48436/32309 # Warm up upload report

Student Name: Huynh Lam Student Number 13264763 Date 4/08/2021

Refer to the Warm Up Tutorial.

Upload your answers on this form as a PDF. This is an individual upload.

Q1) Windows 10 networking.

Do this question before you come to the week 1 lab. Use a Windows laptop or workstation.

Are you using a Home Router, Public Wireless or at Work? Home

To examine your network interfaces use the ipconfig tool.

Which types are active?

- WiFi
- Ethernet adapter VMnet1
- Ethernet Adapter VMnet8
- LAN Adapter

For the active device what are its ip addresses?

IPV4 192.168.0.13 IPV6 fe80::89e7:9603:ffa4:f120%18

Is the IPv4 address public or private? private

How is this address allocated? These addresses are assigned automatically as when they join the network they will be dynamically configured to the network. As the end number of the IPv4 address is 13, this would mean that this is the 13th device on the home network.

There is a third address for the active device called a physical or MAC address.

Run ipconfig again with a command option (*you need to figure it out by yourself*) to see and note the MAC address.

What is the ipconfig option? Ipconfig /all

What is the MAC address? 4C-1D-96-D4-57-BF

Now look at your internet gateway.

Type netstat -r

Look at the IPV4 Route table.

What is the gateway IPV4 address? 192.168.0.1

How does it compare with your IP V4 address found above? The IPv4 address uses 32 bits which means it contains 4 octets separated by dots. However, the MAC address is 48 bits.

48436/32309

Warm up upload report

Now look at UTS on the network.

Type nslookup uts.edu.au.

The results are the DNS and the UTS public IPV4 address starting with 54.

Record DNS. uts.edu.au Record the UTS public IPv4 address 54.79.20.73

Explain how you can use the device IPv4, gateway and dns to figure out your location.

- Router DNS hijack as the hackers can overwrite the DNS settings and your requests can be redirected to malicious sites. This would result in an exposed IP address
- The devices gateway such as routers and switches can be hacked and redirect your requests to their own subnet receiving private information. These packets will contain your IP address.
- Using the IP address you are able to use third-party software to track and locate someone's location with their IP addresses which usually locates the ISP's location

---

Close your windows cmd window by typing exit.

Submission:

Upload your answers as a PDF on this form to Canvas.

48436/32309 # Week 01 Investigations Instructions

Aim:

To introduce Forensic concepts around evidence.

To open a Forensic case, collect evidence and draw a conclusion.

Method:

We **strongly** recommend you create a **Windows 10 virtual machine** and perform all the tutorials of this course on the virtual machine. You can create a snapshot of the virtual machine when the virtual machine is created so that you can roll back if needed.

Perform this lab and answer the questions below. Use the Lab **Report** document to create a **Forensics Report** for your Tutor. Do NOT upload these instructions.

Due Date:

Three days after the lab.

Assessment:

1% and Feedback will be given.

Q1) Digital Evidence ISO 27037.

Read the document in **Readings – Week 1** and answer these questions, you may need to use Google to find all the answers.

a) Explain the four processes used to handle **Digital Evidence**.

b) What is a **Digital Evidence First Responder**?

c) A Standard computer workstation with network connections may contain digital evidence. Name four more **types of devices** that may contain digital evidence.

d) What is **spoliation** in regards to Digital Evidence?

Q2) Evidence Collection – rfc3227.

Read the document in **Readings – Week 1** and answer these questions, you may need to use Google to find all the answers.

a) From a legal point of view, why is it important to collect evidence correctly?

b) Give an example of the **order of volatility** for a typical system, shortest first.

c) Describe what needs to be documented in a **Chain of Custody form**.

d) Name a command line program available on both Windows and Linux used to generate and compare **hashes** of files on a disk.

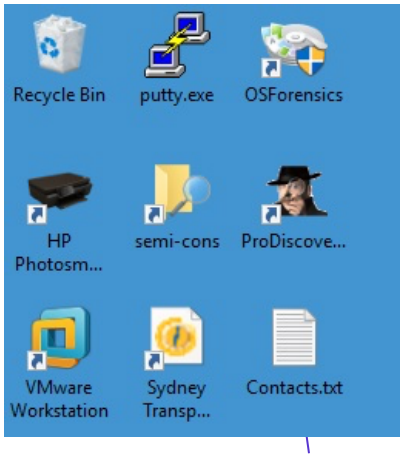
Q3) OSForensics

First generate some evidence. Open your Chrome Browser (Firefox will do as well.)

Go to Google and search for **Seek Roles**. Select **seek.com.au** in the hits found.

Confirm the Seek home page appears. Close Chrome.

Use notepad to save a text file called **Contacts** on your desktop. Include the name **Tony** in your contacts file. See (1)



(1)

Close notepad.

We will later search for evidence of your interaction with Tony

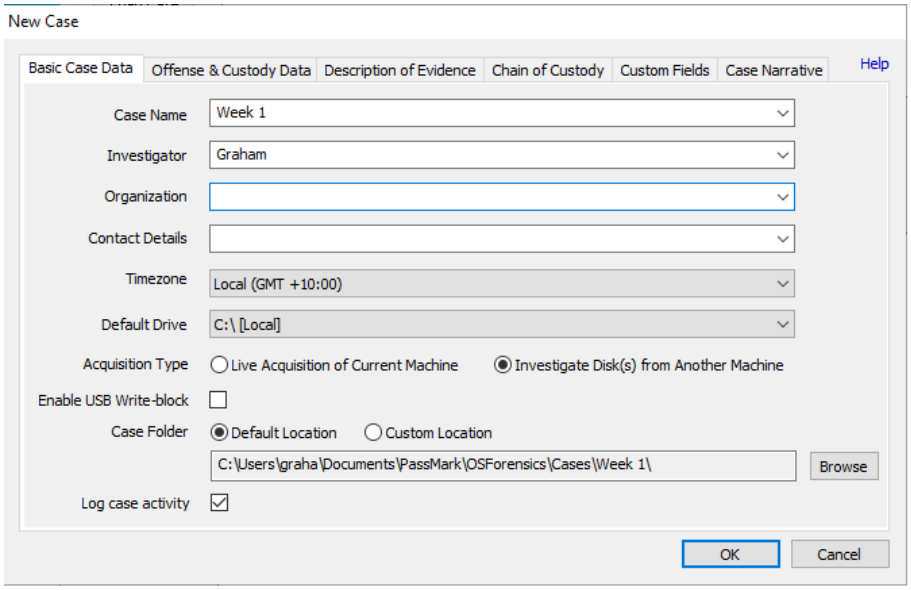
Now we will see how an investigator uses OSForensics to manage his/her investigation.

Download the program.
For Win 10 use https://www.osforensics.com/download.html
Version 7 is the current version (or use the link in canvas).
Right click the downloaded osf.exe file and run as administrator to Install OSForensics on a Windows Laptop, Windows Workstation or Windows Virtual Machine (VM). Accept the defaults.
If you have problems at any stage, ask your group for help. If the problem cannot be resolved, do not worry. Just document what happened and include a snapshot of any error messages to discuss with your tutor.
Run OSForensics. Click the **Continue Using Free Version** button. Note you have 30 days left (we just try OSForensics this week).

a) Add a Forensics Case.

Select **Manage Case** from the Menu Bar at left. Select the **New Case** button.

Name the Case Week 1. Enter your name as the Investigator. Click OK.



Week 01 Investigations Instructions

b) Search for recent activity.

Select User Activity from the menu bar at left.

Click the Scan button at right. Click Yes and OK to add the disk.

Wait a few minutes until your device is scanned. Ignore errors.

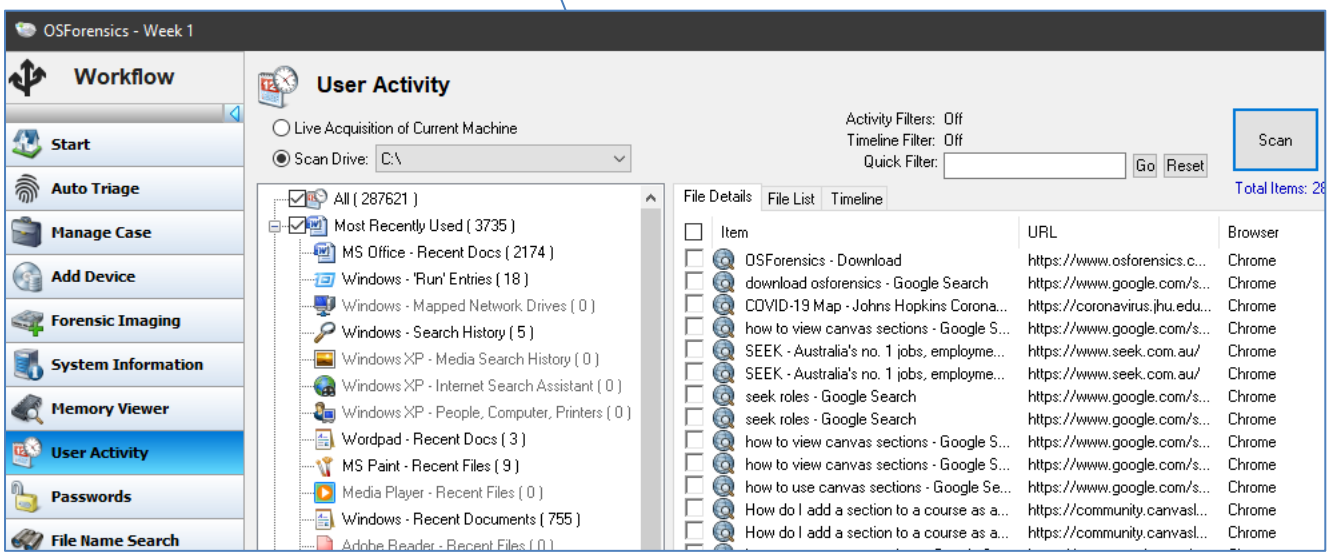
A summary window appears. Click OK.

You should have a list of User Activity.

Sort by Access Time descending.

Confirm you have evidence of your visit to Seek.

You should see Seek in Chrome Browser history.



Take a **screenshot** for your Report.

48436/32309 Week 01 Investigations Instructions

c) Index your text files and then search them.

Select **Create Index** from the menu bar at left. Tick only **Plain Text Files** and then click the **Next** button.

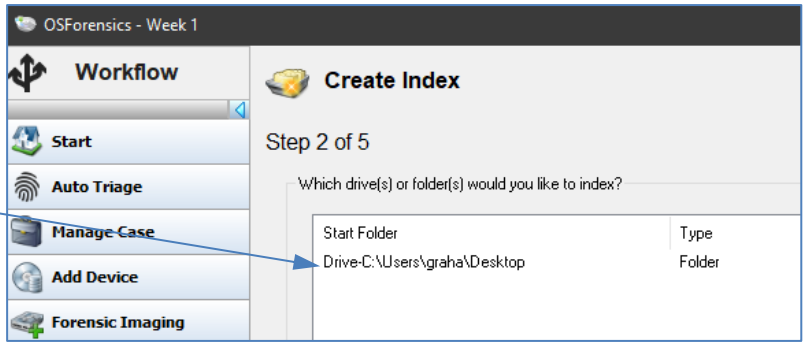
Click **Add** and select specific folder. Search for C:\Users\yourname\Desktop.

Click Ok and OK.

Confirm your result is similar to that shown.

Click Next.

Click Small. Click Next.



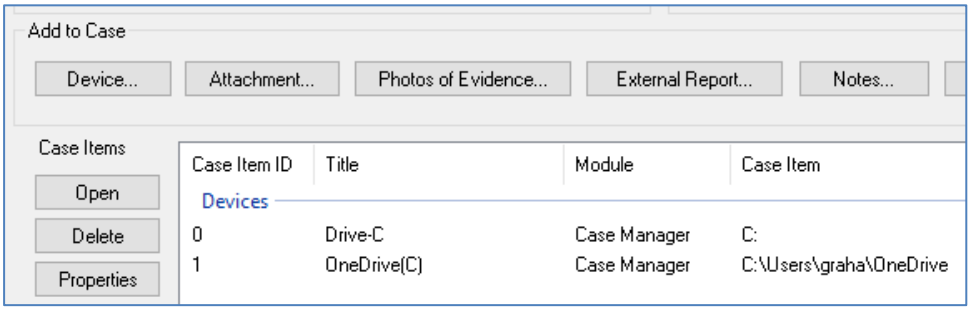
Click the **Start Indexing** button. This may take a few minutes.

If your conacts.txt file was not found, Windows may have moved your desktop to OneDrive.

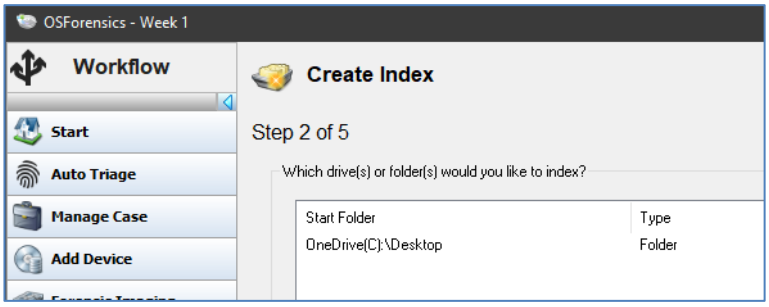
Select Manage Case. Under Add to Case Select Device.

Select Folder/Network Path. Browse to OneDrive. Click OK.

Check your Case looks like that shown.



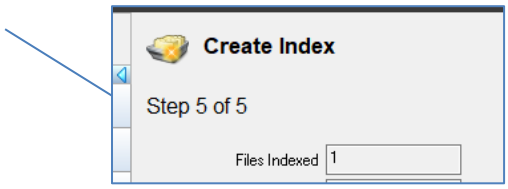
Redo the Create Index using the OneDrive desktop. *(Using 1 thread search in step 3 to reduce memory consumption.)*



Click the **Start Indexing** button. This may take a few minutes.

48436/32309 Week 01 Investigations Instructions

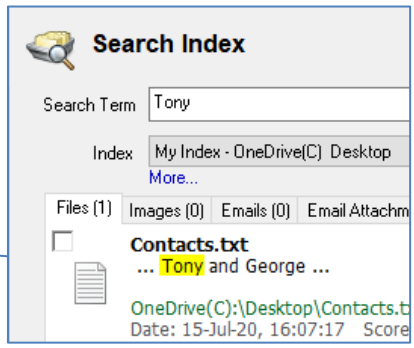
At least one file should be indexed.



Select **Search Index** from the menu bar at left.

Enter **Tony** as the search word. Click the **Search** button.

Confirm you see a match to your contacts file.



Take a screen shot for your Report.

Now we have evidence that the suspect knows Tony.

Close OSForensics.

Conclusion

Have a think and draw a conclusion about using Windows 10 data for Forensics.

Consider the amount of data stored and the use of a tool such as OSForensics in finding evidence.

Submission.

Save your document as a single pdf.

Upload your pdf using the Submit Assignment button on Canvas Week 1 tutorial.

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

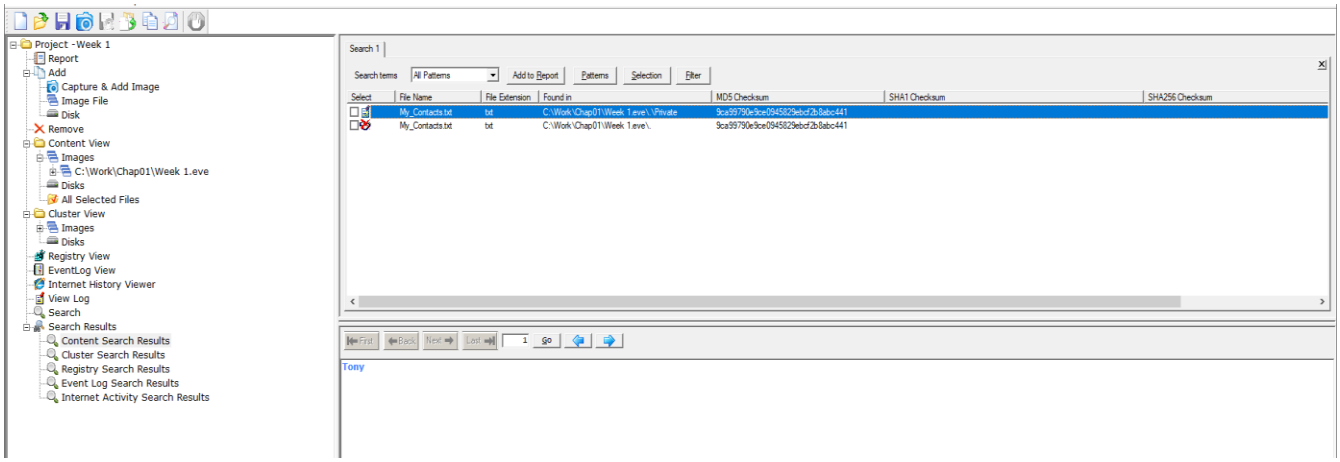
1) Search for a keyword in text files.

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.

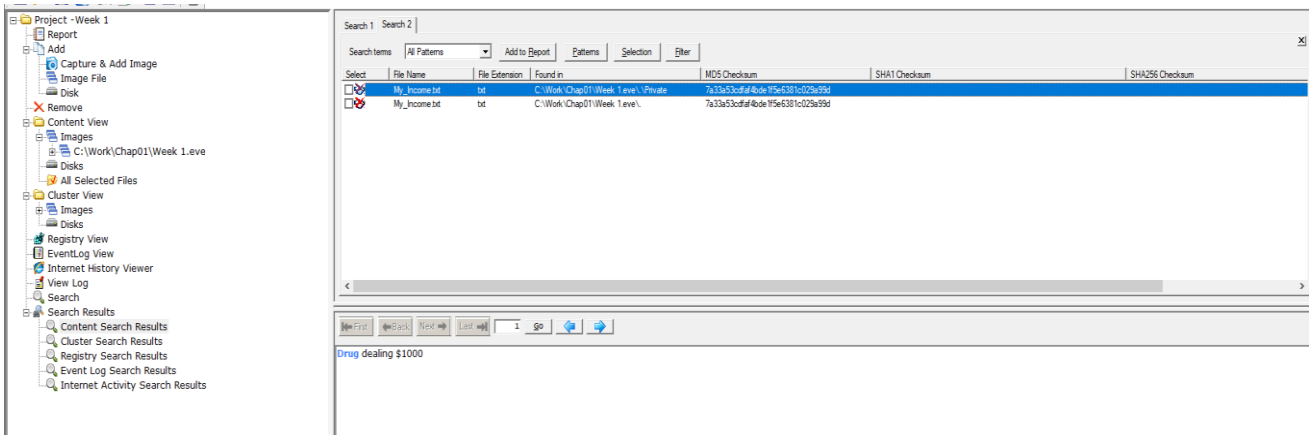
Note the red cross indicating the file has been deleted.

Click the matching file.

The matching pattern will be shown in the data area.

Insert your work area and data area screen shot here.

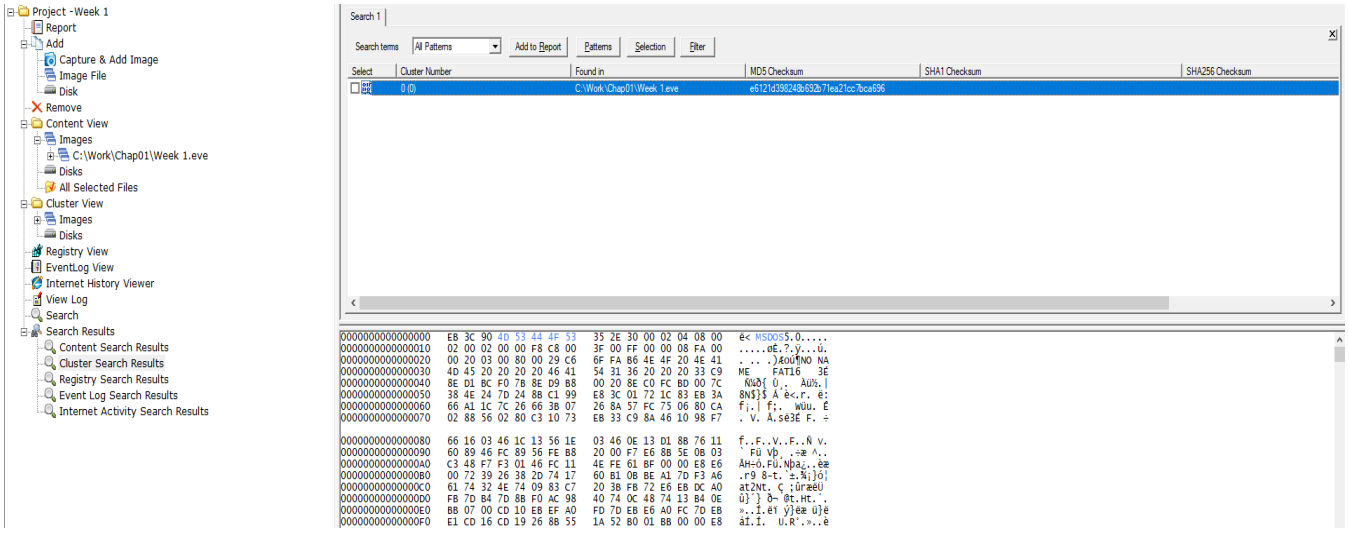
Week 02 Lab Forensics Case Report



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.

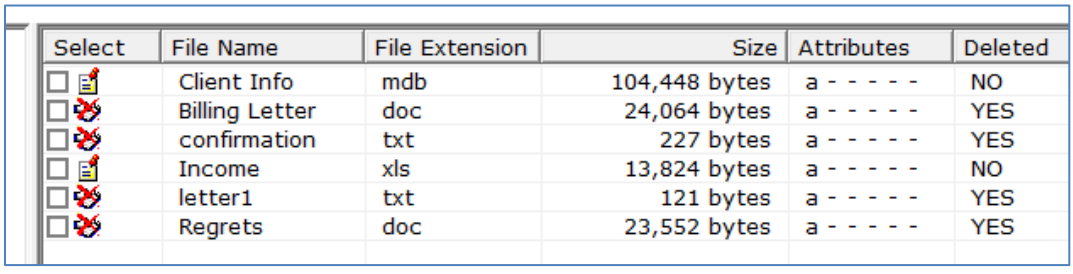
These types of FAT are file systems. FAT32, being a 32-bit file system, supports much larger disks than the FAT16 file system. Under the FAT32 file system, each partition is divided into clusters, each identified by a 32-bit number. Each cluster consists of one or smaller units, known as sectors, depending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

Q4) Advanced – Optional - Analysing an image using ProDiscover

B) Acquisition

Select Letter1.

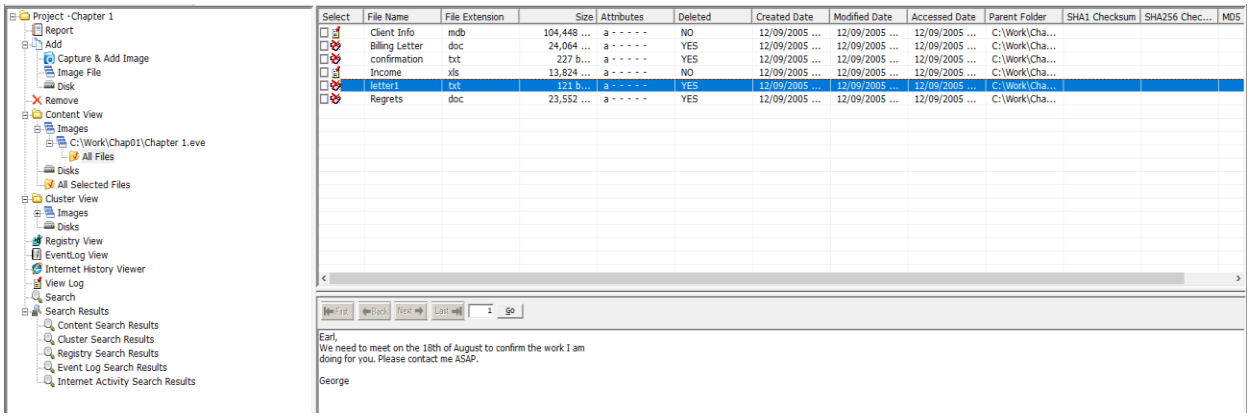
Note its contents in the data area.



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

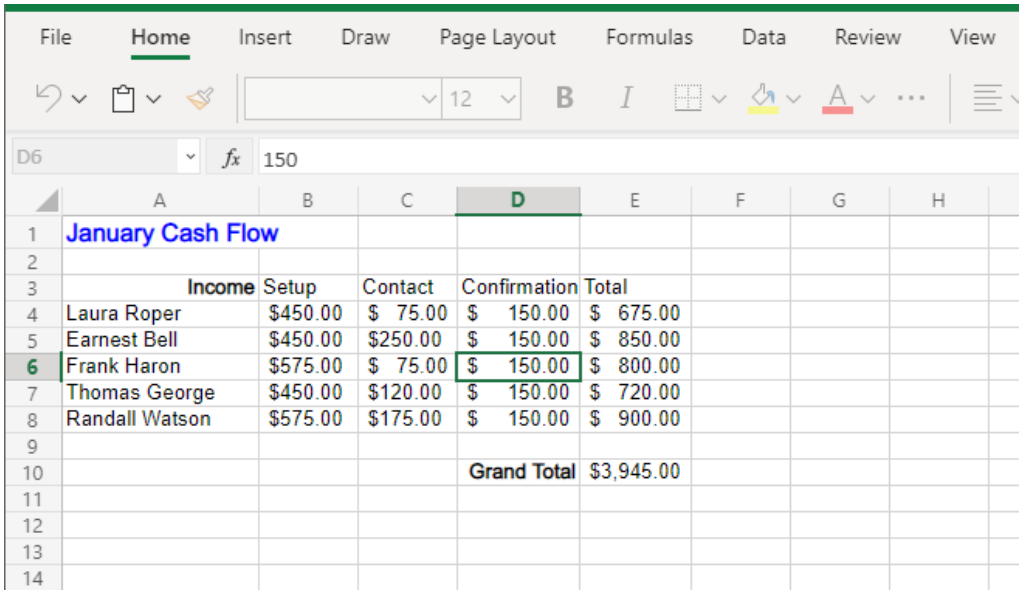
Insert your screen shot of the letter 1 contents here.

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.

48436/32309 Week 03 Browser Files Report

Upload this document as a pdf.

Name: Huynh Lam Student ID: 13264763 Date: 22/08/2021
Activity No.: Cmp1/03

Due Date:

Three days after the lab.

Q1) Chrome Cookie Files – using chrome

A) What is your **complete** chrome version number? 92.0.4515.131. Is it 32 or 64 bit? 64 bit

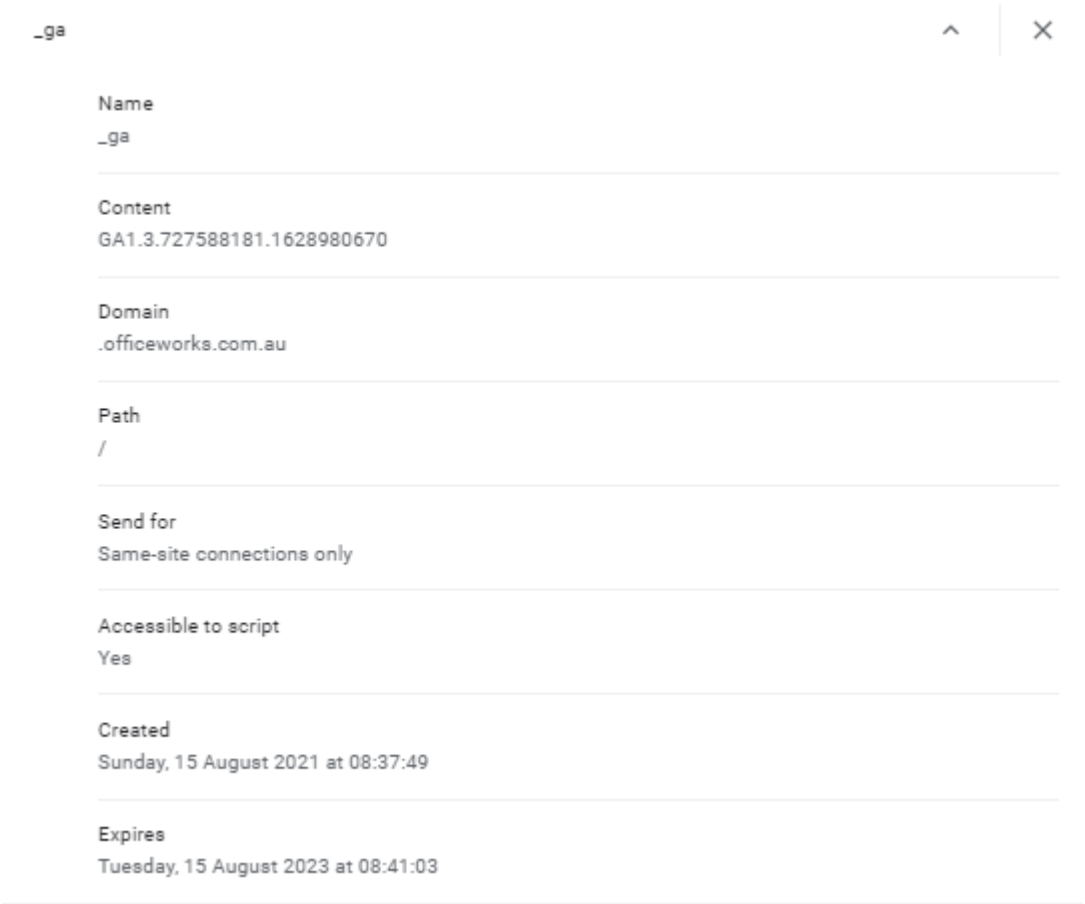
C) Note the 64GB SanDisk micro SDHC Product Code. SDSQUA464

D1) Cookie analysis 1

officeworks.com.au cookies.

What JavaScript library is dropping these cookies? analytics.jsdrops

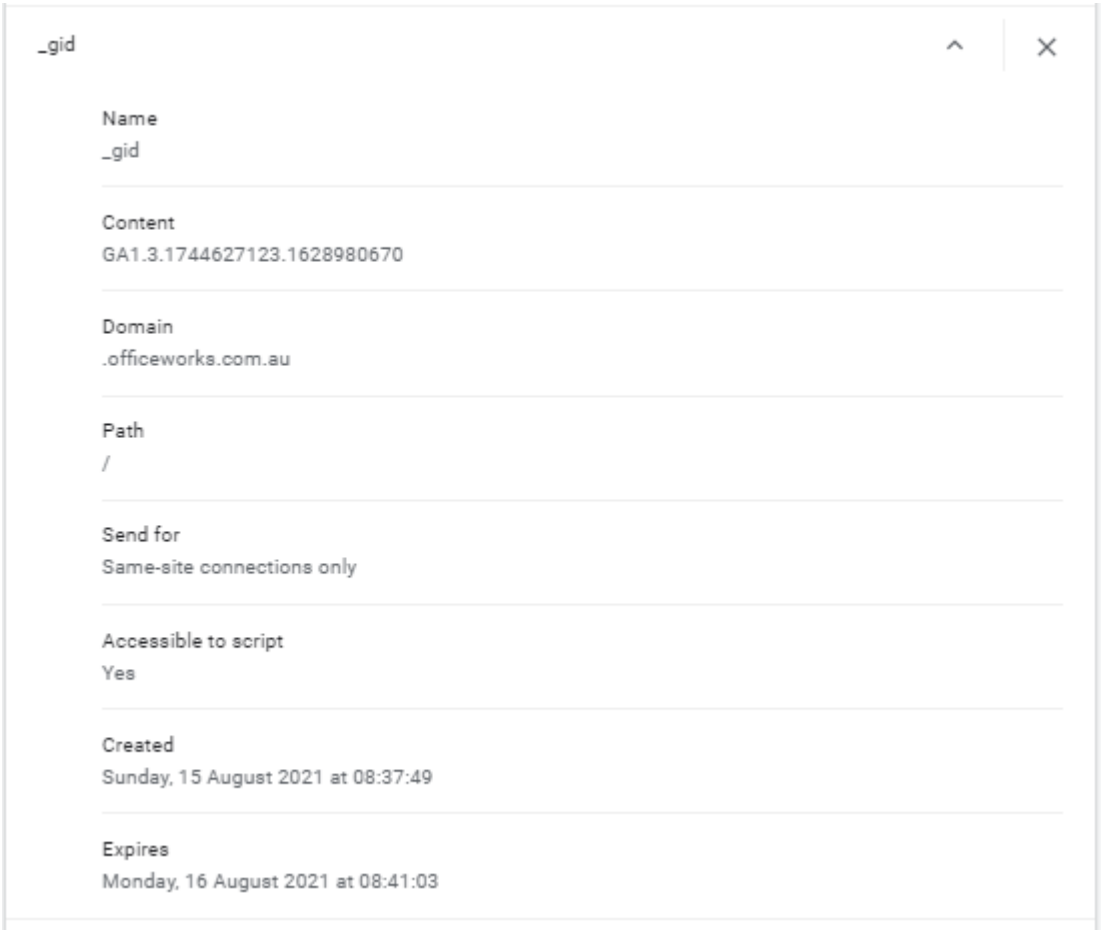
Open the _ga cookie. Take a screen shot of the Name, Content, Domain, Created and Expires.



48436/32309 Week 03 Browser Files Report

What is the cookie lifetime? Lifetime starts on 15th August 2021 08:37:49 and ends on 15th August 2023 08:41:03 (2 years)

Open the _gid cookie. Take a screen shot of the Name, Content, Domain, Created and Expires.



What is the cookie lifetime?

Lifetime starts on 15th August 2021 08:37:49 and ends on 16th August 2021 08:41:03 (1 day)

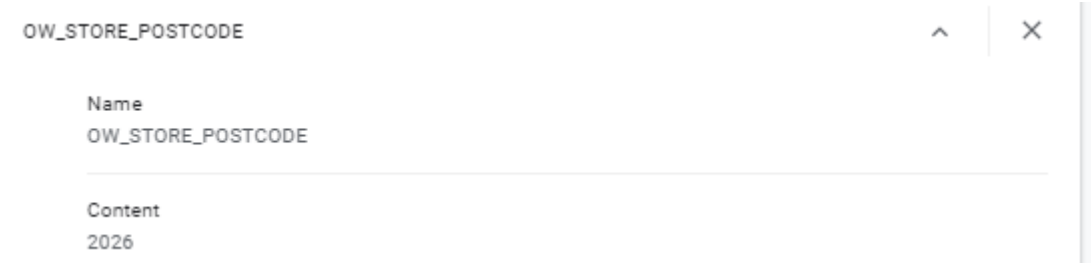
D2) Cookie analysis 2

www.officeworks.com.au cookies.

Select the OW_STORE_POSTCODE cookie.

Explain which details might be of forensic interest. The details of the content would be of forensic interest as this is where the user has set their store which gives information on the postcode of the Officeworks store. As you can see the image below this person has set their cookies to location of 2026 which corresponds to the Glebe store.

Week 03 Browser Files Report



Q2) Chrome Cookie Files – using the cmd line

Copy the Cookies file to C:\Forensics_YourName

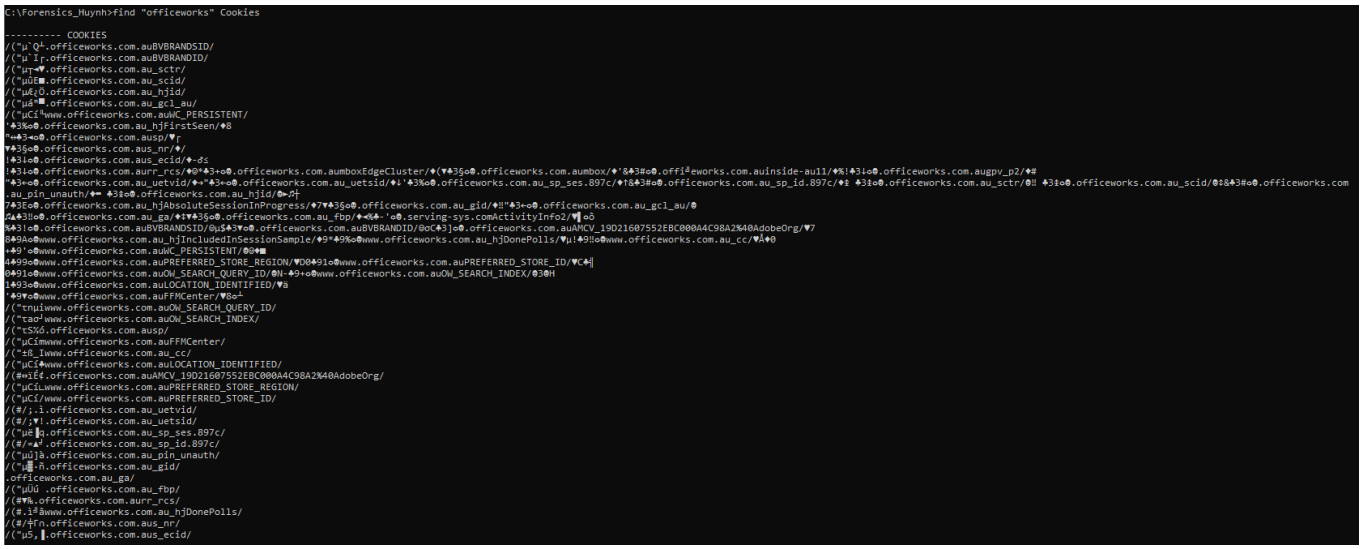
On your laptop open a cmd window and CD to your C:\forensics folder.

```
C:\Forensics_Graham>
```

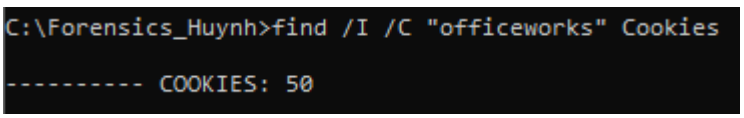
Run find on the term Officeworks in the Cookies file again, this time ignore case and count the number of hits.

Take a screen shot for your report, showing the command syntax and the count.

Command: find "officeworks" Cookies



Command: find /I /C "officeworks" Cookies



Advanced

Copy the Cookies file to your Linux desktop (WSL on Windows 10).

Open a Linux shell window.

Use the strings command to extract text from the Cookies file. Pipe this into grep and search for Officeworks.

Repeat, but this time display only the _ga cookie matches for Officeworks.

Take a screen shot for your report, showing the command syntax and the result.

Command: strings Cookies | grep "officeworks"

```
kali@kali:~/Desktop/Forensics_Huynh$ strings Cookies | grep "officeworks"
.officeworks.com.auBVBRANDSID/
.officeworks.com.auBVBRANDID/
.officeworks.com.au_sctr/
.officeworks.com.au_scid/
.officeworks.com.au_hjid/
.officeworks.com.au_gcl_au/
www.officeworks.com.auWC_PERSISTENT/
.officeworks.com.au_hjFirstSeen/
.officeworks.com.ausp/
.officeworks.com.aus_nr/
.officeworks.com.aus_ecid/
.officeworks.com.aurr_rcs/
.officeworks.com.aumboxEdgeCluster/
.officeworks.com.aumbox/
.officeworks.com.auinside-au11/
.officeworks.com.augpv_p2/
.officeworks.com.au_uetvid/
.officeworks.com.au_uetsid/
.officeworks.com.au_sp_ses.897c/
.officeworks.com.au_sp_id.897c/
.officeworks.com.au_sctr/
.officeworks.com.au_scid/
.officeworks.com.au_pin_unauth/
.officeworks.com.au_hjid/
.officeworks.com.au_hjAbsoluteSessionInProgress/
.officeworks.com.au_gid/
.officeworks.com.au_gcl_au/
.officeworks.com.au_ga/
.officeworks.com.au_fbp/
.officeworks.com.auBVBRANDSID/
.officeworks.com.auBVBRANDID/
.officeworks.com.auAMCV_19D21607552EBC000A4C98A2%40AdobeOrg/
www.officeworks.com.au_hjIncludedInSessionSample/
www.officeworks.com.au_hjDonePolls/
www.officeworks.com.au_cc/
www.officeworks.com.auWC_PERSISTENT/
www.officeworks.com.auPREFERRED_STORE_REGION/
www.officeworks.com.auPREFERRED_STORE_ID/
www.officeworks.com.auOW_SEARCH_QUERY_ID/
www.officeworks.com.auOW_SEARCH_INDEX/
www.officeworks.com.auLOCATION_IDENTIFIED/
```

Command: strings Cookies | grep "officeworks.*_ga"

```
kali@kali:~/Desktop/Forensics_Huynh$ strings Cookies | grep "officeworks.*_ga"
.officeworks.com.au_ga/
.officeworks.com.au_ga/
```

Now search the cookie file for analytics using strings then grep.

Command: strings Cookies | grep"analytics"

```
kali@kali:~/Desktop/Forensics_Huynh$ strings Cookies | grep "analytics"
.analytics.yahoo.comIDSYNC/
.analytics.yahoo.comIDSYNC/
```

What analytics website (if any) did you find? There are analytics from There is analytics from yahoo which is Yahoo's tracker.

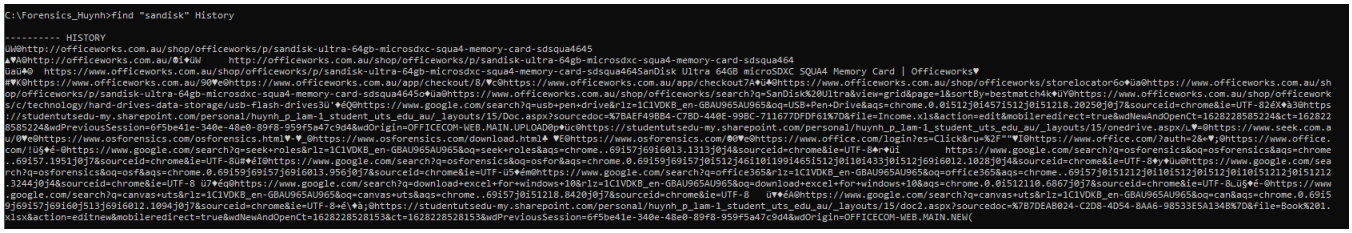
Q3) Chrome history

Copy the History file to C:\Forensics_YourName

Use find to confirm your search for "sandisk"

Take a screen shot for your report.

Command: find "sandisk" history



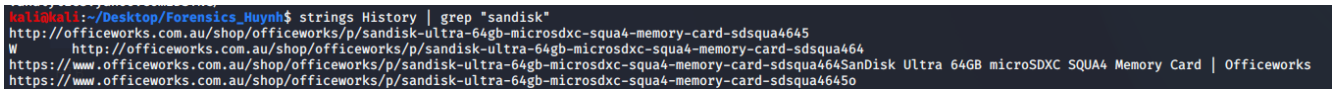
Q3b) Advanced

Copy the History file to your Linux desktop.

Use strings to extract the text and grep to search for 'sandisk'.

Take a screenshot for your report.

Command: strings History | grep "sandisk"



48436/32309 Week 03 Browser Files Report

Q4) Fingerprinting

Note here your Chrome Browser version __ (see Q1)

4A) BrowserLeaks

Using your Laptop, open the Browserleaks website in Chrome.

a) Perform Ip Address detection.
What is your public ip address? 1.40.13.119

What is your AS Number? AS4804

What does ASN mean? Autonomous System Number (ASN) is a globally unique identifier that defines a group of one or more IP prefixes run by one or more network operators that maintain a single, clearly defined routing policy. These groups of IP prefixes are known as autonomous systems

Note TCP/IP Fingerprinting.
What is your OS? Windows (NT kernel)

Where is your IP? Blacktown

What is your _ga cookie date code? 1628983984 What is your _ga date? Your time zone: Sunday, August 15, 2021 9:33:04 AM GMT+10:00

b) Return to the Home Page. Perform Canvas Fingerprinting

Include the probability ratios in your answers.

What is your OS platform and version? Windows 3145/3252, Windows 10 2972/3252

What is your chrome browser version? Chromium 1910/3252

Comment on how accurate is BrowserLeaks in determining your fingerprint. BrowserLeaks is quite accurate in guessing the Operating system/version running and as well as the browser version which they don't have a specific option but the other category is accurate for my version. Their ratio rating for the OS seems very accurate, while the browser ratios are a bit far off each other.

4B) Panopticlick

Using your Laptop, open the Panopticlick website in Chrome.

Click the TEST YOUR BROWSER button.

List any tests your browser passed. Protecting you from fingerprinting, Your browser has a unique fingerprint

Click Show full results.

What is your OS platform and Version? Windows NT 10.0; Win64; x64

What is your Chrome browser Version? Chrome/92.0.4515.131

48436/32309

Week 03 Browser Files Report

What is your Time zone? TIME ZONE: Australia/Sydney

Comment on how accurate is Panopticlick in determining your fingerprint. Panopticlick accuracy is much higher than browser leaks. This is only based on the fact they have guessed my Operating system and exact browser version. There are no ratio checks shown, but has a more accurate output than browser leaks.

Upload Save this report as a pdf and upload.

48436/32309 Week 04 Network Packets and Wireshark Report

Upload this document as a pdf.

Name: Huynh Lam Student ID: 13264763 Date: 28/08/2021
Activity No.: Cmp1/03

Due Date:

Three days after the lab.

Q1) Web Server Forensics

A) See what Builtwith.com does in the Lecture slides week 3.

Run Builtwith against the Officeworks website.

Name two Analytics and Tracking tools detected that have usage that is still growing strongly (has not peaked).

- Adobe Dynamic Tag Management Usage Statistics
- LinkedIn Insights Usage Statistics

Two Content Delivery platforms are Akamai and CloudFront. Compare and contrast these two platforms.

Describe any growth peaks.

- Both companies have a declining graph after hitting their peeks. However, CloudFront had a bit more stable decline than Akamai which had 2 declines. CloudFront revenue is performing better than Akamai and in Australia, CloudFront is the 5th most popular in content delivery platforms

A Content Management System used is Atlassian Cloud. What do you know about Atlassian?

- Atlassian is one of the big leading technology companies in Australia and their cloud usage statistics have been soaring.

B) See what w3techs.com does in the Lecture slides week 3.

Run w3techs against the Officeworks website. (Click the Sites Tab.)

What is the Server side programming language used? PHP

What is the Client side programming language used? JavaScript

What is the Web Server engine? Nginx

48436/32309 Week 04 Network Packets and Wireshark Report

Who hosts this website? Amazon

C) IP details for Officeworks.

What is the IPv4 address? 13.239.126.216 or 52.65.120.234 What cmd line tool did you use? nslookup

Who owns this address? Amazon Technologies What website did you use? https://dnschecker.org/ip-whois-lookup.php

Where is it located?

Address: 410 Terry Ave N.

City: Seattle

StateProv: WA

PostalCode: 98109

Country: US

Q2) DNS

Find a website that displays public dns servers in Australia.

https://public-dns.info/nameserver/au.html

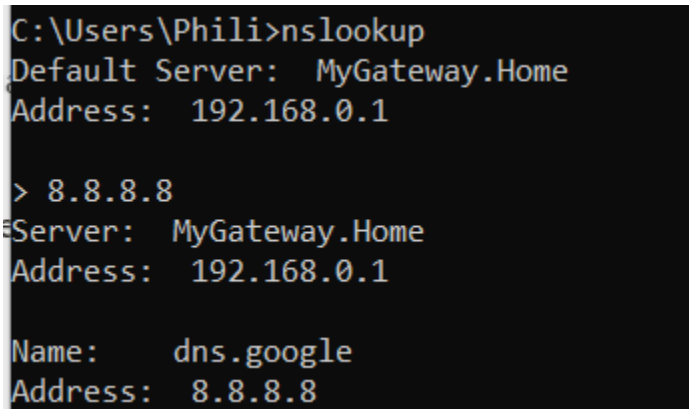
List here two public dns servers supplied by ISPs in the state of NSW.

List the owner, ip address, suburb and AS number.

- Mammoth Media Pty Ltd, 43.229.62.192, Macquarie Park, 133159
- TEFINCOM S.A, 103.86.96.100, Sydney, 136787

8.8.8.8 is the dns for Google. Show here a cmd line lookup tool to name this IP.

48436/32309 Week 04 Network Packets and Wireshark Report



What is the registered name of 8.8.8.8? dns.google

List two more dns with single digit IP addresses. List their registered name and the IPv4 number.

- 1.1.1.1 CloudFlareNet
- 1.0.0.3 CloudFlareNet

Q3) Network cookie collection

Here we will use Wireshark to capture evidence of a suspect visiting a website.

Part 1: Setup

Clear cookies, Set Cookies, Collect cookies. Do all this.

Part 2: Acquisition

In Wireshark, select File, Save As and save the capture as **Officeworks_yourname** of type **pcapng** into this C:\Forensics_yourname folder.

Part 3: Viewing Website visits with Wireshark

Open your saved Wireshark session, **Officeworks_yourname.pcapng**.

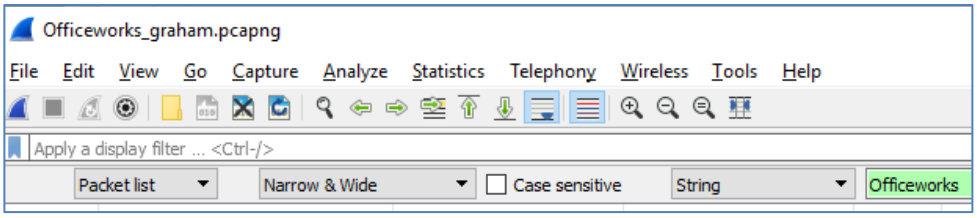
From the menu, select View, Time Display Format. Select Date and Time of Day.

Now search for the visit to the Officeworks web server. From the menu, click Edit, Find Packet.

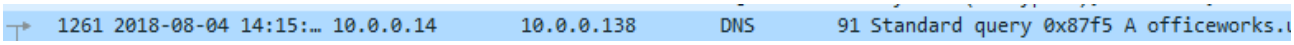
48436/32309 # Week 04 Network Packets and Wireshark Report

Select String and Packet List.

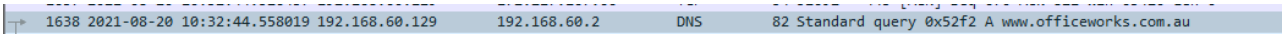
A) Search for the string **Officeworks**.



Select the matching packet in the Packet list window pane. (Arrow at left.).



Take a screenshot for your report. Include the date and time and the matching text.. (yours will be different.)

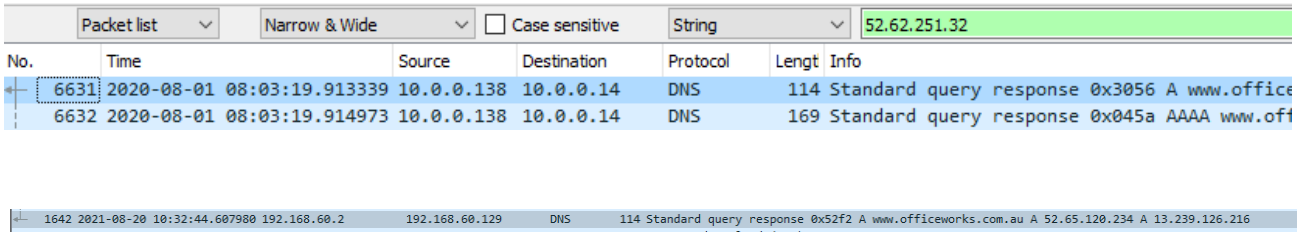


B) In your cmd window, use the nslookup tool to find the ipv4 address for officeworks.com.au

Name: officeworks.com.au Address: 52.62.251.32 or similar.

Locate the first packet with this ip address. (Search from the start).

Take a screenshot for your report. Include the display filter, packet number, date and time, destination address and info. (yours will be different.)



What is the packet TCP/IP protocol? DNS

C) Tracking cookies. (refer to Q1A)

We want to find the IPv4 address of the tracking cookie used. We will filter the packets by dns to remove unwanted packets (noise.)

Enter dns as the display filter top left. Click the find arrow top right. Confirm you only see dns packets.

Use a Packet list String search to find the dns type A request for the following Analytics and Tracking (A&T) tools . Search from the top each time.

Expand the packet detail window. Expand the dns request. Click the link to see the dns response.

Include the packet number and the IPv4 address. One address each is sufficient. (If the response is static write static with the ip address returned.)

- Hotjar Packet Number: 5764 static: 99.86.212.40
- Bazaarvoice Packet Number: 7663 Address: 13.226.107.40
  Find two more A&T cookies.
- EveresTech Packet Number: 2739 Address 13.229.0.102
- Inside-graph Packet Number: 3816 Address: 104.18.30.173

Can you find evidence of a Content Delivery Network (CDN) hosting? Yes

If so which? Akamai

Can you find evidence of A Content Management System (CMS) cookie? Yes

If so which? Contentful

Would you still see these cookies in wireshark while using the Incognito browser?

Yes, because incognito mode only removes the activity's history traces rather than deleting incoming and outgoing traffic.

Close Wireshark.

Q4) Tcpdump filters

Check your interfaces with windump -D

a) Run windump with the right interface and confirm you see packets.

b) Set the filter to **capture only icmp** and then in another window, ping your gateway.

Take a screen shot of the 8 icmp packets for your report. You may have to extend your command window to stop word wrap.

```
C:\Forensics_Huynh>windump -i1 icmp
windump: listening on \Device\NPF_{D72799D2-FCDF-4FB3-AD41-CD5FA3A4BF2A}
11:28:27.153630 IP DESKTOP-LD37IOO.localdomain > 192.168.60.2: ICMP echo request, id 1, seq 5, length 40
11:28:27.153887 IP 192.168.60.2 > DESKTOP-LD37IOO.localdomain: ICMP echo reply, id 1, seq 5, length 40
11:28:28.174887 IP DESKTOP-LD37IOO.localdomain > 192.168.60.2: ICMP echo request, id 1, seq 6, length 40
11:28:28.175502 IP 192.168.60.2 > DESKTOP-LD37IOO.localdomain: ICMP echo reply, id 1, seq 6, length 40
11:28:29.219872 IP DESKTOP-LD37IOO.localdomain > 192.168.60.2: ICMP echo request, id 1, seq 7, length 40
11:28:29.220481 IP 192.168.60.2 > DESKTOP-LD37IOO.localdomain: ICMP echo reply, id 1, seq 7, length 40
11:28:30.252258 IP DESKTOP-LD37IOO.localdomain > 192.168.60.2: ICMP echo request, id 1, seq 8, length 40
11:28:30.252810 IP 192.168.60.2 > DESKTOP-LD37IOO.localdomain: ICMP echo reply, id 1, seq 8, length 40
```

c) Set the filter to **capture dns**.

We want to prove or deny if the suspect searched for or was referred to Officeworks, so we capture 20 packets to see where the browser goes.

Now open a browser and go to Officeworks.com.au

Take a screen shot of the Officeworks dns packets for your report. Yours will be different.

```
C:\Forensics_Huynh>windump -i1 -n -c20 udp port 53
windump: listening on \Device\NPF_{D72799D2-FCDF-4FB3-AD41-CD5FA3A4BF2A}
11:31:41.168091 IP 192.168.60.129.52920 > 192.168.60.2.53:  51240+ A? officeworks.com.au. (36)
11:31:41.196272 IP 192.168.60.2.53 > 192.168.60.129.52920:  51240 2/0/0 A 13.239.126.216, (68)
11:31:41.344713 IP 192.168.60.129.55678 > 192.168.60.2.53:  56433+ A? www.officeworks.com.au. (40)
11:31:41.360522 IP 192.168.60.2.53 > 192.168.60.129.55678:  56433 2/0/0 A[|domain]
11:31:41.523470 IP 192.168.60.129.59967 > 192.168.60.2.53:  22715+ A? cdnjs.cloudflare.com. (38)
11:31:41.543858 IP 192.168.60.2.53 > 192.168.60.129.59967:  22715 2/0/0 A 104.16.18.94[|domain]
11:31:41.597410 IP 192.168.60.129.53568 > 192.168.60.2.53:  48300+ A? images.officeworks.com.au. (43)
11:31:41.614684 IP 192.168.60.2.53 > 192.168.60.129.53568:  48300 2/0/0[|domain]
11:31:41.632579 IP 192.168.60.129.55924 > 192.168.60.2.53:  56177+ A? polyfill.io. (29)
11:31:41.651381 IP 192.168.60.2.53 > 192.168.60.129.55924:  56177 4/0/0 A 151.101.1.26,[|domain]
11:31:41.889196 IP 192.168.60.129.61417 > 192.168.60.2.53:  30592+ A? images.ctfassets.net. (38)
11:31:41.935747 IP 192.168.60.2.53 > 192.168.60.129.61417:  30592 6/0/0 CNAME[|domain]
11:31:42.454635 IP 192.168.60.129.64959 > 192.168.60.2.53:  15451+ A? content-autofill.googleapis.com. (49)
11:31:42.475377 IP 192.168.60.2.53 > 192.168.60.129.64959:  15451 1/0/0 (65)
11:31:42.942937 IP 192.168.60.129.61331 > 192.168.60.2.53:  41085+ A? officeworks.tt.omtrdc.net. (43)
11:31:42.959564 IP 192.168.60.2.53 > 192.168.60.129.61331:  41085 4/0/0[|domain]
11:31:43.343640 IP 192.168.60.129.57456 > 192.168.60.2.53:  29637+ A? mboxedge36.tt.omtrdc.net. (42)
11:31:43.364034 IP 192.168.60.2.53 > 192.168.60.129.57456:  29637 4/0/0 A[|domain]
11:31:43.693017 IP 192.168.60.129.52606 > 192.168.60.2.53:  58524+ A? au11-tracker.inside-graph.com. (47)
11:31:43.716480 IP 192.168.60.2.53 > 192.168.60.129.52606:  58524 3/0/0[|domain]
20 packets captured
2173 packets received by filter
0 packets dropped by kernel
```

Explain the extra websites in the list.

- The Cloudflare website is a free and open-source CDN service which make it faster and easier to load library files on your websites
- polyfill.io is a piece of code (usually JavaScript on the Web) used to provide modern functionality on older browsers that do not natively support it.
- mboxedge36tt.omtrdc.net marketing box, which is an area on a web page used by Adobe Target to show different content to visitors in a campaign.
- au11-tracker.inside-graph.com is a tracking tool

--------- ----------

Q5) whois

Explain the command line.

- whois: WHOIS is a query and response protocol that is widely used for querying databases that store the registered users of an Internet resource, such as a domain name or an IP address block
- curl: CURL is a command-line tool to transfer data to or from a server, using any of the supported protocols (HTTP, FTP, IMAP, POP3, SCP, SFTP, SMTP, TFTP, TELNET, LDAP or FILE)
- ifconfig.me/ip: ifconfig.me is a web service that displays information about your connection, including your public IP address, hostname and User-Agent string

48436/32309 # Week 04 Network Packets and Wireshark Report

When combining the commands (curl -s ifconfig.me/ip) together they will get your remote return your remote IP address and Host as seen by other users online. An addition of whois before this command will search and identify who owns a domain of the IP address and how to get in contact with them.

What is the return ip address of ifconfig.me/ip?

This returns my public IP address which is 1.40.13.119

Upload

Upload your report as a pdf.

Week 05 Metadata Report

Name: Huynh Lam **Student ID: 13264763** **Date: 05/09/2021**
Activity No.: Cmp1/03

Due Date: Three days after the lab.

Setup

You need to download this week's samples onto a Linux Box.

Q1) Hex Viewer – cmd line

We can use xxd -l 256 to see the file signatures.

Note your response in the table →

File	Hex Signature	exe PE Jump address
Trade_secrets.txt	Ascii text	
logo.gif	GIF89a at 00	
MS Office Meta Data.jpg	(JFIF) FFD8 FF	
IMAG1672a.jpg	(JFIF) FFD8 FF	
Cygwin1.dll	(MZ) 4d5a	
Strings.exe	(MZ) 4d5a	D8
Sample.docs	(PK) 504B 0304	
Sample.pdf	(%PDF) 2550 4446	
Flowers.txt	(MZ) 4d5a	80
Cars.txt	(MZ) 4d5a	D8

Can you determine the imposters file type?

- Flowers.txt should be exe
- cars.txt should be exe

Exe files have a PE jump between 80 and FF see slides. Add to the table.(exe only)

Why does the address of the PE marker vary?

- These files are referred to as Portable Executable PE. The name Portable Executable refers to the fact that the format is not architecture specific which means the address of PE being in a different spot is normal

Q2) Magic Files

We use Linux command file on your downloaded files.

Open a Linux shell window and cd to your Forensics folder.

Use the command file to check the file extensions.

file /mnt/c/Forensics_yourname * | cut -c 1-120

Add the responses in the table

Are any files imposters as seen by file?

Imposters: Cars and flowers text files are exe files

Run file again on ls2.exe without using cut.

File	Magic Signature
Trade_secrets.txt	iso-8859 (simple) text, CRLF
logo.gif	version 89a, 220 x 50 pixels
MS Office Meta Data.jpg	JPEG image data, JFIF standard 1.01, resolution (DPI)
IMAG1672a.jpg	JPEG image data, JFIF standard 1.01, resolution (DPI)
cygwin1.dll	PE32 executable (DLL) (console) Intel 80386, for MS Windows
strings.exe	PE32 executable (console) Intel 80386, for MS Windows
Sample.docs	Microsoft Word 2007+
Sample.pdf	PDF document, version 1.5
Flowers.txt	PE32 executable (DLL) (console) Intel 80386, for MS Windows
cars.txt	PE32 executable (console) Intel 80386, for MS Windows

ls2.exe is a compressed form of ls.exe using UPX packing to avoid detection in an IDS.

You can also use xxd on ls2.exe and grep for UPX. Take a screenshot of this cmd and the result.

```
huynh@DESKTOP-LD37IOO:/mnt/c/Forensics_Huynh/Week 05 Samples$ file ls2.exe
ls2.exe: PE32 executable (console) Intel 80386 (stripped to external PDB), for MS Windows, UPX compressed
huynh@DESKTOP-LD37IOO:/mnt/c/Forensics_Huynh/Week 05 Samples$ xxd ls2.exe | grep "UPX"
00000170: 0000 0000 0000 0000 5550 5830 0000 0000  ........UPX0....
000001a0: 5550 5831 0000 0000 00f0 0000 0080 0100  UPX1............
000001c0: 0000 0000 4000 00e0 5550 5832 0000 0000  ....@...UPX2....
000001f0: 332e 3037 0055 5058 210d 0902 08ad f56c  3.07.UPX!......l
huynh@DESKTOP-LD37IOO:/mnt/c/Forensics_Huynh/Week 05 Samples$
```

What is UPX packing?

- UPX (Ultimate Packer for Executables) is an open-source executable packer supporting a number of file formats from different operating systems.
- By packing malware binary files, the data stored within the file becomes unreadable and thus will need to be unpacked in order to become readable again. These require the malware to be unpacked manually

Q3) Editing a File Header

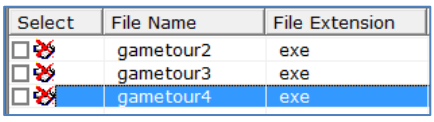
Confirm you have the Image File C08InChp.dd in your Forensics folder.

Run ProDiscover.

Add Image File C08InChp.dd.

Search for FIF case sensitive

Click Show File. You should see a deleted file called gametour4.exe.



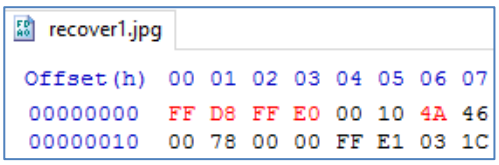
Right click, select copy file, save as Recover1.jpg in your Forensics folder. Exit ProDiscover.

Run HxD.exe in your Forensics folder. (Download and Install HXD as required,)

Open Recover1.jpg

Change the header from 7A 7A 7A 7A to FF D8 FF E0 (see lecture slides).

Change the 7A at address 06 to 4A.



Does the image support the allegation?

- If the image is part of the bike next model that has not been released by the company, then the image does support the allegation otherwise there would be more evidence needed

Q4) File Metadata

Confirm you have downloaded the sample files as in Q1.

Q4 A) docx files

Use the Windows 10 File Explorer.

Right click **Sample.docx** and select properties. Select the details tab.

Note the metadata.

What is the Document Title? Forensic Sample

What is the Document Subject? Forensic

What are the Document Tags? Forensics, Metadata

Who is the Author? G G Lee

When was it last printed? 9/29/2013 4:36 PM

Q4 B) pdf files

Open Sample.pdf with a pdf reader such as pdf-XChange or Chrome. Select the File Tab.

https://www.tracker-software.com/product/pdf-xchange-editor

Check the Document Properties.

Note here data of forensic interest:

List the tag:value pairs of forensic interest and explain what they mean.

The Title Forensic Sample (Title of the PDF Document)

The Keywords Forensics, Metadata (Keywords to specify what the topic is)

The Author G G Lee (The owner or author of this document)

The program that generated the pdf. Microsoft Word 2021 (This is the original program before it was a PDF)

The date last modified 29/09/2013, 16:36:31 (file was last 'Saved' by an application (whether or not its contents were actually modified/changed)

(This is usually the same as the file modify date.)

The PDF Version 1.5 (Version of the PDF)

Q4 C) Changing file dates

You need the Linux Box you used in Q1 again.

Open your Terminal shell and cd to the folder containing your sample files.

Let us now **stat** Sample.pdf

stat Sample.pdf

Note here the file modify date Modify: 2021-08-25 17:38:01.418284500 +1000

Does it match the Meta data date above? No

Now **touch** the modify date.

touch –m Sample.pdf

Use stat to check the modify date is now today Modify: 2021-08-25 18:43:11.042835400 +1000

Does the File modify date still match the pdf metadata date as seen by pdfinfo?

__ The file modify date has changed in Linux WSL, but the pdf properties have stayed the same

D) Exif files

Use the Windows 10 File Explorer to select IMAG1762a.jpg.

Look at the image file properties.

Explain the several dates.

- Date taken is when the photo was taken
- Date created should be the date that a particular physical instance of a file was written to disk
- Date modified should only ever be the date that the file was last 'Saved' by an application (whether or not its contents were actually modified/changed)

What is the camera? HTC Sensation Z710a

Where was the photo taken? Balmoral, Mosman NSW 2088

Explain how you decoded the GPS coordinates.

- Using this link I was able to find the location
- [https://support.google.com/maps/answer/18539?hl=en&co=GENIE.Platform%3DDesktop]
- GPS Latitude: 33°49' 37.86 S
- GPS Longitude: 151°15' 7.42 E

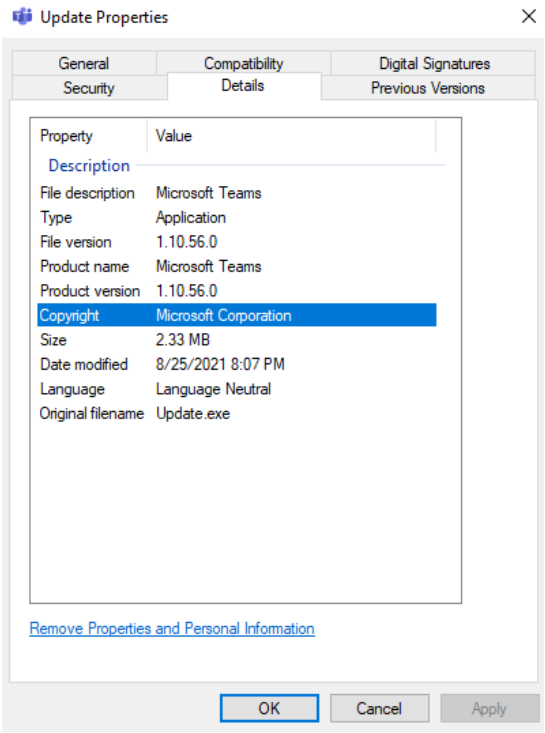
E) Other Metadata Samples

Find more files with interesting metadata. (Email? Photos?)

Describe the file and it's metadata of forensic interest.

Chosen to do Microsoft Teams

- Microsoft teams exe file is an automatic update file when the shortcut is ran
- This has the product detail such as name and version
- Company details which are Microsoft Corporation
- Date modified would be the date that it was installed



Q5) Hashing.

Run Ubuntu on Windows 10. Then cd to /mnt/c/Forensics_yourname.

Week 05 Metadata Report

Create a text file called test with contents "I will pay you \$1000" using echo. Note the back slash. Check with cat test.

Create a second file called test1 with contents "I will pay you \$9000" using echo.

Compare the two file lengths with ls -al

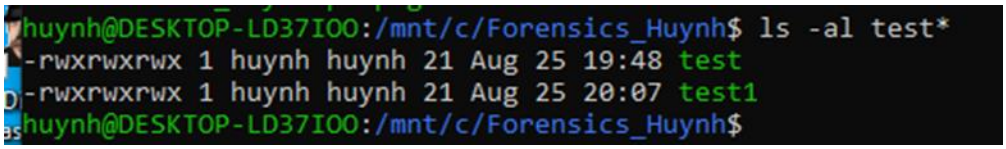
Hash both files with md5 and then sha 256.

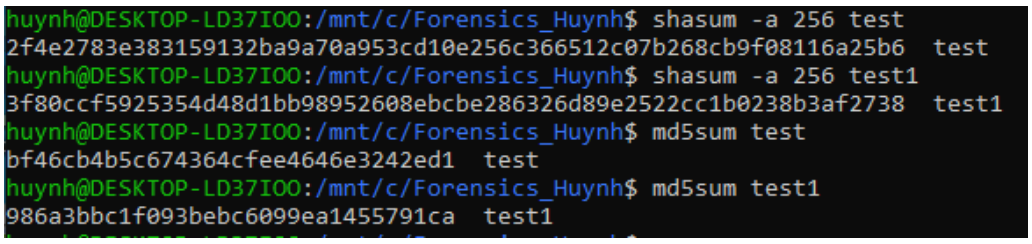
Compare the two md5 hash lengths and compare the two sha 256 hash lengths.

- md5:
  - Test: bf46cb4b5c674364cfee4646e3242ed1
  - Test1: 986a3bbc1f093bebc6099ea1455791ca
- SHA256:
  - Test: 2f4e2783e383159132ba9a70a953cd10e256c366512c07b268cb9f08116a25b6
  - Test2: 3f80ccf5925354d48d1bb98952608ebcbe286326d89e2522cc1b0238b3af2738

Compare the hashes of the two files. The hash length for both hashes is respectively the same number of characters. However, MD5 results in an output of 128 bits whereas SHA256 results output of 256 bits.

Take a screen shot showing the two file lengths, the two MD5 hashes and the two SHA 256 hashes.





Comment on the results as follows:.

- What is the change in file length as seen by ls? There is no change in the file length
- How does MD5 output differ from SHA 256? MD5 results in an output of 128 bits whereas SHA256 results output of 256 bits.
- What is the change in the hash lengths of the two files?
  - SHA256 has 64 characters and is 256 bits
  - MD5 has and is 32 characters 128 bits
- What is the change in the hash values of the two files? Both hashes are alphanumeric characters and have their own respective order which are different to each other
- How good is hashing in protecting a file integrity? Hash values are also useful for verifying the integrity of data. Hashing is useful in verifying the actual integrity of a

file to prevent anybody from changing the content of a file or corrupting it and passing it off as the original file.

- How can you fool hashing? There is a chance that 2 files can output the same hash number. This is very unlikely, but it is called a hash collision. Since a hash function gets us a small number for a big key, there is the possibility that two keys result in the same value.

Explain the 512 and 224 options for SHA 2. These are different hash functions. SHA-512 novel hash functions computed with 64-bit words. SHA-224 are truncated versions of SHA-512. SHA-512/224 is a method for generating initial values for truncated versions of SHA-512. The 2 functions produce the digest of a message, respectively 512 and 224 bits long

What was SHA 3 originally called? Keccak

Is SHA 3 better than SHA 2? In terms of collision potential SHA-3 is better and stronger than SHA-2 since SHA-3 uses more bits

Try this command openssl speed sha256 sha512 What does it show you?

```
huynh@DESKTOP-LD37IOO:/mnt/c/Forensics_Huynh$ openssl speed sha256 sha512
Doing sha256 for 3s on 16 size blocks: 6209863 sha256's in 3.02s
Doing sha256 for 3s on 64 size blocks: 3458342 sha256's in 2.98s
Doing sha256 for 3s on 256 size blocks: 1614439 sha256's in 2.99s
Doing sha256 for 3s on 1024 size blocks: 500173 sha256's in 3.00s
Doing sha256 for 3s on 8192 size blocks: 67417 sha256's in 3.00s
Doing sha256 for 3s on 16384 size blocks: 34454 sha256's in 3.01s
Doing sha512 for 3s on 16 size blocks: 4306907 sha512's in 3.00s
Doing sha512 for 3s on 64 size blocks: 4298864 sha512's in 3.00s
Doing sha512 for 3s on 256 size blocks: 1857715 sha512's in 3.00s
Doing sha512 for 3s on 1024 size blocks: 686953 sha512's in 3.00s
Doing sha512 for 3s on 8192 size blocks: 93469 sha512's in 2.86s
Doing sha512 for 3s on 16384 size blocks: 48735 sha512's in 2.95s
```

type	16 bytes	64 bytes	256 bytes	1024 bytes	8192 bytes	16384 bytes
sha256	32899.94k	74273.12k	138226.22k	170725.72k	184093.35k	187539.65k
sha512	22970.17k	91709.10k	158525.01k	234479.96k	267726.59k	270669.23k

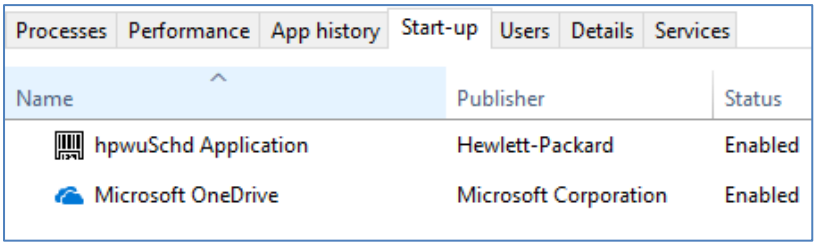
The OpenSSL Speed command shows us the speed output for these algorithms. As you can see we move up the input block size the speed for SHA-3 processes much faster than SHA-2. With a smaller string sizes SHA-2 still performs faster.

Name: Huynh Lam Student ID: 13264763 Date: 11/09/2021
Activity No.: Cmp1/03
Due Date: Three days after the lab.

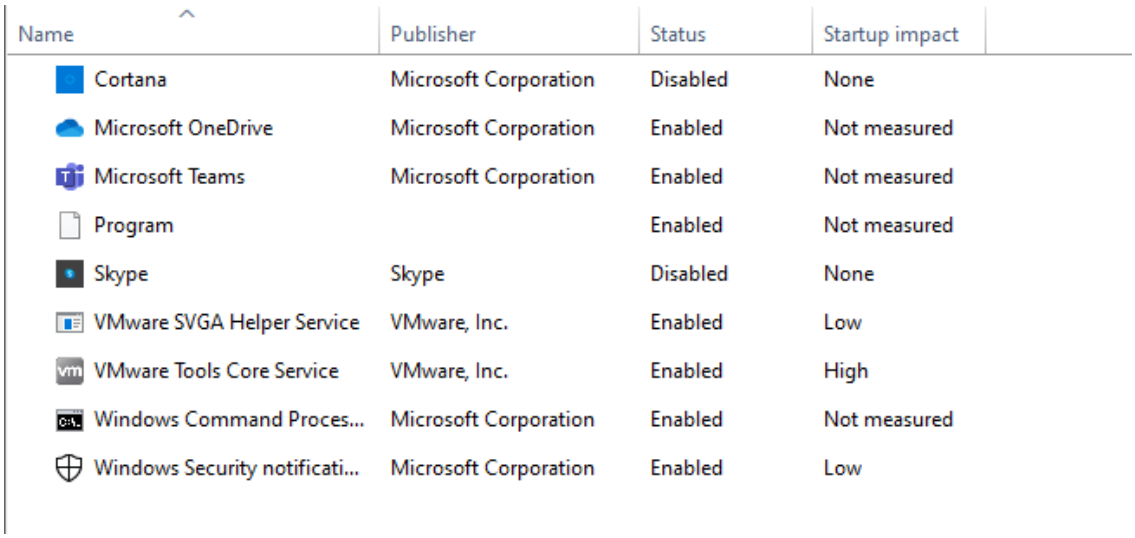
Q1) Registry Startup items - Windows

To find all startup programs, use Task Manager.

Select the Startup tab.



Take a screen shot for your report. Explain each entry.



Name	Publisher	Status	Startup impact
Cortana	Microsoft Corporation	Disabled	None
Microsoft OneDrive	Microsoft Corporation	Enabled	Not measured
Microsoft Teams	Microsoft Corporation	Enabled	Not measured
Program		Enabled	Not measured
Skype	Skype	Disabled	None
VMware SVGA Helper Service	VMware, Inc.	Enabled	Low
VMware Tools Core Service	VMware, Inc.	Enabled	High
Windows Command Proces...	Microsoft Corporation	Enabled	Not measured
Windows Security notificati...	Microsoft Corporation	Enabled	Low

- Cortana is Windows virtual assistant that is able to perform tasks or assist the user with inquiries
- Microsoft OneDrive is is a file hosting service and synchronisation service operated by Microsoft as part of its web version of Office
- Microsoft Teams proprietary business communication platform developed by Microsoft
- Program is was a Microsoft Teams program startup, but since I had to uninstall and reinstall the startup entry is still left
- Skype is a proprietary telecommunications application that specialises in providing VoIP-based videotelephony, videoconferencing and voice calls

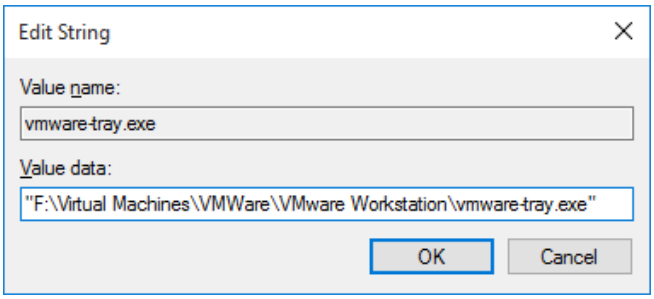
- VMware SVGA Helper Service is a virtual SVGA driver replaces the default VGA driver, which allows for only 640 X 480 resolution and 16-color graphics
- VMware Tools Core Service free set of drivers and utilities that enhances both the performance of a virtual machine's guest operating system and interaction between the guest and the host
- Windows Command Processor is the default command-line interpreter for the Microsoft Windows operating systems.
- Windows Security Notifications to provide notifications about the health and security of the machine

(In a VM you may not see much as these services apply to the host OS.)

Use the Windows Start icon to open regedit. Navigate to:

HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run

Select the first key name. (Exclude the default) Right click and select modify.

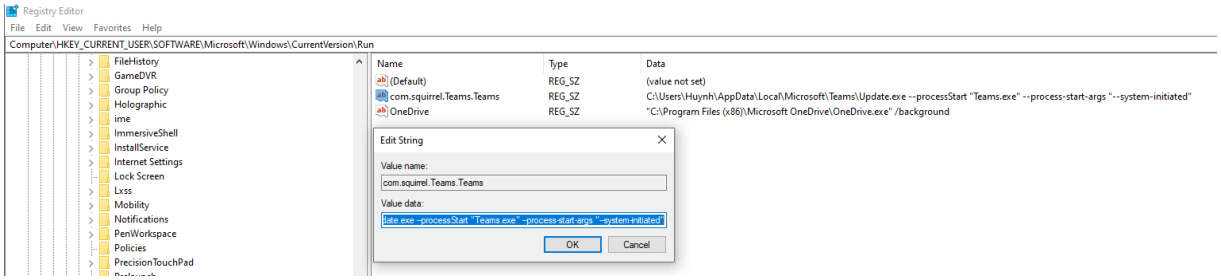


Note the Value name and value data which is the path to the exe file. Take a screen shot for your report.

Yours will be different,

Click Cancel. Never click OK

Explain the purpose of this startup item.



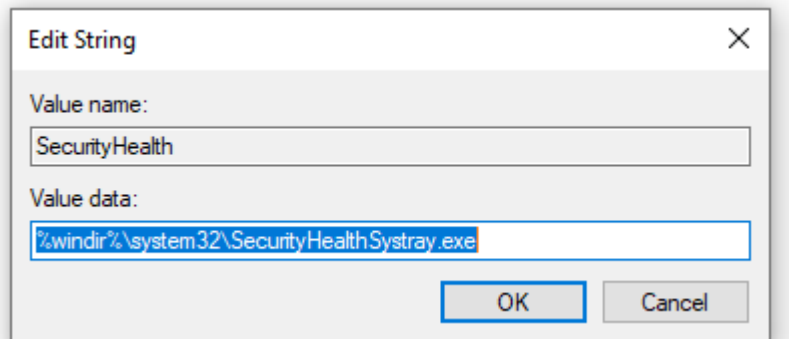
- The purpose of this item is to start Microsoft Teams and starting this Microsoft teams on startup allows it to automatically update whenever it is ran

Can you locate other startup items in the registry?

List a few here.

From the above screenshot:

- OneDrive a file hosting service and synchronisation service operated by Microsoft as part of its web version of Office. If I was signed into office one drive and using its functions, every time on startup OneDrive would automatically sync with your online OneDrive



- SecurityHealth on startup provide notifications about the health and security of the machine

Q2) USB Store

Run regedit and navigate to:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Portable Devices\Devices\

In regedit, under Windows Portable Devices, right click Devices and select export. Save the hive as a text file with name USBStor of type txt in C:\Forensics_yourname. Close regedit. Run Linux.

The export is wrongly encoded for Linux. To fix this open the USBStor.txt file in notepad in Linux. notepad.exe USBStor.txt.

Then save the file with a new name USBStor_UTF8.txt using UTF8 encoding.

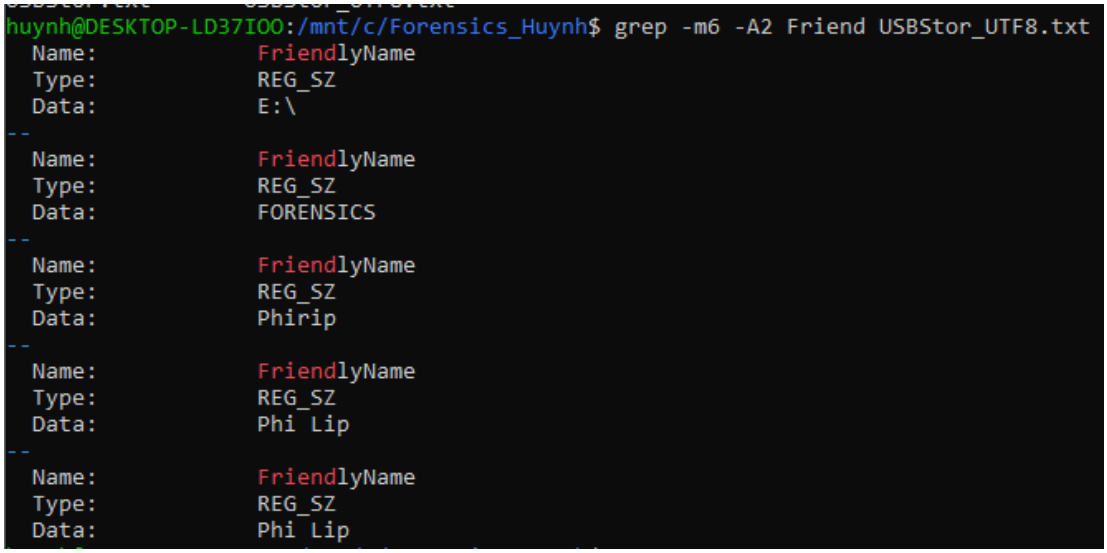
Now use grep to search the file for the keyword Friend.

We need to see 2 lines after the match and stop counting after 6 matches, so we type

grep -m6 -A2 Friend USBStor_UTF8.txt

Your list will be different.

Take a screen shot of this list for your report.



Explain how each item could be of forensic interest.

- These items would be of forensic interests as it keeps track of external devices connected. The data are kept in the registry which makes it retrievable and if there is a case that requires to look at any potential devices that were connected in the past this would be one way to check/confirm it has been used on this device.

Use less to see the GUIDs, in Braces { } in USBStor_UTF8.txt

Record here your laptop USB GUID. {53F56307-B6BF-11D0-94F2-00A0C91EFB8B}

What is the GUID version? Type 1 GUID What is the date of manufacture ? 1996

Can you find other type 1 UUID/GUIDs on your laptop? Disks maybe?

Show it here {96A54D49-F655-11EB-A6F4-000C29D27C0B}

What is it describing?

- Name: FORENSICS (USB I used in one of the labs)
- Type: Reg_EZ
- Version 1
- Date manufactured: 2021-08-06
- MAC Address: 00:0c:29:d2:7c:0b

3) Memory Process Dumps

A) Setup.

Step 1: Clear cookies. Do this.

Step 2: Collect some evidence of web visits into memory. Use Chrome. Do this

B) Get a memory dump.

Open Task Manager. select the Details Tab

Which chrome process has the forensic data? Do some research and tell us your findings

- In the task manager of the browser settings when Officeworks run this takes the lead in the largest process on the chrome list. This means that forensics data on the website would be on the largest file, furthermore there are subframes that have the tracking cookies processes stored. The processes on these would be near the middle of the list.

Dump the three largest memory chrome processes. Copy to your Forensics folder. Close Chrome.

Confirm you are in ubuntu Linux on Windows in your Forensics folder.

Run strings to get three text files.

A) **Explore the dump using grep.**

You may have to choose the right dump file.

Look at the result. If you see evidence, take a screen shot.

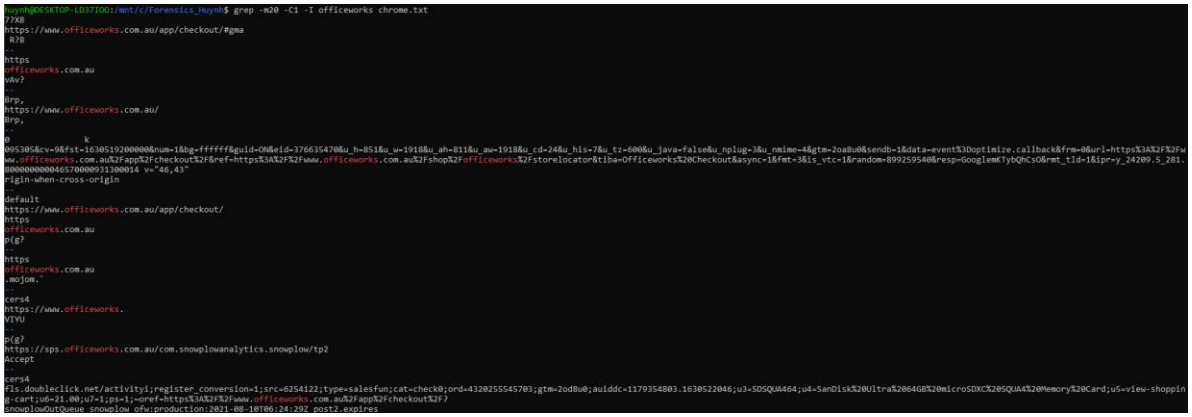
3C1) Look for the keyword cookies.

grep -m 20 -C1 -I cookie chrome.txt | cut -c 1-120

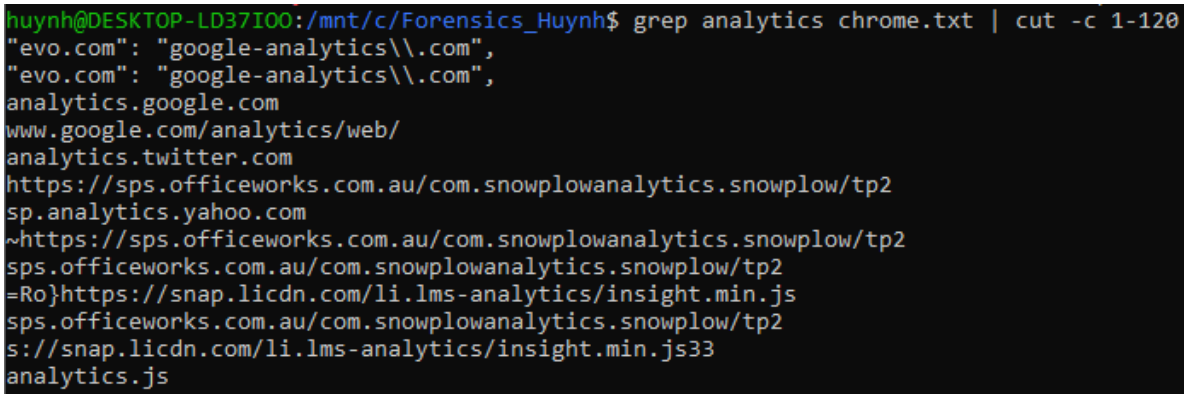
Repeat for the other chrome dump txt files.

Describe the evidence you found. Your results will differ from the samples shown.

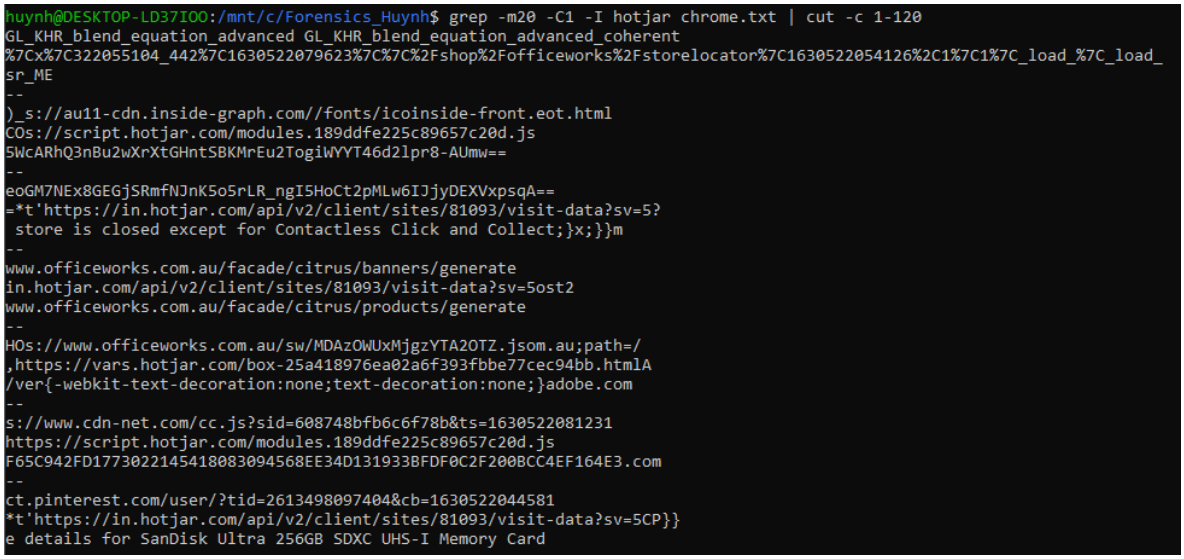
- There is snow analytics seen in this screenshot using the command above



- We can see that yahoo and snowplow analytics already shows in Officeworks



- HotJar and Inside-graph cookies



- CDN Hosting analytics of akamai

```
huynh@DESKTOP-LD37IOO:/mnt/c/Forensics_Huynh$ grep akamai chrome3.txt
9https://statics-marketingsites-wcus-ms-com.akamaized.net/
akamaized.net^*.stream/
akamaiedge.net^
akamaized.net^*/playlist.m3u8?
https://statics-marketingsites-wcus-ms-com.akamaized.net/
akamai-access.com/
9https://statics-marketingsites-wcus-ms-com.akamaized.net/
akamai-grn:0.ac07d217.1630522094.4869e14
x-cdn:akamai
```

- Demdex behavioral Cookies

```
huynh@DESKTOP-LD37IOO:/mnt/c/Forensics_Huynh$ grep -m20 -C1 -I demdex chrome.txt | cut -c 1-120
 * More info available at https://marketing.adobe.com/resources/help/en_US/mcvid/
var e=function(){"use strict";function e(t){"@babel/helpers - typeof";return(e="function"==typeof Symbol&&"symbol"==type
f.prototype.constructor=f;var He="fetchPermissions",Be="[OptIn#registerPlugin] Plugin is invalid.";p.Categories=fe,p.Tim
";t.length%64-56;)t+="\0";for(i=0;i<t.length;i++){if((r=t.charCodeAt(i))>>8)return;c[i>>2]|=r<<(3-i)%4*8}for(c[c.length]
}(o)&&C.parent?new X(e,i,o,C.parent):new ze(e,i,a);return o=null,c.init(),c},function(){function e(){ze.windowLoaded=!0}
--
s.net/dc38r8bijjm5/ogw4VCgQ96IbqI0rEGw4i/5e257d19399ceea004aad147a1594b39/ico_easyReturns_loop.svg")
"https://www.officeworks.com.au" from accessing a frame with origin "https://officeworks.demdex.net".
{.product{margin-left:4px;margin-right:4px;width:calc(50% - 8px);}.product.is-promo-large{width:calc(100% - 8px);}}
--
a23-2d1f-43b1-bbfd-cc6fd88afdc3
/www.officeworks.com.au" from accessing a frame with origin "https://officeworks.demdex.net". Protocols, domains, and po
?ked a frame with origin "https://www.officeworks.com.au" from accessing a frame with origin "https://vars.hotjar.com".
--
@MY&D
/www.officeworks.com.au" from accessing a frame with origin "https://officeworks.demdex.net". Protocols, domains, and po
@sko
--
```

3C2) Show here the Count of the hits for the word Officeworks and the word Seek. Comment on the result.

- Count of Officeworks

First file of the dump should have the most hits as they run the core page of their respective websites and the screenshots reflect, they have the highest hits. The second file dump for chrome searching for Officeworks does not have a high count, only 6 hits appeared. However, in Seek it is different as the second dump had the second highest amount of hits

```
huynh@DESKTOP-LD37IOO:/mnt/c/Forensics_Huynh$ grep -c -i officeworks chrome.txt
2193
huynh@DESKTOP-LD37IOO:/mnt/c/Forensics_Huynh$ grep -c -i officeworks chrome2.txt
6
huynh@DESKTOP-LD37IOO:/mnt/c/Forensics_Huynh$ grep -c -i officeworks chrome3.txt
4913
```

- Count of Seek

```
huynh@DESKTOP-LD37IOO:/mnt/c/Forensics_Huynh$ grep -c -i seek seek.txt
37856
huynh@DESKTOP-LD37IOO:/mnt/c/Forensics_Huynh$ grep -c -i seek seek2.txt
5739
huynh@DESKTOP-LD37IOO:/mnt/c/Forensics_Huynh$ grep -c -i seek seek3.txt
231
```

3C3:

Week 06 Memory and Registry Report

Search for your keywords.

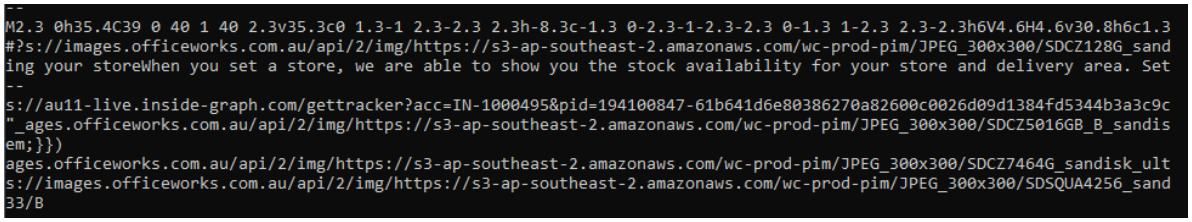
For Officeworks - SanDisk, USB Pen Drive, Glebe.

Comment on the results. Add extra search keyworks. Comment on successful finds.

Take a Screen shot – only the important stuff!.

- SanDisk

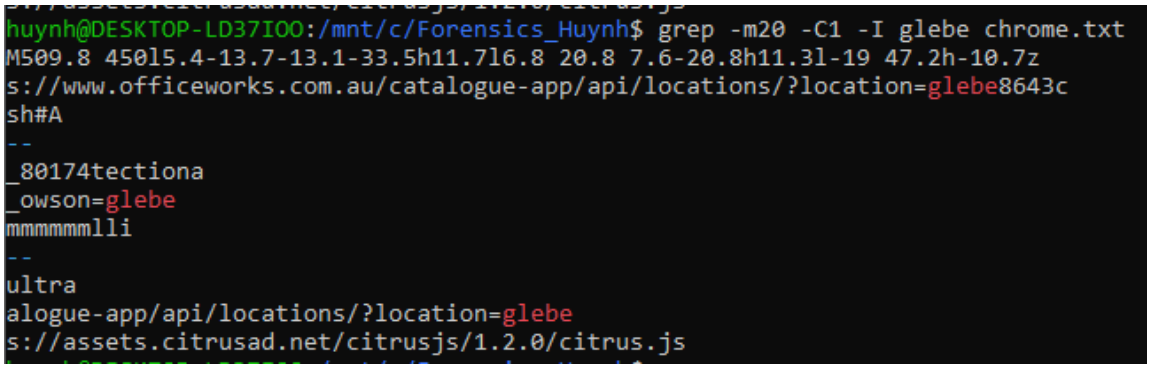
The cookies with the SanDisk are inside-graph cookies



- USB Pen Drive

Cookies are also the same and there are inside-graph

- Glebe search where you can see location is set to glebe and there is a cirtus javascript running which is scalable, auction-based advertising software built for e-commerce retailers



Week 07 Windows Live Report

Name: Huynh Lam **Student ID: 13264763** **Date: 19/09/2021**
Activity No.: Cmp1/03
Due Date: Three days after the lab.

Part One: Examine the Device Volatile Data

Preparation

Download the files

Start Logging

Start ubuntu.

date > Evidence_start.txt

Q1) Local User

whoami >> Evidence_start.txt

Check the contents of your new file with cat and then take a screen shot for your report.

```
huynh@DESKTOP-LD37IOO:/mnt/c/Forensics_Huynh/Week 7$ cat Evidence_start.txt
Wed Sep  8 01:42:28 AEST 2021
huynh
```

Q2) Check Chrome

You might be suspicious that Chrome is an imposter.

Type ./Listdlls.exe | grep -i -m6 chrome.exe | cut -c -80

This may take several seconds to complete..

Take a screen shot for upload.

```
huynh@DESKTOP-LD37IOO:/mnt/c/Forensics_Huynh/Week 7$ ./Listdlls.exe | grep -i -m6 chrome.exe | cut -c -80
chrome.exe pid: 6860
Command line: "C:\Program Files\Google\Chrome\Application\chrome.exe"
0x00000000bebf0000  0x267000  C:\Program Files\Google\Chrome\Application\chrome.
chrome.exe pid: 9800
Command line: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=cra
0x00000000bebf0000  0x267000  C:\Program Files\Google\Chrome\Application\chrome.
```

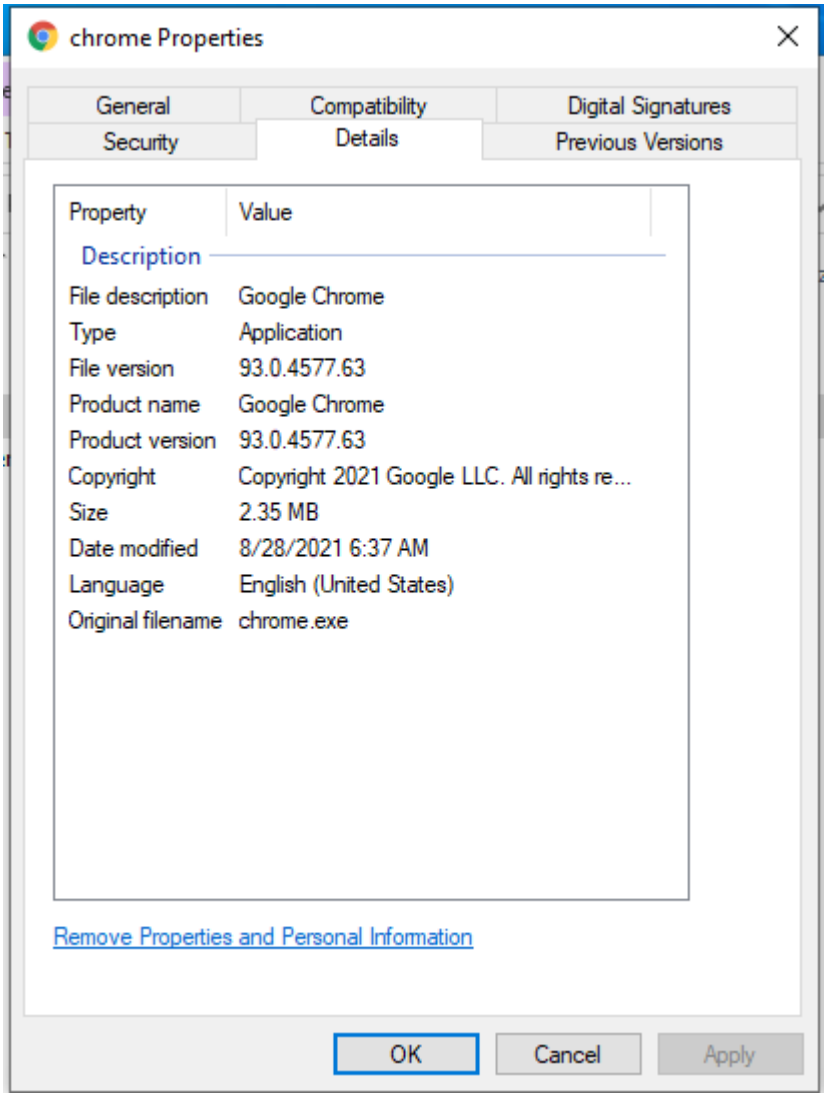
Week 07 Windows Live Report

Locate the chrome.exe file location shown using File Explorer. Right click and select properties.

What items imply the exe file is genuine?

In the properties tab, the details contain some metadata that would imply the exe file is genuine. The screenshot shows that Google signature is left, and you can also look for the product name and version to have additional verification

Take a screen shot showing these items.



Q3) Check Services

To see the processes running services we use tasklist.exe /svc

Confirm you are running Chrome.

What is a cmdline to ONLY show the PIDs in use by chrome as a service?

Take a screenshot of the result

Command: tasklist.exe /svc | grep chrome

```
huynh@DESKTOP-LD37IOO:/mnt/c/Forensics_Huynh/Week 7$ tasklist.exe /svc | grep chrome
chrome.exe                    6860 N/A
chrome.exe                    9800 N/A
chrome.exe                    6916 N/A
chrome.exe                     356 N/A
chrome.exe                    8620 N/A
chrome.exe                    8852 N/A
chrome.exe                   10160 N/A
chrome.exe                    8628 N/A
```

Take another screenshot showing the conhost service

```
huynh@DESKTOP-LD37IOO:/mnt/c/Forensics_Huynh/Week 7$ tasklist.exe /svc | grep conhost
conhost.exe                    856 N/A
conhost.exe                   1820 N/A
conhost.exe                    676 N/A
conhost.exe                   4884 N/A
```

What does the conhost service do? The conhost.exe (Console Windows Host) file is provided by Microsoft. Conhost.exe is required to run in order for Command Prompt to interface with Windows Explorer. One of its duties is to provide the ability to drag and drop files/folders directly into Command Prompt

Part Two: Non Volatile Data

Q4) System Information – cmd line

Confirm you have download this week's tools to C:\Forensics_yourname.

Run ubuntu and cd to your forensics folder. Run PsInfo by typing:

./PsInfo.exe (note the leading dot)

What Product Version and Service Pack number is Windows running?

- Product Version: 6.3

- Service Pack: 0

psInfo can see more. Type ./psInfo.exe -?.

What do the h, s and d flags do?

- H: Shows the installed hotfixes
- S: Shows the installed software
- D: Show disk volume information

Now type:

./PsInfo.exe -h -s -d | strings > PsInfo.txt

Have a look at the new evidence using notepad.

notepad.exe PsInfo.txt

What is the size of the Hard Disk C:\ Drive and the % free?

- Size of the hard drive 60GB
- The percentage free is 44.8%

Close notepad. You used Wireshark in week 4.

Use grep to check PsInfo.txt for Wireshark and any wireless apps installed**.**

Use a screen shot to show the command line and the result.

```
huynh@DESKTOP-LD37IOO:/mnt/c/Forensics_Huynh/Week 7$ cat PsInfo.txt | grep Wireshark
Wireshark 3.4.7 64-bit 3.4.7
```

What is the Wireshark version? 3.4.7

Q5) User Assist

Run ./UserassistView.exe (GUI). Sort by Count descending..

Can you get Chrome in the top 10?

Take a screen shot for upload of the top 10 items.

Item Name	Index	Count	Modified Time	ClassID
UEME_CTLSESSION	2	213		{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}
UEME_CTLSESSION	59	87		{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}
Microsoft.Windows.Explorer	15	36	9/8/2021 1:45:24 AM	{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}
{9E3995AB-1F9C-4F13-B827-48B24B6C7174}\TaskBar\File Explorer.lnk	62	34	9/8/2021 1:45:24 AM	{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}
Chrome	19	25	9/8/2021 1:59:47 AM	{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}
Microsoft.XboxGamingOverlay_8wekyb3d8bbwe!App	26	18	9/7/2021 11:44:39 PM	{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}
{9E3995AB-1F9C-4F13-B827-48B24B6C7174}\TaskBar\Google Chrome.lnk	65	17	9/8/2021 1:59:47 AM	{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}
{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\cmd.exe	25	15	9/8/2021 1:40:37 AM	{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}
Microsoft.Getstarted_8wekyb3d8bbwe!App	1	14	8/5/2021 4:51:45 PM	{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}
Microsoft.WindowsFeedbackHub_8wekyb3d8bbwe!App	3	13	8/5/2021 4:51:45 PM	{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}

Note the Class IDs are GUIDs. What version of the GUIDs are most common? (Week 6).

- Version 4 is the most common amongs this list

Upload

Upload this report when done.

48436/32309 Week 08 Linux Live as User Report

Name: Huynh Lam Student ID: 13264763 Date: 03/09/2021

Activity No.: Cmp1/03

Here we will only use user (non sudo) access commands.

This Lab is for WSL on Windows 10.

If you use another Linux device, such as Terminal on MacOS or a Linux VM, answers may vary.

Reminder: To get the Thorough mark, you need to answer as a Forensics Investigator. (Week 1 module)

Part 1: Examine the device volatile data

Preparation

Logon to your laptop. Open a Terminal shell using ubuntu. CD to your desktop.

Q1) Log your activity

Confirm your OS version.

cat /etc/issue Yours may be different.

Then cat /etc/issue > evidence_start.txt

Type pwd to confirm your location.

Type whoami to confirm your connection

pwd >> evidence_start.txt

whoami >> evidence_start.txt # record your name

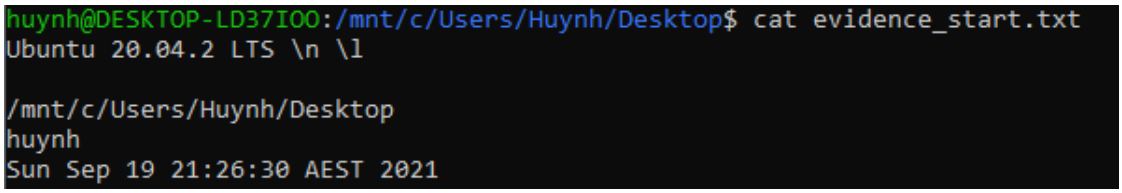
date >> evidence_start.txt # append the date and time

Check the file by typing:

cat evidence_start.txt

You should see the OS version, user name and the start date and time in the text file.

Take a screenshot to upload the contents of evidence_start.txt



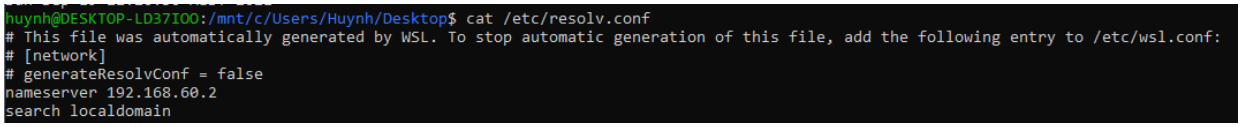
48436/32309 Week 08 Linux Live as User Report

Q2) Check network Details.

To identify the dns server, check /etc/resolv.conf

Type cat /etc/resolv.conf Is it a public or private address? Private

Take a screen shot for upload.



In your shell, type ip addr . Which interfaces are active? <UP>

- eth0
- lo

What are your active IPv4 addresses?

- 192.168.60.129
- 127.0.0.1

Q3) Check Processes

An attacker or virus may set up its own process or hijack an existing process.

We use **ps** to show running tasks.
Type ps - - help simple. What do the -a, -A and the -r flags do?

- - -a: All with tty, except session leaders
- - -A: All processes
- - -r: Only running processes

Let us run a suspicious process, say ping.
In another cmd window start another copy of ubuntu.
Ping a dns.
ping 1.1.1.1 the ping should keep pinging.
Switch back to your original ubuntu shell.

Type ps –Af You should see the ping.

Take a screen shot for upload.

```
huynh@DESKTOP-LD37IOO:/mnt/c/Users/Huynh/Desktop$ ps -Af
UID          PID    PPID  C STIME TTY          TIME CMD
root           1       0  0 21:21 ?        00:00:00 /init
root           6       1  0 21:21 tty1     00:00:00 /init
huynh          7       6  0 21:21 tty1     00:00:00 -bash
root         159       1  0 21:33 tty2     00:00:00 /init
huynh        160     159  0 21:33 tty2     00:00:00 -bash
huynh        173     160  0 21:33 tty2     00:00:00 ping 1.1.1.1
huynh        174       7  0 21:33 tty1     00:00:00 ps -Af
```

Q4) Check Services

We can see installed services by looking at init.d, the service launcher.

ls /etc/init.d Take a screen shot for upload.

```
huynh@DESKTOP-LD37IOO:/mnt/c/Users/Huynh/Desktop$ ls /etc/init.d/
apparmor          cryptdisks        iscsid             multipath-tools  procps           udev
apport            cryptdisks-early  keyboard-setup.sh  open-iscsi       rsync            ufw
atd               dbus              kmod               open-vm-tools    rsyslog          unattended-upgrades
console-setup.sh  hwclock.sh        lvm2               plymouth         screen-cleanup   uuidd
cron              irqbalance        lvm2-lvmpolld      plymouth-log     ssh              x11-common
```

Which ones in the table are running on your device?

- **cron**
- **ssh**
- **x11**

Part 2: Examine the device non-volatile data

Q5) System Information – cmd line

5a) The basic system info is revealed by uname

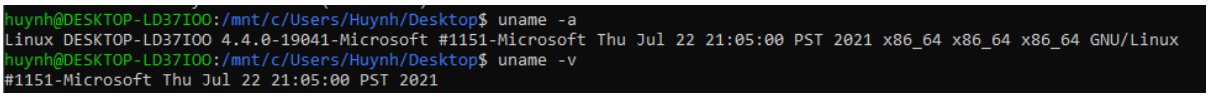
48436/32309 # Week 08 Linux Live as User Report

Type uname –a to see the system summary.

Type uname -v to see the kernel version

Type wsl.exe - - update - - status

Take a screenshot of all three for upload.



Comment on the difference shown for the kernel version

- -a prints all the system information in the command uname whereas using -v argument will only print the kernel version which you can see both commands print out the kernel version in their output.

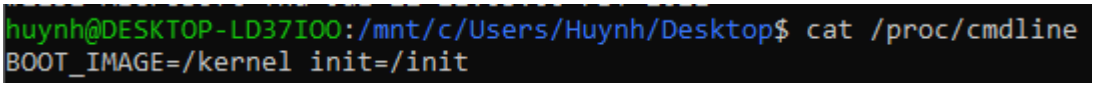
5b) What Linux knows about the hardware is kept in /proc

cat /proc/cmdline # This shows you how the boot image is loaded.

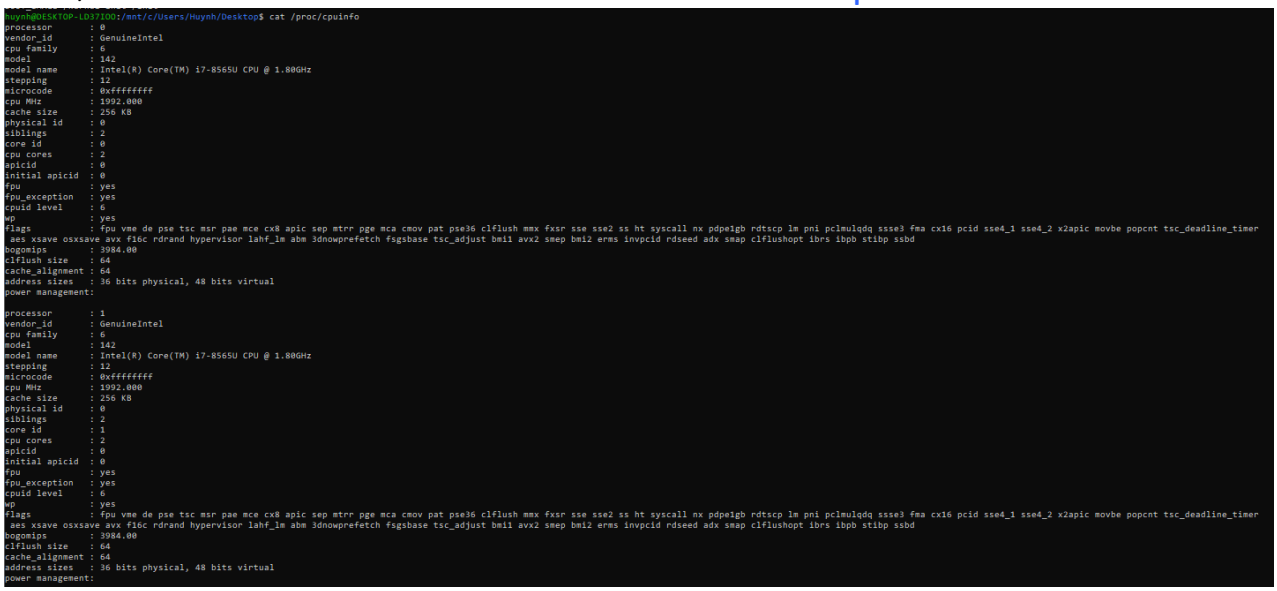
cat /proc/cpuinfo # This shows you the CPU details – some will be virtual if this is a VM.

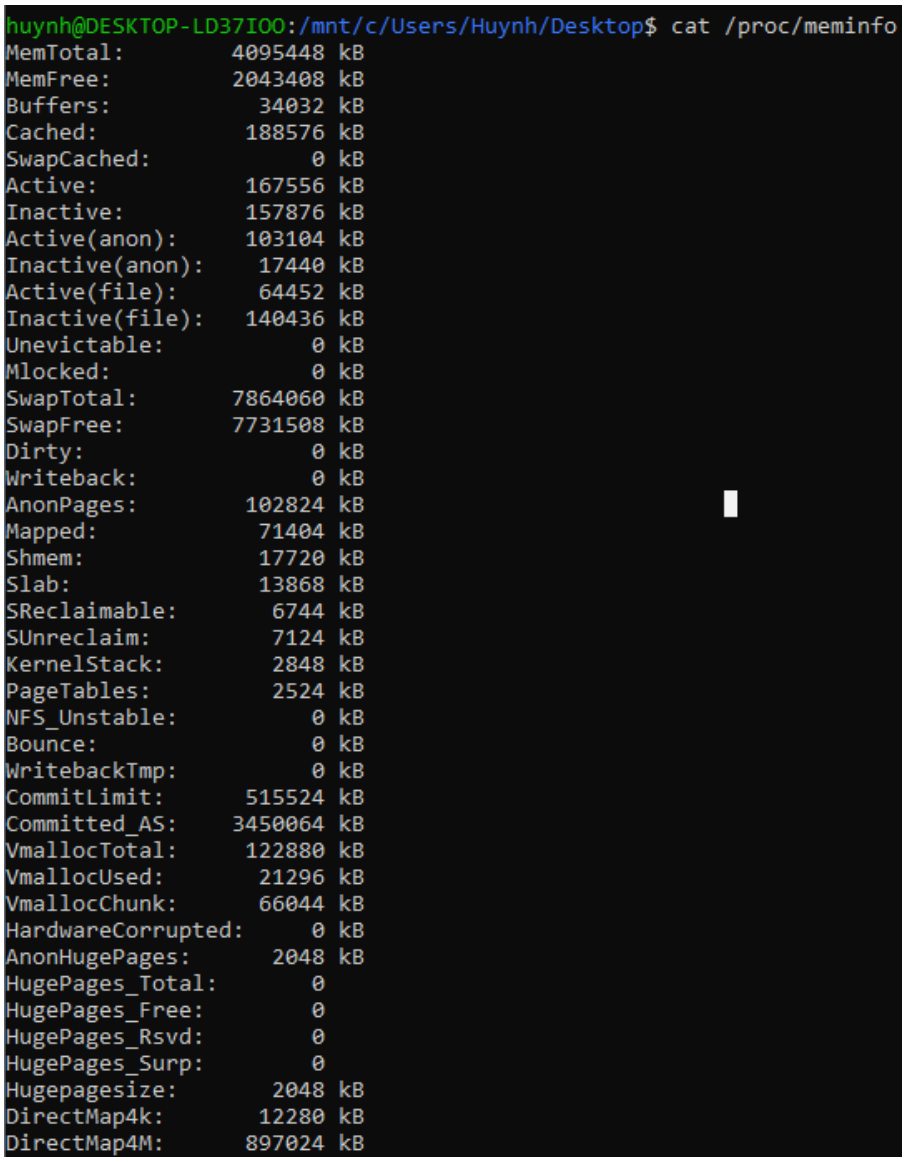
cat /proc/meminfo # Memory management details

Repeat the cat /proc commands with grep as shown on the lecture slide to show the number of processors, cpu model, total and free Memory. Take a screenshot for upload.



Week 08 Linux Live as User Report





5c) We can see the Linux file structure with df

48436/32309 # Week 08 Linux Live as User Report

whatis df ?__ Show information about the file system on which each FILE resides, or all file systems by default.

Type df –ahT Take a screen shot for upload

```
huynh@DESKTOP-LD37IOO:/mnt/c/Users/Huynh/Desktop$ df -ahT
Filesystem     Type         Size  Used Avail Use% Mounted on
rootfs         wslfs         60G   31G   30G  51% /
none           tmpfs         60G   31G   30G  51% /dev
sysfs          sysfs            0     0     0    - /sys
proc           proc             0     0     0    - /proc
devpts         devpts           0     0     0    - /dev/pts
none           tmpfs         60G   31G   30G  51% /run
none           tmpfs         60G   31G   30G  51% /run/lock
none           tmpfs         60G   31G   30G  51% /run/shm
none           tmpfs         60G   31G   30G  51% /run/user
binfmt_misc    binfmt_misc      0     0     0    - /proc/sys/fs/binfmt_misc
tmpfs          tmpfs         60G   31G   30G  51% /sys/fs/cgroup
cgroup         cgroup           0     0     0    - /sys/fs/cgroup/devices
C:\            drvfs         60G   31G   30G  51% /mnt/c
```

What is the Linux root mount symbol ? /

What is this filesystem type? wslfs

5d) User Accounts

We can see the user accounts in /etc/passwd.

cat /etc/passwd | grep bash

Take a screenshot of the users for your report.

```
huynh@DESKTOP-LD37IOO:/mnt/c/Users/Huynh/Desktop$ cat /etc/passwd | grep bash
root:x:0:0:root:/root:/bin/bash
huynh:x:1000:1000:,,,:/home/huynh:/bin/bash
```

Comment on the results.

There are only 2 users in the system. The root account and my personal account Huynh

Close all windows and shells when done.

Bring an empty USB for the week 9 Lab.

48436/32309 Week 09 Disk Analysis Report

Name: Huynh Lam Student ID: 13264763 Date: 10/10/2021
Activity No.: Cmp1/03

In this week's Lab we will use The Sleuth Kit (TSK) tools to gather disk information.

You may have to run apt-get update on your ubuntu before you install fsstat and fls

We will examine a USB with a FAT Partition and a NTFS Partition

We will delete some files and then try and recover them.

Reminder: To get the Thorough mark, you need to answer as a Forensics Investigator. (Week 1 module)

Preparation 1 – Prepare the Evidence on the USB

Insert your small USB Flash Drive.

It will mount as a Drive letter, typically E:\Drive.

Warning! We will ERASE ALL FILES!

Set the volume size to 20 MB. Click next. Click next.

Select the FAT file system. Name the Volume Forensics F

Set the volume size to 20 MB. Click next. Click next.

Select the NTFS file system. Name the Volume Forensics N

Download and copy the Week 5 (Metadata) Sample files from UTS Online to each partition.

Delete the IMAG* file in both partitions.

Also delete the Trade_Secrets.txt file in both partitions.

Preparation 2 – Acquire the Image of the USB Volume

We use ProDiscover (week 2) to acquire images of the two Disk volumes (FAT 16 and NTFS).

If the ProDiscover Licence has expired, uninstall the program and install it again from the Week 2 download.

Do NOT acquire the whole disk.

Mount your USB with the two partitions, Forensics F and Forensics N.

Run ProDiscover. Fill out the Project details. Call the project USB.

Select your Forensics _yourname folder as the destination. Call the image file USBVolume1.dd

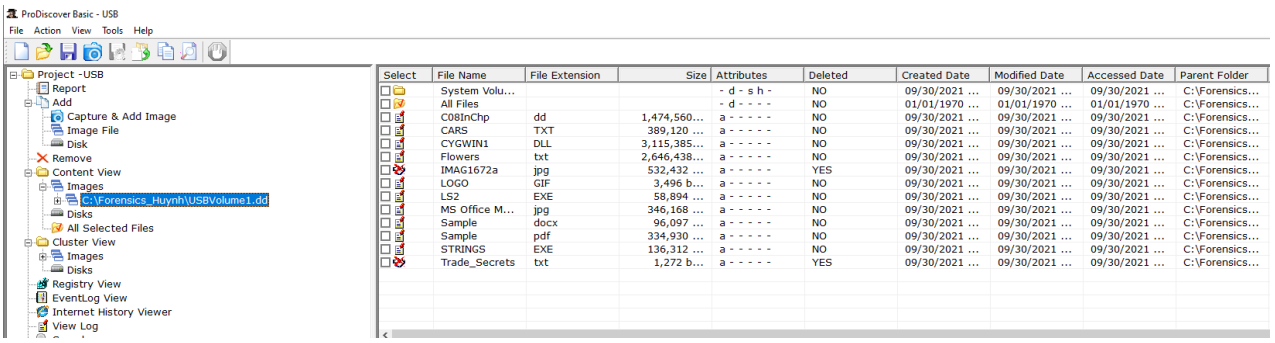
Acquire the Partition.

Confirm your image appears under Content View in the left panel.

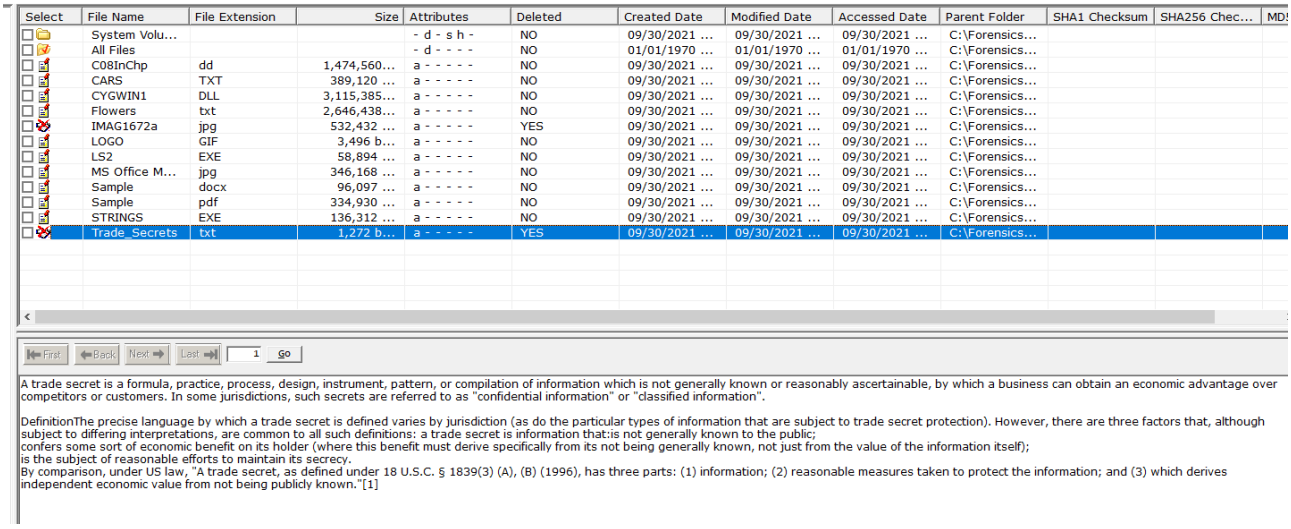
48436/32309

Week 09 Disk Analysis Report

Take a screen shot of the Project tree and list of files for your report.



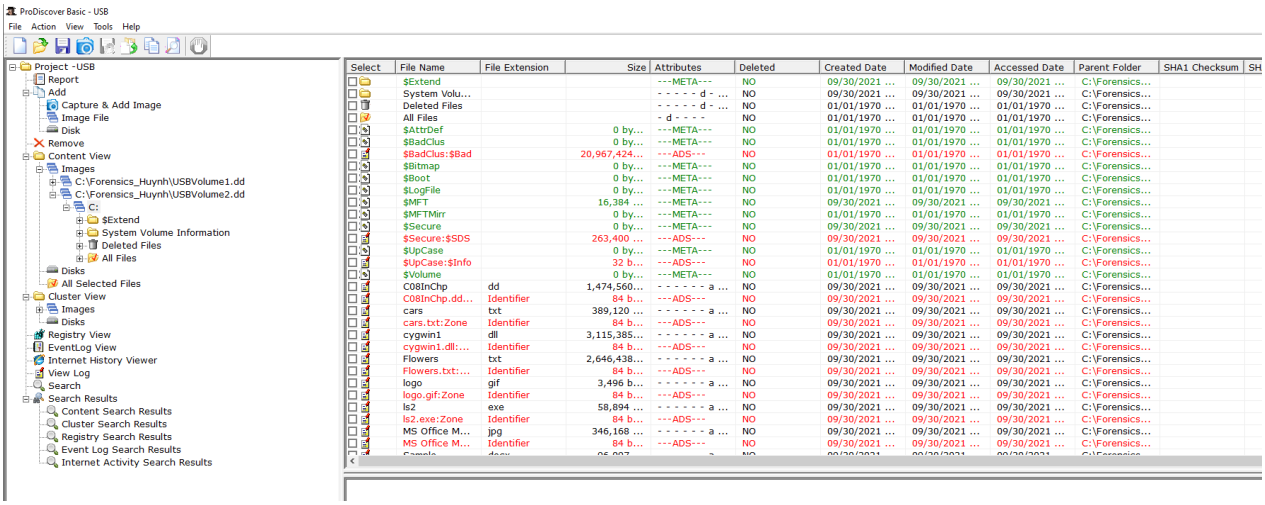
Select the deleted file Trade_Secrets.txt Confirm you can see the contents in the view pane. _ _



Repeat to acquire your Forensics N Volume. Call it USBVolume2.dd

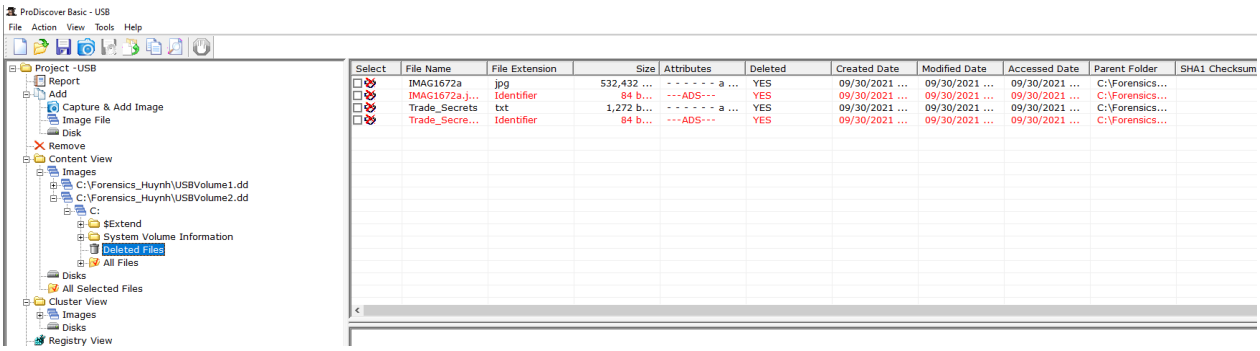
Now with NTFS you need to select the C:\Drive to see the files.

Take a screen shot of the Project tree and list of files for your report.



Also the deleted files have been moved to a separate folder.

Select the deleted file Trade_Secrets.txt Confirm you can see the contents in the view pane. _ __



Q1) MBR Partition Analysis of the USB

Download to your Forensics folder the USBPartition.dd file from Canvas.

Run ubuntu. Change to your Forensics folder.

Run xxd -l 512 to view the partition file.

Confirm the result looks like the MBR in the Lecture slides. _____

Week 09 Disk Analysis Report

```
huynh@DESKTOP-LD37IOO:/mnt/c/Forensics_Huynh$ xxd -l 512 USBPartition.dd
00000000: 33c0 8ed0 bc00 7cfb 5007 501f fcbe 1b7c  3.....|.P.P....|
00000010: bf1b 0650 57b9 e501 f3a4 cbbd be07 b104  ...PW...........
00000020: 386e 007c 0975 1383 c510 e2f4 cd18 8bf5  8n.|.u..........
00000030: 83c6 1049 7419 382c 74f6 a0b5 07b4 078b  ...It.8,t.......
00000040: f0ac 3c00 74fc bb07 00b4 0ecd 10eb f288  ..<.t...........
00000050: 4e10 e846 0073 2afe 4610 807e 040b 740b  N..F.s*.F..~..t.
00000060: 807e 040c 7405 a0b6 0775 d280 4602 0683  .~..t....u..F...
00000070: 4608 0683 560a 00e8 2100 7305 a0b6 07eb  F...V...!.s.....
00000080: bc81 3efe 7d55 aa74 0b80 7e10 0074 c8a0  ..>.}U.t..~..t..
00000090: b707 eba9 8bfc 1e57 8bf5 cbbf 0500 8a56  .......W.......V
000000a0: 00b4 08cd 1372 238a c124 3f98 8ade 8afc  .....r#..$?.....
000000b0: 43f7 e38b d186 d6b1 06d2 ee42 f7e2 3956  C..........B..9V
000000c0: 0a77 2372 0539 4608 731c b801 02bb 007c  .w#r.9F.s......|
000000d0: 8b4e 028b 5600 cd13 7351 4f74 4e32 e48a  .N..V...sQOtN2..
000000e0: 5600 cd13 ebe4 8a56 0060 bbaa 55b4 41cd  V......V.`..U.A.
000000f0: 1372 3681 fb55 aa75 30f6 c101 742b 6160  .r6..U.u0...t+a`
00000100: 6a00 6a00 ff76 0aff 7608 6a00 6800 7c6a  j.j..v..v.j.h.|j
00000110: 016a 10b4 428b f4cd 1361 6173 0e4f 740b  .j..B....aas.Ot.
00000120: 32e4 8a56 00cd 13eb d661 f9c3 496e 7661  2..V.....a..Inva
00000130: 6c69 6420 7061 7274 6974 696f 6e20 7461  lid partition ta
00000140: 626c 6500 4572 726f 7220 6c6f 6164 696e  ble.Error loadin
00000150: 6720 6f70 6572 6174 696e 6720 7379 7374  g operating syst
00000160: 656d 004d 6973 7369 6e67 206f 7065 7261  em.Missing opera
00000170: 7469 6e67 2073 7973 7465 6d00 0000 0000  ting system.....
00000180: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000190: 0000 0000 0000 0000 0000 0000 0000 0000  ................
000001a0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
000001b0: 0000 0000 002c 4463 9316 4336 0000 0020  .....,Dc..C6...
000001c0: 2100 0eac 2a02 0008 0000 00a0 0000 00ac  !...*...........
000001d0: 2b02 0739 3405 00a8 0000 00a0 0000 0000  +..94...........
000001e0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
000001f0: 0000 0000 0000 0000 0000 0000 0000 55aa  ..............U.
```

Take a screenshot of the MBR to upload. Identify the following:

- the last error message,

Week 09 Disk Analysis Report

```
huynh@DESKTOP-LD37IOO:/mnt/c/Forensics_Huynh$ xxd -l 512 USBPartition.dd
00000000: 33c0 8ed0 bc00 7cfb 5007 501f fcbe 1b7c  3.....|.P.P....|
00000010: bf1b 0650 57b9 e501 f3a4 cbbd be07 b104  ...PW...........
00000020: 386e 007c 0975 1383 c510 e2f4 cd18 8bf5  8n.|.u..........
00000030: 83c6 1049 7419 382c 74f6 a0b5 07b4 078b  ...It.8,t.......
00000040: f0ac 3c00 74fc bb07 00b4 0ecd 10eb f288  ..<.t...........
00000050: 4e10 e846 0073 2afe 4610 807e 040b 740b  N..F.s*.F..~..t.
00000060: 807e 040c 7405 a0b6 0775 d280 4602 0683  .~..t....u..F...
00000070: 4608 0683 560a 00e8 2100 7305 a0b6 07eb  F...V...!.s.....
00000080: bc81 3efe 7d55 aa74 0b80 7e10 0074 c8a0  ..>.}U.t..~..t..
00000090: b707 eba9 8bfc 1e57 8bf5 cbbf 0500 8a56  .......W.......V
000000a0: 00b4 08cd 1372 238a c124 3f98 8ade 8afc  .....r#..$?.....
000000b0: 43f7 e38b d186 d6b1 06d2 ee42 f7e2 3956  C..........B..9V
000000c0: 0a77 2372 0539 4608 731c b801 02bb 007c  .w#r.9F.s......|
000000d0: 8b4e 028b 5600 cd13 7351 4f74 4e32 e48a  .N..V...sQOtN2..
000000e0: 5600 cd13 ebe4 8a56 0060 bbaa 55b4 41cd  V......V.`..U.A.
000000f0: 1372 3681 fb55 aa75 30f6 c101 742b 6160  .r6..U.u0...t+a`
00000100: 6a00 6a00 ff76 0aff 7608 6a00 6800 7c6a  j.j..v..v.j.h.|j
00000110: 016a 10b4 428b f4cd 1361 6173 0e4f 740b  .j..B....aas.Ot.
00000120: 32e4 8a56 00cd 13eb d661 f9c3 496e 7661  2..V.....a..Inva
00000130: 6c69 6420 7061 7274 6974 696f 6e20 7461  lid partition ta
00000140: 626c 6500 4572 726f 7220 6c6f 6164 696e  ble.Error loadin
00000150: 6720 6f70 6572 6174 696e 6720 7379 7374  g operating syst
00000160: 656d 004d 6973 7369 6e67 206f 7065 7261  em.Missing opera
00000170: 7469 6e67 2073 7973 7465 6d00 0000 0000  ting system.....
00000180: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000190: 0000 0000 0000 0000 0000 0000 0000 0000  ................
000001a0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
000001b0: 0000 0000 002c 4463 9316 4336 0000 0020  .....,Dc..C6...
000001c0: 2100 0eac 2a02 0008 0000 00a0 0000 00ac  !...*...........
000001d0: 2b02 0739 3405 00a8 0000 00a0 0000 0000  +..94...........
000001e0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
000001f0: 0000 0000 0000 0000 0000 0000 0000 55aa  ..............U.
```

- the four partition types __ _____

```
huynh@DESKTOP-LD37IOO:/mnt/c/Forensics_Huynh$ xxd -l 512 USBPartition.dd
00000000: 33c0 8ed0 bc00 7cfb 5007 501f fcbe 1b7c  3.....|.P.P....|
00000010: bf1b 0650 57b9 e501 f3a4 cbbd be07 b104  ...PW...........
00000020: 386e 007c 0975 1383 c510 e2f4 cd18 8bf5  8n.|.u..........
00000030: 83c6 1049 7419 382c 74f6 a0b5 07b4 078b  ...It.8,t.......
00000040: f0ac 3c00 74fc bb07 00b4 0ecd 10eb f288  ..<.t...........
00000050: 4e10 e846 0073 2afe 4610 807e 040b 740b  N..F.s*.F..~..t.
00000060: 807e 040c 7405 a0b6 0775 d280 4602 0683  .~..t....u..F...
00000070: 4608 0683 560a 00e8 2100 7305 a0b6 07eb  F...V...!.s.....
00000080: bc81 3efe 7d55 aa74 0b80 7e10 0074 c8a0  ..>.}U.t..~..t..
00000090: b707 eba9 8bfc 1e57 8bf5 cbbf 0500 8a56  .......W.......V
000000a0: 00b4 08cd 1372 238a c124 3f98 8ade 8afc  .....r#..$?.....
000000b0: 43f7 e38b d186 d6b1 06d2 ee42 f7e2 3956  C..........B..9V
000000c0: 0a77 2372 0539 4608 731c b801 02bb 007c  .w#r.9F.s......|
000000d0: 8b4e 028b 5600 cd13 7351 4f74 4e32 e48a  .N..V...sQOtN2..
000000e0: 5600 cd13 ebe4 8a56 0060 bbaa 55b4 41cd  V......V.`..U.A.
000000f0: 1372 3681 fb55 aa75 30f6 c101 742b 6160  .r6..U.u0...t+a`
00000100: 6a00 6a00 ff76 0aff 7608 6a00 6800 7c6a  j.j..v..v.j.h.|j
00000110: 016a 10b4 428b f4cd 1361 6173 0e4f 740b  .j..B....aas.Ot.
00000120: 32e4 8a56 00cd 13eb d661 f9c3 496e 7661  2..V.....a..Inva
00000130: 6c69 6420 7061 7274 6974 696f 6e20 7461  lid partition ta
00000140: 626c 6500 4572 726f 7220 6c6f 6164 696e  ble.Error loadin
00000150: 6720 6f70 6572 6174 696e 6720 7379 7374  g operating syst
00000160: 656d 004d 6973 7369 6e67 206f 7065 7261  em.Missing opera
00000170: 7469 6e67 2073 7973 7465 6d00 0000 0000  ting system.....
00000180: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000190: 0000 0000 0000 0000 0000 0000 0000 0000  ................
000001a0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
000001b0: 0000 0000 002c 4463 9316 4336 0000 0020  .....,Dc..C6...
000001c0: 2100 0eac 2a02 0008 0000 00a0 0000 00ac  !...*...........
000001d0: 2b02 0739 3405 00a8 0000 00a0 0000 0000  +..94...........
000001e0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
000001f0: 0000 0000 0000 0000 0000 0000 0000 55aa  ..............U.
```

- the four partitions boot status,
    - Boot status of these partitions are all 00 at the 0E column

- the MBR signature. _____

```
huynh@DESKTOP-LD37IOO:/mnt/c/Forensics_Huynh$ xxd -l 512 USBPartition.dd
00000000: 33c0 8ed0 bc00 7cfb 5007 501f fcbe 1b7c  3.....|.P.P....|
00000010: bf1b 0650 57b9 e501 f3a4 cbbd be07 b104  ...PW...........
00000020: 386e 007c 0975 1383 c510 e2f4 cd18 8bf5  8n.|.u..........
00000030: 83c6 1049 7419 382c 74f6 a0b5 07b4 078b  ...It.8,t.......
00000040: f0ac 3c00 74fc bb07 00b4 0ecd 10eb f288  ..<.t...........
00000050: 4e10 e846 0073 2afe 4610 807e 040b 740b  N..F.s*.F..~..t.
00000060: 807e 040c 7405 a0b6 0775 d280 4602 0683  .~..t....u..F...
00000070: 4608 0683 560a 00e8 2100 7305 a0b6 07eb  F...V...!.s.....
00000080: bc81 3efe 7d55 aa74 0b80 7e10 0074 c8a0  ..>.}U.t..~..t..
00000090: b707 eba9 8bfc 1e57 8bf5 cbbf 0500 8a56  .......W.......V
000000a0: 00b4 08cd 1372 238a c124 3f98 8ade 8afc  .....r#..$?.....
000000b0: 43f7 e38b d186 d6b1 06d2 ee42 f7e2 3956  C..........B..9V
000000c0: 0a77 2372 0539 4608 731c b801 02bb 007c  .w#r.9F.s......|
000000d0: 8b4e 028b 5600 cd13 7351 4f74 4e32 e48a  .N..V...sQOtN2..
000000e0: 5600 cd13 ebe4 8a56 0060 bbaa 55b4 41cd  V......V.`..U.A.
000000f0: 1372 3681 fb55 aa75 30f6 c101 742b 6160  .r6..U.u0...t+a`
00000100: 6a00 6a00 ff76 0aff 7608 6a00 6800 7c6a  j.j..v..v.j.h.|j
00000110: 016a 10b4 428b f4cd 1361 6173 0e4f 740b  .j..B....aas.Ot.
00000120: 32e4 8a56 00cd 13eb d661 f9c3 496e 7661  2..V.....a..Inva
00000130: 6c69 6420 7061 7274 6974 696f 6e20 7461  lid partition ta
00000140: 626c 6500 4572 726f 7220 6c6f 6164 696e  ble.Error loadin
00000150: 6720 6f70 6572 6174 696e 6720 7379 7374  g operating syst
00000160: 656d 004d 6973 7369 6e67 206f 7065 7261  em.Missing opera
00000170: 7469 6e67 2073 7973 7465 6d00 0000 0000  ting system.....
00000180: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000190: 0000 0000 0000 0000 0000 0000 0000 0000  ................
000001a0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
000001b0: 0000 0000 002c 4463 9316 4336 0000 0020  .....,Dc..C6...
000001c0: 2100 0eac 2a02 0008 0000 00a0 0000 00ac  !...*...........
000001d0: 2b02 0739 3405 00a8 0000 00a0 0000 0000  +..94...........
000001e0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
000001f0: 0000 0000 0000 0000 0000 0000 0000 55aa  ..............U.
```

Indicate the location and the value for each. You can use Hex values or circle the item on the screen shot with a label. For the partition types, include the hex and the matching name from the lecture slide.

Q2) GPT Partition Analysis of your Hard Drive

Download gdisk64.exe from Canvas into your Forensics Folder.

To run gdisk type gdisk64.exe 0: (Run cmd.exe as Administrator)

To see the disk partition (GPT), type p (p is for print)

You should see a list of disk partitions.

Take a screen shot for upload.

```
Command (? for help): p
Disk 0:: 125829120 sectors, 60.0 GiB
Sector size (logical): 512 bytes
Disk identifier (GUID): 35E5DE55-642C-4E6A-85B8-7F7F18A536A4
Partition table holds up to 128 entries
Main partition table begins at sector 2 and ends at sector 33
First usable sector is 34, last usable sector is 125829086
Partitions will be aligned on 2048-sector boundaries
Total free space is 4029 sectors (2.0 MiB)

Number  Start (sector)    End (sector)  Size       Code  Name
   1            2048       125827071   60.0 GiB    0700  Microsoft basic data
```

What is the size and name of the first partition?

- Name is Microsoft basic data
- Size is 60 GB

To see the first partition on this disk

type i (i is for information.)

Then type 1 (1 is the partition number)

Confirm you see partition GUID information ___.

Take a screen shot for upload.

```
Command (? for help): i
Using 1
Partition GUID code: EBD0A0A2-B9E5-4433-87C0-68B6B72699C7 (Microsoft basic data)
Partition unique GUID: 1B48ED44-1D14-47EA-B5BF-CBBA55AC3E2E
First sector: 2048 (at 1024.0 KiB)
Last sector: 125827071 (at 60.0 GiB)
Partition size: 125825024 sectors (60.0 GiB)
Attribute flags: 0000000000000000
Partition name: 'Microsoft basic data'
```

Type q to quit gdisk.

Q3) Identify the USB FAT file system using fsstat

Confirm you have the USBVolume1.dd file in your Forensics folder from Preparation 2 above.

Run ubuntu. Change to your Forensics folder.

(You may have to install The Sleuth Kit using apt-get to run fsstat and fls.)

Type fsstat USBVolume1.dd | grep -m30 .

Note the trailing dot. Confirm you see the MBR details for the disk partition. _ ___

Take a screen shot for the report. Yours may be different.

```
huynh@DESKTOP-LD37IOO:/mnt/c/Forensics_Huynh$ fsstat USBVolume1.dd | grep -m30 .
FILE SYSTEM INFORMATION
--------------------------------------------
File System Type: FAT16
OEM Name: MSDOS5.0
Volume ID: 0x5439a266
Volume Label (Boot Sector): NO NAME
Volume Label (Root Directory): FORENSIC F
File System Type Label: FAT16
Sectors before file system: 2048
File System Layout (in sectors)
Total Range: 0 - 40959
* Reserved: 0 - 1
** Boot Sector: 0
* FAT 0: 2 - 160
* FAT 1: 161 - 319
* Data Area: 320 - 40959
** Root Directory: 320 - 351
** Cluster Area: 352 - 40959
METADATA INFORMATION
--------------------------------------------
Range: 2 - 650246
Root Directory: 2
CONTENT INFORMATION
--------------------------------------------
Sector Size: 512
Cluster Size: 512
Total Cluster Range: 2 - 40609
FAT CONTENTS (in sectors)
--------------------------------------------
352-352 (1) -> EOF
```

What is the OEM Name? MSDOS5.0

What is the Volume Root Directory Label? 320-351

First FAT size in sectors = (end – start) = 2-160

Second FAT size in sectors = 161-319

Are the two FAT sizes the same? No

Why or why not? The smaller the partition, the smaller the cluster size and these partitions or FAT sizes goes up and so does the cluster size

Q4) Identify the FAT files using fls

Confirm you have the USBVolume1.dd file in your Forensics folder.

Run ubuntu. Change to your Forensics folder.

Type fls USBVolume1.dd | grep -m30 .

Confirm you see the files for the USB disk partition. _ ___

(You may have to install The Sleuth Kit using apt-get to run fls).

Take a screenshot for your report.

```
huynh@DESKTOP-LD37IOO:/mnt/c/Forensics_Huynh$ fls USBVolume1.dd
r/r 3:  FORENSIC F  (Volume Label Entry)
d/d 6:  System Volume Information
r/r 8:  C08InChp.dd
r/r 9:  cars.txt
r/r 10: cygwin1.dll
r/r 12: Flowers.txt
r/r * 14:       IMAG1672a.jpg
r/r 15: logo.gif
r/r 16: ls2.exe
r/r 19: MS Office Meta Data.jpg
r/r 21: Sample.docx
r/r 23: Sample.pdf
r/r 24: strings.exe
r/r * 27:       Trade_Secrets.txt
v/v 650243:     $MBR
v/v 650244:     $FAT1
v/v 650245:     $FAT2
V/V 650246:     $OrphanFiles
```

What is the inode for ls2.exe? 16

Note * indicates a deleted file.

What are the inodes of the deleted flies.? 14 and 27

Q5) Recover deleted files

To recover the deleted file; we use icat on the inode.

Use icat with the inode for Trade_Secrets.txt

Type icat <Image> <inode>

You should see the deleted file contents! (Your inode may be different.)

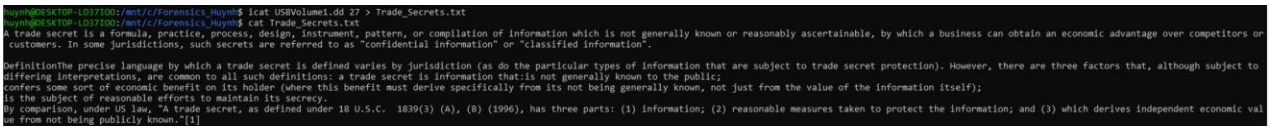
Take a screen shot of the command and the result.

```
huynh@DESKTOP-LD37IOO:/mnt/c/Forensics_Huynh$ icat USBVolume1.dd 27
A trade secret is a formula, practice, process, design, instrument, pattern, or compilation of information which is not generally known or reasonably ascertainable, by which a business can obtain an economic advantage over competitors or
customers. In some jurisdictions, such secrets are referred to as "confidential information" or "classified information".

DefinitionThe precise language by which a trade secret is defined varies by jurisdiction (as do the particular types of information that are subject to trade secret protection). However, there are three factors that, although subject to
differing interpretations, are common to all such definitions: a trade secret is information that:is not generally known to the public;
confers some sort of economic benefit on its holder (where this benefit must derive specifically from its not being generally known, not just from the value of the information itself);
is the subject of reasonable efforts to maintain its secrecy.
By comparison, under US law, "A trade secret, as defined under 18 U.S.C.  1839(3) (A), (B) (1996), has three parts: (1) information; (2) reasonable measures taken to protect the information; and (3) which derives independent economic val
ue from not being publicly known."[1]
```

We can now recover the deleted file. Type

icat <Image> <inode> > Trade_Secrets.txt



When will the technique fail to correctly recover a file?

The inode would have to be altered to fail to retrieve the file's contents. There are also instances where the damage to the hard drive is so severe that data recovery is not possible.

Q6) NTFS analysis with The Sleuth Kit

We will repeat one of the steps we used for USB FAT32. However, NTFS is more complex so we will see a different result.

Type fls USBVolume2.dd Confirm you see the files for the disk partition.

```
huynh@DESKTOP-LD37IOO:/mnt/c/Forensics_Huynh$ fls USBVolume2.dd
r/r 4-128-1:    $AttrDef
r/r 8-128-2:    $BadClus
r/r 8-128-1:    $BadClus:$Bad
r/r 6-128-4:    $Bitmap
r/r 7-128-1:    $Boot
d/d 11-144-4:   $Extend
r/r 2-128-1:    $LogFile
r/r 0-128-6:    $MFT
r/r 1-128-1:    $MFTMirr
r/r 9-128-8:    $Secure:$SDS
r/r 9-144-11:   $Secure:$SDH
r/r 9-144-14:   $Secure:$SII
r/r 10-128-1:   $UpCase
r/r 10-128-4:   $UpCase:$Info
r/r 3-128-3:    $Volume
r/r 38-128-1:   C08InChp.dd
r/r 38-128-3:   C08InChp.dd:Zone.Identifier
r/r 39-128-1:   cars.txt
r/r 39-128-3:   cars.txt:Zone.Identifier
r/r 40-128-1:   cygwin1.dll
r/r 40-128-3:   cygwin1.dll:Zone.Identifier
r/r 41-128-1:   Flowers.txt
r/r 41-128-3:   Flowers.txt:Zone.Identifier
r/r 43-128-3:   logo.gif
r/r 43-128-4:   logo.gif:Zone.Identifier
r/r 44-128-1:   ls2.exe
r/r 44-128-3:   ls2.exe:Zone.Identifier
r/r 45-128-1:   MS Office Meta Data.jpg
r/r 45-128-3:   MS Office Meta Data.jpg:Zone.Identifier
r/r 46-128-1:   Sample.docx
r/r 46-128-3:   Sample.docx:Zone.Identifier
r/r 47-128-1:   Sample.pdf
r/r 47-128-3:   Sample.pdf:Zone.Identifier
r/r 48-128-1:   strings.exe
r/r 48-128-3:   strings.exe:Zone.Identifier
d/d 36-144-1:   System Volume Information
-/r * 42-128-1: IMAG1672a.jpg
-/r * 42-128-3: IMAG1672a.jpg:Zone.Identifier
-/r * 49-128-3: Trade_Secrets.txt
-/r * 49-128-4: Trade_Secrets.txt:Zone.Identifier
V/V 256:        $OrphanFiles
```

Take a screenshot for your report.

Identify the ls2.exe inode 44-128-3 (44 is the inode)

Note the deleted files. inodes

Week 09 Disk Analysis Report

42-128-1(42 is the inode) and 49-128-3 (49 is the inode) (yours will be different)

Which metadata items in the fls display may be of forensic interest? There are metadata files that start with $.

Explain why. These types of files could be of interest on how certain applications and system is running. As you can see there is a logfile which these files of interests can potentially give additional evidence to what the user was doing.

Close your cmd window and remove your USB stick when finished.

48436/32309

Tutorial Week 10 Law Report

Name: Huynh Lam Student ID: 13264763 Date: 17/10/2021 Activity No.: Cmp1/03

Reading	Questions
Week 10 Reading document **1) Evidence ACPO.pdf** **2) Forensic Legal issues.pdf**	Examine the documents below in this week's readings and answer the questions provided. **1) Evidence ACPO.pdf** What are the four principles of computer-based electronic evidence? • Principle 1: No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be relied upon in court. • Principle 2: In circumstances where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions. • Principle 3: An audit trail or other record of all processes applied to computer-based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result. • Principle 4: The person in charge of the investigation (the case officer) has overall responsibility for ensuring that the law and these principles are adhered to. Give examples of how to enforce these principles What items of information should be recovered using a scripted approach (running a set of command line tools via a script)? • process listings. • service listings. • system information. • logged on & registered users. • network information including listening ports, open ports, closing ports. • ARP (address resolution protocol) cache • auto-start information. • registry information. • a binary dump of memory What is the difference between the examination process and the analysis phase? • The examination process is to make evidence visible and explain it's original and significance. First, it should document the content and state of evidence in totality. Documentation allows all parties to discover what is contained in evidence. Finding hidden and obscured data is also part of the process. Once all the information is visible the process of data reduction

3) Exclusionary rule	begins. Finally filtering out what evidence would prove useful for the investigation. • This phase differs from examination in that it looks at the product of the examination for its significance and probative value to the case. The examination is a technical review that is the province of the forensic practitioner.
	2) Forensic Legal issues.pdf **Jurisdiction of case.** Does a Texas Court have the right to assert its jurisdiction over a British Columbian resident? • The Texas Court had no right to assert its jurisdiction over a British Columbian resident
4) D F-issues-in-civil-proceedings.pdf	**Search and seizure of digital evidence** Explain how the forensic investigator needs to consider the privacy of a culprit in any search. • During the initial process of forensic investigation, the use of an improper methodology or unlawful search and seizure can negatively affect the admissibility of the evidence. The forensic investigator must therefore ensure that the privacy of a culprit is not infringed in any search. The legal procedure for searching and seizing computers with a warrant largely mirrors the legal framework for other forensic investigations. How can you detect when a plaintiff fabricates an email by pasting a legitimate header and altering the Subject line? • To find if the emails have been fabricated, you need to look at the email header. The header contains critical components of every email: From, To, Date, and Subject, as well as detailed information about where the email came from and how it was routed to you. Importantly, it also contains the results of the verification process your email provider used to determine if the sending server has permission to send using that domain.
	3) Exclusionary rule Explain the Fruit of the Poisoned Tree' principle used to exclude certain evidence. • In strict cases, when an illegal action is used by police/prosecution to gain any incriminating result, all evidence whose recovery stemmed from the illegal action.

	Now the evidence acquired illegally can be thrown out from a jury An illegal (not done properly) step in an investigation may void all following evidence. How can you minimise this? • The team that is doing the investigation should follow the regulations and guidelines when submitting and obtaining evidence. As investigators are quite good at their jobs and assumptions made tend to be quite correct they will need to obtain evidence legally. By obtaining warrants and proper consent to recording they are able to achieve obtaining evidence legally. A person may track their spouse's activity to gain evidence for divorce proceedings. Name two activities that would be of interest and the type of malware used to gain the evidence. • (GPS) tracking information and malware would be spyware • Text messages and the malware of interest would be keylogging How would the tracked person suspect such a tracker was being used? • The person being tracked could potentially take it to a digital forensic officer and they can perform their analysis such as memory analysis to find hidden programs silently running in the background. There could be a hint of spying as unusual programs installed or browser history/file history being accessed without the primary user opening these applications. How could the victim's attorney gain corroborating evidence of this tracking activity? • The person could look into the person tracking information such as monitoring site's logs or user records to show use by the perpetrator, or the credit card history to show the purchase of the monitoring application. • This may include remotely activating web cameras that are built into computers and mobile devices. Some cameras have an activation light, which indicates when a camera is being used. • The device that is suspected to have tracking activity can be presented to a digital forensic officer where that person can perform malware analysis on the device.