Assignment - 6

of

Cyber Security Laboratory

(CSE612)

Bachelor of Technology (CSE)

By

Ramoliya Kaushal (22000409)

Third Year, Semester 6

Course In-charge: Prof. Ninad Bhavsar

Department of Computer Science and Engineering

School Engineering and Technology

Navrachana University, Vadodara

Spring Semester

(2025)

Q1. Install Autopsy Sleuthkit using the following link:

https://www.sleuthkit.org/autopsy/download.php

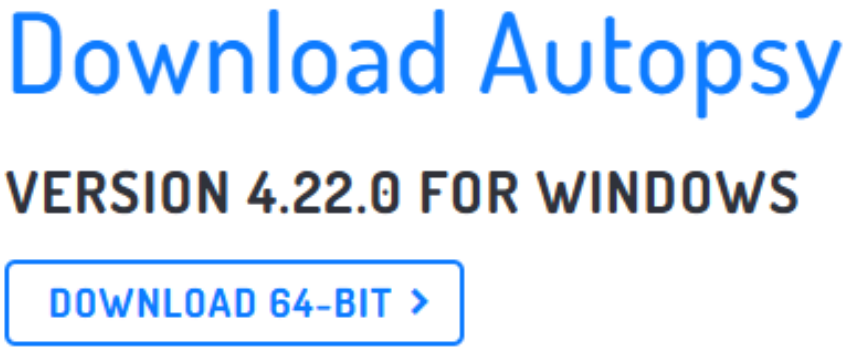
Step-by-Step Installation Guide for Autopsy Sleuthkit (Windows)

Step 1: Download Autopsy

- Open your web browser and navigate to the official Autopsy download page:

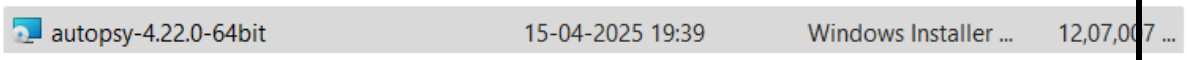
  https://www.sleuthkit.org/autopsy/download.php

- **Click on "Download 64-bit" under the "Version 4.22.0 for Windows" section.**

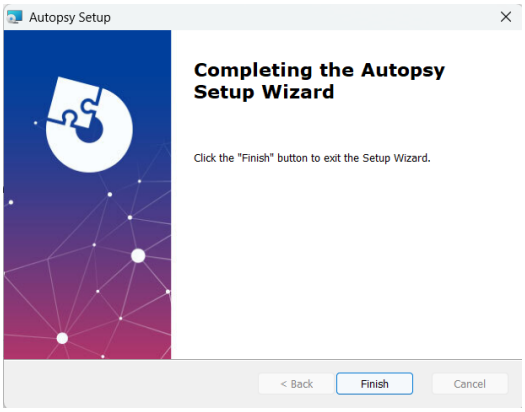


Step 2: Run the Installer

- Locate the downloaded .msi file (e.g., autopsy-4.22.0-64bit.msi) in your Downloads folder.



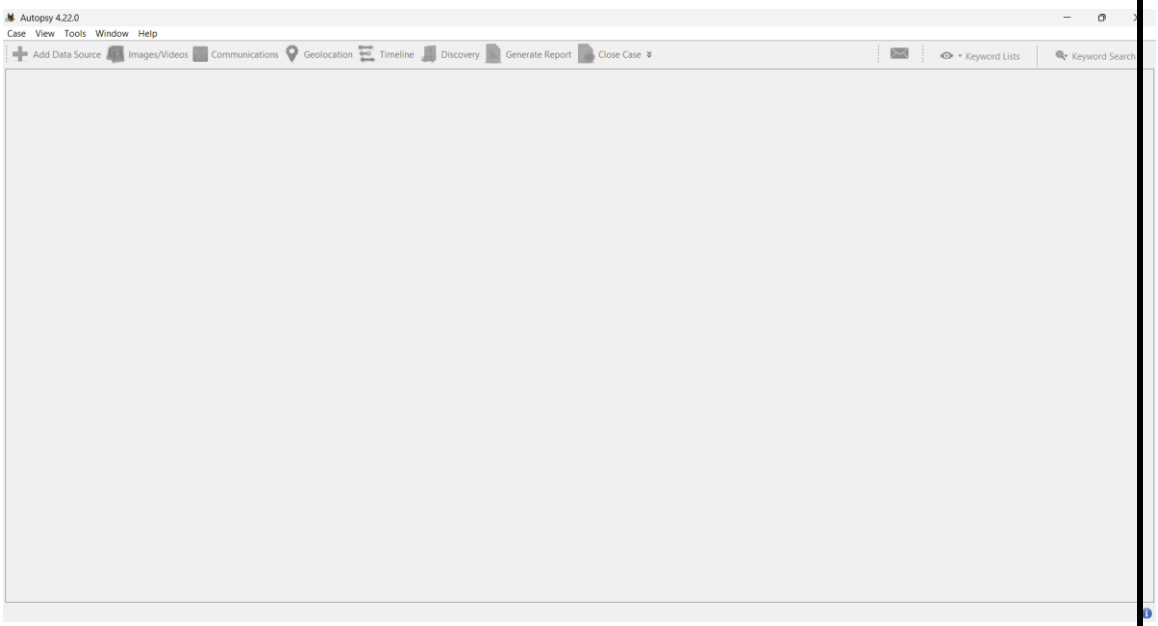
- Double-click the installer to launch it.
- If prompted by User Account Control, click "Yes" to allow the installation.
- Follow the installation wizard:
  - Click "Next" to proceed.
  - Accept the license agreement and click "Next".
  - Choose the installation directory or leave it as default, then click "Next".
  - Click "Install" to begin the installation.
  - Once completed, click "Finish".



Step 3: Launch Autopsy

- After installation, you can launch Autopsy by:
  - Clicking on the Autopsy shortcut on your desktop, or
  - Navigating to Start Menu > Autopsy.

- The Autopsy application will open, and you can start creating or opening cases.



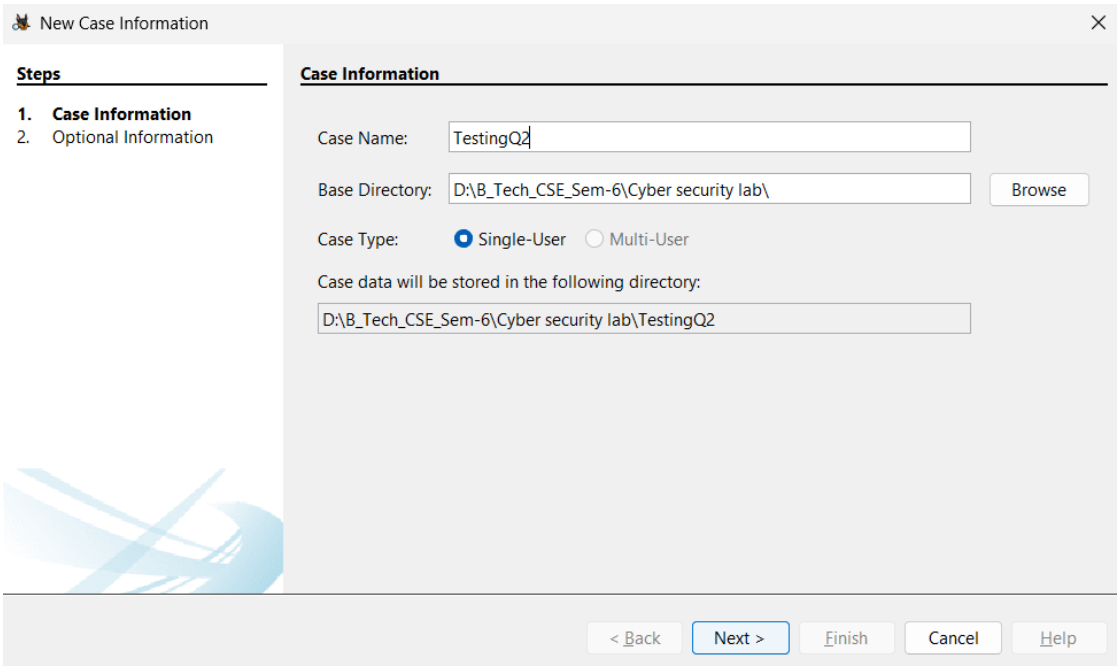
Q2. Demonstrate how the given tool can be used to detect files with deceptive extensions.

Step 1: Open Autopsy

- Launch Autopsy from Start Menu or Desktop.

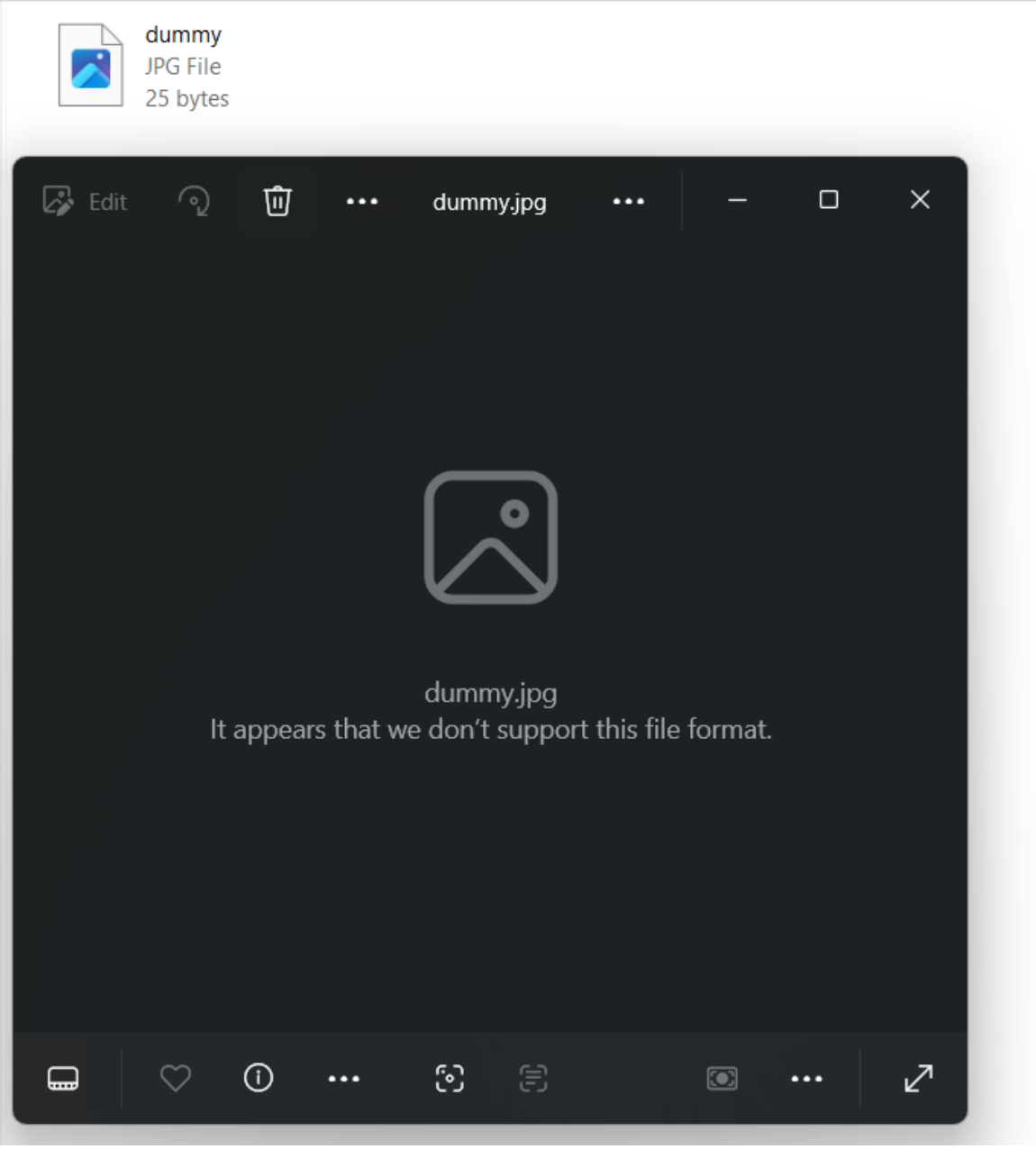
Step 2: Create a New Case

- Click on **"Create New Case"**
- Enter a Case Name (e.g., DeceptiveFilesTest)
- Choose a base directory and click **Next**, then **Finish**



Step 3: Add Data Source

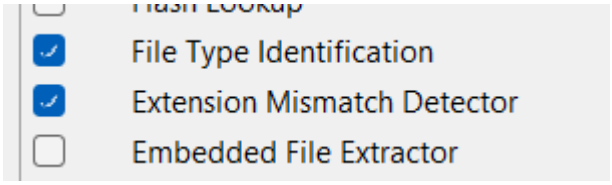
- Click on **"Add Data Source"**
- Choose Disk Image or VM file
- Load the image and proceed



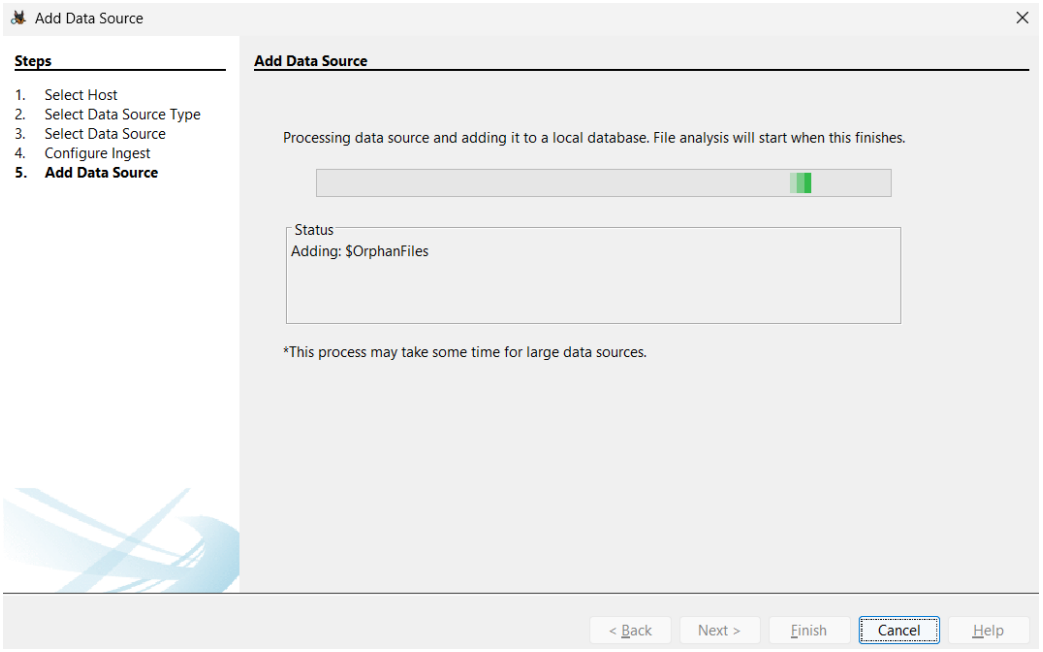
Step 4: Run Ingest Modules

Ensure the following modules are selected:

- File Type Identification
- Extension Mismatch Detector

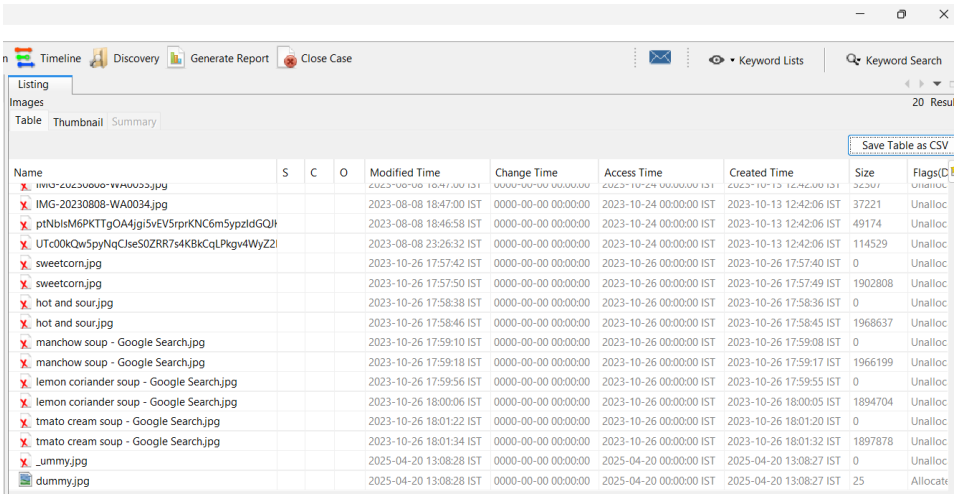


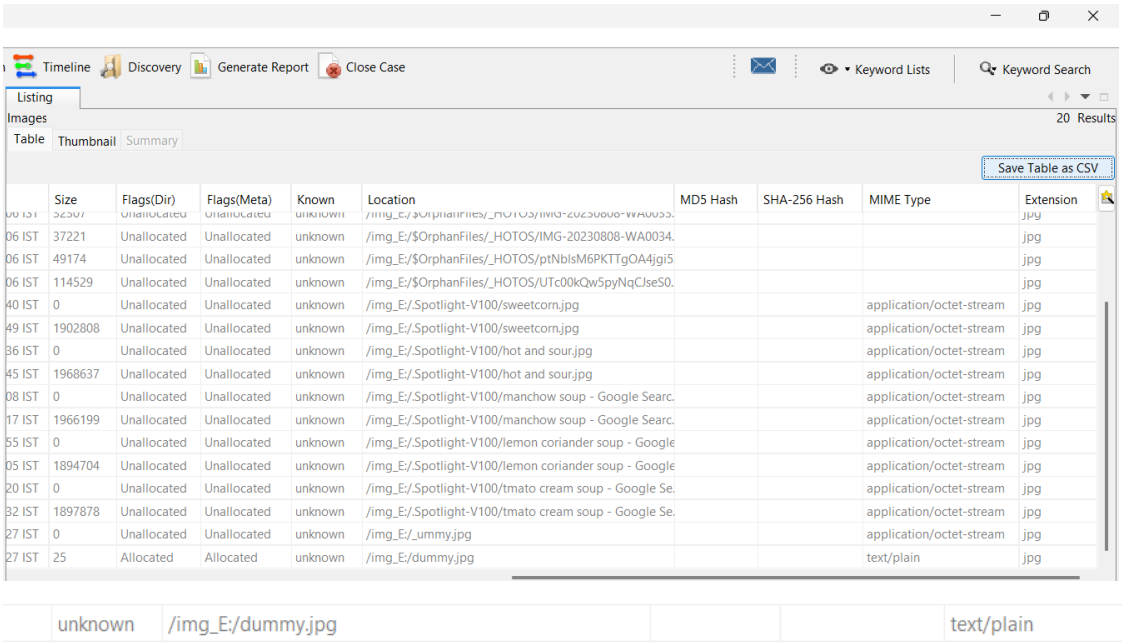
- Click Next and wait for the analysis to complete



Step 5: View Results

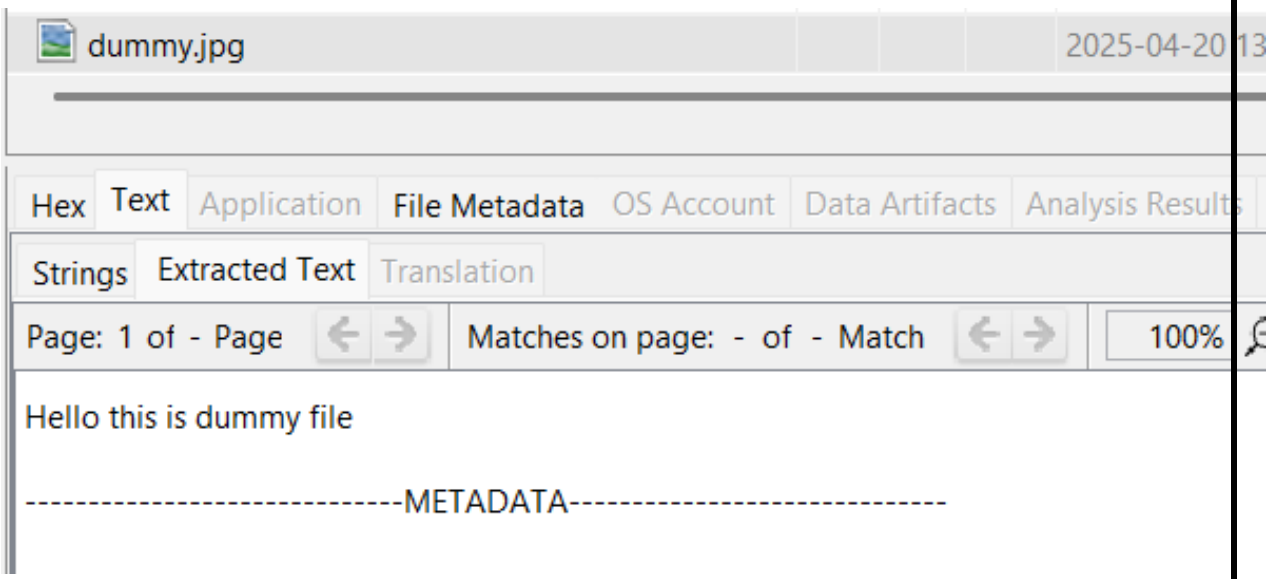
- On the left panel, go to:
  - Results → Extension Mismatch Detected
- Click to expand — this will show all files where the extension doesn't match the actual file type.





Step 6: Investigate Suspicious Files

- Right-click on any suspicious file
- Choose "View in Hex" or "View in Text"
- Use the metadata to understand its real content.



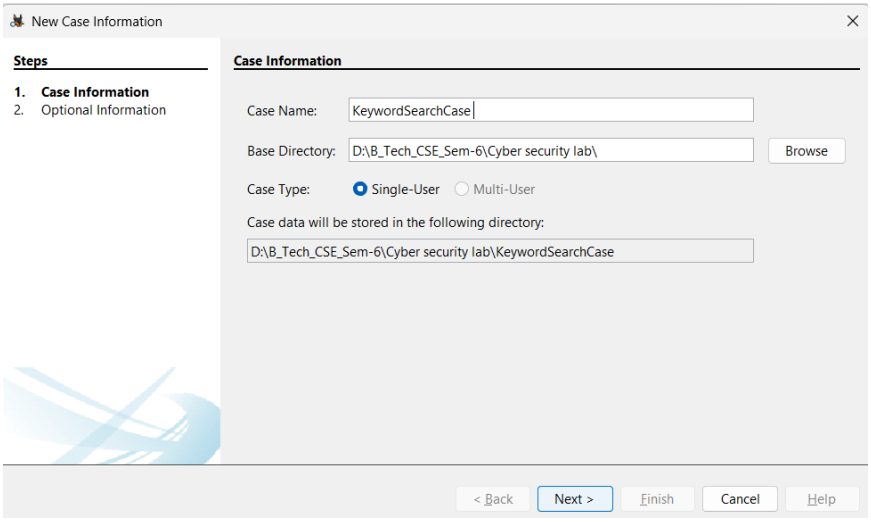
Conclusion: -

Autopsy's Extension Mismatch Detection module is a powerful tool in digital forensics. It automatically scans for files where the extension does not match the actual file type, helping investigators identify potentially harmful or disguised files. This is crucial for detecting malware, phishing content, or intentionally disguised files in criminal investigations.

Q3. Demonstrate how the given tool can be used to perform keyword search through given files where keywords are of the type IP address and URL/Email address.

Step 1: Launch Autopsy

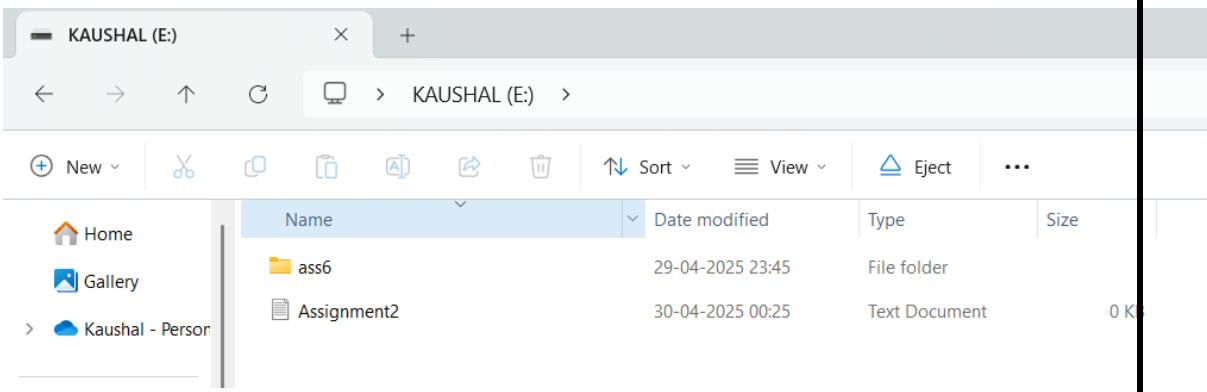
- Open Autopsy.
- Click on "Create New Case" → give it a name like KeywordSearchCase and choose a location.

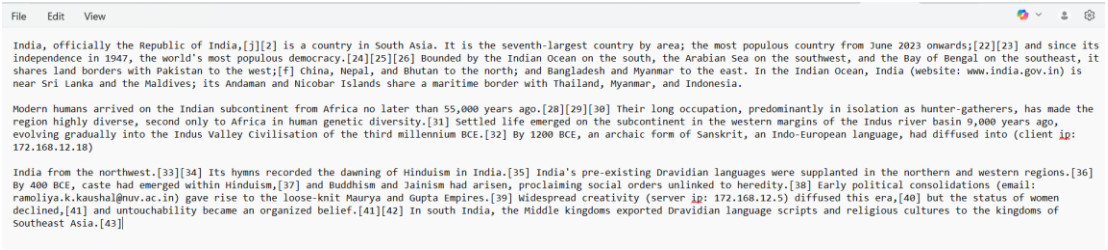


- Click Next and then Finish to start the case.

Step 2: Add Data Source

- **Now add the data source like in Q2:**
  - Click "Add Data Source".
  - Browse and select your txt file

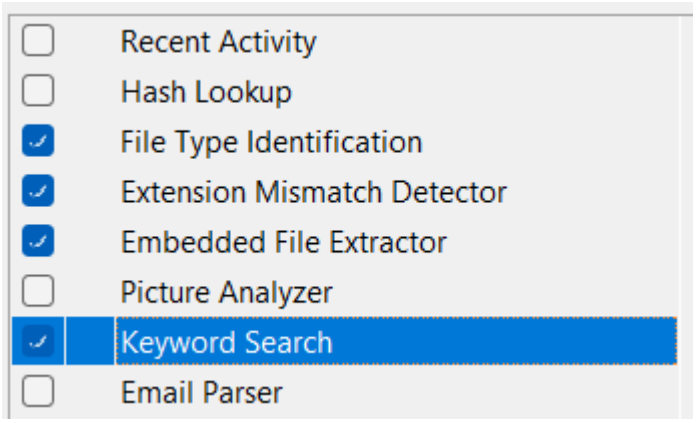




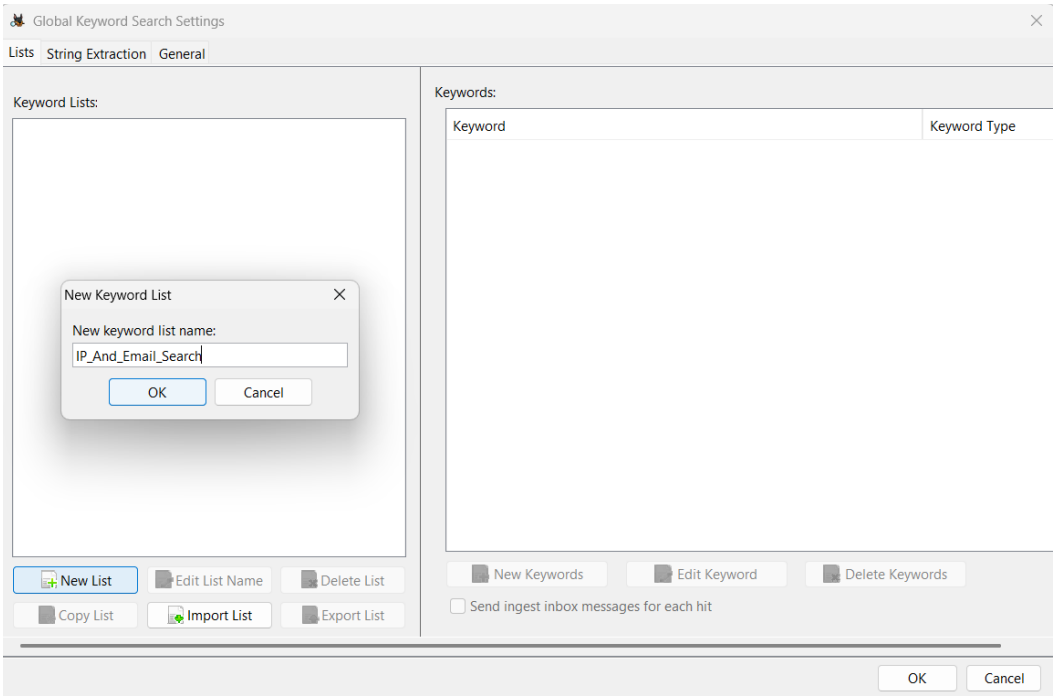
- Leave timezone, sector size default → click Next, then Finish.

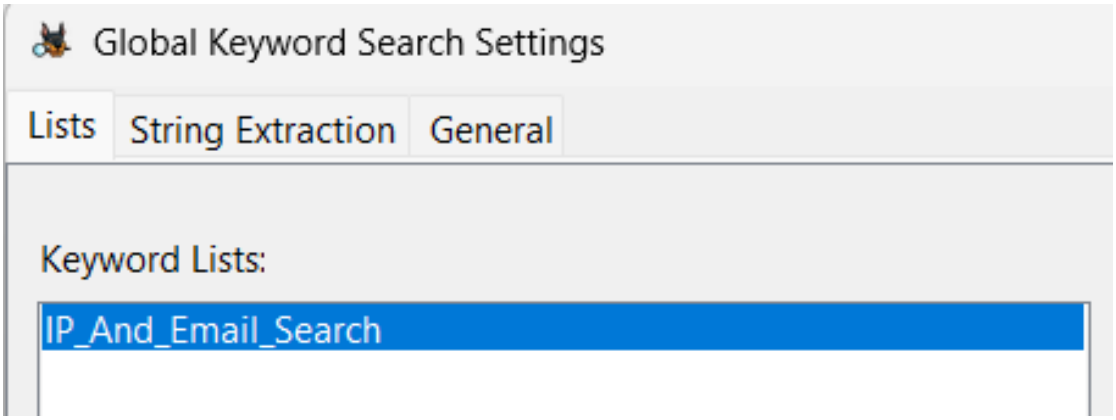
Step 3: Configure Ingest Modules

- Here’s where the magic happens!
- Select the following modules:
  - File Type Identification
  - Keyword Search
  - Extracted Text



- In the Keyword Search settings, click "Keyword Lists..."
- Click on "New List", give it a name like:
  - IP_And_Email_Search

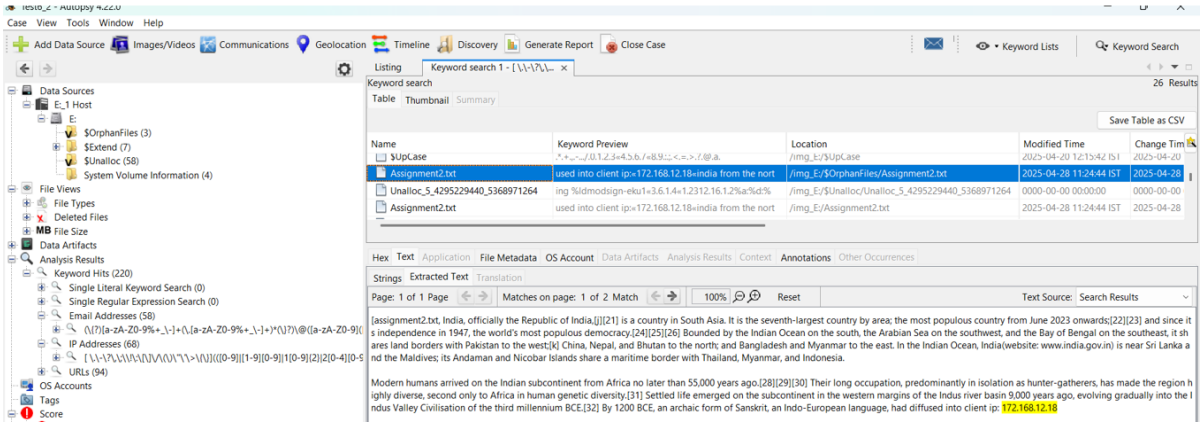




- Click OK to save the list.
- Now Finish adding the data source.

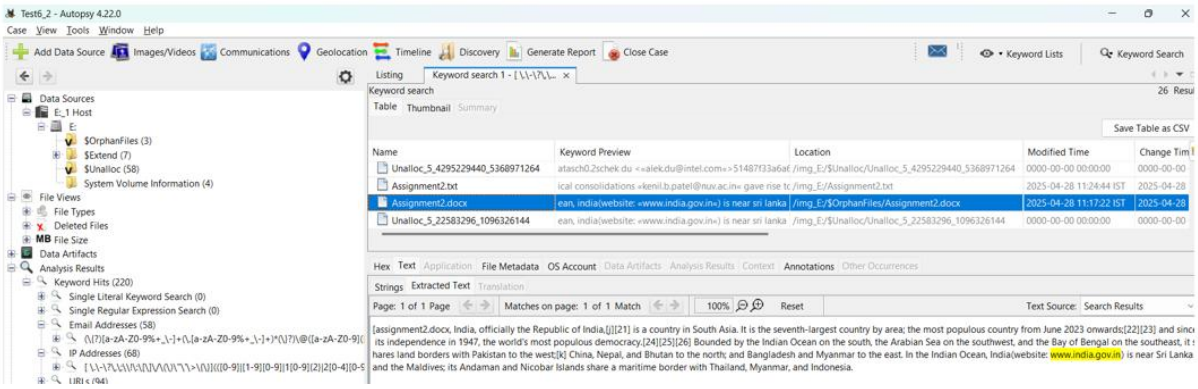
Step 4: Let Autopsy Process

- Wait for Autopsy to process the data. You'll see progress at the bottom.
- Once processing is done, go to the Results section.



Step 5: View Keyword Search Results

- In the left panel, go to:
- Click on each keyword to see the files or locations where they were found (emails, documents, chat logs, HTML pages, etc.).



Conclusion: -Using Autopsy, we can perform keyword-based searches to locate critical digital evidence like IP addresses, URLs, or email addresses. This is especially useful in cybercrime investigations to trace connections, leaked credentials, and digital traces. The tool's ability to scan across all file types and present direct hits makes it efficient and valuable for forensic investigators.