CS 4241

CYBER FORENSICS

LAB REPORTS

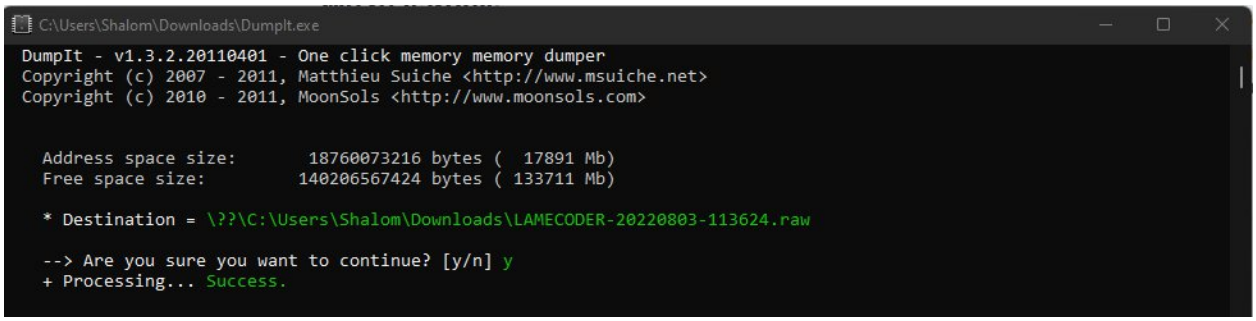
By G Shalom

BT19GCS004

Table Of Contents

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:**
   a. **Overview**
      We have to analyze memory dump files to do memory forensics using volatility tool.
   b. **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
   c. **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
   d. **Algorithm (Step by Step Approach)**
      No algorithms were used
9. **Implementation Details:**
   a. **In case of programming implementation: Please add source code**
      No programming was done.
   b. **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.

```
PS C:\Users\Shalom\Downloads\volatility3-2.0.1\volatility3-2.0.1> py vol.py
Volatility 3 Framework 2.0.1
usage: volatility [-h] [-c CONFIG] [--parallelism [{processes,threads,off}]] [-e EXTEND] [-p PLUGIN_DIRS]
                  [-s SYMBOL_DIRS] [-v] [-l LOG] [-o OUTPUT_DIR] [-q] [-r RENDERER] [-f FILE] [--write-config]
                  [--clear-cache] [--cache-path CACHE_PATH] [--offline] [--single-location SINGLE_LOCATION]
                  [--stackers [STACKERS ...]] [--single-swap-locations [SINGLE_SWAP_LOCATIONS ...]]
                  plugin ...
volatility: error: Please select a plugin to run
```

Run various commands to gain intel.

```
PS C:\Users\Shalom\Downloads\volatility3-2.0.1\volatility3-2.0.1> py vol.py -f "C:\Users\Shalom\Downloads\cridex_memdump\cridex.vmem" windows.pslist
Volatility 3 Framework 2.0.1
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime        File output

4       0       System  0x823c89c8      53      240     N/A     False   N/A     N/A     Disabled
368     4       smss.exe        0x822f1020      3       19      N/A     False   2012-07-22 02:42:31.000000      N/A     Disabled
584     368     csrss.exe       0x822a0598      9       326     0       False   2012-07-22 02:42:32.000000      N/A     Disabled
608     368     winlogon.exe    0x82298700      23      519     0       False   2012-07-22 02:42:32.000000      N/A     Disabled
652     608     services.exe    0x81e2ab28      16      243     0       False   2012-07-22 02:42:32.000000      N/A     Disabled
664     608     lsass.exe       0x81e2a3b8      24      330     0       False   2012-07-22 02:42:32.000000      N/A     Disabled
824     652     svchost.exe     0x82311360      20      194     0       False   2012-07-22 02:42:33.000000      N/A     Disabled
908     652     svchost.exe     0x81e29ab8      9       226     0       False   2012-07-22 02:42:33.000000      N/A     Disabled
1004    652     svchost.exe     0x823001d0      64      1118    0       False   2012-07-22 02:42:33.000000      N/A     Disabled
1056    652     svchost.exe     0x821dfda0      5       60      0       False   2012-07-22 02:42:33.000000      N/A     Disabled
1220    652     svchost.exe     0x82295650      15      197     0       False   2012-07-22 02:42:35.000000      N/A     Disabled
1484    1464    explorer.exe    0x821dea70      17      415     0       False   2012-07-22 02:42:36.000000      N/A     Disabled
1512    652     spoolsv.exe     0x81eb17b8      14      113     0       False   2012-07-22 02:42:36.000000      N/A     Disabled
1640    1484    reader_sl.exe   0x81e7bda0      5       39      0       False   2012-07-22 02:42:36.000000      N/A     Disabled
788     652     alg.exe 0x820e8da0      7       104     0       False   2012-07-22 02:43:01.000000      N/A     Disabled
1136    1004    wuauclt.exe     0x821fcda0      8       173     0       False   2012-07-22 02:43:46.000000      N/A     Disabled
1588    1004    wuauclt.exe     0x8205bda0      5       132     0       False   2012-07-22 02:44:01.000000      N/A     Disabled
```

```
PS C:\Users\Shalom\Downloads\volatility3-2.0.1\volatility3-2.0.1> py vol.py -f "C:\Users\Shalom\Downloads\cridex_memdump\cridex.vmem" windows.pstree
Volatility 3 Framework 2.0.1
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime

4       0       System  0x823c89c8      53      240     N/A     False   N/A     N/A
* 368   4       smss.exe        0x822f1020      3       19      N/A     False   2012-07-22 02:42:31.000000      N/A
** 584  368     csrss.exe       0x822a0598      9       326     0       False   2012-07-22 02:42:32.000000      N/A
** 608  368     winlogon.exe    0x82298700      23      519     0       False   2012-07-22 02:42:32.000000      N/A
*** 664 608     lsass.exe       0x81e2a3b8      24      330     0       False   2012-07-22 02:42:32.000000      N/A
*** 652 608     services.exe    0x81e2ab28      16      243     0       False   2012-07-22 02:42:32.000000      N/A
**** 1056       652     svchost.exe     0x821dfda0      5       60      0       False   2012-07-22 02:42:33.000000      N/A
**** 1220       652     svchost.exe     0x82295650      15      197     0       False   2012-07-22 02:42:35.000000      N/A
**** 1512       652     spoolsv.exe     0x81eb17b8      14      113     0       False   2012-07-22 02:42:36.000000      N/A
**** 908        652     svchost.exe     0x81e29ab8      9       226     0       False   2012-07-22 02:42:33.000000      N/A
**** 1004       652     svchost.exe     0x823001d0      64      1118    0       False   2012-07-22 02:42:33.000000      N/A
***** 1136      1004    wuauclt.exe     0x821fcda0      8       173     0       False   2012-07-22 02:43:46.000000      N/A
***** 1588      1004    wuauclt.exe     0x8205bda0      5       132     0       False   2012-07-22 02:44:01.000000      N/A
**** 788        652     alg.exe 0x820e8da0      7       104     0       False   2012-07-22 02:43:01.000000      N/A
**** 824        652     svchost.exe     0x82311360      20      194     0       False   2012-07-22 02:42:33.000000      N/A
1484    1464    explorer.exe    0x821dea70      17      415     0       False   2012-07-22 02:42:36.000000      N/A
* 1640  1484    reader_sl.exe   0x81e7bda0      5       39      0       False   2012-07-22 02:42:36.000000      N/A
```

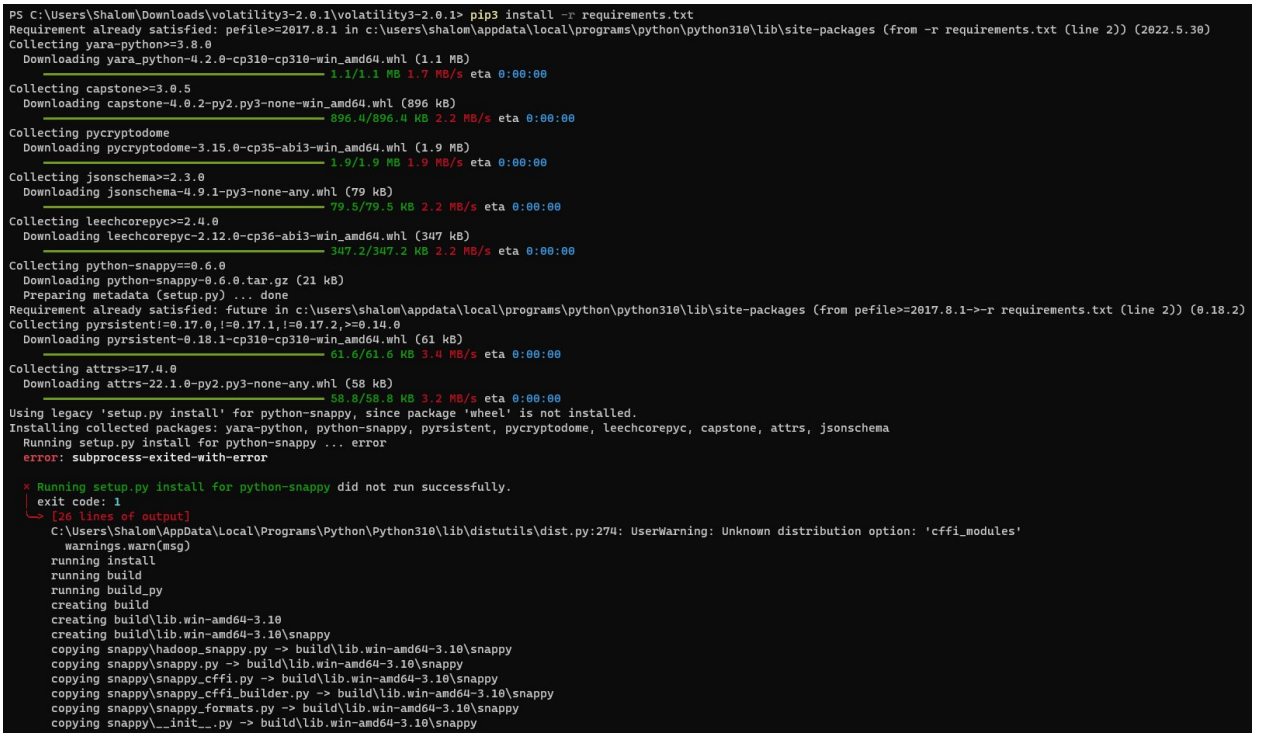
```
PS C:\Users\Shalom\Downloads\volatility3-2.0.1\volatility3-2.0.1> py vol.py -f "C:\Users\Shalom\Downloads\cridex_memdump\cridex.vmem" windows.psscan
Volatility 3 Framework 2.0.1
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime        File output

908     652     svchost.exe     0x2029ab8       9       226     0       False   2012-07-22 02:42:33.000000      N/A     Disabled
664     608     lsass.exe       0x202a3b8       24      330     0       False   2012-07-22 02:42:32.000000      N/A     Disabled
652     608     services.exe    0x202ab28       16      243     0       False   2012-07-22 02:42:32.000000      N/A     Disabled
1640    1484    reader_sl.exe   0x207bda0       5       39      0       False   2012-07-22 02:42:36.000000      N/A     Disabled
1512    652     spoolsv.exe     0x20b17b8       14      113     0       False   2012-07-22 02:42:36.000000      N/A     Disabled
1588    1004    wuauclt.exe     0x225bda0       5       132     0       False   2012-07-22 02:44:01.000000      N/A     Disabled
788     652     alg.exe 0x22e8da0       7       104     0       False   2012-07-22 02:43:01.000000      N/A     Disabled
1484    1464    explorer.exe    0x23dea70       17      415     0       False   2012-07-22 02:42:36.000000      N/A     Disabled
1056    652     svchost.exe     0x23dfda0       5       60      0       False   2012-07-22 02:42:33.000000      N/A     Disabled
1136    1004    wuauclt.exe     0x23fcda0       8       173     0       False   2012-07-22 02:43:46.000000      N/A     Disabled
1220    652     svchost.exe     0x2495650       15      197     0       False   2012-07-22 02:42:35.000000      N/A     Disabled
608     368     winlogon.exe    0x2498700       23      519     0       False   2012-07-22 02:42:32.000000      N/A     Disabled
584     368     csrss.exe       0x24a0598       9       326     0       False   2012-07-22 02:42:32.000000      N/A     Disabled
368     4       smss.exe        0x24f1020       3       19      N/A     False   2012-07-22 02:42:31.000000      N/A     Disabled
1004    652     svchost.exe     0x25001d0       64      1118    0       False   2012-07-22 02:42:33.000000      N/A     Disabled
824     652     svchost.exe     0x2511360       20      194     0       False   2012-07-22 02:42:33.000000      N/A     Disabled
4       0       System  0x25c89c8       53      240     N/A     False   N/A     N/A     Disabled
```

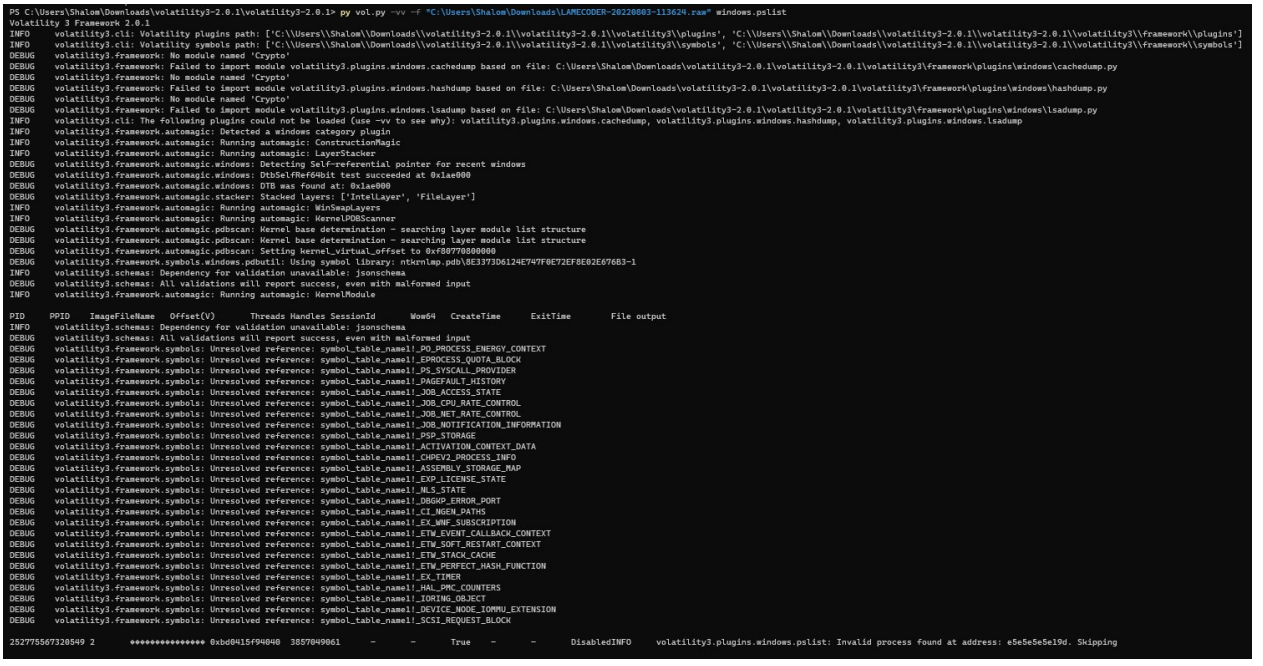
```
PS C:\Users\Shalom\Downloads\volatility3-2.0.1\volatility3-2.0.1> py vol.py -f "C:\Users\Shalom\Downloads\cridex_memdump\cridex.vmem" windows.netscan
Volatility 3 Framework 2.0.1
Progress:  100.00               PDB scanning finished
Offset  Proto   LocalAddr       LocalPort       ForeignAddr     ForeignPort     State   PID     Owner   Created
Traceback (most recent call last):
  File "C:\Users\Shalom\Downloads\volatility3-2.0.1\volatility3-2.0.1\vol.py", line 10, in <module>
    volatility3.cli.main()
  File "C:\Users\Shalom\Downloads\volatility3-2.0.1\volatility3-2.0.1\volatility3\cli\__init__.py", line 625, in main
    CommandLine().run()
  File "C:\Users\Shalom\Downloads\volatility3-2.0.1\volatility3-2.0.1\volatility3\cli\__init__.py", line 333, in run
    renderers[args.renderer]().render(constructed.run())
  File "C:\Users\Shalom\Downloads\volatility3-2.0.1\volatility3-2.0.1\volatility3\cli\text_renderer.py", line 178, in render
    grid.populate(visitor, outfd)
  File "C:\Users\Shalom\Downloads\volatility3-2.0.1\volatility3-2.0.1\volatility3\framework\renderers\__init__.py", line 212, in populate
    for (level, item) in self._generator:
  File "C:\Users\Shalom\Downloads\volatility3-2.0.1\volatility3-2.0.1\volatility3\framework\plugins\windows\netscan.py", line 282, in _generator
    netscan_symbol_table = self.create_netscan_symbol_table(self.context, kernel.layer_name,
  File "C:\Users\Shalom\Downloads\volatility3-2.0.1\volatility3-2.0.1\volatility3\framework\plugins\windows\netscan.py", line 238, in create_netscan_symbol_table
    symbol_filename, class_types = cls.determine_tcpip_version(
  File "C:\Users\Shalom\Downloads\volatility3-2.0.1\volatility3-2.0.1\volatility3\framework\plugins\windows\netscan.py", line 215, in determine_tcpip_version
    raise NotImplementedError("This version of Windows is not supported: {}.{} {}.{}!".format(
NotImplementedError: This version of Windows is not supported: 5.1 15.2600!
```

10. Error Description:

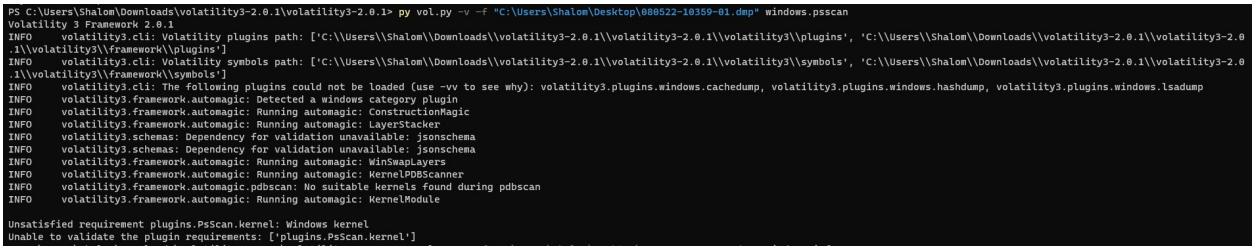
1. Getting all required libraries wasn't possible due to errors in installing snappy library. Also found a link for possible fix (https://stackoverflow.com/questions/42979544/how-to-install-snappy-c-libraries-on-windows-10-for-use-with-python-snappy-in-an) but it resulted in another error, which wasn't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



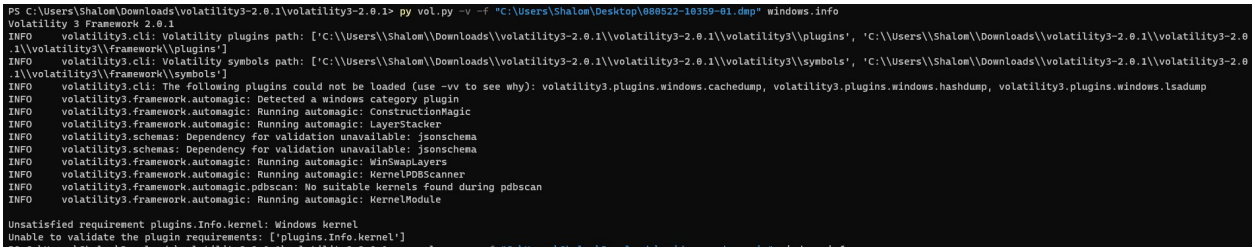
2. Invalid process detected in the memory dump created of Windows 11, possible system issue as Windows XP dump ran fine.



3. Windows Kernel error when tried to analyze memory dumps created automatically by Windows



Tried 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

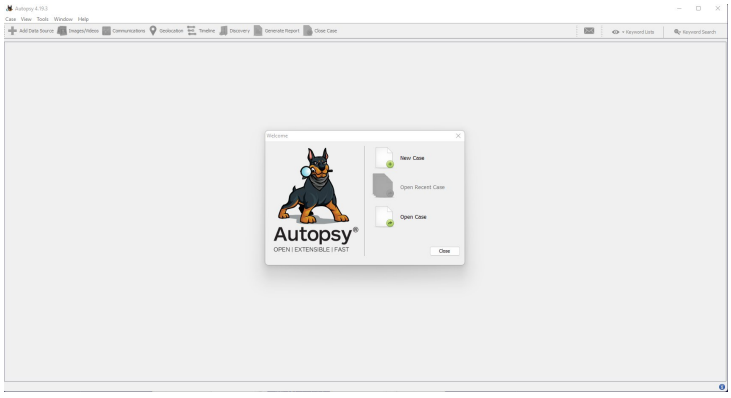
https://infosecwriteups.com/forensics-memory-analysis-with-volatility-6f2b9e859765

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

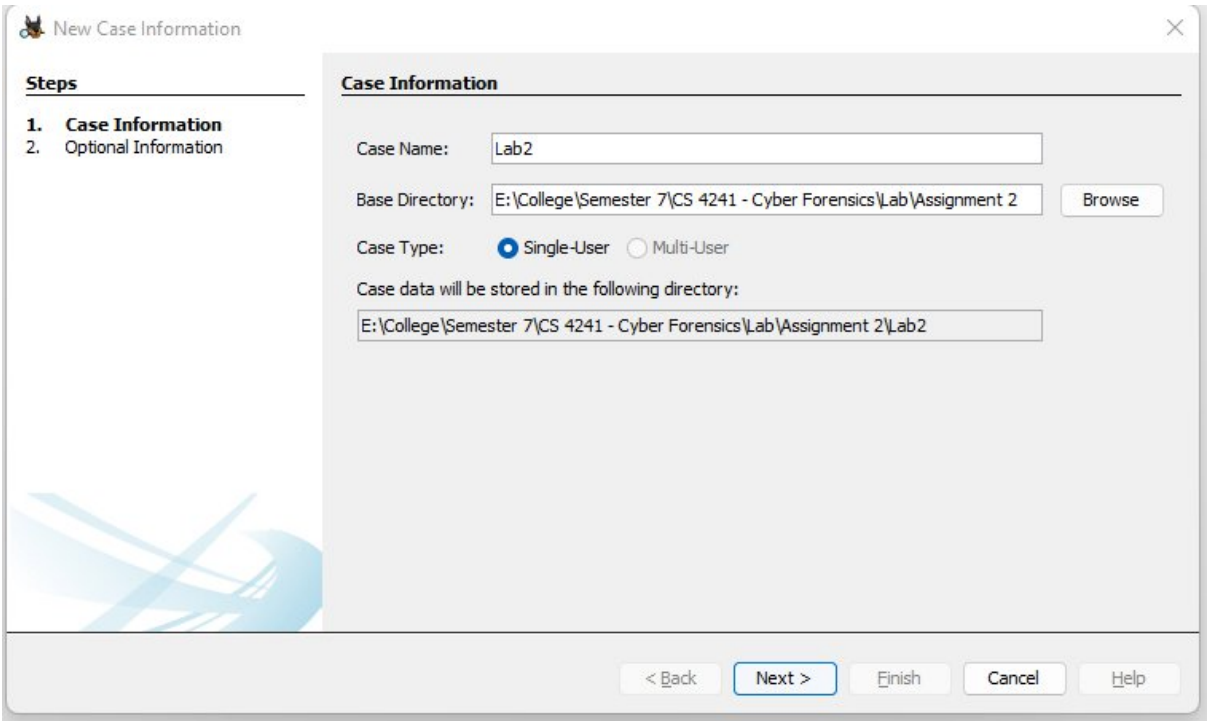
https://www.hackingarticles.in/multiple-ways-to-capture-memory-for-analysis/

Lab Assignment 2

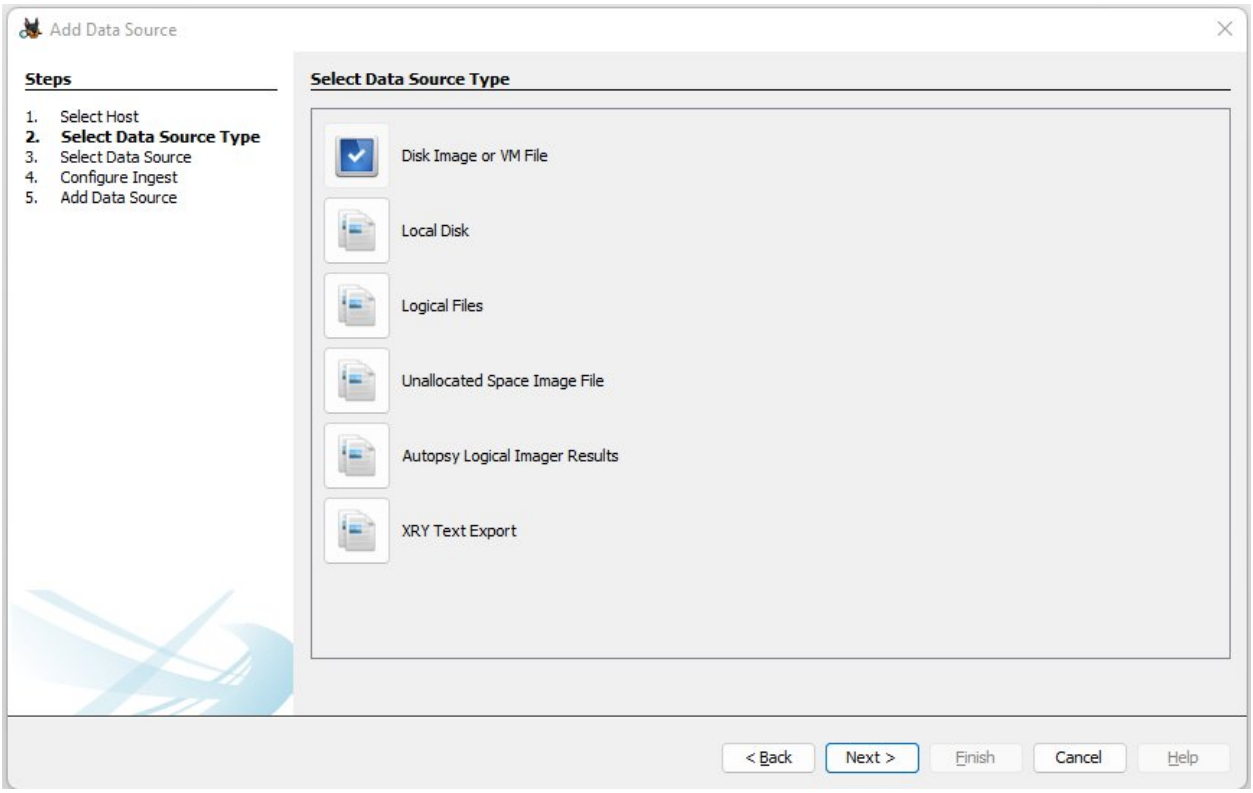
1. **Student Name:** G Shalom Shreyan
2. **Student Email ID:** gshalom.shreyan19@st.niituniversity.in
3. **Program/Experiment Number:** 2
4. **Title of the Program/Experiment:** Wireshark & Autopsy
5. **Date Program/Experiment Performed:** 31/08/2022
6. **Date Report Submitted:** 30/11/2022
7. **Objective:** To analyze Windows & Unix file systems using Autopsy and analyze packets using Wireshark
8. **Description:**
   a. **Overview**
   We have to analyze Linux file system using Autopsy tool.
   b. **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
   c. **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
   d. **Algorithm (Step by Step Approach)**
   No algorithms were used
9. **Implementation Details:**
   a. **In case of programming implementation: Please add source code**
   No programming was done.
   b. **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.

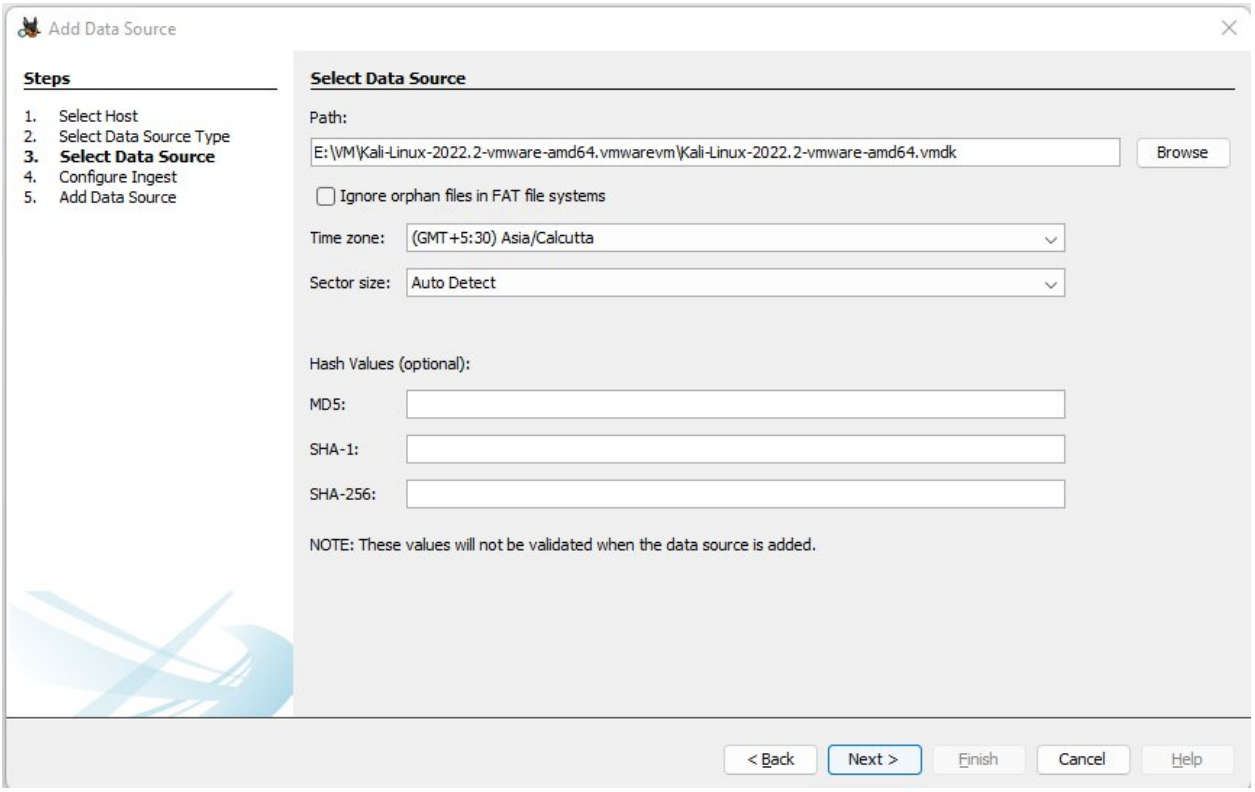


A new case is created and relevant details are entered

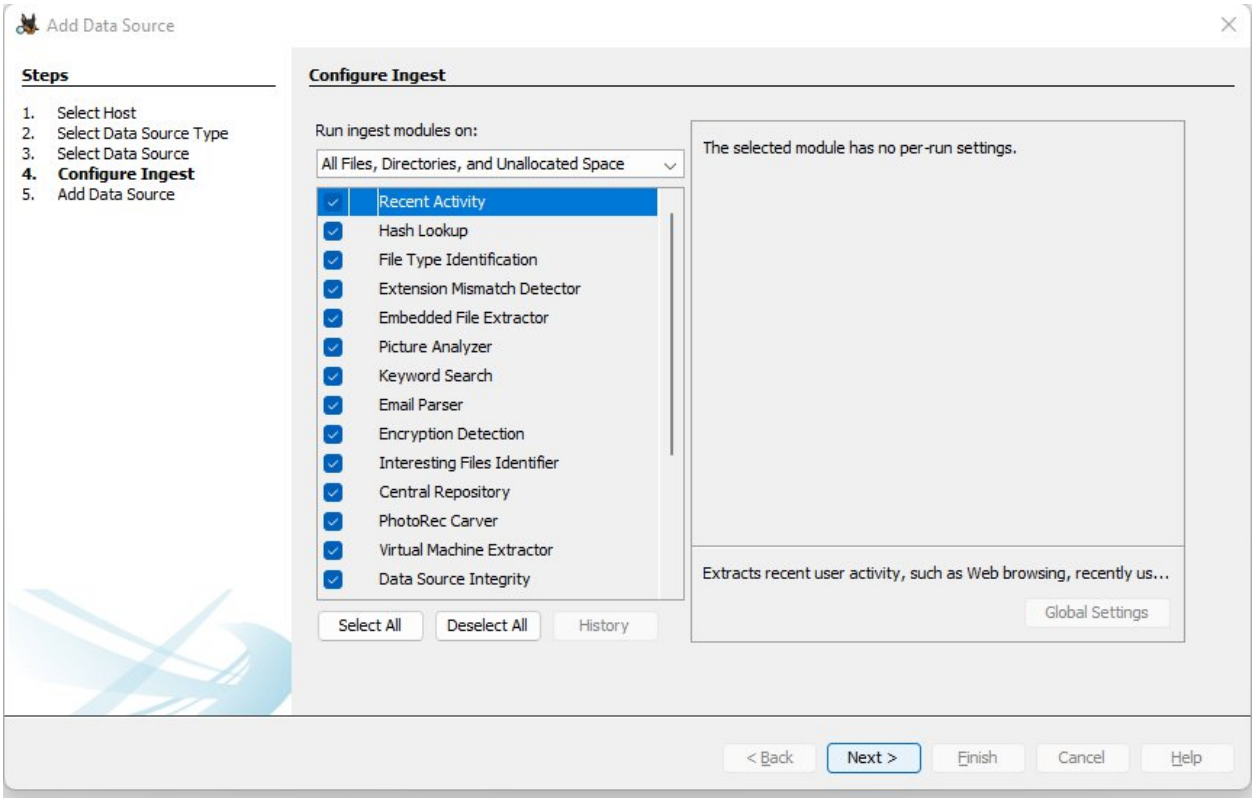


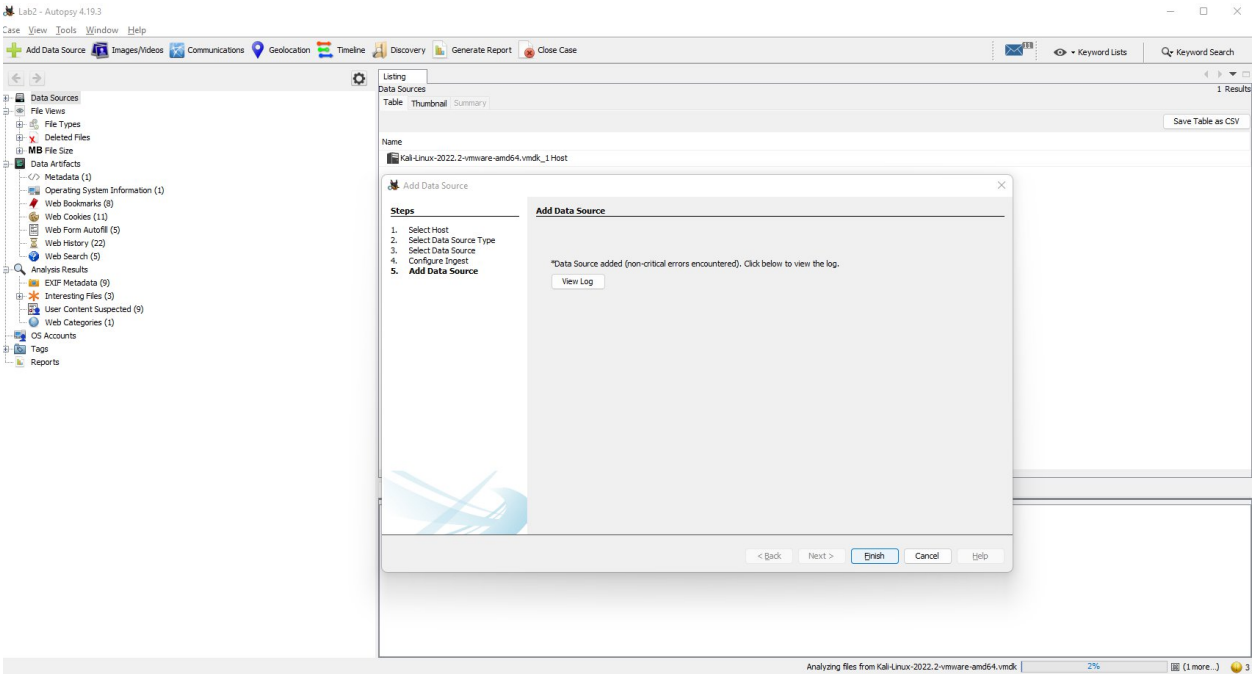
A Kali-Linux VM image will be chosen as a data source





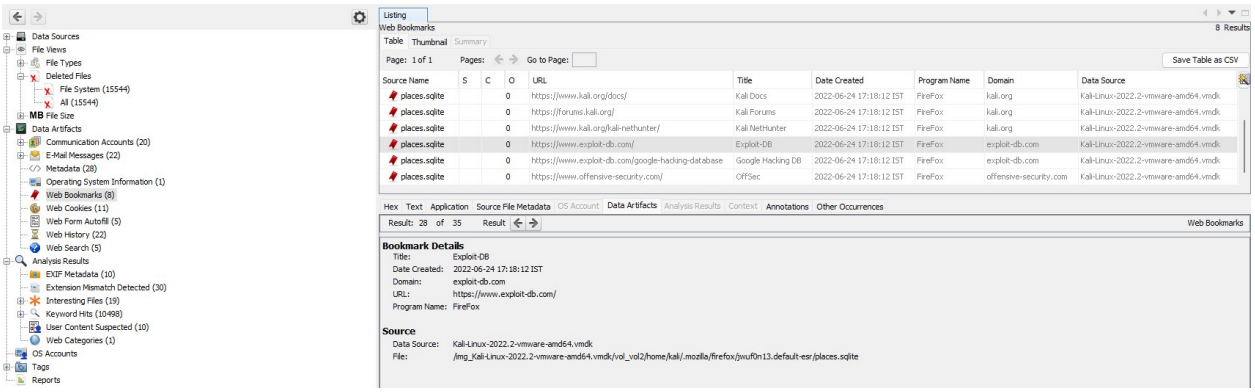
Configure to ingest to include everything to get all information



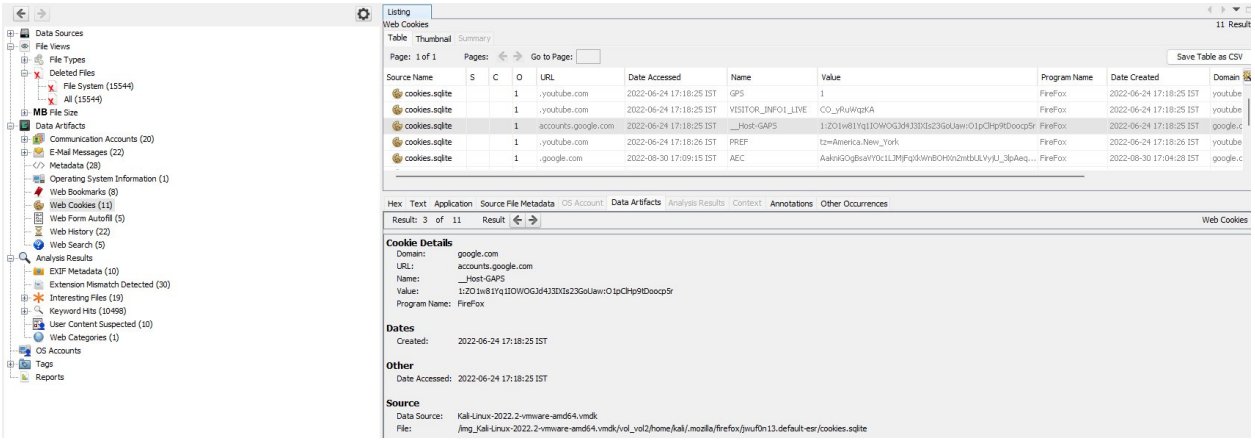


Now we can see the dashboard and all the important information

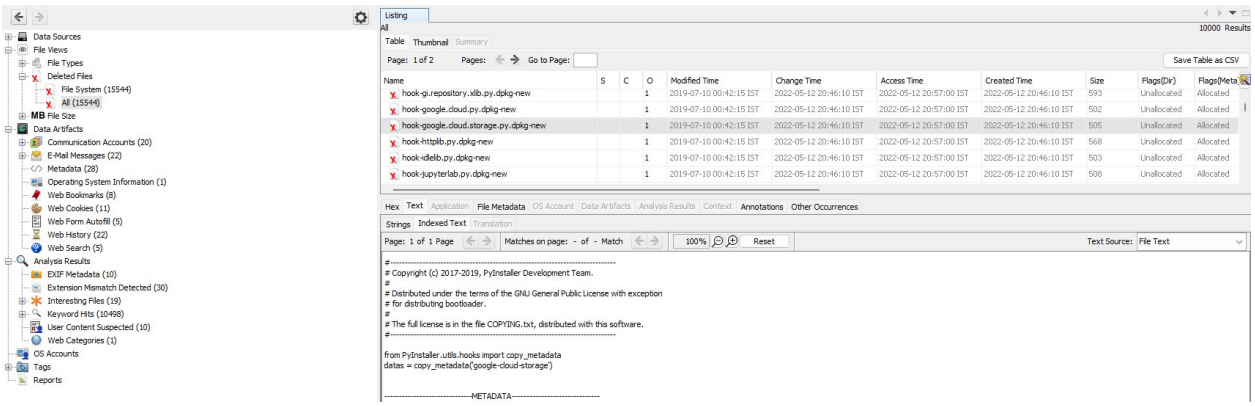
Bookmarks



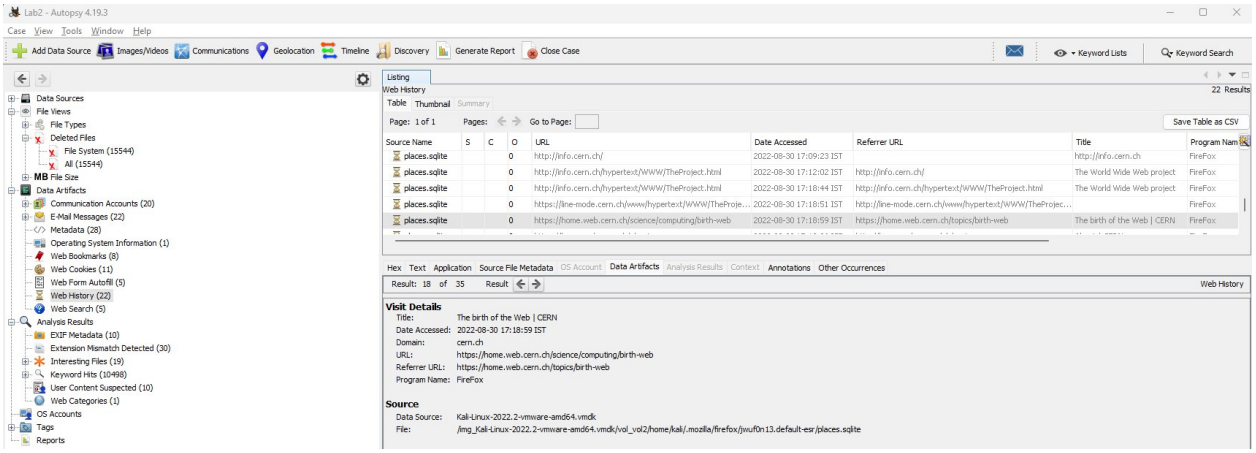
Cookies



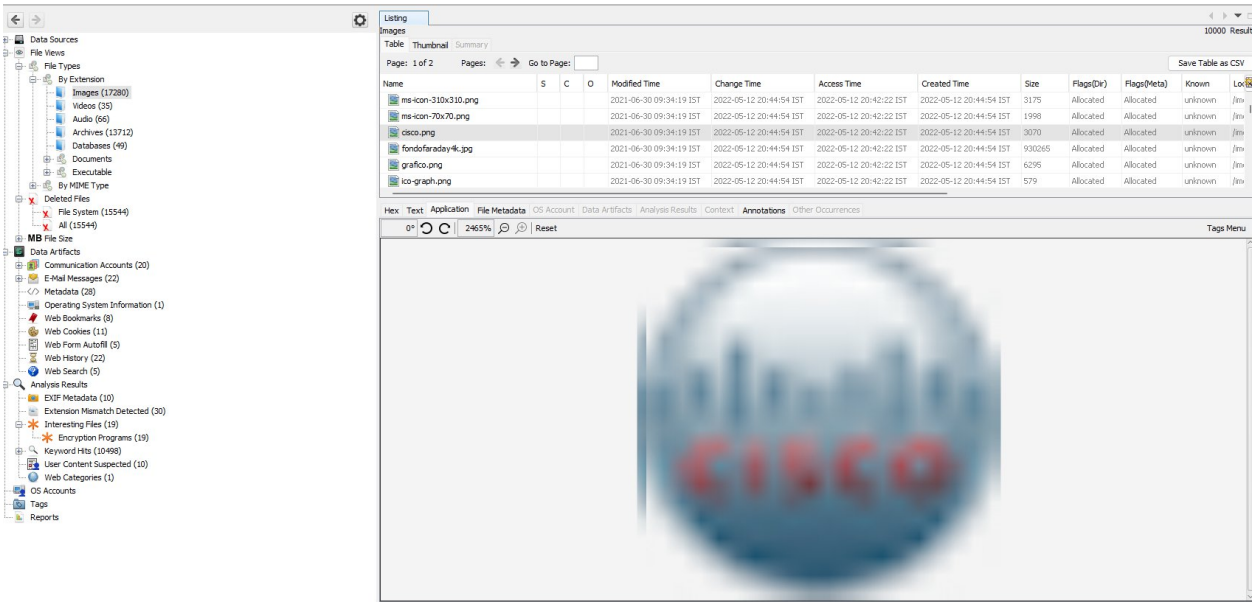
Deleted Files



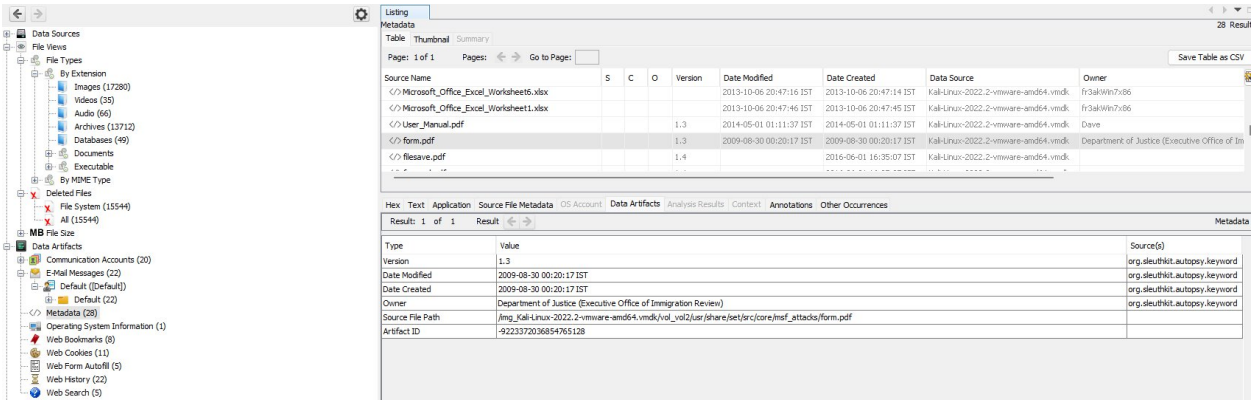
Web History



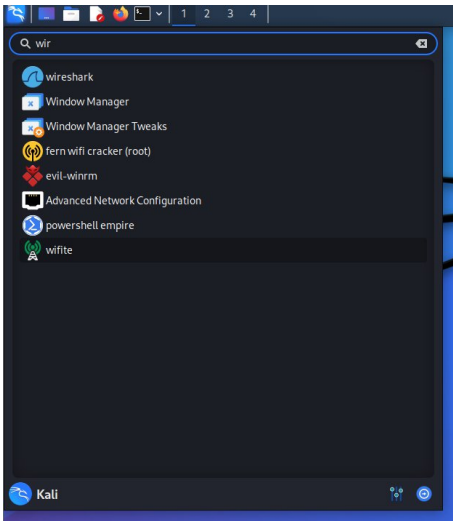
Images



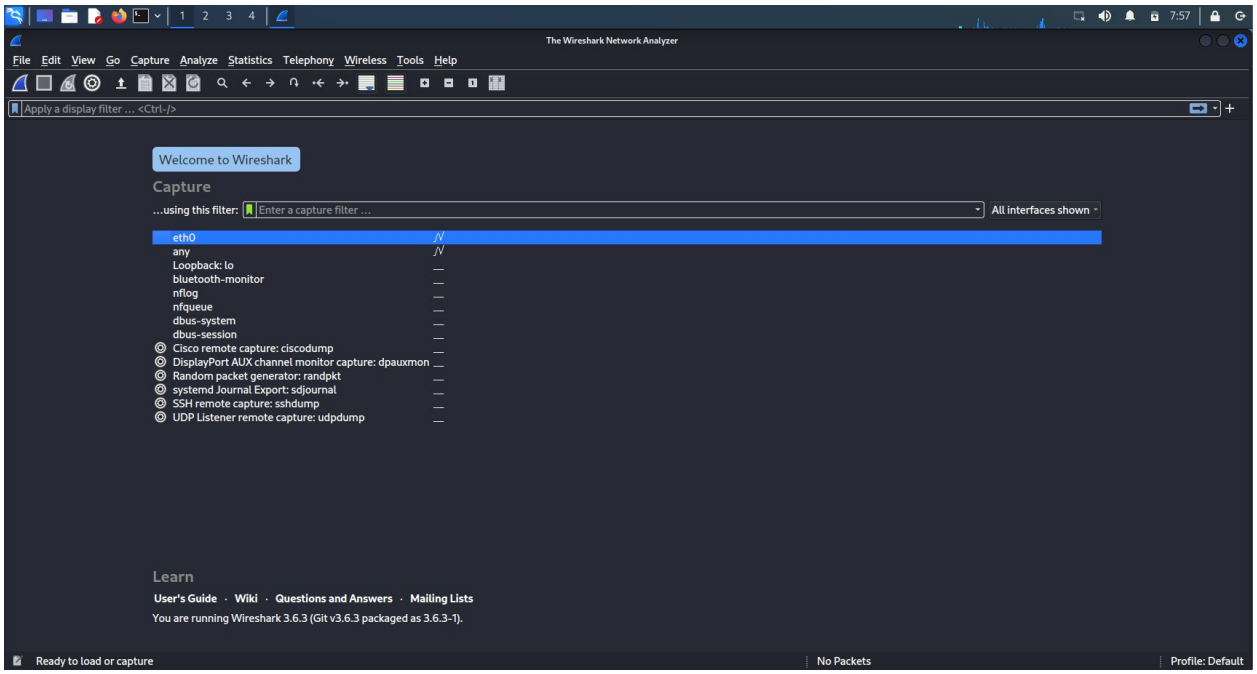
Data Files



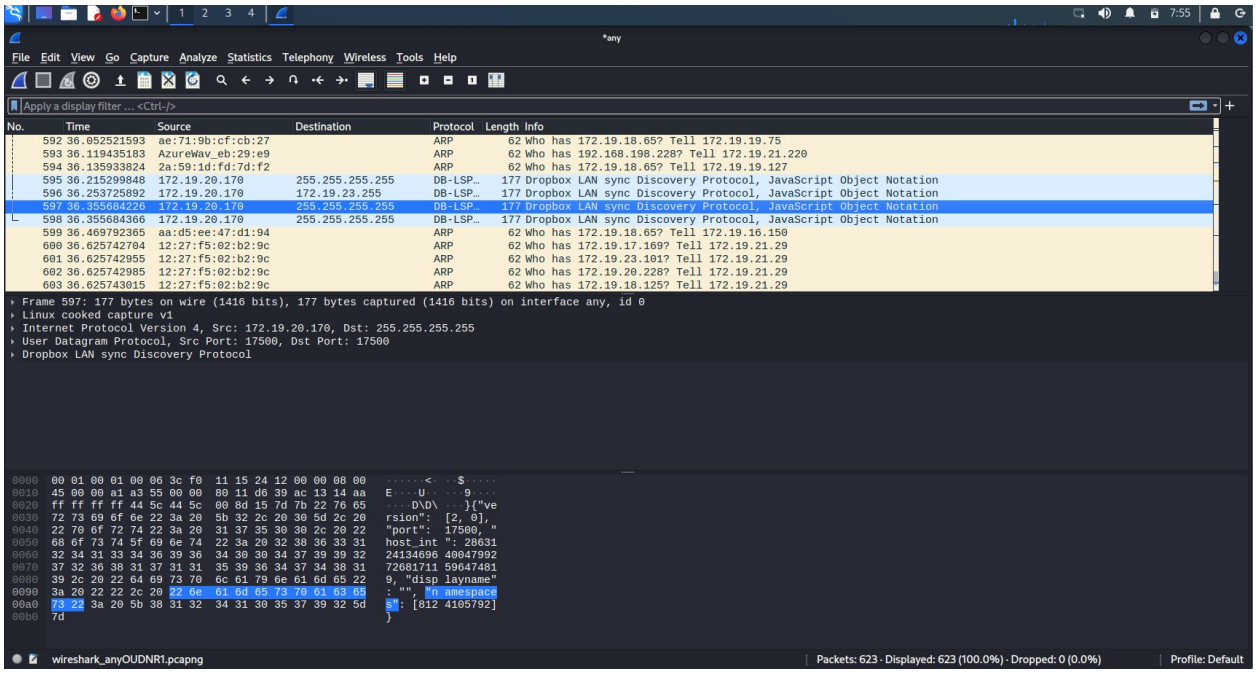
Now, moving on to Wireshark



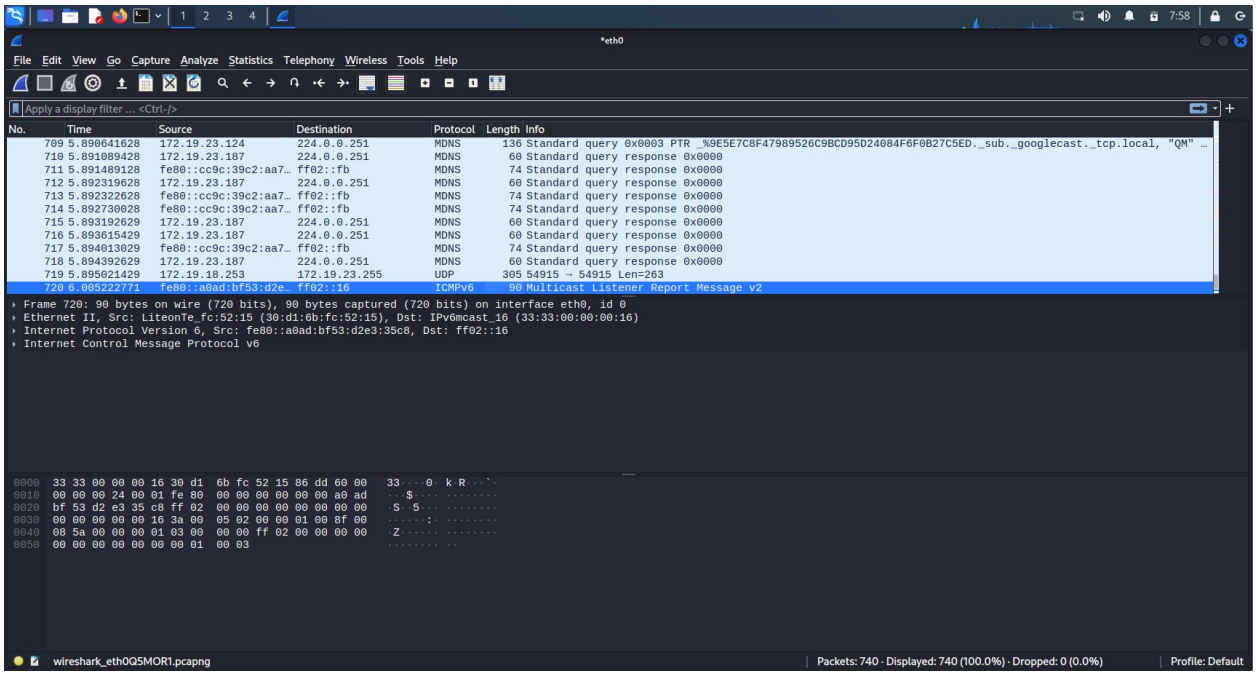
Opening wireshark greets us with this dashboard



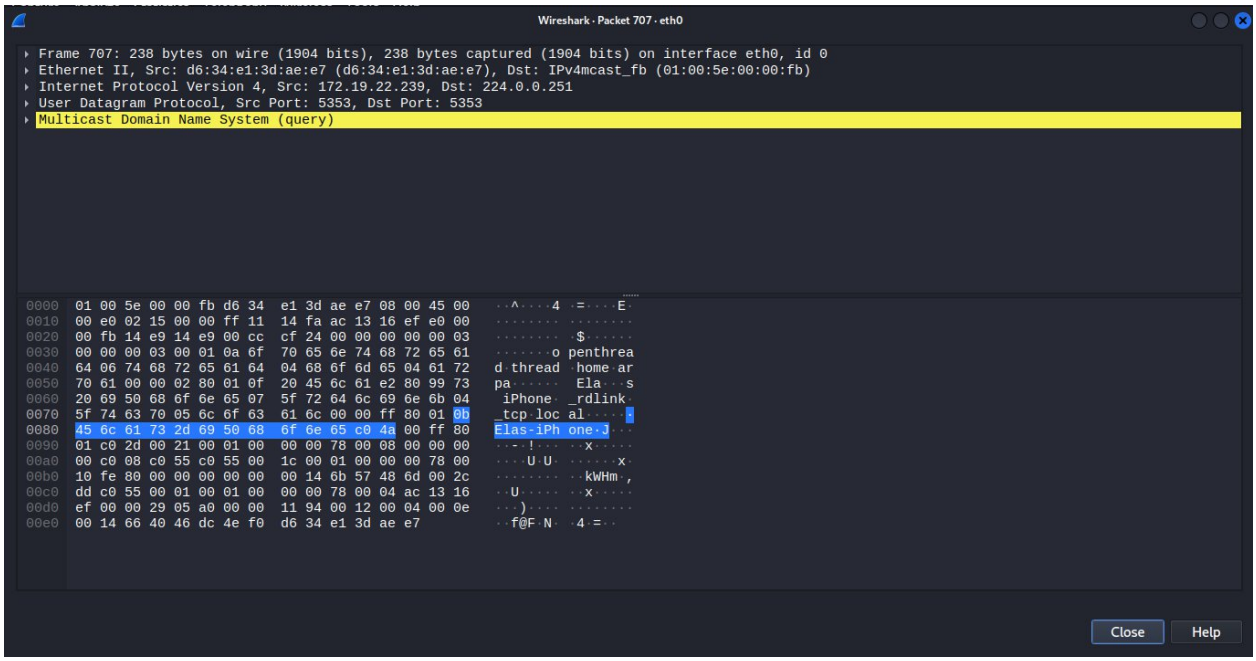
Starting capture of data packets lets us see the data packets travelling and their details

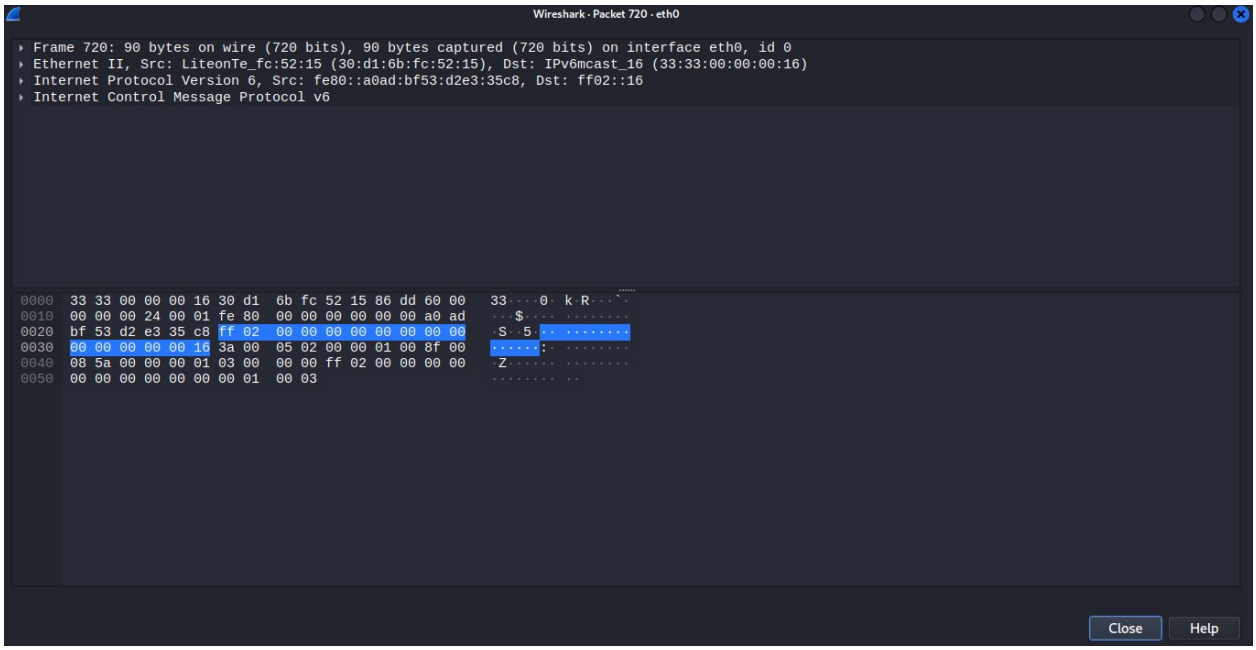


Selecting a data packet lets you know its contents



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:**
   a. **Overview**
      We have to read, write, and manipulate image, audio, video, and PDF metadata.
   b. **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
   c. **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
   d. **Algorithm (Step by Step Approach)**
      No algorithms were used
9. **Implementation Details:**
   a. **In case of programming implementation: Please add source code**
      No programming was done.
   b. **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

```
PS C:\Users\Shalom> cd "C:\Users\Shalom\Downloads\exiftool-12.45"
PS C:\Users\Shalom\Downloads\exiftool-12.45> .\exiftool -v C:\Users\Shalom\Desktop\contract.sol
  ExifToolVersion = 12.45
  FileName = contract.sol
  Directory = C:/Users/Shalom/Desktop
  FileSize = 1515
  FileModifyDate = 1662629628
  FileAccessDate = 1663758383.69242
  FileCreateDate = 1662649477.22618
  FilePermissions = 33206
  FileType = TXT
  FileTypeExtension = TXT
  MIMEType = text/plain
  MIMEEncoding = us-ascii
  Newlines = ..
  LineCount = 51
  WordCount = 164
```

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

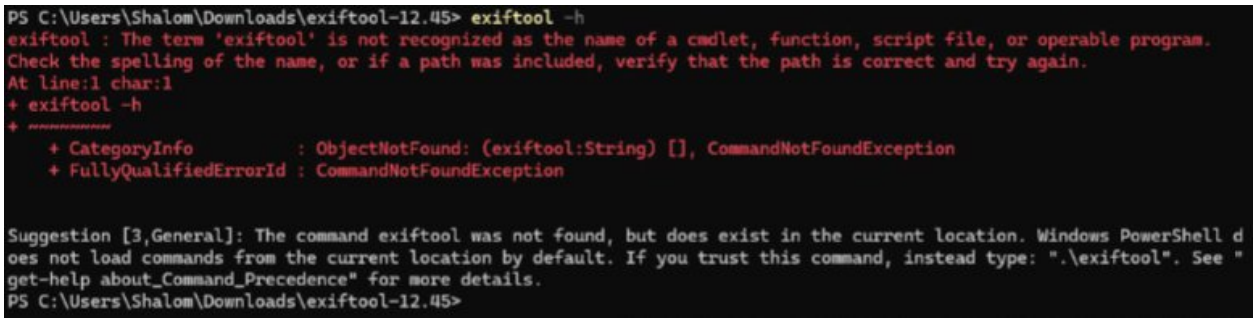
```
PS C:\Users\Shalom\Downloads\exiftool-12.45> .\exiftool C:\Users\Shalom\Desktop\contract.sol
ExifTool Version Number         : 12.45
File Name                       : contract.sol
Directory                       : C:/Users/Shalom/Desktop
File Size                       : 1515 bytes
File Modification Date/Time     : 2022:09:08 15:03:48+05:30
File Access Date/Time           : 2022:09:21 16:41:02+05:30
File Creation Date/Time         : 2022:09:08 20:34:37+05:30
File Permissions                : -rw-rw-rw-
File Type                       : TXT
File Type Extension             : txt
MIME Type                       : text/plain
MIME Encoding                   : us-ascii
Newlines                        : Windows CRLF
Line Count                      : 51
Word Count                      : 164
```

```
PS C:\Users\Shalom\Downloads\exiftool-12.45> .\exiftool -h C:\Users\Shalom\Desktop\contract.sol
<!-- C:/Users/Shalom/Desktop/contract.sol -->
<table>
<tr><td>ExifTool Version Number</td><td>12.45</td></tr>
<tr><td>File Name</td><td>contract.sol</td></tr>
<tr><td>Directory</td><td>C:/Users/Shalom/Desktop</td></tr>
<tr><td>File Size</td><td>1515 bytes</td></tr>
<tr><td>File Modification Date/Time</td><td>2022:09:08 15:03:48+05:30</td></tr>
<tr><td>File Access Date/Time</td><td>2022:09:21 16:41:07+05:30</td></tr>
<tr><td>File Creation Date/Time</td><td>2022:09:08 20:34:37+05:30</td></tr>
<tr><td>File Permissions</td><td>-rw-rw-rw-</td></tr>
<tr><td>File Type</td><td>TXT</td></tr>
<tr><td>File Type Extension</td><td>txt</td></tr>
<tr><td>MIME Type</td><td>text/plain</td></tr>
<tr><td>MIME Encoding</td><td>us-ascii</td></tr>
<tr><td>Newlines</td><td>Windows CRLF</td></tr>
<tr><td>Line Count</td><td>51</td></tr>
<tr><td>Word Count</td><td>164</td></tr>
</table>
```

```
PS C:\Users\Shalom\Downloads\exiftool-12.45> .\exiftool -h C:\Users\Shalom\Desktop\th-259025762.jpg
<!-- C:/Users/Shalom/Desktop/th-259025762.jpg -->
<table>
<tr><td>ExifTool Version Number</td><td>12.45</td></tr>
<tr><td>File Name</td><td>th-259025762.jpg</td></tr>
<tr><td>Directory</td><td>C:/Users/Shalom/Desktop</td></tr>
<tr><td>File Size</td><td>96 kB</td></tr>
<tr><td>Zone Identifier</td><td>Exists</td></tr>
<tr><td>File Modification Date/Time</td><td>2022:08:21 18:32:14+05:30</td></tr>
<tr><td>File Access Date/Time</td><td>2022:09:21 17:09:57+05:30</td></tr>
<tr><td>File Creation Date/Time</td><td>2022:08:21 18:32:14+05:30</td></tr>
<tr><td>File Permissions</td><td>-rw-rw-rw-</td></tr>
<tr><td>File Type</td><td>JPEG</td></tr>
<tr><td>File Type Extension</td><td>jpg</td></tr>
<tr><td>MIME Type</td><td>image/jpeg</td></tr>
<tr><td>JFIF Version</td><td>1.01</td></tr>
<tr><td>Resolution Unit</td><td>inches</td></tr>
<tr><td>X Resolution</td><td>0</td></tr>
<tr><td>Y Resolution</td><td>0</td></tr>
<tr><td>Exif Byte Order</td><td>Big-endian (Motorola, MM)</td></tr>
<tr><td>Image Width</td><td>474</td></tr>
<tr><td>Image Height</td><td>1030</td></tr>
<tr><td>Encoding Process</td><td>Baseline DCT, Huffman coding</td></tr>
<tr><td>Bits Per Sample</td><td>8</td></tr>
<tr><td>Color Components</td><td>3</td></tr>
<tr><td>Y Cb Cr Sub Sampling</td><td>YCbCr4:2:0 (2 2)</td></tr>
<tr><td>Image Size</td><td>474x1030</td></tr>
<tr><td>Megapixels</td><td>0.488</td></tr>
</table>
```

10. Error Description:

Had to use .\exiftool instead of exiftool



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

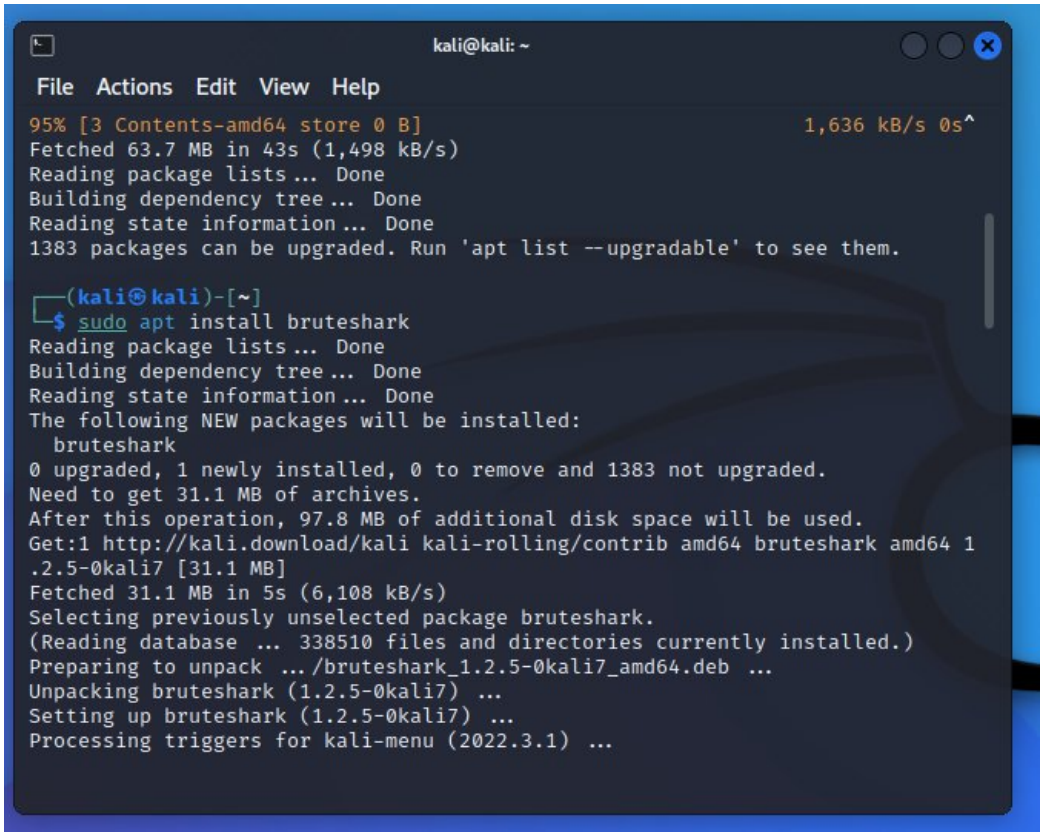
12. Reference:

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

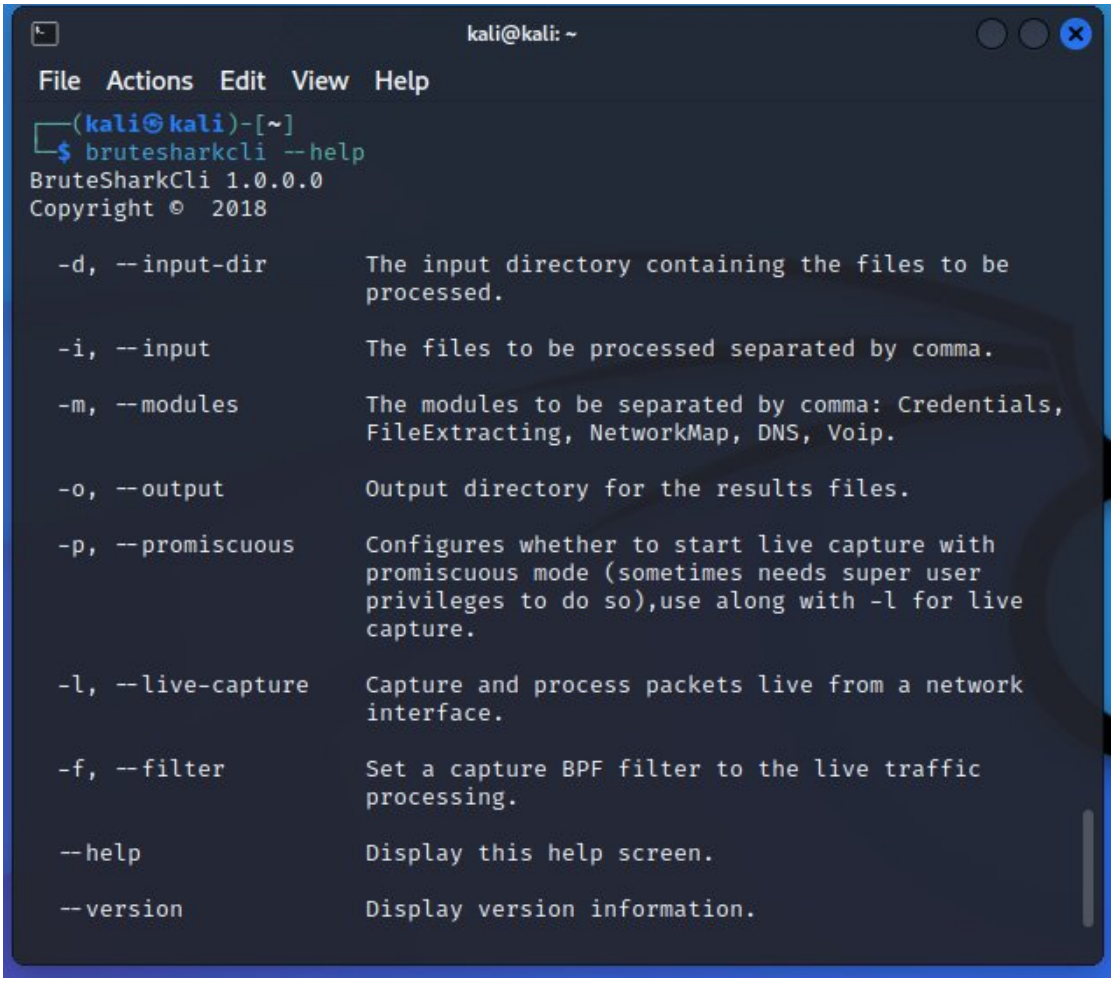
https://twistandclick.com/2022/02/03/using-exiftool-a-beginners-guide/

Lab Assignment 4

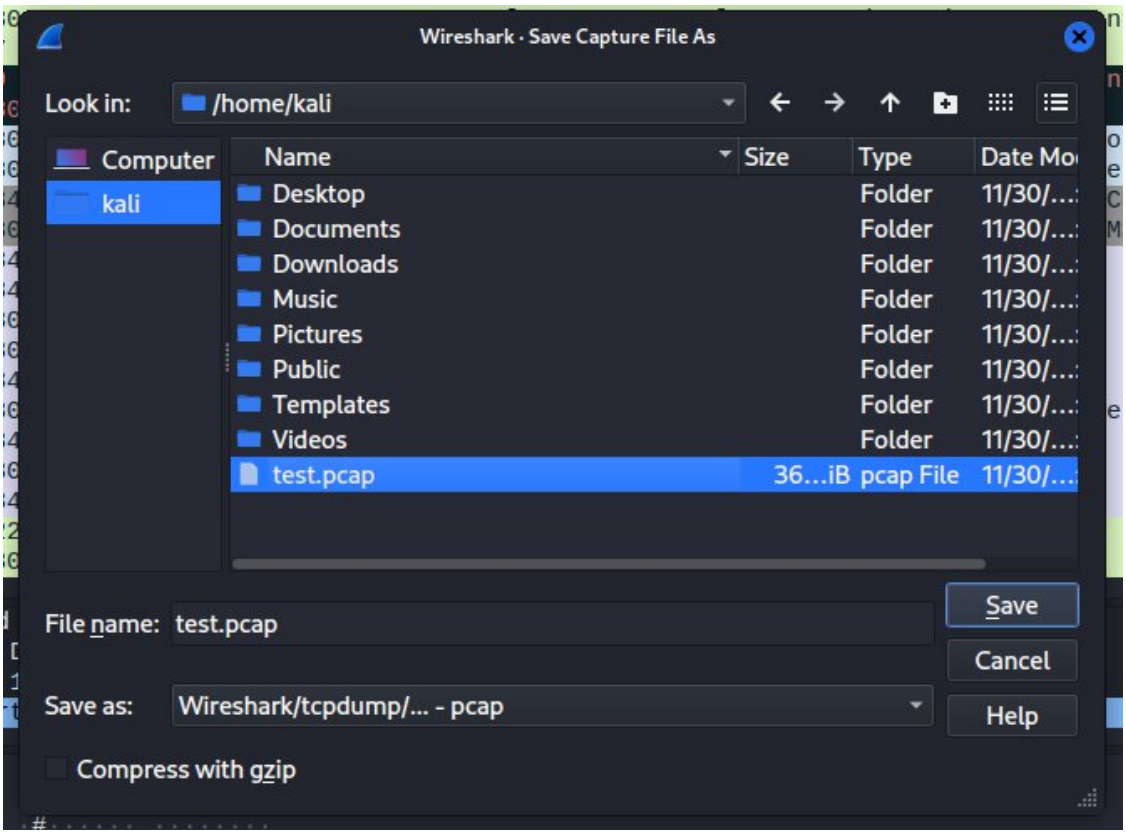
1. **Student Name:** G Shalom Shreyan
2. **Student Email ID:** gshalom.shreyan19@st.niituniversity.in
3. **Program/Experiment Number:** 4
4. **Title of the Program/Experiment:** BruteShark & LiveForensicator
5. **Date Program/Experiment Performed:** 28/09/2022
6. **Date Report Submitted:** 30/11/2022
7. **Objective:** To analyze network traffic using BruteShark & gather system information using LiveForensicator
8. **Description:**
   a. **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.
   b. **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
   c. **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
   d. **Algorithm (Step by Step Approach)**
   No algorithms were used
9. **Implementation Details:**
   a. **In case of programming implementation: Please add source code**
   No programming was done.
   b. **In case of software installation: Please add screenshots. (Step by Step)**
   Install Bruteshark in a Linux Machine



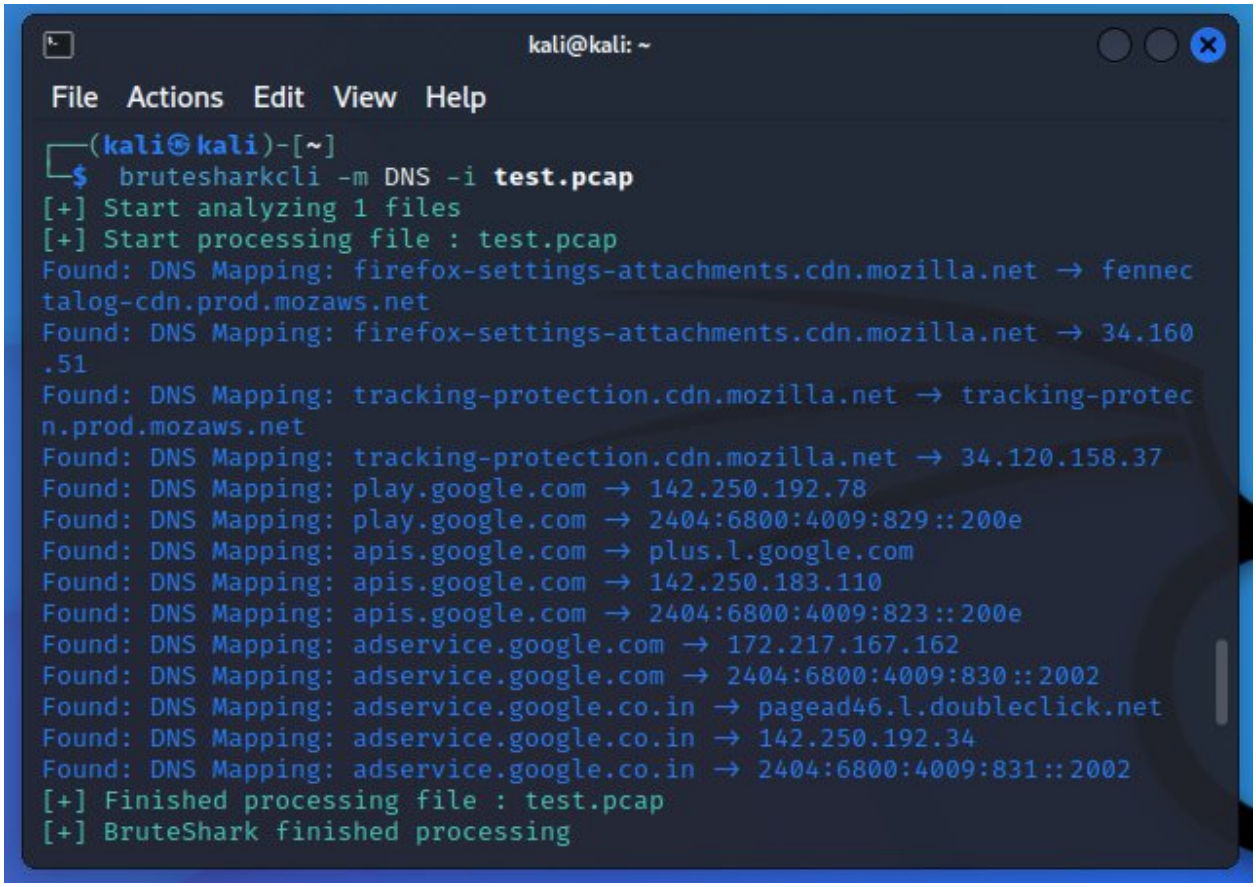
Use the help function to see how to use it



Get PCAP file after analyzing network traffic using Wireshark



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

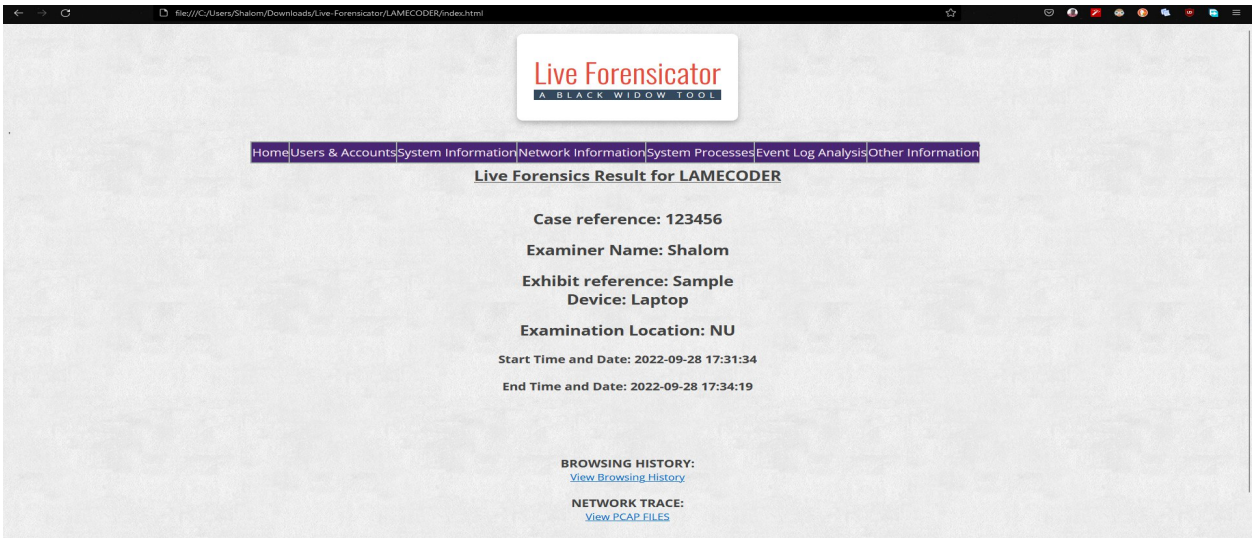


```
┌──(kali㉿kali)-[~]
└─$ sudo brutesharkcli -m voip -l eth0
[+] Started analyzing packets from eth0 device - Press Ctrl + C to stop
```

```
┌──(kali㉿kali)-[~]
└─$ sudo brutesharkcli -m DNS -l eth0 -p
[+] Started analyzing packets from eth0 device (Promiscuous mode) - Press Ctrl + C to s
top
Found: DNS Mapping: push.services.mozilla.com → autopush.prod.mozaws.net
Found: DNS Mapping: push.services.mozilla.com → 34.214.236.46
Found: DNS Mapping: push.services.mozilla.com → 52.13.173.34
Found: DNS Mapping: push.services.mozilla.com → 54.148.84.125
Found: DNS Mapping: example.org → 93.184.216.34
Found: DNS Mapping: ipv4only.arpa → 192.0.0.171
Found: DNS Mapping: ipv4only.arpa → 192.0.0.170
Found: DNS Mapping: example.org → 2606:2800:220:1:248:1893:25c8:1946
Found: DNS Mapping: detectportal.firefox.com → detectportal.prod.mozaws.net
Found: DNS Mapping: detectportal.firefox.com → prod.detectportal.prod.cloudops.mozgcp.
net
Found: DNS Mapping: detectportal.firefox.com → 34.107.221.82
Found: DNS Mapping: detectportal.firefox.com → 2600:1901:0:38d7::
Found: DNS Mapping: push.services.mozilla.com → 35.160.184.41
Found: DNS Mapping: push.services.mozilla.com → 54.148.69.31
Found: DNS Mapping: push.services.mozilla.com → 34.218.168.248
Found: DNS Mapping: push.services.mozilla.com → 54.186.169.128
```

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



Home | Users & Accounts | System Information | Network Information | System Processes | Event Log Analysis | Other Information

PROCESSES | SCHEDULED TASK | REGISTRY

▾ Processes

Handles	StartTime	PM	VM	SI	Id	ProcessName	Path	Product	FileVersion
173	28-09-2022 17:17:38	2138112	4408770560	3	13500	ACCIMonitor	C:\Windows\System32\ASUSACCI\ACCIMonitor.exe	Armoury Crate Control Interface Monitor	1.0.0.0
418	28-09-2022 10:08:39	25677824	298315776	3	17180	AcPowerNotification	C:\Program Files (x86)\ASUS\ArmouryDevice\dll\AcPowerNotification\AcPowerNotification.exe	AcPowerNotification	1.0.5.12
209	28-09-2022 11:18:26	2772992	88027136	3	13792	adb	C:\Users\Shalom\AppData\Local\Android\sdk\platform-tools\adb.exe		
93	26-09-2022 15:43:02	1019904	22033758085120	0	7016	AggregatorHost	C:\Windows\System32\AggregatorHost.exe		
299	28-09-2022 10:52:48	3530752	105652224	3	1896	Amazon Music Helper	C:\Program Files\WindowsApps\AmazonMobileLLC.AmazonMusic_9.2.1.0_x86__kc6t79cpj4tp0\Amazon Music Helper.exe	Amazon Music Helper	9.2.1.2362
145	26-09-2022 15:43:00	2449408	4389457920	0	2760	amdfendrsr	C:\Windows\System32\amdfendrsr.exe	AMD Crash Defender Service	21.30.0.16
611	28-09-2022 10:09:45	35774464	2203644669952	3	17092	ApplicationFrameHost	C:\Windows\system32\ApplicationFrameHost.exe	Microsoft® Windows® Operating System	10.0.22000.1 (WinBuild.160101.0800)
194	28-09-2022 10:08:57	2494464	4420640768	3	17104	ArmouryCrate.DenoiseAI	C:\Program Files\ASUS\ARMOURY CRATE Service\DenoiseAIPlugin\ArmouryCrate.DenoiseAI.exe	ARMOURY CRATE DenoiseAI	1.0.0.1
1604	26-09-2022 15:43:02	115912704	5140914176	0	4912	ArmouryCrate.Service	C:\Program Files\ASUS\ARMOURY CRATE Service\ArmouryCrate.Service.exe	ARMOURY CRATE Service	5.2.5.0
11892	28-09-2022 10:08:49	61775872	5163331584	3	11676	ArmouryCrate.UserSessionHelper	C:\Program Files\ASUS\ARMOURY CRATE Service\ArmouryCrate.UserSessionHelper.exe	ARMOURY CRATE Service	5.2.5.0
322	26-09-2022 15:43:02	2596864	4385001472	0	4884	ArmouryCrateControlInterface	C:\Windows\System32\ASUSACCI\ArmouryCrateControlInterface.exe	Armoury Crate Control Interface	1.0.0.20
276	28-09-2022 10:08:39	4595712	4449230848	3	24580	ArmourySocketServer	C:\Program Files (x86)\ASUS\ArmouryDevice\dll\ArmourySocketServer\ArmourySocketServer.exe	ArmourySocketServer	0.0.11.25
288	28-09-2022 10:09:04	14856192	239124480	3	9104	ArmourySwAgent	C:\Program Files (x86)\ASUS\ArmouryDevice\dll\SwAgent\ArmourySwAgent.exe	ArmourySwAgent	2.0.0.17
223	28-09-2022 10:08:39	1622016	4423852032	3	23732	AsHotplugCtrl	C:\Program Files\ASUS\ASUS Hotplug Controller\AsHotplugCtrl.exe	ASUS Hotplug Controller	2.0.0.0
460	28-09-2022 10:08:56	28180480	322383872	3	5044	asus_framework	C:\Program Files (x86)\ASUS\ArmouryDevice\asus_framework.exe	ASUS NodeJS Web Framework	3.1.0.2
277	28-09-2022 10:08:39	27918336	149217280	3	16820	asus_framework	C:\Program Files (x86)\ASUS\ArmouryDevice\asus_framework.exe	ASUS NodeJS Web Framework	3.1.0.2
319	26-09-2022 15:43:02	5730304	4457390080	0	4996	AsusAppService	C:\Windows\System32\DriverStore\FileRepository\asusscl2.inf_amd64_9d7f2049d0193da1\AsusAppService \AsusAppService.exe	ASUS App Service	1.0.15.0
158	26-09-2022 15:43:00	1835008	36429824	0	2768	AsusCertService	C:\Program Files (x86)\ASUS\AsusCertService\AsusCertService.exe	AsusCertService.exe	1.0.0.2

Home | Users & Accounts | System Information | Network Information | System Processes | Event Log Analysis | Other Information

User(s) Information

▾ Current User Information

*
LAMECODER\Shalom

▾ System Details

Name	DNSHostName	Domain	Manufacturer	Model	PrimaryOwnerName	TotalPhysicalMemory	Workgroup
LAMECODER	LameCoder	WORKGROUP	ASUSTeK COMPUTER INC.	ASUS TUF Gaming A17 FA707RM_FA707RM	Shalom	16371519488	WORKGROUP

▾ Logon Sessions

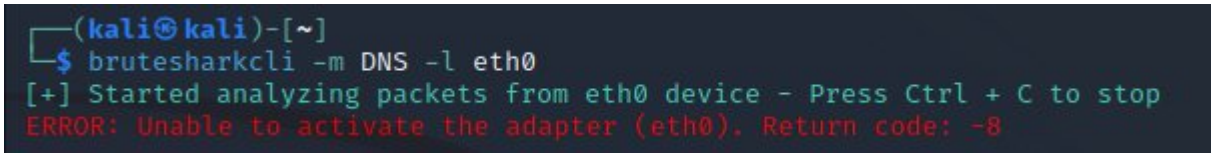
LogonID	LogonType	StartTime	Start Time
999	0	20220926154300.740055+330	26-09-2022 15:43:00
997	5	20220926154300.865056+330	26-09-2022 15:43:00
996	5	20220926154300.802554+330	26-09-2022 15:43:00
187655693	2	20220928100832.906433+330	28-09-2022 10:08:32
104205482	2	20220927141528.932973+330	27-09-2022 14:15:28
1053619	2	20220926154354.991712+330	26-09-2022 15:43:54
100485	2	20220926154300.849431+330	26-09-2022 15:43:00
187085221	2	20220928084300.046046+330	28-09-2022 08:43:00
67416	2	20220926154300.786932+330	26-09-2022 15:43:00
67381	2	20220926154300.786932+330	26-09-2022 15:43:00
187078483	2	20220928084300.002045+330	28-09-2022 08:43:00

▾ User Profile

Caption	LocalPath	SID	Last Used
	C:\Users\Shalom	S-1-5-21-1168329554-2931876401-1422521201-1001	28-09-2022 17:32:02
	C:\Windows\ServiceProfiles\NetworkService	S-1-5-20	28-09-2022 17:32:02
	C:\Windows\ServiceProfiles\LocalService	S-1-5-19	28-09-2022 17:32:02
	C:\Windows\system32\config\systemprofile	S-1-5-18	28-09-2022 17:32:02

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

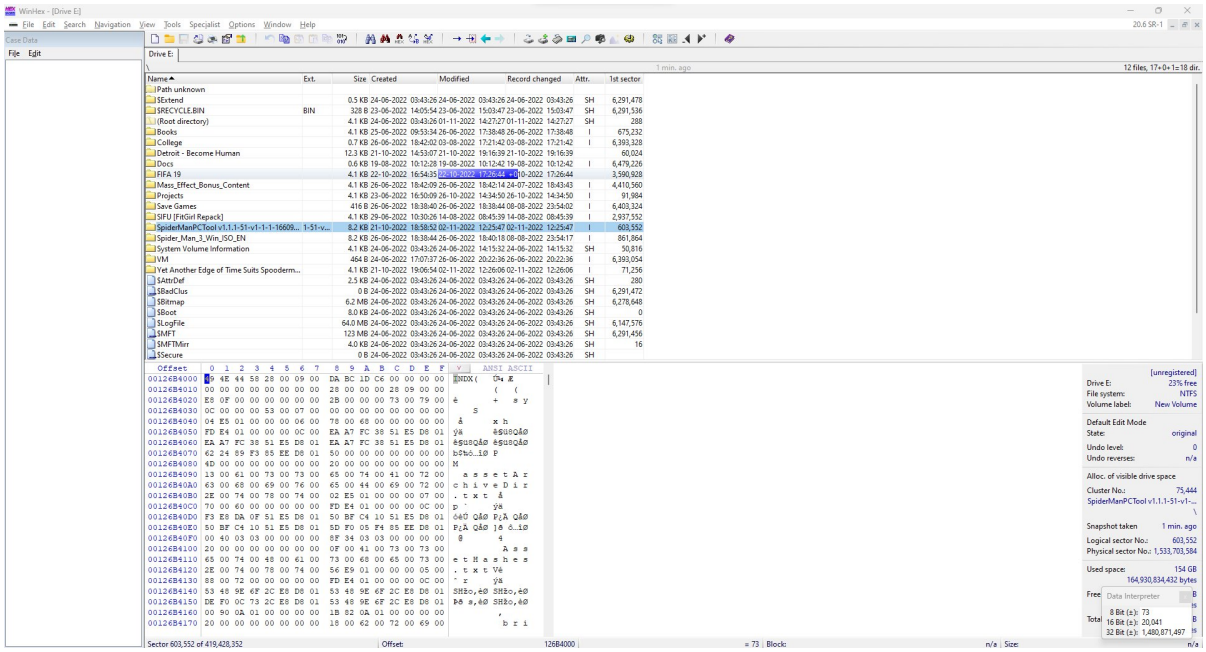
12. Reference:

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

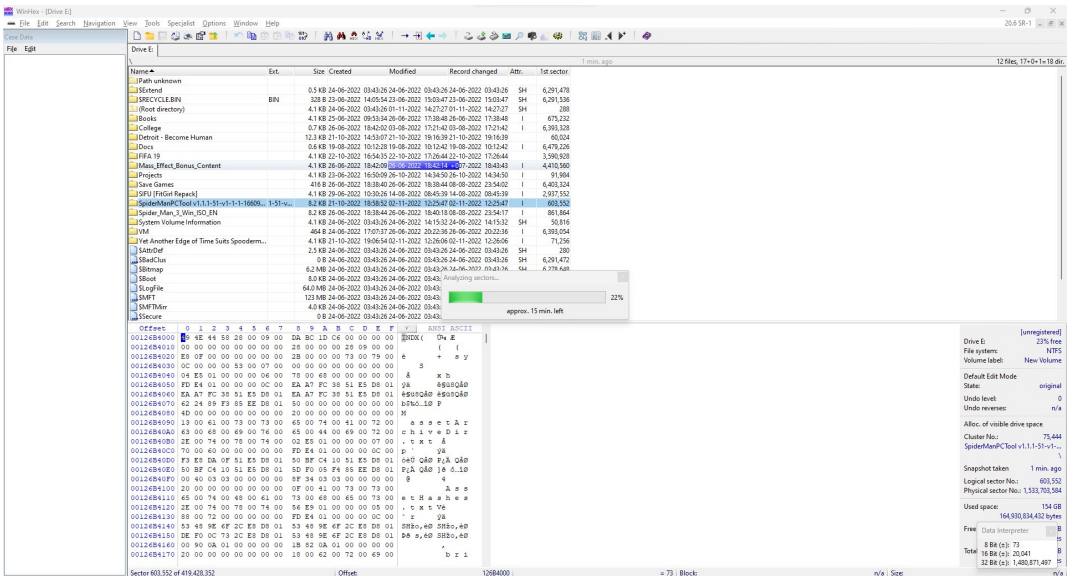
https://github.com/Johnng007/Live-Forensicator

Lab Assignment 5

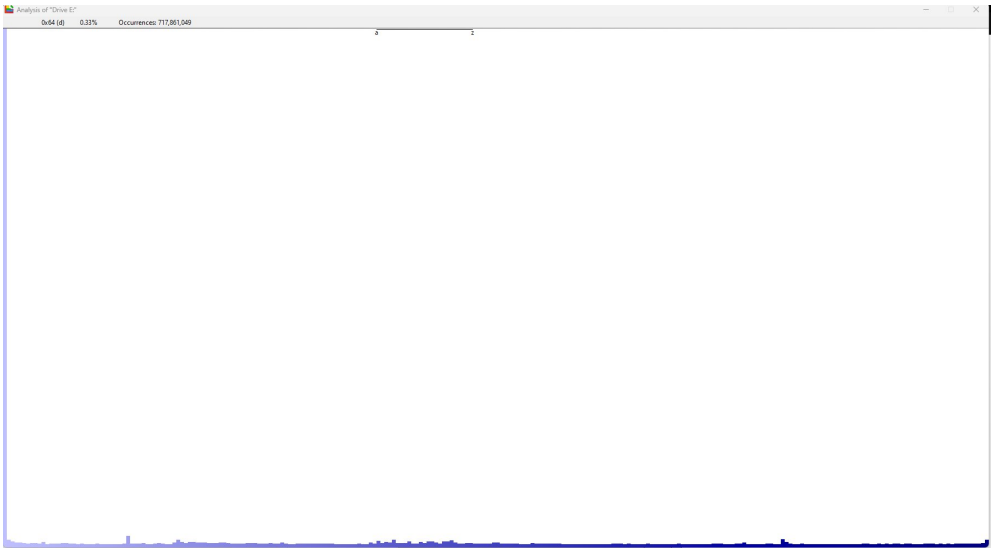
1. **Student Name:** G Shalom Shreyan
2. **Student Email ID:** gshalom.shreyan19@st.niituniversity.in
3. **Program/Experiment Number:** 5
4. **Title of the Program/Experiment:** WinHex tool
5. **Date Program/Experiment Performed:** 2/11/2022
6. **Date Report Submitted:** 30/11/2022
7. **Objective:** To edit hex values using winhex tool
8. **Description:**
   a. **Overview**
   We have to view and modify hex values using WinHex tool.
   b. **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
   c. **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
   d. **Algorithm (Step by Step Approach)**
   No algorithms were used
9. **Implementation Details:**
   a. In case of programming implementation: Please add source code
   No programming was done.
   b. In case of software installation: Please add screenshots. (Step by Step)
   Running WinHex and scanning a specific drive leads us to the below screenshot.



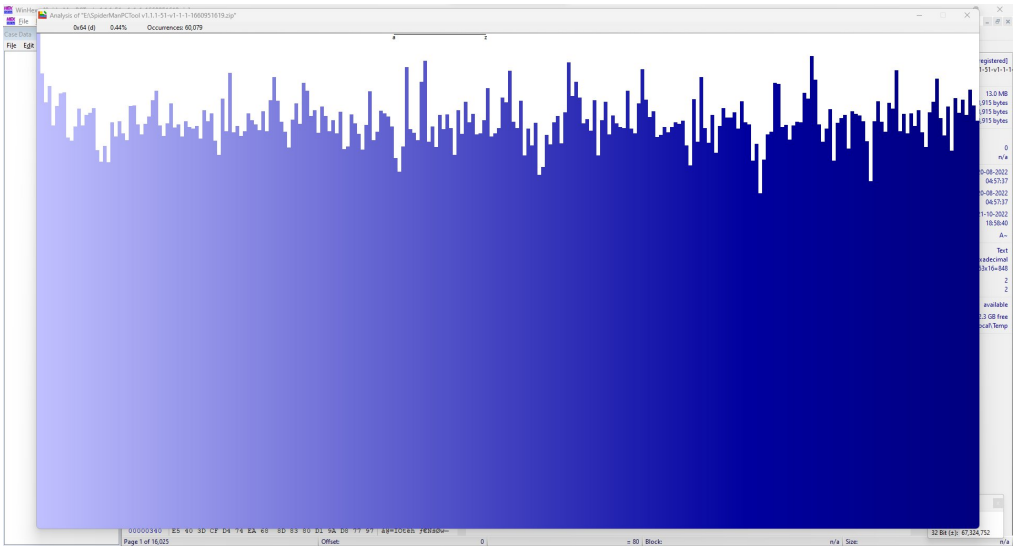
We can also specifically analyze a file



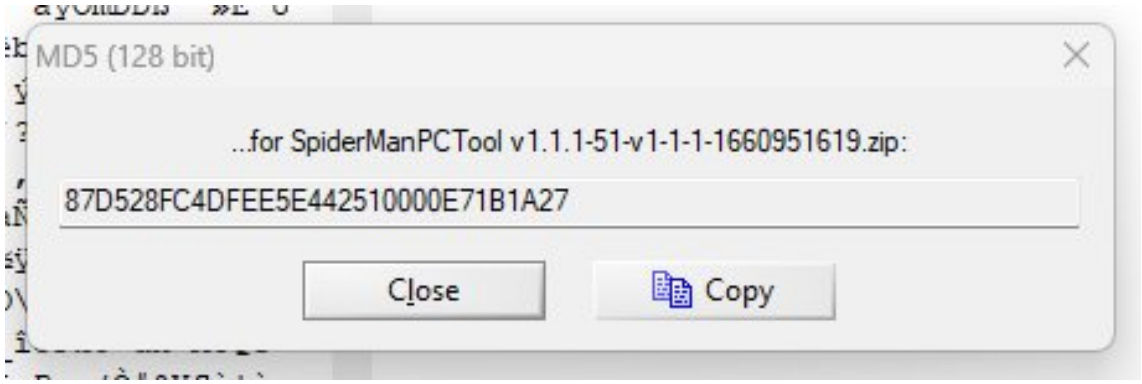
Analyzing the whole disk shows the below graph



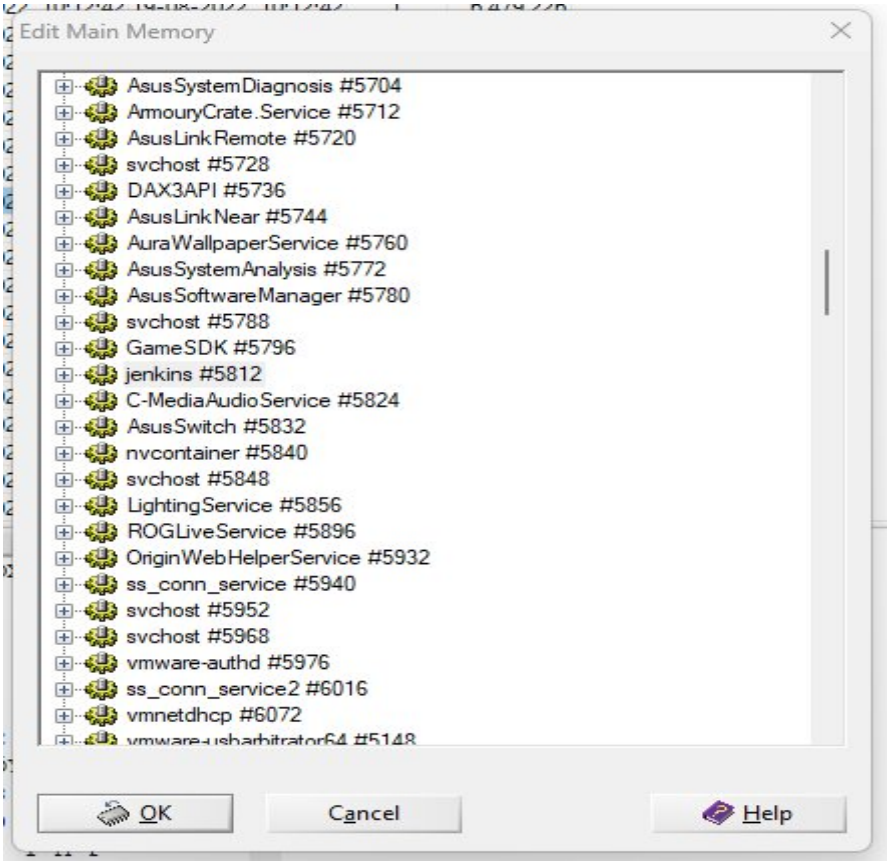
Analyzing a specific file shows the below graph



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

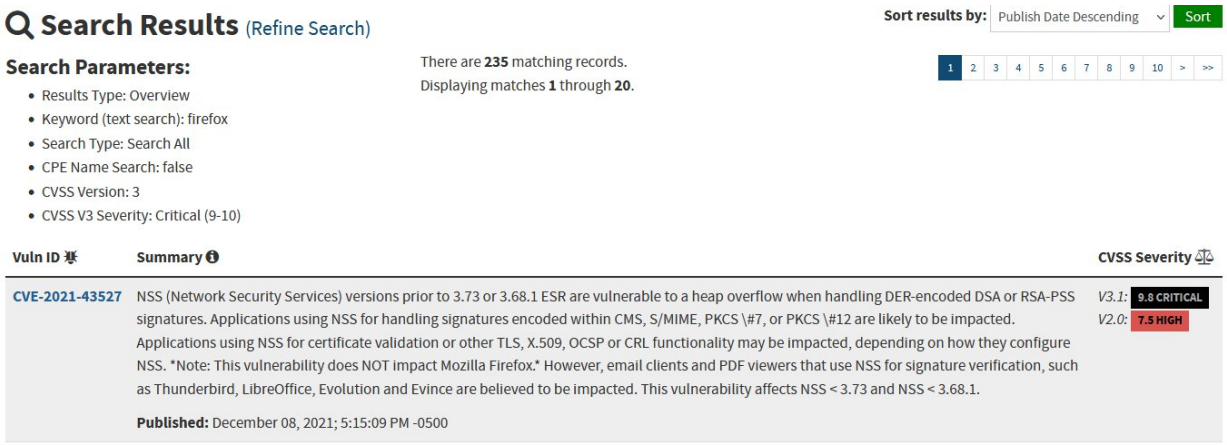
12. Reference:

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

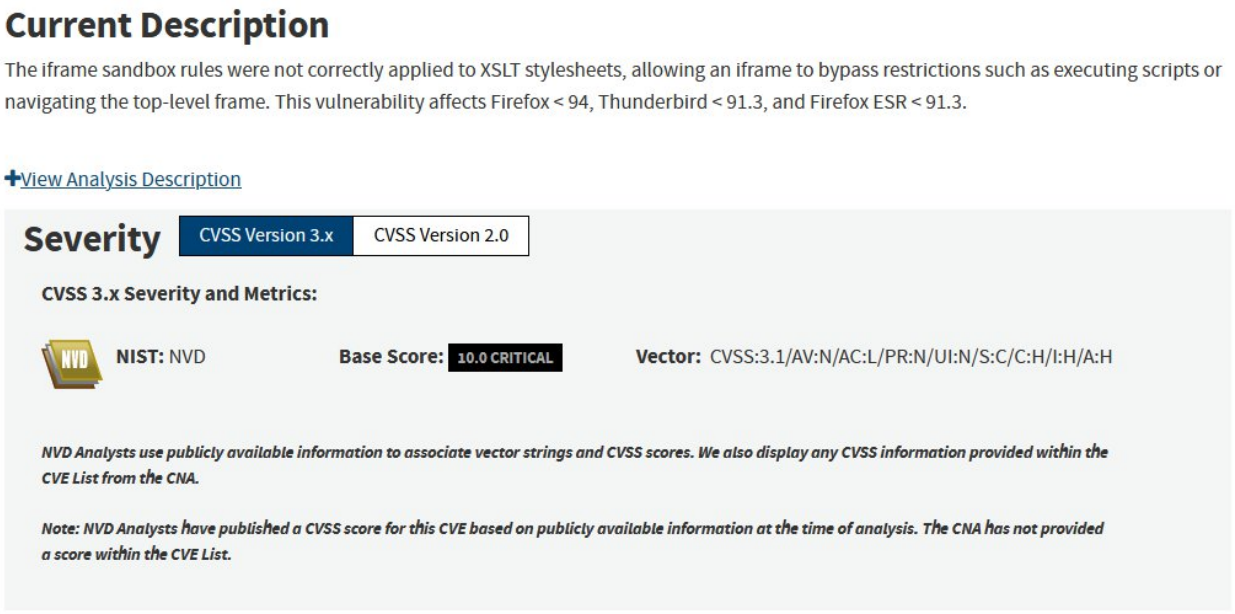
https://x-ways.net/winhex/analysis.html

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:**
   a. **Overview**
   We have to perform an attack on a browser like Chrome, Firefox, Edge and do forensic investigation
   b. **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
   c. **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
   d. **Algorithm (Step by Step Approach)**
   No algorithms were used
9. **Implementation Details:**
   a. In case of programming implementation: Please add source code
   No programming was done.
   b. 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

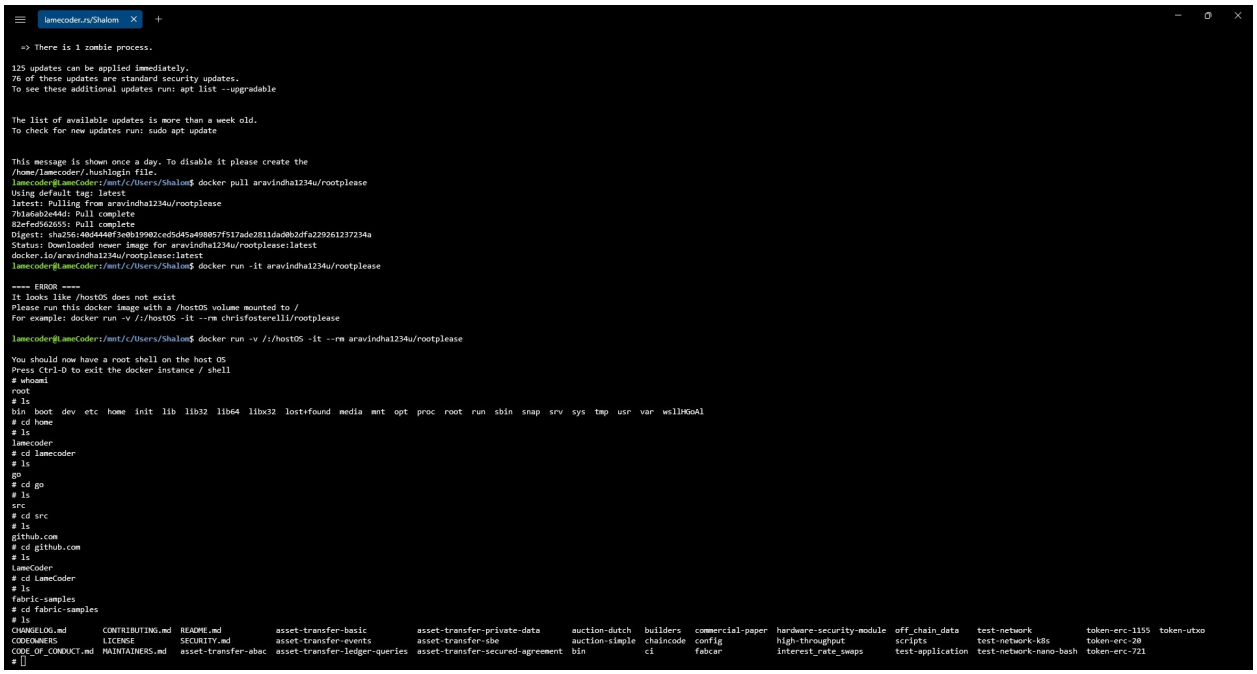
11. Conclusion: Browser forensics has successfully been completed

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

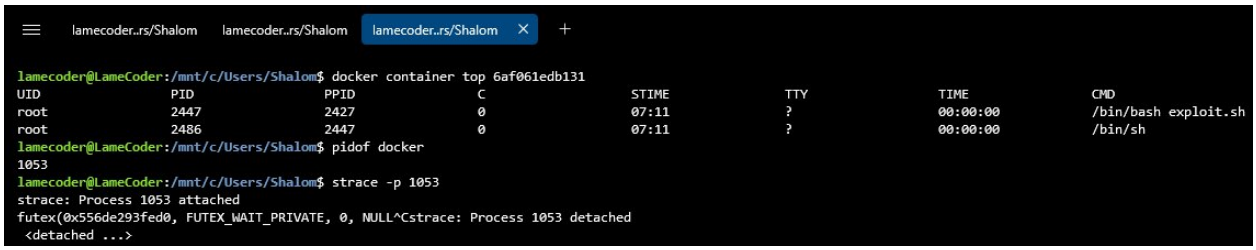
Lab Assignment 7

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:**
   a. **Overview**
      We have to perform an attack using a docker container and perform introspection & strace to find system calls.
   b. **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
   c. **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
   d. **Algorithm (Step by Step Approach)**
      No algorithms were used
9. **Implementation Details:**
   a. **In case of programming implementation: Please add source code**
      No programming was done.
   b. **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/