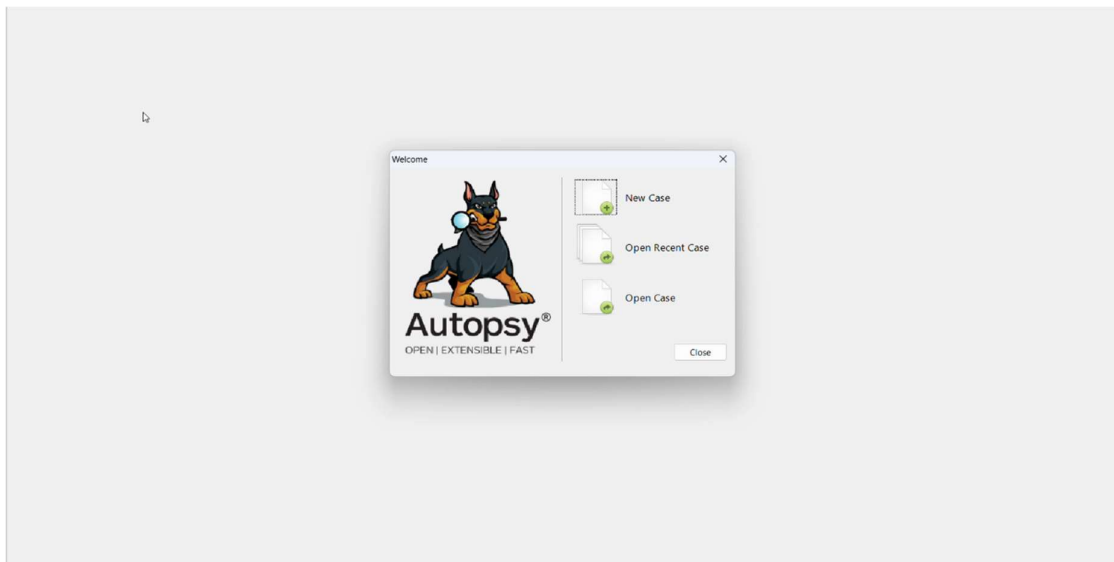


Forensic Analysis of the DD Image Using Autopsy

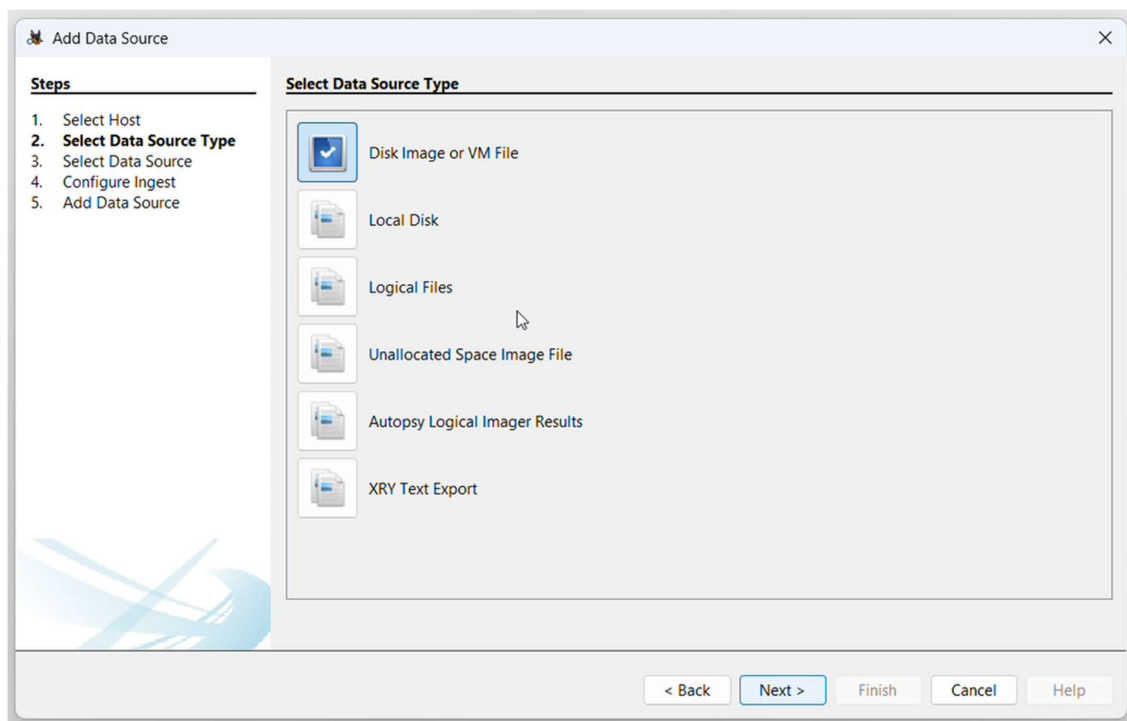
Once the .dd image was created, I utilized Autopsy, a digital forensics tool, to investigate the image's contents. Here are the steps I took:

1: Opened Autopsy and selected "Create New Case" to start the investigation



2: Entered the case name, base directory, and optional case details, such as the examiner's name, to set up the case.

3: Clicked "Next" to proceed, then chose "Add Data Source" to include the DD image for analysis.



4: In the Ingest Module Configuration screen, I selected the essential modules required for analyzing files, web activity, deleted data, and keywords, then clicked "Next."

5: Autopsy began analyzing the image using the selected modules. Shortly after, results started to appear, including active files, deleted files, browsing history, and user activity. All findings were organized and displayed in the left panel under the Tree View.

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	File Type
CYSS238 Research Methodology				2024-07-23 23:39:52 PKT	0000-00-00 00:00:00	2024-10-14 00:00:00 PKT	2024-10-14 06:41:07 PKT	0	Ur
CYSS101 Applied Cryptography				2024-10-13 21:55:56 PKT	0000-00-00 00:00:00	2024-10-14 00:00:00 PKT	2024-10-14 06:41:08 PKT	0	Ur
CYSS103 Network Security				2024-07-23 23:39:42 PKT	0000-00-00 00:00:00	2024-10-14 00:00:00 PKT	2024-10-14 06:41:10 PKT	0	Ur
CYSS201 Digital Forensics				2024-07-23 23:39:48 PKT	0000-00-00 00:00:00	2024-10-14 00:00:00 PKT	2024-10-14 06:41:14 PKT	0	Ur
Screen Recording 2024-10-14 210955.mp4				2024-10-14 21:09:56 PKT	0000-00-00 00:00:00	2024-10-15 00:00:00 PKT	2024-10-14 21:19:14 PKT	360018427	Ur
New folder				2024-10-15 12:43:30 PKT	0000-00-00 00:00:00	2024-10-15 00:00:00 PKT	2024-10-15 12:43:28 PKT	0	Ur
TUDY				2024-10-15 12:43:30 PKT	0000-00-00 00:00:00	2024-10-15 00:00:00 PKT	2024-10-15 12:43:28 PKT	0	Ur
TranscriptJiff				2024-10-17 10:33:26 PKT	0000-00-00 00:00:00	2024-10-17 00:00:00 PKT	2024-10-17 10:33:25 PKT	0	Ur
TranscriptJiff				2024-10-17 10:37:10 PKT	0000-00-00 00:00:00	2024-10-16 00:00:00 PKT	2024-10-17 10:33:25 PKT	317759	Ur
BANK STAT.pdf				2024-10-17 10:33:34 PKT	0000-00-00 00:00:00	2024-10-16 00:00:00 PKT	2024-10-17 10:33:21 PKT	10376	Ur
Profile Report (1) (1).pdf				2024-10-17 10:33:42 PKT	0000-00-00 00:00:00	2024-10-16 00:00:00 PKT	2024-10-17 10:33:51 PKT	76895	Ur
114(1) (Return of Income for a person deriving inc				2024-10-17 10:33:40 PKT	0000-00-00 00:00:00	2024-10-16 00:00:00 PKT	2024-10-17 10:33:51 PKT	391115	Ur
TAX Certificate.pdf				2024-10-17 10:33:52 PKT	0000-00-00 00:00:00	2024-10-16 00:00:00 PKT	2024-10-17 10:33:51 PKT	3113543	Ur
New folder				2024-10-17 10:35:56 PKT	0000-00-00 00:00:00	2024-10-17 00:00:00 PKT	2024-10-17 10:35:55 PKT	0	Ur
Screenshot 2025-03-13 100907.png				2025-03-13 10:09:10 PKT	0000-00-00 00:00:00	2025-03-13 00:00:00 PKT	2025-03-13 10:12:09 PKT	270284	Ur
Screenshot 2025-03-13 101112.png				2025-03-13 10:11:14 PKT	0000-00-00 00:00:00	2025-03-13 00:00:00 PKT	2025-03-13 10:12:09 PKT	291000	Ur
Screenshot 2025-03-13 100811.png				2025-03-13 10:08:14 PKT	0000-00-00 00:00:00	2025-03-13 00:00:00 PKT	2025-03-13 10:12:10 PKT	546796	Ur
Updated SZABIST Need-Based Scholarship Applica				2024-10-17 10:37:38 PKT	0000-00-00 00:00:00	2024-10-23 00:00:00 PKT	2024-10-17 10:37:51 PKT	384783	Ur
Lecture 1-2 Information Security.pptx				2024-10-16 21:14:54 PKT	0000-00-00 00:00:00	2024-10-23 00:00:00 PKT	2024-10-17 09:07:41 PKT	30859048	Ur
Lecture 2 Information Security controls fundame				2023-09-19 04:53:50 PKT	0000-00-00 00:00:00	2024-10-23 00:00:00 PKT	2024-10-17 09:07:44 PKT	6653155	Ur
Lecture 3 Information Security.pptx				2023-09-11 02:14:08 PKT	0000-00-00 00:00:00	2024-10-23 00:00:00 PKT	2024-10-17 09:07:44 PKT	20429409	Ur
Lecture5-6 Information Security.pptx				2023-10-10 04:48:36 PKT	0000-00-00 00:00:00	2024-10-23 00:00:00 PKT	2024-10-17 09:07:46 PKT	42599765	Ur

USB Image Analysis Summary:

Add Data Source

Steps

1. Select Host
2. Select Data Source Type
3. Select Data Source
4. **Configure Ingest**
5. Add Data Source

Configure Ingest

Run ingest modules on:

All Files, Directories, and Unallocated Space

- ☒ Recent Activity
- ☒ Hash Lookup
- ☒ File Type Identification
- ☒ Extension Mismatch Detector
- ☒ Embedded File Extractor
- ☒ Picture Analyzer
- ☒ Keyword Search
- ☒ Email Parser
- ☒ Encryption Detection
- ☒ Interesting Files Identifier
- ☒ Central Repository
- ☒ PhotoRec Carver
- ☒ Virtual Machine Extractor

Global Settings

The selected module has no per-run settings.

Extracts recent user activity, such as Web browsing, rec..

< Back Next Finish Cancel Help

After imaging the USB with FTK Imager and analyzing it in Autopsy, key findings emerged:

- **Existing Files:** Documents, images, and executables, some manually copied.
- **Recovered Deleted Files:** Personal documents, login-related texts, and setup files—possible signs of data exfiltration.
- **Sensitive Data:** Cached passwords, credentials, and notes indicate private information storage.
- **Web Activity:** Limited browser cache suggests file downloads.
- **Hidden Files:** Some files marked as system-related, hinting at concealment or malware.
- **File Timeline:** Usage patterns reveal suspicious deletions close to imaging time.

Conclusion:

This investigation highlights how USBs can hold crucial evidence, with recovered deleted files—especially sensitive data—being a critical aspect.