

NAME : SATHYAPRAKASH SAHOO

CLASS : BSC. TY. CS

ROLL NO : CS- 4124

DIV : 2 BATCH : C

SUBJECT : CYBER FORENSICS - PRACTICAL

PRACTICAL NO. 1

AIM : Creating a Forensic Image using FTK Imager.

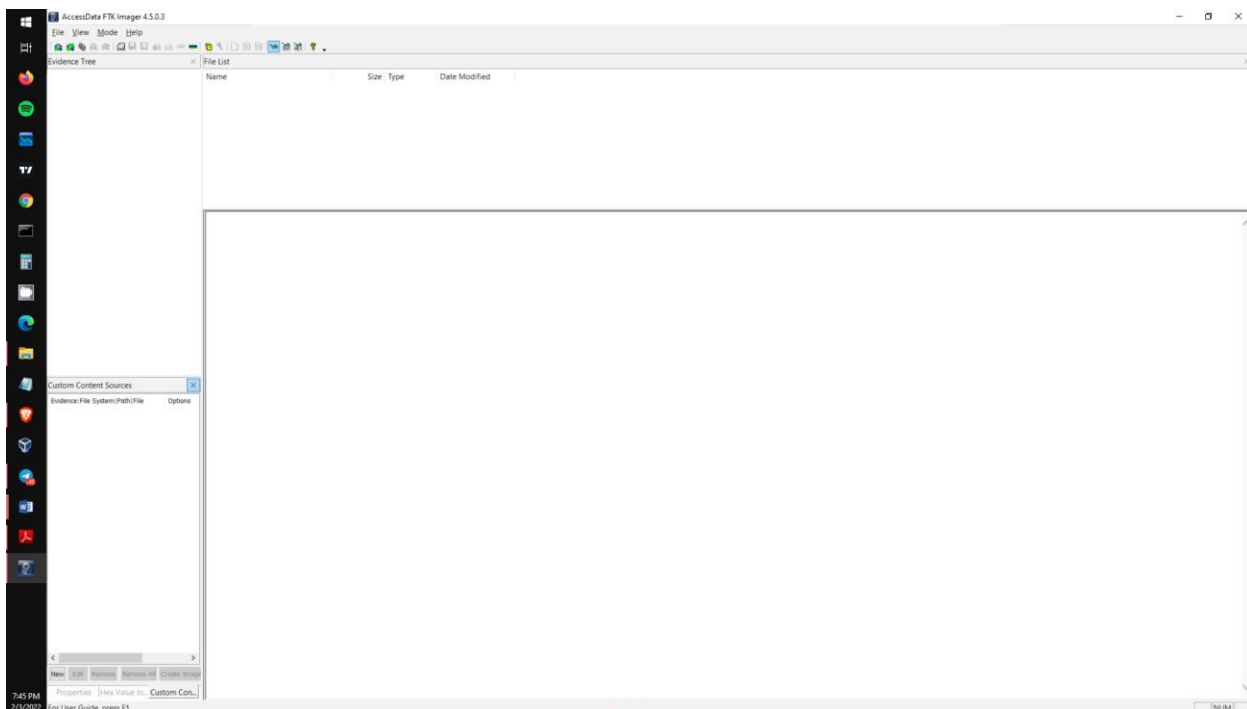
1. Creating Forensic Image.
2. Check Integrity of Data.
3. Analyze Forensic Image.

STEPS : follow the below steps -

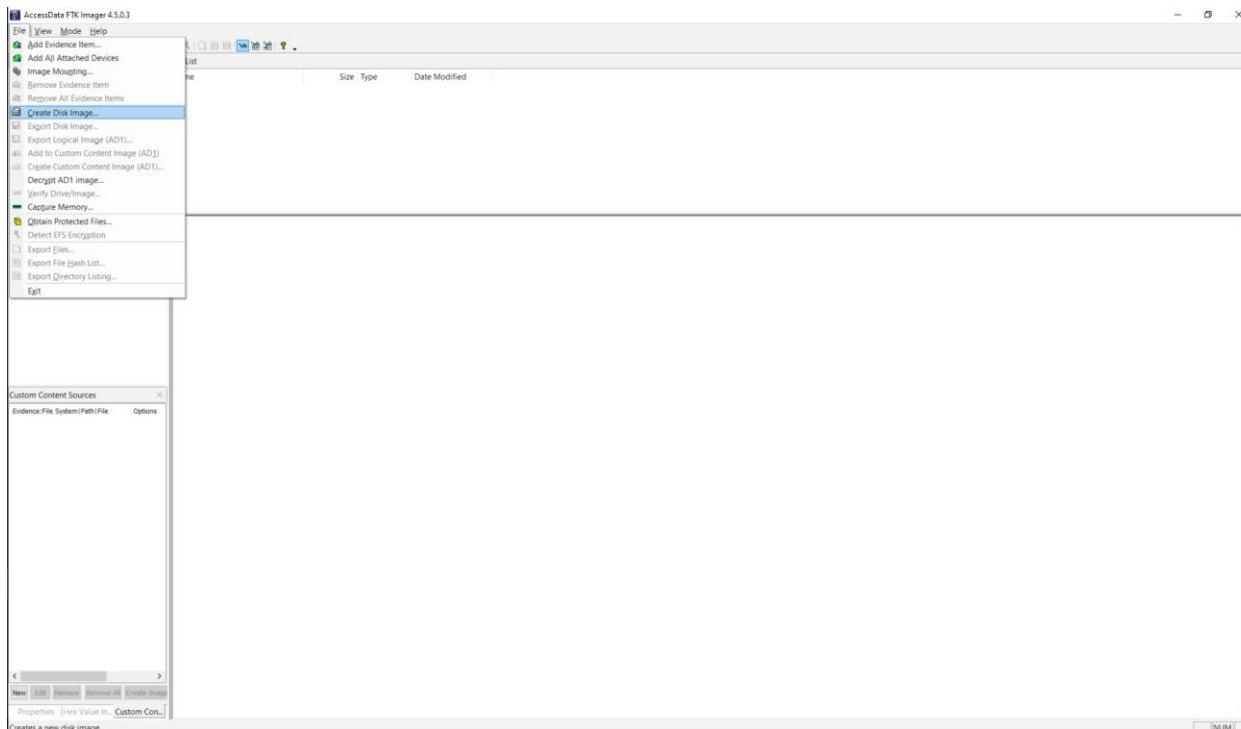
1. Creating Forensic Image

Step 1 :-Download FTK Imager from google chrome And install.

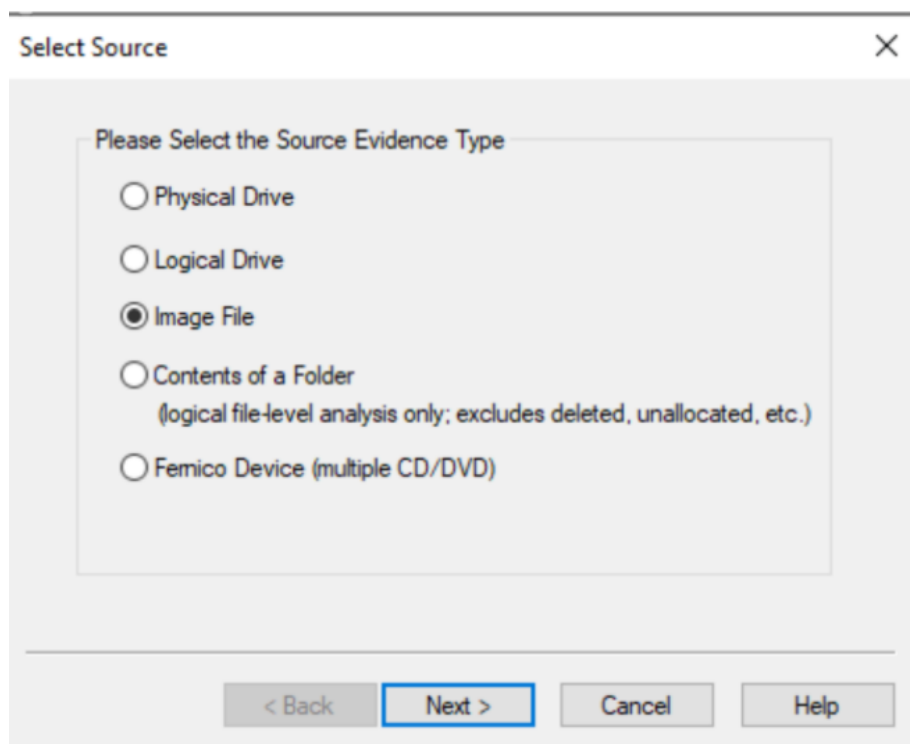
Step 2 :-Launch FTK Imager by clicking on the 'Access Data FTK Imager' icon.

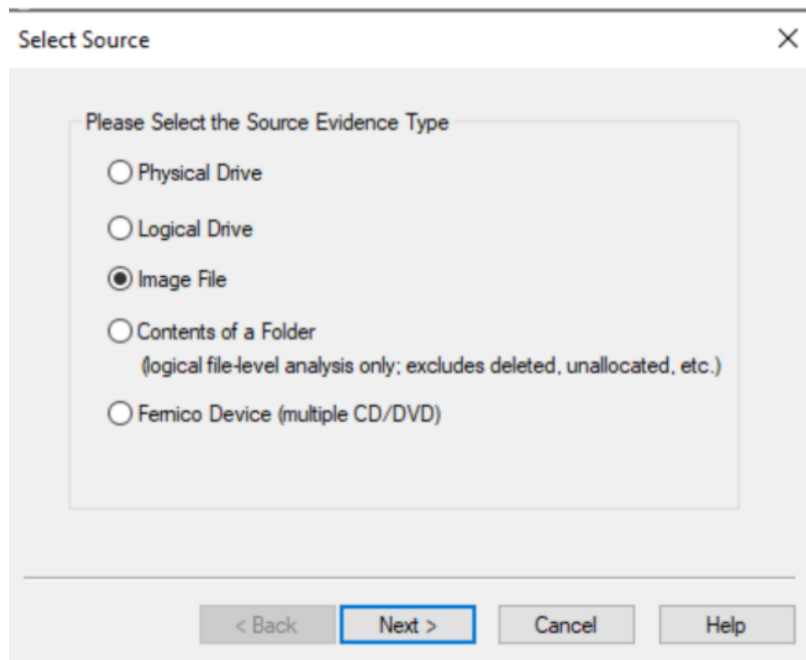


Step 3 :-Click file and look over the various options for creating images. We will be using 'Create Disk Image' option.



Step 4 :-Click 'Create Disk Image' . A window will appear.Click on Image file. Browse the source path of any file that you want to create a forensic image. Click Finish.





Step 5 :-Capture Image box will appear click on add and fill all the details about the image. I have entered :-

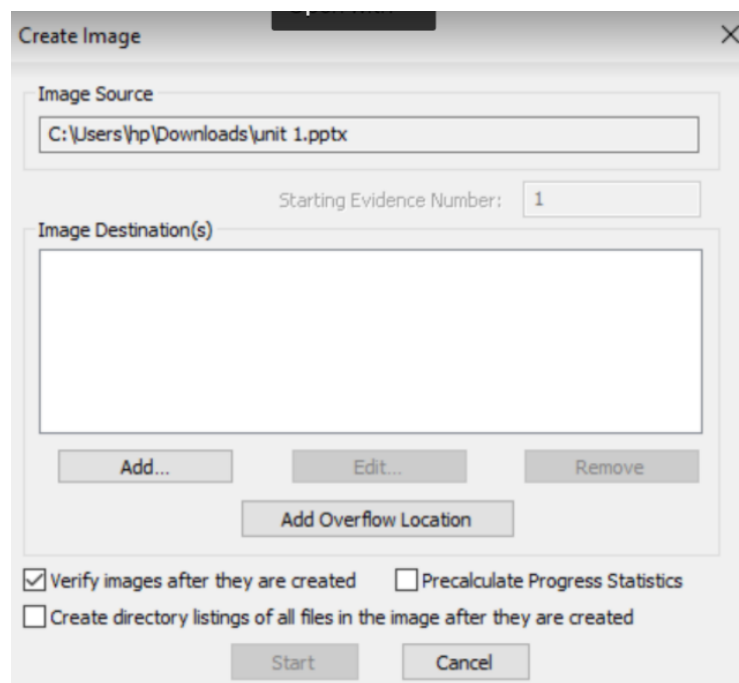
Case Number: 101.

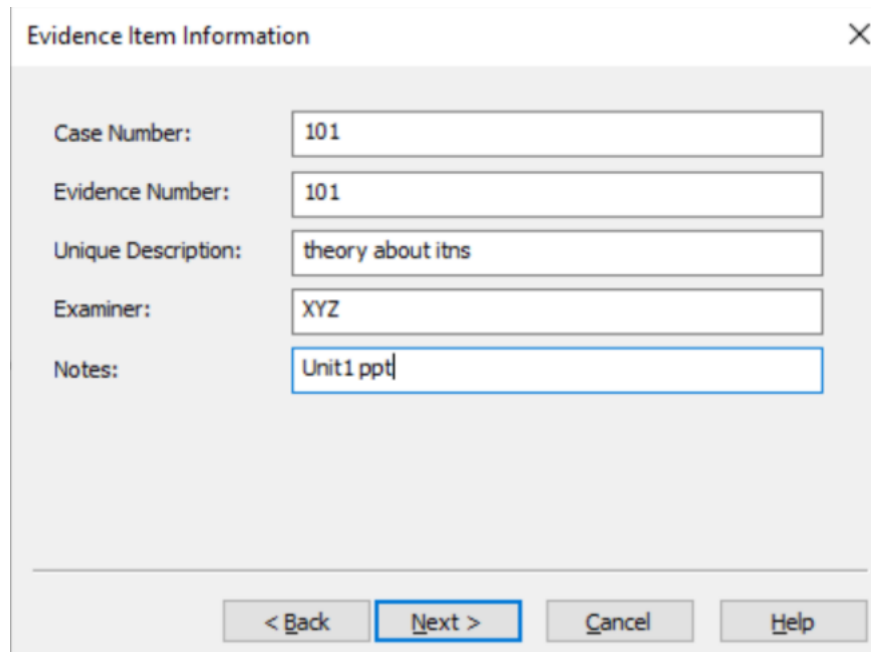
Evidence Number: 101.

Unique Description: Theory about ITNS.

Examiner: XYZ.

Notes: Unit1 ppt.





Evidence Item Information

Case Number: 101

Evidence Number: 101

Unique Description: theory about itns

Examiner: XYZ

Notes: Unit1 ppt

< Back Next > Cancel Help

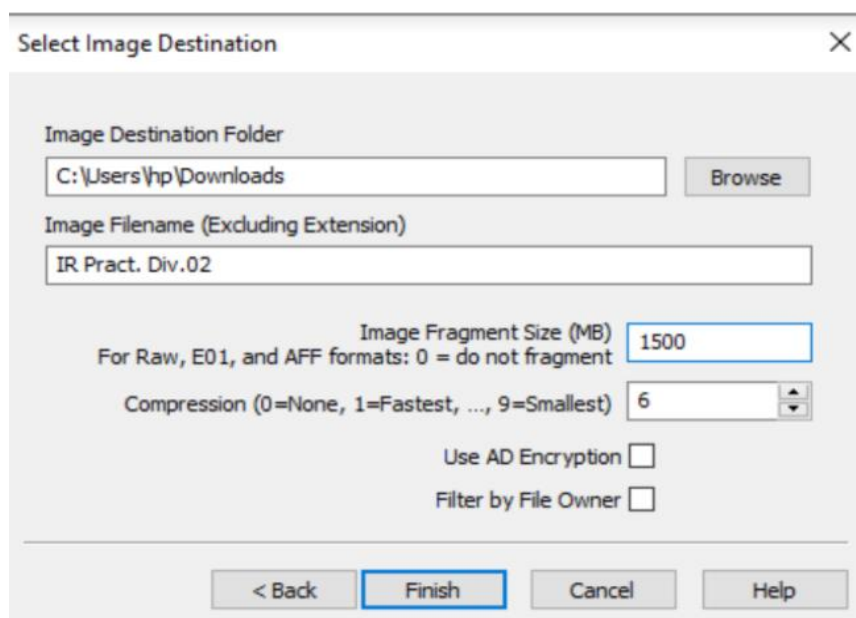
Step 6 :-Select Image Destination. Browse the image destination folder where you want to save the image.

Give name to that image.

Give Image_fragment size = 1500

Compression =6

Click on Finish.



Select Image Destination

Image Destination Folder
C:\Users\hp\Downloads Browse

Image Filename (Excluding Extension)
IR Pract. Div.02

Image Fragment Size (MB) 1500
For Raw, E01, and AFF formats: 0 = do not fragment

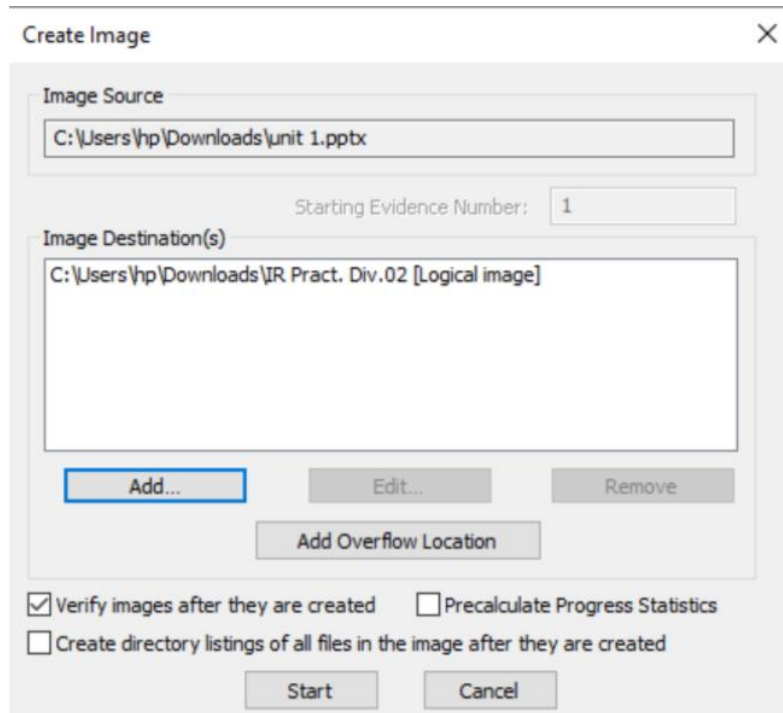
Compression (0=None, 1=Fastest, ..., 9=Smallest) 6

Use AD Encryption ☐

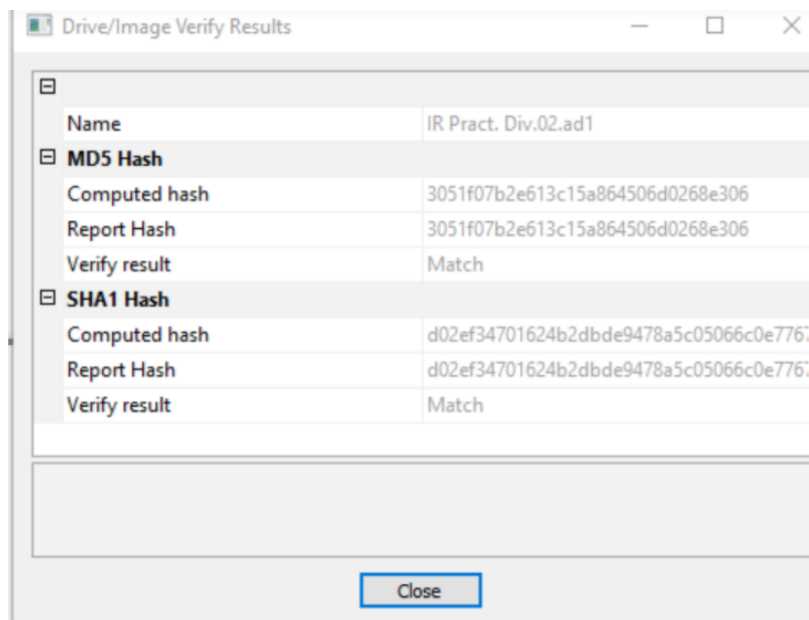
Filter by File Owner ☐

< Back Finish Cancel Help

Step 7 :-A window will appear. Click on “start”.The image will created.

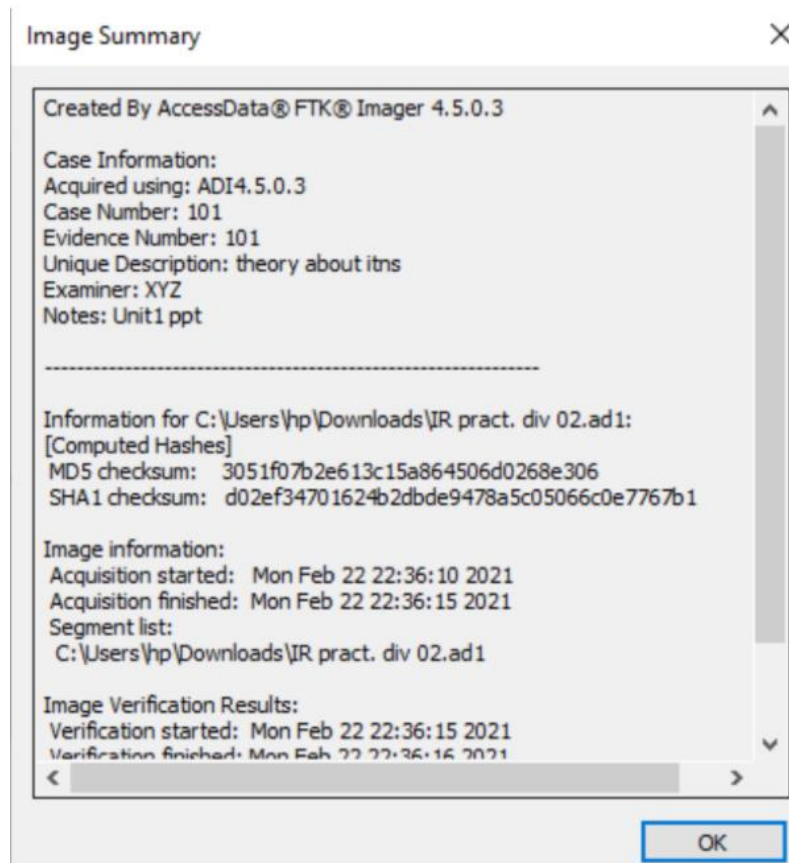


Step 8 :-The following window will appear once the image has been completed. Note that both MD5 and SHA1 hash have been created and verified.



2. Check Integrity of Data

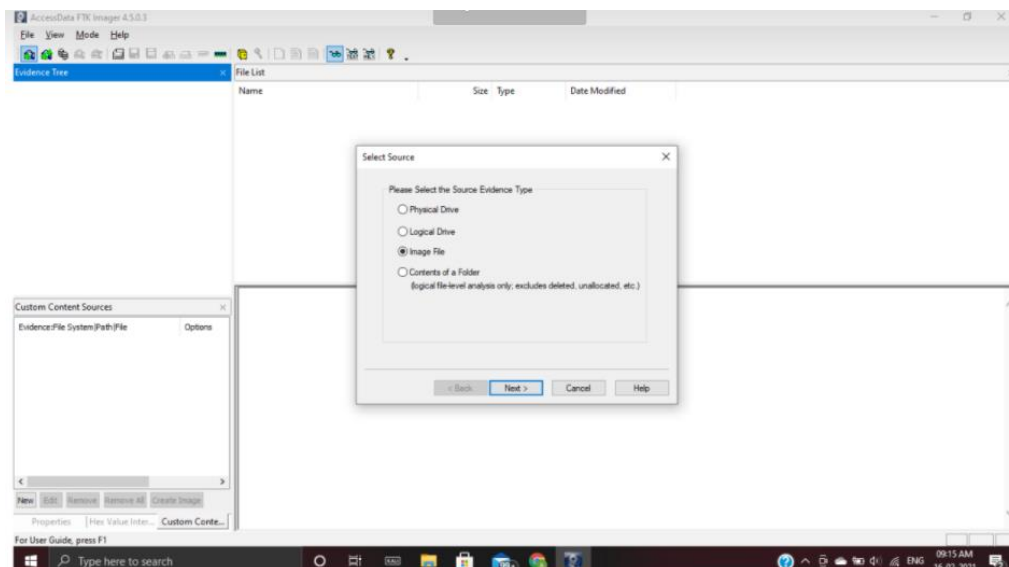
Step 9 :-Click on “Image summary” to view the following results pertaining to the image that has just been created.

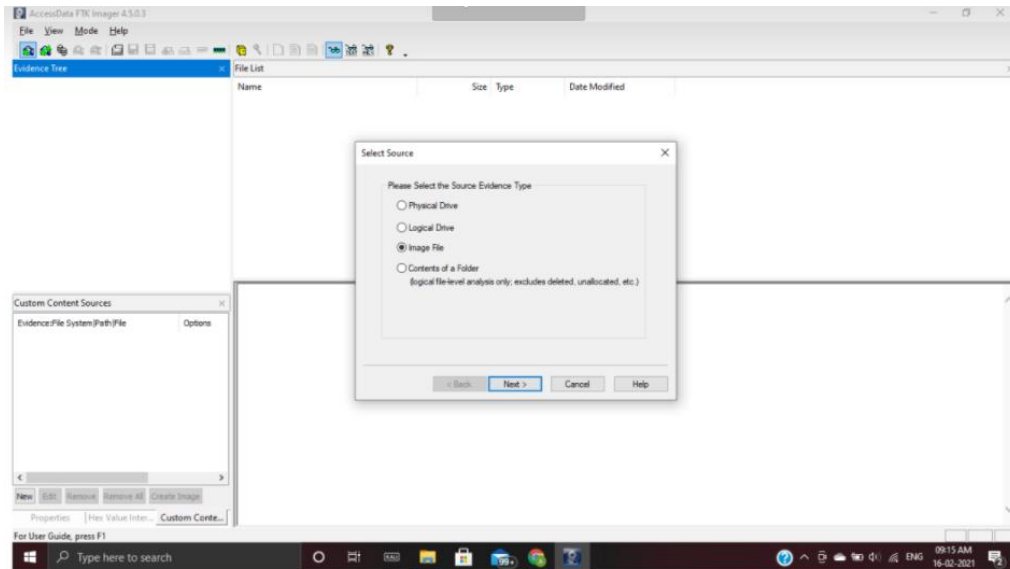


3. Analyze Forensic Image

Step 10 :- For analyzing forensic image, open FTK Imager, Click on “Add evidence Item”.

Click on “Image file”. Browse the source path of that image where you have stored it previously. Click on open. After click “finish”





Step 11 :- Here we can analyze the image.

