D. B. J. COLLEGE, CHIPLUN

Page No. : _____

DEPARTMENT OF COMPUTER SCIENCE

Expt. No.

Name : Piyush Pandurang Binate Class : TYCS Roll No.: 523

Title of Experiment : Creating a Forensic image using FTK Imager.

Date

Sub titles : Assignment/ Problem Solution, Flow chart/Algorithm, Problem Listing, Input Screen, Output Screen, Comments (If any)

Aim :- To study creating a forensic image using FTK Imager / Encase Imager :

- Creating Forensic Image
- Check integrity of data
- Analyze Forensic Image.

Software / Hardware Requirements :-

FTK imager, printer, computer.

Theory :-

Forensic Toolkit FTK is a computer forensics software made by Access Data.
It scans a hard drive looking for various information. It can for example locates deleted emails and scan a disk for text strings to be used them as a password dictionary to crack encryption.
The toolkit also includes a standalone disk imaging program called FTK imager.
The FTK imager is a simple but concise tool. It saves an image of a hard disk in one file or image of a hard disk in one file or in segments that way be later on reconstructed.

Remark

Signature

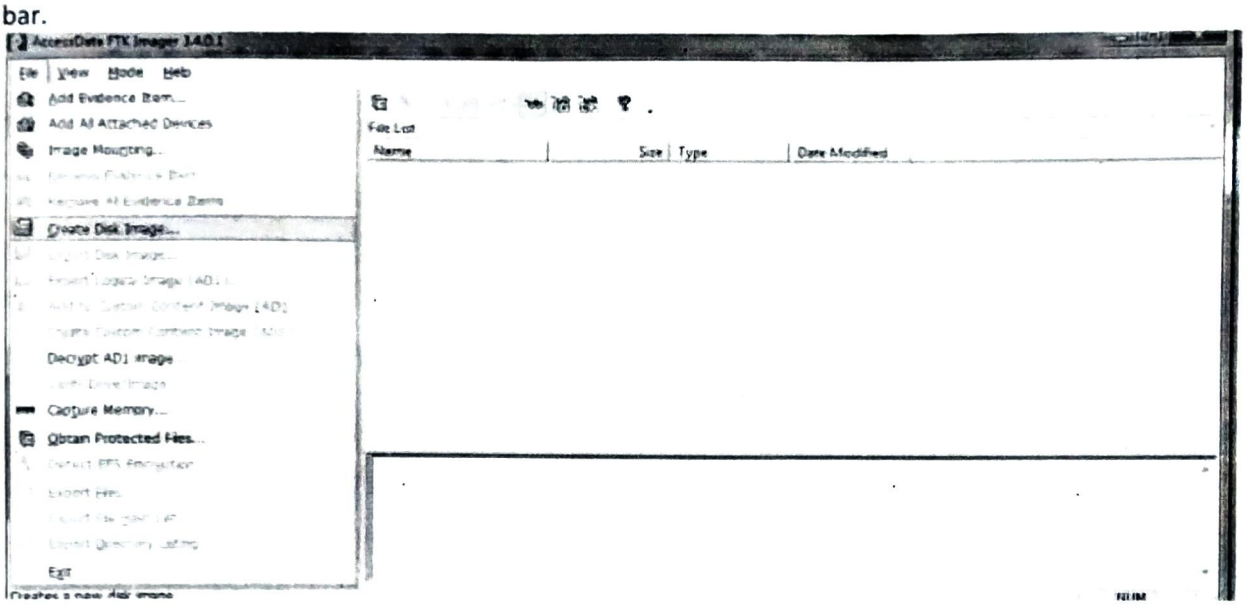
It calculates MD5 hash values and confirms the integrity of the data before closing the files. The result is an image file that can be saved in several formats including DD raw.

Conclusion :-

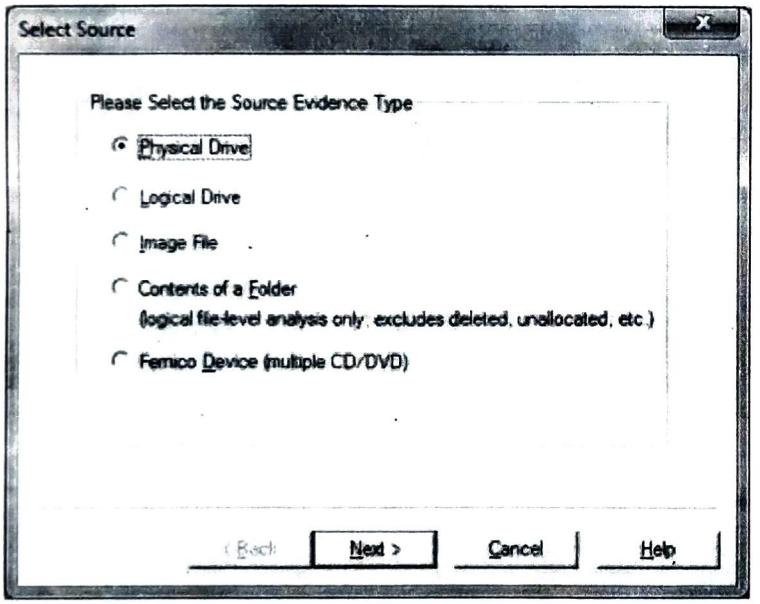
The given steps/program are done using FTK imager and its successful output basis been obtained.

Practical No – 1

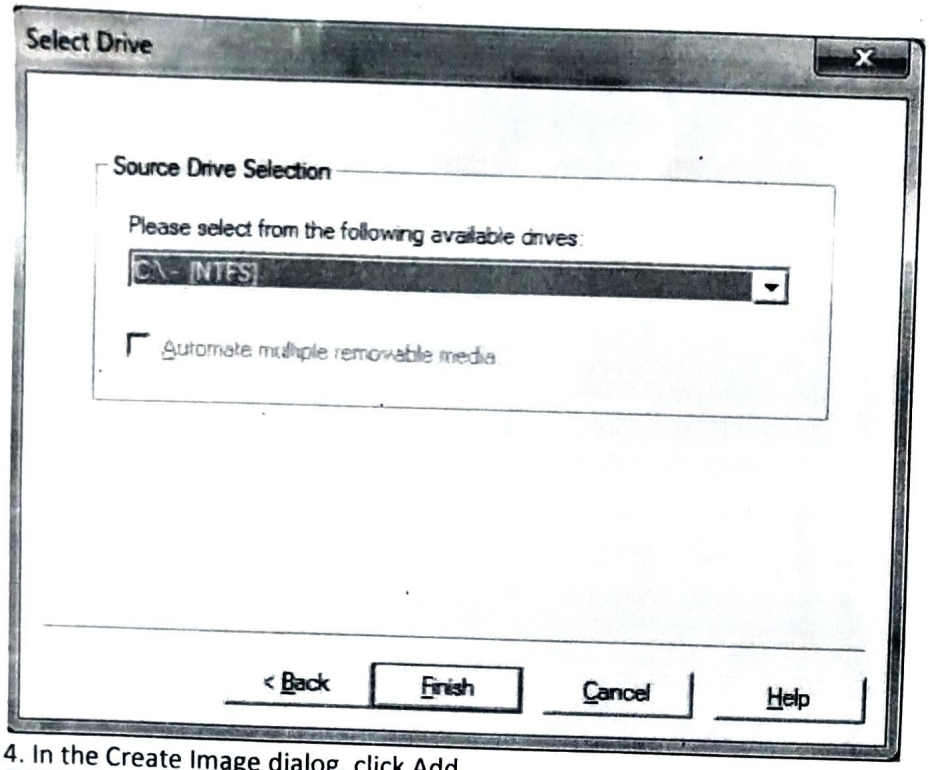
Steps: Creating Forensic Image 1. Click File, and then Create Disk Image, or click the button on the tool bar.



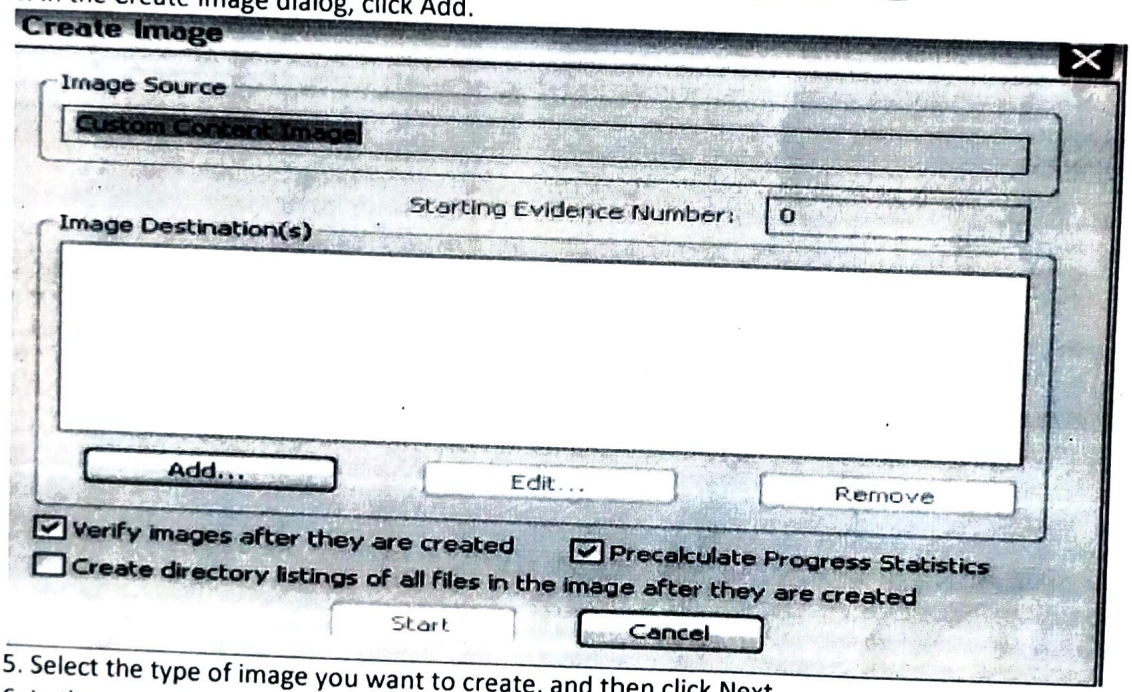
2. Select the source you want to make an image of and click Next.



3. Select the drive or browse to the source of the image you want, and then click Finish.

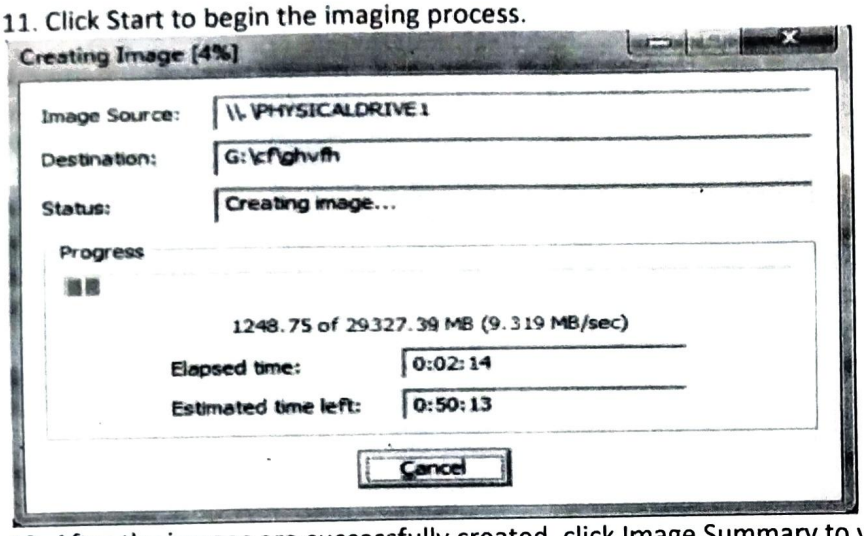


4. In the Create Image dialog, click Add.



5. Select the type of image you want to create, and then click Next
6. In the Image Destination Folder field, type the location path where you want to save the image file, or click Browse to find to the desired location'
7. In the Image Filename field, specify a name for the image file but do not specify a file extension. 8. In the Image Fragment Size field, specify the maximum size in MB for each fragment of the image file
9. Click Finish. You return to the Create Image dialog.
10. To add another image destination (i.e., a different saved location or image file type), click Add, and repeat steps 5– 10. To make changes to an image destination, select the destination you want to change and click Edit. To delete an image destination, select the destination and click Remove.

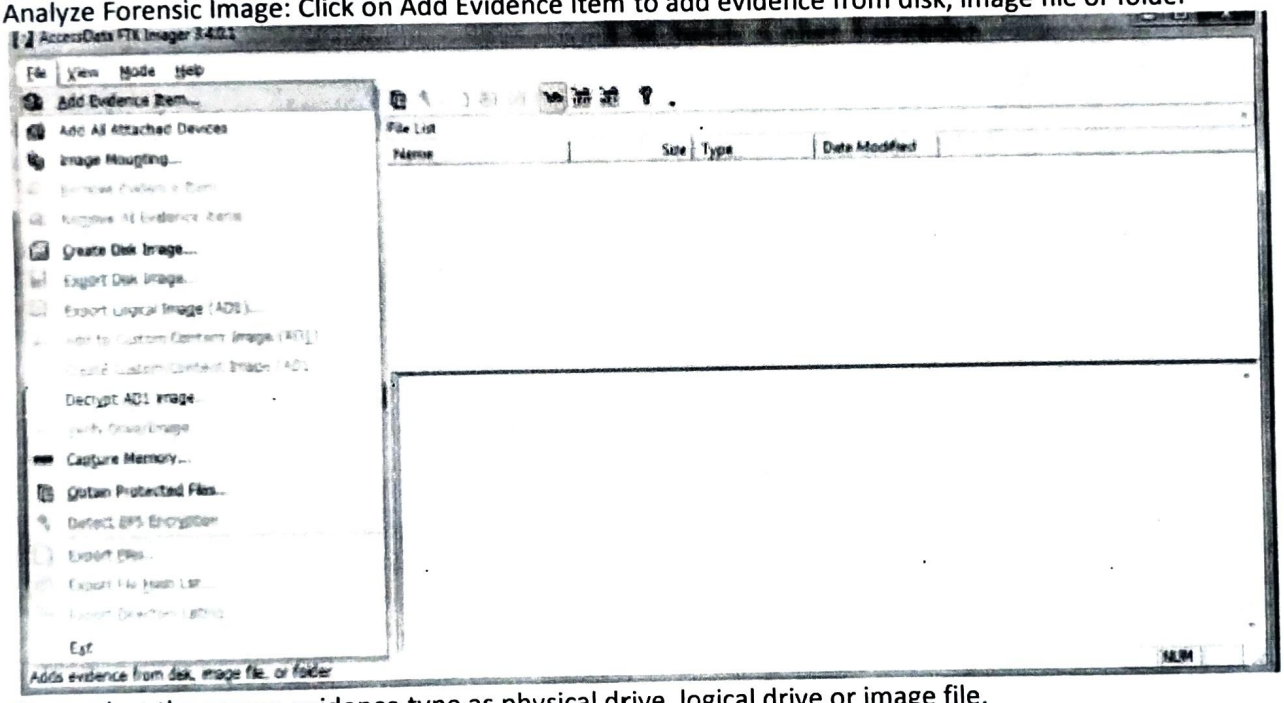
11. Click Start to begin the imaging process.



12. After the images are successfully created, click Image Summary to view detailed file information, including MD5 and SHA1 checksums.

13. When finished, click Close

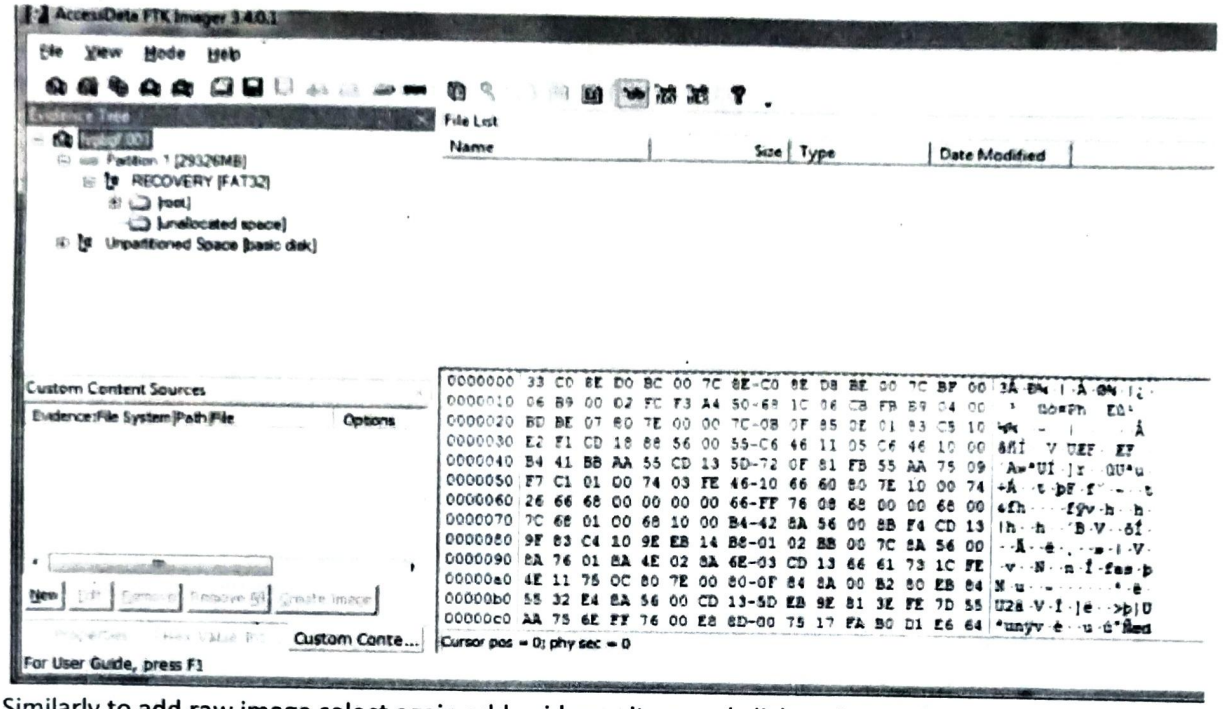
Analyze Forensic Image: Click on Add Evidence Item to add evidence from disk, image file or folder



Now select the source evidence type as physical drive, logical drive or image file.

Select virtual drive image & click on open option. Select the source path and click on finish.

Now select Evidence Tree and analyze the virtual disk as physical disk.



Similarly to add raw image select again add evidence item and click on image file and click on open option. Click on finish.