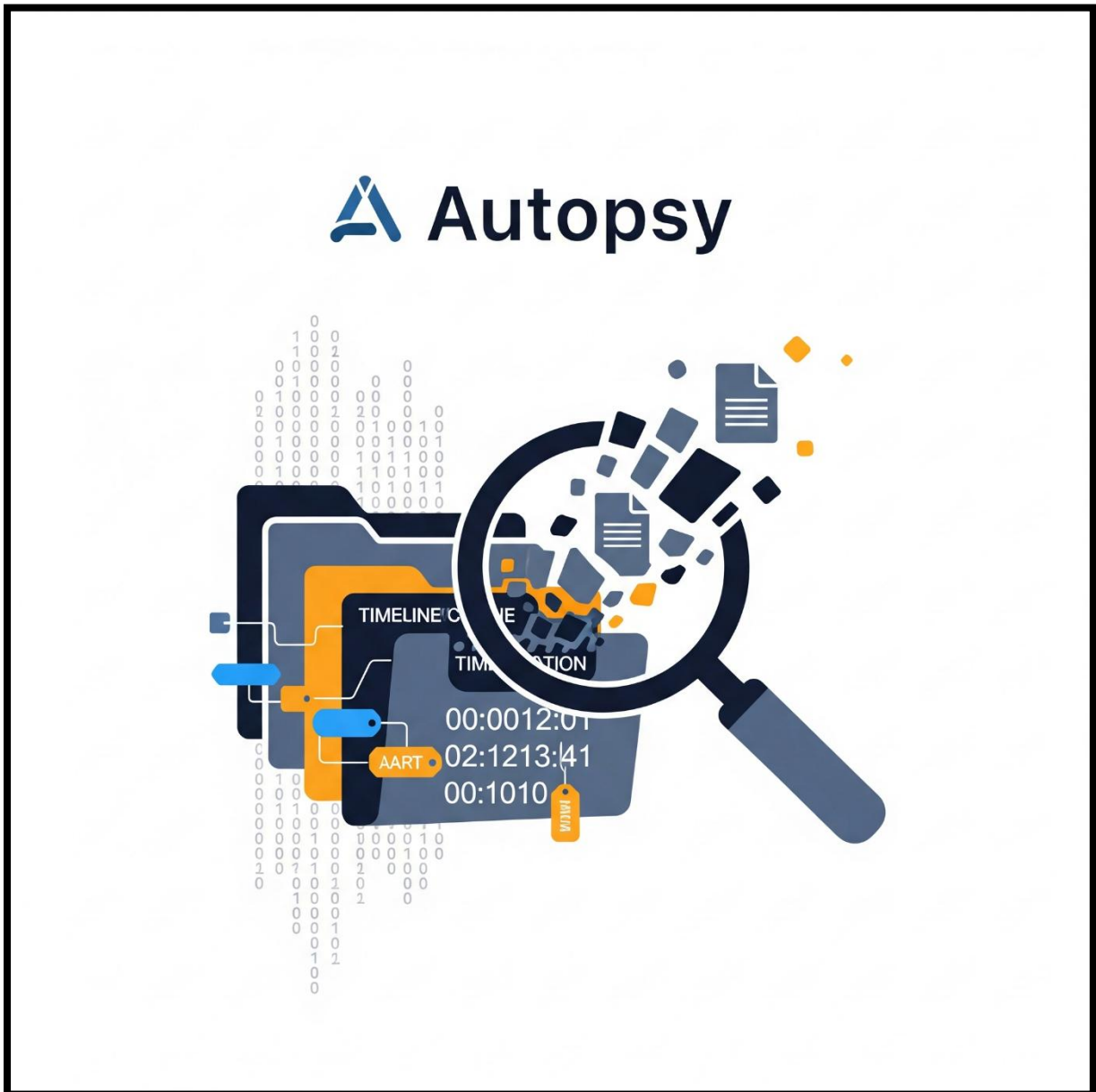


Day 15 of Learning Cyber Security**Platform: Windows 10/11/12**

Name: Ayesha Nadeem

Topic: Autopsy



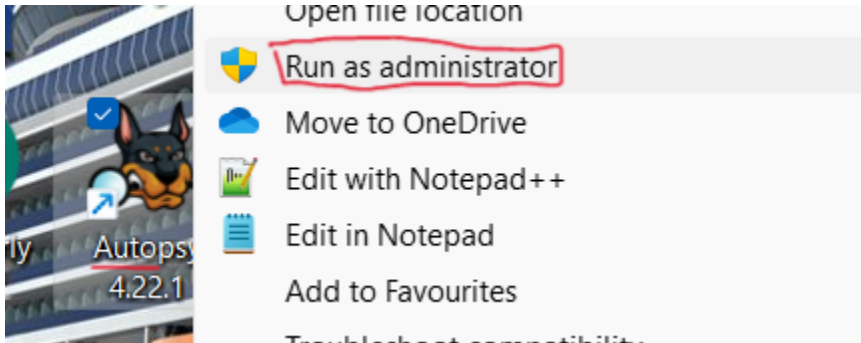
Contact Me: ayeshanm8@gmail.com

Date: 15th July, 2025

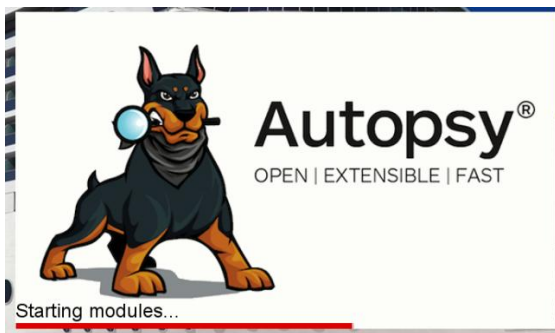
Applied Cyber Security © 2025 by Ayesha Nadeem is licensed under CC BY-NC 4.0. To view a copy of this license, visit <https://creativecommons.org/licenses/by-nc/4.0/>

Autopsy of my USB

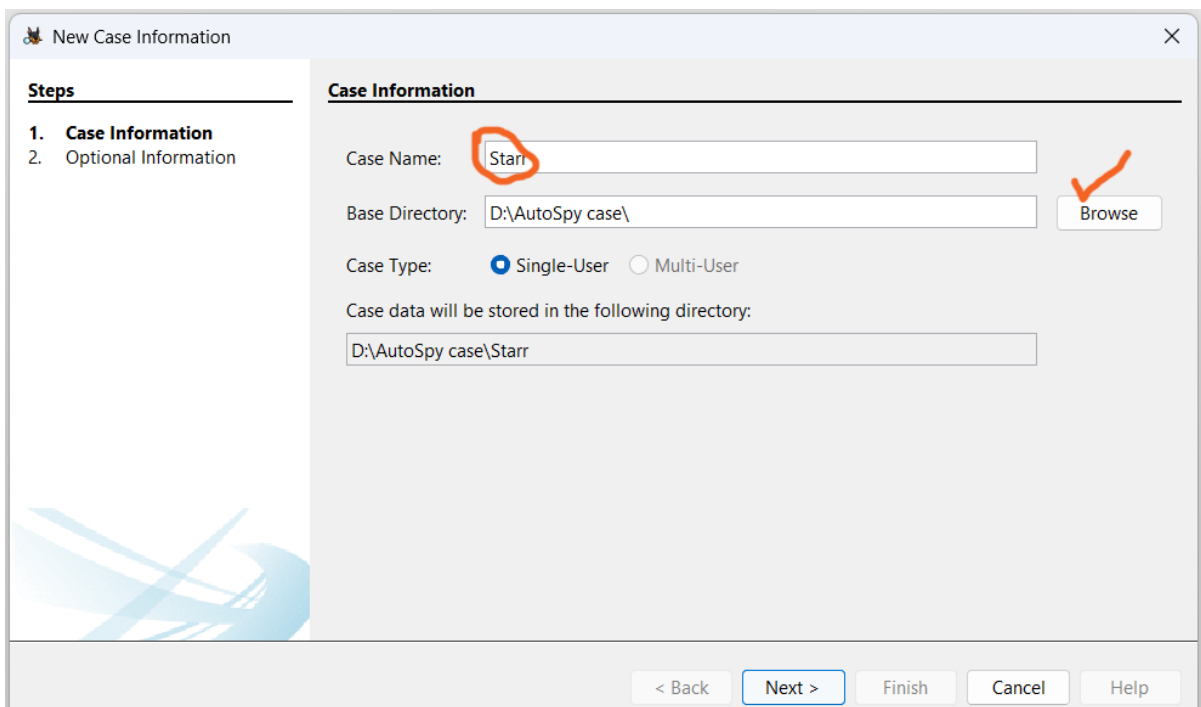
Step 1: Run application as administrator



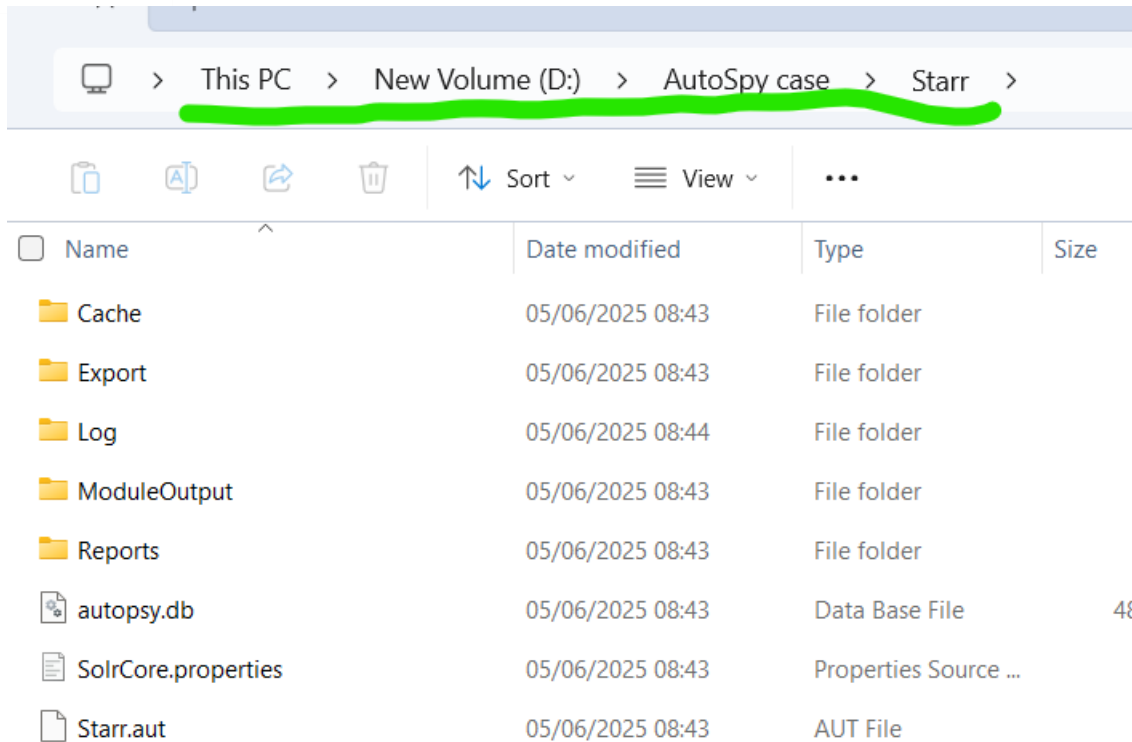
Step 2: Running



Step 3: Set any casename of your choice and set location of your case.



So it saves here.....



Step 4: Give any case number and set examiner details

New Case Information

Steps

1. Case Information
2. **Optional Information**

Optional Information

Case

Number: 1

Examiner

Name: Ayesha Nadeem

Phone:

Email:

Notes:

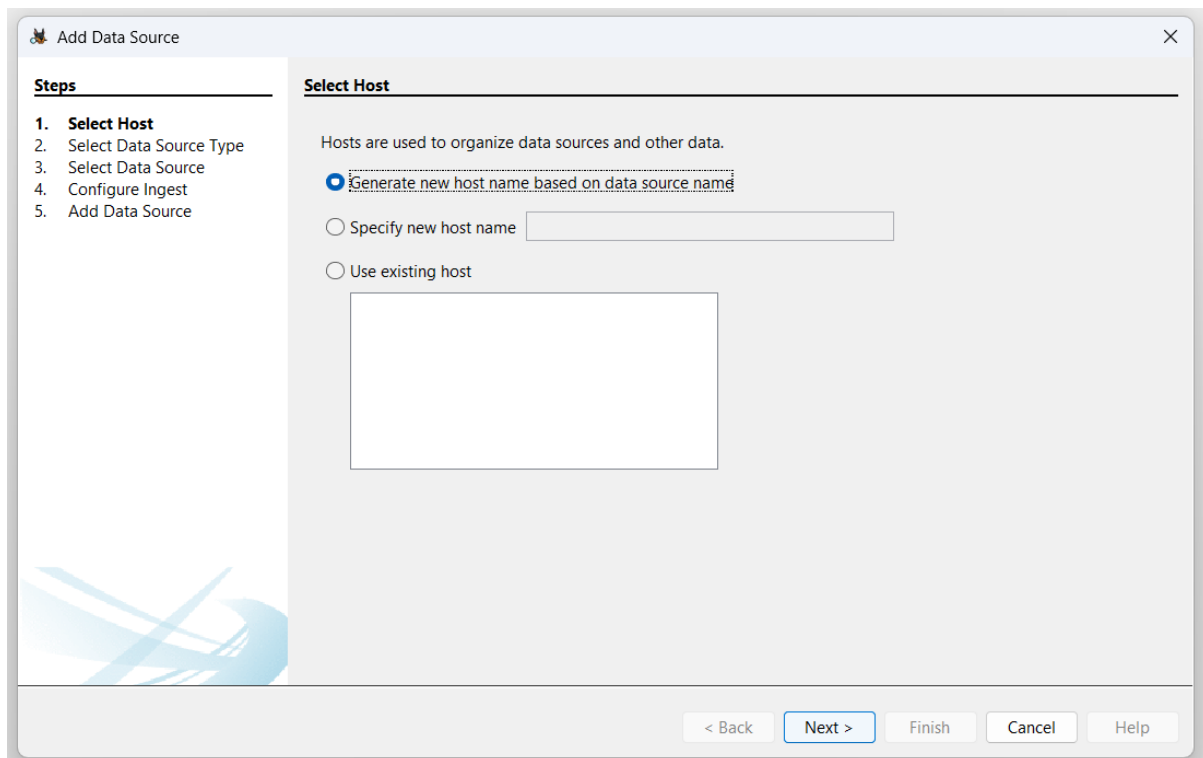
Organization

Organization analysis is being done for: Not Specified Manage Organizations

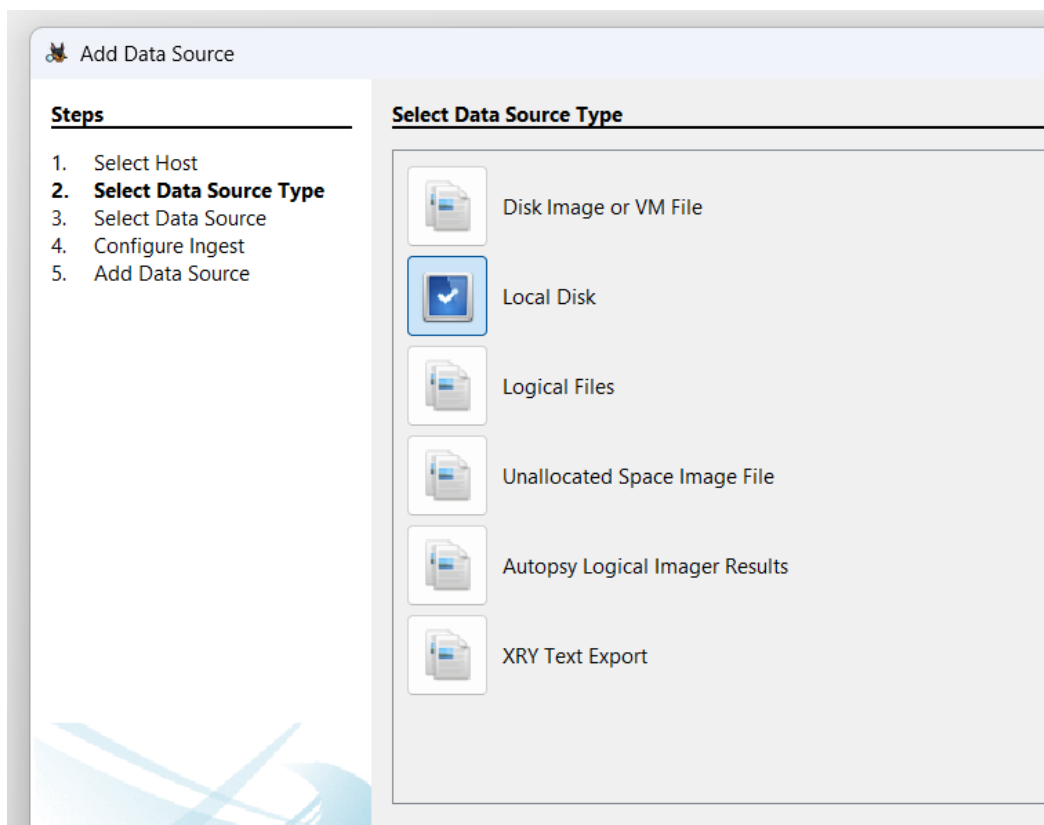
< Back Next > Finish Cancel Help

Click on finish

Step 5: Landed in this page. Do nothing just click next



Step 5: Select local disk



Step 6: Select disk on which you want to perform a test.

Add Data Source

Steps

1. Select Host
2. Select Data Source Type
- 3. Select Data Source**
4. Configure Ingest
5. Add Data Source

Select Data Source

Local Disk: **HOME USER (F:)** Select Disk

Timezone: (GMT+5:00) Asia/Karachi

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

☐ Make a VHD image of the drive while it is being analyzed
ModuleOutput\Image Writer\HOME USER (F) 1749093989393.vhd Browse

☐ Update case to use VHD file upon completion
Note that at least one ingest module must be run to create a complete copy

Sector Size: Auto Detect

< Back **Next >** Finish Cancel Help

source

Select Local Disk

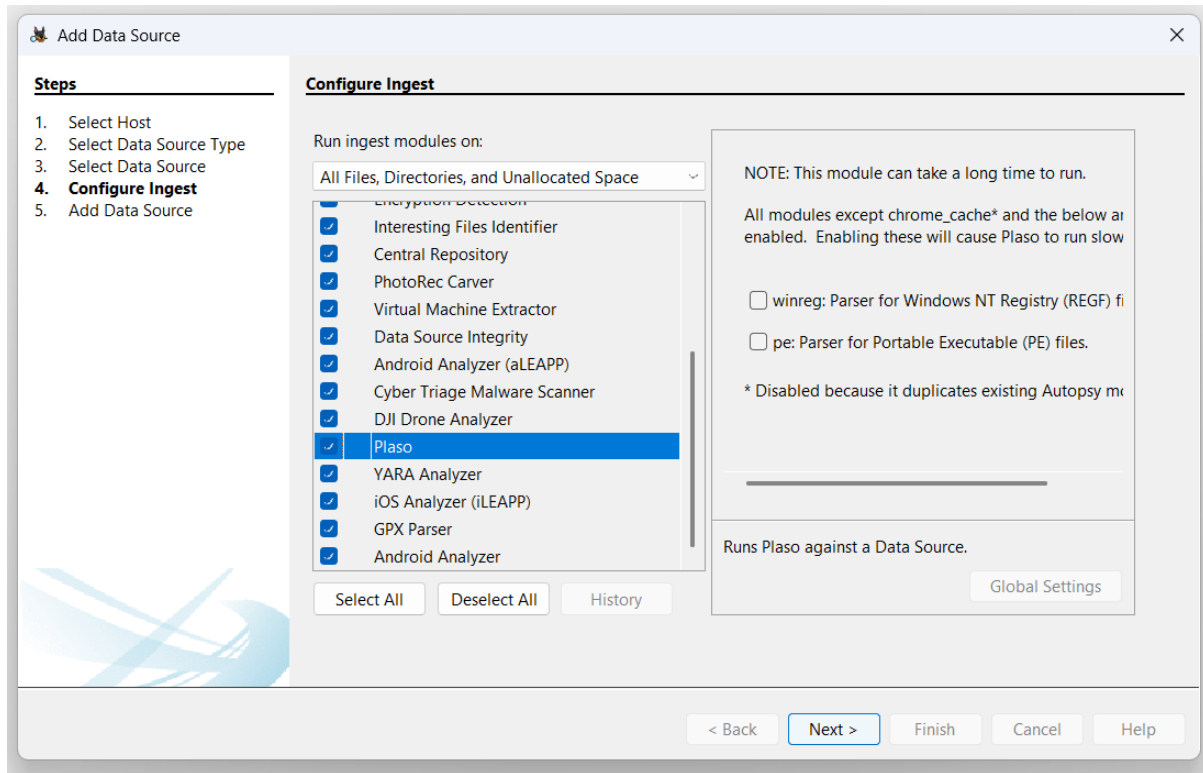
Select a local disk:

Disk Name	Disk Size
Drive 0	476.9 GB
Drive 1	3.8 GB
HOME USER (F:)	3.7 GB
New Volume (D:)	237.8 GB

OK Cancel Refresh Local Disks

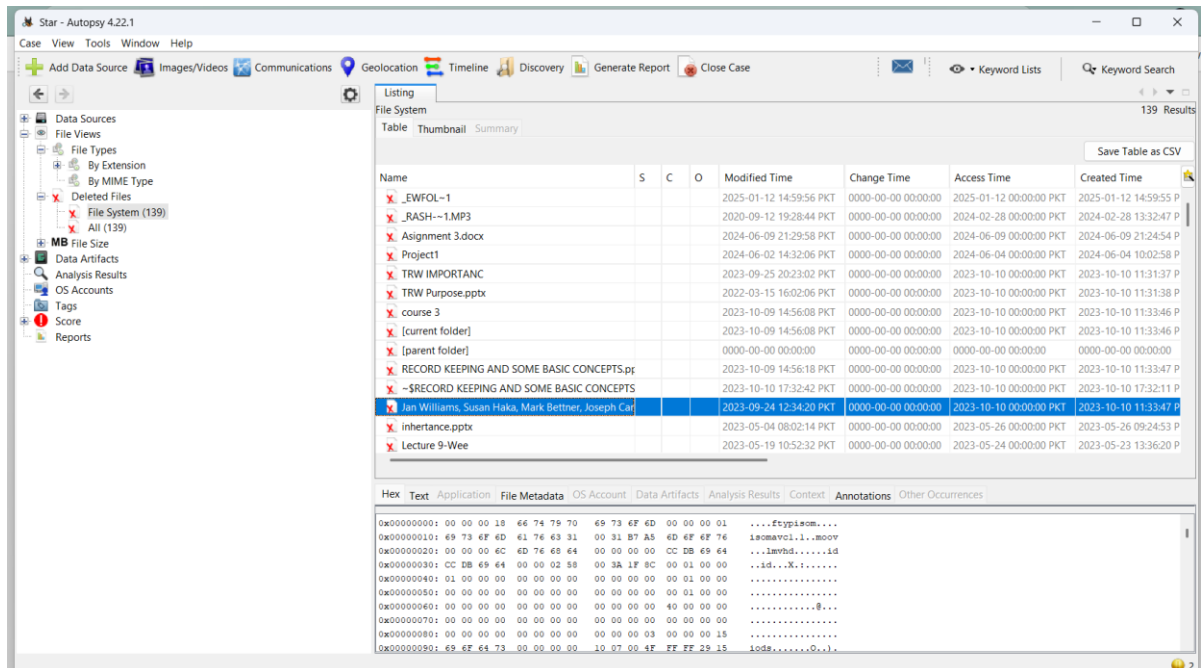
The more the disk size, more time it will take to extract data and vice versa.

Step 7: Tick all

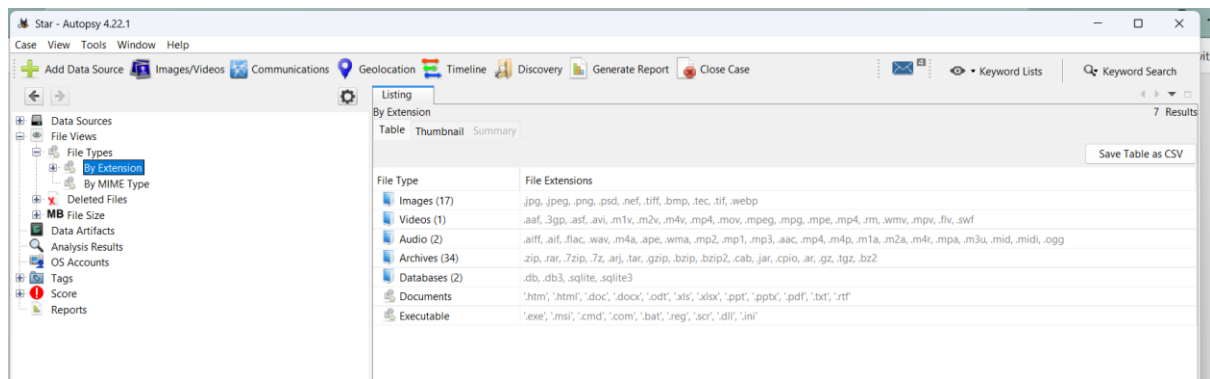


Now search the USB content:

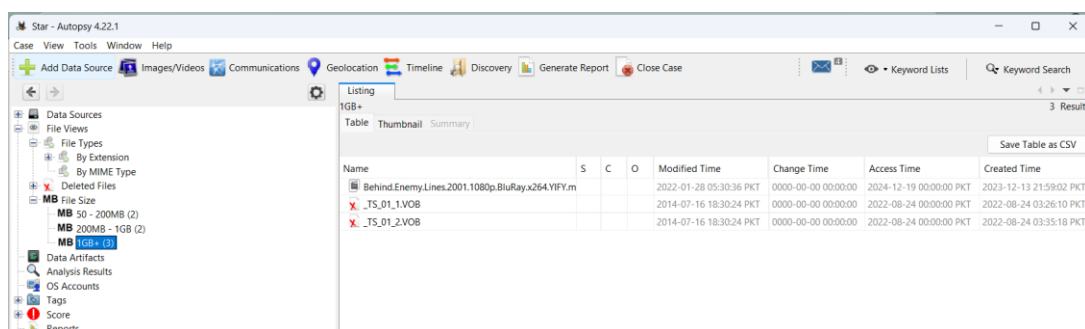
Step 8: Showed all files that are even deleted from USB.



Step 9: Look out Extension



Step 10: Data shown according to file sizes



Step 11: Check for harmful file if exist.

