



122 lines (97 loc) · 3.66 KB

Preview

Code

Blame



Raw



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.

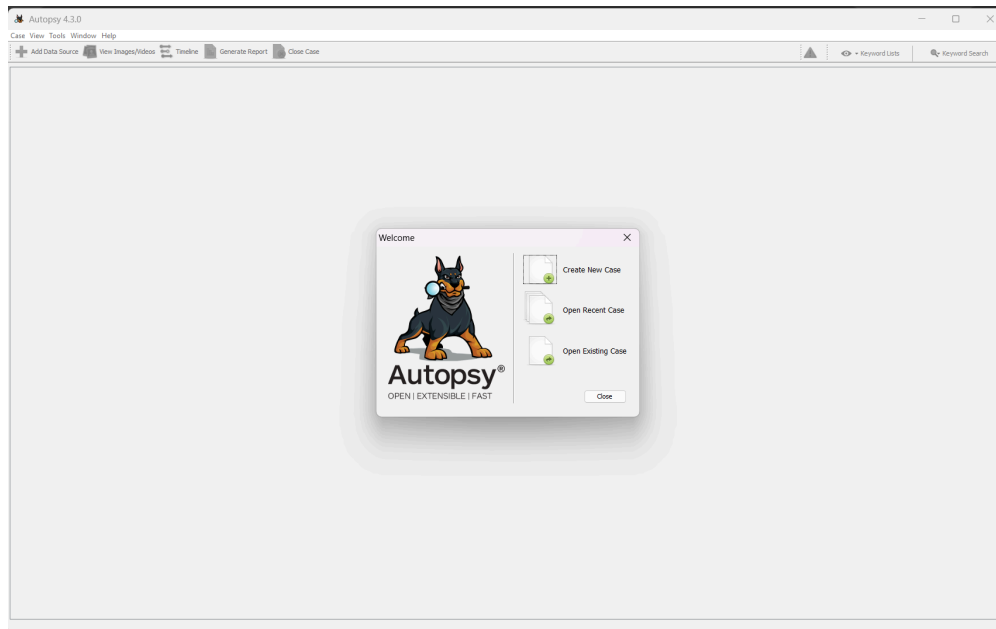
Steps

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.

New Case Information

Steps

1. Case Info
2. **Additional Information**

Additional Information

Optional: Set Case Number and Examiner

Case Number:

Examiner:

< Back Next > **Finish** Cancel Help

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`).

Add Data Source

Steps

1. **Select Data Source**
2. Configure Ingest Modules
3. Add Data Source

Select Data Source

Select data source type:

Browse for an image file:

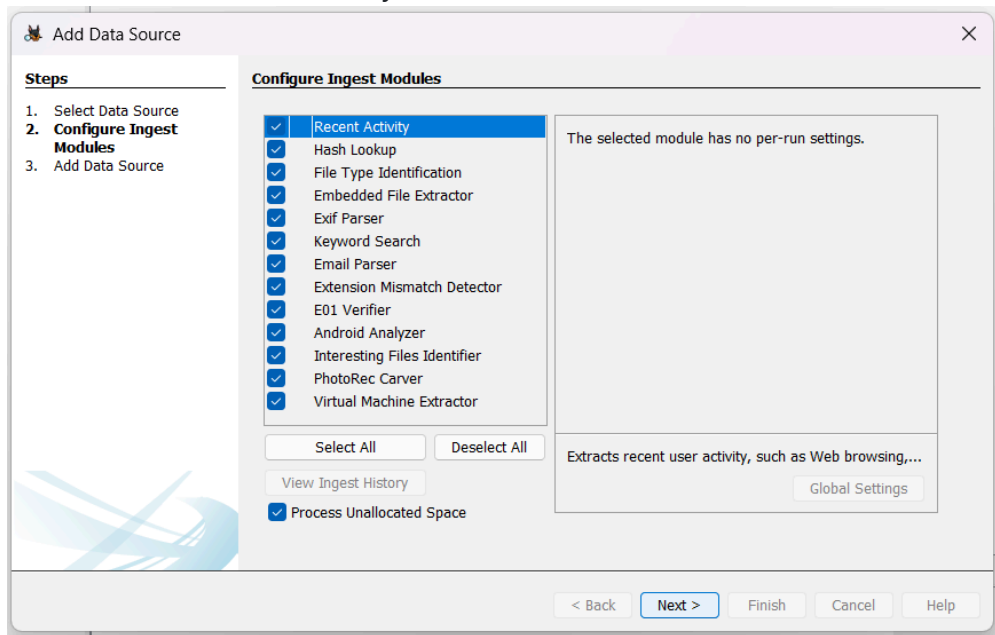
Please select the input timezone:

☐ Ignore orphan files in FAT file systems
(faster results, although some data will not be searched)

< Back **Next >** Finish Cancel Help

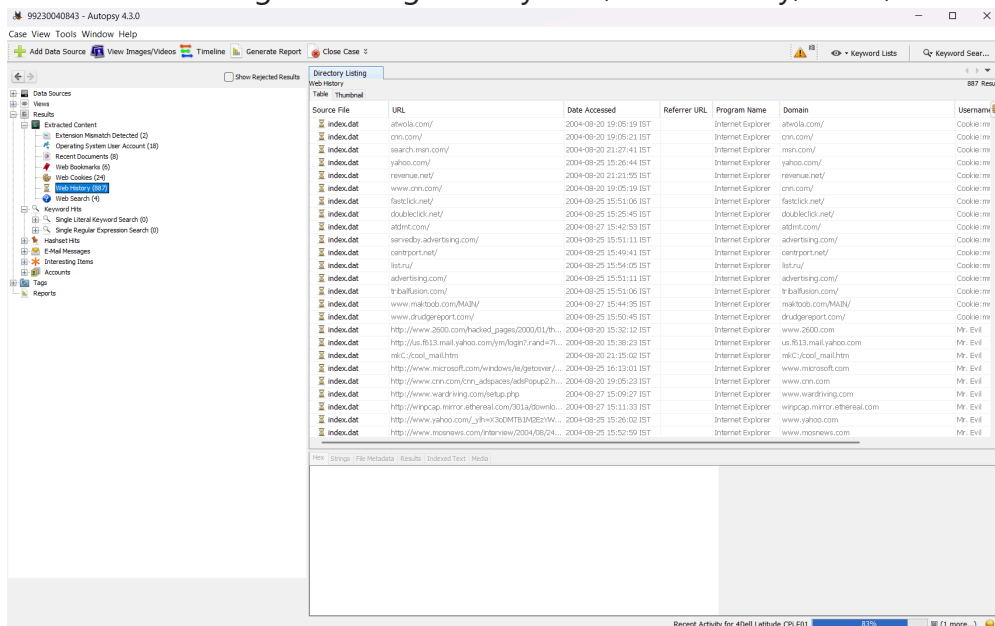
- **Configure Ingest Modules:**
 - File Type Identification
 - Keyword Search
 - Hash Lookup

- (Enable/disable as per requirement)
- Click **Next** to start the analysis.



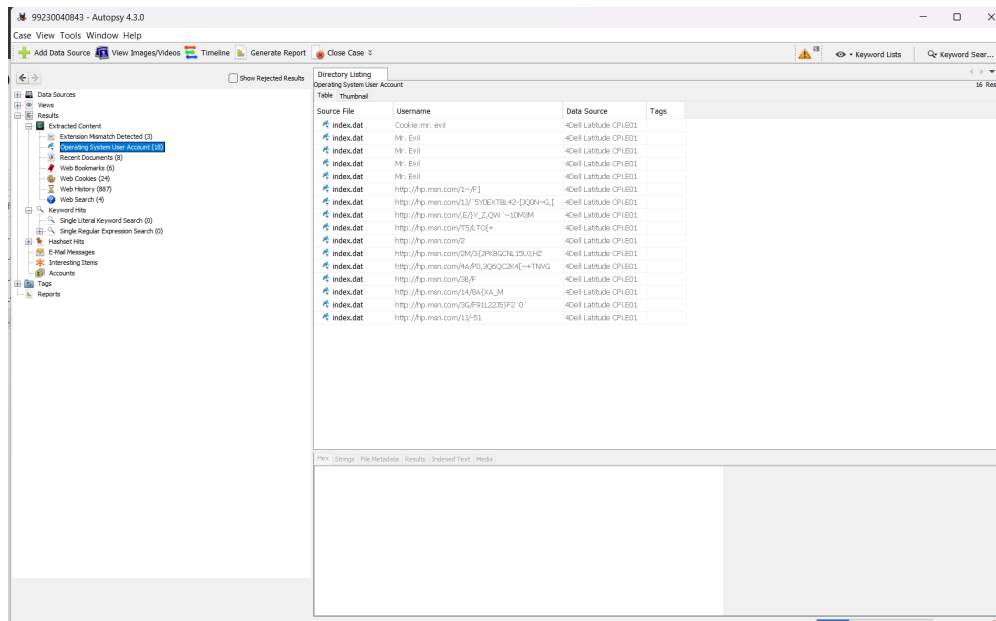
Step 4: Initial Analysis & Overview

- **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.



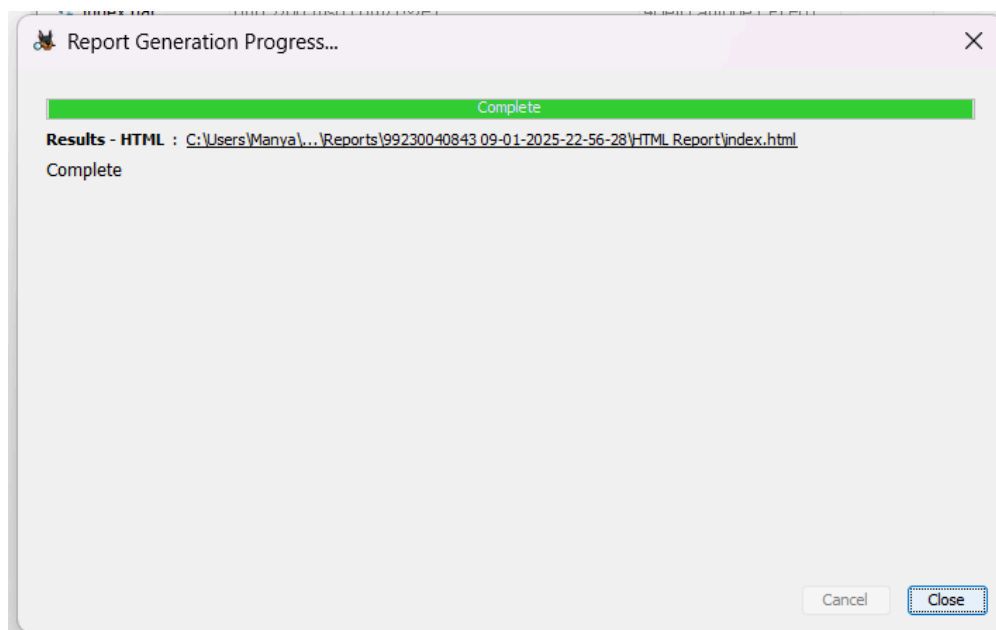
Step 5: Detailed Analysis

- **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.

Report Navigation

- Case Summary
- E-Mail Messages (1)
- Extension Mismatch Detected (3)
- Operating System User Account (18)
- Recent Documents (8)
- Tagged Files (0)
- Tagged Results (0)
- Thumbnails (0)
- Web Bookmarks (6)
- Web Cookies (24)
- Web History (887)
- Web Search (4)

Autopsy Forensic Report

Warning, this report was run before ingest services completed!


HTML Report Generated on: 2025/09/01 22:36:28

Case: 99230040843
Case Number: 99230040369
Examiner: Bhuvan
Number of Images: 1

Image Information:

4Dell Latitude CPLE01

Timezone: Asia/Calcutta
Path: C:\Users\Manyal\Downloads\Autopsy\drive-download-20250828T144801Z-1-0014Dell Latitude CPLE01



Powered by Autopsy Open Source Digital Forensics Platform - www.sleuthkit.org

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.