

# Windows EnCase Forensics

## Overview:

Practice the basic functions supported by *EnCase Forensics*

---

### Exercise 1: Starting a New Case

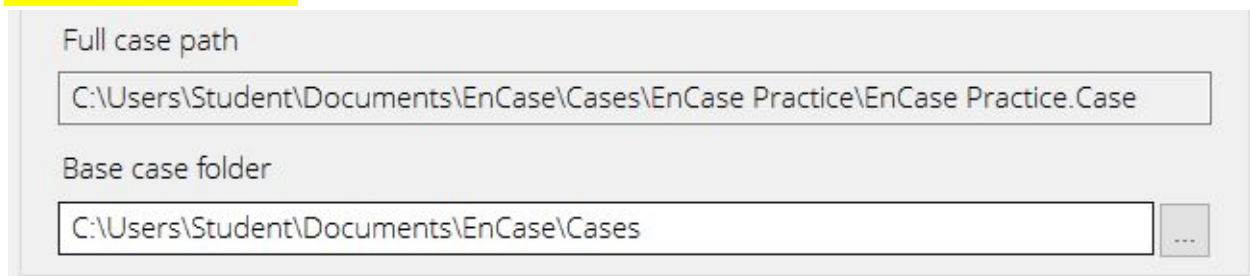
Launch EnCase 8 – make sure that you are in the **EnCase forensics** mode (on the top-left corner of the software, you should see *EnCase Forensic Training*, NOT acquisition mode.)

In the main Home page of EnCase, click the “New Case” button under CASE FILE to begin a new case. A new Options window will pop-up. Use the *#1 Basic Template* and name the case “EnCase Practice”.

At the bottom left hand corner, under *Case Information*, you may fill in “Case Number”, “Examiner Name” and a “Description” information by clicking on the name. 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.

#### Encase folder defaults:



The screenshot shows the 'Options' window in EnCase. It has two sections: 'Full case path' and 'Base case folder'. The 'Full case path' text box contains the path 'C:\Users\Student\Documents\EnCase\Cases\EnCase Practice\EnCase Practice.Case'. The 'Base case folder' text box contains the path 'C:\Users\Student\Documents\EnCase\Cases' and has a small button with three dots to its right.

Click “OK” at the bottom of the *Options* window. 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 previous page, in this case, the main Home page. In 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, click on the blue go-forward arrow to go back to your Case Home page.

## Add a Raw Image to the exist case

Under EVIDENCE, you click **Add Evidence**. The third Home page, *Add Evidence*, is open to allow you to add the given images to the case you just created.

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 Desktop\images folder, 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”, 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.

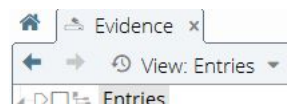


Figure 1. Green Arrow to go back

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 by clicking on the Evidence tab 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 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), or 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?**

**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.

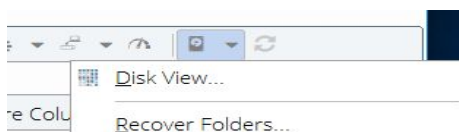


Figure 3. Disk View...



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 “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 the 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.

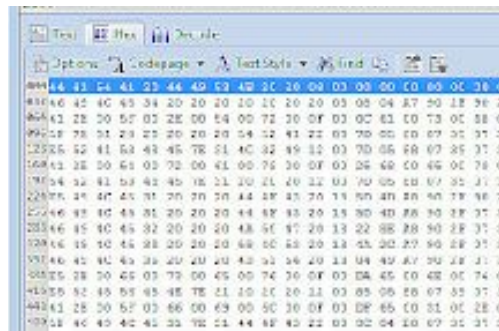


Figure 5. Resize the hex view to be 32 bytes per-row

(**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: Examine 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?**

**D**

---

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 exist 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”**

legacy evidence files(E01)

current evidence files(Ex01)

safeback files(001)

vmware files(vmdk)

legacy logical evidence files(L01)

current logical evidence file(Lx01)

virtual pc file(vhd)

---

Now you have two evidences 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).**

**HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\TimeZoneInformation**

---

Before starting the evidence analysis, you should verify that 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”.

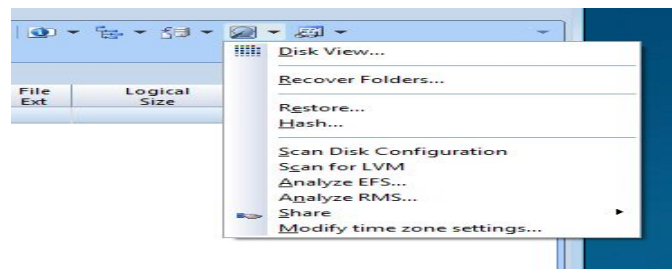


Figure 6. Verify or modify time zone settings

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

**disk icon → modify time zone settings → edit time properties information in the window**

---

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 *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 “Options” button from the top menu.

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

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. This visual aide may increase the likelihood of successfully identifying patterns.

---

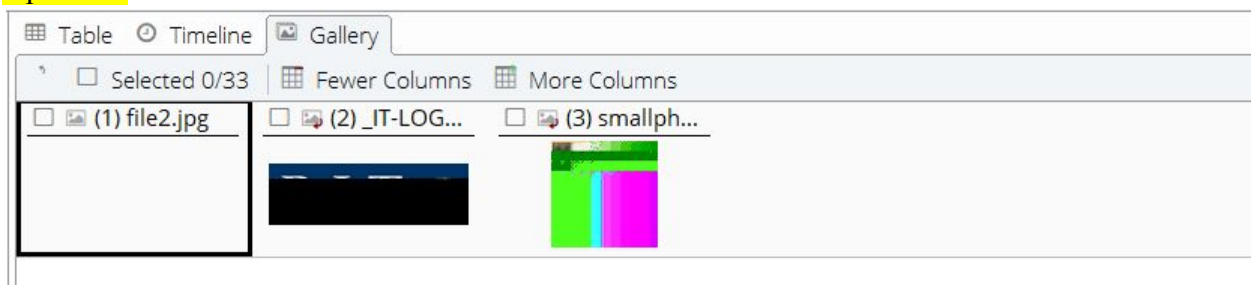
#### Gallery View

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 file signature analysis is done.

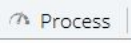
#### Question 7: In the WinLabRaw image, how many pictures are shown in Gallery View before performing file signature analysis?

3 pictures



#### 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.

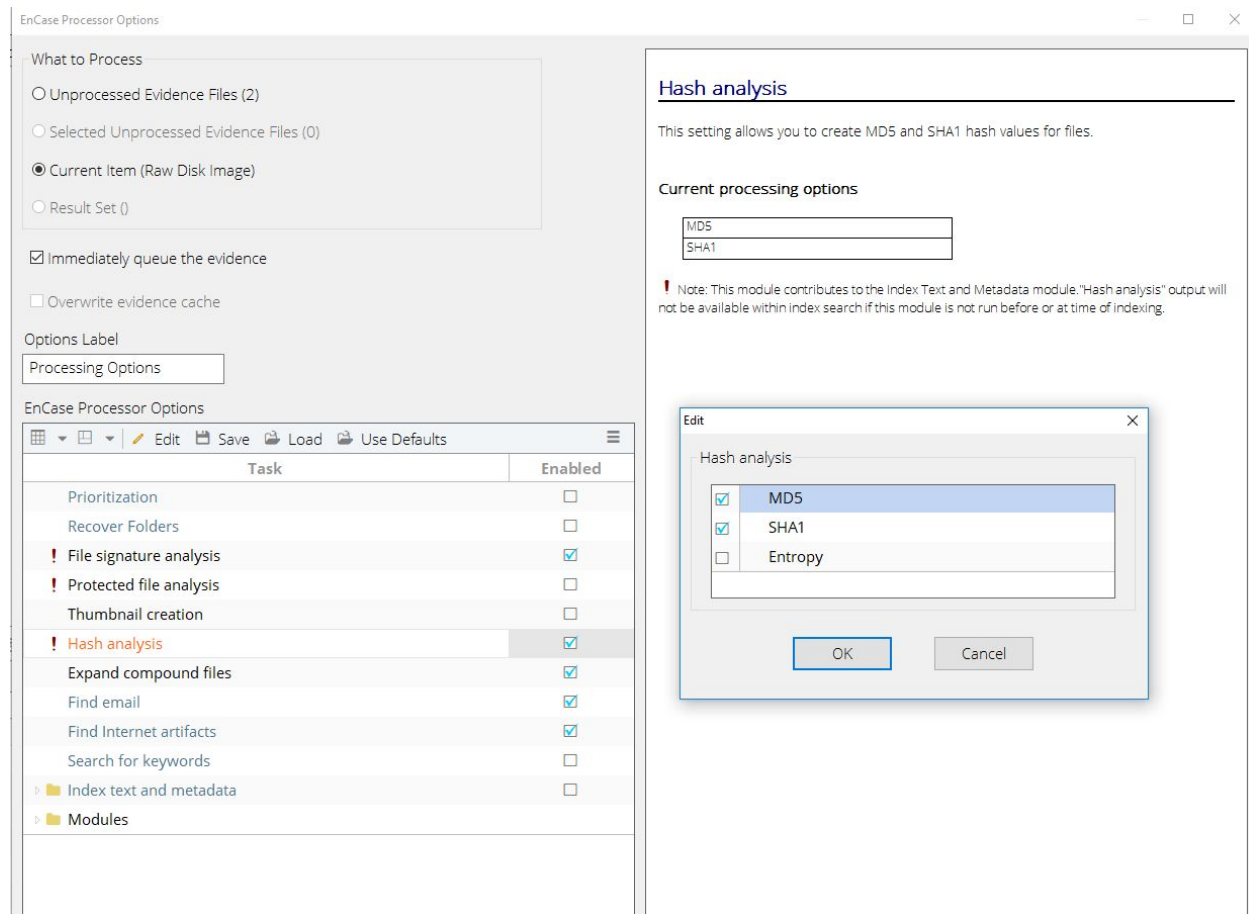


Figure 7. Evidence Process Task List

### **Recover folders.**

Recover Folders will recover all deleted folders.

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

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

FAT ⇒ searches through the unallocated clusters of a specific FAT partition for the . or .. signature of a deleted file.

NTFS ⇒ parses through the current MFT artifacts for files without parent folders. Recovered files are placed in recovered folder in root of NTFS.

## 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?

Name, extensions, category, viewer, header signature, header GREP, header case sensitive, footer signature, footer GREP, footer case sensitive, unique tag default length, user defined, disabled.

---

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

edit the filetypes.ini file with updated header and extension info

---

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 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.

**Match**⇒ indicates data in the file header, extension, and File Signature table all match.

**Alias**⇒ the header is in the File Signature table but the file extension is incorrect (for example, a JPG file with a .ttf extension). This indicates a file with a renamed extension.

**Unknown** ⇒ neither the header nor the file extension is in the File Signature table.

**Bad Signature** ⇒ 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

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

file2.jpg

\_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.

file4, file3.xls, file5.csv, file6, file7.zip

---



**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?**

**no**

---

## 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 hash(s) or “digital fingerprint” of a file.

The Evidence Processor’s *Hash Analysis* that we have run 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 Disk Image hyperlink. In this way, the Disk Image evidence view will be refreshed 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?

1-6, 9, 15-16, 19, 21-23, 25-28

fseventsd, .trashes, \_RASHE~1.L2I, folder5, New Folder, DATA DISK, \_ILE1.DOC, \_IT-LOGO.GIF, smallphoto-tiger.jpg, New Text Document.txt, \_ILE12.zip, \_DO, \_\_sdkft\_\_.out, volume boot, Primary FAT, Secondary FAT, unallocated clusters

---

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

integrity checks to verify that data has not been altered, verification of the correct operation of tools and procedures, signature analysis

---

## Compound Files

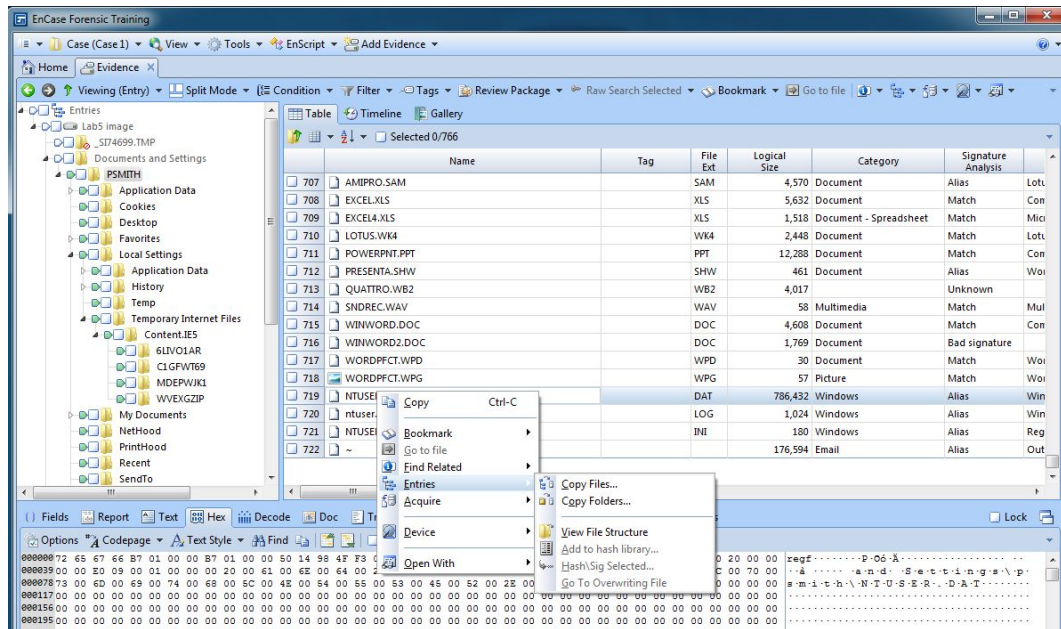
Compound files are files with multiple layers and/or metadata such as Outlook Express email folders (.dbx), registry files, or OLE files.

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 archives and 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 **WinLabEncase** image.

**View -> Evidence** and click on WinLabEncase image,

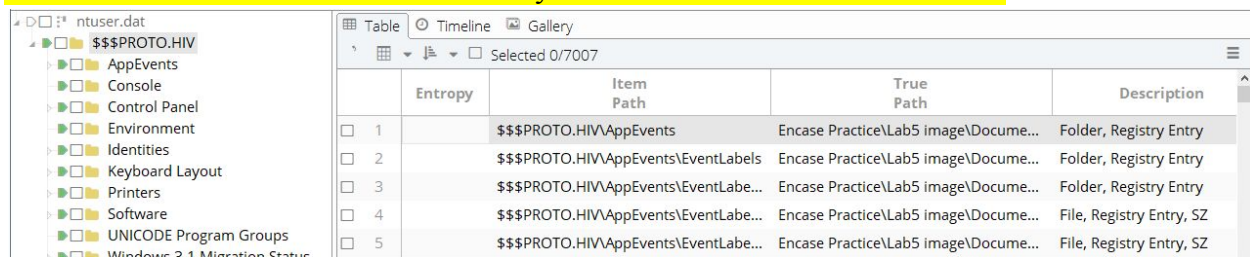
In the Table view locate the file “Documents and Settings\PSMITH\NTUSER.DAT” and expand the EnCase image to find the “Documents and Settings\PSMITH\NTUSER.DAT” file **by right click the file and choose Entries -> View File Structures**. (Note: other registry files exist in C:\windows\system32\config 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?**

**KEYS! This information can show the keys that were last modified and when.**



Example:

Name	AppEvents
Logical Size	9
Category	Folder
Last Written	01/23/04 11:57:38 AM
MDS	bd3a734ab6b8bed87a2f133ef6c7cdb0
Item Path	\$\$\$PROTO.HIVAppEvents

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

microsoft 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 WinLabRaw image, we will skip these one to save time.)

Double click on “Find Email” and check **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 Manger (View -> Processor Manager, or via EnCase Home page).

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

### **Searching for Email**

EnCase can search various types of email artifacts including Outlook (2000/2003), Outlook Express, Exchange, Lotus Notes, AOL and Thunderbird’s MBOX, etc.  
The processed e-mail will be found under the 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?**

There are two emails from Pat Smith to bconrad@raytheon.com  
The first is an initial proposal email. The second is a follow up.

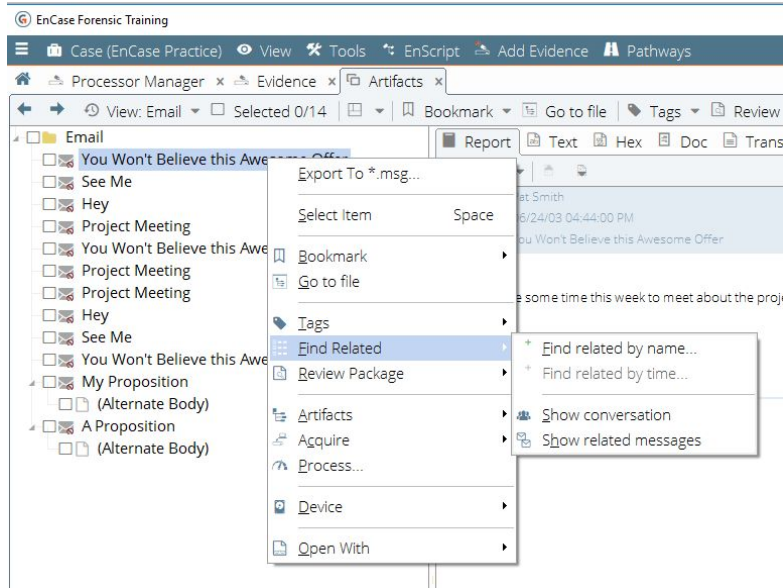
Proposal: “I’d like to offer you some material from my company in exchange for a position in your company”

Follow Up: “It’s been a week since I sent you my proposal. Have you had a chance to consider it” ?

---

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”, choose **Find related -> Show related messages**.



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

**Show Conversation** ⇒ After processing, EnCase uses email header metadata (including message ID and in-reply-to headers) to reconstruct email conversation threads. Without this, Encase cannot construct a conversation thread.

**Show Related Messages** ⇒ All email messages with identical subject lines.

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

Thumbnails are small sized copies of the original image.

The thumbnails are:

diagram images from pat smith's documents directory(some placed confidential folder)

unrelated temp internet/IE5 files(mostly gifs)

\$\$\$PROTO.HIV policies/MRUlists/schemes/extensions

SPL files

IE cache files(mostly gifs)

## Searching for Internet Artifacts

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

mozilla bookmarks:

<http://www.aerospace-technology.com/contractors/indexAtoZ.html>

<http://www.jsfirm.com/searchcontractors.asp>

internet explorer url's

[jobs.yahoo.com](http://jobs.yahoo.com), [monster.com](http://monster.com), [boeing.com](http://boeing.com), [raytheon.com](http://raytheon.com)

visited links

[psmith@file:///C:/Documents%20and%20Settings/psmith/My%20Documents/Confidential/diagram.gif](file:///C:/Documents%20and%20Settings/psmith/My%20Documents/Confidential/diagram.gif)

[psmith@file:///C:/Documents%20and%20Settings/psmith/My%20Documents/Confidential/Project%2047x.doc](file:///C:/Documents%20and%20Settings/psmith/My%20Documents/Confidential/Project%2047x.doc)

Daily

[psmith@file:///C:/Documents%20and%20Settings/psmith/My%20Documents/Confidential/Project%20238x.rtf](file:///C:/Documents%20and%20Settings/psmith/My%20Documents/Confidential/Project%20238x.rtf)

---

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

I did not find any differences

---

## Searching in EnCase


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

- **Index searches** – Evidence data is indexed prior to 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 WinLabRaw image, click on “Process”  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 a term “this” in the text box to instantly show all variations of the occurrence of that term. This displays 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-click on the tile and choose **Go to file**, then view the content at the low pane by choose 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.**

secret.txt ⇒ “this is a secret” [in text]

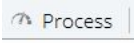
file1.doc ⇒ “this is some text” [in text]

file2.jpg ⇒ “this is some information” [in transcript]

---

## 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 Evidence tab of WinLabRaw image, click on “Process” . Click on the hyperlink of “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.

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

skip contents for known files

undelete entries before searching

use initialized size

---

When the search is done, to view the search results, let’s open 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?**

microsoft ⇒ 4  
computer ⇒ 0  
this ⇒ 16

---

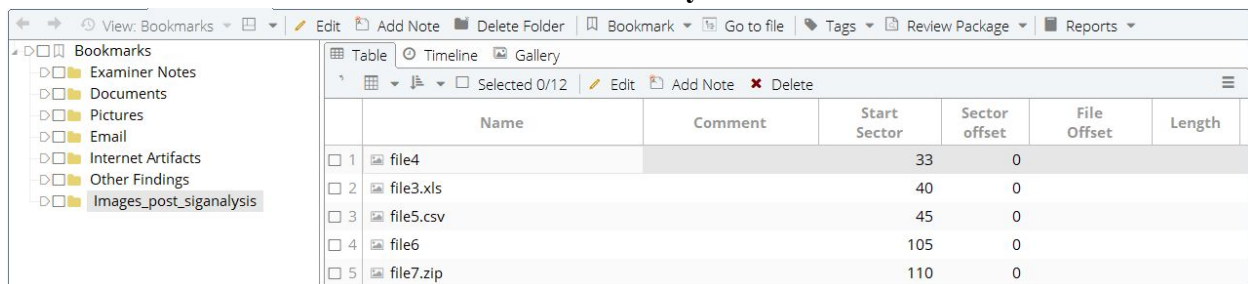
## Bookmarks and Tags

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 the “Gallery”. Blue-check the additional images that you identified after “Signature Analysis”. Right click and select **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.



The screenshot shows the EnCase interface with the 'Bookmarks' tab selected. On the left, a tree view shows folders like 'Examiner Notes', 'Documents', 'Pictures', 'Email', 'Internet Artifacts', 'Other Findings', and 'Images\_post\_siganalysis'. The main area displays a table of bookmarked items.

	Name	Comment	Start Sector	Sector offset	File Offset	Length
<input type="checkbox"/> 1	file4		33	0		
<input type="checkbox"/> 2	file3.xls		40	0		
<input type="checkbox"/> 3	file5.csv		45	0		
<input type="checkbox"/> 4	file6		105	0		
<input type="checkbox"/> 5	file7.zip		110	0		

## 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 color (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 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.



Internet Explorer (Windows)

History

Typed URL

Visited Link

Daily

Cache

Code

Image

HTML

Unknown Type

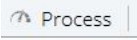
Table

Timeline

Gallery

Selected 0/530

	Name	Re	Re	Re	Re	File Ext	Logical Size	Item Type	Category
1	index.dat					dat	256	Document	Internet
2	index.dat					dat	256	Document	Internet
3	index.dat					dat	256	Document	Internet
4	index.dat					dat	256	Document	Internet

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

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

data carving

selected default file types to carve:

archive / document / email / picture

search: unallocated and file slack

Export to → carved files export folder

