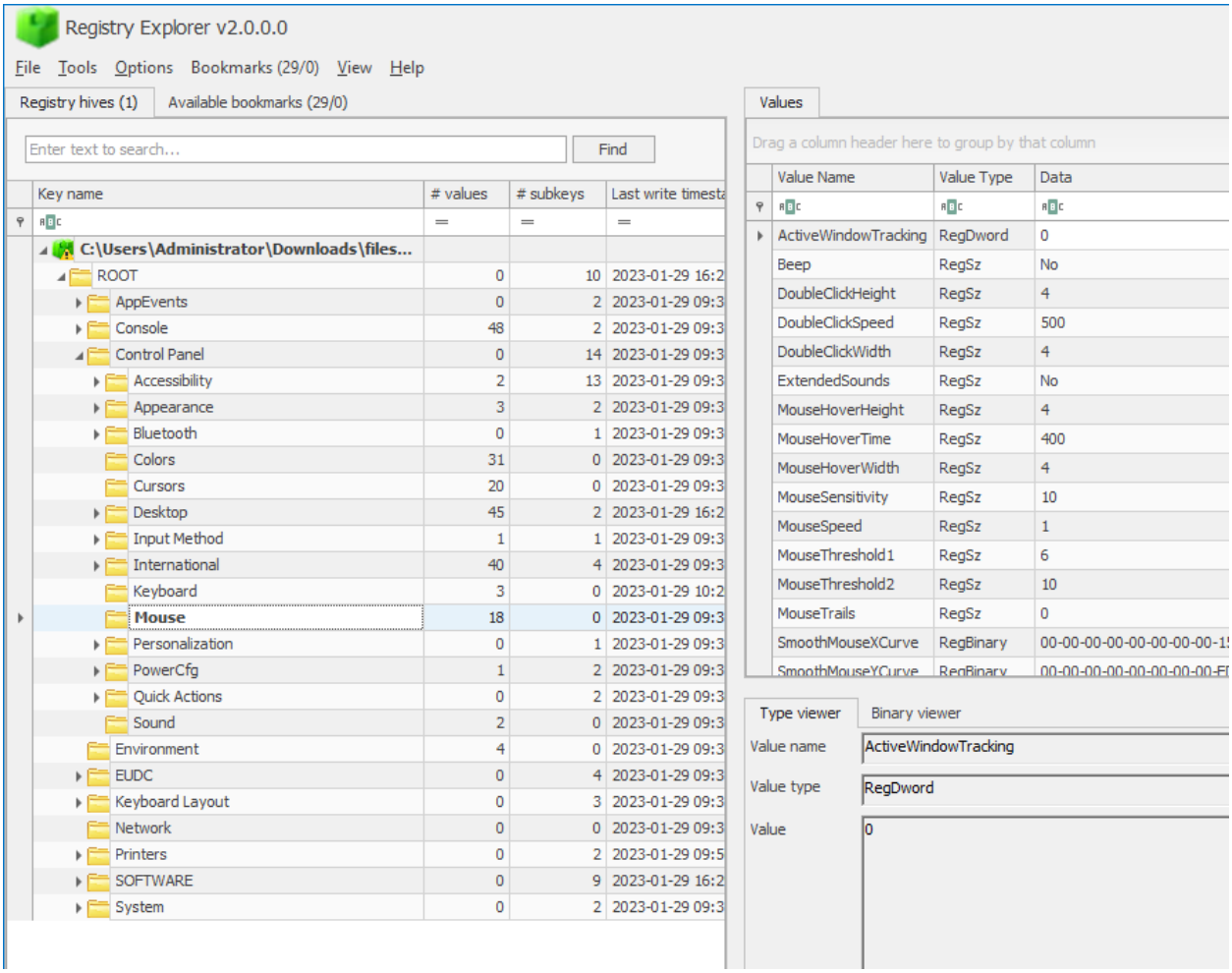
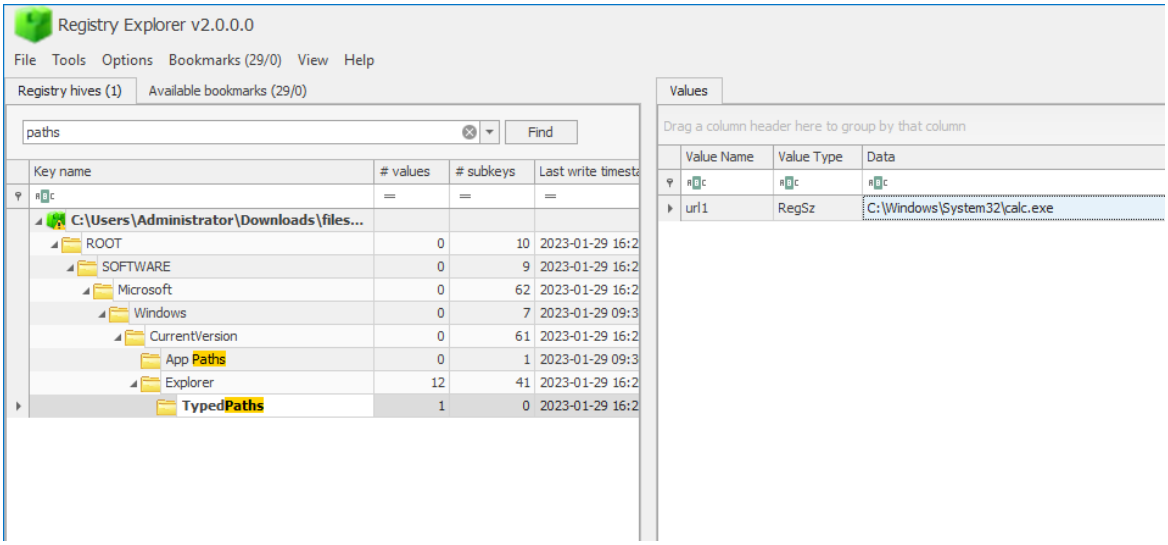
I opened the explorer and navigated to the mouse configs. This led me to the following answers.



Answer 1A: As we can see the DoubleClickSpeed is 500 ms.

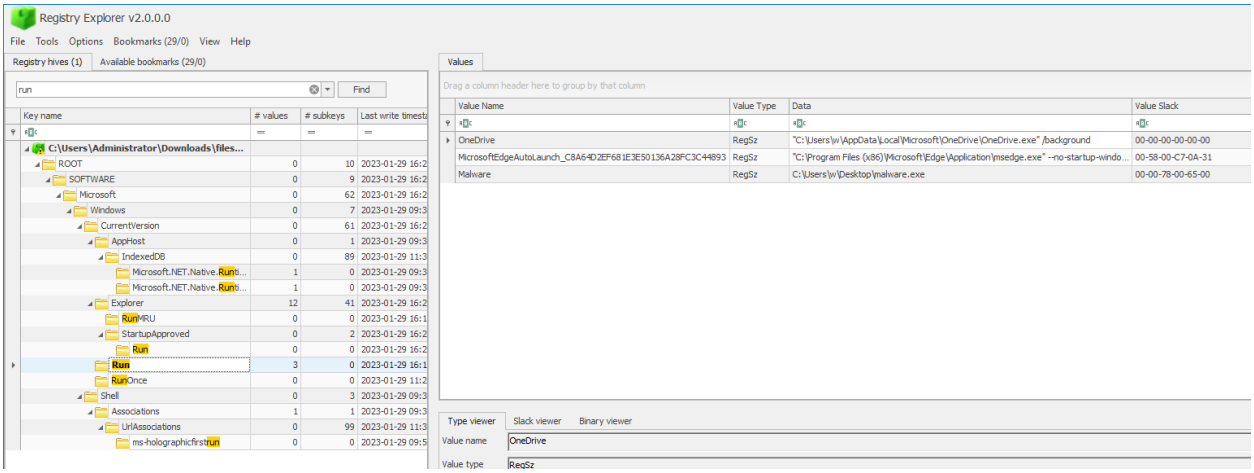


Answer 1B: The most recent typedpaths is the calc.exe.

Answer 1C: For the malware question, I looked up the commonly changed registry keys to achieve presistace.

> This allows the malware to persist even after the system has been rebooted.
>
> Malware achieves persistence by modifying the registry keys in one of AutoStart Extention Points (ASEPs). Below are some of the registry keys that malware mostly achieves its persistence by editing the registry keys at the User Level:
>
> - HKEY_CURRENT_USERSoftwareMicrosoftWindowsCurrentVersionRun
> - HKEY_CURRENT_USERSoftwareMicrosoftWindowsCurrentVersionRunOnce

Finding these registry keys, I see the malware.exe .



Hence this is the new value added to the registry by the virus.

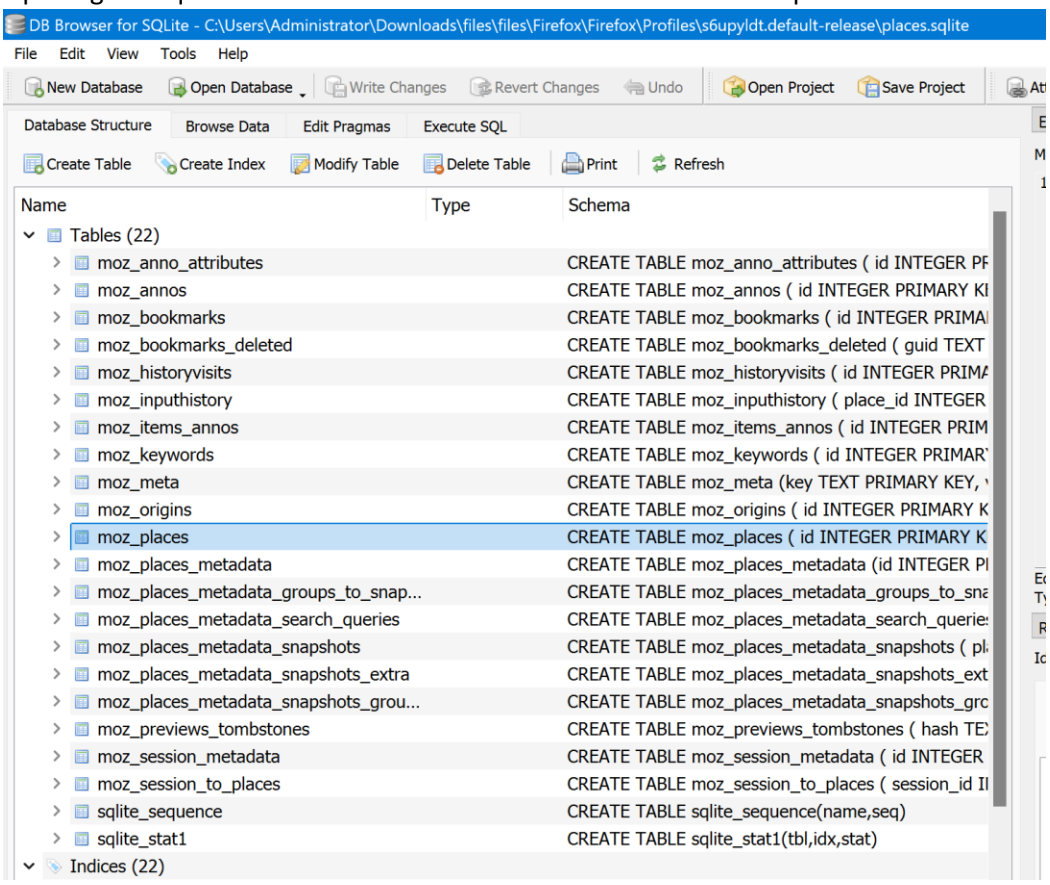
Answer 2A:

Running the decrypt tool and giving the firefox folder as an argument we see the answers.

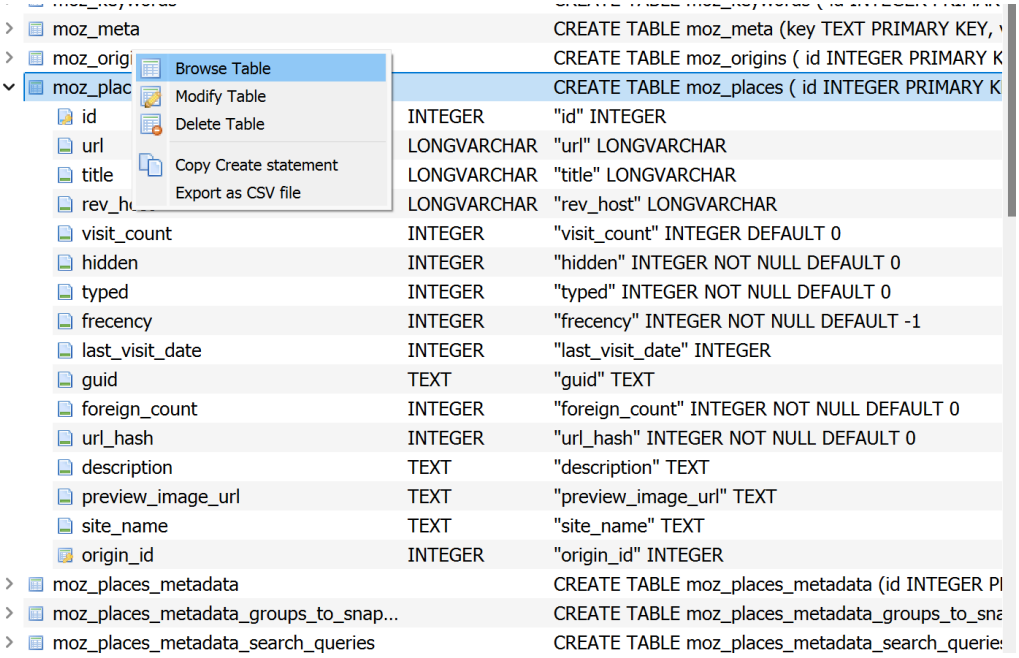
```
PS C:\Users\Administrator\Downloads\firefox_decrypt-main\firefox_decrypt-main> python .\firefox_decrypt.py C:\Users\Admi
nistrator\Downloads\files\files\Firefox\Firefox
2024-08-27 10:37:10,905 - WARNING - Running with unsupported encoding 'locale': cp1252 - Things are likely to fail from
here onwards
Select the Mozilla profile you wish to decrypt
1 -> Profiles/83bm17p1.default
2 -> Profiles/s6upyldt.default-release
2

Website:   https://www.reddit.com
Username: 'hackerman'
Password: 'sup3rs3cur3p4ssw0rd'
PS C:\Users\Administrator\Downloads\firefox_decrypt-main\firefox_decrypt-main>
```

Answer 2B:

Opening the sqlite database of in the default-release folder of the profiles. `



Inside the Places.sqlite the moz_places contains the tables for the browser history.



DB Browser for SQLite - C:\Users\Administrator\Downloads\files\files\Firefox\Firefox\Profiles\s6upyldt.default-release\places.sqlite

File Edit View Tools Help

New Database | Open Database | Write Changes | Revert Changes | Undo | Open Project | Save Project

Database Structure | Browse Data | Edit Pragmas | Execute SQL

moz_anno_attributes | moz_places | moz_places

moz_places

Table: moz_places | Filter in any column

	id	url	title	
	Fil...	Filter	Filter	Filter
1	1	https://support.mozilla.org/products...	NULL	gro.all:
2	2	https://support.mozilla.org/kb/...	NULL	gro.all:
3	3	https://www.mozilla.org/contribute/	NULL	gro.all:
4	4	https://www.mozilla.org/about/	NULL	gro.all:
5	5	https://www.mozilla.org/privacy/...	NULL	gro.all:
6	6	https://www.mozilla.org/firefox/...	NULL	gro.all:
7	7	https://www.mozilla.org/en-US/...	Firefox Privacy Notice — Mozilla	gro.all:
8	8	https://www.amazon.com/exec/obidos/...	NULL	moc.noz
9	9	https://www.amazon.com/s/...	Amazon.com : BlackHat Go	moc.noz
10	10	https://www.amazon.com/s?...	Amazon.com : BlackHat Go	moc.noz
11	11	https://www.amazon.com/Black-Hat-Go-...	Amazon.com: Black Hat Go: Go ...	moc.noz
12	12	https://www.amazon.com/s/...	Amazon.com : BlackHat Python	moc.noz
13	13	https://www.amazon.com/s?...	Amazon.com : BlackHat Python	moc.noz
14	14	https://www.amazon.com/Black-Hat-...	Black Hat Python, 2nd Edition: Pytho...	moc.noz
15	15	https://www.amazon.com/s/...	Amazon.com : BlackHat GraphQL	moc.noz
16	16	https://www.amazon.com/s?...	Amazon.com : BlackHat GraphQL	moc.noz
17	17	https://www.amazon.com/Black-Hat-...	Amazon.com: Black Hat GraphQL: ...	moc.noz
18	23	https://www.reddit.com/	Reddit - Dive into anything	moc.tid
19	24	https://www.google.com/search?...	python dowwnload - Google Search	moc.elg
20	25	https://www.python.org/downloads/	Download Python | Python.org	gro.noh
21	26	https://www.python.org/ftp/python/...	python-3.11.1-amd64(1).exe	gro.noh
22	27	http://tryhackme.com/	NULL	moc.emk

From these records we see that the most visited website is amazon.com.

Answer 2C:

In the same moz_places table we see that the python 3.11 exe was the last downloaded file by suspect and that link was visited.

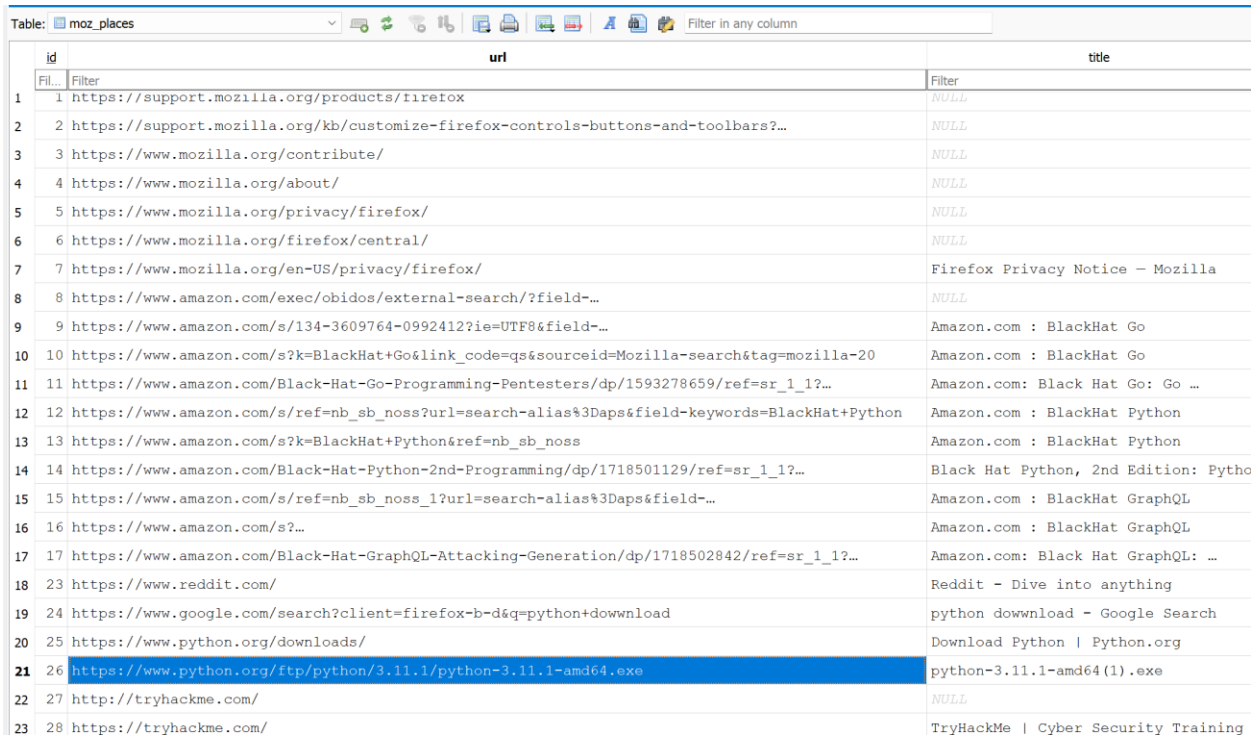
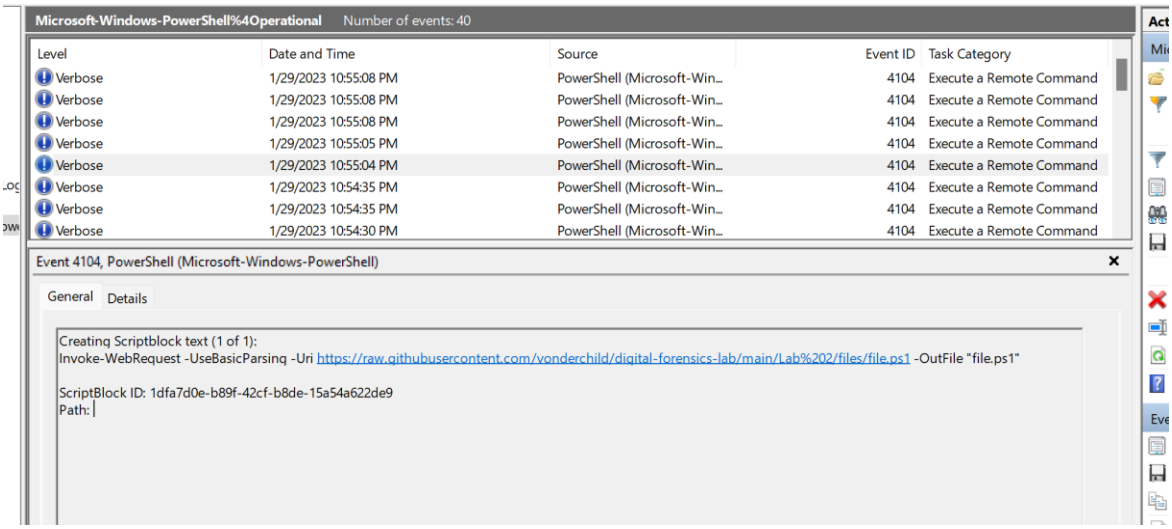


Table: moz_places — Filter in any column

	id	url	title
1	1	https://support.mozilla.org/products/firefox	NULL
2	2	https://support.mozilla.org/kb/customize-firefox-controls-buttons-and-toolbars?…	NULL
3	3	https://www.mozilla.org/contribute/	NULL
4	4	https://www.mozilla.org/about/	NULL
5	5	https://www.mozilla.org/privacy/firefox/	NULL
6	6	https://www.mozilla.org/firefox/central/	NULL
7	7	https://www.mozilla.org/en-US/privacy/firefox/	Firefox Privacy Notice — Mozilla
8	8	https://www.amazon.com/exec/obidos/external-search/?field-…	NULL
9	9	https://www.amazon.com/s/134-3609764-0992412?ie=UTF8&field-…	Amazon.com : BlackHat Go
10	10	https://www.amazon.com/s?k=BlackHat+Go&link_code=qs&sourceid=Mozilla-search&tag=mozilla-20	Amazon.com : BlackHat Go
11	11	https://www.amazon.com/Black-Hat-Go-Programming-Pentesters/dp/1593278659/ref=sr_1_1?…	Amazon.com: Black Hat Go: Go …
12	12	https://www.amazon.com/s/ref=nb_sb_noss?url=search-alias%3Daps&field-keywords=BlackHat+Python	Amazon.com : BlackHat Python
13	13	https://www.amazon.com/s?k=BlackHat+Python&ref=nb_sb_noss	Amazon.com : BlackHat Python
14	14	https://www.amazon.com/Black-Hat-Python-2nd-Programming/dp/1718501129/ref=sr_1_1?…	Black Hat Python, 2nd Edition: Pytho
15	15	https://www.amazon.com/s/ref=nb_sb_noss_1?url=search-alias%3Daps&field-…	Amazon.com : BlackHat GraphQL
16	16	https://www.amazon.com/s?…	Amazon.com : BlackHat GraphQL
17	17	https://www.amazon.com/Black-Hat-GraphQL-Attacking-Generation/dp/1718502842/ref=sr_1_1?…	Amazon.com: Black Hat GraphQL: …
18	23	https://www.reddit.com/	Reddit - Dive into anything
19	24	https://www.google.com/search?client=firefox-b-d&q=python+dowwnload	python dowwnload - Google Search
20	25	https://www.python.org/downloads/	Download Python | Python.org
21	26	https://www.python.org/ftp/python/3.11.1/python-3.11.1-amd64.exe	python-3.11.1-amd64(1).exe
22	27	http://tryhackme.com/	NULL
23	28	https://tryhackme.com/	TryHackMe | Cyber Security Training

Answer 3A:

Analyzing the logs we see that the command executed is as follows:



Microsoft-Windows-PowerShell%4Operational — Number of events: 40

Level	Date and Time	Source	Event ID	Task Category
Verbose	1/29/2023 10:55:08 PM	PowerShell (Microsoft-Win…	4104	Execute a Remote Command
Verbose	1/29/2023 10:55:08 PM	PowerShell (Microsoft-Win…	4104	Execute a Remote Command
Verbose	1/29/2023 10:55:08 PM	PowerShell (Microsoft-Win…	4104	Execute a Remote Command
Verbose	1/29/2023 10:55:05 PM	PowerShell (Microsoft-Win…	4104	Execute a Remote Command
Verbose	1/29/2023 10:55:04 PM	PowerShell (Microsoft-Win…	4104	Execute a Remote Command
Verbose	1/29/2023 10:54:35 PM	PowerShell (Microsoft-Win…	4104	Execute a Remote Command
Verbose	1/29/2023 10:54:35 PM	PowerShell (Microsoft-Win…	4104	Execute a Remote Command
Verbose	1/29/2023 10:54:30 PM	PowerShell (Microsoft-Win…	4104	Execute a Remote Command

Event 4104, PowerShell (Microsoft-Windows-PowerShell)

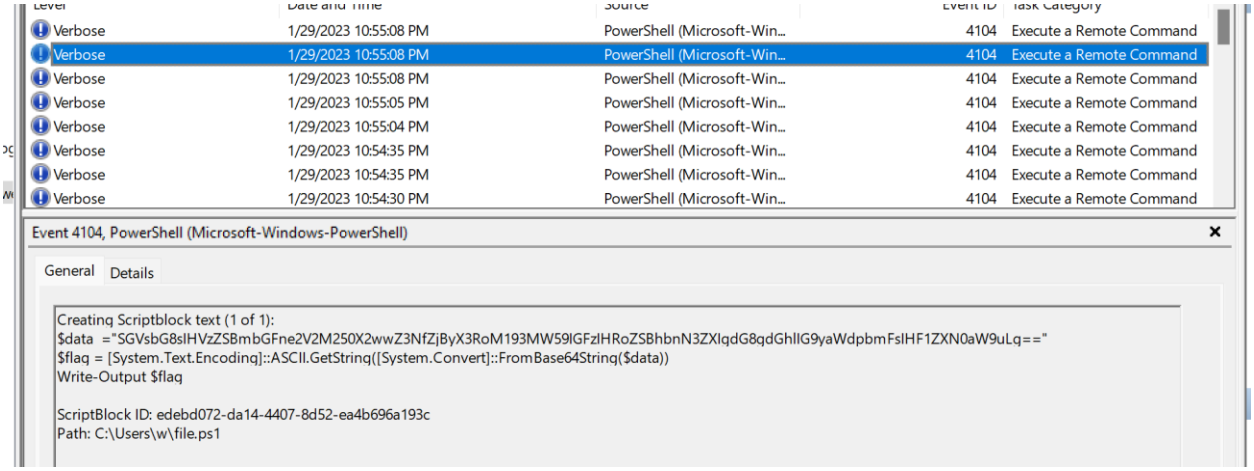
General Details

Creating Scriptblock text (1 of 1):
Invoke-WebRequest -UseBasicParsing -Uri https://raw.githubusercontent.com/yonderchild/digital-forensics-lab/main/Lab%202/files/file.ps1 -OutFile "file.ps1"

ScriptBlock ID: 1dfa7d0e-b89f-42cf-b8de-15a54a622de9
Path:

Answer 3B:

Analyzing the logs,I see the the data sent.



Decrypting it from base64:

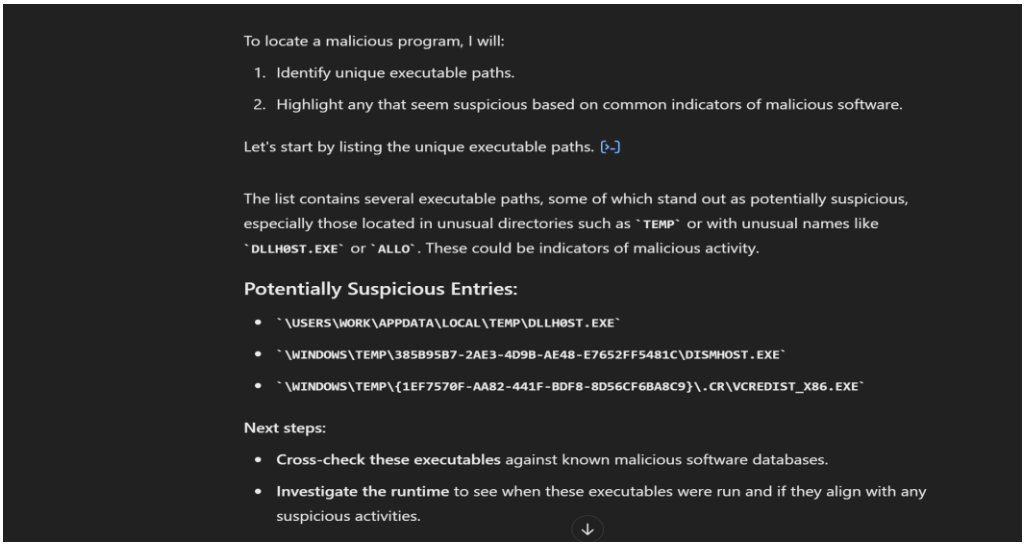
Hello, use flag{ev3nt_l0gs_f0r_th3_w1n} as the answer to the original question.

Answer 4:

Using the prefetch folder that is given I execute the following command to run the tool.

This redirects the output to the csv format in the tools folder.

Giving the timeline file to chatgpt it gives top 3 suspicious files.



At row 59 we see the file which is misnamed and is run from a non standard path as it is the only one that stands out. DLLH0ST instead of DLLHOST renaming error. Hence it is the malware.

52	#########	\VOLUME{01d95894c528b62b-44c53985}\WINDOWS\SYSTEM32\CONSENT.EXE
53	#########	\VOLUME{01d95894c528b62b-44c53985}\WINDOWS\SYSTEM32\CONSENT.EXE
54	#########	\VOLUME{01d95894c528b62b-44c53985}\WINDOWS\SYSTEM32\CONSENT.EXE
55	#########	\VOLUME{01d95894c528b62b-44c53985}\WINDOWS\SYSTEM32\CSRSS.EXE
56	#########	\VOLUME{01d95894c528b62b-44c53985}\WINDOWS\SYSTEM32\DASHOST.EXE
57	#########	\VOLUME{01d95894c528b62b-44c53985}\WINDOWS\SYSTEM32\DEFRAG.EXE
58	#########	\VOLUME{01d95894c528b62b-44c53985}\WINDOWS\TEMP\385B95B7-2AE3-4D9B-AE48-E7652FF5481C\DISMHOST.EXE
59	#########	\VOLUME{01d95894c528b62b-44c53985}\USERS\WORK\APPDATA\LOCAL\TEMP\DLLH0ST.EXE
60	#########	\VOLUME{01d95894c528b62b-44c53985}\WINDOWS\SYSTEM32\DLLHOST.EXE
61	#########	\VOLUME{01d95894c528b62b-44c53985}\WINDOWS\SYSTEM32\DLLHOST.EXE
62	#########	\VOLUME{01d95894c528b62b-44c53985}\WINDOWS\SYSTEM32\DLLHOST.EXE
63	#########	\VOLUME{01d95894c528b62b-44c53985}\WINDOWS\SYSTEM32\DLLHOST.EXE
64	#########	\VOLUME{01d95894c528b62b-44c53985}\WINDOWS\SYSTEM32\DLLHOST.EXE
65	#########	\VOLUME{01d95894c528b62b-44c53985}\WINDOWS\SYSTEM32\DLLHOST.EXE
66	#########	\VOLUME{01d95894c528b62b-44c53985}\WINDOWS\SYSTEM32\DLLHOST.EXE