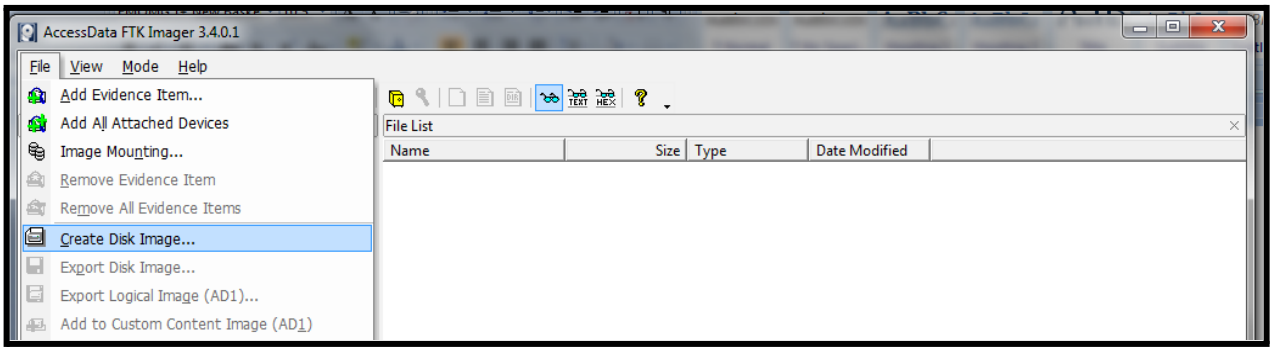
# Practical No. 01

**AIM** - Creating Forensic Images FTK Imager.

FTK Imager allows you to write an image file to a single destination or to simultaneously write multiple image files to multiple destinations.

## To Create a Forensic Image (FTK Imager) -

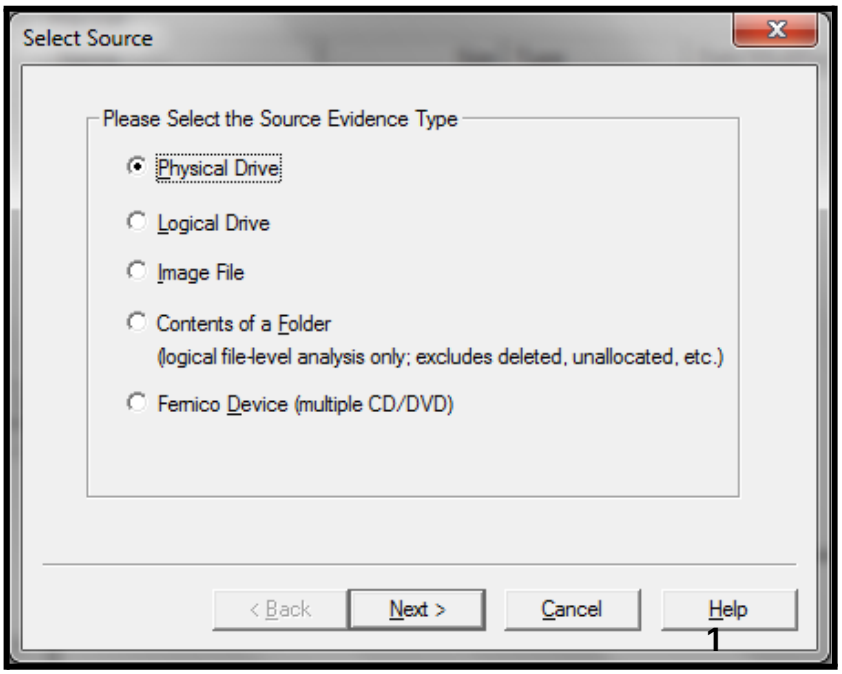
1. Click "**File**", and then Create Disk Image, or click the button on the Toolbar.



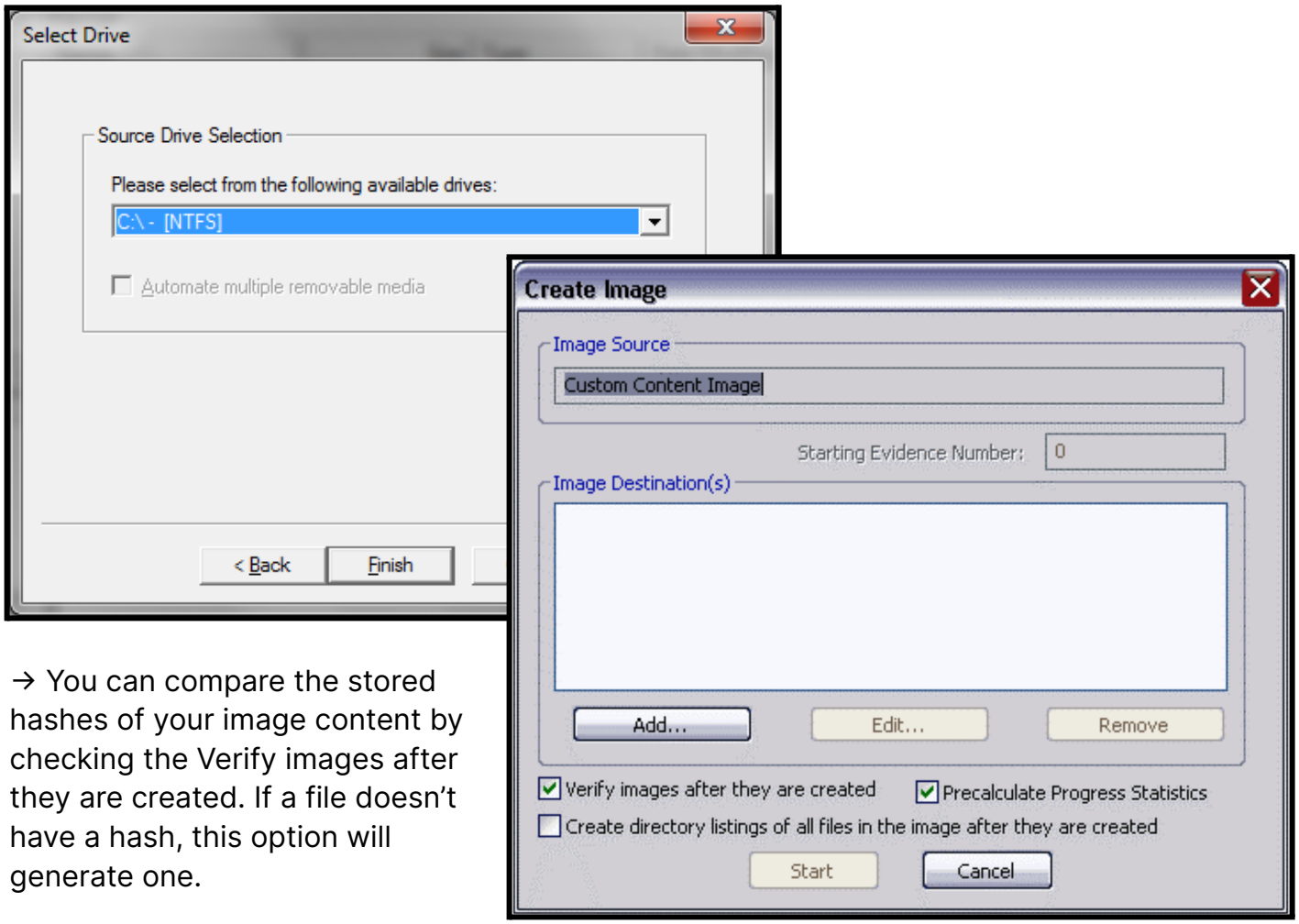

2. Select the source you want to make an image of and Click Next.

NOTE →

If you select Logical Drive to select a floppy or CD as a source, you can check the Automate multiple removable media box to create groups of images. Imager will automatically increment the case numbers with each image, and if something interrupts the process, you may assign the case number manually.



3. Select the Drive OR Browse to the source of image you want → "**Finish**" → Create Image Dialog → "**Add**"

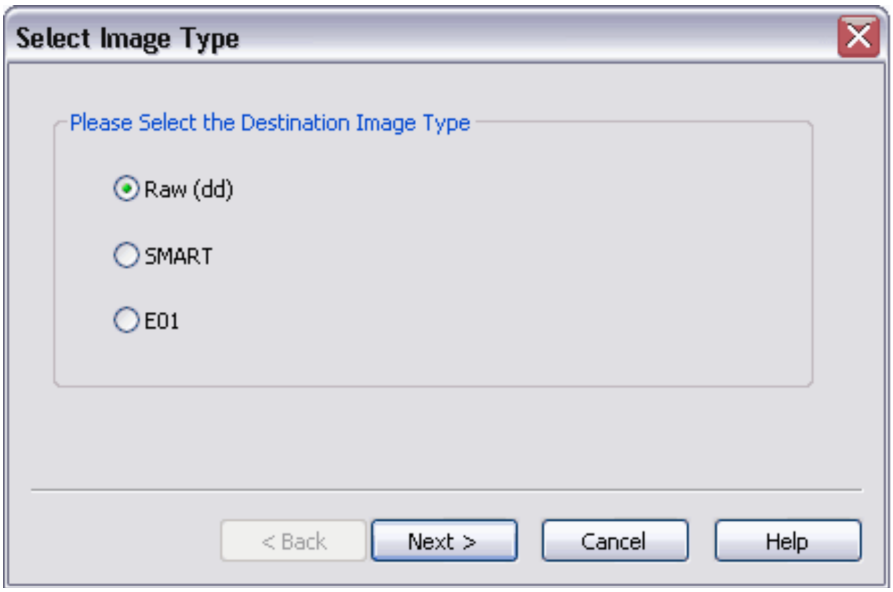



→ You can compare the stored hashes of your image content by checking the Verify images after they are created. If a file doesn't have a hash, this option will generate one.

→ You can list the entire contents of your images with path, creation dates, whether files were deleted, and other metadata. The list is saved in a tab-separated value format.

4. Select the type of image you want to create, and then click Next.

   **NOTE** → If you are creating an image of a CD or DVD, this step is skipped because all CD/DVD images are created in the ISOBuster CUE format.




The raw image type is not compressed. If you select the Raw (dd) type, be sure to have adequate space for the resulting image.

If you select SMART or E01 as the image type, complete the fields in the Evidence Item Information dialog, and click Next.

Raw (dd): This is the image format most commonly used by modern analysis tools. These raw file formatted images do not contain headers, metadata, or magic values. The raw format typically includes padding for any memory ranges that were intentionally skipped (i.e., device memory) or that could not be read by the acquisition tool, which helps maintain spatial integrity (relative offsets among data).

SMART: This file format is designed for Linux file systems. This format keeps the disk images as pure bitstreams with optional compression. The file consists of a standard 13-byte header followed by a series of sections. Each section includes its type string, a 64-bit offset to the next section, its 64-bit size, padding, and a CRC, in addition to actual data or comments, if applicable.

E01: this format is a proprietary format developed by Guidance Software's EnCase. This format compresses the image file. An image with this format starts with case information in the header and footer, which contains an MD5 hash of the entire bit stream. This case information contains the date and time of acquisition, examiner's name, special notes and an optional password.

AFF: Advance Forensic Format (AFF) was developed by Simson Garfinkel and Basis Technology. Its latest implementation is AFF4. The goal is to create a disk image format that does not lock the user into a proprietary format that may prevent them from being able to properly analyze it.

5. In the Image Destination Folder field, type the location path where you want to save the image file, or click Browse to find the desired location.

   NOTE → If the destination folder you select is on a drive that does not have sufficient free space to store the entire image file, FTK Imager prompts for a new destination folder when all available space has been used in the first location.

6. In the Image Filename field, specify a name for the image file but do not specify a file extension.

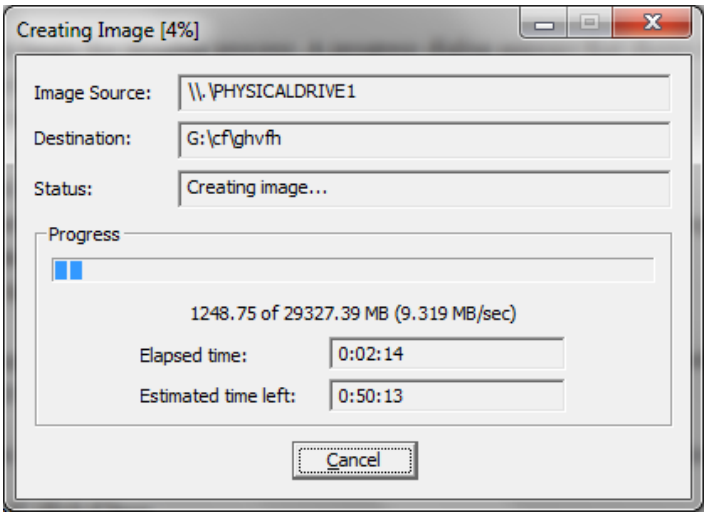
7. In the Image Fragment Size field, specify the maximum size in MB for each fragment of the image file. The s01 format is limited by design to sizes between 1 MB and 2047 MB (2 GB). Compressed block pointers are 31- bit numbers (the high bit is a compressed flag), which limits the size of any one segment to two gigabytes.

   TIP → If you want to transfer the image file to CD, accept the default fragment size of 650 MB.

8. Click "**Finish**" You return to the Create Image dialog.

9. 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**".

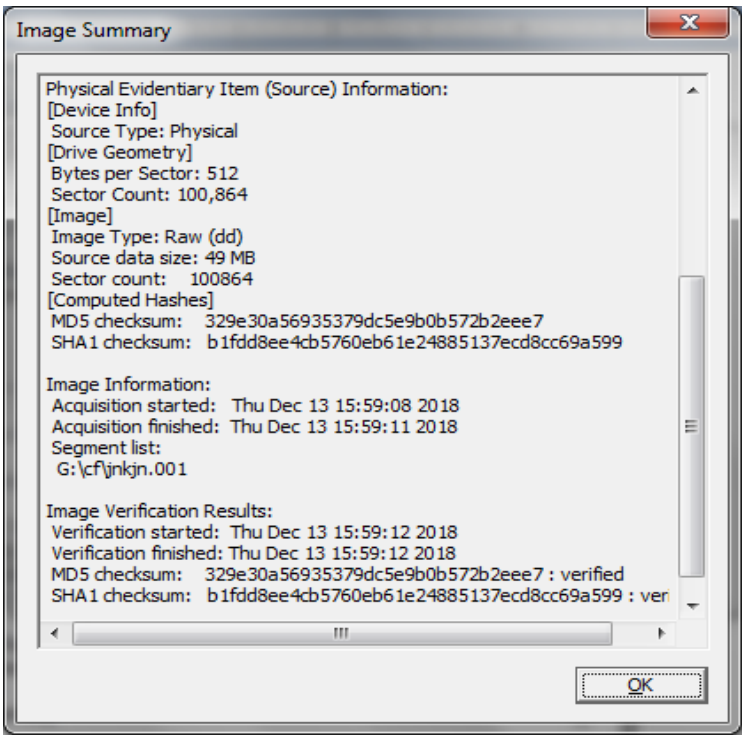
10. Click Start to begin the imaging process. A progress dialog appears that shows the following →




- The source that is being imaged.
- The location where the image is being saved.
- The status of the imaging process.
- A graphical progress bar.
- The amount of data in MB that has been copied and the total amount to be copied.
- Elapsed time after the imaging process began.
- Estimated time left until the process is complete.

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

**NOTE** → This option is available only if you created an image file of a physical or logical drive.

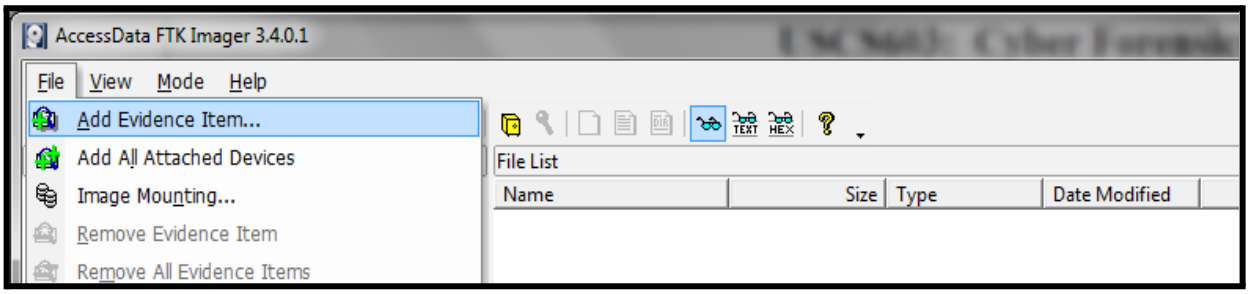



12. When finished, click "**Close**".

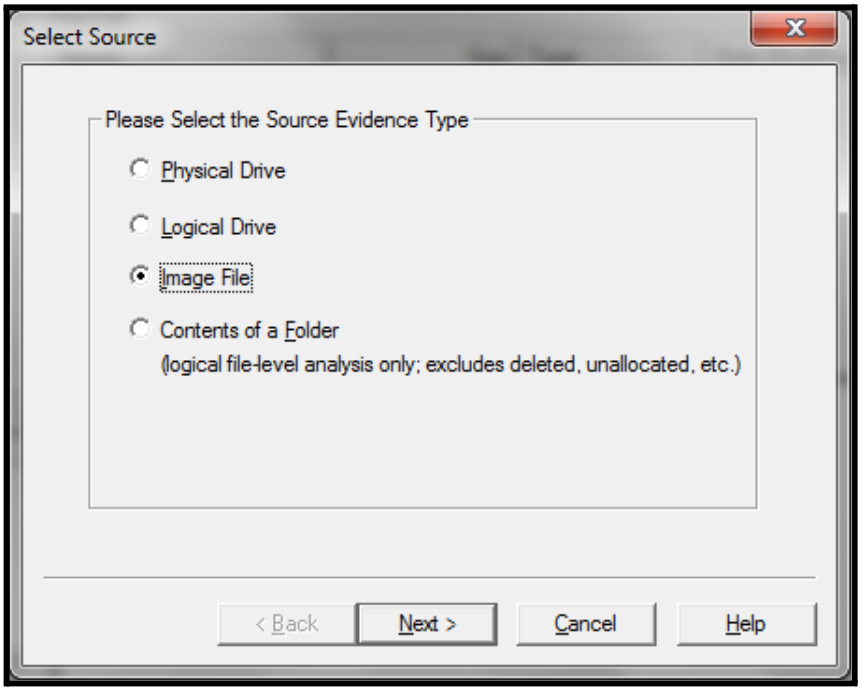
**NOTE** → The image file (*.001) as well as the image summary file from above (*.txt) have been saved onto the 'Drive'. The .001 extension may be left as is, or can be changed to .dd. The .001 extension is used due to the fact that many times the file to be imaged is very large and must be split into multiple chunks. In that case, you would have *.001, *.002, etc.

## Analyze Forensic Image -

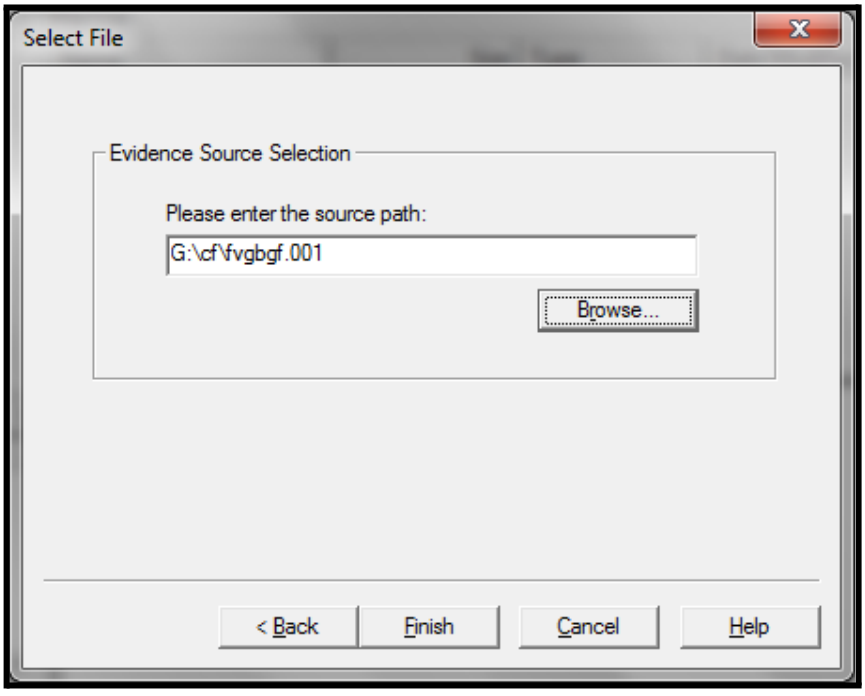
13. Click on Add Evidence Item to add evidence from disk, image file or folder.



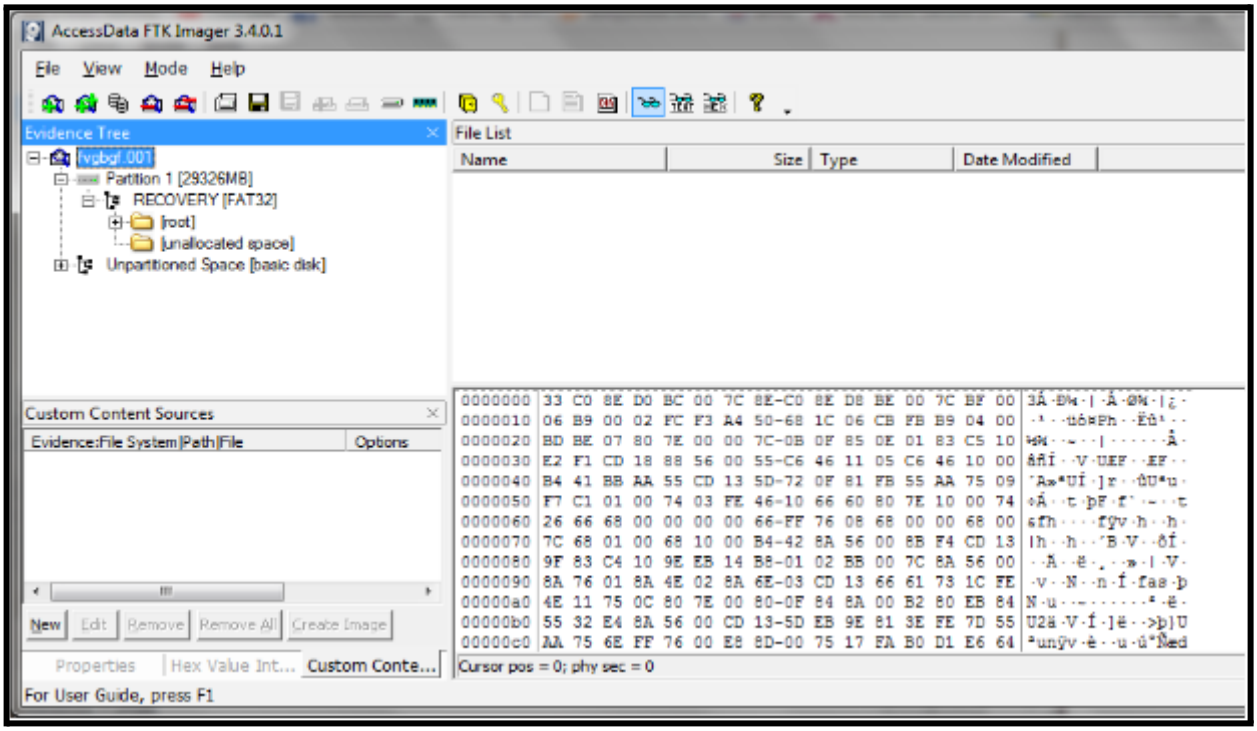
14. Now select the source evidence type as physical drive, logical drive or image file. We have selected the image file and clicked on "**Next**".




15. Virtual Drive Image → Open → Select the Source Path → Finish.



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




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

18. Now raw images will be added as a physical drive to analyze.