2. Click either **Calculate**, or **Verify** according to what displays in the Command column, to begin hashing the evidence file.

The *Progress* dialog appears and displays the status of the verification. If the image file has a stored hash, when the verification is complete, the dialog shows and compares both hashes. Completing these processes may take some time, depending on the size of the evidence, the processor type, and the amount of available RAM.

Mounting an Image to a Drive

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, 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: Encrypted images cannot be mounted as either a drive or physical device.

Benefits of Image Mounting

The ability to mount an image with AccessData forensic products provides the following benefits:

- Mount a full disk image with its partitions all at once; the disk is assigned a Physical Drive name and the partitions are automatically assigned a drive letter beginning with either the first available, or any available drive letter of your choice.
- A full disk image mounted physically, and assigned a Physical Drive name that can be read using Imager or with any Windows application that performs Physical Name Querying.
- Mount images of multiple drives and/or partitions. The mounted images remain mounted until unmounted or until Imager is closed.
- Mounted images can be easily unmounted in any order, individually, or all at once.
- A logically mounted image may be viewed in Windows Explorer as though it were a drive attached to the computer, providing the following benefits:
  - File types with Windows associations can be viewed in their native or associated application, when that application is installed locally.
  - Anti-virus applications can be run on the mounted image.
  - Because the logically mounted image is seen as a drive in Windows Explorer, it can be shared, and viewed from remote computers when Remote Access has been configured correctly.
  - Files can be copied from the mounted image to another location.
- Mount NTFS / FAT partitions contained within images as writable block devices. This feature caches sections of a read-only image to a temporary location allowing the user to “write” to the image without compromising the integrity of the original image.

  Once mounted via the write cache mount method, the data can then be leveraged by any 3rd party tools which require write access.

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 or 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, and 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; the disk image partitions can be mounted Logically.

Mounting an Image as Read-Only

To mount an image

1. If you already have the desired image added as evidence in the case, 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:
   - Right-click and choose **Mount Image to Drive.**
   - Select the image from the Evidence tree. Right-click and choose **Mount Image to Drive**.
   - Click **Tools > Mount Image to Drive,** then browse to the image on your local drive or on a network drive you have access to.
3. Enter 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. After selecting an image, the Map Type will default to the supported mapping based on the image type selected. Click the drop-down to display other available map types.
4. Select the Mount Type to use for mounting.

   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.
6. Click the *Mount Method* drop-down to select **Block Device / Read Only** or **File System / Read Only**.

Note: If you are mounting an HFS image of a Mac drive, you must choose **File System / Read Only** to view contents of the drive. Otherwise, it will appear empty, and may prompt you to format the drive.

7. Click **Mount**.

   All the related mount information will be displayed in the 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 the program is closed.

8. Click **Close** to return to the main window.

Mounting a Drive Image as Writable

When mounting an image as writable, you must be working with a physical image, and the mount type you select must be Physical & Logical. This is the only option that provides the **Block Device /Writable** Mount Method.

To mount a drive image as writable

1. In the *Examiner*, click **Tools > Mount Image to Drive**.
2. Select a full disk image such as 001/Raw dd, E01, or S01 file type.
3. In the *Mount Type* drop-down, select **Physical & Logical**.
4. In the *Drive Letter* drop-down, select **Next Available** (default), or select a different drive letter.

Note: Check your existing mappings. If you map to a drive letter that is already in use, the original will prevail and you will not be able to see the mapped image contents.

5. In the *Mount Method* drop-down, select **Block Device / Writable**.
6. In the *Write Cache Folder* text box, type or click **Browse** to navigate to the folder where you want the Write Cache files to be created and saved.
7. Click **Mount.**

   You will see the mapped images in the Mapped Image List.

To view or add to the writable mapped drive image

1. On your Windows desktop, click **Start > Computer** (or **My Computer**).
2. Find the mapped drive letter in your Hard Disk Drives list. It should be listed by the name of the Image that was mounted, then the drive letter.
3. Double-click on it as you would any other drive.
4. As a test, right-click and choose **New > Folder.**
5. Enter a name for the folder and press **Enter**.
6. The folder you created is displayed in the Folder view.
7. Mapped images remain mapped until unmapped, or until the application is shut down.

Unmounting an Image

To unmount a mounted image

1. Click **File > Image Mounting.** The *Map Image to Drive* dialog opens.
2. Highlight the images to unmount, click **Unmount.** To unmount multiple mappings, click the first, then Shift-click the last to select a block of contiguous mappings. Click a file, then Ctrl-click individual files to select multiple non-contiguous mappings.)
3. Click **Done** to close the *Map Image to Drive* dialog.

Restoring an Image to a Disk

A physical image such as 001 (RAW/dd), E01, or S01, can be restored to a drive of equal or greater size to the original, un-compressed drive.

To restore an image to a disk

1. Connect a target drive to your computer.
2. In the *Examiner*, click **Tools > Restore Image to Disk**.
3. Click **Browse** to locate and select the source image. It must be a full-disk image such as 001 (Raw/dd), E01, or S01.

   The source image must be a disk image. A custom content image such as AD1 will not work for this feature.
4. Click the *Destination Drive* drop-down, select the target drive you connected in Step 1. If you do not see that drive in the list, click **Refresh**.
5. Mark the **Zero-fill remainder of destination drive** check box if the drive is larger than the original un-compressed drive.
6. Mark the **Notify operating system to rescan partition table when complete** check box to allow the new drive to be seen by the OS. If you plan to connect the drive in a different computer there is no need to do this step.

   When you are finished selecting options, click **Restore Image** to continue.

Performing Final Carve Processing

When you have selections saved as carved files from any file in the Hex viewer, performing Final Carve Processing carves the files, saves them, adds them to the case, and even creates or assigns them to bookmarks you specified when the data was selected.

Final Carve Processing jobs can be monitored in the Progress Window as Additional Analysis Jobs.