CSEC 730 - Advanced Computer Forensics

Shriram Karpoora Sundara Pandian (KP)

Lab 3 - Encase Lab

PART I: Familiar with EnCase

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

Fields | Report | Text | Hex | Doc | Transcript | Picture | Console

100%

Name	.fseventsd
File Ext	fseventsd
Logical Size	0
Category	Folder
Last Accessed	08/07/08
File Created	08/07/08 05:00:11 PM
Last Written	08/07/08 05:00:10 PM
Item Path	Disk Image\.fseventsd
True Path	EnCase Practice\Disk Image\.fseventsd
Description	Folder, Deleted, Hidden
Is Deleted	•
Initialized Size	0

Volume

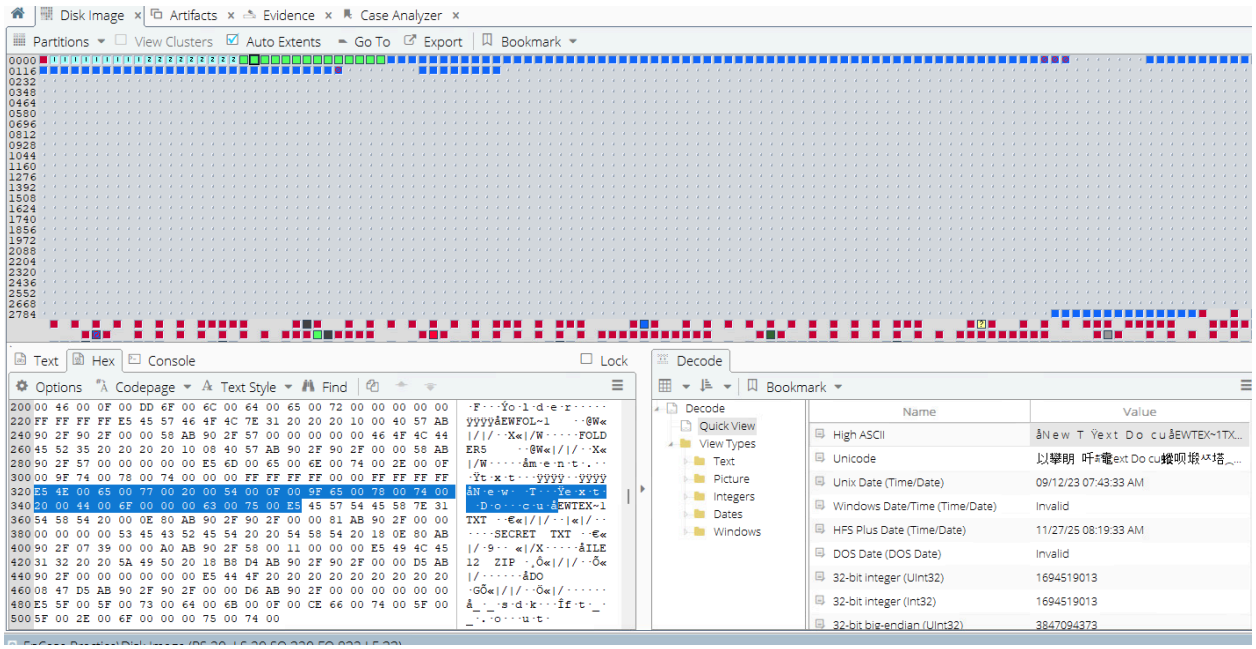
File System	FAT12
Sectors per cluster	1
Bytes per sector	512
Total Sectors	2,880
Total Capacity	1,457,664 Bytes (1.4 MB)
Total Clusters	2,847
Unallocated	1,399,808 Bytes (1.3 MB)
Free Clusters	2,734
Allocated	57,856 Bytes (56.5 KB)
Volume Name	DATA DISK
Volume Offset	0
Drive Type	Fixed

Device

Name	Disk Image
File Path	C:\Users\Student\Desktop\images\WinLabRaw.img
Drive Type	Fixed
Interface	None
GUID	85a26a5af3be93c34b1a27b9ed75b1f1

Based on the above information, the file system type is FAT12.

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?

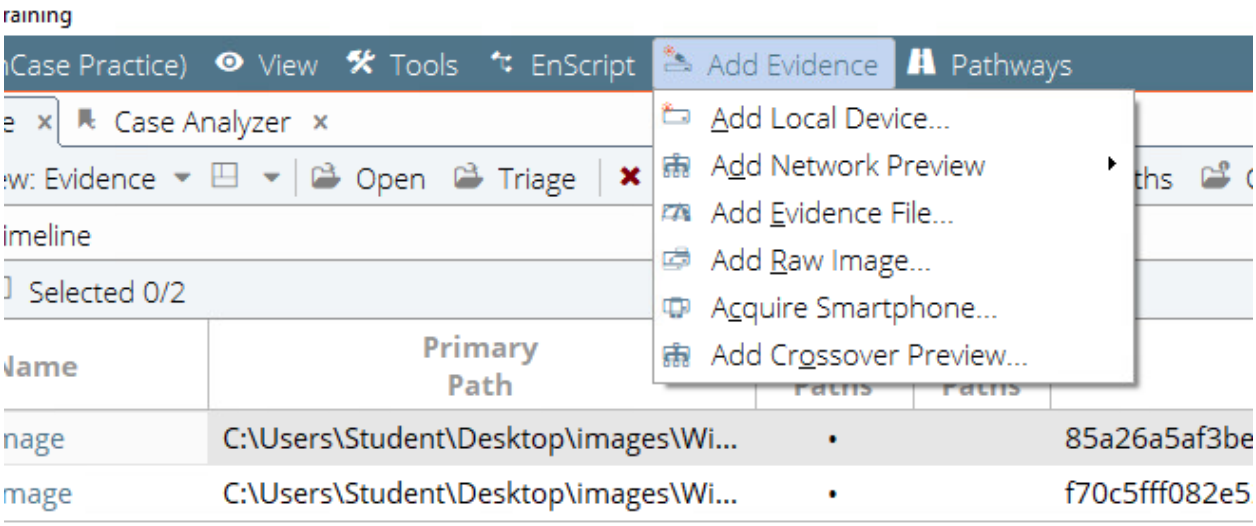


The deleted files' starting character in hex is E5.

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

These are types of files can be added,

- Local Device
- Network Preview
- Evidence File
- Raw Image
- Acquire Smartphone
- Crossover Preview


raining
Case Practice)
View
Tools
EnScript
Add Evidence
Pathways
Case Analyzer
Add Local Device...
Add Network Preview
Add Evidence File...
Add Raw Image...
Acquire Smartphone...
Add Crossover Preview...
w: Evidence
Open
Triage
ths
imeline
Selected 0/2
Name
Primary Path
nage
C:\Users\Student\Desktop\images\Wi...
85a26a5af3be
mage
C:\Users\Student\Desktop\images\Wi...
f70c5fff082e5

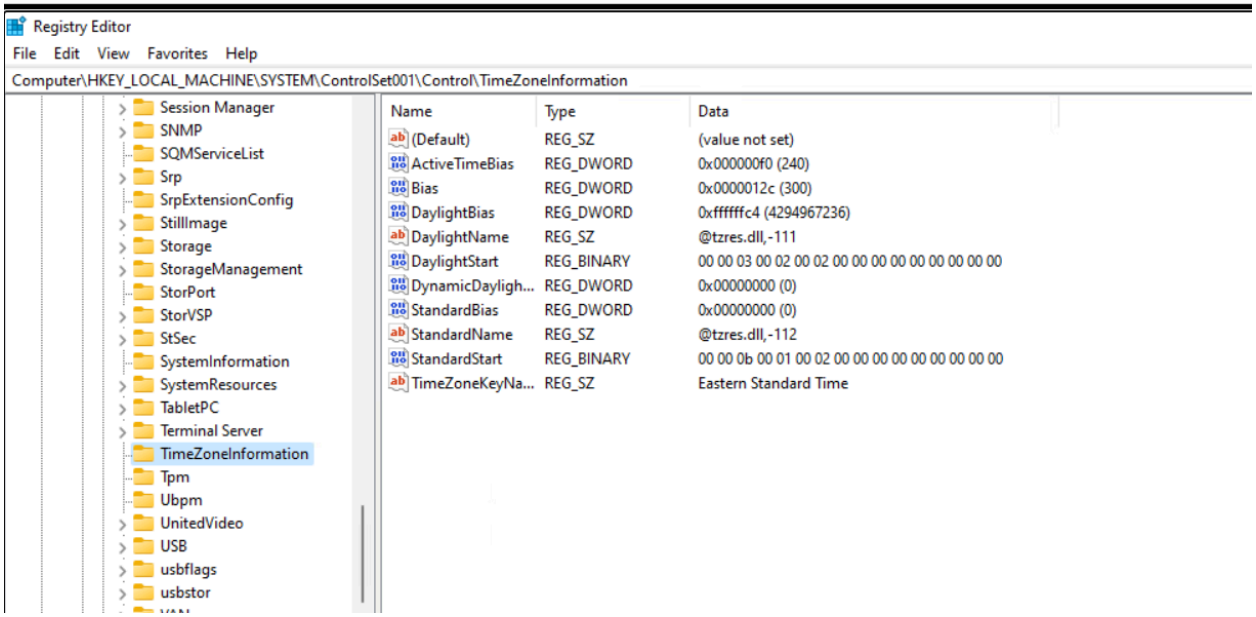
<u>Exercise 2</u>: Analyzing Evidence using Encase

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TimeZoneInformation
This registry holds the timezone information of the windows system.

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

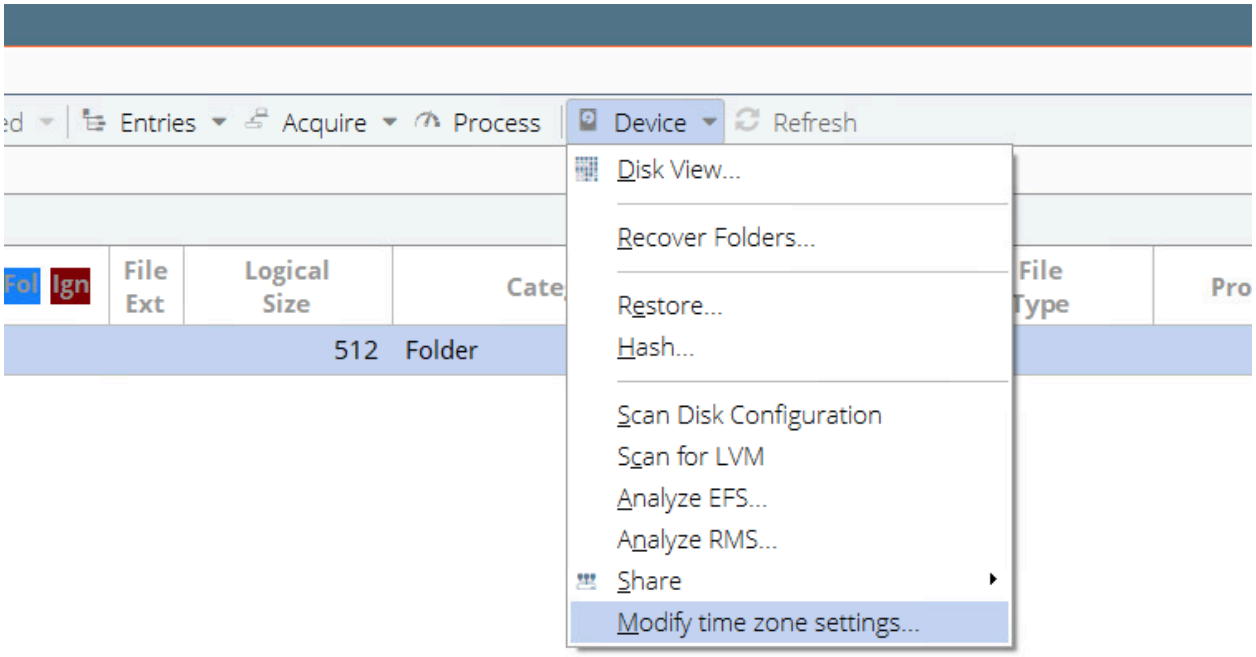
According to encase, the Time Zone information resides at this location.

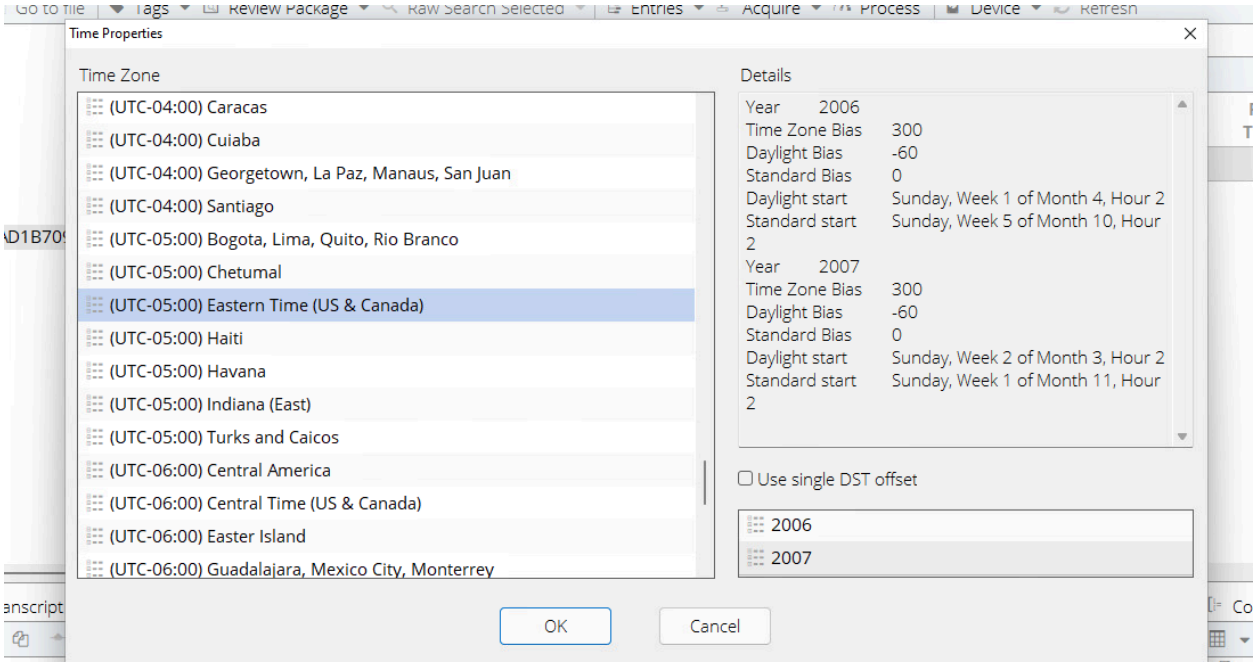
HKLM\System\ControlSet00X\Control\Time Zone Information.



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

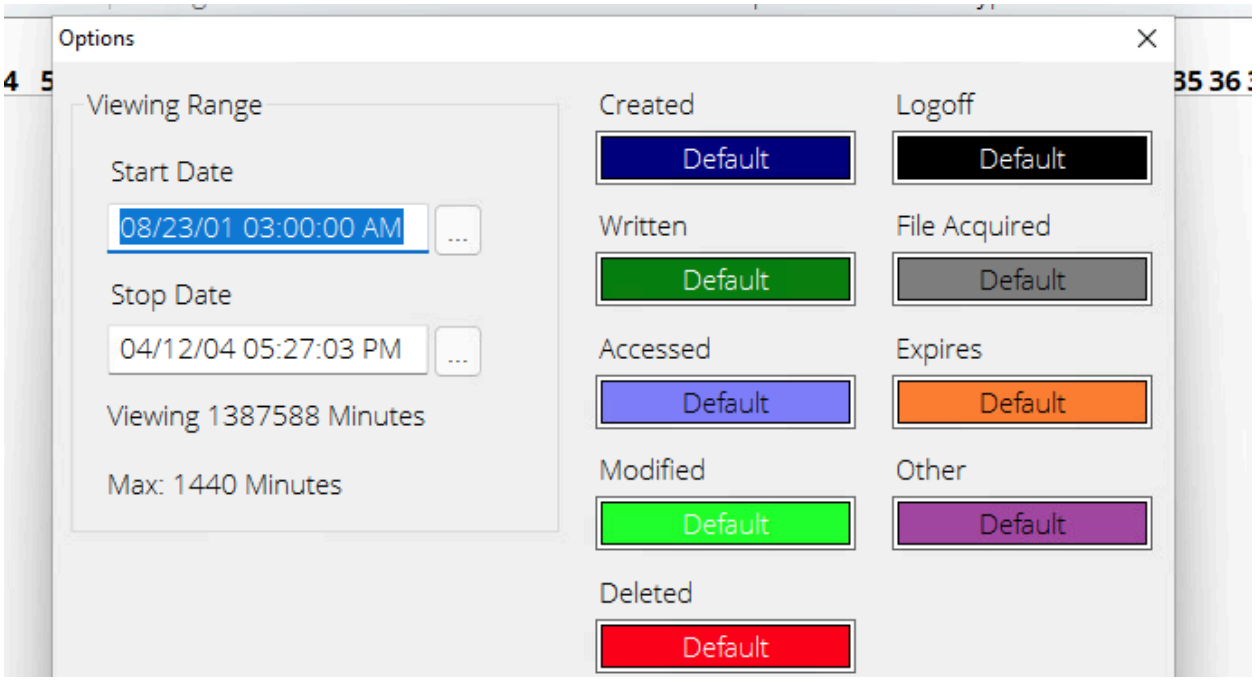
We can go to the Device>Modify time zone settings…

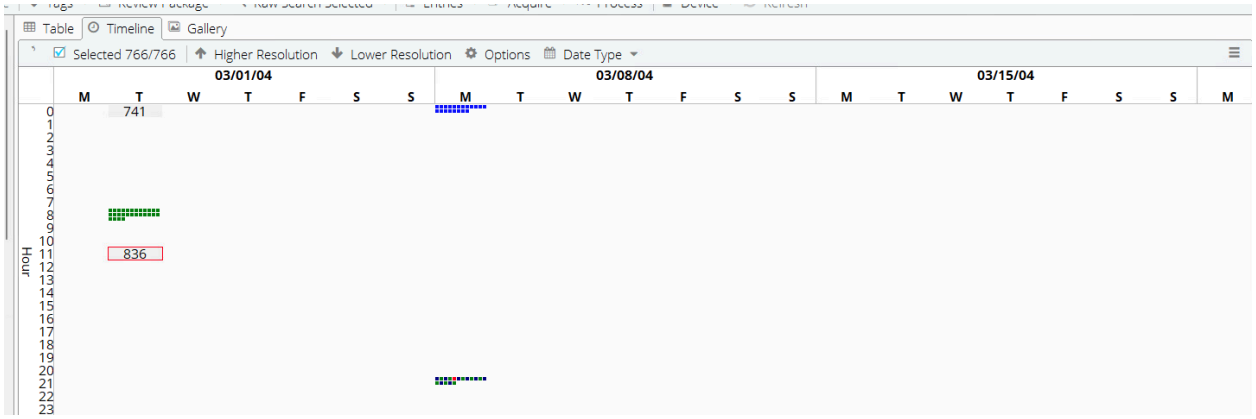


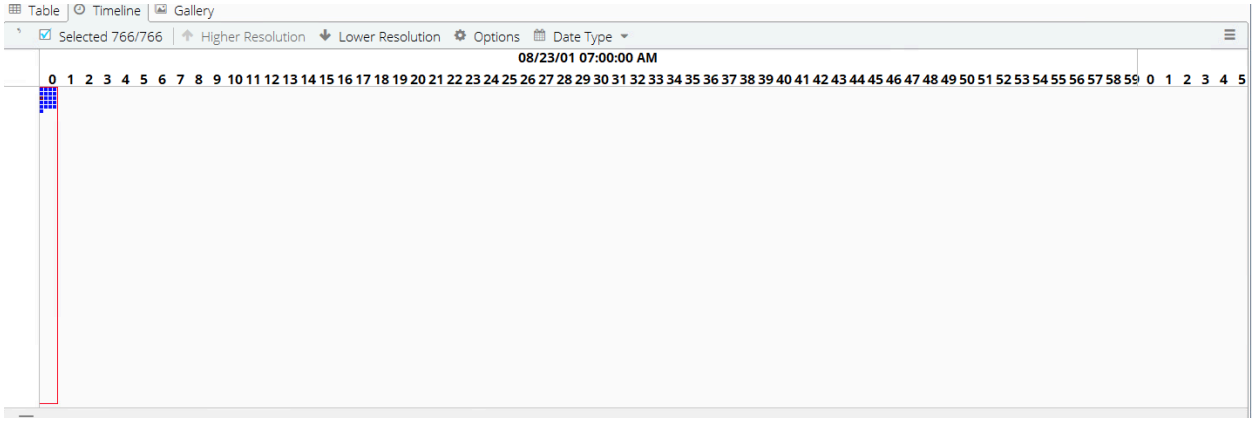


Question 6: Why is Timeline View useful for your investigation?

We can see different kinds of file easily like accessed, modified and created files. It gives a broad perspective to investigate effectively for finding the patterns and file previews easily rather than looking in the file menu.

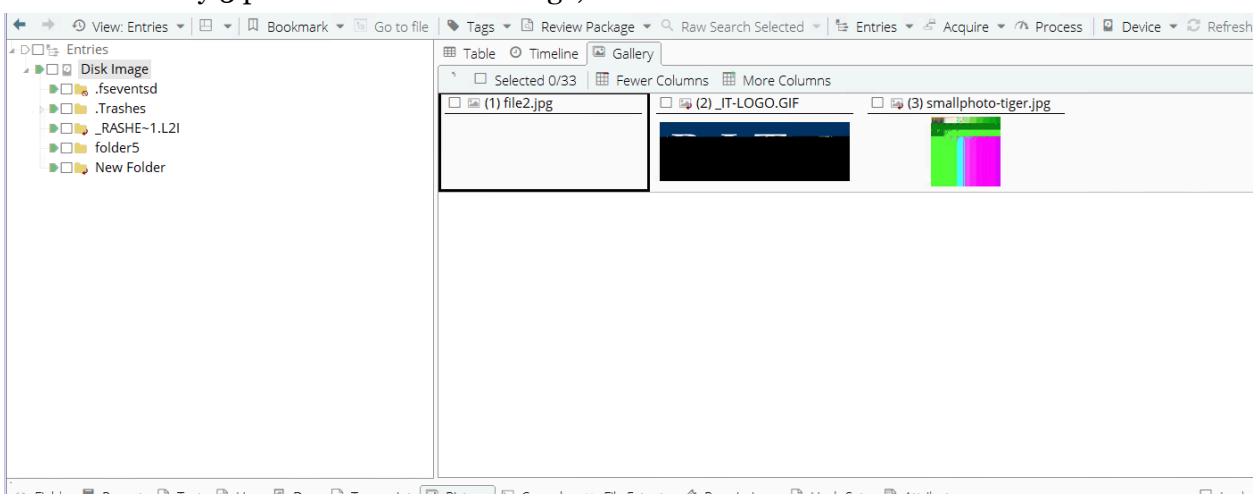


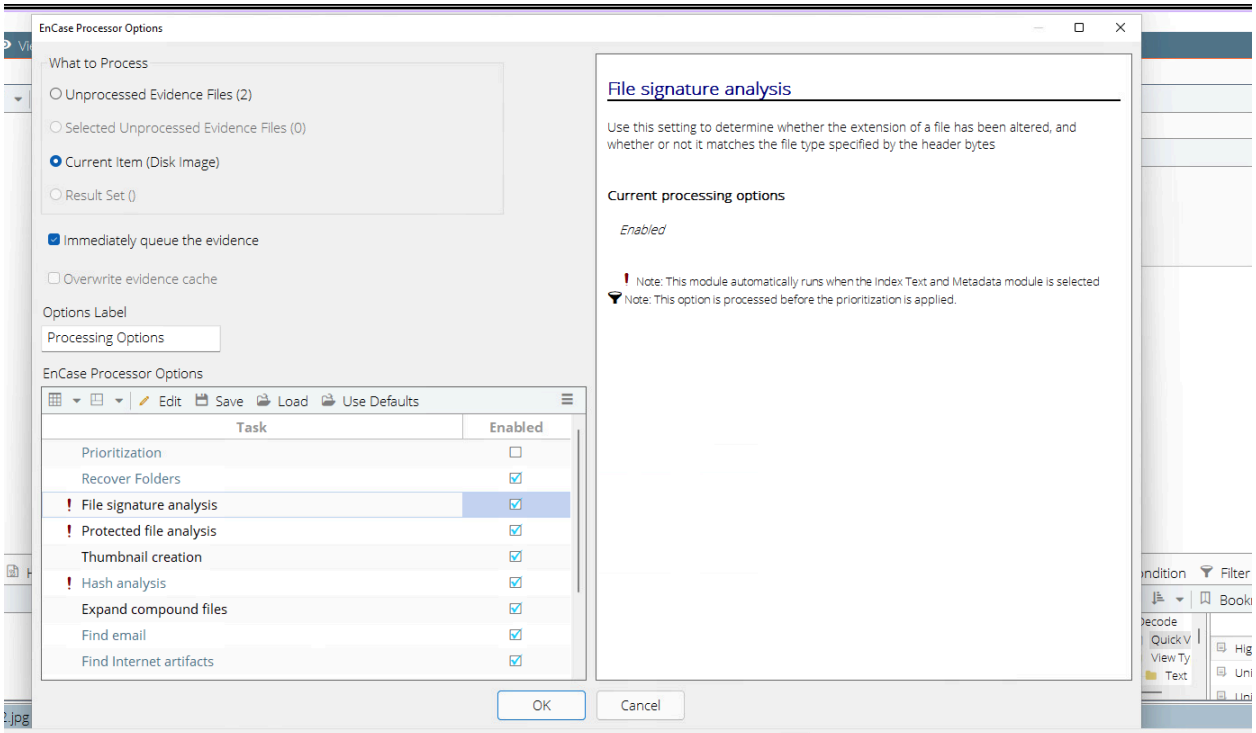




Question 7: In the WinLabRaw image, how many pictures are shown in Gallery View before performing file signature analysis?

There are totally 3 pictures in this raw image, we can see below.





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

According to the EnCase User Guide (page 134), EnCase uses different methods to recover deleted folders for FAT and NTFS file systems:
FAT File System:
For finding the deleted folders on FAT file, encase scans the unallocated clusters based on signatures. It works accordingly:

- First Encase will look for the signature.
- If the signature is found, it will check the folder details.
- Finally if the folder is deleted, it will recover the contents of the folder.

NTFS File Systems:
For finding the deleted folders from NTFS file system we have to parse the Master File Table (MFT) and check entries whether the folder is marked as deleted or not. It works accordingly:

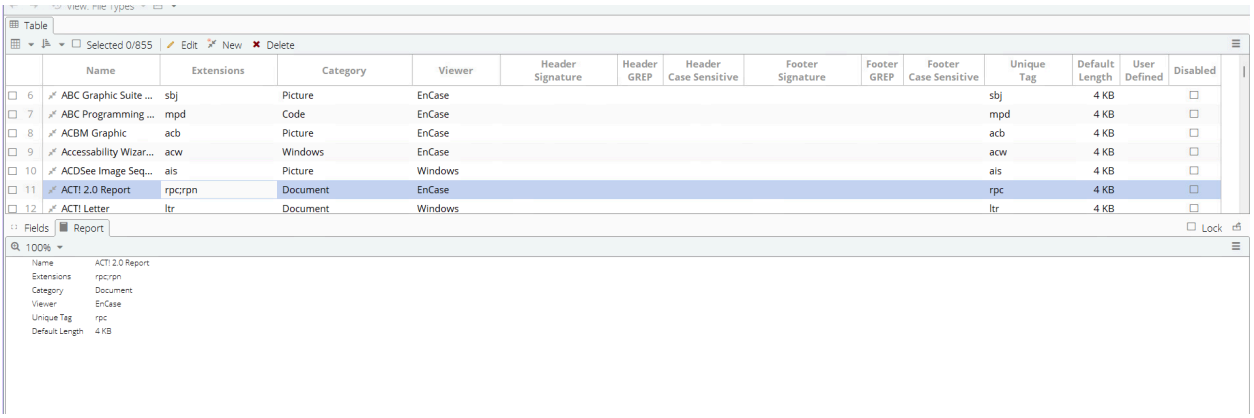
- Looks for the folders where the delete flag is set and recovers based on that.

Encase tries to recover folders with their folder structures and has a lot of filter options, We can customize them accordingly, also the degree of recovery depends on the amount of fragmentation, and size of the drive, whether it is overwritten much or not.
We can enable or disable the recovery of the deleted folders.

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

There are total 855 file types in this image, information listed for each file type is

- 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



	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
6	ABC Graphic Suite ...	sbj	Picture	EnCase							sbj	4 KB		
7	ABC Programming ...	mpd	Code	EnCase							mpd	4 KB		
8	ACBM Graphic	acb	Picture	EnCase							acb	4 KB		
9	Accessability Wizar...	acw	Windows	EnCase							acw	4 KB		
10	ACDSee Image Seq...	ais	Picture	Windows							ais	4 KB		
11	ACT! 2.0 Report	rpc;rpn	Document	EnCase							rpc	4 KB		
12	ACT! Letter	ltr	Document	Windows							ltr	4 KB		

Name	ACT! 2.0 Report
Extensions	rpc;rpn
Category	Document
Viewer	EnCase
Unique Tag	rpc
Default Length	4 KB

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

- We can use the file signature analysis to check whether it can match anything. If not we can update the file signature table, because encase uses signature to match the file type to give the information.

- We can export the file type and check with third party tools.
- We can also create a custom signature in encase for investigating it further.

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.

- Alias
- Unknown
- Match
- Bad Signature

	File Ext	Logical Size	Category	Signature Analysis	File Type	Protected	Protection complexity	Last Accessed	File Created
7	L2I	0	Folder					08/07/08	08/07/08 05:00:11 PM
8		0	Folder					12/16/03	12/16/03 09:26:46 PM
9		0	Folder					12/16/03	12/16/03 09:26:46 PM
10		0	Unknown						
11		3,276	Picture	Alias	Windows grap...			12/16/03	12/16/03 08:56:08 PM
12	Tr...	4,096	None	Unknown				08/07/08	08/07/08 05:00:11 PM
13	D...	0	Document					12/16/03	12/16/03 09:02:26 PM
14	doc	19,456	Document	Match	Compound Do...			08/07/08	12/16/03 09:02:26 PM
15	jpg	25	Picture	Bad signature				08/07/08	12/16/03 09:04:28 PM
16	xls	2,057	Picture	Alias	JPEG Image Sta...			08/07/08	12/16/03 08:57:24 PM
17	csv	904	Picture	Alias	JPEG Image Sta...			08/07/08	12/16/03 08:58:18 PM
18	doc	4,096	Document	Bad signature				08/07/08	08/07/08 10:00:09 PM
19	GIF	2,053	Picture					12/16/03	12/16/03 09:10:39 PM

These are four types in the signature Analysis column.

1. Alias: This means, that the file has been found and it has the match with the file in Encase Database, but it means that the header information is correct but the extension is not matched with it properly.
2. Unknown: So Encase tried it to match with the signature on the Encase Database and couldn't find it. So it displays as Unknown type.
3. Match: It means encase found the file type match based on the signature analysis and the signature matched with the one in the database.
4. Bad Signature: This is an interesting one, it means file is corrupted and somehow or somebody could have changed the format of the file, which could be the possibility. Even though the file has a bad signature, it can still be accessible.

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

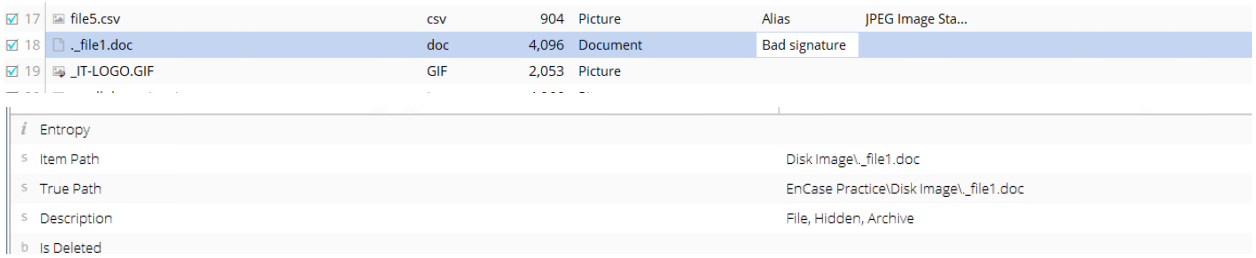
So we are looking for the bad signature which has a mismatch with the signature.

We have two file bad signature, one is file2.jpg

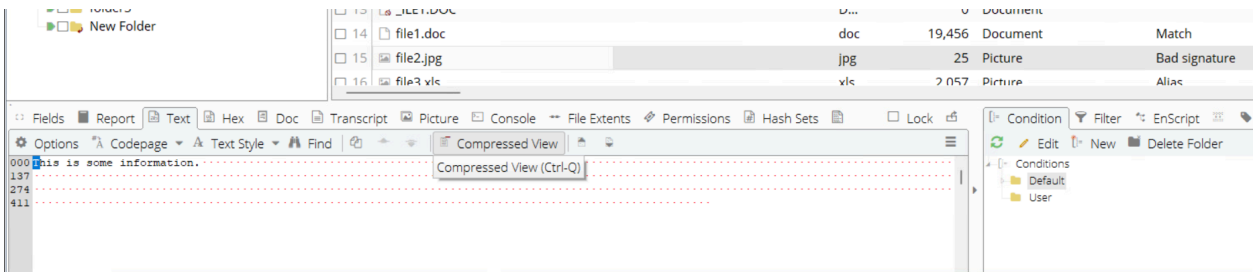
12	Tr...	4,096	None	Unknown		08/07/08	08/07/08 05:00:11 PM
13	D...	0	Document			12/16/03	12/16/03 09:02:26 PM
14	doc	19,456	Document	Match	Compound Do...	08/07/08	12/16/03 09:02:26 PM
15	jpg	25	Picture	Bad signature		08/07/08	12/16/03 09:04:28 PM
16	xls	2,057	Picture	Alias	JPEG Image Sta...	08/07/08	12/16/03 08:57:24 PM
17	csv	904	Picture	Alias	JPEG Image Sta...	08/07/08	12/16/03 08:58:18 PM
18	doc	4,096	Document	Bad signature		08/07/08	08/07/08 10:00:09 PM

s	Item Path	Disk Image\file2.jpg
s	True Path	EnCase Practice\Disk Image\file2.jpg
s	Description	File, Archive
b	Is Deleted	
	Entry Modified	

Second one is ._file.doc



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



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?

It is simple and straightforward with encase, that before the signature analysis if the .jpg file is changed into a .txt file, it will not display it in the graphics view. Because Encase works based on the file extension and as the file extension is .txt, it will simply leave that file.
But after the signature analysis encase will go through the file types thoroughly, if it found this file type is graphical, then it will display its content on the graphics tab regardless of its file extension.

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

The following files/dirs will not have hashes generated:

- Directories and Folders: The Directories simply store files and it wont have any data content on them. But they do have the information about the files they store inside them. So no hash will be generated.
- OS files: Registry hives, boot files and system related files needed for the proper functioning of the OS will not have hash generated for them.

- Encrypted and deleted files: Encrypted files simply can't have hashes as the content is encrypted, and some of the deleted files are overwritten it is difficult to get the hash out of it.
- Device Files: Device files like service file, User based files, and Disk Management files won't have the hashes.
- Free Cluster: The unallocated spaces and clusters in the disk won't have any hash generated for them.

ture ysis	File Type	MD5	SHA1	True Path	Description	Is Delet
				EnCase Practice\Disk Image\.fseventsd	Folder, Deleted, Hidden	•
n		6999badf387b4632f9b4058ebe63b4...	488e293abc87c7c0498f...	EnCase Practice\Disk Image\.fsevents...	File, Deleted, Archive	•
				EnCase Practice\Disk Image\.fsevents...	File, Deleted, Archive	•
				EnCase Practice\Disk Image\.Trashes	Folder, Hidden	
				EnCase Practice\Disk Image\.Trashes\...	Folder, Deleted	•
n		5ecad39c470178e1b0ef93e534b60fda	36dfed64b95c28cf63cce...	EnCase Practice\Disk Image\.Trashes\...	File, Deleted, Hidden, Archive	•
				EnCase Practice\Disk Image_RASHE~...	Folder, Deleted, Overwritten, Hidden	•
				EnCase Practice\Disk Image\folder5	Folder	
				EnCase Practice\Disk Image\New Fold...	Folder, Deleted, Overwritten	•

These are the description we can find :

- File
- Deleted
- Archive
- Hidden
- Overwritten

Alias	JPEG Image Sta...	c08ea9a345bda6186268e384fa70fbc5	303c308383e3c3549d6c...	EnCase Practice\Disk Image\file5.csv	File, Archive
Bad signature		0f46b2c34962b7a19587a3cf654aec8a	2fb41b32535f3f580f2eb...	EnCase Practice\Disk Image\._file1.doc	File, Hidden, Archive
				EnCase Practice\Disk Image_IT-LOG...	File, Deleted, Overwritten, Archive
				EnCase Practice\Disk Image\smallpho...	File, Deleted, Overwritten, Archive
Alias	GIF	9cecbdbbe294a8531aedeae5873517...	69392aa43e72d42d1bf7...	EnCase Practice\Disk Image\file6	File, Archive
Alias	JPEG Image Sta...	edd17fbcae897f7144159b5aaebb4bc5	e60a6e6bb30a9af26fbd...	EnCase Practice\Disk Image\file7.zip	File, Archive
				EnCase Practice\Disk Image\New Text...	File, Deleted, Archive
Match	Text	508ff7a91db0a80a13151f786fbb6e43	38dc57ababe48208e527...	EnCase Practice\Disk Image\secret.txt	File, Archive

Above screenshot shows if the file is overwritten, we don't have hash, if the file is Deleted and Archived, no hash, but the crucial point here is File is Deleted and hidden and Archive will have the Hash generated.
Deleted files are still hidden and archived, so they still exist somewhere in the system so they have the hash.

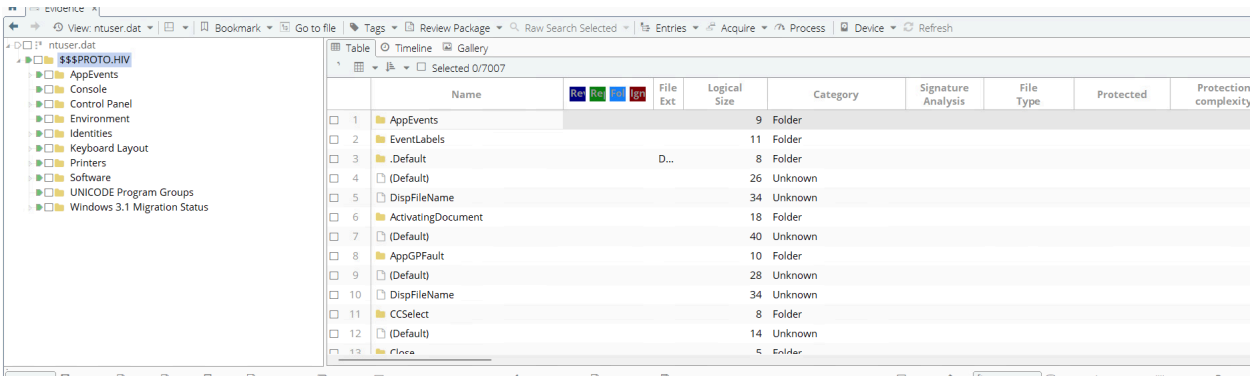
Question 16: What are the three most common uses for hash analysis?

The main use case of hash analysis are:

- Checking the integrity of the files.
- Identify the file and Verify it.
- For filtering the file types based on the hash matching.
- Finding the corrupt file.

- Checking the authenticity of the file.

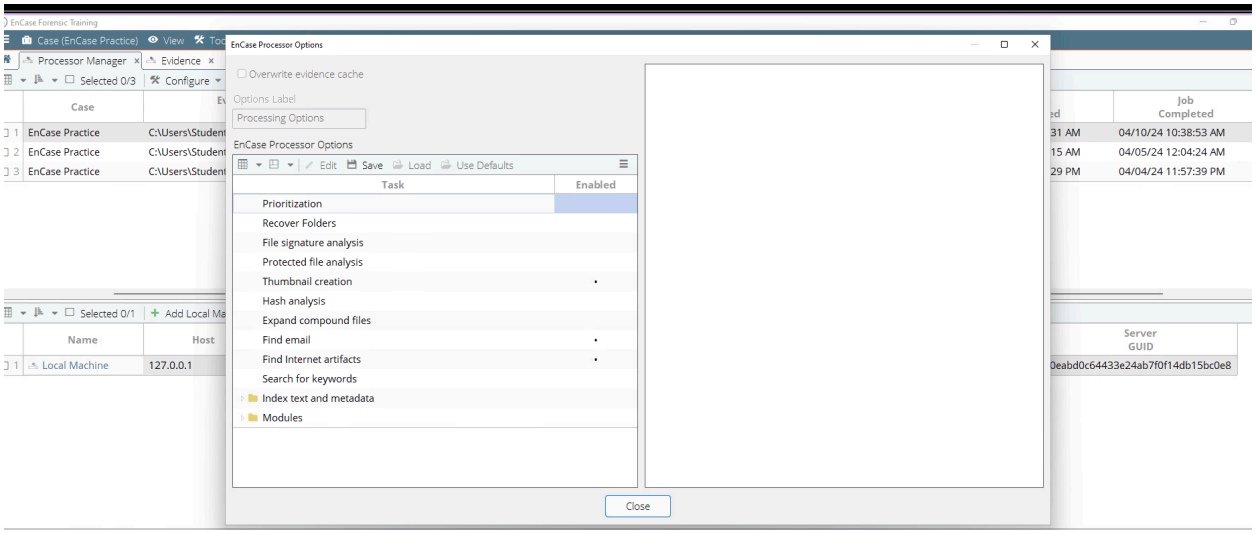
Question 17: What kind of important information do you get?



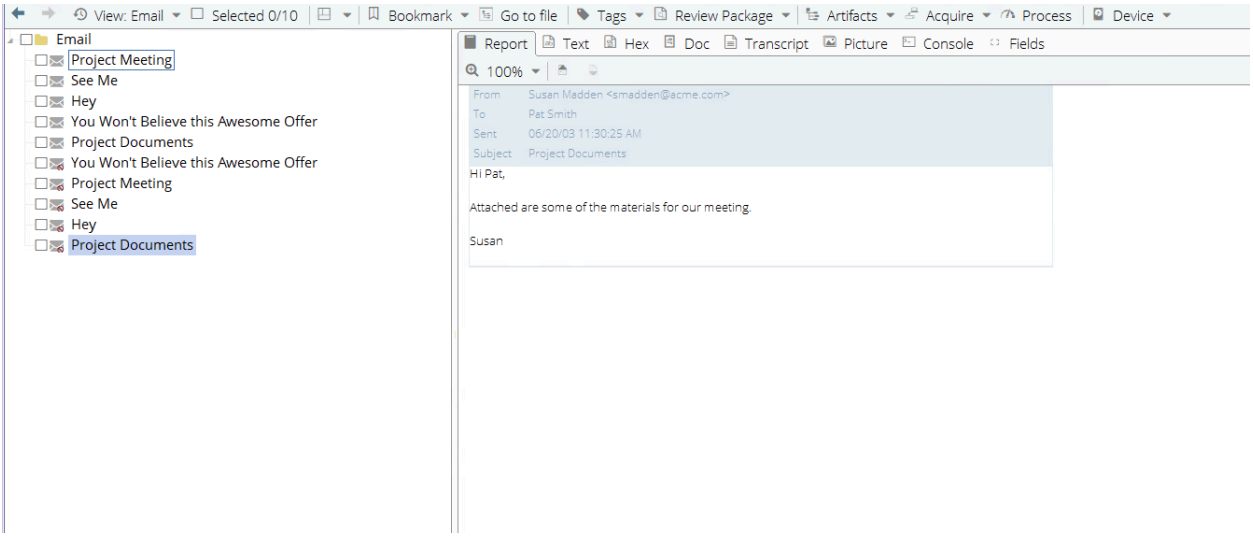
NTuser.dat has all the user specific information and the environment set by them, it has their customized settings, Softwares, Environment settings and Control panel settings, these are the important settings to find the links that are needed for the process.

Also it has the following things:

- The Recent files that have been used and opened.
- User Customization options.
- User device settings and other important things used like printers and network details.
- Internet History and other typed URLs and Bookmarks of the user.
- User Application settings and Jumplists.



List of emails



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

So from the inbox I found the following information

- Susan wanted to meet pat for discussing about the project and its details over weekend
- It seems like there was an outburst at the meeting for some reason.
- Scott wants to have a drink with pat to discuss about the outburst having concern.
- John is a director who wants to meet pat regarding the outburst and these mails were between June 20th of June to 24th of June.

100%

From Pat Smith <psmith@acme.com>
To bconrad@raytheon.com
Sent 06/24/03 01:06:52 PM
Subject A Proposition

I'd like to offer you some material from my company in exchange for a position in your company.

Pat Smith
psmith@acme.com

Attachments

Name (Alternate Body)
Logical Size 128

(Alternate Body)

From Pat Smith <psmith@acme.com>
To bconrad@raytheon.com
Sent 07/01/03 11:04:39 AM
Subject My Proposition

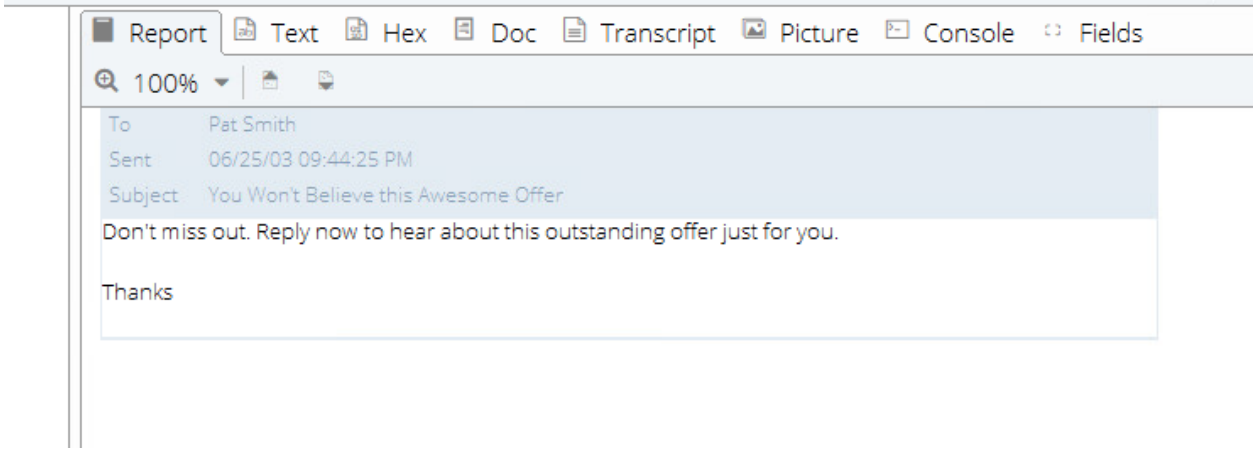
It's been a week since I sent you my proposal. Have you had a chance to consider it?

Pat

Attachments

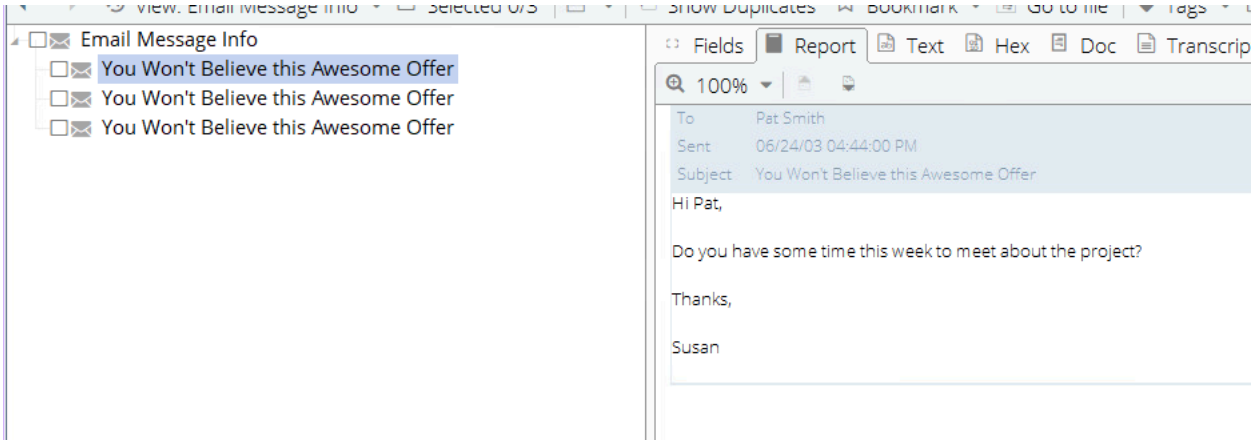
Name (Alternate Body)
Logical Size 94

(Alternate Body)



From these emails we can notice something going on, and Pat is trying to offer something to someone in exchange for a job in their company.

Related message with deleted items.

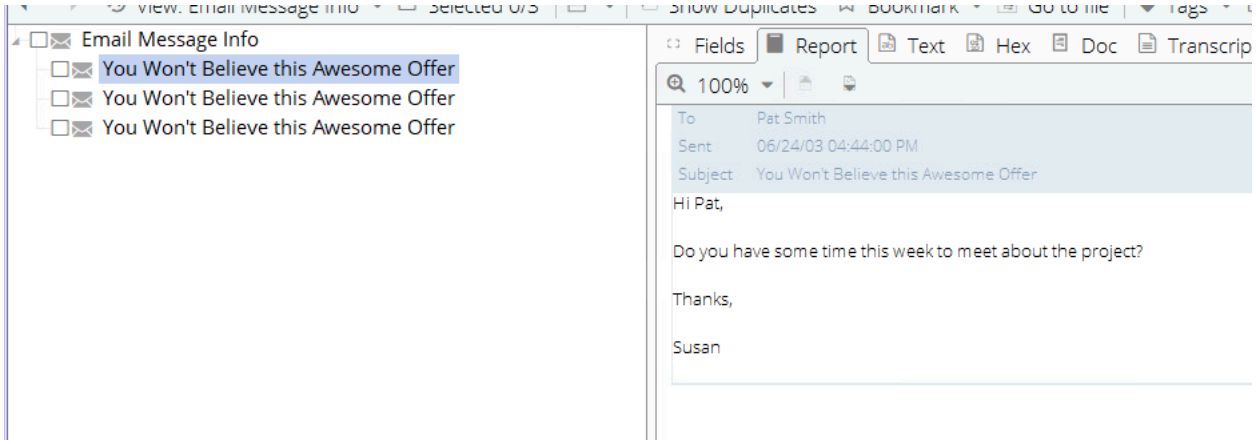


Question 19: Read the EnCase User Guide on p. 243, and briefly describe what are the *Show conversation* and *Show related messages* features.

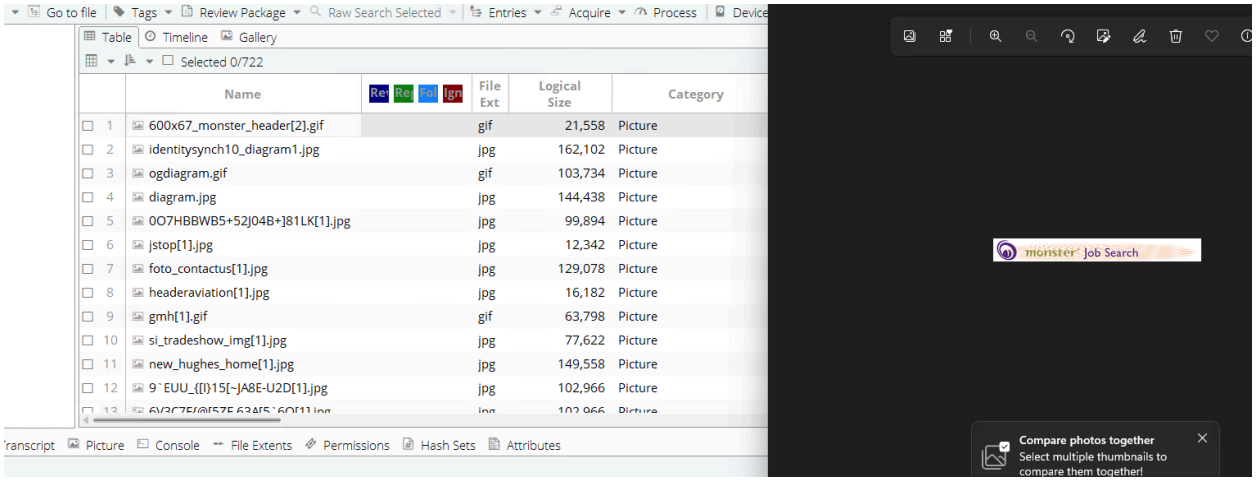
So From my understanding both show conversation and show related messages are important to display the email conversation and both works differently.

Show conversation, will check the header of the emails, and header field like. Message ID, reply ID and thread ID, Based on these factors, encase will group together these emails. These will be effective only after running the process “Find Email” from the process manager. This sometimes, won’t reconstruct everything, but most of the times it will have everything we need.

For Related message, some of the content or context of the mails will match and those emails will be grouped together, like below example which is easy to follow and understand.



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



It seems like presentation slide.

to file | Tags | Review Package | Raw Search Selected | Entries | Acquire | Process | Device | Refresh

Table | Timeline | Gallery

Selected 0/722

	Name	Ret	Re	Fo	Ign	File Ext	Logical Size	Category	Signature Analysis	File Type	Protected
13	6V3C7F{@[5ZF,63A[5`6O[1].jpg					jpg	102,966	Picture			
14	logo[1].gif					gif	77,622	Picture			
15	jobs[1].jpg					jpg	195,126	Picture			
16	header_redone_clouds[1].jpg					jpg	29,238	Picture			
17	ql_bg[1].gif					gif	58,422	Picture			
18	8MBAZ[-V~3DP-C3ZX5,ZU[1].jpg					jpg	102,966	Picture			
19	si_cobra_img[1].jpg					jpg	77,622	Picture			
20	166x116_emp_entry_box[1].gif					gif	137,526	Picture			
21	foot[1].gif					gif	24,630	Picture			
22	si_mars_img[1].jpg					jpg	77,622	Picture			
23	bbip[1].jpg					jpg	111,414	Picture			
24	+PXLJAZW4041~W_!_HFLX5[1].jpg					jpg	170,550	Picture			
25	islogo100w[1].jpg					jpg	143,670	Picture			

There are a lot of thumbnails associated here, and it seems like a lot of presentation slides that he may have prepared for his presentation.

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

- **Monster.com**
- **Jobs.com**
- **Hughes.com**
- **boeing.com**
- **raytheon.com (Ray Jobs)**

We can see he is visiting lot of job sites and trying to find a job

Visit Count	1
Url Name	file:///C:/Documents%20and%20Settings/psmith/My%20Documents/Confidential/Project%20238x.rtf
Url Host	/
Net Show Url	file:///C:/Documents and Settings/psmith/My Documents/Confidential/Project 238x.rtf
Record Last	03/09/04 08:30:31 AM

URL

1

file:///C:/Documents%20and%20Settings/psmith/My%20Documents/Confidential/diagram.gif

/

file:///C:/Documents and Settings/psmith/My Documents/Confidential/diagram.gif

03/09/04 08:30:38 AM

Visit Count	1
Url Name	file:///C:/Documents%20and%20Settings/psmith/My%20Documents/Confidential/Project%2047x.doc
Url Host	/
Net Show Url	file:///C:/Documents and Settings/psmith/My Documents/Confidential/Project 47x.doc
Record Last	03/09/04 08:30:12 AM

Options | Codepage | Text Style | Find | Compressed View

```
A HREF="http://www.jsfirm.com/searchcontractors.asp" ADD_DATE="1078839058" ID="rdf:#$43mQa3">Aviation jobs and Aviation employees JSfirm.
```

JSfirm has Aviation Jobs and Aviation employees and he also tried to use hotmail.

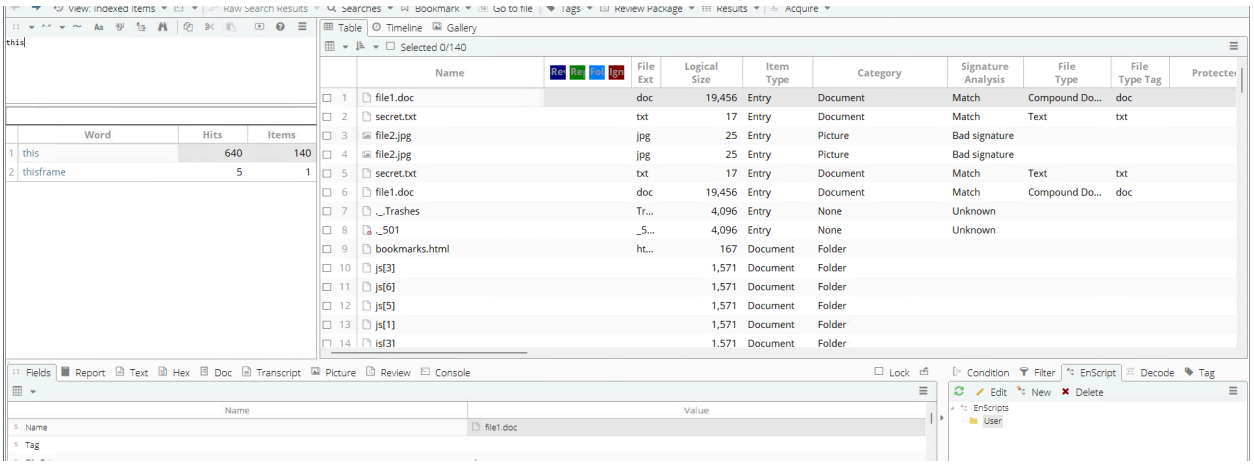
This is the crucial information because, He has a message to one from JSfirm that he needs jobs in exchange for something he is going to share.

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.)

It will affect our search because it refers to searches on the space which are unallocated, and there is a chance that this unallocated space is not overwritten and has deleted files in it.

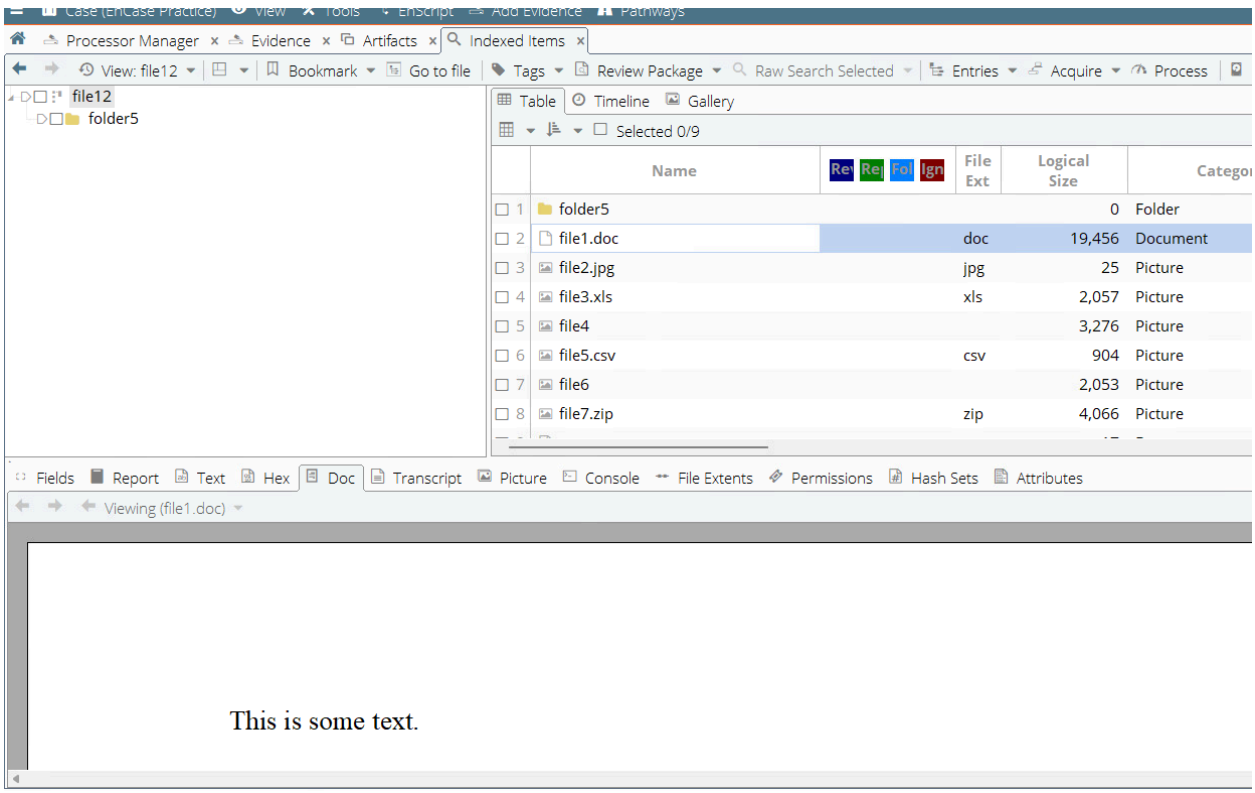
Checking out these unallocated space will give internet history, bookmarks and downloads which are deleted and not overwritten yet, so it is still recoverable from that.

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

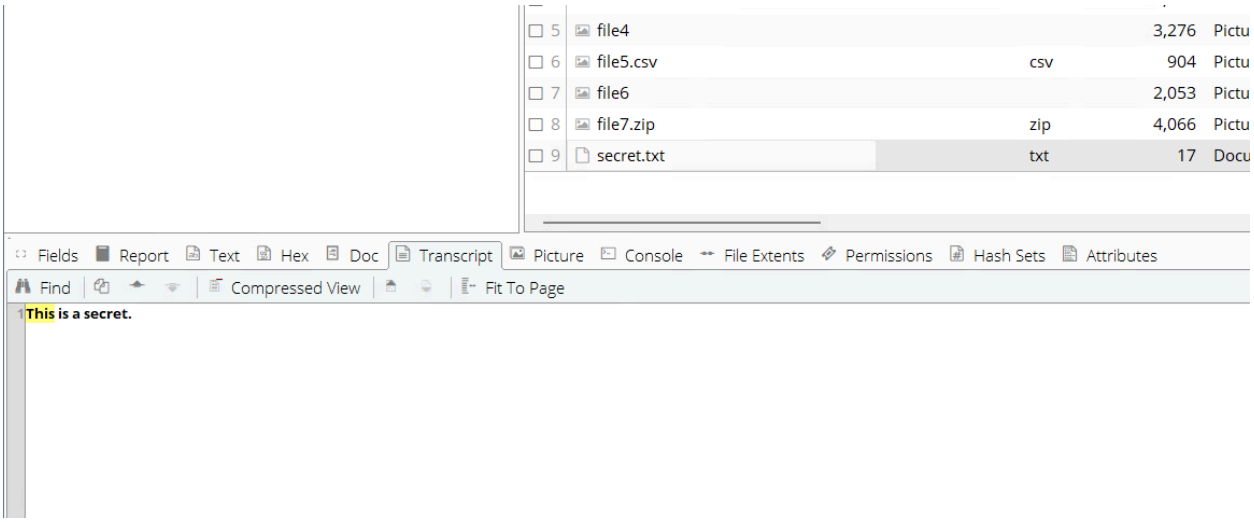


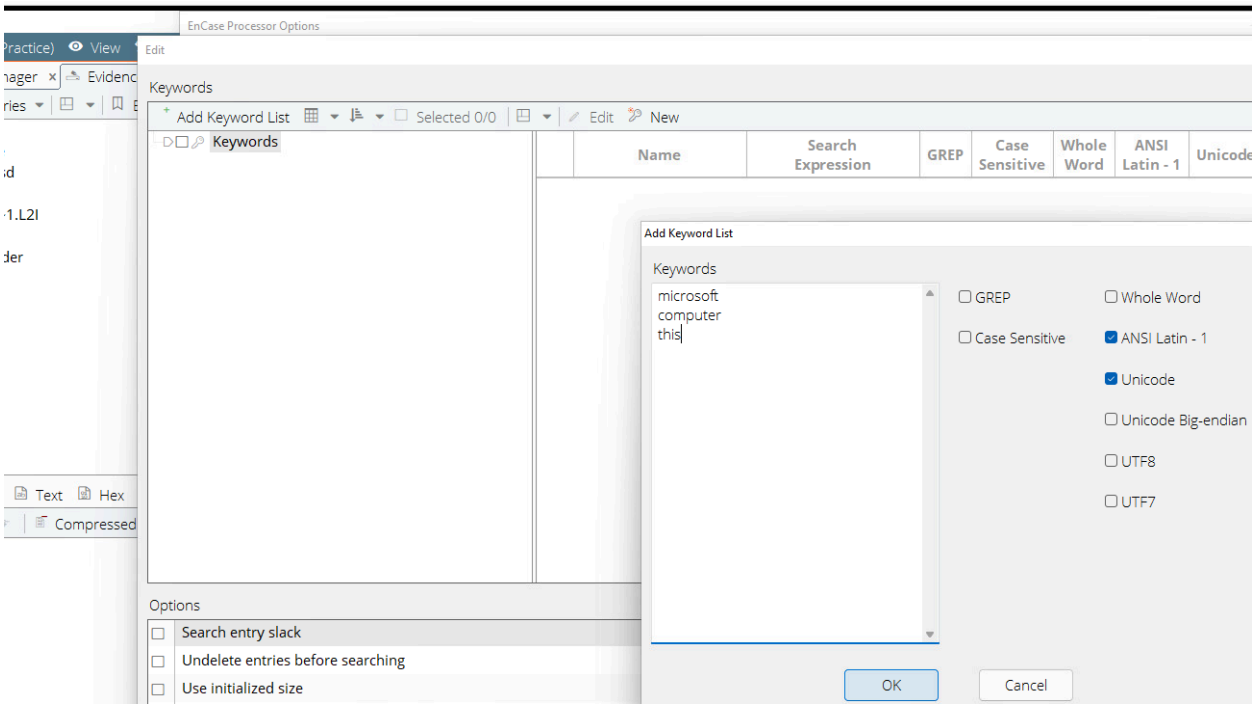
These are the files has this keyword.

1. **File.doc**



2. Secret.txt


file4 3,276 Pictu
file5.csv csv 904 Pictu
file6 2,053 Pictu
file7.zip zip 4,066 Pictu
secret.txt txt 17 Docu
Fields Report Text Hex Doc Transcript Picture Console File Extents Permissions Hash Sets Attributes
Find Compressed View Fit To Page
This is a secret.

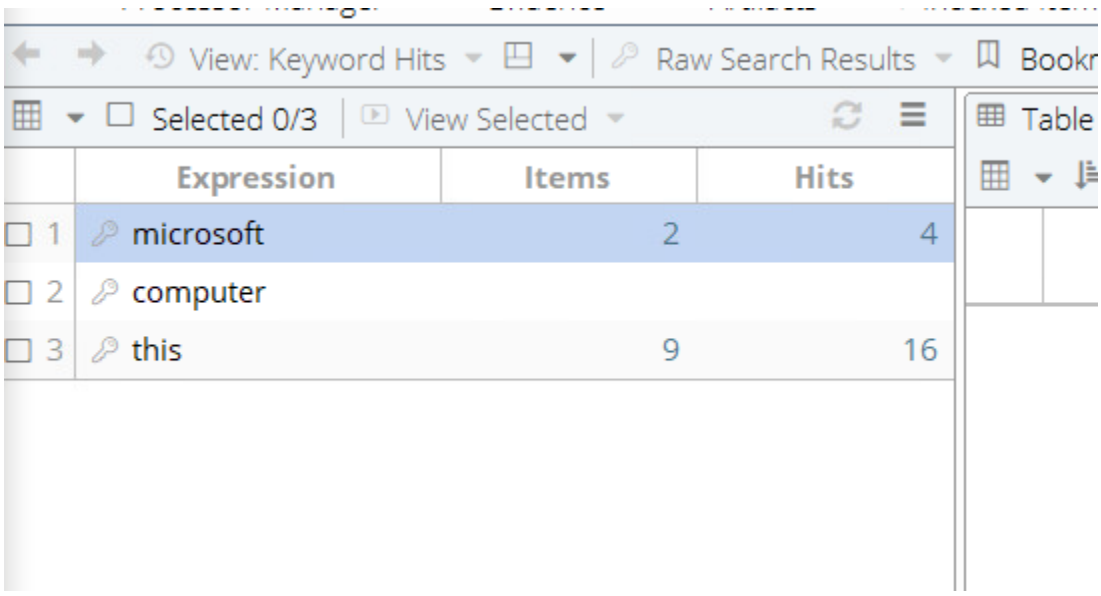

EnCase Processor Options
Edit
Keywords
Add Keyword List Selected 0/0 Edit New
Keywords
Name Search Expression GREP Case Sensitive Whole Word ANSI Latin - 1 Unicode
Add Keyword List
Keywords
microsoft
computer
this
GREP
Case Sensitive
Whole Word
ANSI Latin - 1
Unicode
Unicode Big-endian
UTF8
UTF7
OK
Cancel
Options
Search entry slack
Undelete entries before searching
Use initialized size

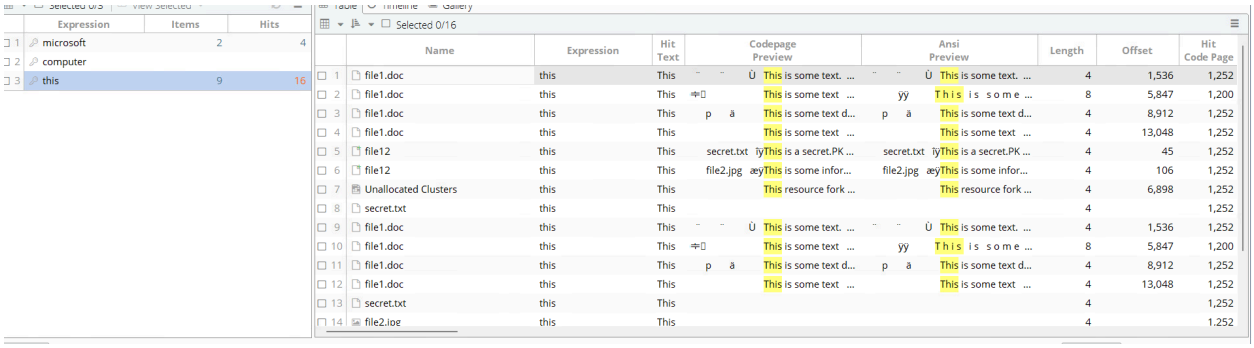
Question 24: What are the other search options besides "Search entry slack"? (p. 266)

We have other things than search entry slack

- Undelete entries before searching: It will undelete the files that are deleted before searching for the keyword.
- Use initialized size: Some applications won't have same size before they initialize size bigger than their actual need for future need and sometimes smaller to launch the application faster. So it will search based on the initialized size.
- Skip contents for known files: To search only known files that are identified by the hash library.

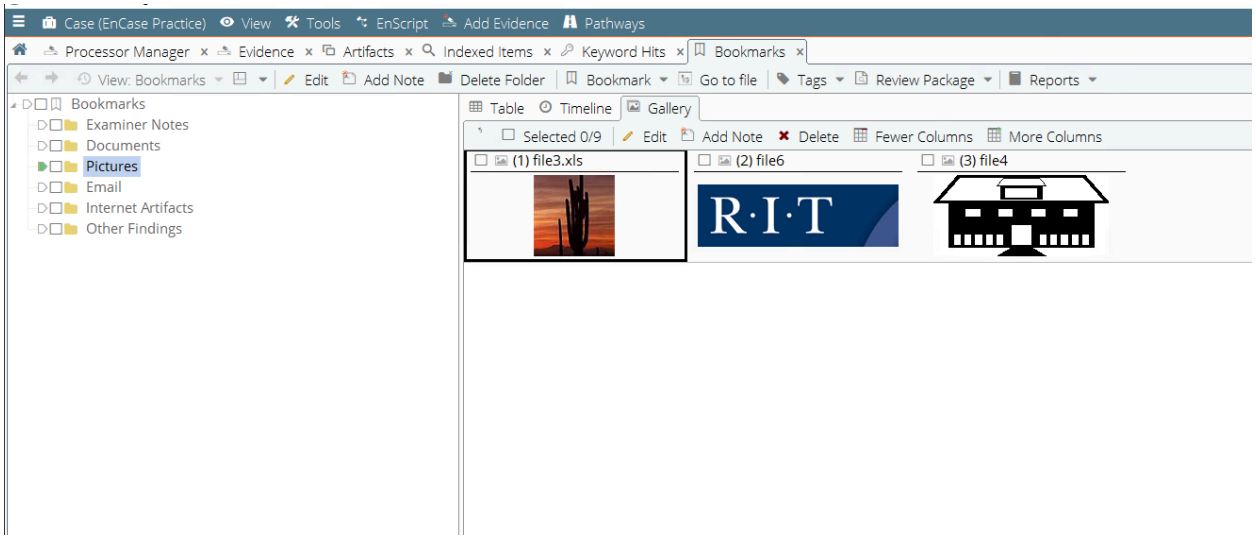
Question 25: How many hits do you get for Microsoft, computer, and this respectively?





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

I have created the bookmark successfully and included three images that I found after signature analysis.



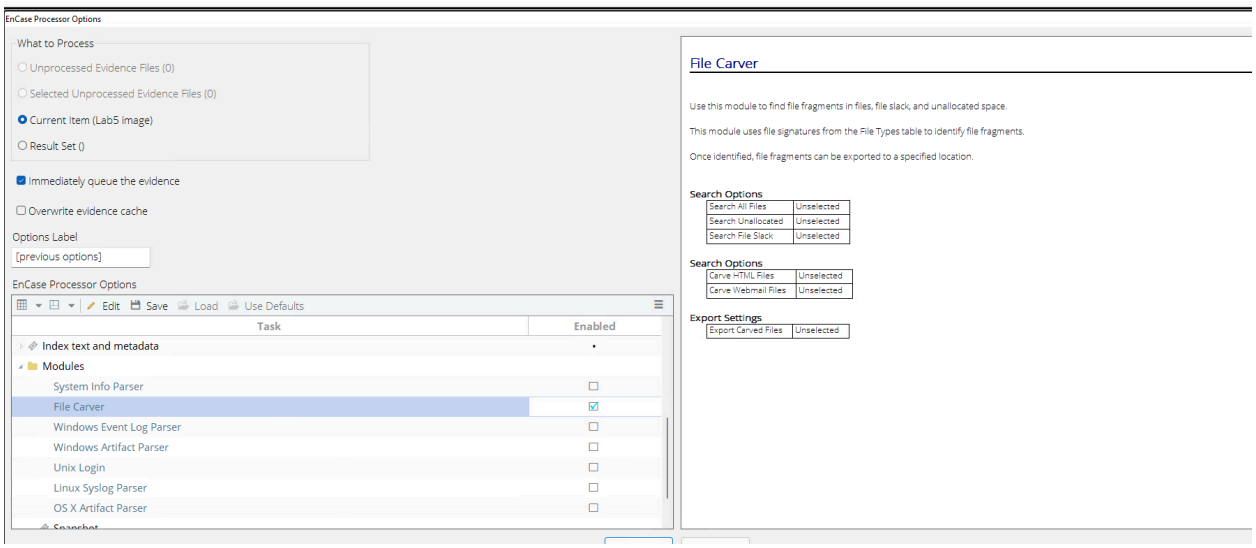
Action 27: Show the tagged Files in the Table view.

	Name	Revie	Repor	Follo	Ignor	Files	File Ext	Logical Size	Categ
22	file7.zip						zip	4,066	Picture
23	New Text Document.txt						txt	0	Document
24	secret.txt					Files	txt	17	Document
25	_ILE12.ZIP						ZIP	0	Archive
26	_DO							0	Unknown
27	__sdkft__.out						out	0	None
28	file12							12,047	Archive
29	Volume Boot							512	Unknown

We can see that secret.txt is marked as a suspicious File.

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

We can use file carver to find the left fragments, file slack and unallocated space present in the disk. As everything in encase works on matching the signature, it uses the file types table to match and find the fragments accordingly.



I want to carve the pictures and store them in the carved files folder, we can see the results after the process is completed.