Forensic Investigation Report

Investigation Title:

Forensic Analysis and Malware Investigation Report

Prepared For:

Cyborts

Prepared By:

Hamza Ali

Date:

05-July-2025

Confidentiality Notice:

Table of Contents

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

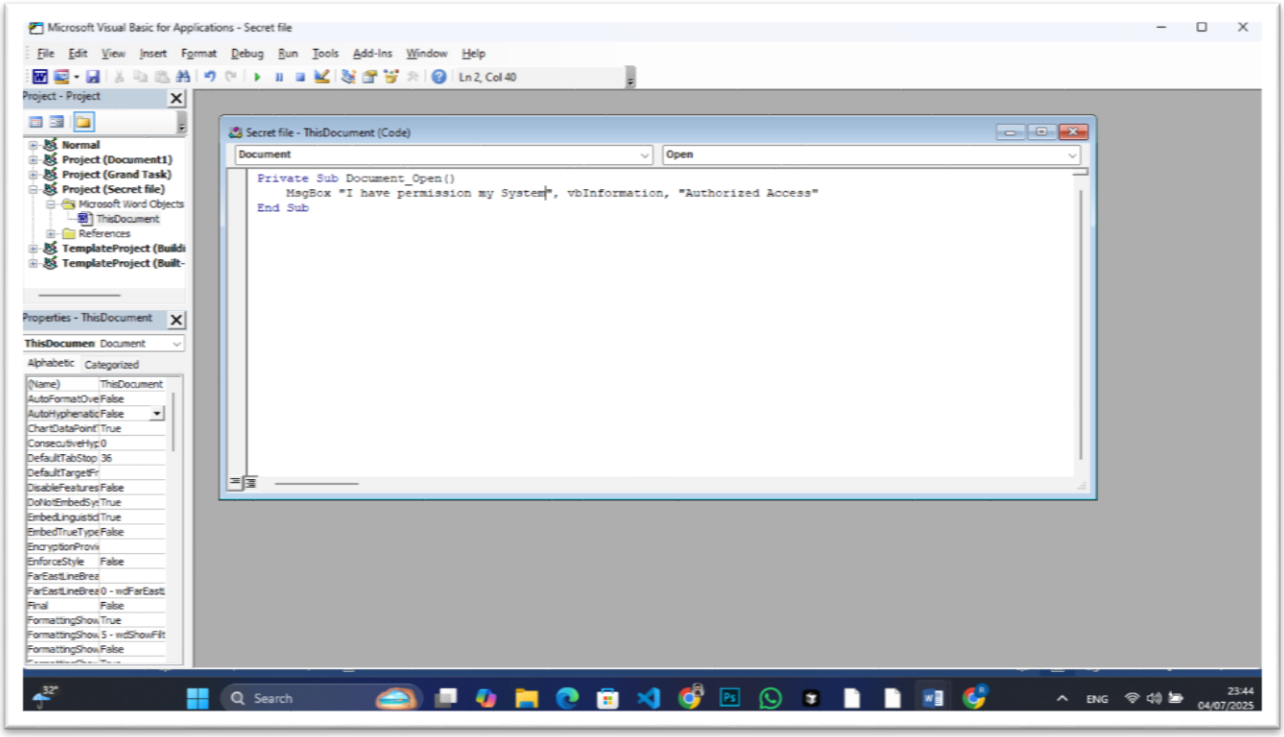

Figure 1 Creating a malicious (.doc) file using MS Word

Sending Mail

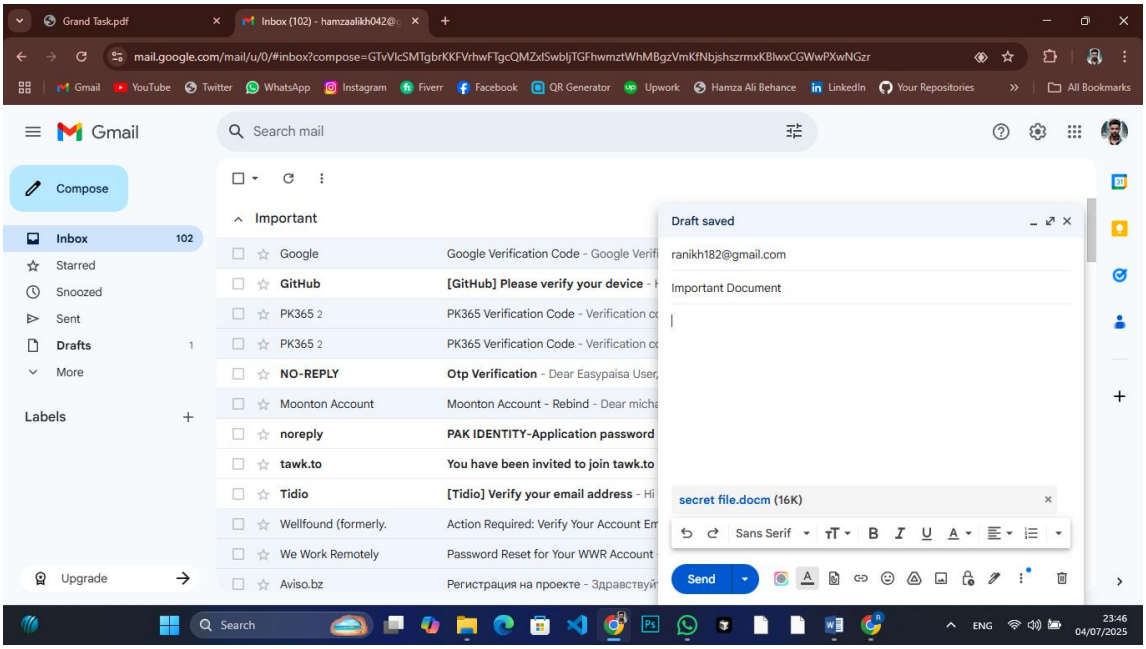

Figure 2 Sending Malicious (.doc) file through Email

Receiving Mail in Spam

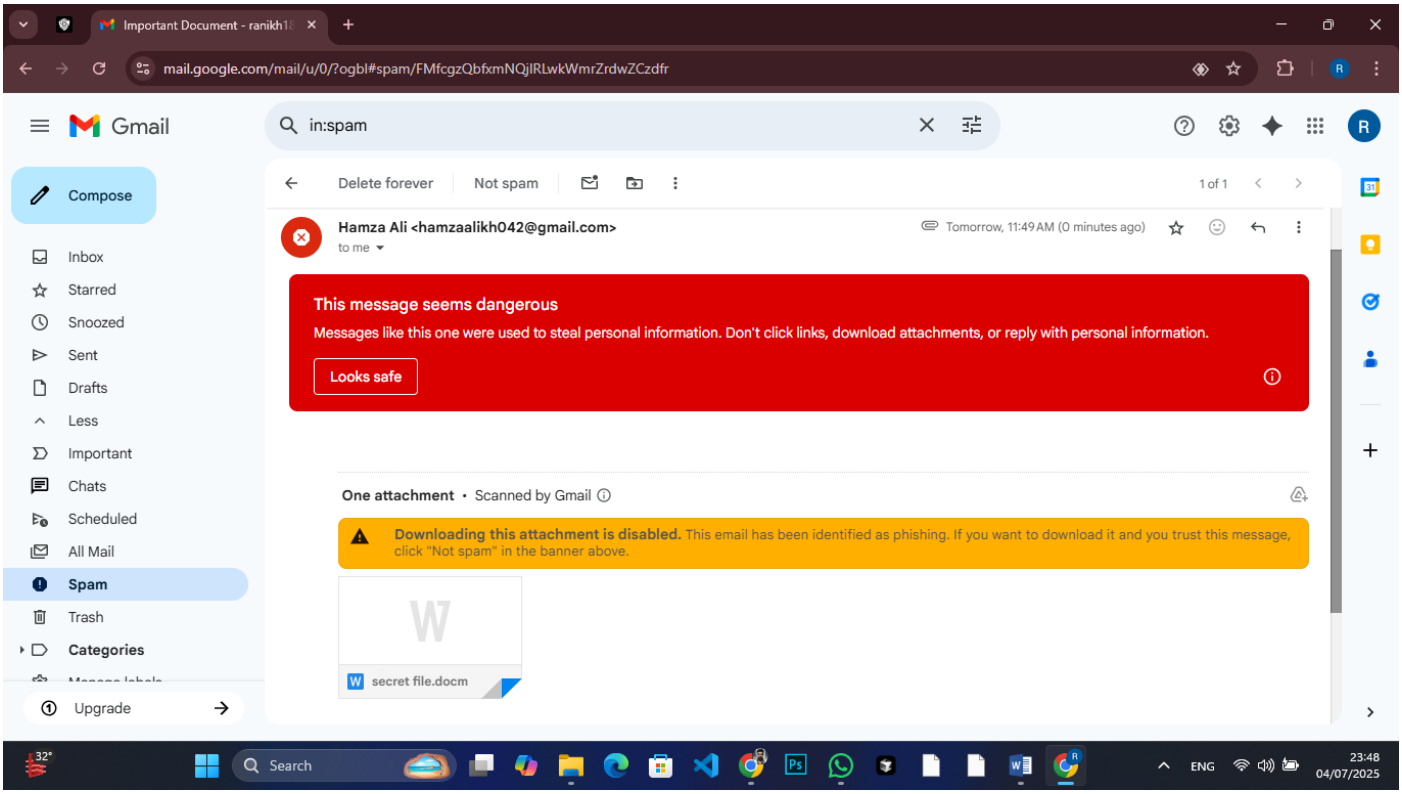

Figure 3 Receive malicious (.doc) file in spam

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

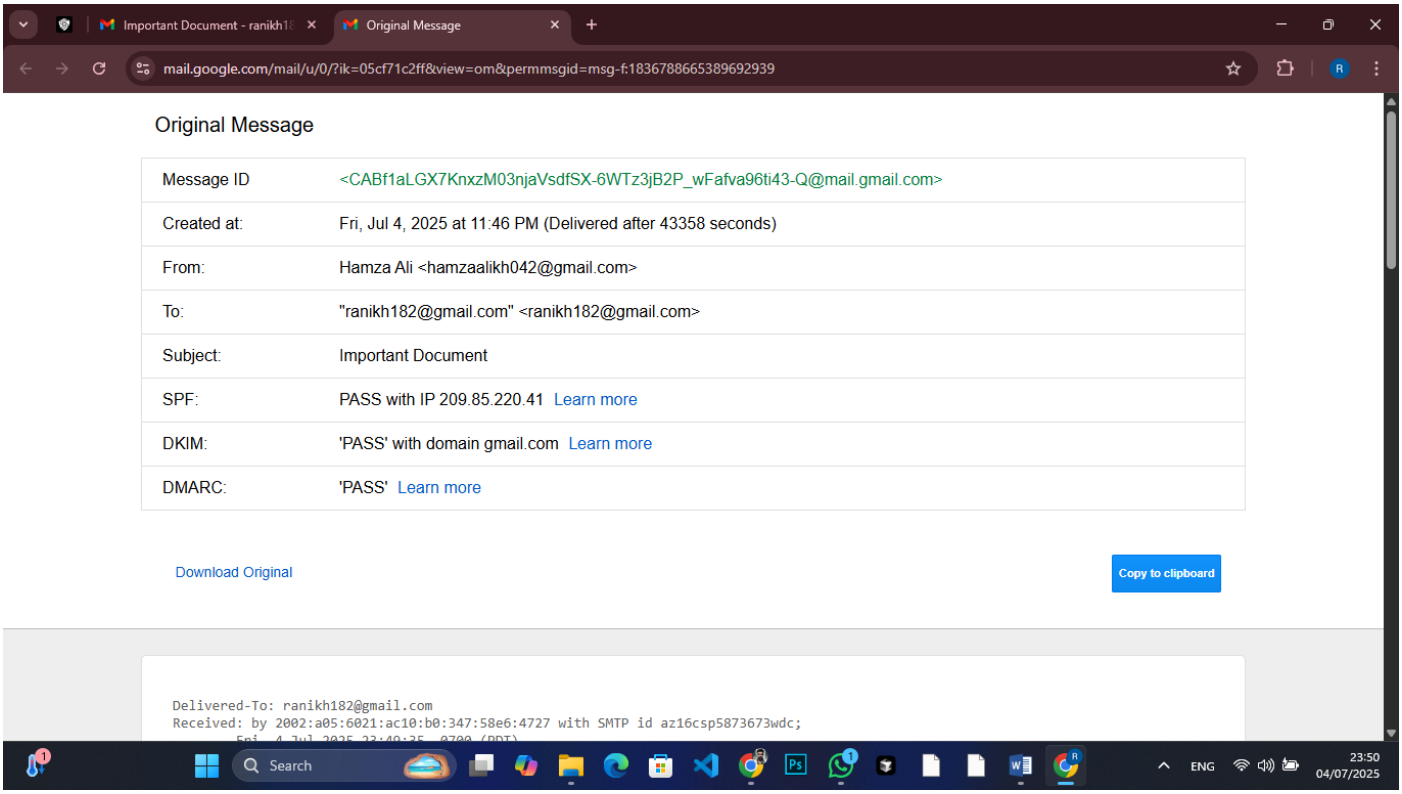

Figure 4 Sender Detail and download headers

SYSTool EML Viewer Analyze the Headers

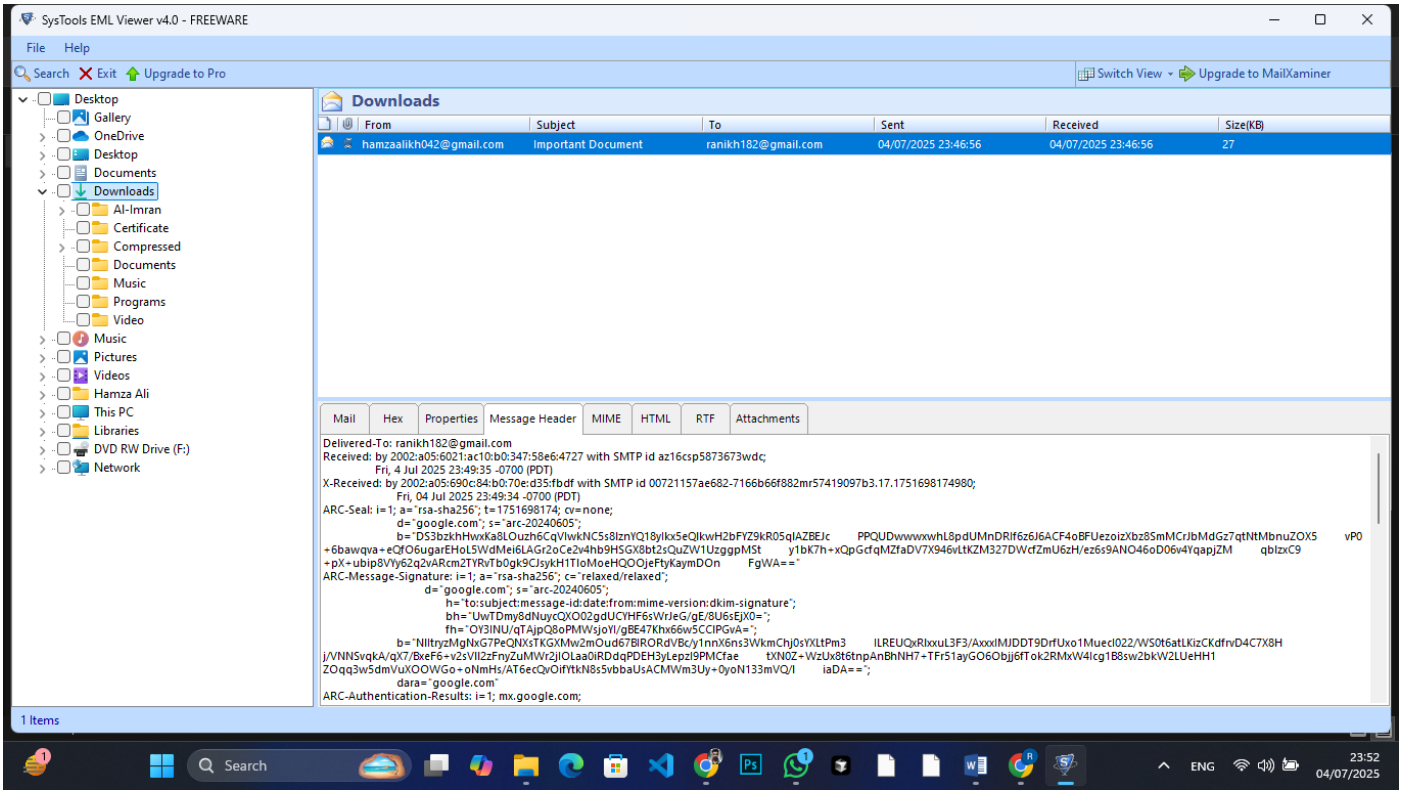

Figure 5 Email Header Analyze

Opening Malicious (.doc) file using word

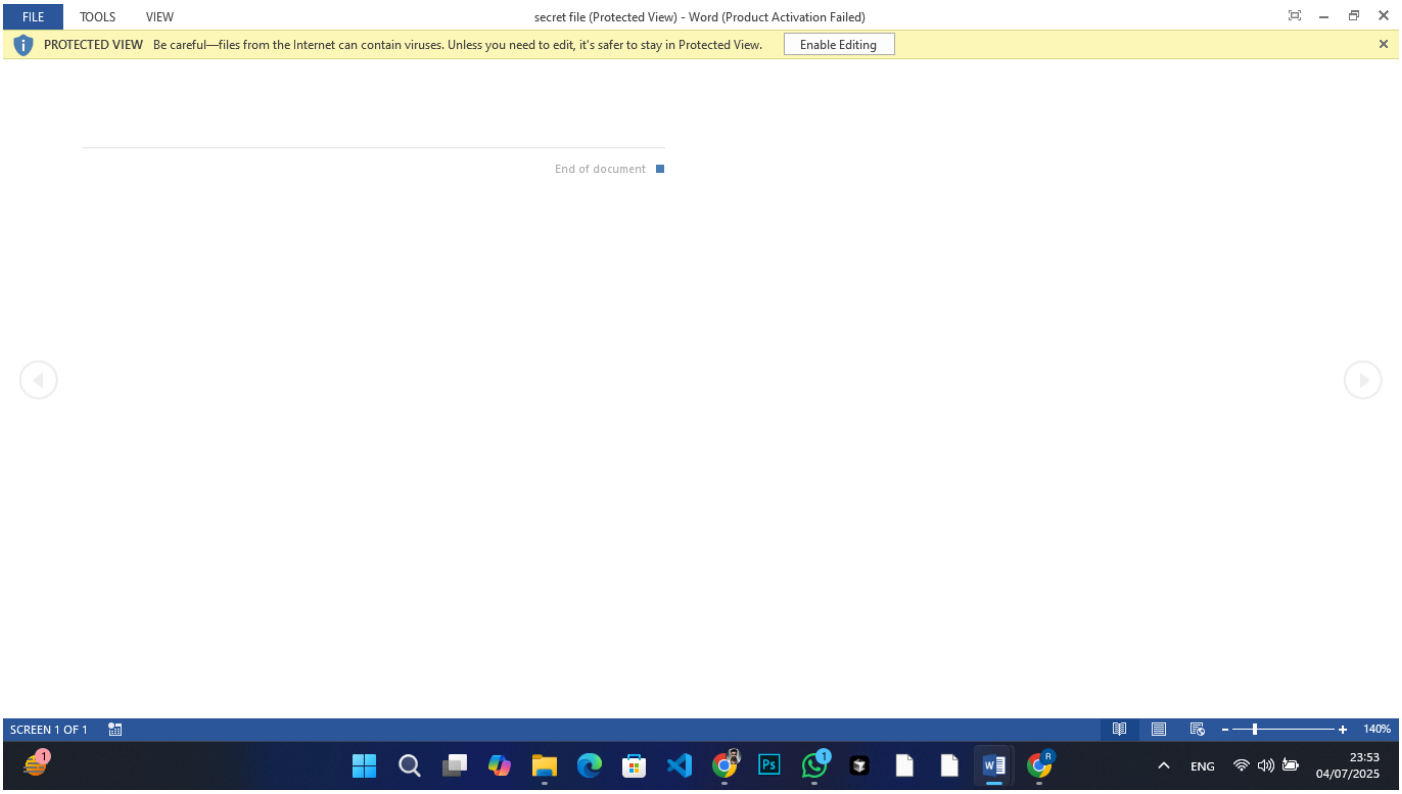

Figure 6 opening malicious (.doc) file

Show the message Malicious (.doc) file

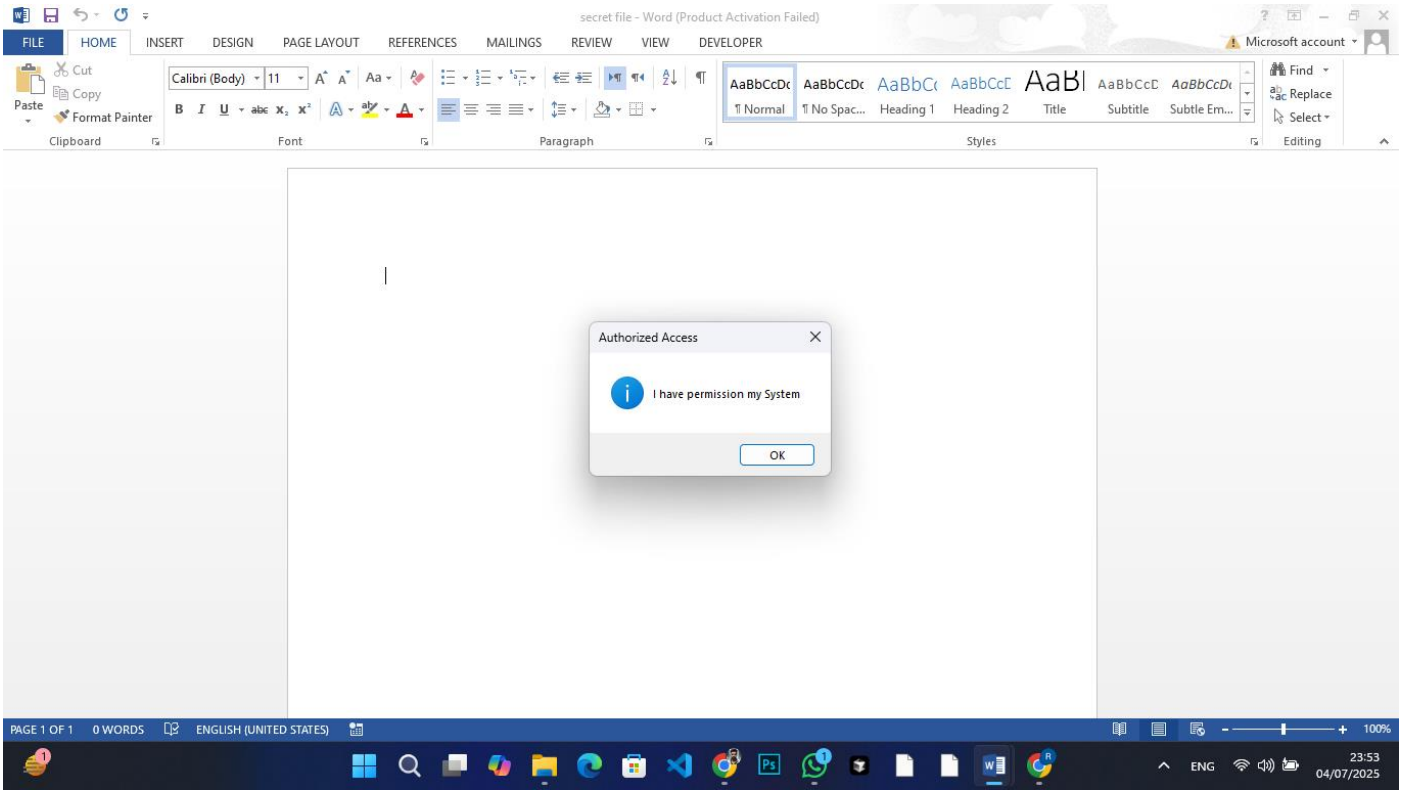

Figure 7 Malicious (.doc) File message

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

Create a Memory dump file using FTK imager

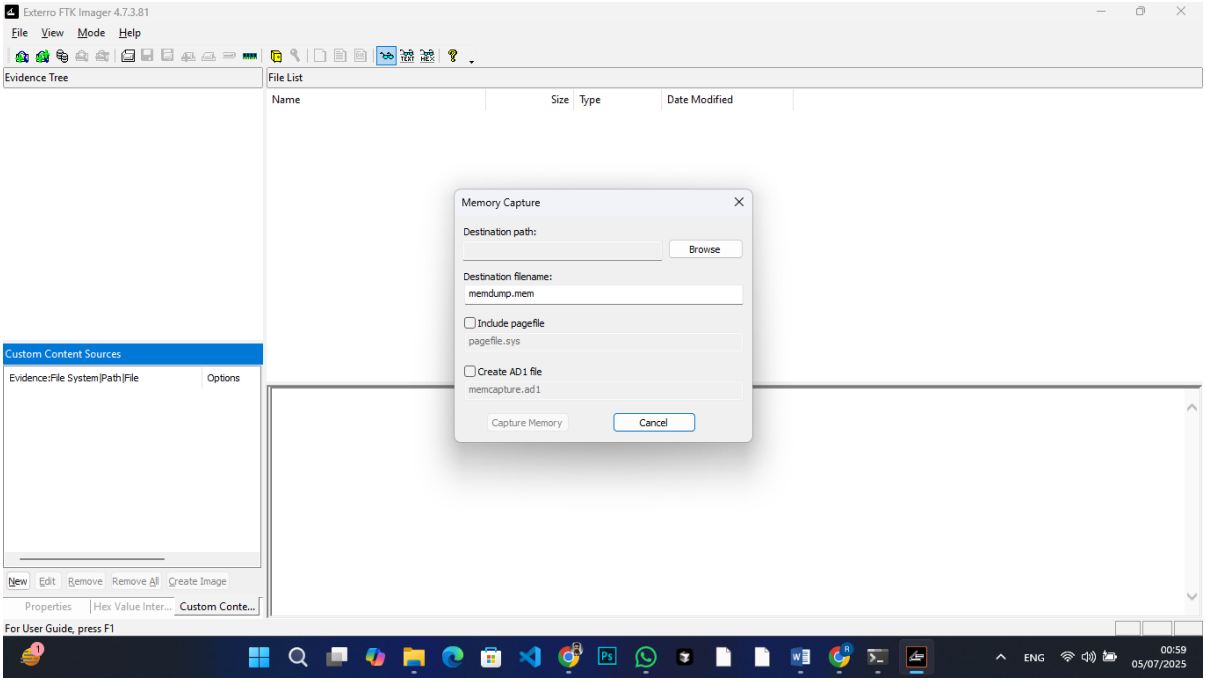

Figure 8 FTK Imager

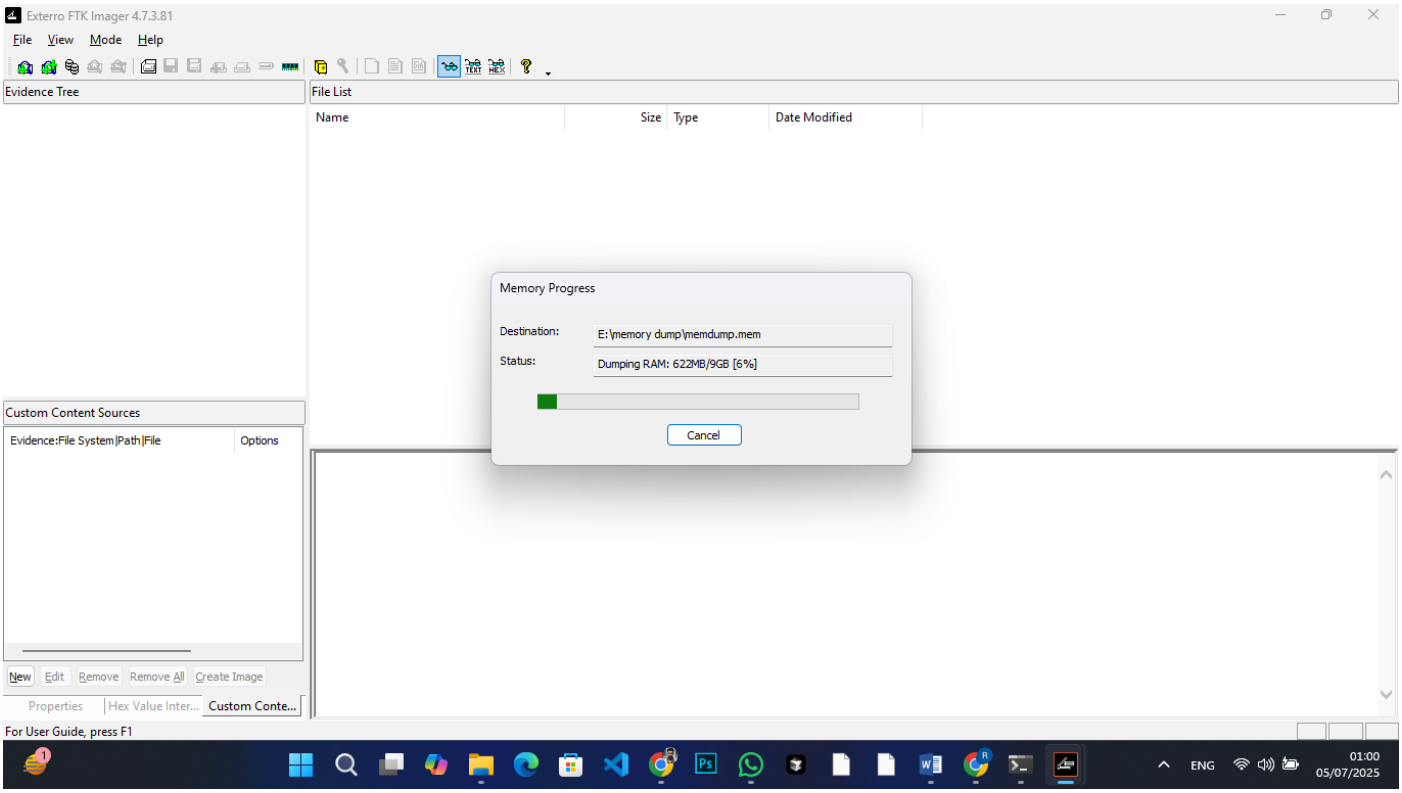

Figure 9 FTK imager creating a Memory dump file

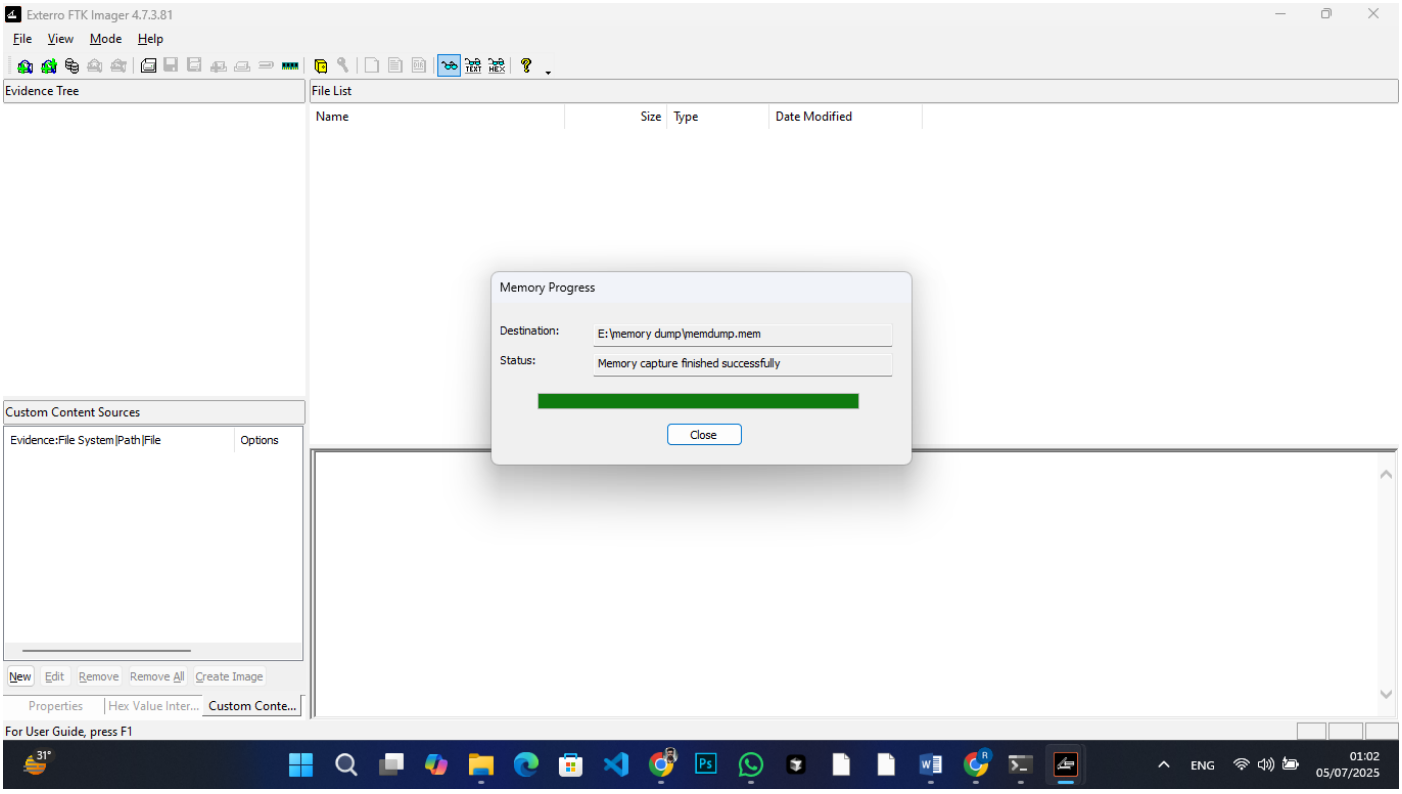

Figure 10 Completing Memory Dump file

Volatility 3

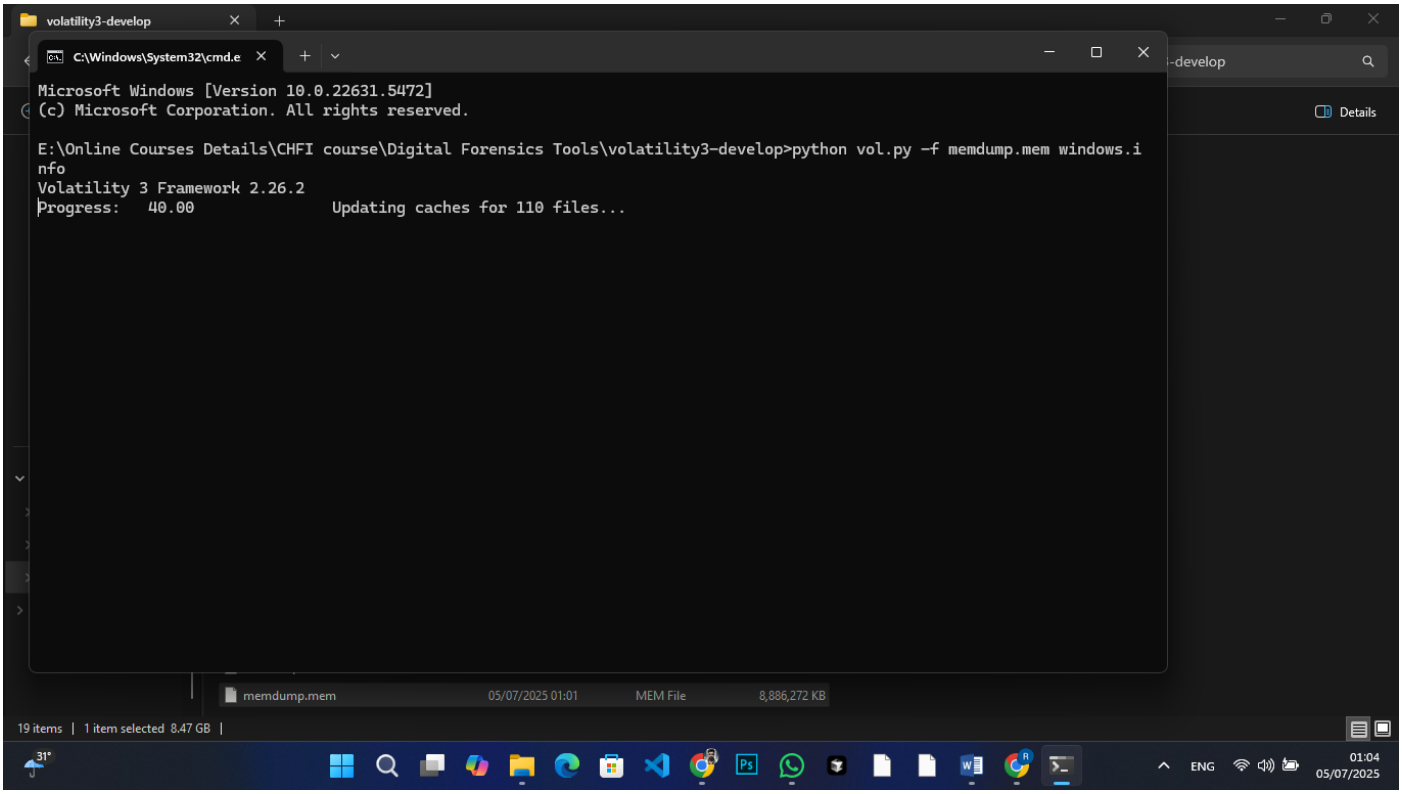

Figure 11 volatility 3

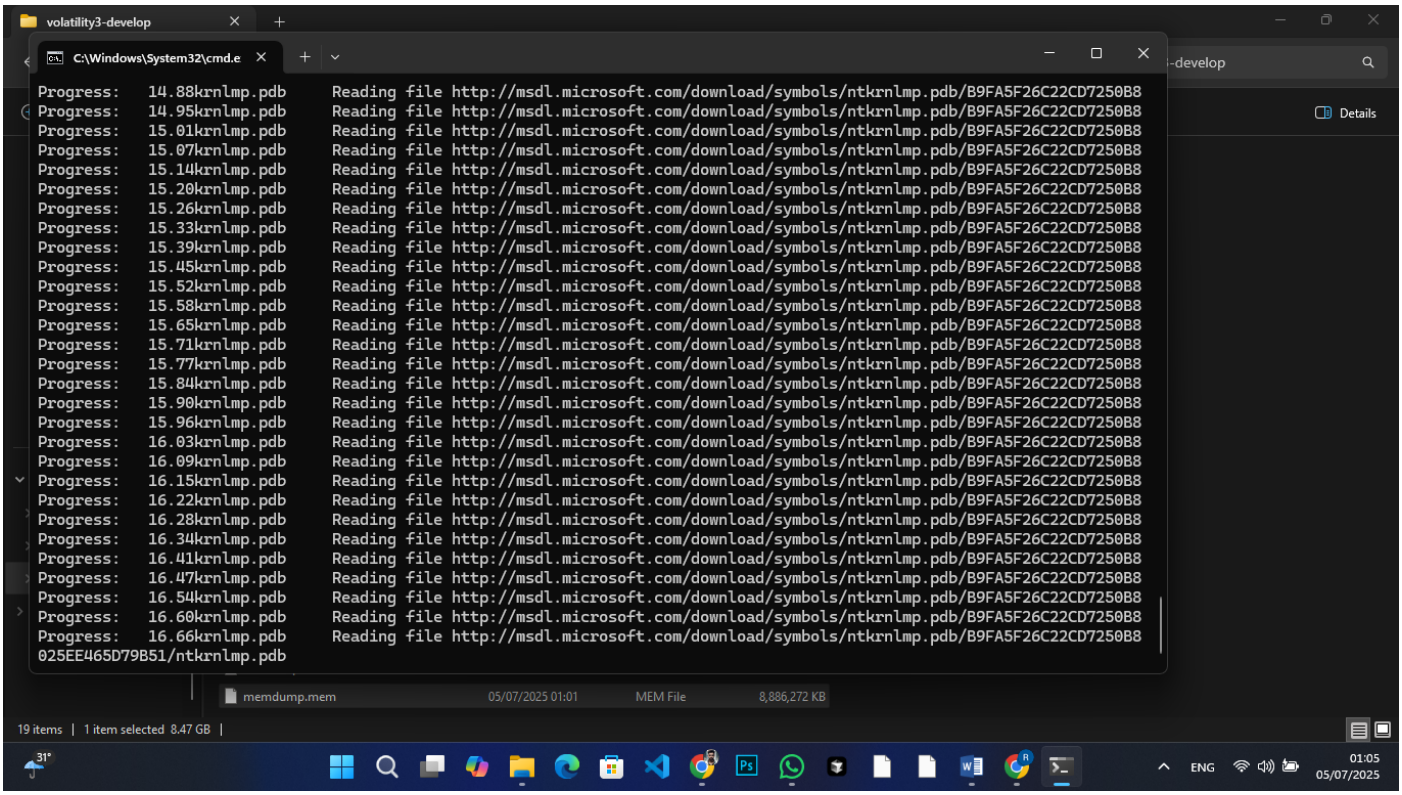

Figure 12 Volatility 3 collecting a Window info

Volatility 3 Window Info

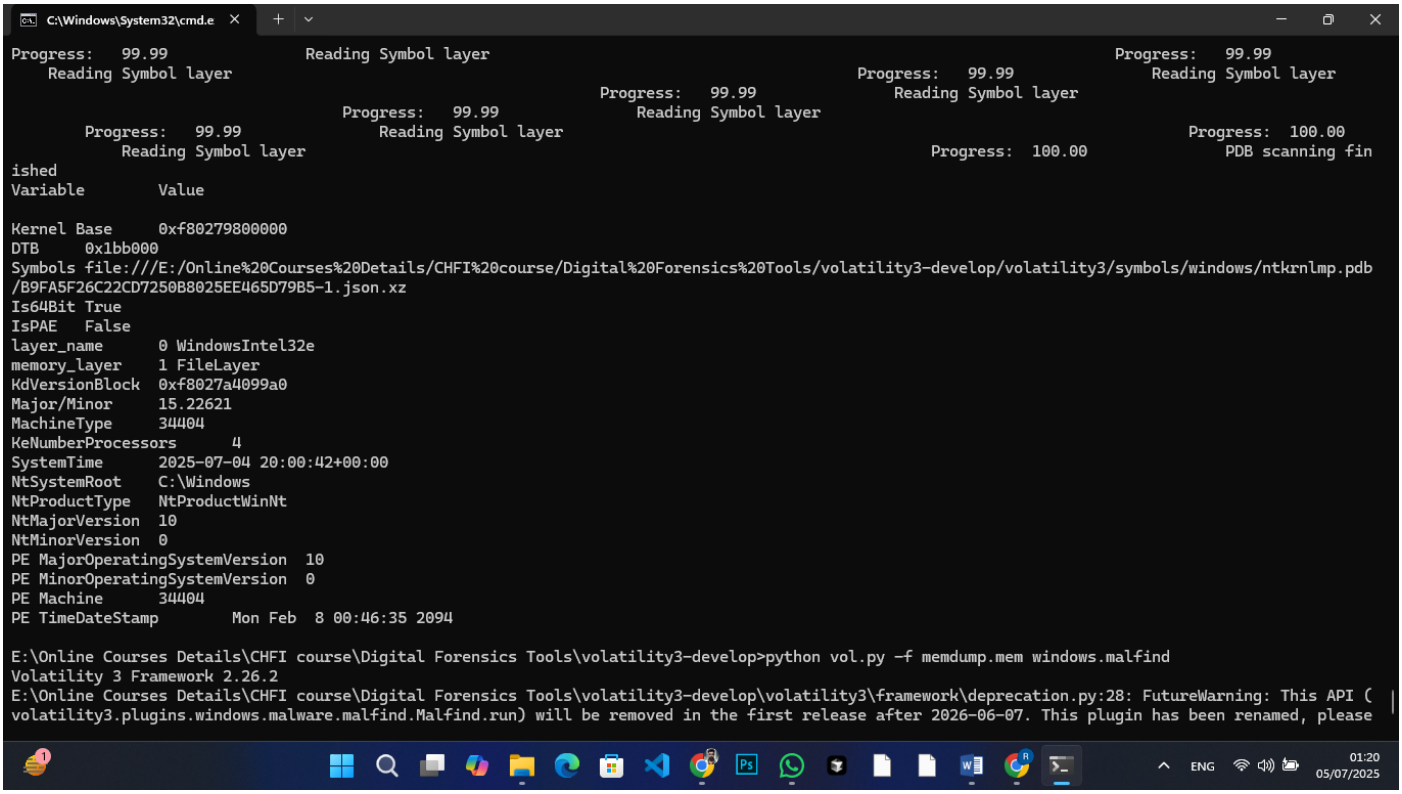

Figure 13 Volatility 3 Window info

Malfind Plugin Collecting using Volatility 3

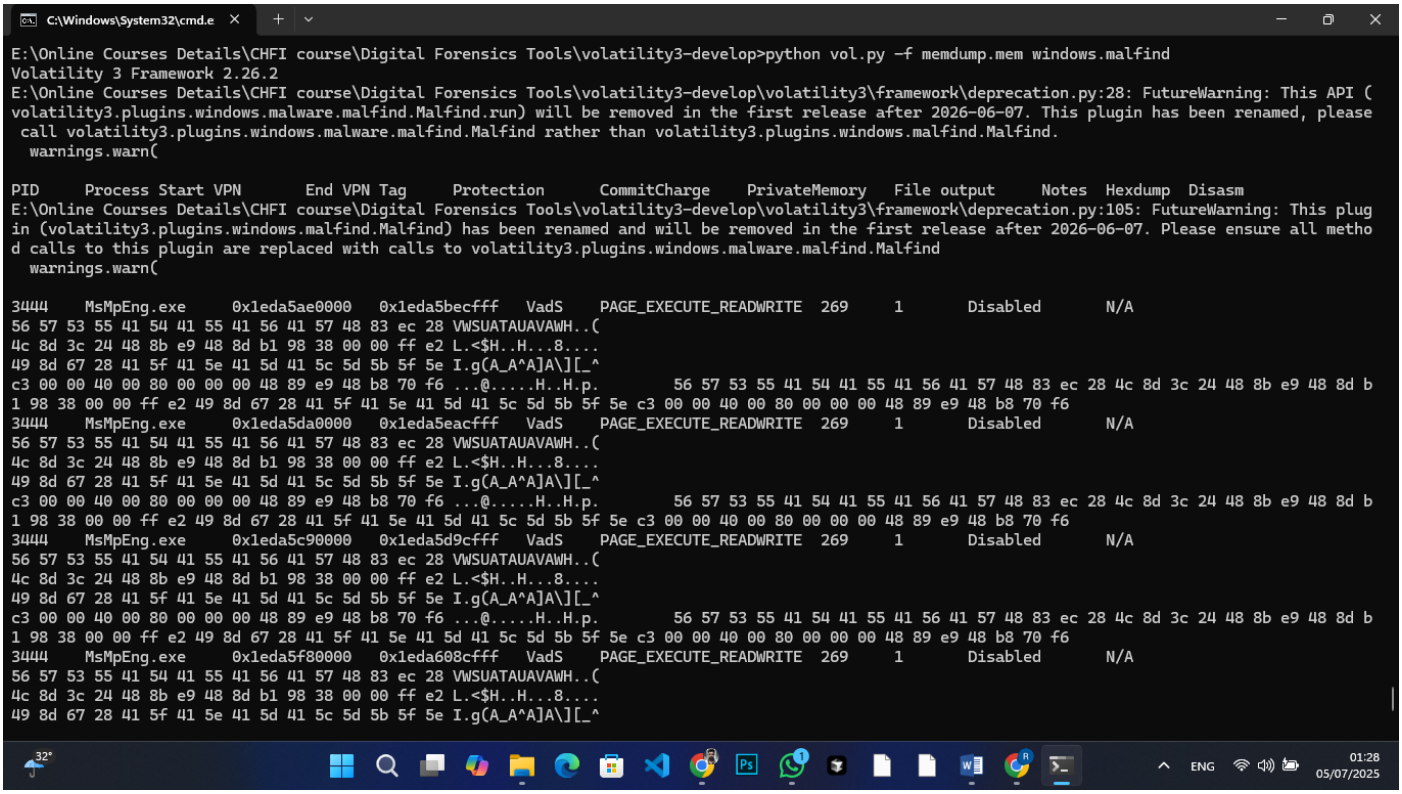

Figure 14 Volatility 3 Malfind collecting

Malfind plugin Find some Suspicious

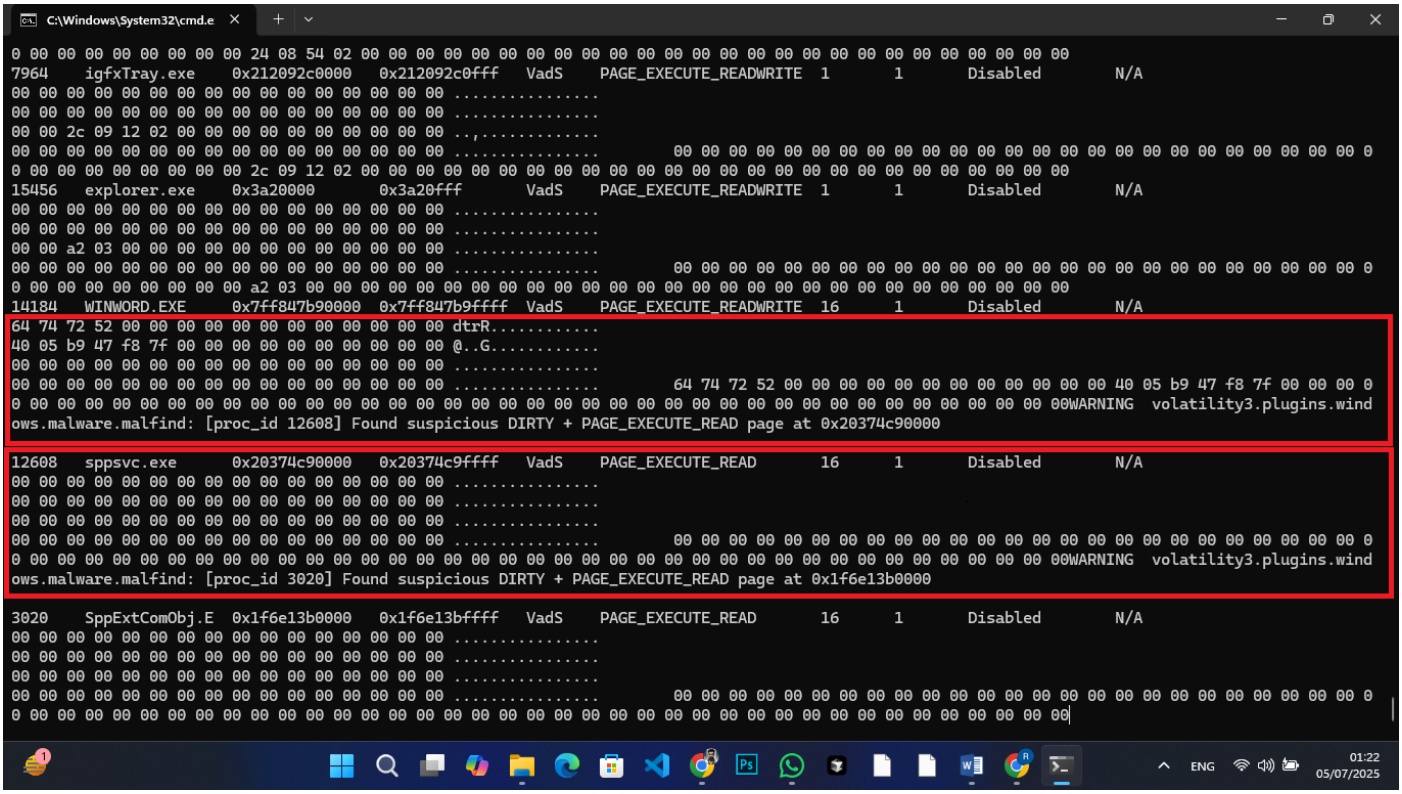

Figure 15 find Some Suspicious using volatility 3

Idrmodules Plugin in Volatility 3

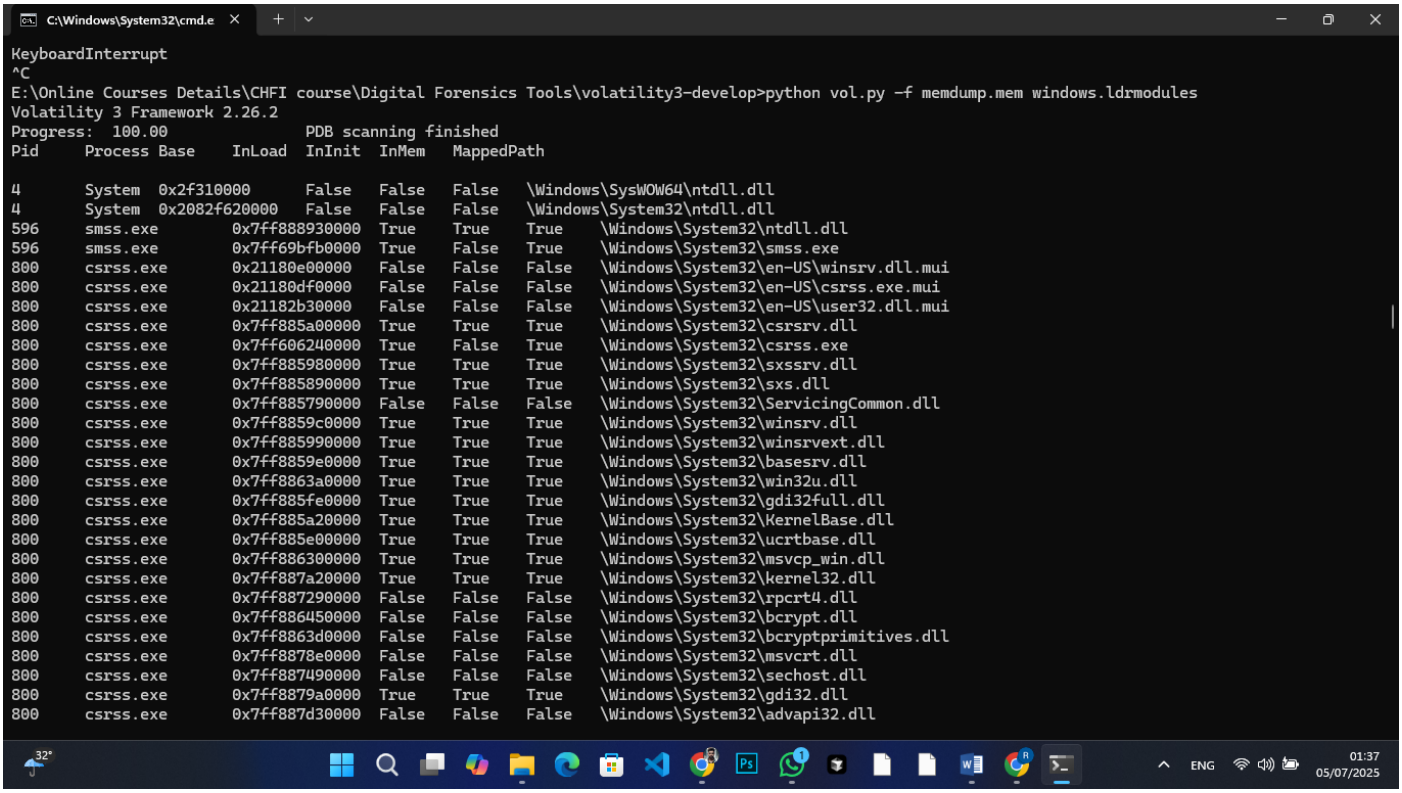

Figure 16 Idrmodules plugin in Volatility 3

5.3 What user activity helped the malware persist?

Evidence Upload in FTK Imager

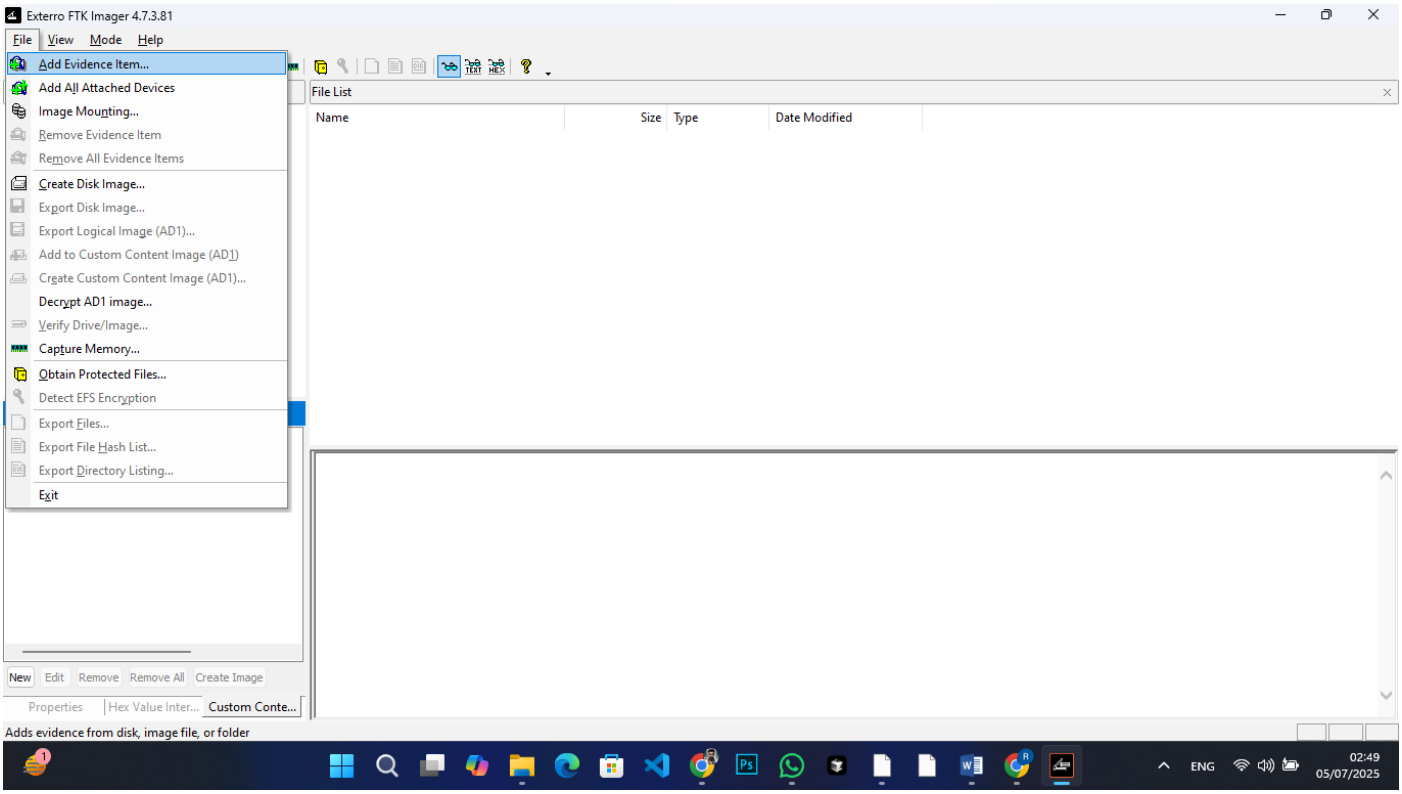

Figure 17 Evidence Upload in FTK Imager

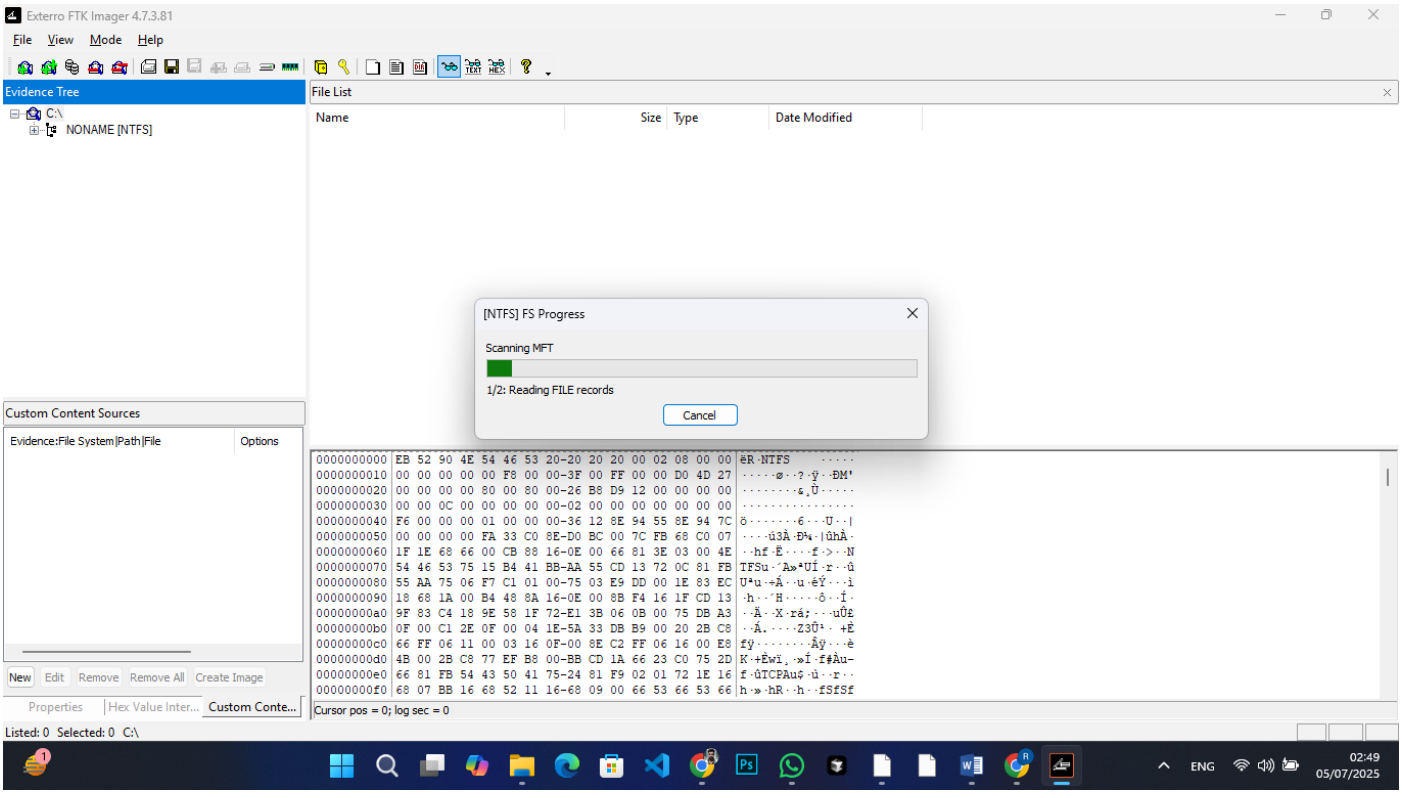

Figure 18 Evidence Loaded in FTK Imager

Export System Hive in Desktop Hive Folder

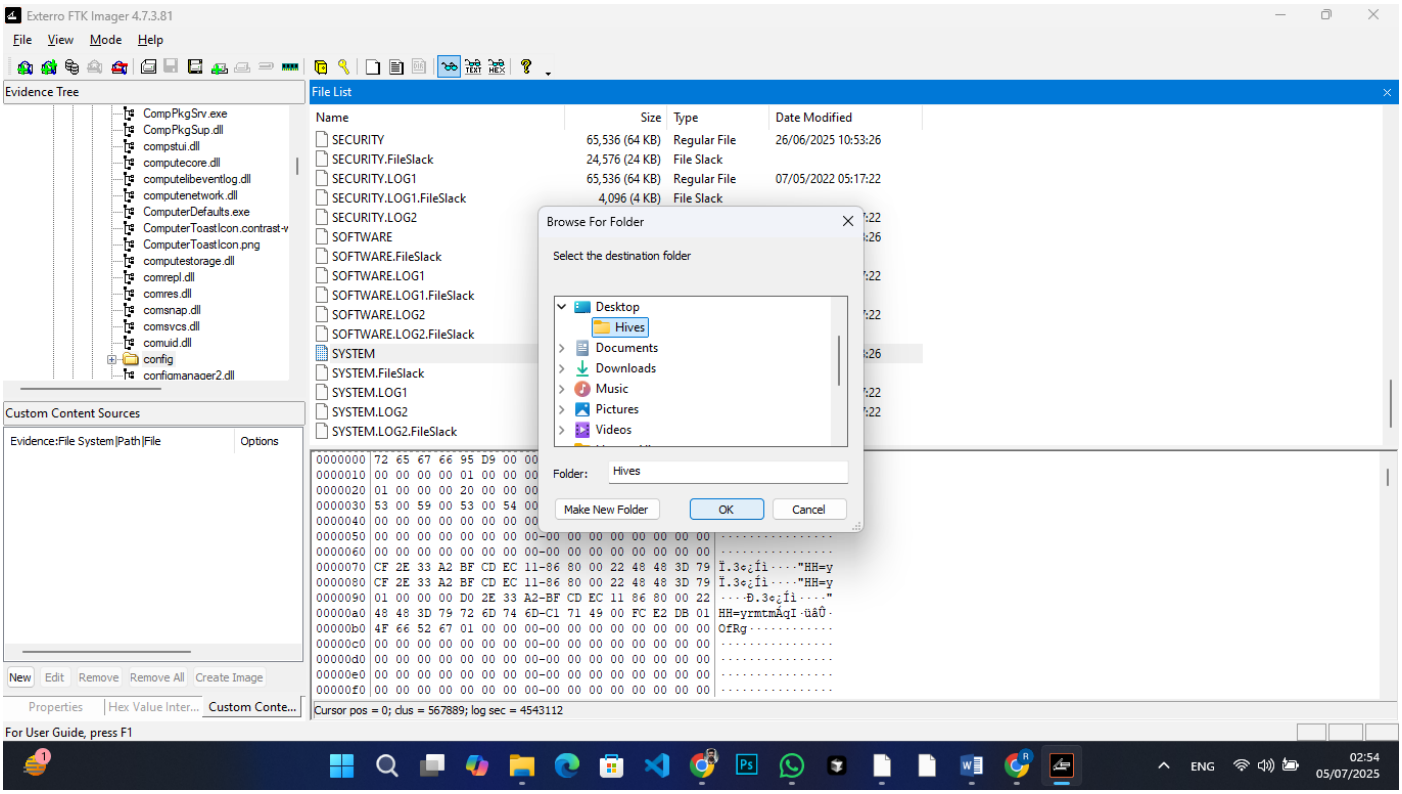

Figure 19 System Registry Export

Export Software Hive in Desktop Hive Folder

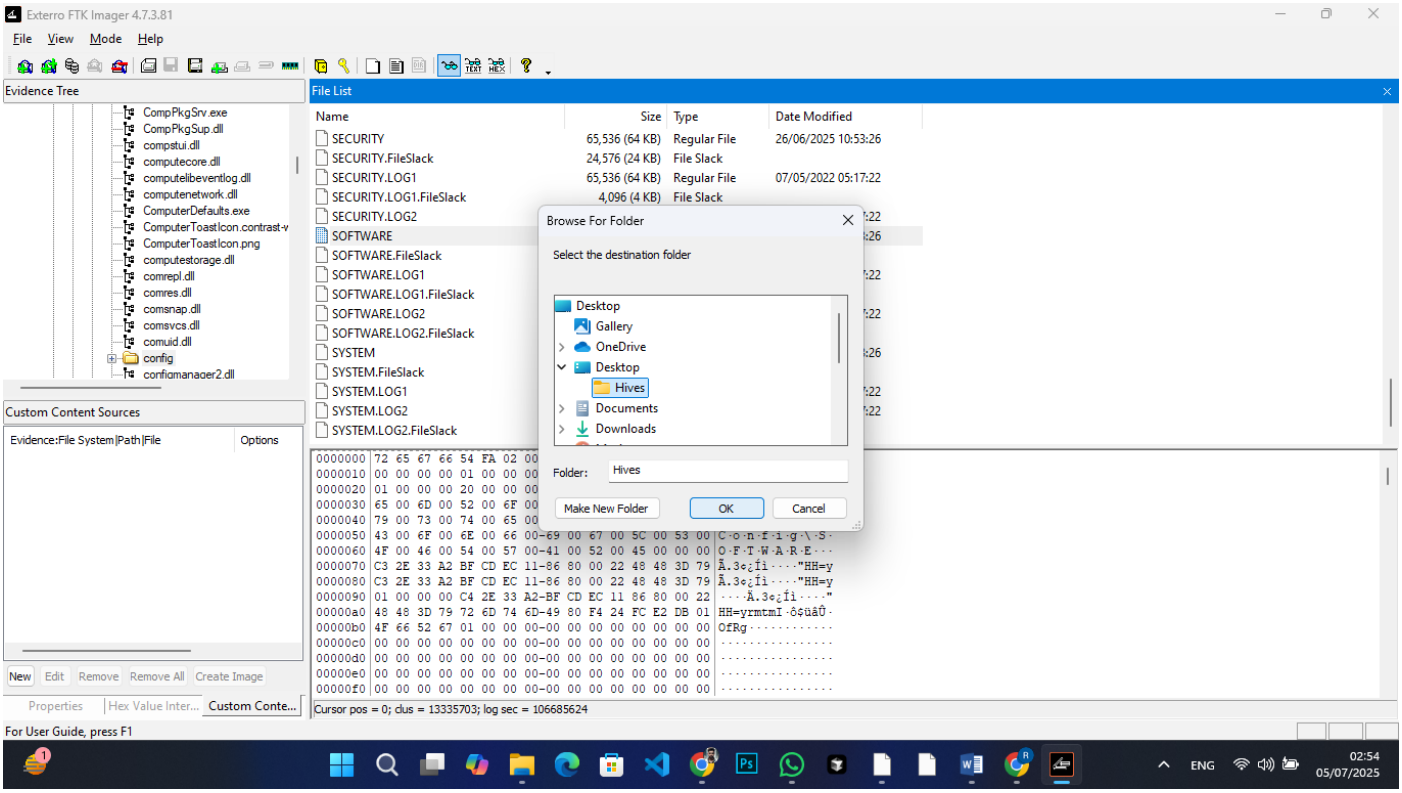

Figure 20 Software Registry Export

Export NTUSER.DAT hive in Desktop Hive Folder

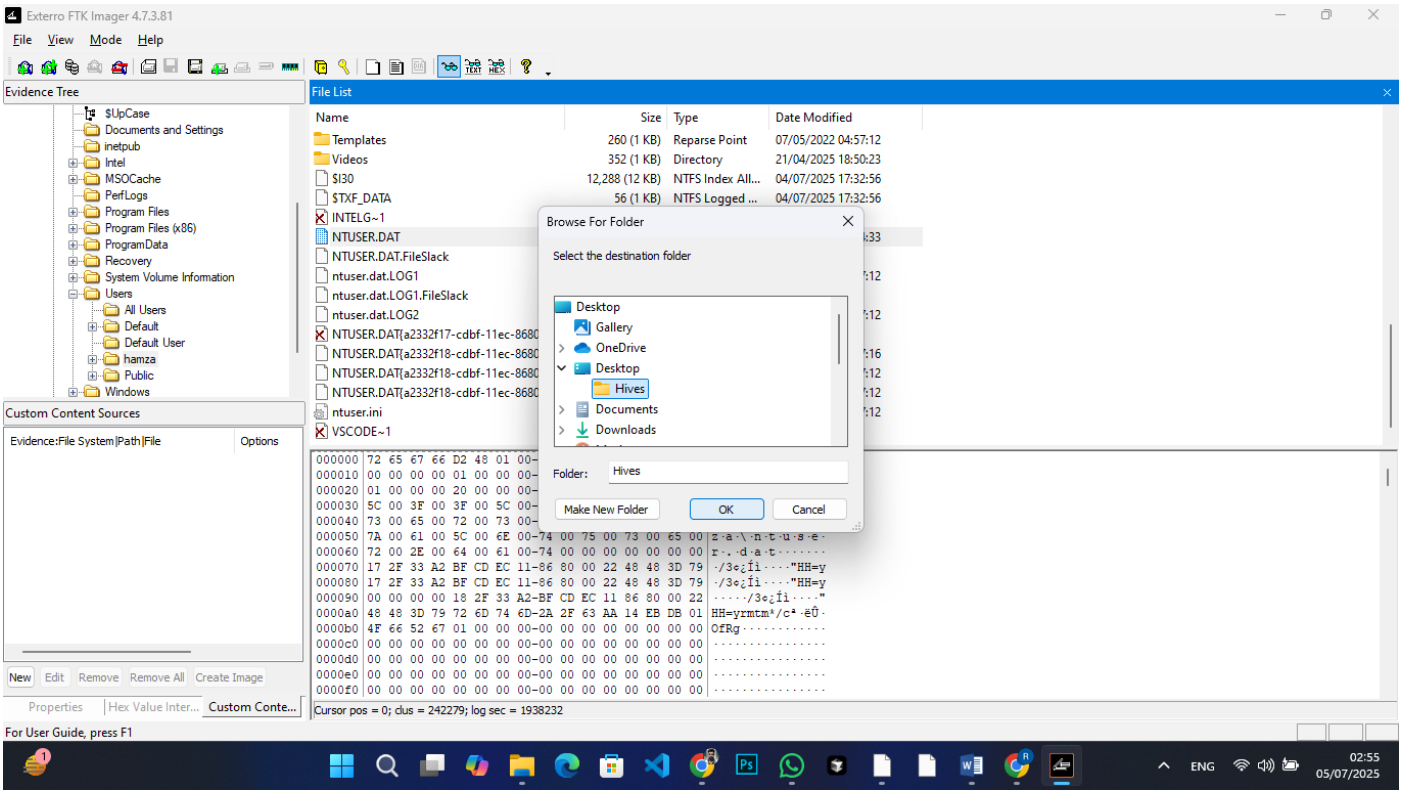

Figure 21 NTUSER.DAT Registry Export

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

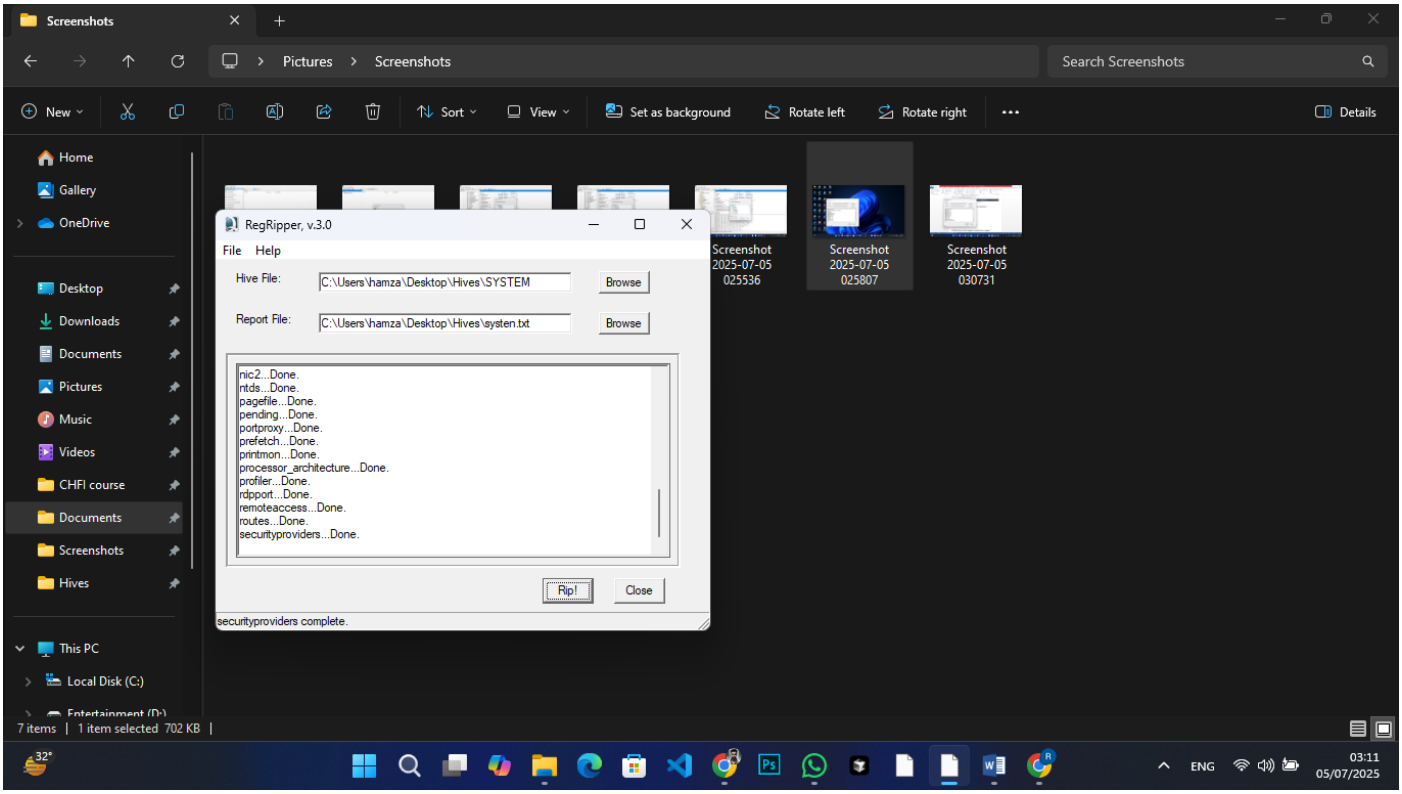

Figure 22 System Registry hive convert to Text file

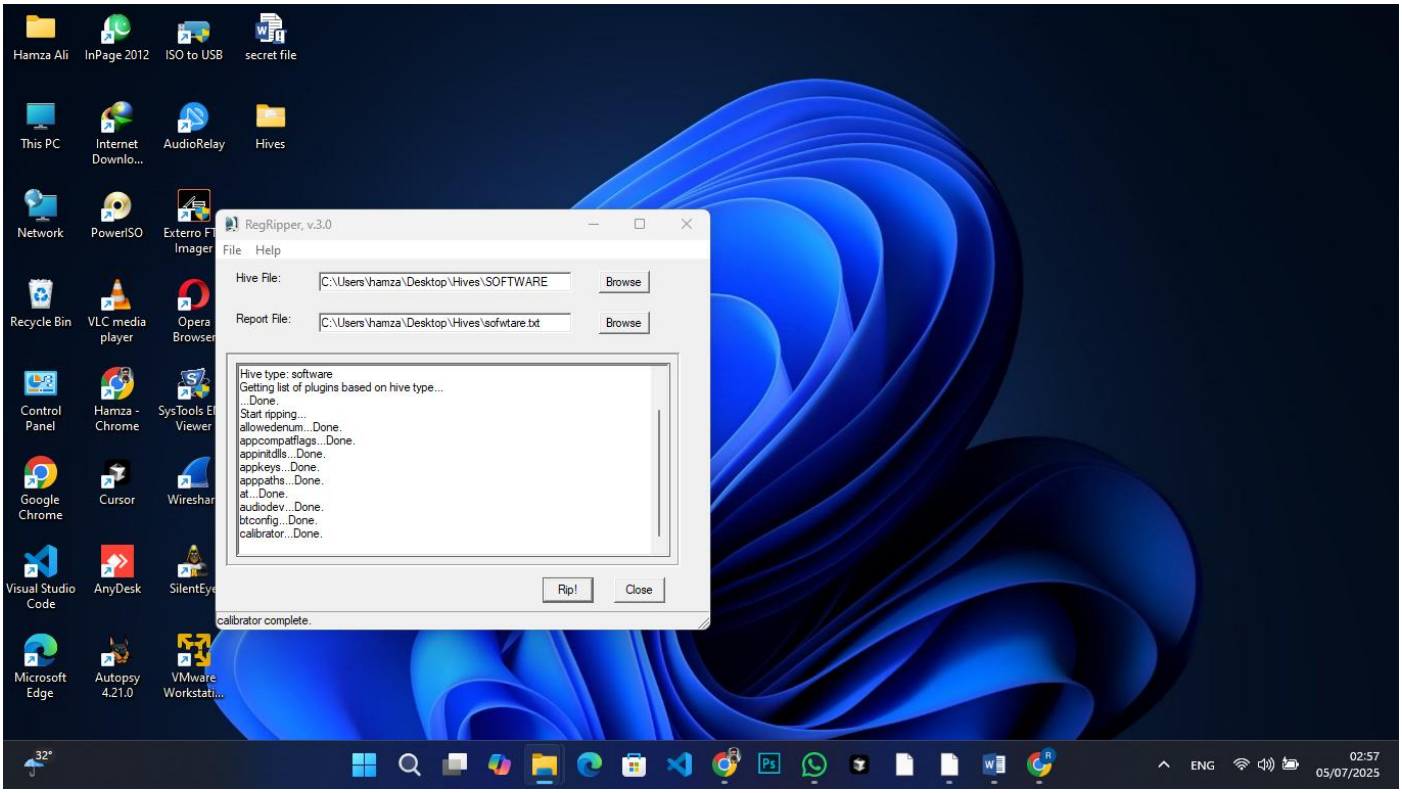

Figure 23 Software Registry Hive Convert to Text File

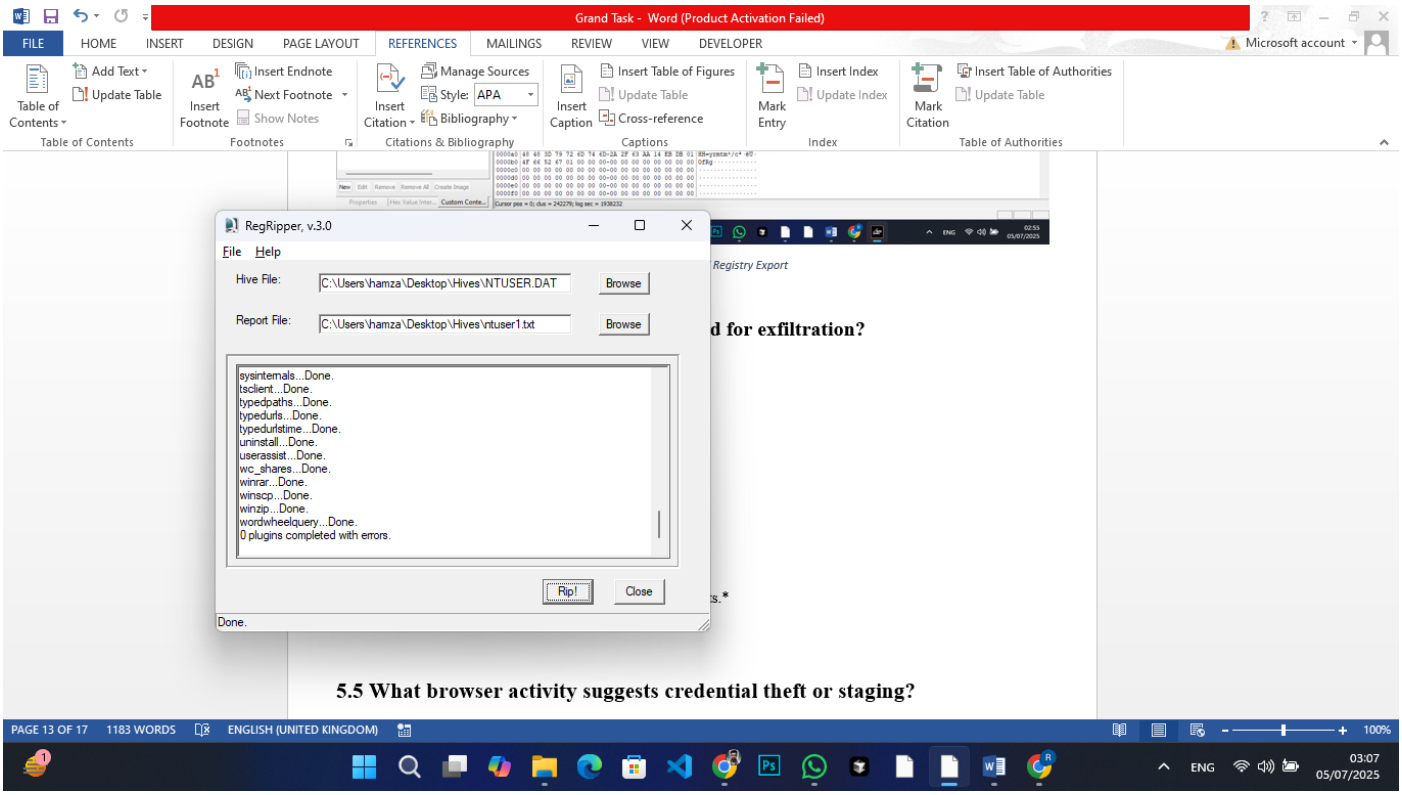

Figure 24 NTUSER.DAT hive file convert to text file

System Hive (.txt) file

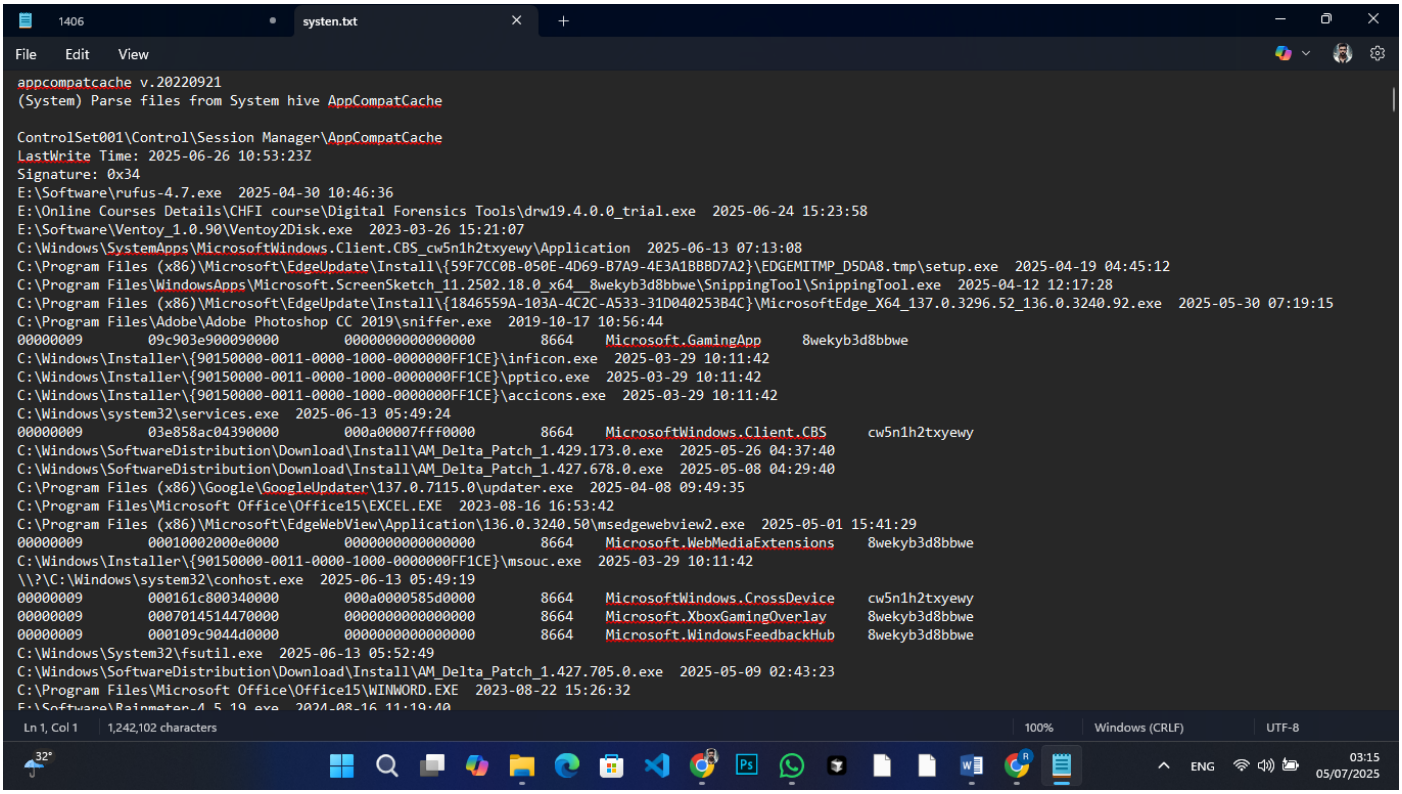

Figure 25 System Hive (.txt) file

Software (.txt) file

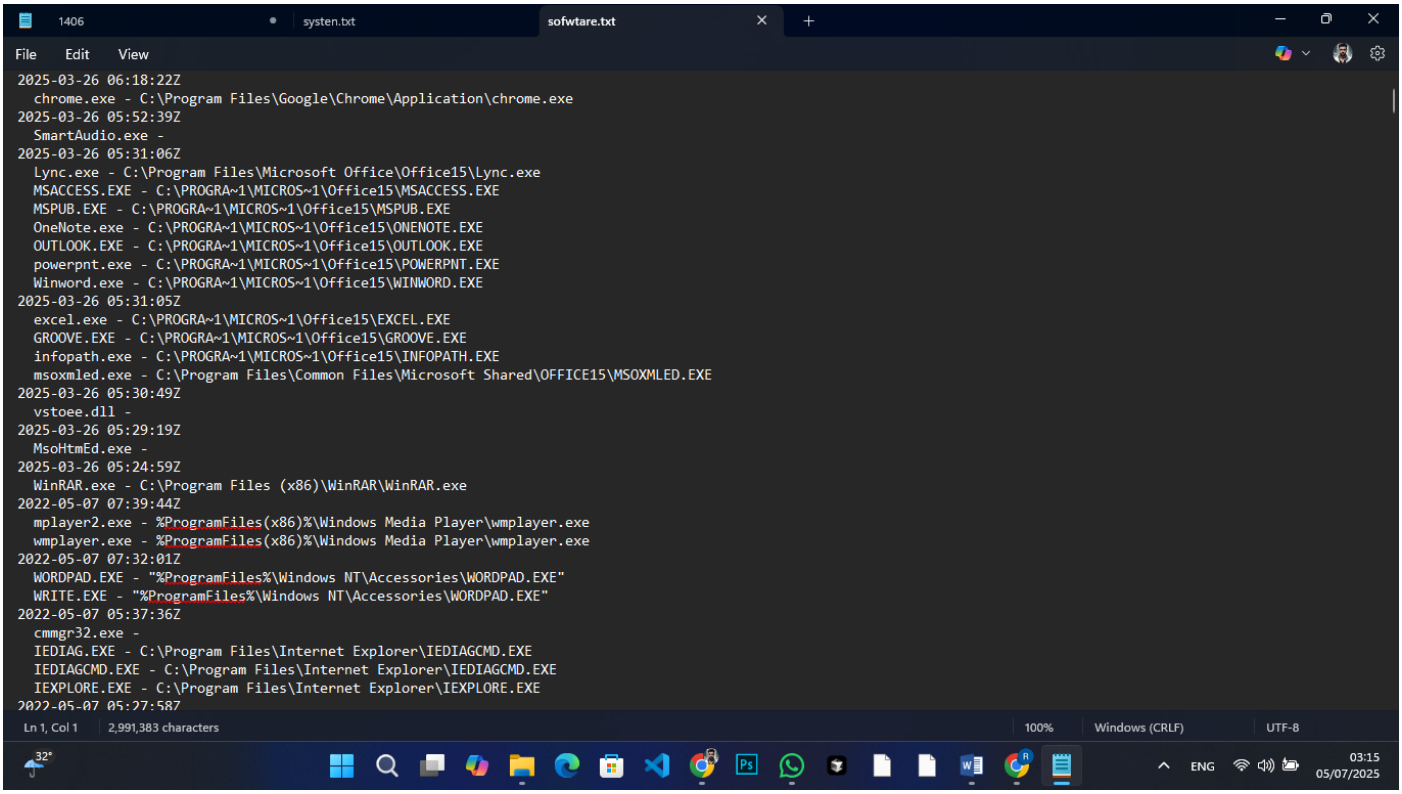

Figure 26 Software (.txt) file

NTUSER.DAT (.txt) file

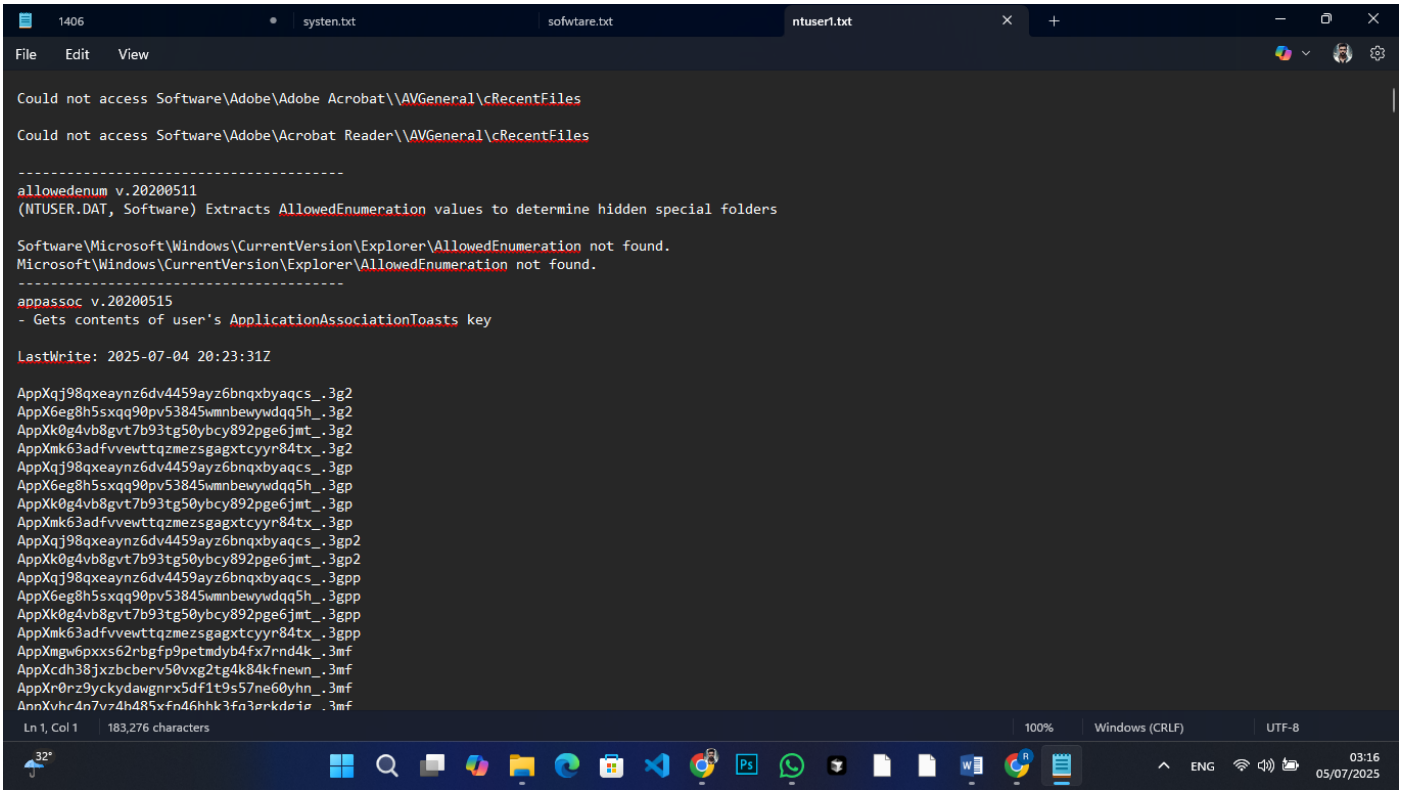

Figure 27 NTUSER.DAT (.txt) file

5.4 What deleted or hidden files were staged for exfiltration?

Shrink Local Disk D: for create a New Partition

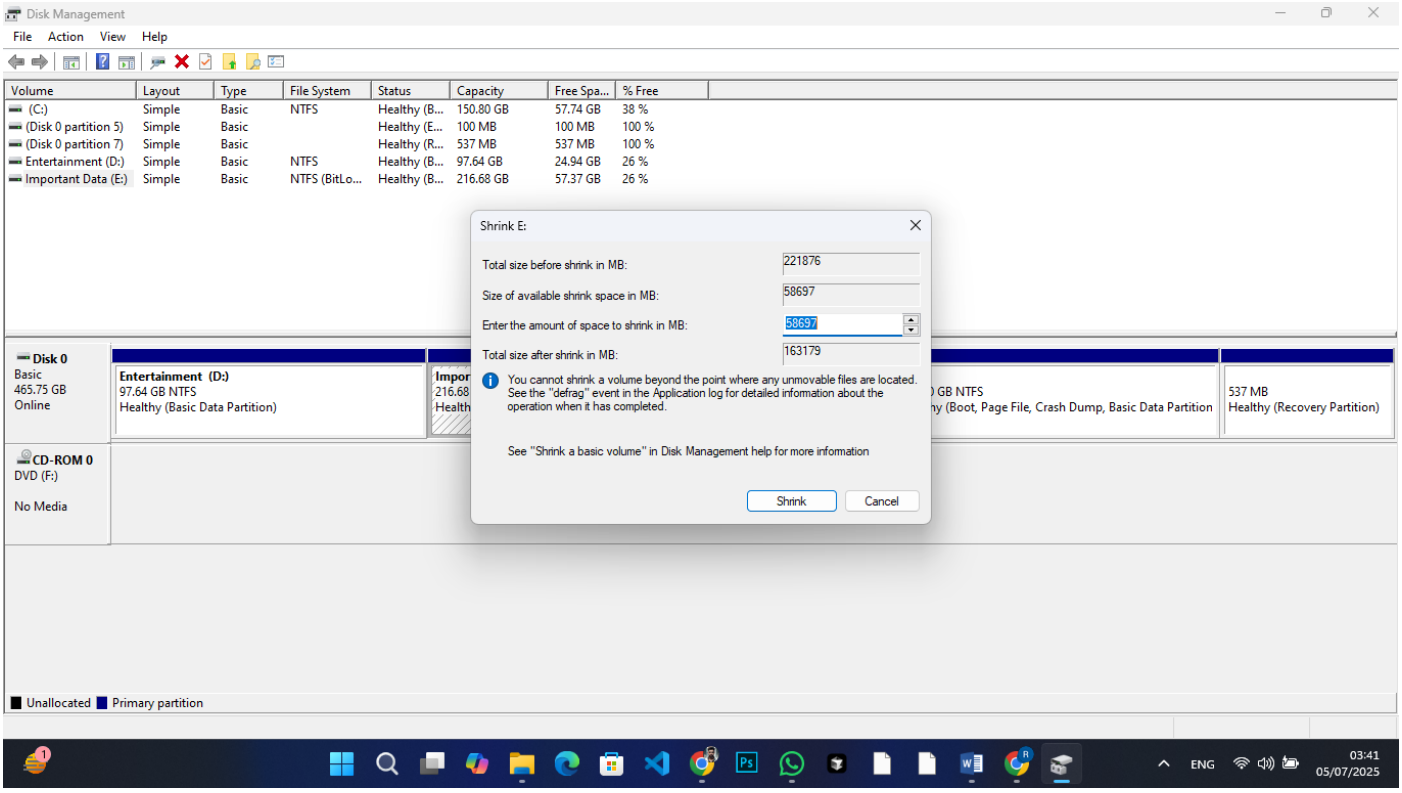

Figure 28 Shrink Partition

Create a New Partition

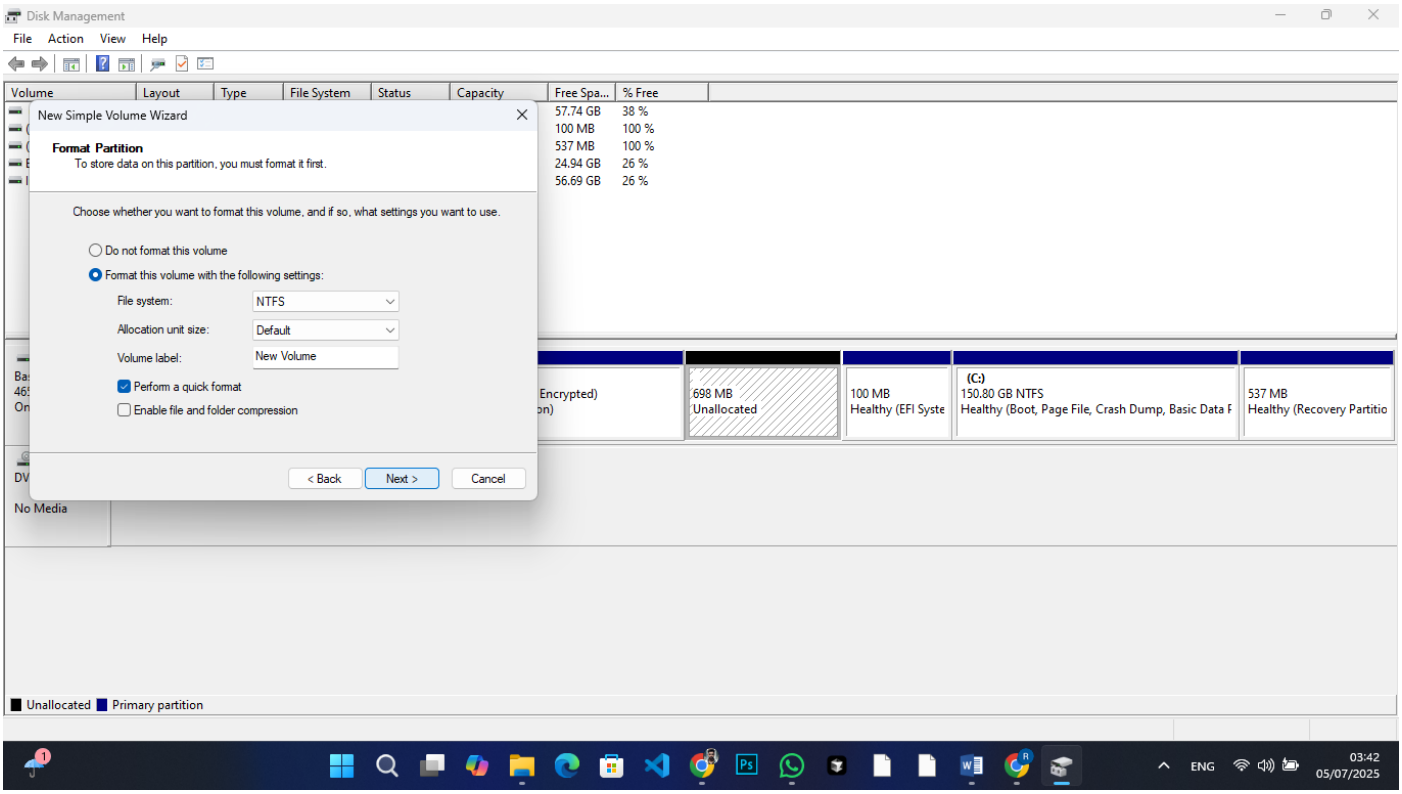

Figure 29 Create New Partition

Some Pictures are Copy in this Partition

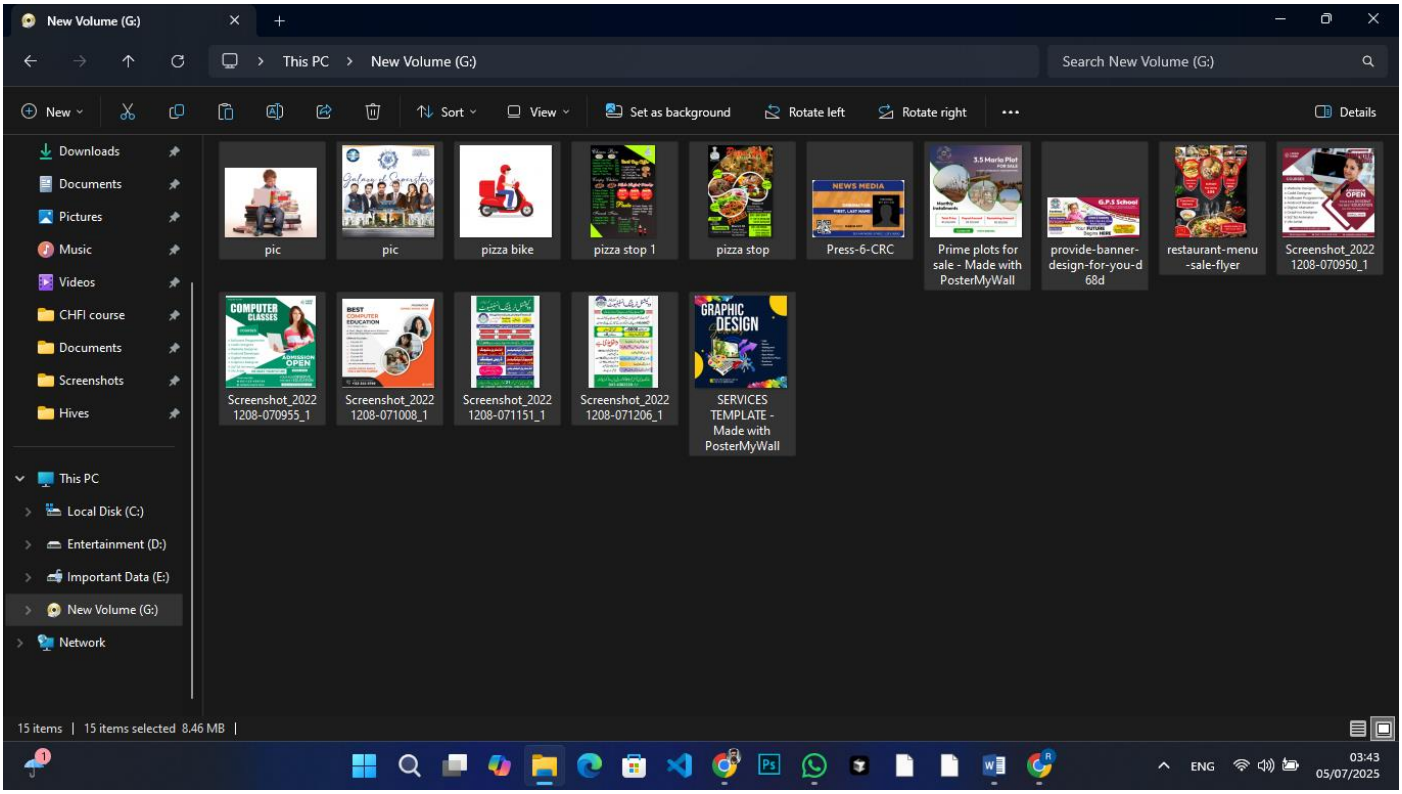

Figure 30 Copy Some Pictures

Format this Partition

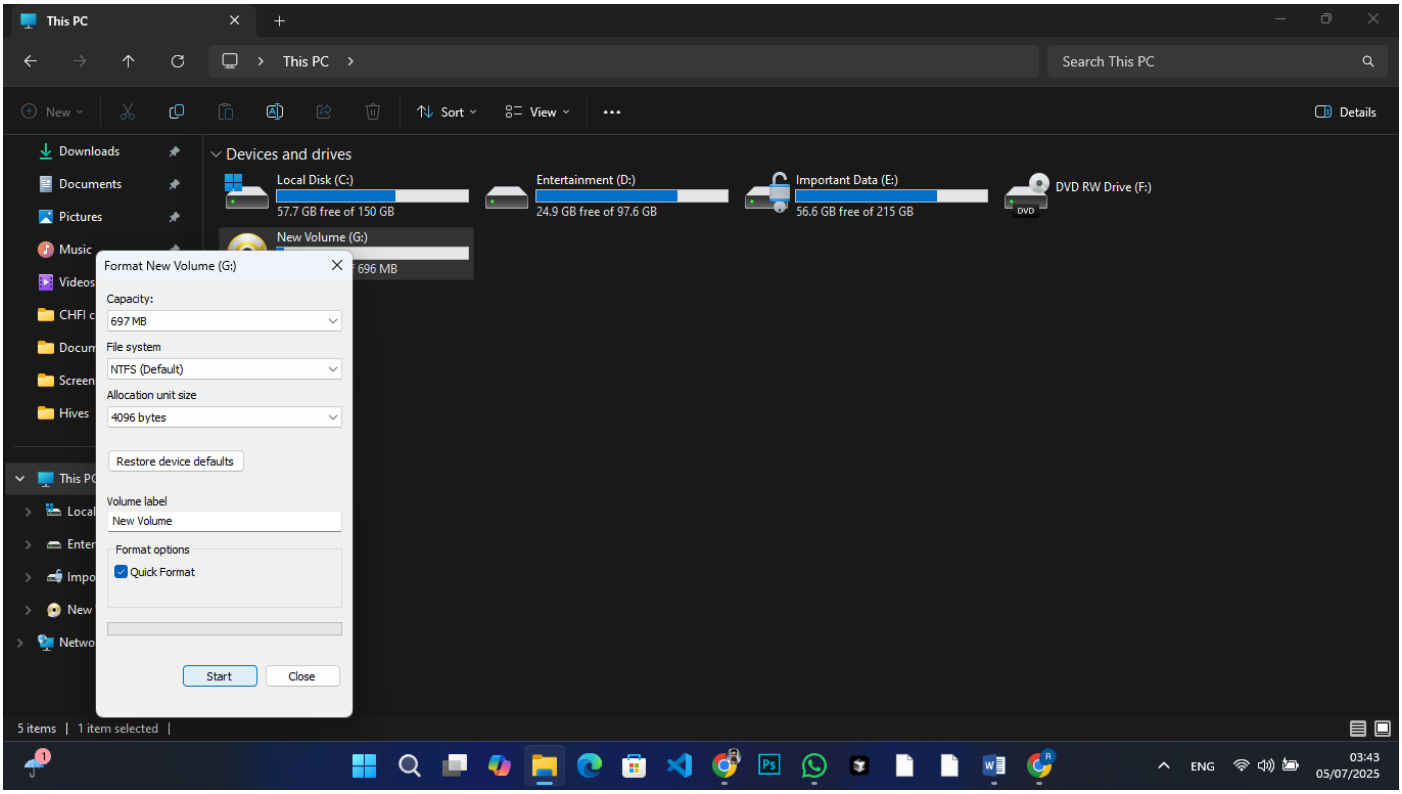

Figure 31 Format This Partition

Creating Image File using FTK Imager on this Partition

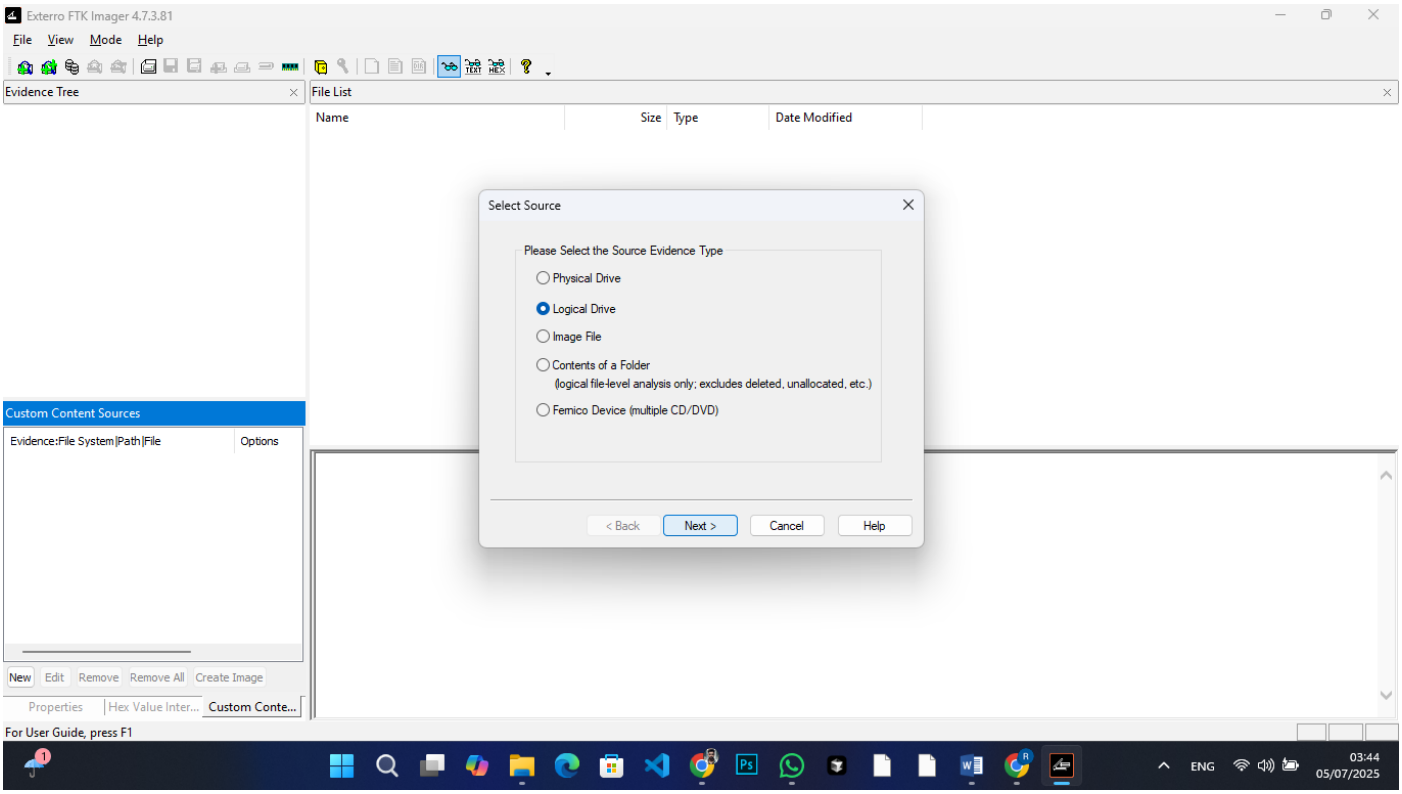

Figure 32 Select Logical Drive

Select Image Type (E01)

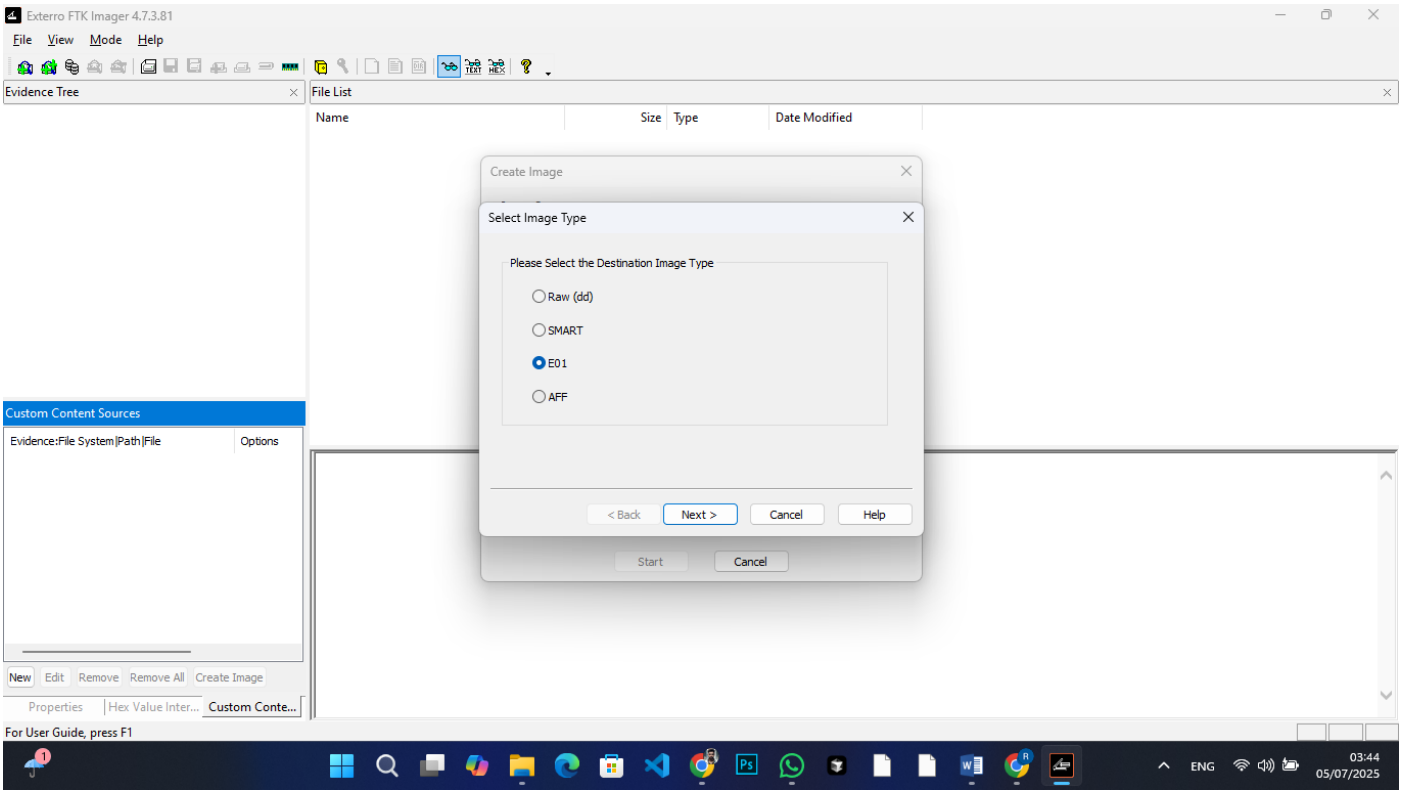

Figure 33 Select Image Type (E01)

Creating Image

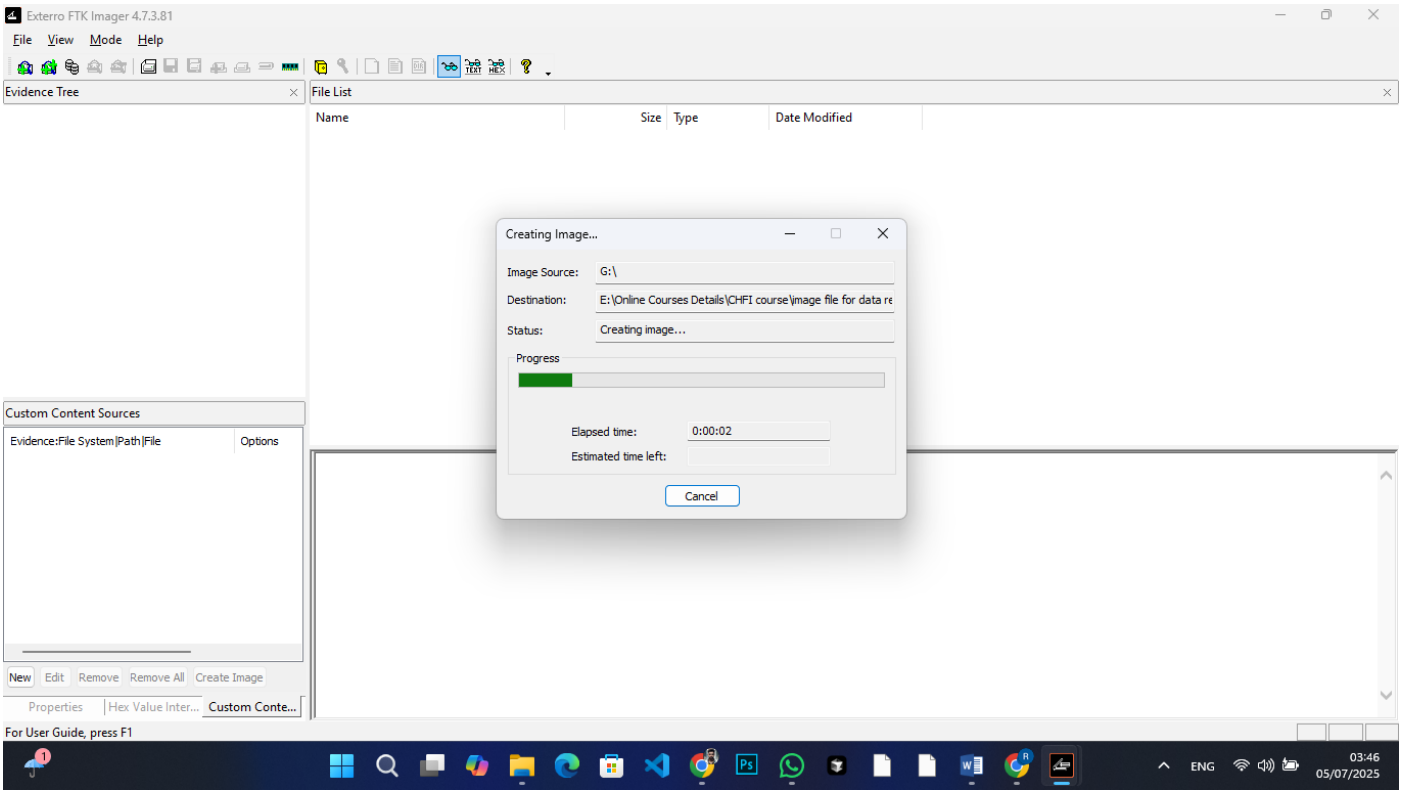

Figure 34 Creating Image

Image Summary

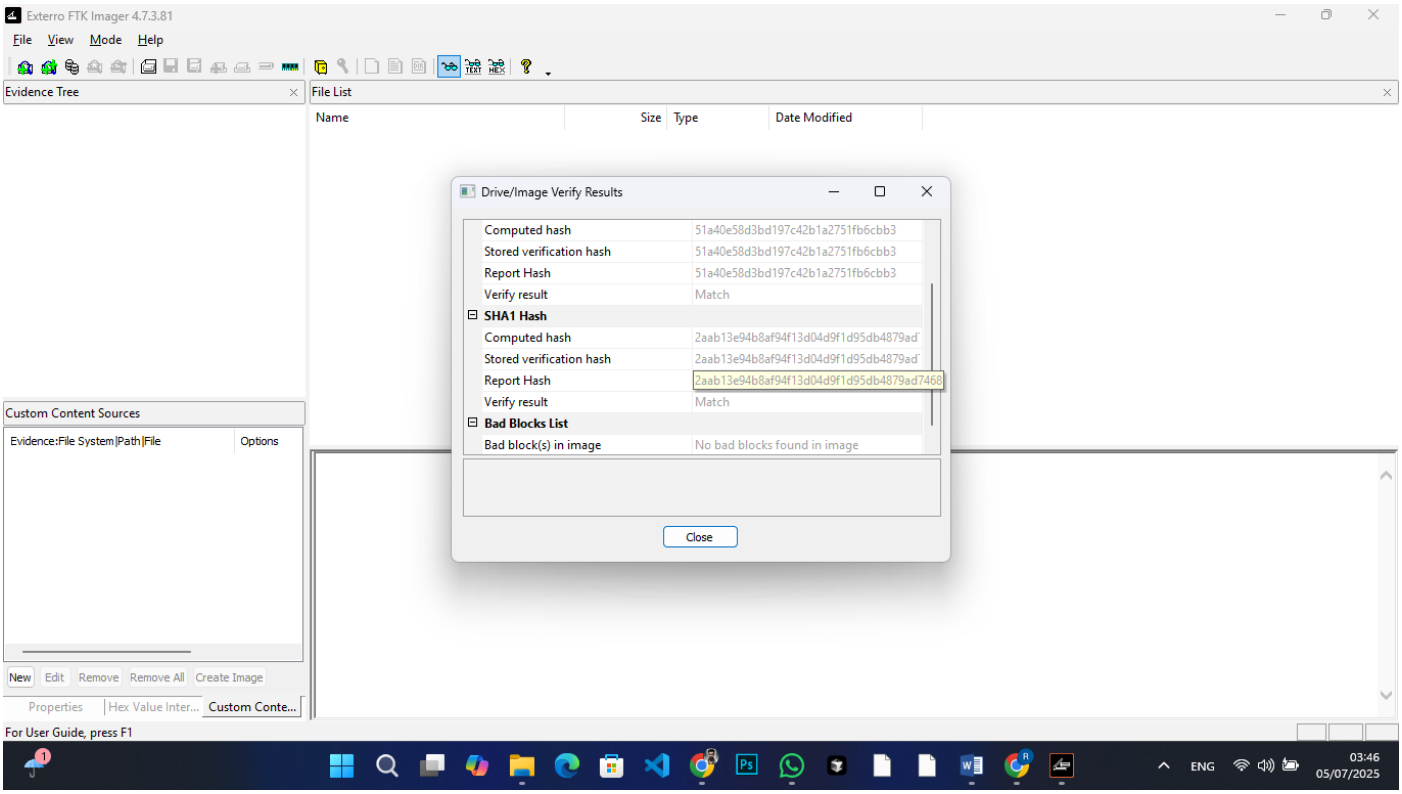

Figure 35 Image Summary

Data Recovery from image using Autopsy

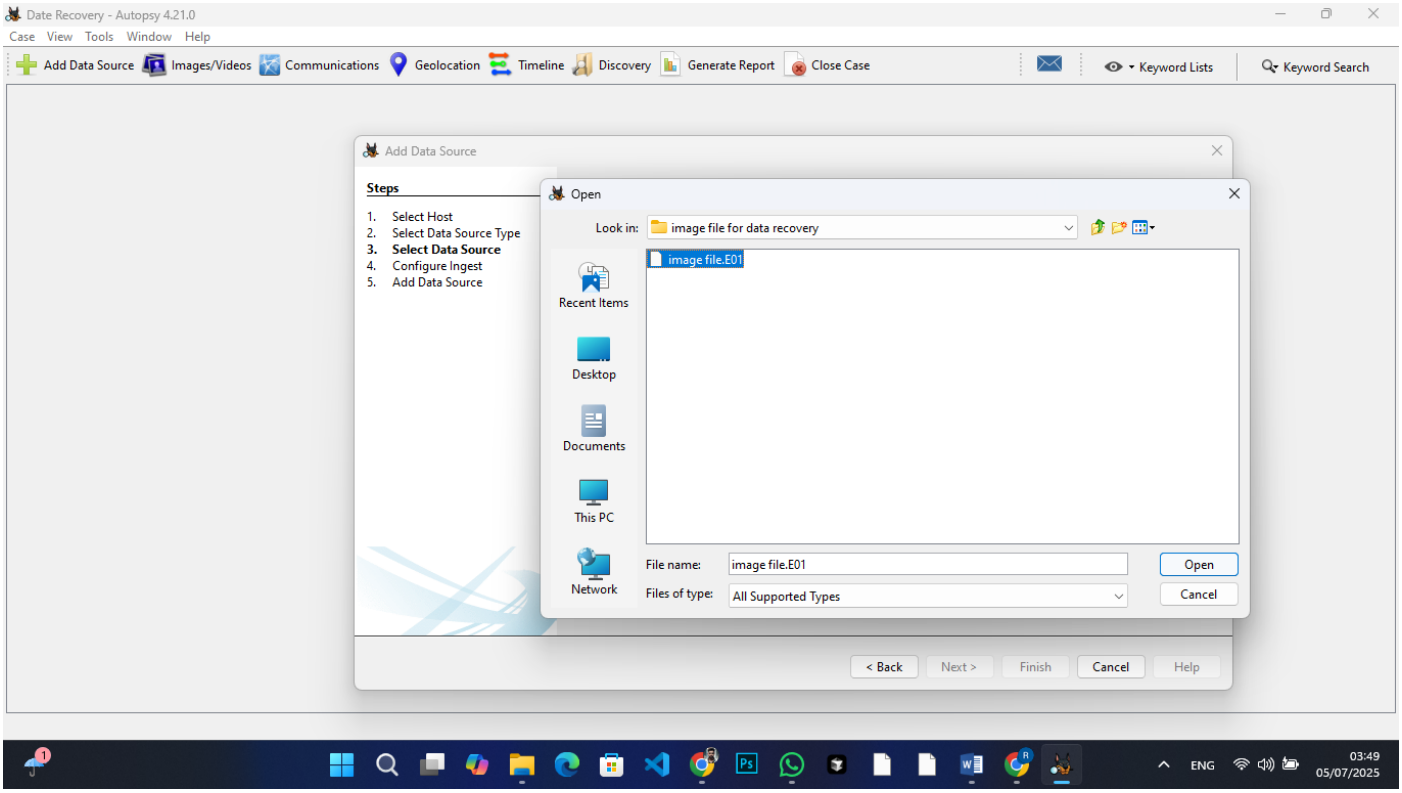

Figure 36 Select Image File

Select Configuration in autopsy

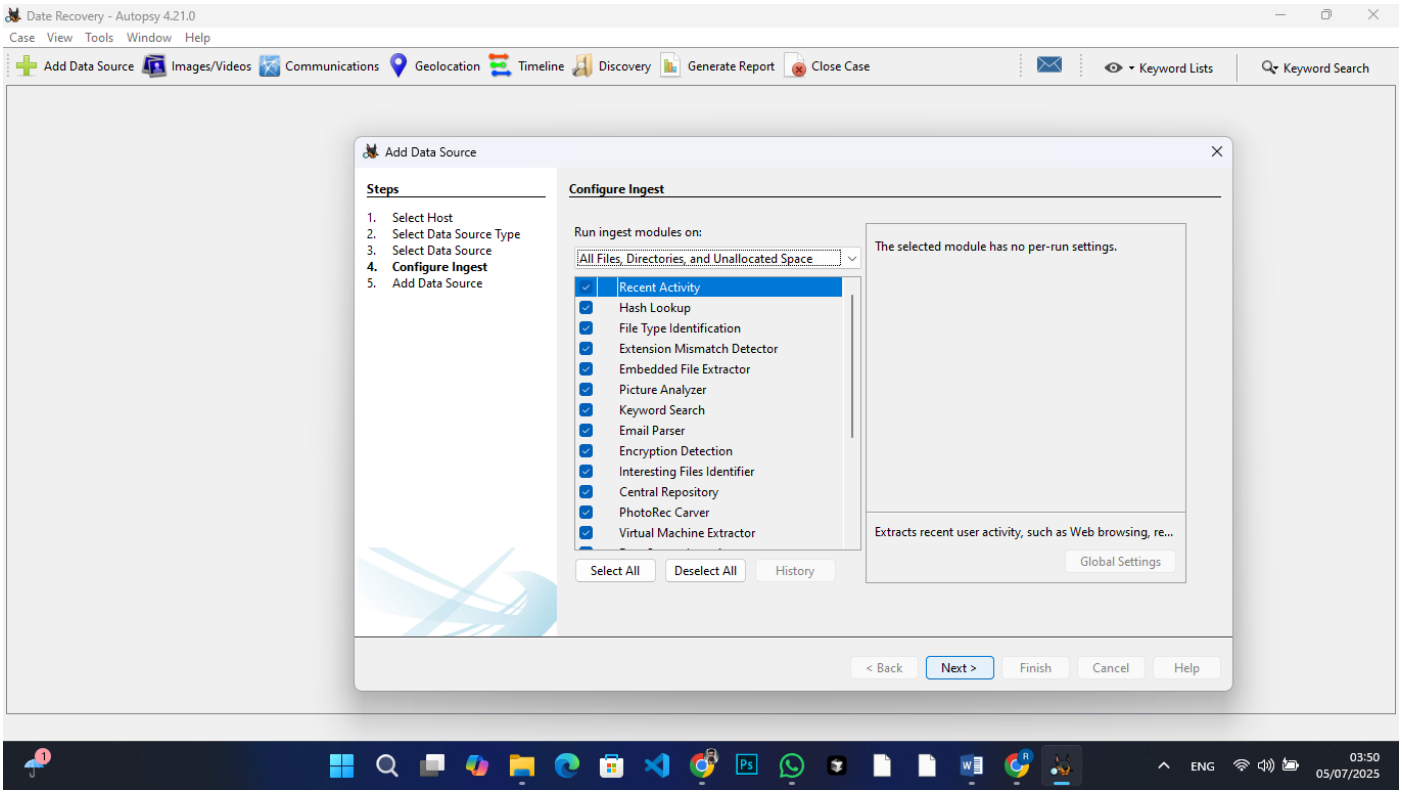

Figure 37Configuration Import

Load Image File in Autopsy

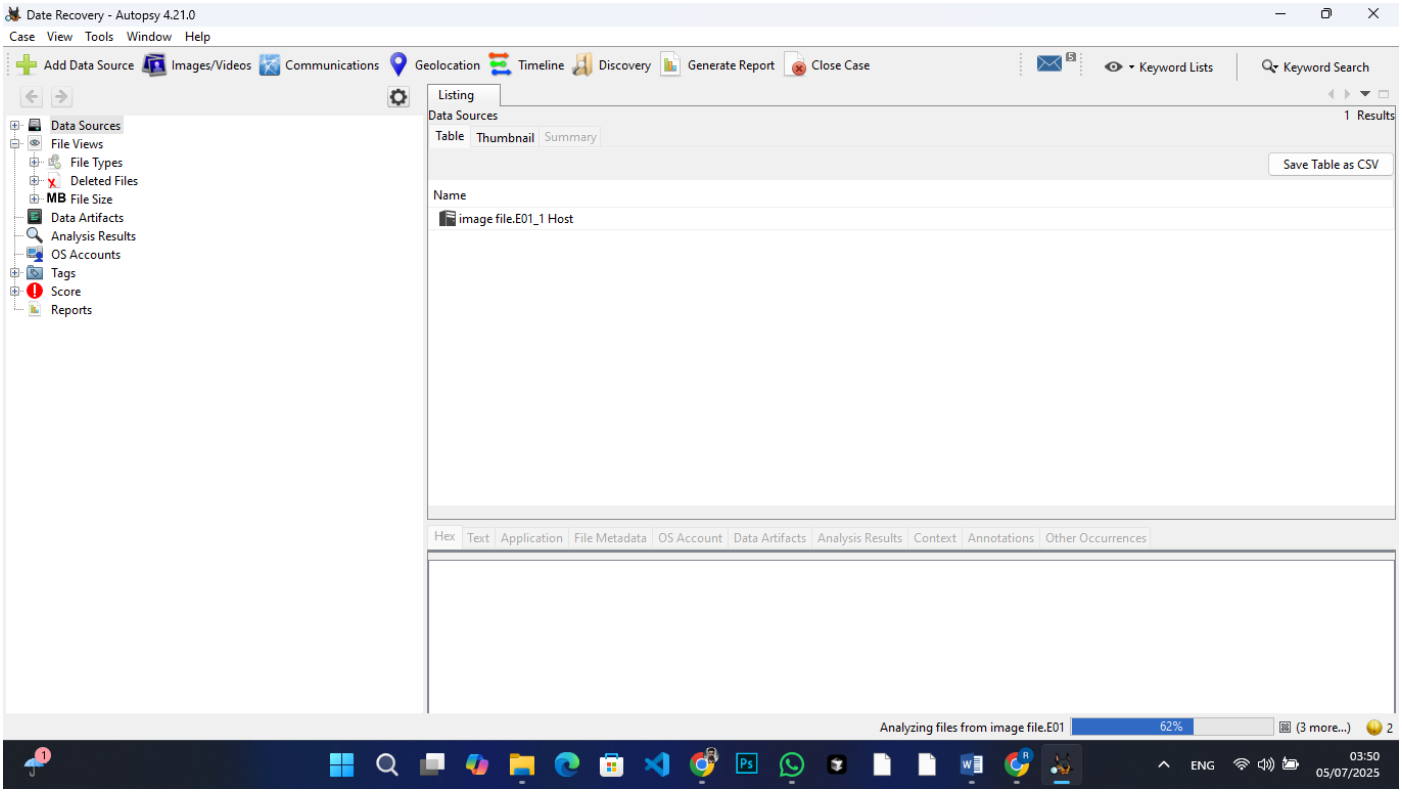

Figure 38 Load Image File in Autopsy

Deleted Files from Autopsy

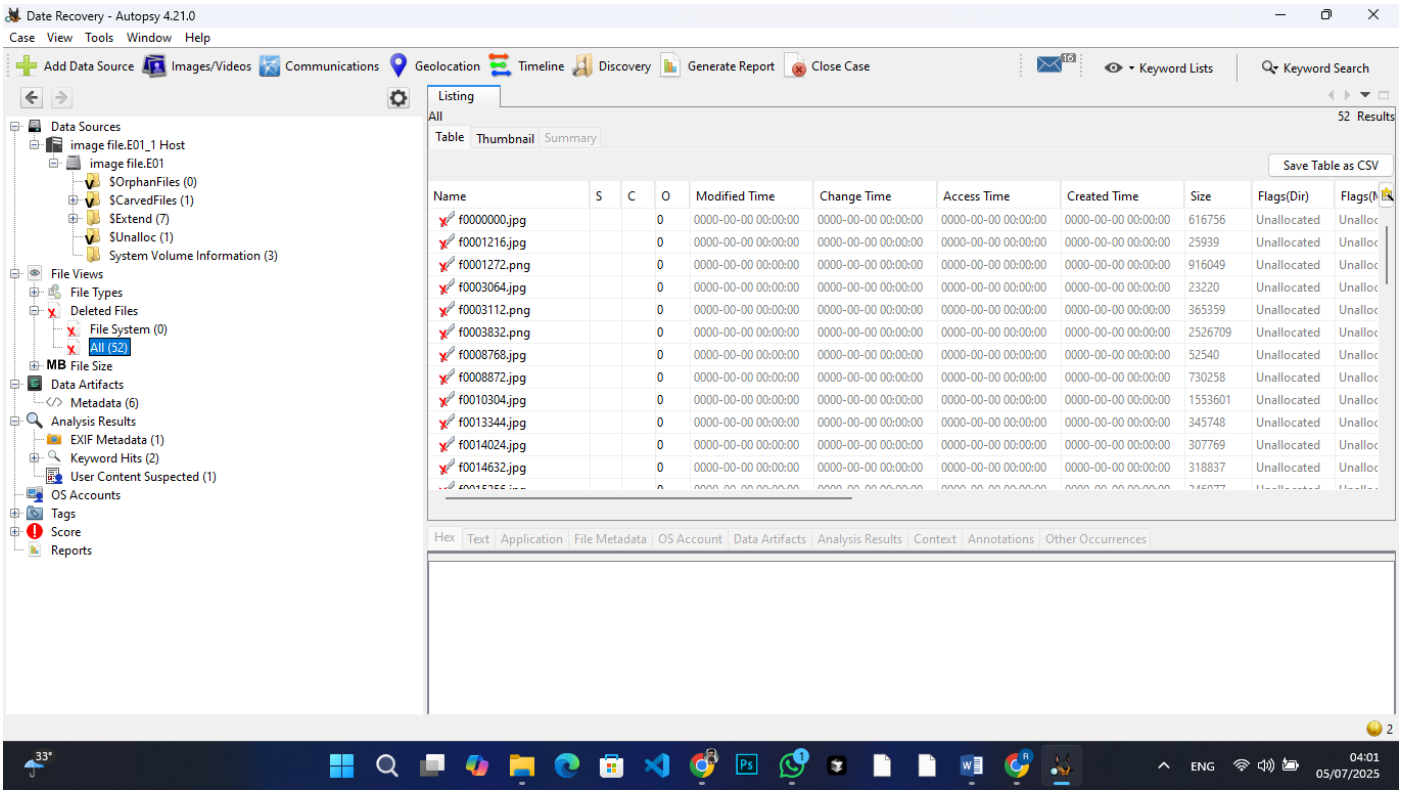

Figure 39 Deleted Files

Export Deleted Files

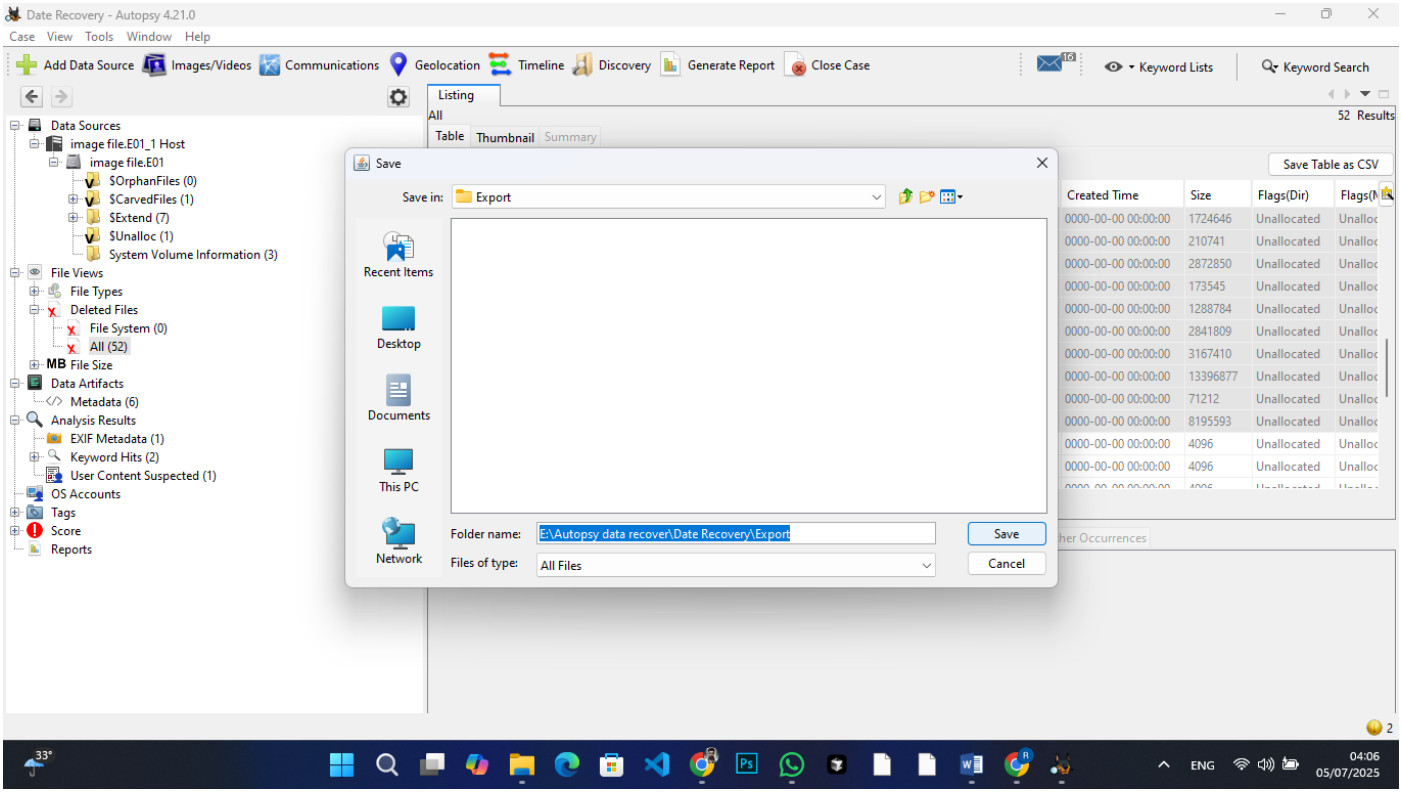

Figure 40 Export Deleted Files

All Images Recover

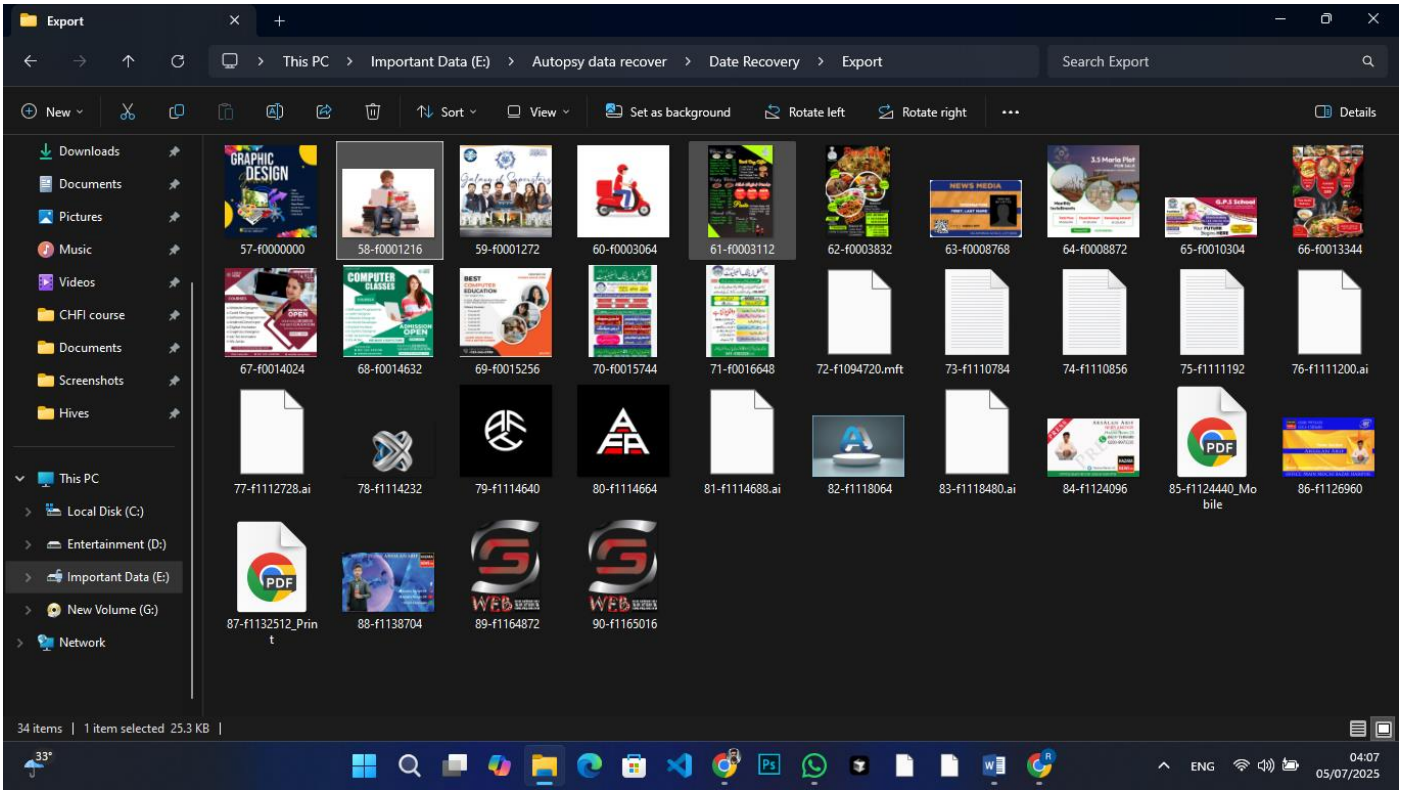

Figure 41 All Images Recover

Image Metadata Using Exif Tool

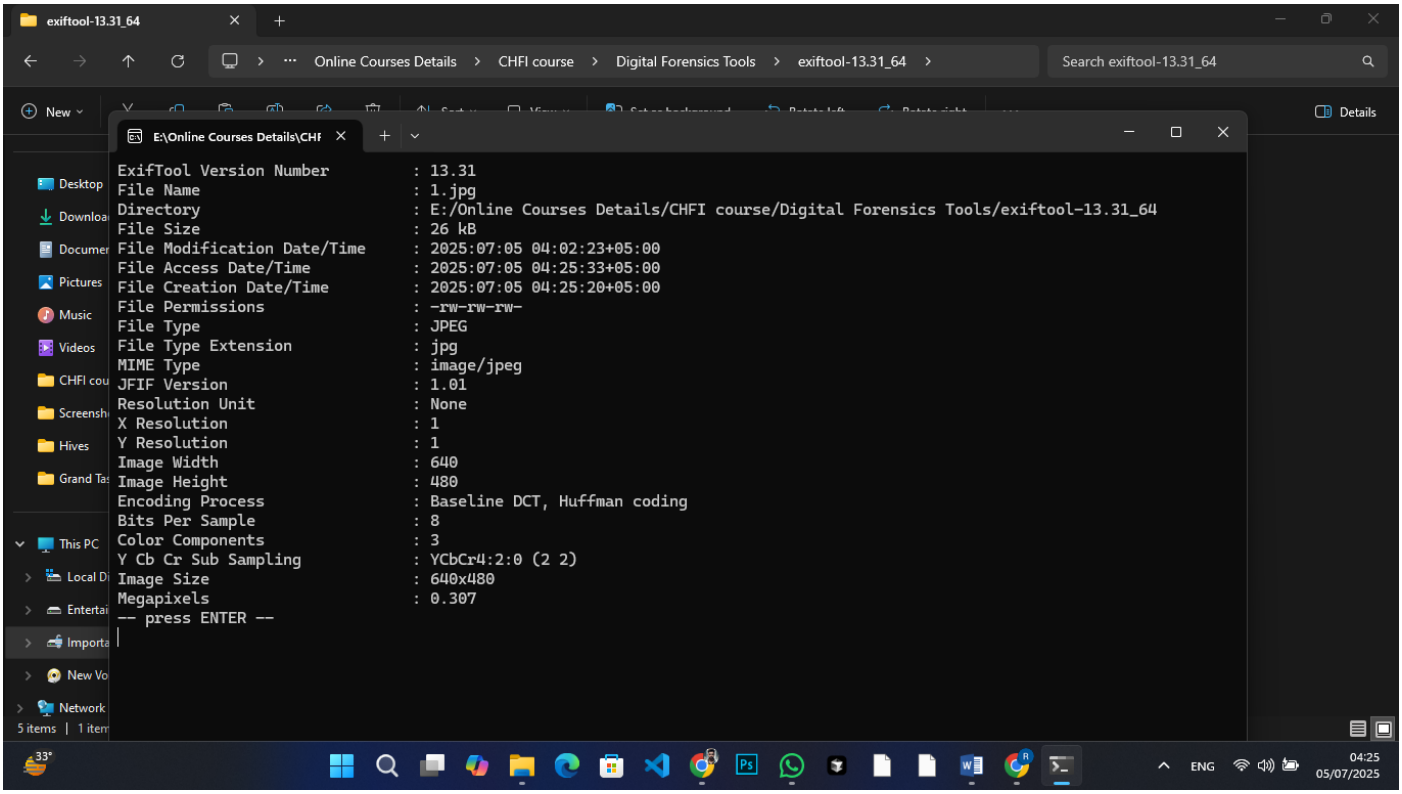

Figure 42 Image Metadata Using Exif Tool

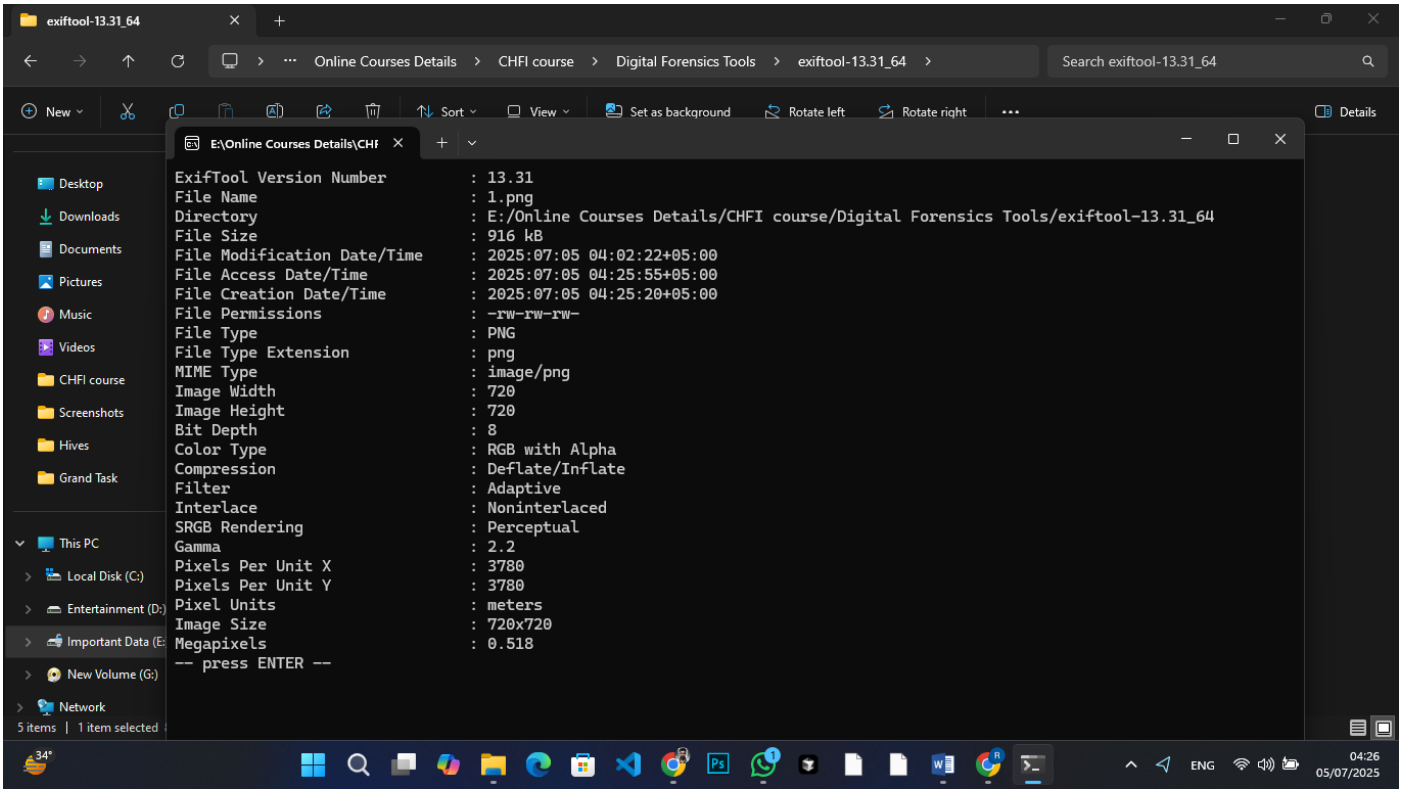

Figure 43 Image Metadata Using Exif Tool

5.5 What browser activity suggests credential theft or staging?

Browser History Examiner (Tool)

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

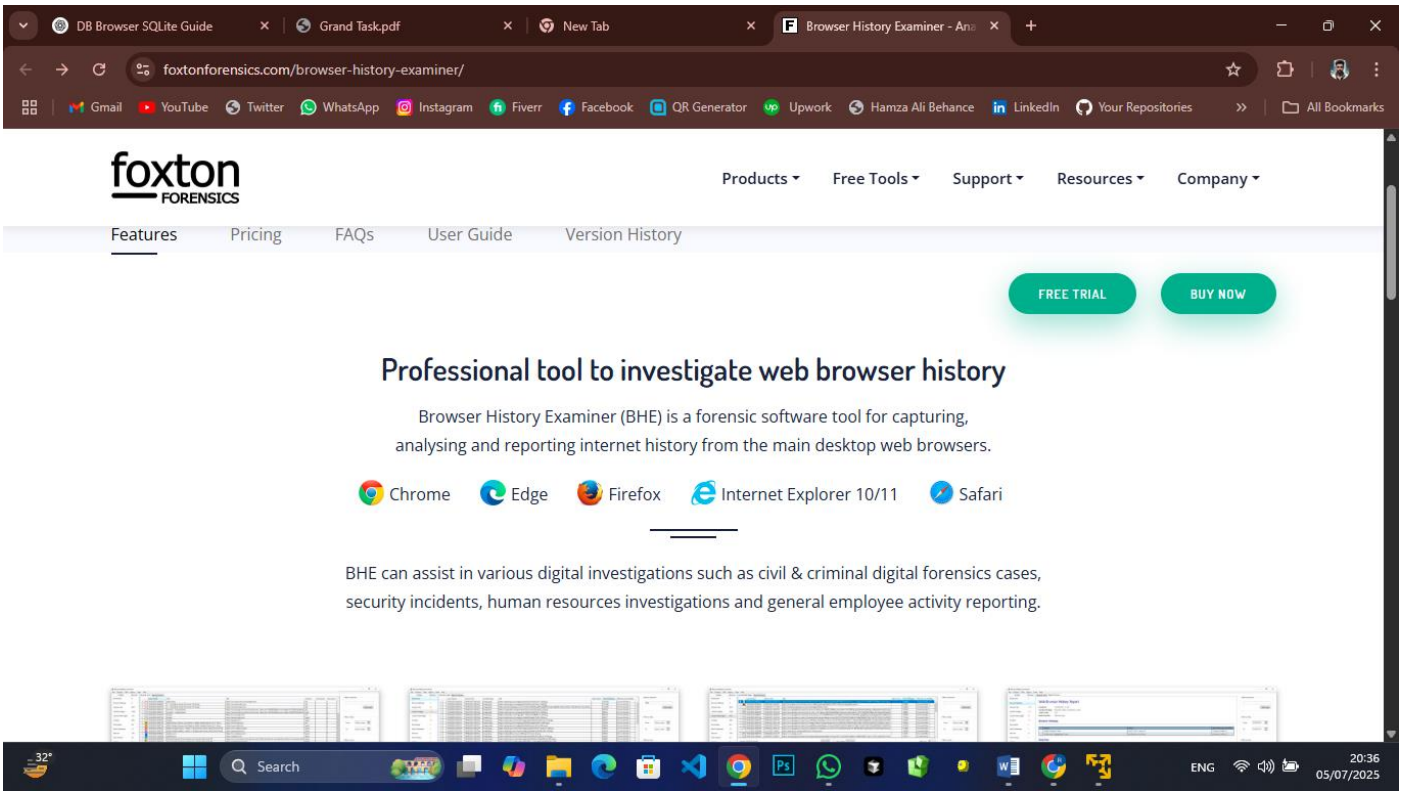

Figure 44 Browser History Examiner

I install the tool than open trial version

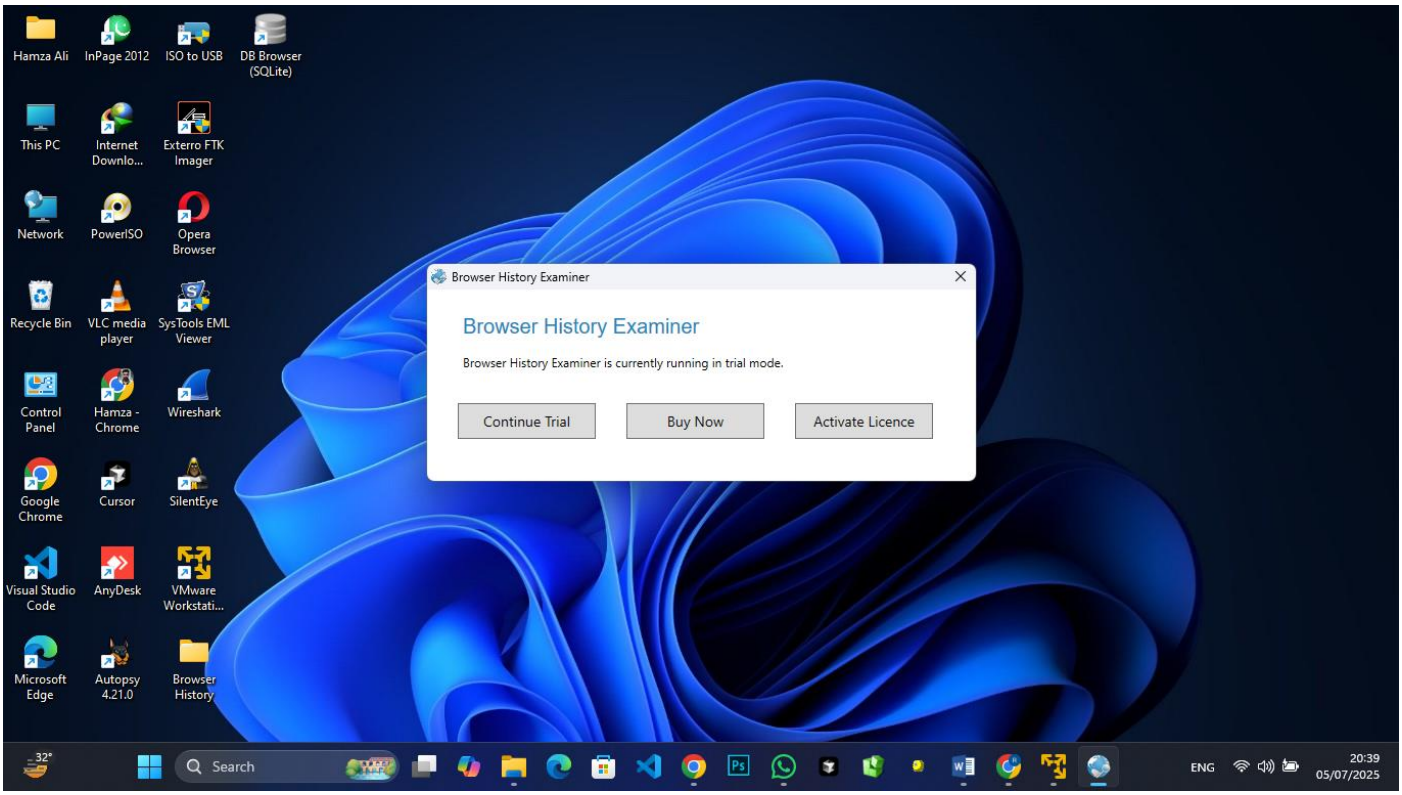

Figure 45 click Trial Version

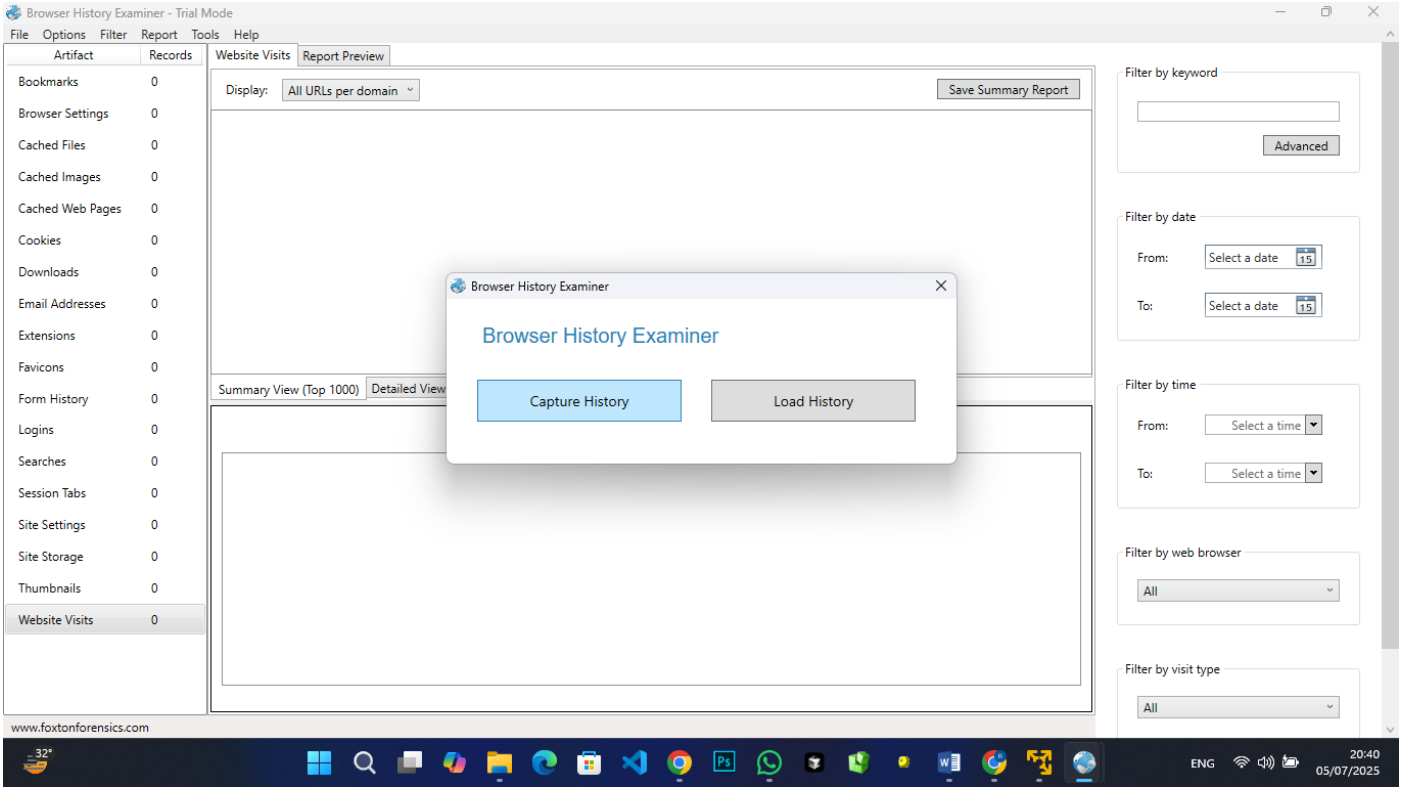

Figure 46 Capture Memory

Select history from this Computer

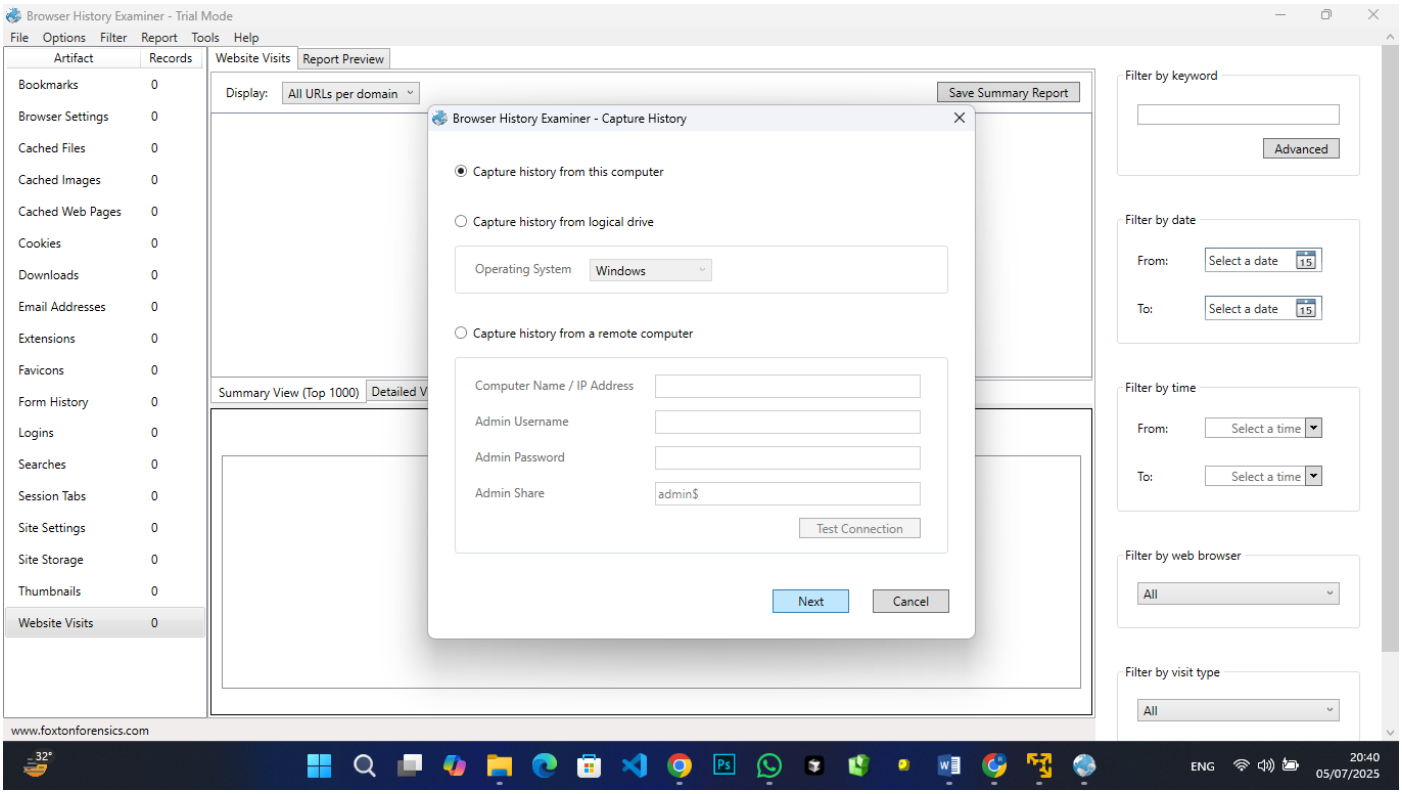

Figure 47 Select History from this Computer

Choose Browsers

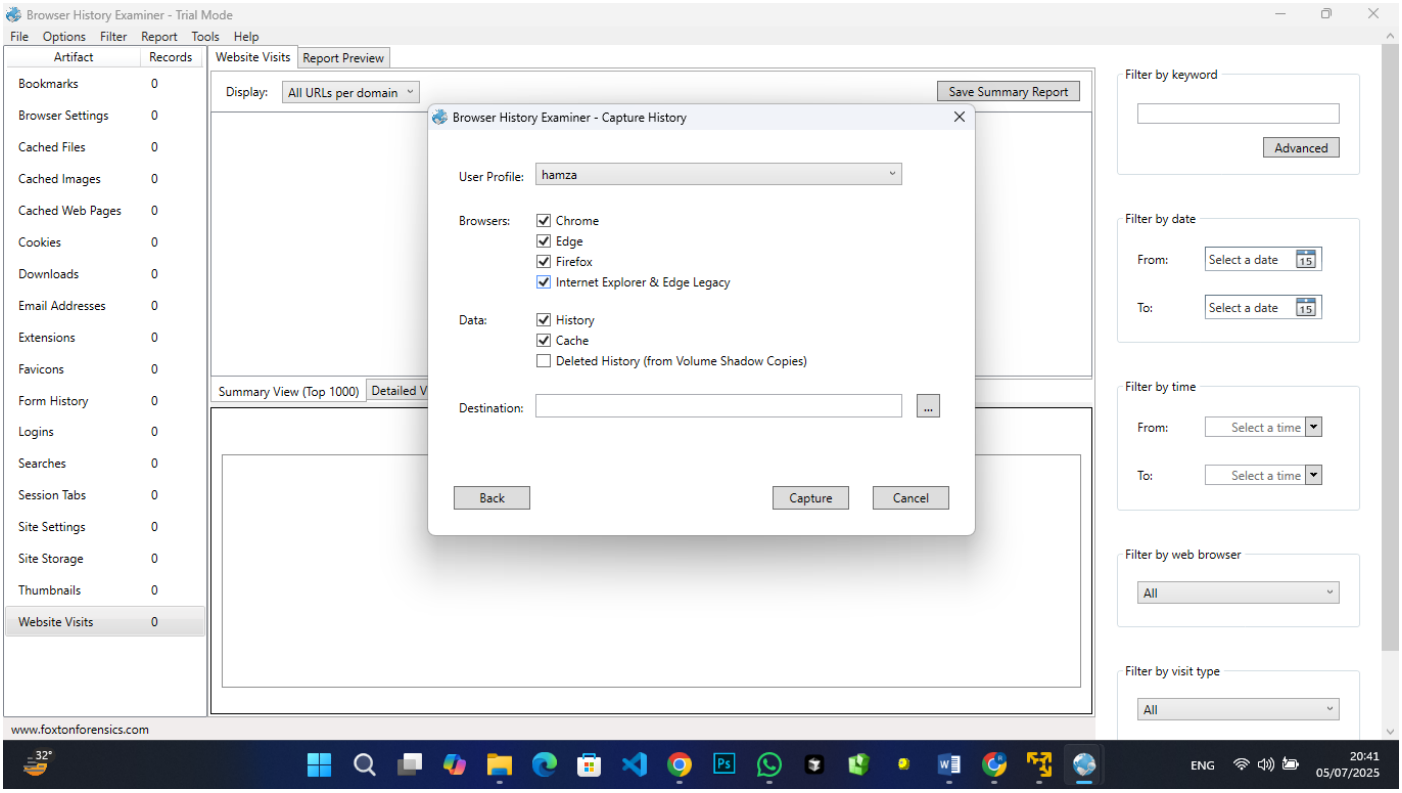

Figure 48 choose Browsers

Choose Destination Where save the files

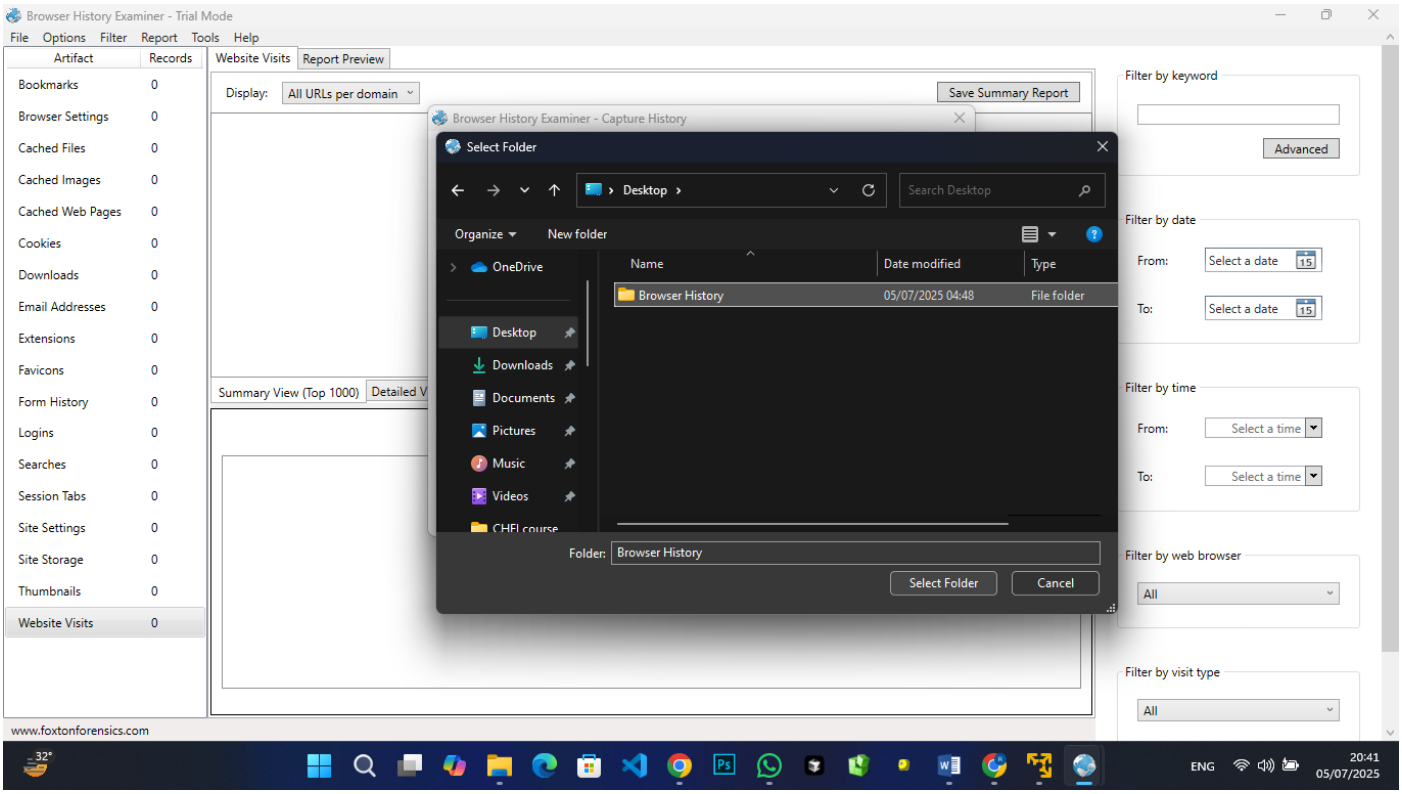

Figure 49 choose Destination

And then Start Capture Memory

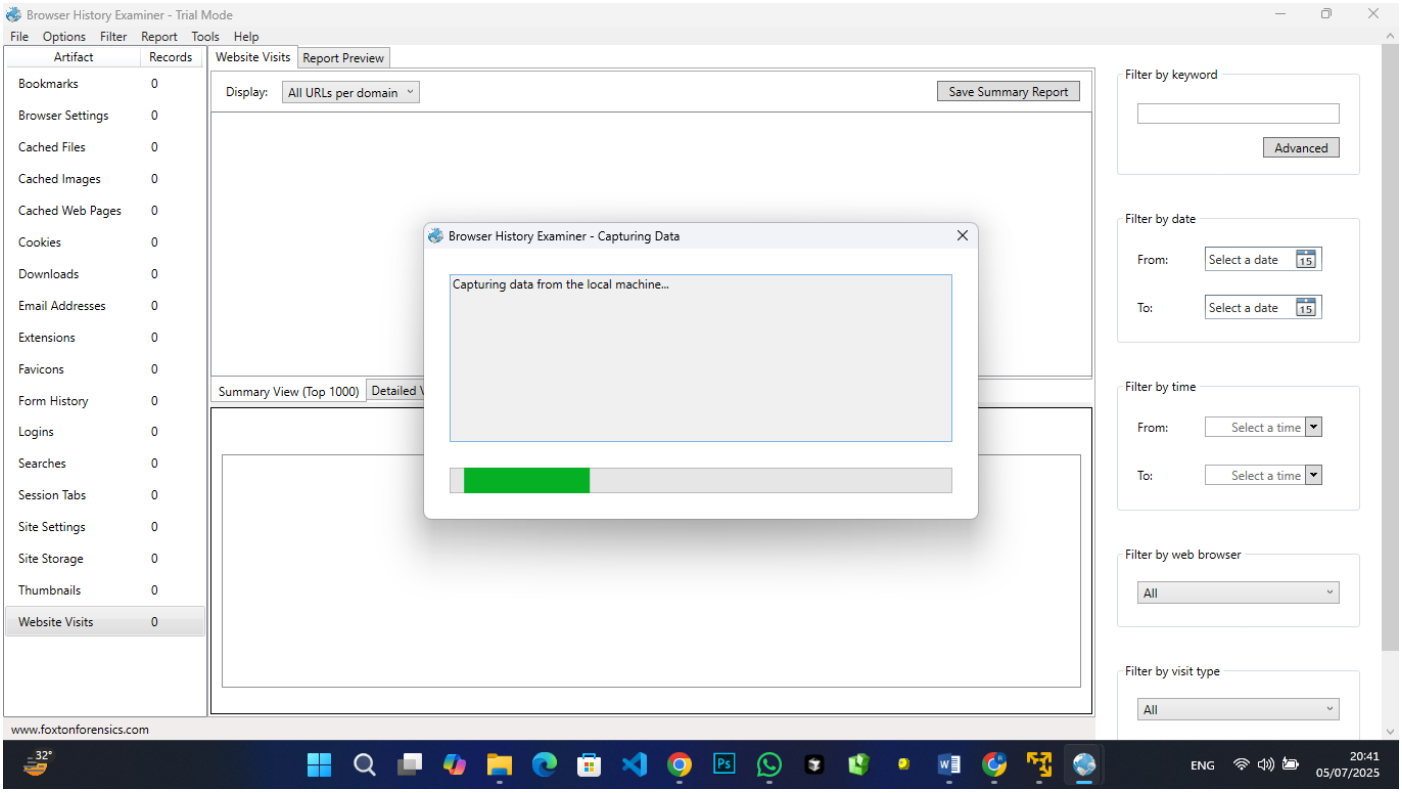

Figure 50 Capturing Browser History and Details

All Browsers History

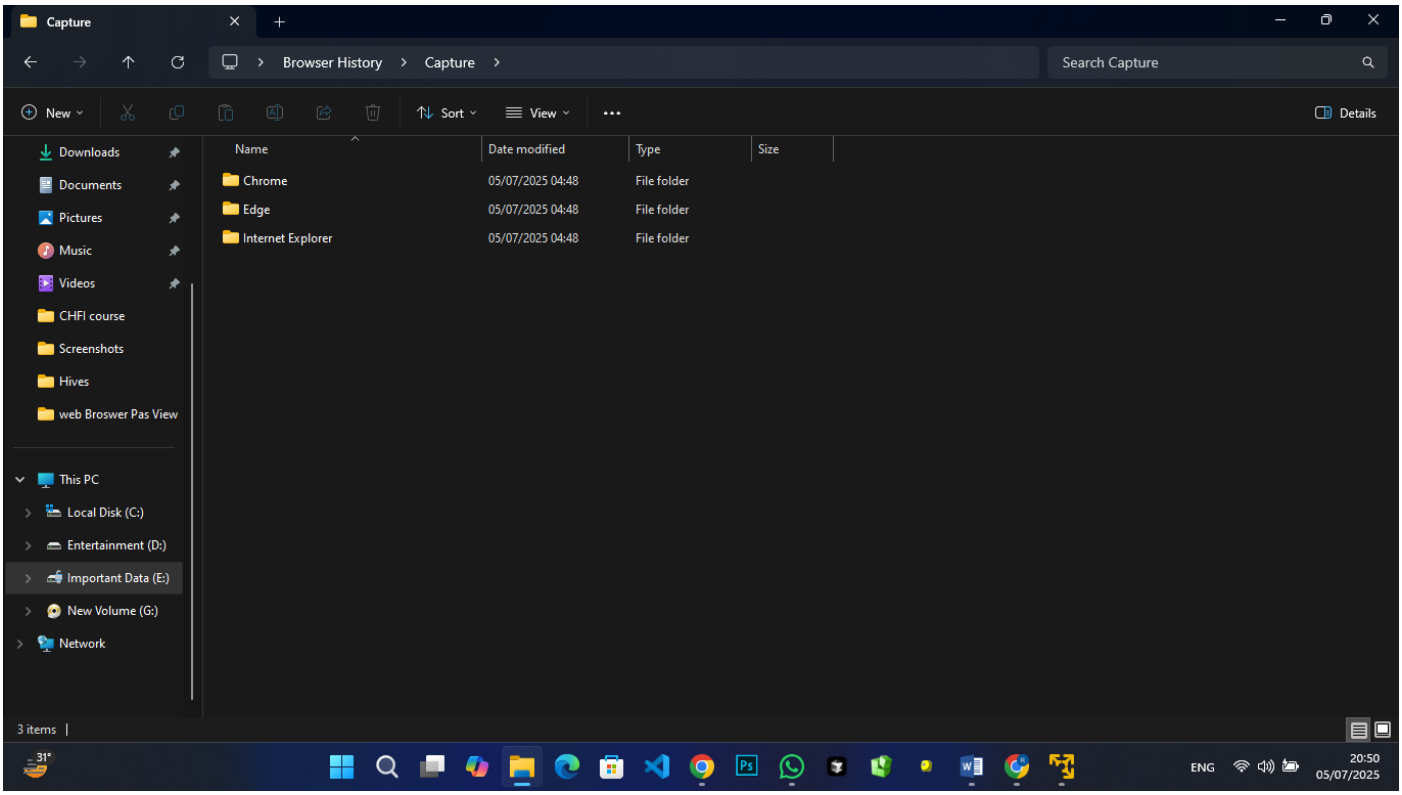

Figure 51 All Browsers History

Chrome history Profile-2 (All Recent Websites)

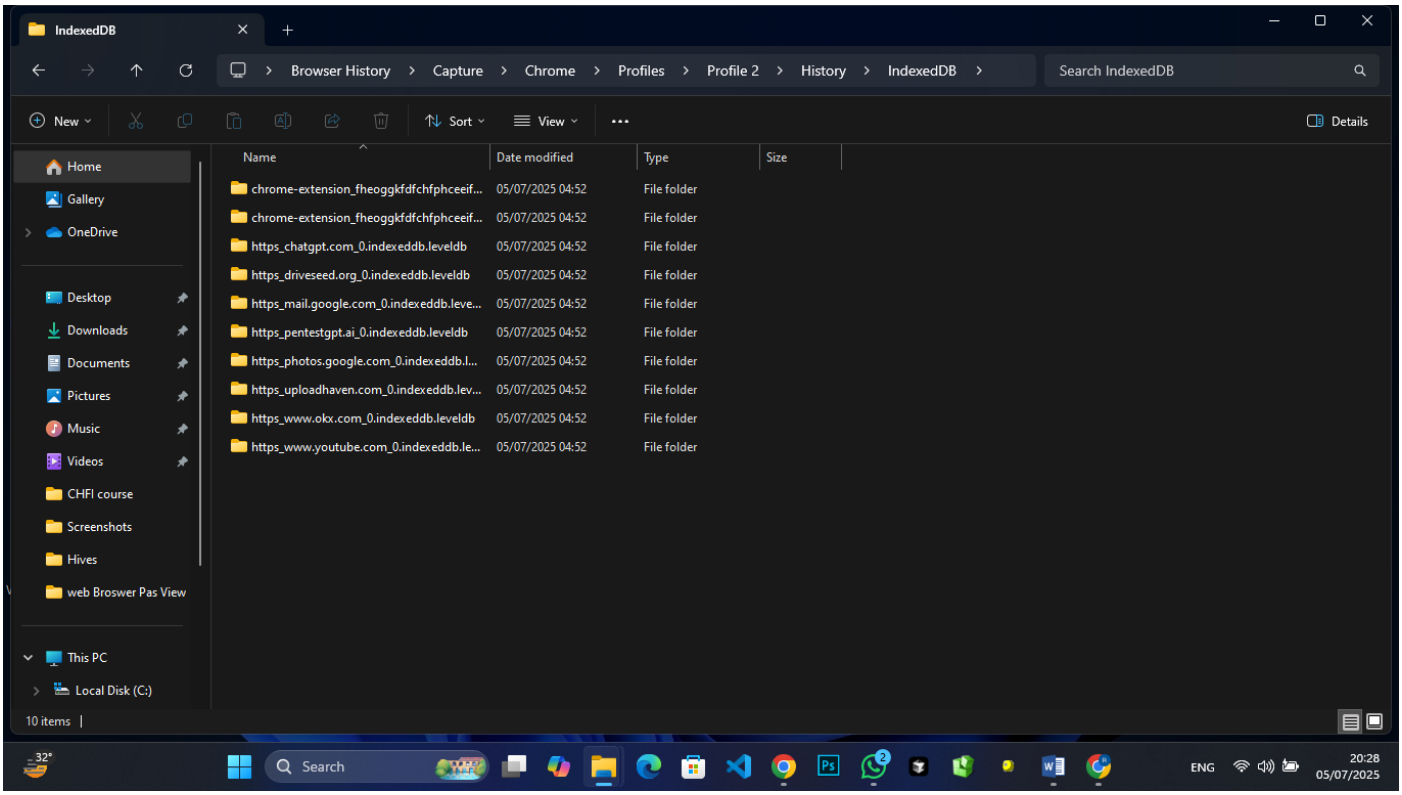

Figure 52 All Recent Websites

Login Details with websites Timestamps

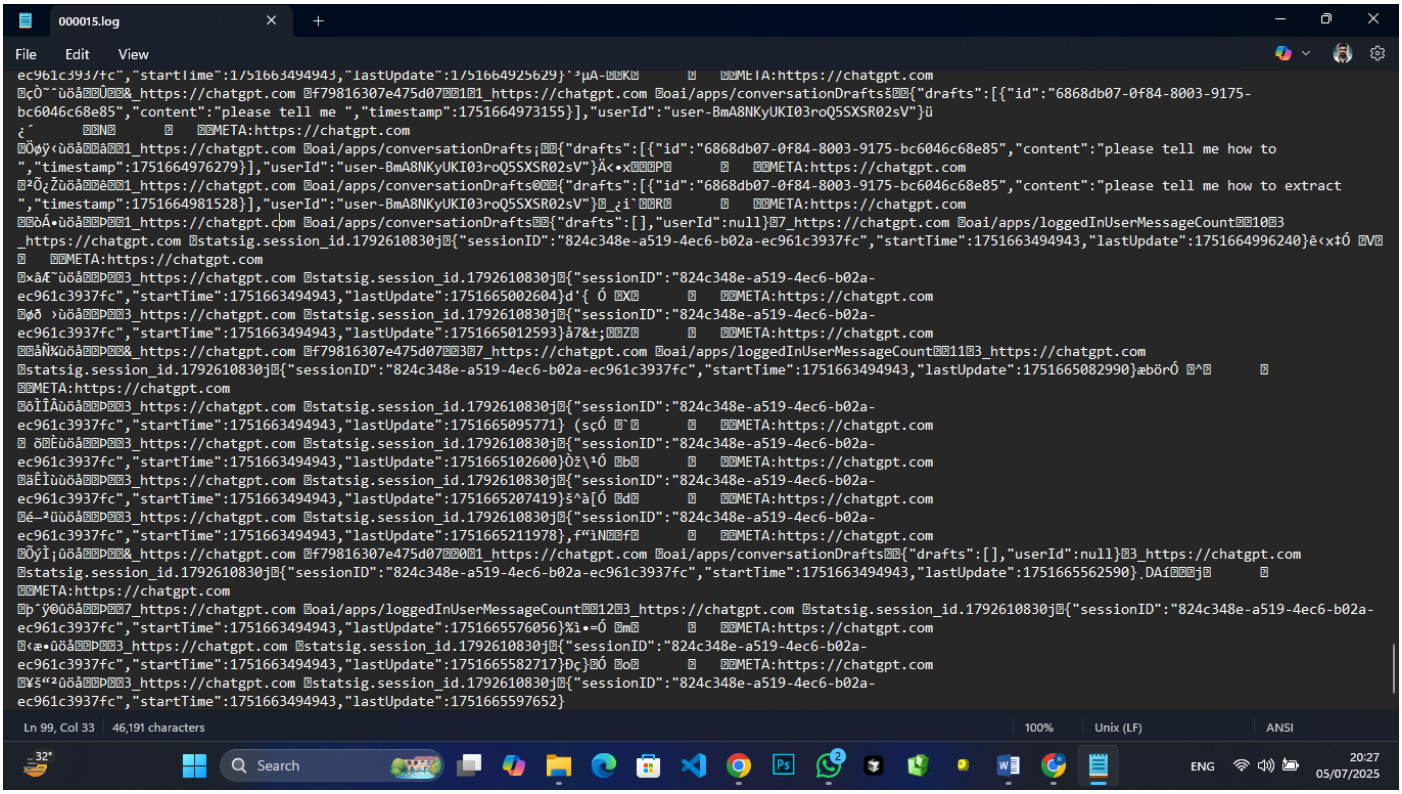

Figure 53 Browser websites login details with Timestamps

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

Search (eventvwr.msc) in run command

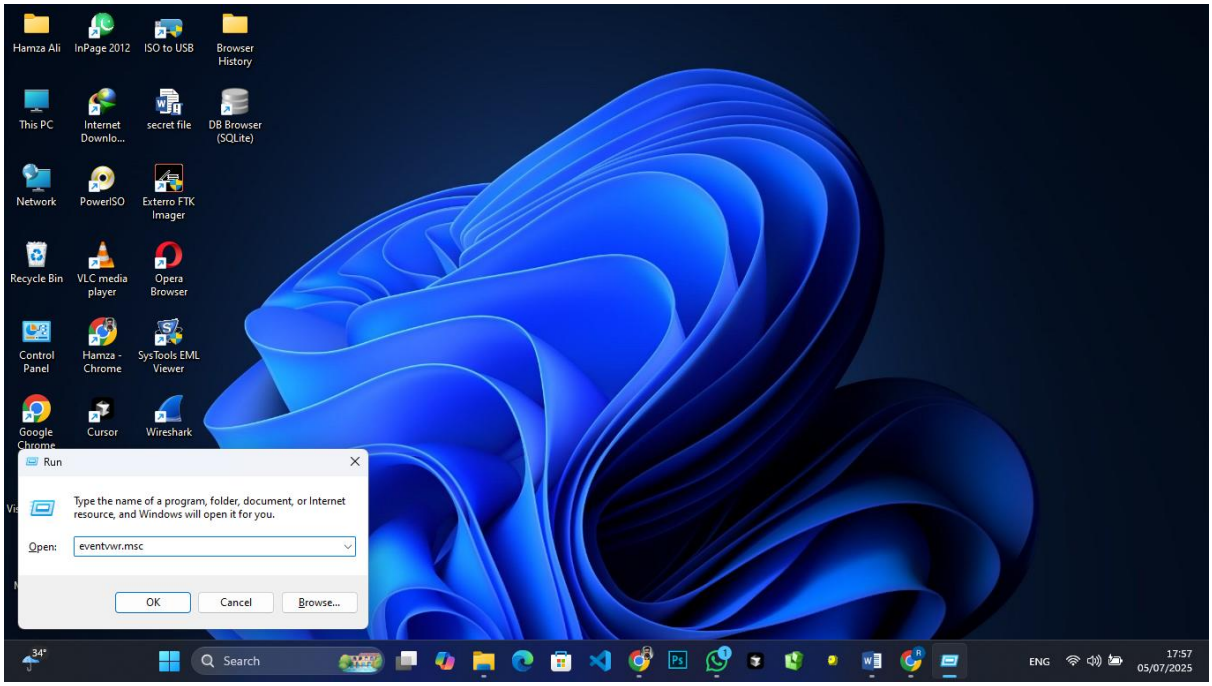

Figure 54 Search window event viewer

Opening Window Event Viewer

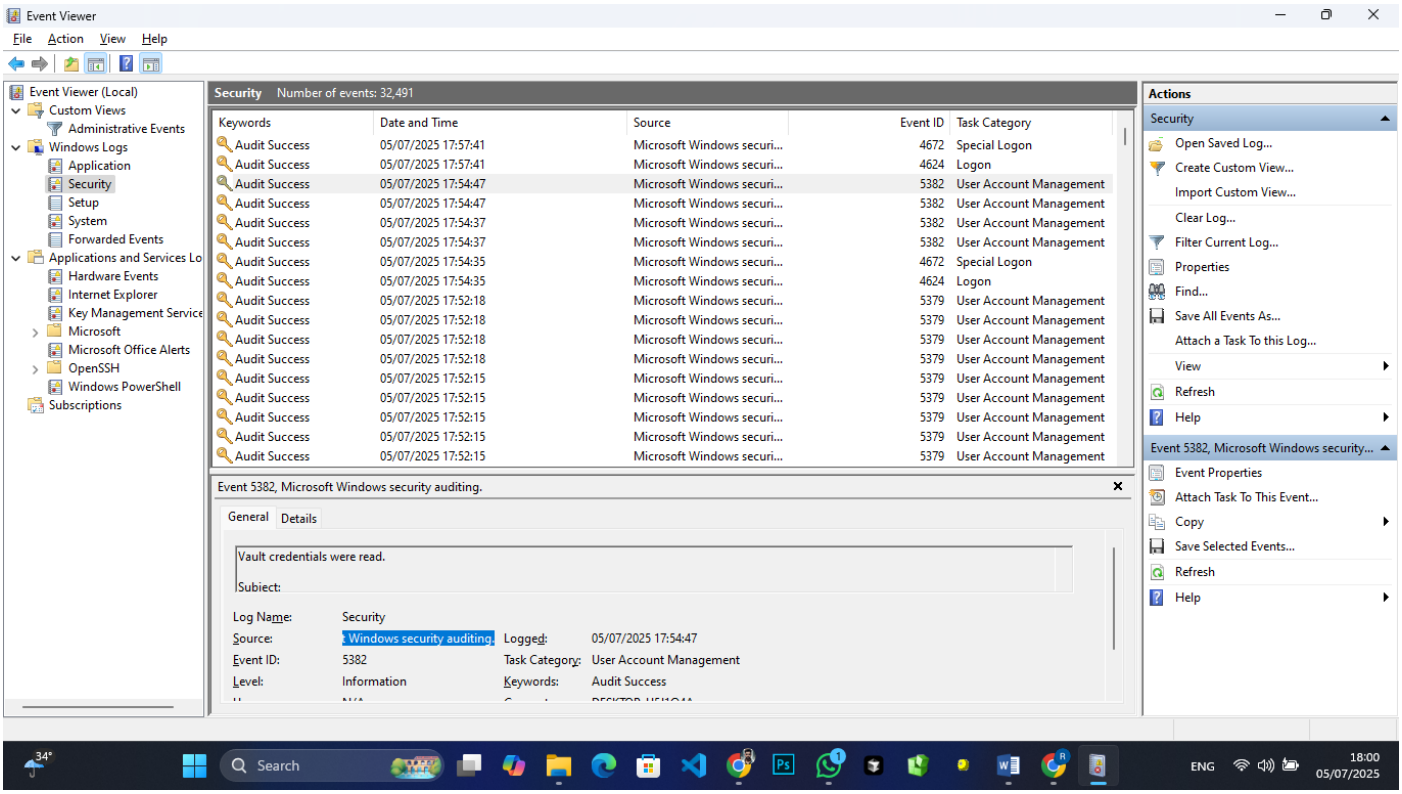

Figure 55 Window Event Viewer Security details

5.7 What network artifacts indicate exfiltration?

Device Linux

Open Wireshark through the terminal

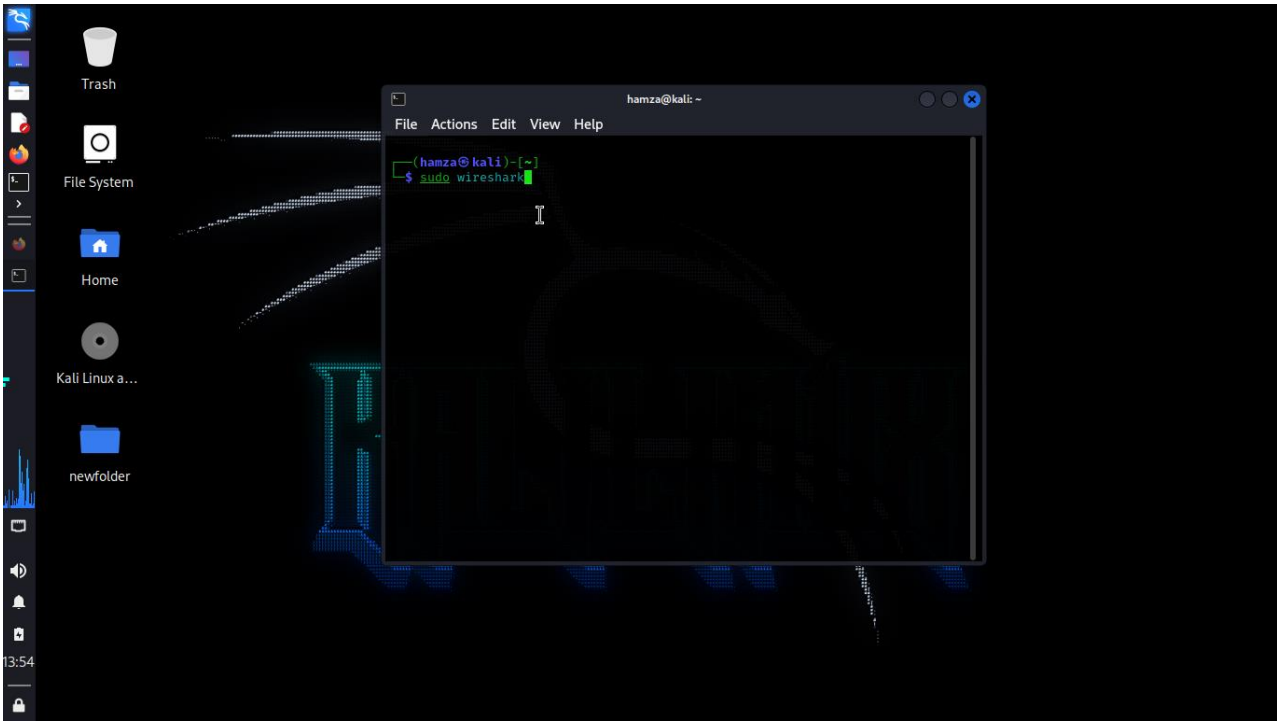

Figure 56 Open Wireshark through Linux terminal

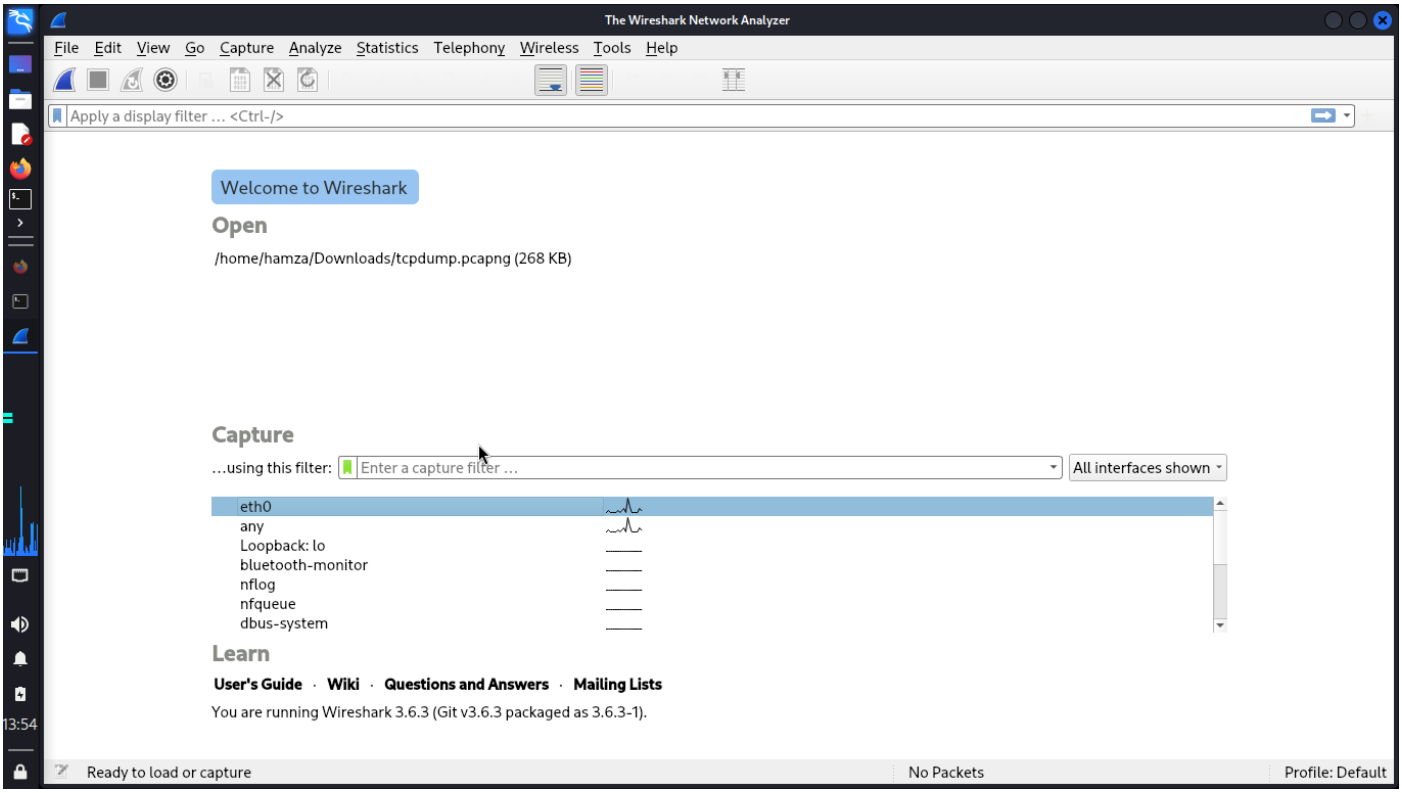

Figure 57 Click eth0

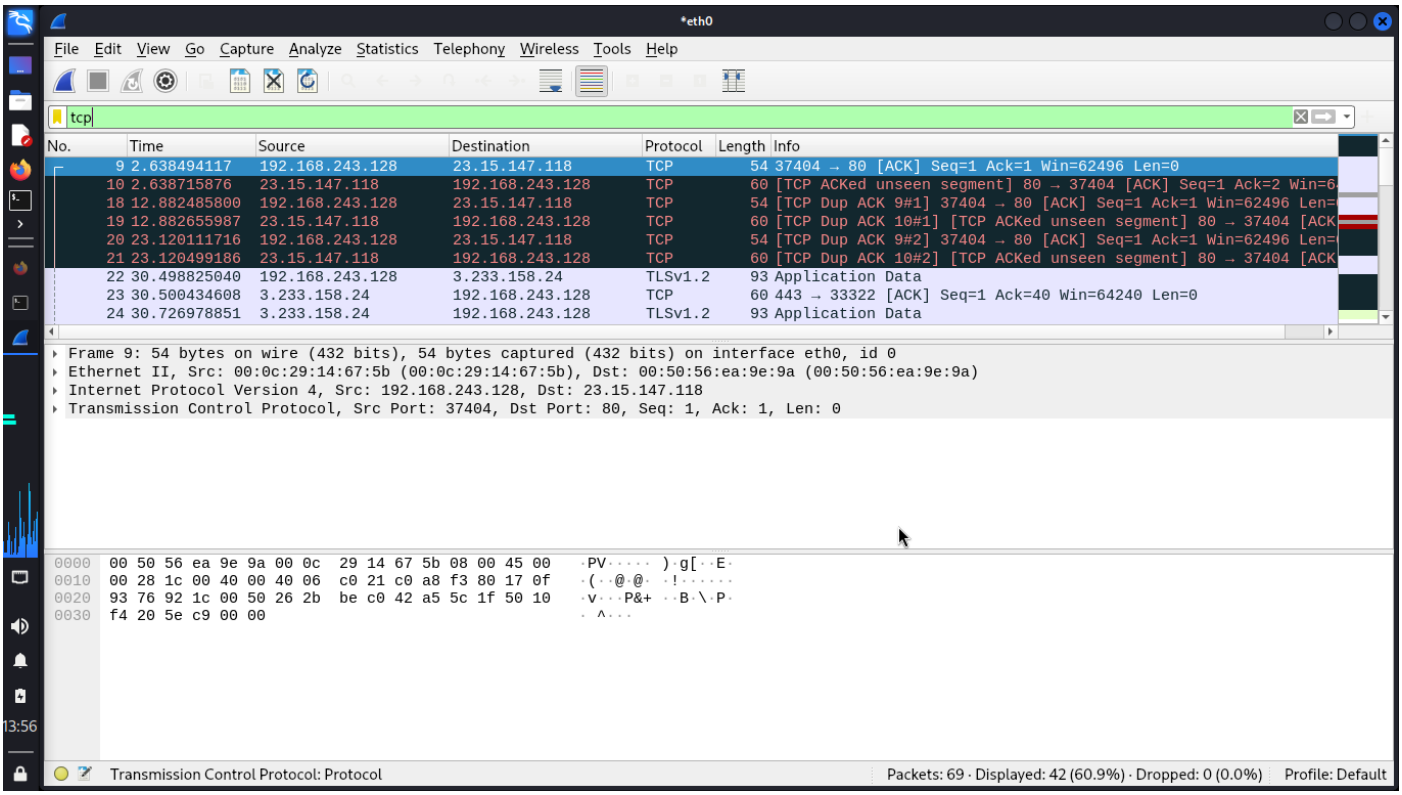

Figure 58 Filter TCP in Wireshark

Save the Tcpdump.pcap file

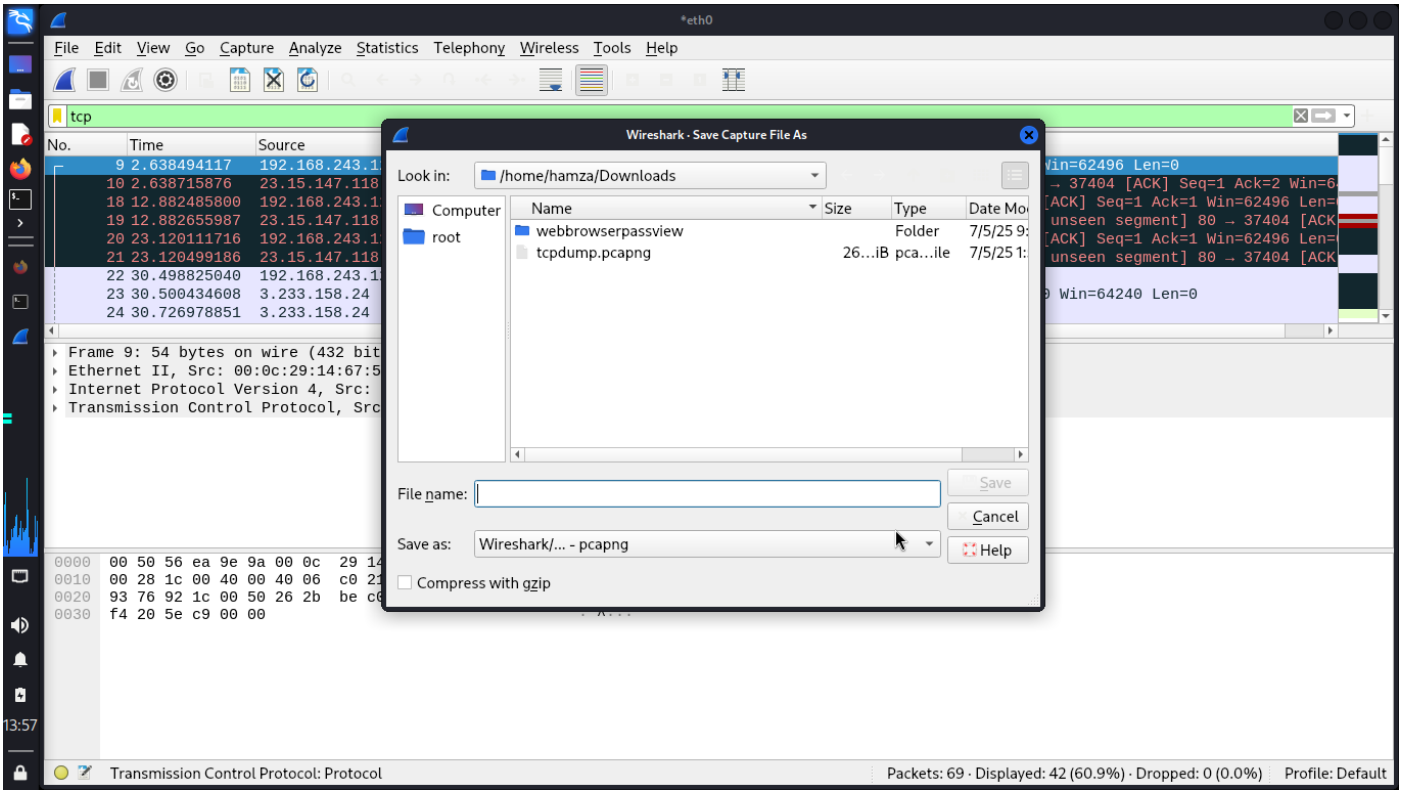

Figure 59 save the tecpdump.pcap file

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

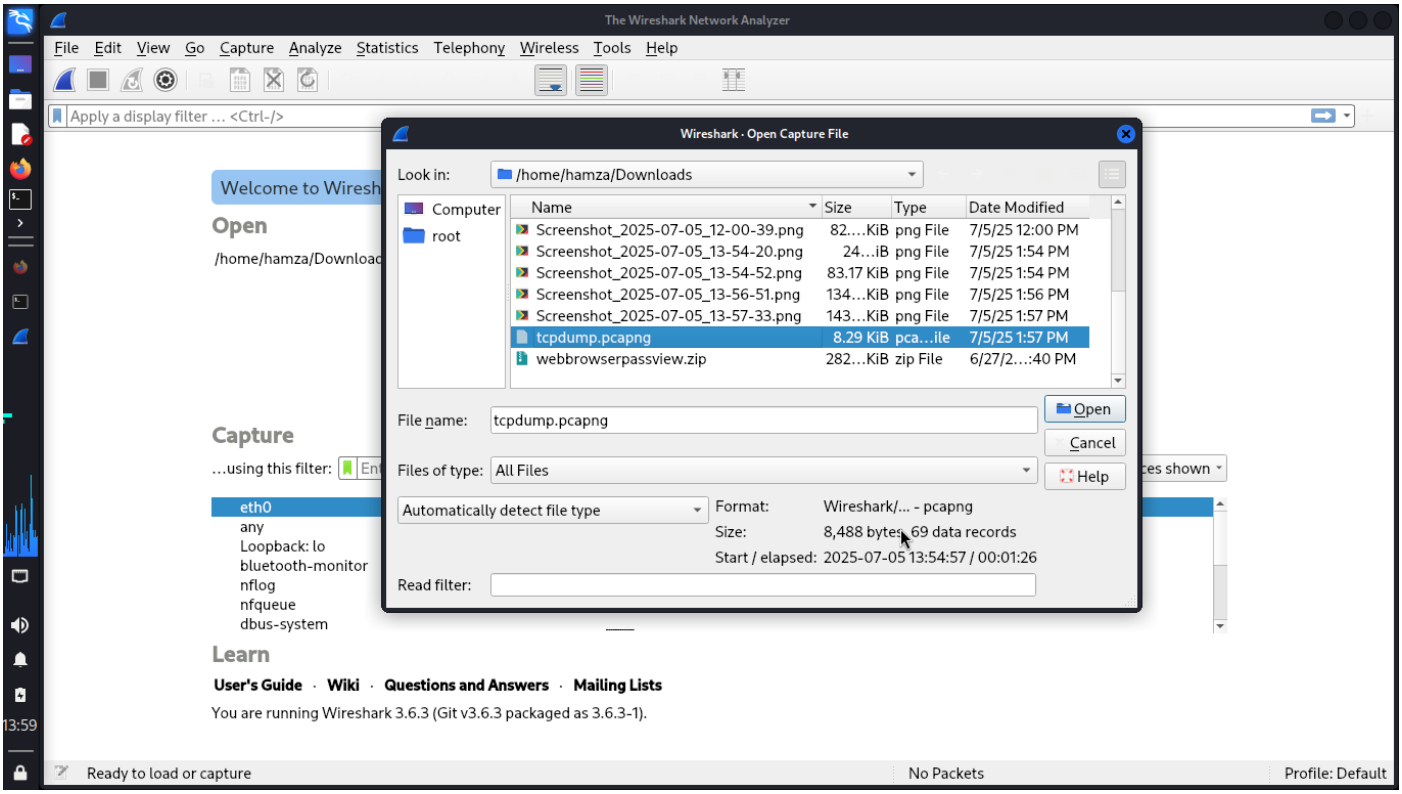

Figure 60 open file (tcpdump.pcap)

Click on Statistics tab and then click on Protocol Hierarchy

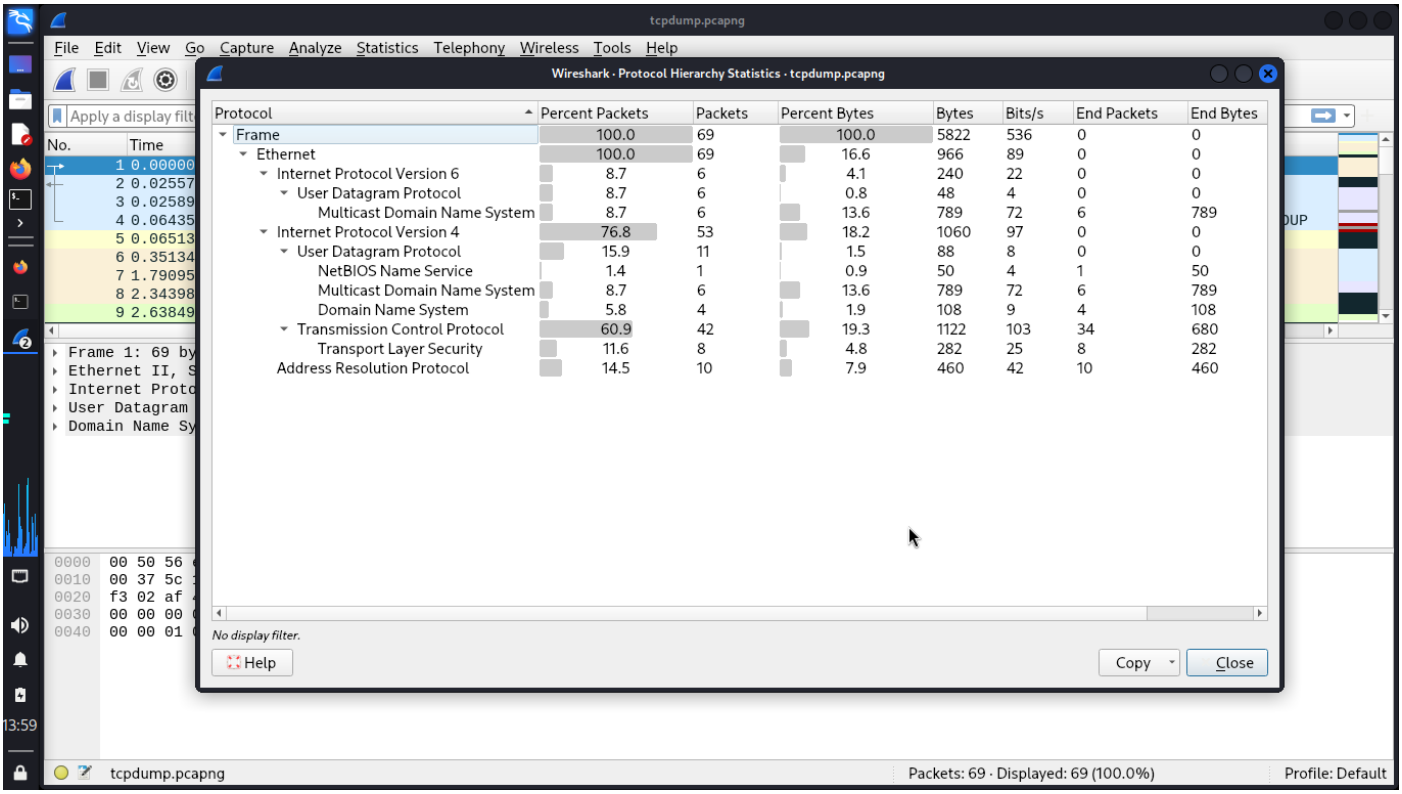

Figure 61 Protocol Hierarchy

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

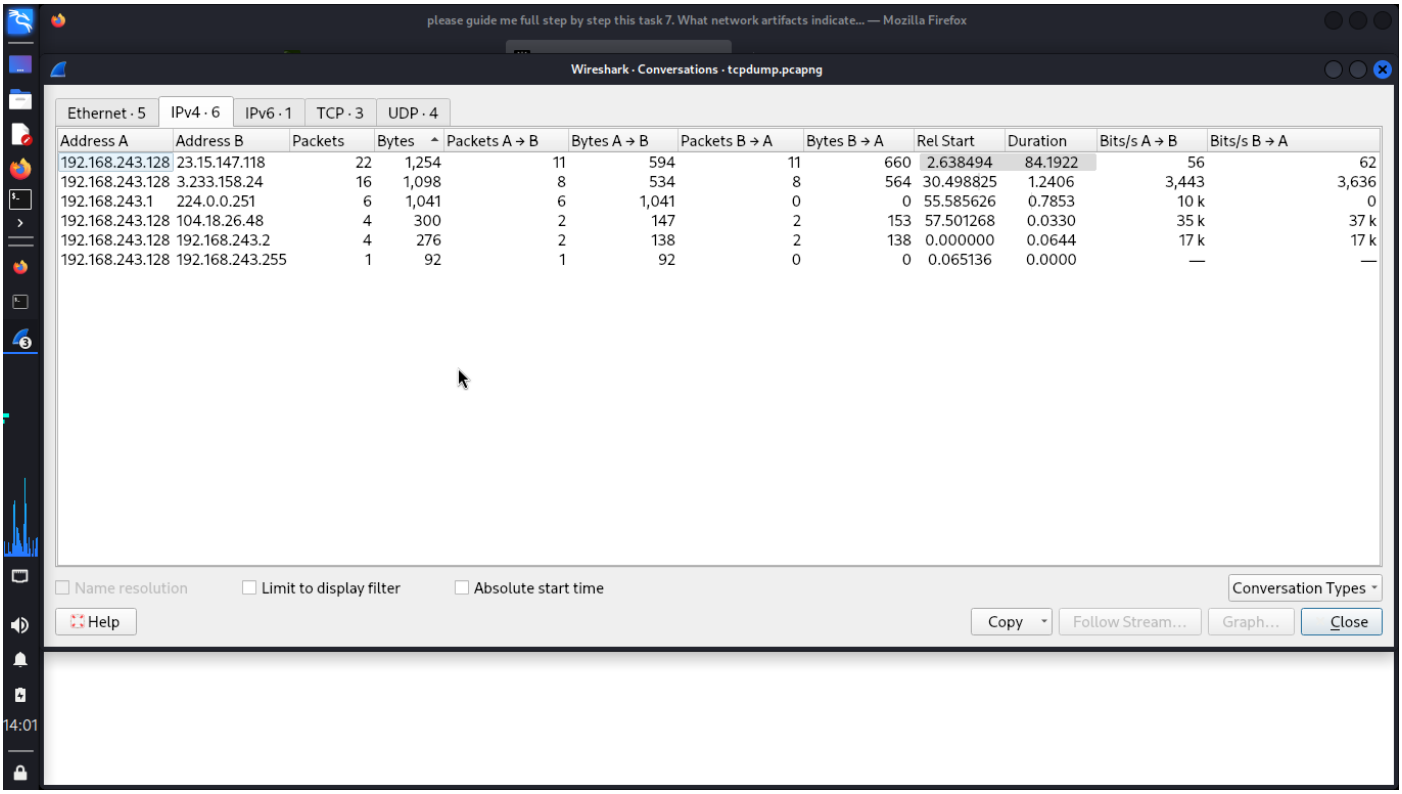

Figure 62 IP4-6 and Sort by Bytes

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

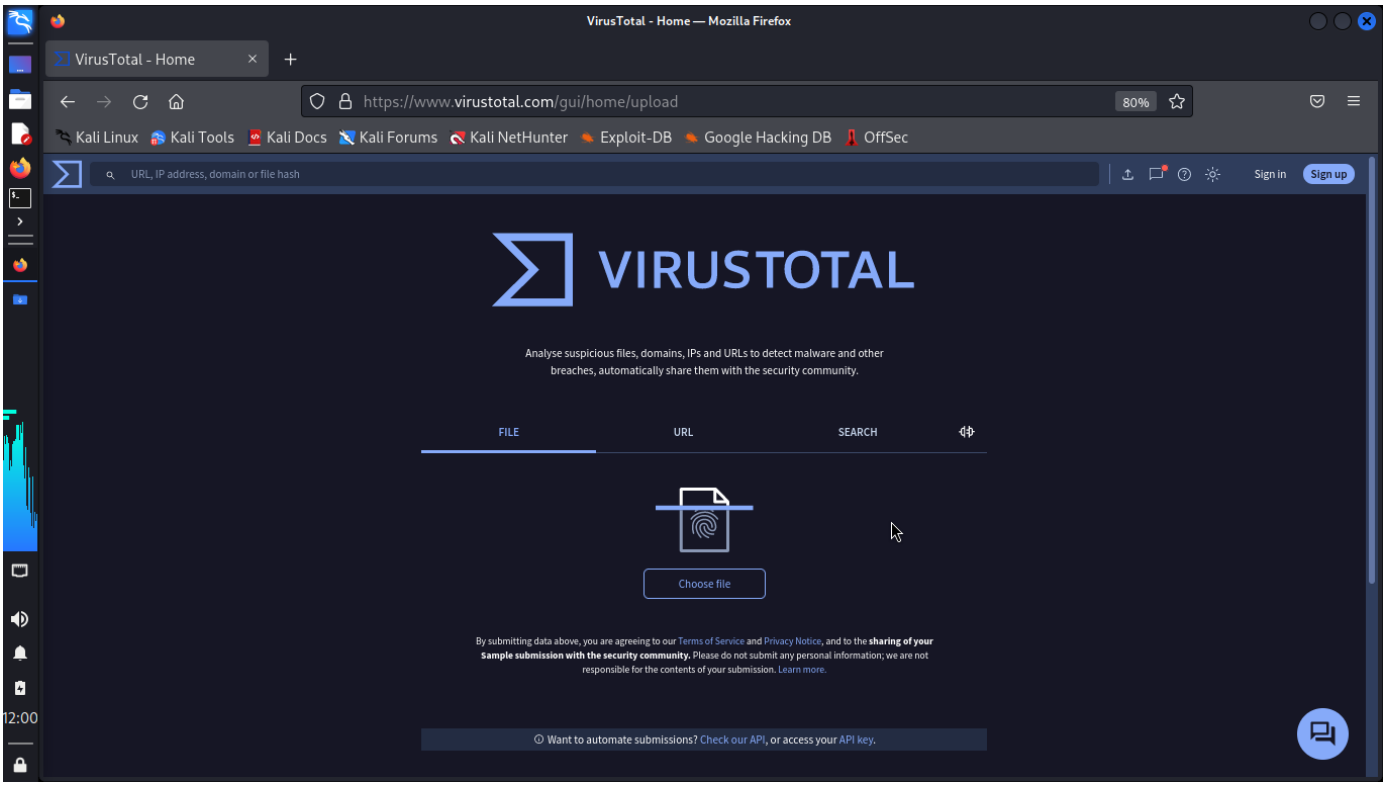

Figure 63 Virus Total

Upload a Malware (.exe) file

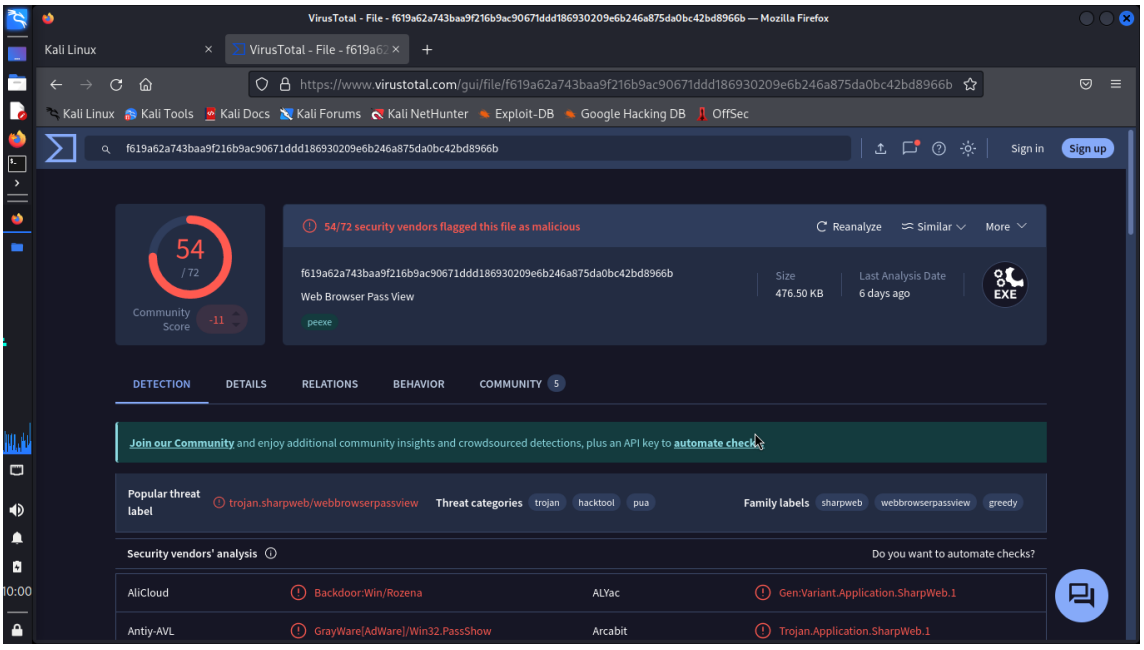

Figure 64upload a (.exe) file

Hashes (.exe) file and Other Details

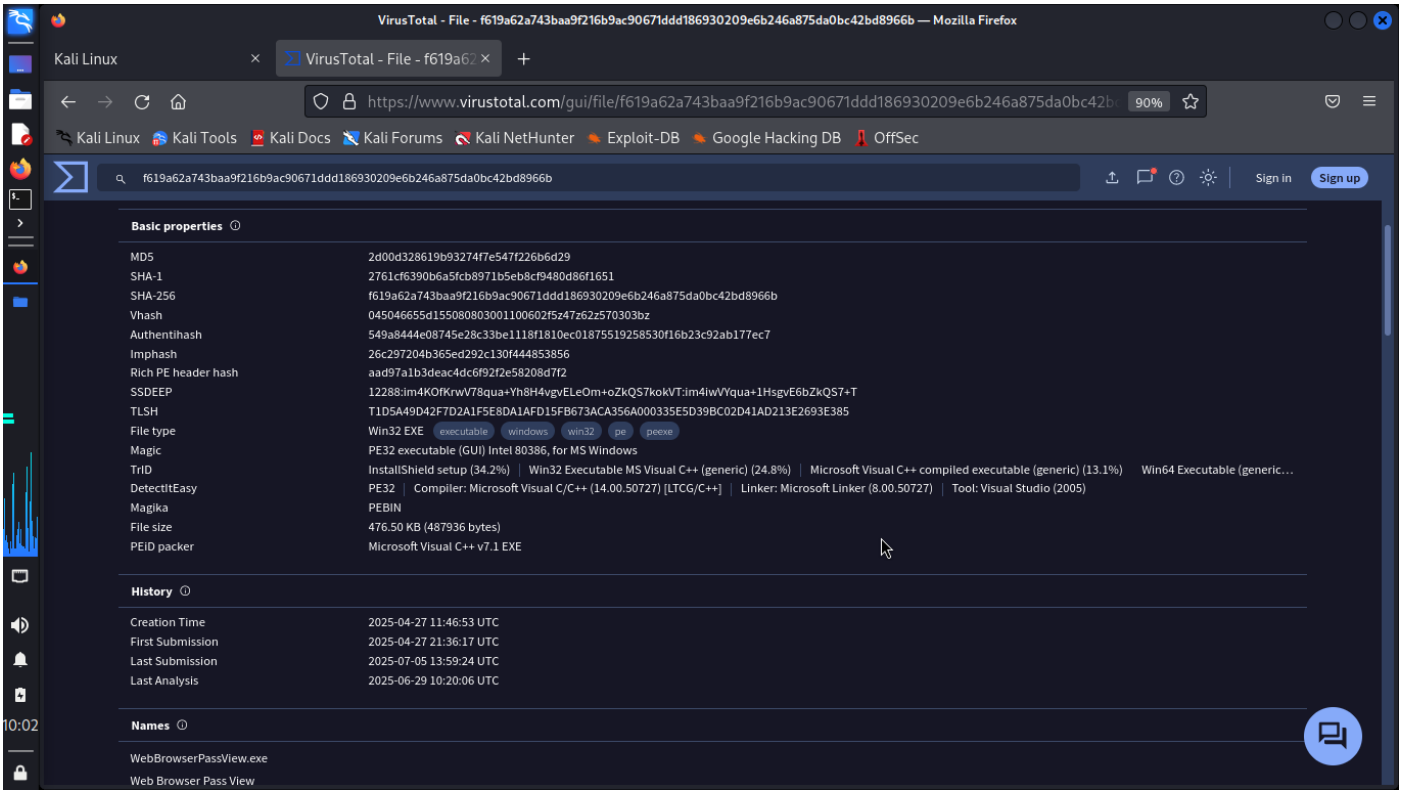

Figure 65 Hashes and Other Details (.exe) file

Created and IP Address Details

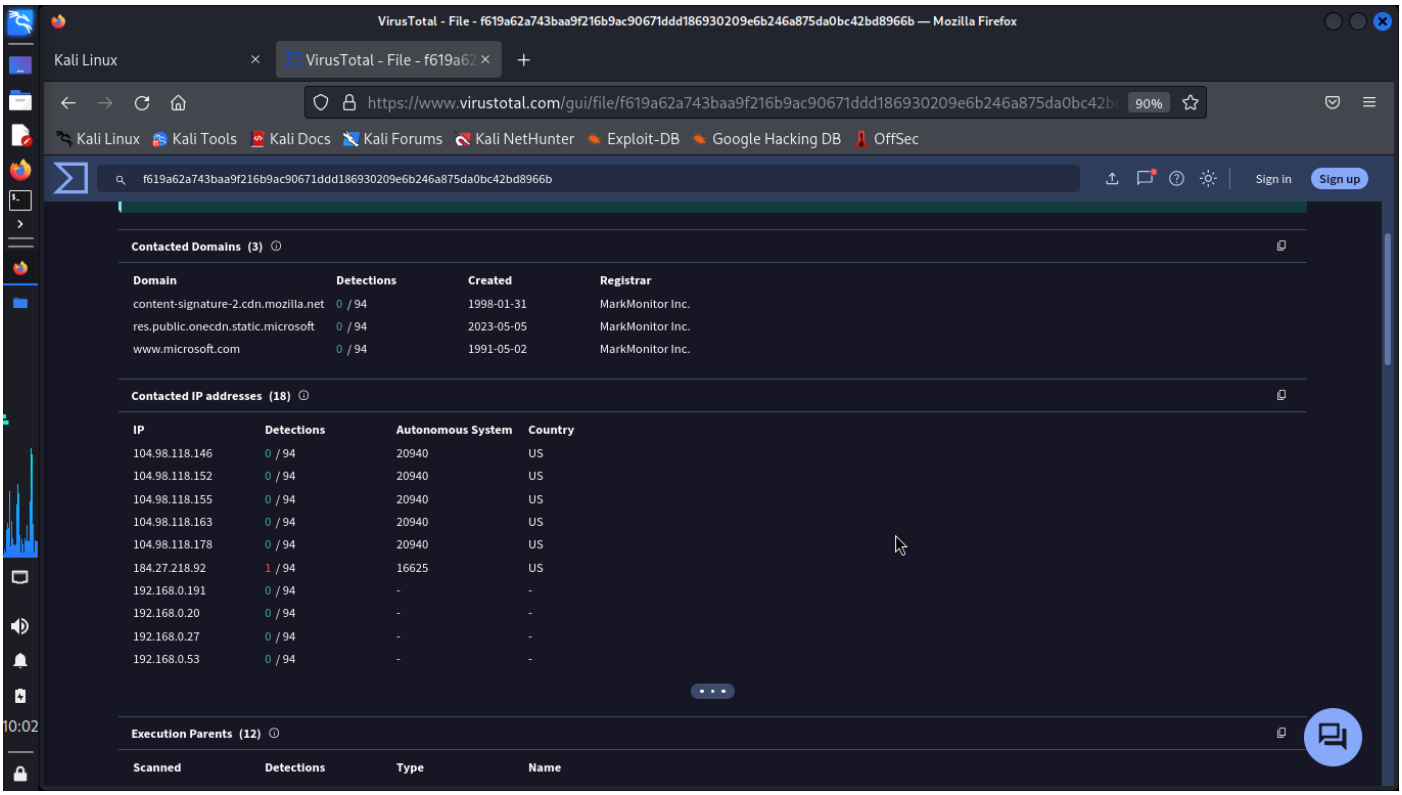

Figure 66 Created and IPs Details

Malware Detection Details

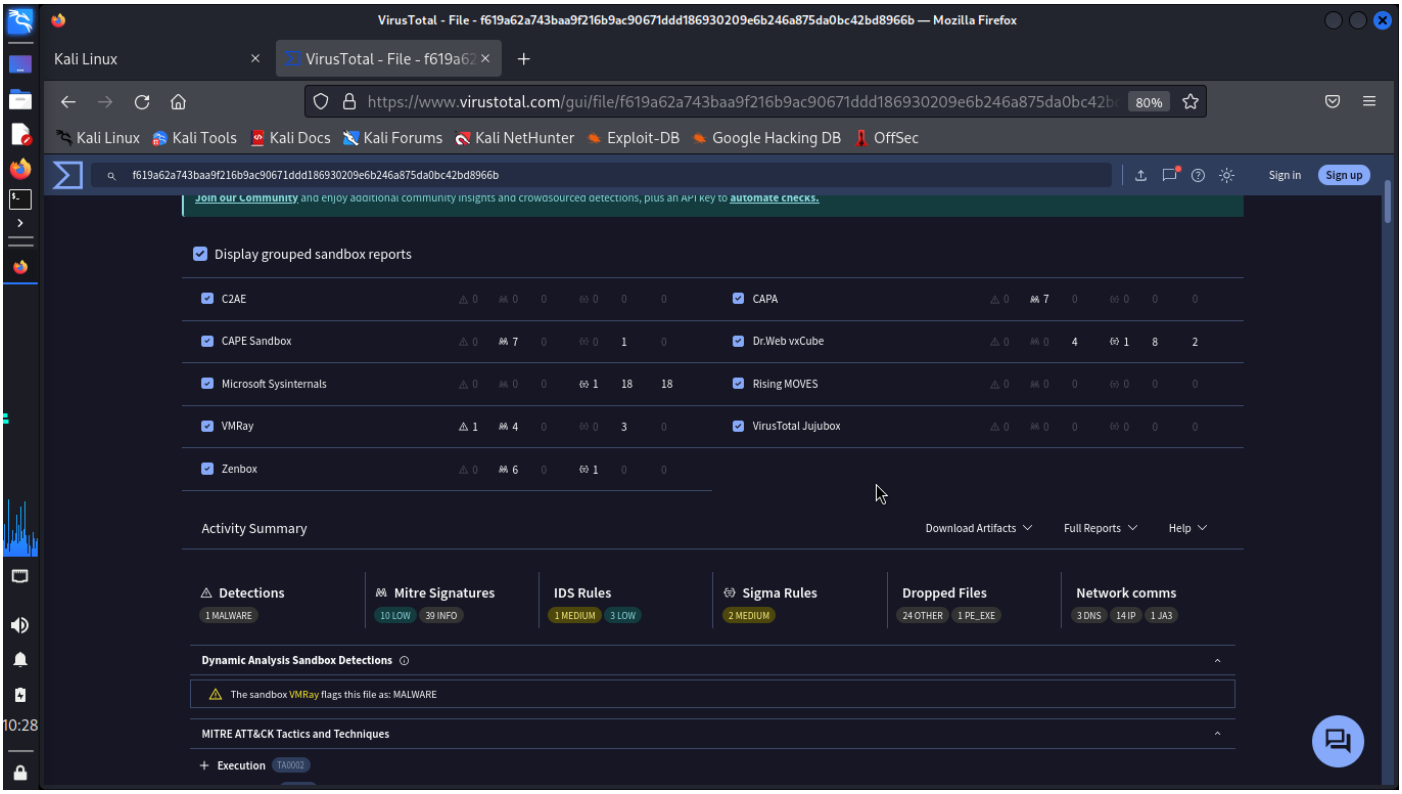

Figure 67 Malware Detection Details

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.