

Forensic Investigation Report

Investigation Title:

Forensic Analysis and Malware Investigation Report

Prepared For:

Cyborts

Prepared By:

Hamza Ali

Date:

05-July-2025

Confidentiality Notice:

This document contains sensitive information and is intended for authorized person only.

Table of Contents

1. Executive Summary
2. Introduction
3. Scope and Objectives
4. Methodology
5. Investigation Findings
 - 5.1 How was the system initially compromised?
 - 5.2 What evidence shows malware executed in memory only (file less)?
 - 5.3 What user activity helped the malware persist?
 - 5.4 What deleted or hidden files were staged for exfiltration?
 - 5.5 What browser activity suggests credential theft or staging?
 - 5.6 Can you build a precise attack timeline using event logs?
 - 5.7 What network artifacts indicate exfiltration?
 - 5.8 What malware behaviours and system changes were observed?

6. Chain of Custody

7. Conclusion

8. Recommendations and Mitigations

1. Executive Summary

This investigation simulates a phishing attack to analyse the initial compromise and subsequent malware activity on a Windows system. Using a combination of email analysis, memory forensics, registry examination, file recovery, browser artifact analysis, event log correlation, and network traffic inspection, we identified a file less malware infection that persisted through user activity and staged data for exfiltration. The report details the attack timeline, evidentiary artifacts, and provides actionable recommendations to mitigate similar threats in the future.

2. Introduction

The purpose of this investigation is to simulate and analyse a phishing-based compromise to understand the attack vectors, malware behaviour, and persistence mechanisms involved. This exercise aims to enhance detection and response capabilities by thoroughly examining system artifacts, memory, network traffic, and user activity. The investigation was conducted in a controlled environment with authorized access to ensure comprehensive forensic analysis.

3. Scope and Objectives

This digital forensics task aims to investigate a simulated cyberattack involving a phishing compromise, focusing on identifying the initial breach vector, malware behaviour, persistence mechanisms, and data exfiltration indicators. The objective is to apply forensic techniques on system artifacts, memory, network captures, and logs to reconstruct the attack timeline, uncover hidden or deleted evidence, and provide a comprehensive analysis of the malware's impact and persistence on the compromised system.

4. Methodology

The investigation employed a multi-faceted approach combining phishing simulation, forensic analysis, and malware behaviour examination. Tools such as Volatility were used for memory forensics, Autopsy and FTK for file recovery, and Wireshark for network traffic capture. Registry hives and browser artifacts were analysed to identify persistence and credential theft, while Windows event logs were correlated to build a precise attack timeline. All findings were documented with supporting evidence for a thorough understanding of the compromise.

5. Investigation Findings

5.1. How was the system initially compromised?

Create a malicious (.doc) file using MS Word

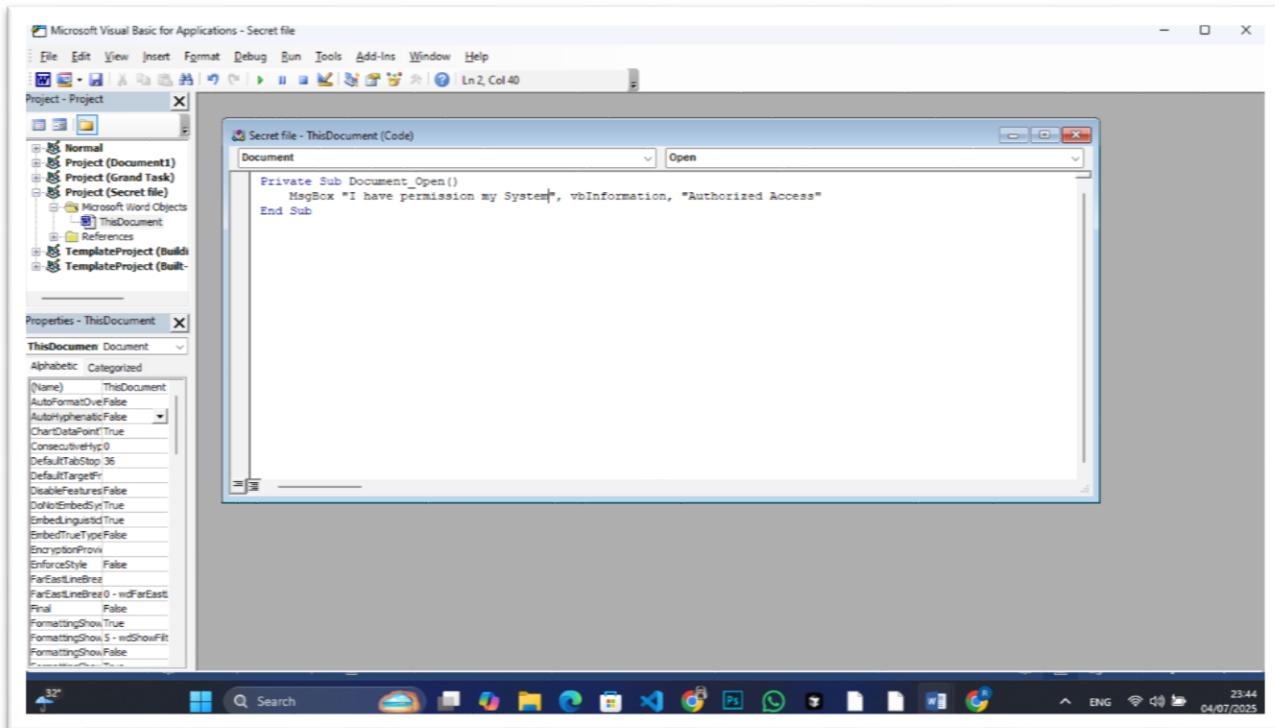


Figure 1 Creating a malicious (.doc) file using MS Word

Sending Mail

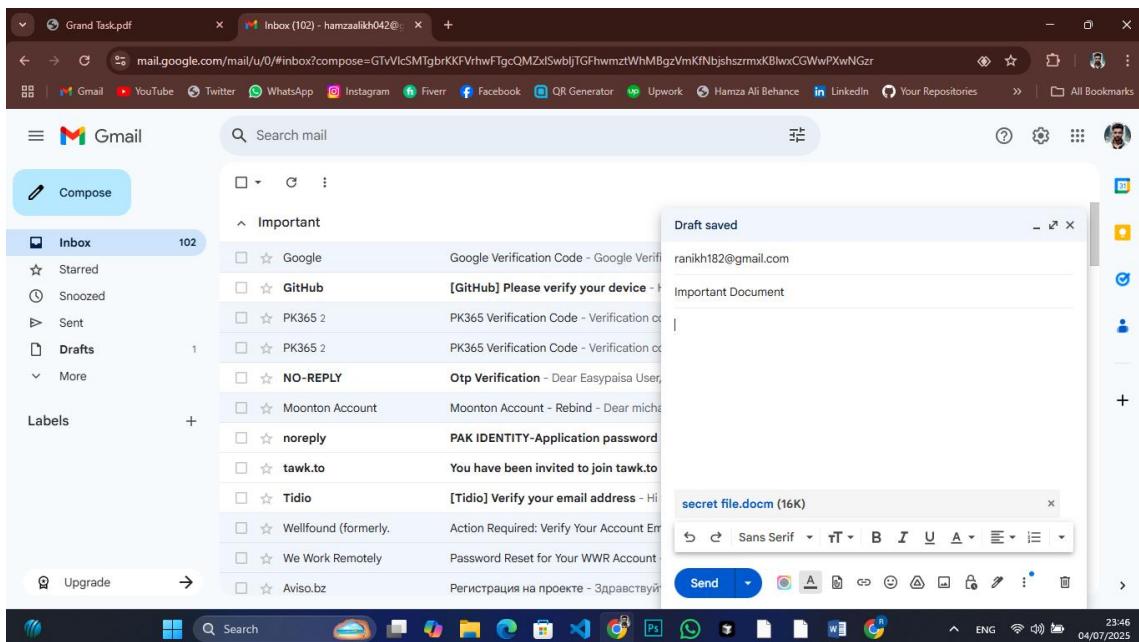


Figure 2 Sending Malicious (.doc) file through Email

Receiving Mail in Spam

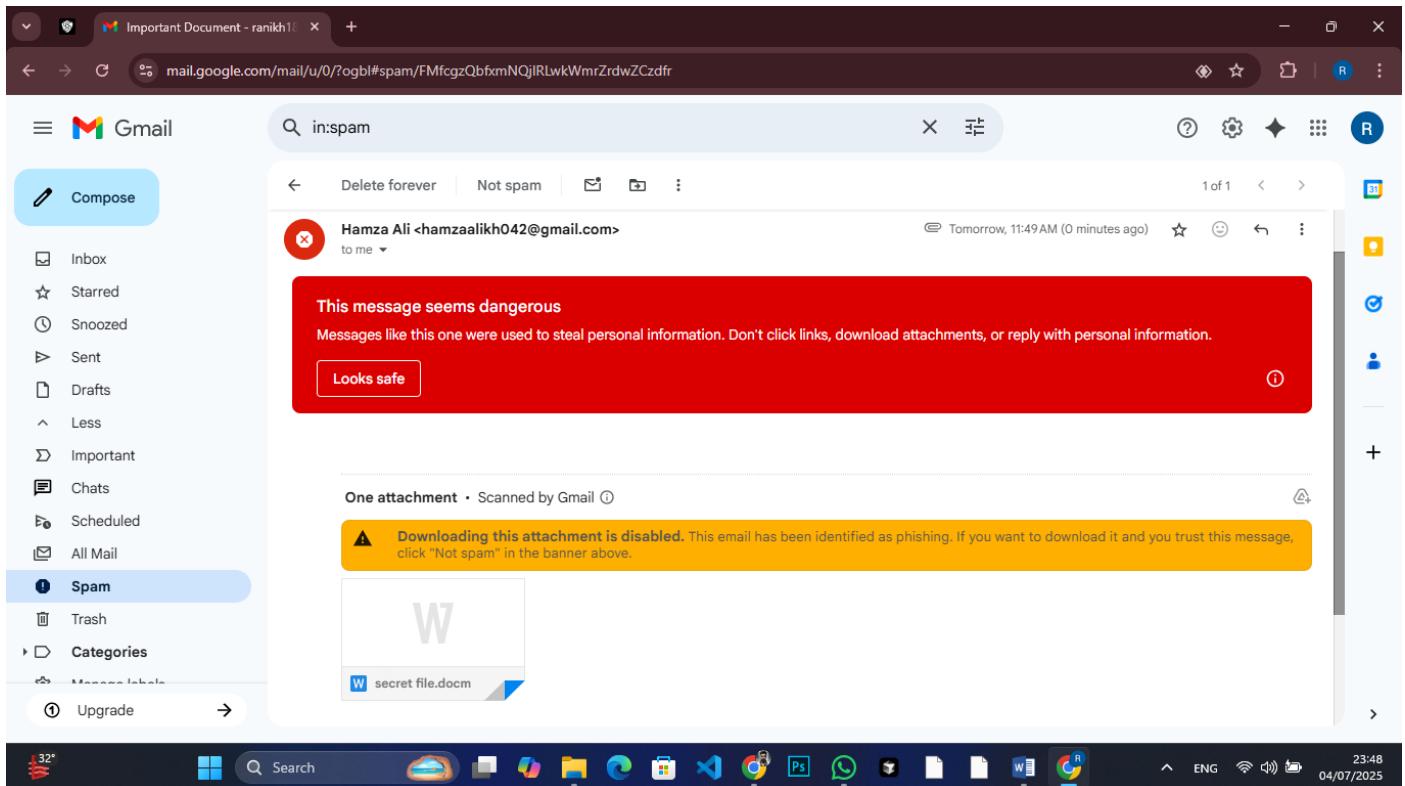


Figure 3 Receive malicious (.doc) file in spam

Check Sender Mail details and download (.eml) file for analysing

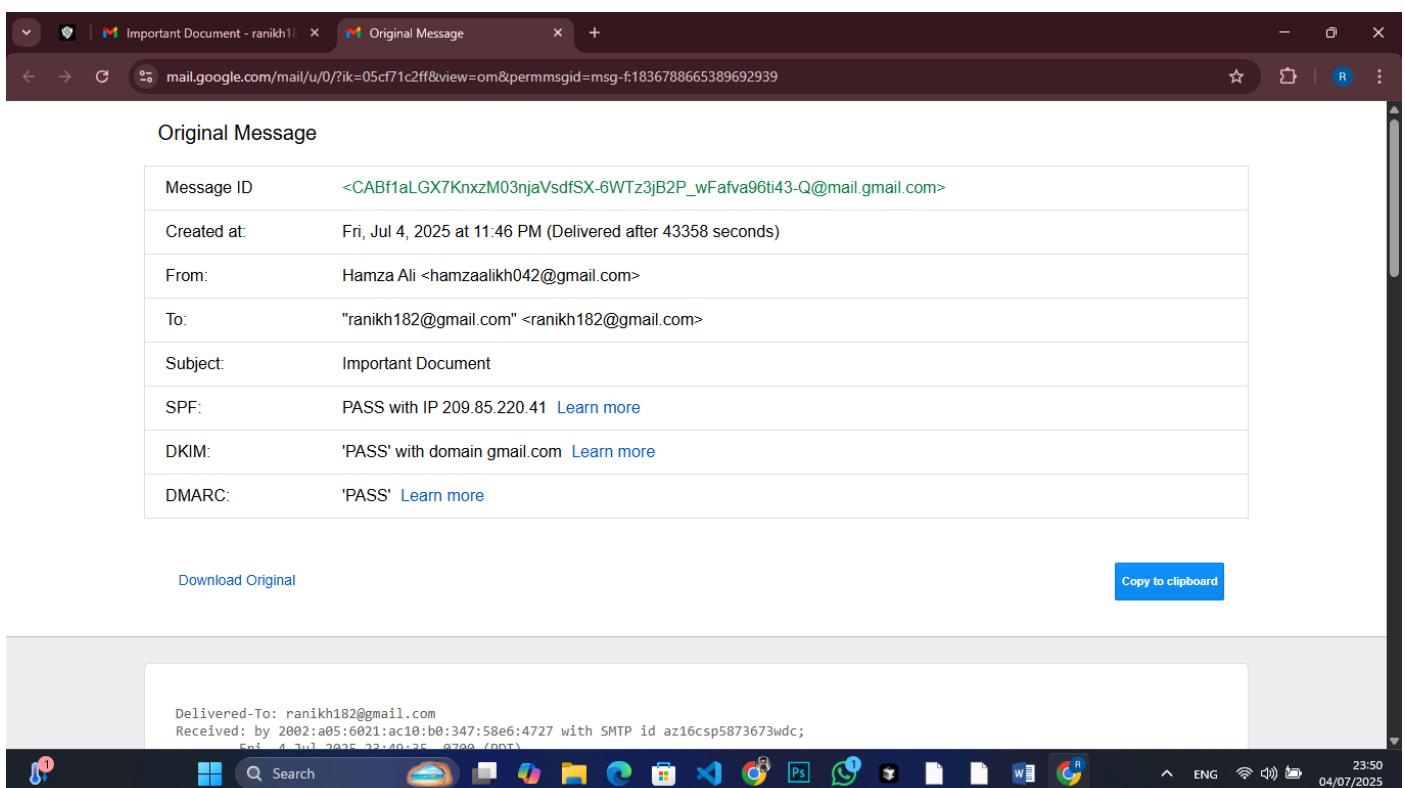


Figure 4 Sender Detail and download headers

SYSTool EML Viewer Analyze the Headers

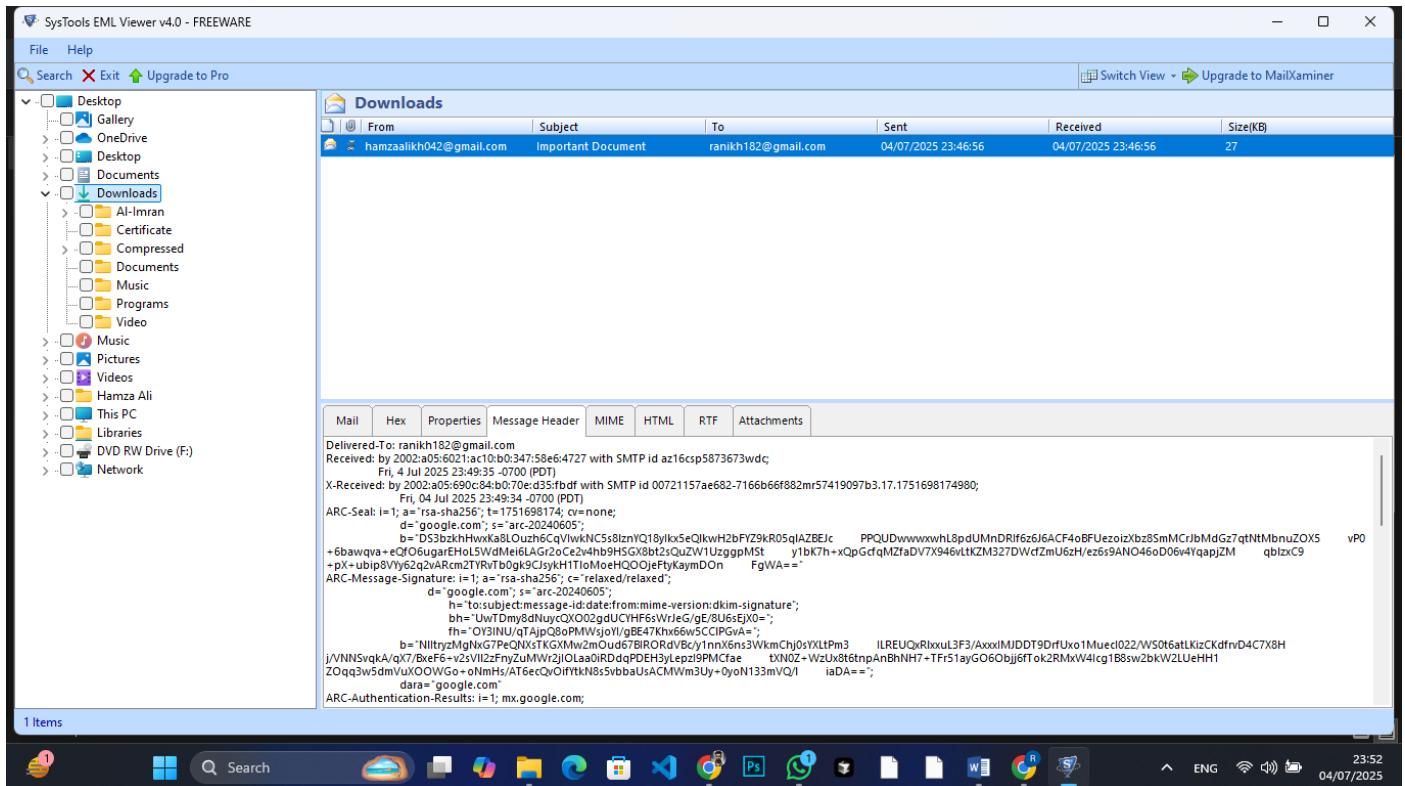


Figure 5 Email Header Analyze

Opening Malicious (.doc) file using word

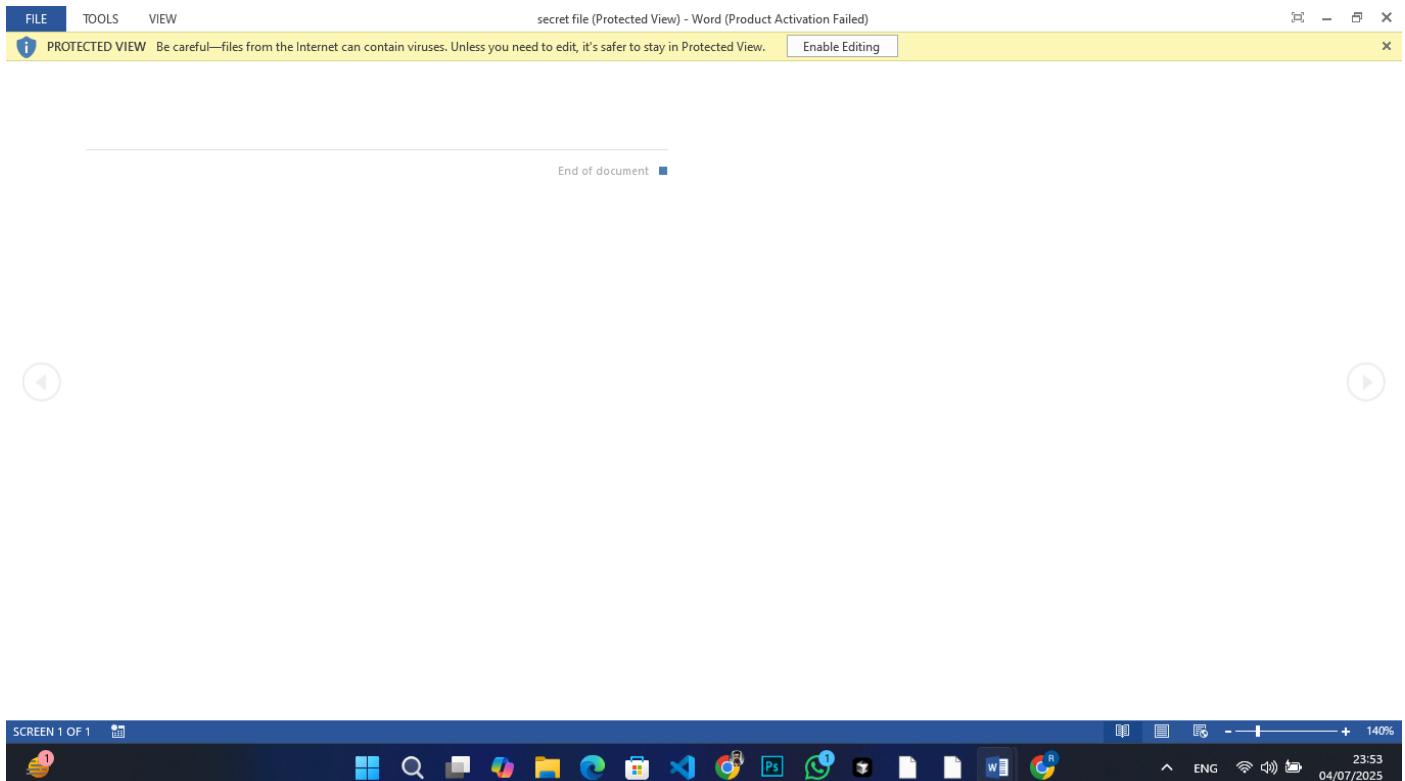


Figure 6 opening malicious (.doc) file

Show the message Malicious (.doc) file

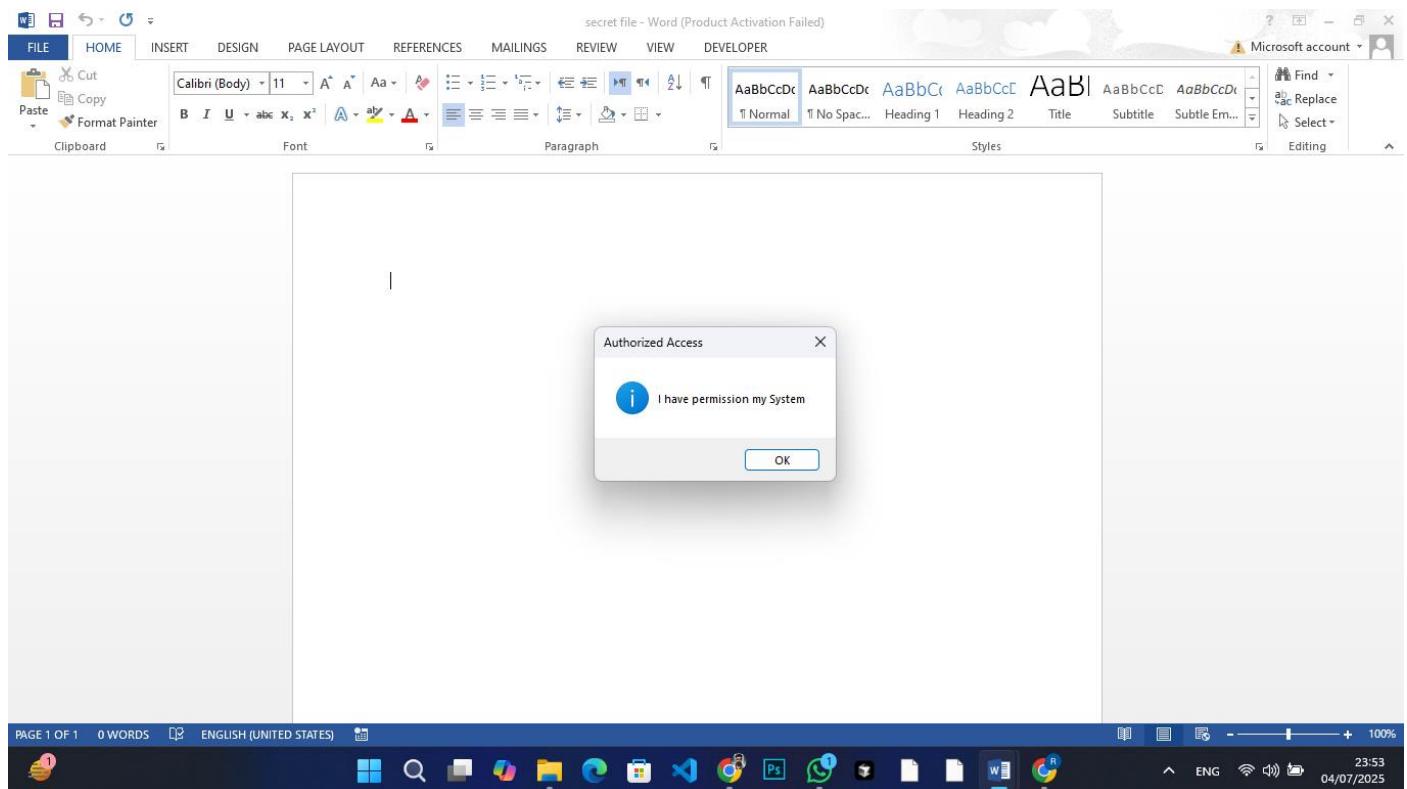


Figure 7 Malicious (.doc) File message

5.2 What evidence shows malware executed in memory only (fileless)?

Create a Memory dump file using FTK imager

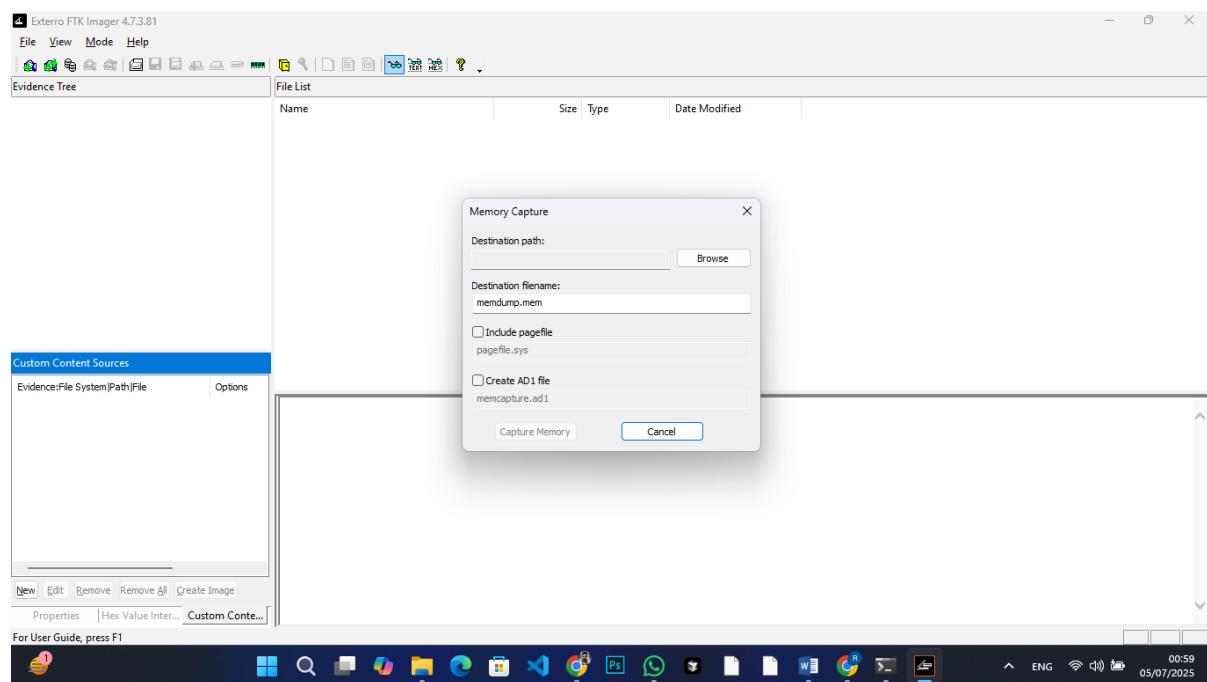


Figure 8 FTK Imager

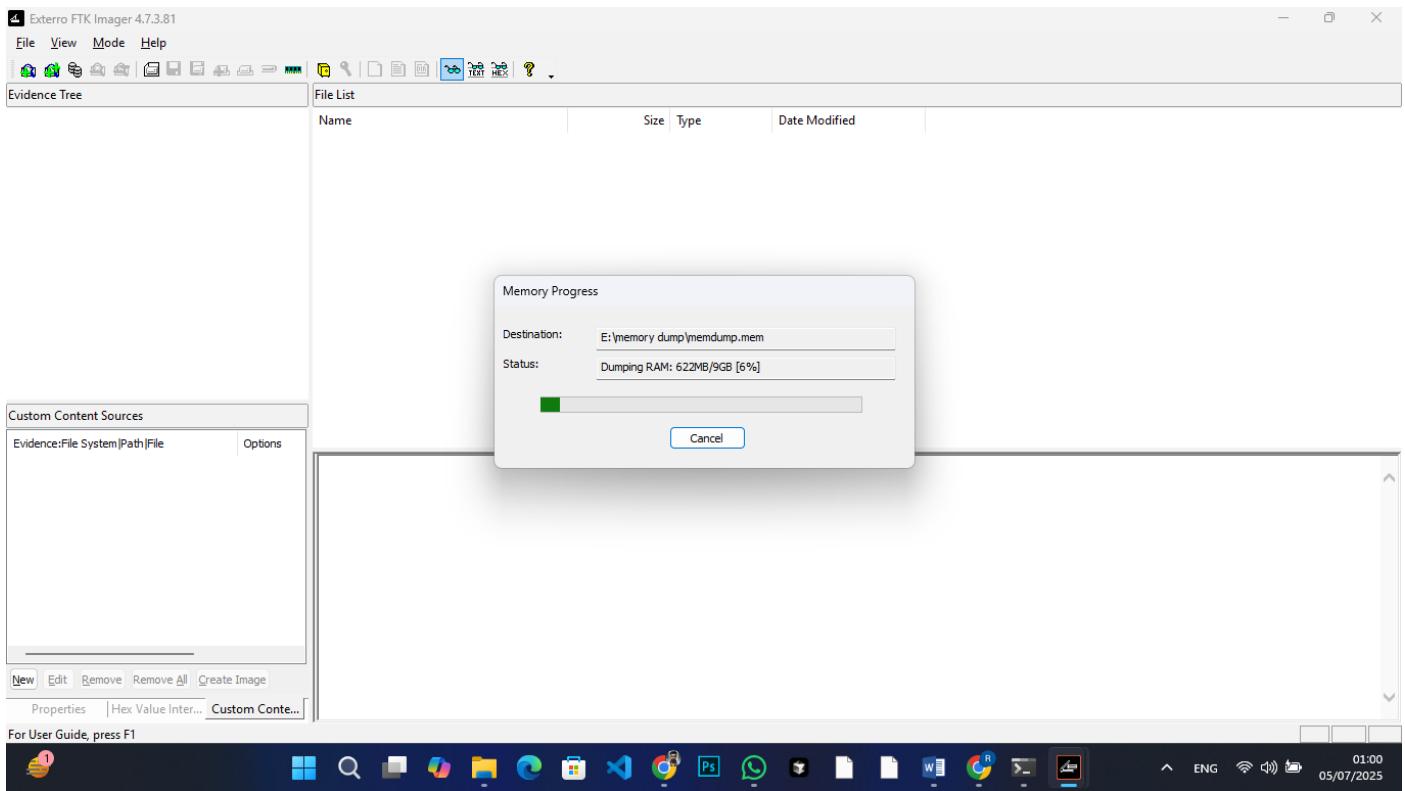


Figure 9 FTK imager creating a Memory dump file

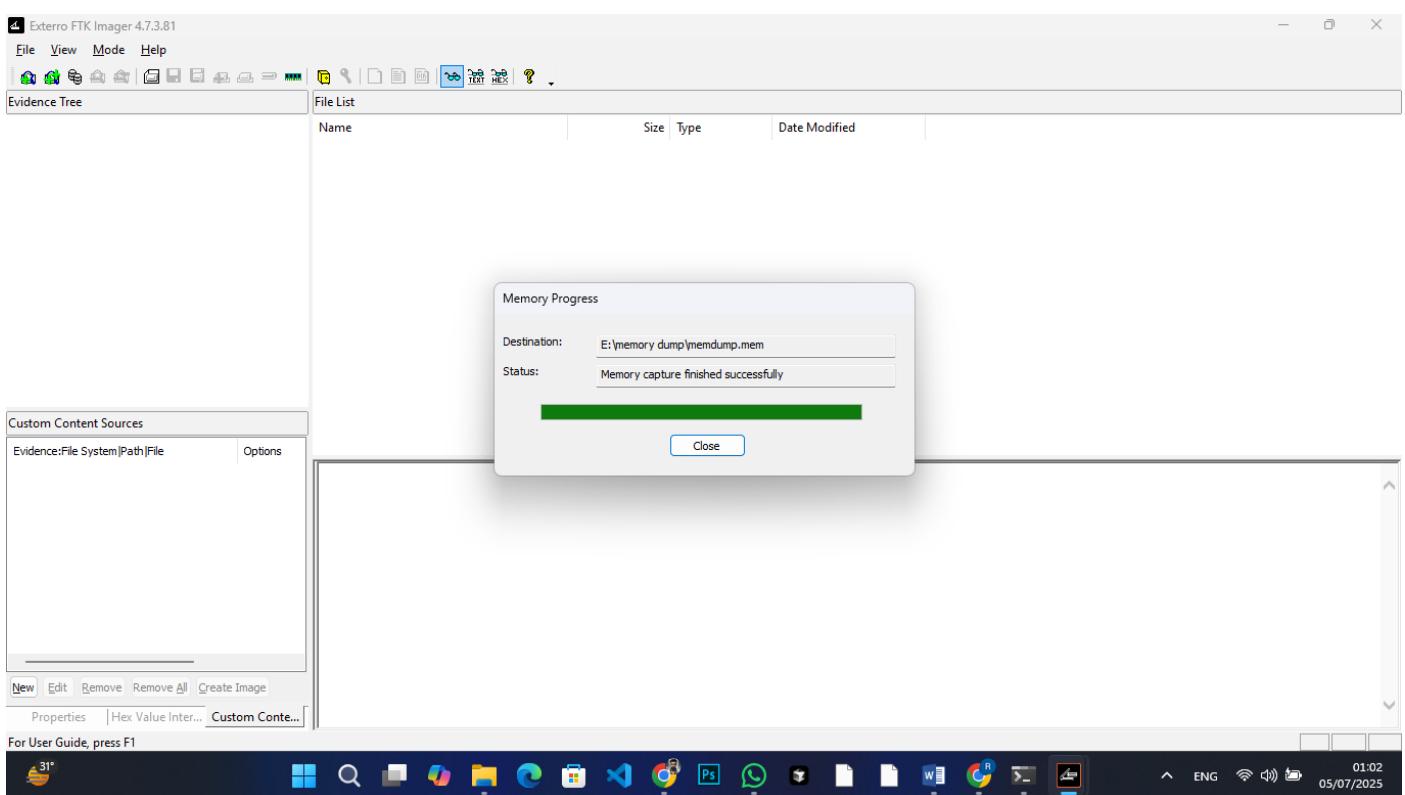


Figure 10 Completing Memory Dump file

Volatility 3

Microsoft Windows [Version 10.0.22631.5472]
(c) Microsoft Corporation. All rights reserved.
E:\Online Courses Details\CHFI course\Digital Forensics Tools\volatility3-develop>python vol.py -f memdump.mem windows.info
Volatility 3 Framework 2.26.2
Progress: 40.00 Updating caches for 110 files...

memdump.mem 05/07/2025 01:01 MEM File 8,886,272 KB

19 items | 1 item selected 8.47 GB |

31° ENG 01:04 05/07/2025

Figure 11 volatility 3

Progress: 14.88krnlmp.pdb Reading file http://msdl.microsoft.com/download/symbols/ntkrnlmp.pdb/B9FA5F26C22CD7250B8
Progress: 14.95krnlmp.pdb Reading file http://msdl.microsoft.com/download/symbols/ntkrnlmp.pdb/B9FA5F26C22CD7250B8
Progress: 15.01krnlmp.pdb Reading file http://msdl.microsoft.com/download/symbols/ntkrnlmp.pdb/B9FA5F26C22CD7250B8
Progress: 15.07krnlmp.pdb Reading file http://msdl.microsoft.com/download/symbols/ntkrnlmp.pdb/B9FA5F26C22CD7250B8
Progress: 15.14krnlmp.pdb Reading file http://msdl.microsoft.com/download/symbols/ntkrnlmp.pdb/B9FA5F26C22CD7250B8
Progress: 15.20krnlmp.pdb Reading file http://msdl.microsoft.com/download/symbols/ntkrnlmp.pdb/B9FA5F26C22CD7250B8
Progress: 15.26krnlmp.pdb Reading file http://msdl.microsoft.com/download/symbols/ntkrnlmp.pdb/B9FA5F26C22CD7250B8
Progress: 15.33krnlmp.pdb Reading file http://msdl.microsoft.com/download/symbols/ntkrnlmp.pdb/B9FA5F26C22CD7250B8
Progress: 15.39krnlmp.pdb Reading file http://msdl.microsoft.com/download/symbols/ntkrnlmp.pdb/B9FA5F26C22CD7250B8
Progress: 15.45krnlmp.pdb Reading file http://msdl.microsoft.com/download/symbols/ntkrnlmp.pdb/B9FA5F26C22CD7250B8
Progress: 15.52krnlmp.pdb Reading file http://msdl.microsoft.com/download/symbols/ntkrnlmp.pdb/B9FA5F26C22CD7250B8
Progress: 15.58krnlmp.pdb Reading file http://msdl.microsoft.com/download/symbols/ntkrnlmp.pdb/B9FA5F26C22CD7250B8
Progress: 15.65krnlmp.pdb Reading file http://msdl.microsoft.com/download/symbols/ntkrnlmp.pdb/B9FA5F26C22CD7250B8
Progress: 15.71krnlmp.pdb Reading file http://msdl.microsoft.com/download/symbols/ntkrnlmp.pdb/B9FA5F26C22CD7250B8
Progress: 15.77krnlmp.pdb Reading file http://msdl.microsoft.com/download/symbols/ntkrnlmp.pdb/B9FA5F26C22CD7250B8
Progress: 15.84krnlmp.pdb Reading file http://msdl.microsoft.com/download/symbols/ntkrnlmp.pdb/B9FA5F26C22CD7250B8
Progress: 15.90krnlmp.pdb Reading file http://msdl.microsoft.com/download/symbols/ntkrnlmp.pdb/B9FA5F26C22CD7250B8
Progress: 15.96krnlmp.pdb Reading file http://msdl.microsoft.com/download/symbols/ntkrnlmp.pdb/B9FA5F26C22CD7250B8
Progress: 16.03krnlmp.pdb Reading file http://msdl.microsoft.com/download/symbols/ntkrnlmp.pdb/B9FA5F26C22CD7250B8
Progress: 16.09krnlmp.pdb Reading file http://msdl.microsoft.com/download/symbols/ntkrnlmp.pdb/B9FA5F26C22CD7250B8
Progress: 16.15krnlmp.pdb Reading file http://msdl.microsoft.com/download/symbols/ntkrnlmp.pdb/B9FA5F26C22CD7250B8
Progress: 16.22krnlmp.pdb Reading file http://msdl.microsoft.com/download/symbols/ntkrnlmp.pdb/B9FA5F26C22CD7250B8
Progress: 16.28krnlmp.pdb Reading file http://msdl.microsoft.com/download/symbols/ntkrnlmp.pdb/B9FA5F26C22CD7250B8
Progress: 16.34krnlmp.pdb Reading file http://msdl.microsoft.com/download/symbols/ntkrnlmp.pdb/B9FA5F26C22CD7250B8
Progress: 16.41krnlmp.pdb Reading file http://msdl.microsoft.com/download/symbols/ntkrnlmp.pdb/B9FA5F26C22CD7250B8
Progress: 16.47krnlmp.pdb Reading file http://msdl.microsoft.com/download/symbols/ntkrnlmp.pdb/B9FA5F26C22CD7250B8
Progress: 16.54krnlmp.pdb Reading file http://msdl.microsoft.com/download/symbols/ntkrnlmp.pdb/B9FA5F26C22CD7250B8
Progress: 16.60krnlmp.pdb Reading file http://msdl.microsoft.com/download/symbols/ntkrnlmp.pdb/B9FA5F26C22CD7250B8
Progress: 16.66krnlmp.pdb Reading file http://msdl.microsoft.com/download/symbols/ntkrnlmp.pdb/B9FA5F26C22CD7250B8
025EE465D79851/ntkrnlmp.pdb

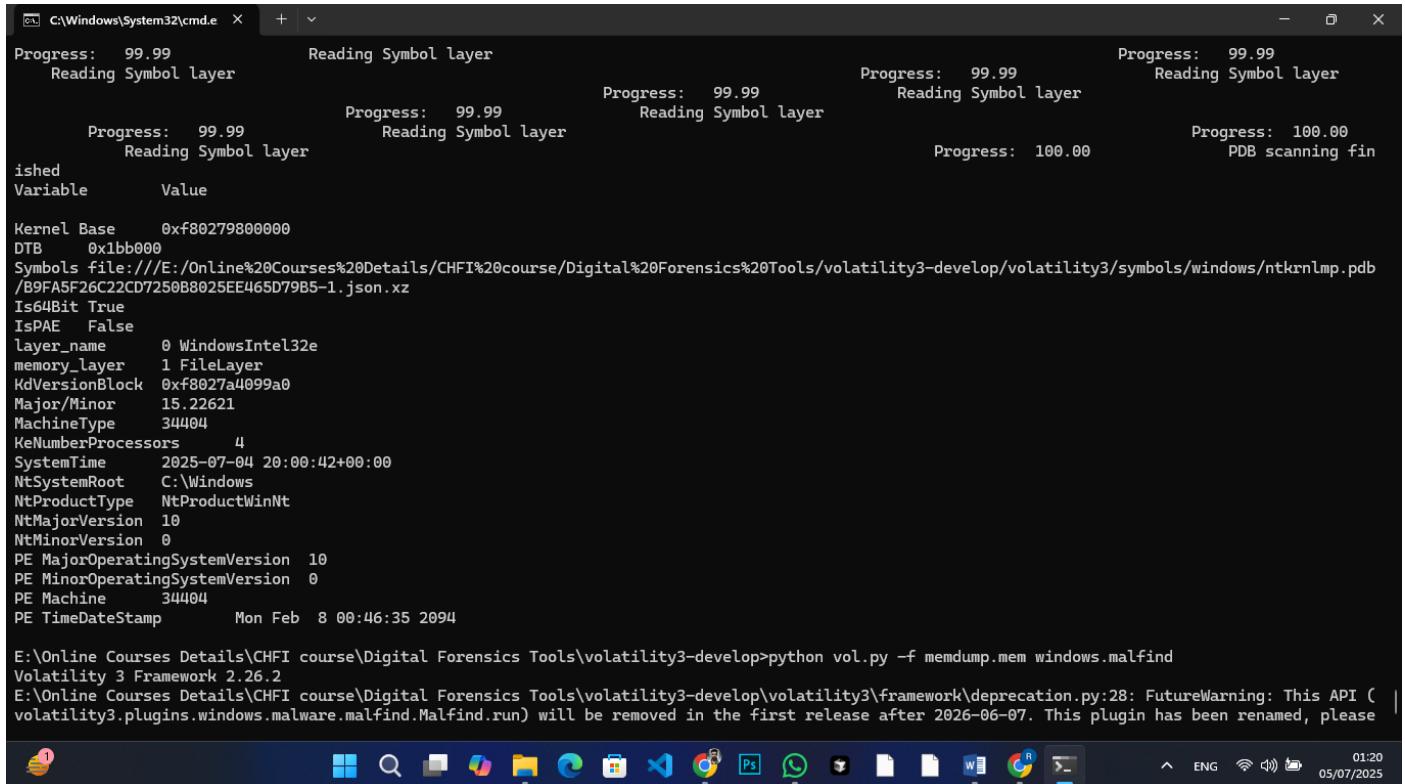
memdump.mem 05/07/2025 01:01 MEM File 8,886,272 KB

19 items | 1 item selected 8.47 GB |

31° ENG 01:05 05/07/2025

Figure 12 Volatility 3 collecting a Window info

Volatility 3 Window Info



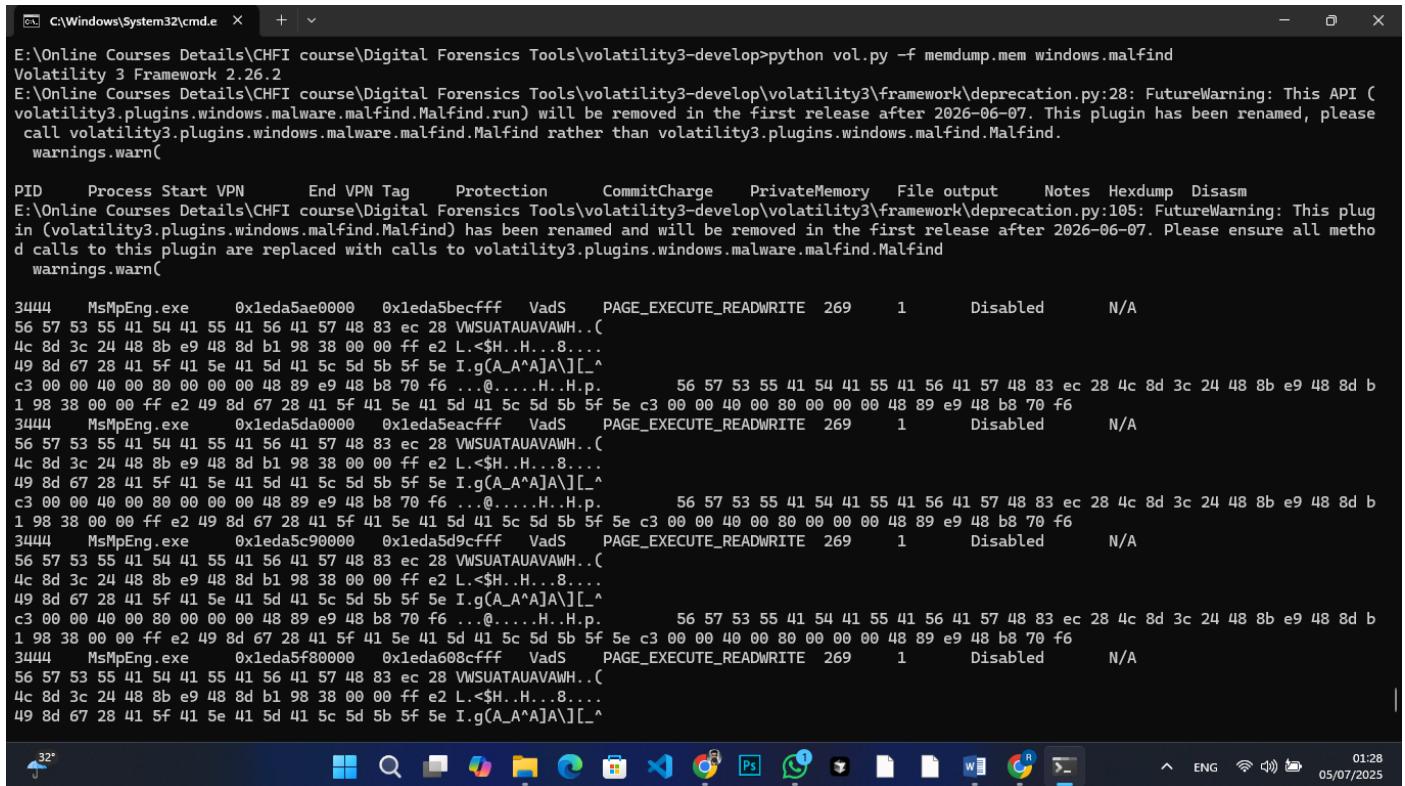
```
Progress: 99.99          Reading Symbol layer          Progress: 99.99          Reading Symbol layer          Progress: 99.99          Reading Symbol layer
Reading Symbol layer      Progress: 99.99          Reading Symbol layer      Progress: 99.99          Reading Symbol layer      Progress: 100.00          PDB scanning fin
Reading Symbol layer      Progress: 99.99          Reading Symbol layer      Progress: 100.00          PDB scanning fin
ish Variable           Value
Kernel Base    0xf80279800000
DTB        0x1bb000
Symbols file:///E:/Online%20Courses%20Details/CHFI%20course/Digital%20Forensics%20Tools/volatility3-develop/volatility3/symbols/windows/ntkrnlmp.pdb
/B9FA5F26C2CD7250B8025EE465D79B5-1.json.xz
Is64Bit True
IsPAE False
layer_name     0 WindowsIntel32e
memory_layer   1 FileLayer
KdVersionBlock 0xf8027a4099a0
Major/Minor    15.22621
MachineType   34404
KeNumberProcessors 4
SystemTime     2025-07-04 20:00:42+00:00
NtSystemRoot   C:\Windows
NtProductType NtProductWinNt
NtMajorVersion 10
NtMinorVersion 0
PE MajorOperatingSystemVersion 10
PE MinorOperatingSystemVersion 0
PE Machine     34404
PE TimeStamp    Mon Feb 8 00:46:35 2094

E:\Online Courses Details\CHFI course\Digital Forensics Tools\volatility3-develop>python vol.py -f memdump.mem windows.malfind
Volatility 3 Framework 2.26.2
E:\Online Courses Details\CHFI course\Digital Forensics Tools\volatility3-develop\volatility3\framework\deprecation.py:28: FutureWarning: This API ( | volatility3.plugins.windows.malware.malfind.Malfind.run) will be removed in the first release after 2026-06-07. This plugin has been renamed, please
| volatility3.plugins.windows.malware.malfind.Malfind rather than volatility3.plugins.windows.malfind.Malfind.

01:20
05/07/2025
```

Figure 13 Volatility 3 Window info

Malfind Plugin Collecting using Volatility 3



```
E:\Online Courses Details\CHFI course\Digital Forensics Tools\volatility3-develop>python vol.py -f memdump.mem windows.malfind
Volatility 3 Framework 2.26.2
E:\Online Courses Details\CHFI course\Digital Forensics Tools\volatility3-develop\volatility3\framework\deprecation.py:28: FutureWarning: This API ( | volatility3.plugins.windows.malware.malfind.Malfind.run) will be removed in the first release after 2026-06-07. This plugin has been renamed, please
| volatility3.plugins.windows.malware.malfind.Malfind rather than volatility3.plugins.windows.malfind.Malfind.

warnings.warn(
PID  Process Start VPN      End VPN Tag      Protection      CommitCharge      PrivateMemory      File output      Notes      Hexdump      Disasm
E:\Online Courses Details\CHFI course\Digital Forensics Tools\volatility3-develop\volatility3\framework\deprecation.py:105: FutureWarning: This plug
in (volatility3.plugins.windows.malware.malfind.Malfind) has been renamed and will be removed in the first release after 2026-06-07. Please ensure all metho
d calls to this plugin are replaced with calls to volatility3.plugins.windows.malware.malfind.Malfind
warnings.warn(
56 57 53 55 41 54 41 55 41 56 41 57 48 83 ec 28 VWSUATAUAVAWH..( 56 57 53 55 41 54 41 55 41 56 41 57 48 83 ec 28 4c 8d 3c 24 48 8b e9 48 8d b
4c 8d 3c 24 48 8b e9 48 8d b1 98 38 00 00 ff e2 L.<$H..H..8...
49 8d 67 28 41 5f 41 5e 41 5d 41 5c 5d 5b 5f 5e I.g(A_A^A]A]L.^
c3 00 00 40 00 80 00 00 00 48 89 e9 48 b8 70 f6 ...@.....H..H.p. 56 57 53 55 41 54 41 55 41 56 41 57 48 83 ec 28 4c 8d 3c 24 48 8b e9 48 8d b
1 98 38 00 00 ff e2 49 8d 67 28 41 5f 41 5e 41 5d 41 5c 5d 5b 5f 5e c3 00 00 40 00 80 00 00 00 48 89 e9 48 b8 70 f6
3444 MsMpEng.exe 0x1eda5beffff VadS PAGE_EXECUTE_READWRITE 269 1 Disabled N/A
56 57 53 55 41 54 41 55 41 56 41 57 48 83 ec 28 VWSUATAUAVAWH..( 56 57 53 55 41 54 41 55 41 56 41 57 48 83 ec 28 4c 8d 3c 24 48 8b e9 48 8d b
4c 8d 3c 24 48 8b e9 48 8d b1 98 38 00 00 ff e2 L.<$H..H..8...
49 8d 67 28 41 5f 41 5e 41 5d 41 5c 5d 5b 5f 5e I.g(A_A^A]A]L.^
c3 00 00 40 00 80 00 00 00 48 89 e9 48 b8 70 f6 ...@.....H..H.p. 56 57 53 55 41 54 41 55 41 56 41 57 48 83 ec 28 4c 8d 3c 24 48 8b e9 48 8d b
1 98 38 00 00 ff e2 49 8d 67 28 41 5f 41 5e 41 5d 41 5c 5d 5b 5f 5e c3 00 00 40 00 80 00 00 00 48 89 e9 48 b8 70 f6
3444 MsMpEng.exe 0x1eda5c90000 0x1eda5d9cff VadS PAGE_EXECUTE_READWRITE 269 1 Disabled N/A
56 57 53 55 41 54 41 55 41 56 41 57 48 83 ec 28 VWSUATAUAVAWH..( 56 57 53 55 41 54 41 55 41 56 41 57 48 83 ec 28 4c 8d 3c 24 48 8b e9 48 8d b
4c 8d 3c 24 48 8b e9 48 8d b1 98 38 00 00 ff e2 L.<$H..H..8...
49 8d 67 28 41 5f 41 5e 41 5d 41 5c 5d 5b 5f 5e I.g(A_A^A]A]L.^
c3 00 00 40 00 80 00 00 00 48 89 e9 48 b8 70 f6 ...@.....H..H.p. 56 57 53 55 41 54 41 55 41 56 41 57 48 83 ec 28 4c 8d 3c 24 48 8b e9 48 8d b
1 98 38 00 00 ff e2 49 8d 67 28 41 5f 41 5e 41 5d 41 5c 5d 5b 5f 5e c3 00 00 40 00 80 00 00 00 48 89 e9 48 b8 70 f6
3444 MsMpEng.exe 0x1eda5f80000 0x1eda608cff VadS PAGE_EXECUTE_READWRITE 269 1 Disabled N/A
56 57 53 55 41 54 41 55 41 56 41 57 48 83 ec 28 VWSUATAUAVAWH..( 56 57 53 55 41 54 41 55 41 56 41 57 48 83 ec 28 4c 8d 3c 24 48 8b e9 48 8d b
4c 8d 3c 24 48 8b e9 48 8d b1 98 38 00 00 ff e2 L.<$H..H..8...
49 8d 67 28 41 5f 41 5e 41 5d 41 5c 5d 5b 5f 5e I.g(A_A^A]A]L.^
01:28
05/07/2025
```

Figure 14 Volatility 3 Malfind collecting

Malfind plugin Find some Suspicious

Figure 15 find Some Suspicious using volatility 3

Idrmodules Plugin in Volatility 3

```
C:\Windows\System32\cmd.exe X + ^ 
KeyboardInterrupt
^C
E:\Online Courses Details\CHFI course\Digital Forensics Tools\volatility3-develop>python vol.py -f memdump.mem windows.ldrmodules
Volatility 3 Framework 2.26.2
Progress: 100.00          PDB scanning finished
Pid  Process Base  InLoad  InInit  InMem   MappedPath
4    System  0x2f310000  False   False   \Windows\SysWOW64\ntdll.dll
4    System  0x2082f620000 False  False   \Windows\System32\ntdll.dll
596  smss.exe 0x7ff888930000 True   True   \Windows\System32\ntdll.dll
596  smss.exe 0x7ff69bfb0000 True   False  \Windows\System32\smss.exe
800  csrss.exe 0x21180d00000 False  False   \Windows\System32\en-US\winsrv.dll.mui
800  csrss.exe 0x21180df0000 False  False   \Windows\System32\en-US\csrss.exe.mui
800  csrss.exe 0x21182b30000 False  False   \Windows\System32\en-US\user32.dll.mui
800  csrss.exe 0x7ff885a00000 True   True   \Windows\System32\csrssv.dll
800  csrss.exe 0x7ff606240000 True   False  \Windows\System32\csrss.exe
800  csrss.exe 0x7ff885980000 True   True   \Windows\System32\sxssrv.dll
800  csrss.exe 0x7ff885890000 True   True   \Windows\System32\sxs.dll
800  csrss.exe 0x7ff885790000 False  False  \Windows\System32\ServicingCommon.dll
800  csrss.exe 0x7ff8859c0000 True   True   \Windows\System32\winsrv.dll
800  csrss.exe 0x7ff885990000 True   True   \Windows\System32\winsrvext.dll
800  csrss.exe 0x7ff8859e0000 True   True   \Windows\System32\basesrv.dll
800  csrss.exe 0x7ff8863a0000 True   True   \Windows\System32\wln32u.dll
800  csrss.exe 0x7ff885fe0000 True   True   \Windows\System32\gdi32full.dll
800  csrss.exe 0x7ff885a20000 True   True   \Windows\System32\KernelBase.dll
800  csrss.exe 0x7ff885e00000 True   True   \Windows\System32\ucrtbase.dll
800  csrss.exe 0x7ff886300000 True   True   \Windows\System32\msvcp_win.dll
800  csrss.exe 0x7ff887a20000 True   True   \Windows\System32\kernel32.dll
800  csrss.exe 0x7ff887290000 False  False  \Windows\System32\rpcrt4.dll
800  csrss.exe 0x7ff886450000 False  False  \Windows\System32\bcrypt.dll
800  csrss.exe 0x7ff8863d0000 False  False  \Windows\System32\bcryptprimitives.dll
800  csrss.exe 0x7ff8878e0000 False  False  \Windows\System32\msvcrt.dll
800  csrss.exe 0x7ff887490000 False  False  \Windows\System32\sechost.dll
800  csrss.exe 0x7ff8879a0000 True   True   \Windows\System32\gdi32.dll
800  csrss.exe 0x7ff887d30000 False  False  \Windows\System32\advapi32.dll
```

Figure 16 Idrmodules plugin in Volatility 3

5.3 What user activity helped the malware persist?

Evidence Upload in FTK Imager

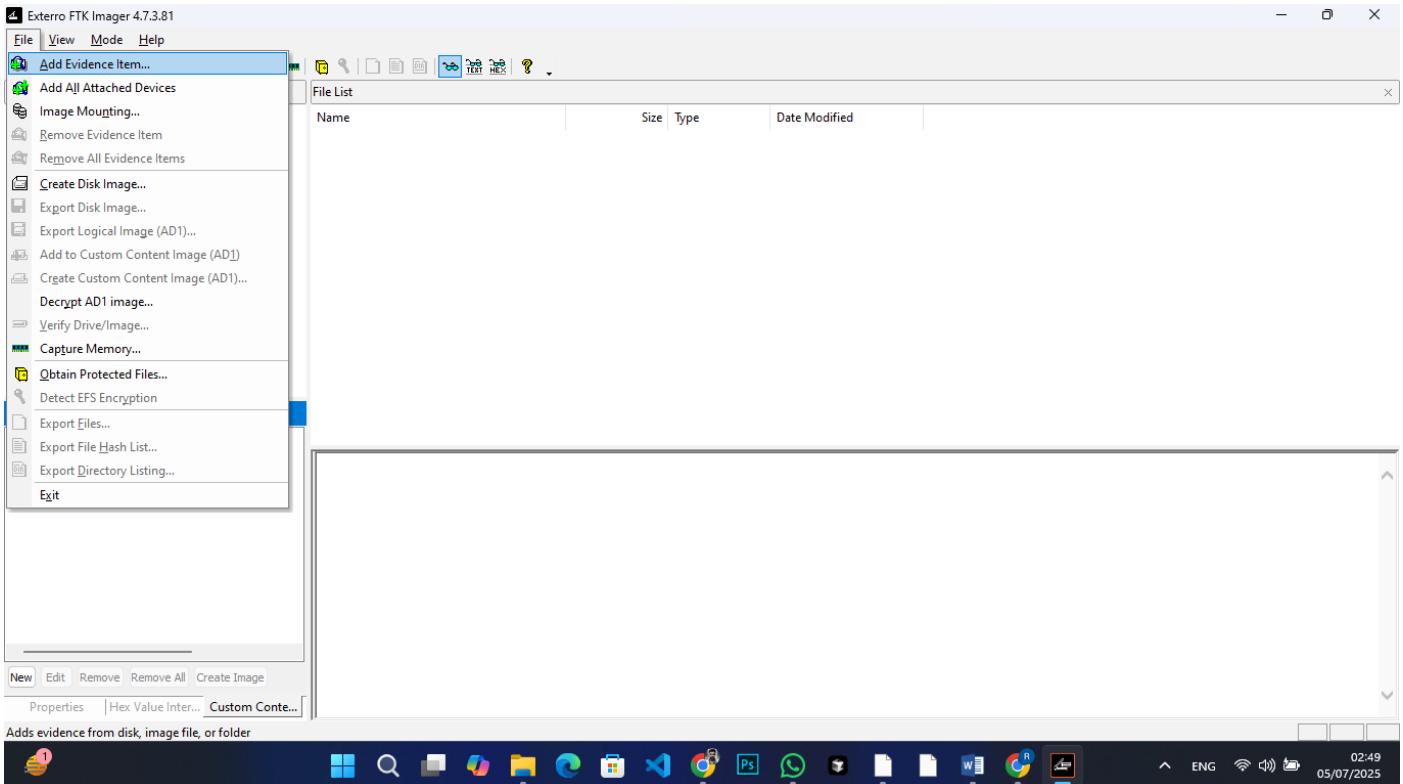


Figure 17 Evidence Upload in FTK Imager

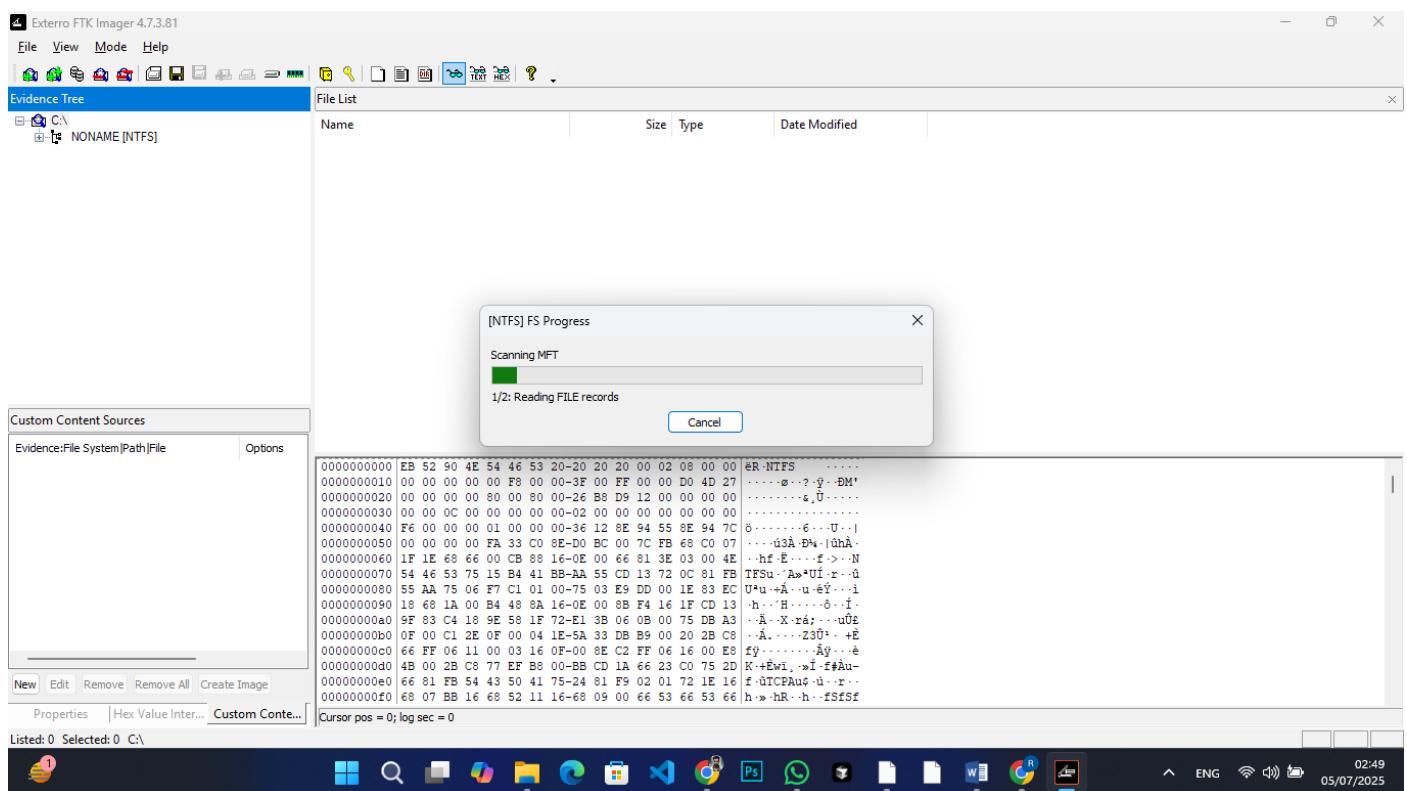


Figure 18 Evidence Loaded in FTK Imager

Export System Hive in Desktop Hive Folder

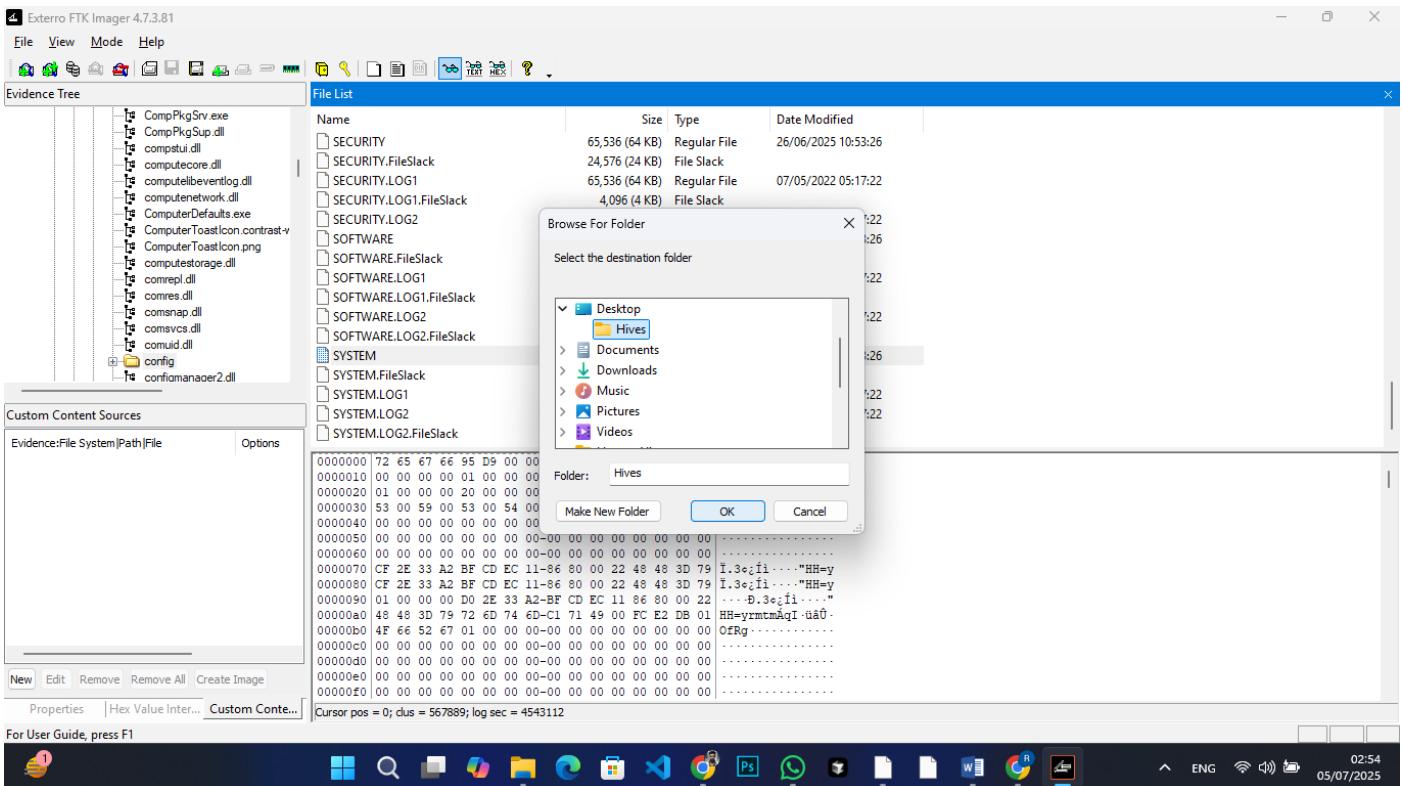


Figure 19 System Registry Export

Export Software Hive in Desktop Hive Folder

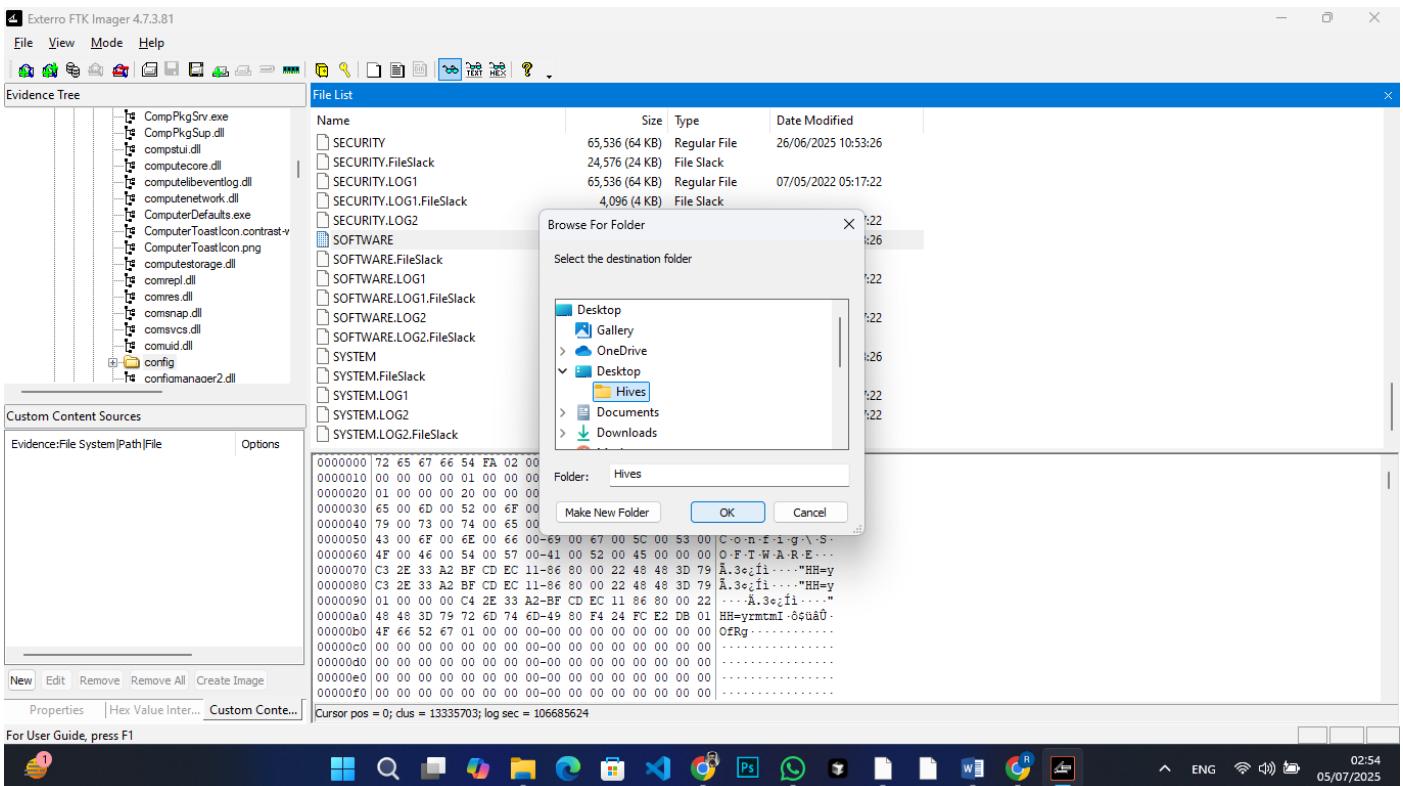


Figure 20 Software Registry Export

Export NTUSER.DAT hive in Desktop Hive Folder

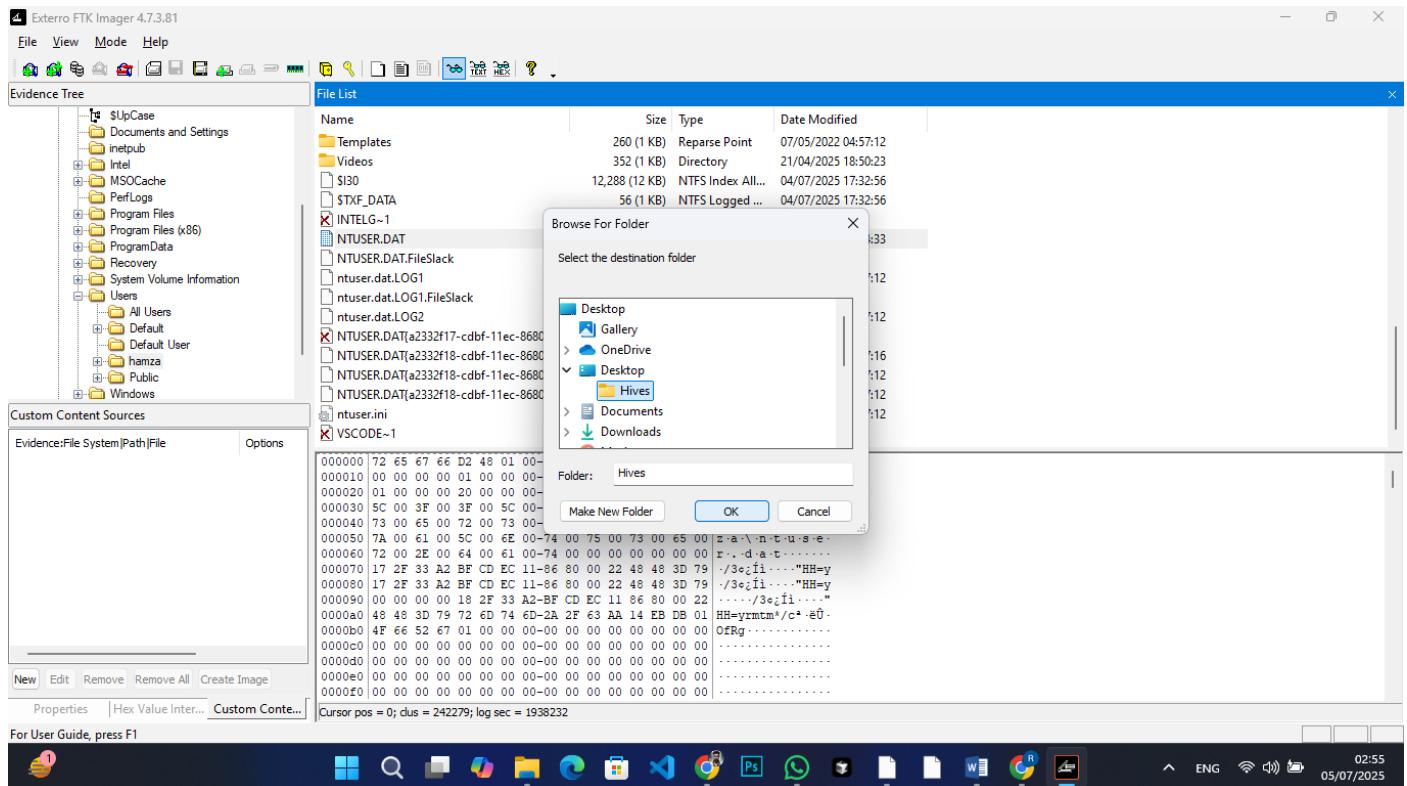


Figure 21 NTUSER.DAT Registry Export

Registry Hives convert to readable Text file using (Reg Ripper Tool)

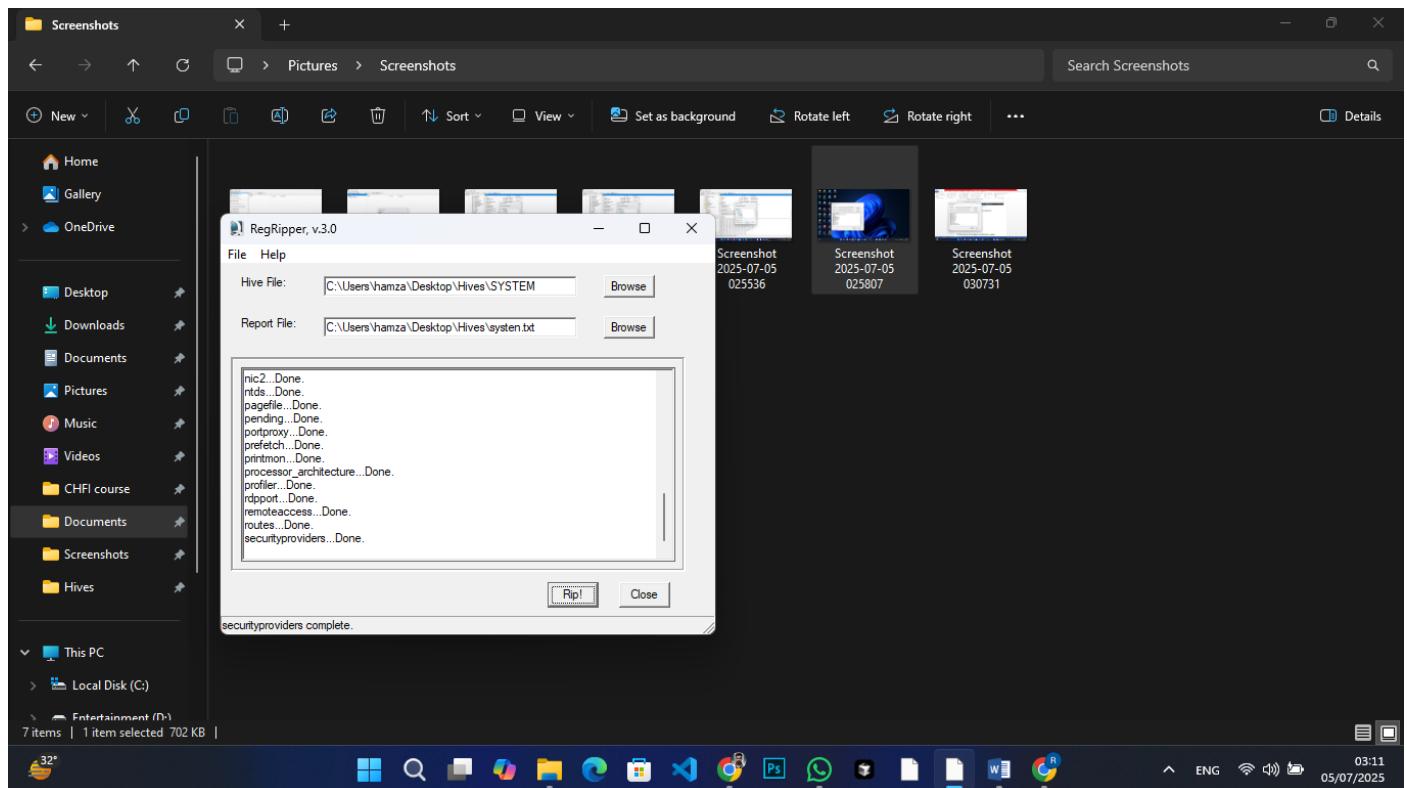


Figure 22 System Registry hive convert to Textfile

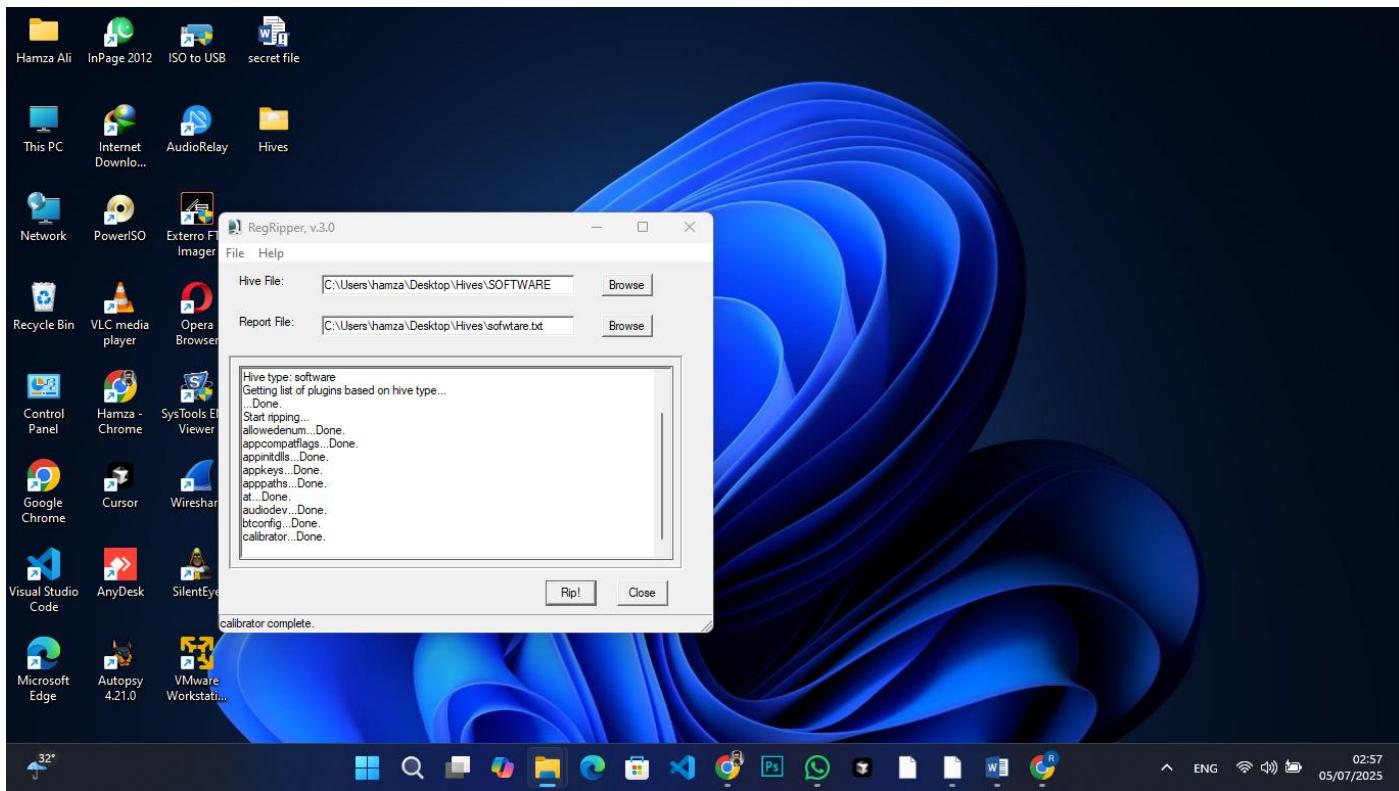


Figure 23 Software Registry Hive Convert to Text File

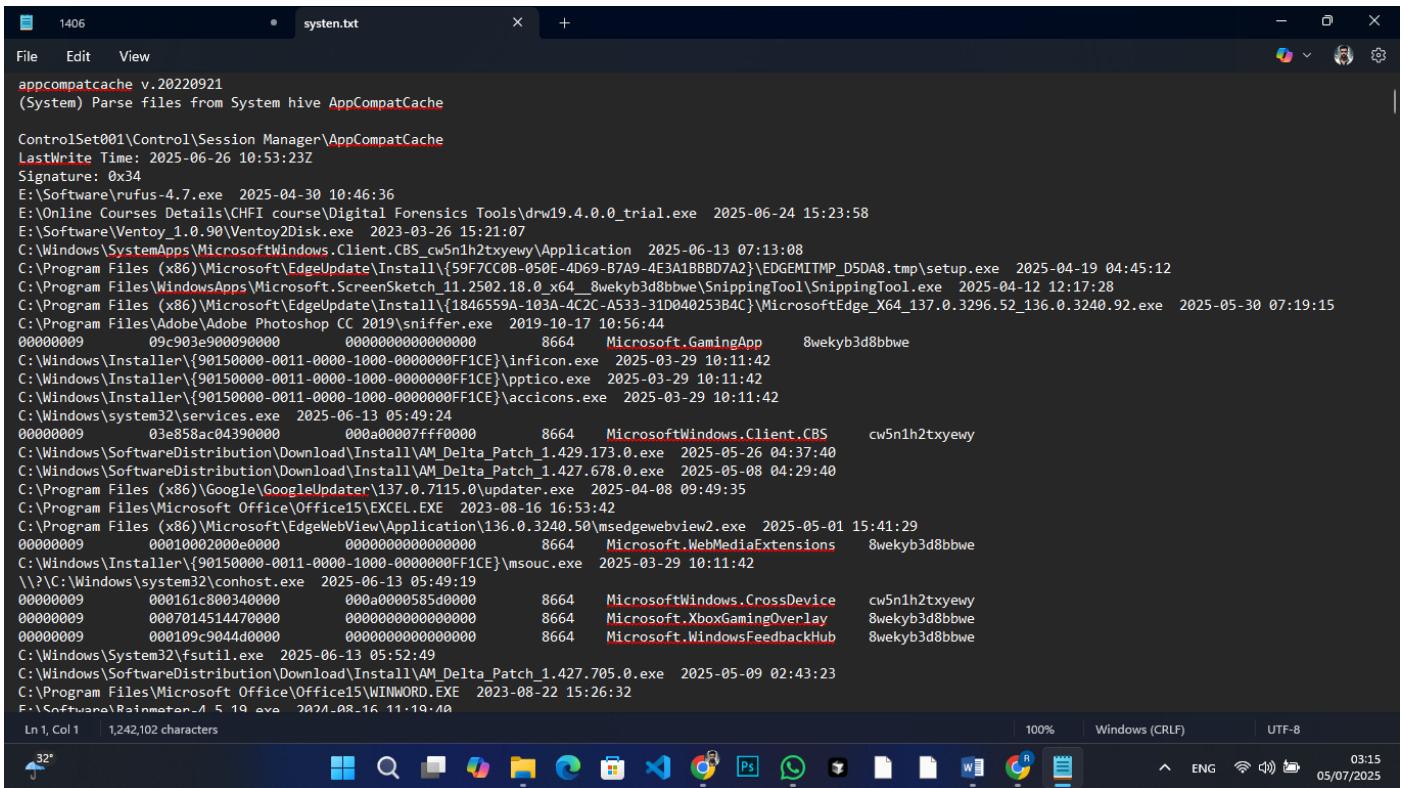
sysinternals... Done.
lscclient... Done.
typedpaths... Done.
typedurls... Done.
typedurertime... Done.
uninstall... Done.
userassist... Done.
wc_shares... Done.
winrar... Done.
winscp... Done.
winzip... Done.
wordwheelquery... Done.
0 plugins completed with errors.

d for exfiltration?

5.5 What browser activity suggests credential theft or staging?

Figure 24 NTUSER.DAT hive file convert to text file

System Hive (.txt) file



1406 system.txt

```
appcompatcache v.20220921
(System) Parse files from System hive AppCompatCache

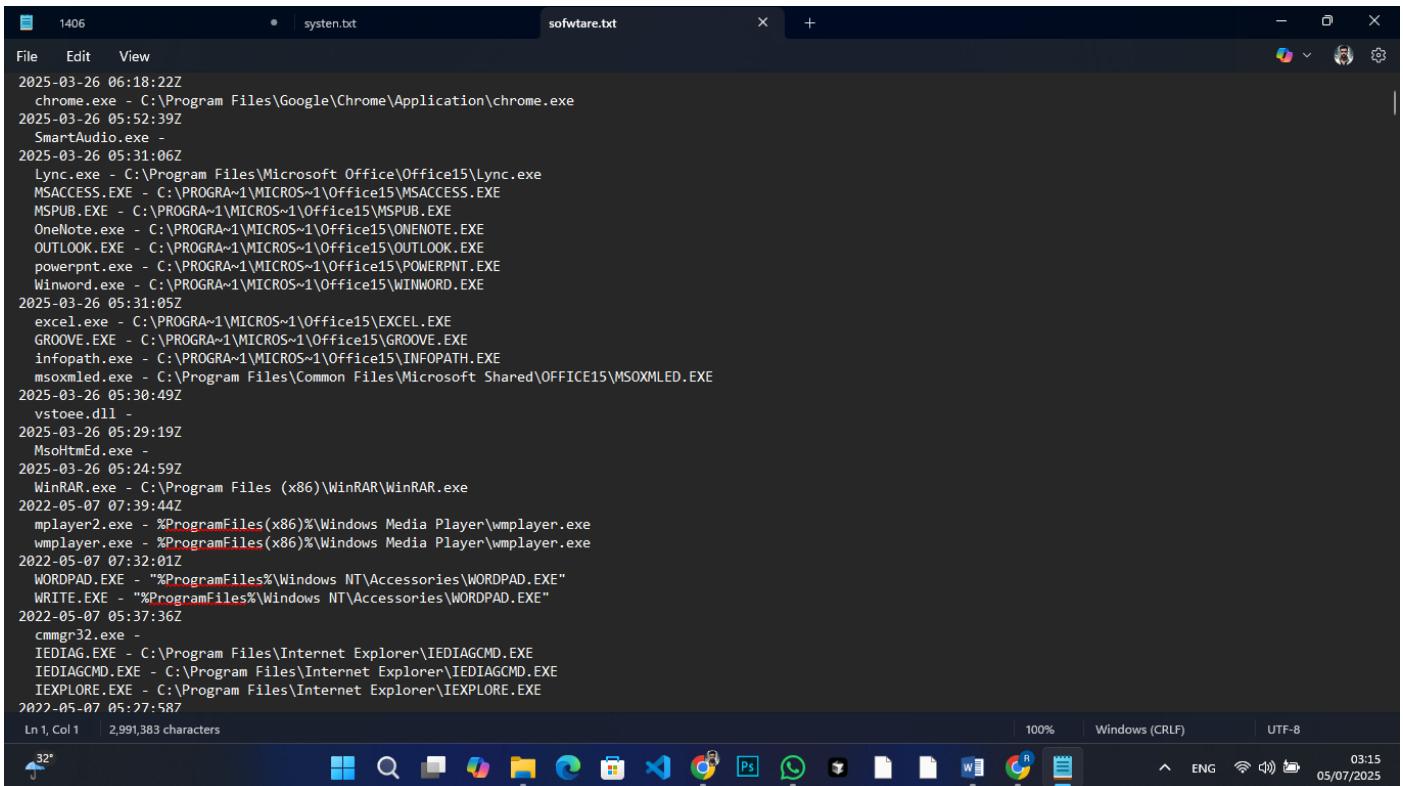
ControlSet001\Control\Session Manager\AppCompatCache
LastWrite Time: 2025-06-26 10:53:23
Signature: 0x34
E:\Software\rufus-4.7.exe 2025-04-30 10:46:36
E:\Online Course Details\CHFI course\Digital Forensics Tools\drw19.4.0.0_trial.exe 2025-06-24 15:23:58
E:\Software\Ventoy_1.0.90\Ventoy2Disk.exe 2023-03-26 15:21:07
C:\Windows\SystemApps\MicrosoftWindows.Client.CBS_cw5n1h2txyewy\Application 2025-06-13 07:13:08
C:\Program Files (x86)\Microsoft\EdgeUpdate\Install\{59F7CC0B-050E-4D69-B7A9-4E3A1BBBD7A2}\EDGEMITMP_D5DA8.tmp\setup.exe 2025-04-19 04:45:12
C:\Program Files\WindowsApps\Microsoft.ScreenSketch.11.2502.18.0_x64_8wekyb3d8bbwe\SnippingTool.exe 2025-04-12 12:17:28
C:\Program Files (x86)\Microsoft\EdgeUpdate\Install\{1846559A-103A-4C2C-A533-31D040253B4C}\MicrosoftEdge_X64_137.0.3296.52_136.0.3240.92.exe 2025-05-30 07:19:15
C:\Program Files\Adobe\Adobe Photoshop CC 2019\sniffer.exe 2019-10-17 10:56:44
00000009 09c903e900000000 0000000000000000 8664 Microsoft.GamingApp 8wekyb3d8bbwe
C:\Windows\Installer\{90150000-0011-0000-1000-000000FF1CE}\inficon.exe 2025-03-29 10:11:42
C:\Windows\Installer\{90150000-0011-0000-1000-000000FF1CE}\pptico.exe 2025-03-29 10:11:42
C:\Windows\Installer\{90150000-0011-0000-1000-000000FF1CE}\accicons.exe 2025-03-29 10:11:42
C:\Windows\system32\services.exe 2025-06-13 05:49:24
00000009 03e858ac04390000 000a0007ffff0000 8664 Microsoft.Windows.Client.CBS cw5n1h2txyewy
C:\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.429.173.0.exe 2025-05-26 04:37:40
C:\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.427.678.0.exe 2025-05-08 04:29:40
C:\Program Files (x86)\Google\GoogleUpdater\137.0.7115.0\update.exe 2025-04-08 09:49:35
C:\Program Files\Microsoft Office\Office15\EXCEL.EXE 2023-08-16 16:53:42
C:\Program Files (x86)\Microsoft\EdgeWebView\Application\136.0.3240.50\msedgewebview2.exe 2025-05-01 15:41:29
00000009 00010002000e0000 0000000000000000 8664 Microsoft.WebMediaExtensions 8wekyb3d8bbwe
C:\Windows\Installer\{90150000-0011-0000-1000-000000FF1CE}\msouc.exe 2025-03-29 10:11:42
\\?\C:\Windows\system32\conhost.exe 2025-06-13 05:49:19
00000009 000161c800340000 000a000585d0000 8664 Microsoft.Windows.CrossDevice cw5n1h2txyewy
00000009 0007014514470000 0000000000000000 8664 Microsoft.XboxGamingOverlay 8wekyb3d8bbwe
00000009 000109c9044d0000 0000000000000000 8664 Microsoft.WindowsFeedbackHub 8wekyb3d8bbwe
C:\Windows\System32\fsutil.exe 2025-06-13 05:52:49
C:\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.427.705.0.exe 2025-05-09 02:43:23
C:\Program Files\Microsoft Office\Office15\WINWORD.EXE 2023-08-22 15:26:32
F:\Software\Rainmeter-1.5.19.exe 2021-08-16 11:10:40
```

Ln 1, Col 1 | 1,242,102 characters | 100% | Windows (CRLF) | UTF-8

32° ENG 03:15 05/07/2025

Figure 25 System Hive (.txt) file

Software (.txt) file



1406 software.txt

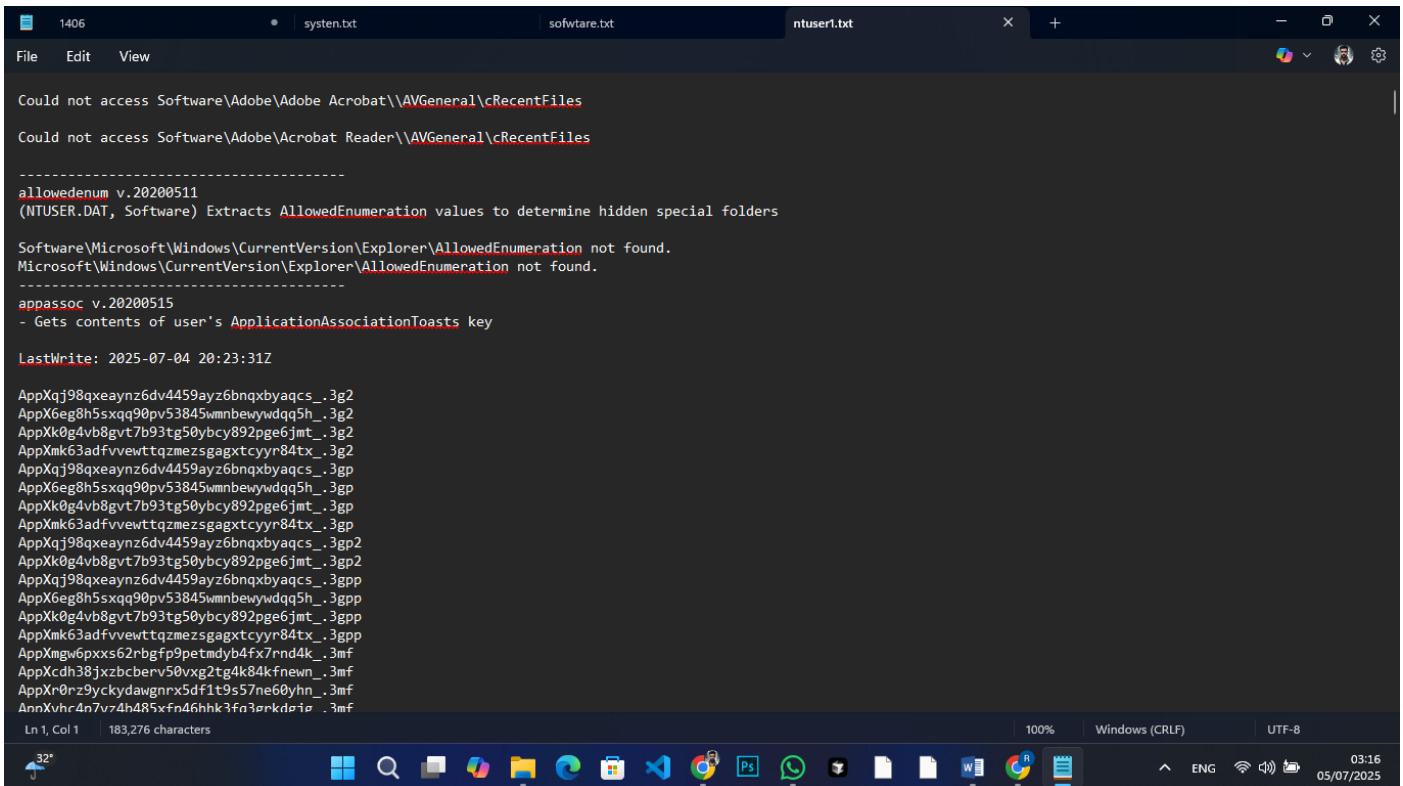
```
2025-03-26 06:18:22
chrome.exe - C:\Program Files\Google\Chrome\Application\chrome.exe
2025-03-26 05:52:39Z
SmartAudio.exe -
2025-03-26 05:31:06Z
Lync.exe - C:\Program Files\Microsoft Office\Office15\Lync.exe
MSACCESS.EXE - C:\PROGRA~1\MICROS~1\Office15\MSACCESS.EXE
MSPUB.EXE - C:\PROGRA~1\MICROS~1\Office15\MSPUB.EXE
OneNote.exe - C:\PROGRA~1\MICROS~1\Office15\ONENOTE.EXE
OUTLOOK.EXE - C:\PROGRA~1\MICROS~1\Office15\OUTLOOK.EXE
powerpnt.exe - C:\PROGRA~1\MICROS~1\Office15\POWERPNT.EXE
Winword.exe - C:\PROGRA~1\MICROS~1\Office15\WINWORD.EXE
2025-03-26 05:31:05Z
excel.exe - C:\PROGRA~1\MICROS~1\Office15\EXCEL.EXE
GROOVE.EXE - C:\PROGRA~1\MICROS~1\Office15\GROOVE.EXE
infopath.exe - C:\PROGRA~1\MICROS~1\Office15\INFOPATH.EXE
msoxmled.exe - C:\Program Files\Common Files\Microsoft Shared\OFFICE15\MSOXMLED.EXE
2025-03-26 05:30:49Z
vstoee.dll
2025-03-26 05:29:19Z
MshtmEd.exe -
2025-03-26 05:24:59Z
WinRAR.exe - C:\Program Files (x86)\WinRAR\WinRAR.exe
2022-05-07 07:39:44Z
mplayer2.exe - %ProgramFiles%(x86)%\Windows Media Player\wmplayer.exe
wmplayer.exe - %ProgramFiles%(x86)%\Windows Media Player\wmplayer.exe
2022-05-07 07:32:01Z
WORDPAD.EXE - "%ProgramFiles%\Windows NT\Accessories\WORDPAD.EXE"
WRITE.EXE - "%ProgramFiles%\Windows NT\Accessories\WORDPAD.EXE"
2022-05-07 05:37:36Z
cmngr32.exe -
IEDIAG.EXE - C:\Program Files\Internet Explorer\IEDIAGCMD.EXE
IEDIAGCMD.EXE - C:\Program Files\Internet Explorer\IEDIAGCMD.EXE
EXPLORE.EXE - C:\Program Files\Internet Explorer\EXPLORE.EXE
2022-05-07 05:27:58Z
```

Ln 1, Col 1 | 2,991,383 characters | 100% | Windows (CRLF) | UTF-8

32° ENG 03:15 05/07/2025

Figure 26 Software (.txt) file

NTUSER.DAT (.txt) file



```
1406 system.txt software.txt ntuser1.txt
File Edit View
Could not access Software\Adobe\Adobe Acrobat\AVGeneral\cRecentFiles
Could not access Software\Adobe\Acrobat Reader\AVGeneral\cRecentFiles
-----
allowedenum v.20200511
(NTUSER.DAT, Software) Extracts AllowedEnumeration values to determine hidden special folders
Software\Microsoft\Windows\CurrentVersion\Explorer\AllowedEnumeration not found.
Microsoft\Windows\CurrentVersion\Explorer\AllowedEnumeration not found.
-----
appassoc v.20200515
- Gets contents of user's ApplicationAssociationToasts key
LastWrite: 2025-07-04 20:23:31Z

AppXqj98qxeaynz6dv4459ayz6bnqxbqaacs_.3g2
AppX6eg8h5sqq90pv53845wmmbewywdq5h_.3g2
AppXk0g4vb8gv7b93tg50ybcy892pge6jmt_.3g2
AppXmk63adfviewttqmezsgagxtcyrr84tx_.3g2
AppXqj98qxeaynz6dv4459ayz6bnqxbqaacs_.3gp
AppX6eg8h5sqq90pv53845wmmbewywdq5h_.3gp
AppXk0g4vb8gv7b93tg50ybcy892pge6jmt_.3gp
AppXmk63adfviewttqmezsgagxtcyrr84tx_.3gp
AppXqj98qxeaynz6dv4459ayz6bnqxbqaacs_.3gp2
AppXk0g4vb8gv7b93tg50ybcy892pge6jmt_.3gp2
AppXqj98qxeaynz6dv4459ayz6bnqxbqaacs_.3gpp
AppX6eg8h5sqq90pv53845wmmbewywdq5h_.3gpp
AppXk0g4vb8gv7b93tg50ybcy892pge6jmt_.3gpp
AppXmk63adfviewttqmezsgagxtcyrr84tx_.3gpp
AppXmgw6pxxs62rbgfp9petmby4fx7rnd4k_.3mf
AppXcdh38jxzbcberv50vxp2t4kfnewn_.3mf
AppXr0rz5ycydkydawgnrxsdf1t9s57ne60yhn_.3mf
AnnXvhc4n7vz4h485xfnd6hhk3fa3arkdai_.3mf
Ln 1, Col 1 183,276 characters
100% Windows (CRLF) UTF-8
32° ENG 03:16 05/07/2025
```

Figure 27 NTUSER.DAT (.txt) file

5.4 What deleted or hidden files were staged for exfiltration?

Shrink Local Disk D: for create a New Partition

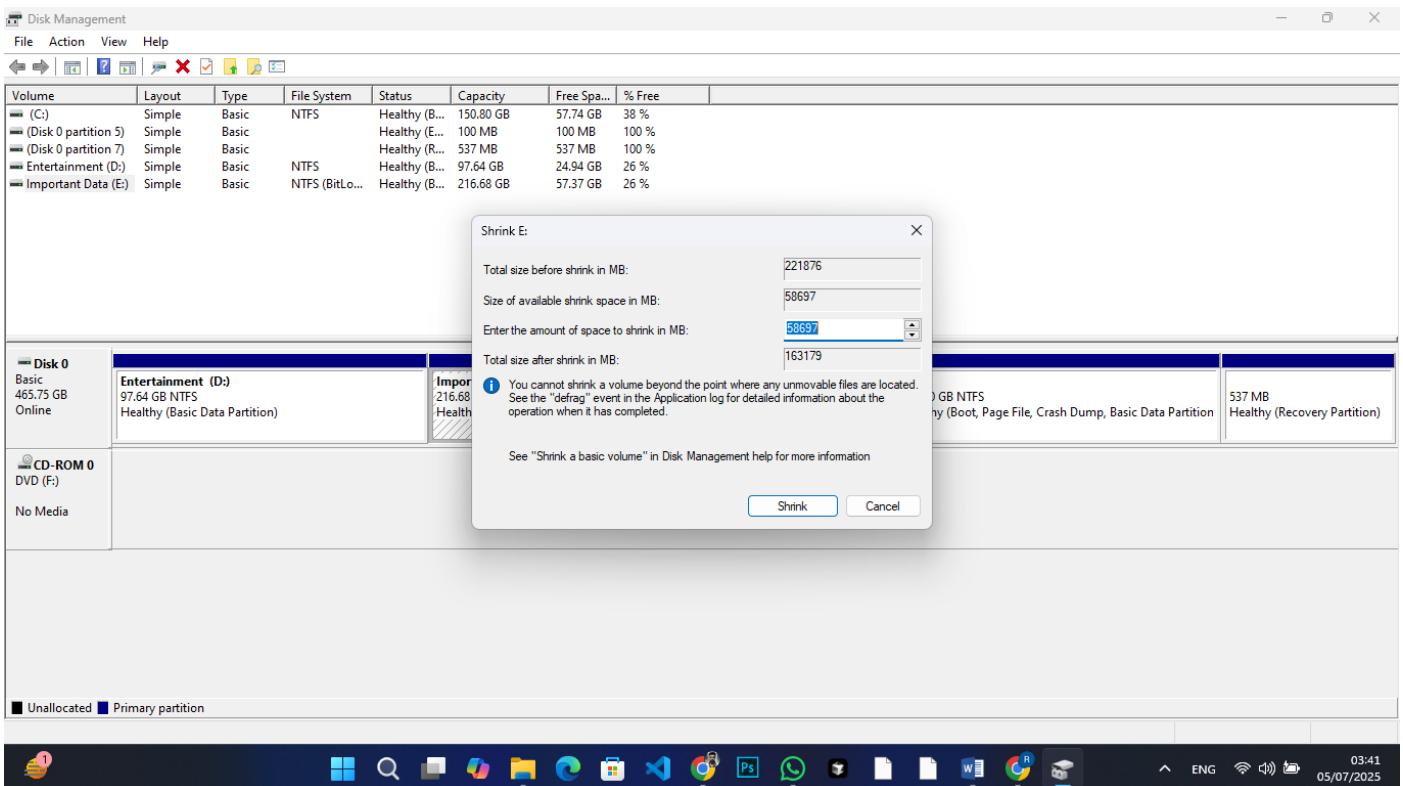


Figure 28 Shrink Partition

Create a New Partition

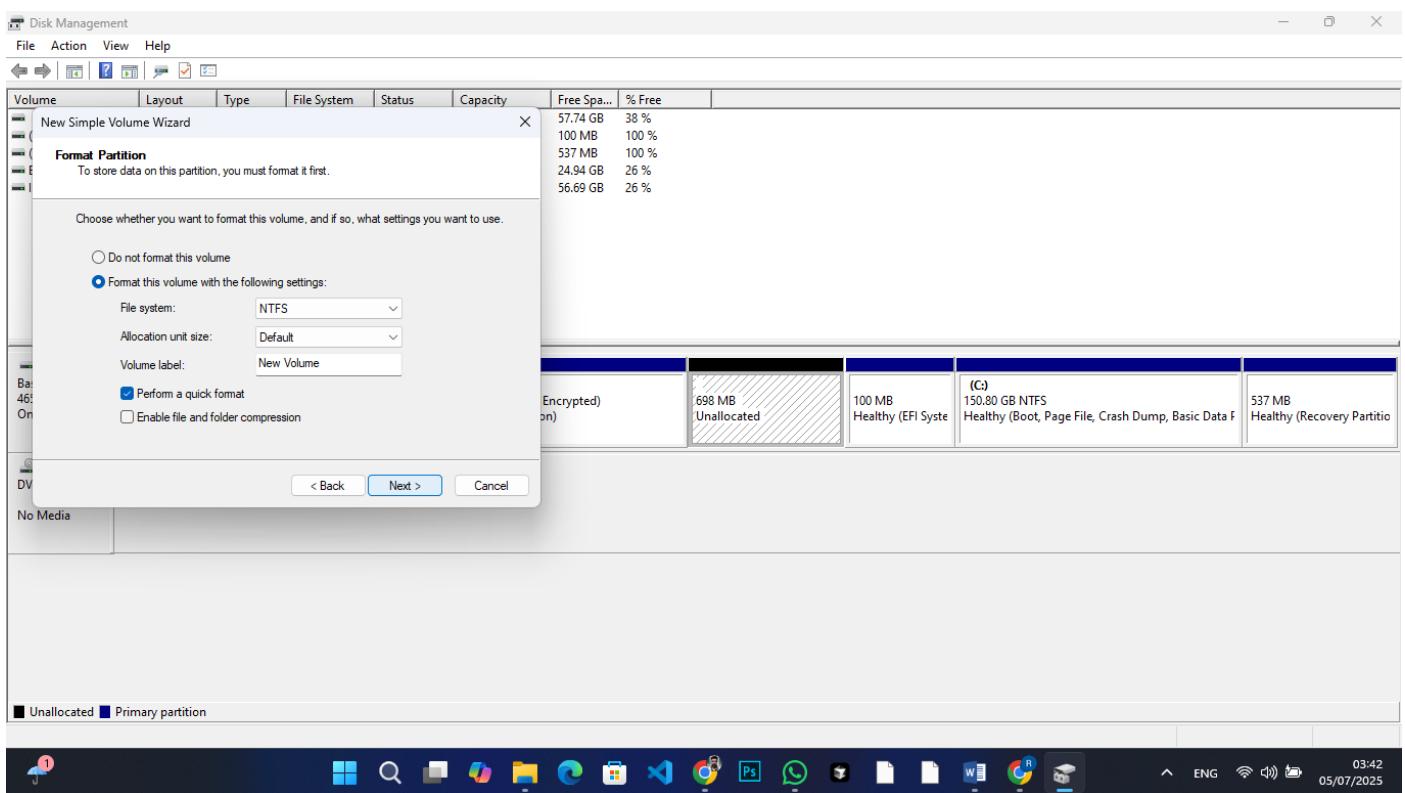


Figure 29 Create New Partition

Some Pictures are Copy in this Partition

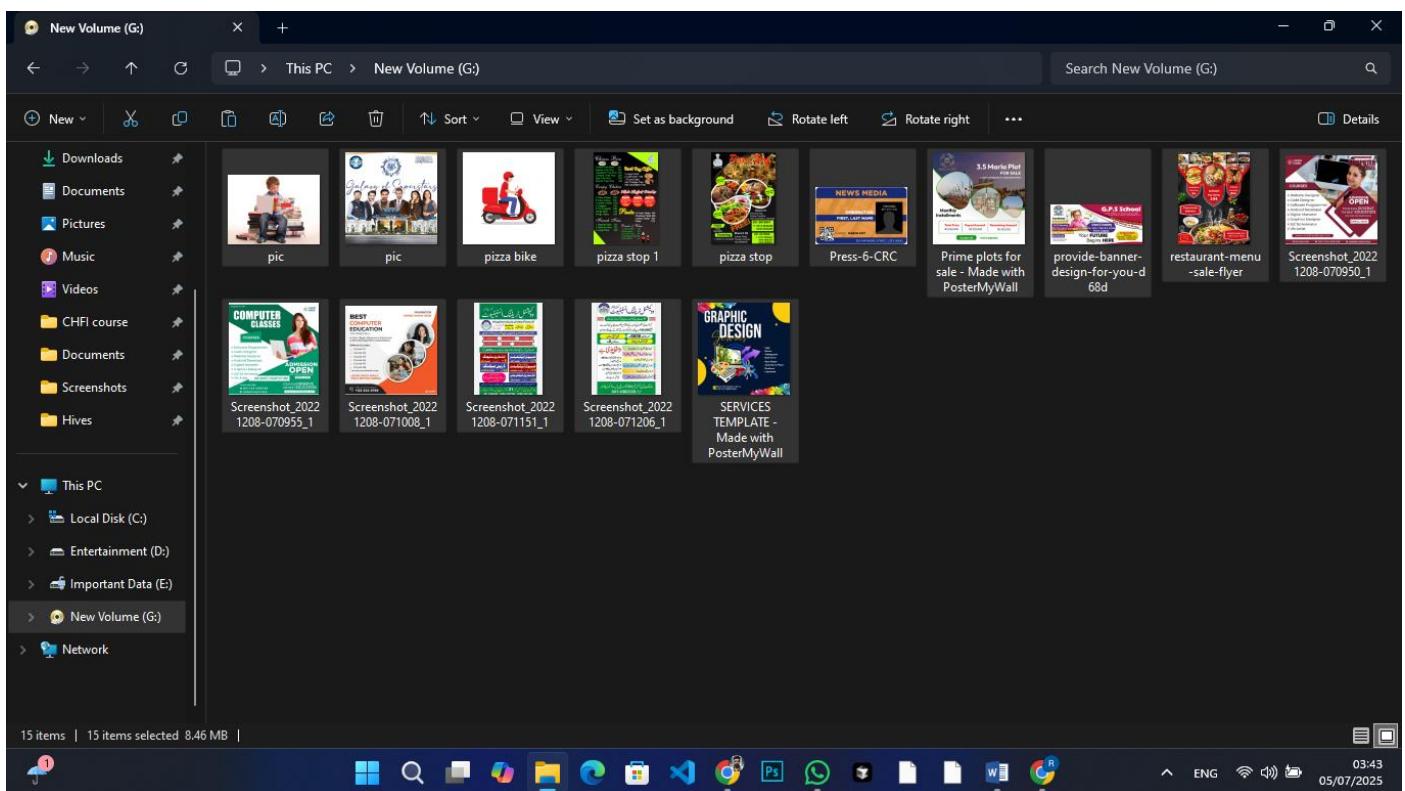


Figure 30 Copy Some Pictures

Format this Partition

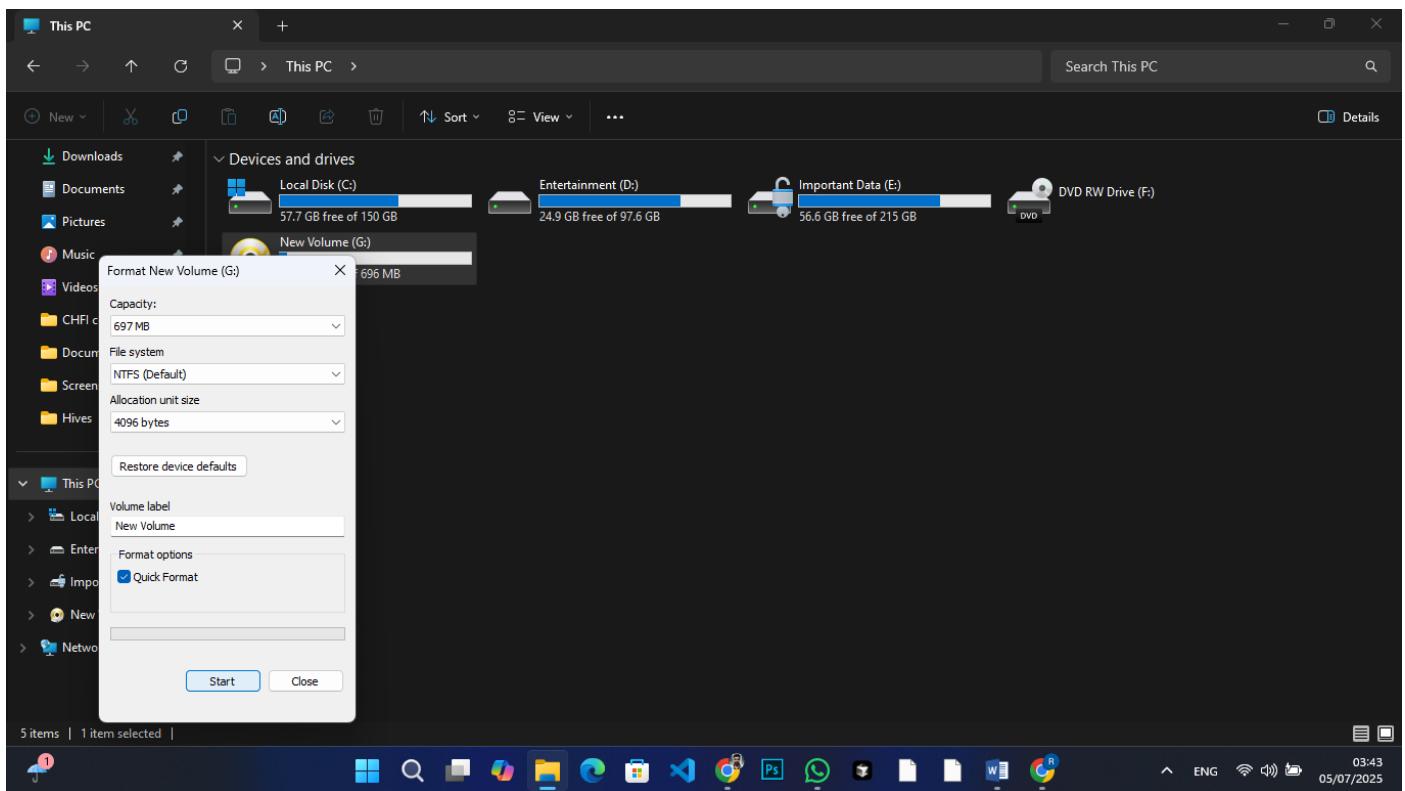


Figure 31 Format This Partition

Creating Image File using FTK Imager on this Partition

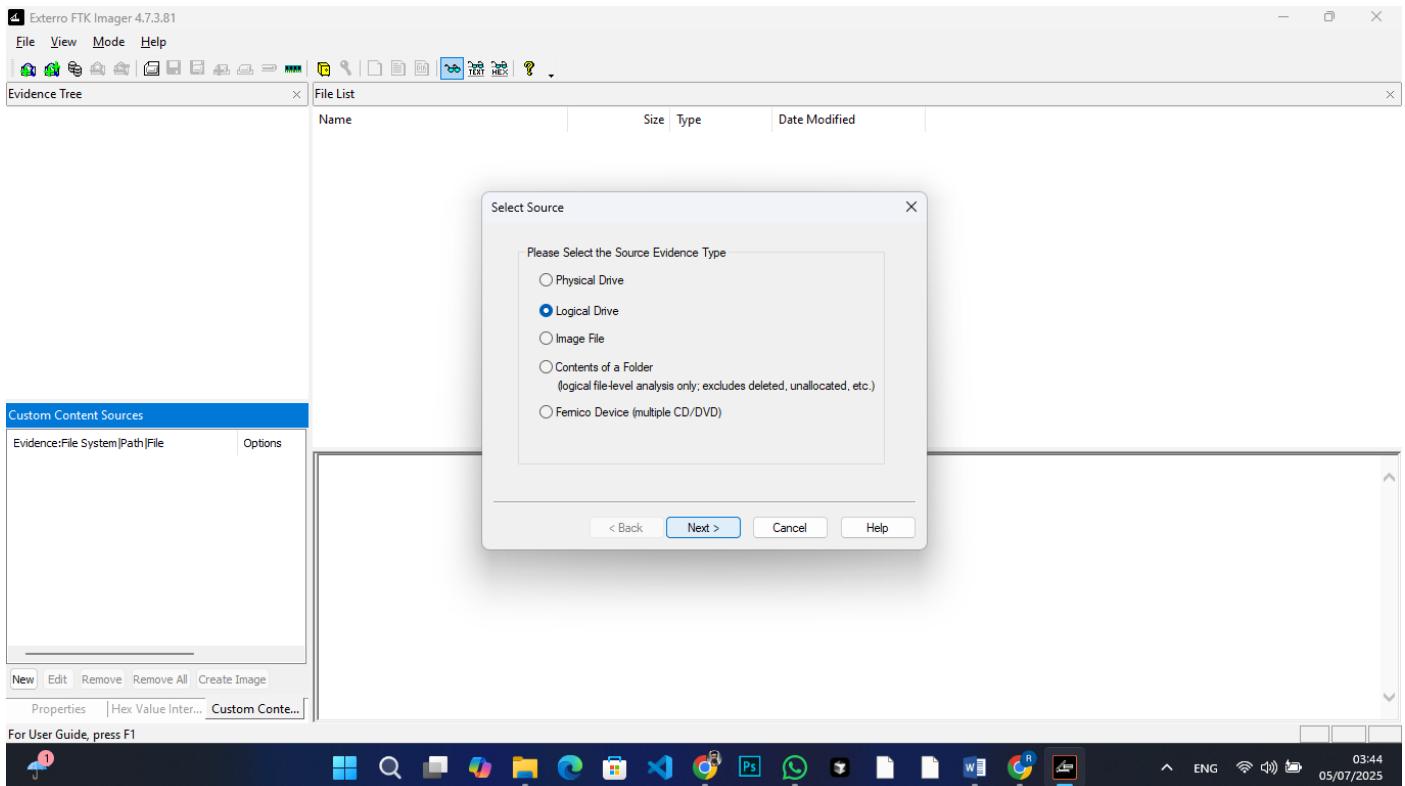


Figure 32 Select Logical Drive

Select Image Type (E01)

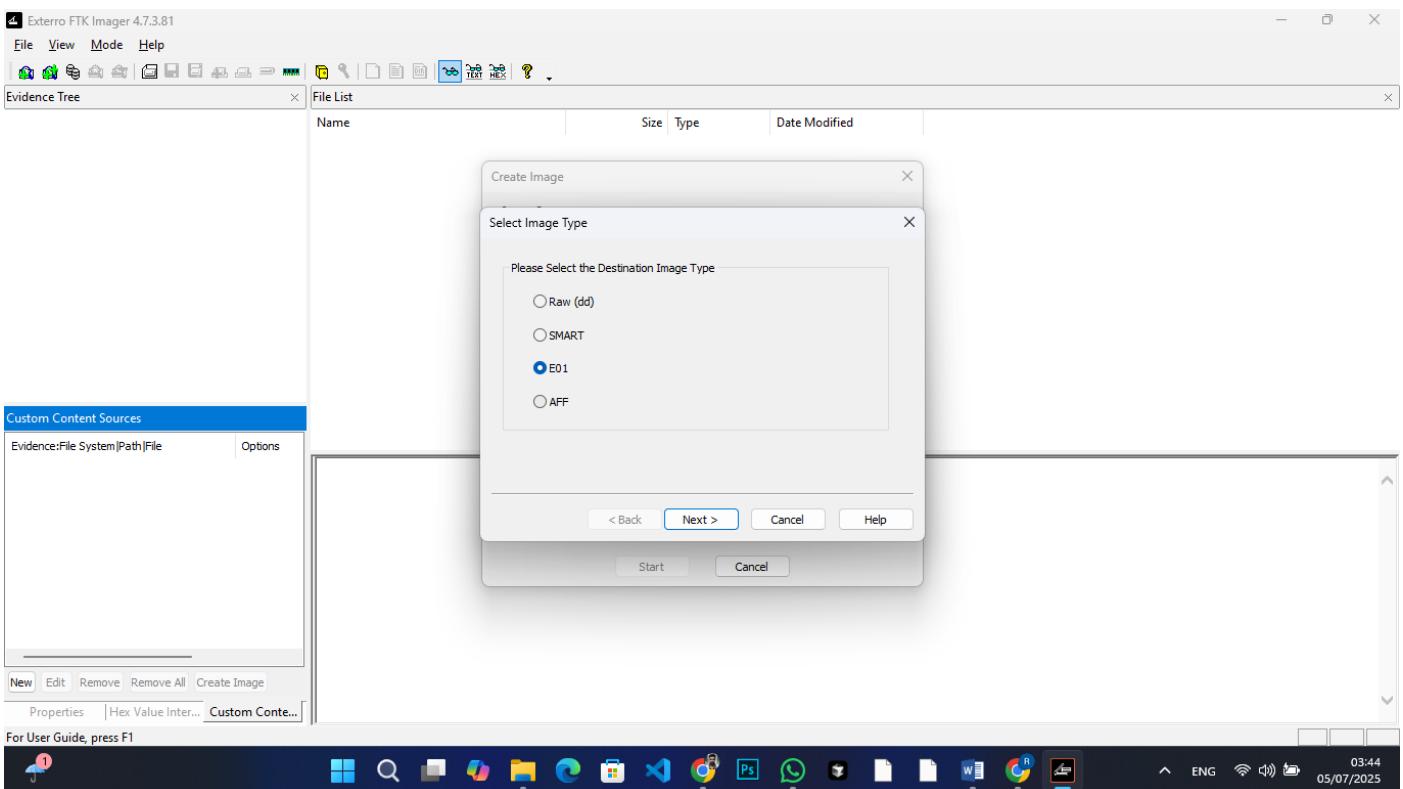


Figure 33 Select Image Type (E01)

Creating Image

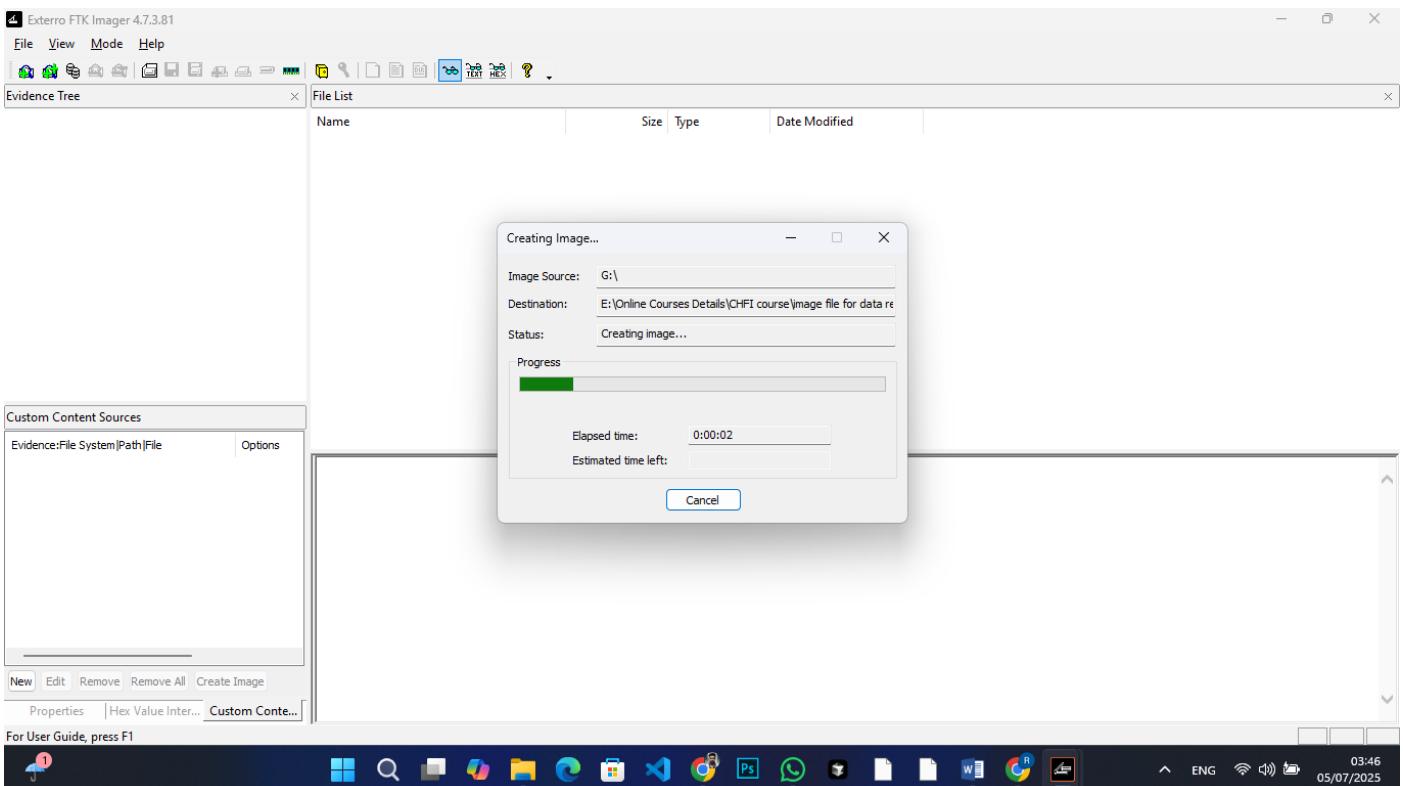


Figure 34 Creating Image

Image Summary

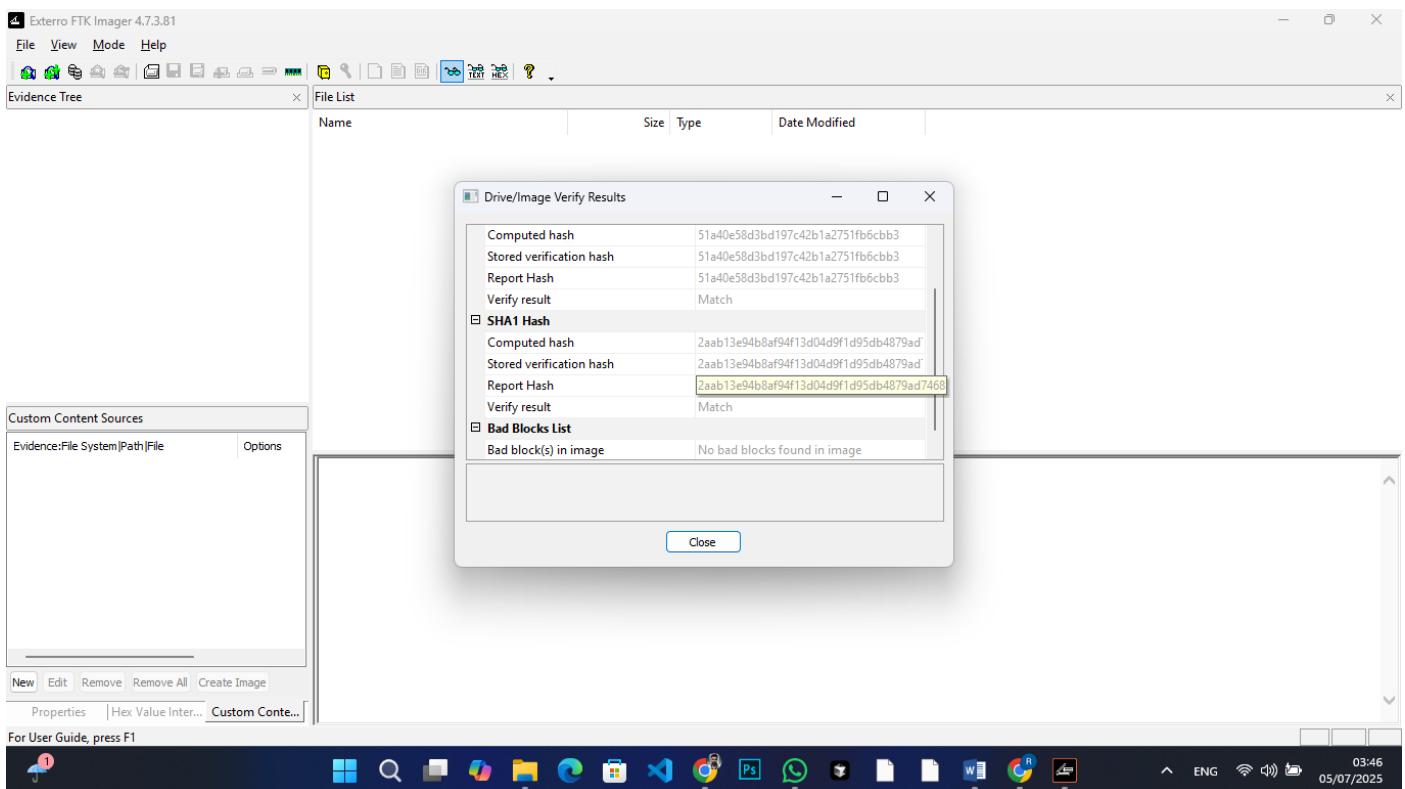


Figure 35 Image Summary

Data Recovery from image using Autopsy

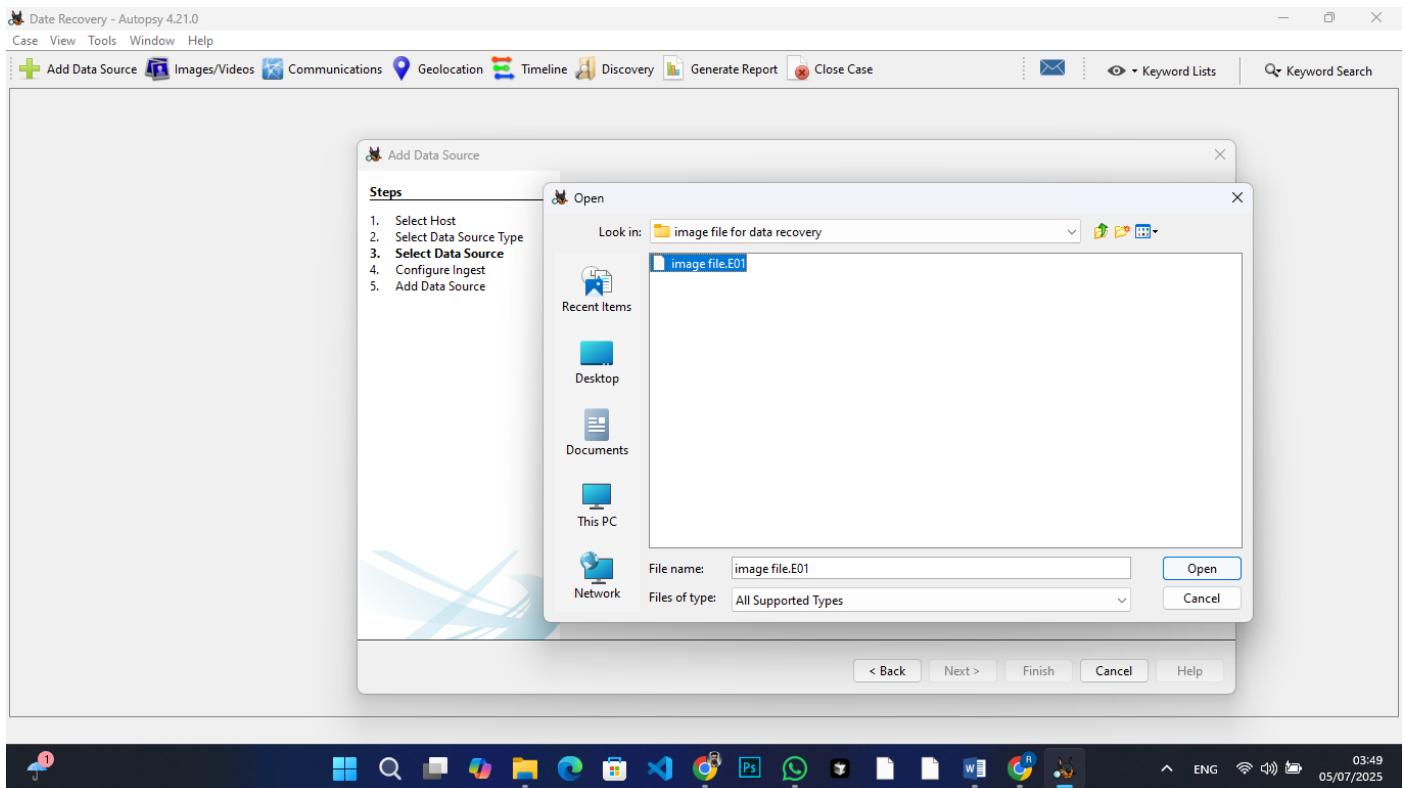


Figure 36 Select Image File

Select Configuration in autopsy

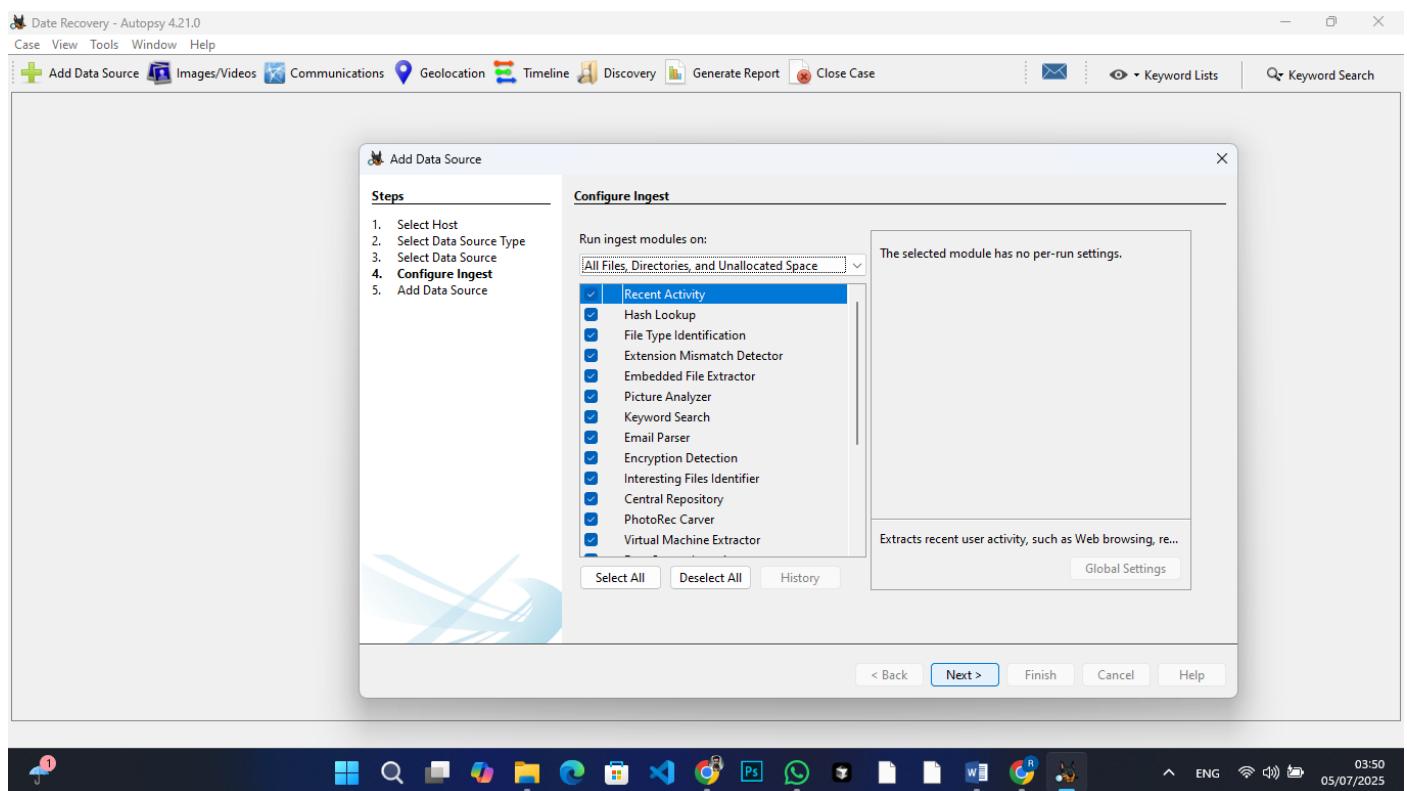


Figure 37 Configuration Import

Load Image File in Autopsy

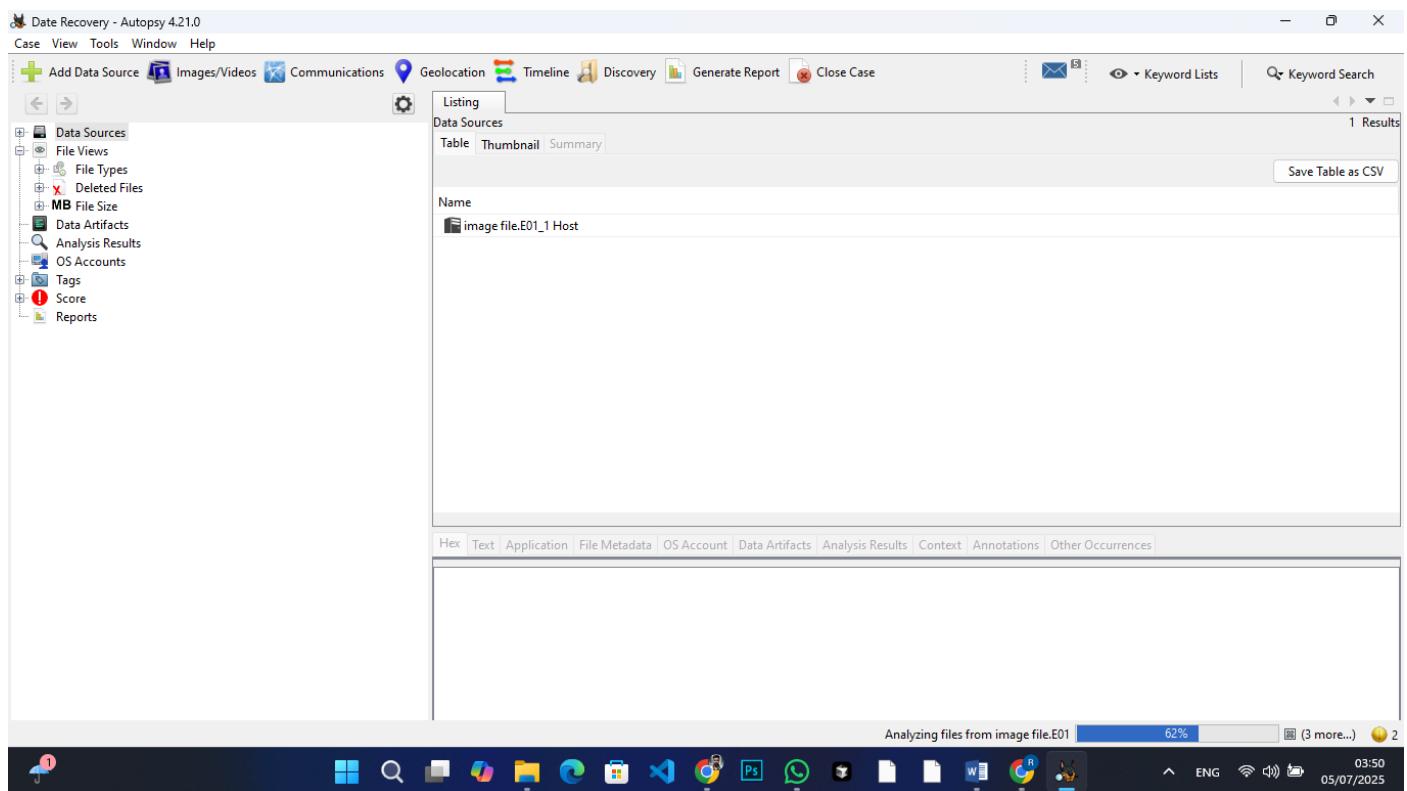


Figure 38 Load Image File in Autopsy

Deleted Files from Autopsy

Figure 39 Deleted Files

Export Deleted Files

Figure 40 Export Deleted Files

All Images Recover

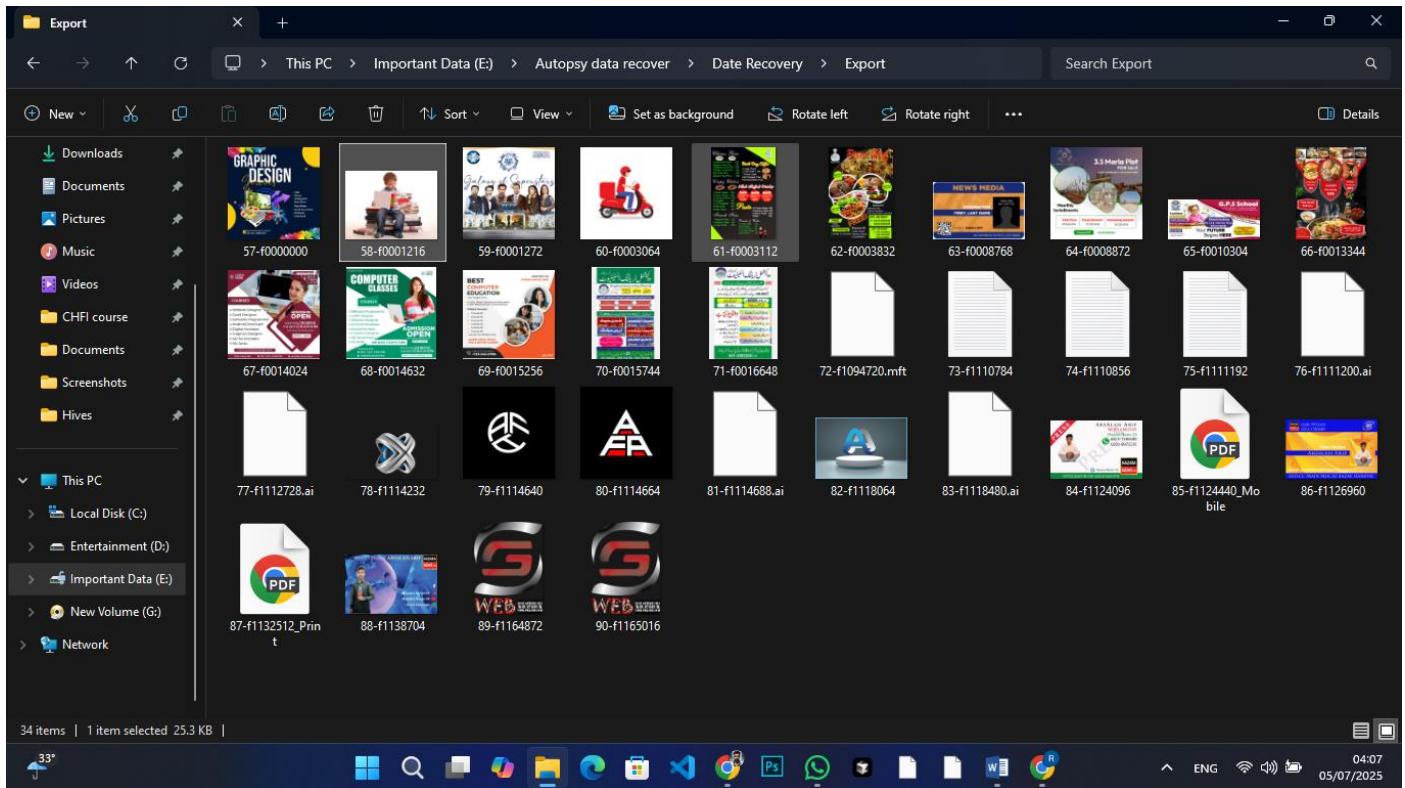


Figure 41 All Images Recover

Image Metadata Using Exif Tool

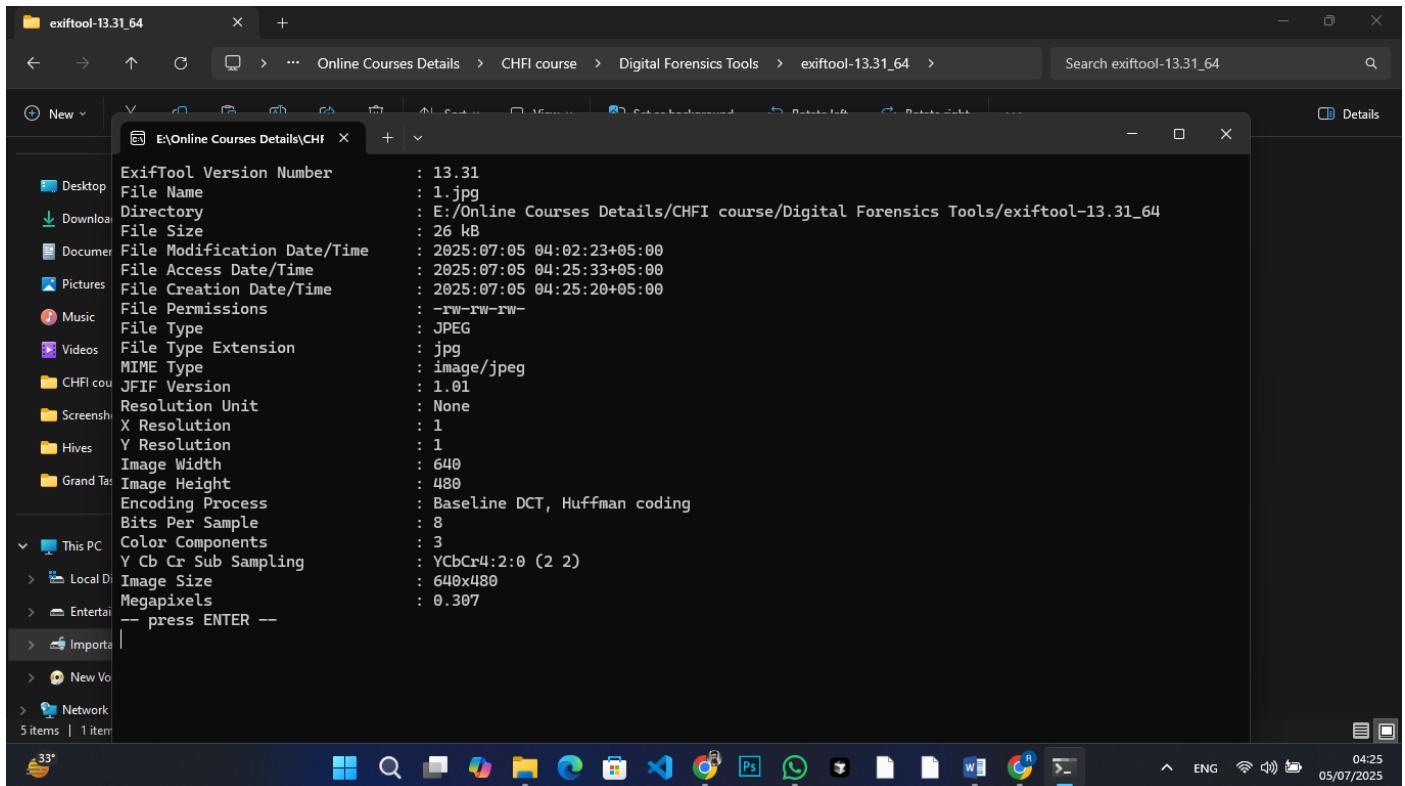


Figure 42 Image Metadata Using Exif Tool

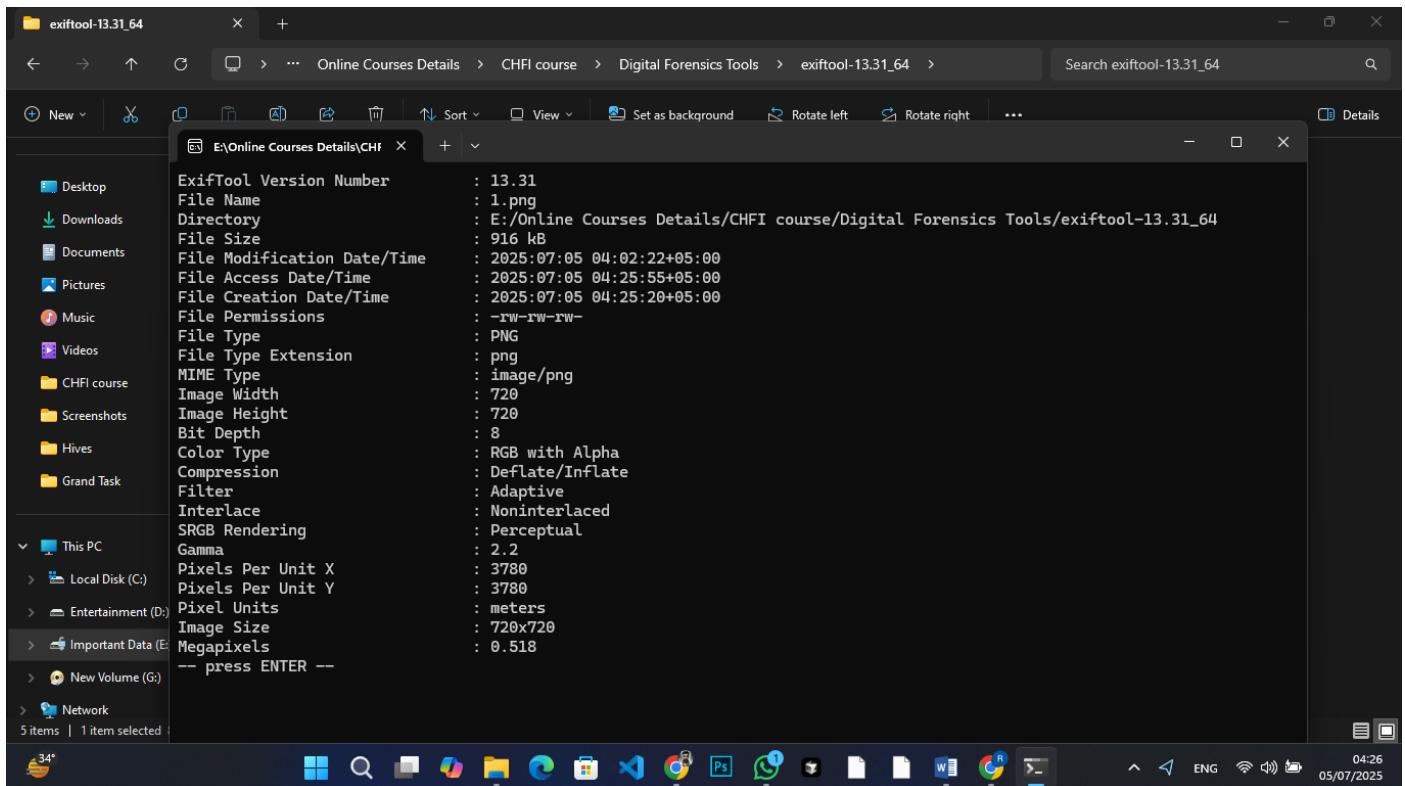


Figure 43 Image Metadata Using Exif Tool

5.5 What browser activity suggests credential theft or staging?

Browser History Examiner (Tool)

Tool Download link: <https://www.foxtonforensics.com/browser-history-examiner/>

foxton
FORENSICS

Products ▾ Free Tools ▾ Support ▾ Resources ▾ Company ▾

Features Pricing FAQs User Guide Version History

FREE TRIAL BUY NOW

Professional tool to investigate web browser history

Browser History Examiner (BHE) is a forensic software tool for capturing, analysing and reporting internet history from the main desktop web browsers.

Chrome Edge Firefox Internet Explorer 10/11 Safari

BHE can assist in various digital investigations such as civil & criminal digital forensics cases, security incidents, human resources investigations and general employee activity reporting.

Figure 44 Browser History Examiner

I install the tool than open trial version

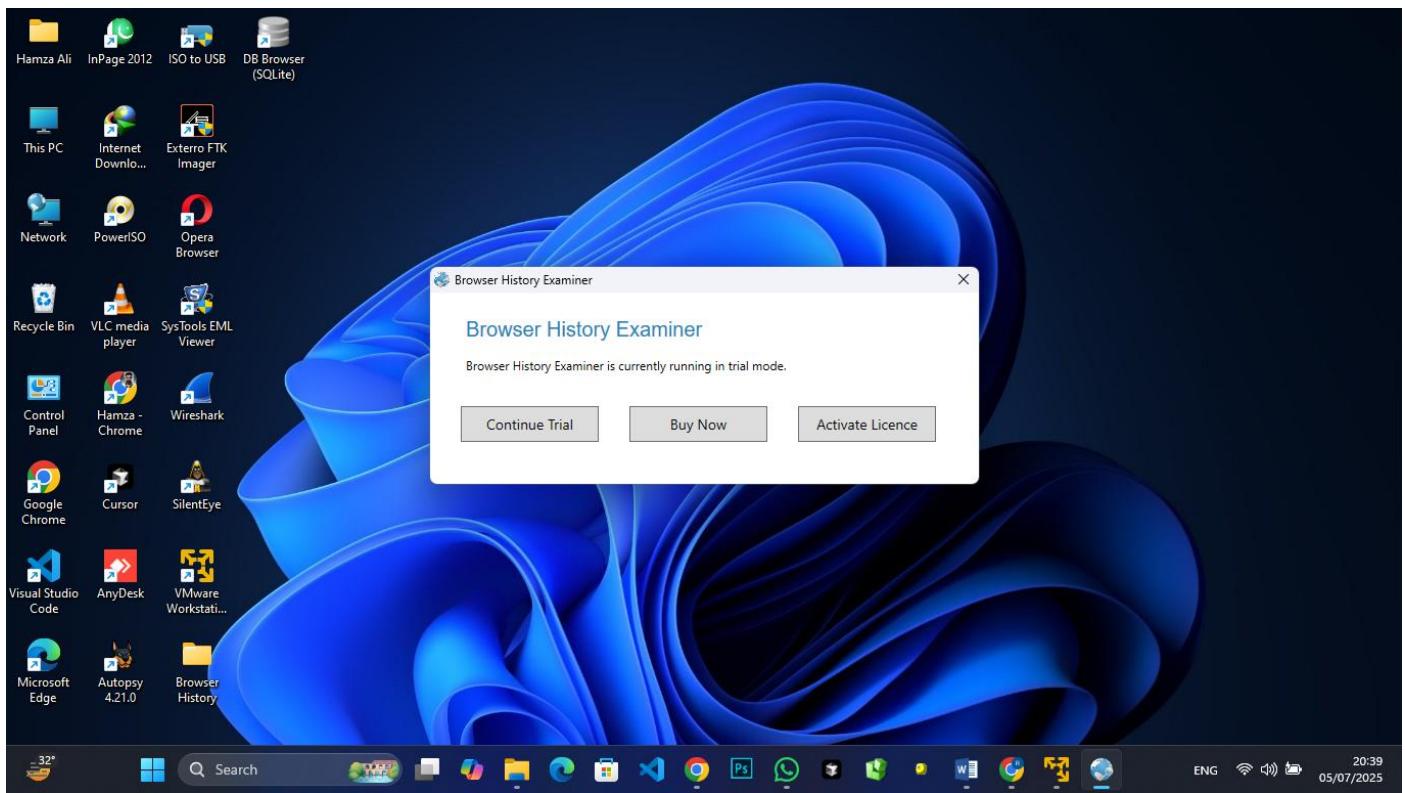


Figure 45 click Trial Version

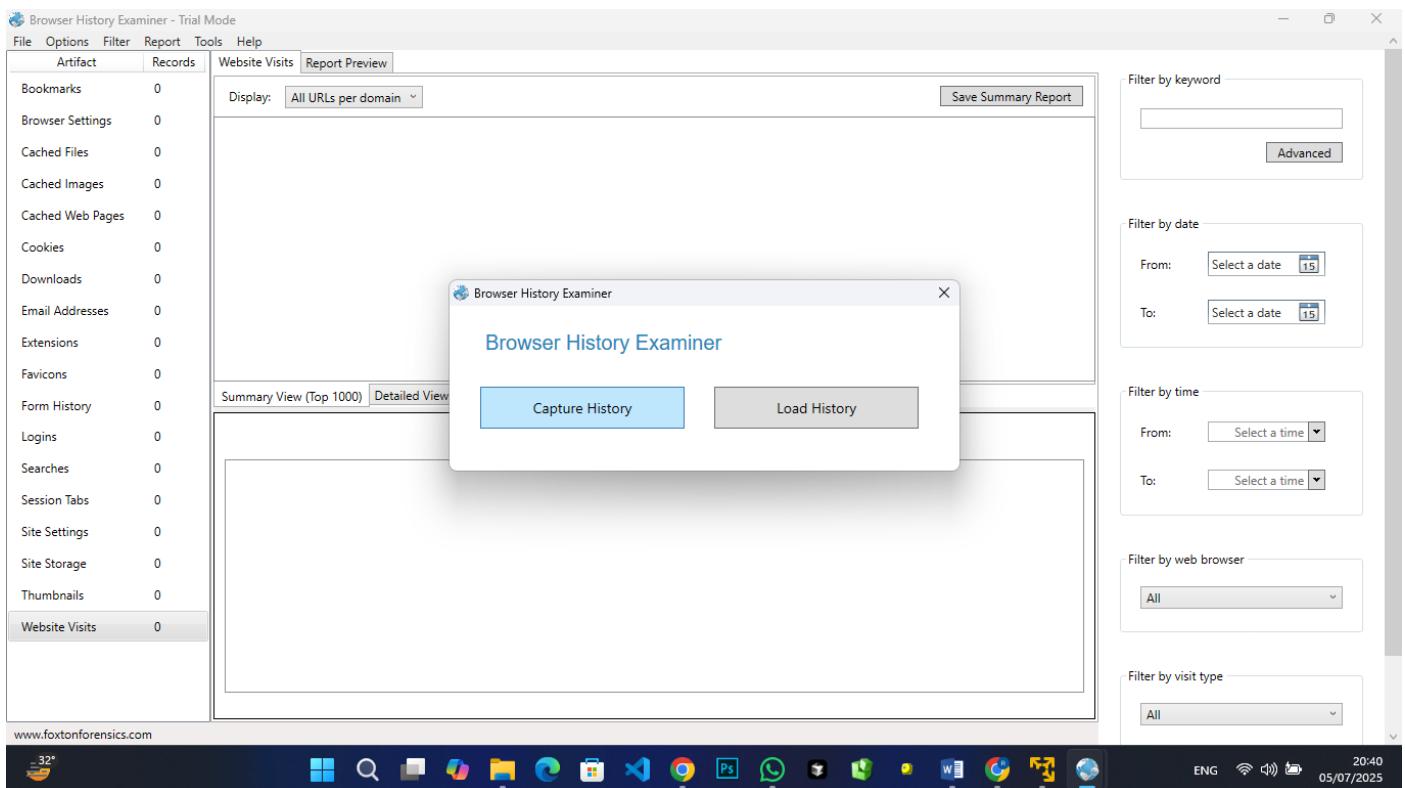


Figure 46 Capture Memory

Select history from this Computer

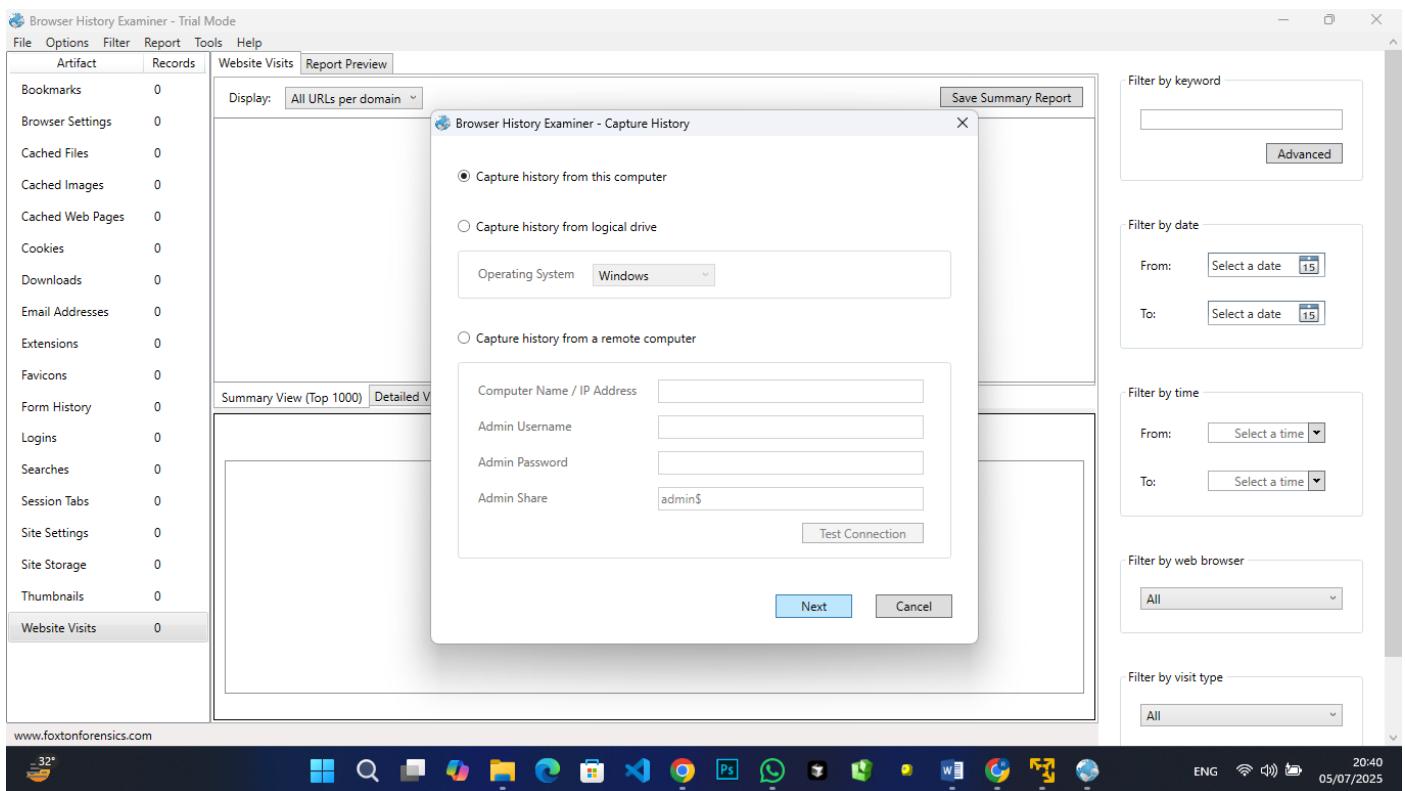


Figure 47 Select History from this Computer

Choose Browsers

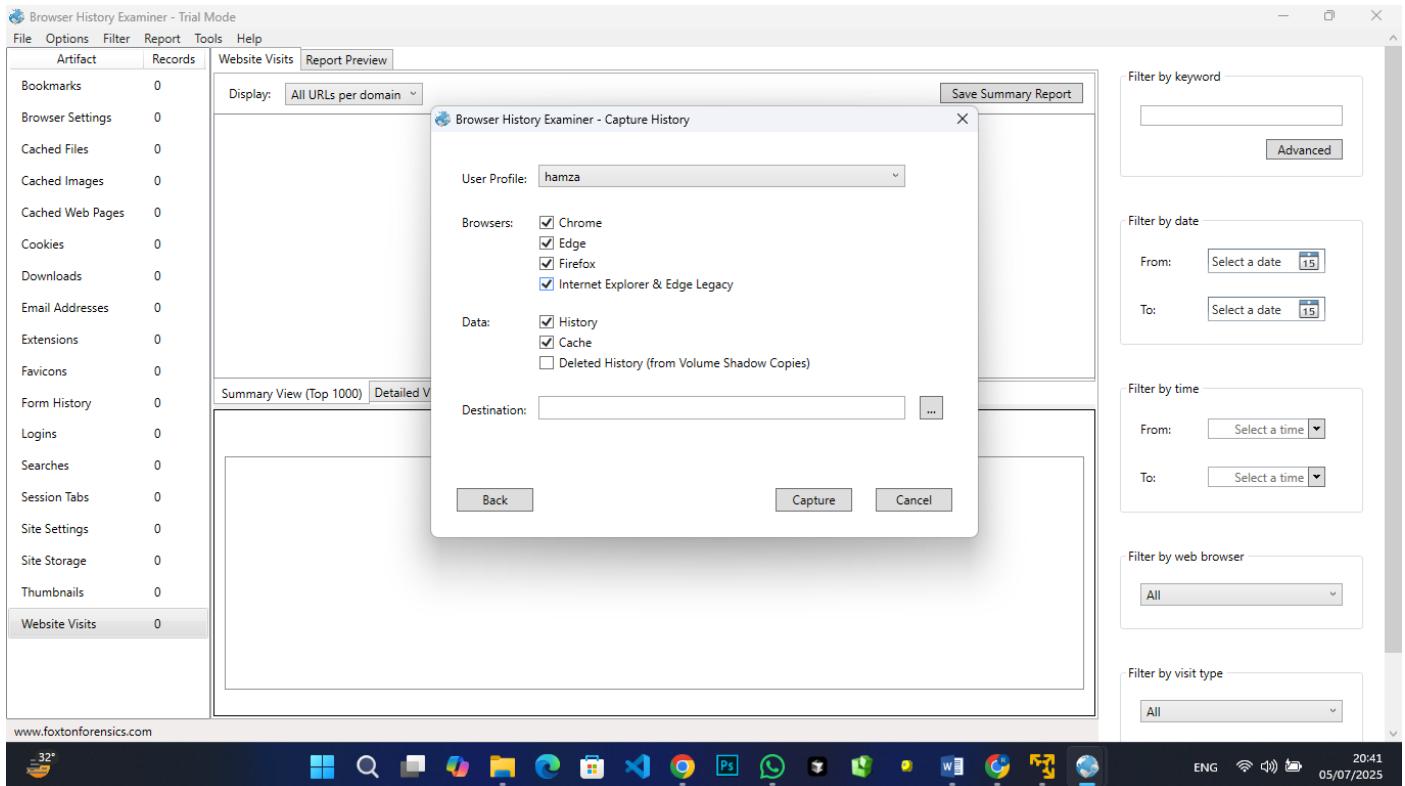


Figure 48 choose Browsers

Choose Destination Where save the files

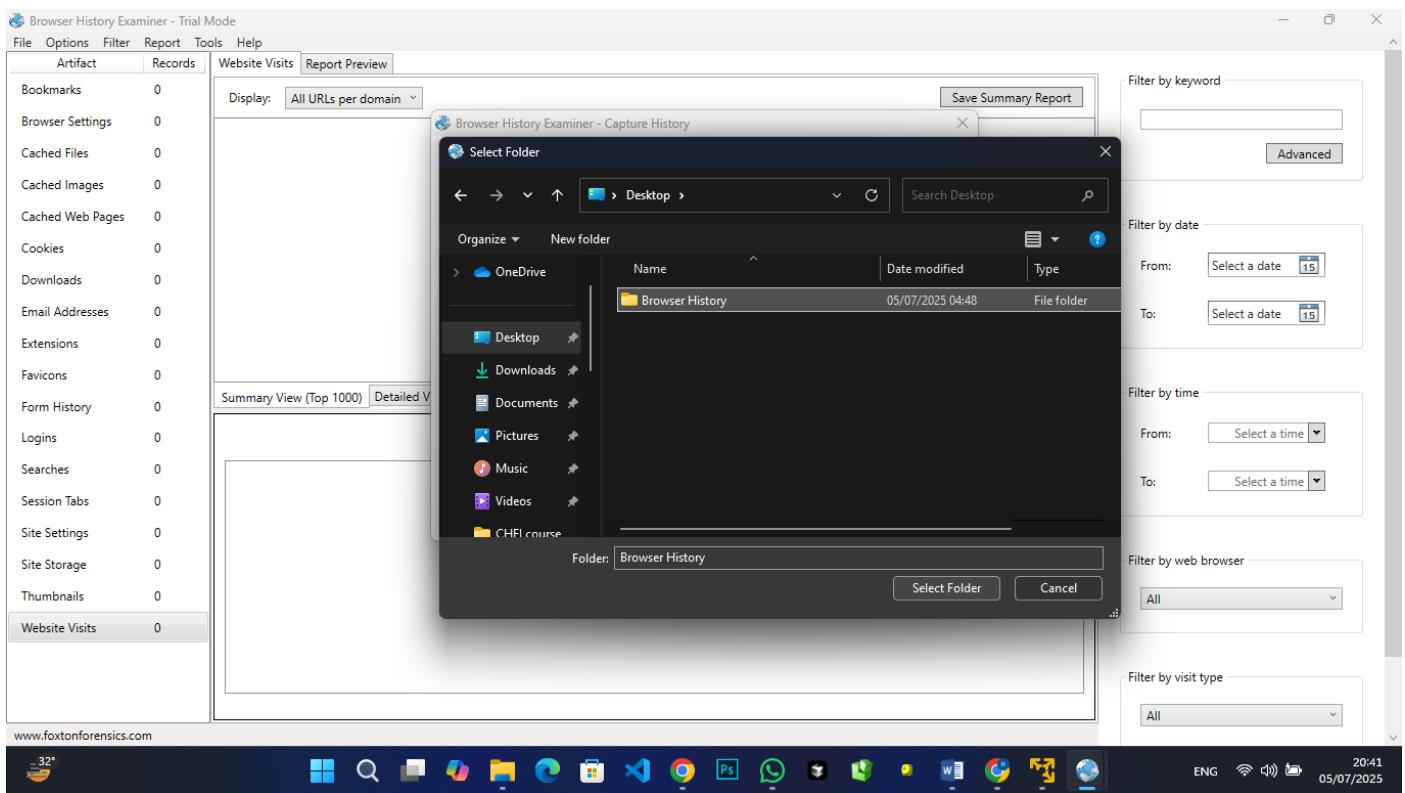


Figure 49 choose Destination

And then Start Capture Memory

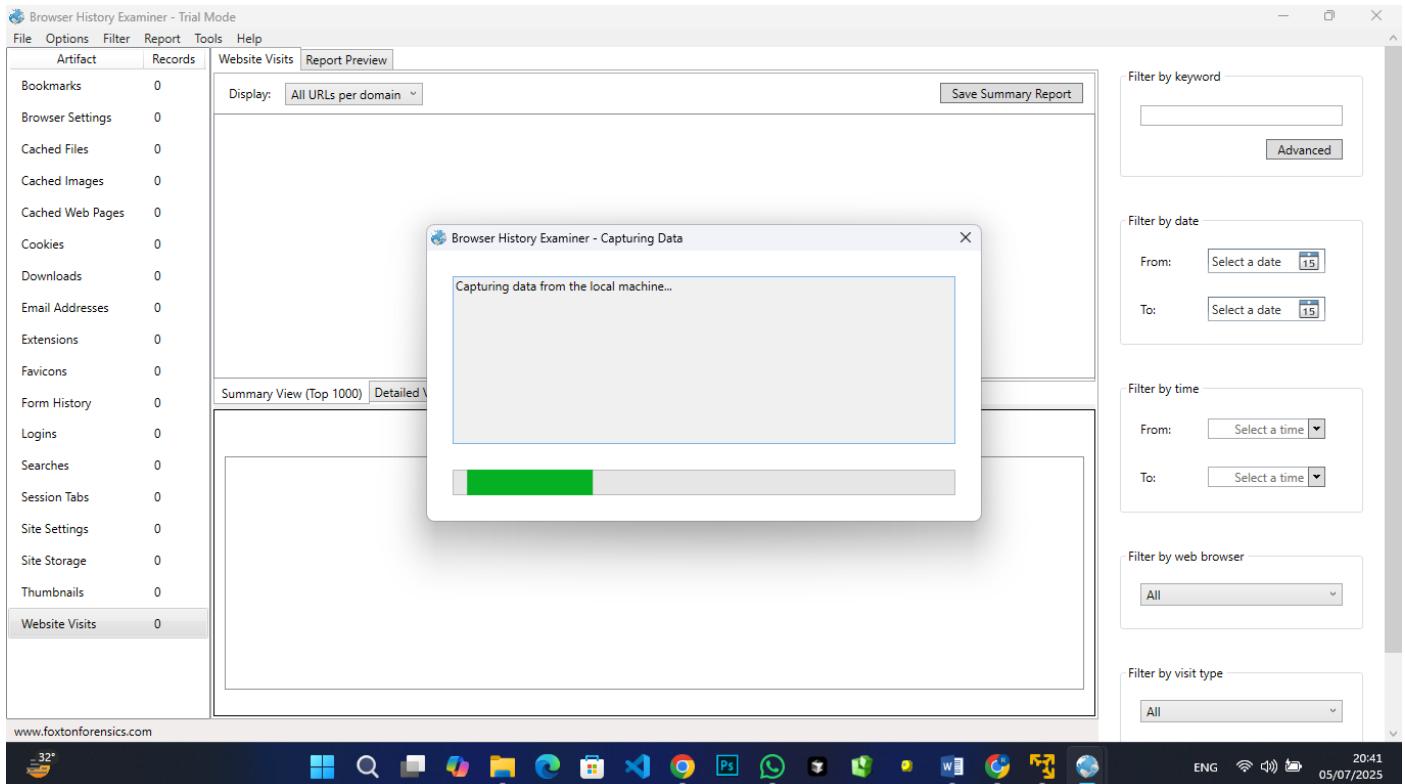


Figure 50 Capturing Browser History and Details

All Browsers History

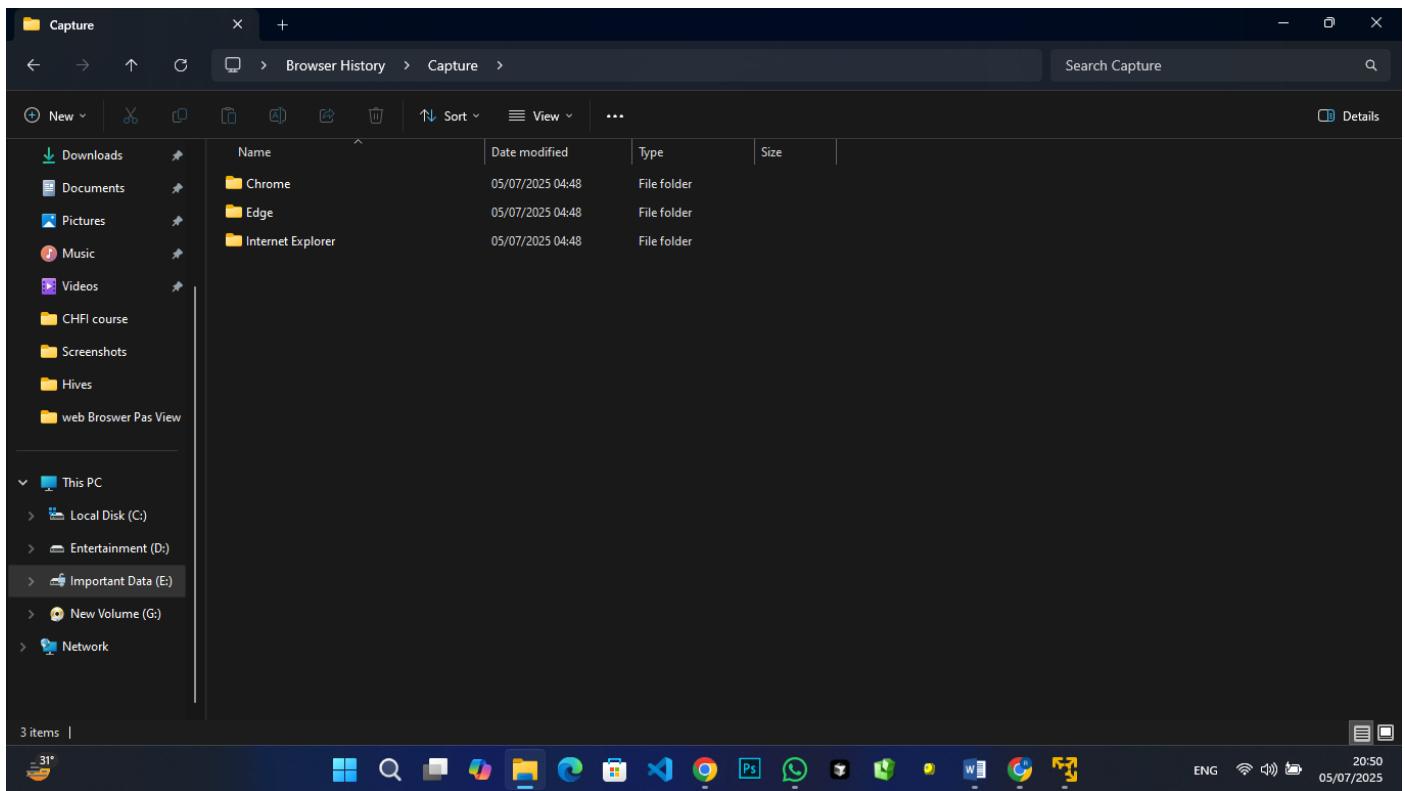


Figure 51 All Browsers History

Chrome history Profile-2 (All Recent Websites)

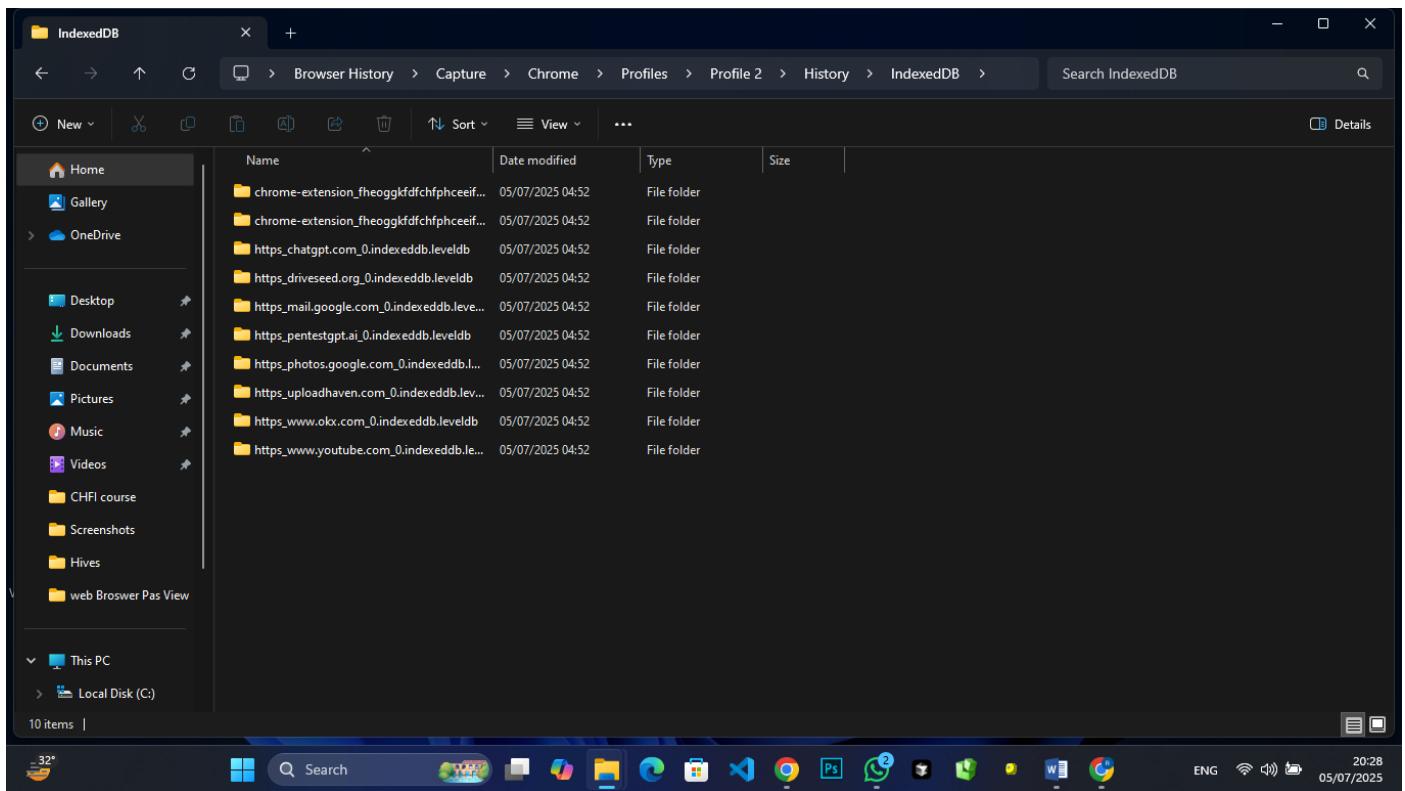


Figure 52 All Recent Websites

Login Details with websites Timestamps

Figure 53 Browser websites login details with Timestamps

5.6 Can you build a precise attack timeline using event logs?

Search (eventvwr.msc) in run command

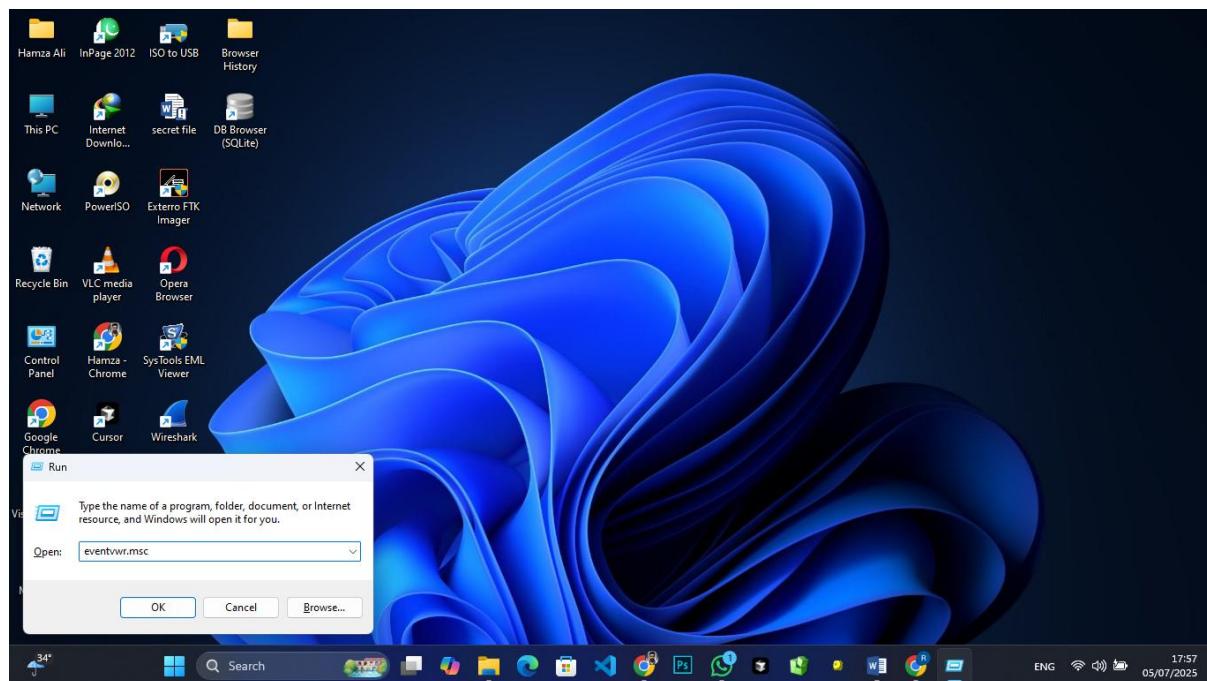


Figure 54 Search window event viewer

Opening Window Event Viewer

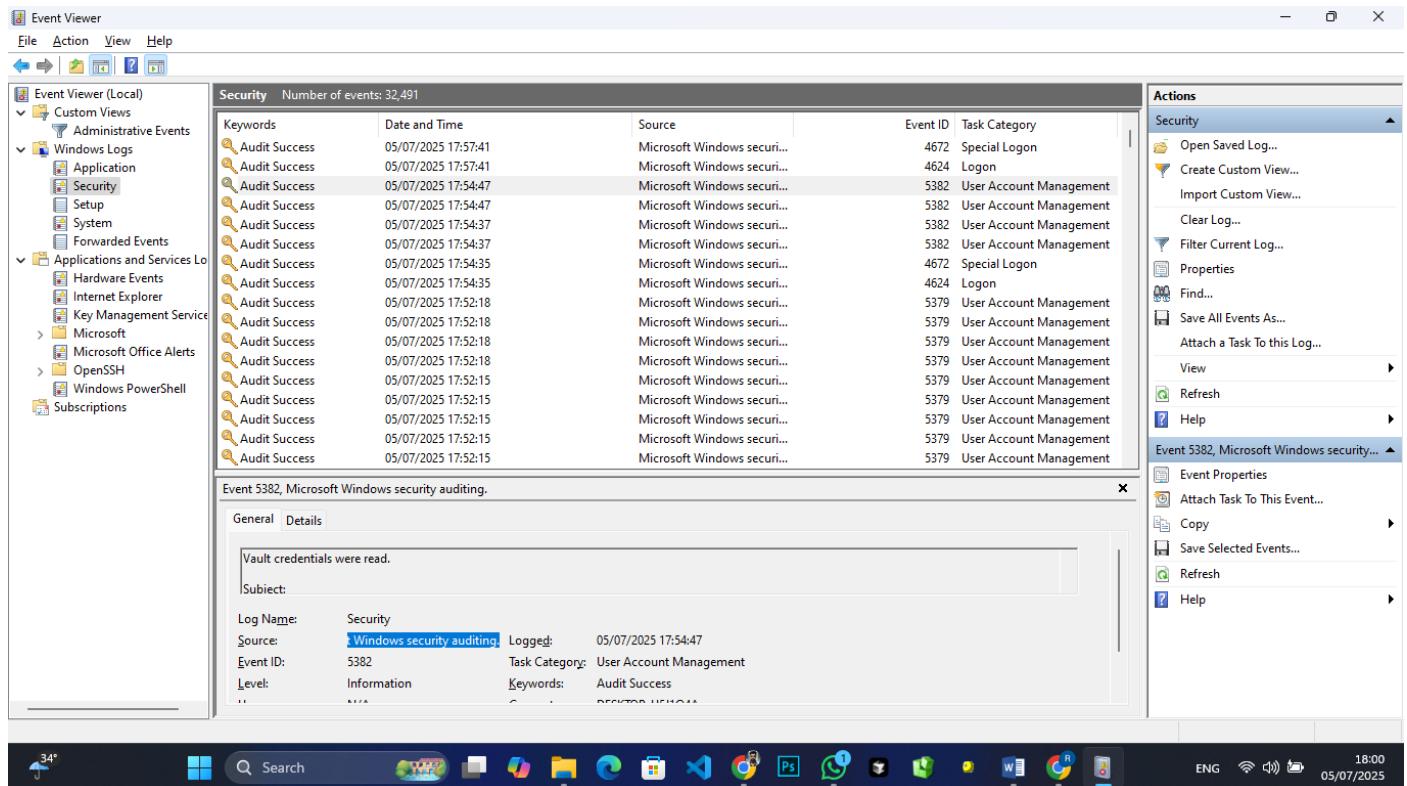


Figure 55 Window Event Viewer Security details

5.7 What network artifacts indicate exfiltration?

Device Linux

Open Wireshark through the terminal

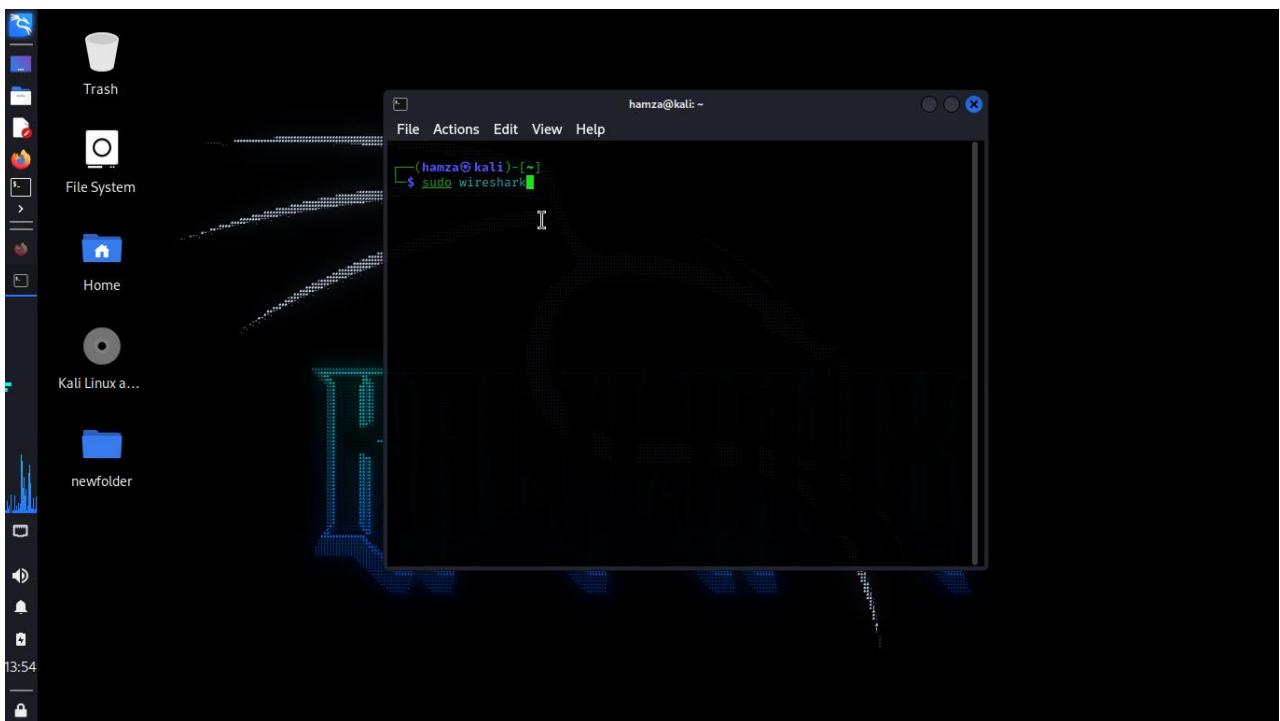


Figure 56 Open Wireshark through Linux terminal

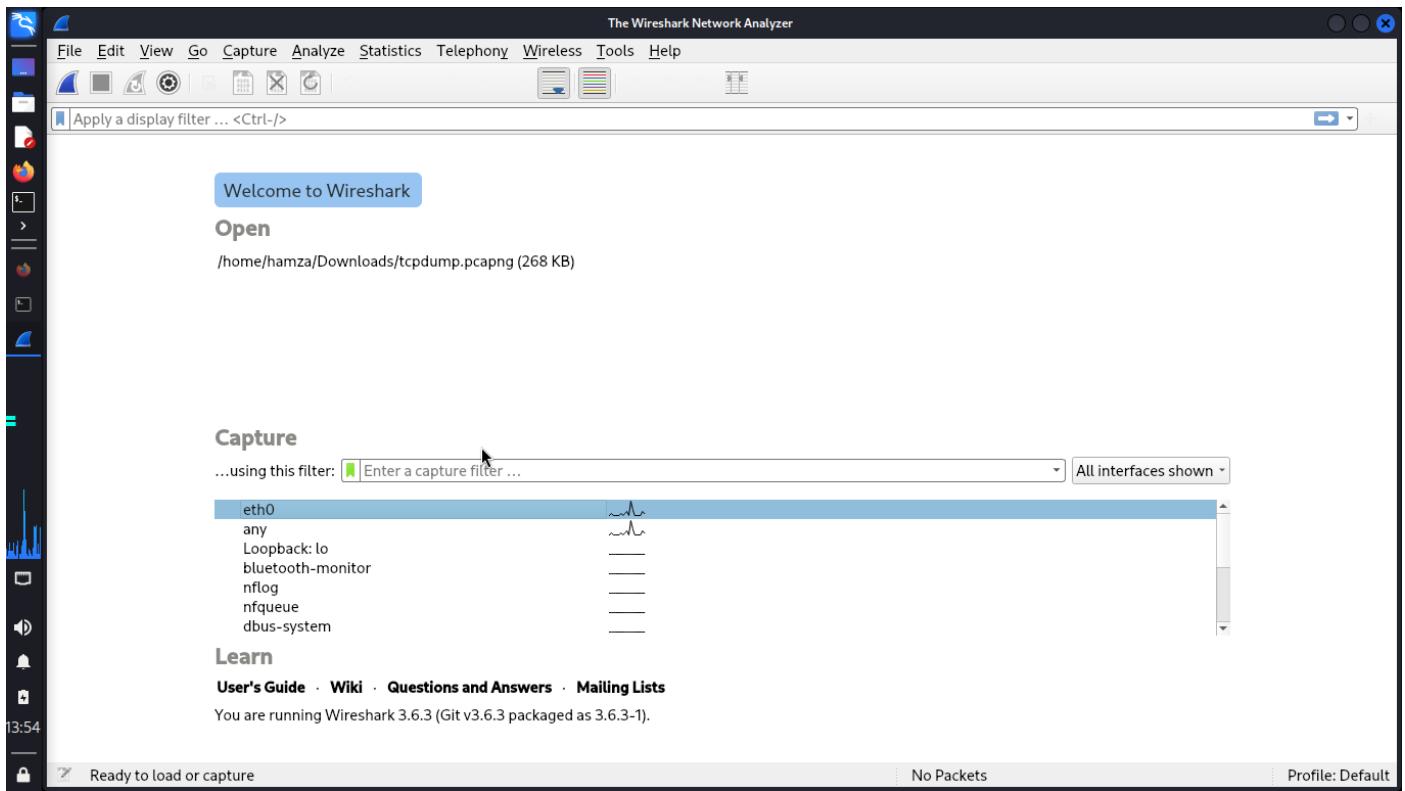


Figure 57 Click eth0

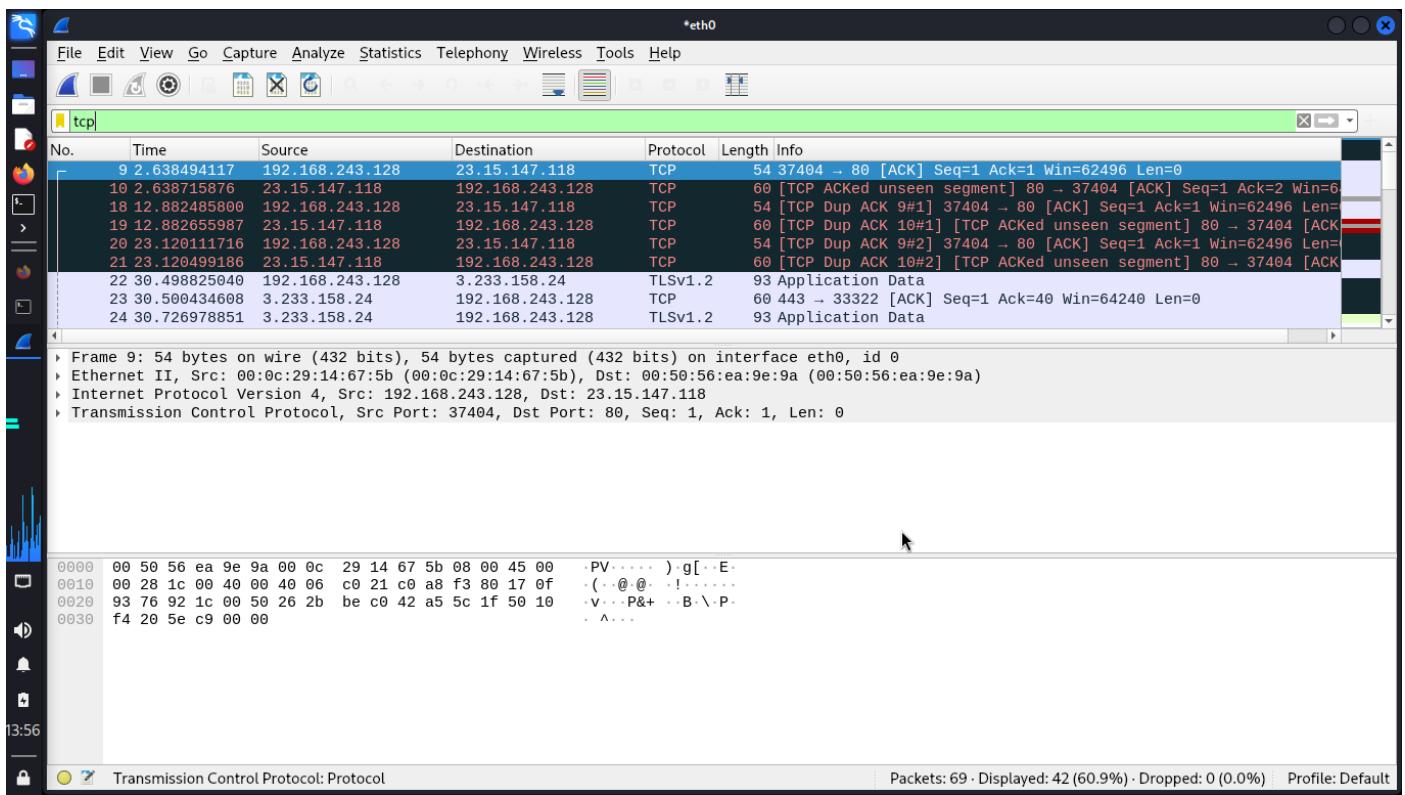


Figure 58 Filter TCP in Wireshark

Save the Tcpdump.pcap file

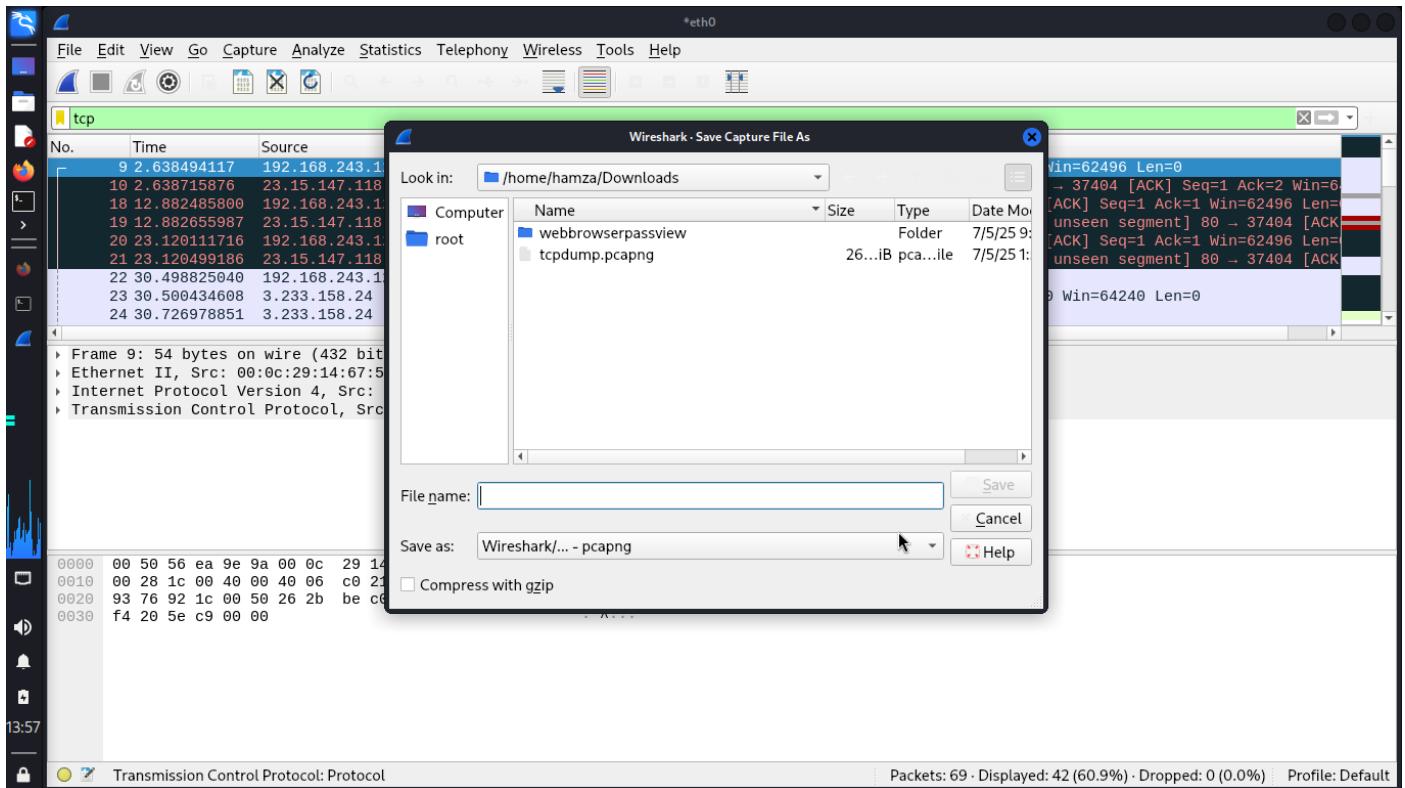


Figure 59 save the tecpdump.pcap file

And then reopen Wireshark and open the file (tcpdump.pcap)

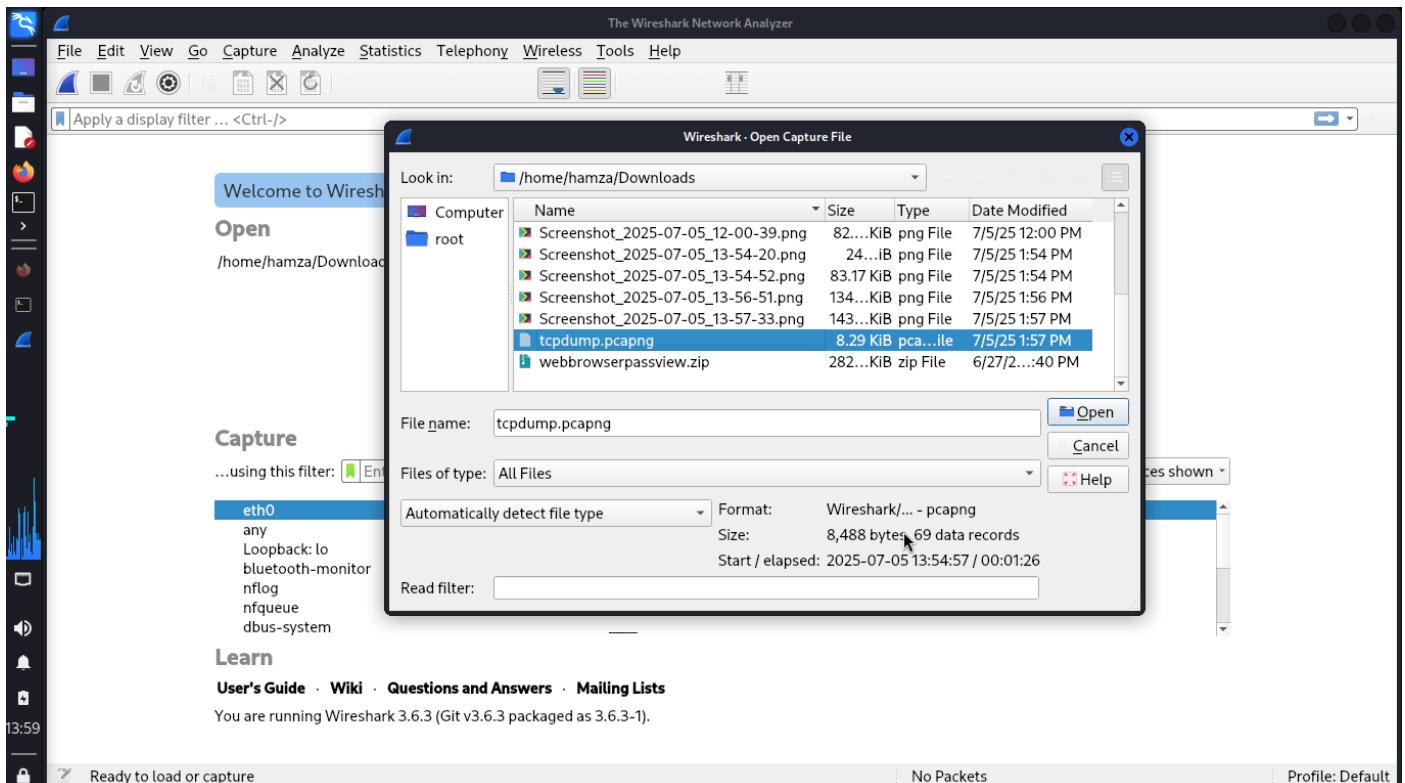


Figure 60 open file (tcpdump.pcap)

Click on Statistics tab and then click on Protocol Hierarchy

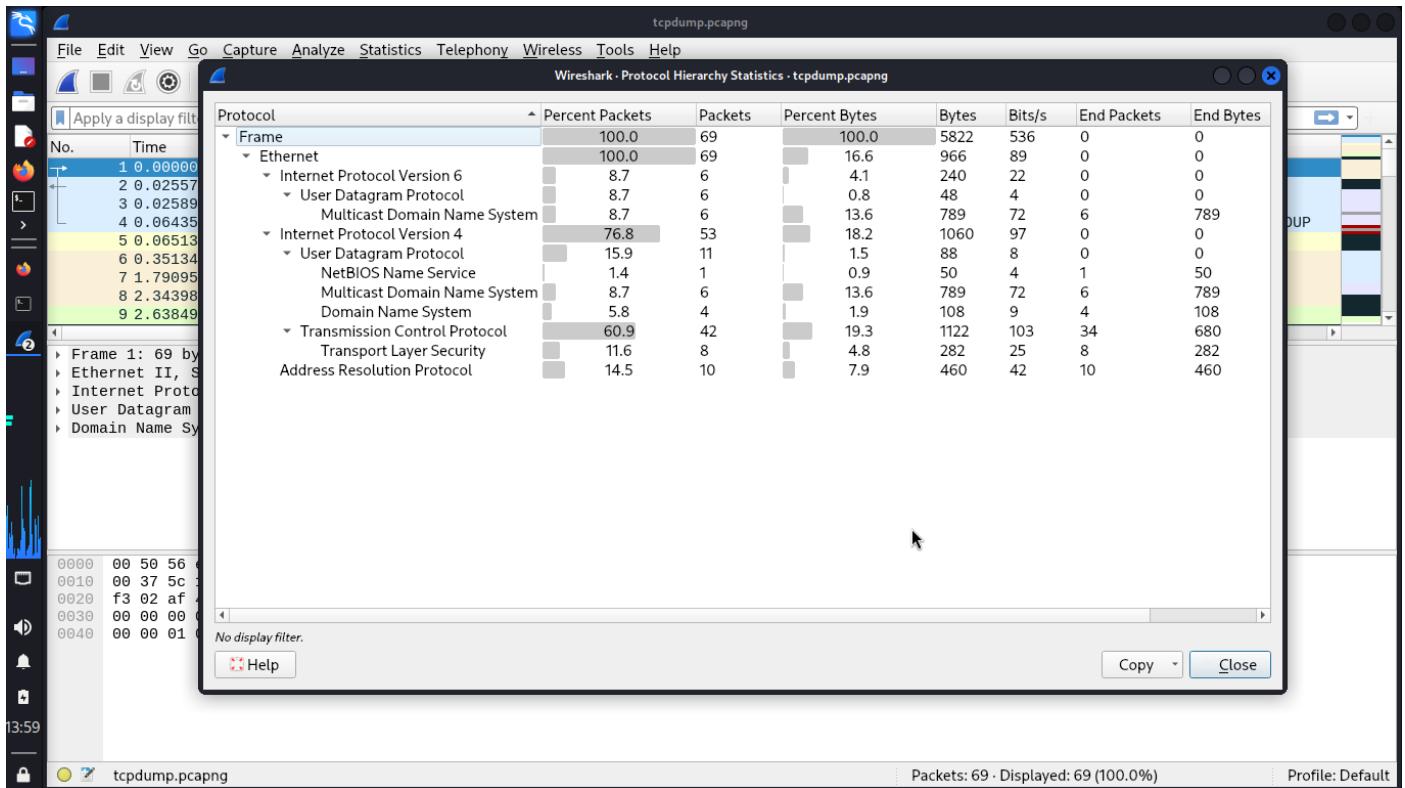


Figure 61 Protocol Hierarchy

Click on Statistics tab and then click on Conversation IP4-6 and sort by Bytes

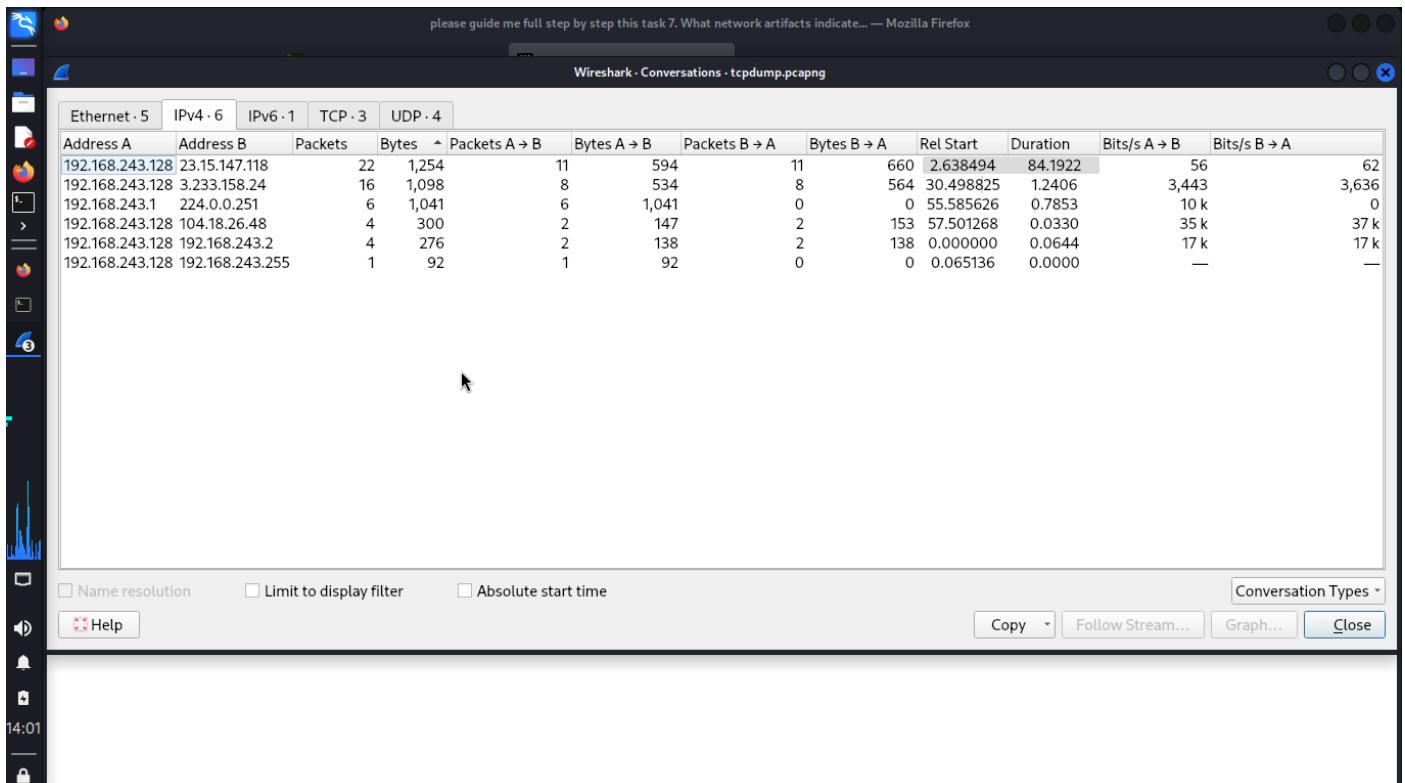


Figure 62 IP4-6 and Sort by Bytes

5.8 What malware behaviours and system changes were observed?

Device: Linux

Virus Total (Tool) use for Malicious file analyse

Tool link: <https://www.virustotal.com/gui/home/upload>

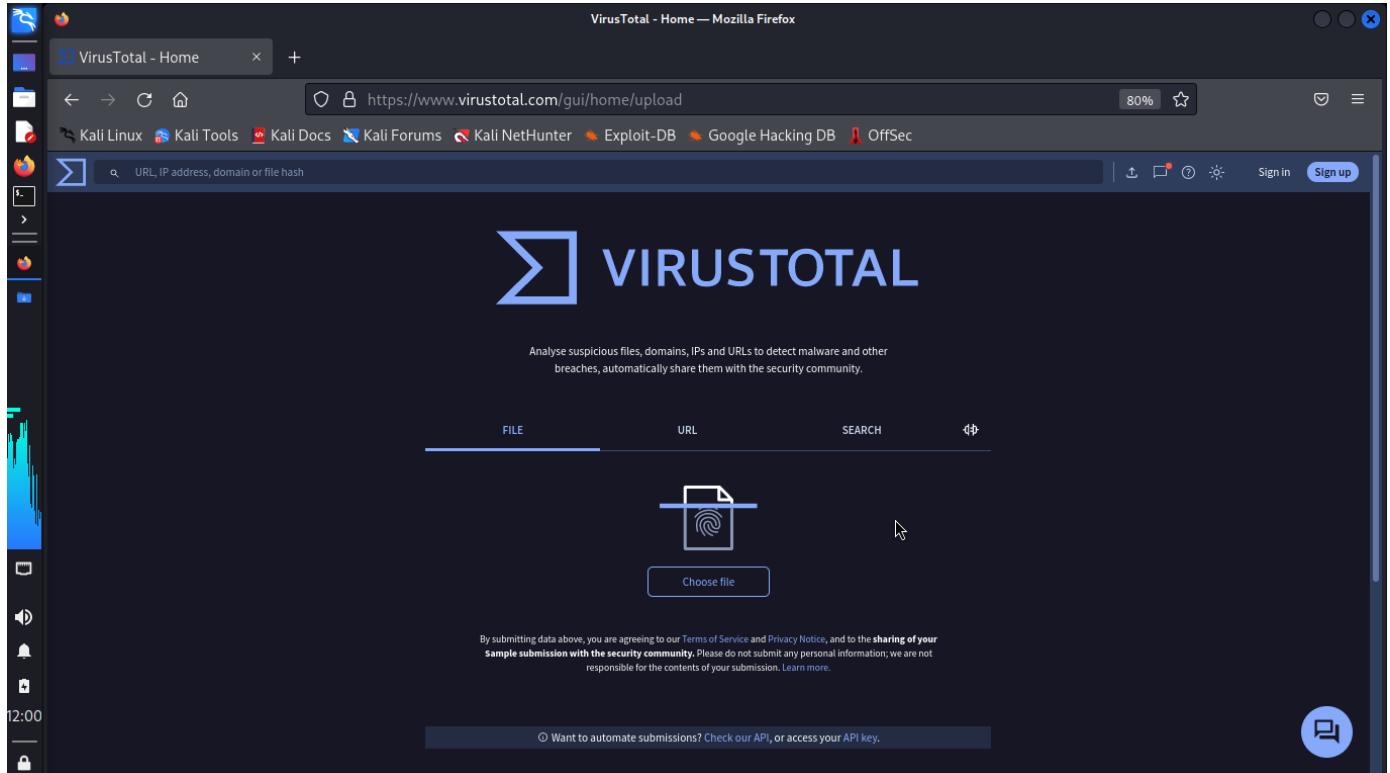


Figure 63 Virus Total

Upload a Malware (.exe) file

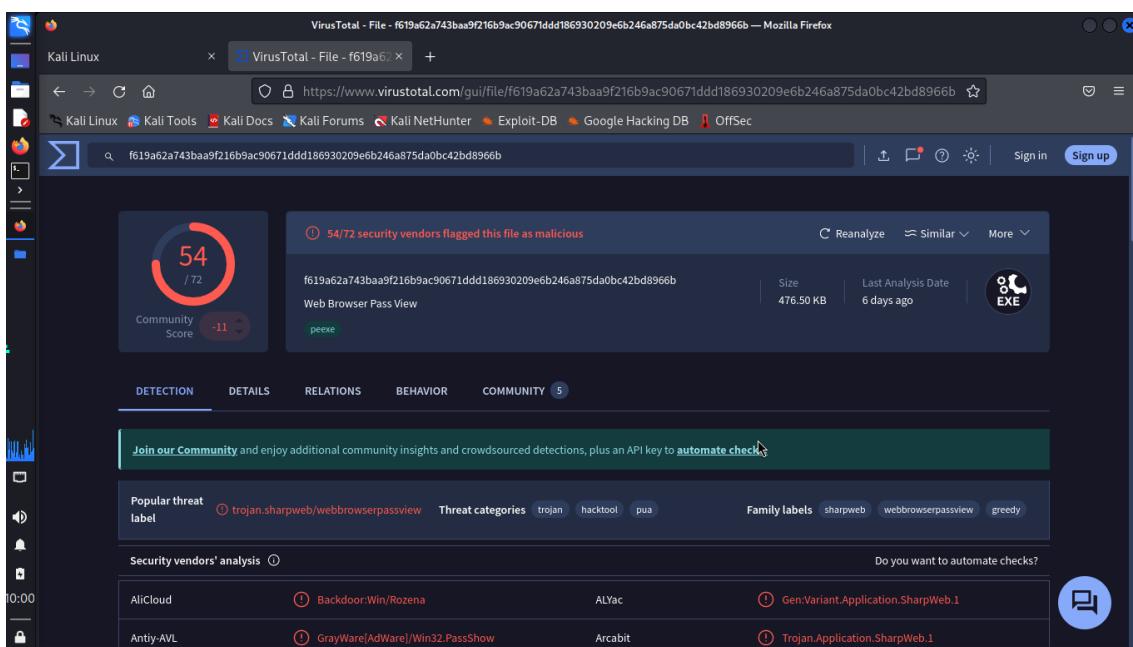


Figure 64 upload a (.exe) file

Hashes (.exe) file and Other Details

The screenshot shows the VirusTotal analysis interface for a file with MD5 hash 2d00d328619b93274f7e547f226b6d29. The 'Basic properties' section includes:

Property	Value
MD5	2d00d328619b93274f7e547f226b6d29
SHA-1	2761cf6390b6a5fcba8971b5eb8cf9480d86f1651
SHA-256	f619a62a743baa9f216b9ac90671ddd186930209e6b246a875da0bc42bd8966b
Vhash	f619a62a743baa9f216b9ac90671ddd186930209e6b246a875da0bc42bd8966b
Authentihash	45046655d155080803001100602f5247z62z570303bz
Imphash	549a8444e08745e28c33be1118f1810ec01875519258530f16b23c92ab177ec7
Rich PE header hash	aad97a1b3deac4dc6f92f2e58208d7f2
SSDeep	12288:m4K0FkrwV78qua+Yh8f4vgvELeOm+oZkQS7kokVT:im4iwVYqua+1HsgvE6bzQ57+T
TLSH	T1D5A49d42F7D2A1F5E8D1AFD15FB673AC356A000335E5D39BC02D41AD213E2693E385
File type	Win32 EXE (executable, windows, win32, pe, pexe)
Magic	PE32 executable (GUI) Intel 80386, for MS Windows
TrID	InstallShield setup (34.2%) Win32 Executable MS Visual C++ (generic) (24.8%) Microsoft Visual C++ compiled executable (generic) (13.1%) Win64 Executable (generic...)
DetectItEasy	PE32 Compiler: Microsoft Visual C/C++ (14.00.50727) [LTCG/C++]
MagikA	Linker: Microsoft Linker (8.00.50727) Tool: Visual Studio (2005)
PEBIN	PEBIM
File size	476.50 KB (487936 bytes)
PEID packer	Microsoft Visual C++ v7.1 EXE

The 'History' section shows submission details:

Event	Date
Creation Time	2025-04-27 11:46:53 UTC
First Submission	2025-04-27 21:36:17 UTC
Last Submission	2025-07-05 13:59:24 UTC
Last Analysis	2025-06-29 10:20:06 UTC

The 'Names' section lists file aliases:

Name
WebBrowserPassView.exe
Web Browser Pass View

Figure 65 Hashes and Other Details (.exe) file

Created and IP Address Details

The screenshot shows the VirusTotal analysis interface for the same file. The 'Contacted Domains (3)' section lists:

Domain	Detections	Created	Registrar
content-signature-2.cdn.mozilla.net	0 / 94	1998-01-31	MarkMonitor Inc.
res.public.onecdn.static.microsoft	0 / 94	2023-05-05	MarkMonitor Inc.
www.microsoft.com	0 / 94	1991-05-02	MarkMonitor Inc.

The 'Contacted IP addresses (18)' section lists:

IP	Detections	Autonomous System	Country
104.98.118.146	0 / 94	20940	US
104.98.118.152	0 / 94	20940	US
104.98.118.155	0 / 94	20940	US
104.98.118.163	0 / 94	20940	US
104.98.118.178	0 / 94	20940	US
184.27.218.92	1 / 94	16625	US
192.168.0.191	0 / 94	-	-
192.168.0.20	0 / 94	-	-
192.168.0.27	0 / 94	-	-
192.168.0.53	0 / 94	-	-

The 'Execution Parents (12)' section lists:

Scanned	Detections	Type	Name

Figure 66 Created and IPs Details

Malware Detection Details

Figure 67 Malware Detection Details

6. Chain of Custody

Question No	Date & Time	Action Taken	Tool Used	Device	Verified By
1	04-Jul-2025 & 11:55 PM	Create Malicious .doc file using MS Word and SYSTool viewer use Email Header Analyse	MS Word , SYSTool EML viewer	Window	Hamza Ali
2	05-Jul-2025 & 01:30 AM	Create Memory dump using FTK Imager and Analyse through Volatility-3	FTK Imager , Volatility-3	Window	Hamza Ali
3	05-Jul-2025 & 03:15 AM	Copy hives through FTK Imager and Convert to readable text format using Reg Ripper	FTK Imager, Reg Ripper	Window	Hamza Ali
4	05-Jul-2025 & 04:25 AM	Create an image local DiskG using FTK Imager and Data Recover using Autopsy and Images Metadata collecting through Exzif	FTK Imager, Autopsy, Exzif	Window	Hamza Ali
5	05-Jul-2025 & 08:30 PM	Google Chrome History and web data and security	System	Window	Hamza Ali

6	05-Jul-2025 & 06:00 AM	Check window timestamps logon and logoff and other timestamps	Window Event Viewer	Window	Hamza Ali
7	05-Jul-2025 & 11:24 PM	Check suspicious IPs	Wireshark	Linux	Hamza Ali
8	05-Jul-2025 & 9:00 PM	Analyse malicious (.exe) file and collecting details	Virustotal.com	Linux	Hamza Ali

7. Conclusion

The forensic investigation successfully identified the initial compromise vector as a phishing attack leveraging a malicious document attachment. Memory analysis confirmed the presence of file less malware executing solely in memory, evading traditional file-based detection. Persistence was achieved through registry modifications and user activity that facilitated malware survival across reboots. Deleted and hidden files staged for exfiltration were recovered, indicating data theft attempts. Browser artifacts revealed evidence of credential theft and session manipulation. Correlation of event logs enabled the construction of a precise attack timeline, while network traffic analysis uncovered suspicious encrypted communications to external IPs, confirming data exfiltration. Behavioural and static malware analysis highlighted significant system changes and malicious activity consistent with the attack.

8. Recommendation

1. Enhance Email Security:

Implement advanced email filtering and phishing detection mechanisms, including sandboxing of attachments and user awareness training to reduce phishing risks.

2. Deploy Endpoint Detection and Response (EDR):

Use EDR solutions capable of detecting fileless malware and anomalous memory activity to improve early detection and response.

3. Harden Persistence Controls:

Regularly audit and restrict registry keys and scheduled tasks to prevent unauthorized persistence mechanisms.

4. Implement Data Loss Prevention (DLP):

Monitor and control sensitive data movement to detect and block unauthorized exfiltration attempts.

5. Strengthen Credential Security:

Enforce multi-factor authentication and regularly review browser and system credential storage practices.

6. Maintain Comprehensive Logging:

Ensure detailed logging and centralized log management to facilitate timely forensic investigations and incident response.

7. Conduct Regular Security Assessments:

Perform periodic penetration testing and forensic readiness exercises to identify and mitigate vulnerabilities proactively.