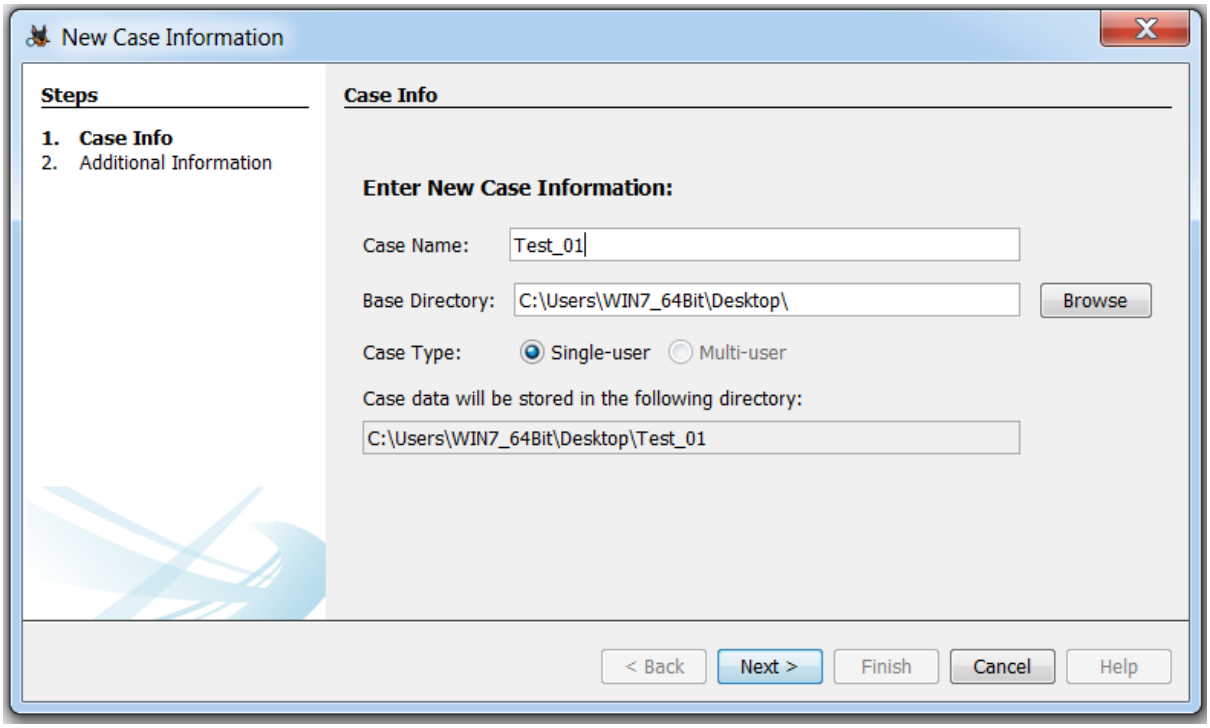
Practical 1

Aim: **File System Analysis [Autopsy]**

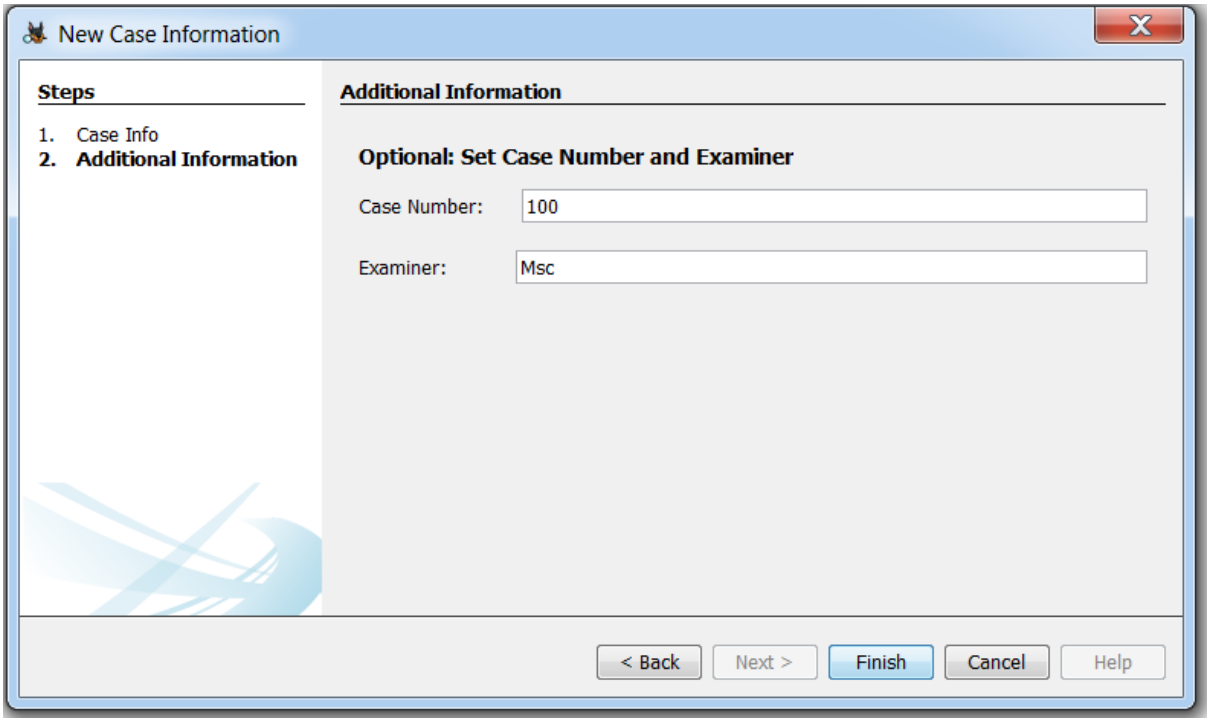
Step-1: Start Autopsy Tool

Step-2: Click Create New Case

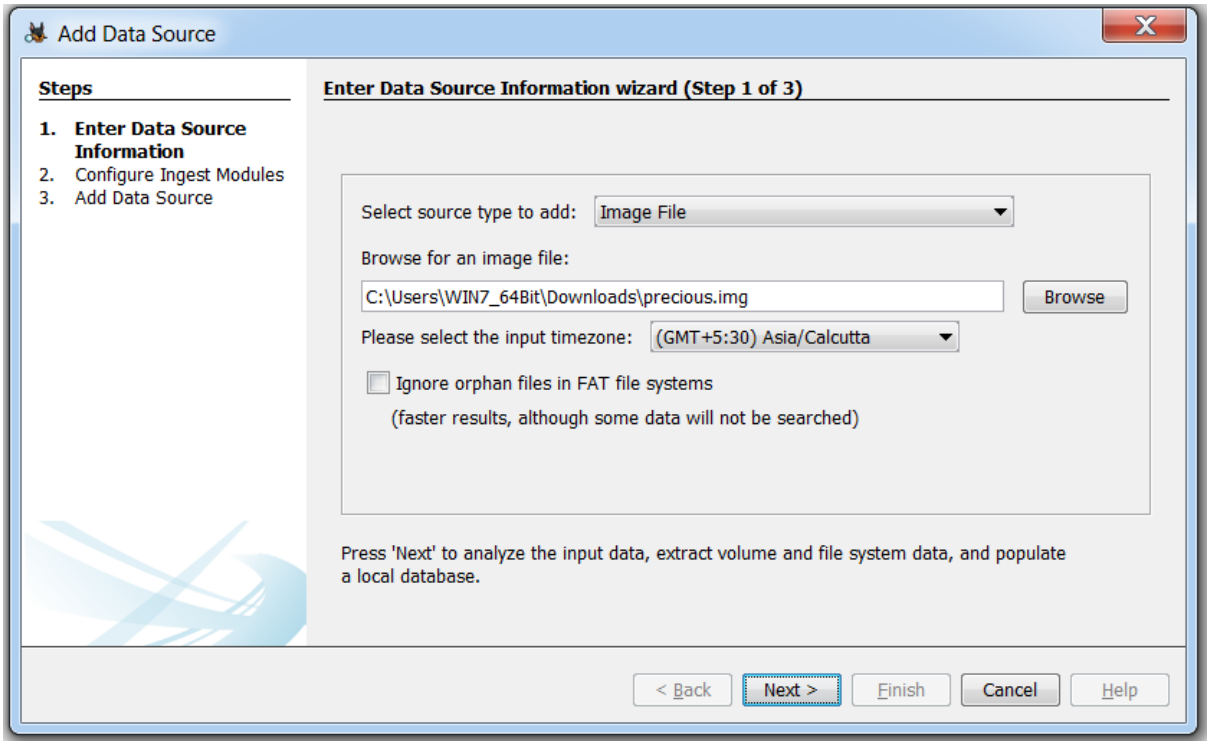
Step-3: Enter the Details.



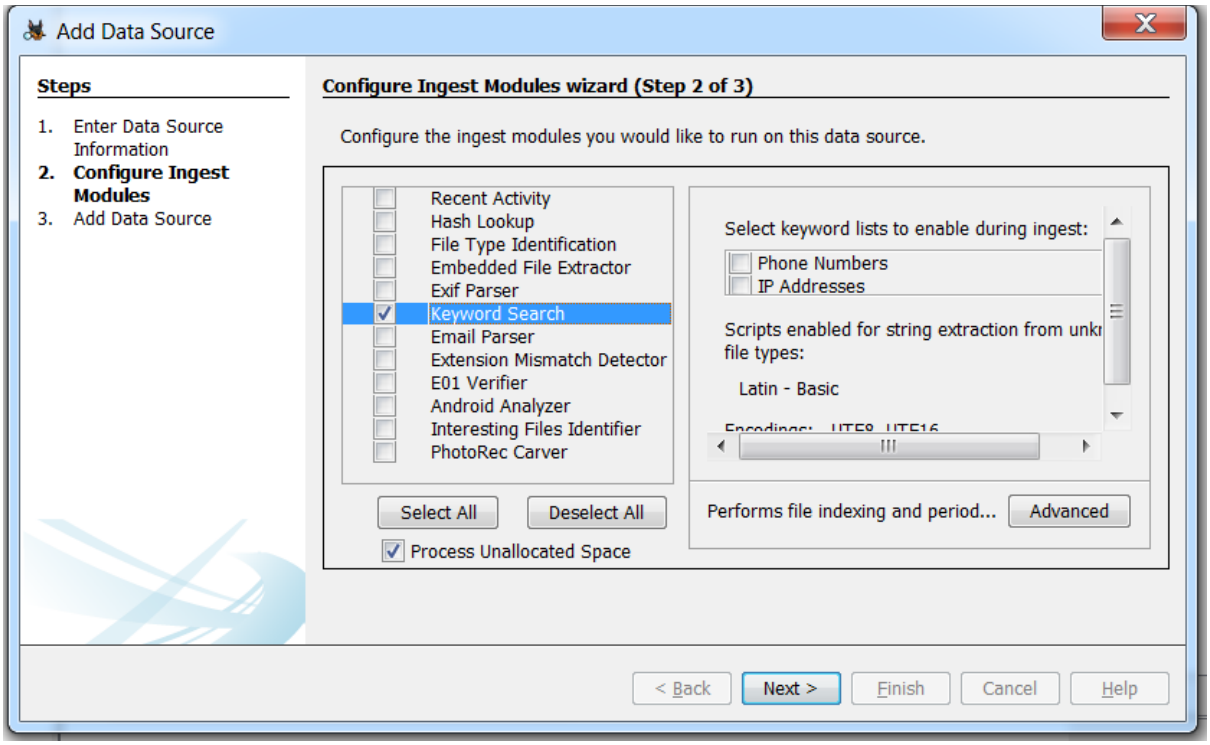
Step-4: Enter The Case Name & Case Examiner Name.

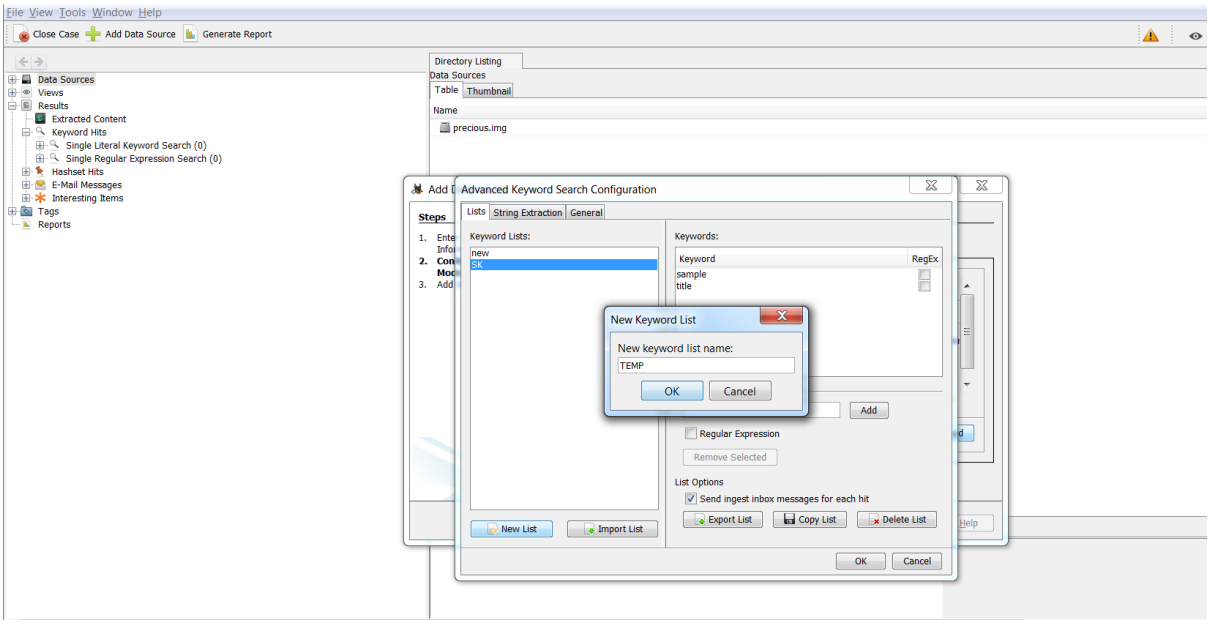


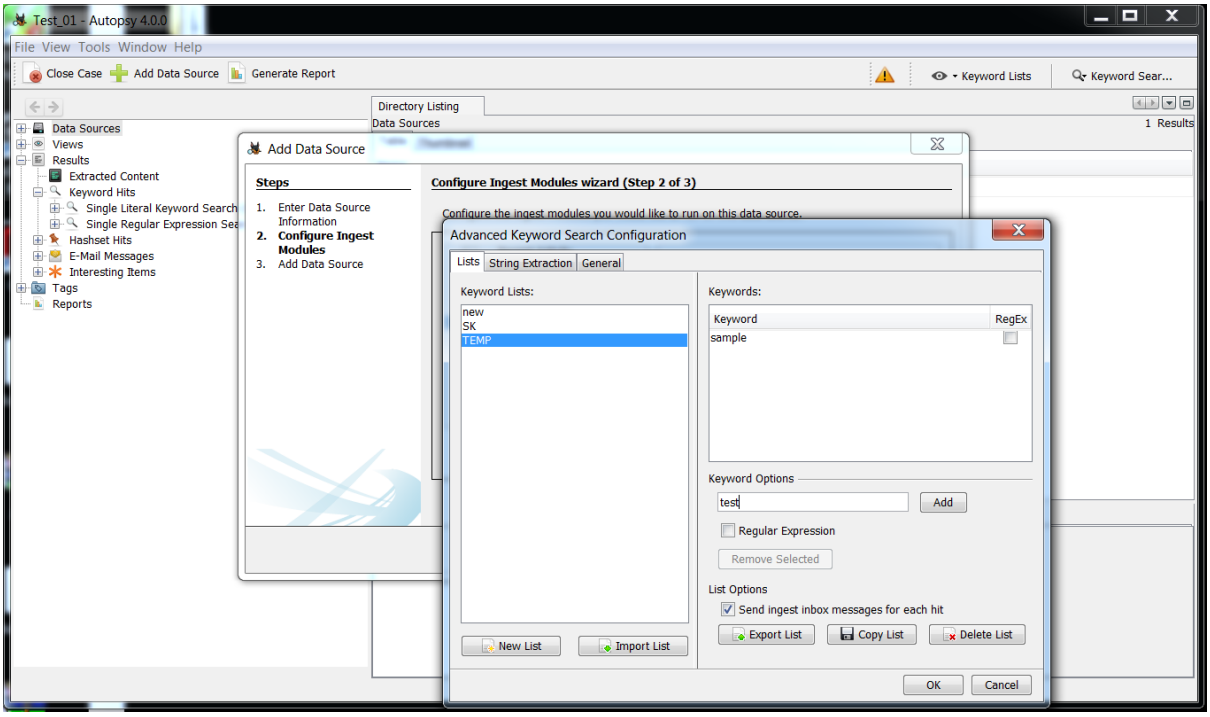
Step-5: After Clicking The Finish Button In The Above Window,
A New Window Will Open For Retrieving The Datasource, Select Disk Image or VM File Then Browse The .img File Present In The Directory Click Next.



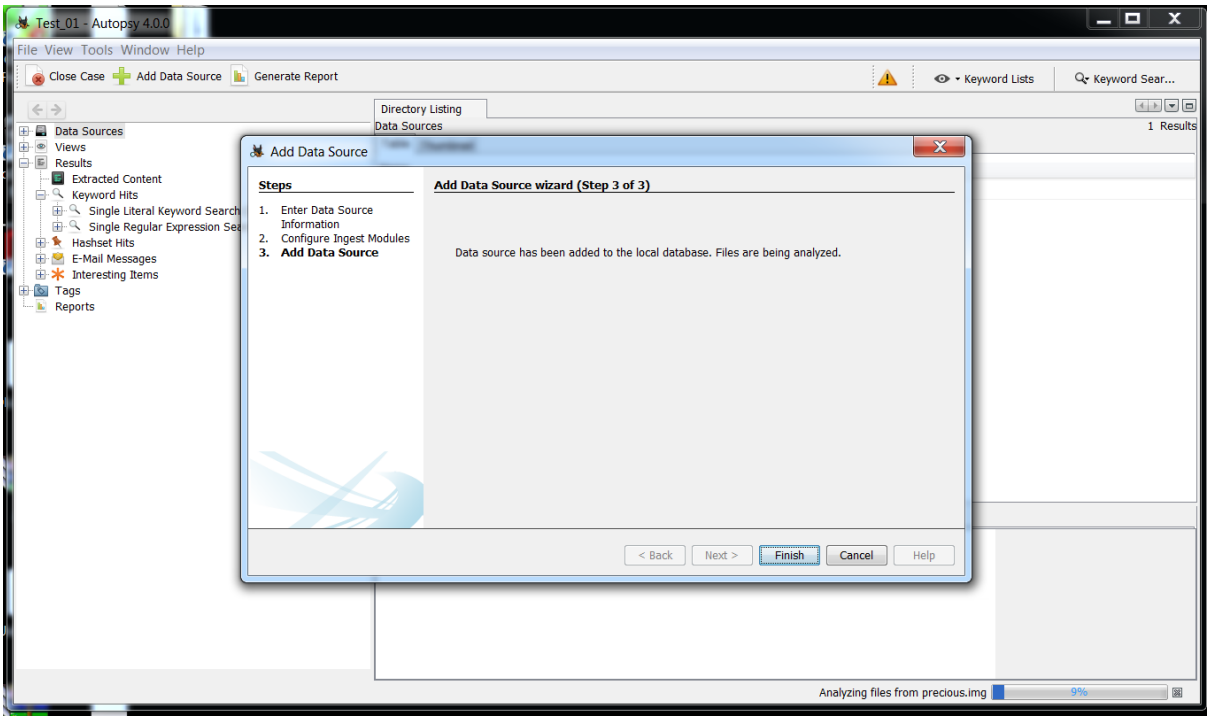
Step-6: The Next Step Provides A Ingest Wizard Panel Which Aims At Increasing The Search Capability. Select as Desired And Proceed To The Next Step.


Add Data Source
Steps
1. Enter Data Source Information
2. Configure Ingest Modules
3. Add Data Source
Configure Ingest Modules wizard (Step 2 of 3)
Configure the ingest modules you would like to run on this data source.
Recent Activity
Hash Lookup
File Type Identification
Embedded File Extractor
Exif Parser
Keyword Search
Email Parser
Extension Mismatch Detector
E01 Verifier
Android Analyzer
Interesting Files Identifier
PhotoRec Carver
Select keyword lists to enable during ingest:
Phone Numbers
IP Addresses
Scripts enabled for string extraction from unkr
file types:
Latin - Basic
Select All
Deselect All
Process Unallocated Space
Performs file indexing and period...
Advanced
< Back
Next >
Finish
Cancel
Help

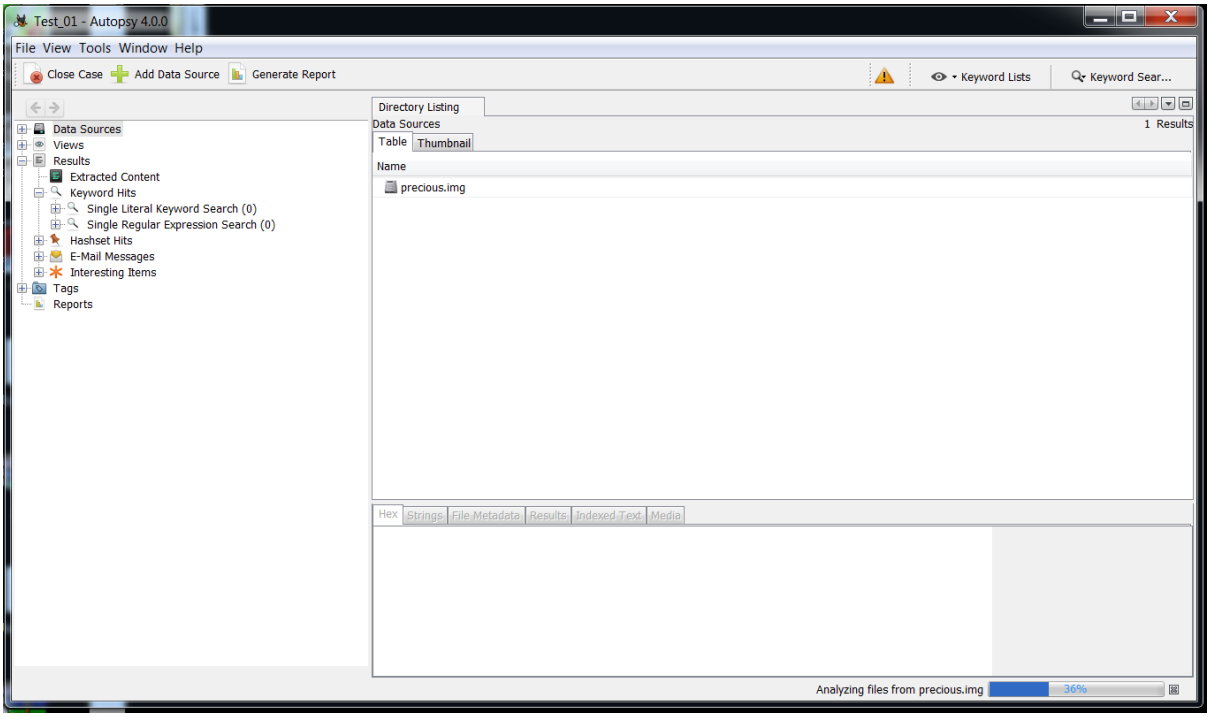

File View Tools Window Help
Close Case
Add Data Source
Generate Report
Data Sources
Views
Results
Extracted Content
Keyword Hits
Single Literal Keyword Search (0)
Single Regular Expression Search (0)
Hashset Hits
E-Mail Messages
Interesting Items
Tags
Reports
Directory Listing
Data Sources
Table
Thumbnail
Name
precious.img
Advanced Keyword Search Configuration
Lists
String Extraction
General
Keyword Lists:
new
SK
Keywords:
Keyword
RegEx
sample
title
New Keyword List
New keyword list name:
TEMP
OK
Cancel
Add
Regular Expression
Remove Selected
List Options
Send ingest inbox messages for each hit
New List
Import List
Export List
Copy List
Delete List
OK
Cancel

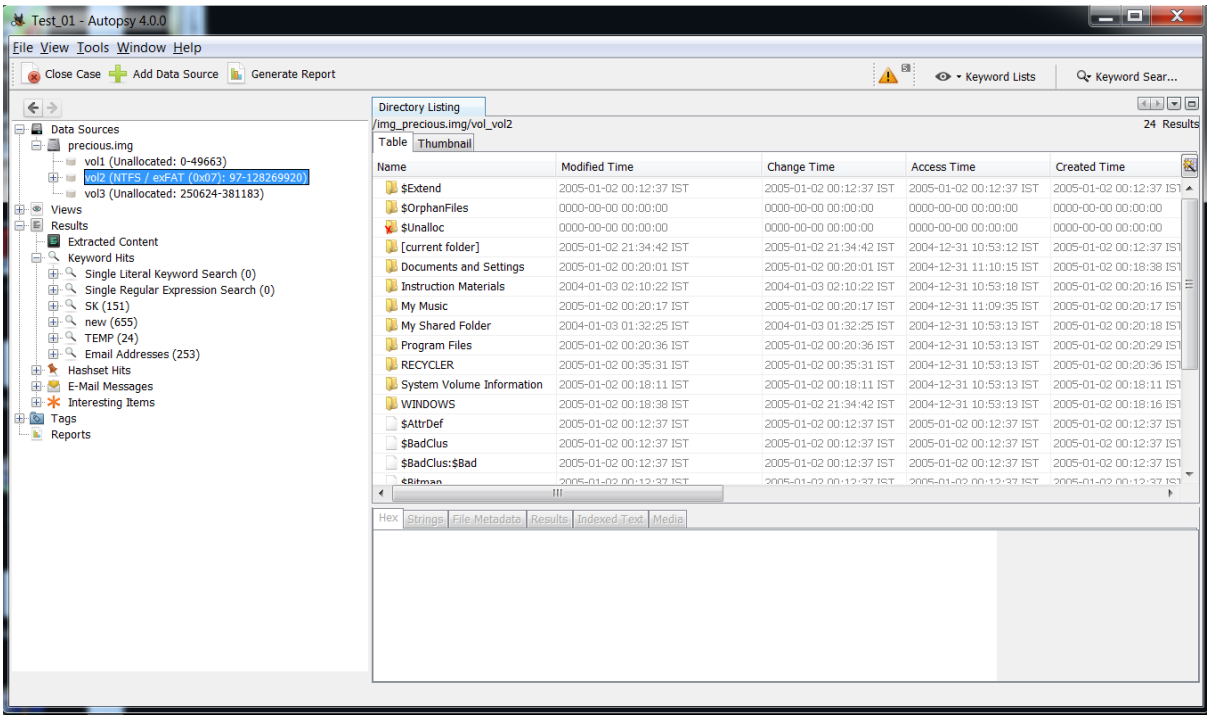


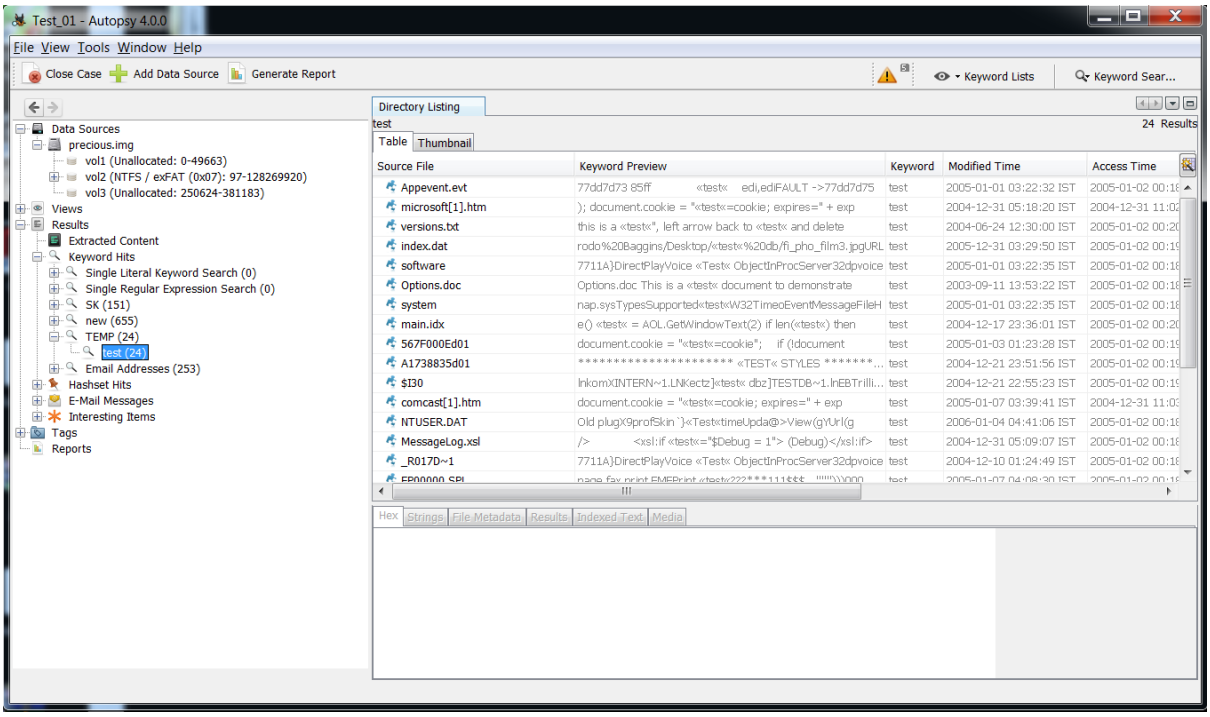
Step-7: In the Resulting Window, You'll Be Notified That The Files Are Being Analysed. Proceed to Finish.

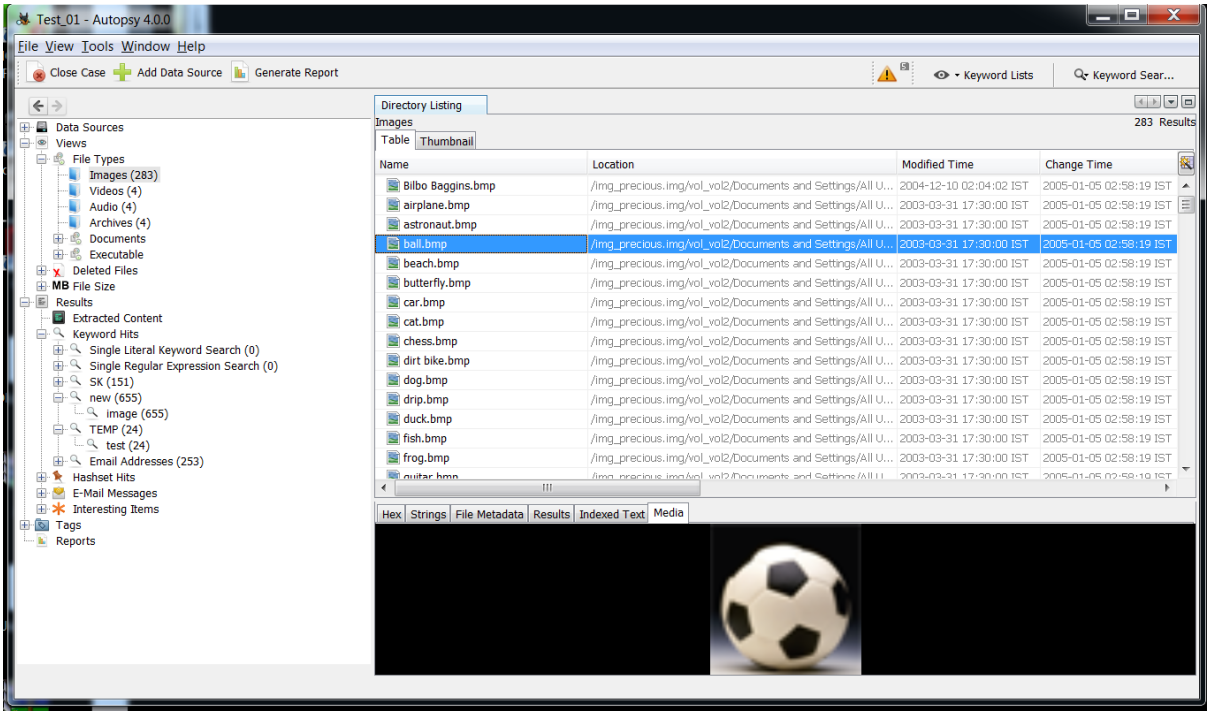


Step-8: After The Image Is Indexed The Tree Will Be Populated By The File System, Extracted Content, Keyword Searches, And The Hash List (If Any Were Used). This Tree Can Be To Retrieve The Information About The Image File Under Observation

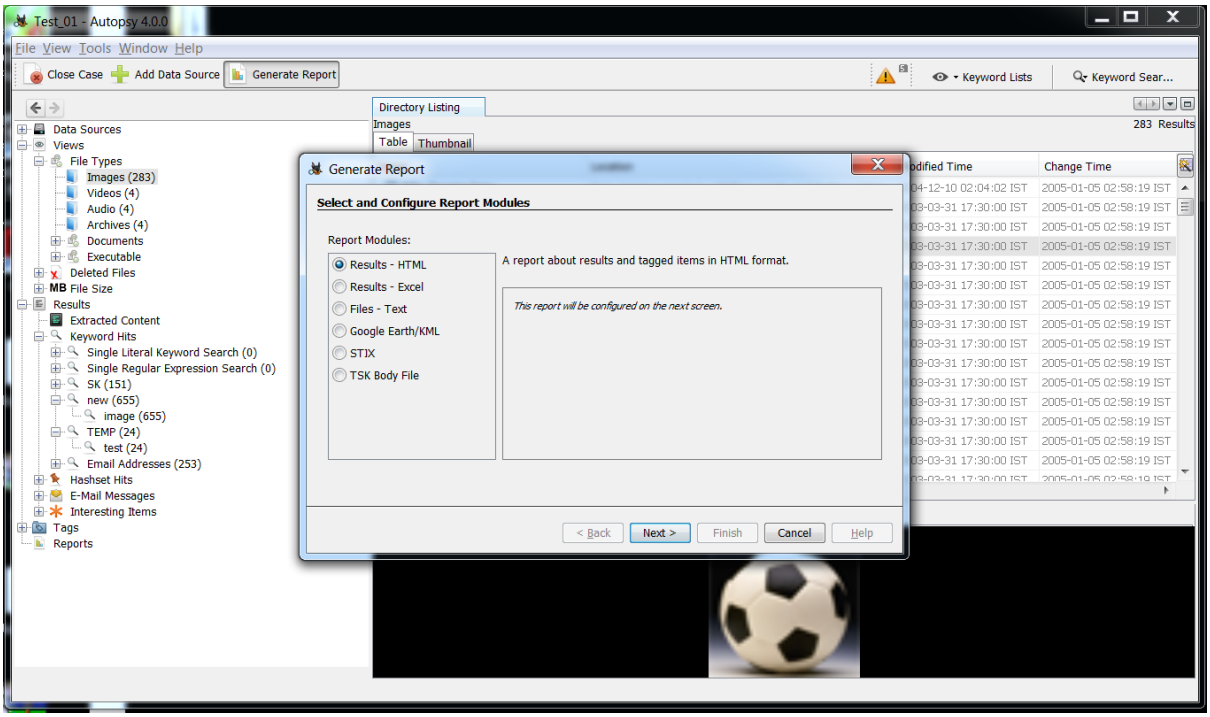


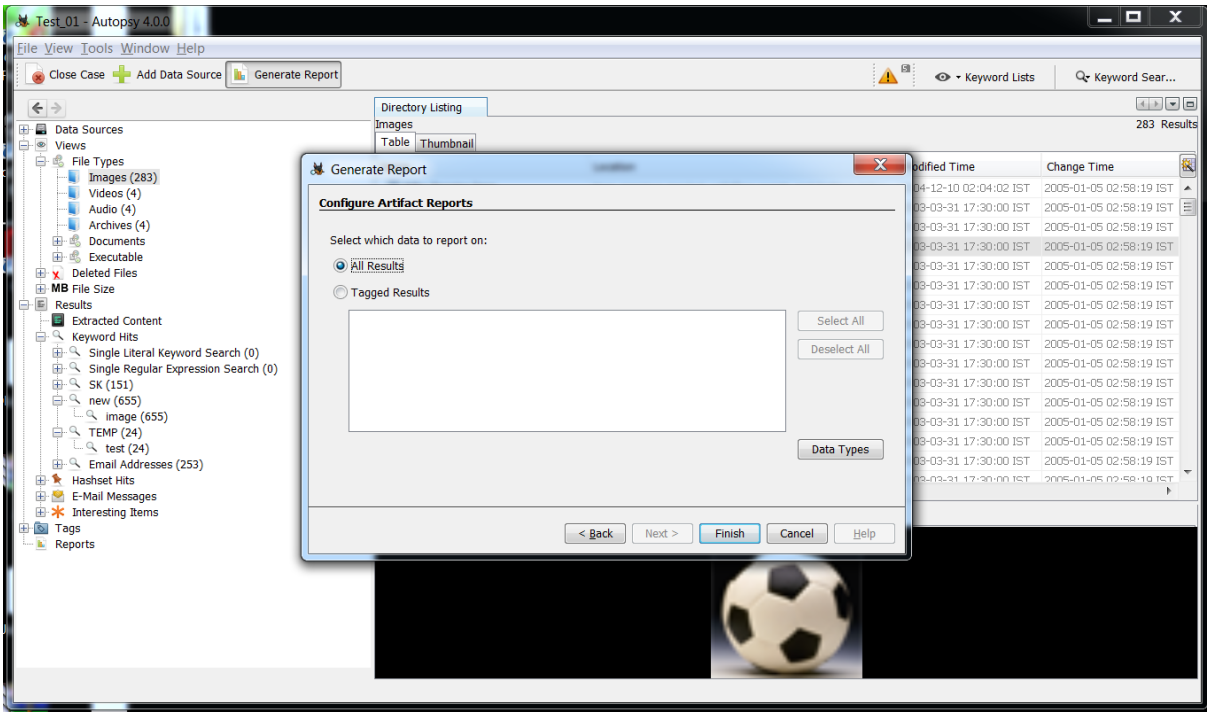


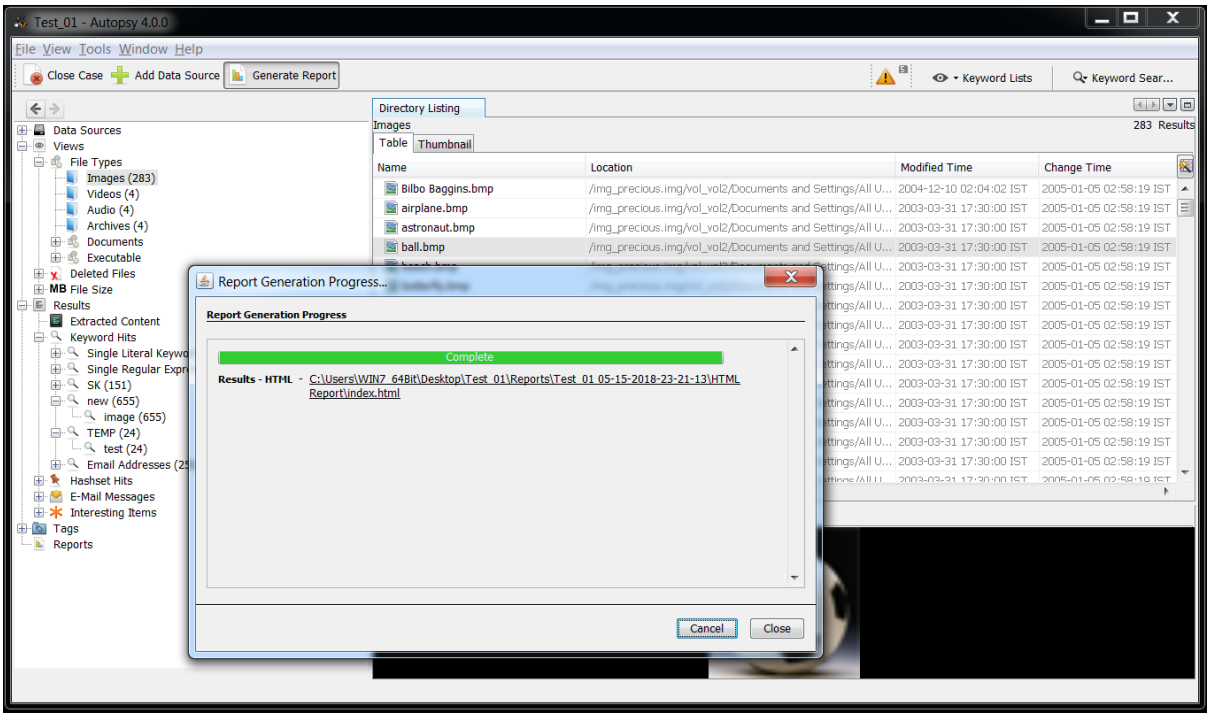


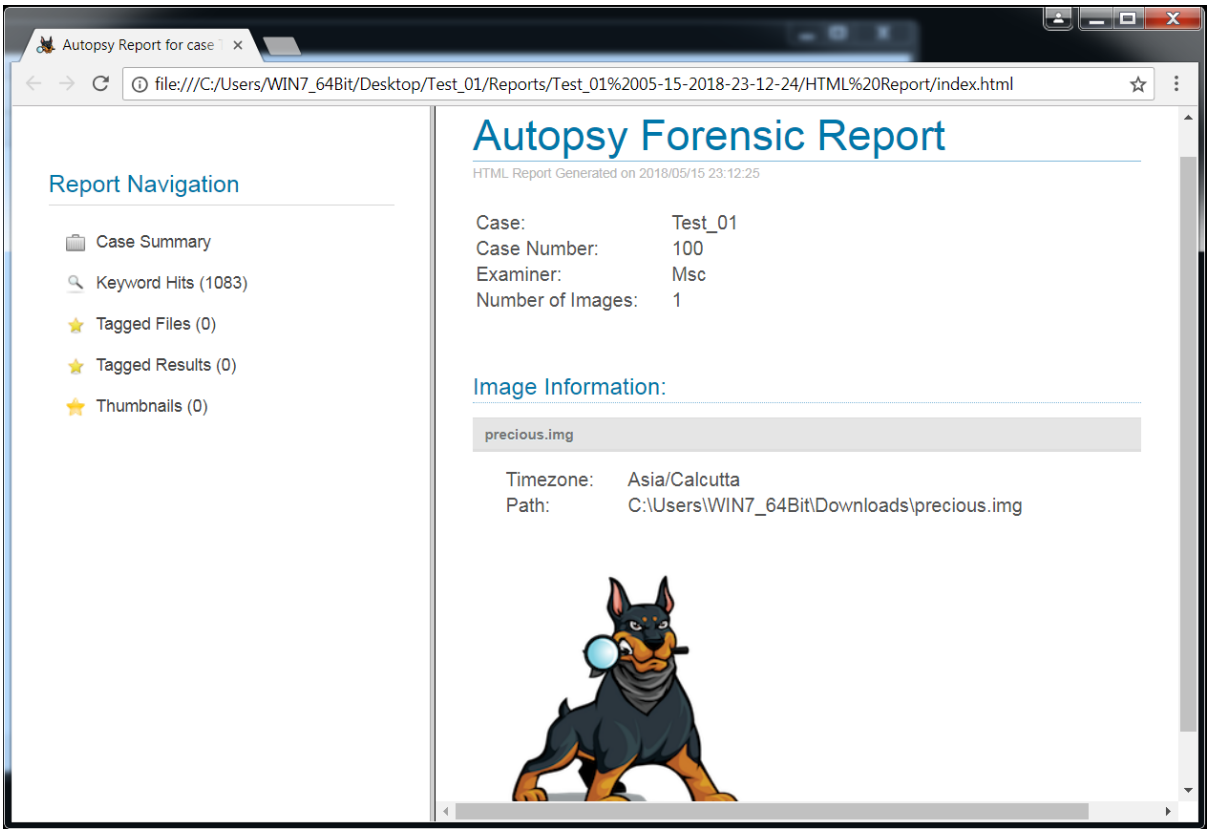


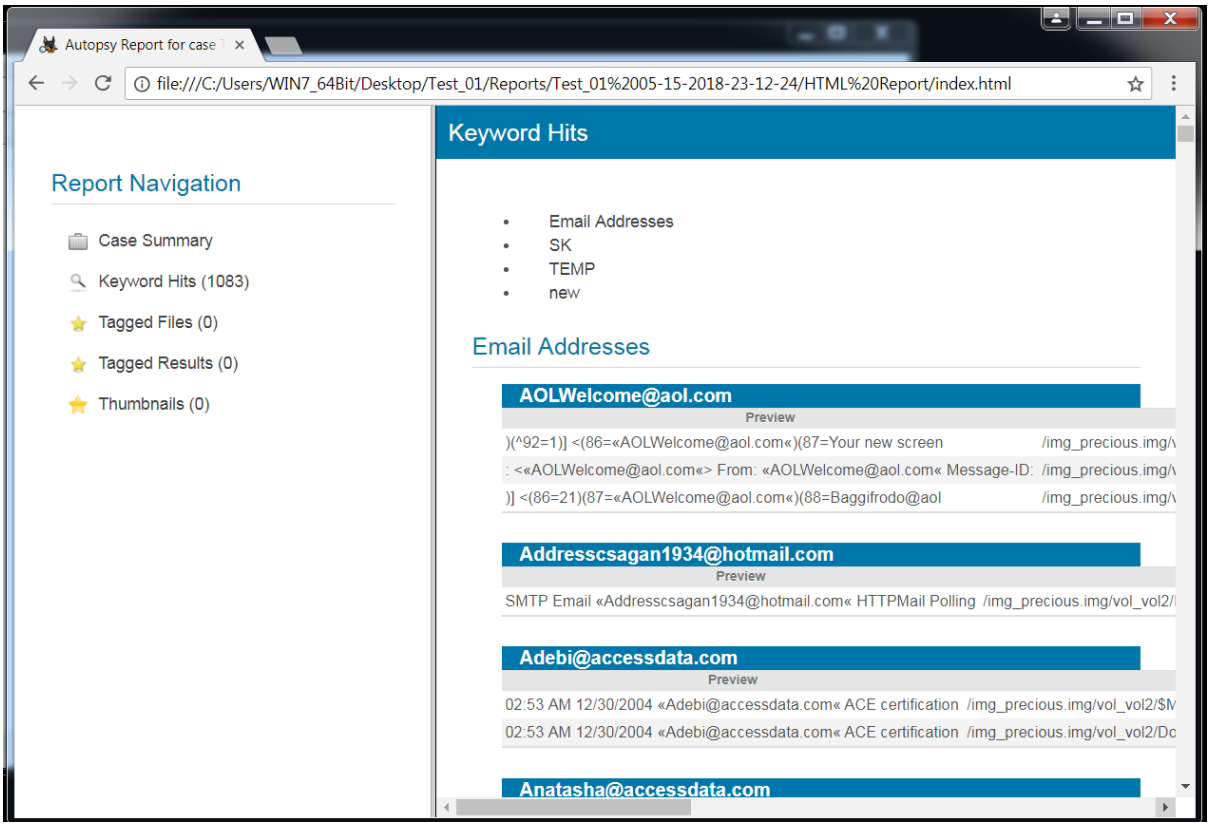
STEP 9: Generate Report in the appropriate format.

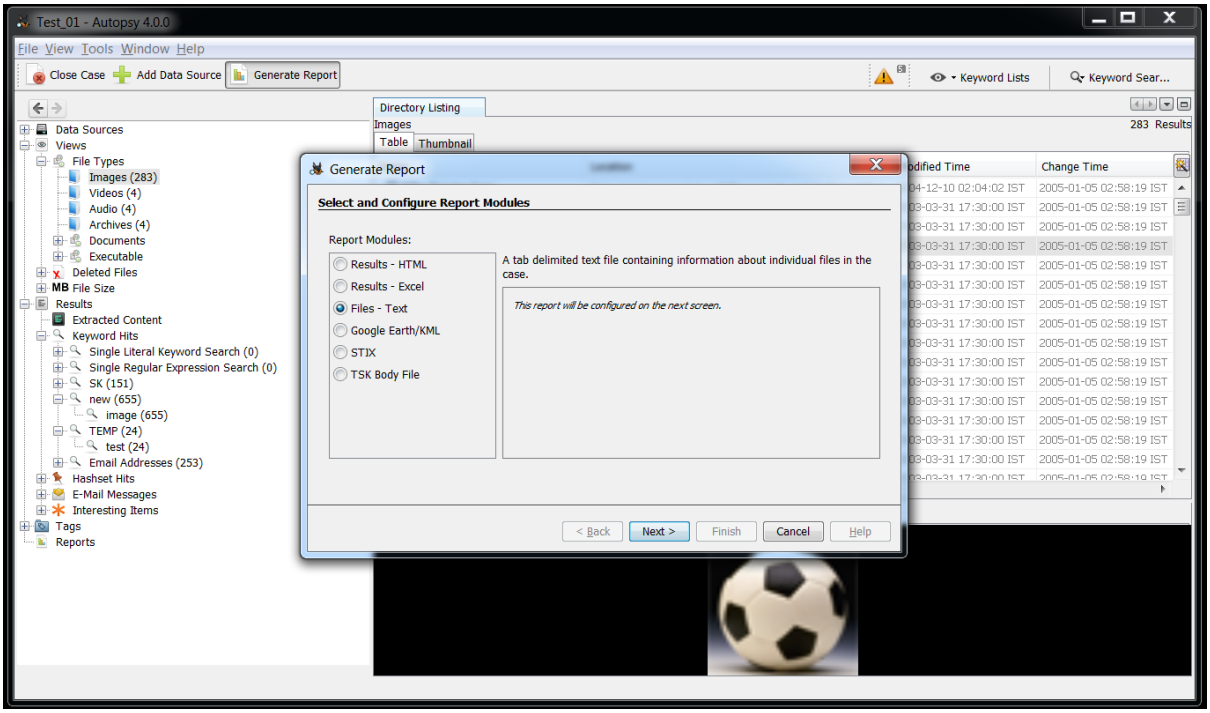

Test_01 - Autopsy 4.0.0
File View Tools Window Help
Close Case
Add Data Source
Generate Report
Keyword Lists
Keyword Sear...
Directory Listing
Images
283 Results
Table
Thumbnail
Data Sources
Views
File Types
Images (283)
Videos (4)
Audio (4)
Archives (4)
Documents
Executable
Deleted Files
MB File Size
Results
Extracted Content
Keyword Hits
Single Literal Keyword Search (0)
Single Regular Expression Search (0)
SK (151)
new (655)
image (655)
TEMP (24)
test (24)
Email Addresses (253)
Hashset Hits
E-Mail Messages
Interesting Items
Tags
Reports
Generate Report
Select and Configure Report Modules
Report Modules:
Results - HTML
Results - Excel
Files - Text
Google Earth/KML
STIX
TSK Body File
A report about results and tagged items in HTML format.
This report will be configured on the next screen.
< Back
Next >
Finish
Cancel
Help
Change Time

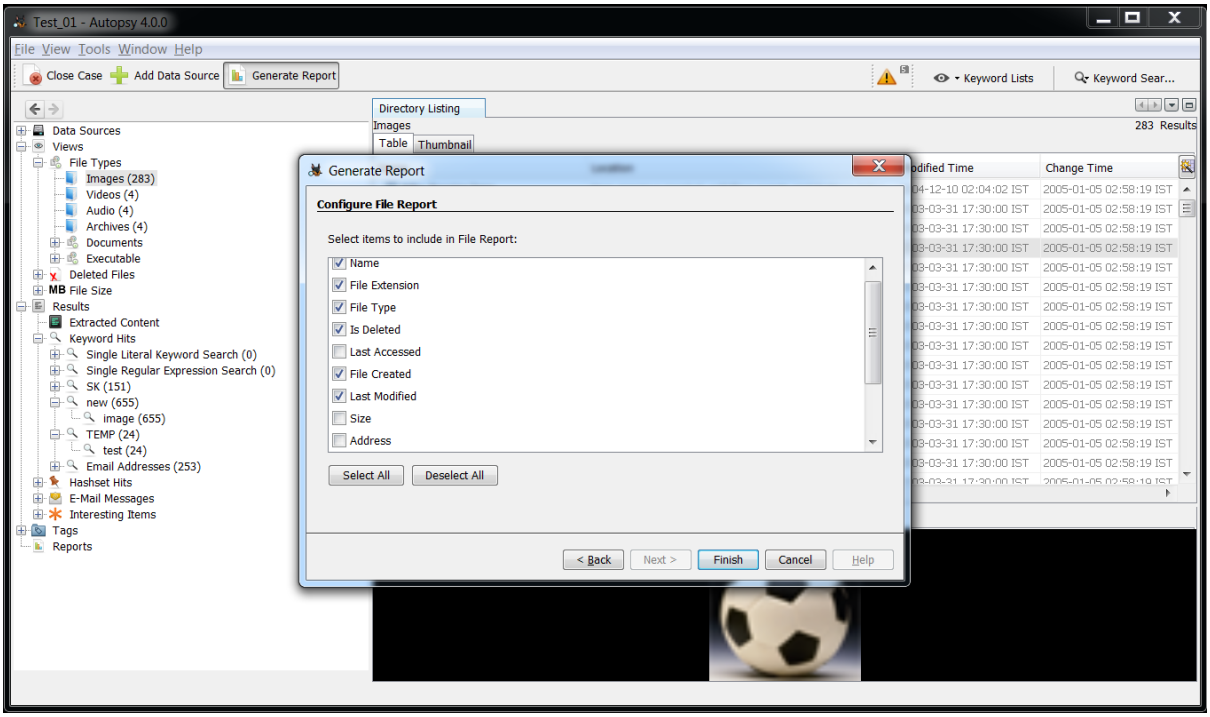

Test_01 - Autopsy 4.0.0
File View Tools Window Help
Close Case
Add Data Source
Generate Report
Keyword Lists
Keyword Sear...
Directory Listing
Images
283 Results
Table
Thumbnail
Data Sources
Views
File Types
Images (283)
Videos (4)
Audio (4)
Archives (4)
Documents
Executable
Deleted Files
MB File Size
Results
Extracted Content
Keyword Hits
Single Literal Keyword Search (0)
Single Regular Expression Search (0)
SK (151)
new (655)
image (655)
TEMP (24)
test (24)
Email Addresses (253)
Hashset Hits
E-Mail Messages
Interesting Items
Tags
Reports
Generate Report
Configure Artifact Reports
Select which data to report on:
All Results
Tagged Results
Select All
Deselect All
Data Types
< Back
Next >
Finish
Cancel
Help
Change Time

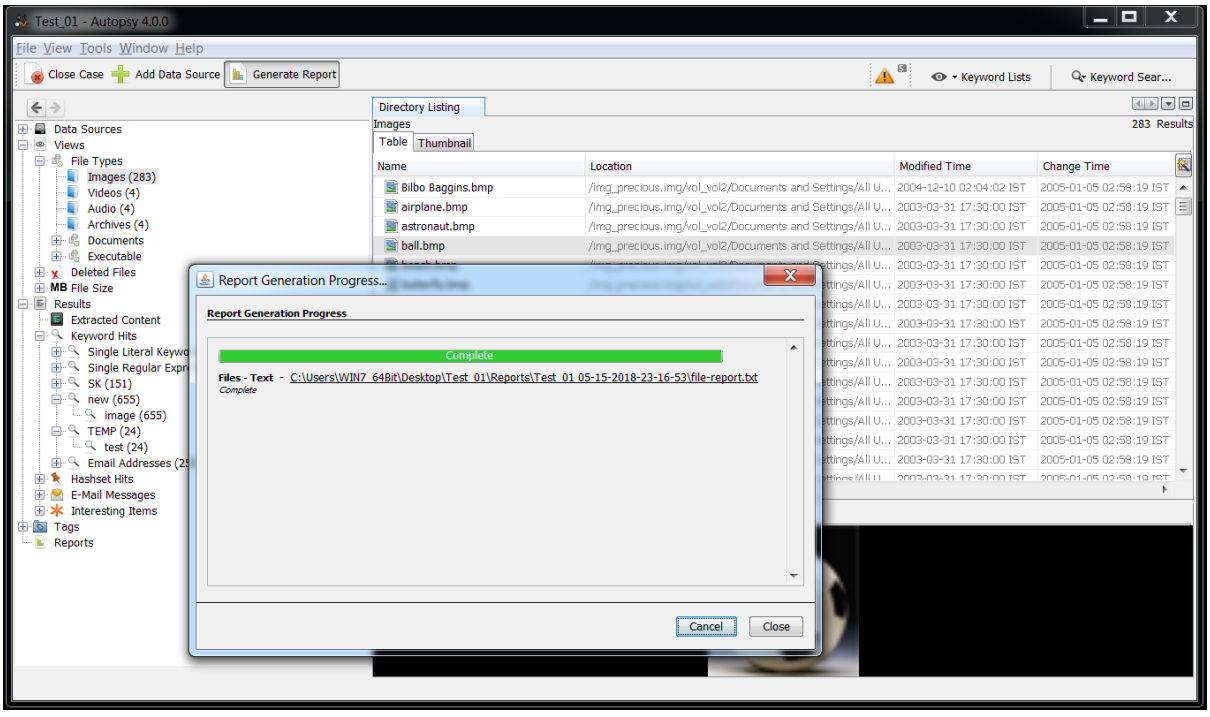

Test_01 - Autopsy 4.0.0
File View Tools Window Help
Close Case
Add Data Source
Generate Report
Keyword Lists
Keyword Sear...
Directory Listing
Images
283 Results
Table
Thumbnail
Name
Location
Modified Time
Change Time
Bilbo Baggins.bmp
airplane.bmp
astronaut.bmp
ball.bmp
Report Generation Progress...
Report Generation Progress
Complete
Results - HTML - C:\Users\WIN7_64Bit\Desktop\Test_01\Reports\Test_01 05-15-2018-23-21-13\HTML Report\index.html
Cancel
Close

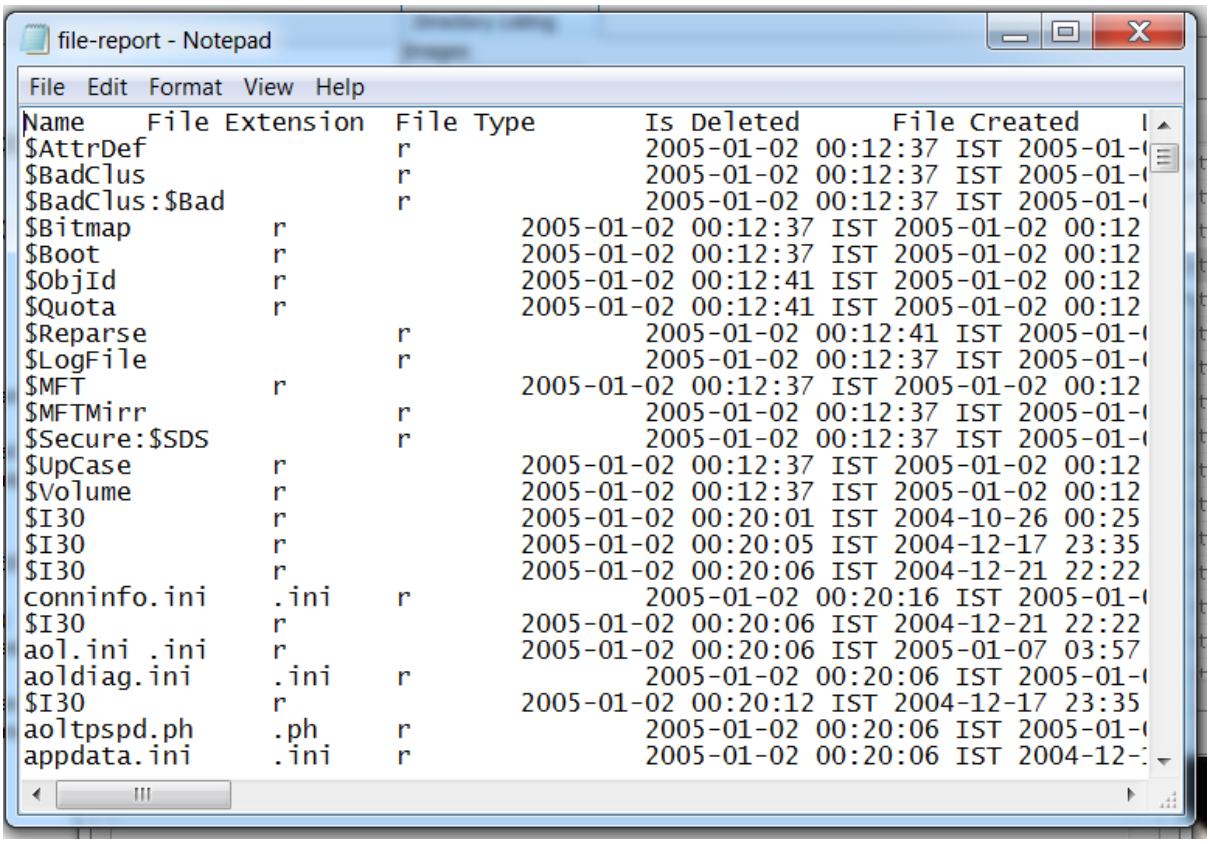

Autopsy Report for case
file:///C:/Users/WIN7_64Bit/Desktop/Test_01/Reports/Test_01%2005-15-2018-23-12-24/HTML%20Report/index.html
Report Navigation
Case Summary
Keyword Hits (1083)
Tagged Files (0)
Tagged Results (0)
Thumbnails (0)
Autopsy Forensic Report
HTML Report Generated on 2018/05/15 23:12:25
Case: Test_01
Case Number: 100
Examiner: Msc
Number of Images: 1
Image Information:
precious.img
Timezone: Asia/Calcutta
Path: C:\Users\WIN7_64Bit\Downloads\precious.img


Autopsy Report for case
file:///C:/Users/WIN7_64Bit/Desktop/Test_01/Reports/Test_01%2005-15-2018-23-12-24/HTML%20Report/index.html
Report Navigation
Case Summary
Keyword Hits (1083)
Tagged Files (0)
Tagged Results (0)
Thumbnails (0)
Keyword Hits
Email Addresses
SK
TEMP
new
Email Addresses
AOLWelcome@aol.com
Preview
)(^92=1)] <(86=«AOLWelcome@aol.com«)(87=Your new screen /img_precious.img/
: <«AOLWelcome@aol.com«> From: «AOLWelcome@aol.com« Message-ID: /img_precious.img/
)] <(86=21)(87=«AOLWelcome@aol.com«)(88=Baggifrodo@aol /img_precious.img/
Addresscsagan1934@hotmail.com
Preview
SMTP Email «Addresscsagan1934@hotmail.com« HTTPMail Polling /img_precious.img/vol_vol2/
Adebi@accessdata.com
Preview
02:53 AM 12/30/2004 «Adebi@accessdata.com« ACE certification /img_precious.img/vol_vol2/$M
02:53 AM 12/30/2004 «Adebi@accessdata.com« ACE certification /img_precious.img/vol_vol2/Dc
Anatasha@accessdata.com


Test_01 - Autopsy 4.0.0
File View Tools Window Help
Close Case
Add Data Source
Generate Report
Keyword Lists
Keyword Sear...
Directory Listing
Images
283 Results
Table
Thumbnail
Data Sources
Views
File Types
Images (283)
Videos (4)
Audio (4)
Archives (4)
Documents
Executable
Deleted Files
MB File Size
Results
Extracted Content
Keyword Hits
Single Literal Keyword Search (0)
Single Regular Expression Search (0)
SK (151)
new (655)
image (655)
TEMP (24)
test (24)
Email Addresses (253)
Hashset Hits
E-Mail Messages
Interesting Items
Tags
Reports
Generate Report
Select and Configure Report Modules
Report Modules:
Results - HTML
Results - Excel
Files - Text
Google Earth/KML
STIX
TSK Body File
A tab delimited text file containing information about individual files in the case.
This report will be configured on the next screen.
< Back
Next >
Finish
Cancel
Help
Modified Time
Change Time


Test_01 - Autopsy 4.0.0
File View Tools Window Help
Close Case
Add Data Source
Generate Report
Keyword Lists
Keyword Sear...
Directory Listing
Images
283 Results
Table
Thumbnail
Data Sources
Views
File Types
Images (283)
Videos (4)
Audio (4)
Archives (4)
Documents
Executable
Deleted Files
File Size
Results
Extracted Content
Keyword Hits
Single Literal Keyword Search (0)
Single Regular Expression Search (0)
SK (151)
new (655)
image (655)
TEMP (24)
test (24)
Email Addresses (253)
Hashset Hits
E-Mail Messages
Interesting Items
Tags
Reports
Generate Report
Configure File Report
Select items to include in File Report:
Name
File Extension
File Type
Is Deleted
Last Accessed
File Created
Last Modified
Size
Address
Select All
Deselect All
< Back
Next >
Finish
Cancel
Help
Modified Time
Change Time


Test_01 - Autopsy 4.0.0
File View Tools Window Help
Close Case
Add Data Source
Generate Report
Keyword Lists
Keyword Sear...
Directory Listing
Images
283 Results
Table
Thumbnail
Name
Location
Modified Time
Change Time
Bilbo Baggins.bmp
airplane.bmp
astronaut.bmp
ball.bmp
Report Generation Progress...
Report Generation Progress
Complete
Files - Text - C:\Users\WIN7_64Bit\Desktop\Test_01\Reports\Test_01 05-15-2018-23-16-53\file-report.txt
Complete
Cancel
Close



file-report - Notepad

File Edit Format View Help

Name	File Extension	File Type	Is Deleted	File Created
$AttrDef		r	2005-01-02 00:12:37 IST	2005-01-
$BadClus		r	2005-01-02 00:12:37 IST	2005-01-
$BadClus:$Bad		r	2005-01-02 00:12:37 IST	2005-01-
$Bitmap		r	2005-01-02 00:12:37 IST	2005-01-02 00:12
$Boot		r	2005-01-02 00:12:37 IST	2005-01-02 00:12
$ObjId		r	2005-01-02 00:12:41 IST	2005-01-02 00:12
$Quota		r	2005-01-02 00:12:41 IST	2005-01-02 00:12
$Reparse		r	2005-01-02 00:12:41 IST	2005-01-
$LogFile		r	2005-01-02 00:12:37 IST	2005-01-
$MFT		r	2005-01-02 00:12:37 IST	2005-01-02 00:12
$MFTMirr		r	2005-01-02 00:12:37 IST	2005-01-
$Secure:$SDS		r	2005-01-02 00:12:37 IST	2005-01-
$UpCase		r	2005-01-02 00:12:37 IST	2005-01-02 00:12
$Volume		r	2005-01-02 00:12:37 IST	2005-01-02 00:12
$I30		r	2005-01-02 00:20:01 IST	2004-10-26 00:25
$I30		r	2005-01-02 00:20:05 IST	2004-12-17 23:35
$I30		r	2005-01-02 00:20:06 IST	2004-12-21 22:22
conninfo.ini	.ini	r	2005-01-02 00:20:16 IST	2005-01-
$I30		r	2005-01-02 00:20:06 IST	2004-12-21 22:22
aol.ini .ini		r	2005-01-02 00:20:06 IST	2005-01-07 03:57
aoldiag.ini	.ini	r	2005-01-02 00:20:06 IST	2005-01-
$I30		r	2005-01-02 00:20:12 IST	2004-12-17 23:35
aoltpspd.ph	.ph	r	2005-01-02 00:20:06 IST	2005-01-
appdata.ini	.ini	r	2005-01-02 00:20:06 IST	2004-12-

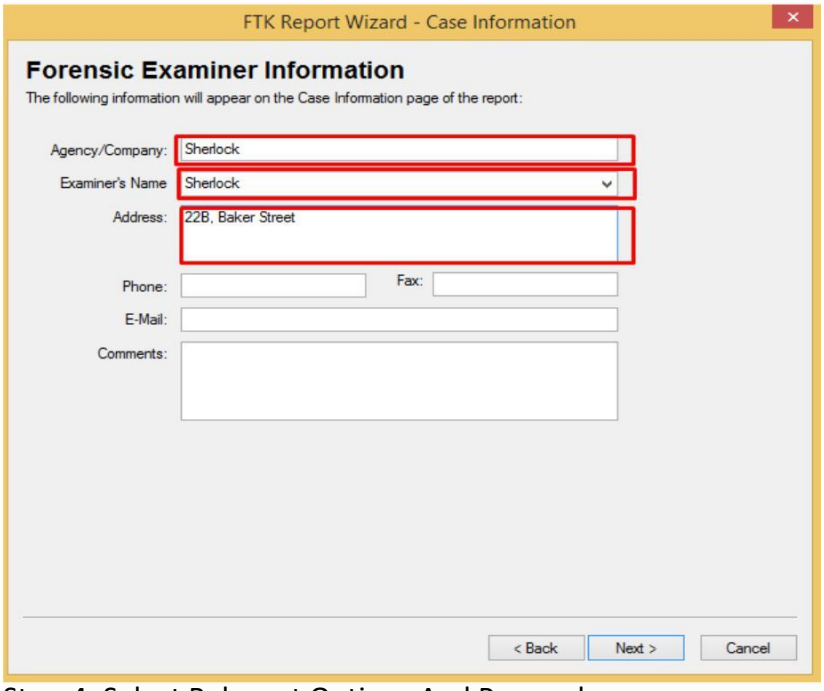
Signature:

Practical 2

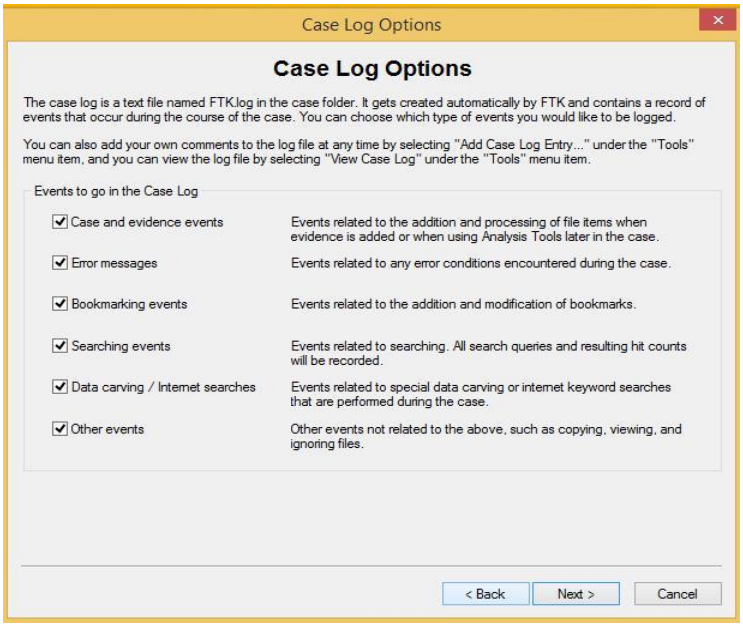
Aim: **Using Windows Forensics Toolkit [Access Data FTK]**

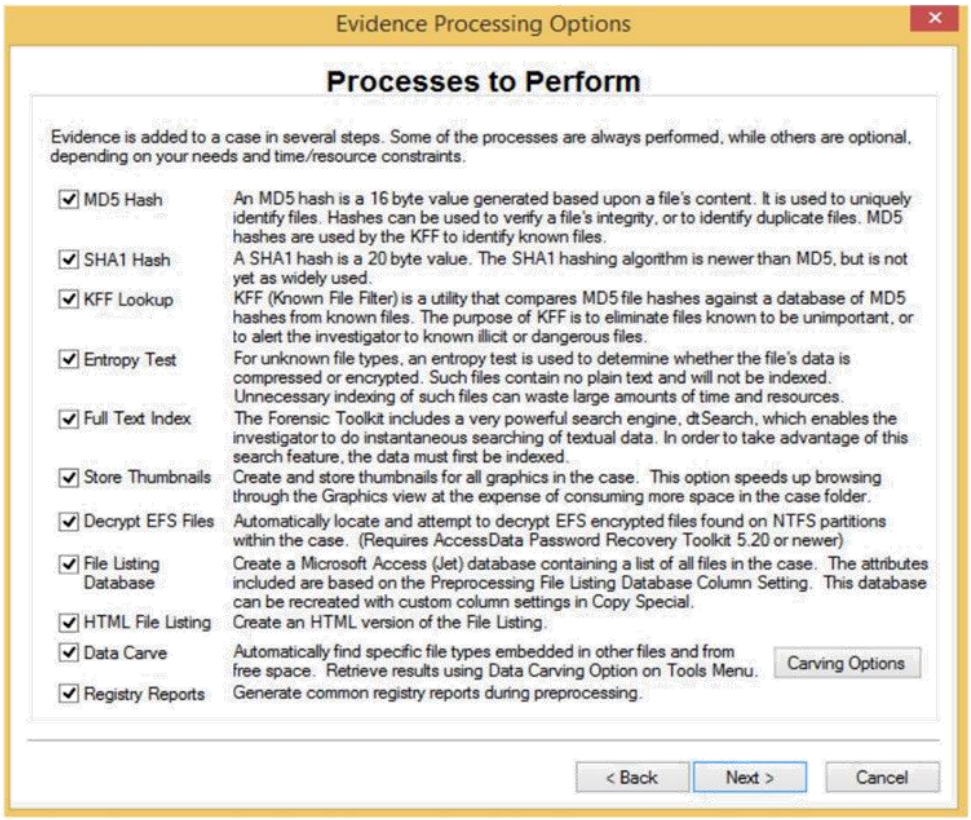
Step-1: Open Forensic Toolkit

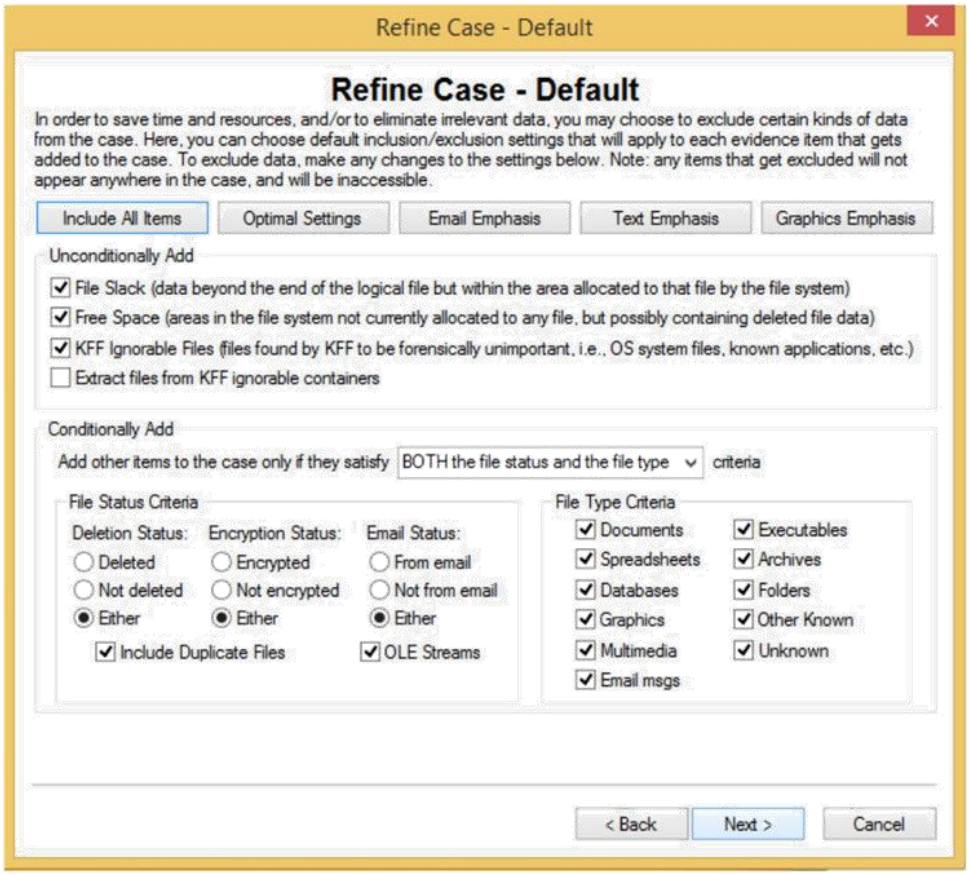
Step-2: We can

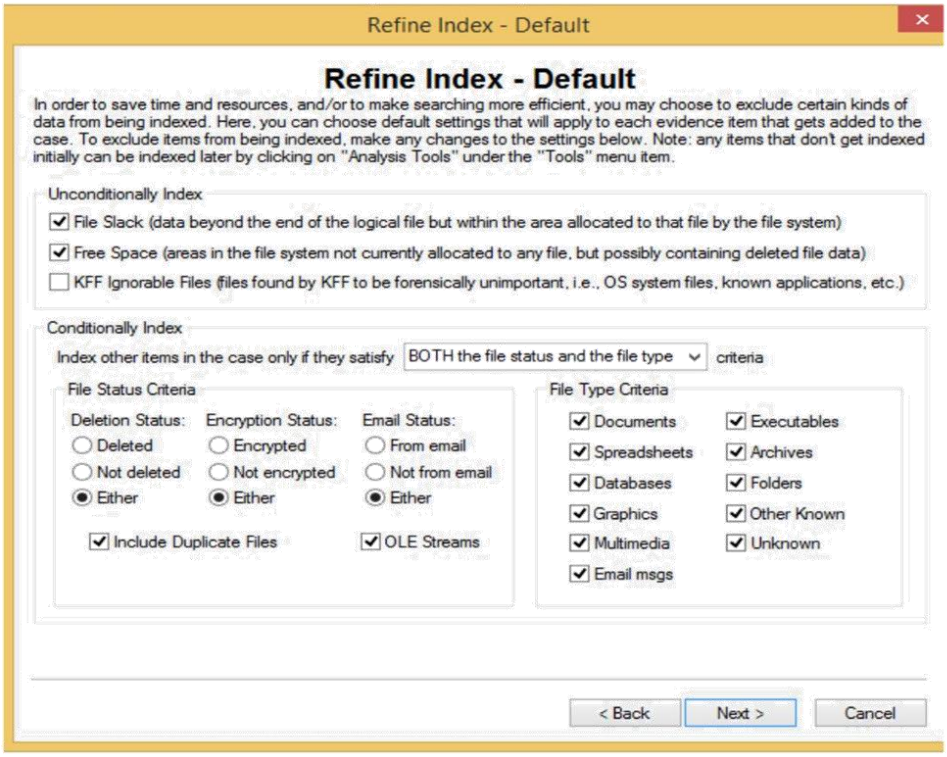


Step-4: Select Relevant Options And Proceed.



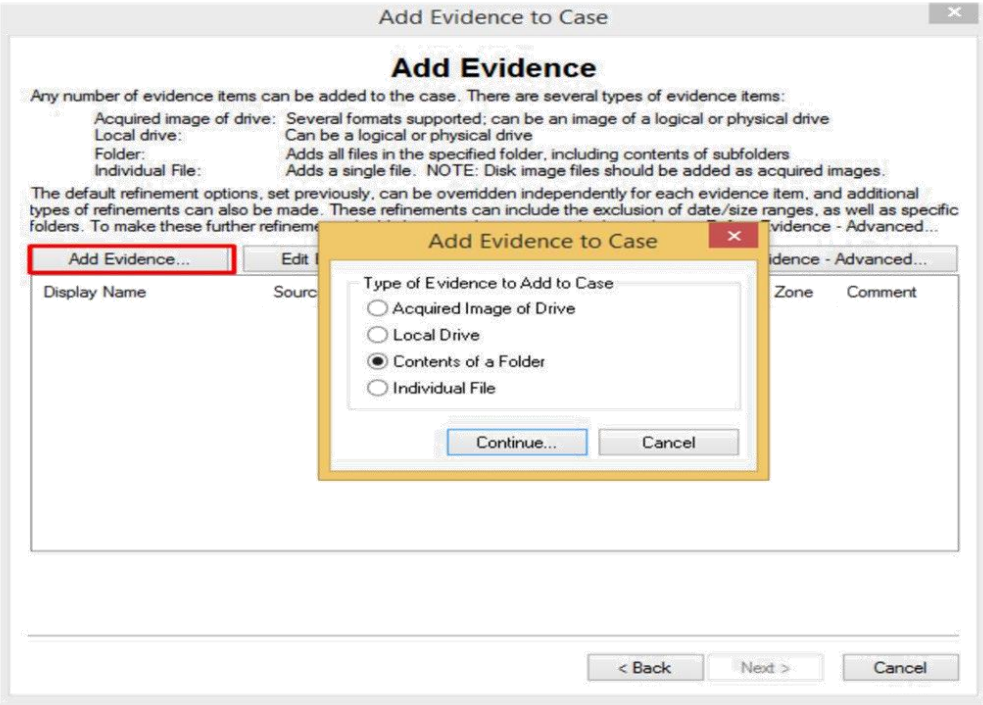

Evidence Processing Options
Processes to Perform
Evidence is added to a case in several steps. Some of the processes are always performed, while others are optional, depending on your needs and time/resource constraints.
MD5 Hash
An MD5 hash is a 16 byte value generated based upon a file's content. It is used to uniquely identify files. Hashes can be used to verify a file's integrity, or to identify duplicate files. MD5 hashes are used by the KFF to identify known files.
SHA1 Hash
A SHA1 hash is a 20 byte value. The SHA1 hashing algorithm is newer than MD5, but is not yet as widely used.
KFF Lookup
KFF (Known File Filter) is a utility that compares MD5 file hashes against a database of MD5 hashes from known files. The purpose of KFF is to eliminate files known to be unimportant, or to alert the investigator to known illicit or dangerous files.
Entropy Test
For unknown file types, an entropy test is used to determine whether the file's data is compressed or encrypted. Such files contain no plain text and will not be indexed. Unnecessary indexing of such files can waste large amounts of time and resources.
Full Text Index
The Forensic Toolkit includes a very powerful search engine, dtSearch, which enables the investigator to do instantaneous searching of textual data. In order to take advantage of this search feature, the data must first be indexed.
Store Thumbnails
Create and store thumbnails for all graphics in the case. This option speeds up browsing through the Graphics view at the expense of consuming more space in the case folder.
Decrypt EFS Files
Automatically locate and attempt to decrypt EFS encrypted files found on NTFS partitions within the case. (Requires AccessData Password Recovery Toolkit 5.20 or newer)
File Listing Database
Create a Microsoft Access (Jet) database containing a list of all files in the case. The attributes included are based on the Preprocessing File Listing Database Column Setting. This database can be recreated with custom column settings in Copy Special.
HTML File Listing
Create an HTML version of the File Listing.
Data Carve
Automatically find specific file types embedded in other files and from free space. Retrieve results using Data Carving Option on Tools Menu.
Carving Options
Registry Reports
Generate common registry reports during preprocessing.
< Back
Next >
Cancel


Refine Case - Default
Refine Case - Default
In order to save time and resources, and/or to eliminate irrelevant data, you may choose to exclude certain kinds of data from the case. Here, you can choose default inclusion/exclusion settings that will apply to each evidence item that gets added to the case. To exclude data, make any changes to the settings below. Note: any items that get excluded will not appear anywhere in the case, and will be inaccessible.
Include All Items
Optimal Settings
Email Emphasis
Text Emphasis
Graphics Emphasis
Unconditionally Add
File Slack (data beyond the end of the logical file but within the area allocated to that file by the file system)
Free Space (areas in the file system not currently allocated to any file, but possibly containing deleted file data)
KFF Ignorable Files (files found by KFF to be forensically unimportant, i.e., OS system files, known applications, etc.)
Extract files from KFF ignorable containers
Conditionally Add
Add other items to the case only if they satisfy BOTH the file status and the file type criteria
File Status Criteria
Deletion Status:
Deleted
Not deleted
Either
Encryption Status:
Encrypted
Not encrypted
Either
Email Status:
From email
Not from email
Either
Include Duplicate Files
OLE Streams
File Type Criteria
Documents
Spreadsheets
Databases
Graphics
Multimedia
Email msgs
Executables
Archives
Folders
Other Known
Unknown
< Back
Next >
Cancel

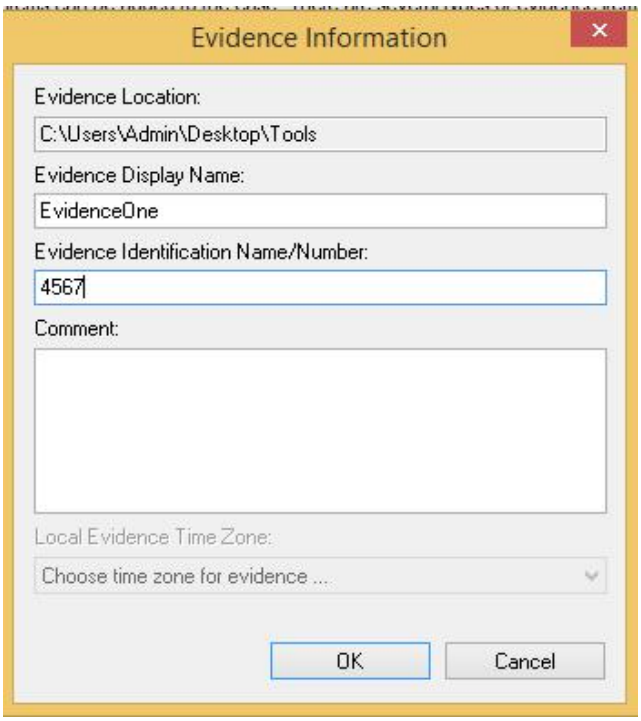


Step-5: Adding Evidence.

We Can Add Evidence Now Or Later Via The File Menu. The Evidence Can Be In The Form Of Accquired Image Of Drive Local Drive Contents Of A Folder Individual File According To The Option Selected We Will Be Presented With The Relevant Popup Screen. For Now We Will Be Going With The Contents Of A Folder Option.

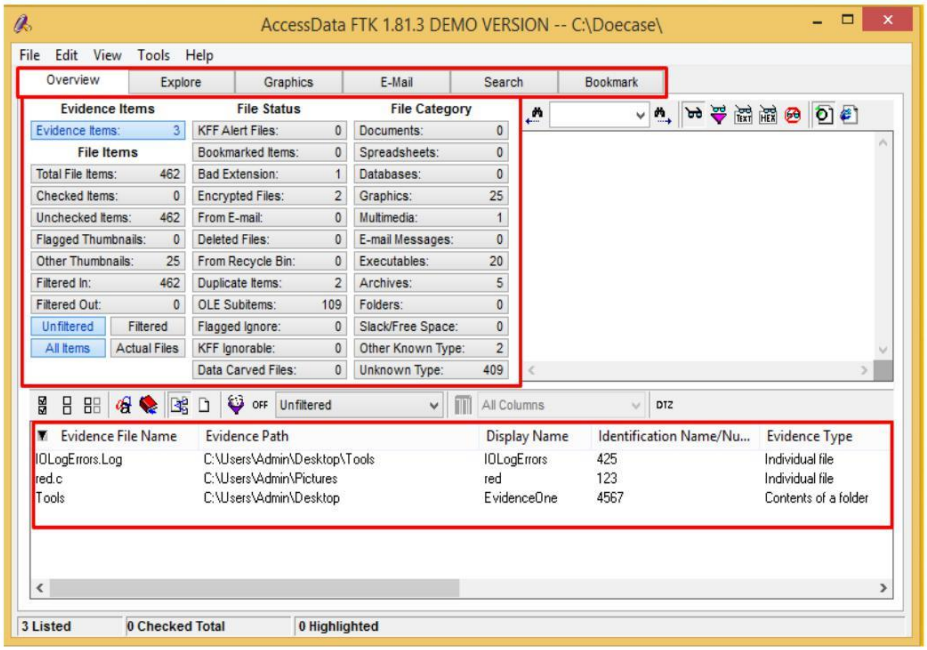


Select The Folder In The Resulting Pop Up And The Fill The Relevant Details Asked

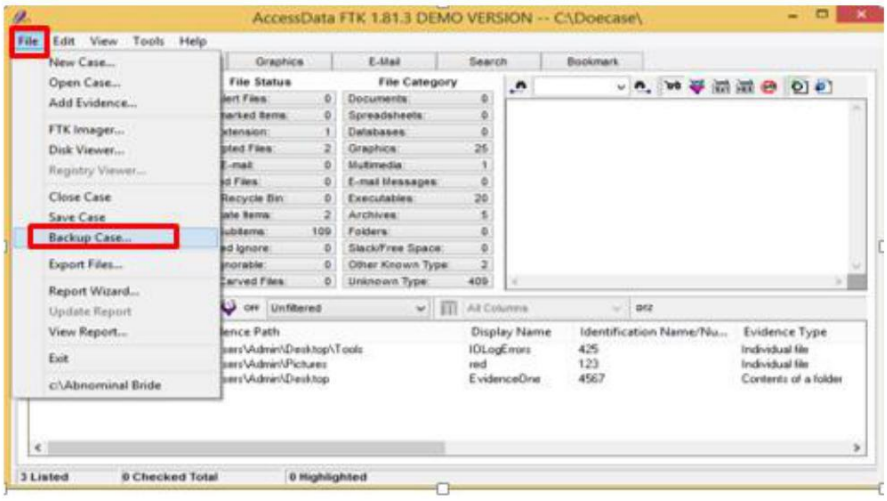


Click OK And Then Next To Proceed With The Processing Of The Selected Folder.

Step-6: We'll Be Presented With Findings From The Evidences Added Into The Case We Can Search, Refine, Examine The Data In The Evidence With The Help Of The Options Provided In The Access Toolkit.

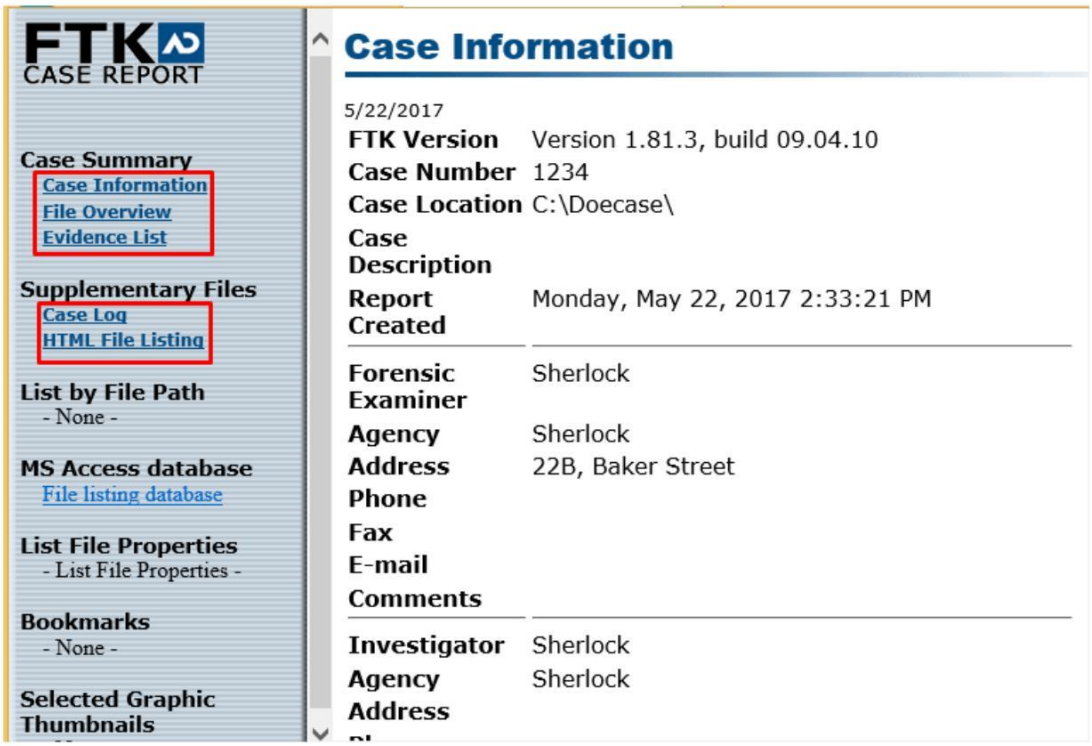


Step-7: We Can Create The Backup Of The Case By Selecting The Backup Case Option In The File Menu And Then Providing The Location For Keeping The Backup File.



Step-8: We Can Generate Report By Starting Out The Report Wizard Present In The File Menu. Select The Required Options In The Resulting Dialog Box To Generate The Report.

Finally A Report Will Be Generated With The Options Provided To Traverse Through Certain Options.



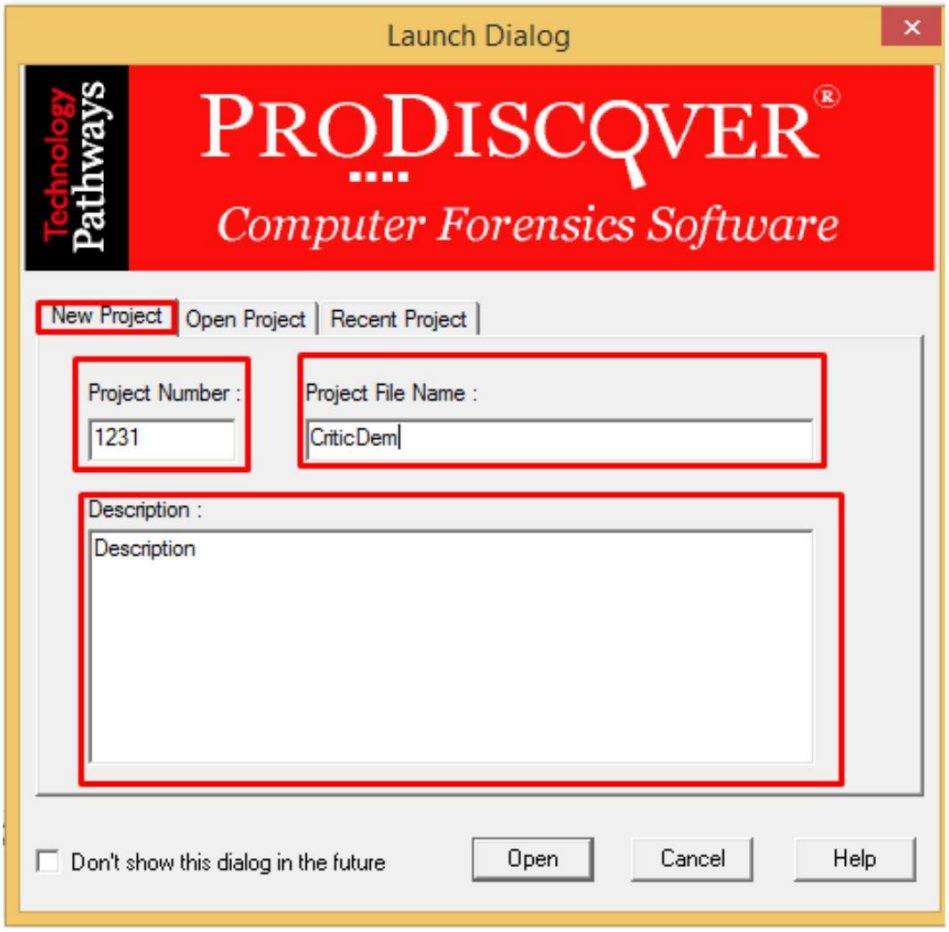
Signature :

Practical 3

Aim : **Using Data Acquisition Tools [ProDiscover Pro]**

Step-1: Open ProDiscover Basic

Step-2: Start A New Project By Filling All The Information As Required.
Then Click Open.



Step-3: To Create An Image For Investigation

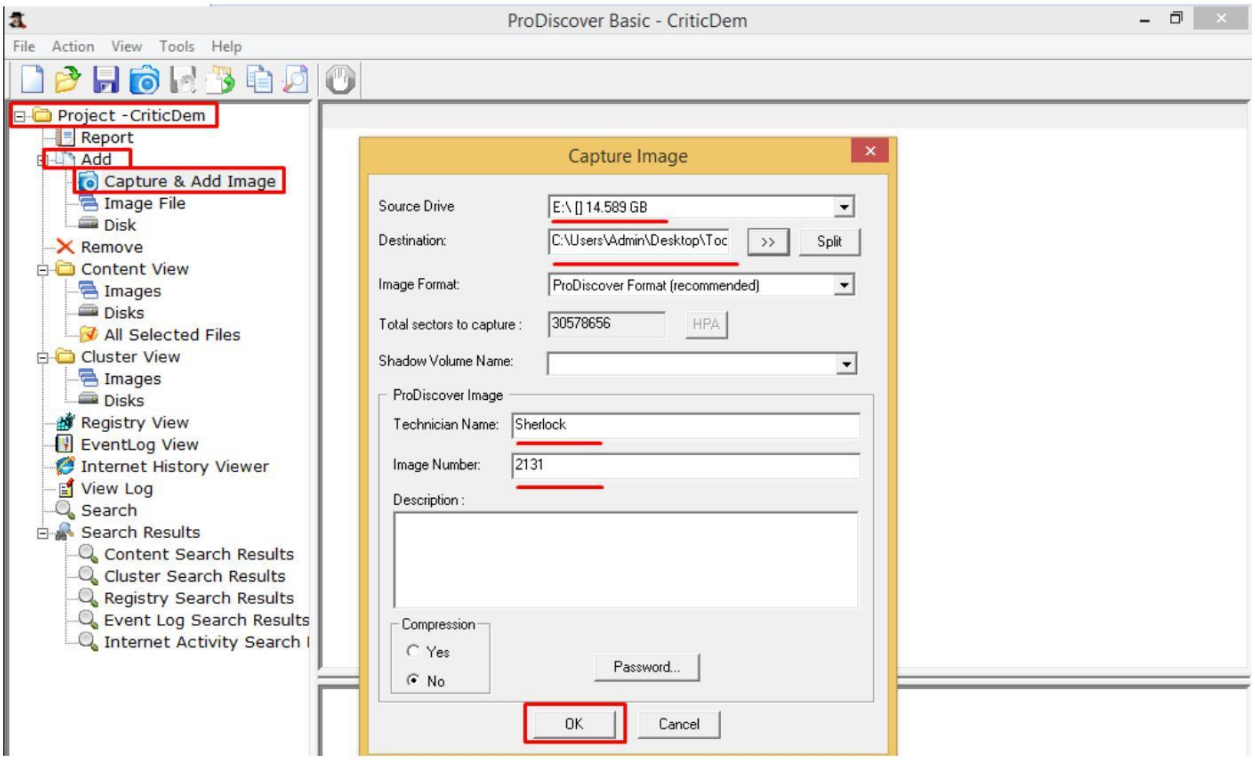
Purpose, Click Add -> Capture & Add Image

In The Resulting Popup Enter The Needed Information.

The Source Drive Can Be Any Drive Which You Want To Investigate Upon.

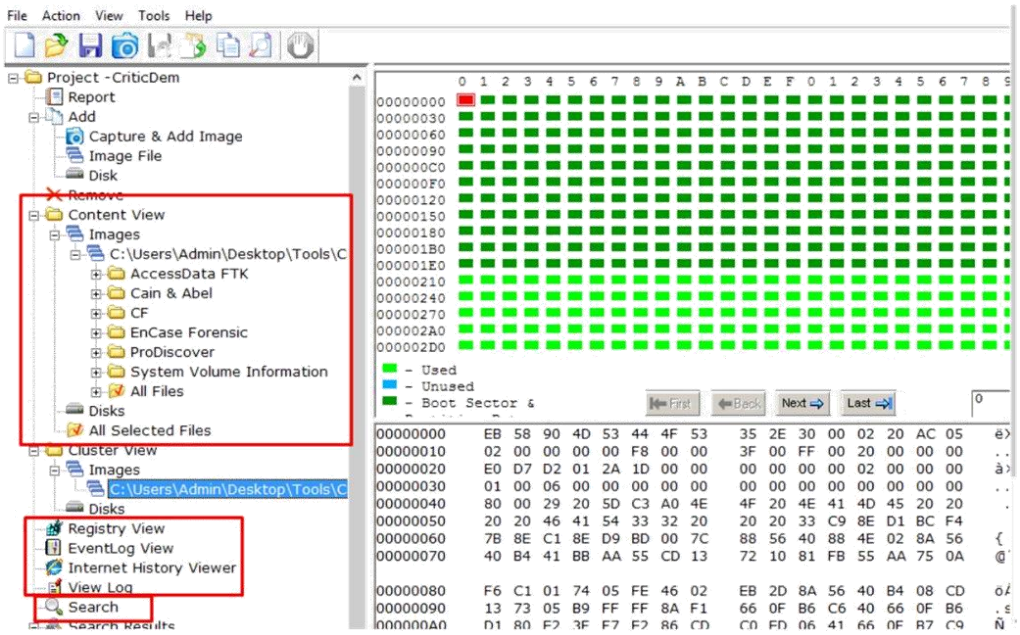
It Can Be A USB Drive, Physical Drive On The System Or Something Else.

Once Done Filling All The Necessary Information, Click OK.

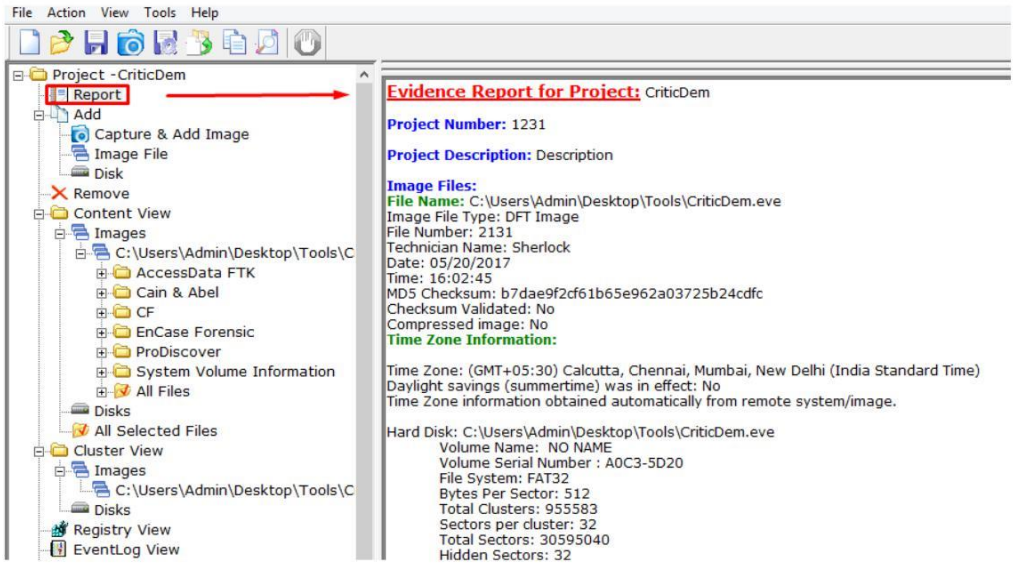


The Tool Will Now Start The Process Of Making An Image From The Given Drive.

Step-4: Now The Image Will Be Processed And The Contents Will be Presented In The Left Tab. We Can Investigate The Image By Searching The Drive Using The Search Option. The Deleted Files, Registry Files And Many More Data Can Be Viewed.



We Can Also View The Report By Clicking On The Report Tab



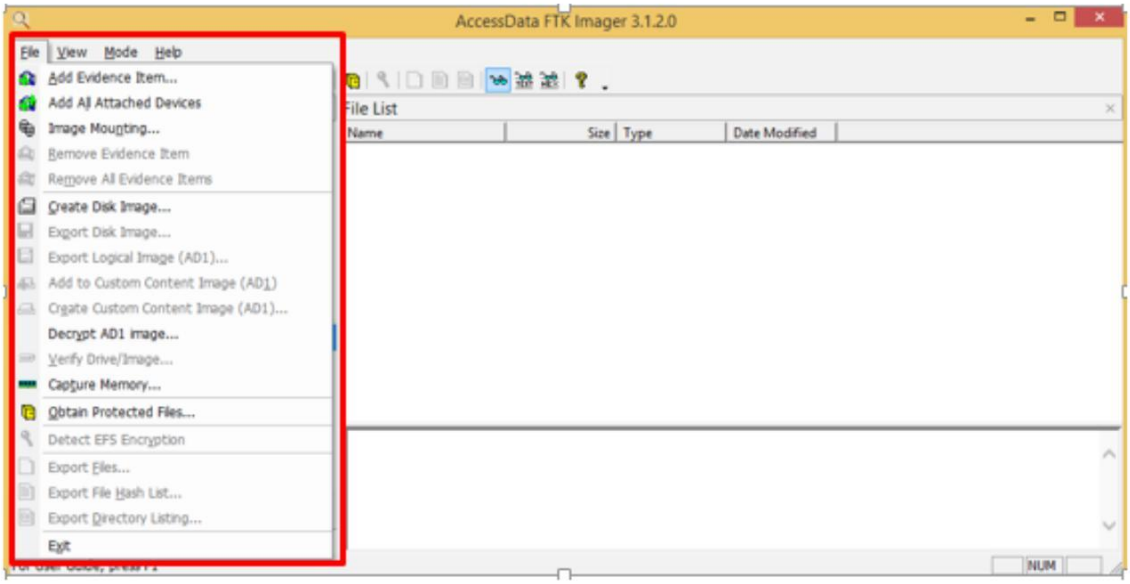
Signature:

Practical 4

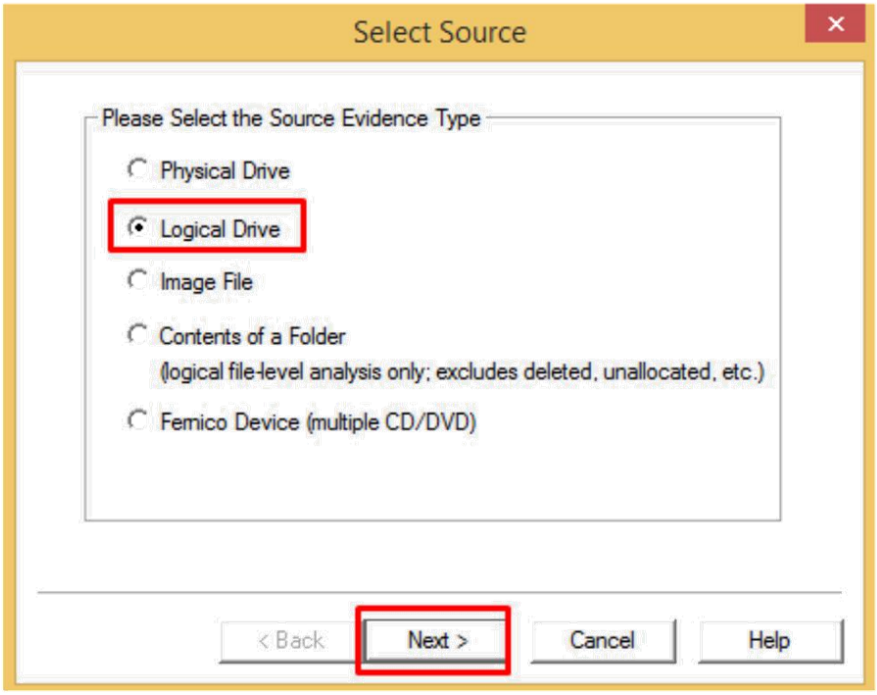
Aim : **Using File Recovery Tools [FTK Imager] Creating Image**

Step-1: Open Access FTK Imager

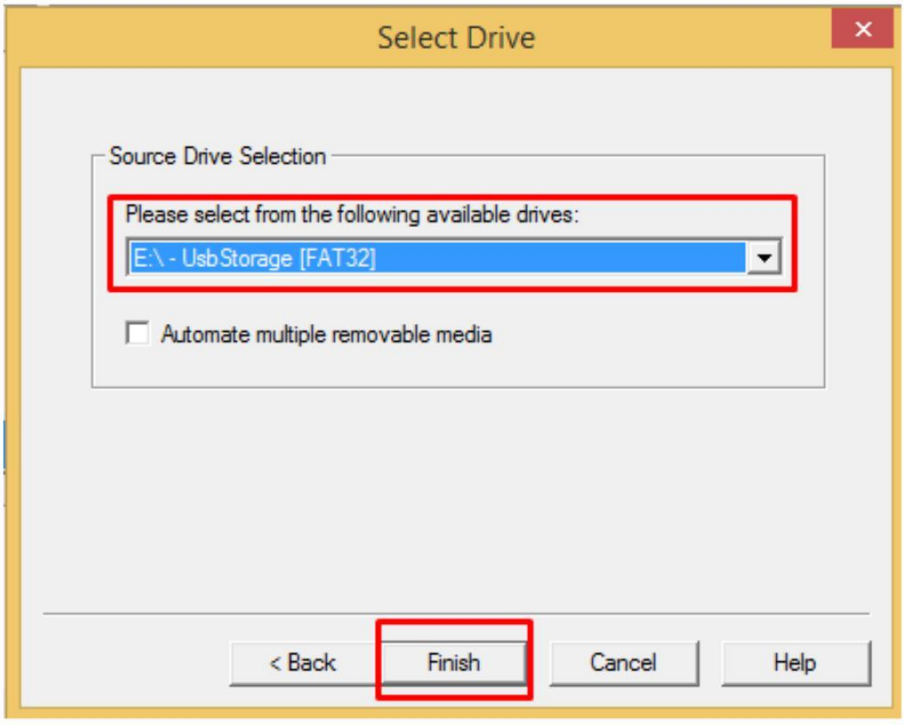
Step-2: In The Resulting Application, Many Options Will Be Provided
We Will Proceed With Creating A Disk Image Of A Logical Drive. Select Create Disk Image.



Step-3: In The Resulting Popup,
Select Logical Drive And Click Next.

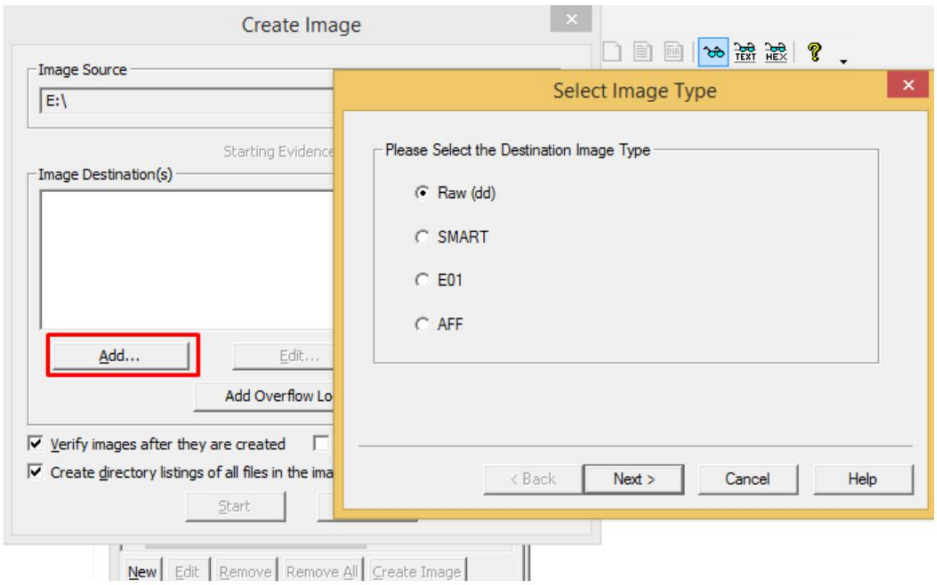


Select A Drive And Click Finish.

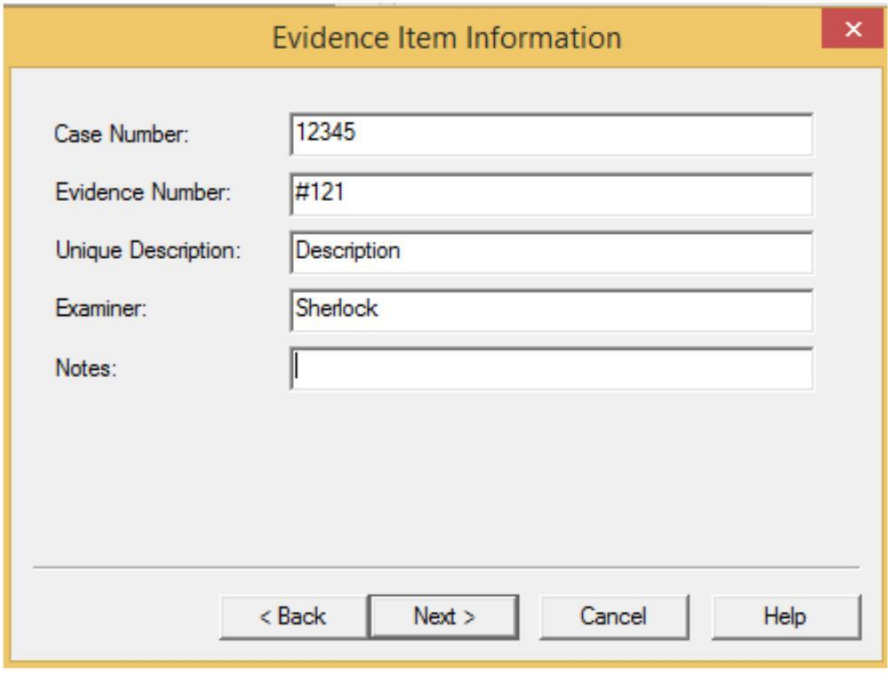


Step-4: Creating Image – Configuring Options

In The Resulting Popup, Click Add And Select The Image Type.
We Will Go With Raw Type Here.

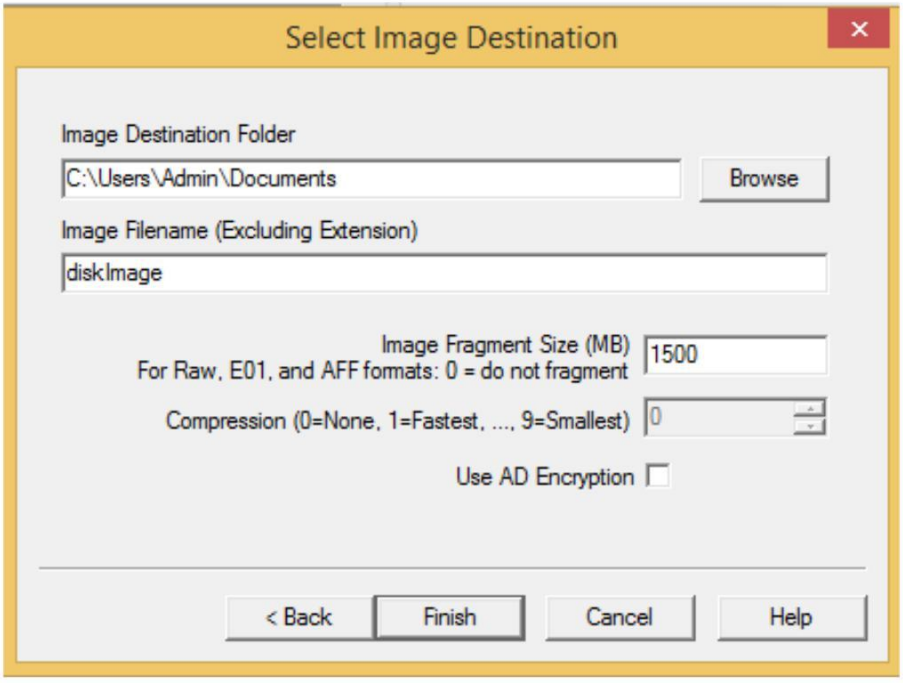


Proceed With Filling The Required Information In The Resulting Popup.

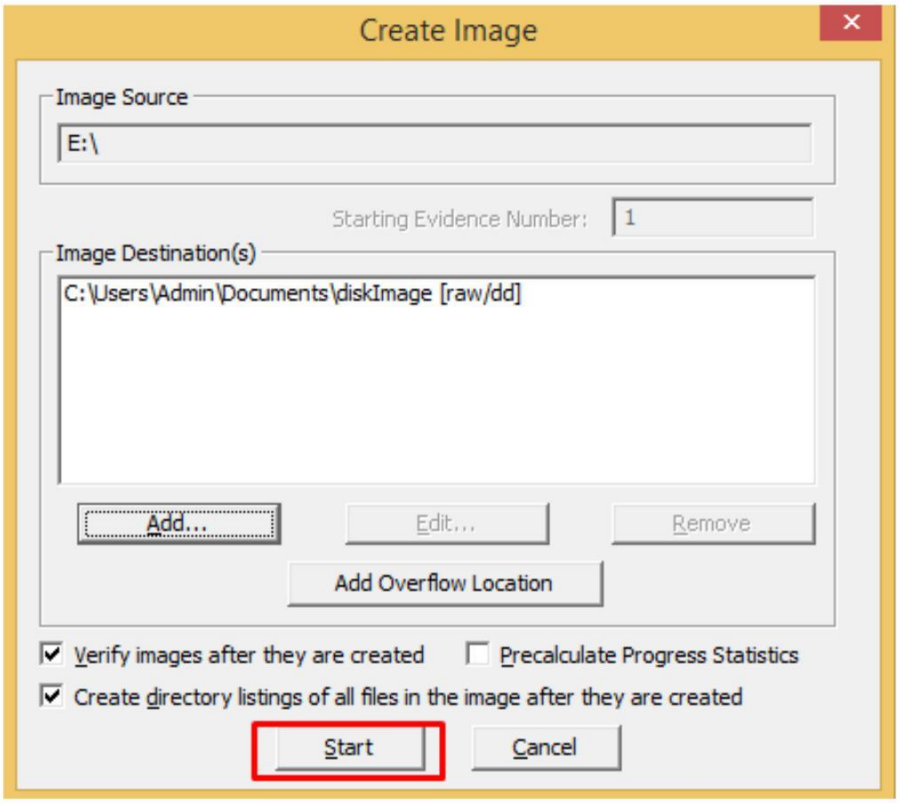


Provide The Location For The Disk Image File To Be Stored.

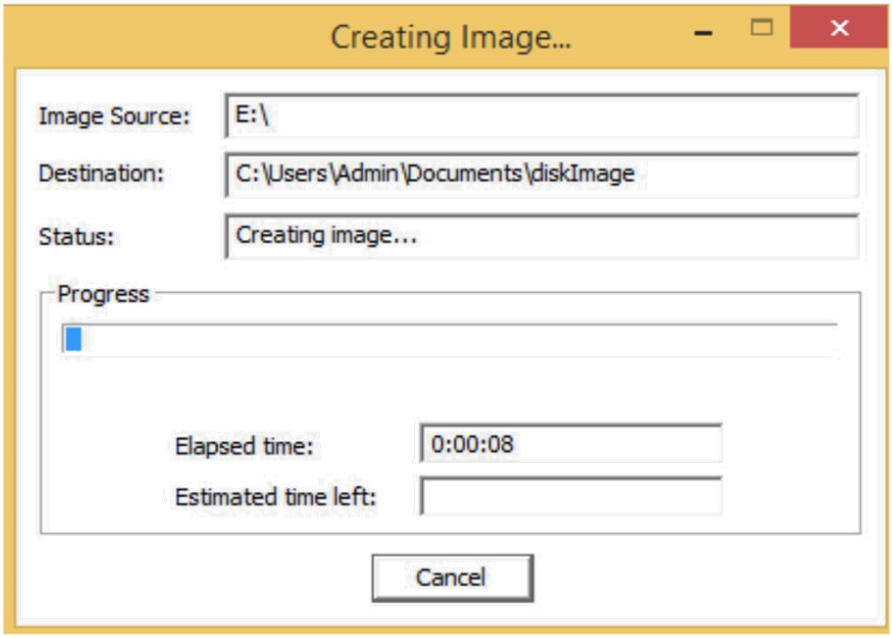
Click Finish.



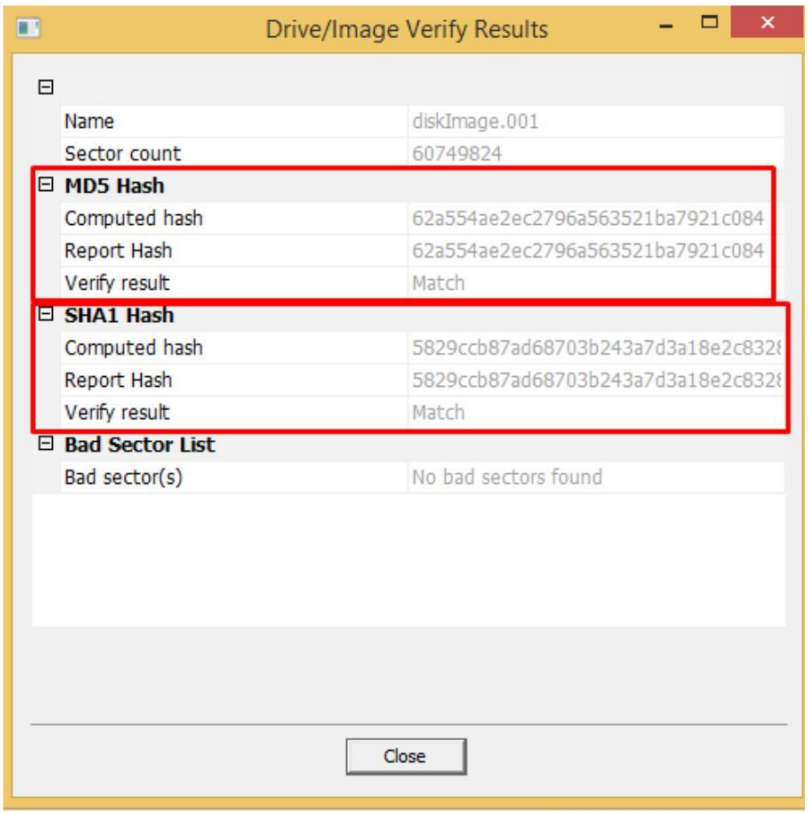
Click Start To Proceed With The Creating Of The Image.



A Dialog Box Showing The Progress Of The Process Will Be Shown.



Step-5: After The Processing, A Dialog Box Will Show The Results.



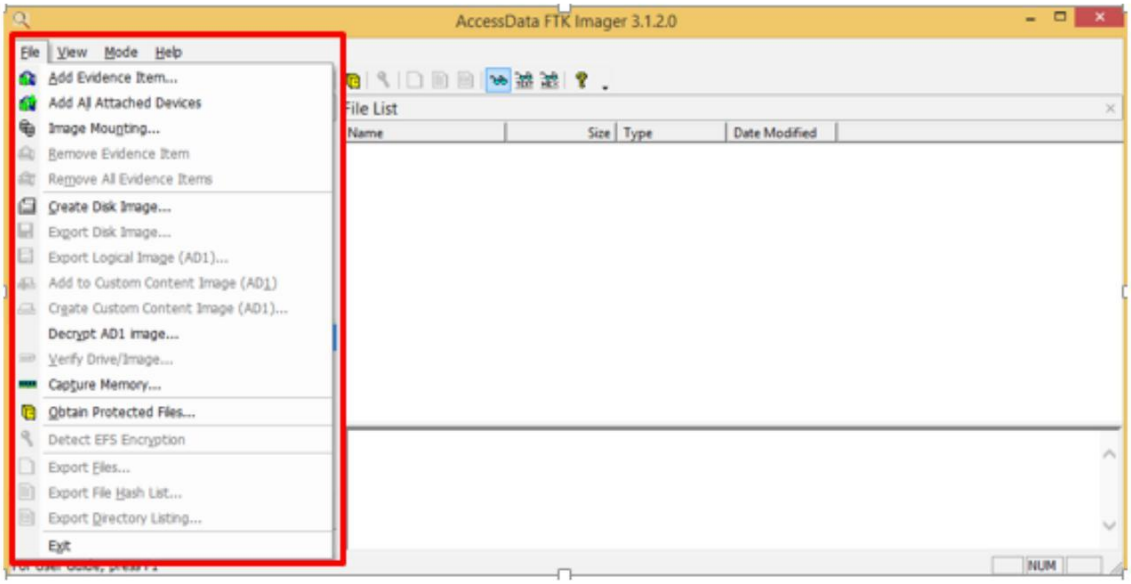
Signature :

Practical 5

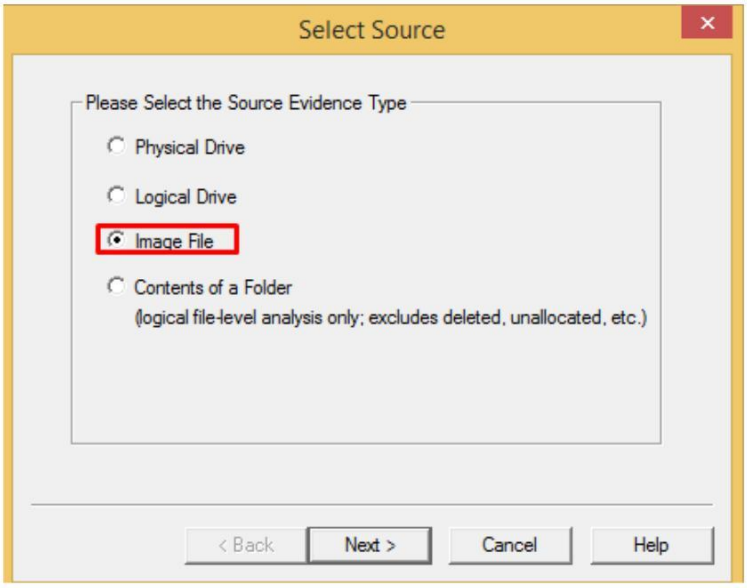
Aim : **Using File Recovery Tools [FTK Imager] Using Evidence**

Step-1: Open Access FTK Imager

Step-2: In The Resulting Application, Many Options Will Be Provided
We Will Proceed With Adding An Evidence File. Select Add Evidence Item.

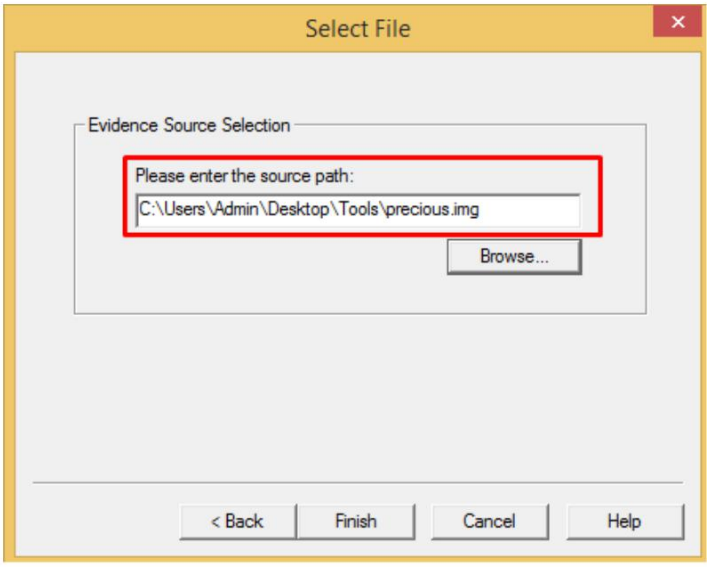


Step-3: In The Resulting Popup Select The Image File Option And Click Next

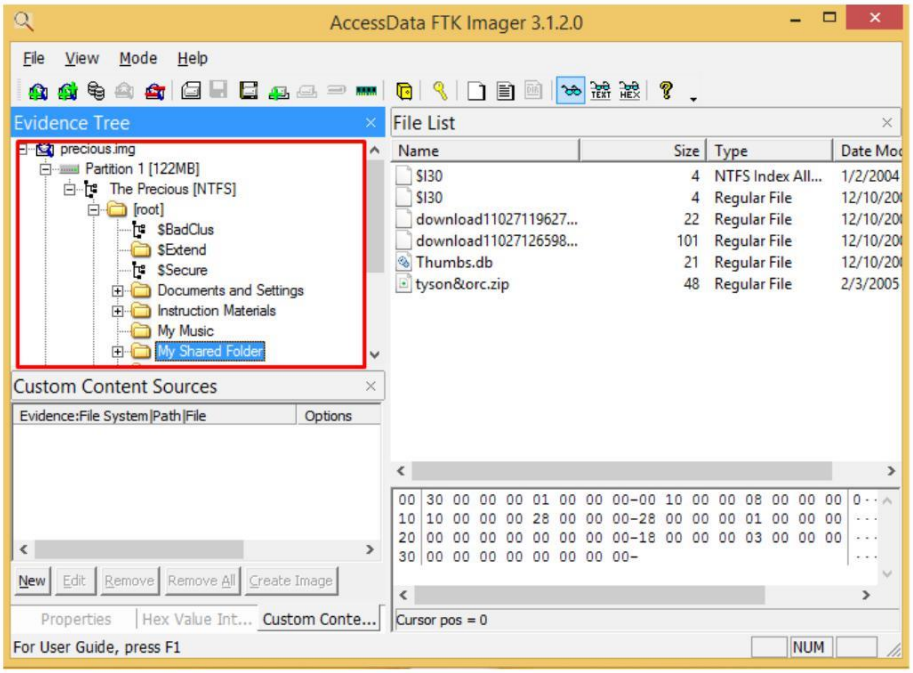


Step-4: Provide The Location Of The Image File To Be Used

Click Finish.



The Application Will Process The Image File And Provide A Display For Its Content.

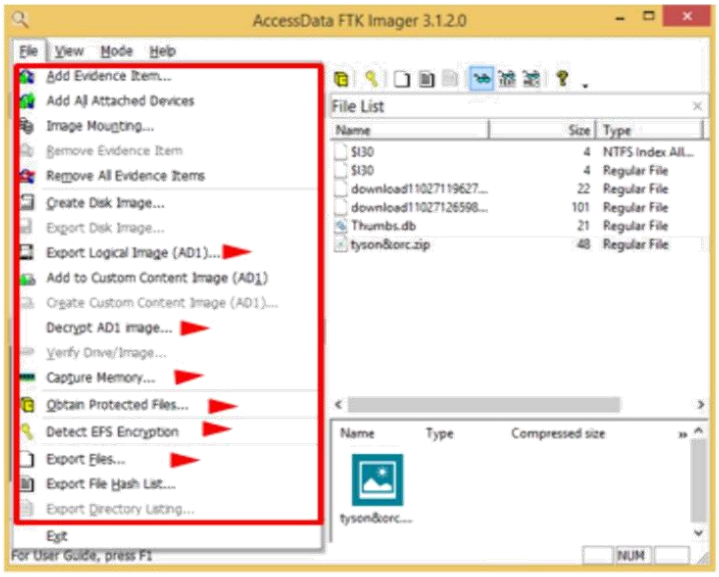


Step-6: In The File Menu, There Are Various Options That Can Be Used

Capture Memory,

Export Files,

Decrypt AD1 Image



Step-7: The Image Directory Can Also Be Browsed To Retrieve Information About Deleted Files, Registry Files And So On.

Signature :

Practical 6

Aim: **Using Steganography Tools [S-Tools]**

Step-1: Open S-Tools

Step-2: Create A .bmp Image File & .txt File

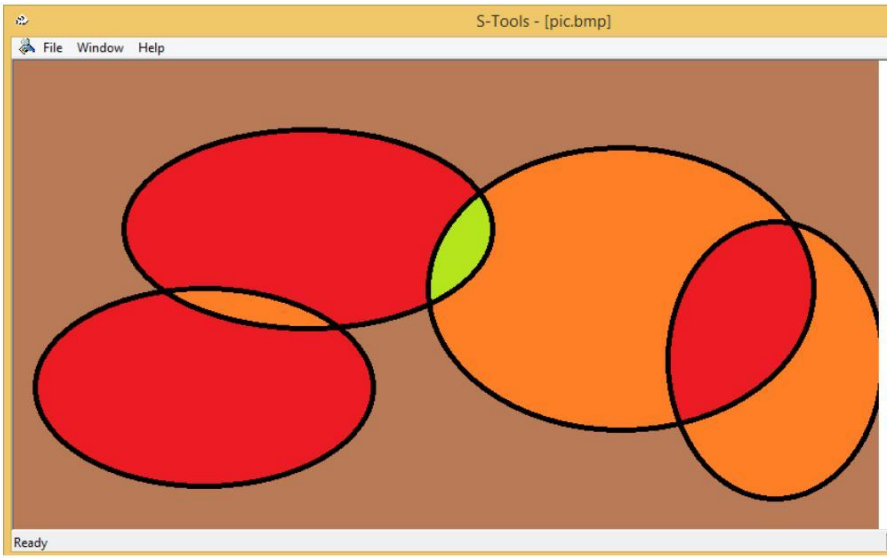
Supported file types for audio and image files are shown below:

Audio - *.wav

Image - *.bmp and *.gif

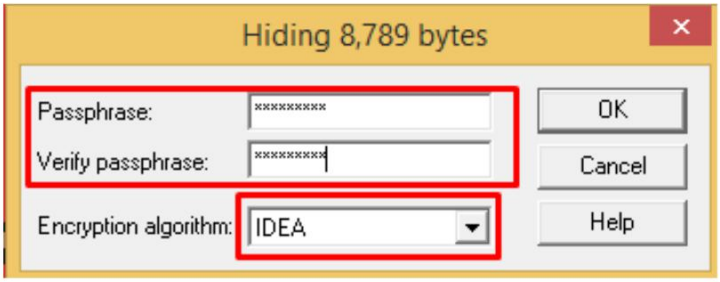
Step-3: Drag & Drop The Two Files (Image & Text)

First Drag The Image & Then The Text File



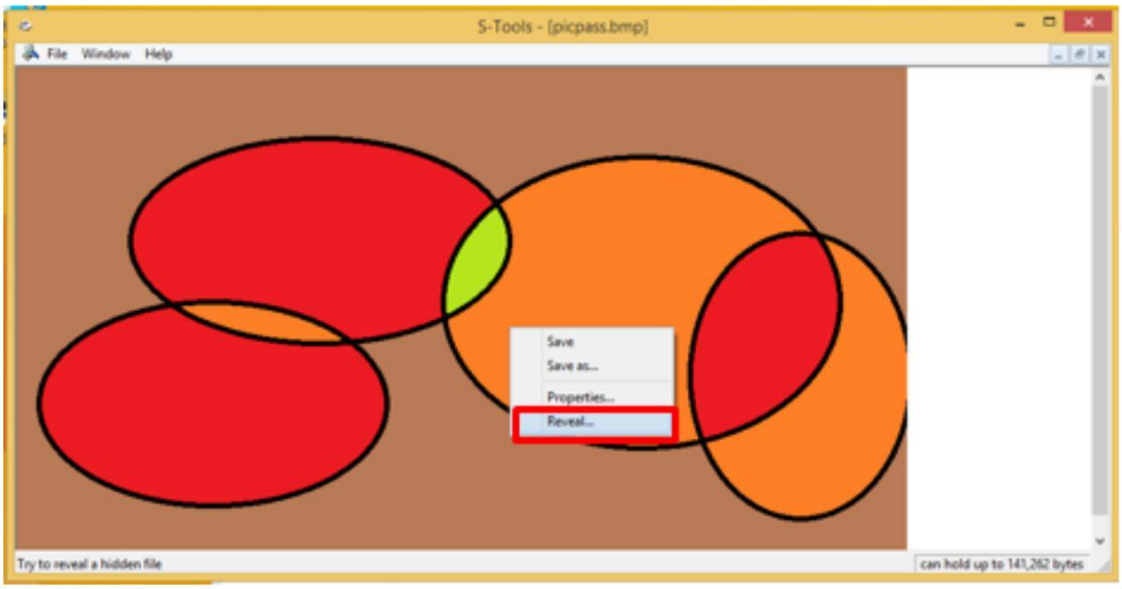
Step-4: When The Text File Is Dragged Over The Image File,

A Dialog Box Will Open Prompting For The Passphrase And The Algorithm To Be Used.

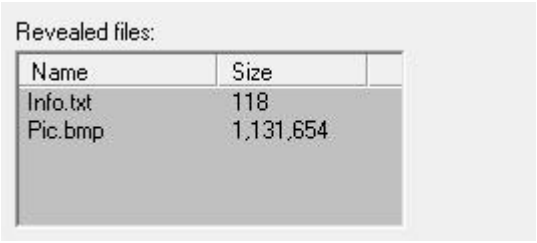


Step-5: Save The Image Into The Desired Location Of Your System.

Step-6: To Obtain The Hidden Text. Open The Saved Image File, Right Click On the Image File
In The Resulting Popup, Click Reveal.



Step-7: Enter The Passphrase You Have Entered Before While Hiding the File A Detailed View Of The Items Contained In The File Will Be Shown.



Step-8: Right Click On The Text File And Save It. The Saved File Will Contain The Text That Was Hidden In The Image File.

Signature :

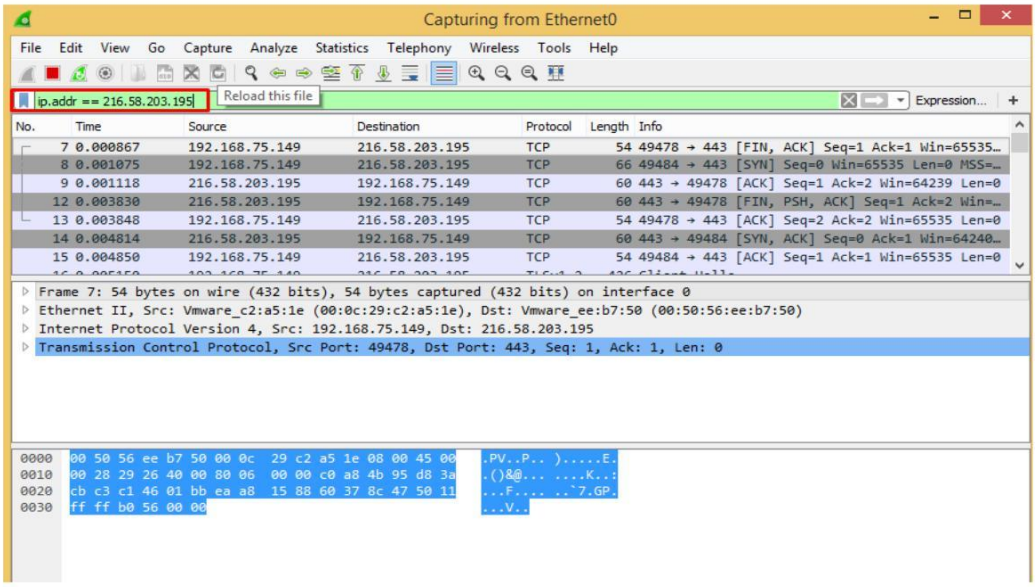
Practical 7

Aim: **Using Log & Traffic Capturing & Analysis Tools [Wireshark]**

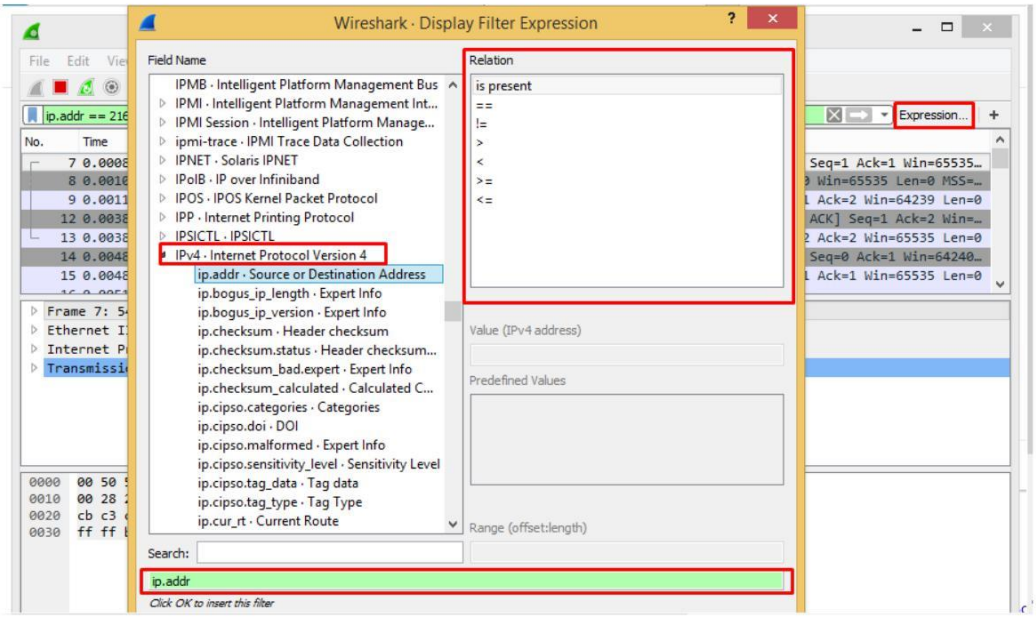
Step-1: Open Wireshark

Step-2: Filtering Packets

We Can Filter Packet By Entering Expressions In The Filter Bar.



Filter Expressions Can Be Added By Clicking The Expression Button Present On The Right Side Of The Filter Bar. The Relations And The Entities Can Be Added With The Help Of The Resulting Dialog Box.

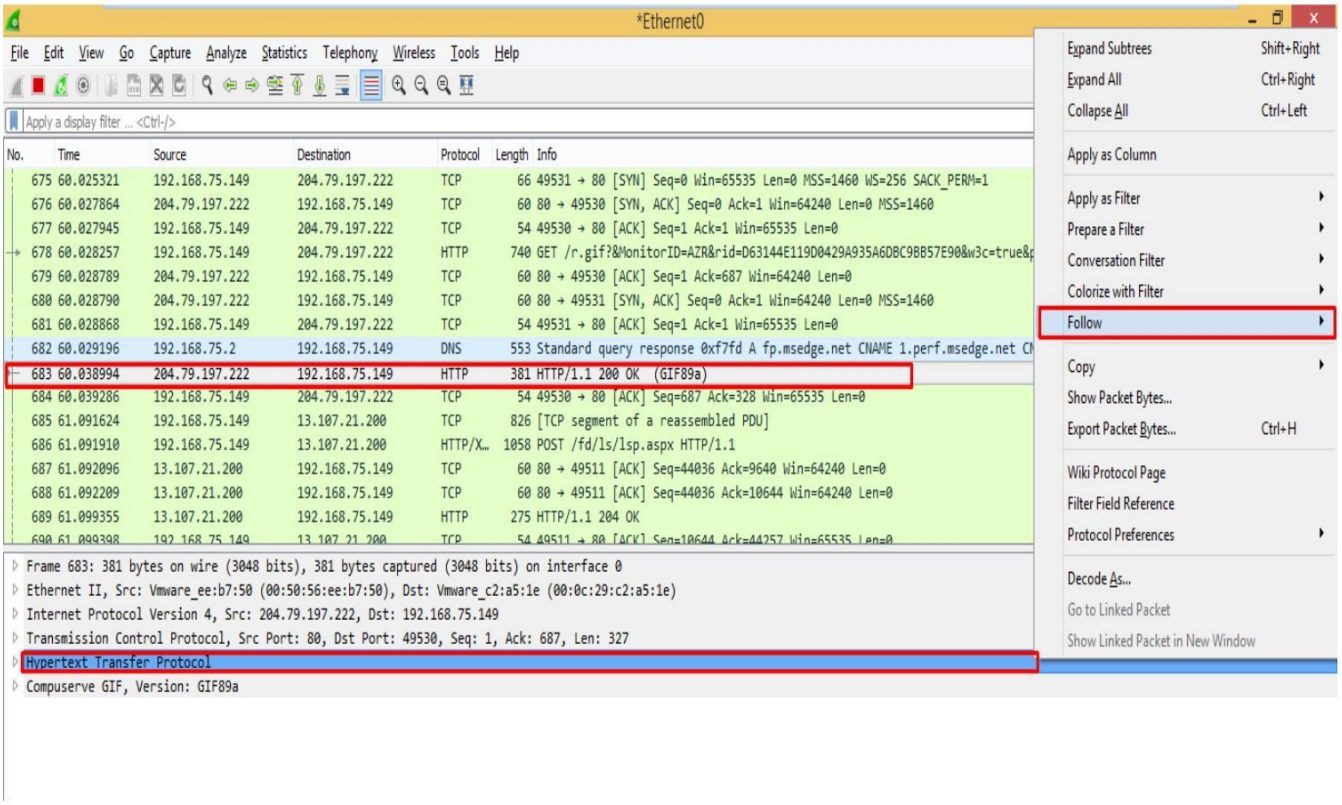


Step-3: Analyzing A Packet.

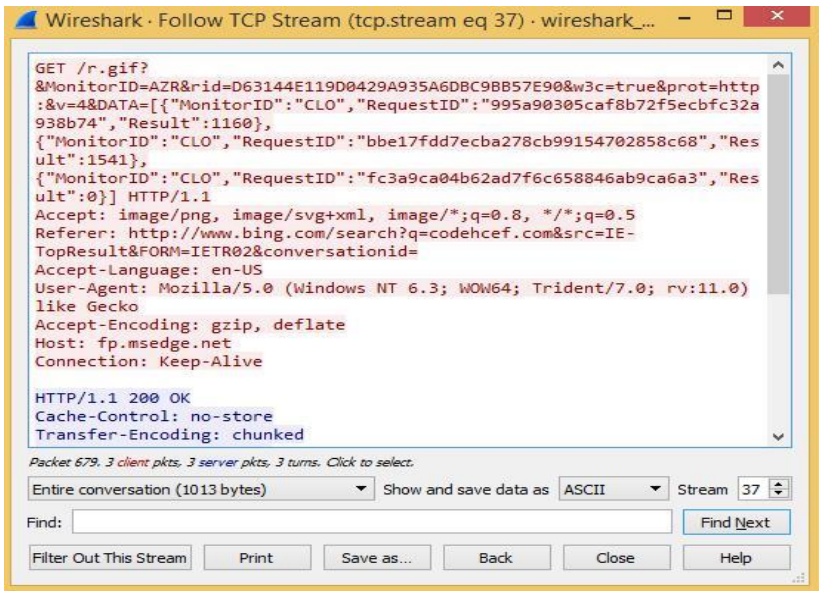
Select A Packet.

Right Click On The Packet Data Available Below

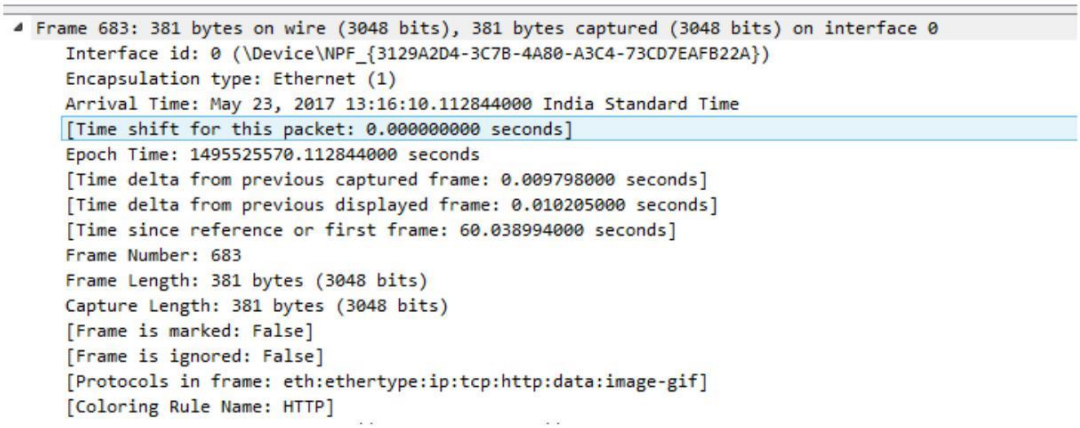
Click Follow -> TCP



A Information For The Particular Packet Will Be Provided In The Resulting Popup Box.



Step-4: We Can Further Inspect The Packet Data By Expanding The Frame Or Other Options Available.



Step-5: Depending On The Analysis More Filters Can Be Added And Inspected.

Signature :

Practical 8

Aim: **Using Email Forensics Tools [Access Data FTK]**

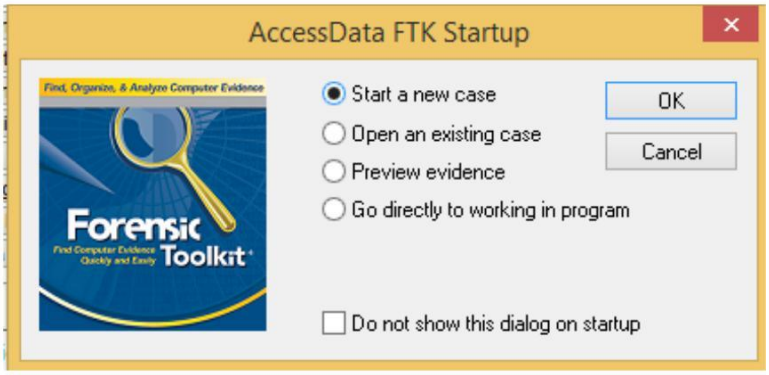
Step-1: Open Forensic Toolkit

Step-2: We can

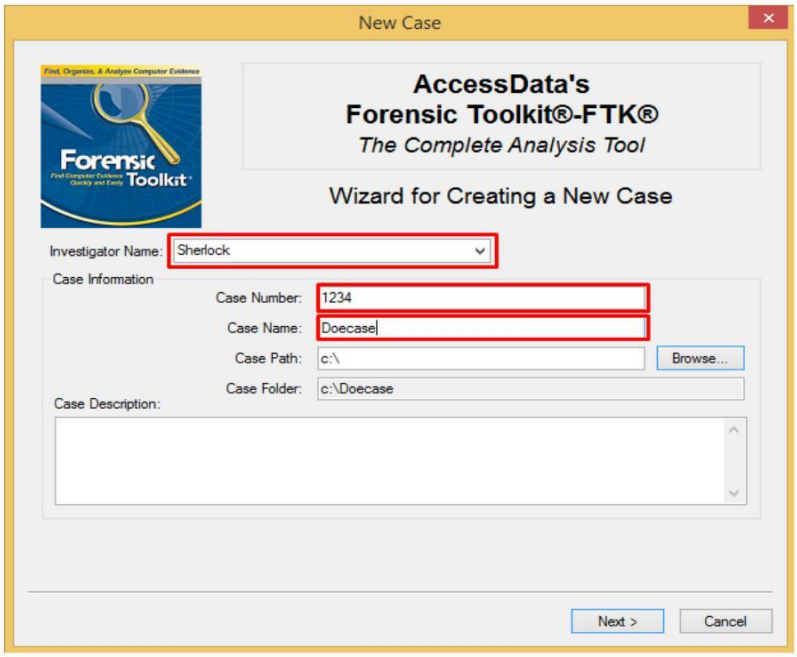
Start A New Case

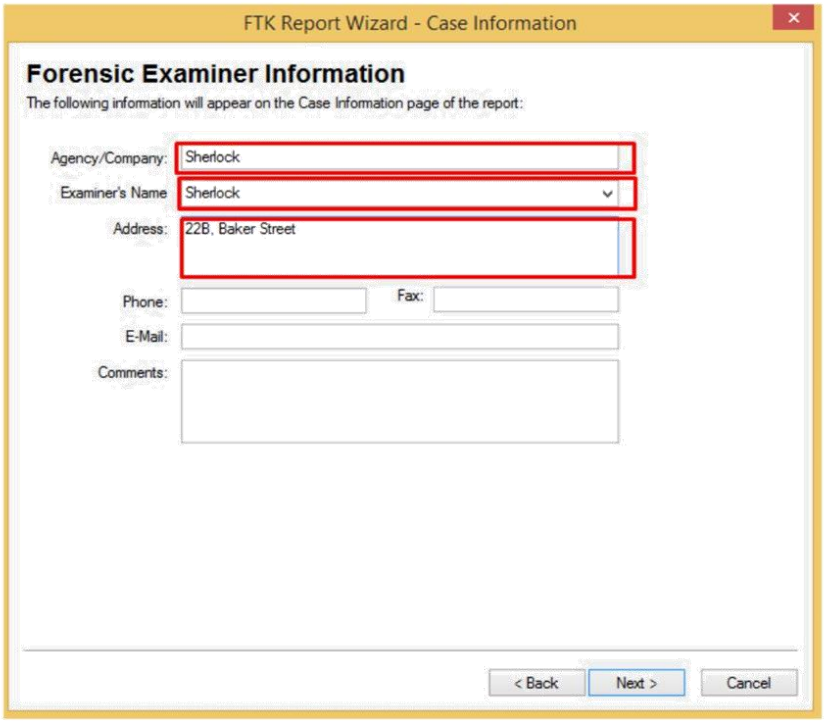
Open An Existing Case According To The Need.

Select Start A New Case -> Click OK

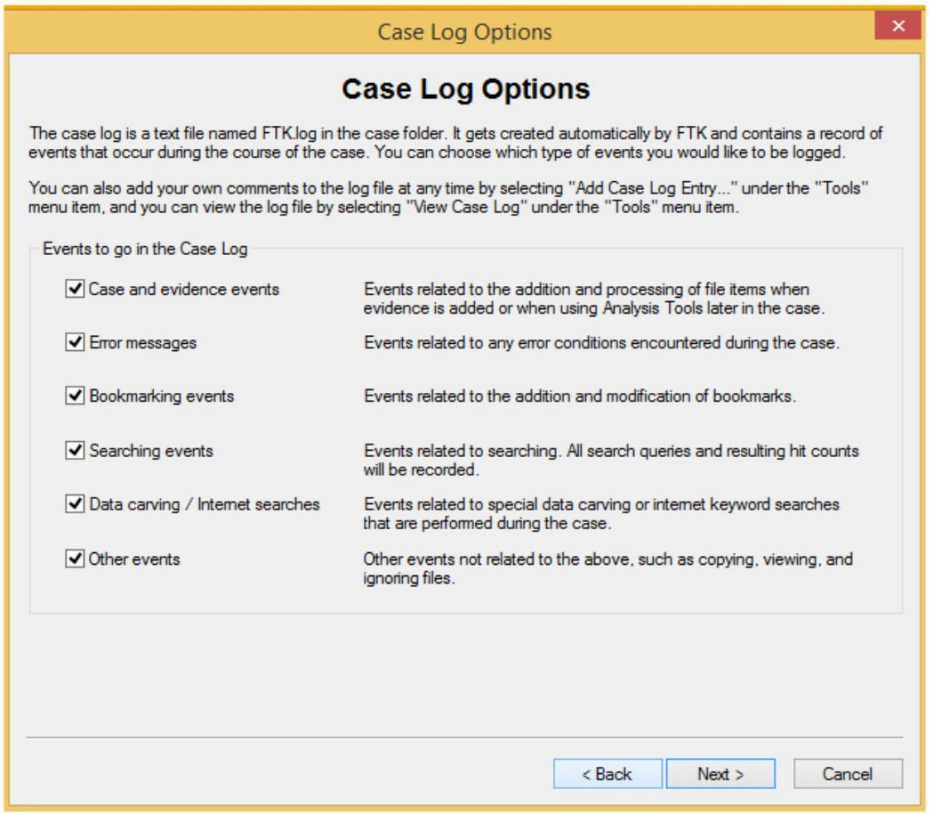


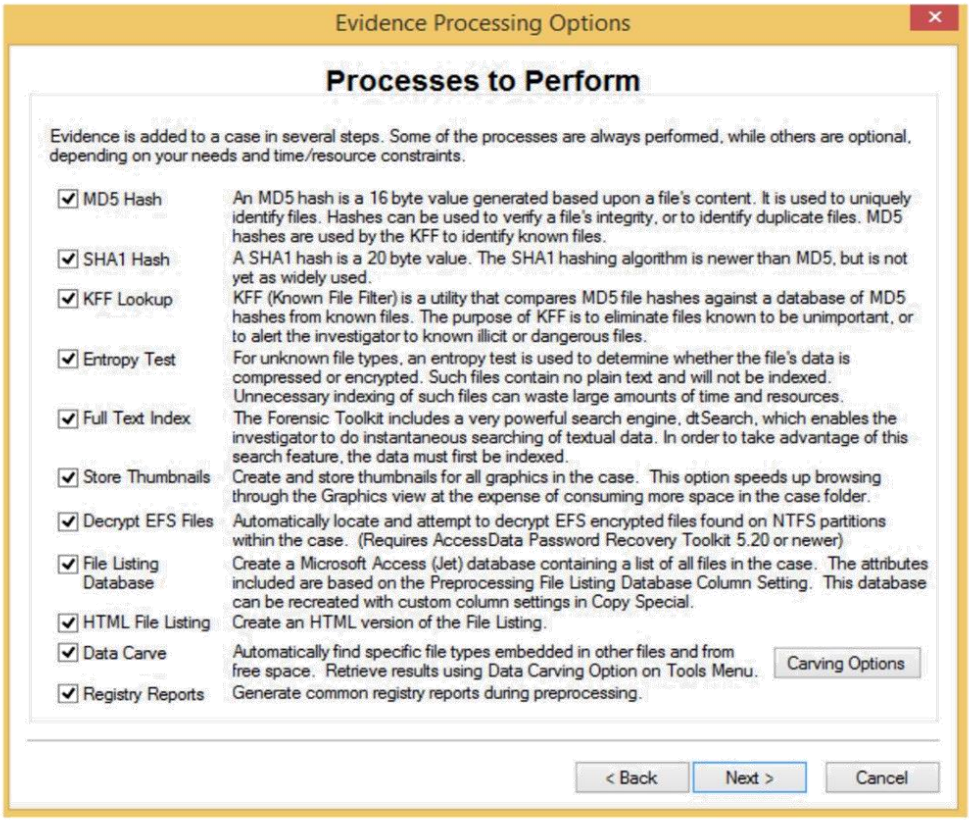
Step-3: Fill The Required Information As Asked



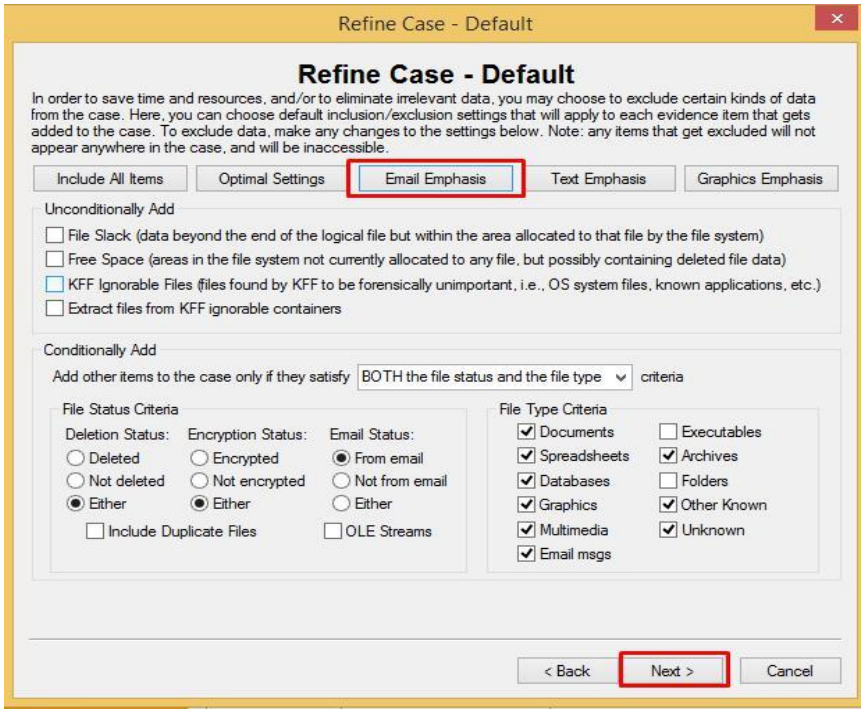


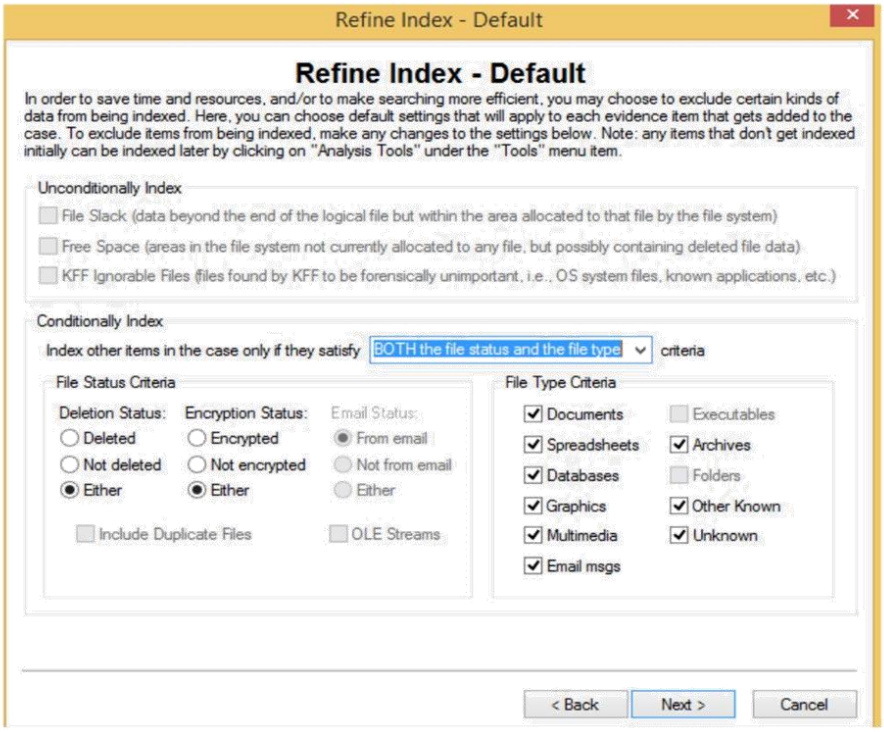
Step-4: Select Relevant Options And Proceed.





Step-5: Click On Email Emphasis & Then Next.





Step-6: Adding Evidence. We Can Add Evidence Now Or Later Via The File Menu.

The Evidence Can Be In The Form Of

Acquired Image Of Drive

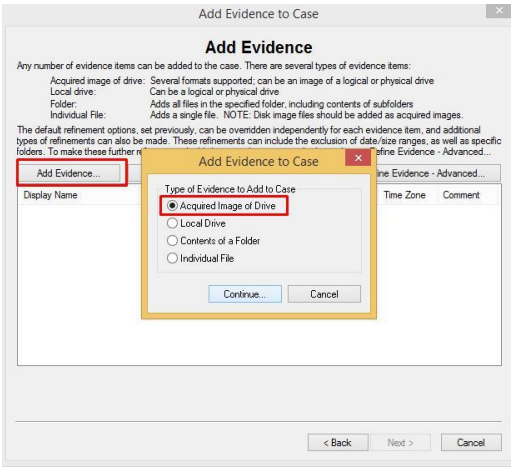
Local Drive

Contents Of A Folder

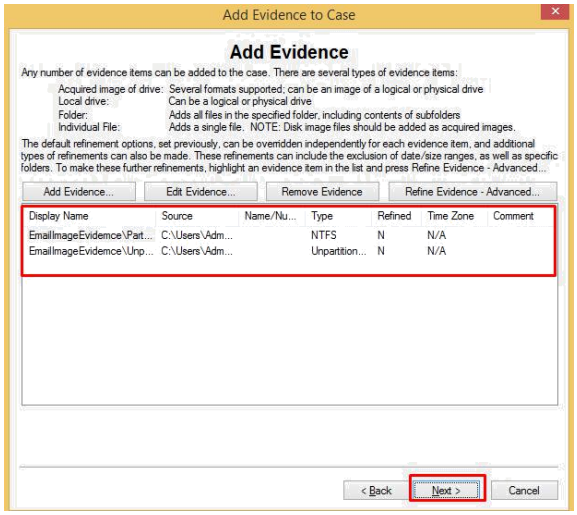
Individual File

According To The Option Selected We Will Be Presented With The Relevant Popup Screen.

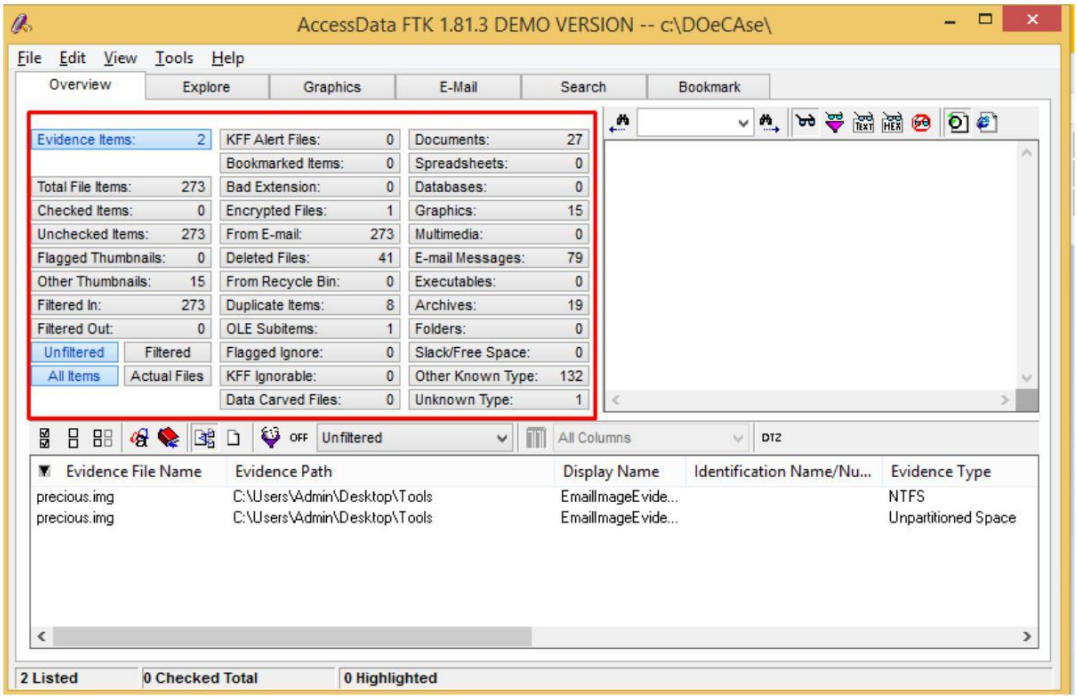
For This Practical We Will Be Going With The Acquired Image Of Drive Option.



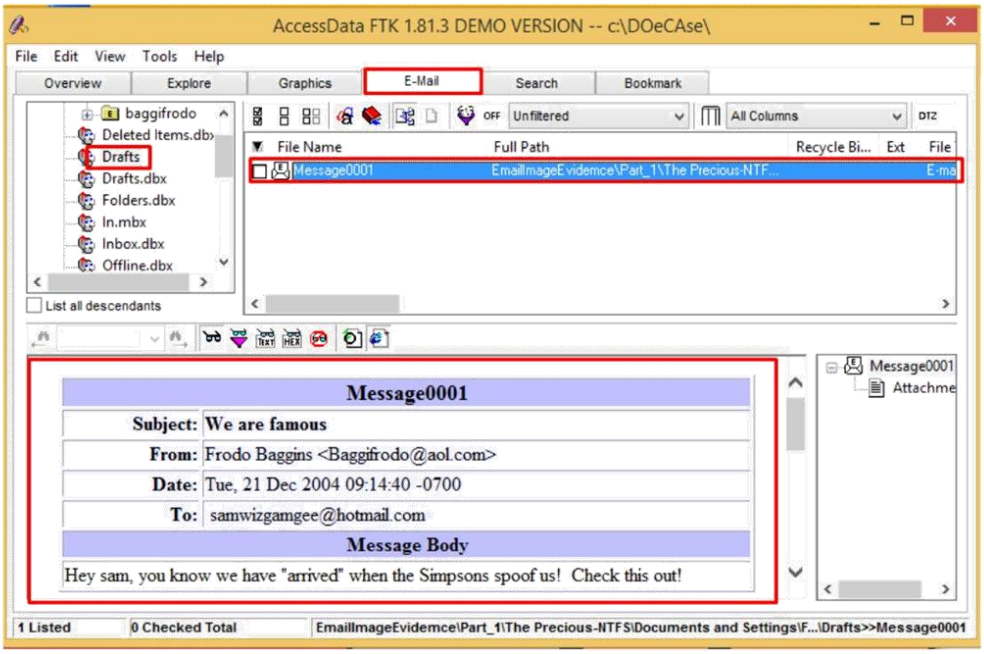
In The Resulting Popup, Load The Desired Image File And Proceed.



Step-7: Once The Loading Process Is Completed, You Can See The Data That Has Been Loaded In The Overview Tab.



Go To The Email Tab, Present In The Application Window. We Can View All The Emails And Analyze A Single Email By Traversing Down To That Specified Email And Viewing It.



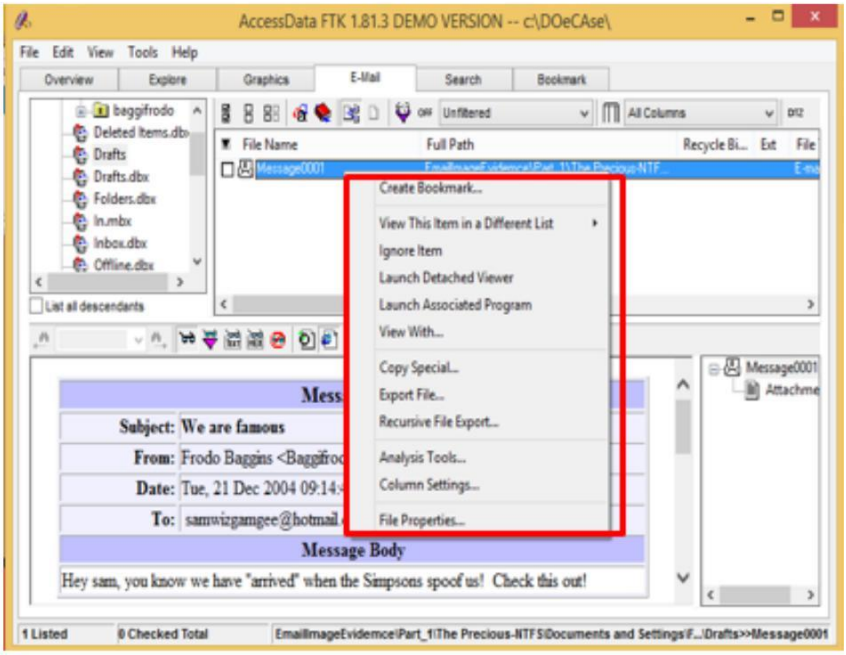
Step-8: Additional Steps Can Be Performed Like,

Exporting The File

Performing Analysis w.r.t SHA,MD5

And Many More.

To Do So, Right Click The Desired Email And Select The Required Option.



Signature :

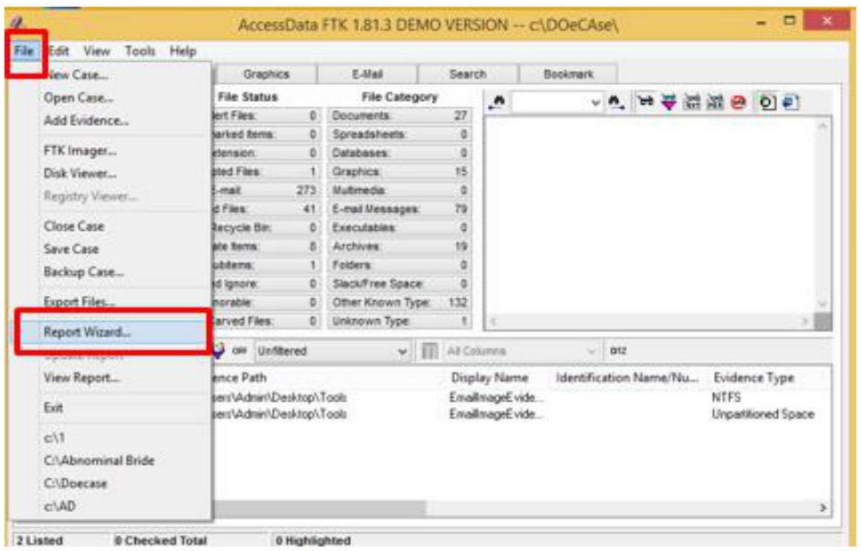
Practical 9

Aim: **Writing Reports Using FTK [Access Data FTK]**

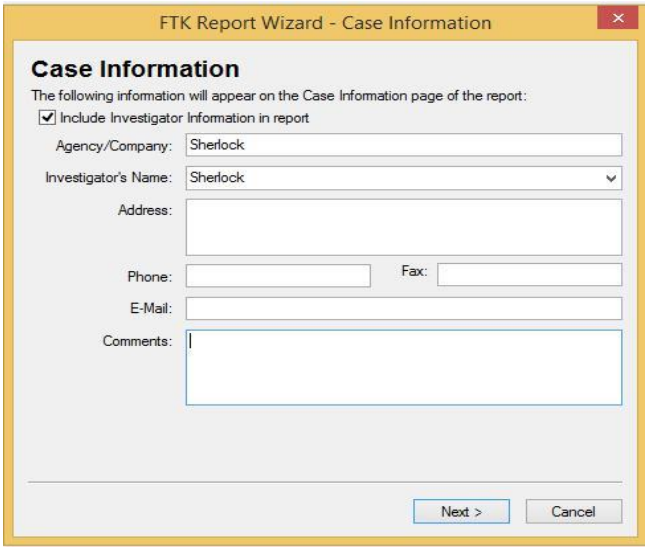
Step-1: Open Access Data FTK

Step-2: Start A New Case Or Load An Existing Case By Adding Evidence And Filling In Required Information

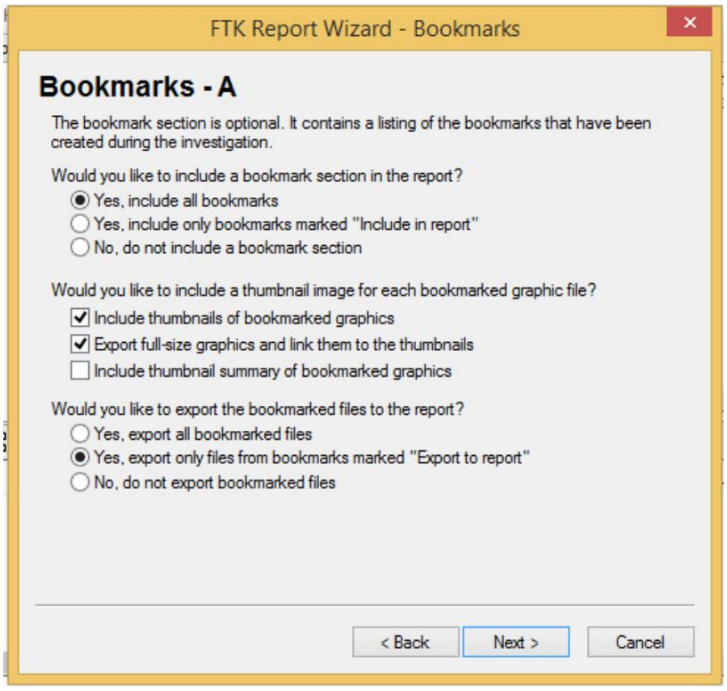
Step-3 To Generate A Report, Report Wizard Needs To Be Started, Go To File Menu, Click Report Wizard.

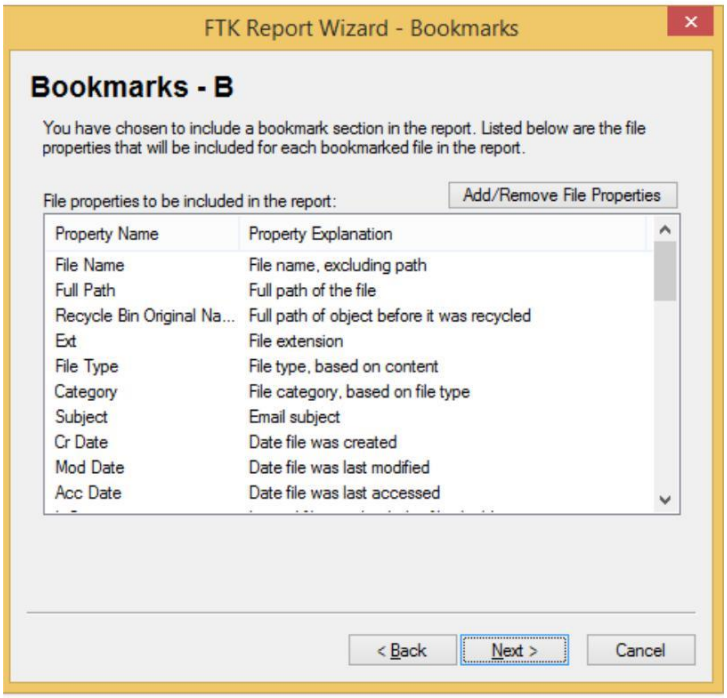


Step-4: In The Resulting Dialog Box, Fill The Necessary Information

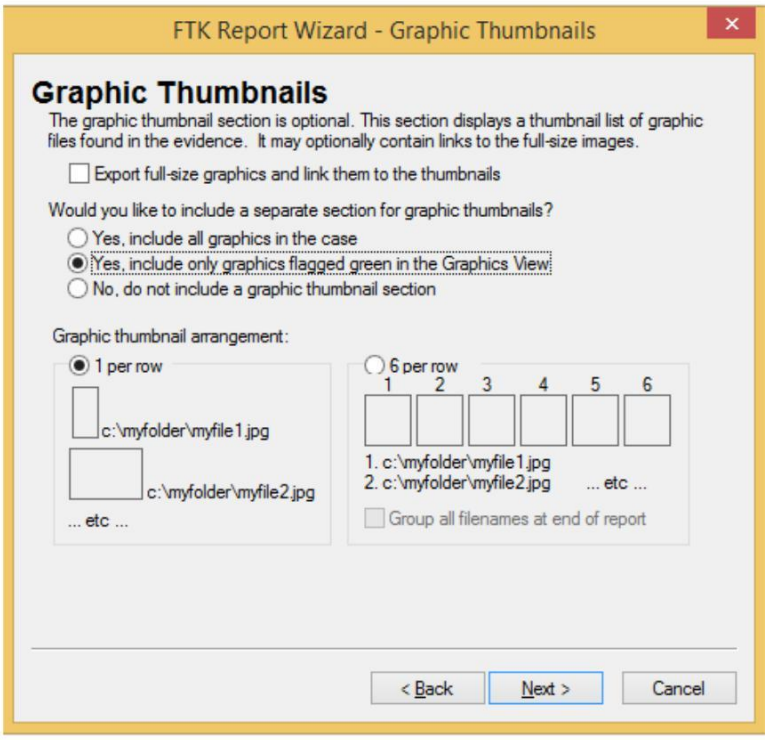


Step-5: Configuring Bookmarks Information

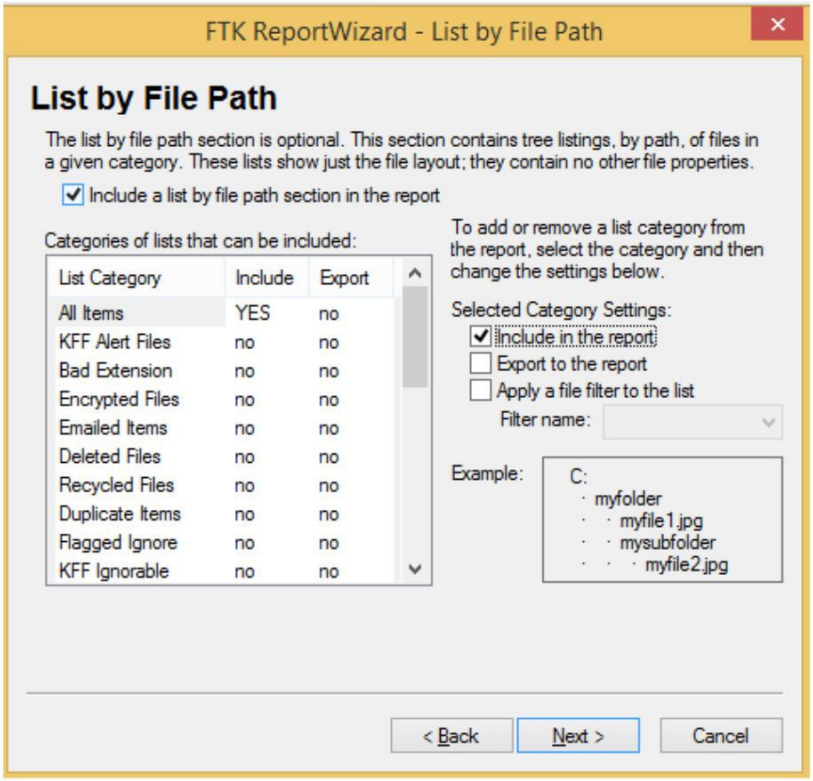


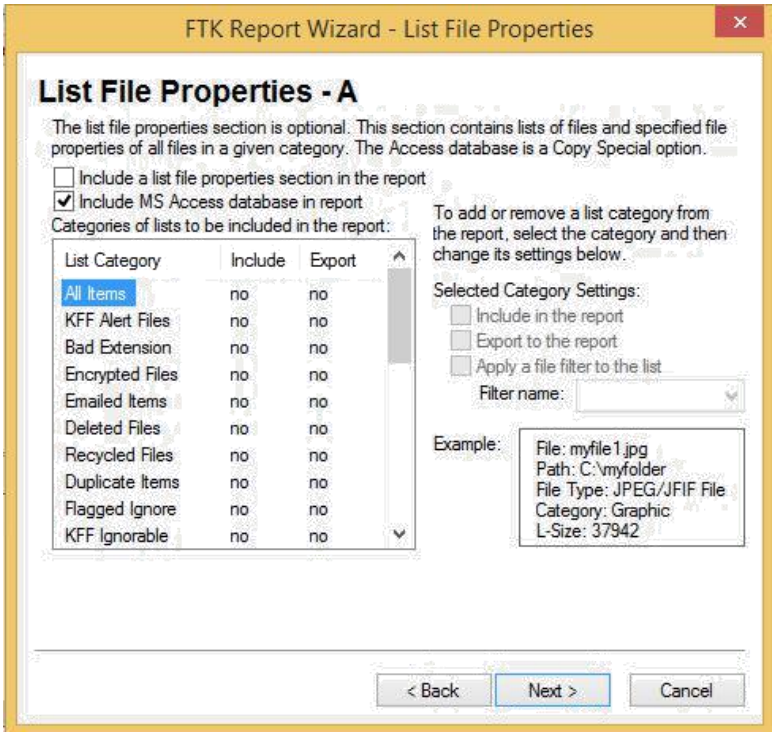


Step-6: Configuring Graphics Information

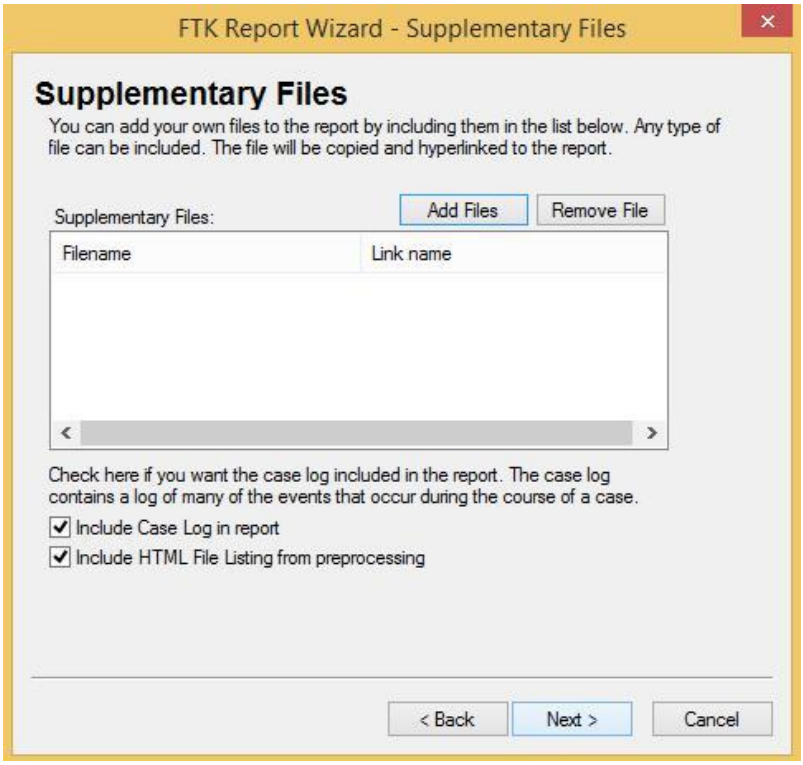


Step-7: Configuring File Listing

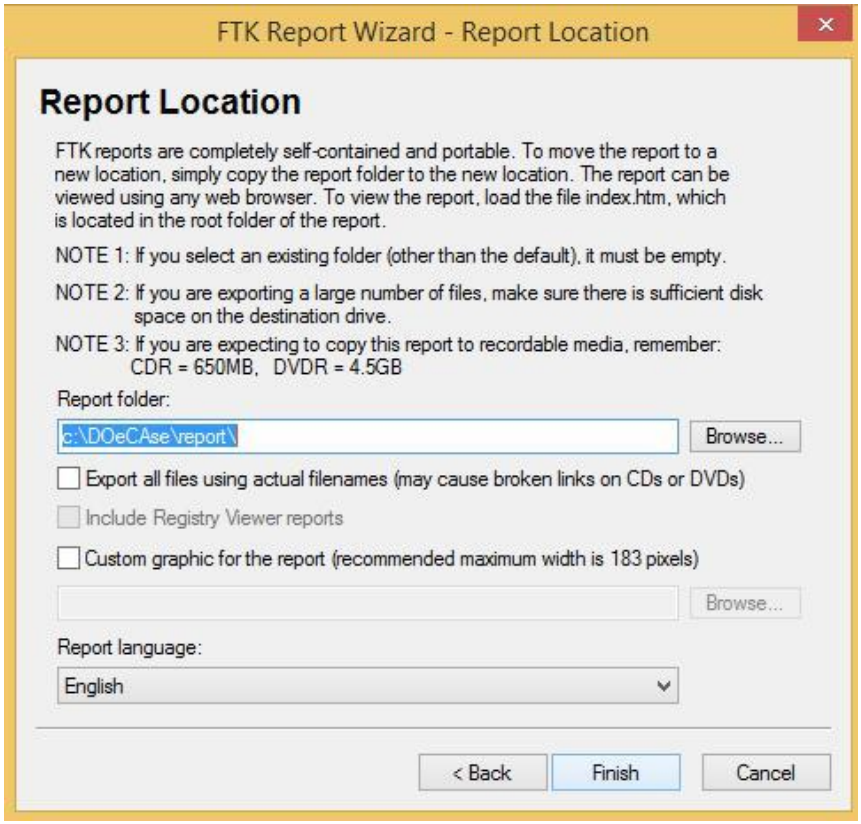




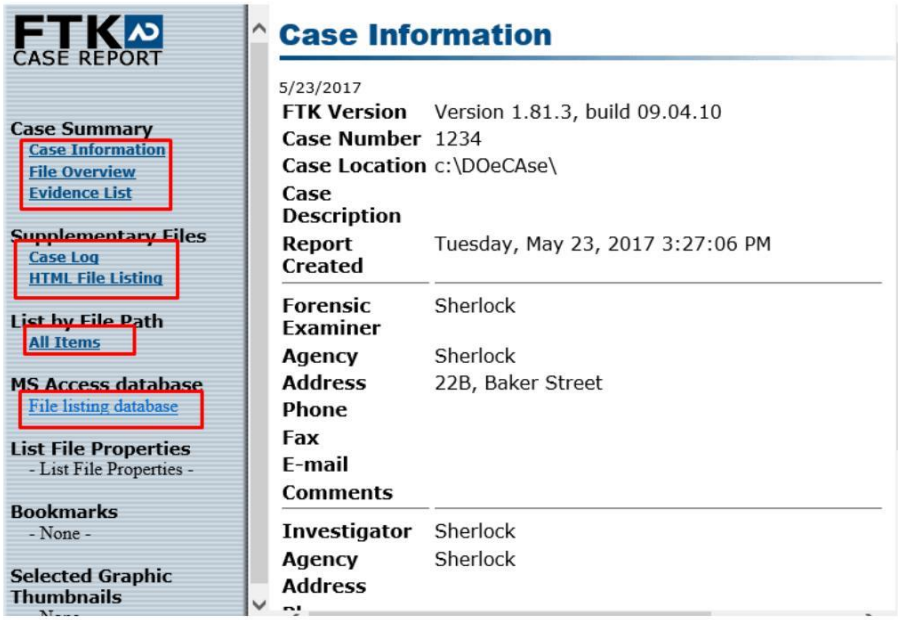
Step-8: Adding Supplementary Files If Needed.



Step-9: Provide The Location Where The Report Should Be Saved And Click Finish.



Step-10: Finally The Report Can Be Viewed & The Information About The Case Can Be Seen.



Signature:

Practical 10

Aim: **Performing Password Cracking [Cain & Abel]**

Step-1: Make Sure That pwdump(Password Hashing Tool) & Cain & Abel Are Installed

Step-2: Creating Users

Open Command Line As Administrator

Type In Command

net user username password /add

Here, Username & Password Can Be Used As Desired
Create 2-3 users.

To Add Simple Password Like 1234 or 5star etc Make Sure You Have Disabled The Password Complexity In The Windows

To Do So,

Go To Security Management (Windows + R) Enter secpol.msc
Go To Account Policies -> Password Policy
Disable The Password Must Meet Complexity Requirement Option

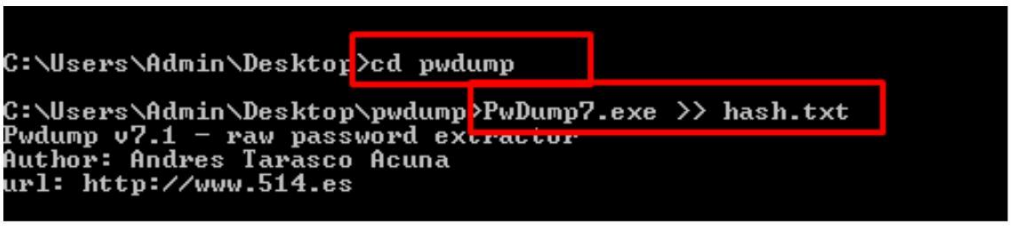
Step-3: Now Navigate To The pwdump Folder Present In Your System.

Type Command,

Pwdump7.exe >> hash.txt

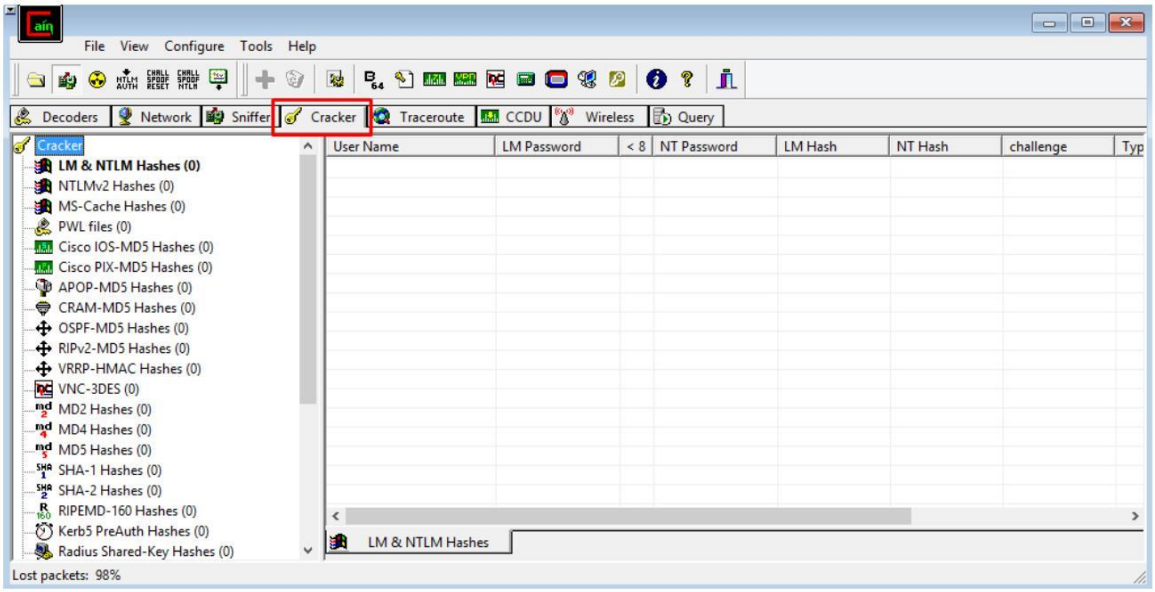
Pwdump7(We have installed The pwdump 7th release)

This Will Create The Hashes Of The Passwords Of The User Accounts & Store It In File Named hash.txt In The Same Folder.

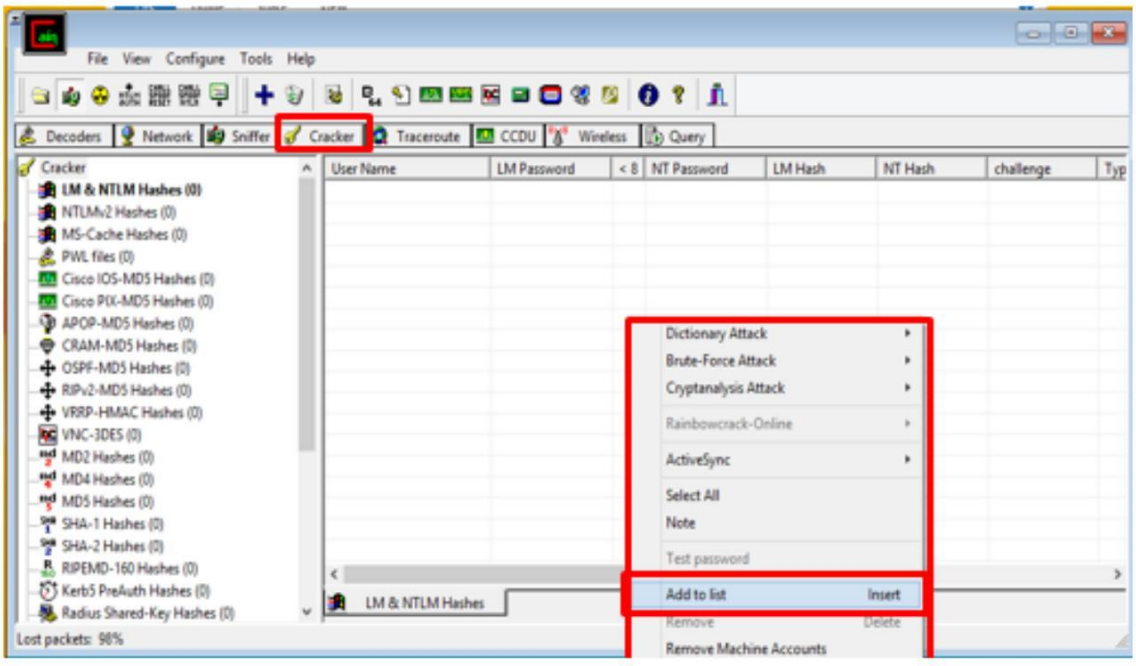


Step-4: Start Cain & Abel As Administrator

Step-5: Go To The Cracker Tab



Step-6: Right Click On The White Window Present In The Cracker Tab.
Click Add To List In The Resulting Popup Window.

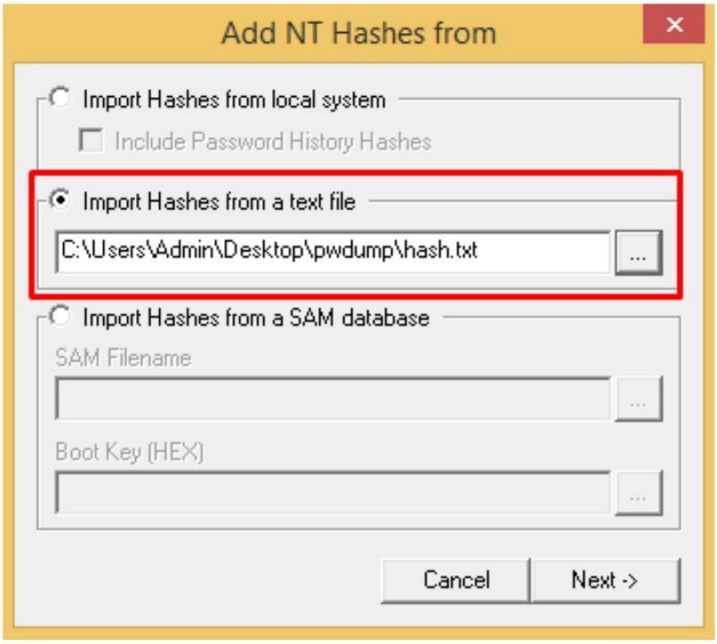


Step-7: In The Resulting Popup,

Select Import Hashes From A Text File.

Load The Hash File Obtained Using pwdump.

Click Next.



Step-8: It Will Present The List Of The Users On The System With Their Selected Attributes.

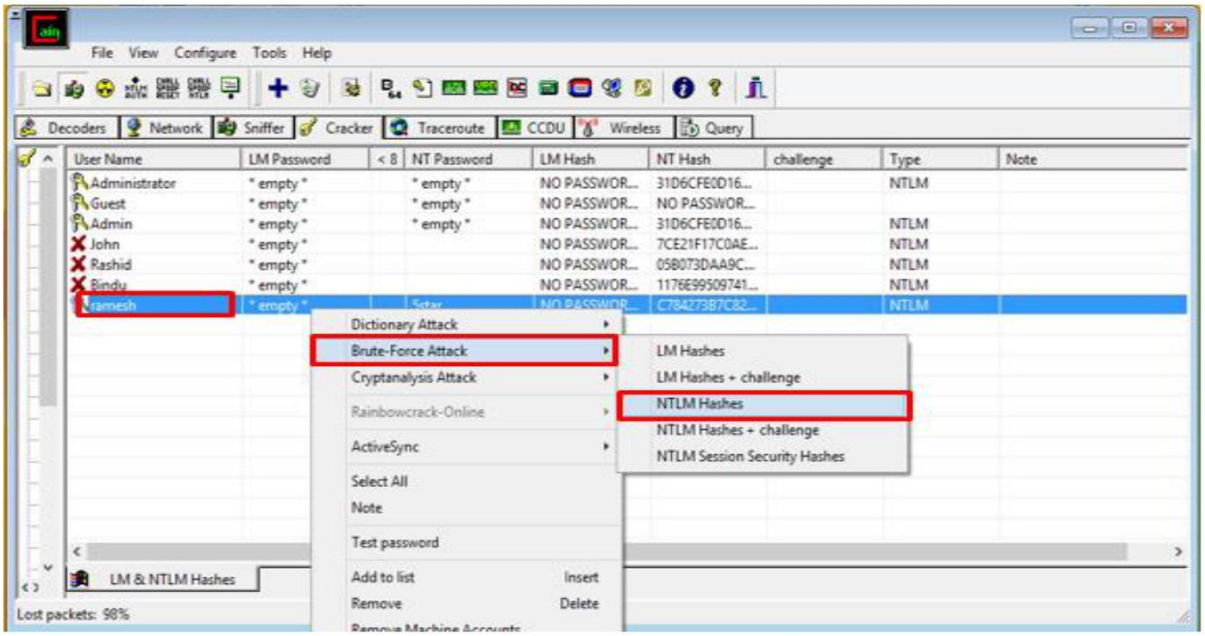
User Name	LM Password	< 8	NT Password	LM Hash	NT Hash	challenge	Type	Note
Administrator	* empty *		* empty *	NO PASSWOR...	31D6CFE0D16...		NTLM	
Guest	* empty *		* empty *	NO PASSWOR...	NO PASSWOR...			
Admin	* empty *		* empty *	NO PASSWOR...	31D6CFE0D16...		NTLM	
John	* empty *			NO PASSWOR...	7CE21F17C0AE...		NTLM	
Rashid	* empty *			NO PASSWOR...	05B073DAA9C...		NTLM	
Bindu	* empty *			NO PASSWOR...	1176E99509741...		NTLM	
ramesh	* empty *			NO PASSWOR...	C784273B7C82...		NTLM	

Step-9: Select An Account,

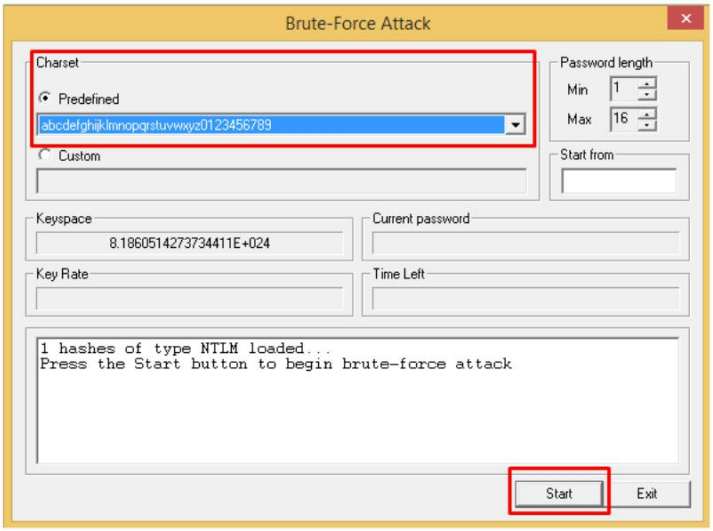
Right Click On That User Account

Select Brute-Force Attack

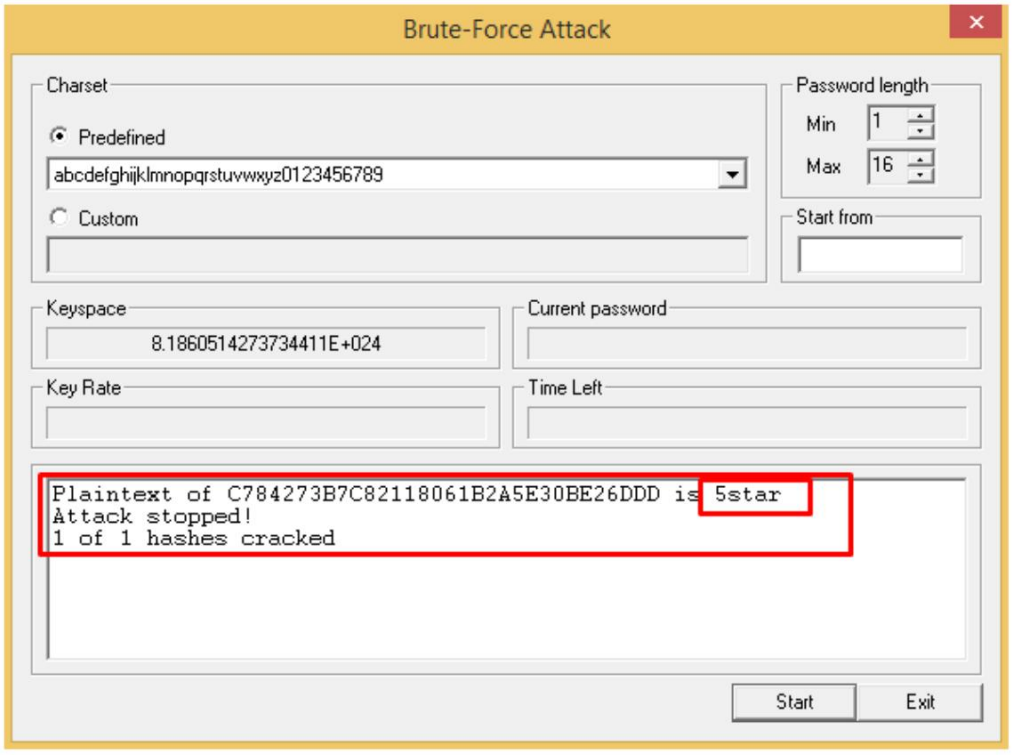
Select NTLM Hashes



Step-10: Select Relevant Charset & Click Start



Step-11: Once Start Is Clicked, The Application Will Process The Hash And Present With The Password For The Selected User Account.



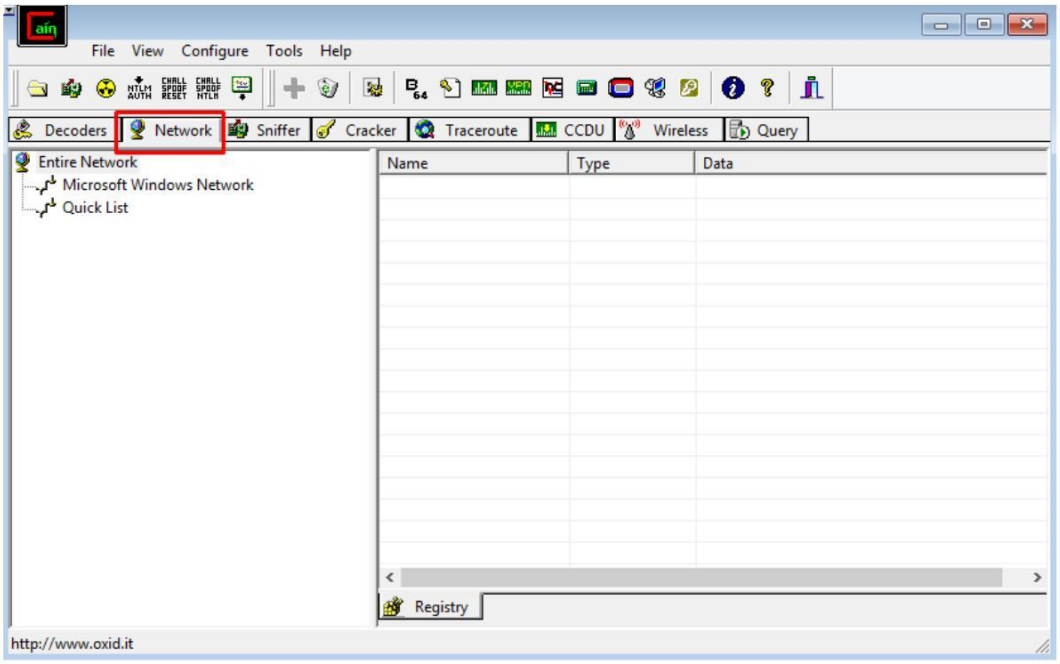
Signature:

Practical 11

Aim : **Managing Remote Registry, Network Enumeration, Services, s. IDs [Cain & Abel]**

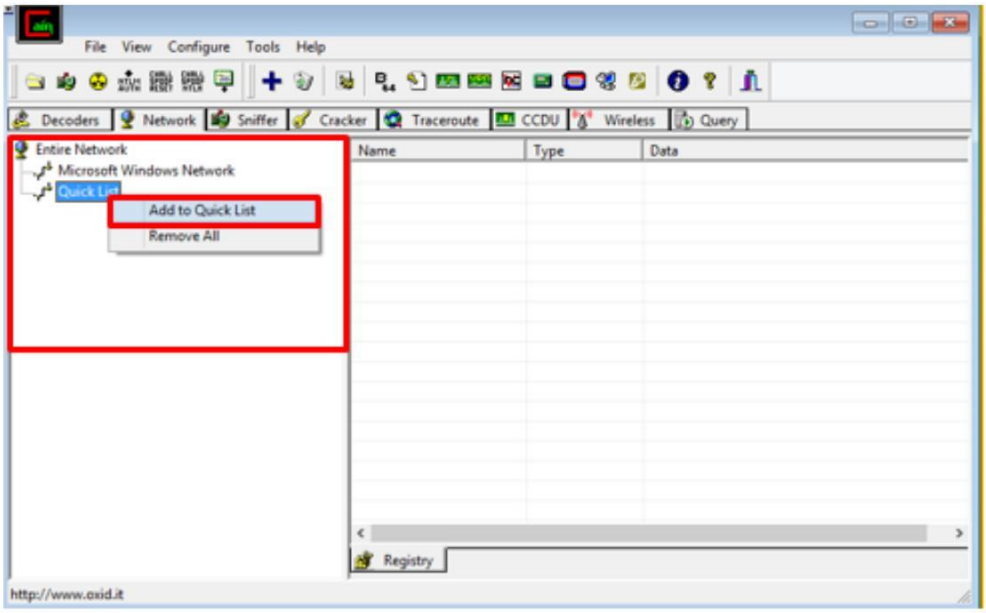
Step-1: Open Cain & Abel As Administrator

Step-2: Go To Network Tab

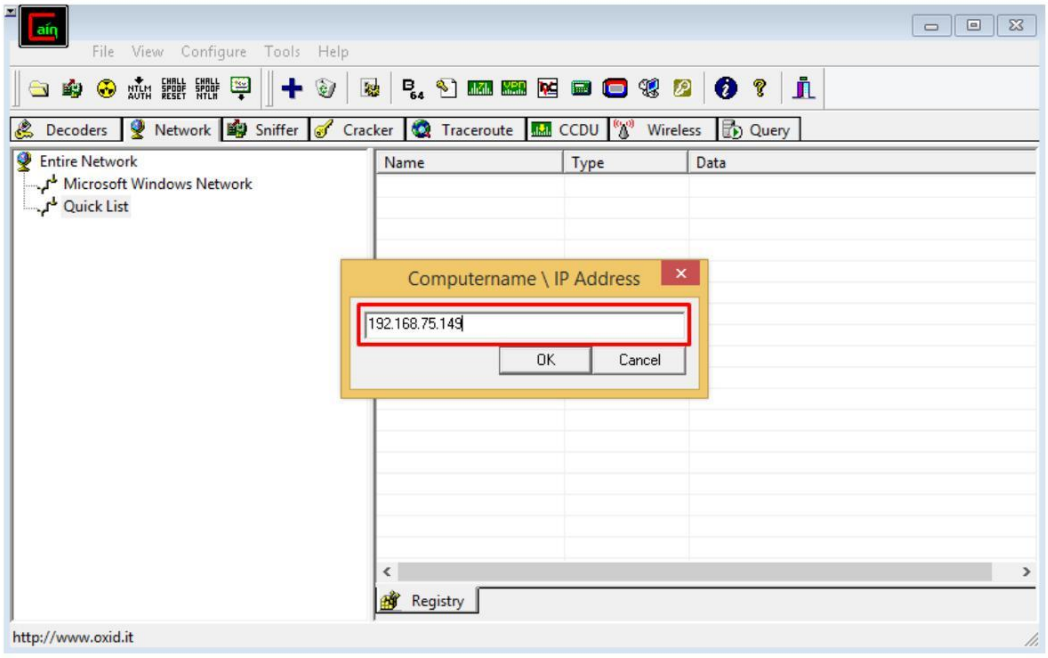


Step-3: Expand Entire Network

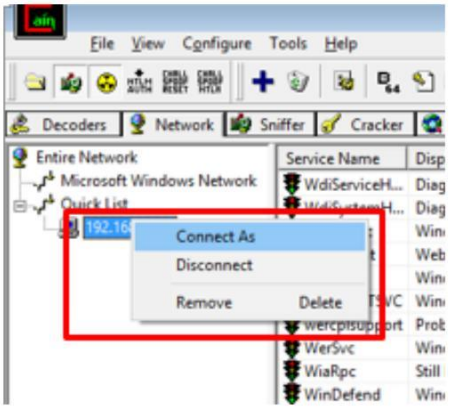
Right Click Quick List & Select Add To Quick List.



Step-4: In The Resulting Popup Box, Enter The IP Address Of The System You Want To Study (You Can Use Your Own System's IP Address To Examine Your Registry)

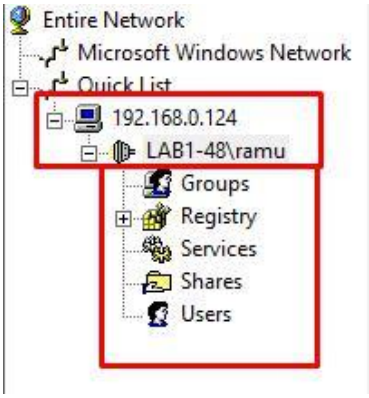


To Access Other System's Registry & Services, Use That System's IP Address Right Click On The Account And Enter User Credentials (Necessary Only If Using Accessing Other System)



Step-5: Double Click To Expand, This Will Provide Access To The

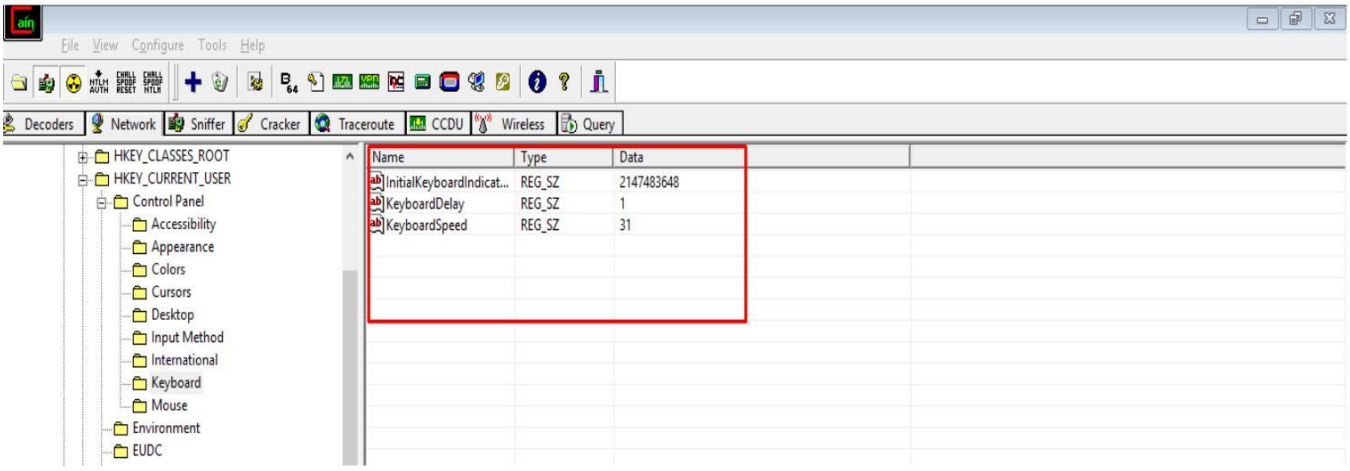
a. Groups
b. Registry
c. Services
d. Shares
e. Users



Step-6 Make Sure To Start 'Remote Registry' Service In Both The PCs,
Including Yours & The System You Are Investigating At.

a. Do Windows + R & Type services.msc
b. Start Remote Registry Service

Step-7 You Can Make Changes In The Registry By Traversing Through The Folders



Step-8: Changes Can Also Be Done In Services Section, Groups, Shares & Users (Network Enumeration) Can Be Viewed As Well.

Signature:

Practical 12

Aim: **Performing Sniffing [Cain & Abel]**

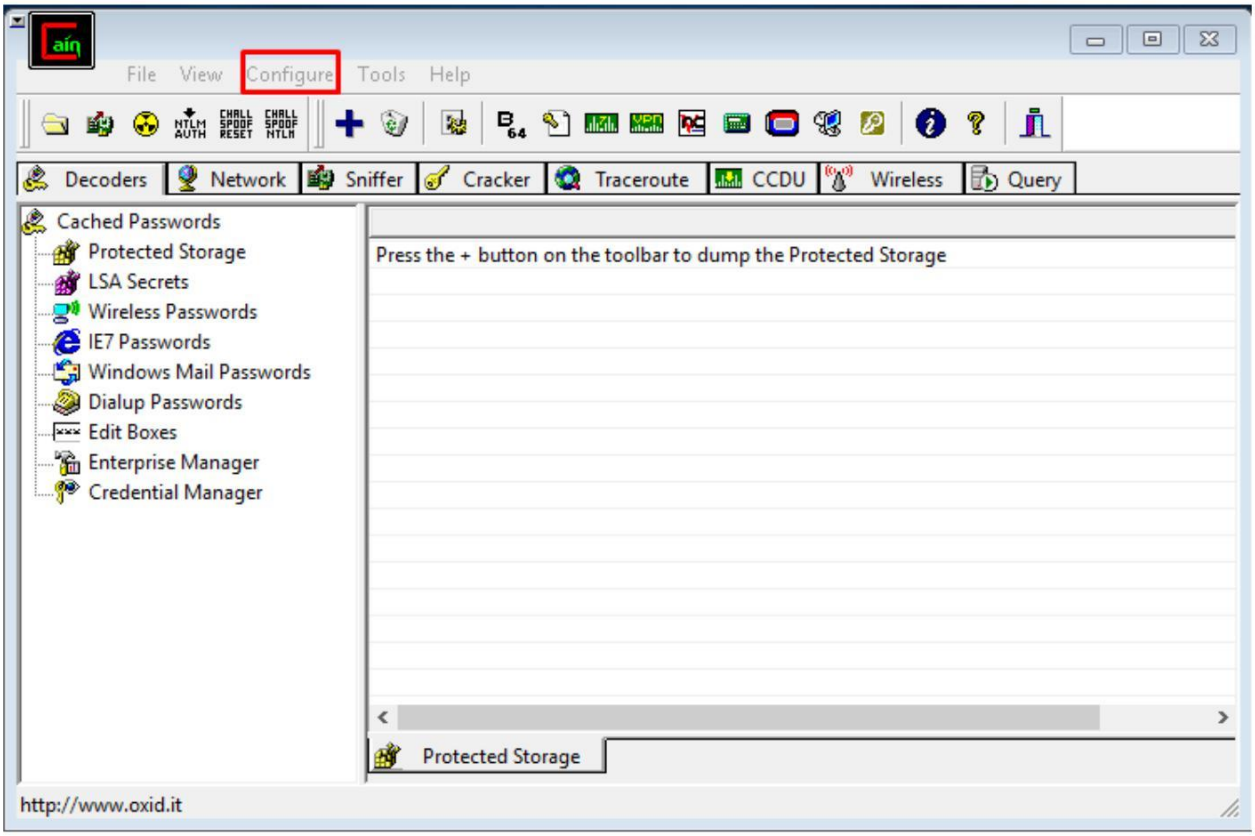
Steps :

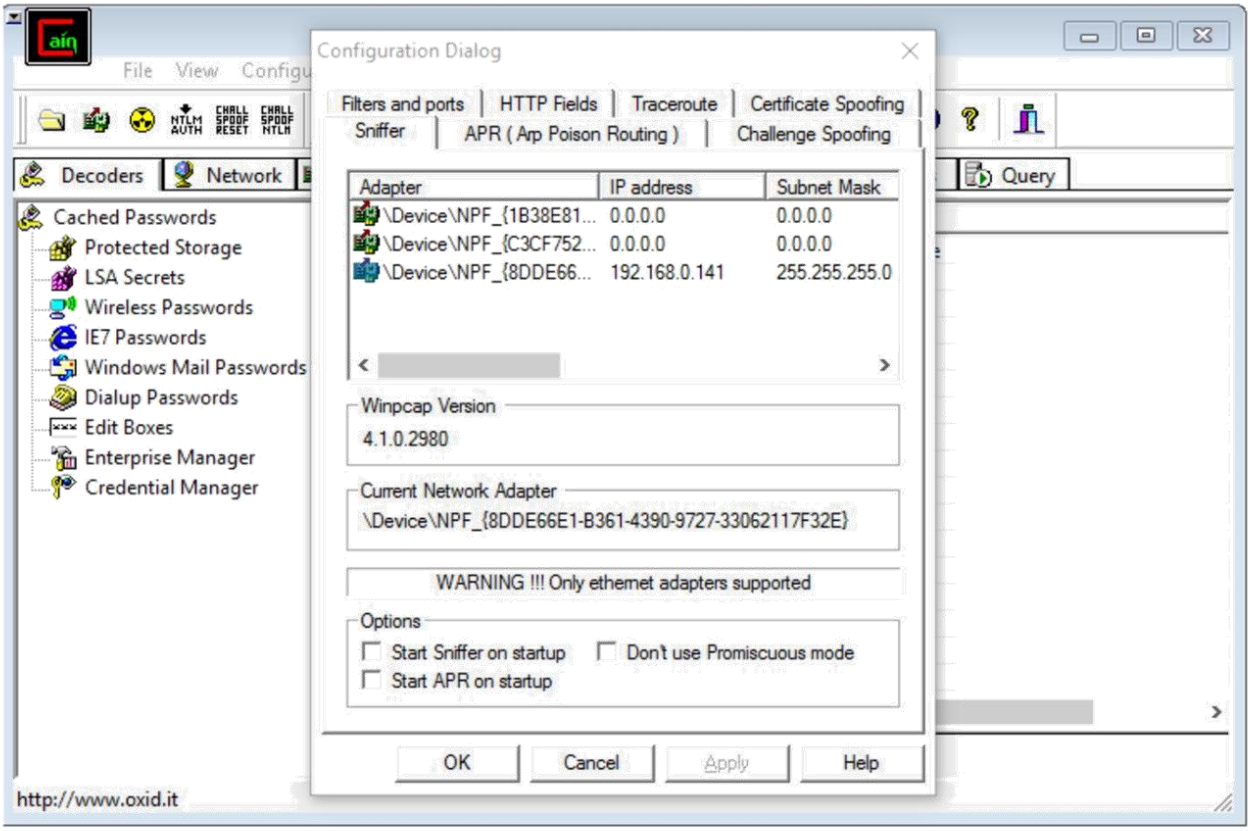
(Note : Go to command prompt & type ipconfig & note down your IP Address.)

1. Open Cain & Abel By Running It As Administrator.

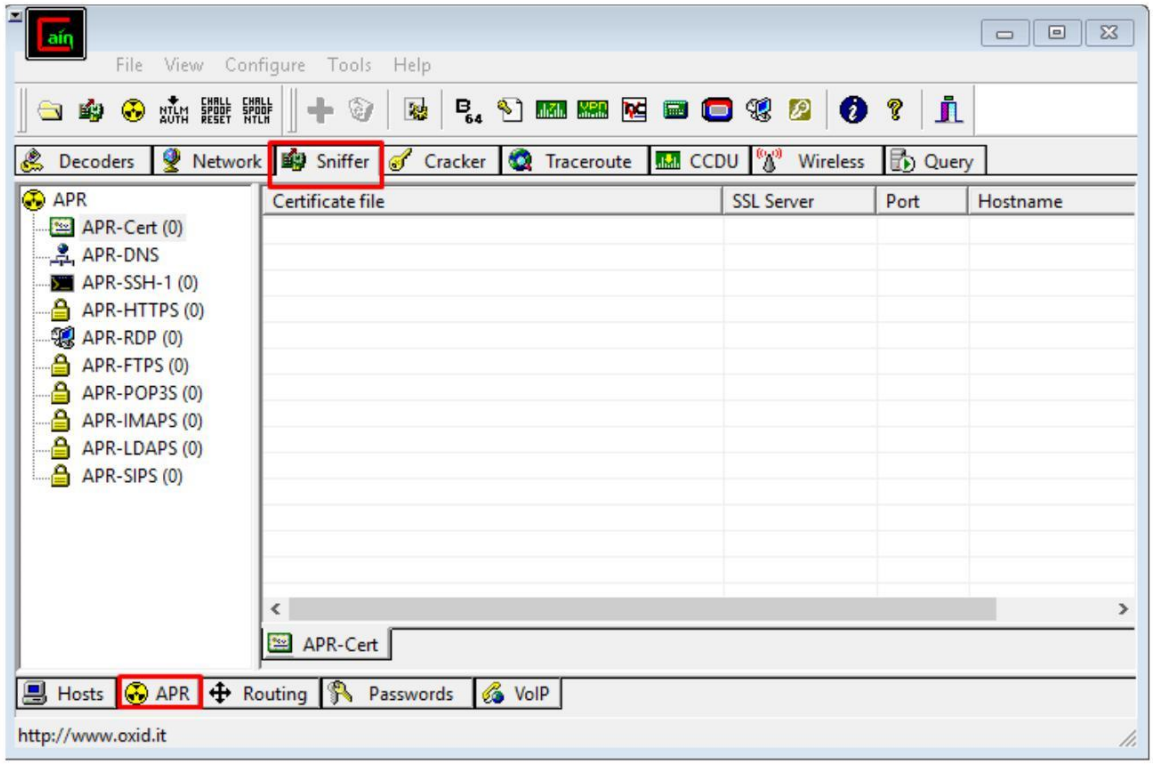
(Note: Firewall Exception Might Occur, Press OK)

2. Go To Configure & Select Your IP Address, Press Apply & OK.

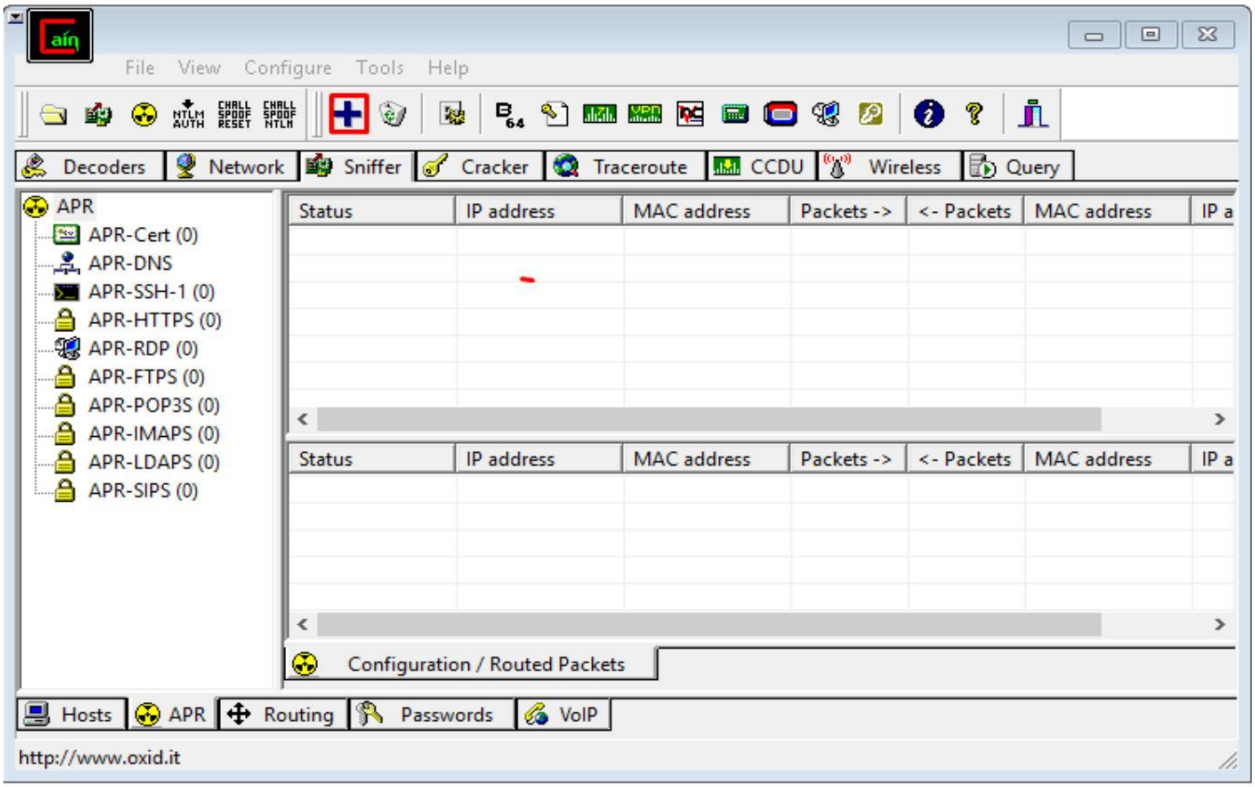




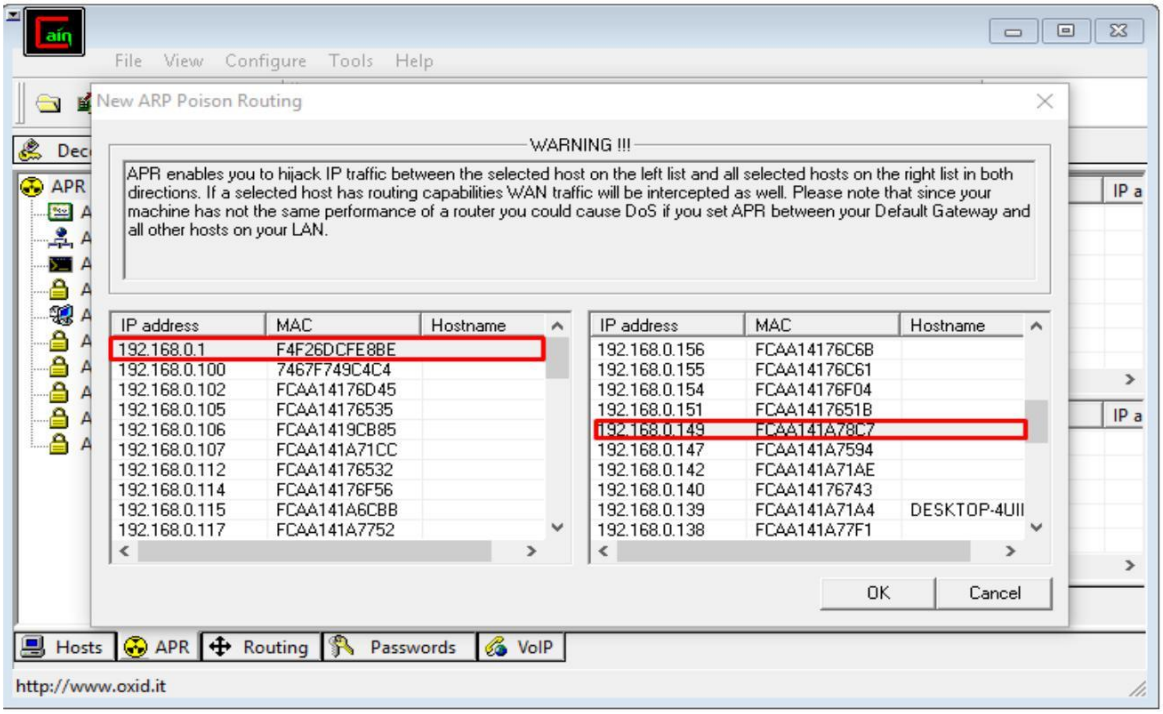
3. Now Go To Sniffer Tab On Top & Select APR Tab From Bottom.



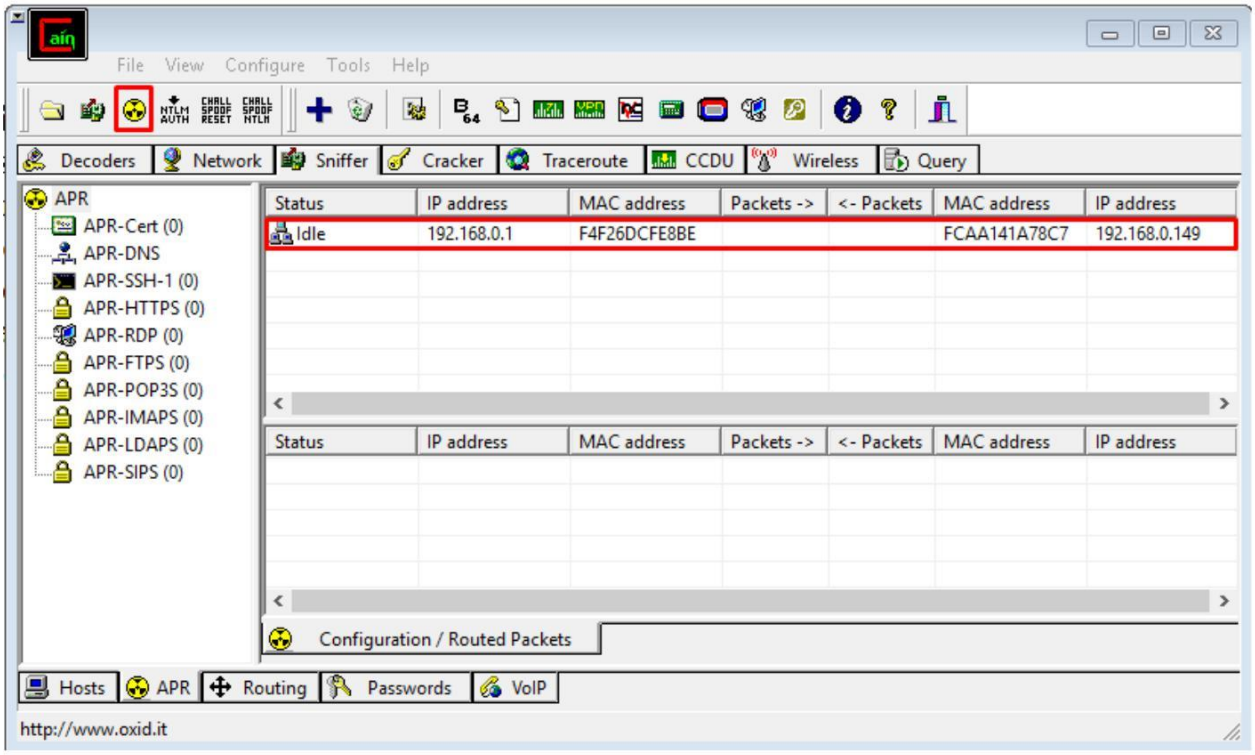
4. Single Click On The Right Above Part Of APR And Then Click On "+" Icon On Top Left.



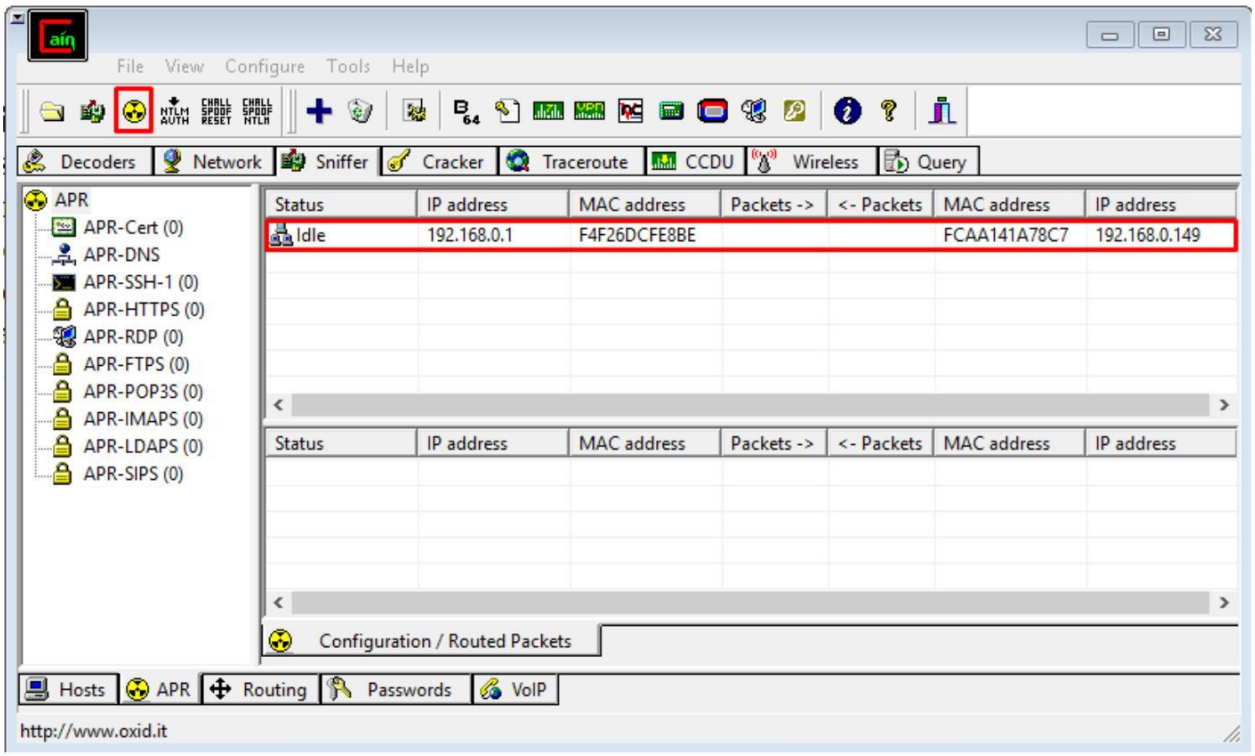
5. Now Select Your Subnet & Machine With The Target IP Address & Press OK.



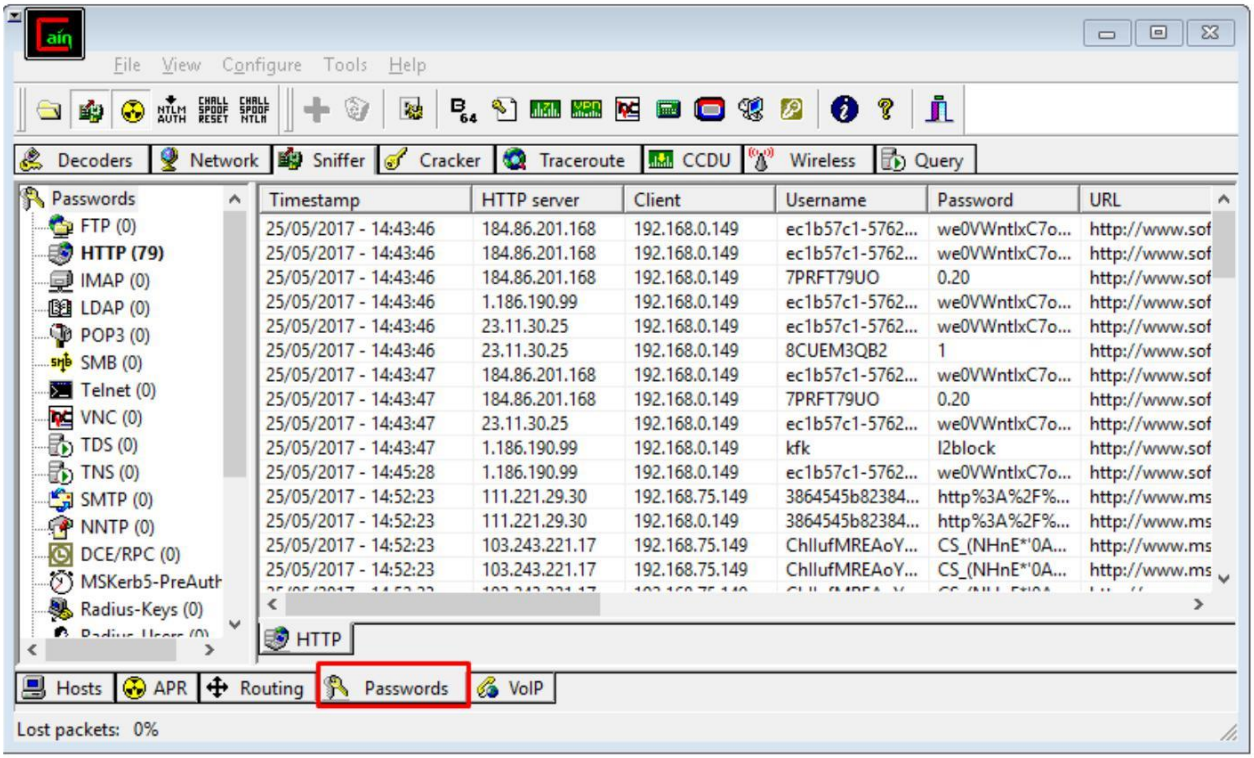
6. Select The Listed Machine & Click On Poison Icon On The Top Left.



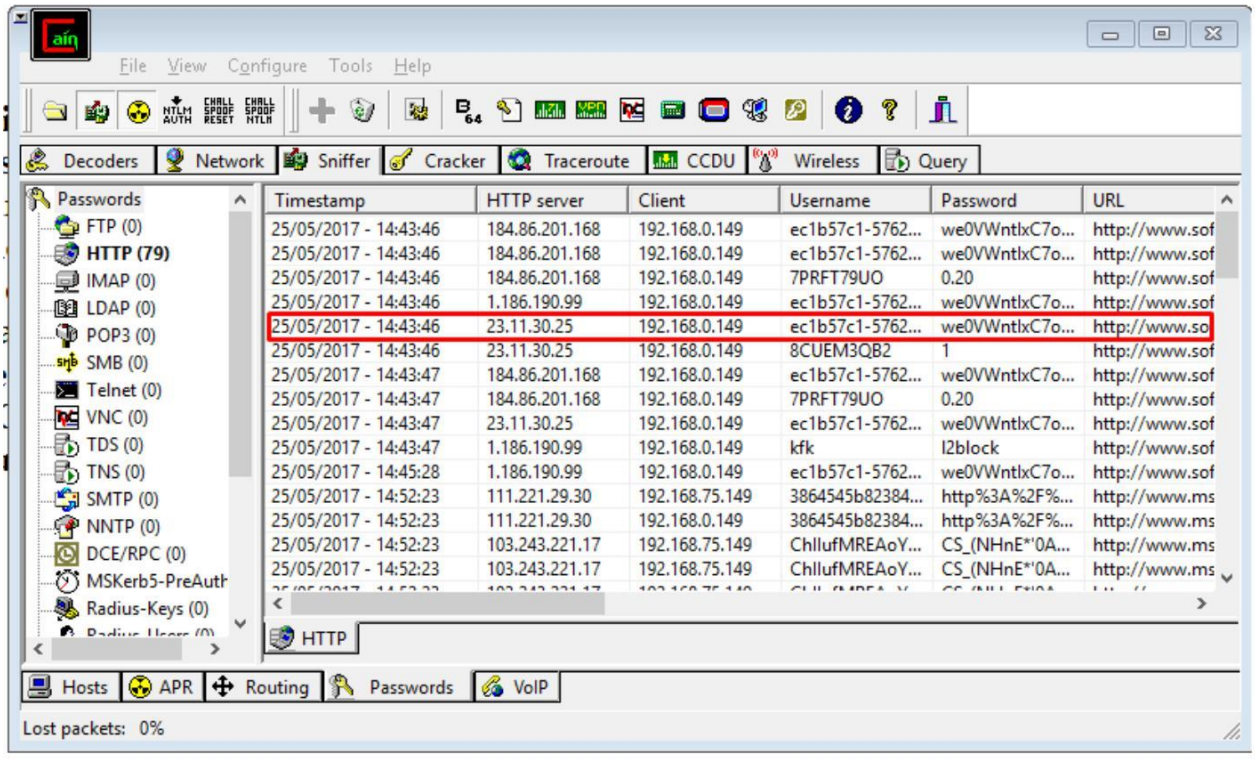
(Note : If You Get AN Exception : "Couldn't bind HTTPS acceptor socket", Press OK)



7. Go To Passwords Tab At The Bottom.



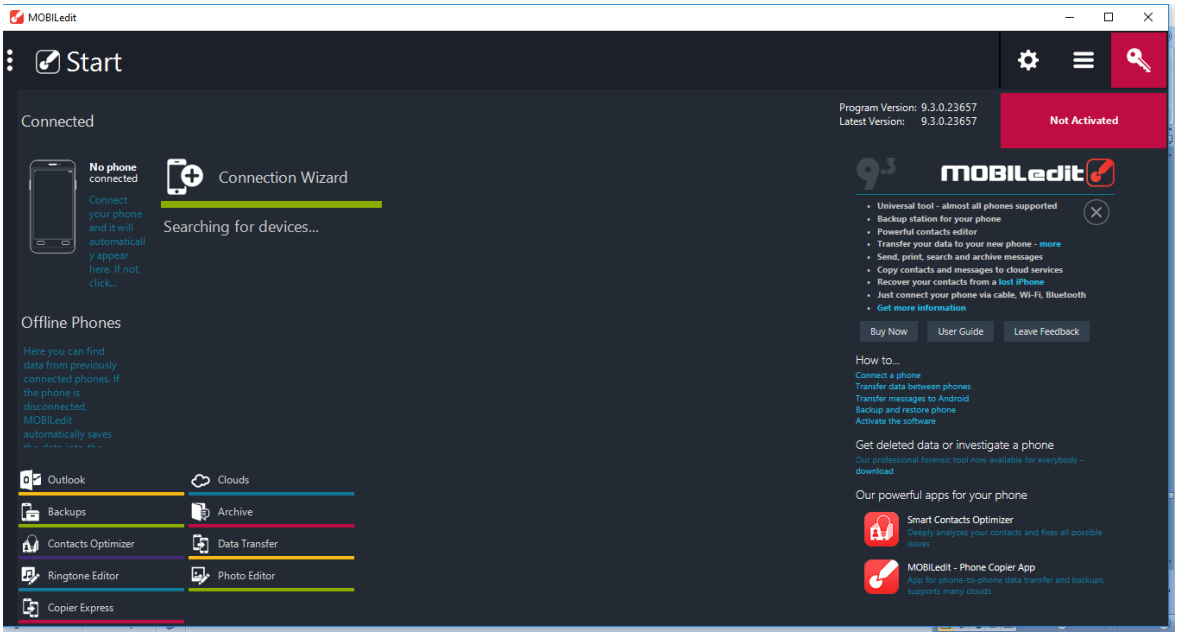
8. Sniffed Logs With All Information With Password Is Now Visible.

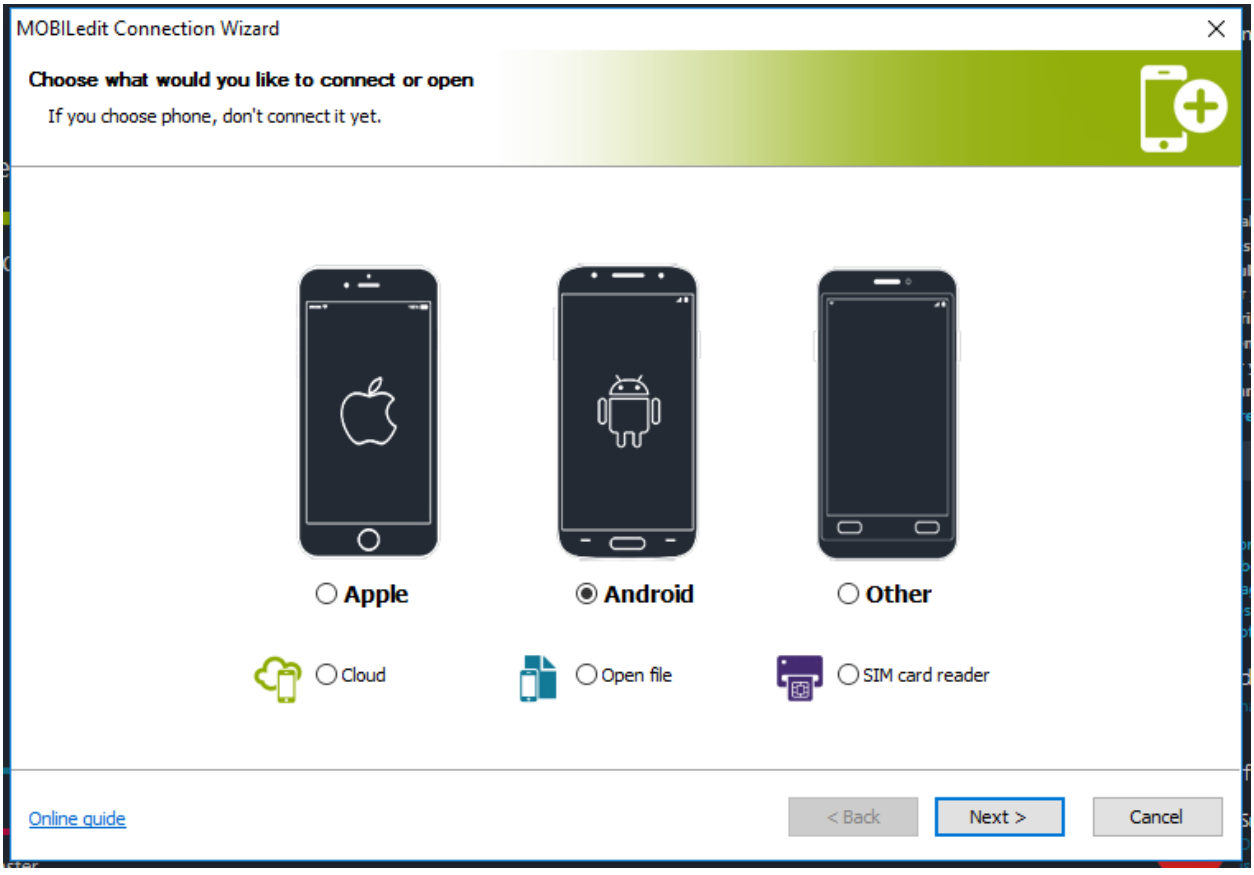


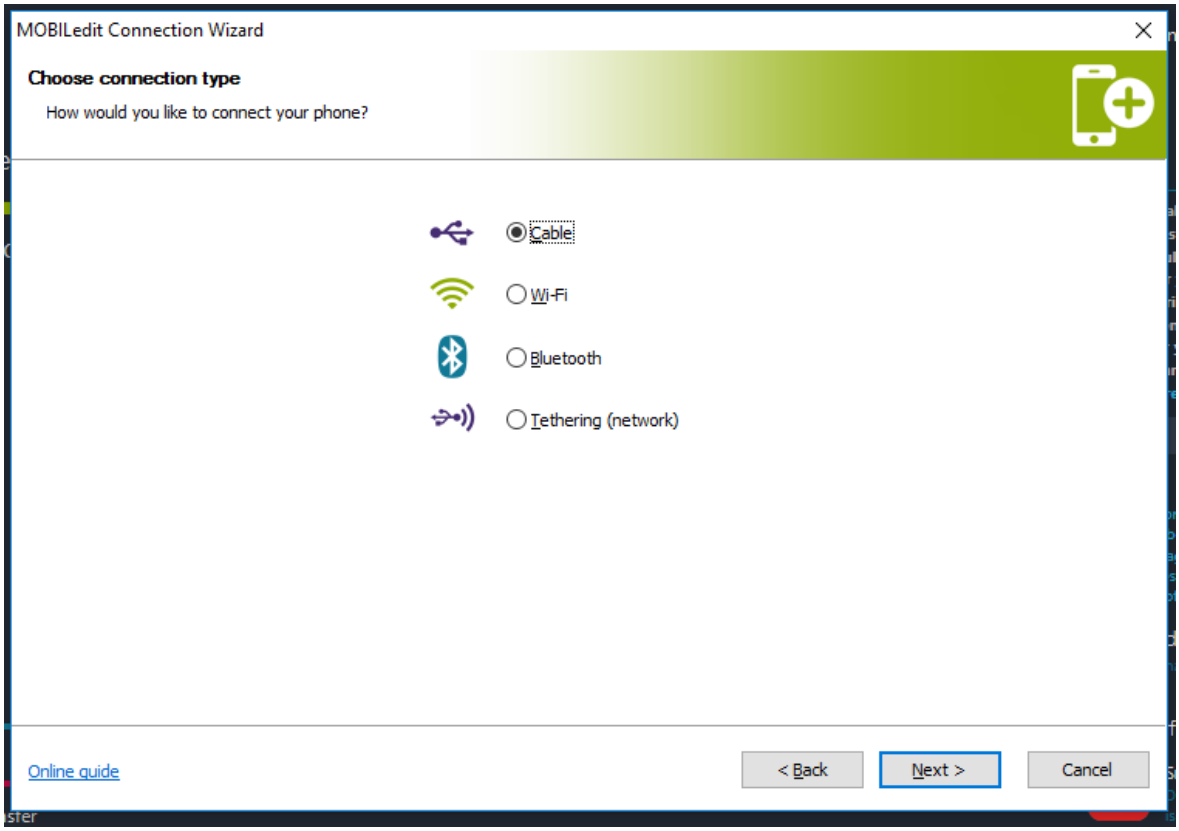
Signature:

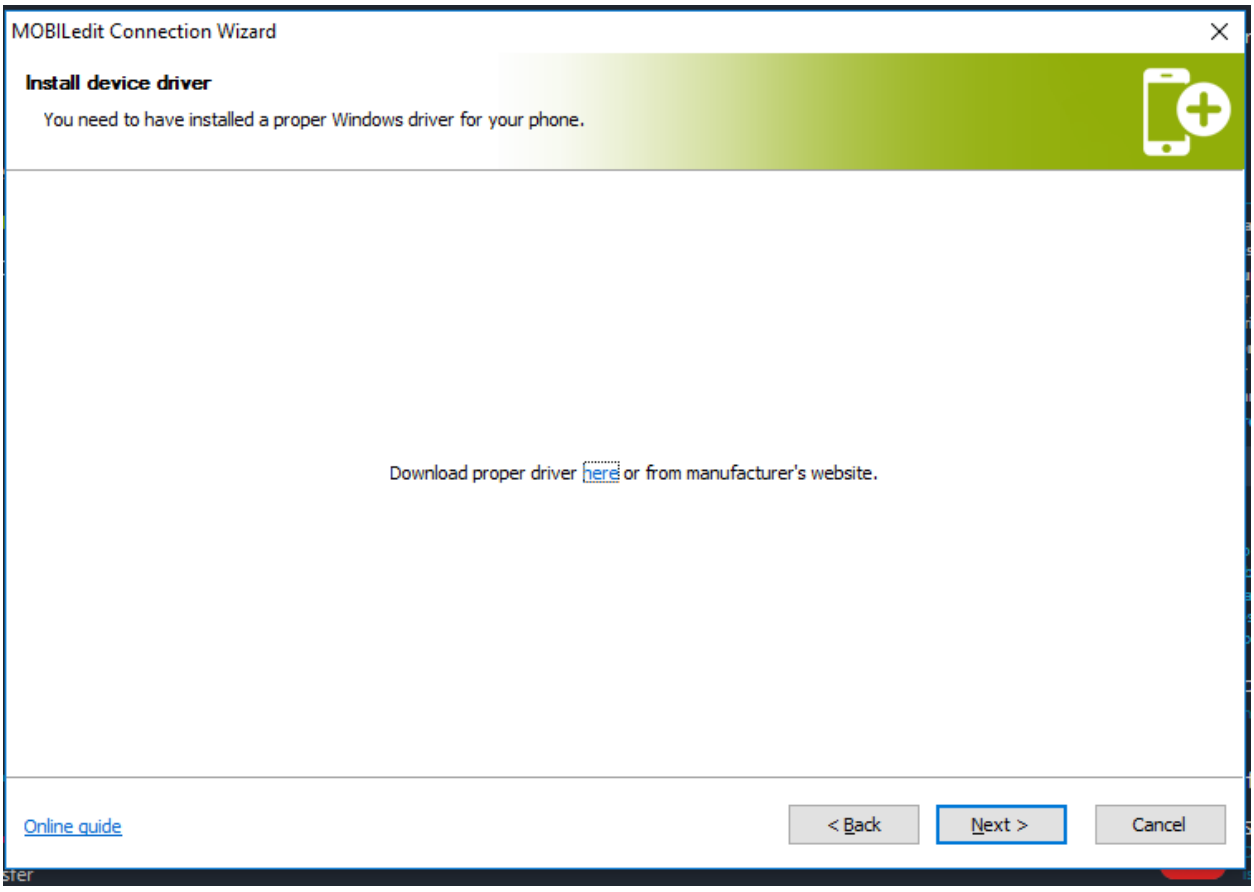
Practical 13

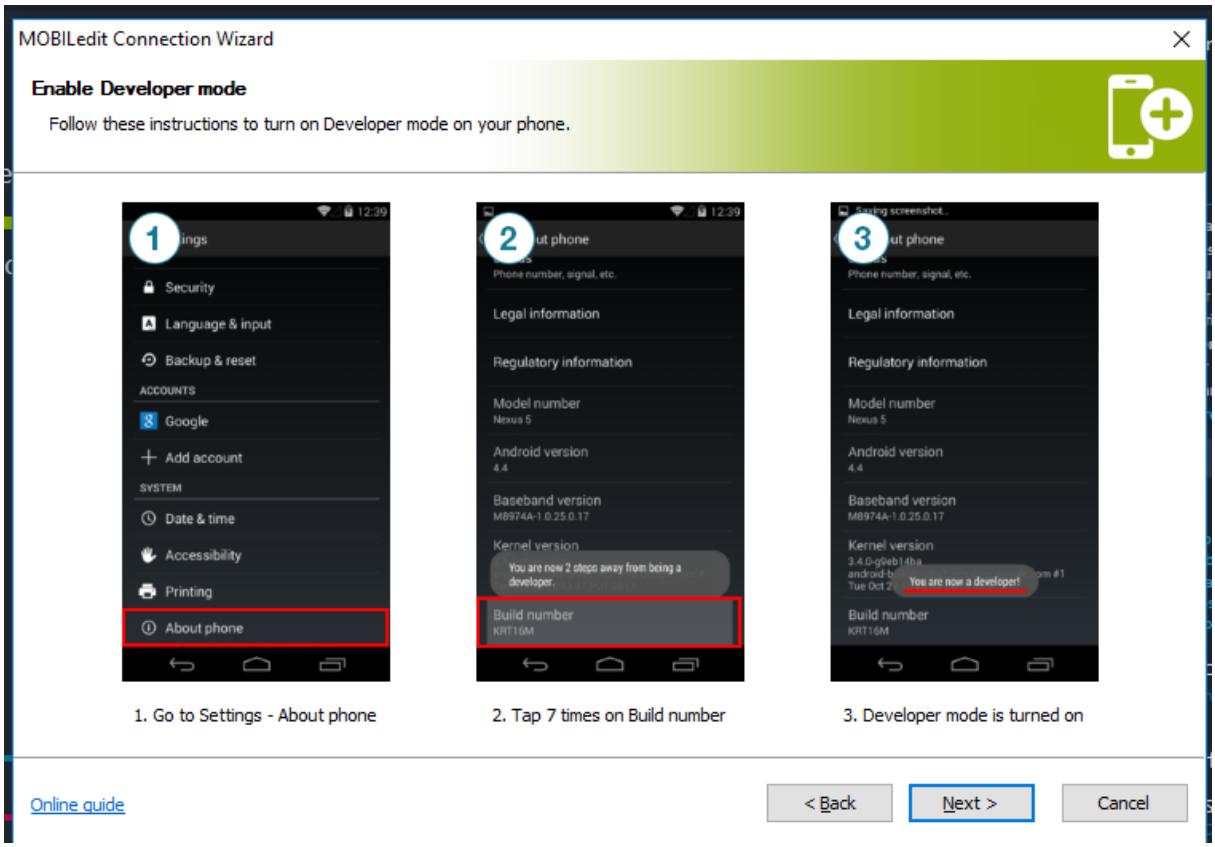
Aim: Using Mobile Forensics Tools[Mobiledit].

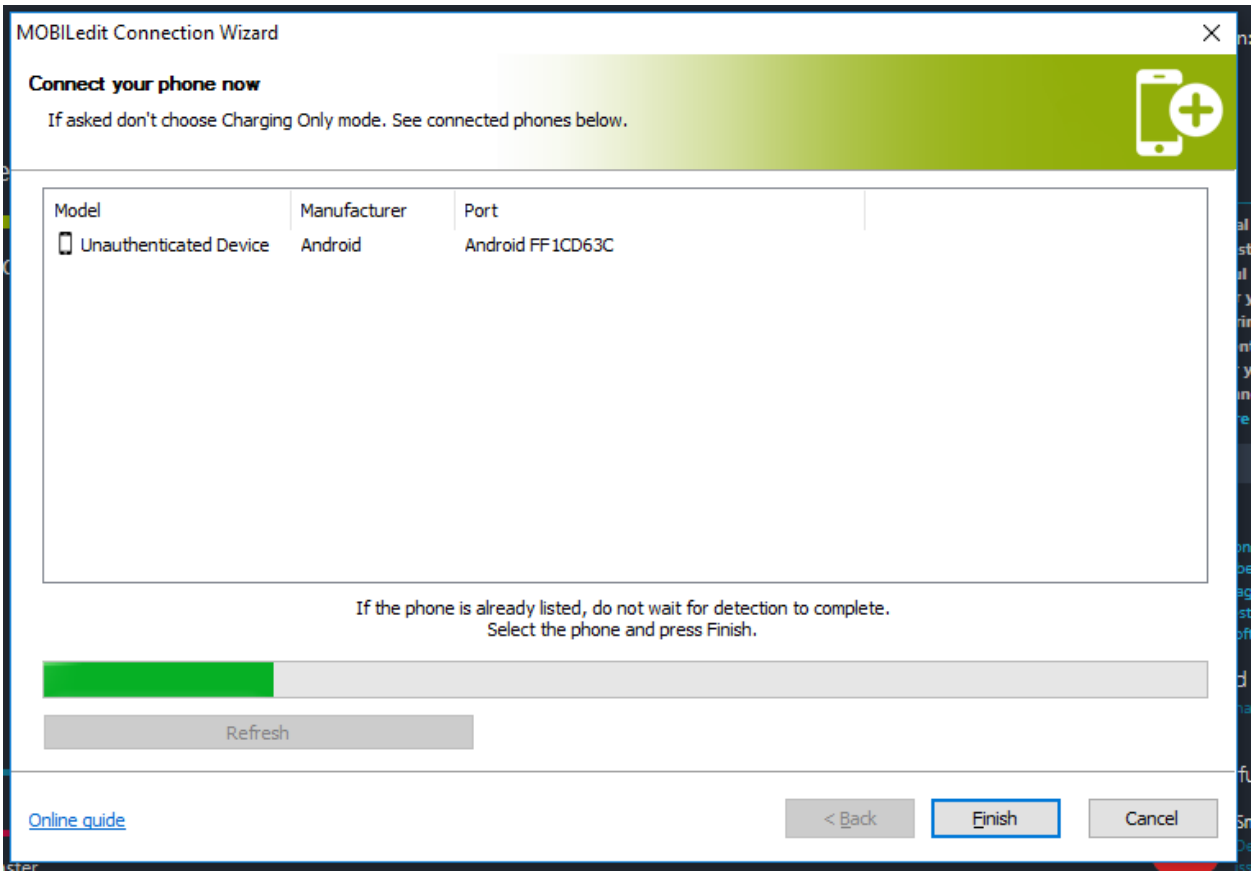


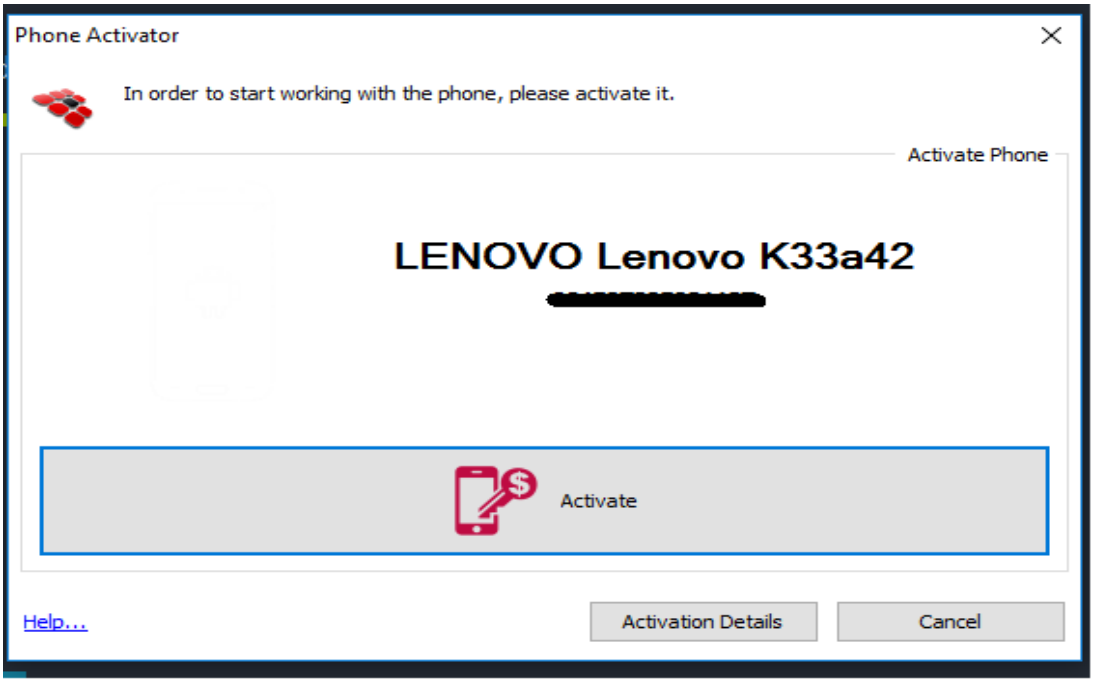


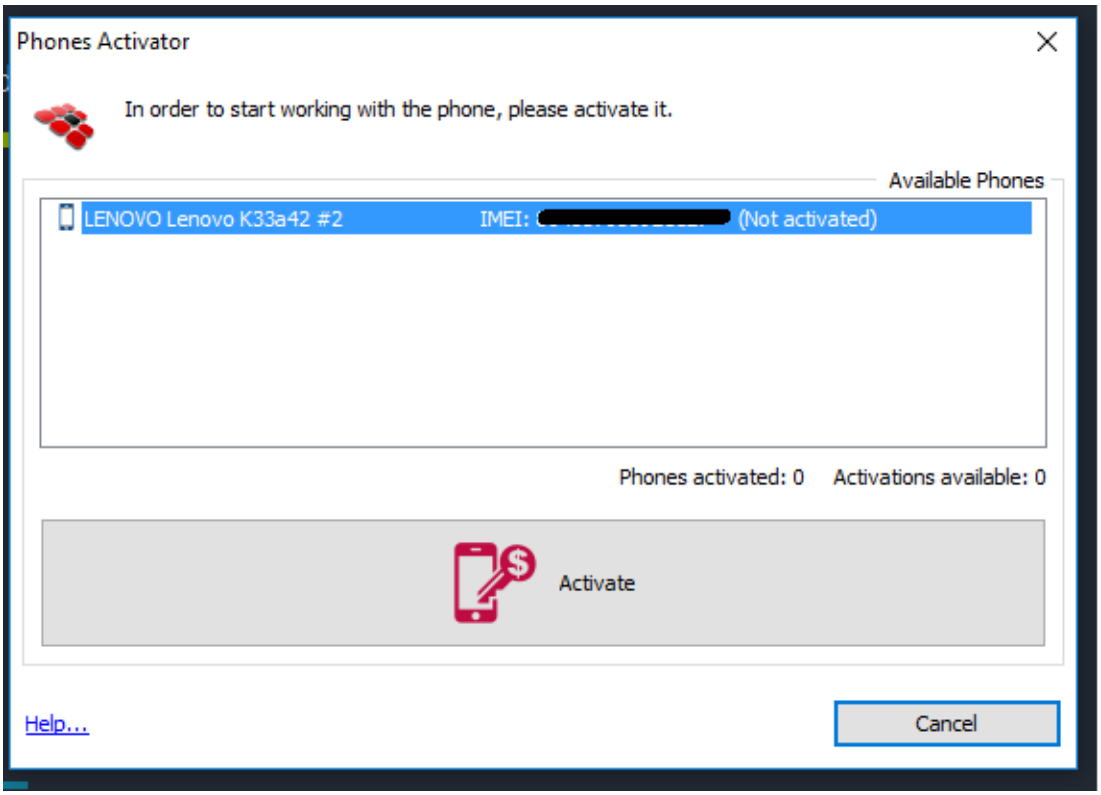

MOBILedit Connection Wizard
Choose connection type
How would you like to connect your phone?
Cable
Wi-Fi
Bluetooth
Tethering (network)
Online guide
< Back
Next >
Cancel

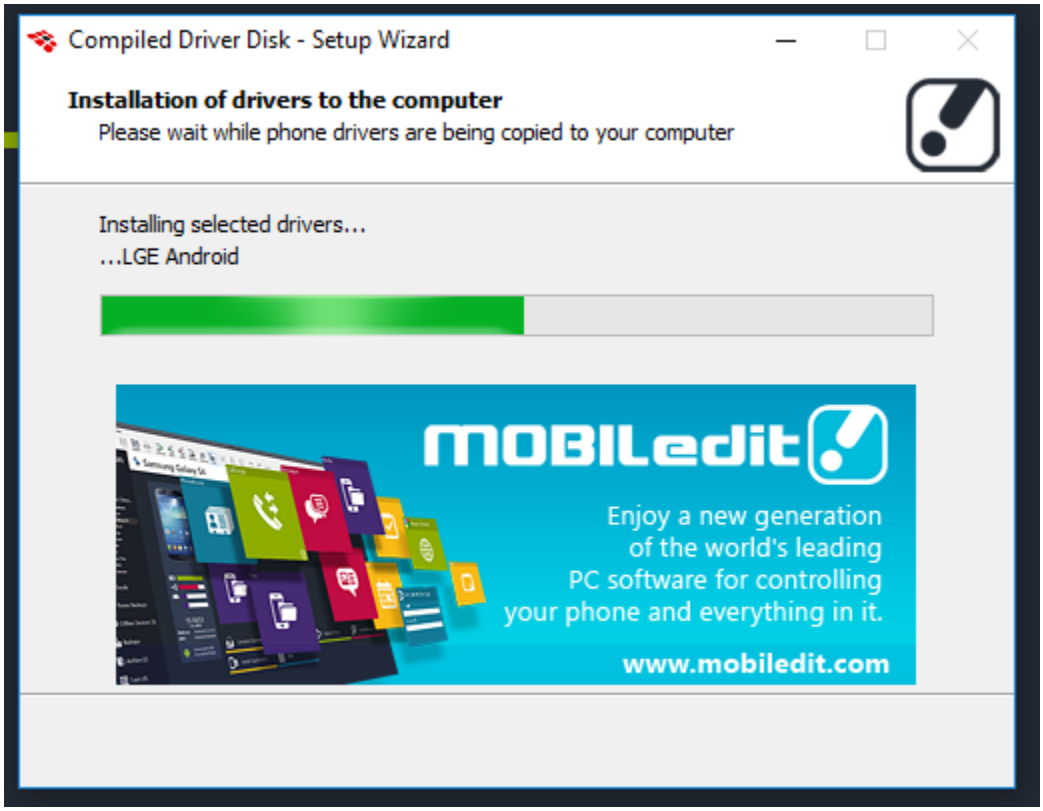

MOBILedit Connection Wizard
Install device driver
You need to have installed a proper Windows driver for your phone.
Download proper driver here or from manufacturer's website.
Online guide
< Back
Next >
Cancel


MOBILedit Connection Wizard
Enable Developer mode
Follow these instructions to turn on Developer mode on your phone.
1
Security
Language & input
Backup & reset
ACCOUNTS
Google
Add account
SYSTEM
Date & time
Accessibility
Printing
About phone
2
Legal information
Regulatory information
Model number
Android version
Baseband version
Kernel version
Build number
You are now 2 steps away from being a developer.
3
You are now a developer!
1. Go to Settings - About phone
2. Tap 7 times on Build number
3. Developer mode is turned on
Online guide
< Back
Next >
Cancel

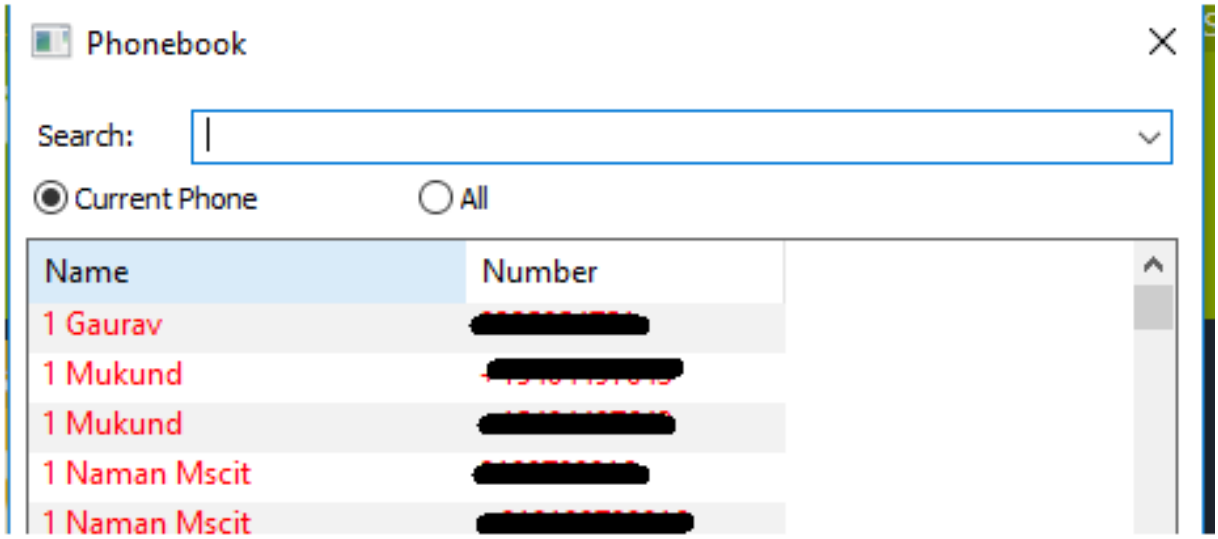

MOBILedit Connection Wizard
Connect your phone now
If asked don't choose Charging Only mode. See connected phones below.
Model
Manufacturer
Port
Unauthenticated Device
Android
Android FF1CD63C
If the phone is already listed, do not wait for detection to complete.
Select the phone and press Finish.
Refresh
Online guide
< Back
Finish
Cancel

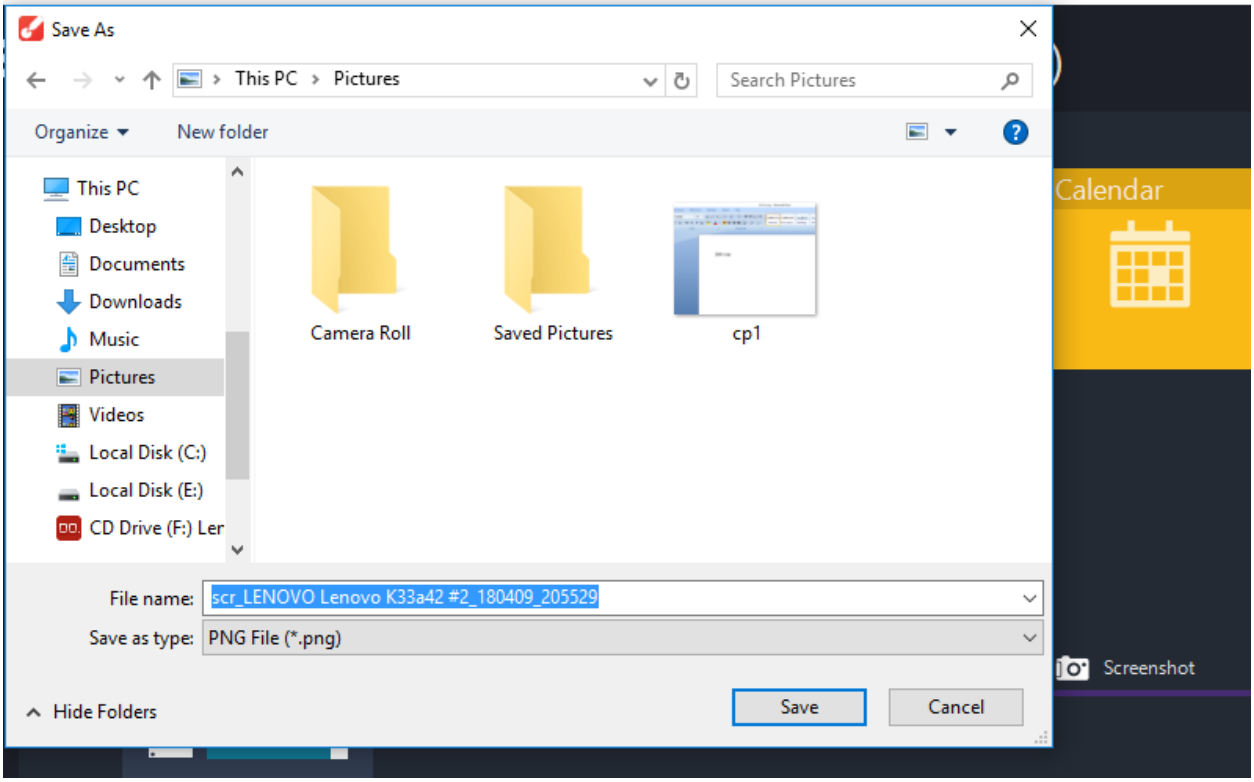

Phone Activator
In order to start working with the phone, please activate it.
Activate Phone
LENOVO Lenovo K33a42
[redacted]
Activate
Help...
Activation Details
Cancel

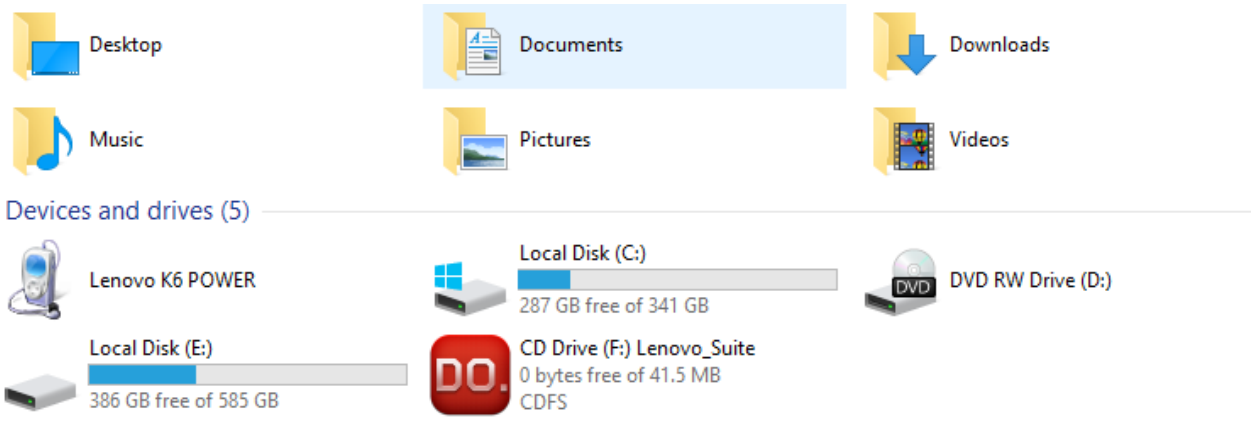

Phones Activator
In order to start working with the phone, please activate it.
Available Phones
LENOVO Lenovo K33a42 #2
IMEI: [redacted]
(Not activated)
Phones activated: 0
Activations available: 0
Activate
Help...
Cancel

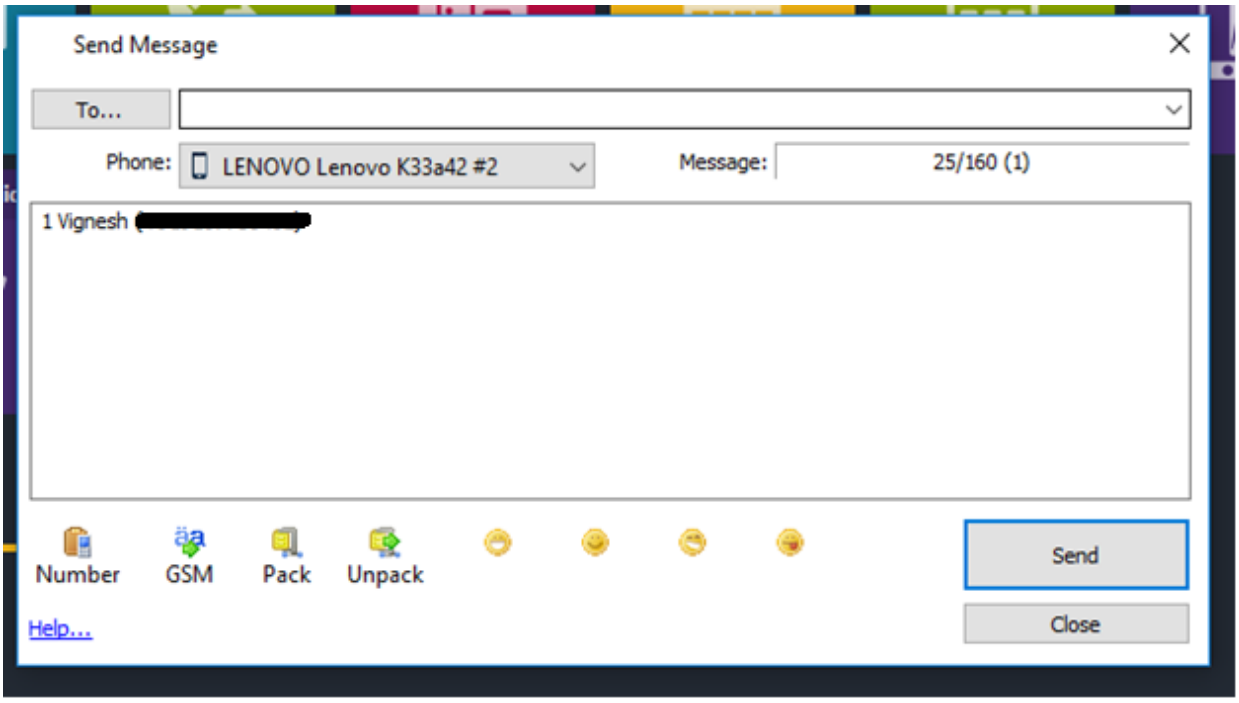

Compiled Driver Disk - Setup Wizard
Installation of drivers to the computer
Please wait while phone drivers are being copied to your computer
Installing selected drivers...
...LGE Android
MOBILedit
Enjoy a new generation
of the world's leading
PC software for controlling
your phone and everything in it.
www.mobiledit.com


MOBILedit
LENOVO Lenovo K33a42 #2 (Not activated)
Phonebook
Call Logs
Messages
Calendar
Applications
Application Data
User Files
Document Providers
Media
Files
NOT ACTIVATED!
8:53:24 PM
Android
IMEI:
USB


Phonebook
Search:
Current Phone
All
Name
Number
1 Gaurav
1 Mukund
1 Mukund
1 Naman Mscit
1 Naman Mscit


Save As
This PC
Pictures
Search Pictures
Organize
New folder
This PC
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
Local Disk (E:)
CD Drive (F:) Ler
Camera Roll
Saved Pictures
cp1
File name:
scr_LENOVO Lenovo K33a42 #2_180409_205529
Save as type:
PNG File (*.png)
Hide Folders
Save
Cancel
Calendar
Screenshot

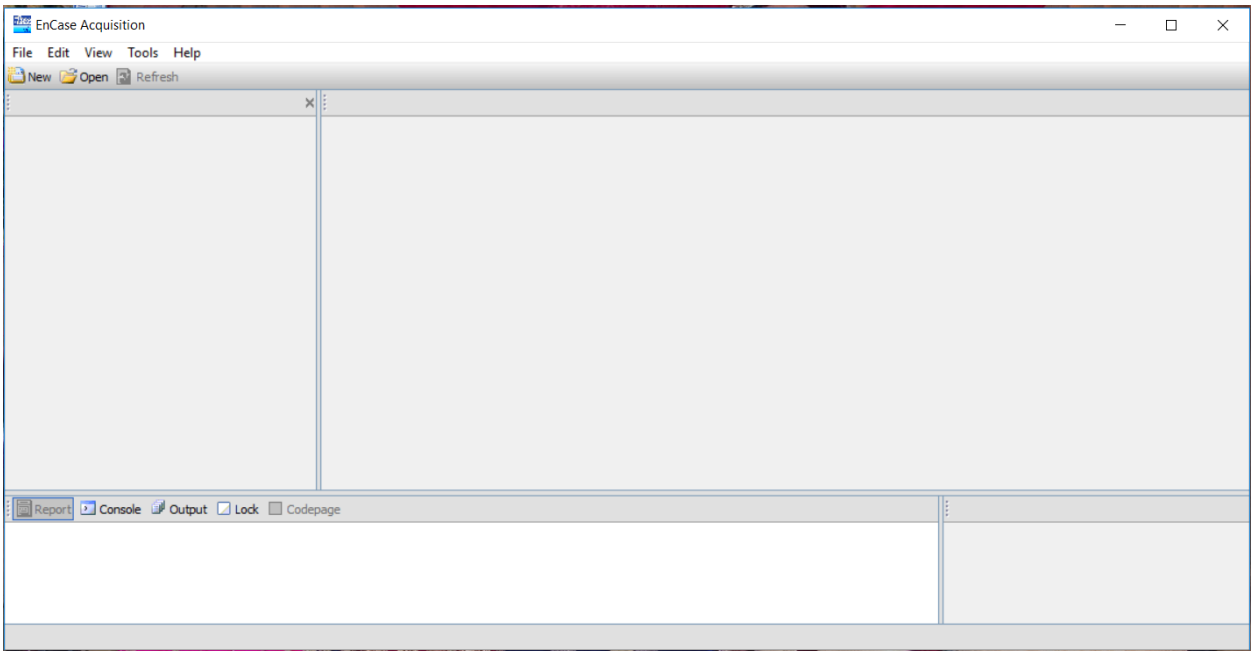

Desktop
Documents
Downloads
Music
Pictures
Videos
Devices and drives (5)
Lenovo K6 POWER
Local Disk (C:)
287 GB free of 341 GB
DVD RW Drive (D:)
Local Disk (E:)
386 GB free of 585 GB
CD Drive (F:) Lenovo_Suite
0 bytes free of 41.5 MB
CDFS

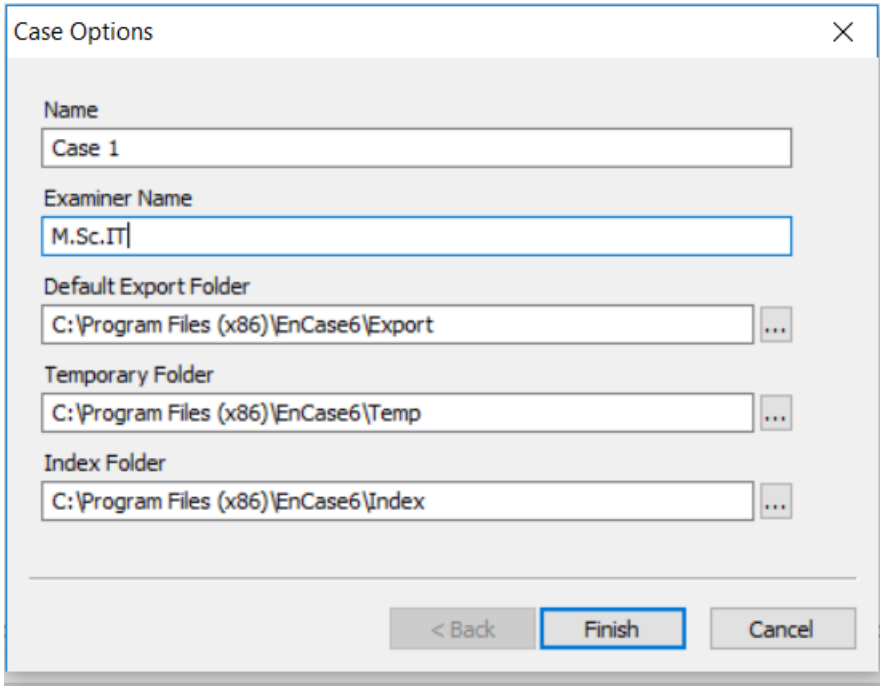

Send Message
To...
Phone:
LENOVO Lenovo K33a42 #2
Message:
25/160 (1)
1 Vignesh
Number
GSM
Pack
Unpack
Send
Close
Help...

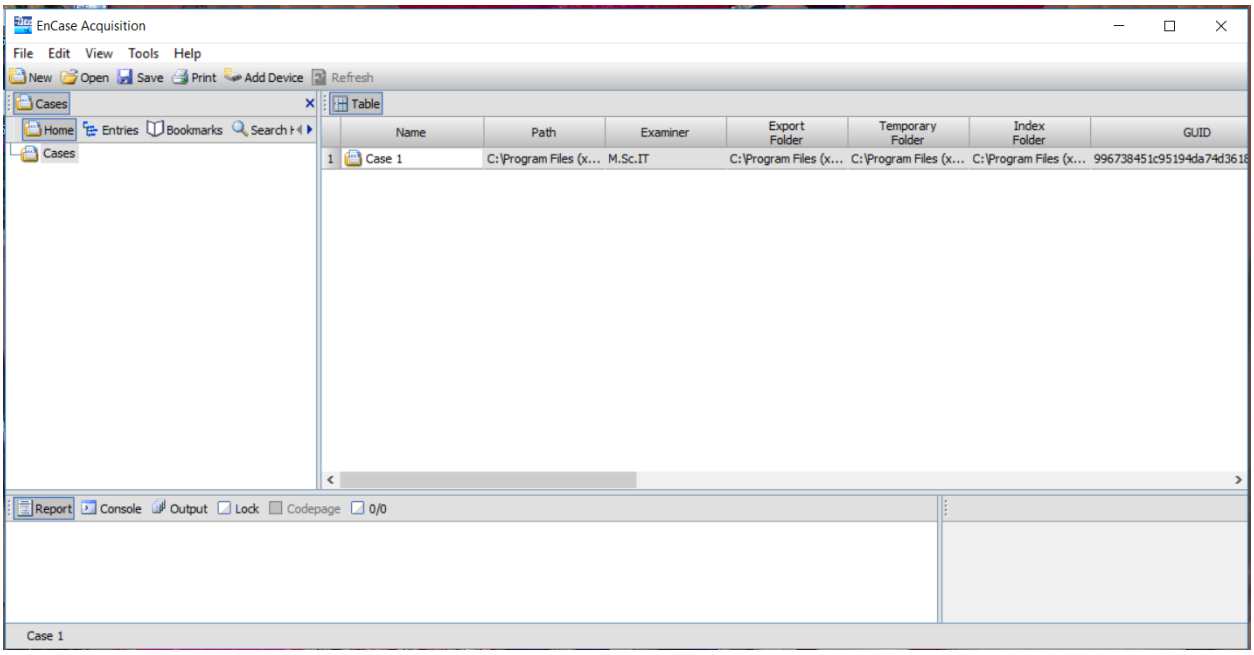
Signature:

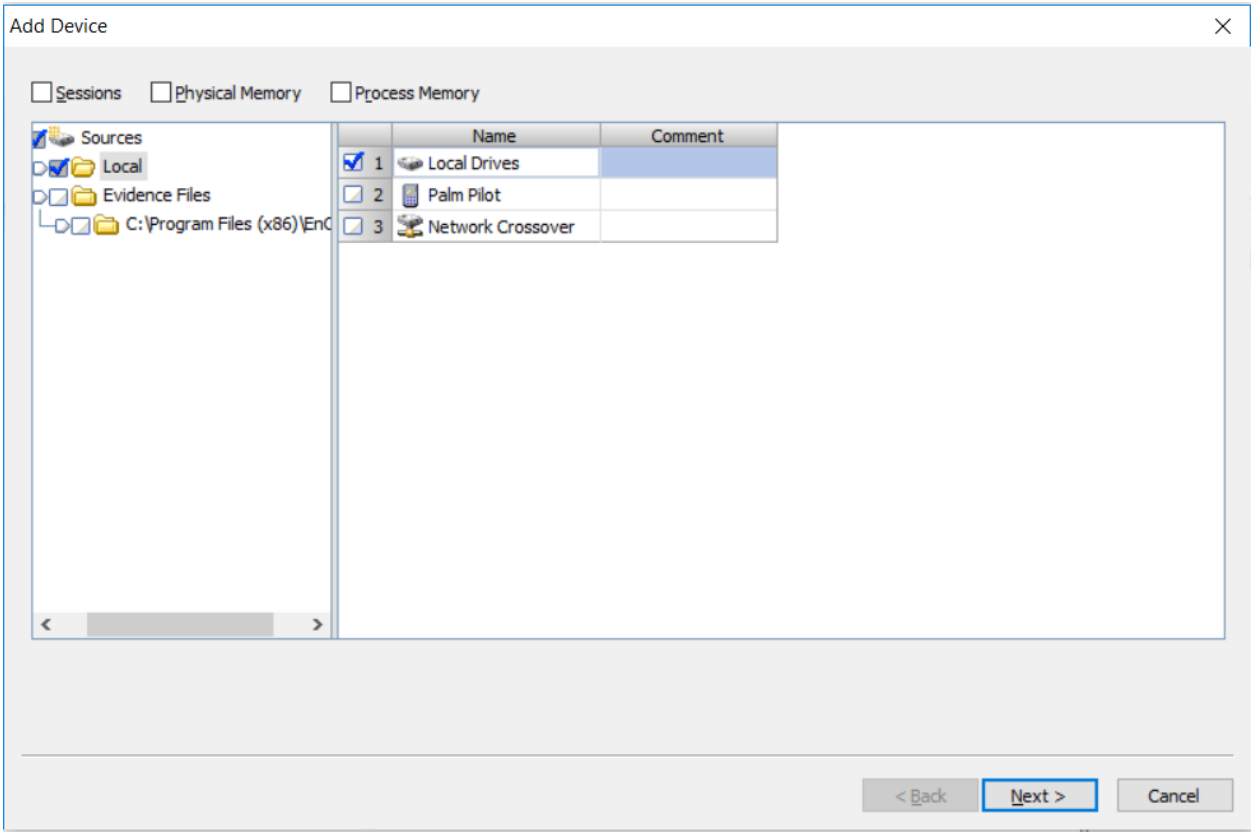
Practical 14

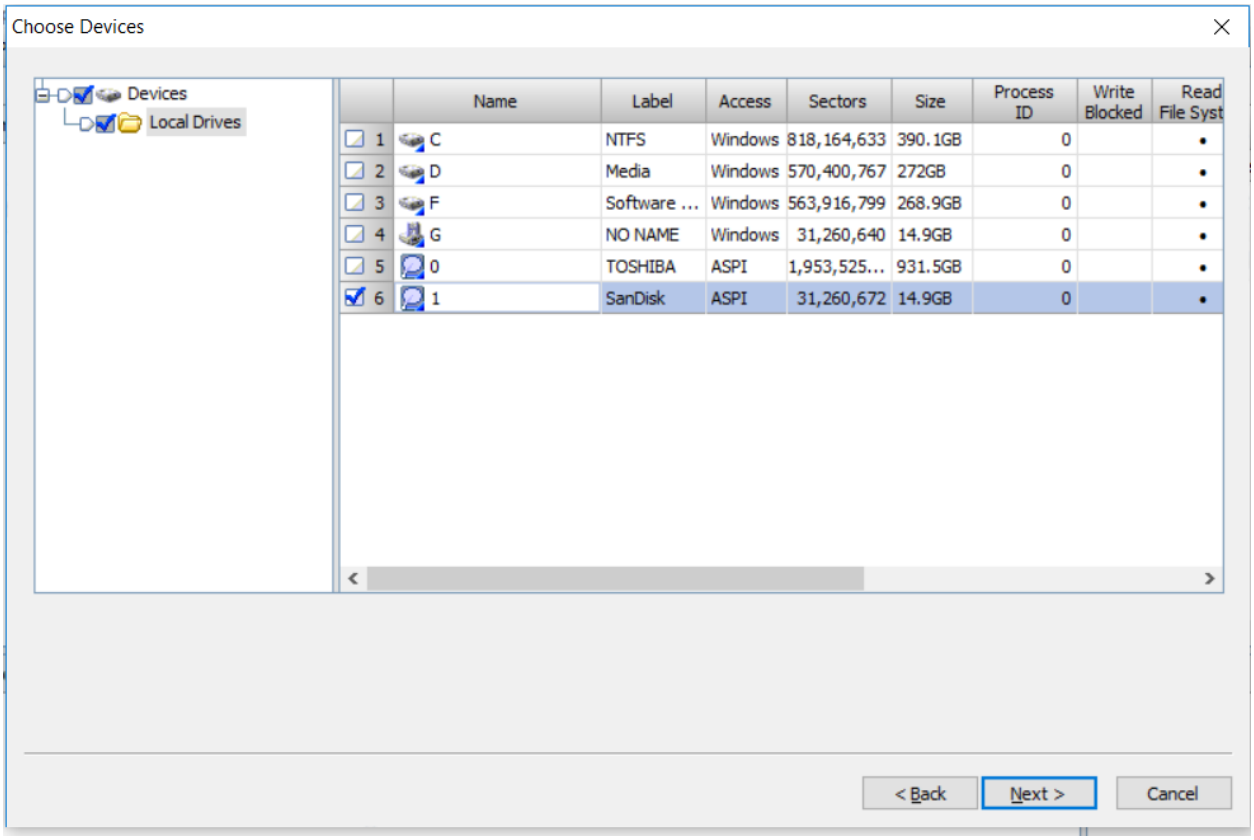
Aim: Forensic investigation using Encase.

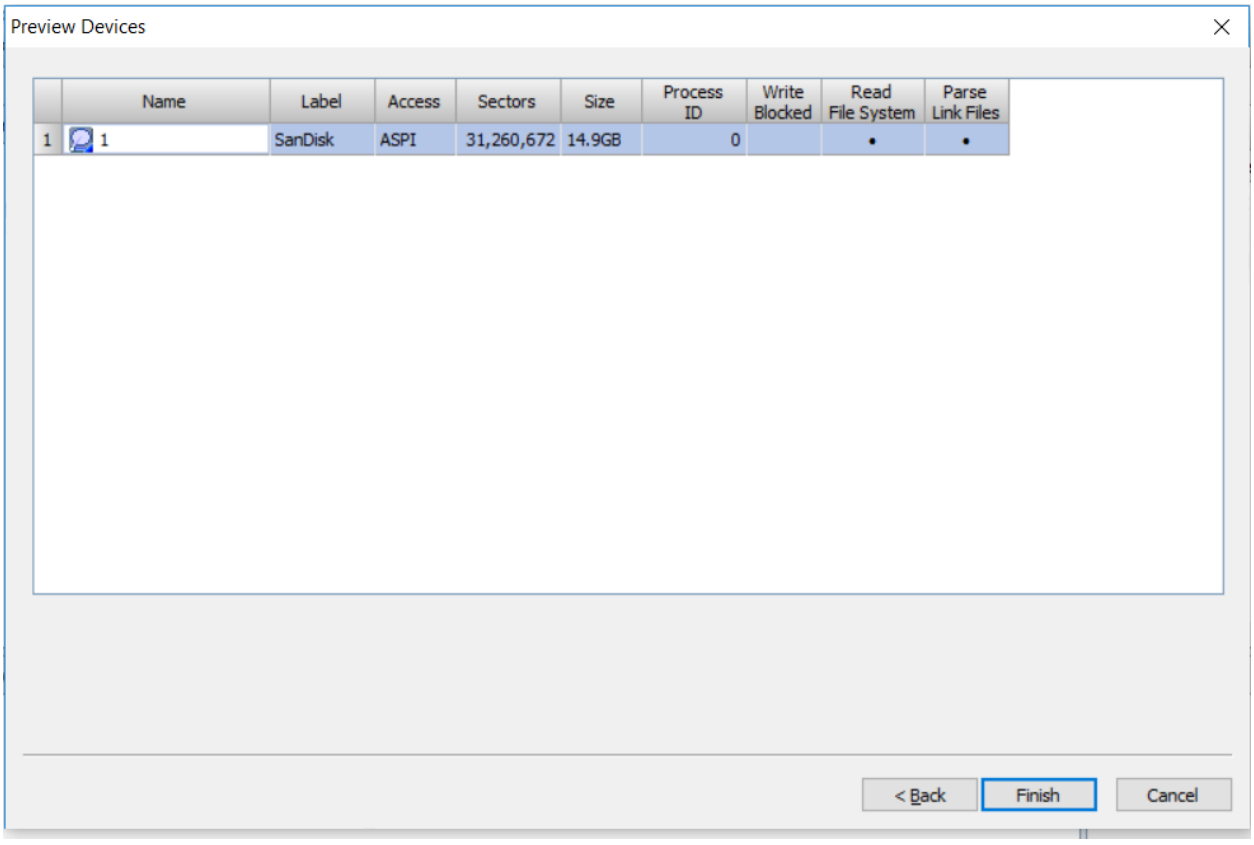


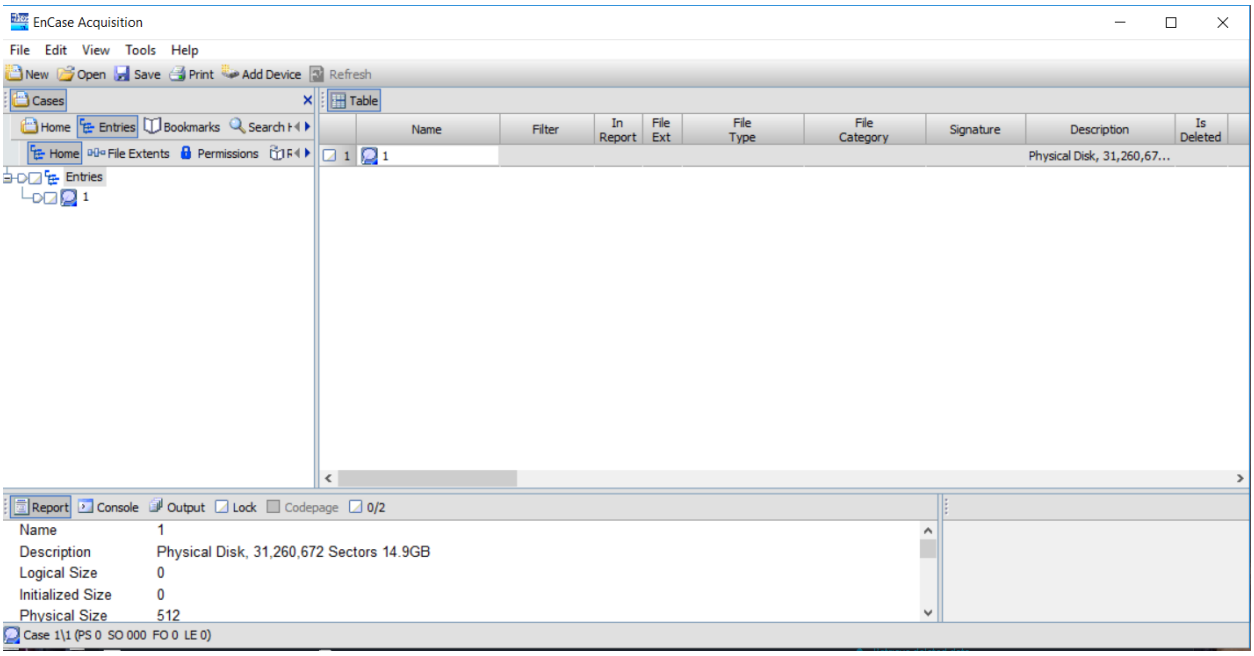


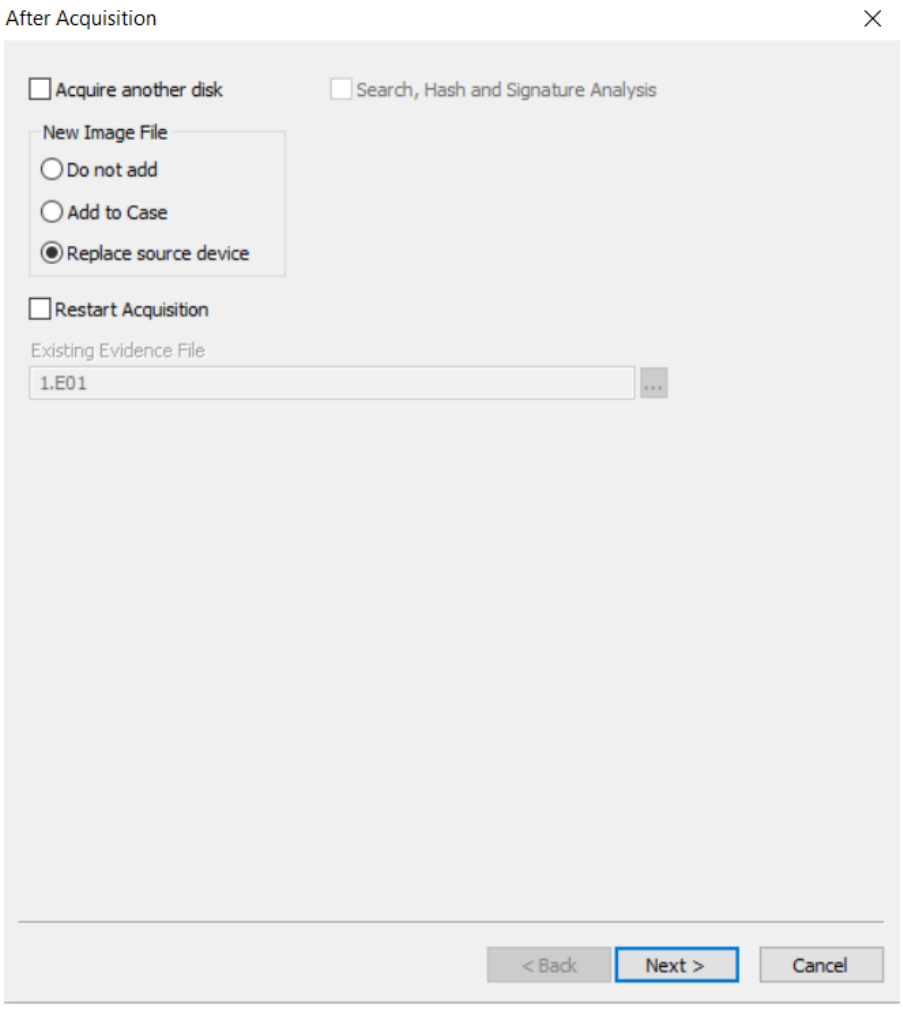

EnCase Acquisition
File Edit View Tools Help
New Open Save Print Add Device Refresh
Cases
Table
Home Entries Bookmarks Search
Cases
Name Path Examiner Export Folder Temporary Folder Index Folder GUID
1 Case 1 C:\Program Files (x... M.Sc.IT C:\Program Files (x... C:\Program Files (x... C:\Program Files (x... 996738451c95194da74d3618
Report Console Output Lock Codepage 0/0
Case 1

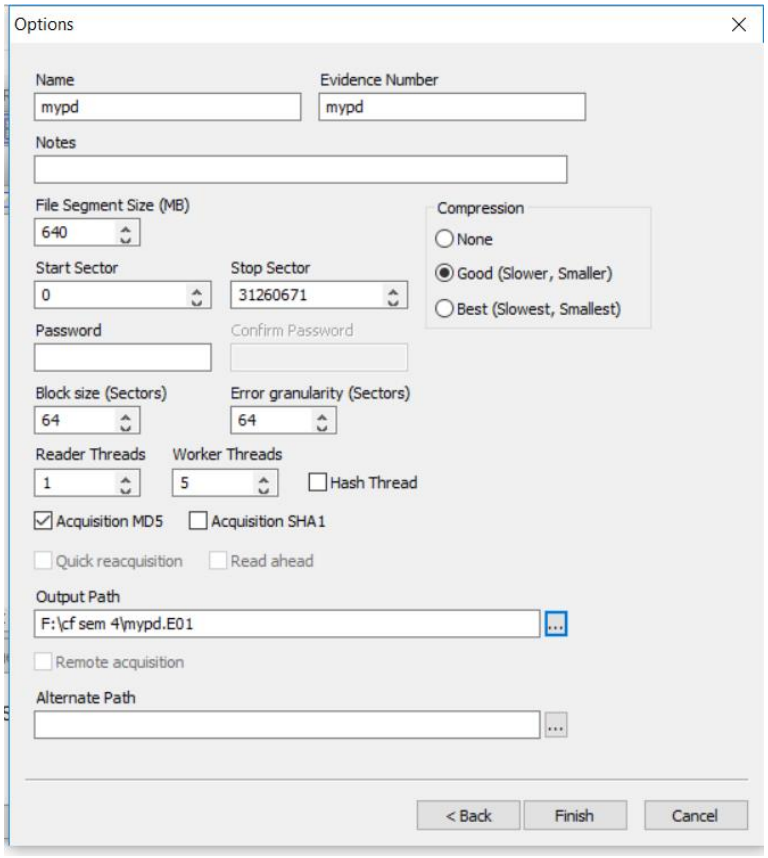

Add Device
Sessions Physical Memory Process Memory
Sources
Local
Evidence Files
C:\Program Files (x86)\EnC
Name Comment
1 Local Drives
2 Palm Pilot
3 Network Crossover
< Back Next > Cancel

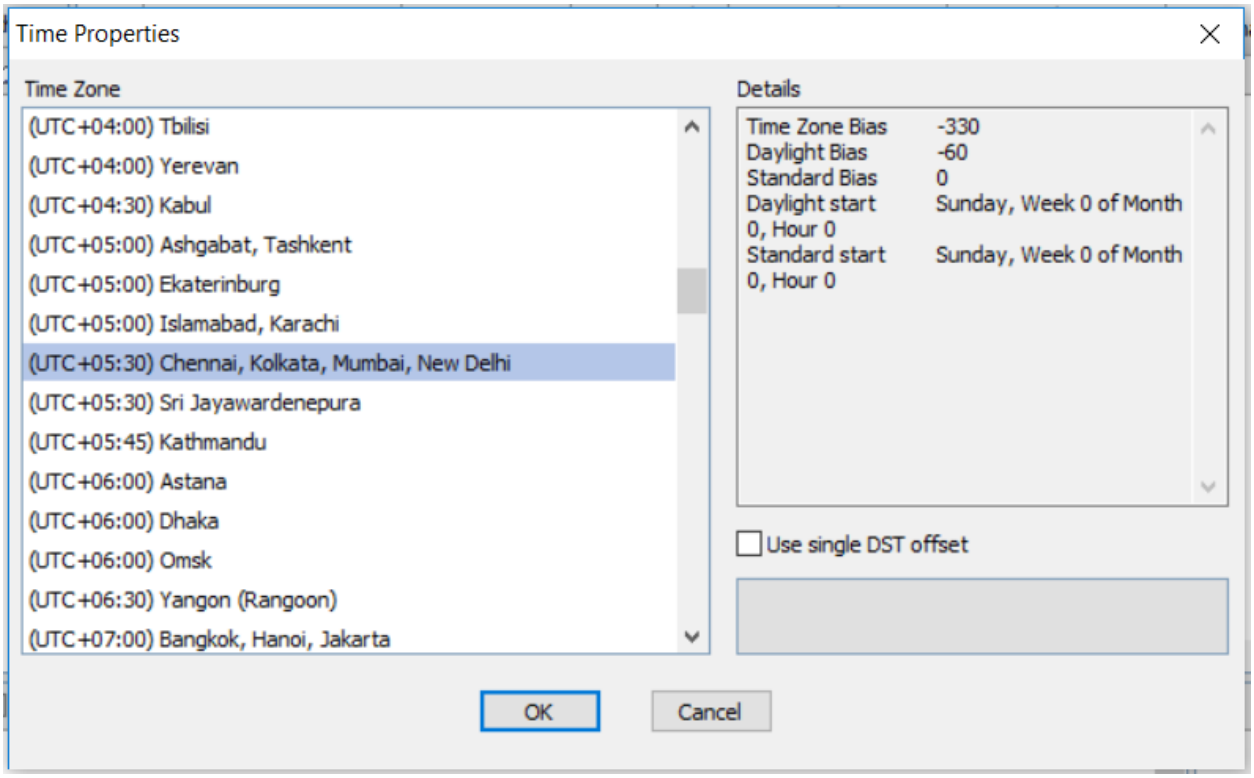

Choose Devices
Devices
Local Drives
Name
Label
Access
Sectors
Size
Process ID
Write Blocked
Read File Syst
1 C NTFS Windows 818,164,633 390.1GB 0
2 D Media Windows 570,400,767 272GB 0
3 F Software ... Windows 563,916,799 268.9GB 0
4 G NO NAME Windows 31,260,640 14.9GB 0
5 0 TOSHIBA ASPI 1,953,525... 931.5GB 0
6 1 SanDisk ASPI 31,260,672 14.9GB 0
< Back
Next >
Cancel

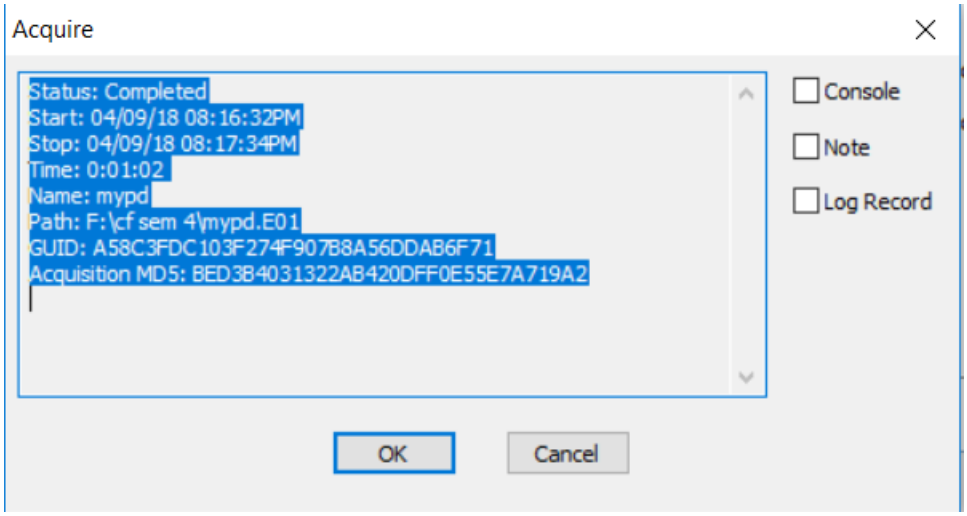

Preview Devices
Name
Label
Access
Sectors
Size
Process ID
Write Blocked
Read File System
Parse Link Files
1 1 SanDisk ASPI 31,260,672 14.9GB 0
< Back
Finish
Cancel

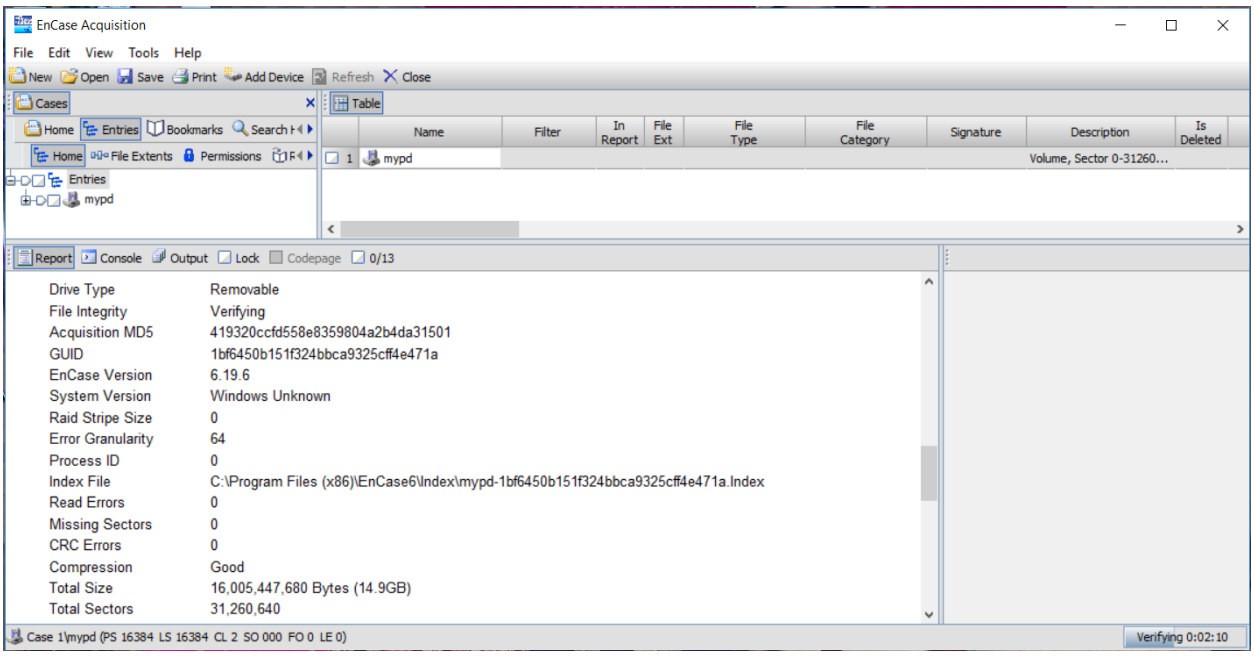

EnCase Acquisition
File Edit View Tools Help
New Open Save Print Add Device Refresh
Cases
Table
Home Entries Bookmarks Search
Home File Extents Permissions
Entries
1
Name Filter In Report File Ext File Type File Category Signature Description Is Deleted
1 1
Physical Disk, 31,260,67...
Report Console Output Lock Codepage 0/2
Name 1
Description Physical Disk, 31,260,672 Sectors 14.9GB
Logical Size 0
Initialized Size 0
Physical Size 512
Case 1\1 (PS 0 SO 000 FO 0 LE 0)

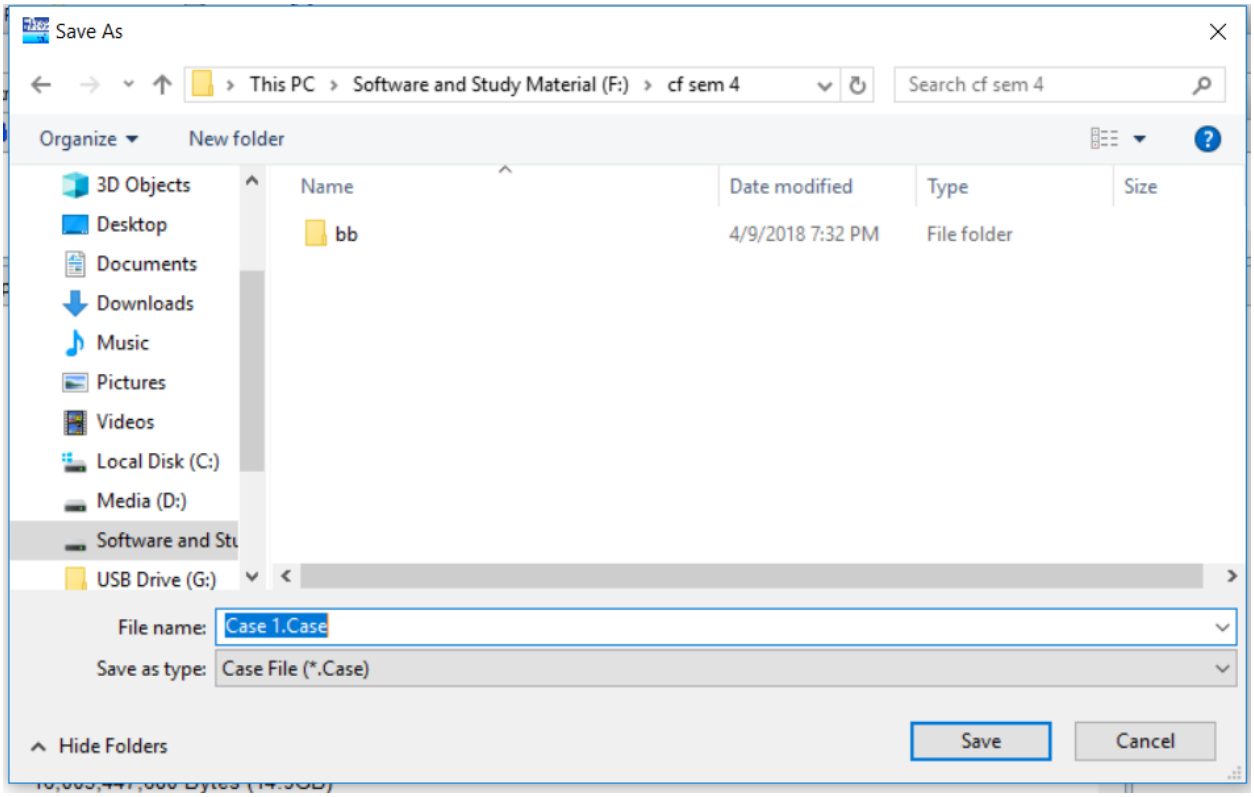

After Acquisition
Acquire another disk
Search, Hash and Signature Analysis
New Image File
Do not add
Add to Case
Replace source device
Restart Acquisition
Existing Evidence File
1.E01
< Back
Next >
Cancel

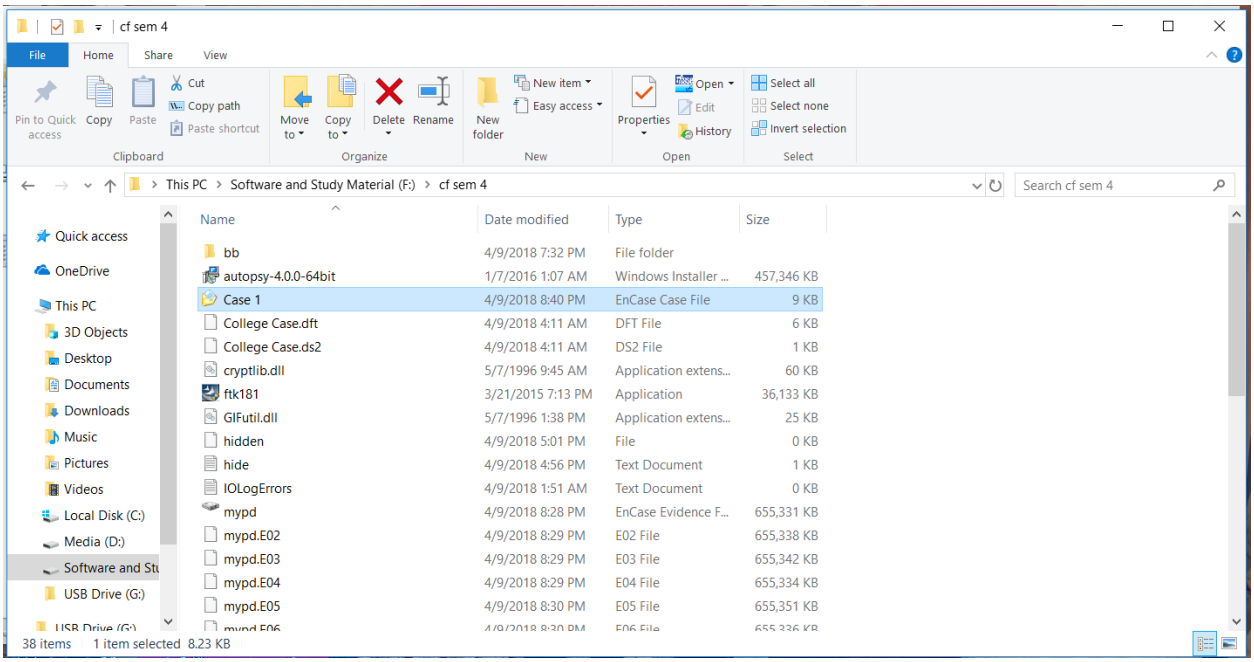

Options
Name
mypd
Evidence Number
mypd
Notes
File Segment Size (MB)
640
Compression
None
Good (Slower, Smaller)
Best (Slowest, Smallest)
Start Sector
0
Stop Sector
31260671
Password
Confirm Password
Block size (Sectors)
64
Error granularity (Sectors)
64
Reader Threads
1
Worker Threads
5
Hash Thread
Acquisition MD5
Acquisition SHA1
Quick reacquisition
Read ahead
Output Path
F:\cf sem 4\mypd.E01
Remote acquisition
Alternate Path
< Back
Finish
Cancel

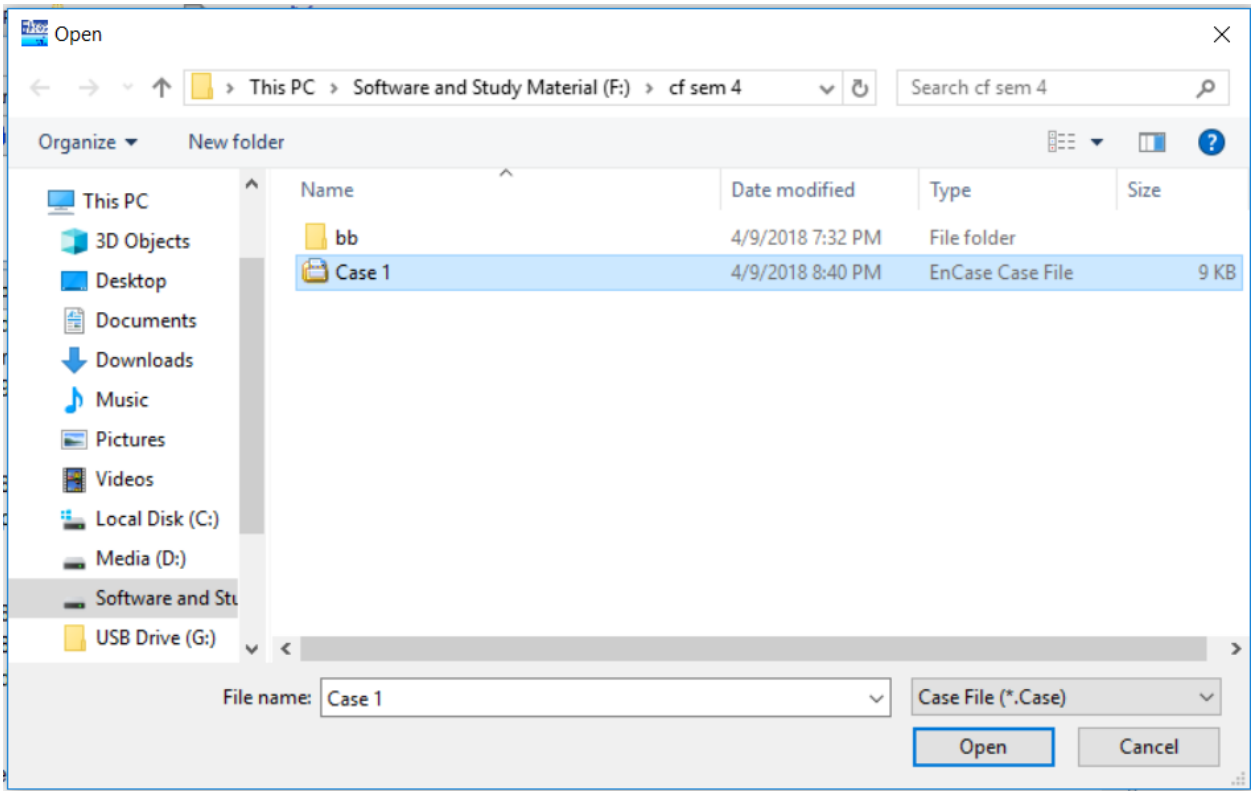

Time Properties
Time Zone
(UTC+04:00) Tbilisi
(UTC+04:00) Yerevan
(UTC+04:30) Kabul
(UTC+05:00) Ashgabat, Tashkent
(UTC+05:00) Ekaterinburg
(UTC+05:00) Islamabad, Karachi
(UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi
(UTC+05:30) Sri Jayawardenepura
(UTC+05:45) Kathmandu
(UTC+06:00) Astana
(UTC+06:00) Dhaka
(UTC+06:00) Omsk
(UTC+06:30) Yangon (Rangoon)
(UTC+07:00) Bangkok, Hanoi, Jakarta
Details
Time Zone Bias -330
Daylight Bias -60
Standard Bias 0
Daylight start Sunday, Week 0 of Month 0, Hour 0
Standard start Sunday, Week 0 of Month 0, Hour 0
Use single DST offset
OK
Cancel

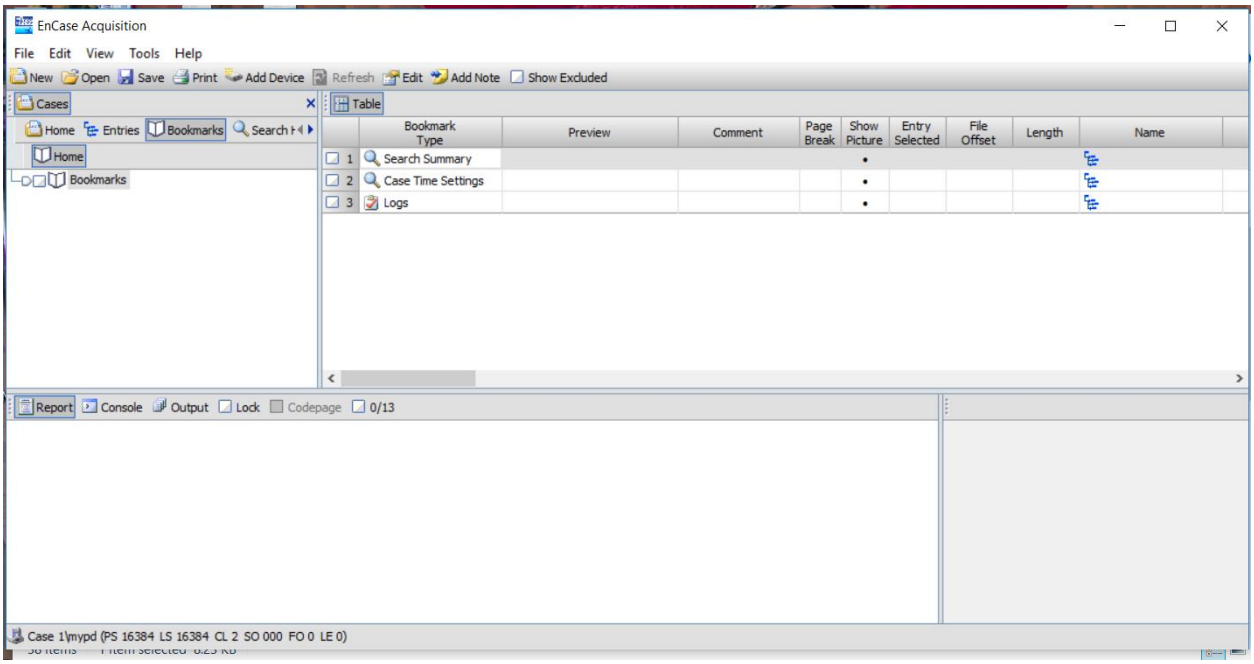

Acquire
Status: Completed
Start: 04/09/18 08:16:32PM
Stop: 04/09/18 08:17:34PM
Time: 0:01:02
Name: mypd
Path: F:\cf sem 4\mypd.E01
GUID: A58C3FDC103F274F907B8A56DDAB6F71
Acquisition MD5: BED3B4031322AB420DFF0E55E7A719A2
Console
Note
Log Record
OK
Cancel


EnCase Acquisition
File Edit View Tools Help
New Open Save Print Add Device Refresh Close
Cases
Table
Home Entries Bookmarks Search
Home File Extents Permissions
Entries
mypd
Name Filter In Report File Ext File Type File Category Signature Description Is Deleted
1 mypd
Volume, Sector 0-31260...
Report Console Output Lock Codepage 0/13
Drive Type Removable
File Integrity Verifying
Acquisition MD5 419320ccfd558e8359804a2b4da31501
GUID 1bf6450b151f324bbca9325cff4e471a
EnCase Version 6.19.6
System Version Windows Unknown
Raid Stripe Size 0
Error Granularity 64
Process ID 0
Index File C:\Program Files (x86)\EnCase6\Index\mypd-1bf6450b151f324bbca9325cff4e471a.Index
Read Errors 0
Missing Sectors 0
CRC Errors 0
Compression Good
Total Size 16,005,447,680 Bytes (14.9GB)
Total Sectors 31,260,640
Case 1\mypd (PS 16384 LS 16384 CL 2 SO 000 FO 0 LE 0)
Verifying 0:02:10


Save As
This PC › Software and Study Material (F:) › cf sem 4
Search cf sem 4
Organize
New folder
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
Media (D:)
Software and Stu
USB Drive (G:)
Name
Date modified
Type
Size
bb
4/9/2018 7:32 PM
File folder
File name:
Case 1.Case
Save as type:
Case File (*.Case)
Hide Folders
Save
Cancel


cf sem 4
File
Home
Share
View
Cut
Copy path
Paste shortcut
Pin to Quick access
Copy
Paste
Move to
Copy to
Delete
Rename
New folder
New item
Easy access
Properties
Open
Edit
History
Select all
Select none
Invert selection
Clipboard
Organize
New
Open
Select
This PC › Software and Study Material (F:) › cf sem 4
Search cf sem 4
Quick access
OneDrive
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
Media (D:)
Software and Stu
USB Drive (G:)
Name
Date modified
Type
Size
bb 4/9/2018 7:32 PM File folder
autopsy-4.0.0-64bit 1/7/2016 1:07 AM Windows Installer ... 457,346 KB
Case 1 4/9/2018 8:40 PM EnCase Case File 9 KB
College Case.dft 4/9/2018 4:11 AM DFT File 6 KB
College Case.ds2 4/9/2018 4:11 AM DS2 File 1 KB
cryptlib.dll 5/7/1996 9:45 AM Application extens... 60 KB
ftk181 3/21/2015 7:13 PM Application 36,133 KB
GlFutil.dll 5/7/1996 1:38 PM Application extens... 25 KB
hidden 4/9/2018 5:01 PM File 0 KB
hide 4/9/2018 4:56 PM Text Document 1 KB
IOLogErrors 4/9/2018 1:51 AM Text Document 0 KB
mypd 4/9/2018 8:28 PM EnCase Evidence F... 655,331 KB
mypd.E02 4/9/2018 8:29 PM E02 File 655,338 KB
mypd.E03 4/9/2018 8:29 PM E03 File 655,342 KB
mypd.E04 4/9/2018 8:29 PM E04 File 655,334 KB
mypd.E05 4/9/2018 8:30 PM E05 File 655,351 KB
38 items
1 item selected 8.23 KB


Open
This PC › Software and Study Material (F:) › cf sem 4
Search cf sem 4
Organize
New folder
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
Media (D:)
Software and Stu
USB Drive (G:)
Name
Date modified
Type
Size
bb
4/9/2018 7:32 PM
File folder
Case 1
4/9/2018 8:40 PM
EnCase Case File
9 KB
File name:
Case 1
Case File (*.Case)
Open
Cancel


EnCase Acquisition
File Edit View Tools Help
New Open Save Print Add Device Refresh Edit Add Note Show Excluded
Cases
Table
Home Entries Bookmarks Search
Home
Bookmarks
Bookmark Type
Preview
Comment
Page Break
Show Picture
Entry Selected
File Offset
Length
Name
1 Search Summary
2 Case Time Settings
3 Logs
Report Console Output Lock Codepage 0/13
Case 1\mypd (PS 16384 LS 16384 CL 2 SO 000 FO 0 LE 0)

Signature: