Week 2

Title:

Recover Deleted Evidence and Uncover Hidden Metadata

Saad Naveed

Cybersecurity & Digital Forensics

DF Internee

Company: Cyborts

Date: 8th July 2025

Submission: 15th July 2025

Objective

Perform forensic analysis on a previously captured disk image to identify, recover, and document deleted, hidden, or suspicious files — including embedded metadata and timestamps.

Step 1: Mount Forensic Image in Autopsy

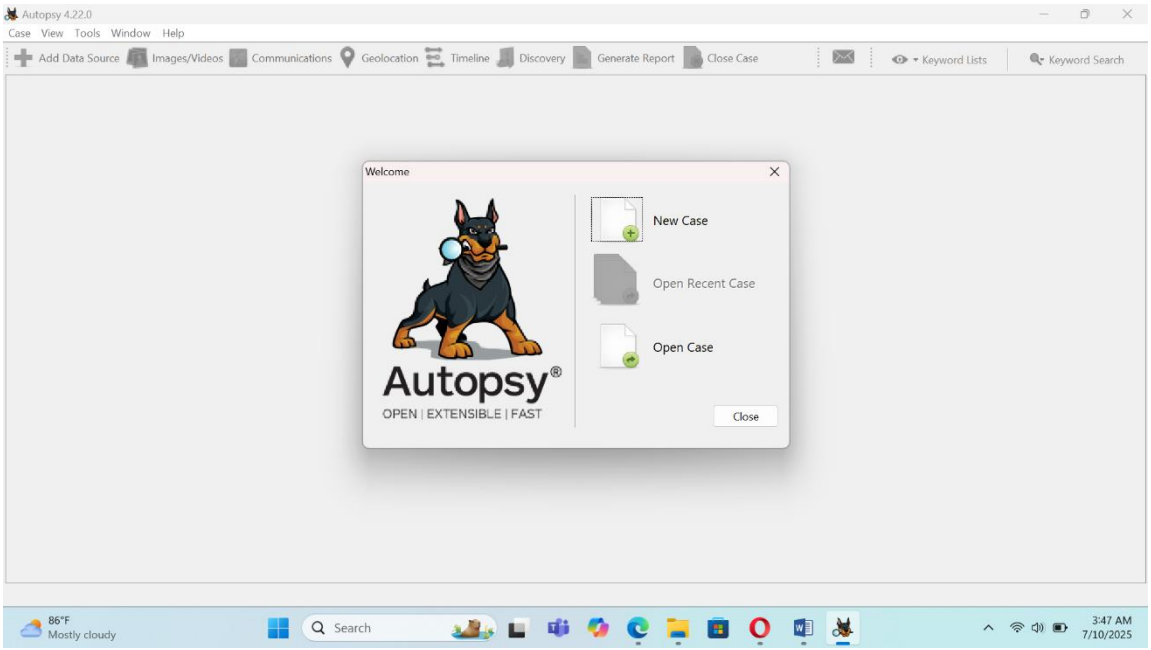
- **Open Autopsy**

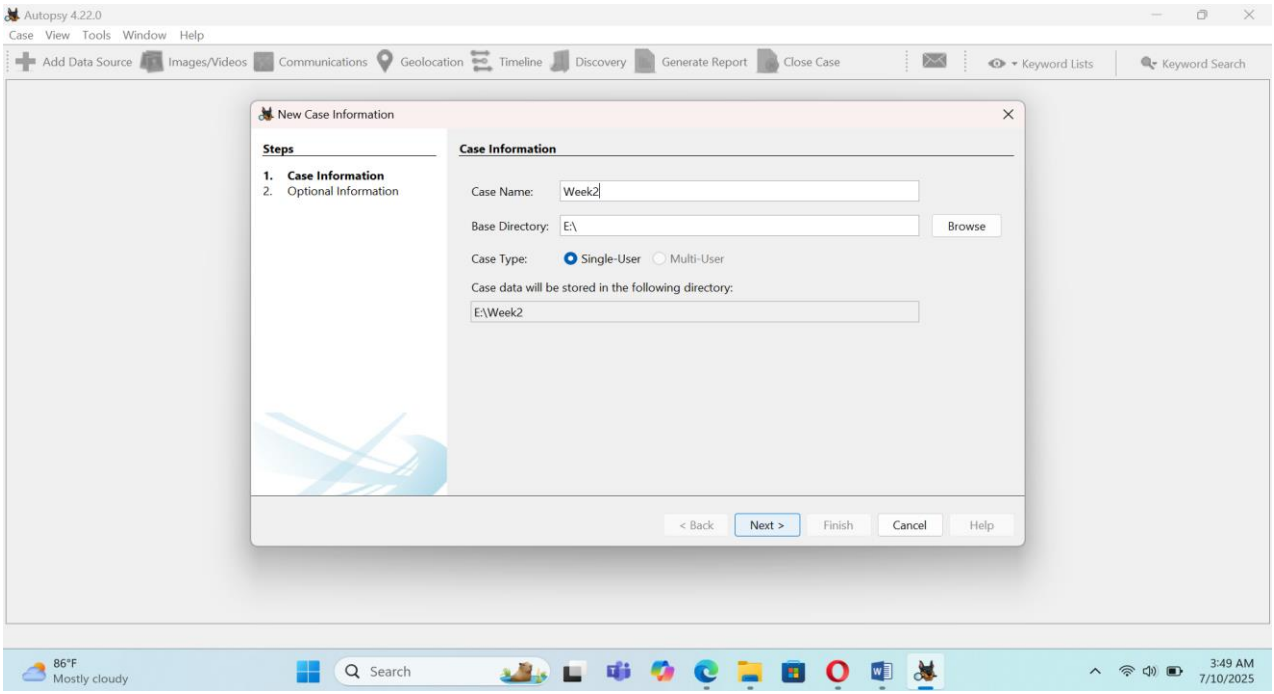
Create a new case:

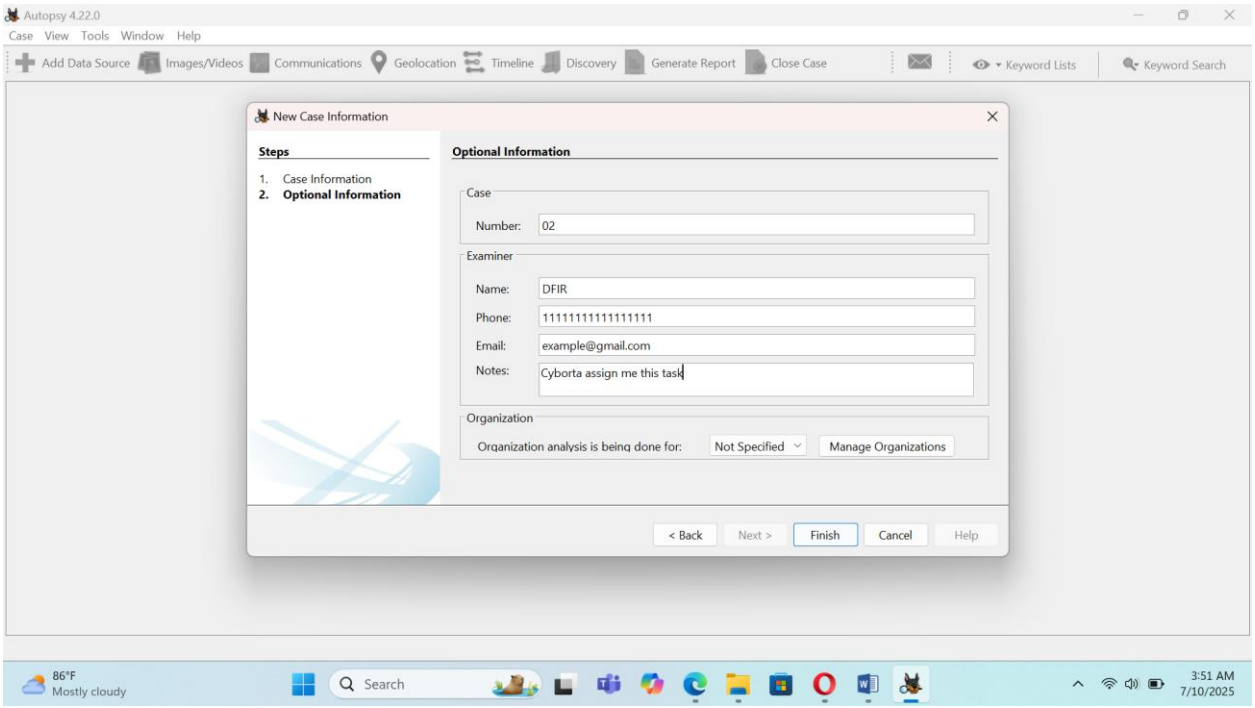
- Case Name: Week2
- Base Directory: I choose folder

Add Data Source:

- I Select “Disk Image ”
- Browse and choose my Week 1 image (usb_image.dd)
- Check **Ingest Modules** (File Type Identification, Recent Activity, etc.)
- Keep image in **read-only** (Autopsy does this by default)




Autopsy 4.22.0
Case View Tools Window Help
Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case
Keyword Lists Keyword Search
New Case Information
Steps
1. Case Information
2. Optional Information
Case Information
Case Name: Week2
Base Directory: E:\
Browse
Case Type: Single-User Multi-User
Case data will be stored in the following directory:
E:\Week2
< Back Next > Finish Cancel Help
86°F
Mostly cloudy
Search
3:49 AM
7/10/2025


Autopsy 4.22.0
Case View Tools Window Help
Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case
Keyword Lists Keyword Search
New Case Information
Steps
1. Case Information
2. Optional Information
Optional Information
Case
Number: 02
Examiner
Name: DFIR
Phone: 11111111111111111
Email: example@gmail.com
Notes: Cyborta assign me this task
Organization
Organization analysis is being done for: Not Specified
Manage Organizations
< Back Next > Finish Cancel Help
86°F
Mostly cloudy
Search
3:51 AM
7/10/2025

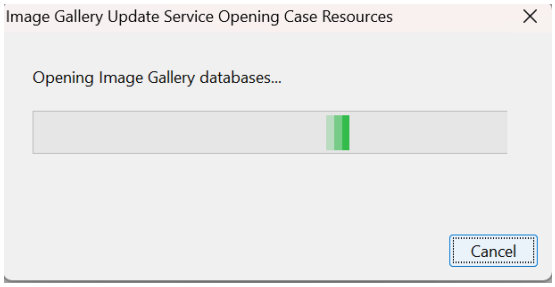
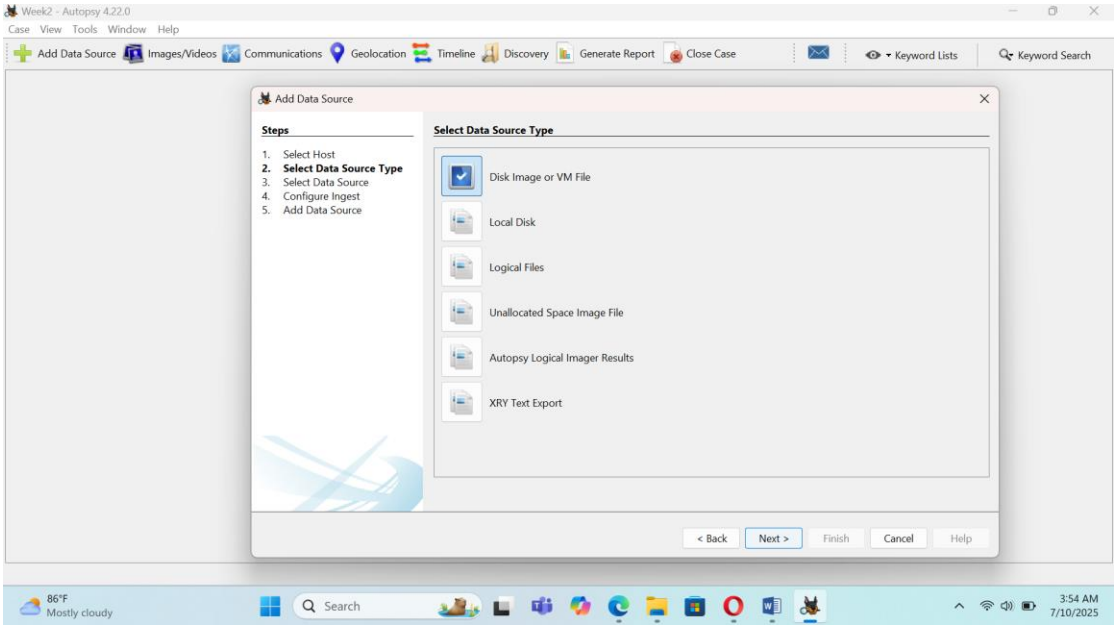
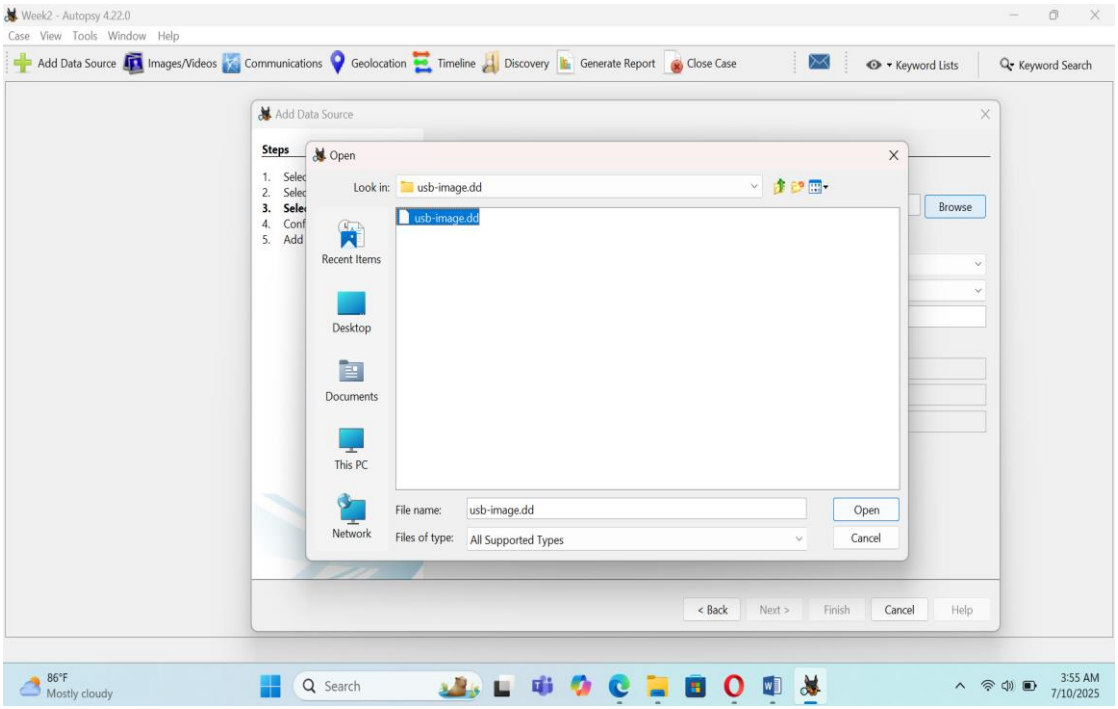
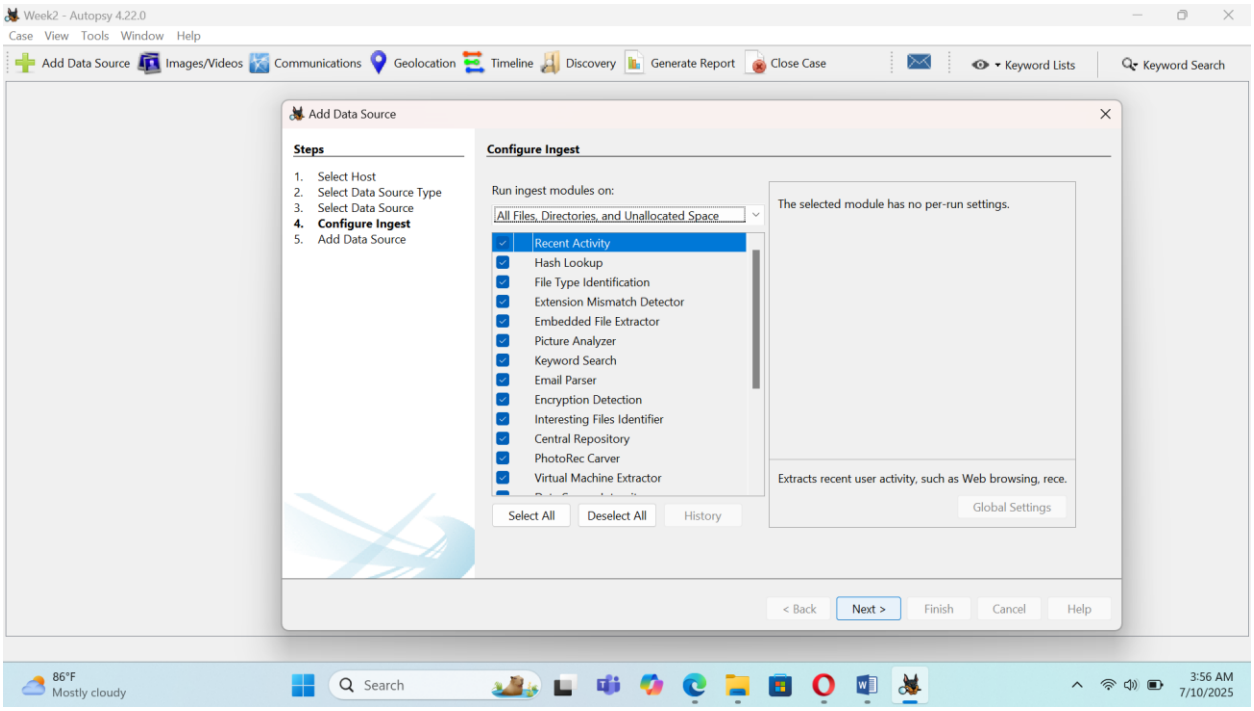
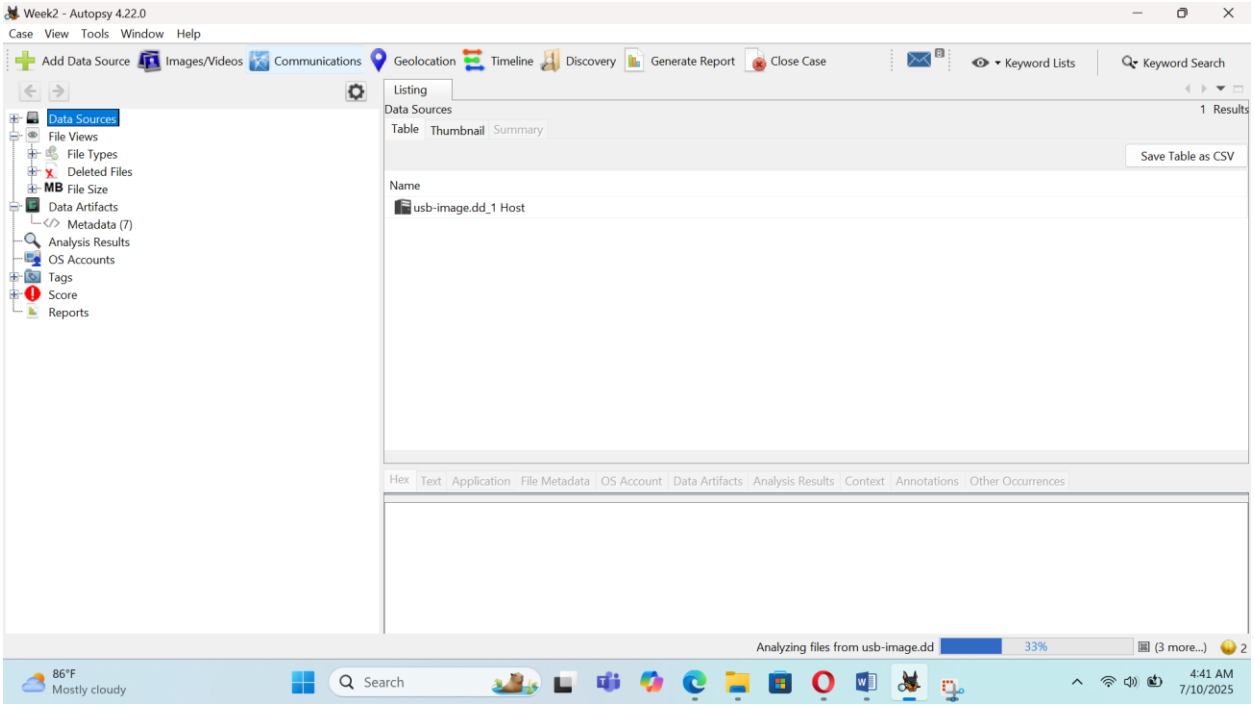


Image Gallery Update Service Opening Case Resources
Opening Image Gallery databases...
Cancel


Week2 - Autopsy 4.22.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
Add Data Source
Steps
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source
Select Data Source Type
Disk Image or VM File
Local Disk
Logical Files
Unallocated Space Image File
Autopsy Logical Imager Results
XRY Text Export
< Back
Next >
Finish
Cancel
Help
86°F
Mostly cloudy
Search
3:54 AM
7/10/2025


Week2 - Autopsy 4.22.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
Add Data Source
Steps
Open
Look in: usb-image.dd
usb-image.dd
Recent Items
Desktop
Documents
This PC
Network
File name: usb-image.dd
Files of type: All Supported Types
Open
Cancel
Browse
< Back
Next >
Finish
Cancel
Help
86°F
Mostly cloudy
Search
3:55 AM
7/10/2025





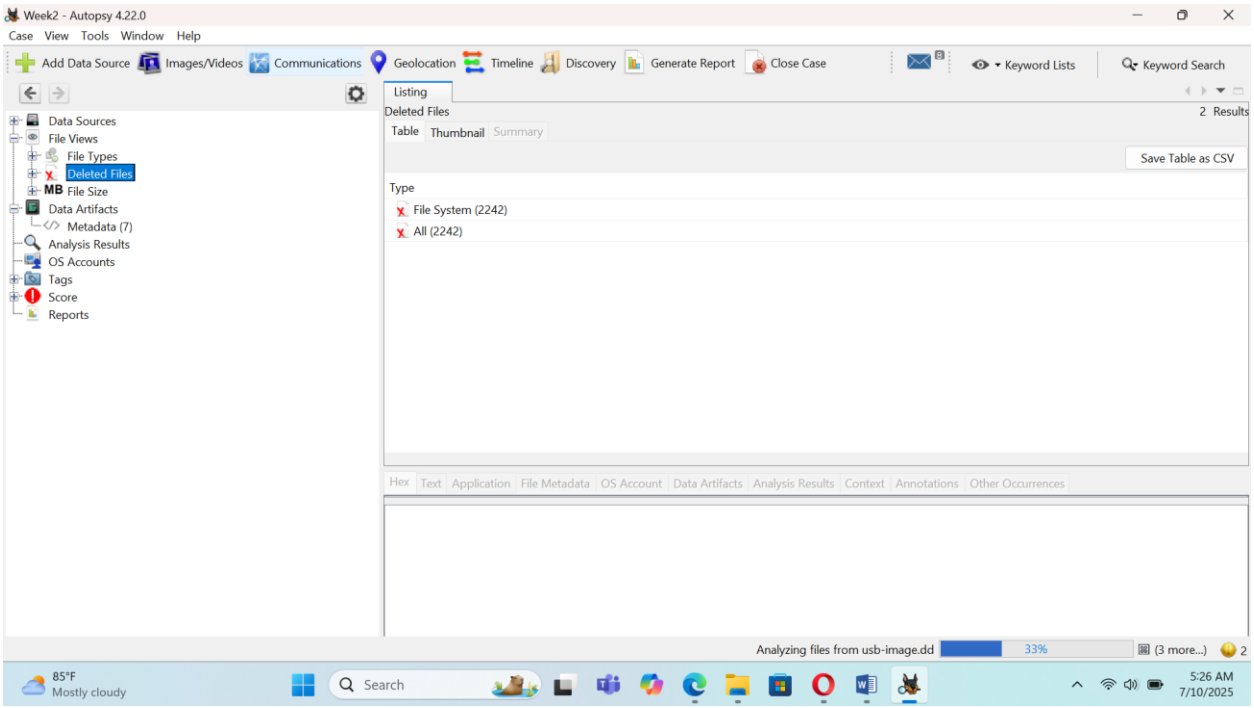
Step 2: Recover Deleted Files

- I select **"Deleted Files"** node in left panel

Autopsy shows recoverable deleted files

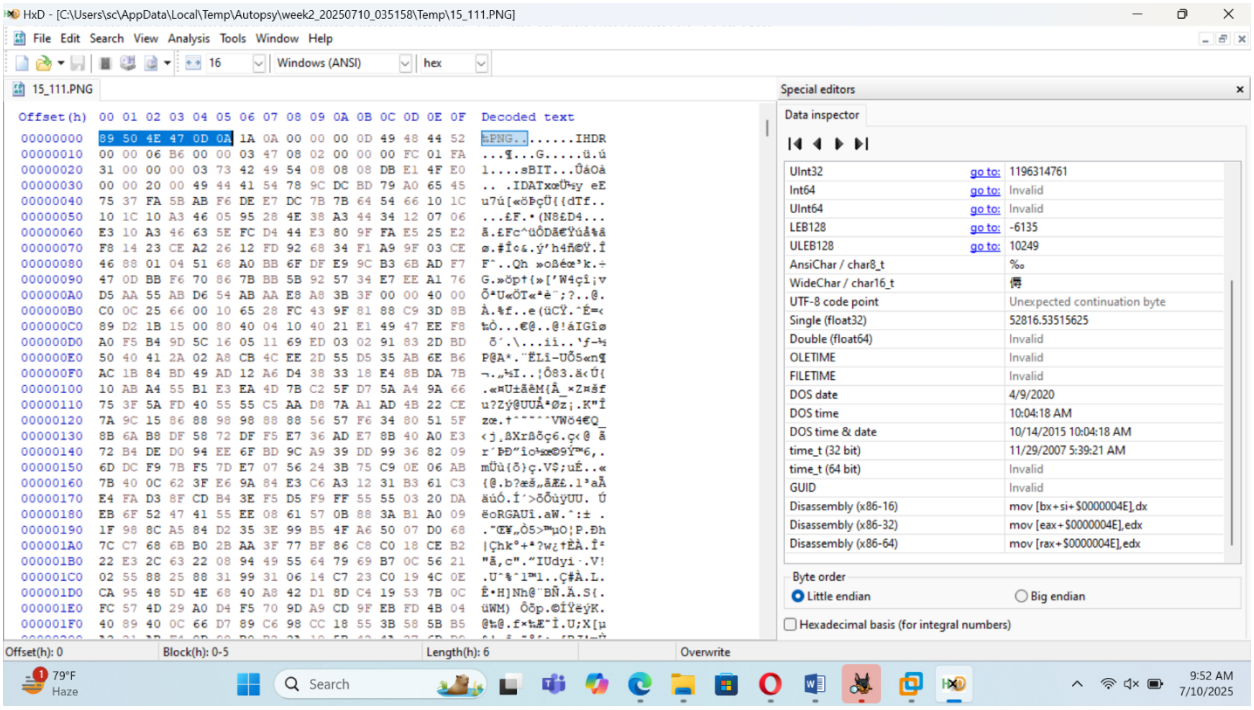
Recover **at least 5** deleted files:

- Right-click → Extract/Export

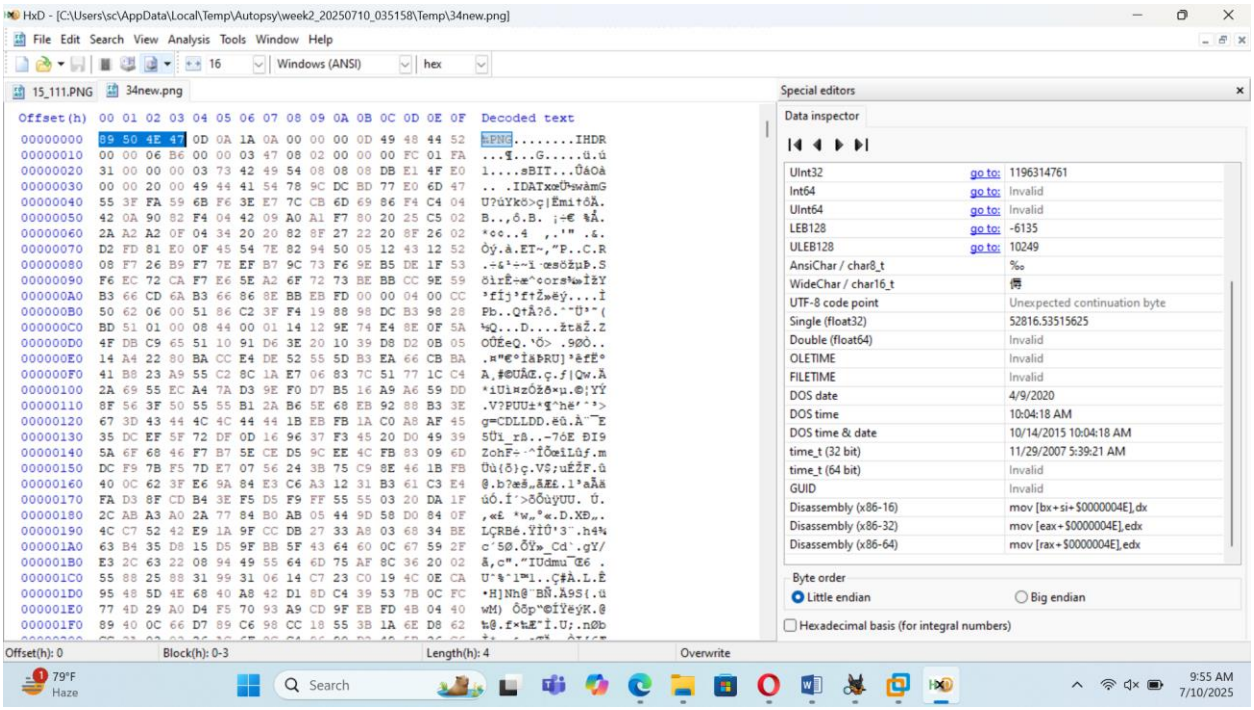


File No.	File Name	File Type	Path	Notes
1	new.png	.png	/img_usb-image.dd/.Trash-1000/files/new.png	Recovered
2	Title01.pdf	.pdf	/img_usb-image.dd/.Trash-1000/files/Title01.pdf	Recovered
3	111.png	.png	/img_usb-image.dd/.Trash-1000/files/111.png	Recovered
4	1.PNG	.PNG	/img_usb-image.dd/$OrphanFiles/1.PNG	Recovered
5	3.PNG	.PNG	/img_usb-image.dd/$OrphanFiles/3.PNG	Recovered

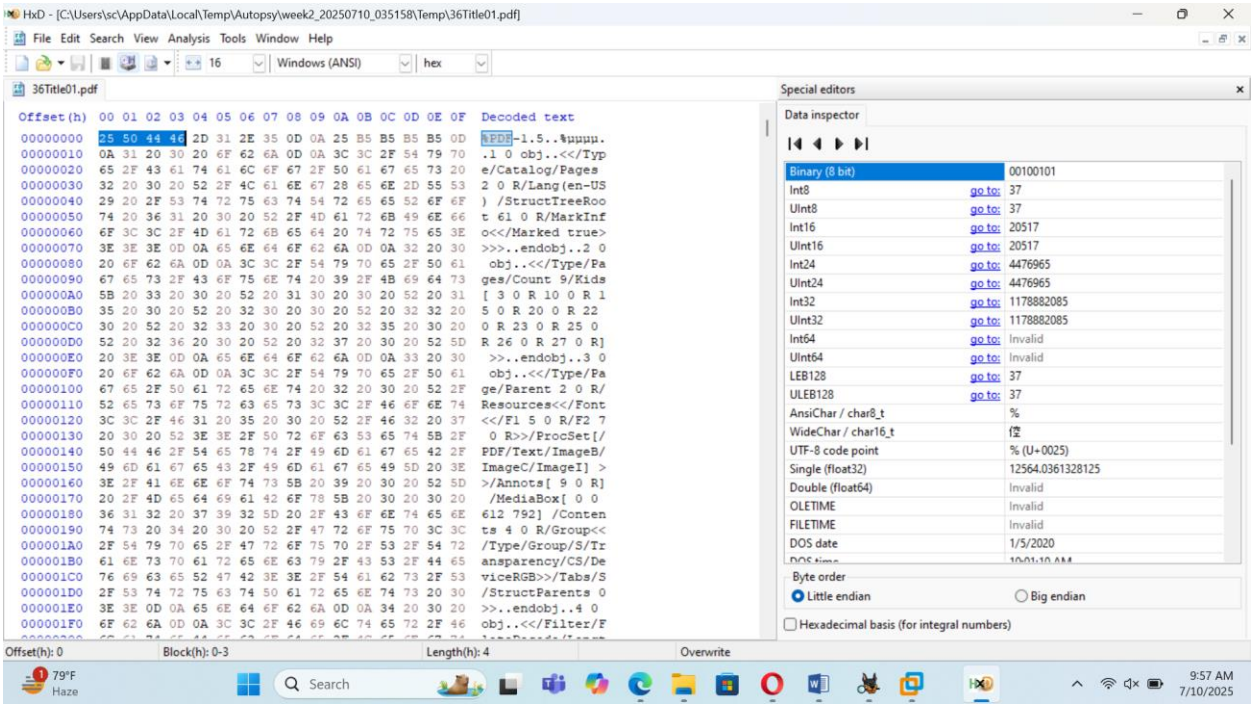
This file header is showing .png file.



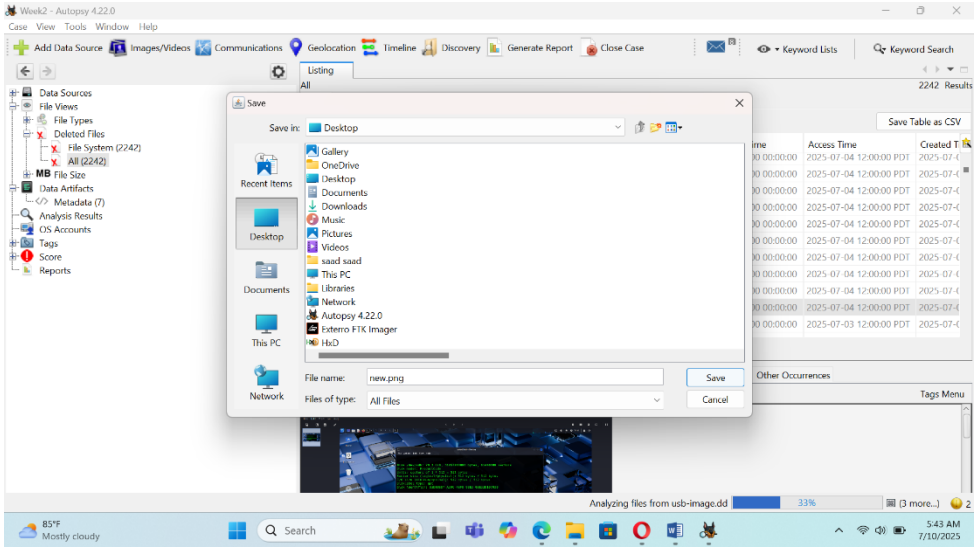
This file name new.png is and its header showing .png file.



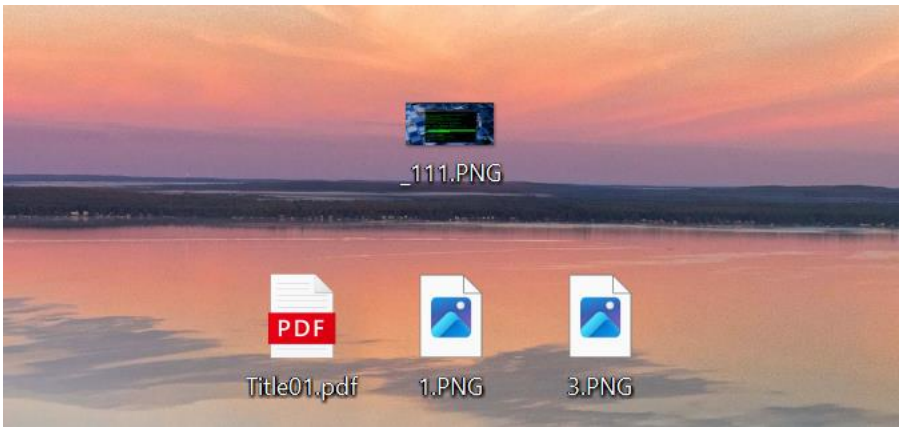
This file header showing its .pdf file.



This screenshot showing file successfully extract on desktop.



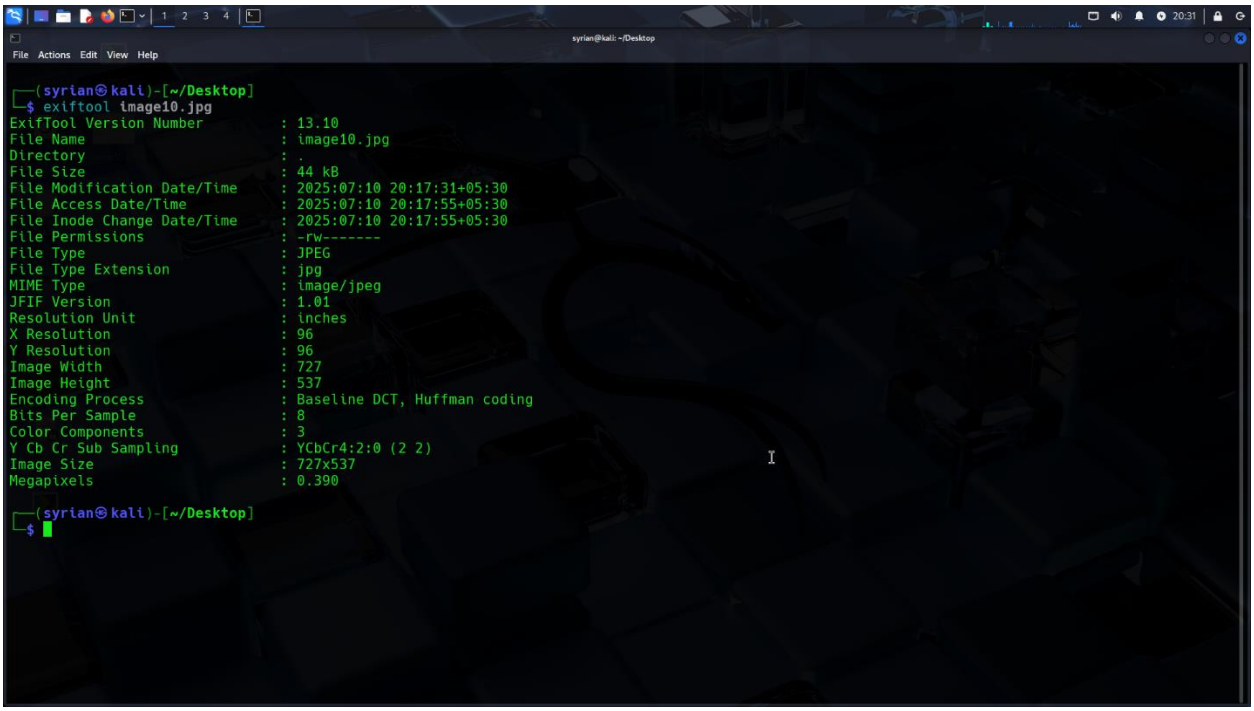
Showing extracted files.



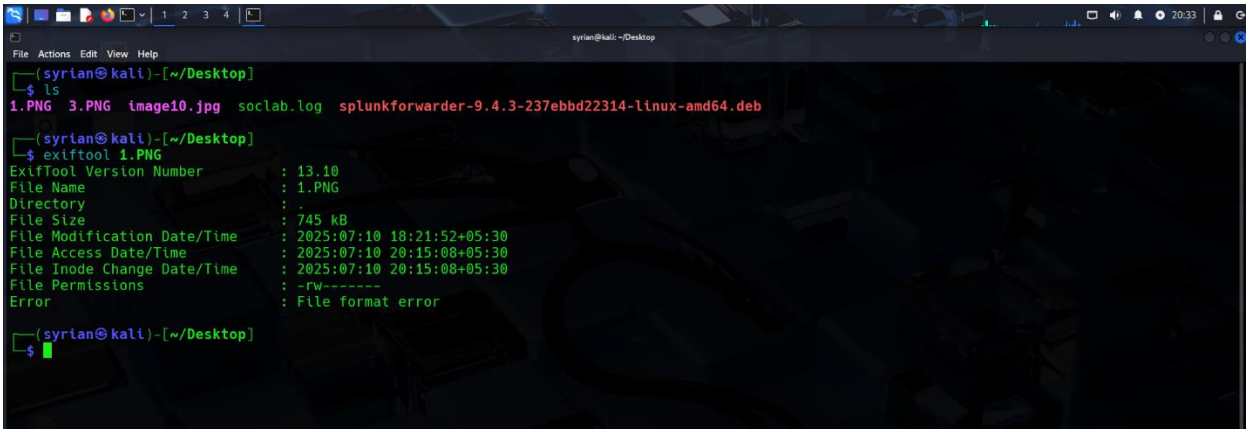
Now Using Kali:

Open kali Linux and paste here extracted files.

Now using Exiftool and extracted file image10.jpg and this showing jpg metadata.

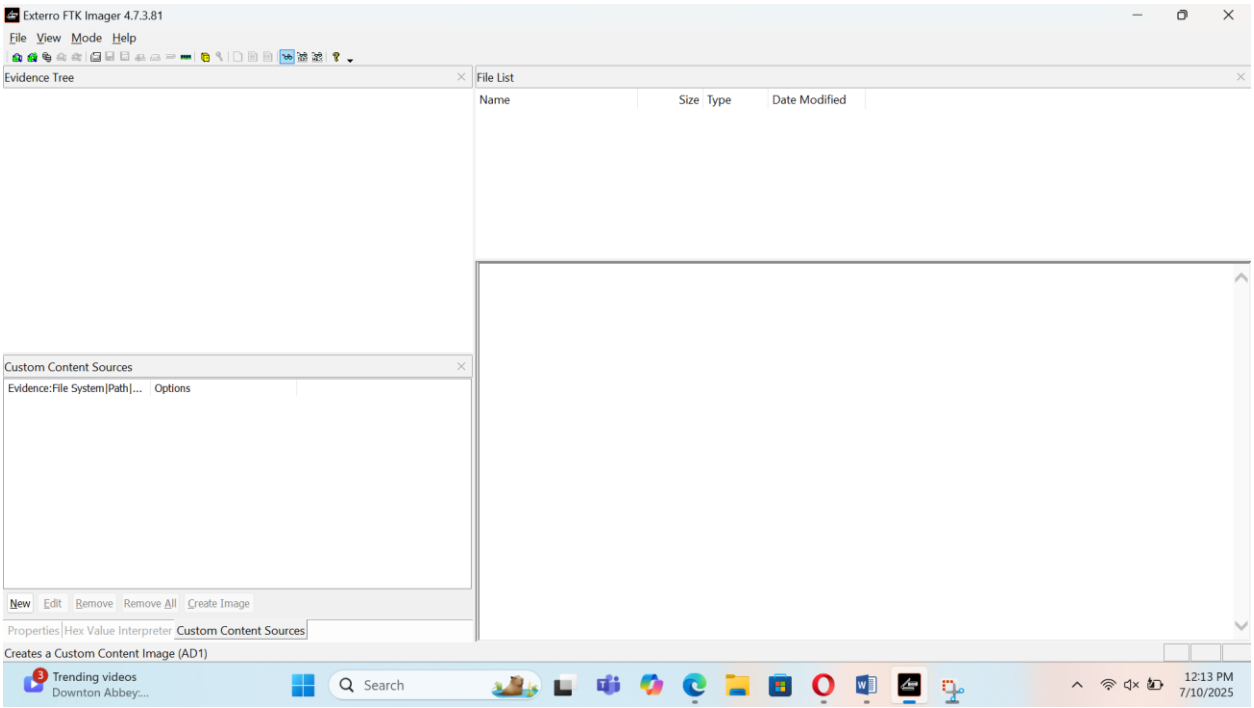


Now using another file PNG file and extract metadata.

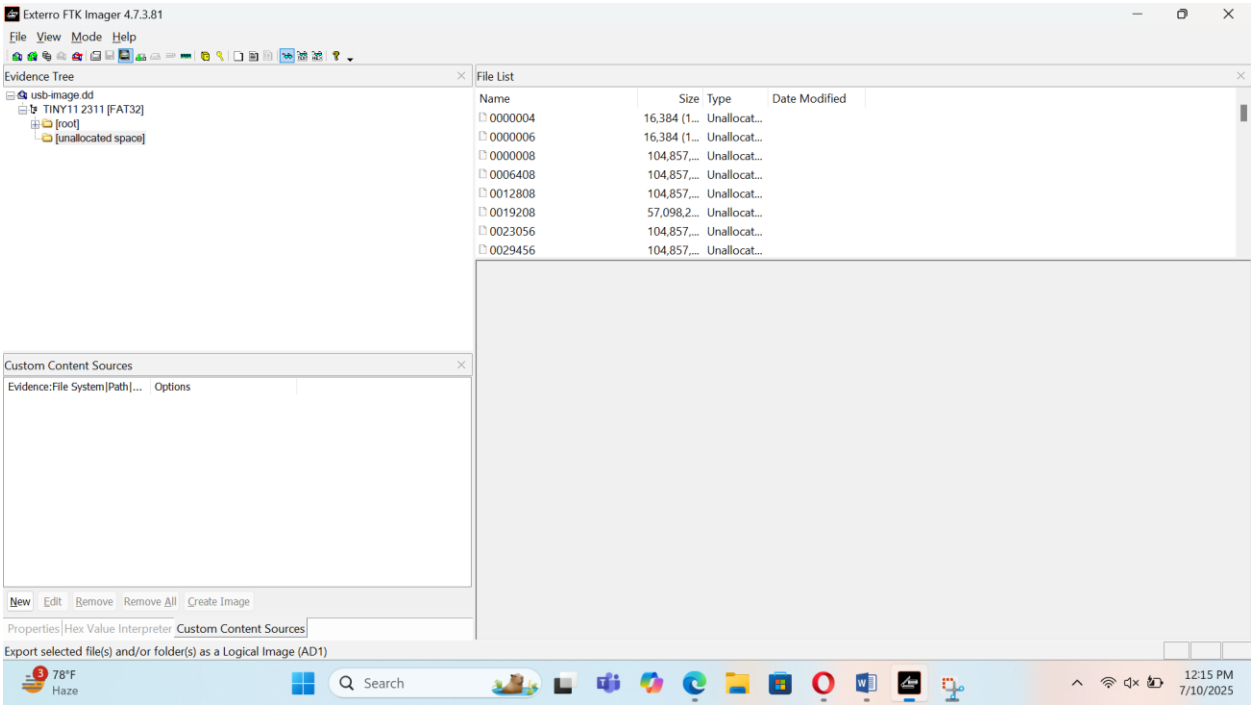


Scan unallocated space for deleted files.

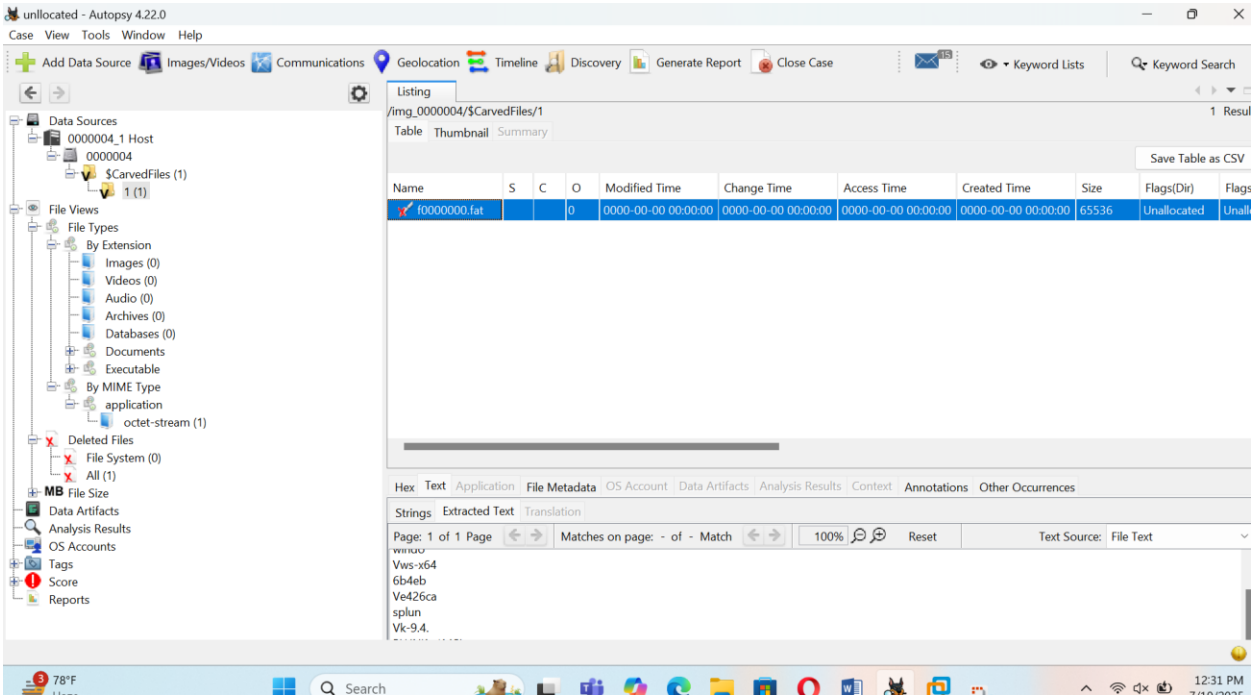
Analyze unallocated space through FTK imager open FTK imager.

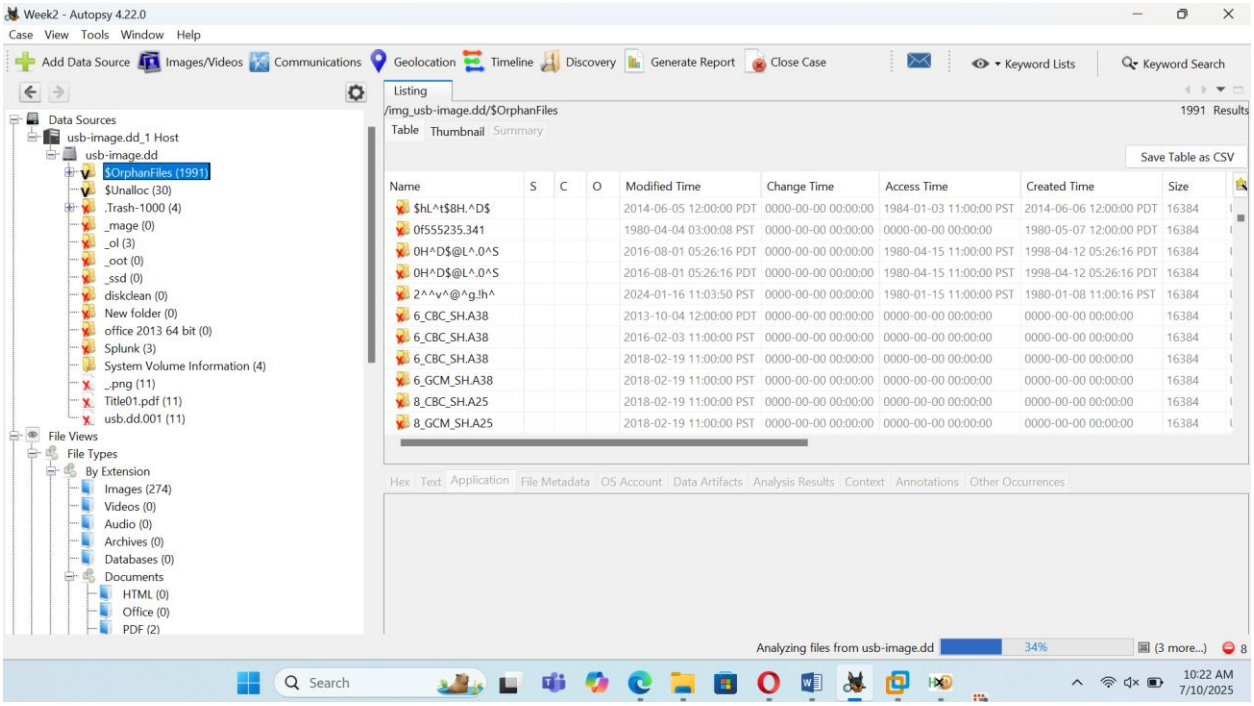


Now load image file in FTK imager and here is showing unallocated space and one file export on desktop.

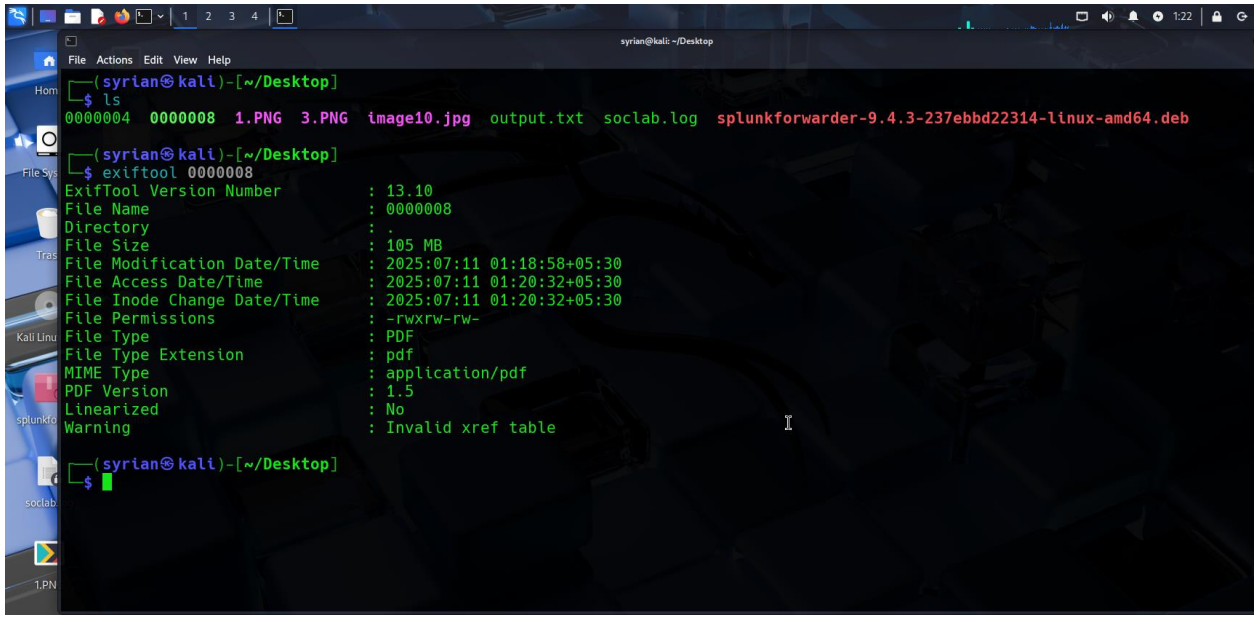


Now identify unallocated file location through Autopsy and I uploaded here that file which I export on desktop.



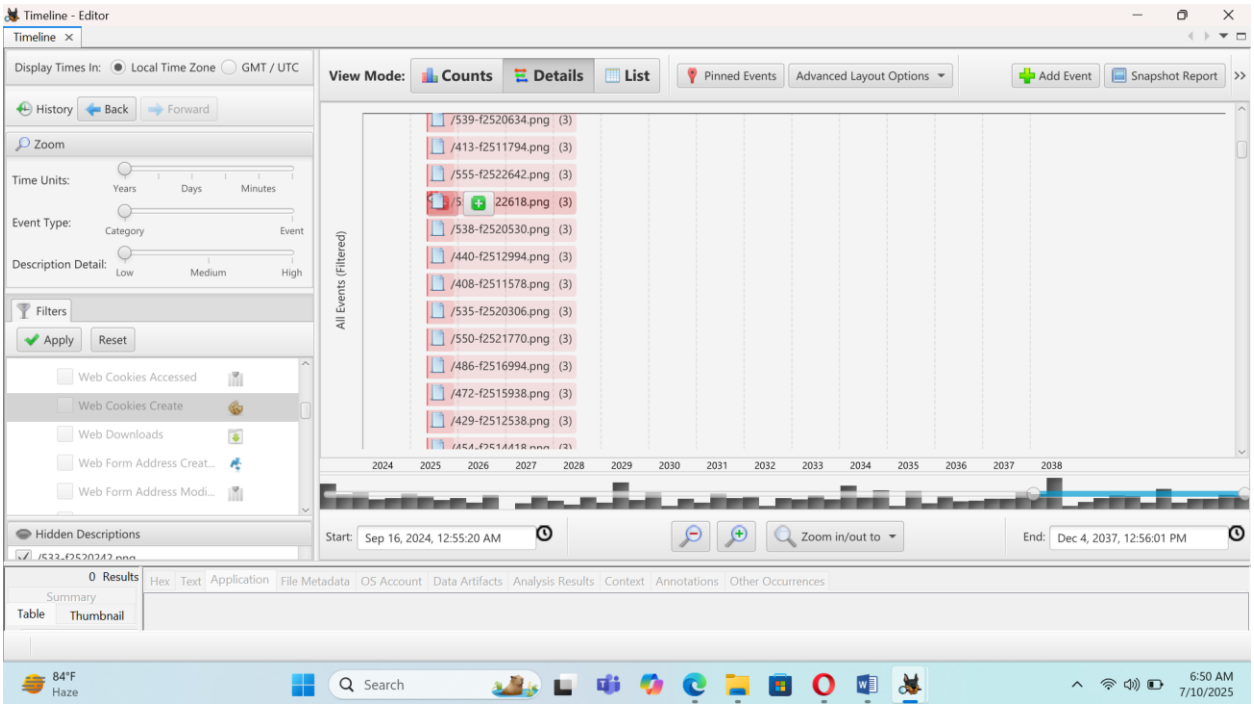


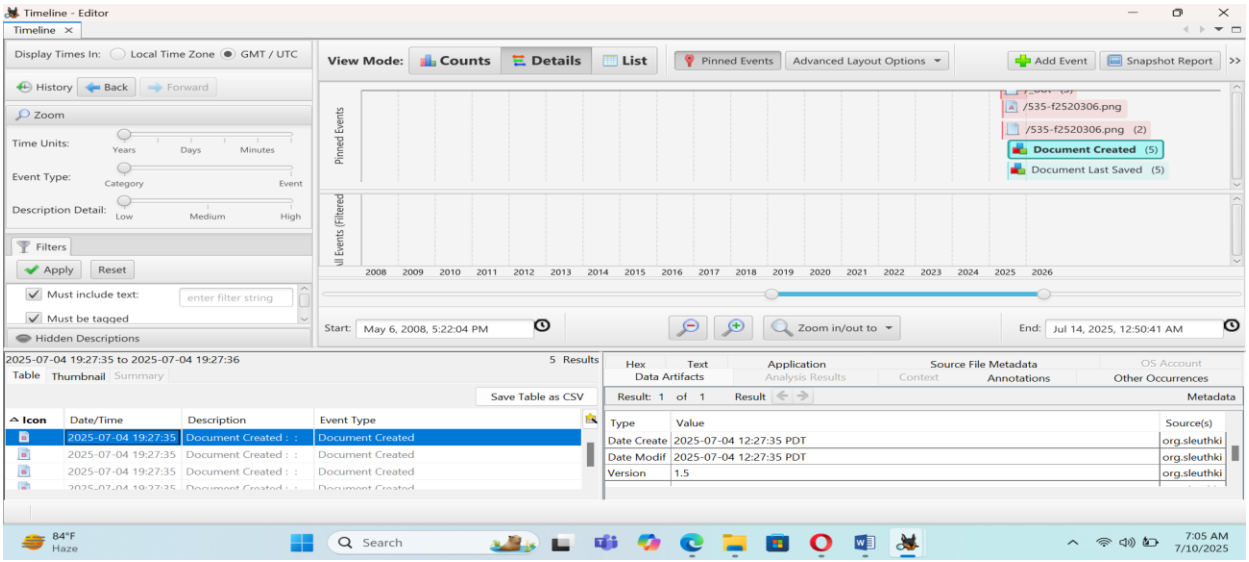
Found unallocated space file.



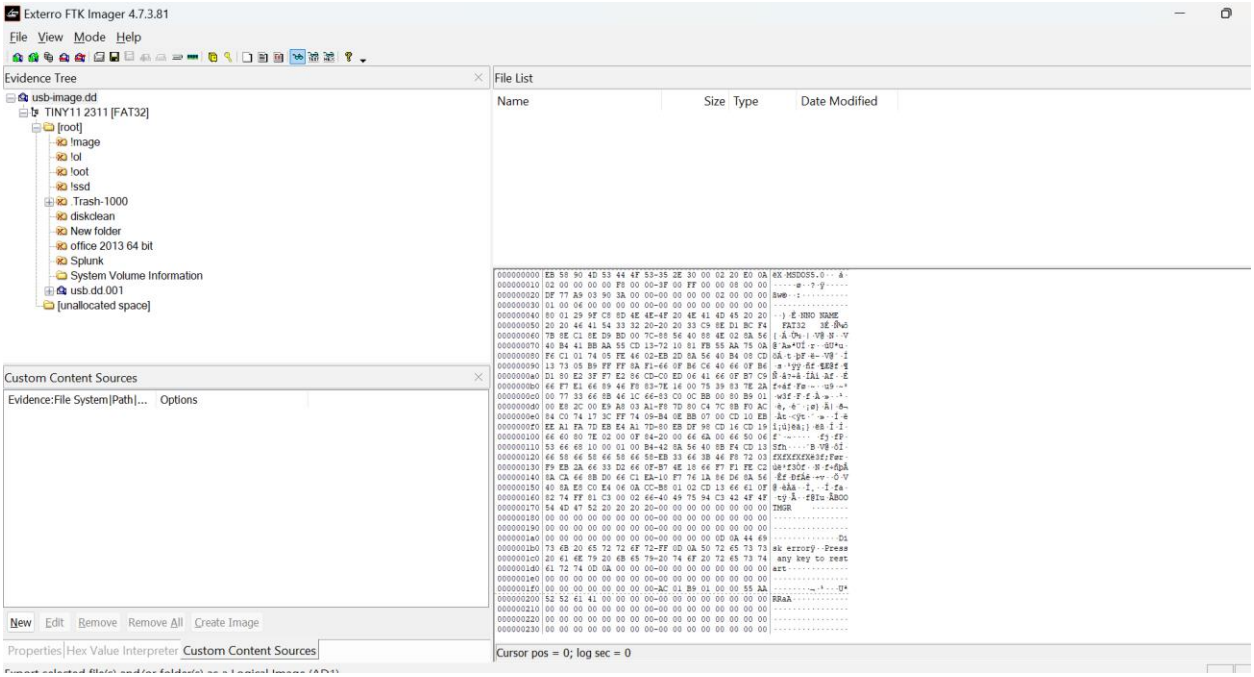
Step 3: Timeline Linking

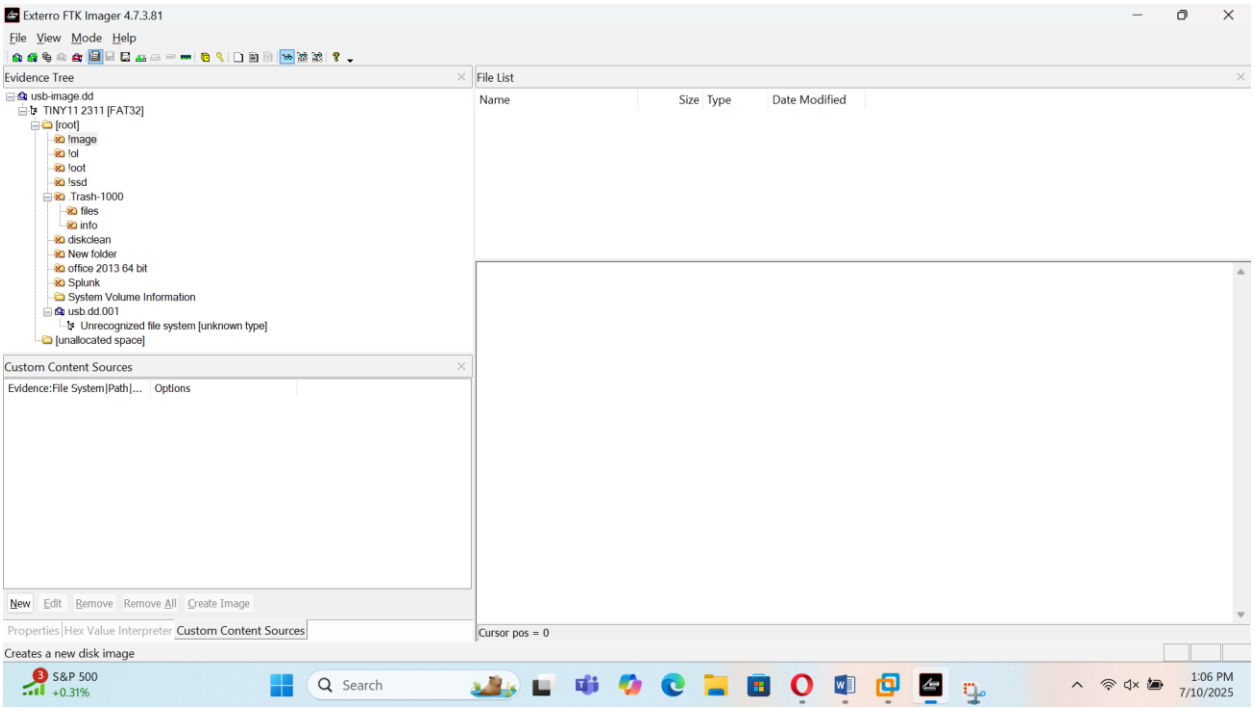
- In Autopsy, select to **"Timeline"** module
- Filter by Time Range and File Types
- I track user actions:
- When files were created, opened, deleted





Step 6 Document Suspicious Findings:





During my analysis using FTK Imager, I carefully reviewed the file system, metadata, and file headers. No password-protected, encrypted, or renamed files were identified. All timestamps appeared consistent and there was no sign of tampering. Based on this examination, no suspicious findings were observed in the recovered files from this disk image.

Conclusion

In this task, I analyzed a disk image using **Autopsy** and **FTK Imager** to recover deleted and hidden files. I was able to successfully recover **five deleted files** like images and a PDF. These files were found in the system's Trash and hidden folders.

Then, I used **ExifTool in Kali Linux** to check the **metadata** of the recovered image files. This helped me see extra information like file creation time and other hidden details.

Next, I scanned the **unallocated space** (empty space where deleted data can still exist) and found another file. I exported it using FTK Imager and confirmed its location with Autopsy.

I also checked the **timeline** of file activities like when files were created, opened, or deleted.

In the end, I **didn't find any suspicious activity** no hidden, renamed, encrypted, or password-protected files. All the file details and timestamps were normal.

This task helped me improve my practical skills in digital forensics like file recovery, metadata checking, and timeline analysis.