



**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.

Processes	Performance	App history	Start-up	Users	Details	Services
Name			Publisher	Status		
 hpwuSchd Application			Hewlett-Packard	Enabled		
 Microsoft OneDrive			Microsoft Corporation	Enabled		

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 Processes	Microsoft Corporation	Enabled	Not measured
 Windows Security notification	Microsoft Corporation	Enabled	Low

- Cortana is Windows virtual assistant that is able to perform tasks or assist the user with inquiries
- Microsoft OneDrive 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

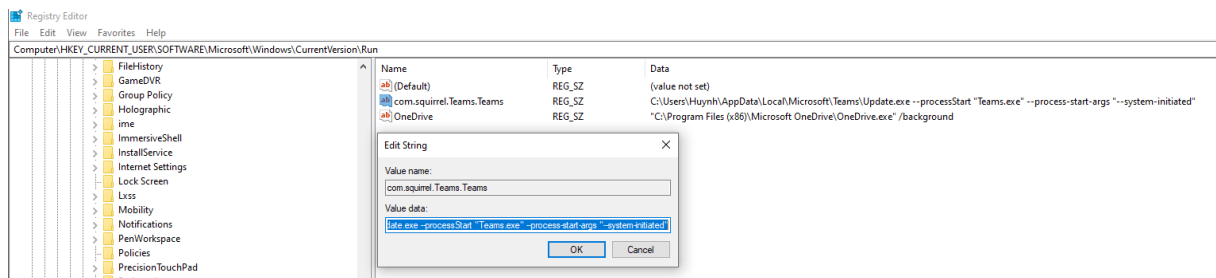
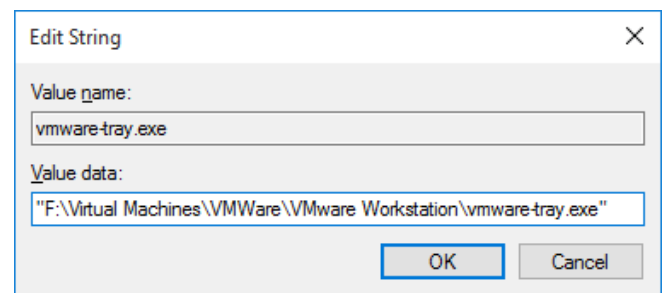
Select the first key name. (Exclude the default)  
Right click and select **modify**.

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.



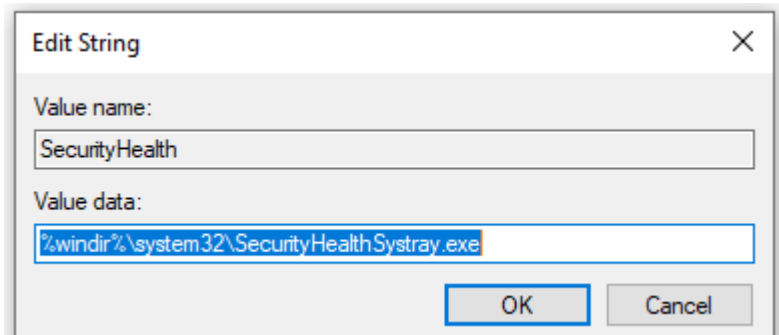
- The purpose of this item is to start Microsoft Teams and starting this Microsoft teams on startup allows it to automatically update whenever it is ran

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.

```

huynh@DESKTOP-LD37I00:/mnt/c/Forensics_Huynh$ grep -m6 -A2 Friend USBStor_UTF8.txt
Name:      FriendlyName
Type:      REG_SZ
Data:      E:\
--
Name:      FriendlyName
Type:      REG_SZ
Data:      FORENSICS
--
Name:      FriendlyName
Type:      REG_SZ
Data:      Phirip
--
Name:      FriendlyName
Type:      REG_SZ
Data:      Phi Lip
--
Name:      FriendlyName
Type:      REG_SZ
Data:      Phi Lip

```

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-LD37I00:/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

```
huyhng@DESKTOP-LD37100: /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(){if("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]}<<((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=10}
s.net/dc38r8bijm5/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-cc6fd88afd3
/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-LD37I00:/mnt/c/Forensics_Huynh$ grep -c -i officeworks chrome.txt
2193
huynh@DESKTOP-LD37I00:/mnt/c/Forensics_Huynh$ grep -c -i officeworks chrome2.txt
6
huynh@DESKTOP-LD37I00:/mnt/c/Forensics_Huynh$ grep -c -i officeworks chrome3.txt
4913
```

- Count of Seek

```
huynh@DESKTOP-LD37I00:/mnt/c/Forensics_Huynh$ grep -c -i seek seek.txt
37856
huynh@DESKTOP-LD37I00:/mnt/c/Forensics_Huynh$ grep -c -i seek seek2.txt
5739
huynh@DESKTOP-LD37I00:/mnt/c/Forensics_Huynh$ grep -c -i seek seek3.txt
231
```

3C3:

Search for your keywords.

For Officeworks - **SanDisk, USB Pen Drive, Glebe.**

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

Take a Screen shot – only the important stuff!.

- SanDisk

The cookies with the SanDisk are inside-graph cookies

```
--
M2.3 0h35.4C39 0 40 1 40 2.3v35.3c0 1.3-1 2.3-2.3 2.3h-8.3c-1.3 0-2.3-1-2.3-2.3 0-1.3 1-2.3 2.3-2.3h6V4.6H4.6v30.8h6c1.3
#?s://images.officeworks.com.au/api/2/img/https://s3-ap-southeast-2.amazonaws.com/wc-prod-pim/JPEG_300x300/SDCZ128G_sand
ing your storeWhen you set a store, we are able to show you the stock availability for your store and delivery area. Set
--
s://au11-live.inside-graph.com/gettracker?acc=IN-1000495&pid=194100847-61b641d6e80386270a82600c0026d09d1384fd5344b3a3c9c
"ages.officeworks.com.au/api/2/img/https://s3-ap-southeast-2.amazonaws.com/wc-prod-pim/JPEG_300x300/SDCZ5016GB_B_sandis
em;)))
ages.officeworks.com.au/api/2/img/https://s3-ap-southeast-2.amazonaws.com/wc-prod-pim/JPEG_300x300/SDCZ7464G_sandisk_ult
s://images.officeworks.com.au/api/2/img/https://s3-ap-southeast-2.amazonaws.com/wc-prod-pim/JPEG_300x300/SDSQUA4256_sand
33/B
```

- USB Pen Drive

Cookies are also the same and there are inside-graph

```
M2.3 0h35.4C39 0 40 1 40 2.3v35.3c0 1.3-1 2.3-2.3 2.3h-8.3c-1.3 0-2.3-1-2.3-2.3 0-1.3 1-2.3 2.3-2.3h6V4.6H4.6v30.8h6c1.3 0 2.3 1 2.3 2.3 0 1.3-1 2.3-2.3 2.3h2.3c1 40 0 39 0 37.7V2.3C0 1 1 0 2.3 0z
#?s://images.officeworks.com.au/api/2/img/https://s3-ap-southeast-2.amazonaws.com/wc-prod-pim/JPEG_300x300/SDCZ128G_sandisk_128gb_ultra_usb_3.0_flash_drive.jpg/fit?size=190x190&auth=MJAS0Tcw0DkwMg
ing your storeWhen you set a store, we are able to show you the stock availability for your store and delivery area. Set your store to guarantee you know the stock levels during your shopping experience.f
s://au11-live.inside-graph.com/gettracker?acc=IN-1000495&pid=194100847-61b641d6e80386270a82600c0026d09d1384fd5344b3a3c9c78017fbb3a18e15-0-0&c1=OK&dev=1&url=https%3A%3F%2Fwww.officeworks.com.au&cid=
"ages.officeworks.com.au/api/2/img/https://s3-ap-southeast-2.amazonaws.com/wc-prod-pim/JPEG_300x300/SDCZ5016GB_B_sandisk_cruzer_blade_16gb_usb_flash_drive.jpg/fit?size=190x190&auth=MJAS0Tcw0DkwMg
em;)))
ages.officeworks.com.au/api/2/img/https://s3-ap-southeast-2.amazonaws.com/wc-prod-pim/JPEG_300x300/SDCZ7464G_sandisk_ultra_luxe_usb_3.1_flash_drive_64gb.jpg/fit?size=190x190&auth=MJAS0Tcw0DkwMg
s://images.officeworks.com.au/api/2/img/https://s3-ap-southeast-2.amazonaws.com/wc-prod-pim/JPEG_300x300/SDSQUA4256_sandisk_ultra_256gb_microsdxc_squa4_memory_card.jpg/fit?size=190x190&auth=MJAS0Tcw0DkwMg
```

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

```
huyhnh@DESKTOP-LD37100:/mnt/c/Forensics_Huynh$ grep -m20 -C1 -I glebe chrome.txt
M509.8 45015.4-13.7-13.1-33.5h11.7l6.8 20.8 7.6-20.8h11.3l-19 47.2h-10.7z
s://www.officeworks.com.au/catalogue-app/api/locations/?location=glebe8643c
sh#A
--
_80174tectiona
_owson=glebe
mmmmmmlli
--
ultra
atalogue-app/api/locations/?location=glebe
s://assets.citrusad.net/citrusjs/1.2.0/citrus.js
```