Put Student Name(s) ↓	Put Student IDs ↓	Due Date	Grade Weight
Ishan Aakash Patel	146151238	As Posted	6%

Name	Lab3: Memory Forensics Challenge

Instructions	• It is an Individual assignment. Put your name + Student ID in the empty spaces above.
	• Submit via the BB relevant link ONLY. NO submission via email please. Be sure to submit the final version file ONLY.
	• Show your genuine signs of your work is done on your machine. This includes:
	  ○ Screenshots that show your desktop background with Date/Time.
	  ○ Show a pop-up bx that shows "your name + IP".
	  ○ Show your logged account when applicable. Optional: Your photo.
	• Submit your report name: CYT215-Lab3-Student Name & ID

Challenge Scenario	You are a memory forensic analyst. One of the clients of your company, lost the access to their system due to an unknown error. He is supposedly a very popular "environmental" activist. As a part of the investigation. he told us that his go to applications are browsers, his password managers etc. We hope that you can dig into this memory dump and find his important stuff and give it back to us.
Challenge Questions To be Answered	In this challenge, there are 3 flags to find. You will need to use Volatility to perform a memory dump and investigate to locate the flags. This is a Capture the Flag (CTF) exercise, where the objective is to discover the hidden flags. To help you get started, there are several write-ups available online. Here is one useful resource: https://mmox.me/posts/writeups/memlabs-lab2/ https://www.youtube.com/watch?v=c7DTCH2ajqM Using the write-up linked above and the YouTube as a reference, you will create your own documentation on how you solved the challenge and found the 3 flags. Your write-up should include clear screenshots showing each step you took to find all 3 flags on your system (with time stamps from the Linux command line). This will ensure that you are not copying write ups from online and trying the challenge yourself on your machine. Any copied screenshots or writeups will receive an automatic ZERO. Please run the tools on your own machine/ Virtual Machine. Utilize the provided write-up and other online resources to learn how to use Volatility and analyze memory files for artifacts.

	At the end of your report, answer the following question: 1. What is the purpose of Volatility? 2. Why is it important to analyze memory dumps? 3. How difficult did you find this challenge? Prerequisites – Install a Linux VM On this VM, install Volatility. Guides below: https://www.youtube.com/watch?v=AJ0denKsXyw&t=528s (volatility 3) https://github.com/volatilityfoundation/volatility3 (Volatility 3) https://github.com/volatilityfoundation/volatility (Volatility 2) https://blog.onfvp.com/post/volatility-cheatsheet/ - Cheat sheet for commands Volatility 2 vs Volatility 3
Students Work	• Go to the challenge https://github.com/stuxnet999/MemLabs/tree/master/Lab%202 • Download the raw image on your VIRTUAL MACHINE. https://mega.nz/file/ChoDHaja#1XvuQd49c7-7kgJvPXIEAst-NXi8L3ggwienE1uoZTk

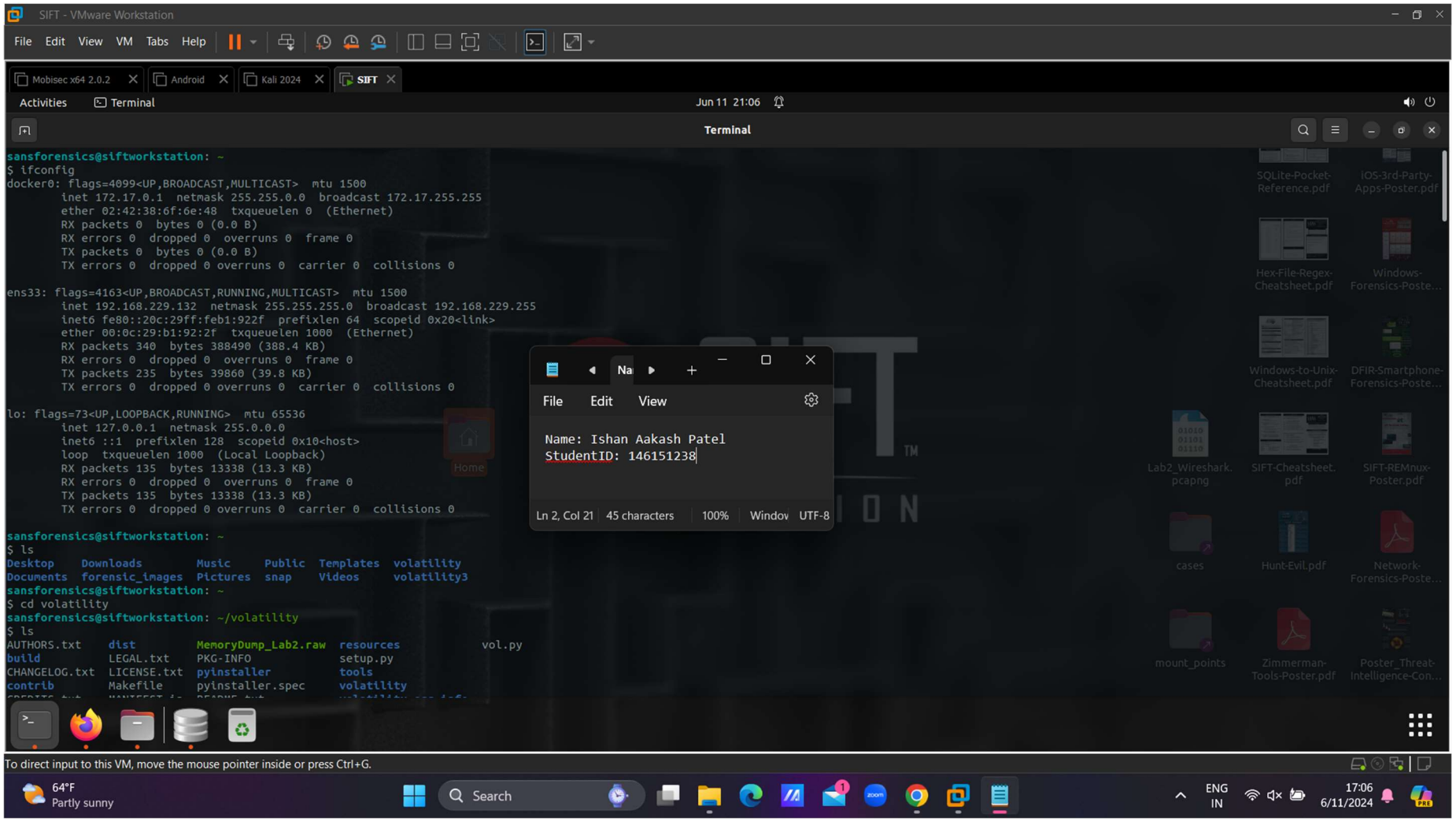
required for this activity	• Follow the following writeups and tutorials to find the 3 flags to the challenge: https://mmox.me/posts/writeups/memlabs-lab2/ https://www.youtube.com/watch?v=c7DTCH2ajqM There are several other resources on google as well for this challenge. Use them all as a reference to learn. • Document each step (WITH command line screenshots) to show steps how you retrieved each flag. At the end of your report, answer the following questions: 1. What is the purpose of Volatility? 2. Why is it important to analyze memory dumps? 3. How difficult did you find this challenge? **Your write up/report can go below this table.** ENSURE THAT YOU ARE DOING THIS LAB IN A VIRTUAL MACHINE.
Grading Alerts	• If you do NOT use this template or delete any part of it or use any other template, you will be degraded. • If you do NOT follow the fie naming convention, you will be degraded. • If you do NOT submit your file in PDF; you will be degraded. • If you do NOT show your account real name (when applicable); you will be degraded. • If you do NOT show your machine desktop background (with date & time) and IP, you will be degraded. If you do NOT write (in your own words) your learning experience for the activity practices, you will be degraded.

START WRITE UP BELOW THIS

Memlabs Lab-2

I am using SIFT virtual machine for this particular Lab and I installed volatility in the SIFT VM.

My IP address.



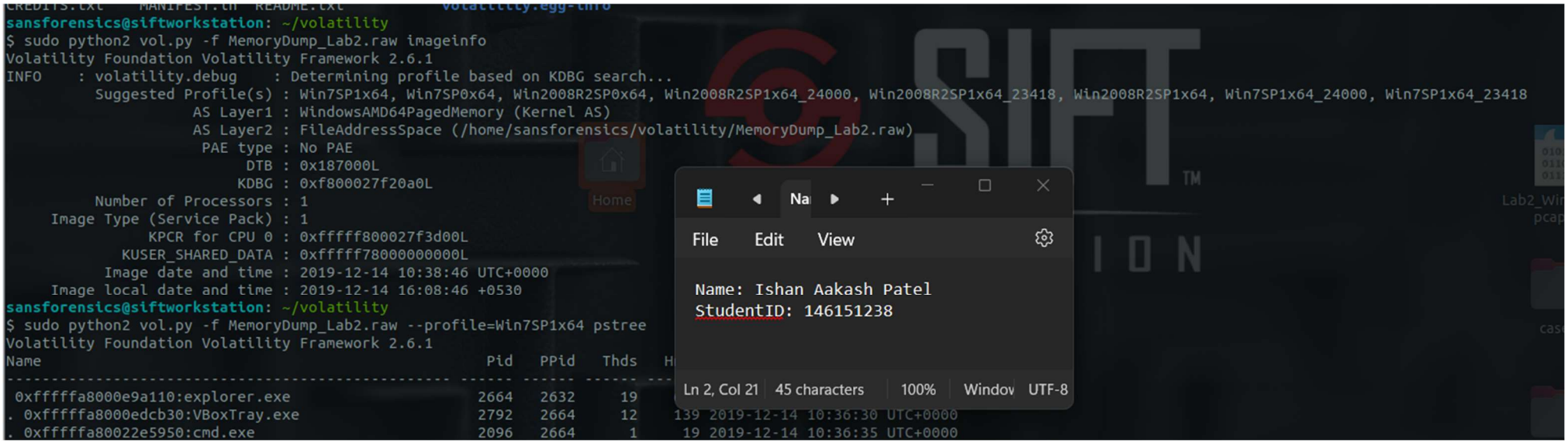
Stage 1

Step 1: Identify the Memory Profile

First, we need to identify the correct profile for Volatility to use with the memory dump.

```
vol.py -f MemoryDump_Lab2.raw imageinfo
```

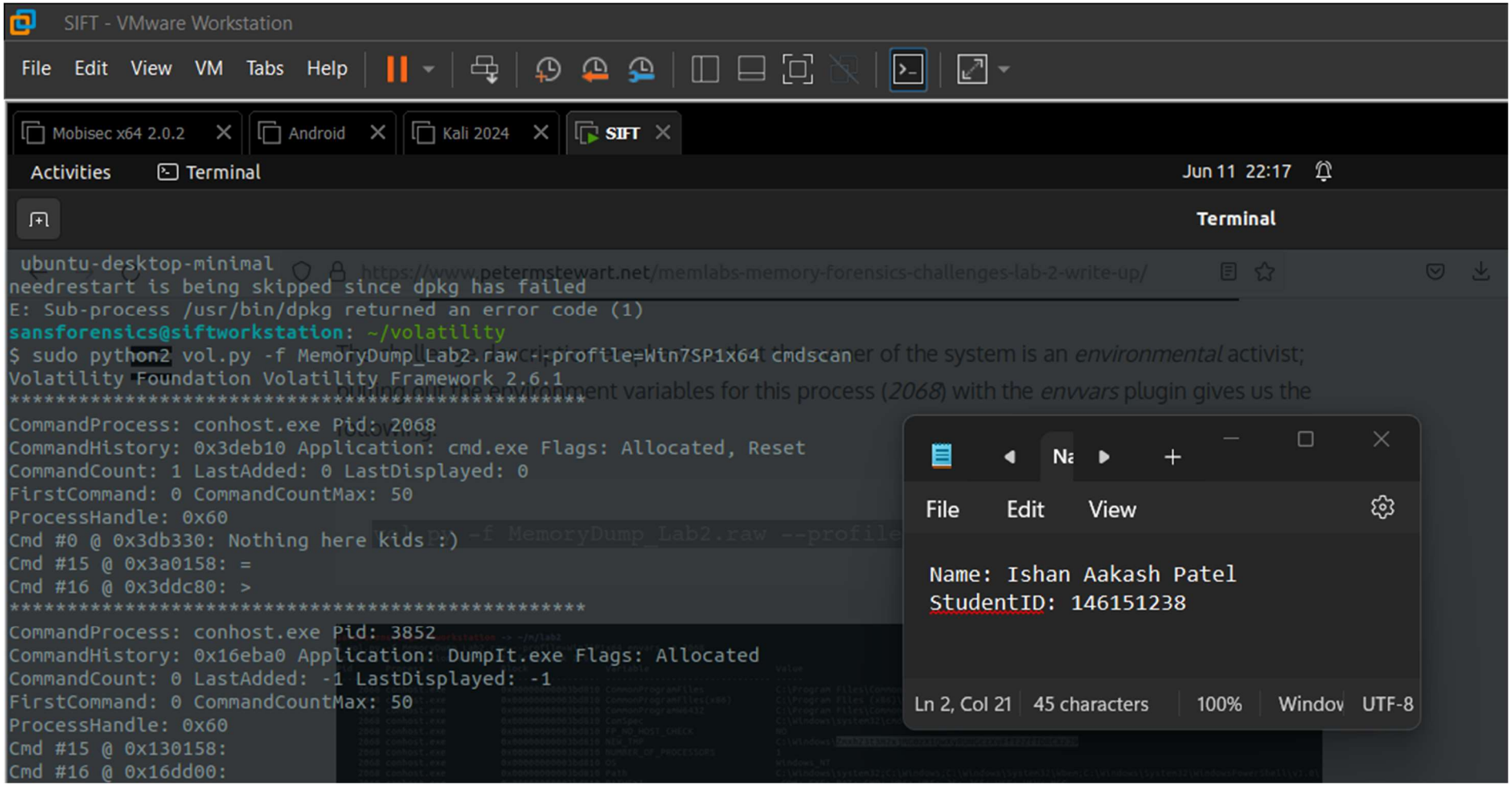
Based on the output, we determine that `Win7SP1x64` is the appropriate profile.



Step 2: Check Command-Line Output

We use the `cmdscan` plugin to look for unusual command-line activity.

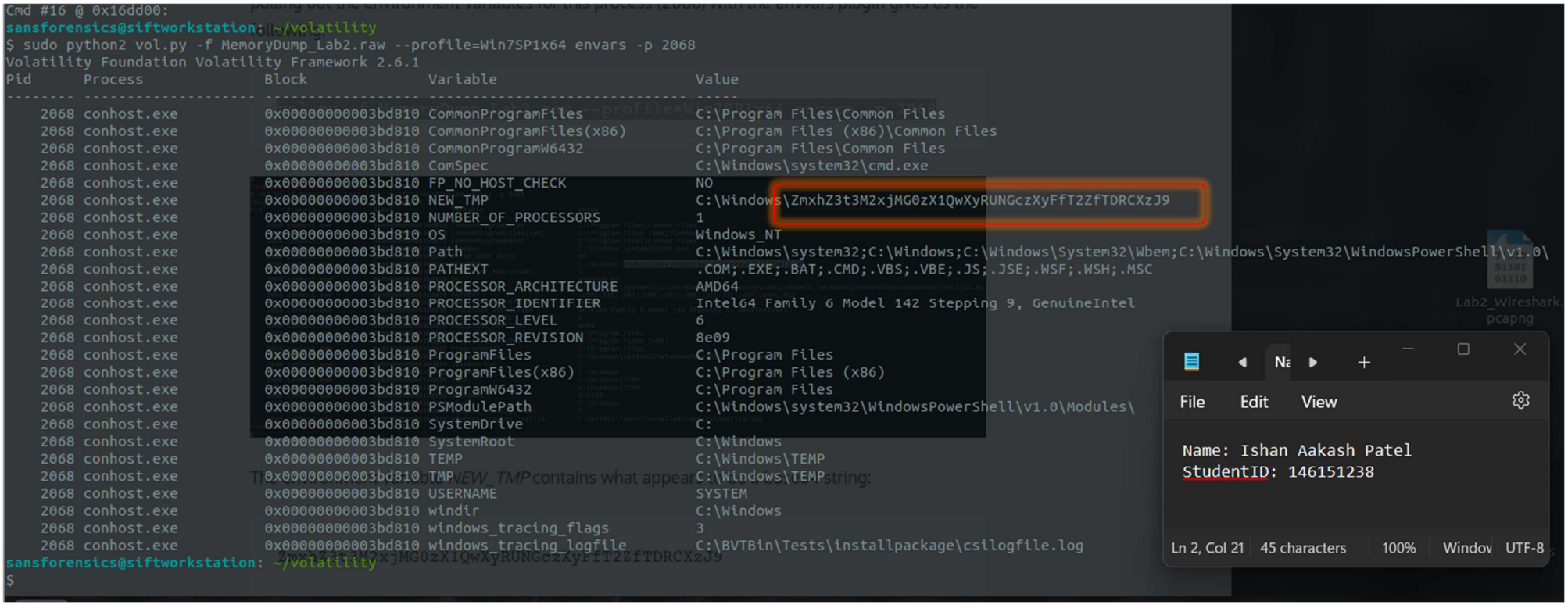
```
vol.py -f MemoryDump_Lab2.raw --profile=Win7SP1x64 cmdscan
```



Step 3: Examine Environment Variables

The challenge description mentions environmental activism. We check environment variables for suspicious strings using the `envvars` plugin.

```
vol.py -f MemoryDump_Lab2.raw --profile=Win7SP1x64 envars -p 2068
```

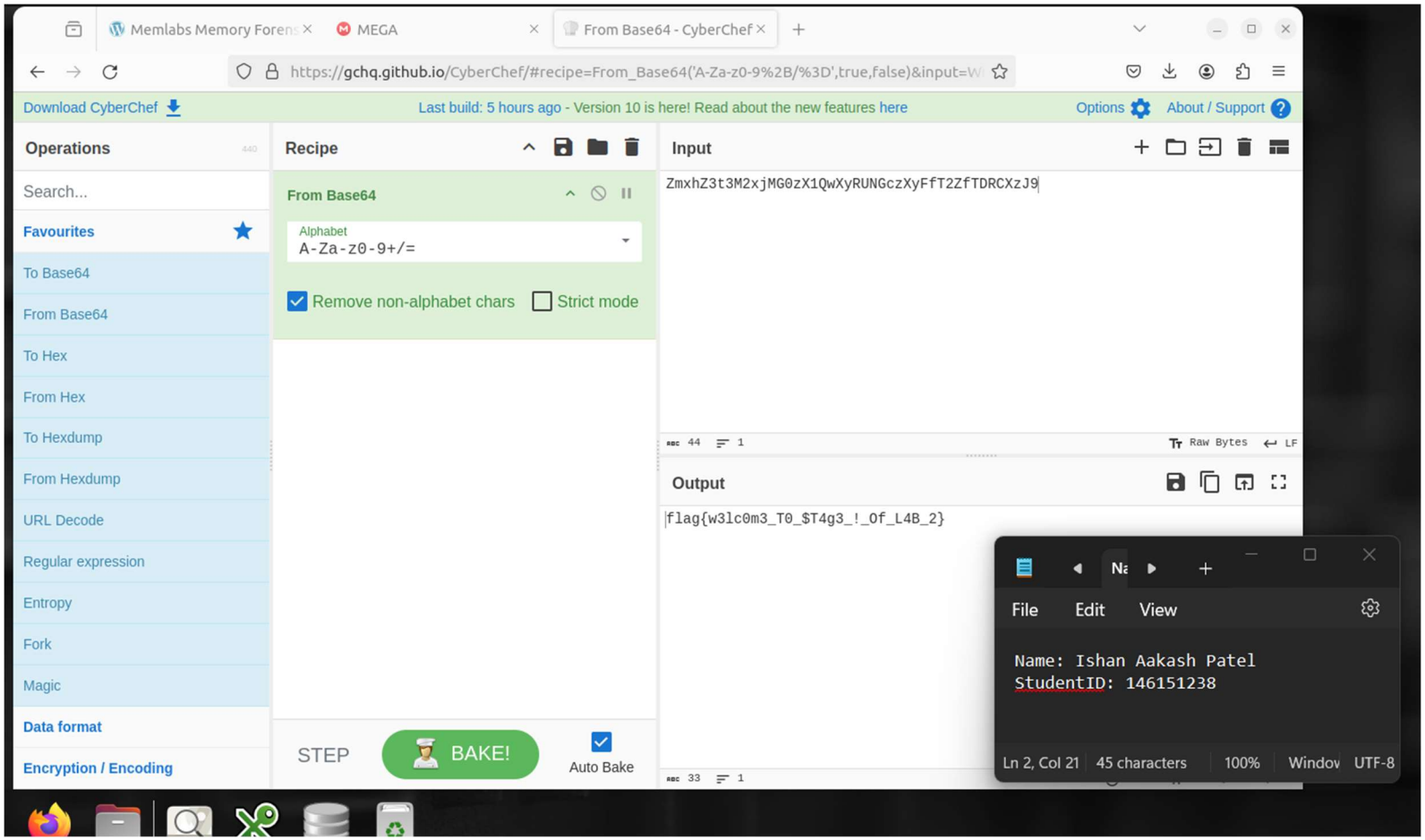


Step 4: Decode Base64 String

We find a base64 string in the environment variables, specifically in `NEW_TMP`. We decode it using CyberChef to get our first flag.

Base64 String: `ZmxhZ3t3M2xjMG0zX1QwXyRUNGczXyFfT2ZfTDRCXzJ9`

Decoded Flag: `flag{w3lc0m3_T0_$T4g3_!_Of_L4B_2}`



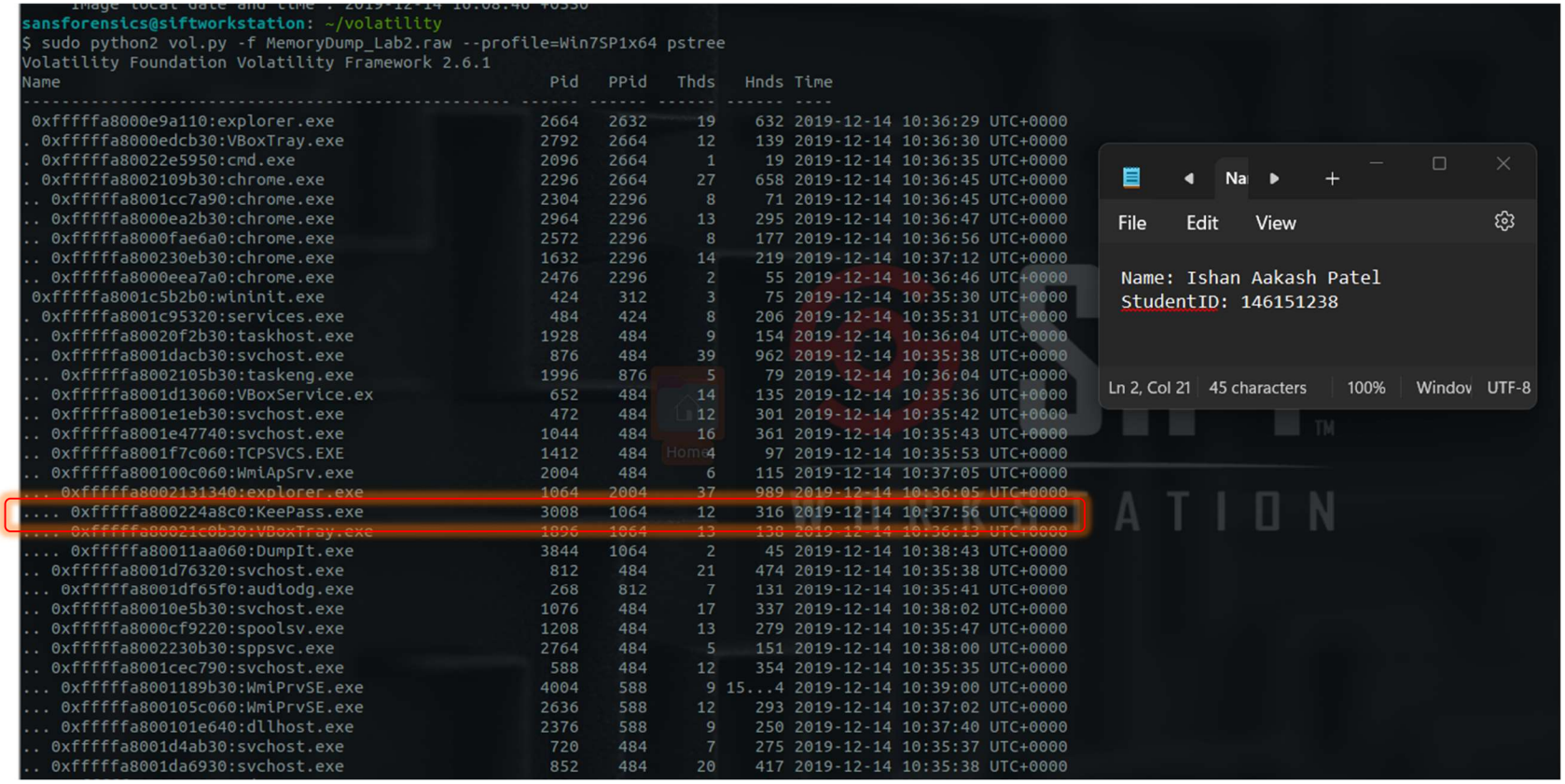
Stage - 2

Step 1: Analyze Process Tree

We use the `pstree` plugin to display a hierarchical list of processes running on the system at the time of the memory dump. This helps us identify key applications such as web browsers and password managers.

```
vol.py -f MemoryDump_Lab2.raw --profile=Win7SP1x64 pstree
```

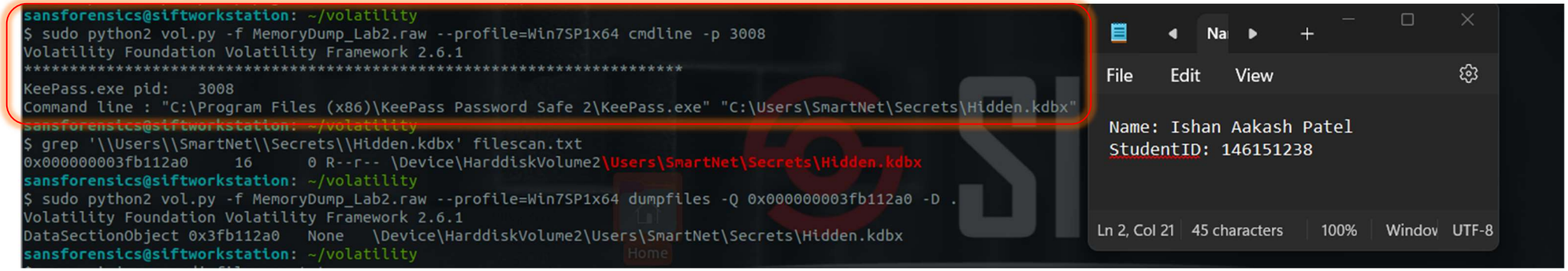
The process tree shows that Chrome and the KeePass password manager were running, providing leads for further investigation.



Step 2: Analyze KeePass Process

We identified the KeePass process (PID 3008) from the process tree. Now, we find the command line associated with it.

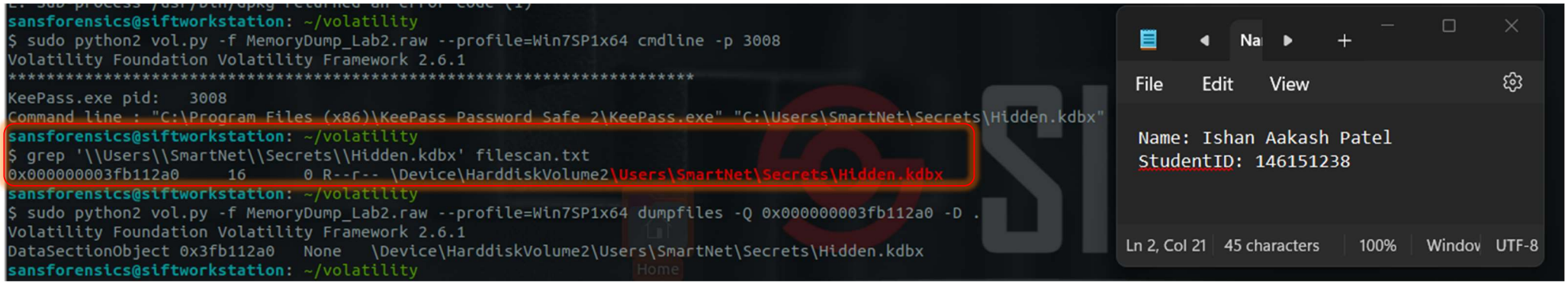
```
vol.py -f MemoryDump_Lab2.raw --profile=Win7SP1x64 cmdline -p 3008
```



Step 3: Locate KeePass Database File

We search for the KeePass database file using `grep` on the filescan output.

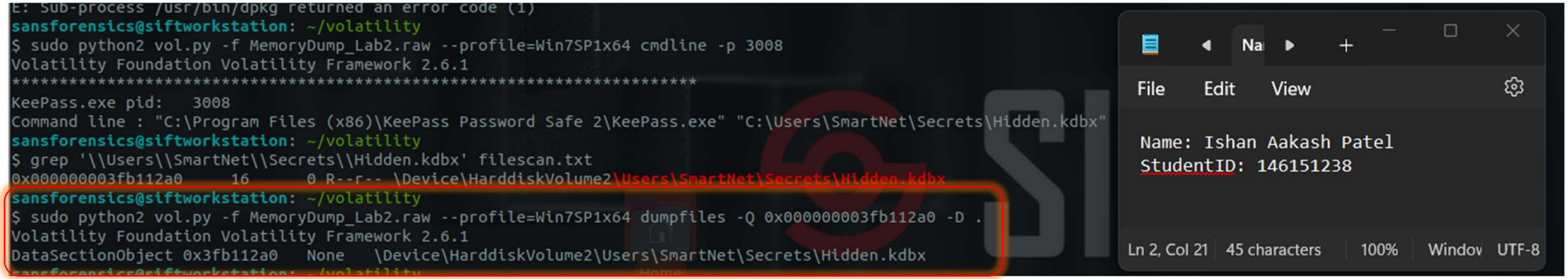
```
grep '\\Users\\SmartNet\\Secrets\\Hidden.kdbx' filescan.txt
```



Step 4: Extract KeePass Database File

We extract the database file from the memory dump using its offset.

```
vol.py -f MemoryDump_Lab2.raw --profile=Win7SP1x64 dumpfiles -Q 0x000000003fb112a0 -D .
```



Step 5: Find KeePass Password

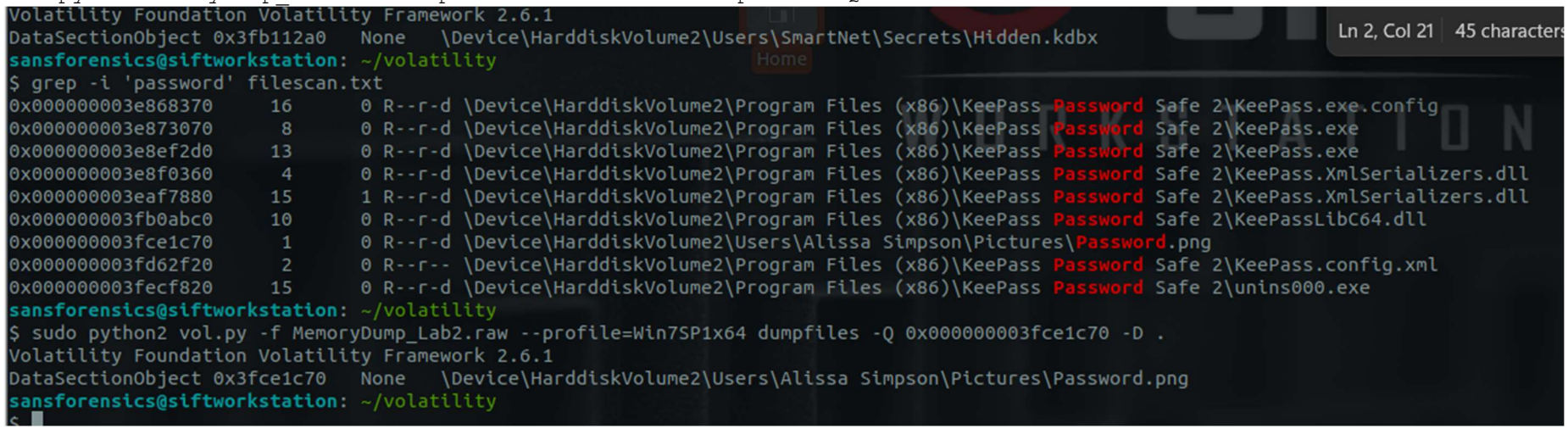
We search for a password using `grep` on the filescan output and locate a file named `Password.png`.

```
grep -i 'password' filescan.txt
```

Step 6: Extract Password Image

We extract the `Password.png` file from the memory dump using its offset.

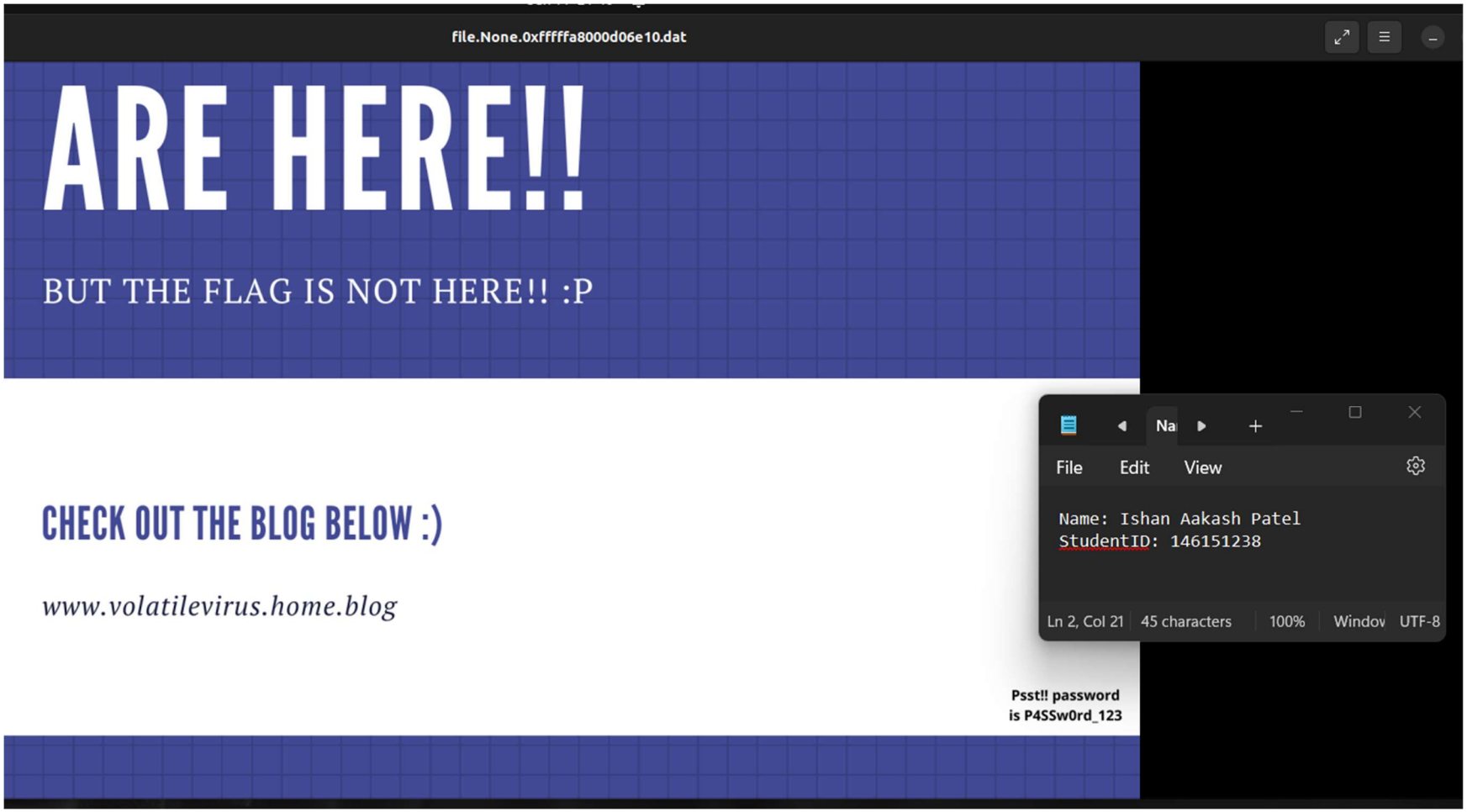
```
vol.py -f MemoryDump_Lab2.raw --profile=Win7SP1x64 dumpfiles -Q 0x000000003fce1c70 -D .
```



Step 7: Retrieve Password from Image

We open the `Password.png` file and find the password in the lower right-hand corner.

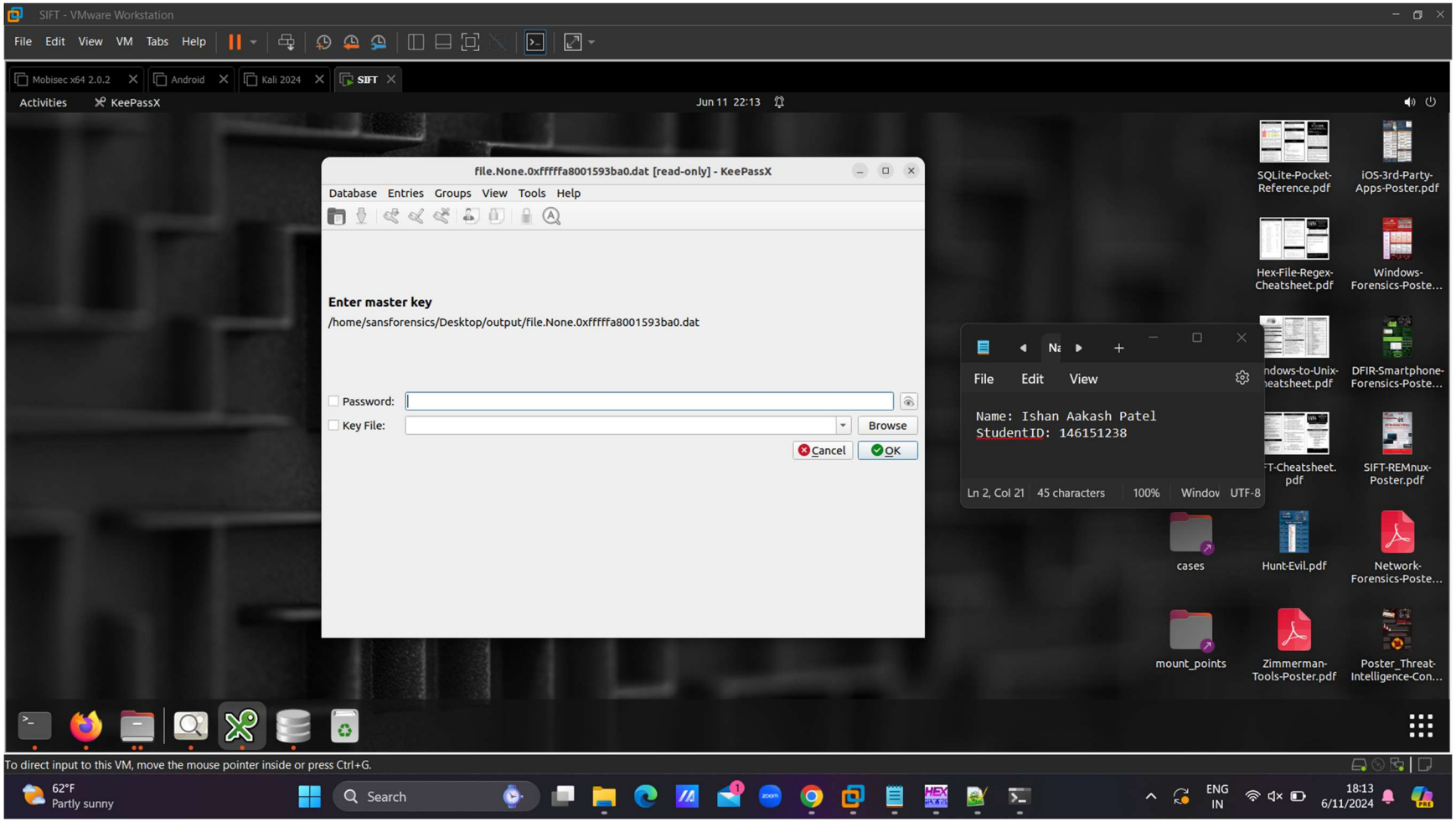
Password: `P4SSw0rd_123`

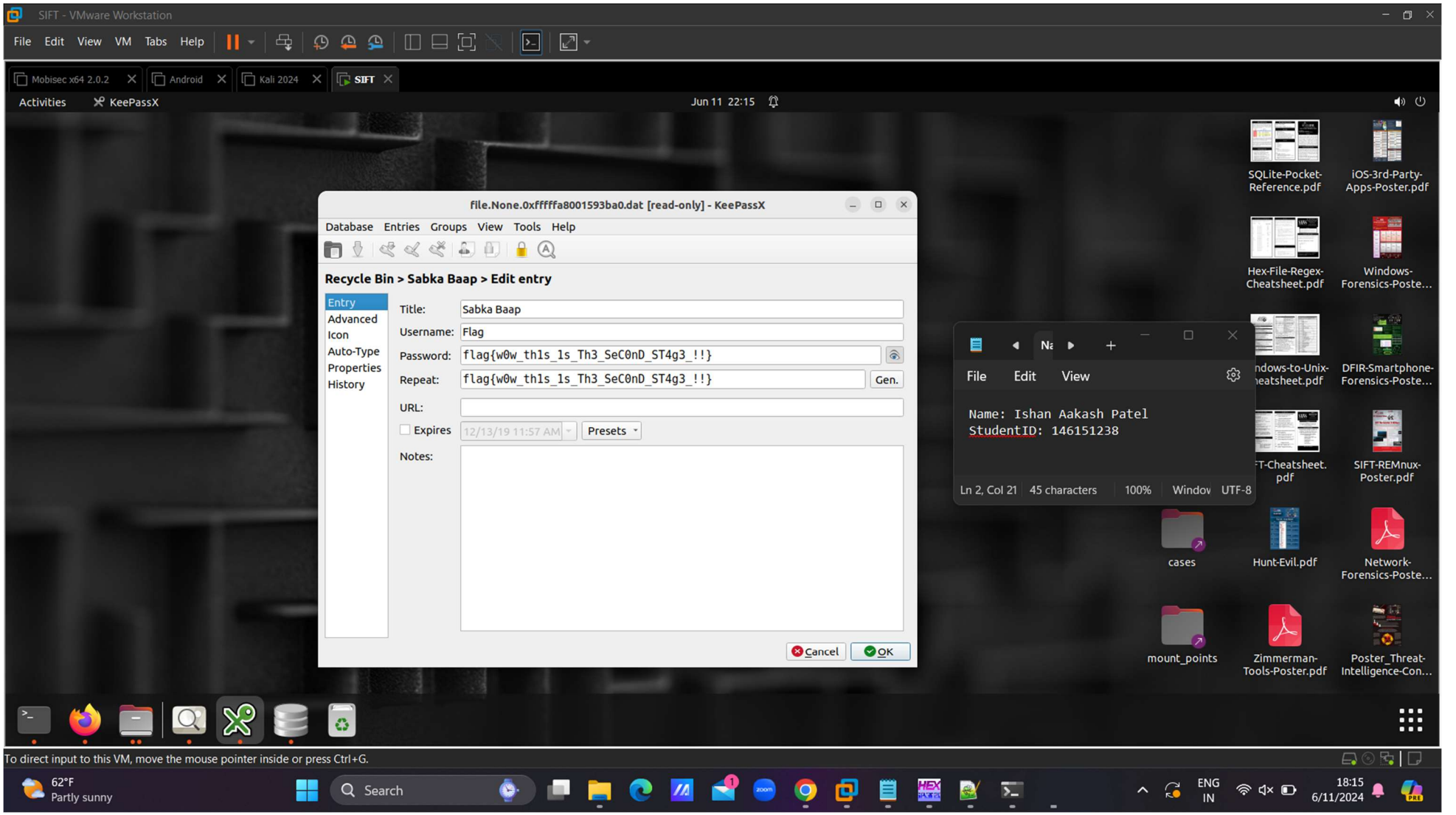


Step 8: Open KeePass Database

We use the password to open the KeePass database and find the flag for Stage 2. (Note : Install keepassX)

Flag: `flag{w0w_th1s_1s_Th3_SeC0nD_ST4g3_!!}`




SIFT - VMware Workstation
File Edit View VM Tabs Help
Mobisec x64 2.0.2
Android
Kali 2024
SIFT
Activities
KeePassX
Jun 11 22:15
file.None.0xfffffa8001593ba0.dat [read-only] - KeePassX
Database Entries Groups View Tools Help
Recycle Bin > Sabka Baap > Edit entry
Entry
Advanced
Icon
Auto-Type
Properties
History
Title: Sabka Baap
Username: Flag
Password: flag{w0w_th1s_1s_Th3_SeC0nD_ST4g3_!!}
Repeat: flag{w0w_th1s_1s_Th3_SeC0nD_ST4g3_!!}
Gen.
URL:
Expires
12/13/19 11:57 AM
Presets
Notes:
Cancel
OK
File Edit View
Name: Ishan Aakash Patel
StudentID: 146151238
Ln 2, Col 21 45 characters 100% Windov UTF-8
SQLite-Pocket-Reference.pdf
iOS-3rd-Party-Apps-Poster.pdf
Hex-File-Regex-Cheatsheet.pdf
Windows-Forensics-Poste...
DFIR-Smartphone-Forensics-Poste...
SIFT-REMnux-Poster.pdf
cases
Hunt-Evil.pdf
Network-Forensics-Poste...
mount_points
Zimmerman-Tools-Poster.pdf
Poster_Threat-Intelligence-Con...
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
62°F
Partly sunny
Search
ENG
IN
18:15
6/11/2024

Stage 3

Step 1: Locate Chrome History File

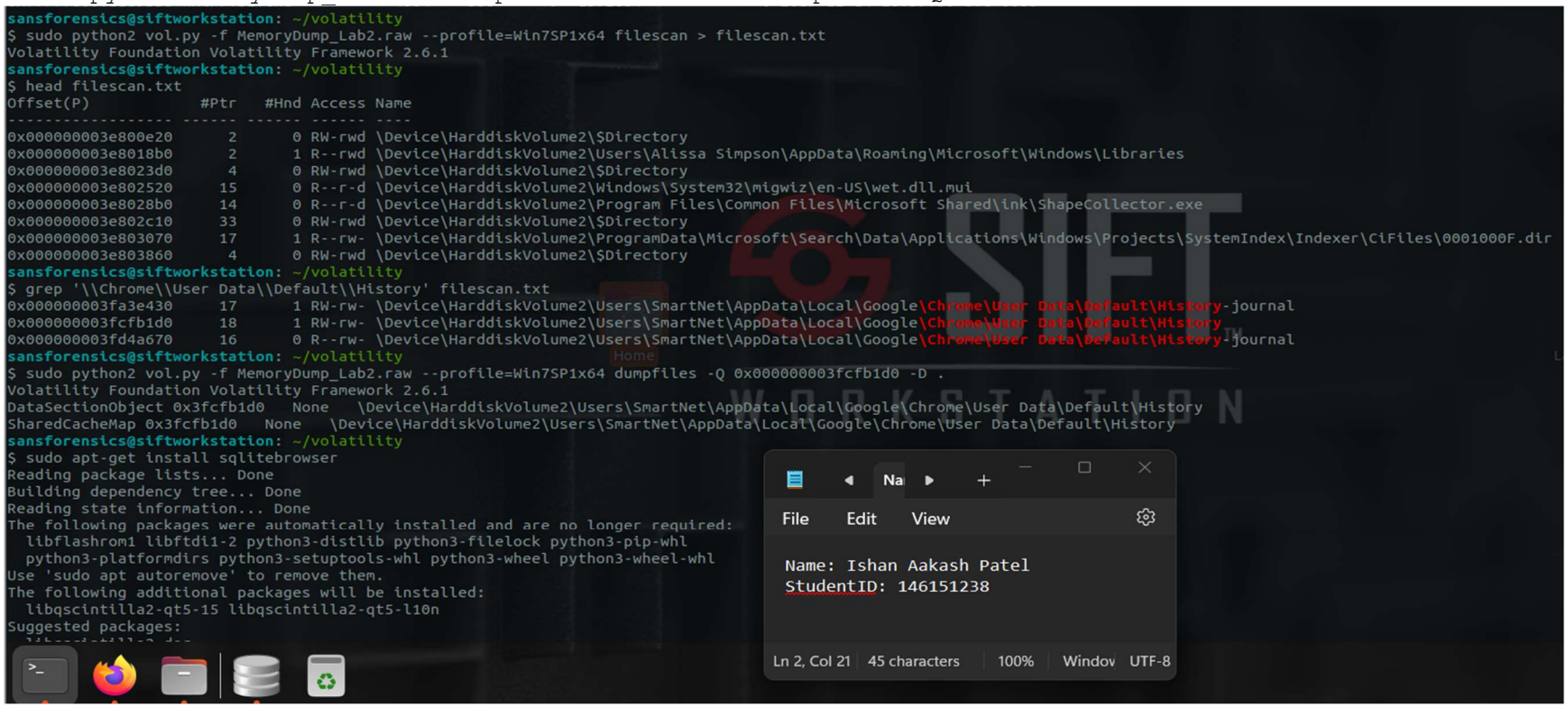
We use `grep` on the filescan output to find the location of the Chrome History file.

```
grep '\\Chrome\\User Data\\Default\\History' filescan.txt
```

Step 2: Extract Chrome History File

We extract the History file from the memory dump using its offset.

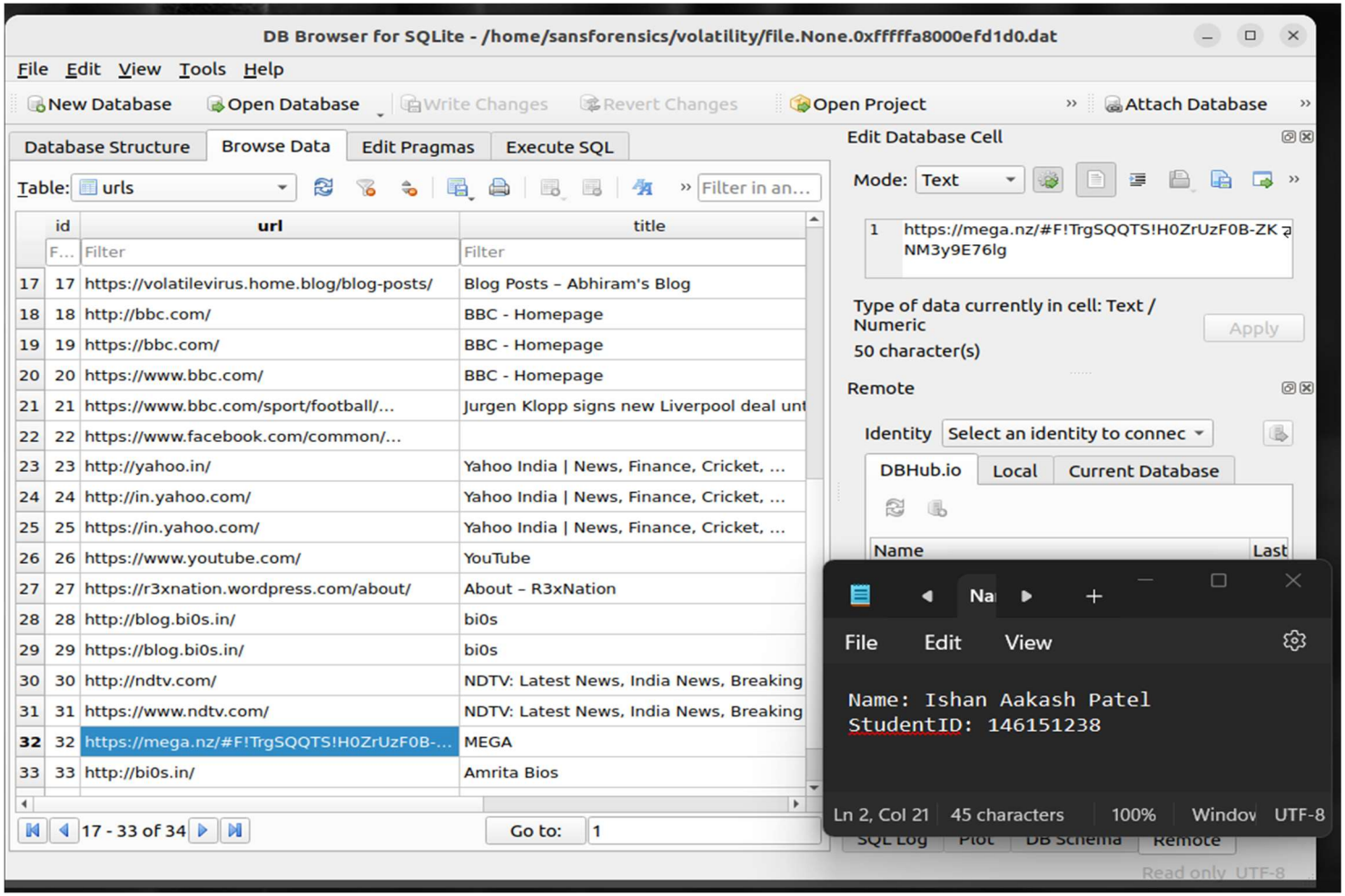
```
vol.py -f MemoryDump_Lab2.raw --profile=Win7SP1x64 dumpfiles -Q 0x000000003fcfb1d0 -D .
```



Step 3: Analyze Chrome History File

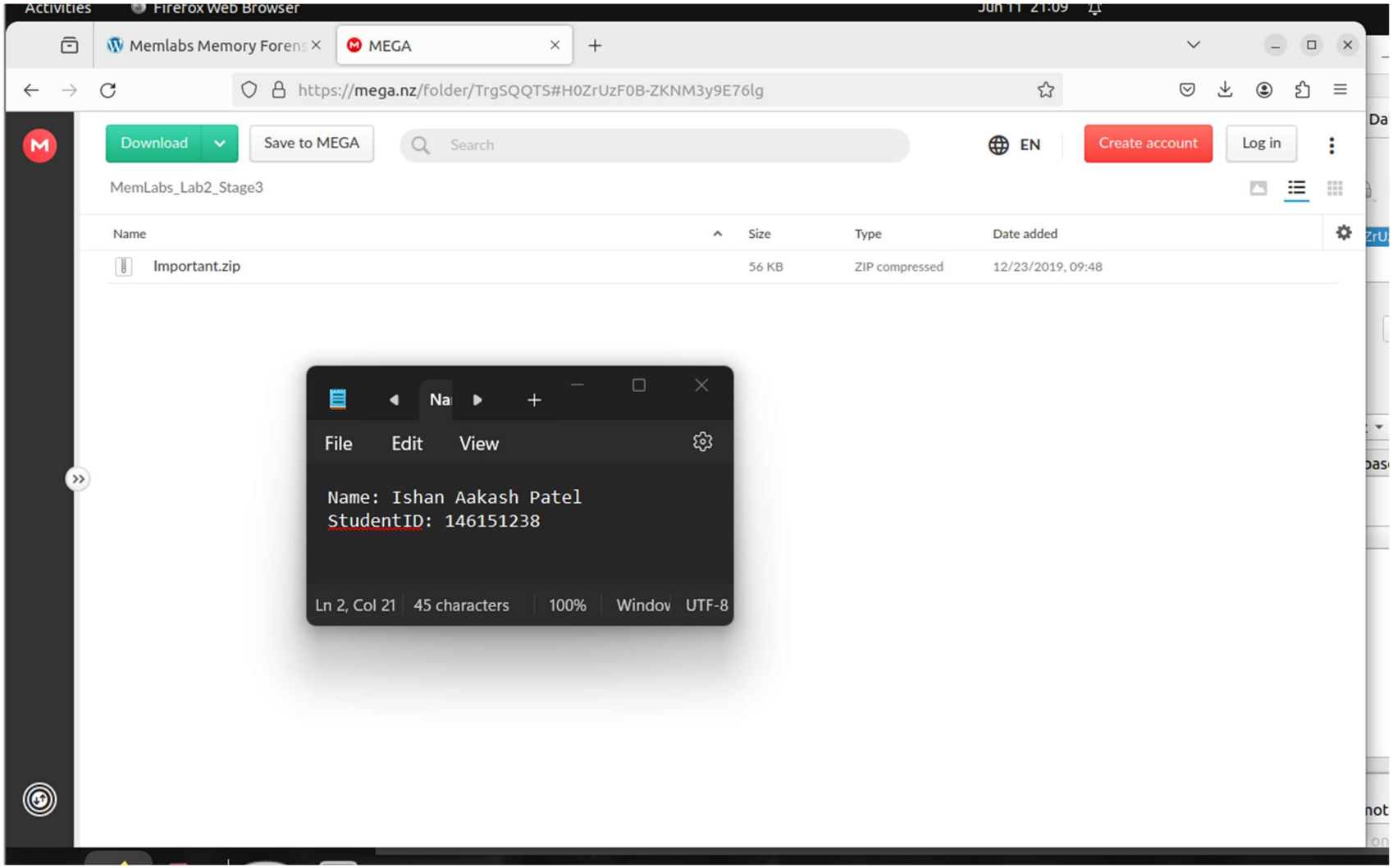
We open the History file, which is a SQLite database, using the sqlite3 command-line tool or a GUI application.

```
sqlite3 History
```



Step 4: Investigate MEGA Site

We find that the MEGA file-sharing website was visited and download a ZIP file named `MemLab_Lab2_Stage3.zip`.

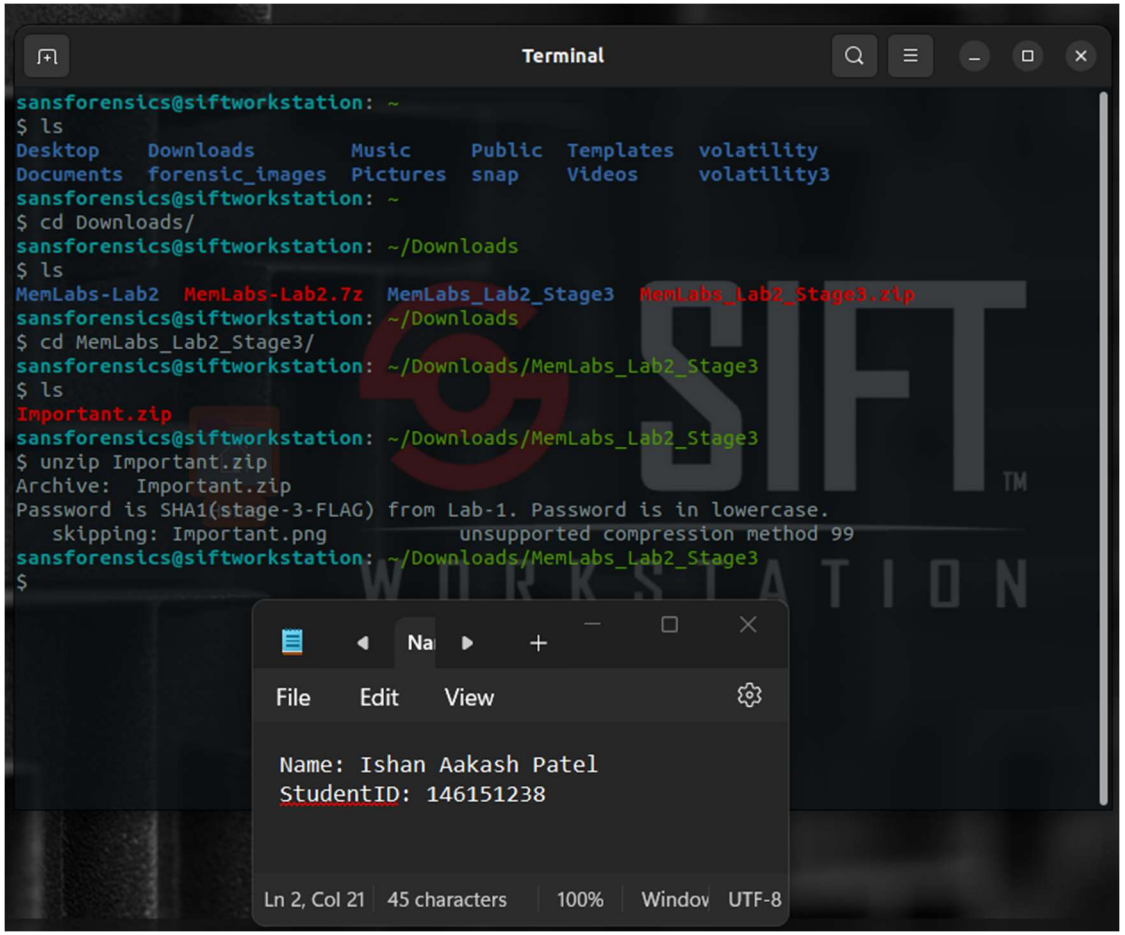


Step 5: Extract ZIP File

We use the SHA1 hash from Lab 1 as the password to extract the ZIP file using CyberChef.

Password SHA1 Hash: `6045dd90029719a039fd2d2ebcca718439dd100a`

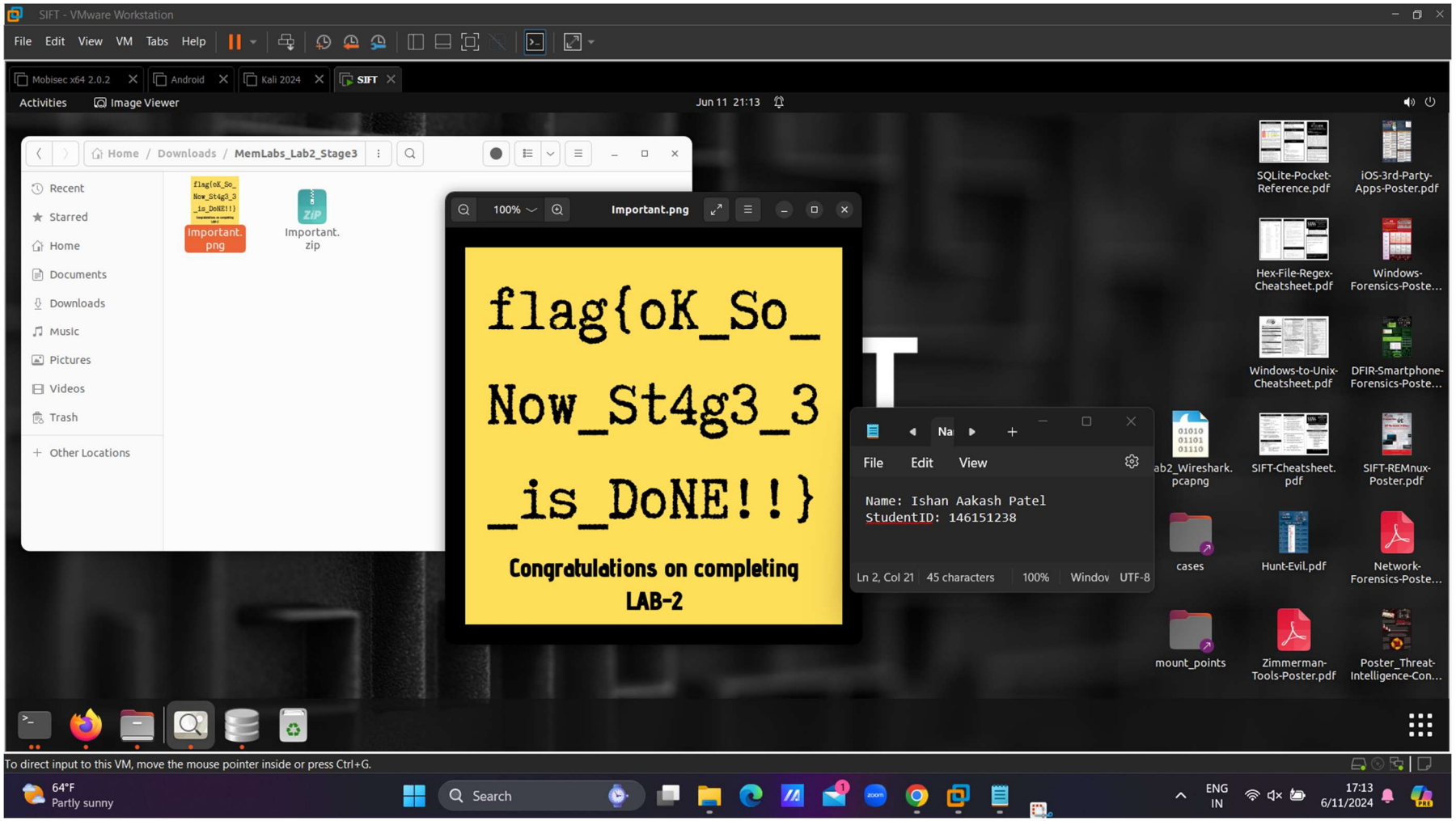
Extracted File: `Important.png`



Step 7: Retrieve Flag from Image

We open `Important.png` and find our third flag.

Flag: `flag{oK_So_Now_St4g3_3_is_DoNE!!}`



Questions and Answers

1. **What is the purpose of Volatility?** Volatility is a tool used for analyzing memory dumps to extract digital artifacts, helping in digital forensics and incident response.
2. **Why is it important to analyze memory dumps?** Analyzing memory dumps is important because it provides insights into the state of a system at a specific point in time, revealing running processes, open files, network connections, and other critical information that can aid in investigations.
3. **How difficult did you find this challenge?** I found this challenge moderately difficult. It required careful attention to detail and a good understanding of Volatility commands, but following the provided resources and write-ups made it manageable.

Learning Experience

This memory forensics challenge was a great learning experience for me. I had to use Volatility to analyze a memory dump and uncover hidden flags. Throughout the process, I learned how to use various Volatility plugins to investigate system processes, browser history, and password managers. It was interesting to see how much information can be retrieved from a memory dump and how it can be used to solve real-world problems. The challenge also helped me improve my skills in using command-line tools and understanding digital forensics concepts.