FTK-IMAGER

AIM: To familiarize Bit level Forensic Analysis of evidential image

DESCRIPTION:

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.

Need for a Forensic Image :

- In today's world of crime, many cases have been solved by using this technique, as evidence apart from what is available through an operating system, has been found using this technique, as incriminating data might have deleted to prevent discovery during the investigation. Unless that data is overwritten and deleted securely, it can be recovered.
- One of the advantages includes the prevention of the loss of critical files.

- When you suspect a custodian of deleting or altering files. A complete forensic image will, to a certain extent, allow you to recover deleted files. It can also potentially be used to identify files that have been renamed or hidden.
- When you expect that the scope of your investigation could increase at a later date. If you aren't sure about the scope of your project, ALWAYS OVER COLLECT. It's better to have too much data than not enough, and you can't get much more data than a forensic image.
- When you expect that you or someone in your organization may need to certify or testify to the forensic soundness of the collection. In most cases, this need will never arise, but will almost certainly come into play in any criminal or potential criminal proceedings.
- The Imaging of random access memory (RAM) can be enabled by using Live imaging. Live imaging can bypass most encryption.

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.

With FTK Imager, you can:

- Create forensic images or perfect copies of local hard drives, floppy and Zip disks, DVDs, folders, individual files, etc. without making changes to the original evidence.
- Preview files and folders on local hard drives, network drives, floppy diskettes, Zip disks, CDs, and DVDs.
- You can also preview the contents of the forensic images that might be stored on a local machine or drive.
- You can also mount an image for a read-only view that will also allow you to view the contents of the forensic image exactly as the user saw it on the original drive.

- Export files and folders from forensic images.
- View and recover files that have been deleted from the Recycle Bin, but have not yet been overwritten on the drive.

Pros Of FTK Imager

- It has a simple user interface and advanced searching capabilities.
- FTK supports EFS decryption.
- It produces a case log file.
- It has significant bookmarking and salient reporting features.
- FTK Imager is free.

Cons Of FTK Imager

- FTK does not support scripting features.
- It does not have multitasking capabilities.
- There is no progress bar to estimate the time remaining.
- FTK does not have a timeline view.

PROCEDURE:

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

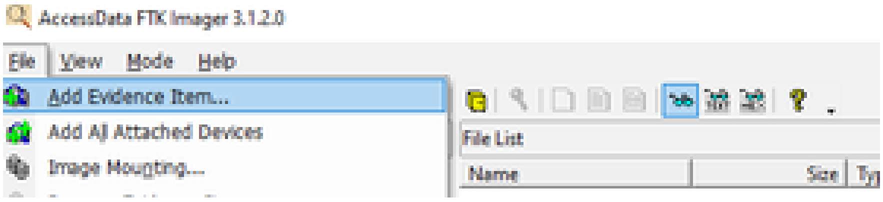
FTK Imager from Access Data, which can be downloaded using the following link: FTK Imager from Access DataA Hard Drive that you would like to create an image of.

Method :

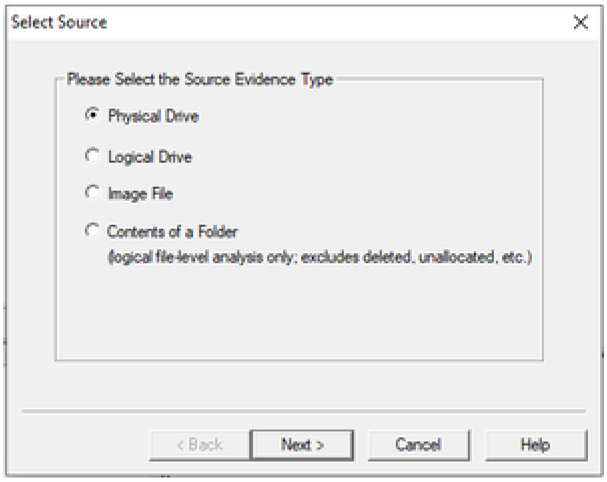
Step 1: Download and install the FTK imager on your machine.

Step 2: Click and open the FTK Imager, once it is installed. You should be greeted with the FTK Imager dashboard.

Step 3: In the menu navigation bar, you need to click on the *File* tab which will give you a drop-down, like given in the image below, just click on the first one that says, *Add Evidence Item*.



Step 4: After that, there will be a pop-up window that will ask you to Select the Source of the Evidence. If you have connected a physical hard drive to the laptop/computer you are using to make the forensic image, then you will select the Physical Drive here. Click on *Next.* Now, Select the *Physical Drive* that you would like to use. Please make sure that you are selecting the right drive, or you will waste your time exporting a forensic image of your own OS drive.


Select Source

Please Select the Source Evidence Type

● Physical Drive

○ Logical Drive

○ Image File

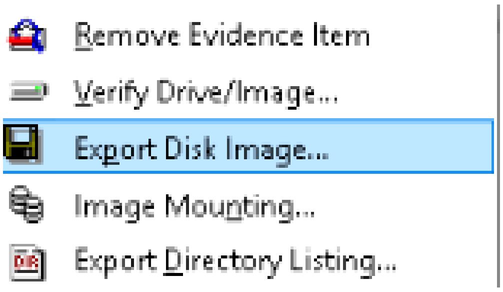
○ Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)

Step 5: Now, we will export the forensic images.

- Right-click on the Physical Drive that you would like to export in the FTK Imager window. Select *Export Disk Image* here.
- Click the *Add* button for the Image Destination.
- Select the Type of Forensic Image you would like to export. Select *E01* and Click *Next.*

- After that, you will have to enter information regarding the case now. You can either leave them blank or keep it general, this part is totally upon you.
- Next, you will need to Choose the Destination that you would like to export the forensic image and Name the Image.

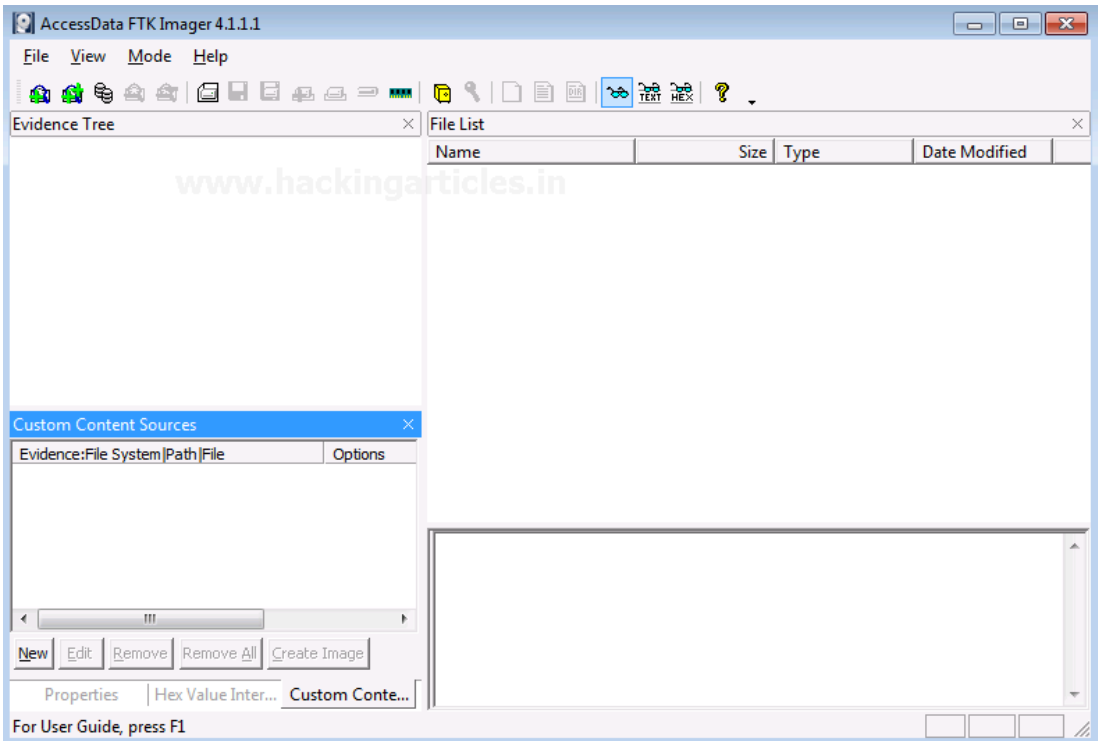
Lastly, you will need to wait for the Forensic Image to be created and then verified. The speed of creating the forensic image will vary based on your hardware. Once both have occurred, you have your forensic images ready.



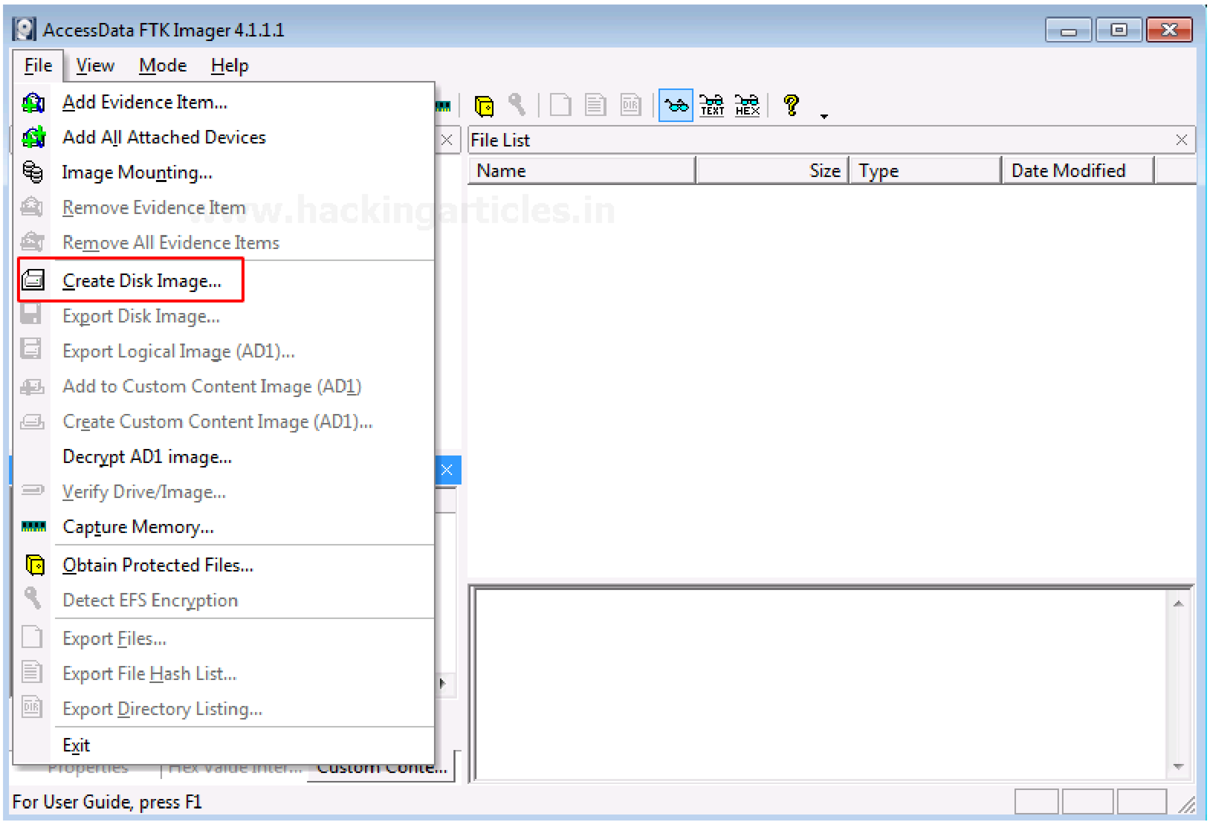
Creating a Forensic Image

Forensic Imaging is one of the most crucial steps involved in digital forensic investigation. It is the process of making an archival or backup copy of the entire hard drive. It is a storage file that contains all the necessary information to boot to the operating system. However, this imaged disk needs to be applied to the hard drive to work. One cannot restore a hard drive by placing the disk image files on it as it needs to be opened and installed on the drive using an imaging program. A single hard drive can store many disk images on it. Disk images can also be stored on flash drives with a larger capacity.

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.

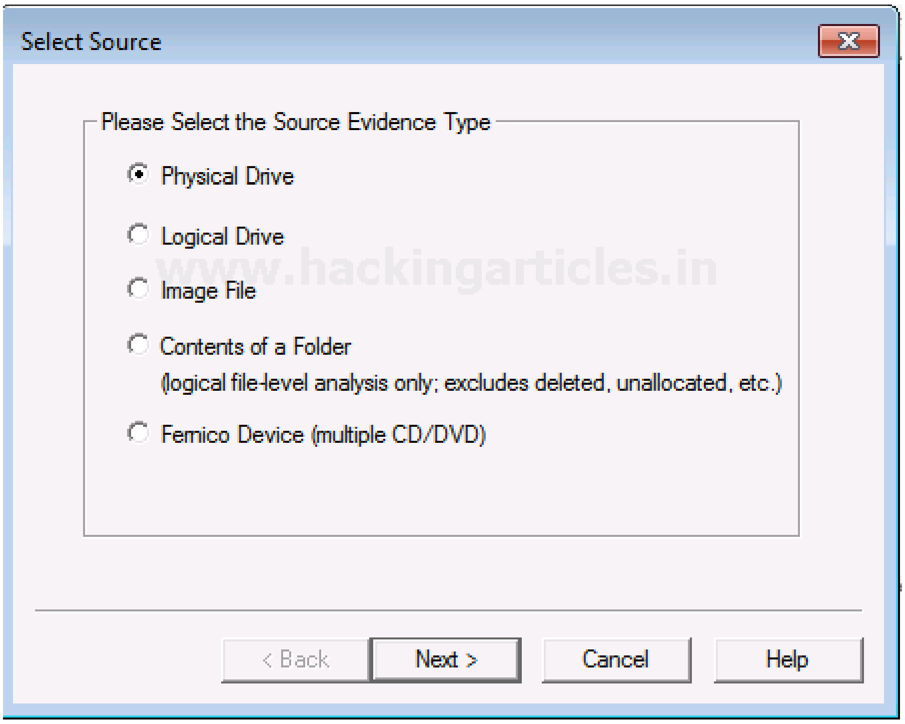

AccessData FTK Imager 4.1.1.1
File View Mode Help
Evidence Tree
File List
Name Size Type Date Modified
www.hackingarticles.in
Custom Content Sources
Evidence:File System|Path|File Options
New Edit Remove Remove All Create Image
Properties Hex Value Inter... Custom Conte...
For User Guide, press F1

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

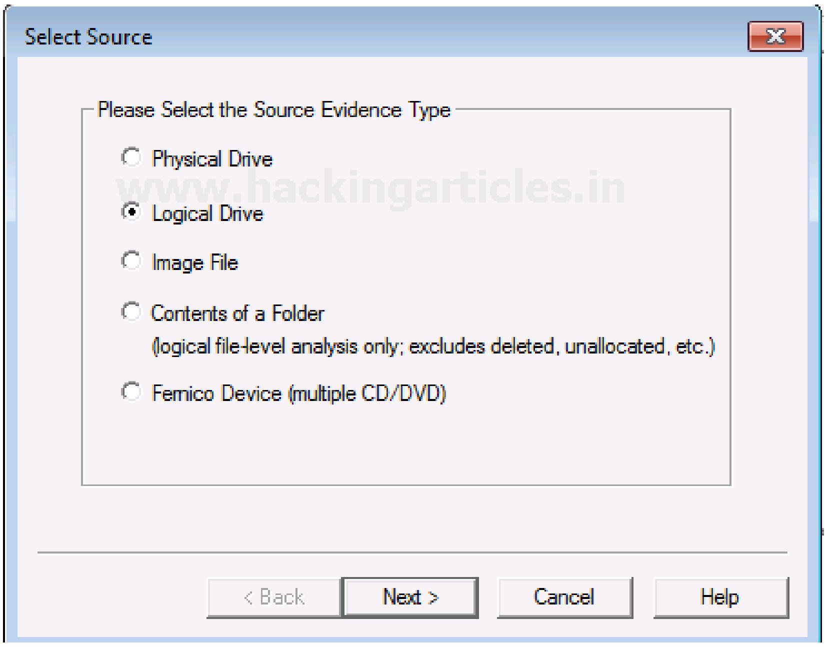


Now you can choose the source based on the drive you have. It can be a physical or a logical Drive depending on your evidence.

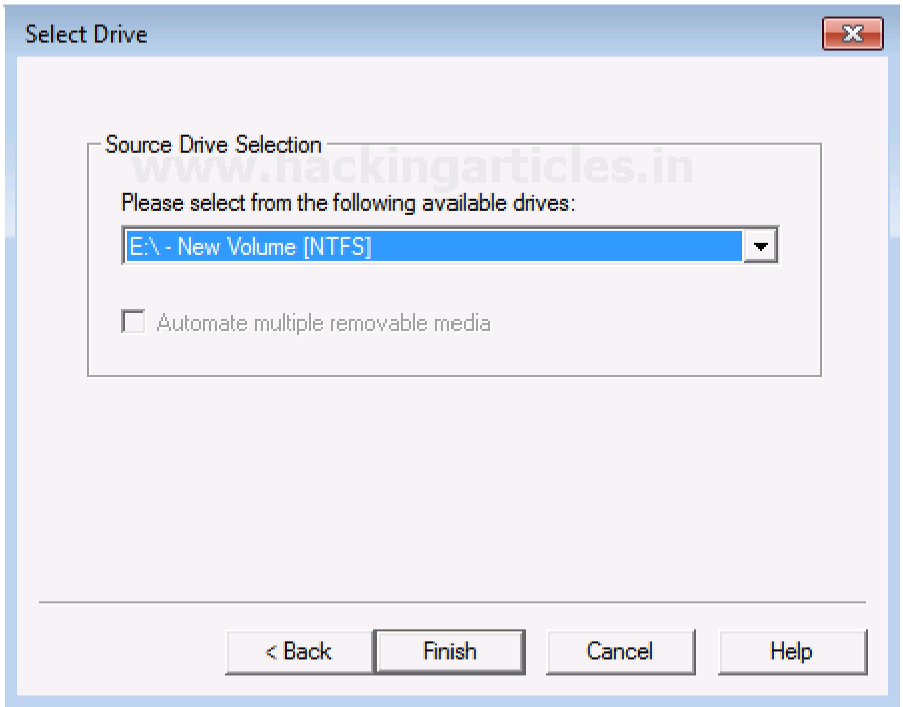
A Physical Drive is the primary storage hardware or the component within a device, which is used to store, retrieve, and organize data.


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.)
○ Ferrico Device (multiple CD/DVD)
< Back
Next >
Cancel
Help

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.


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.)
○ Ferrico Device (multiple CD/DVD)
< Back
Next >
Cancel
Help

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



Select Drive

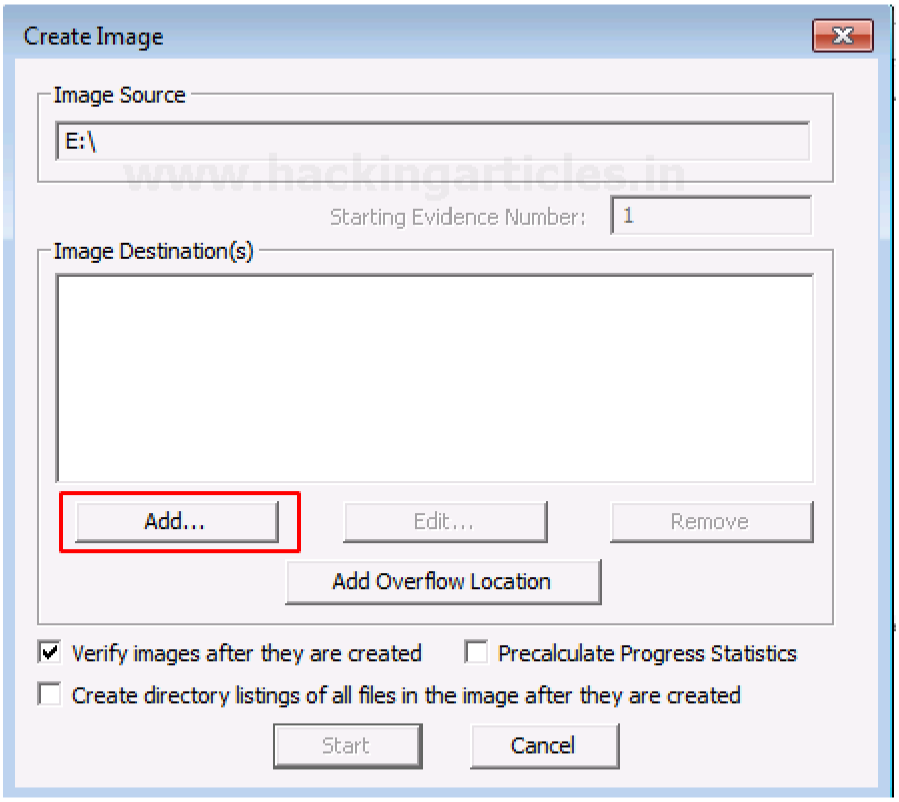
Source Drive Selection

Please select from the following available drives:

E:\ - New Volume [NTFS]

□ Automate multiple removable media

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.



Create Image

Image Source

E:\

Starting Evidence Number: 1

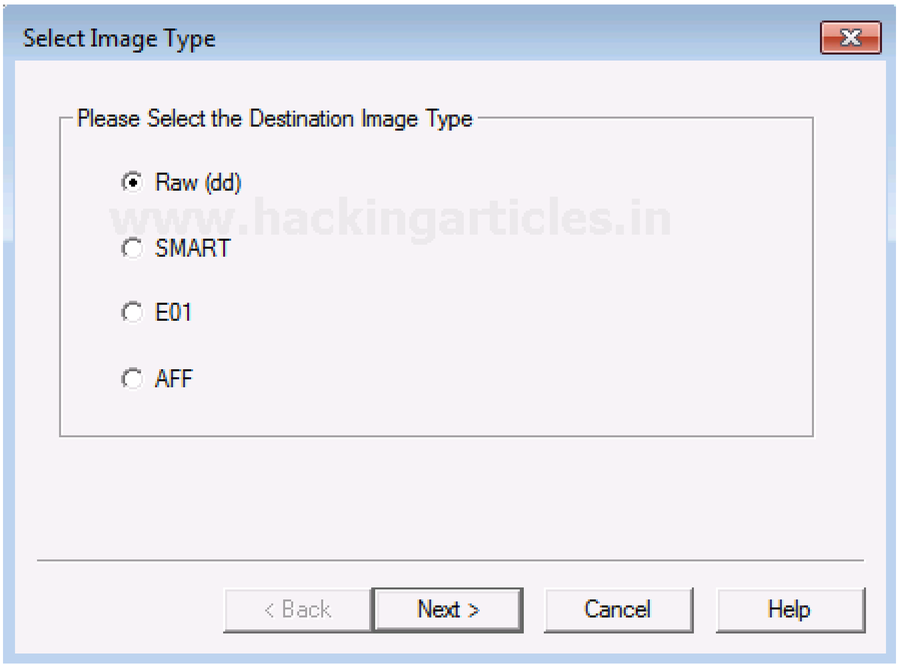
Image Destination(s)

☑ Verify images after they are created □ Precalculate Progress Statistics

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

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.

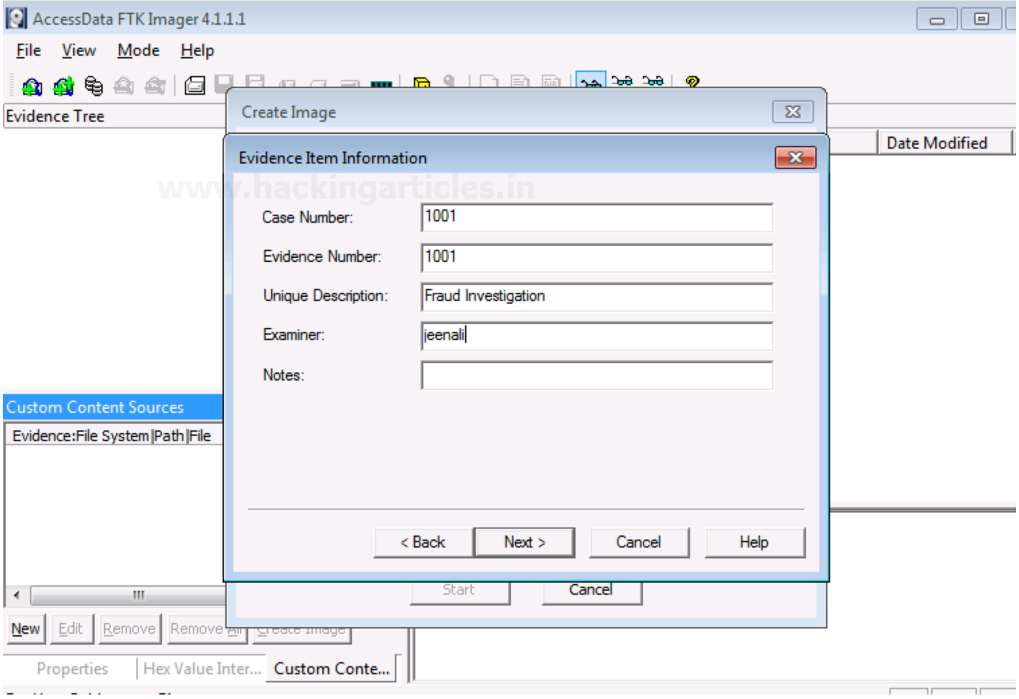


Select Image Type

Please Select the Destination Image Type

● Raw (dd)
○ SMART
○ E01
○ AFF

Now, add the details of the image to proceed.


AccessData FTK Imager 4.1.1.1
File View Mode Help
Evidence Tree
Create Image
Date Modified
Custom Content Sources
Evidence:File System|Path|File
New Edit Remove Remove All Create Image
Start Cancel
Properties Hex Value Inter... Custom Conte...

Evidence Item Information

Case Number: 1001

Evidence Number: 1001

Unique Description: Fraud Investigation

Examiner: jeenali

Notes:

< Back | Next > | Cancel | Help

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

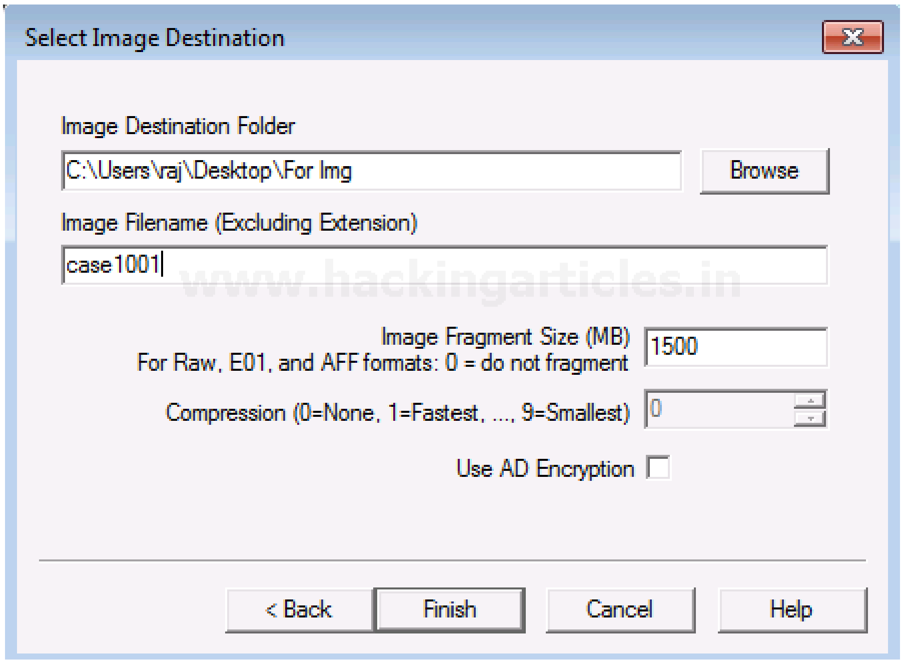

Select Image Destination

Image Destination Folder: C:\Users\raj\Desktop\For Img

Image Filename (Excluding Extension): case1001

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 □

< Back | Finish | Cancel | Help

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.

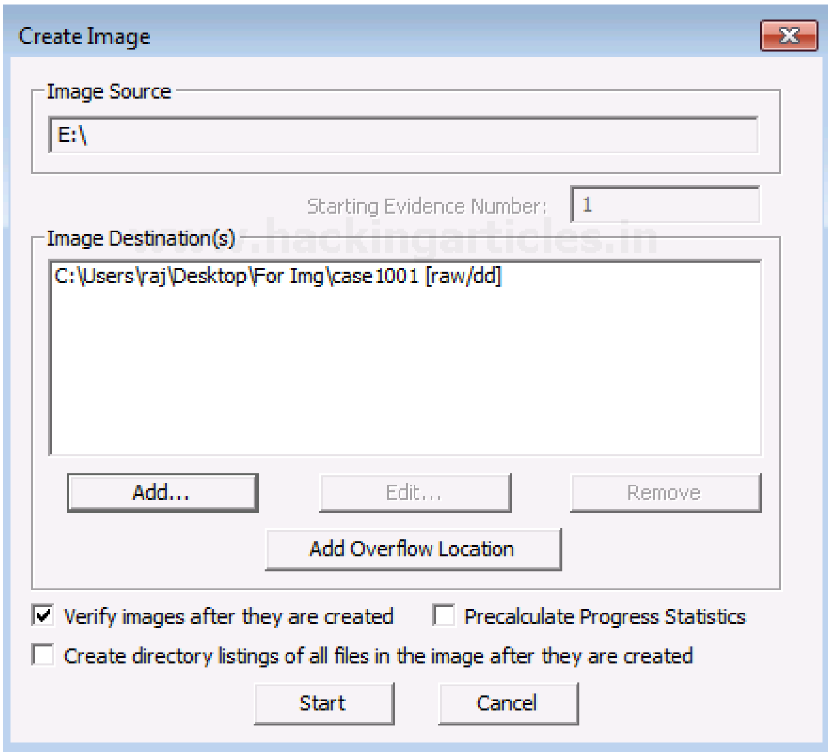

Create Image

Image Source: E:\

Starting Evidence Number: 1

Image Destination(s): C:\Users\raj\Desktop\For Img\case1001 [raw/dd]

☑ Verify images after they are created

□ Precalculate Progress Statistics

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

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

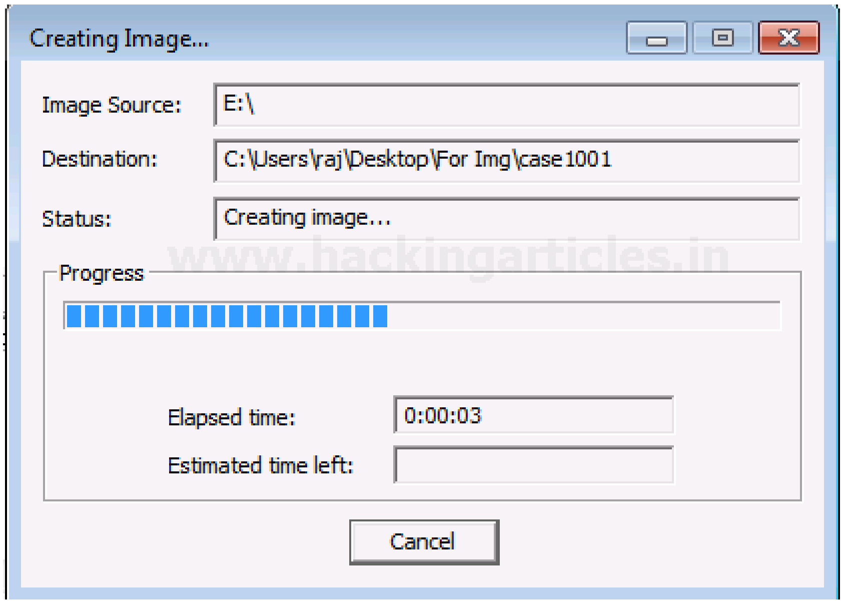

Creating Image...

Image Source: E:\

Destination: C:\Users\raj\Desktop\For Img\case1001

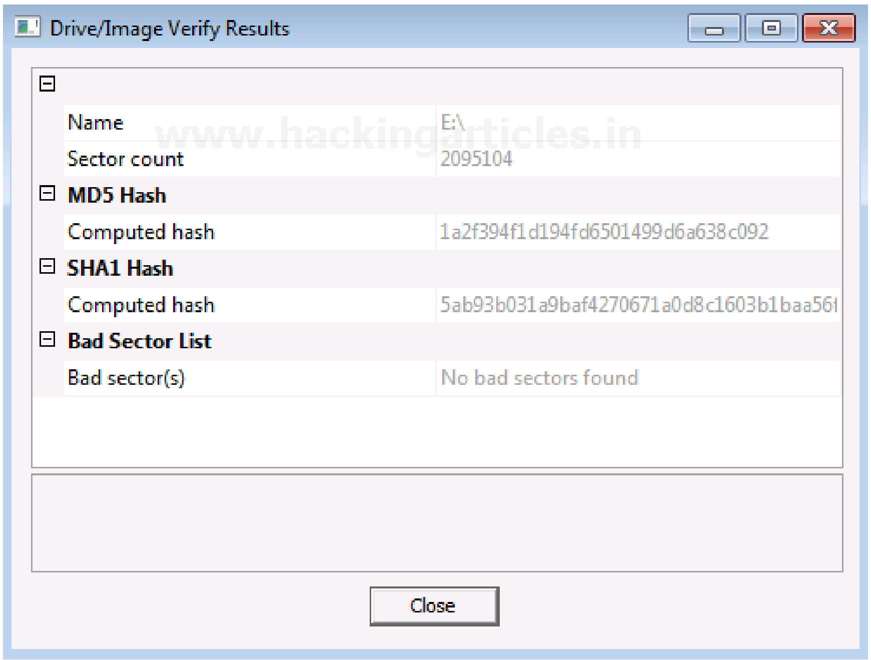
Status: Creating image...

Progress

Elapsed time: 0:00:03

Estimated time left:

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



Drive/Image Verify Results

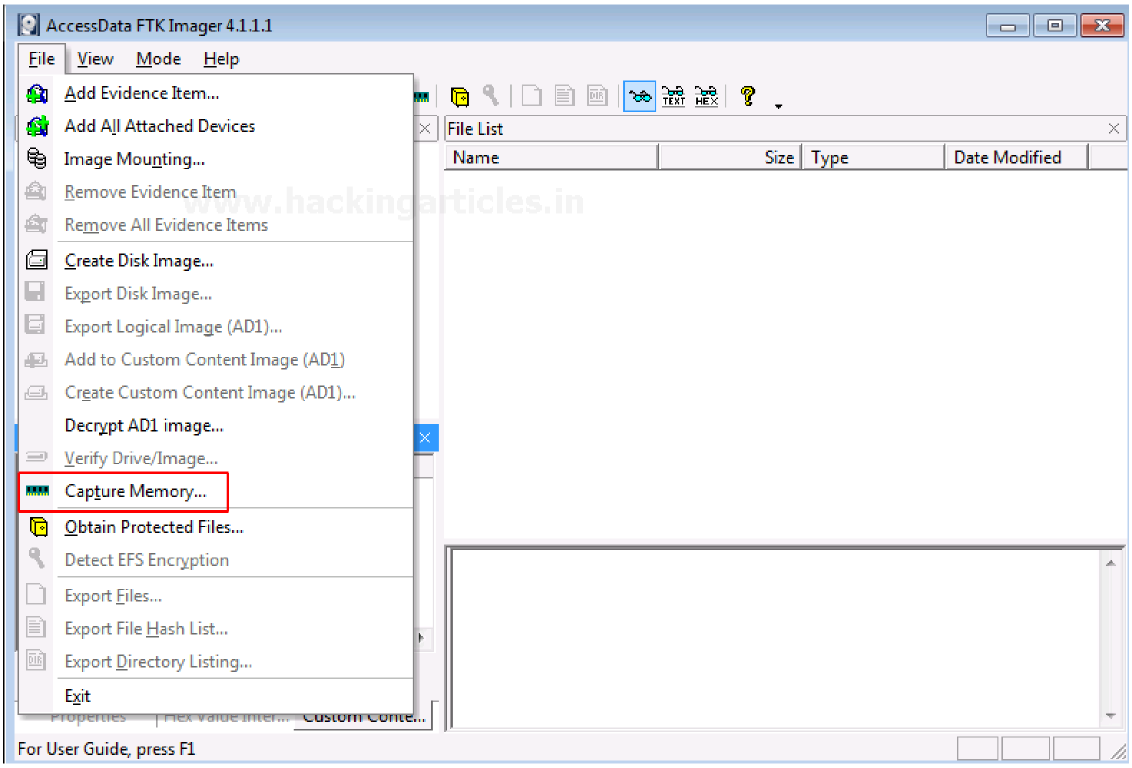
Name	E:\
Sector count	2095104
MD5 Hash	
Computed hash	1a2f394f1d194fd6501499d6a638c092
SHA1 Hash	
Computed hash	5ab93b031a9baf4270671a0d8c1603b1baa56
Bad Sector List	
Bad sector(s)	No bad sectors found

Capturing Memory

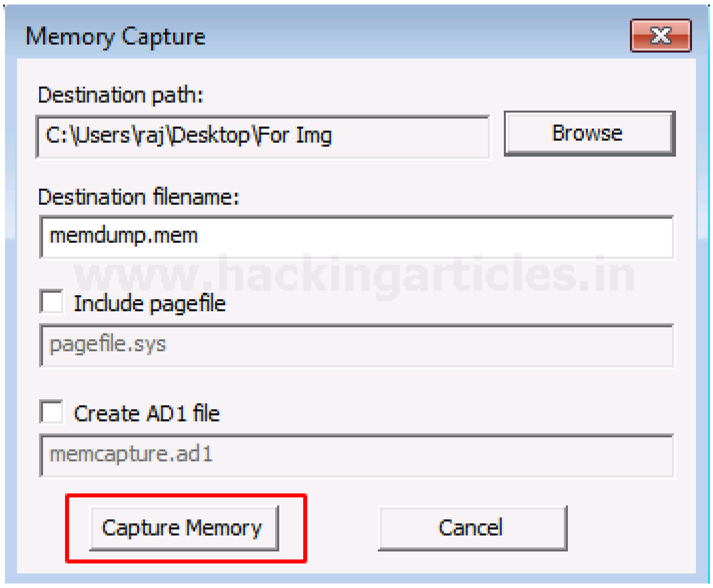
It is the method of capturing and dumping the contents of a volatile content into a non-volatile storage device to preserve it for further investigation. A ram analysis can only be successfully conducted when the acquisition has been performed accurately without corrupting the image of the volatile memory. 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.*



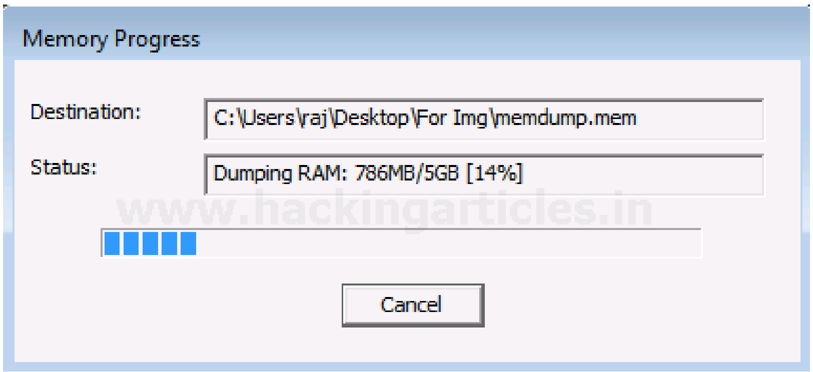
Destination path: C:\Users\raj\Desktop\For Img

Destination filename: memdump.mem

□ Include pagefile: pagefile.sys

□ Create AD1 file: memcapture.ad1

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



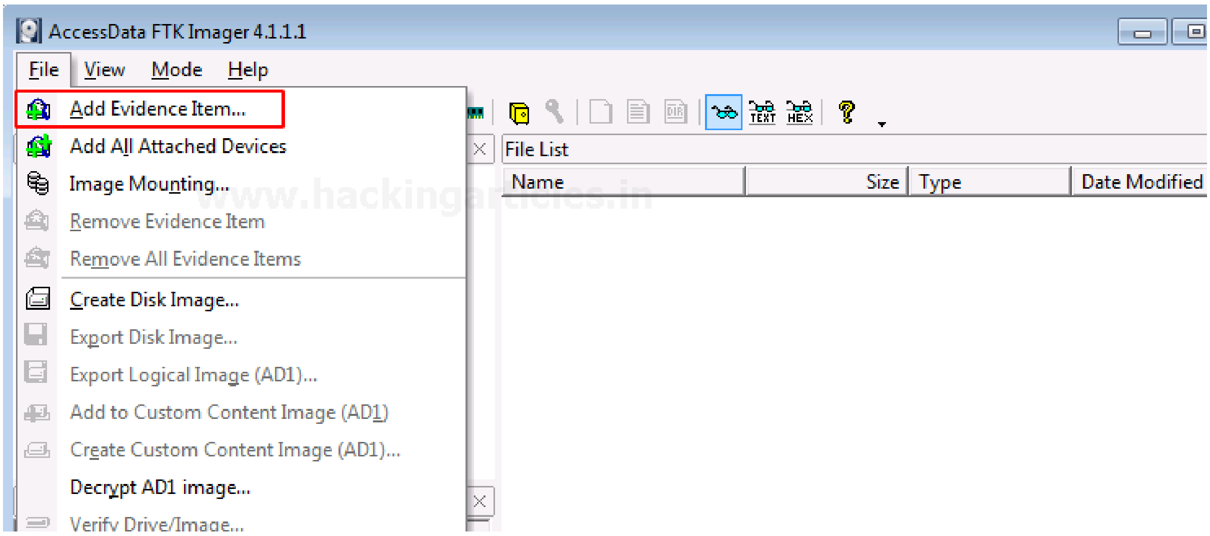
Memory Progress

Destination: C:\Users\raj\Desktop\For Img\memdump.mem

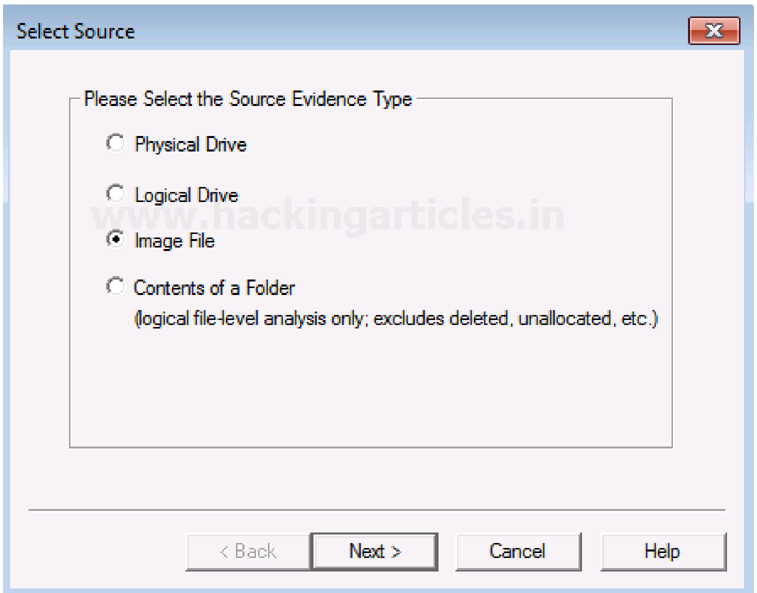
Status: Dumping RAM: 786MB/5GB [14%]

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.



Select Source

Please Select the Source Evidence Type

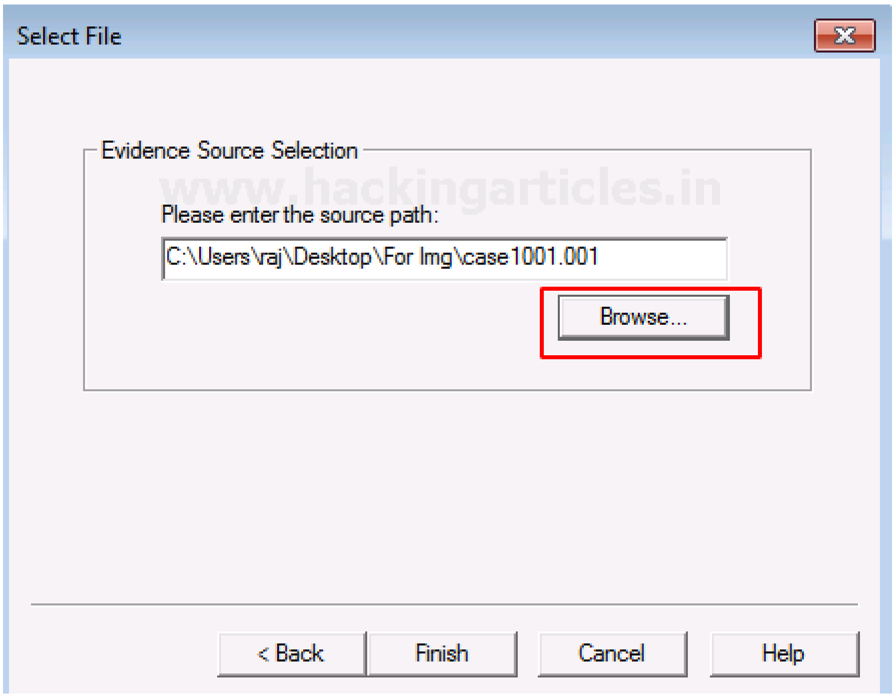
○ Physical Drive

○ Logical Drive

● Image File

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

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

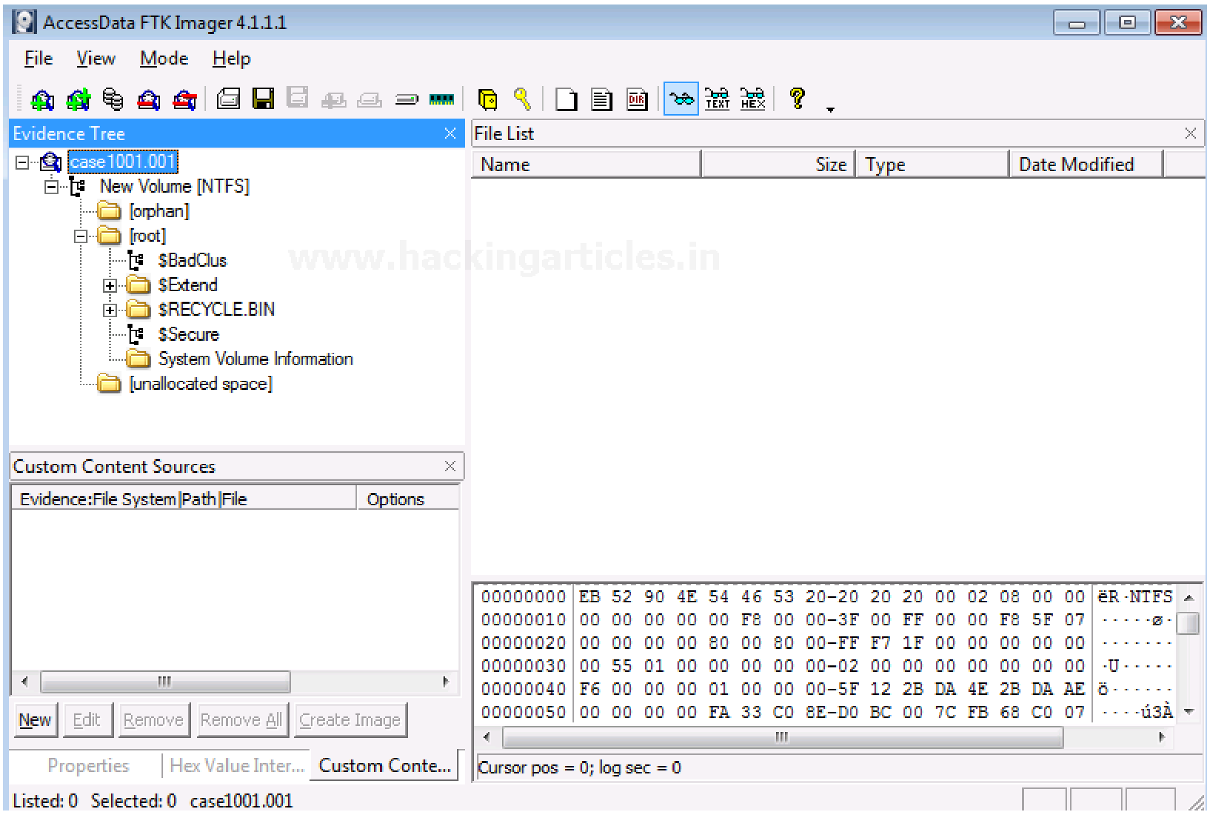


Select File

Evidence Source Selection

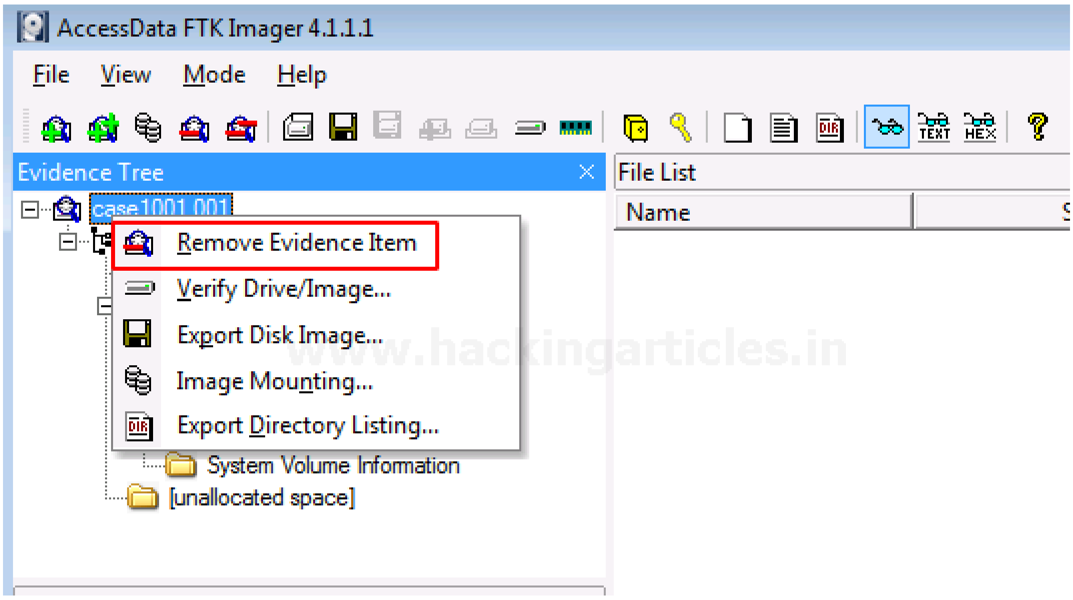
Please enter the source path:
C:\Users\raj\Desktop\For Img\case1001.001

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.


AccessData FTK Imager 4.1.1.1
File View Mode Help
Evidence Tree
case1001.001
New Volume [NTFS]
[orphan]
[root]
$BadClus
$Extend
$RECYCLE.BIN
$Secure
System Volume Information
[unallocated space]
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...
Cursor pos = 0; log sec = 0
Listed: 0 Selected: 0 case1001.001

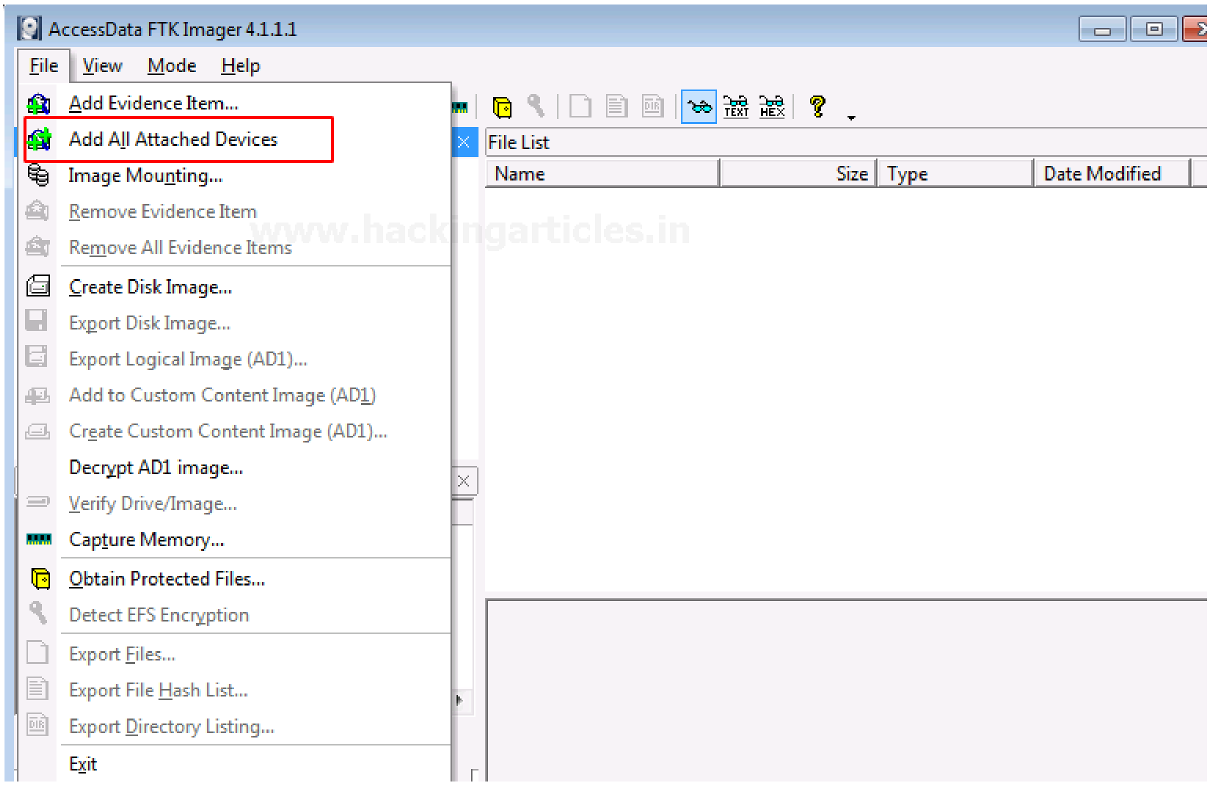
```
00000000 EB 52 90 4E 54 46 53 20-20 20 20 00 02 08 00 00 ëR·NTFS
00000010 00 00 00 00 00 F8 00 00-3F 00 FF 00 00 F8 5F 07 ·····ø·
00000020 00 00 00 00 80 00 80 00-FF F7 1F 00 00 00 00 00 ·······
00000030 00 55 01 00 00 00 00 00-02 00 00 00 00 00 00 00 ·U·····
00000040 F6 00 00 00 01 00 00 00-5F 12 2B DA 4E 2B DA AE ö······
00000050 00 00 00 00 FA 33 C0 8E-D0 BC 00 7C FB 68 C0 07 ····ú3À
```

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

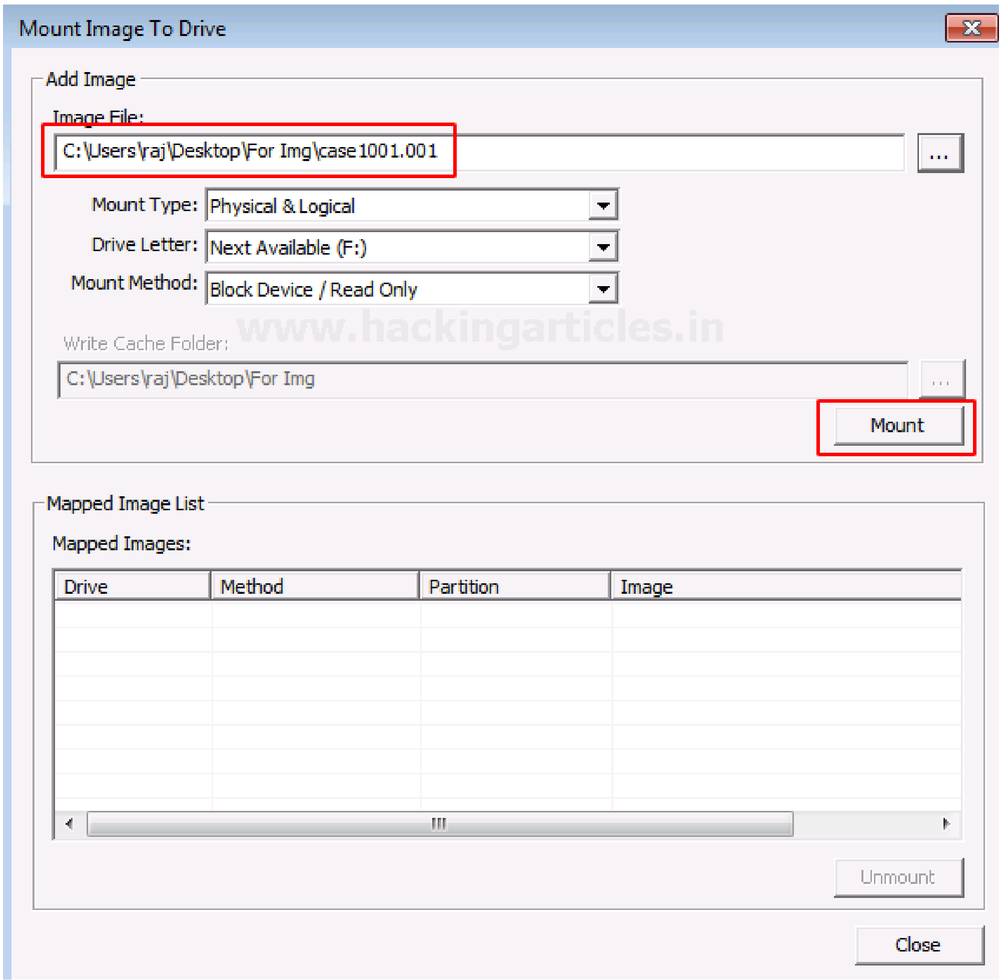


Mounting Image to Drive

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*.



Mount Image To Drive

Add Image

Image File: C:\Users\raj\Desktop\For Img\case1001.001

Mount Type: Physical & Logical

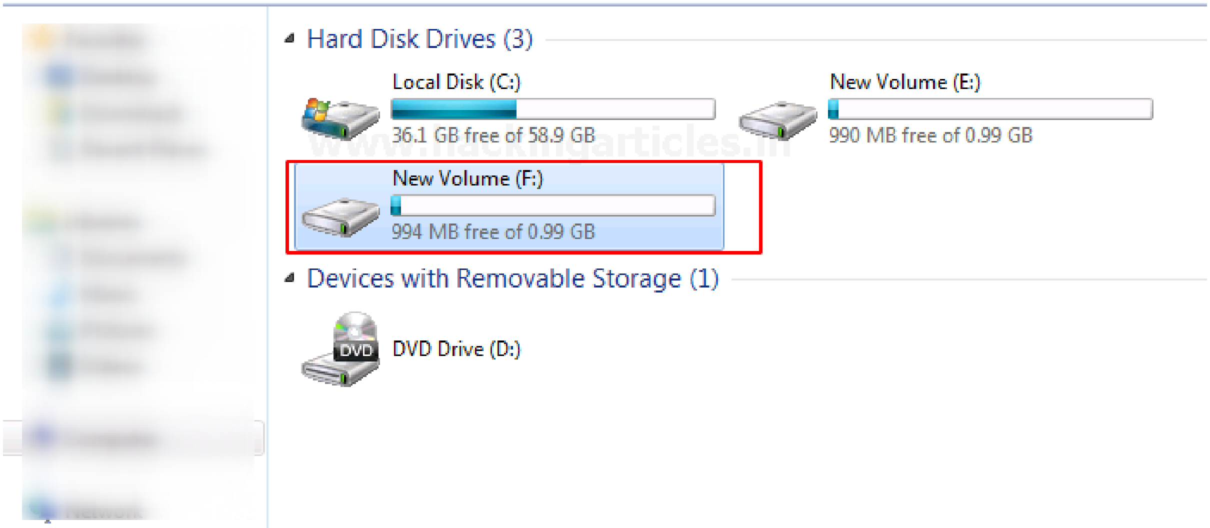
Drive Letter: Next Available (F:)

Mount Method: Block Device / Read Only

Write Cache Folder: C:\Users\raj\Desktop\For Img

Drive	Method	Partition	Image

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



Hard Disk Drives (3)

Local Disk (C:) 36.1 GB free of 58.9 GB

New Volume (E:) 990 MB free of 0.99 GB

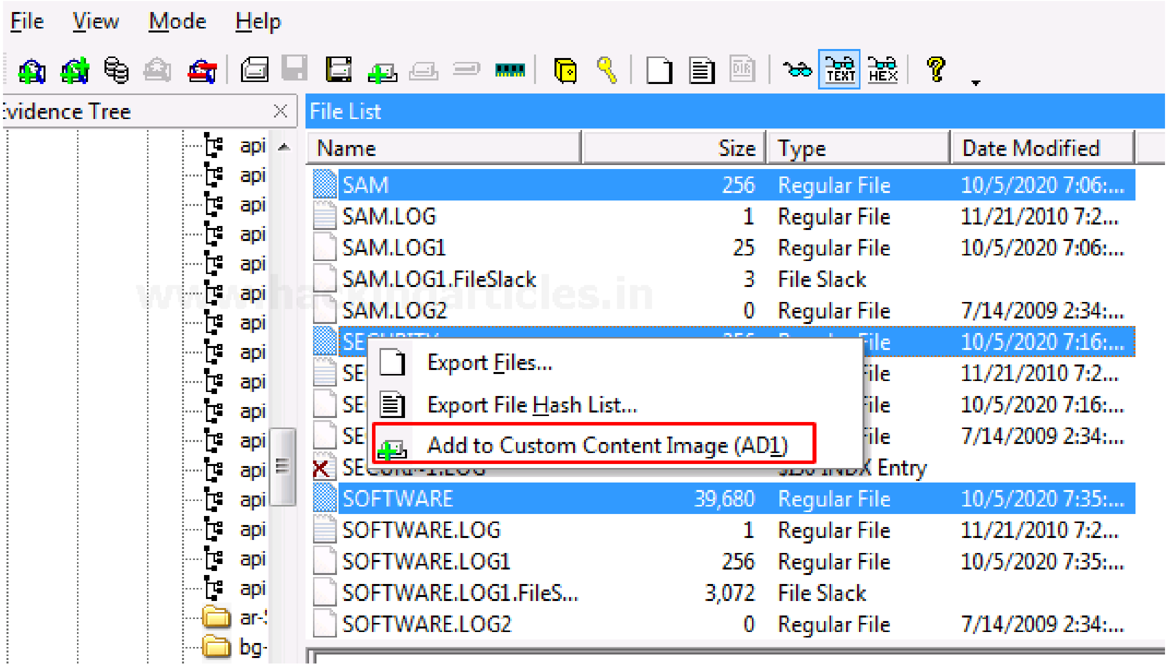
New Volume (F:) 994 MB free of 0.99 GB

Devices with Removable Storage (1)

DVD Drive (D:)

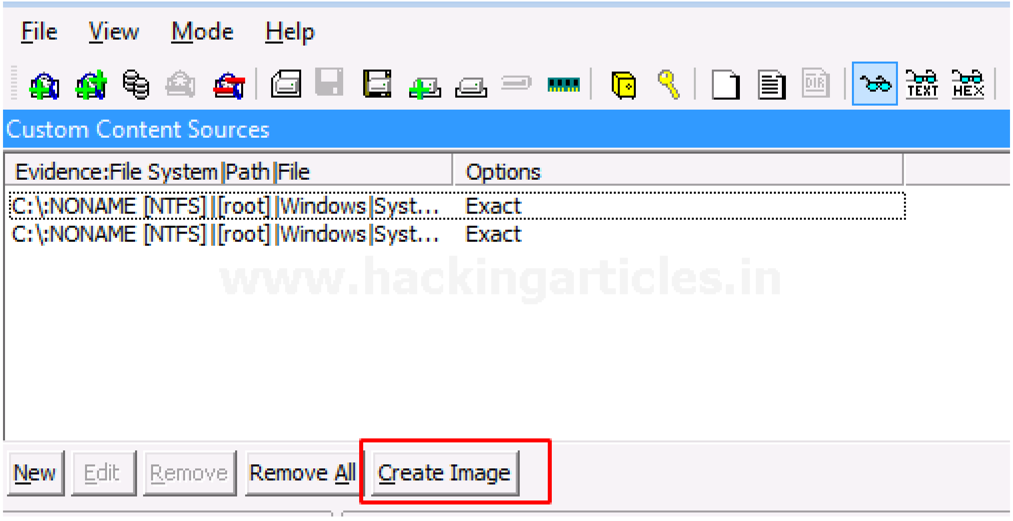
Custom Content Image with AD Encryption

FTK imager has a feature that allows it to encrypt files of a particular type according to the requirement of the examiner. Click on the files that you want to add to the custom content Image along with AD encryption.



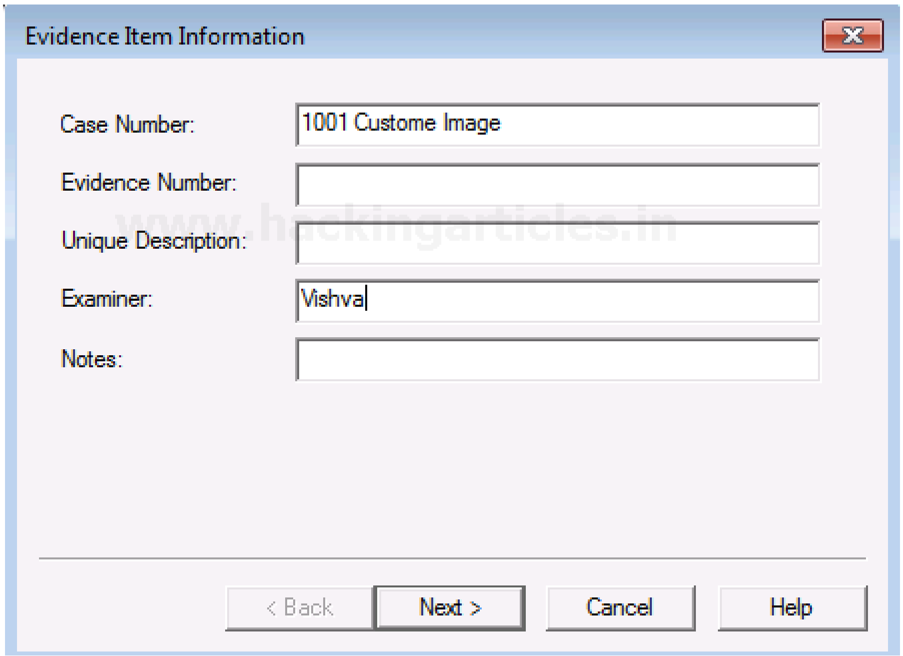
Name	Size	Type	Date Modified
SAM	256	Regular File	10/5/2020 7:06:...
SAM.LOG	1	Regular File	11/21/2010 7:2...
SAM.LOG1	25	Regular File	10/5/2020 7:06:...
SAM.LOG1.FileSlack	3	File Slack	
SAM.LOG2	0	Regular File	7/14/2009 2:34:...
SE		ile	10/5/2020 7:16:...
SE		ile	11/21/2010 7:2...
SE		ile	10/5/2020 7:16:...
SE		ile	7/14/2009 2:34:...
SE		X Entry	
SOFTWARE	39,680	Regular File	10/5/2020 7:35:...
SOFTWARE.LOG	1	Regular File	11/21/2010 7:2...
SOFTWARE.LOG1	256	Regular File	10/5/2020 7:35:...
SOFTWARE.LOG1.FileS...	3,072	File Slack	
SOFTWARE.LOG2	0	Regular File	7/14/2009 2:34:...

All the selected files will be displayed in a new window and then click on Create Image to proceed.



Evidence:File System|Path|File	Options
C:\:NONAME [NTFS]|[root]|Windows|Syst...	Exact
C:\:NONAME [NTFS]|[root]|Windows|Syst...	Exact

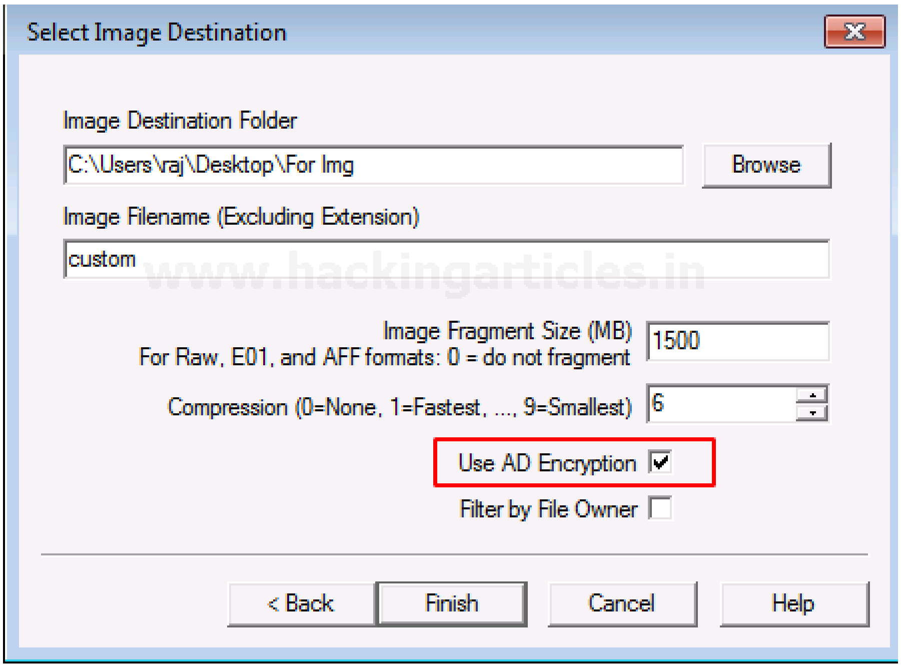
Fill in the required details for the evidence that is to be created.



Evidence Item Information

Case Number:	1001 Custome Image
Evidence Number:	
Unique Description:	
Examiner:	Vishva
Notes:	

Now add the destination of the image file that is to be created, name the image file and then check the box with AD encryption, and then click on Finish.



Select Image Destination

Image Destination Folder: C:\Users\raj\Desktop\For Img

Image Filename (Excluding Extension): custom

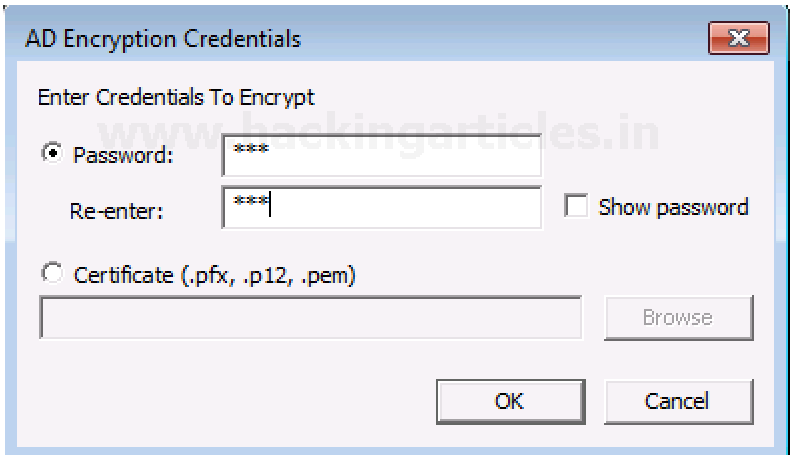
Image Fragment Size (MB) For Raw, E01, and AFF formats: 0 = do not fragment: 1500

Compression (0=None, 1=Fastest, ..., 9=Smallest): 6

Use AD Encryption ☑

Filter by File Owner □

A new window will pop-up to encrypt the image, Now renter and re-enter the password that you want to add for your image.



AD Encryption Credentials

Enter Credentials To Encrypt

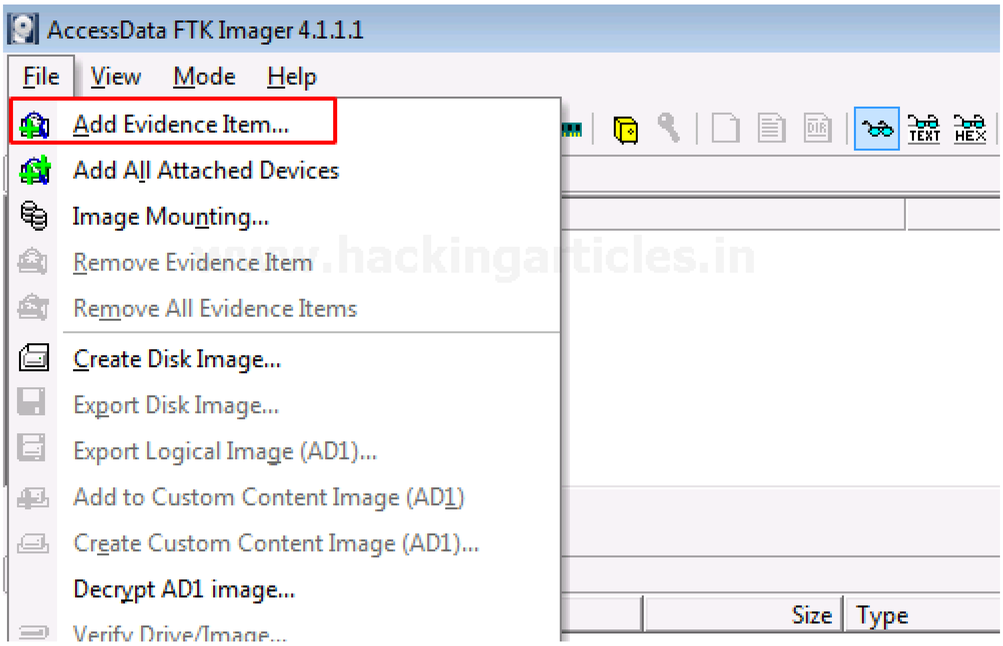
● Password: ***

Re-enter: ***

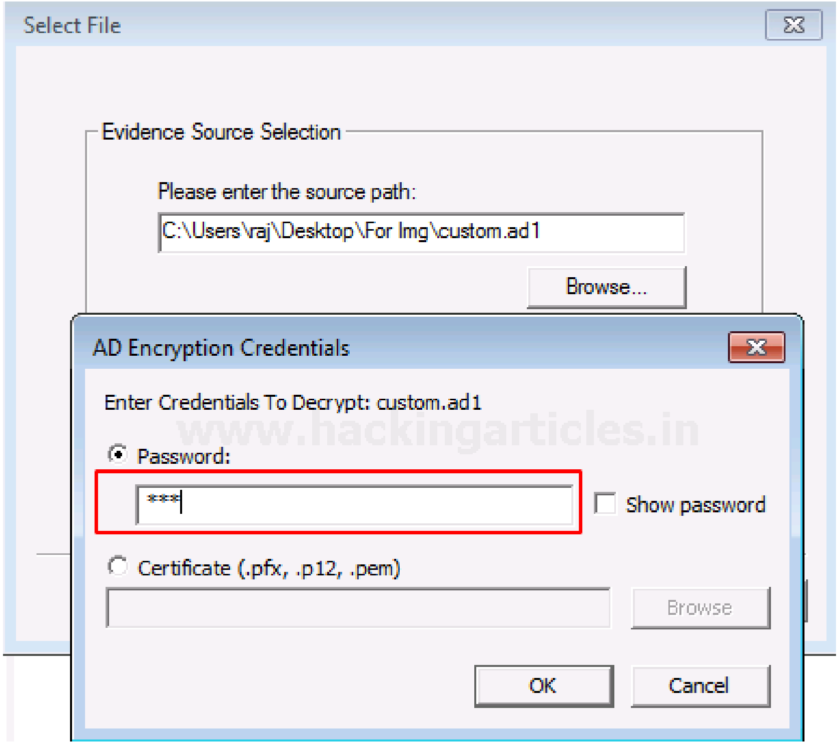
□ Show password

○ Certificate (.pfx, .p12, .pem)

Now to see the encrypted files, click on *File> Add Evidence Item…*



The window to decrypt the encrypted files will appear once you add the file source. Enter the password and click OK.



Please enter the source path: C:\Users\raj\Desktop\For Img\custom.ad1

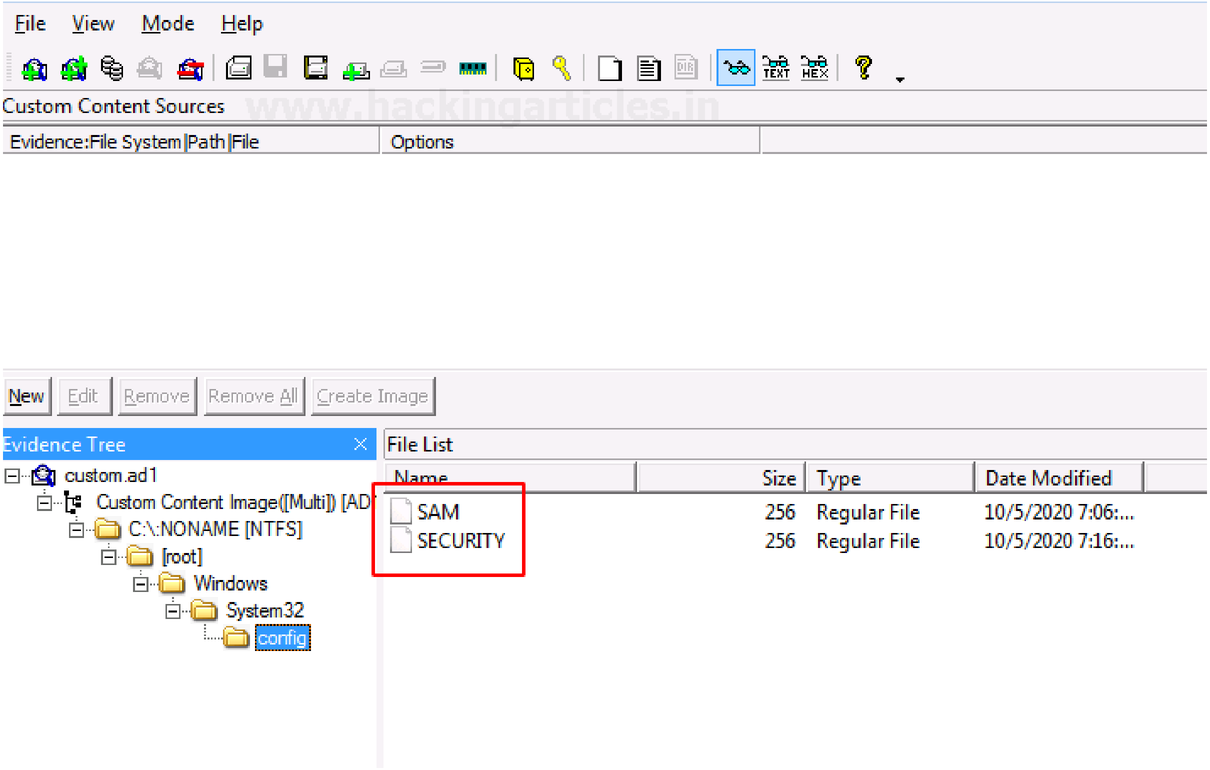
Enter Credentials To Decrypt: custom.ad1

● Password: ***

□ Show password

○ Certificate (.pfx, .p12, .pem)

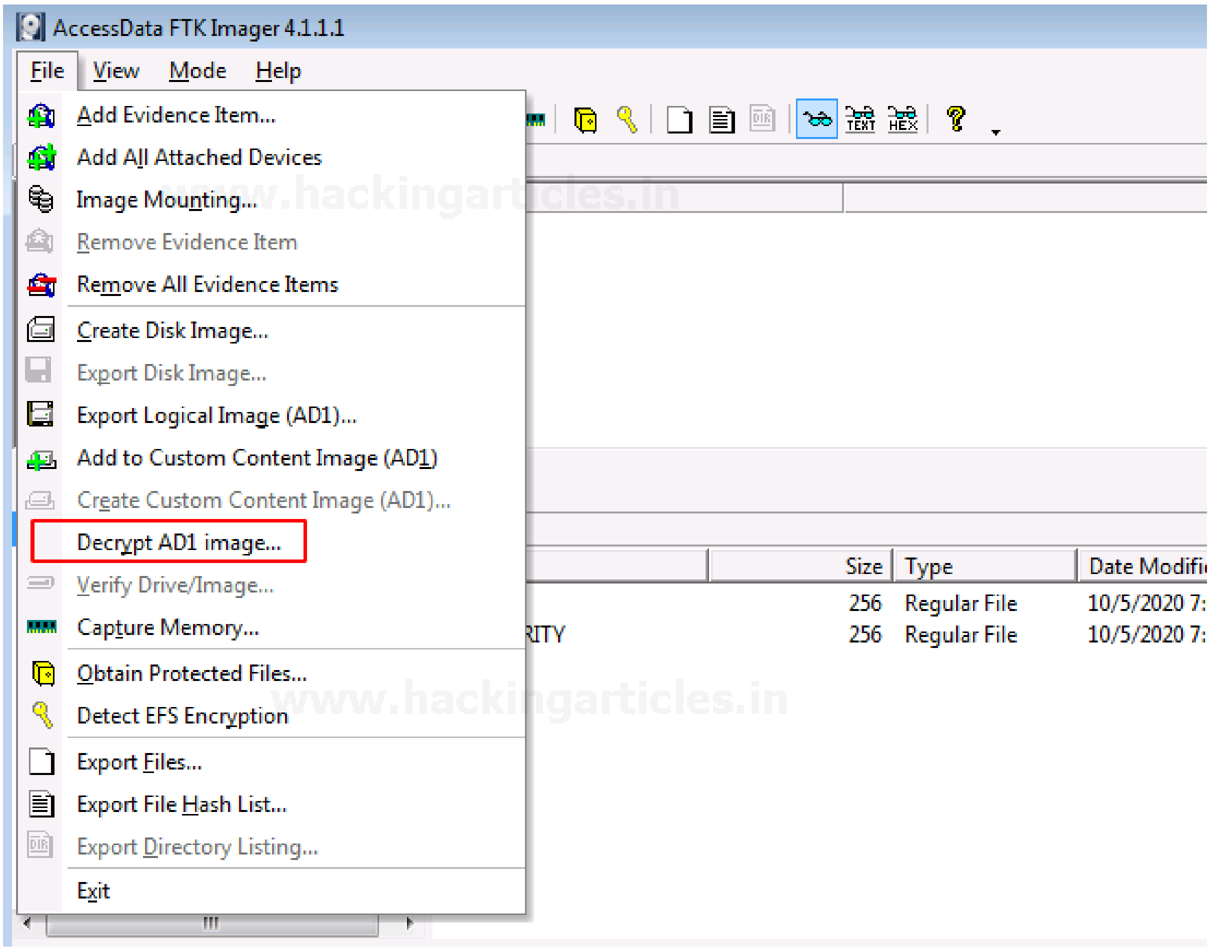
You will now see the two encrypted files on entering the valid passwords.



Name	Size	Type	Date Modified
SAM	256	Regular File	10/5/2020 7:06:...
SECURITY	256	Regular File	10/5/2020 7:16:...

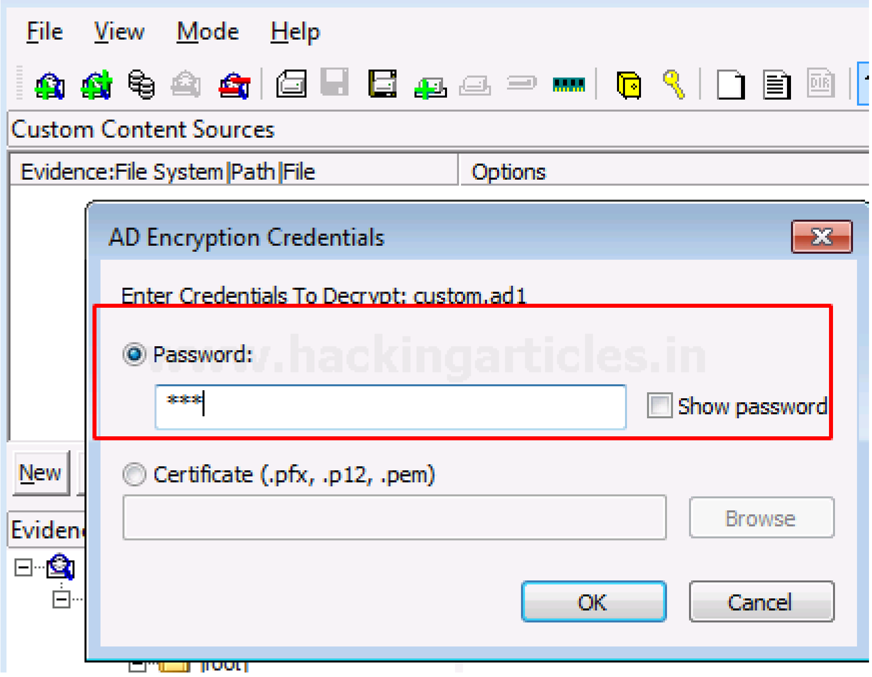
Decrypt AD1 Image

To decrypt the custom content image, click on *File> Decrypt AD1 Image***.**



Size	Type	Date Modifi
256	Regular File	10/5/2020 7:
256	Regular File	10/5/2020 7:

Now you need to enter the password for the image file that was encrypted and click on Ok.



Enter Credentials To Decrypt: custom.ad1

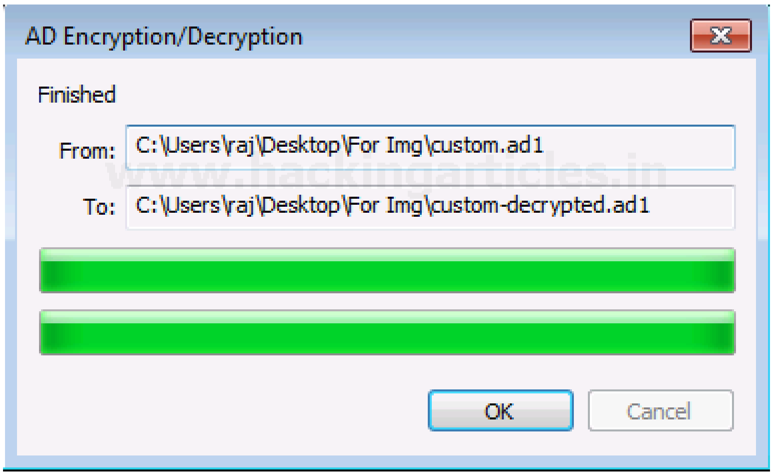
● Password:

***

□ Show password

○ Certificate (.pfx, .p12, .pem)

Now, wait for a few minutes till the decrypted image is created.

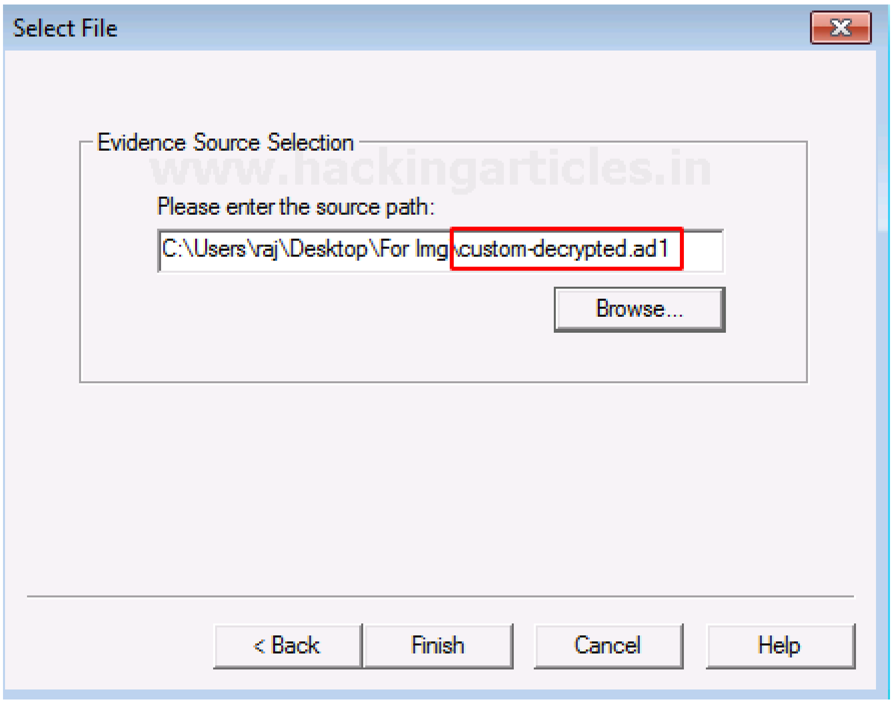


Finished

From: C:\Users\raj\Desktop\For Img\custom.ad1

To: C:\Users\raj\Desktop\For Img\custom-decrypted.ad1

To view the decrypted custom content image, add the path of the decrypted file and click on Finish.

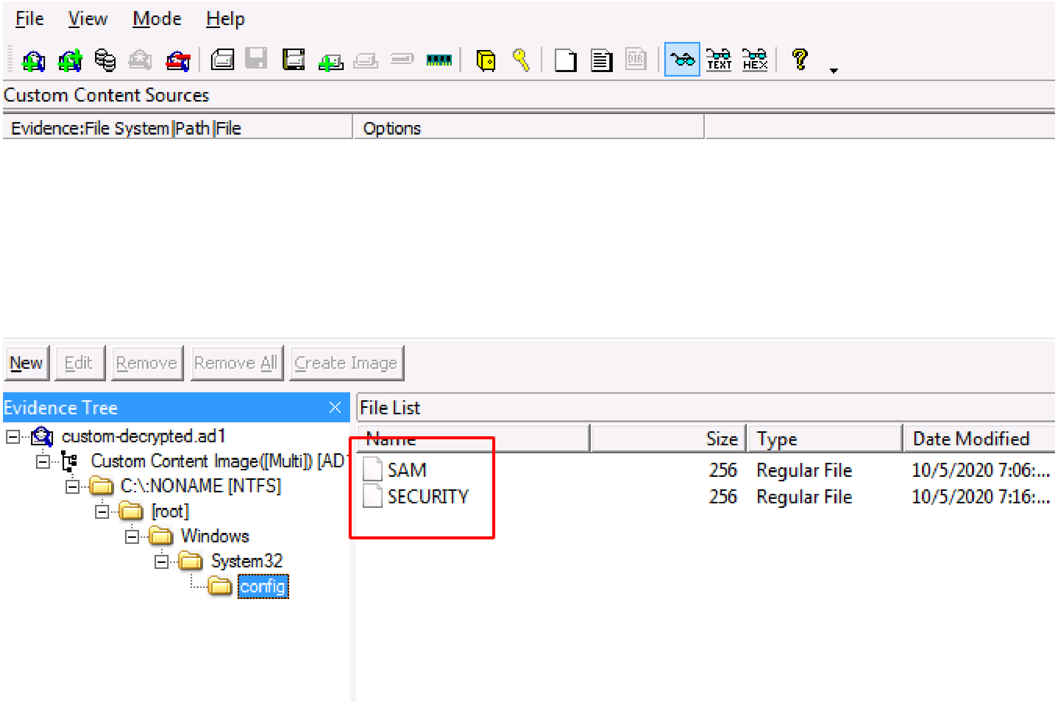


Evidence Source Selection

Please enter the source path:

C:\Users\raj\Desktop\For Img\custom-decrypted.ad1

You will now be able to see the encrypted files by using the correct password to decrypt it.

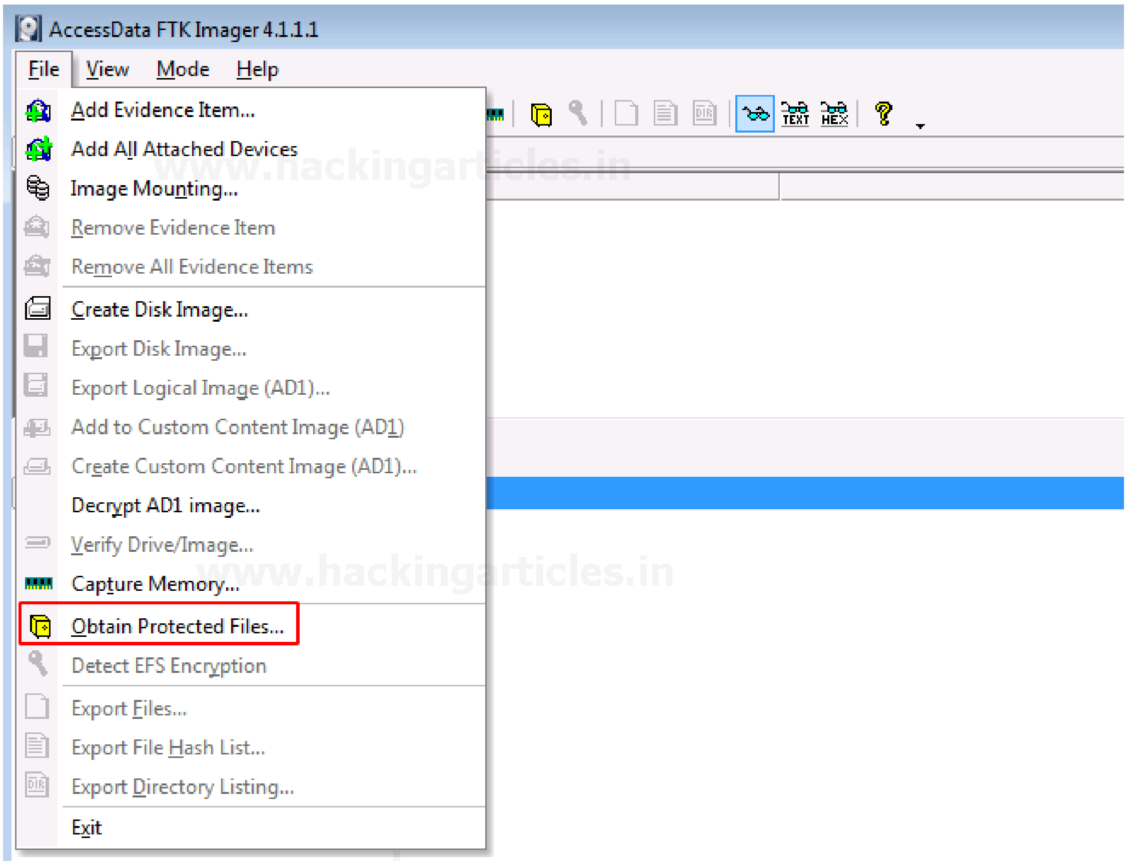


custom-decrypted.ad1
Custom Content Image([Multi]) [AD1]
C:\:NONAME [NTFS]
[root]
Windows
System32
config

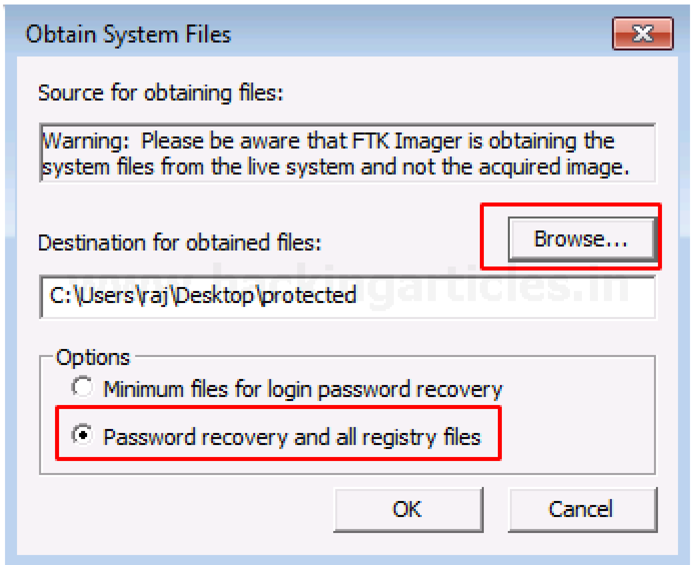
Name	Size	Type	Date Modified
SAM	256	Regular File	10/5/2020 7:06:...
SECURITY	256	Regular File	10/5/2020 7:16:...

Obtain Protected Files

Certain files are protected on recovery, to obtain those files, click on *File> Obtain Protected Files*



A new window will pop and click on browse to add the destination of the file that is protected and click on the option that says password recovery and all registry files and click on OK.


Obtain System Files

Source for obtaining files:

Warning: Please be aware that FTK Imager is obtaining the system files from the live system and not the acquired image.

Destination for obtained files:

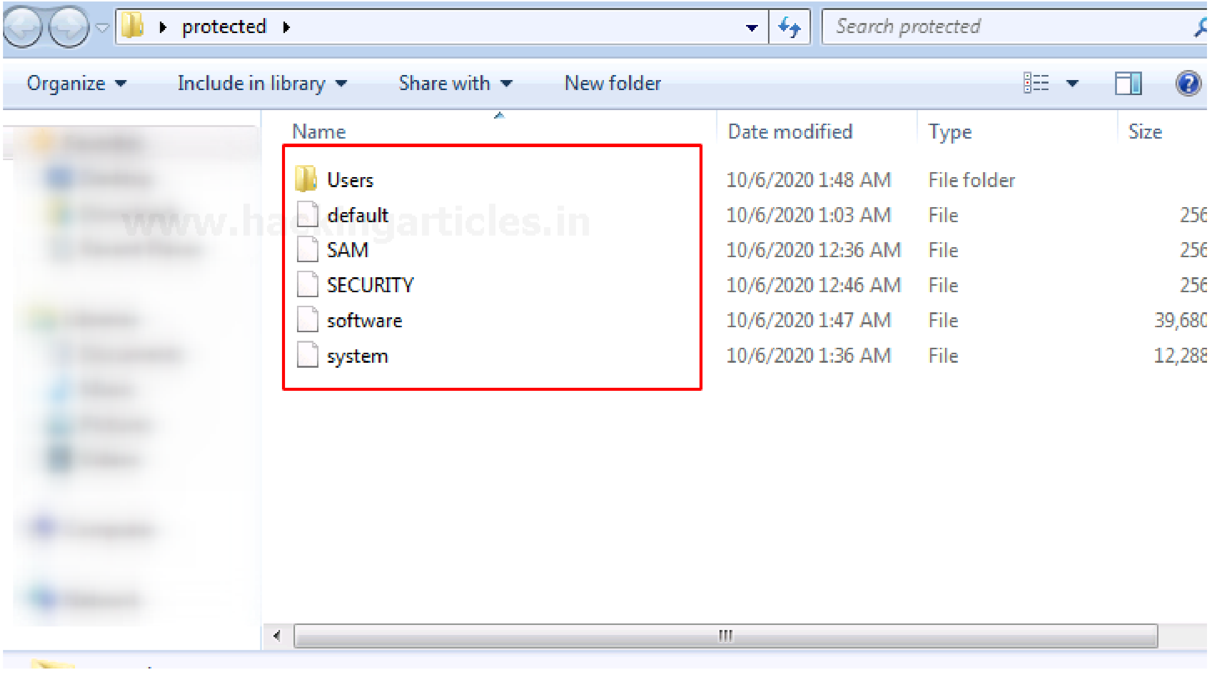
C:\Users\raj\Desktop\protected

Options

○ Minimum files for login password recovery

● Password recovery and all registry files

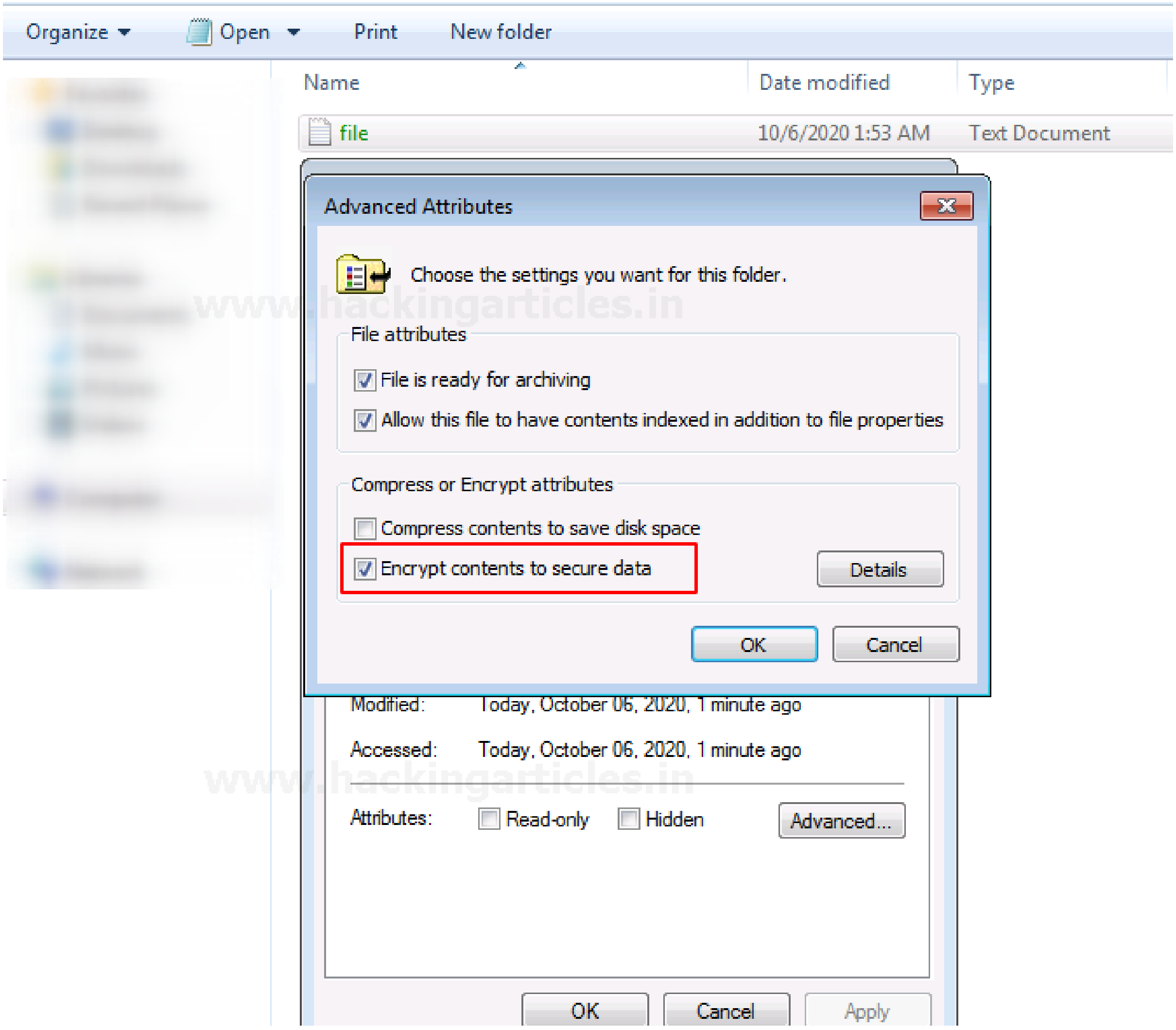
Now you will see all the protected files in one place



Name	Date modified	Type	Size
Users	10/6/2020 1:48 AM	File folder	
default	10/6/2020 1:03 AM	File	256
SAM	10/6/2020 12:36 AM	File	256
SECURITY	10/6/2020 12:46 AM	File	256
software	10/6/2020 1:47 AM	File	39,680
system	10/6/2020 1:36 AM	File	12,288

Detect EFS Encryption

When a folder or a file is encrypted, we can detect it using this feature of the FTK Imager. A file is encrypted in a folder to secure its content.



file 10/6/2020 1:53 AM Text Document

Advanced Attributes

Choose the settings you want for this folder.

File attributes

☑ File is ready for archiving

☑ Allow this file to have contents indexed in addition to file properties

Compress or Encrypt attributes

□ Compress contents to save disk space

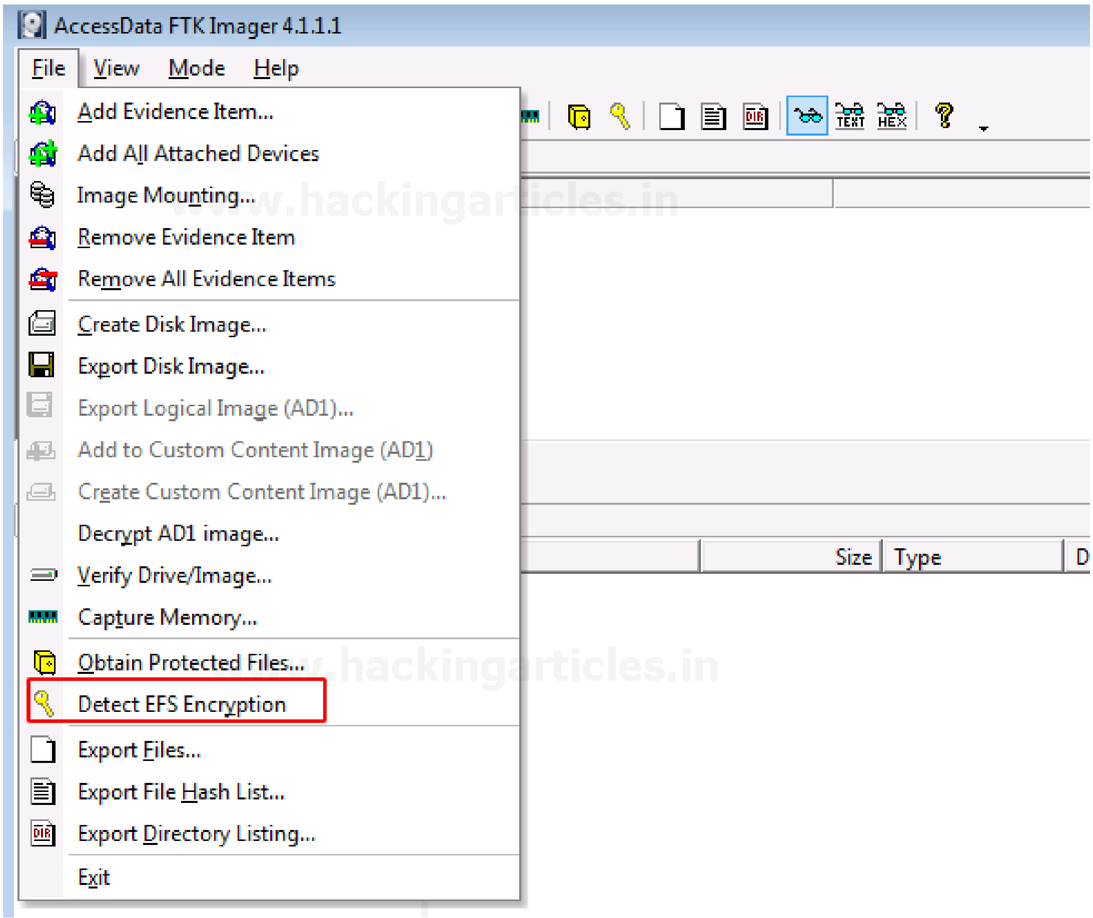
☑ Encrypt contents to secure data

Modified: Today, October 06, 2020, 1 minute ago

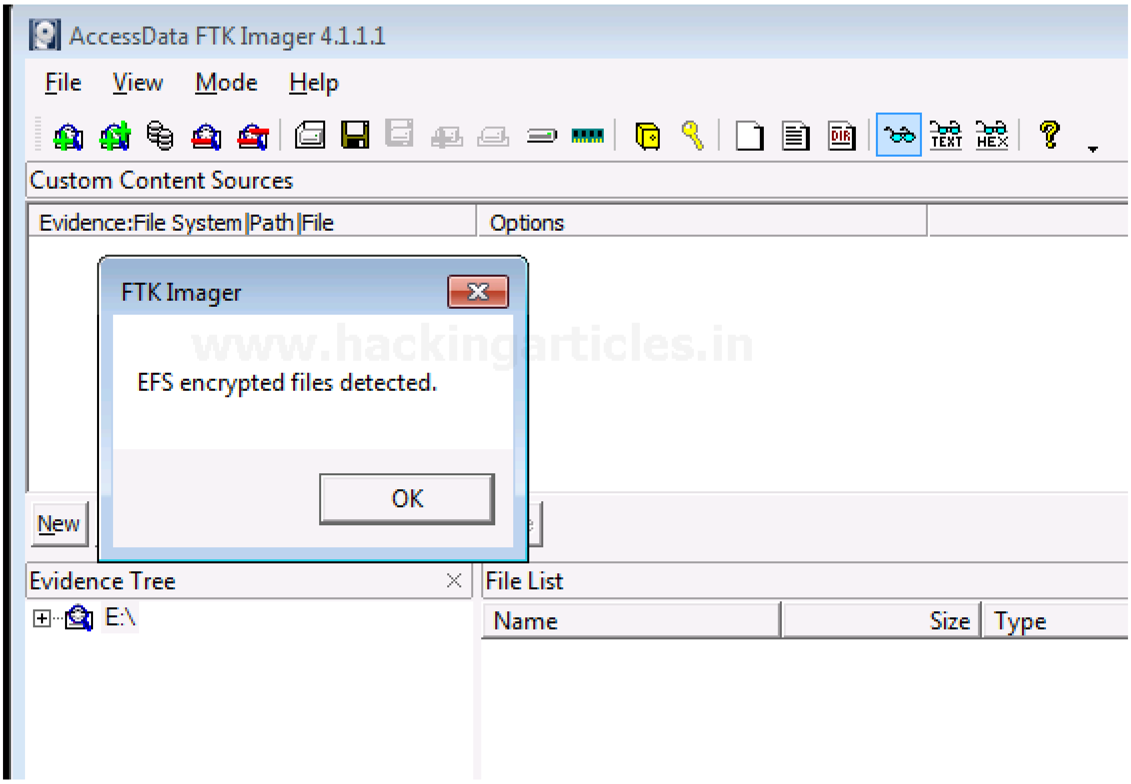
Accessed: Today, October 06, 2020, 1 minute ago

Attributes: □ Read-only □ Hidden

To detect the EFS encryption, click on *File >Detect EFS Encryption*

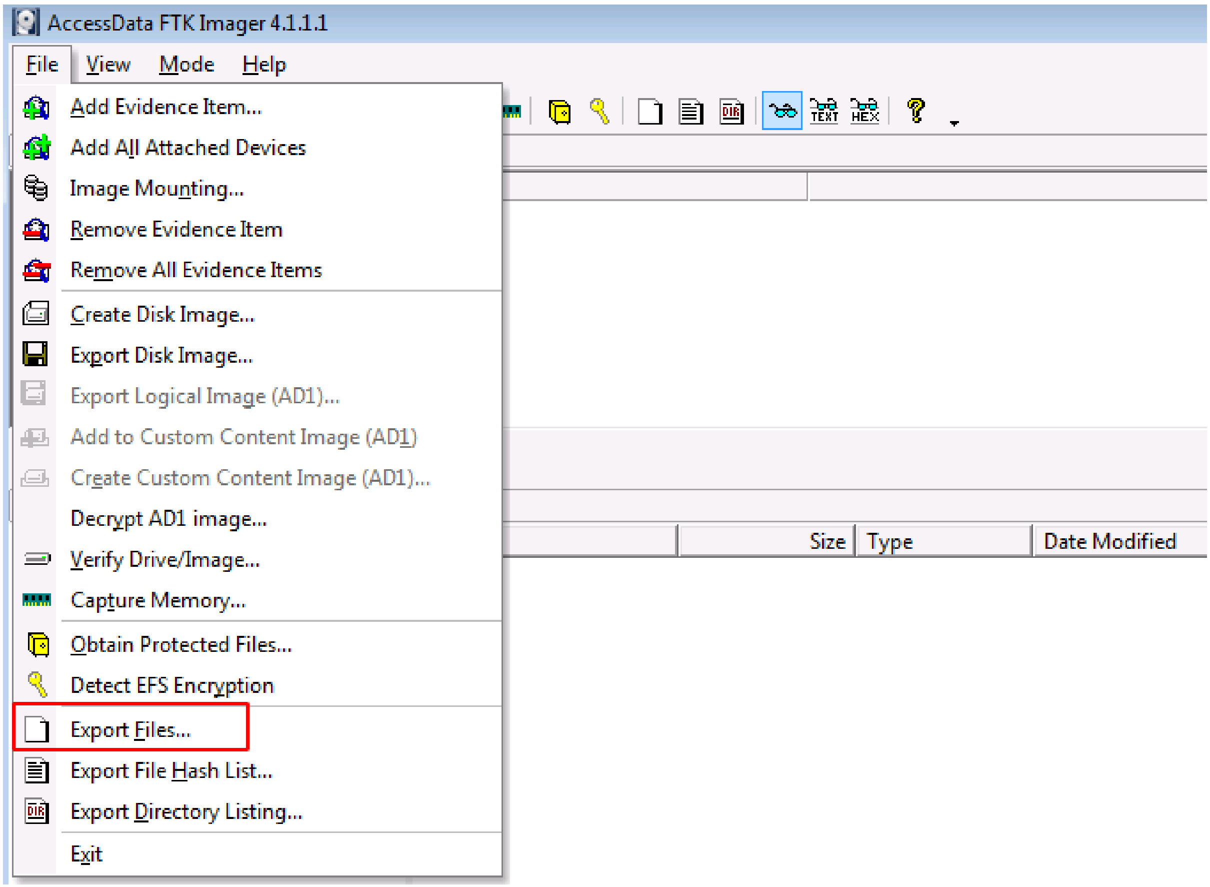


You can see that the encryption is detected.

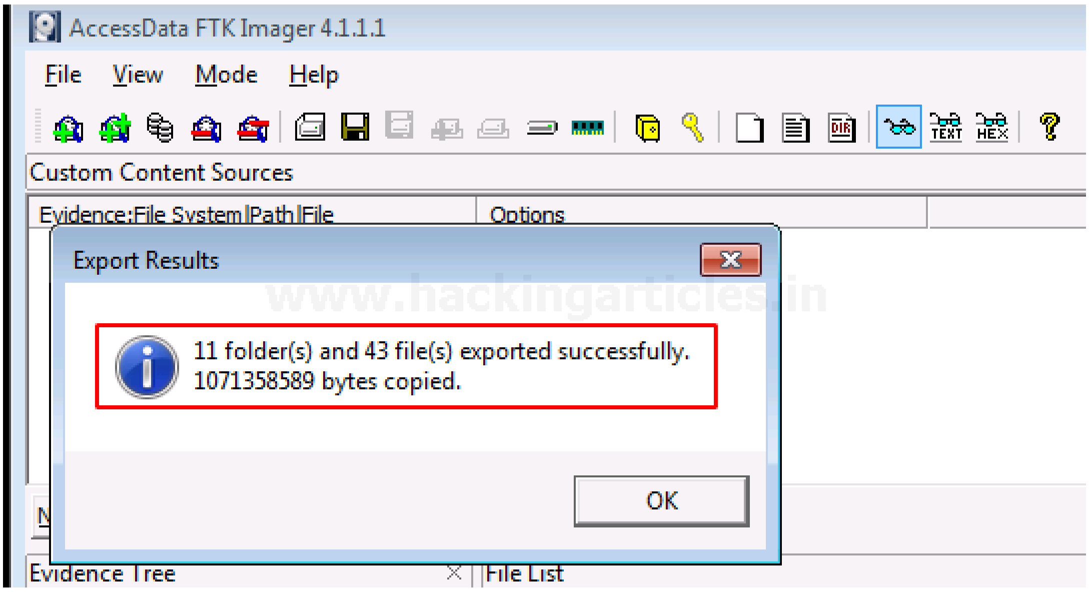

EFS encrypted files detected.

Export Files

To export the files and folders from the imaged file to your folder, you can click *File > Export Files*



You can now see the results of the export of the number of files and folders that have been copied to the system.



11 folder(s) and 43 file(s) exported successfully.
1071358589 bytes copied.