Ex No-5: Use Autopsy to create a case and import evidence

AIM:

To analyze a forensic disk image using Autopsy and extract digital evidence.

Description:

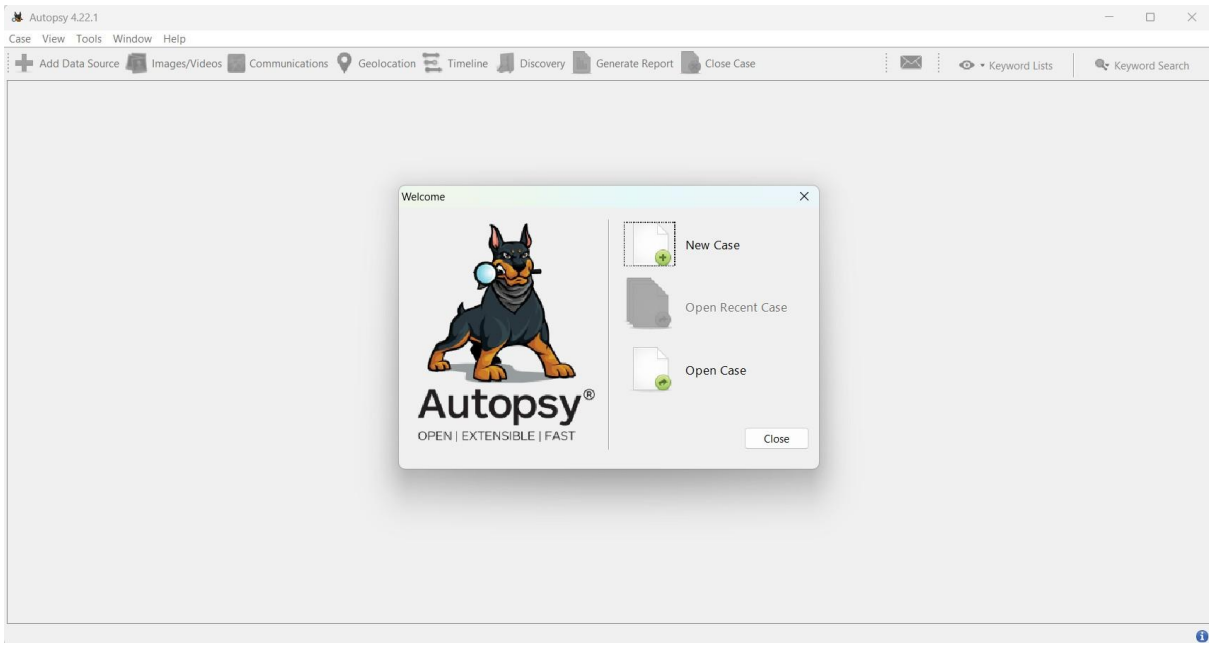
Autopsy is an open-source digital forensics platform used for analyzing and extracting data from digital devices. Here's a step-by-step process on how to use Autopsy for a basic forensic investigation.

1. Installation

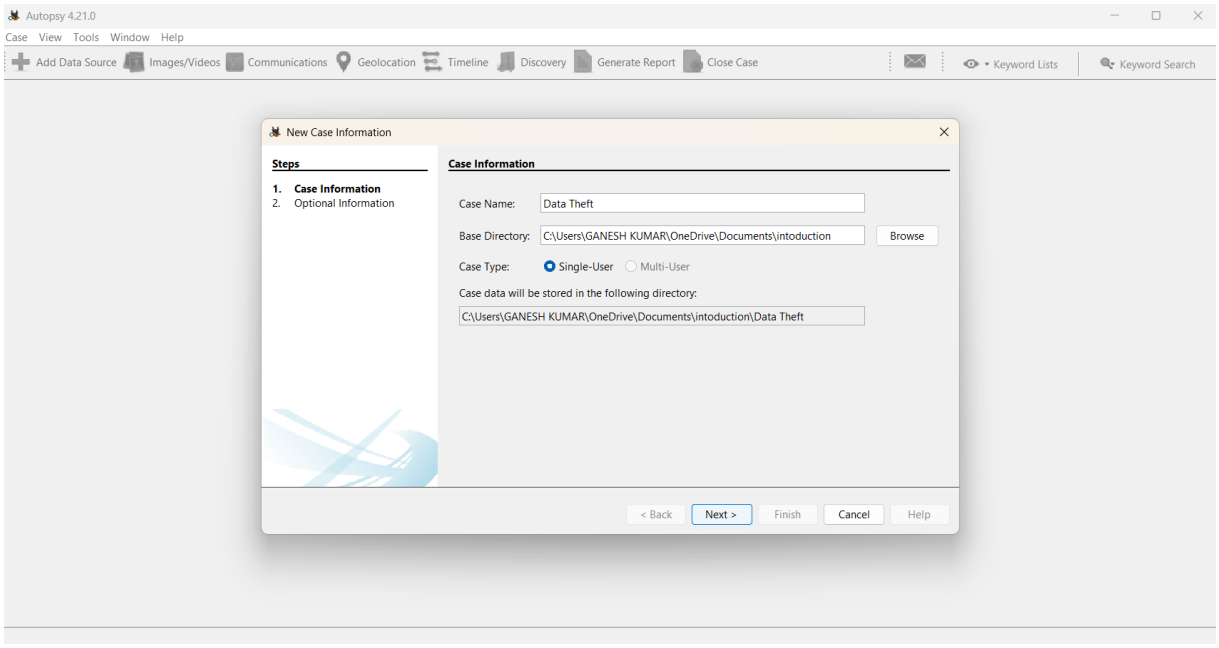
- Download and Install: Autopsy can be downloaded from the official website. Follow the installation instructions based on your operating system (Windows, Linux, or macOS).

2. Starting a New Case

- Create a new case by clicking on New Case

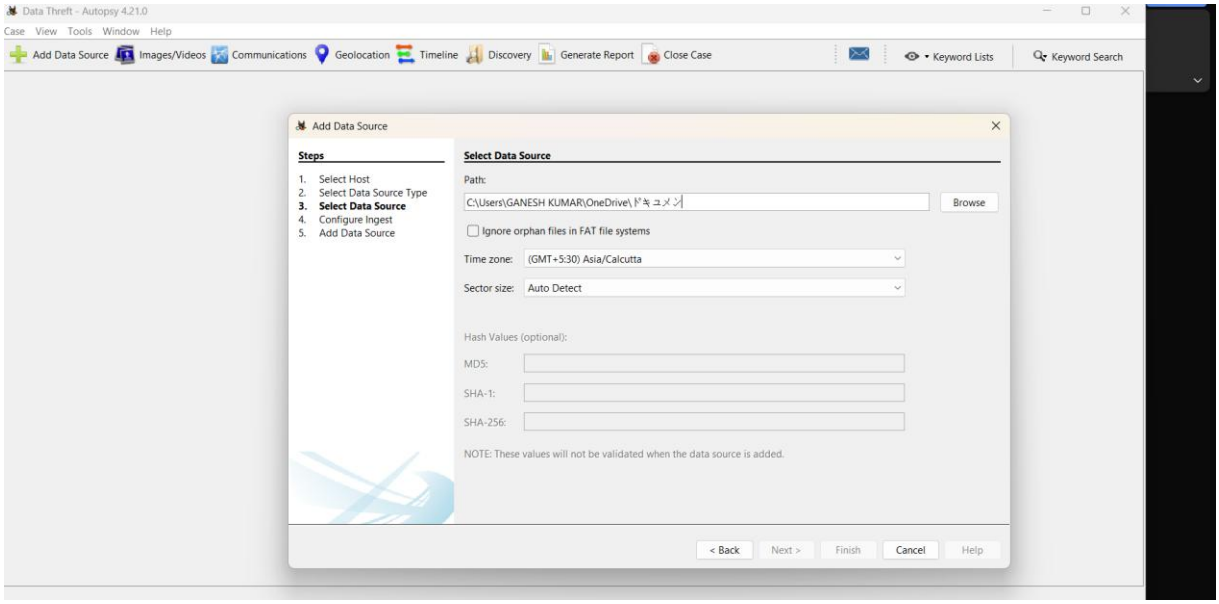


Step-2: Enter the case name and location where the case data will be stored. Fill in the details like the case number, examiner's name, etc., and click Next.



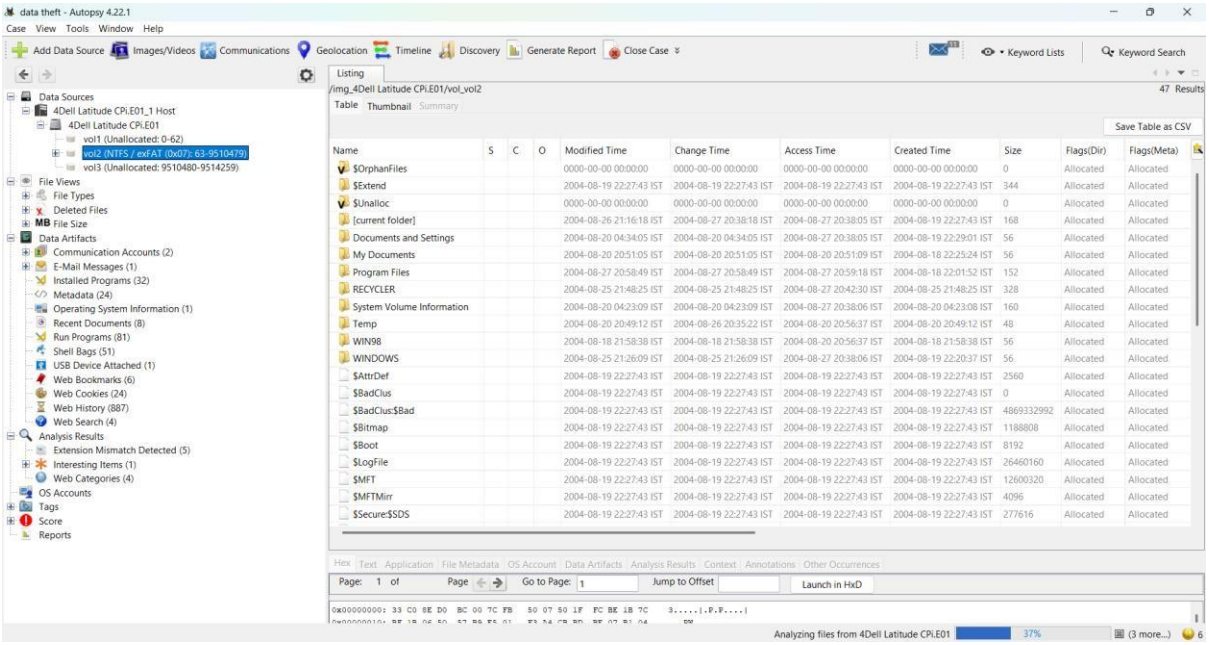
Step-3: Adding a Data Soucre

- Choose the Type of Data Source
- Select the Data Source
- Configure Ingest Modules
- Start Analysis



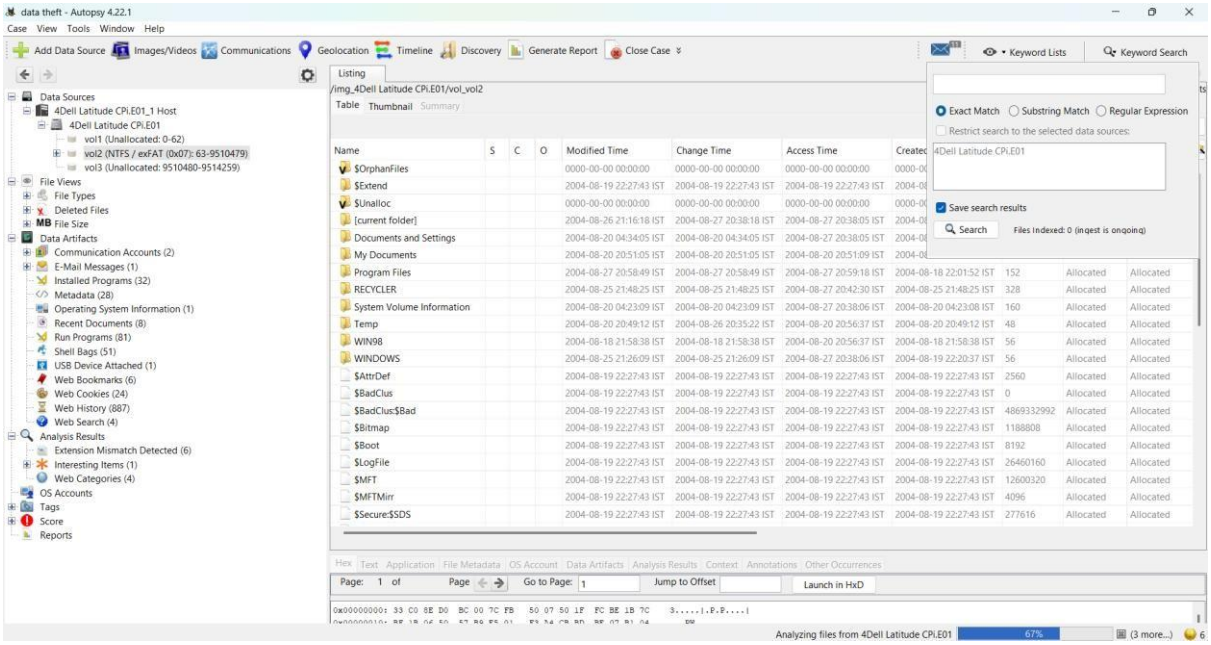
Step-4: Initial Analysis and Overview

- Ingest Progress
- Explore the Resulting Artifacts
- Use the Tree Viewer



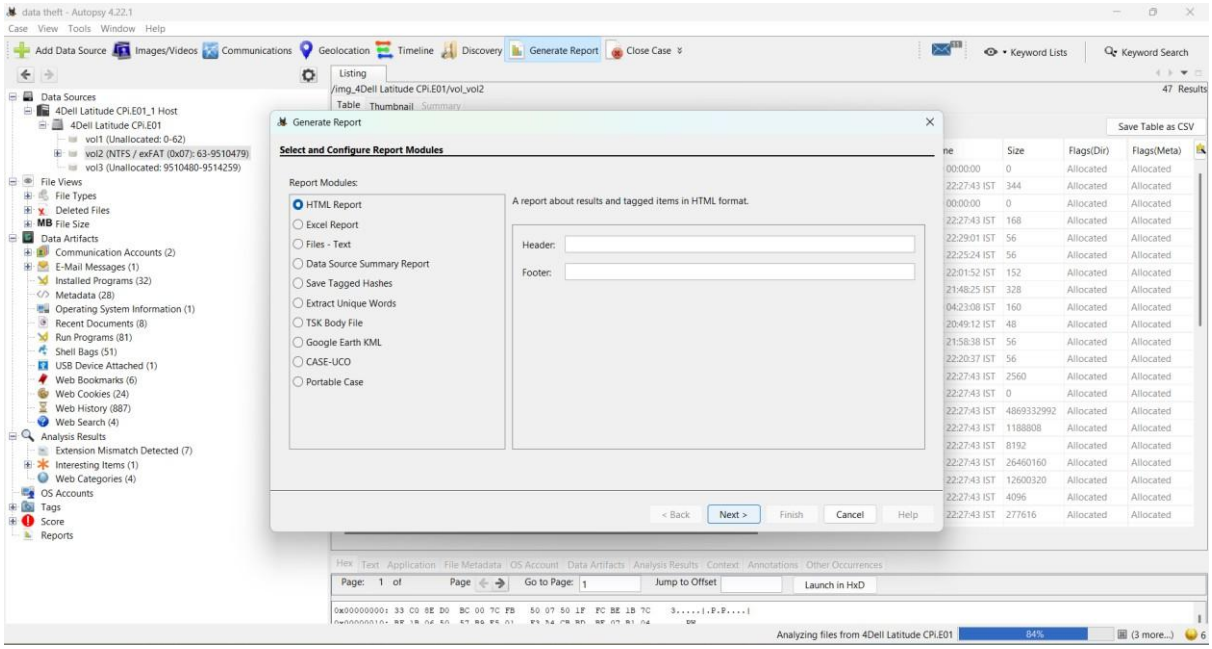
Step-5: Detailed Analysis

- Keyword Search:
- You can perform specific keyword searches using the Keyword Search module.
- Use pre-configured lists or enter custom keywords.
- File Analysis:
- Navigate through files and folders under the File Types or File System section.
- Open, view, or export files for further examination.
- Timeline Analysis:
- Use the Timeline module to visualize events based on timestamps.
- This can help track user activity over time.
- Hash Analysis:
- Compare file hashes with known databases to identify known good or bad files.

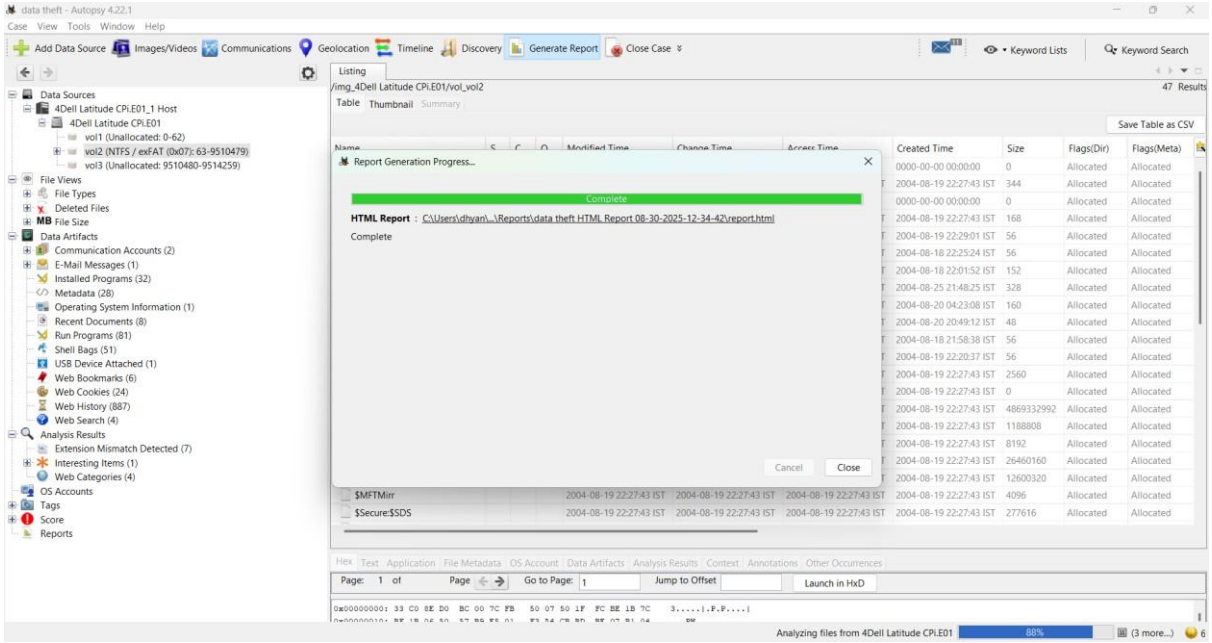


Step-6: Reporting

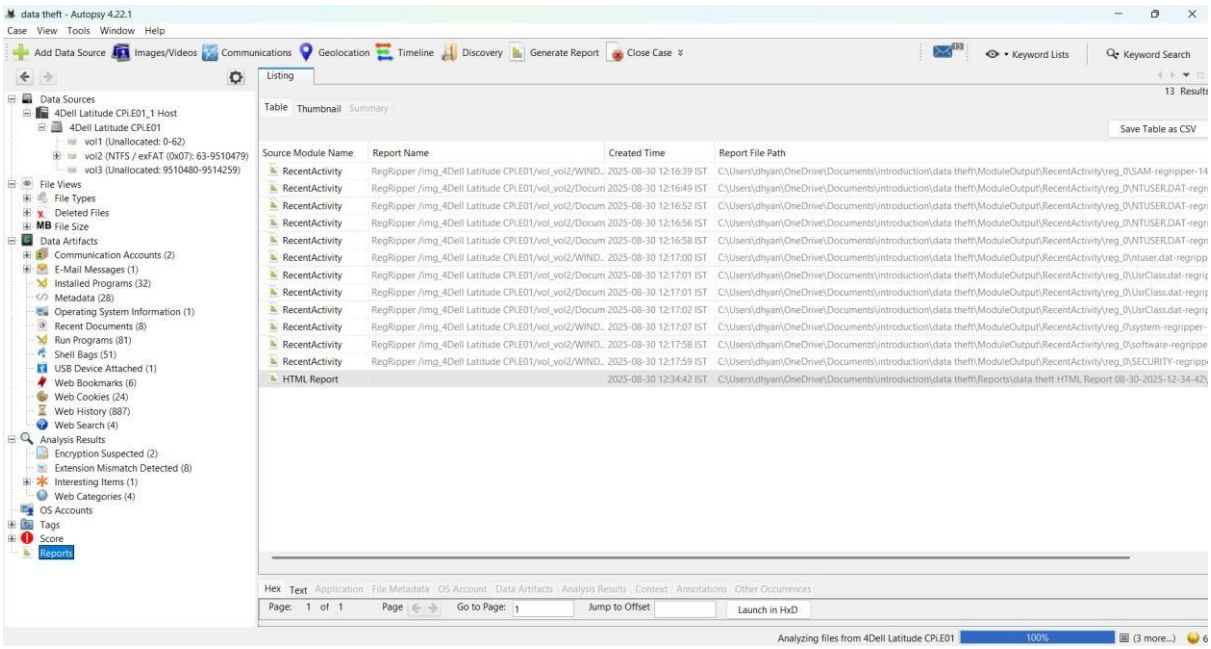
- Generate a Report:
- After analyzing the data, click on Generate Report from the toolbar.
- Choose the type of report (HTML, CSV, Excel, etc.).
- Select which parts of the analysis you want to include in the report.
- Export Findings:
- Export individual files or artifacts that you need for your report or further analysis.
- Final Review:
- Review the report to ensure it includes all relevant information.
- Save or print the report for use in your case.



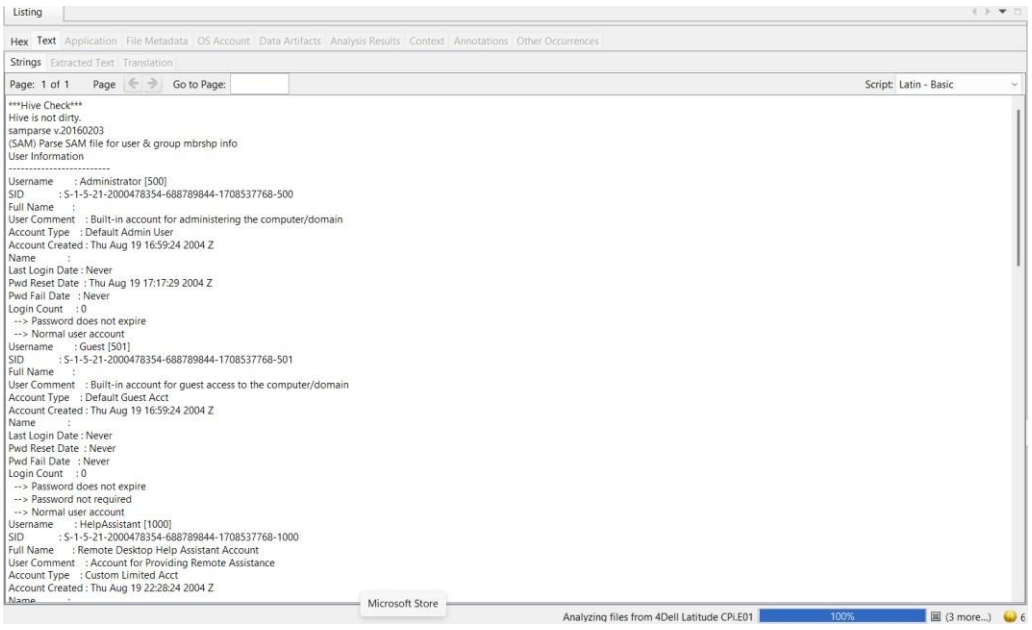
Report Generation Progress



Reports



Text in the report



Step-7: Case Closure

- Close the Case:
- Once you have completed your investigation, close the case within Autopsy.
- Archiving:
- Ensure all data and reports are properly archived according to your organization's policies.