**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.



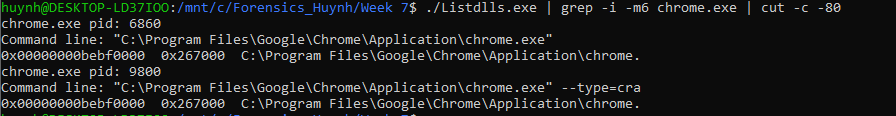
Q2) Check Chrome

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.

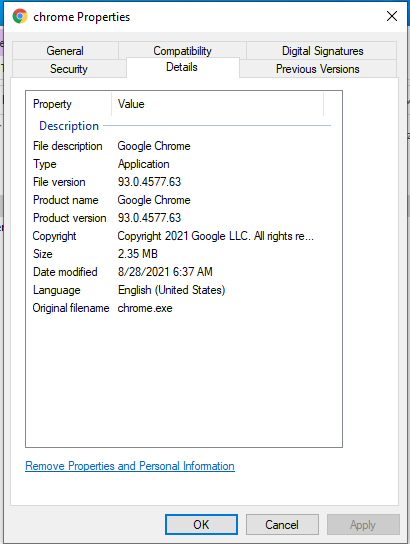


Locate the chrome.exe file location shown using File Explorer. Right click and select properties.

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

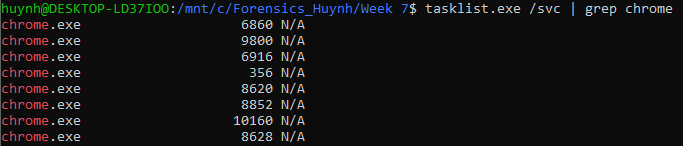
To see the processes running services we use tasklist.exe /svc

Confirm you are running Chrome.

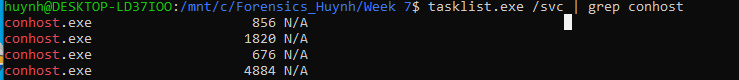
What is a cmdline to ONLY show the PIDs in use by chrome as a service?

Take a screenshot of the result

Command: tasklist.exe /svc | grep chrome



Take another screenshot showing the conhost service



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.



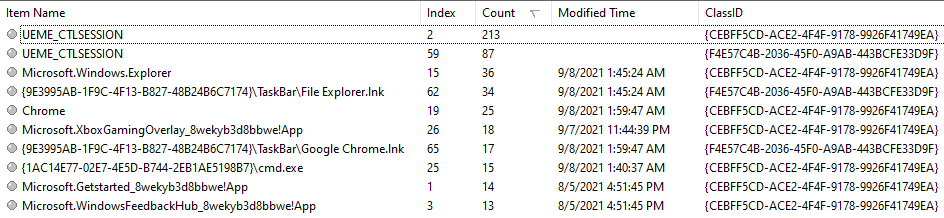
What is the Wireshark version? 3.4.7

# 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.



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.