**Finding the digital evidences for planning for mass shooting using Disk Forensics**

**Digital forensics (Disk forensics)**

**CDAC, Noida**

**CYBER GYAN VIRTUAL INTERNSHIP PROGRAM**

**Submitted By:**

Soumyasish Sarkar

Project Trainee, (May-June) 2025

**BONAFIDE CERTIFICATE**

This is to certify that this project report entitled “Finding the digital evidences for planning for mass shooting using Disk Forensics” submitted to CDAC Noida, is a Bonafede record of work done by Soumyasish Sarkar under my supervision from 19th May 2025 to 29th June 2025

**Declaration by Author(s)**

This is to declare that this report has been written by me. No part of the report is plagiarized from other sources. All information included from other sources have been duly acknowledged. I aver that if any part of the report is found to be plagiarized, I shall take full responsibility for it.

Name of Author: Soumyasish Sarkar

**TABLE OF CONTENTS**

1. Introduction .......................................................... 1

2. Problem Statement ............................................... 1

3. Learning Objective ................................................. 1

4. Approach ............................................................... 1

5. Implementation ….................................................. 2

5.1 FTK Imager Analysis ............................................. 2

5.2 Autopsy Analysis…................................................ 5

5.3 Volatility Memory Forensics................................ 13

6. Attack Timeline.….................................................. 16

7. Conclusion and Recommendations ....................... 17

8. Project Link………..…................................................ 17

9. List of References …................................................ 17

**ACKNOWLEDGEMENT**

I would like to extend my deepest gratitude to my internship mentors and project guide for their constant support and technical guidance during this internship project. This project allowed me to gain hands-on experience with real-world disk forensics investigation, and I learned how to work with forensic image formats, disk analysis tools, and memory forensics frameworks. I am also thankful to CDAC and the training coordinators for providing a simulated environment and curated datasets like the 2018 Lone Wolf scenario to perform practical digital investigations.

Sincerely,

Soumyasish Sarkar

**1 INTRODUCTION**

**Finding the digital evidences for planning for mass shooting using Disk Forensics**

**2.** **PROBLEM STATEMENT**

The project aimed to simulate a real-world disk forensic investigation using the 2018 Lone Wolf scenario. A fictional suspect’s disk and memory images were examined using FTK Imager, Autopsy, and Volatility to uncover evidence of a planned mass shooting. Digital artifacts such as planning documents, escape logistics, and ideological motivations were recovered from disk partitions and memory snapshots. This exercise emphasized the role of disk forensics in identifying, extracting, and documenting digital evidence to support criminal investigations.

**3. LEARNING OBJECTIVE**

* Gained practical experience in loading and navigating .E01 forensic disk images using FTK Imager.
* Understood the structure of a Windows file system and recovered files from different partitions.
* Performed keyword searches and timeline analysis using Autopsy to locate hidden or deleted files.
* Analyzed volatile memory using Volatility to uncover running processes, browser activity, and in-memory strings.
* Developed skills in compiling forensic reports with step-by-step documentation and evidence-based findings.

**4. APPROACH**

**Tools and Technologies Used:**

**FTK Imager**: Used to load and preview the LoneWolf.E01 disk image and export discovered documents.

**Autopsy**: Used to ingest the disk image, perform keyword searches, recover deleted files, and analyze recent activity.

**Volatility**: Employed for memory analysis on memdump.mem to find running processes, unsaved documents, and browser traces.

**Infrastructure Setup:**

**Platform**: Windows 11 (Host OS)

**RAM**: 16 GB | **Disk**: 512 GB SSD

**Evidence files**: LoneWolf.E01 through LoneWolf.E09 (~13.5 GB), memdump.mem (17 GB), pagefile.sys (2.9 GB)

**Network configuration**: Not applicable (disk and memory analysis was conducted offline in a controlled environment)

**5. IMPLEMENTATIONS:**

**5.1** **FTK Imager Analysis:**

The basic steps that are followed to create a new project are as follows:

First case name and location of the project has been given.

Loaded the full set of .E01 files (LoneWolf.E01 to E09) in FTK Imager.

Navigated to Basic Data Partition → Users → jcloudy.

Exported the following critical evidence files:

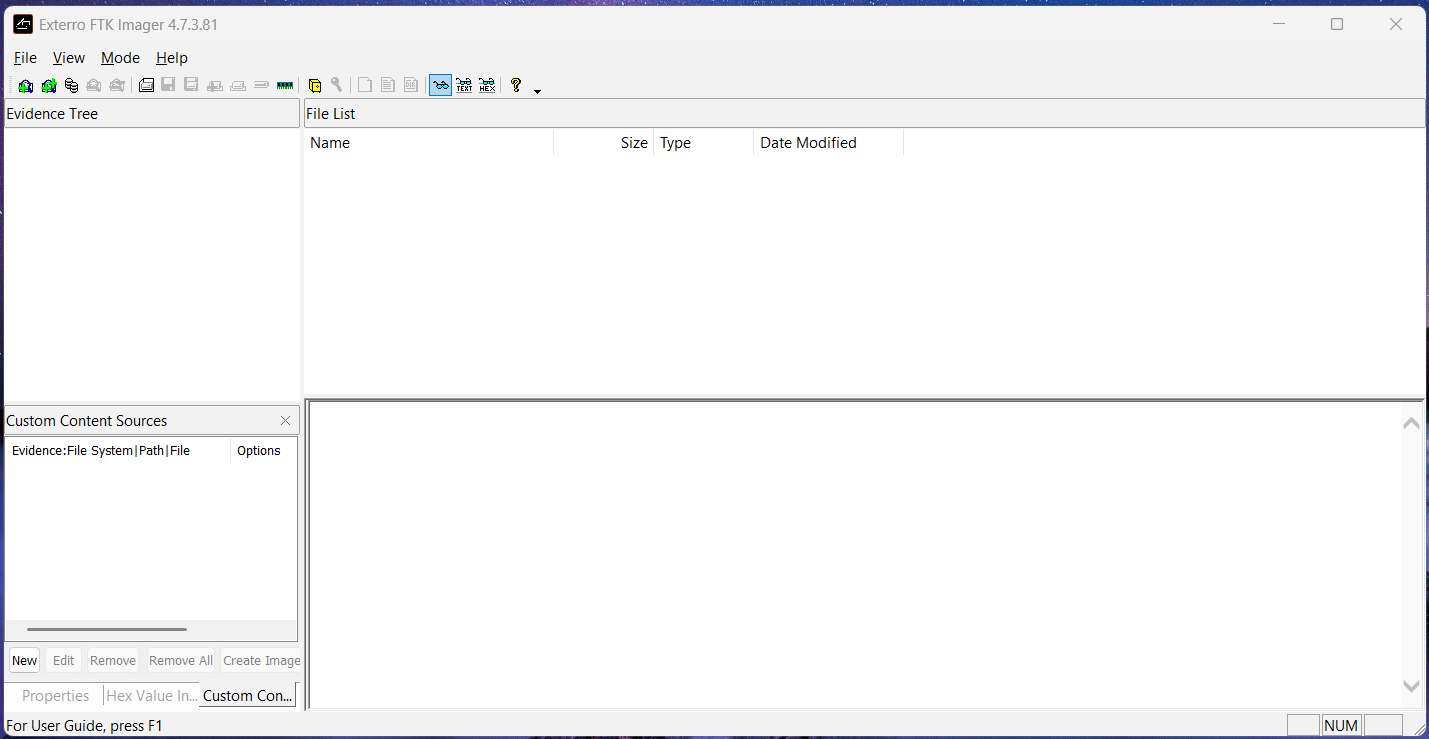
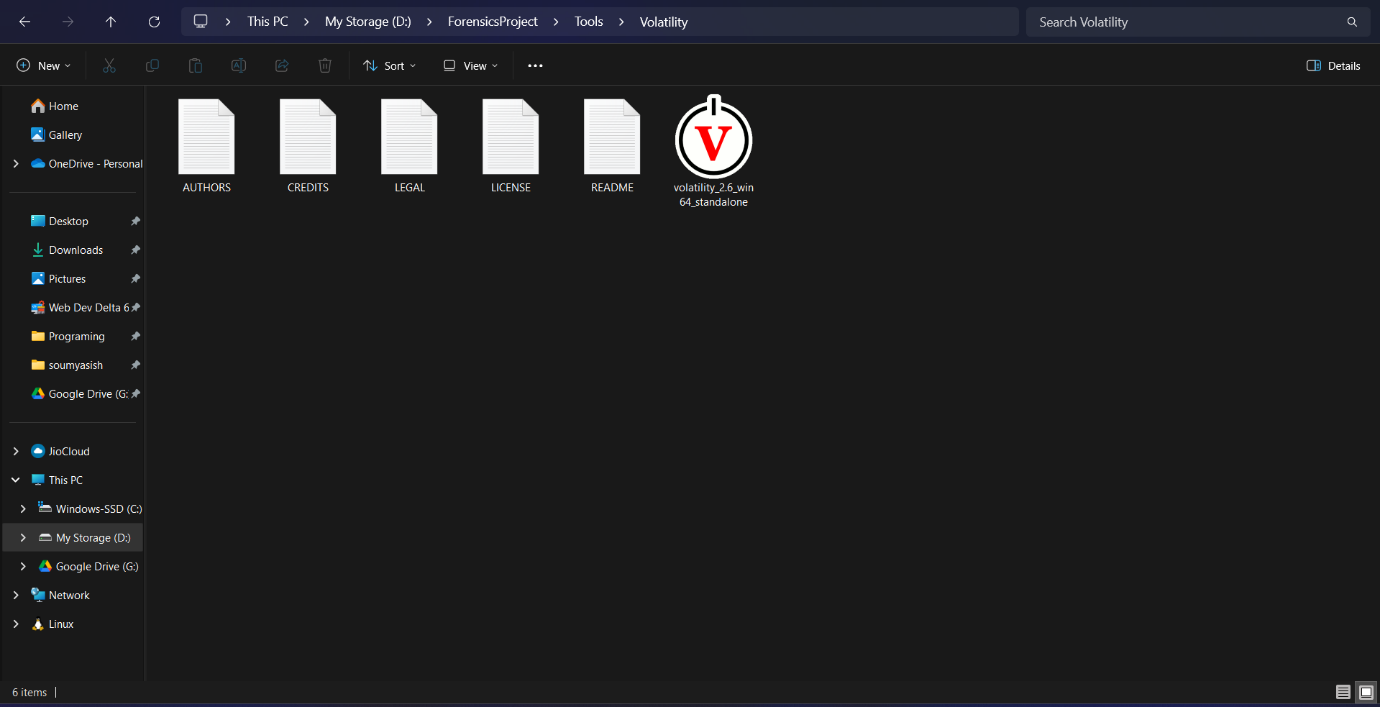
planning.docx: Lists targets, weapon details, and logistics.

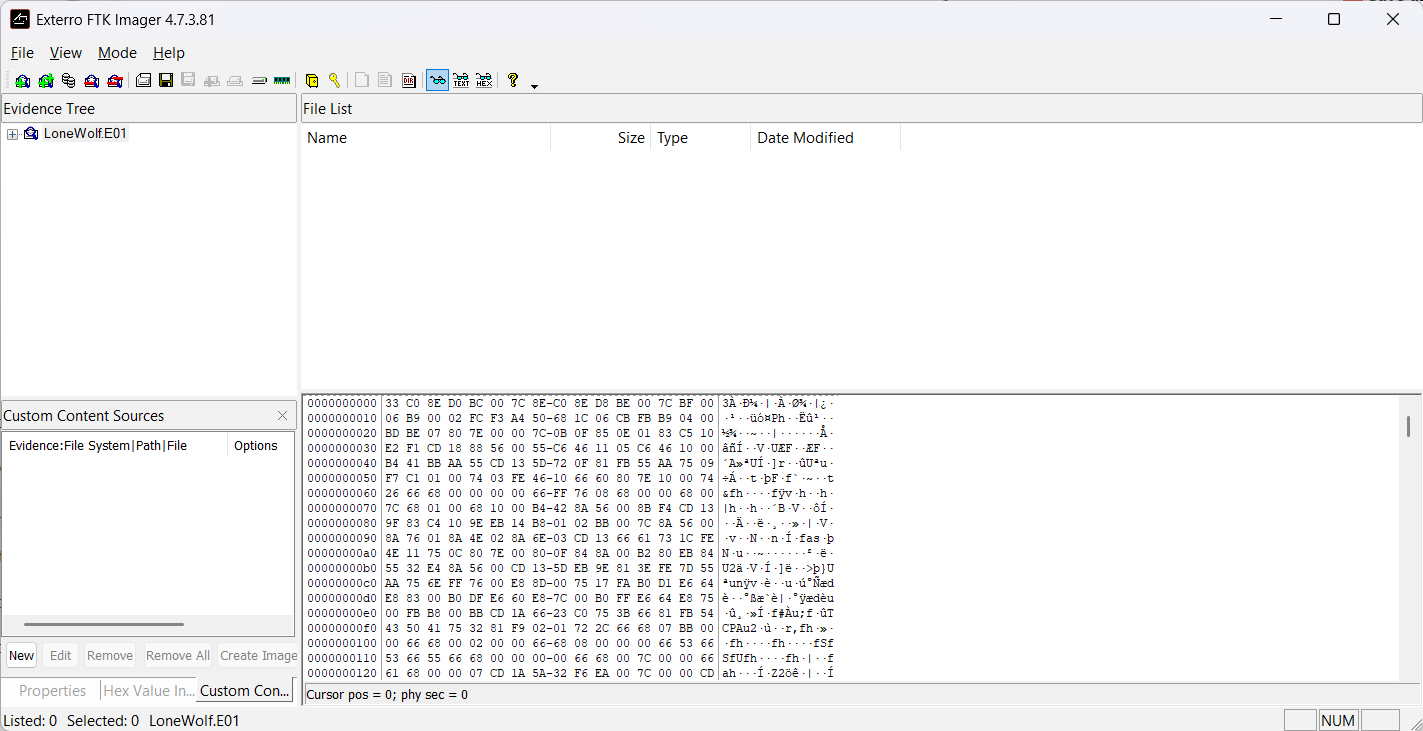
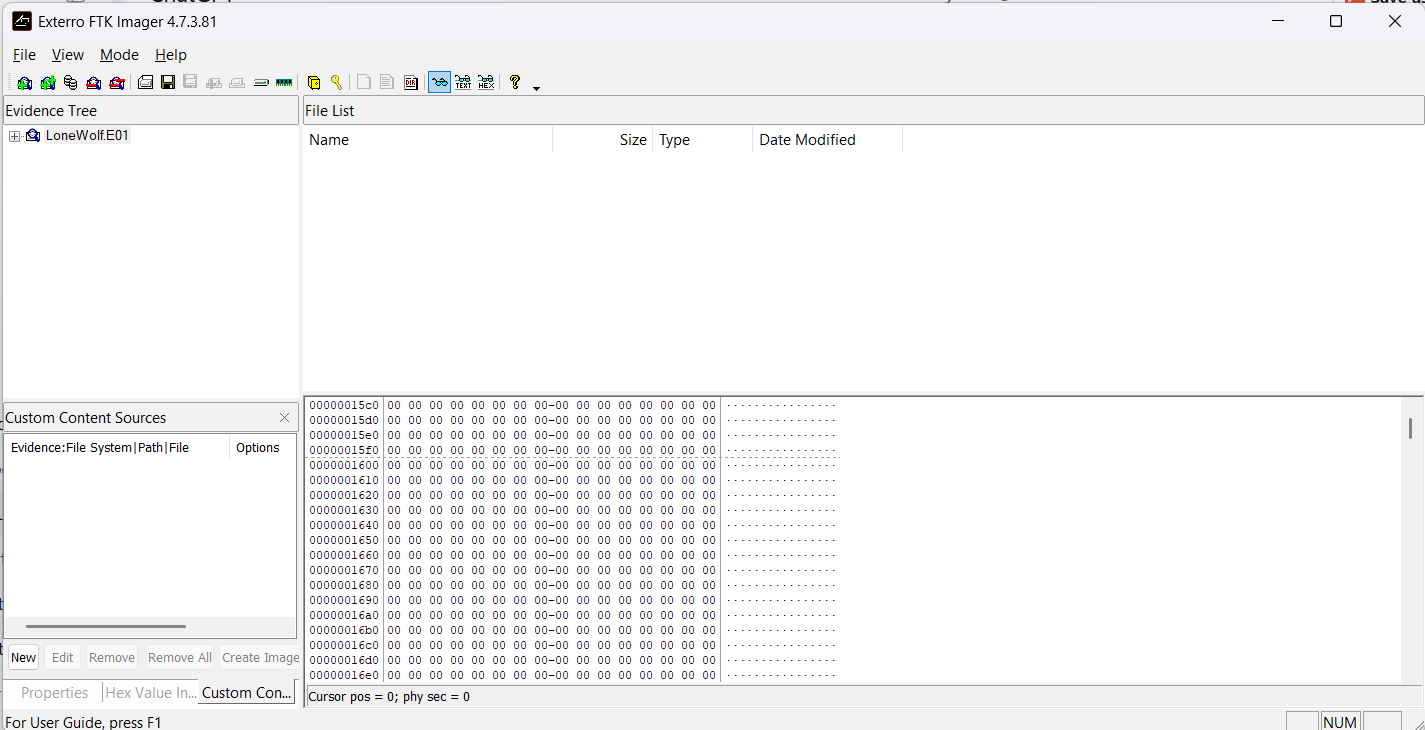
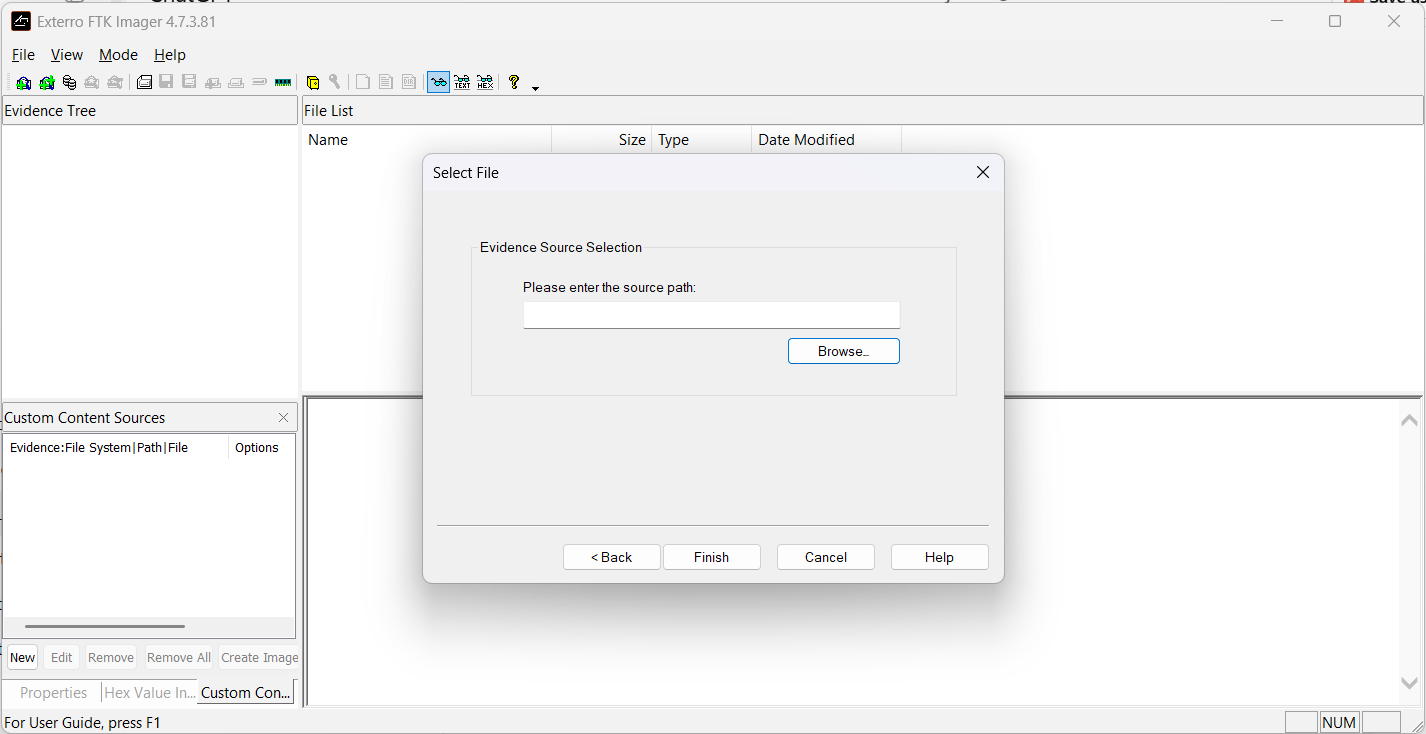
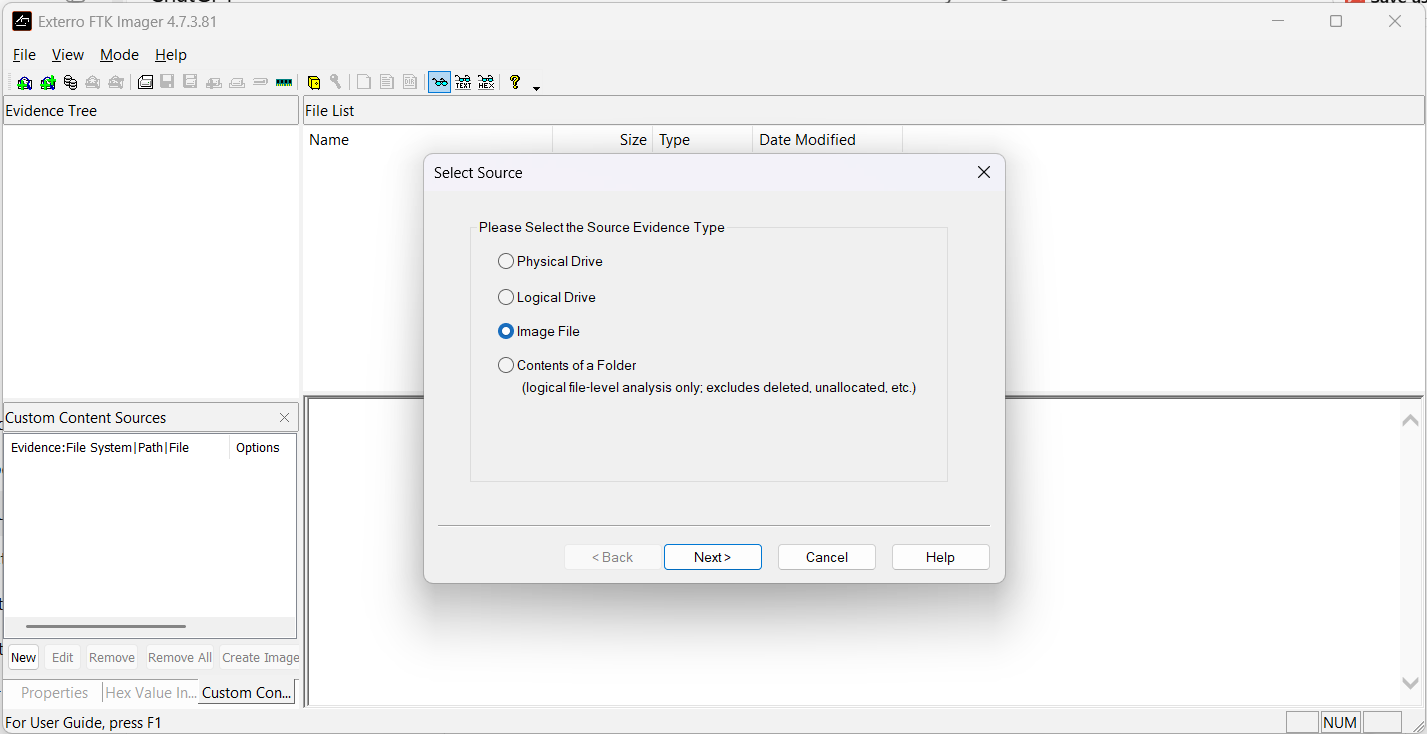
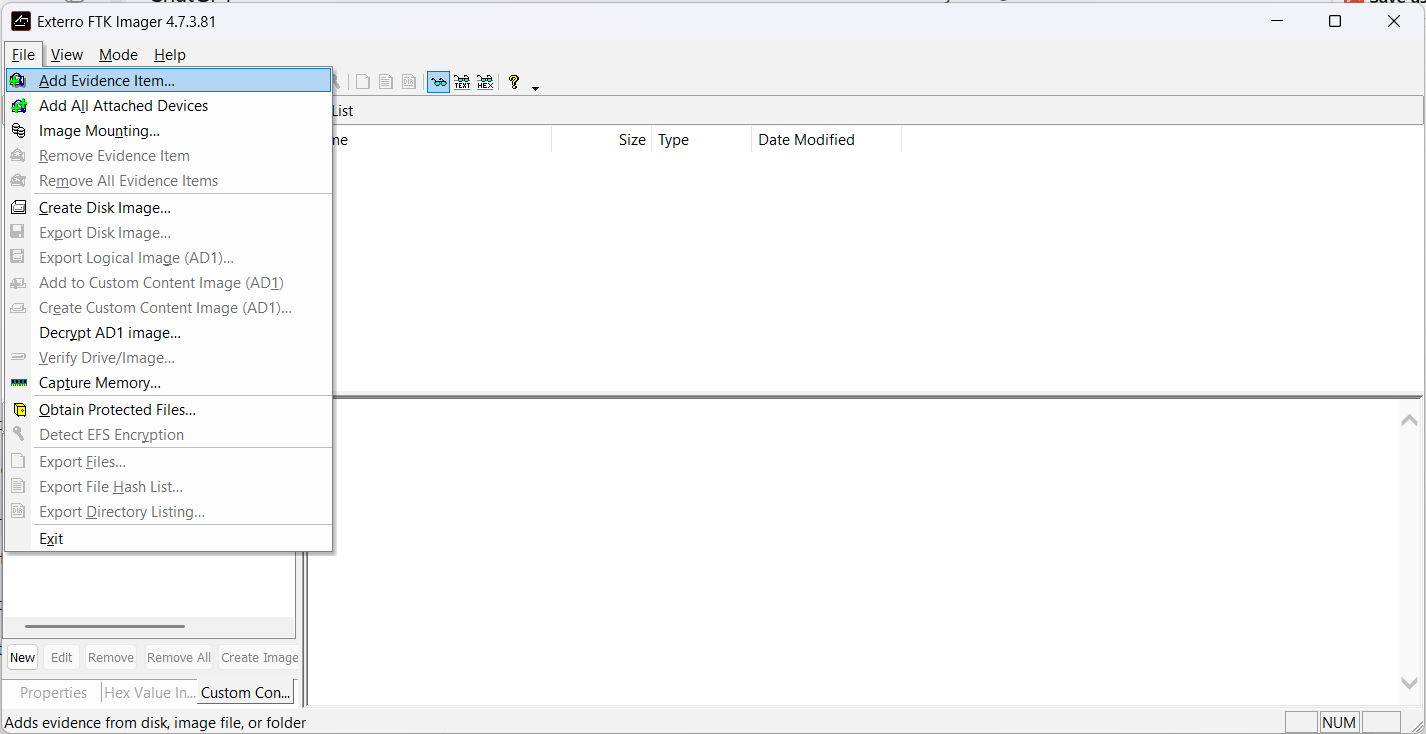
manifesto.txt: Ideological justification and threats.

airport\_escape\_notes.txt: Travel route planning post-attack.

farewell\_note.txt: Final emotional message referencing cloud backups and a contact named Paul.

Documented metadata, file paths, and took screenshots for each recovered file.





**5.2** **Autopsy Analysis:**

Created a new Autopsy case and added the .E01 disk image.

Enabled ingest modules: Recent Activity, File Type Identification, Keyword Search, Deleted File Recovery.

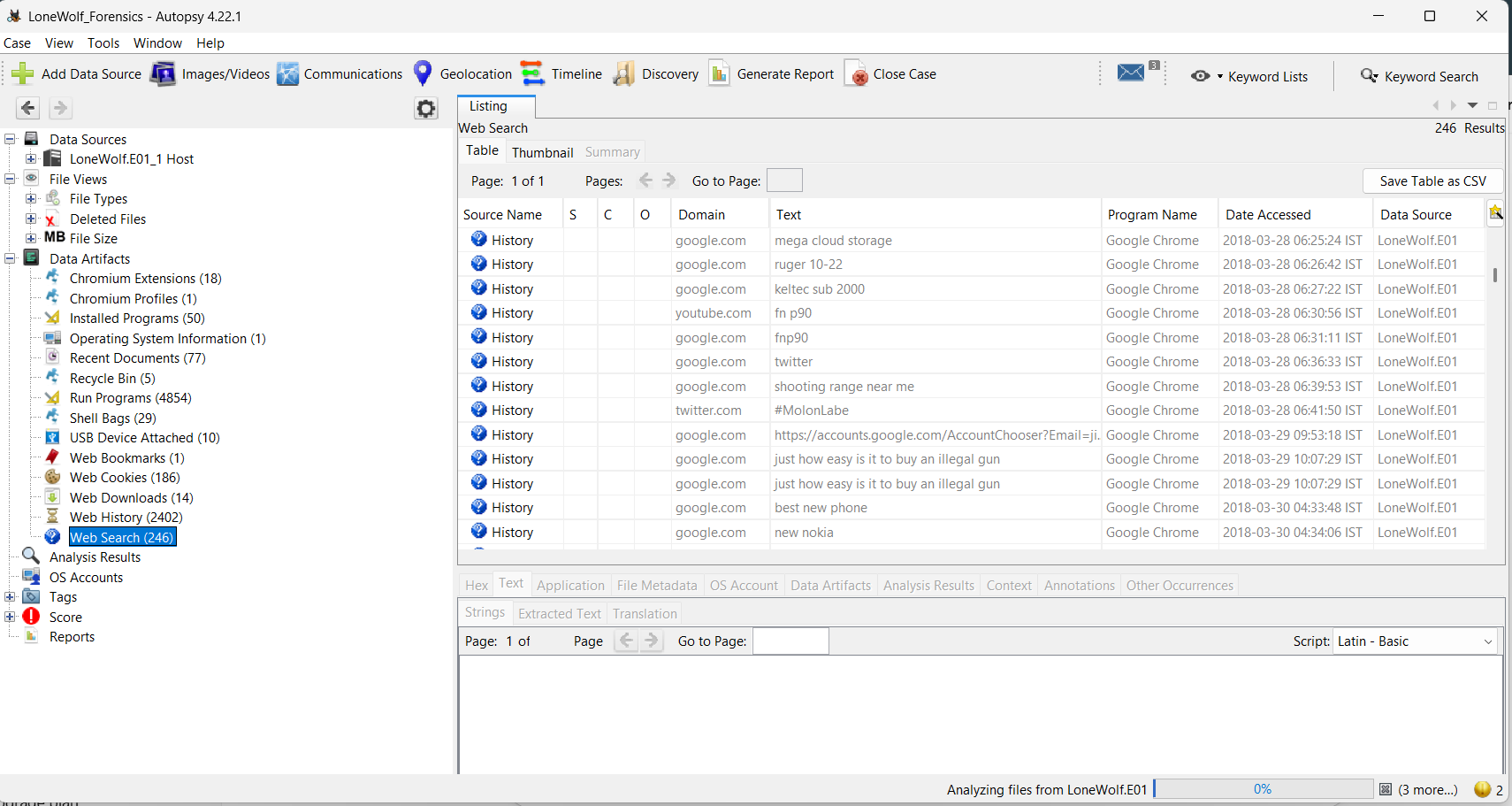
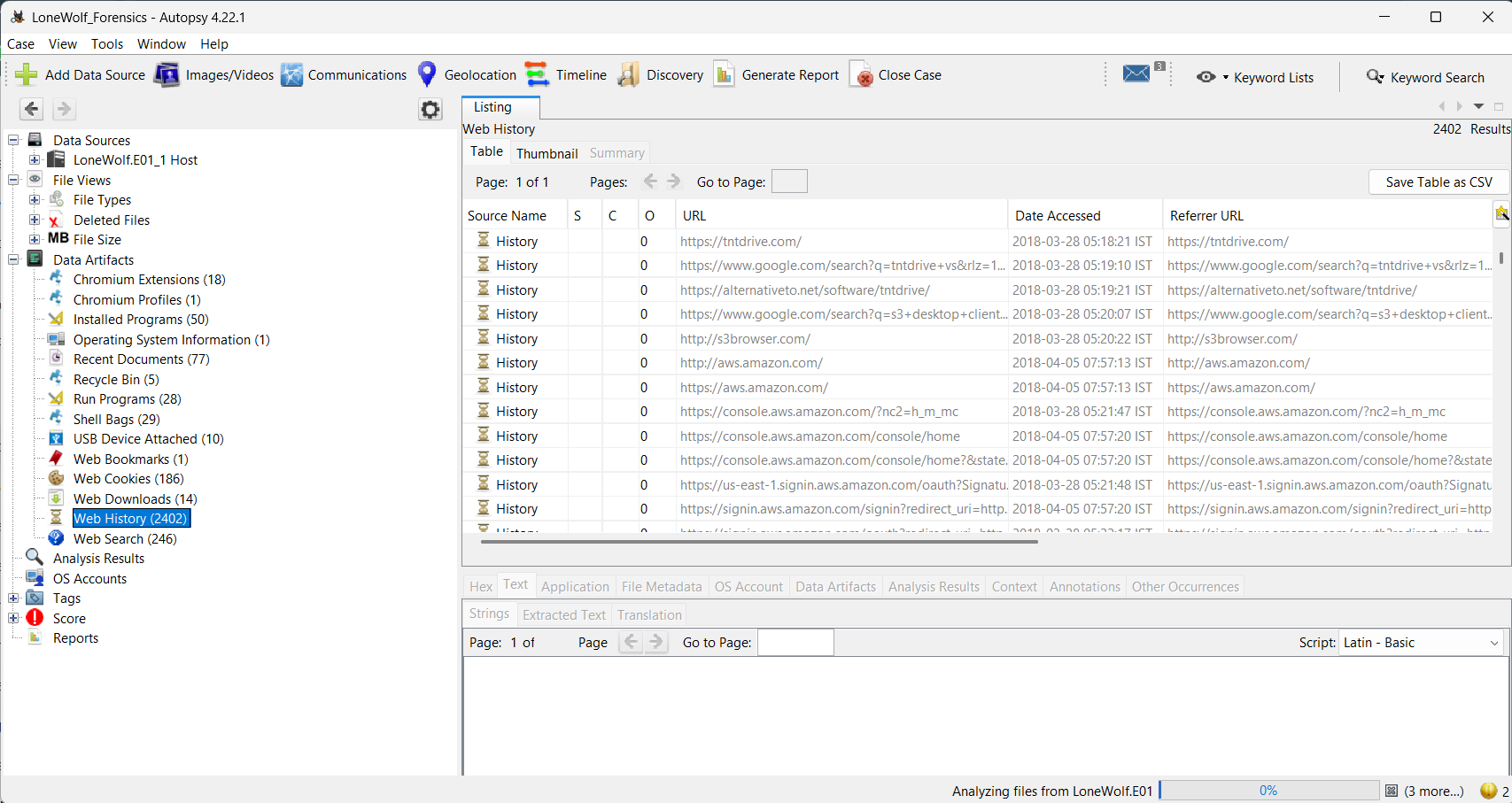
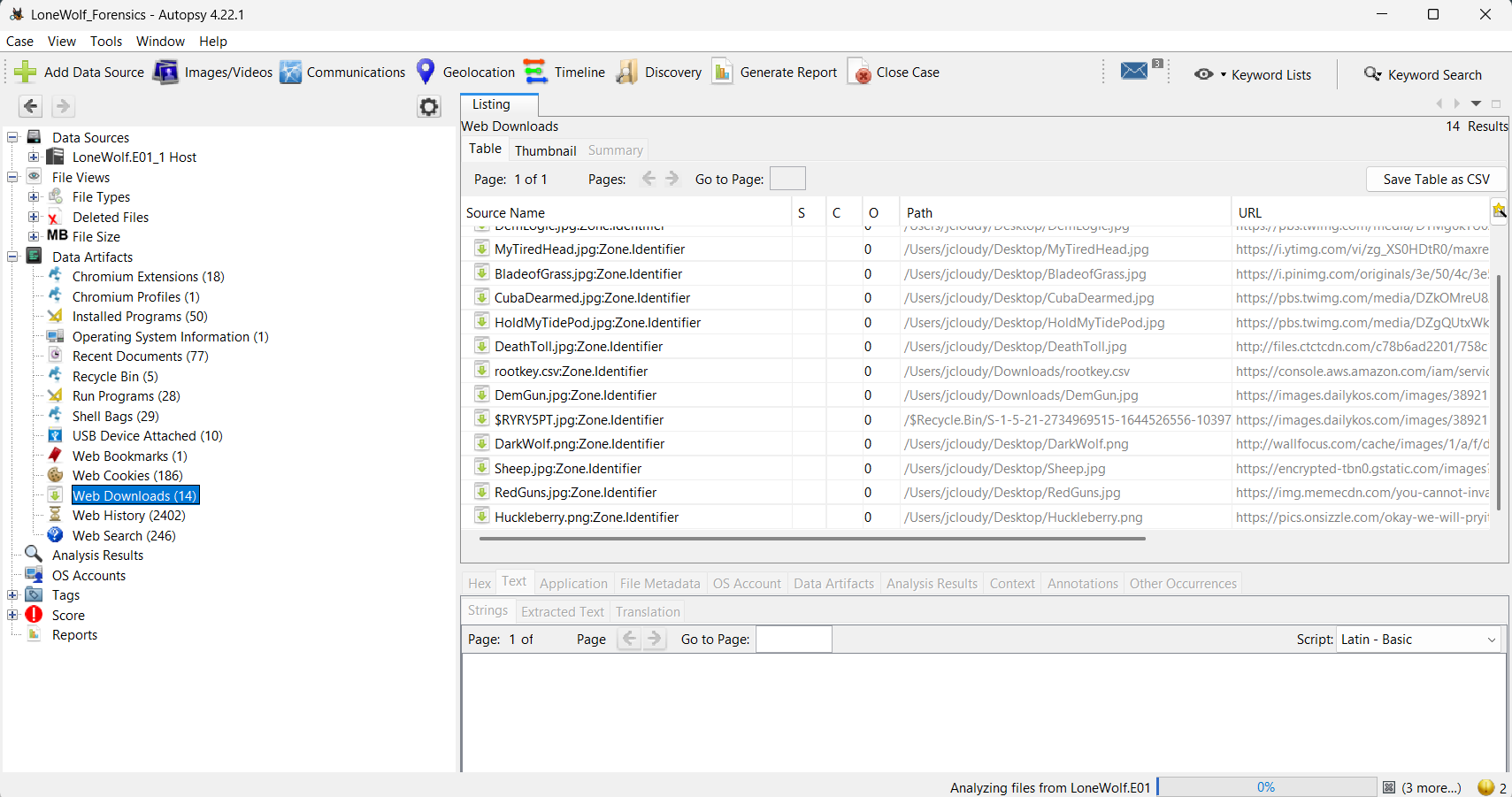
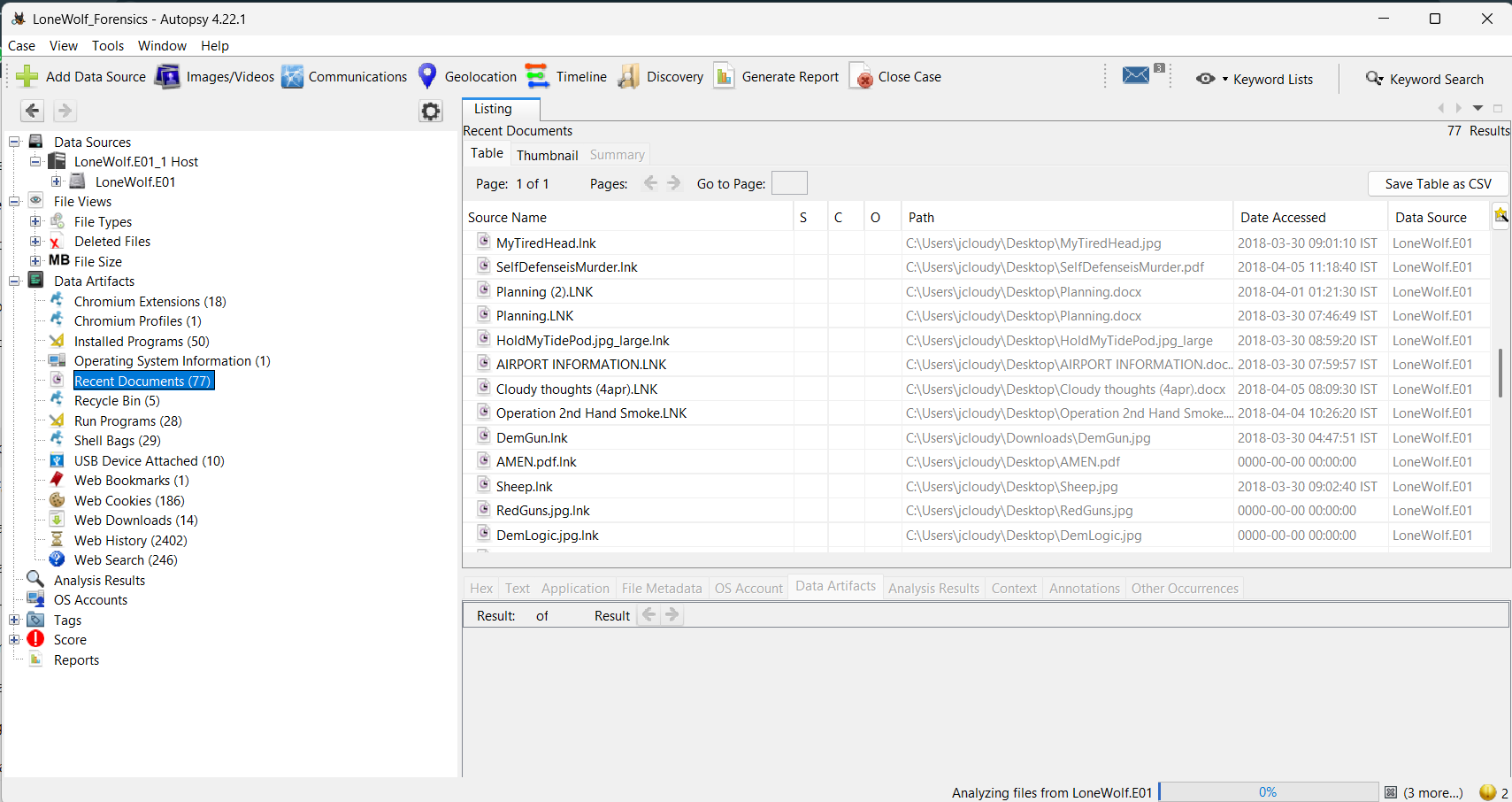
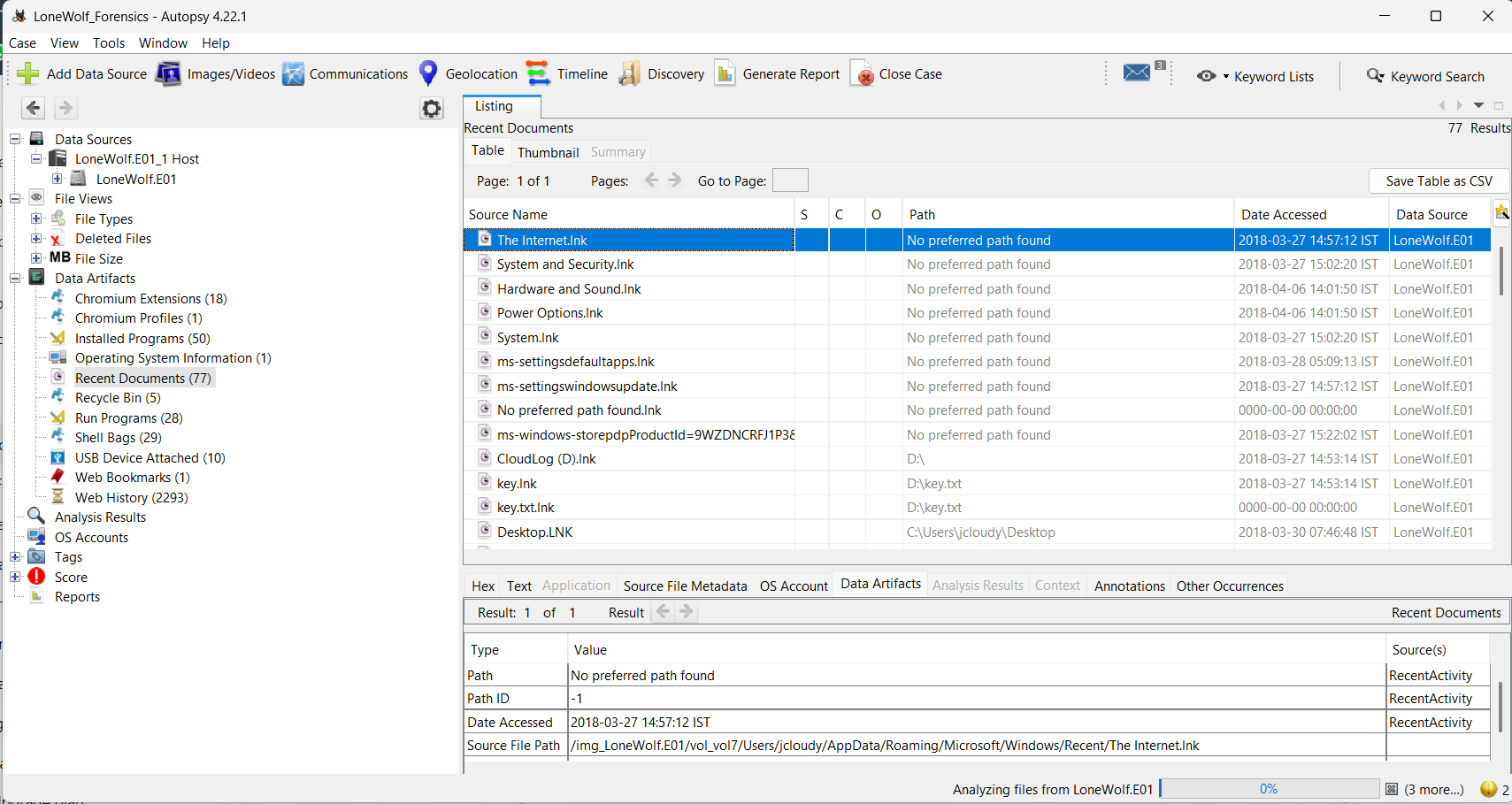
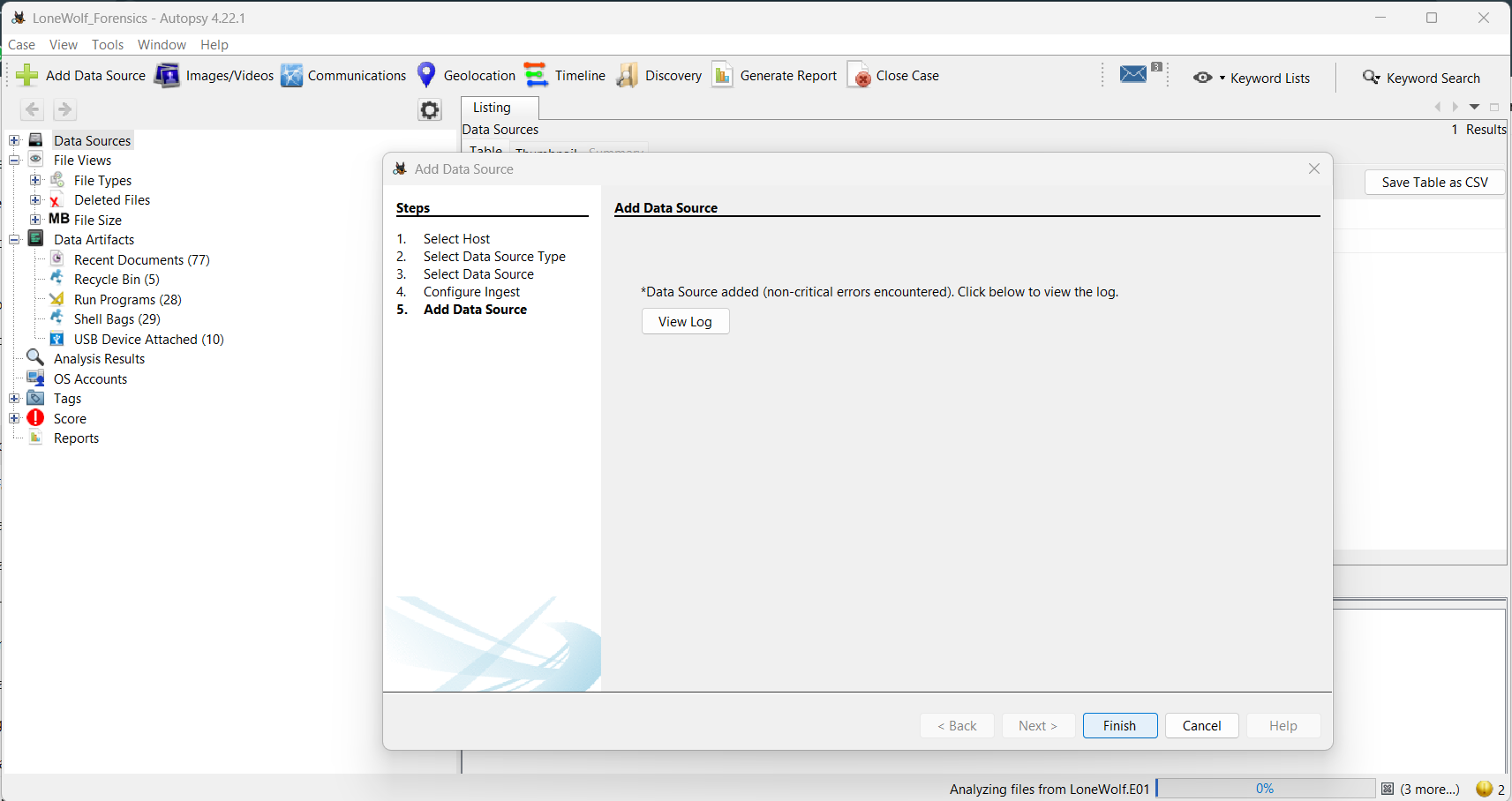
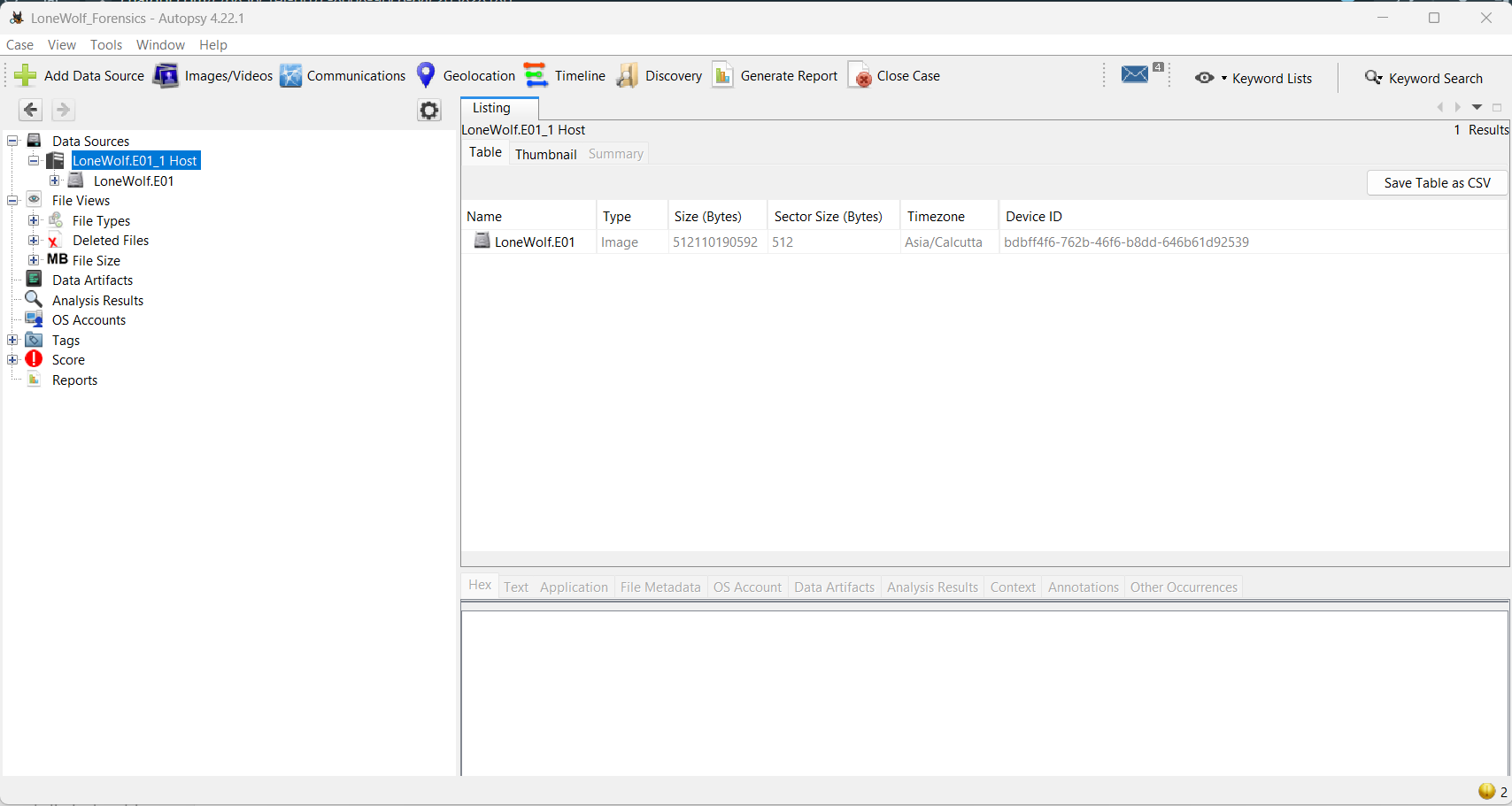
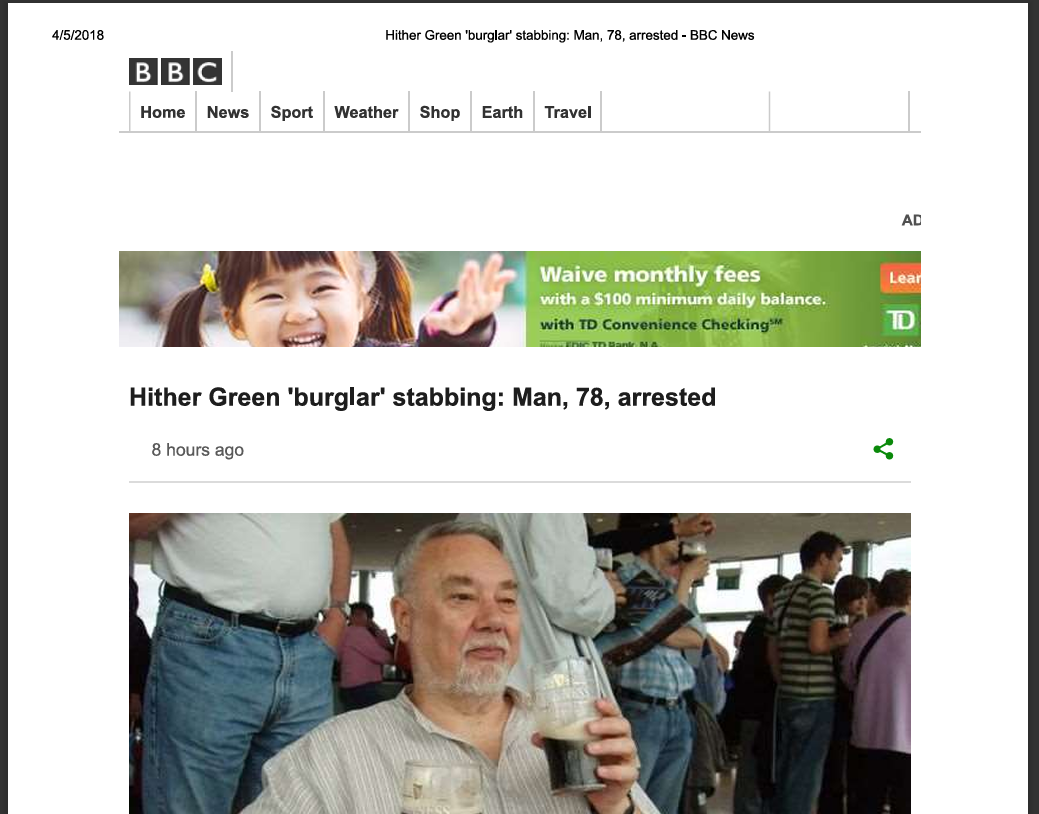
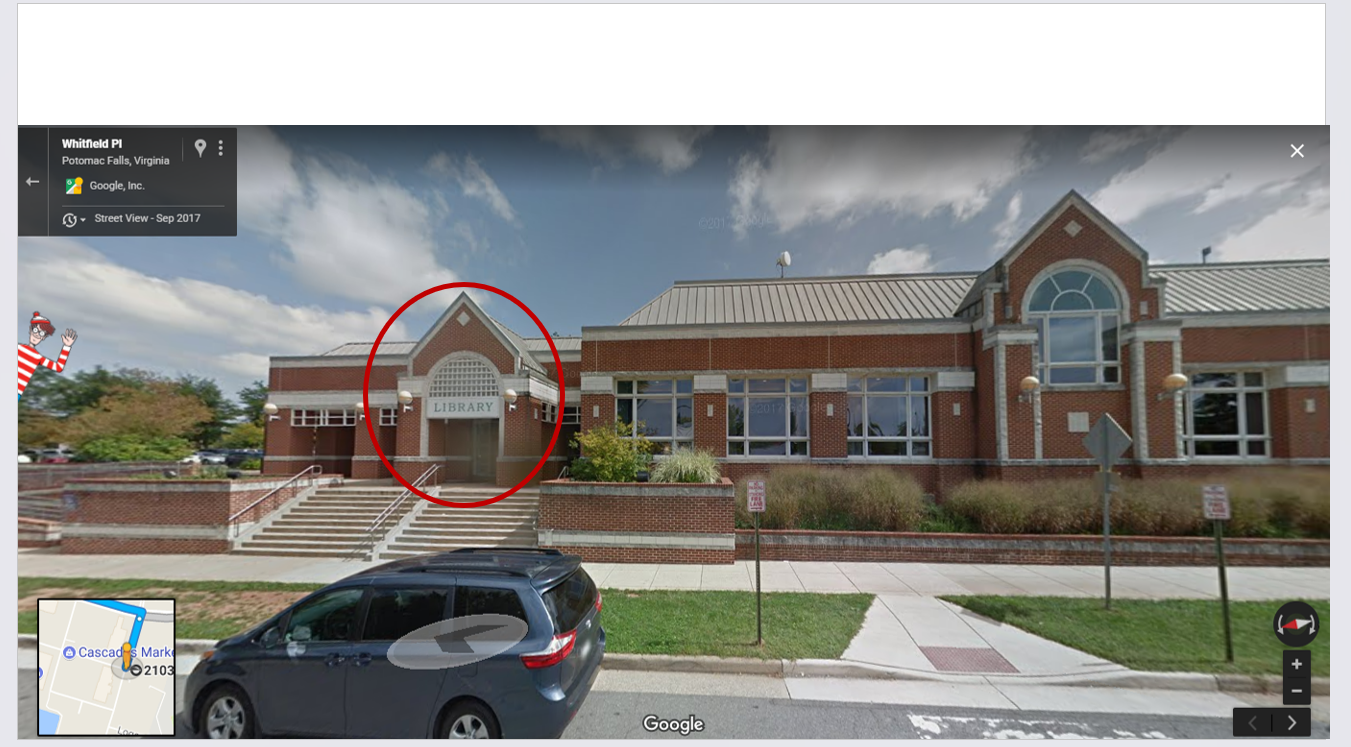
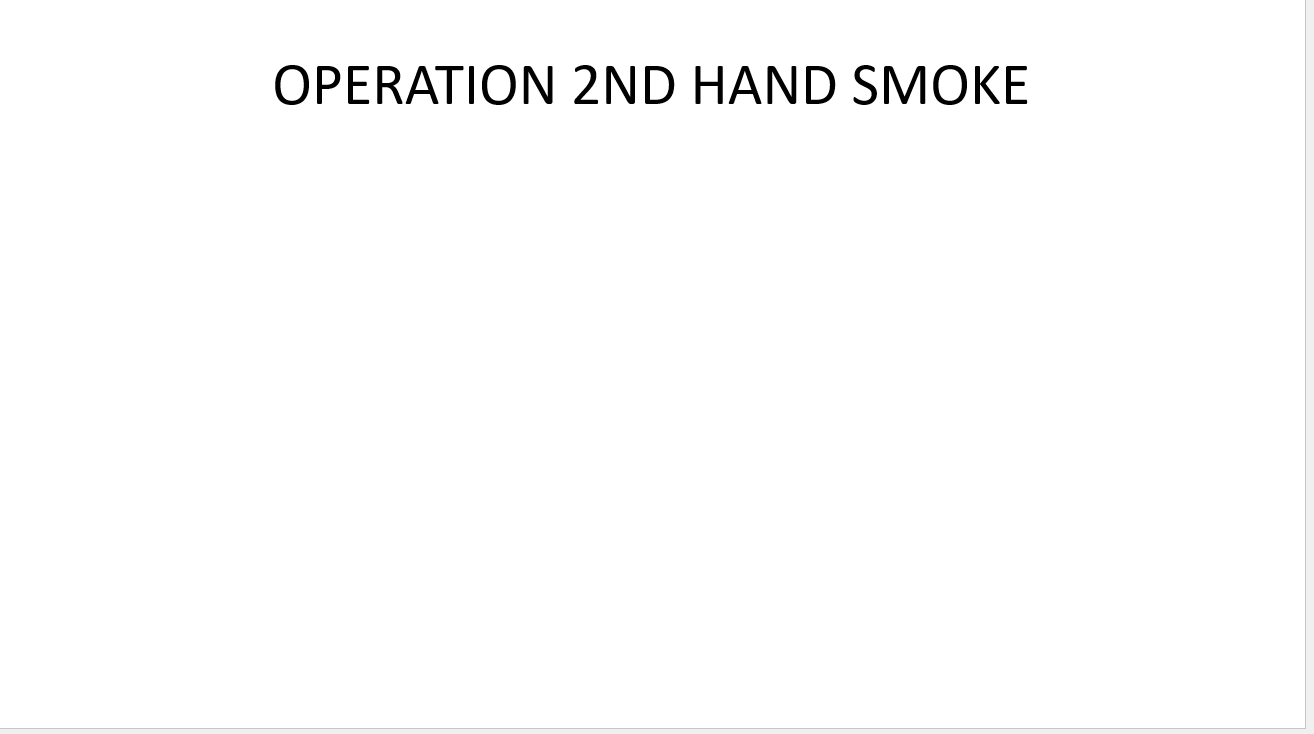
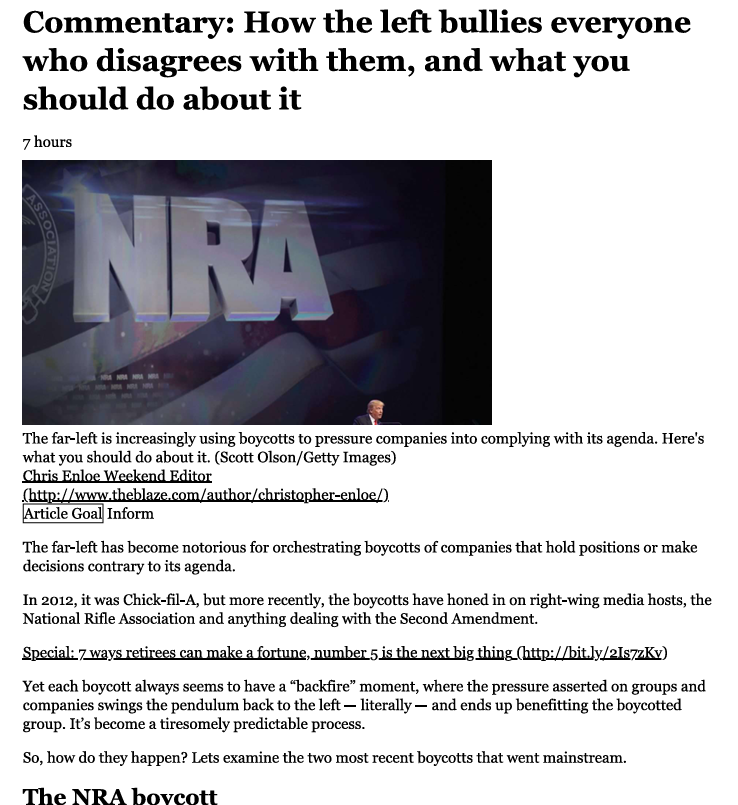
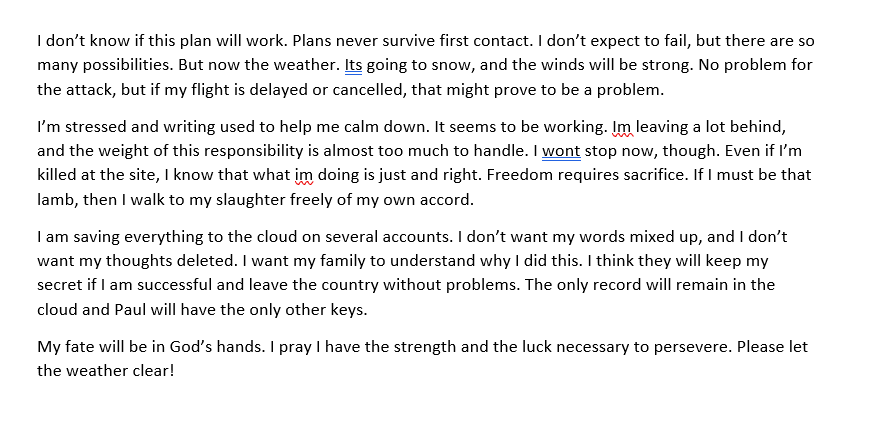
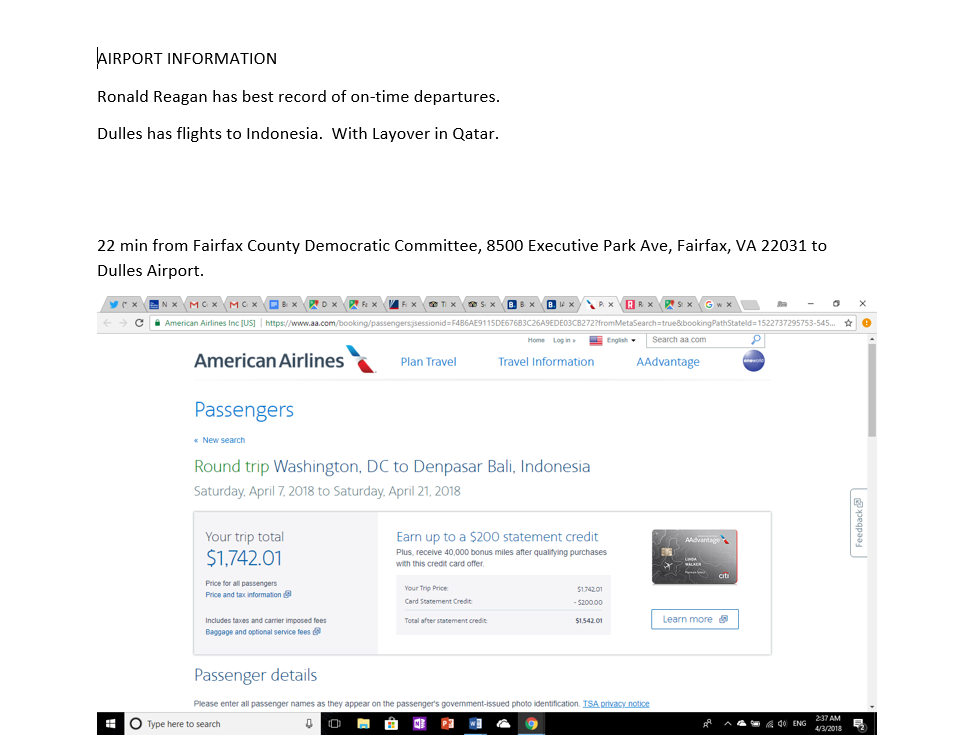
Performed keyword searches with terms like: shoot, cloud, Paul, target, Indonesia, escape.

Located web artifacts pointing to Google Drive, Dropbox, and Gmail logins.

Found browser history involving flights, airport research, and escape plans.

Exported browser cache, deleted documents, and text-based logs containing keywords.

Took timeline screenshots and generated evidence logs (.csv) for documentation.



**5.3** **Volatility Memory Forensics:**

Executed volatility\_2.6\_win64\_standalone.exe and verified profile as Win7SP1x64.

Ran the following commands:

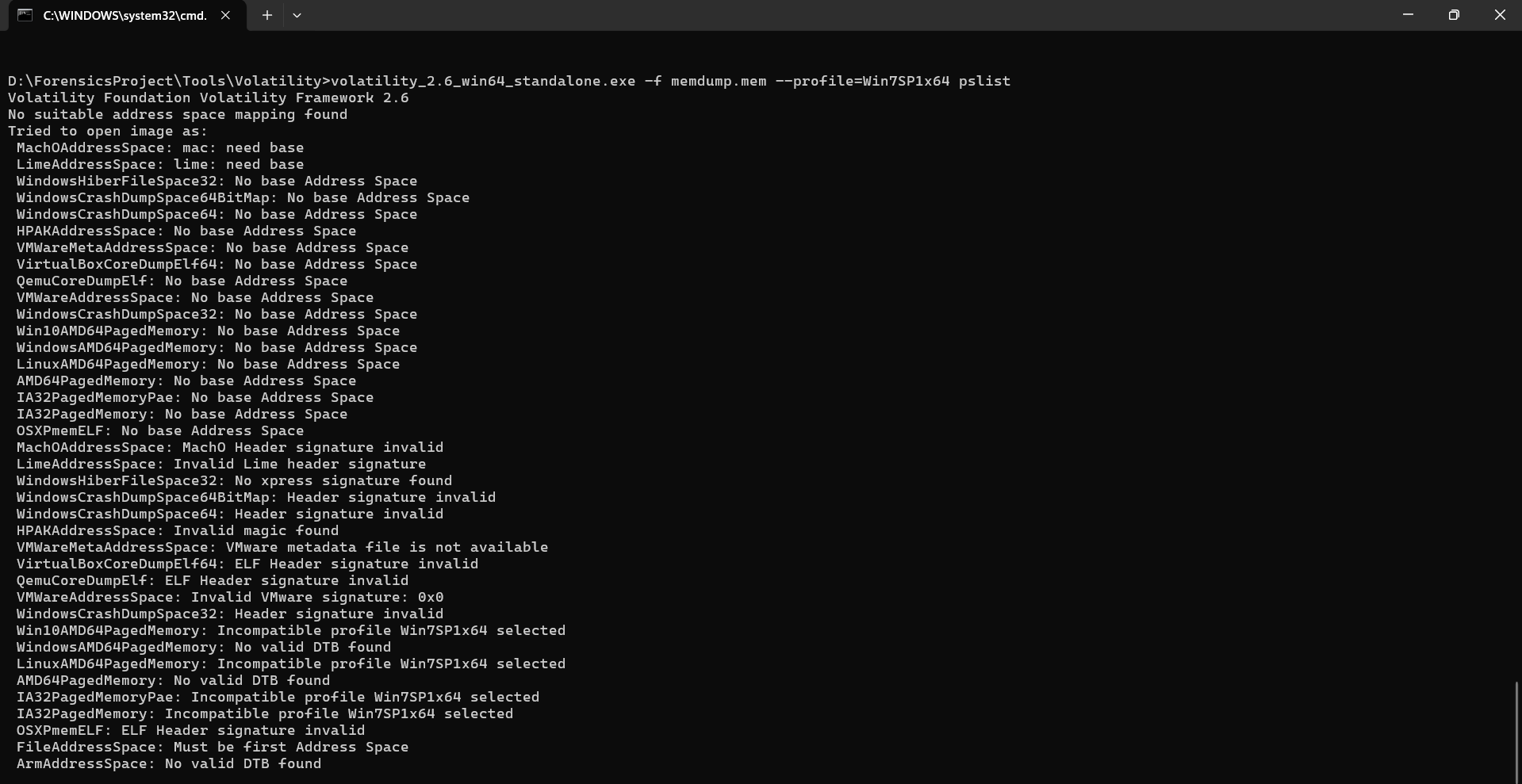
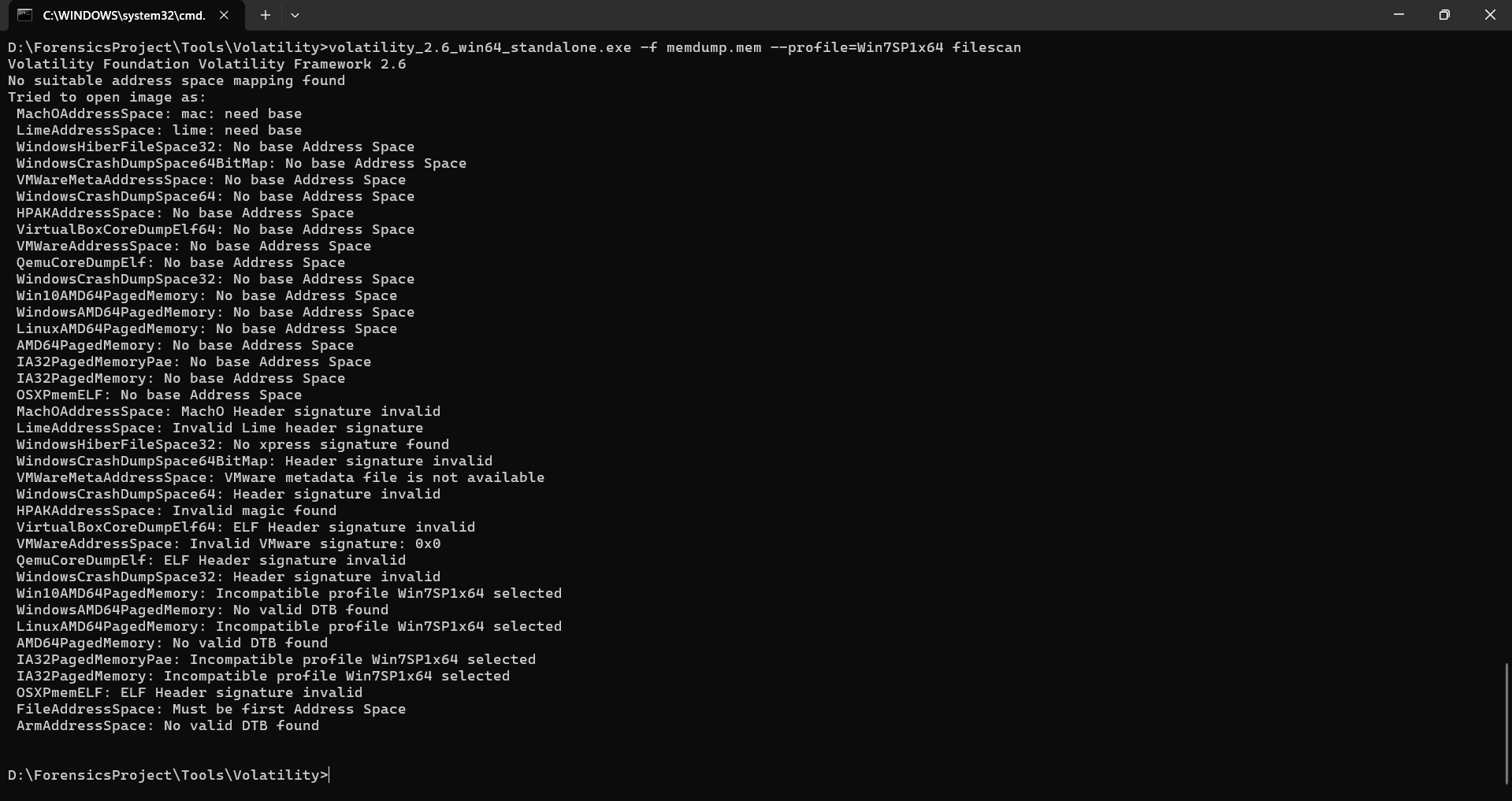
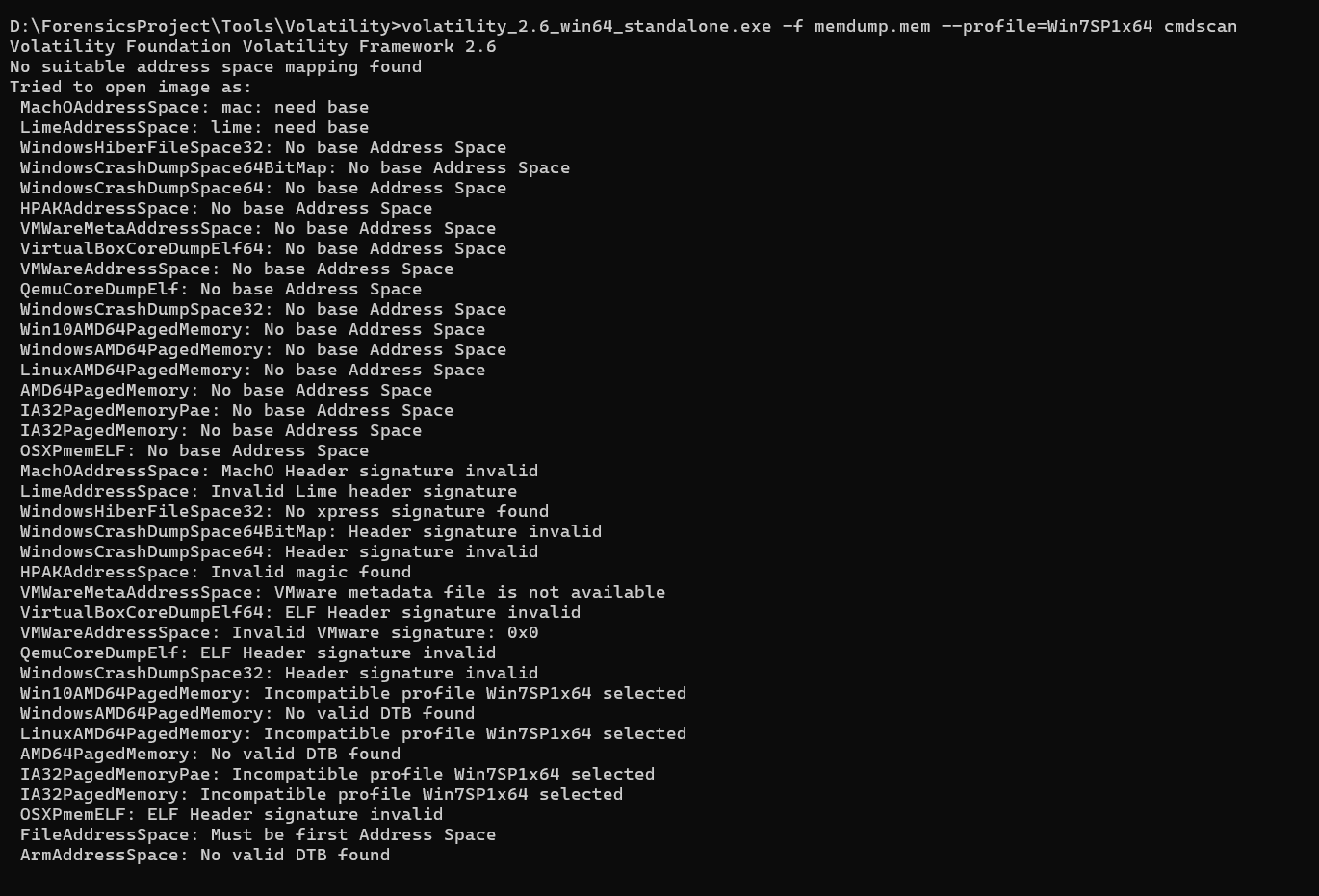
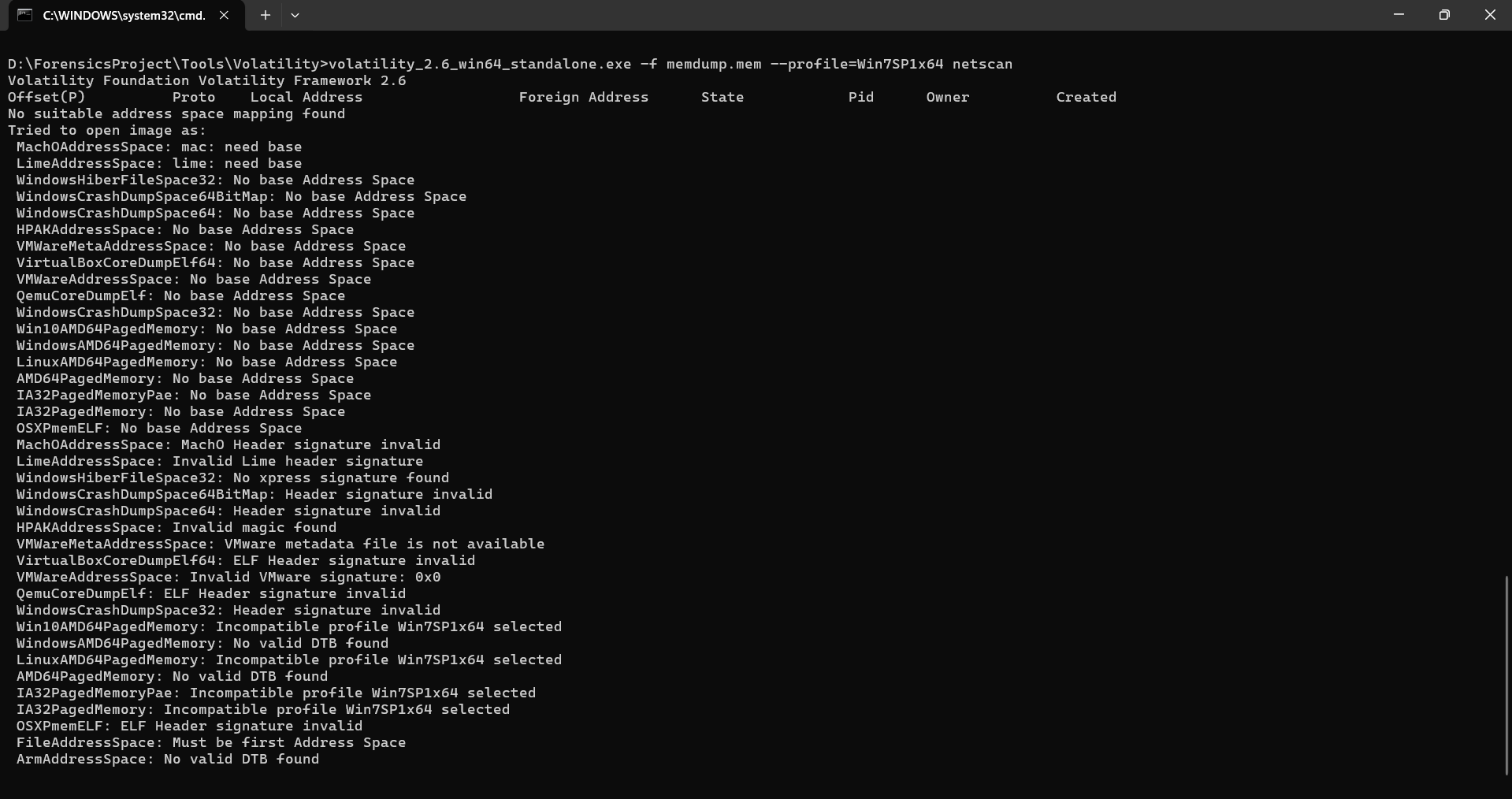
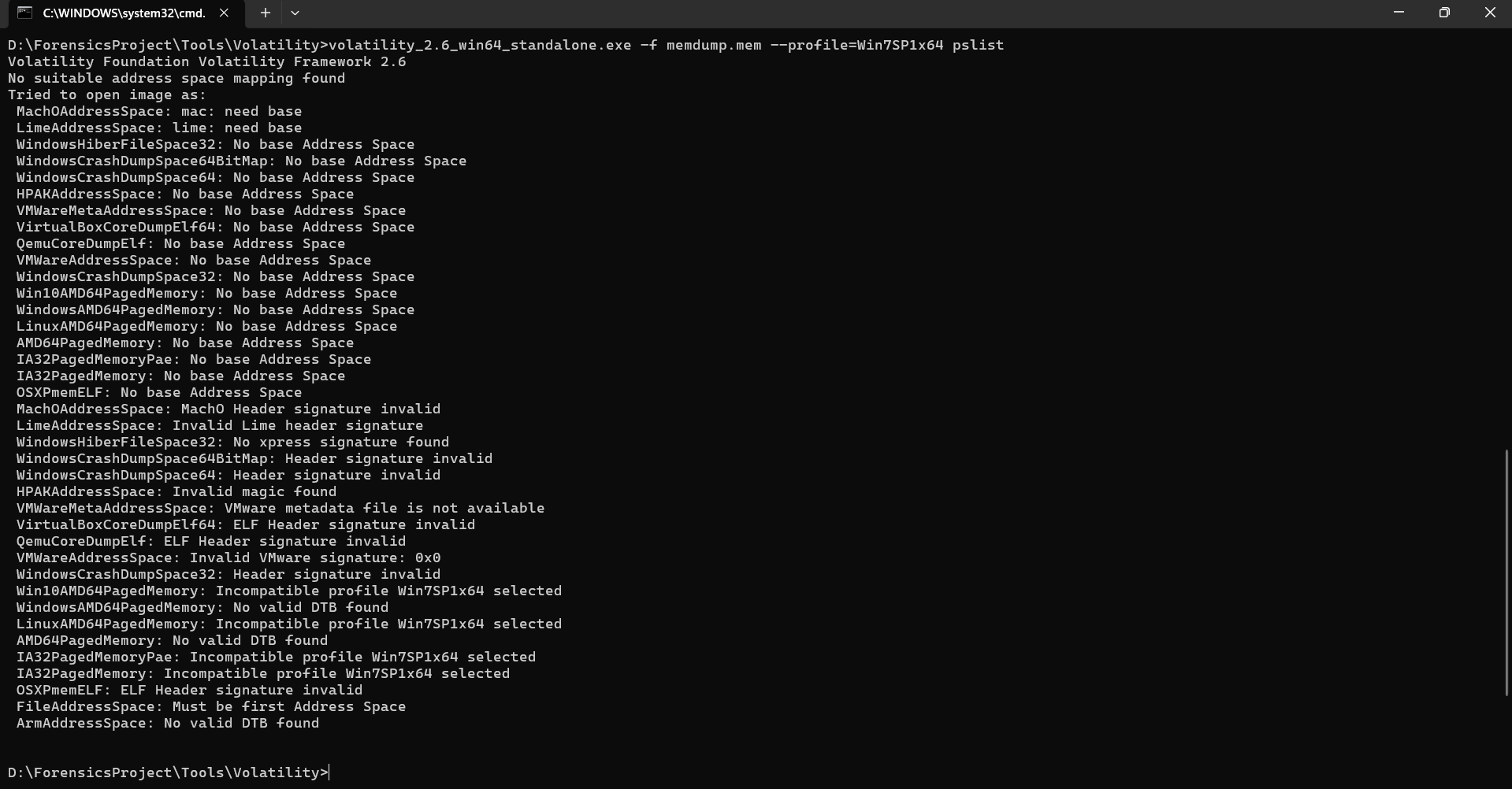
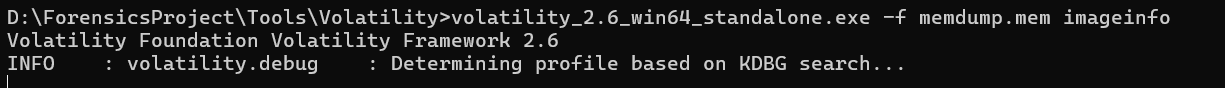
pslist: Identified active processes like chrome.exe, notepad.exe

filescan + dumpfiles: Located and extracted Chrome History database

strings: Extracted raw memory strings that included Paul, cloud, freedom, ammo, and airport names

Confirmed the presence of unsaved planning documents in memory.

Validated that cloud storage-related activities were still present in RAM, supporting evidence of in-progress data synchronization.



**6. ATTACK TIMELINE**

To construct a timeline of the intended attack during the “Town Hall For Our Lives” event scheduled for Saturday, April 7, 2018, at 21030 Whitfield Place, Sterling, VA, 20165, it is presumed that the suspect, Jimcloudy, planned to initiate the mass shooting between 12:30 PM and 1:00 PM. During this window, he would enter the venue and carry out the assault.

After executing the attack, the suspect intended to exit through the library entrance and proceed immediately to Dulles International Airport — aiming to leave before law enforcement could arrive at the scene. The estimated travel time to the airport ranged between 13 to 20 minutes.

The suspect had reportedly purchased his flight ticket online a few days before the attack. His planned destination was Denpasar, Bali, Indonesia, with the flight scheduled to depart the United States on April 8, 2018, for a journey exceeding 22 hours. Furthermore, the suspect had reserved accommodation at Sea Breeze Candidasa, located approximately 1 hour and 30 minutes from Denpasar, suggesting premeditated efforts to escape and remain undetected after the event.

**7. CONCLUSION & RECOMMENDATIONS:**

**Conclusion:**

The investigation uncovered concrete digital evidence of an intended mass shooting. The suspect had left behind a digital trail that included planning notes, escape blueprints, and cloud backup intentions. Browser traces, file activity logs, and memory content all validated the planned attack. The combined use of disk and memory forensics allowed a full reconstruction of the suspect’s intentions, mindset, and preparedness.

**Recommendations:**

Integrate memory acquisition into every disk forensic investigation.

Use keyword scanning tools to detect early warning signs of violent planning.

Develop alert systems for repeated access to weapons/ammunition websites.

Conduct digital behavior analysis in suspicious environments (schools, forums).

Improve awareness among the public for reporting online radical behavior.

**8. PROJECT LINK:**

* [https://github.com/soumyasish-sarkar/ForensicsProject](https://github.com/soumyasish-sarkar/ForensicsProject" \t "_new)

**9. LIST OF REFERENCES:**

* <https://digitalcorpora.org/corpora/scenarios/2018-lone-wolf-scenario/>
* <https://www.autopsy.com/download/>
* <https://github.com/volatilityfoundation/volatility>
* <https://sqlitebrowser.org/>
* <https://medium.com/@tusharcool118/autopsy-tutorial-for-digital-forensics-707ea5d5994d>
* <https://www.geeksforgeeks.org/analysis-of-data-source-using-autopsy/>
* <https://www.youtube.com/watch?v=wpev6WdnvEU>