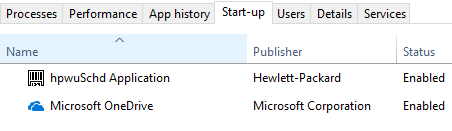
**Name: Huynh Lam Student ID: 13264763 Date: 11/09/2021 Activity No.: Cmp1/03**

**Due Date:** Three days after the lab.

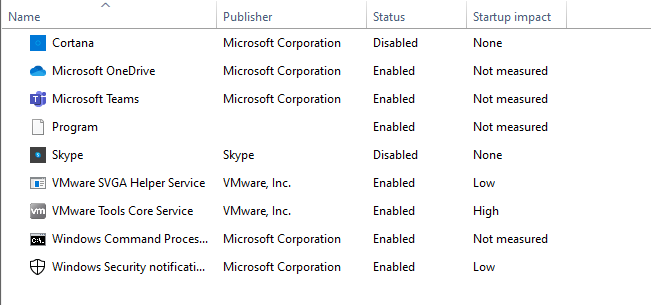
# Q1) Registry Startup items - Windows

To find all startup programs, use Task Manager.

Select the Startup tab.



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

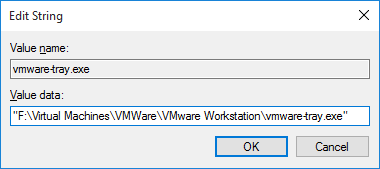


* Cortana is Windows virtual assistant that is able to perform tasks or assist the user with inquiries
* Microsoft OneDrive is is a file hosting service and synchronisation service operated by Microsoft as part of its web version of Office
* Microsoft Teams proprietary business communication platform 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

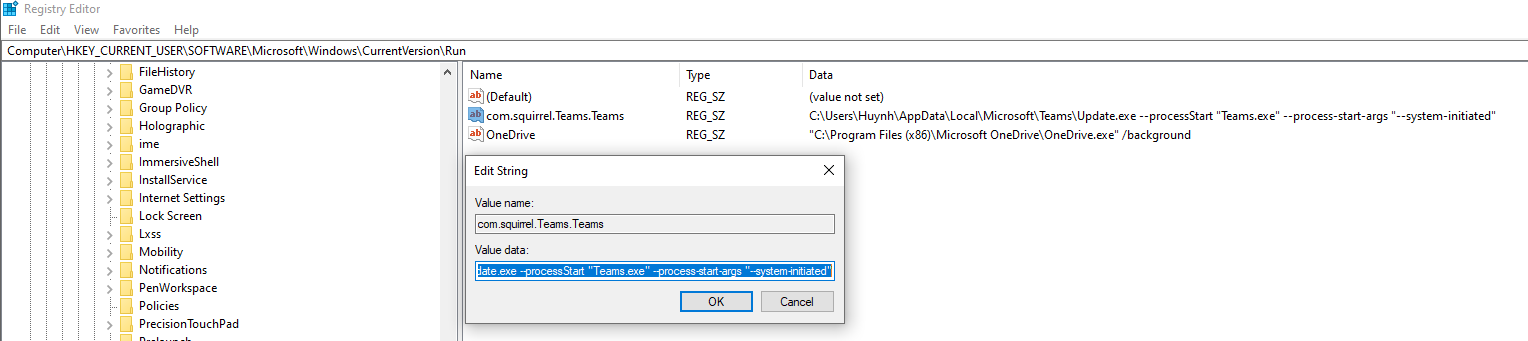
Select the first key name. (Exclude the default) Right click and select modify.

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.



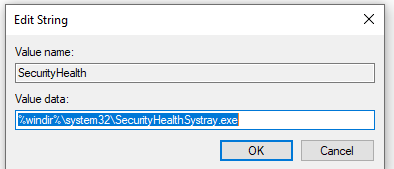
* The purpose of this item is to start Microsoft Teams and starting this Microsoft teams on startup allows it to automatically update whenever it is ran

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.

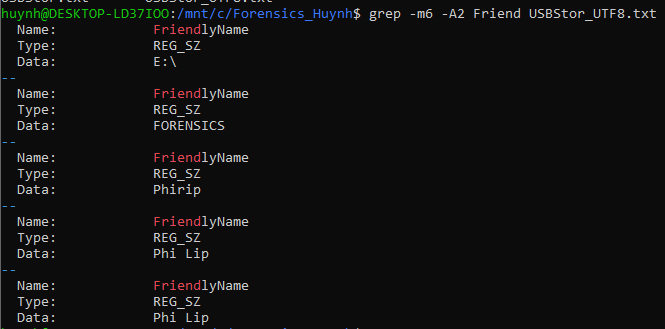
Now use grep to search the file for the keyword Friend.

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

1. **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.

1. 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.

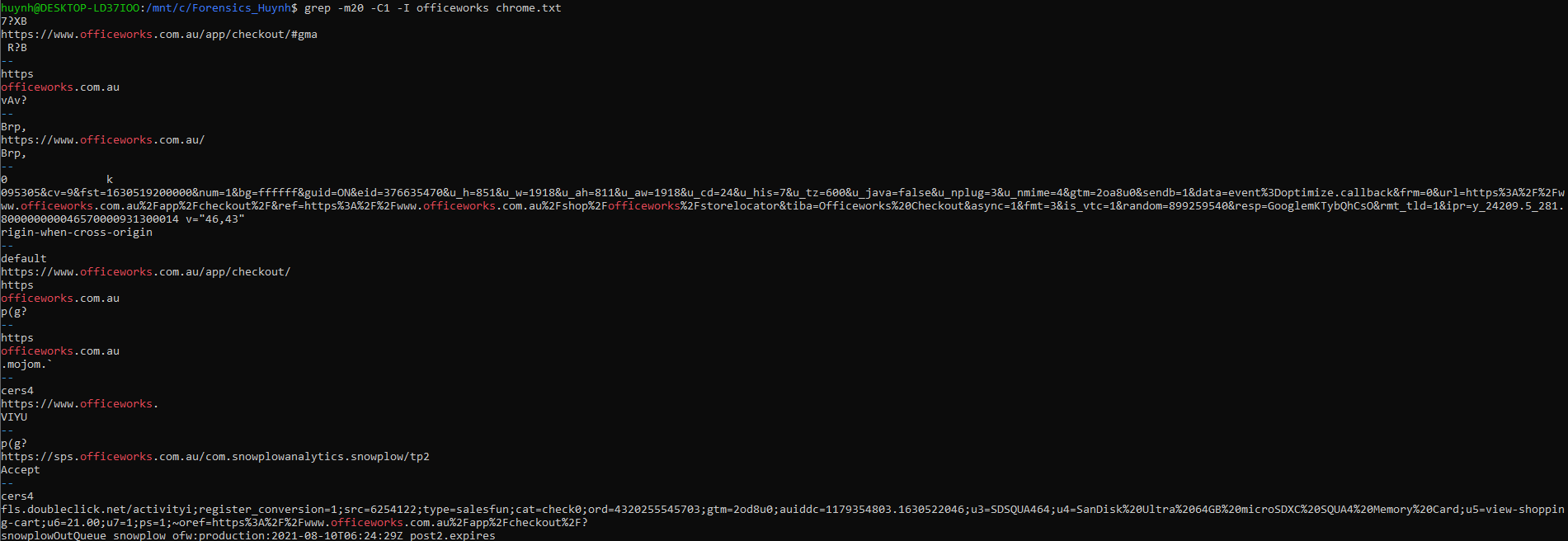
3C1) Look for the keyword cookies.

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

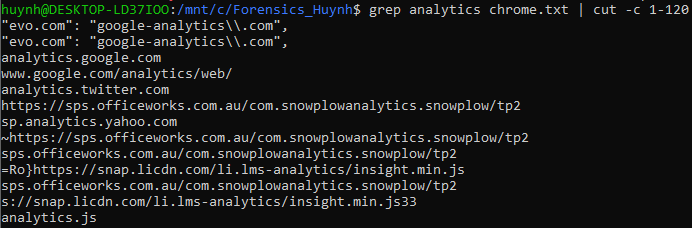
Repeat for the other chrome dump txt files.

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

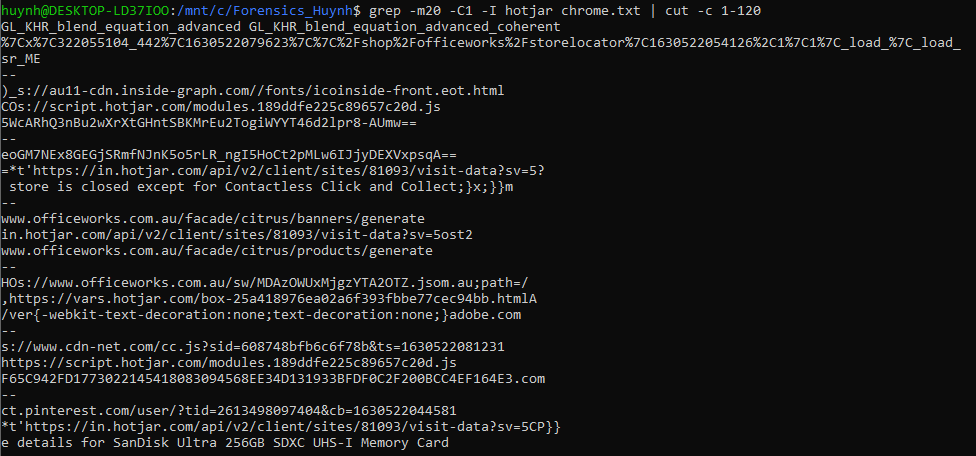
* There is snow analytics seen in this screenshot using the command above



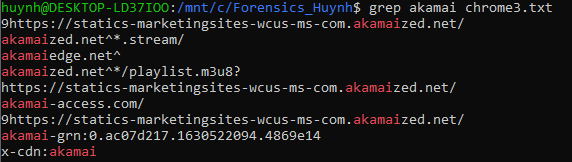
* We can see that yahoo and snowplow analytics already shows in Officeworks



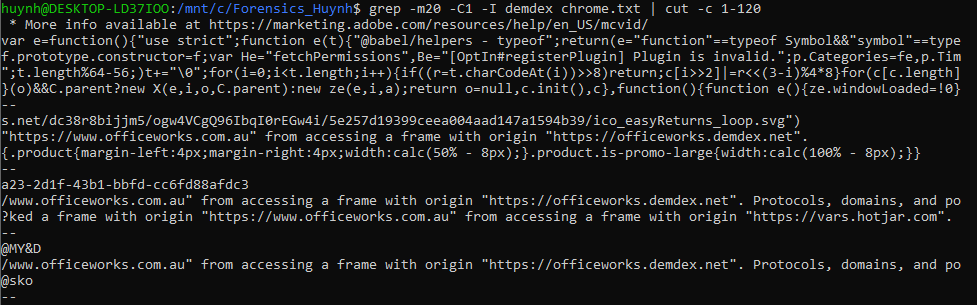
* HotJar and Inside-graph cookies



* CDN Hosting analytics of akamai



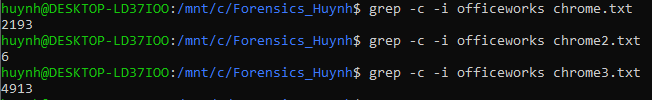
* Demdex behavioral Cookies



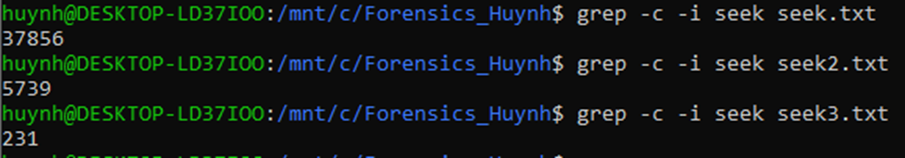
3C2) Show here the Count of the hits for the word Officeworks and the word Seek. Comment on the result.

* 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



* Count of Seek



3C3:

Search for your keywords.

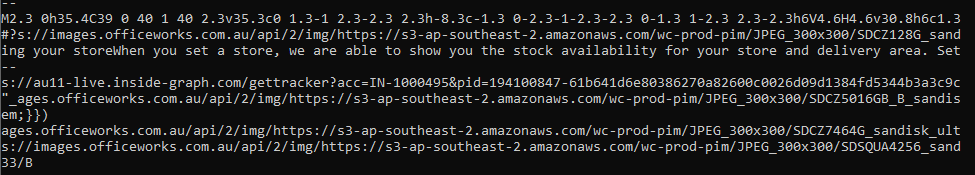
For Officeworks - SanDisk, USB Pen Drive, Glebe.

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

Take a Screen shot – only the important stuff!.

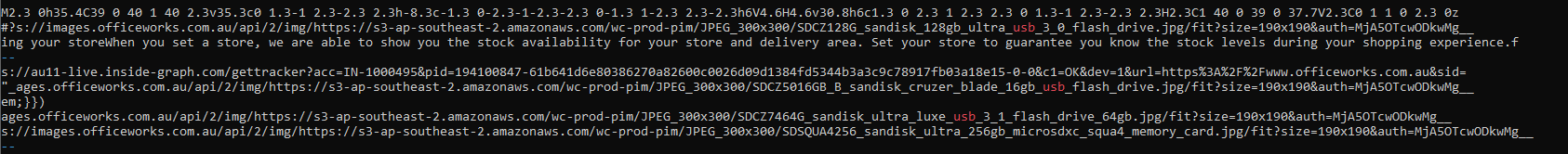
* SanDisk

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

