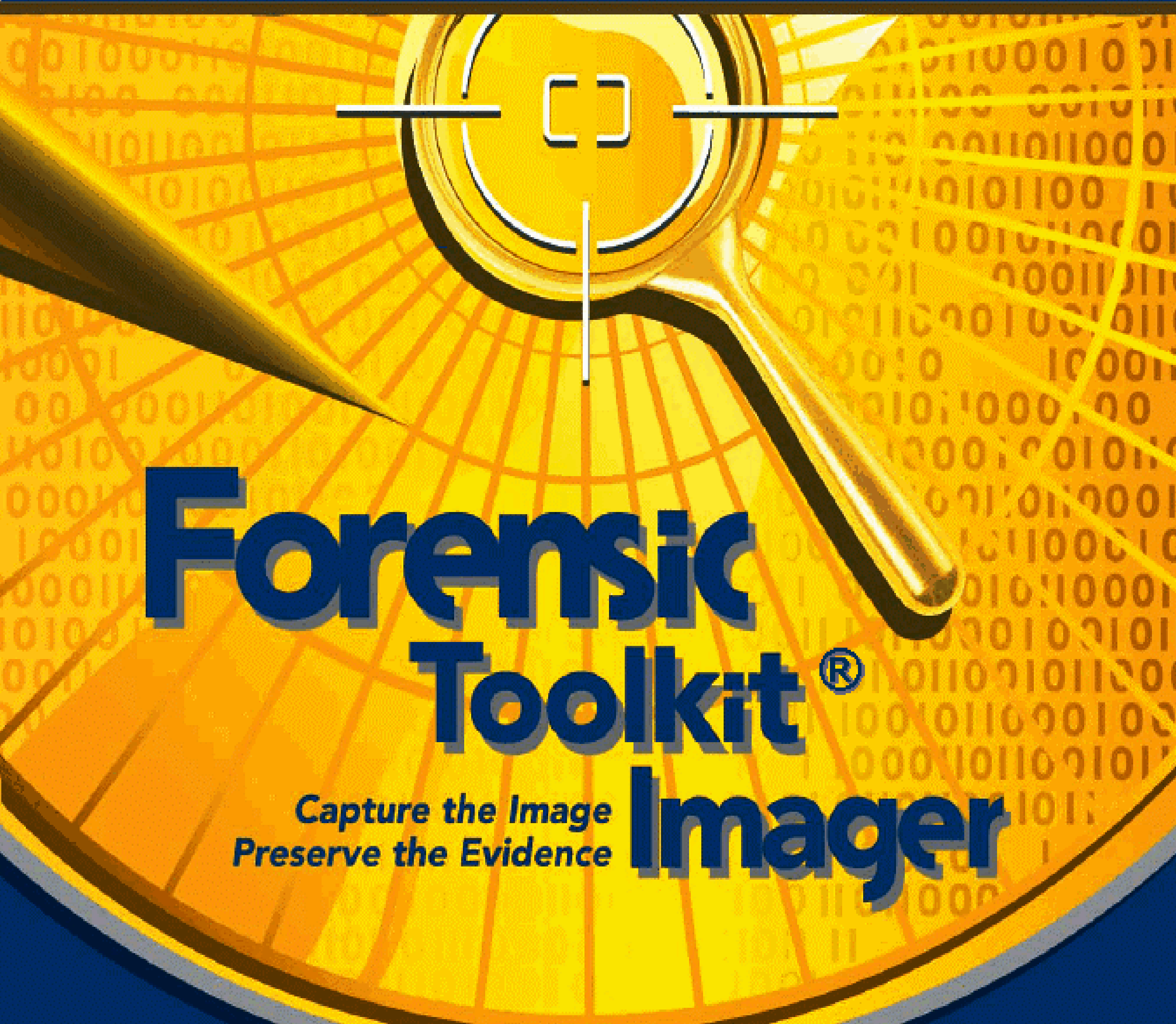
USER GUIDE

Find, Organize, & Analyze Computer Evidence



Forensic Toolkit® Imager

Capture the Image
Preserve the Evidence

AccessData

Legal Notices

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

Forensic Toolkit is a registered trademark of AccessData Corp.
FTK is a trademark of AccessData Corp.
FTK Imager is a trademark of AccessData Corp.
LicenseManager is a trademark of AccessData Corp.

Third-Party Trademarks

All third-party trademarks are the property of their respective owners.

CONTENTS

FTK Imager

Chapter A Supported Image Formats

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
- Preview the contents of forensic images stored on the local machine or on a network drive
- Export files and folders from forensic images.
- 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 free space.

When you acquire computer evidence, you can use FTK Imager to create an image of the source drives or files. You 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. FTK Imager verifies that the image hash and the drive hash match when 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 FTK to perform a complete and thorough forensic examination and create a report of your findings.

FTK Imager Interface

The FTK Imager interface window is divided into seven 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, and then Reset docked windows.

Menu Bar

Use the menu bar to access all the features of FTK Imager.

From the File menu you can access features such as the Add Evidence Item wizard, the Create Disk Image wizard, and the Export File Hash List feature. The View menu allows you to customize the appearance of FTK Imager, including showing or hiding panes and control bars. 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.

To show or hide the menu bar, select View, and then Menu Bar. You can also right-click the menu bar to access the menu.

The Command Line

Imager supports four command line options:

- /CreateDirListing= creates a directory listing
- /VerifyImage= verifies an image
- /EnableDebugLog= enables logging to the FTKImageDebug.log file

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

Preview Modes

FTK Imager offers three modes for previewing electronic data:

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 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.

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 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.

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. Underneath each source are the folders and files it contains.

Click the plus sign next to a source or folder 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.

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

Adding Evidence Items

To add an evidence item to the Evidence Tree:

1 Click **File**, and then **Add Evidence Item**, or click the button on the tool bar.

2 Select the source you want to preview and click **Next**.

3 Select the drive or browse to the source you want to preview, and then click **Finish**. The evidence item appears in the Evidence Tree.

4 Repeat these steps to add additional evidence items.

Adding All Attached Devices

You can add data from the devices attached to a machine by clicking File, and then Add All Attached Devices, or by clicking the button.

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

Removing Evidence Items

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**, and then **Remove Evidence Item**, or click the button on the tool bar. The evidence item is removed from the Evidence Tree. To remove all evidence items at once, click **File**, and then **Remove All Evidence Items**, or click the button on the tool bar.

Obtaining Protected Registry Files

The Windows operating system does not allow you to copy or save live registry files. 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 drive. FTK Imager provides a much easier solution. It bypasses the Windows operating system and allows you to copy registry files underneath the Windows file lock.

To obtain the protected registry files using FTK Imager:

1. Launch FTK Imager.
2. Click **File**, and then **Obtain Protected Files**, or click the button on the toolbar.
3. Designate a destination directory and file options, then click **OK**.

    - 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.

    FTK Imager exports the selected files to the designated location.

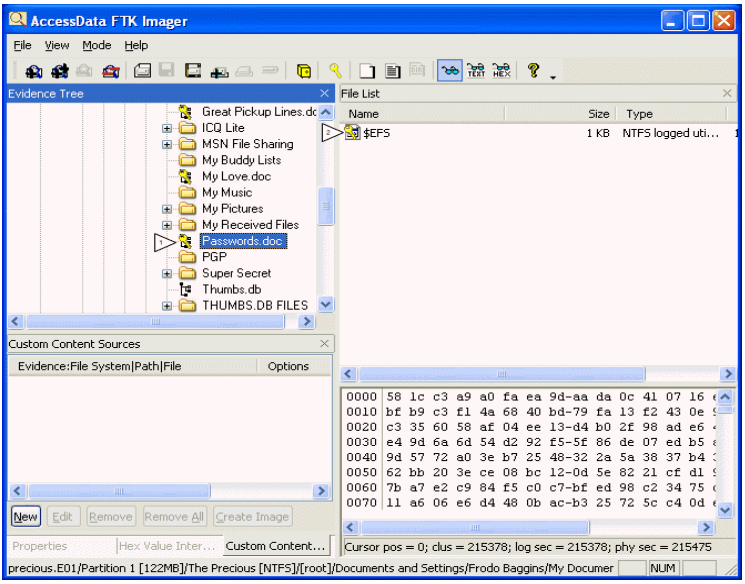
4. Add the files to the case.

5 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.

Detecting EFS Encryption

You can check for encrypted data on a physical drive or an image with FTK Imager. The information is displayed in the Explore and File List windows with the key icon:



Name	Size	Type
$EFS	1 KB	NTFS logged uti...

```
0000 58 1c c3 a9 a0 fa ea 9d-aa da 0c 41 07 16
0010 bf b9 c3 f1 4a 68 40 bd-79 fa 13 f2 43 0e
0020 c3 35 60 58 af 04 ee 13-d4 b0 2f 98 ad e6
0030 e4 9d 6a 6d 54 d2 92 f5-5f 86 de 07 ed b5
0040 9d 57 72 a0 3e b7 25 48-32 2a 5a 38 37 b4
0050 62 bb 20 3e ce 08 bc 12-0d 5e 82 21 cf d1
0060 7b a7 e2 c9 84 f5 c0 c7-bf ed 98 c2 34 75
0070 11 a6 06 e6 d4 48 0b ac-b3 25 72 5c c4 0d
```

Cursor pos = 0; clus = 215378; log sec = 215378; phy sec = 215475

precious.E01/Partition 1 [122MB]/The Precious [NTFS]/[root]/Documents and Settings/Frodo Baggins/My Documer

To detect encrypted files, click **Detect Encryption** from the File menu, or click the 🔑 button on the tool bar. The program will scan the evidence and notify you if encrypted files were located.

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.

To create a forensic image:

1 Click **File**, and then **Create Disk Image**, or click the button on the tool bar.

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**.

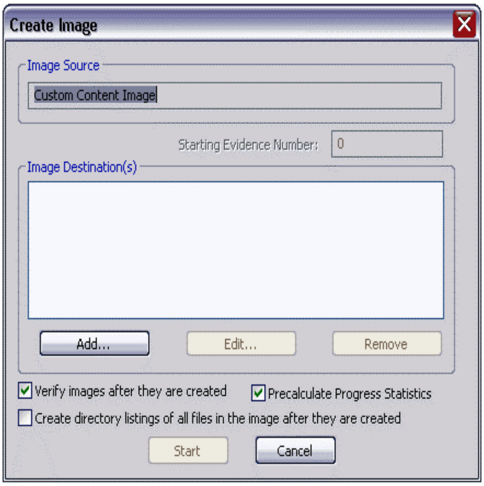


Image Source: Custom Content Image

Starting Evidence Number: 0

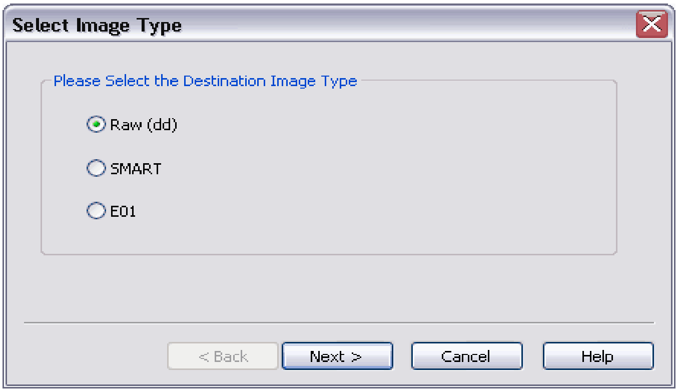
☑ Verify images after they are created ☑ Precalculate Progress Statistics

□ 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.
- 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, and 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 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**.

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

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.

Tip: If you want to transfer the image file to CD, accept the default fragment size of 650 MB.

9 Click **Finish**. You 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 make changes to 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 after the imaging process began
- Estimated time left 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

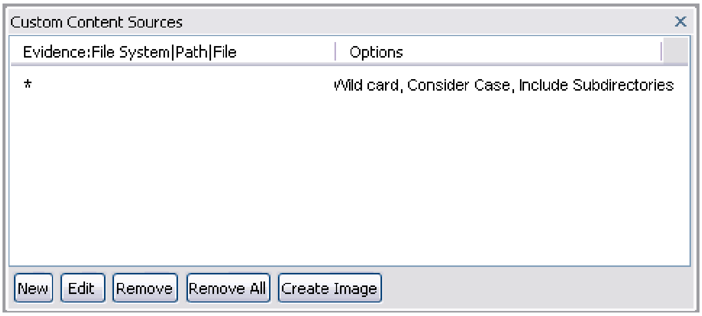
FTK Imager allows you to customize your image to decrease the time and memory required to store important information and evidence. With the Custom Content Image feature, you can select specific files from a live file system or an existing image to make a smaller, more specific image. You can also search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

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

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 move to an image.

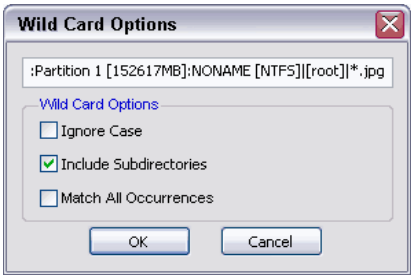
2 From the File menu, click **Add to Custom Content Image**, or right-click each item to open the Export menu. The item is listed in the Custom Content sources pane. Repeat this step until you've collected the evidence you want.



Evidence:File System|Path|File	Options
*	Wild card, Consider Case, Include Subdirectories

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.

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

:Partition 1 [152617MB]:NONAME [NTFS]|[root]|*.jpg

Wild Card 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:

- The question mark (?) to replace any single character in the file name and extension
- The asterisk (*) to replace any series of characters in a file name and extension

Note: Use the pipe character to separate directories and files.

The check box options can be used individually or combined 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 My Documents folder.

Other examples of wild card filtering:

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

3 When your list is ready, you can create the custom content image. From the File menu, click **Create Custom Content Image,** or click the button from the tool bar, or click **Create Image** on the Custom Content pane. The Create Custom Content dialog opens.

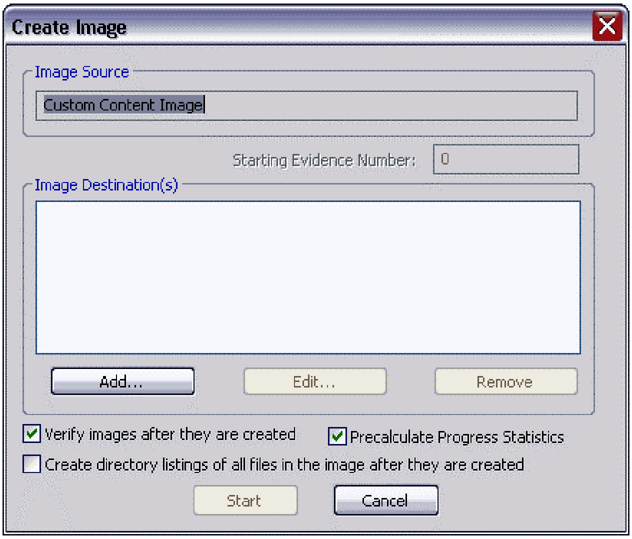

Create Image

Image Source: Custom Content Image

Starting Evidence Number: 0

Image Destination(s)

☑ Verify images after they are created

☑ Precalculate Progress Statistics

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

Click **Add** to specify the location to which you want to save the image file.

Use the Edit button to change the destination. You can also choose to verify images as you create them, calculate progress statistics, and create a list of the files contained in your image.

4 Click **Start** when you are ready to create the custom image.

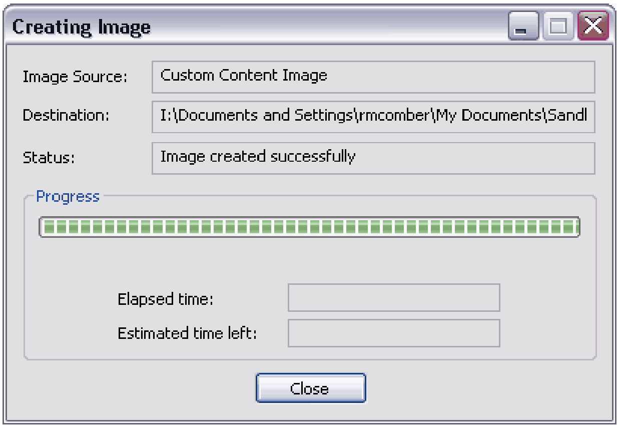


Image Source: Custom Content Image
Destination: I:\Documents and Settings\rmcomber\My Documents\Sandl
Status: Image created successfully
Elapsed time:
Estimated time left:

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

Exporting Forensic Images

To export or convert an existing image file to a different format, follow the same steps as creating a forensic image. The difference is that exporting a forensic image takes its source from the evidence tree, while creating a forensic image provides a wizard to select the source.

Exporting Files

Exporting or copying files from an evidence item allows you to print, e-mail, or organize the 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.

Tip: Shift-click to select a block of adjacent files. Ctrl-click to select a series of non-adjacent files.

3 Select File, and then Export Files, or click the 🗋 button on the tool bar.

4 In the Browse for Folder dialog, browse to the location where you want to export the 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.

Tip: Shift-click to select a block of adjacent files. Ctrl-click to select a series of non-adjacent files.

3 Select File, and then Export File Hash List, or click the 🗎 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.

Exporting Logical Images

FTK Imager gives you the option of exporting a logical image of a single folder. Although a logical image is not a true forensic image (i.e., it does not include slack space), exporting a logical image allows you to easily save specific information for future reference.

To export an AD1 logical image:

1 In the Evidence Tree, select the folder you want to export as a logical image.

2 Select File, and then Export AD1 Logical Image.

Tip: You can also 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 where you want to save the new image file, or click **Browse** to find 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.

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 no size limit.

Tip: If you want to copy the image file to CD, accept the default 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.

7 Click **Finish**. You return to the Create Image dialog.

8 Click **Add** to specify a destination for your custom image. After you have specified a destination, you can edit or remove by highlighting it and clicking **Edit** or **Remove**.

- 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 how much time and storage space creating the custom image will require before you start.

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

To make changes to an image destination, select the destination you want to change and click **Edit**.

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

10 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 after the export process began
- Estimated time left until the process is complete

11 When the Status field reads “Image created successfully,” click **Close**.

You can also view the files and the hashes (MD5 and SHA1) of your custom image by clicking the **Image Summary** button.

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. From the File menu, click **Export Directory Listing**, or click the icon.
3. Select the location to save the 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. Select File, and then Verify Drive/Image, or click the 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 left until the process is complete
3. Once the verification process has successfully completed, the Drive/Image Verify Results summary screen appears, showing the:

- Name of the drive or image that was verified
- Number of sectors in the drive or image
- MD5 hash that was computed for the drive or image
- SHA1 hash that was computed for the drive or image

If you verified an image that contains its own hash value, such as a SMART or EnCase image, the following information is also displayed:

- The hash value stored inside the image
- Whether the hash value stored in the image matches the hash value computed by FTK Imager

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

Properties/Hex Value Interpreter

FTK Imager's lower-left pane has two tabs: Properties and Hex Value Interpreter.

The Properties tab displays a variety of information about the object currently selected in the Evidence Tree or File List. Properties include information such as object type, size, and location on the storage media, flags, and timestamps.

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

Importing Sets of Files

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

For example, if you're tracing 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, then select the files you want to include in the new image, and then click **Add**.

6 On the Create Custom Content Image dialog, click **Create Image**.

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 left 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.

Accessing 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.

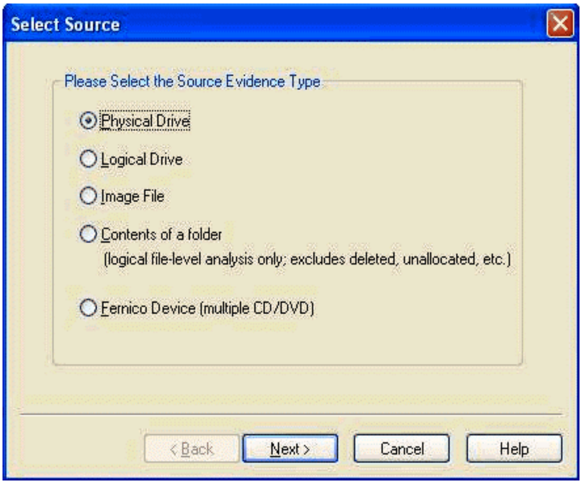
Integrating a Fernico FAR System

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.

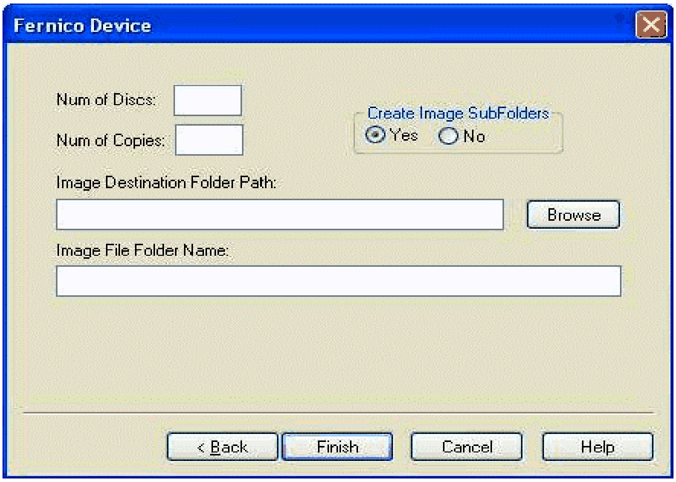
Accessing the Fernico FAR System from Imager

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)
< Back
Next >
Cancel
Help

To access the Fernico FAR system:

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



2 In the **Num of Discs** field, type the amount of discs loaded into the device.

3 In the **Num of Copies** field, type the amount of copies to be places on the discs.

4 The Fernico device will image all subfolders by default. You can 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 information on the Fernico FAR System, see the Fernico documentation.

Comments

We value your feedback. Please report any errors to: documentation@accessdata.com .

APPENDIX A

Supported Image Formats

FTK® Imager supports these file systems and image formats:

File Systems	FAT 12, FAT 16, FAT 32 NTFS Ext2, Ext3 HFS, HFS+ Reiser
Hard Disk Image Formats	Encase SnapBack Safeback 2.0 and under Expert Witness Linux DD ICS Ghost (forensic images only) SMART VMWare

CD and DVD Image Formats	Alcohol (*.mds) CloneCD (*.ccd) ISO IsoBuster CUE Nero (*.nrg) Pinnacle (*.pdi) PlexTools (*.pxi) Roxio (*.cif) Virtual CD (*.vc4)
Logical Image Formats	AD1 Custom Content Image