Vellore Institute of Technology

(Deemed to be University under section 3 of the UGC Act, 1956)

WINTER SEMESTER 2019-20
DIGITAL FORENSICS (CSE4004)
LAB ASSIGNMENT - 2

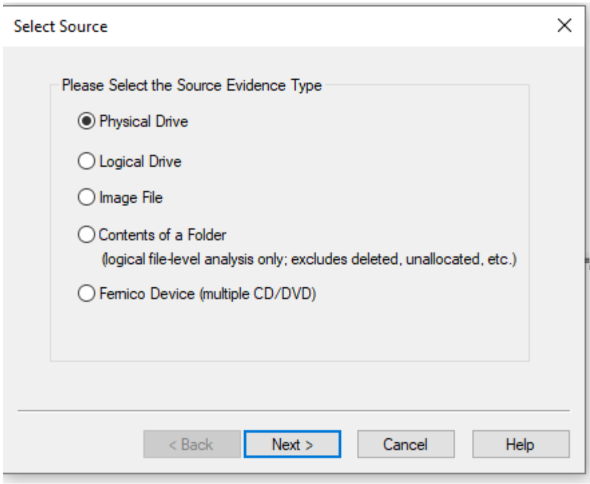
Dishi Jain
17BCB0055

FTK IMAGER

FTK Imager is a data preview and imaging tool that lets you quickly assess electronic evidence to determine if further analysis with a forensic tool such as Access Data® Forensic Toolkit® (FTK) is warranted. FTK Imager can also create perfect copies (forensic images) of computer data without making changes to the original evidence. With FTK Imager, you can:

- Create forensic images of local hard drives, floppy diskettes, Zip disks, CDs, and DVDs, entire folders, or individual files from various places within the media.
- Preview files and folders on local hard drives, network drives, floppy diskettes, Zip disks, CDs, and DVDs
- Preview the contents of forensic images stored on the local machine or on a network drive
- Mount an image for a read-only view that leverages Windows Explorer to see the content of the image exactly as the user saw it on the original drive
- Export files and folders from forensic images.
- See and recover files that have been deleted from the Recycle Bin, but have not yet been overwritten on the drive.
- Create hashes of files using either of the two hash functions available in FTK Imager: Message Digest 5 (MD5) and Secure Hash Algorithm (SHA-1)

- PHYSICAL DRIVE – Generally this is the type used, more info is recovered when using this. All of the data from entire disks is selected.
- The partition to be studied is selected from the drop down menu.
- \\.\PHYSICALDRIVE is how the system reads an recognizes physical



Select Source

Please Select the Source Evidence Type

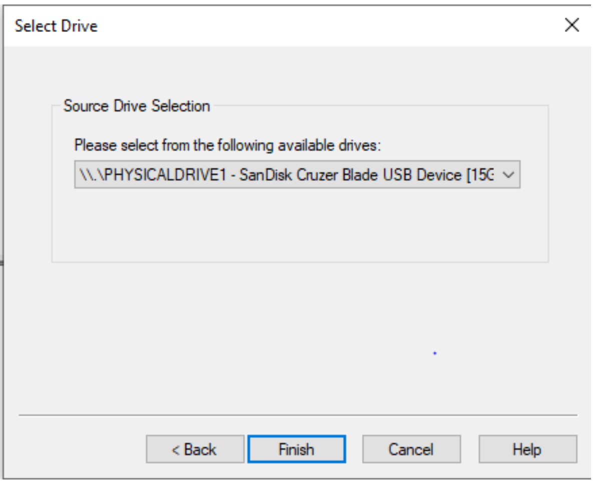
● Physical Drive

○ Logical Drive

○ Image File

○ Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)

○ Femico Device (multiple CD/DVD)



Select Drive

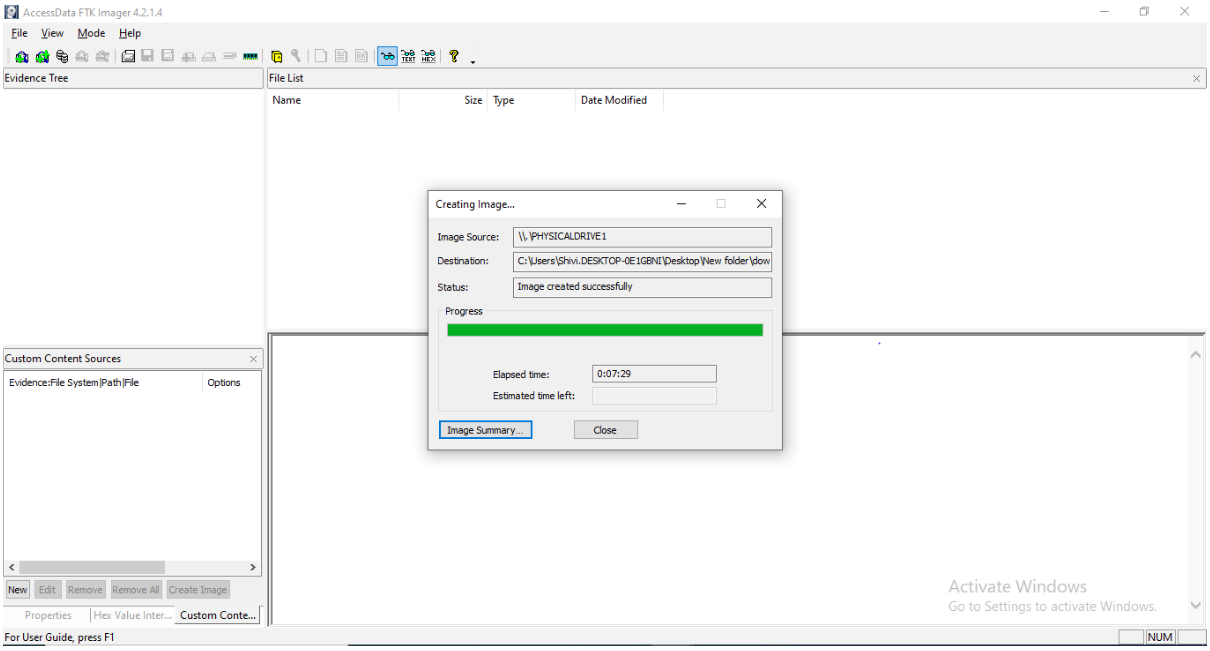
Source Drive Selection

Please select from the following available drives:

\\.\PHYSICALDRIVE1 - SanDisk Cruzer Blade USB Device [15G

Once everything is selected, click on finish.

The, image summary is given after a few time.



AccessData FTK Imager 4.2.1.4

Creating Image...

Image Source: \\.\PHYSICALDRIVE1

Destination: C:\Users\Shivi.DESKTOP-0E1GBNI\Desktop\New folder\dow

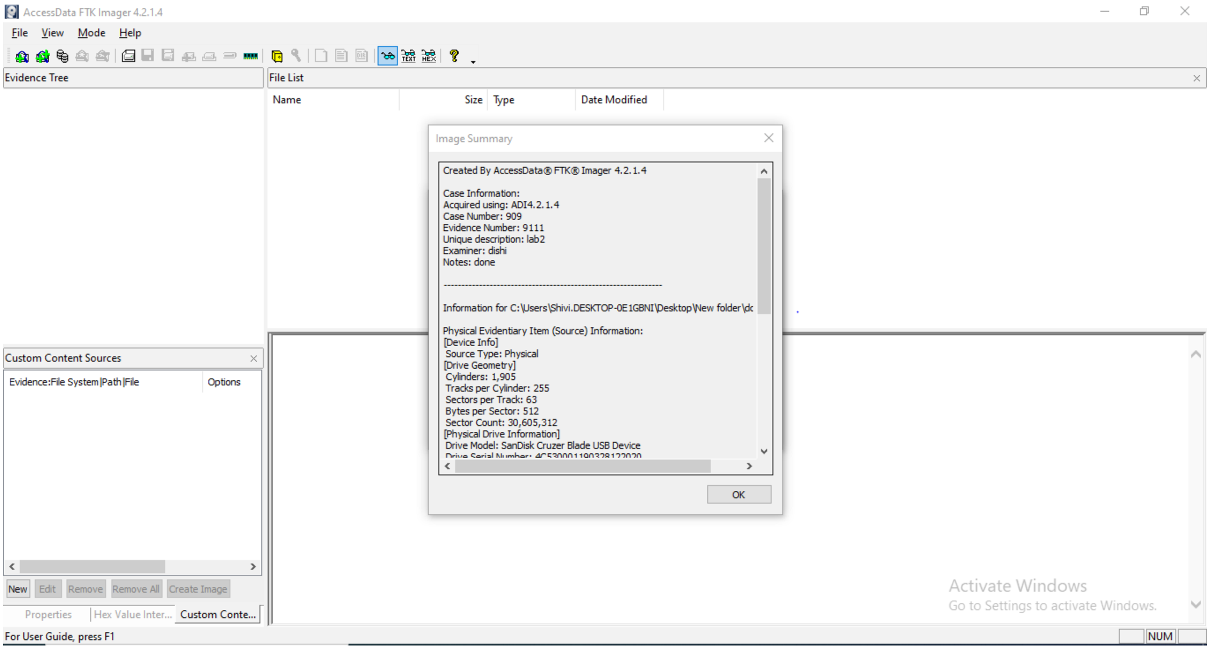
Status: Image created successfully

Progress

Elapsed time: 0:07:29

Estimated time left:

- Hereby is the image summary.



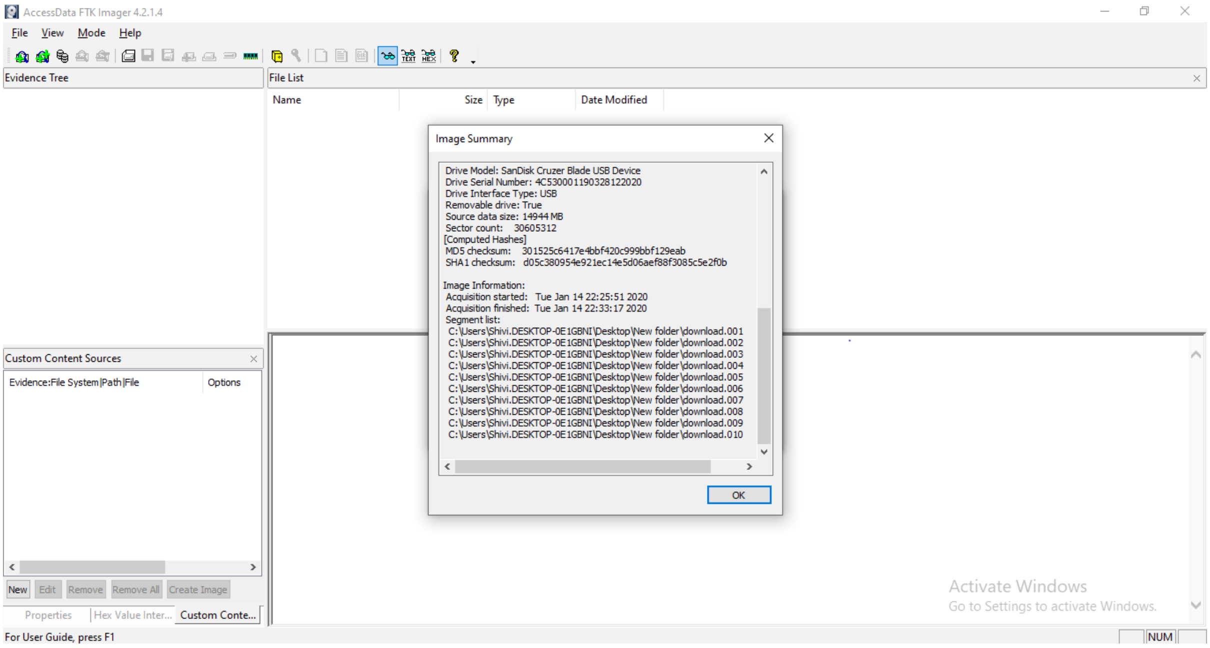
```
Created By AccessData® FTK® Imager 4.2.1.4

Case Information:
Acquired using: ADI4.2.1.4
Case Number: 909
Evidence Number: 9111
Unique description: lab2
Examiner: dishi
Notes: done

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

Information for C:\Users\Shivi.DESKTOP-0E1GBNI\Desktop\New folder\dc

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 1,905
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 30,605,312
[Physical Drive Information]
 Drive Model: SanDisk Cruzer Blade USB Device
 Drive Serial Number: 4C530001190328122020
```



```
 Drive Model: SanDisk Cruzer Blade USB Device
 Drive Serial Number: 4C530001190328122020
 Drive Interface Type: USB
 Removable drive: True
 Source data size: 14944 MB
 Sector count:    30605312
[Computed Hashes]
 MD5 checksum:    301525c6417e4bbf420c999bbf129eab
 SHA1 checksum:   d05c380954e921ec14e5d06aef88f3085c5e2f0b

Image Information:
 Acquisition started:   Tue Jan 14 22:25:51 2020
 Acquisition finished:  Tue Jan 14 22:33:17 2020
 Segment list:
  C:\Users\Shivi.DESKTOP-0E1GBNI\Desktop\New folder\download.001
  C:\Users\Shivi.DESKTOP-0E1GBNI\Desktop\New folder\download.002
  C:\Users\Shivi.DESKTOP-0E1GBNI\Desktop\New folder\download.003
  C:\Users\Shivi.DESKTOP-0E1GBNI\Desktop\New folder\download.004
  C:\Users\Shivi.DESKTOP-0E1GBNI\Desktop\New folder\download.005
  C:\Users\Shivi.DESKTOP-0E1GBNI\Desktop\New folder\download.006
  C:\Users\Shivi.DESKTOP-0E1GBNI\Desktop\New folder\download.007
  C:\Users\Shivi.DESKTOP-0E1GBNI\Desktop\New folder\download.008
  C:\Users\Shivi.DESKTOP-0E1GBNI\Desktop\New folder\download.009
  C:\Users\Shivi.DESKTOP-0E1GBNI\Desktop\New folder\download.010
```