Georgia State University
CIS 8630 - Business Computer Forensics and Incident Response

Workshop Protocol

Introduction To EnCase 7

David McDonald
(with special thanks to Richard Baskerville)

Acknowledgement:
Parts of this protocol are based on *Encase 7.04 User's Guide* Copyright 2012 Guidance Software

Version 2.3
7 September 2013

Department of Computer Information Systems
35 Broad St., NW. POB 4015
Atlanta, GA 30302-4015
USA

Table of Contents

Table of Figures

Protocol Notation

In the workshop protocol that follows, an arrow (→) at the beginning of a paragraph denotes an instruction that the participant should execute as part of their activities during the workshop.

Creating a Case

Starting a New Case

→ Log on to your EnCase lab computer. On the Home screen **click** on: "New Case" under the "Case Files" heading. The following Options dialog box will open:

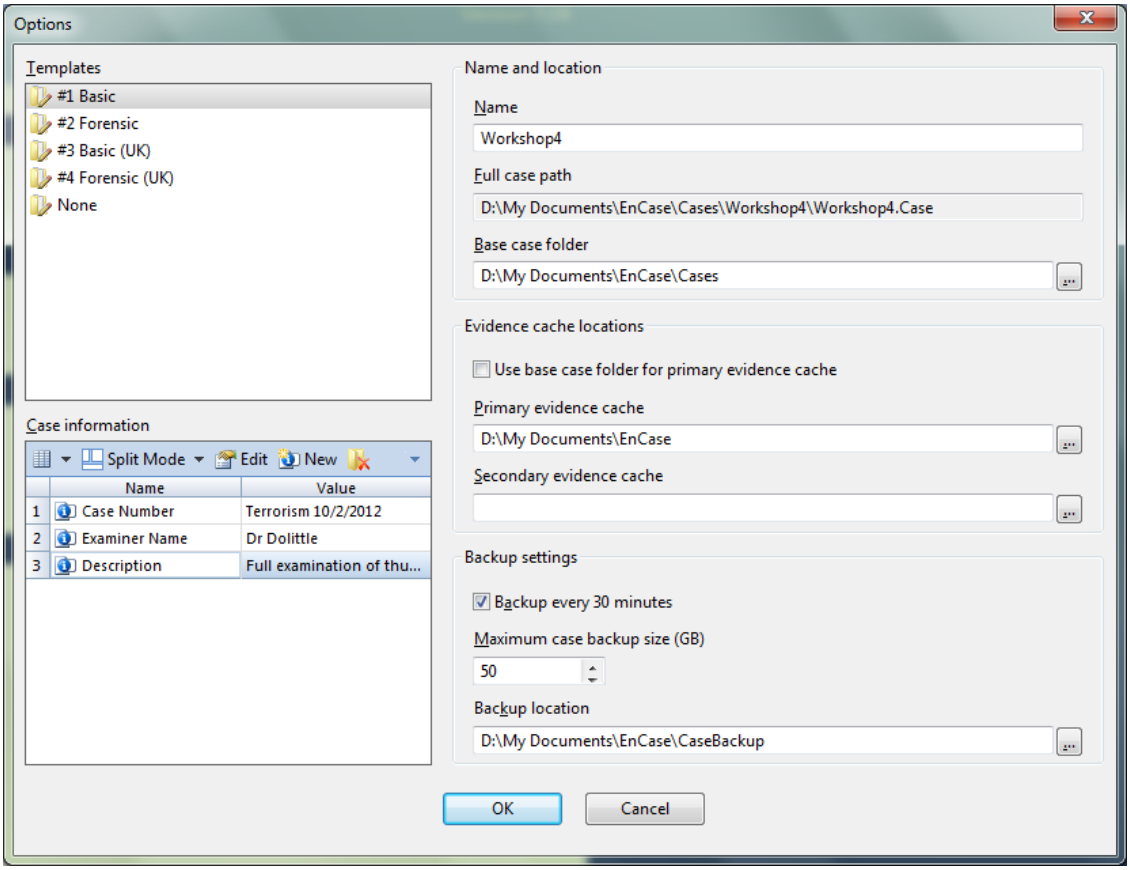


Figure 1 - New case dialog box

→ Provide a **Name** (Under **Name and location**) to this case for identification purposes. In figure 1 above, this name is "Workshop4."

For now, use the default **Template** (i.e., "#1 Basic)**.**

→ Under the **Case Information** section, highlight the **Case Number** row and click on "Edit" in the mini-toolbar. Define a value for **Case Number, Examiner Name,** and **Description.**

→ Click **OK**, and then **OK** again to any dialog boxes which may pop-up pertaining to Encase default file locations

Copying Evidence Files

→ Most course resources are found in the *C:\Dayspace\Lab Evidence Files* folder on the VM web site. For this lesson, the following two files are required:

1. EnCaseWrkshp4E.E01
2. EnCaseWrkshp4E.E01.txt

EnCaseWrkshp4E.E01 is an EnCase evidence file created from a thumb drive using the FTK imager available on the Helix CD. This imager records hash verification information in the file EnCaseWrkshp4.E01.txt Because the file includes case information and block CRC codes, a simple hash of the evidence file, outside of the EnCase utilities will NOT produce a matching hash. The hash for EnCase evidence files can only be calculated by EnCase.

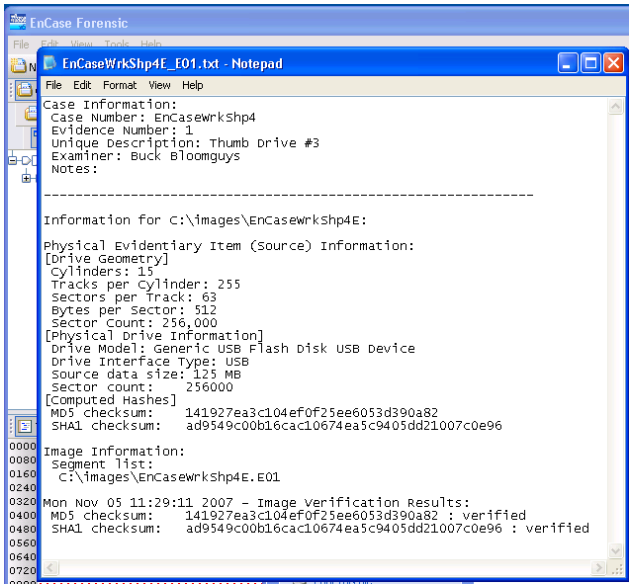


Figure 2. Imaging record accompanying evidence file.

Case Management

Before starting investigation and acquiring media, consider how to access the case once it has been created. It may be necessary for more than one investigator to view the information simultaneously. In such a case, the evidence file should be placed on a central file server and copies in case file placed on each investigator's computer (since case files cannot be accessed by more than one person at a time).

With Encase7, the necessary folders are created by default under: *c:\My Documents\Encase\Cases* (see figure 3).

→ Open the Workshop4 folder you just created and notice the sub-folders automatically created.

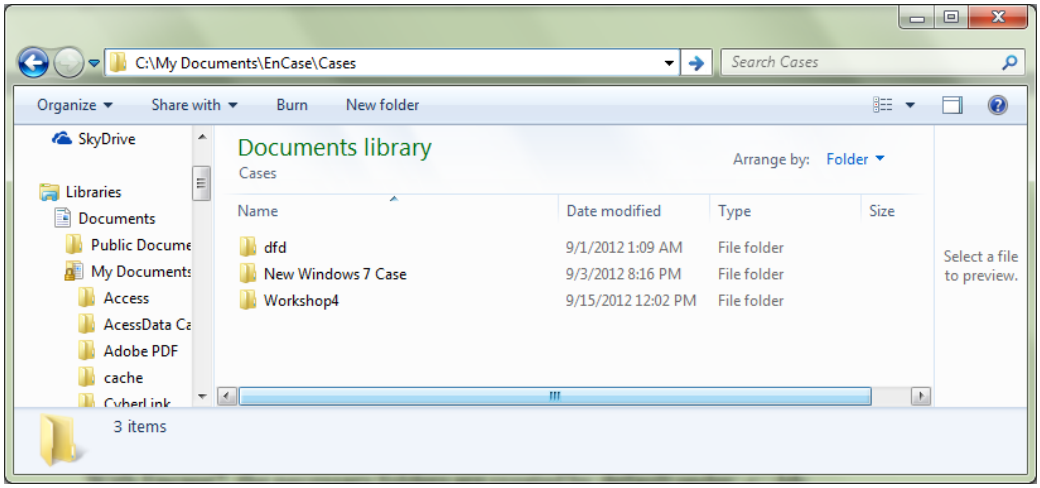


Figure 3. Creating folder structure,

The EnCase forensic methodology strongly recommends that the examiner uses a second hard drive, or at least a second partition on the boot hard drive, for the acquisition and examination of digital evidence. It is preferable to wipe an entire drive or partition, rather than individual folders, to ensure all of the temporary, suspect related data is destroyed. This will aid in deflecting any claims of cross contamination by the opposing counsel if the forensic hard drive is used in other cases.

→ On the EnCase home screen, click on **Add Evidence** found under the **Evidence** heading (see figure 4)**.**

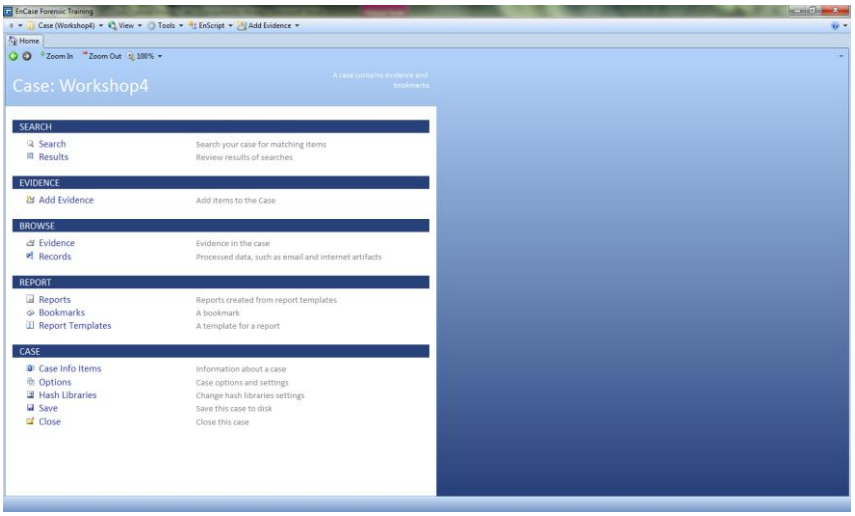


Figure 4. Home screen.

→ On the Add Evidence screen (figure 5), click on **Add Evidence File**.

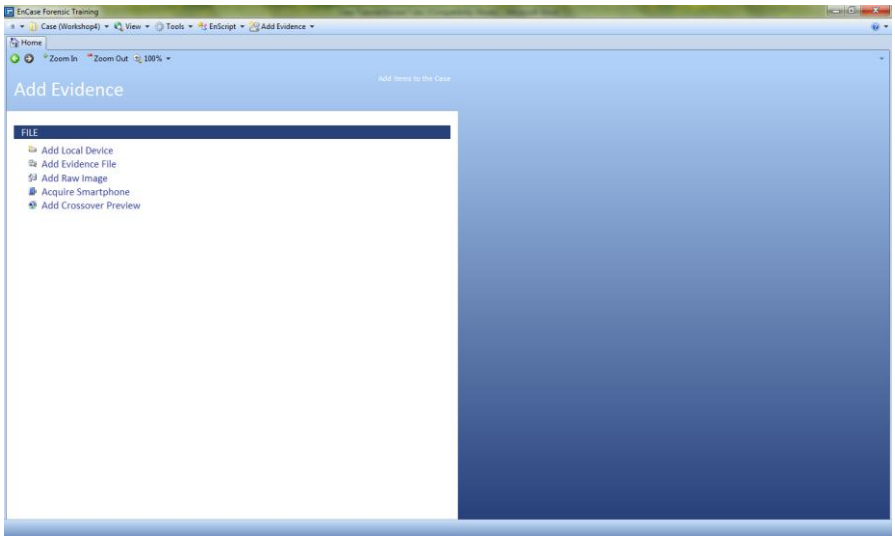


Figure 5. Adding an evidence file to a new case.

→ Navigate to: *c:\Dayspace\Lab Evidence Files* and open "EncaseWrkShp4E.E01" file.

The WrkShp4E evidence file is now loaded into the case you've created. Thumb Drive #3 should appear under Evidence on the left-side of the screen. Encase initially provides the user with a number of meta-data items on the right-side of the screen…the most

important of which is the MD5 hash value (see figure 6). This view of the case is called "Evidence view." Notice the top tab is labeled "Evidence ."

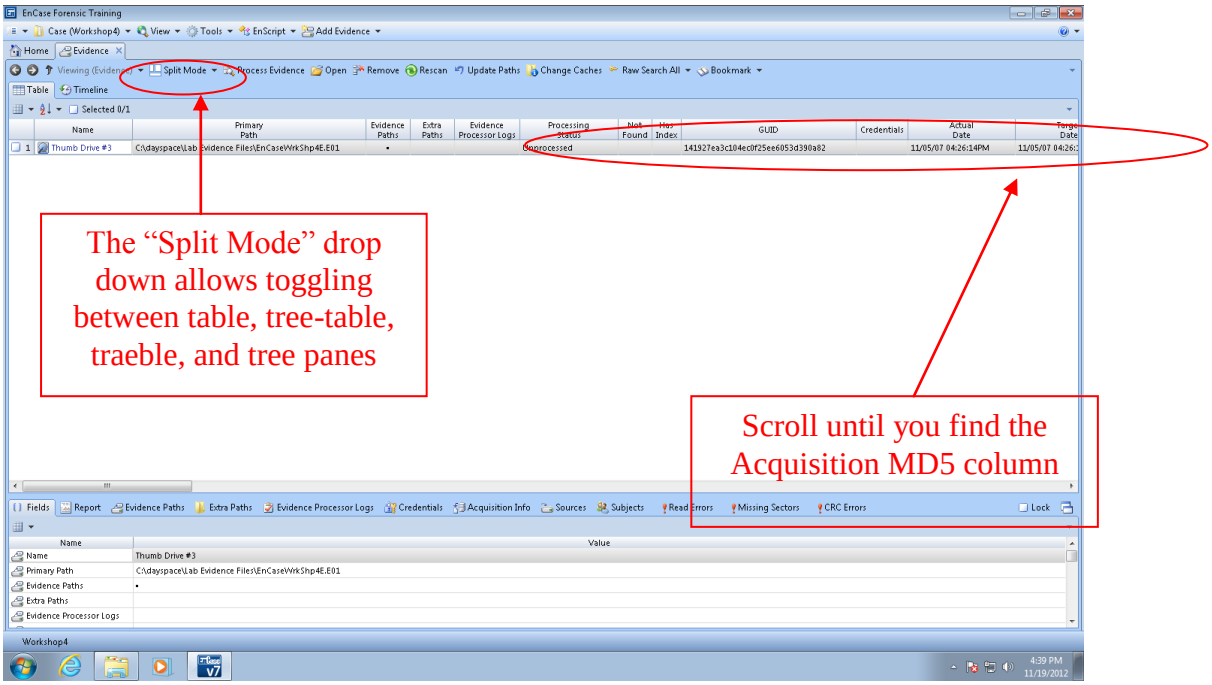


Figure 6. Initial meta-data screen for the new case.

→ Scroll to the right and select the value for "Acquisition MD5"

→ Right-click and **Copy**.

→ Warning! If you do not do this step first, the "Acquisition MD5" column will empty when processing a new case. If you do not obtain this information now, a different sequence of steps will be necessary.

→ Use Notepad to open the "EnCaseWrkshp4E.E01.txt" file in the Dayspace, Lab Evidence folder (see Figure 2).

→ Locate the MD5 original acquisition hash value and click **Enter** to place your cursor just under the original MD5 hash. **Paste** the value you copied from the Encase meta-data screen. Are they the same?

The Encase Evidence File

The central component of the EnCase methodology is the evidence file with the extension ".E01" or "EX01" (for evidence files created in Encase 7). The E stands for an Encase file, just as .docx indicates a MS Word file. This file contains three basic components (the header, checksum, and data blocks) to work together to provide a secure and self-checking description of the state of the computer disk at the time of analysis. On large capacity drives, the evidence files created will begin with .E01 and continue with .E02, E03,…E0*n* until all the data has been acquired.

Cyclical redundancy check (CRC)

The cyclical redundancy check is a variation of the checksum, and works much the same way. The advantage of the CRC is that it is order sensitive. That is, the string "1234" and "4321" will produce the same checksum, but not the same CRC. In fact, the odds that two sectors containing different data will produce the same CRC is roughly one in a billion.

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 disc does not match the value that is recomputed by the drive hardware after the sector is read. If this happens, a low level 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 supplies information relevant to the investigation. EnCase archives of this and other information inside the evidence file along with the contents of the disc. 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. 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. 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.

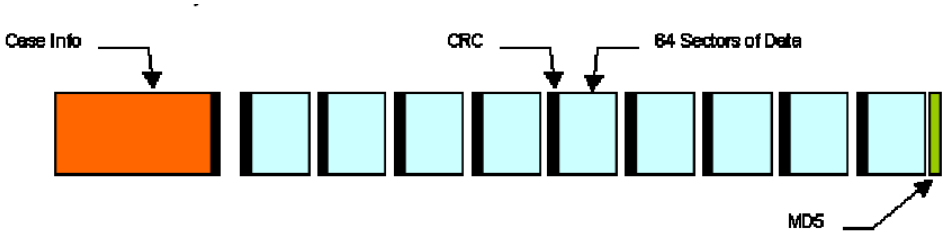


Figure 7. Evidence file organization

Compression

Compression technology allows EnCase to store data from a large disk in a relatively small file. It uses an industry-standard compression algorithm that achieves an average size reduction of 50%. If most of the disc is unused, the compression ratio may be much higher. This can result in great savings in this storage space. Compressed evidence files take longer to generate because of 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.

Automatic Verification

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 a small evidence file but can take a long time for hard disk files. During the verification process, the investigator can continue working on the case normally. If the case is saved in closed while verification process is running, the verification process is canceled. This process then starts over when the cases reopened.

Navigating the Case View

→ Use the "Split Mode" drop-down menu and select **Tree-table** (see figure 6 earlier).

→ **Click** on Thumb Drive #3 entry on the Table View

Besides changing the appearance of the panes, the actual evidence may be viewed in different modes. The "Viewing" drop-down menu to change back and forth between the initial Entry view to Evidence view (Entry view shown in figure 8 below).

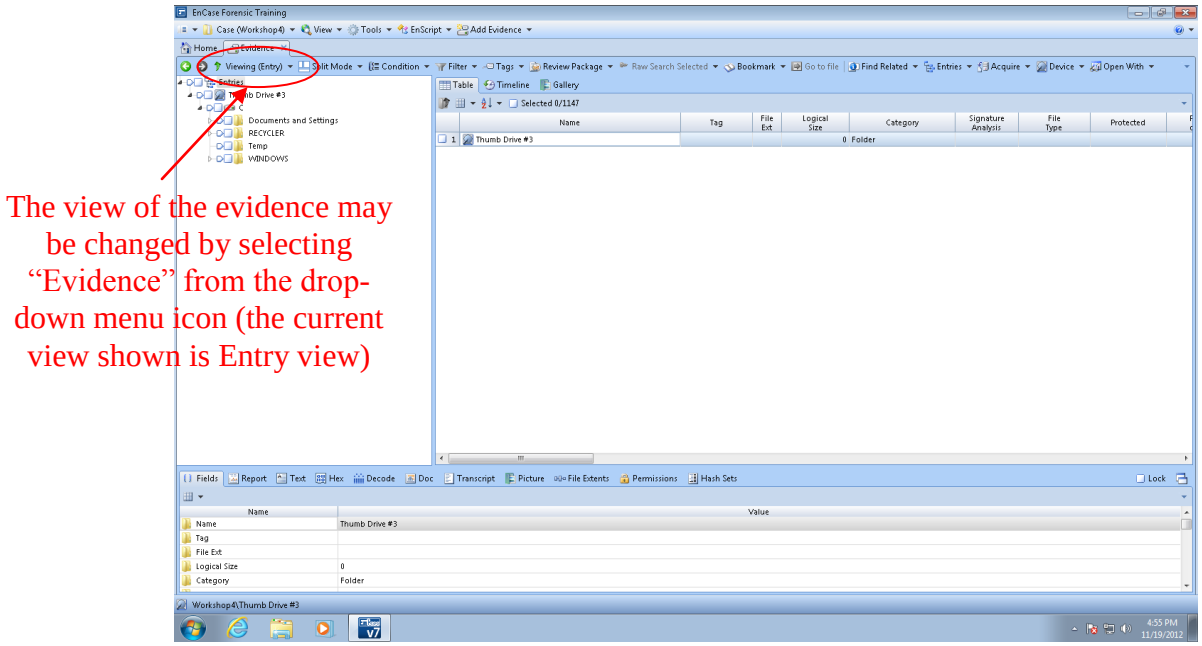


Figure 8. Using the drop-down Viewing menu to change to between Evidence and Entry views

The case entry view is used to navigate through the evidence that has been added to the case. From this view, you can view the files on a single piece of evidence or all the files found on several pieces of evidence. The picture gallery, timeline, disk view, and evidence table are all accessed from the case view.

→ Using the Evidence viewing drop-down, **toggle** between Evidence and Entry views.

→ Are there any differences to the drop-down menu selections in Evidence and Entry views?

→ Make sure Encase is now opened in *case entry view*."

Basic Layout

The screen is initially divided into three sections (see figure 9), referred to as the tree pane (left pane), table pane (right pane), and view pane (bottom pane).

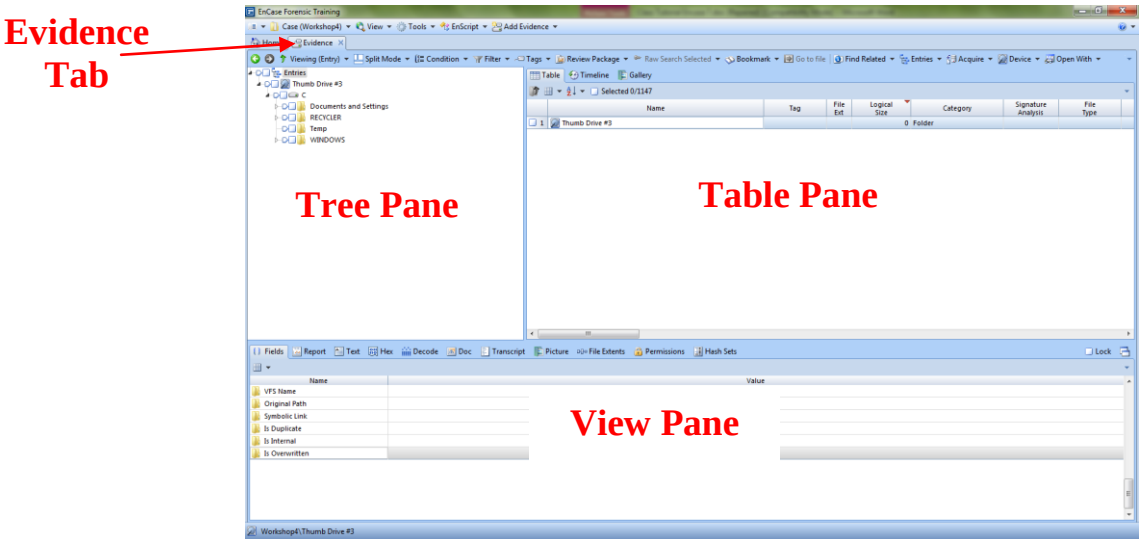


Figure 9. View of the three panes.

Tree Pane (Left Pane)

This view works like Windows Explorer, providing the user with a tree structured view of the evidence, and illustrating the relationship of each folder hierarchically. It presents each evidence file is a folder that contains additional folders and files. Only evidence files and folders contained within them are displayed in this view. Individual files' contents are not displayed. An icon that quickly identifies the type of evidence precedes each evidence file.

The transparent triangle with the apex facing left can be used to expand (triangle faces downward and turns black) and contract the tree structure. You can right click on a folder to bring up the context menu, with the choice to expand or contract everything from the selected position. Everything in the case will be affected by right clicking on the case folder (Figure 10 below) .

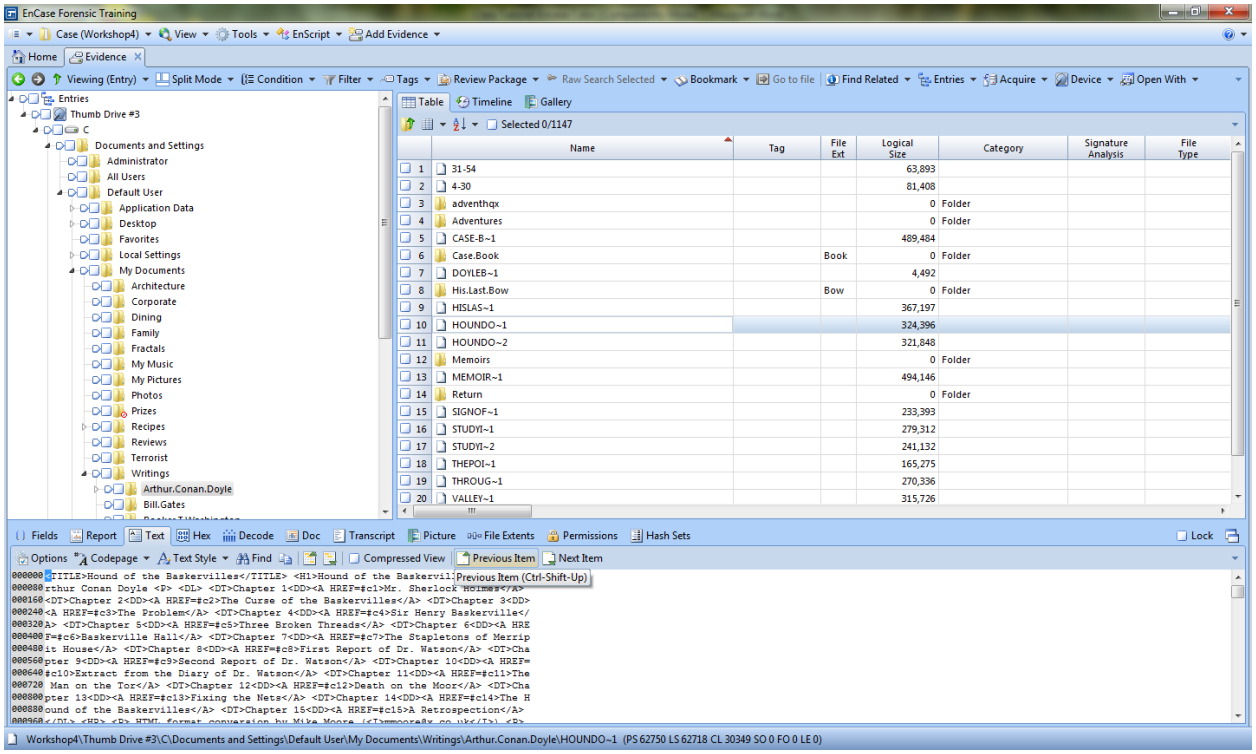


Figure 10. Highlighting tree pane affects table pane.

Highlighting the set include area (looks like a “home base plate”) will show all contents in the table pane from the set include folder downward through the hierarchy (see figure 11)

Set include marker (shown in green)

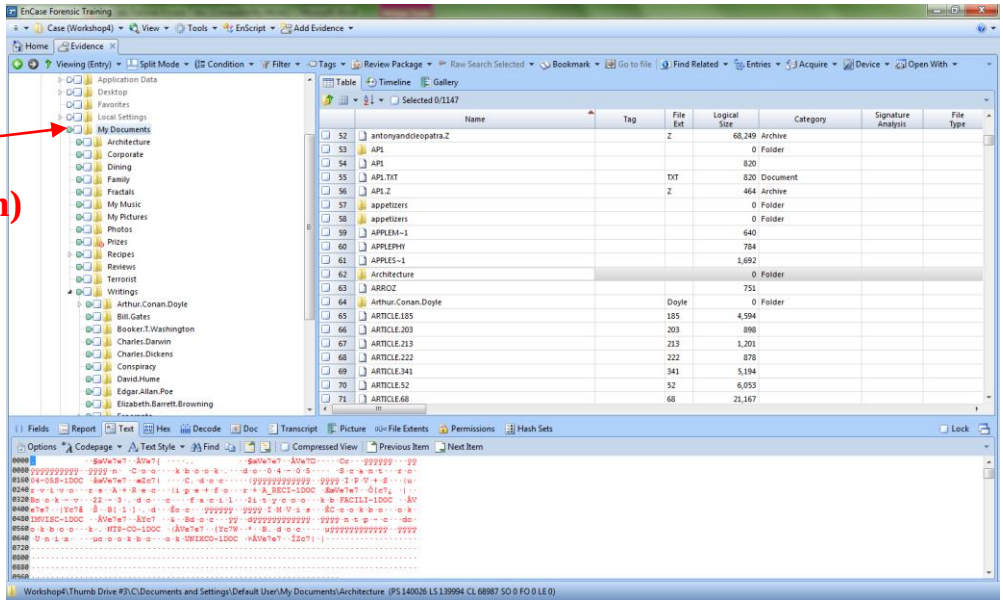


Figure 11. "Home Plate" expansion of right pane.

Table Pane (Right Pane)

The table pane view displays the subfolders and files that are contained within the folder that is highlighted in the tree pane. Highlighting a folder in the tree pane affects the display in the right pane. Figure 12 shows "Star.Trek.Stories" folder highlighted in the Tree pane and the contents of this folder are displayed in the Table pane.

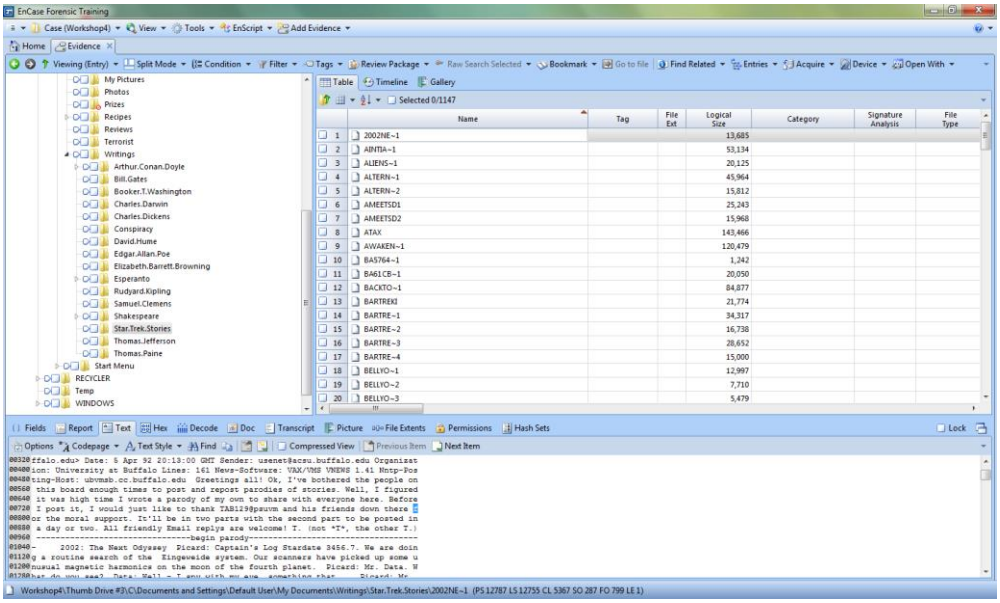


Figure 12. Tree view item chosen...table view displays contents of the chosen folder

View Pane (Bottom Pane)

The view pane displays the contents of the item selected in the table pane. The view pane has default settings that should be understood. The contents of a file are checked to see if it is an image that can be decoded internally. If so it will automatically switch to a picture of you in the bottom pane and display the image.

A large amount of evidence gathering is conducted from the view pane. Here, the user can select various amounts of data and bookmark that information which can then be included in the report. The examiner can also select different formats from the tabs above the view pane. Depending upon which tab is chosen, sub-menus may or may not be present. Figure 13 shows the sub-menus for a Text tab view. Figure 14 shows the Picture tab view has no accompanying sub-menus. Figure 15 shows the both hex and text values in the view pane.

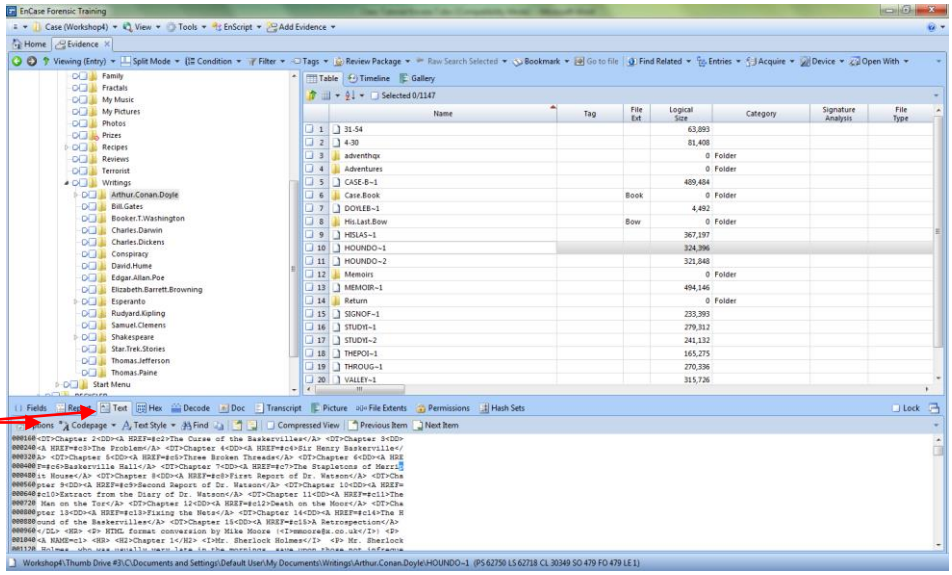


Figure 13. View pane with Text tab chosen (note the sub-menus).

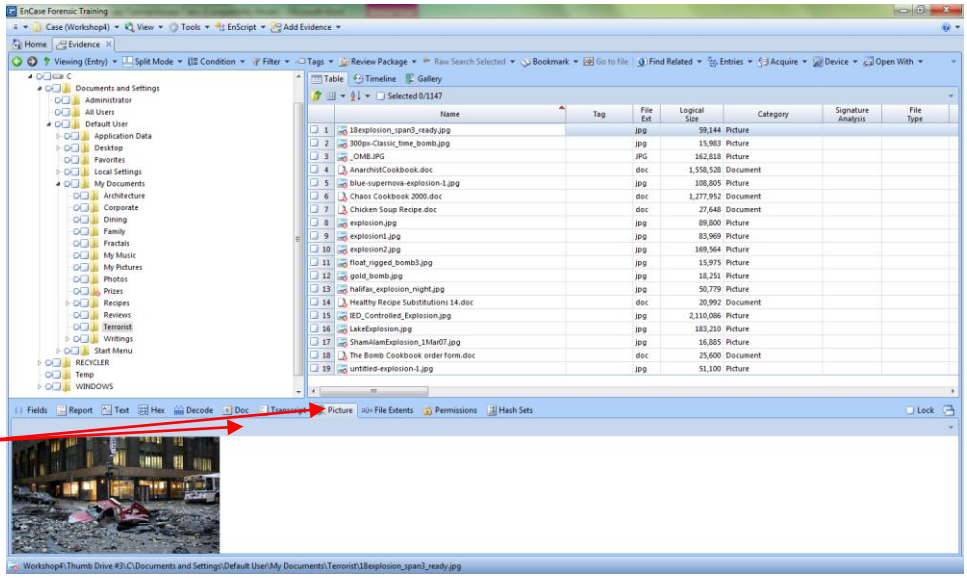


Figure 14. View pane with the Picture tab chosen (note no sub-menus).

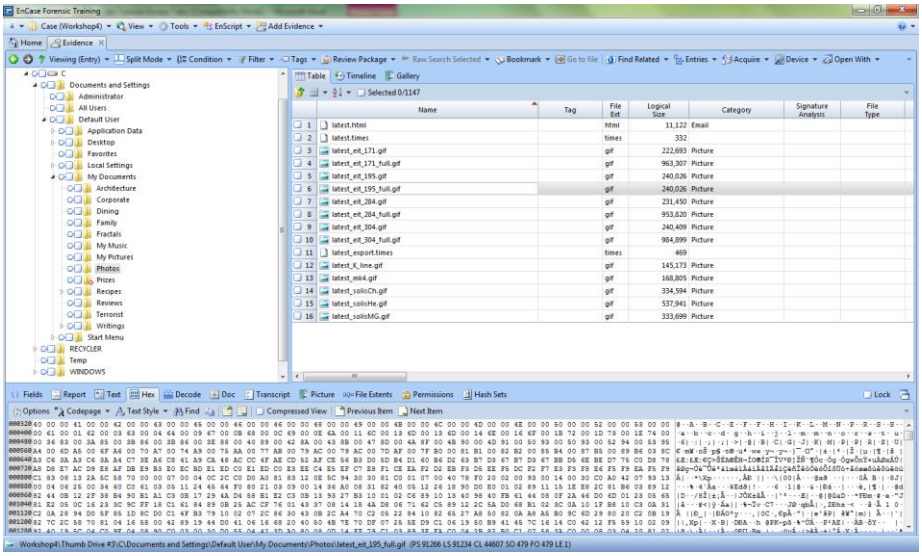


Figure 15. View pane using the Hex tab (note the sub-menus).

Figure 16 is showing the file highlighted in the table pane as text in the view pane. Notice the text entry is using the entire width of the view pane. Encase allows the user to customize how items may be viewed.

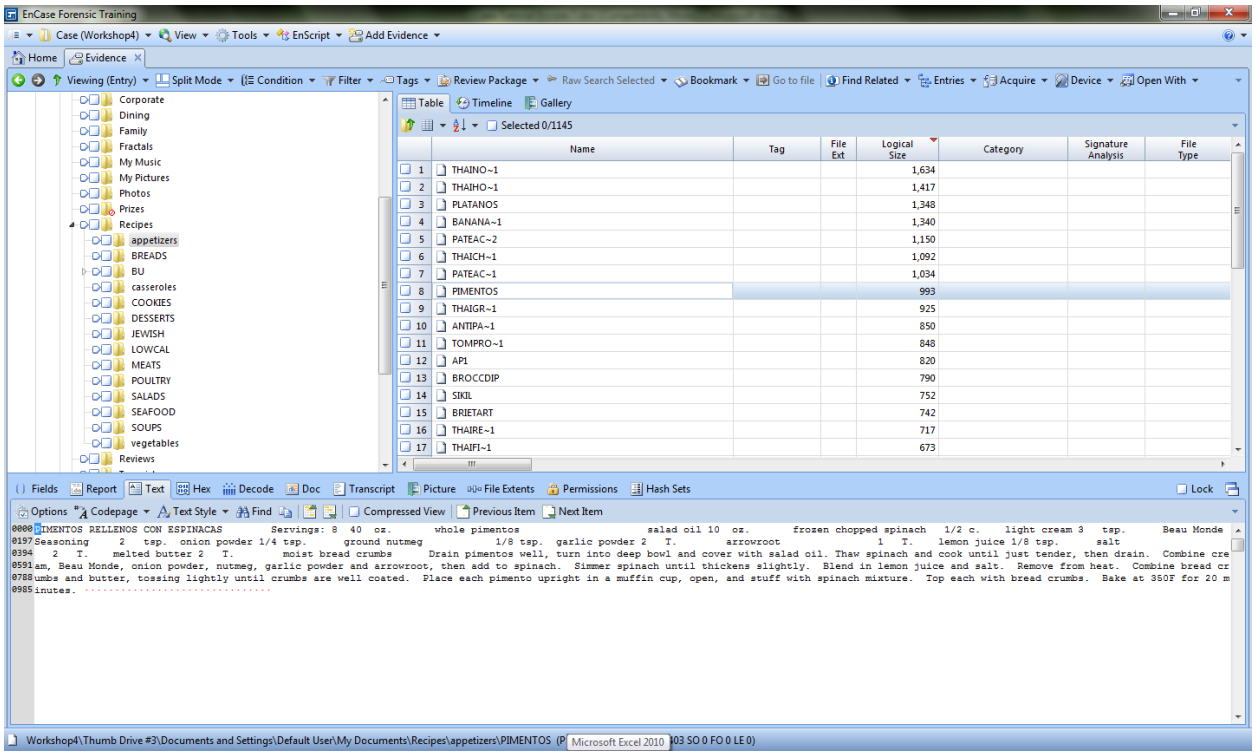


Figure 16. Default text view in view pane

→ Use a text submenu to define how you wish to view the text. Selecting the drop-down **Text** Styles submenu. Choose the entry **Text Styles.** The dialog to define a new style will open (see figure 17). Choose **New** from the choices at the top of the dialog box.

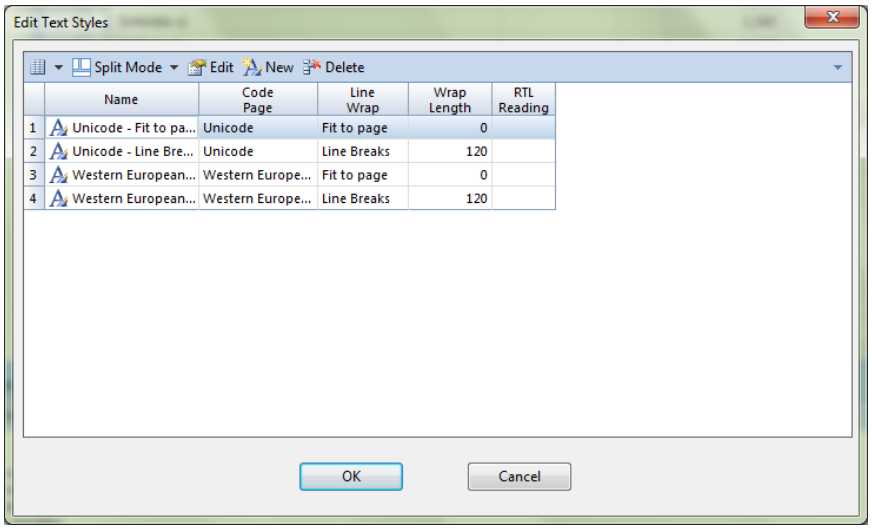


Figure 17. Creating or editing a new text style

→ Name the new text style **ASCII 80.** Under "Line Wrap" select **Line Breaks**. Change the "Wrap Length" to **80**. Switch to the "Code Page" tab. Code pages are in alphabetical order. Choose **Latin 9 (ISO).** Click **OK.**

View the text which was in the view pane. It is now 80 columns wide with line breaks in the appropriate locations. Notice how much more readable this view is to the default view. Also note the "Text Styles" drop-down now shows the new entry you've just created. The ASCII 80 style will be available for all future cases.

One last note, both the tree pane and table pane make it simple for an examiner to locate and restore files which were deleted from the suspect's drive.

→ Navigate to the "Terrorist" directory in the tree pane. Notice that deletion indicator icons (red circle with a diagonal bar) show that all of the files in this directory (in the table pane) had been deleted from the original media.

→ Similarly, navigate to the "Prizes" folder in the tree pane. Notice the same deletion indicator icon is present on the folder itself indicating the entire folder was deleted. Naturally, any files shown in the table pane also show the deletion indicator icons (see figure 18) .

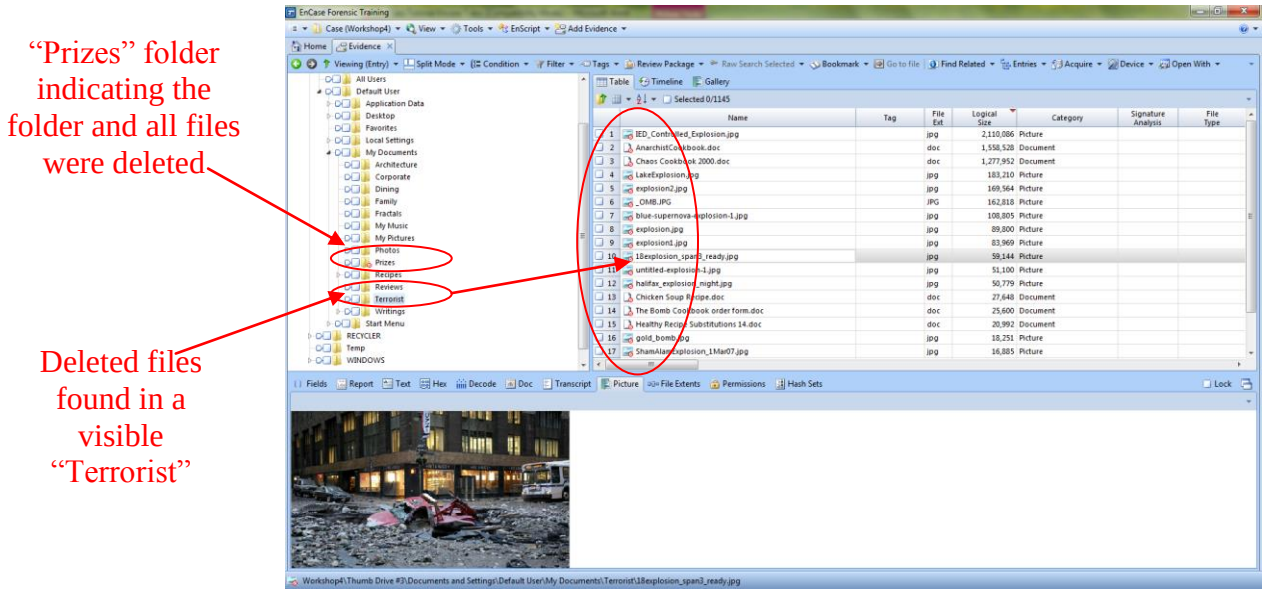


Figure 18. Deleted files and folders (restored automatically by EnCase).

The GPS

It is important to be aware of your current positioning within the case, especially when documenting the location of evidence found in unallocated space. A status bar provides a "GPS" provides precise location of evidence using the following six codes (figure 19).

1. PS: Physical sector number
2. LS: logical sector number
3. CL: cluster number
4. SO: sector offset -- the distance in bytes from the beginning of the sector
5. FO: file offset -- the distance in bytes from the beginning of the file
6. LE: length -- the number of bytes in the selected area

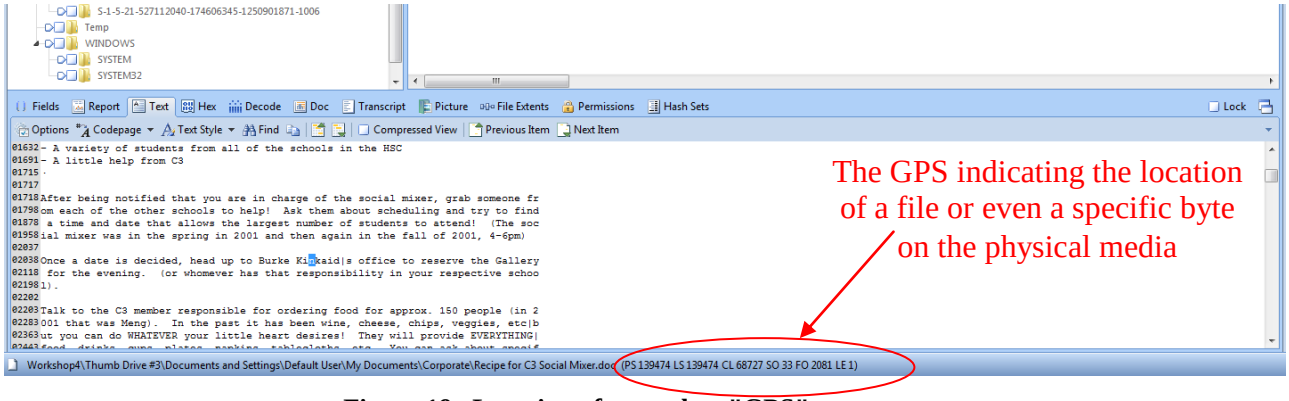


Figure 19. Location of status bar "GPS".

Any evidence in the table or view pane will show the precise location as to where that file or character (byte) may be found on the original drive media. As we progress through Encase 7, the full value of the GPS will be revealed.

The GPS functions similarly to windows explorer in providing a means to browse through the evidence. Where it is possible to recover deleted files or directories automatically, these are recovered and appear in the table view. Files and directories recovered from deleted entries appear with a red circle with a stroke across it.

Searching the Case

Encase provides a powerful search engine to locate information anywhere on the physical or logical media. After creating a case file, a search may be conducted on keywords and their options. Additionally, Encase 7 now provides two basic methods for searching for data. The method found in previous versions of Encase is now known as a "Raw Search All," while the newly added method is called an "Indexed Search." In a Raw Search All, a keyword is created on a search word, term, or expression. This is an ad hoc search method and can take quite a while with media sizes in the multi-gigabyte or terabyte range. Thus, the Indexed Search was created. Many readers are familiar with new operating systems that also index the contents of the hard drive. When searching in these OSs, an indexed search brings back almost instantaneous results. The same process is used within Encase 7 to significantly speed up locating search terms.

Using Keywords for a Raw Search All

Keywords and keyword files are used to define and store search terms. Keywords can be divided into groups (folders) and structured in the keyword view. This structure is used in the bookmark view to display the results of the search.

→ Make sure the Viewing Tab is in Evidence view, not Entry view (refer back to figure 8).

→ On the Evidence tab menus, choose the drop-down menu, **Raw Search All**, and select the submenu, **New Raw Search All…**

→ In the New Raw Search All dialog box, rename the keyword file to Bombs.keywords, keeping the default path intact (see figure 20).

→ In the same dialog box, click on **New** (note the checkbox choices for searching).

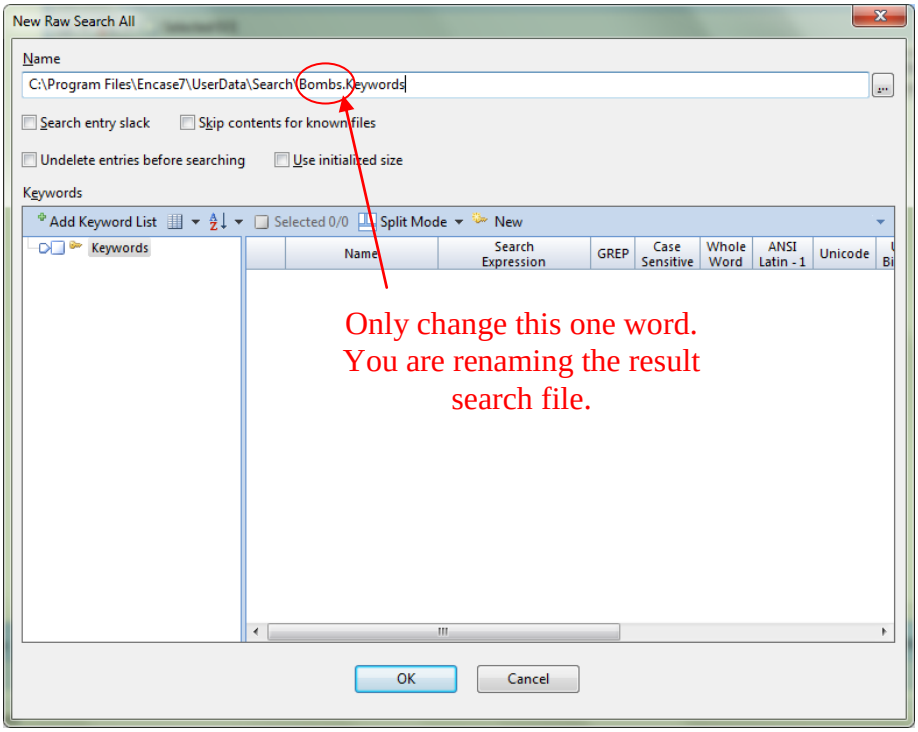


Figure 20. Rename the Raw Search keywords file

→ Create a search expression, "pipe bomb" (singular) and provide the name, "Pipe Bomb Search Term," and check the "Unicode" checkbox (see figure 21). Click **OK**.

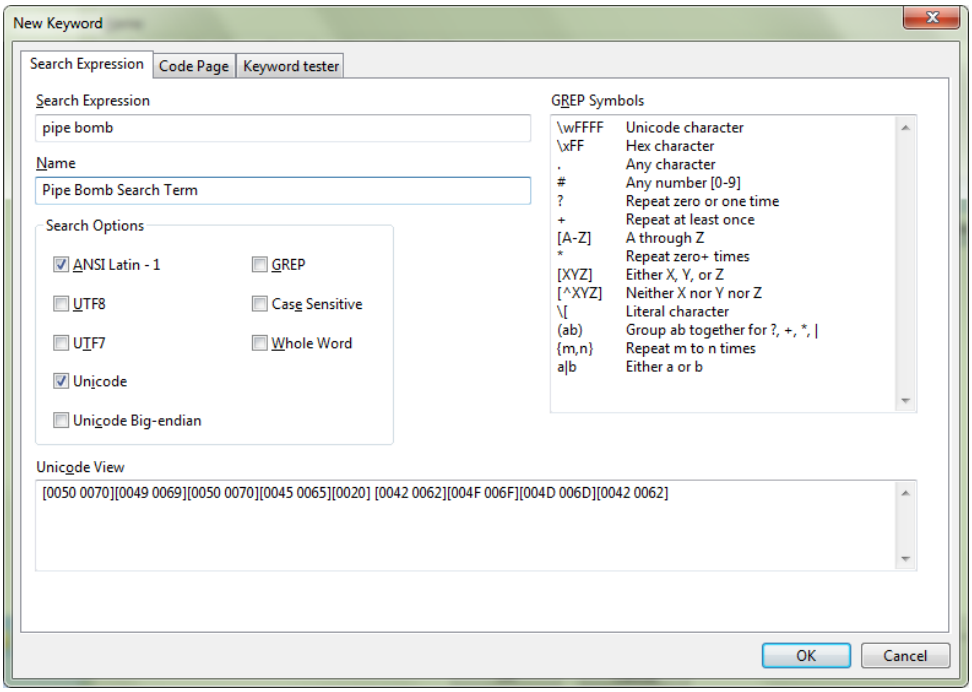


Figure 21. Creating a Raw Search All Search Expression

- → When returned to the opened dialog box, click on New again and follow the exact same process and create another search term for "time bomb"
- → Before closing the "New Raw Search All" dialog by clicking **OK**, notice that both pipe bomb and time bomb search terms are checked. Any unchecked search term will not be processed.

The user will now be back in the default "Viewing (Evidence)" view of Encase. To complete the search:

- → Select the **View** menu and then select **Search.** This will bring up the "Search" tab. This action will actually perform the "Raw Search All" action before displaying the tab.
- → Click on the **Keyword** menu to see the results of the search.
- → Click on the "time bomb" entry and note the results in the table pane (see figure 22).

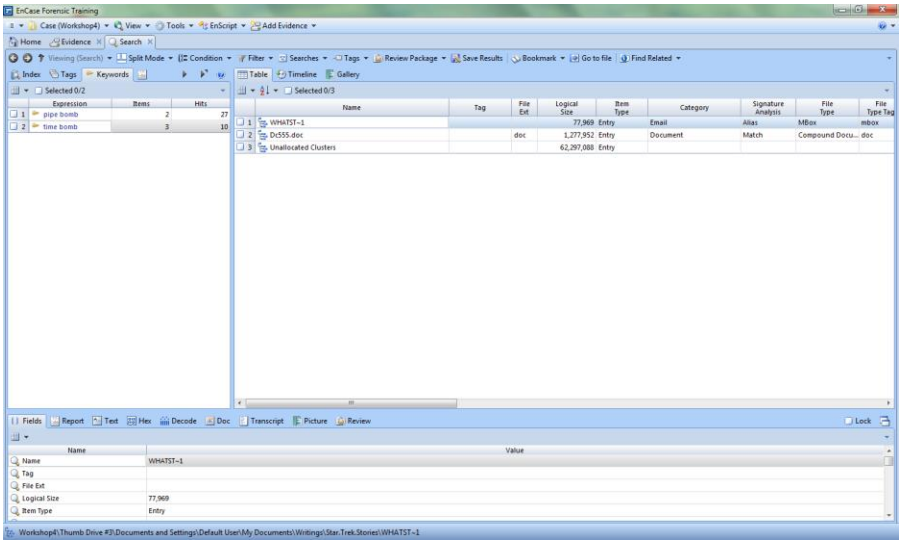


Figure 22. Search results

To view the results of the search, simply highlight the entry in the table pane you wish to view. Make sure the Text tab is chosen and change the Text Styles to "Western European Windows – Line Breaks (120)." A scroll through the text will show search hits in yellow. A quicker way to locate the hits is by using the Find function.

- → Select the "time bomb" expression under the Keyword tab.
- → In the table pane highlight "Dc555.doc"
- → Make sure the view pane has the Text tab selected.
- → Right-click anywhere on the text in the view pane.
- → Use a **CTRL-F** to bring up the Find dialog box.
- → Enter in the find dialog box the Expression "time bomb" and press **OK.**

This action will bring you to the first occurrence of the search term in the document or clusters which have been highlighted in the table pane. To view the next occurrence, simply press **F3**. Press **F3** to continue to view the next, etc.

- → Continuing the search through the text, keep pressing **F3** until the entry associated with "DRY ICE" is located

A more complex alternative is to use the "Review" tab on the view pane. This will show the starting character location of all the search hits at one location. If one of the hits is of particular interest, simply click on the hyperlinked number to the right of the text-of-interest. This will bring you to the area of the document in which this text is found.

Finding the Location of the Original File

Often, the examiner will need to reference the original location of a file in question as a result of a search hit of interest. This is a relatively simple process.

- → Select the "time bomb" expression under the Keyword tab.
- → In the table pane **Right-click** "WHATST~1". Notice the Email file Category shown in the "Category" column and "Mbox" as the File Type.
- → **Select** "Go to file" in the menu which appears (see figure 23).

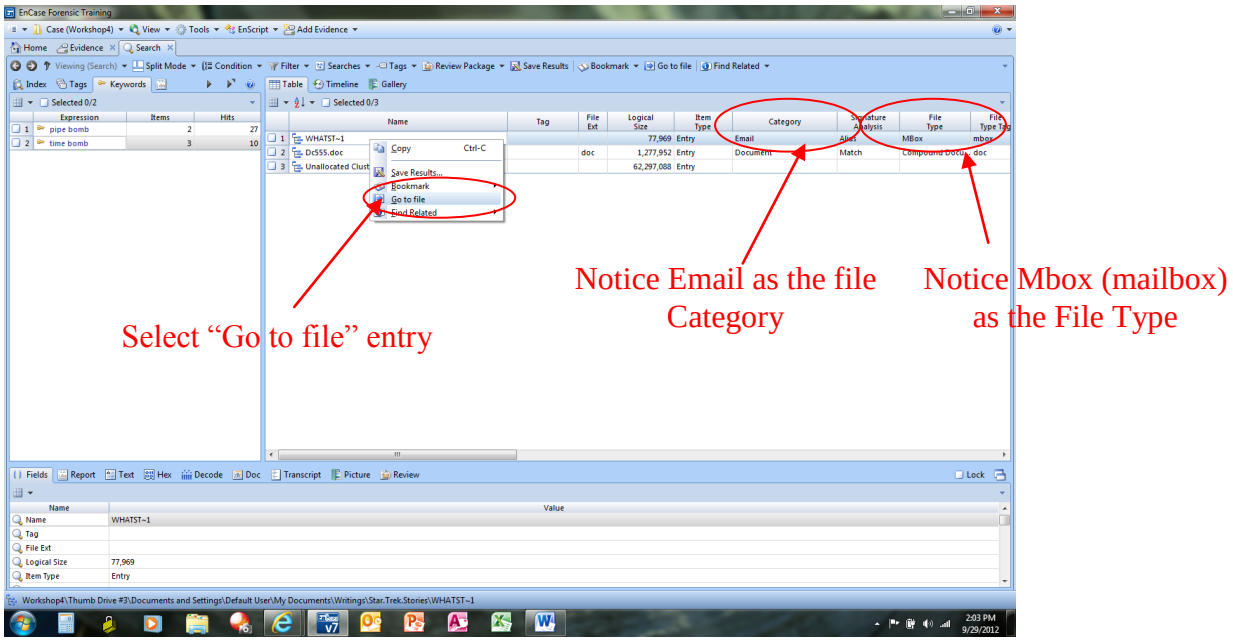


Figure 23. Finding the Original Location of a File of Interest

Encase now shows the original Entry view with "Star.Trek.Stories" highlighted in the tree pane and the file of interest, "WHATST~1" displayed in the table pane. Use the Viewing menu to return to the Search tab panes (see figure 24).

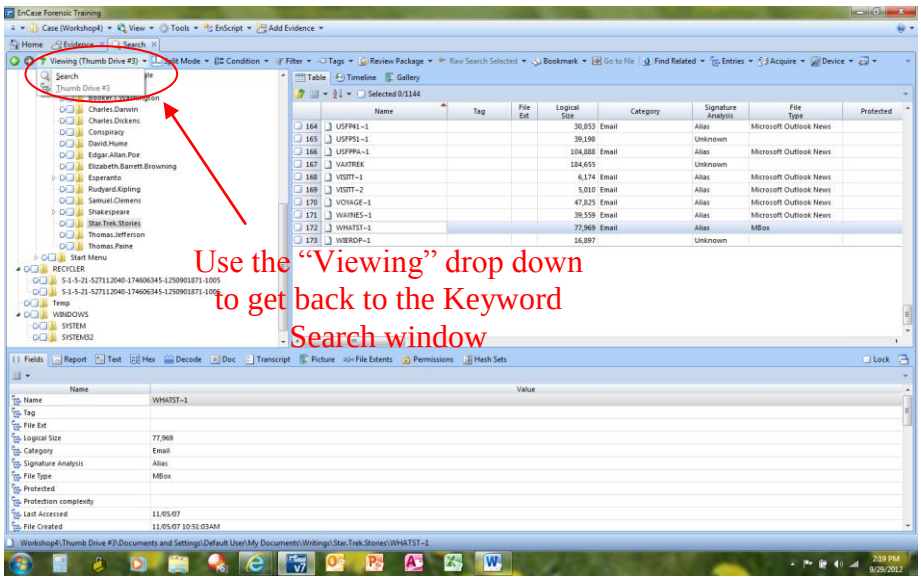


Figure 24. Use the "Viewing" drop down to toggle between the Entry view and the Search view

Modifying, Reusing, or Importing Raw Search All Keyword Groups

The keyword file created at the start of the Raw Search All process may be edited (modified or added to) or used in another case. The examiner must know the location of the keyword file to be modified or added to another case. In this tutorial, the path to the keyword file (shown in figure 20 above) is: "C:\Program Files\Encase7\UserData\Search\Bombs.Keywords"

- → **Close** the Search tab. Make sure the Evidence tab is showing and is in Evidence (not Entry) view. This is the original view when the case was first opened.
- → **Click** on the "Raw Search All" menu, "Edit" submenu (figure 25).

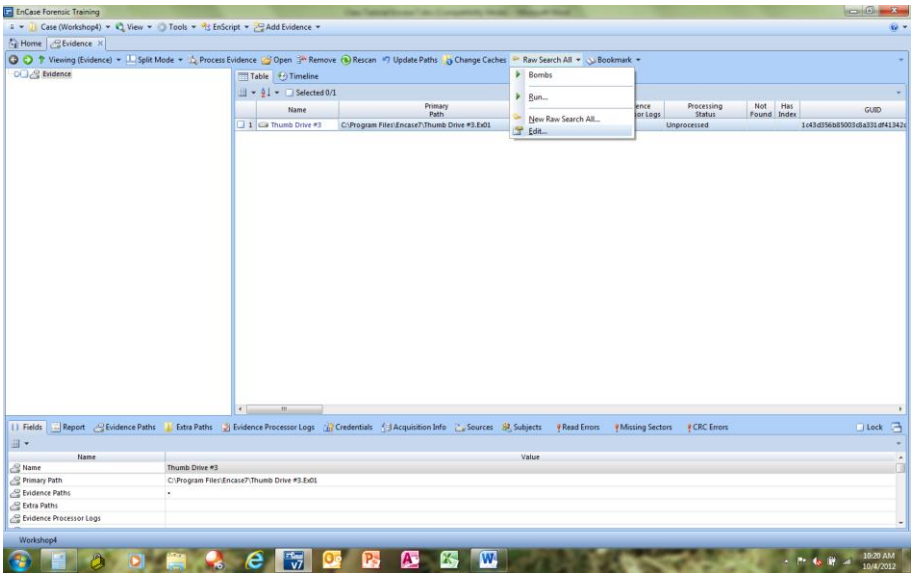


Figure 25. Modifying or Reusing Prior Searches

- → **Enter the path** to the desired search file and press **Open**. The dialog box shown in figure 20 will open. Note the title of the dialog has changed from "New" to "Edit." This dialog box will function exactly as it did earlier in this tutorial.
- → **Highlight** the entry "time bomb" search and click on the **Edit** menu and change the search expression so that it will be case sensitive.
- → **Click OK**. Click **Yes** when asked if you wish to overwrite the prior search file.

Using Keywords for an Indexed Search

Encase 7 has significantly changed from all earlier versions. Prior to this release, many forensic functions had to be carried-out manually. With this new release, the most useful tools to process a case are done automatically with the "Case Processor." Indexed

Searching is one such function. The Case Processor will be discussed more fully in later tutorials.

Setting up the Case Processor for Indexed Searching

In Encase 7.08, the Case Processor has changed slightly. There are now two components which make up the Case Processor. The first is the "Processor Manager" accessed from the Home screen (see figure 26a below). The Processor Manager is used to process multiple evidence files or media simultaneously. It is also used to show the results of a processing job (figure 26b). The Processor Manager will *not* be used in this course.

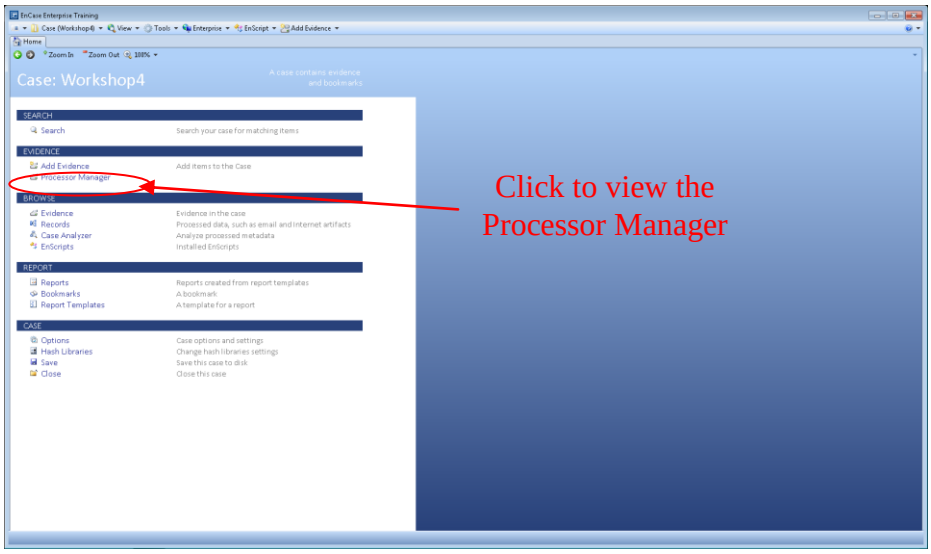


Figure 26a. Accessing the Processor Manager

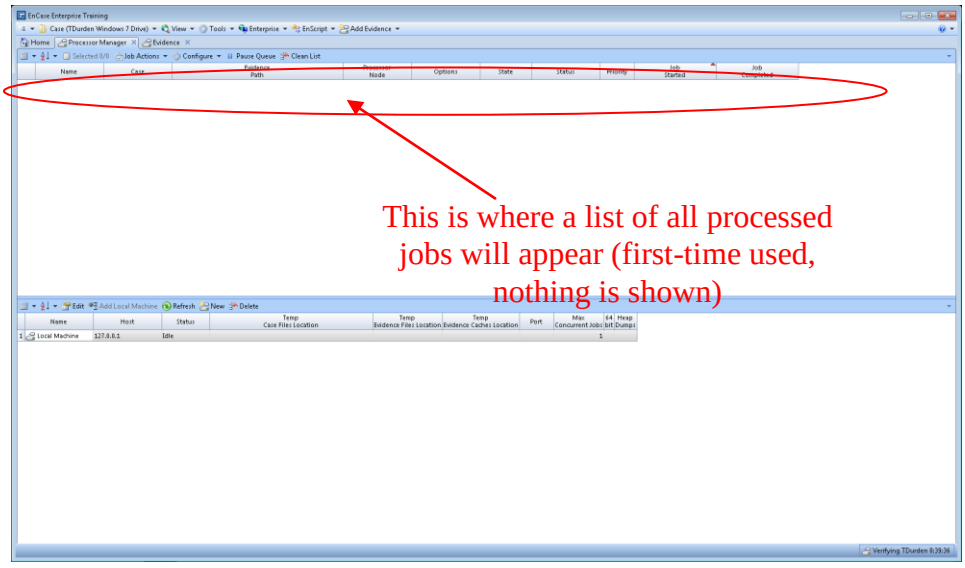


Figure 26b. Processor Manager (nothing shown as previously processed)

To actually process an evidence file, go to **Browse Evidence** from the "Home" tab.

→ **Click** on "Process Evidence->Process…" menu (see figure 26c)

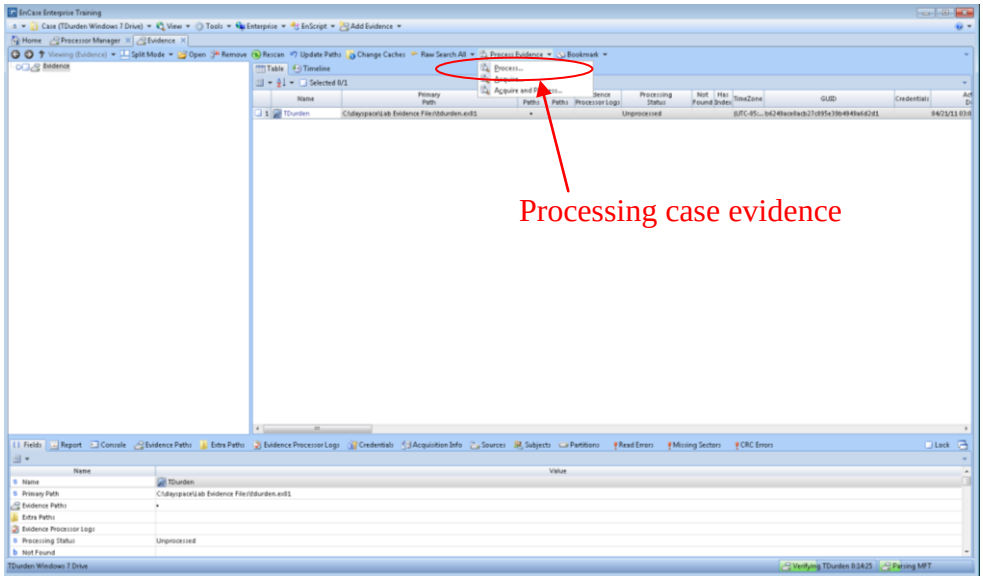


Figure 26c. Processing a Case

→ The Process Case dialog box will open providing a number of processing options
→ **Uncheck** all items except for the four items shown in figure 26d.
→ **Click** on the expand triangle next to the "Index text and metadata" entry and **Check** "Personal Information." Note the descriptions of any highlighted items in the right section of this dialog box.
→ Make sure "Current item" and "Immediately queue the evidence" are selected (defaults)

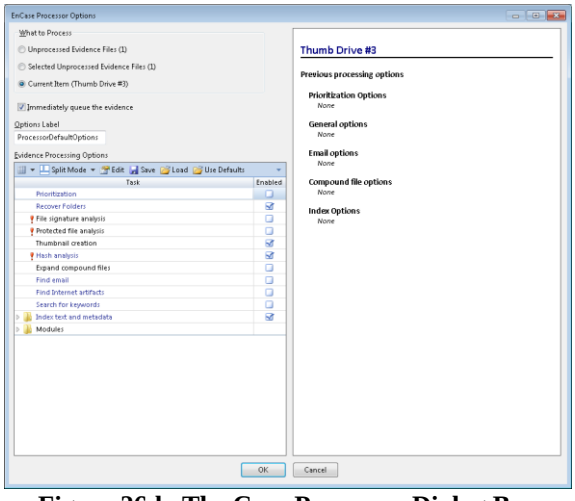


Figure 26d. The Case Processor Dialog Box

→ Click OK to begin processing the case. Note the progress bar at the lower right status bar on the Home screen.

It may take many minutes (even hours) for the case processor to finish. Be patient. When finished, Encase has created an index of all repeating elements in the case.

The Encase Evidence Processor screen may appear slightly different than the one shown above. The screen above reflects an instance where the case has been saved and then re-opened. If the case has not yet been saved, then the screen below will contain items which are defaults and cannot be checked. When processing is finished, the Process Manager will not have a single line listing the job which has just completed.

Using Indexed Searching

As previously mentioned, creating an index for searching saves an incredible amount of time in performing searches through large amounts of data. In this section, an indexed search is used to retrieve keyword similar to the method used in a Raw Search All.

In the prior Raw Search All section, the search for pipe bombs and time bombs uncovered the possibility of a bomb made from dry ice. Notice how quickly data are processed in the next example.

→ Make sure the "Search" tab is open and the evidence viewing options drop-down is set to "Viewing (Search) see figure 27.

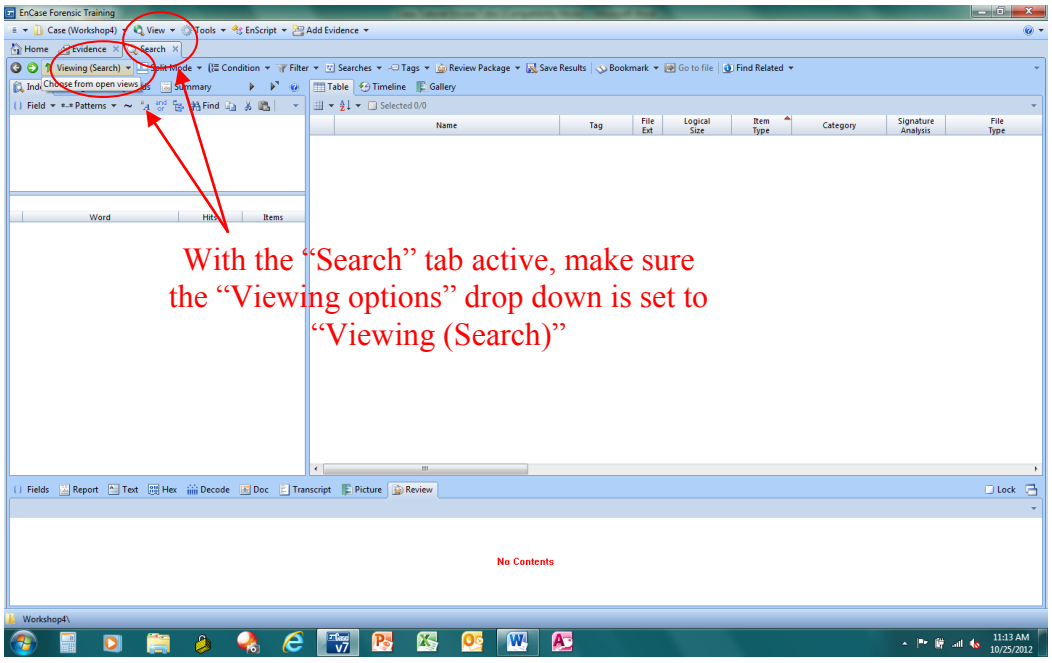


Figure 27. First step to perform an Indexed Search

→ In the left upper pane, type the word "dry" and notice how quickly the search hits appear in the panel just under where "dry" was entered (see figure 28).

All incidences of the characters "dry" appear. In this example, the word "dry" appears 864 times in 186 documents. However, to accomplish a search for "dry ice," a compound search should be used. The icons shown above the search panel allow for a number of options, the key option for this example is the use of a Boolean operator between the words "dry" and "ice."

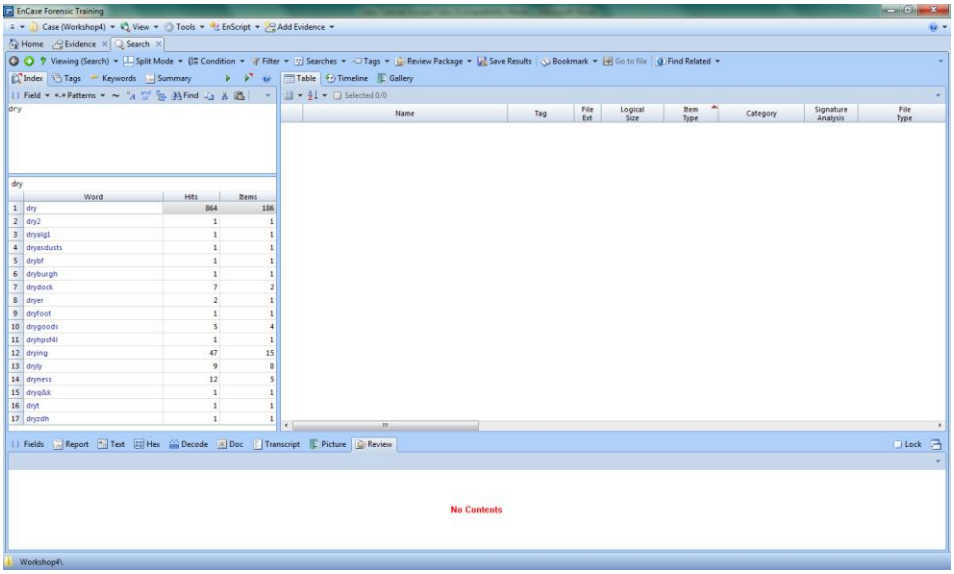


Figure 28. The results for an Indexed Search on the word "dry"

→ In the same panel in which the word "dry" was typed, click on the Logic icon to add the boolean operator "and." Alternately, the user may simply type "and."
→ Now, type in the word "ice." Do *not* press the "Enter" key.

The search hits panel reflects the entries for for the word "ice" only. The whole word "ice" appears 357 times in 77 documents.

→ Now press the "Enter" key
→ Scroll down through the documents found in the table pane. How many documents contained both words (see figure 29)?

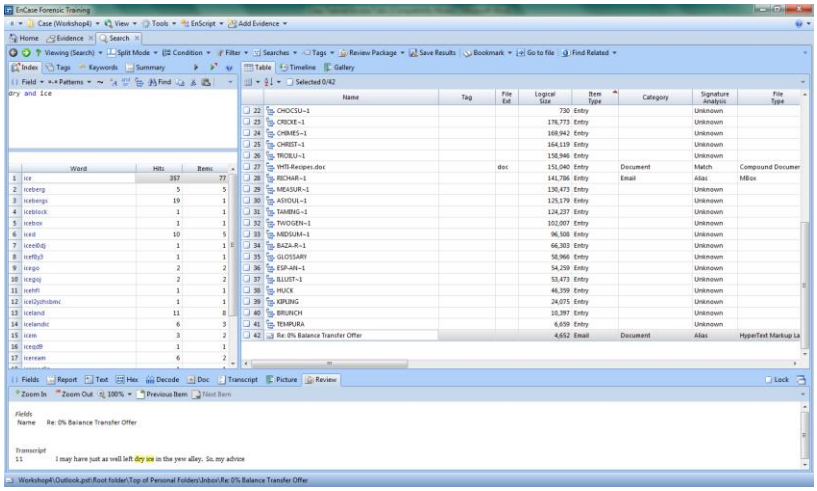


Figure 29. Documents containing both the words "dry" and "ice"

- → Choose any of the documents
- → In the View Pane, use the "Review" tab to see the context of the search hits.
- → Select a few more documents.
- → Notice that most hits do not combine the search term; i.e., "dry ice" does not appear together in most of the documents

The Indexed Search method is excellent for rapidly finding single items terms. But, as shown in the prior example, word combinations such as "dry ice" return a number of false positives. This is because the Indexed Search creates indexes on *single* words only, not word combinations such as "dry ice." The Raw Search All method, although a much slower process, is better suited to find words in context. With this said, there is a way to combine words for an Indexed Search. This method is shown under the **Searching and Viewing Emails** section below.

Bookmarking Your Findings

Overview

EnCase allows individual files, groups of files, portions of files, and data structures to be selected, annotated, and stored in a special set of folders. These marked data items are *bookmarks*, and the folders where they are stored are *bookmark folders*.

EnCase stores bookmarks in the same Case folder which was created for a given case. Bookmarks and the organization of their folders are essential to creating a solid and presentable body of case evidence. Bookmarks and bookmark folders are the basis for a *forensic report*.

Working with Bookmark Types

EnCase provides several types of bookmarks.

1. Raw text bookmarks. A.k.a. highlight data or sweeping bookmarks.
2. Data structure bookmarks
3. Notable file bookmark
4. Multiple notable file bookmark. A.k.a. file group bookmark
5. Notes bookmark
6. Table bookmark
7. Transcript bookmark

Raw Text Bookmarks - Highlighted Data or Sweeping Bookmarks

You create raw text bookmarks in EnCase by clicking and dragging raw text in the View pane, just as you would drag-click to highlight content in a text editor. This is done from the **Text**, **Hex**, or **Decode** tabs of the View pane.

To create a raw text sweeping bookmark:

- → If the **Search tab** is not opened, go to the **View menu** and select **Search**.
- → On the **Search tab**, select **Keywords**. Under the keyword searches which were created earlier, click on the "Time Bomb" search entry.
- → In the **Table View pane**, click the "Dc555.doc" file.
- → In the **View pane**, select the **Text tab** and Choose the text style **Western European (Windows) – Line Breaks (120)** (see figure 30).

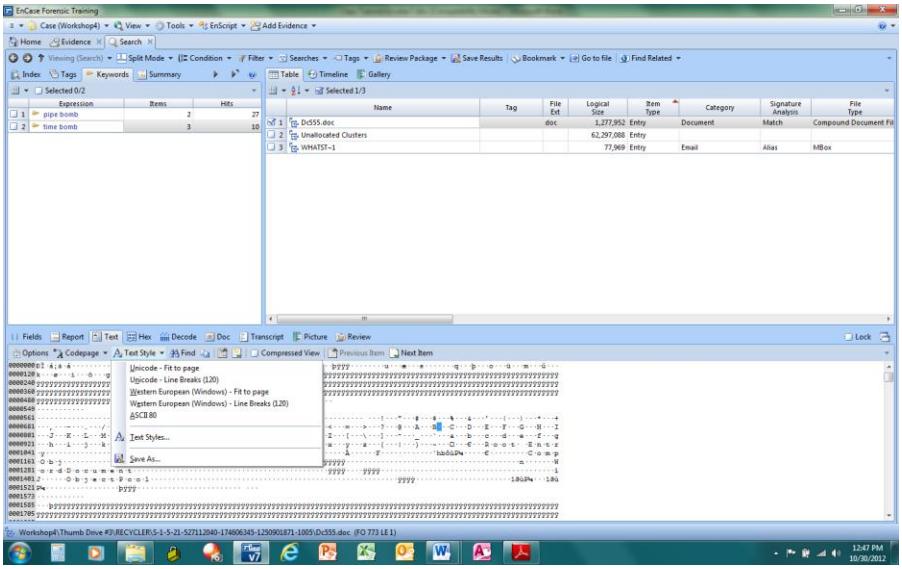


Figure 30. Viewing the contents of a document to create a bookmark

→ **Click on the Find Button** and search for "Uses for dry ice"

→ **Highlight** the entire section (down to the next heading, "FUSE IGNITION."

→ On the menu bar, **click the drop-down entry Bookmark** > **Raw text** or right click the highlighted text and click **Bookmark** > **Raw text**.

→ The Raw Text dialog displays. Type some identifying text in the **Comments** box on the **Properties** tab that makes it easy to identify the bookmarked content (figure 31).

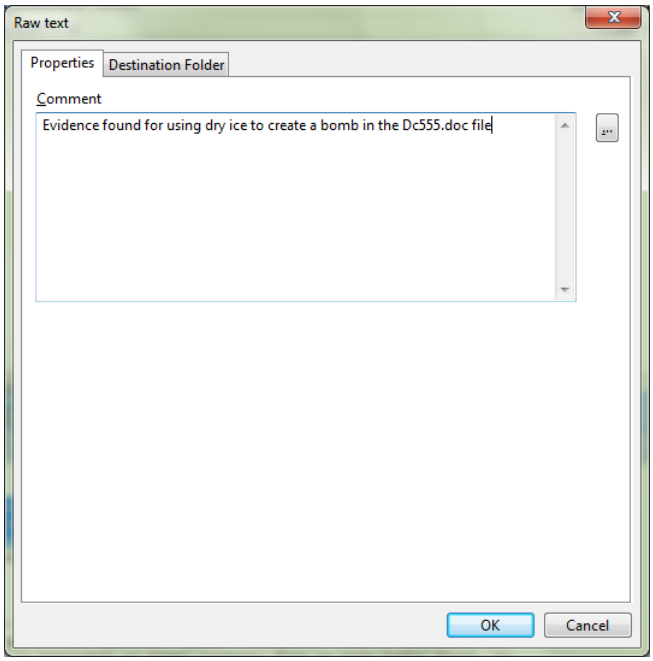


Figure 31. The Raw Text bookmark dialog box

→ **Click the Destination Folder** tab in the Raw Text bookmark dialog box. This tab displays the bookmark folder hierarchy for the current case.

→ **Click the bookmark folder** in which to place this sweeping bookmark. In the example below, the **Document** folder is selected (figure 32). Note that you can always rename bookmark folders or move the bookmark later. Also, you can easily create new folders from the bookmark dialog box.

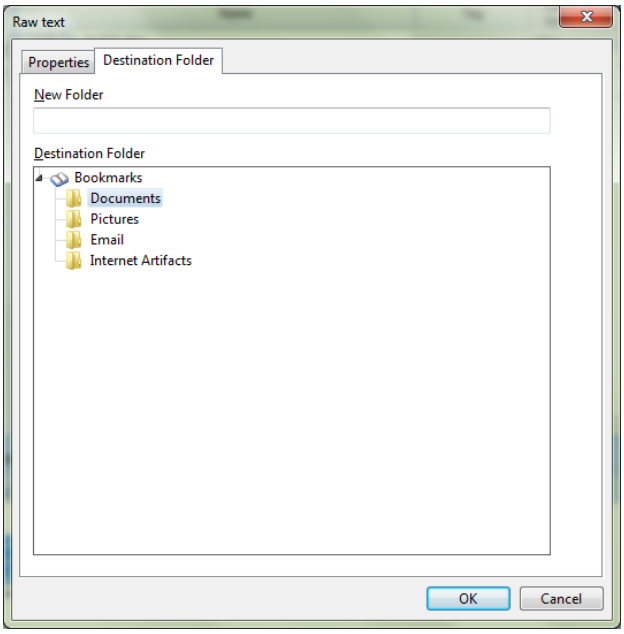


Figure 32. Placing a bookmark in a folder

→ Click **OK** to create the bookmarked content in the highlighted folder.

Data Structure Bookmarks

Data structure bookmarks mark items such as a Windows partition entry, a Unix text date, or encoded text. Data structure bookmarks is really a misnomer. A sweeping bookmark is generally used but the text which has been highlighted is meaningless. Thus, the investigator can use Encase's "Decode" capability to interpret the data and present it in a more meaningful format.

This section describes one example of creating a sweeping data structure bookmark on an html data item. Some common data structure files, such as all graphics files, are automatically interpreted by Encase. However, there are many other data structures for which Encase can easily analyze and interpret.

To create a data structure bookmark:

→ If the **Search tab** is not opened, go to the **View menu** and select **Search**.

- → On the **Search tab**, select **Index**. **Enter** the term "html" to quickly search for an html data structured file
- → Select "Latest.html" in the Table pane.
- → Examine the file content in the View pane using the **Text** tab. Most users will recognize this format as an html encoded text file.
- → **Sweep or Highlight** the entire file contents (or use a CTRL-A to select all).
- → Click the **Decode** tab. The View Types tree displays inside the left part of the View pane.
- → Since the examiner is investigating html data in this example, expand the **Text** folder and click on the "html" option.
- → The **html** option yields a satisfactory representation of the data, as shown in figure 33 below.

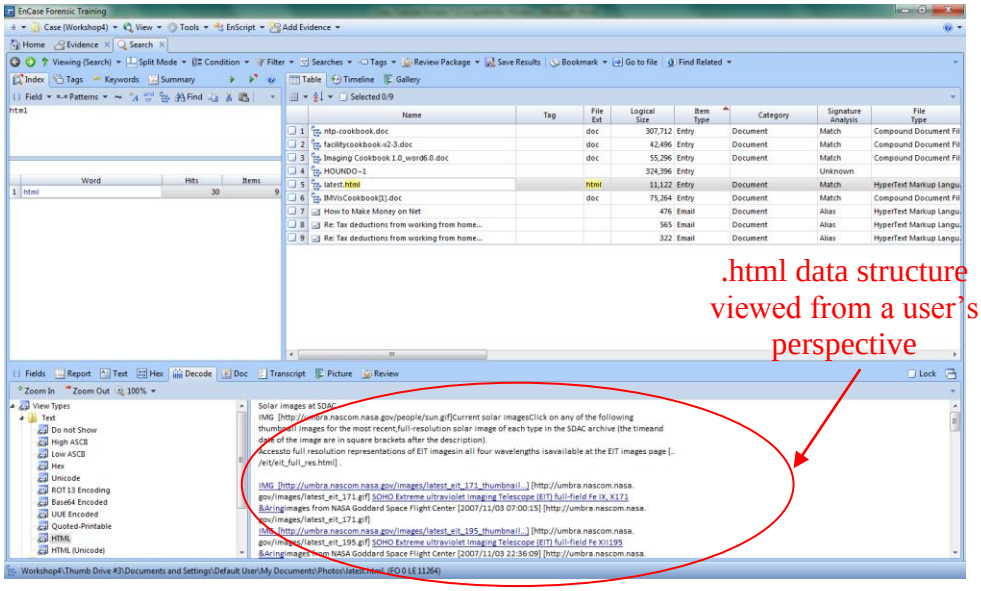


Figure 33. Using the Decode tab to interpret a data structure

- → To bookmark the data, right click the **interpreted html** code in the View pane, and select **Bookmark** > **Data Structure** *or* on the menu bar, click **Bookmark** > **Data Structure**.
- → In the Data Structure dialog, type "Translated HTML Code" in the **Comments** box and click the **Destination Folder** tab.
- → In the **Destination Folder** box, click the **"Internet Artifacts"** bookmark folder to store this data structure bookmark.
- → Click **OK**.

Notable File Bookmarks

Use notable file bookmarks to mark one or more files. You can assign notable files into a bookmark folder either singly or as a selection of files.

Single Notable File Bookmarks

To bookmark a single notable file:

From the appropriate tab, select the file of interest in the Table pane by clicking its row. In the figure 34, the "My Documents/Corporate" folder highlighted in the Tree pane and the graphic file of interest, "PYP_BOMB.jpg," is highlighted in the Table pane.

- → **Right-click** on the PYP_BOMB.jpg file
- → On the toolbar, click **Bookmark** > **Single item...**

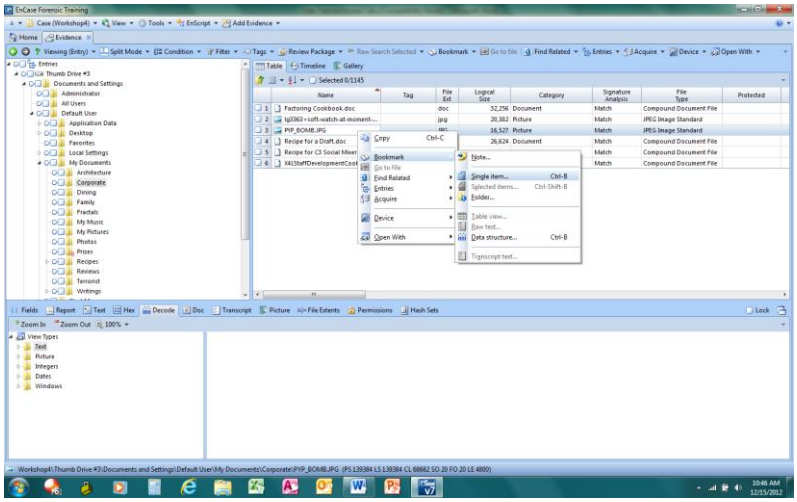


Figure 34. Selecting a Notable File bookmark

- → The Single item dialog opens. On the **Properties** tab, type some identifying text in the **Comment**. Alternatively, you can use the browse button to view a list of existing comments, and select one of those.
- → **Click on the Destination Folder** tab to display the case's bookmark folder hierarchy. Click the **"Pictures"** bookmark folder as the location in which you want to store the bookmark.
- → Click **OK**.

Multiple Notable Files Bookmarks or File Group Bookmarks

You can also select a group of notable files to bookmark. This feature allows you to quickly store a collection of notable files into a bookmark folder, which can contain other bookmarks.

Note: You cannot use this bookmark selection with sweeping bookmarks.

To bookmark a selection of notable files:

→ In the Tree pane, select the "My Documents/Terrorists" folder.

→ In the Table pane, **check** the three files that have the word "explosion" as part of the filename.

→ On the toolbar, click **Bookmark** > **Selected items...** (figure 35).

This is an alternate method to using a right-click. Both do the same thing. Also note the lower-right corner of the file icons have a ∅ symbol attached indicating a deleted file (or folder). In this example, the icon appears next to a deleted graphic.

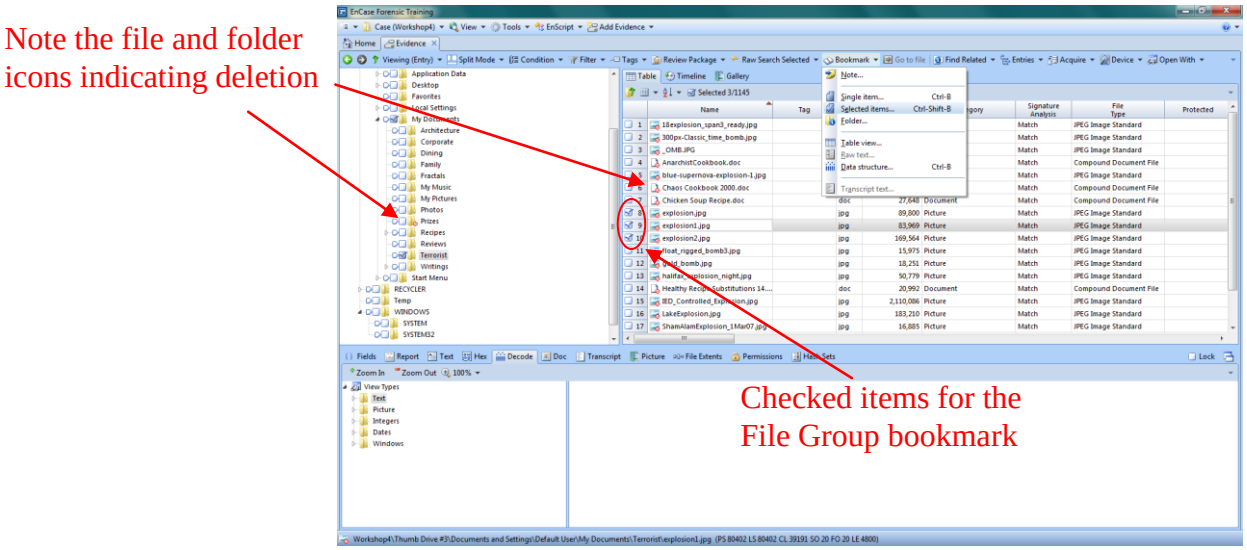


Figure 35. Selecting a File Group to bookmark

The "Selected Items" dialog box opens allowing for the naming of a new folder for the selected group (figure 36).

→ First highlight the **Pictures** bookmark folder. Under **New Folder** type **"Deleted Pictures."** This will create a Deleted Pictures bookmark subfolder in the Pictures bookmark folder.

→ Click **OK**.

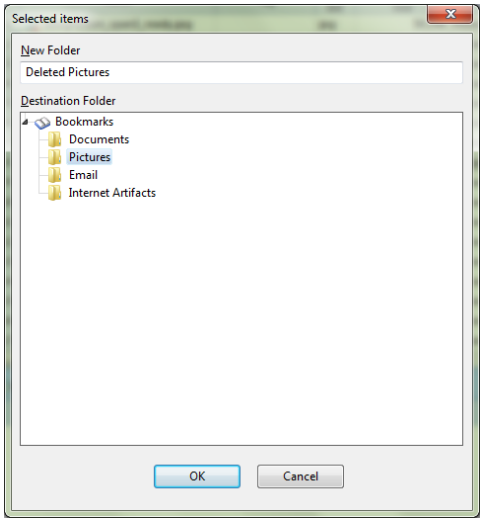


Figure 36. Creating a File Group bookmark folder

Table Bookmarks

You can select the contents of all document and folders shown in the Table pane with a Table bookmark. By highlighting any folder in the Tree pane, the investigator can bookmark all files and folders found within the highlighted folder. The bookmark allows the investigator to choose some or all meta data items associated with the bookmarked files and folders. Table bookmarks are especially useful for representing evidence data in reports.

- → In the Tree pane, **highlight** the folder **Writings** found under My Documents and click on the **Set Include** icon. This looks like a home plate next to the name of the folder.
- → Using Set Include with display all sub-folder *and* files found under a parent. Notice the listing in the Table pane.
- → In the Tree pane, **check the Select All** checkbox for Writings
- → **Right-click** on any item in the Table pane and choose Bookmark->Table View. Alternately, the Bookmarks drop-down menu at the top of Encase may have been used.
- → In the Properties dialog box, the first of three needed to process this bookmark, enter the fields as shown in figure 37 below.

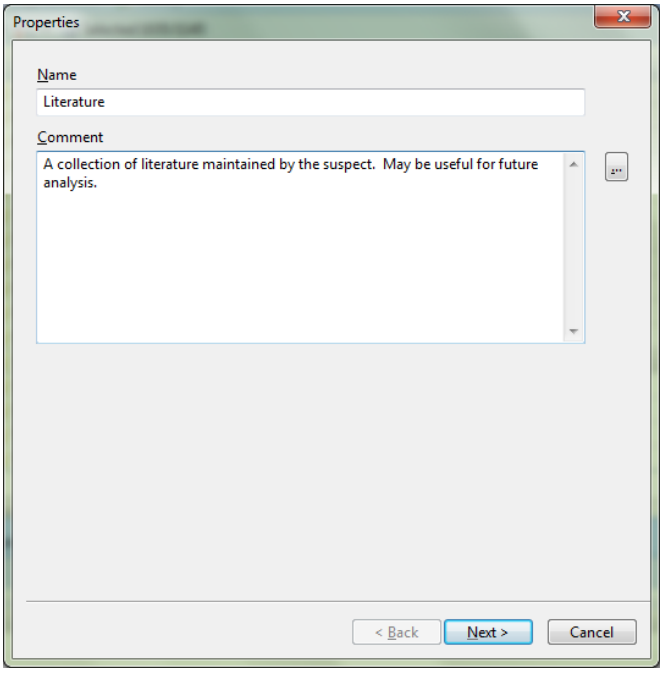


Figure 37. First step to create a Table bookmark

→ Click the **Next** button.
→ In the **Destination Folder** dialog, enter the text as shown in figure 38 below. Make sure the root, Bookmarks, is highlighted

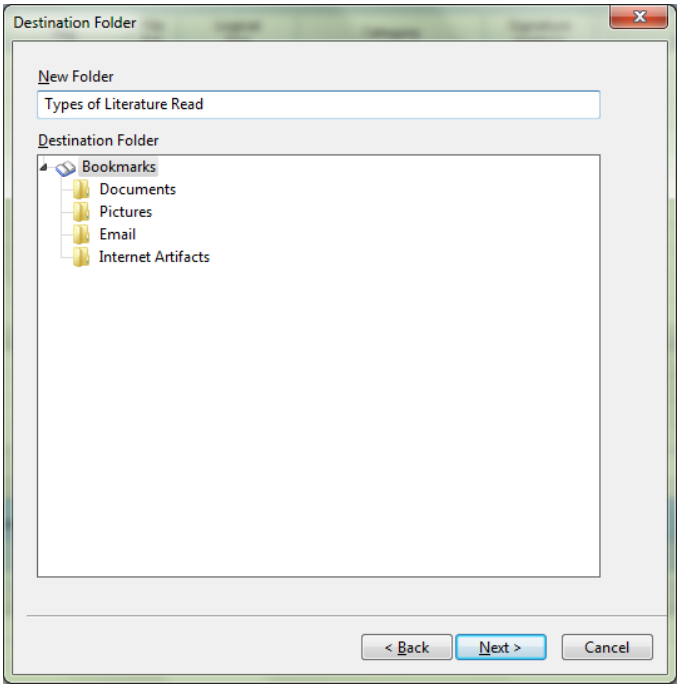


Figure 38. Step two to create a Table bookmark

- → Click **Next**.
- → The last dialog box contains all the metadata associated with every item found under the Writings folder. For this exercise, **scroll through** the list and **check** any items you wish (see figure 39). This is for demo purposes only.
- → Click **Finish**.

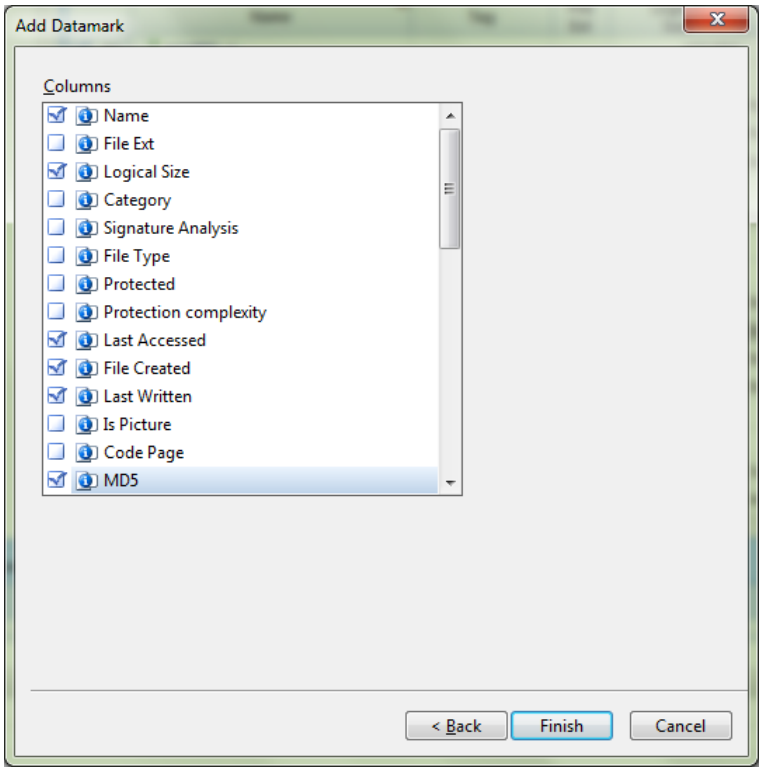


Figure 39. Step three to create a Table bookmark

A subsequent tutorial will cover report creation, but to provide the reader a better understanding of what the Table bookmark does, try the following:

- → Go to the **View** menu and **Select Bookmarks**
- → In the listing of currently available bookmarks, **check** "Types of Literature Read."
- → **Click on the Report** tab in the View pane

The table bookmark is now visible with the column headings selected in figure 39.

Transcript Bookmarks

If the **Transcript** tab in the Viewer pane is active, you can bookmark transcript text

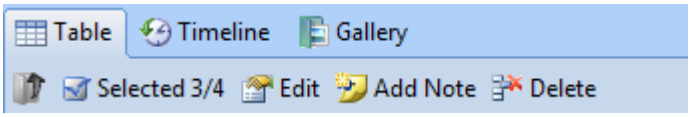
The **Transcript** tab extracts text from a file containing mixtures of text and formatting or graphic characters. The transcript view is useful for creating bookmarks inside files that are not normally stored as plain text, such as Excel spreadsheets. Transcript view is especially useful for seeing the context of keyword search results.

Notes Bookmarks

Notes differ from other bookmarks in that you use them with other bookmarks to annotate report data. They do not mark distinct evidence items like other types of bookmarks. A notes bookmark has a field reserved only for comment text that can hold up to 1000 characters.

To create a notes bookmark:

- → Click the **Bookmarks** tab.
- → On the Table toolbar, click **Add Note**.



- → The **New Bookmark** dialog opens.
- → Type a **Name** for the note bookmark, then type text in the **Comment** box or browse for a list of previous comments. This is the bookmark text to which the note will be added.

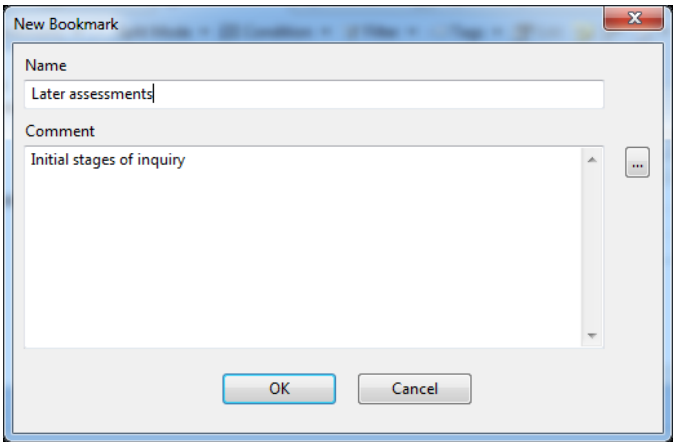


Figure 40 . Adding a Notes bookmark

- → Click **OK.**

Viewing Notes Bookmarks

If you display note bookmarks (**Bookmarks** > **Table)** in Tree-Table view, each displays as a data row in a flattened bookmark hierarchy.

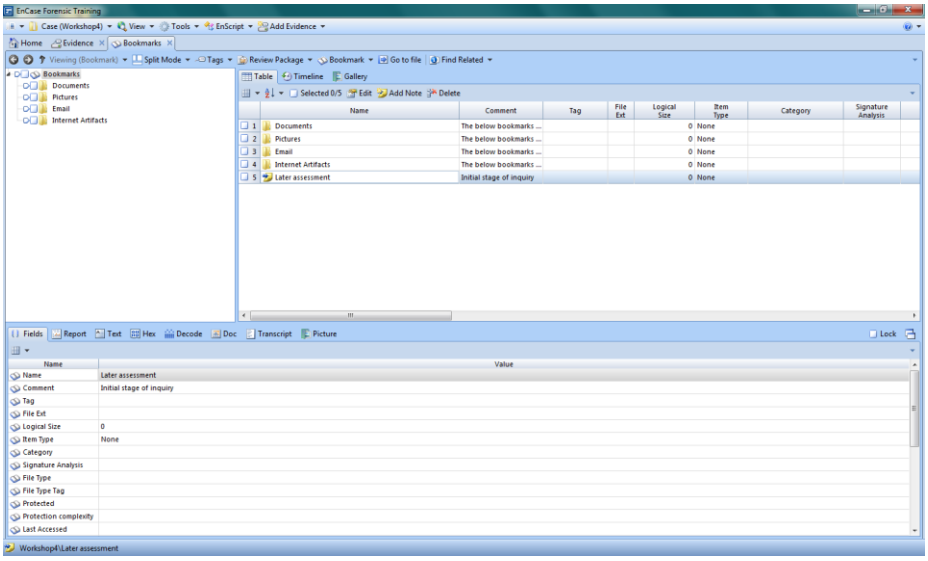


Figure 41. Using the Bookmarks tab to show a Notes bookmark

To show the notes in their true order in the bookmark folder hierarchy,

→ **Click Split Mode** on the Bookmark toolbar and select **Traeble** view.

Use the **Report** tab in the View pane to show how the note actually displays in reports.

Bookmarking Pictures in Gallery View

One of the most frequent uses for bookmarking items is to bookmark pictures or photos in **Gallery** view. The procedure for bookmarking pictures is almost the same as bookmarking single or multiple notable file items.

To bookmark a picture in **Gallery** view:

→ Click the **Gallery** tab and browse through the pictures.

→ Right click the image to be bookmarked (in the example shown in figure 42, it is the "Manchester.jpg" file) and click **Bookmark** > **Single item...**

→ The Single item dialog opens. On the **Properties** tab, type identifying text in the **Comment** box.

→ Click the **Destination Folder** tab to display the case's bookmark folder hierarchy. Click the **"Pictures"** bookmark folder to store the bookmark.

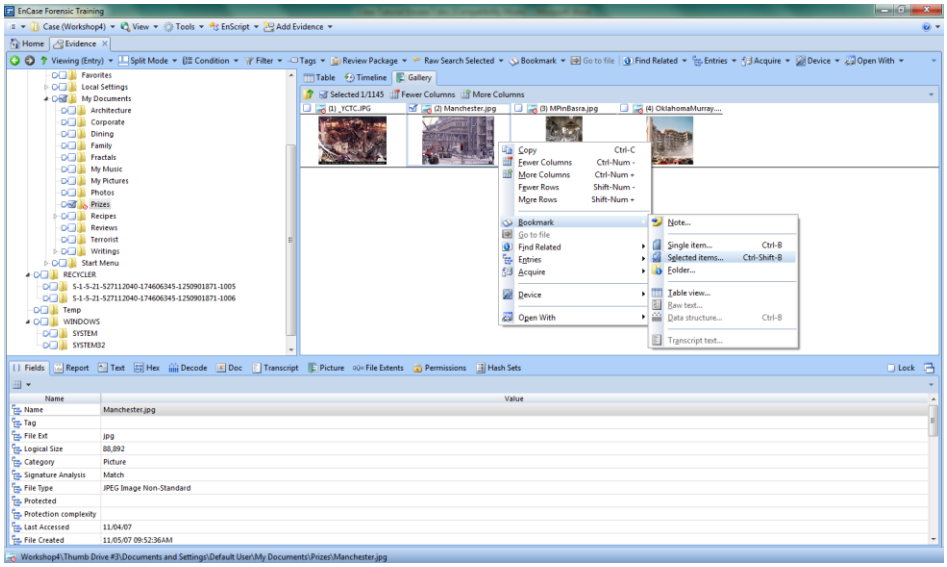


Figure 42. Bookmark a graphic

→ Click **OK**.

Working with Bookmark Folders

The bookmark folder structure is essential for organizing your bookmarks. You have a great deal of flexibility in creating a folder structure that suits a particular case.

Bookmark folders are organized according to a standard tree structure, with a folder named "Bookmark" at the top the hierarchy. The various bookmark folders (and subfolders) are beneath this node.

If you are not using the default bookmark folders, assign bookmark folder names that identify their content or are meaningful to your case team. For example, you can organize the folders by type of computer evidence, or by relevance to a particular part of the case.

Note: Bookmark folders are nonspecific in nature. Any default folder or folder you create can hold any data type or content.

Bookmark Template Folders

When a new case is created in Encase7, the examiner may choose one of four default reports. Most commonly, the #1 Basic template and the #3 Forensic template (unless you are in England). The **#1 Basic** template, include a selection of default bookmark folders. Guidance Software provides the **#1 Basic** template and the **#3 Forensic** template with a set of default bookmark folders. Depending on your needs, you may want to choose one of these when creating a new case from the Case Options dialog.

To display the set of default bookmark folders for the **#1 Basic** template, start a case and choose the **#1 Basic** template. To view the bookmark folders included in the template:

→ Click **View** > **Bookmarks**

- → In the **Bookmarks** tab, the Bookmarks root node folder displays at the top of the tree pane.
- → To expand the **Bookmarks** folder, click its tab. This displays the default bookmark folders (shown both in the Tree and Table panes).

It is recommended to use the supplied labels for the bookmark folders to organize the types of bookmarked content (Documents, Pictures, Email, and Internet Artifacts). Although this folder organization is entirely flexible, bookmark folders are directly linked to the Report template that is also included in the default templates.

If a case grows to where it needs more bookmark folders or a greater level of bookmark organization, you can create new folders or modify the folder organization, but you may need to make changes to the Report template. Creating your own report templates and reporting in general will be discussed in a separate tutorial.

Creating New Bookmark Folders

You can create new folders and subfolders at different levels of the bookmark folder hierarchy.

To create a new bookmark folder:

- → In the Tree pane, right click the **Bookmark** root folder.
- → Click **New Folder**...
- → A new folder displays one level beneath the **Bookmark** root folder highlighted in blue.
- → Type a name for the folder and click **Enter**.
- → To create a new subfolder, repeat the process at the folder level.

To edit a bookmark folder:

- → Click the **Bookmark** tab to display the tree of bookmark folders.
- → Select the bookmark folder you want to edit, right click to display its context menu and click **Edit**.
- → The **Edit <"Folder Name">** dialog opens.
- → Edit either **Name** or **Comment** for the bookmark folder, or both, and click **OK**.

To delete a bookmark folder:

- → In the Tree or Table view of the **Bookmark** tab, click the **Bookmark** folder you want to delete.

- → Right click the folder and click **Delete Folder...**
- → A delete confirmation prompt displays. Click **Yes** to delete the folder. Use caution, since deleting a bookmark folder also deletes any bookmarked items in the folder.

Bookmarks are used to mark files or files sections that are of interest. These marks are saved in the case file and can be viewed at any time by clicking on the bookmark tab. They may be viewed in the table view for organization purposes, or the report view for final viewing purposes. *If a device or compound file is removed or "dismounted" from the case file, bookmarks and search hits will be unavailable*.

E-Mail

E-mail messages will have a typical format with data fields such as from, to, subject, created date, sent date, received date, header, and attachments. There are a variety of e-mail application programs, each of which has its own file formats for this data. In addition to a variety of different data file formats, e-mail programs may encrypt the file. It is up to the examiner to survey systems under examination to determine what e-mail clients may have existed on the system. Emails are stored in what is known as a **compound file**. Compound files are single directory entries but are really made up of a number of individual contained files. Microsoft Outlook's .pst or .ost are two such types of compound files.

Viewing Compound Files

Compound files are compressed files or files in an embedded structure, such as ZIP files, PST email files, etc. For all the data to be seen in a compound file, it needs to be run through the Evidence Processor. Compound files that have been deconstructed and parsed are called "mounted" files.

To see the file structure of a compound file (manually mount), click that file and select **View File Structure.** However, it is much simpler to use the Evidence Processor. To view the contents of a compound evidence file, highlight the file and view it using the **Records** tab.

The following can be expanded and viewed after processing:

- Registry files
- OLE files
- Compressed files
- Lotus Notes files
- MS Exchange files
- Exchange Server Synchronization
- Outlook express email
- Microsoft outlook email
- Macintosh .pax files
- Windows thumbs.db files
- American online.art files
- Office 2007 docs
- ZIP and RAR archive files

- thumbs.db
- Internet files

Searching and Viewing Emails

You can open .PST and other types of mail storage files and view the individual emails within. You can view the higher order of email folder structure on the **Evidence** tab. Once the Evidence Processor is run, you can double click the email file of interest, such as the Inbox, to drill down to the individual mail messages.

The default view for Email is the Tree view. This shows the report in full screen, in as close to native format as possible. Empty fields do not display in the report view. The **Fields** tab shows all available metadata about the email and its collection, including the Transport Msg ID.

Use the **Search Results** tab to find email to view data across multiple repositories. You may also want to view all your indexed evidence and then show only items with an item type of Email. You can further drill down by finding subsets of sender, date range, etc.

EnCase allows you to track email threads and view related messages. Before you can analyze email threading, you must have already run the Evidence Processor against your case evidence with the **Find email** option selected (see figures 26 above and 43 below). To avoid displaying the same message multiple times, EnCase removes duplicate messages in both the Show Conversation and Show Related email views.

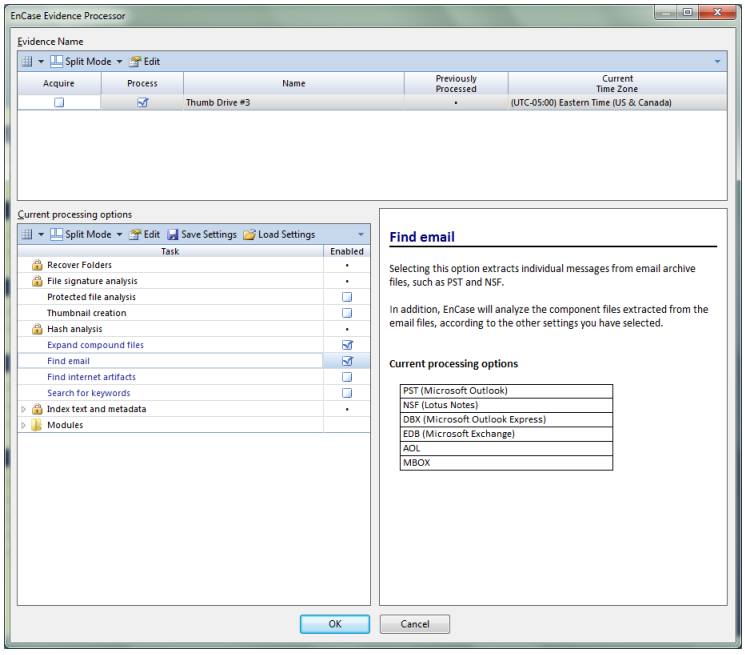


Figure 43. Using the Case Processor for emails and compound files

Viewing email messages

- → Under the **View** menu, open the **Records** tab. A listing of all emails and email containers is shown in the Table pane
- → In the Table pane, click on "Outlook.pst." The Tree view now shows the contents of this email container.
- → In Tree view, **open the Top of Personal Folders** and **Highlight the Inbox**.
- → Highlight any email listed in the Table view
- → **Click** on the **Report** tab in the View pane. The details about the message content is displayed
- → **Click** on the **Fields** tab. The metadata about the email is displayed.
- → **Click** on the **Doc** tab. This is what a user would see in the body of the email. All hyperlinks and graphics are available to the examiner (see figure 44)

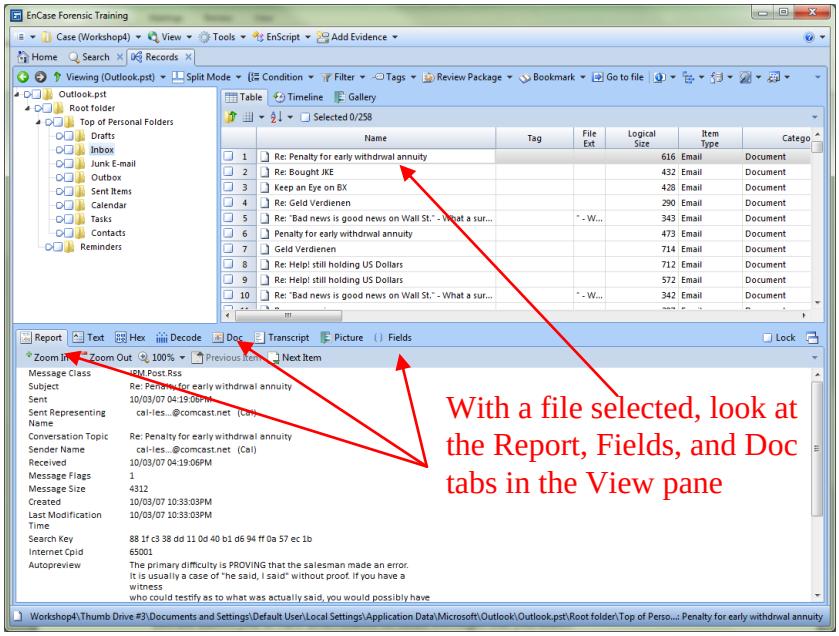


Figure 44. Examining emails

Viewing Attachments

In the tree view, email attachments are shown with a paperclip icon on top of the email icon.
EnCase allows you to view attachments on email messages that you select.
To view the content of an attachment:

- → In the **Table** pane, simply **double-click** on the message which has attachments.
- → In the new Table pane, the examiner will see a listing of all attachments from the original email.

→ Click the **Doc** button in the View pane and EnCase displays the contents of the message attachment.

Searching emails

Searching emails requires a minor added complexity to a typical Indexed search. For this example, we'll use the "dry ice" search term which failed in the introduction to Indexed searching. Raw Text searches will not examine the contents of an email in a compound container, such as a .pst file. Thus, the problem is how to keep terms together for an Indexed search. We saw that using the **AND** operator did not keep the search terms together. I.e., we returned any documents which contained both the words "dry" and "ice," but not necessarily together. To solve this dilemma, the **within** function is used in the indexed search term. The syntax for this function is "w/*an integer*." The "w" stands for "within," the forward slash is part of the syntax, and the *integer* is a user supplied, whole number indicating how many words the second word may be away from the first word.

→ If the **Search** tab is not open, go to the **View** menu and open this tab.

→ **Click** on the **Index** tab.

→ **Enter** the word, "dry" add a space and then type "w/1," add another space and type "ice." This is the command to find any instance of the word "dry" followed within *one word* the word "ice." Essentially, this allows us to create a two or more word indexed search term (see figure 45).

→ Hit **Enter** (this is essential to activate the search).

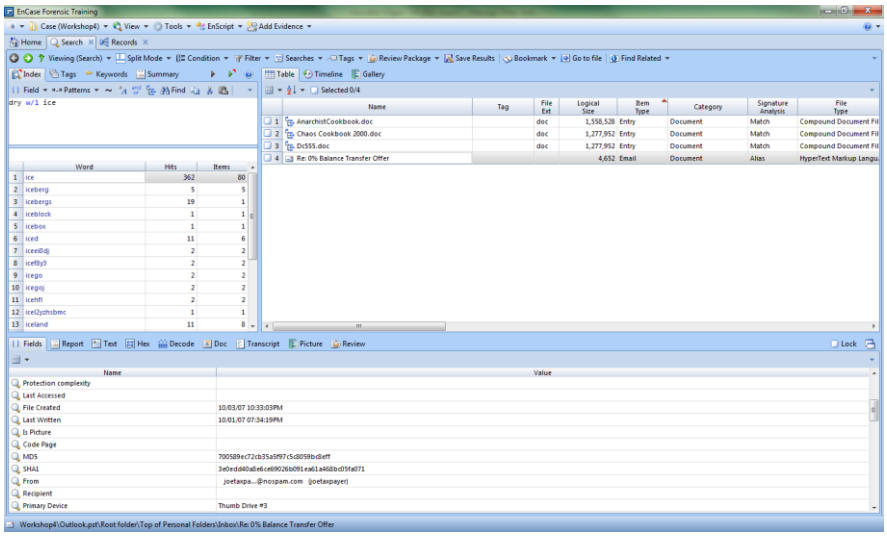


Figure 45. Creating a complex, indexed search term

The Table pane shows the four results from this search. The last item is actually an email found in the Outlook.pst file. To view the data, metadata, and contents of this email, use the same methodology listed under **Viewing email messages.**

If the reader would like to view this same message in-context of the Outlook.pst file:

- → Simple **right-click** on the email and choose the **Go to file** menu option
- → Scroll through the Table pane until you see the chosen email highlighted (in this example, it is item #59.
- → In the View pane, with the **Doc or Transcript** tab chosen, notice the email message does contain the words "dry ice."

Adding Raw Images to EnCase

Raw image files can be added to EnCase in much the same way that an EnCase evidence file is acquired from a device.

Copying and Verifying Raw Images

→ Log on to your EnCase lab computer. Open the workshop case folder:

My Documents\Encase\Cases\Workshop4

→ Open a second Windows Explorer window. From the C:\Dayspace\Lab Evidence Files folder, copy the first two files shown below into the Workshop4 folder:

1. WrkshpFlppy1.dd
2. WrkshpFlppy1.dd_audit.log
3. md5deep.exe

→ Use the second Windows Explorer window from the prior step and navigate to the C:\Dayspace\Tools\SimpleWinImageTools folder. Copy the md5Deep.exe file into the *My Documents\Encase\Cases\Workshop4* folder:

WrkshpFlppy1.dd is a 1.4k raw image file created from a floppy drive using the imager available on the Helix CD. This imager records hash verification information in the file WrkshpFlppy1.dd_audit.log. After downloading, use the following process to verify that that the MD5 hash of your copy of the image duplicates exactly the verified hash recorded in the file WrkshpFlppy1.dd_audit.log.

→ Select "Run" from the *start* menu, and enter the command "cmd" to bring up a command window.

→ Change directories with the command:

```
cd " C:\Users\bgates\Documents\EnCase\Cases\Workshop4"
```

→ View the text file containing the original verified hash using Notepad to open:

```
WrkshpFlppy1.dd_audit.log
```

→ Calculate the MD5 hash for the image file using the md5deep program:

```
md5deep -e WrkshpFlppy1.dd
```

→ Compare the MD5 hash for the image file with the log file you opened in Notepad:

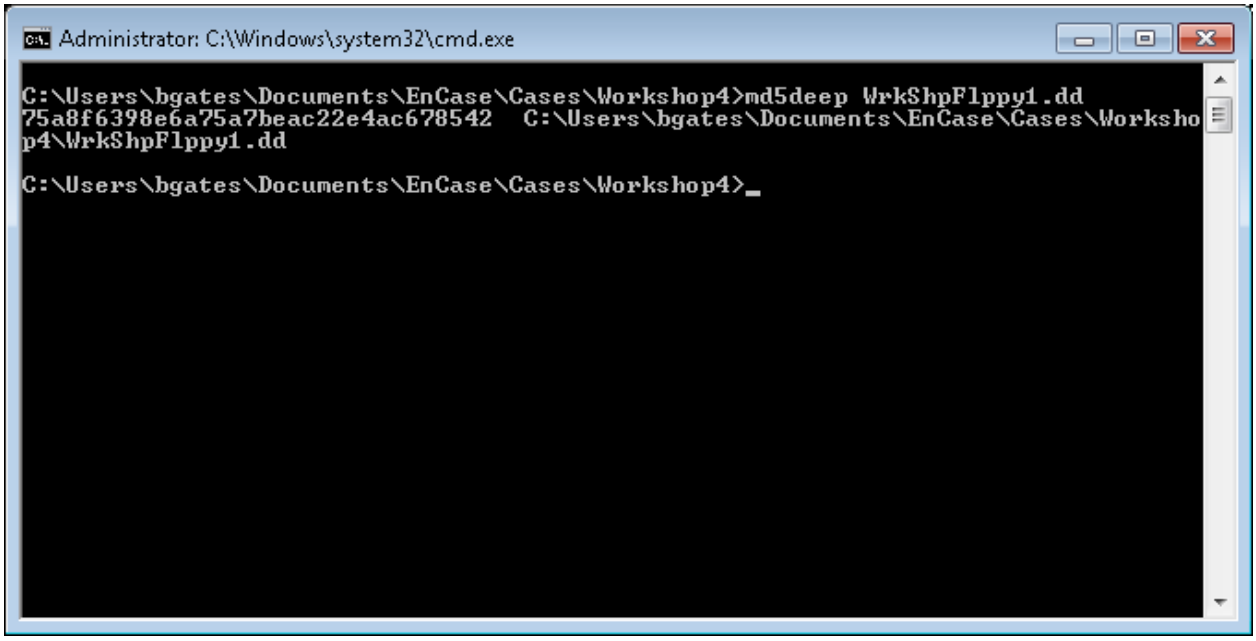


Figure 46. Verifying the image hash.

Adding Devices or Raw Images

In preparation for the acquisition of evidence, devices (such as local drives, Palm pilots, etc.) must first be added to the case. Any raw device images must be added in the same way.

→ In the "Add Raw Image" dialog box, **click on New**. In the "New File" dialog box, **Select the Image WrkshpFlppy.dd and click OK, t**he **image file is now added to the case** (See figure 48 below)**.**

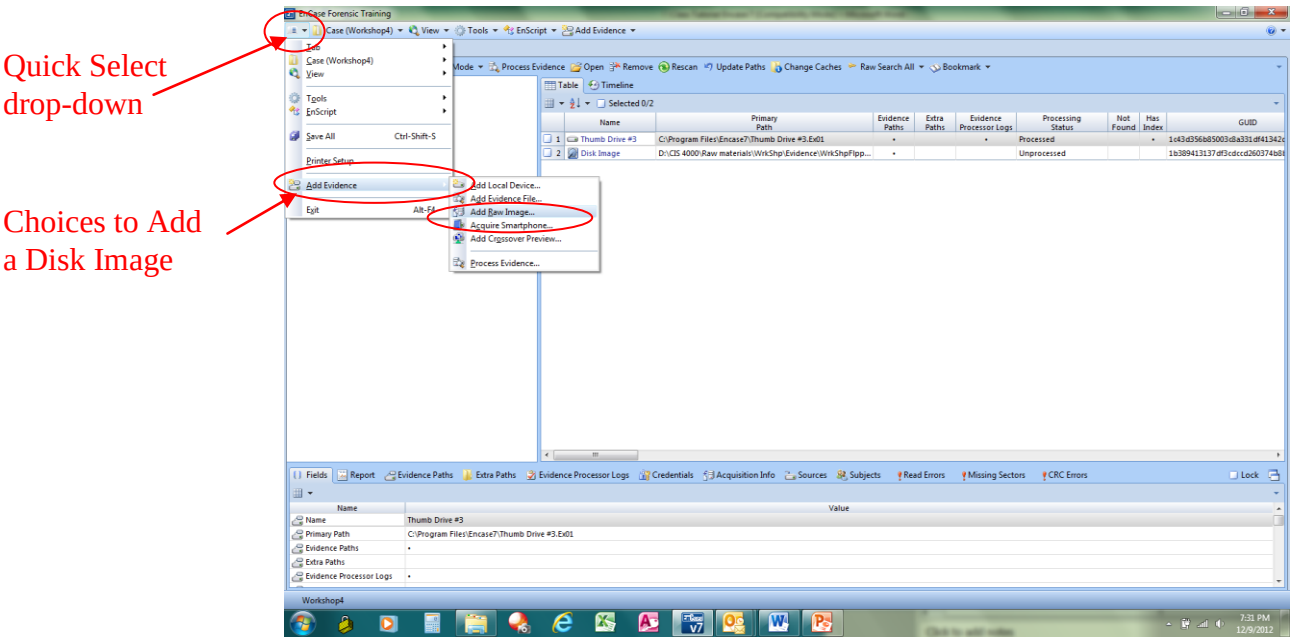


Figure 47. Shortcut for acquiring any media

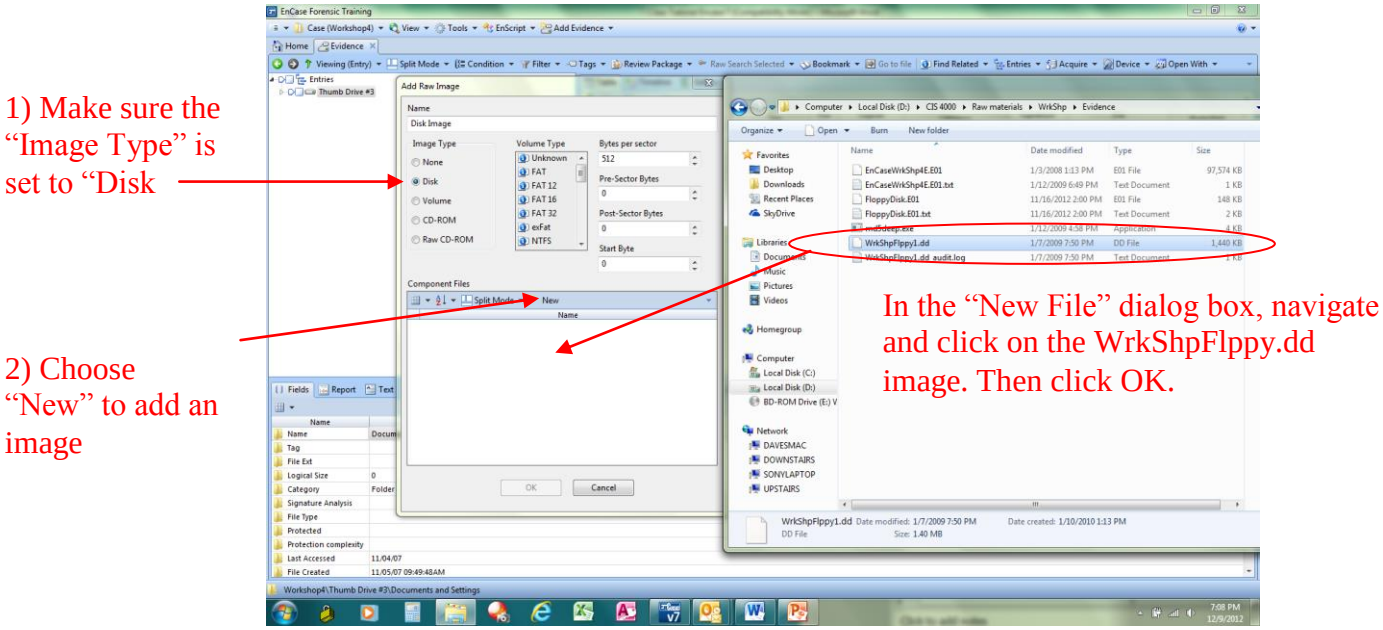


Figure 48. Acquiring a Floppy Disk Image

→ In **Tree View**, scroll to the right until you see the "Verification MD5" column. Right click on the hash value and **Copy** to the clipboard.

→ **Open** the "WrkShpFlppy1.dd_audit.log." It is a text file so no special processing is required. **Paste** the MD5 has from the prior step into the log file under the MD5 has value when the floppy was originally acquired. Do these values match??

Acquiring and Processing Evidence

The Raw image which has added to the case has yet to be processed. The examiner will both acquire the raw image and process it simultaneously. In doing so, the acquisition will convert the raw image to an Encase evidence file as well as rename the original raw image name. The processing will automatically retrieve a number of forensic artifacts which will be useful to the examiner. One, in particular, is the recovery of deleted folders and files.

Process the new evidence is accomplished similar to the method shown earlier in this tutorial (see figures 26a-26d)

→ On the Home screen, under the "Evidence" heading, **click on** "Process Evidence."

→ The **Encase Evidence Processor** dialog opens. Keep all the default choices.

→ In the "Process" column, check the box for the newly acquired **Disk Image**. Also, make sure "Recover Folders" is checked (see figure 49). This checkbox must be checked first.

→ Next check the "Acquire" checkbox next to the "Process" checkbox. You must check the "Process" checkbox first. (why?)

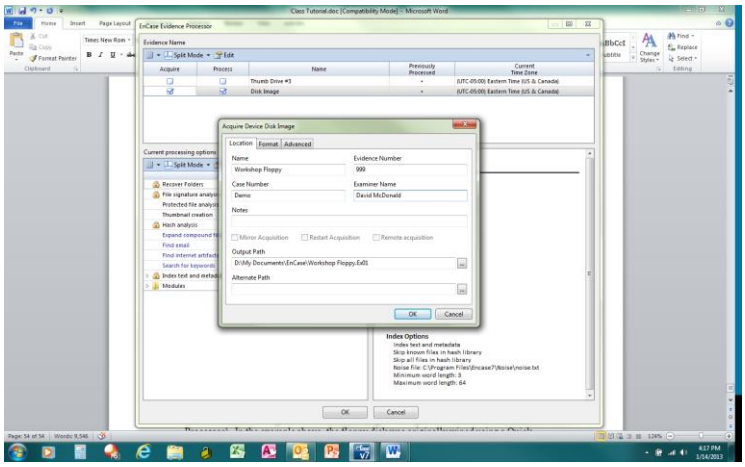


Figure 49. Acquiring and Processing added evidence

→ In the Acquire Device Disk Image dialog box, change the name to "Workshop Floppy." What is the output path for the evidence file which will be created?

→ Click **OK**, and then **OK** again.

Notice that all files and folders which were deleted from the original floppy new appear in the tree view for the floppy. The Case Processor will automatically restore all folders and files which the original user deleted (as long as this option is checked in the Case Processor). In the example above, the floppy disk was originally wiped using a Quick Format option. When first added to the case, there were no files or folders visible.

Also note that the name of this image has been changed from a generic "Disk Image" to "Workshop Floppy," a name the examiner has provided.