CREATING A DISK IMAGE AND INVESTIGATING IT USING AUTOPSY

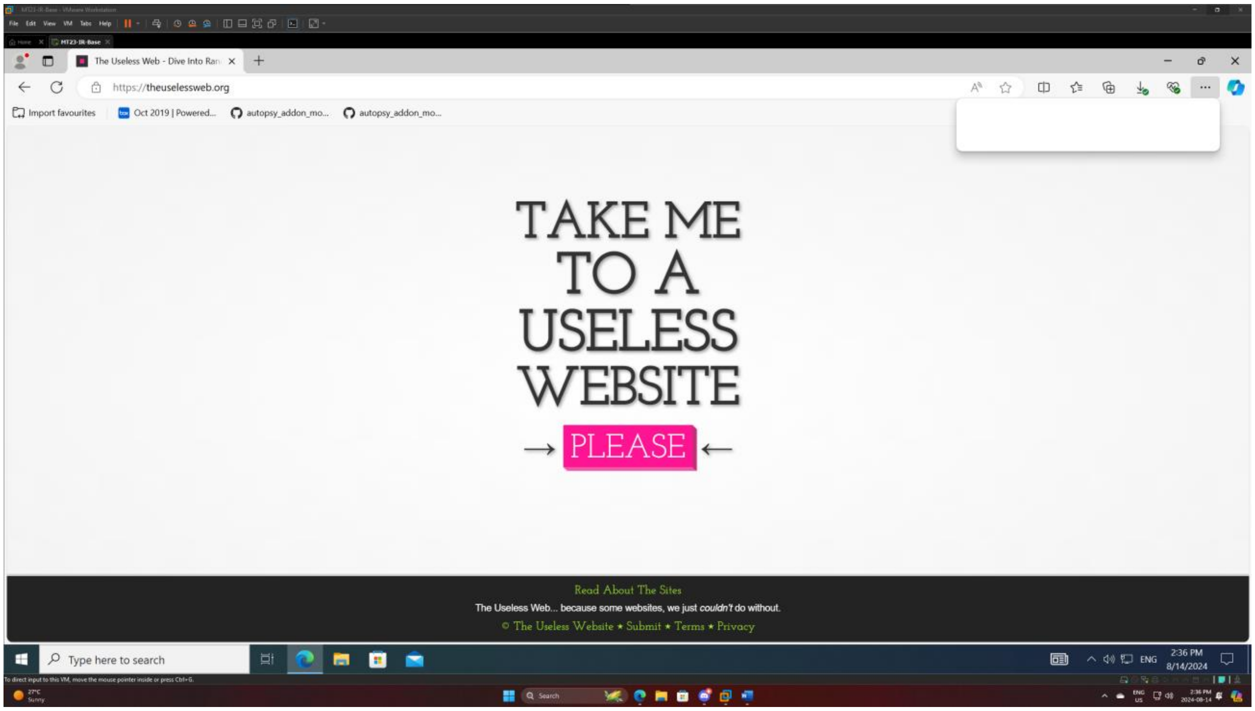
Jordan Patterson

2024

Table of Contents

Virtual Machine preparation:

I Began this assignment by visiting the 10 websites provided in the assignment instructions.



TAKE ME TO A USELESS WEBSITE

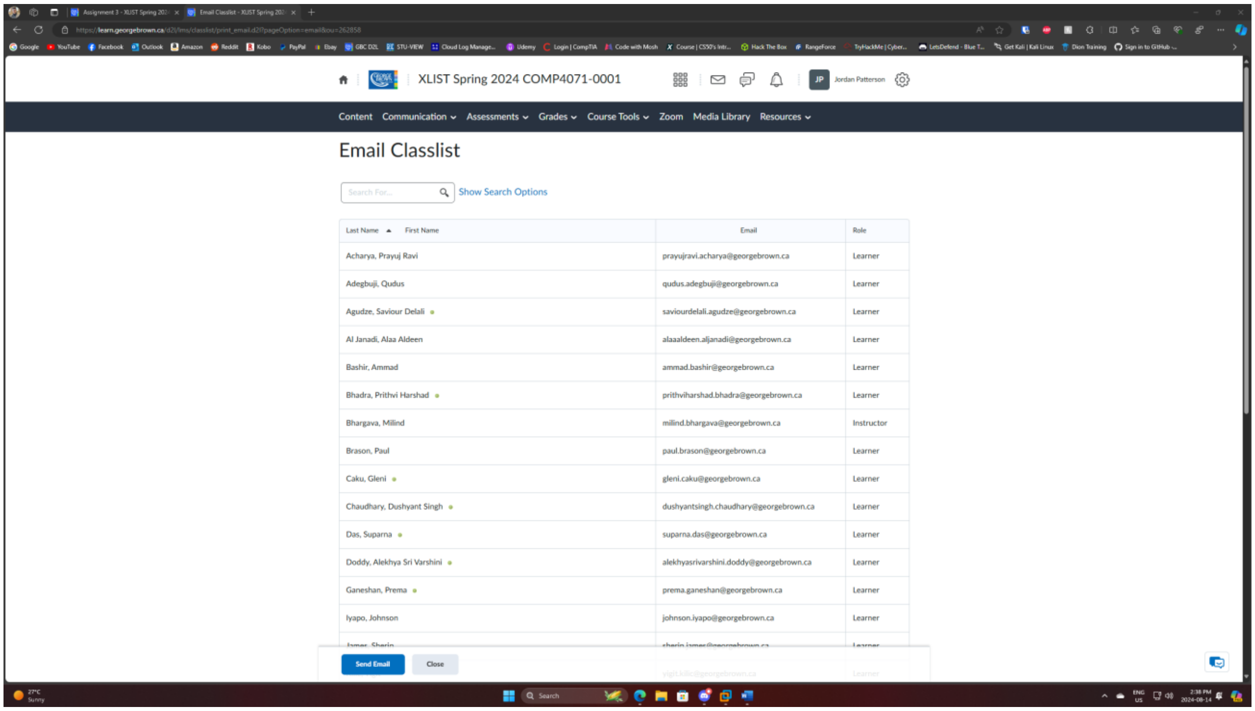
→ PLEASE ←

Read About The Sites

The Useless Web... because some websites, we just *couldn't* do without.

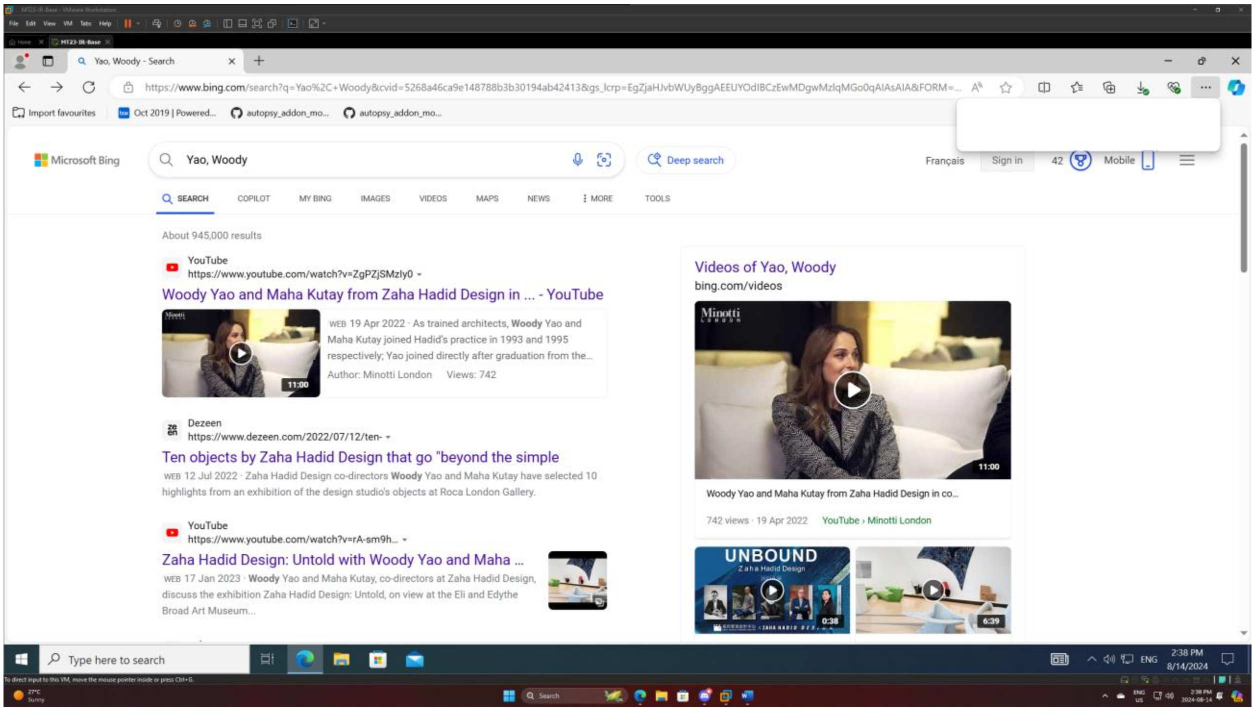
© The Useless Website ★ Submit ★ Terms ★ Privacy

Once all 10 sites were visited, I procured a list of all of my classmates names from D2L and searched for them each one at a time and visited the first 5 search results for each classmate.



Email Classlist

Last Name ▲ First Name	Email	Role
Acharya, Prayuj Ravi	prayujravi.acharya@georgebrown.ca	Learner
Adegbuji, Qudus	qudus.adegbuji@georgebrown.ca	Learner
Agudze, Saviour Delali ●	saviourdelali.agudze@georgebrown.ca	Learner
Al Janadi, Alaa Aldeen	alaaaldeen.aljanadi@georgebrown.ca	Learner
Bashir, Ammad	ammad.bashir@georgebrown.ca	Learner
Bhadra, Prithvi Harshad ●	prithviharshad.bhadra@georgebrown.ca	Learner
Bhargava, Milind	milind.bhargava@georgebrown.ca	Instructor
Brason, Paul	paul.brason@georgebrown.ca	Learner
Caku, Gleni ●	gleni.caku@georgebrown.ca	Learner
Chaudhary, Dushyant Singh ●	dushyantsingh.chaudhary@georgebrown.ca	Learner
Das, Suparna ●	suparna.das@georgebrown.ca	Learner
Doddy, Alekhya Sri Varshini ●	alekhyasrivarshini.doddy@georgebrown.ca	Learner
Ganeshan, Prema ●	prema.ganeshan@georgebrown.ca	Learner
Iyapo, Johnson	johnson.iyapo@georgebrown.ca	Learner
James, Sherin	sherin.james@georgebrown.ca	Learner
[illegible]	yigit.kilic@georgebrown.ca	Learner



About 945,000 results

YouTube
https://www.youtube.com/watch?v=ZgPZjSMzIy0
Woody Yao and Maha Kutay from Zaha Hadid Design in ... - YouTube
WEB 19 Apr 2022 · As trained architects, **Woody** Yao and Maha Kutay joined Hadid's practice in 1993 and 1995 respectively; Yao joined directly after graduation from the...
Author: Minotti London Views: 742

Dezeen
https://www.dezeen.com/2022/07/12/ten-
Ten objects by Zaha Hadid Design that go "beyond the simple
WEB 12 Jul 2022 · Zaha Hadid Design co-directors **Woody** Yao and Maha Kutay have selected 10 highlights from an exhibition of the design studio's objects at Roca London Gallery.

YouTube
https://www.youtube.com/watch?v=rA-sm9h...
Zaha Hadid Design: Untold with Woody Yao and Maha ...
WEB 17 Jan 2023 · **Woody** Yao and Maha Kutay, co-directors at Zaha Hadid Design, discuss the exhibition Zaha Hadid Design: Untold, on view at the Eli and Edythe Broad Art Museum...

Videos of Yao, Woody
bing.com/videos
Woody Yao and Maha Kutay from Zaha Hadid Design in co...
742 views · 19 Apr 2022 YouTube › Minotti London

I then visited Phishtank.org, navigated to their phish search section, and visited the first 10 websites that were validated as phishing and still online.

All sites visited:

https://docs.google.com/presentation/d/1wRmE87a5ZYfMlCs87z_VUyvMkBQyiiBC-Ehep6B-U2w/pub?start=false&loop=false&delayms=3000&slide=id.p

http://validacion01020.serv00.net

https://onlinegtcgtq.netlify.app/

https://notontop.com/extracte_wordprees/flbigsar/affinity-access/ss.html

https://docs.google.com/presentation/d/e/2PACX-1vQ2jnybVRYpr1ValOAVcoxIJ2xOt9RH7uNhVZ1TY00_Ag3LZK1KZ-HwSueffnq62cBjQUBIfU_RBKYK/pub?start=false&loop=false&delayms=3000&slide=id.p

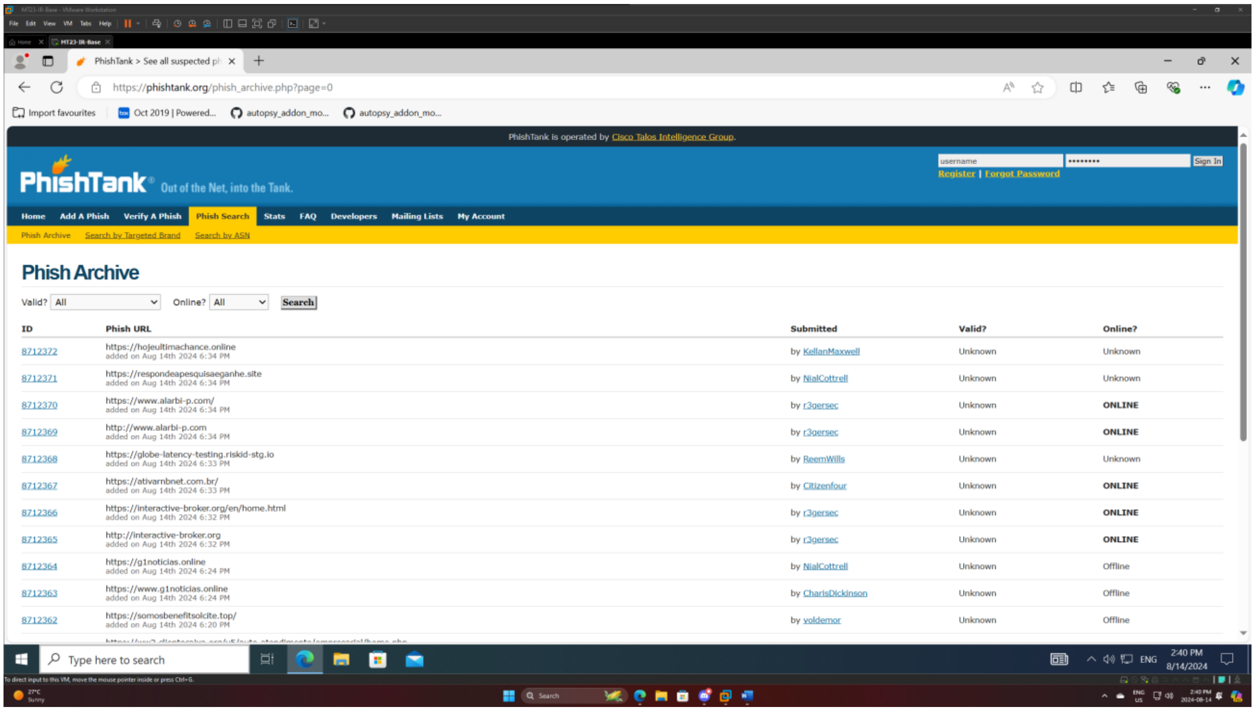
https://7739707.weebly.com/

https://docs.google.com/presentation/d/1McJ1lzI94YhSLQarmYOmSEv5JdUtDGCWLnK5n9y-hfs/pub?start=false&loop=false&delayms=3000&pli=1&slide=id.p

https://bonusnot.com/s/vKmul

https://xazjm.hp.peraichi.com/

https://02i1yah030ei-i9i1oi2-winios12-ios19.netlify.app/



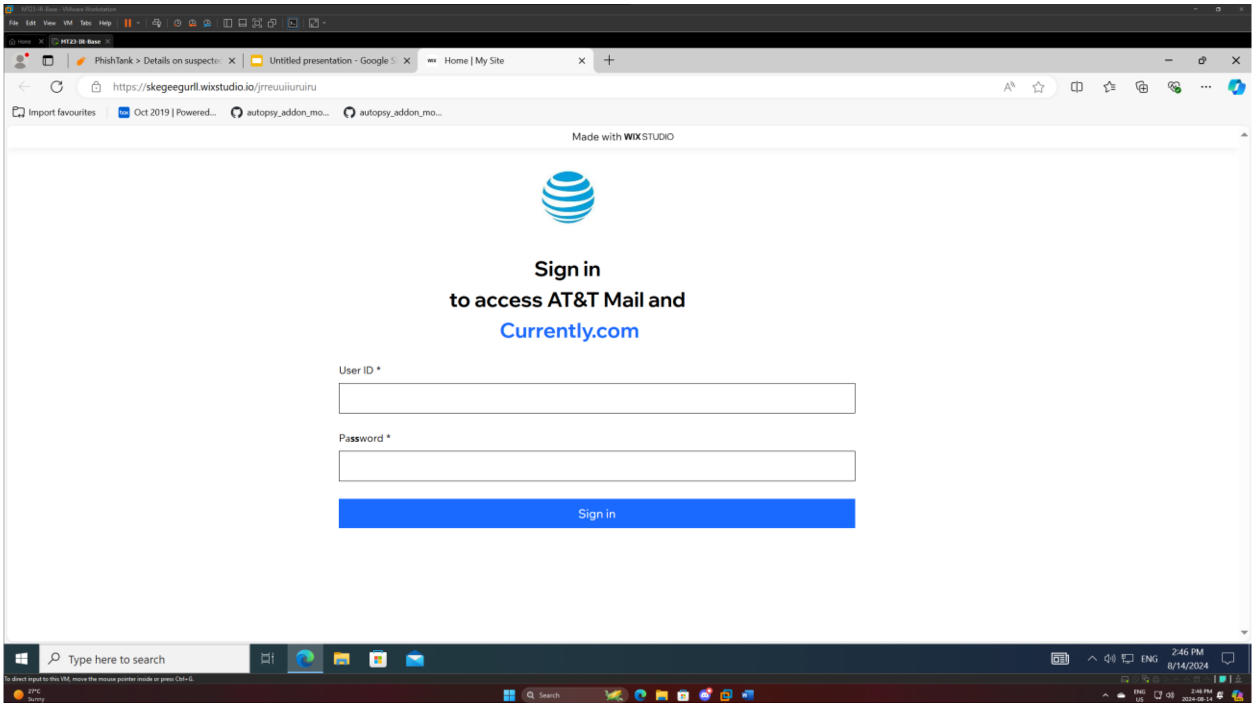
Phish Archive

Valid? All Online? All Search

ID	Phish URL	Submitted	Valid?	Online?
8712372	https://hojeultimachance.online added on Aug 14th 2024 6:34 PM	by KellanMaxwell	Unknown	Unknown
8712371	https://respondeapesquisaeganhe.site added on Aug 14th 2024 6:34 PM	by NialCottrell	Unknown	Unknown
8712370	https://www.alarbi-p.com/ added on Aug 14th 2024 6:34 PM	by r3gersec	Unknown	**ONLINE**
8712369	http://www.alarbi-p.com added on Aug 14th 2024 6:34 PM	by r3gersec	Unknown	**ONLINE**
8712368	https://globe-latency-testing.riskid-stg.io added on Aug 14th 2024 6:33 PM	by ReemWills	Unknown	Unknown
8712367	https://ativarnbnet.com.br/ added on Aug 14th 2024 6:33 PM	by Citizenfour	Unknown	**ONLINE**
8712366	https://interactive-broker.org/en/home.html added on Aug 14th 2024 6:32 PM	by r3gersec	Unknown	**ONLINE**
8712365	http://interactive-broker.org added on Aug 14th 2024 6:32 PM	by r3gersec	Unknown	**ONLINE**
8712364	https://g1noticias.online added on Aug 14th 2024 6:24 PM	by NialCottrell	Unknown	Offline
8712363	https://www.g1noticias.online added on Aug 14th 2024 6:24 PM	by CharisDickinson	Unknown	Offline
8712362	https://somosbenefitsolcite.top/ added on Aug 14th 2024 6:20 PM	by voldemor	Unknown	Offline

If any site required personal information or sign-in credentials, I generated them using https://www.fakenamegenerator.com/

Example of a phishing site that was visited during this exercise:


PhishTank > Details on suspecte
Untitled presentation - Google S
Home | My Site
https://skegeegurll.wixstudio.io/jrreuuiiuruiru
Import favourites
Oct 2019 | Powered...
autopsy_addon_mo...
autopsy_addon_mo...
Made with WIX STUDIO
Type here to search
2:46 PM
8/14/2024
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

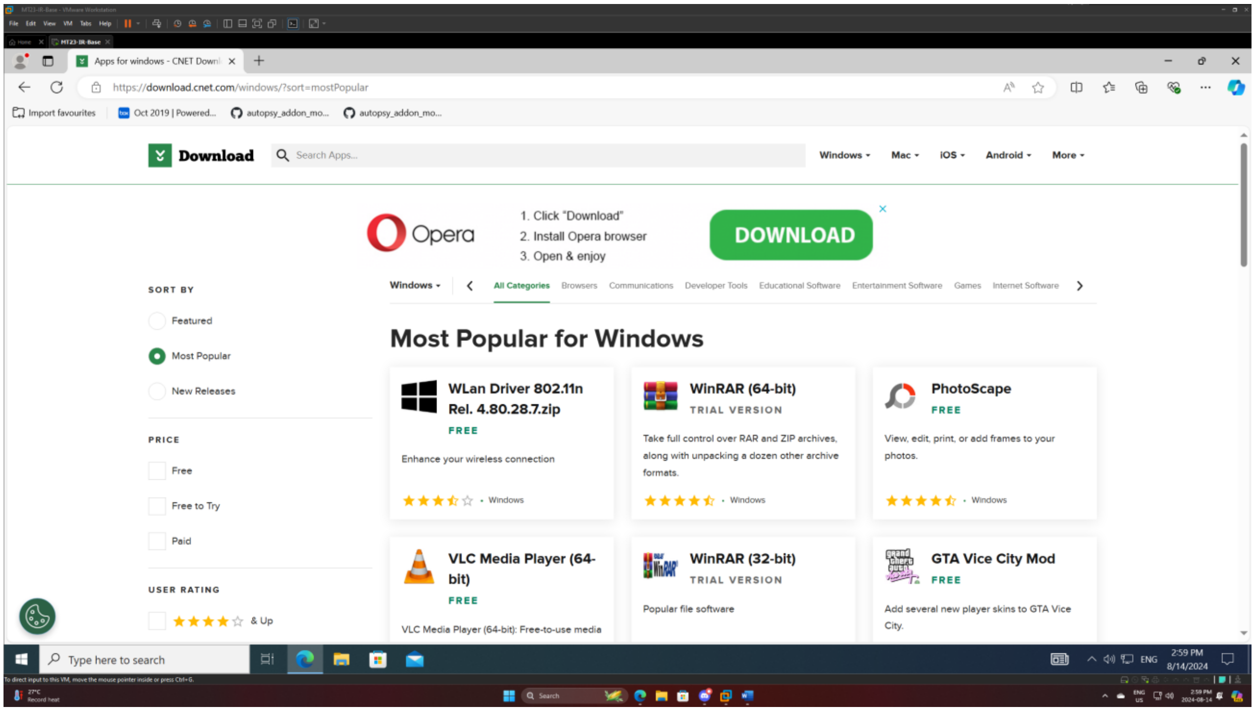
Sign in
to access AT&T Mail and
Currently.com

User ID *

Password *

Sign in

Once this task was completed, I visited the website https://download.cnet.com/windows/?sort=mostPopular and then select and downloaded10 non-security related applications.



Most Popular for Windows

WLan Driver 802.11n Rel. 4.80.28.7.zip
FREE
Enhance your wireless connection
Windows

WinRAR (64-bit)
TRIAL VERSION
Take full control over RAR and ZIP archives, along with unpacking a dozen other archive formats.
Windows

PhotoScape
FREE
View, edit, print, or add frames to your photos.
Windows

VLC Media Player (64-bit)
FREE
VLC Media Player (64-bit): Free-to-use media

WinRAR (32-bit)
TRIAL VERSION
Popular file software

GTA Vice City Mod
FREE
Add several new player skins to GTA Vice City.

The chosen applications were the following:

https://download.cnet.com/vlc-media-player-64-bit/3000-13632_4-75761094.html

https://download.cnet.com/need-for-speed-underground-2/3000-7513_4-10331372.html

https://download.cnet.com/marvell-libertas-802-11gb-wireless-lan-client-adapter/3000-2112_4-166388.html

https://download.cnet.com/sketchup-make-2017/3000-6677_4-10257337.html

https://download.cnet.com/poweriso-64-bit/3000-2646_4-76116067.html

https://download.cnet.com/virtualdj-2020/3000-18502_4-10212112.html

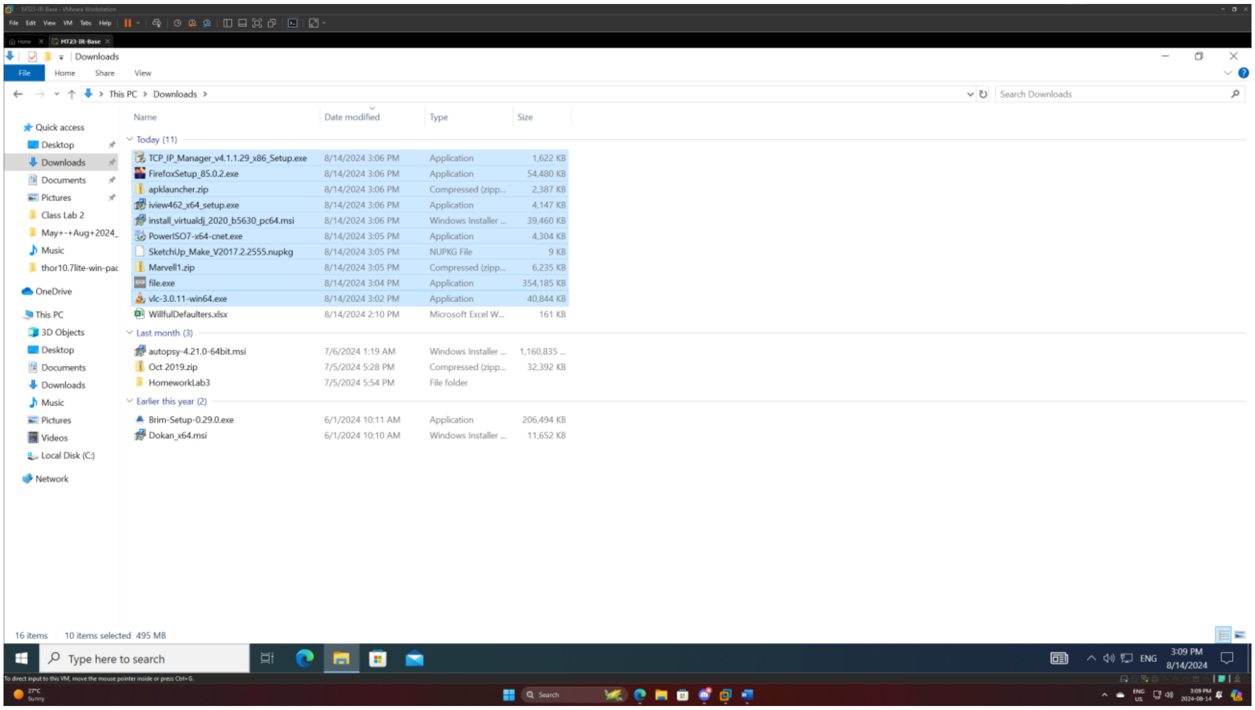
https://download.cnet.com/irfanview-64-bit/3000-2192_4-76444710.html

https://download.cnet.com/apk-installer-and-launcher/3000-20432_4-75915554.html

https://download.cnet.com/mozilla-firefox-64-bit/3000-2356_4-76472513.html

https://download.cnet.com/tcpip-manager/3000-2085_4-75031125.html

The list of applications provided to me by the links above:

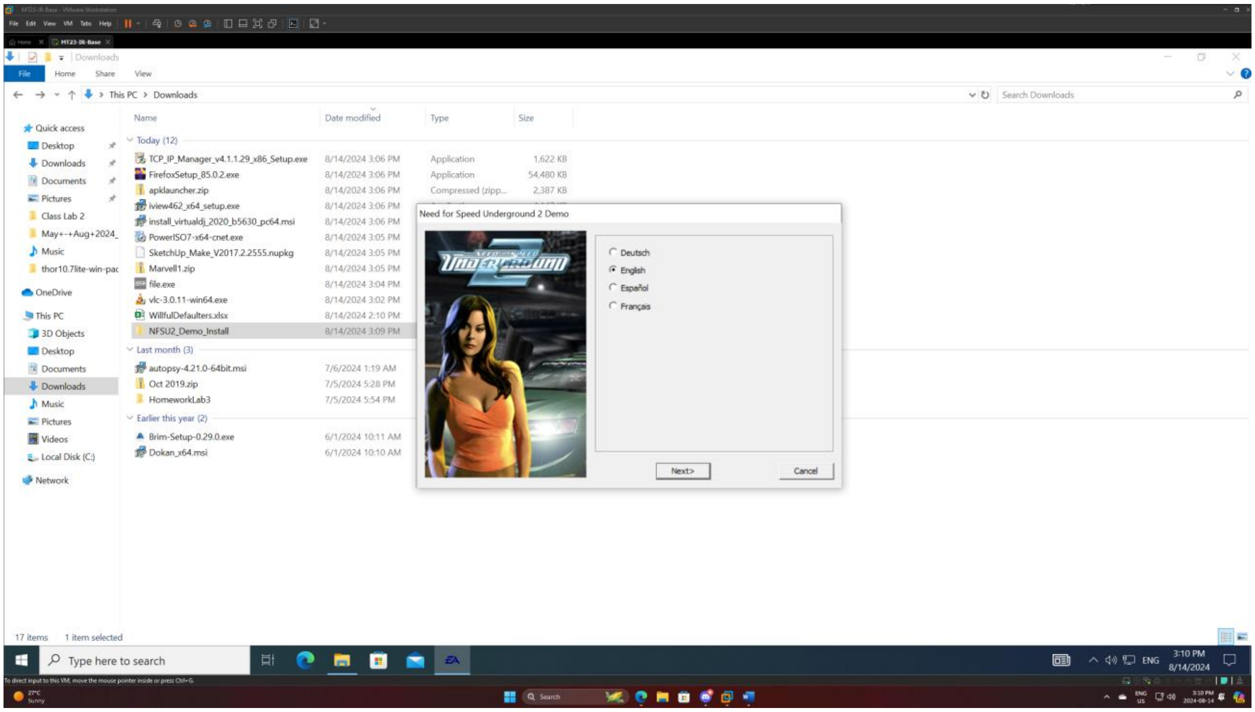


This PC › Downloads ›

Name	Date modified	Type	Size
Today (11)			
TCP_IP_Manager_v4.1.1.29_x86_Setup.exe	8/14/2024 3:06 PM	Application	1,622 KB
FirefoxSetup_85.0.2.exe	8/14/2024 3:06 PM	Application	54,480 KB
apklauncher.zip	8/14/2024 3:06 PM	Compressed (zipp...	2,387 KB
iview462_x64_setup.exe	8/14/2024 3:06 PM	Application	4,147 KB
install_virtualdj_2020_b5630_pc64.msi	8/14/2024 3:06 PM	Windows Installer ...	39,460 KB
PowerISO7-x64-cnet.exe	8/14/2024 3:05 PM	Application	4,304 KB
SketchUp_Make_V2017.2.2555.nupkg	8/14/2024 3:05 PM	NUPKG File	9 KB
Marvell1.zip	8/14/2024 3:05 PM	Compressed (zipp...	6,235 KB
file.exe	8/14/2024 3:04 PM	Application	354,185 KB
vlc-3.0.11-win64.exe	8/14/2024 3:02 PM	Application	40,844 KB
WillfulDefaulters.xlsx	8/14/2024 2:10 PM	Microsoft Excel W...	161 KB
Last month (3)			
autopsy-4.21.0-64bit.msi	7/6/2024 1:19 AM	Windows Installer ...	1,160,835 ...
Oct 2019.zip	7/5/2024 5:28 PM	Compressed (zipp...	32,392 KB
HomeworkLab3	7/5/2024 5:54 PM	File folder	
Earlier this year (2)			
Brim-Setup-0.29.0.exe	6/1/2024 10:11 AM	Application	206,494 KB
Dokan_x64.msi	6/1/2024 10:10 AM	Windows Installer ...	11,652 KB

16 items 10 items selected 495 MB

Once all of the installation files were acquired, I installed all of them



This PC › Downloads

Name	Date modified	Type	Size
Today (12)			
TCP_IP_Manager_v4.1.1.29_x86_Setup.exe	8/14/2024 3:06 PM	Application	1,622 KB
FirefoxSetup_85.0.2.exe	8/14/2024 3:06 PM	Application	54,480 KB
apklauncher.zip	8/14/2024 3:06 PM	Compressed (zipp...	2,387 KB
iview462_x64_setup.exe	8/14/2024 3:06 PM		
install_virtualdj_2020_b5630_pc64.msi	8/14/2024 3:06 PM		
PowerISO7-x64-cnet.exe	8/14/2024 3:05 PM		
SketchUp_Make_V2017.2.2555.nupkg	8/14/2024 3:05 PM		
Marvell1.zip	8/14/2024 3:05 PM		
file.exe	8/14/2024 3:04 PM		
vlc-3.0.11-win64.exe	8/14/2024 3:02 PM		
WillfulDefaulters.xlsx	8/14/2024 2:10 PM		
NFSU2_Demo_Install	8/14/2024 3:09 PM		
Last month (3)			
autopsy-4.21.0-64bit.msi	7/6/2024 1:19 AM		
Oct 2019.zip	7/5/2024 5:28 PM		
HomeworkLab3	7/5/2024 5:54 PM		
Earlier this year (2)			
Brim-Setup-0.29.0.exe	6/1/2024 10:11 AM		
Dokan_x64.msi	6/1/2024 10:10 AM		

Need for Speed Underground 2 Demo

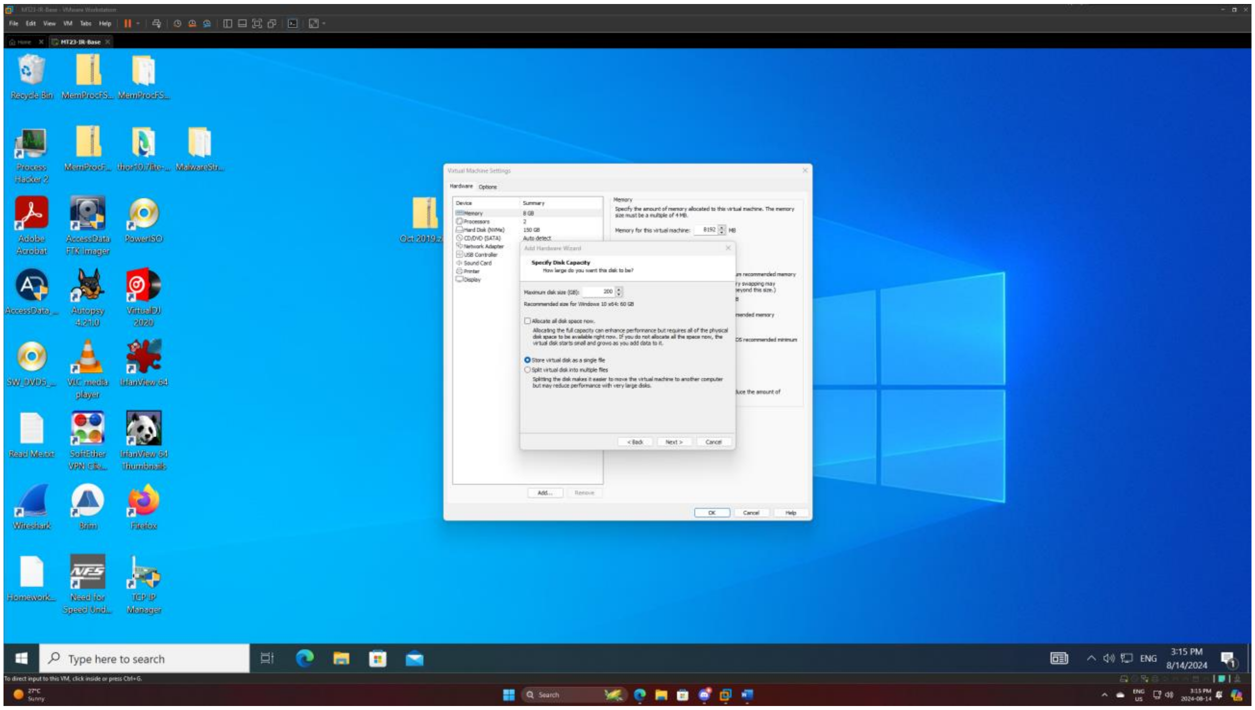
○ Deutsch
● English
○ Español
○ Français

Next> Cancel

17 items 1 item selected

VM Drive Cloning:

For my next step I opened the VM's properties and created a secondary 200gb disk comprised of a single file.



Virtual Machine Settings

Device	Summary
Memory	8 GB
Processors	2
Hard Disk (NVMe)	150 GB
CD/DVD (SATA)	Auto detect
Network Adapter	
USB Controller	
Sound Card	
Printer	
Display	

Memory

Specify the amount of memory allocated to this virtual machine. The memory size must be a multiple of 4 MB.

Memory for this virtual machine: 8192 MB

Add Hardware Wizard

Specify Disk Capacity

How large do you want this disk to be?

Maximum disk size (GB): 200

Recommended size for Windows 10 x64: 60 GB

□ Allocate all disk space now.

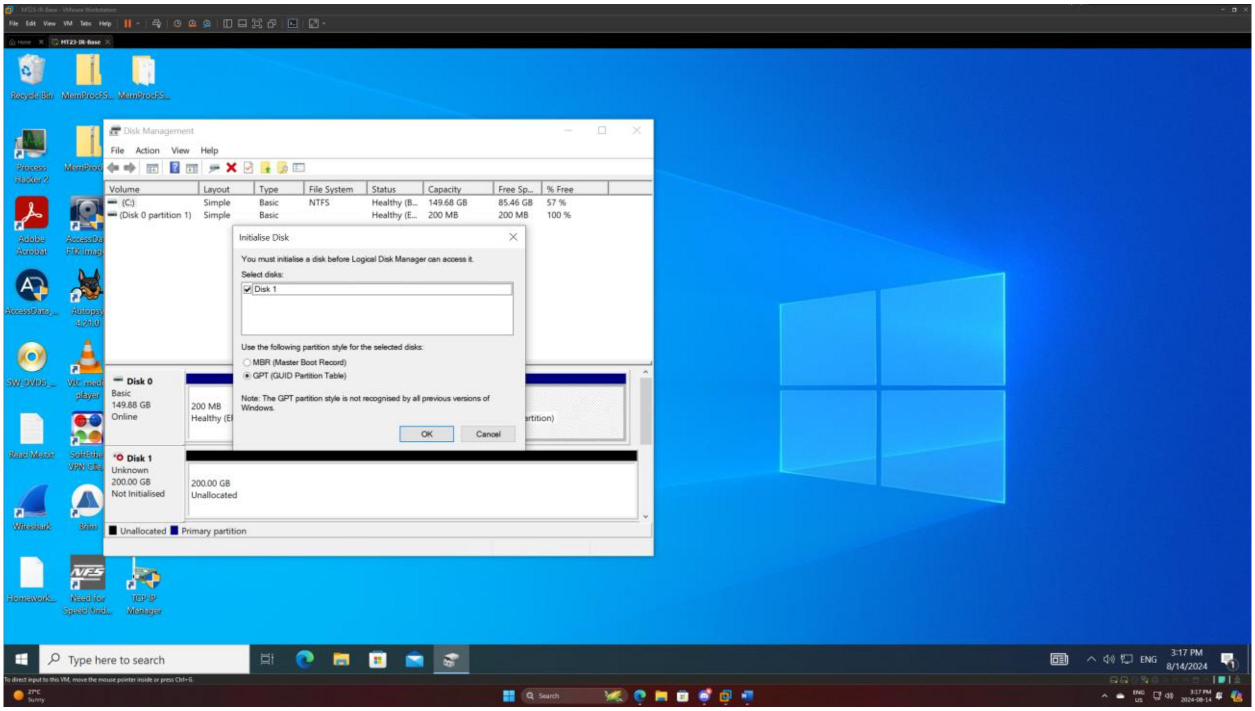
Allocating the full capacity can enhance performance but requires all of the physical disk space to be available right now. If you do not allocate all the space now, the virtual disk starts small and grows as you add data to it.

● Store virtual disk as a single file

○ Split virtual disk into multiple files

Splitting the disk makes it easier to move the virtual machine to another computer but may reduce performance with very large disks.

Within the VM, I initialized and properly formatted the new disk



Disk Management

Volume	Layout	Type	File System	Status	Capacity	Free Sp...	% Free
(C:)	Simple	Basic	NTFS	Healthy (B...	149.68 GB	85.46 GB	57 %
(Disk 0 partition 1)	Simple	Basic		Healthy (E...	200 MB	200 MB	100 %

Initialise Disk

You must initialise a disk before Logical Disk Manager can access it.

Select disks:

☑ Disk 1

Use the following partition style for the selected disks:

○ MBR (Master Boot Record)

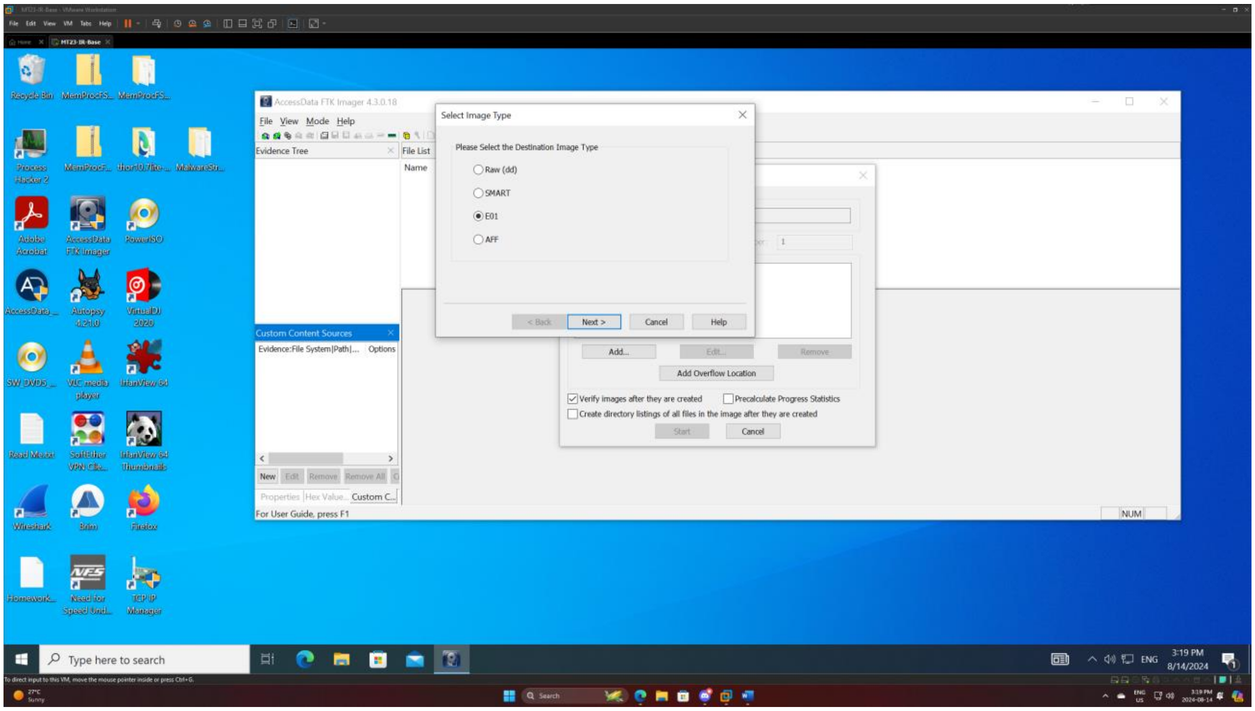
● GPT (GUID Partition Table)

Note: The GPT partition style is not recognised by all previous versions of Windows.

Disk 0 Basic 149.88 GB Online — 200 MB Healthy (E

Disk 1 Unknown 200.00 GB Not Initialised — 200.00 GB Unallocated

Using FTK Imager, I then cloned the C: Drive of the VM to the newly created drive using the E01 Image type.

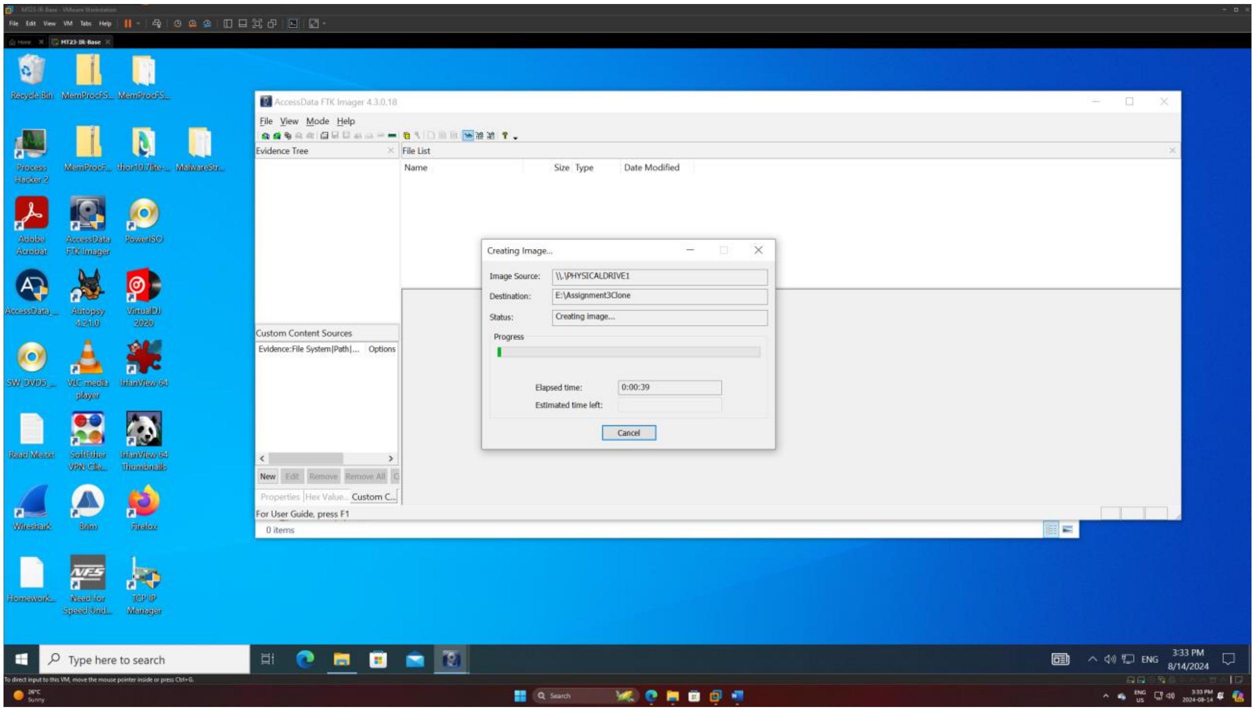


Select Image Type

Please Select the Destination Image Type

○ Raw (dd)
○ SMART
● E01
○ AFF

☑ Verify images after they are created
□ Precalculate Progress Statistics
□ Create directory listings of all files in the image after they are created



Creating Image...

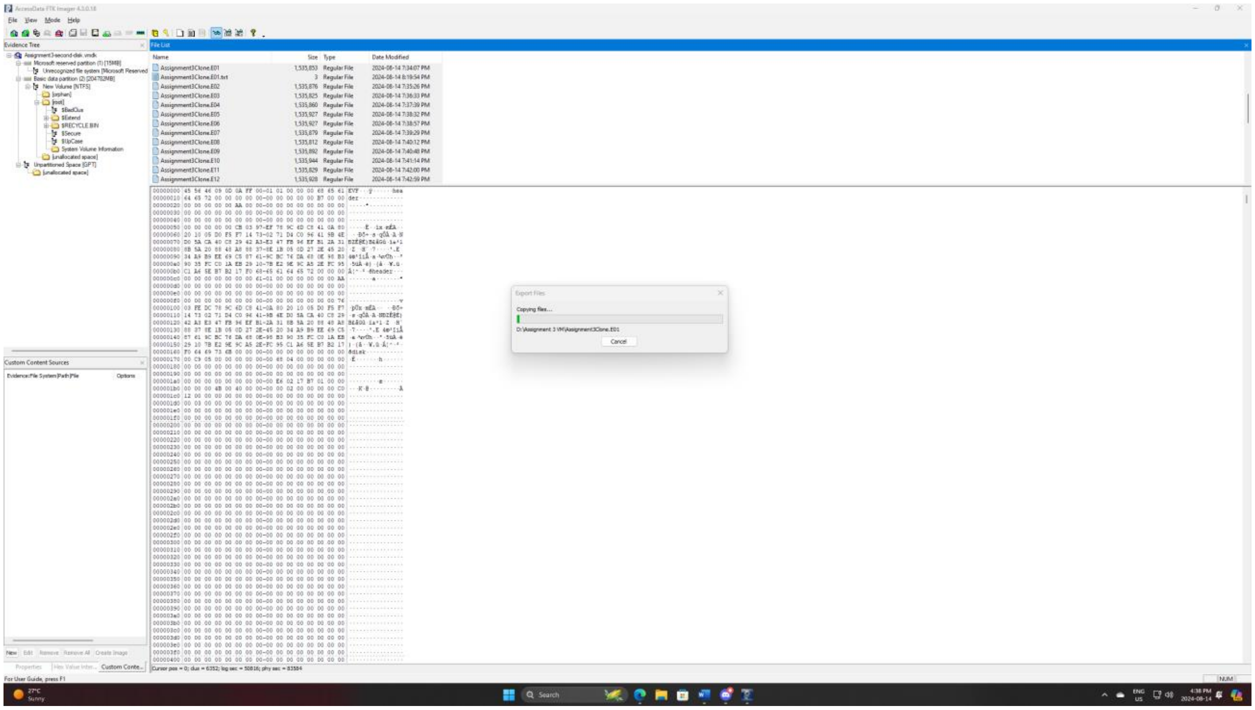
Image Source: \\.\PHYSICALDRIVE1
Destination: E:\Assignment3Clone
Status: Creating image...
Elapsed time: 0:00:39
Estimated time left:

Once the drive was cloned, I shut down the VM

Autopsy Analysis:

On my host machine, I opened FTK Imager and mounted my VM’s secondary 200gb drive.

I then copied the .E01 files created based of the image of my VM’s C: drive onto my host machine using FTK Imager.



Name	Size	Type	Date Modified
Assignment3Clone.E01	1,535,853	Regular File	2024-08-14 7:34:07 PM
Assignment3Clone.E01.txt	3	Regular File	2024-08-14 8:19:54 PM
Assignment3Clone.E02	1,535,876	Regular File	2024-08-14 7:35:26 PM
Assignment3Clone.E03	1,535,825	Regular File	2024-08-14 7:36:33 PM
Assignment3Clone.E04	1,535,860	Regular File	2024-08-14 7:37:39 PM
Assignment3Clone.E05	1,535,927	Regular File	2024-08-14 7:38:32 PM
Assignment3Clone.E06	1,535,927	Regular File	2024-08-14 7:38:57 PM
Assignment3Clone.E07	1,535,879	Regular File	2024-08-14 7:39:29 PM
Assignment3Clone.E08	1,535,812	Regular File	2024-08-14 7:40:12 PM
Assignment3Clone.E09	1,535,892	Regular File	2024-08-14 7:40:48 PM
Assignment3Clone.E10	1,535,944	Regular File	2024-08-14 7:41:14 PM
Assignment3Clone.E11	1,535,829	Regular File	2024-08-14 7:42:00 PM
Assignment3Clone.E12	1,535,928	Regular File	2024-08-14 7:42:59 PM

Export Files

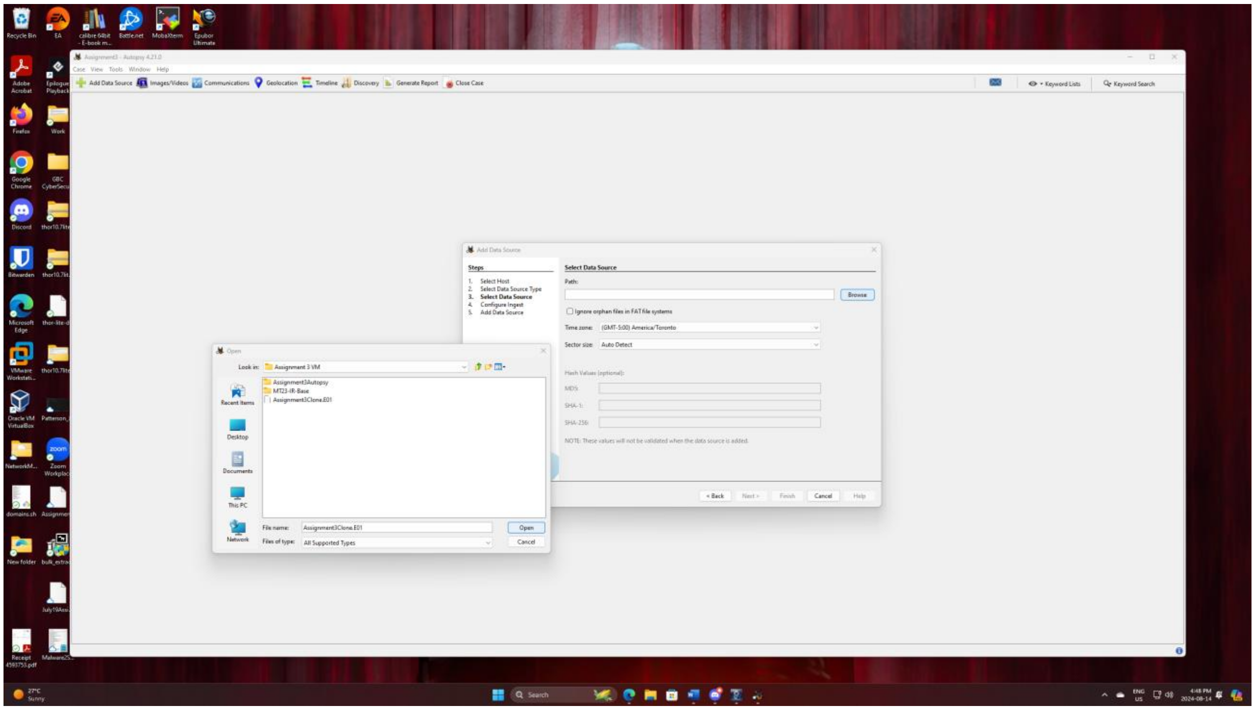
Copying files...

D:\Assignment 3 VM\Assignment3Clone.E01

Cancel

Cursor pos = 0; dus = 6352; log sec = 50816; phy sec = 83584

Once copied, I loaded the .E01 files into Autopsy for further analysis.



Add Data Source

Steps

1. Select Host
2. Select Data Source Type
3. **Select Data Source**
4. Configure Ingest
5. Add Data Source

Select Data Source

Path:

□ Ignore orphan files in FAT file systems

Time zone: (GMT-5:00) America/Toronto

Sector size: Auto Detect

Hash Values (optional):

MD5:

SHA-1:

SHA-256:

NOTE: These values will not be validated when the data source is added.

Open

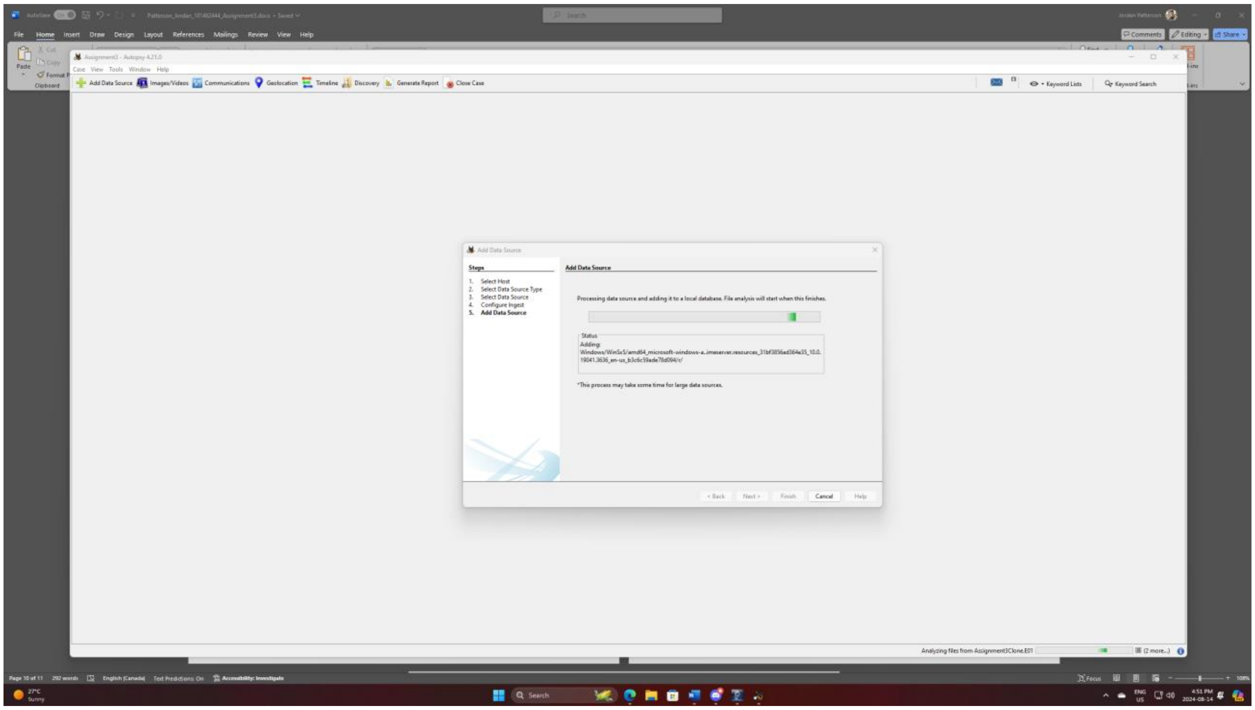
Look in: Assignment 3 VM

Assignment3Autopsy
MT23-IR-Base
Assignment3Clone.E01

File name: Assignment3Clone.E01

Files of type: All Supported Types

Autopsy Beginning Analysis:



Add Data Source

Steps

1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. **Add Data Source**

Add Data Source

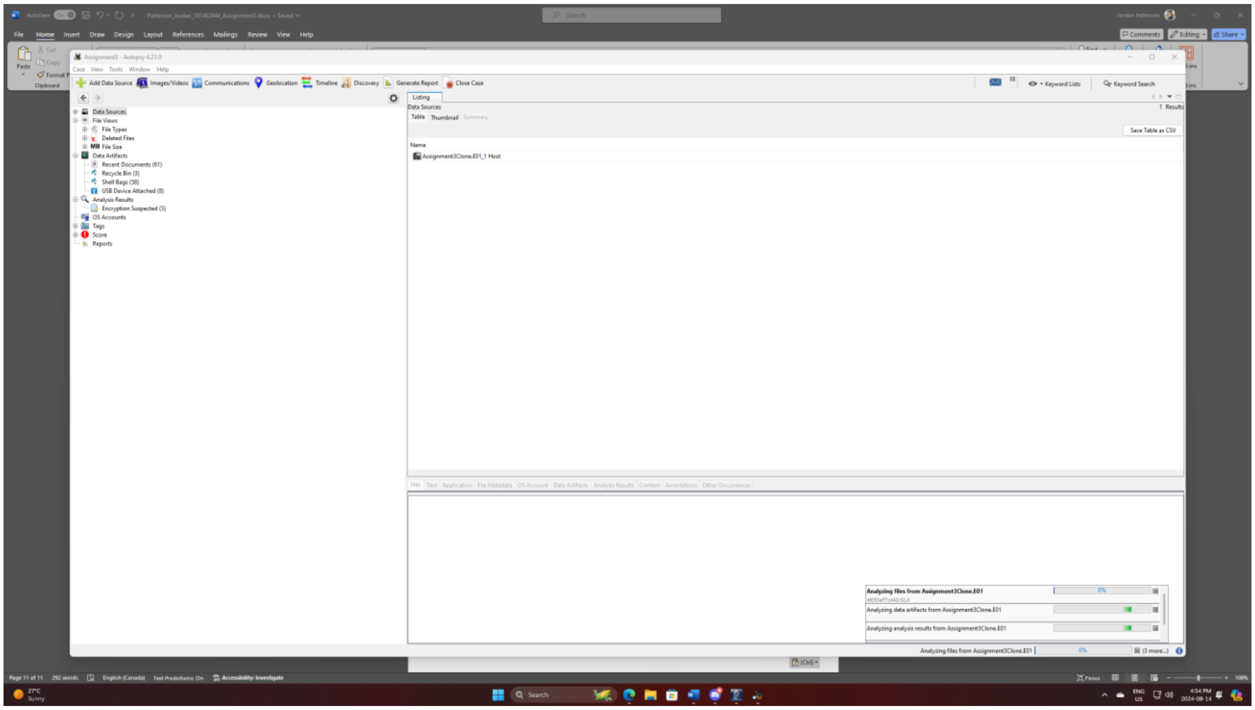
Processing data source and adding it to a local database. File analysis will start when this finishes.

Status
Adding:
Windows/WinSxS/amd64_microsoft-windows-a..imeserver.resources_31bf3856ad364e35_10.0.19041.3636_en-us_b3c6c59ade78d094/r/

*This process may take some time for large data sources.

Analyzing files from Assignment3Clone.E01

Autopsy Analysis in Progress:



Data Sources
File Views
File Types
Deleted Files
File Size
Data Artifacts
Recent Documents (61)
Recycle Bin (3)
Shell Bags (58)
USB Device Attached (8)
Analysis Results
Encryption Suspected (5)
OS Accounts
Tags
Score
Reports

Data Sources — 1 Results

Name
Assignment3Clone.E01_1 Host

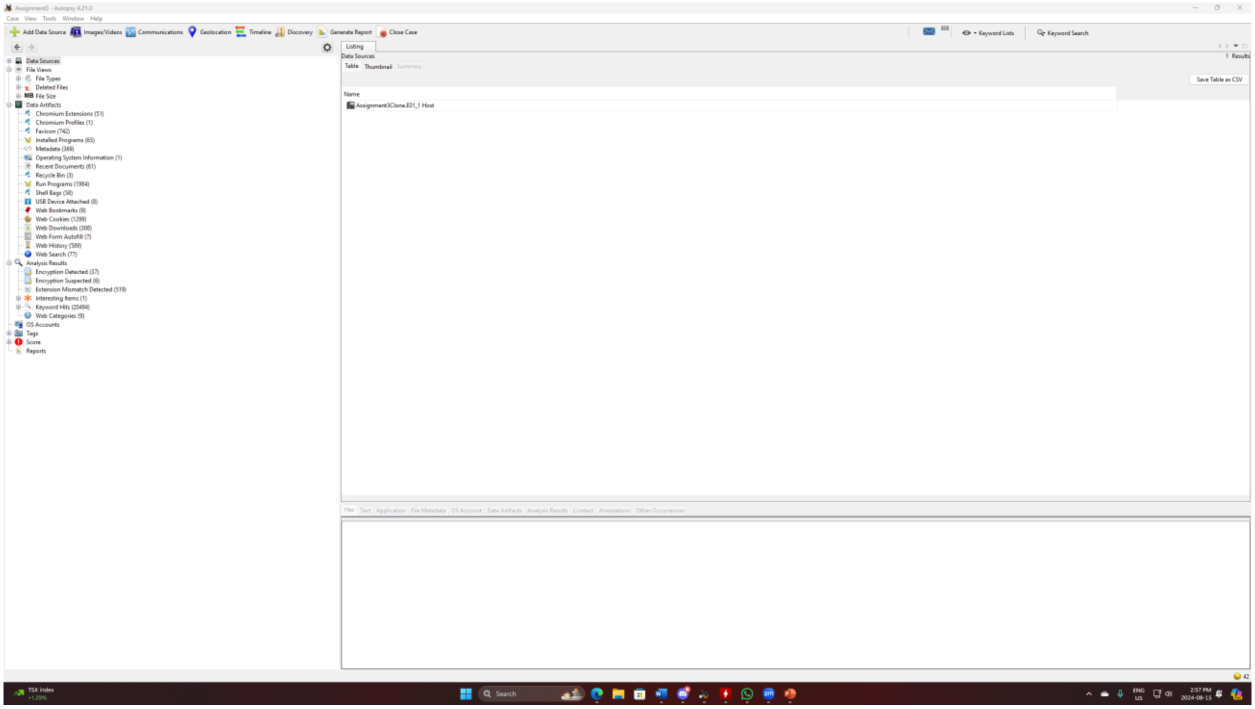
Analyzing files from Assignment3Clone.E01 — 0%

Analyzing data artifacts from Assignment3Clone.E01

Analyzing analysis results from Assignment3Clone.E01

Analyzing files from Assignment3Clone.E01 — 0% (3 more...)

Autopsy Analysis Complete:



Data Sources
File Views
File Types
Deleted Files
File Size
Data Artifacts
Chromium Extensions (51)
Chromium Profiles (1)
Favicon (742)
Installed Programs (65)
Metadata (369)
Operating System Information (1)
Recent Documents (61)
Recycle Bin (3)
Run Programs (1984)
Shell Bags (58)
USB Device Attached (8)
Web Bookmarks (9)
Web Cookies (1299)
Web Downloads (308)
Web Form Autofill (7)
Web History (589)
Web Search (77)
Analysis Results
Encryption Detected (37)
Encryption Suspected (6)
Extension Mismatch Detected (519)
Interesting Items (1)
Keyword Hits (20494)
Web Categories (9)
OS Accounts
Tags
Score
Reports

Data Sources — 1 Results

Name
Assignment3Clone.E01_1 Host

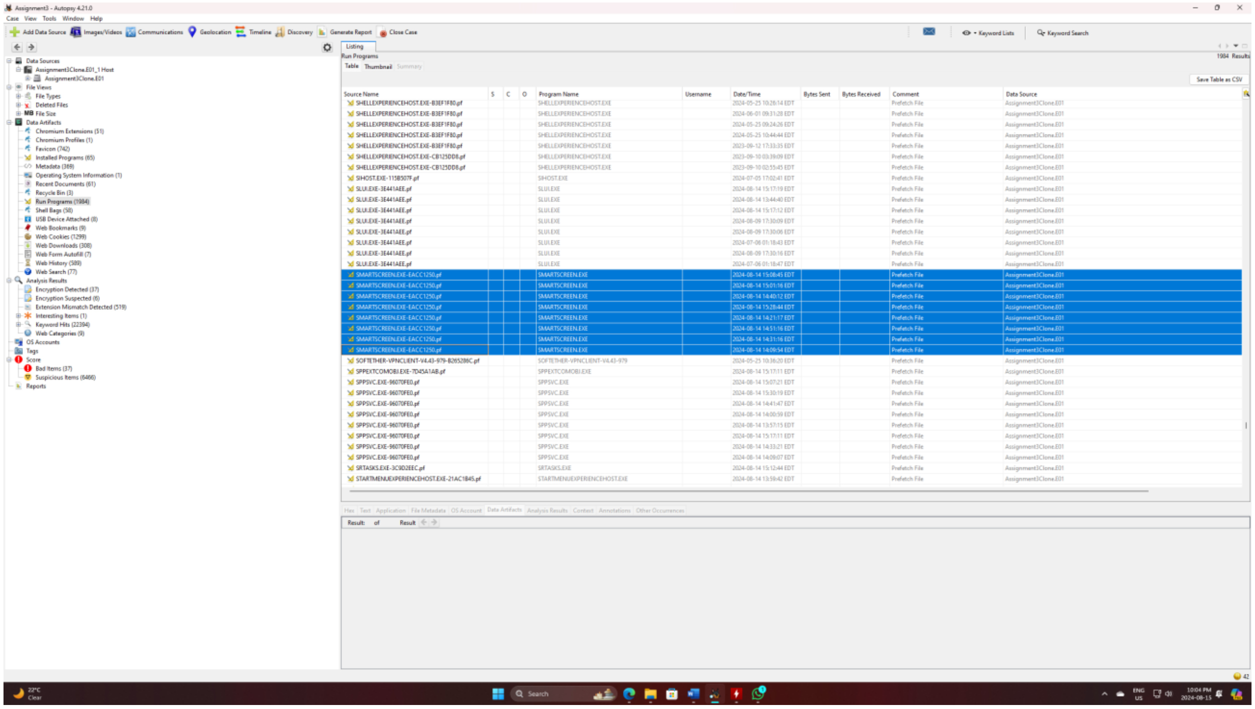
Assignment Questions:

How many times was smartscreen invoked including timestamps for each?

In Autopsy, under “Data Artifacts” I found the “Run Programs” tab. Since I was looking for the amound of time SmartScreen was executed, I decided to start my search there. I found that Smartscreen was invoked 8 times on my virtual machine.

The timestamps were as follows:

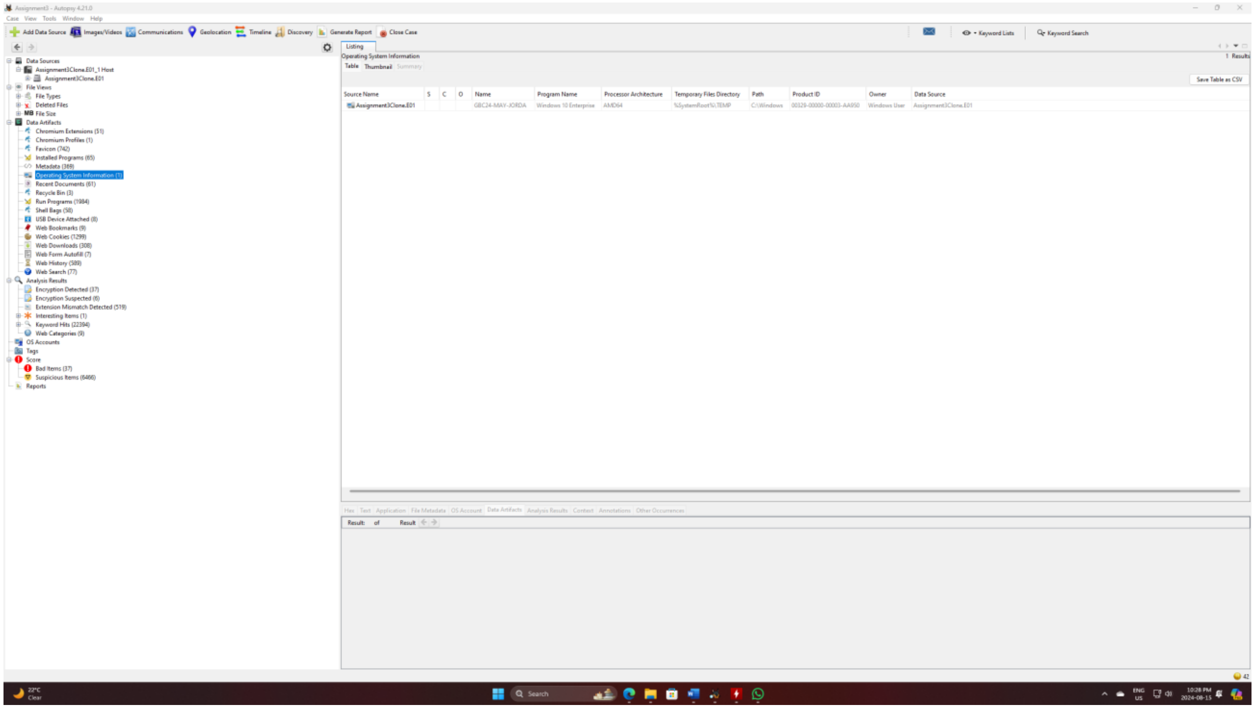
2024-08-14 15:08:45 EDT
2024-08-14 15:01:16 EDT
2024-08-14 14:40:12 EDT
2024-08-14 15:28:44 EDT
2024-08-14 14:21:17 EDT
2024-08-14 14:51:16 EDT
2024-08-14 14:31:16 EDT
2024-08-14 14:09:54 EDT



Source Name	S	C	O	Program Name	Username	Date/Time	Bytes Sent	Bytes Received	Comment	Data Source
SHELLEXPERIENCEHOST.EXE-B3EF1F80.pf				SHELLEXPERIENCEHOST.EXE		2024-05-25 10:26:14 EDT			Prefetch File	Assignment3Clone.E01
SHELLEXPERIENCEHOST.EXE-B3EF1F80.pf				SHELLEXPERIENCEHOST.EXE		2024-06-01 09:31:28 EDT			Prefetch File	Assignment3Clone.E01
SHELLEXPERIENCEHOST.EXE-B3EF1F80.pf				SHELLEXPERIENCEHOST.EXE		2024-05-25 09:24:26 EDT			Prefetch File	Assignment3Clone.E01
SHELLEXPERIENCEHOST.EXE-B3EF1F80.pf				SHELLEXPERIENCEHOST.EXE		2024-05-25 10:44:44 EDT			Prefetch File	Assignment3Clone.E01
SHELLEXPERIENCEHOST.EXE-B3EF1F80.pf				SHELLEXPERIENCEHOST.EXE		2023-09-12 17:33:35 EDT			Prefetch File	Assignment3Clone.E01
SHELLEXPERIENCEHOST.EXE-CB125DD8.pf				SHELLEXPERIENCEHOST.EXE		2023-09-10 03:39:09 EDT			Prefetch File	Assignment3Clone.E01
SHELLEXPERIENCEHOST.EXE-CB125DD8.pf				SHELLEXPERIENCEHOST.EXE		2023-09-10 02:55:45 EDT			Prefetch File	Assignment3Clone.E01
SIHOST.EXE-115B507F.pf				SIHOST.EXE		2024-07-05 17:02:41 EDT			Prefetch File	Assignment3Clone.E01
SLUI.EXE-3E441AEE.pf				SLUI.EXE		2024-08-14 15:17:19 EDT			Prefetch File	Assignment3Clone.E01
SLUI.EXE-3E441AEE.pf				SLUI.EXE		2024-08-14 13:44:40 EDT			Prefetch File	Assignment3Clone.E01
SLUI.EXE-3E441AEE.pf				SLUI.EXE		2024-08-14 15:17:12 EDT			Prefetch File	Assignment3Clone.E01
SLUI.EXE-3E441AEE.pf				SLUI.EXE		2024-08-09 17:30:09 EDT			Prefetch File	Assignment3Clone.E01
SLUI.EXE-3E441AEE.pf				SLUI.EXE		2024-08-09 17:30:06 EDT			Prefetch File	Assignment3Clone.E01
SLUI.EXE-3E441AEE.pf				SLUI.EXE		2024-07-06 01:18:43 EDT			Prefetch File	Assignment3Clone.E01
SLUI.EXE-3E441AEE.pf				SLUI.EXE		2024-08-09 17:30:16 EDT			Prefetch File	Assignment3Clone.E01
SLUI.EXE-3E441AEE.pf				SLUI.EXE		2024-07-06 01:18:47 EDT			Prefetch File	Assignment3Clone.E01
SMARTSCREEN.EXE-EACC1250.pf				SMARTSCREEN.EXE		2024-08-14 15:08:45 EDT			Prefetch File	Assignment3Clone.E01
SMARTSCREEN.EXE-EACC1250.pf				SMARTSCREEN.EXE		2024-08-14 15:01:16 EDT			Prefetch File	Assignment3Clone.E01
SMARTSCREEN.EXE-EACC1250.pf				SMARTSCREEN.EXE		2024-08-14 14:40:12 EDT			Prefetch File	Assignment3Clone.E01
SMARTSCREEN.EXE-EACC1250.pf				SMARTSCREEN.EXE		2024-08-14 15:28:44 EDT			Prefetch File	Assignment3Clone.E01
SMARTSCREEN.EXE-EACC1250.pf				SMARTSCREEN.EXE		2024-08-14 14:21:17 EDT			Prefetch File	Assignment3Clone.E01
SMARTSCREEN.EXE-EACC1250.pf				SMARTSCREEN.EXE		2024-08-14 14:51:16 EDT			Prefetch File	Assignment3Clone.E01
SMARTSCREEN.EXE-EACC1250.pf				SMARTSCREEN.EXE		2024-08-14 14:31:16 EDT			Prefetch File	Assignment3Clone.E01
SMARTSCREEN.EXE-EACC1250.pf				SMARTSCREEN.EXE		2024-08-14 14:09:54 EDT			Prefetch File	Assignment3Clone.E01
SOFTETHER-VPNCLIENT-V4.43-979-B265286C.pf				SOFTETHER-VPNCLIENT-V4.43-979		2024-05-25 10:36:20 EDT			Prefetch File	Assignment3Clone.E01
SPPEXTCOMOBJ.EXE-7D45A1AB.pf				SPPEXTCOMOBJ.EXE		2024-08-14 15:17:11 EDT			Prefetch File	Assignment3Clone.E01
SPPSVC.EXE-96070FE0.pf				SPPSVC.EXE		2024-08-14 15:07:21 EDT			Prefetch File	Assignment3Clone.E01
SPPSVC.EXE-96070FE0.pf				SPPSVC.EXE		2024-08-14 15:30:19 EDT			Prefetch File	Assignment3Clone.E01
SPPSVC.EXE-96070FE0.pf				SPPSVC.EXE		2024-08-14 14:41:47 EDT			Prefetch File	Assignment3Clone.E01
SPPSVC.EXE-96070FE0.pf				SPPSVC.EXE		2024-08-14 14:00:59 EDT			Prefetch File	Assignment3Clone.E01
SPPSVC.EXE-96070FE0.pf				SPPSVC.EXE		2024-08-14 13:57:15 EDT			Prefetch File	Assignment3Clone.E01
SPPSVC.EXE-96070FE0.pf				SPPSVC.EXE		2024-08-14 15:17:11 EDT			Prefetch File	Assignment3Clone.E01
SPPSVC.EXE-96070FE0.pf				SPPSVC.EXE		2024-08-14 14:33:21 EDT			Prefetch File	Assignment3Clone.E01
SPPSVC.EXE-96070FE0.pf				SPPSVC.EXE		2024-08-14 14:09:07 EDT			Prefetch File	Assignment3Clone.E01
SRTASKS.EXE-3C9D2EEC.pf				SRTASKS.EXE		2024-08-14 15:12:44 EDT			Prefetch File	Assignment3Clone.E01
STARTMENUEXPERIENCEHOST.EXE-21AC1B45.pf				STARTMENUEXPERIENCEHOST.EXE		2024-08-14 13:59:42 EDT			Prefetch File	Assignment3Clone.E01

Hostname and OEM vendor of the machine

The Hostname of the machine is GBC24-May-Jordan.
I initially found this information in the “Operating System Information” tab. The OEM vendor information of the machine has not been captured by Autopsy. Upon checking for the Registry key HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\OEMInformation in the regripper reports, it was not present. For this reason, the OEM vendor information could not be found. I suspect that the OEM vendor would be VMWare Inc. considering this is a VM created and running in VMWare.

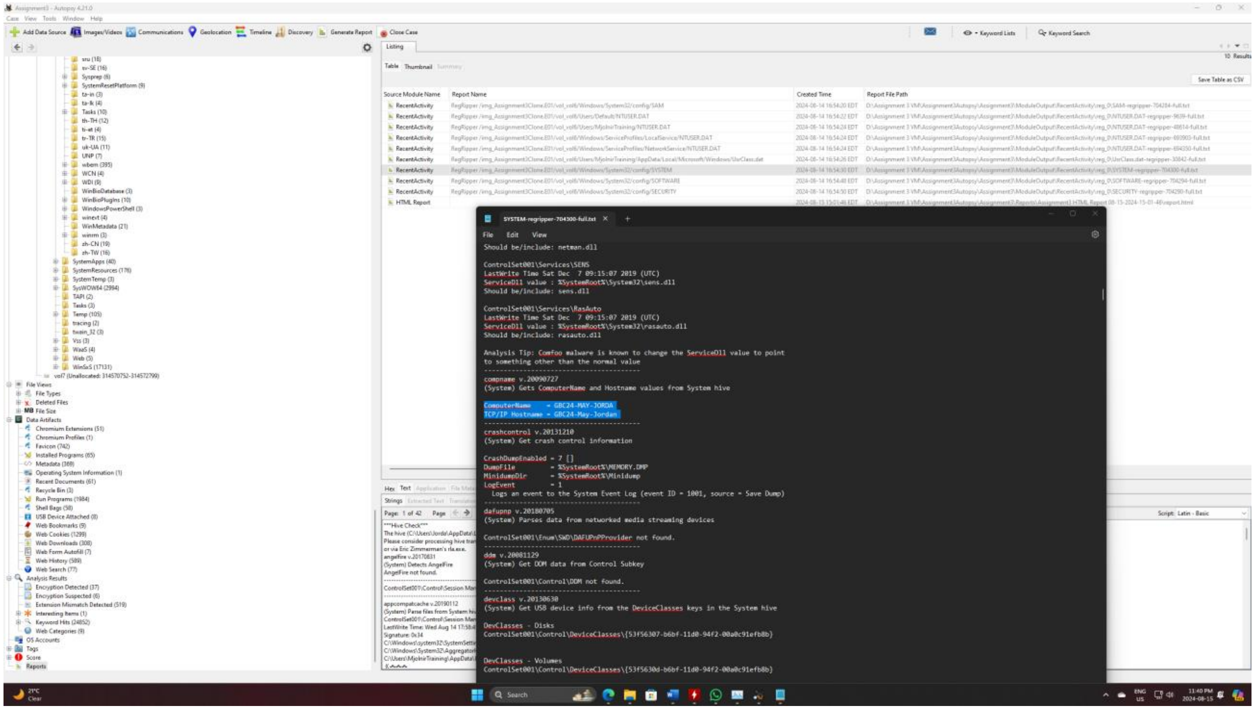


Operating System Information

Source Name	S	C	O	Name	Program Name	Processor Architecture	Temporary Files Directory	Path	Product ID	Owner	Data Source
Assignment3Clone.E01				GBC24-MAY-JORDA	Windows 10 Enterprise	AMD64	%SystemRoot%\TEMP	C:\Windows	00329-00000-00003-AA950	Windows User	Assignment3Clone.E01

I more clearly confirmed the hostname by opening the following Regripper report to get the information directly from the systems Registry.

RegRipper /img_Assignment3Clone.E01/vol_vol6/Windows/System32/config/SYSTEM



Source Module Name	Report Name	Created Time	Report File Path
RecentActivity	RegRipper /img_Assignment3Clone.E01/vol_vol6/Windows/System32/config/SAM	2024-08-14 16:54:20 EDT	D:\Assignment 3 VM\Assignment3Autopsy\Assignment3\ModuleOutput\RecentActivity\reg_D_SAM-regripper-704284-full.txt
RecentActivity	RegRipper /img_Assignment3Clone.E01/vol_vol6/Users/Default/NTUSER.DAT	2024-08-14 16:54:22 EDT	D:\Assignment 3 VM\Assignment3Autopsy\Assignment3\ModuleOutput\RecentActivity\reg_D_NTUSER.DAT-regripper-9639-full.txt
RecentActivity	RegRipper /img_Assignment3Clone.E01/vol_vol6/Users/MjolnirTraining/NTUSER.DAT	2024-08-14 16:54:24 EDT	D:\Assignment 3 VM\Assignment3Autopsy\Assignment3\ModuleOutput\RecentActivity\reg_D_NTUSER.DAT-regripper-48614-full.txt
RecentActivity	RegRipper /img_Assignment3Clone.E01/vol_vol6/Windows/ServiceProfiles/LocalService/NTUSER.DAT	2024-08-14 16:54:24 EDT	D:\Assignment 3 VM\Assignment3Autopsy\Assignment3\ModuleOutput\RecentActivity\reg_D_NTUSER.DAT-regripper-693903-full.txt
RecentActivity	RegRipper /img_Assignment3Clone.E01/vol_vol6/Windows/ServiceProfiles/NetworkService/NTUSER.DAT	2024-08-14 16:54:24 EDT	D:\Assignment 3 VM\Assignment3Autopsy\Assignment3\ModuleOutput\RecentActivity\reg_D_NTUSER.DAT-regripper-694350-full.txt
RecentActivity	RegRipper /img_Assignment3Clone.E01/vol_vol6/Users/MjolnirTraining/AppData/Local/Microsoft/Windows/UsrClass.dat	2024-08-14 16:54:26 EDT	D:\Assignment 3 VM\Assignment3Autopsy\Assignment3\ModuleOutput\RecentActivity\reg_D_UsrClass.dat-regripper-30842-full.txt
RecentActivity	RegRipper /img_Assignment3Clone.E01/vol_vol6/Windows/System32/config/SYSTEM	2024-08-14 16:54:30 EDT	D:\Assignment 3 VM\Assignment3Autopsy\Assignment3\ModuleOutput\RecentActivity\reg_D_SYSTEM-regripper-704300-full.txt
RecentActivity	RegRipper /img_Assignment3Clone.E01/vol_vol6/Windows/System32/config/SOFTWARE	2024-08-14 16:54:40 EDT	D:\Assignment 3 VM\Assignment3Autopsy\Assignment3\ModuleOutput\RecentActivity\reg_D_SOFTWARE-regripper-704294-full.txt
RecentActivity	RegRipper /img_Assignment3Clone.E01/vol_vol6/Windows/System32/config/SECURITY	2024-08-14 16:54:50 EDT	D:\Assignment 3 VM\Assignment3Autopsy\Assignment3\ModuleOutput\RecentActivity\reg_D_SECURITY-regripper-704290-full.txt
HTML Report		2024-08-15 15:01:46 EDT	D:\Assignment 3 VM\Assignment3Autopsy\Assignment3\Reports\Assignment3 HTML Report 08-15-2024-15-01-46\report.html

SYSTEM-regripper-704300-full.txt

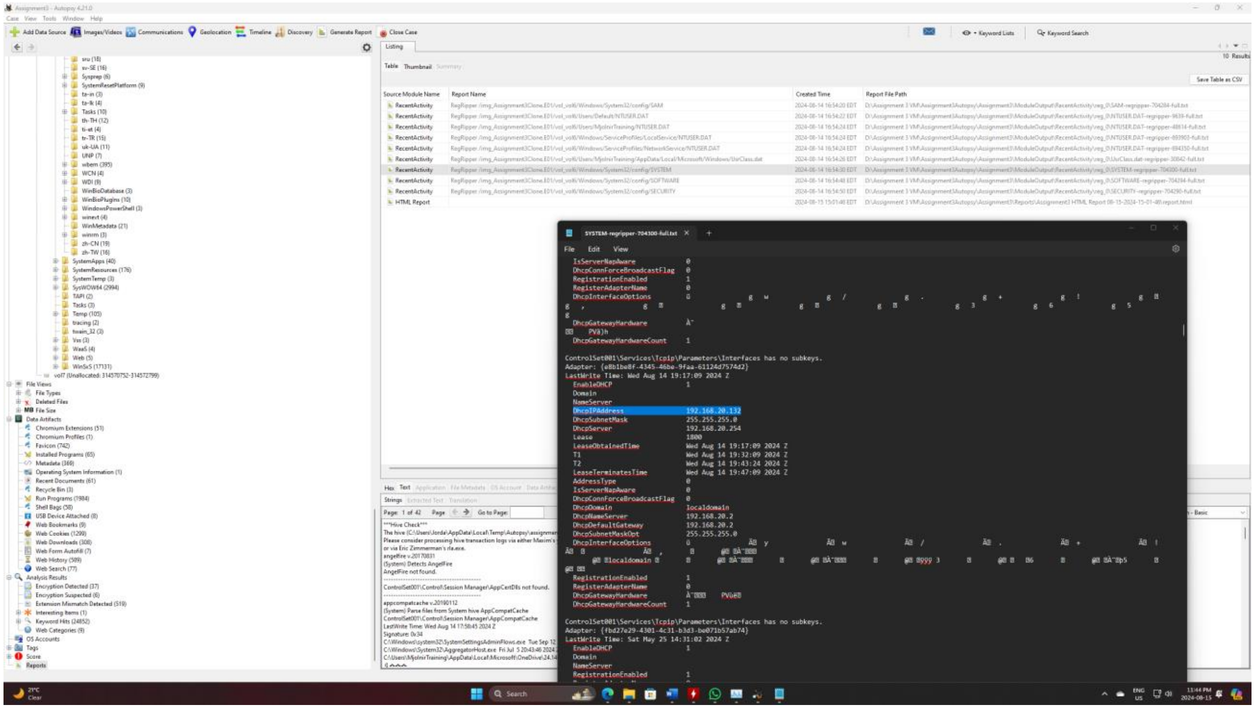
```
Should be/include: netman.dll

ControlSet001\Services\SENS
LastWrite Time Sat Dec  7 09:15:07 2019 (UTC)
ServiceDll value : %SystemRoot%\System32\sens.dll
Should be/include: sens.dll

ControlSet001\Services\RasAuto
LastWrite Time Sat Dec  7 09:15:07 2019 (UTC)
ServiceDll value : %SystemRoot%\System32\rasauto.dll
Should be/include: rasauto.dll

Analysis Tip: Comfoo malware is known to change the ServiceDll value to point
to something other than the normal value
----------------------------------------
compname v.20090727
(System) Gets ComputerName and Hostname values from System hive

ComputerName    = GBC24-MAY-JORDA
TCP/IP Hostname = GBC24-May-Jordan
----------------------------------------
crashcontrol v.20131210
(System) Get crash control information

CrashDumpEnabled = 7 []
DumpFile         = %SystemRoot%\MEMORY.DMP
MinidumpDir      = %SystemRoot%\Minidump
LogEvent         = 1
  Logs an event to the System Event Log (event ID = 1001, source = Save Dump)
----------------------------------------
dafupnp v.20180705
(System) Parses data from networked media streaming devices

ControlSet001\Enum\SWD\DAFUPnPProvider not found.
----------------------------------------
ddm v.20081129
(System) Get DDM data from Control Subkey

ControlSet001\Control\DDM not found.
----------------------------------------
devclass v.20130630
(System) Get USB device info from the DeviceClasses keys in the System hive

DevClasses - Disks
ControlSet001\Control\DeviceClasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b}


DevClasses - Volumes
ControlSet001\Control\DeviceClasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
```

IP address of the machine

In the following registry report:

RegRipper /img_Assignment3Clone.E01/vol_vol6/Windows/System32/config/SYSTEM

I was able to determine the IP address along with other Networking information. The IP address of this system is 192.168.20.132.



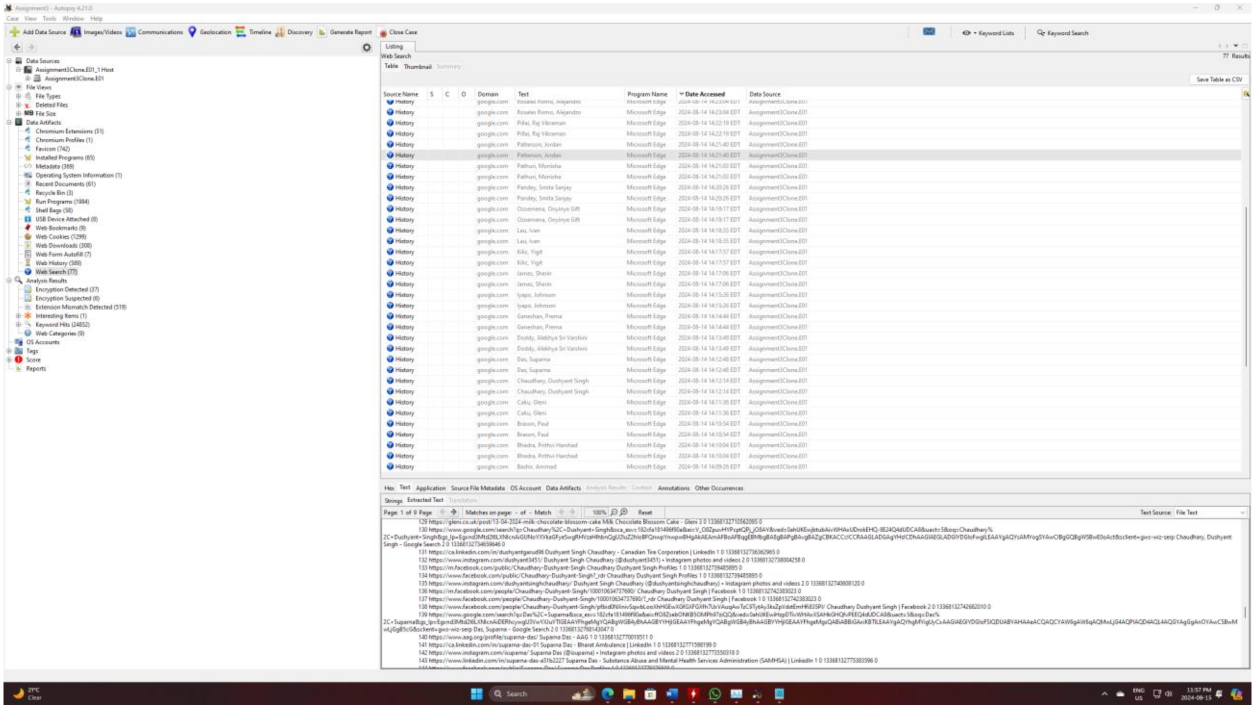
Source Module Name	Report Name	Created Time	Report File Path
RecentActivity	RegRipper /img_Assignment3Clone.E01/vol_vol6/Windows/System32/config/SAM	2024-08-14 16:54:20 EDT	D:\Assignment 3 VM\Assignment3Autopsy\Assignment3\ModuleOutput\RecentActivity\reg_0\SAM-regripper-704284-full.txt
RecentActivity	RegRipper /img_Assignment3Clone.E01/vol_vol6/Users/Default/NTUSER.DAT	2024-08-14 16:54:22 EDT	D:\Assignment 3 VM\Assignment3Autopsy\Assignment3\ModuleOutput\RecentActivity\reg_0\NTUSER.DAT-regripper-9639-full.txt
RecentActivity	RegRipper /img_Assignment3Clone.E01/vol_vol6/Users/MjolnirTraining/NTUSER.DAT	2024-08-14 16:54:24 EDT	D:\Assignment 3 VM\Assignment3Autopsy\Assignment3\ModuleOutput\RecentActivity\reg_0\NTUSER.DAT-regripper-48814-full.txt
RecentActivity	RegRipper /img_Assignment3Clone.E01/vol_vol6/Windows/ServiceProfiles/LocalService/NTUSER.DAT	2024-08-14 16:54:24 EDT	D:\Assignment 3 VM\Assignment3Autopsy\Assignment3\ModuleOutput\RecentActivity\reg_0\NTUSER.DAT-regripper-693903-full.txt
RecentActivity	RegRipper /img_Assignment3Clone.E01/vol_vol6/Windows/ServiceProfiles/NetworkService/NTUSER.DAT	2024-08-14 16:54:24 EDT	D:\Assignment 3 VM\Assignment3Autopsy\Assignment3\ModuleOutput\RecentActivity\reg_0\NTUSER.DAT-regripper-694350-full.txt
RecentActivity	RegRipper /img_Assignment3Clone.E01/vol_vol6/Users/MjolnirTraining/AppData/Local/Microsoft/Windows/UsrClass.dat	2024-08-14 16:54:26 EDT	D:\Assignment 3 VM\Assignment3Autopsy\Assignment3\ModuleOutput\RecentActivity\reg_0\UsrClass.dat-regripper-30842-full.txt
RecentActivity	RegRipper /img_Assignment3Clone.E01/vol_vol6/Windows/System32/config/SYSTEM	2024-08-14 16:54:30 EDT	D:\Assignment 3 VM\Assignment3Autopsy\Assignment3\ModuleOutput\RecentActivity\reg_0\SYSTEM-regripper-704300-full.txt
RecentActivity	RegRipper /img_Assignment3Clone.E01/vol_vol6/Windows/System32/config/SOFTWARE	2024-08-14 16:54:48 EDT	D:\Assignment 3 VM\Assignment3Autopsy\Assignment3\ModuleOutput\RecentActivity\reg_0\SOFTWARE-regripper-704294-full.txt
RecentActivity	RegRipper /img_Assignment3Clone.E01/vol_vol6/Windows/System32/config/SECURITY	2024-08-14 16:54:50 EDT	D:\Assignment 3 VM\Assignment3Autopsy\Assignment3\ModuleOutput\RecentActivity\reg_0\SECURITY-regripper-704290-full.txt
HTML Report		2024-08-15 15:01:48 EDT	D:\Assignment 3 VM\Assignment3Autopsy\Assignment3\Reports\Assignment3 HTML Report 08-15-2024-15-01-48\report.html

SYSTEM-regripper-704300-full.txt

```
  IsServerNapAware              0
  DhcpConnForceBroadcastFlag    0
  RegistrationEnabled           1
  RegisterAdapterName           0
  DhcpInterfaceOptions          0
  DhcpGatewayHardware           À¨
      PVä}h
  DhcpGatewayHardwareCount      1

ControlSet001\Services\Tcpip\Parameters\Interfaces has no subkeys.
Adapter: {e8b1be8f-4345-46be-9faa-61124d7574d2}
LastWrite Time: Wed Aug 14 19:17:09 2024 Z
  EnableDHCP                    1
  Domain
  NameServer
  DhcpIPAddress                 192.168.20.132
  DhcpSubnetMask                255.255.255.0
  DhcpServer                    192.168.20.254
  Lease                         1800
  LeaseObtainedTime             Wed Aug 14 19:17:09 2024 Z
  T1                            Wed Aug 14 19:32:09 2024 Z
  T2                            Wed Aug 14 19:43:24 2024 Z
  LeaseTerminatesTime           Wed Aug 14 19:47:09 2024 Z
  AddressType                   0
  IsServerNapAware              0
  DhcpConnForceBroadcastFlag    0
  DhcpDomain                    localdomain
  DhcpNameServer                192.168.20.2
  DhcpDefaultGateway            192.168.20.2
  DhcpSubnetMaskOpt             255.255.255.0
  DhcpInterfaceOptions          0
      localdomain
  RegistrationEnabled           1
  RegisterAdapterName           0
  DhcpGatewayHardware           À¨     PVüe
  DhcpGatewayHardwareCount      1

ControlSet001\Services\Tcpip\Parameters\Interfaces has no subkeys.
Adapter: {fbd27e29-4301-4c31-b3d3-be071b57ab74}
LastWrite Time: Sat May 25 14:31:02 2024 Z
  EnableDHCP                    1
  Domain
  NameServer
  RegistrationEnabled           1
```

What was the auto suggest when you googled, was it completely off the target?

When googling the Auto Suggest seemed to be on target. In Autopsy, I opened the “Web Search” tab and viewed all of the searches that were made on this VM. All searches seemed to correspond to what I had intended to search for. I did not find any other information in Autopsy regarding Auto Suggest results.

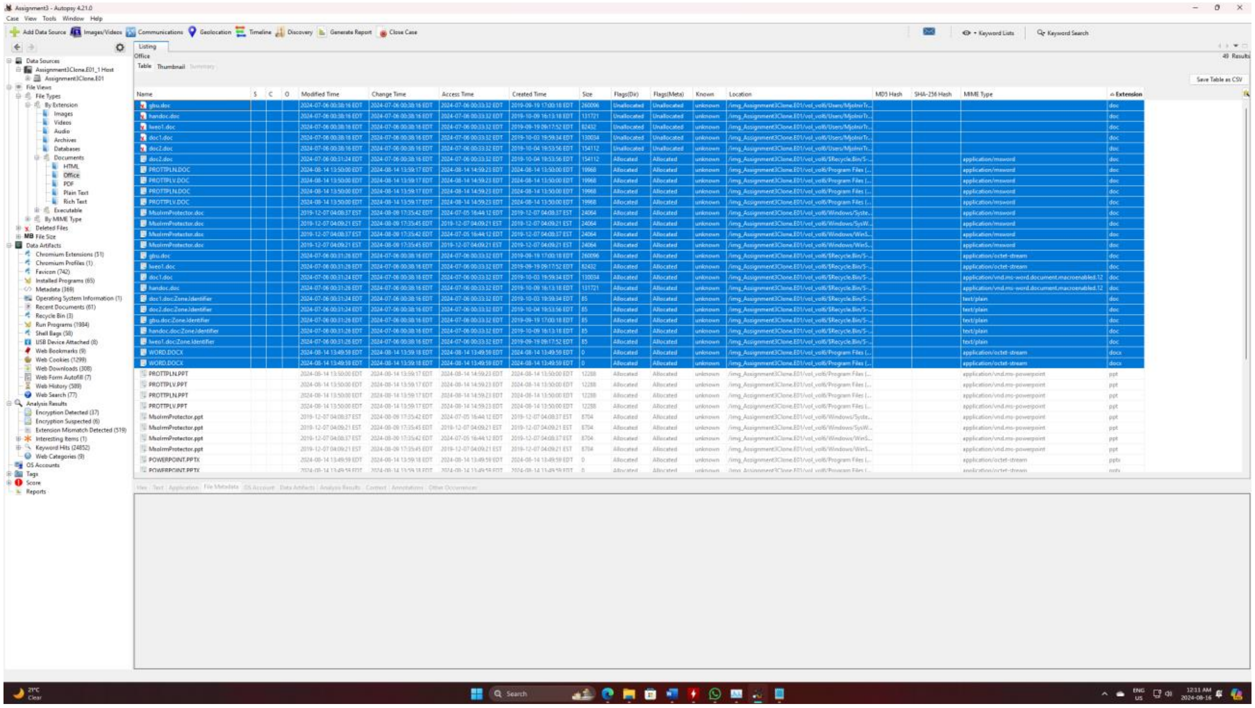


Source Name	S	C	O	Domain	Text	Program Name	Date Accessed	Data Source
History				google.com	Rosales Romo, Alejandro	Microsoft Edge	2024-08-14 14:23:04 EDT	Assignment3Clone.E01
History				google.com	Rosales Romo, Alejandro	Microsoft Edge	2024-08-14 14:23:04 EDT	Assignment3Clone.E01
History				google.com	Pillai, Raj Vikraman	Microsoft Edge	2024-08-14 14:22:19 EDT	Assignment3Clone.E01
History				google.com	Pillai, Raj Vikraman	Microsoft Edge	2024-08-14 14:22:19 EDT	Assignment3Clone.E01
History				google.com	Patterson, Jordan	Microsoft Edge	2024-08-14 14:21:40 EDT	Assignment3Clone.E01
History				google.com	Patterson, Jordan	Microsoft Edge	2024-08-14 14:21:40 EDT	Assignment3Clone.E01
History				google.com	Pathuri, Monisha	Microsoft Edge	2024-08-14 14:21:03 EDT	Assignment3Clone.E01
History				google.com	Pathuri, Monisha	Microsoft Edge	2024-08-14 14:21:03 EDT	Assignment3Clone.E01
History				google.com	Pandey, Smita Sanjay	Microsoft Edge	2024-08-14 14:20:26 EDT	Assignment3Clone.E01
History				google.com	Pandey, Smita Sanjay	Microsoft Edge	2024-08-14 14:20:26 EDT	Assignment3Clone.E01
History				google.com	Ozoemena, Onyinye Gift	Microsoft Edge	2024-08-14 14:19:17 EDT	Assignment3Clone.E01
History				google.com	Ozoemena, Onyinye Gift	Microsoft Edge	2024-08-14 14:19:17 EDT	Assignment3Clone.E01
History				google.com	Lau, Ivan	Microsoft Edge	2024-08-14 14:18:35 EDT	Assignment3Clone.E01
History				google.com	Lau, Ivan	Microsoft Edge	2024-08-14 14:18:35 EDT	Assignment3Clone.E01
History				google.com	Kilic, Yigit	Microsoft Edge	2024-08-14 14:17:57 EDT	Assignment3Clone.E01
History				google.com	Kilic, Yigit	Microsoft Edge	2024-08-14 14:17:57 EDT	Assignment3Clone.E01
History				google.com	James, Sherin	Microsoft Edge	2024-08-14 14:17:06 EDT	Assignment3Clone.E01
History				google.com	James, Sherin	Microsoft Edge	2024-08-14 14:17:06 EDT	Assignment3Clone.E01
History				google.com	Iyapo, Johnson	Microsoft Edge	2024-08-14 14:15:26 EDT	Assignment3Clone.E01
History				google.com	Iyapo, Johnson	Microsoft Edge	2024-08-14 14:15:26 EDT	Assignment3Clone.E01
History				google.com	Ganeshan, Prema	Microsoft Edge	2024-08-14 14:14:44 EDT	Assignment3Clone.E01
History				google.com	Ganeshan, Prema	Microsoft Edge	2024-08-14 14:14:44 EDT	Assignment3Clone.E01
History				google.com	Doddy, Alekhya Sri Varshini	Microsoft Edge	2024-08-14 14:13:49 EDT	Assignment3Clone.E01
History				google.com	Doddy, Alekhya Sri Varshini	Microsoft Edge	2024-08-14 14:13:49 EDT	Assignment3Clone.E01
History				google.com	Das, Suparna	Microsoft Edge	2024-08-14 14:12:48 EDT	Assignment3Clone.E01
History				google.com	Das, Suparna	Microsoft Edge	2024-08-14 14:12:48 EDT	Assignment3Clone.E01
History				google.com	Chaudhary, Dushyant Singh	Microsoft Edge	2024-08-14 14:12:14 EDT	Assignment3Clone.E01
History				google.com	Chaudhary, Dushyant Singh	Microsoft Edge	2024-08-14 14:12:14 EDT	Assignment3Clone.E01
History				google.com	Caku, Gleni	Microsoft Edge	2024-08-14 14:11:36 EDT	Assignment3Clone.E01
History				google.com	Caku, Gleni	Microsoft Edge	2024-08-14 14:11:36 EDT	Assignment3Clone.E01
History				google.com	Brason, Paul	Microsoft Edge	2024-08-14 14:10:54 EDT	Assignment3Clone.E01
History				google.com	Brason, Paul	Microsoft Edge	2024-08-14 14:10:54 EDT	Assignment3Clone.E01
History				google.com	Bhadra, Prithvi Harshad	Microsoft Edge	2024-08-14 14:10:04 EDT	Assignment3Clone.E01
History				google.com	Bhadra, Prithvi Harshad	Microsoft Edge	2024-08-14 14:10:04 EDT	Assignment3Clone.E01
History				google.com	Bashir, Ammad	Microsoft Edge	2024-08-14 14:09:26 EDT	Assignment3Clone.E01

```
        129 https://gleni.co.uk/post/13-04-2024-milk-chocolate-blossom-cake Milk Chocolate Blossom Cake - Gleni 3 0 13368132710562095 0
        130 https://www.google.com/search?q=Chaudhary%2C+Dushyant+Singh&sca_esv=182cfa181496f90a&ei=V_O8ZpuvHYPcptQPj_jO8AY&ved=0ahUKEwjbtubAivWHAxUDrokEHQ-8E24Q4dUDCA8&uact=5&oq=Chaudhary%
2C+Dushyant+Singh&gs_lp=Egxnd3Mtd2l6LXNlcnAiGUNoYXVkaGFyeSwgRHVzaHlhbnQgU2luZ2hIoBFQnwpYnwpwBHgAkAEAmAFBoAFBqgEBMbgBA8gBAPgBAvgBAZgCBKACCcICCRAAGLADGAgYHsICDhAAGIAEGLADGIYDGIoFwgILEAAYgAQYsAMYogSYAwCIBgGQBgWSBwE0oAct&sclient=gws-wiz-serp Chaudhary, Dushyant
Singh - Google Search 2 0 13368132734659646 0
        131 https://ca.linkedin.com/in/dushyantgarud96 Dushyant Singh Chaudhary - Canadian Tire Corporation | LinkedIn 1 0 13368132736362965 0
        132 https://www.instagram.com/dushyant3451/ Dushyant Singh Chaudhary (@dushyant3451) • Instagram photos and videos 2 0 13368132738004258 0
        133 https://m.facebook.com/public/Chaudhary-Dushyant-Singh Chaudhary Dushyant Singh Profiles 1 0 13368132739485895 0
        134 https://www.facebook.com/public/Chaudhary-Dushyant-Singh?_rdr Chaudhary Dushyant Singh Profiles 1 0 13368132739485895 0
        135 https://www.instagram.com/dushyantsinghchaudhary/ Dushyant Singh Chaudhary (@dushyantsinghchaudhary) • Instagram photos and videos 2 0 13368132740608120 0
        136 https://m.facebook.com/people/Chaudhary-Dushyant-Singh/100010634737690/ Chaudhary Dushyant Singh | Facebook 1 0 13368132742383023 0
        137 https://www.facebook.com/people/Chaudhary-Dushyant-Singh/100010634737690/?_rdr Chaudhary Dushyant Singh | Facebook 1 0 13368132742383023 0
        138 https://www.facebook.com/people/Chaudhary-Dushyant-Singh/pfbid0NXnivSqwbLooXhHGEwXGfGXFGXfh7UsVAuqAwTzC9TytAy3ksZpVdstEmH6835Pl/ Chaudhary Dushyant Singh | Facebook 2 0 13368132742682010 0
        139 https://www.google.com/search?q=Das%2C+Suparna&sca_esv=182cfa181496f90a&ei=ffO8ZsebONKB5OMPh97ziQQ&ved=0ahUKEwiHzpDTivWHAxXSAHkGHQfvPEEQ4dUDCA8&uact=5&oq=Das%
2C+Suparna&gs_lp=Egxnd3Mtd2l6LXNlcnAiDERhcywgU3VwYXJuYTIGEAAYFhgeMgYQABgWGB4yBhAAGBYYHjIGEAAYFhgeMgYQABgWGB4yBhAAGBYYHjIGEAAYFhgeMgsQABiABBiGAxiKBTILEAAYgAQYhgMYigUyCxAAGIAEGIYDGIoFSIQDUABYAHAAeACQAQCYAWGgAWGqAQMwLjG4AQPIAQD4AQL4AQGYAgGgAnOYAwCSBwM
wLjGgB5cG&sclient=gws-wiz-serp Das, Suparna - Google Search 2 0 13368132768143047 0
        140 https://www.aag.org/profile/suparna-das/ Suparna Das - AAG 1 0 13368132770018511 0
        141 https://ca.linkedin.com/in/suparna-das-01 Suparna Das - Bharat Ambulance | LinkedIn 1 0 13368132771598199 0
        142 https://www.instagram.com/isuparna/ Suparna Das (@isuparna) • Instagram photos and videos 2 0 13368132773550318 0
        143 https://www.linkedin.com/in/suparna-das-a51b2227 Suparna Das - Substance Abuse and Mental Health Services Administration (SAMHSA) | LinkedIn 1 0 13368132775383596 0
```

Who is the author of all word documents?

I first found all of the word documents by going into the “FileViews” tab and then into the “Documents” tab and then chooseing Office files. Once the office files were displayed I sorted them by filetype. This revealed that 25 word documents were found on the system. 23 .doc and 2 .docx files.



Office

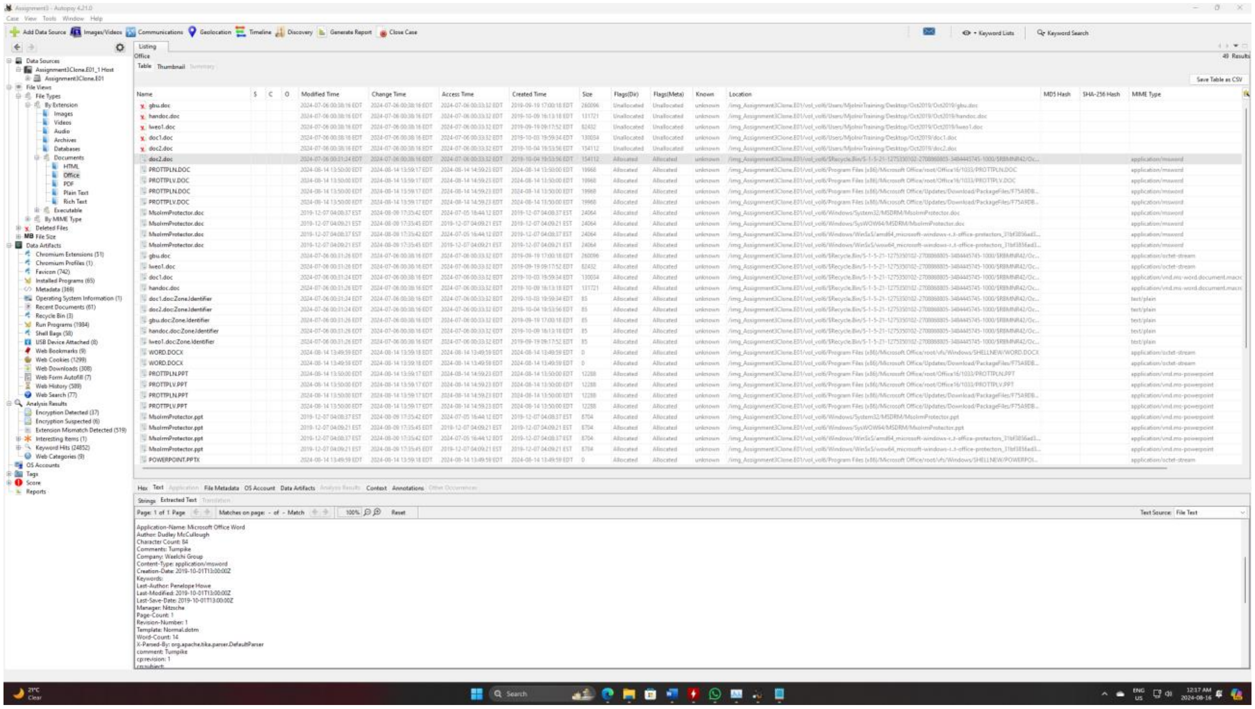
49 Results

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location	MD5 Hash	SHA-256 Hash	MIME Type	Extension
gbu.doc				2024-07-06 00:38:16 EDT	2024-07-06 00:38:16 EDT	2024-07-06 00:33:32 EDT	2019-09-19 17:00:18 EDT	260096	Unallocated	Unallocated	unknown	/img_Assignment3Clone.E01/vol_vol6/Users/MjolnirTr...				doc
handoc.doc				2024-07-06 00:38:16 EDT	2024-07-06 00:38:16 EDT	2024-07-06 00:33:32 EDT	2019-10-09 16:13:18 EDT	131721	Unallocated	Unallocated	unknown	/img_Assignment3Clone.E01/vol_vol6/Users/MjolnirTr...				doc
lweo1.doc				2024-07-06 00:38:16 EDT	2024-07-06 00:38:16 EDT	2024-07-06 00:33:32 EDT	2019-09-19 09:17:52 EDT	82432	Unallocated	Unallocated	unknown	/img_Assignment3Clone.E01/vol_vol6/Users/MjolnirTr...				doc
doc1.doc				2024-07-06 00:38:16 EDT	2024-07-06 00:38:16 EDT	2024-07-06 00:33:32 EDT	2019-10-03 19:59:34 EDT	130034	Unallocated	Unallocated	unknown	/img_Assignment3Clone.E01/vol_vol6/Users/MjolnirTr...				doc
doc2.doc				2024-07-06 00:38:16 EDT	2024-07-06 00:38:16 EDT	2024-07-06 00:33:32 EDT	2019-10-04 19:53:56 EDT	154112	Unallocated	Unallocated	unknown	/img_Assignment3Clone.E01/vol_vol6/Users/MjolnirTr...				doc
doc2.doc				2024-07-06 00:31:24 EDT	2024-07-06 00:38:16 EDT	2024-07-06 00:33:32 EDT	2019-10-04 19:53:56 EDT	154112	Allocated	Allocated	unknown	/img_Assignment3Clone.E01/vol_vol6/$Recycle.Bin/S-...			application/msword	doc
PROTTPLN.DOC				2024-08-14 13:50:00 EDT	2024-08-14 13:59:17 EDT	2024-08-14 14:59:23 EDT	2024-08-14 13:50:00 EDT	19968	Allocated	Allocated	unknown	/img_Assignment3Clone.E01/vol_vol6/Program Files (...			application/msword	doc
PROTTPLV.DOC				2024-08-14 13:50:00 EDT	2024-08-14 13:59:17 EDT	2024-08-14 14:59:23 EDT	2024-08-14 13:50:00 EDT	19968	Allocated	Allocated	unknown	/img_Assignment3Clone.E01/vol_vol6/Program Files (...			application/msword	doc
PROTTPLN.DOC				2024-08-14 13:50:00 EDT	2024-08-14 13:59:17 EDT	2024-08-14 14:59:23 EDT	2024-08-14 13:50:00 EDT	19968	Allocated	Allocated	unknown	/img_Assignment3Clone.E01/vol_vol6/Program Files (...			application/msword	doc
PROTTPLV.DOC				2024-08-14 13:50:00 EDT	2024-08-14 13:59:17 EDT	2024-08-14 14:59:23 EDT	2024-08-14 13:50:00 EDT	19968	Allocated	Allocated	unknown	/img_Assignment3Clone.E01/vol_vol6/Program Files (...			application/msword	doc
MsoIrmProtector.doc				2019-12-07 04:08:37 EST	2024-08-09 17:35:42 EDT	2024-07-05 16:44:12 EDT	2019-12-07 04:08:37 EST	24064	Allocated	Allocated	unknown	/img_Assignment3Clone.E01/vol_vol6/Windows/Syste...			application/msword	doc
MsoIrmProtector.doc				2019-12-07 04:09:21 EST	2024-08-09 17:35:45 EDT	2019-12-07 04:09:21 EST	2019-12-07 04:09:21 EST	24064	Allocated	Allocated	unknown	/img_Assignment3Clone.E01/vol_vol6/Windows/SysW...			application/msword	doc
MsoIrmProtector.doc				2019-12-07 04:08:37 EST	2024-08-09 17:35:42 EDT	2024-07-05 16:44:12 EDT	2019-12-07 04:08:37 EST	24064	Allocated	Allocated	unknown	/img_Assignment3Clone.E01/vol_vol6/Windows/WinS...			application/msword	doc
MsoIrmProtector.doc				2019-12-07 04:09:21 EST	2024-08-09 17:35:45 EDT	2019-12-07 04:09:21 EST	2019-12-07 04:09:21 EST	24064	Allocated	Allocated	unknown	/img_Assignment3Clone.E01/vol_vol6/Windows/WinS...			application/msword	doc
gbu.doc				2024-07-06 00:31:26 EDT	2024-07-06 00:38:16 EDT	2024-07-06 00:33:32 EDT	2019-09-19 17:00:18 EDT	260096	Allocated	Allocated	unknown	/img_Assignment3Clone.E01/vol_vol6/$Recycle.Bin/S-...			application/octet-stream	doc
lweo1.doc				2024-07-06 00:31:28 EDT	2024-07-06 00:38:16 EDT	2024-07-06 00:33:32 EDT	2019-09-19 09:17:52 EDT	82432	Allocated	Allocated	unknown	/img_Assignment3Clone.E01/vol_vol6/$Recycle.Bin/S-...			application/octet-stream	doc
doc1.doc				2024-07-06 00:31:24 EDT	2024-07-06 00:38:16 EDT	2024-07-06 00:33:32 EDT	2019-10-03 19:59:34 EDT	130034	Allocated	Allocated	unknown	/img_Assignment3Clone.E01/vol_vol6/$Recycle.Bin/S-...			application/vnd.ms-word.document.macroenabled.12	doc
handoc.doc				2024-07-06 00:31:26 EDT	2024-07-06 00:38:16 EDT	2024-07-06 00:33:32 EDT	2019-10-09 16:13:18 EDT	131721	Allocated	Allocated	unknown	/img_Assignment3Clone.E01/vol_vol6/$Recycle.Bin/S-...			application/vnd.ms-word.document.macroenabled.12	doc
doc1.doc:Zone.Identifier				2024-07-06 00:31:24 EDT	2024-07-06 00:38:16 EDT	2024-07-06 00:33:32 EDT	2019-10-03 19:59:34 EDT	85	Allocated	Allocated	unknown	/img_Assignment3Clone.E01/vol_vol6/$Recycle.Bin/S-...			text/plain	doc
doc2.doc:Zone.Identifier				2024-07-06 00:31:24 EDT	2024-07-06 00:38:16 EDT	2024-07-06 00:33:32 EDT	2019-10-04 19:53:56 EDT	85	Allocated	Allocated	unknown	/img_Assignment3Clone.E01/vol_vol6/$Recycle.Bin/S-...			text/plain	doc
gbu.doc:Zone.Identifier				2024-07-06 00:31:26 EDT	2024-07-06 00:38:16 EDT	2024-07-06 00:33:32 EDT	2019-09-19 17:00:18 EDT	85	Allocated	Allocated	unknown	/img_Assignment3Clone.E01/vol_vol6/$Recycle.Bin/S-...			text/plain	doc
handoc.doc:Zone.Identifier				2024-07-06 00:31:26 EDT	2024-07-06 00:38:16 EDT	2024-07-06 00:33:32 EDT	2019-10-09 16:13:18 EDT	85	Allocated	Allocated	unknown	/img_Assignment3Clone.E01/vol_vol6/$Recycle.Bin/S-...			text/plain	doc
lweo1.doc:Zone.Identifier				2024-07-06 00:31:28 EDT	2024-07-06 00:38:16 EDT	2024-07-06 00:33:32 EDT	2019-09-19 09:17:52 EDT	85	Allocated	Allocated	unknown	/img_Assignment3Clone.E01/vol_vol6/$Recycle.Bin/S-...			text/plain	doc
WORD.DOCX				2024-08-14 13:49:59 EDT	2024-08-14 13:59:18 EDT	2024-08-14 13:49:59 EDT	2024-08-14 13:49:59 EDT	0	Allocated	Allocated	unknown	/img_Assignment3Clone.E01/vol_vol6/Program Files (...			application/octet-stream	docx
WORD.DOCX				2024-08-14 13:49:59 EDT	2024-08-14 13:59:18 EDT	2024-08-14 13:49:59 EDT	2024-08-14 13:49:59 EDT	0	Allocated	Allocated	unknown	/img_Assignment3Clone.E01/vol_vol6/Program Files (...			application/octet-stream	docx
PROTTPLN.PPT				2024-08-14 13:50:00 EDT	2024-08-14 13:59:17 EDT	2024-08-14 14:59:23 EDT	2024-08-14 13:50:00 EDT	12288	Allocated	Allocated	unknown	/img_Assignment3Clone.E01/vol_vol6/Program Files (...			application/vnd.ms-powerpoint	ppt
PROTTPLV.PPT				2024-08-14 13:50:00 EDT	2024-08-14 13:59:17 EDT	2024-08-14 14:59:23 EDT	2024-08-14 13:50:00 EDT	12288	Allocated	Allocated	unknown	/img_Assignment3Clone.E01/vol_vol6/Program Files (...			application/vnd.ms-powerpoint	ppt
PROTTPLN.PPT				2024-08-14 13:50:00 EDT	2024-08-14 13:59:17 EDT	2024-08-14 14:59:23 EDT	2024-08-14 13:50:00 EDT	12288	Allocated	Allocated	unknown	/img_Assignment3Clone.E01/vol_vol6/Program Files (...			application/vnd.ms-powerpoint	ppt
PROTTPLV.PPT				2024-08-14 13:50:00 EDT	2024-08-14 13:59:17 EDT	2024-08-14 14:59:23 EDT	2024-08-14 13:50:00 EDT	12288	Allocated	Allocated	unknown	/img_Assignment3Clone.E01/vol_vol6/Program Files (...			application/vnd.ms-powerpoint	ppt
MsoIrmProtector.ppt				2019-12-07 04:08:37 EST	2024-08-09 17:35:42 EDT	2024-07-05 16:44:12 EDT	2019-12-07 04:08:37 EST	8704	Allocated	Allocated	unknown	/img_Assignment3Clone.E01/vol_vol6/Windows/Syste...			application/vnd.ms-powerpoint	ppt
MsoIrmProtector.ppt				2019-12-07 04:09:21 EST	2024-08-09 17:35:45 EDT	2019-12-07 04:09:21 EST	2019-12-07 04:09:21 EST	8704	Allocated	Allocated	unknown	/img_Assignment3Clone.E01/vol_vol6/Windows/SysW...			application/vnd.ms-powerpoint	ppt
MsoIrmProtector.ppt				2019-12-07 04:08:37 EST	2024-08-09 17:35:42 EDT	2024-07-05 16:44:12 EDT	2019-12-07 04:08:37 EST	8704	Allocated	Allocated	unknown	/img_Assignment3Clone.E01/vol_vol6/Windows/WinS...			application/vnd.ms-powerpoint	ppt
MsoIrmProtector.ppt				2019-12-07 04:09:21 EST	2024-08-09 17:35:45 EDT	2019-12-07 04:09:21 EST	2019-12-07 04:09:21 EST	8704	Allocated	Allocated	unknown	/img_Assignment3Clone.E01/vol_vol6/Windows/WinS...			application/vnd.ms-powerpoint	ppt
POWERPOINT.PPTX				2024-08-14 13:49:59 EDT	2024-08-14 13:59:18 EDT	2024-08-14 13:49:59 EDT	2024-08-14 13:49:59 EDT	0	Allocated	Allocated	unknown	/img_Assignment3Clone.E01/vol_vol6/Program Files (...			application/octet-stream	pptx
POWERPOINT.PPTX				2024-08-14 13:49:59 EDT	2024-08-14 13:59:18 EDT	2024-08-14 13:49:59 EDT	2024-08-14 13:49:59 EDT	0	Allocated	Allocated	unknown	/img_Assignment3Clone.E01/vol_vol6/Program Files (...			application/octet-stream	pptx

After looking at the text and metadata of all of the documents only 1 seemed to have a legitimate author.

Doc2.doc found at the path below was authored by someone named Dudley McCullough and then further authored by Penelope Howe. The company that they/the file belongs to is Waelchi Group.

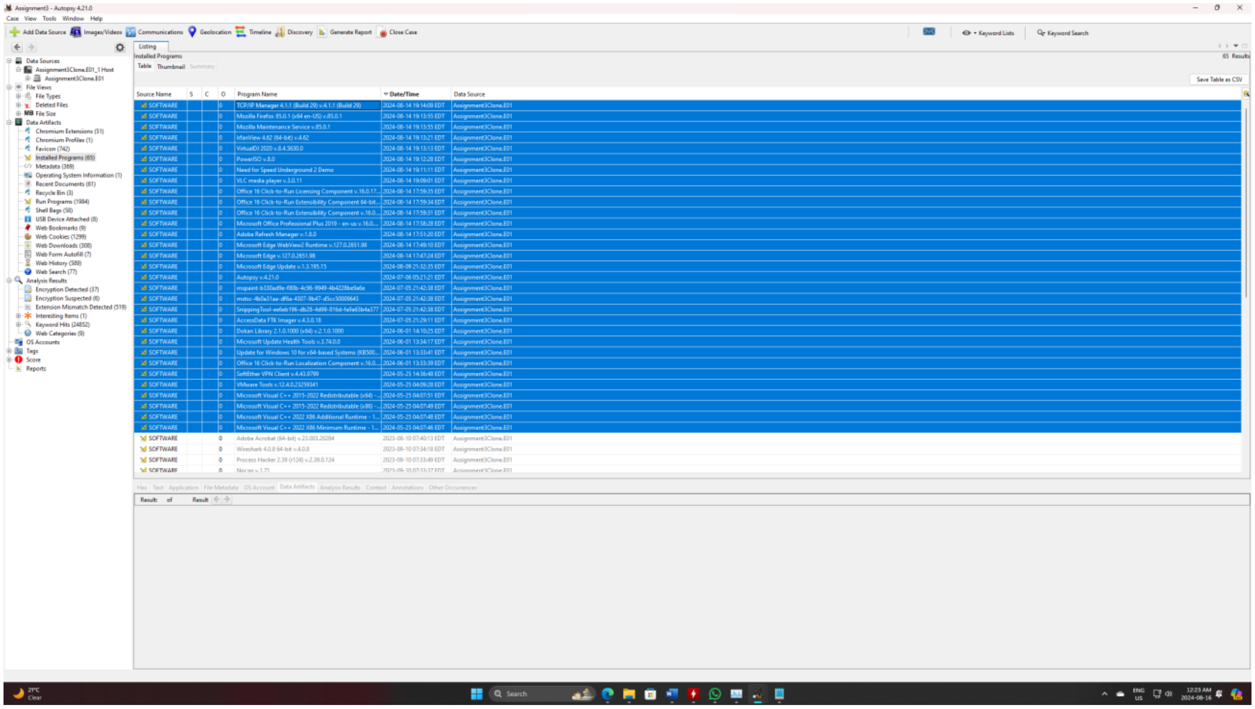
/img_Assignment3Clone.E01/vol_vol6/$Recycle.Bin/S-1-5-21-1275350102-2708868805-3484445745-1000/$RBMNR42/Oct2019/doc2.doc



```
Application-Name: Microsoft Office Word
Author: Dudley McCullough
Character Count: 84
Comments: Turnpike
Company: Waelchi Group
Content-Type: application/msword
Creation-Date: 2019-10-01T13:00:00Z
Keywords:
Last-Author: Penelope Howe
Last-Modified: 2019-10-01T13:00:00Z
Last-Save-Date: 2019-10-01T13:00:00Z
Manager: Nitzsche
Page-Count: 1
Revision-Number: 1
Template: Normal.dotm
Word-Count: 14
X-Parsed-By: org.apache.tika.parser.DefaultParser
comment: Turnpike
cp:revision: 1
cp:subject:
```

What applications were installed in 2024 and their paths?

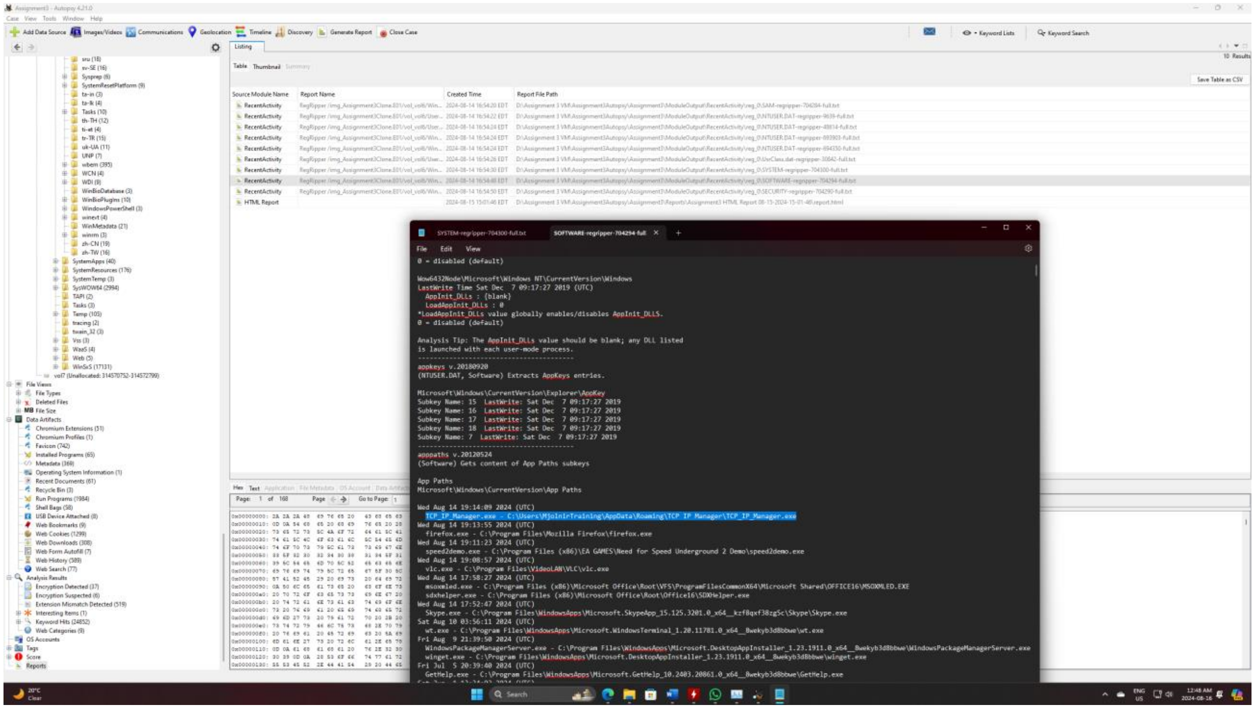
I inspected the “Installed Programs” tab of Autopsy and found that 31 applications in the list were installed in 2024.



Source Name	S	C	O	Program Name	Date/Time	Data Source
SOFTWARE			0	TCP/IP Manager 4.1.1 (Build 29) v.4.1.1 (Build 29)	2024-08-14 19:14:09 EDT	Assignment3Clone.E01
SOFTWARE			0	Mozilla Firefox 85.0.1 (x64 en-US) v.85.0.1	2024-08-14 19:13:55 EDT	Assignment3Clone.E01
SOFTWARE			0	Mozilla Maintenance Service v.85.0.1	2024-08-14 19:13:55 EDT	Assignment3Clone.E01
SOFTWARE			0	IrfanView 4.62 (64-bit) v.4.62	2024-08-14 19:13:21 EDT	Assignment3Clone.E01
SOFTWARE			0	VirtualDJ 2020 v.8.4.5630.0	2024-08-14 19:13:13 EDT	Assignment3Clone.E01
SOFTWARE			0	PowerISO v.8.0	2024-08-14 19:12:28 EDT	Assignment3Clone.E01
SOFTWARE			0	Need for Speed Underground 2 Demo	2024-08-14 19:11:11 EDT	Assignment3Clone.E01
SOFTWARE			0	VLC media player v.3.0.11	2024-08-14 19:09:01 EDT	Assignment3Clone.E01
SOFTWARE			0	Office 16 Click-to-Run Licensing Component v.16.0.17...	2024-08-14 17:59:35 EDT	Assignment3Clone.E01
SOFTWARE			0	Office 16 Click-to-Run Extensibility Component 64-bit...	2024-08-14 17:59:34 EDT	Assignment3Clone.E01
SOFTWARE			0	Office 16 Click-to-Run Extensibility Component v.16.0...	2024-08-14 17:59:31 EDT	Assignment3Clone.E01
SOFTWARE			0	Microsoft Office Professional Plus 2019 - en-us v.16.0...	2024-08-14 17:58:28 EDT	Assignment3Clone.E01
SOFTWARE			0	Adobe Refresh Manager v.1.8.0	2024-08-14 17:51:20 EDT	Assignment3Clone.E01
SOFTWARE			0	Microsoft Edge WebView2 Runtime v.127.0.2651.98	2024-08-14 17:49:10 EDT	Assignment3Clone.E01
SOFTWARE			0	Microsoft Edge v.127.0.2651.98	2024-08-14 17:47:24 EDT	Assignment3Clone.E01
SOFTWARE			0	Microsoft Edge Update v.1.3.195.15	2024-08-09 21:32:35 EDT	Assignment3Clone.E01
SOFTWARE			0	Autopsy v.4.21.0	2024-07-06 05:21:21 EDT	Assignment3Clone.E01
SOFTWARE			0	mspaint-b330ad9e-f80b-4c96-9949-4b4228be9a6e	2024-07-05 21:42:38 EDT	Assignment3Clone.E01
SOFTWARE			0	mstsc-4b0a31aa-df6a-4307-9b47-d5cc50009643	2024-07-05 21:42:38 EDT	Assignment3Clone.E01
SOFTWARE			0	SnippingTool-ee6eb196-db28-4d99-816d-fa9a63b4a377	2024-07-05 21:42:38 EDT	Assignment3Clone.E01
SOFTWARE			0	AccessData FTK Imager v.4.3.0.18	2024-07-05 21:29:11 EDT	Assignment3Clone.E01
SOFTWARE			0	Dokan Library 2.1.0.1000 (x64) v.2.1.0.1000	2024-06-01 14:10:25 EDT	Assignment3Clone.E01
SOFTWARE			0	Microsoft Update Health Tools v.3.74.0.0	2024-06-01 13:34:17 EDT	Assignment3Clone.E01
SOFTWARE			0	Update for Windows 10 for x64-based Systems (KB500...	2024-06-01 13:33:41 EDT	Assignment3Clone.E01
SOFTWARE			0	Office 16 Click-to-Run Localization Component v.16.0...	2024-06-01 13:33:39 EDT	Assignment3Clone.E01
SOFTWARE			0	SoftEther VPN Client v.4.43.9799	2024-05-25 14:36:48 EDT	Assignment3Clone.E01
SOFTWARE			0	VMware Tools v.12.4.0.23259341	2024-05-25 04:09:28 EDT	Assignment3Clone.E01
SOFTWARE			0	Microsoft Visual C++ 2015-2022 Redistributable (x64) -...	2024-05-25 04:07:51 EDT	Assignment3Clone.E01
SOFTWARE			0	Microsoft Visual C++ 2015-2022 Redistributable (x86) -...	2024-05-25 04:07:49 EDT	Assignment3Clone.E01
SOFTWARE			0	Microsoft Visual C++ 2022 X86 Additional Runtime - 1...	2024-05-25 04:07:48 EDT	Assignment3Clone.E01
SOFTWARE			0	Microsoft Visual C++ 2022 X86 Minimum Runtime - 1...	2024-05-25 04:07:46 EDT	Assignment3Clone.E01
SOFTWARE			0	Adobe Acrobat (64-bit) v.23.003.20284	2023-09-10 07:40:13 EDT	Assignment3Clone.E01
SOFTWARE			0	Wireshark 4.0.8 64-bit v.4.0.8	2023-09-10 07:34:18 EDT	Assignment3Clone.E01
SOFTWARE			0	Process Hacker 2.39 (r124) v.2.39.0.124	2023-09-10 07:33:49 EDT	Assignment3Clone.E01
SOFTWARE			0	Npcap v.1.71	2023-09-10 07:33:37 EDT	Assignment3Clone.E01

I then removed items from the list that were clearly components of the same install (example: Mozilla Maintenance Service is a part of Mozilla Firefox) and any installs that were clearly just a windows update or windows component updated by a Windows update. This left us with 12 legitimate installations 2024.

While the “Installed Programs” tab provided me with a list of applications installed in 2024, it did not seem to give me their path but instead gave me where the programs information was stored in the registry. I then opened the regripper Registry SOFTWARE report and searched for the applications in my list to get their actual installation paths.



Source Module Name	Report Name	Created Time	Report File Path
RecentActivity	RegRipper /img_Assignment3Clone.E01/vol_vol6/Win...	2024-08-14 16:54:20 EDT	D:\Assignment 3 VM\Assignment3Autopsy\Assignment3\ModuleOutput\RecentActivity\reg_0\SAM-regripper-704284-full.txt
RecentActivity	RegRipper /img_Assignment3Clone.E01/vol_vol6/User...	2024-08-14 16:54:22 EDT	D:\Assignment 3 VM\Assignment3Autopsy\Assignment3\ModuleOutput\RecentActivity\reg_0\NTUSER.DAT-regripper-9639-full.txt
RecentActivity	RegRipper /img_Assignment3Clone.E01/vol_vol6/User...	2024-08-14 16:54:24 EDT	D:\Assignment 3 VM\Assignment3Autopsy\Assignment3\ModuleOutput\RecentActivity\reg_0\NTUSER.DAT-regripper-48814-full.txt
RecentActivity	RegRipper /img_Assignment3Clone.E01/vol_vol6/Win...	2024-08-14 16:54:24 EDT	D:\Assignment 3 VM\Assignment3Autopsy\Assignment3\ModuleOutput\RecentActivity\reg_0\NTUSER.DAT-regripper-693903-full.txt
RecentActivity	RegRipper /img_Assignment3Clone.E01/vol_vol6/Win...	2024-08-14 16:54:24 EDT	D:\Assignment 3 VM\Assignment3Autopsy\Assignment3\ModuleOutput\RecentActivity\reg_0\NTUSER.DAT-regripper-694330-full.txt
RecentActivity	RegRipper /img_Assignment3Clone.E01/vol_vol6/User...	2024-08-14 16:54:26 EDT	D:\Assignment 3 VM\Assignment3Autopsy\Assignment3\ModuleOutput\RecentActivity\reg_0\UsrClass.dat-regripper-30842-full.txt
RecentActivity	RegRipper /img_Assignment3Clone.E01/vol_vol6/Win...	2024-08-14 16:54:30 EDT	D:\Assignment 3 VM\Assignment3Autopsy\Assignment3\ModuleOutput\RecentActivity\reg_0\SYSTEM-regripper-704300-full.txt
RecentActivity	RegRipper /img_Assignment3Clone.E01/vol_vol6/Win...	2024-08-14 16:54:48 EDT	D:\Assignment 3 VM\Assignment3Autopsy\Assignment3\ModuleOutput\RecentActivity\reg_0\SOFTWARE-regripper-704294-full.txt
RecentActivity	RegRipper /img_Assignment3Clone.E01/vol_vol6/Win...	2024-08-14 16:54:50 EDT	D:\Assignment 3 VM\Assignment3Autopsy\Assignment3\ModuleOutput\RecentActivity\reg_0\SECURITY-regripper-704290-full.txt
HTML Report		2024-08-15 15:01:46 EDT	D:\Assignment 3 VM\Assignment3Autopsy\Assignment3\Reports\Assignment3 HTML Report 08-15-2024-15-01-46\report.html

```
0 = disabled (default)

Wow6432Node\Microsoft\Windows NT\CurrentVersion\Windows
LastWrite Time Sat Dec  7 09:17:27 2019 (UTC)
  AppInit_DLLs : {blank}
  LoadAppInit_DLLs : 0
*LoadAppInit_DLLs value globally enables/disables AppInit_DLLS.
0 = disabled (default)

Analysis Tip: The AppInit_DLLs value should be blank; any DLL listed
is launched with each user-mode process.
----------------------------------------
appkeys v.20180920
(NTUSER.DAT, Software) Extracts AppKeys entries.

Microsoft\Windows\CurrentVersion\Explorer\AppKey
Subkey Name: 15  LastWrite: Sat Dec  7 09:17:27 2019
Subkey Name: 16  LastWrite: Sat Dec  7 09:17:27 2019
Subkey Name: 17  LastWrite: Sat Dec  7 09:17:27 2019
Subkey Name: 18  LastWrite: Sat Dec  7 09:17:27 2019
Subkey Name: 7  LastWrite: Sat Dec  7 09:17:27 2019
----------------------------------------
apppaths v.20120524
(Software) Gets content of App Paths subkeys

App Paths
Microsoft\Windows\CurrentVersion\App Paths

Wed Aug 14 19:14:09 2024 (UTC)
  TCP_IP_Manager.exe - C:\Users\MjolnirTraining\AppData\Roaming\TCP IP Manager\TCP_IP_Manager.exe
Wed Aug 14 19:13:55 2024 (UTC)
  firefox.exe - C:\Program Files\Mozilla Firefox\firefox.exe
Wed Aug 14 19:11:23 2024 (UTC)
  speed2demo.exe - C:\Program Files (x86)\EA GAMES\Need for Speed Underground 2 Demo\speed2demo.exe
Wed Aug 14 19:08:57 2024 (UTC)
  vlc.exe - C:\Program Files\VideoLAN\VLC\vlc.exe
Wed Aug 14 17:58:27 2024 (UTC)
  msoxmled.exe - C:\Program Files (x86)\Microsoft Office\Root\VFS\ProgramFilesCommonX64\Microsoft Shared\OFFICE16\MSOXMLED.EXE
  sdxhelper.exe - C:\Program Files (x86)\Microsoft Office\Root\Office16\SDXHelper.exe
Wed Aug 14 17:52:47 2024 (UTC)
  Skype.exe - C:\Program Files\WindowsApps\Microsoft.SkypeApp_15.125.3201.0_x64__kzf8qxf38zg5c\Skype\Skype.exe
Sat Aug 10 03:56:11 2024 (UTC)
  wt.exe - C:\Program Files\WindowsApps\Microsoft.WindowsTerminal_1.20.11781.0_x64__8wekyb3d8bbwe\wt.exe
Fri Aug  9 21:39:50 2024 (UTC)
  WindowsPackageManagerServer.exe - C:\Program Files\WindowsApps\Microsoft.DesktopAppInstaller_1.23.1911.0_x64__8wekyb3d8bbwe\WindowsPackageManagerServer.exe
  winget.exe - C:\Program Files\WindowsApps\Microsoft.DesktopAppInstaller_1.23.1911.0_x64__8wekyb3d8bbwe\winget.exe
Fri Jul  5 20:39:40 2024 (UTC)
  GetHelp.exe - C:\Program Files\WindowsApps\Microsoft.GetHelp_10.2403.20861.0_x64__8wekyb3d8bbwe\GetHelp.exe
```

The installed programs and their Paths are:

TCP/IP Manager 4.1.1

C:\Users\MjolnirTraining\AppData\Roaming\TCP IP Manager\TCP_IP_Manager.exe

Mozilla Firefox 85.0.1

C:\Program Files\Mozilla Firefox\firefox.exe

VirtualDJ 2020 v.8.4.5630.0

C:\Program Files\VirtualDJ\virtualdj8.exe

PowerISO v.8.0

C:\Program Files\PowerISO

Need for Speed Underground 2 Demo

C:\Program Files (x86)\EA GAMES\Need for Speed Underground 2 Demo\speed2demo.exe

VLC media player v.3.0.11

C:\Program Files\VideoLAN\VLC\vlc.exe

Microsoft Office Professional Plus 2019 - en-us v.16.0.17830.20138

C:\Program Files (x86)\Microsoft Office\Root\Office16

Autopsy v.4.21.0

C:\Program Files\Autopsy-4.21.0

AccessData FTK Imager v.4.3.0.18

C:\Users\MJOLNI~1\AppData\Local\Temp\{0693925F-95B9-4E99-9732-7C461AECC0CF}\AccessData_FTK_Imager_(x64).msi

Dokan Library 2.1.0.1000 (x64) v.2.1.0.1000

C:\Users\MjolnirTraining\Downloads\Dokan_x64.msi

SoftEther VPN Client v.4.43.9799

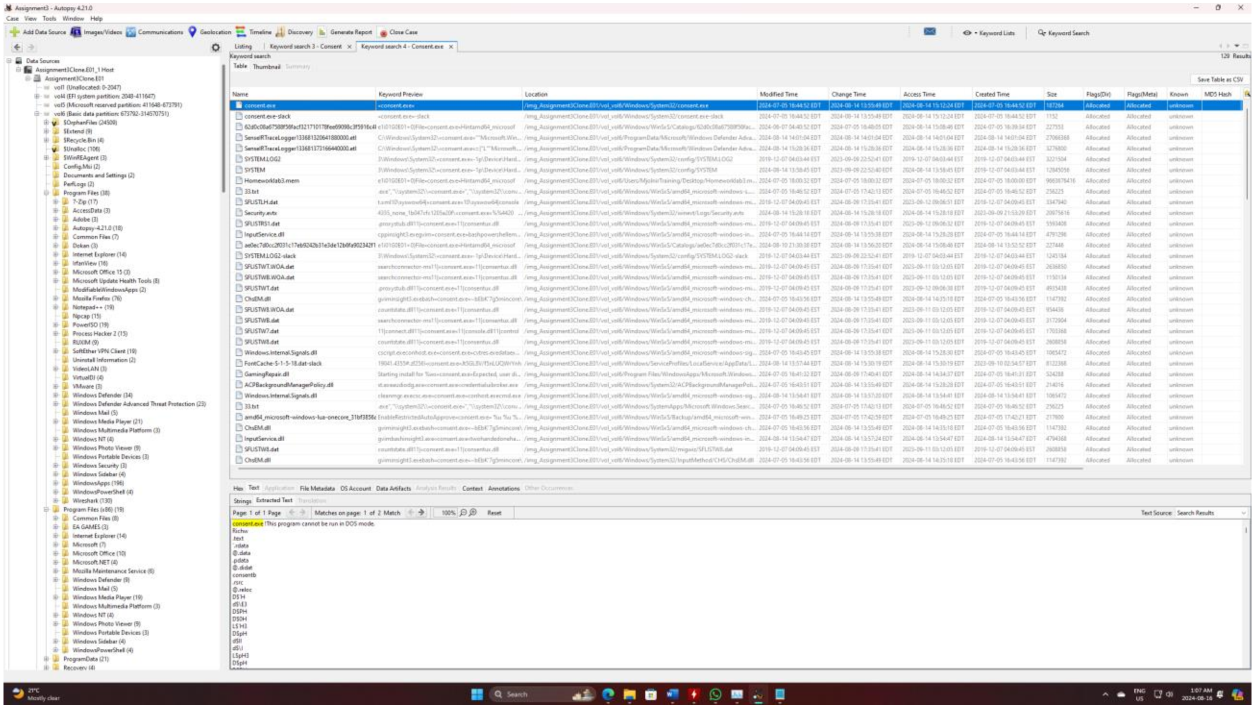
C:\Program Files\SoftEther VPN Client\vpnclient_x64.exe

VMware Tools v.12.4.0.23259341

C:\Program Files\VMware\VMware Tools\vmtoolsd.exe

Can you find consent?

I ran a keyword search for Consent and found a long list of consent. The consent that I believe we are looking for is found in /Windows/System32/Consent.exe



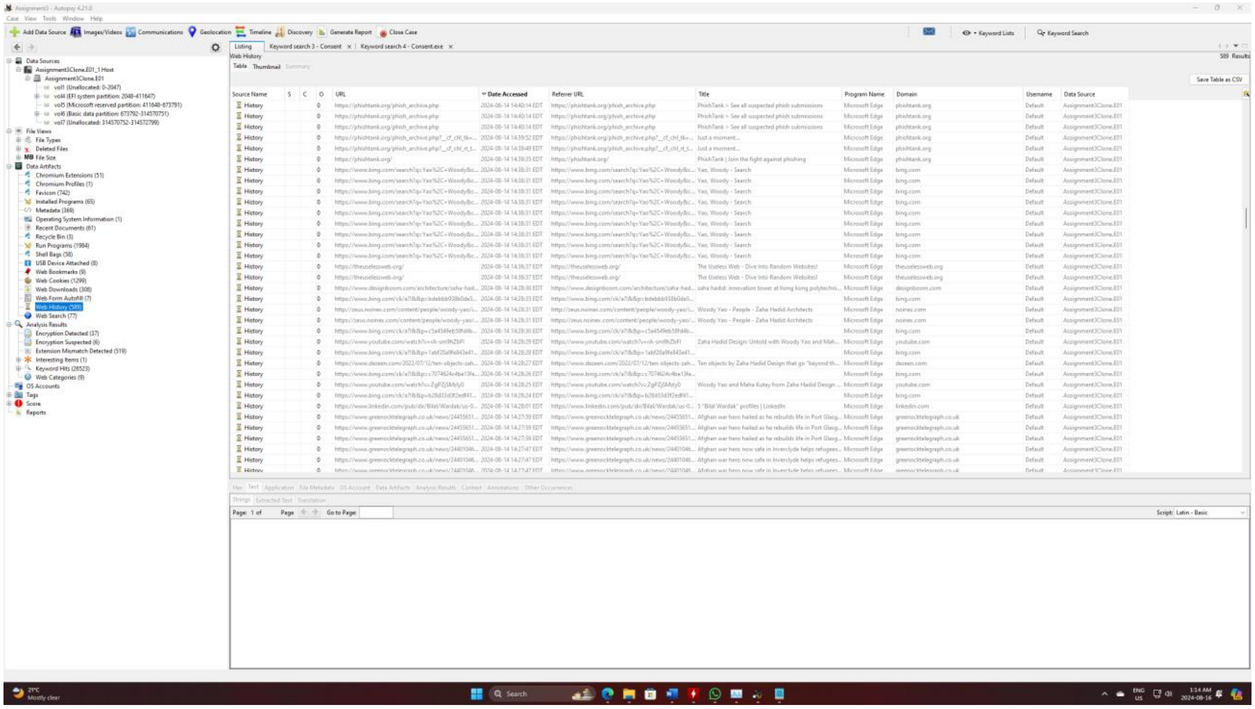
```
Data Sources
  Assignment3Clone.E01_1 Host
    Assignment3Clone.E01
      vol1 (Unallocated: 0-2047)
      vol4 (EFI system partition: 2048-411647)
      vol5 (Microsoft reserved partition: 411648-673791)
      vol6 (Basic data partition: 673792-314570751)
        $OrphanFiles (24509)
        $Extend (9)
        $Recycle.Bin (4)
        $Unalloc (106)
        $WinREAgent (3)
        Config.Msi (2)
        Documents and Settings (2)
        PerfLogs (2)
        Program Files (38)
          7-Zip (17)
          AccessData (3)
          Adobe (3)
          Autopsy-4.21.0 (18)
          Common Files (7)
          Dokan (3)
          Internet Explorer (14)
          IrfanView (16)
          Microsoft Office 15 (3)
          Microsoft Update Health Tools (8)
          ModifiableWindowsApps (2)
          Mozilla Firefox (76)
          Notepad++ (19)
          Npcap (15)
          PowerISO (19)
          Process Hacker 2 (15)
          RUXIM (9)
          SoftEther VPN Client (19)
          Uninstall Information (2)
          VideoLAN (3)
          VirtualDJ (4)
          VMware (3)
          Windows Defender (34)
          Windows Defender Advanced Threat Protection (23)
          Windows Mail (5)
          Windows Media Player (21)
          Windows Multimedia Platform (3)
          Windows NT (4)
          Windows Photo Viewer (9)
          Windows Portable Devices (3)
          Windows Security (3)
          Windows Sidebar (4)
          WindowsApps (196)
          WindowsPowerShell (4)
          Wireshark (130)
        Program Files (x86) (19)
          Common Files (8)
          EA GAMES (3)
          Internet Explorer (14)
          Microsoft (7)
          Microsoft Office (10)
          Microsoft.NET (4)
          Mozilla Maintenance Service (6)
          Windows Defender (9)
          Windows Mail (5)
          Windows Media Player (19)
          Windows Multimedia Platform (3)
          Windows NT (4)
          Windows Photo Viewer (9)
          Windows Portable Devices (3)
          Windows Sidebar (4)
          WindowsPowerShell (4)
        ProgramData (21)
        Recovery (4)
```

Name	Keyword Preview	Location	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	MD5 Hash
consent.exe	«consent.exe»	/img_Assignment3Clone.E01/vol_vol6/Windows/System32/consent.exe	2024-07-05 16:44:52 EDT	2024-08-14 13:55:49 EDT	2024-08-14 15:12:24 EDT	2024-07-05 16:44:52 EDT	187264	Allocated	Allocated	unknown	
consent.exe-slack	«consent.exe»-slack	/img_Assignment3Clone.E01/vol_vol6/Windows/System32/consent.exe-slack	2024-07-05 16:44:52 EDT	2024-08-14 13:55:49 EDT	2024-08-14 15:12:24 EDT	2024-07-05 16:44:52 EDT	1152	Allocated	Allocated	unknown	
62d0c08a67588f58facf321710178fee69098c3f5916c4l	e1\01G0E01+0|File«consent.exe»Hintamd64_microsof	/img_Assignment3Clone.E01/vol_vol6/Windows/WinSxS/Catalogs/62d0c08a67588f58fac...	2024-06-07 04:40:52 EDT	2024-07-05 16:48:05 EDT	2024-08-14 15:08:46 EDT	2024-07-05 16:39:34 EDT	227553	Allocated	Allocated	unknown	
SenseIRTraceLogger133681320641880000.etl	C:\Windows\System32\«consent.exe»"Microsoft.Win...	/img_Assignment3Clone.E01/vol_vol6/ProgramData/Microsoft/Windows Defender Adva...	2024-08-14 14:01:04 EDT	2024-08-14 14:01:04 EDT	2024-08-14 14:01:04 EDT	2024-08-14 14:01:04 EDT	27066368	Allocated	Allocated	unknown	
SenseIRTraceLogger133681373166440000.etl	C:\Windows\System32\«consent.exe»:|"L""Microsoft...	/img_Assignment3Clone.E01/vol_vol6/ProgramData/Microsoft/Windows Defender Adva...	2024-08-14 15:28:36 EDT	2024-08-14 15:28:36 EDT	2024-08-14 15:28:36 EDT	2024-08-14 15:28:36 EDT	3276800	Allocated	Allocated	unknown	
SYSTEM.LOG2	3\Windows\System32\«consent.exe»-1p\Device\Hard...	/img_Assignment3Clone.E01/vol_vol6/Windows/System32/config/SYSTEM.LOG2	2019-12-07 04:03:44 EST	2023-09-09 22:52:41 EDT	2019-12-07 04:03:44 EST	2019-12-07 04:03:44 EST	3221504	Allocated	Allocated	unknown	
SYSTEM	3\Windows\System32\«consent.exe»-1p\Device\Hard...	/img_Assignment3Clone.E01/vol_vol6/Windows/System32/config/SYSTEM	2024-08-14 13:58:45 EDT	2023-09-09 22:52:40 EDT	2024-08-14 13:58:45 EDT	2019-12-07 04:03:44 EST	12845056	Allocated	Allocated	unknown	
Homeworklab3.mem	e1\01G0E01+0|File«consent.exe»Hintamd64_microsof	/img_Assignment3Clone.E01/vol_vol6/Users/MjolnirTraining/Desktop/Homeworklab3.m...	2024-07-05 18:00:32 EDT	2024-07-05 18:00:32 EDT	2024-07-05 18:00:32 EDT	2024-07-05 18:00:00 EDT	9663676416	Allocated	Allocated	unknown	
33.txt	.exe","\\system32\\«consent.exe»","\\system32\\conv...	/img_Assignment3Clone.E01/vol_vol6/Windows/WinSxS/amd64_microsoft-windows-s...	2024-07-05 16:46:52 EDT	2024-07-05 17:42:13 EDT	2024-07-05 16:46:52 EDT	2024-07-05 16:46:52 EDT	256225	Allocated	Allocated	unknown	
SFLISTLH.dat	t.xml10\syswow64|«consent.exe»10\syswow64|console	/img_Assignment3Clone.E01/vol_vol6/Windows/WinSxS/amd64_microsoft-windows-mi...	2019-12-07 04:09:45 EST	2024-08-09 17:35:41 EDT	2023-09-12 09:06:51 EDT	2019-12-07 04:09:45 EST	3347940	Allocated	Allocated	unknown	
Security.evtx	4355_none_1b047cfc1205a20f\«consent.exe»%%4420 ...	/img_Assignment3Clone.E01/vol_vol6/Windows/System32/winevt/Logs/Security.evtx	2024-08-14 15:28:18 EDT	2024-08-14 15:28:18 EDT	2024-08-14 15:28:18 EDT	2023-09-09 21:53:29 EDT	20975616	Allocated	Allocated	unknown	
SFLISTRS1.dat	.proxystub.dll11|«consent.exe»11|consentux.dll	/img_Assignment3Clone.E01/vol_vol6/Windows/WinSxS/amd64_microsoft-windows-mi...	2019-12-07 04:09:45 EST	2024-08-09 17:35:41 EDT	2023-09-12 09:06:32 EDT	2019-12-07 04:09:45 EST	5593408	Allocated	Allocated	unknown	
InputService.dll	cppinsight3.exegvim«consent.exe»bashpowershellem...	/img_Assignment3Clone.E01/vol_vol6/Windows/WinSxS/amd64_microsoft-windows-in...	2024-07-05 16:44:14 EDT	2024-08-14 13:55:38 EDT	2024-08-14 15:28:28 EDT	2024-07-05 16:44:14 EDT	4791296	Allocated	Allocated	unknown	
ae0ec7d0cc2f031c17eb9242b31e3de12b0fa902342f1	e1\01G0E01+0|File«consent.exe»Hintamd64_microsof	/img_Assignment3Clone.E01/vol_vol6/Windows/WinSxS/Catalogs/ae0ec7d0cc2f031c17e...	2024-08-10 21:30:38 EDT	2024-08-14 13:56:20 EDT	2024-08-14 15:08:46 EDT	2024-08-14 13:52:52 EDT	227448	Allocated	Allocated	unknown	
SYSTEM.LOG2-slack	3\Windows\System32\«consent.exe»-1p\Device\Hard...	/img_Assignment3Clone.E01/vol_vol6/Windows/System32/config/SYSTEM.LOG2-slack	2019-12-07 04:03:44 EST	2023-09-09 22:52:41 EDT	2019-12-07 04:03:44 EST	2019-12-07 04:03:44 EST	1245184	Allocated	Allocated	unknown	
SFLISTWT.WOA.dat	searchconnector-ms11|«consent.exe»11|consentux.dll	/img_Assignment3Clone.E01/vol_vol6/Windows/WinSxS/amd64_microsoft-windows-mi...	2019-12-07 04:09:45 EST	2024-08-09 17:35:41 EDT	2023-09-11 03:12:05 EDT	2019-12-07 04:09:45 EST	2636850	Allocated	Allocated	unknown	
SFLISTWB.WOA.dat	searchconnector-ms11|«consent.exe»11|consentux.dll	/img_Assignment3Clone.E01/vol_vol6/Windows/WinSxS/amd64_microsoft-windows-mi...	2019-12-07 04:09:45 EST	2024-08-09 17:35:41 EDT	2023-09-11 03:12:05 EDT	2019-12-07 04:09:45 EST	1150134	Allocated	Allocated	unknown	
SFLISTWT.dat	.proxystub.dll11|«consent.exe»11|consentux.dll	/img_Assignment3Clone.E01/vol_vol6/Windows/WinSxS/amd64_microsoft-windows-mi...	2019-12-07 04:09:45 EST	2024-08-09 17:35:41 EDT	2023-09-12 09:06:38 EDT	2019-12-07 04:09:45 EST	4935438	Allocated	Allocated	unknown	
ChsEM.dll	gvíminsight3.exebash«consent.exe»~bEbK`7g5mincore\	/img_Assignment3Clone.E01/vol_vol6/Windows/WinSxS/amd64_microsoft-windows-ch...	2024-07-05 16:43:56 EDT	2024-08-14 13:55:49 EDT	2024-08-14 14:35:18 EDT	2024-07-05 16:43:56 EDT	1147392	Allocated	Allocated	unknown	
SFLISTW8.WOA.dat	countstate.dll11|«consent.exe»11|consentux.dll	/img_Assignment3Clone.E01/vol_vol6/Windows/WinSxS/amd64_microsoft-windows-mi...	2019-12-07 04:09:45 EST	2024-08-09 17:35:41 EDT	2023-09-11 03:12:05 EDT	2019-12-07 04:09:45 EST	954436	Allocated	Allocated	unknown	
SFLISTWB.dat	searchconnector-ms11|«consent.exe»11|consentux.dll	/img_Assignment3Clone.E01/vol_vol6/Windows/WinSxS/amd64_microsoft-windows-mi...	2019-12-07 04:09:45 EST	2024-08-09 17:35:41 EDT	2023-09-11 03:12:05 EDT	2019-12-07 04:09:45 EST	3172904	Allocated	Allocated	unknown	
SFLISTW7.dat	11|connect.dll11|«consent.exe»11|console.dll11|control	/img_Assignment3Clone.E01/vol_vol6/Windows/WinSxS/amd64_microsoft-windows-mi...	2019-12-07 04:09:45 EST	2024-08-09 17:35:41 EDT	2023-09-11 03:12:05 EDT	2019-12-07 04:09:45 EST	1703368	Allocated	Allocated	unknown	
SFLISTW8.dat	countstate.dll11|«consent.exe»11|consentux.dll	/img_Assignment3Clone.E01/vol_vol6/Windows/WinSxS/amd64_microsoft-windows-mi...	2019-12-07 04:09:45 EST	2024-08-09 17:35:41 EDT	2023-09-11 03:12:05 EDT	2019-12-07 04:09:45 EST	2808858	Allocated	Allocated	unknown	
Windows.Internal.Signals.dll	cscript.execonhost.exe«consent.exe»cvtres.exedataex...	/img_Assignment3Clone.E01/vol_vol6/Windows/WinSxS/amd64_microsoft-windows-sig...	2024-07-05 16:43:45 EDT	2024-08-14 13:55:38 EDT	2024-08-14 15:28:30 EDT	2024-07-05 16:43:45 EDT	1065472	Allocated	Allocated	unknown	
FontCache-S-1-5-18.dat-slack	19041.4355#.d256i«consent.exe»Jt5GL8V/f5nLUQWrYnh	/img_Assignment3Clone.E01/vol_vol6/Windows/ServiceProfiles/LocalService/AppData/L...	2024-08-14 13:57:44 EDT	2024-08-14 15:30:19 EDT	2024-08-14 15:30:19 EDT	2023-09-10 02:54:57 EDT	8122368	Allocated	Allocated	unknown	
GamingRepair.dll	Starting install for %ws«consent.exe»Expected, user di...	/img_Assignment3Clone.E01/vol_vol6/Program Files/WindowsApps/Microsoft.Windows...	2024-07-05 16:41:32 EDT	2024-08-09 17:40:41 EDT	2024-08-14 14:34:37 EDT	2024-07-05 16:41:31 EDT	524288	Allocated	Allocated	unknown	
ACPBackgroundManagerPolicy.dll	st.exeaudiodg.exe«consent.exe»credentialuibroker.exe	/img_Assignment3Clone.E01/vol_vol6/Windows/System32/ACPBackgroundManagerPoli...	2024-07-05 16:43:51 EDT	2024-08-14 13:55:49 EDT	2024-08-14 15:28:28 EDT	2024-07-05 16:43:51 EDT	214016	Allocated	Allocated	unknown	
Windows.Internal.Signals.dll	cleanmgr.execsc.exe«consent.exe»conhost.execmd.exe	/img_Assignment3Clone.E01/vol_vol6/Windows/WinSxS/amd64_microsoft-windows-sig...	2024-08-14 13:54:41 EDT	2024-08-14 13:57:20 EDT	2024-08-14 13:54:41 EDT	2024-08-14 13:54:41 EDT	1065472	Allocated	Allocated	unknown	
33.txt	.exe","\\system32\\«consent.exe»","\\system32\\conv...	/img_Assignment3Clone.E01/vol_vol6/Windows/SystemApps/Microsoft.Windows.Searc...	2024-07-05 16:46:52 EDT	2024-07-25 17:42:13 EDT	2024-07-05 16:46:52 EDT	2024-07-05 16:46:52 EDT	256225	Allocated	Allocated	unknown	
amd64_microsoft-windows-lua-onecore_31bf3856(	EnableRestrictedAutoApprove«consent.exe» %u %u %...	/img_Assignment3Clone.E01/vol_vol6/Windows/WinSxS/Backup/amd64_microsoft-win...	2024-07-05 16:49:25 EDT	2024-07-05 17:42:59 EDT	2024-07-05 16:49:25 EDT	2024-07-05 17:42:21 EDT	217800	Allocated	Allocated	unknown	
ChsEM.dll	gvíminsight3.exebash«consent.exe»~bEbK`7g5mincore\	/img_Assignment3Clone.E01/vol_vol6/Windows/WinSxS/amd64_microsoft-windows-ch...	2024-07-05 16:43:56 EDT	2024-08-14 13:55:49 EDT	2024-08-14 14:35:18 EDT	2024-07-05 16:43:56 EDT	1147392	Allocated	Allocated	unknown	
InputService.dll	gvimbashinsight3.exe«consent.exe»twohandedoneha...	/img_Assignment3Clone.E01/vol_vol6/Windows/WinSxS/amd64_microsoft-windows-in...	2024-08-14 13:54:47 EDT	2024-08-14 13:57:24 EDT	2024-08-14 13:54:47 EDT	2024-08-14 13:54:47 EDT	4794368	Allocated	Allocated	unknown	
SFLISTW8.dat	countstate.dll11|«consent.exe»11|consentux.dll	/img_Assignment3Clone.E01/vol_vol6/Windows/System32/migwiz/SFLISTW8.dat	2019-12-07 04:09:45 EST	2024-08-09 17:35:41 EDT	2023-09-11 03:12:05 EDT	2019-12-07 04:09:45 EST	2808858	Allocated	Allocated	unknown	
ChsEM.dll	gvíminsight3.exebash«consent.exe»~bEbK`7g5mincore\	/img_Assignment3Clone.E01/vol_vol6/Windows/System32/InputMethod/CHS/ChsEM.dll	2024-07-05 16:43:56 EDT	2024-08-14 13:55:49 EDT	2024-08-14 14:35:18 EDT	2024-07-05 16:43:56 EDT	1147392	Allocated	Allocated	unknown	

```
consent.exe !This program cannot be run in DOS mode.
Richw
.text
`.rdata
@.data
.pdata
@.didat
consentb
.rsrc
@.reloc
DS'H
d$\E3
DSPH
DS0H
LS'H3
DSpH
d$II
d$\I
LSpH3
DSpH
```

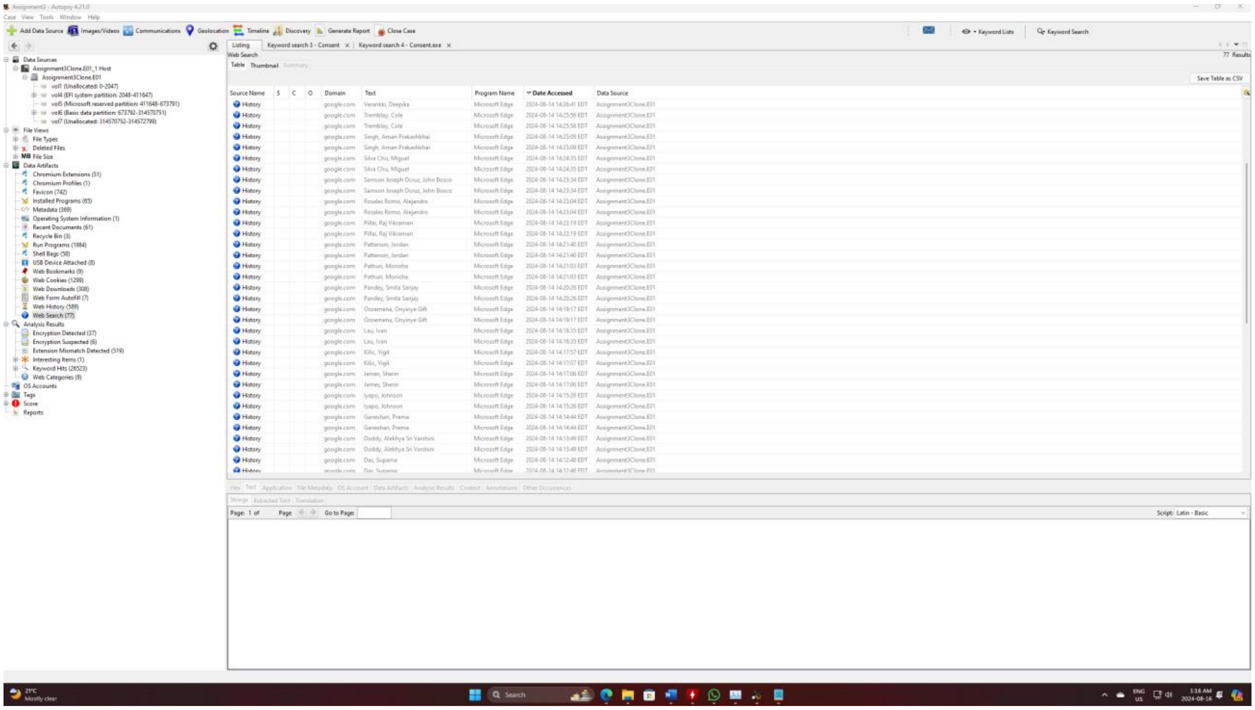
Explain what happened using the analysis in Autopsy

Using the “web History” time we can see that the user of this VM visited several time wasting and phishing websites as well as sites that contain possible malicious downloads. There were also sites and social media profiles visited pertaining to certain individuals.



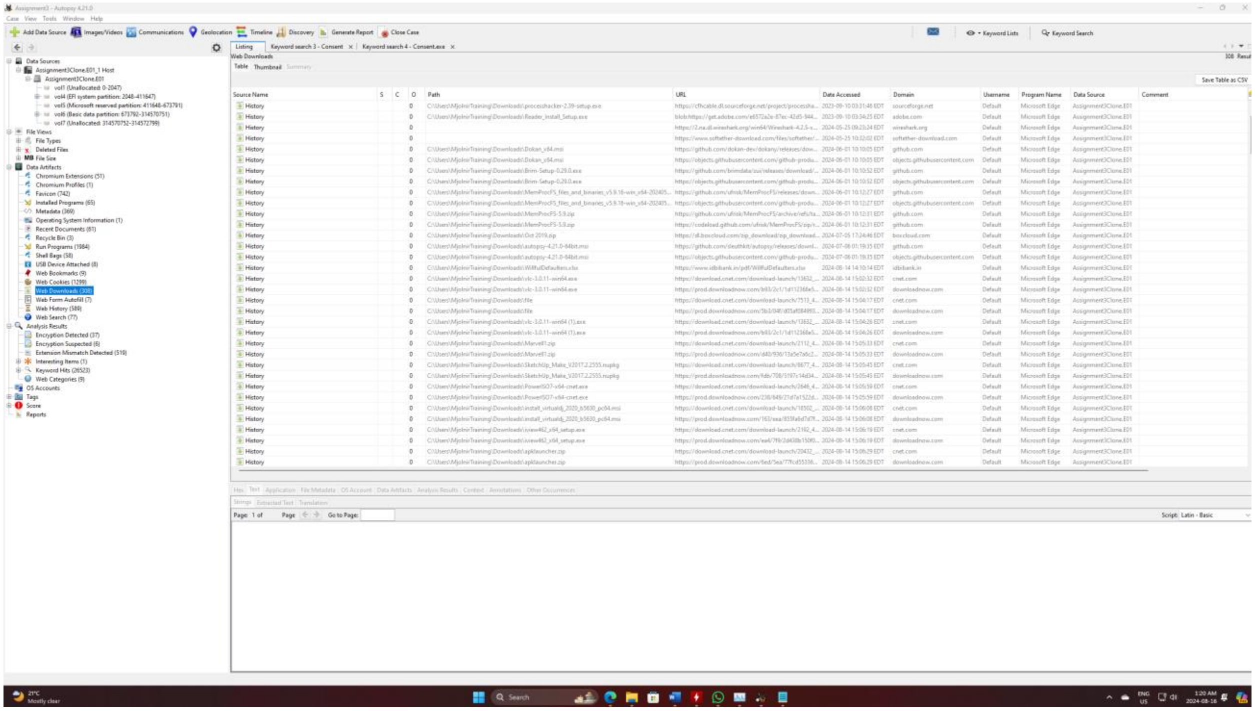
Source Name	S	C	O	URL	Date Accessed	Referer URL	Title	Program Name	Domain	Username	Data Source
History			0	https://phishtank.org/phish_archive.php	2024-08-14 14:40:14 EDT	https://phishtank.org/phish_archive.php	PhishTank > See all suspected phish submissions	Microsoft Edge	phishtank.org	Default	Assignment3Clone.E01
History			0	https://phishtank.org/phish_archive.php	2024-08-14 14:40:14 EDT	https://phishtank.org/phish_archive.php	PhishTank > See all suspected phish submissions	Microsoft Edge	phishtank.org	Default	Assignment3Clone.E01
History			0	https://phishtank.org/phish_archive.php	2024-08-14 14:40:14 EDT	https://phishtank.org/phish_archive.php	PhishTank > See all suspected phish submissions	Microsoft Edge	phishtank.org	Default	Assignment3Clone.E01
History			0	https://phishtank.org/phish_archive.php?__cf_chl_tk=...	2024-08-14 14:39:52 EDT	https://phishtank.org/phish_archive.php?__cf_chl_tk=...	Just a moment...	Microsoft Edge	phishtank.org	Default	Assignment3Clone.E01
History			0	https://phishtank.org/phish_archive.php?__cf_chl_rt_t...	2024-08-14 14:39:49 EDT	https://phishtank.org/phish_archive.php?__cf_chl_rt_t...	Just a moment...	Microsoft Edge	phishtank.org	Default	Assignment3Clone.E01
History			0	https://phishtank.org/	2024-08-14 14:39:35 EDT	https://phishtank.org/	PhishTank | Join the fight against phishing	Microsoft Edge	phishtank.org	Default	Assignment3Clone.E01
History			0	https://www.bing.com/search?q=Yao%2C+Woody&c...	2024-08-14 14:38:31 EDT	https://www.bing.com/search?q=Yao%2C+Woody&c...	Yao, Woody - Search	Microsoft Edge	bing.com	Default	Assignment3Clone.E01
History			0	https://www.bing.com/search?q=Yao%2C+Woody&c...	2024-08-14 14:38:31 EDT	https://www.bing.com/search?q=Yao%2C+Woody&c...	Yao, Woody - Search	Microsoft Edge	bing.com	Default	Assignment3Clone.E01
History			0	https://www.bing.com/search?q=Yao%2C+Woody&c...	2024-08-14 14:38:31 EDT	https://www.bing.com/search?q=Yao%2C+Woody&c...	Yao, Woody - Search	Microsoft Edge	bing.com	Default	Assignment3Clone.E01
History			0	https://www.bing.com/search?q=Yao%2C+Woody&c...	2024-08-14 14:38:31 EDT	https://www.bing.com/search?q=Yao%2C+Woody&c...	Yao, Woody - Search	Microsoft Edge	bing.com	Default	Assignment3Clone.E01
History			0	https://www.bing.com/search?q=Yao%2C+Woody&c...	2024-08-14 14:38:31 EDT	https://www.bing.com/search?q=Yao%2C+Woody&c...	Yao, Woody - Search	Microsoft Edge	bing.com	Default	Assignment3Clone.E01
History			0	https://www.bing.com/search?q=Yao%2C+Woody&c...	2024-08-14 14:38:31 EDT	https://www.bing.com/search?q=Yao%2C+Woody&c...	Yao, Woody - Search	Microsoft Edge	bing.com	Default	Assignment3Clone.E01
History			0	https://www.bing.com/search?q=Yao%2C+Woody&c...	2024-08-14 14:38:31 EDT	https://www.bing.com/search?q=Yao%2C+Woody&c...	Yao, Woody - Search	Microsoft Edge	bing.com	Default	Assignment3Clone.E01
History			0	https://www.bing.com/search?q=Yao%2C+Woody&c...	2024-08-14 14:38:31 EDT	https://www.bing.com/search?q=Yao%2C+Woody&c...	Yao, Woody - Search	Microsoft Edge	bing.com	Default	Assignment3Clone.E01
History			0	https://www.bing.com/search?q=Yao%2C+Woody&c...	2024-08-14 14:38:31 EDT	https://www.bing.com/search?q=Yao%2C+Woody&c...	Yao, Woody - Search	Microsoft Edge	bing.com	Default	Assignment3Clone.E01
History			0	https://theuselessweb.org/	2024-08-14 14:36:37 EDT	https://theuselessweb.org/	The Useless Web - Dive Into Random Websites!	Microsoft Edge	theuselessweb.org	Default	Assignment3Clone.E01
History			0	https://theuselessweb.org/	2024-08-14 14:36:37 EDT	https://theuselessweb.org/	The Useless Web - Dive Into Random Websites!	Microsoft Edge	theuselessweb.org	Default	Assignment3Clone.E01
History			0	https://www.designboom.com/architecture/zaha-had...	2024-08-14 14:28:36 EDT	https://www.designboom.com/architecture/zaha-had...	zaha hadid: innovation tower at hong kong polytechni...	Microsoft Edge	designboom.com	Default	Assignment3Clone.E01
History			0	https://www.bing.com/ck/a?!&&p=bdebbb938b0da5...	2024-08-14 14:28:35 EDT	https://www.bing.com/ck/a?!&&p=bdebbb938b0da5...		Microsoft Edge	bing.com	Default	Assignment3Clone.E01
History			0	http://zeus.noinex.com/content/people/woody-yao/i...	2024-08-14 14:28:31 EDT	http://zeus.noinex.com/content/people/woody-yao/i...	Woody Yao - People - Zaha Hadid Architects	Microsoft Edge	noinex.com	Default	Assignment3Clone.E01
History			0	https://zeus.noinex.com/content/people/woody-yao/...	2024-08-14 14:28:31 EDT	https://zeus.noinex.com/content/people/woody-yao/...	Woody Yao - People - Zaha Hadid Architects	Microsoft Edge	noinex.com	Default	Assignment3Clone.E01
History			0	https://www.bing.com/ck/a?!&&p=c5a4549eb58fd4b...	2024-08-14 14:28:30 EDT	https://www.bing.com/ck/a?!&&p=c5a4549eb58fd4b...		Microsoft Edge	bing.com	Default	Assignment3Clone.E01
History			0	https://www.youtube.com/watch?v=rA-sm9hZbFI	2024-08-14 14:28:29 EDT	https://www.youtube.com/watch?v=rA-sm9hZbFI	Zaha Hadid Design: Untold with Woody Yao and Mah...	Microsoft Edge	youtube.com	Default	Assignment3Clone.E01
History			0	https://www.bing.com/ck/a?!&&p=1abf20a9fe843e41...	2024-08-14 14:28:28 EDT	https://www.bing.com/ck/a?!&&p=1abf20a9fe843e41...		Microsoft Edge	bing.com	Default	Assignment3Clone.E01
History			0	https://www.dezeen.com/2022/07/12/ten-objects-zah...	2024-08-14 14:28:27 EDT	https://www.dezeen.com/2022/07/12/ten-objects-zah...	Ten objects by Zaha Hadid Design that go "beyond th...	Microsoft Edge	dezeen.com	Default	Assignment3Clone.E01
History			0	https://www.bing.com/ck/a?!&&p=c7074624c4be13fe...	2024-08-14 14:28:26 EDT	https://www.bing.com/ck/a?!&&p=c7074624c4be13fe...		Microsoft Edge	bing.com	Default	Assignment3Clone.E01
History			0	https://www.youtube.com/watch?v=ZgPZjSMdy0	2024-08-14 14:28:25 EDT	https://www.youtube.com/watch?v=ZgPZjSMdy0	Woody Yao and Maha Kutay from Zaha Hadid Design ...	Microsoft Edge	youtube.com	Default	Assignment3Clone.E01
History			0	https://www.bing.com/ck/a?!&&p=b28d33d3f2edf41...	2024-08-14 14:28:24 EDT	https://www.bing.com/ck/a?!&&p=b28d33d3f2edf41...		Microsoft Edge	bing.com	Default	Assignment3Clone.E01
History			0	https://www.linkedin.com/pub/dir/Bilal/Wardak/us-0...	2024-08-14 14:28:01 EDT	https://www.linkedin.com/pub/dir/Bilal/Wardak/us-0...	5 "Bilal Wardak" profiles | LinkedIn	Microsoft Edge	linkedin.com	Default	Assignment3Clone.E01
History			0	https://www.greenocktelegraph.co.uk/news/24455651...	2024-08-14 14:27:59 EDT	https://www.greenocktelegraph.co.uk/news/24455651...	Afghan war hero hailed as he rebuilds life in Port Glasg...	Microsoft Edge	greenocktelegraph.co.uk	Default	Assignment3Clone.E01
History			0	https://www.greenocktelegraph.co.uk/news/24455651...	2024-08-14 14:27:59 EDT	https://www.greenocktelegraph.co.uk/news/24455651...	Afghan war hero hailed as he rebuilds life in Port Glasg...	Microsoft Edge	greenocktelegraph.co.uk	Default	Assignment3Clone.E01
History			0	https://www.greenocktelegraph.co.uk/news/24455651...	2024-08-14 14:27:59 EDT	https://www.greenocktelegraph.co.uk/news/24455651...	Afghan war hero hailed as he rebuilds life in Port Glasg...	Microsoft Edge	greenocktelegraph.co.uk	Default	Assignment3Clone.E01
History			0	https://www.greenocktelegraph.co.uk/news/24401046...	2024-08-14 14:27:47 EDT	https://www.greenocktelegraph.co.uk/news/24401046...	Afghan war hero now safe in Inverclyde helps refugees...	Microsoft Edge	greenocktelegraph.co.uk	Default	Assignment3Clone.E01
History			0	https://www.greenocktelegraph.co.uk/news/24401046...	2024-08-14 14:27:47 EDT	https://www.greenocktelegraph.co.uk/news/24401046...	Afghan war hero now safe in Inverclyde helps refugees...	Microsoft Edge	greenocktelegraph.co.uk	Default	Assignment3Clone.E01
History			0	https://www.greenocktelegraph.co.uk/news/24401046...	2024-08-14 14:27:47 EDT	https://www.greenocktelegraph.co.uk/news/24401046...	Afghan war hero now safe in Inverclyde helps refugees...	Microsoft Edge	greenocktelegraph.co.uk	Default	Assignment3Clone.E01

The user of this VM also ran several google searches for the names of individuals. These names correspond the individuals described in the previous point.



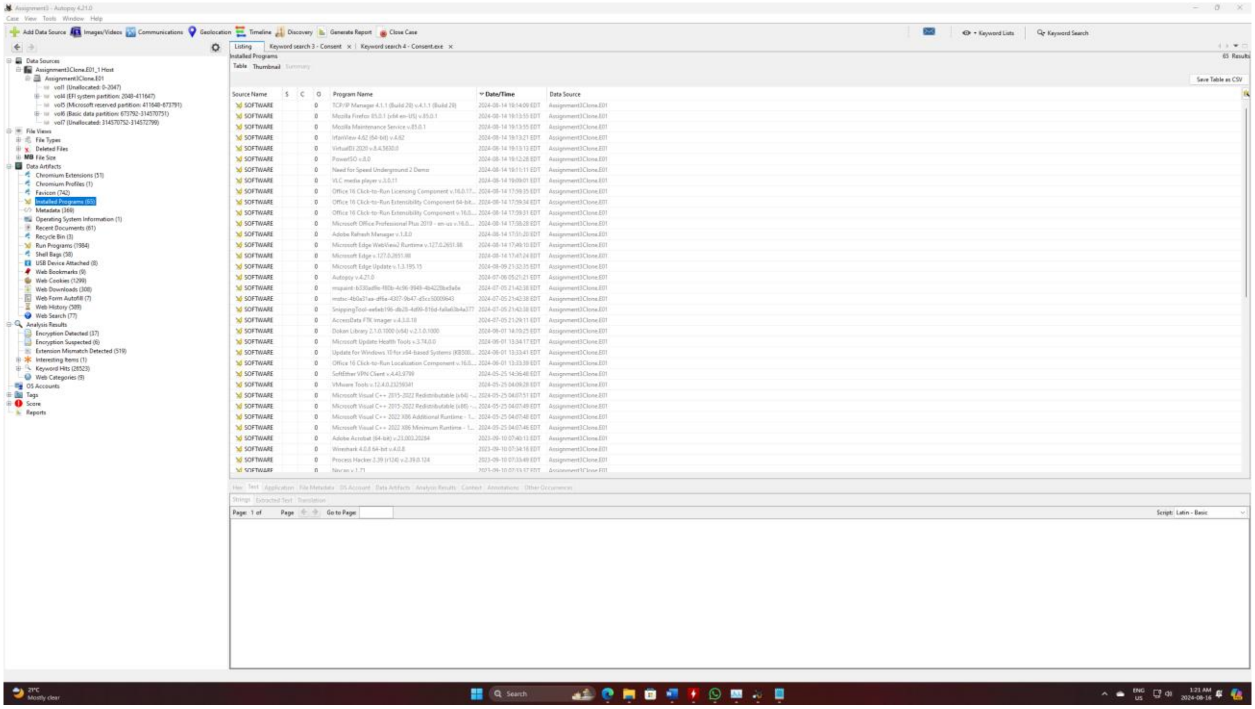
Source Name	S	C	O	Domain	Text	Program Name	Date Accessed	Data Source
History				google.com	Verankki, Deepika	Microsoft Edge	2024-08-14 14:26:41 EDT	Assignment3Clone.E01
History				google.com	Tremblay, Cole	Microsoft Edge	2024-08-14 14:25:56 EDT	Assignment3Clone.E01
History				google.com	Tremblay, Cole	Microsoft Edge	2024-08-14 14:25:56 EDT	Assignment3Clone.E01
History				google.com	Singh, Aman Prakashbhai	Microsoft Edge	2024-08-14 14:25:09 EDT	Assignment3Clone.E01
History				google.com	Singh, Aman Prakashbhai	Microsoft Edge	2024-08-14 14:25:09 EDT	Assignment3Clone.E01
History				google.com	Silva Chu, Miguel	Microsoft Edge	2024-08-14 14:24:35 EDT	Assignment3Clone.E01
History				google.com	Silva Chu, Miguel	Microsoft Edge	2024-08-14 14:24:35 EDT	Assignment3Clone.E01
History				google.com	Samson Joseph Dcruz, John Bosco	Microsoft Edge	2024-08-14 14:23:34 EDT	Assignment3Clone.E01
History				google.com	Samson Joseph Dcruz, John Bosco	Microsoft Edge	2024-08-14 14:23:34 EDT	Assignment3Clone.E01
History				google.com	Rosales Romo, Alejandro	Microsoft Edge	2024-08-14 14:23:04 EDT	Assignment3Clone.E01
History				google.com	Rosales Romo, Alejandro	Microsoft Edge	2024-08-14 14:23:04 EDT	Assignment3Clone.E01
History				google.com	Pillai, Raj Vikraman	Microsoft Edge	2024-08-14 14:22:19 EDT	Assignment3Clone.E01
History				google.com	Pillai, Raj Vikraman	Microsoft Edge	2024-08-14 14:22:19 EDT	Assignment3Clone.E01
History				google.com	Patterson, Jordan	Microsoft Edge	2024-08-14 14:21:40 EDT	Assignment3Clone.E01
History				google.com	Patterson, Jordan	Microsoft Edge	2024-08-14 14:21:40 EDT	Assignment3Clone.E01
History				google.com	Pathuri, Monisha	Microsoft Edge	2024-08-14 14:21:03 EDT	Assignment3Clone.E01
History				google.com	Pathuri, Monisha	Microsoft Edge	2024-08-14 14:21:03 EDT	Assignment3Clone.E01
History				google.com	Pandey, Smita Sanjay	Microsoft Edge	2024-08-14 14:20:26 EDT	Assignment3Clone.E01
History				google.com	Pandey, Smita Sanjay	Microsoft Edge	2024-08-14 14:20:26 EDT	Assignment3Clone.E01
History				google.com	Ozoemena, Onyinye Gift	Microsoft Edge	2024-08-14 14:19:17 EDT	Assignment3Clone.E01
History				google.com	Ozoemena, Onyinye Gift	Microsoft Edge	2024-08-14 14:19:17 EDT	Assignment3Clone.E01
History				google.com	Lau, Ivan	Microsoft Edge	2024-08-14 14:18:35 EDT	Assignment3Clone.E01
History				google.com	Lau, Ivan	Microsoft Edge	2024-08-14 14:18:35 EDT	Assignment3Clone.E01
History				google.com	Kilic, Yigit	Microsoft Edge	2024-08-14 14:17:57 EDT	Assignment3Clone.E01
History				google.com	Kilic, Yigit	Microsoft Edge	2024-08-14 14:17:57 EDT	Assignment3Clone.E01
History				google.com	James, Sherin	Microsoft Edge	2024-08-14 14:17:06 EDT	Assignment3Clone.E01
History				google.com	James, Sherin	Microsoft Edge	2024-08-14 14:17:06 EDT	Assignment3Clone.E01
History				google.com	Iyapo, Johnson	Microsoft Edge	2024-08-14 14:15:26 EDT	Assignment3Clone.E01
History				google.com	Iyapo, Johnson	Microsoft Edge	2024-08-14 14:15:26 EDT	Assignment3Clone.E01
History				google.com	Ganeshan, Prema	Microsoft Edge	2024-08-14 14:14:44 EDT	Assignment3Clone.E01
History				google.com	Ganeshan, Prema	Microsoft Edge	2024-08-14 14:14:44 EDT	Assignment3Clone.E01
History				google.com	Doddy, Alekhya Sri Varshini	Microsoft Edge	2024-08-14 14:13:49 EDT	Assignment3Clone.E01
History				google.com	Doddy, Alekhya Sri Varshini	Microsoft Edge	2024-08-14 14:13:49 EDT	Assignment3Clone.E01
History				google.com	Das, Suparna	Microsoft Edge	2024-08-14 14:12:48 EDT	Assignment3Clone.E01
History				google.com	Das, Suparna	Microsoft Edge	2024-08-14 14:12:48 EDT	Assignment3Clone.E01

Circling back to the sites identified as having potential malicious downloads, by using the “web downloads” tab we can see that the user did in fact download applications from these sites.



Source Name	S	C	O	Path	URL	Date Accessed	Domain	Username	Program Name	Data Source	Comment
History			0	C:\Users\MjolnirTraining\Downloads\processhacker-2.39-setup.exe	https://cfhcable.dl.sourceforge.net/project/processha...	2023-09-10 03:31:46 EDT	sourceforge.net	Default	Microsoft Edge	Assignment3Clone.E01	
History			0	C:\Users\MjolnirTraining\Downloads\Reader_Install_Setup.exe	blob:https://get.adobe.com/e6572a2e-87ec-42d5-944...	2023-09-10 03:34:25 EDT	adobe.com	Default	Microsoft Edge	Assignment3Clone.E01	
History			0		https://2.na.dl.wireshark.org/win64/Wireshark-4.2.5-x...	2024-05-25 09:23:24 EDT	wireshark.org	Default	Microsoft Edge	Assignment3Clone.E01	
History			0		https://www.softether-download.com/files/softether/...	2024-05-25 10:32:02 EDT	softether-download.com	Default	Microsoft Edge	Assignment3Clone.E01	
History			0	C:\Users\MjolnirTraining\Downloads\Dokan_x64.msi	https://github.com/dokan-dev/dokany/releases/dow...	2024-06-01 10:10:05 EDT	github.com	Default	Microsoft Edge	Assignment3Clone.E01	
History			0	C:\Users\MjolnirTraining\Downloads\Dokan_x64.msi	https://objects.githubusercontent.com/github-produ...	2024-06-01 10:10:05 EDT	objects.githubusercontent.com	Default	Microsoft Edge	Assignment3Clone.E01	
History			0	C:\Users\MjolnirTraining\Downloads\Brim-Setup-0.29.0.exe	https://github.com/brimdata/zui/releases/download/...	2024-06-01 10:10:52 EDT	github.com	Default	Microsoft Edge	Assignment3Clone.E01	
History			0	C:\Users\MjolnirTraining\Downloads\Brim-Setup-0.29.0.exe	https://objects.githubusercontent.com/github-produ...	2024-06-01 10:10:52 EDT	objects.githubusercontent.com	Default	Microsoft Edge	Assignment3Clone.E01	
History			0	C:\Users\MjolnirTraining\Downloads\MemProcFS_files_and_binaries_v5.9.16-win_x64-202405...	https://github.com/ufrisk/MemProcFS/releases/down...	2024-06-01 10:12:27 EDT	github.com	Default	Microsoft Edge	Assignment3Clone.E01	
History			0	C:\Users\MjolnirTraining\Downloads\MemProcFS_files_and_binaries_v5.9.16-win_x64-202405...	https://objects.githubusercontent.com/github-produ...	2024-06-01 10:12:27 EDT	objects.githubusercontent.com	Default	Microsoft Edge	Assignment3Clone.E01	
History			0	C:\Users\MjolnirTraining\Downloads\MemProcFS-5.9.zip	https://github.com/ufrisk/MemProcFS/archive/refs/ta...	2024-06-01 10:12:31 EDT	github.com	Default	Microsoft Edge	Assignment3Clone.E01	
History			0	C:\Users\MjolnirTraining\Downloads\MemProcFS-5.9.zip	https://codeload.github.com/ufrisk/MemProcFS/zip/r...	2024-06-01 10:12:31 EDT	github.com	Default	Microsoft Edge	Assignment3Clone.E01	
History			0	C:\Users\MjolnirTraining\Downloads\Oct 2019.zip	https://dl.boxcloud.com/zip_download/zip_download...	2024-07-05 17:24:46 EDT	boxcloud.com	Default	Microsoft Edge	Assignment3Clone.E01	
History			0	C:\Users\MjolnirTraining\Downloads\autopsy-4.21.0-64bit.msi	https://github.com/sleuthkit/autopsy/releases/downl...	2024-07-06 01:19:35 EDT	github.com	Default	Microsoft Edge	Assignment3Clone.E01	
History			0	C:\Users\MjolnirTraining\Downloads\autopsy-4.21.0-64bit.msi	https://objects.githubusercontent.com/github-produ...	2024-07-06 01:19:35 EDT	objects.githubusercontent.com	Default	Microsoft Edge	Assignment3Clone.E01	
History			0	C:\Users\MjolnirTraining\Downloads\WilfulDefaulters.xlsx	https://www.idbibank.in/pdf/WilfulDefaulters.xlsx	2024-08-14 14:10:14 EDT	idbibank.in	Default	Microsoft Edge	Assignment3Clone.E01	
History			0	C:\Users\MjolnirTraining\Downloads\vlc-3.0.11-win64.exe	https://download.cnet.com/download-launch/13632_...	2024-08-14 15:02:32 EDT	cnet.com	Default	Microsoft Edge	Assignment3Clone.E01	
History			0	C:\Users\MjolnirTraining\Downloads\vlc-3.0.11-win64.exe	https://prod.downloadnow.com/b93/2c1/1d112368e5...	2024-08-14 15:02:32 EDT	downloadnow.com	Default	Microsoft Edge	Assignment3Clone.E01	
History			0	C:\Users\MjolnirTraining\Downloads\file	https://download.cnet.com/download-launch/7513_4...	2024-08-14 15:04:17 EDT	cnet.com	Default	Microsoft Edge	Assignment3Clone.E01	
History			0	C:\Users\MjolnirTraining\Downloads\file	https://prod.downloadnow.com/5b3/04f/d05af084993...	2024-08-14 15:04:17 EDT	downloadnow.com	Default	Microsoft Edge	Assignment3Clone.E01	
History			0	C:\Users\MjolnirTraining\Downloads\vlc-3.0.11-win64 (1).exe	https://download.cnet.com/download-launch/13632_...	2024-08-14 15:04:26 EDT	cnet.com	Default	Microsoft Edge	Assignment3Clone.E01	
History			0	C:\Users\MjolnirTraining\Downloads\vlc-3.0.11-win64 (1).exe	https://prod.downloadnow.com/b93/2c1/1d112368e5...	2024-08-14 15:04:26 EDT	downloadnow.com	Default	Microsoft Edge	Assignment3Clone.E01	
History			0	C:\Users\MjolnirTraining\Downloads\Marvel1.zip	https://download.cnet.com/download-launch/2112_4...	2024-08-14 15:05:33 EDT	cnet.com	Default	Microsoft Edge	Assignment3Clone.E01	
History			0	C:\Users\MjolnirTraining\Downloads\Marvel1.zip	https://prod.downloadnow.com/d40/936/13a5e7a6c2...	2024-08-14 15:05:33 EDT	downloadnow.com	Default	Microsoft Edge	Assignment3Clone.E01	
History			0	C:\Users\MjolnirTraining\Downloads\SketchUp_Make_V2017.2.2555.nupkg	https://download.cnet.com/download-launch/8677_4...	2024-08-14 15:05:45 EDT	cnet.com	Default	Microsoft Edge	Assignment3Clone.E01	
History			0	C:\Users\MjolnirTraining\Downloads\SketchUp_Make_V2017.2.2555.nupkg	https://prod.downloadnow.com/fdb/708/5197c14d34...	2024-08-14 15:05:45 EDT	downloadnow.com	Default	Microsoft Edge	Assignment3Clone.E01	
History			0	C:\Users\MjolnirTraining\Downloads\PowerISO7-x64-cnet.exe	https://download.cnet.com/download-launch/2646_4...	2024-08-14 15:05:59 EDT	cnet.com	Default	Microsoft Edge	Assignment3Clone.E01	
History			0	C:\Users\MjolnirTraining\Downloads\PowerISO7-x64-cnet.exe	https://prod.downloadnow.com/238/849/21d7a1522d...	2024-08-14 15:05:59 EDT	downloadnow.com	Default	Microsoft Edge	Assignment3Clone.E01	
History			0	C:\Users\MjolnirTraining\Downloads\install_virtualdj_2020_b5630_pc64.msi	https://download.cnet.com/download-launch/18502_...	2024-08-14 15:06:08 EDT	cnet.com	Default	Microsoft Edge	Assignment3Clone.E01	
History			0	C:\Users\MjolnirTraining\Downloads\install_virtualdj_2020_b5630_pc64.msi	https://prod.downloadnow.com/163/eea/855fa8d7d7f...	2024-08-14 15:06:08 EDT	downloadnow.com	Default	Microsoft Edge	Assignment3Clone.E01	
History			0	C:\Users\MjolnirTraining\Downloads\iview462_x64_setup.exe	https://download.cnet.com/download-launch/2192_4...	2024-08-14 15:06:19 EDT	cnet.com	Default	Microsoft Edge	Assignment3Clone.E01	
History			0	C:\Users\MjolnirTraining\Downloads\iview462_x64_setup.exe	https://prod.downloadnow.com/ea4/7f9/2d408b150f0...	2024-08-14 15:06:19 EDT	downloadnow.com	Default	Microsoft Edge	Assignment3Clone.E01	
History			0	C:\Users\MjolnirTraining\Downloads\apklauncher.zip	https://download.cnet.com/download-launch/20432_...	2024-08-14 15:06:29 EDT	cnet.com	Default	Microsoft Edge	Assignment3Clone.E01	
History			0	C:\Users\MjolnirTraining\Downloads\apklauncher.zip	https://prod.downloadnow.com/6ed/5ea/77fcd55336...	2024-08-14 15:06:29 EDT	downloadnow.com	Default	Microsoft Edge	Assignment3Clone.E01	

Navigating to the “Installed Programs” tab we can see that the user of this VM went ahead and installed those downloaded potentially malicious pieces of software.



Installed Programs

Source Name	S	C	O	Program Name	Date/Time	Data Source
SOFTWARE			0	TCP/IP Manager 4.1.1 (Build 28) v.4.1.1 (Build 28)	2024-08-14 18:14:09 EDT	Assignment3Clone.E01
SOFTWARE			0	Mozilla Firefox 85.0.1 (x64 en-US) v.85.0.1	2024-08-14 18:13:55 EDT	Assignment3Clone.E01
SOFTWARE			0	Mozilla Maintenance Service v.85.0.1	2024-08-14 18:13:55 EDT	Assignment3Clone.E01
SOFTWARE			0	IrfanView 4.62 (64-bit) v.4.62	2024-08-14 18:13:21 EDT	Assignment3Clone.E01
SOFTWARE			0	VirtualDJ 2020 v.8.4.5630.0	2024-08-14 18:13:13 EDT	Assignment3Clone.E01
SOFTWARE			0	PowerISO v.8.0	2024-08-14 18:12:28 EDT	Assignment3Clone.E01
SOFTWARE			0	Need for Speed Underground 2 Demo	2024-08-14 18:11:11 EDT	Assignment3Clone.E01
SOFTWARE			0	VLC media player v.3.0.11	2024-08-14 18:09:01 EDT	Assignment3Clone.E01
SOFTWARE			0	Office 16 Click-to-Run Licensing Component v.16.0.17...	2024-08-14 17:59:35 EDT	Assignment3Clone.E01
SOFTWARE			0	Office 16 Click-to-Run Extensibility Component 64-bit...	2024-08-14 17:59:34 EDT	Assignment3Clone.E01
SOFTWARE			0	Office 16 Click-to-Run Extensibility Component v.16.0....	2024-08-14 17:59:31 EDT	Assignment3Clone.E01
SOFTWARE			0	Microsoft Office Professional Plus 2019 - en-us v.16.0....	2024-08-14 17:58:28 EDT	Assignment3Clone.E01
SOFTWARE			0	Adobe Refresh Manager v.1.8.0	2024-08-14 17:51:20 EDT	Assignment3Clone.E01
SOFTWARE			0	Microsoft Edge WebView2 Runtime v.127.0.2651.98	2024-08-14 17:49:10 EDT	Assignment3Clone.E01
SOFTWARE			0	Microsoft Edge v.127.0.2651.98	2024-08-14 17:47:24 EDT	Assignment3Clone.E01
SOFTWARE			0	Microsoft Edge Update v.1.3.195.15	2024-08-09 21:32:35 EDT	Assignment3Clone.E01
SOFTWARE			0	Autopsy v.4.21.0	2024-07-06 05:21:21 EDT	Assignment3Clone.E01
SOFTWARE			0	mspaint-b330adfe-f80b-4c96-9949-4b4228be8a6e	2024-07-05 21:42:38 EDT	Assignment3Clone.E01
SOFTWARE			0	mstsc-4b0a31aa-df6a-4307-9b47-d5cc50009643	2024-07-05 21:42:38 EDT	Assignment3Clone.E01
SOFTWARE			0	SnippingTool-eefeb196-db28-4d99-816d-fa9a63b4a377	2024-07-05 21:42:38 EDT	Assignment3Clone.E01
SOFTWARE			0	AccessData FTK Imager v.4.3.0.18	2024-07-05 21:29:11 EDT	Assignment3Clone.E01
SOFTWARE			0	Dokan Library 2.1.0.1000 (x64) v.2.1.0.1000	2024-06-01 14:10:25 EDT	Assignment3Clone.E01
SOFTWARE			0	Microsoft Update Health Tools v.3.74.0.0	2024-06-01 13:34:17 EDT	Assignment3Clone.E01
SOFTWARE			0	Update for Windows 10 for x64-based Systems (KB500...	2024-06-01 13:33:41 EDT	Assignment3Clone.E01
SOFTWARE			0	Office 16 Click-to-Run Localization Component v.16.0....	2024-06-01 13:33:39 EDT	Assignment3Clone.E01
SOFTWARE			0	SoftEther VPN Client v.4.43.9799	2024-05-25 14:36:48 EDT	Assignment3Clone.E01
SOFTWARE			0	VMware Tools v.12.4.0.23259341	2024-05-25 04:09:28 EDT	Assignment3Clone.E01
SOFTWARE			0	Microsoft Visual C++ 2015-2022 Redistributable (x64) -...	2024-05-25 04:07:51 EDT	Assignment3Clone.E01
SOFTWARE			0	Microsoft Visual C++ 2015-2022 Redistributable (x86) -...	2024-05-25 04:07:49 EDT	Assignment3Clone.E01
SOFTWARE			0	Microsoft Visual C++ 2022 X86 Additional Runtime - 1...	2024-05-25 04:07:48 EDT	Assignment3Clone.E01
SOFTWARE			0	Microsoft Visual C++ 2022 X86 Minimum Runtime - 1...	2024-05-25 04:07:46 EDT	Assignment3Clone.E01
SOFTWARE			0	Adobe Acrobat (64-bit) v.23.003.20284	2023-09-10 07:40:13 EDT	Assignment3Clone.E01
SOFTWARE			0	Wireshark 4.0.8 64-bit v.4.0.8	2023-09-10 07:34:16 EDT	Assignment3Clone.E01
SOFTWARE			0	Process Hacker 2.39 (r124) v.2.39.0.124	2023-09-10 07:33:49 EDT	Assignment3Clone.E01
SOFTWARE			0	Npcap v.1.71	2023-09-10 07:33:37 EDT	Assignment3Clone.E01

At this stage the machine was cloned and the image taken to complete this analysis.