EXPERIMENT NO : 03 (i)

Analysis of forensic images using open-source tool - FTK Imager

Aim: To perform Analysis of forensic images using open-source tool - FTK Imager

Theory:

A Forensic Image is most often needed to verify the integrity of the image after an acquisition of a Hard Drive has occurred. This is usually performed by law enforcement for court because, after a forensic image has been created, its integrity can be checked to verify that it has not been tampered with. Forensic Imaging is defined as the processes and tools used in copying an electronic media such as a hard-disk drive for conducting investigations and gathering evidence that will be presentable in the law of court. This copy not only includes files that are visible to the operating system but every bit of data, every sector, partition, files, folders, master boot records, deleted files, and unallocated spaces. The image is an identical copy of all the drive structures and contents.

Further, a forensic image can be backed up and/or tested on without damaging the original copy or evidence.

Also, you can create a forensic image from a running or dead machine. It is a literal snapshot in time that has integrity checking.

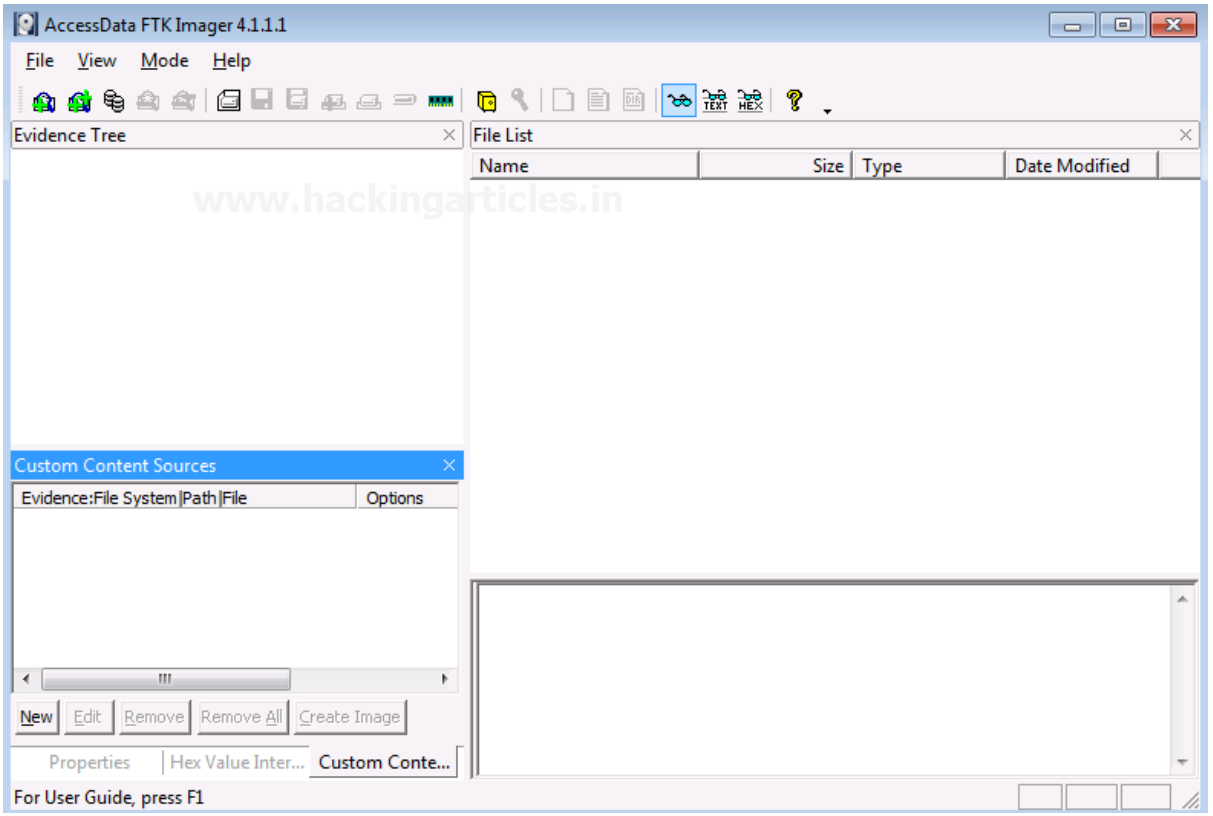
What Is FTK Imager?

FTK Imager is a tool for creating disk images and is absolutely free to use. It was developed by The Access Data Group. It is a tool that helps to preview data and for imaging.

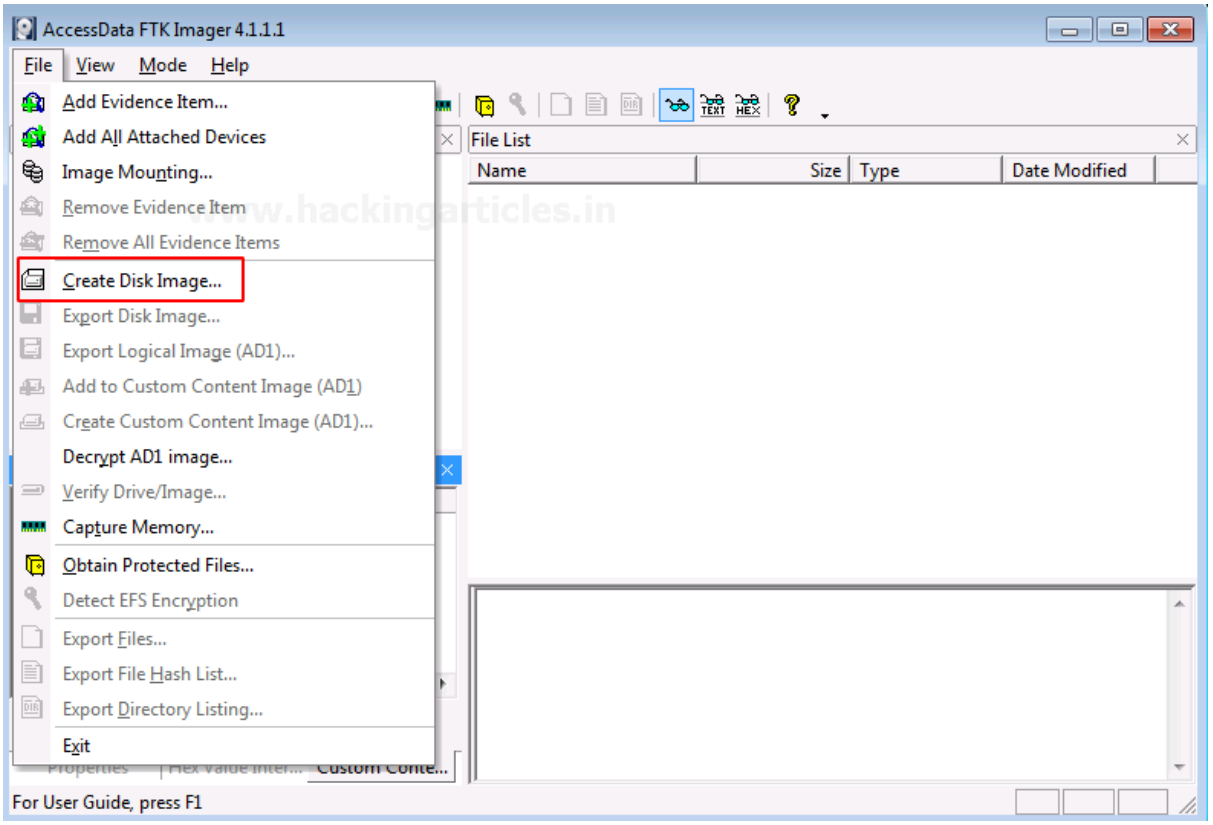
To create a forensic image with FTK imager, we will need the following:

1. FTK Imager from Access Data, which can be downloaded using the following link: FTK Imager from Access Data
2. A Hard Drive that you would like to create an image of.

Open FTK Imager by AccessData after installing it, and you will see the window pop-up which is the first page to which this tool opens.

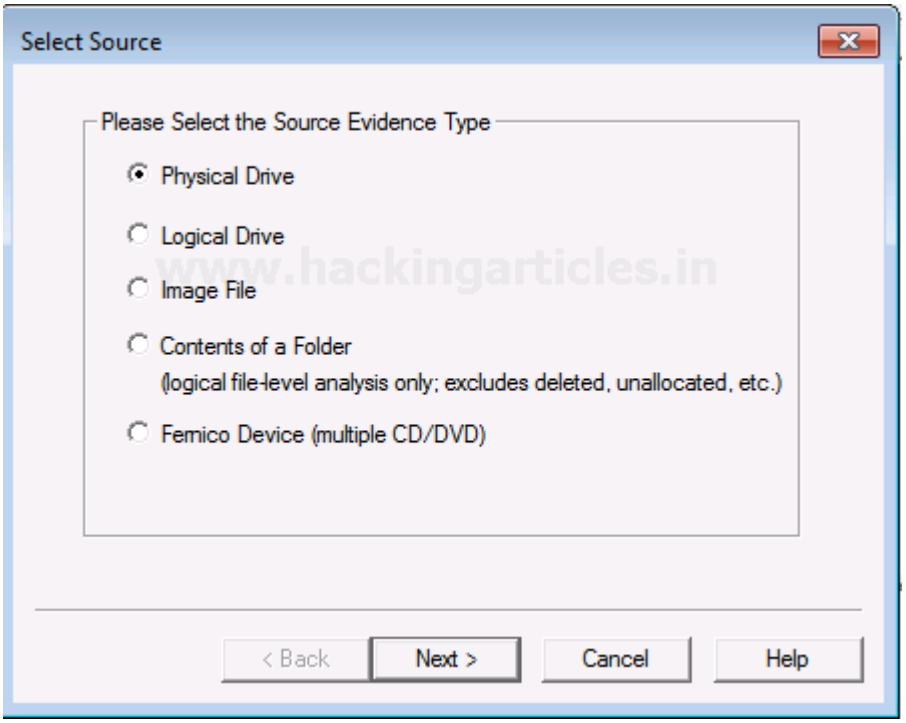


Now, to create a Disk Image. Click on File > Create Disk Image.

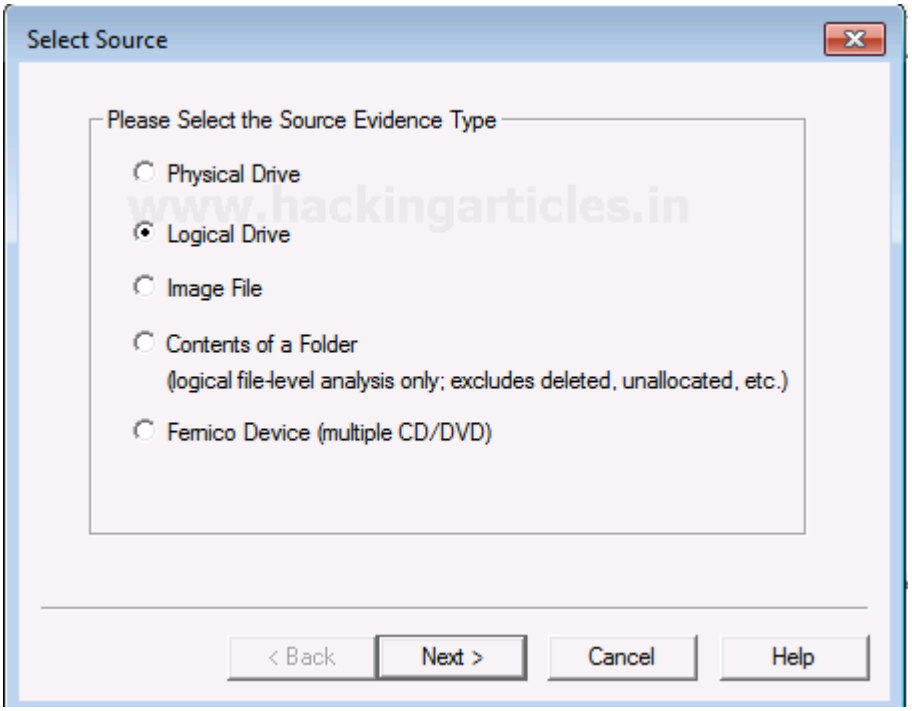


Now you can choose the source based on the drive you have. It can be a physical or a logical Drive depending on your evidence.

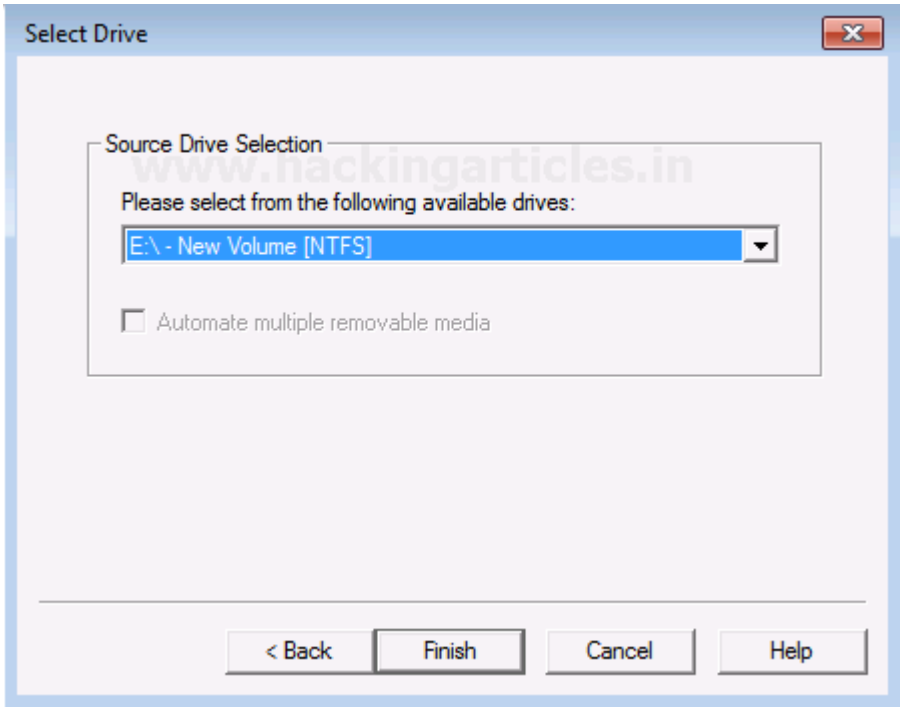
A **Physical Drive** is the primary storage hardware or the component within a device, which is used to store, retrieve, and organize data.



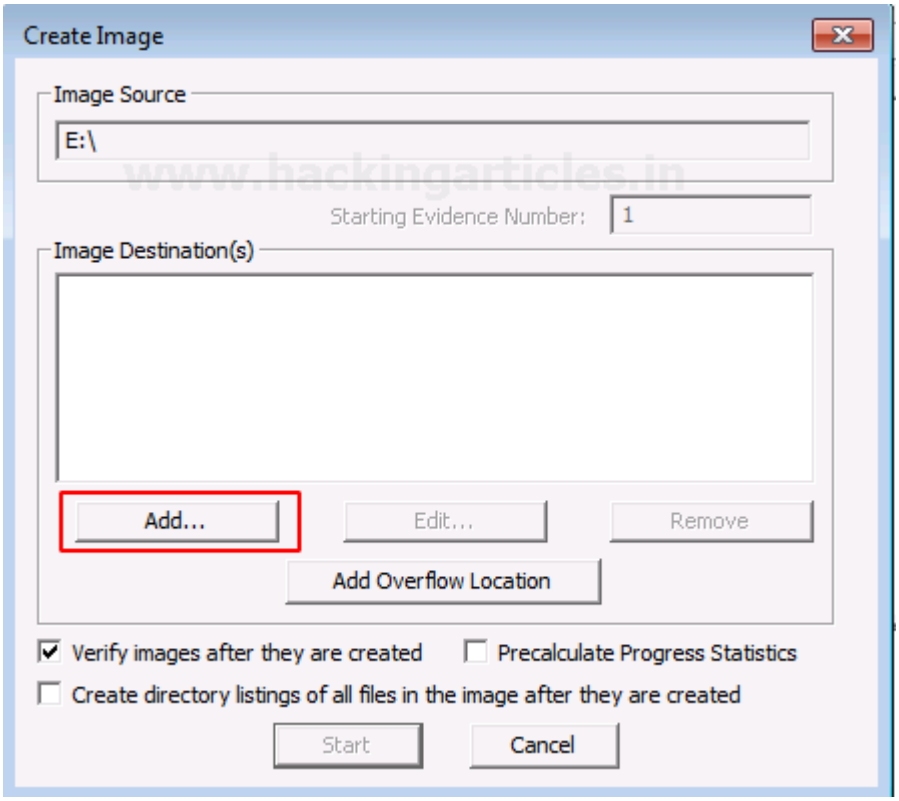
A **Logical Drive** is generally a drive space that is created over a physical hard disk. A logical drive has its parameters and functions because it operates independently.



Now choose the source of your drive that you want to create an image copy of.



Add the Destination path of the image that is going to be created. From the forensic perspective, It should be copied in a separate hard drive and multiple copies of the original evidence should be created to prevent loss of evidence.



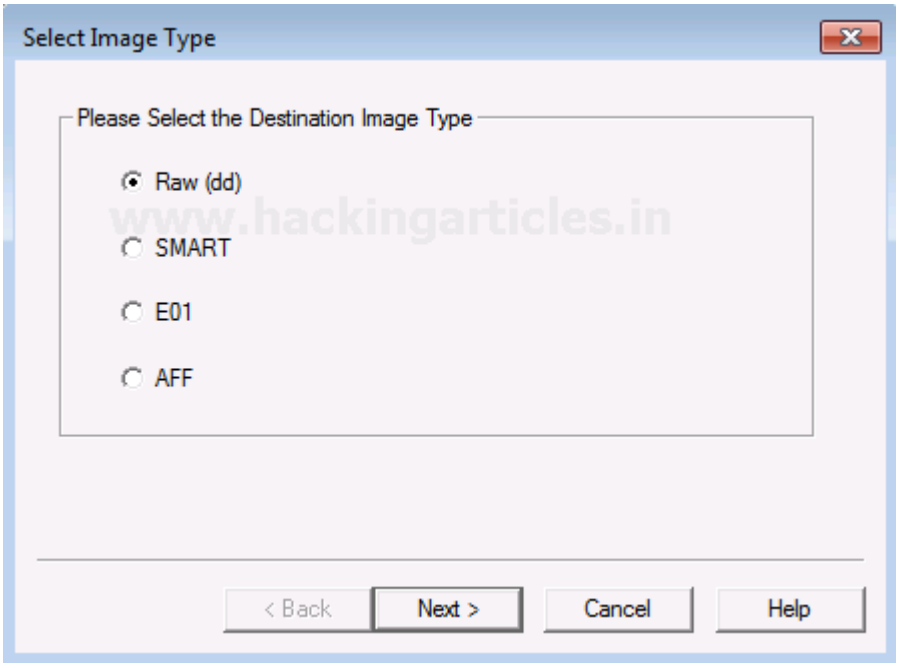
Select the format of the image that you want to create. The different formats for creating the image are:

Raw(dd): It is a bit-by-bit copy of the original evidence which is created without any additions and or deletions. They do not contain any metadata.

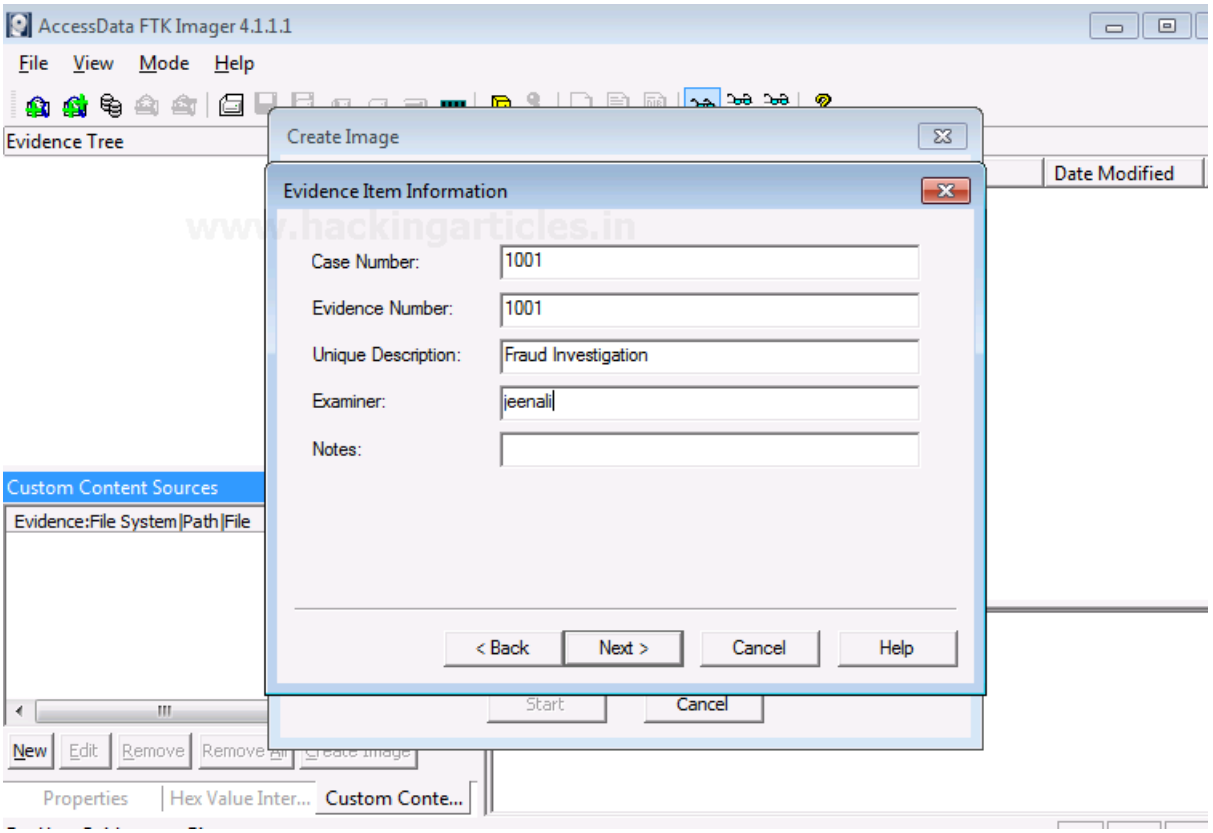
SMART: It is an image format that was used for Linux which is not popularly used anymore.

E01: It stands for EnCase Evidence File, which is a commonly used format for imaging and is similar to

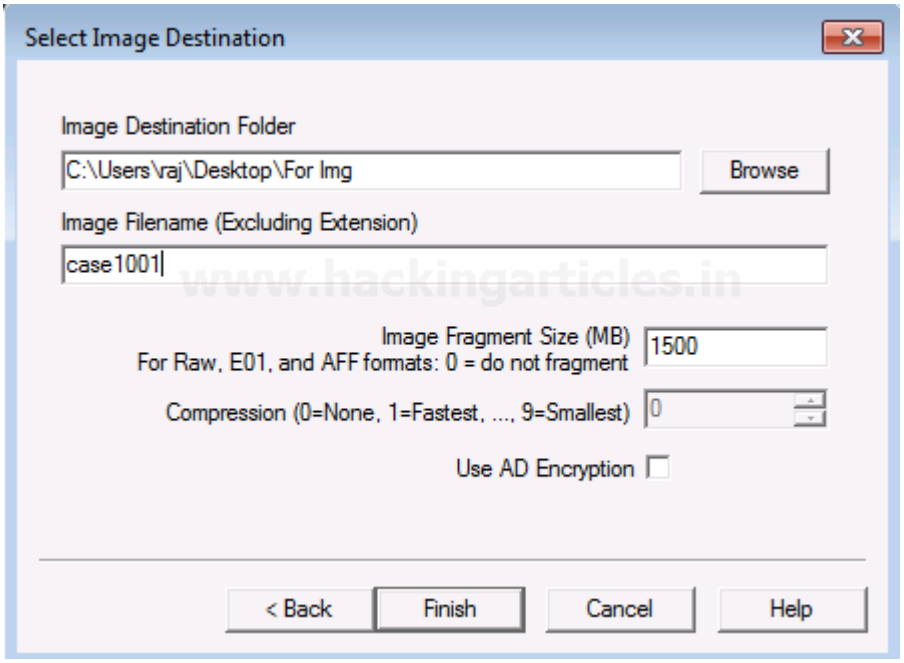
AFF: It stands for Advanced Forensic Format that is an open-source format type.



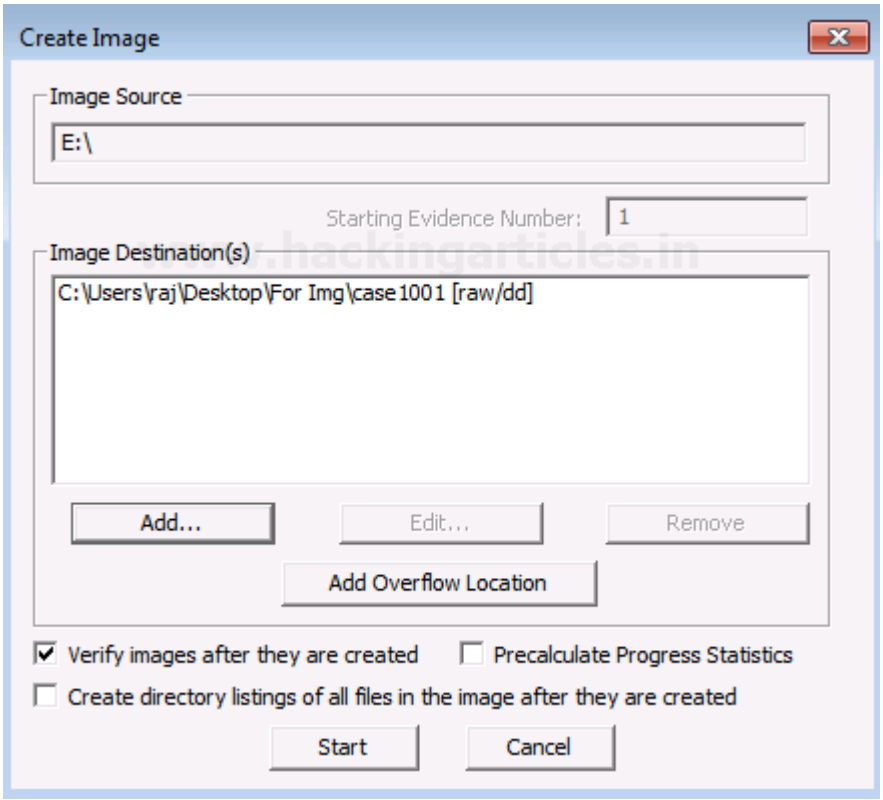
Now, add the details of the image to proceed.



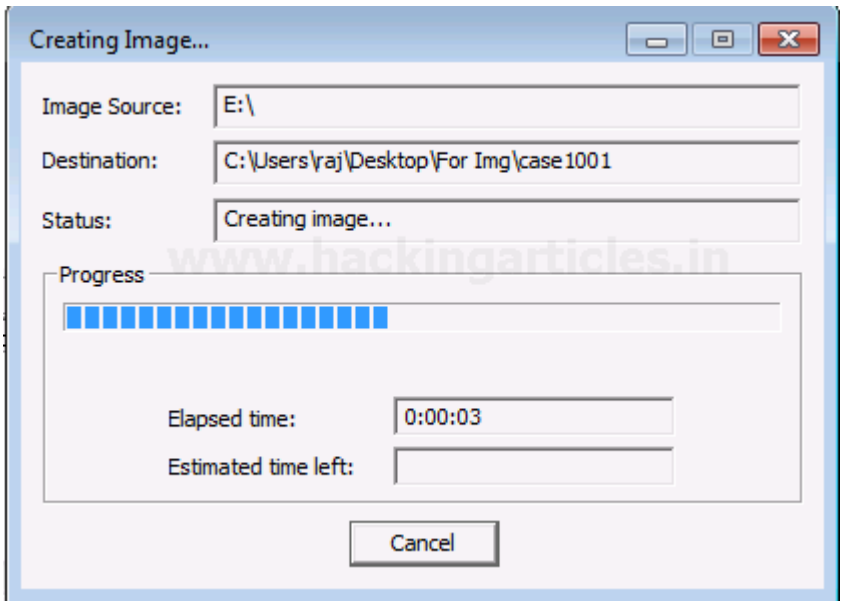
Now finally add the destination of the image file, name the image file and then click on Finish.



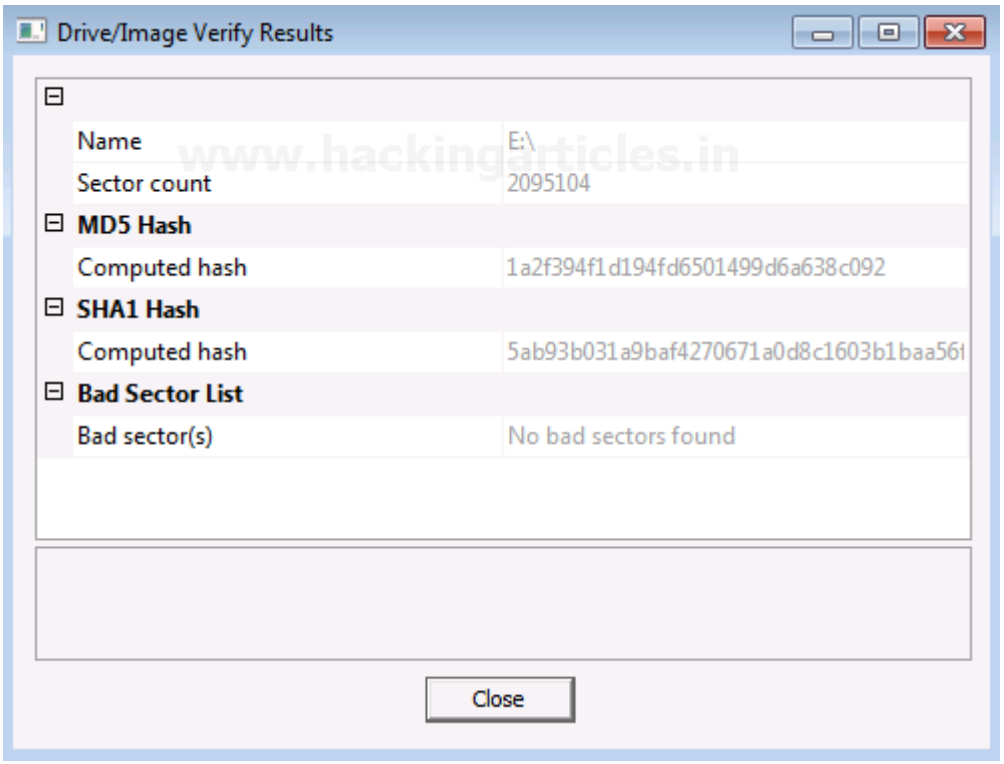
Once you have added the destination path, you can now start with the Imaging and also click on the verify option to generate a hash.



Now let us wait for a few minutes for the image to be created.



After the image is created, a Hash result is generated which verifies the MD5 Hash, SHA1 Hash, and the presence of any bad sector.

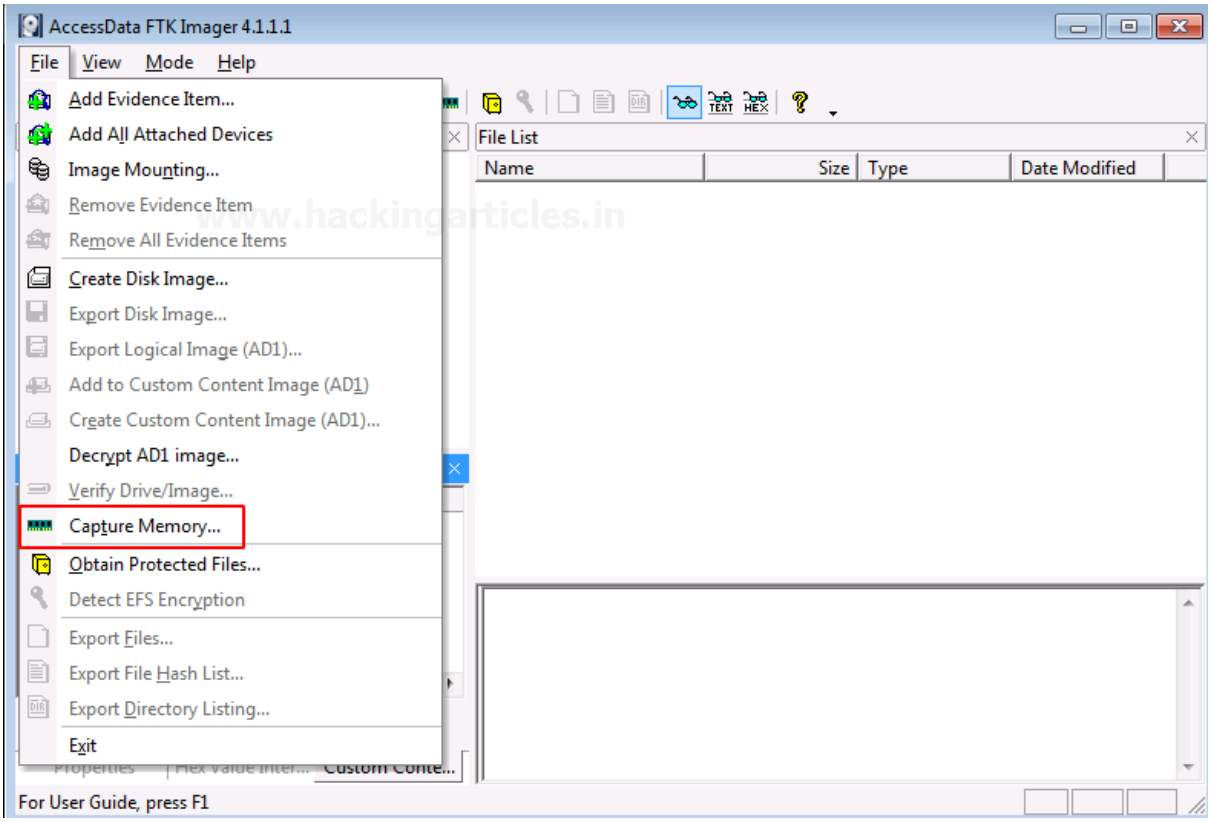


Capturing Memory

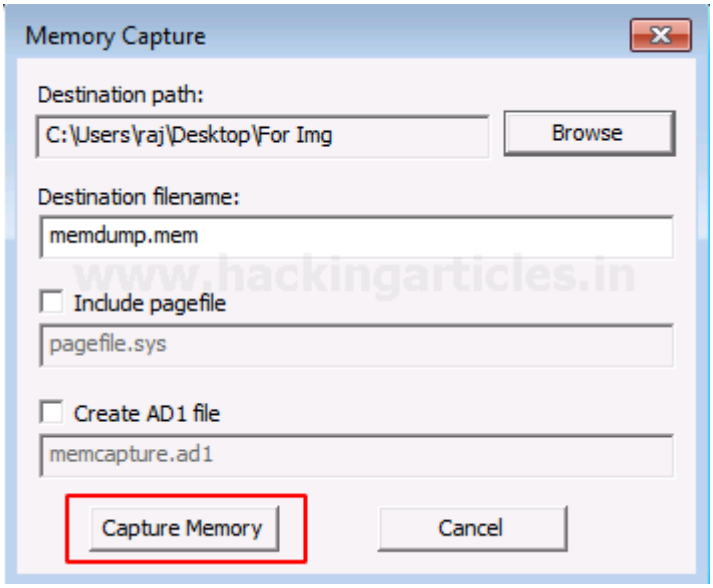
It is the method of capturing and dumping the contents of a volatile content into a non-volatile storage device to preserve it for further investigation. A ram analysis can only be successfully conducted when the acquisition has been performed accurately without corrupting the image of the volatile memory. In this phase, the investigator has to be careful about his decisions to collect the volatile data as it won't exist after the system undergoes a reboot.

Now, let us begin with capturing the memory.

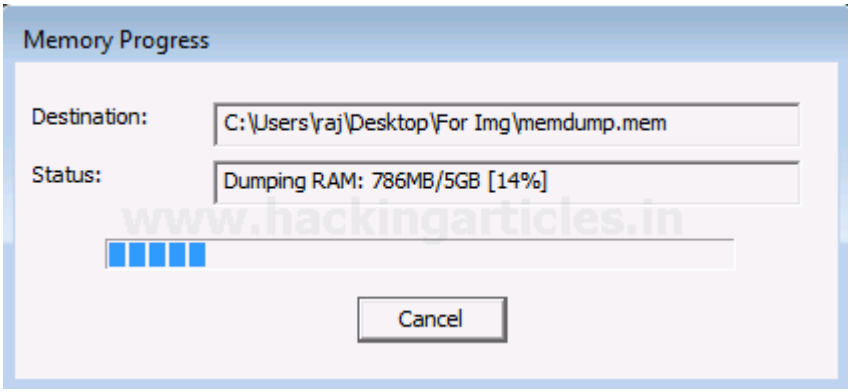
To capture the memory, click on **File > Capture Memory**.



Choose the destination path and the destination file name, and click on capture memory.

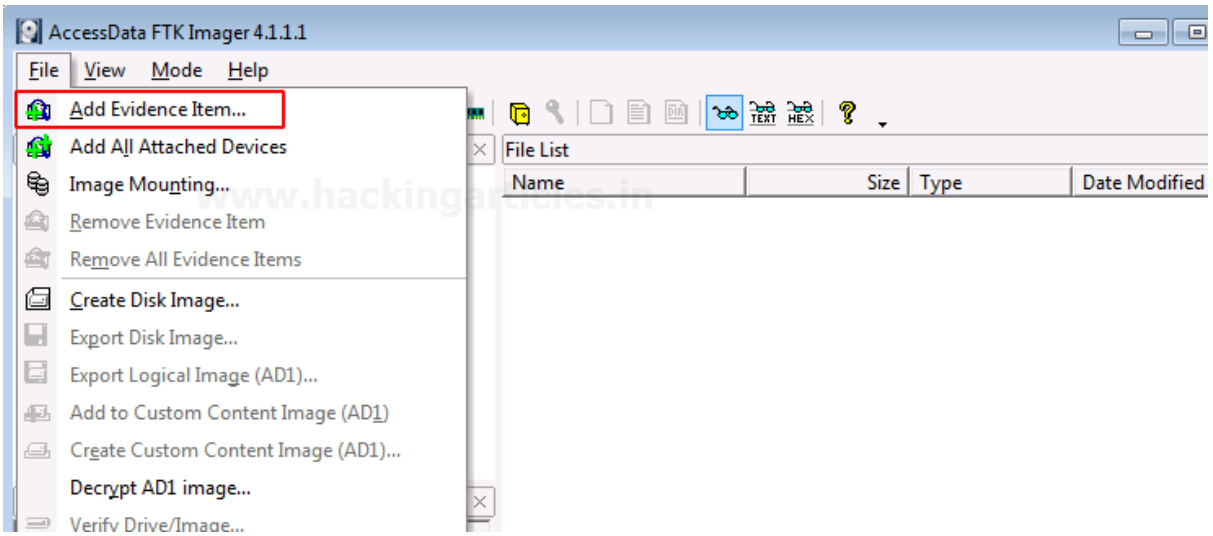


Now let us wait for a few minutes till the ram is being captured.

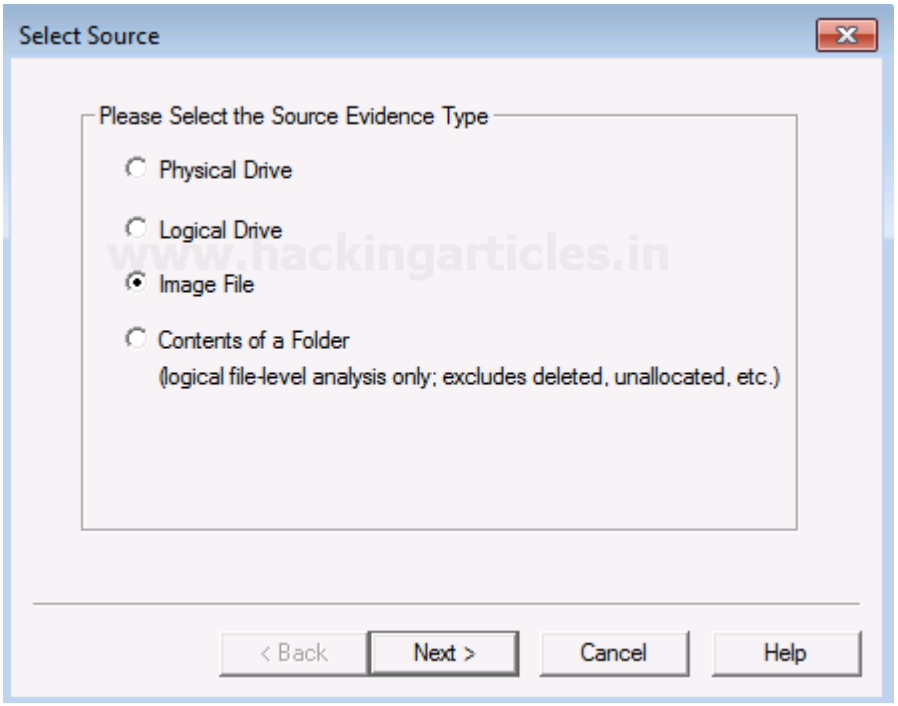


Analyzing Image Dump

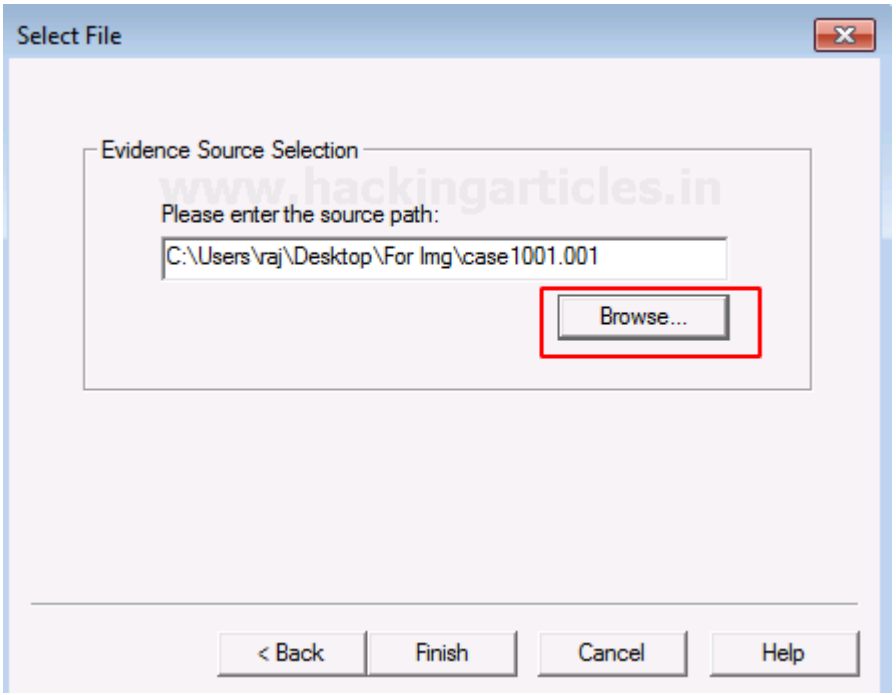
Now let us analyze the Dump RAW Image once it has been acquired using FTK imager. To start with analysis, click on **File> Add Evidence Item.**



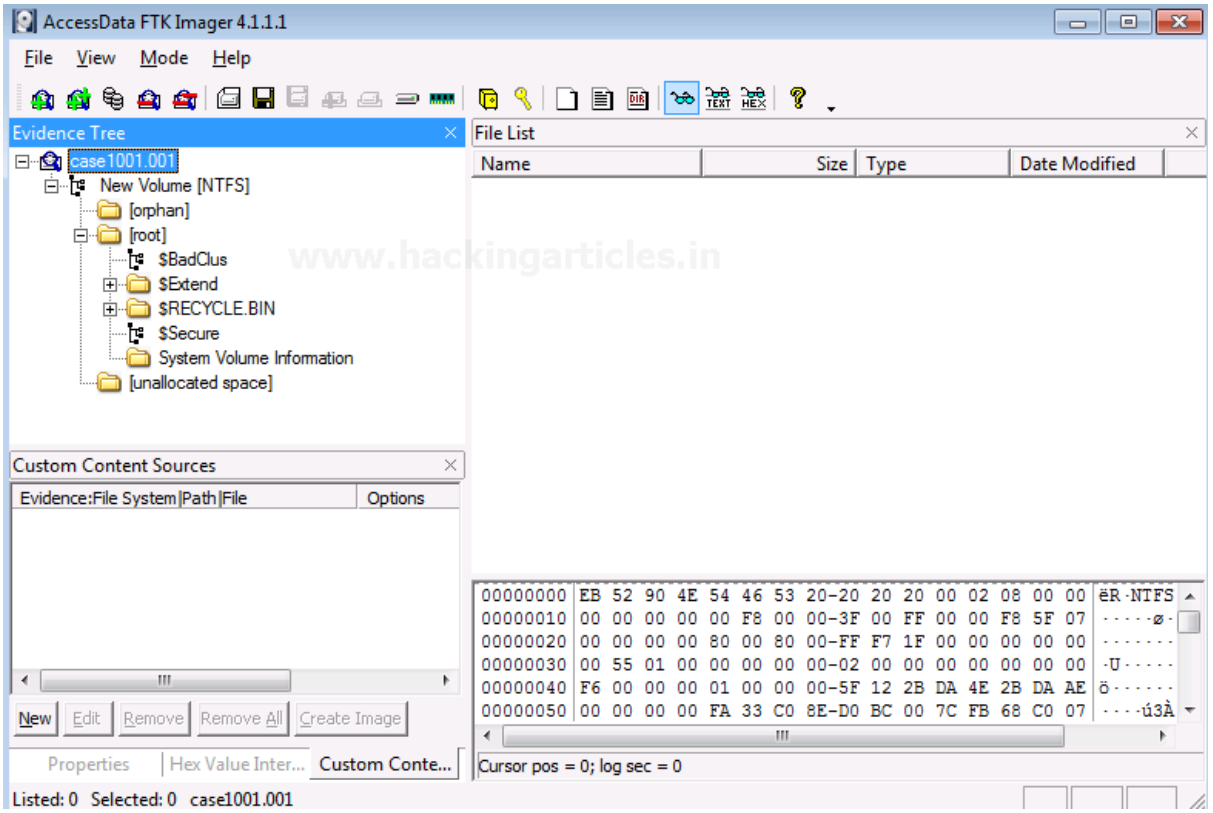
Now select the source of the dump file that you have already created, so here you have to select the image file option and click on Next.



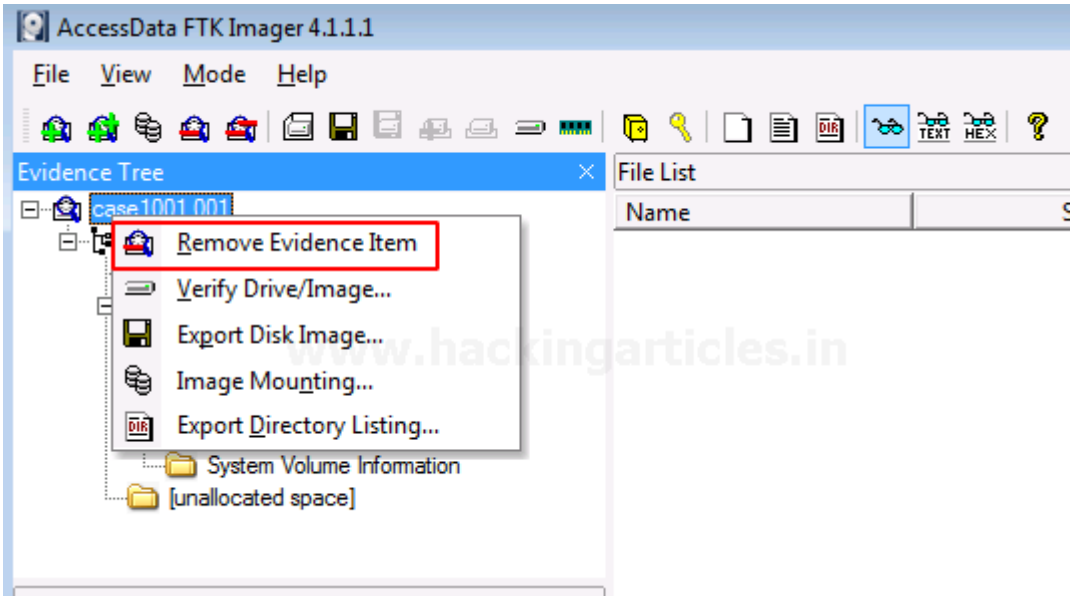
Choose the path of the image dump that you have captured by clicking on Browse.



Once the image dump is attached to the analysis part, you will see an evidence tree which has the contents of the files of the image dump. This could have deleted as well as overwritten data.

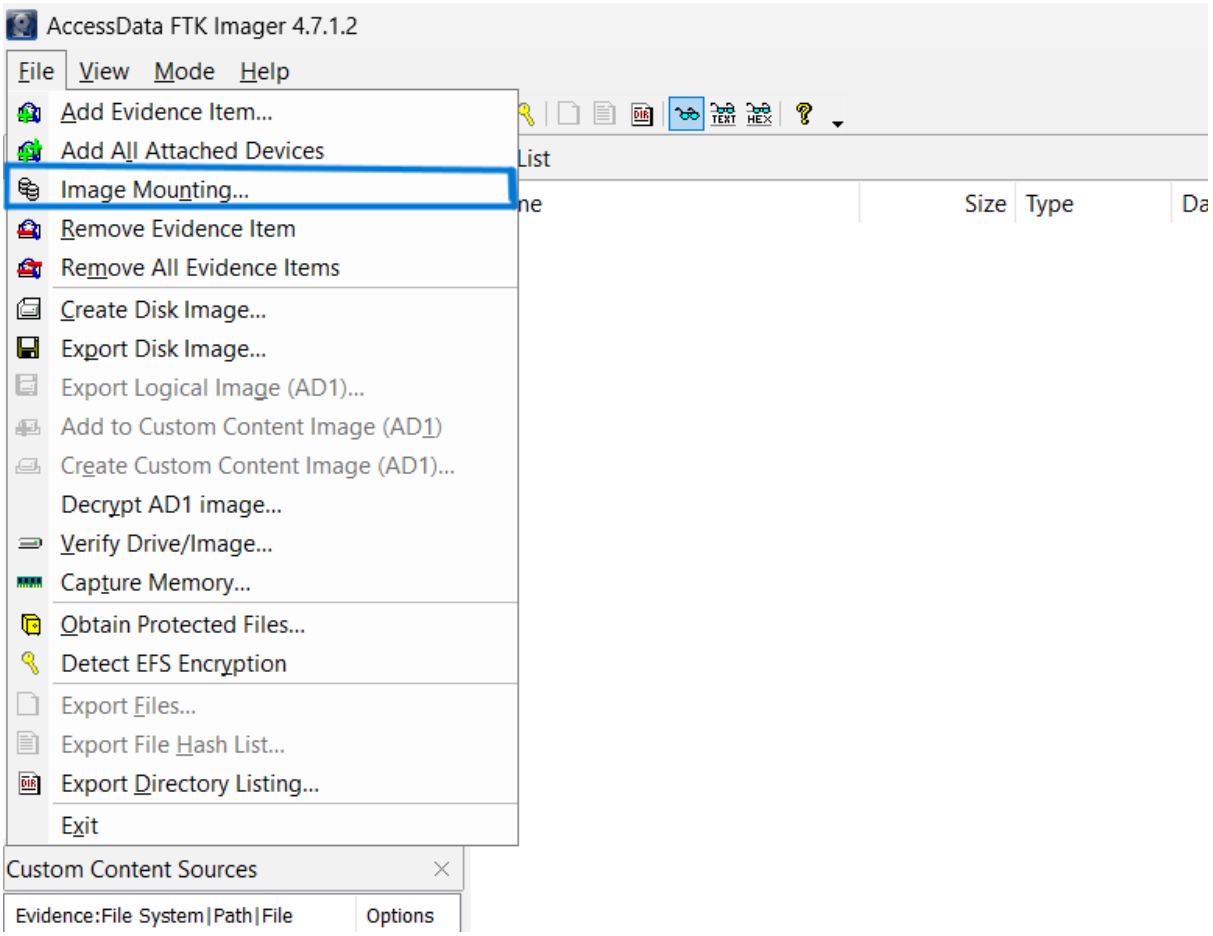


To analyze other things further, we will now remove this evidence item by right-clicking on the case and click on **Remove Evidence Item**

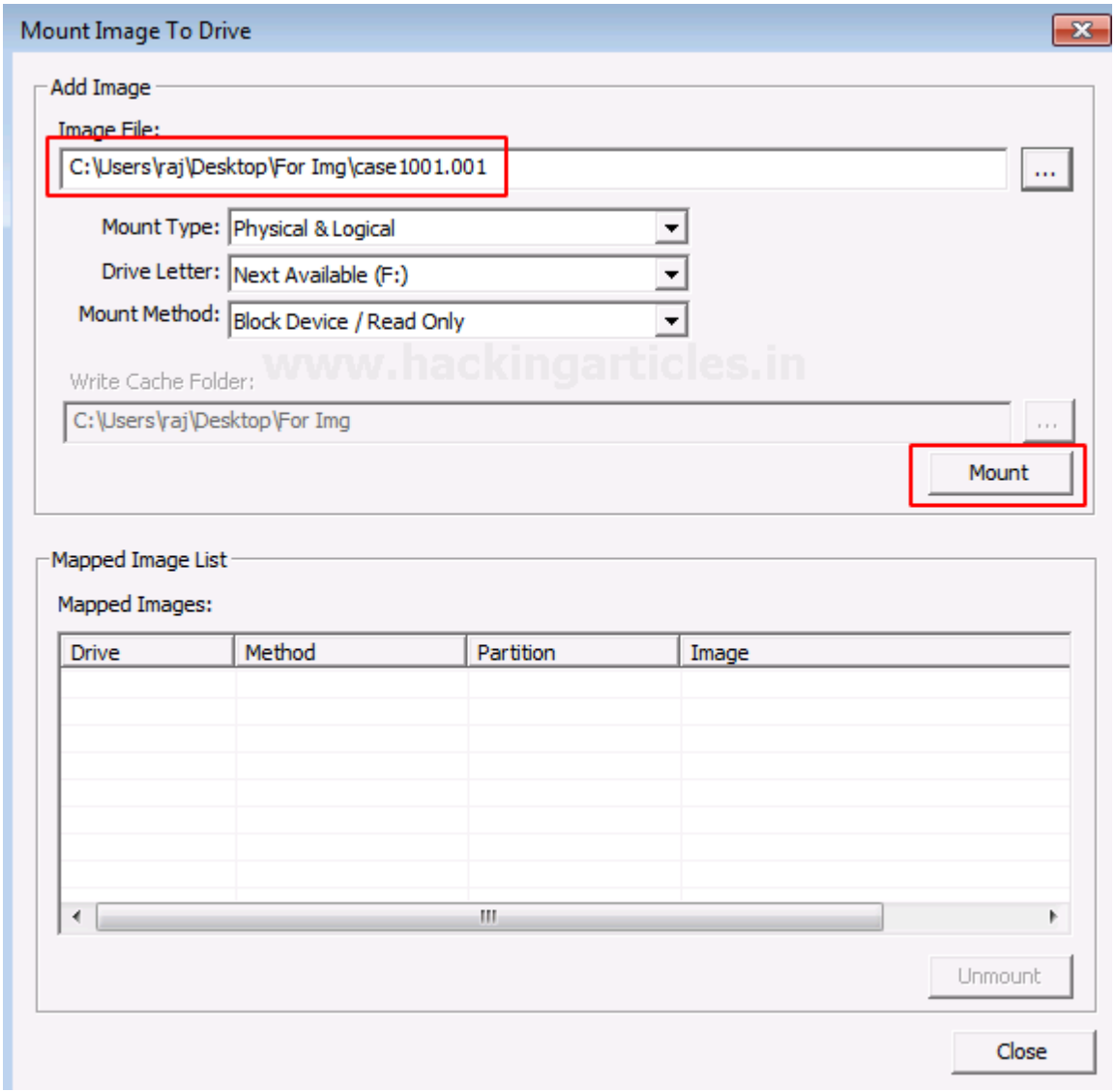


Mounting Image to Drive

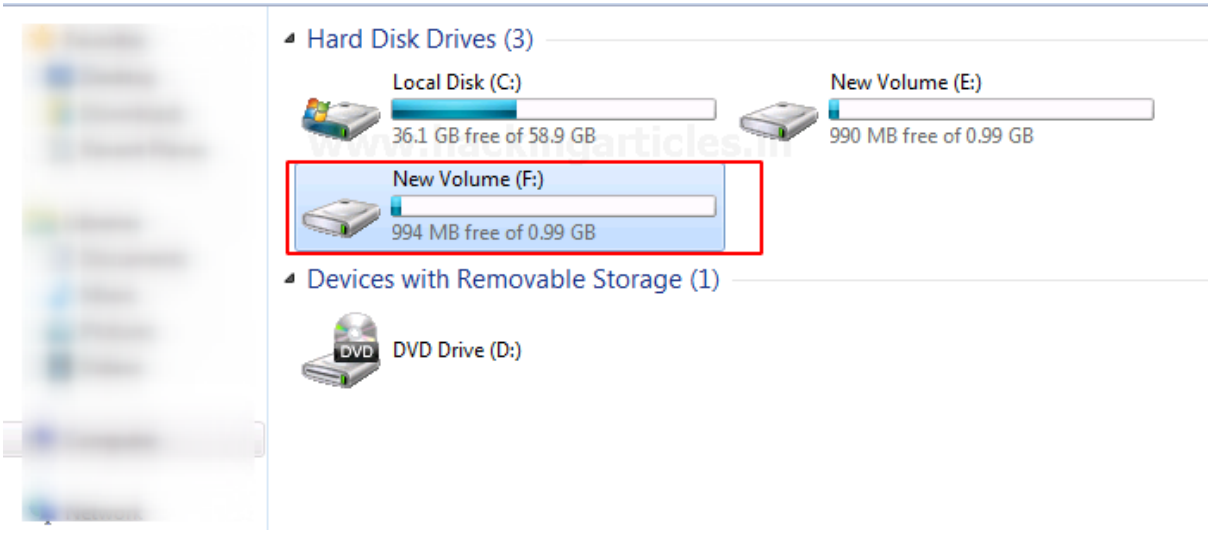
To mount the image as a drive in your system, click on **File > Image Mounting**



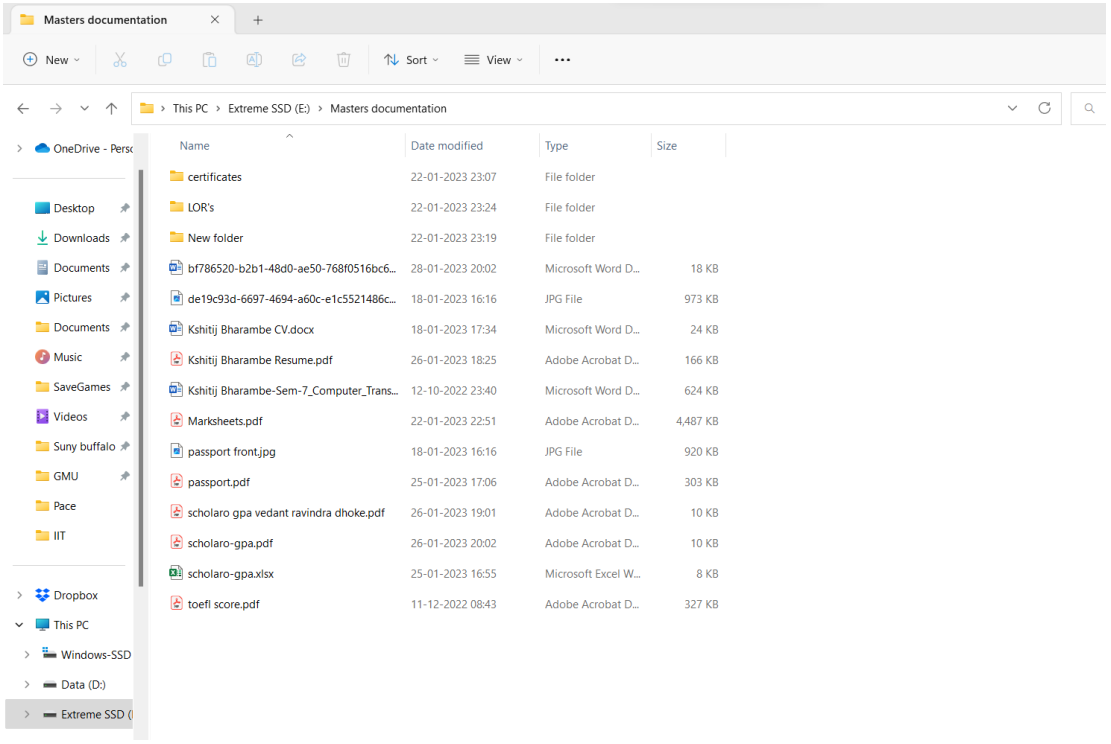
Once the Mount Image to Drive window appears, you can add the path to the image file that you want to mount and click on Mount.

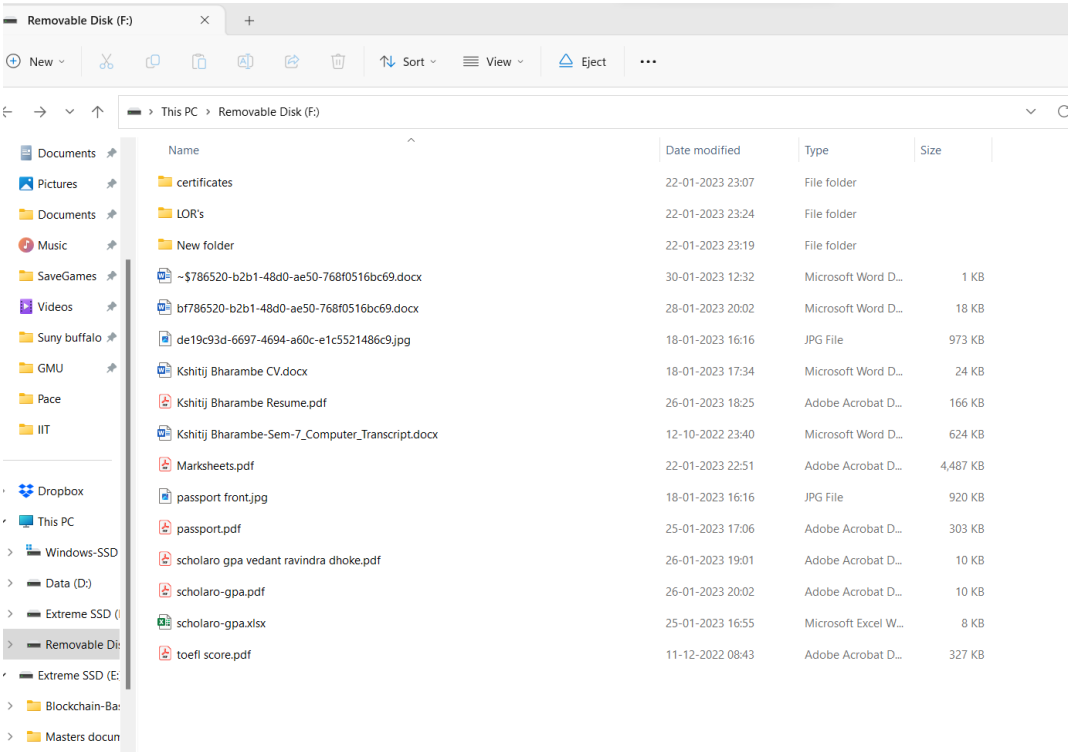


Now you can see that the image file has now been mounted as a drive.



Output:





Conclusion:FTK Imager is a powerful digital forensics tool used to acquire, analyze, and examine digital evidence from various sources, including hard drives.It offers a user-friendly interface with features that allow for fast and efficient data acquisition, analysis, and reporting.Overall, FTK Imager is a valuable tool for digital forensic investigators, law enforcement agencies, and other organizations that deal with digital evidence.