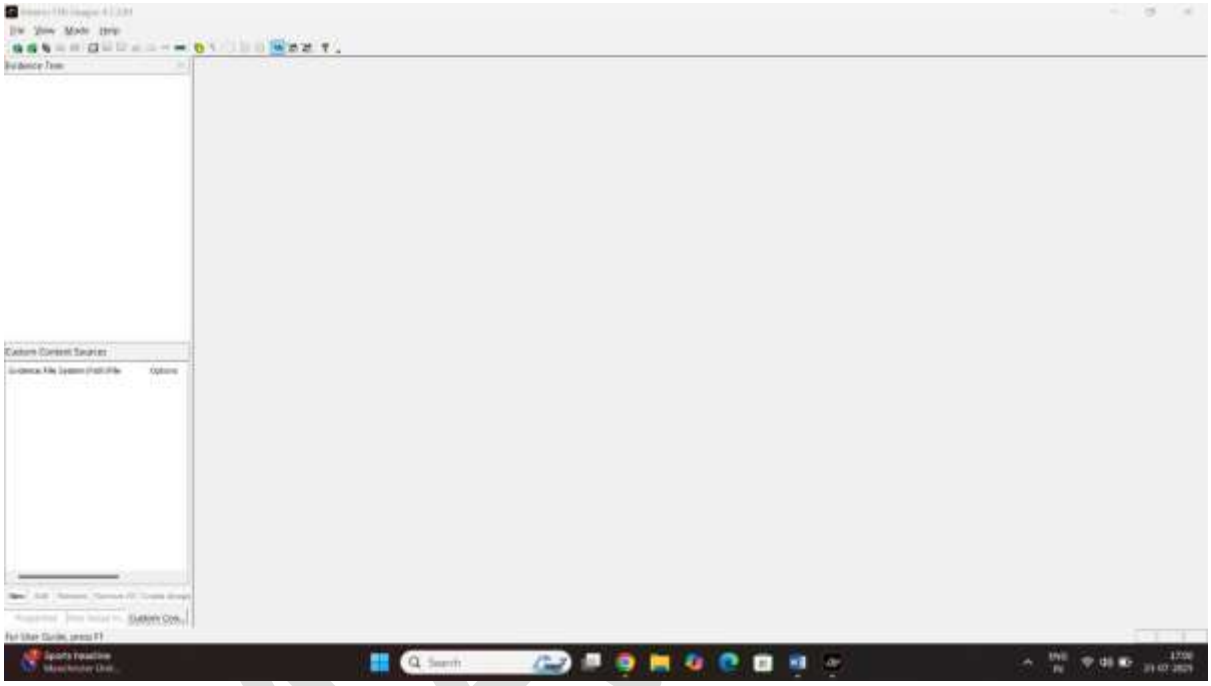
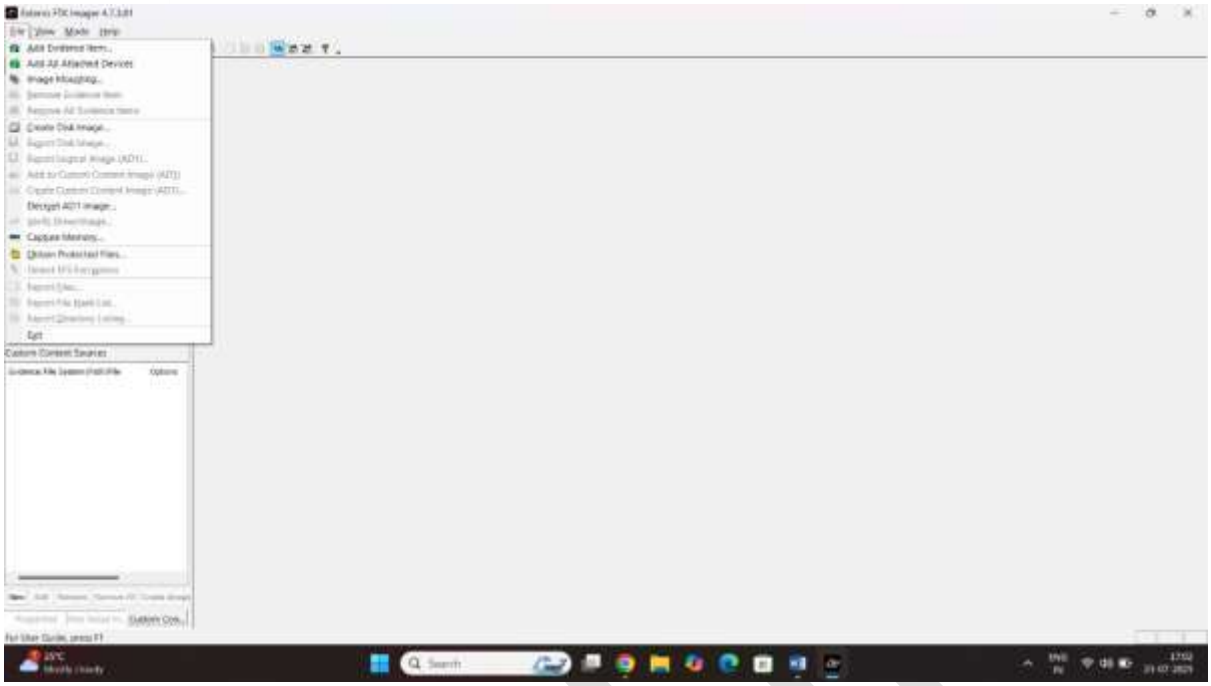
Module 4 : Data acquision and duplication

Lab1 mount image on windows using ftk imager

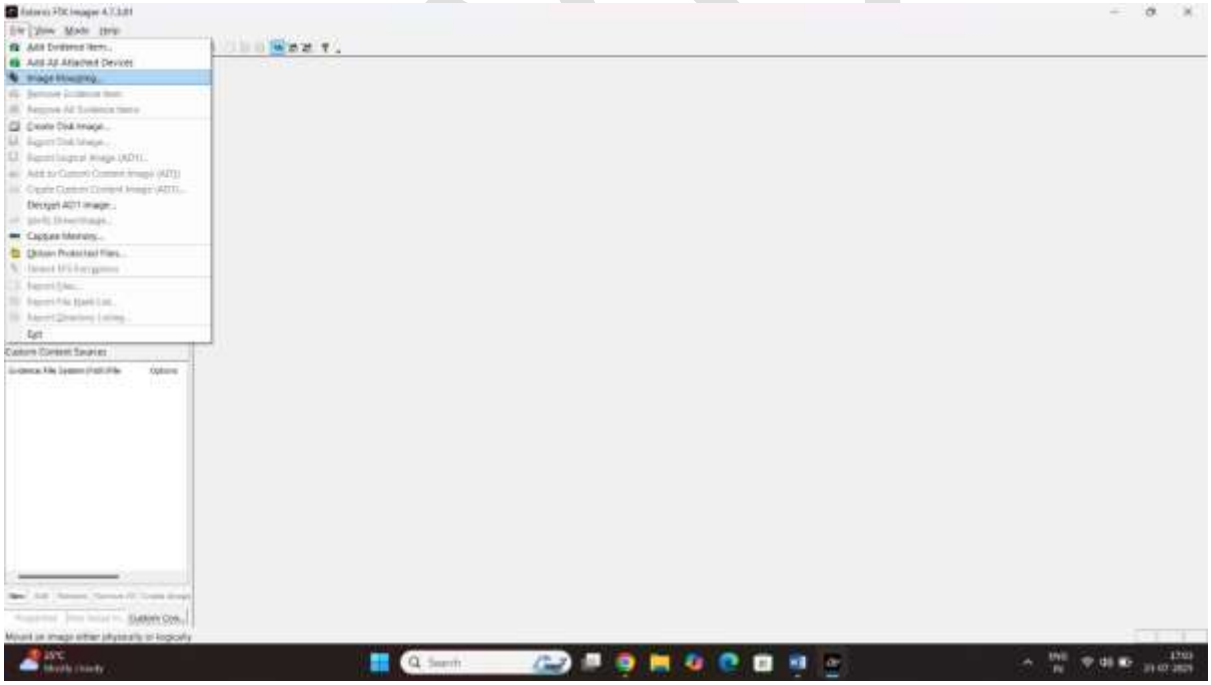
Step1 start the ftk imager



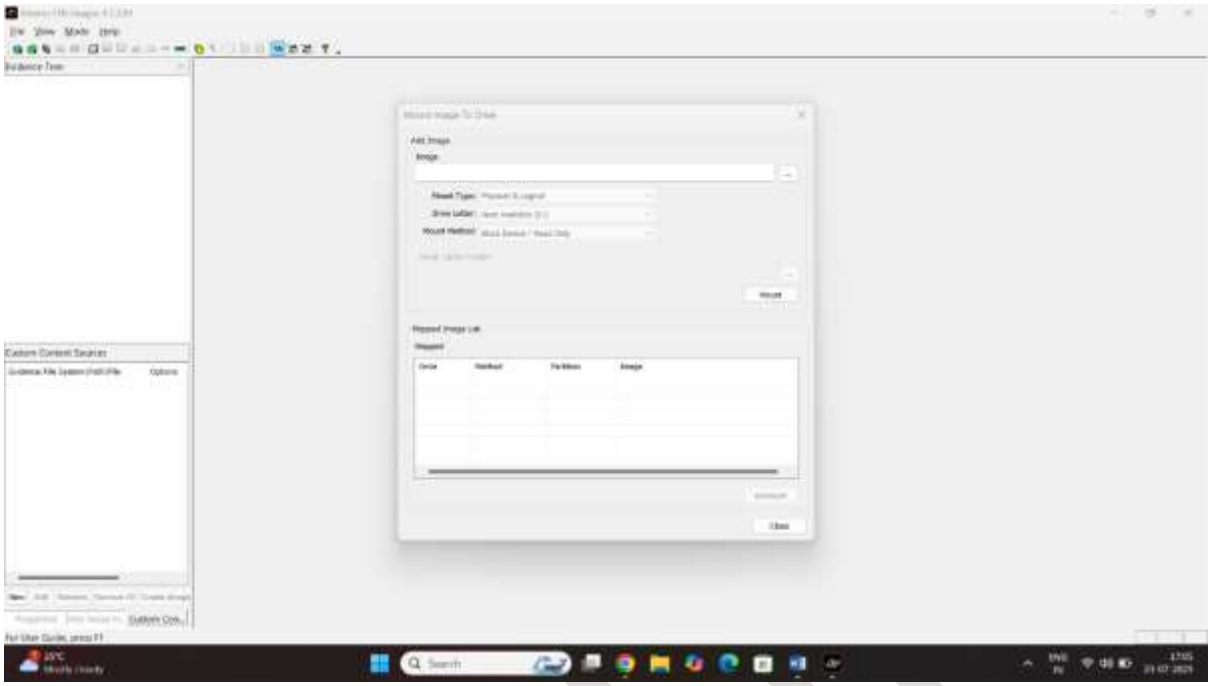
Step2 click on the file



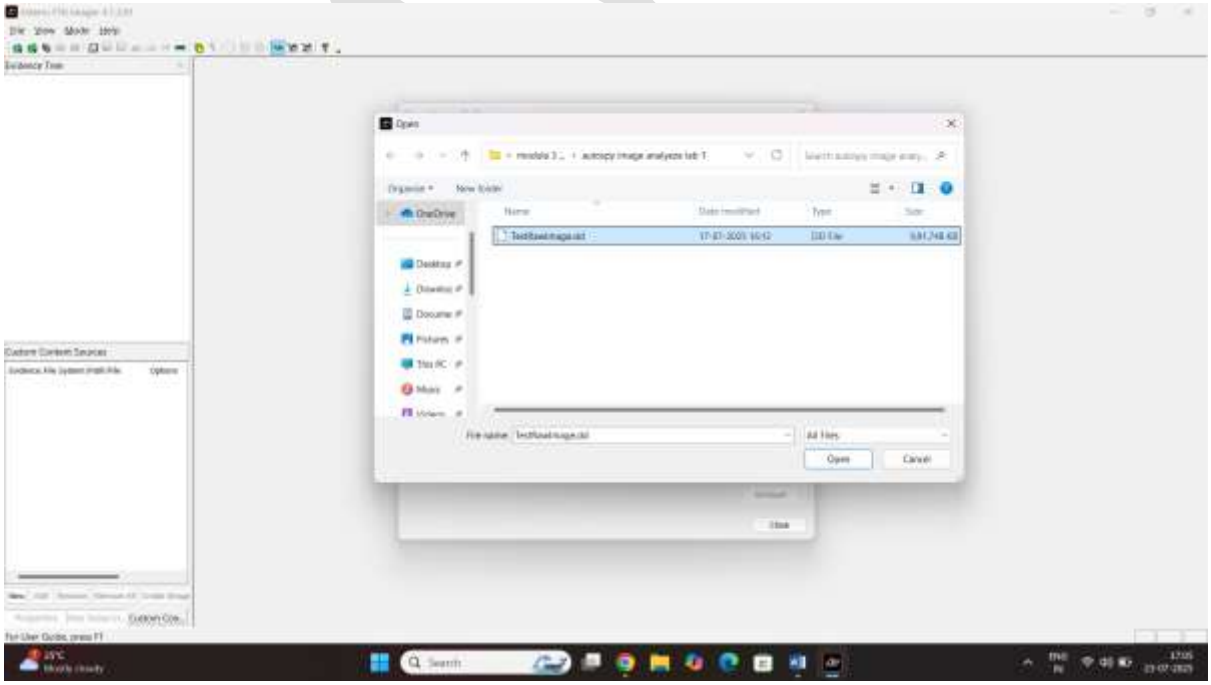
Step3: select the image mount

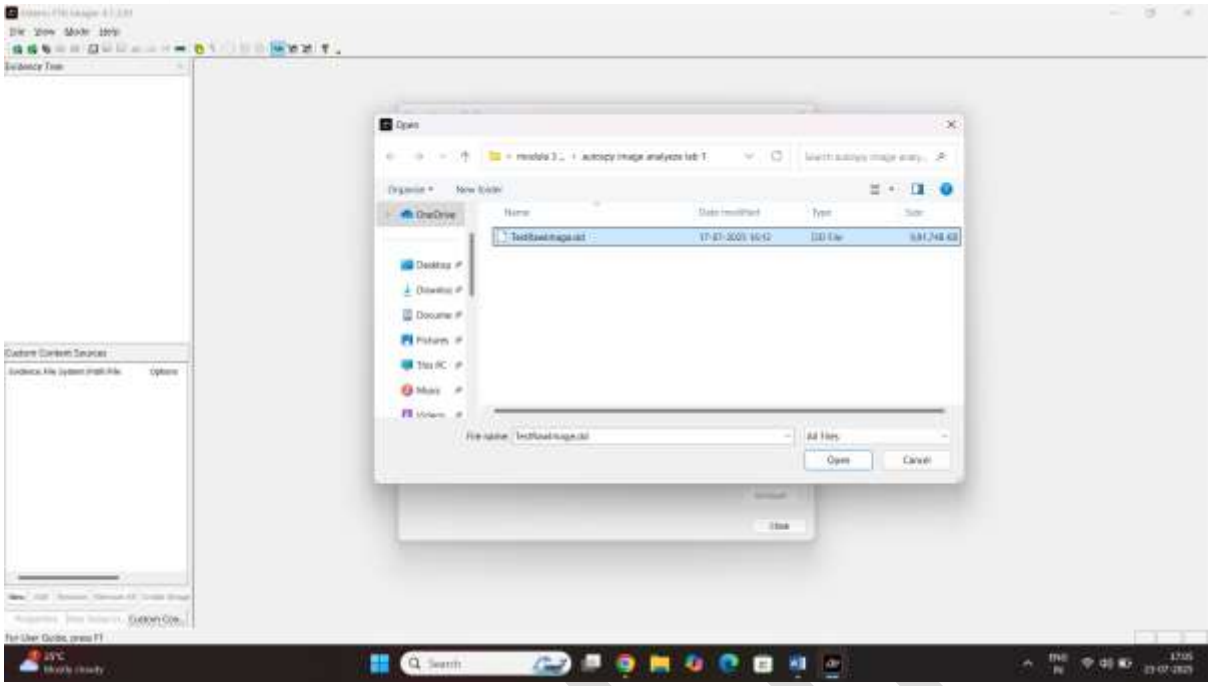


Step4: select the d.d image path

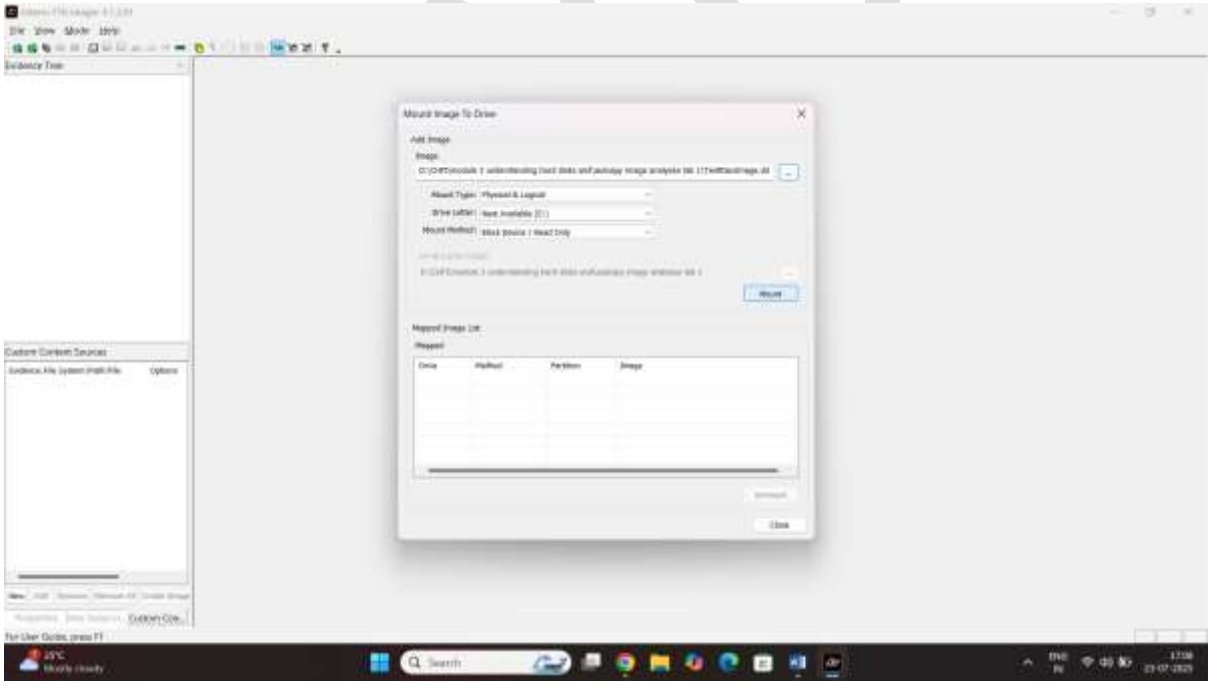


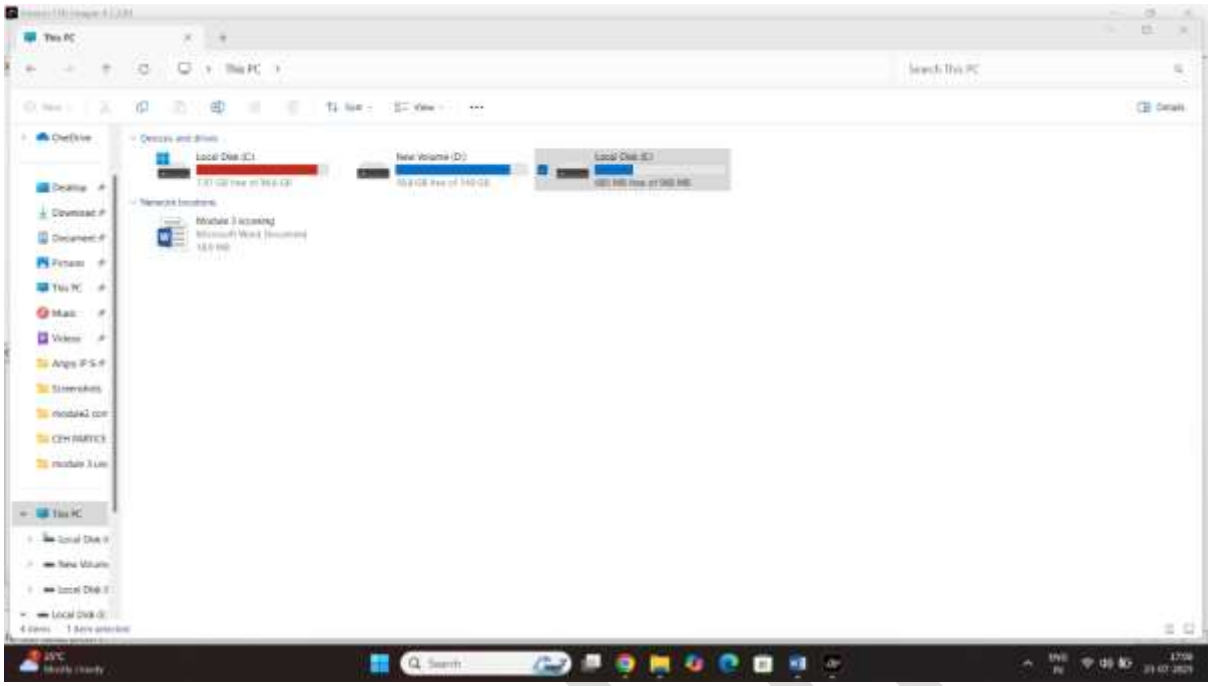
Step5: select the image path of dd image

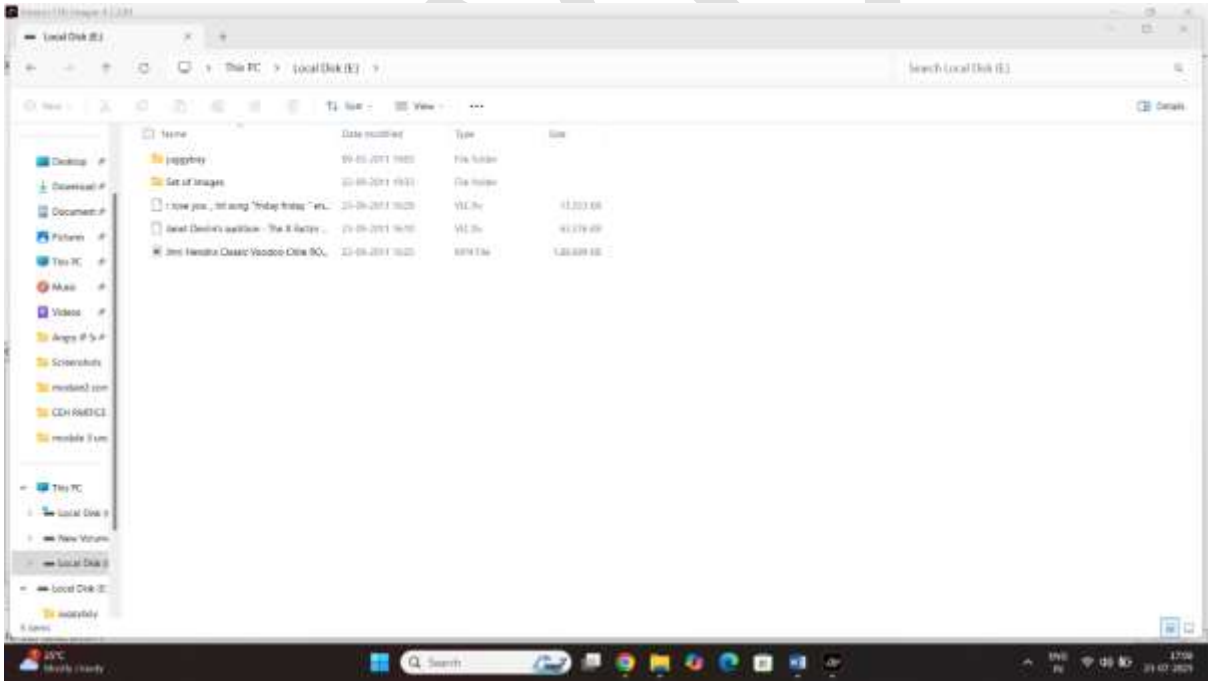




Step6 click on the mount option



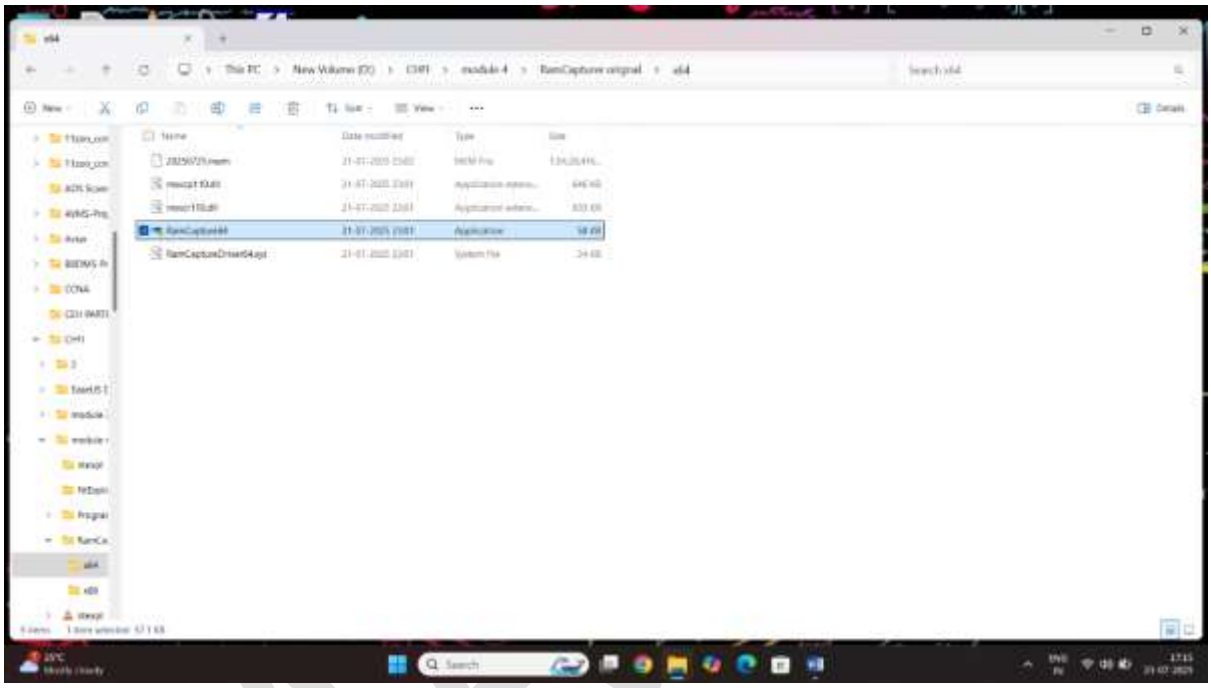




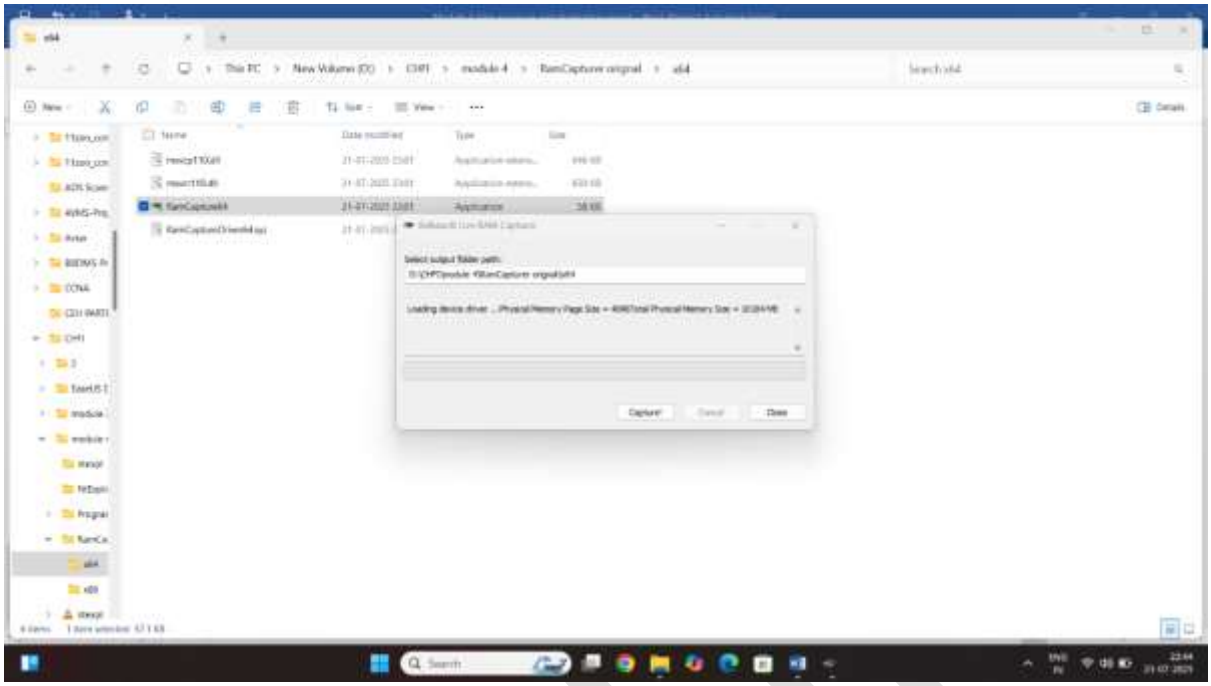
Lab2 Acquire RAM from window and linux workestion

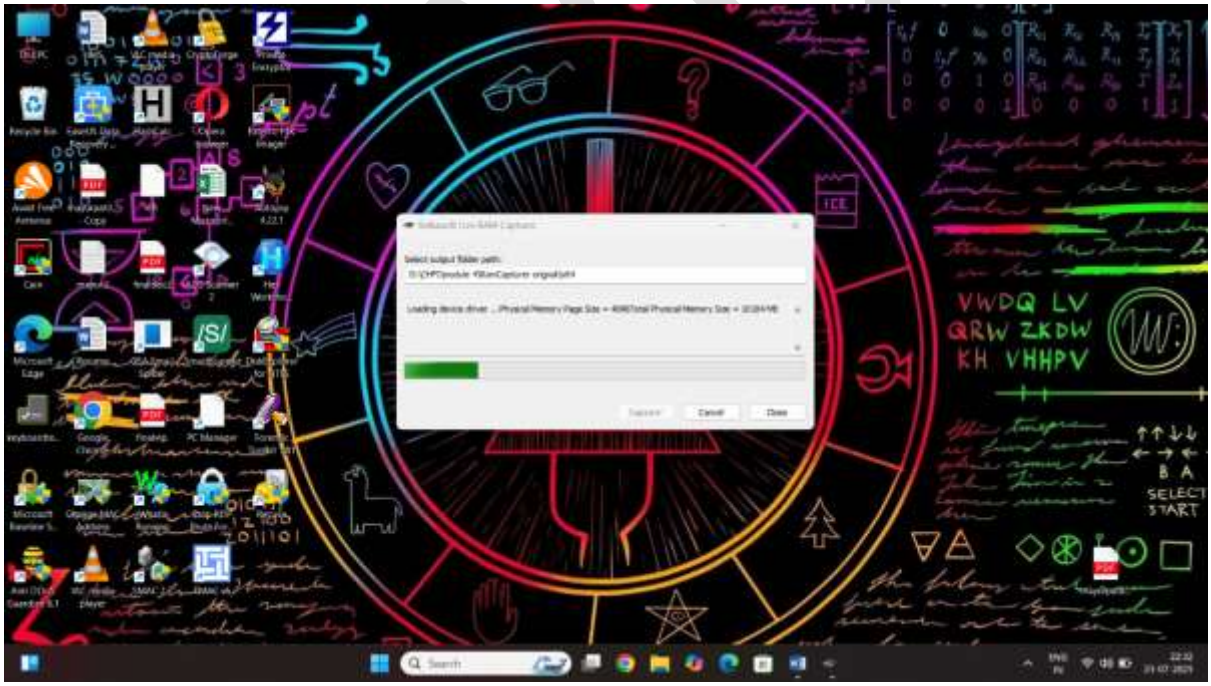
There was tool called RAM capture

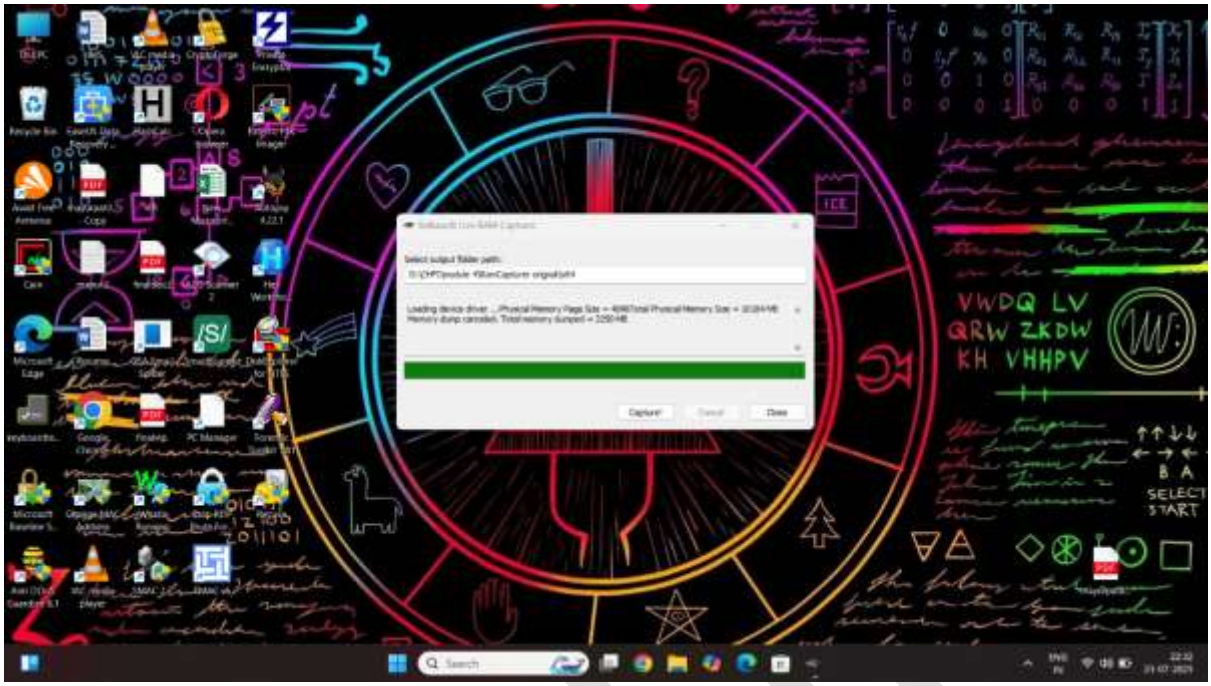
Step1: start the application



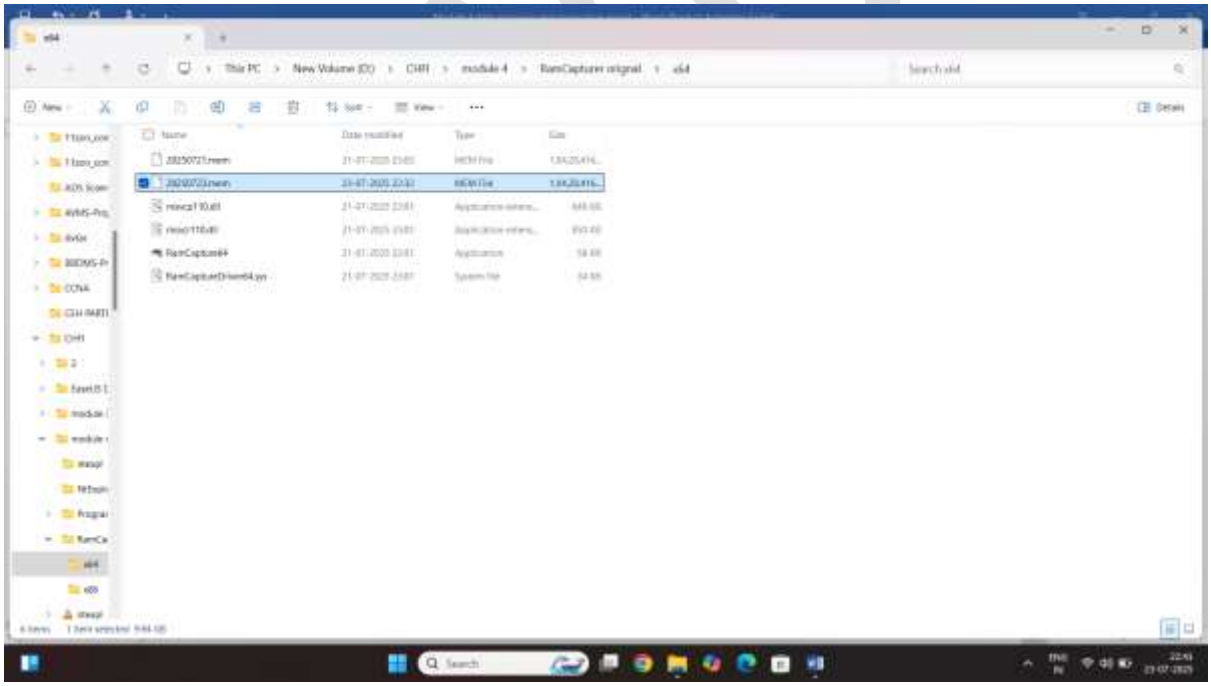
Step2 clcik on capture







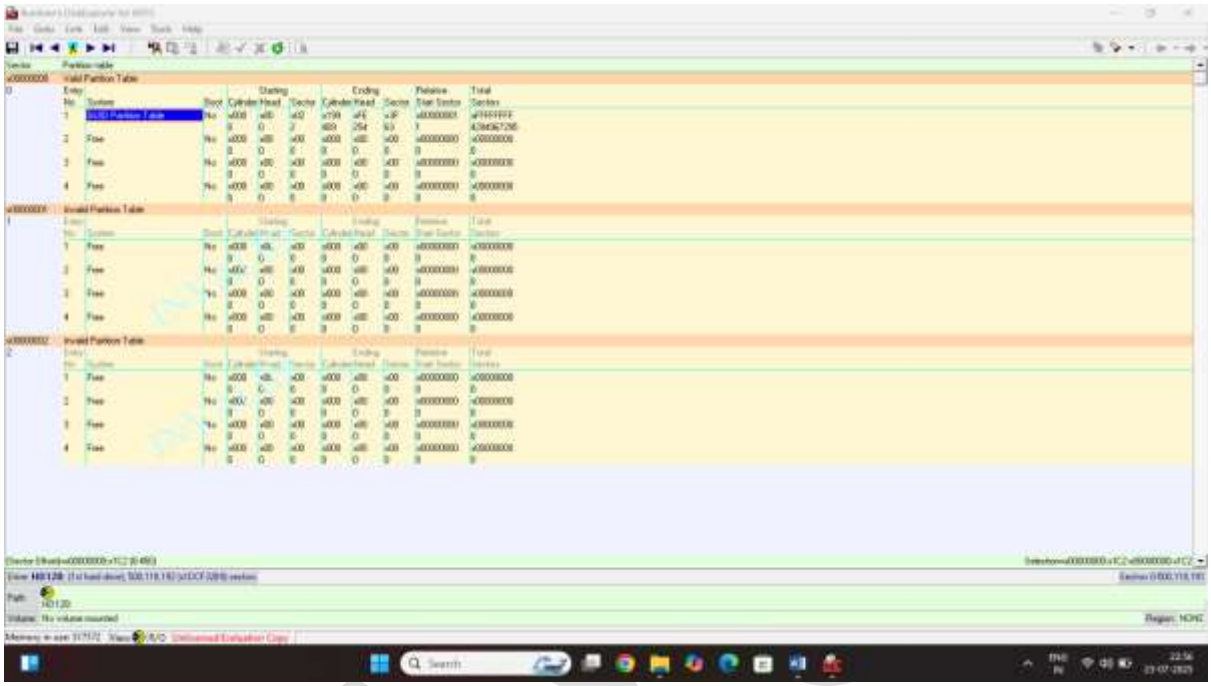
Store the recover of the data in folder



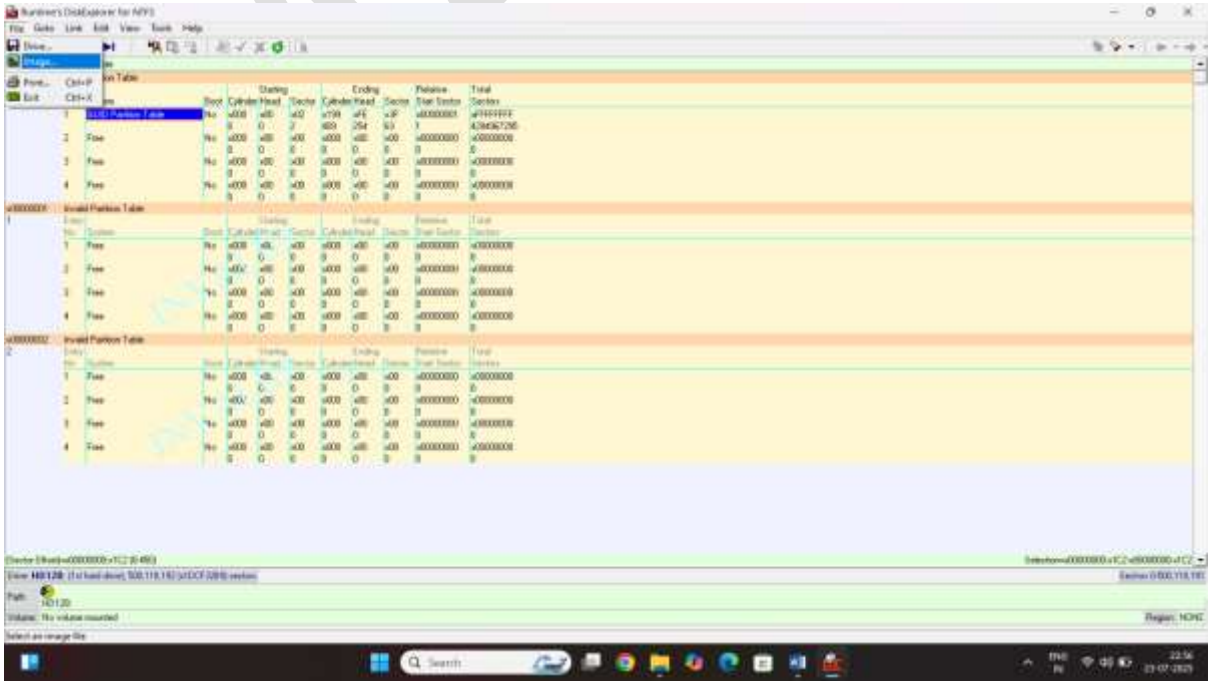
Lab 4 create customized image from an image containing NTFS file system

There was tool called Disk exploar for /NTFS

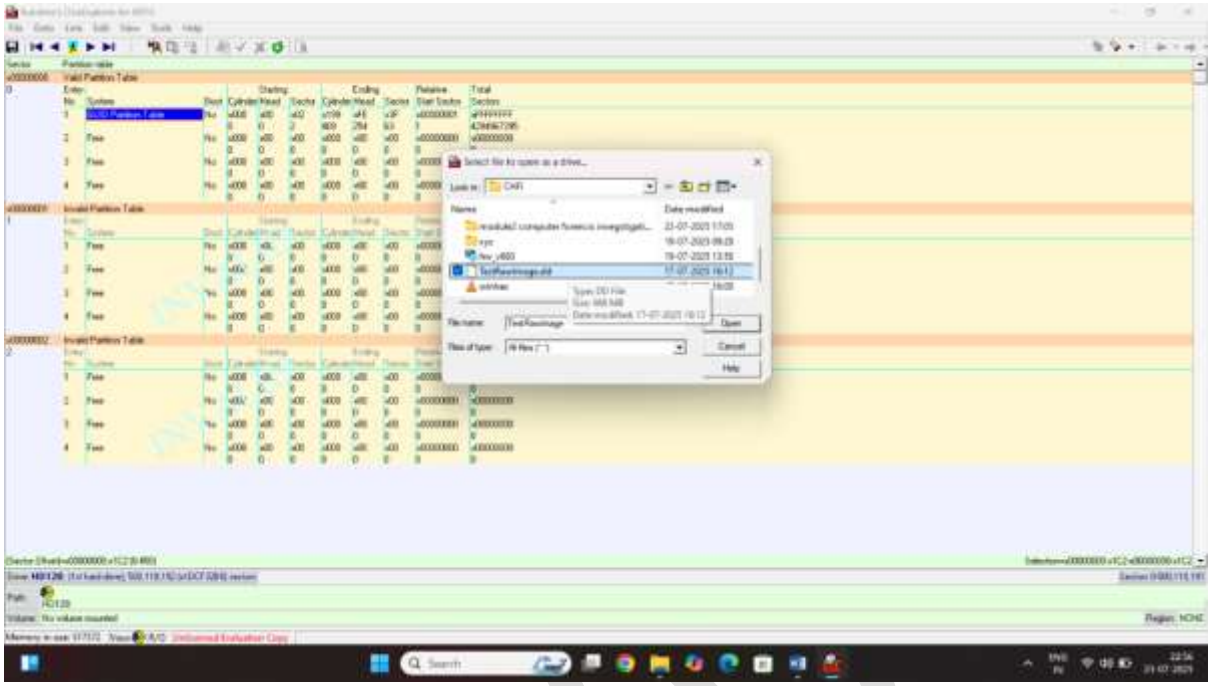
Step1: start the disk exploar



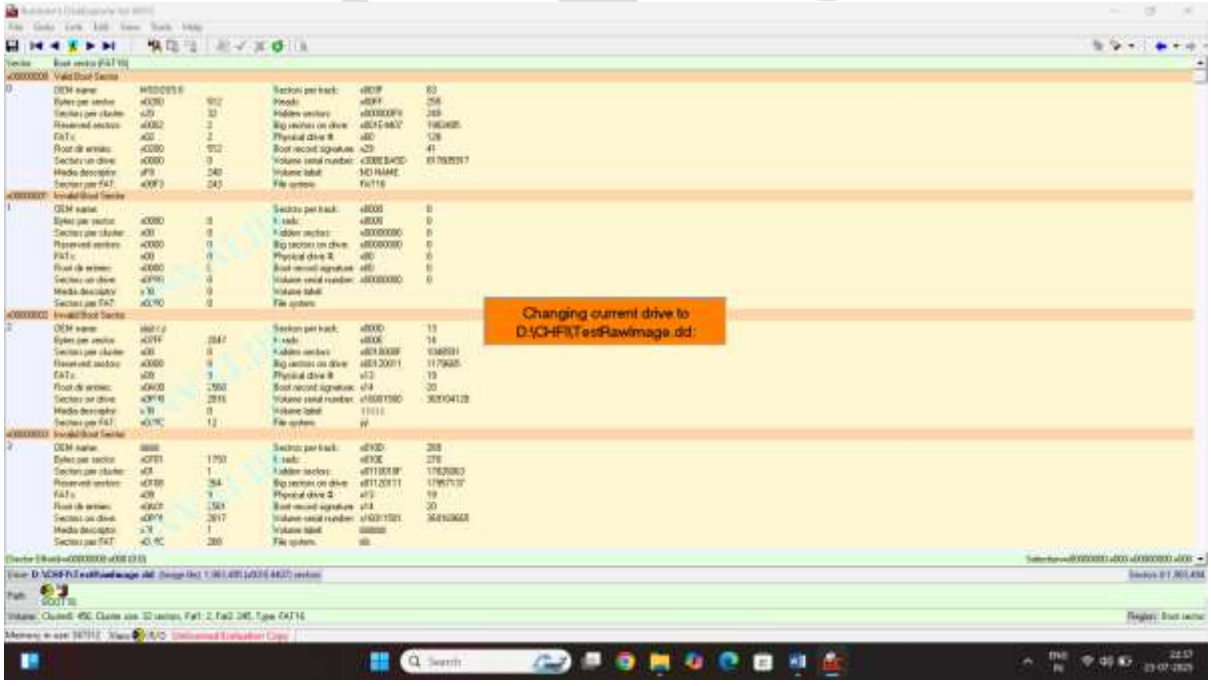
Step2: click on the file and select the iamge option



Step3 select the image file path



Result:

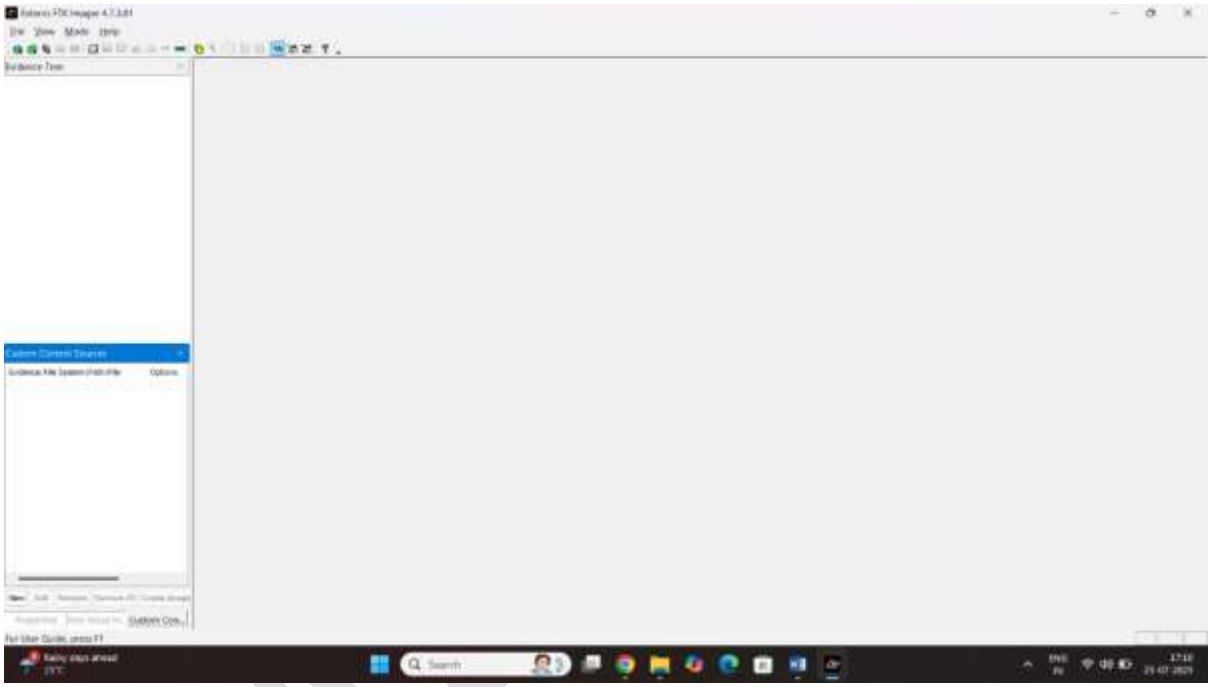


Lab6 view content of forensic image file

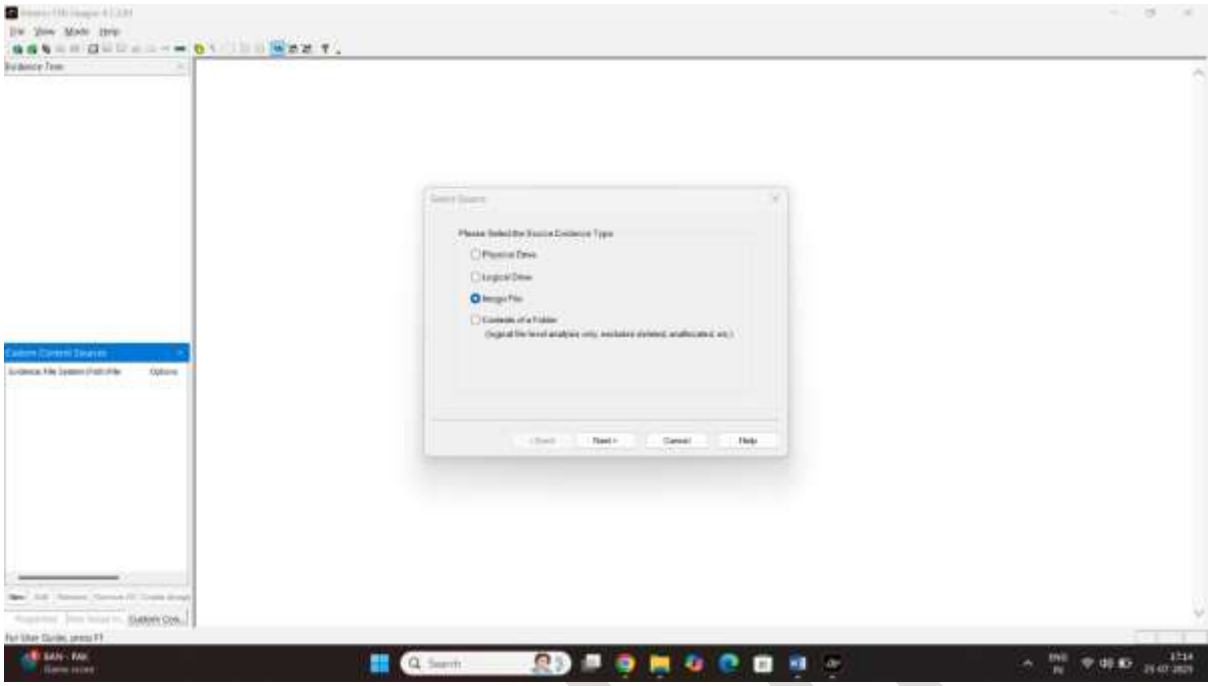
How to access a data D.D image file reading

There was tool called FTK image

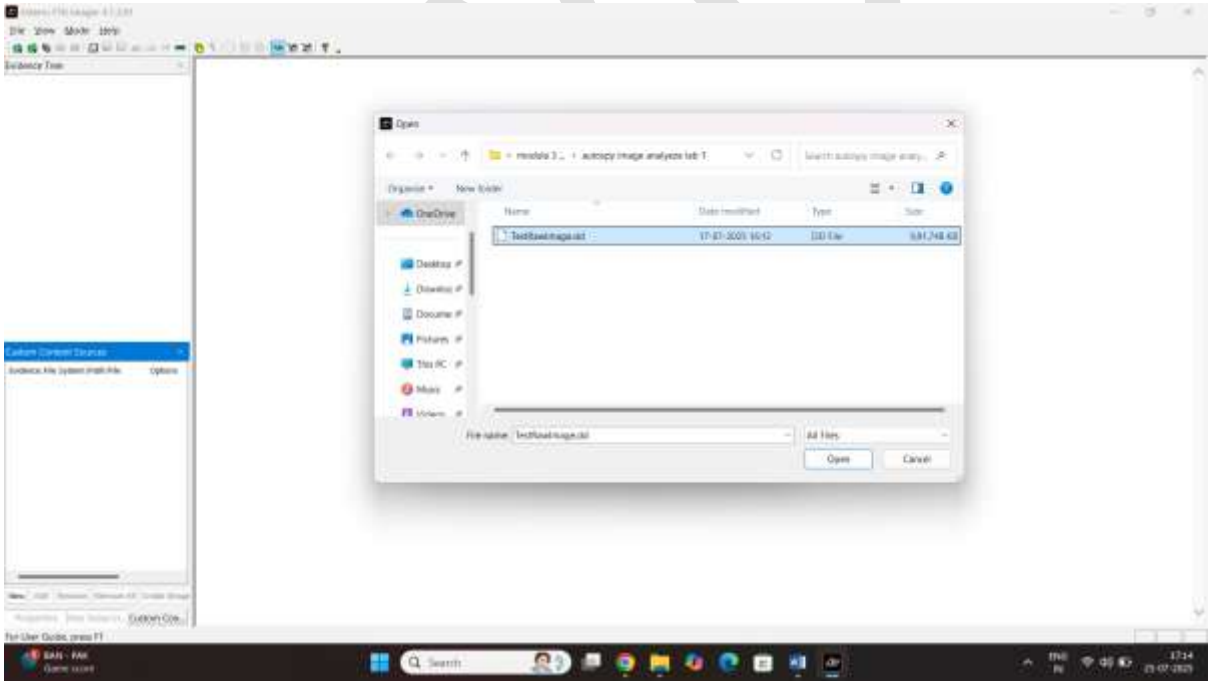
Step1 start the ftk imager



Step2 click on the file select add evidence itam

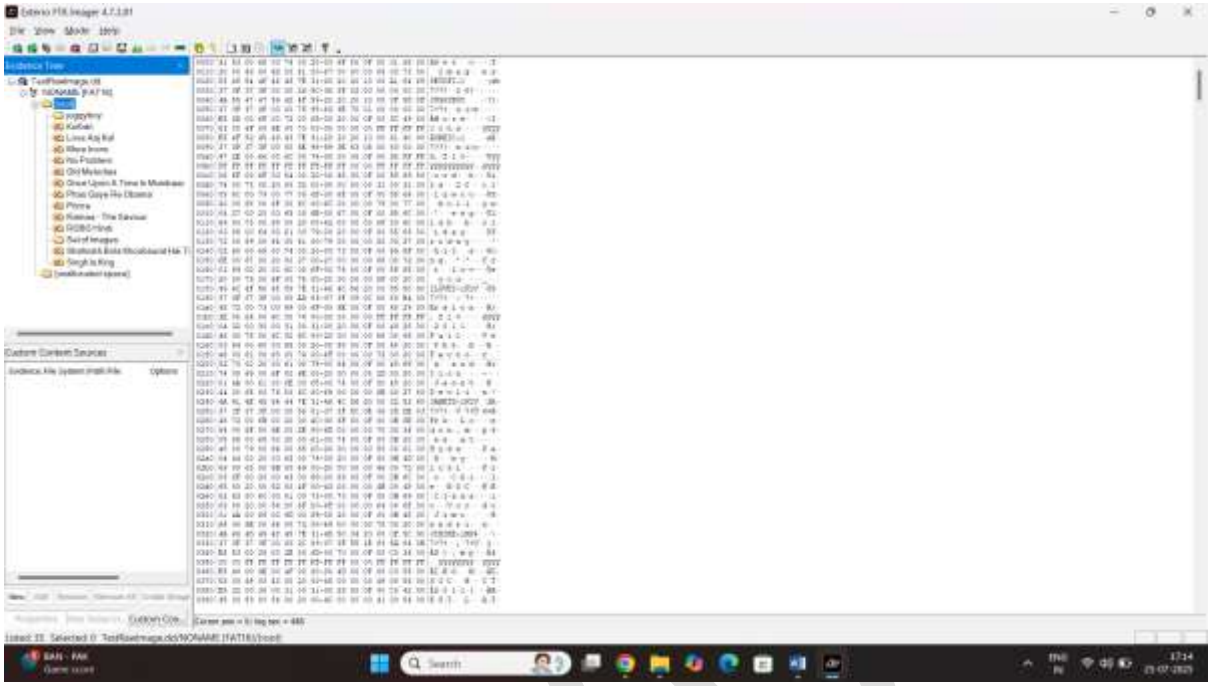


Step3 click on the image



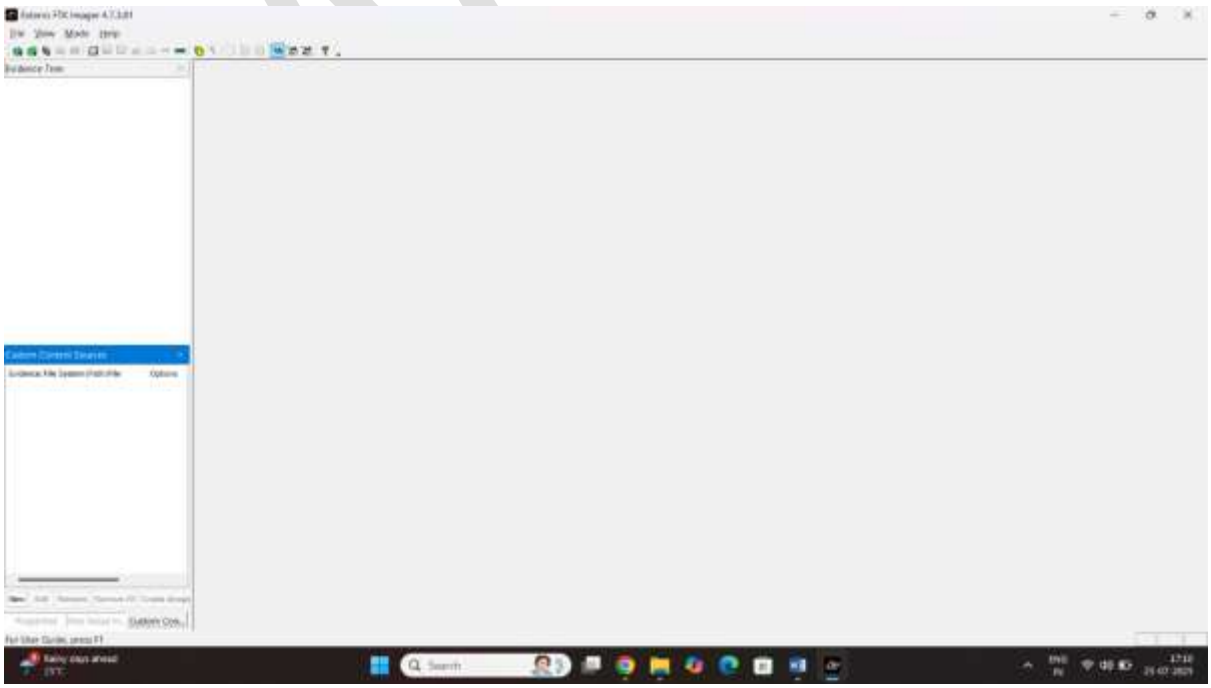
Step4 select the dd.image

Step5 click on the + button

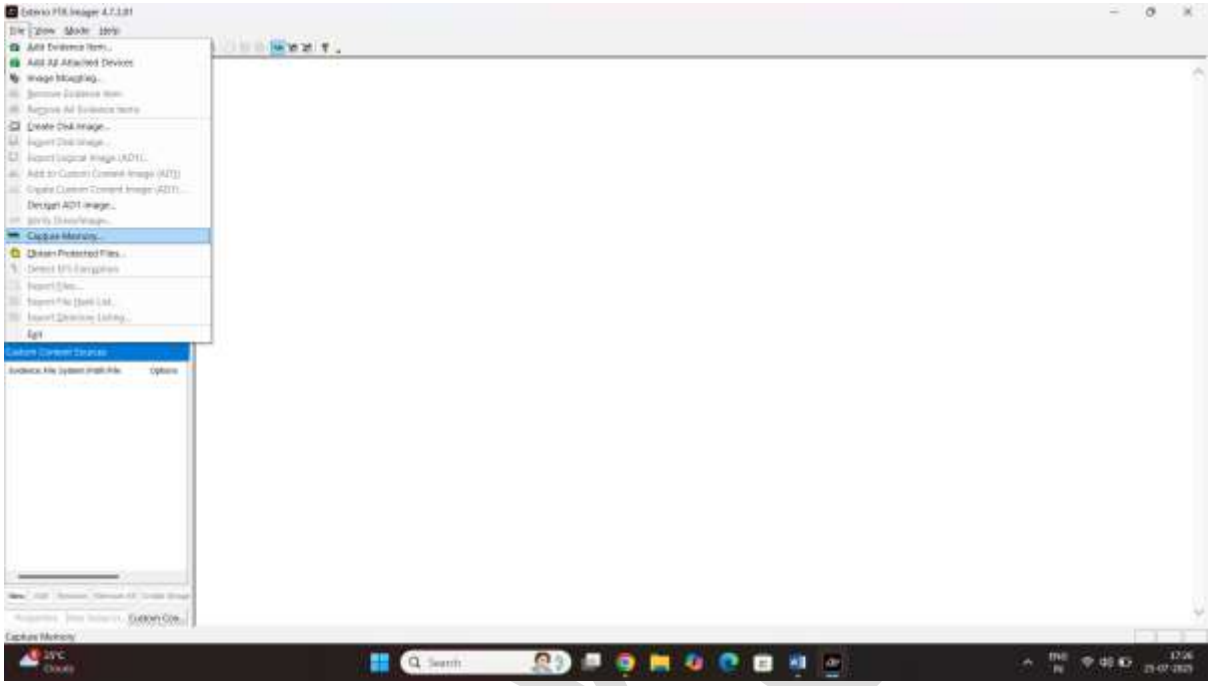


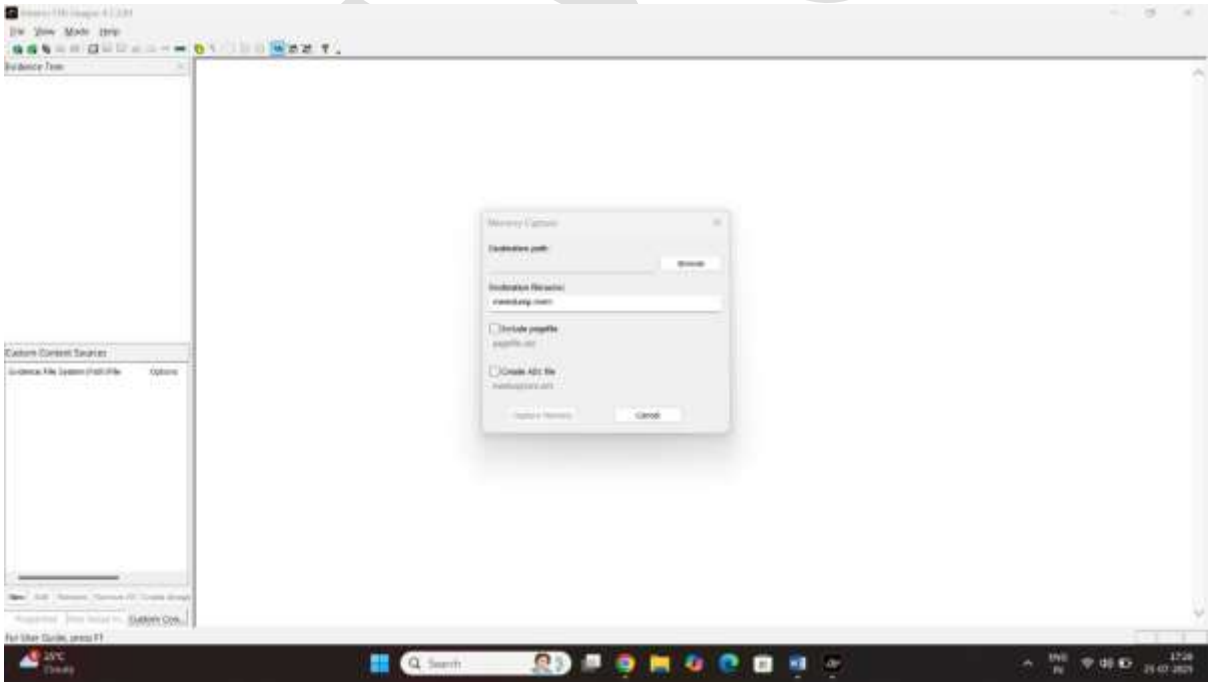
How to ftk image ram capture method

Step1: start the ftk imager

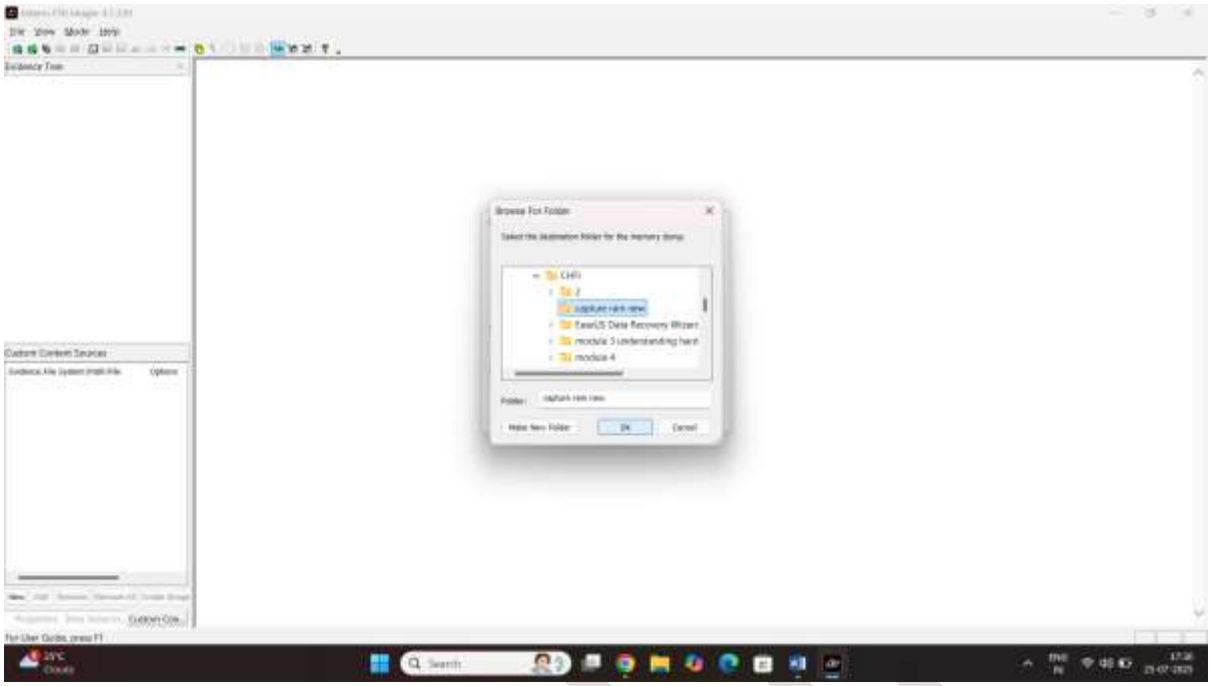


Step2:click on the file and select the option capture the ram

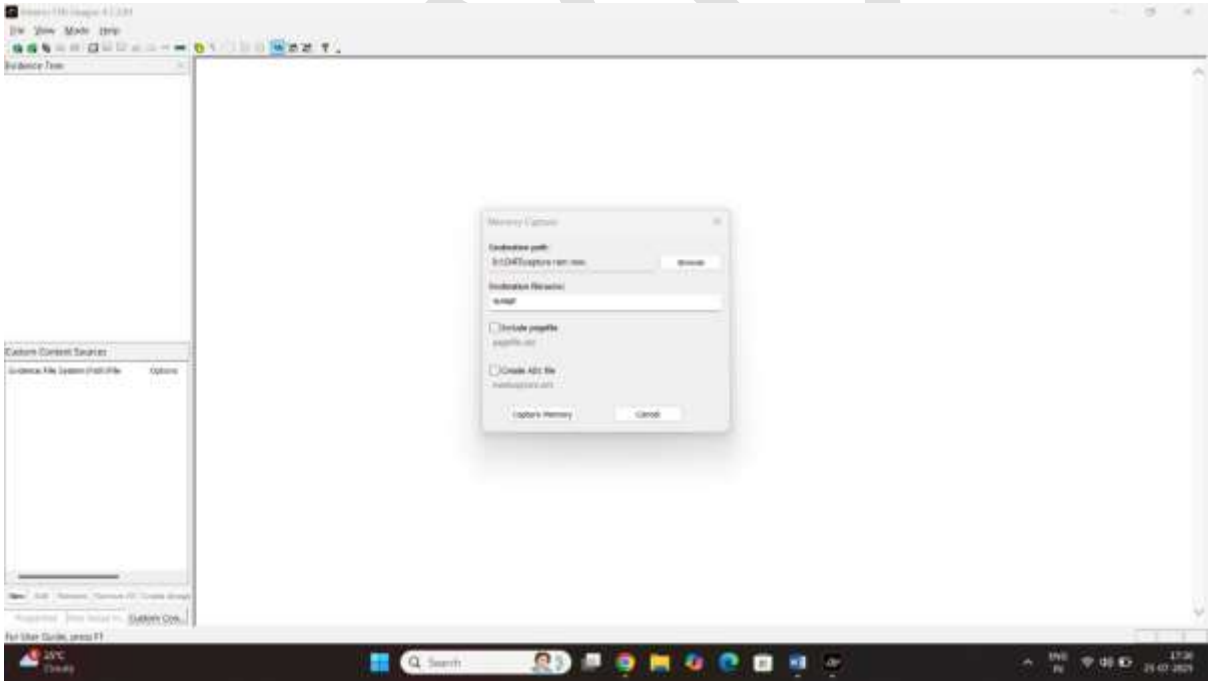




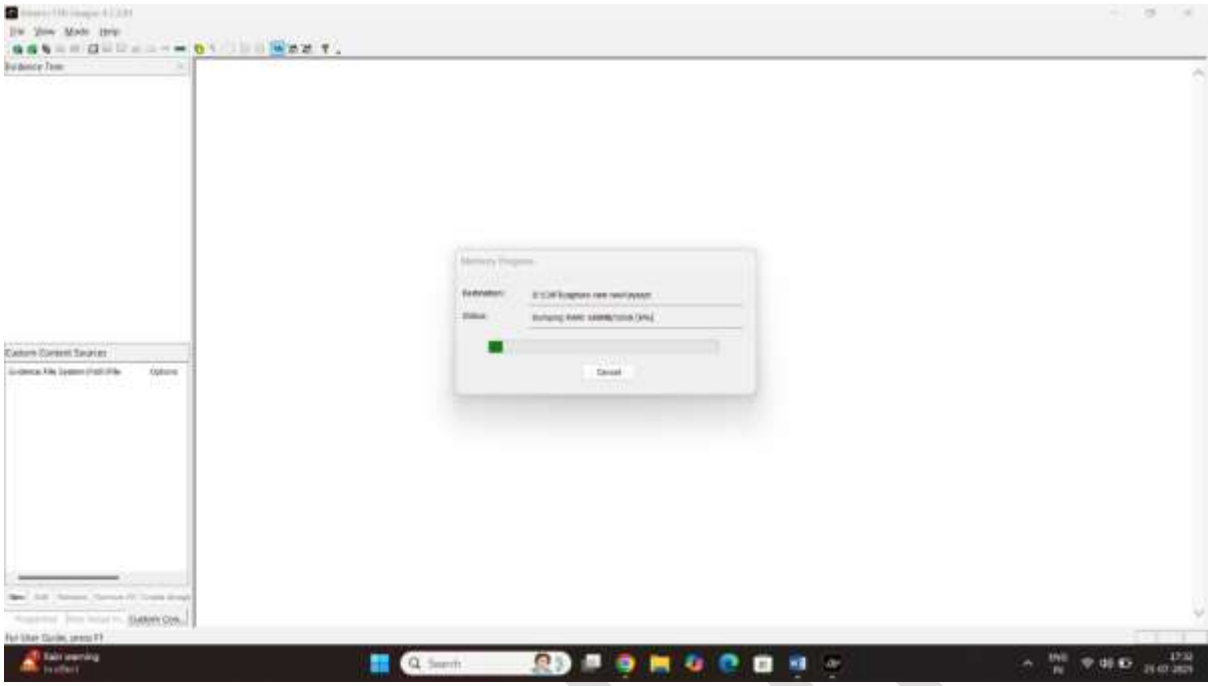
Step3 select the destination path and destination filename

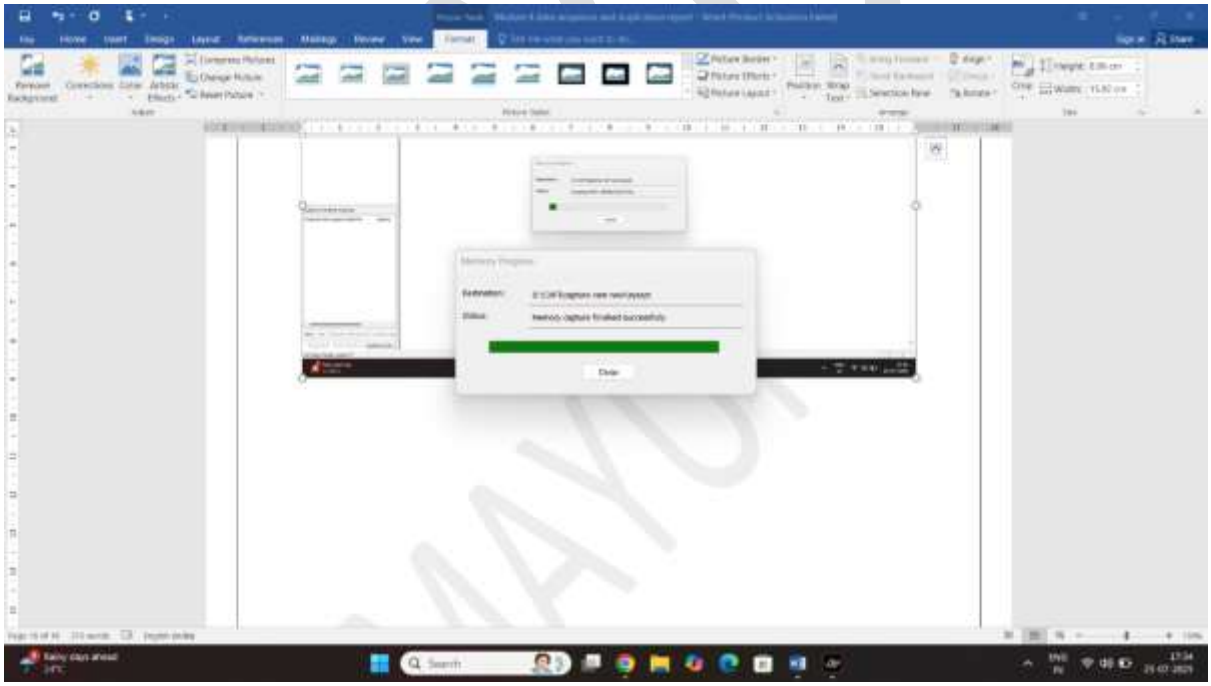


Select the file destination

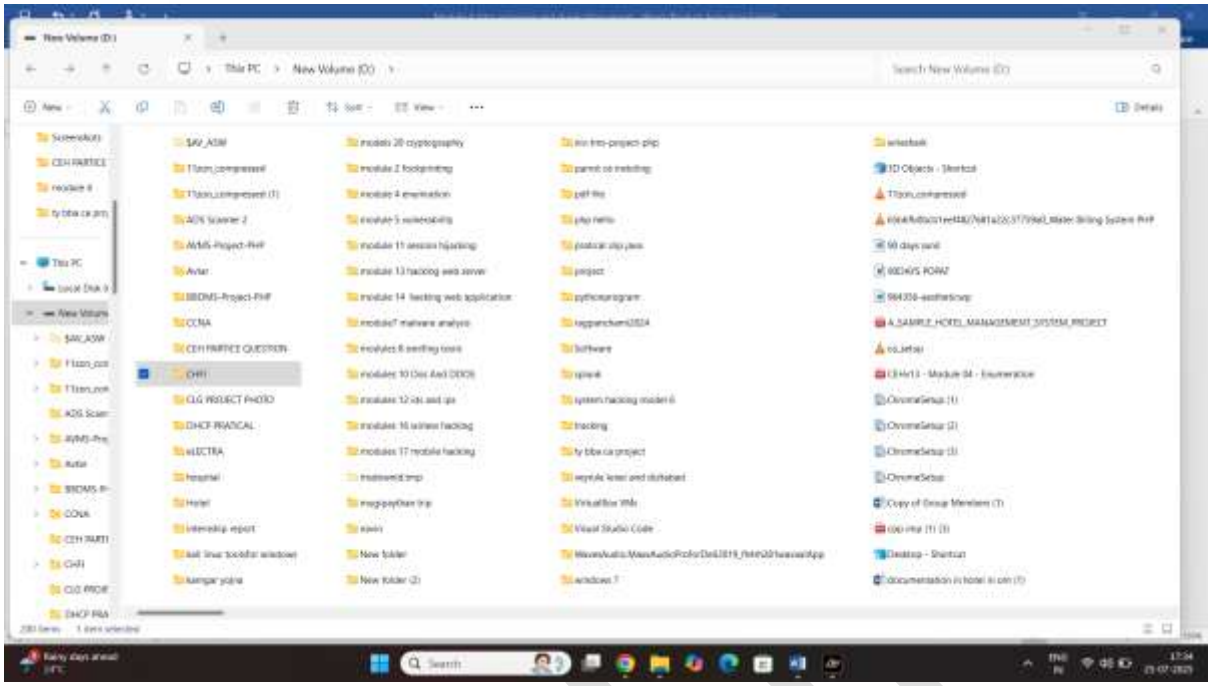


Step4: click on the capture

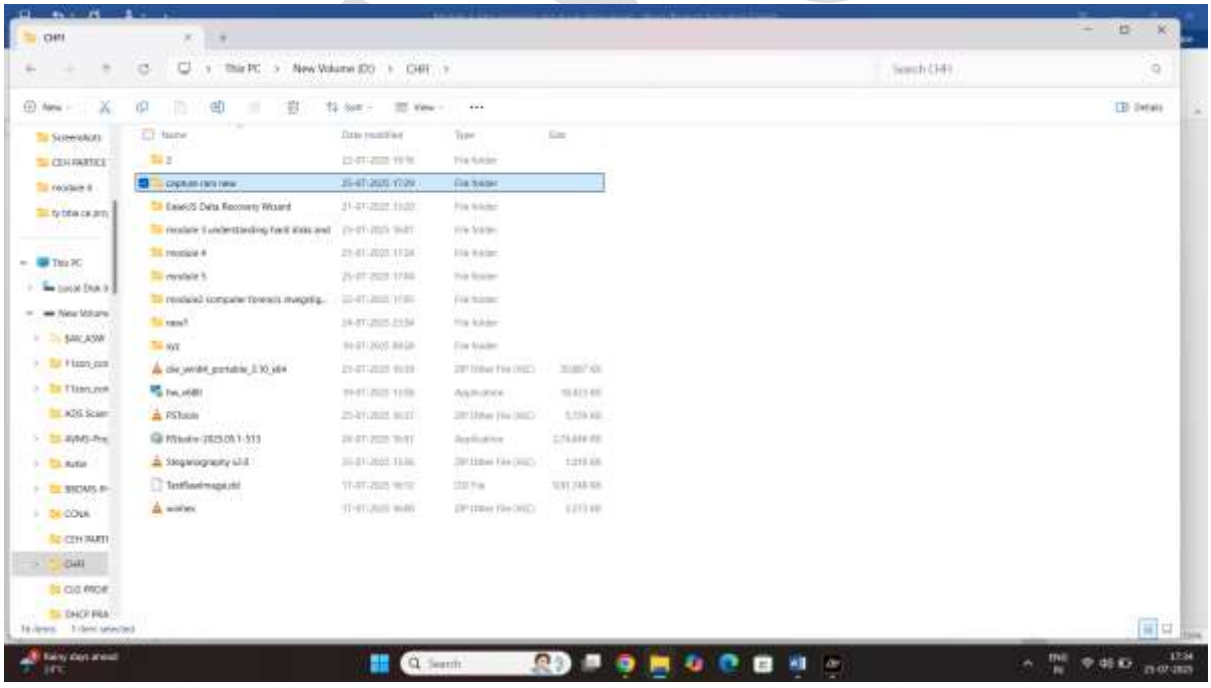




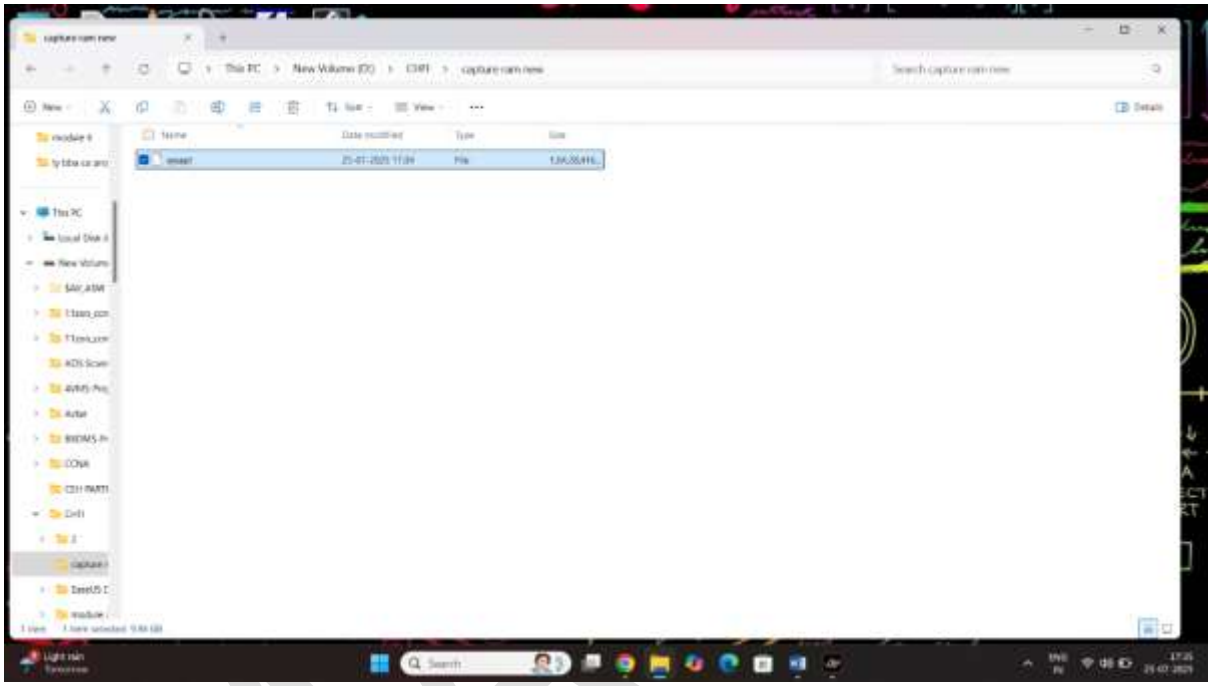
Step5 go to destination D drive and select the folder



Step6 Select the make folder for new ram capture



Click on file

Result:

Capture the ram store the file sysapt file because I am not open / and this file all ram sensitive data store in file