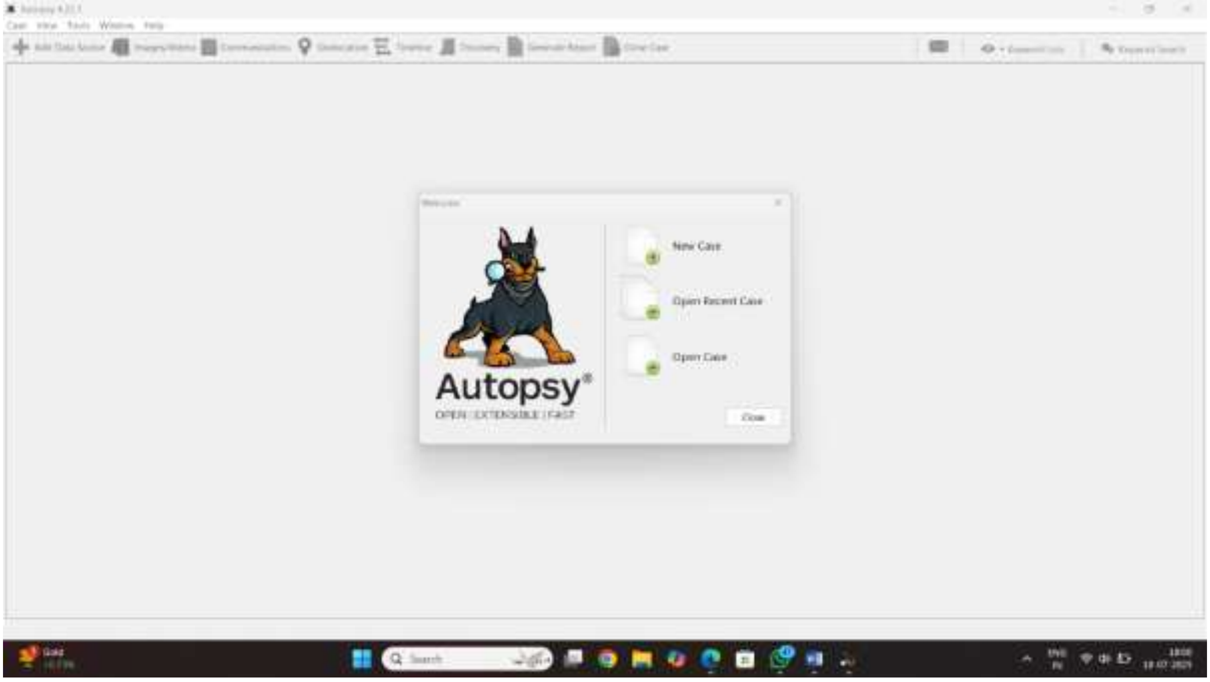
Module 3 Understanding Hard Disks and File System

Lab1 Analyze File System of a Linux and Windows Image

Using Autopsy

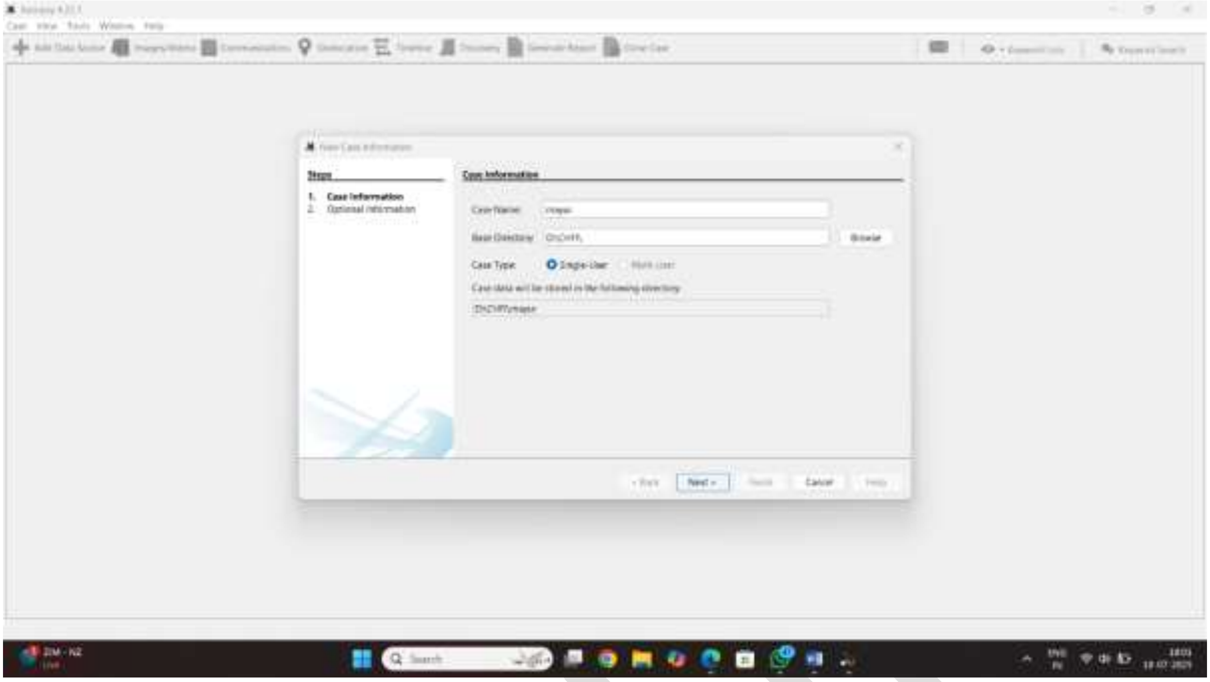
Step1: download the autopsy in windows

Step2: start the autopsy and click on the new cause



Step3: enter case name

Step4: select the case file destination



Case Name: mayur

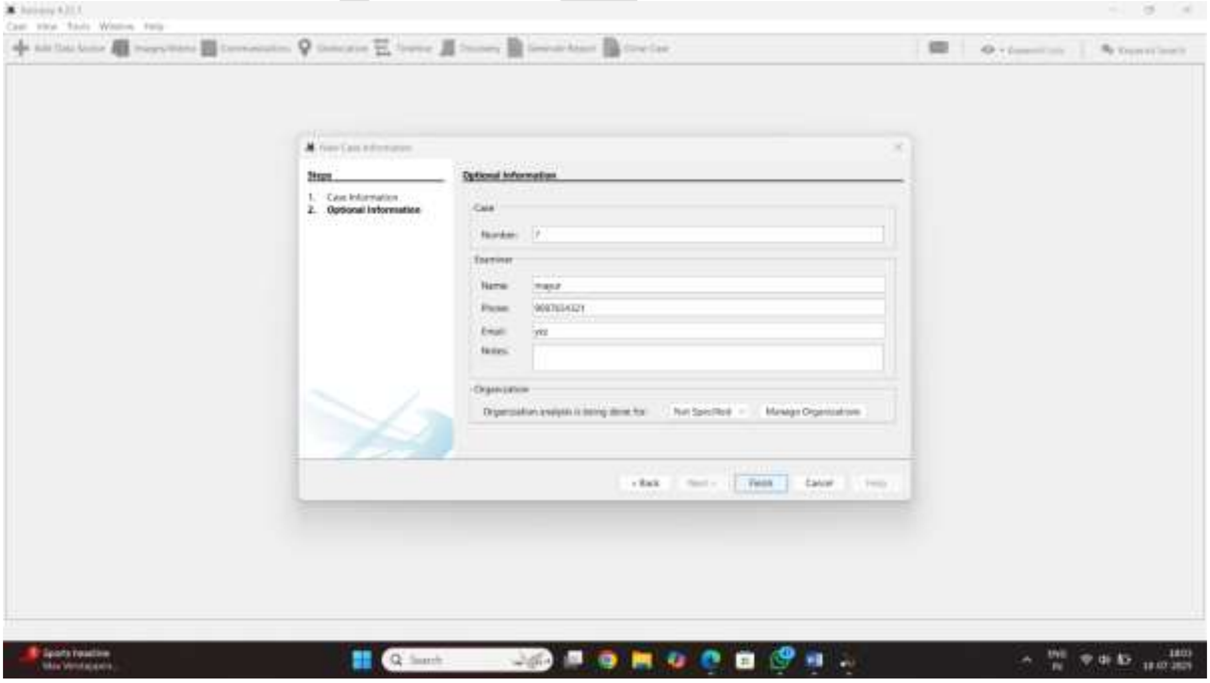
Base Directory: D:\CHFI\

Case Type: ● Single-User ○ Multi-User

Case data will be stored in the following directory:

D:\CHFI\mayur

Step5 select the cause number, name ,email, m.number click on next



Number: 7

Name: mayur

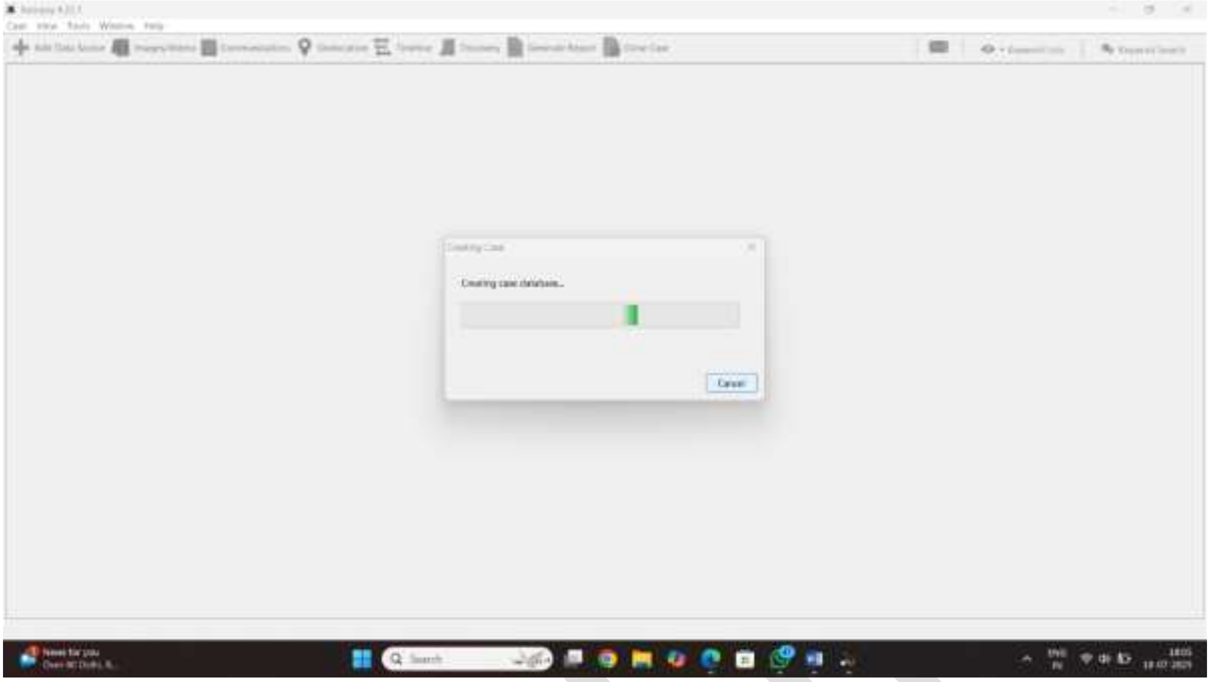
Phone: 9087654321

Email: xyz

Notes:

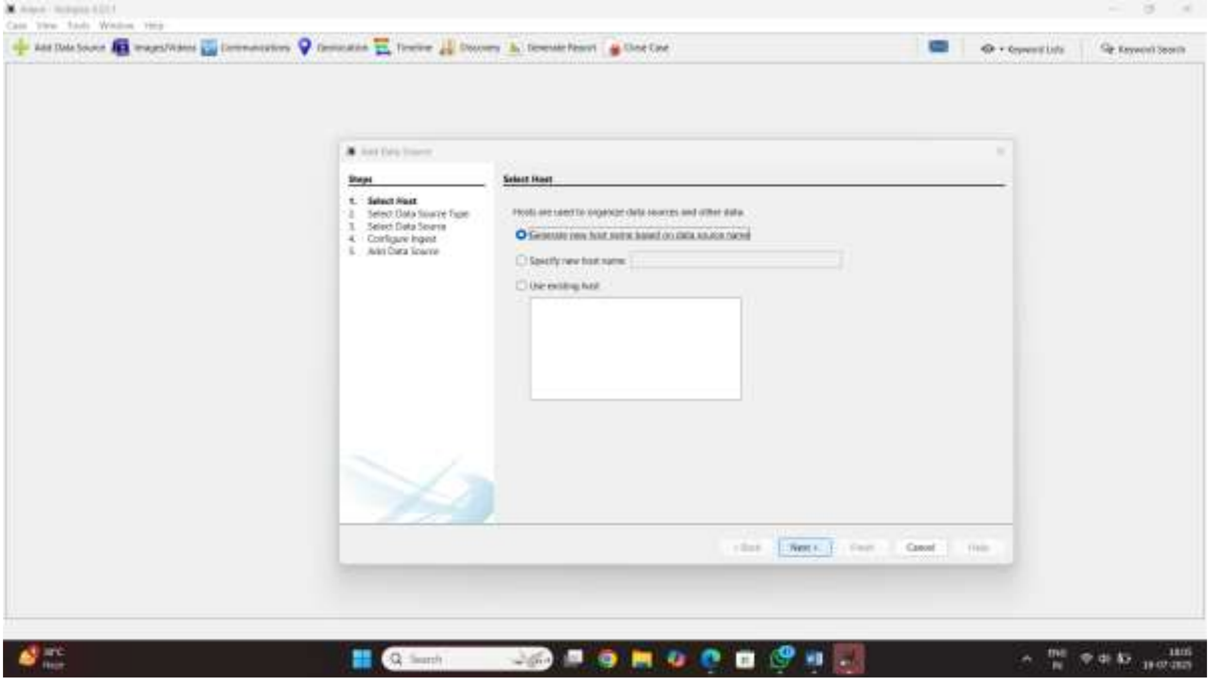
Organization analysis is being done for: Not Specified

Step6 creating data base cause file


Creating Case

Creating case database...

Step7 select host click on the next


Add Data Source

Steps

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

Select Host

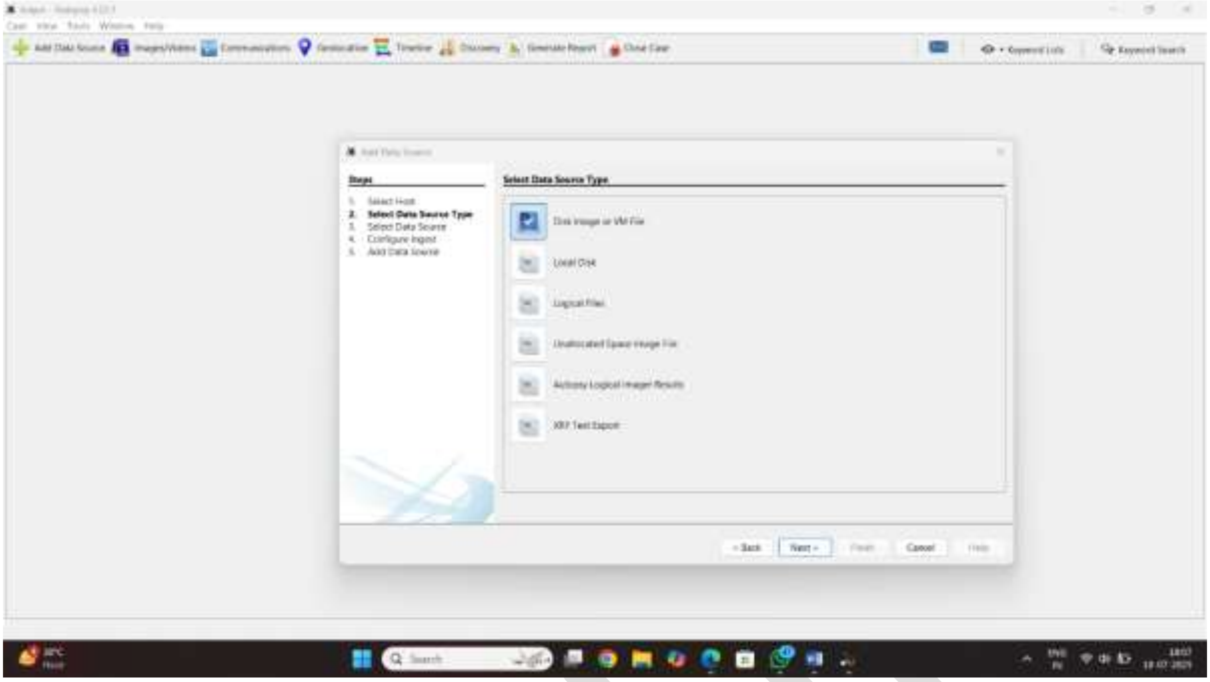
Hosts are used to organize data sources and other data.

● Generate new host name based on data source name

□ Specify new host name

□ Use existing host

Step8 select the data source type



Add Data Source

Steps

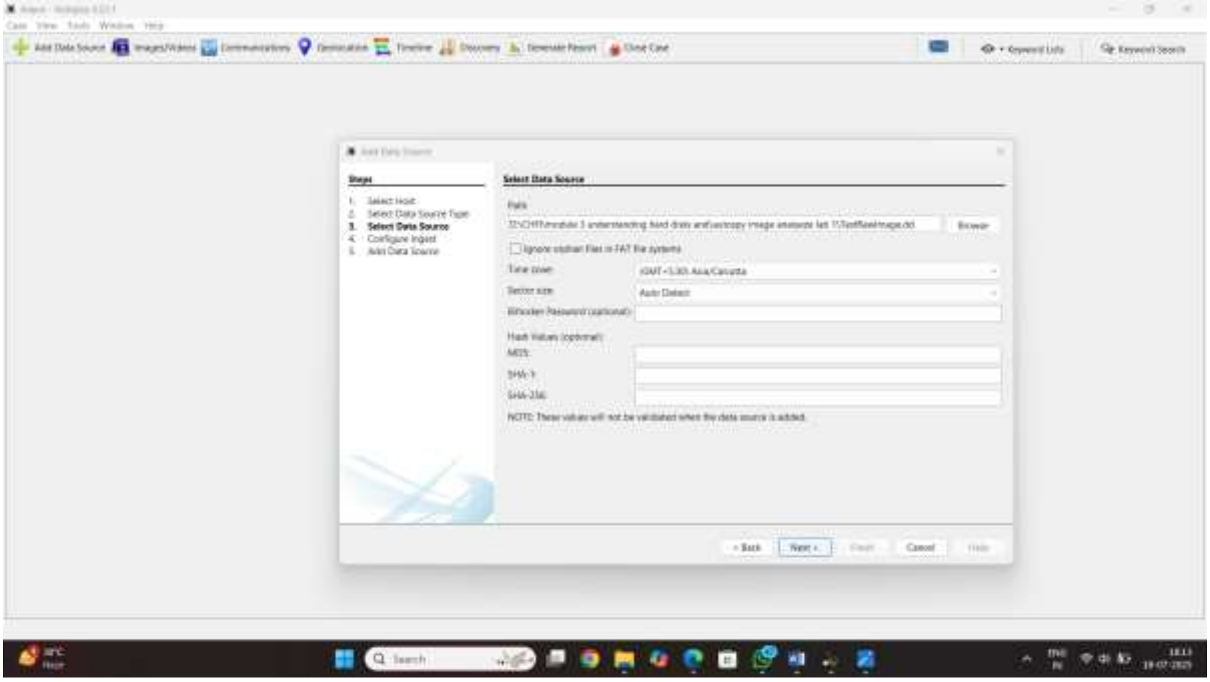
1. Select Host
2. **Select Data Source Type**
3. Select Data Source
4. Configure Ingest
5. Add Data Source

Select Data Source Type

- Disk Image or VM File
- Local Disk
- Logical Files
- Unallocated Space Image File
- Autopsy Logical Imager Results
- XRY Text Export

Select the disk image or vm file click on the next

Step9 select the data source type /image path folder



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

Path: [illegible]

□ Ignore orphan files in FAT file systems

Time zone: (GMT+5:30) Asia/Calcutta

Sector size: Auto Detect

Bitlocker Password (optional):

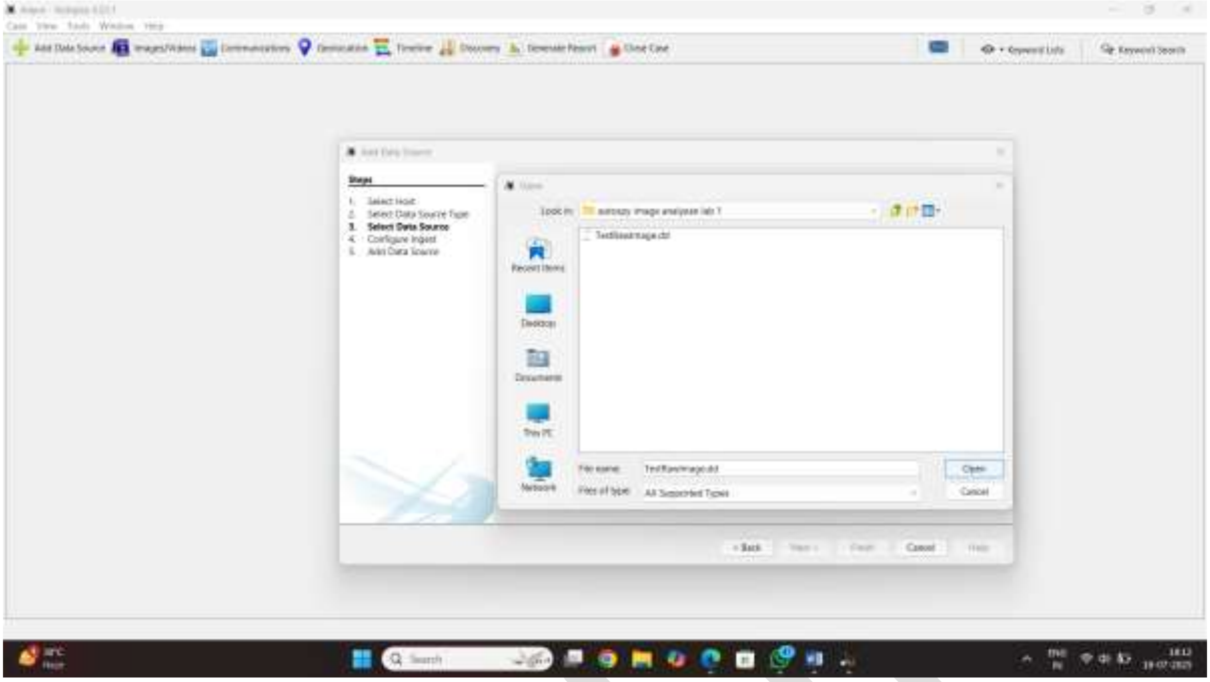
Hash Values (optional):

MD5:

SHA-1:

SHA-256:

NOTE: These values will not be validated when the data source is added.



Steps

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

Look in: autopsy image analyse lab 1

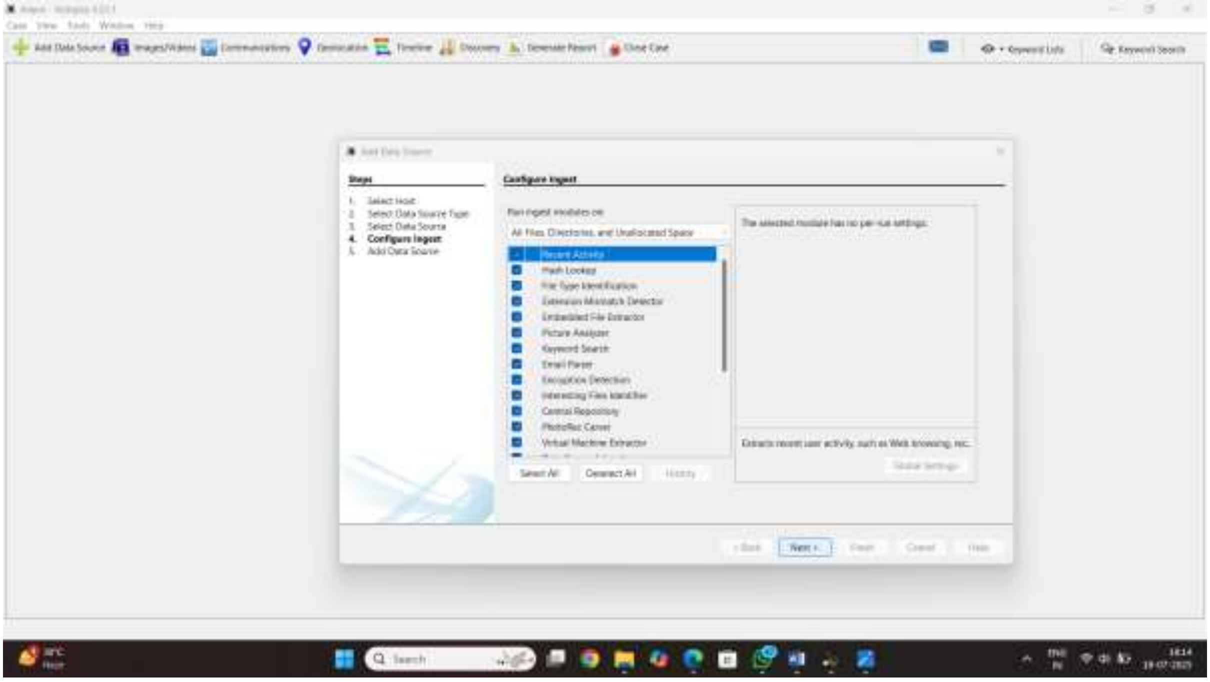
TestRawImage.dd

File name: TestRawImage.dd

Files of type: All Supported Types

Click in the next

Step10 configure ingest



Steps

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

Configure Ingest

Run ingest modules on:

All Files, Directories, and Unallocated Space

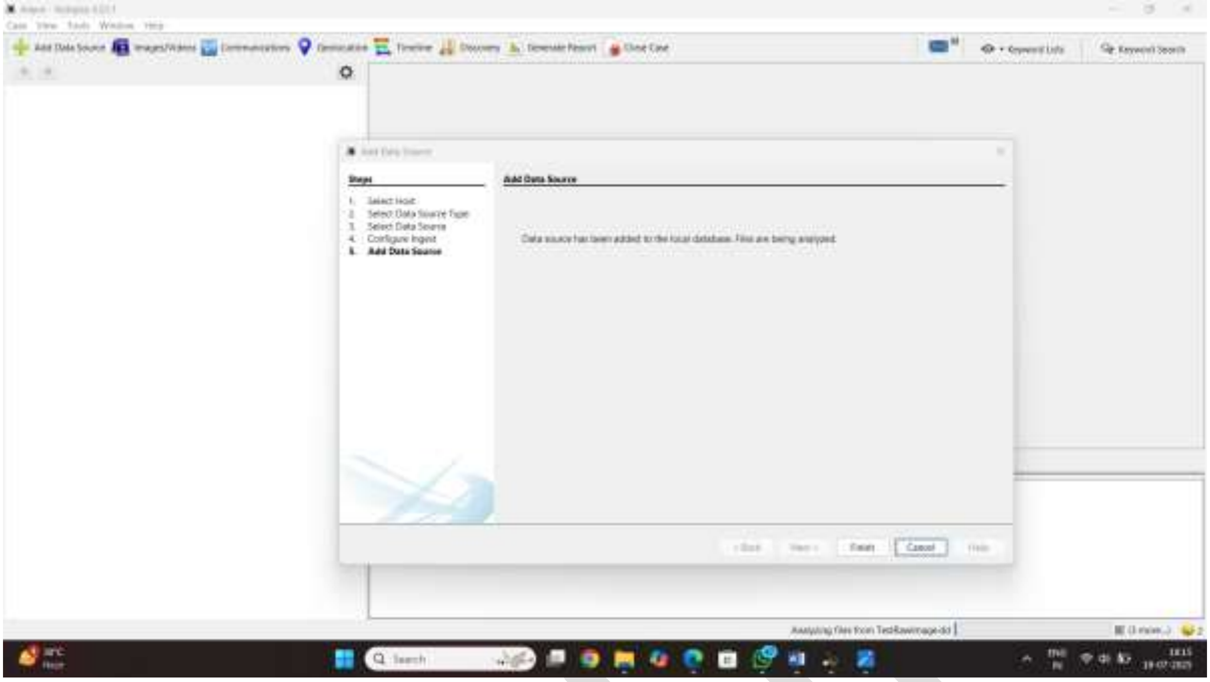
- ☑ Recent Activity
- ☑ Hash Lookup
- ☑ File Type Identification
- ☑ Extension Mismatch Detector
- ☑ Embedded File Extractor
- ☑ Picture Analyzer
- ☑ Keyword Search
- ☑ Email Parser
- ☑ Encryption Detection
- ☑ Interesting Files Identifier
- ☑ Central Repository
- ☑ PhotoRec Carver
- ☑ Virtual Machine Extractor

The selected module has no per-run settings.

Extracts recent user activity, such as Web browsing, etc.

Click on the next

Step11: add data source



Add Data Source

Steps

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

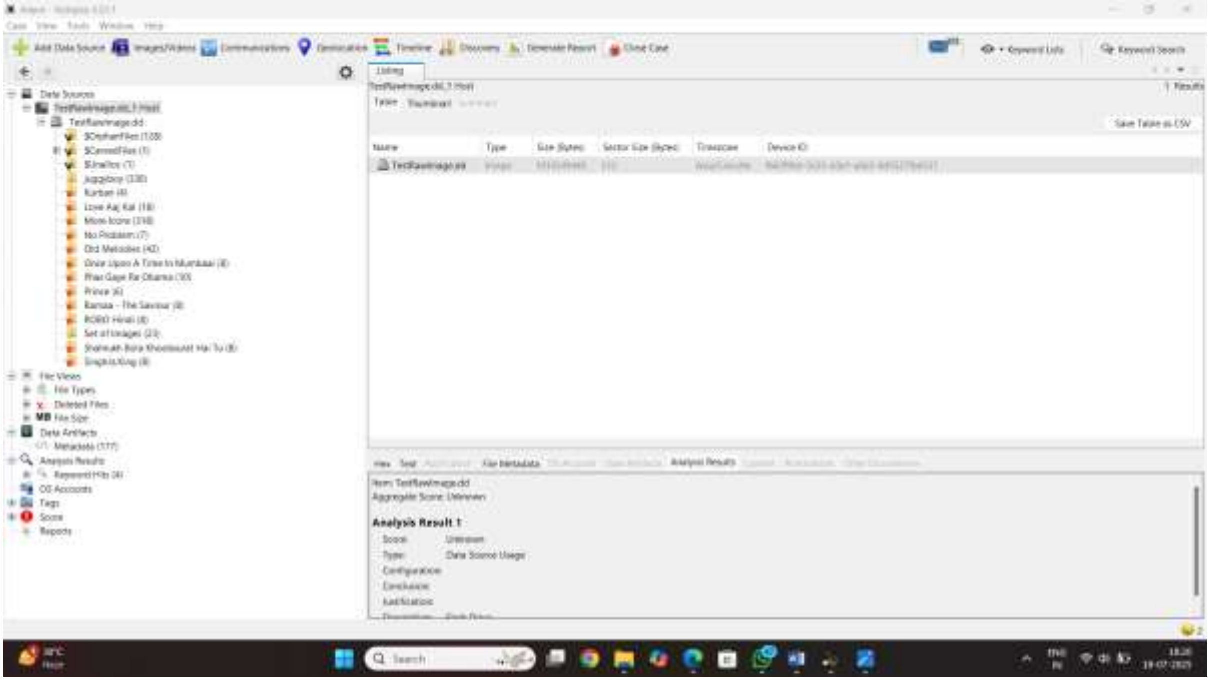
Add Data Source

Data source has been added to the local database. Files are being analyzed.

Analyzing files from TestRawImage.dd

Click on the next

Anaylze the image of content



- Data Sources
  - TestRawImage.dd_1 Host
    - TestRawImage.dd
      - $OrphanFiles (133)
      - $CarvedFiles (1)
      - $Unalloc (1)
      - Jaggabay (330)
      - Kurban (4)
      - Love Aaj Kal (18)
      - More Icons (318)
      - No Problem (7)
      - Old Melodies (40)
      - Once Upon A Time In Mumbaai (8)
      - Phas Gaye Re Obama (10)
      - Prince (6)
      - Ramaa - The Saviour (8)
      - ROBO Hindi (8)
      - Set of Images (23)
      - Shahrukh Bola Khoobsurat Hai Tu (8)
      - Singh is Kinng (8)
- File Views
  - File Types
  - Deleted Files
  - MB File Size
- Data Artifacts
  - Metadata (177)
- Analysis Results
  - Keyword Hits (4)
- OS Accounts
- Tags
- Score
- Reports

TestRawImage.dd_1 Host

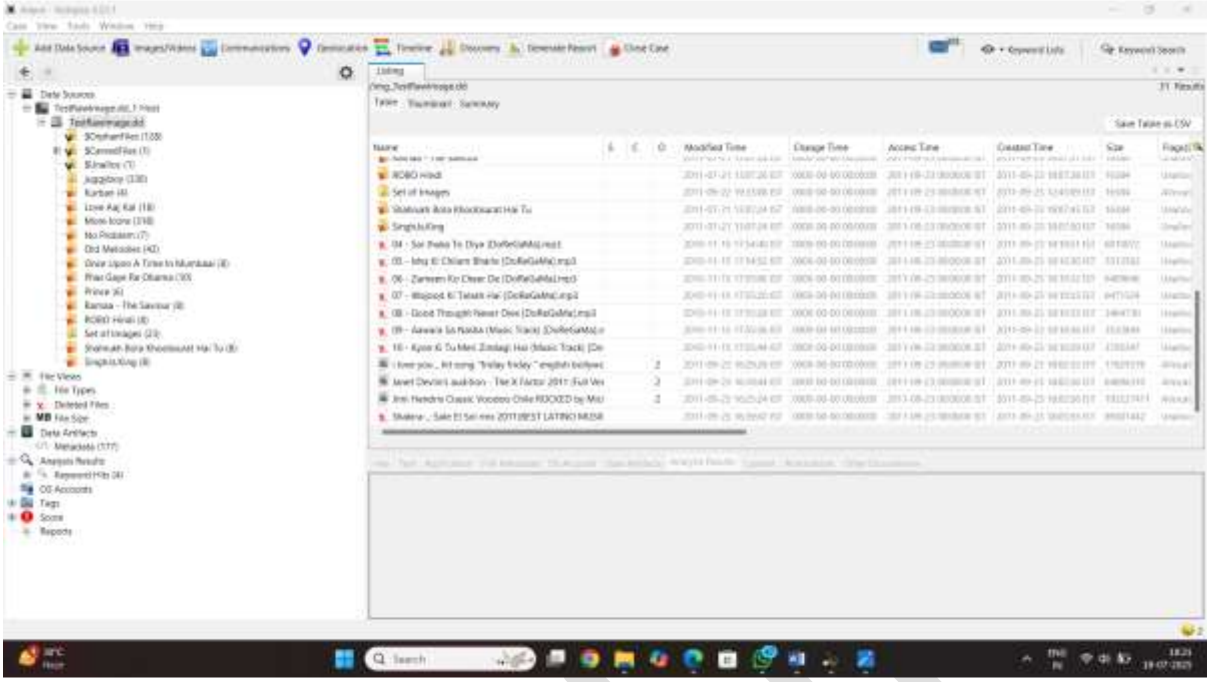
1 Results

Name	Type	Size (Bytes)	Sector Size (Bytes)	Timezone	Device ID
TestRawImage.dd	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

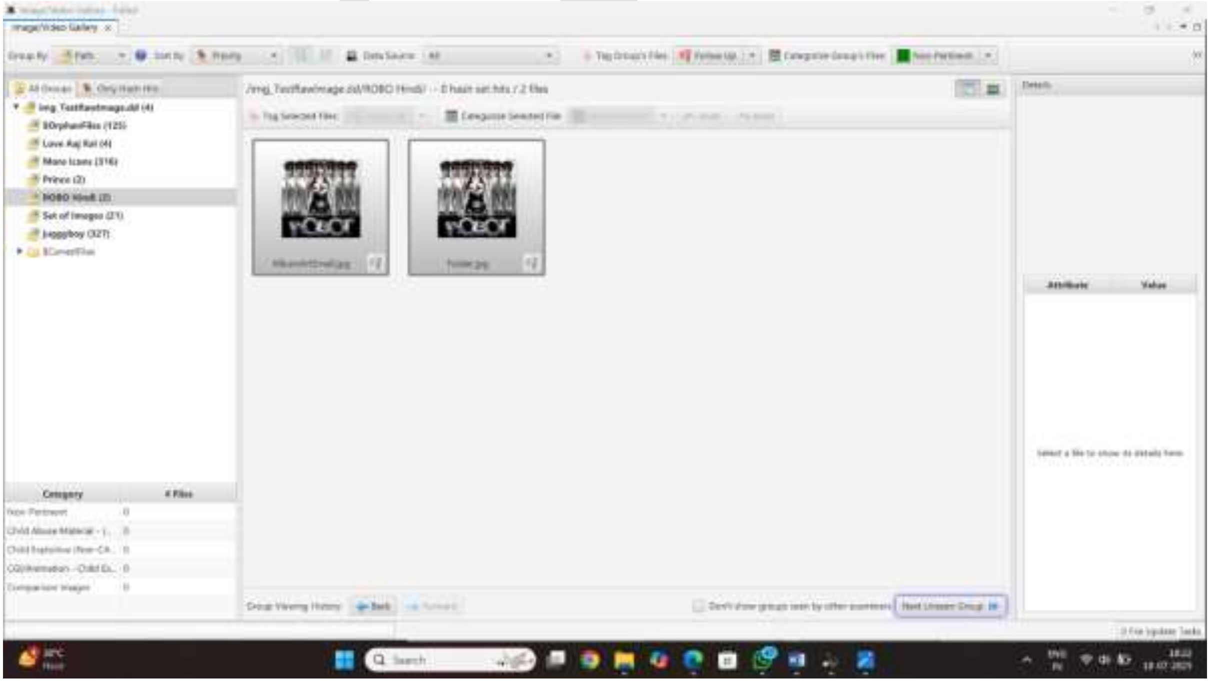
Item: TestRawImage.dd
Aggregate Score: Unknown

Analysis Result 1

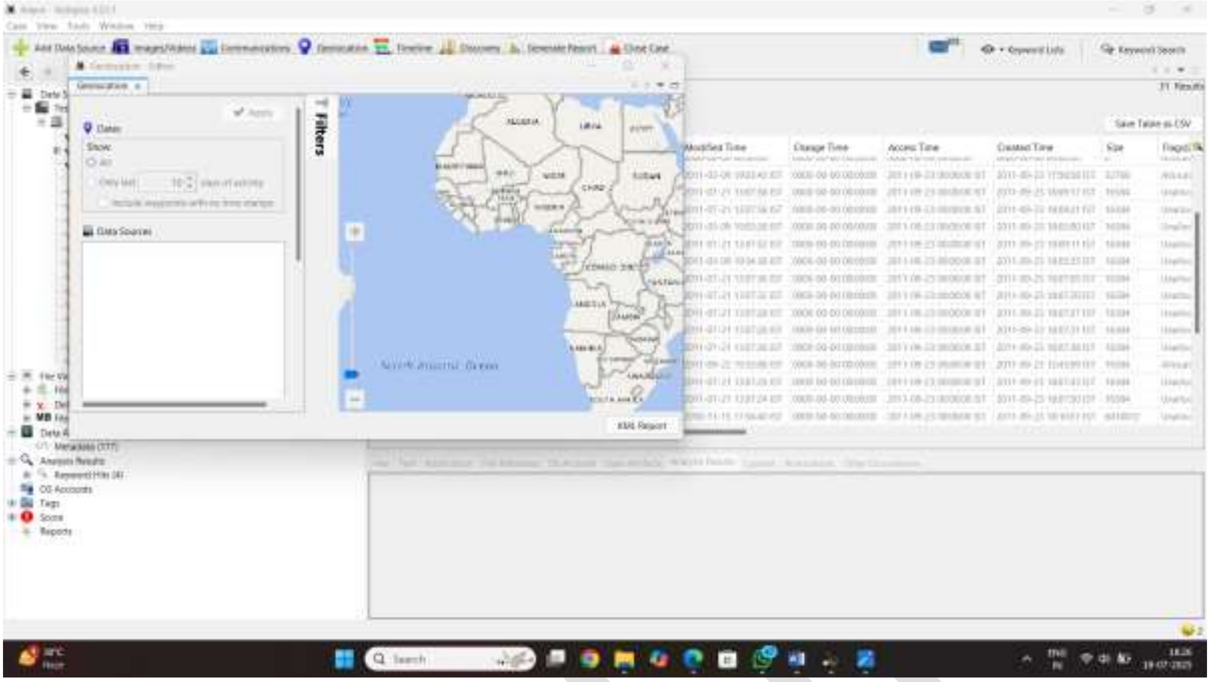
Score: Unknown
Type: Data Source Usage
Configuration:
Conclusion:
Justification:
Description: Flash Drive



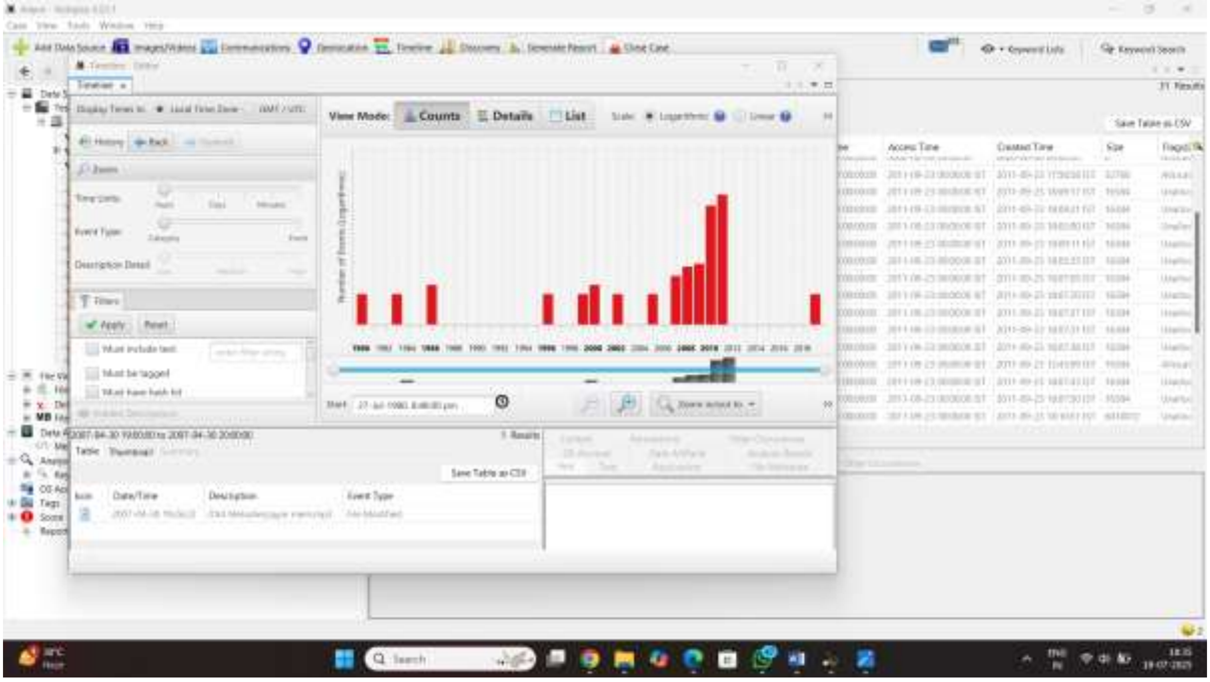
Step12 click on the image/videos option they vezible of image of folder

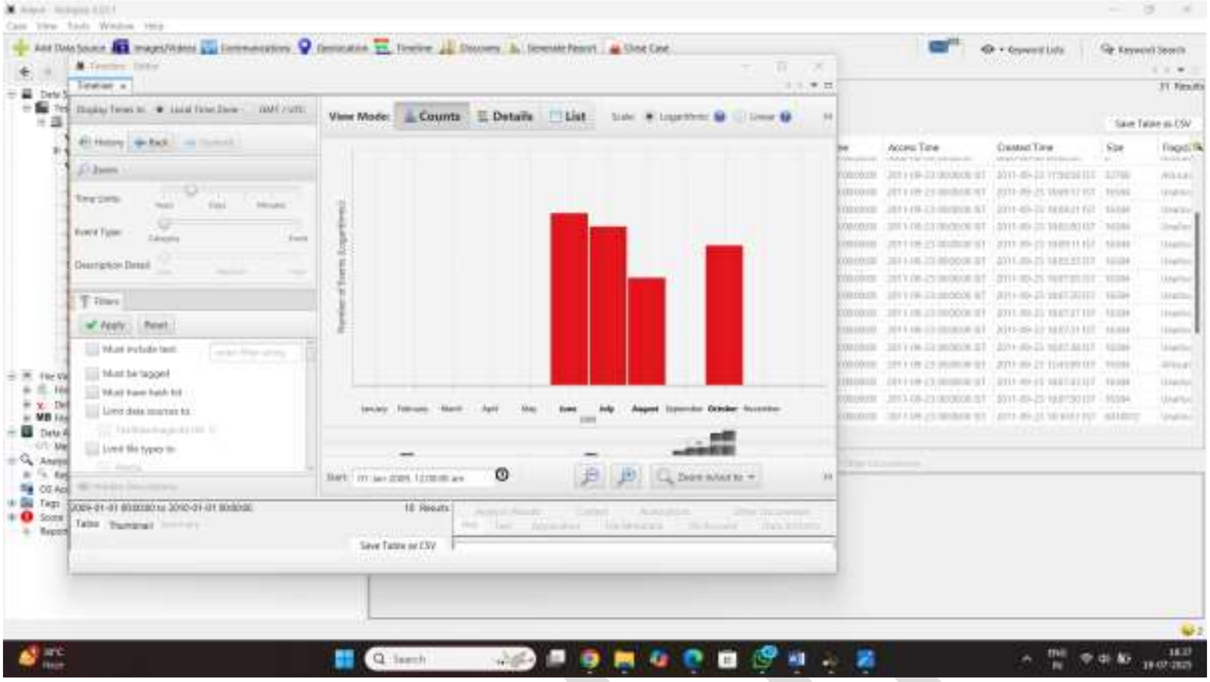


Step13 location on pic they are option in gelocation click on that and select the picture



Step14 timeline chart option

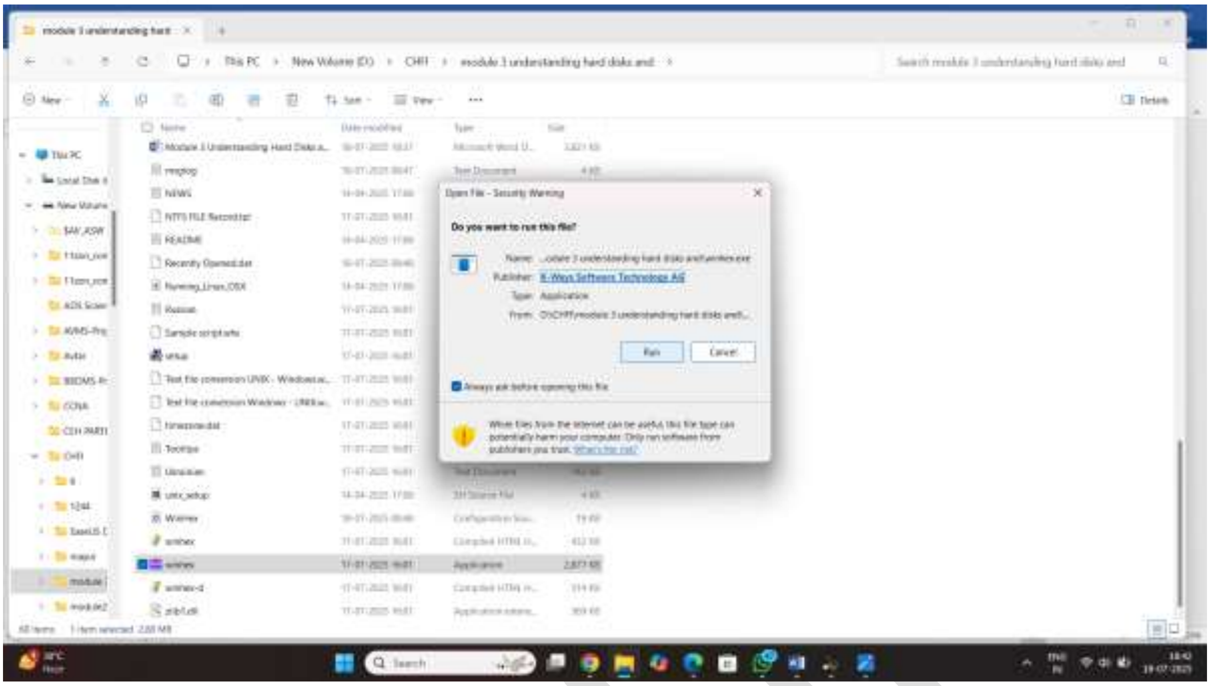




Lab2 recover delited data file image from hard disk there was tool called winhex

Step1 download the winhex

Step2 start the winhex



Open File - Security Warning

Do you want to run this file?

Name: ...odule 3 understanding hard disks and\winhex.exe

Publisher: X-Ways Software Technology AG

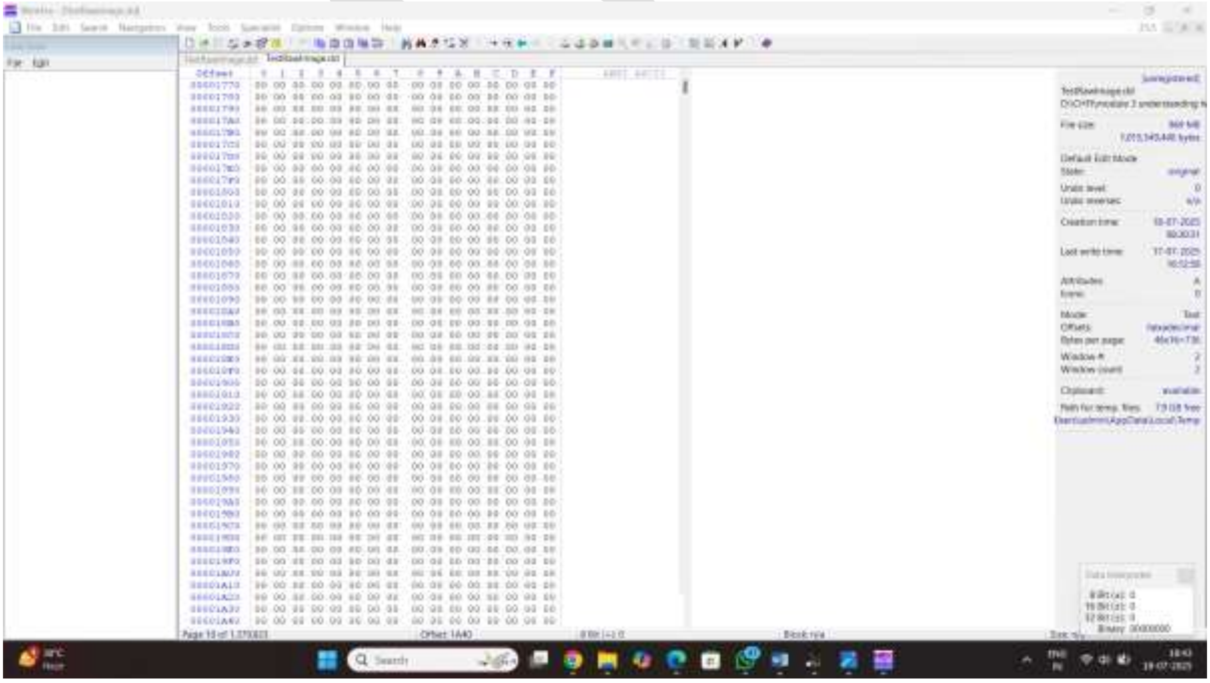
Type: Application

From: D:\CHFI\module 3 understanding hard disks and\...

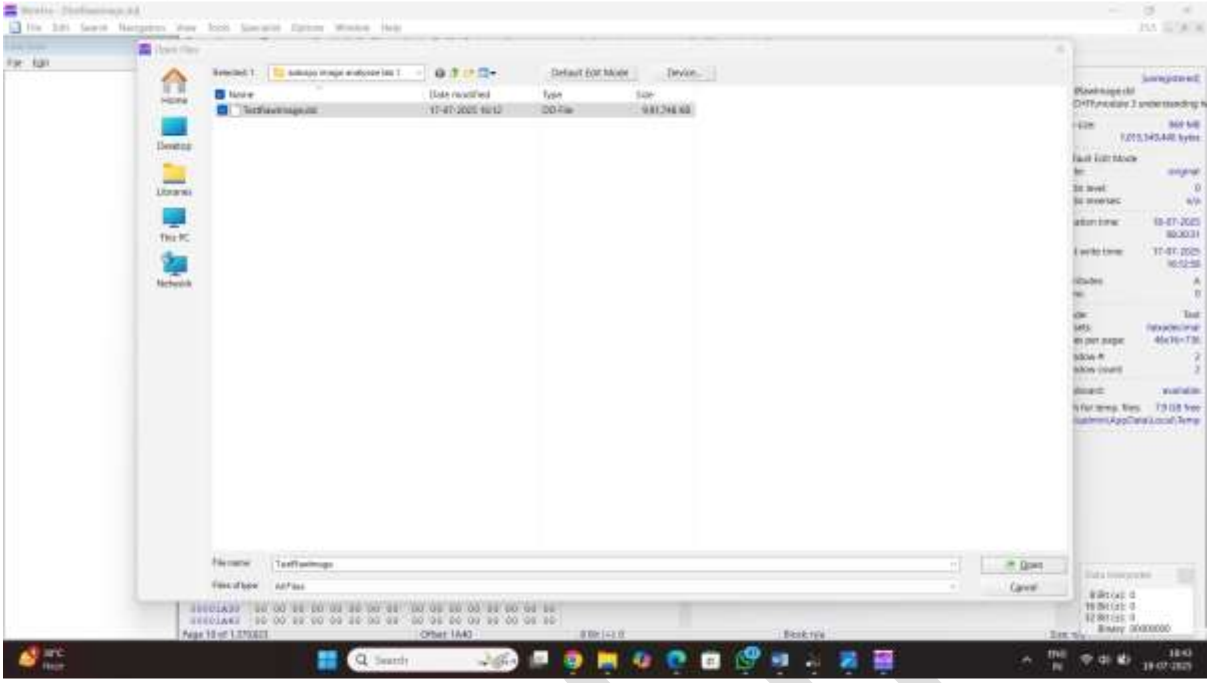
☑ Always ask before opening this file

While files from the Internet can be useful, this file type can potentially harm your computer. Only run software from publishers you trust. What's the risk?

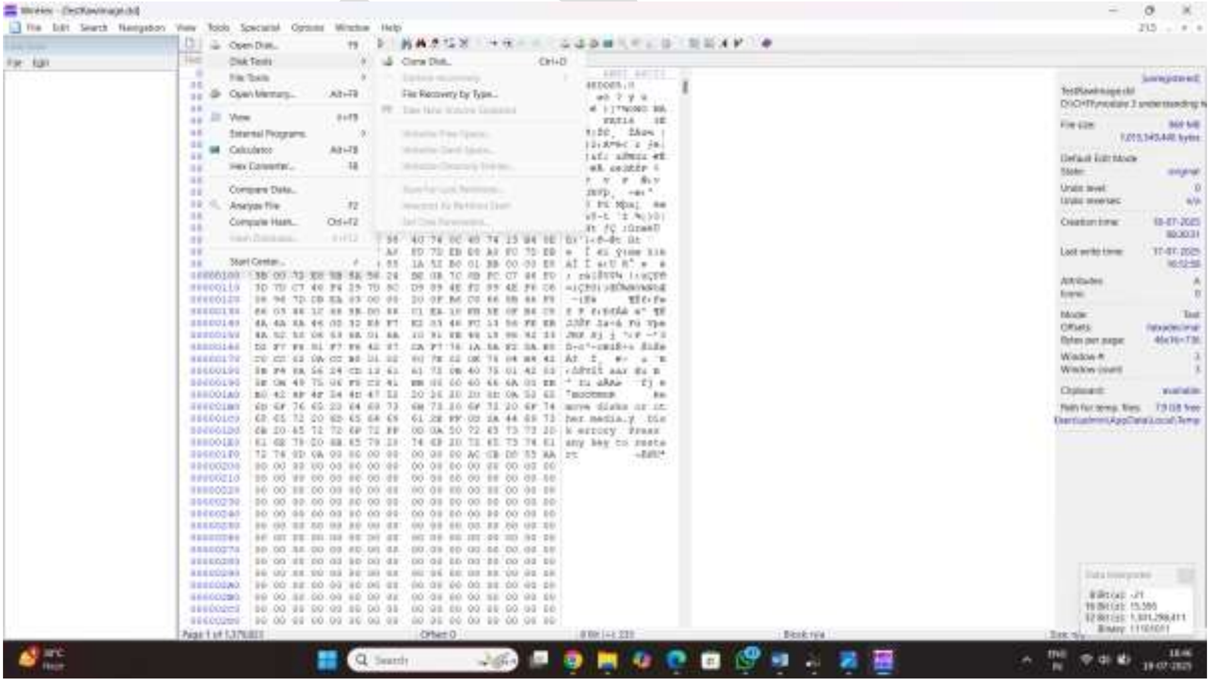
Step3 click on the open file



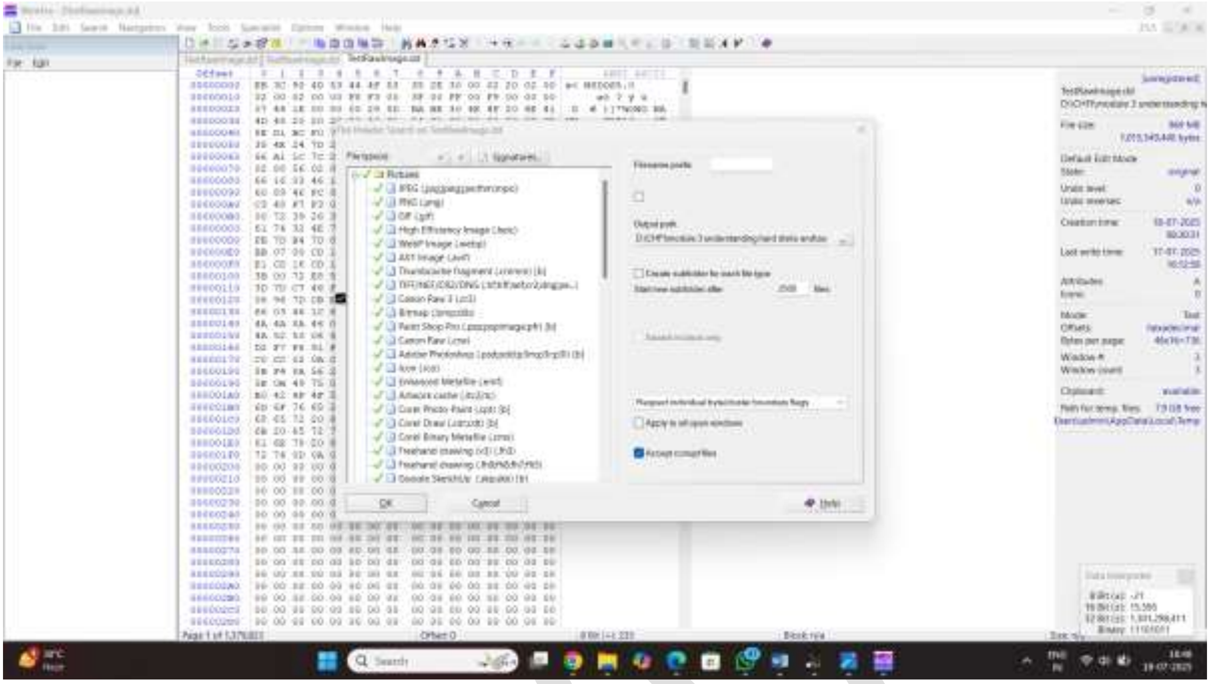
Step4: select the dd image



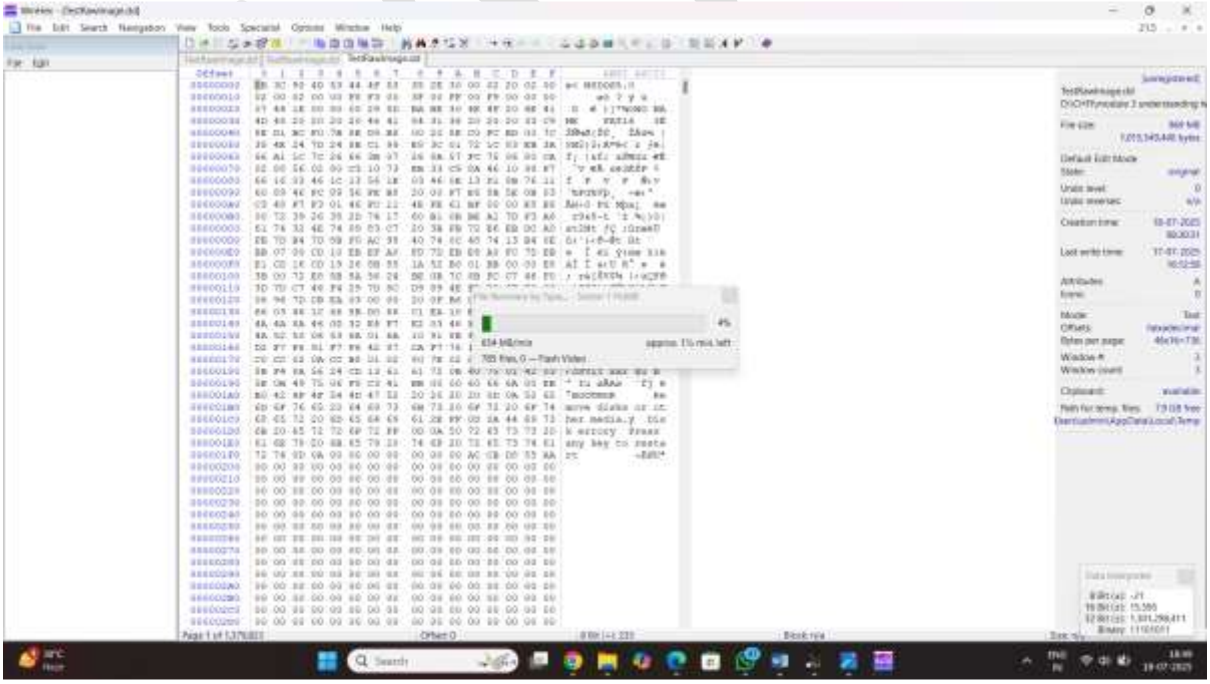
Step5 open disk tool select the option file recovery

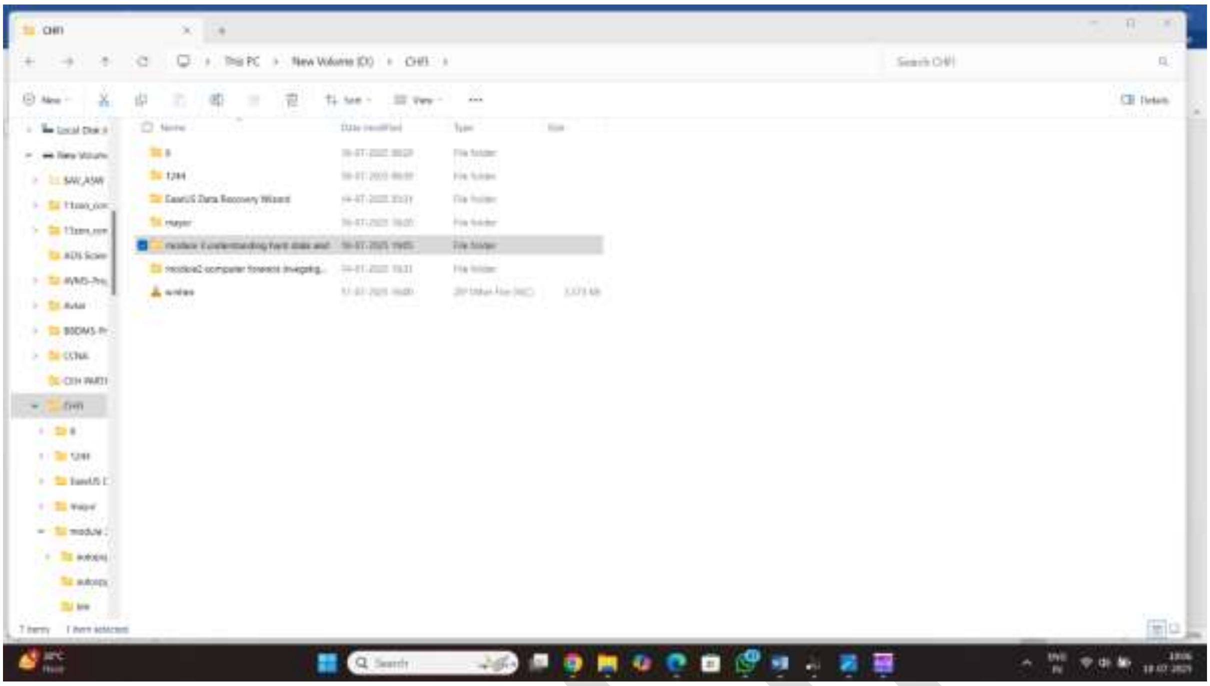


Step6: select the folder recover of data



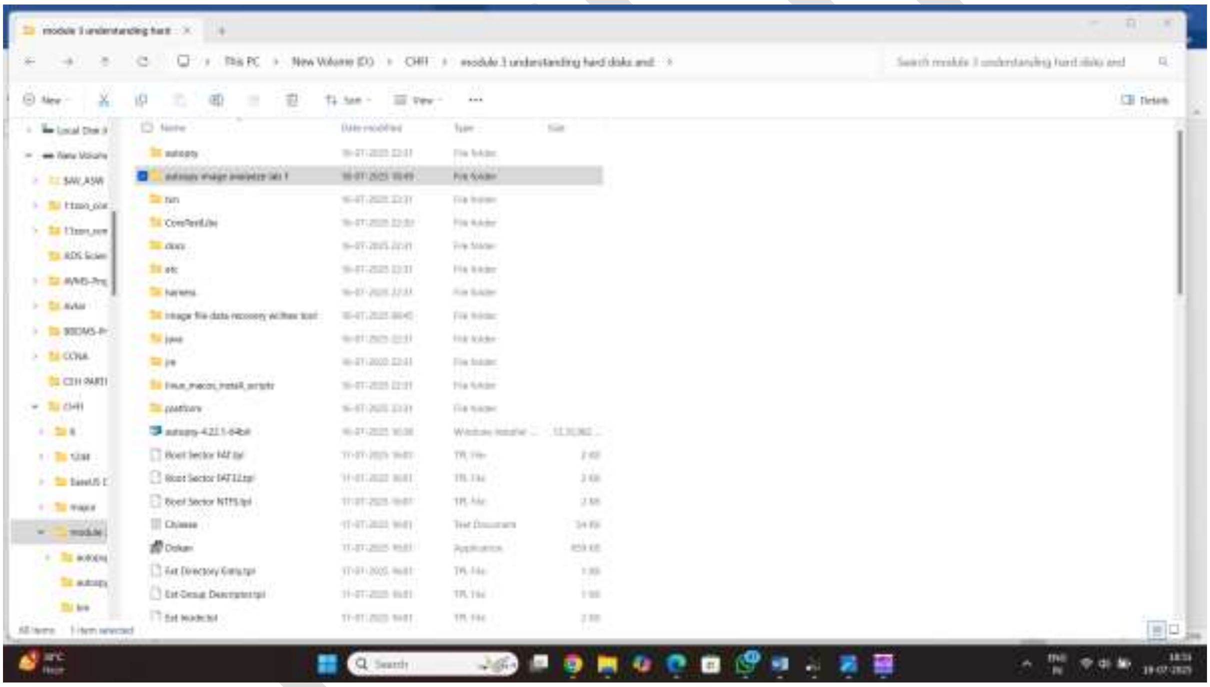
Click on next





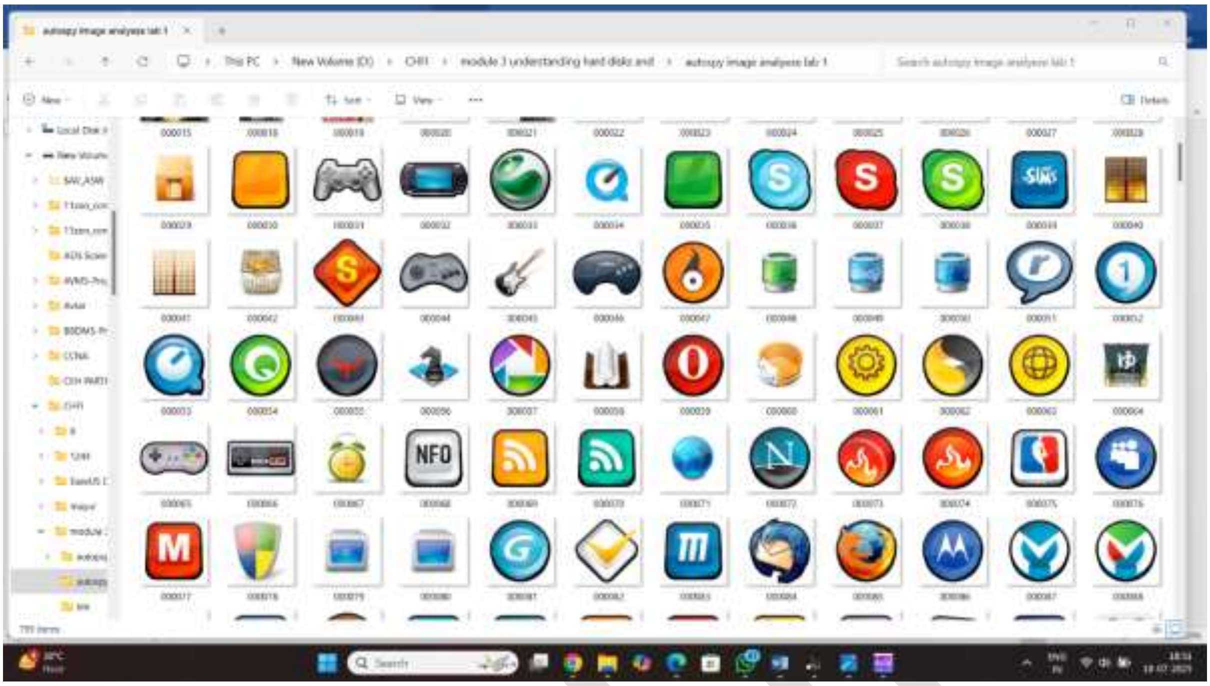
This PC › New Volume (D:) › CHFI ›

Name	Date modified	Type	Size
8	16-07-2025 08:29	File folder	
1244	16-07-2025 08:09	File folder	
EaseUS Data Recovery Wizard	14-07-2025 23:31	File folder	
major	16-07-2025 16:05	File folder	
module 3 understanding hard disks and	18-07-2025 19:05	File folder	
module2 computer forensic imaging...	14-07-2025 19:31	File folder	
winlnes	17-07-2025 16:00	ZIP (WinRAR) File (WIC)	3,573 KB



This PC › New Volume (D:) › CHFI › module 3 understanding hard disks and ›

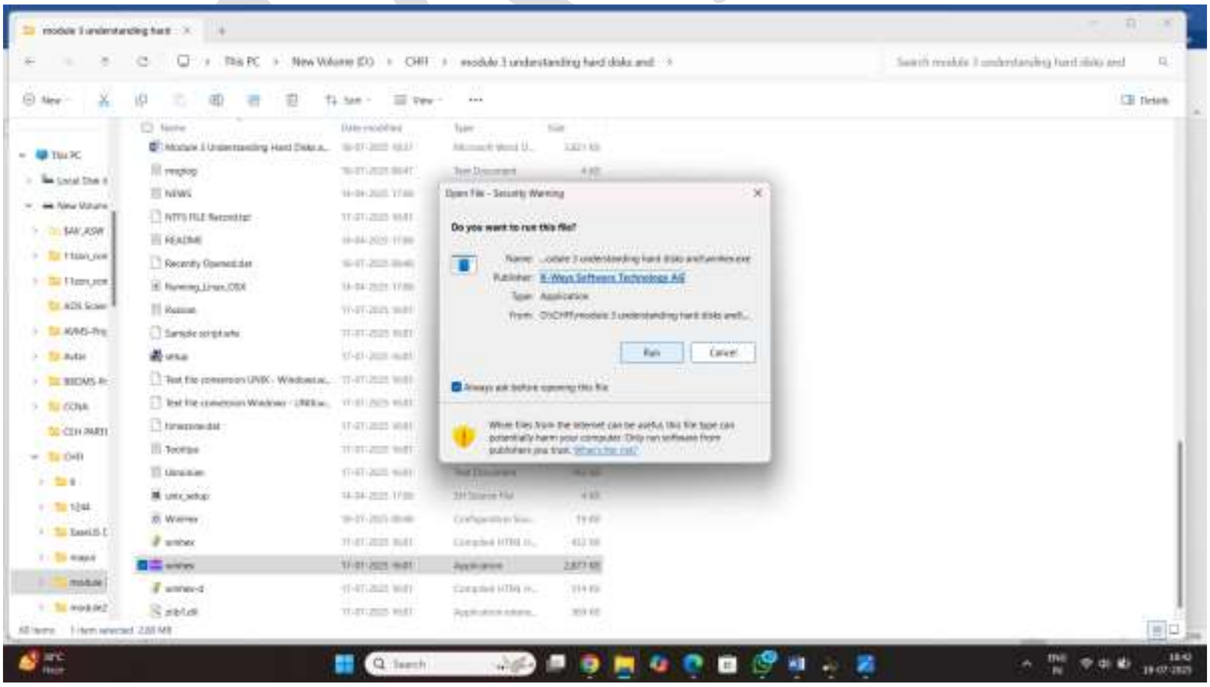
Name	Date modified	Type	Size
autopsy	16-07-2025 22:31	File folder	
autopsy image analyzer lab 1	18-07-2025 10:49	File folder	
bin	16-07-2025 22:31	File folder	
CoreFileLibs	16-07-2025 22:31	File folder	
docs	16-07-2025 22:31	File folder	
etc	16-07-2025 22:31	File folder	
harness	16-07-2025 22:31	File folder	
image file data recovery wi thee tool	18-07-2025 08:45	File folder	
java	16-07-2025 22:31	File folder	
jre	16-07-2025 22:31	File folder	
linux_macos_install_scripts	16-07-2025 22:31	File folder	
platform	16-07-2025 22:31	File folder	
autopsy-4.22.1-64bit	16-07-2025 10:38	Windows Installer ...	12,30,382 ...
Boot Sector FAT.tpl	11-07-2025 16:01	TPL File	2 KB
Boot Sector FAT32.tpl	11-07-2025 16:01	TPL File	2 KB
Boot Sector NTFS.tpl	11-07-2025 16:01	TPL File	2 KB
Chinese	11-07-2025 16:01	Text Document	34 KB
Diskan	11-07-2025 16:01	Application	859 KB
Ext Directory Entry.tpl	11-07-2025 16:01	TPL File	1 KB
Ext Group Descriptor.tpl	11-07-2025 16:01	TPL File	1 KB
Ext Inode.tpl	11-07-2025 16:01	TPL File	2 KB



This PC › New Volume (D:) › CHFI › module 3 understanding hard disks and › autopsy image analyses lab 1

Lab3 how to identify image hex value

Step1 Start the hex value



This PC › New Volume (D:) › CHFI › module 3 understanding hard disks and ›

Open File - Security Warning

Do you want to run this file?

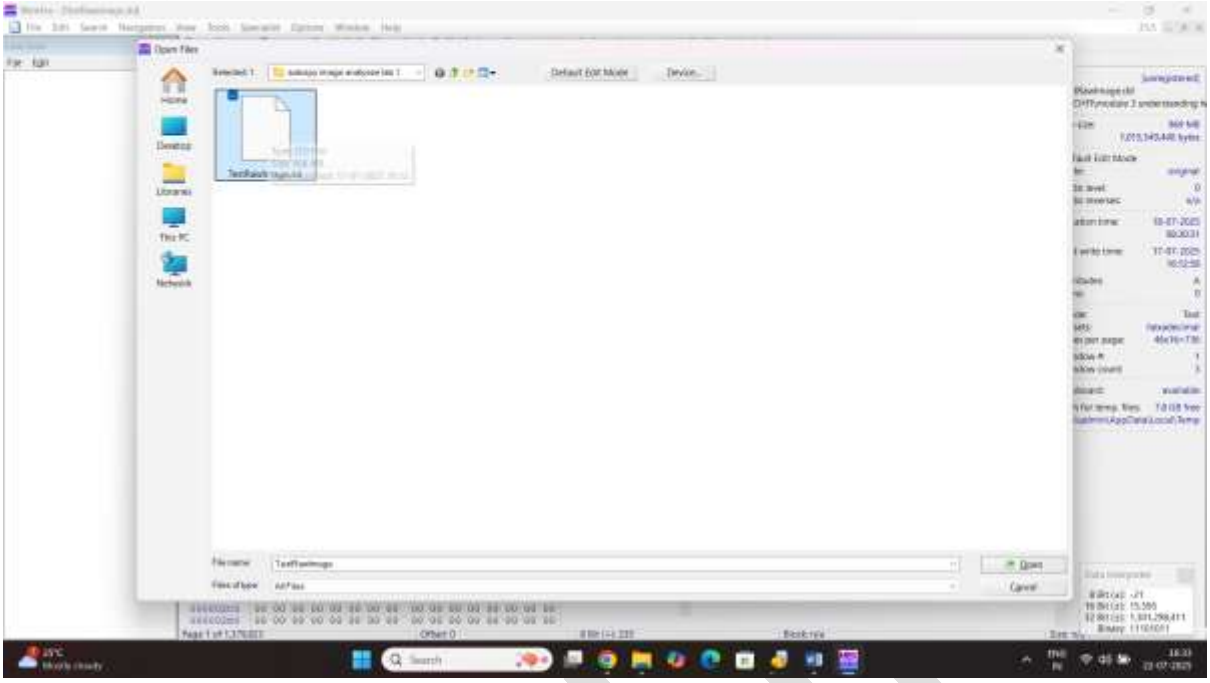
Name: ...odule 3 understanding hard disks and\winhex.exe
Publisher: X-Ways Software Technology AG
Type: Application
From: D:\CHFI\module 3 understanding hard disks and\...

Run | Cancel

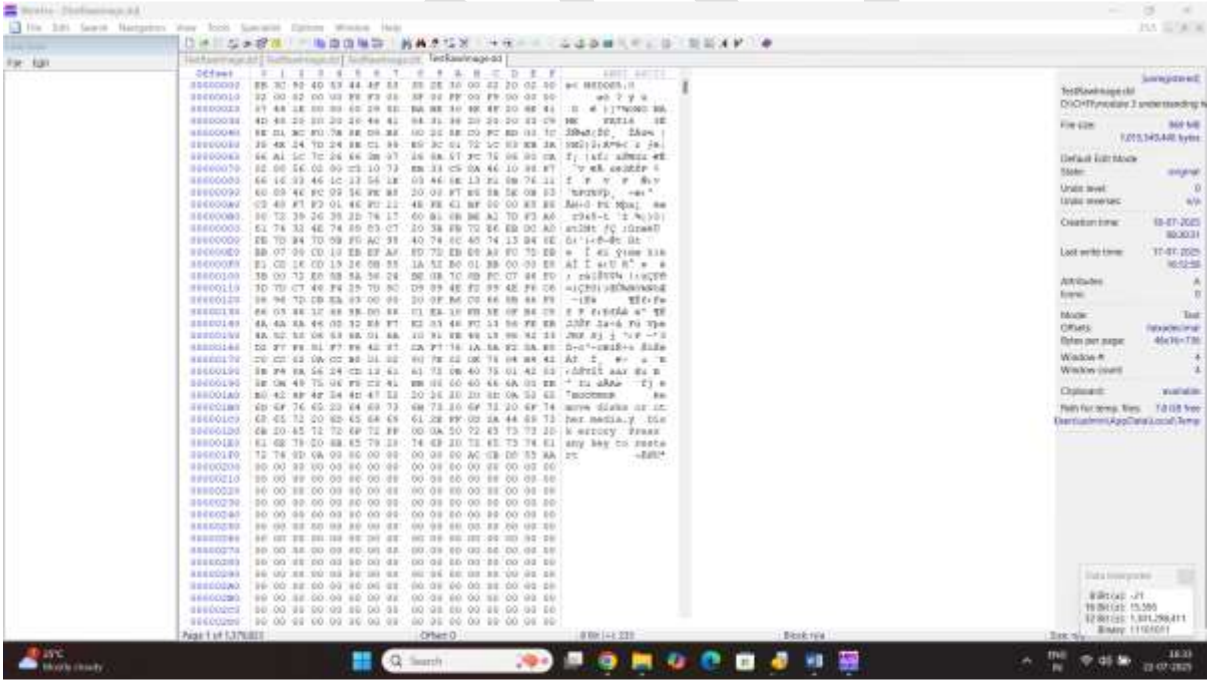
☑ Always ask before opening this file

While files from the Internet can be useful, this file type can potentially harm your computer. Only run software from publishers you trust. What's the risk?

Step2 select the dd image file


Open Files
Home
Desktop
Libraries
This PC
Network
Default Edit Mode
Device...
File name:
Files of type:
Open
Cancel

Result:


Offset
File size
Default Edit Mode
Creation time
Last write time
Attributes
Mode
Offsets
Bytes per page
Clipboard