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.

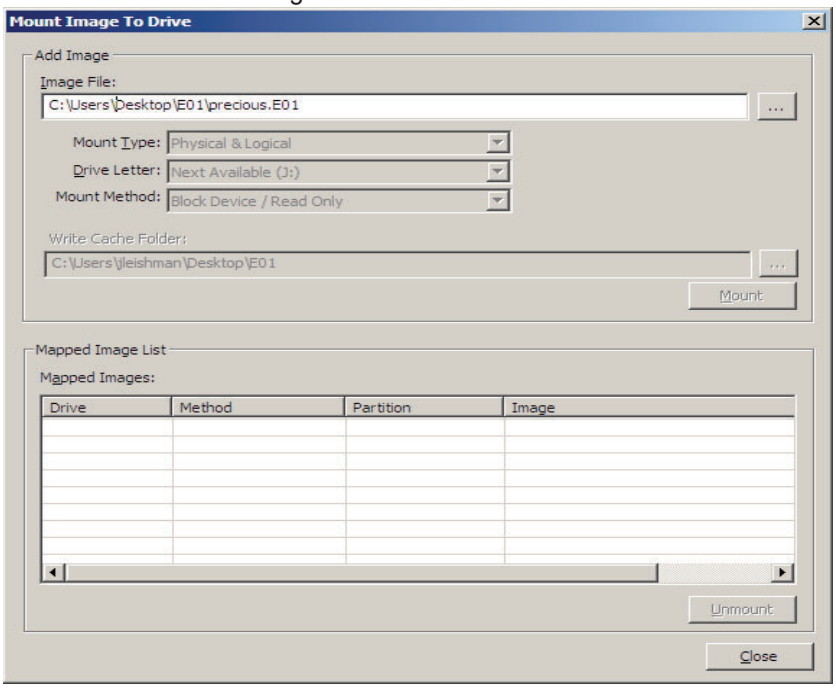
   If you do not already have the desired image added as evidence, begin with Step 2.

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.

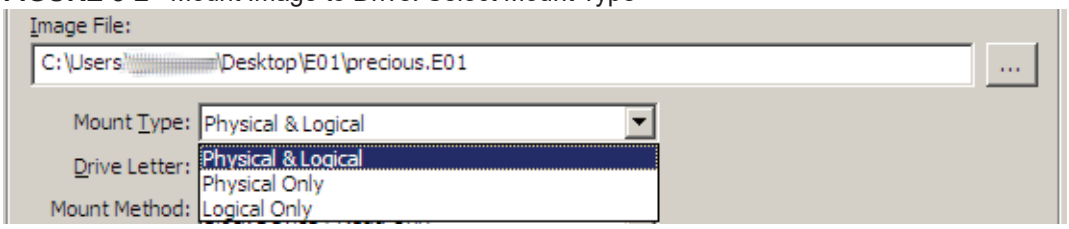
   After selecting an image, the Mount Type will default to the supported mapping based on the image type selected. Click the drop-down to display other available Mount Types.

FIGURE 5-1 Mount Image to Drive



4. Select the *Mount Type* to use for mounting.

FIGURE 5-2 Mount Image to Drive: Select Mount Type

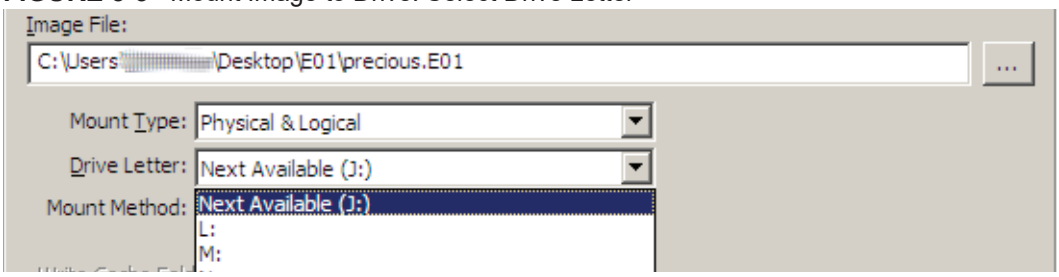


Available Mount Types are *Physical & Logical*, *Physical Only*, and *Logical Only*.

If the *Mount Type* selected includes *Logical*, you can select the Drive Letter to assign as the mount point.

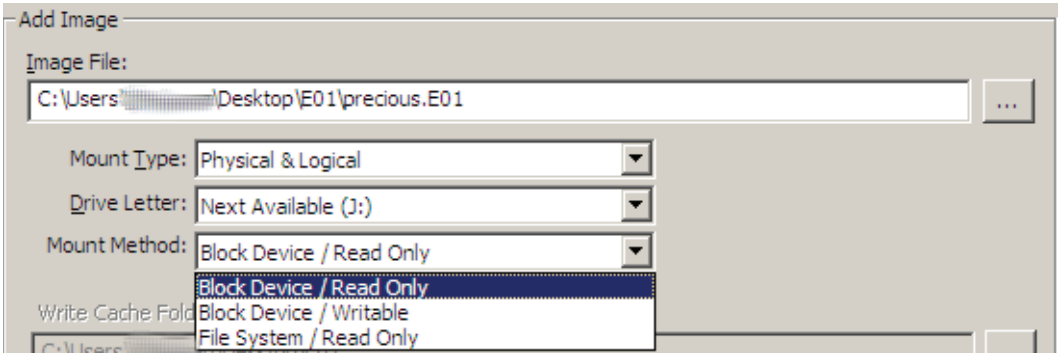
5. Click the Drive Letter drop-down to see all drive letters that are available for assignment to the mounted image

FIGURE 5-3 Mount Image to Drive: Select Drive Letter



6. Select the drive letter to use for this mounting.
7. Click the *Mount Method* drop-down to select from the available Mount Methods.

FIGURE 5-4 Mount Image to Drive: Select Mount Method



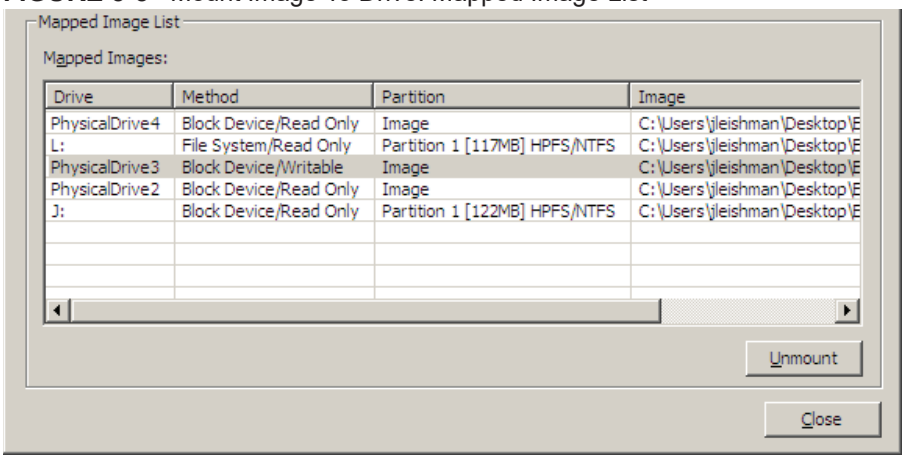
Available Mount Methods are shown and described in the following table:

TABLE 5-1 Mount Image: Mount Methods

Mount Method	Description
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*.

FIGURE 5-5 Mount Image To Drive: Mapped Image List



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.