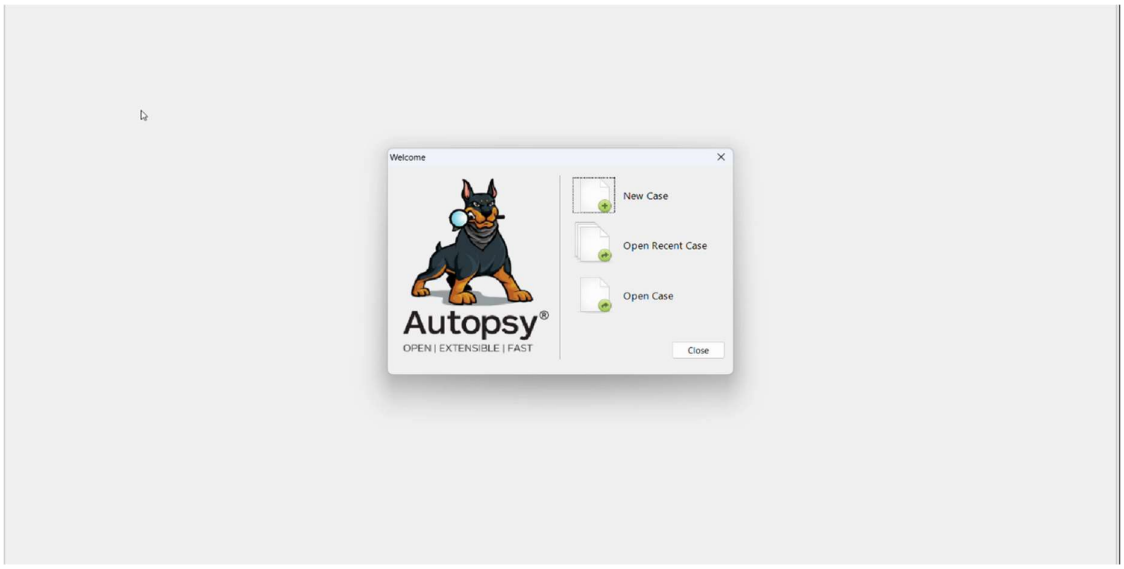
Forensic Analysis of the DD Image Using Autopsy

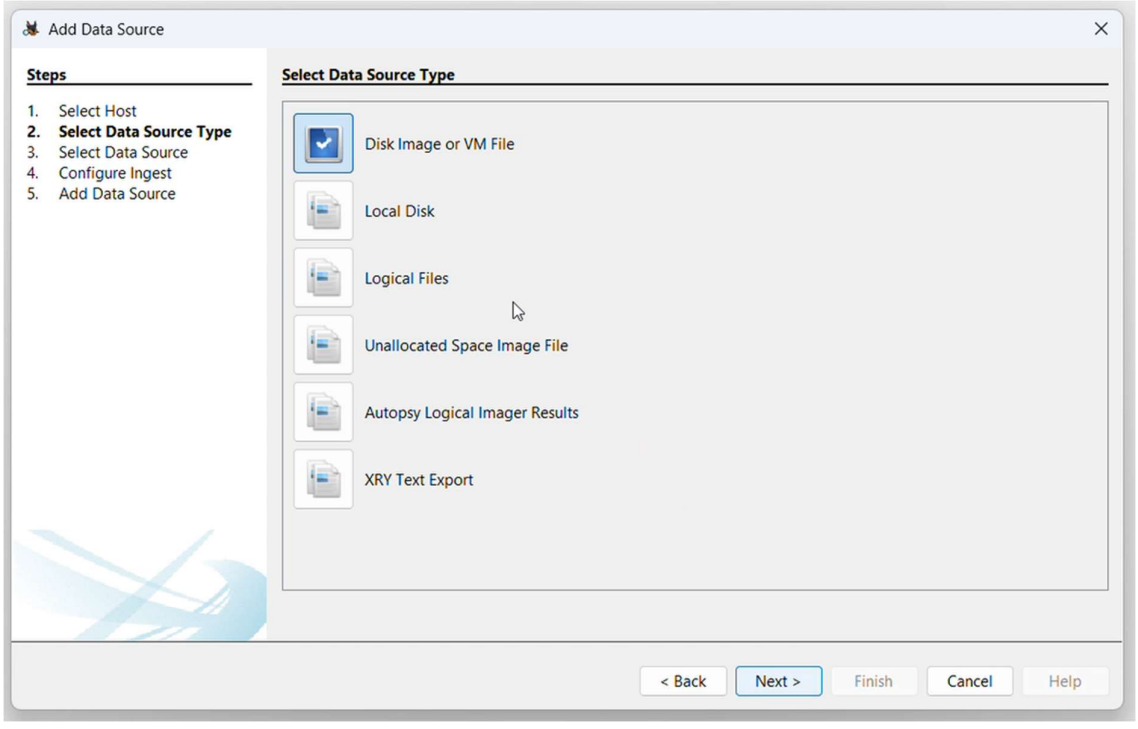
Once the .dd image was created, I utilized Autopsy, a digital forensics tool, to investigate the image's contents. Here are the steps I took:

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



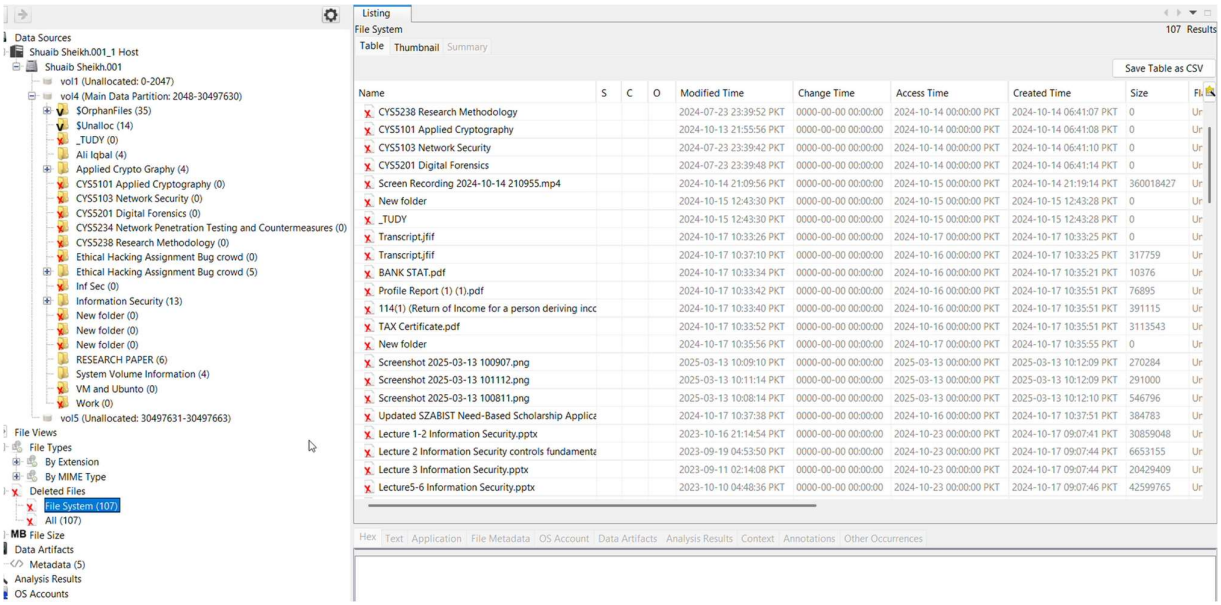
2: Entered the case name, base directory, and optional case details, such as the examiner's name, to set up the case.

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

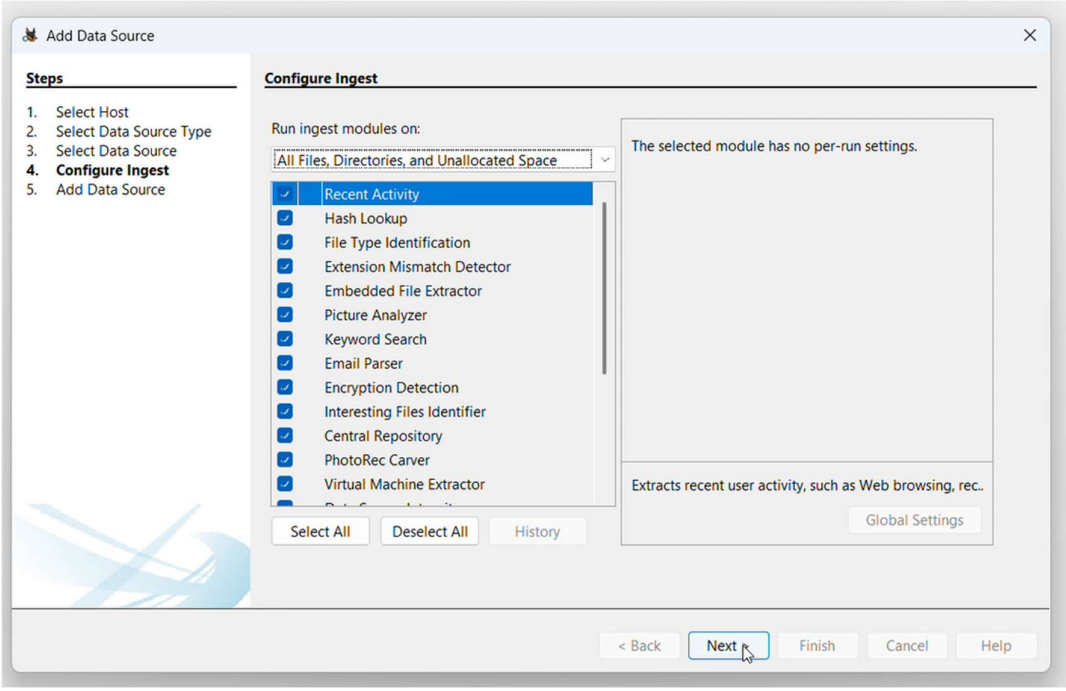


4: In the Ingest Module Configuration screen, I selected the essential modules required for analyzing files, web activity, deleted data, and keywords, then clicked "Next."

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.



USB Image Analysis Summary:



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.