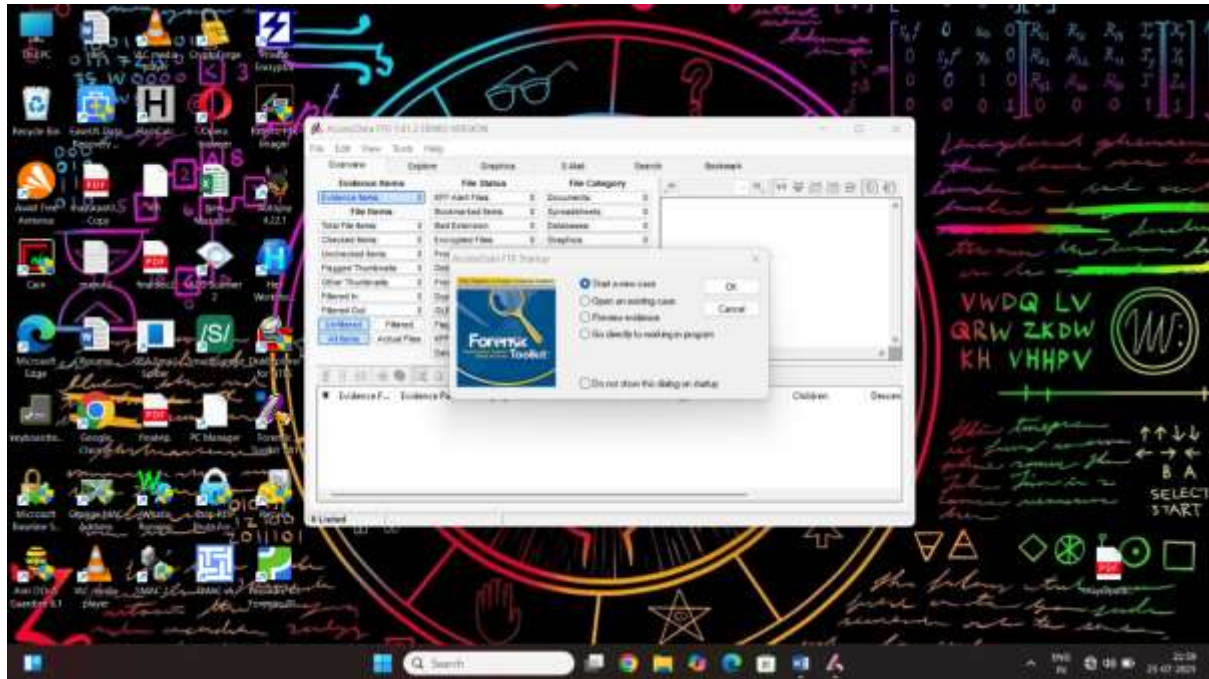


Module 5 Defeating anti forensics techniques

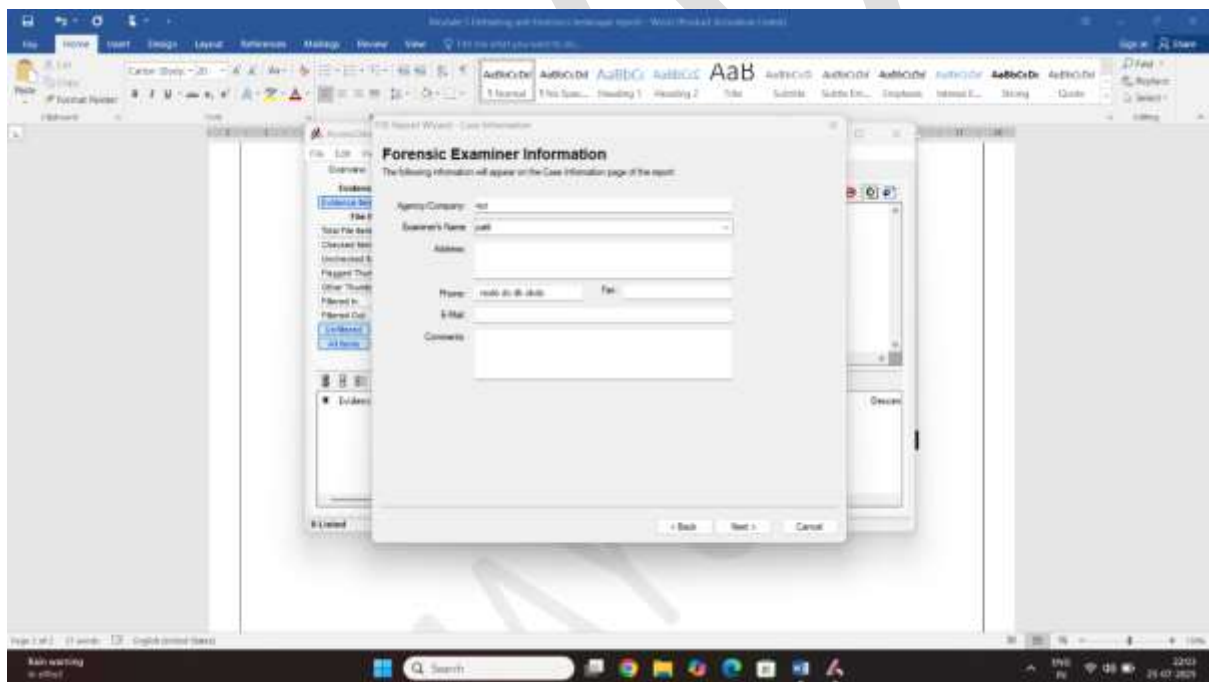
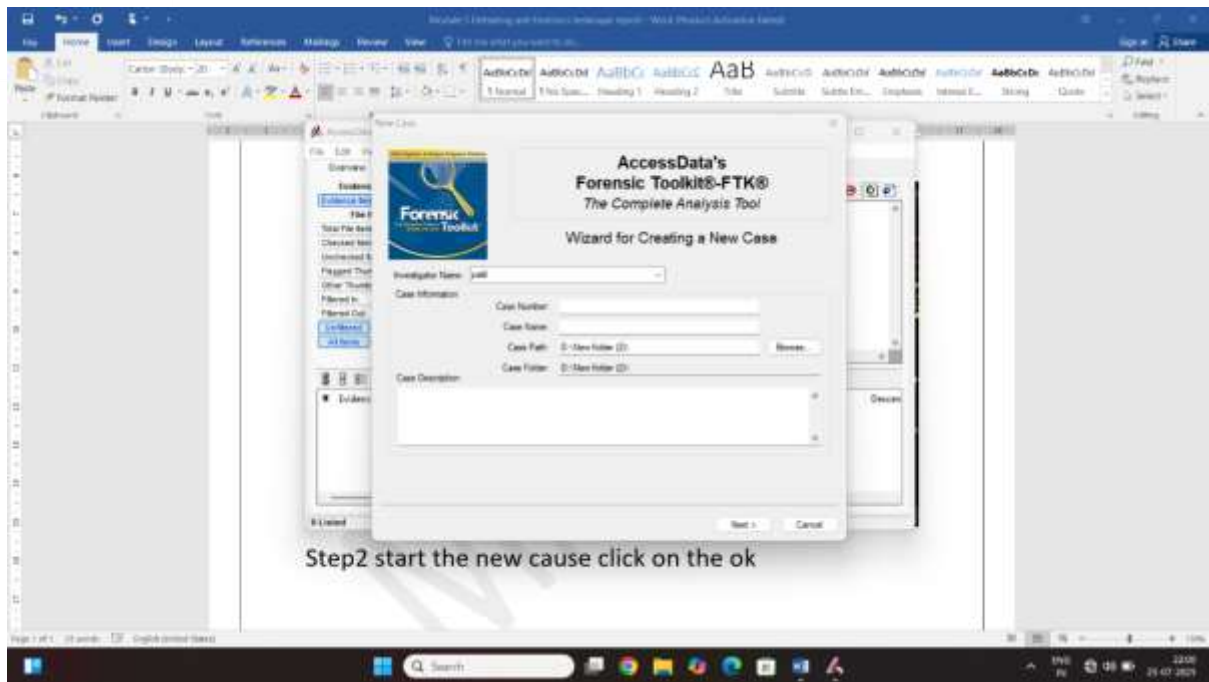
lab 1 using forensic tool

step1 start the forensic tool



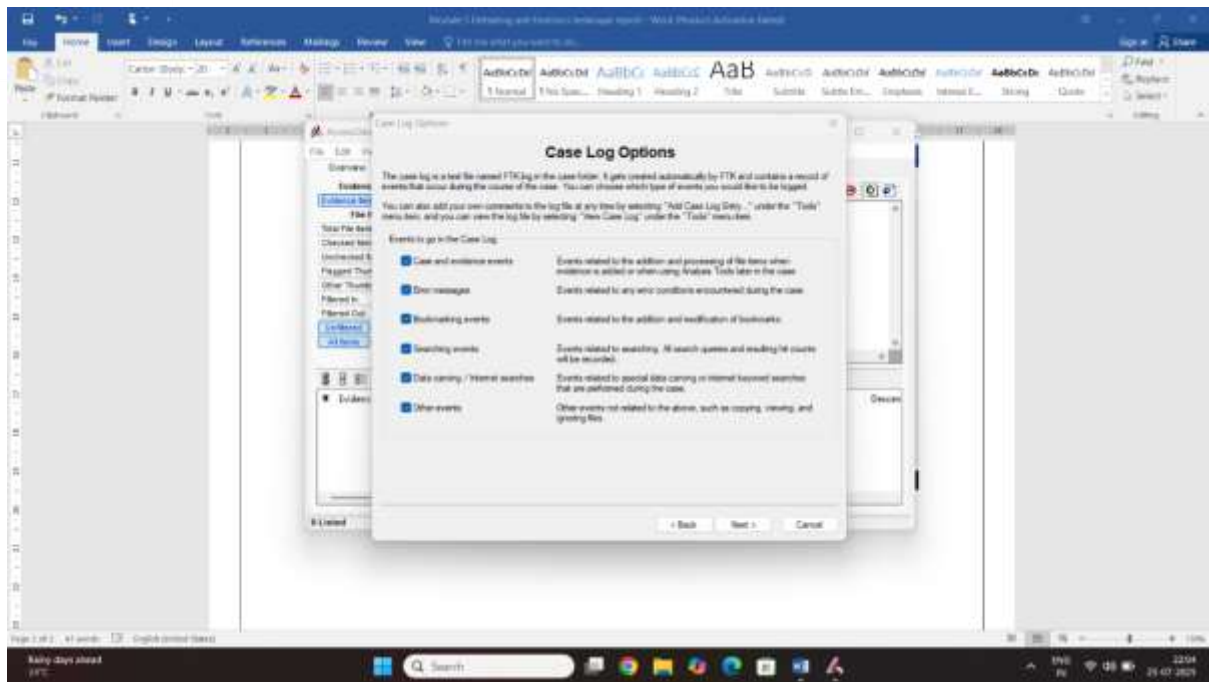
Step2 start the new cause click on the ok

Step3 enter cause details , name , number, and destination file etc

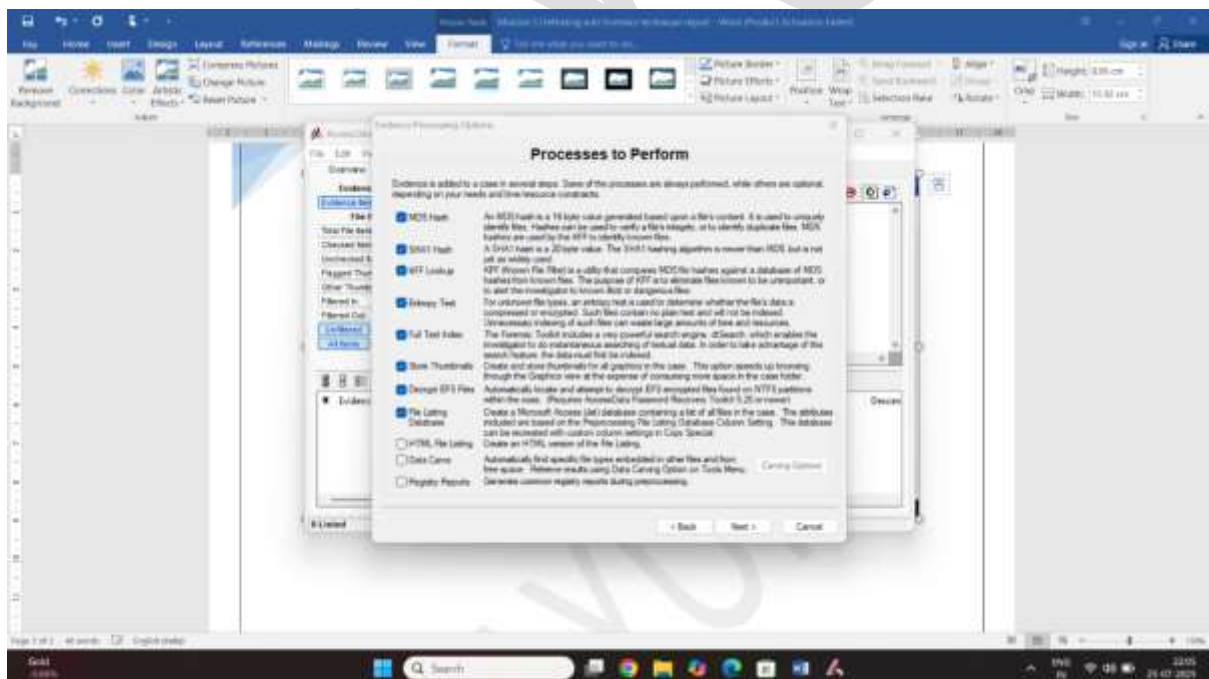


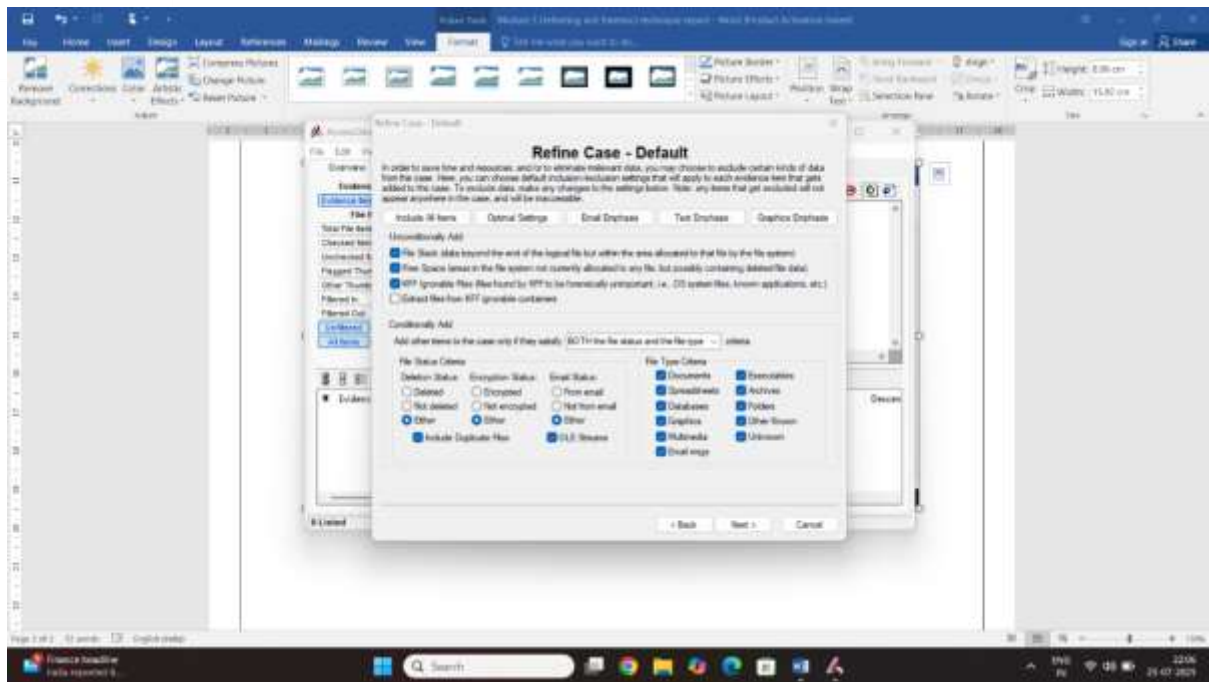
Click on the next

Step4 select case log option

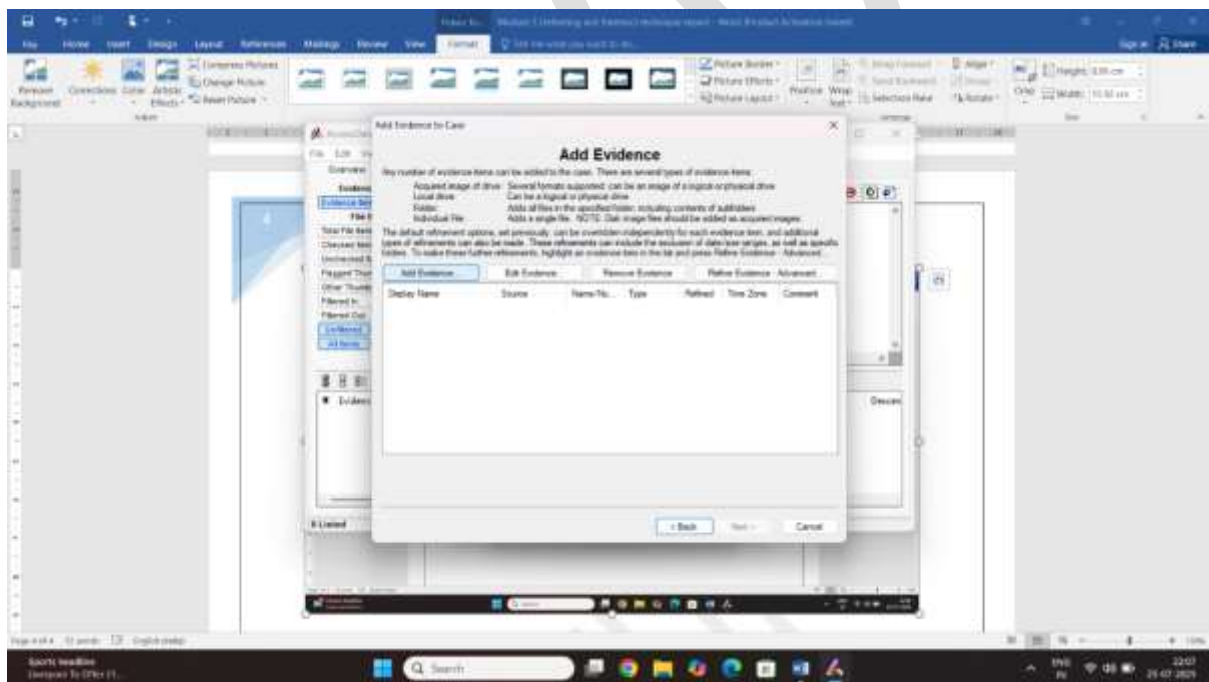


Step5 select the process to performe

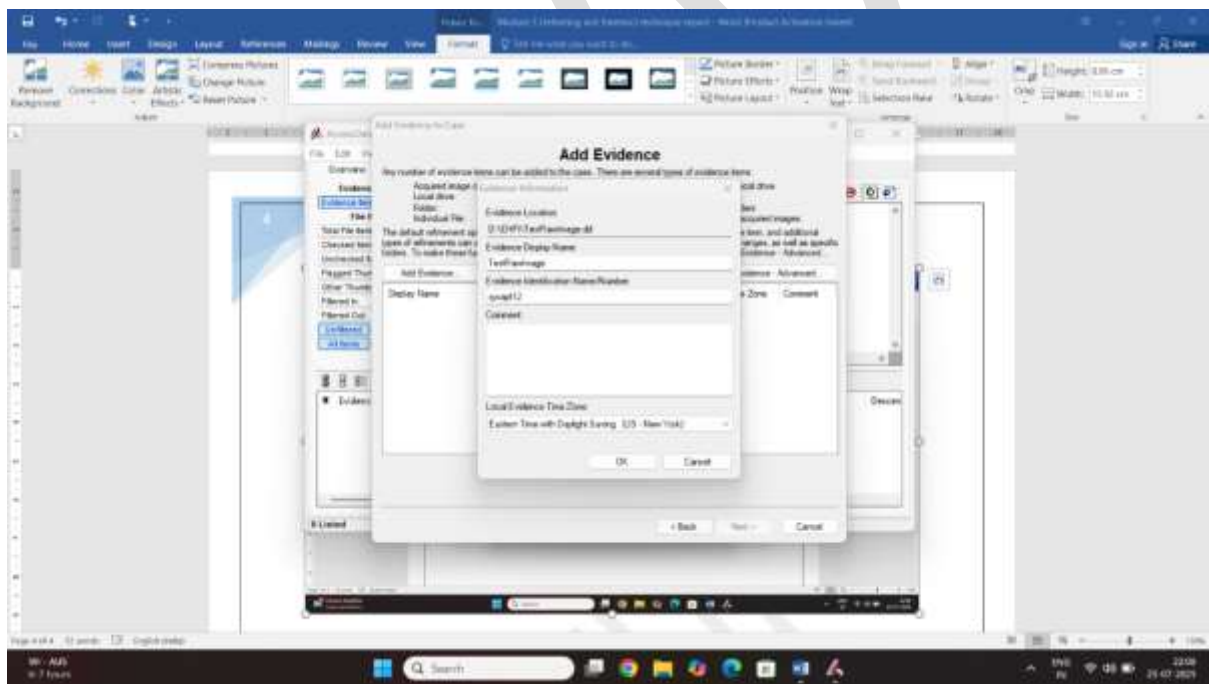
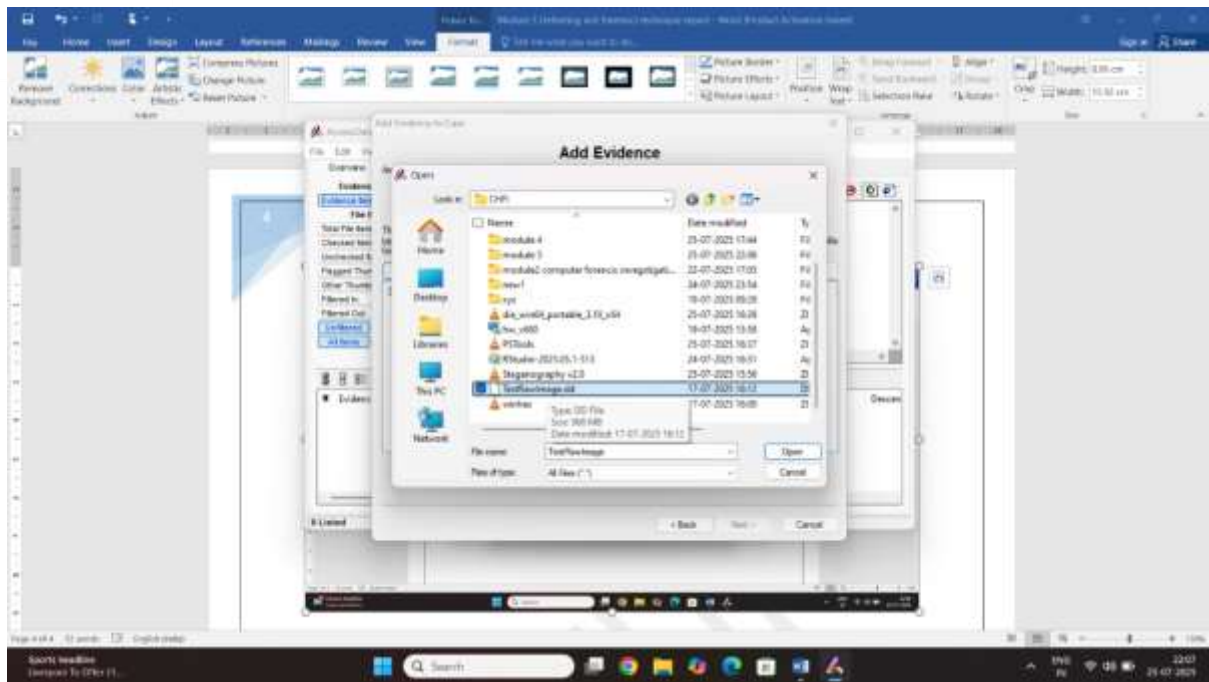




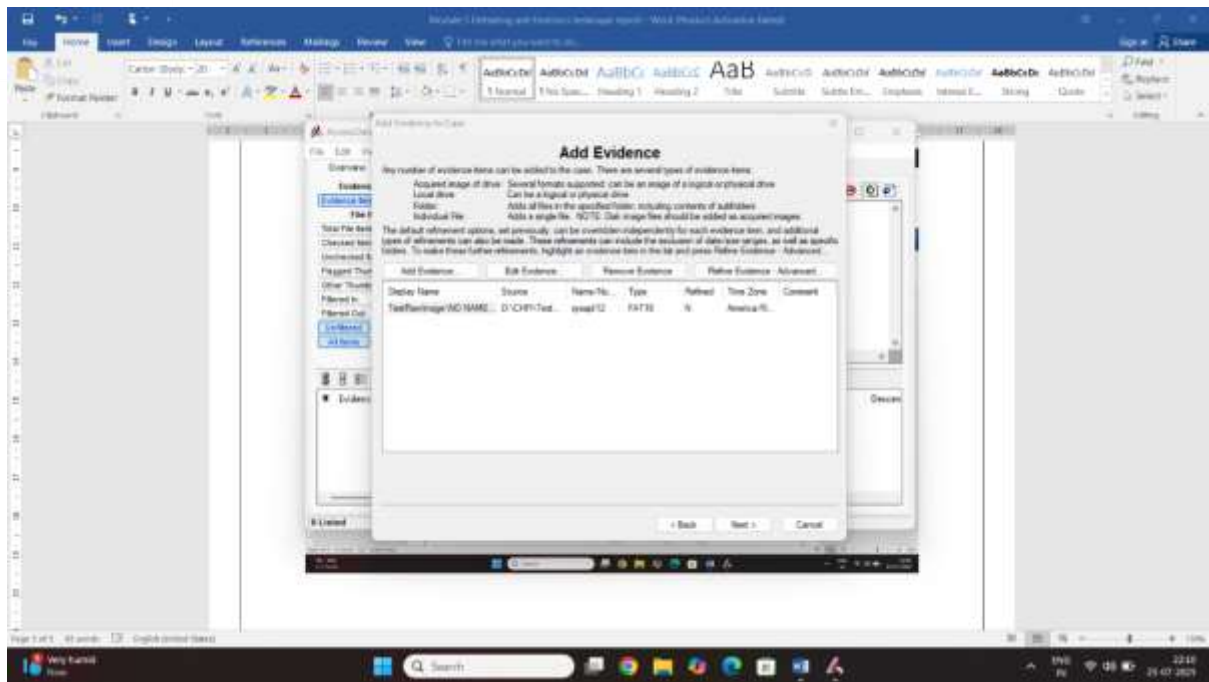
Step6 add evidence file dd image click on



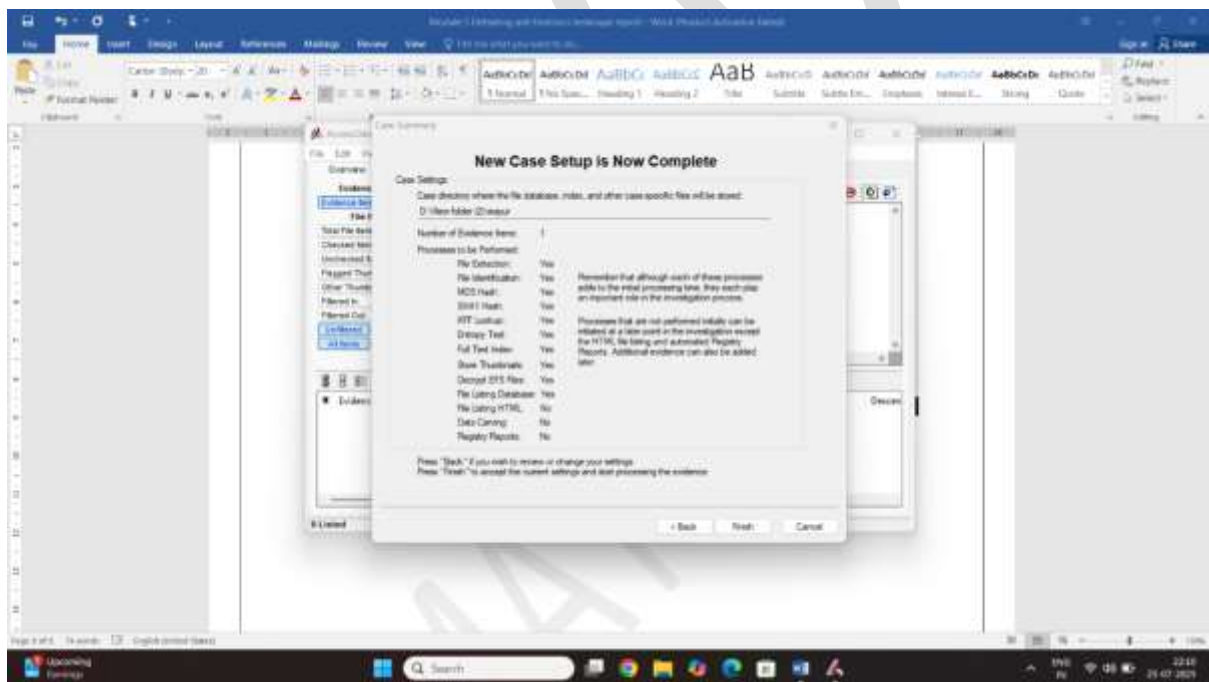
Step7 select the d.d image



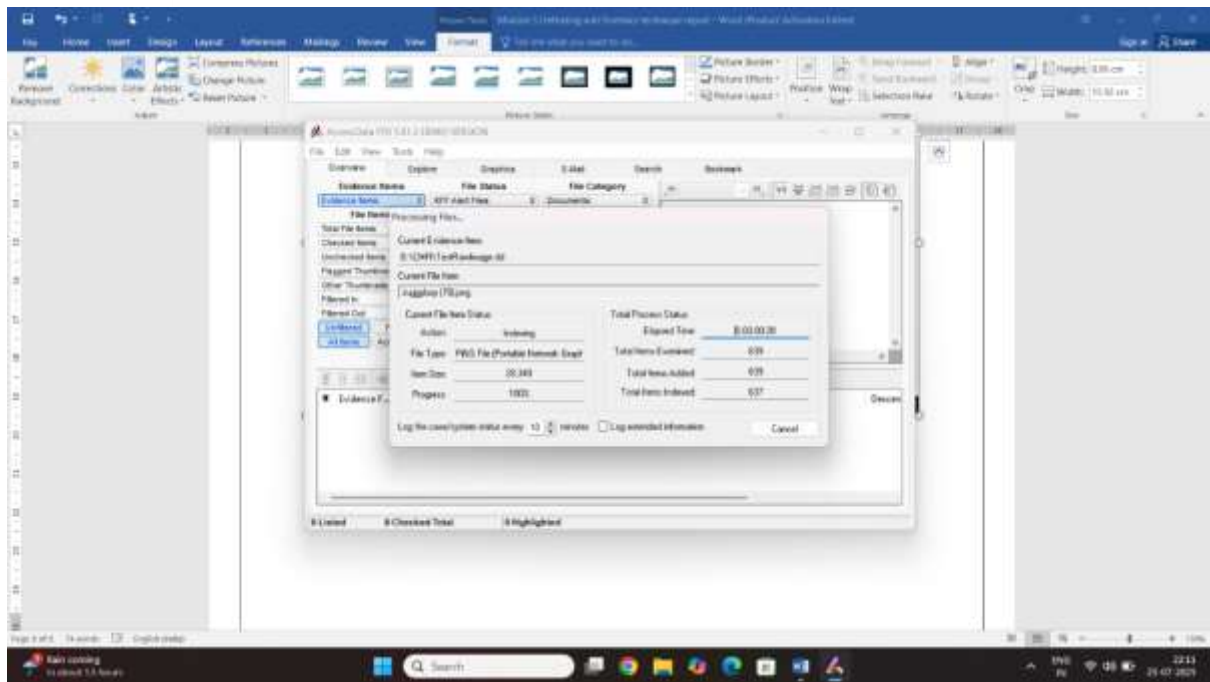
Step8 add successful evidence file



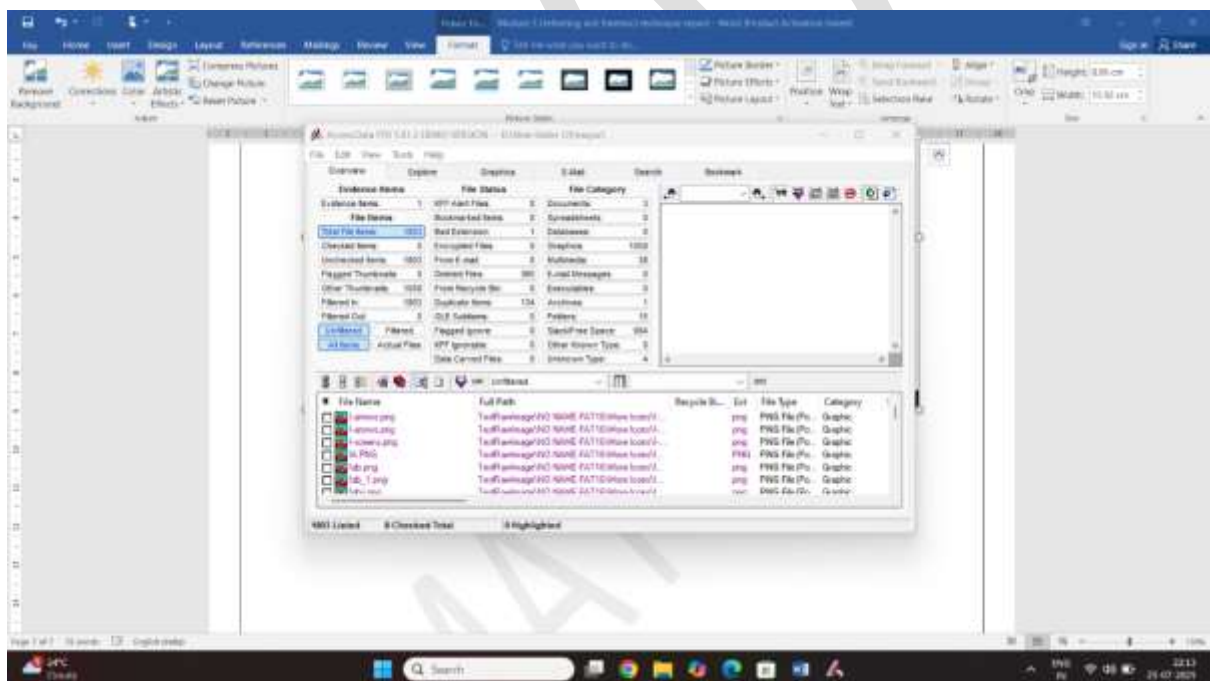
Click on the next

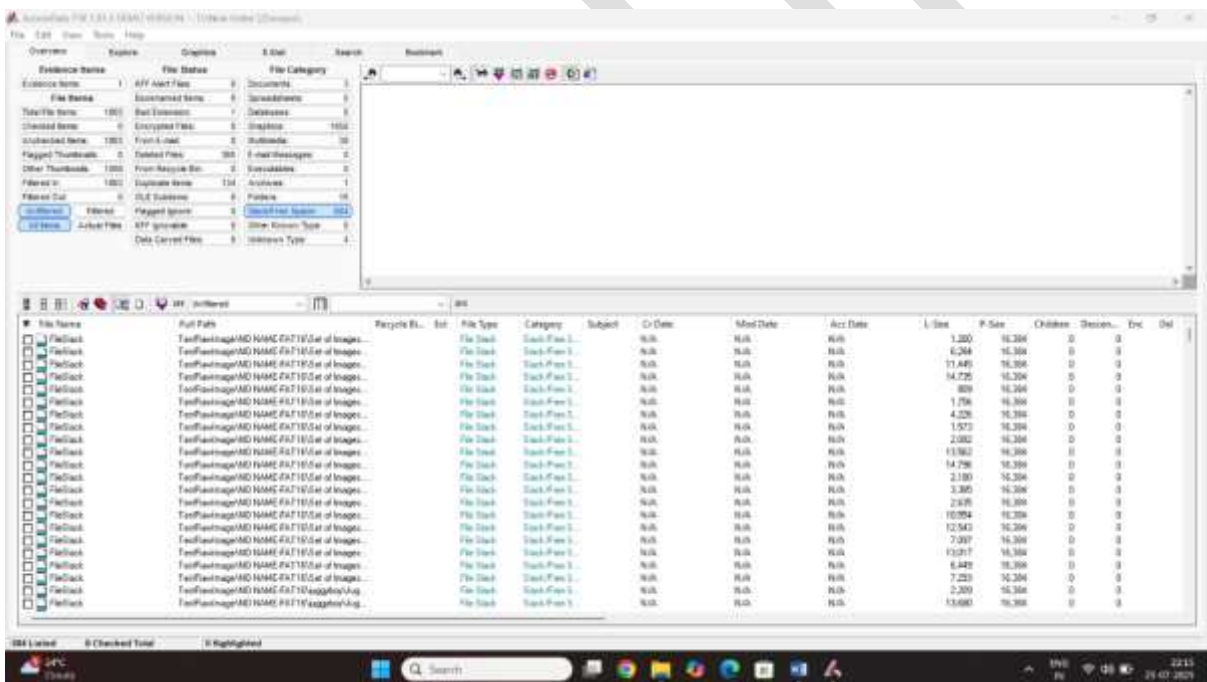
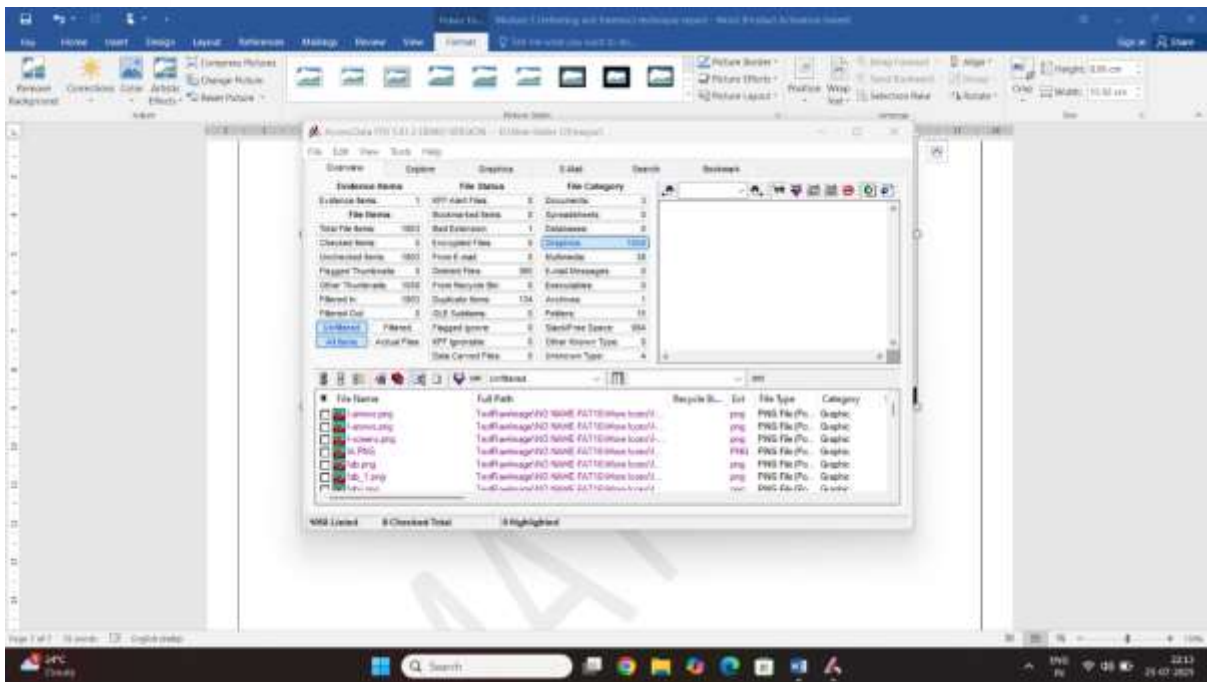


Carving the data process



Result



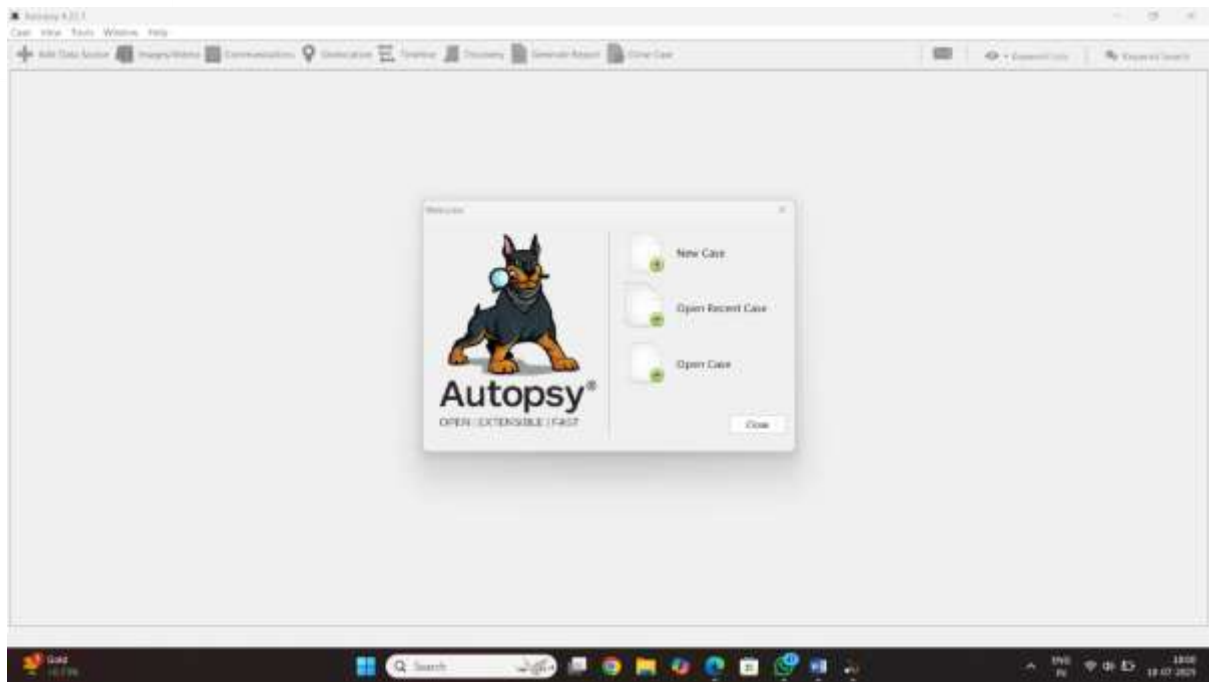


Lab2 SSD file carving on a windows file system

Using Autopsy

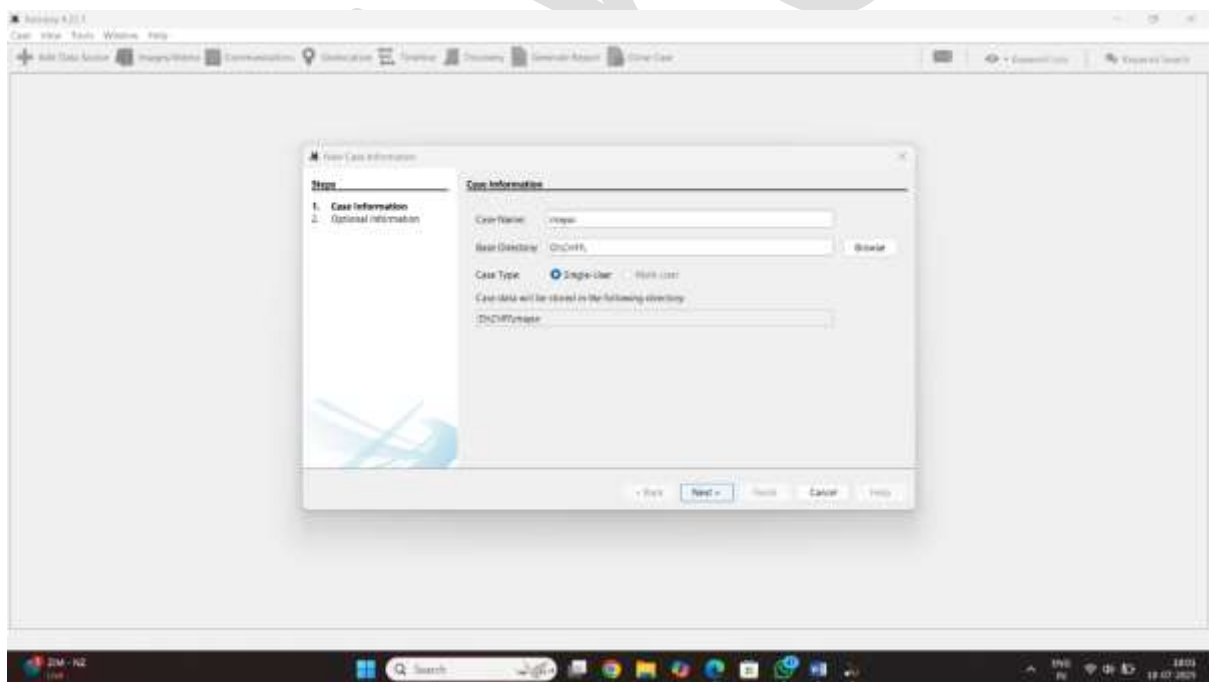
Step1: download the autopsy in windows

Step2: start the autopsy and click on the new cause

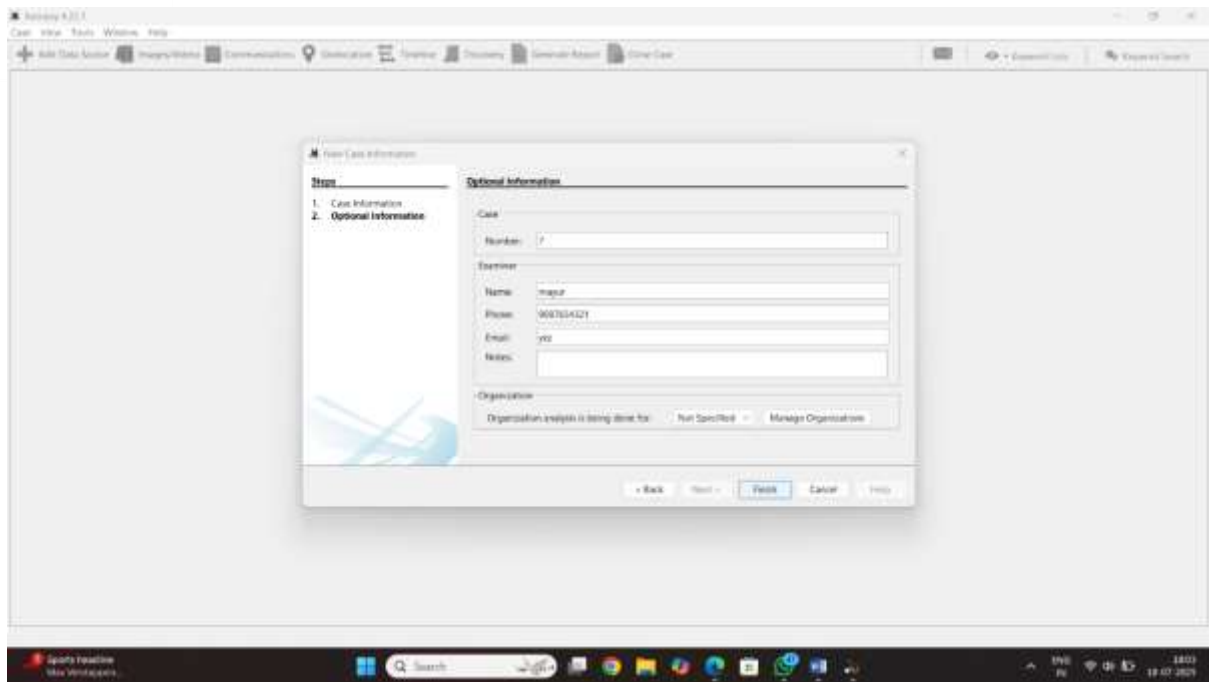


Step3: enter case name

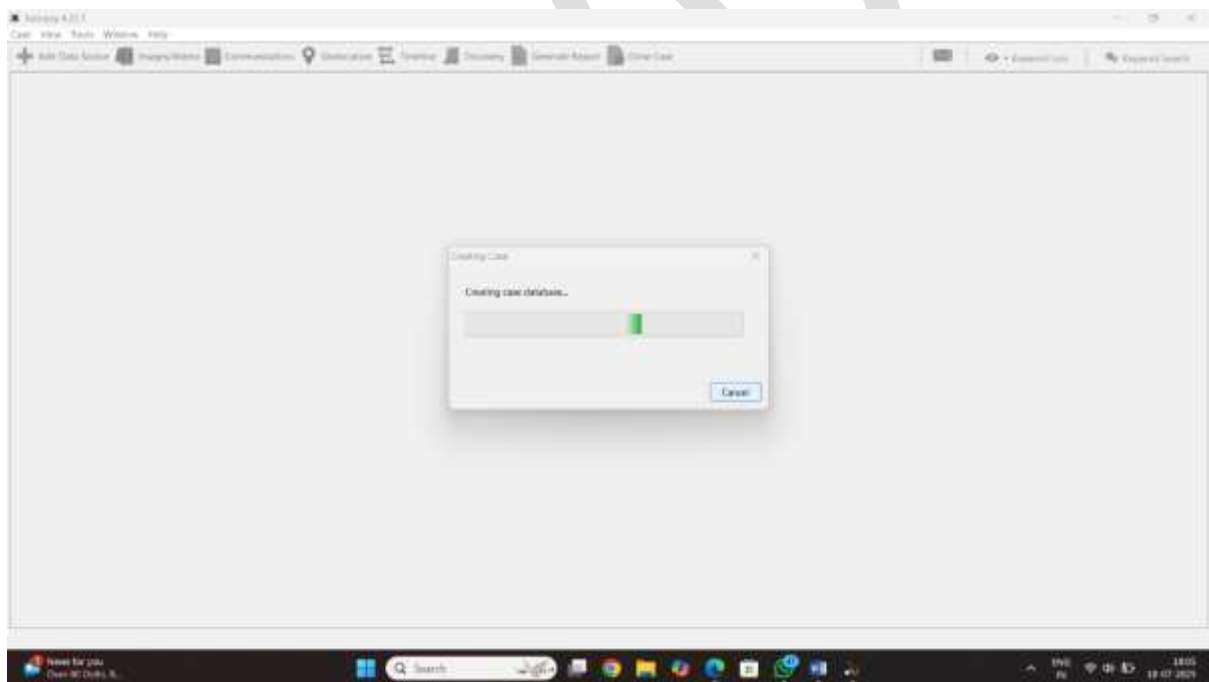
Step4: select the case file destination



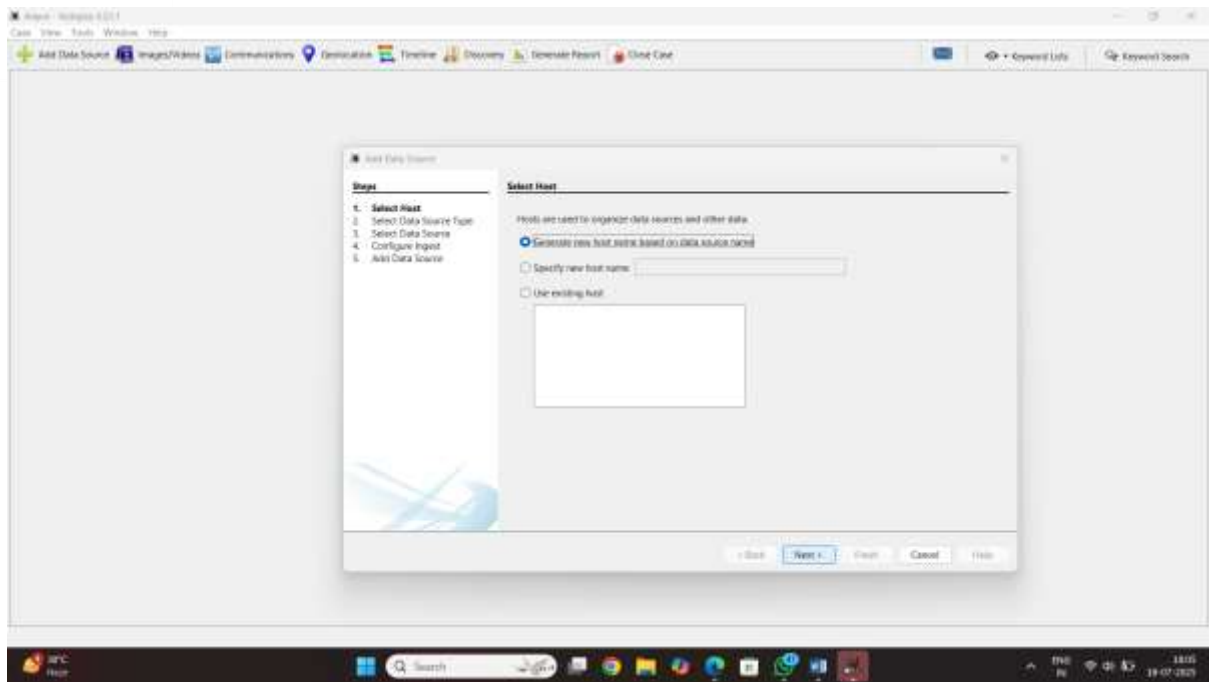
Step5 select the cause number, name ,email,
m.number click on next



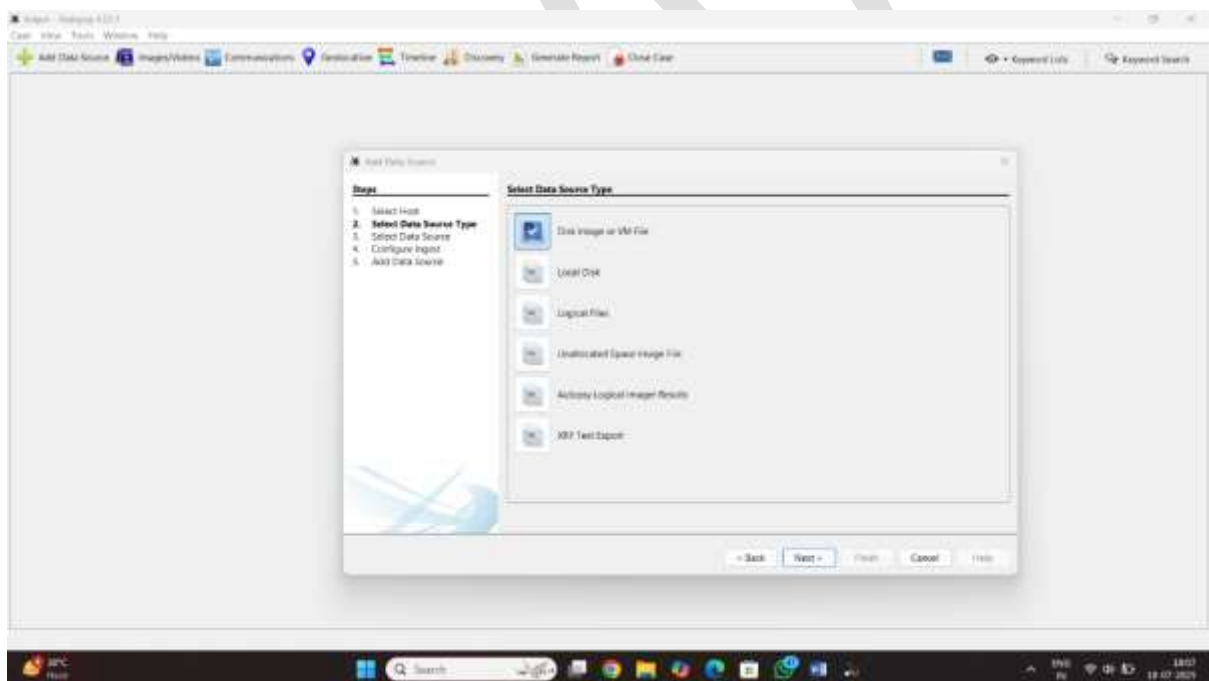
Step6 creating data base cause file



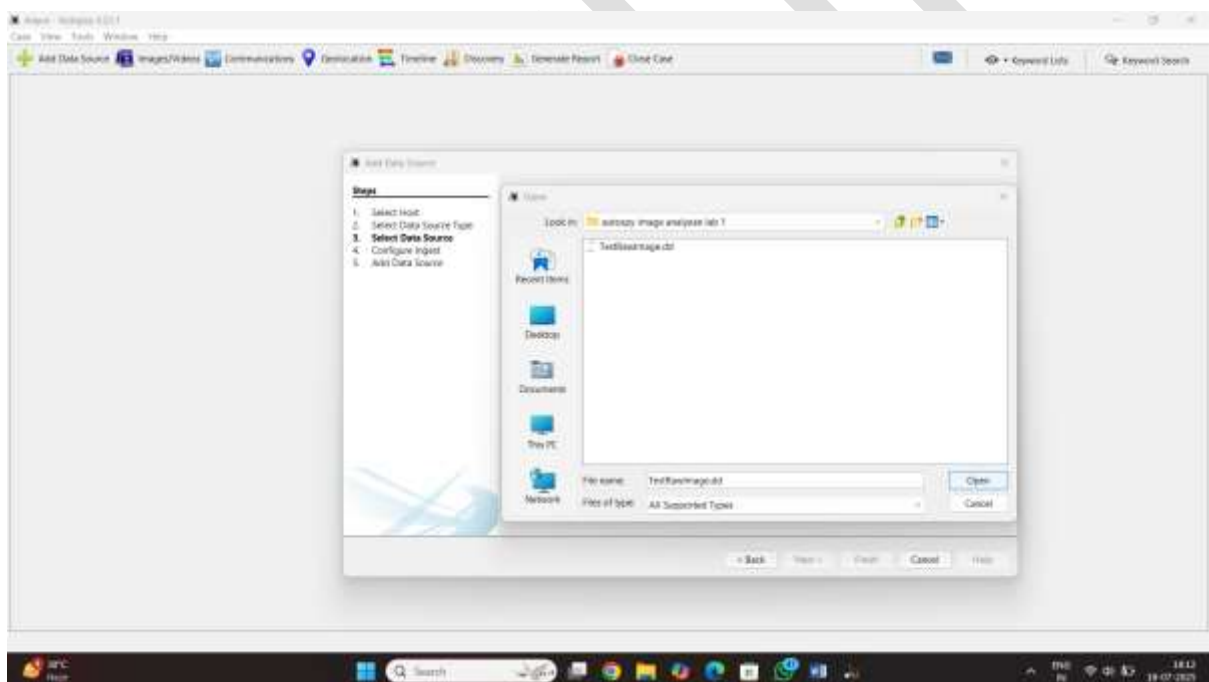
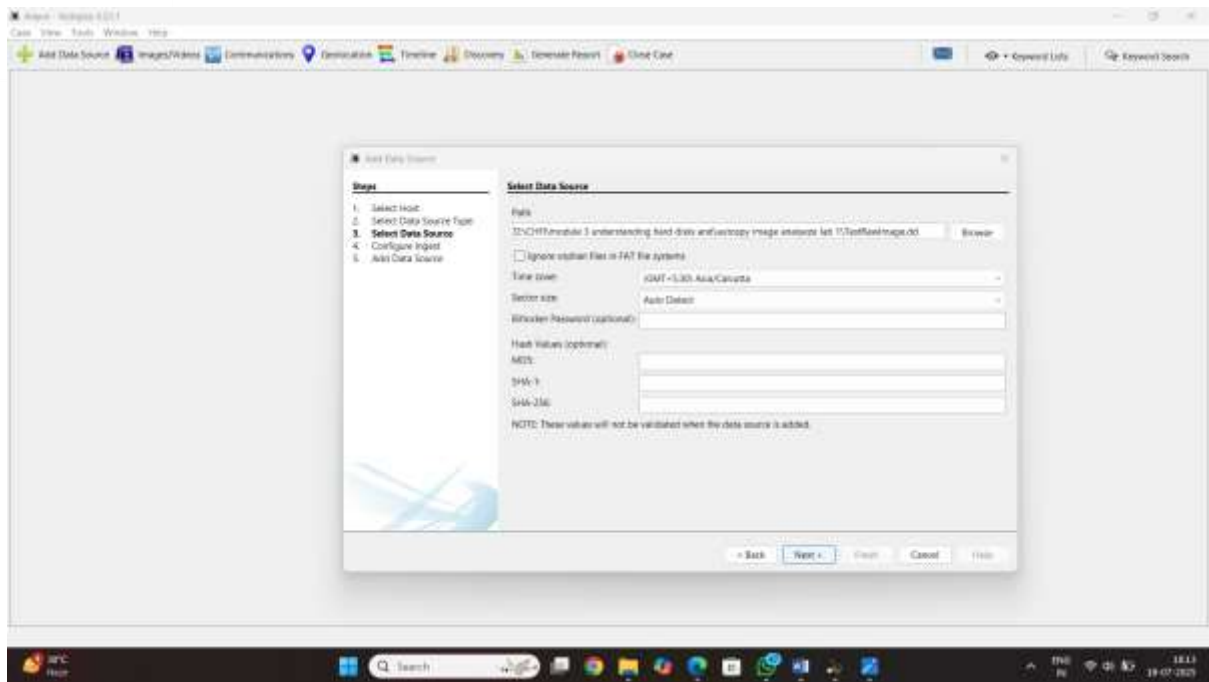
Step7 select host click on the next



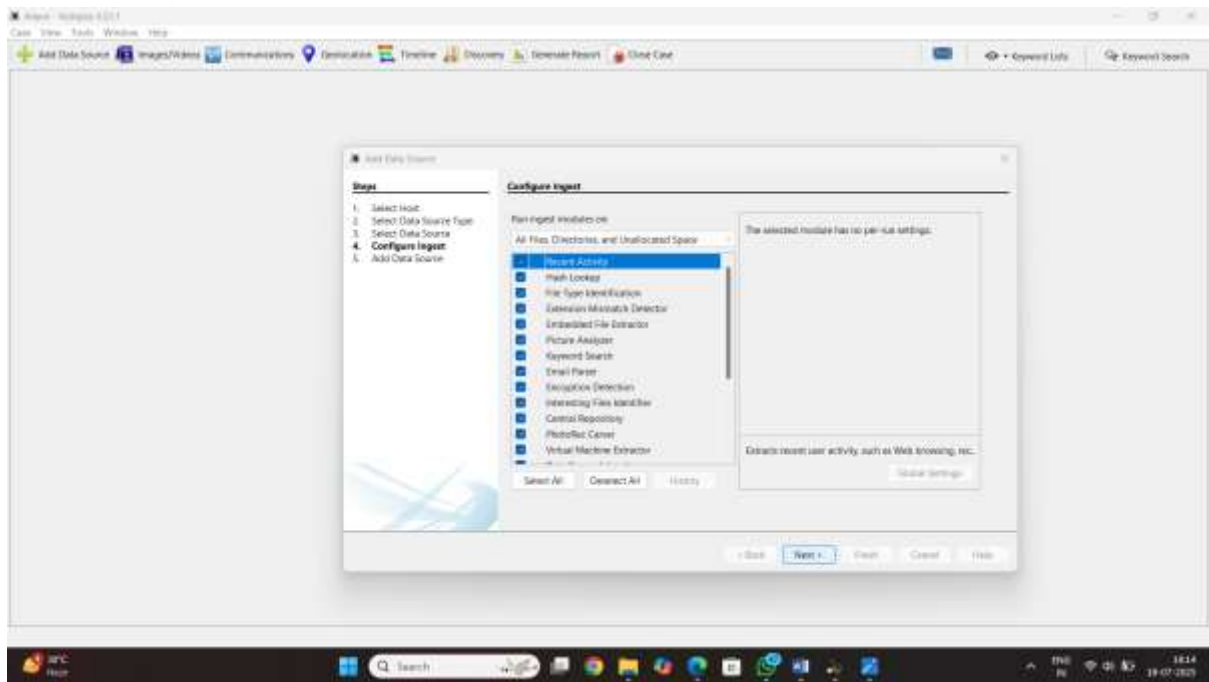
Step8 select the data source type



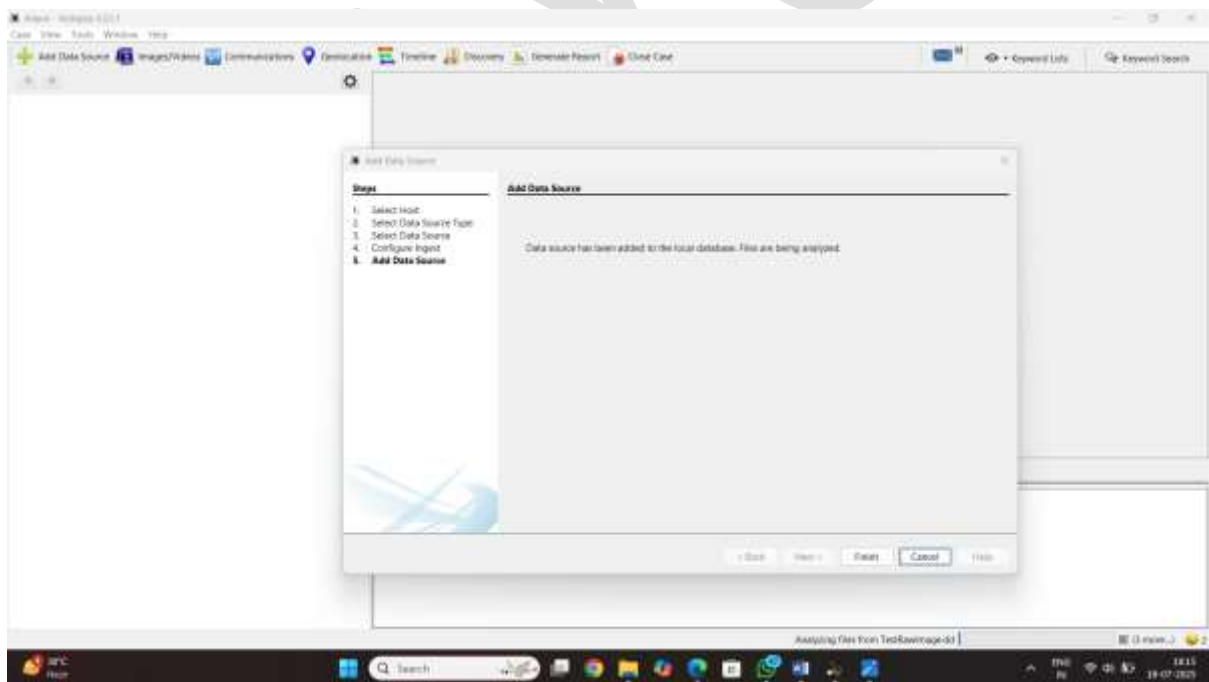
Select the disk image or vm file click on the next
Step9 select the data source type /image path folder



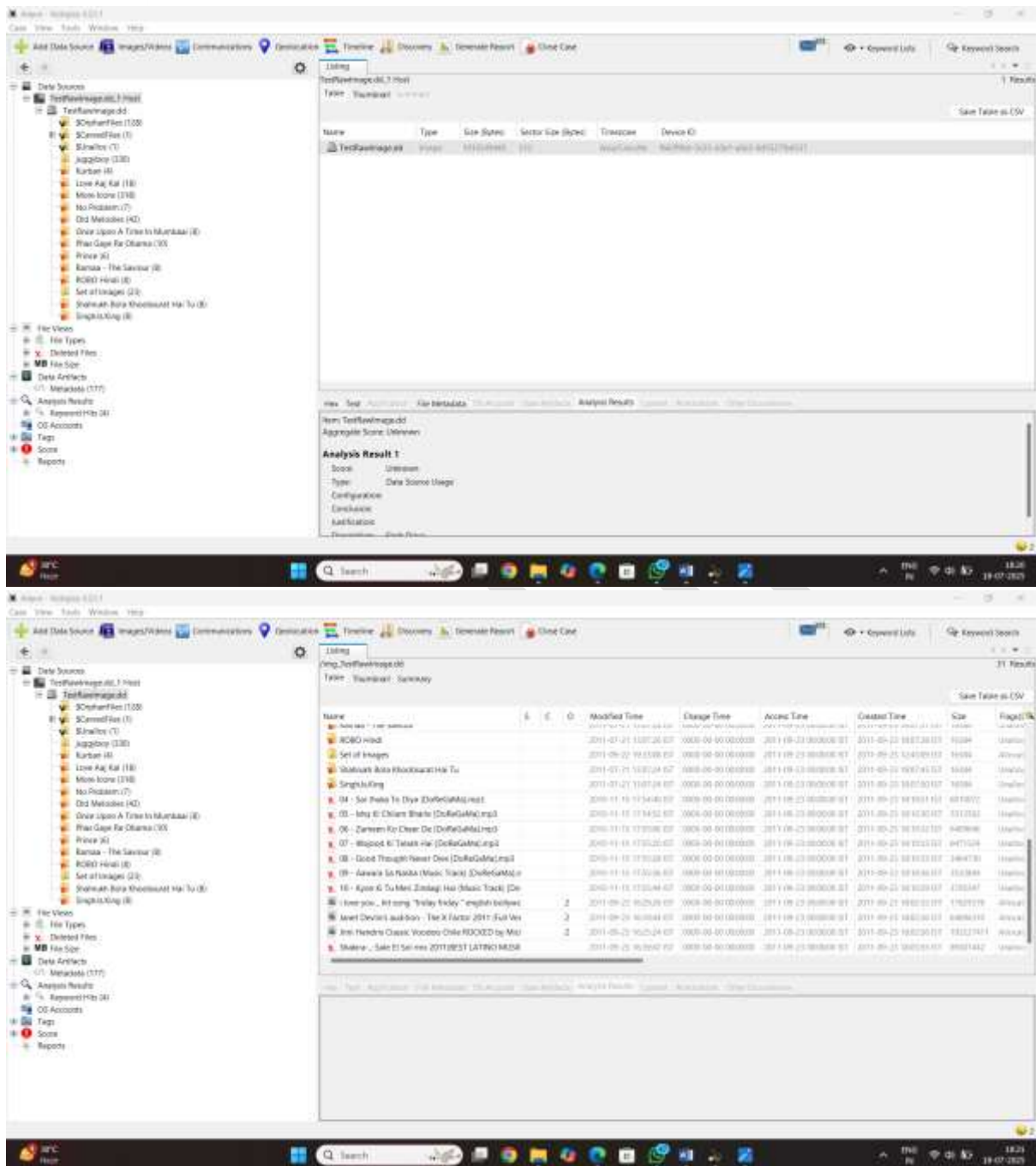
Click in the next
Step10 configure ingest



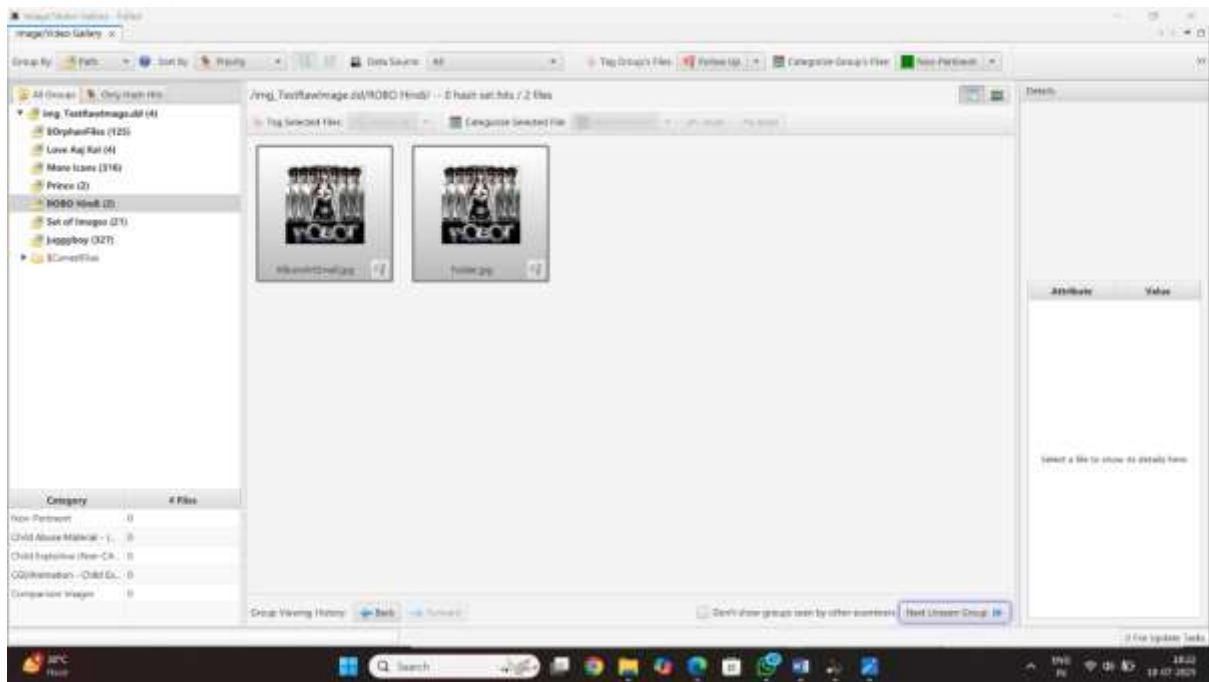
Click on the next
Step11: add data source



Click on the next
Analyze the image of content



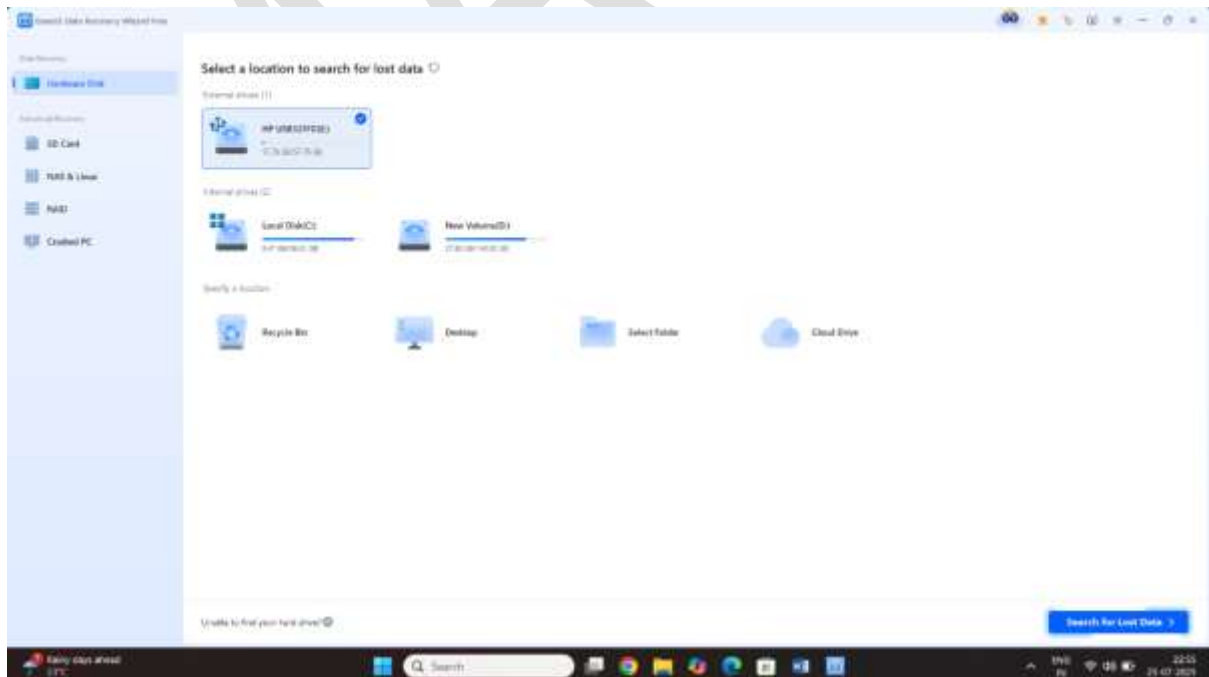
Step12 click on the image/videos option they vezeble of image of folder



Lab3 recover data form deleted Disk partition

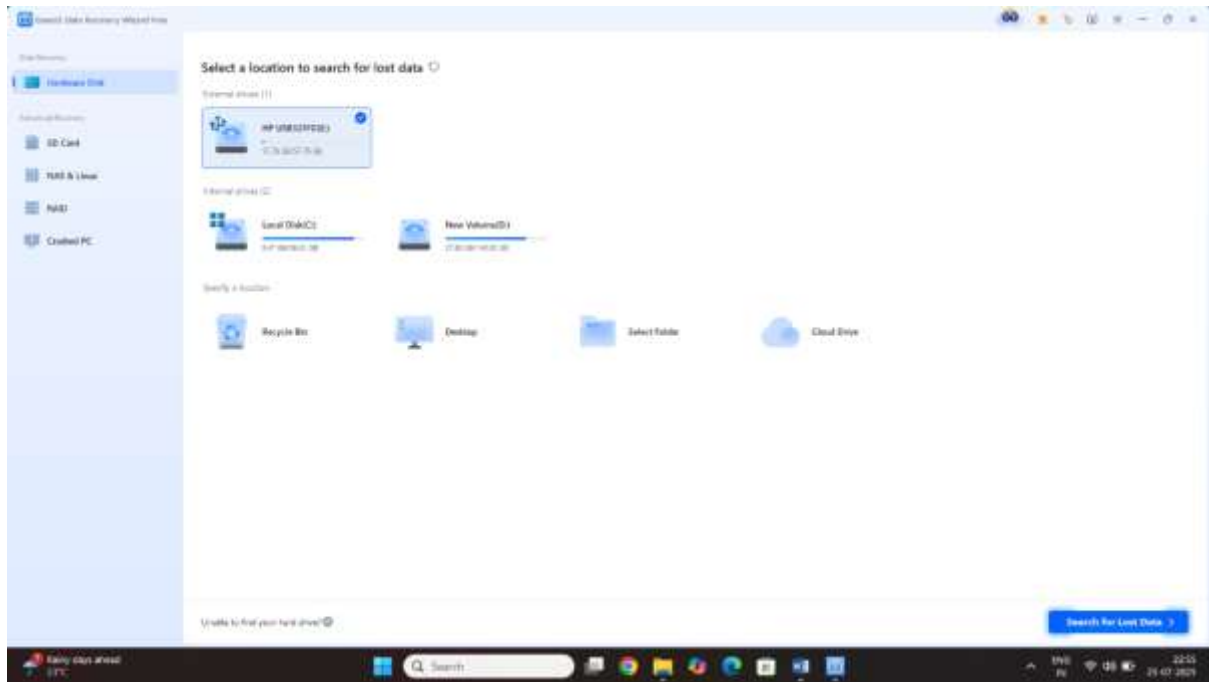
There was tool called ease us data recovery

Step1 start the data recovery tool

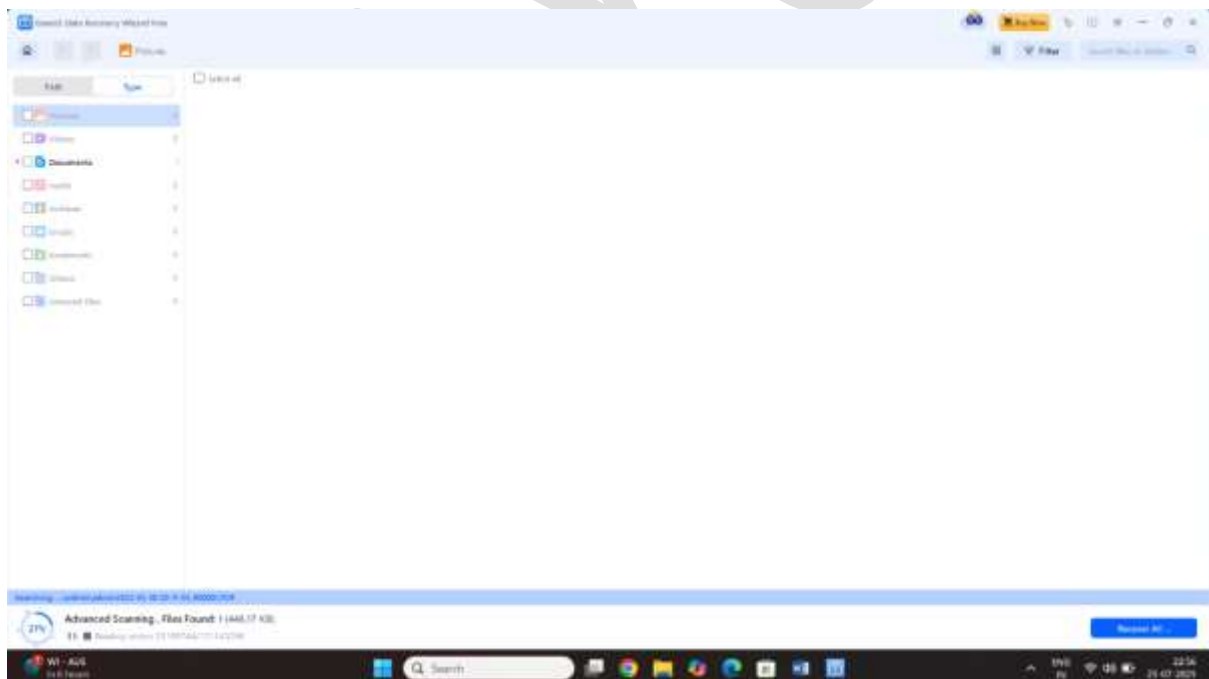


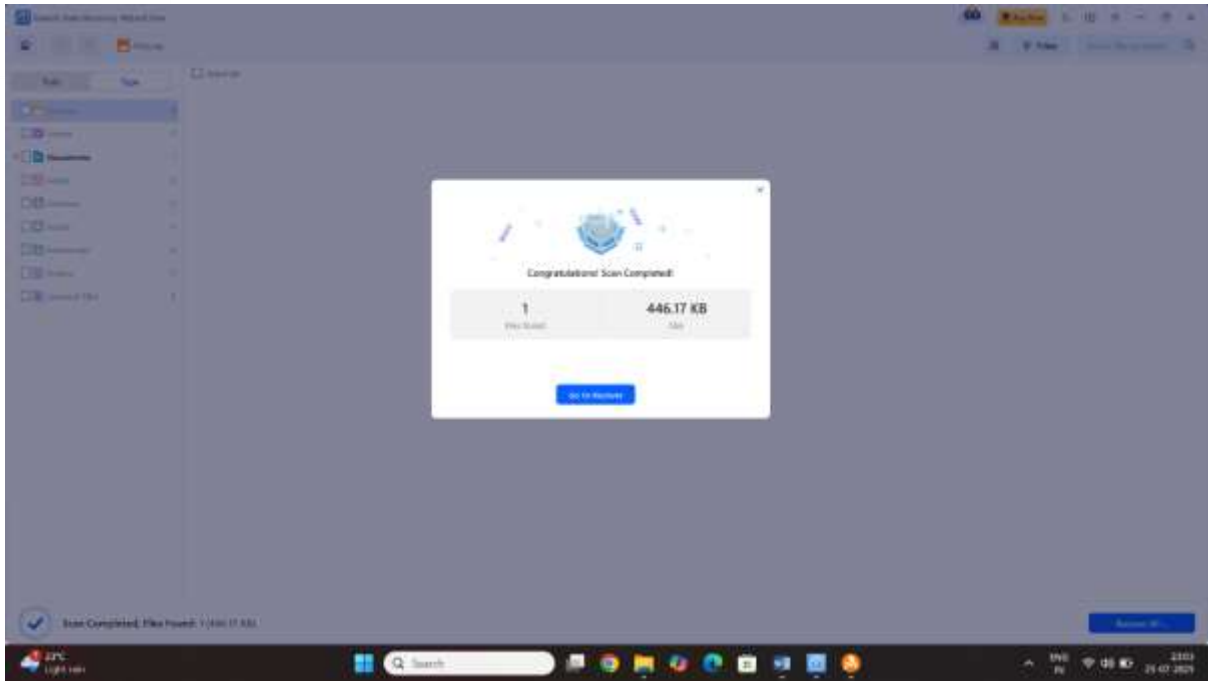
Step2 select the ease lost partition

Step3 click on search for lost data

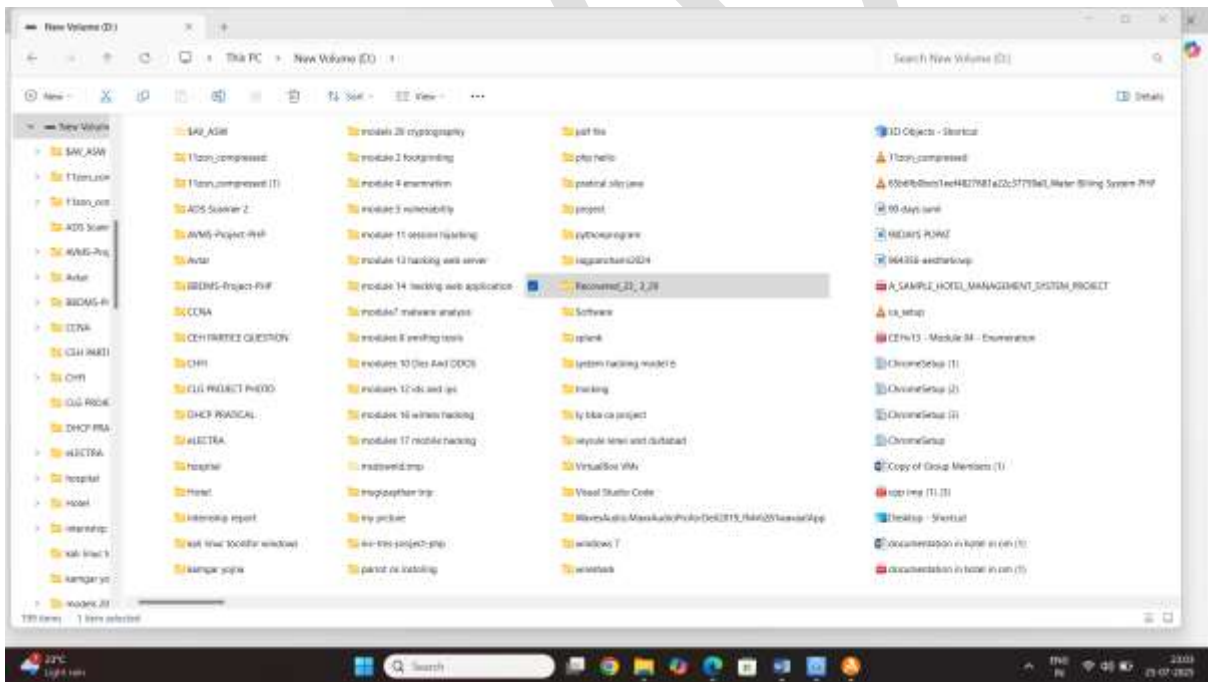


Step4 start the data recovery process

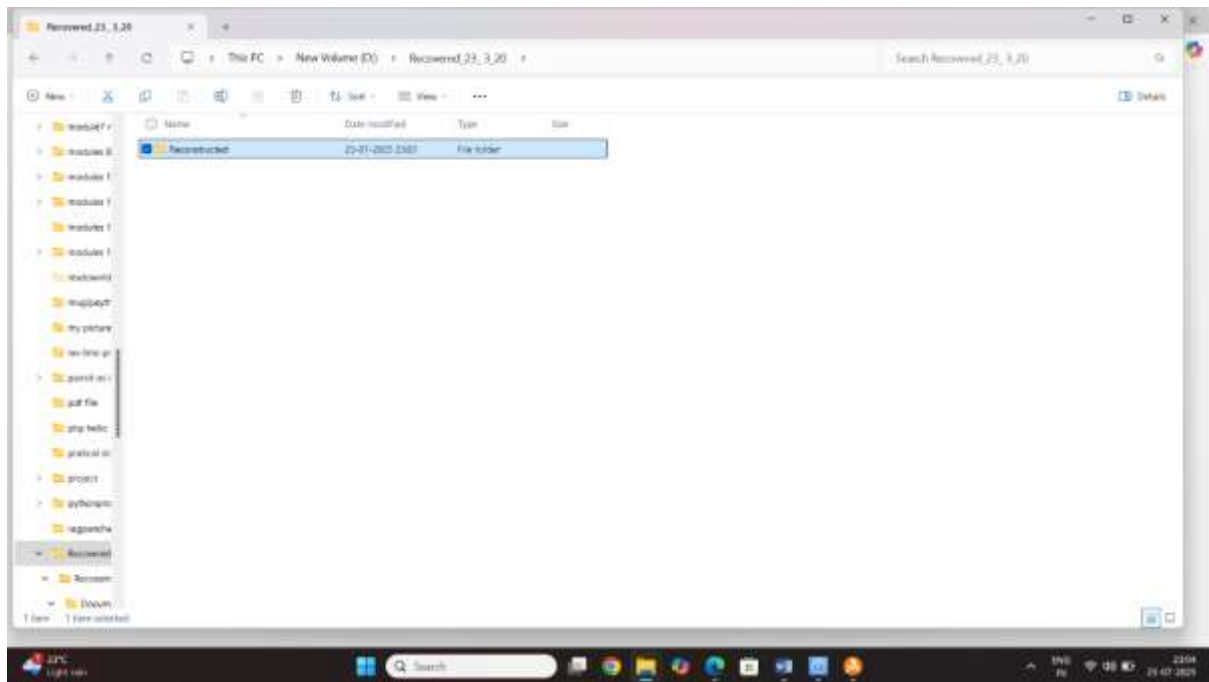




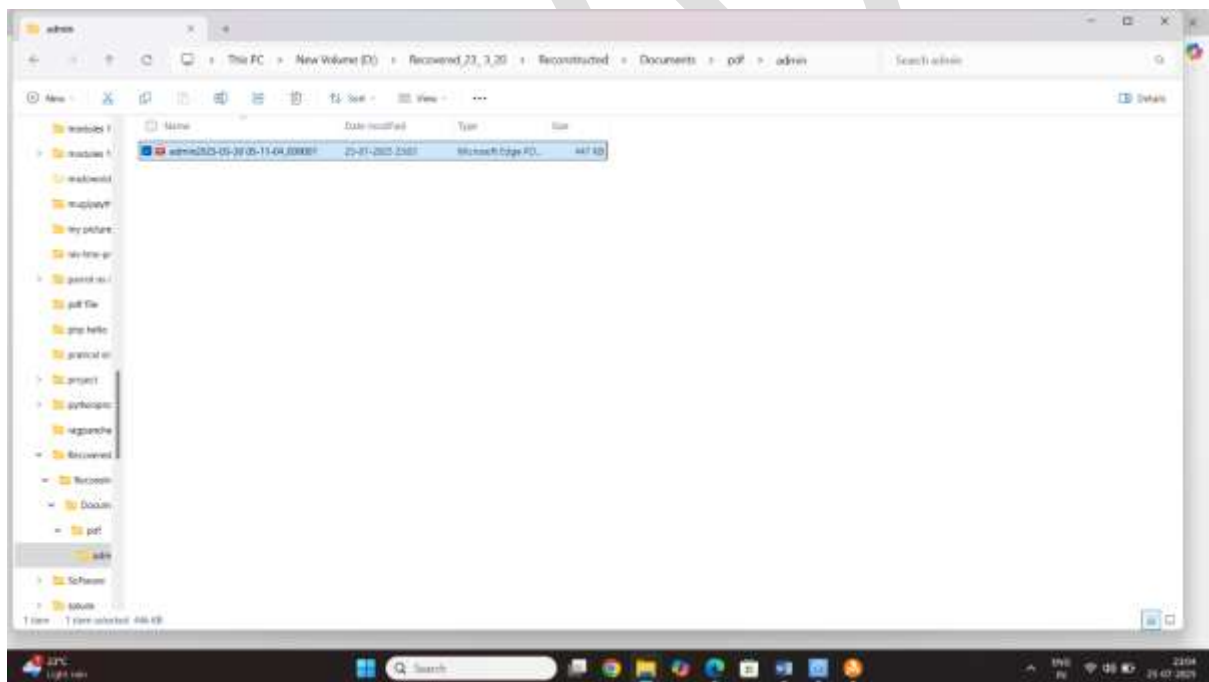
Click the go to recover option



store the recovery data in folder



Result:

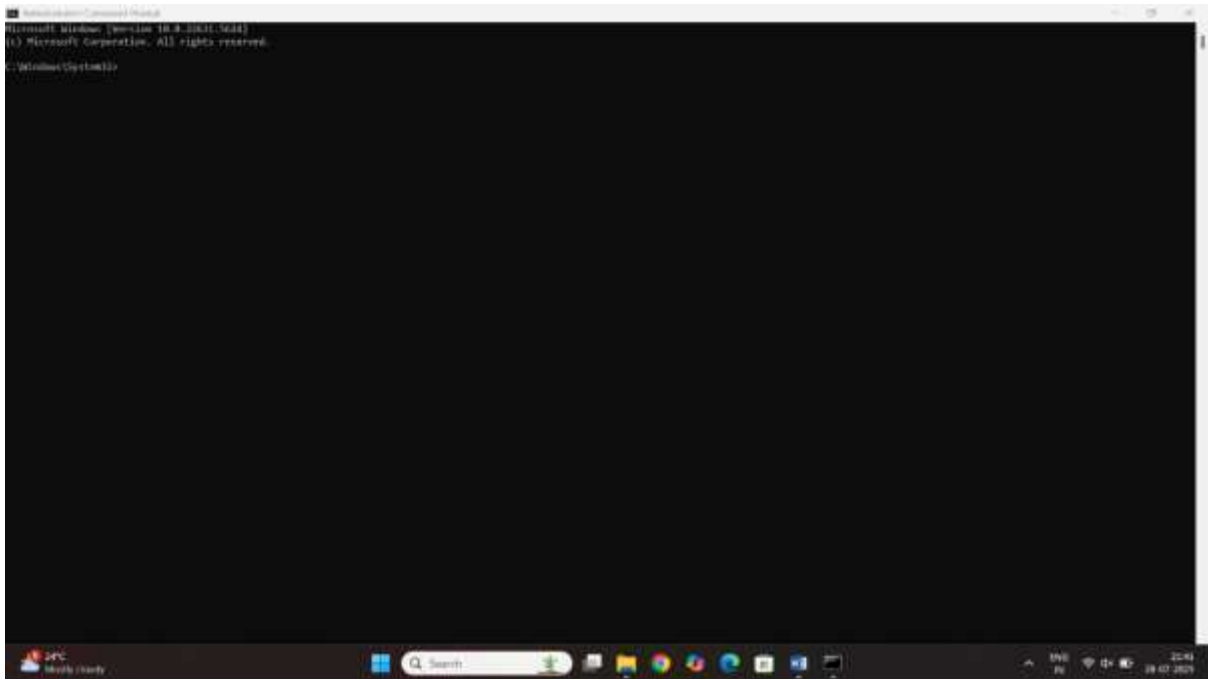


Lab4 hash captering the windows system

Using pwdump7

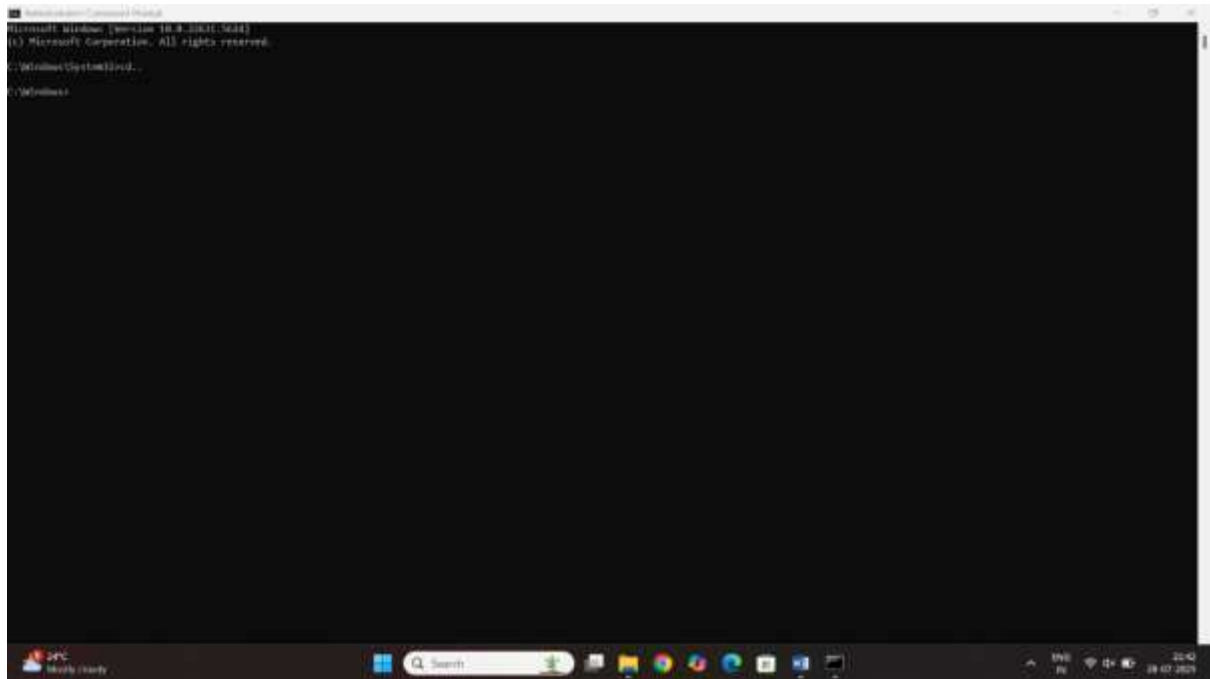
Step1 download the pwdump7

Step2 go to cmd and run as administrative

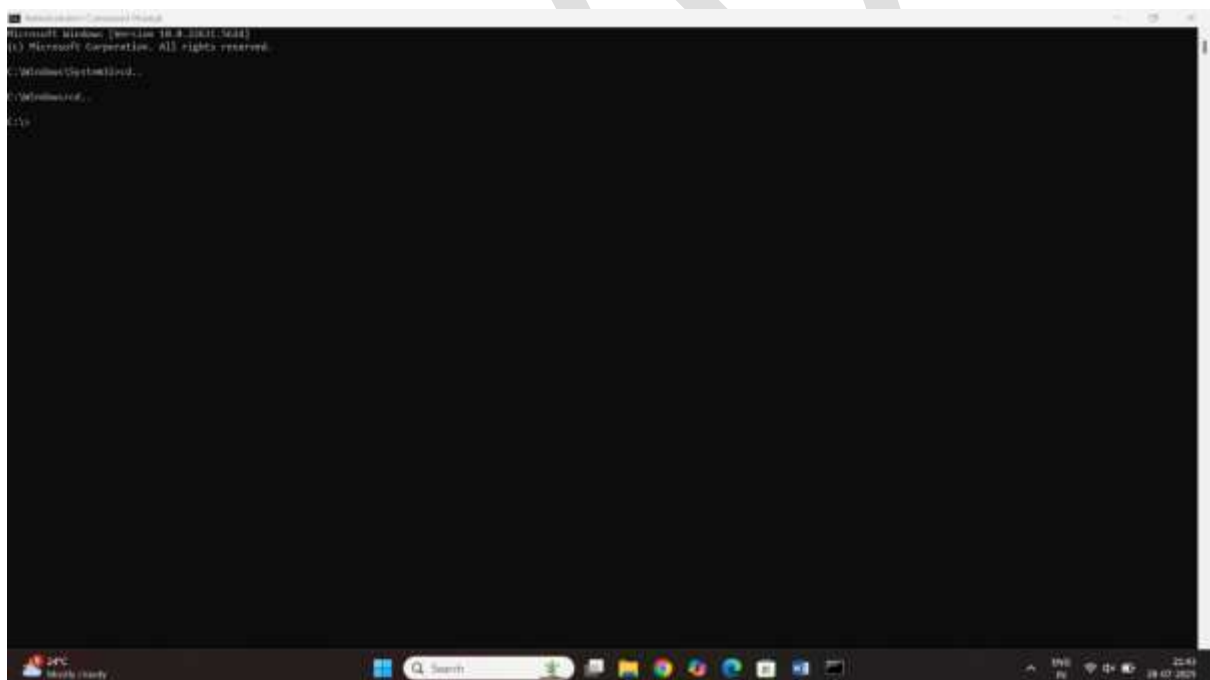


Step3 go to c: drive

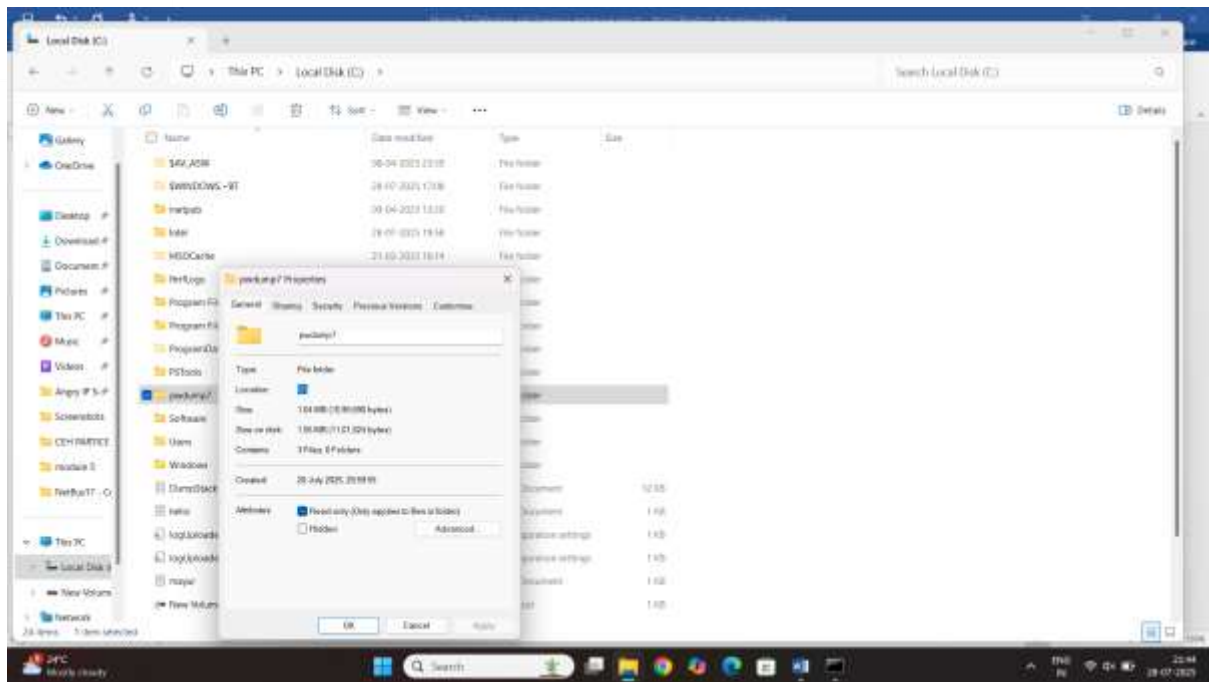
Command: cd..



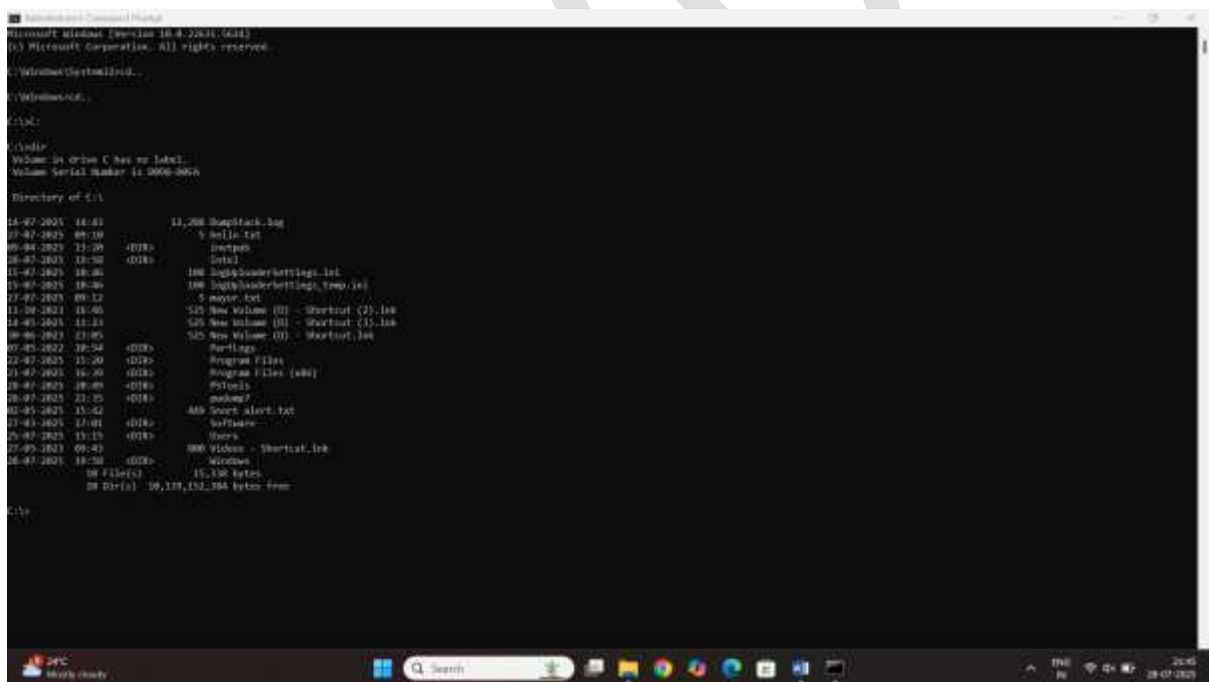
cd..



Step4 type the path of pwdump7 tool check this path in pc



Step5 type the path in cmd



Step6 go to pwdump tool

```
C:\Windows>cd C:\Users\joe\AppData\Local\Microsoft\OneDrive\OneDrive.exe

C:\Users\joe>xcopy /f /d /e /v "C:\Program Files\Foxit Software\Foxit Reader\Foxit Reader.exe" "C:\Users\joe\AppData\Local\Microsoft\OneDrive\OneDrive.exe"

Volume in drive C has no label.
Volume Serial Number is 0000-000A

Directory of C:\

11-07-2025   16:41                12,388 Foxitack.log
11-07-2025   09:10                 5 hello.txt
09-04-2025   11:08         <DIR>          install
09-07-2025   13:50         <DIR>          Intel
10-07-2025   16:30        148 LogHoundSettings.ini
11-07-2025   16:26       108 LogHoundSettings.tmp.kl
11-07-2025   09:12             5 mycor.txt
11-10-2025   18:36       525 New Volume (D) - Startup (2).log
10-05-2025   11:23       525 New Volume (G) - Startup (3).log
10-07-2025   17:09       145 New Volume (I) - Startup.log
07-09-2025   16:54         <DIR>          Settings
11-07-2025   13:20         <DIR>          Program Files
11-07-2025   16:08         <DIR>          Program Files (x86)
09-07-2025   09:49         <DIR>          PTools
10-07-2025   22:29         <DIR>          patches
10-05-2025   15:42        446 Shortcut.alert.txt
11-03-2025   17:01         <DIR>          Software
10-07-2025   15:15         <DIR>          Users
11-05-2025   09:03       889 Xidex - Startup.log
10-07-2025   18:50         <DIR>          Windows
      10 File(s)            11,148 bytes
     10 Dir(s)    10,119,562,196 bytes free

C:\usbdev?>
'usbdev?' is not recognized as an internal or external command,
operable program or batch file.

C:\usb dev?>

C:\usbdev\usb?>

Volume in drive C has no label.
Volume Serial Number is 0000-000A

Directory of C:\usbdev\

10-07-2025   22:25         <DIR>
10-07-2025   22:25           1,812 usb_device12.dll
10-07-2025   22:25           77,814 usbdev7.cnv
10-07-2025   22:25              522 readme.txt
      4 File(s)            1,880,688 bytes
     1 Dir(s)    10,119,416,736 bytes free

C:\usbdev%>
```

Step7 type the command

Pwdump7.exe

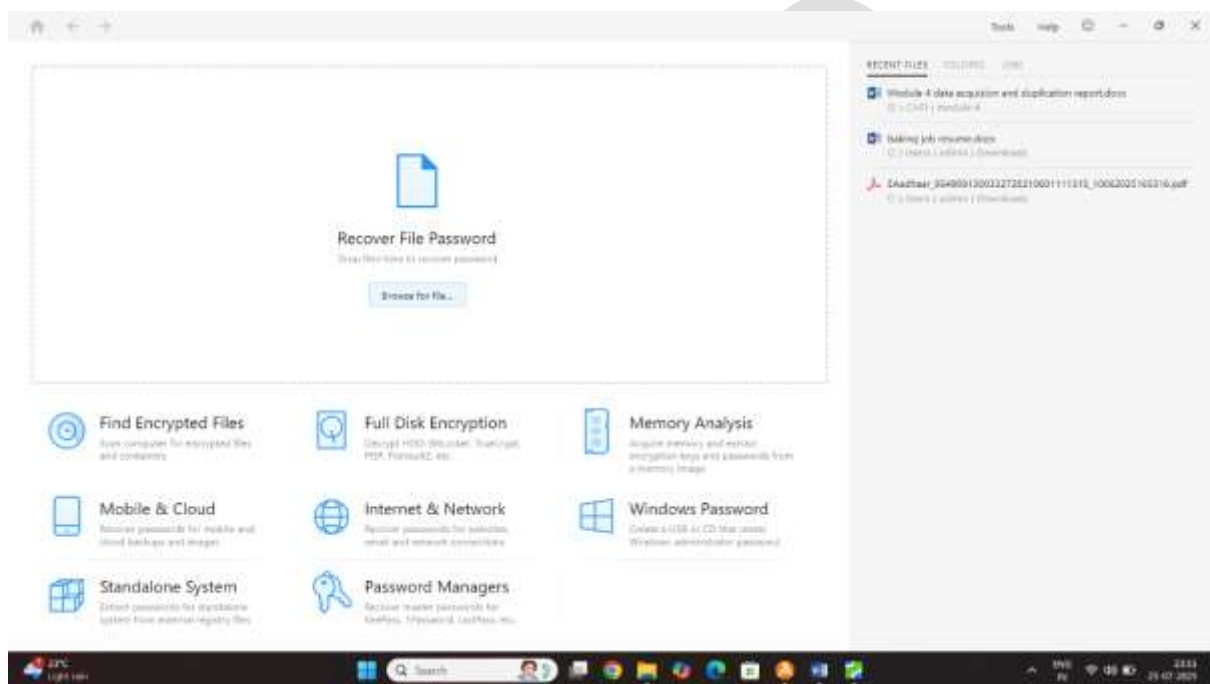
Result:

[illegible]

Lab5 cark application password

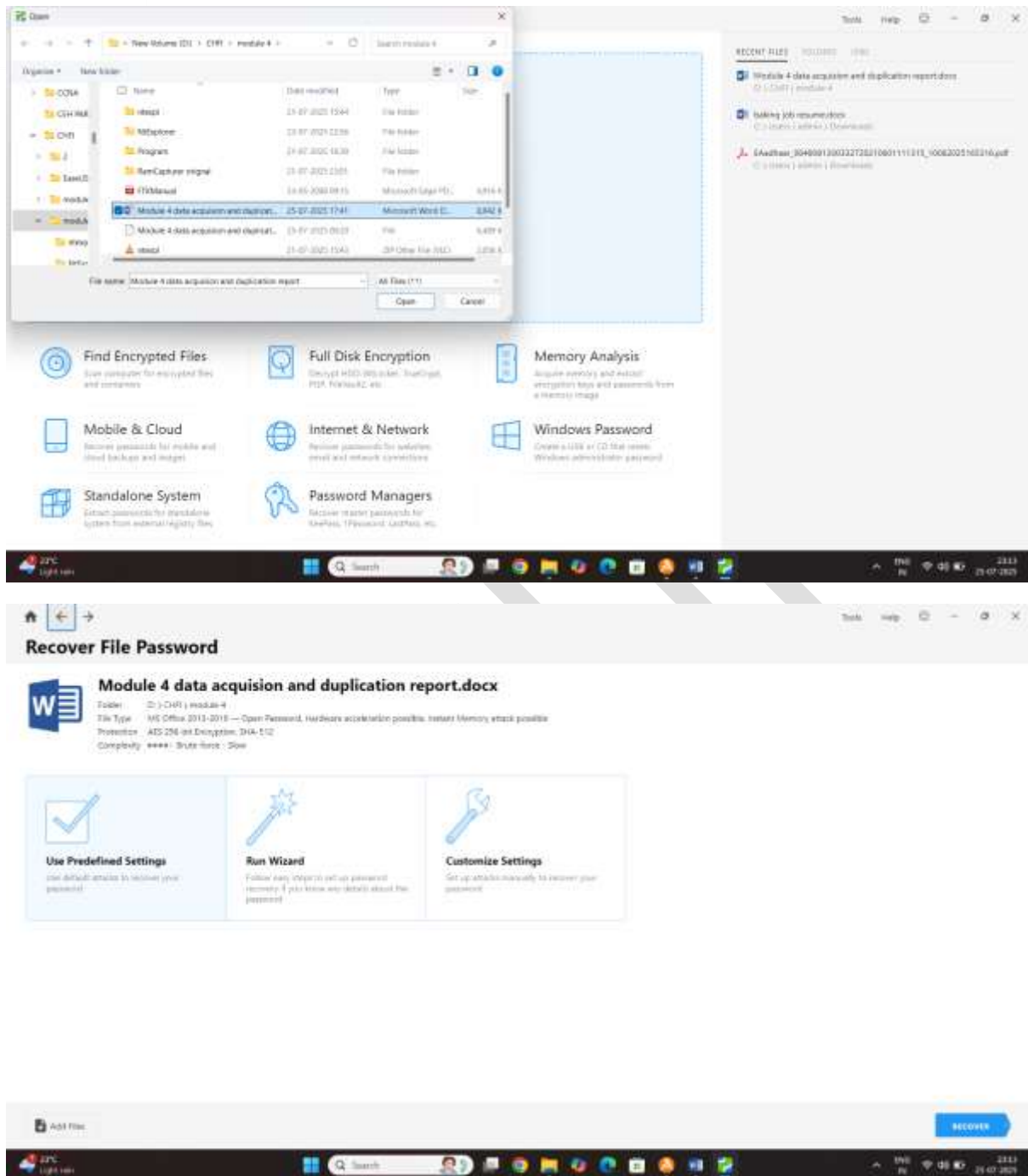
There was tool called password forensic tool kit

Step1 start the application



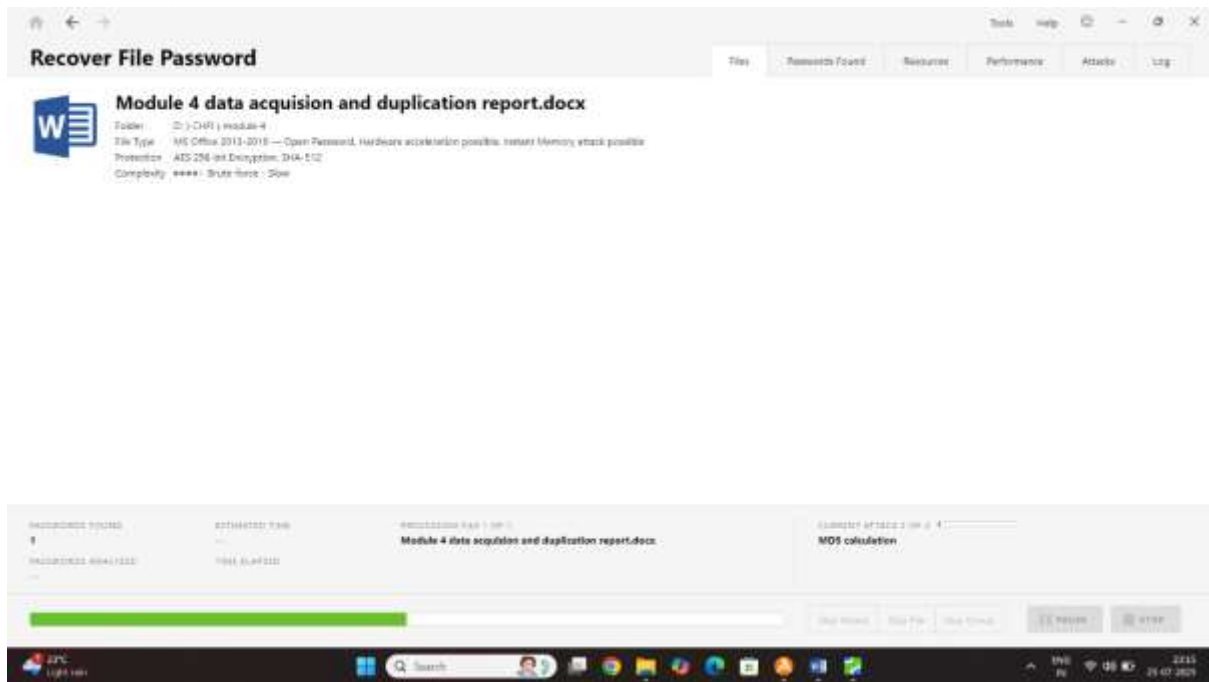
Step2 click on the browse option

Select the crack the password file

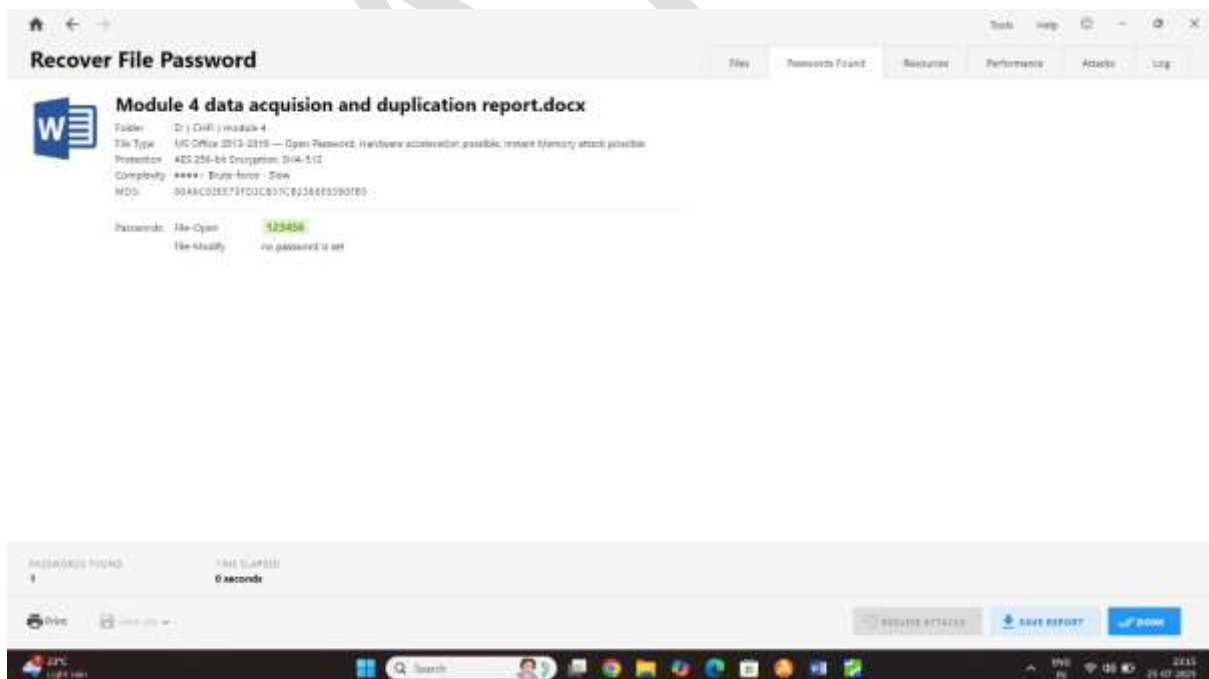


Step3 click on predefined setting option

Click on the recover



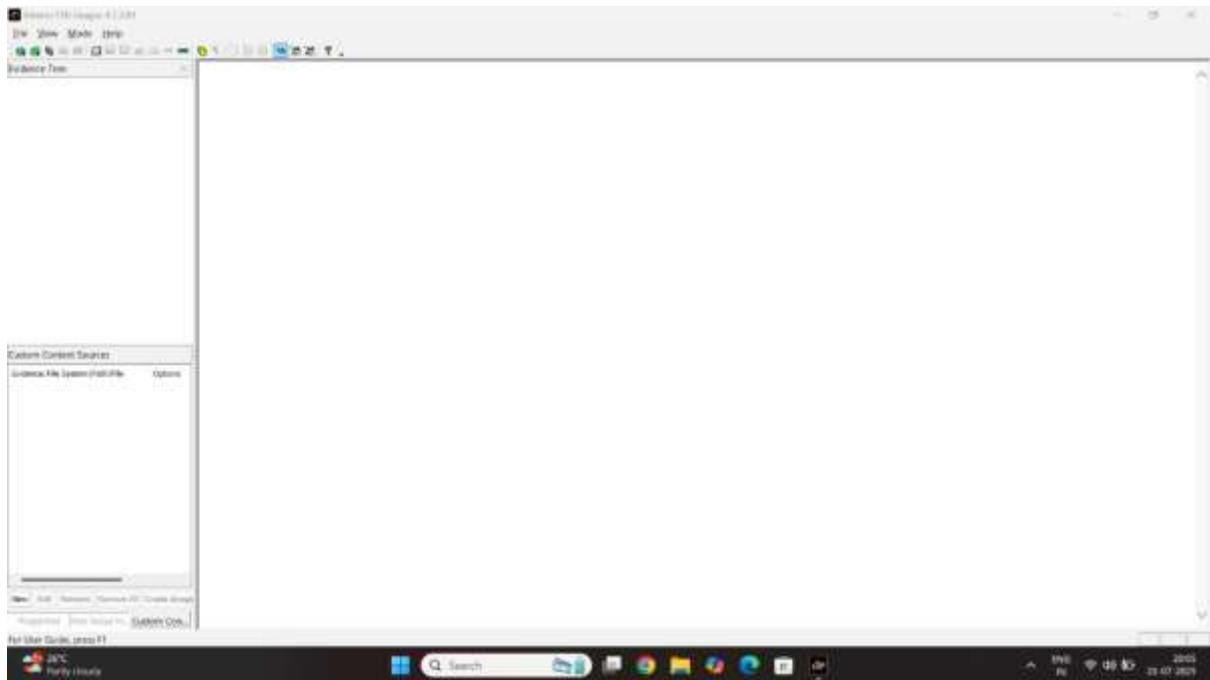
Result:
crack the successful password of word file



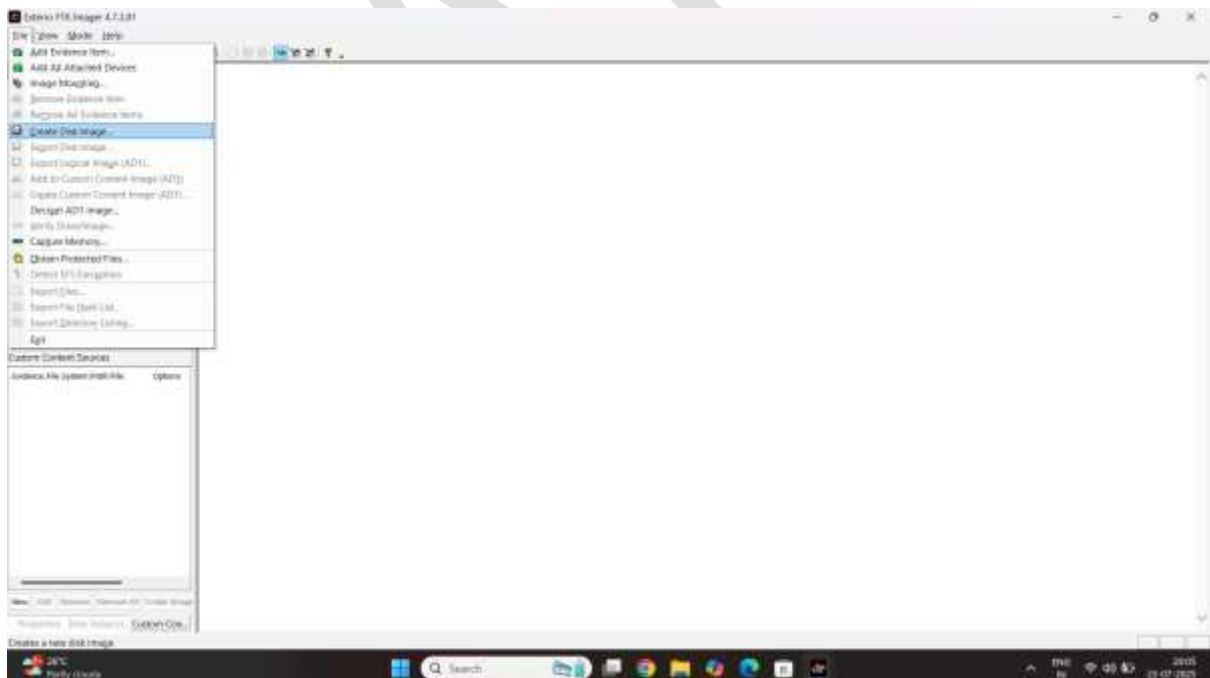
Lab6 create disk image file a hard disk partition

Using ftk

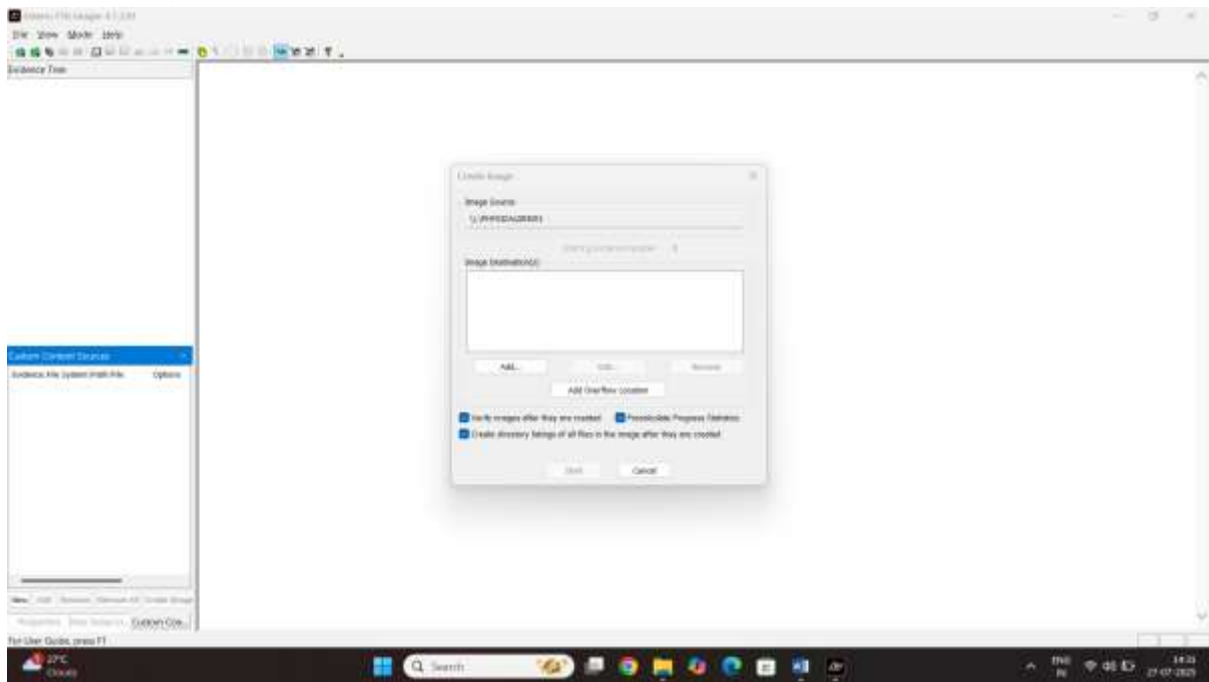
Step1 start the ftk application



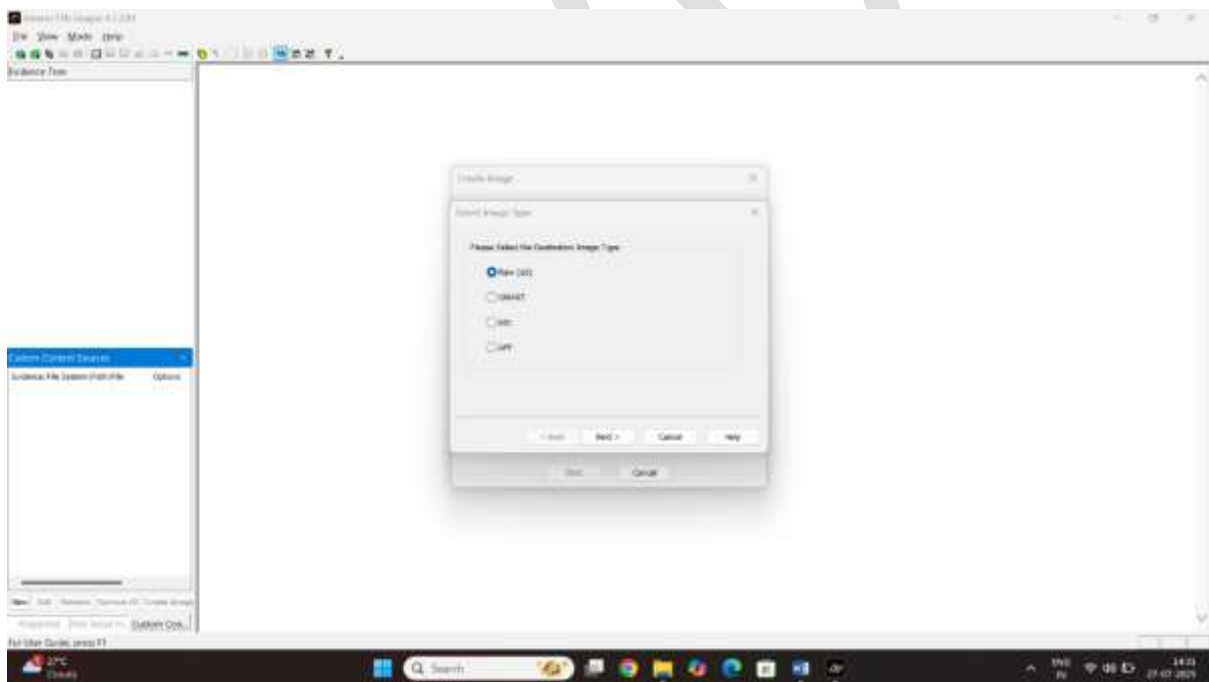
Step2: click on the file option



Step3 select the add option

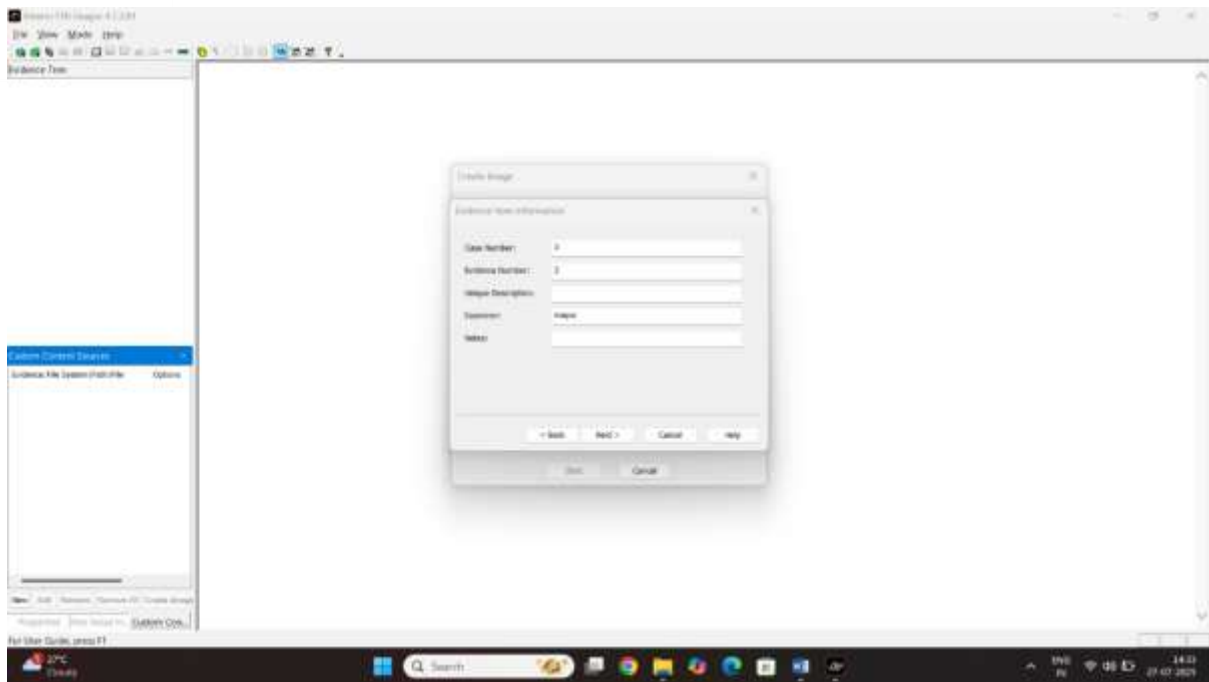


Step4 select the file extinction raw

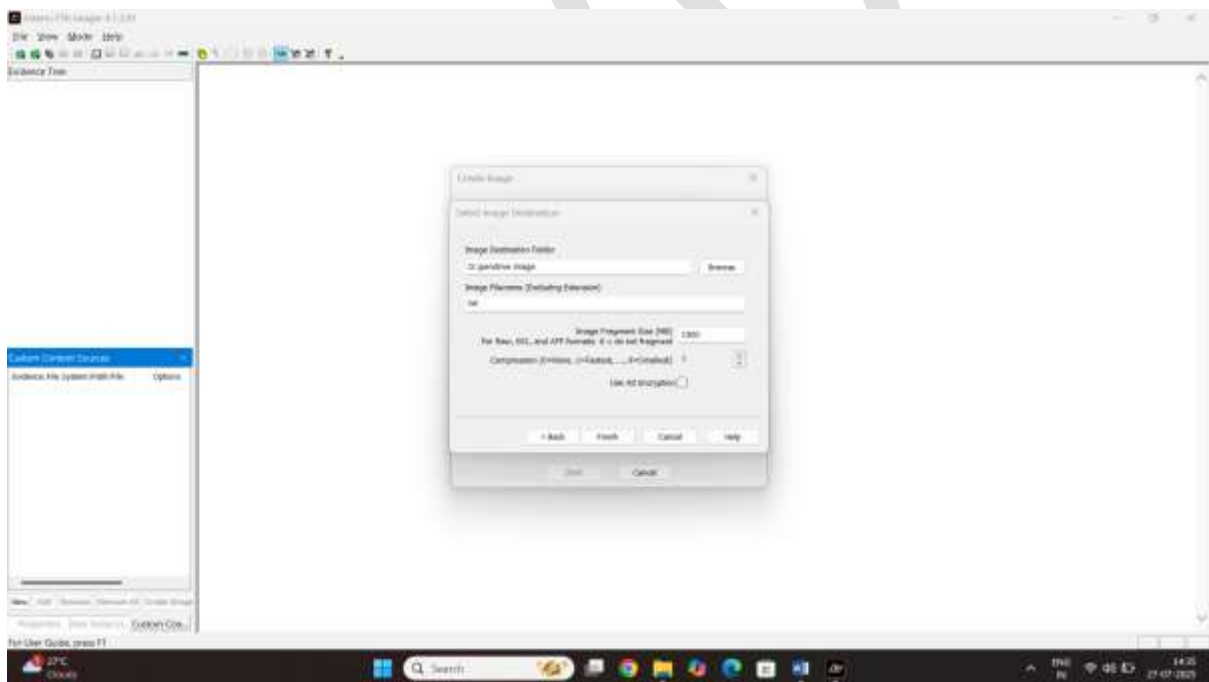


Click on the next

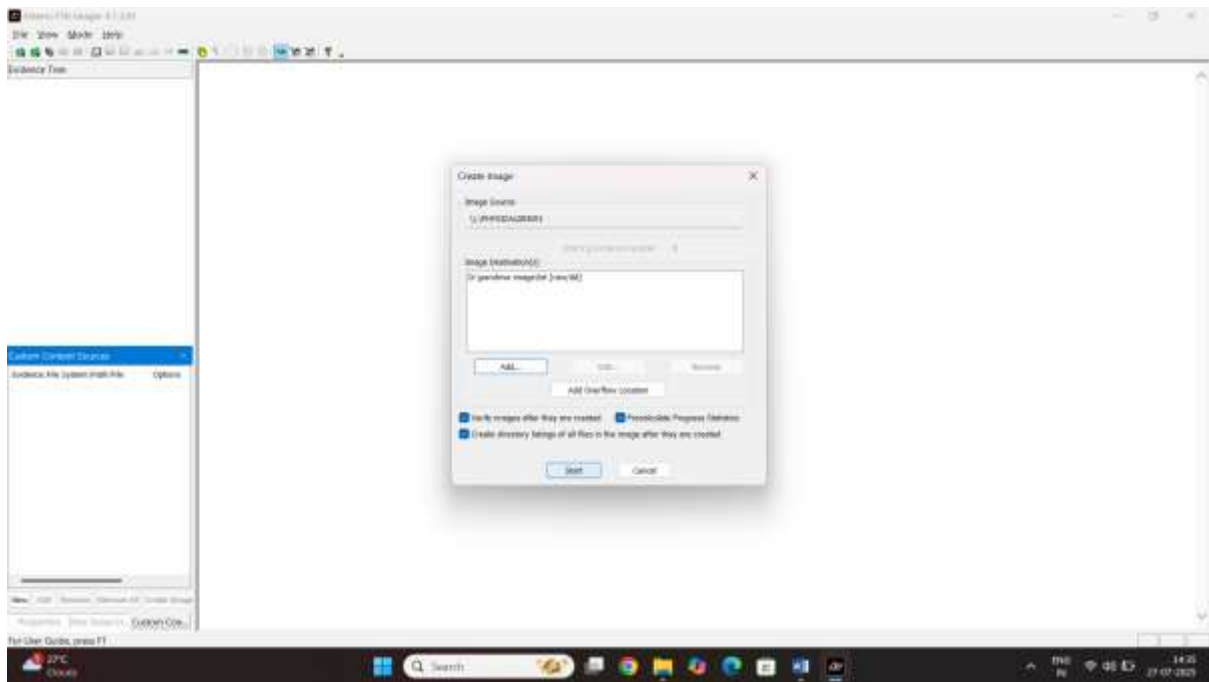
Step5 enter the causes details



Step6 select the image destination folder

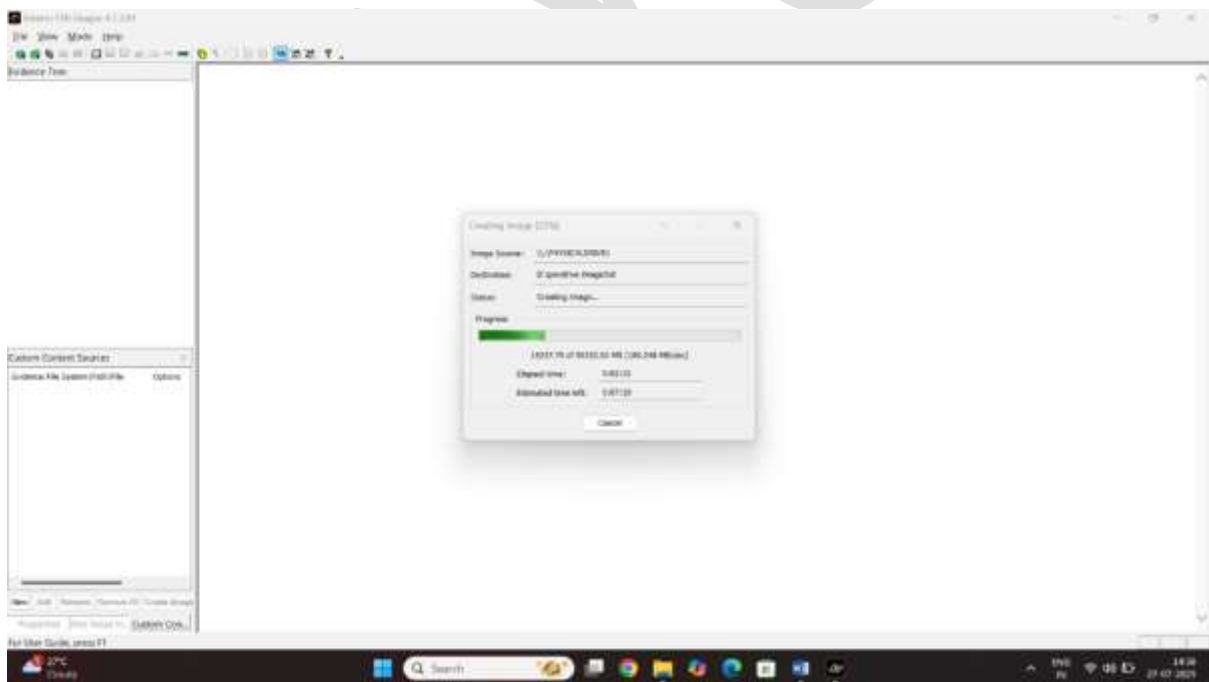


Click on the next

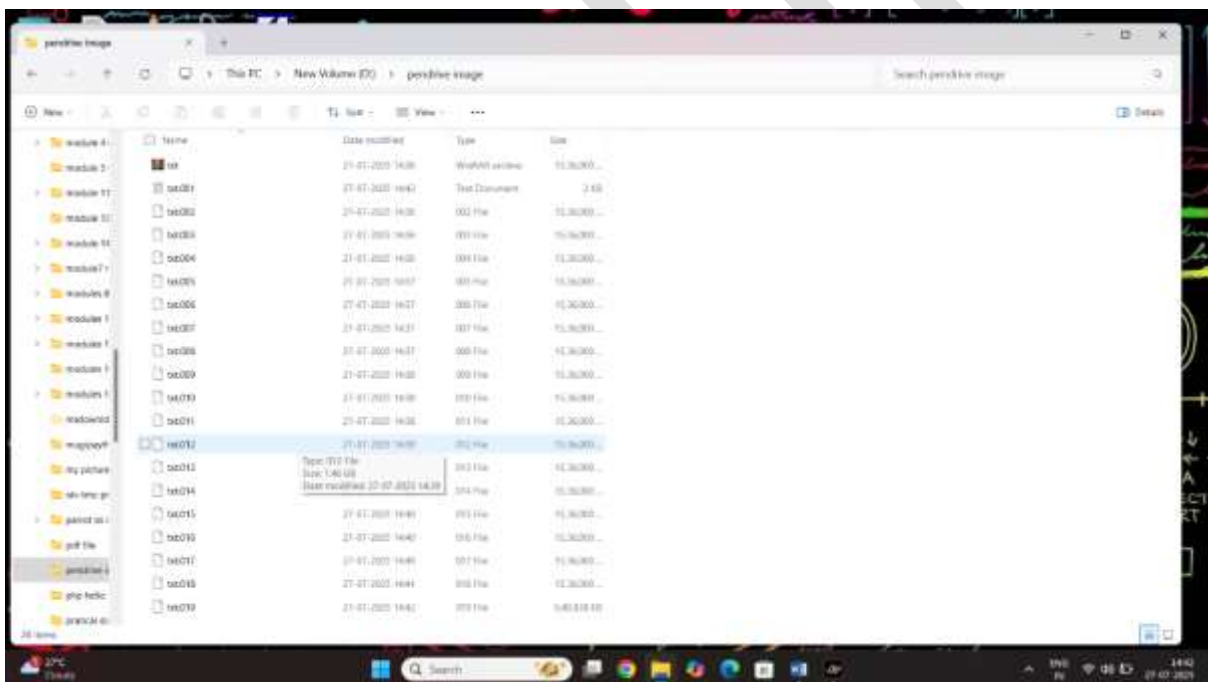
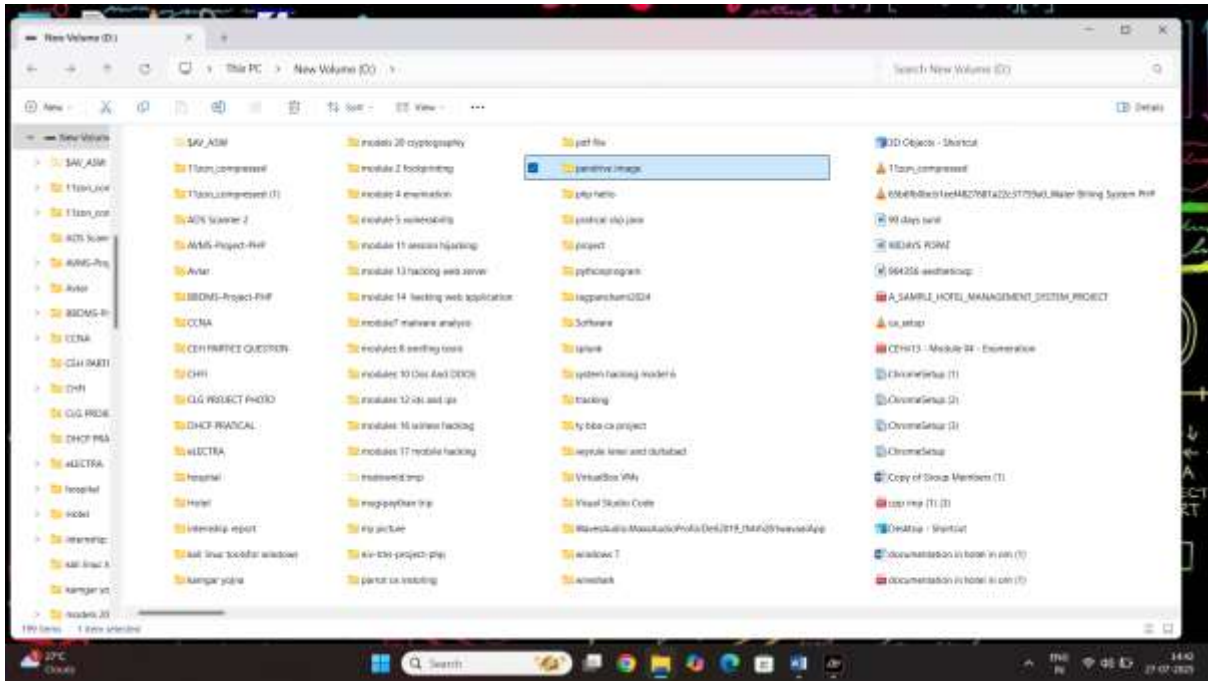


Step7 Click on the start option

Step8 creating image process on



Result:

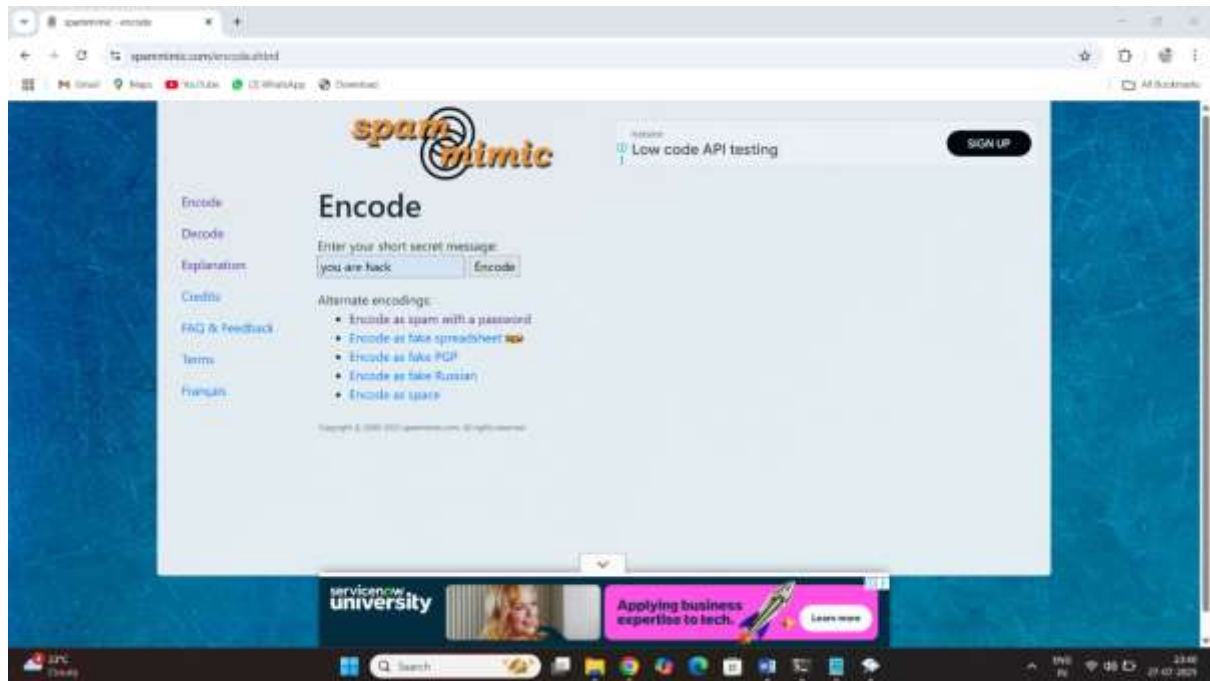


Lab 7 how to detect stegnographic using spam mimic web site

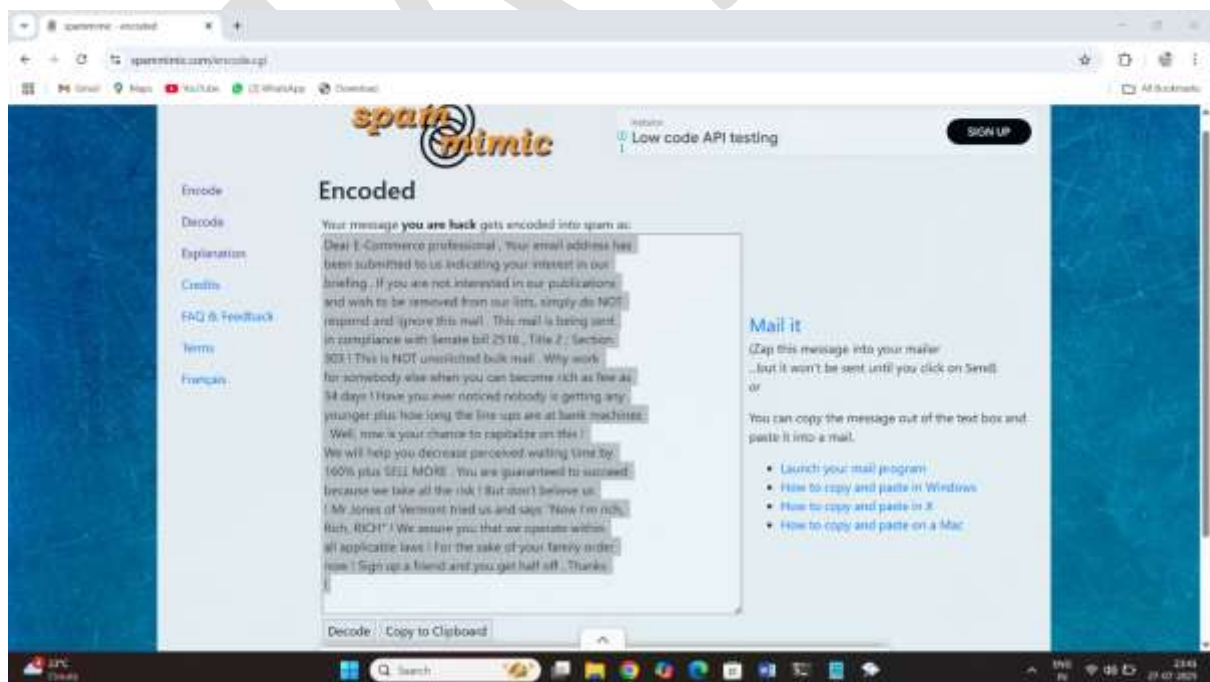


Step1: click on the website open the website

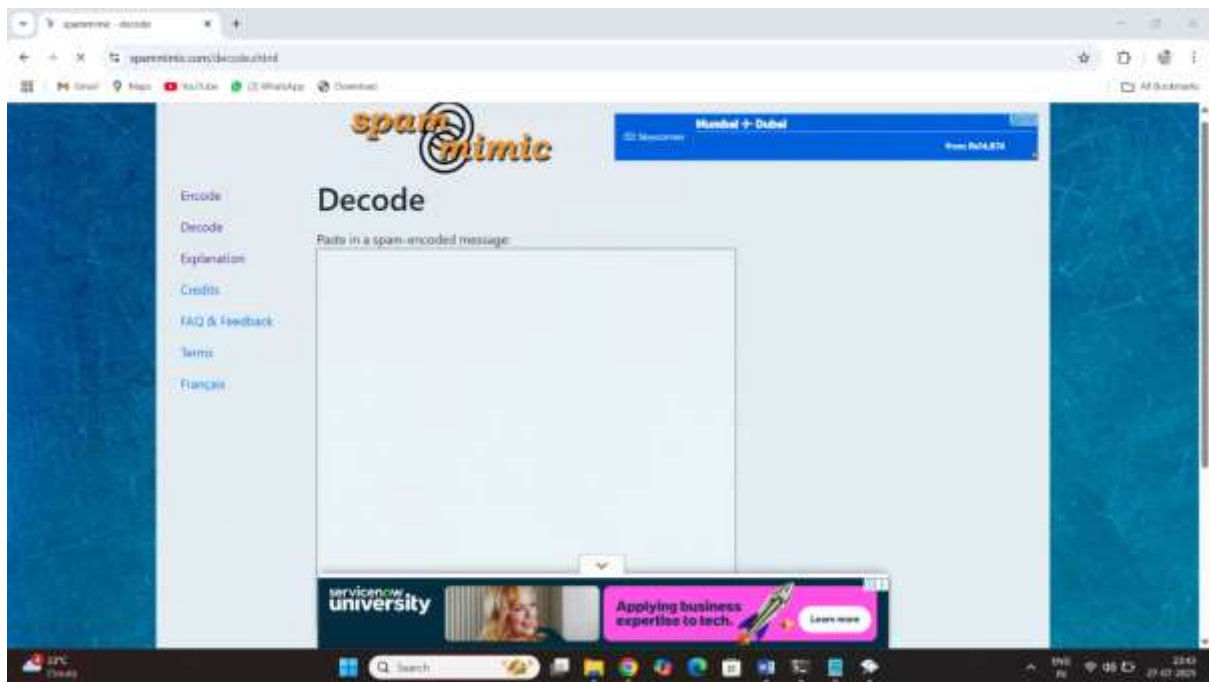
Step2: click the encode and type the text



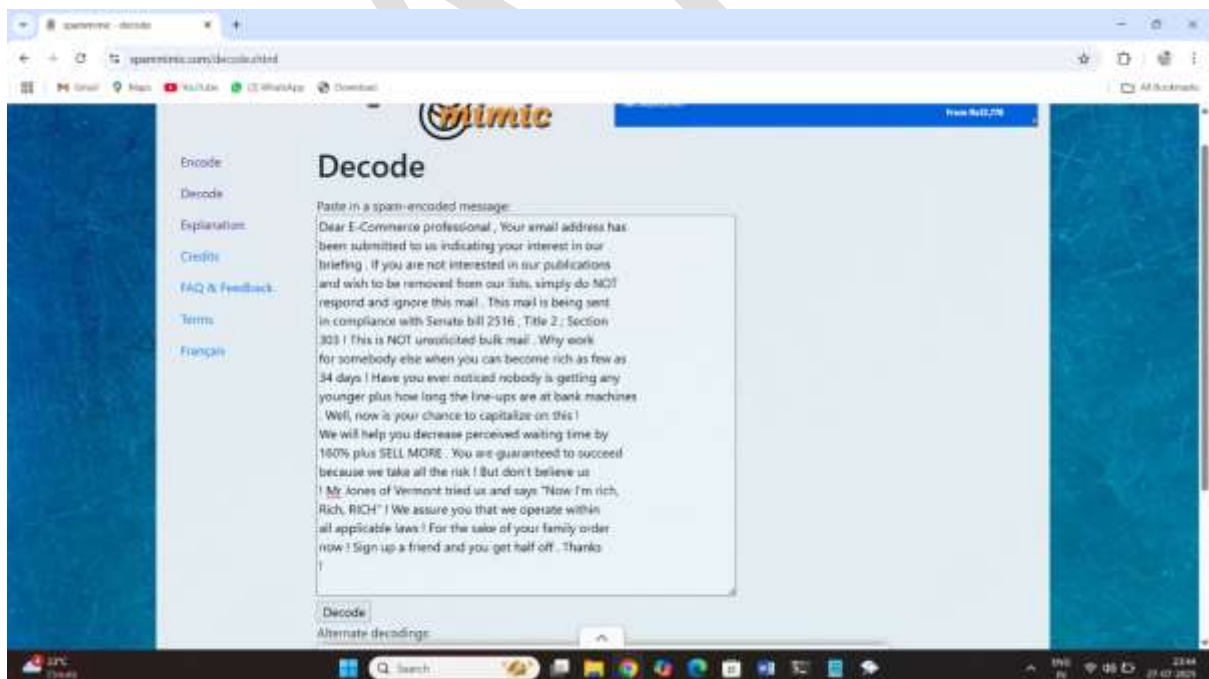
Step3: type the code and copy the code



Step4: click on the decode and paste the code click the decode

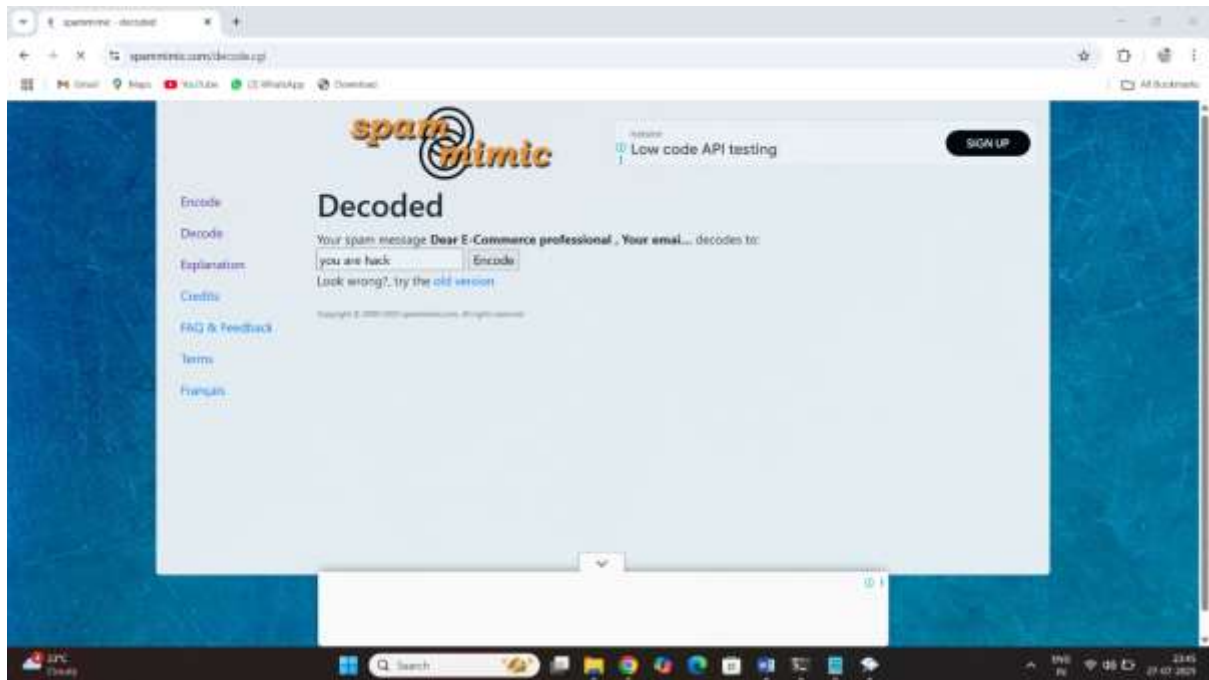


Step5 paste the code



Step6 Click on the decode

Result:



Lab8 data streaming/detect alternate data stream

Data streaming is the continuous transmission of data, typically in real-time or near real-time, as it's generated.

Instead of waiting for all the data to be collected (like downloading a file), you process it **on the fly**—as it comes in.

Step1: click on note pad Create the txt file

Example mayur45.txt/Create the file

Step2 open the cmd and type the command
Dir/checking the command create the txt file

```

01-04-2025 15:59 <DIR>      indian-wordlist-main
01-04-2025 15:58      221,437 indian-wordlist-main.zip
02-04-2025 16:13      18,422,312 ipscan-3.9.1-setup.exe
02-04-2025 15:22      3,216,766 Kevin_Mitnick_-_The_Art_of_Intrusion.pdf
14-04-2025 22:08          5 mayur45.txt
04-04-2025 19:12      1,818,624 MBASASetup-x64-EN.msi
07-04-2025 15:38      384,889 Metasploit-cheat-sheet.pdf
02-04-2025 18:18      865,884,584 metasploitable-linux-2.0.0 (1).zip
05-04-2025 01:02      871,116,238 metasploitable-linux-2.0.0 (2).zip
10-03-2025 14:45      865,884,584 metasploitable-linux-2.0.0.zip
17-03-2025 08:35      3,358,692 Module_3_scanning (1).pdf

```

Step3:type the file// notepad mayur45.chv13

```

C:\Users\admin>notepad mayur45.txt
notepad mayur45.txt
C:\Users\admin>

```

Volume in drive C has no label.
Volume Serial Number is C09B-0MCA

Directory of C:\Users\admin

```

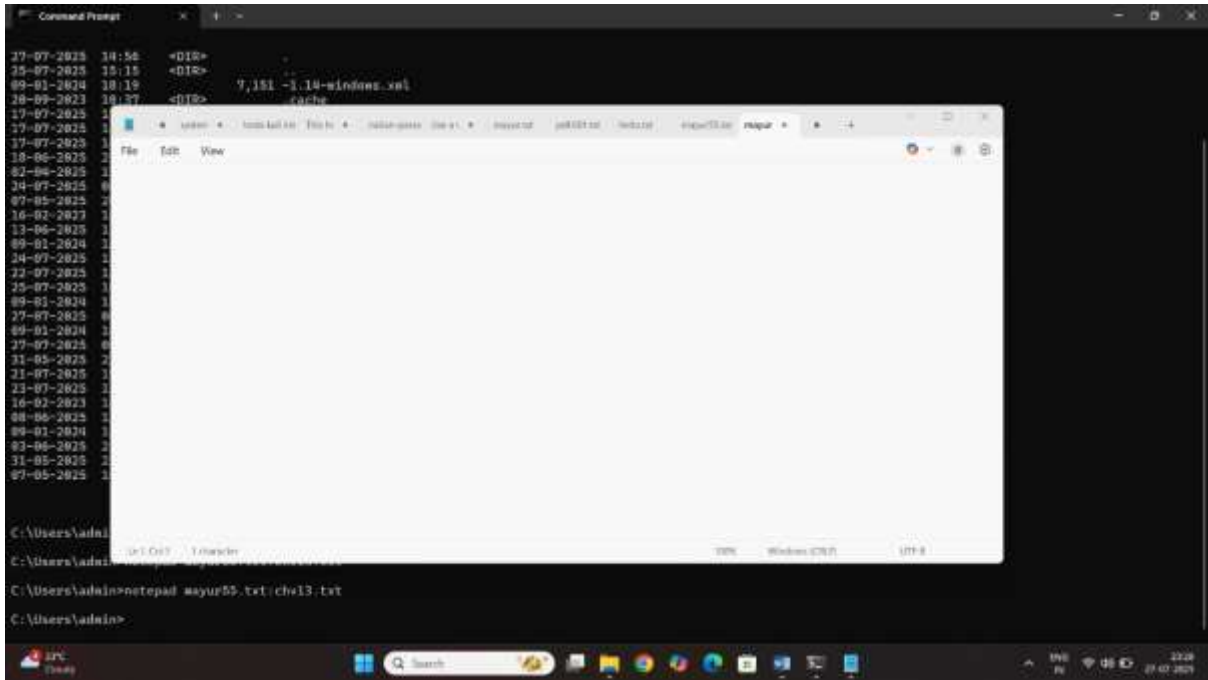
27-07-2025 14:56 <DIR>      .
28-07-2025 15:15 <DIR>      ..
09-01-2024 18:19      7,151 -1.18-windows.xml
20-09-2023 10:37 <DIR>      .cache
17-07-2025 15:45 <DIR>      .icloud
17-07-2025 15:23 <DIR>      .openjfx
17-07-2025 16:40      158 .packettracer
18-06-2025 21:32 <DIR>      .splunk
02-04-2025 19:16 <DIR>      .swt
24-07-2025 08:49 <DIR>      .VirtualBox
07-05-2025 20:15 <DIR>      .vscode
10-02-2023 18:35 <DIR>      3D Objects
13-04-2025 11:09      12 chv13.txt
09-01-2024 18:18 <DIR>      Contacts
24-07-2025 15:26 <DIR>      Desktop
22-07-2025 15:39 <DIR>      Documents
25-07-2025 16:25 <DIR>      Downloads
09-01-2024 18:19 <DIR>      Favorites
27-07-2025 09:19      8 kali.txt
09-01-2024 18:18 <DIR>      Links
27-07-2025 09:15      14 mayur55.txt
21-09-2025 23:24 <DIR>      Music
21-07-2025 19:29 <DIR>      New folder
23-07-2025 11:48 <DIR>      New folder (2)
16-02-2023 18:37 <DIR>      OneDrive
08-06-2025 13:14 <DIR>      Pictures
09-01-2024 18:18 <DIR>      Searches
03-06-2025 21:49 <DIR>      SecurityScans
31-05-2025 23:28 <DIR>      Videos
07-05-2025 16:16 <DIR>      VirtualBox VMs
          5 File(s)      7,327 bytes
        28 Dir(s) 12,196,904,968 bytes free

```

C:\Users\admin>notepad mayur55.txt

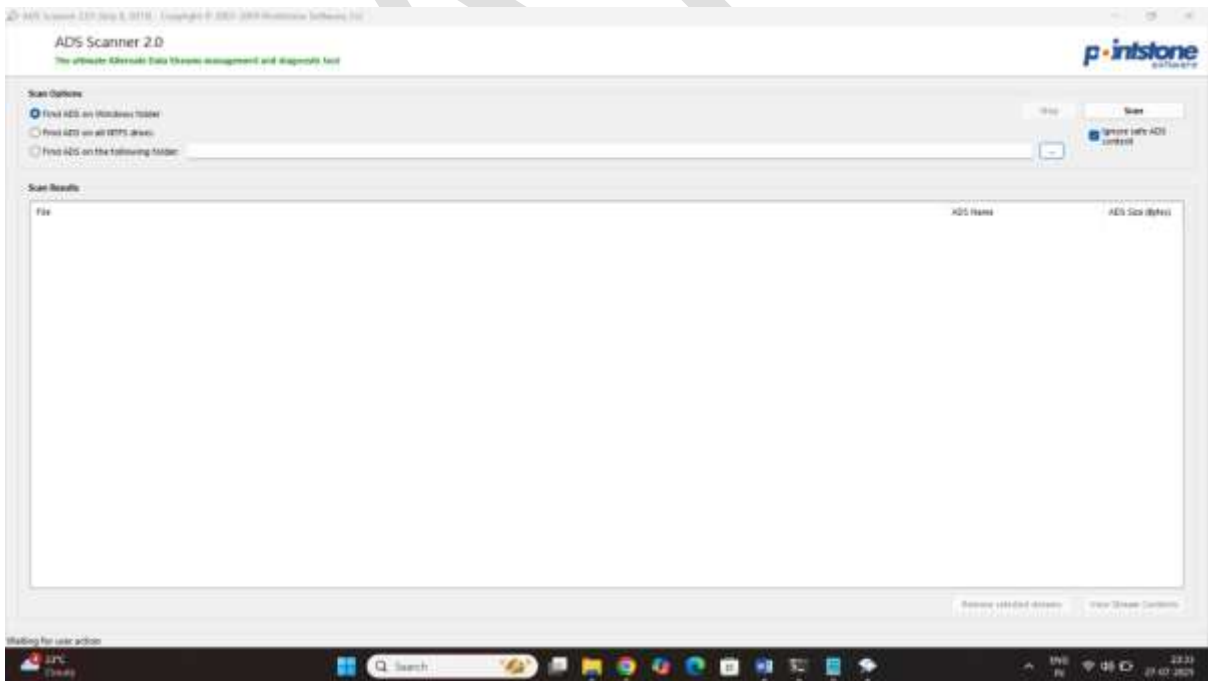
C:\Users\admin>

Result:

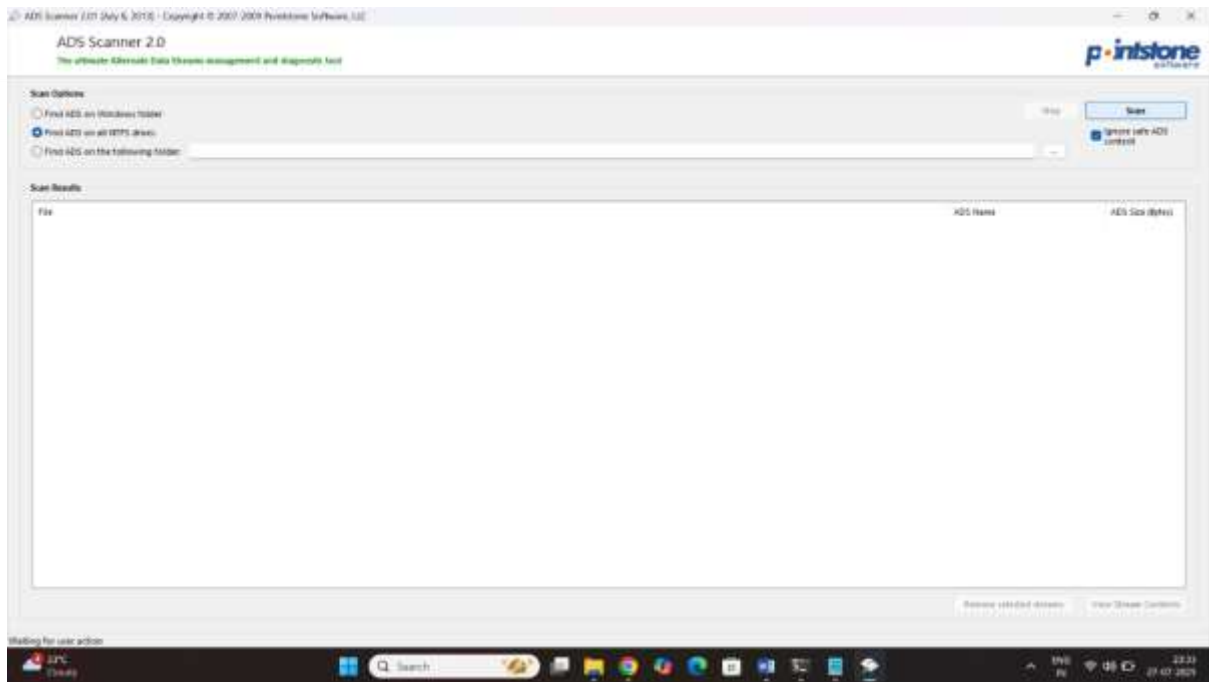


Lab 9How to find hide file in system using Ads scanner

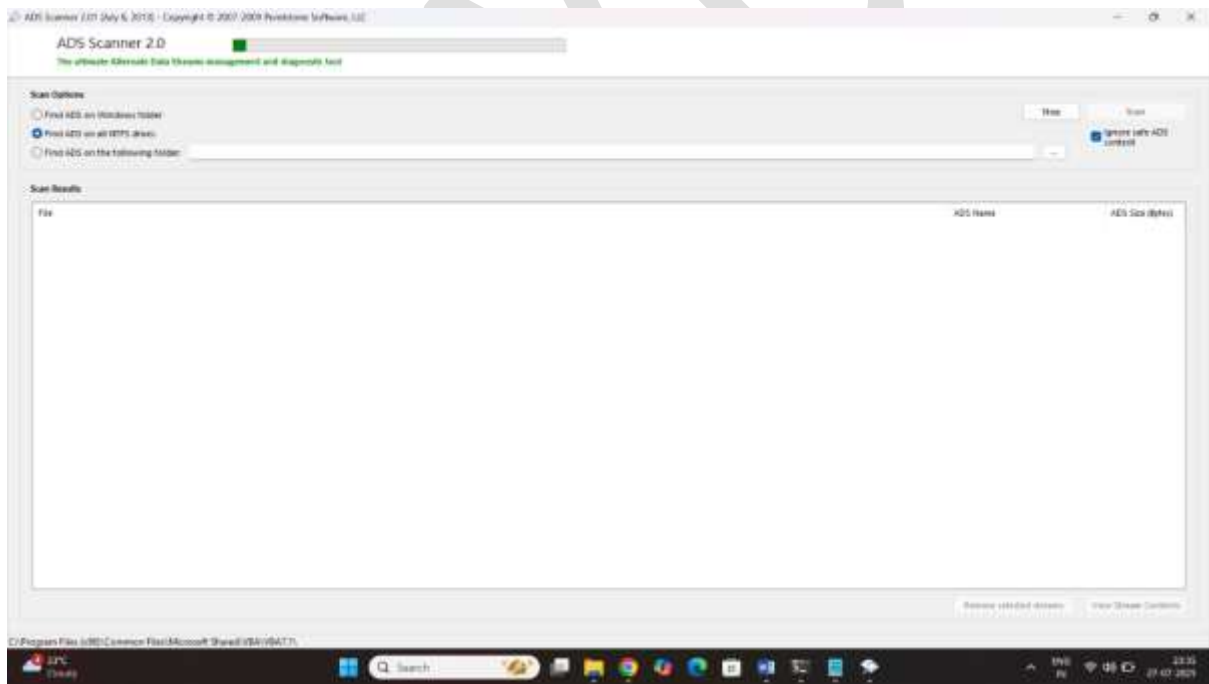
Step1 start the application



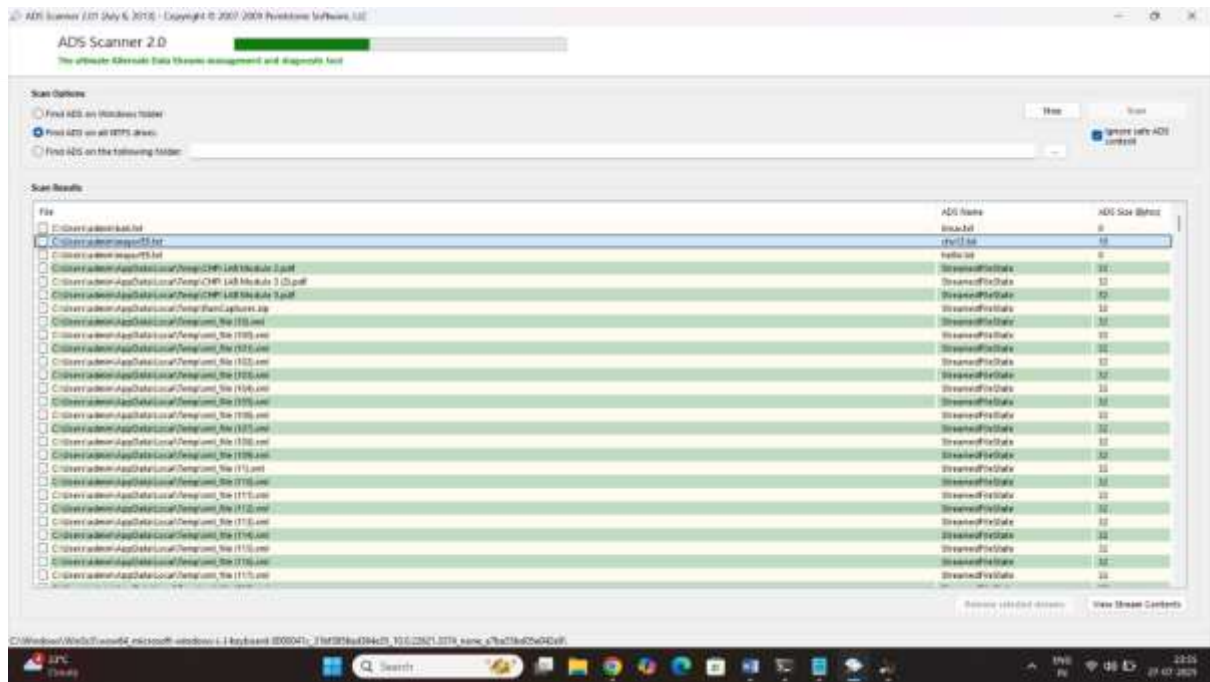
Step2 choice the any option click on the scan



Step3 active the scanning process

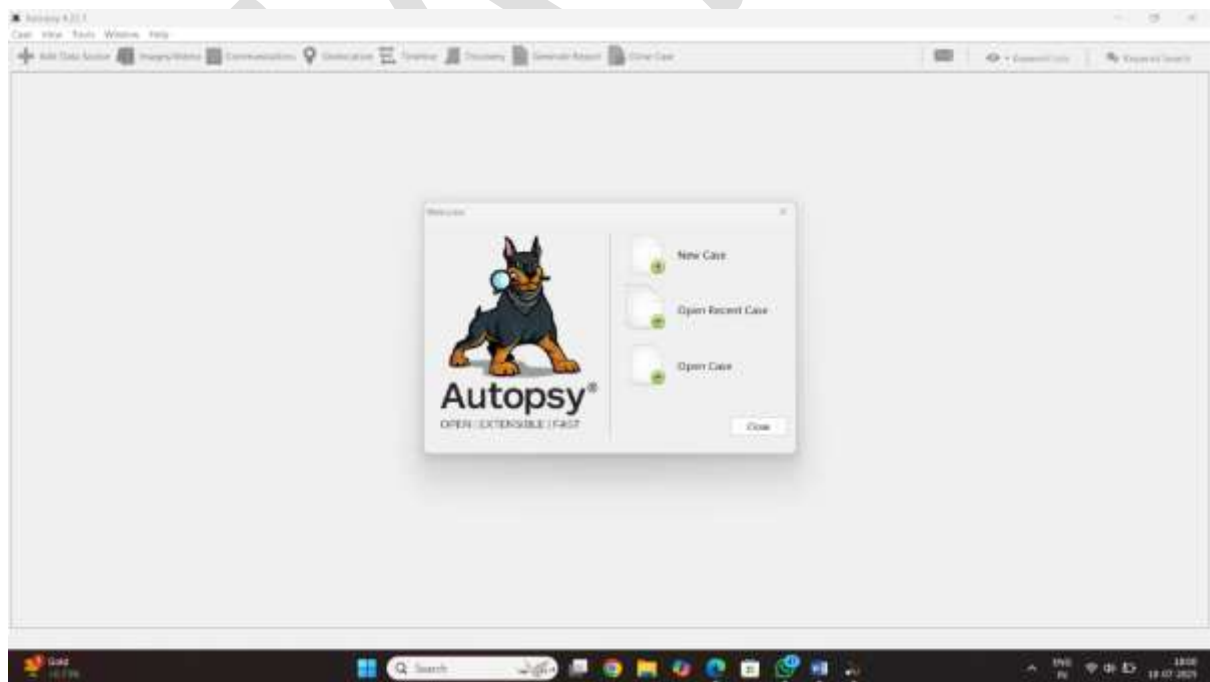


Result:



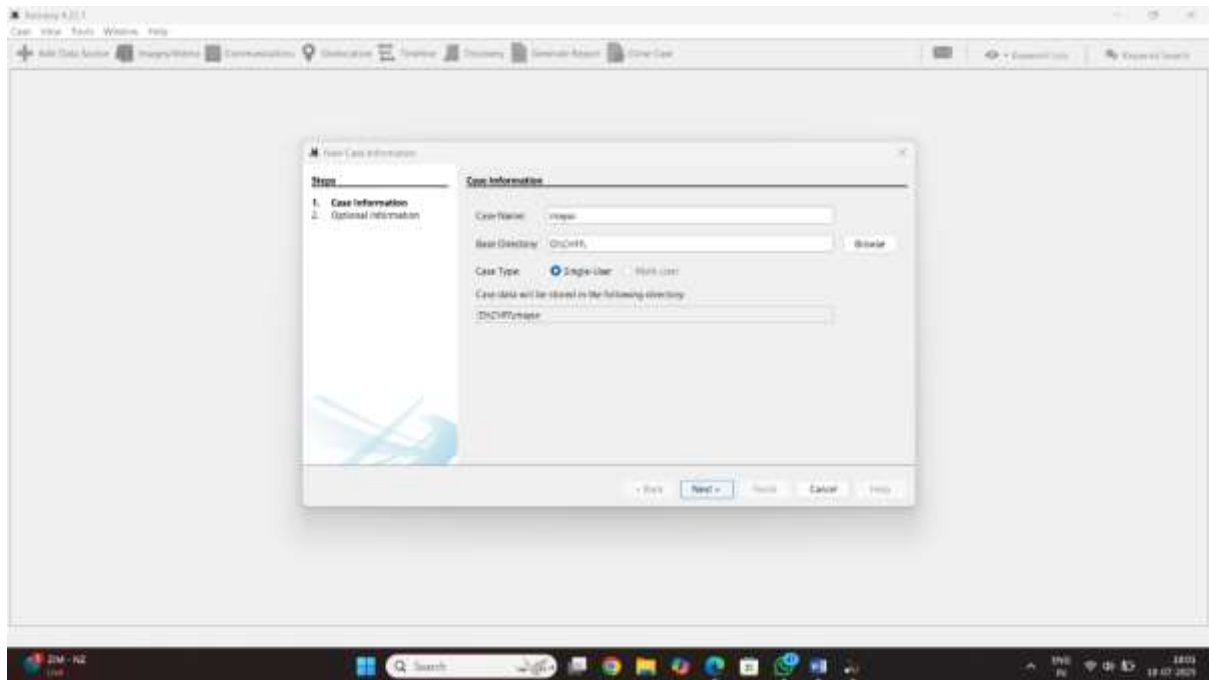
Lab 10 detect file extension mismatch using autopsy

Step2: start the autopsy and click on the new cause

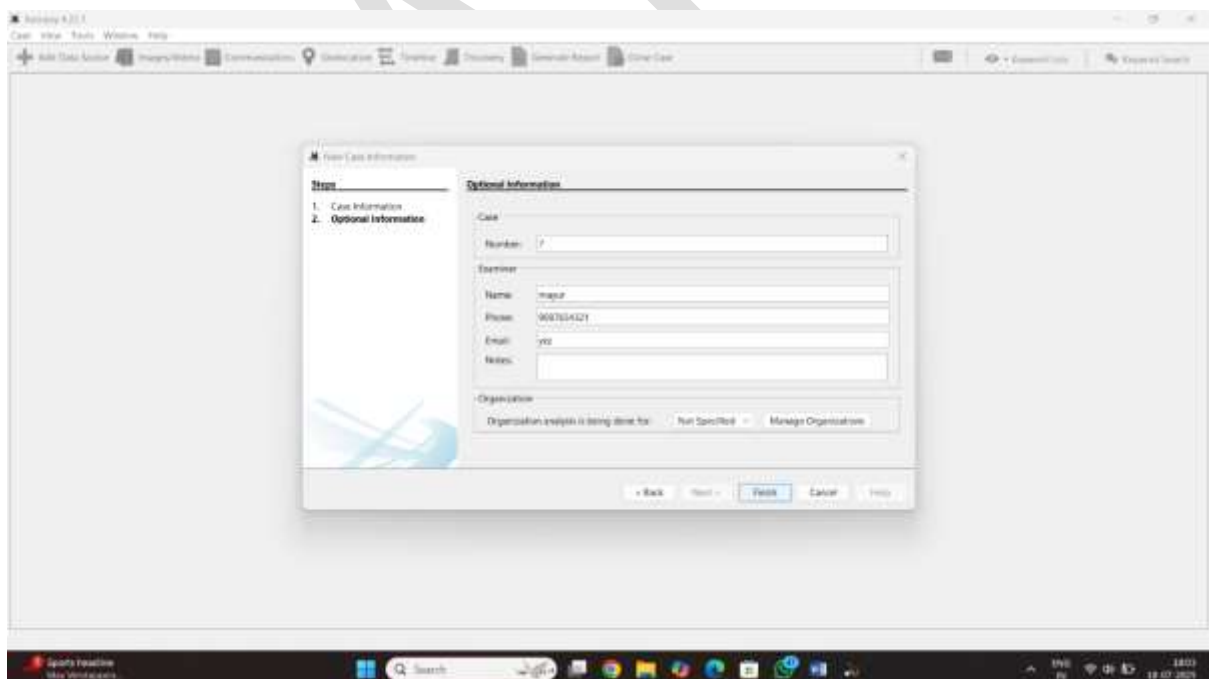


Step3: enter case name

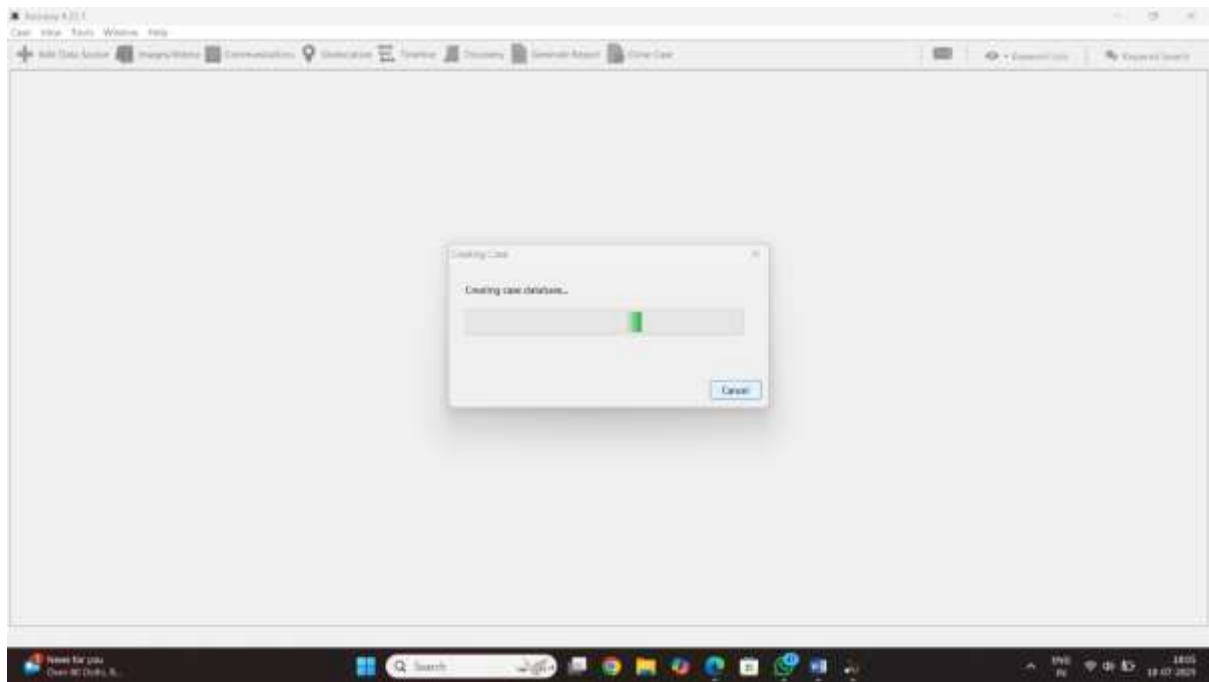
Step4: select the case file destination



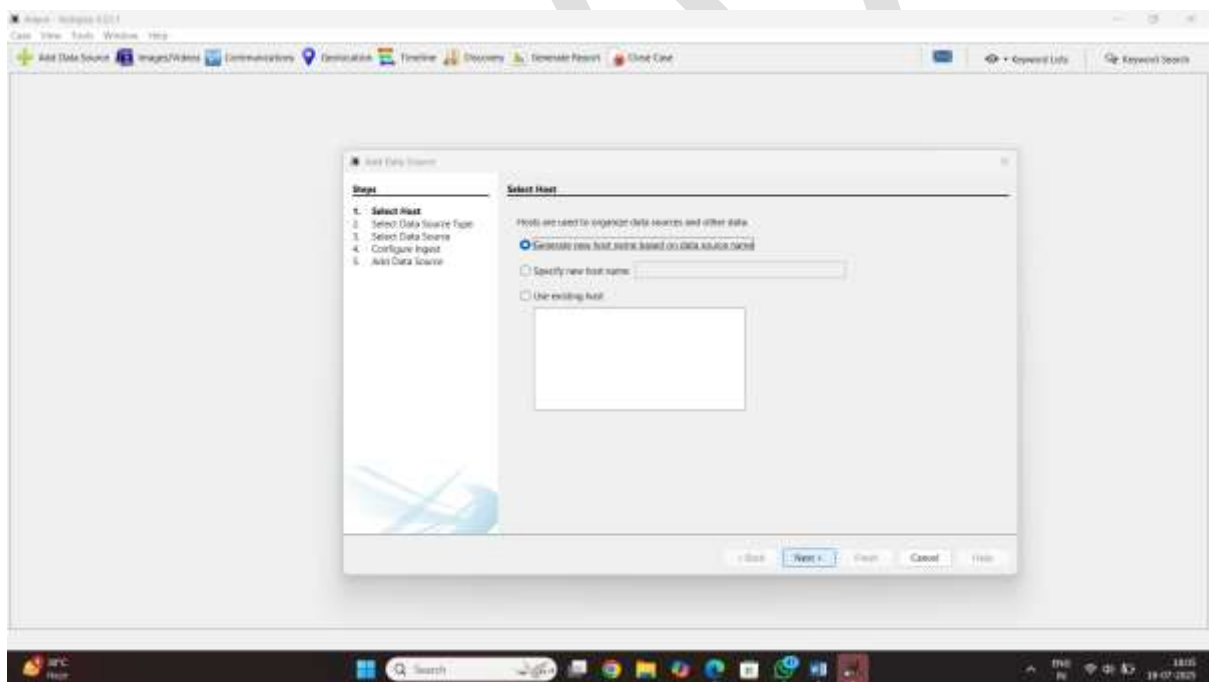
Step5 select the cause number, name ,email, m.number click on next



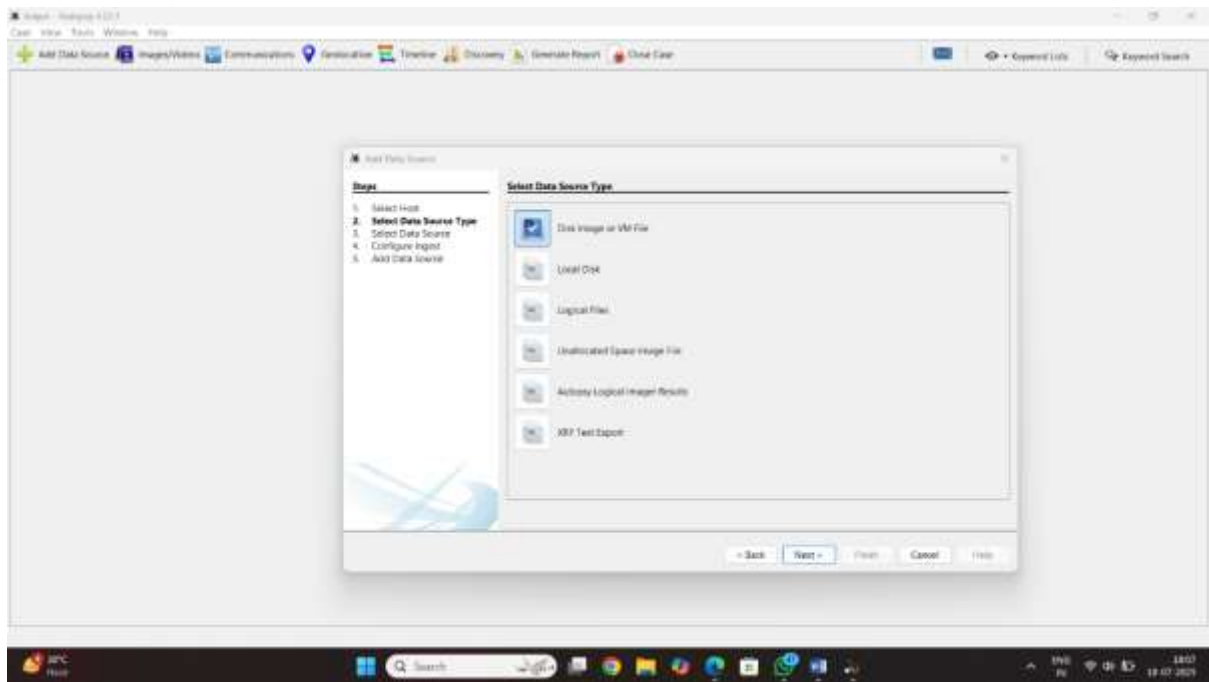
Step6 creating data base cause file



Step7 select host click on the next

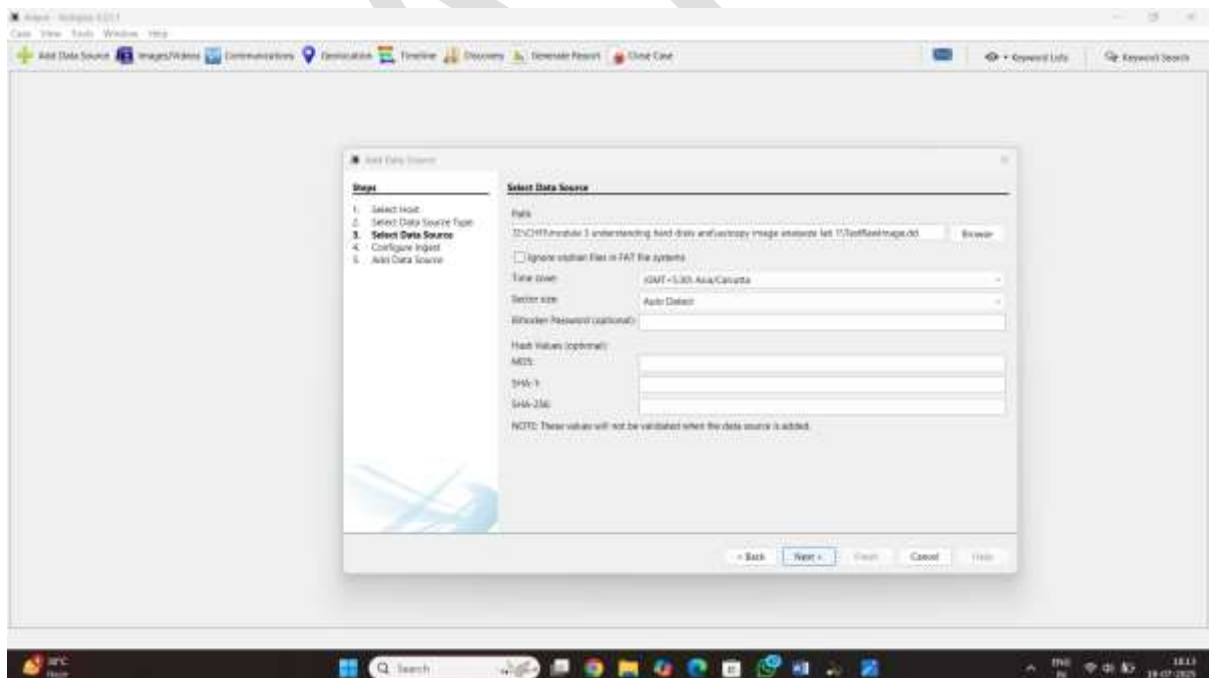


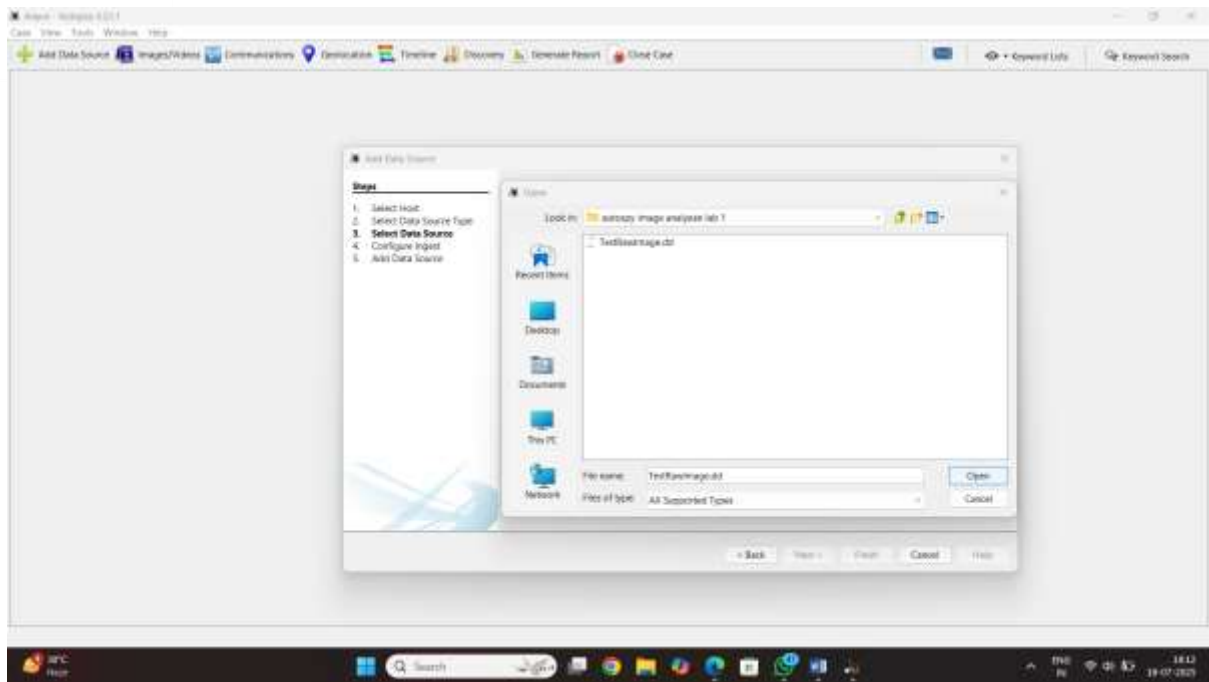
Step8 select the data source type



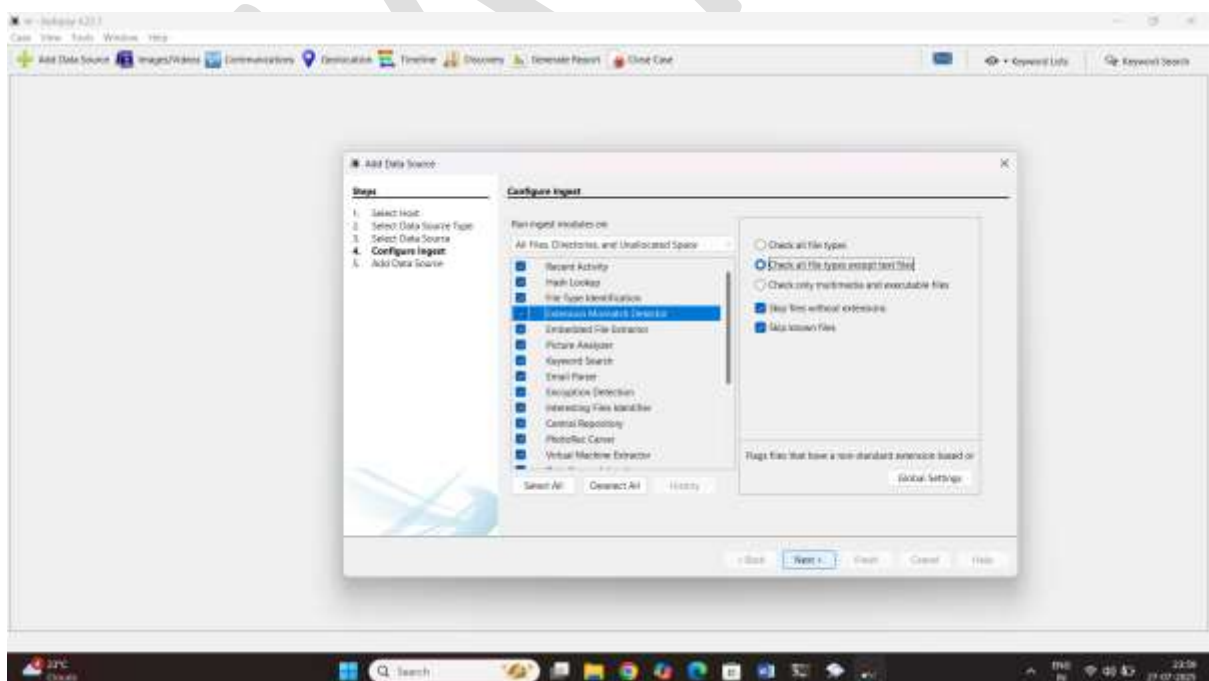
Select the disk image or vm file click on the next

Step9 select the data source type /image path folder



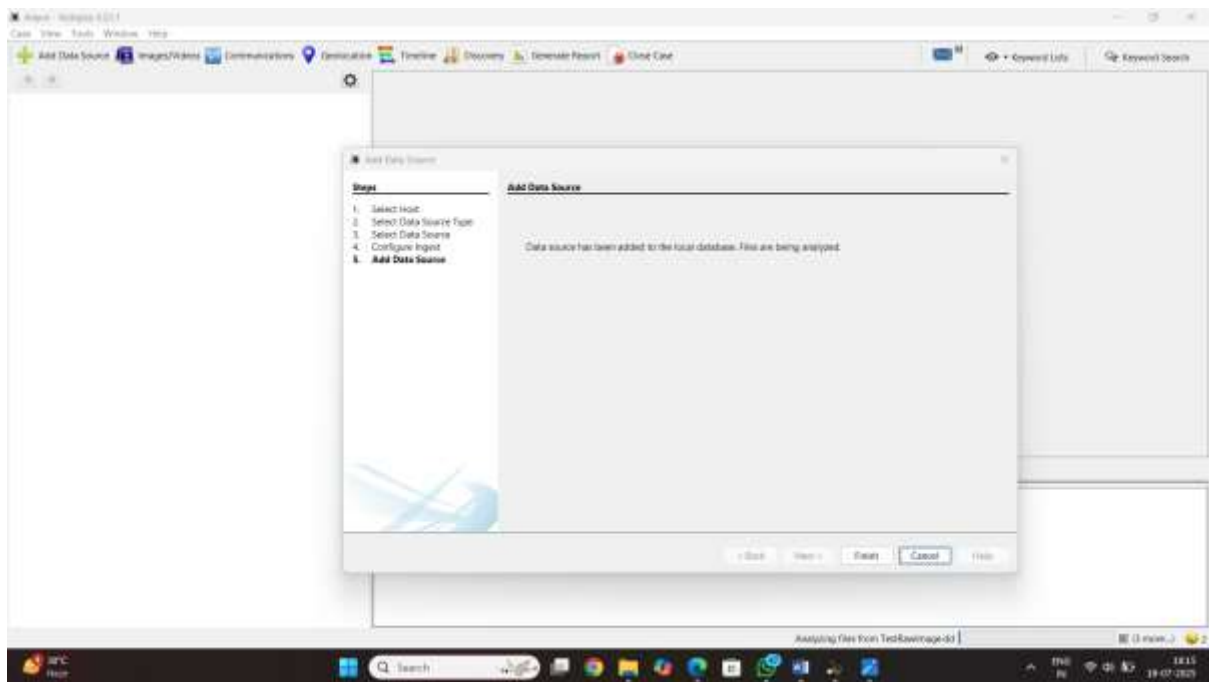


Click in the next
Step10 configure ingest
Select the option extension mismatch option

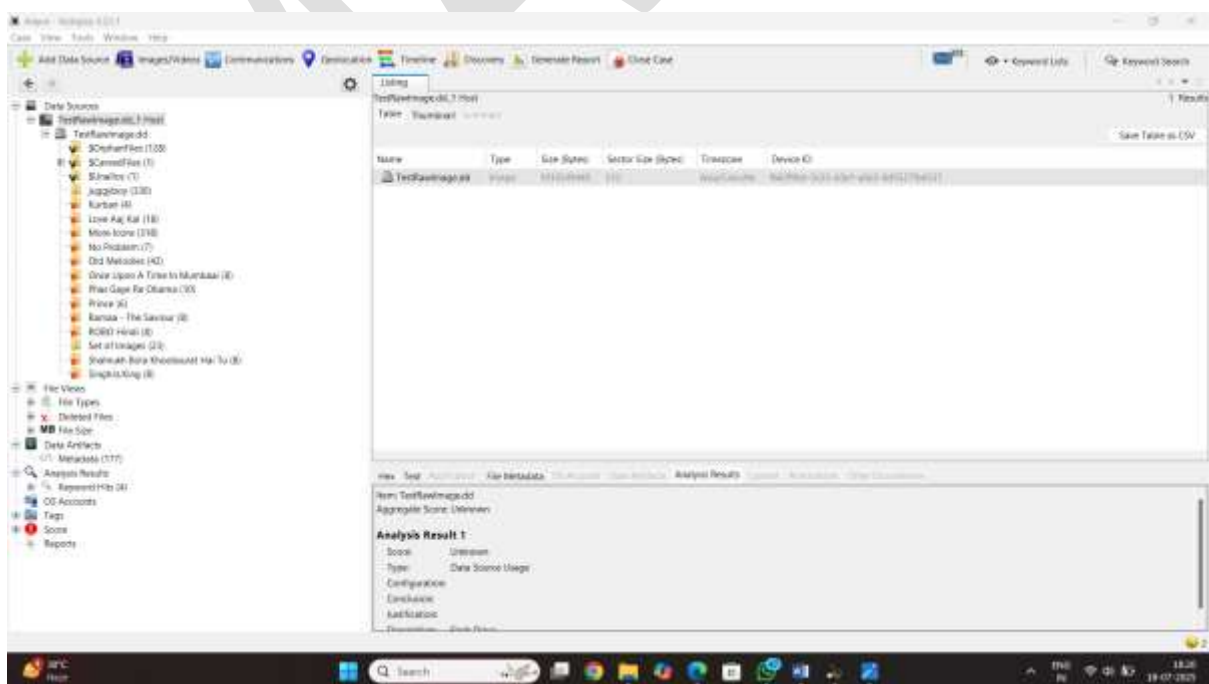


Click on the next

Step11: add data source

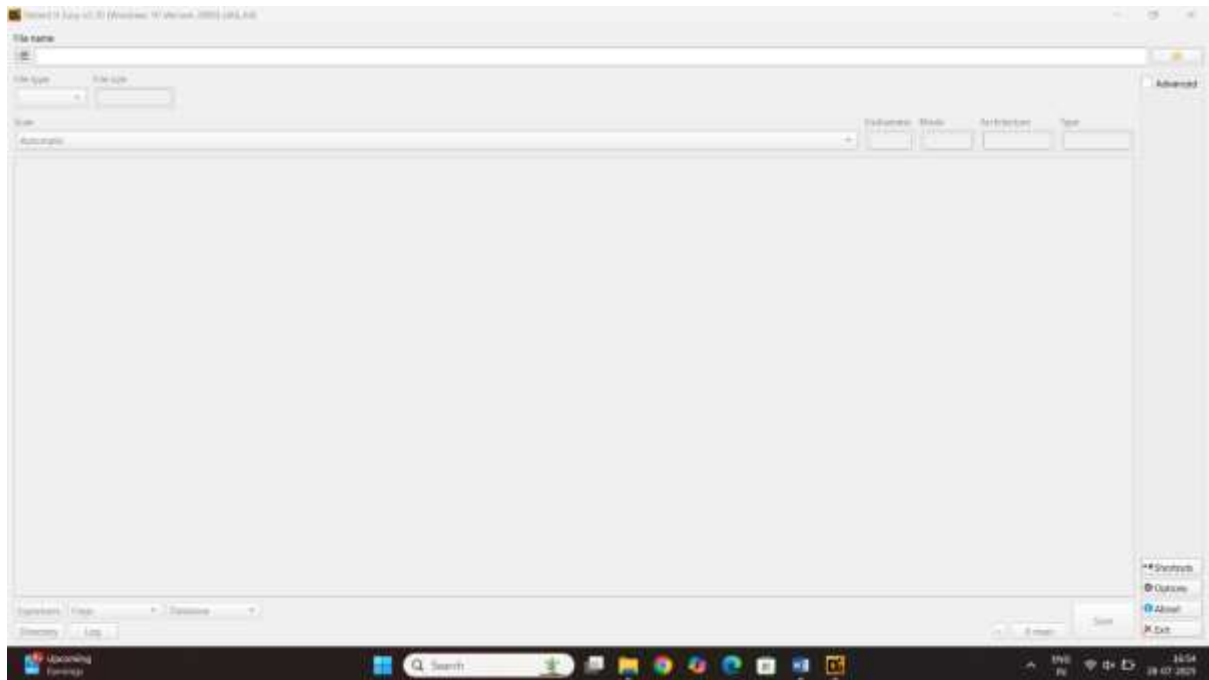


Click on the next
Analyze the image of content

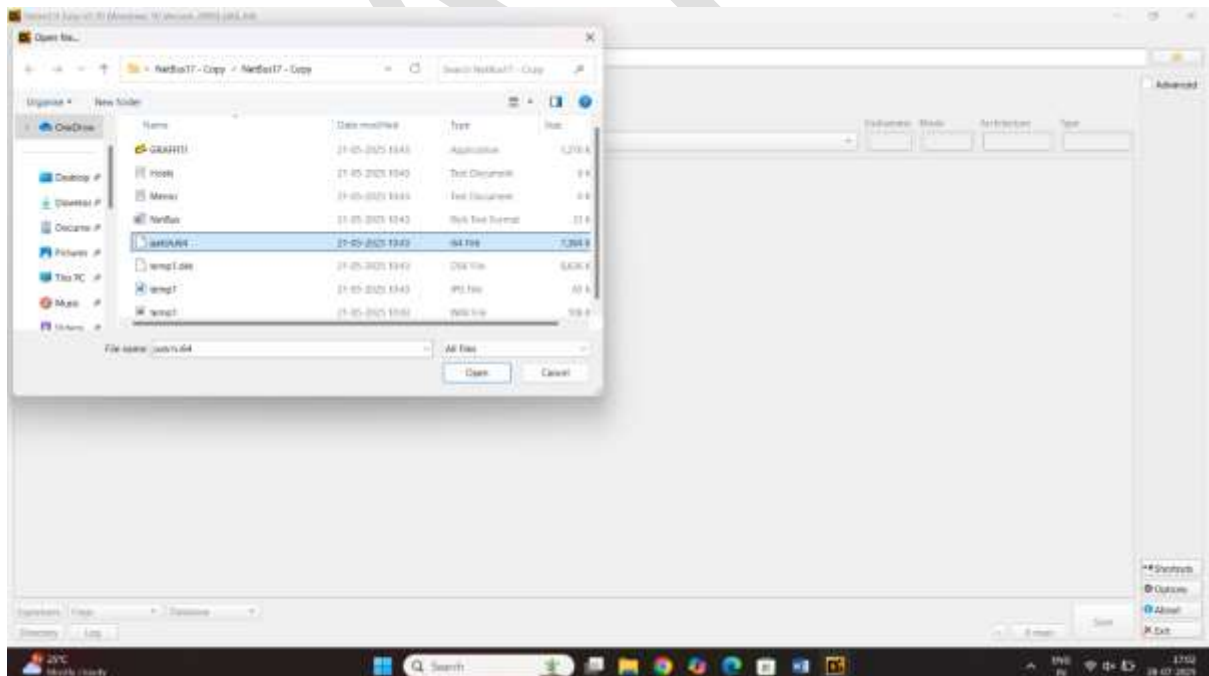


Lab11 unpack program packers using die.exe tool

Step1 start the tool



Step2 select the file unpacker



Step3 click on the scan option scan

