Creating an Evidence File

CREATING AN EVIDENCE FILE FROM A FLOPPY DISKETTE

An evidence file can be created from any type of media that the computer system recognizes. Similar procedures are used to image various types of media. This lesson begins by discussing specific procedures to acquire a floppy diskette and then discusses options that apply to other media.

Perform the following before inserting a floppy diskette into the laboratory machine:

1. Write-protect the floppy (you should see light through both holes)
2. Inspect the floppy for damage especially on the slide
3. Label the floppy with a tag or marker

With a case open within EnCase® Forensic (EnCase), select the **Add Device** icon.

Place the floppy in the lab machine's floppy drive, and place a check in the **Local Drives** box in the Table Pane.

Click **Next>**.

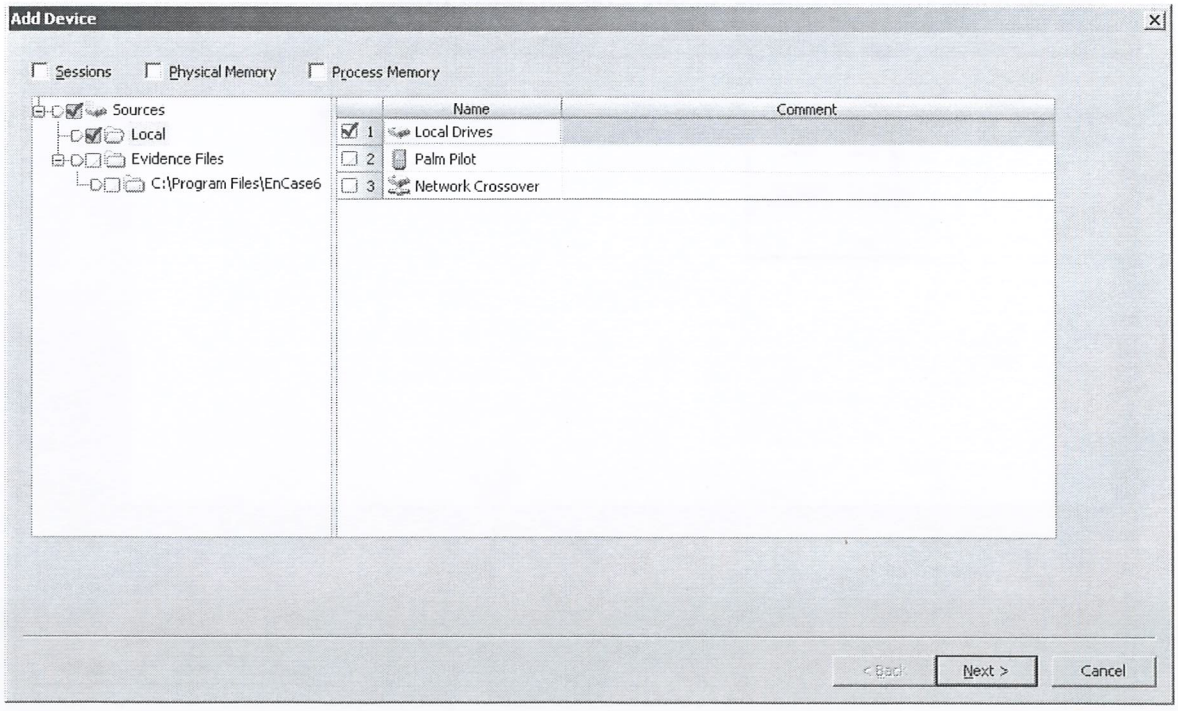

Figure 3-1 Selecting a local drive

The local devices will be displayed in the following dialog box. Select the Local Drives folder in the Tree Pane, then put a check in the checkbox next to the A in the Table Pane and click **Next>**.

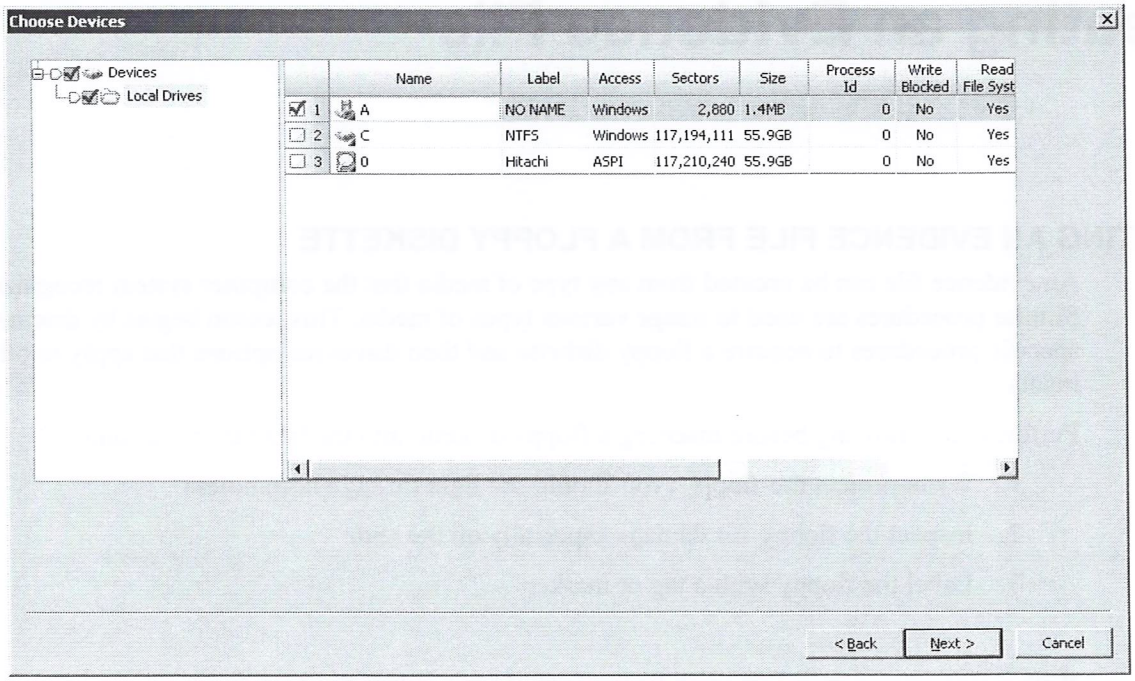

Figure 3-2 Selecting the floppy drive

EnCase will access and display the selected drive. To change the Evidence Name, Number, and to add notes, right-click on the floppy icon and select **Edit...**

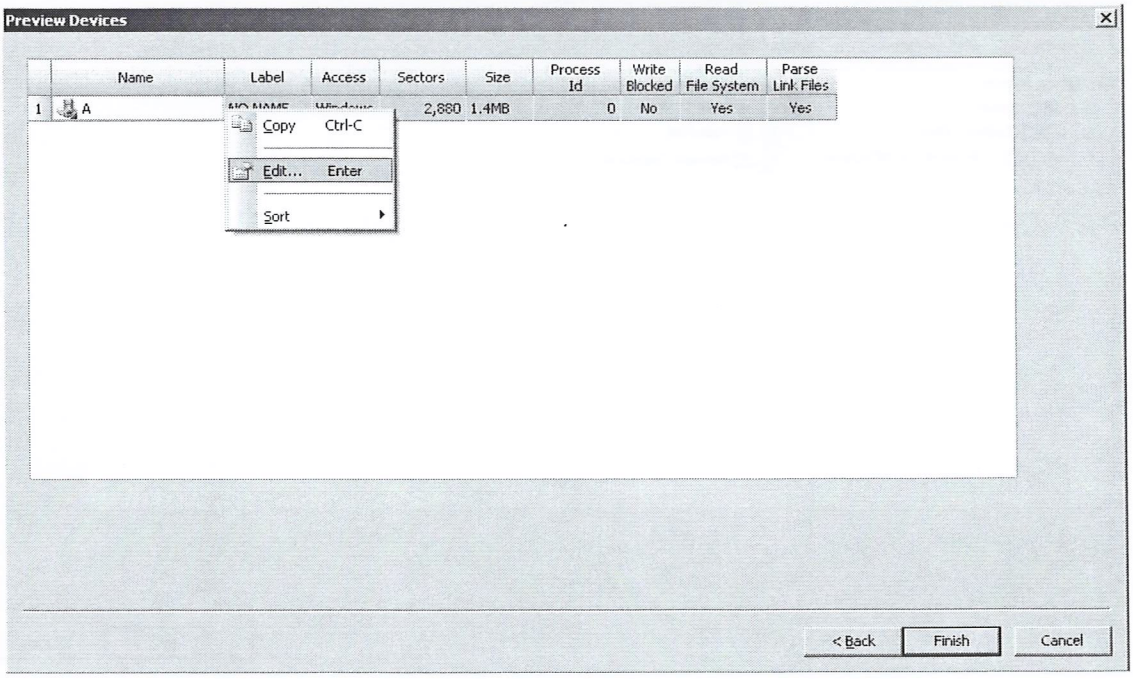

Figure 3-3 Preparing to edit device attributes

When the desired modifications have been made, select **OK** then **Next>**.

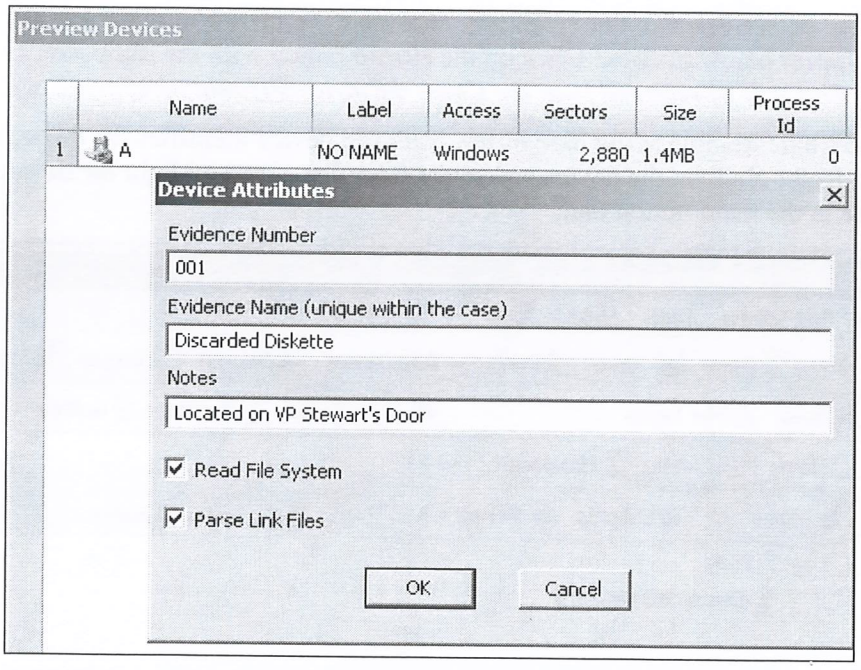

Figure 3-4 Editing device attributes

EnCase will now display the modified Evidence Name. Select **Finish**.

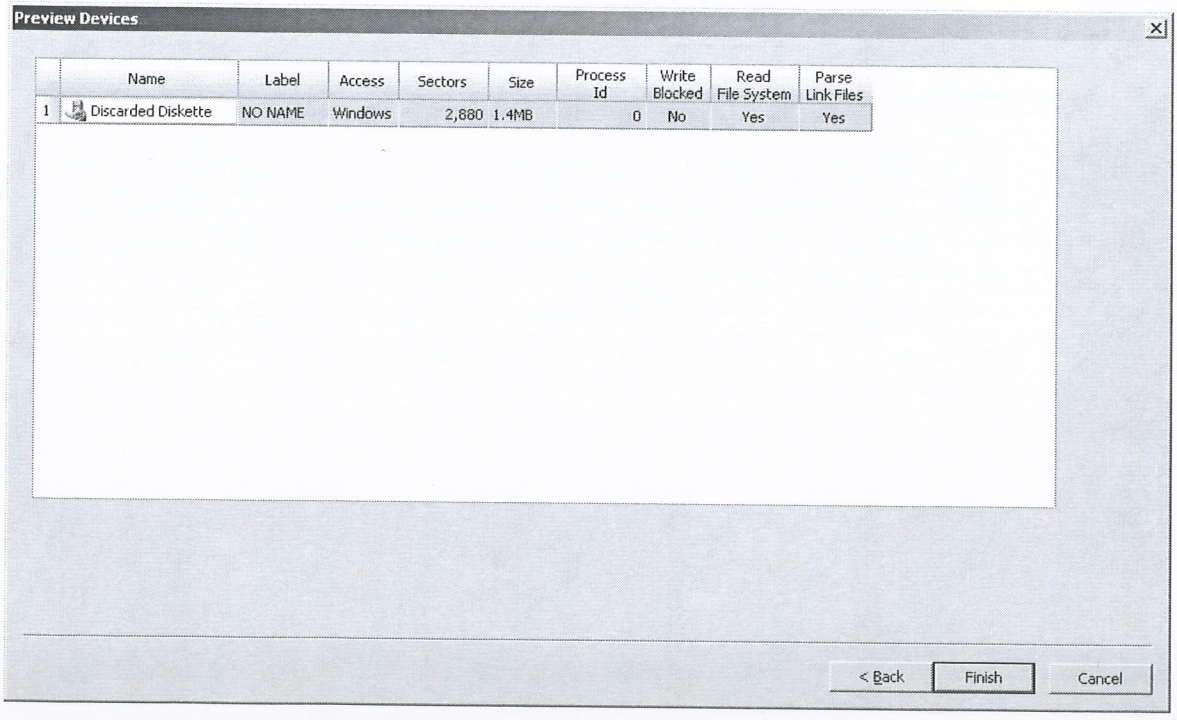

Figure 3-5 Accepting final changes

EnCase will then add the device to the case as a preview.

To see the device name in the Tree Pane, click on the **Entries** button. Another row of buttons should appear below Entries. Click on the **Home** button with the same icon as the Entries button. *This will be referred to as the **Cases→Entries→Home** view.*

The small blue triangle at the base of the displayed device identifies the device as a previewed device. Right-click on the device and select **Acquire...** or highlight the device and click **Acquire** in the main button bar.

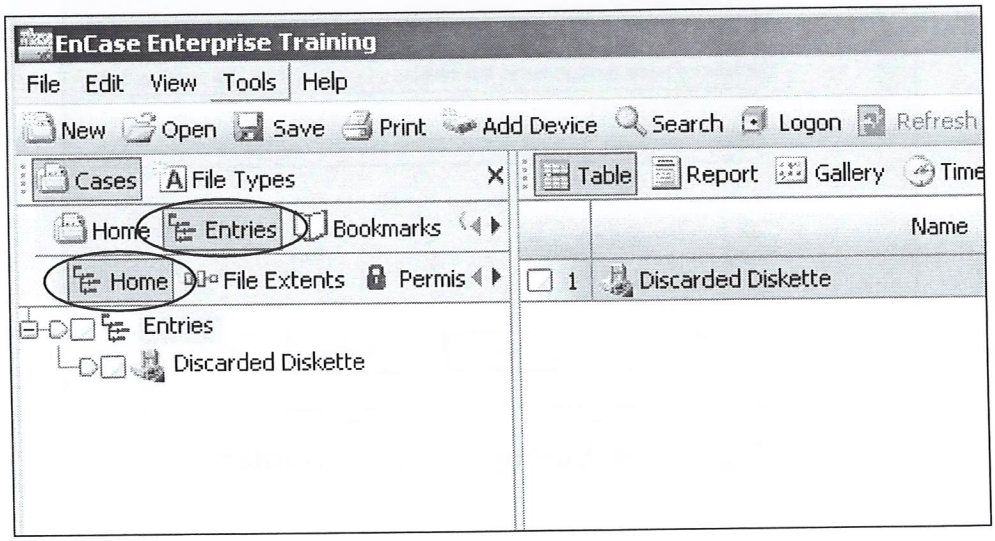

Figure 3-6 Acquiring from the preview

Upon selecting Acquire, an After Acquisition window is displayed with several available options. Selecting **Acquire another disk** will allow the examiner to acquire several devices one after another such as floppy disks or CDs.

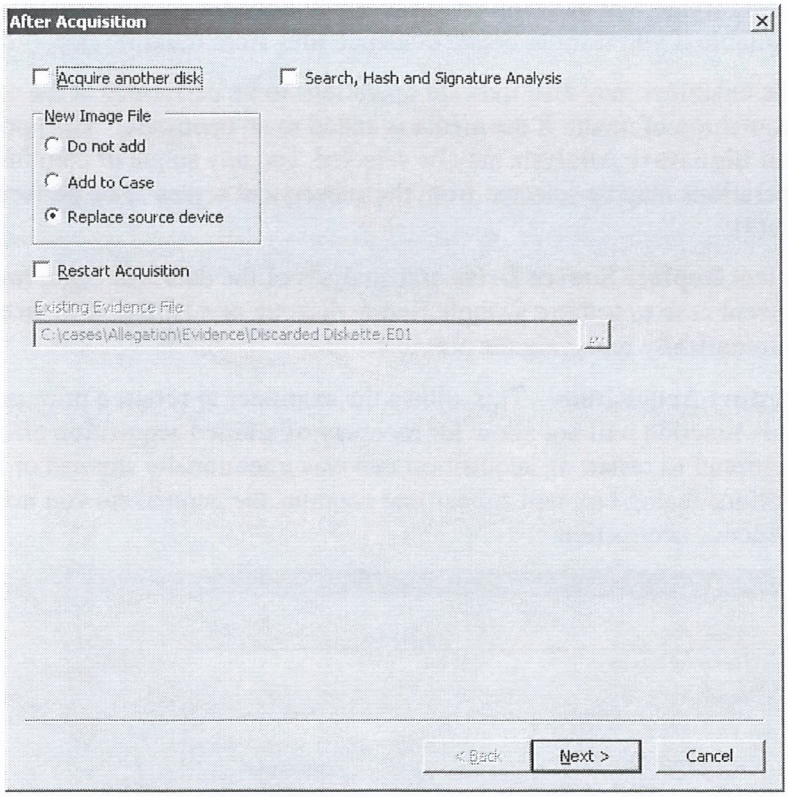

Figure 3-7 After Acquisition window

The examiner has three options for the evidence file once it is created.

- **Do not add** – This option will leave the evidence file in the saved location upon completion of the acquisition. This is used for acquiring images to a central server or acquiring images that will not be examined immediately. This process leaves the live access to the drive available to image other devices. This can be used when evidence files are to be created from dozens of floppy diskettes or other media and analyzed on another computer system later.
- **Add to Case** – This option will add the new evidence file to the case, but will not replace the live device. This is used for adding acquired images to the case, but leaving the live access to the drive available to image other devices. This can be used when evidence files are to be created from floppy diskettes and analyzed on this computer system later.

- **Replace source device** – This option is used for hard drive acquisition or for acquiring a single piece of removable media. This will add the new evidence file to the case replacing the live preview. Any search hits, hashing, bookmarks, etc., of the live device during triage will be resolved to the newly added evidence file. This option is not available if you want to create evidence files from multiple floppy diskettes.

  The examiner may also indicate operations to be performed at the conclusion of an acquisition of media if the media is added to an open case. The option **Search, Hash and Signature Analysis** may be selected, and any single or combination of the three operations may be selected from the subsequent screen to be performed on the evidence file(s).

  Select **Replace Source Drive** and analysis of the data will begin immediately within the current case to acquire a single floppy diskette or a hard disk to an evidence file automatically replacing the preview.

- **Restart Acquisition** – This allows the examiner to restart a prior acquisition process. This function will not allow for recovery of a failed acquisition effort, but will allow an examiner to restart an acquisition that was intentionally stopped or interrupted. An Options dialog box will appear that contains the parameters you need to set prior to evidence acquisition.

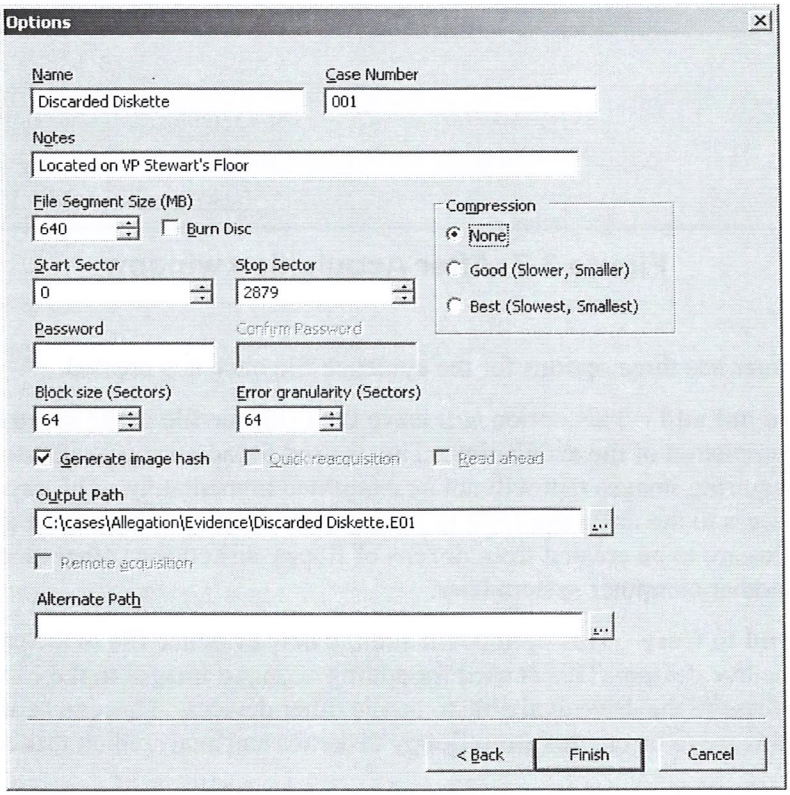

Figure 3-8 Options window for Acquire operation

- **File Segment Size** – Select the **File Segment Size** for archiving purposes (the 640 megabytes default makes files that fit on CDs; seven 640 MB files fit well on a DVD). The minimum is 1 MB, the maximum is 2000 MB.
- **Burn Disc** will allow the direct burning of the evidence files to Compact Disc
- **Compression** – The level of compression has no effect on the evidence, but may affect the amount of time that it takes to acquire the evidence file. Because compression is a computationally intensive process, it may take up to three times longer to create a compressed evidence file than to create an uncompressed one. However, in most cases, the compressed file will be two to three times smaller than an uncompressed evidence file.
- **Sectors to Acquire** – By default the **Start Sector** and **Stop Sector** boxes will display the total sectors on the media. If the media contains a restored image such as one generated by a forensic acquisition tool, you may select only the sectors containing the restored image, excluding the unused sectors.
- **Password** – If the evidence file is to be protected from unauthorized use, enter a password (the same password is typed twice to ensure the password was typed correctly). Do not use this feature if there is a chance the password will be forgotten. The password must be entered every time the evidence file or a case that refers to it is opened. ***There is no simple way to recover a forgotten password.***
- **Block Size** – The number of sectors (copied from the subject's drive) that will be contained within each data block.
- **Error granularity** – When a read error was found during an acquisition in EnCase versions 1 through 4, the entire 64-sector block of data containing the read error was "zeroed out." This option, which was introduced with version 5, allows the investigator to specify the number of sectors that will be "zeroed" around the sector, from 64 (default) to 1 (64, 32, 16, 8, 4, 2, 1). The lower the granularity value, the slower the acquisition.
- **Generate Image Hash** – Select **Generate Image Hash** to prompt EnCase to generate an MD5 hash of the contents of the disk being acquired. This value can later be compared to the hash of the evidence file contents to confirm that the data is identical.
- **Quick Reacquisition** – This option will allow an already created/stored evidence file to be duplicated with different settings. The settings that are subject to change with this option are the password (add or delete), file segment size, and the start/stop sectors. To change compression, block size, or error granularity, this option must not be selected. Other settings cannot be changed. Reacquiring an evidence file is discussed later.
- **Read Ahead** – If selected, data will be read from the subject's hard drive while other data is being written to the evidence file in an effort to speed up the acquisition process.
- **Output Path** – Type the path and name of the output file or browse to select the path, and then enter a unique file name to designate the evidence file.
- **Alternate Path** – Provides an alternate destination drive to use in the event that the **Output Path** destination drive should become full.

When all appropriate options are selected and the appropriate **Output Path** and filename are selected, click **Finish**.

If **Add to Case** is selected, the previewed device will remain in the case, an evidence file will be created for the acquired device, and the created evidence file will be added to the case.

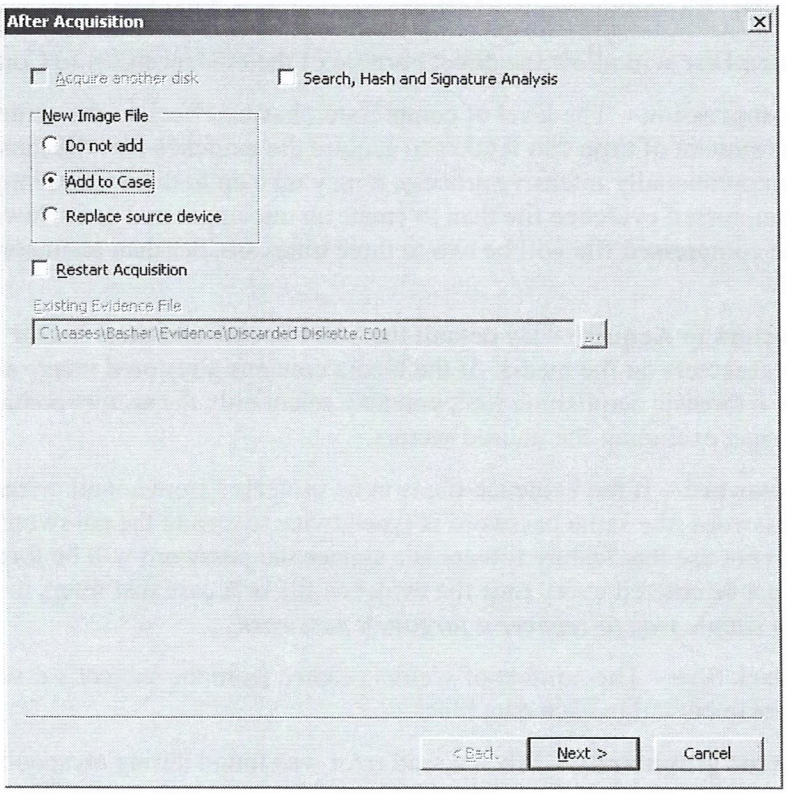

Figure 3-9 After Acquisition window with "Add to Case" selected

When the acquisition is completed with **Add to Case** selected, the following information appears documenting when the acquisition was made, how long it took, where the evidence file was stored, and the hash value generated. If **Do Not Add** was selected, the same information appears minus the acquisition hash data. The examiner may choose to save this data for retrieval later, as a Note bookmark, in the Console (for exporting and saving elsewhere), or as a Log Record bookmark. None of the above is selected in the initial default.

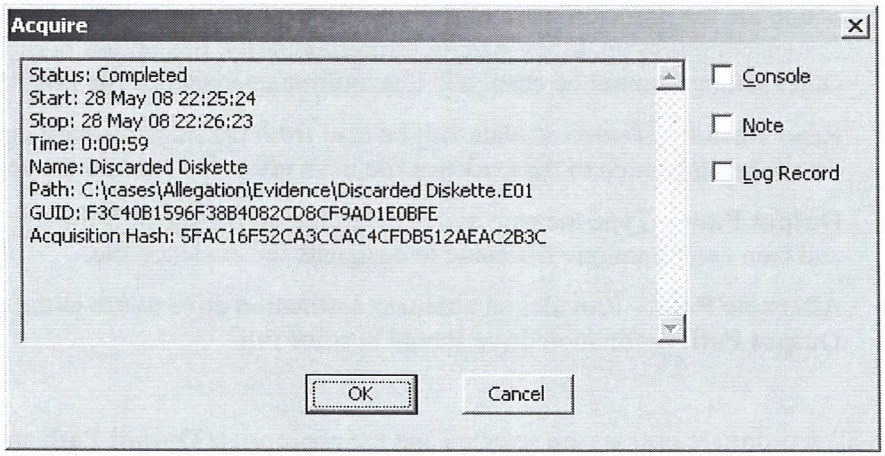

Figure 3-10 Message displayed when "Add to Case" is selected and acquisition is complete

If more than one floppy device is to be acquired, select **Acquire Another Disk**. The examiner may select **Add to Case**, to provide the ability for immediate examination or **Do Not Add** for the creation of evidence files for later examination in a different case file.

When selecting **Acquire another Disk** and **Add to Case**, the following status screen is displayed. When selecting **Acquire another Disk** and **Do Not Add**, the same status screen is displayed without the acquisition hash data. The examiner may choose to preserve this information as previously described. The examiner must then insert the next diskette to be imaged and click on **Next Disk**.

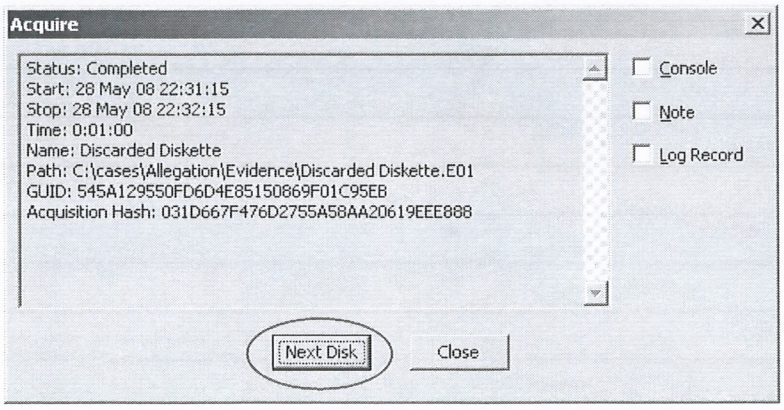

Figure 3-11 Option "Next Disk" replacing the "OK" option

It is recommended that the examiner either rename each floppy diskette imaged or allow EnCase to automatically include or increment a number within the evidence name and evidence number items (beginning with the second floppy diskette). This will allow the examiner to track the different floppy devices imaged. Also the same options are used with subsequent floppy images.

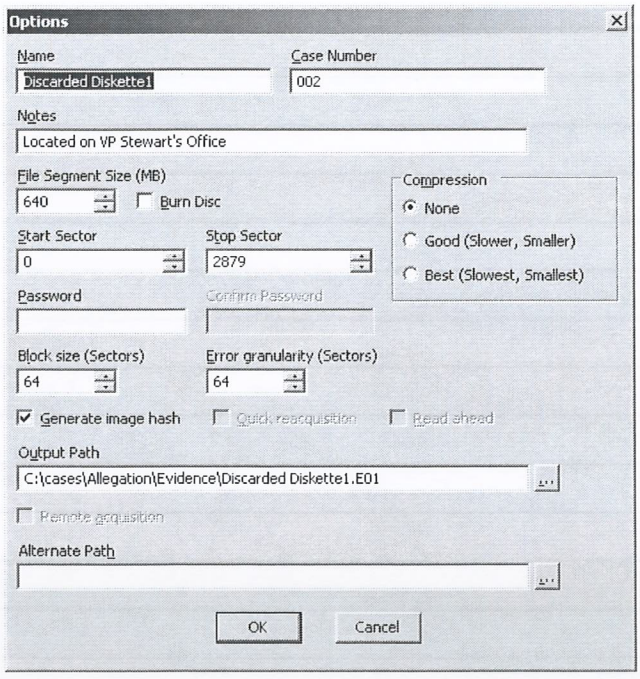

Figure 3-12 Automatic insertion of "1" in evidence name to number floppies imaged

Notes

Notes

Notes

Lesson 4

EnCase® Concepts

EVIDENCE FILE

The central component of the EnCase® methodology is the evidence file. This file contains three basic components (header, checksum, and data blocks) that work together to provide a secure and self-checking description of the state of a computer disk at the time of analysis.

Cyclical Redundancy Check (CRC)

The Cyclical Redundancy Check (CRC) is a variation of the checksum and works in much the same way. The advantage of the CRC is that it's order-sensitive. The string "1234" and "4321" will produce the same checksum, but not the same CRC. Most hard drives store one CRC for every sector. When a read error is generated from a disk, this usually means that the CRC value of the sector on the disk does not match the value that is recomputed by the drive hardware after the sector is read. If this happens a low-level, disk-read error occurs.

Evidence File Format

Each file is an exact, sector-by-sector copy of a floppy or hard disk. When a file is created, the user provides information relevant to the investigation. The EnCase® program (EnCase) archives this and other information inside the evidence file along with the contents of the disk. Every byte of the file is verified using a 32-bit CRC making it extremely difficult if not impossible to tamper with the evidence once it has been acquired. The odds of two data blocks that contain different data producing the same CRC are roughly one-in-four billion. This allows the investigators and legal team to confidently stand by the evidence in court.

Rather than compute a CRC value for the entire disk image, EnCase computes a CRC for every block of 64 sectors (32 KB) written to the evidence file by default. This provides a good compromise between integrity and speed. A typical disk image will have many tens of thousands of CRC checks. The investigator will be able to identify the location of any error in the file and disregard that group of sectors, if necessary.

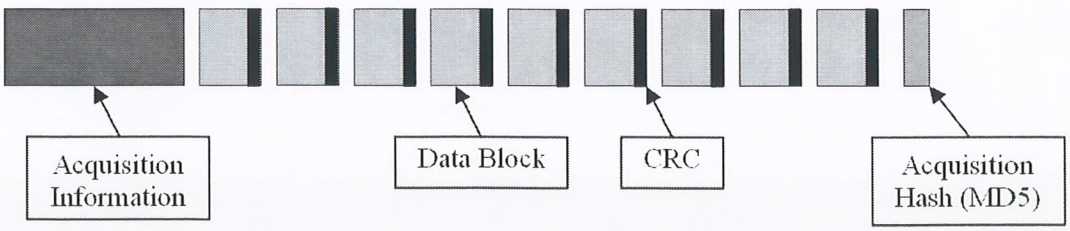

Figure 4-1 Parts of a complete EnCase evidence file

EnCase calculates an MD5 hash when it acquires a physical drive or logical volume. The hash value is written into the evidence file and becomes part of the documentation of the evidence. When an evidence file is added to a case, EnCase automatically verifies the CRC values and recomputes the hash value for the evidence data within evidence file. The hash value that is stored in the evidence file and the hash value that is computed when the evidence file is added to a case appear in the report immediately confirming that the evidence file has not changed since acquisition. At any time while using EnCase, select the Case view, right-click on the physical drive or logical volume, and select **Hash** to re-compute the hash value of the drive or volume.

Compression

Compression technology allows EnCase to store the data from a large disk in a relatively small file. EnCase uses an industry-standard compression algorithm to achieve an average size reduction of 50%. If most of the disk contains text data, the compression ratio may be much higher. However if the majority of the media contains compressed data, such as JPG files, video data, and similar types of files, the compression realized may be minimal. Compressed evidence files take longer to generate due to the additional processing time required to compress the information. Compression ***never*** has any effect on the final evidence, and compressed blocks are checked for validity in the same way as uncompressed ones. If a device is acquired with and without compression to two different evidence files, the resulting hash values stored within both evidence files will be the same. The hash computation during acquisition occurs prior to compression of the data. The hash value stored within the evidence file represents a hash of the device.

Verifying an Evidence File Automatically

Whenever an evidence file is added to a case, EnCase will begin to verify the integrity of the entire disk image in the background. This is usually quite fast for small (floppy) evidence files, but can take longer for hard disk evidence files. The investigator may conduct his examination while the verification occurs.

CASE FILE

The case file is a text file that contains information specific to one case. The case file contains pointers to one or more evidence files or previewed devices, bookmarks, search results, sorts, hash analysis results, signature analysis reports, etc. When the user runs EnCase, a case file must be created before media can be previewed or evidence files can be analyzed.

CASE BACKUP FILE

The backup file is an auto-saved backup of the open case file. The backup file is saved in the folder where EnCase is installed, by default C:\Program Files\EnCase5\Backup, with the same file name as the .CASE file, but with a .CBAK extension.

If there is an error with the .CASE file, the .CBAK file may be opened. When the .CBAK file is saved, EnCase will give you the option to promote the .CBAK file to the .CASE file. By default the .CBAK file is saved every 10 minutes. If the .CBAK file is promoted to the working .CASE file, a new .CBAK file will be auto-saved in 10 minutes.

Change the auto-save by going to **Tools→Options→Global**, and change the **Auto Save Minutes** to the selected minutes. Though not recommended, choosing **0** will disable the auto-save function.

ENCASE® CONFIGURATION FILES

The EnCase configuration files are a series of initialization (.INI) files that contain global settings for EnCase. These files contain the signature table, file types, file viewers, filters, global keywords, etc. These files apply global configurations to every case and evidence file used within the EnCase® environment. They are stored (by default) in the folder where EnCase is installed usually C:\Program Files\ EnCase6\Config.

Notes