## EXPERIMENT-03

**Aim :**

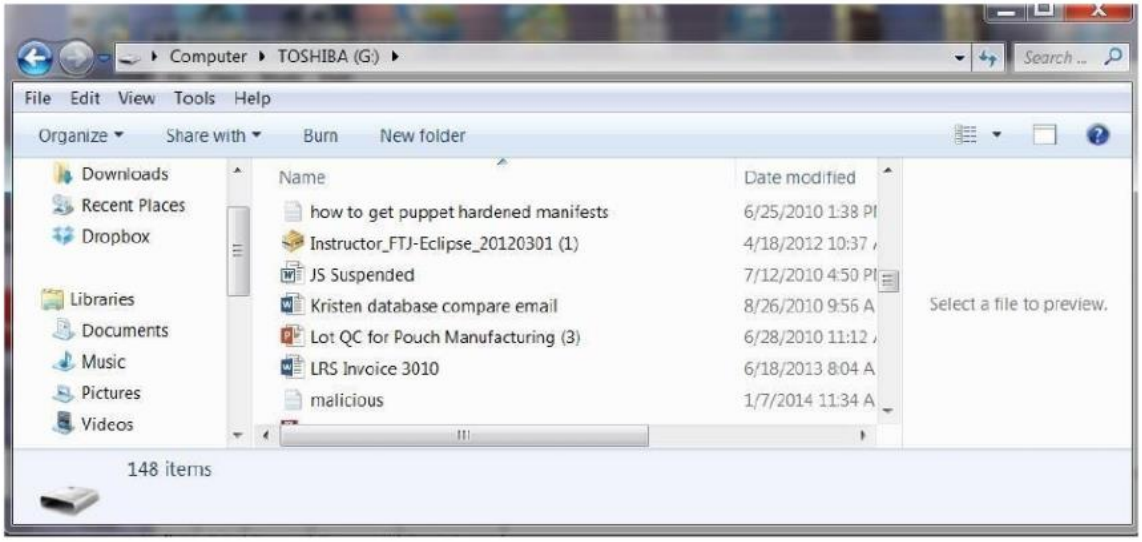
How to Recover Deleted Files using Forensics Tools

**Step-01: Create a File**

To demonstrate how to recover deleted files, let's create a malicious document. We will call this document "Malicious" and create it with Notepad in Windows


**Step 2: Delete the File**

Next, now that we have completed our plans to take over the world, let's delete the file because we no longer need it and we don't want to leave behind any evidence of our malicious plans.




Right-click on the malicious file and select delete.

**Step 3: Create an Image**

The first step a forensic investigator will do when examining your computer is to make a bit-by-bit copy of your hard drive or in this case your flash drive.

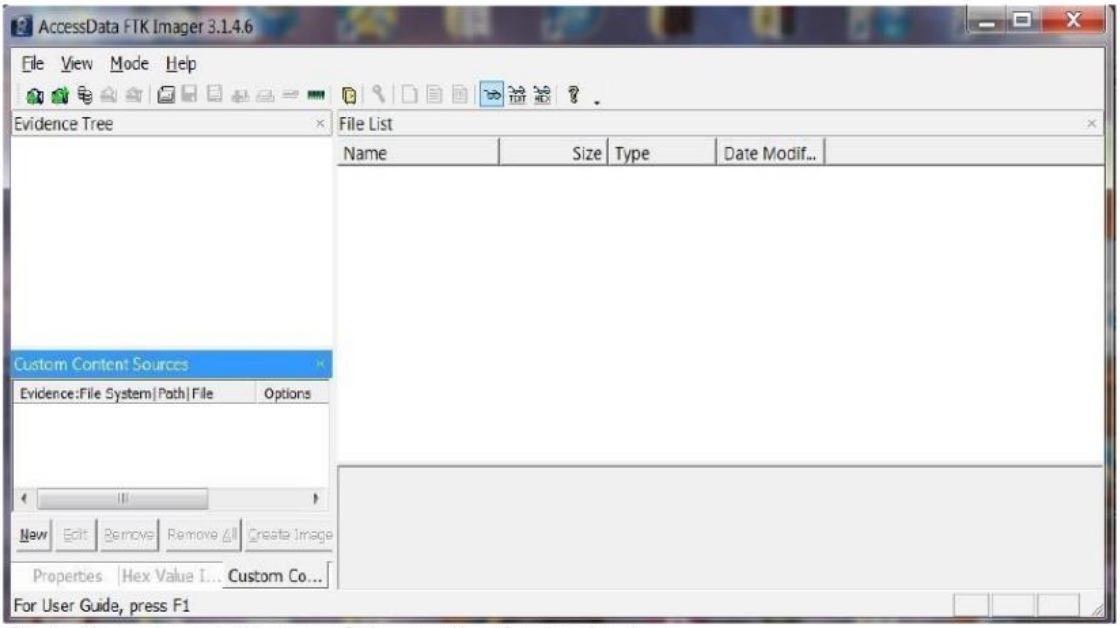
There are numerous tools that can do this and in Linux, we have the dd command that does an excellent job of making bit-by-bit copies (it's on all Linux distributions including BackTrack).

File backups and copies are not forensically sound as they will not copy deleted files and folders and in many cases will actually change the data.

Most forensic investigators use commercial tools. The two most popular being Encase by Guidance Software and Forensic Tool Kit by Access Data.

FTK, as it is commonly known in the industry, has a free imager that creates a bit-by-bit copy of the drive. This imager is probably the most widely used in the industry and its price is right, so let's use it

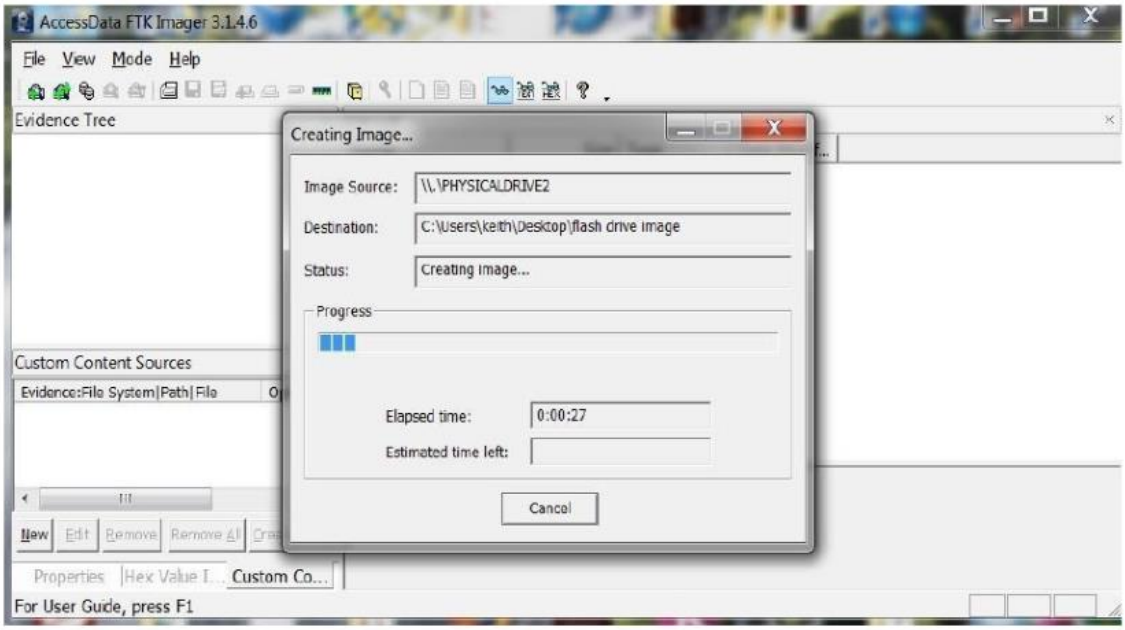
Now that have downloaded the **FTK imager**, we need to create a bit-by-bit image of the flash drive.




Go to the menu at the top of the application and select:

**File -> Create Image**

- It will open a wizard that will walk you through the process of opening a case and ask you for a case number, evidence number, examiner name, etc.
- Finally, it will ask for a location of the physical drive you want to image, a destination directory and a name for the image file.
- When you are done with all these administrative tasks, FTK Imager will begin the process of creating a forensically sound bit-by-bit image of your drive.



Now that we've created an image of the flash drive, we are ready to recover the deleted files.

**Step 4: Recover Deleted Files**

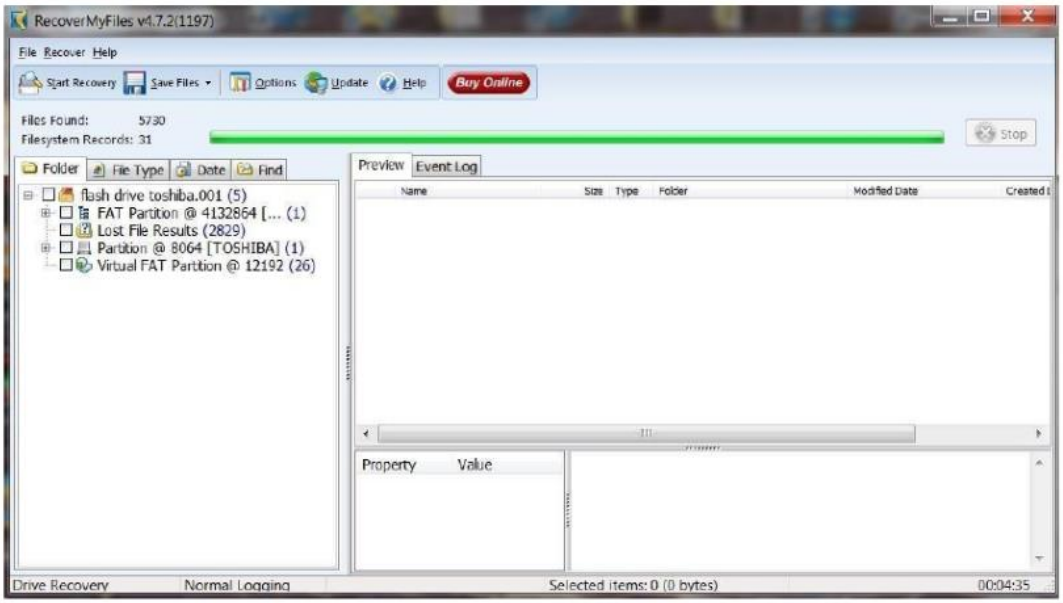
Once you have installed RecoverMyFiles, select the Start Recovery icon in the upper left corner.

It will ask you to select either Recover Files or Recover Drive.

Select Recover a Drive. It will then search and display all your drives like that in the screenshot below.

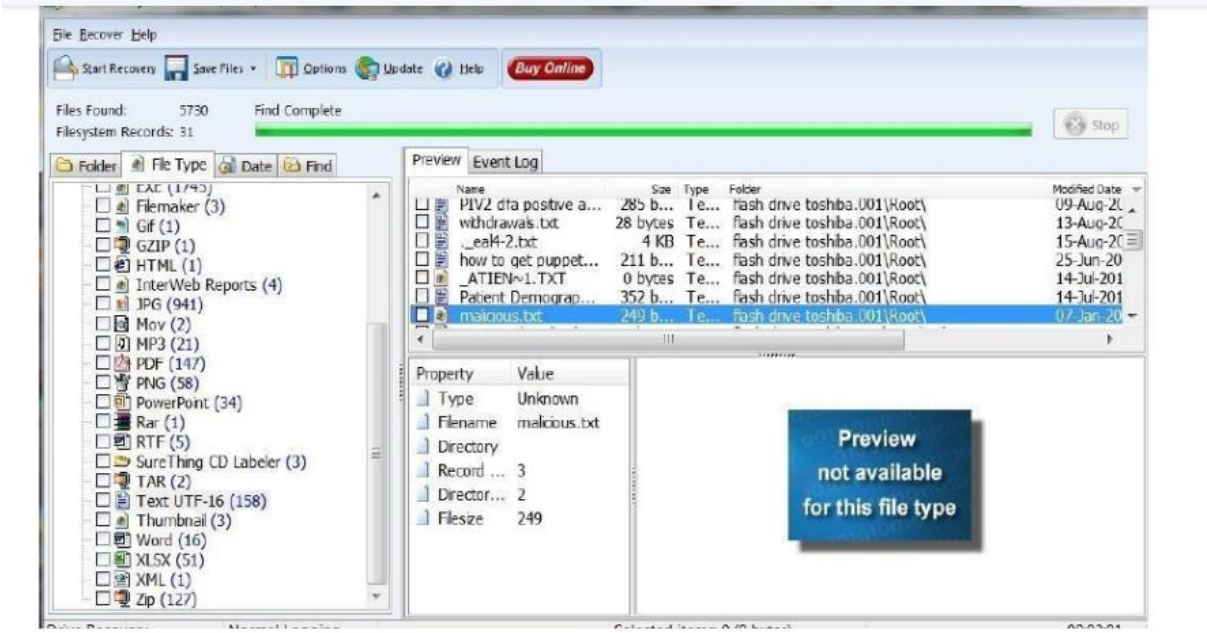
Since we are using a forensic image, select Add Image button to the right. You will need to provide a path to your image file created with FTK

Once you select an image file, start the automatic file recovery. When the recovery is completed,




Once you select an image file, start the automatic file recovery. When the recovery is completed,

- Then selected the File Type tab above the Explorer window to categorize the files by type.
- There are numerous file types recovered from this flash drive.
- Since our malicious document was a .txt, I have selected the TXT UTF-16 file type.
- It then puts all 158 .txt files on display in the upper right window.
- It has recovered our malicious.txt file and everything on it. Busted!




**Result:**

Thus, the forensic tools executed successfully, and the evidence was captured and analyzed accurately.