTK Imager

There are several ways to export data from FTK Imager. Each is discussed below.

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 from one format type to another. 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.

Note: This feature comes in handy if your OS fails, but the drive is still operational. Image your drive and export your data, photos, etc. from the image.

**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.
    - 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. Do one of the following:
    - Click **File > Export Files**.
    - Click the **Export Files** button on the *Toolbar*.
4. In the *Browse for Folder* dialog box, browse to the location where you want to save the exported files.
5. Click **OK**. The files are copied to the specified location.

Exporting By SID

Windows assigns unique identifiers to each process, user, machine, and so forth within its system. A system identifier (SID) is unique to the system, and most often applies to users.

The *Export to Logical Image (AD1)* and *Add to Custom Content Image (AD1)* features now allow the user to select and export files owned by particular SID(s), or add them to the image.
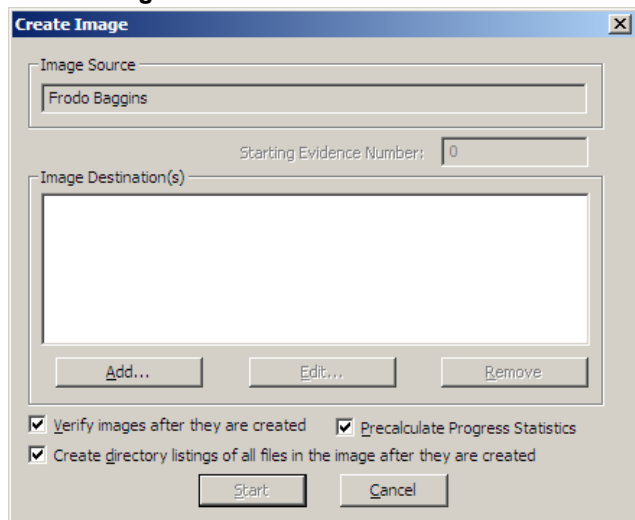
Select Image Destination
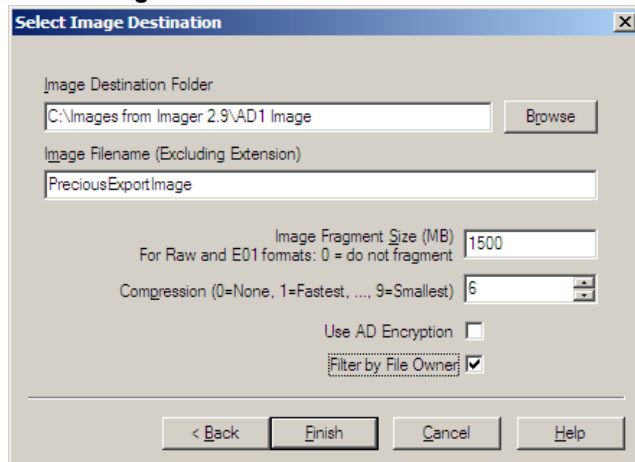
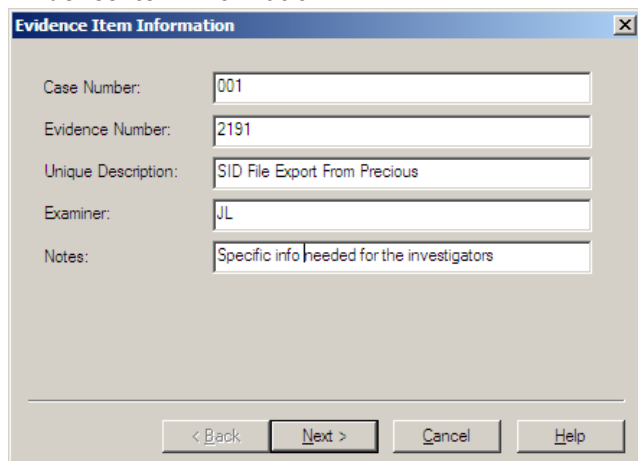**To export a list of files according to the SID of the file owner**

1. Begin by selecting an item from the *Evidence Tree*.

2. Right-click on the selected evidence item

3. Choose one of the following:

    ● **Export Logical Image (AD1)**

    ● **Add to Custom Content Image (AD1)**
        When added to a Custom Content Image, you will see the item in the Custom Content Sources box.

4. When all desired items are added to the *Custom Content Image*, click **Create Image**.
    This will take you to the same screen you would see if you had directly selected *Export Logical Image*.

5. In the *Create Image* dialog box, click **Add** to specify an image destination

Create Image.

6. Specify *Evidence Item Information.*
    All Evidence Item Information is optional, but it is helpful to have the information easily accessible in case it is called into question at any time after creation
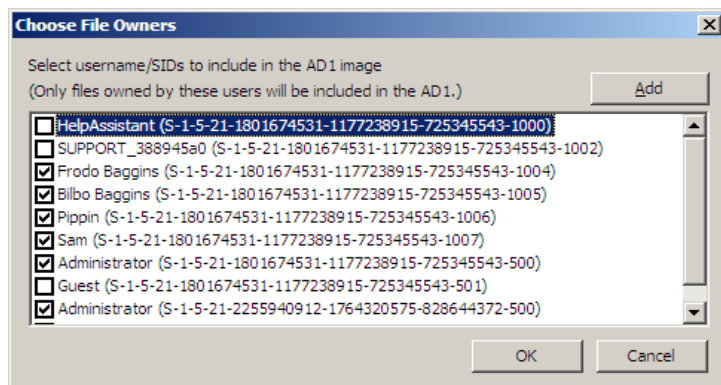

Evidence Item Information.

7. Click **Next**.

8. Specify *Image Destination Folder* and *Image Filename* (without extension)

9. Choose a fragment size for the image.

10. Choose a compression level based on the following information:

    ● 0=No Compression

    ● 1=Fastest, Least Compression (faster, and also slightly smaller than a 0-compression file)

    ● 9=Slowest, Most Compression (smallest file, slowest to create).

    ● Numbers between 1 and 9 produce an image with varying levels of compression to speed ratio.

11. Accept the default Image Fragment Size, or specify the Image Fragment Size to use.

    ● Default Image Fragment Size = 1500 MB

    ● To save images segments that can be burned to a CD, specify 650 MB.

    ● To save image segments that can be burned to a DVD, specify 4000 MB.

    ● 0 creates a single-file (non-fragmented) image. Use this if you will never need to use smaller media for storage or transport of the image data.

12. Mark **Use AD Encryption** if you wish to apply either passworded encryption or use a certificate for encryption for the resulting AD1 image file.

13. Mark **Filter by File Owner** to bring up a list of users found in the evidence that you can select from for exporting.

14. Click **Finish**.

Choose File Owners

15. In the *Choose File Owners* dialog box, mark the names of the Users and their SIDs whose files you want to export.

    15a. If the desired SID does not appear on the list, click **Add** to manually enter one.

        Copy and paste the SID from another location, or type it in manually. This allows a user to create an image containing files owned by the SID of a domain account.

> **Note:** User-entered SID(s)/Name(s) persist only as long as this instance of Imager is open.

16. Click **OK**.

    The exported file will be created in the destination you specified in Step 2.

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 sub folders are hashed.

> **Note:** Click the first, then Shift-click the last to select a block of contiguous files.
> Click one, then Ctrl-click individual files to select multiple non-contiguous files.
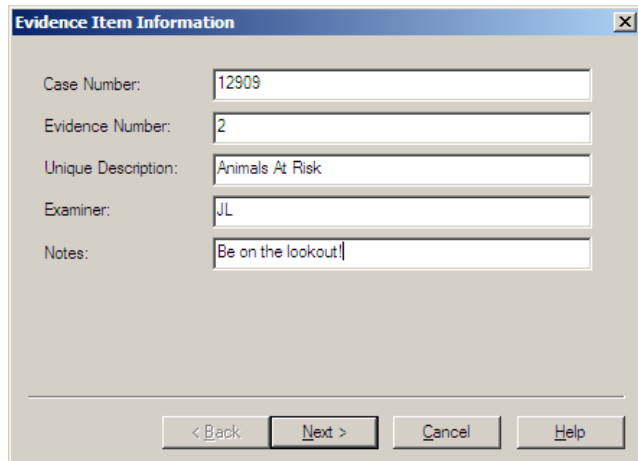
3. Do one of the following:

   - Click **File > Export File Hash List**

   - Click the **Export File Hash List** button ▤ on the *Toolbar*.

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

When creating or exporting a forensic image, you can enter information and notes about the evidence contained in the image you are creating. This information is saved to the same location as the image file, with the same name, but with a .TXT extension. For example, if your image were named AD1test.ad1, your Evidence Item Information would be saved in the same folder as AD1Test.ad1.TXT.

Evidence Item Information

You can enter the following information:

- The number of the case with which the evidence item is associated
- 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. Do one of the following:
   - Click **File > Export AD1 Logical Image,** or **Add to Custom Content Image (AD1)**
   - Right-click the folder and select **Export AD1 Logical Image** or **Add to Custom Content Image (AD1)** from the quick menu.
3. In the *Create Image* dialog, click **Add**.
4. Enter the Evidence Item Information as discussed above.
5. Click **Next**.
6. In the Image Destination Folder field, do one of the following:
   - Type the path for the new image file
   - Click **Browse** to select the desired location.

Important: 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. This works, however, all related image files must then 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 new image file, but do not specify an extension.
8. In the *Image Fragment Size* field, specify the maximum size in MB for each fragment of the new image file. Image Fragment Size has no maximum 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.

9. Click **Finish** to save these settings and exit to the Create Image dialog.

   9a. To add another image destination (i.e., a different, additional saved location), click **Add** and repeat steps 4-7.

   9b. To change an image destination, select the destination to change and click **Edit**.

   9c. To delete an image destination, select the destination and click **Remove**.

10. Mark the additional options as desired:

    ● Check **Verify Images after they are created** to check the image hash signature. This detects whether the content of the original data has changed since 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.

11. 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

Creating Image (Progress Dialog Box)
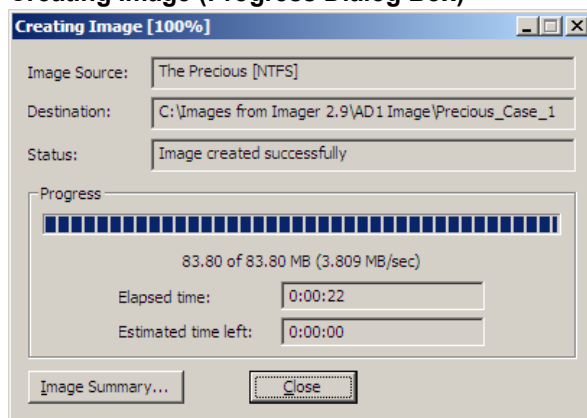
12. By default, when the image creation is complete, a status box opens to display a window showing the files and the hashes (MD5 and SHA1) of your custom image.

13. Click **Close** when you are done viewing the hash information.

14. Click **Close** again to return to the Creating Image dialog. At this point, the Status window will say Image Created Successfully.

15. Click **Image Summary** to open the Image Summary window that displays the *Image Creation Log* showing the Evidence Item Information you entered at the beginning.

16. Click **OK** to return to the Creating Image dialog.

17. Click **Close** to exit back to Imager.

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. Do one of the following:
   - Click **File > Export Directory Listing**.
   - Click the **Export Directory Listing** button .
3. Select the location for the saved file, and type in a file name.
4. Click **Save**.

Decrypting AD1 Images

You can use Imager to decrypt AD1 images that have AccessData encryption.

To decrypt AD1 images

1. Open AccessData FTK Imager.
2. Click **File > Decrypt AD1 Image**.
3. In the *Choose a file/image to encrypt or decrypt* dialog, browse to the location of the AD1 encrypted image, select it, and click **Open**.
4. In the *Save decrypted file/image* to dialog, browse to the location where you want to store the decrypted AD1 image and click **Save**.
5. In the *AD Encryption Credentials* dialog, enter the password for the encrypted image and click **OK**.
6. After the decryption process completes, in the *AD Encryption Decryption* dialog, click **OK**.

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. Do one of the following:

   - Click **File > Verify Drive/Image**.

   - Click the **Verify Drive/Image** button ⊟ on the *Toolbar*.

   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
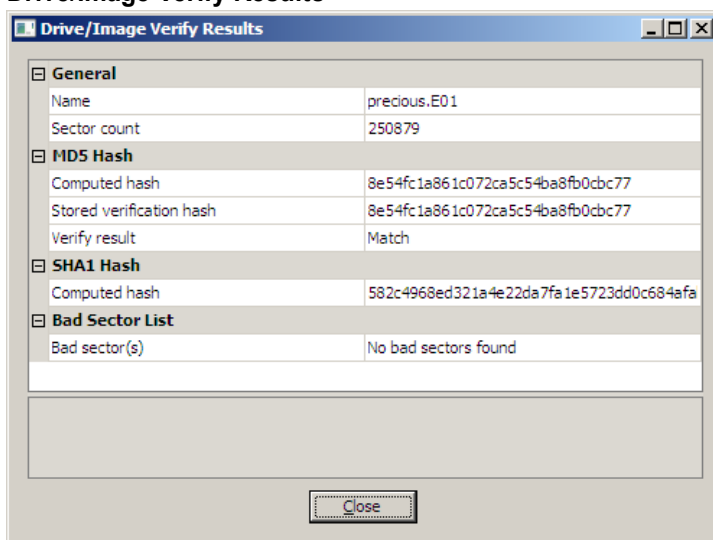
   - Estimated time remaining until the process is complete

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

Drive/Image Verify Results

   - 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

You can copy any of the results on the Verify Results screen (for example, the MD5 or SHA1 hash values).

To copy data from the Verify Results screen

1. Click the result to highlight it

2. Right-click and select **Copy** from the quick menu.

3. 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, and click **Add**.
7. On the *Create Custom Content Image* dialog, click **Create Image**.

Appendix A File Systems and Drive Image Formats

This appendix lists the file systems and image formats that AD Imager recognizes.

File Systems

The following table lists AccessData Imager-identified and analyzed file systems:

Identified and Analyzed File Systems

● APFS	● HFS
● CDFS	● HFS+
● exFAT	● NTFS
● Ext2FS	● ReiserFS3
● Ext3FS	● VXFS
● Ext4FS	● XFS
● FAT12, FAT16, FAT32	

Whole Disk Encrypted

The following table lists AccessData Imager-identified and analyzed Whole Disk Encryption (WDE) decryption products (these all require the investigator to enter the password, AccessData forensic products don't "crack" these):

Recognized and Analyzed Whole Disk Encryption Formats

● PGP®	● Utimaco
● Credant	● Guardian Edge
● SafeBoot	● EFS
● JFS	● LVM
● VMware	● LVM2
● UFS1	● UFS2

Hard Disk Image Formats

The following table lists AccessData Imager-identified and analyzed hard disk image formats:

Identified and Analyzed Hard Disk Image Formats

● Encase, including 6.12	● SnapBack
● Safeback 2.0 and under	● Expert Witness
● Linux DD	● ICS
● Ghost (forensic images only)	● SMART
● AccessData Logical Image (AD1)	● Advanced Forensics Format (AFF)

CD and DVD Image Formats

The following table lists AccessData Imager-identified and analyzed CD and DVD image formats:

Identified and Analyzed CD and DVD File Systems and Formats

● Alcohol (*.mds)	● IsoBuster CUE
● PlexTools (*.pxi)	● CloneCD (*.ccd)
● Nero (*.nrg)	● Roxio (*.cif)
● ISO	● Pinnacle (*.pdi)
● Virtual CD (*.vc4)	● CD-RW,
● VCD	● CD-ROM
● DVD+MRW	● DVCD
● DVD-RW	● DVD-VFR
● DVD+RW Dual Layer	● DVD-VR
● BD-R SRM-POW	● BD-R DL
● BD-R SRM	● CloneCD (*.ccd)
● HD DVD-R	● HD DVD-RW DL
● SVCD	● HD DVD
● HD DVD-RW	● DVD-RAM,
● CD-ROM XA	● CD-MRW,
● DVD+VR	● DVD+R
● DVD+R Dual Layer	● BD-RE
● DVD-VRW	● BD-ROM
● HD DVD-R DL	● BD-R RRM
● BDAV	● Pinnacle (*.pdi)
● HD DVD-RAM	● ISO
● CD-R	● Virtual CD (*.vc4)
● SACD	● DVD+RW
● DVD-ROM	● VD-R
● DVD-VM	● DVD-R Dual Layer
● DVD+VRW	● BD-R SRM+POW
● BD-R	● BD-RE DL

Appendix B 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 > Logicube Forensic MD5**.

4. In the Logicube MD5 dialog box, 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.

# Appendix C 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 when you are adding evidence to a case.
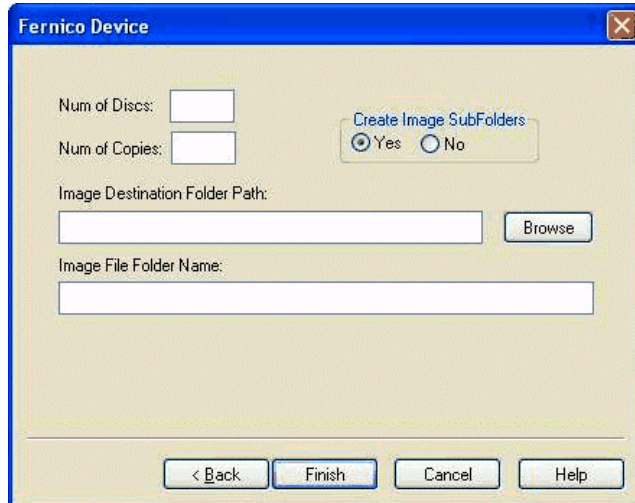
Select Source
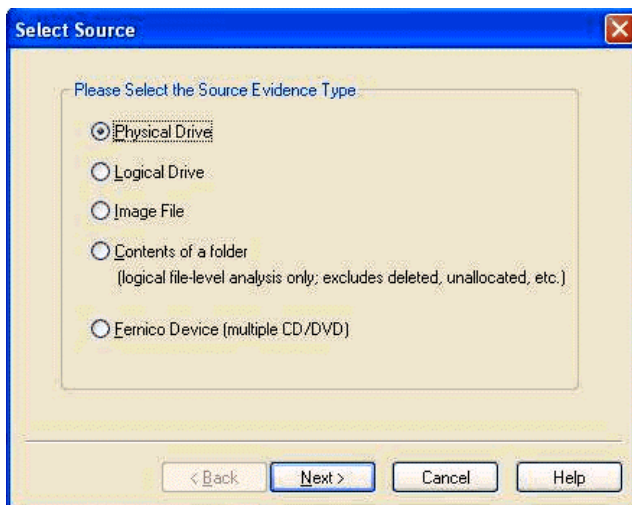
To access the Fernico FAR system
1. Select the Fernico Device (multiple CD/DVD), and then click Next. The Fernico Device dialog opens.

Fernico Device

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 sub folders by default. Select the **No** radio button if you don't want sub folders 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 that came with your Fernico FAR System.