iGNITE Technologies

# DIGITAL FORENSIC

# FTK IMAGER

WWW.HACKINGARTICLES.IN

# Table Of Content

# Abstract

FTK Imager is an open-source software by AccessData that is used for creating accurate copies of the original evidence without actually making any changes to it. The Image of the original evidence is remaining the same and allows us to copy data at a much faster rate, which can be soon be preserved and can be analyzed further.

The FTK imager also provides you with the inbuilt integrity checking function which generates a hash report which helps in matching the hash of the evidence before and after creating the image of the original Evidence.

# Introduction To Images And FTK Imager

The data acquisition of a Hard Drive is known as an **image**, a forensic image perhaps when performed in an investigation. Creating a forensics image is one of the **most crucial steps** involved in **digital forensic investigation**.

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.

## Fun fact!

You can create a forensic image from either a **running** or **dead machine**. It is a literal **snapshot** in time that has integrity checking.

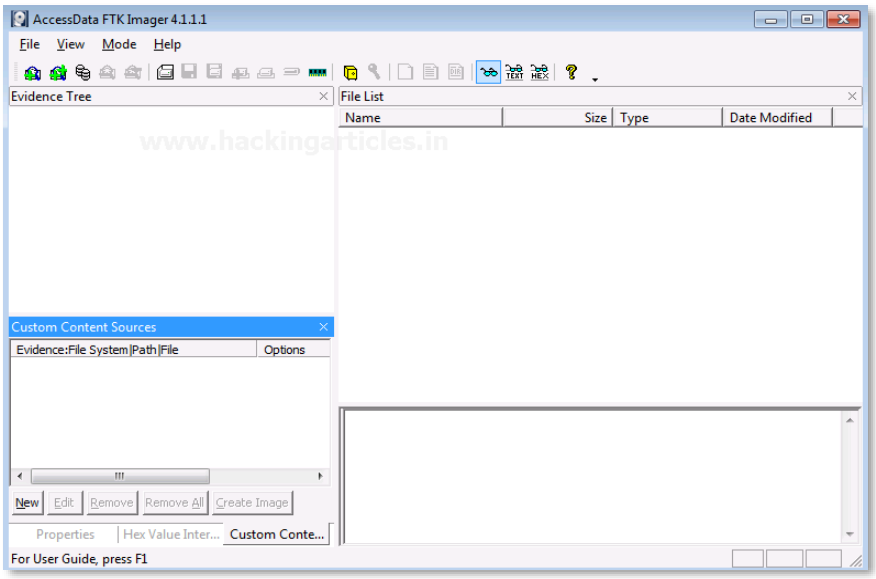
We often need to **verify the integrity of** the forensics image, as it provides a means for us to maintain **evidence integrity**, and ensure that it **is not tampered with.**

Although FTK imager is generally utilized as an imager and preview tool, it has capabilities enough to assist forensic investigators during the examination of digital devices with other matters as well.

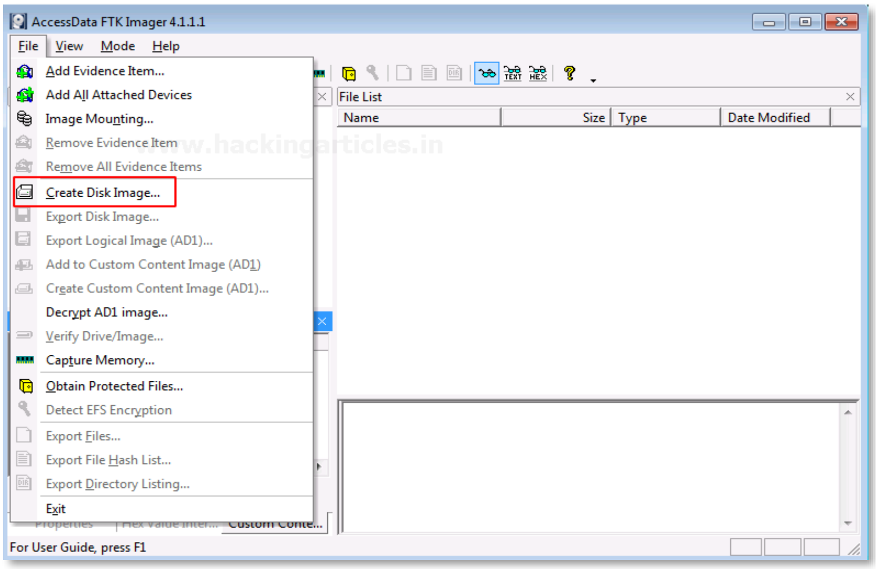
So let's get started, we'll be exploring the options FTK imager offers us in the **File** tab.

# Creating A Forensics Image

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.

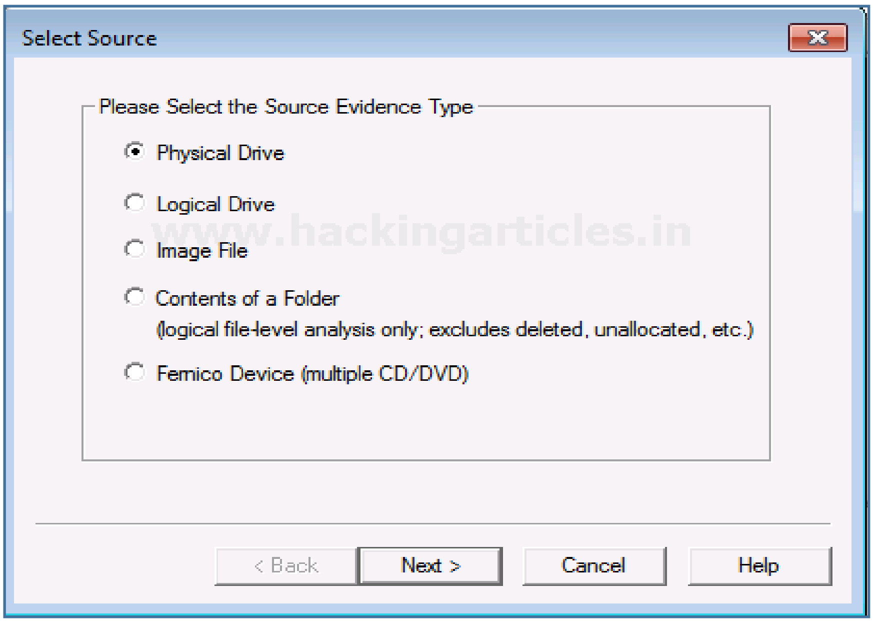

AccessData FTK Imager 4.1.1.1
File View Mode Help
Evidence Tree
File List
Name Size Type Date Modified
www.hackingarticles.in
Custom Content Sources
Evidence:File System|Path|File Options
New Edit Remove Remove All Create Image
Properties Hex Value Inter... Custom Conte...
For User Guide, press F1

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.



Please Select the Source Evidence Type

● Physical Drive

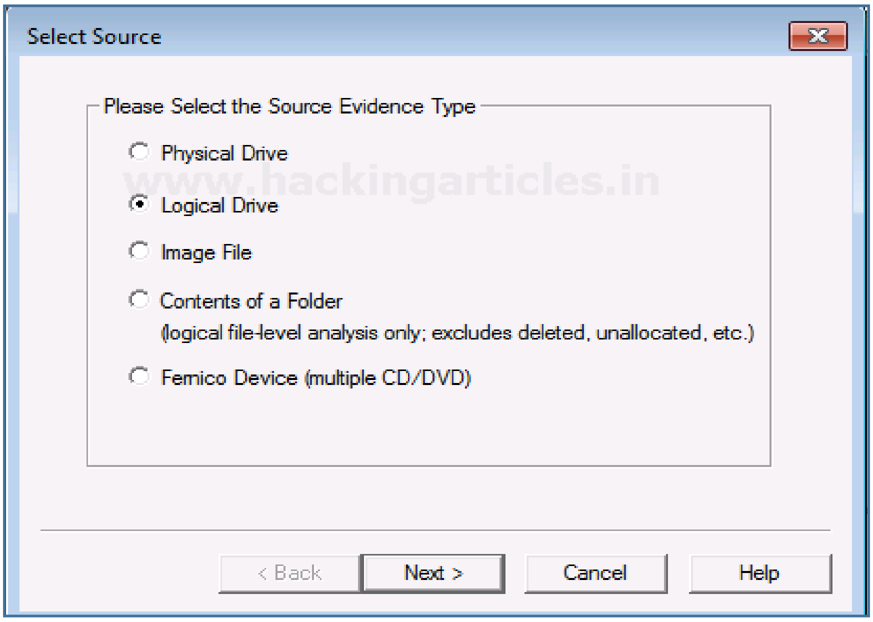
○ Logical Drive

○ Image File

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

○ Femico Device (multiple CD/DVD)

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.



Please Select the Source Evidence Type

○ Physical Drive

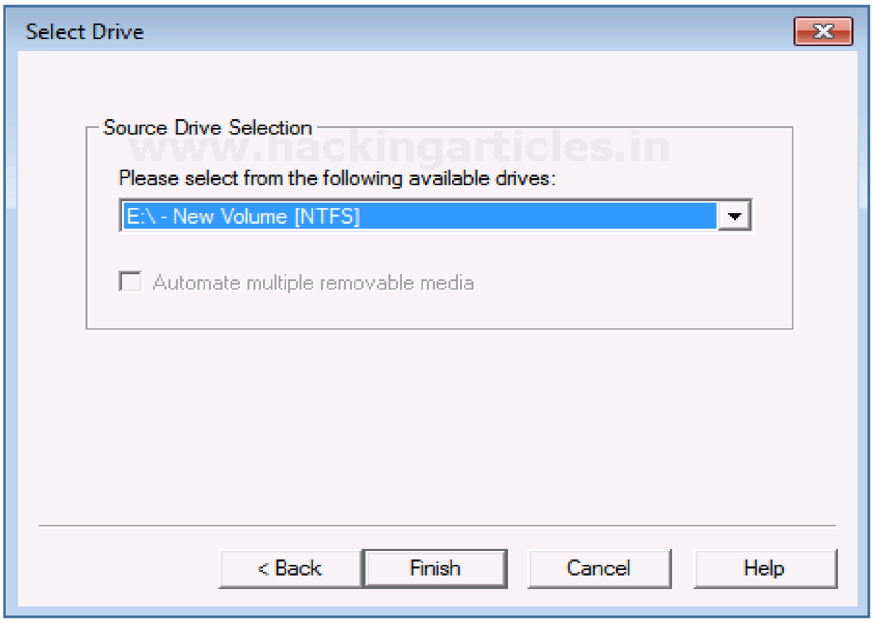
● Logical Drive

○ Image File

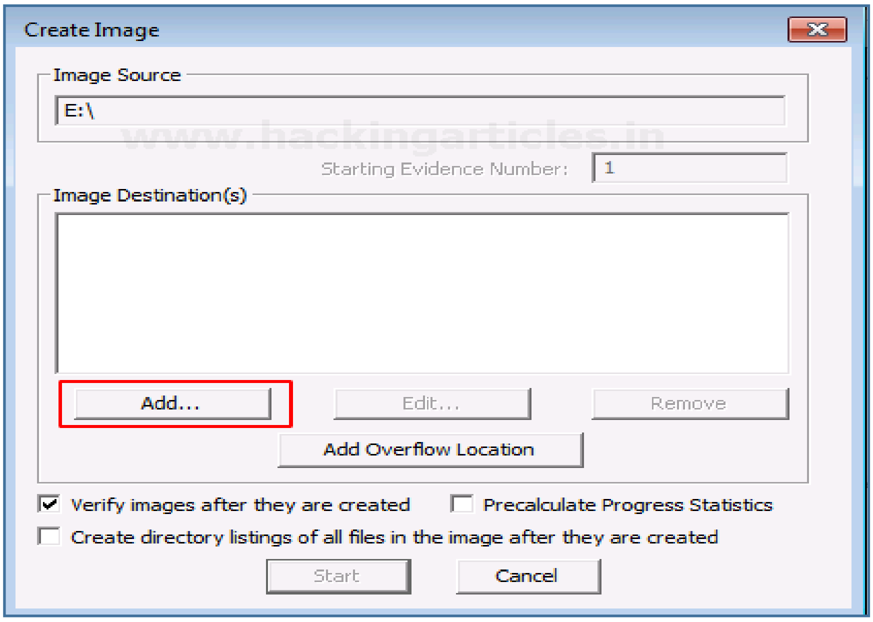
○ Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)

○ Femico Device (multiple CD/DVD)

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
< Back
Finish
Cancel
Help

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)
Add...
Edit...
Remove
Add Overflow Location
☑ Verify images after they are created
□ Precalculate Progress Statistics
□ Create directory listings of all files in the image after they are created
Start
Cancel

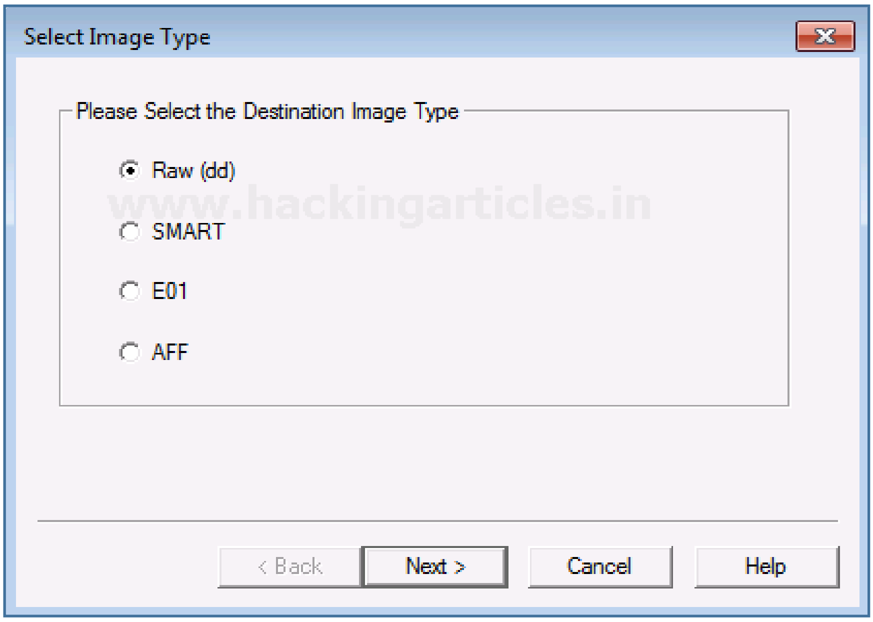
Select the format of the image that you want to create. The different formats for creating the image are:

**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.



Please Select the Destination Image Type

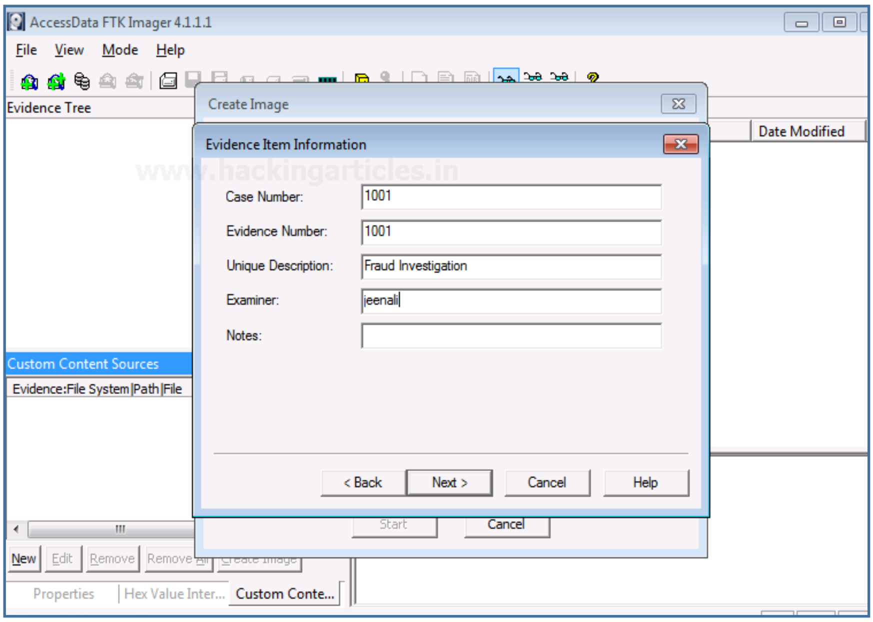
● Raw (dd)

○ SMART

○ E01

○ AFF

A Now, add the details of the image to proceed.



Case Number: 1001

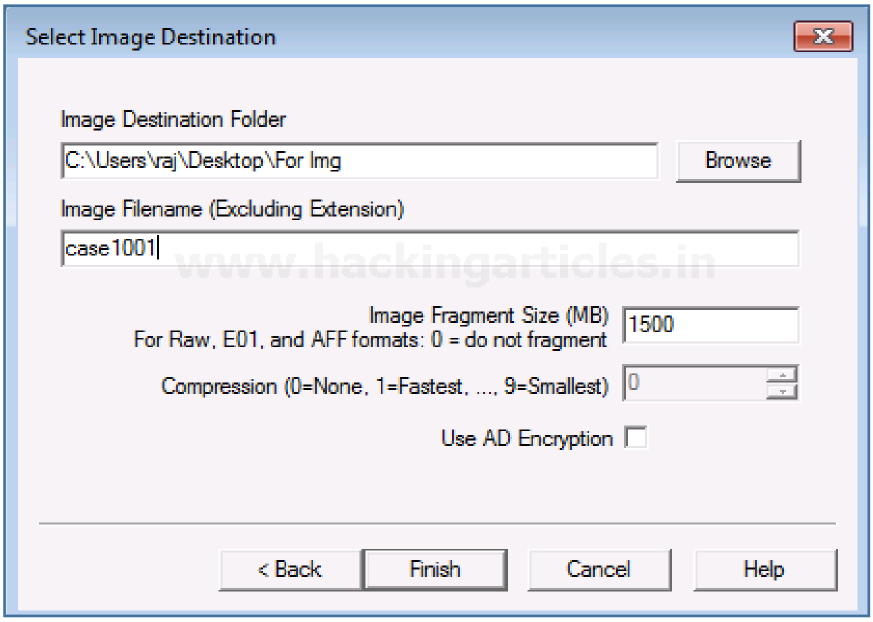
Evidence Number: 1001

Unique Description: Fraud Investigation

Examiner: jeenali

Notes:

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

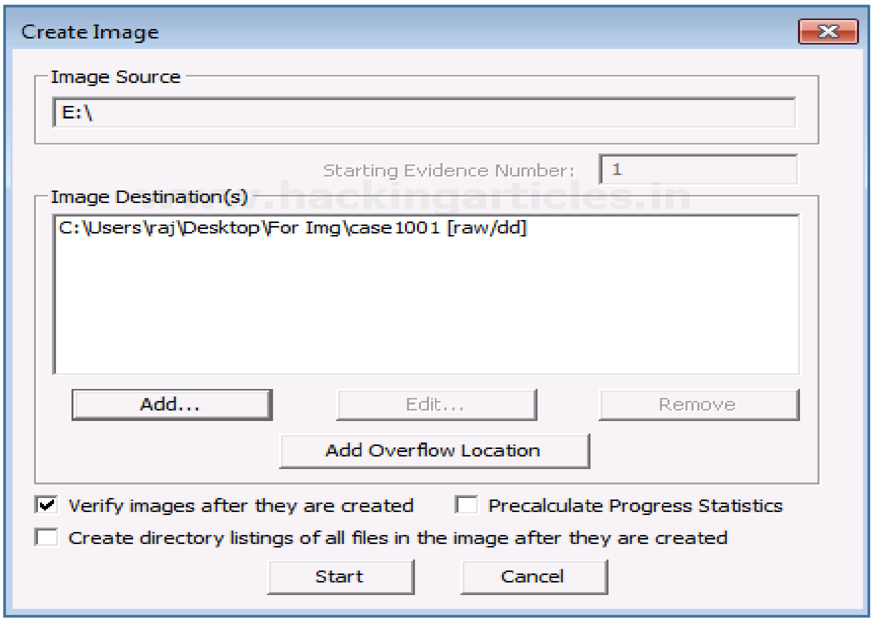
Image Filename (Excluding Extension): case1001

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 □

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.

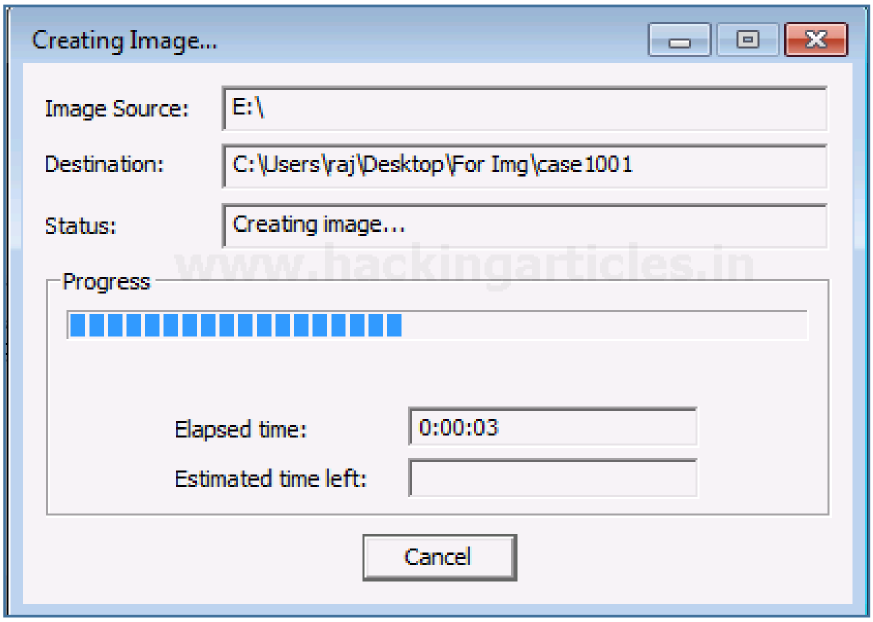


Image Source: E:\

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

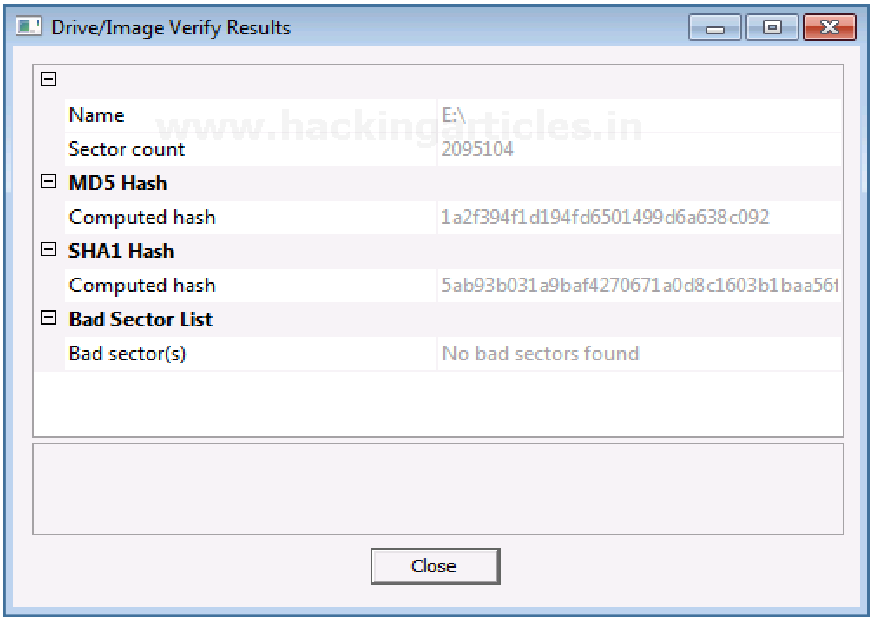
Status: Creating image…

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.



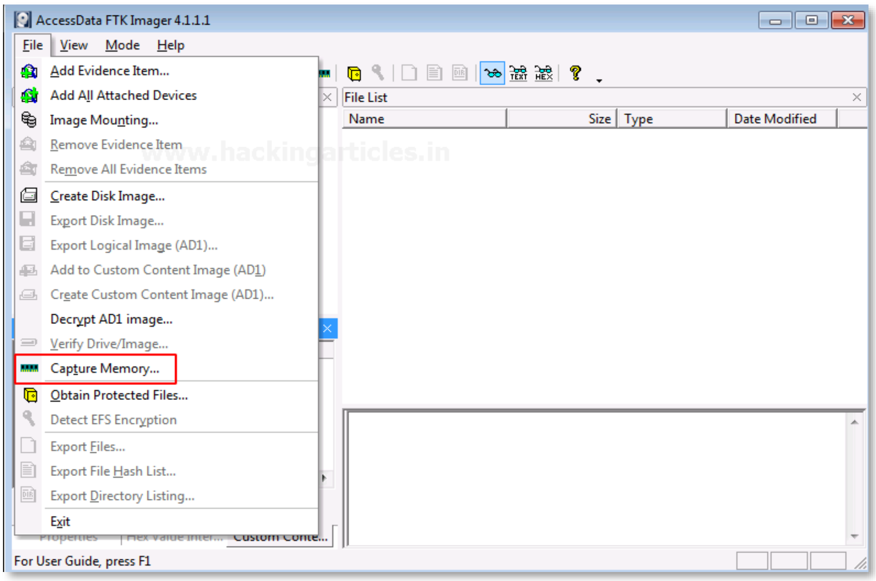
| | |
|---|---|
| Name | E:\ |
| Sector count | 2095104 |
| **MD5 Hash** | |
| Computed hash | 1a2f394f1d194fd6501499d6a638c092 |
| **SHA1 Hash** | |
| Computed hash | 5ab93b031a9baf4270671a0d8c1603b1baa56 |
| **Bad Sector List** | |
| Bad sector(s) | No bad sectors found |

# Capturing Memory

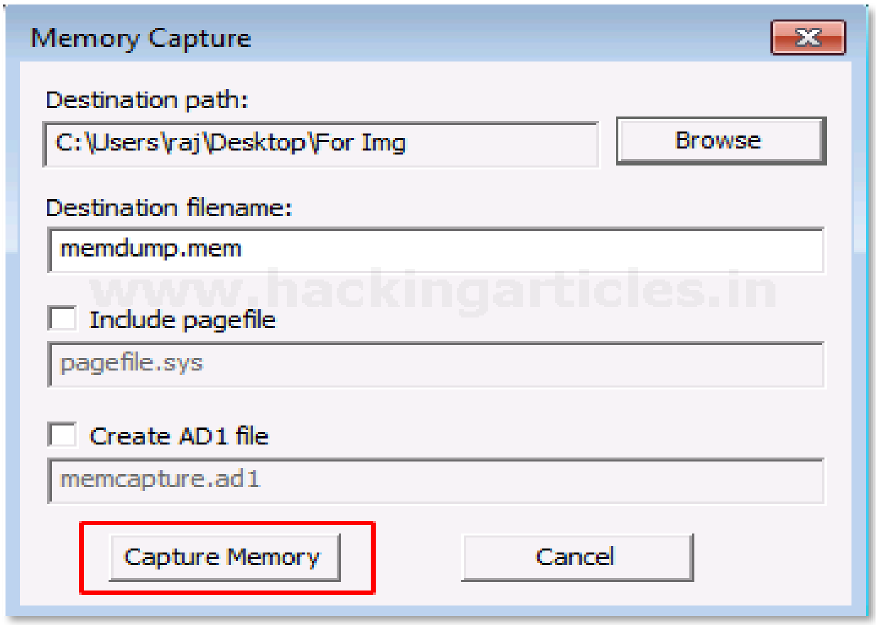
It is the method of capturing and dumping the contents of a volatile content into a non-volatile storage device to preserve it for further investigation. A ram analysis can only be successfully conducted when the acquisition has been performed accurately without corrupting the image of the volatile memory.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



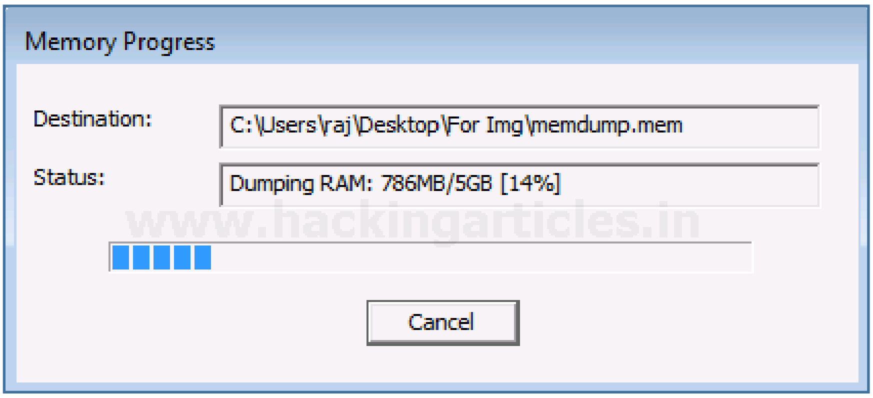
Destination path:
C:\Users\raj\Desktop\For Img

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.



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

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

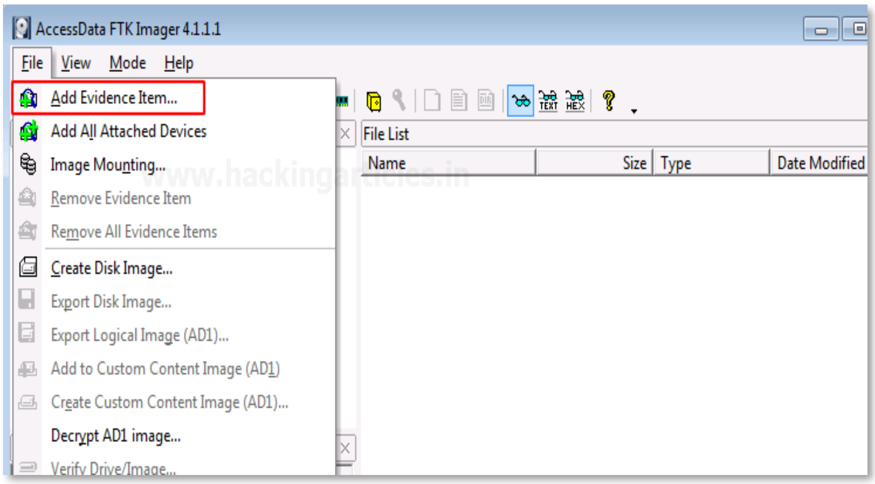
### Fun fact!

You can get lucky with RAM captures at time as they contain:

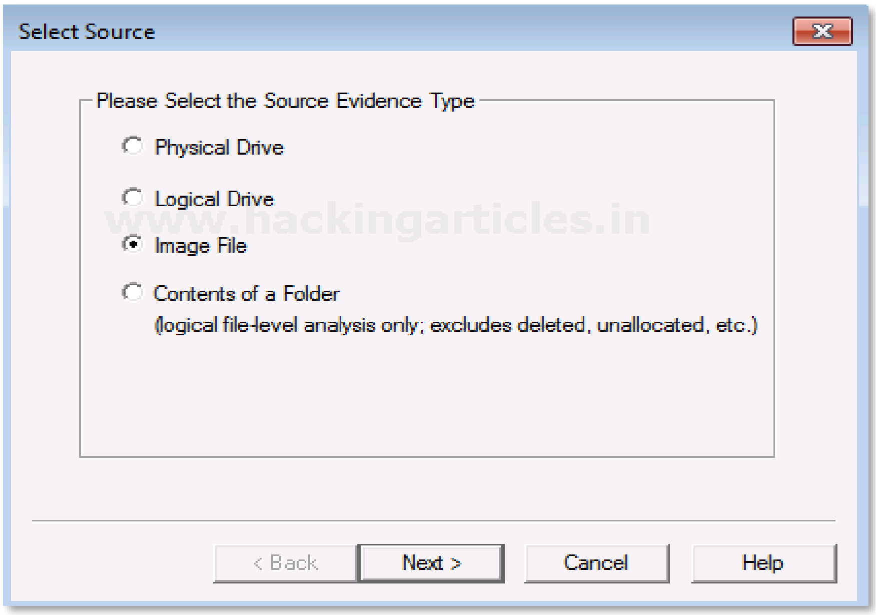
- Passwords
- Credentials
- Unsaved documents

# Analyzing Image Dump

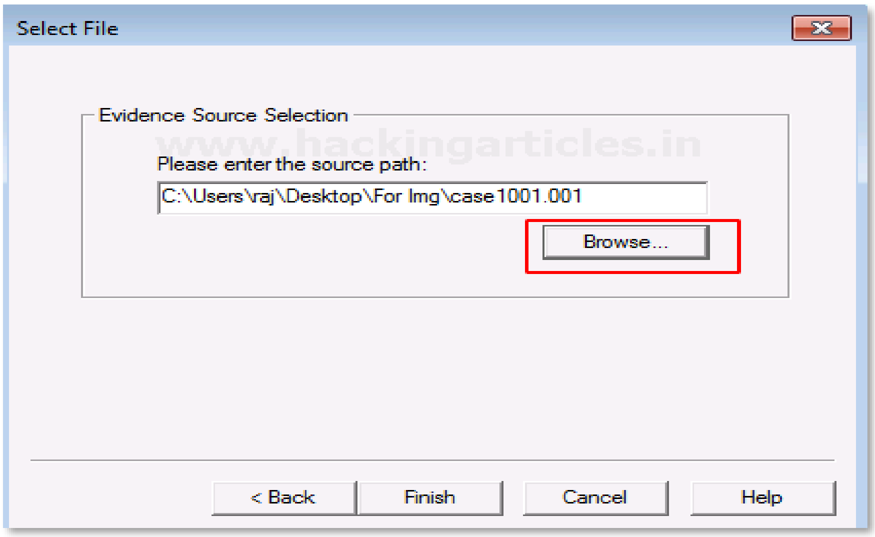
I Now let us analyze the Dump RAW Image once it has been acquired using FTK imager. To start with analysis, click on **File> Add Evidence Item.**



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.

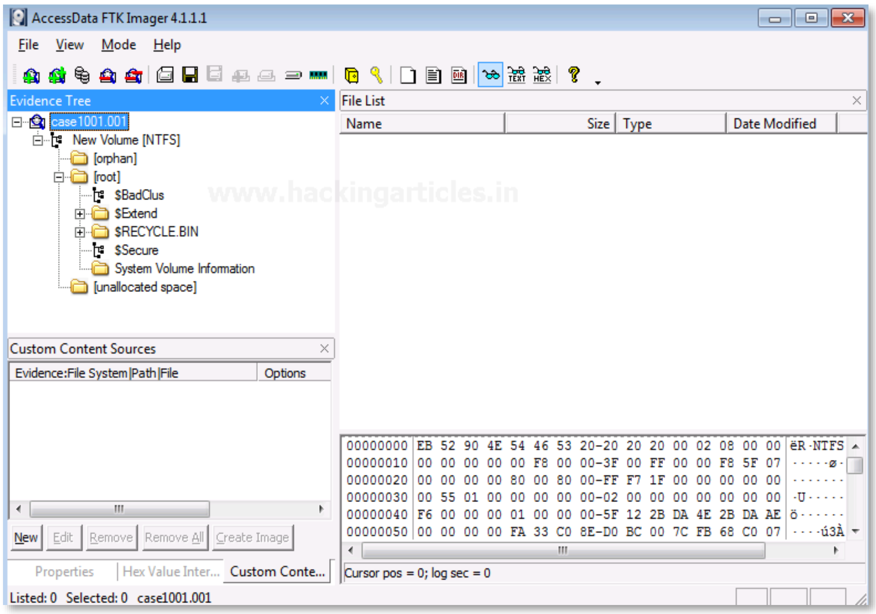

Select Source
Please Select the Source Evidence Type
○ Physical Drive
○ Logical Drive
● Image File
○ Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)
< Back
Next >
Cancel
Help

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



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.



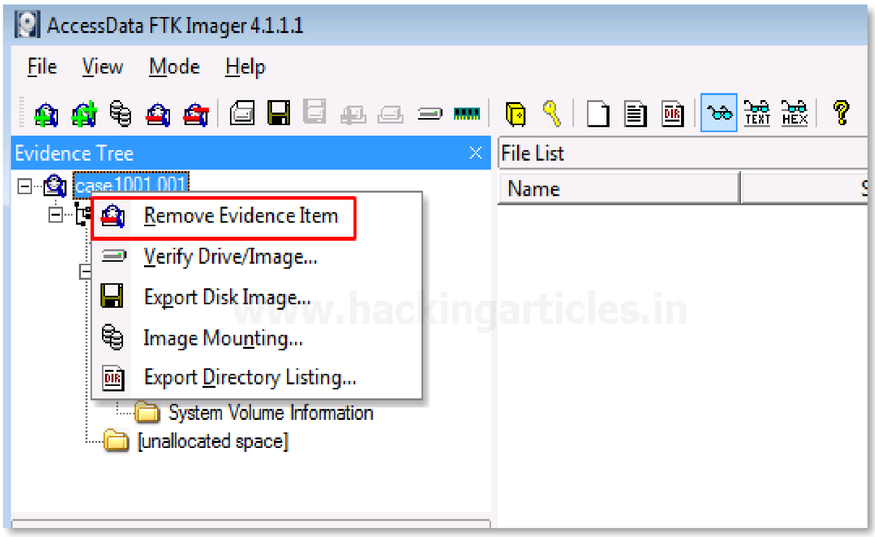
```
case1001.001
  New Volume [NTFS]
    [orphan]
    [root]
      $BadClus
      $Extend
      $RECYCLE.BIN
      $Secure
      System Volume Information
    [unallocated space]
```

```
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
```

Cursor pos = 0; log sec = 0

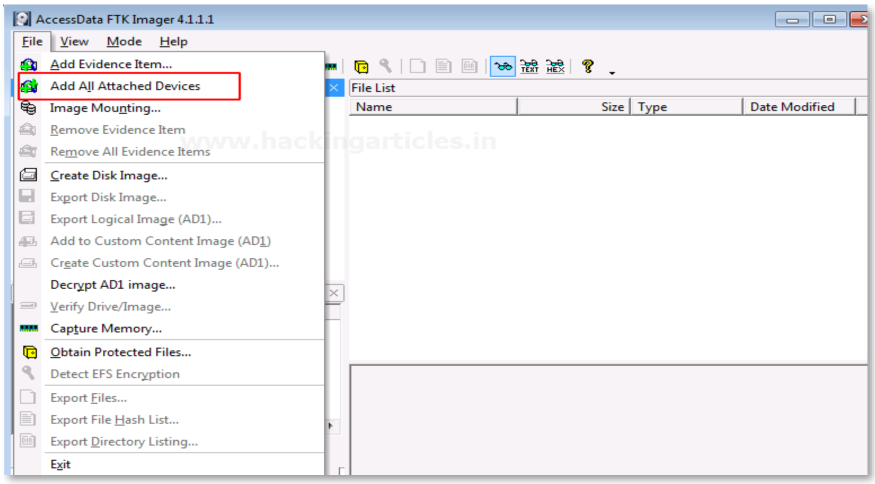
Listed: 0 Selected: 0 case1001.001

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.

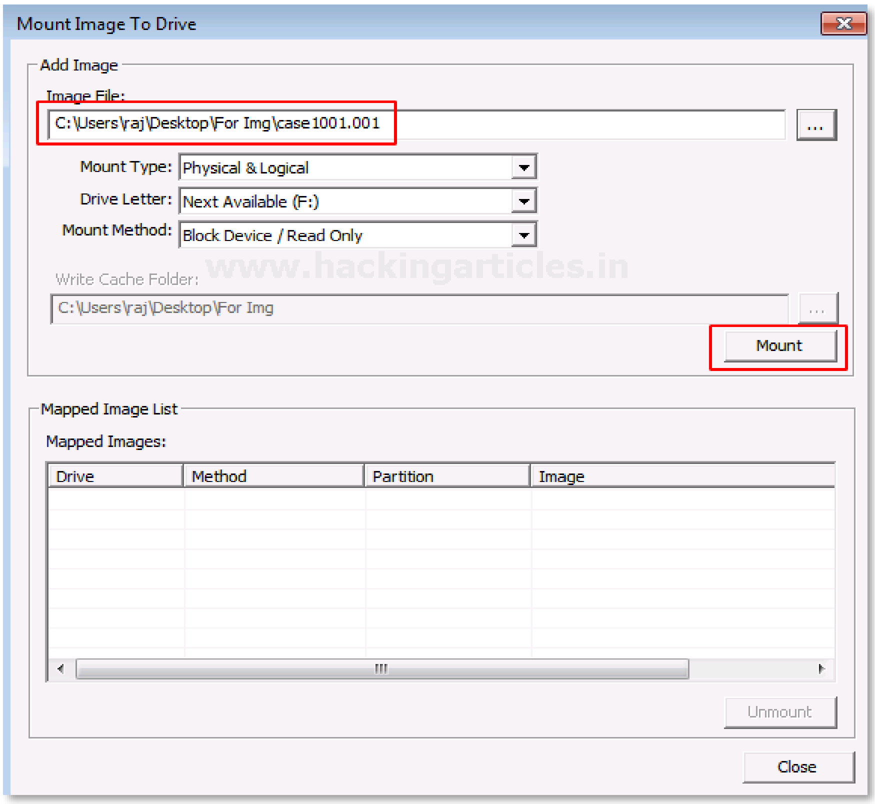


Image File: C:\Users\raj\Desktop\For Img\case1001.001

Mount Type: Physical & Logical

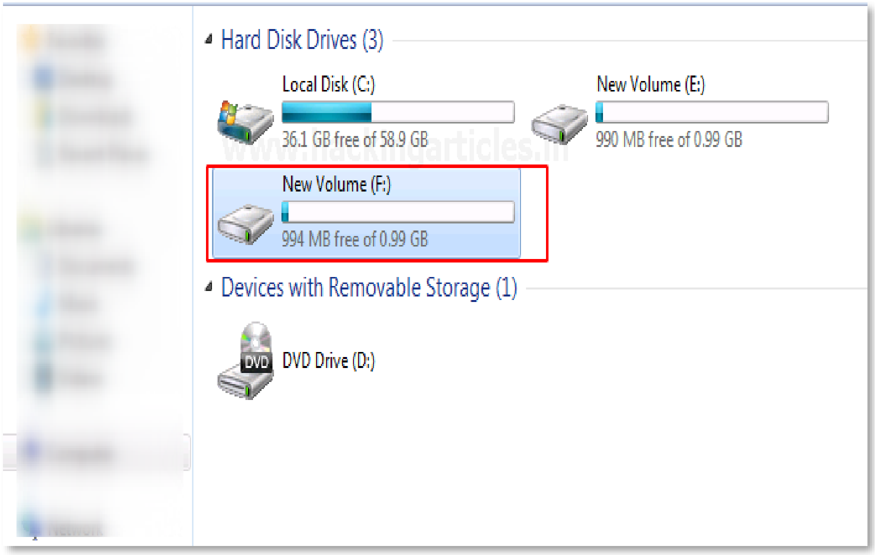
Drive Letter: Next Available (F:)

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.

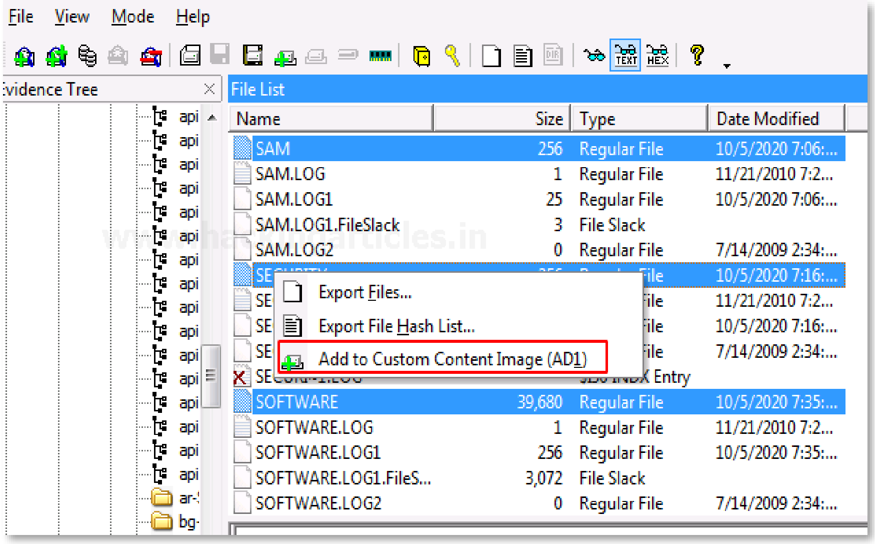


## Fun fact!

Mounting the image to a drive allows you to copy files or directories from the image file onto existing hard disks, **making the workflow much easier!**
However you still won’t be able to delete or add files thought.

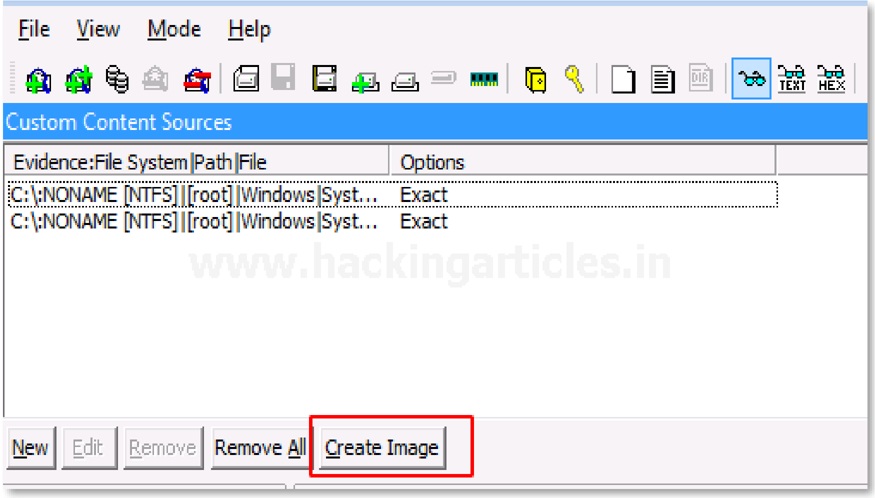
# Custom Content Image with AD Encryption

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.



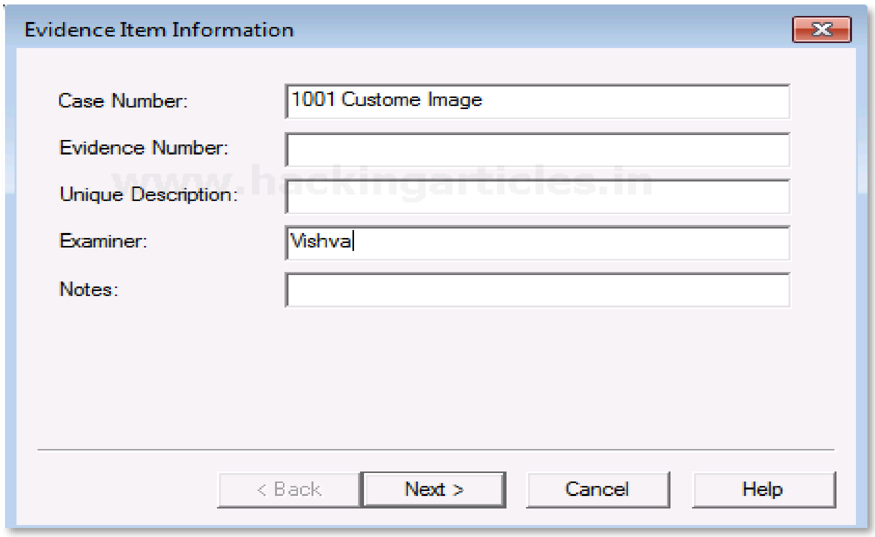
| Name | Size | Type | Date Modified |
|---|---|---|---|
| SAM | 256 | Regular File | 10/5/2020 7:06:... |
| SAM.LOG | 1 | Regular File | 11/21/2010 7:2... |
| SAM.LOG1 | 25 | Regular File | 10/5/2020 7:06:... |
| SAM.LOG1.FileSlack | 3 | File Slack | |
| SAM.LOG2 | 0 | Regular File | 7/14/2009 2:34:... |
| 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.



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.

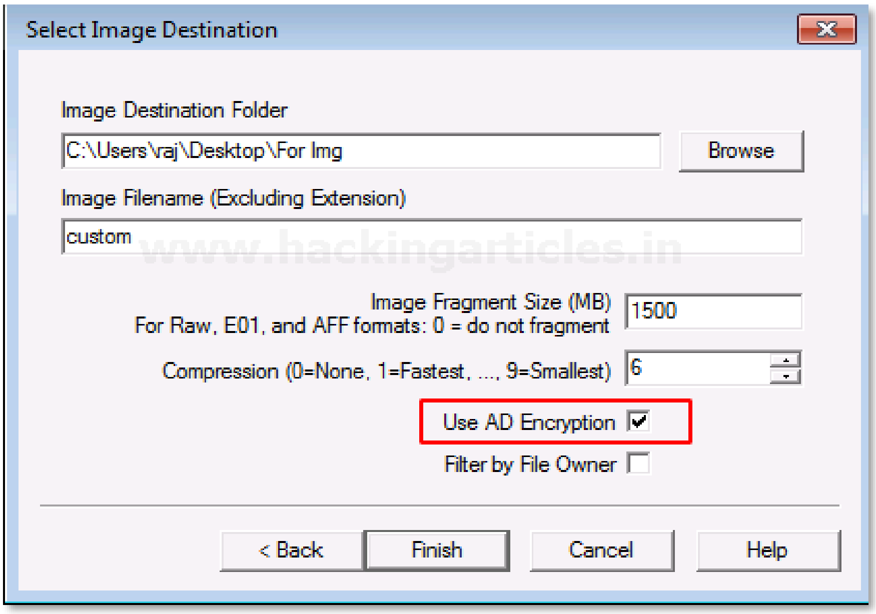


Image Destination Folder: C:\Users\raj\Desktop\For Img

Image Filename (Excluding Extension): custom

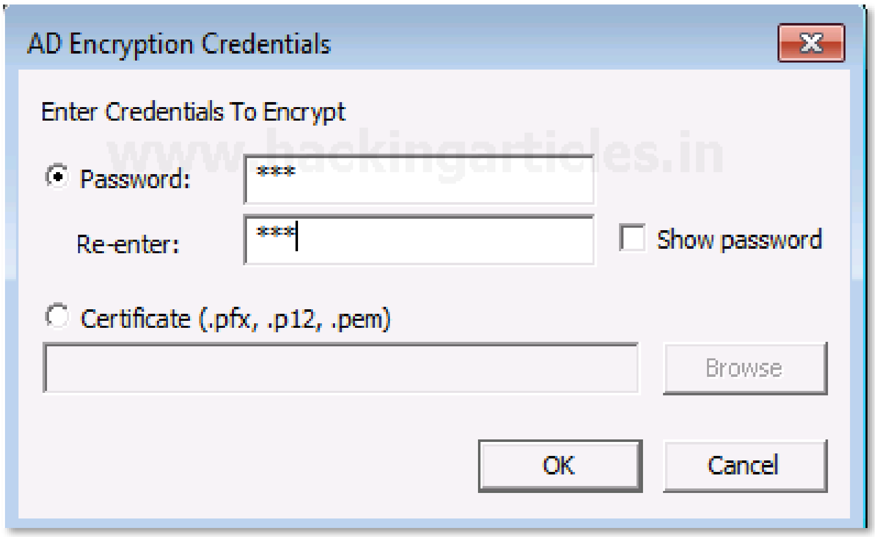
Image Fragment Size (MB) For Raw, E01, and AFF formats: 0 = do not fragment: 1500

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

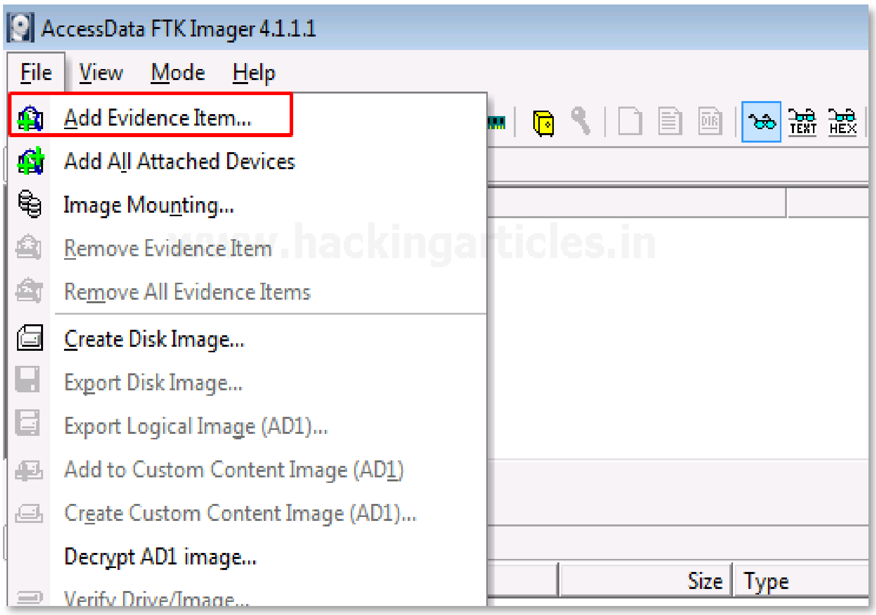
Use AD Encryption ☑

Filter by File Owner □

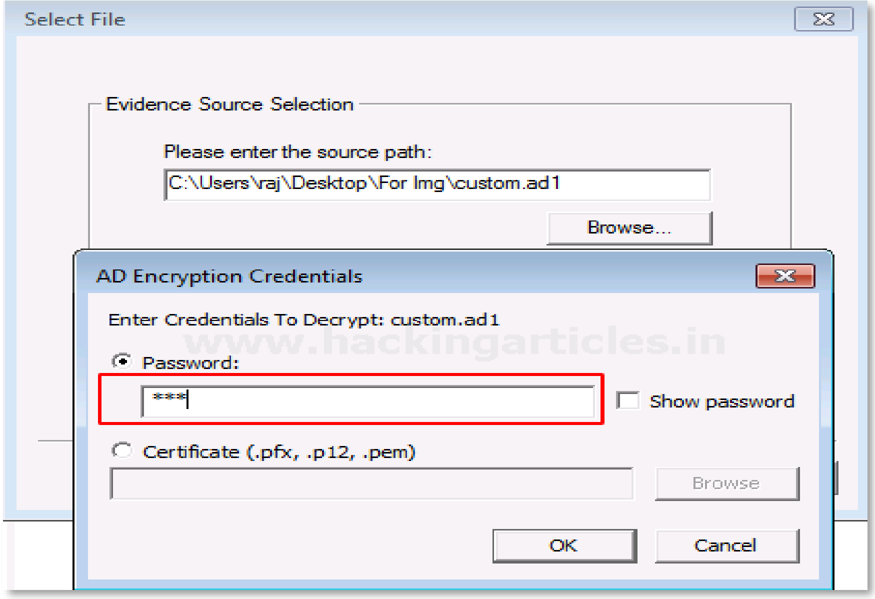
A new window will pop-up to encrypt the image, Now renter and re-enter the password that you want to add for your image.


AD Encryption Credentials
Enter Credentials To Encrypt
● Password: ***
Re-enter: ***
□ Show password
○ Certificate (.pfx, .p12, .pem)
Browse
OK
Cancel

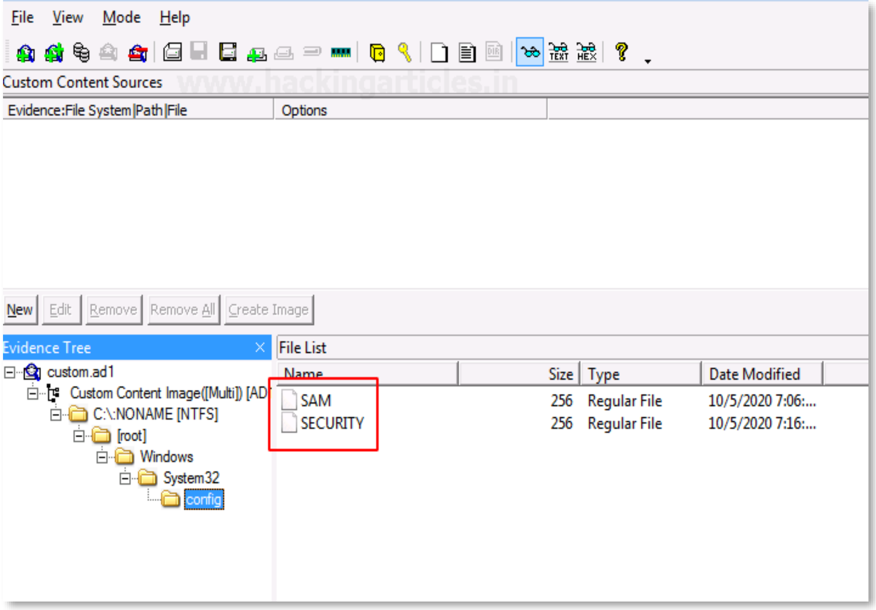
Now to see the encrypted files, click on **File> Add Evidence Item**...



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


Select File
Evidence Source Selection
Please enter the source path:
C:\Users\raj\Desktop\For Img\custom.ad1
Browse...
AD Encryption Credentials
Enter Credentials To Decrypt: custom.ad1
● Password:
***
□ Show password
○ Certificate (.pfx, .p12, .pem)
Browse
OK
Cancel

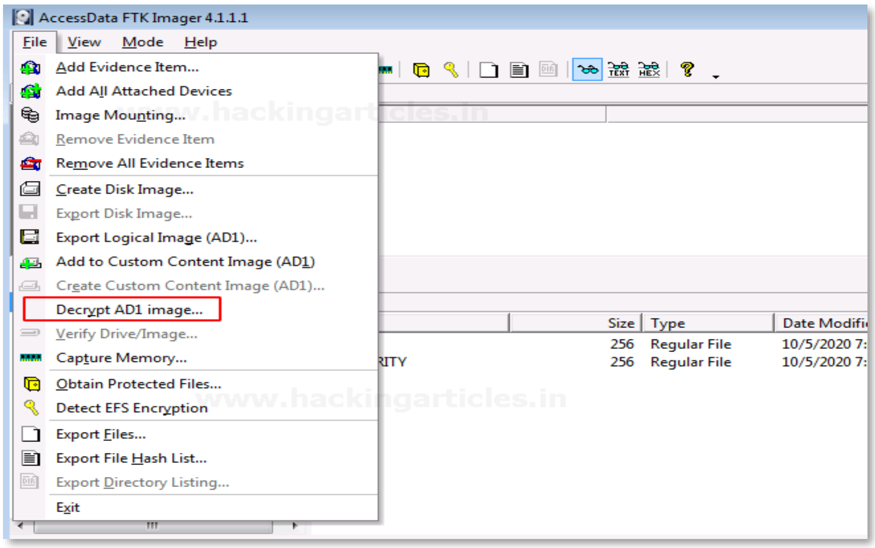
You will now see the two encrypted files on entering the valid passwords.



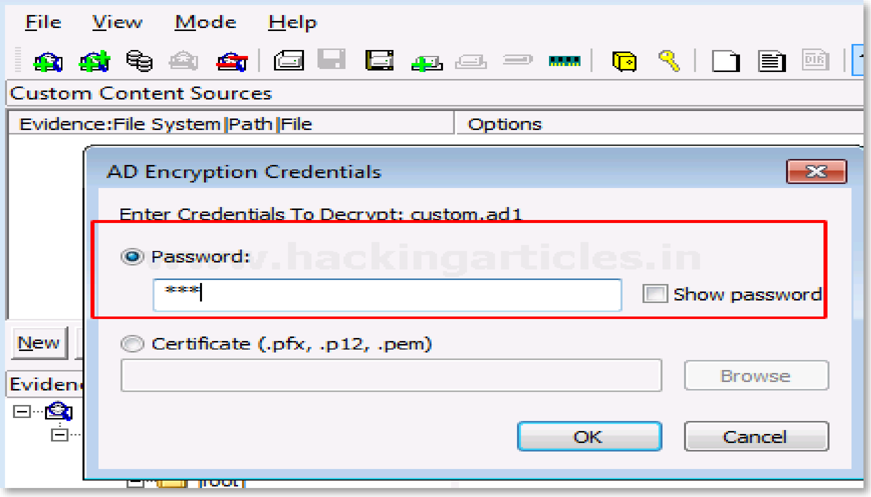
| Name | Size | Type | Date Modified |
|---|---|---|---|
| SAM | 256 | Regular File | 10/5/2020 7:06:... |
| SECURITY | 256 | Regular File | 10/5/2020 7:16:... |

# Decrypt AD1 Image

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

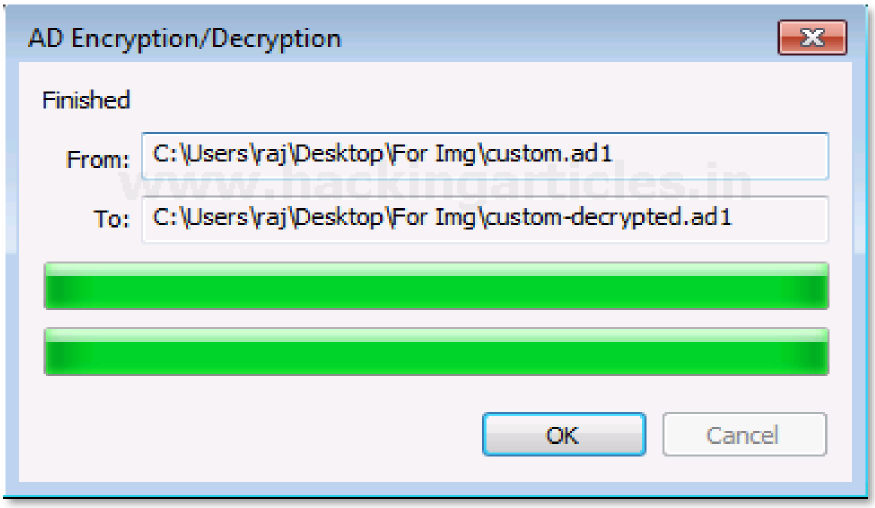


Now you need to enter the password for the image file that was encrypted and click on Ok.



File
View
Mode
Help
Custom Content Sources
Evidence:File System|Path|File
Options
New
Eviden
AD Encryption Credentials
Enter Credentials To Decrypt: custom.ad1
● Password:
***
□ Show password
○ Certificate (.pfx, .p12, .pem)
Browse
OK
Cancel

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

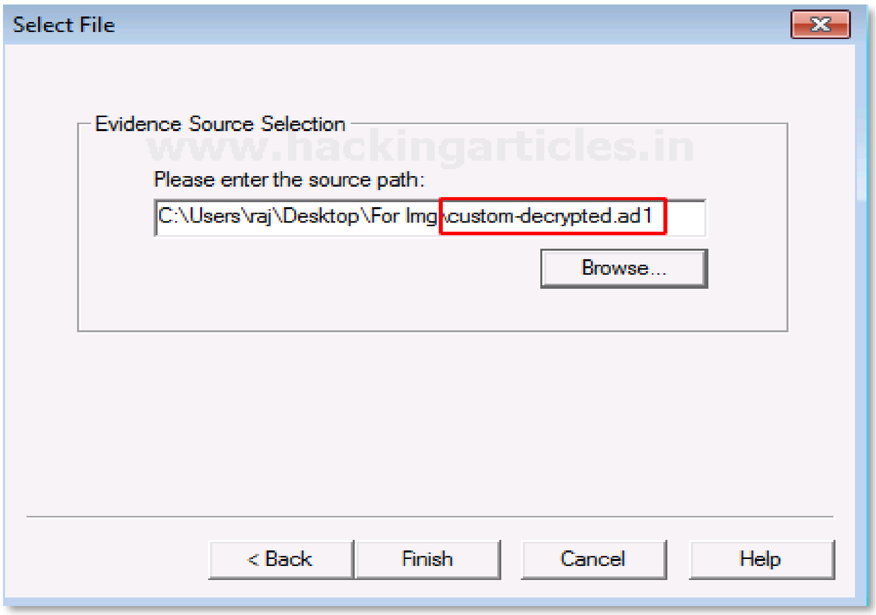


Finished

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

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

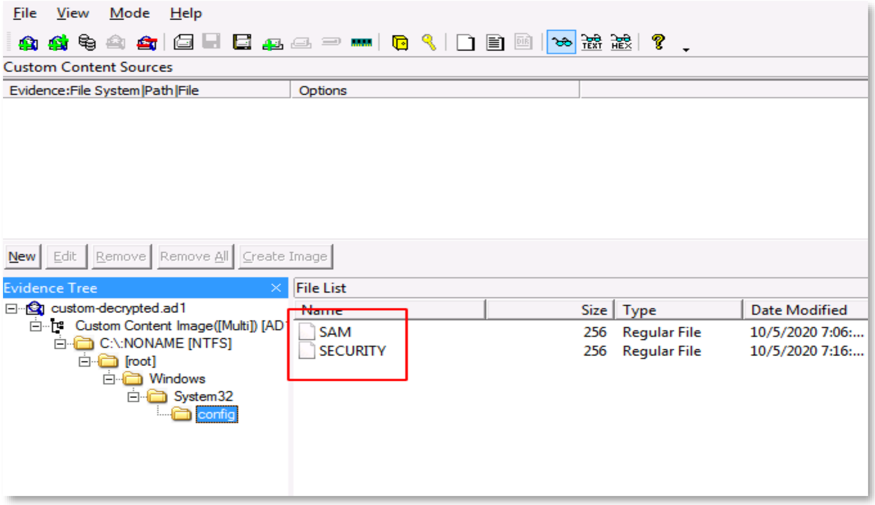
To view the decrypted custom content image, add the path of the decrypted file and click on Finish.



Please enter the source path:

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

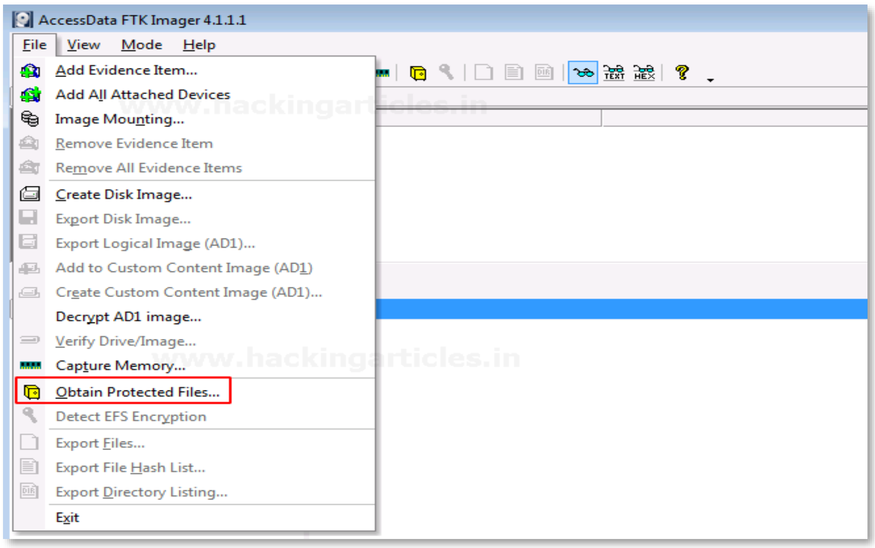
You will now be able to see the encrypted files by using the correct password to decrypt it.



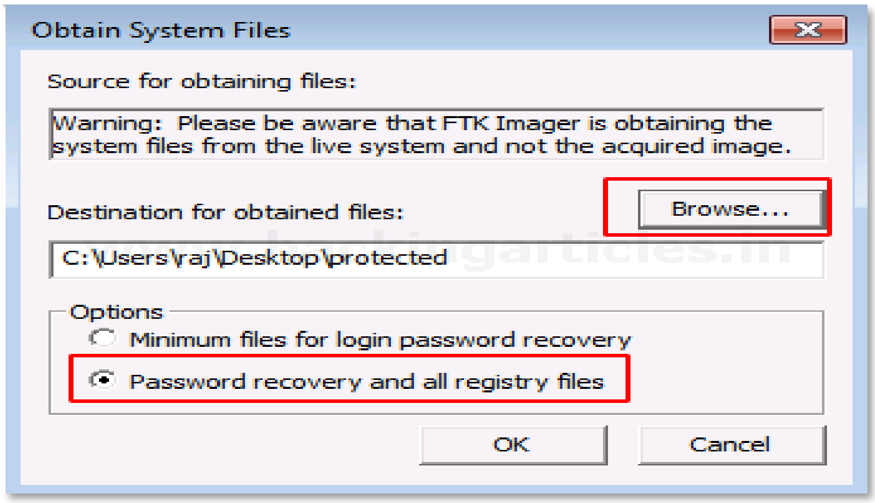
```
Name        Size  Type          Date Modified
SAM         256   Regular File  10/5/2020 7:06:...
SECURITY    256   Regular File  10/5/2020 7:16:...
```

# 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.

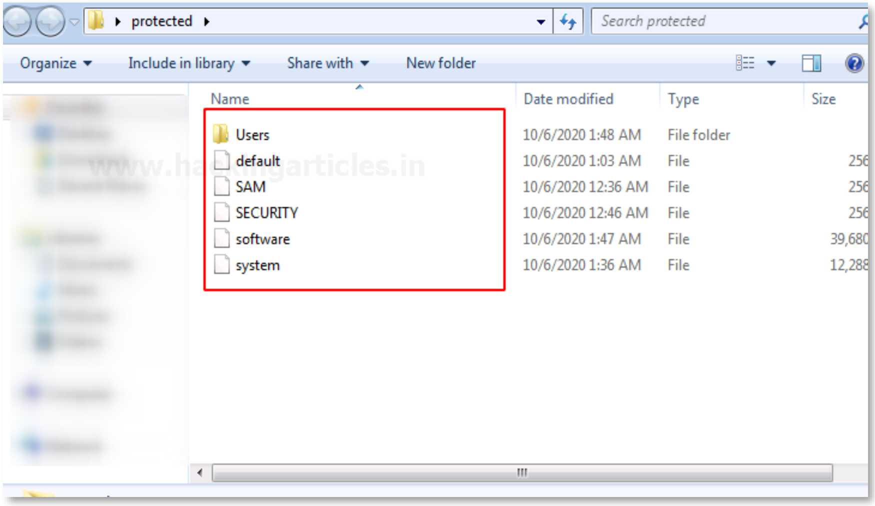


Warning: Please be aware that FTK Imager is obtaining the system files from the live system and not the acquired image.

Destination for obtained files: C:\Users\raj\Desktop\protected

Options
○ Minimum files for login password recovery
● Password recovery and all registry files

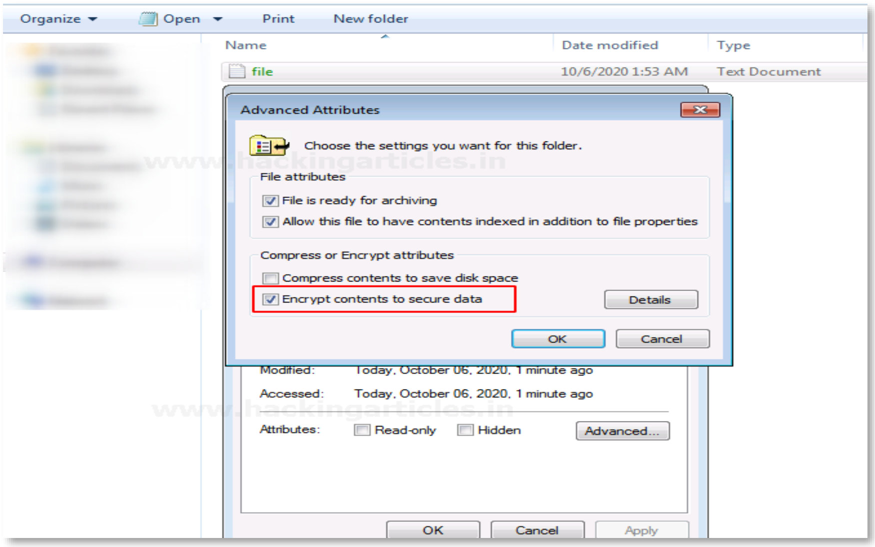
Now you will see all the protected files in one place



| 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

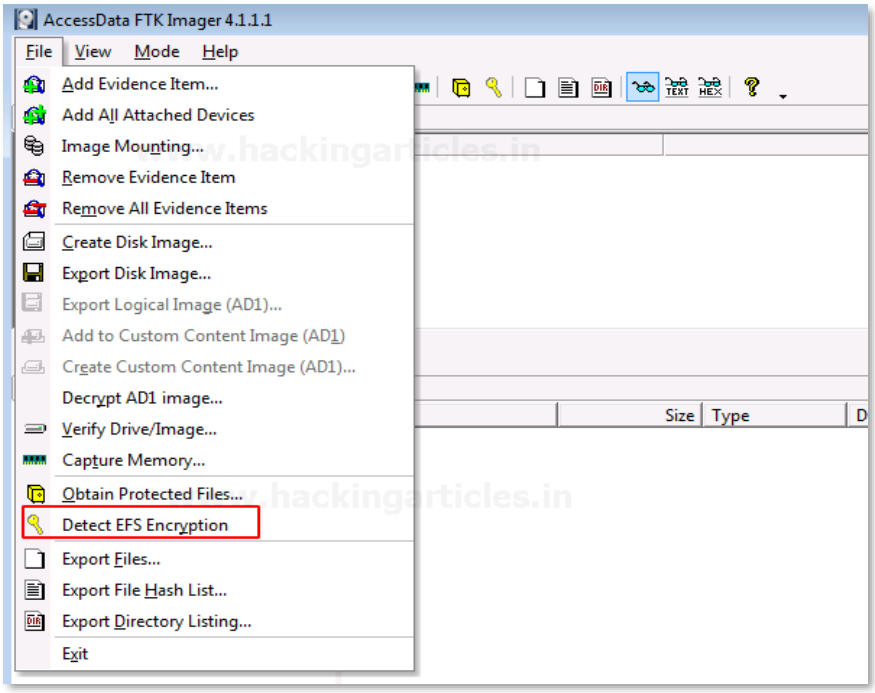
☑ Encrypt contents to secure data

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

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

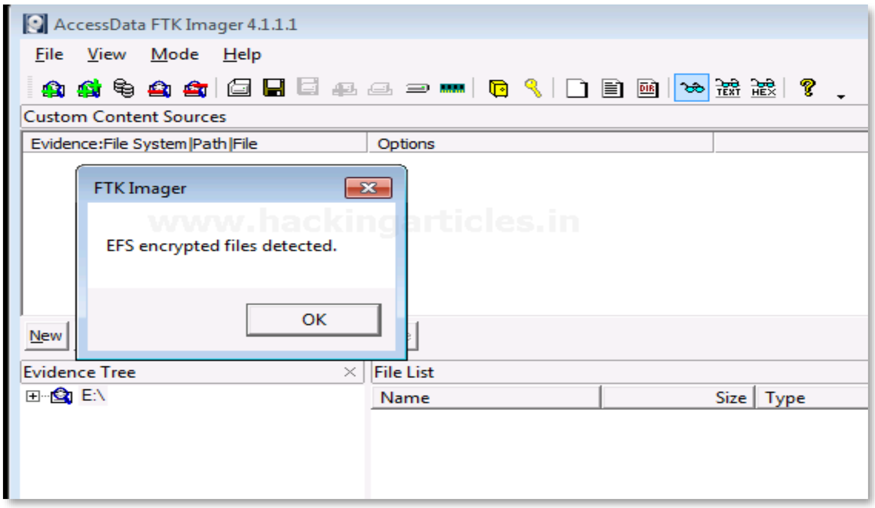
Attributes: ☐ Read-only ☐ Hidden

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



AccessData FTK Imager 4.1.1.1

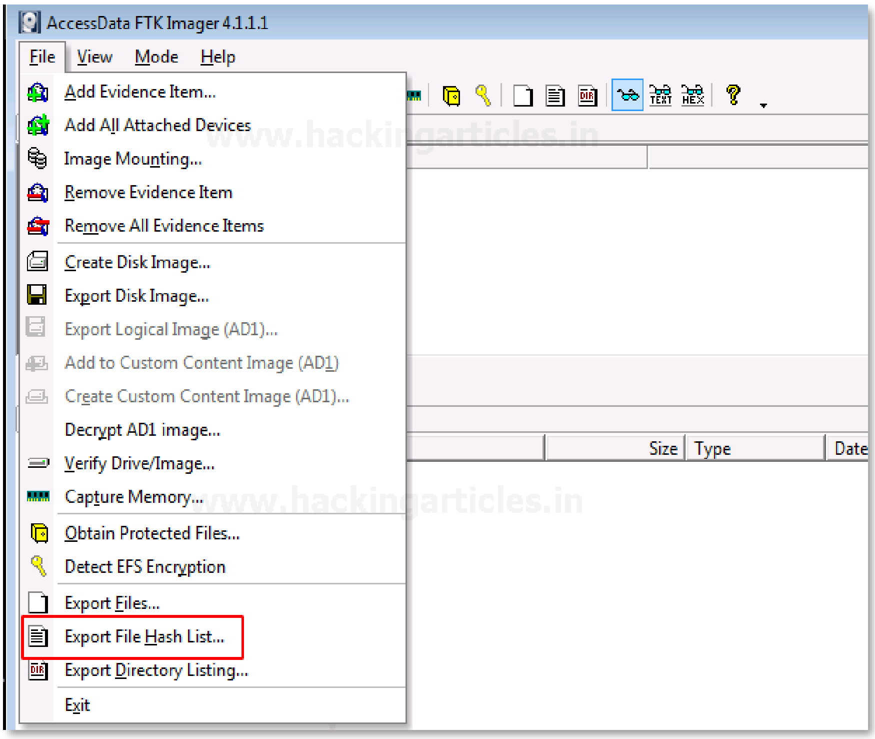
You can see that the encryption is detected.



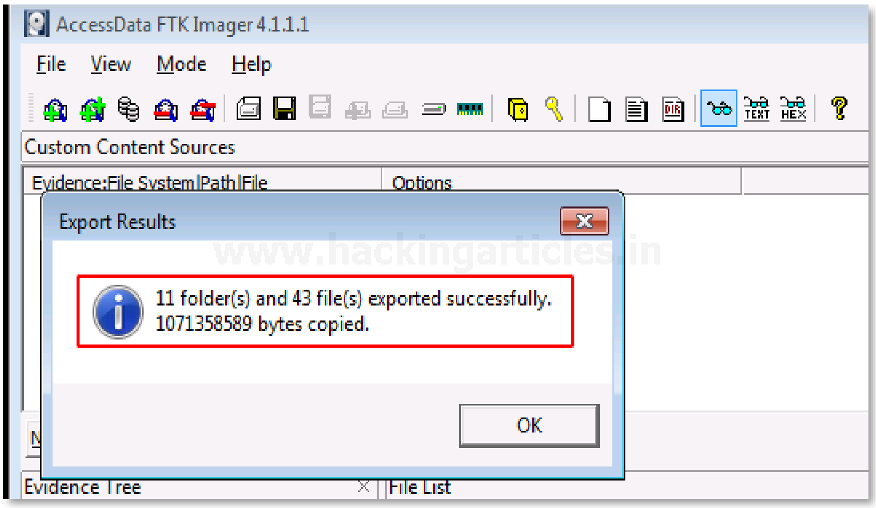
EFS encrypted files detected.

# 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.

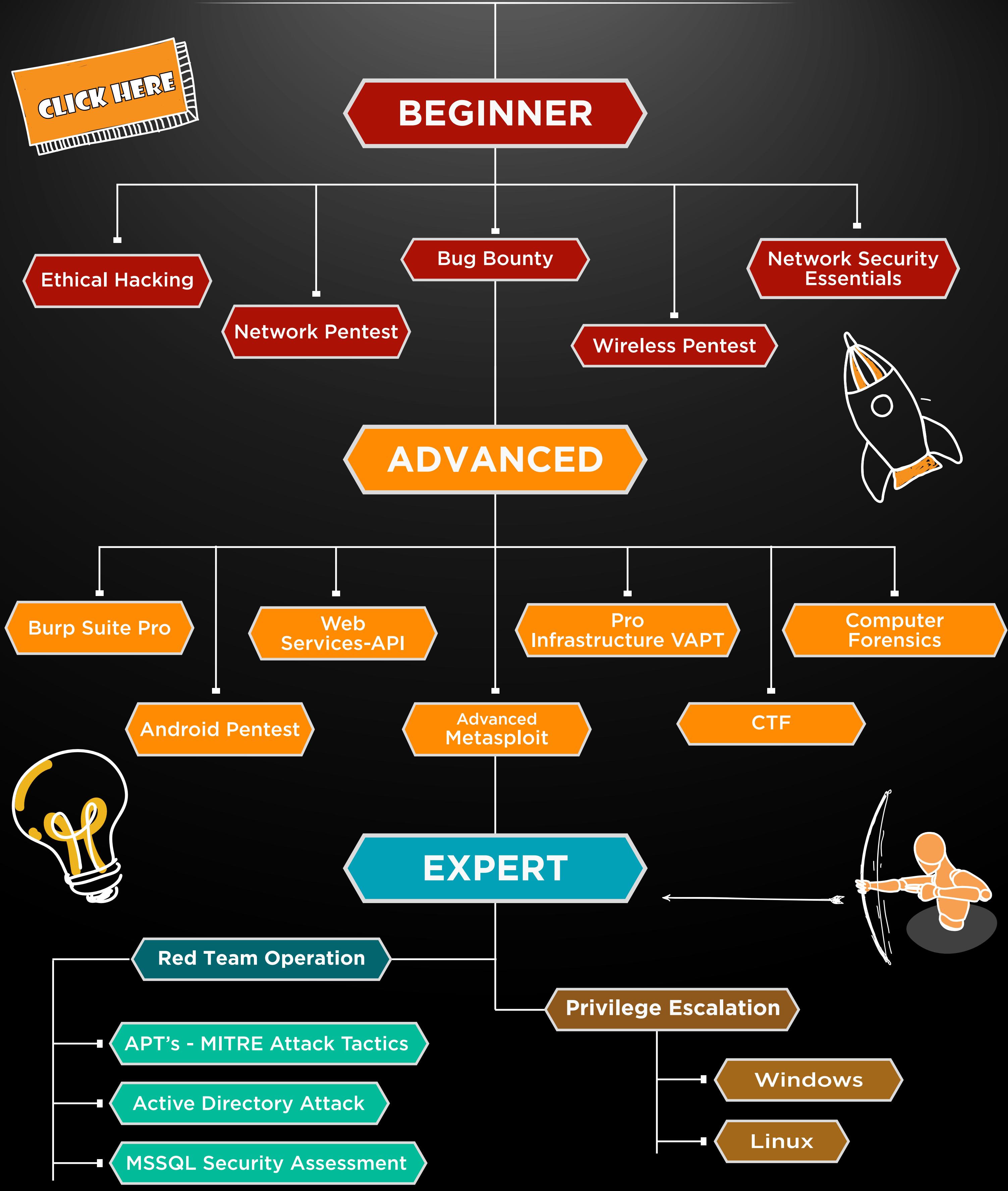


11 folder(s) and 43 file(s) exported successfully.
1071358589 bytes copied.

iGNITE Technologies

# JOIN OUR TRAINING PROGRAMS

CLICK HERE



www.ignitetechnologies.in