48436/32309

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

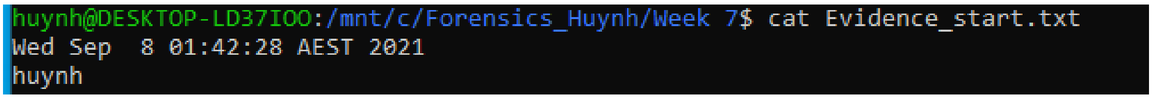
Start ubuntu.

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
```

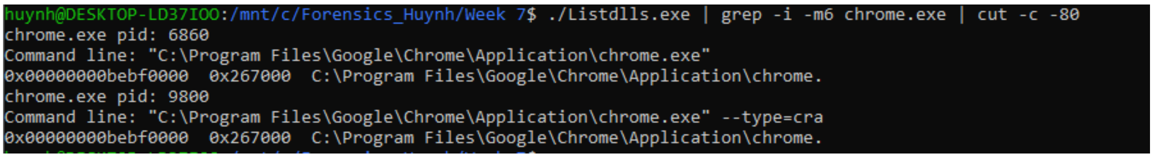
Q2) Check Chrome

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.



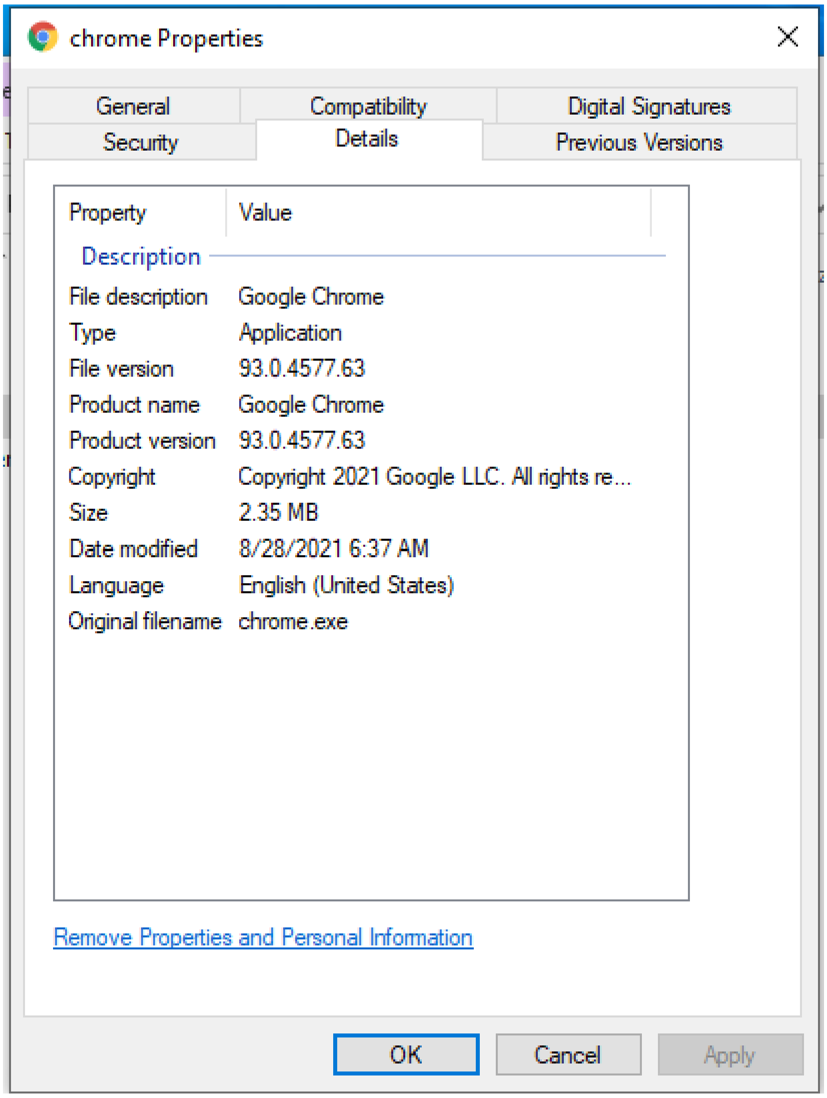
```
huynh@DESKTOP-LD37IOO:/mnt/c/Forensics_Huynh/Week 7$ ./Listdlls.exe | grep -i -m6 chrome.exe | cut -c -80
chrome.exe pid: 6860
Command line: "C:\Program Files\Google\Chrome\Application\chrome.exe"
0x00000000bebf0000  0x267000  C:\Program Files\Google\Chrome\Application\chrome.
chrome.exe pid: 9800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

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.



Property	Value
Description	
File description	Google Chrome
Type	Application
File version	93.0.4577.63
Product name	Google Chrome
Product version	93.0.4577.63
Copyright	Copyright 2021 Google LLC. All rights re...
Size	2.35 MB
Date modified	8/28/2021 6:37 AM
Language	English (United States)
Original filename	chrome.exe

Q3) Check Services

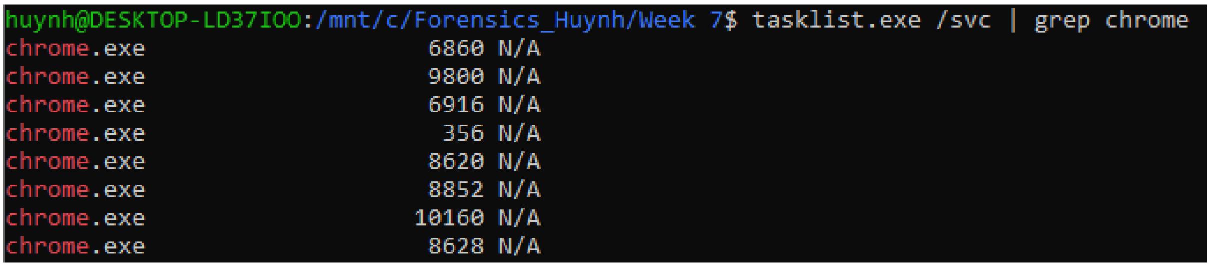
To see the processes running services we use tasklist.exe /svc

Confirm you are running Chrome.

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

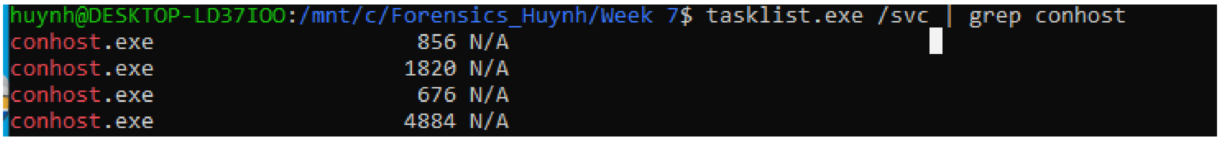
Take a screenshot of the result

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

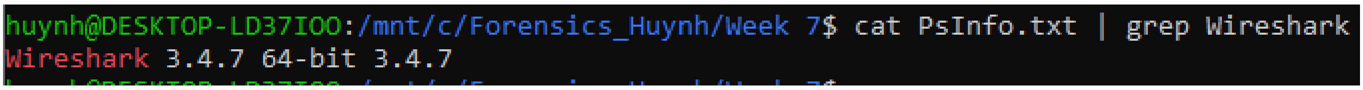
What is the size of the Hard Disk C:\ Drive and the % free?

- 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
```

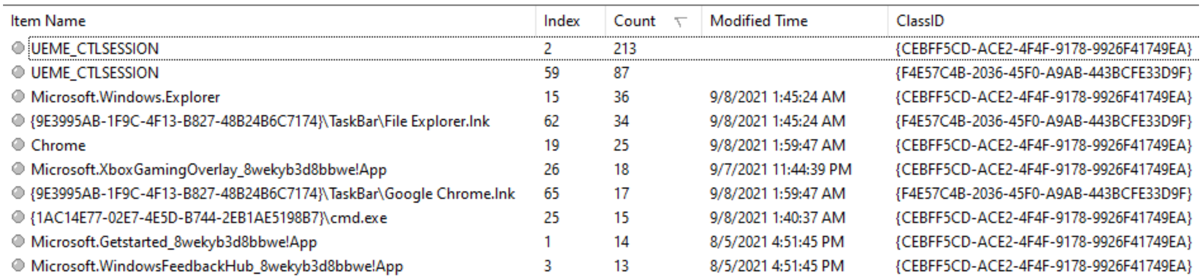
What is the Wireshark version? 3.4.7

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.