



Bhuvaneshwar-Naidu / DF_Lab



Code

Issues

Pull requests

Actions

Projects

Wiki

Security



DF_Lab / Exp_5_Autopsy.md



Bhuvaneshwar-Naidu Update Exp_5_Autopsy.md

ef559f8 · now



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.

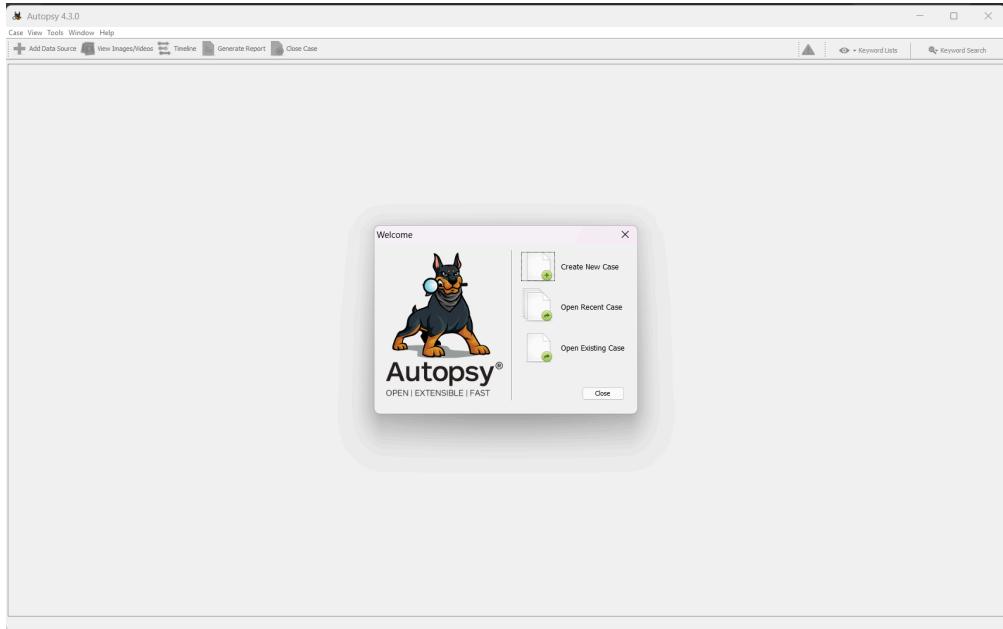
Steps

Step 1: Installation

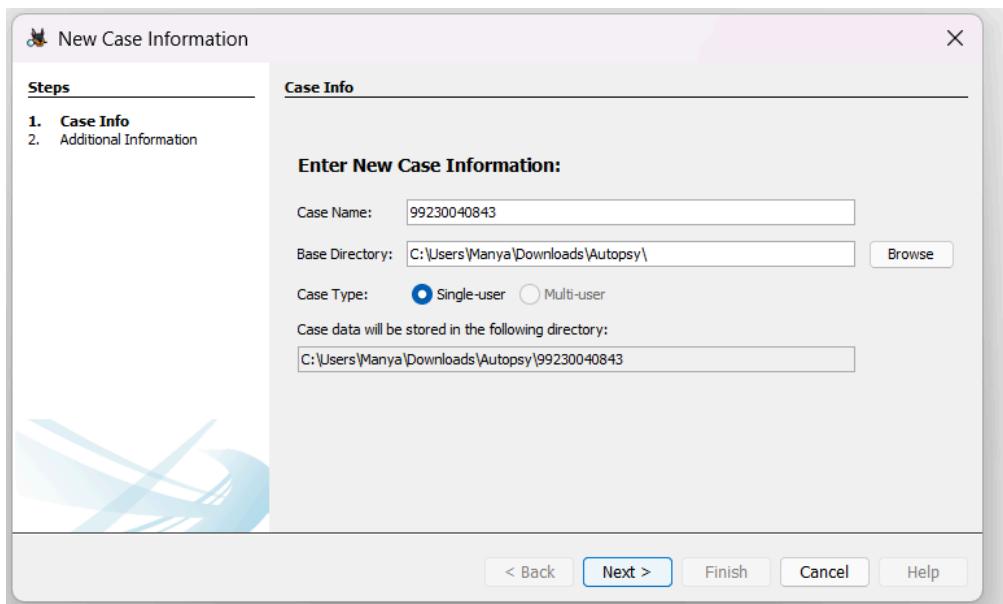
- Download & Install Autopsy from the [official website](#).
- Follow installation instructions for your OS (Windows/Linux/macOS).

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

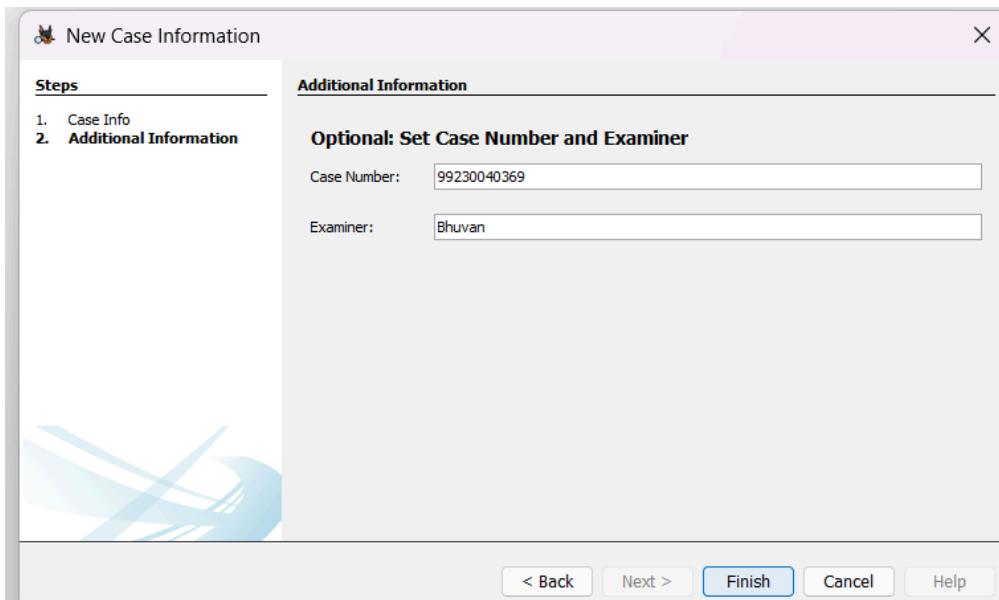
Additional Information

Optional: Set Case Number and Examiner

Case Number: 99230040369

Examiner: Bhuvan

< 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

Select Data Source

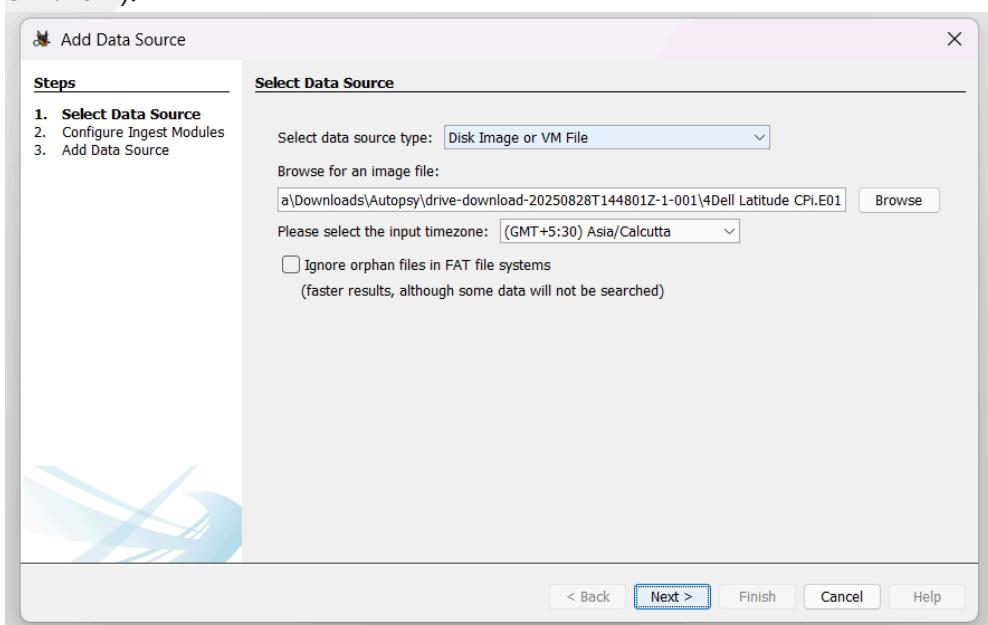
Select data source type: Disk Image or VM File

Browse for an image file:
a\Downloads\Autopsy\drive-download-20250828T144801Z-1-001\4Dell Latitude CPi.E01

Please select the input timezone: (GMT+5:30) Asia/Calcutta

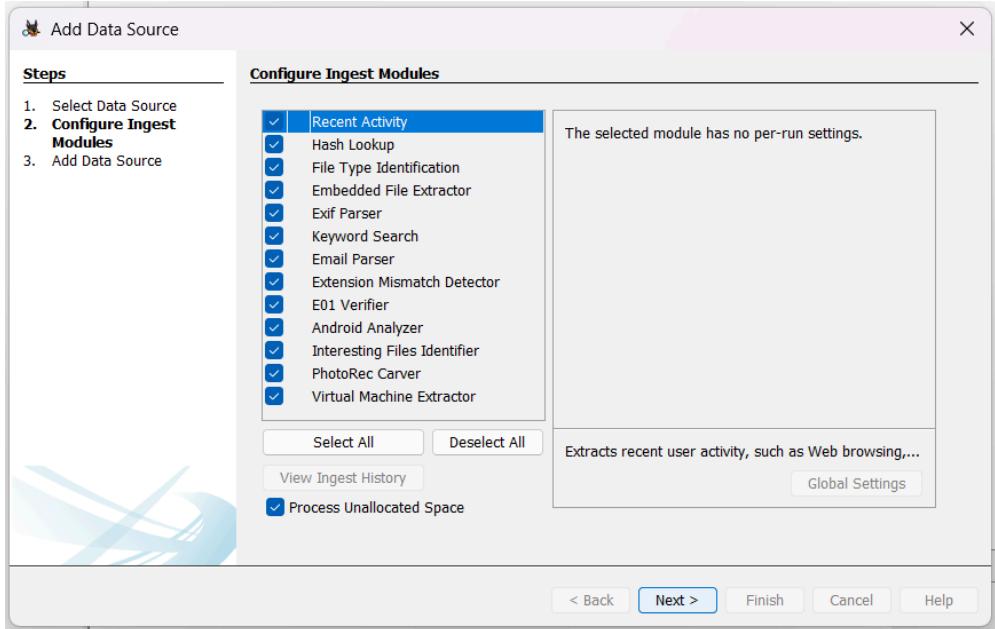
Ignore orphan files in FAT file systems
(faster results, although some data will not be searched)

< 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.



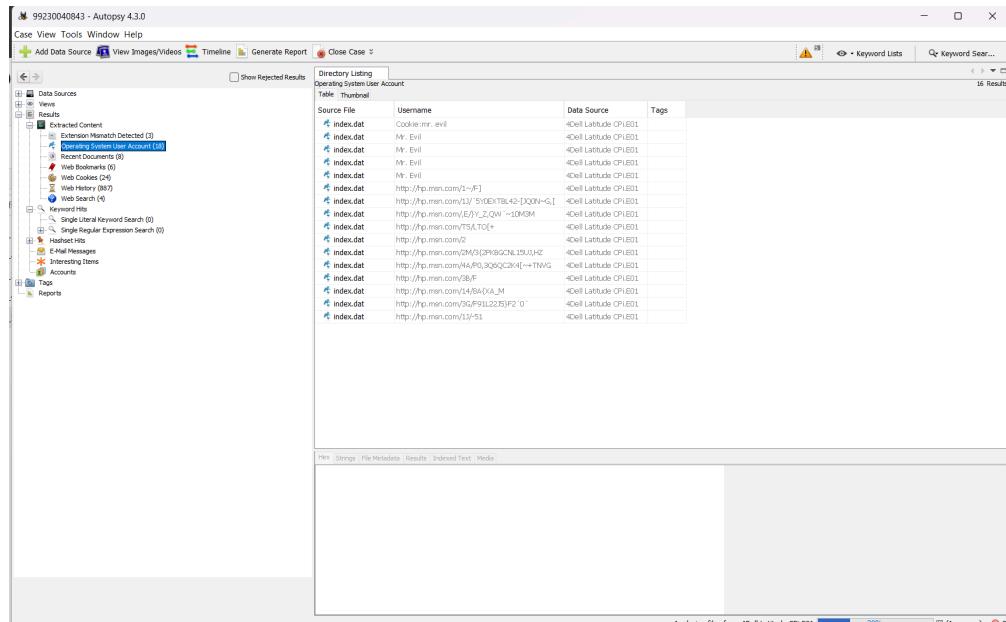
Step 4: Initial Analysis & Overview

- **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.

Source File	URL	Date Accessed	Referrer URL	Program Name	Domain	Username
index.dat	alwola.com/	2004-09-20 19:05:19 IST		Internet Explorer	alwola.com/	Cookie:m
index.dat	cnn.com/	2004-09-20 19:05:21 IST		Internet Explorer	cnn.com/	Cookie:m
index.dat	search.msn.com/	2004-09-20 21:27:41 IST		Internet Explorer	msn.com/	Cookie:m
index.dat	yahoo.com/	2004-09-25 15:26:44 IST		Internet Explorer	yahoo.com/	Cookie:m
index.dat	revenue.net/	2004-09-20 21:21:50 IST		Internet Explorer	revenue.net/	Cookie:m
index.dat	www.cnn.com/	2004-09-20 19:05:19 IST		Internet Explorer	cnn.com/	Cookie:m
index.dat	fastclick.net/	2004-09-25 15:51:06 IST		Internet Explorer	fastclick.net/	Cookie:m
index.dat	doubleclick.net/	2004-09-25 15:25:45 IST		Internet Explorer	doubleclick.net/	Cookie:m
index.dat	admt.com/	2004-09-27 15:42:53 IST		Internet Explorer	admt.com/	Cookie:m
index.dat	servedby.advertising.com/	2004-09-25 15:51:11 IST		Internet Explorer	advertising.com/	Cookie:m
index.dat	comcast.net/	2004-09-25 15:54:03 IST		Internet Explorer	comcast.net/	Cookie:m
index.dat	lulu.com/	2004-09-25 15:54:03 IST		Internet Explorer	lulu.com/	Cookie:m
index.dat	advertising.com/	2004-09-25 15:51:12 IST		Internet Explorer	advertising.com/	Cookie:m
index.dat	tr.balfusion.com/	2004-09-25 15:51:05 IST		Internet Explorer	tr.balfusion.com/	Cookie:m
index.dat	www.mal-tools.com/MALIN/	2004-09-27 15:44:35 IST		Internet Explorer	mal-tools.com/MALIN/	Cookie:m
index.dat	www.drudgereport.com/	2004-09-25 15:50:45 IST		Internet Explorer	drudgereport.com/	Cookie:m
index.dat	http://www.2000.com/hacked_pages/2000/01/.../	2004-09-20 15:32:12 IST		Internet Explorer	www.2000.com	Mr_Evil
index.dat	http://us.8113.mail.yahoo.com/ym/login/rand=1.../	2004-09-20 15:38:23 IST		Internet Explorer	us.8113.mail@yahoo.com	Mr_Evil
index.dat	mIC_cool_mailltm	2004-09-20 21:15:02 IST		Internet Explorer	mIC_cool_mailltm	Mr_Evil
index.dat	http://www.microsoft.com/windows/e/getserver/...	2004-09-25 16:13:01 IST		Internet Explorer	www.microsoft.com	Mr_Evil
index.dat	http://www.cnn.com/cnn/adspages/adPopUp2.../	2004-09-20 19:05:23 IST		Internet Explorer	www.cnn.com	Mr_Evil
index.dat	http://www.ward.living.com/setup.php	2004-09-27 15:09:27 IST		Internet Explorer	www.ward.living.com	Mr_Evil
index.dat	http://www.yahoo.mirror.ethereal.com/201a/brownr...	2004-09-27 15:11:33 IST		Internet Explorer	wncap.mirror.ethereal.com	Mr_Evil
index.dat	http://www.yahoo.com_jwh/X3DMMTB1M0E1W...	2004-09-25 15:26:02 IST		Internet Explorer	www.yahoo.com	Mr_Evil
index.dat	http://www.msnnews.com/interview/2004/08/24.../	2004-09-25 15:32:59 IST		Internet Explorer	www.msnnews.com	Mr_Evil

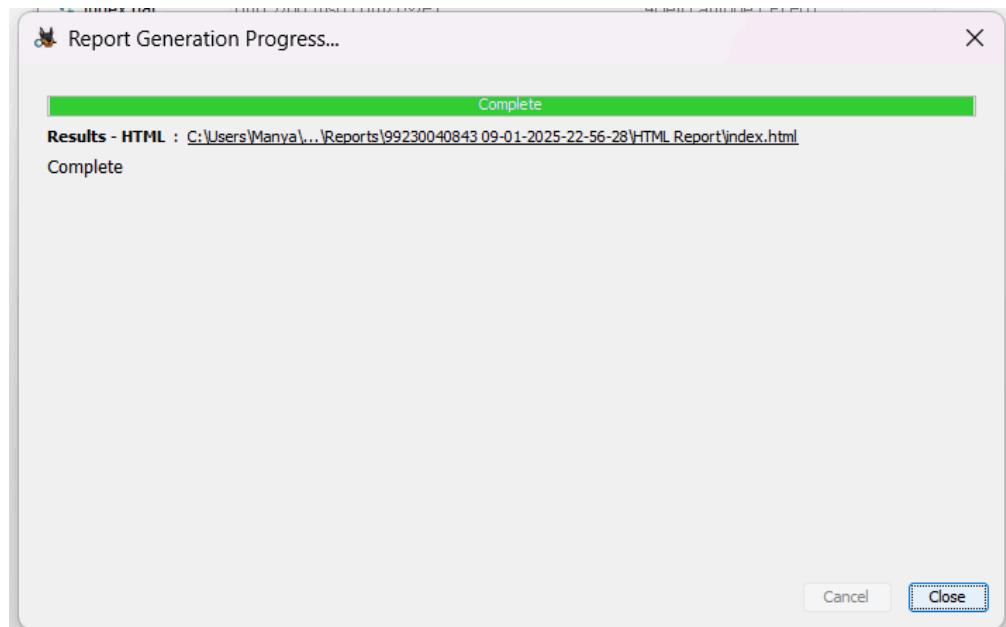
Step 5: Detailed Analysis

- **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

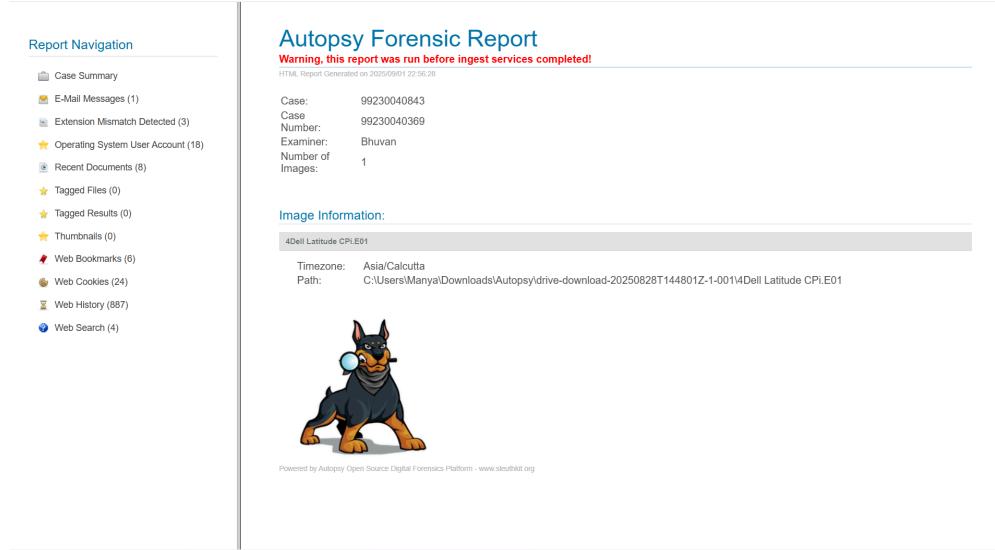
- Click **Generate Report** from the toolbar.
- Choose report type: HTML, CSV, Excel, etc.
- Select which parts of analysis to include.



- 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.



The screenshot shows the Autopsy Forensic Report interface. On the left, there is a 'Report Navigation' sidebar with various links such as Case Summary, E-Mail Messages, Extension Mismatch Detected, Operating System User Account, Recent Documents, Tagged Files, Tagged Results, Thumbnails, Web Bookmarks, Web Cookies, Web History, and Web Search. The main area is titled 'Autopsy Forensic Report' and contains a warning message: 'Warning, this report was run before ingest services completed!'. It shows case details: Case: 99230040843, Case Number: 99230040369, Examiner: Bhuvan, and Number of Images: 1. Below this is an 'Image Information' section with a sub-section for '4Dell Latitude CPI:E01'. It shows Timezone: Asia/Calcutta and Path: C:\Users\Manya\Downloads\Autopsy\drive-download-20250828T144801Z-1-0014Dell Latitude CPI:E01. At the bottom, there is a small illustration of a Doberman Pinscher holding a ball in its mouth.

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.