

CSEC 730 - Advanced Computer Forensics

Lab 3 –EnCase Forensic Lab

Please submit your report (in PDF format) to the assignment submission folder under *MyCourses* > *Assignments* by the due date.

Objective

In this lab, you will practice the basic functions supported by *EnCase Forensic*, one of the industrial-leading digital forensic tools. In my opinion, *EnCase Forensic* is the most sophisticated forensic analysis tool. This lab will only introduce you to the fundamental features of this tool.

Lab Setup

In both Homework 3 and FTK lab, you used the Windows *FTK and EnCase* virtual machine. ***EnCase 8*** is also installed on the same virtual machine.

In case you need to re-login to the VM, the Windows login credential is:

Username: Student

Password: student

The following image files will be used for this lab and they are located in Desktop\Images folder.

1) WinLabRaw.img – Raw Image from dd

2) WinLabEnCase.E01 -- EnCase evidence file

Note: “WinLabEnCase Image” in this documentation = “Lab5 image” in your EnCase image.

Deliverables:

Submit your lab report answering all the questions in this document.

PART I: Familiar with EnCase

Exercise 1: Starting a New Case

Launch EnCase 8 – make sure that you are in the **EnCase forensics** mode (on the top-left corner of the software, you should see *EnCase Forensic Training*, NOT acquisition mode.)

On the main Home page of EnCase, create a new case using the *#1 Basic Template* and name the case “EnCase Practice”.

You may fill in “Case Number”, “Examiner Name” and “Description” information. This case information is optional.

Record the defaults that EnCase gives you for its folders. It is safe to use these defaults in our experiments.

Then another Home page for your case, *EnCase Practice*, containing SEARCH, EVIDENCE, BROWSE, REPORT, and CASE functions will show up. You may notice that the go-back arrow below the Home tab turns to blue now. When you click on the blue go-back arrow, you will go to the previous page, in this case, the main Home page. On this page, your newly created “EnCase Practice” case hyperlink is listed under RECENT CASES. You can always open this case by clicking on this hyperlink.

Now, go back to your Case Home page.

Add a Raw Image to the existing case

Under EVIDENCE, you click **Add Evidence**.

To add the given raw image, click *Add Raw Image*, and fill in “WinLabRaw” in the “Name” field.

Under “Image Type” choose “Disk”. Under Component Files, click New, locate and select the “WinLabRaw.img” file from the Desktop\images folder, and click “Open”. Click “OK”.

The image is now added to your case, and a new Evidence page is created. Double-click on the hyperlink of “WinLabRaw”, and you will be able to view the files and folders from the image. You can always switch between pages using the top-left blue go-back arrow (Figure 1 below) or blue go-forward arrow.

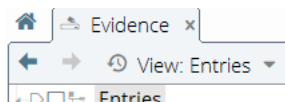


Figure 1. Green Arrow to go back

At this point, your *EnCase Practice* case is ready for your examination.

Save the case using the Case (EnCase Practice) drop-down menu's **Save**.

Navigating the EnCase Evidence

Let's go back to our evidence to explore our Disk Image evidence page.

You may have to click the hyperlink to locate the "WinLabRaw" case.

Under the Evidence tab, click the "Choose a viewing mode" (right next to "View Entries") drop-down sub-menu, by default, you are in a Tree-Table view where the screen is divided into three sections: **Tree Pane at left**, **Table Pane at right**, and **View Pane at bottom**.

The Tree View at the left pane shows a list of files and folders. When you **green-select** a directory in the tree by clicking on the polygon next to the tree of the folder name in the Tree Pane (see Figure 2 below), the files/subdirs in that directory are shown in the Table Pane located on the top right of the EnCase screen. Each row shows one file/subdir displaying the file's name and other attributes such as MAC times, file extension, size, md5 sh1 hashes, deleted, etc.

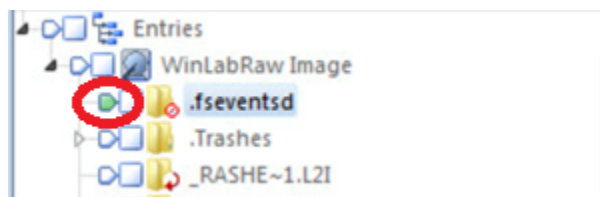


Figure 2. Green-select the folder ".fseventsd"

If you click on any file/row in the Table View, this file/row will be highlighted. The View Pane at the bottom will display the content of this highlighted file. The Fields tab in the View Pane provides you with a table of the metadata for the highlighted item. The file content can be displayed in various views such as text, hex, doc (for Microsoft Word), Picture, etc.

After you are done with the selected folder ".fseventsd", remove the green select by clicking on the polygon again to deactivate green-select.

Now, green-select "Entries" in the Tree Pane. You will see every file/dir is shown in the Table pane. The first file, *Disk Image (the raw image we added to this case)*, is highlighted by default. Its content is displayed on the View Pane at bottom. Explore each column in the Table view (with Table tab selected).

Click on the "Report" tab in the View Pane and read the Report content. After you are done, remove this green-select.

Question 1: Based on the information of the Disk Image Report, what is the file system of this raw Image?

- The file system of this raw image is Fat12.

Next, choose “Disk View...” from the Evidence tab’s top drop-down sub-menu located at the top right-hand corner (see Figure 3 below), then click the first sector (in red), the volume boot (see Figure 4 below), and read the text in the bottom pane. You should also see the file system information in the volume boot although most of the part is unreadable.

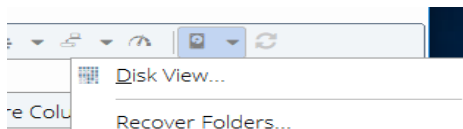


Figure 3. Disk View...

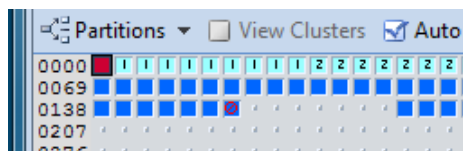


Figure 4. Disk view of the image’s volume boot

In the “Disk View”, the green sectors represent the clusters used by the root directory. Click the first green sector, the root directory content will be shown in the bottom pane. Click the “Hex” tab to display the content in hex view. Since each file/dir entry in the root directory uses 32 bytes to store information such as the filename and extension, entry type, the address of the first data cluster, the length of the file, etc., you will resize the hex view’s width to be 32 bytes by moving the cursor on the right edge and dragging the right edge of the View Pane to right (or left). As shown in Figure 5 below, the first column in grey color indicates the offset of each row and the second row of the Hex view starts at offset 032. With this setting, each row of the View Pane displays the metadata information for one file or subdir. The first 8-byte represents the file’s filename.

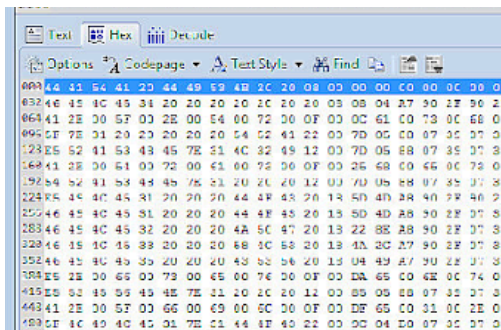


Figure 5. Resize the hex view to 32 bytes per row

(Hint: If you are not able to fit 32 bytes per row on the screen, change the display settings of the virtual machine to 1280x720)

Question 2: Exam the root directory content in the View Pane of “Disk View”, What is the first character (in Hex) of the filename of a deleted file?

- The first character, in Hex, of the filename of a deleted file is E5.

Next, you may click on the sectors in different colors, to see their contents and try to understand various information displayed on the pane. After you have had enough fun, close the Disk View by clicking the “x” on the Disk Image tab.

Now let’s add the EnCase Image, WinLabEnCase.E01 located at Desktop\images, to the existing case via EnCase’s “Add Evidence” from the top menu, choose **Add Evidence File...**

Question 3: What type of files can be added using EnCase’s “Add Evidence Files”

- The type of files that can be added using EnCase’s “Add Evidence Files” are Legacy Evidence File, Current Evidence file, SafeBack file, vmware file, Legacy Logical evidence file, current logical evidence file, and virtual pc file.

Now you have two pieces of evidence added into the case. You can view either one by selecting it from the “Evidence” page/tab, or via *View->Evidence* from the top *View* menu.

Exercise 2: Analyzing Evidence using Encase

Click on the Evidence tab and go to the “WinLabEnCase (Lab5 image)” evidence page.

Set the Time Zone

EnCase will utilize the time zone setting of your examiner workstation if no time zone is set for the evidence.

When you acquire a computer as evidence it is important to make note of the computer’s time and time zone, especially if you need to correlate evidence from different time zones (never assume the time or time zone on a computer is correct.)

Question 4: Where does the Time Zone information reside in a Windows system? (Hint: See EnCase User guide).

- The time zone information reside in Eastern time US & Canada.

Before starting the evidence analysis, you should verify that the time zone settings for the evidence are configured properly and modify the time zone setting if necessary.

In our case, since our simple image does not include the time zone setting for the system, let’s assume the computer’s time zone is “Eastern Time”.

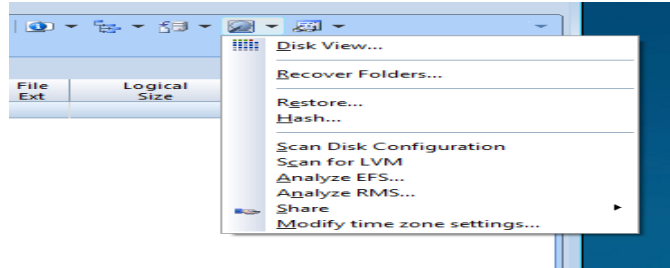


Figure 6. Verify or modify time zone settings

Question 5: How do you verify (or modify) the EnCase Time Zone Settings?

- According to the user guid, you can verify by clicking on the device and then Modify time zone settings. Then it will show you the time zone that it is set to.

Now that you have the evidence added and the time zone set, you can analyze the evidence.

Timeline View

The Timeline view gives you a graphical overview of file creation, modification, and access times and dates in a calendar view. It allows you to look for patterns.

Green Select the WinLabEnCase Image and click on the Timeline tab in the Views pane.

The timeline view can be zoomed from a yearly view to a minute-by-minute view using the *Higher Resolution* button and *Lower Resolution* button.

The colored dots represent activity on a particular file. The legend for the colors can be found by clicking the “Options” button from the top menu.

Question 6: Why is Timeline View useful for your investigation?

- The timeline view is useful for investigation because then you can see what was done to or with a file on what day of what month of what year. This way you can see which files could be malicious any file that was used on a specified date that can be a potential evidence file.

Gallery View

The Gallery view allows you to quickly see all the pictures in the case. Now let’s switch to the “WinLabRaw” image via **View -> Evidence** then open the “WinLabRaw” image. Green select the Disk Image, in the Views pane, select the **Gallery** tab.

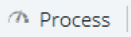
You will now see all of the pictures contained in the WinLabRaw image. However, please be aware that the Gallery view displays graphics files based on file extension. If a graphic file's extension has been changed to .txt. The file will not originally be shown in the Gallery view until the file signature analysis is done.

Question 7: In the WinLabRaw image, how many pictures are shown in Gallery View before performing file signature analysis?

- There are 3 image files that are shown before performing file signature analysis.

Process the Evidence

“Process the Evidence” contains major forensic analysis functions in EnCase. For example, *File signature analysis*, *Thumbnail creation*, *Hash analysis*, *Find email*, *Find internet artifacts*, *Search for keywords*, and many more.

Under the Evidence tab, click on “Process” . The Evidence Processor Task will show as Figure 7 below. You have the freedom to enable the tasks to run. For example, you may want to run certain tasks in the beginning, such as file signature and hash analysis, then later add other options, such as parsing compound files.

Tasks you must run in a specific step are marked with a red “!”. Note: If a task name is listed in a **blue** font, click on its task name to configure it. If a task name is listed in a **black** font, no further configuration is necessary.

Select the WinLabRaw image, enable at least the five tasks as shown in Figure 7, and run the evidence processor.

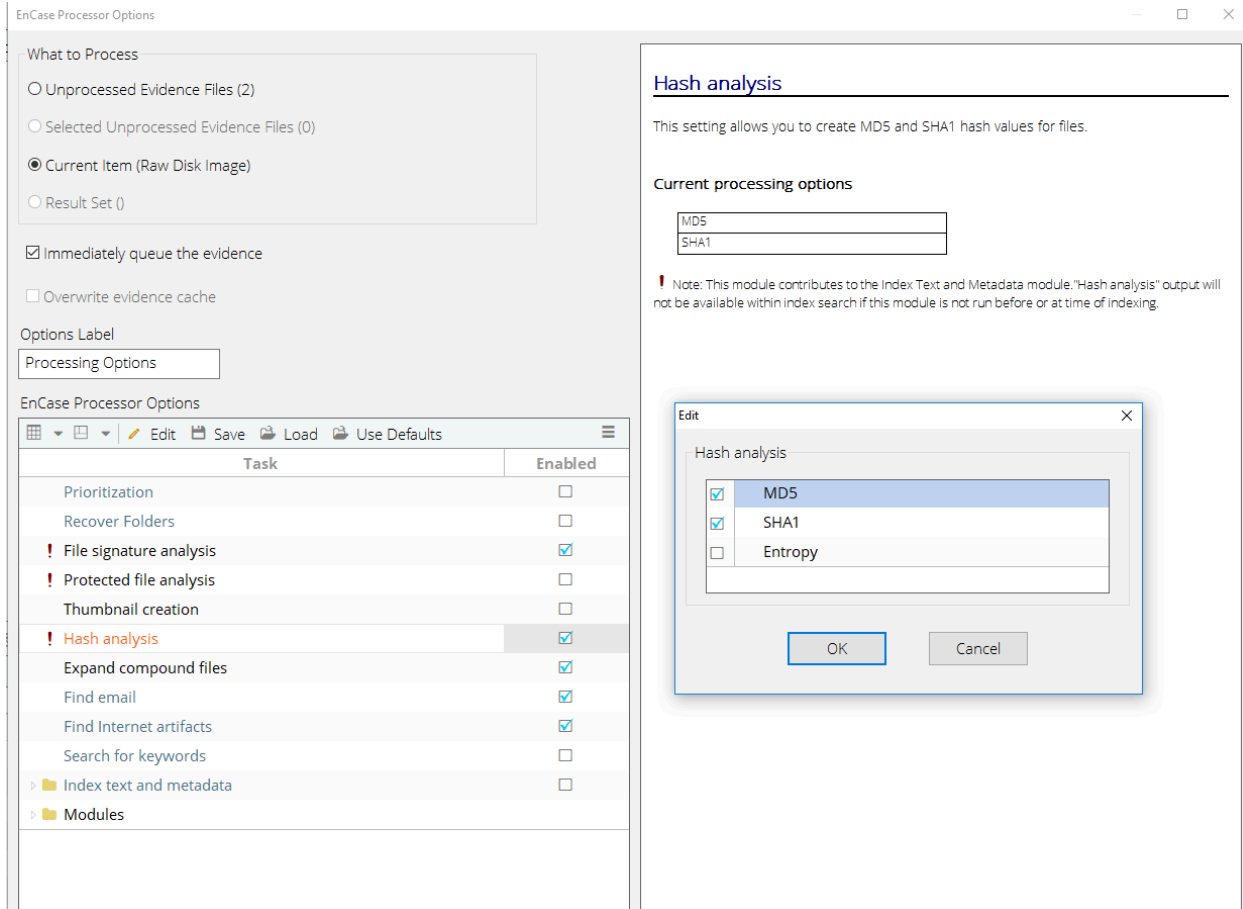


Figure 7. Evidence Process Task List

Recover folders.

Recover Folders will recover all deleted folders.

Note: For our image, you may not see anything interesting.

Question 8: How do EnCase's Recover Folders recover deleted folders for FAT and NTFS file systems? (Hint: See EnCase User Guide p. 134)

- EnCase's Recover Folder recovers deleted folders for FAT by "searching through the unallocated clusters of a specific FAT partition for the "dot, double-dot" signature of a deleted folder. When the signature matches, EnCase can rebuild files and folders that were in the deleted folder"
- For NTFS, it recovers the "folders from Unallocated Clusters and continues to parse through the current Master File Table (MFT) artifacts for files without parent folders. This operation is particularly useful when a drive is reformatted or the MFT is corrupted. Recovered files are placed in the gray Recovered Folders virtual folder in the root of the NTFS partition."

File Signature Analysis

A file type (JPEG, Word Document, MP3 file) can be determined by the file's extension and by a header that precedes the data in the file. If a file's extension has been changed, then the only way to determine its type is by looking at its header.

Encase has a list of known file extensions and headers that it uses to identify files.

From the EnCase top "View" menu, select "File Types" to see the list of file types.

Question 9: What information is listed for each file type?

- The information that is listed for each file type are the Name, Extension, Category, Viewer, Header Signature, Header GREP, Header Case Sensitive, Footer Signature, Footer GREP, footer Case Sensitive, Unique Tag, Default Length, User Defined, and Disabled.

Question 10: What can an investigator do if the header of a file is valid but unknown in the current setting of the EnCase?

- The investigator can update the file signature table in Encase. Attempt to open the file in various applications, and maybe, use third party tools.

When EnCase finished the file signature analysis. Select the WinLabRaw image and take a look at the "Signature Analysis" and "Signature" Columns in the "Table" view.

Question 11: What different terms do you see in the Signature Analysis column? (Hint: See EnCase User Guide p. 271: Finding Data Using Signature Analysis). Include the definitions for each term.

- The terms that I see in the Signature Analysis column are Alias, Unknown, Bad signature, Bad signature. Alias means the header is in the File Signature table but the file extension is incorrect. Unknown means neither the header nor the file extension is in the File Signature table. Bad signature means the file's extension has a header signature listed in the File Signature table, but the file header found in the case does not match the File Signature table for that extension. Match indicates data in the file header, extension, and File Signature table all match.

Question 12: Do you find any signature mismatch? List all of them.

- Yes, I found two files with a signature mismatch. The files are file2.jp, and file1.doc.
-

Examine the WinLabRaw image in the gallery view again.

Question 13: Are there any graphics files on the WinLabRaw image whose file extensions have been changed? List them.

- yes there are graphics files on the WinLabRaw image whose file extensions have been changed. and they are file7.zip, file4, file5.csv, file3.xls, file6.
-

Question 14: If a file's extension has been changed to a non-graphics file type (such as changing jpg to txt), will it be displayed in the Gallery view before signature analysis?

- According to the user guide, the files in the gallery are shown using their extension by default in Encase. There if the file extension has been changed to a non-graphics file type it would not displaye in the Gallery view before signature analysis.
-

Hash Analysis

A hash is a digital fingerprint of a file or collection of data. EnCase uses the MD5 (and/or SHA1) algorithm to create a hash(s) or “digital fingerprint” of a file.

The Evidence Processor’s *Hash Analysis* that we ran earlier has created the MD5 and SHA-1 hash values for the Raw image.

Check the WinLabRaw image evidence in the table view, and make sure that the hash columns are filled. (Note: If the hashes are not shown, click on the Evidence tab, and use the green go-back arrow to the first Evidence page, then click on the Disk Image hyperlink. In this way, the Disk Image evidence view will be relished to include the evidence process result.)

Examining the hash columns of the Table View, you will notice that not all items have their hashes generated. From the description column, read the descriptions of the items that do not have hash values, and answer the following questions.

Question 15: What items (files/dirs) will not have hashes generated?

- The items that will not have hashes generated are the files or directories that has logical size of zero or falls into the unknown category.

Question 16: What are the three most common uses for hash analysis?

- The most common uses of hash analysis in EnCase are to identify when a chunk of data changes, to verify that data has not changed, and to compare a hash value against a library of known good and bad hashes.

Compound Files

Compound files are files with multiple layers and/or metadata such as Outlook Express email folders (.dbx), registry files, or OLE files.

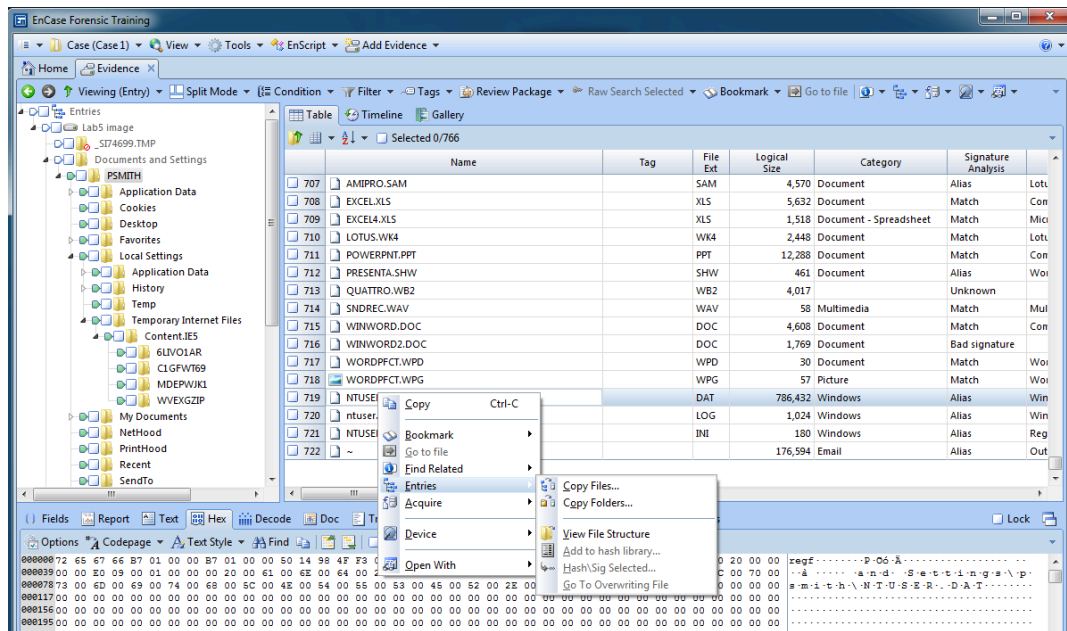
In EnCase, you have several ways to expand the compound files. You can run the EnCase Evidence Processor on the EnCase image, select **Expand compound files** to expand all registry files OR you can expand the individual compound file.

Here we will try the second method by only expanding the individual compound file. Let’s look at the NTUSER.DAT registry file from the **WinLabEncase** image.

View -> Evidence and click on WinLabEncase image,

In the Table view locate the file “Documents and Settings\PSMITH\NTUSER.DAT” and expand the EnCase image to find the “Documents and Settings\PSMITH\NTUSER.DAT” file **by**

right-click the file and choose **Entries -> View File Structures**. (Note: other registry files exist in C:\windows\system32\config folder. They are not included in this image.)



Double-click on ntuser.dat blue link.

Question 17: What kind of important information do you get?

- The type of important information that you would get are User profile information, recently accessed documents, application usage data, start menu customization, network settings and mapped drives, and typed URLs.

Now let's try *Searching for Email, Thumbnail Creation* and *Find Internet artifacts* from the WinLabEnCase image using the EnCase Evidence processor.

ONLY check "Find Email", "Thumbnail Creation", and "Find Internet artifacts." (In a real scenario, you will check all. Since we have tried the top functions earlier in the WinLabRaw image, we will skip these to save time.)

Double-click on "Find Email" and check the **Search for Additional Lost or Deleted Items** box for a search for deleted e-mails.

Double-click the **Find Internet artifacts** hyperlink and choose "Search unallocated space for Internet artifacts".

Click OK to run the processor.

You can see the process status in Processor Manager (View -> Processor Manager, or via EnCase Home page).

After the processes are done, let's check the results.

Searching for Email

EnCase can search various types of email artifacts including Outlook (2000/2003), Outlook Express, Exchange, Lotus Notes, AOL, Thunderbird's MBOX, etc.
The processed e-mail will be found under View -> Artifacts.

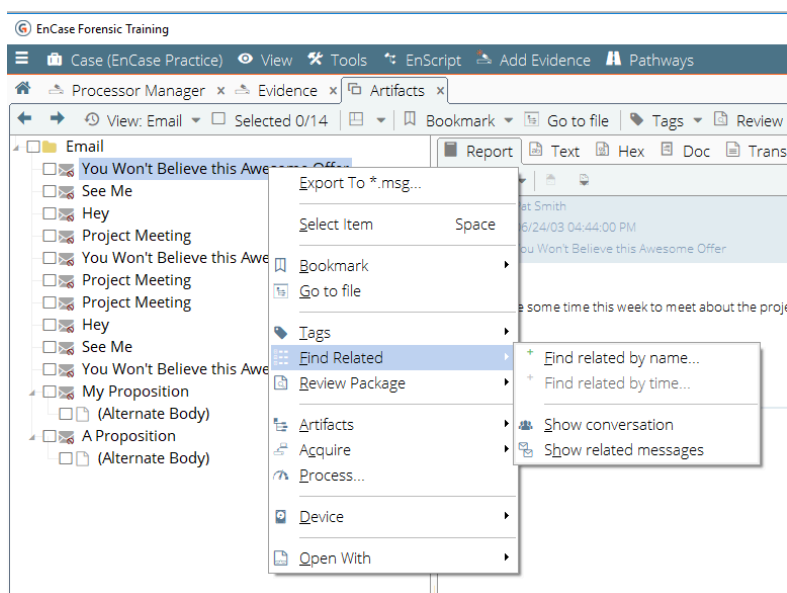
A list of processed e-mail archives will be displayed under the Email Folder. To open an e-mail archive, click on the hyperlink of the name of the archive

Question 18: What interesting information do you see from emails?

- From reading some of the emails, I see that an employee of a company is trying to get a job in another company by giving some materials from his current company. Second, it looks like he had, maybe a burst of anger in one of the staff meetings. The employee is definitely on to something not good.

EnCase also supports two forms of e-mail threading analysis, **Conversations** and **Related messages**.

Double-click on *Deleted Items.dbx*. Right-click the first message "You Won't Believe this Awesome Offer", and choose **Find Related -> Show related messages**.



Question 19: Read the EnCase User Guide on p. 243, and briefly describe what are the *Show conversation* and *Show related messages* features.

- The "Show Conversation" feature is used for email threading, which is based on information related to email conversation threads found in the email message headers. EnCase makes use of email header metadata, such as Message-ID and in-reply-to headers, to rebuild email conversation threads. This reconstruction process is carried out during processing, which means that conversations are not available on data that has not been processed. To display an email conversation, you need to select an email or email store in the Evidence tab and choose "Show Conversation" from the Find Related menu.
 - The "Show Related Messages" feature displays all email messages that have the same subject lines and groups them together. This feature can be more helpful than sorting through conversation threads. To use this feature, select an email or email store in the Evidence tab, and choose "Show Related Messages" from the Find Related menu. However, since this feature only searches the subject line of a message, the displayed emails may not always be related, depending on the uniqueness of the subject line.
-

Question 20: View -> Artifacts, you should also see Thumbnails under WinLabEncase Image. Click on Thumbnails and explain what these thumbnails are.

- These thumbnails are all the files that have been identified as pictures or images. This view allows you to quickly scan through visual data within the evidence, making it easier to identify and analyze images without having to open each one individually.
-

Searching for Internet Artifacts

Internet history contains rich evidence. EnCase will collect Internet-related artifacts, such as browser histories and cached web pages. You also have the option to search unallocated space for Internet artifacts.

The processed Internet artifacts will be found under View -> Artifacts. Select the Internet folder and then click on the Internet hyperlink.

Question 21: What kind of information do you see in the Internet artifact?

- In the internet artifact, you can see the user's interaction with a web browser such as Internet Explorer, or just internet behavior in general. Some of the things you can see are History, Typed URLs, Visited Links, Daily internet activity, Cache, Code, Cookies, Bookmarks, etc.

Question 22: In general, how does “search unallocated space for internet artifacts” affect your search results on the Internet? (In our simple case, you may not find any differences.)

- EnCase allows you to search for internet artifacts in unallocated space on your hard drive. This means that the software scans for any remnants of internet activity that may not be part of the current file system structure. These remnants could include web pages, images, or any other data that was previously saved to the drive.
 - Searching unallocated space during an internet artifact search can potentially provide a more comprehensive set of results. This is because it may contain previously deleted or inaccessible data. However, in cases where the internet browser's data is largely intact and has not been deleted, searching the unallocated space may not yield any additional results.
-

Searching in EnCase

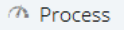
There are three principal methods of searching through evidence in EnCase:

- **Index searches** – Evidence data is indexed before searching
- **Keyword searches through raw data** – Searches based on non-indexed, raw data
- **Tag searches** – Searches based on tags

Generating an index can take time, however, the trade-off in time spent creating the index yields a greater payoff with near instantaneous search times.

Using EnCase indexing search

Text indexing allows you to quickly query the transcript of entries. Creating an index builds a list of words from the contents of an evidence file that contain pointers to their occurrence in the file. Two steps are involved in using the index: Generating an index and Searching an Index.

Under the Evidence tab of the WinLabRaw image, click on “Process” . Only check “Index Text And MetaData” and only set **index slack and Unallocated**, then click OK to run the processor.

To search an index, open View -> Indexed Items.

Enter the term “this” in the text box to instantly show all variations of the occurrence of that term. This is displayed in the indexed data in the table below the search query box.

Click a hyperlinked term to show all occurrences of that term in the right Table pane.

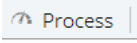
You can read the file by right-clicking on the tile and choosing **Go to file**, then view the content at the low pane by choosing text, Doc, Transcript, or Picture depending on the file type.

Question 23: What are the results? List 2 files that contain the term “this” in their contents.

- The results are 630 hits of the word “this” in 132 files. Two files that contain the term “this” in their contents are “bookmarks.html” and “You won’t Believe this Awesome Offer” email file.

Raw Keyword Searches

This option runs a raw keyword search during the processing. You can either use Evidence Process **Search for Keywords** before analysis or the Raw Keyword search function outside the Evidence Processor during analysis.

Go back to the Evidence tab of WinLabRaw image, and click on “Process” . Click on the hyperlink “Search for keywords” to add keywords.

Use “New” to add a single keyword and “Add Keyword List” to add multiple keywords at once. We will add the following keywords:

microsoft
computer
this

Click on “**Add Keyword List**” and add these keywords, then click OK.

Choose the option of “Search entry slack” at the bottom left checkboxes. Click “OK”.

At the processor window, click OK. Search starts.

Question 24: What are the other search options besides “Search entry slack”? (p. 266)

- The other search options besides “Search entry slack” are Undelete entries before searching, Use initialized size, and Search only slack are of known items in Hash Library or skip contents for known files.

When the search is done, to view the search results, let’s open the View -> **Keyword Hits** tab.

To see the result of any keyword, simply click on its hit number.

Question 25: How many hits do you get for Microsoft, computer, and this respectively?

- For Microsoft, there are 4 hits. For computers, there are 0 hits, and for this, there are 16 hits.

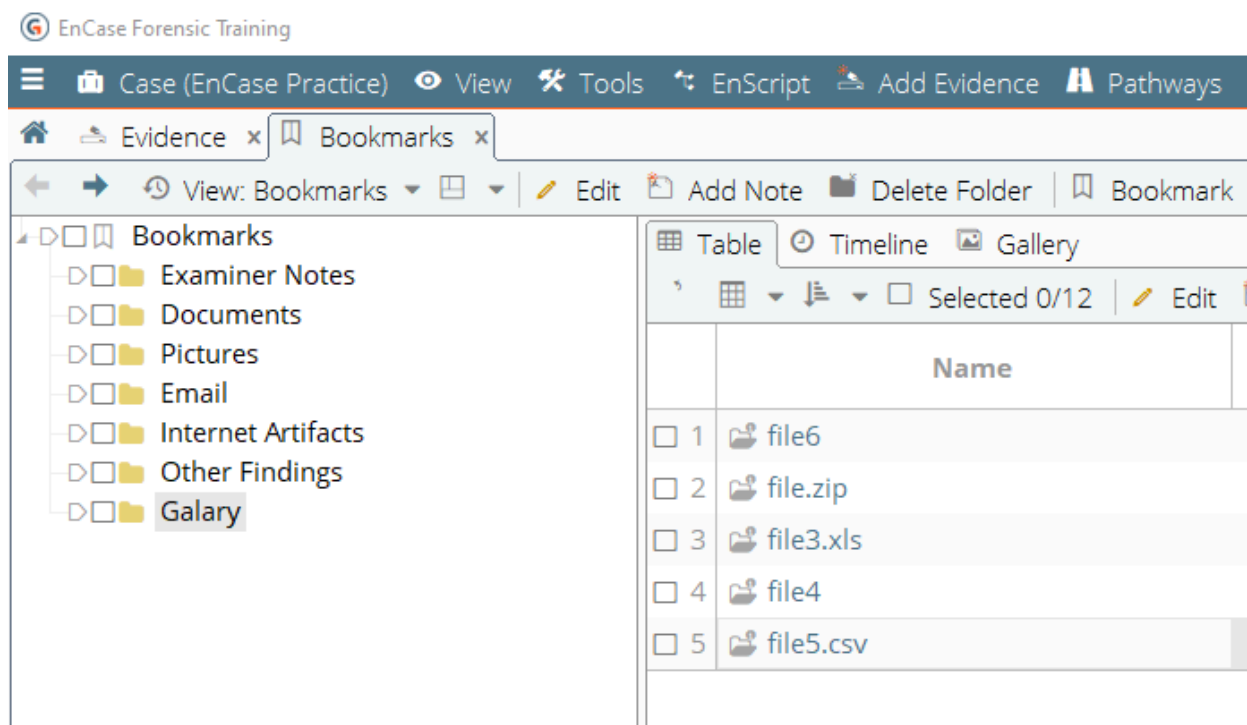
Bookmarks and Tags

Bookmarks allow you to mark folders, files, search results, or parts of a file for later reference and for inclusion in reports.

Bookmarking in Evidence View

Go to the WinLabRaw image Evidence tab, green-select Disk Image, and click on “Gallery”. Blue-check the additional images that you identified after “Signature Analysis”. Right-click and select the **Bookmark** drop-down menu to create bookmarks for the selected entry (or entries) by selecting Single item... Or Selected items... (for multiple entries). Place the evidence bookmarks in the appropriate folder of your case report template or you can create a new folder. To view the bookmarking you created: “view” -> Bookmarks

Action 26: Include a screenshot of the bookmarks you created in the Bookmarks tab.



Tags

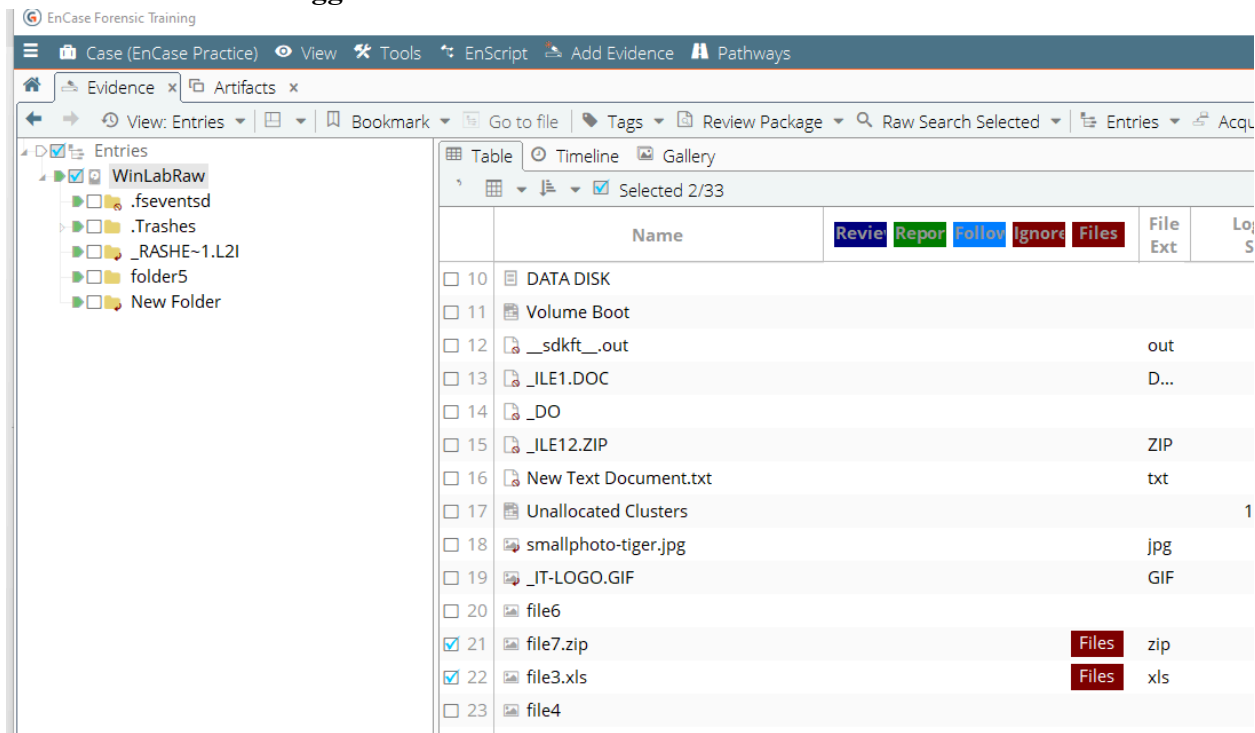
The EnCase tagging feature allows you to mark evidence items from Records, Evidence, or Bookmarks for review. You can use the default tags created by EnCase or define your own tags. Tags tab can be found from the Records, Evidence, or Bookmark tabs,


Let's create a tag and then tag the two files from your keyword search exercise using this tag.

Click “Tags” -> Manage tags...., then create a tag named **Suspicious Files**, displayed as “**Files**” in red (right-click the Background Color and choose edit).

Select and blue-check any two files, then use “Tags -> Tag selected items...” to tag them using the “Files” tag. Go back to the evidence tab, the tag should be shown in the Table view of the “Tag” column.

Action 27: Show the tagged Files in the Table view.



Finally, we will try additional functions in the EnCase Evidence Processor. Let's go back to WinlabEnCase image Evidence. click on “Process”  Process.

Action 28: Expend Modules, and choose one function from Modules. Explain this function and show your results below.

- In the Modules, I chose the Windows Artifact Parser. The Windows Artifact Parser is a single module that searches for common Windows OS artifacts with potential forensic value. These include Link files, Recycle Bin artifacts, and MFT transaction logs.

EnCase Forensic Training

Case (EnCase Practice) View Tools EnScript Add Evidence Pathways

Evidence x Artifacts x

View: Artifacts Bookmark Go to file Tags Review Package Artifacts

Artifacts

- file12
 - Windows Artifact Parser
 - Windows Artifact Parser
 - ShellBags Parser
 - ntuser.dat
 - Link Parser

Table Timeline Gallery

Selected 0/8

	Name	Re	Re	Fe	Ig	Fi	File Ext
<input type="checkbox"/> 1	file12						
<input type="checkbox"/> 2	Windows Artifact Parser						
<input type="checkbox"/> 3	Windows Artifact Parser						
<input type="checkbox"/> 4	ShellBags Parser						
<input type="checkbox"/> 5	ntuser.dat						dat
<input type="checkbox"/> 6	ShellBags						
<input type="checkbox"/> 7	Link Parser						
<input type="checkbox"/> 8	Link Files						

EnCase Forensic Training

Case (EnCase Practice) View Tools EnScript Add Evidence Pathways

Evidence x Artifacts x

View: Link records Bookmark Go to file

Link records

Table Timeline

Selected 0/27

	Name	File Offset	Base Path
<input type="checkbox"/> 1	Launch Internet Explorer Browser.Ink	0	C:\Program Files\Internet Explorer\iexplore.exe
<input type="checkbox"/> 2	Sample Music.Ink	0	C:\Documents and Settings\All Users\Documents\My Music\Sar
<input type="checkbox"/> 3	Sample Pictures.Ink	0	C:\Documents and Settings\All Users\Documents\My Pictures\S
<input type="checkbox"/> 4	cleanup.log.Ink	0	C:\Documents and Settings\psmith\Local Settings\Application D
<input type="checkbox"/> 5	Confidential.Ink	0	C:\Documents and Settings\psmith\My Documents\Confidentia
<input type="checkbox"/> 6	diagram.gif.Ink	0	C:\Documents and Settings\psmith\My Documents\Confidentia
<input type="checkbox"/> 7	Outlook Express.Ink	0	C:\Documents and Settings\psmith\Local Settings\Application D
<input type="checkbox"/> 8	Project 238x.rtf.Ink	0	C:\Documents and Settings\psmith\My Documents\Confidentia
<input type="checkbox"/> 9	Project 47x.doc.Ink	0	C:\Documents and Settings\psmith\My Documents\Confidentia
<input type="checkbox"/> 10	test.eml.Ink	0	C:\Documents and Settings\psmith\Desktop\test.eml
<input type="checkbox"/> 11	You Won't Believe this Awesome Offer.eml.Ink	0	C:\Documents and Settings\psmith\Desktop\You Won't Believe
<input type="checkbox"/> 12	Magnifier.Ink	0	C:\WINDOWS\system32\magnify.exe
<input type="checkbox"/> 13	Narrator.Ink	0	C:\WINDOWS\system32\narrator.exe
<input type="checkbox"/> 14	On-Screen Keyboard.Ink	0	C:\WINDOWS\system32\osk.exe
<input type="checkbox"/> 15	Utility Manager.Ink	0	C:\WINDOWS\system32\utilman.exe
<input type="checkbox"/> 16	Windows Media Player.Ink	0	C:\Program Files\Windows Media Player\wmplayer.exe