

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



**NAVRACHANA
UNIVERSITY**

a UGC recognized University

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.

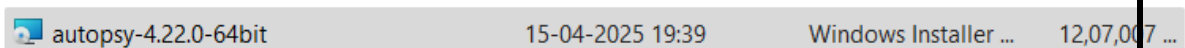
Download Autopsy

VERSION 4.22.0 FOR WINDOWS

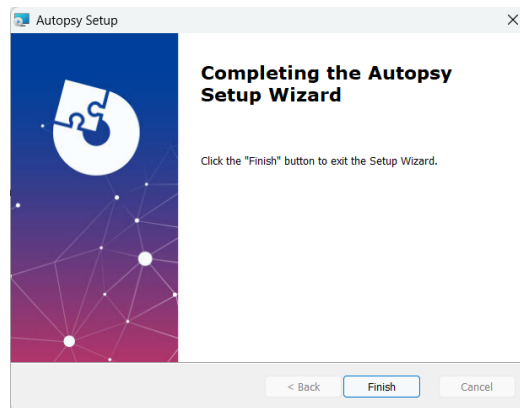
DOWNLOAD 64-BIT >

Step 2: Run the Installer

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

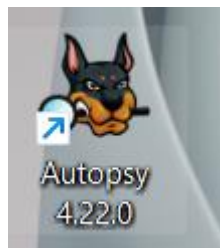


- Double-click the installer to launch it.
- If prompted by User Account Control, click "Yes" to allow the installation.
- Follow the installation wizard:
 - Click "Next" to proceed.
 - Accept the license agreement and click "Next".
 - Choose the installation directory or leave it as default, then click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

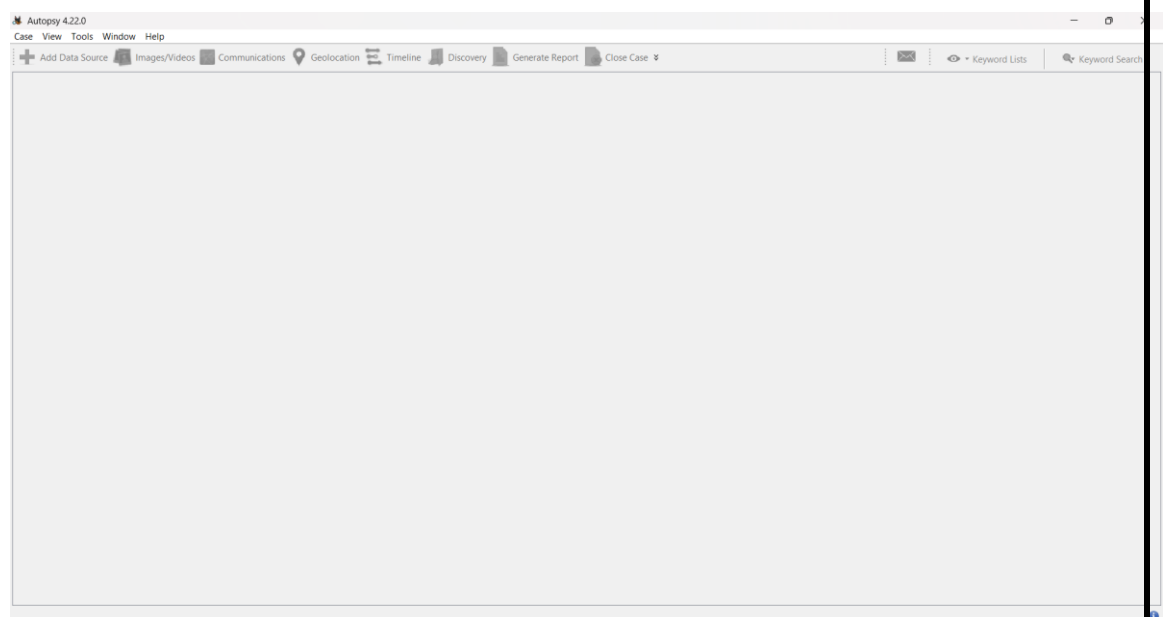


Step 3: Launch Autopsy

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

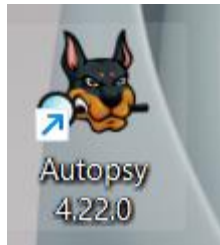


- The Autopsy application will open, and you can start creating or opening cases.



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.

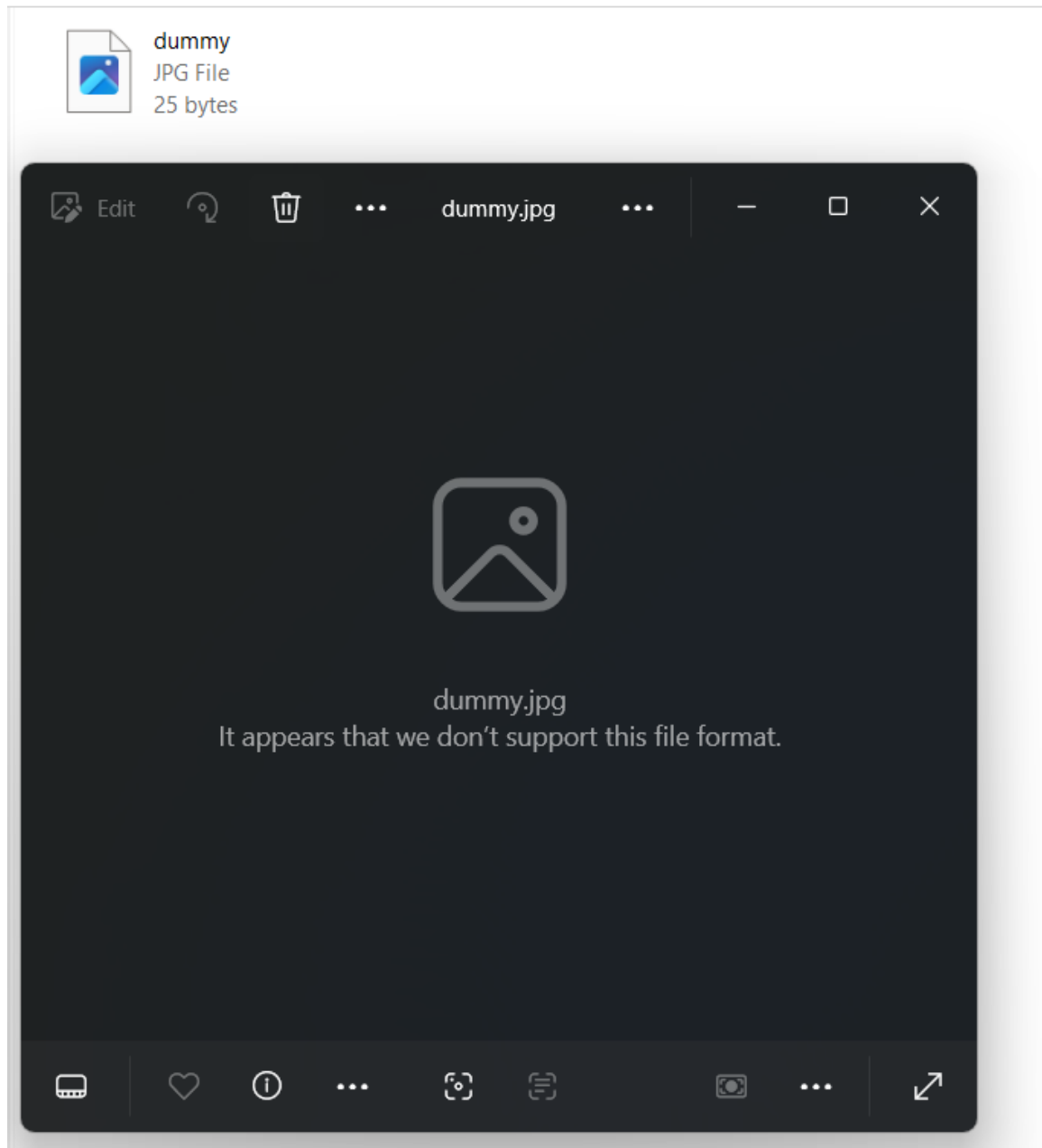
**Step 2: Create a New Case**

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

A screenshot of the "New Case Information" dialog box in Autopsy. The dialog has a title bar with a small dog icon and the text "New Case Information". On the left, there is a "Steps" section with two items: "1. Case Information" (selected) and "2. Optional Information". The main area is titled "Case Information" and contains several fields: "Case Name:" with the value "TestingQ2", "Base Directory:" with the value "D:\B_Tech_CSE_Sem-6\Cyber security lab\" and a "Browse" button, "Case Type:" with radio buttons for "Single-User" (selected) and "Multi-User", and "Case data will be stored in the following directory:" with the value "D:\B_Tech_CSE_Sem-6\Cyber security lab\TestingQ2". At the bottom, there are five buttons: "< Back", "Next >" (highlighted in blue), "Finish", "Cancel", and "Help".

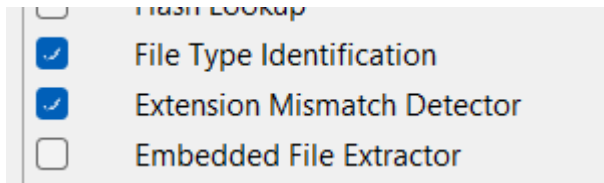
Step 3: Add Data Source

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

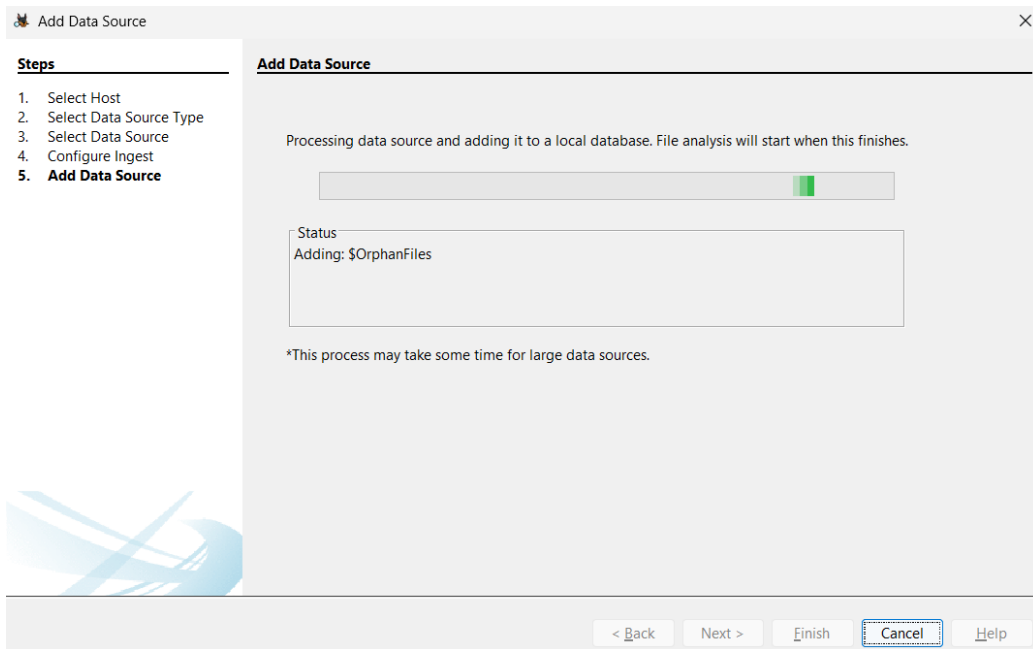
**Step 4: Run Ingest Modules**

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.

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags
IMG-20230808-WA0034.jpg				2023-08-08 18:47:00 IST	0000-00-00 00:00:00	2023-10-24 00:00:00 IST	2023-10-13 12:42:06 IST	37221	Unalloc
ptNblsM6PKTTgOA4jgi5vE5rprKNC6m5ypzldGQJh				2023-08-08 18:46:58 IST	0000-00-00 00:00:00	2023-10-24 00:00:00 IST	2023-10-13 12:42:06 IST	49174	Unalloc
UTc00Kw5pyNqClse50ZRR7s4KBkCqLPkgy4WyZ2l				2023-08-08 23:26:32 IST	0000-00-00 00:00:00	2023-10-24 00:00:00 IST	2023-10-13 12:42:06 IST	114529	Unalloc
sweetcorn.jpg				2023-10-26 17:57:42 IST	0000-00-00 00:00:00	2023-10-26 00:00:00 IST	2023-10-26 17:57:40 IST	0	Unalloc
sweetcorn.jpg				2023-10-26 17:57:50 IST	0000-00-00 00:00:00	2023-10-26 00:00:00 IST	2023-10-26 17:57:49 IST	1902808	Unalloc
hot and sour.jpg				2023-10-26 17:58:38 IST	0000-00-00 00:00:00	2023-10-26 00:00:00 IST	2023-10-26 17:58:36 IST	0	Unalloc
hot and sour.jpg				2023-10-26 17:58:46 IST	0000-00-00 00:00:00	2023-10-26 00:00:00 IST	2023-10-26 17:58:45 IST	1968637	Unalloc
manchow soup - Google Search.jpg				2023-10-26 17:59:10 IST	0000-00-00 00:00:00	2023-10-26 00:00:00 IST	2023-10-26 17:59:08 IST	0	Unalloc
manchow soup - Google Search.jpg				2023-10-26 17:59:18 IST	0000-00-00 00:00:00	2023-10-26 00:00:00 IST	2023-10-26 17:59:17 IST	1966199	Unalloc
lemon coriander soup - Google Search.jpg				2023-10-26 17:59:56 IST	0000-00-00 00:00:00	2023-10-26 00:00:00 IST	2023-10-26 17:59:55 IST	0	Unalloc
lemon coriander soup - Google Search.jpg				2023-10-26 18:00:06 IST	0000-00-00 00:00:00	2023-10-26 00:00:00 IST	2023-10-26 18:00:05 IST	1894704	Unalloc
tmato cream soup - Google Search.jpg				2023-10-26 18:01:22 IST	0000-00-00 00:00:00	2023-10-26 00:00:00 IST	2023-10-26 18:01:20 IST	0	Unalloc
tmato cream soup - Google Search.jpg				2023-10-26 18:01:34 IST	0000-00-00 00:00:00	2023-10-26 00:00:00 IST	2023-10-26 18:01:32 IST	1897878	Unalloc
_ummy.jpg				2025-04-20 13:08:28 IST	0000-00-00 00:00:00	2025-04-20 00:00:00 IST	2025-04-20 13:08:27 IST	0	Unalloc
dummy.jpg				2025-04-20 13:08:28 IST	0000-00-00 00:00:00	2025-04-20 00:00:00 IST	2025-04-20 13:08:27 IST	25	Allocat

	Size	Flags(Dir)	Flags(Meta)	Known	Location	MD5 Hash	SHA-256 Hash	MIME Type	Extension
00 IST	32307	Unallocated	Unallocated	unknown	/img_E:/\$OrphanFiles/_HOTOS/IMG-20230808-WA0034				jpg
06 IST	49174	Unallocated	Unallocated	unknown	/img_E:/\$OrphanFiles/_HOTOS/ptNblsM6PKTTgOA4jgi5				jpg
06 IST	114529	Unallocated	Unallocated	unknown	/img_E:/\$OrphanFiles/_HOTOS/UTc00kQw5pyNqCJseS0				jpg
40 IST	0	Unallocated	Unallocated	unknown	/img_E:/Spotlight-V100/sweetcorn.jpg			application/octet-stream	jpg
49 IST	1902808	Unallocated	Unallocated	unknown	/img_E:/Spotlight-V100/sweetcorn.jpg			application/octet-stream	jpg
36 IST	0	Unallocated	Unallocated	unknown	/img_E:/Spotlight-V100/hot and sour.jpg			application/octet-stream	jpg
45 IST	1968637	Unallocated	Unallocated	unknown	/img_E:/Spotlight-V100/hot and sour.jpg			application/octet-stream	jpg
08 IST	0	Unallocated	Unallocated	unknown	/img_E:/Spotlight-V100/manchow soup - Google Search			application/octet-stream	jpg
17 IST	1966199	Unallocated	Unallocated	unknown	/img_E:/Spotlight-V100/manchow soup - Google Search			application/octet-stream	jpg
55 IST	0	Unallocated	Unallocated	unknown	/img_E:/Spotlight-V100/lemon coriander soup - Google Search			application/octet-stream	jpg
05 IST	1894704	Unallocated	Unallocated	unknown	/img_E:/Spotlight-V100/lemon coriander soup - Google Search			application/octet-stream	jpg
20 IST	0	Unallocated	Unallocated	unknown	/img_E:/Spotlight-V100/tmato cream soup - Google Search			application/octet-stream	jpg
32 IST	1897878	Unallocated	Unallocated	unknown	/img_E:/Spotlight-V100/tmato cream soup - Google Search			application/octet-stream	jpg
27 IST	0	Unallocated	Unallocated	unknown	/img_E:/_ummy.jpg			application/octet-stream	jpg
27 IST	25	Allocated	Allocated	unknown	/img_E:/dummy.jpg			text/plain	jpg

unknown	/img_E:/dummy.jpg			text/plain	jpg
---------	-------------------	--	--	------------	-----

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.

dummy.jpg 2025-04-20 13

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results

Strings Extracted Text Translation

Page: 1 of - Page < > Matches on page: - of - Match < > 100%

Hello this is dummy file

-----METADATA-----

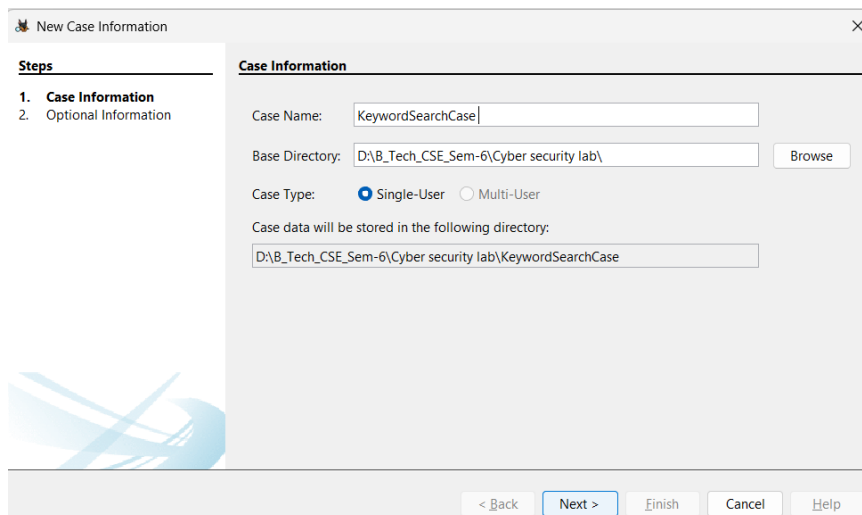
Conclusion: -

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

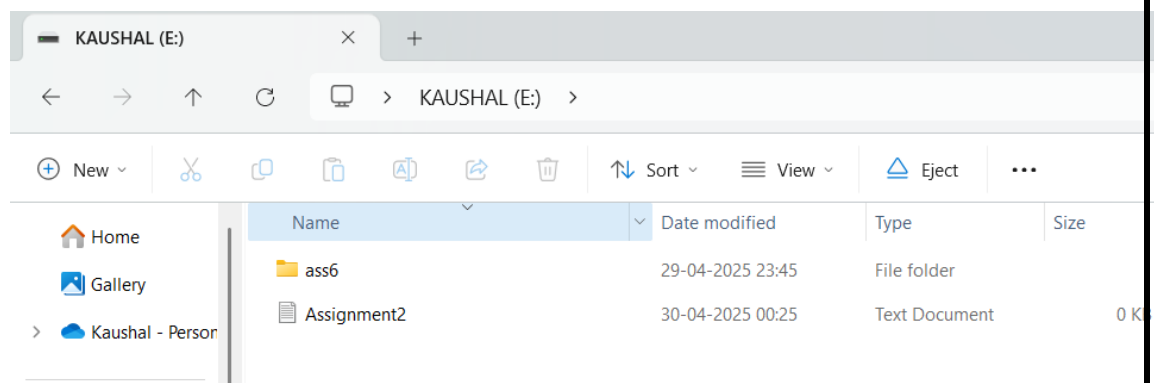
- Open Autopsy.
- Click on "Create New Case" → give it a name like KeywordSearchCase and choose a location.

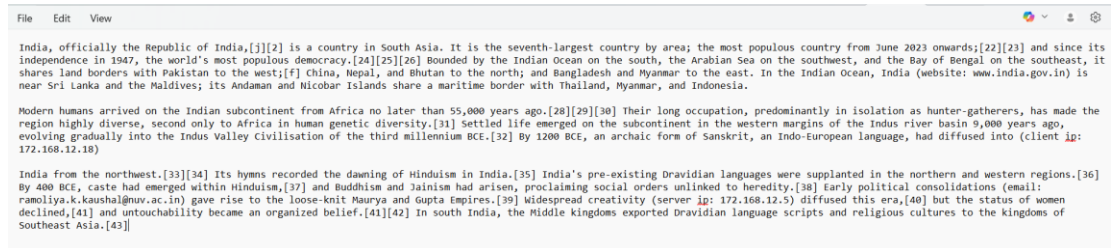


- Click Next and then Finish to start the case.

Step 2: Add Data Source

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

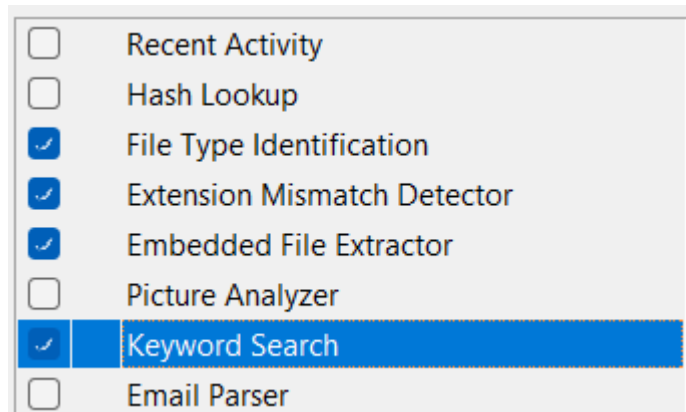




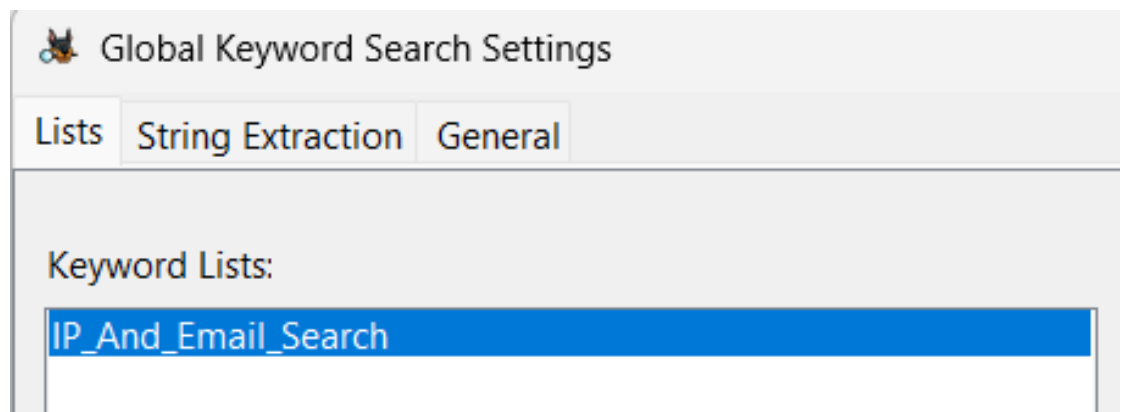
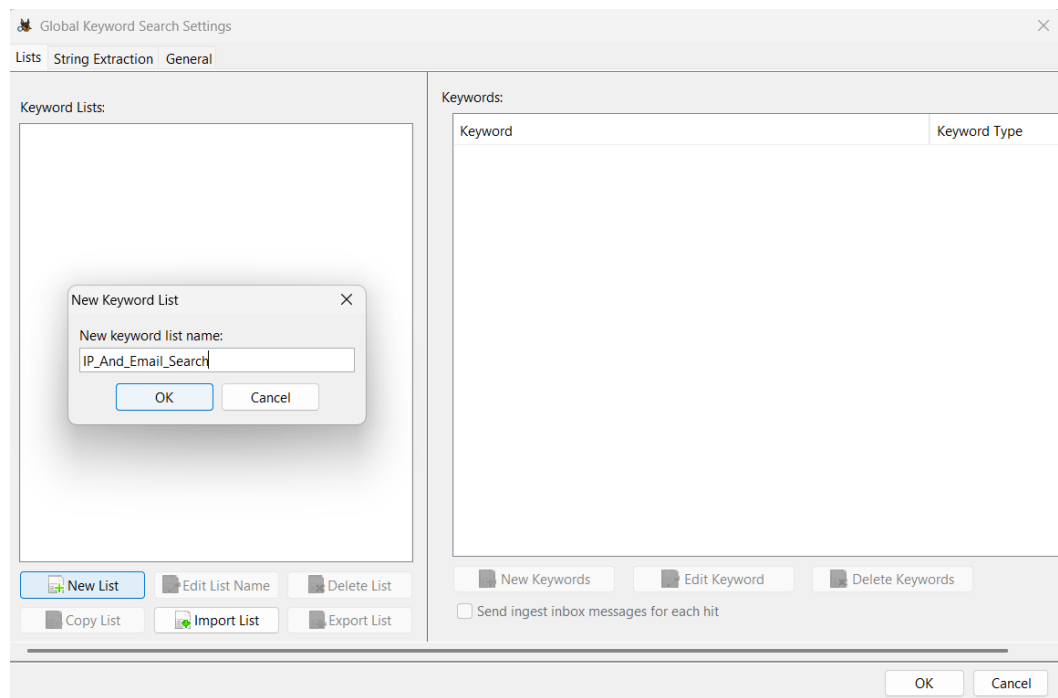
- Leave timezone, sector size default → click Next, then Finish.

Step 3: Configure Ingest Modules

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



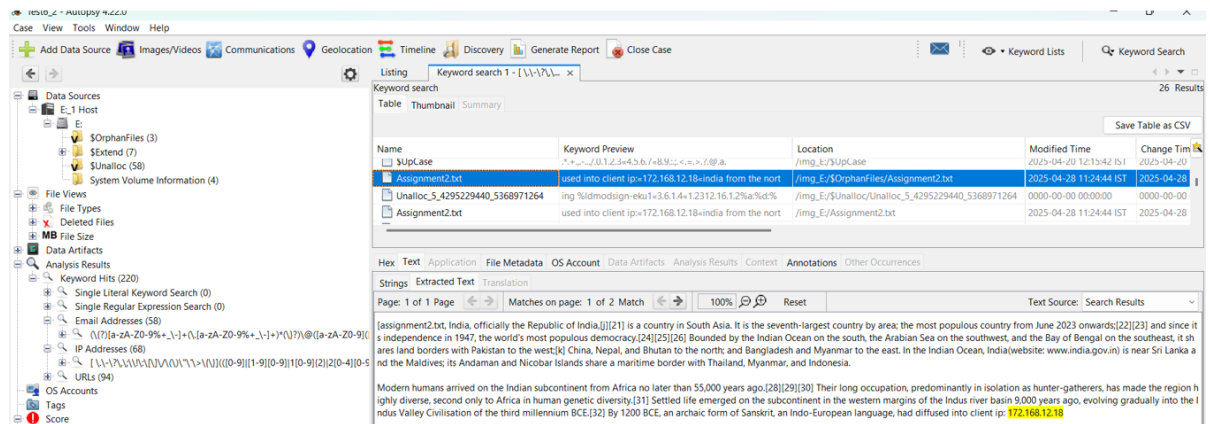
- In the Keyword Search settings, click "Keyword Lists..."
- Click on "New List", give it a name like:
 - IP_And_Email_Search



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

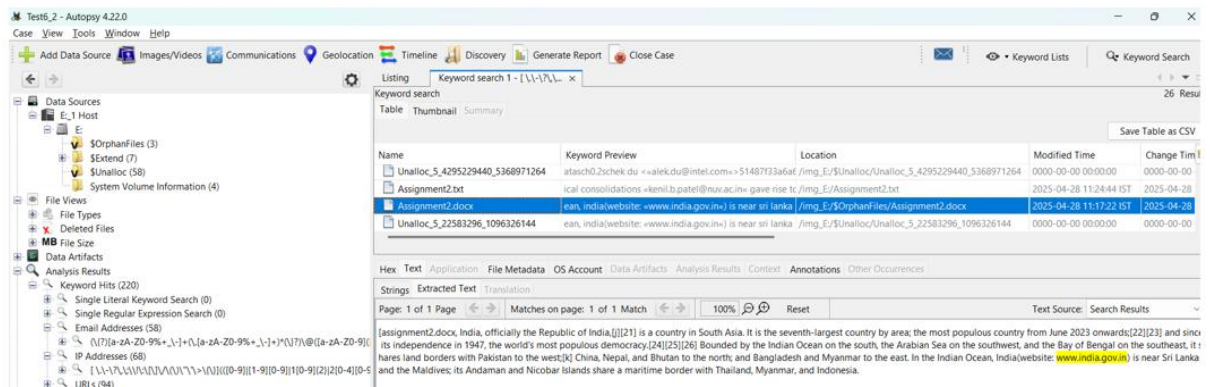
Step 4: Let Autopsy Process

- 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.