

3 Shital Divekar

Aim: Creating a Forensic Image using FTK Imager/Encase Imager.

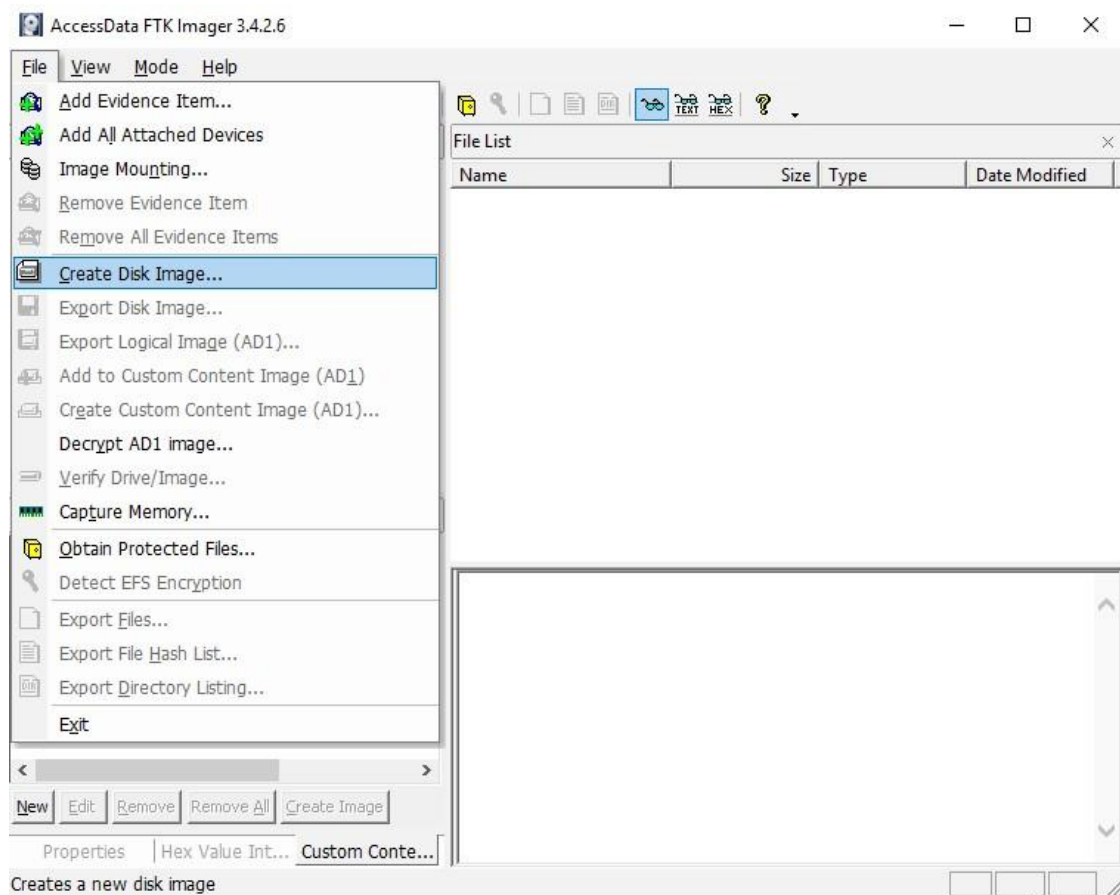
Info: FTK Imager is a data preview and imaging tool used to acquire data (evidence) in a forensically sound manner by creating copies of data without making changes to the original evidence.

Steps:

- Creating Forensic Image
- Check Integrity of Data
- Analyse Forensic Image

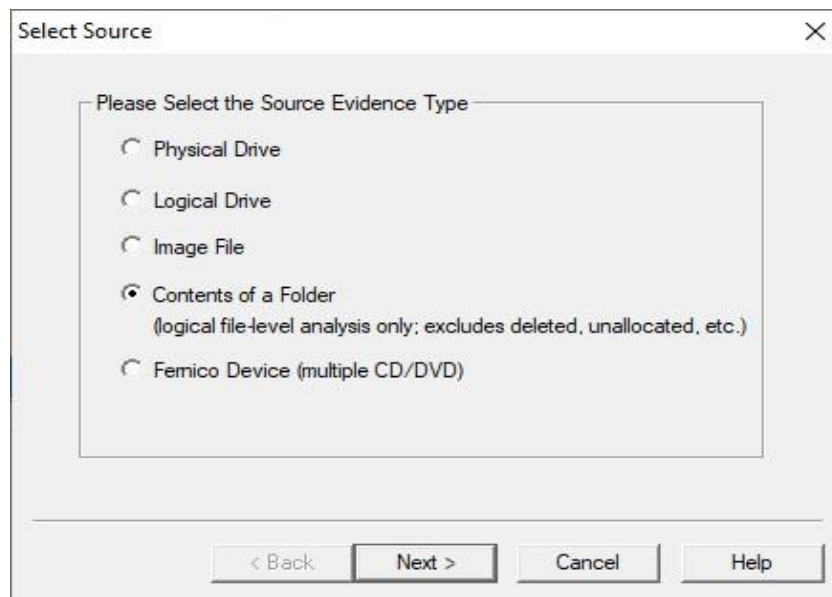
➤Creating Forensic Image

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

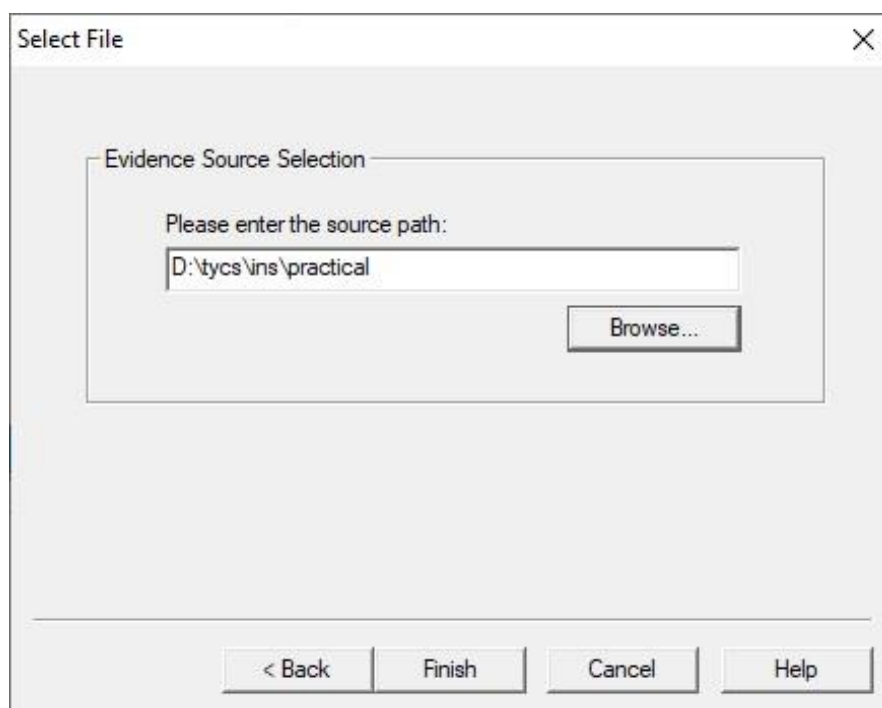


2. Select the source evidence type you want to make an image of and click Next.

3 Shital Divekar

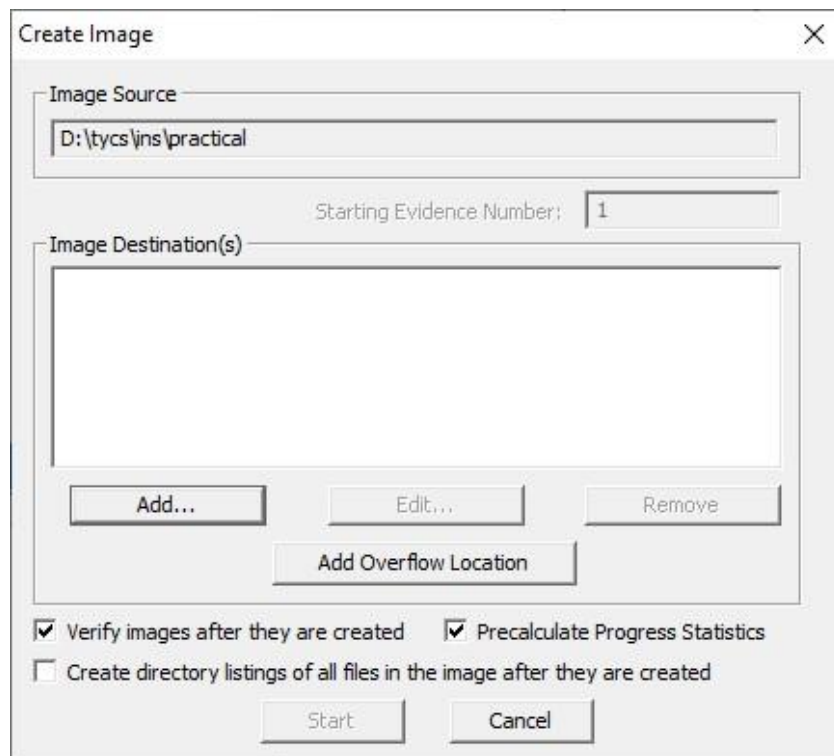


3. Select the source evidence file with path .

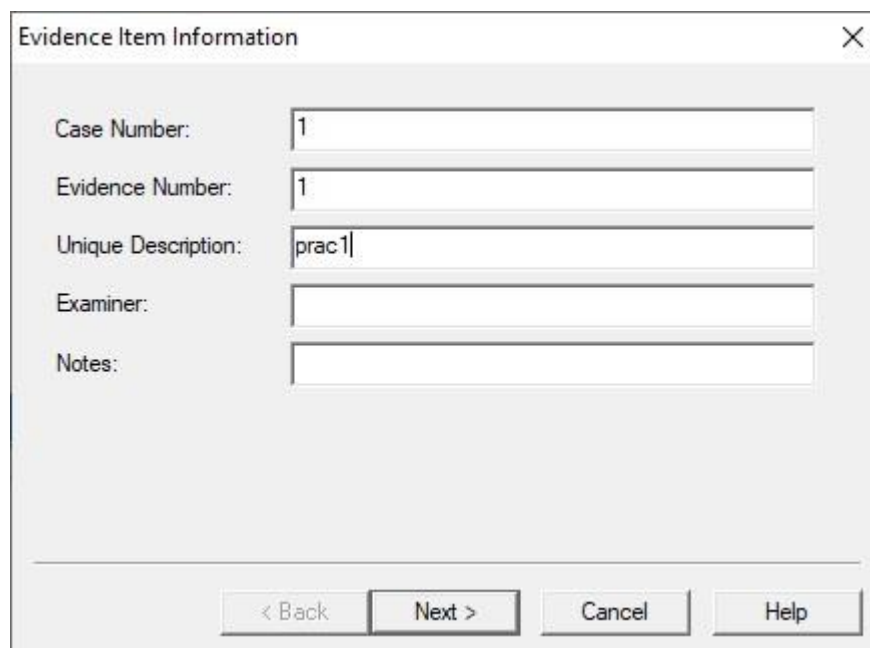


Click on “add” to add image destination

3 Shital Divekar



The 'Create Image' dialog box is used to configure the creation of a new image file. It features a close button (X) in the top right corner. The 'Image Source' field contains the path 'D:\tycs\jns\practical'. The 'Starting Evidence Number' is set to '1'. The 'Image Destination(s)' section includes a large empty text area for specifying the destination path, with buttons for 'Add...', 'Edit...', 'Remove', and 'Add Overflow Location' below it. At the bottom, there are three checkboxes: 'Verify images after they are created' (checked), 'Precalculate Progress Statistics' (checked), and 'Create directory listings of all files in the image after they are created' (unchecked). 'Start' and 'Cancel' buttons are located at the very bottom.

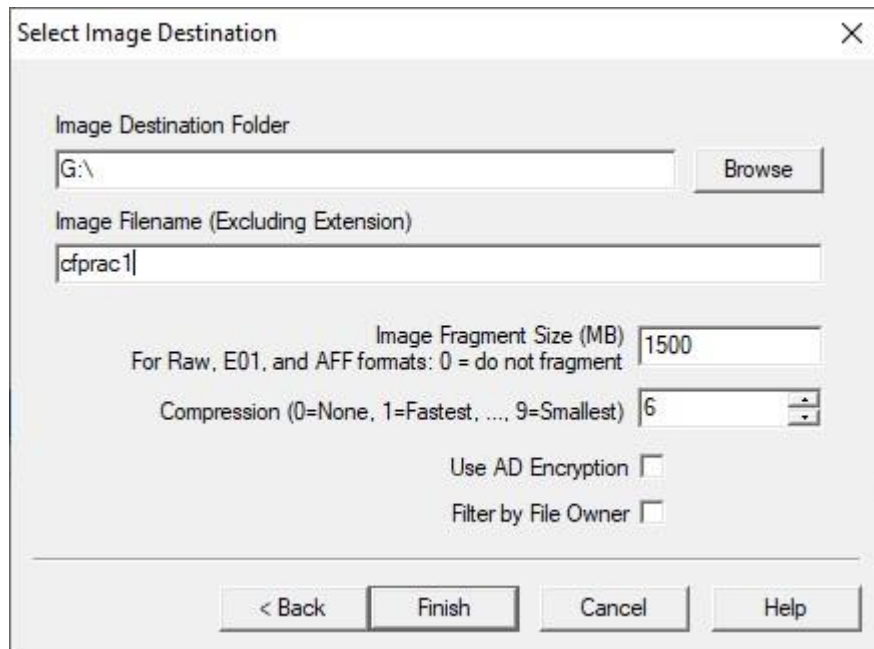


The 'Evidence Item Information' dialog box is used to enter details about the evidence item. It has a close button (X) in the top right corner. The fields are: 'Case Number' (1), 'Evidence Number' (1), 'Unique Description' (prac1), 'Examiner' (empty), and 'Notes' (empty). At the bottom, there are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'.

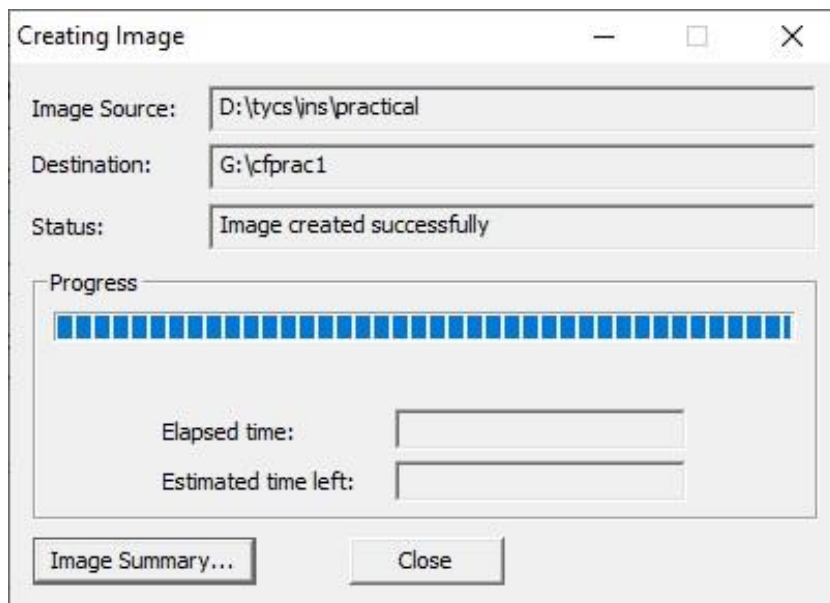
4. In the Image Destination Folder field, type the location path where you want to save the image file, or click **Browse** to find to the desired location.

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

3 Shital Divekar

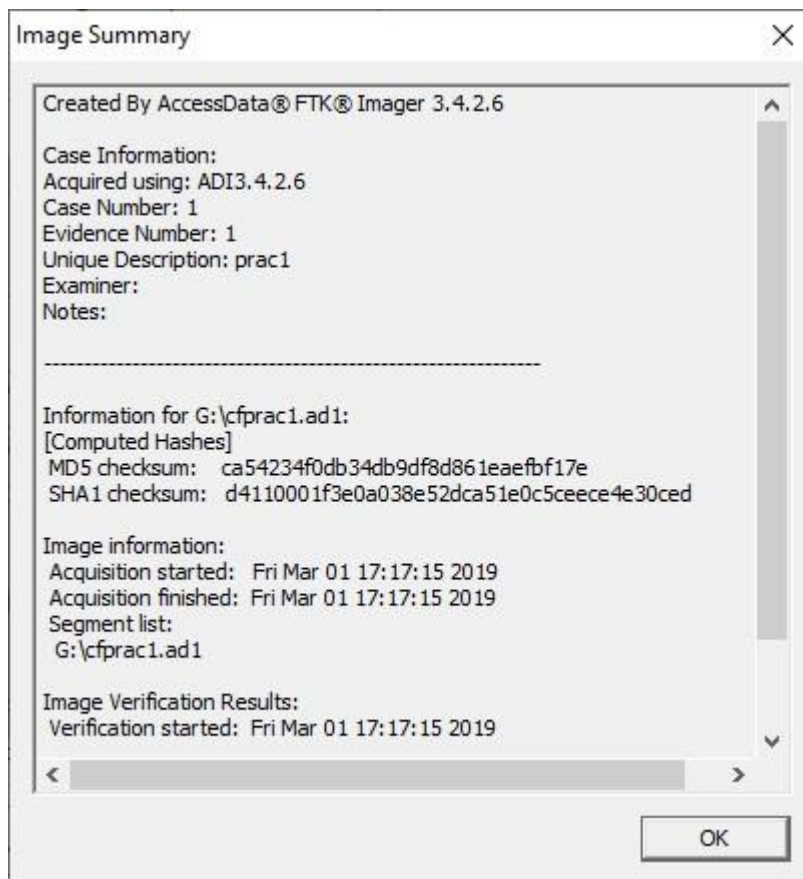


5. After adding the image destination path click on finish and start the image processing.



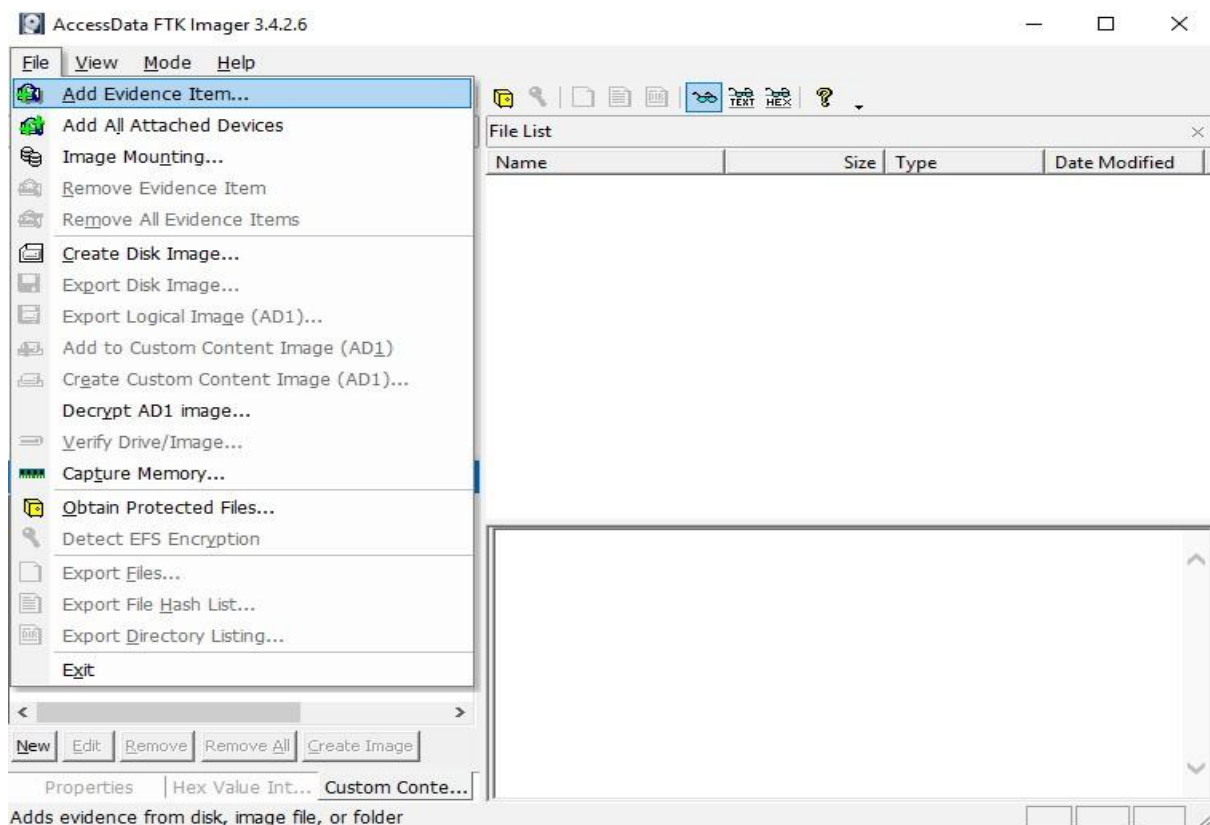
6. After the images are successfully created, click Image Summary to view detailed file information, including MD5 and SHA1 checksums.

3 Shital Divekar



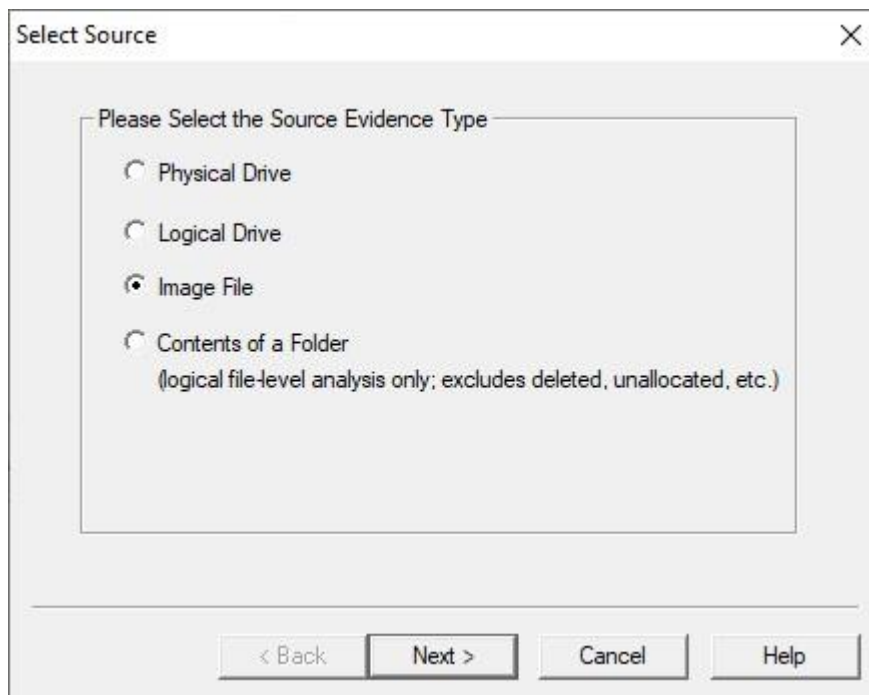
Analyze Forensic Image:

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

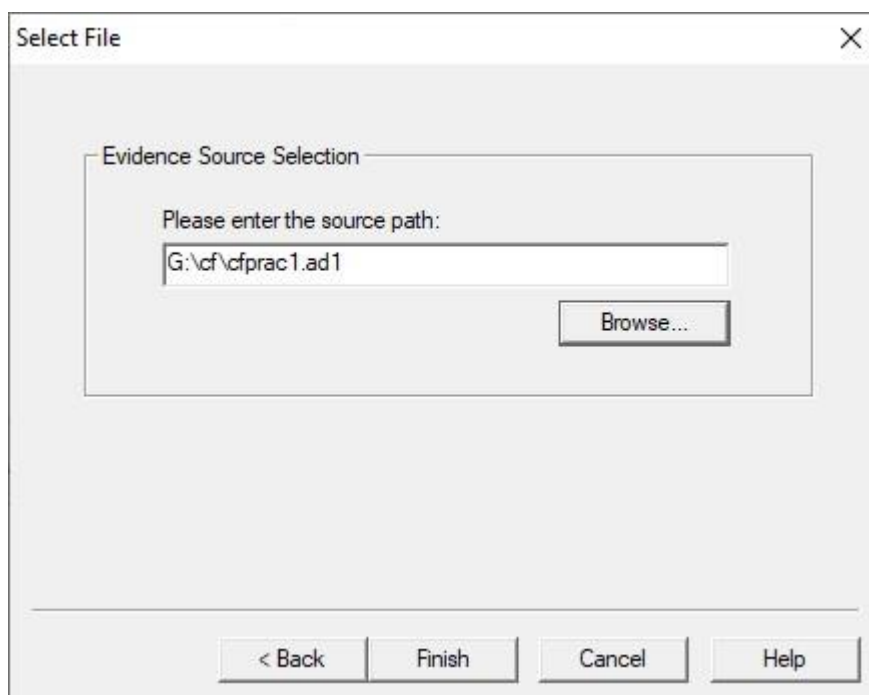


3 Shital Divekar

Now select the source evidence type as image file.



Open the created evidence image file



Now select Evidence Tree and analyze the image file .

3 Shital Divekar

