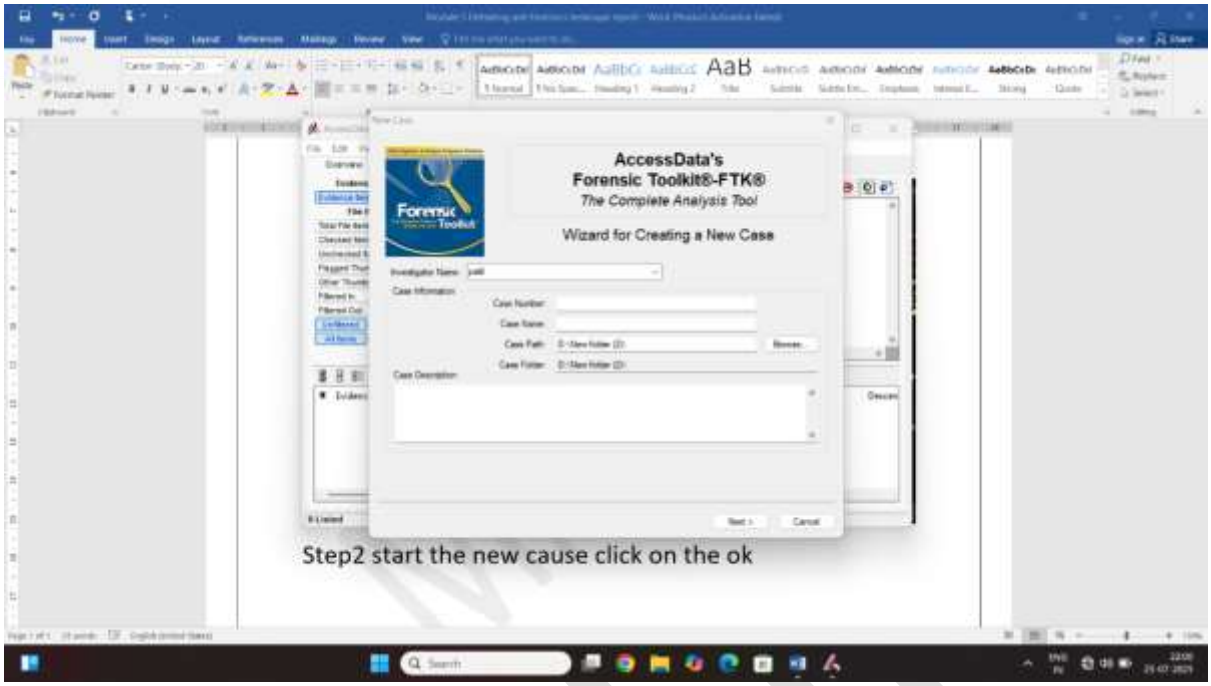
Module 5 Defeating anti forensics techniques

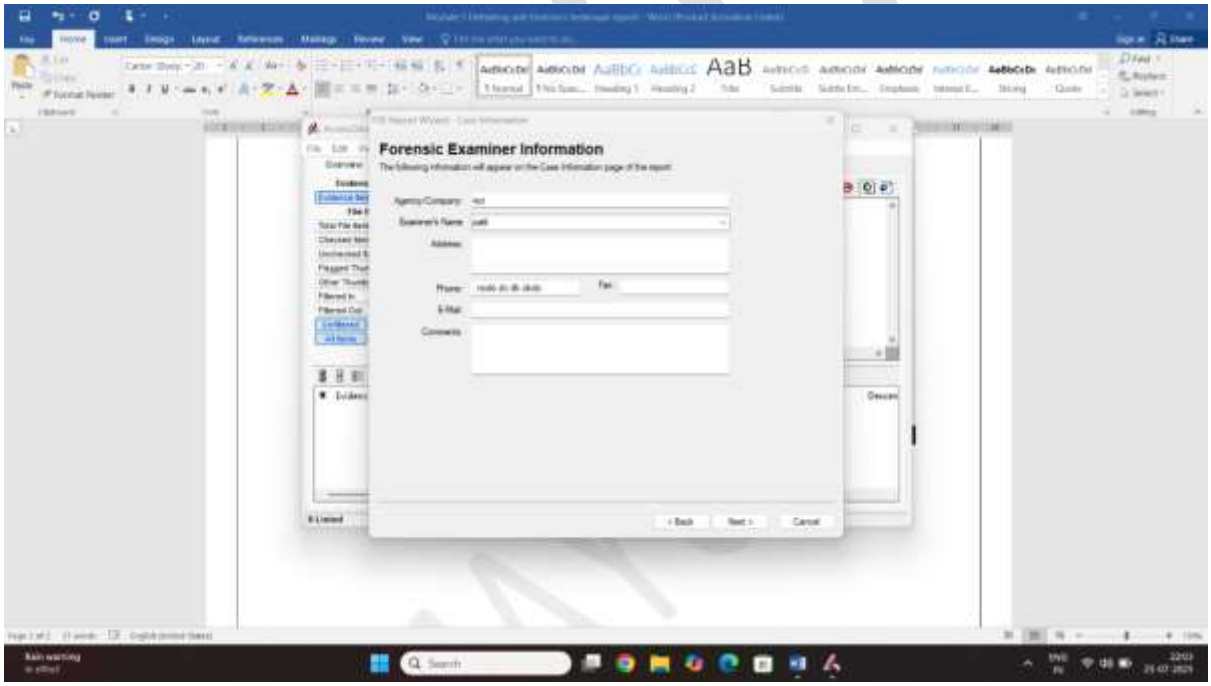
lab 1 using forensic tool

step1 start the forensic tool

Step2 start the new cause click on the ok

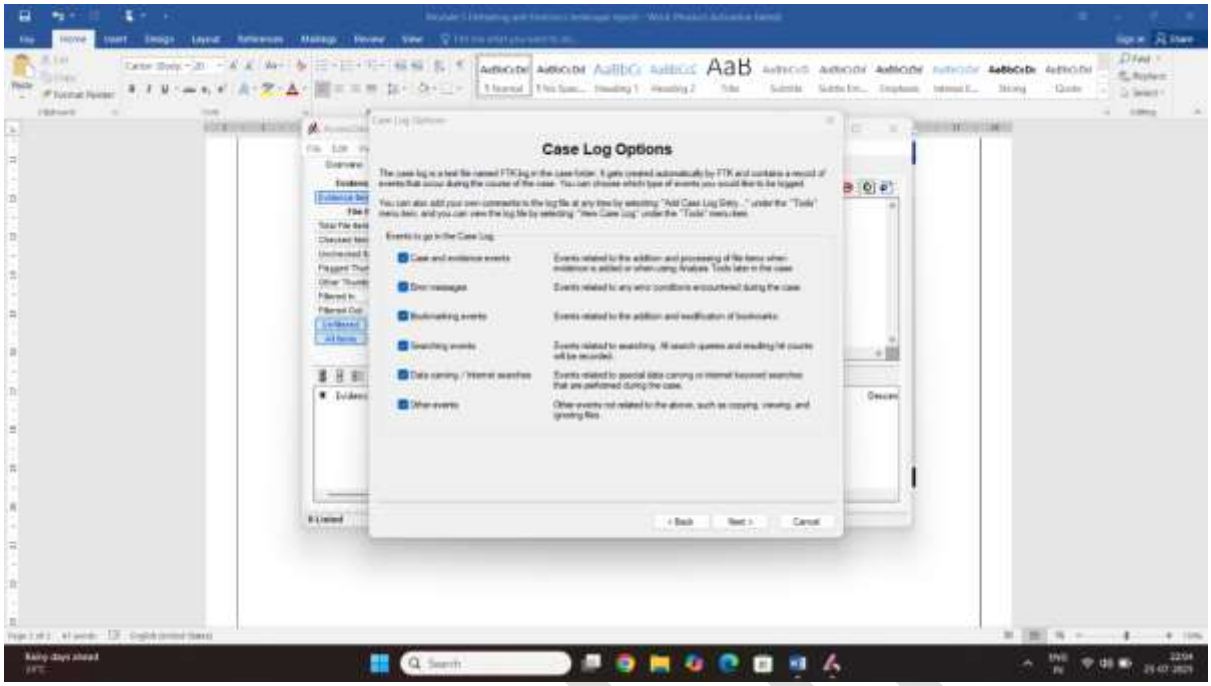
Step3 enter cause details , name , number, and destination file etc



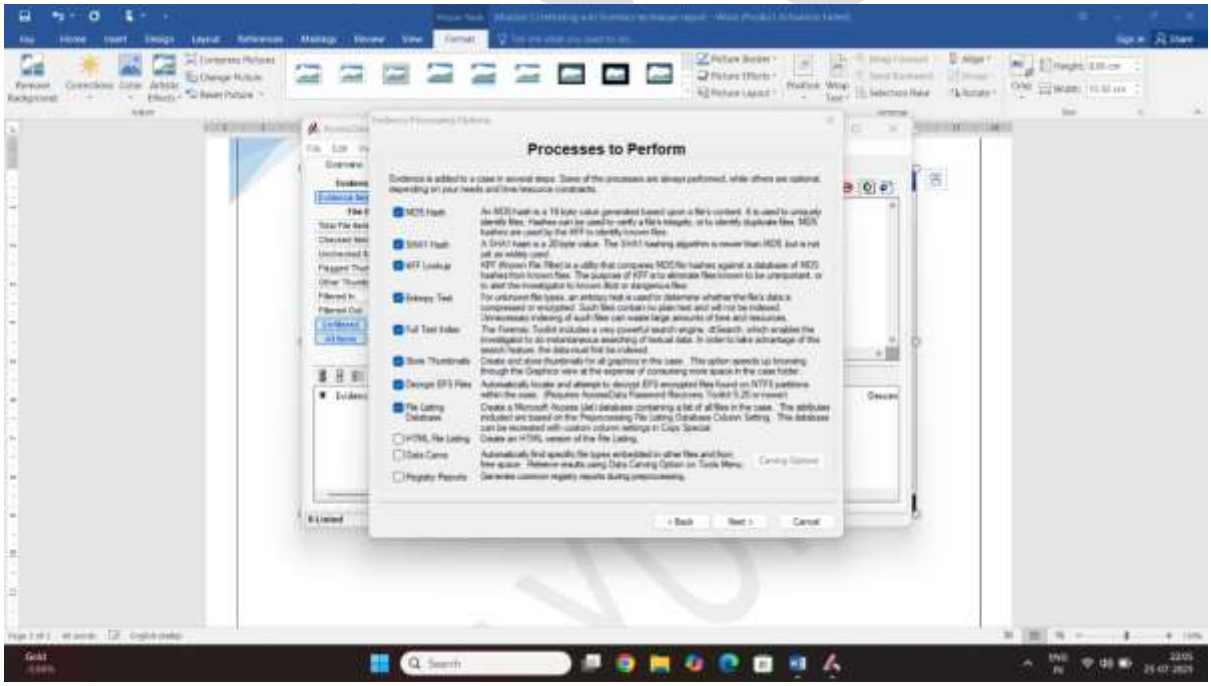


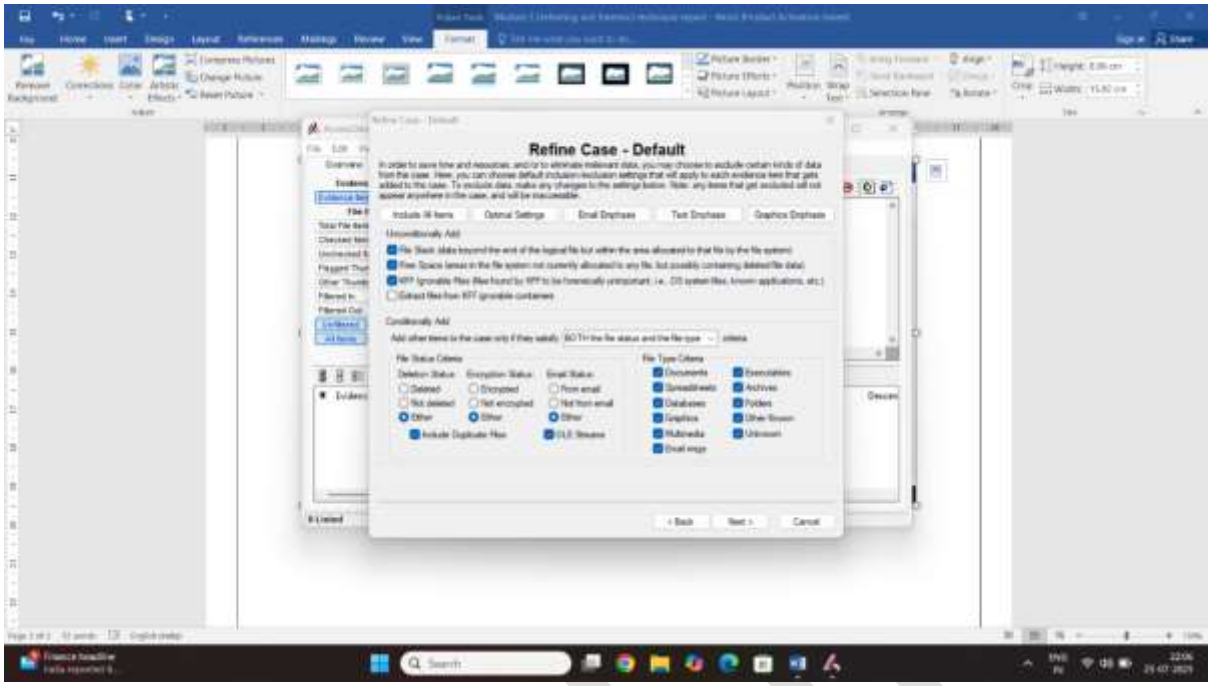
Click on the next

Step4 select case log option

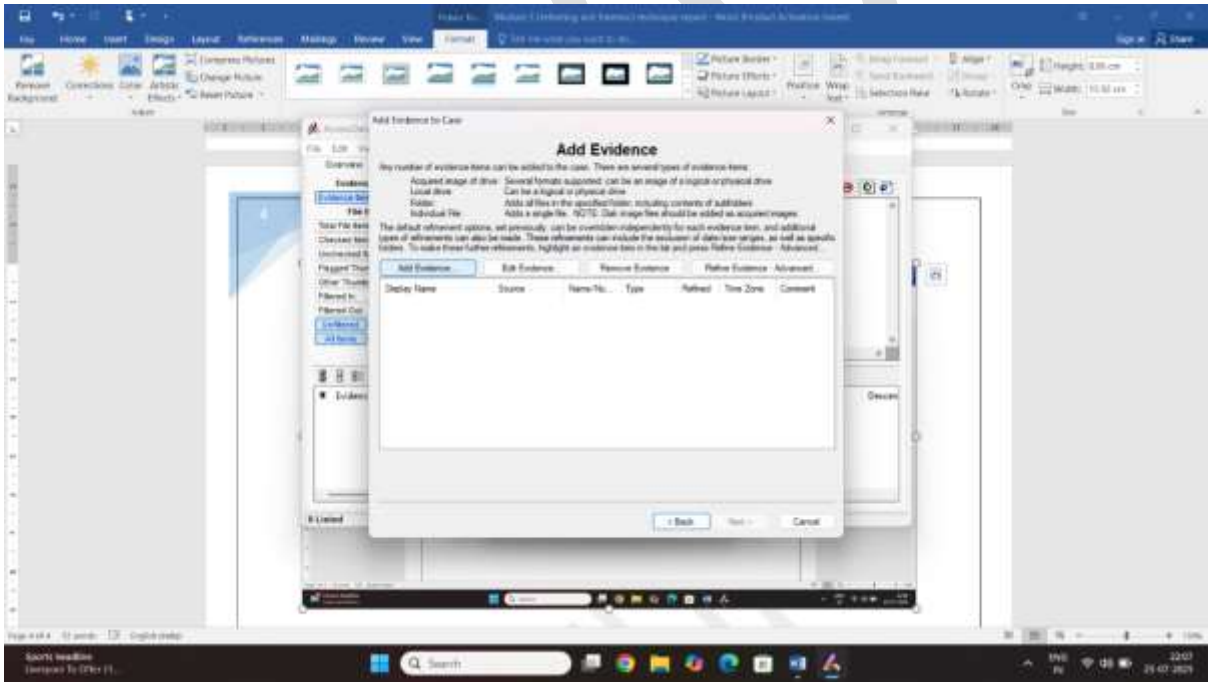


Step5 select the process to perfrome

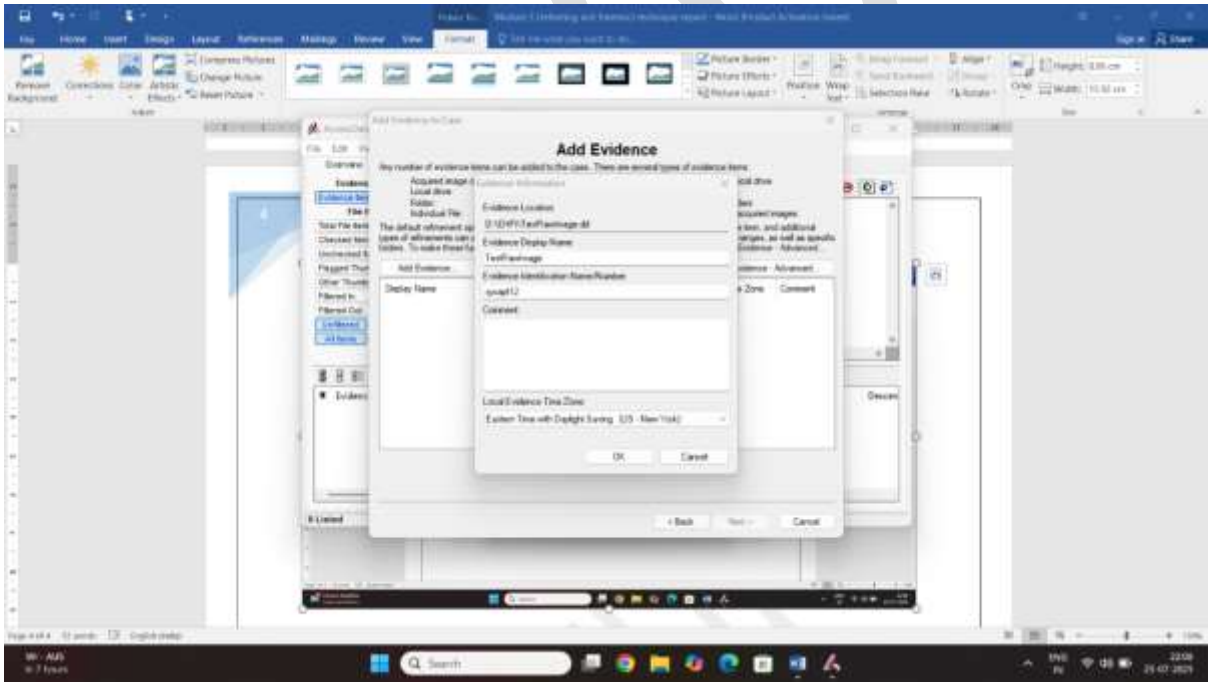




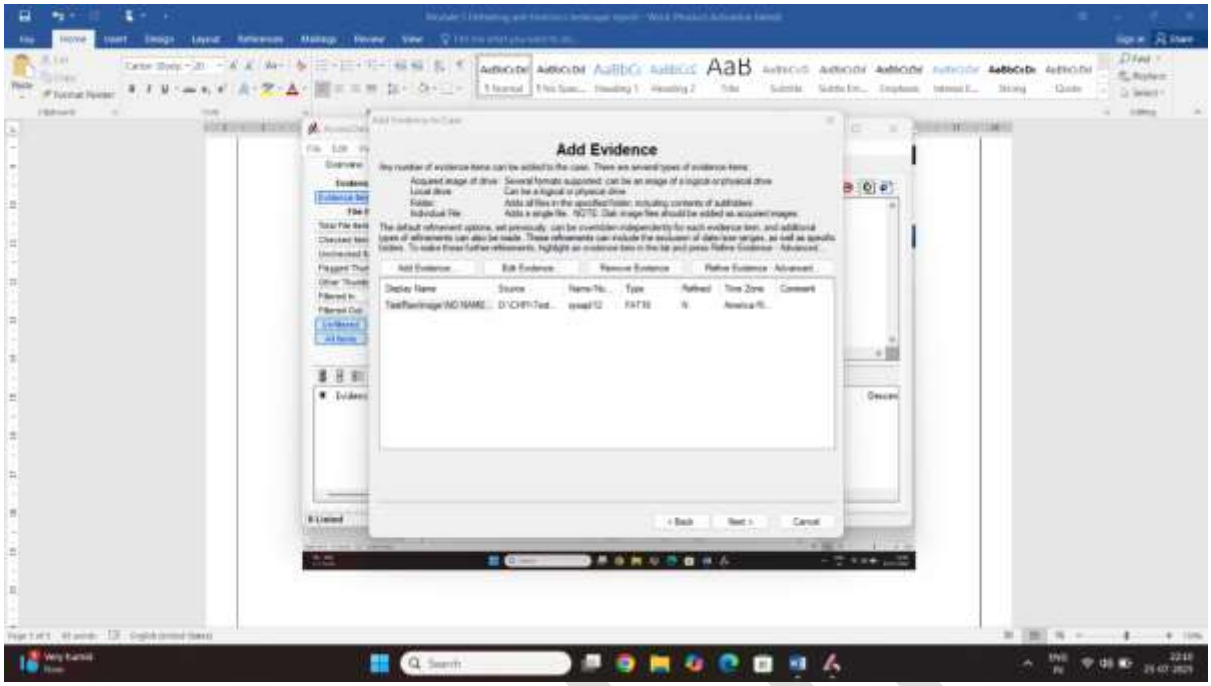
Step6 add evidence file dd image click on



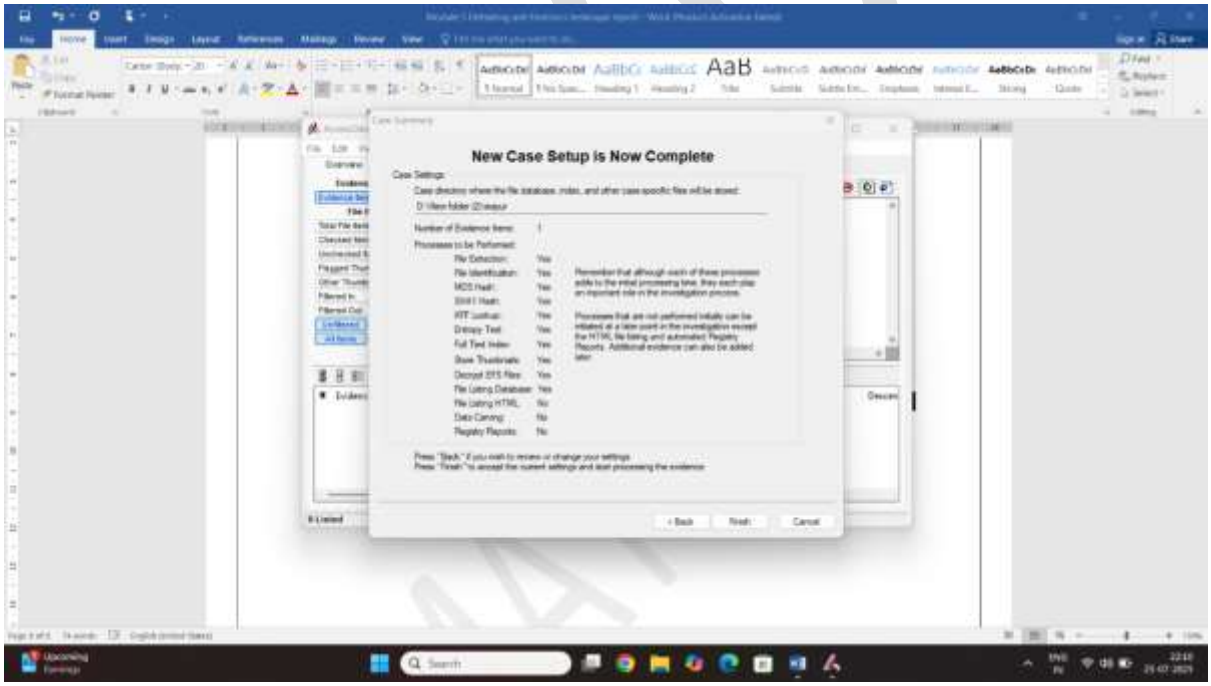
Step7 select the d.d image



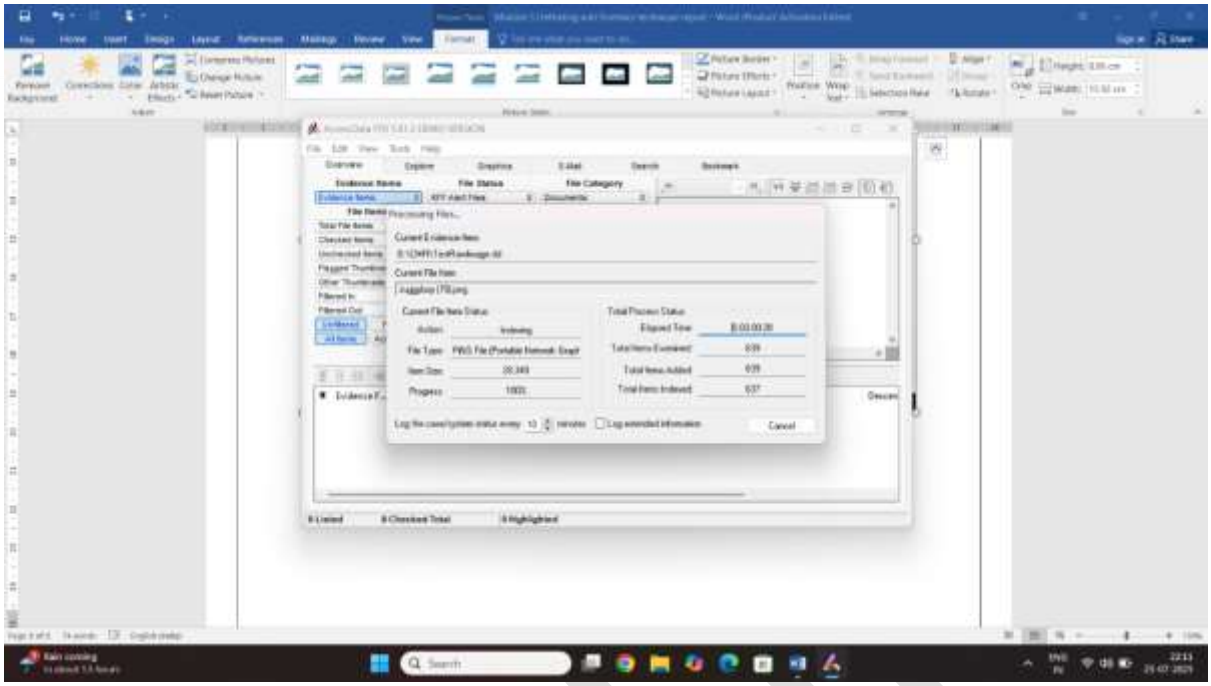
Step8 add successful evidence file



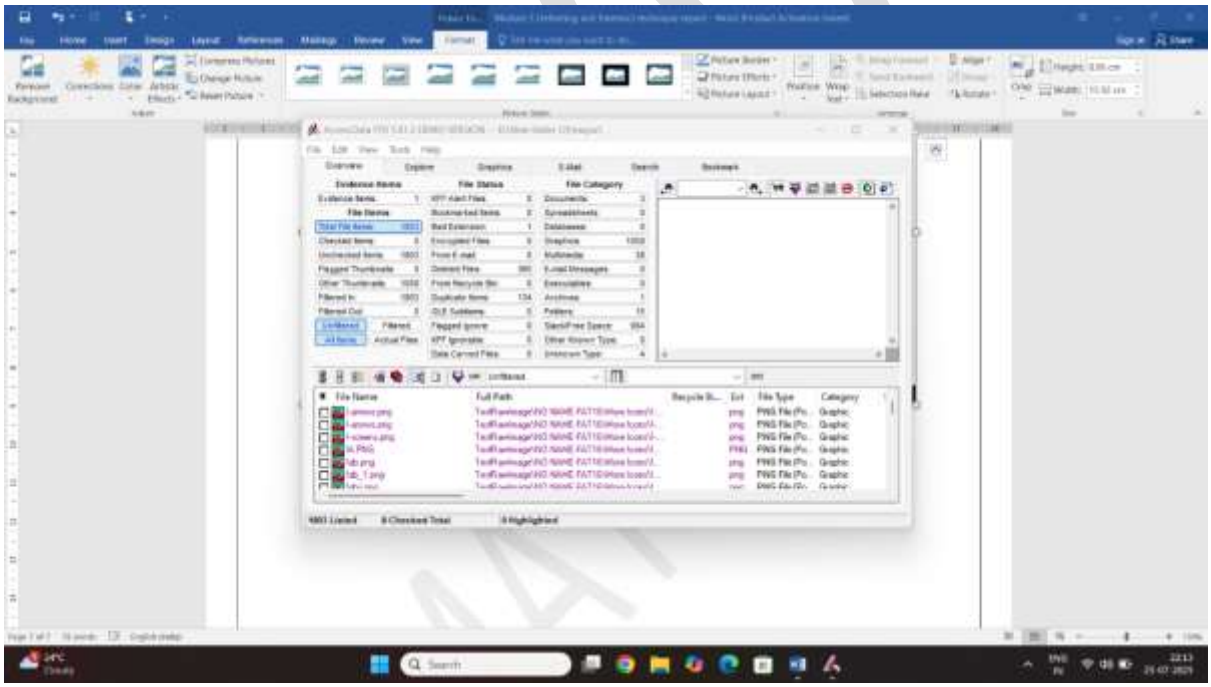
Click on the next

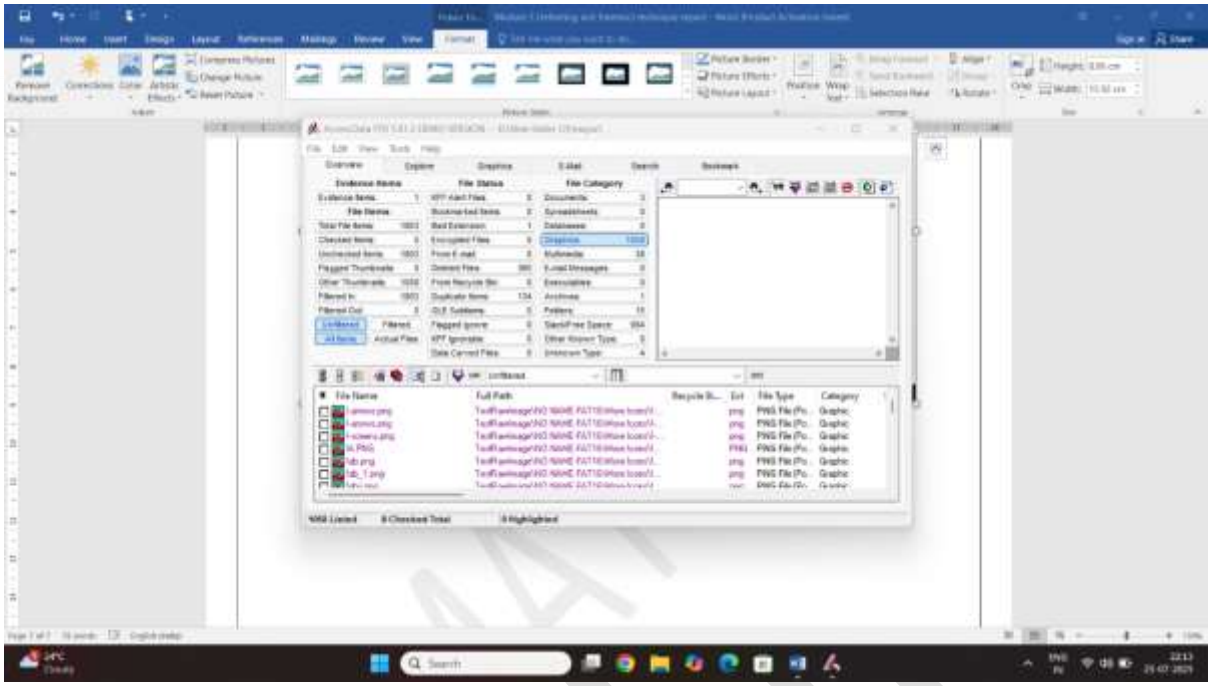


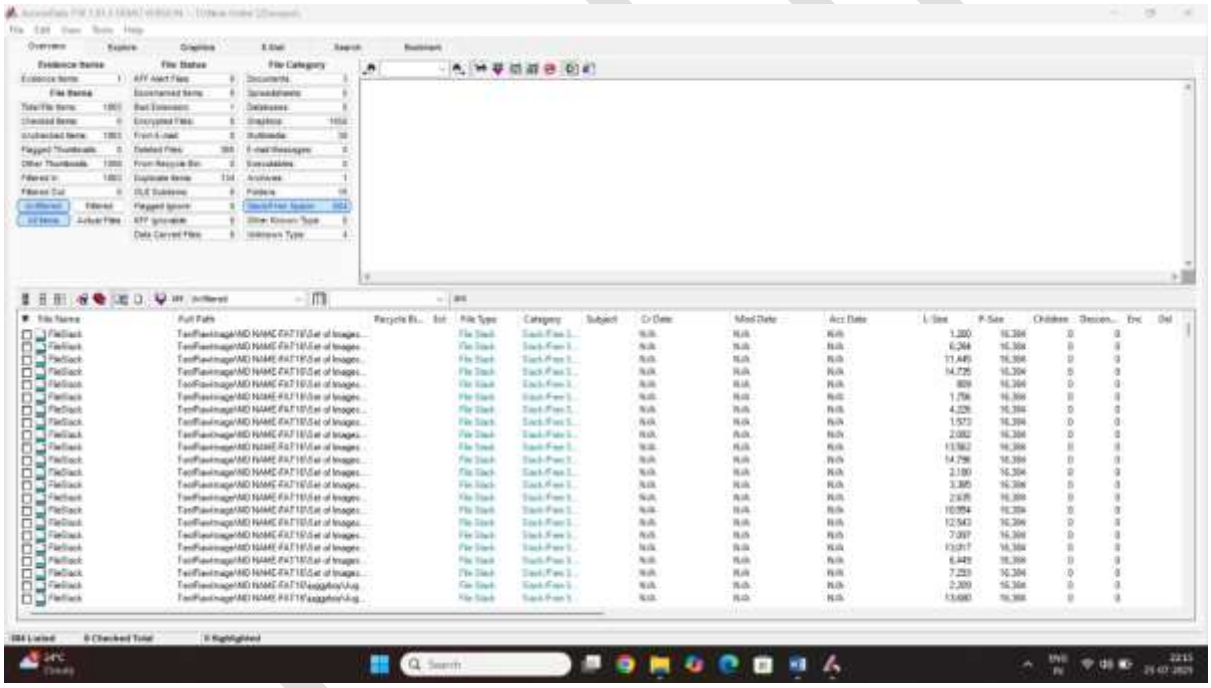
Carving the data process



Result





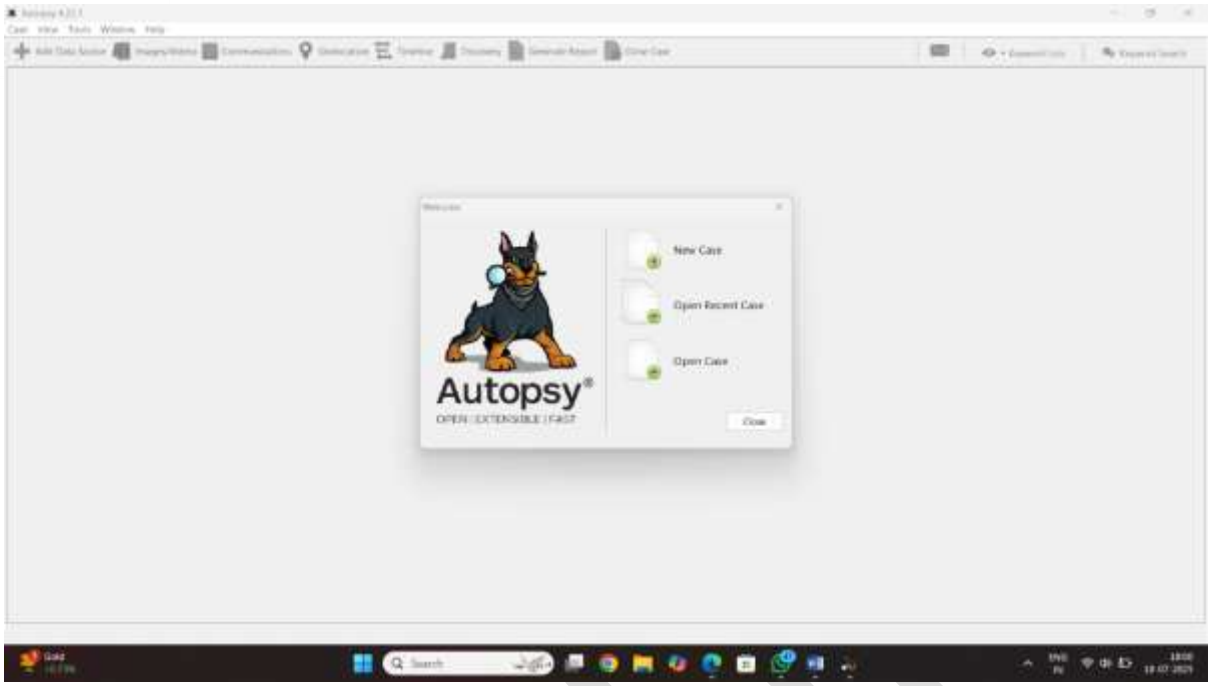


Lab2 SSD file carving on a windows file system

Using Autopsy

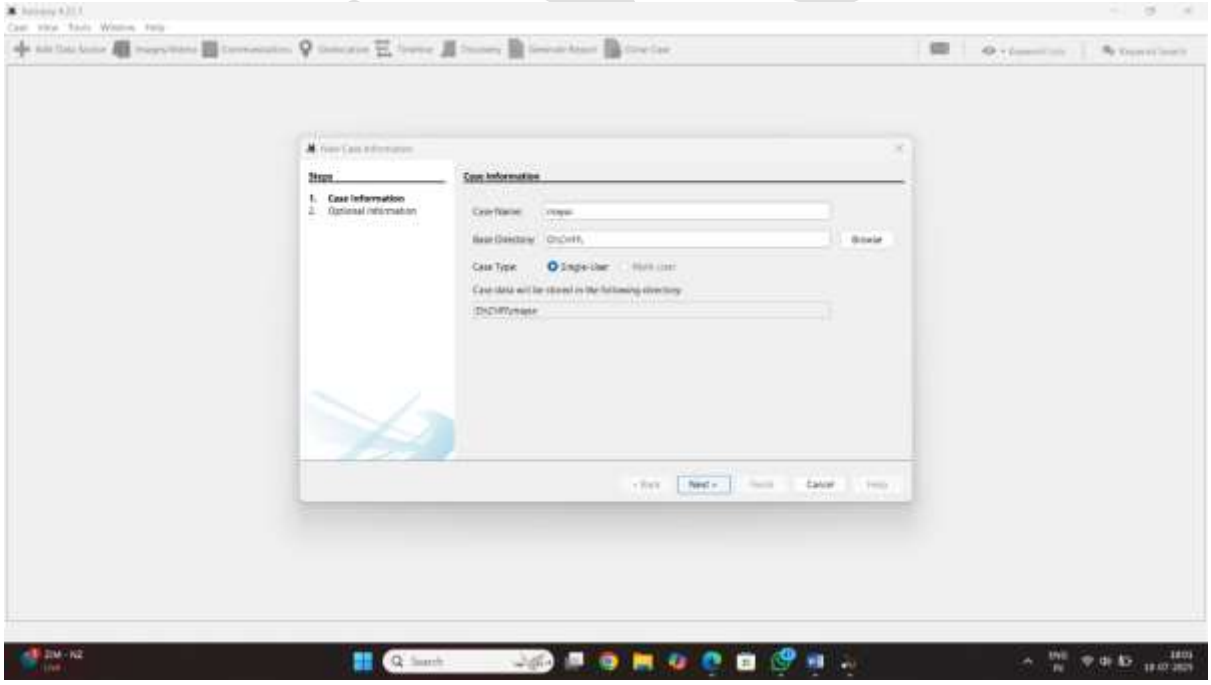
Step1: download the autopsy in windows

Step2: start the autopsy and click on the new cause

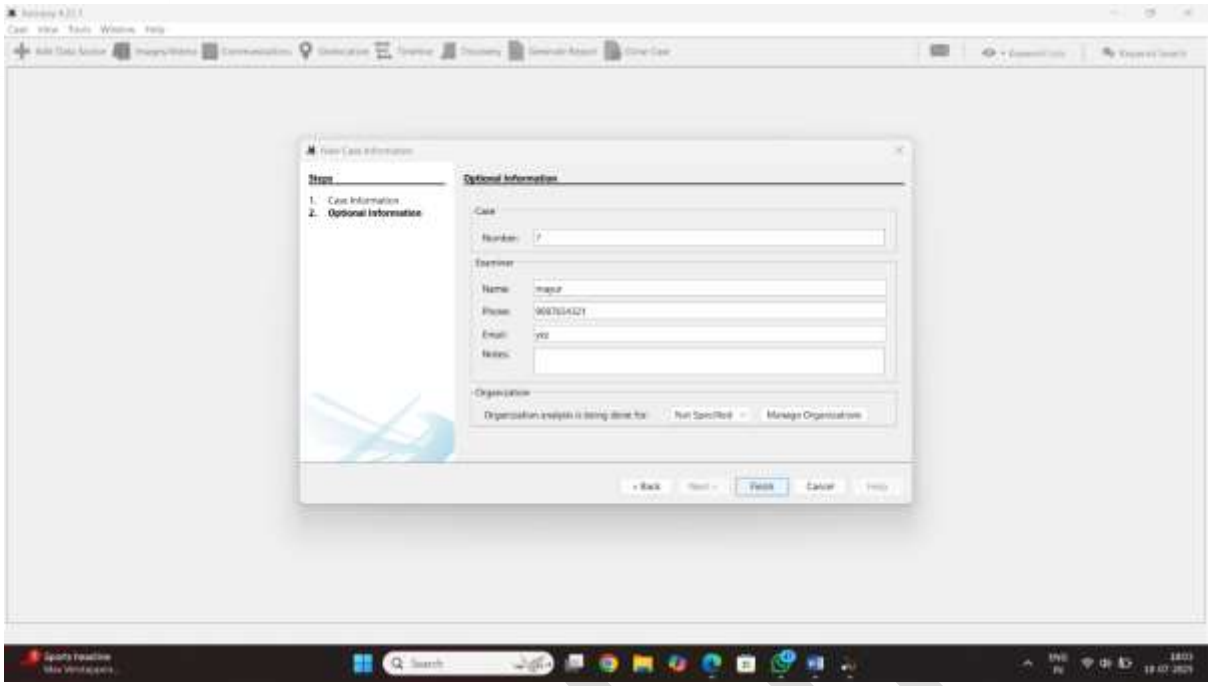


Step3: enter case name

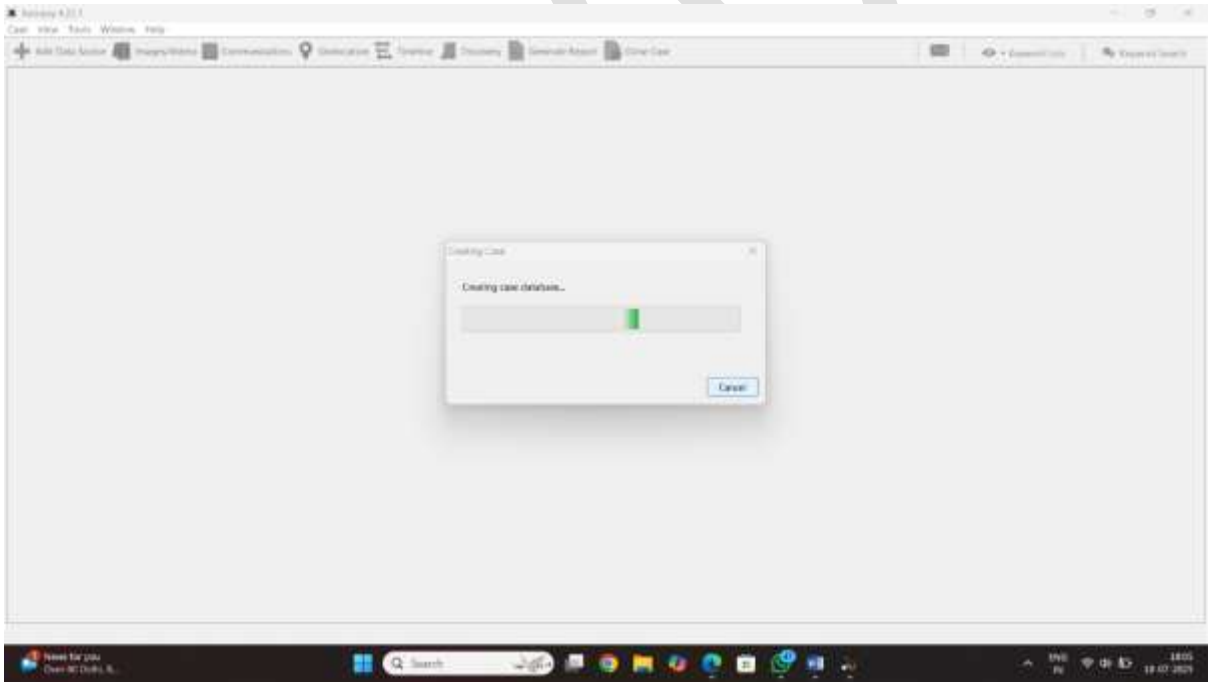
Step4: select the case file destination



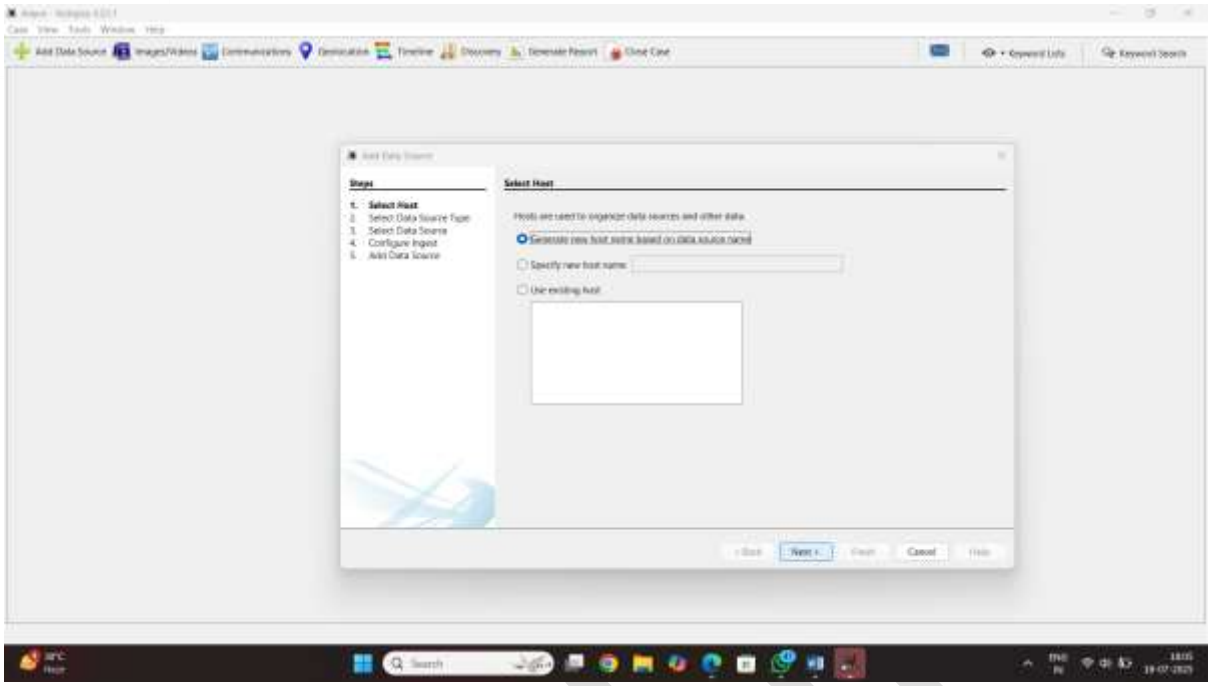
Step5 select the cause number, name ,email, m.number click on next



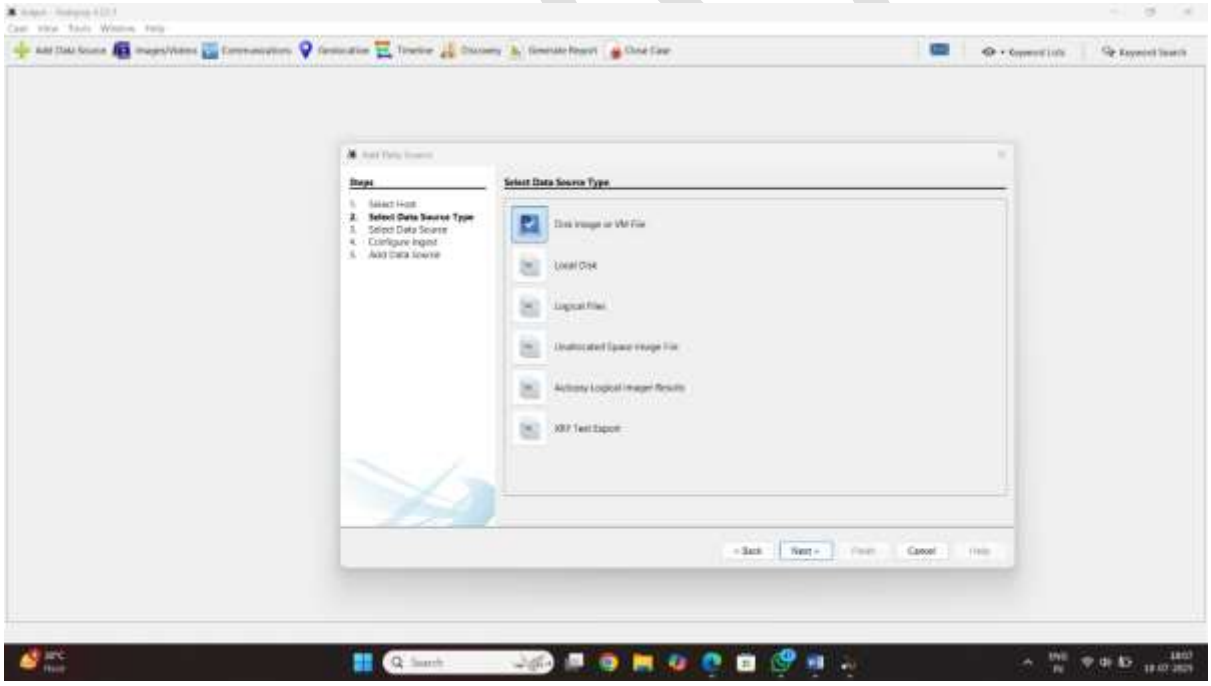
Step6 creating data base cause file



Step7 select host click on the next

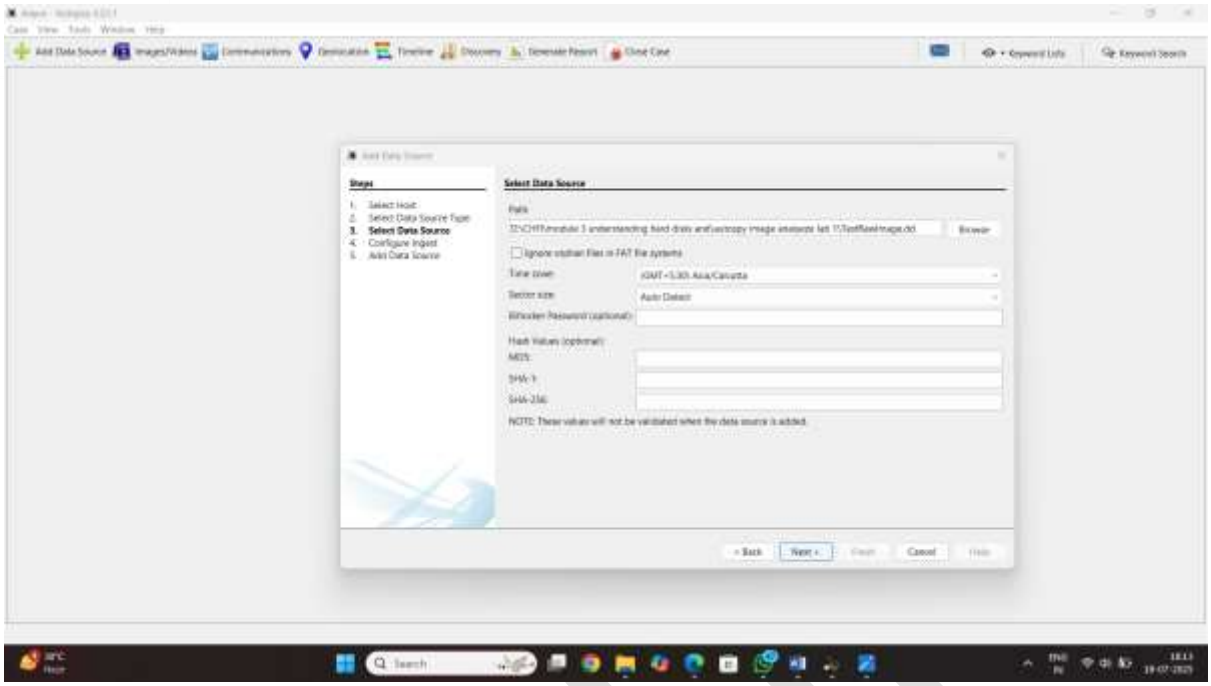


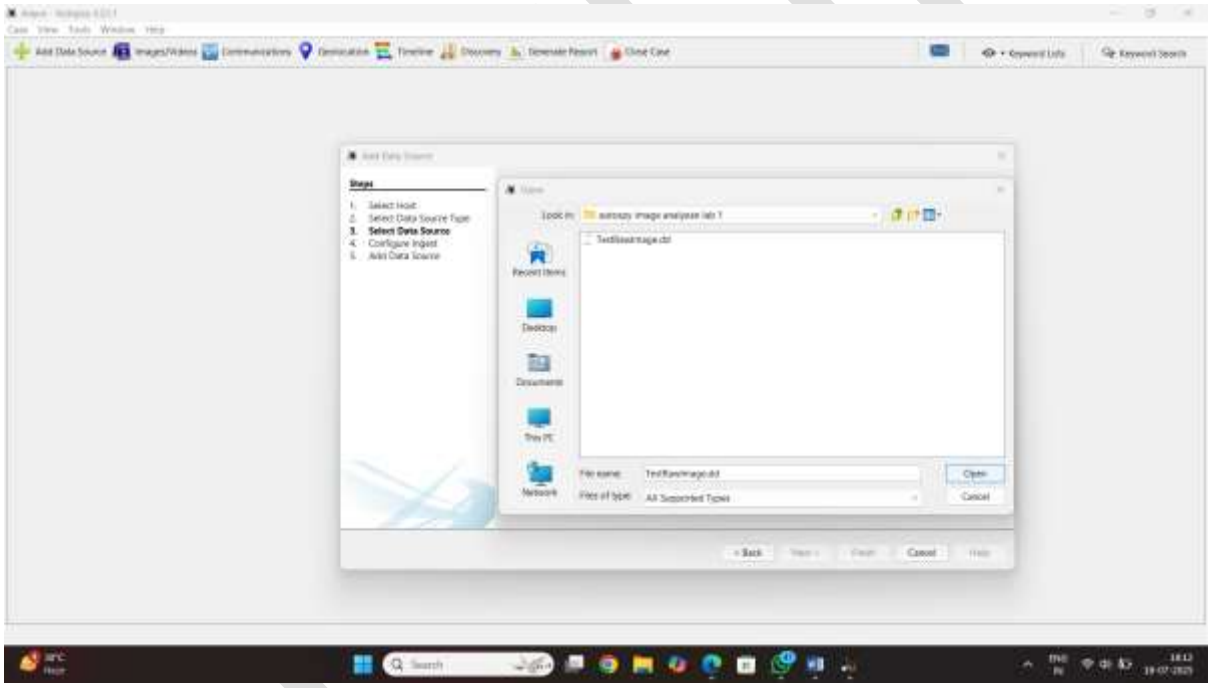
Step8 select the data source type



Select the disk image or vm file click on the next

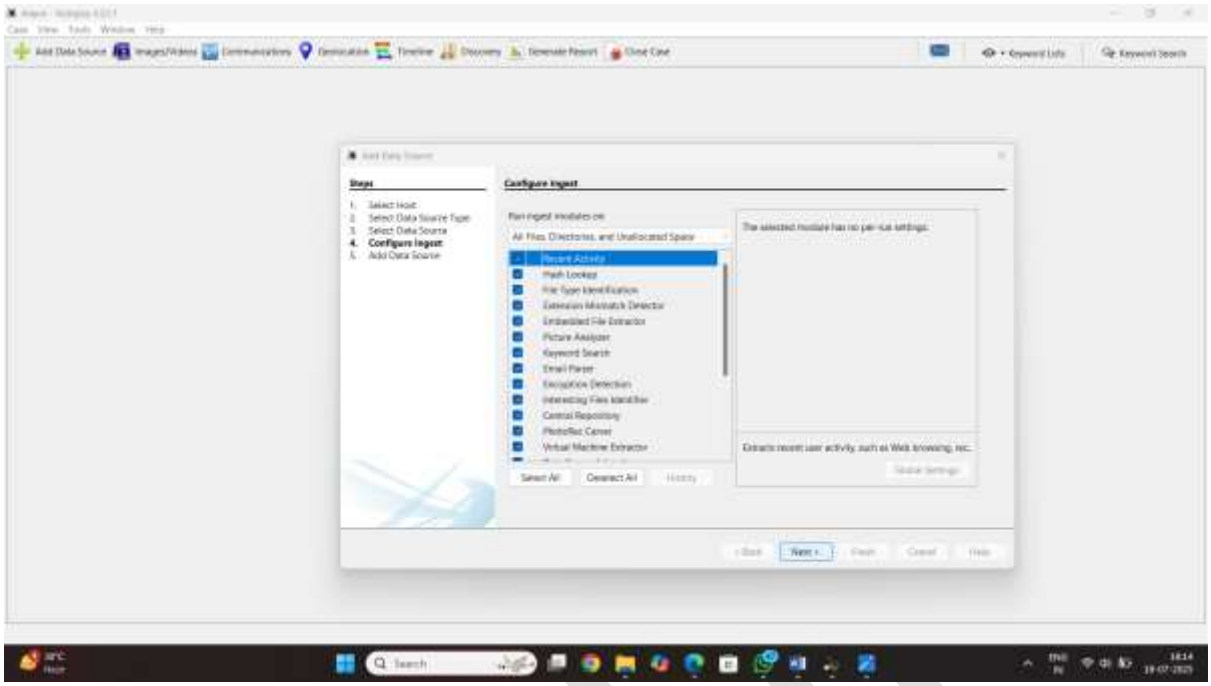
Step9 select the data source type /image path folder





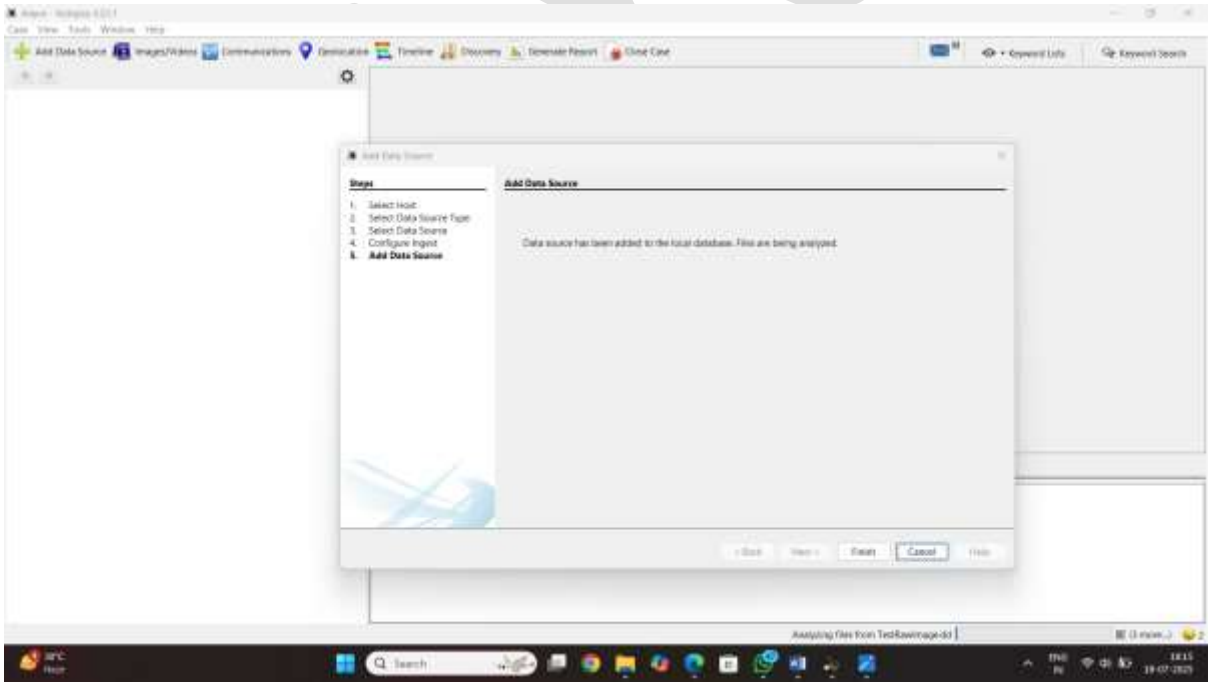
Click in the next

Step10 configure ingest



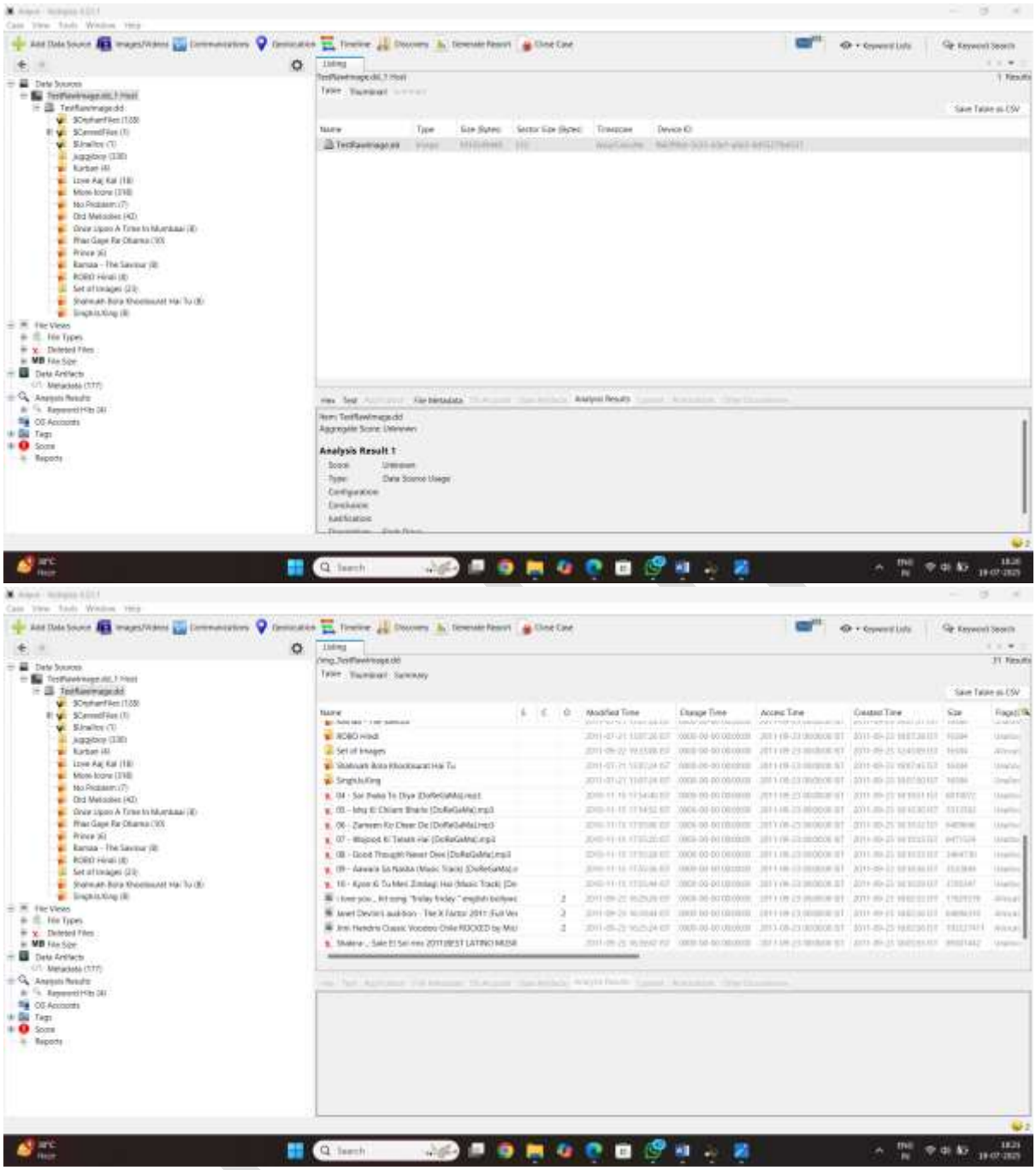
Click on the next

Step11: add data source

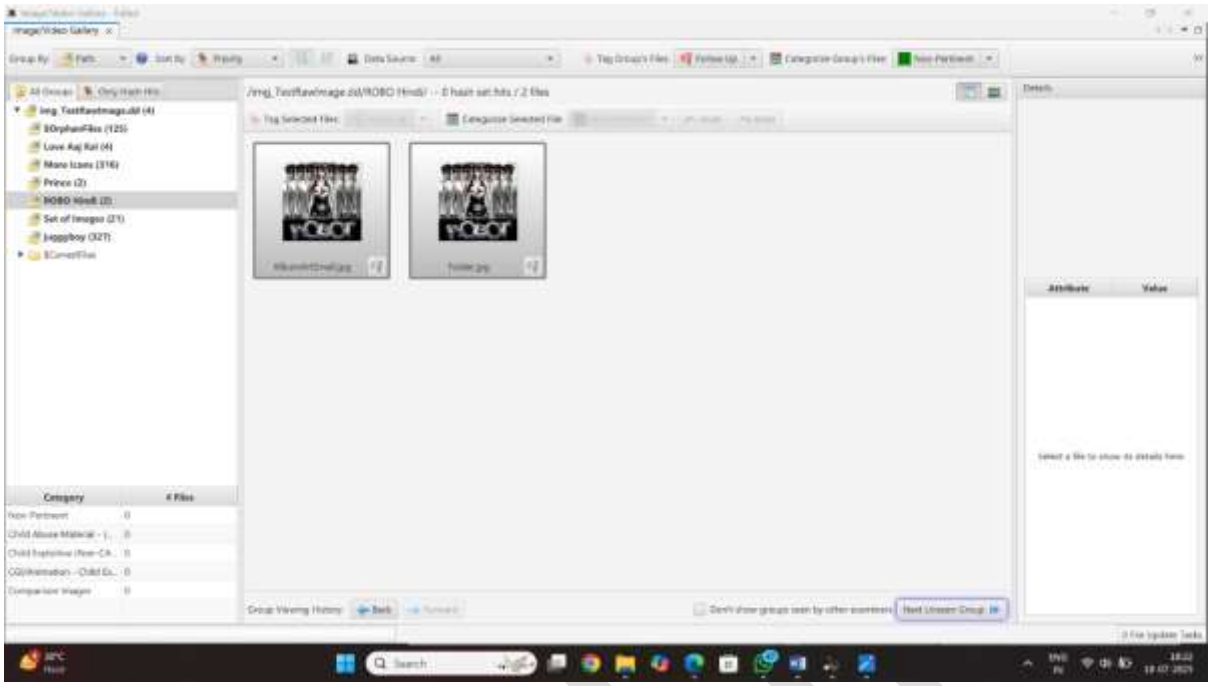


Click on the next

Anaylze the image of content



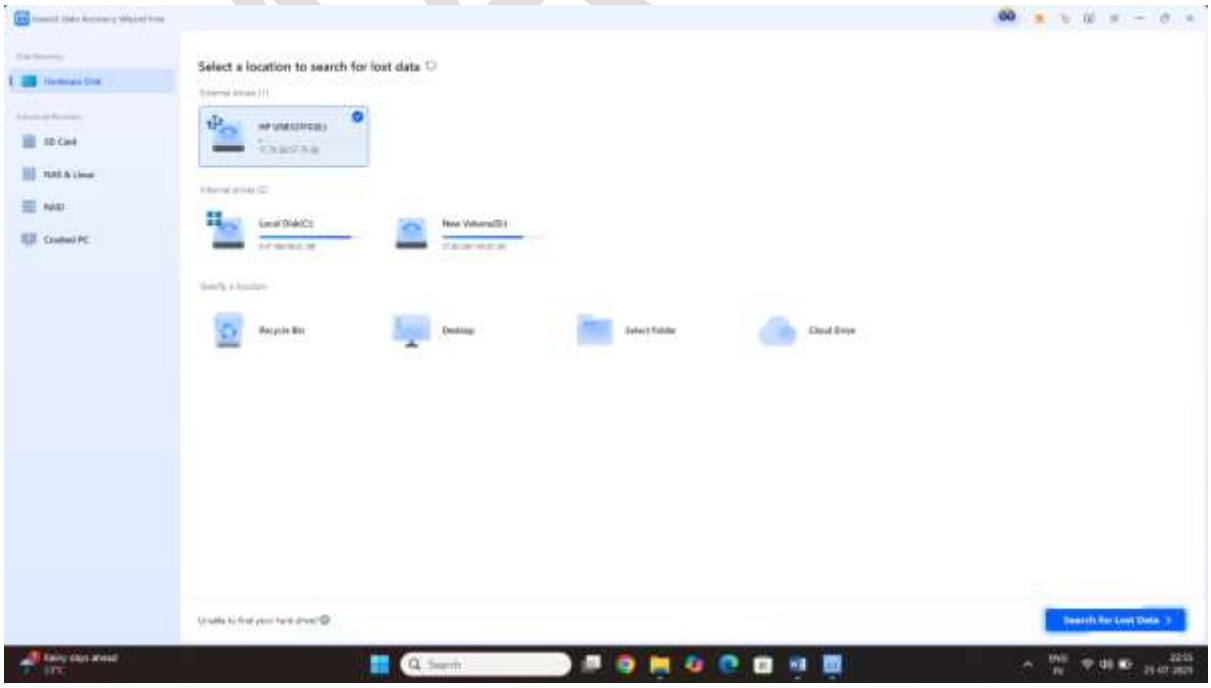
Step12 click on the image/videos option they vezible of image of folder



Lab3 recover data form deleted Disk partition

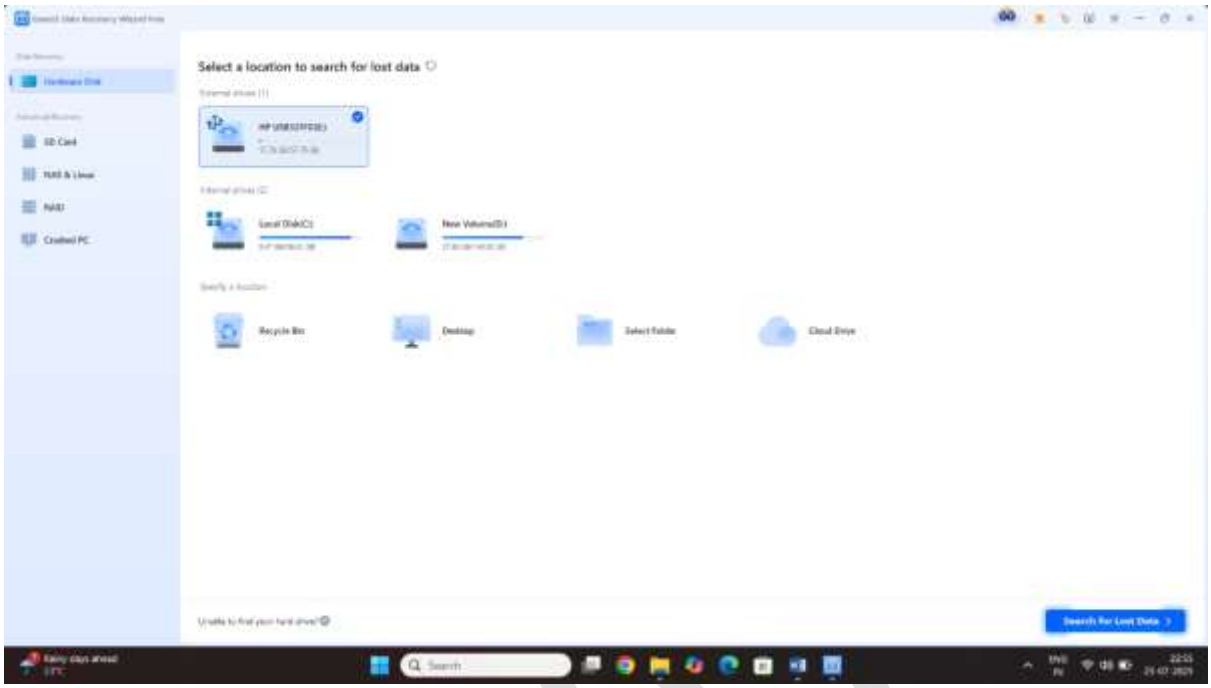
There was tool called ease us data recovery

Step1 start the data recovery tool

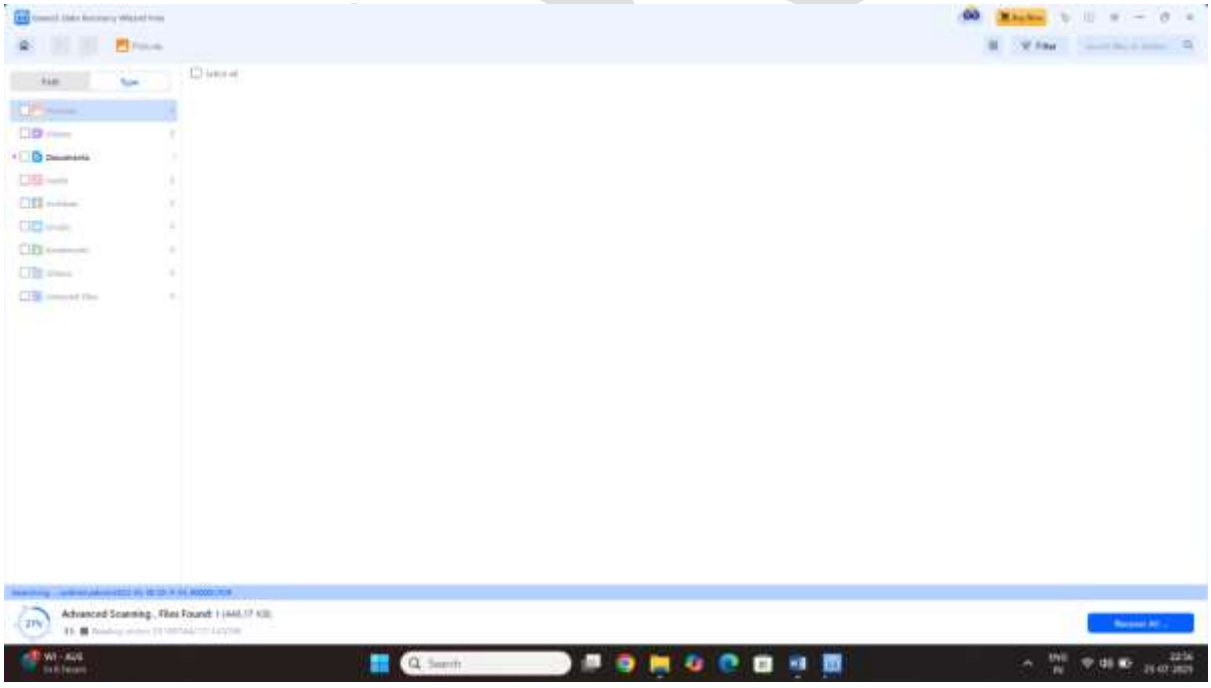


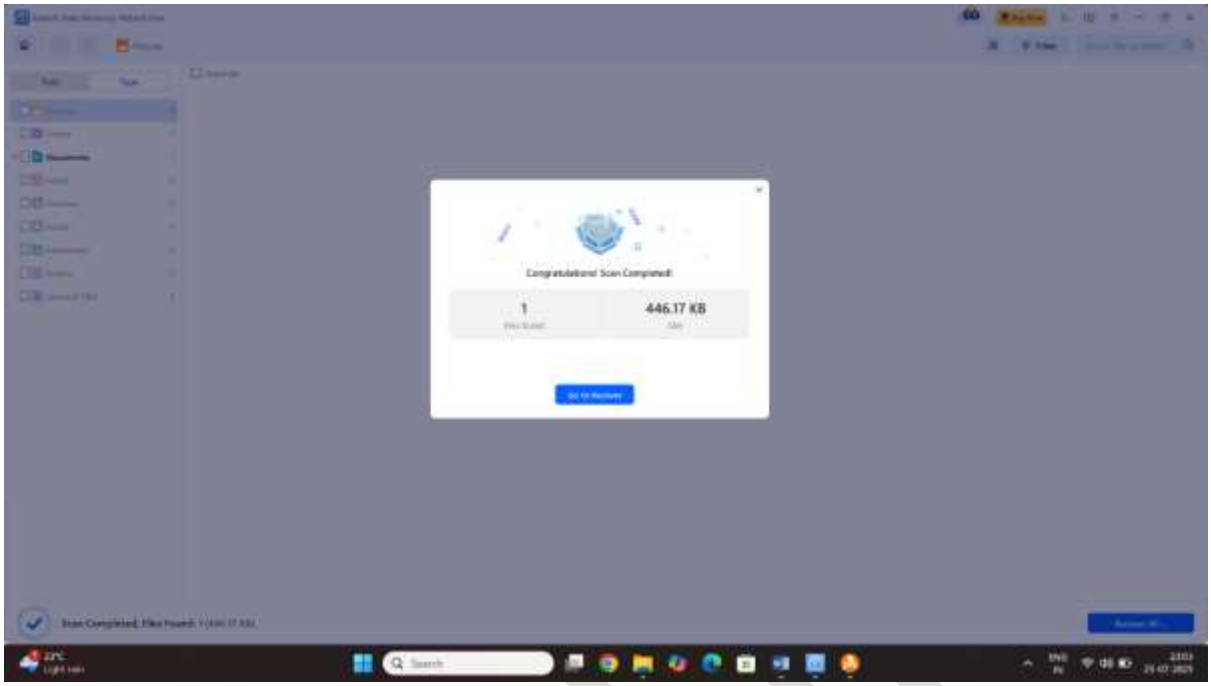
Step2 select the ease lost partition

Step3 click on search for lost data

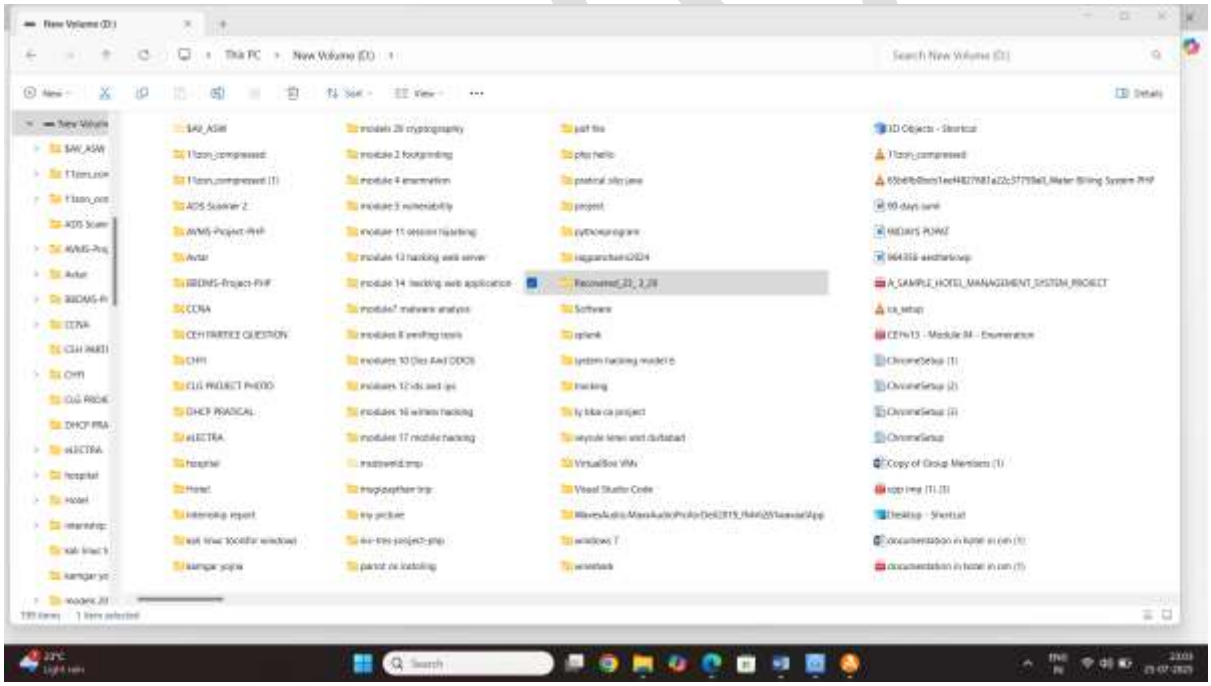


Step4 start the data recovery process

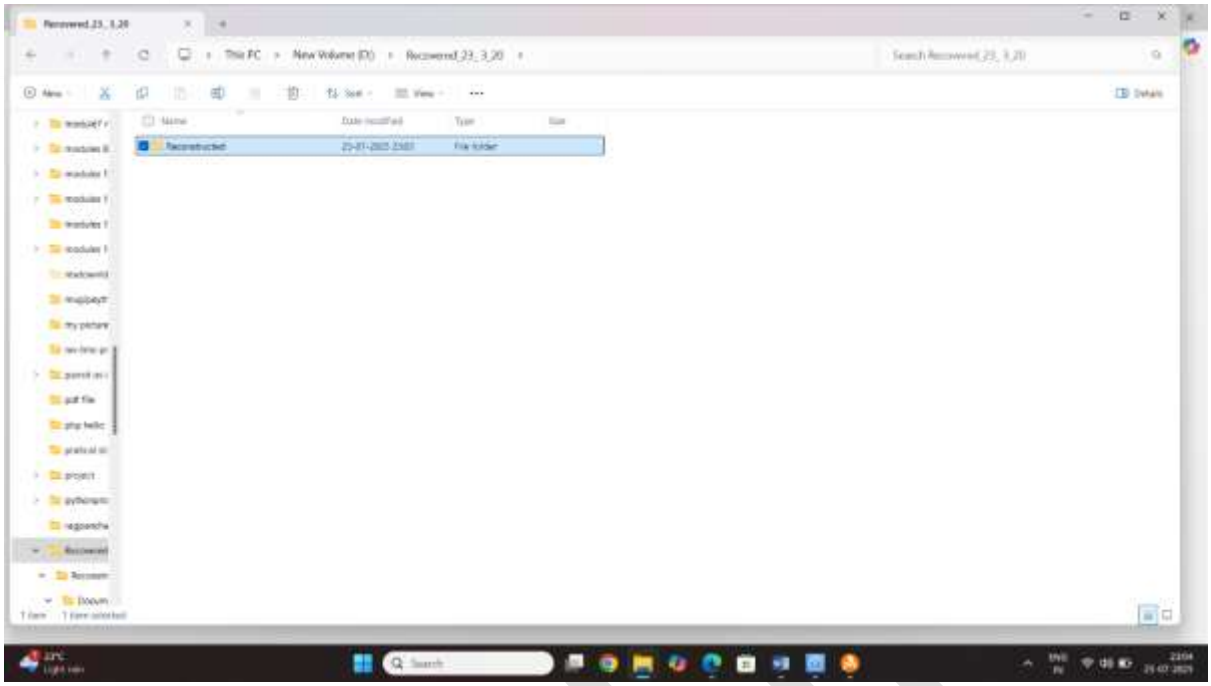




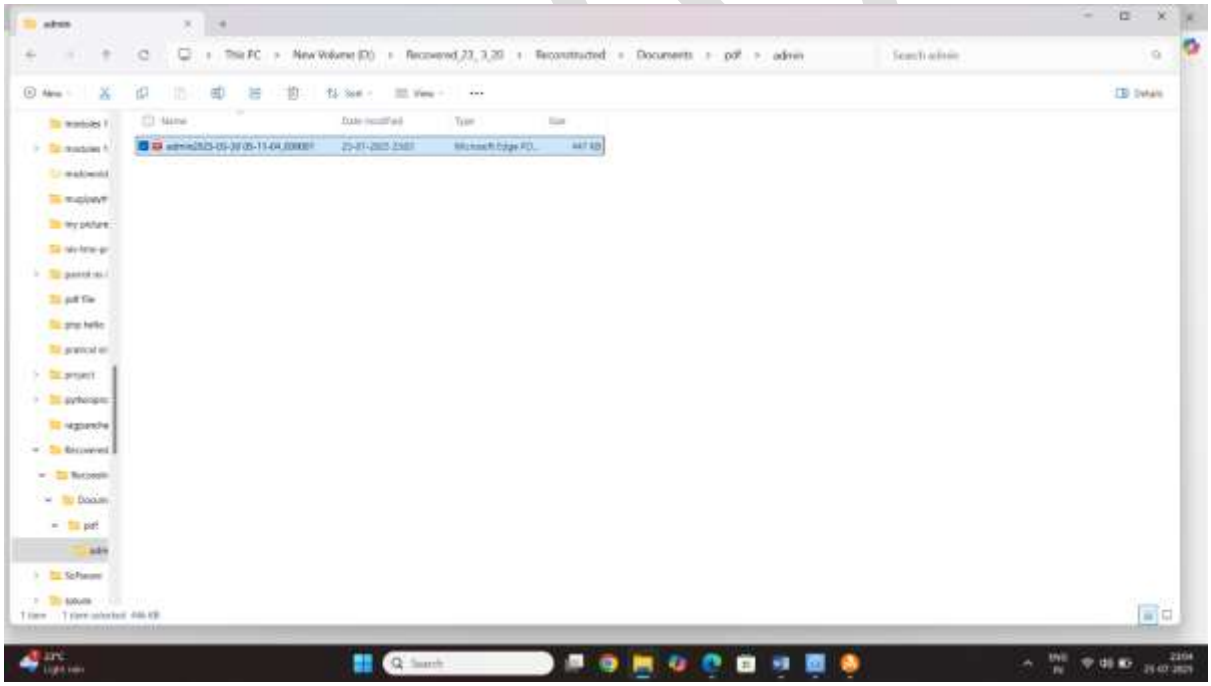
Click the go to recover option



store the recovery data in folder



Result:

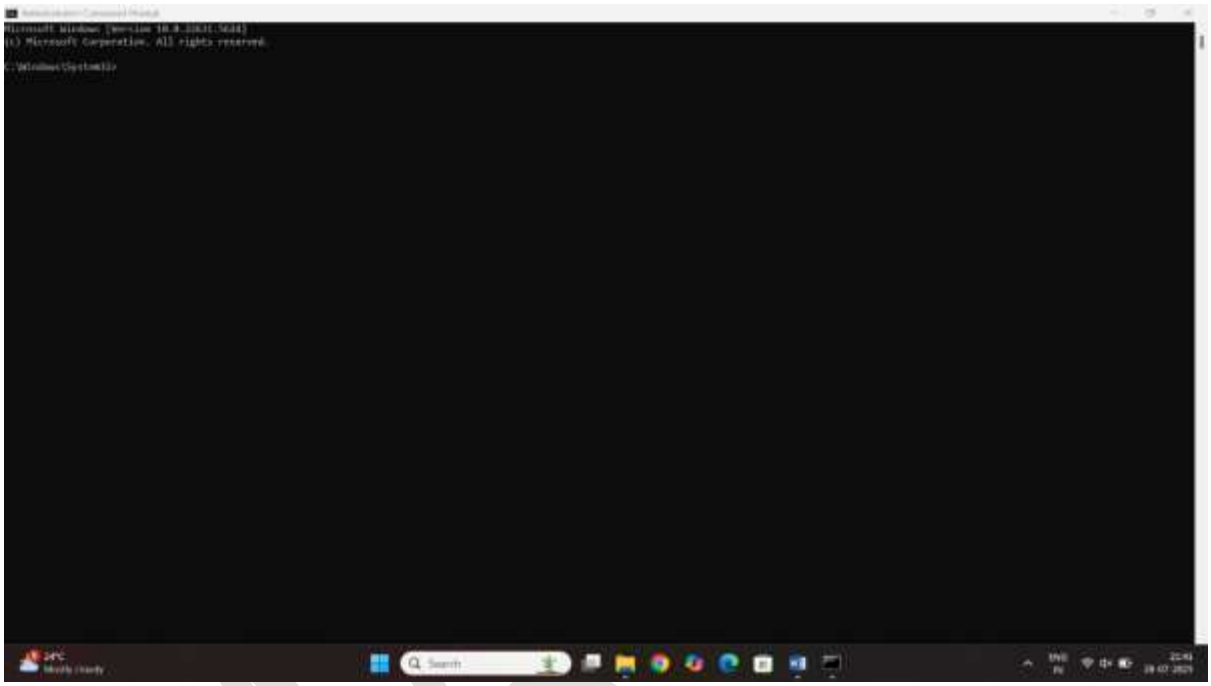


Lab4 hash captering the windows system

Using pwdump7

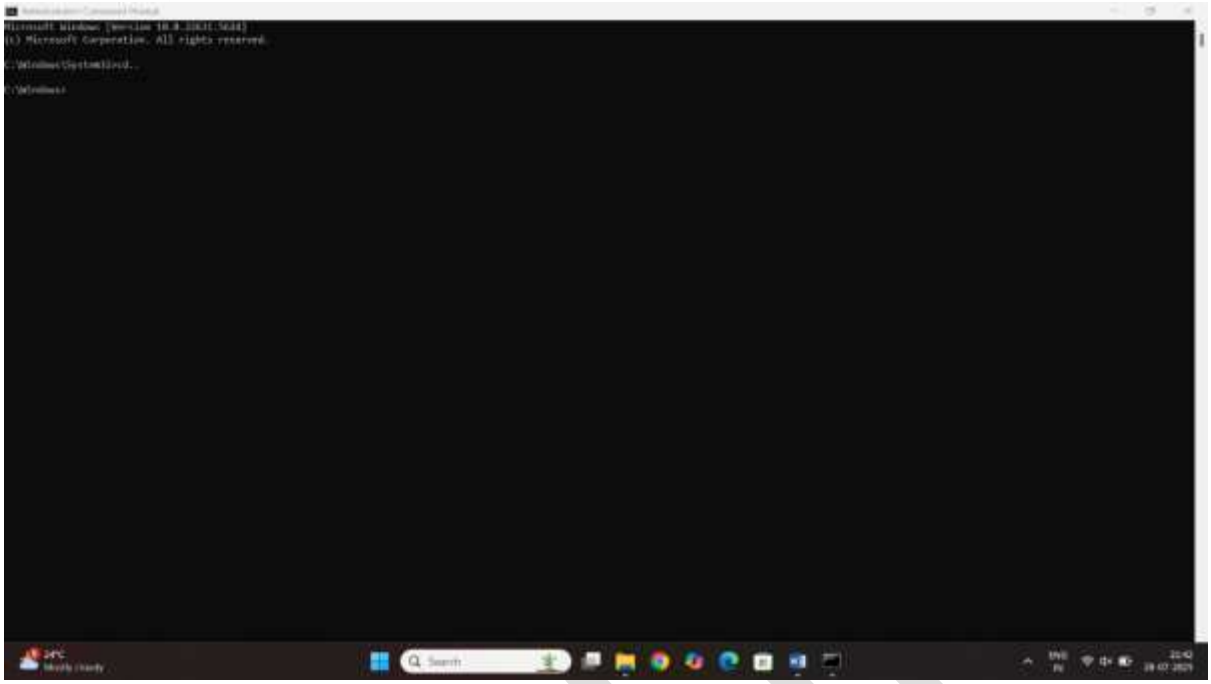
Step1 download the pwdump7

Step2 go to cmd and run as administrative

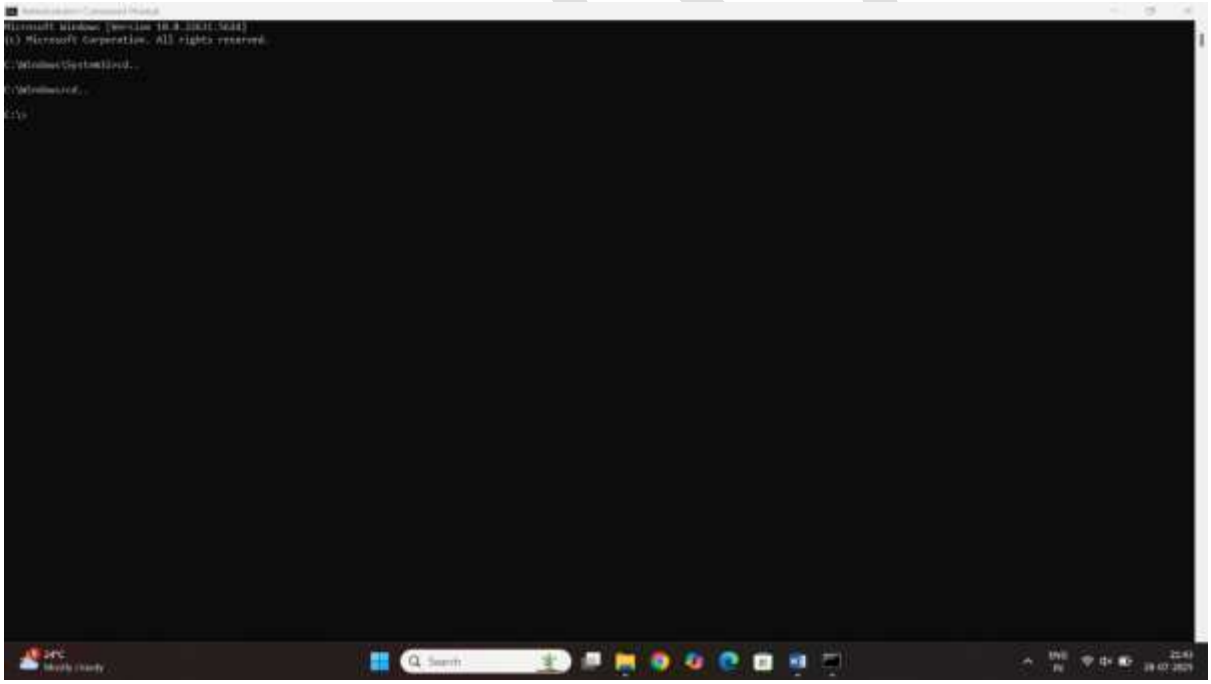


Step3 go to c: drive

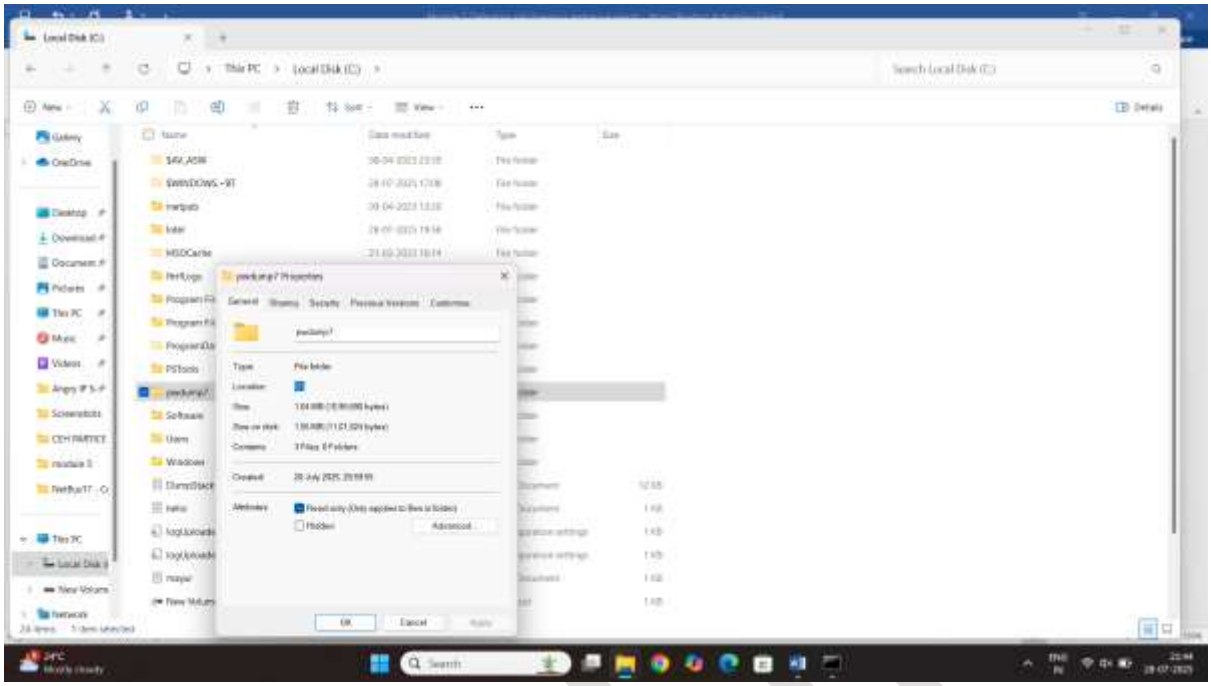
Command: cd..



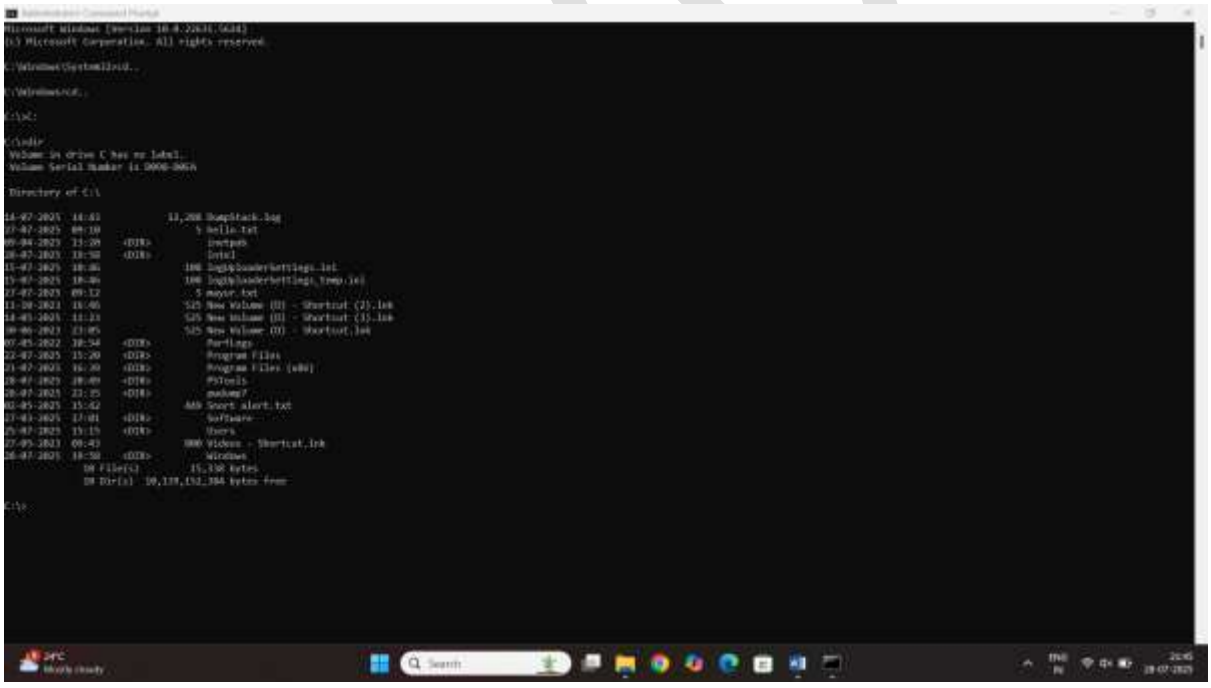
cd..



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



Step5 type the path in cmd

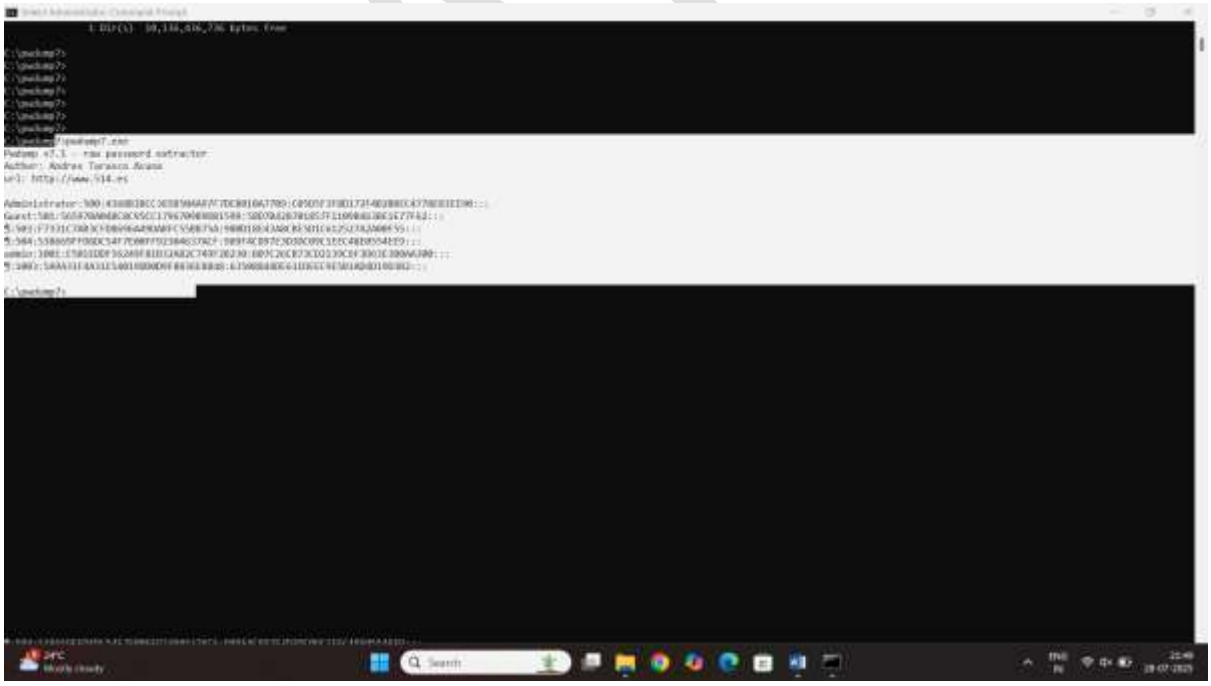


Step6 go to pwdump tool

Step7 type the command

Pwdump7.exe

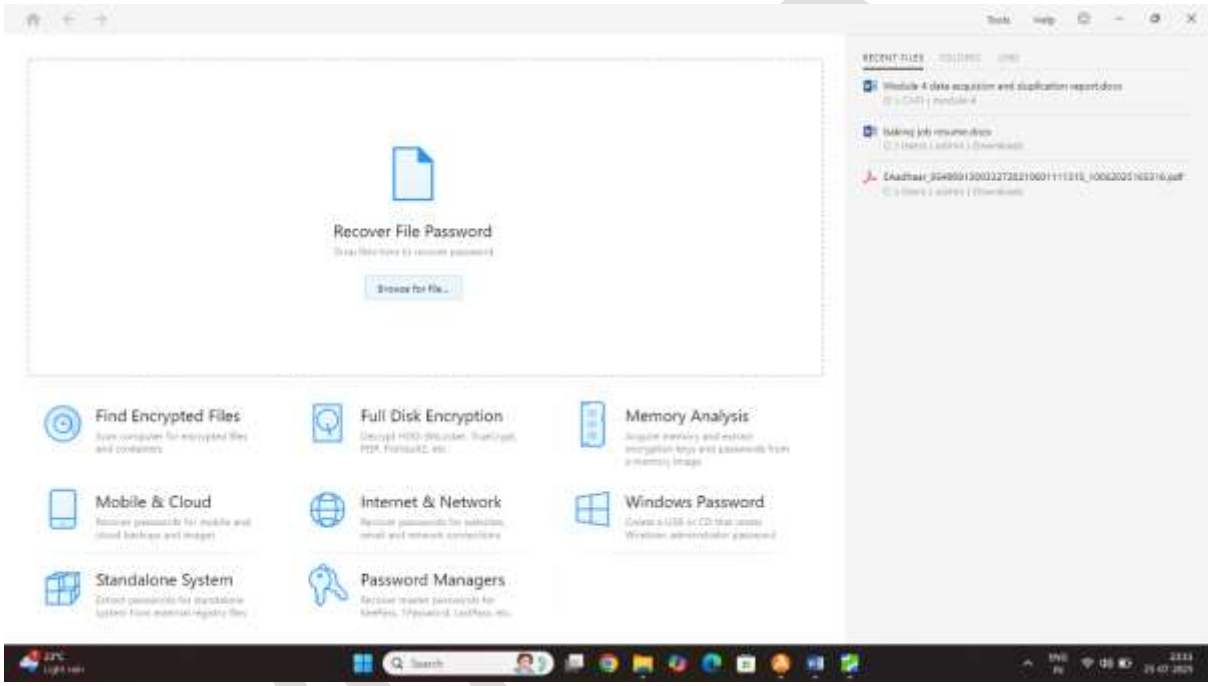
Result:



Lab5 cark application password

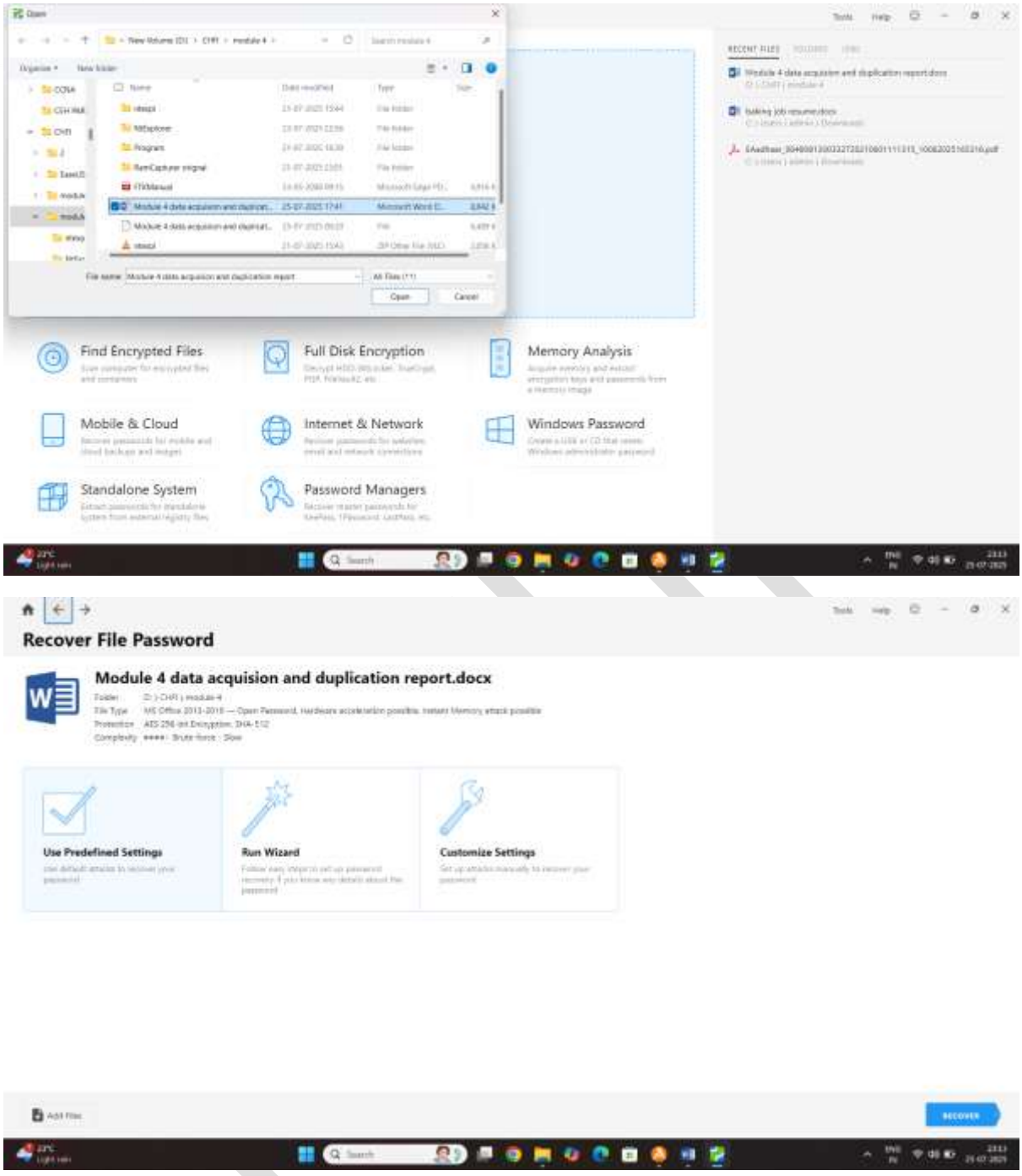
There was tool called password forensic tool kit

Step1 start the application



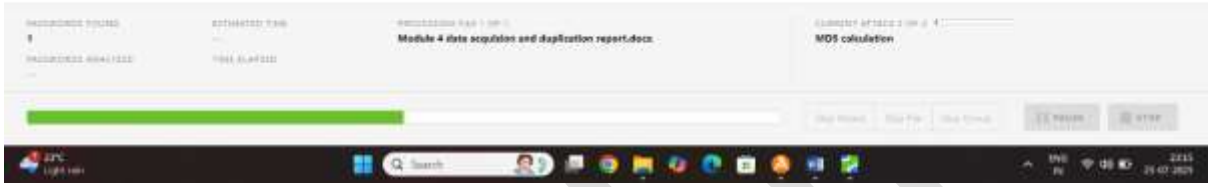
Step2 click on the browse option

Select the crack the password file



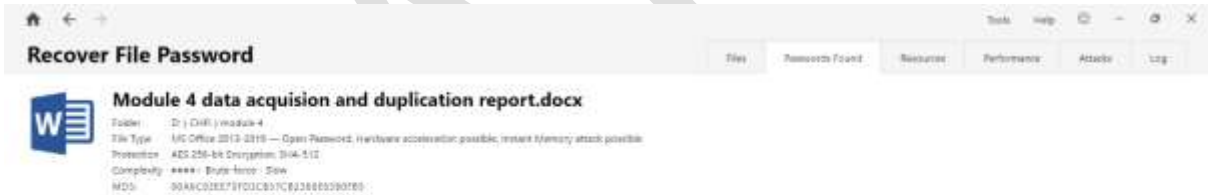
Step3 click on predefined setting option

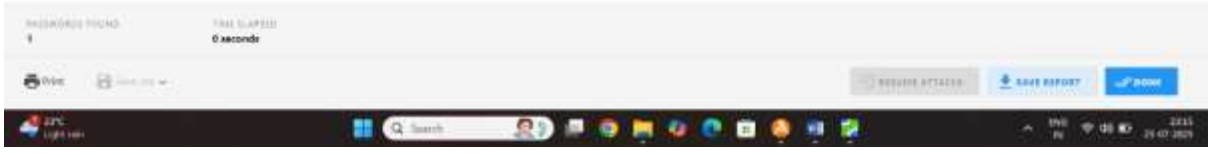
Click on the recover



Result:

crack the successful password of word file

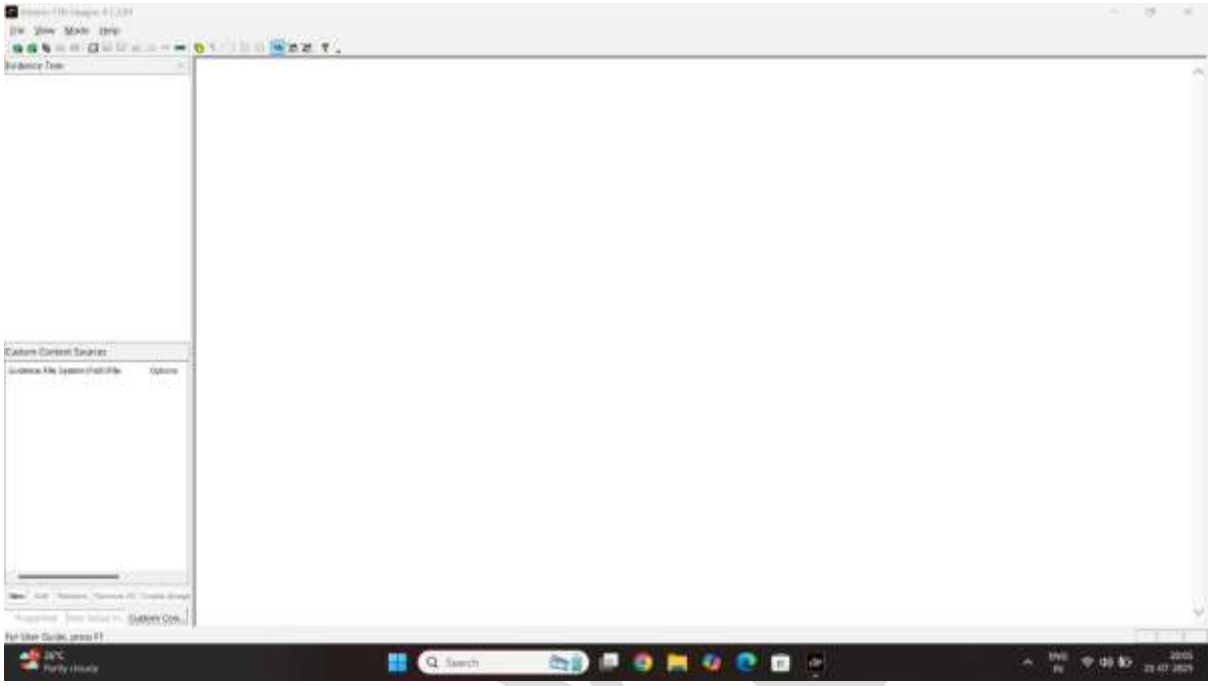




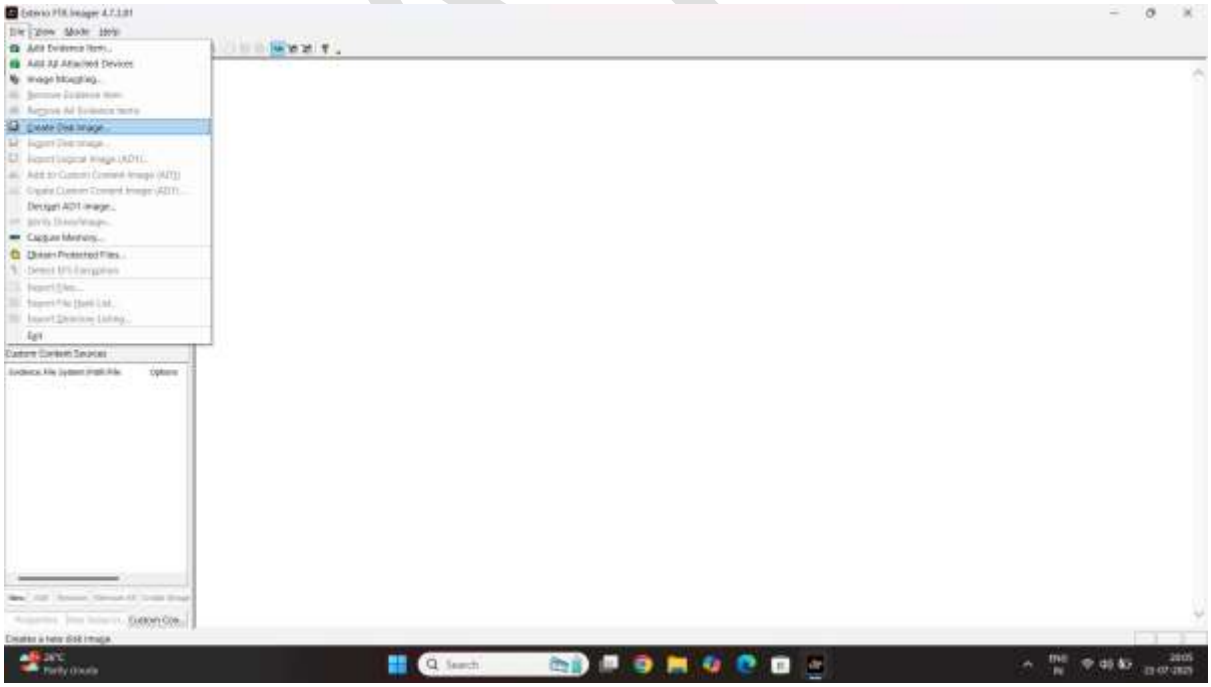
Lab6 create disk image file a hard disk partition

Using ftk

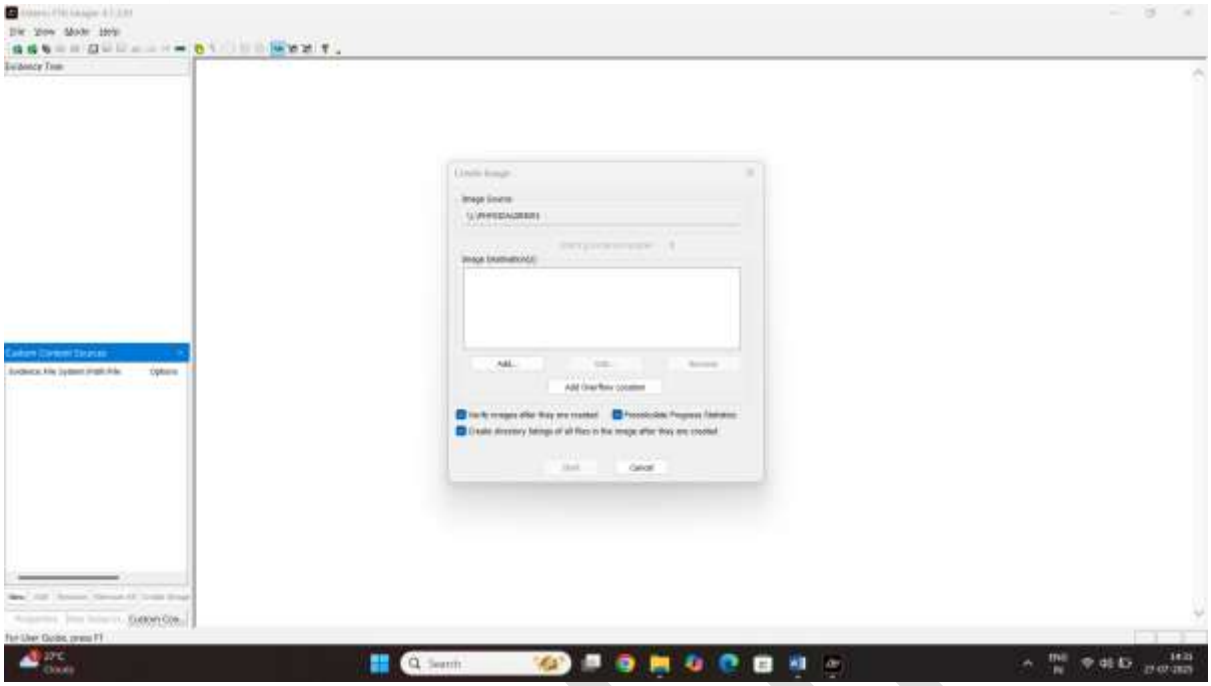
Step1 start the ftk application



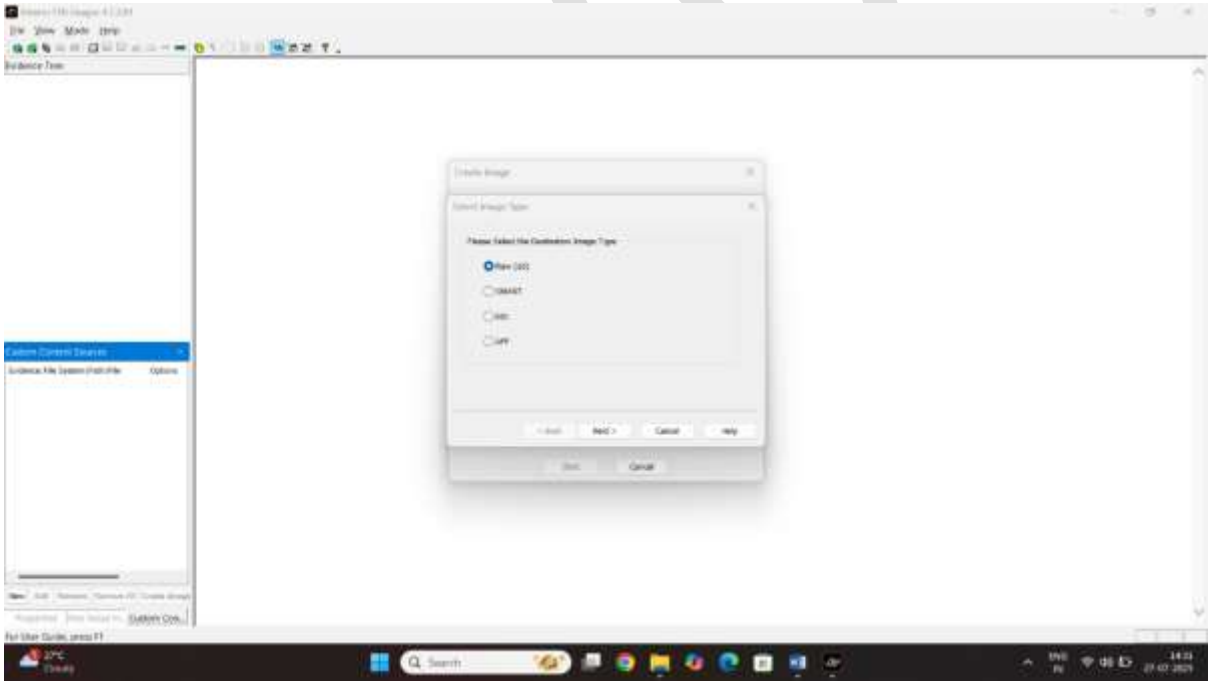
Step2: click on the file option



Step3 select the add option

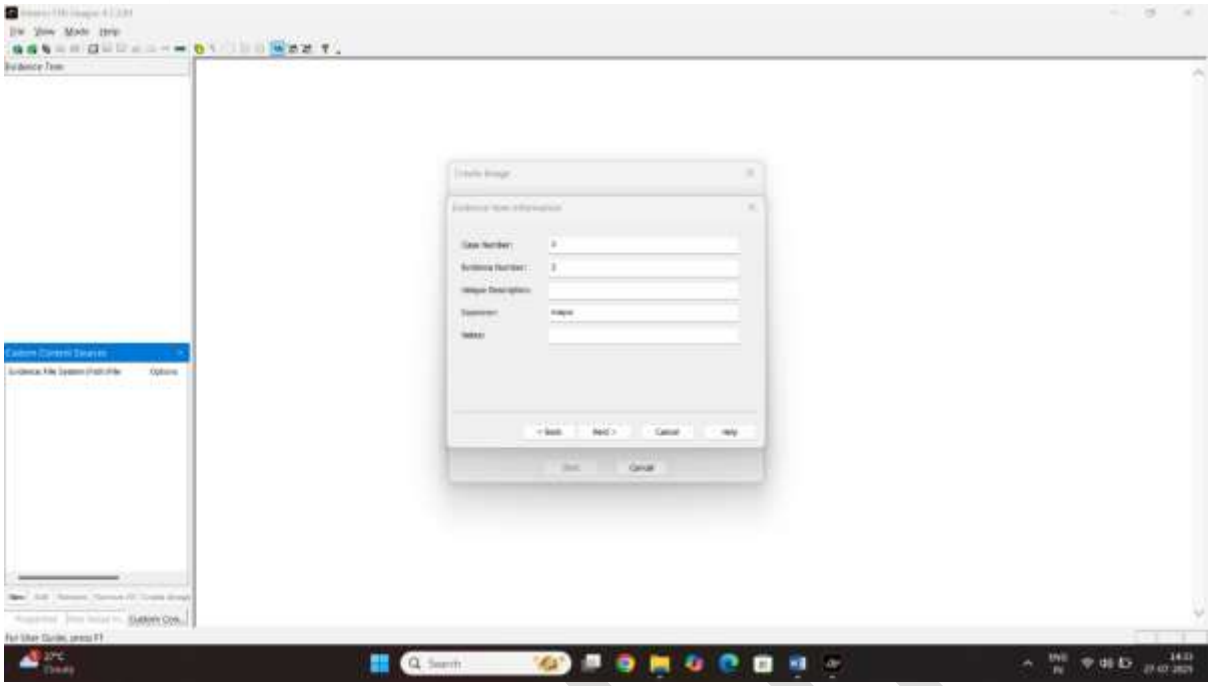


Step4 select the file extinction raw

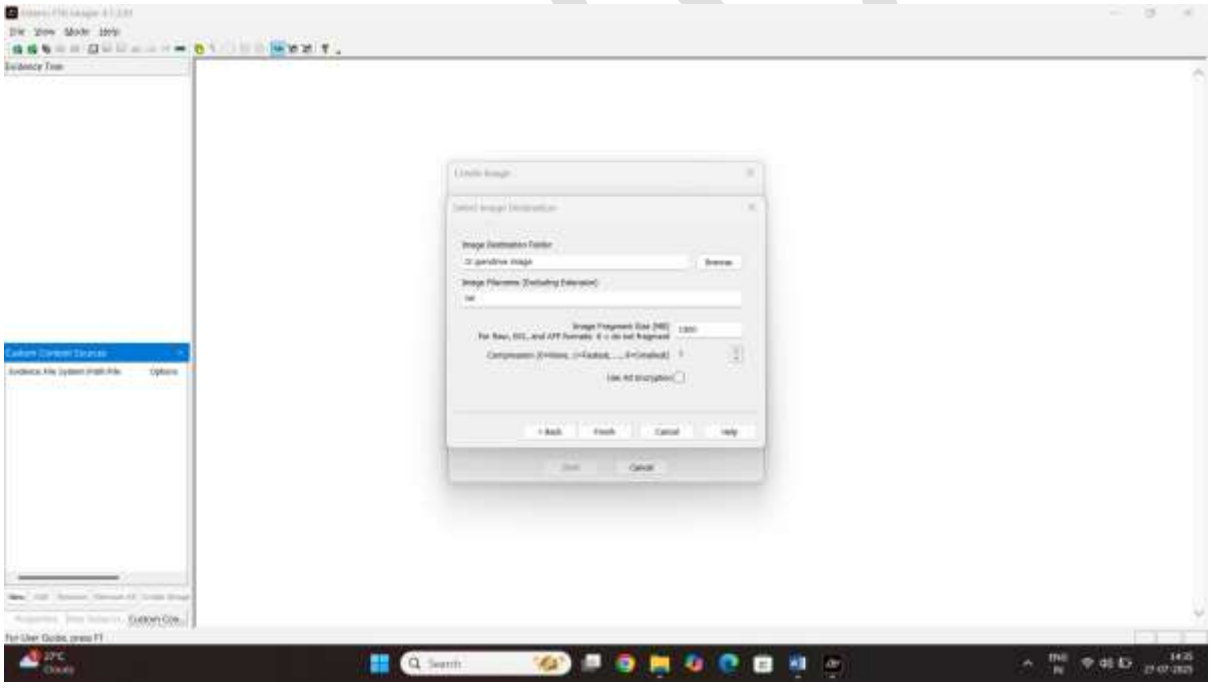


Click on the next

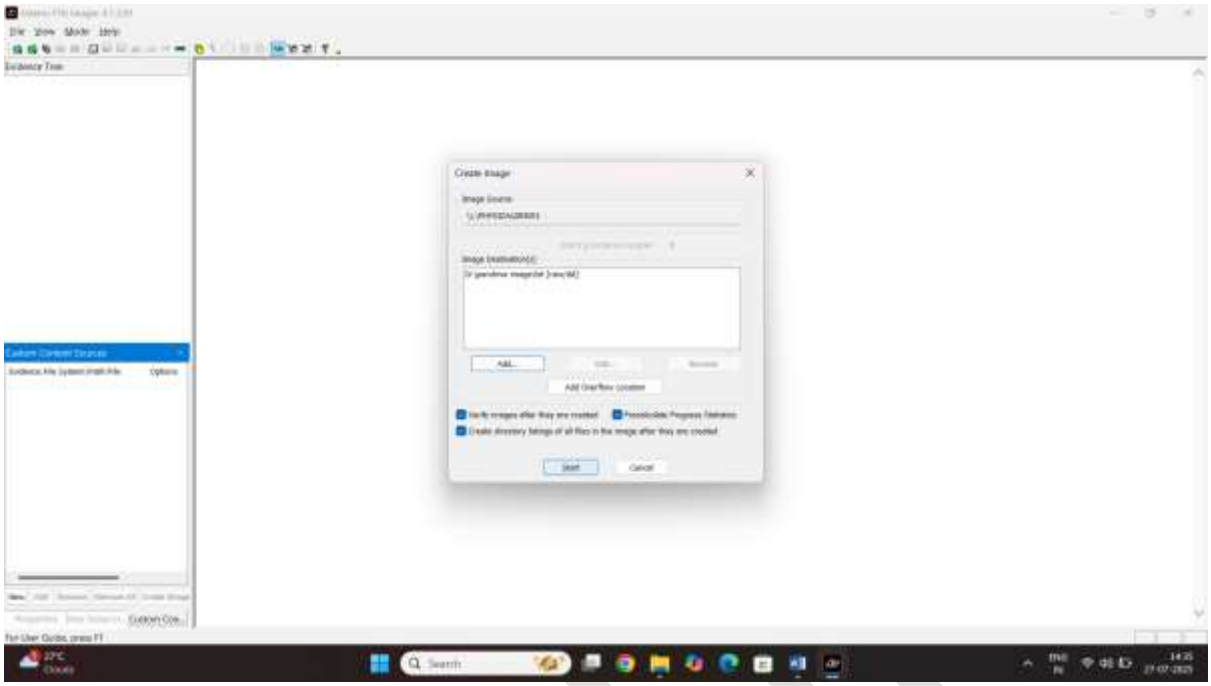
Step5 enter the causes details



Step6 select the image destination folder

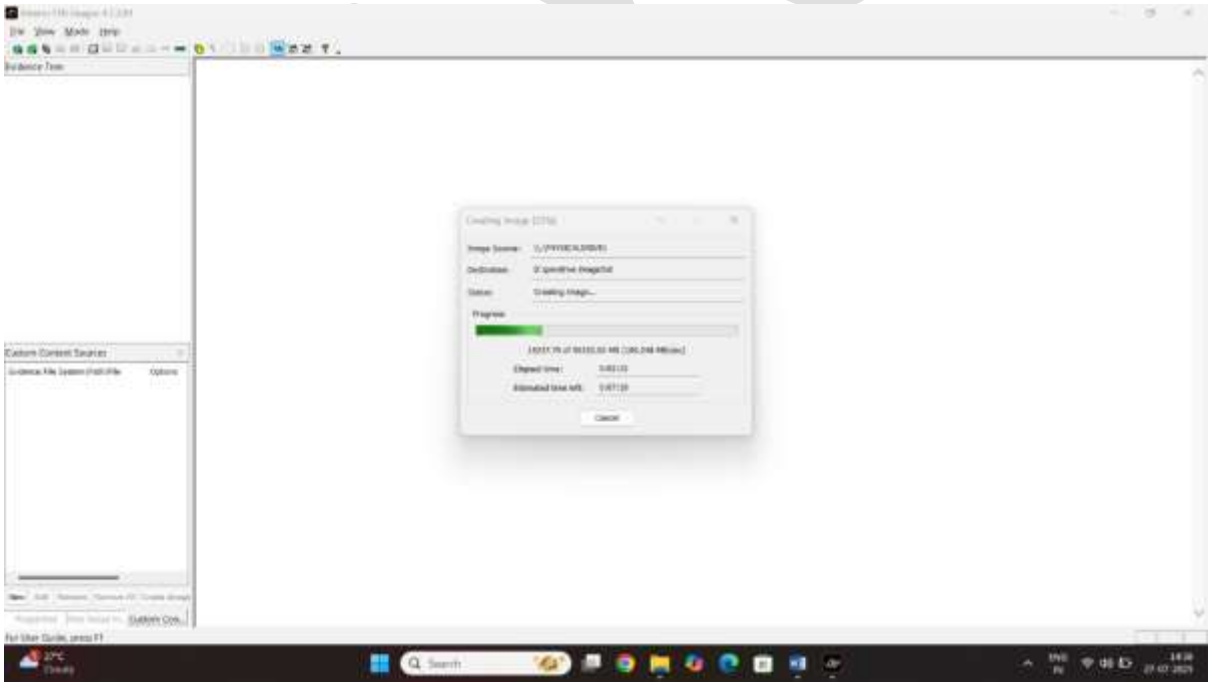


Click on the next

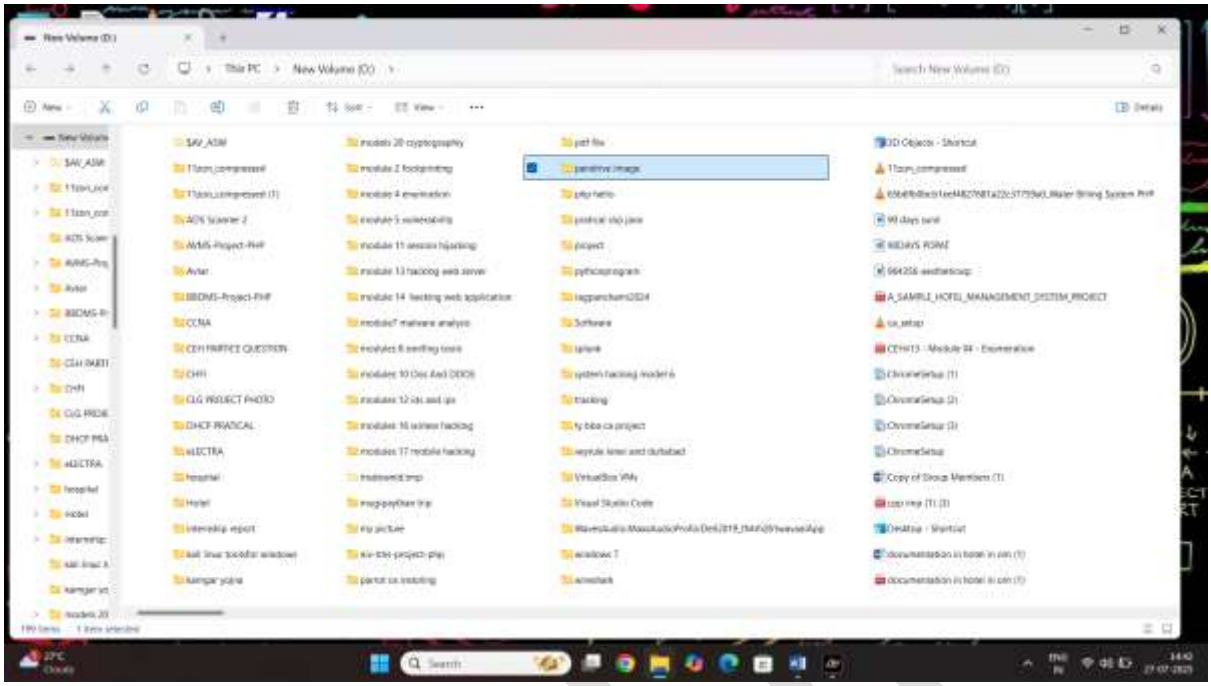


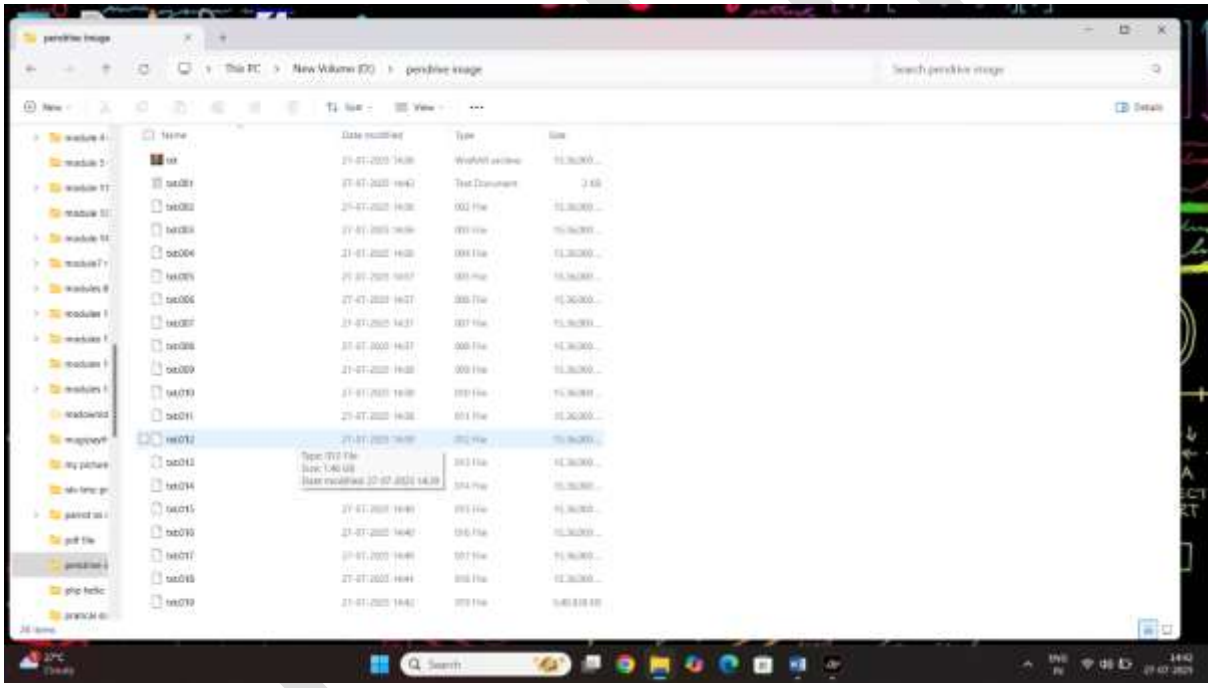
Step7 Click on the start option

Step8 creating image process on



Result:

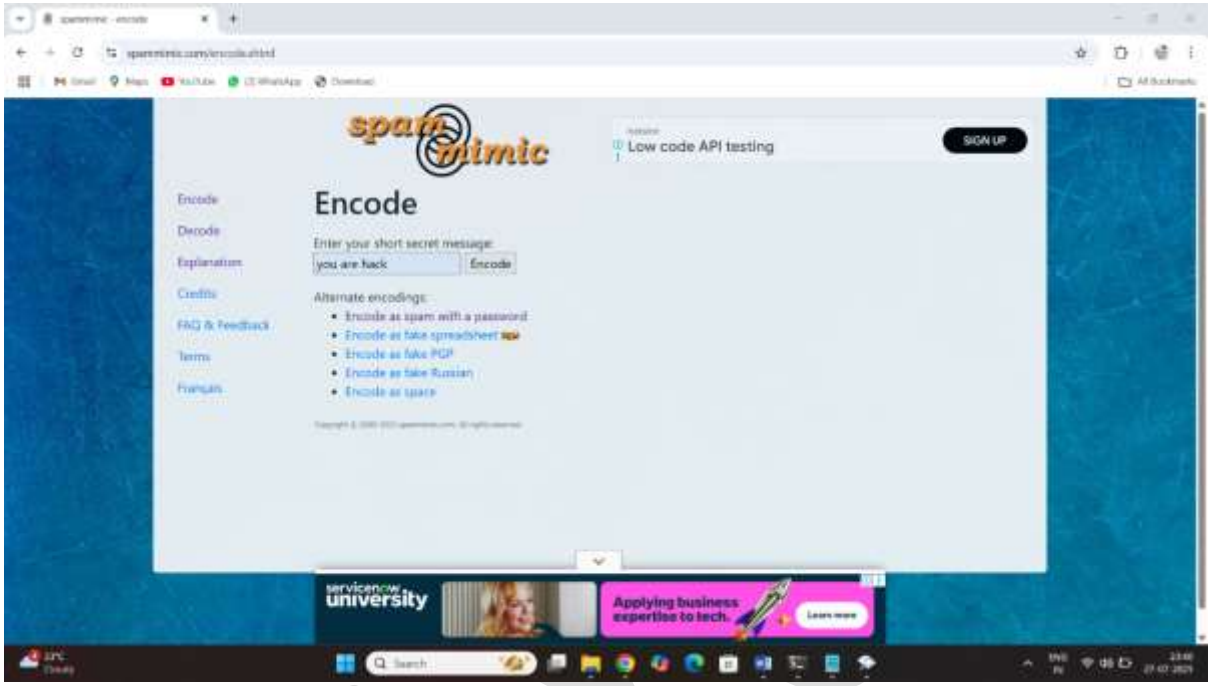




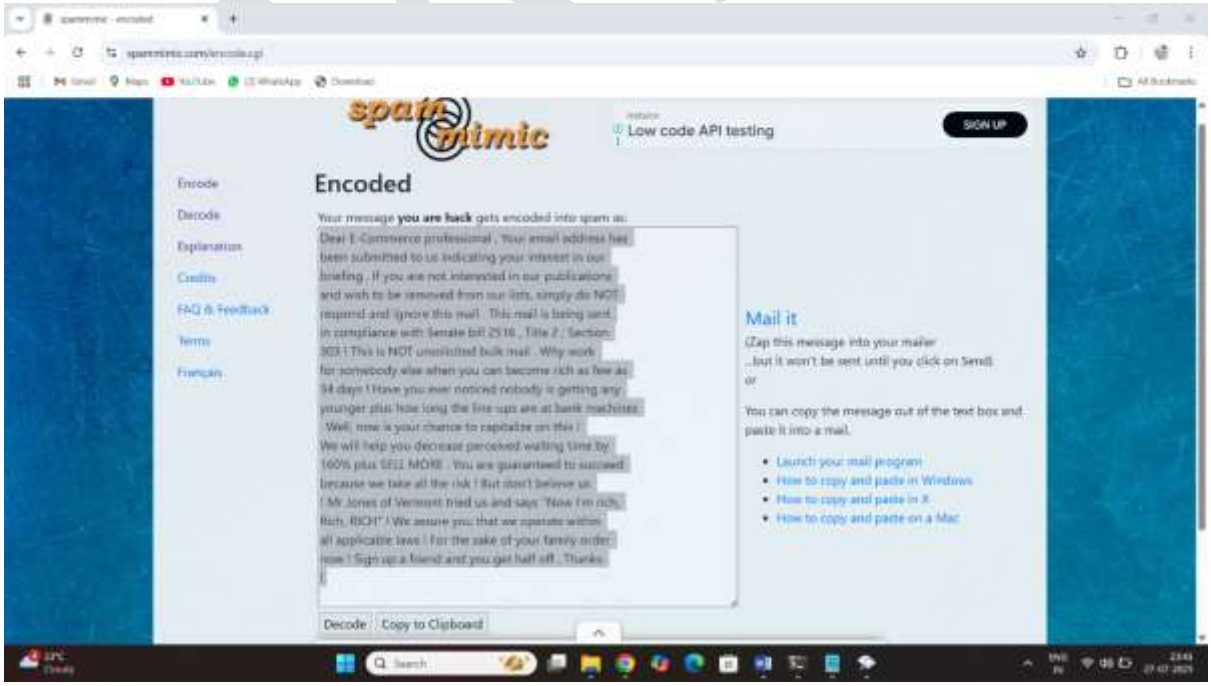
Lab 7 how to detect stegnographic usimg spam mimic web site

Step1: click on the website open the website

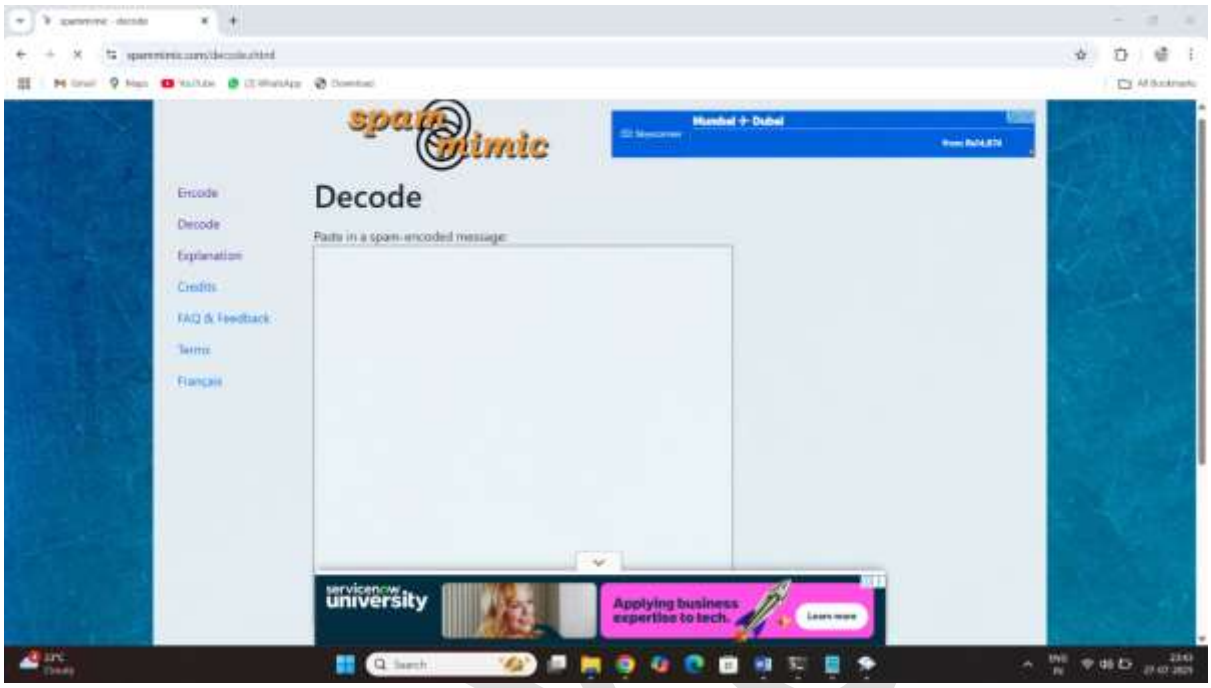
Step2: click the encode and type the text



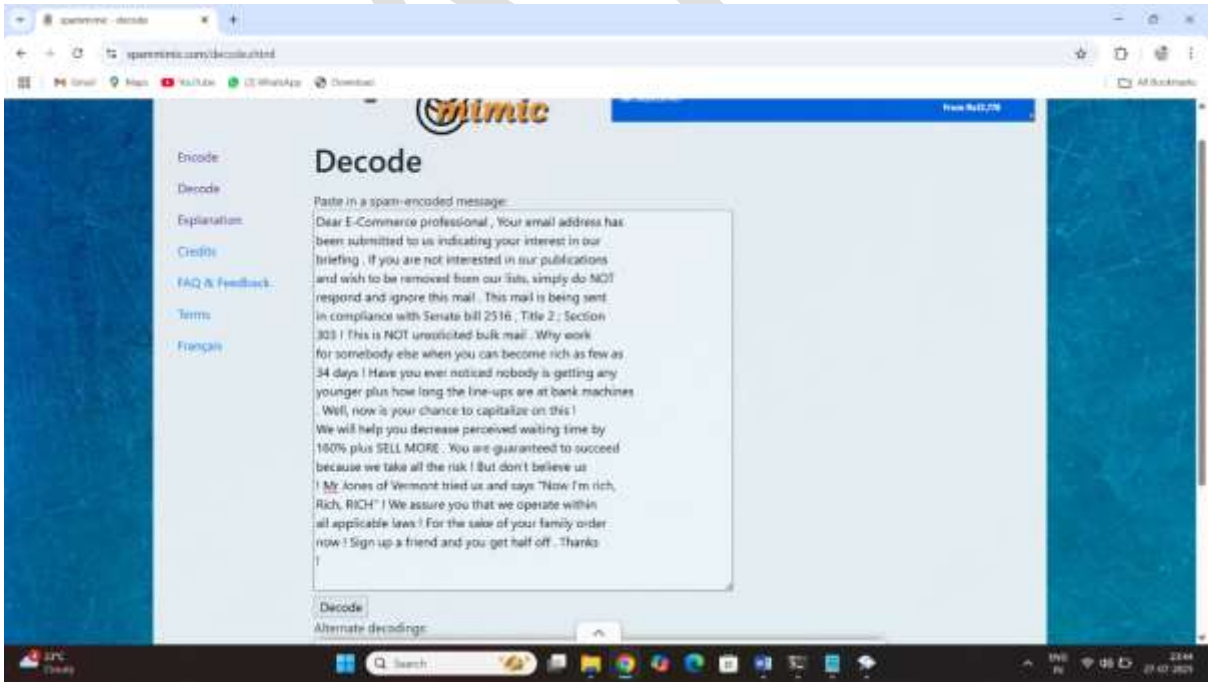
Step3: type the code and copy the code



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

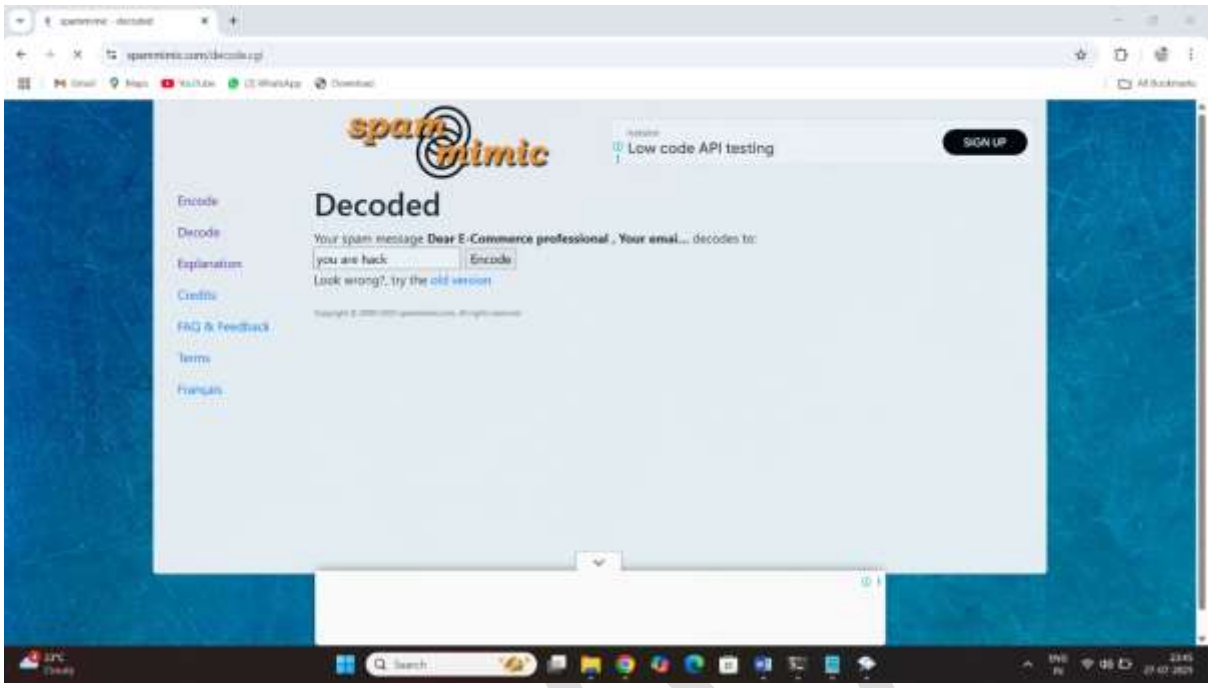


Step5 paste the code



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.

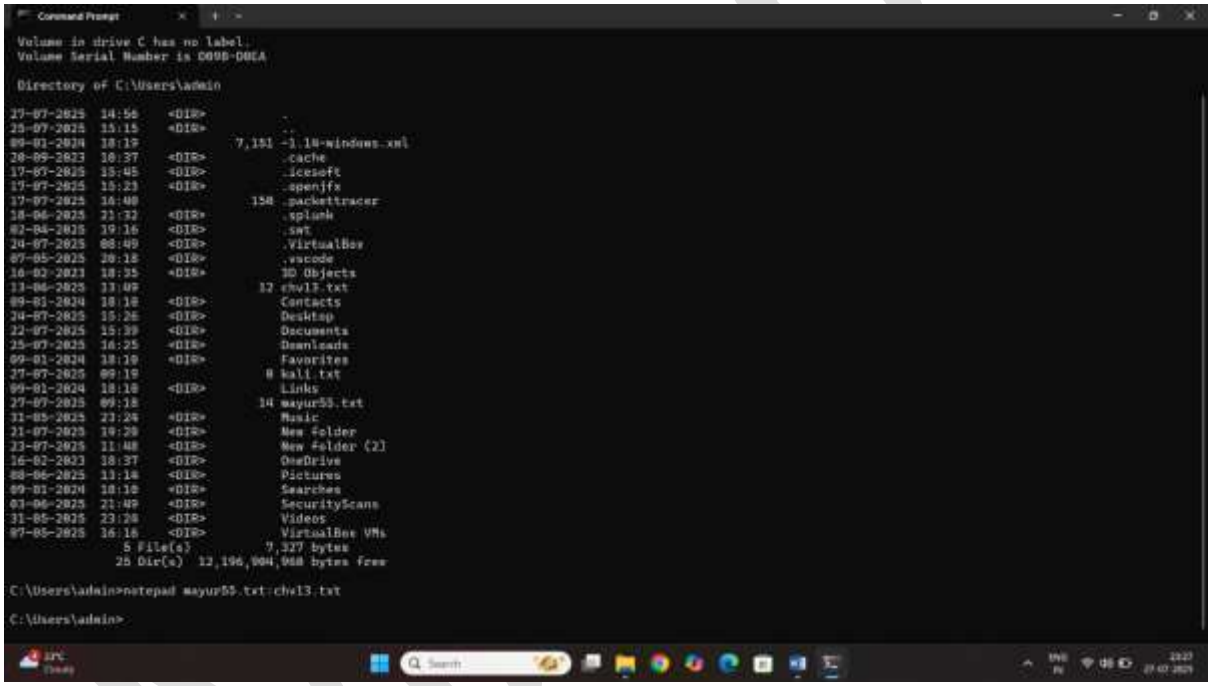
Instead of waiting for all the data to be collected (like downloading a file), you process it **on the fly**—as it comes in.

Step1: click on note pad Create the txt file

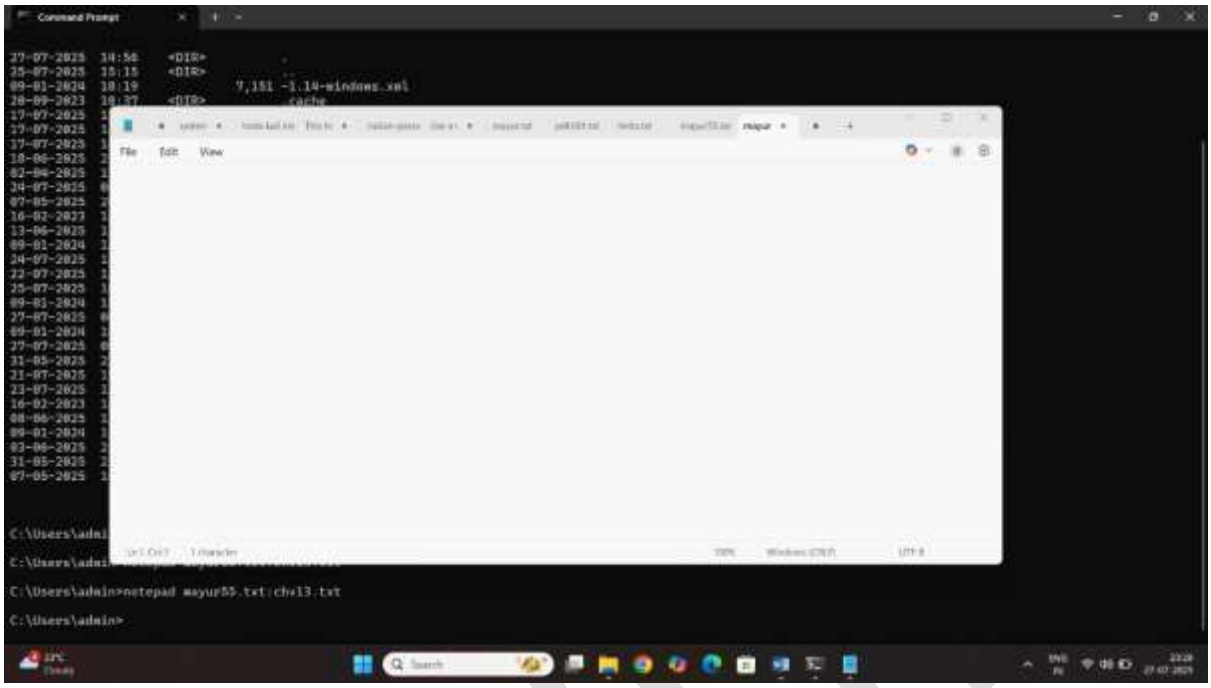
Example mayur45.txt/Create the file

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

Step3:type the file// notepad mayur45.chv13

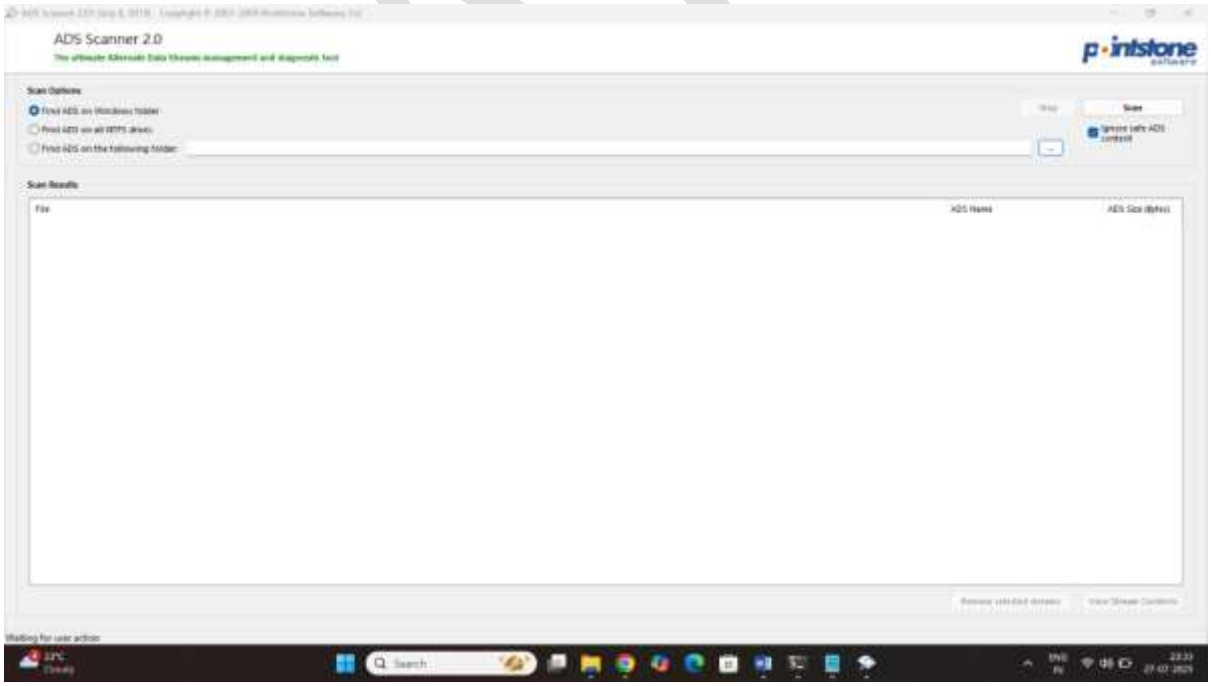


Result:

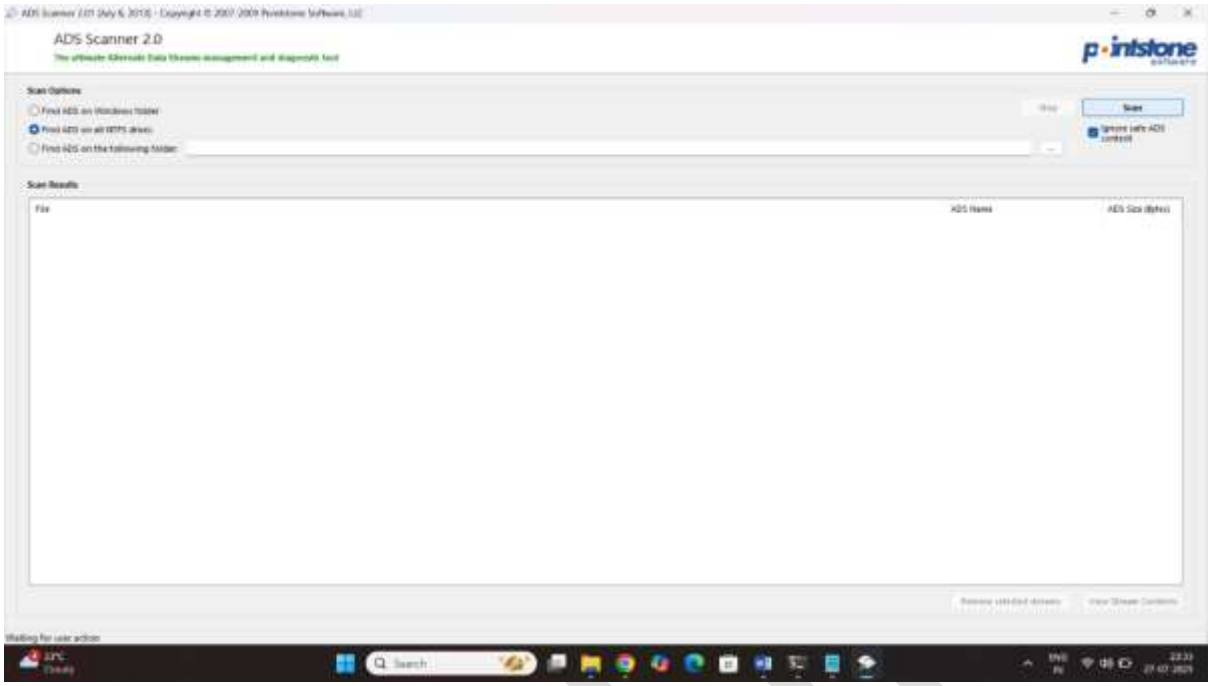


Lab 9How to find hide file in system using Ads scanner

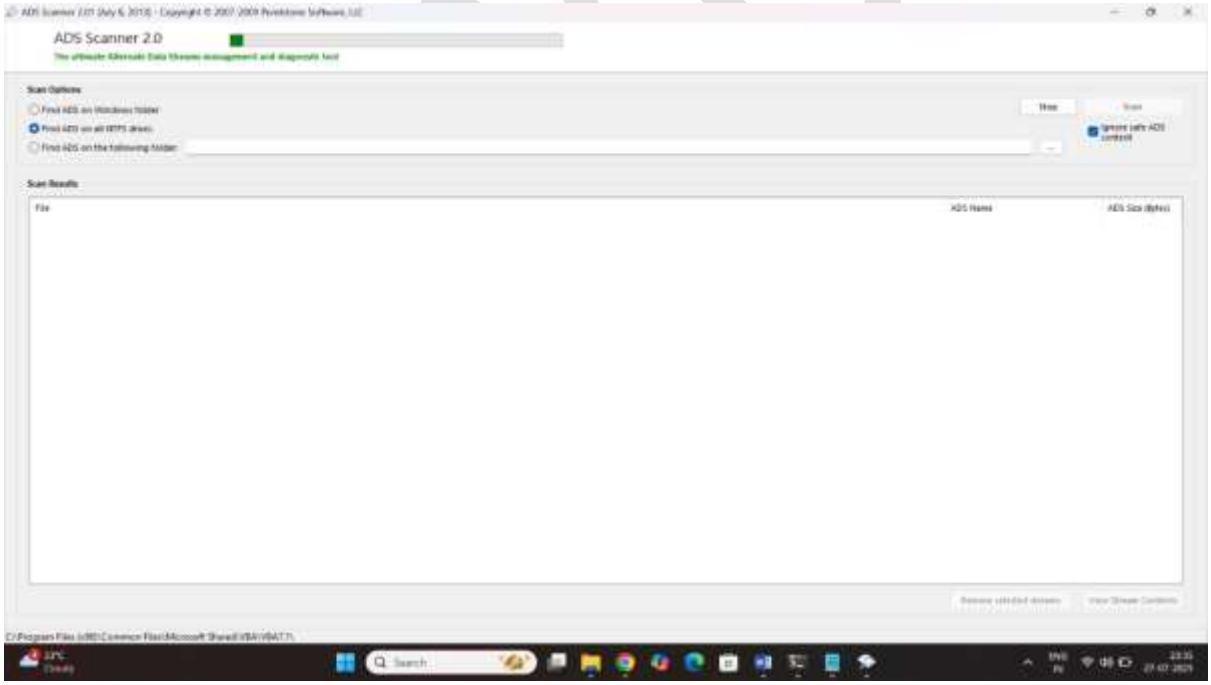
Step1 start the application



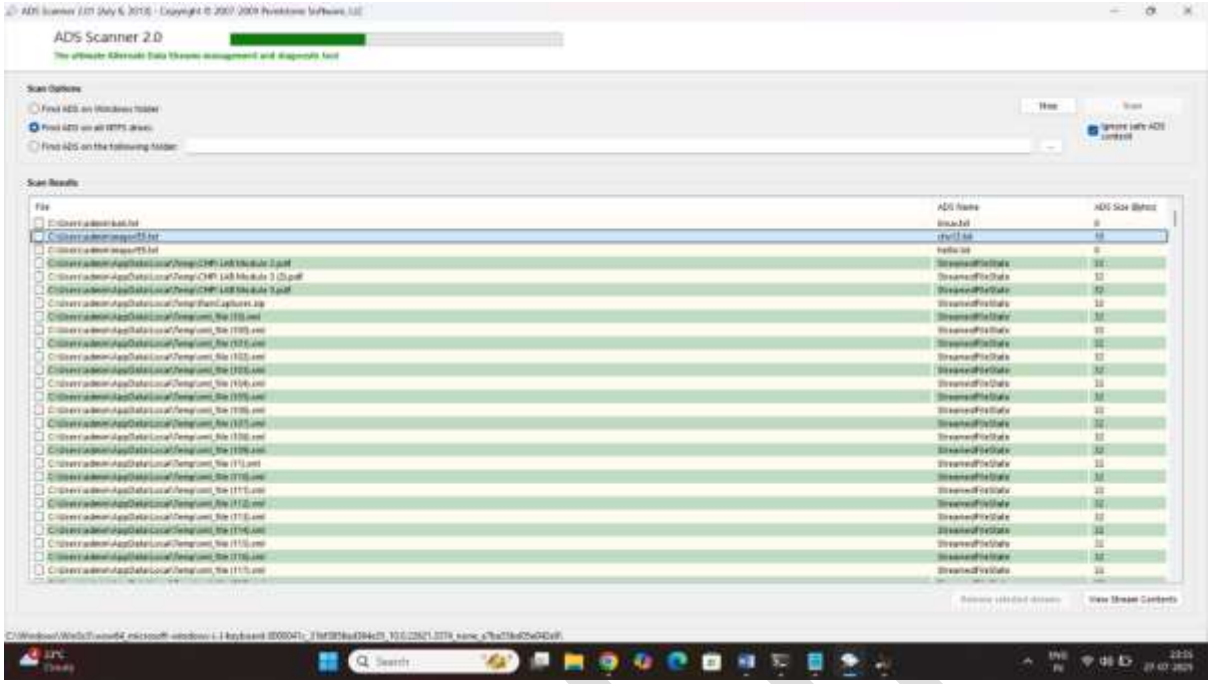
Step2 choice the any option click on the scan



Step3 active the scanning process

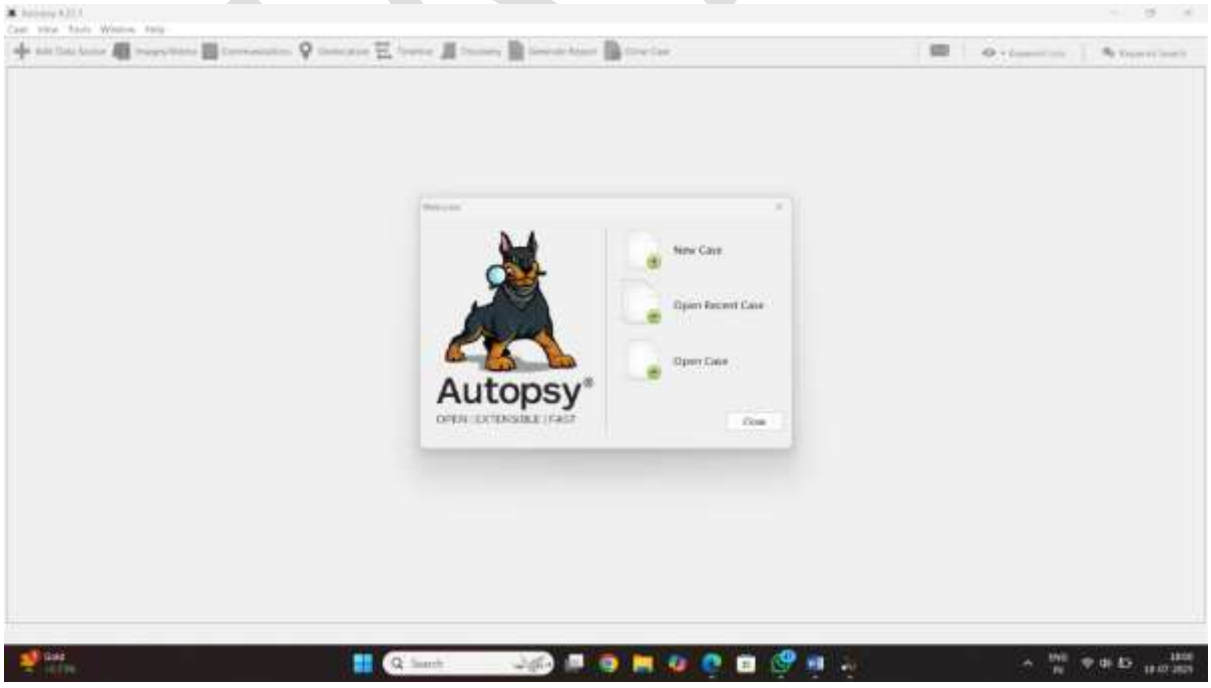


Result:



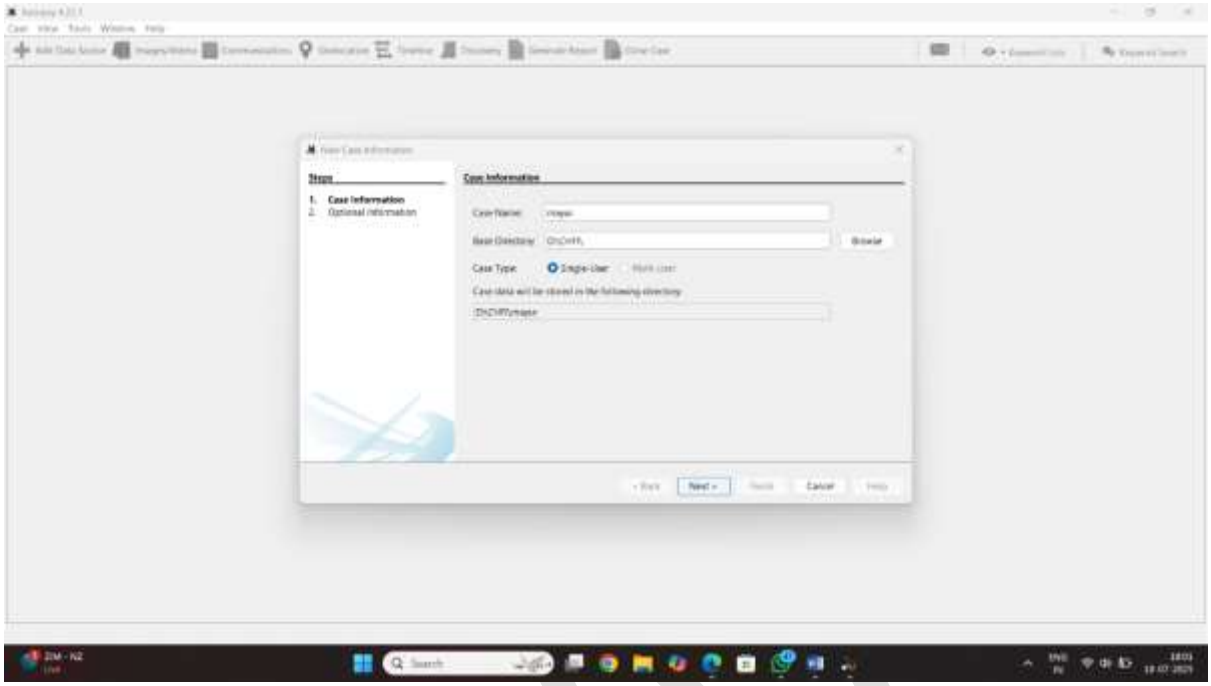
Lab 10 detect file extension mismatch using autopsy

Step2: start the autopsy and click on the new cause

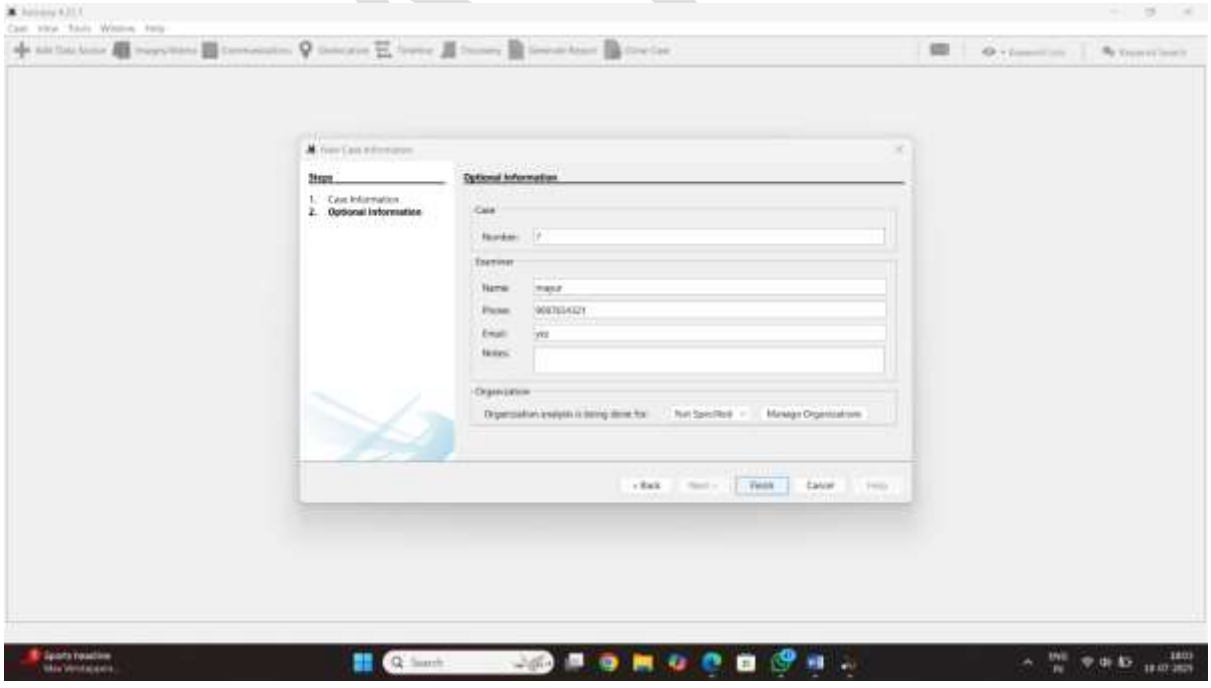


Step3: enter case name

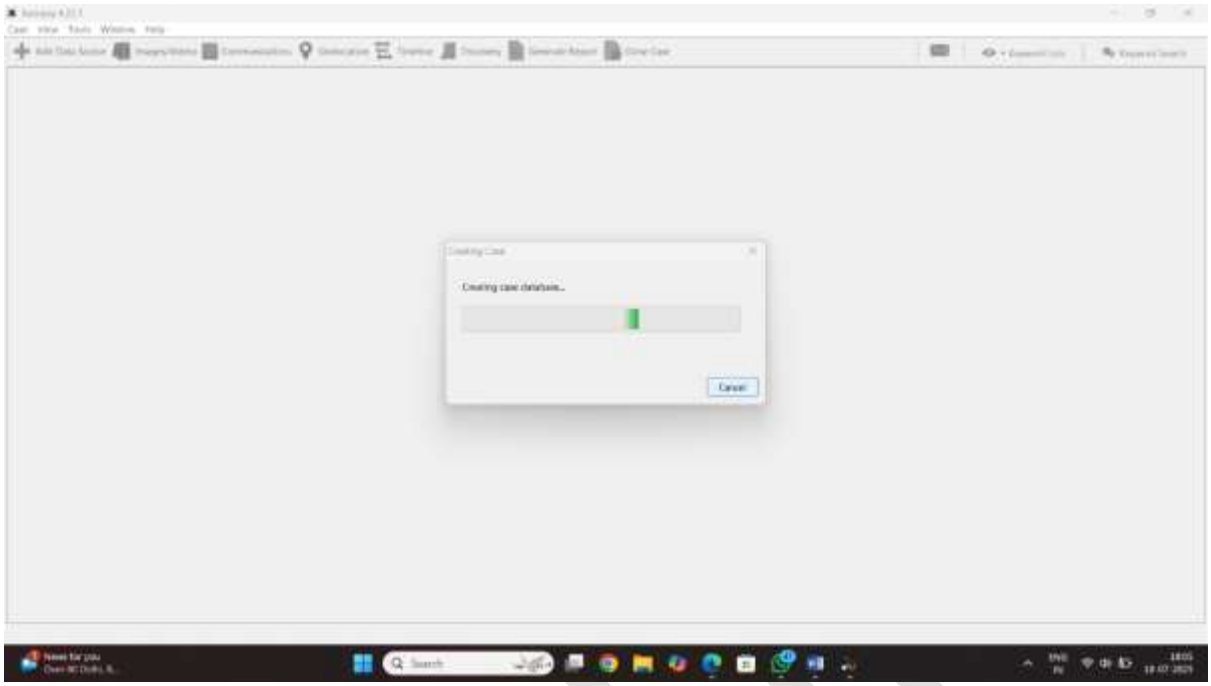
Step4: select the case file destination



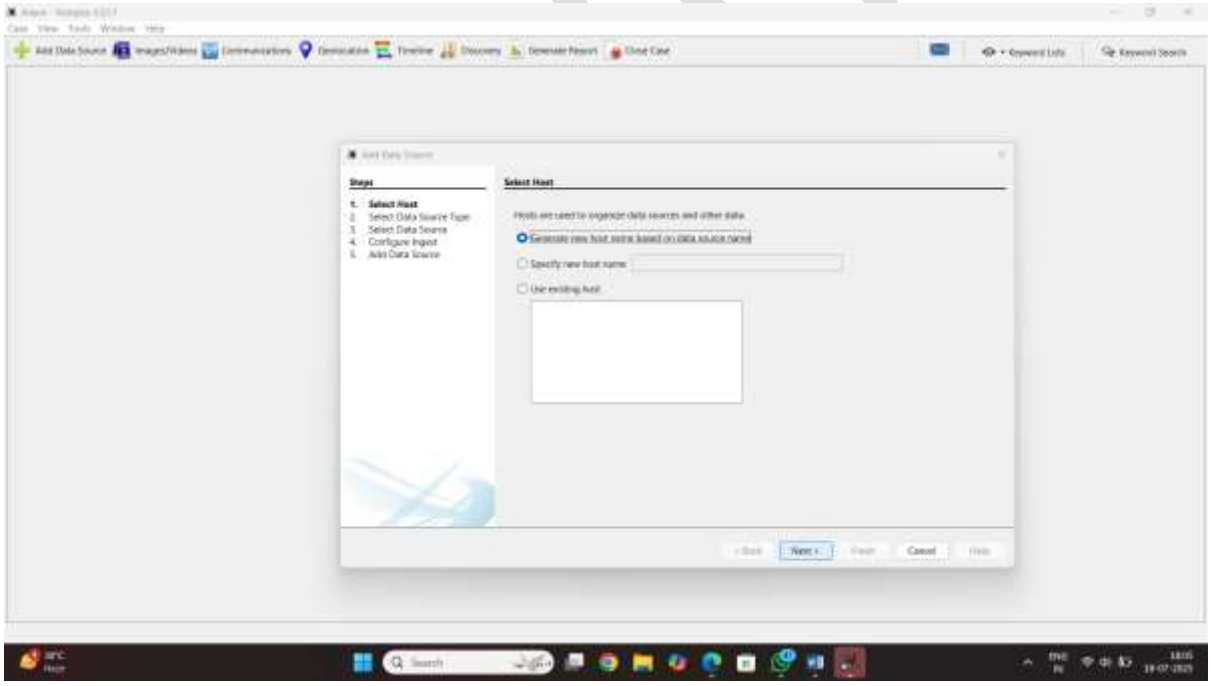
Step5 select the cause number, name ,email, m.number click on next



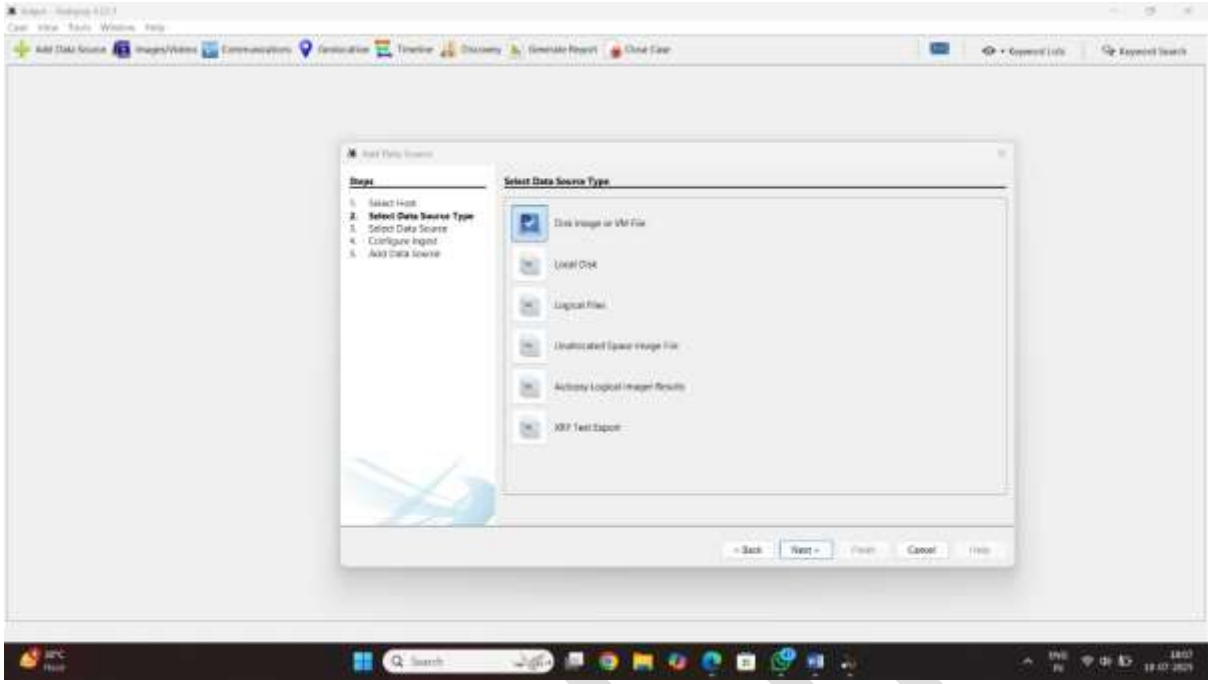
Step6 creating data base cause file



Step7 select host click on the next

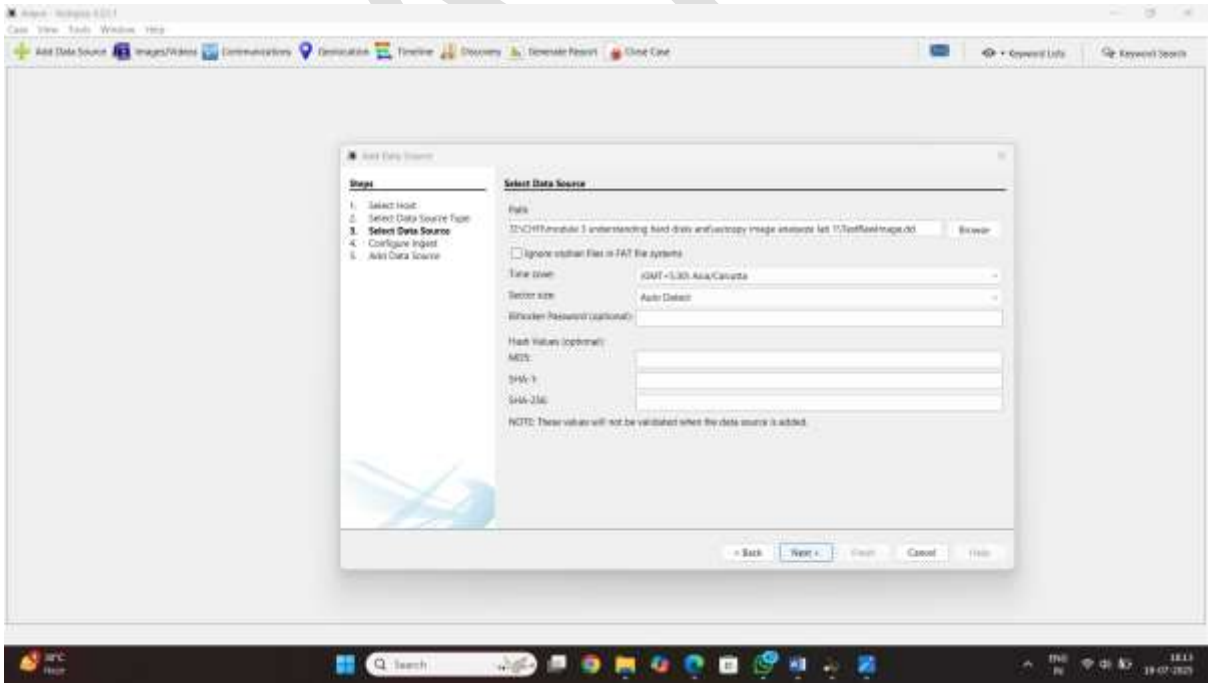


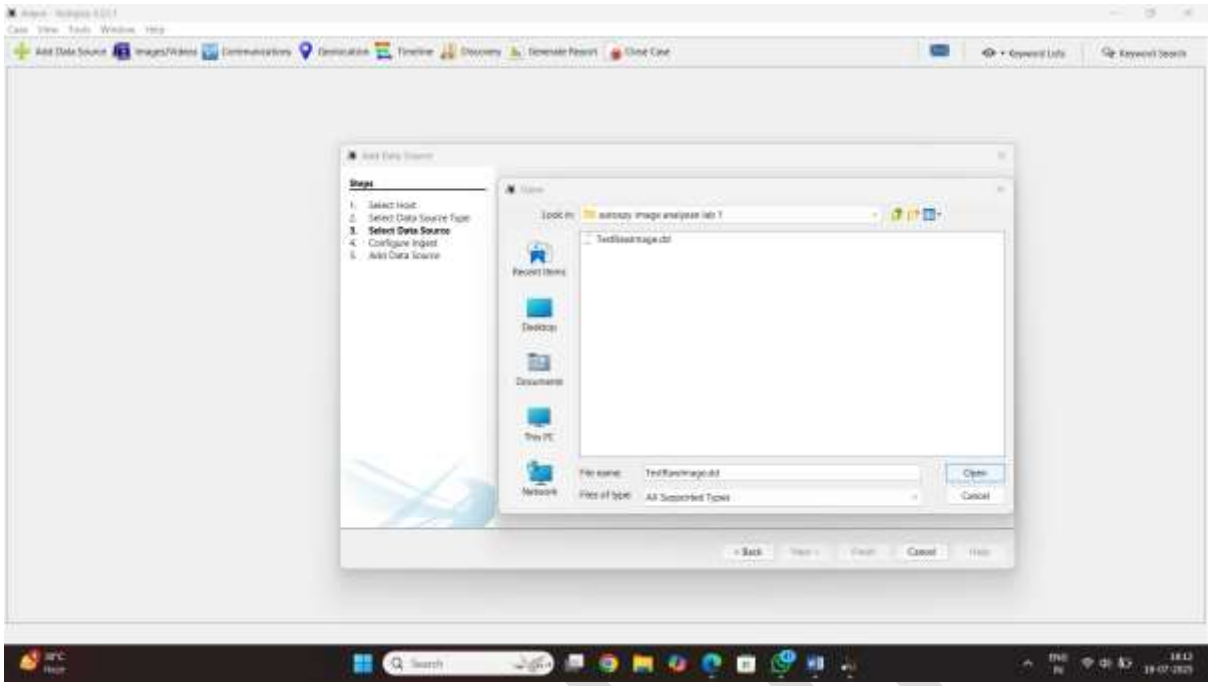
Step8 select the data source type



Select the disk image or vm file click on the next

Step9 select the data source type /image path folder

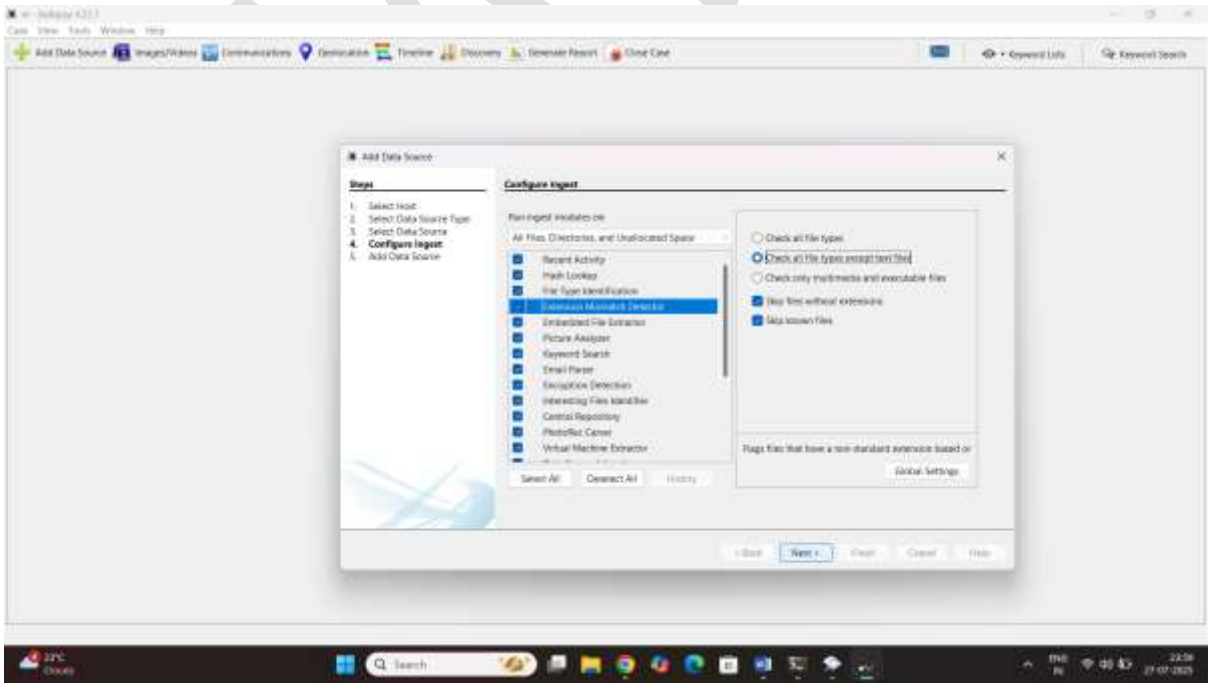




Click in the next

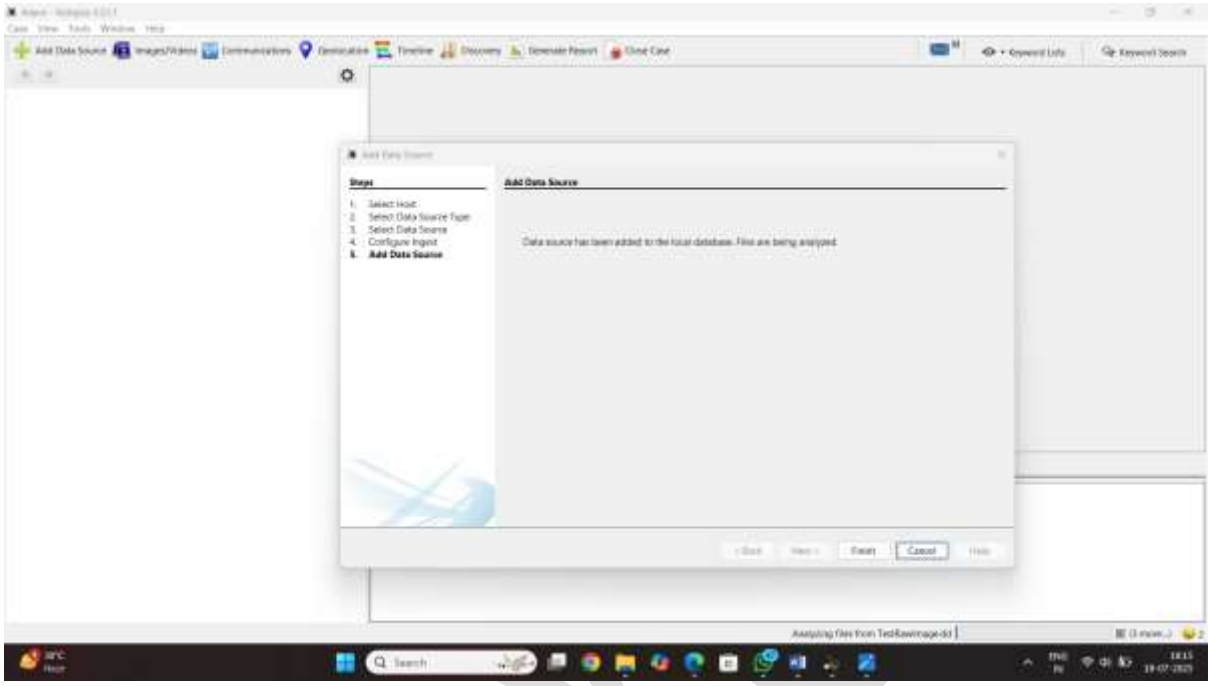
Step10 configure ingest

Select the option extension mismatch option



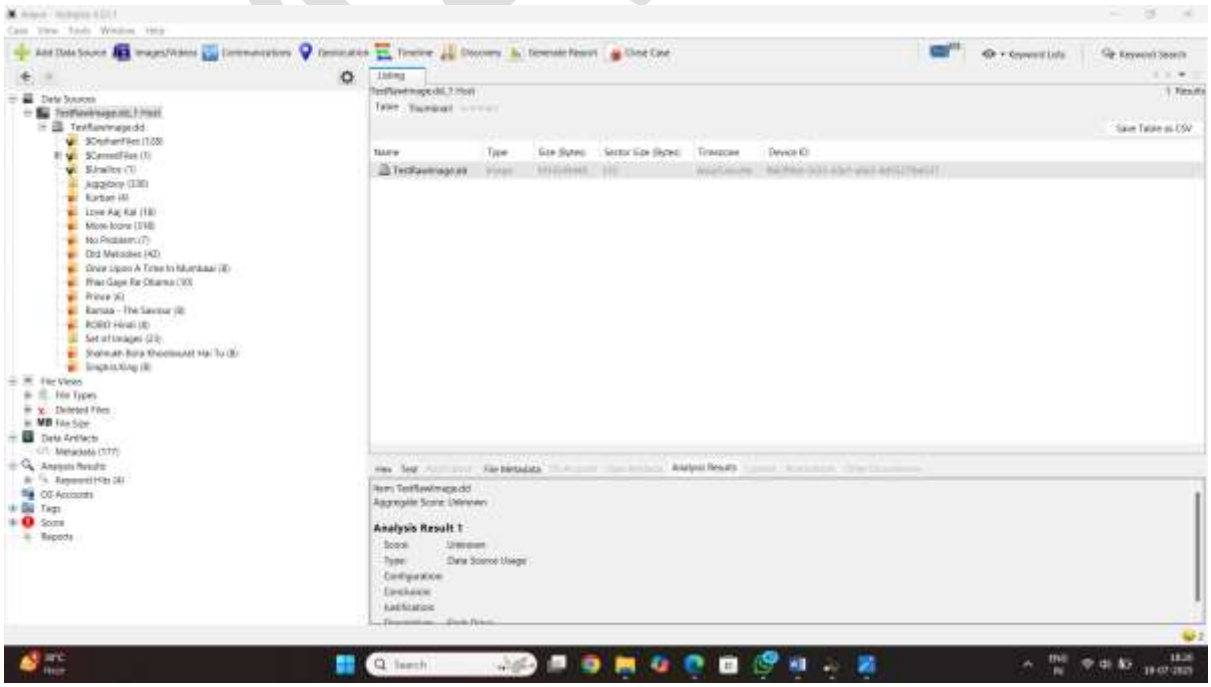
Click on the next

Step11: add data source



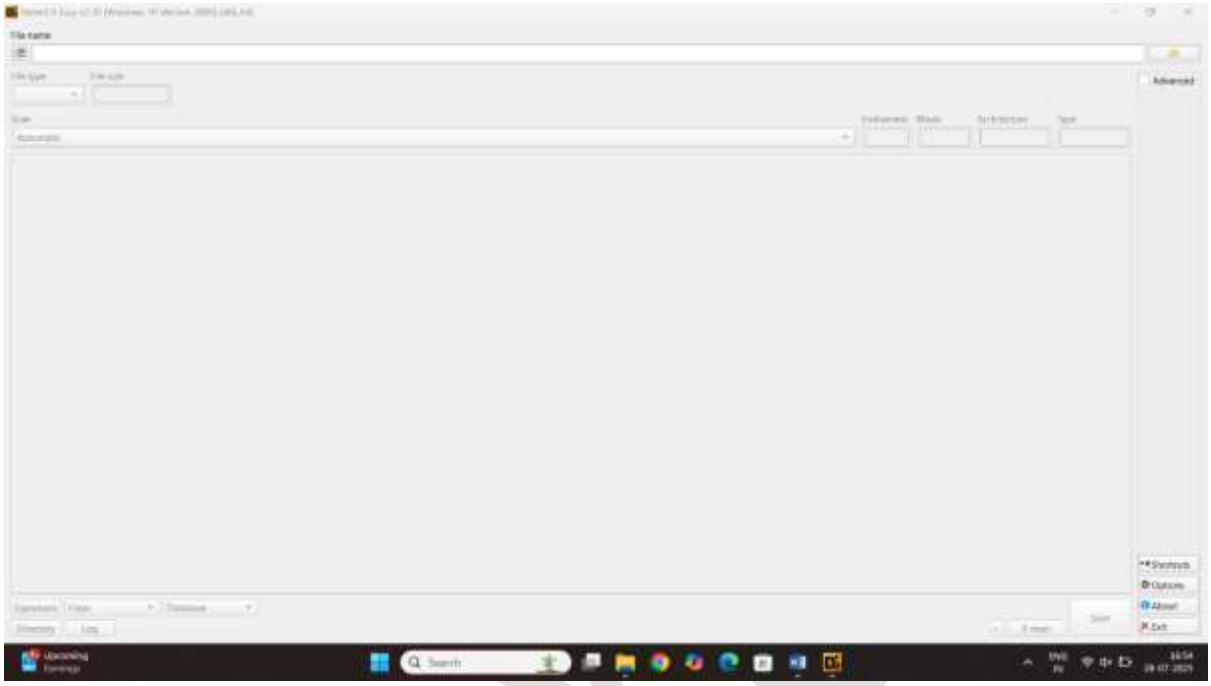
Click on the next

Anaylze the image of content

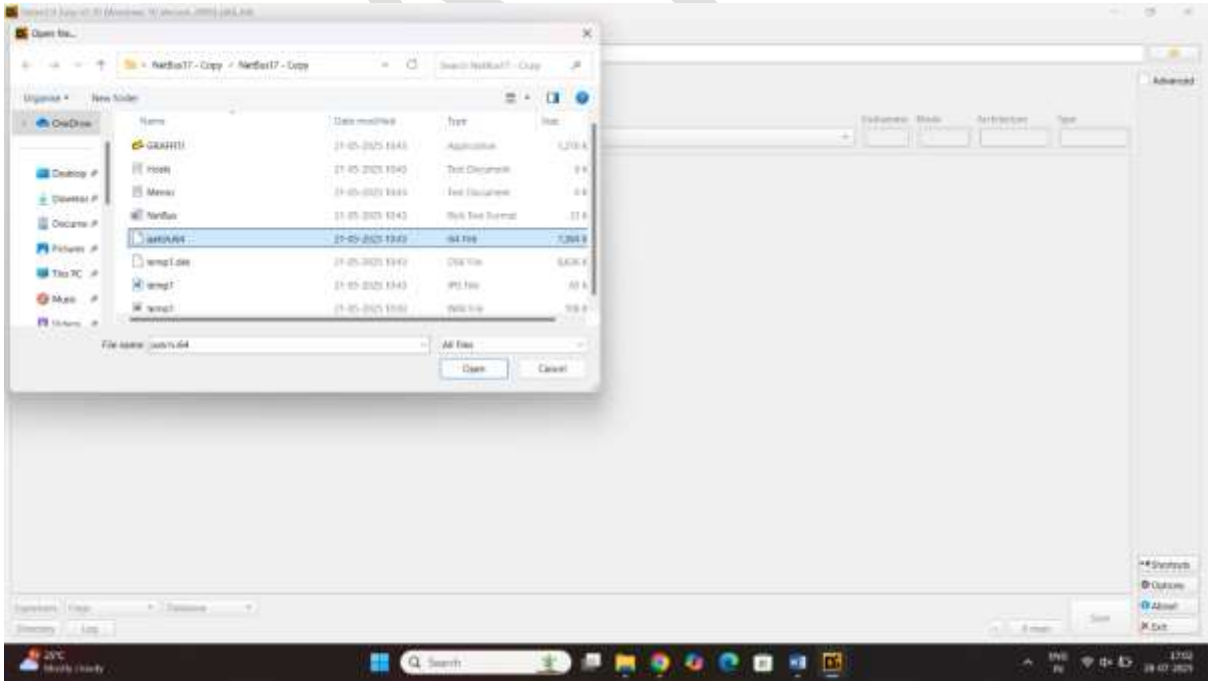


Lab11 unpack program packers using die.exe tool

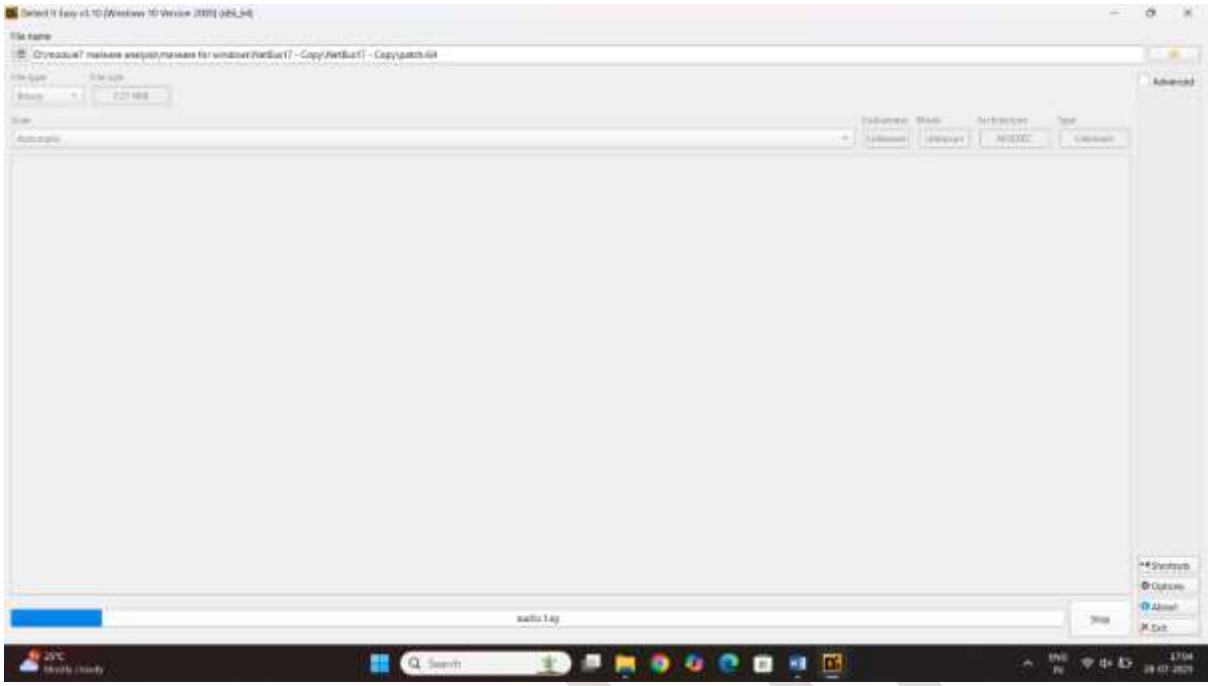
Step1 start the tool



Step2 select the file unpacker



Step3 click on the scan option scan



Result: