CS 4241

**CYBER FORENSICS**

LAB REPORTS

By G Shalom

BT19GCS004

Table Of Contents

|  |  |  |  |
| --- | --- | --- | --- |
| S.No | Date | Report | Page No |
| 1 | 3/8/22 | Volatility | 3 |
| 2 | 31/8/22 | Wireshark & Autopsy | 7 |
| 3 | 21/9/22 | EXIF Tool | 15 |
| 4 | 28/9/22 | BruteShark & LiveForensicator | 18 |
| 5 | 2/11/22 | WinHex | 24 |
| 6 | 9/11/22 | Browser Forensics | 27 |
| 7 | 23/11/22 | Container Forensics | 29 |

Lab Assignment 1

**1. Student Name:** G Shalom Shreyan

**2. Student Email ID:** gshalom.shreyan19@st.niituniversity.in

**3. Program/Experiment Number:** 1

**4. Title of the Program/Experiment:** Memory Forensics

**5. Date Program/Experiment Performed:** 10/08/2022

**6. Date Report Submitted:** 30/11/2022

**7. Objective:** To analyze memory dump files using volatility tool

**8. Description:**

1. **Overview**

We have to analyze memory dump files to do memory forensics using volatility tool.

1. **System Requirement: (Software and Hardware)**
   * Python version 2.6 or later
   * A Windows, Linux, or Mac OS X machine
   * Distorm3 for analysis of 64-bit Windows

* Git
* Volatility tool
* DumpIt tool

1. **Configuration of the System used by you to perform the experiment/installation**

AMD Ryzen 7 6800H with Radeon Graphics 3.20 GHz

16.0 GB (15.2 GB usable)

64-bit operating system, x64-based processor

Windows 11 Home Single Language 22621.819

NVIDIA GeForce RTX 3060 Laptop GPU

1. **Algorithm (Step by Step Approach)**

No algorithms were used

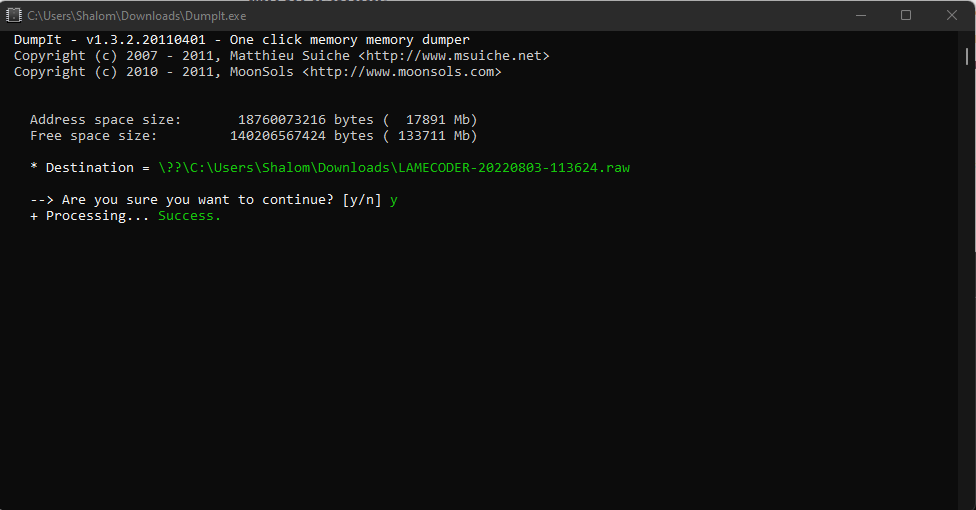
**9. Implementation Details:**

1. **In case of programming implementation: Please add source code**

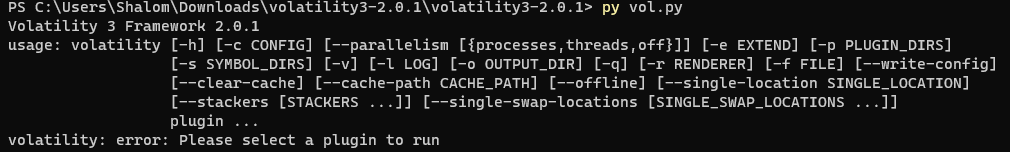
No programming was done.

1. **In case of software installation: Please add screenshots. (Step by Step)**

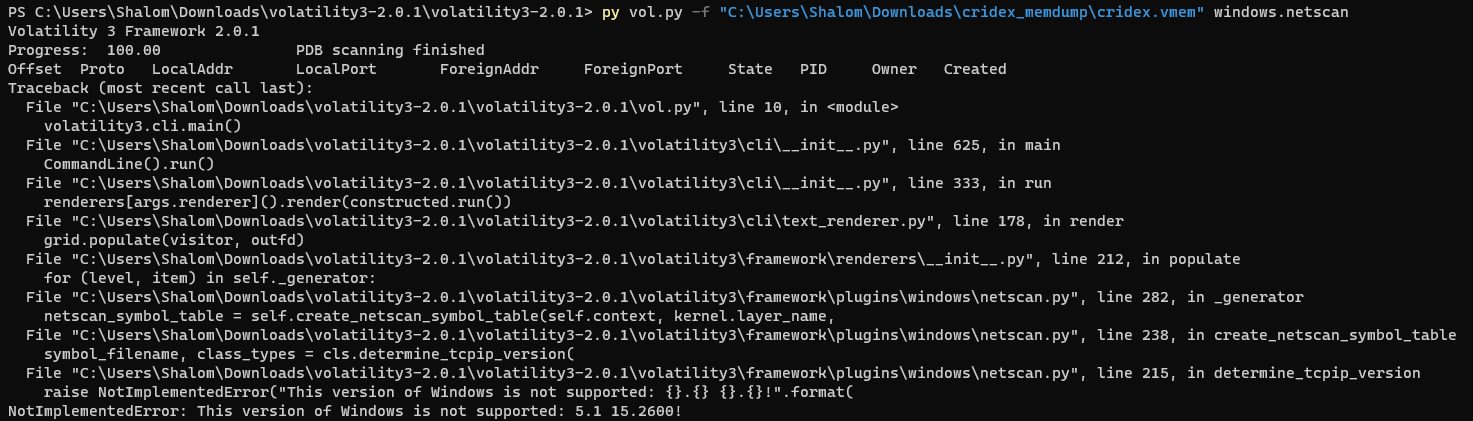
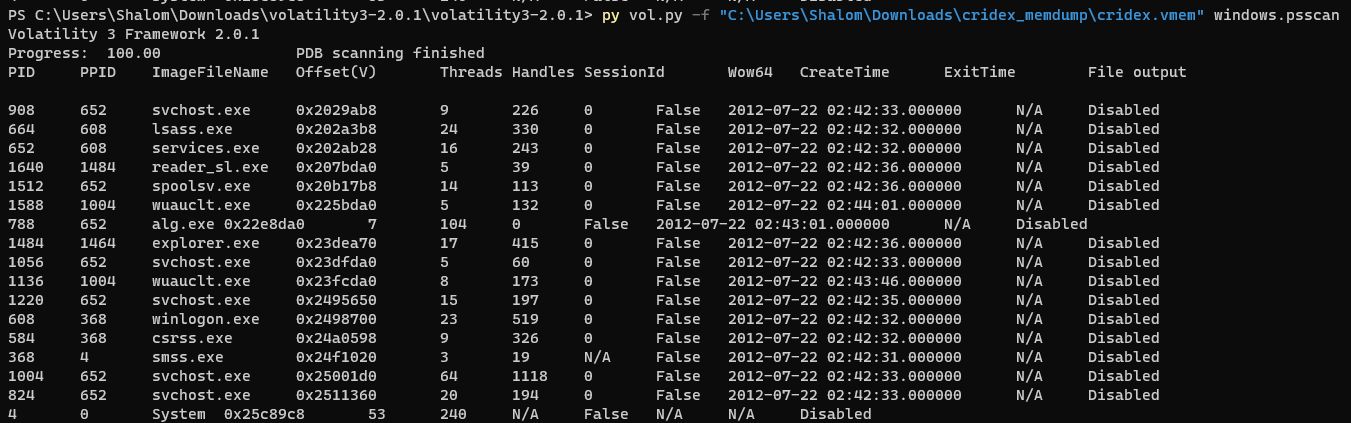
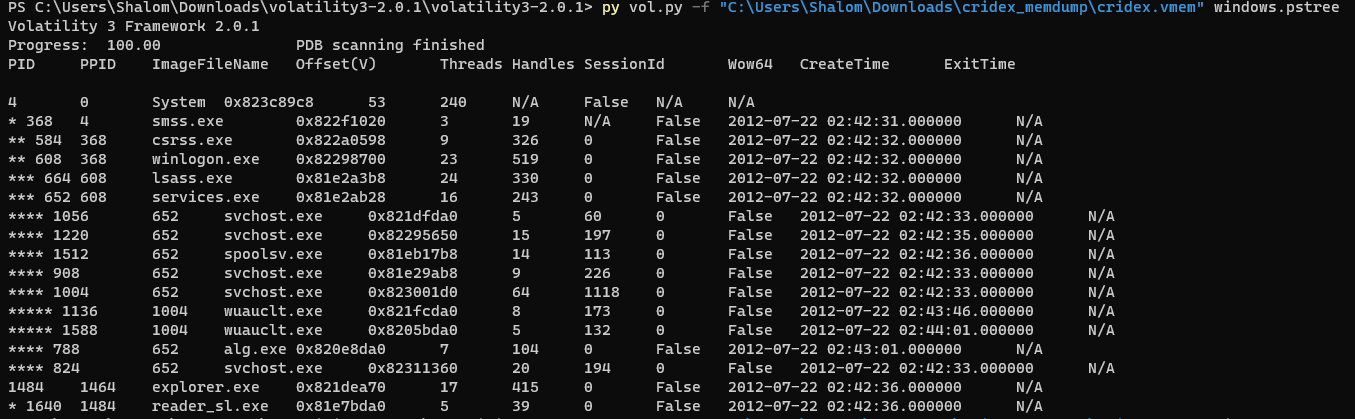
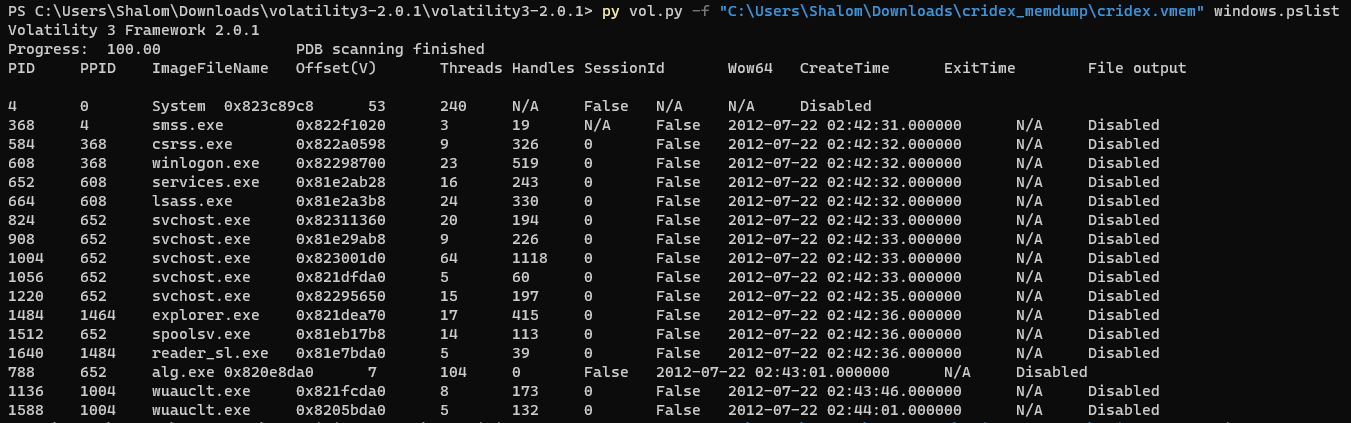
DumpIt tool (from <https://github.com/thimbleweed/All-In-USB/tree/master/utilities/DumpIt)> was downloaded to create a raw memory dump. The tool was run and a physical memory dump of the Windows machine was generated.



Volatility tool (https://github.com/volatilityfoundation/volatility3) was downloaded . Run vol.py to check if it is working fine or not.

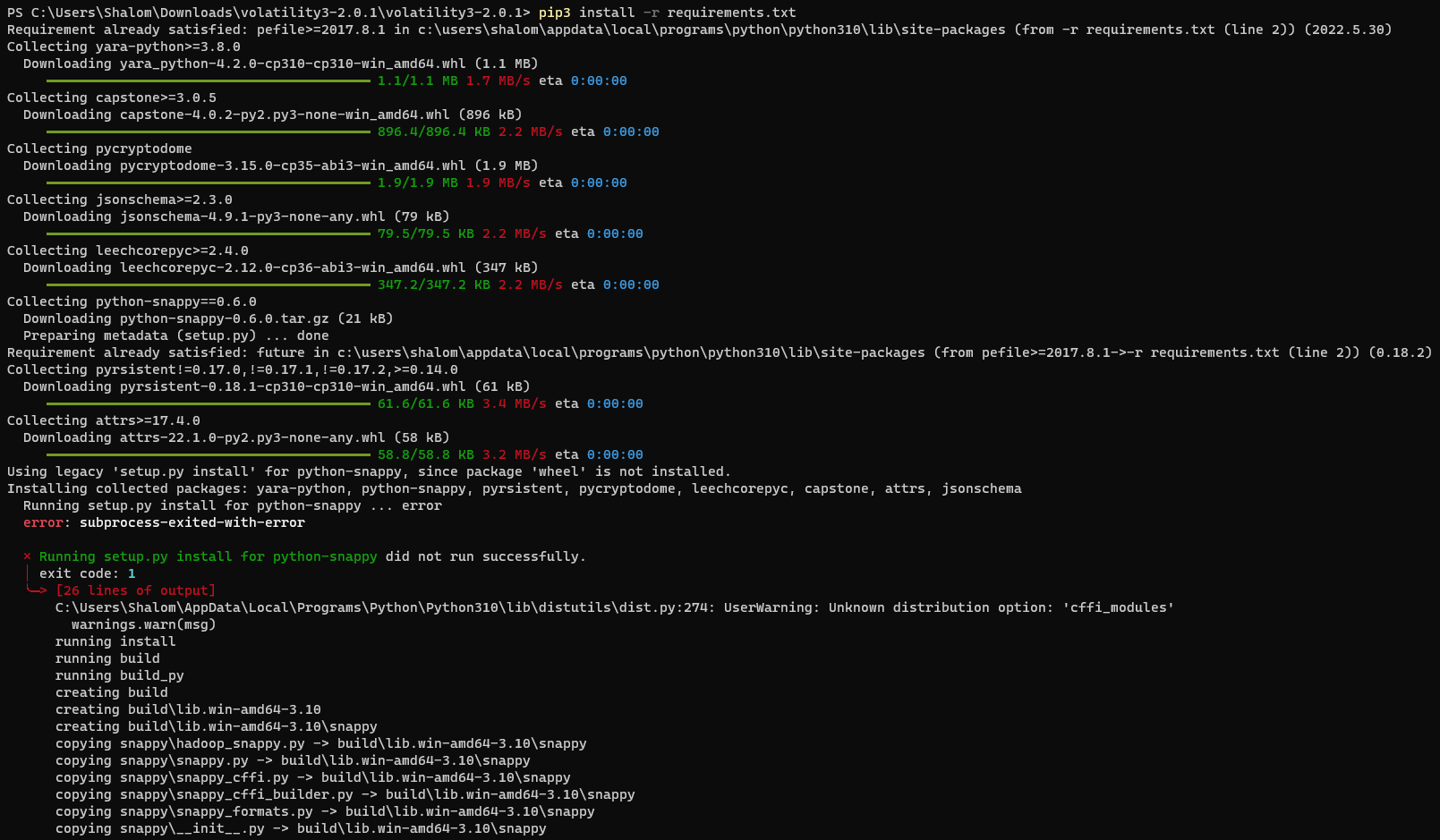


Run various commands to gain intel.

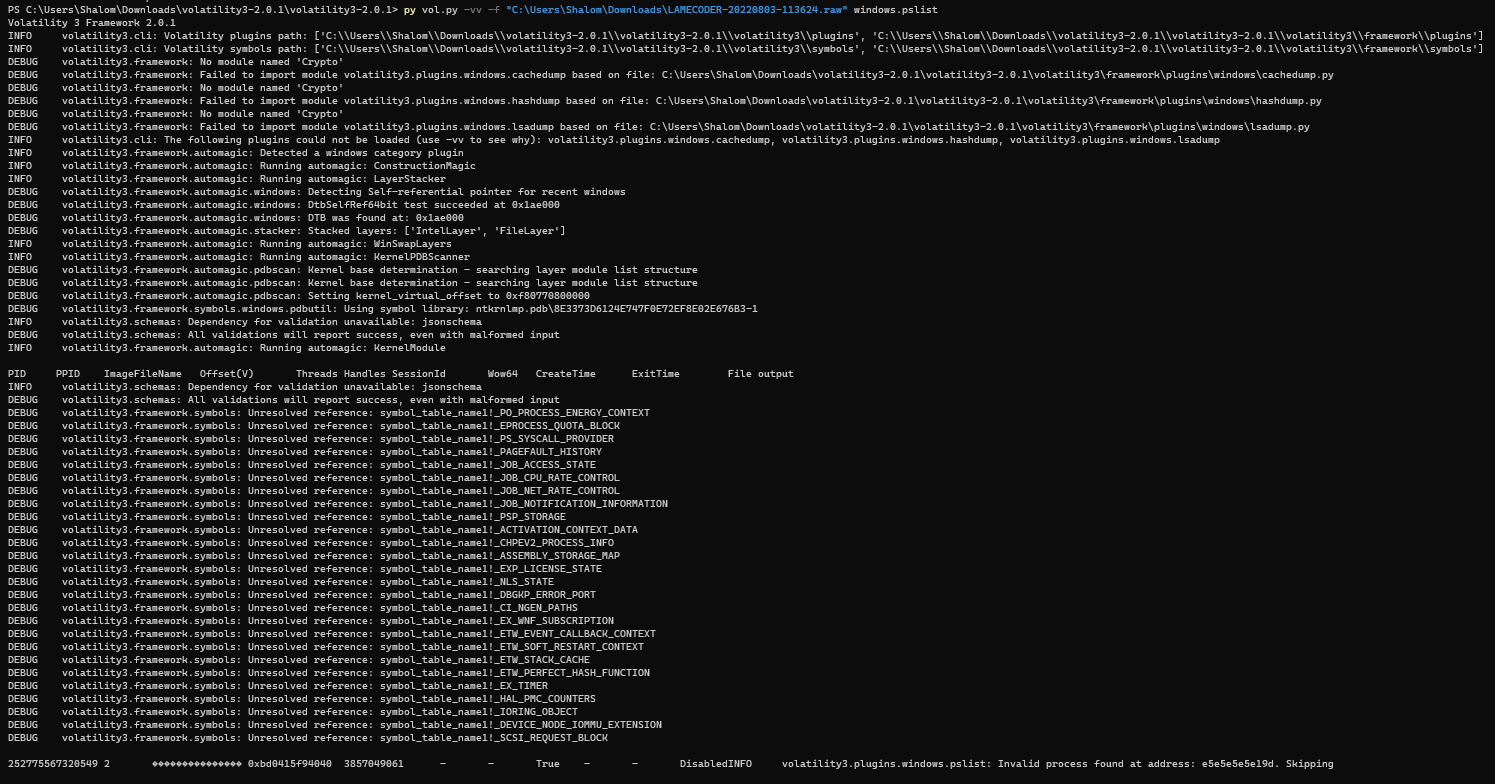


**10. Error Description:**

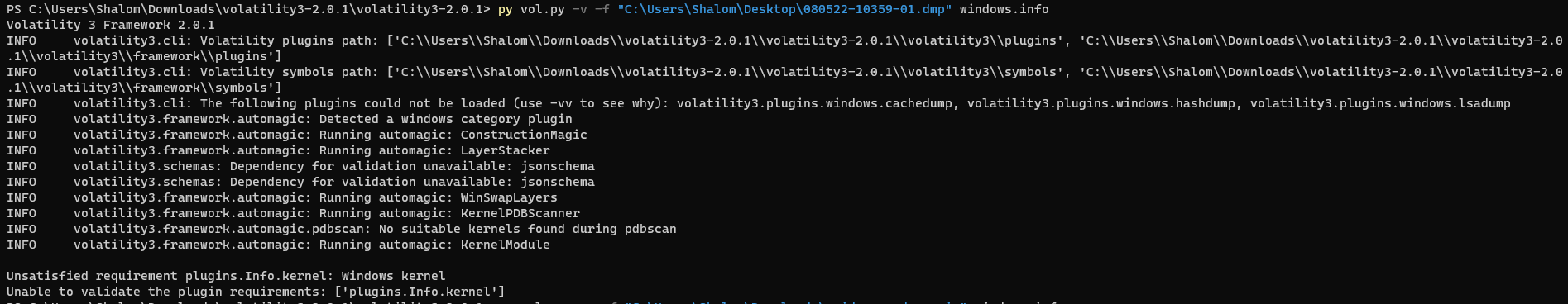
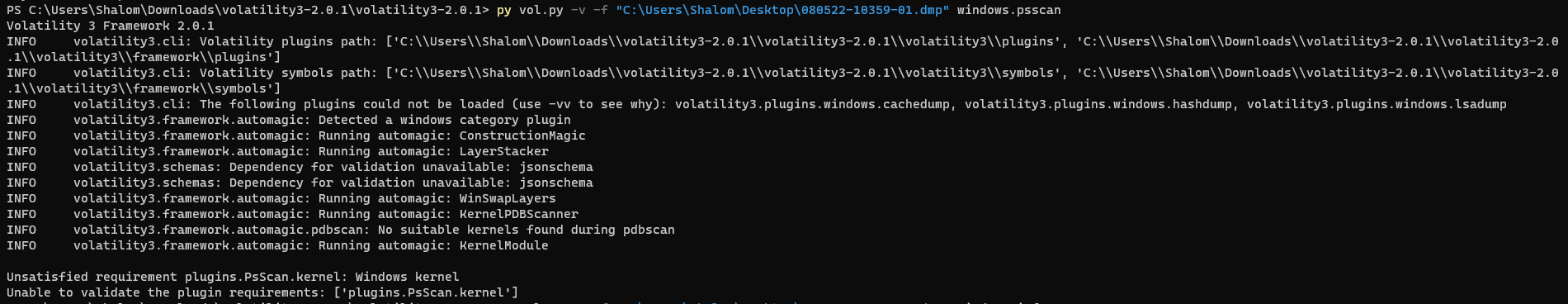
1. Getting all required libraries wasn’t possible due to errors in installing snappy library. Also found a link for possible fix (https://stackoverflow.com/questions/42979544/how-to-install-snappy-c-libraries-on-windows-10-for-use-with-python-snappy-in-an) but it resulted in another error, which wasn’t fixable.



1. Invalid process detected in the memory dump created of Windows 11, possible system issue as Windows XP dump ran fine.



1. Windows Kernel error when tried to analyze memory dumps created automatically by WindowsTried getting a profile but was not able to detect kernel



**11. Conclusion:** Memory analysis has been successfully done

**12. Reference:**

<https://github.com/volatilityfoundation/volatility/wiki/Memory-Samples>

<https://neoslab.com/2020/04/28/how-to-extract-data-from-windows-memory-dump-using-volatility-cUNHMlhCTmxtTGdENEhRek1NWTlOdz09>

<https://blog.cyberhacktics.com/memory-forensics-on-windows-10-with-volatility/>

<https://github.com/volatilityfoundation/volatility3>

<https://infosecwriteups.com/forensics-memory-analysis-with-volatility-6f2b9e859765>

<https://www.youtube.com/watch?v=gHbejxlPbRQ>

<https://www.hackingarticles.in/multiple-ways-to-capture-memory-for-analysis/>

Lab Assignment 2

**1. Student Name:** G Shalom Shreyan

**2. Student Email ID:** gshalom.shreyan19@st.niituniversity.in

**3. Program/Experiment Number:** 2

**4. Title of the Program/Experiment:** Wireshark & Autopsy

**5. Date Program/Experiment Performed:** 31/08/2022

**6. Date Report Submitted:** 30/11/2022

**7. Objective:** To analyze Windows & Unix file systems using Autopsy and analyze packets using Wireshark

**8. Description:**

1. **Overview**

We have to analyze Linux file system using Autopsy tool.

1. **System Requirement: (Software and Hardware)**
   * 64-bit AMD64/x86-64 or 32-bit x86 CPU architecture.
   * At least 500 MB available RAM
   * At least 500 MB of available disk space
   * It requires a minimum resolution of 1280 × 1024 or higher.
   * A Windows, Linux, or Mac OS X machine

* Wireshark tool
* Autopsy tool

1. **Configuration of the System used by you to perform the experiment/installation**

AMD Ryzen 7 6800H with Radeon Graphics 3.20 GHz

16.0 GB (15.2 GB usable)

64-bit operating system, x64-based processor

Windows 11 Home Single Language 22621.819

NVIDIA GeForce RTX 3060 Laptop GPU

1. **Algorithm (Step by Step Approach)**

No algorithms were used

**9. Implementation Details:**

1. **In case of programming implementation: Please add source code**

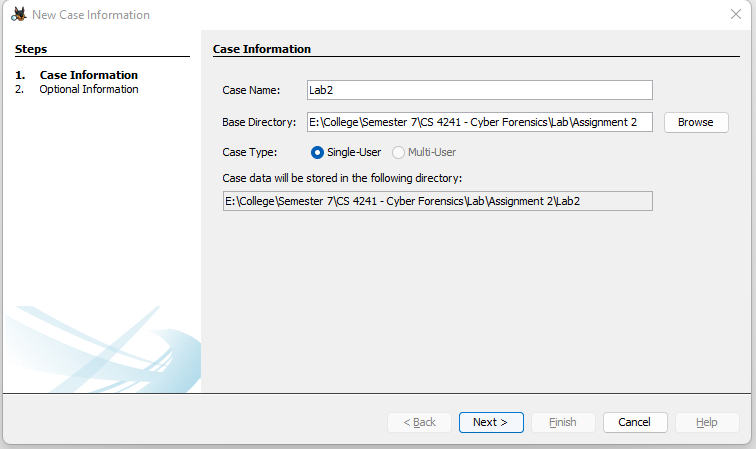
No programming was done.

1. **In case of software installation: Please add screenshots. (Step by Step)**

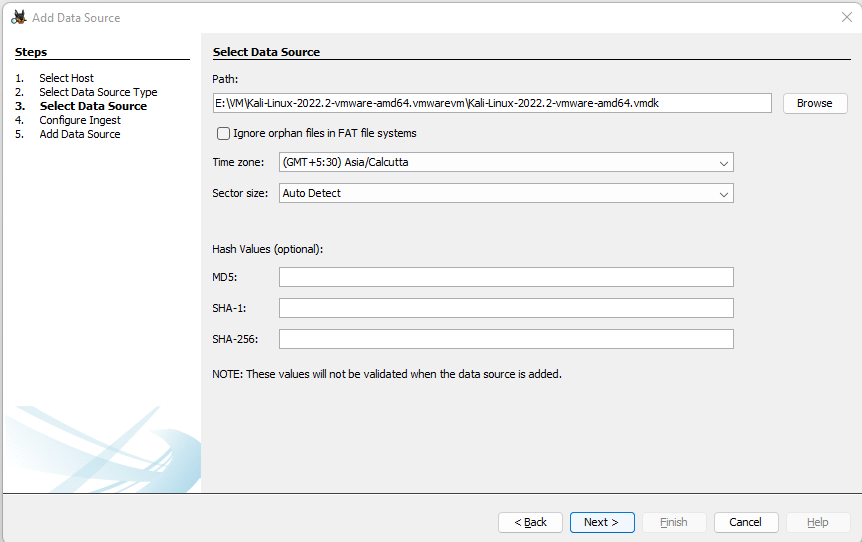
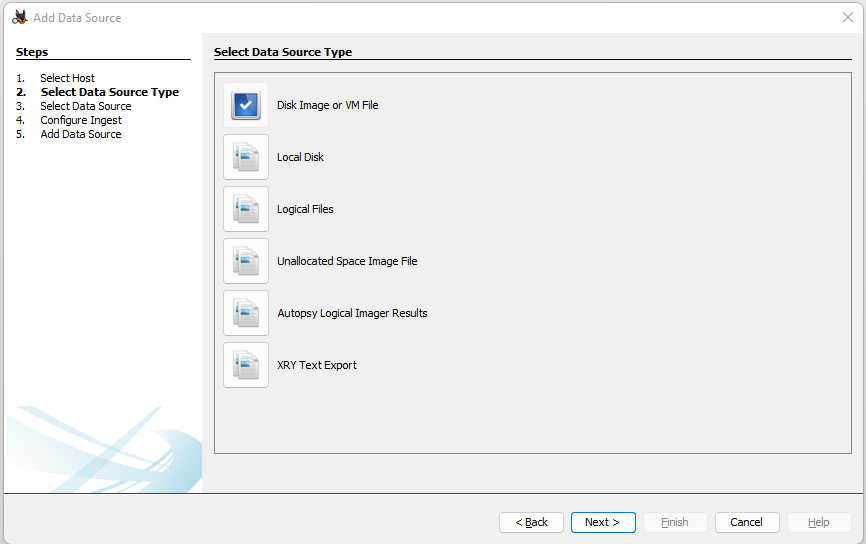
Autopsy tool was downloaded from <https://www.autopsy.com/download/.> Opening the application shows the below screen.



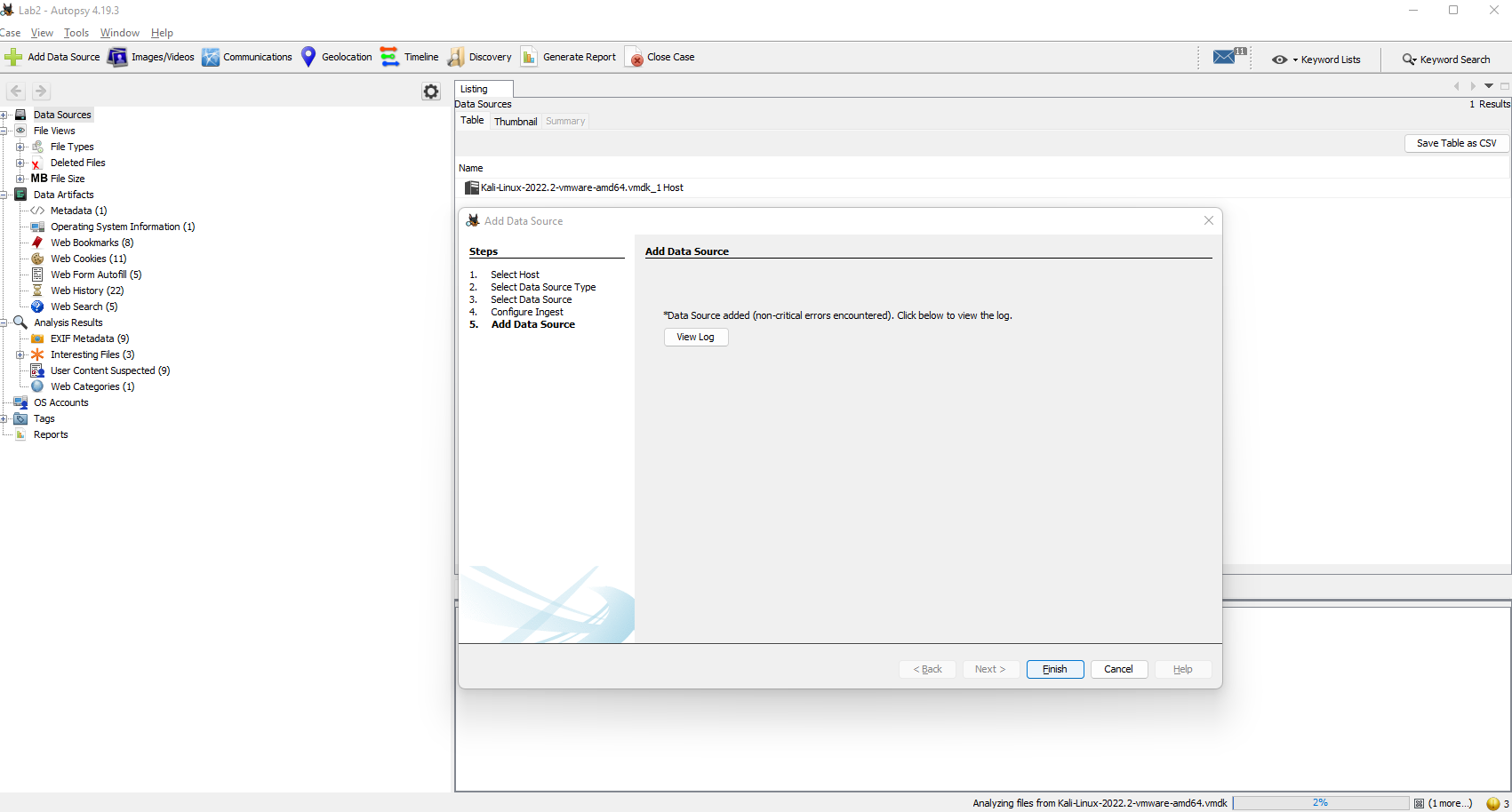
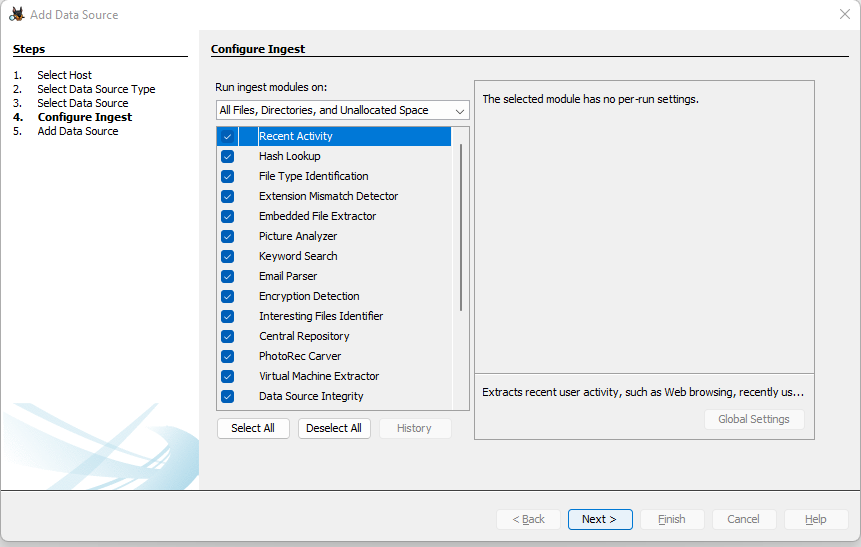
A new case is created and relevant details are entered



A Kali-Linux VM image will be chosen as a data source

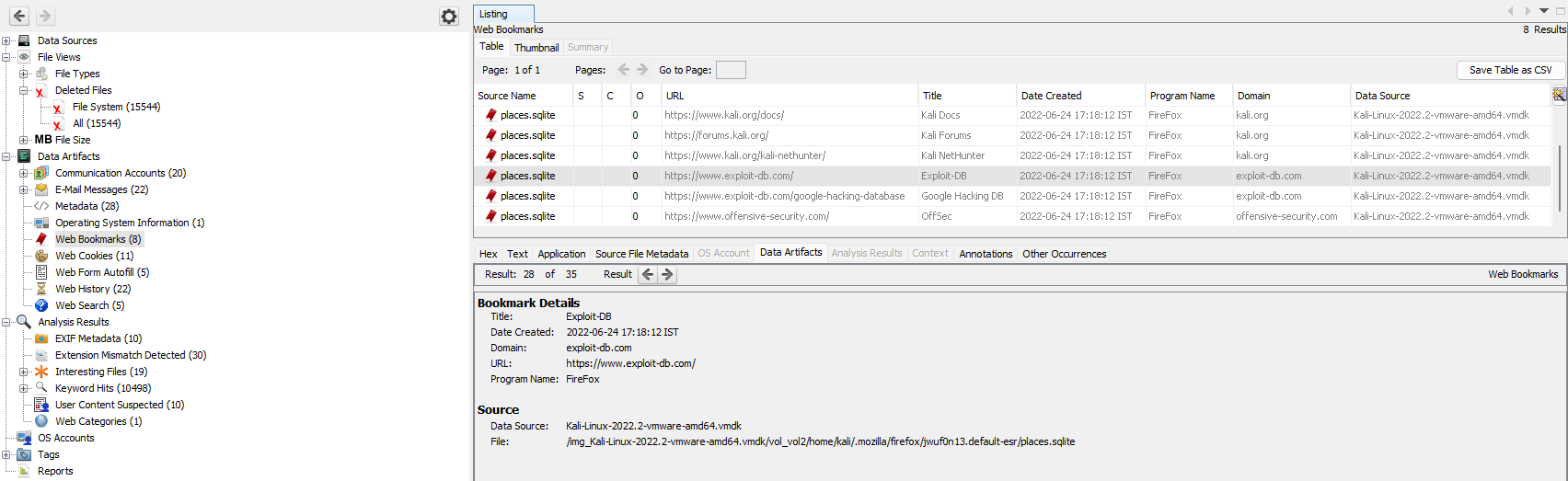


Configure to ingest to include everything to get all information

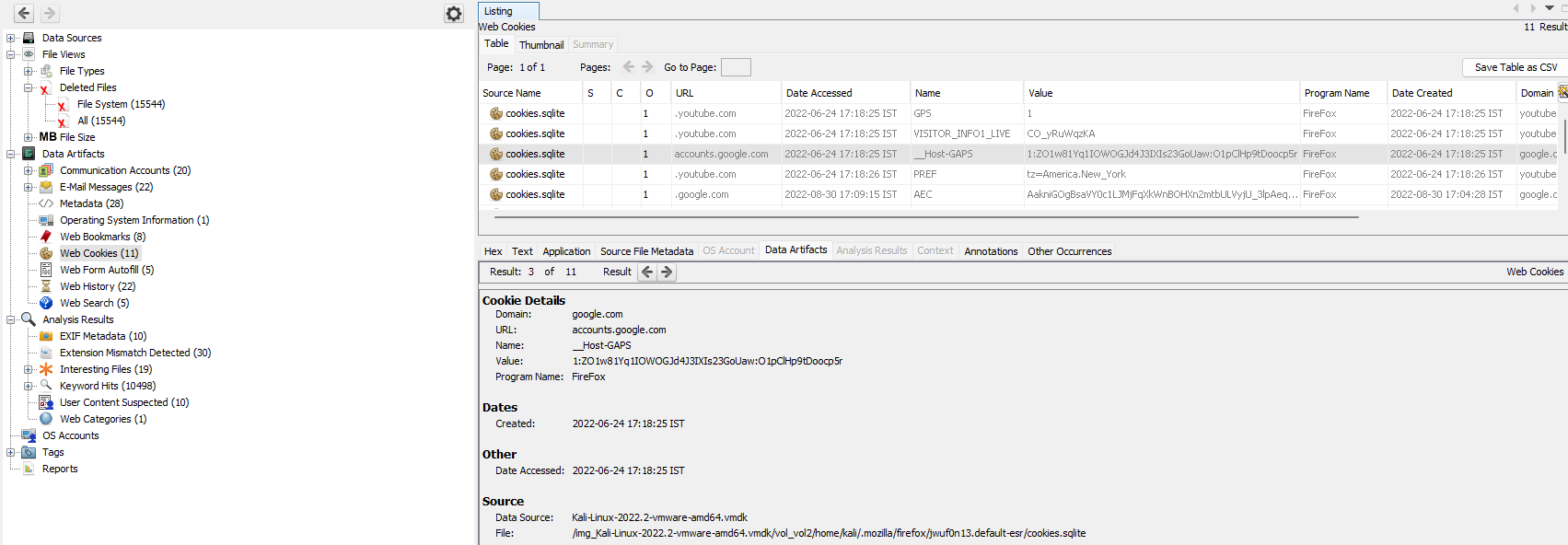


Now we can see the dashboard and all the important information

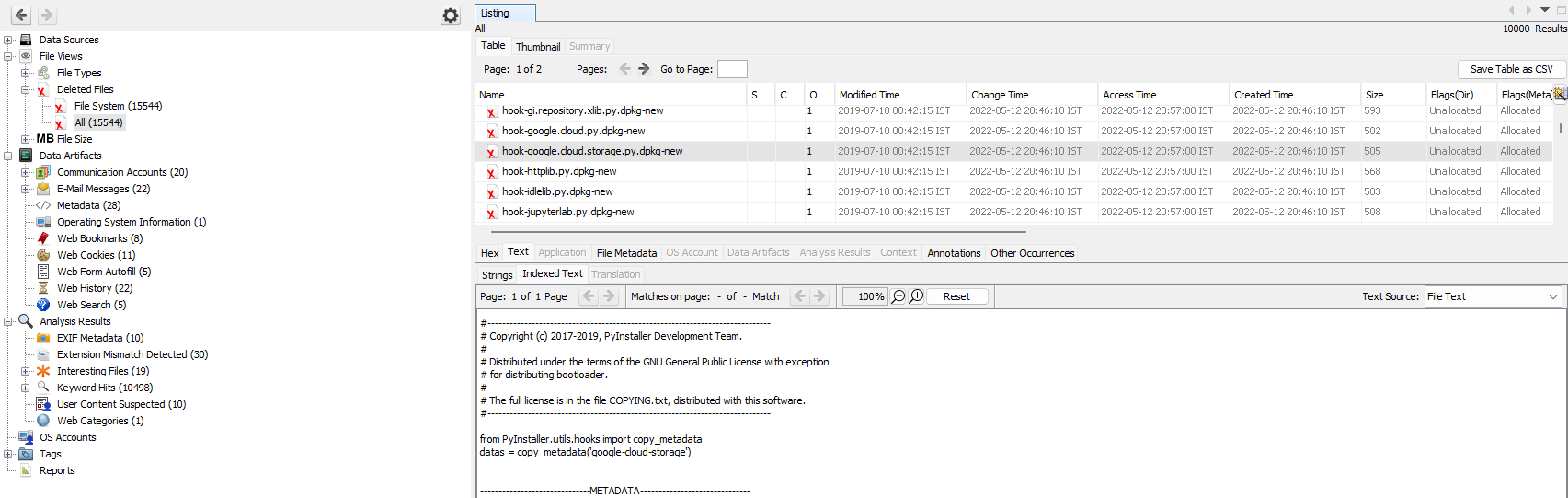
Bookmarks



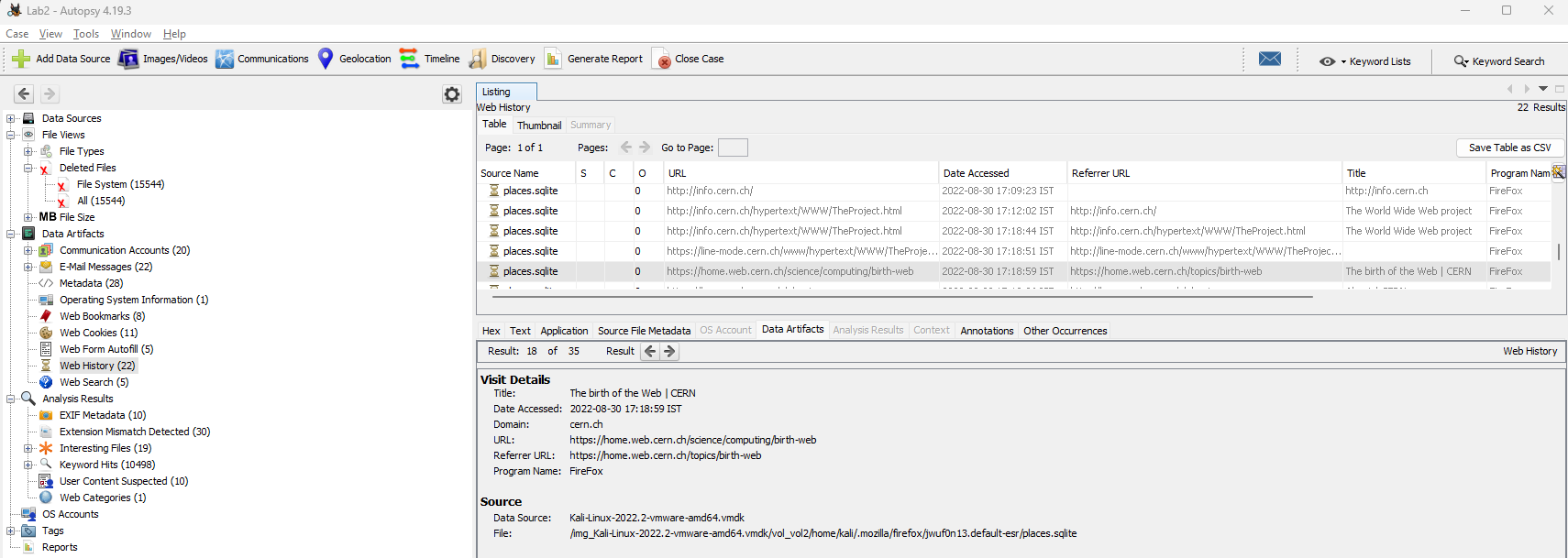
Cookies



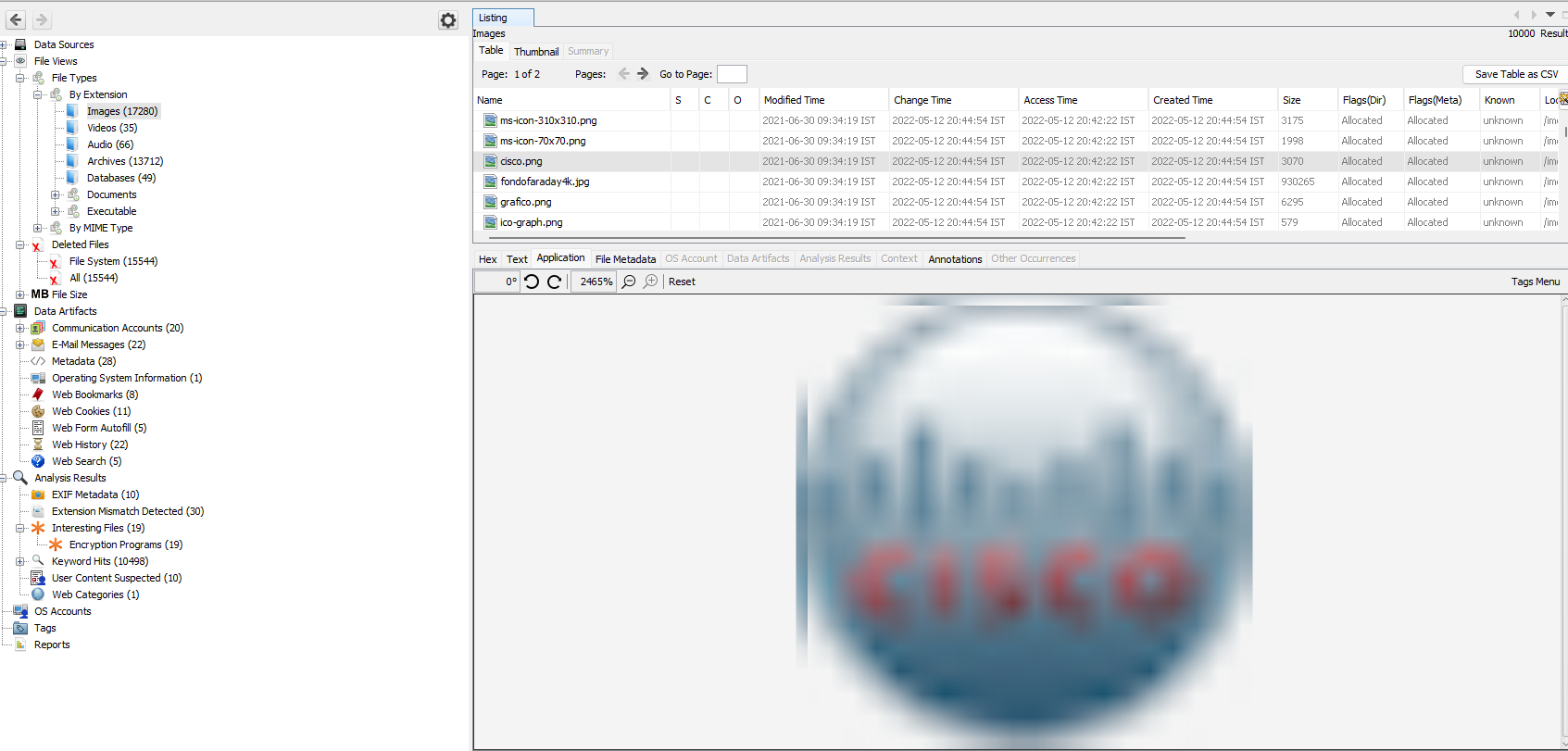
Deleted Files



Web History



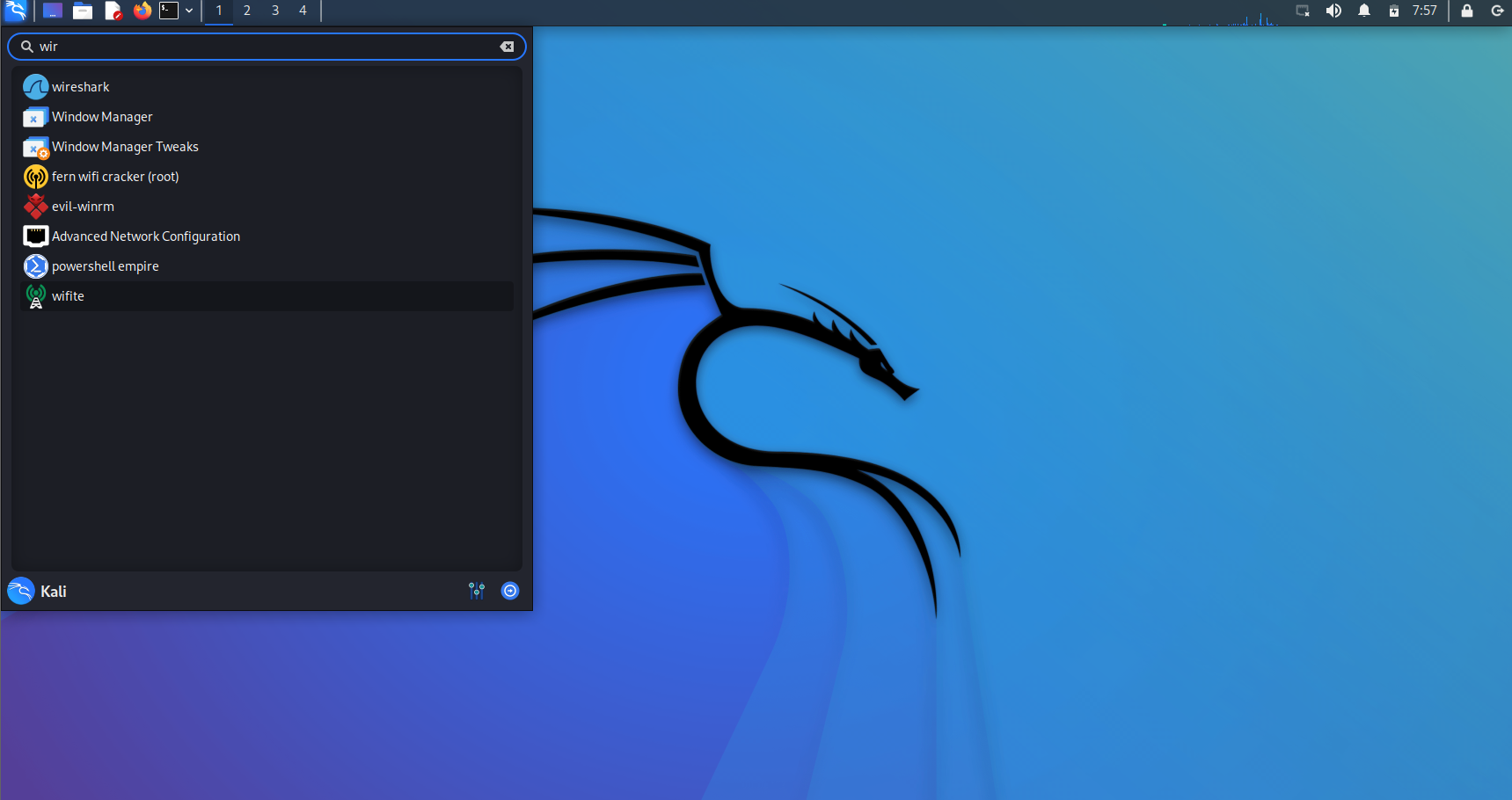
Images



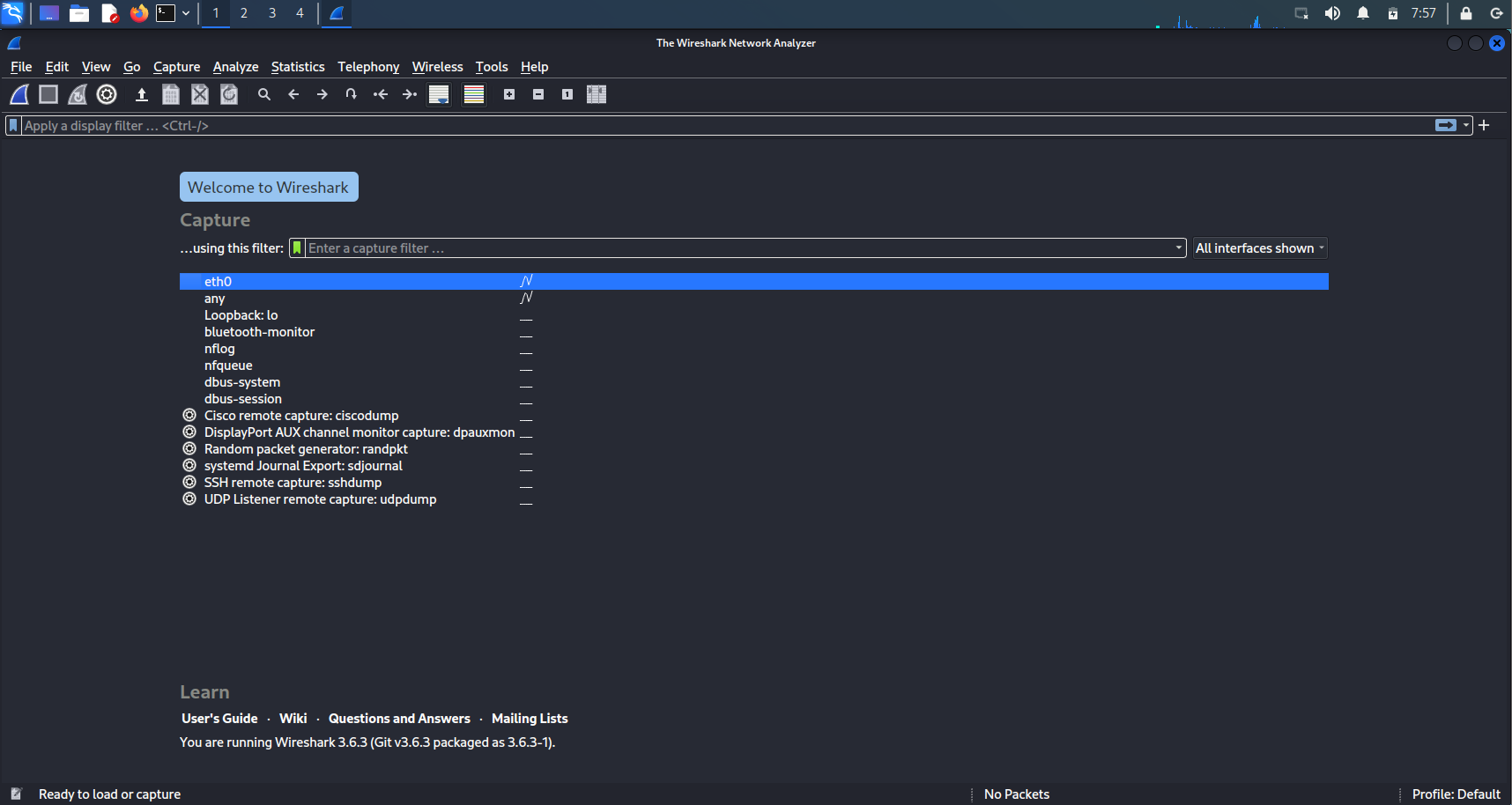
Data Files



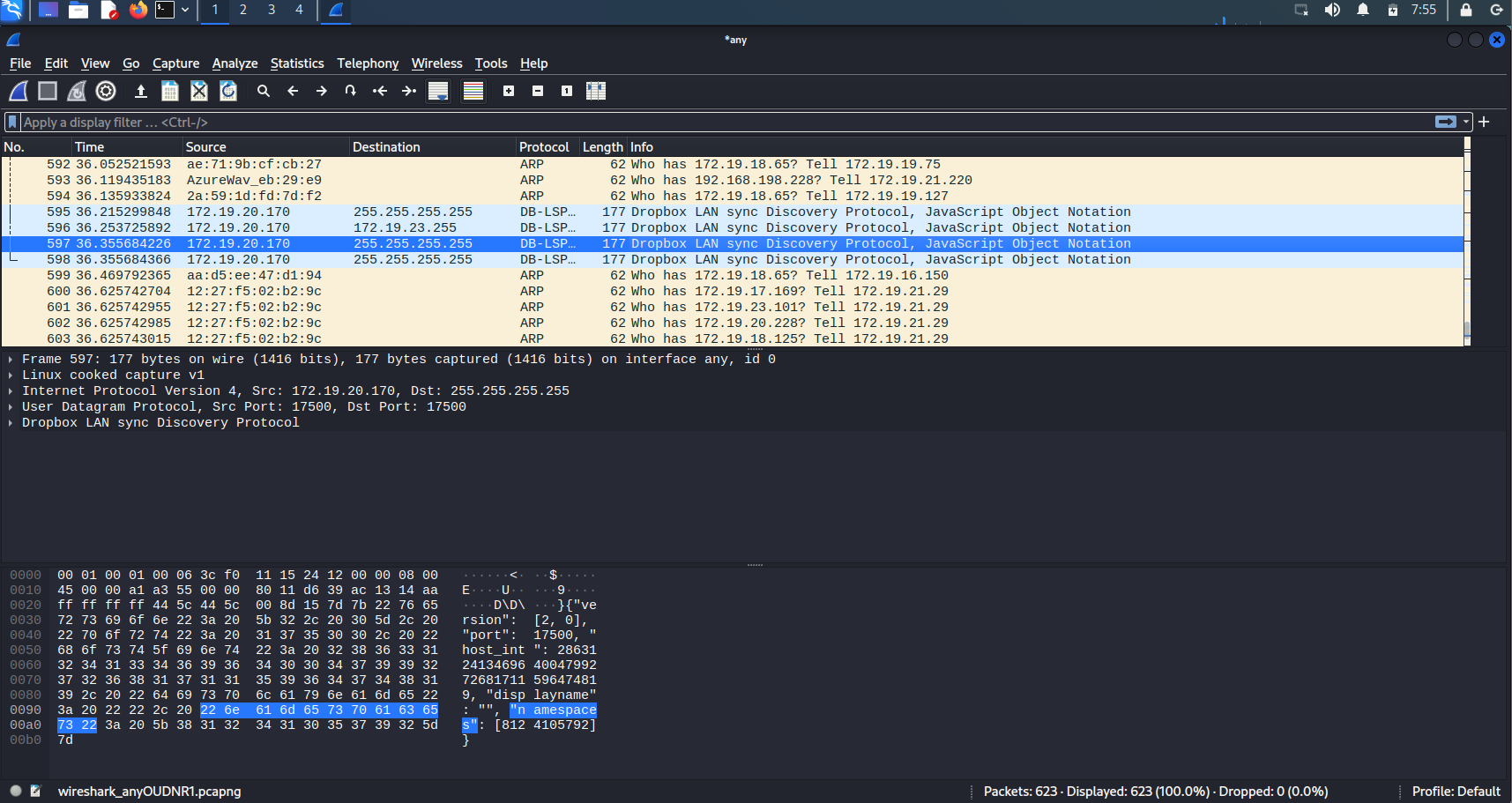
Now, moving on to Wireshark



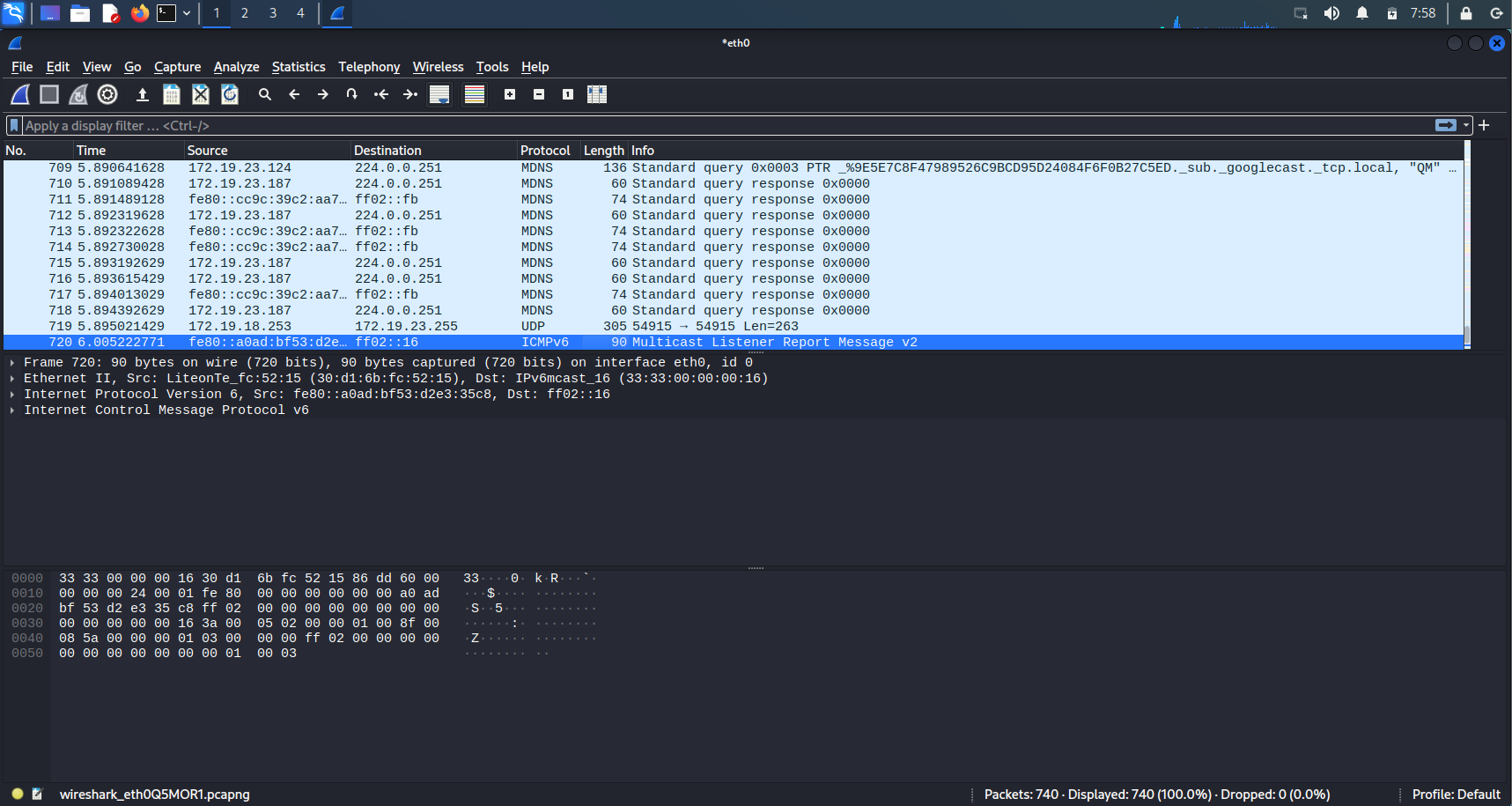
Opening wireshark greets us with this dashboard



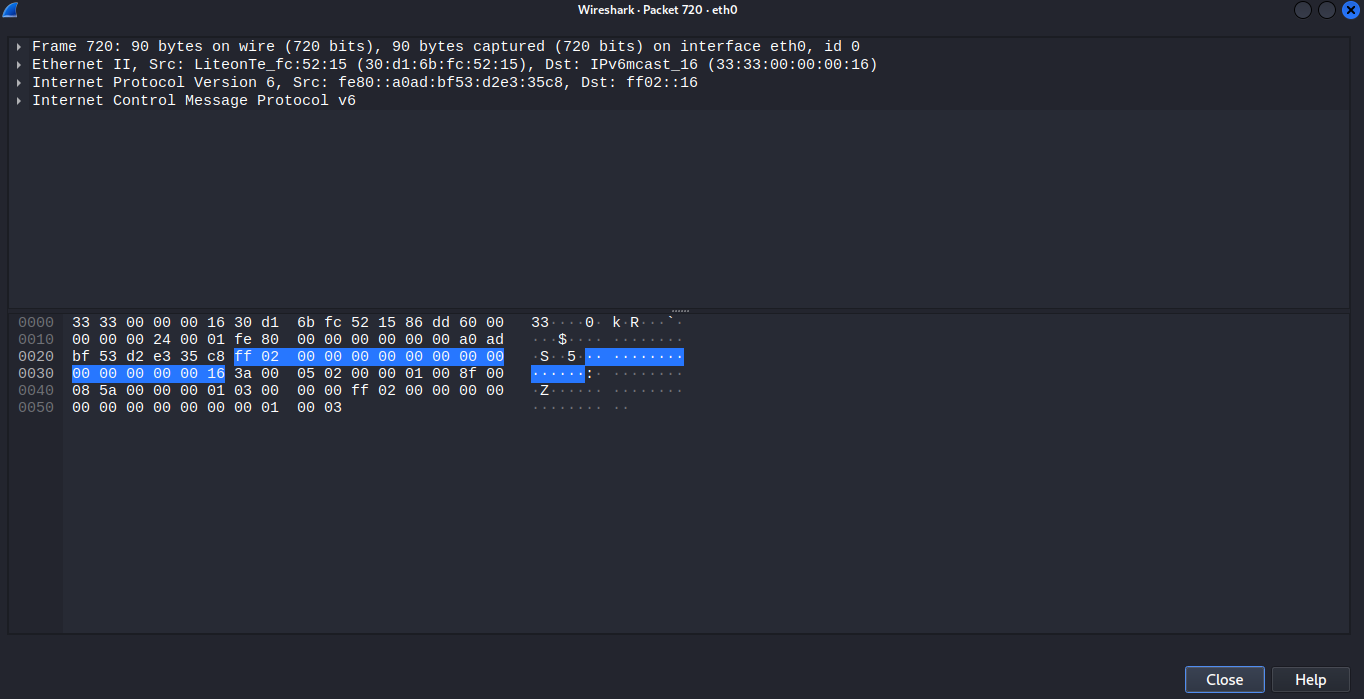
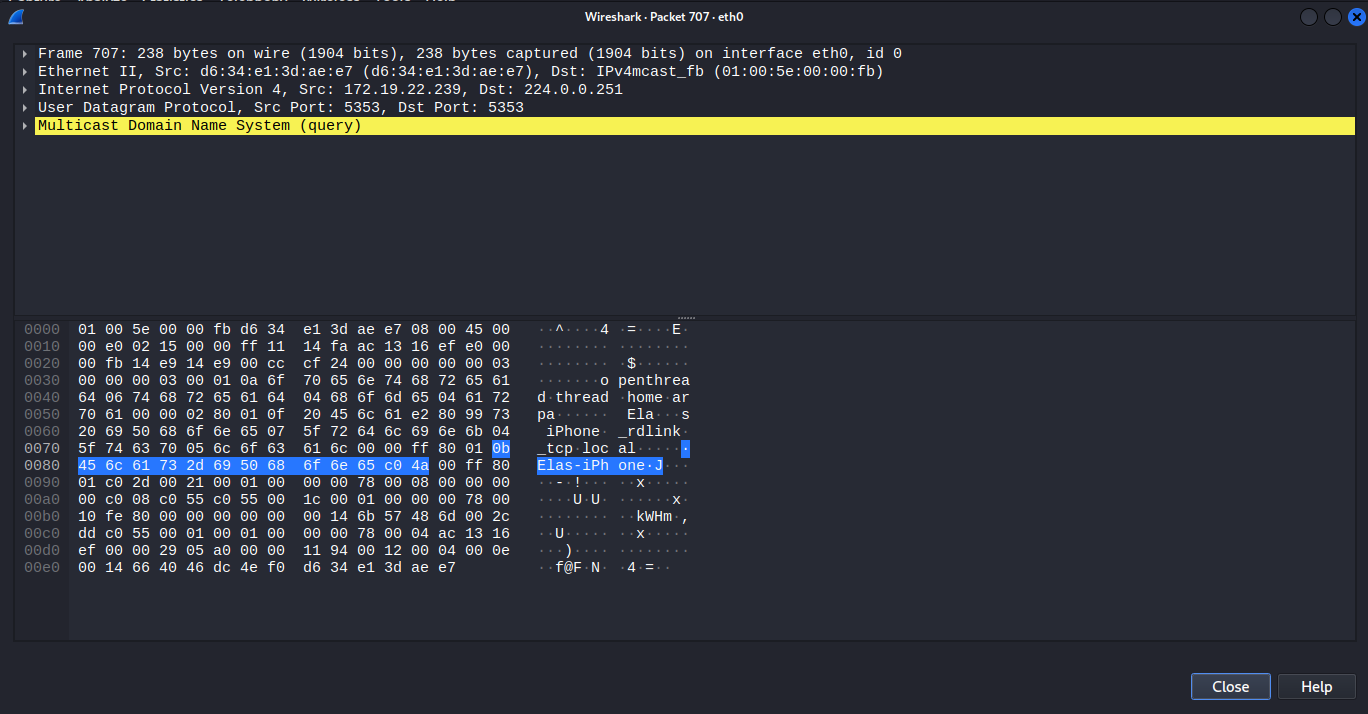
Starting capture of data packets lets us see the data packets travelling and their details



Selecting a data packet lets you know its contents



Double clicking on it gives a more detailed view about it



**10. Error Description:**

No errors were faced

**11. Conclusion:** Disk forensics has been successfully completed and analysis of data packets has been done using Wireshark

**12. Reference:**

<https://www.autopsy.com/download/>

<https://www.wireshark.org/>

Lab Assignment 3

**1. Student Name:** G Shalom Shreyan

**2. Student Email ID:** gshalom.shreyan19@st.niituniversity.in

**3. Program/Experiment Number:** 3

**4. Title of the Program/Experiment:** EXIF Tool

**5. Date Program/Experiment Performed:** 21/09/2022

**6. Date Report Submitted:** 30/11/2022

**7. Objective:** To read metadata of files using EXIFTool

**8. Description:**

1. **Overview**

We have to read, write, and manipulate image, audio, video, and PDF metadata.

1. **System Requirement: (Software and Hardware)**
   * Perl 5.004 or later
   * At least 500 MB available RAM
   * At least 500 MB of available disk space
   * A Windows, Linux, or Mac OS X machine

* EXIF tool

1. **Configuration of the System used by you to perform the experiment/installation**

AMD Ryzen 7 6800H with Radeon Graphics 3.20 GHz

16.0 GB (15.2 GB usable)

64-bit operating system, x64-based processor

Windows 11 Home Single Language 22621.819

NVIDIA GeForce RTX 3060 Laptop GPU

1. **Algorithm (Step by Step Approach)**

No algorithms were used

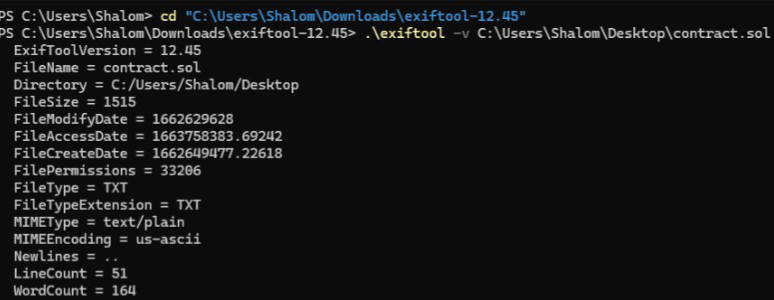
**9. Implementation Details:**

1. **In case of programming implementation: Please add source code**

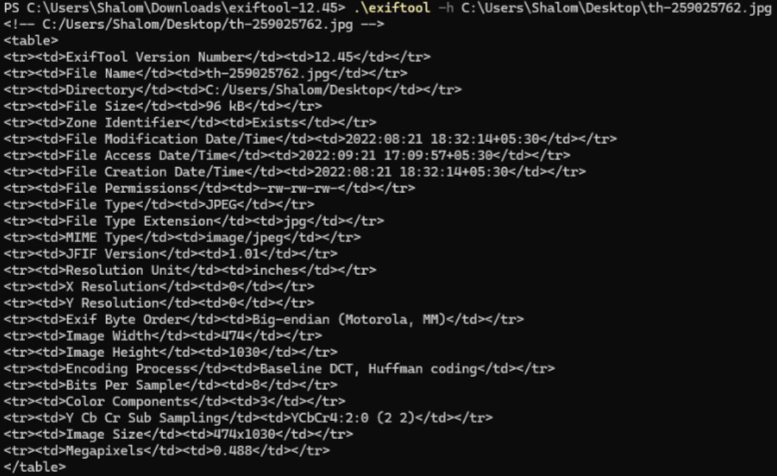
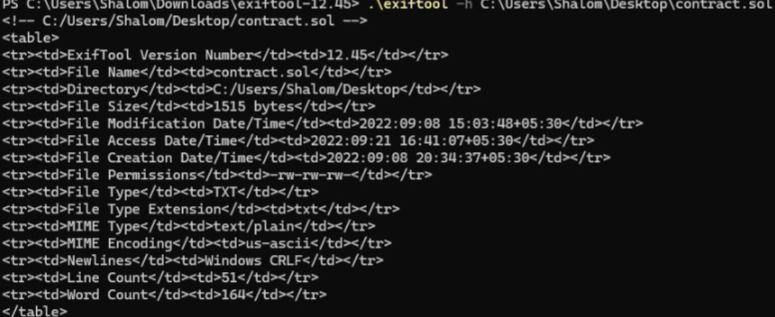
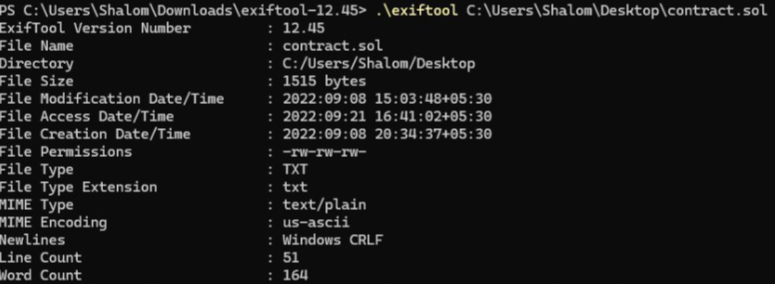
No programming was done.

1. **In case of software installation: Please add screenshots. (Step by Step)**

Download EXIFTool from <https://exiftool.org/index.html#running.> After succesful download, Run the tool using terminal after extracting and removing (-k) from the .exe tool

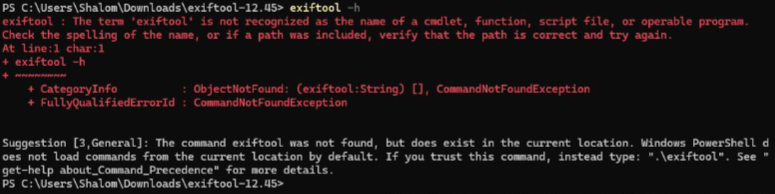


Different commands can be used to get more and different metadata about various files



**10. Error Description:**

Had to use .\exiftool instead of exiftool



**11. Conclusion:** Metadata about various files has been successfully observed using EXIFTool

**12. Reference:**

<https://www.exiftool.org/dummies.html>

<https://twistandclick.com/2022/02/03/using-exiftool-a-beginners-guide/>

Lab Assignment 4

**1. Student Name:** G Shalom Shreyan

**2. Student Email ID:** gshalom.shreyan19@st.niituniversity.in

**3. Program/Experiment Number:** 4

**4. Title of the Program/Experiment:** BruteShark & LiveForensicator

**5. Date Program/Experiment Performed:** 28/09/2022

**6. Date Report Submitted:** 30/11/2022

**7. Objective:** To analyze network traffic using BruteShark & gather system information using LiveForensicator

**8. Description:**

1. **Overview**

We have to perform network traffic analysis to identify weaknesses using BruteShark. We also need to gather different system information for further review for anomalous behaviour or unexpected data entryusing Live Forensicator.

1. **System Requirement: (Software and Hardware)**
   * Npcap driver/libpcap driver
   * At least 500 MB available RAM
   * At least 500 MB of available disk space
   * A Windows, Linux, or Mac OS X machine

* BruteSharkCLI tool
* Live Forensicator tool

1. **Configuration of the System used by you to perform the experiment/installation**

AMD Ryzen 7 6800H with Radeon Graphics 3.20 GHz

16.0 GB (15.2 GB usable)

64-bit operating system, x64-based processor

Windows 11 Home Single Language 22621.819

NVIDIA GeForce RTX 3060 Laptop GPU

1. **Algorithm (Step by Step Approach)**

No algorithms were used

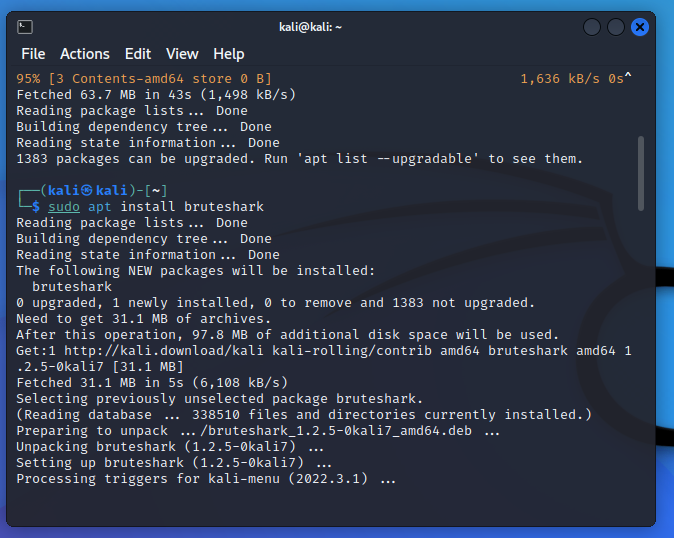
**9. Implementation Details:**

1. **In case of programming implementation: Please add source code**

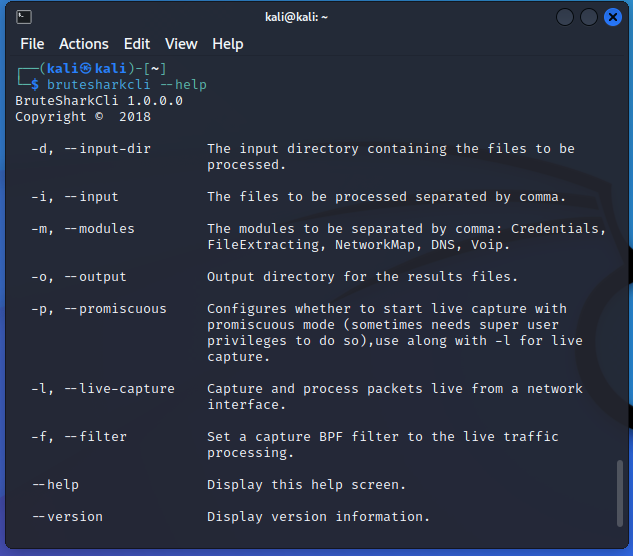
No programming was done.

1. **In case of software installation: Please add screenshots. (Step by Step)**

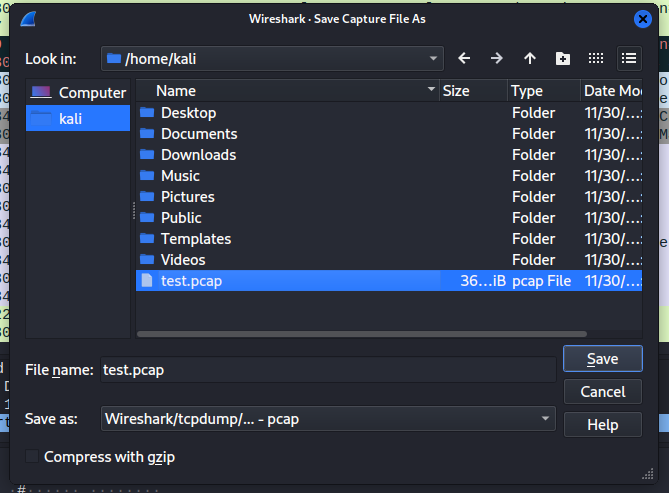
Install Bruteshark in a Linux Machine



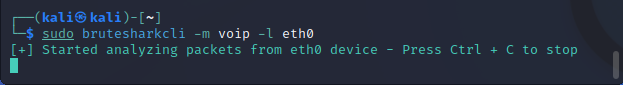
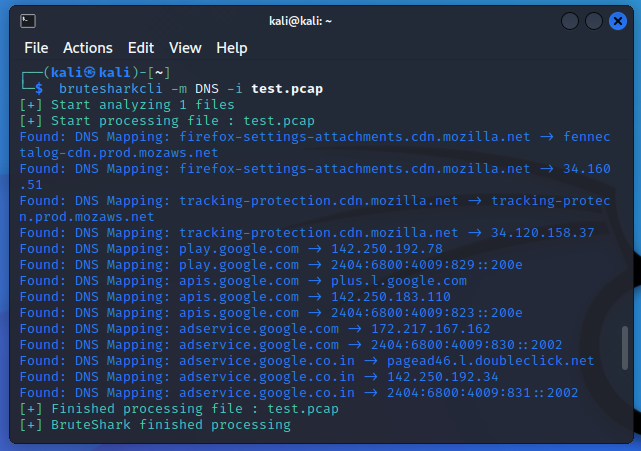
Use the help function to see how to use it



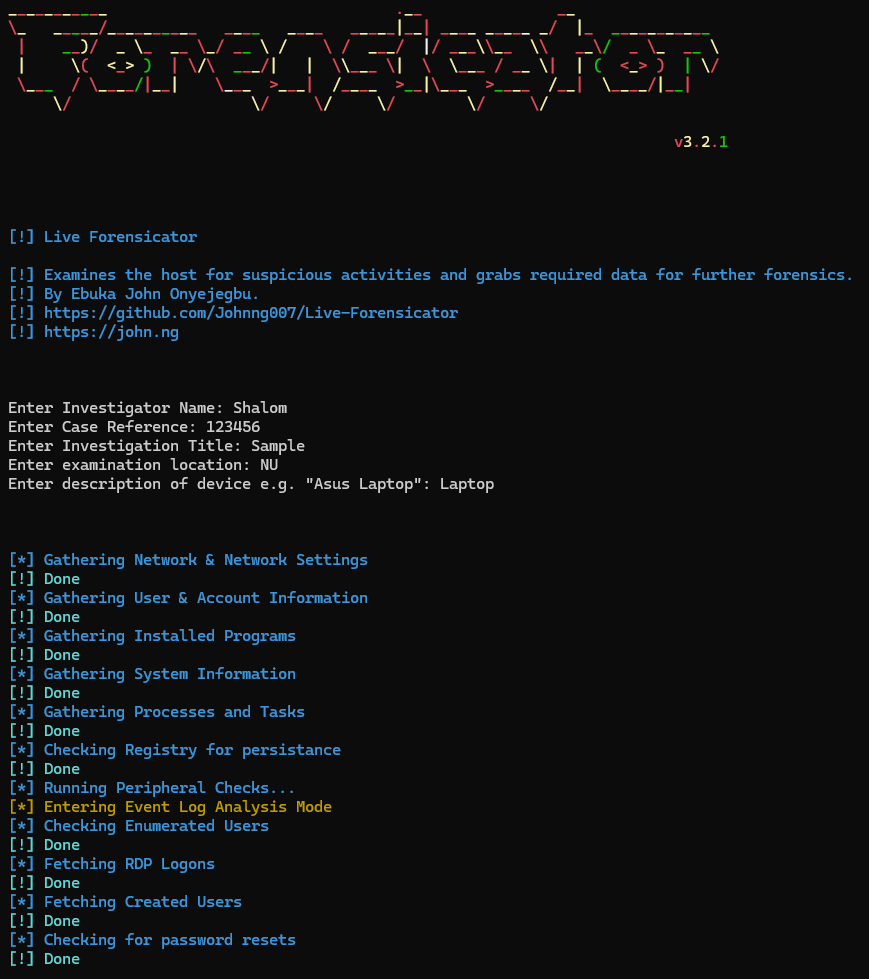
Get PCAP file after analyzing network traffic using Wireshark



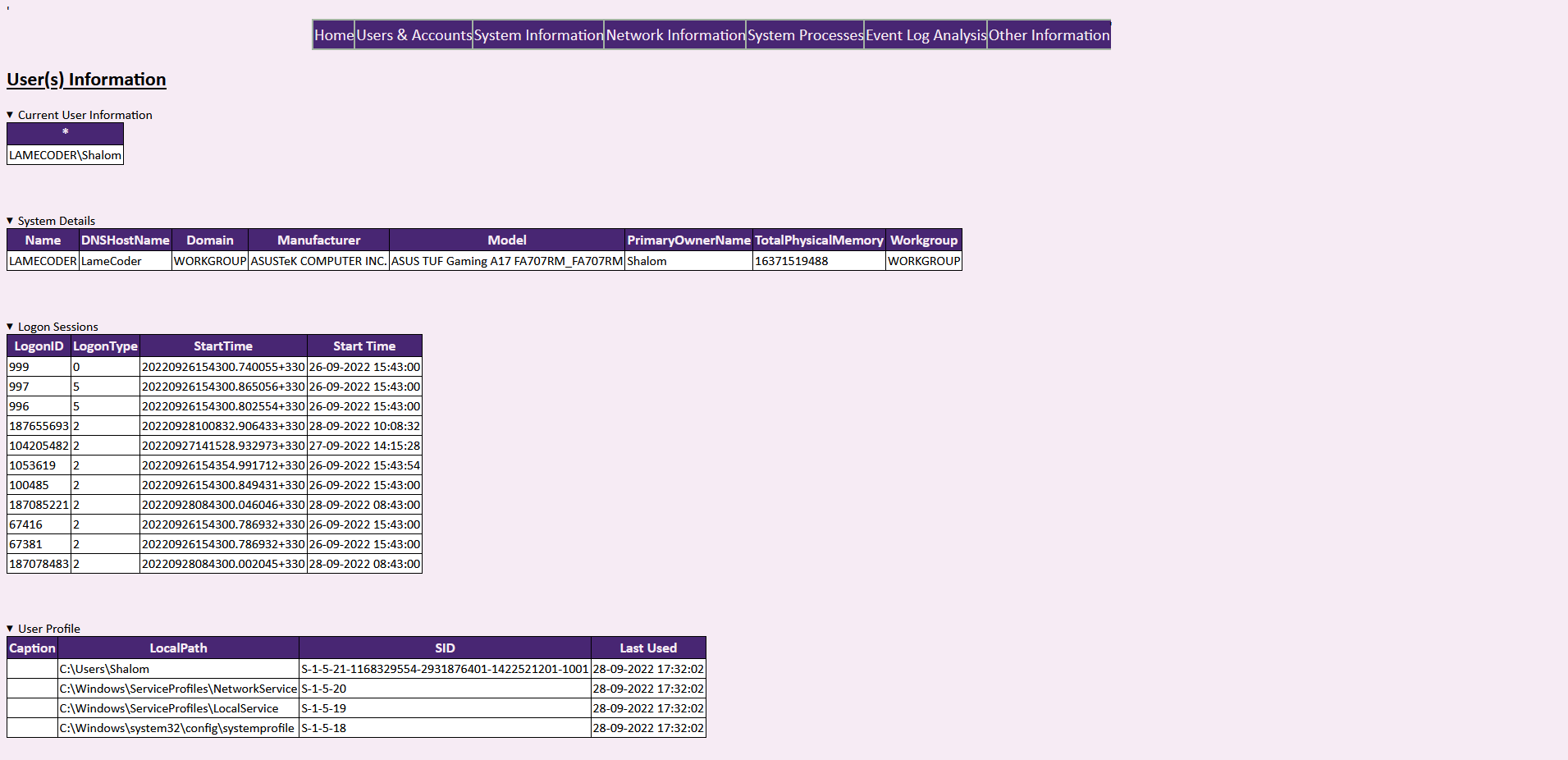
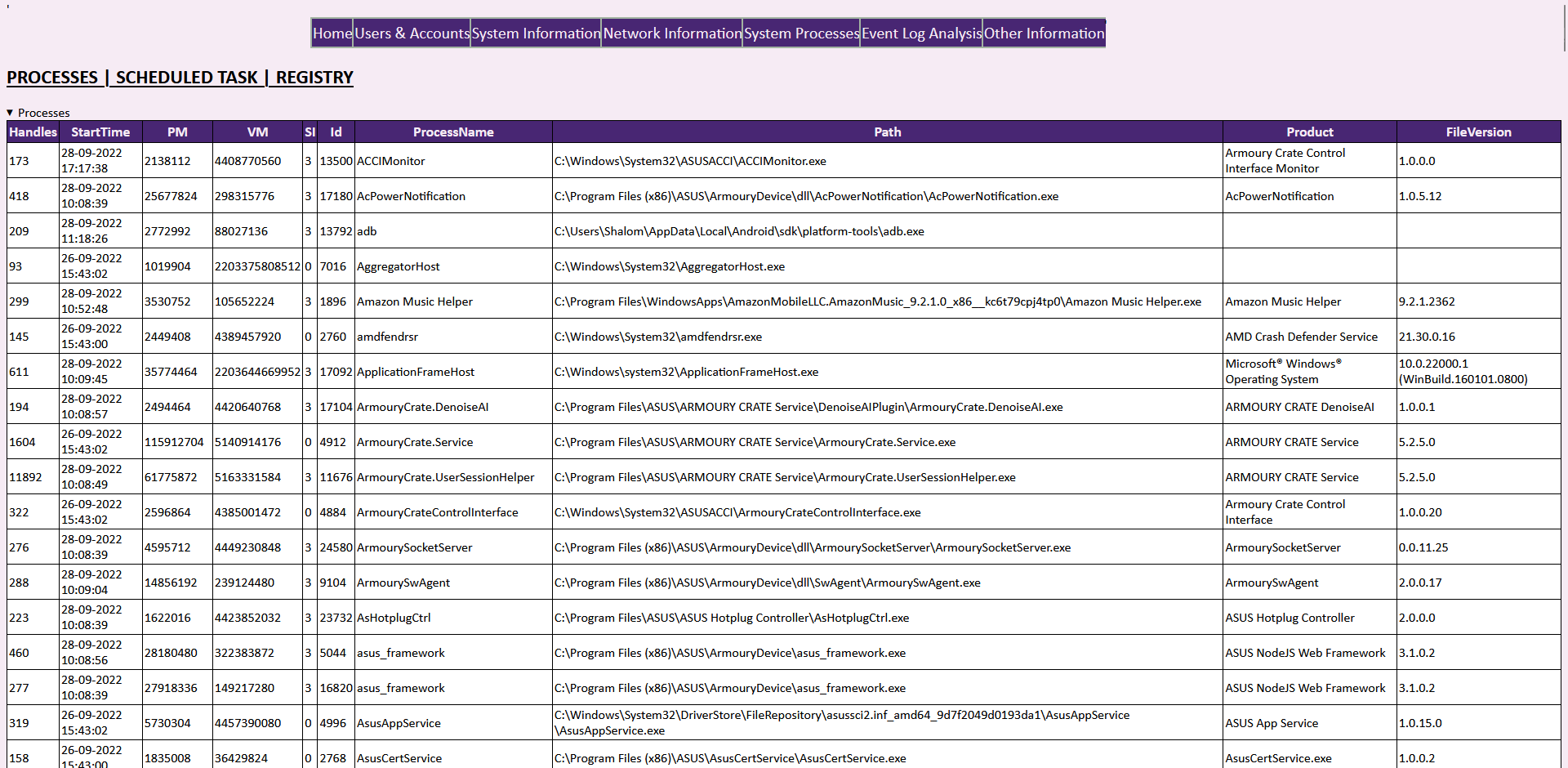
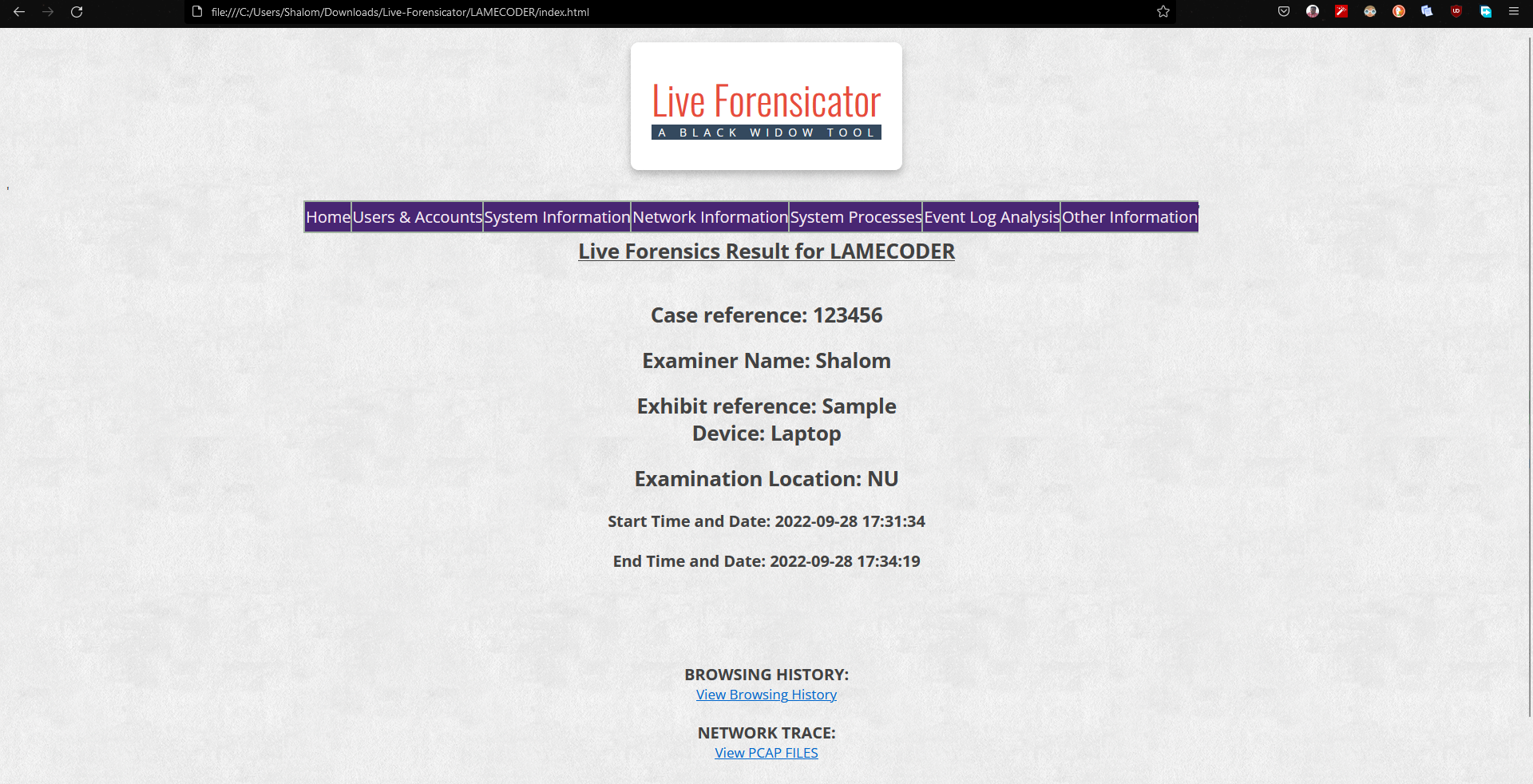
Run various commands to get information about the newly generated PCAP file



Clone the github repository of Live Forensicator and execute the application. The below screen will be shown.

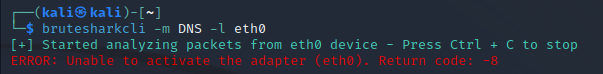


After all data is collected, the information collected is showcased in the below format

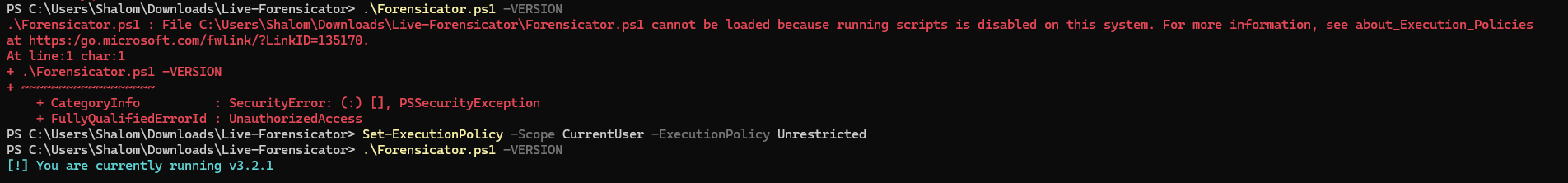


**10. Error Description:**

Had to use sudo for live packet capturing in BruteShark



Running scripts were disabled in the system so had to unrestrict it for LiveForensicator



**11. Conclusion:** System information was gathered using Live Forensicator

**12. Reference:**

<https://www.kali.org/tools/bruteshark/>

<https://github.com/Johnng007/Live-Forensicator>

Lab Assignment 5

**1. Student Name:** G Shalom Shreyan

**2. Student Email ID:** gshalom.shreyan19@st.niituniversity.in

**3. Program/Experiment Number:** 5

**4. Title of the Program/Experiment:** WinHex tool

**5. Date Program/Experiment Performed:** 2/11/2022

**6. Date Report Submitted:** 30/11/2022

**7. Objective:** To edit hex values using winhex tool

**8. Description:**

1. **Overview**

We have to view and modify hex values using WinHex tool.

1. **System Requirement: (Software and Hardware)**
   * At least 500 MB available RAM
   * At least 500 MB of available disk space
   * A Windows 95+, Linux, or Mac OS X machine

* WinHex tool

1. **Configuration of the System used by you to perform the experiment/installation**

AMD Ryzen 7 6800H with Radeon Graphics 3.20 GHz

16.0 GB (15.2 GB usable)

64-bit operating system, x64-based processor

Windows 11 Home Single Language 22621.819

NVIDIA GeForce RTX 3060 Laptop GPU

1. **Algorithm (Step by Step Approach)**

No algorithms were used

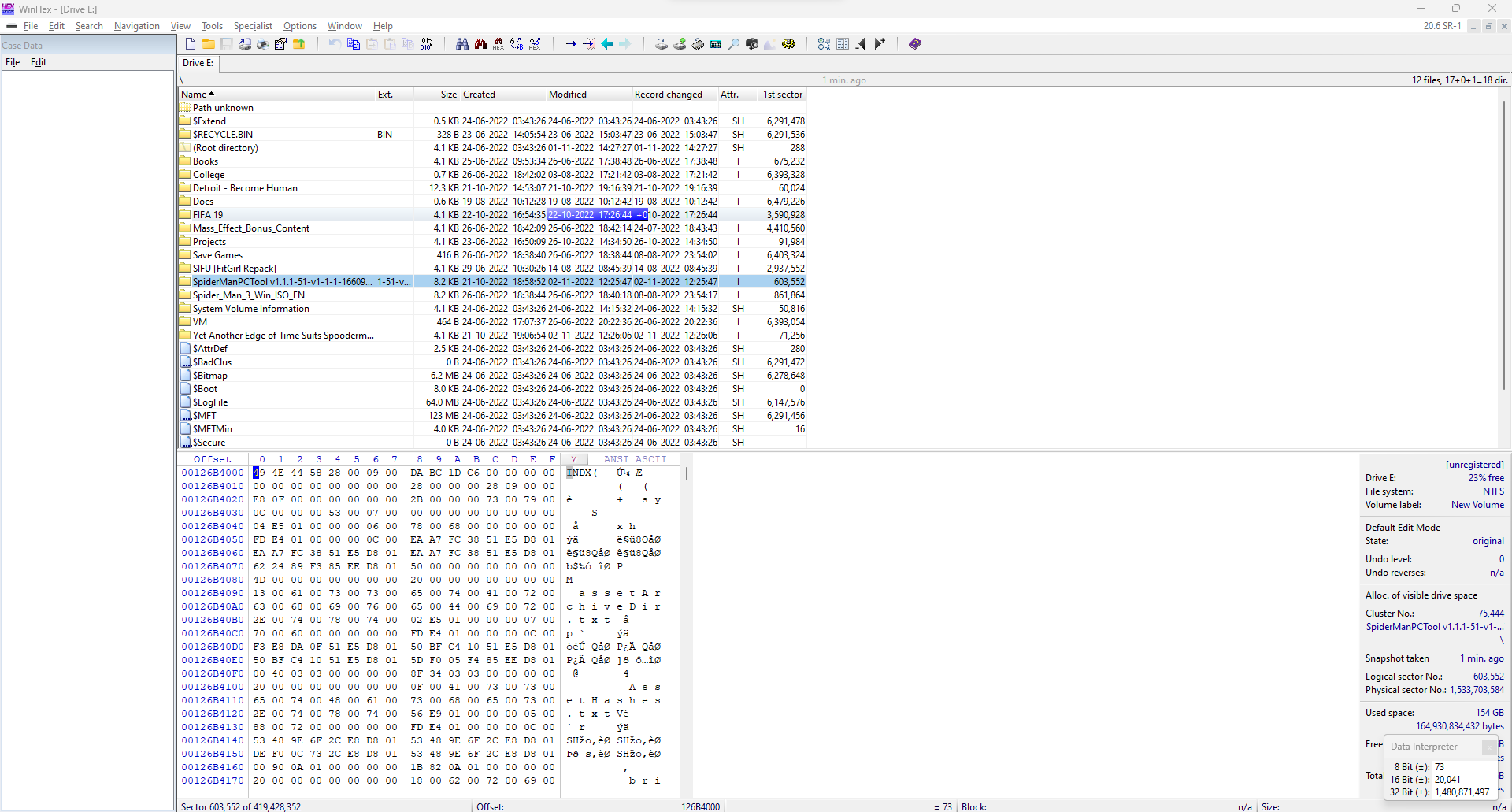
**9. Implementation Details:**

1. **In case of programming implementation: Please add source code**

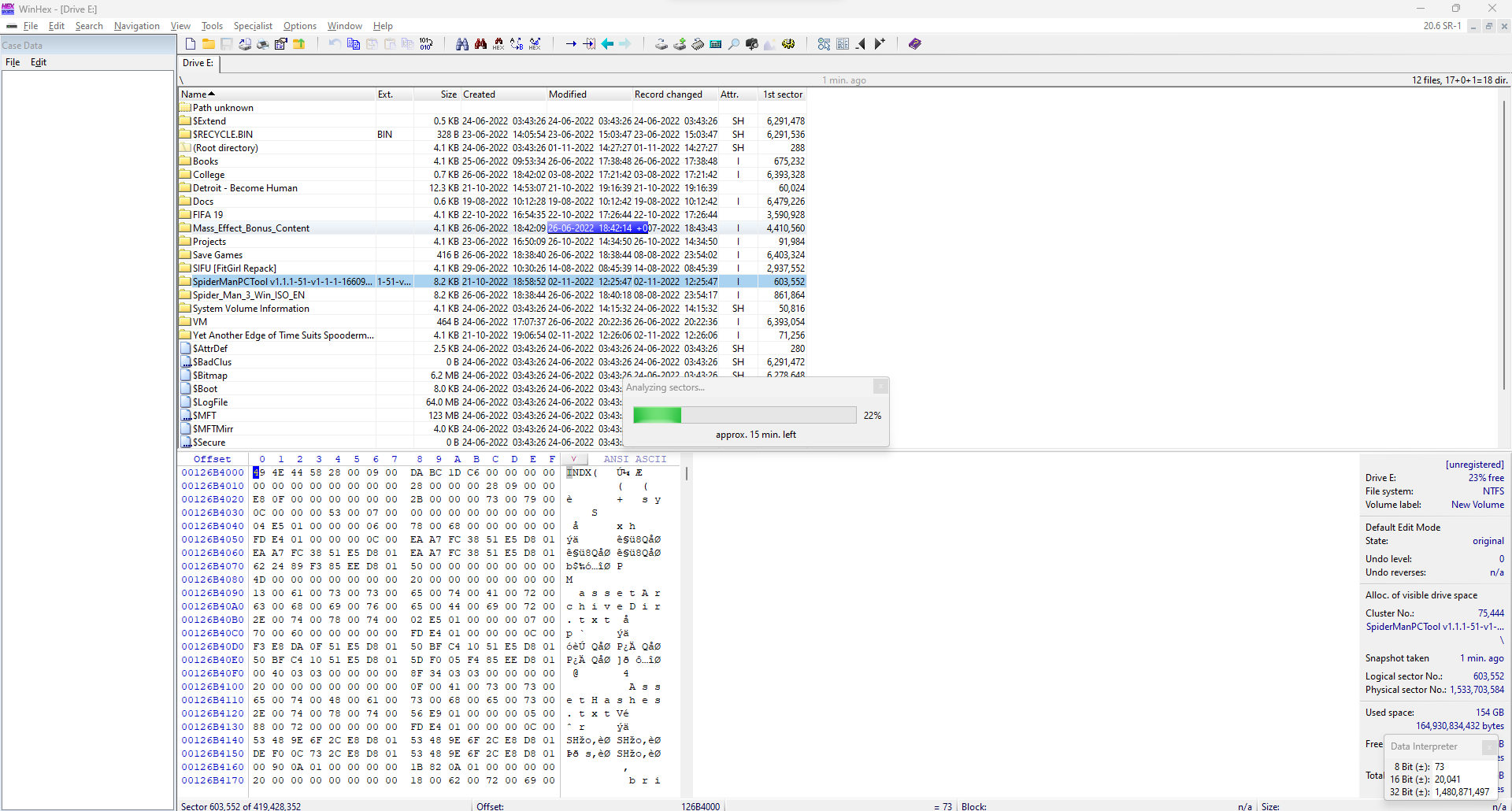
No programming was done.

1. **In case of software installation: Please add screenshots. (Step by Step)**

Running WinHex and scanning a specific drive leads us to the below screenshot.



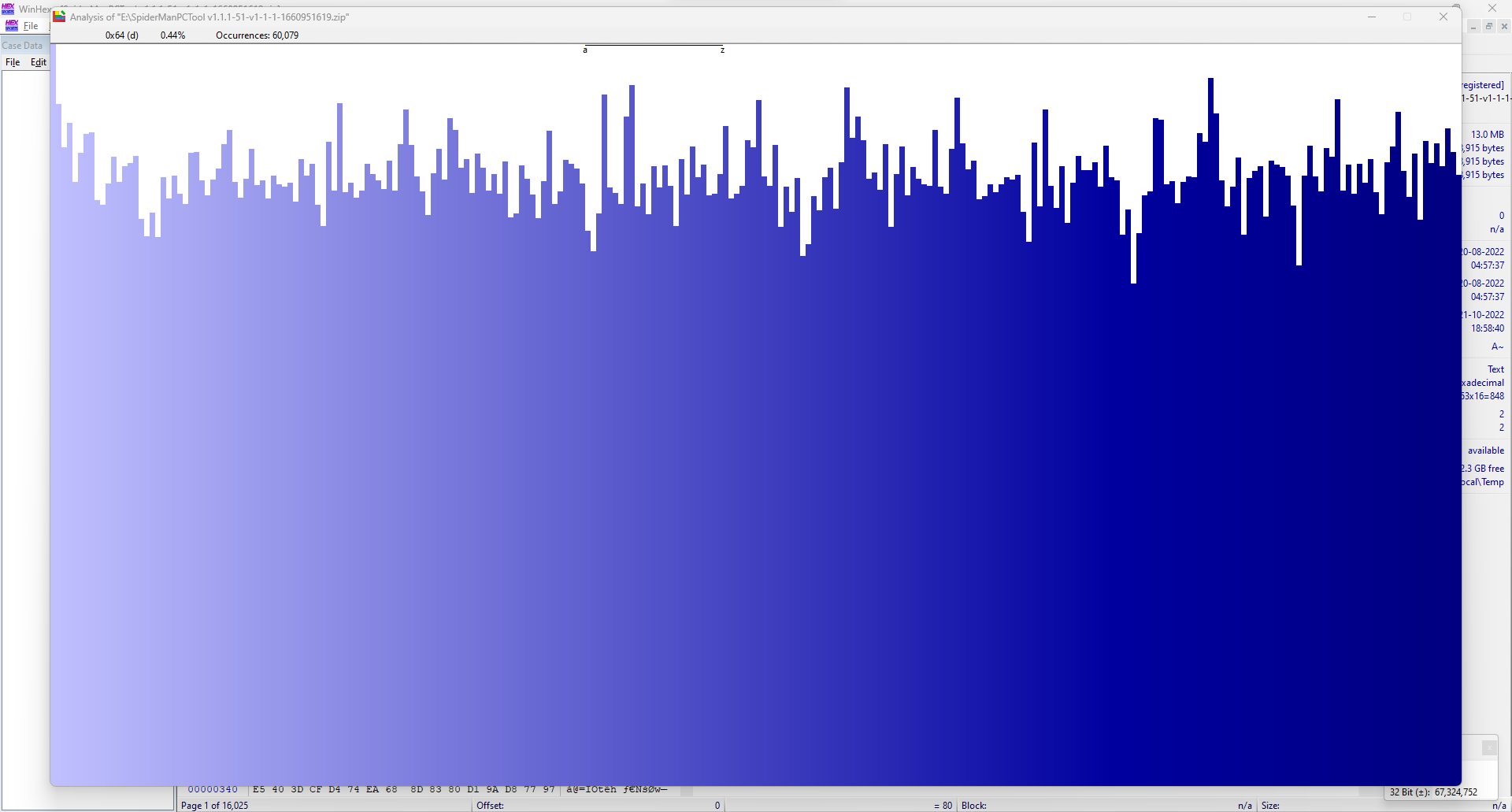
We can also specifically analyze a file



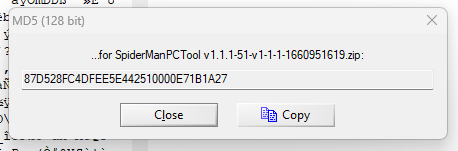
Analyzing the whole disk shows the below graph



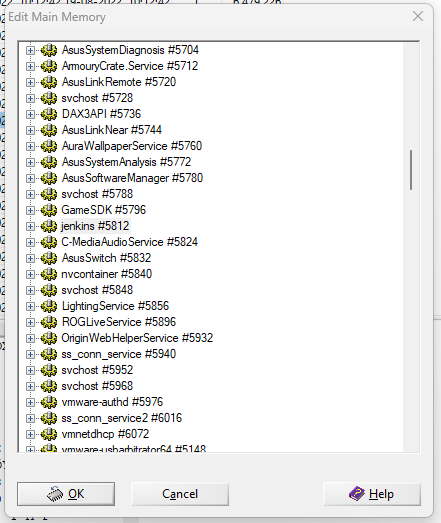
Analyzing a specific file shows the below graph



Hash values can also be easily seen



Services running in the main memory can also be viewed



**10. Error Description:**

No errors were faced

**11. Conclusion:** We have successfully analyzed files from a drive using WinHex tool

**12. Reference:**

<https://winhex.en.softonic.com/>

<https://x-ways.net/winhex/analysis.html>

Lab Assignment 6

**1. Student Name:** G Shalom Shreyan

**2. Student Email ID:** gshalom.shreyan19@st.niituniversity.in

**3. Program/Experiment Number:** 6

**4. Title of the Program/Experiment:** Browser Forensics

**5. Date Program/Experiment Performed:** 9/11/2022

**6. Date Report Submitted:** 30/11/2022

**7. Objective:** To perform an attack on a browser and perform forensics on the browser

**8. Description:**

1. **Overview**

We have to perform an attack on a browser like Chrome, Firefox, Edge and do forensic investigation

1. **System Requirement: (Software and Hardware)**
   * At least 500 MB available RAM
   * An Intel Pentium 4 processor or later that's SSE3 capable
   * At least 500 MB of available disk space
   * A Windows 7 or later, Ubuntu 18.04+, or Mac OS High Sierra 10.13 or later machine

* Chrome, Firefox or Edge Browser

1. **Configuration of the System used by you to perform the experiment/installation**

AMD Ryzen 7 6800H with Radeon Graphics 3.20 GHz

16.0 GB (15.2 GB usable)

64-bit operating system, x64-based processor

Windows 11 Home Single Language 22621.819

NVIDIA GeForce RTX 3060 Laptop GPU

1. **Algorithm (Step by Step Approach)**

No algorithms were used

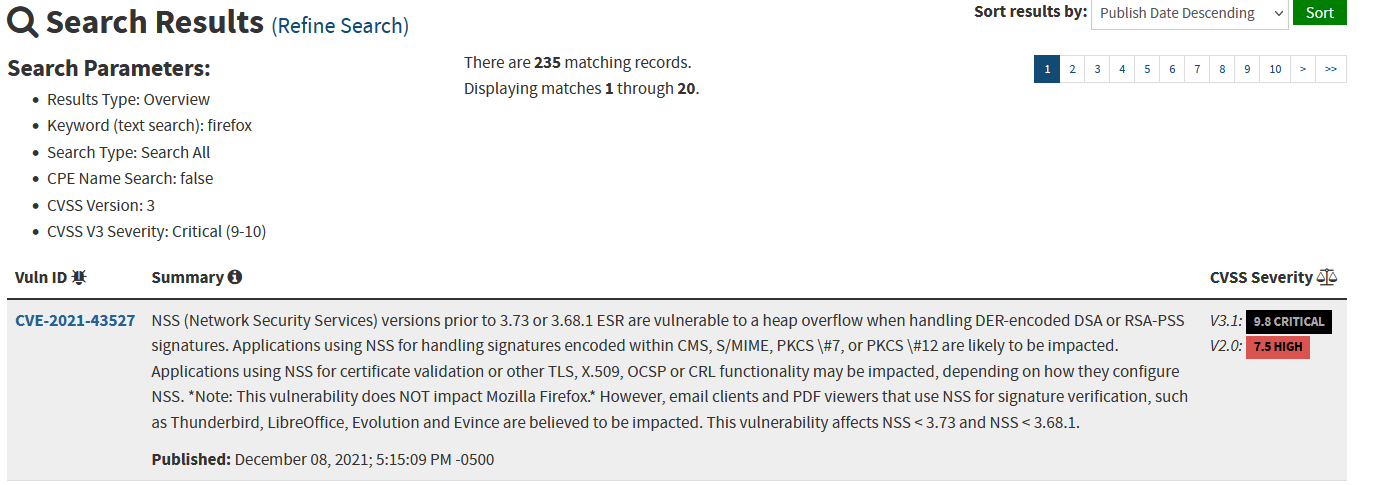
**9. Implementation Details:**

1. **In case of programming implementation: Please add source code**

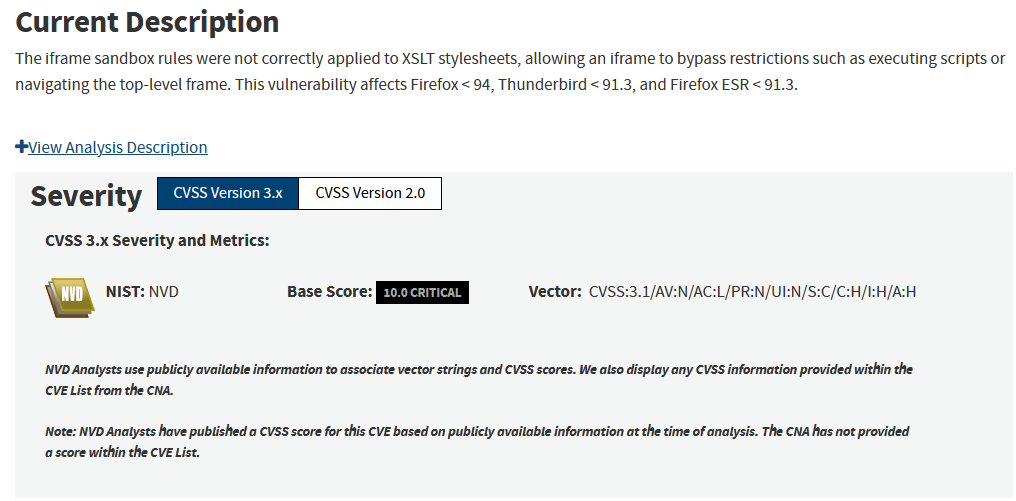
No programming was done.

1. **In case of software installation: Please add screenshots. (Step by Step)**

Search for critical vulnerabilities on the NIST website



Select an attack and perform it on the browser



After the attack is done, use browser forensics tools like Autopsy, Hindsight, BrowsingHistoryView etc to do investigation

**10. Error Description:**

No errors were faced

**11. Conclusion:** Browser forensics has successfully been completed

**12. Reference:**

<https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&query=firefox&search_type=all&isCpeNameSearch=false&cvss_version=3&cvss_v3_severity=CRITICAL>

Lab Assignment 7

**1. Student Name:** G Shalom Shreyan

**2. Student Email ID:** gshalom.shreyan19@st.niituniversity.in

**3. Program/Experiment Number:** 7

**4. Title of the Program/Experiment:** Container Forensics

**5. Date Program/Experiment Performed:** 23/11/2022

**6. Date Report Submitted:** 30/11/2022

**7. Objective:** To perform an attack using a docker container and perform forensic actions

**8. Description:**

1. **Overview**

We have to perform an attack using a docker container and perform introspection & strace to find system calls.

1. **System Requirement: (Software and Hardware)**
   * 64-bit processor with Second Level Address Translation (SLAT)
   * 4GB system RAM
   * At least 500 MB of available disk space
   * A Windows 10 64 bit or higher
   * Docker
2. **Configuration of the System used by you to perform the experiment/installation**

AMD Ryzen 7 6800H with Radeon Graphics 3.20 GHz

16.0 GB (15.2 GB usable)

64-bit operating system, x64-based processor

Windows 11 Home Single Language 22621.819

NVIDIA GeForce RTX 3060 Laptop GPU

1. **Algorithm (Step by Step Approach)**

No algorithms were used

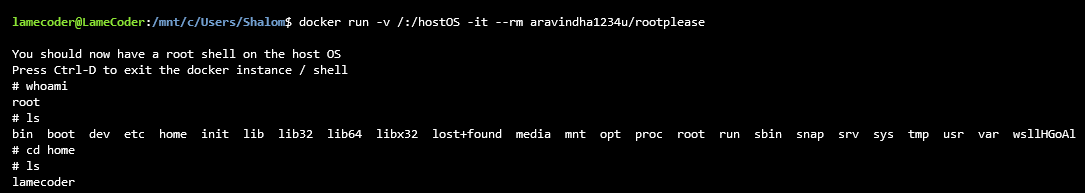
**9. Implementation Details:**

1. **In case of programming implementation: Please add source code**

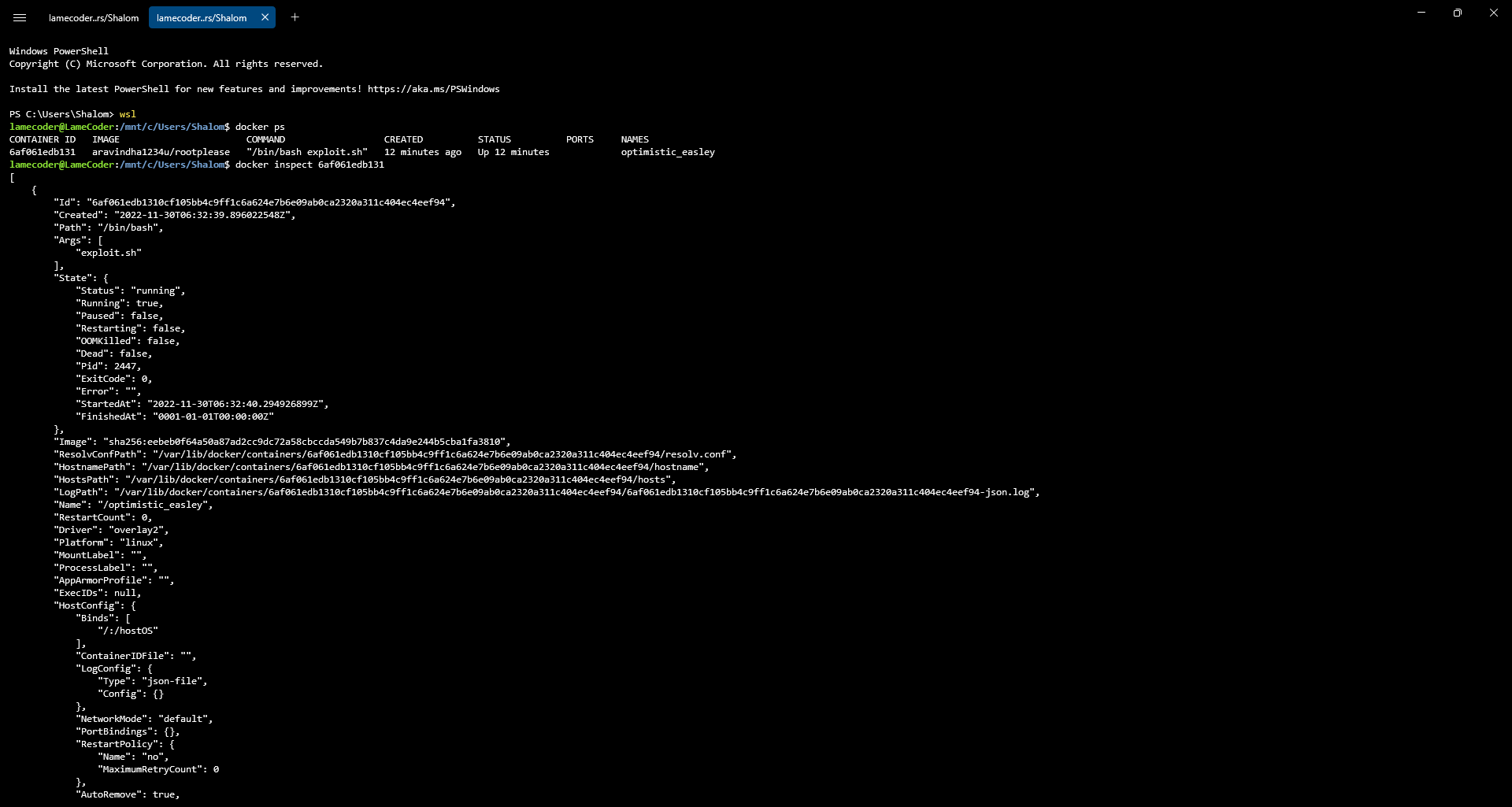
No programming was done.

1. **In case of software installation: Please add screenshots. (Step by Step)**

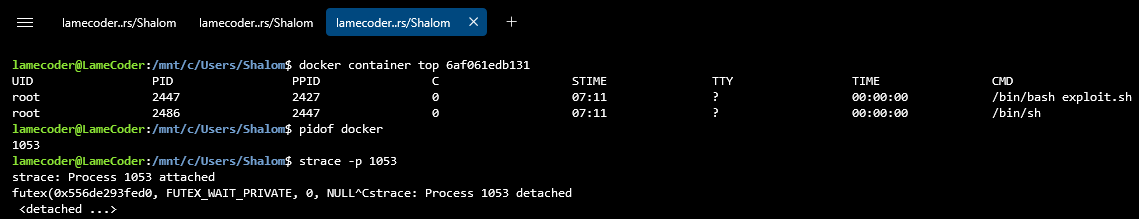
Use the image (https://hub.docker.com/r/aravindha1234u/rootplease) to perform Privilege escalation via Docker. If we happen to have gotten access to a user-account on a machine, and that user is a member of the ‘docker’ group, running the image will provide us with a root shell with admin privileges.



Doing inspection of the docker container returns the following output



Using strace to find system calls in the linux machine, which returned the below output



**10. Error Description:**

No errors were faced

**11. Conclusion:** Container forensics has been completed on the malicious container

**12. Reference:**

<https://fosterelli.co/privilege-escalation-via-docker>

<https://www.howtoforge.com/linux-strace-command/>