PRACTICAL 1

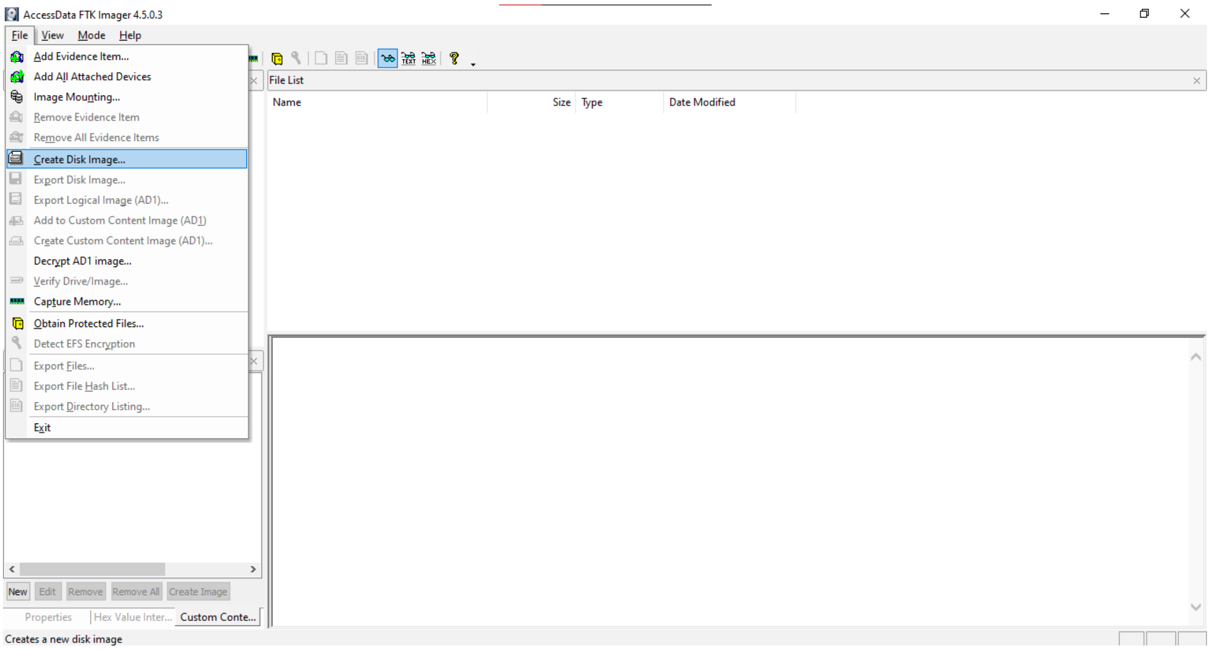
AIM: Creating a Forensic Image using FTK Imager/Encase Imager:

- Creating Forensic Image

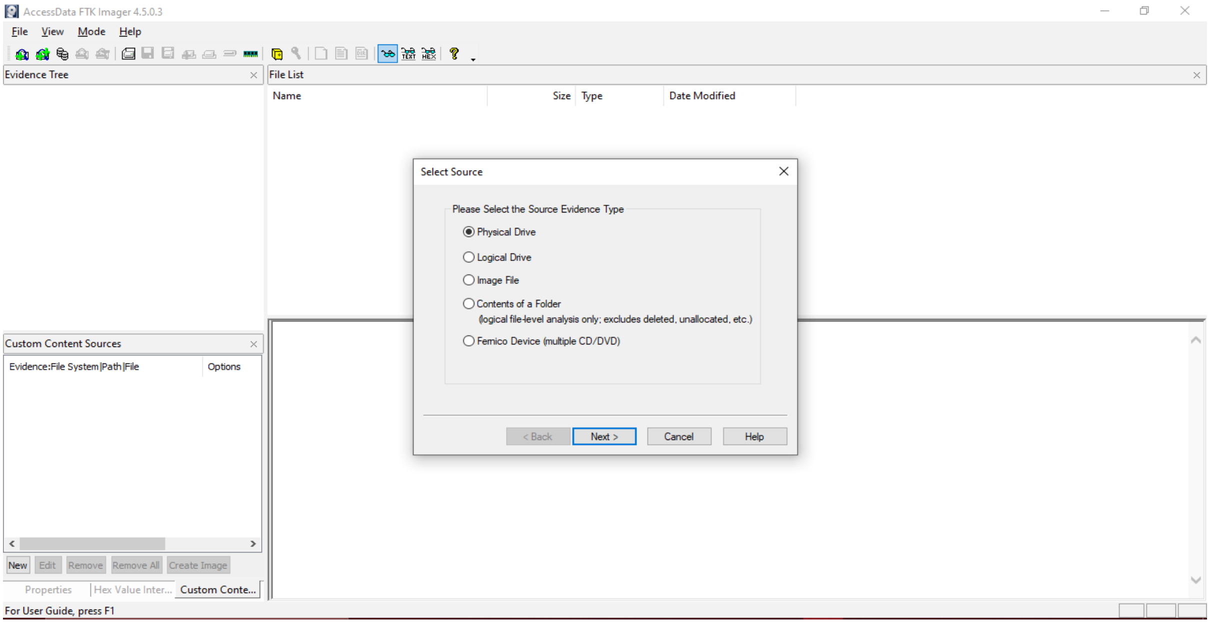
- Check Integrity of Data - Analyze Forensic Image

-Creating Forensic Image.

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



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



Select Source

Please Select the Source Evidence Type

● Physical Drive

○ Logical Drive

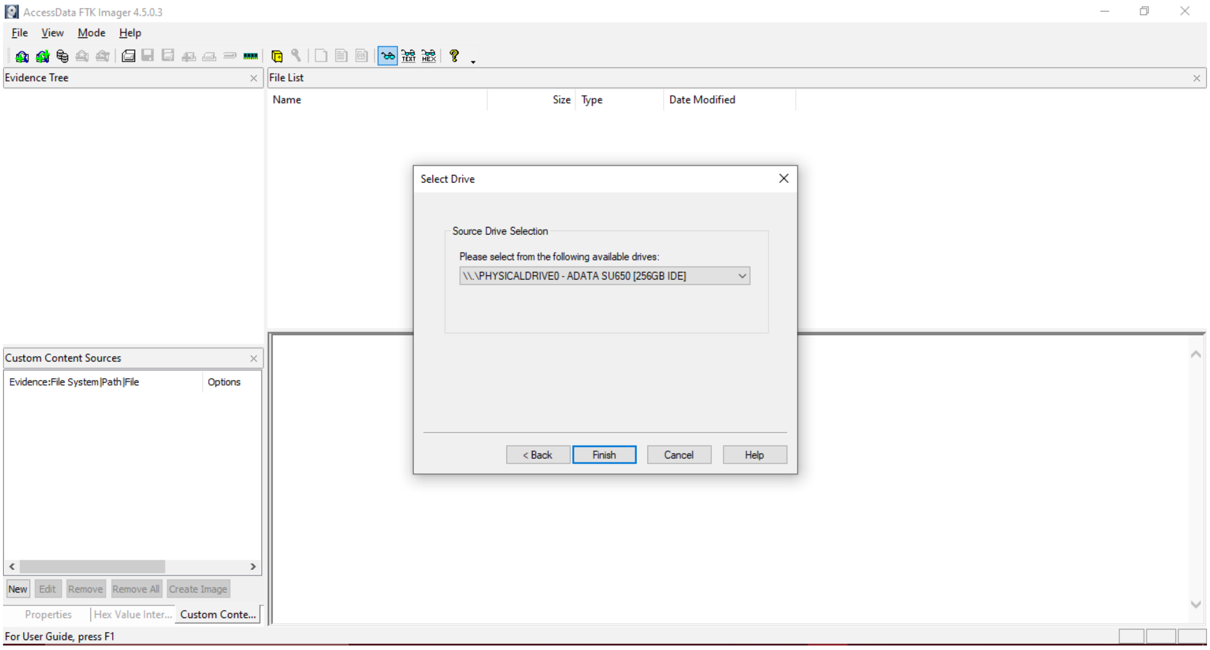
○ Image File

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

○ Fernico Device (multiple CD/DVD)

< Back | Next > | Cancel | Help

Step3: Select the source evidence drive with path.



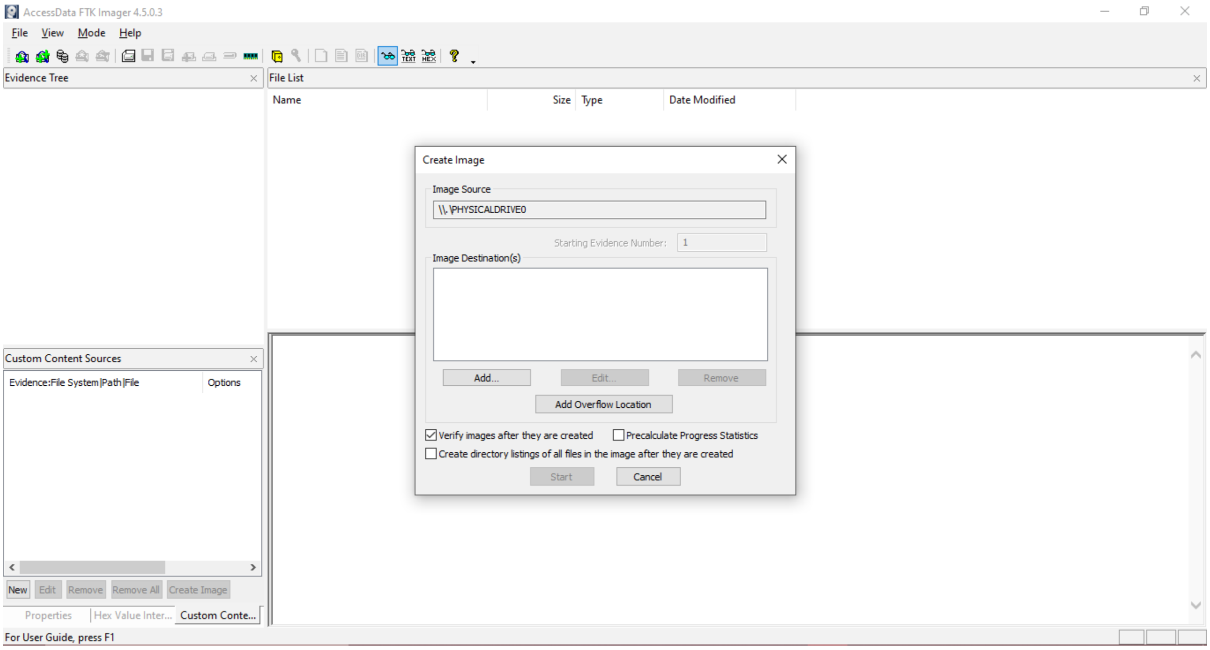
Select Drive

Source Drive Selection

Please select from the following available drives:

\\.\PHYSICALDRIVE0 - ADATA SU650 [256GB IDE]

Click on “add” to add image destination.



Create Image

Image Source

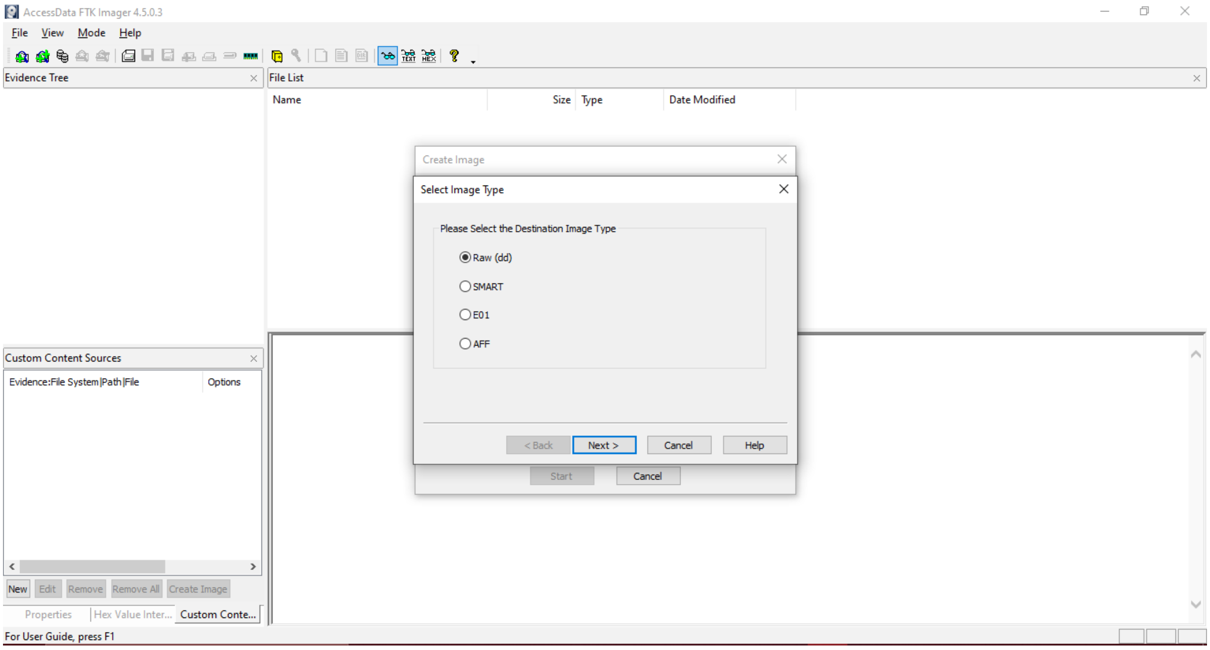
\\.\PHYSICALDRIVE0

Starting Evidence Number: 1

Image Destination(s)

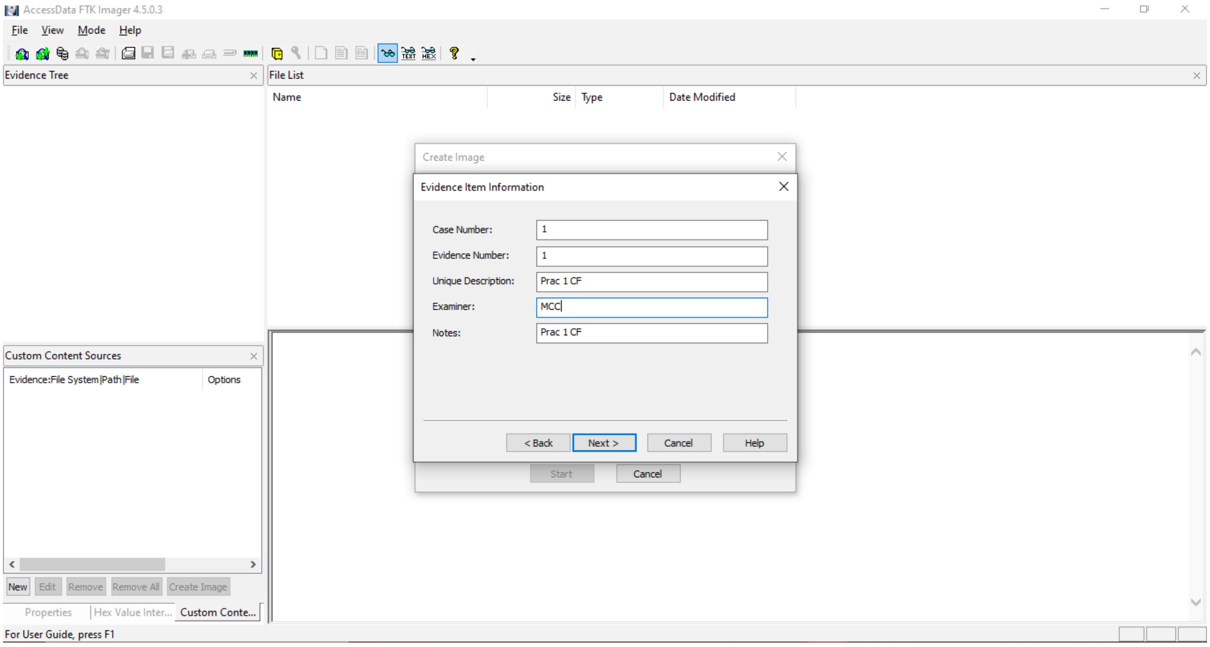
☑ Verify images after they are created □ Precalculate Progress Statistics

□ Create directory listings of all files in the image after they are created


AccessData FTK Imager 4.5.0.3
File View Mode Help
Evidence Tree
File List
Name Size Type Date Modified
Custom Content Sources
Evidence:File System|Path|File Options
New Edit Remove Remove All Create Image
Properties Hex Value Inter... Custom Conte...
For User Guide, press F1
Create Image
Select Image Type
< Back Next > Cancel Help
Start Cancel

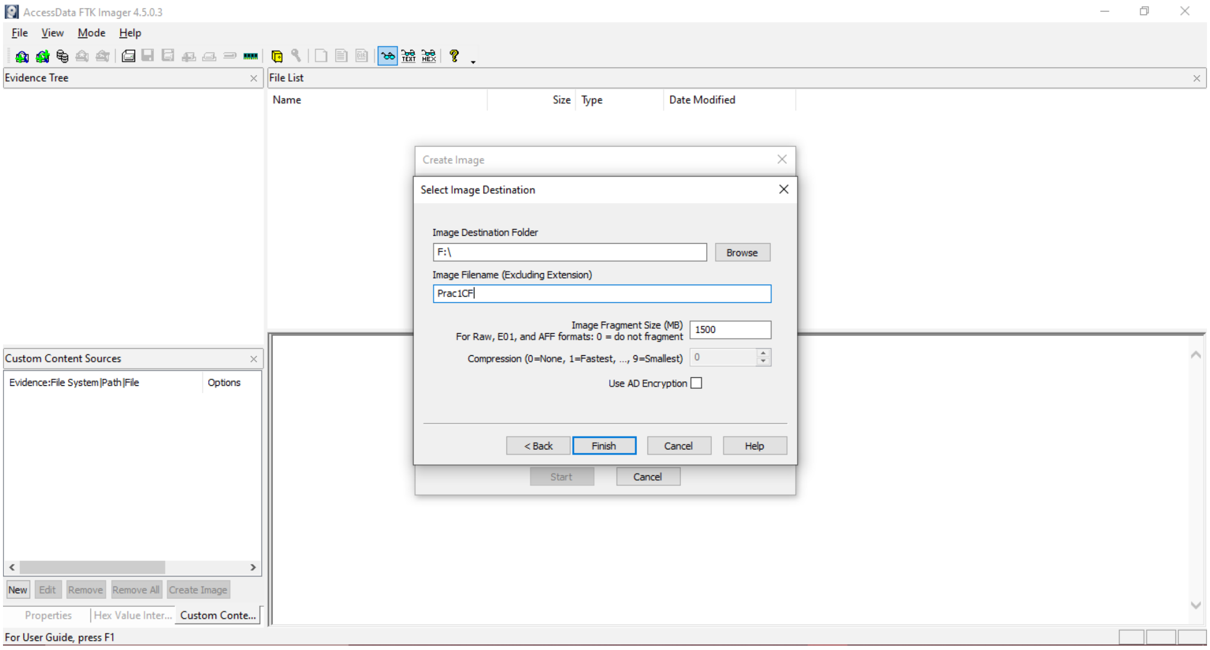
Please Select the Destination Image Type

● Raw (dd)
○ SMART
○ E01
○ AFF


AccessData FTK Imager 4.5.0.3
File View Mode Help
Evidence Tree
File List
Name Size Type Date Modified
Custom Content Sources
Evidence:File System|Path|File Options
New Edit Remove Remove All Create Image
Properties Hex Value Inter... Custom Conte...
For User Guide, press F1
Create Image
Evidence Item Information
< Back Next > Cancel Help
Start Cancel

Case Number:	1
Evidence Number:	1
Unique Description:	Prac 1 CF
Examiner:	MCC
Notes:	Prac 1 CF

Step4: 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.



Select Image Destination

Image Destination Folder: F:\

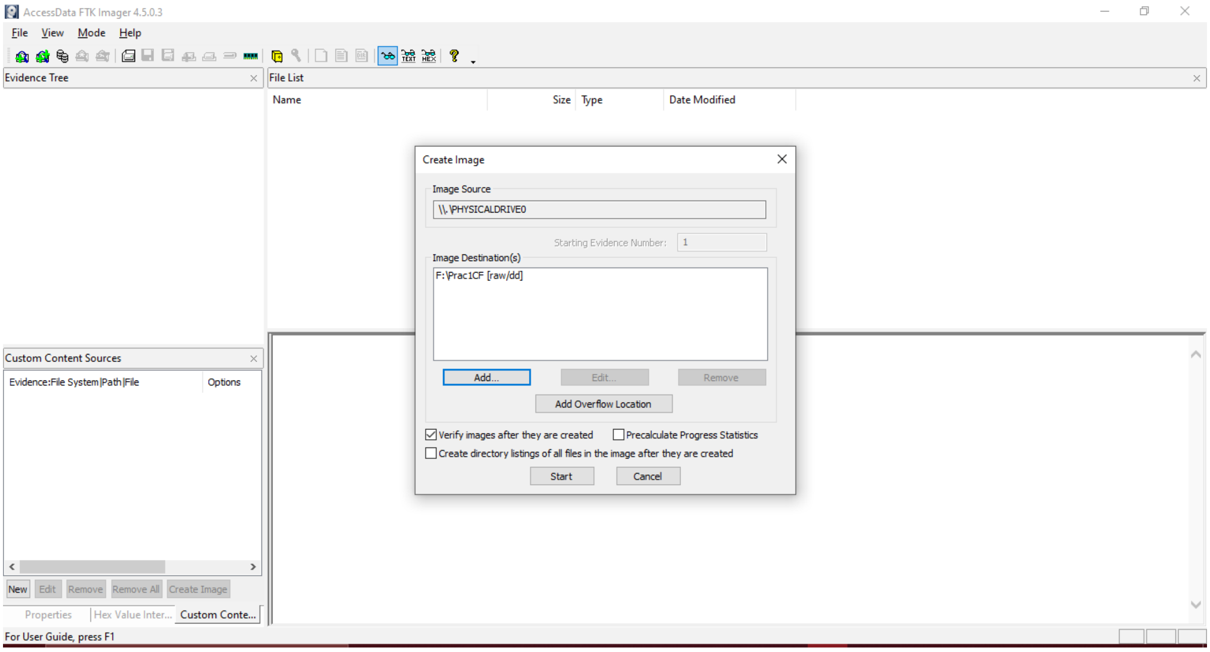
Image Filename (Excluding Extension): Prac1CF

Image Fragment Size (MB) For Raw, E01, and AFF formats: 0 = do not fragment: 1500

Compression (0=None, 1=Fastest, ..., 9=Smallest): 0

Use AD Encryption □

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



Create Image

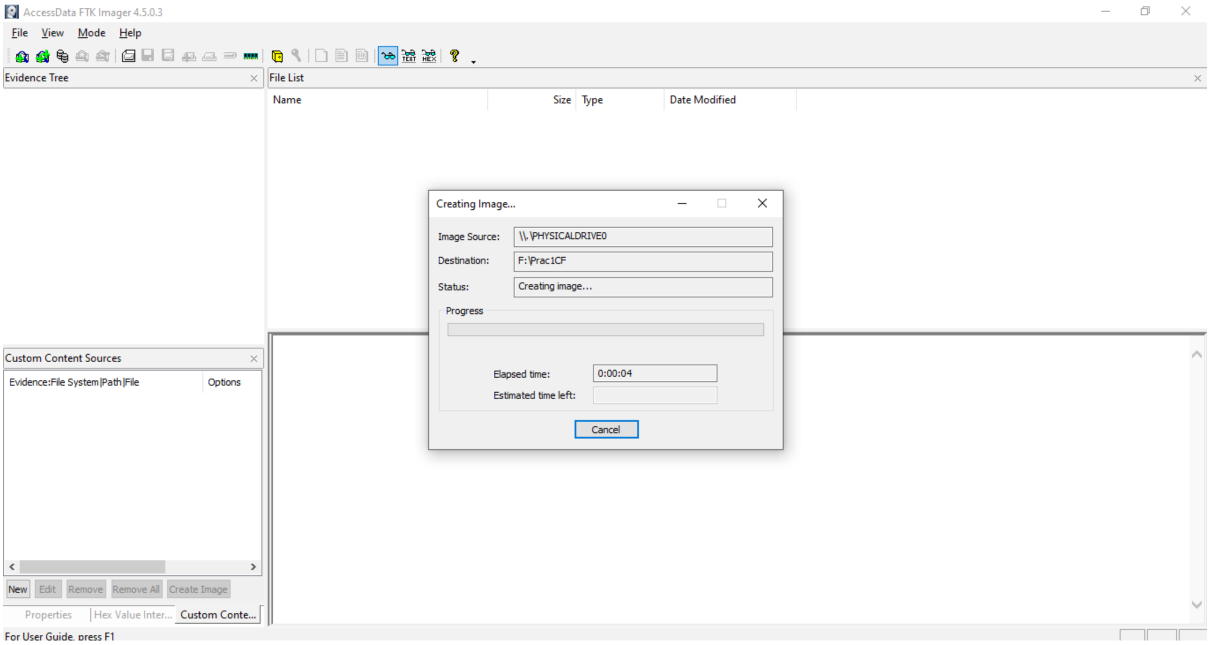
Image Source: \\.\PHYSICALDRIVE0

Starting Evidence Number: 1

Image Destination(s): F:\Prac1CF [raw/dd]

☑ Verify images after they are created □ Precalculate Progress Statistics

□ Create directory listings of all files in the image after they are created


AccessData FTK Imager 4.5.0.3
File View Mode Help
Evidence Tree
File List
Name Size Type Date Modified
Custom Content Sources
Evidence:File System|Path|File Options
New Edit Remove Remove All Create Image
Properties Hex Value Inter... Custom Conte...
For User Guide, press F1

Creating Image...

Image Source: \\.\PHYSICALDRIVE0

Destination: F:\Prac1CF

Status: Creating image...

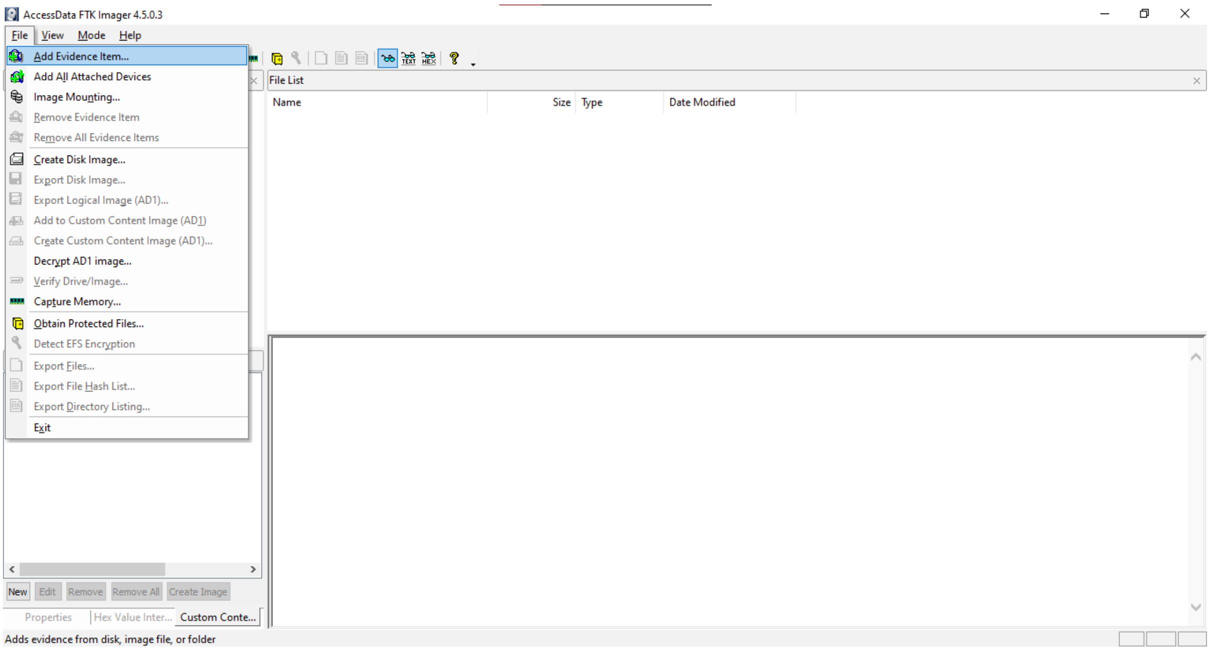
Progress

Elapsed time: 0:00:04

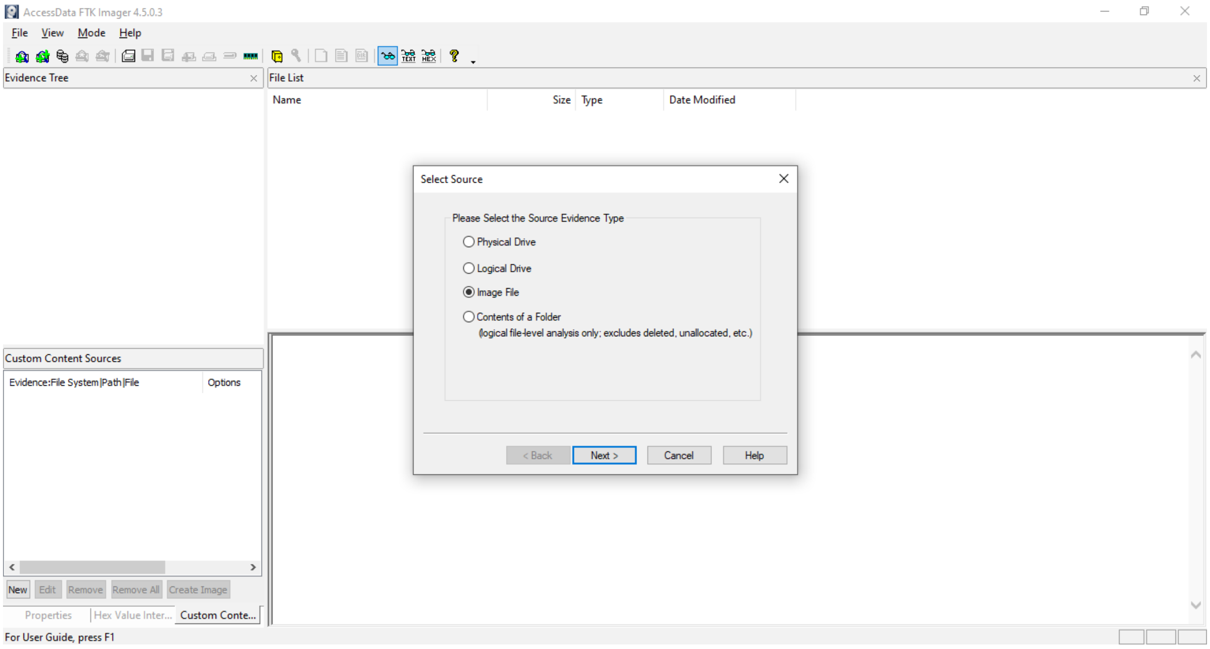
Estimated time left:

Analyse Forensic Image:

Step 6: The images are successfully created. Now Click on Add Evidence Item to add evidence from disk, image file or folder.


AccessData FTK Imager 4.5.0.3
File View Mode Help
Add Evidence Item...
Add All Attached Devices
Image Mounting...
Remove Evidence Item
Remove All Evidence Items
Create Disk Image...
Export Disk Image...
Export Logical Image (AD1)...
Add to Custom Content Image (AD1)
Create Custom Content Image (AD1)...
Decrypt AD1 image...
Verify Drive/Image...
Capture Memory...
Obtain Protected Files...
Detect EFS Encryption
Export Files...
Export File Hash List...
Export Directory Listing...
Exit
File List
Name Size Type Date Modified
New Edit Remove Remove All Create Image
Properties Hex Value Inter... Custom Conte...
Adds evidence from disk, image file, or folder

Now select the source evidence type as image file.



Select Source

Please Select the Source Evidence Type

○ Physical Drive

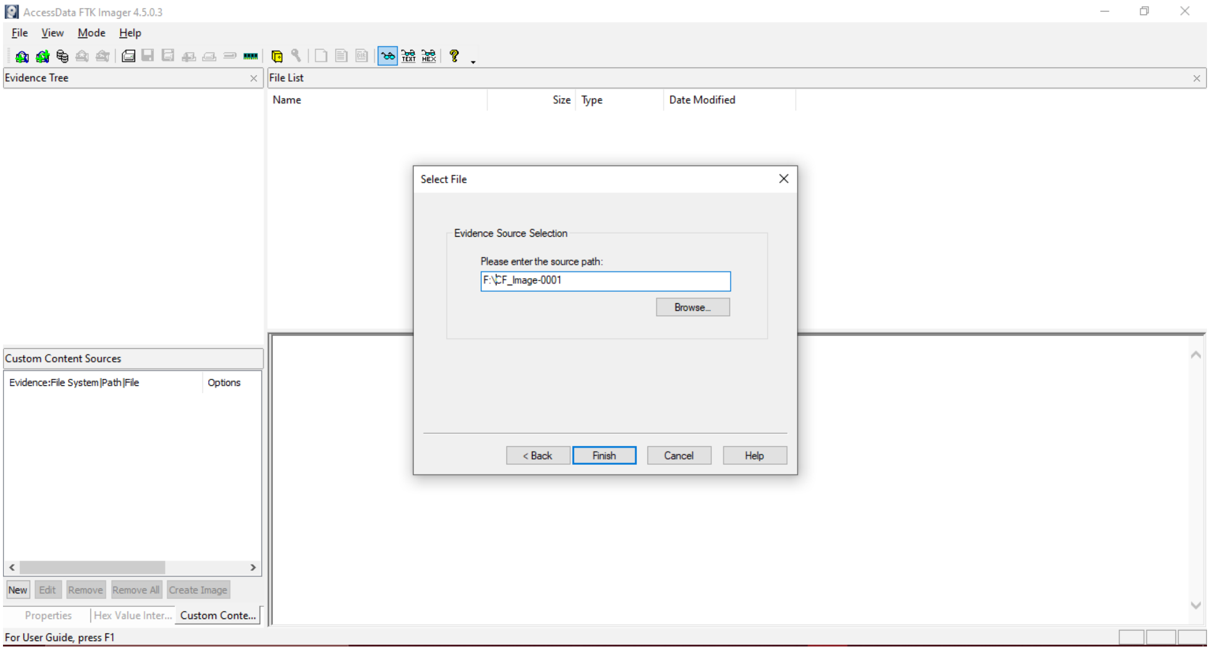
○ Logical Drive

● Image File

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

< Back | Next > | Cancel | Help

Open the created evidence image file.



Select File

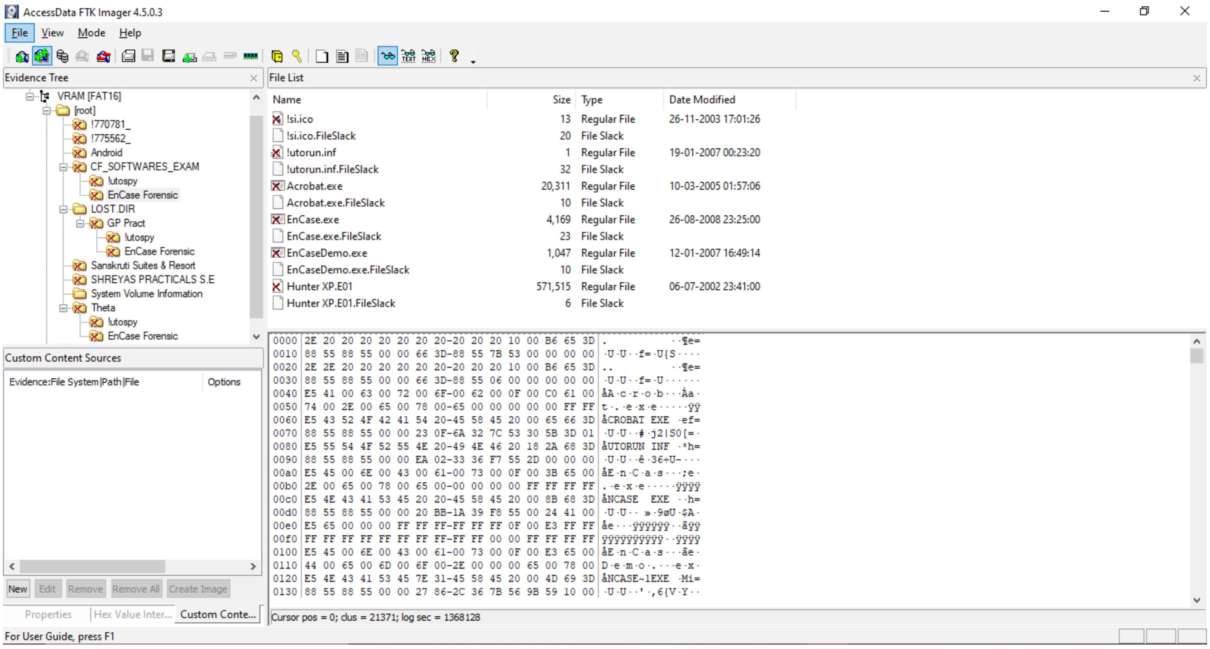
Evidence Source Selection

Please enter the source path:
F:\CF_Image-0001

Browse...

< Back | Finish | Cancel | Help

Step 7: Now select Evidence Tree and analyse the image file.



```
VRAM [FAT16]
  [root]
    !770781_
    !775562_
    Android
    CF_SOFTWARES_EXAM
      !utospy
      EnCase Forensic
    LOST.DIR
      GP Pract
        !utospy
        EnCase Forensic
    Sanskruti Suites & Resort
    SHREYAS PRACTICALS S.E
    System Volume Information
    Theta
      !utospy
      EnCase Forensic
```

Name	Size	Type	Date Modified
!si.ico	13	Regular File	26-11-2003 17:01:26
!si.ico.FileSlack	20	File Slack	
!utorun.inf	1	Regular File	19-01-2007 00:23:20
!utorun.inf.FileSlack	32	File Slack	
Acrobat.exe	20,311	Regular File	10-03-2005 01:57:06
Acrobat.exe.FileSlack	10	File Slack	
EnCase.exe	4,169	Regular File	26-08-2008 23:25:00
EnCase.exe.FileSlack	23	File Slack	
EnCaseDemo.exe	1,047	Regular File	12-01-2007 16:49:14
EnCaseDemo.exe.FileSlack	10	File Slack	
Hunter XP.E01	571,515	Regular File	06-07-2002 23:41:00
Hunter XP.E01.FileSlack	6	File Slack	

```
0000 2E 20 20 20 20 20 20 20-20 20 20 10 00 B6 65 3D .          ··¶e=
0010 88 55 88 55 00 00 66 3D-88 55 7B 53 00 00 00 00 ·U·U··f=·U{S····
0020 2E 2E 20 20 20 20 20 20-20 20 20 10 00 B6 65 3D ..         ··¶e=
0030 88 55 88 55 00 00 66 3D-88 55 06 00 00 00 00 00 ·U·U··f=·U······
0040 E5 41 00 63 00 72 00 6F-00 62 00 0F 00 C0 61 00 åA·c·r·o·b···Àa·
0050 74 00 2E 00 65 00 78 00-65 00 00 00 00 00 FF FF t·.·e·x·e·····ÿÿ
0060 E5 43 52 4F 42 41 54 20-45 58 45 20 00 65 66 3D åCROBAT EXE ·ef=
0070 88 55 88 55 00 00 23 0F-6A 32 7C 53 30 5B 3D 01 ·U·U··#·j2|S0[=·
0080 E5 55 54 4F 52 55 4E 20-49 4E 46 20 18 2A 68 3D åUTORUN INF ·*h=
0090 88 55 88 55 00 00 EA 02-33 36 F7 55 2D 00 00 00 ·U·U··ê·36÷U-···
00a0 E5 45 00 6E 00 43 00 61-00 73 00 0F 00 3B 65 00 åE·n·C·a·s···;e·
00b0 2E 00 65 00 78 00 65 00-00 00 00 00 FF FF FF FF .·e·x·e·····ÿÿÿÿ
00c0 E5 4E 43 41 53 45 20 20-45 58 45 20 00 8B 68 3D åNCASE  EXE ··h=
00d0 88 55 88 55 00 00 20 BB-1A 39 F8 55 00 24 41 00 ·U·U·· »·9øU·$A·
00e0 E5 65 00 00 00 FF FF FF-FF FF FF 0F 00 E3 FF FF åe···ÿÿÿÿÿÿ··ãÿÿ
00f0 FF FF FF FF FF FF FF FF-FF FF 00 00 FF FF FF FF ÿÿÿÿÿÿÿÿÿÿ··ÿÿÿÿ
0100 E5 45 00 6E 00 43 00 61-00 73 00 0F 00 E3 65 00 åE·n·C·a·s···ãe·
0110 44 00 65 00 6D 00 6F 00-2E 00 00 00 65 00 78 00 D·e·m·o·.···e·x·
0120 E5 4E 43 41 53 45 7E 31-45 58 45 20 00 4D 69 3D åNCASE~1EXE ·Mi=
0130 88 55 88 55 00 00 27 86-2C 36 7B 56 9B 59 10 00 ·U·U··'·,6{V·Y··
```

Cursor pos = 0; clus = 21371; log sec = 1368128