48436/32309 Week 02 Lab Forensics Case Report

Upload this document as a pdf.

Name: Huynh Lam Student ID: 13264763 Date: 15/08/2021

Activity No.: Cmp1/03

Q1) The Order of Volatility

How does the effect of time on volatile data cause problems for the forensics process?

All data is volatile, however. As time passes the veracity of the information goes down, and the ability to recall or validate the data also decreases. It is extremely difficult to verify that stored information has not been subverted or changed. Volatility is important when collecting evidence. There are certain types of data on top of the volatility list which become virtually impossible to recover within a short amount of time such as CPU registers and frame buffers. However, going down the chain to the more persistent and harder to alter the type of data. These layers are where devices have a longer life expectancy which means there isn't a battle against time to extract this information.

Why does the first responder consider volatility before executing any command?

Gathering data according to the order of volatility helps to preserve rather than destroy. Doing something to one layer destroys information in all layers above it. The Point of the order of volatility is the opposite: doing something in one layer destroys information in all layers above it. The first responder will need to carefully execute a command as a simple command to retrieve information can destroy the contents of registers, MMUs, physical memory, and time stamping in the file systems.

Q2) Live or Post Mortem?

Indicate what is the worry with the effect of a live analysis on disk based evidence.

The problem is that live analysis often changes evidence by writing to the hard drive. File timestamps, Registry keys, swap files, and memory are just some of the items that can be affected when conducting analysis on a live computer system. Often, once the live analyst is done, the resulting MD5 hash will not match the hash collected prior to the live collection. Another worry is that the hacker might use anti-forensics techniques to delay/destroy certain evidence such as leaving rootkits. There are also some common challenges are lack of availability of proper guidelines for collection acquisition and presentation of electronic evidence and depending on the size of data it is practically impossible to do a live analysis on everything.

What is the advantage of a remote live analysis when you are not sure if an intrusion has happened?

Live investigations allow investigators to capture volatile information that would not normally be present in a post-mortem investigation. This information can consist of running processes, event logs, network information, registered drivers, and registered services. Running services tell us the types of services that may be running on a computer. These services run at a much higher priority than processes, and many users are unaware that these services exist. By conducting a live investigation, we can see the state of these services, which could prove crucial to our investigation.

Viewing running processes with the associated open network ports is one of the most important features of analysing the system state. To peek into a system and correctly assess what processes are running and what ports they may be using is critical when trying to perform an investigative triage. the priority, the number of threads, number of handles, memory usage, and uptime. Trying to assess what someone is currently doing, or even what they have done in the past, this information is critical. In addition, in the world of memory-resident executables, analysing the current process list is vital.

Why is a Live Analysis the best option when you suspect the files on disk may be encrypted?
When encryption is applied to a data object, the contents of that object are illegible. Encryption, by default, is designed to obfuscate, and sometimes compress, the contents of the data object it encrypts. Once encrypted, the object's contents are hidden and are pretty much impossible to interpret.

When you use live forensics, the chances are significantly greater to view the encrypted file's contents. If the document is open, it will most likely be loaded into physical memory. In a live forensic environment, the investigator could image the physical memory of the computer system and glean useful information about what files and programs the suspect may be currently using. So, before pulling the plug, it may be worth our while to examine the contents of the physical memory.

In the case of whole disk encryption, a forensic examiner using live forensics techniques would be able to view the content of the drive when it is mounted by the suspect. Simply put, because the drive is presently being used, it is unencrypted.

Q3) Capturing an image using ProDiscover

C) Analysis

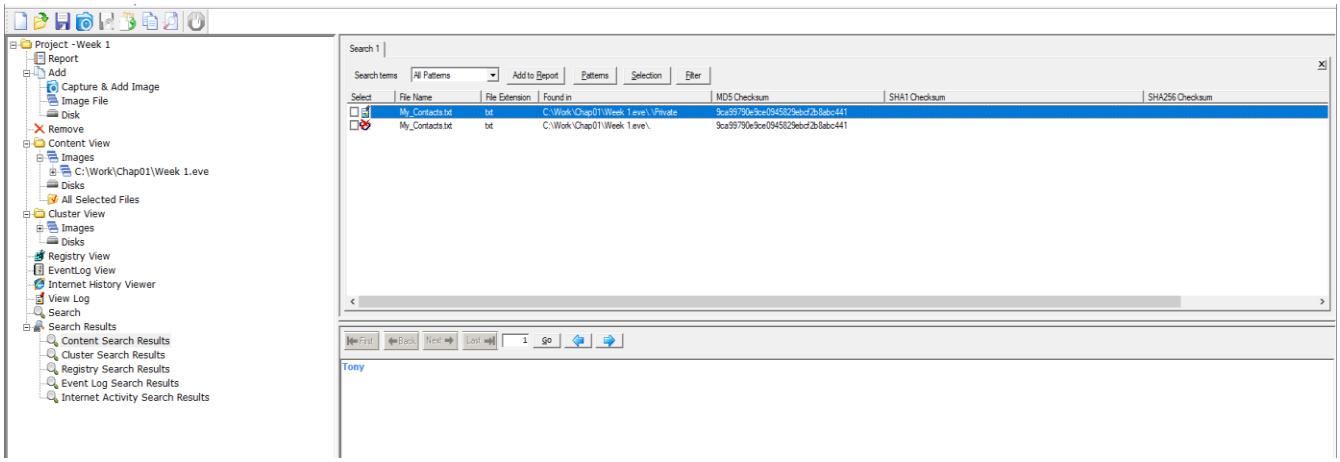
1) Search for a keyword in text files.

The search results appear.

Click the matching file in the work area.

The matching pattern will be shown in the data area.

Inset here your screen shot showing the work area and the data area result.



2) Search for a deleted file on disk.

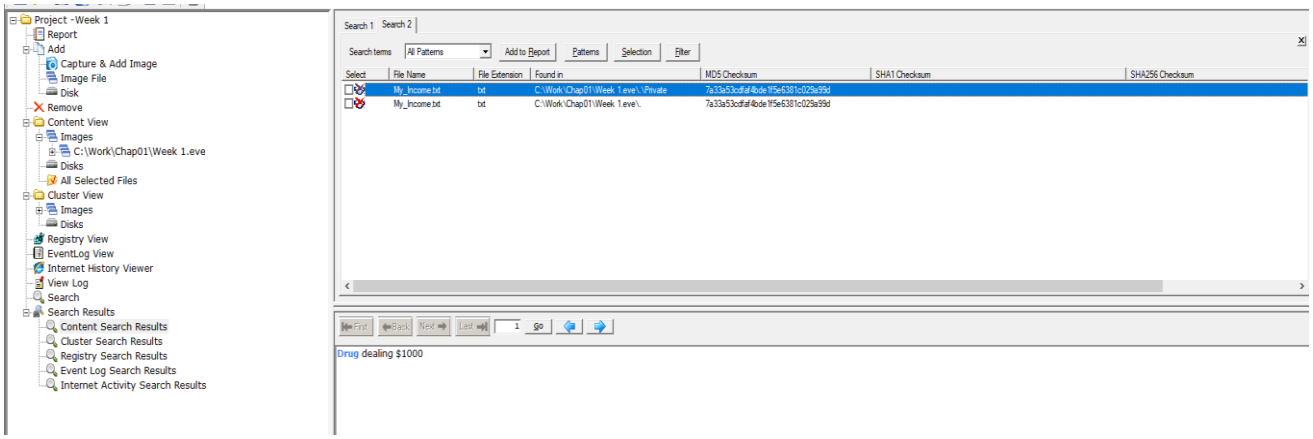
Note the red cross indicating the file has been deleted.

Click the matching file.

The matching pattern will be shown in the data area.

Insert your work area and data area screen shot here.

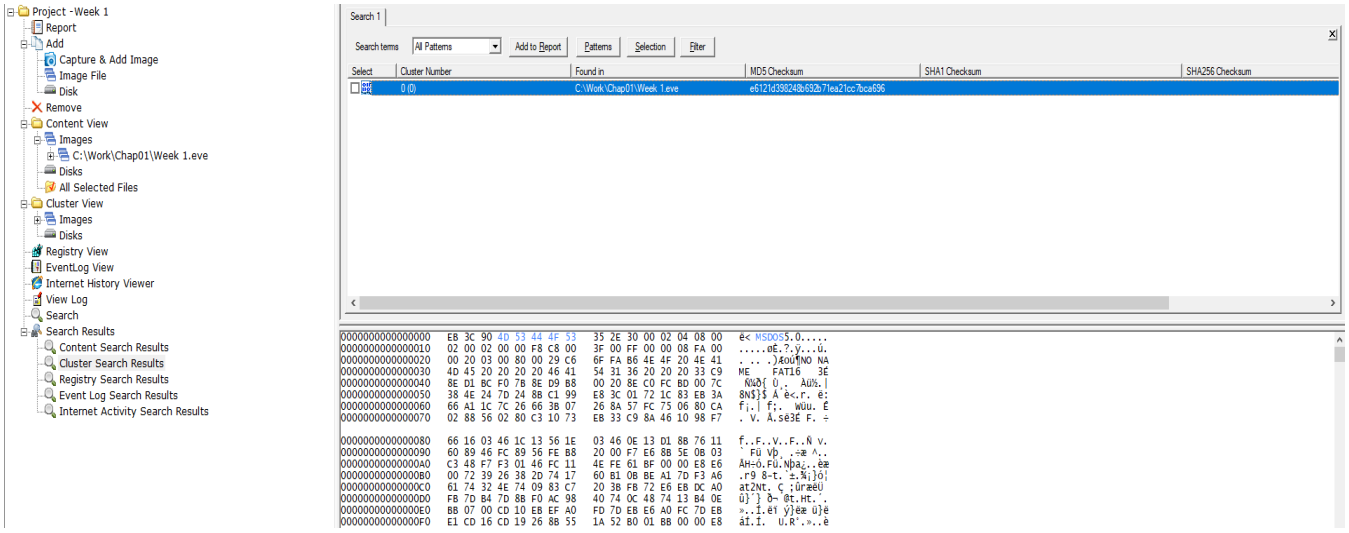
Week 02 Lab Forensics Case Report



3) Search for a cluster on disk.

When finished, the Cluster Search Results will list any matches.

Insert your screen shot showing the word MSDOS here.



What does FAT16 (or FAT32) mean? How does it relate to clusters? Add your answer here.

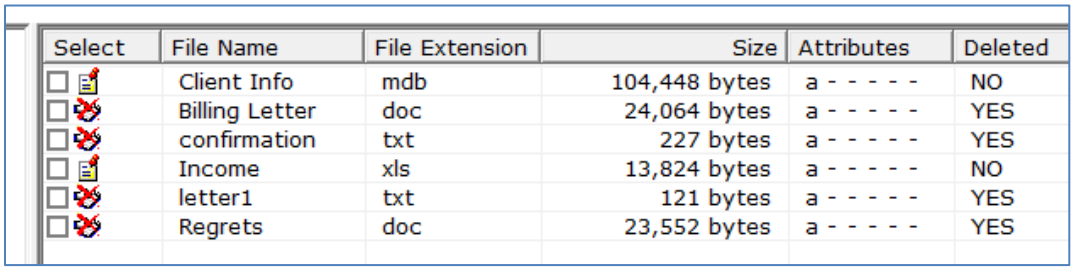
These types of FAT are file systems. FAT32, being a 32-bit file system, supports much larger disks than the FAT16 file system. Under the FAT32 file system, each partition is divided into clusters, each identified by a 32-bit number. Each cluster consists of one or smaller units, known as sectors, depending on the size of the partition.

Q4) Advanced – Optional - Analysing an image using ProDiscover

B) Acquisition

Select Letter1.

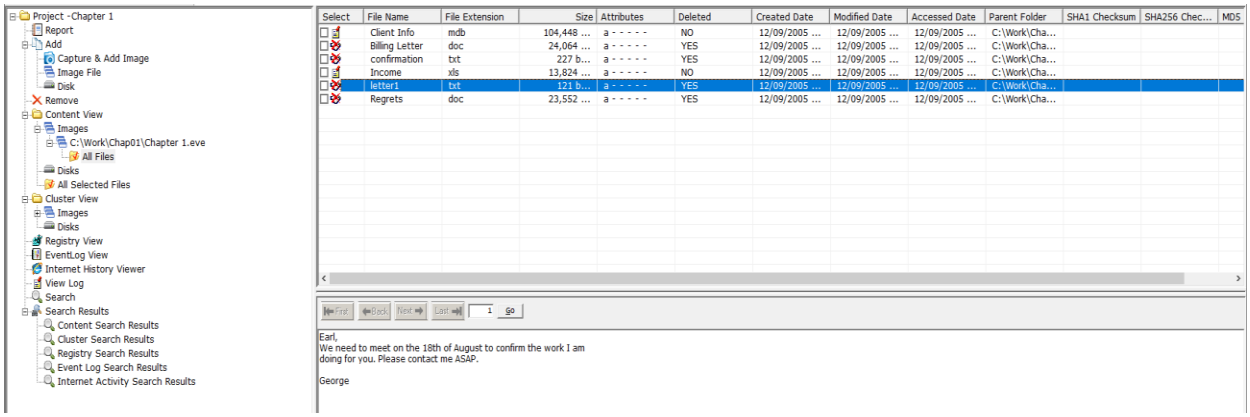
Note its contents in the data area.



Select	File Name	File Extension	Size	Attributes	Deleted
	Client Info	mdb	104,448 bytes	a - - - - -	NO
	Billing Letter	doc	24,064 bytes	a - - - - -	YES
	confirmation	txt	227 bytes	a - - - - -	YES
	Income	xls	13,824 bytes	a - - - - -	NO
	letter1	txt	121 bytes	a - - - - -	YES
	Regrets	doc	23,552 bytes	a - - - - -	YES

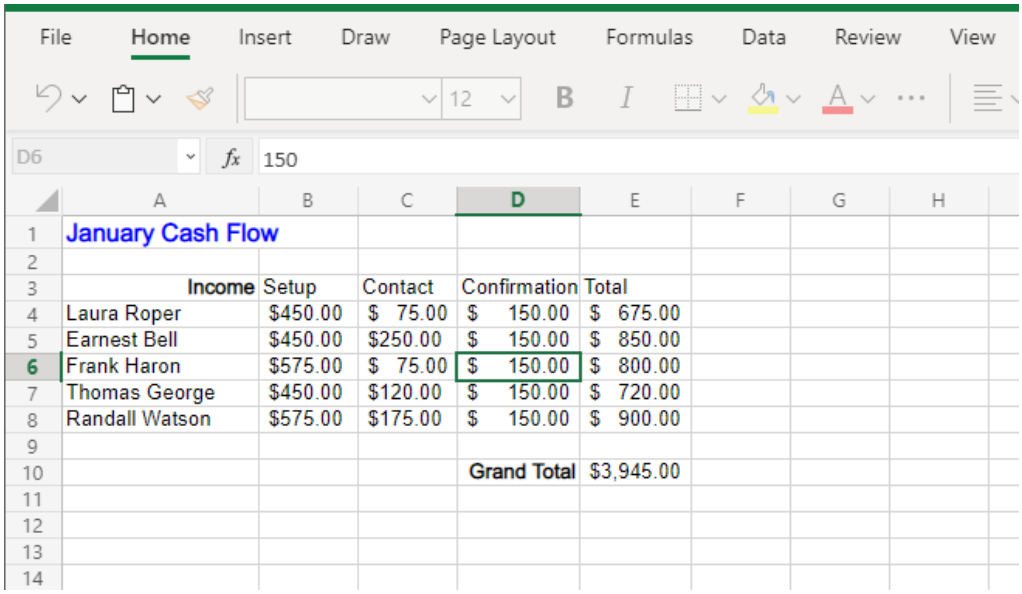
Insert your screen shot of the letter 1 contents here.

48436/32309 Week 02 Lab Forensics Case Report



C) Analysis

Insert here a screen shot of the spreadsheet.



	A	B	C	D	E	F	G	H
1	January Cash Flow							
2								
3	Income	Setup	Contact	Confirmation	Total			
4	Laura Roper	$450.00	$ 75.00	$ 150.00	$ 675.00			
5	Earnest Bell	$450.00	$250.00	$ 150.00	$ 850.00			
6	Frank Haron	$575.00	$ 75.00	$ 150.00	$ 800.00			
7	Thomas George	$450.00	$120.00	$ 150.00	$ 720.00			
8	Randall Watson	$575.00	$175.00	$ 150.00	$ 900.00			
9								
10				Grand Total	$3,945.00			
11								
12								
13								
14								

Examine enough files to determine if the allegation is proven or not.

D) ProDiscover Report

When finished, right click the ProDiscover report, and copy only the useful items here.

48436/32309

Week 02 Lab Forensics Case Report

These 2 screenshots include important items as the first screenshot have details on the case such as who is working on it, dates, files and MD5 checksum. The second screenshot indicates list of evidence with interest which means they are important to the case to prove an allegation.

Image Files:
File Name: C:\Work\Chap01\Chapter 1.eve
Image File Type: DFT Image
File Number: InChap02
Technician Name: Joe Friday
Date: 07/29/2006
Time: 12:09:05
MD5 Checksum: a117773bcf1fc88ec0ab8e0a349fbbcb
Checksum Validated: No
Compressed image: No
Time Zone Information:

Time Zone: (GMT-08:00) Pacific Time (US & Canada); Tijuana (Pacific Standard Time)
Daylight savings (summertime) was in effect: Yes
Time Zone information obtained automatically from remote system/image.

Hard Disk: C:\Work\Chap01\Chapter 1.eve
Volume Name:
File System: FAT12
Bytes Per Sector: 512
Total Clusters: 2847
Sectors per cluster: 1
Total Sectors: 2880
Hidden Sectors: 0
Total Capacity: 1440 KB
Start Sector: 0
End Sector: 2879

Evidence of Interest:

Total Evidence Items of Interest: 4

Hard Disk: A:\
List of Files:

C:\Work\Chap01\Chapter 1.eve\Regrets.doc
MD5 Checksum: EBCFBF22BDF81A60F6A16709D30C1DAD
Created:Modified:Last Accessed:
Cluster Chain:
Start Cluster End Cluster Total Clusters

Investigator's comments: Conversation between Randall Watson, who is another client of his business

---

C:\Work\Chap01\Chapter 1.eve\Income.xls
MD5 Checksum: 6A2E65AFC5AF4FC5F9DA2859DF134EAC
Created:12/09/2005 06:59:06Modified:12/09/2005 06:52:18Last Accessed:12/09/2005 00:00:00
Cluster Chain:
Start Cluster End Cluster Total Clusters

254 (FE) 280 (118) 27

Investigator's comments: List of payments and clients

C:\Work\Chap01\Chapter 1.eve\Billing Letter.doc
MD5 Checksum: 9FE241D0DDE27E83442010B3EEE5AD32
Created:Modified:Last Accessed:
Cluster Chain:
Start Cluster End Cluster Total Clusters

Investigator's comments: Business was done with Laura and the domain host is IT Connection Servers. George has breached company's policy

---

C:\Work\Chap01\Chapter 1.eve\confirmation.txt
MD5 Checksum: 18E391549E4A8BC990B264F590FB33BB
Created:Modified:Last Accessed:
Cluster Chain:
Start Cluster End Cluster Total Clusters

Investigator's comments: Confirmation of business between George and Laura

---

C:\Work\Chap01\Chapter 1.eve Hard Disk A:\ : **Evidence of Interest:** 4

Indicate here why the allegation is proven or not.

This evidence of interest would prove that George's allegation of breaking the company's policy is true. The billing letter.doc includes an email to Laura where he is using IT Connection Servers to host the website and the payments go directly to George. This is where he is creating his own private business of setting up his clients with websites. The confirmation.txt and Regrets.doc are where he is communicating with his clients for websites purposes. The last document is Income.xls shows all his clients and payments received from them.

For all Questions - Report Submission.

Save this report as a single pdf.

Upload this pdf to Canvas.