



### DIGITAL FORENSIC FTK IMAGER

#### **Table of Contents**

Introduction to images and FTK Imager	5
Creating a forensics image	7
Capturing Memory	13
Analyzing Image Dump	16
Mounting Image to drive	20
Custom Content Image with AD Encryption	23
Decrypt AD1 Image	28
Obtain Protected Files	32
Detect EFS Encryption	35
Export Files	38
About Us	41



#### 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 & FTK Imager

#### **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.



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.



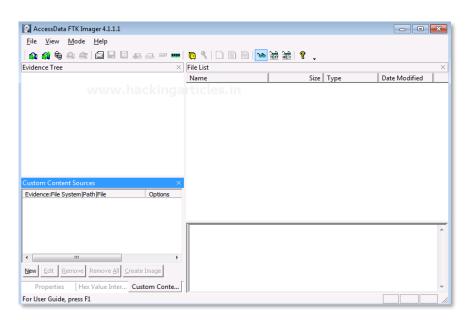
### **Creating A Forensics Image**

()

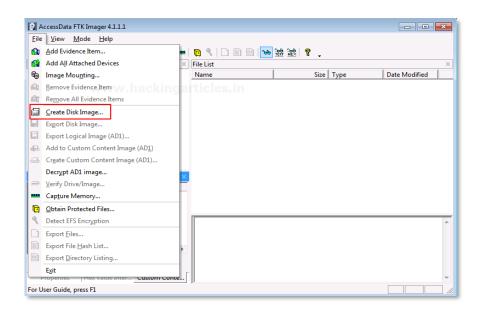


### **Creating A Forensics Image**

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.



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	t Source	×
	Please Select the Source Evidence Type Physical Drive Conjcal Drive Image File Contents of a Folder (logical file-level analysis only; excludes deleted, unallocated, etc.)	
	C Femico 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 C Logical Drive
<ul> <li>Image File</li> <li>Contents of a Folder (logical file-level analysis only; excludes deleted, unallocated, etc.)</li> </ul>
C Femico 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]	
< 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:\	ockingarticle	e in
	Starting Evidence Number:	1
Image Destination(s)		
Add	Edit	Remove
	Add Overflow Location	]
Verify images after they	are created 🗌 Precalcula	te 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.

Sele	ect Image Type	×
	<ul> <li>Please Select the Destination Image Type</li> <li>Raw (dd)</li> <li>SMART</li> <li>C SMART</li> <li>C E01</li> <li>C AFF</li> </ul>	
_	< Back Next > Cancel Help	

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

AccessData FTK Imager 4.1.	11			
	.1.1			
<u>F</u> ile <u>V</u> iew <u>M</u> ode <u>H</u> elp				
🔒 🏩 🗣 🛳 🖛 🖾	í	<u>► 9   ► ► ► ► ► ► ► ►</u>		
Evidence Tree	Create Image		23	
	Evidence Item Informat	tion	× (	Date Modified
WW	v.hackingai			
	Case Number:	1001		
	Evidence Number:	1001		
	Unique Description:	Fraud Investigation		
	Examiner:	jeenali		
	Notes:			
Custom Content Sources				
Evidence:File System  Path  File				
		< Back Next > Cancel Help		
		< Back Next > Cancel Help		
III		Start Cancel		
New Edit Remove Remove	Hill Zieace muaße			
Properties Hex Value In	nter Custom Conte			



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 Browse
Image Filename (Excluding Extension)           case1001
Image Fragment Size (MB)
Compression (0=None, 1=Fastest,, 9=Smallest) 0
< 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)	hackingartici	es.in
Add	Edit	Remove
	Add Overflow Location	
	y are created 🛛 🗍 Precalcula	-
	y are created  Precalcula s of all files in the image after th Start  Cancel	-



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	ww.hackingarticles.in		
Elapsed time: 0:00:03 Estimated time left:			
	Cancel		

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 Sector count	E:\_ticles.in		
MD5 Hash			
Computed hash	1a2f394f1d194fd6501499d6a638c092		
SHA1 Hash			
Computed hash	5ab93b031a9baf4270671a0d8c1603b1baa561		
Bad Sector List			
Bad sector(s)	No bad sectors found		
Close			



### Capturing Memory

.

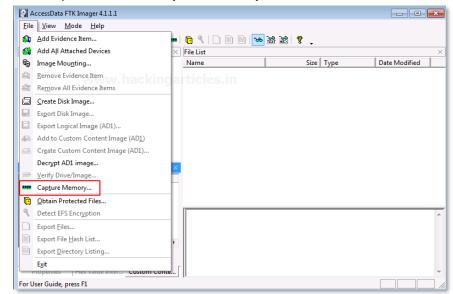
()

### **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.



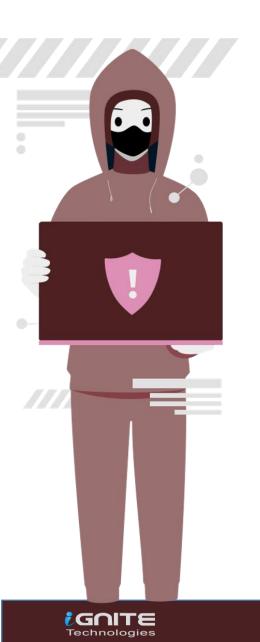
Choose the destination path and the destination file name, and click on capture memory.

Memory Capture
Destination path: C:\Users\raj\Desktop\For Img Browse
Destination filename:
memdump.mem
🗍 Include pagefile
pagefile.sys
Create AD1 file
memcapture.ad1
Capture Memory Cancel



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

Memory Prog	ress
Destination:	C:\Users\raj\Desktop\For Img\memdump.mem
Status:	Dumping RAM: 786MB/5GB [14%]
	ww.hackingarticles.in
	Cancel





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

- Passwords
- Credentials
- Unsaved documents

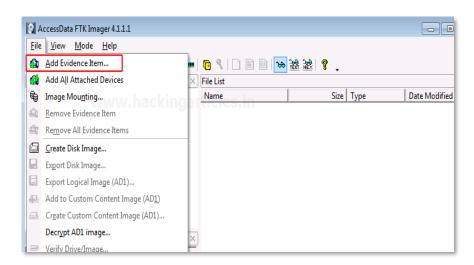
### Analysing Image Dump

-

()

### **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 Cogical 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.

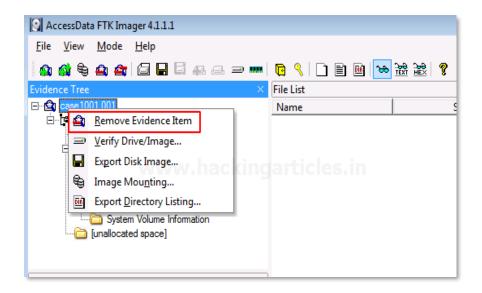
Select File	×
Evidence Source Selection Please enter the source path: C:\Users\raj\Desktop\For Img\case1001.001 Browse	
< Back Finish Cancel Help	

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															-			x
<u>F</u> ile <u>V</u> iew <u>M</u> ode <u>H</u> elp																		
		<b>0</b>	) 🖹	DIR	æ		證	ę										
Evidence Tree	×	File List		_					•									×
⊡ <b>©</b> 1 case1001.001		Name							Size	Tvp	e			D	ate N	Iodifie	be	_
New Volume [NTFS]					_					-76	-							_
[orphan]																		
iroot]																		
BadClus WWW.ha																		
⊕-     ⊕     SEctend     sRECYCLE.BIN																		
SRECTCLE.BIN																		
System Volume Information																		
[unallocated space]																		
Custom Content Sources	×																	
Evidence:File System Path File Options																		
		00000000	EB 5	2 90	4F.	54	46	53	20-20	20	20	00	02	08	00 0	0 ëR	-NTES	
		00000010				00	F8 (	00	00-3F	00	FF	00	00	F8	5F 0	_	ø	
		00000020	00 0	0 00	00	80	00 1	80	00-FF	F7	1F	00	00	00	00 0	0		-
	F	00000030							00-02			00			00 0		• • • • •	
		00000040								_			_		DA A		· · ú3À	
New Edit Remove Remove All Create Image		00000050	00 0	0 00	00	rA			0E-D0	БС	00	10	гB	08			- · u 3A	
Properties Hex Value Inter Custom Conte.	Г	Cursor pos =	0.100		. 0	_	_			-	_	_	-	_				_
		jeursor pos =	- 0, log	sec =										-			1	-
Listed: 0 Selected: 0 case1001.001	_		_	_	_	_	_	_		_	_	_	_					11



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



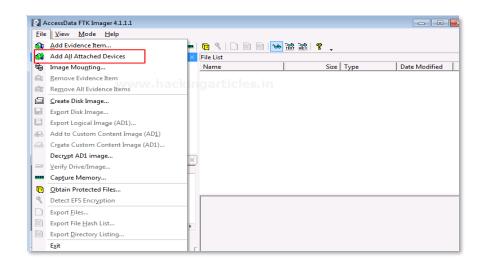


# **Mounting Image to Drive**

()

### **Mounting Image To Drive**

To mount the image as a drive in your system, click on File > Image Mounting

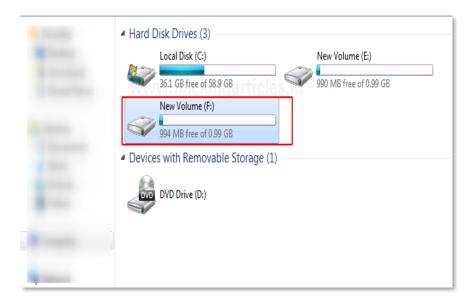


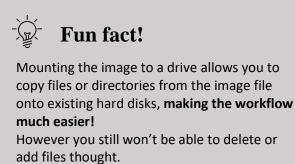
Once the Mount Image to Drive window appears, you can add the path to the image file that you want to mount and click on Mount.

lount Image T	o Drive			<b>—</b> ×
Add Image	j\Desktop\For Img\case	1001.001		
Drive Le	ype: Physical & Logical tter: Next Available (F: hod: Block Device / Rea	-	<b>.</b> ↓ ticles.in	
C:\Users\ra	j\Desktop\For Img			Mount
-Mapped Imag Mapped Imag				
Drive	Method	Partition	Image	
_				
•				•
				Unmount
				Close



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







### Custom Content Image with AD Encryption

#### **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.

<u>F</u> ile <u>V</u> iew <u>M</u> ode	<u>H</u> elp				
🏨 🚳 🗣 🚔 🚘	88	🛛 🚛 💷 🚥 📘 📴	9 🗋 🗎		-
vidence Tree	×	File List			
	api 🔺	Name	Size	Туре	Date Modified
	api	SAM	256	Regular File	10/5/2020 7:06:
	api	SAM.LOG	1	Regular File	11/21/2010 7:2
	api api	SAM.LOG1	25	Regular File	10/5/2020 7:06:
	api	SAM.LOG1.FileSlack	3	File Slack	
	api	SAM.LOG2	0	Regular File	7/14/2009 2:34:
	api	SE Export Files	200	<u> </u>	10/5/2020 7:16:
tr	api			ile	11/21/2010 7:2
	api	SE E Export File <u>H</u> ash I	List	ile	10/5/2020 7:16:
	api		Content Image (AD		7/14/2009 2:34:
	api≡	X SECOND-ILCO	20,500	JEO IN VER Entry	10/5/2020 7 25
	api		39,680	Regular File	10/5/2020 7:35:
	api api	SOFTWARE.LOG	1	Regular File	11/21/2010 7:2
	api	SOFTWARE.LOGI	256 3.072	Regular File File Slack	10/5/2020 7:35:
	ar-	SOFTWARE.LOG1.FileS	5,072	Regular File	7/14/2009 2:34:
	bg-		0	Regular The	7/14/2003 2:34

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

<u>F</u> ile <u>V</u> iew <u>M</u> ode <u>H</u> elp
🕼 🏟 😂 🚔 🖾 🔚 🖬 🗸 🚑 🛥 🖘 🔜 🗎 🗎 🔤 🐱 😹
Custom Content Sources
Evidence:File System  Path  File Options
C:\:NONAME [NTFS] [[root]  Windows Syst Exact
C:\:NONAME [NTFS] [[root]  Windows Syst Exact
www.hackingarticles.in
New Edit Remove All Create Image



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

vidence Item Informat	ion 🧾
Case Number:	1001 Custome Image
Evidence Number:	
Unique Description:	h <del>ackingarticles.in</del> _
Examiner:	Vishva
Notes:	
	< Back Next > Cancel Help

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)	rowse
<sup>custom</sup> www.hackingarticles.in	
Image Fragment Size (MB) For Raw, E01, and AFF formats: 0 = do not fragment	
Compression (0=None, 1=Fastest,, 9=Smallest)  6	-
Use AD Encryption 🔽	
Filter by File Owner 🕅	
< Back Finish Cancel	Help



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:     ***     S.IN
Re-enter: Show password
C Certificate (.pfx, .p12, .pem)
Browse
OK Cancel

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

<b>Q</b> A	AccessData FTK Imager 4.1.1.1					
<u>F</u> ile	<u>V</u> iew <u>M</u> ode <u>H</u> elp					
	<u>A</u> dd Evidence Item	🛄 🔂 😽 🗀 🗎 🖬 🔂 🙀				
	Add All Attached Devices					
6	Image Mou <u>n</u> ting					
4	Remove Evidence Item	ticles.in				
â	Re <u>m</u> ove All Evidence Items					
a	<u>C</u> reate Disk Image					
	Export Disk Image					
6	Export Logical Image (AD1)					
æ	Add to Custom Content Image (AD <u>1</u> )					
a	Cr <u>e</u> ate Custom Content Image (AD1)					
	Decrypt AD1 image					
-	Verify Drive/Image	Size Type				



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

Select	t 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
	***
-	C Certificate (.pfx, .p12, .pem)
	Browse
	OK Cancel

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

<u>F</u> ile <u>V</u> iew <u>M</u> ode <u>H</u> elp							
🏩 🏩 🗣 🚔 🖆 🖬 🖬 🚛		a 🤉 🗖	🖹 🗟 <mark>२</mark> 😹	9. <del>30</del>	<b>?</b>		
Custom Content Sources	nacking				• •		
Evidence:File System Path File	Options	CITCION					
New Edit Remove Remove All Create	Image						
Evidence Tree X	File List						
⊡ <mark>©a</mark> custom.ad1	Name		Siz	ze T	уре	Date Modified	
⊡[ Custom Content Image([Multi]) [AD ⊡⊡ C:\:NONAME [NTFS]	JAIVI				egular File	10/5/2020 7:06:	
	SECURITY		25	56 R	egular File	10/5/2020 7:16:	
🖻 🛅 Windows		,					
⊡ <mark>⊡</mark> System32							



## Decrypt ADI Image

()

### **Decrypt AD1 Image**

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

<b>A</b>	ccessData FTK Imager 4.1.1.1					
<u>F</u> ile	<u>V</u> iew <u>M</u> ode <u>H</u> elp	_				
	Add Evidence Item	••   🖸 🔍   🗋	🖹 🖻  🐱		12 <b>?</b> .	
6	Add All Attached Devices					
6	Image Mounting	icles.in				
4	<u>R</u> emove Evidence Item					
-	Remove All Evidence Items					
	<u>C</u> reate Disk Image					
	Export Disk Image					
	Export Logical Image (AD1)					
42	Add to Custom Content Image (AD <u>1</u> )					
æ	Create Custom Content Image (AD1)					
	Decrypt AD1 image			Size	Туре	Date Modifi
-	Verify Drive/Image			256	Regular File	10/5/2020 7
-	Cap <u>t</u> ure Memory	ЯΤY		256	Regular File	10/5/2020 7
	Obtain Protected Files	a a seti a la				
8	Detect EFS Encryption	igarticie				
	Export <u>F</u> iles					
	Export File <u>H</u> ash List					
DIR	Export Directory Listing					
	Exit					
< _	4 III					

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

<u>F</u> ile <u>V</u> iew	<u>M</u> ode <u>H</u> elp
🔒 🚳 🗣 🖉	à 🚖   🕞 🖃 🚍 🚙 🛥 🚥   📴 🔍   🗋 🗎 🕮
Custom Conten	t Sources
Evidence:File Sys	stem  Path  File Options
	cryption Credentials
@ Pa	** Show password
New O Ce	rtificate (.pfx, .p12, .pem) Browse
	OK Cancel



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

AD Encry	ption/Decryption	×	
Finished			
From:	C:\Users\raj\Desktop\For Img\custom.ad1		
то:	To: C:\Users\raj\Desktop\For Img\custom-decrypted.ad1		
_			
	OK Canc	el	

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

Select	File	×
[	Evidence Source Selection Please enter the source path:	
	C:\Users\raj\Desktop\For Img\custom-decrypted.ad1 Browse	
	browse	
		_
	< Back Finish Cancel Help	



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

<u>F</u> ile <u>V</u> iew <u>M</u> ode <u>H</u> elp					
🏨 🏟 🗣 🚔 🖆 🖬 🖬 🗸	a = 📖 📴	9 🥄 🗋 🗉	🗎 🖻 🛛 🐱 😹	R .	
Custom Content Sources					
Evidence:File System  Path  File	Options				
New Edit Remove Remove All Create	: Image				
Evidence Tree ×	File List				
⊡😋 custom-decrypted.ad1	Name		Size	e Type	Date Modified
E Custom Content Image([Multi]) [AD	SAM		250		10/5/2020 7:06:
i⊡ inonAME [NTFS]	SECURITY		250	5 Regular File	10/5/2020 7:16:
iroot i [iroot]					
⊡ ⊡ System32					
iiii config					



### **Obtain Protected Files**

)

()



#### **Obtain Protected Files**

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

<u>F</u> ile	<u>V</u> iew <u>M</u> ode <u>H</u> elp	_
ŝ	Add Evidence Item	媥 🔁 🥄 🗋 📄 📾  🏍 😹 🤗
<b>G</b>	Add All Attached Devices	ticlos in
9	Image Mou <u>n</u> ting	
â	Remove Evidence Item	
<b>e</b> t	Re <u>m</u> ove All Evidence Items	
	<u>C</u> reate Disk Image	
	Export Disk Image	
E	Export Logical Image (AD1)	
j,	Add to Custom Content Image (AD <u>1</u> )	
a.	Cr <u>e</u> ate Custom Content Image (AD1)	
	Decrypt AD1 image	
_	Verify Drive/Image	
	Cap <u>t</u> ure Memory	articles.in
D	Obtain Protected Files	1
٩	Detect EFS Encryption	
	Export <u>F</u> iles	
	Export File <u>H</u> ash List	
<u>110</u>	Export <u>D</u> irectory Listing	
	Exit	1

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: Browse				
C:\Users\raj\Desktop\protected				
Options O Minimum files for login password recovery				
Password recovery and all registry files				
OK Cancel				



Now you will see all the protected files in one place

Name	Date modified	Туре	Siz
📔 Users	10/6/2020 1:48 AM	File folder	
default anticles in	10/6/2020 1:03 AM	File	
SAM	10/6/2020 12:36 AM	File	
SECURITY	10/6/2020 12:46 AM	File	
software	10/6/2020 1:47 AM	File	
system	10/6/2020 1:36 AM	File	



### Detect EFS Encryption

()

### **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.

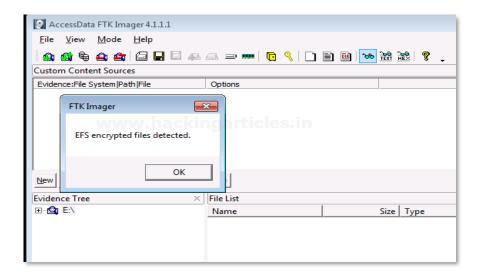
	×		
N	ame	Date modified	Туре
[	] file	10/6/2020 1:53 AM	Text Document
	Advanced Attributes		3
	Compress contents to secure data	ed in addition to file properties	
www	Modified: Ioday, October 06, 2020, Accessed: Today, October 06, 2020, Attributes: Read-only Hidde	1 minute ago	

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

<b>A</b>	ccessData FTK Imager 4.1.1.1	
<u>F</u> ile	<u>V</u> iew <u>M</u> ode <u>H</u> elp	
	Add Evidence Item	📟 🔁 🔧 🗋 🖹 📾  🐱 📆 📆 🎈 🖕
<b>1</b>	Add All Attached Devices	
6	Image Mounting	licles.in
	<u>R</u> emove Evidence Item	
-	Re <u>m</u> ove All Evidence Items	
	<u>C</u> reate Disk Image	
	Export Disk Image	
E	Export Logical Image (AD1)	
42	Add to Custom Content Image (AD <u>1</u> )	
æ	Cr <u>e</u> ate Custom Content Image (AD1)	
4	Decrypt AD1 image	Size Type D
=	Verify Drive/Image	
-	Cap <u>t</u> ure Memory	
	Obtain Protected Files	irticles.in
3	Detect EFS Encryption	
	Export <u>F</u> iles	
	Export File <u>H</u> ash List	
810	Export Directory Listing	
	Exit	
_		



You can see that the encryption is detected.





### **Export Files** E F D 0

20

#### **Export Files**

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

<b>A</b>	ccessData FTK Imager 4.1.1.1	
<u>F</u> ile	<u>V</u> iew <u>M</u> ode <u>H</u> elp	
	Add Evidence Item	📟 📴 🔧 🗋 🖹 🎯 🐱 🚟 🔡 🂡 🖕
	Add All Attached Devices	garticles in
6	Image Mou <u>n</u> ting	
	<u>R</u> emove Evidence Item	
4	Remove All Evidence Items	
0	<u>C</u> reate Disk Image	
	Export Disk Image	
	Export Logical Image (AD1)	
42	Add to Custom Content Image (AD <u>1</u> )	
æ	Create Custom Content Image (AD1)	
	Decrypt AD1 image	Size Type Date
1	Verify Drive/Image	
	Capture Memory	jarticles.in
	Obtain Protected Files	
8	Detect EFS Encryption	
	Export <u>F</u> iles	
Đ	Export File <u>H</u> ash List	
DIR	Export Directory Listing	
	Exit	]

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

AccessData FTK Imager 4.1.1.1	
<u>F</u> ile <u>V</u> iew <u>M</u> ode <u>H</u> elp	
🏩 🏩 😂 🖾 🔚 🖬 📾 🗛 🛥 🚥 📙 🎙   🗋 🗎 🔛 😿 😹 💡	
Custom Content Sources	
Eyidence:File System  Path  File	Options
Export Results	
www.hackingarticles.in	
11 folder(s) and 43 file(s) exported successfully. 1071358589 bytes copied.	
ОК	
Evidence Tree X File List	





0

#### About Us

#### "Simple training makes Deep Learning"

**"IGNITE"** is having a Worldwide name in IT field. As we provide High-quality cybersecurity training and consulting services that fulfil students, government and corporate Requirements.

We are working towards the vision to **"Develop India a Cyber Secured Country"**. With an outreach to over eighty thousand students and over a thousand major colleges, Ignite Technologies in Association with RMAR stands out to be a trusted brand in the Education and the Information Security structure.

We provide training and education in the field of Ethical Hacking & Information Security to the students from the schools and the colleges as well as the corporate. These training can be provided at the client's location or even at Ignite's Training Center.

We have trained over 10,000 + individuals across the globe, ranging from students to security experts of different colleges and organizations. Our Trainers are acknowledged as Security Researcher by the Top Companies like - Facebook, Google, Microsoft, Adobe, Nokia, Paypal, Blackberry, AT&T and many more. Over with this, they are having International Experience of training more than 400+ individuals.



### What We Offer



The Ethical Hacking course has been structured in such a way that a technical or a non-technical applicant can easily absorb its features and indulge his/her career in the field of IT security.

### 😹 Bug Bounty 2.0

A bug bounty program is a pact offered by many websites and web developers by which folks can receive appreciation and reimbursement for reporting bugs, especially those affecting to exploits and vulnerabilities.

Over with this training, an indivisual is thus able to determine and report bugs to the authorized before the general public is aware of them, preventing incidents of widespread abuse.



The Network Penetration Testing training will build up the basic as well advance skills of an indivisual with the concept of Network Security & Organizational Infrastructure. Thereby this course will make the indivisual stand out of the crowd within just 45 days.



This training will make you think like an "Adversary" with its systematic structure & real Environment Practice that contains more than 75 practicals on Windows Server 2016 & Windows 10. This course is especially designed for the professionals to enhance their Cyber Security Skills



The CTF 2.0 is the latest edition that provides more advance module connecting to real infrastructure organization as well as supporting other students preparing for global certification. This curriculum is very easily designed to allow a fresher or specialist to become familiar with the entire content of the course.

#### **O** Infrastructure Penetration Testing

This course is designed for Professional and provides an hands-on experience in Vulnerability Assessment Penetration Testing & Secure configuration Testing for Applications Servers, Network Deivces, Container and etc.

### Digital Forensic

Digital forensics provides a taster in the understanding of how to conduct investigations in order for business and legal audien ces to correctly gather and analyze digital evidence.