Ex. No 5: Use Autopsy to Create a Case and Import Evidence

Aim

To perform a forensic investigation using **Autopsy**, by creating a case, importing evidence, analyzing artifacts, and generating a forensic report.

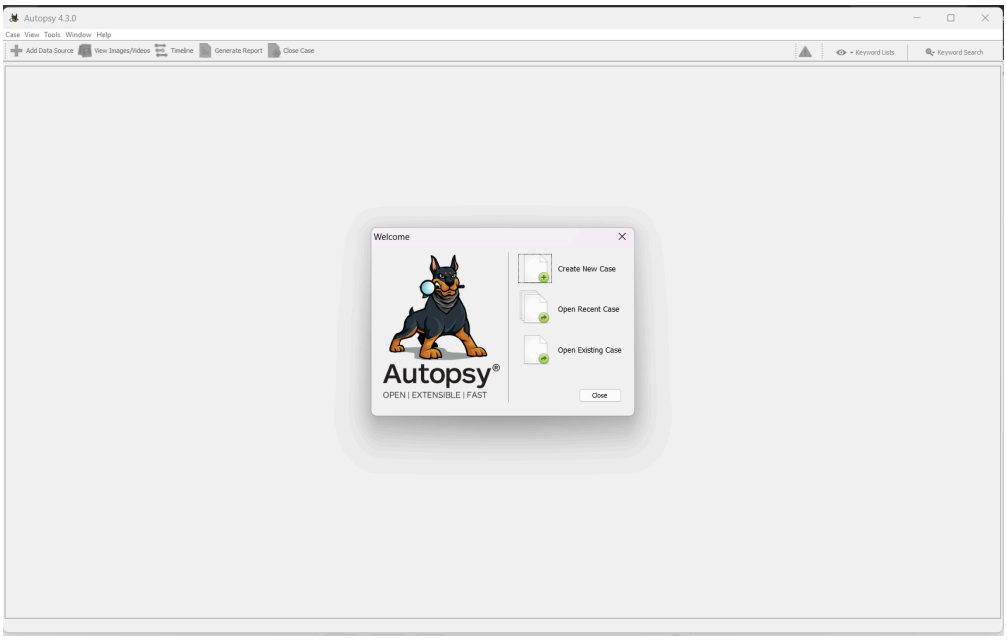
Steps

Step 1: Installation

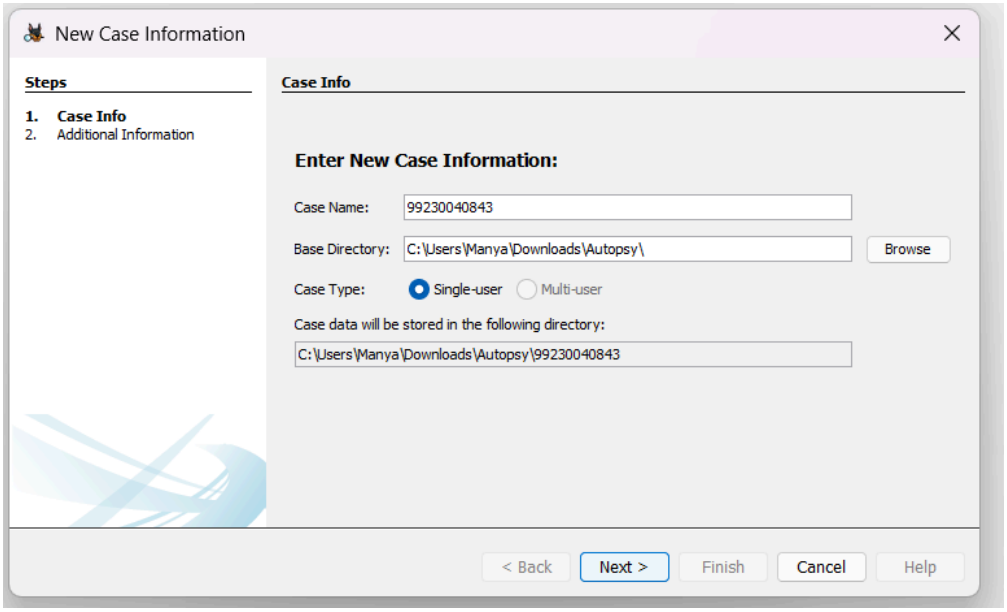
- **Download & Install** Autopsy from the official website.
- Follow installation instructions for your OS (Windows/Linux/macOS).

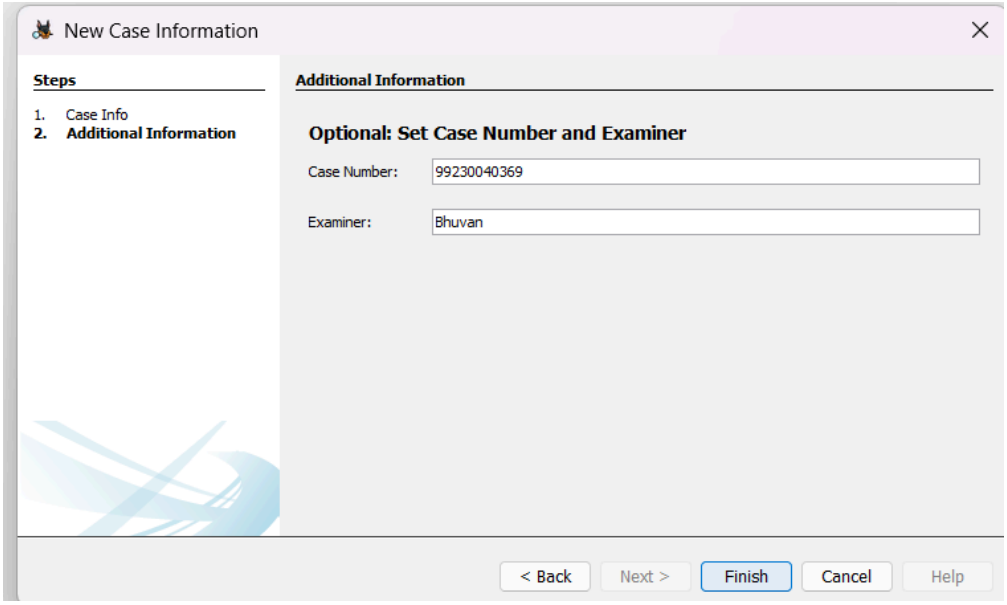
Step 2: Starting a New Case

- Open **Autopsy**.
- Click **New Case**.



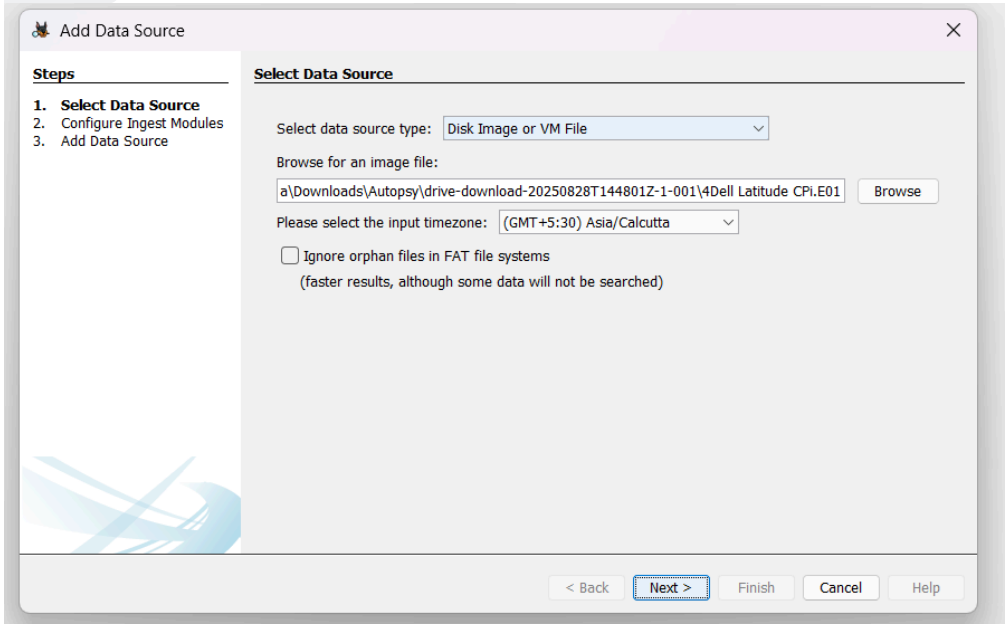
- Enter:
  - Case name
  - Case location (storage path)
  - Case number, examiner's name, etc.
- Click **Next** to proceed.





Step 3: Adding a Data Source

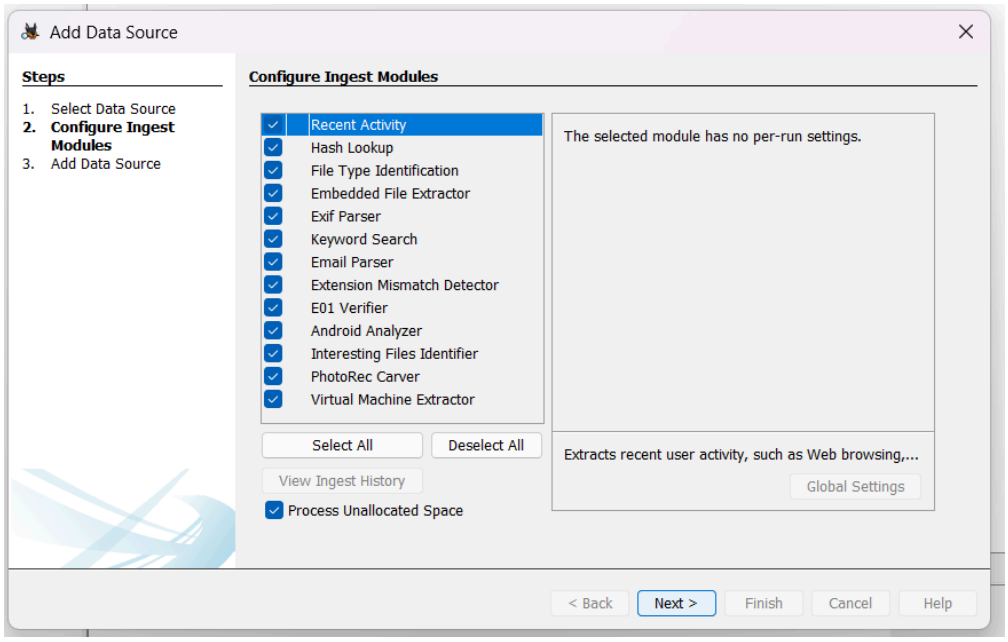
- After creating a case, Autopsy will prompt you to add a **data source**.
- Choose the source type:
  - Disk images (`.E01` , `.dd` , `.raw`)
  - Directories
  - Logical files
  - Local disks
- Browse and select the image file (e.g., `4Dell Latitude CPi.E01` , `4Dell Latitude CPi.E02`).



- **Configure Ingest Modules**:
  - File Type Identification
  - Keyword Search
  - Hash Lookup

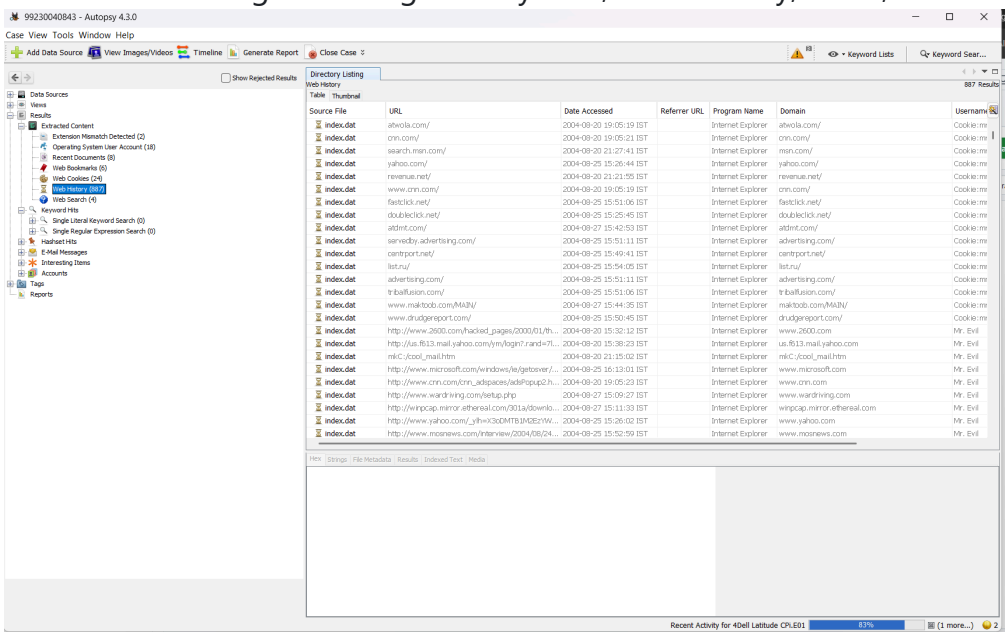
- (Enable/disable as per requirement)

- Click **Next** to start the analysis.



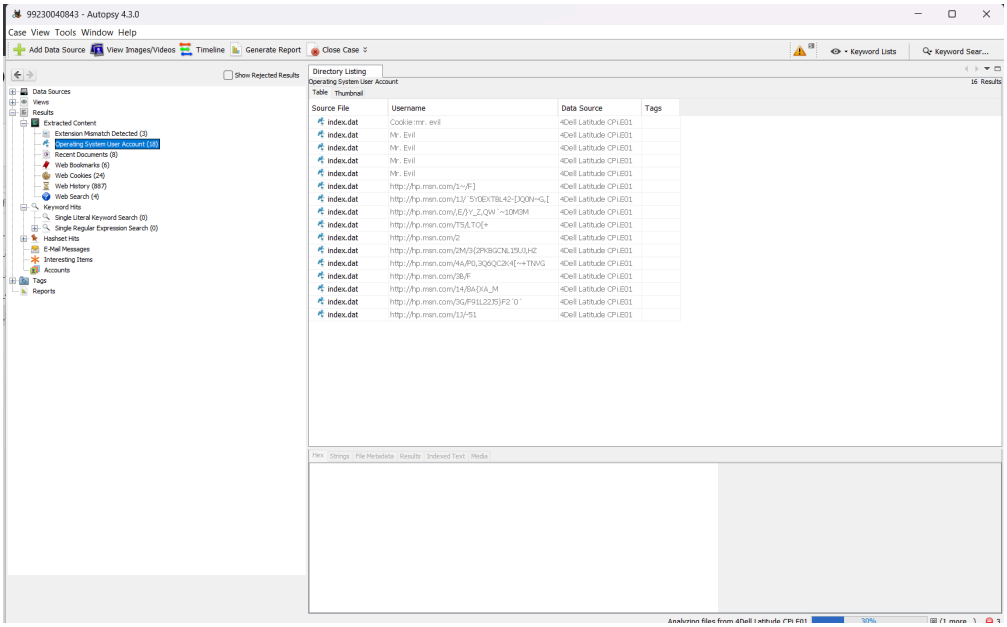
Step 4: Initial Analysis & Overview

- **Ingest Progress**: Progress is shown in the lower-left corner.
- **Artifacts Categorization**:
  - File system metadata
  - Web artifacts
  - Communication records
- **Tree Viewer**: Navigate through File System, Web History, Email, etc.



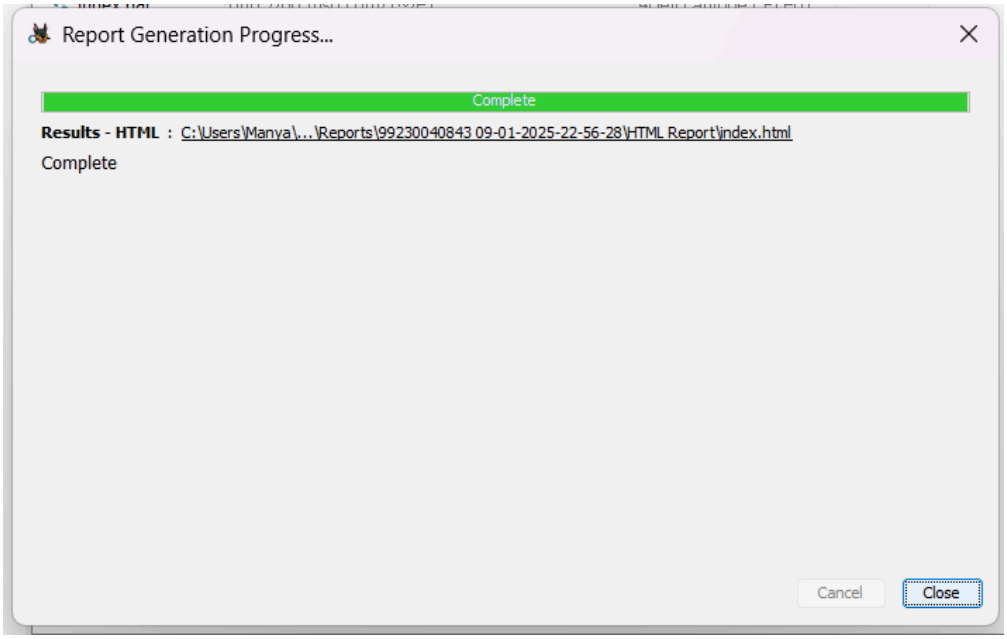
Step 5: Detailed Analysis

- **Keyword Search**: Use pre-configured or custom keyword lists.
- **File Analysis**: Open, preview, or export files.
- **Timeline Analysis**: Visualize user activity across time.
- **Hash Analysis**: Compare with known hash databases (good/bad files).



Step 6: Reporting

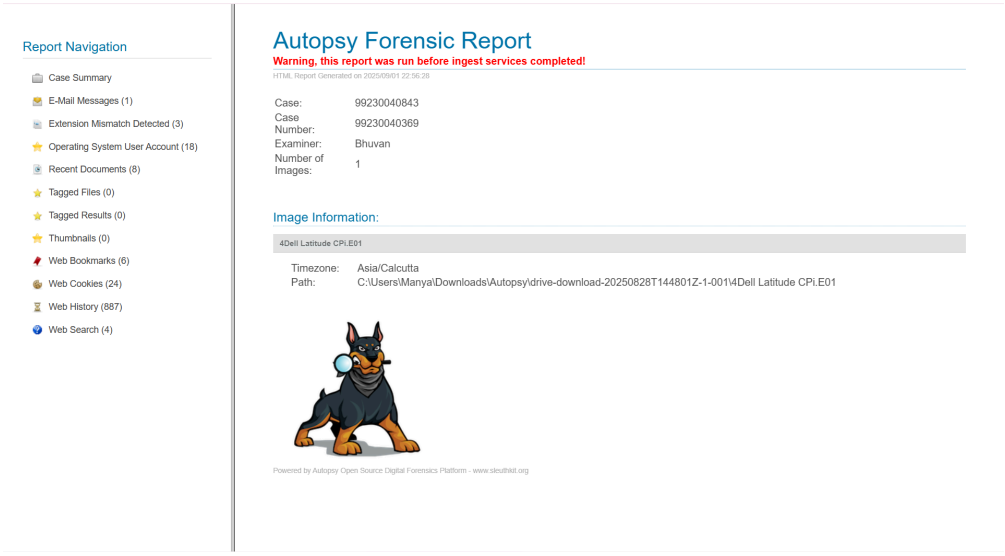
- Click **Generate Report** from the toolbar.
- Choose report type: HTML, CSV, Excel, etc.
- Select which parts of analysis to include.



- Export findings (files or artifacts). - Review and finalize the report.

Step 7: Case Closure

- Close the case in Autopsy.
- Archive data & reports as per organizational policy.



Rubrics

Criteria	Mark Allotted	Mark Awarded
1. GitHub Activity & Submission Regularity	3	
2. Application of Forensic Tools & Practical Execution	3	
3. Documentation & Reporting	2	
4. Engagement, Problem-Solving & Team Collaboration	2	
Total	10	

Result

Successfully created a case in Autopsy, imported a forensic disk image, analyzed artifacts, and generated a forensic report.