Digital Forensics

SRN : PES1UG20CS825	NAME : PREM SAGAR J S	SEC : 'H'

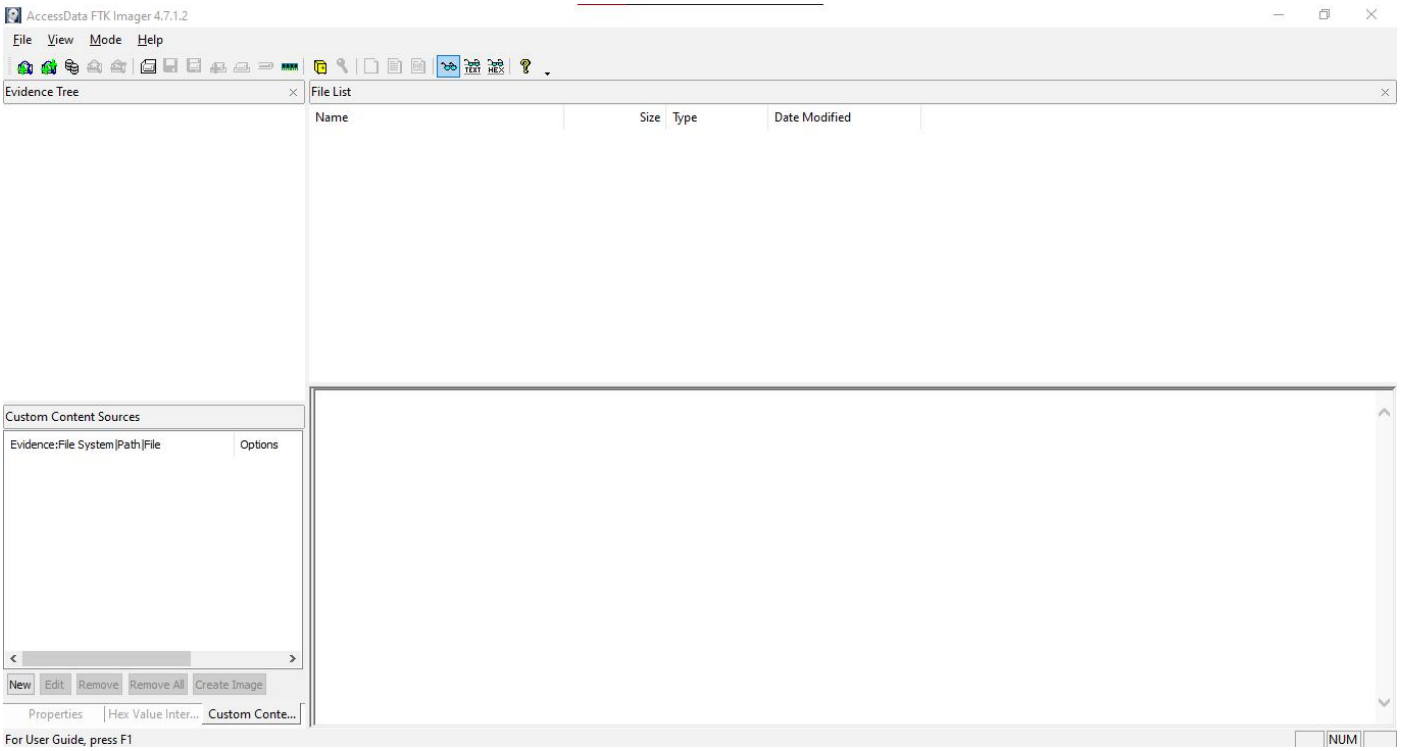
Lab Assignment - 2

Lab 2: Evidence Acquisition Using FTK Imager

1. USB Drive Acquisition from FTK imager (With out write blocker)

- FTK imager can create an image and paging file for windows; along with capturing volatile memory for analysis purpose.

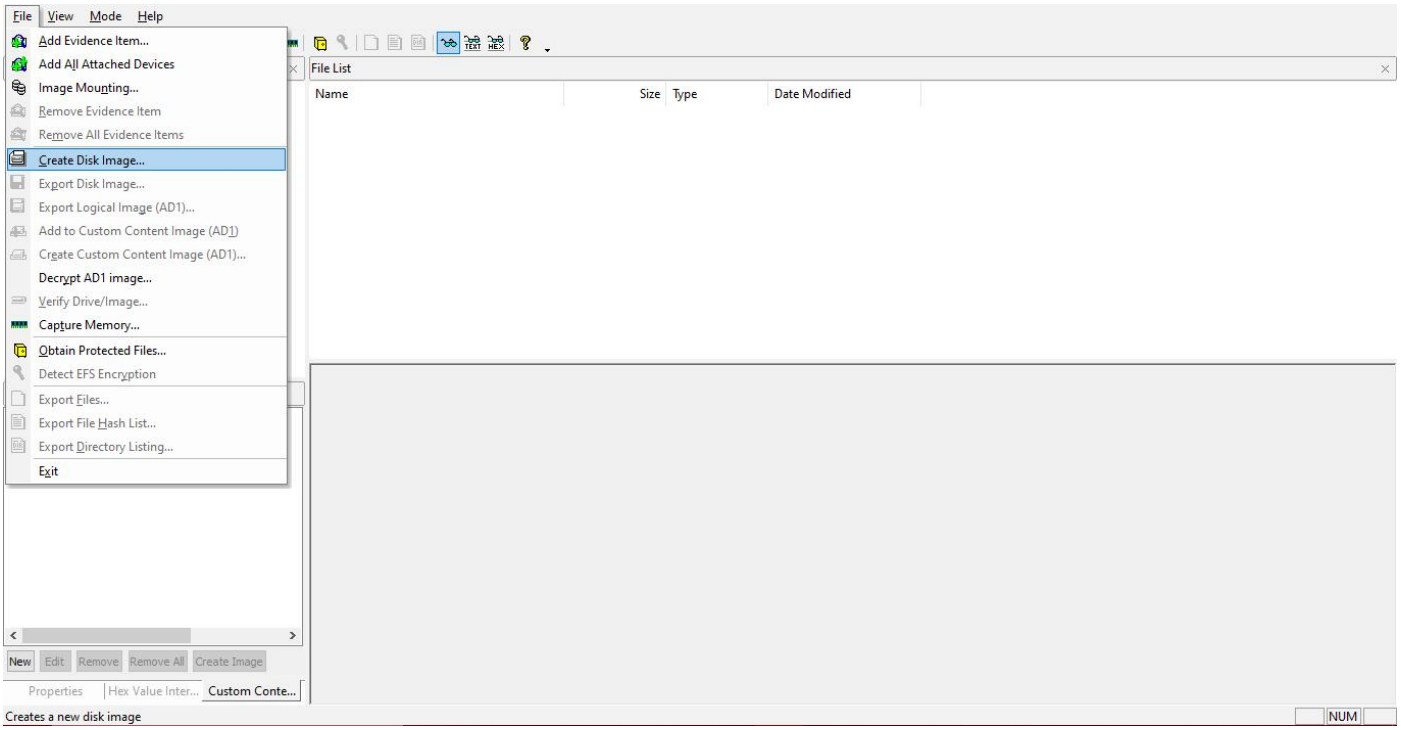
- FTK Imager has been downloaded and installed successfully.



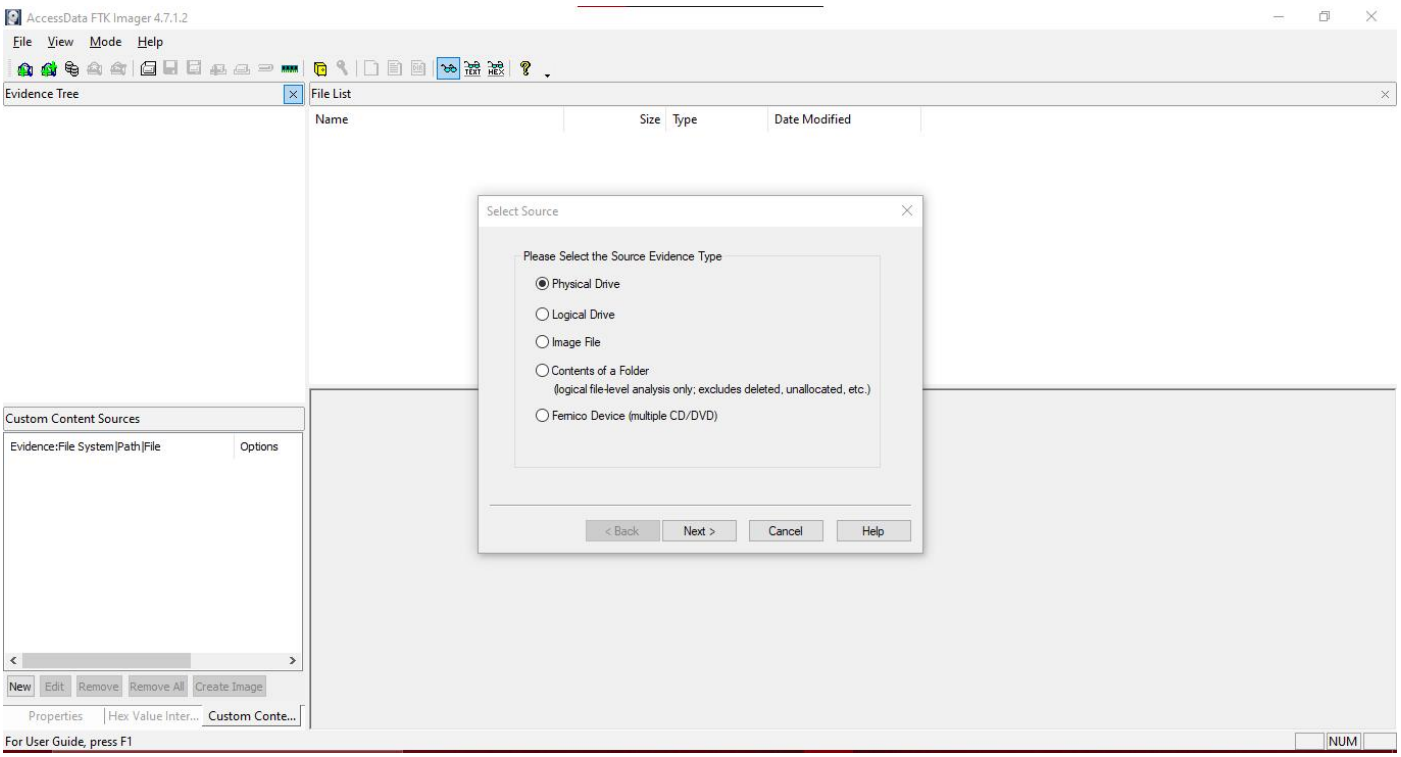
- I have connected a pen-drive to the PC with with some data.

- **FTK Imager** application is running.

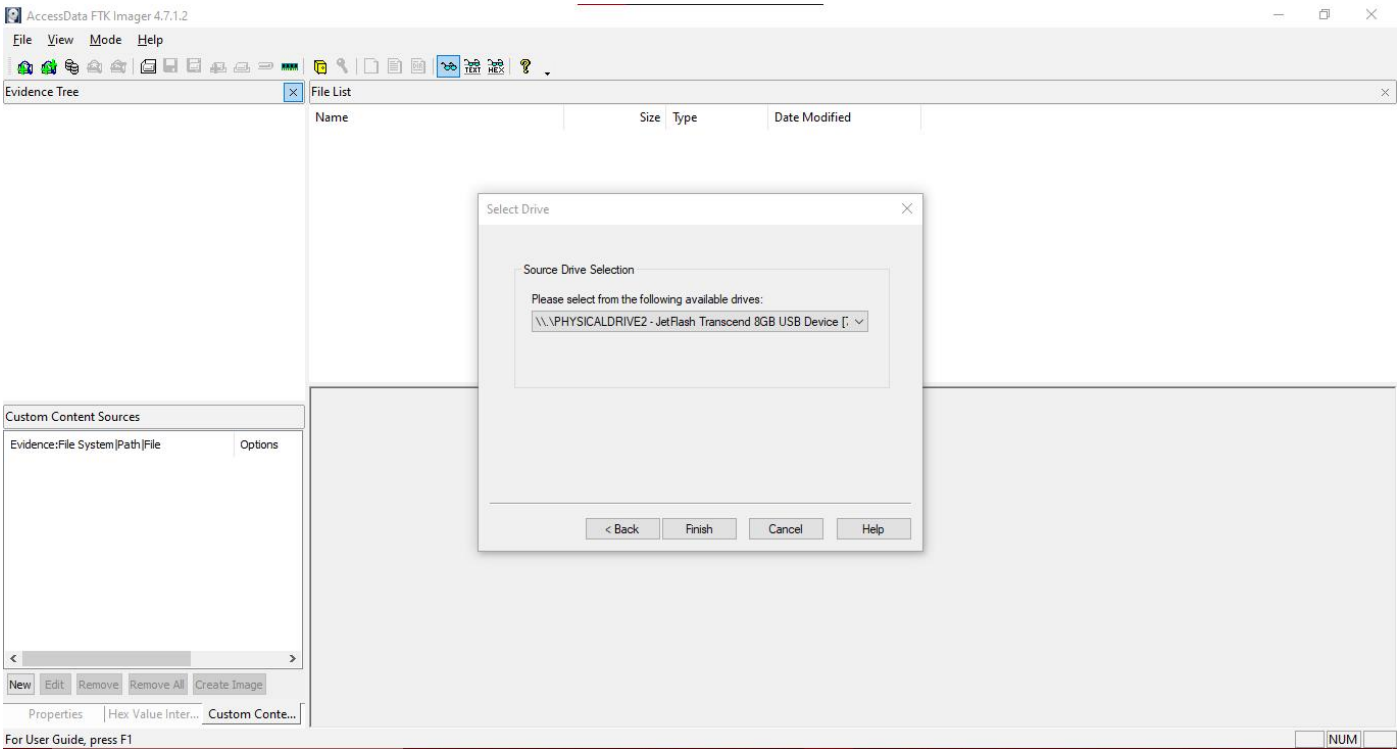
➢ Selecting **Create Disk Image** option in the file section of the menu.



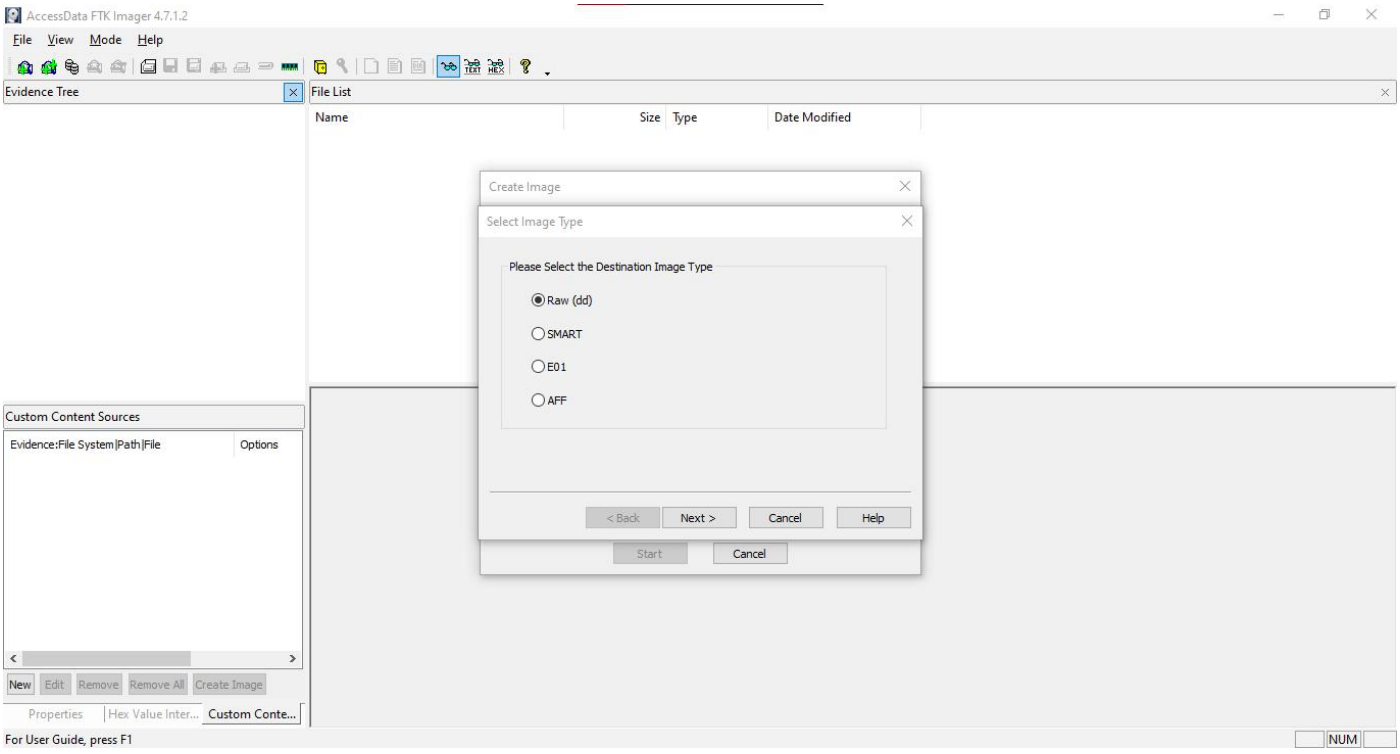
➢ Selecting the Source Evidence Type as **Physical Device.**



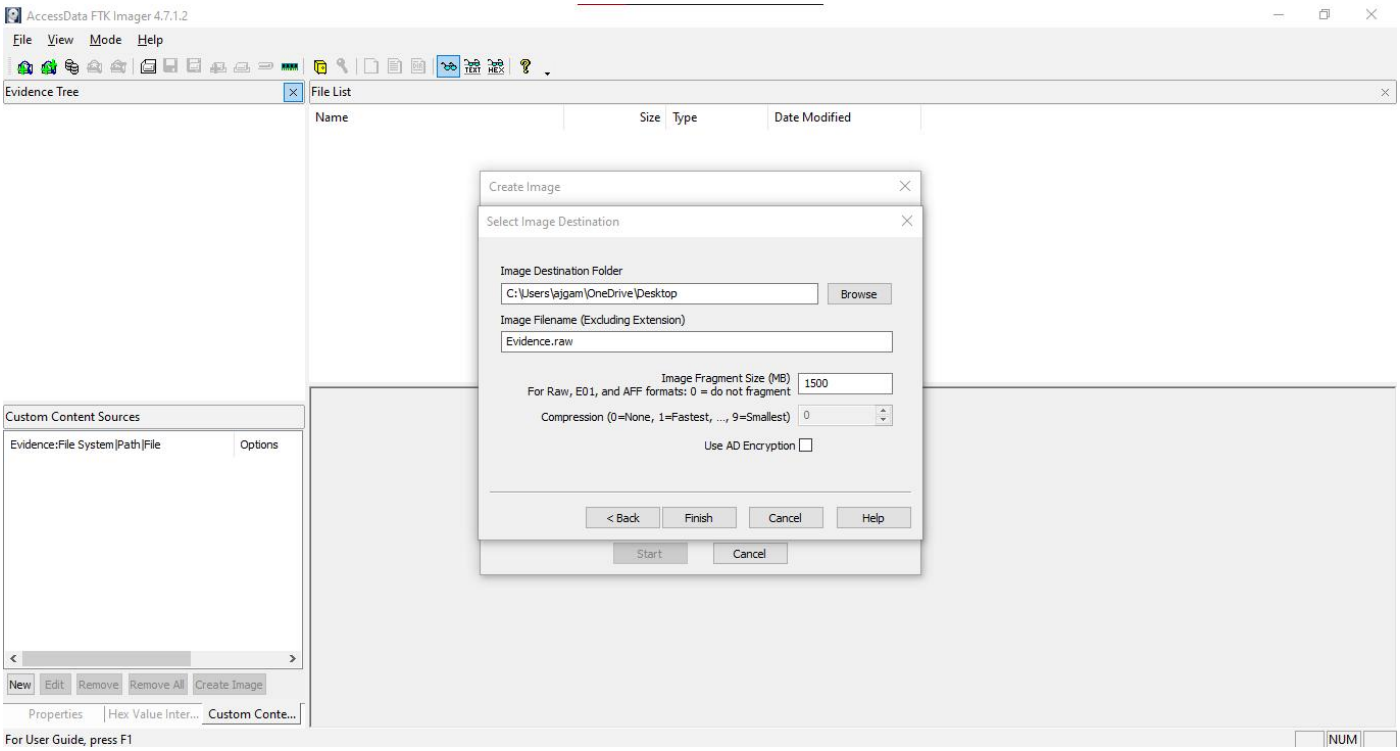
- Selecting the Source Pen-drive from the available drives in the PC.
- Pen-Drive (JetFlash Transcend 8GB USB Device)



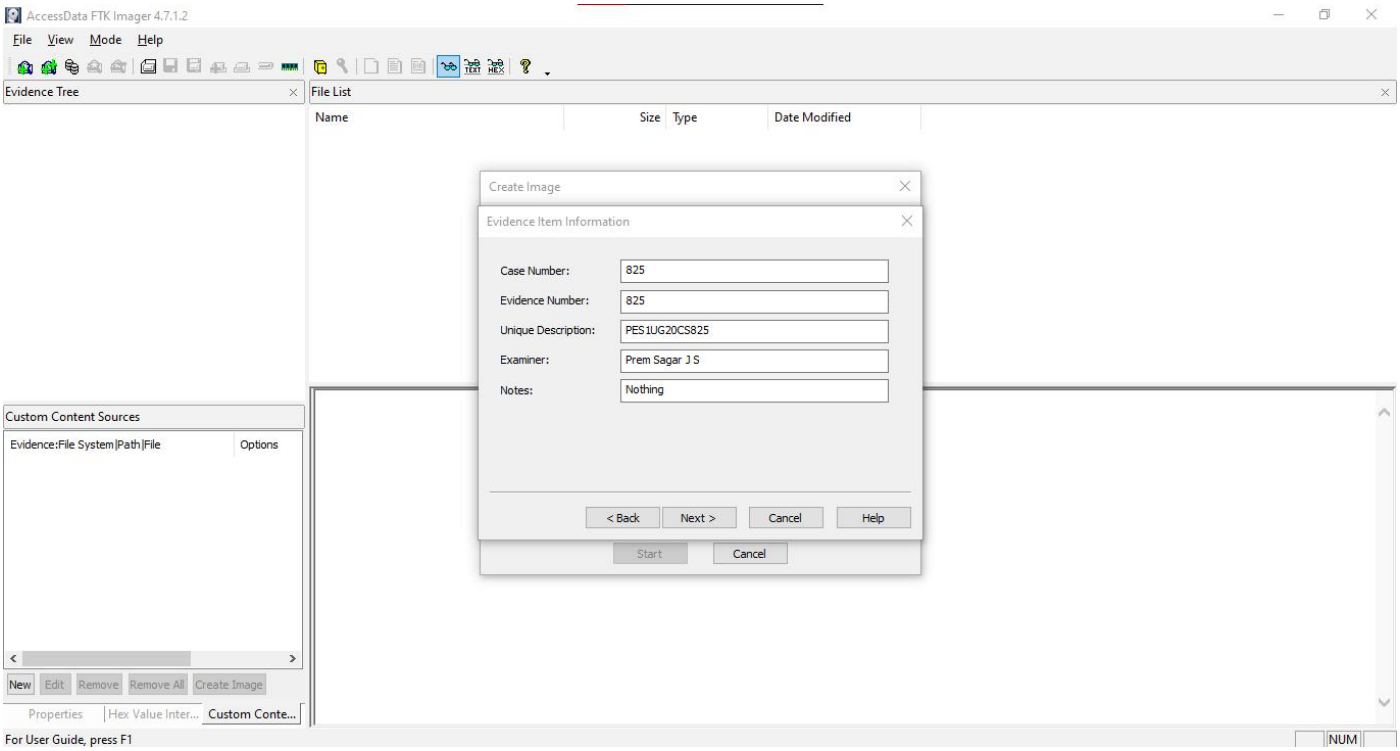
- Selecting **Destination Image Type** as Raw (dd).



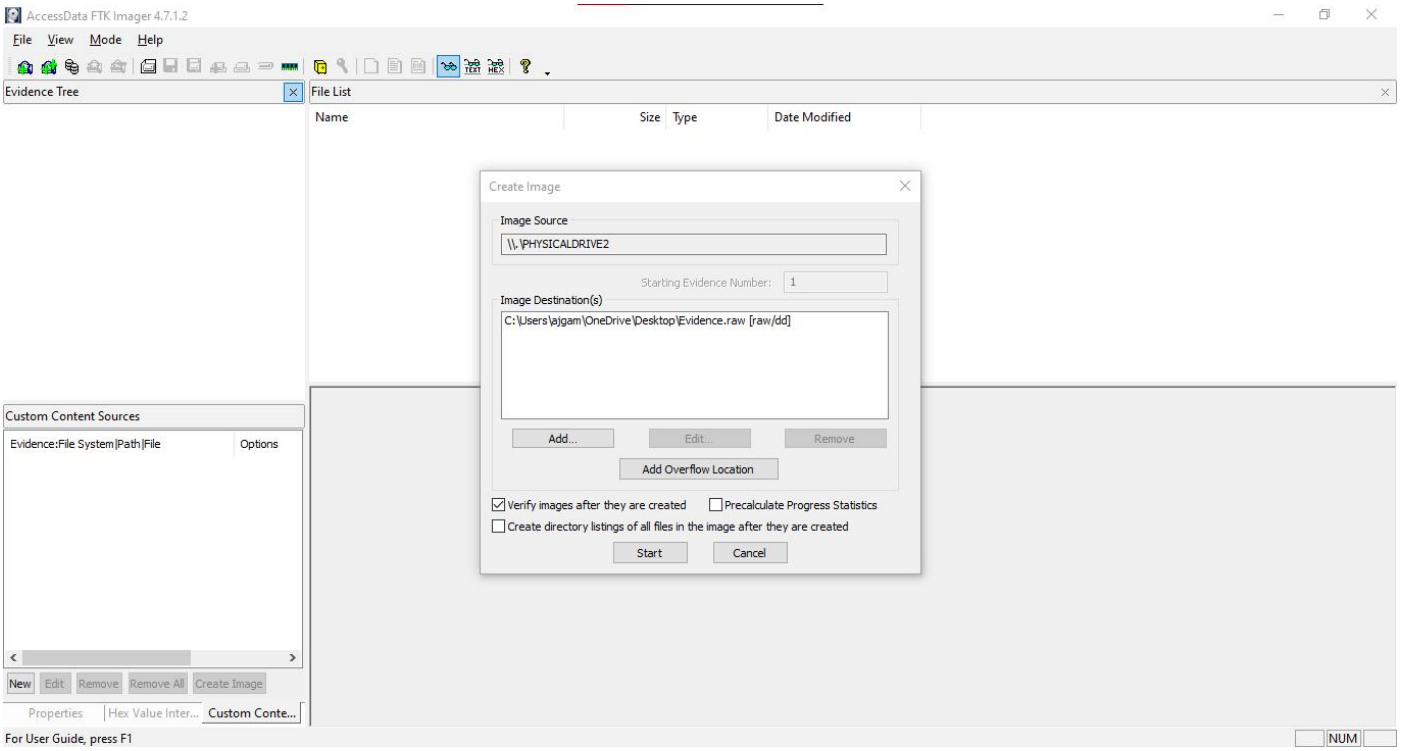
- Selecting destination folder where I want my images are supposed be stored and naming the image name as **evidence.raw**



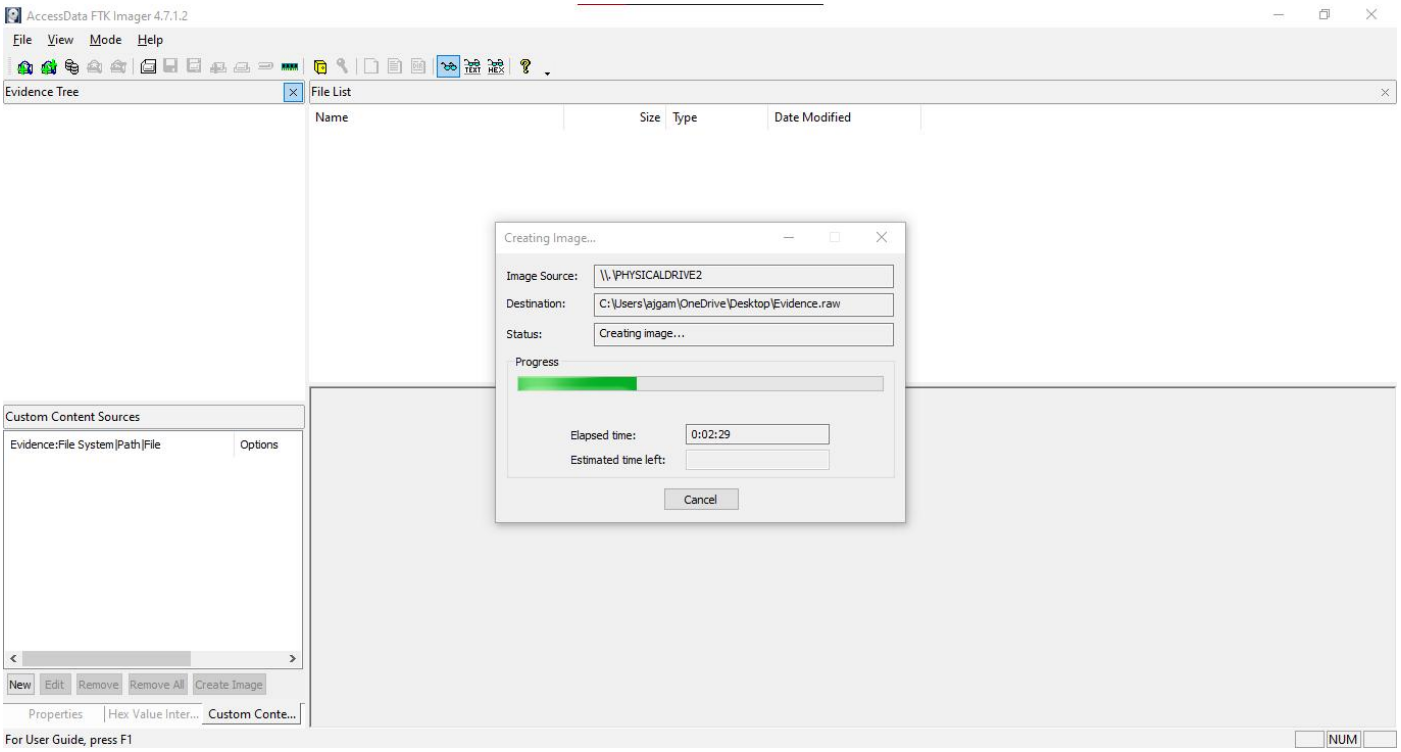
- Filling up the Evidence Item Information.
- Case No : 825 (SRN)



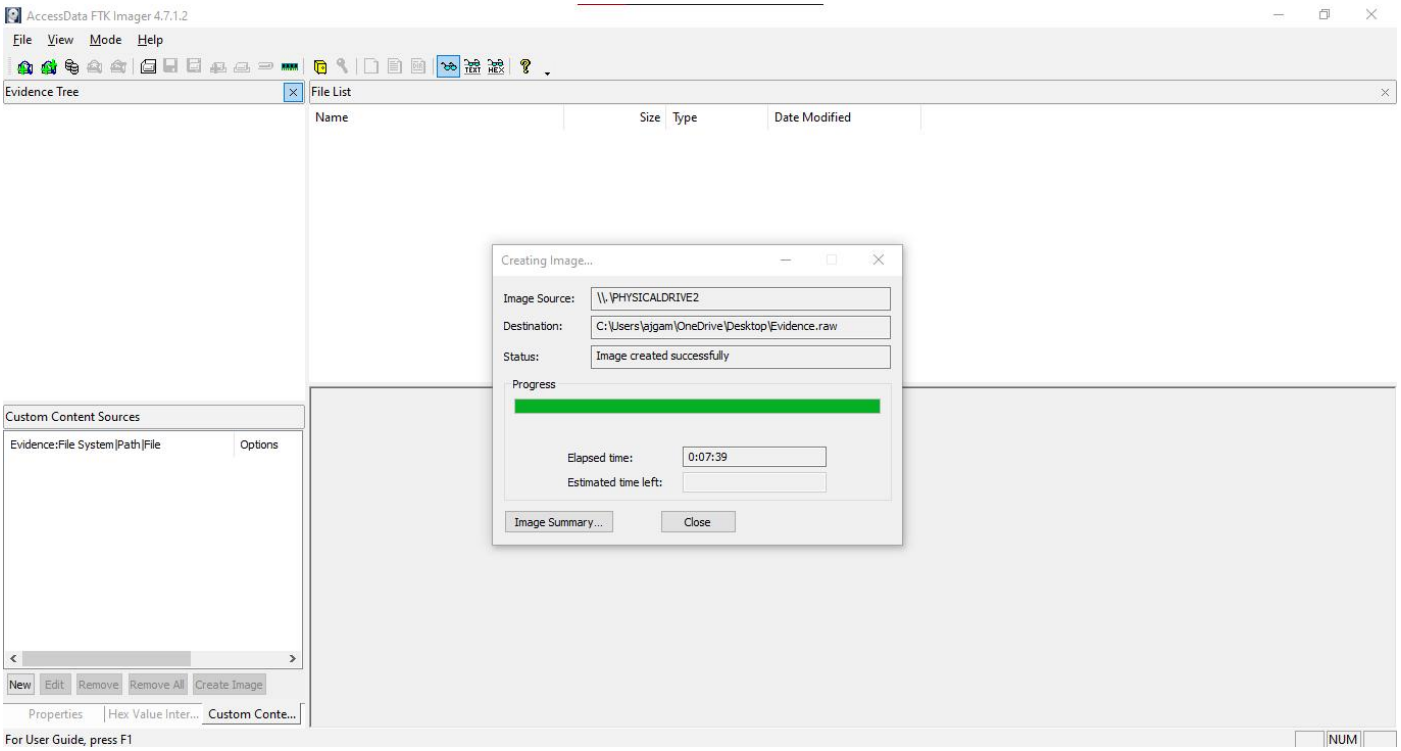
➢ Finally starting the image creation process.



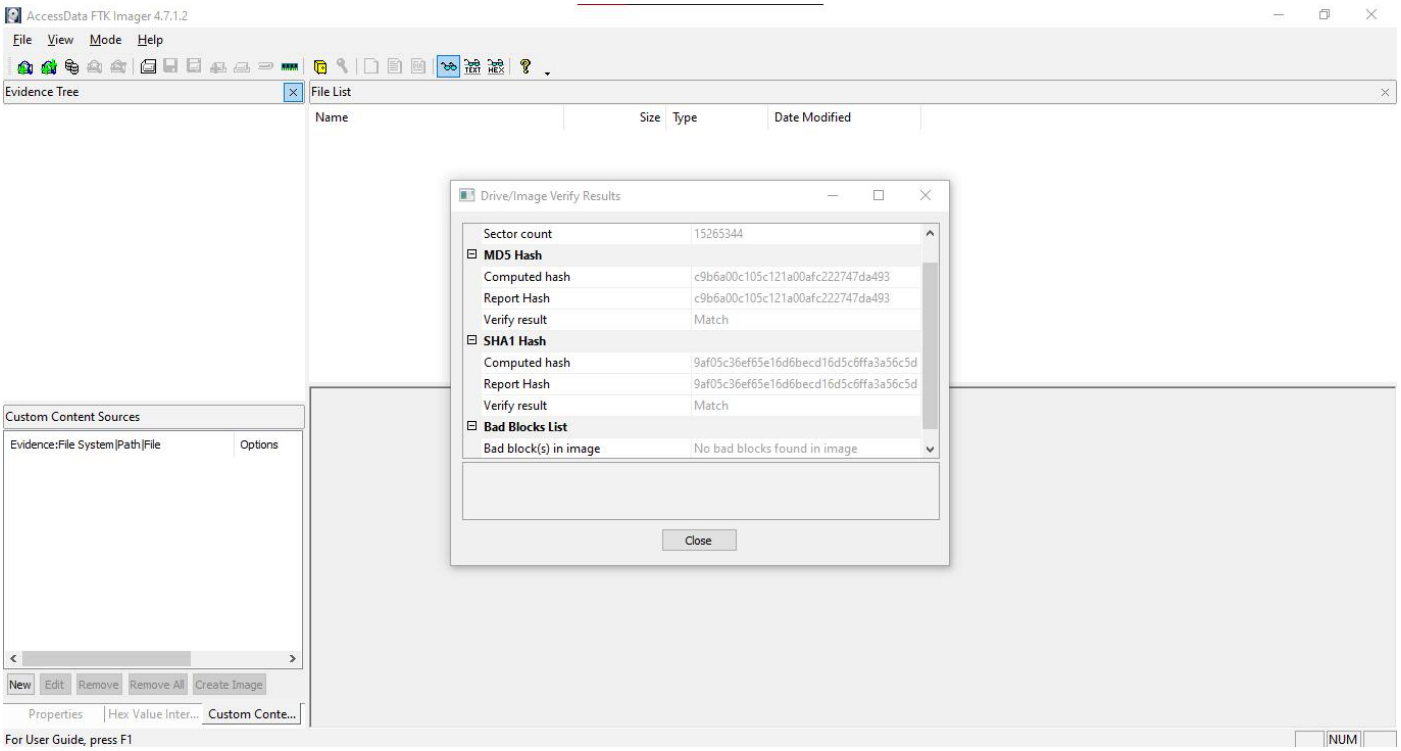
➢ Image Creation Process is Started



➢ Image Created Successfully

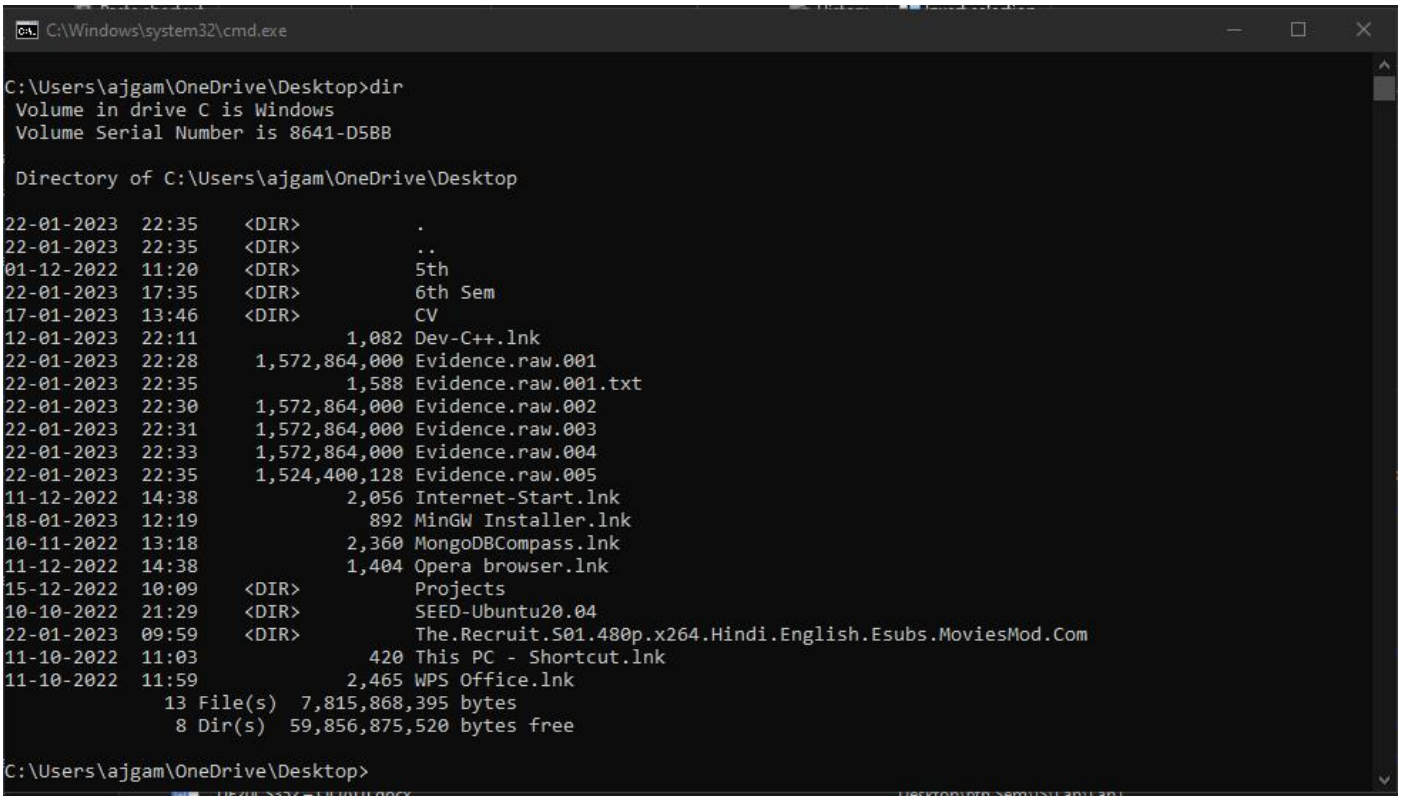


➢ Image verification results.



➢ As we can see after the process is successfully completed all of the created evidence images are in the destination folder the Desktop.

➢ To view the created images we are going to use **dir Command** in the cmd.



```
C:\Windows\system32\cmd.exe

C:\Users\ajgam\OneDrive\Desktop>dir
 Volume in drive C is Windows
 Volume Serial Number is 8641-D5BB

 Directory of C:\Users\ajgam\OneDrive\Desktop

22-01-2023  22:35    <DIR>          .
22-01-2023  22:35    <DIR>          ..
01-12-2022  11:20    <DIR>          5th
22-01-2023  17:35    <DIR>          6th Sem
17-01-2023  13:46    <DIR>          CV
12-01-2023  22:11             1,082 Dev-C++.lnk
22-01-2023  22:28     1,572,864,000 Evidence.raw.001
22-01-2023  22:35             1,588 Evidence.raw.001.txt
22-01-2023  22:30     1,572,864,000 Evidence.raw.002
22-01-2023  22:31     1,572,864,000 Evidence.raw.003
22-01-2023  22:33     1,572,864,000 Evidence.raw.004
22-01-2023  22:35     1,524,400,128 Evidence.raw.005
11-12-2022  14:38             2,056 Internet-Start.lnk
18-01-2023  12:19               892 MinGW Installer.lnk
10-11-2022  13:18             2,360 MongoDBCompass.lnk
11-12-2022  14:38             1,404 Opera browser.lnk
15-12-2022  10:09    <DIR>          Projects
10-10-2022  21:29    <DIR>          SEED-Ubuntu20.04
22-01-2023  09:59    <DIR>          The.Recruit.S01.480p.x264.Hindi.English.Esubs.MoviesMod.Com
11-10-2022  11:03               420 This PC - Shortcut.lnk
11-10-2022  11:59             2,465 WPS Office.lnk
              13 File(s)  7,815,868,395 bytes
               8 Dir(s)  59,856,875,520 bytes free

C:\Users\ajgam\OneDrive\Desktop>
```

```
Evidence.raw.001.txt - Notepad
File  Edit  Format  View  Help
Created By AccessData® FTK® Imager 4.7.1.2

Case Information:
Acquired using: ADI4.7.1.2
Case Number: 825
Evidence Number: 825
Unique description: PES1UG20CS825
Examiner: Prem Sagar J S
Notes: Nothing

---------------------------------------------------------------

Information for C:\Users\ajgam\OneDrive\Desktop\Evidence.raw:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 950
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 15,265,344
[Physical Drive Information]
 Drive Model: JetFlash Transcend 8GB USB Device
 Drive Serial Number: SF1CEKXV
 Drive Interface Type: USB
 Removable drive: True
 Source data size: 7453 MB
 Sector count:    15265344
[Computed Hashes]
 MD5 checksum:    c9b6a00c105c121a00afc222747da493
 SHA1 checksum:   9af05c36ef65e16d6becd16d5c6ffa3a56c5dd48

Image Information:
 Acquisition started:   Sun Jan 22 22:27:23 2023
 Acquisition finished:  Sun Jan 22 22:35:02 2023
 Segment list:
  C:\Users\ajgam\OneDrive\Desktop\Evidence.raw.001
  C:\Users\ajgam\OneDrive\Desktop\Evidence.raw.002
  C:\Users\ajgam\OneDrive\Desktop\Evidence.raw.003
  C:\Users\ajgam\OneDrive\Desktop\Evidence.raw.004
  C:\Users\ajgam\OneDrive\Desktop\Evidence.raw.005

Image Verification Results:
 Verification started:  Sun Jan 22 22:35:05 2023
 Verification finished: Sun Jan 22 22:35:37 2023
 MD5 checksum:    c9b6a00c105c121a00afc222747da493 : verified
 SHA1 checksum:   9af05c36ef65e16d6becd16d5c6ffa3a56c5dd48 : verified
```

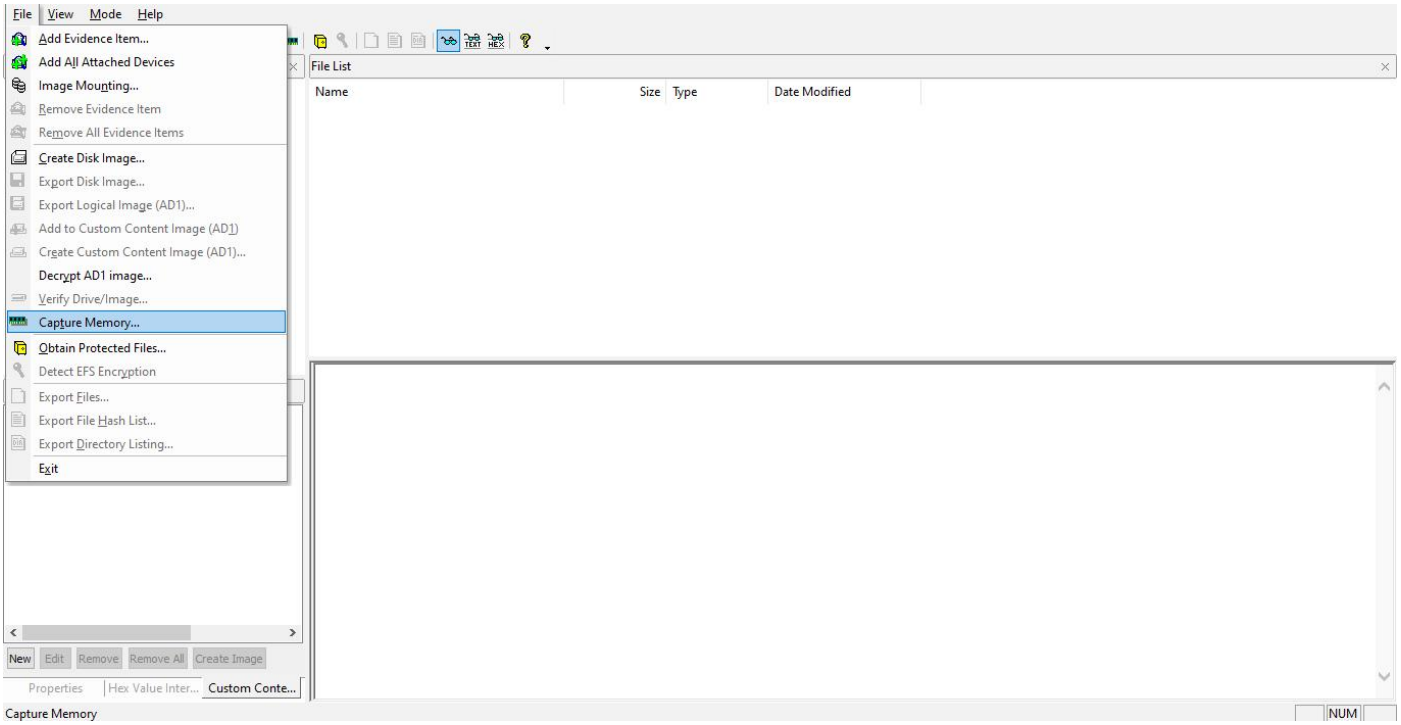
2. Memory Acquisition Using FTK imager

Source: Suspect Workstation
Destination: External USB Disk

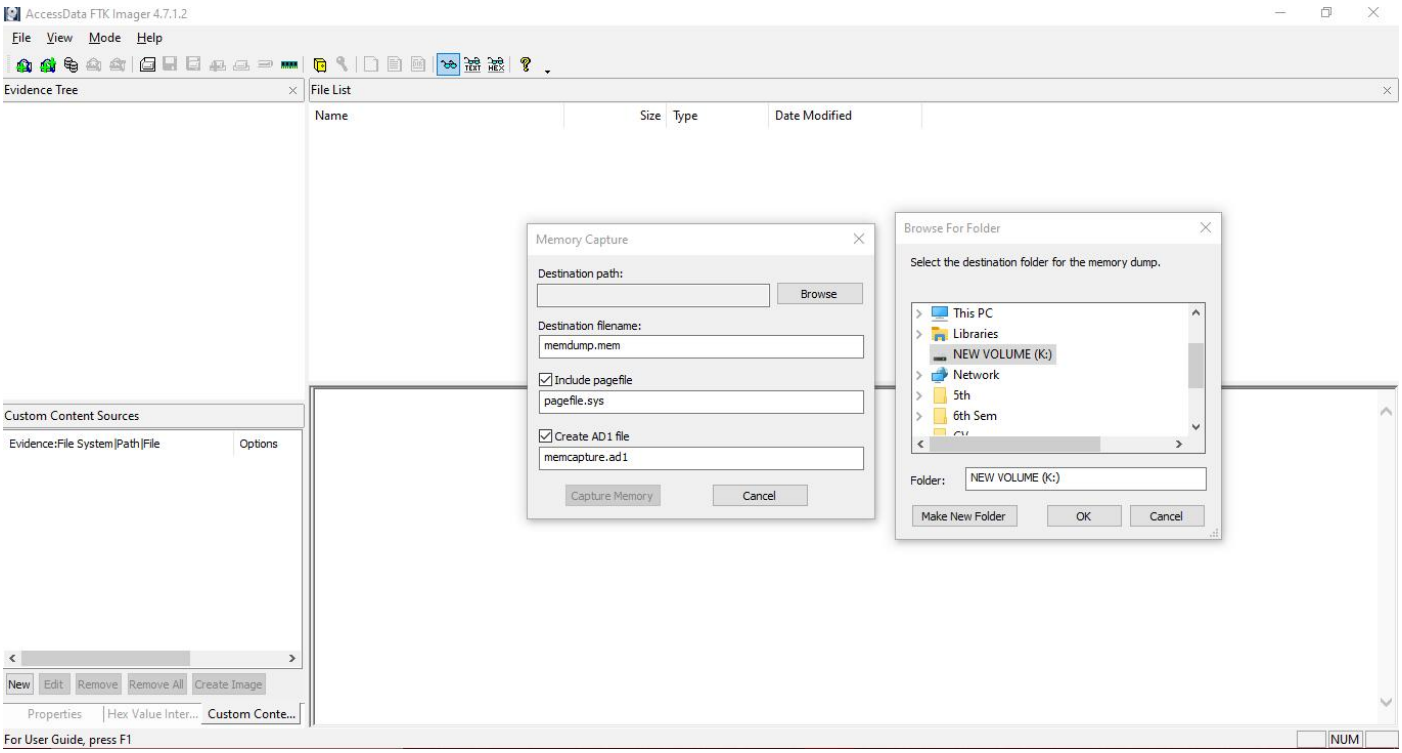
Steps:

File-Capture Memory-enter appropriate details-Capture Memory--Done--Close

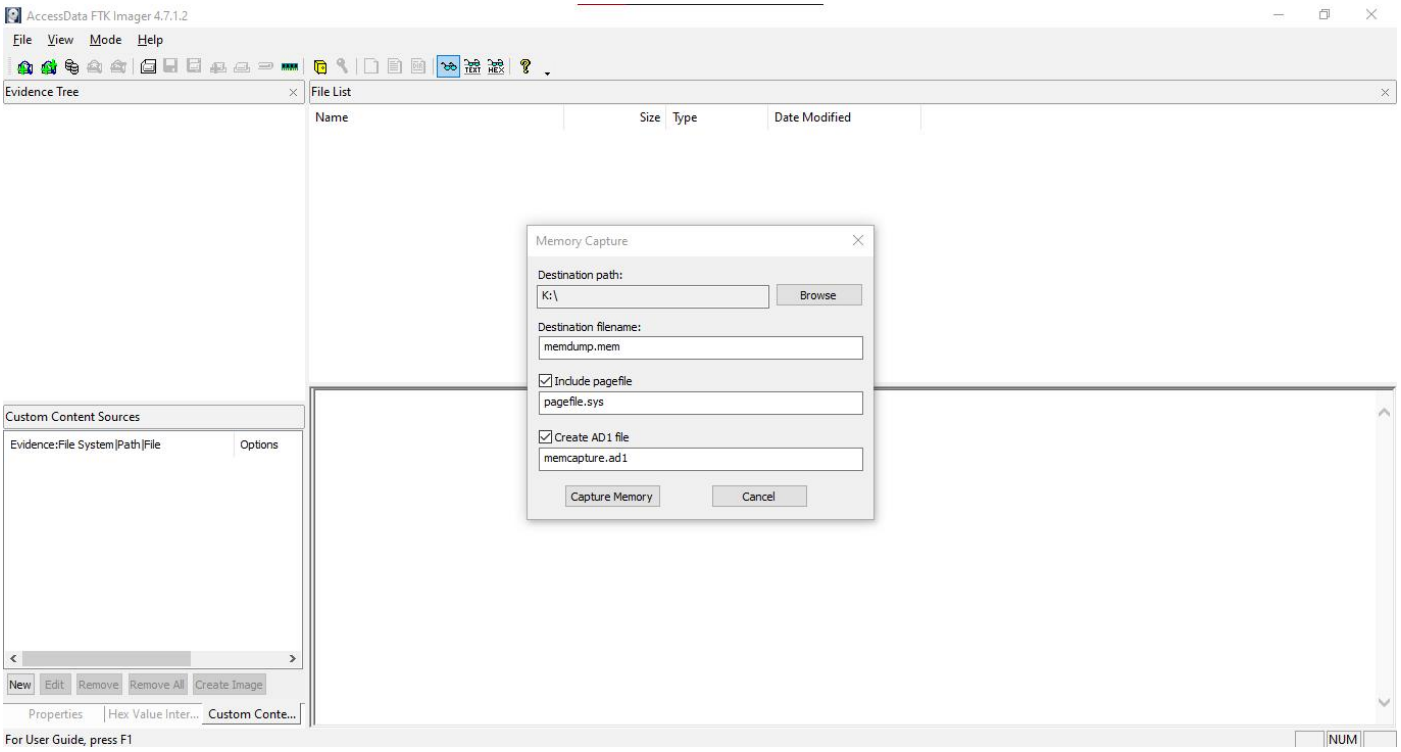
- Pen Drive has been connected to the PC.
- And selecting the capture memory option from the File section of the menu.



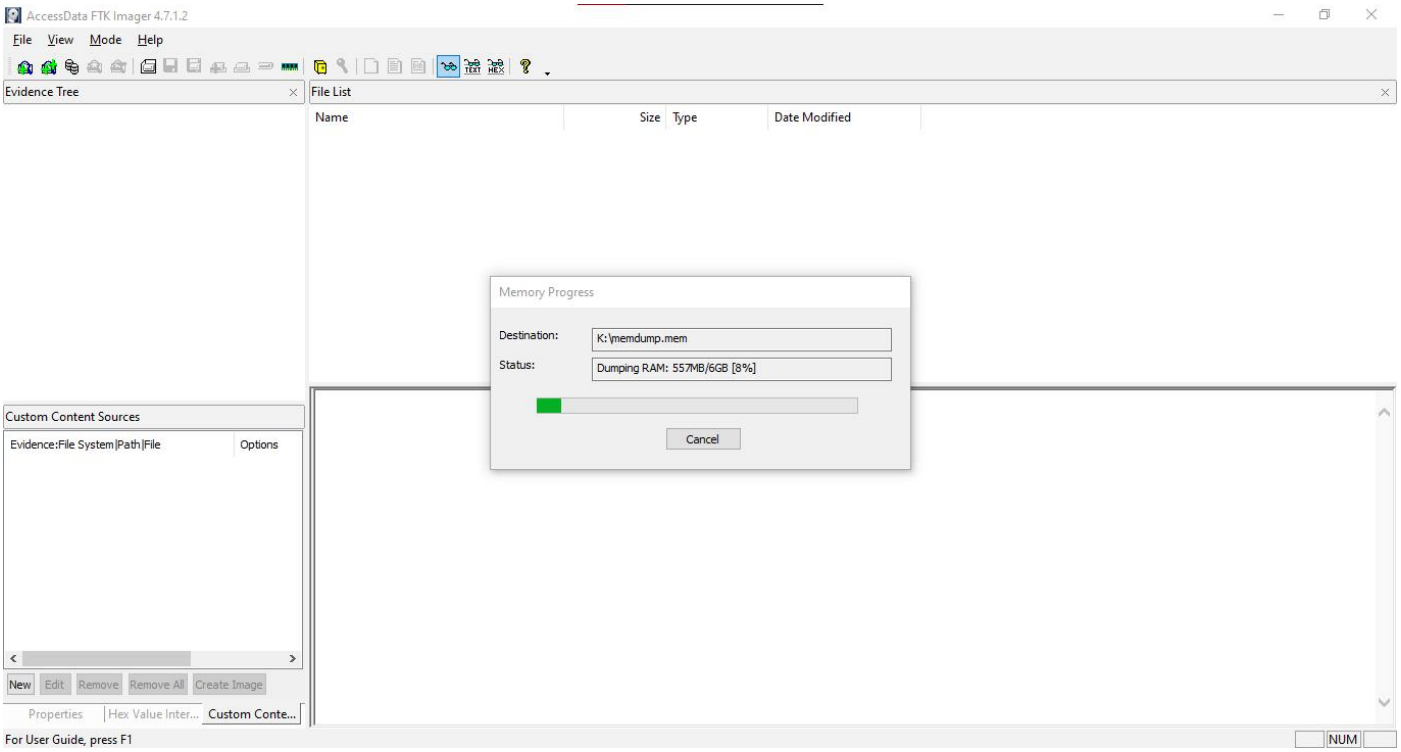
➢ Selecting the destination path as the Pen-Drive (Volume :K)



➢ All the necessary settings are done and now we start capturing memory



- Process has been started



- After the completion of the dumping process.
- A file **memdump.mem** has been created in the pendrive.
- Memdump.mem contains all the captured memory that has been dumped.
- Using DIR command to view the Volume K:\’s Directory