

CYBER FORENSICS

INDEX

Sr.NO	Name	Date	Sign
1.	File System Analysis using The Sleuth Kit (Autopsy)		
2.	Using Forensic Toolkit (FTK) & Email forensics & Writing report using FTK (AccessData FTK)		
3.	Using File Recovery Creating Image Tools [AccessData's FTK Imager tool]		
4.	Using Log Capturing and Analysis tools & Traffic capturing (wireshark)		
5.	Using Web attack detection tools (wireshark)		
6.	Using Data acquisition tools (ProDiscover Basic.)		
7.	Using Steganography tools (S tools)		
8.	Using Password Cracking tools (Cain & Abel)		
9.	Managing Remote Registry, Network Enumeration, Services, s. IDs [Cain & Abel]		
10.	Performing Sniffing [Cain & Abel]		
11.	Forensic Investigation using EnCase (Encase)		
12.	Using Mobile Forensics software tools (Mobiledit Forensics)		

Practical 1

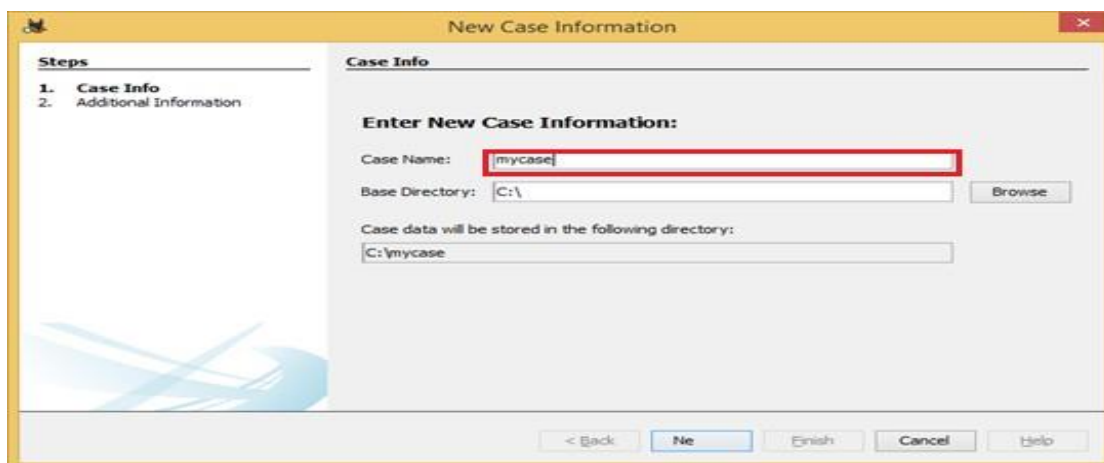
Aim: **File System Analysis [Autopsy]**

Step-1: Start Autopsy Tool

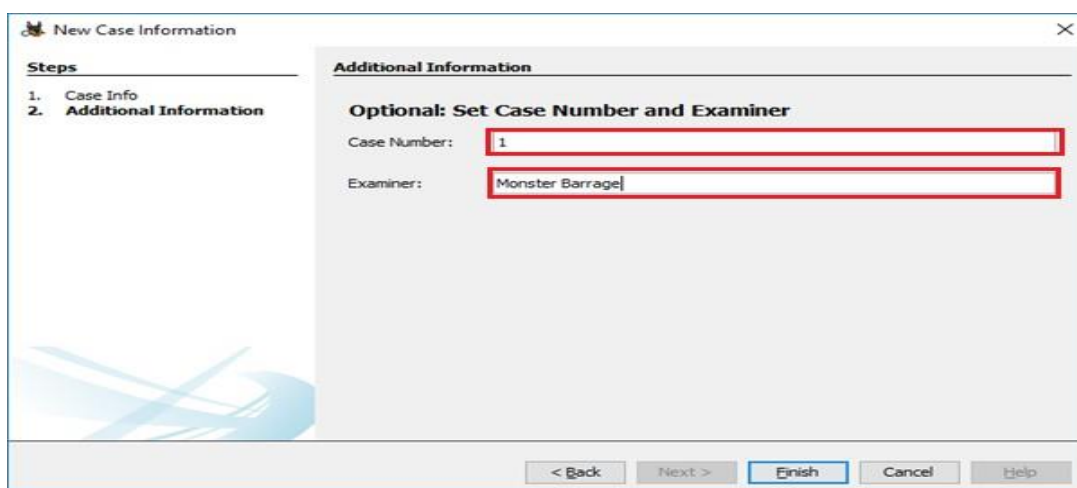
Step-2: Click Create New Case



Step-3: Enter The Details

The image shows the 'New Case Information' dialog box, specifically the 'Case Info' step. The 'Steps' panel on the left shows '1. Case Info' and '2. Additional Information'. The main area is titled 'Enter New Case Information:'. It contains three input fields: 'Case Name:' with the value 'mycase' (highlighted with a red rectangle), 'Base Directory:' with the value 'C:\', and 'Case data will be stored in the following directory:' with the value 'C:\mycase'. There is a 'Browse' button next to the 'Base Directory' field. At the bottom, there are buttons for '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'.

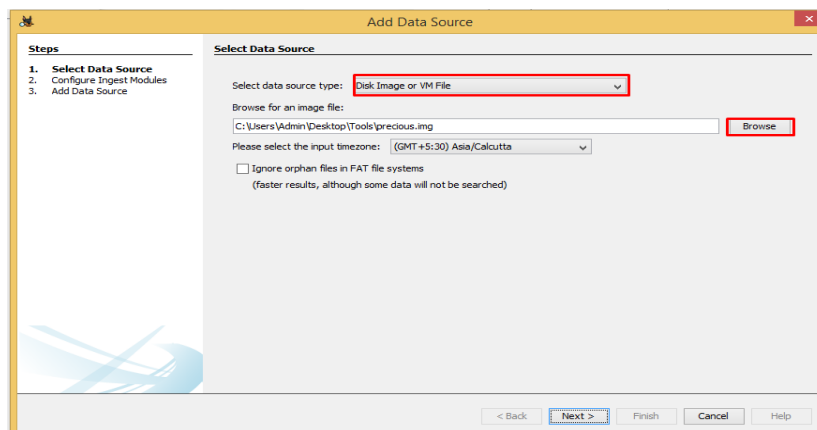
Step-4: Enter The Case Name & Case Examiner Name

The image shows the 'New Case Information' dialog box, specifically the 'Additional Information' step. The 'Steps' panel on the left shows '1. Case Info' and '2. Additional Information'. The main area is titled 'Optional: Set Case Number and Examiner'. It contains two input fields: 'Case Number:' with the value '1' (highlighted with a red rectangle), and 'Examiner:' with the value 'Monster Barrage' (highlighted with a red rectangle). At the bottom, there are buttons for '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'.

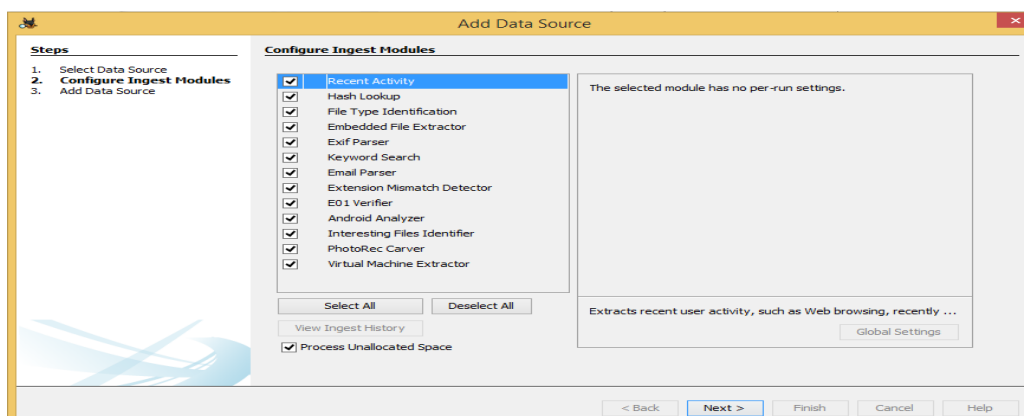
Step-5: After Clicking The Finish Button In The Above Window,

A New Window Will Open For Retrieving The Datasource,
Select Disk Image or VM File

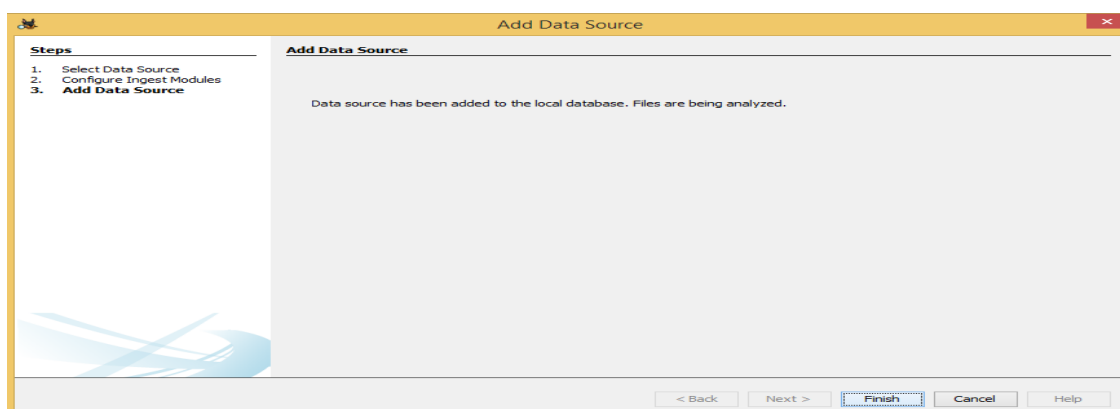
Then Browse The .img File Present In The Directory
Click Next



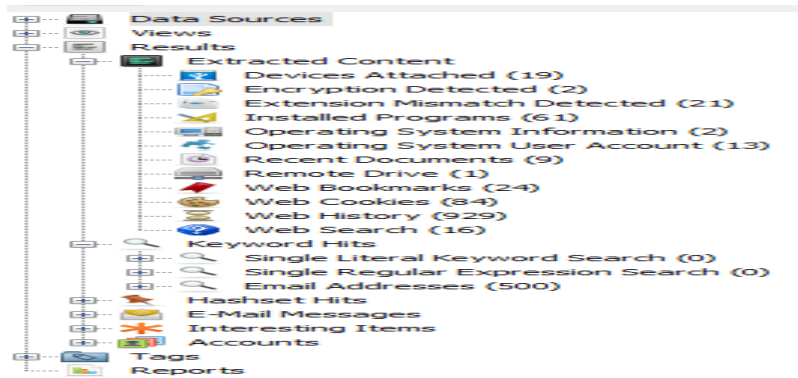
Step-6: The Next Step Provides A Ingest Wizard Panel Which Aims At Increasing The Search Capability. Select As Desired And Proceed To The Next Step.



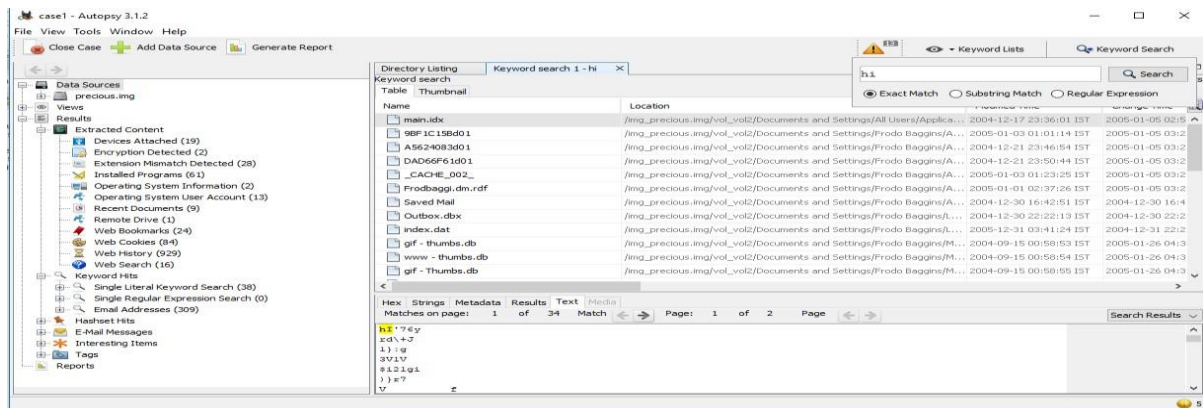
Step-7: In The Resulting Window, You'll Be Notified That The Files Are Being Analyzed.
Proceed To Finish.



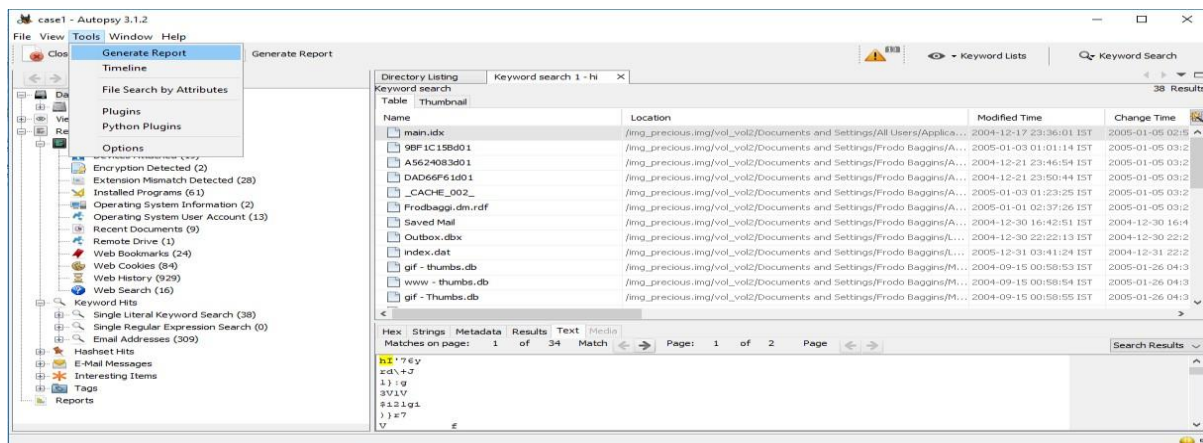
Step-8: After The Image Is Indexed The Tree Will Be Populated By The File System, Extracted Content, Keyword Searches, And The Hash List (If Any Were Used). This Tree Can Be To Retrieve The Information About The Image File Under Observation.

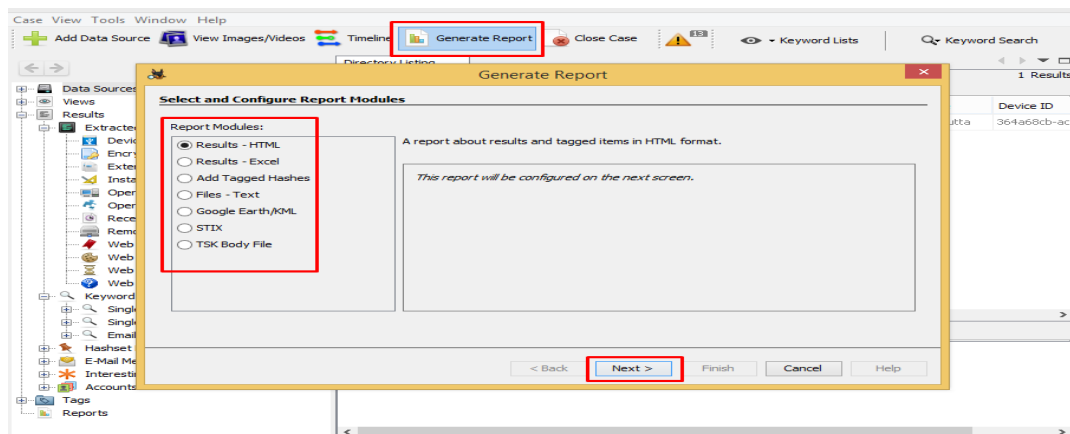


The Investigator can also Search by keyword



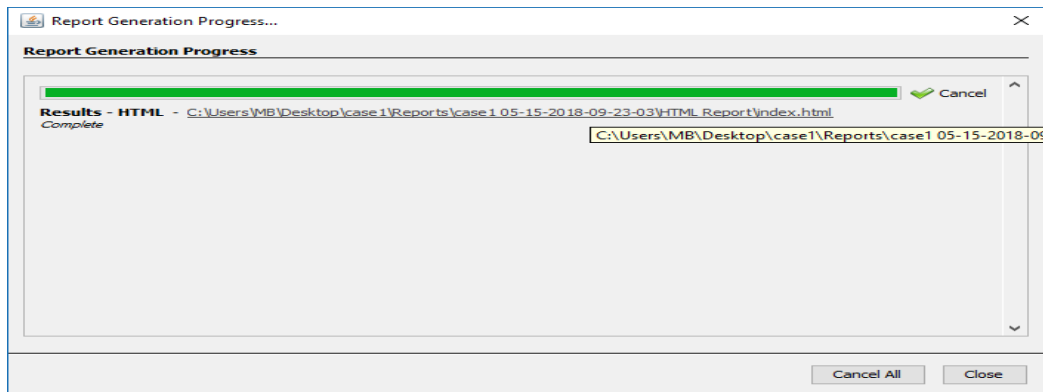
Should Generate A Report. This Will Allow The Investigator To Have An Idea Of What Type Of Information Is Available And What To Expect.



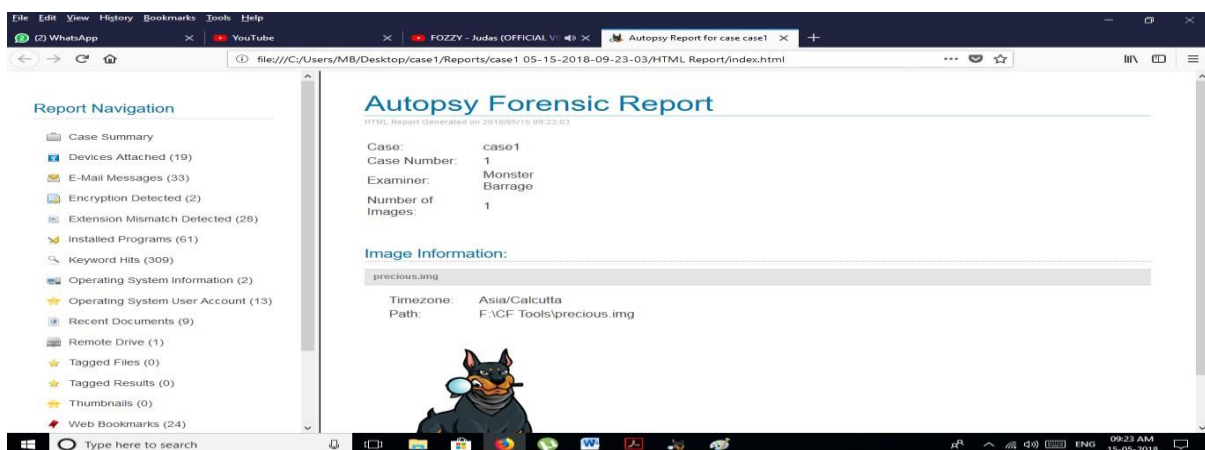


Click Next And Then Finish

.Step-9: View The Generated Report As Provided By The Tool.



Click On the Link

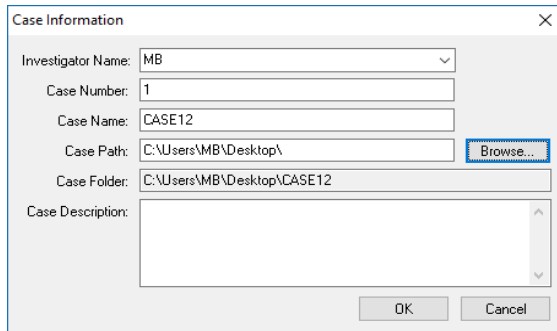


Practical 2

Aim: Using Forensic Toolkit (FTK) & Writing report using FTK (AccessData FTK)

Step-1: Open Forensic Toolkit

Step-2: We can



Case Information

Investigator Name: MB

Case Number: 1

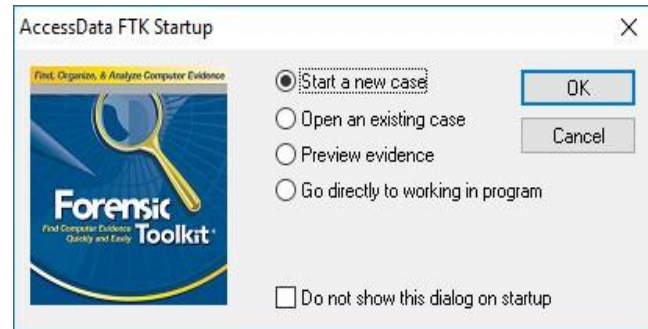
Case Name: CASE12

Case Path: C:\Users\MB\Desktop\ Browse...

Case Folder: C:\Users\MB\Desktop\CASE12

Case Description:

OK Cancel



AccessData FTK Startup

☒ Start a new case

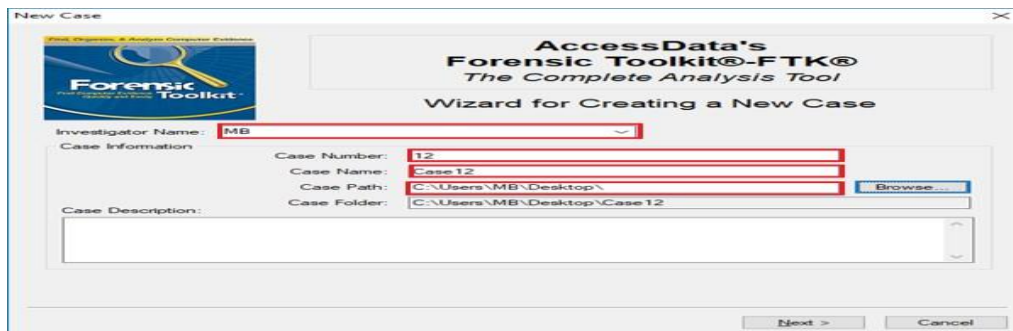
☐ Open an existing case

☐ Preview evidence

☐ Go directly to working in program

☐ Do not show this dialog on startup

OK Cancel



New Case

AccessData's Forensic Toolkit®-FTK®
The Complete Analysis Tool

Wizard for Creating a New Case

Investigator Name: MB

Case Information

Case Number: 12

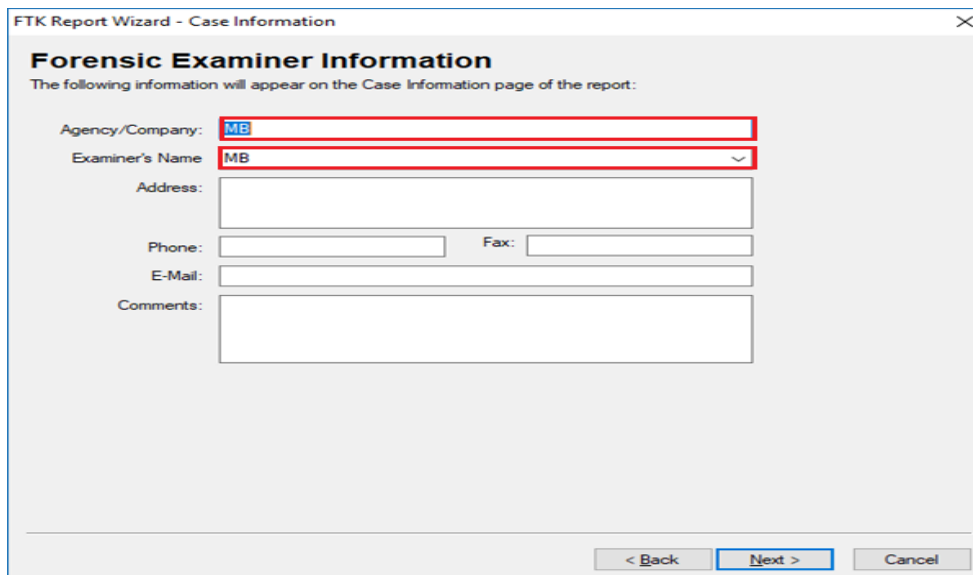
Case Name: Case12

Case Path: C:\Users\MB\Desktop\ Browse...

Case Folder: C:\Users\MB\Desktop\Case12

Case Description:

Next > Cancel



FTK Report Wizard - Case Information

Forensic Examiner Information

The following information will appear on the Case Information page of the report:

Agency/Company: MB

Examiner's Name: MB

Address:

Phone: Fax:

E-Mail:

Comments:

< Back Next > Cancel

Step-4: Select Relevant Options And Proceed.

Case Log Options

The case log is a text file named FTKlog in the case folder. It gets created automatically by FTK and contains a record of events that occur during the course of the case. You can choose which type of events you would like to be logged. You can also add your own comments to the log file at any time by selecting "Add Case Log Entry..." under the "Tools" menu item, and you can view the log file by selecting "View Case Log" under the "Tools" menu item.

Events to go in the Case Log:

- ☒ Case and evidence events
- ☒ Error messages
- ☒ Bookmarking events
- ☒ Searching events
- ☒ Data carving / Internet searches
- ☒ Other events

Events related to the addition and processing of file items when evidence is added or when using Analysis Tools later in the case.

Events related to any error conditions encountered during the case.

Events related to the addition and modification of bookmarks.

Events related to searching. All search queries and resulting hit counts will be recorded.

Events related to special data carving or internet keyword searches that are performed during the case.

Other events not related to the above, such as copying, viewing, and ignoring files.

< Back Next > Cancel

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
- ☒ SHA1 Hash
- ☒ KFF Lookup
- ☒ Entropy Test
- ☒ Full Text Index
- ☒ Store Thumbnails
- ☒ Decrypt EFS Files
- ☒ File Listing Database
- ☒ HTML File Listing
- ☒ Data Carve
- ☒ Registry Reports

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.

A SHA1 hash is a 20 byte value. The SHA1 hashing algorithm is newer than MD5, but is not yet as widely used.

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.

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.

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.

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.

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).

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.

Create an HTML version of the File Listing.

Automatically find specific file types embedded in other files and from free space. Retrieve results using Data Carving Option on Tools Menu.

Generate common registry reports during preprocessing.

Carving Options

< 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.

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			File Type Criteria		
Deletion Status:	Encryption Status:	Email Status:	<input checked="" type="checkbox"/> Documents	<input checked="" type="checkbox"/> Executables	
<input type="radio"/> Deleted	<input type="radio"/> Encrypted	<input type="radio"/> From email	<input checked="" type="checkbox"/> Spreadsheets	<input checked="" type="checkbox"/> Archives	
<input type="radio"/> Not deleted	<input type="radio"/> Not encrypted	<input type="radio"/> Not from email	<input checked="" type="checkbox"/> Databases	<input checked="" type="checkbox"/> Folders	
<input checked="" type="radio"/> Either	<input checked="" type="radio"/> Either	<input checked="" type="radio"/> Either	<input checked="" type="checkbox"/> Graphics	<input checked="" type="checkbox"/> Other Known	
<input checked="" type="checkbox"/> Include Duplicate Files	<input checked="" type="checkbox"/> OLE Streams		<input checked="" type="checkbox"/> Multimedia	<input checked="" type="checkbox"/> Unknown	
			<input checked="" type="checkbox"/> Email msgs		

< Back Next > Cancel

Refine Index - Default

Refine Index - Default

In order to save time and resources, and/or to make searching more efficient, you may choose to exclude certain kinds of data from being indexed. Here, you can choose default settings that will apply to each evidence item that gets added to the case. To exclude items from being indexed, make any changes to the settings below. Note: any items that don't get indexed initially can be indexed later by clicking on "Analysis Tools" under the "Tools" menu item.

Unconditionally Index

- ☒ 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.)

Conditionally Index

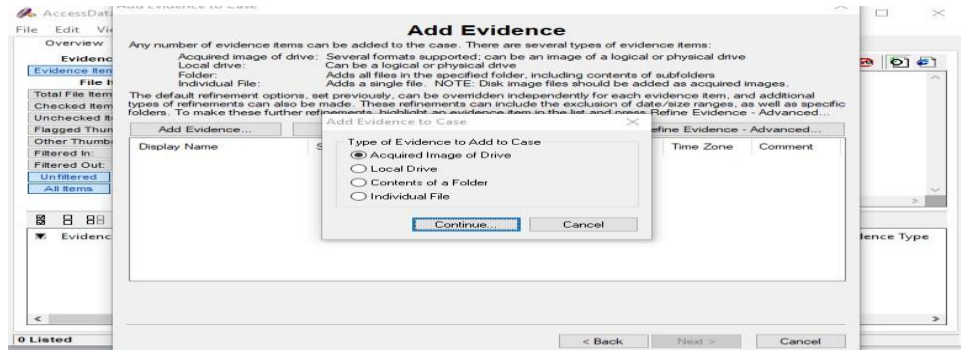
Index other items in the case only if they satisfy BOTH the file status and the file type criteria

File Status Criteria			File Type Criteria		
Deletion Status:	Encryption Status:	Email Status:	<input checked="" type="checkbox"/> Documents	<input checked="" type="checkbox"/> Executables	
<input type="radio"/> Deleted	<input type="radio"/> Encrypted	<input type="radio"/> From email	<input checked="" type="checkbox"/> Spreadsheets	<input checked="" type="checkbox"/> Archives	
<input type="radio"/> Not deleted	<input type="radio"/> Not encrypted	<input type="radio"/> Not from email	<input checked="" type="checkbox"/> Databases	<input checked="" type="checkbox"/> Folders	
<input checked="" type="radio"/> Either	<input checked="" type="radio"/> Either	<input checked="" type="radio"/> Either	<input checked="" type="checkbox"/> Graphics	<input checked="" type="checkbox"/> Other Known	
<input checked="" type="checkbox"/> Include Duplicate Files	<input checked="" type="checkbox"/> OLE Streams		<input checked="" type="checkbox"/> Multimedia	<input checked="" type="checkbox"/> Unknown	
			<input checked="" type="checkbox"/> Email msgs		

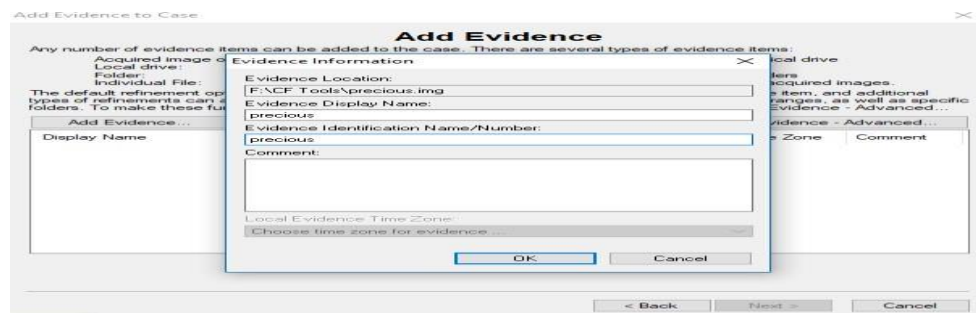
< Back Next > Cancel

Step-5: Adding Evidence.

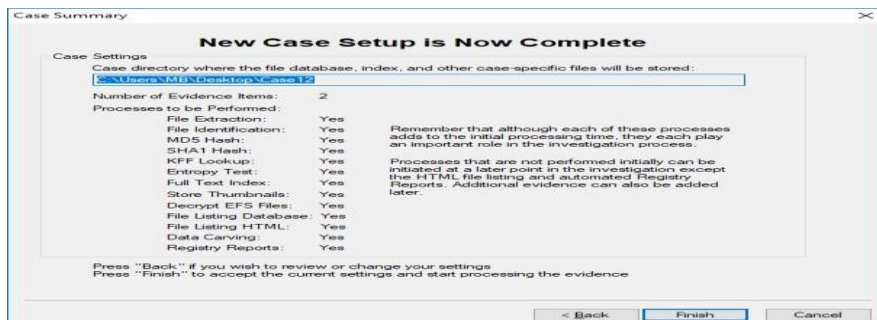
We Can Add Evidence Now Or Later Via The File Menu. The Evidence Can Be In The Form Of Acquired Image Of Drive Local Drive Contents Of A Folder Individual File According To The Option Selected We Will Be Presented With The Relevant Popup Screen. For Now We Will Be Going With The Contents Of A Folder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



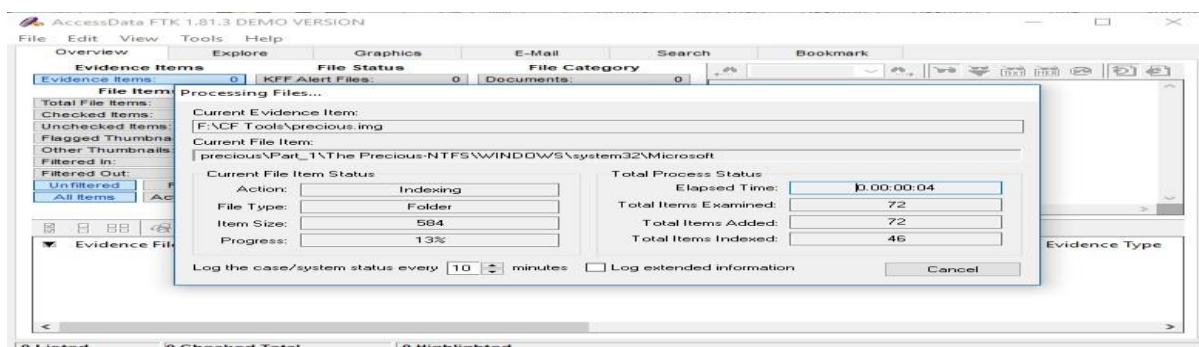
Select The Image File



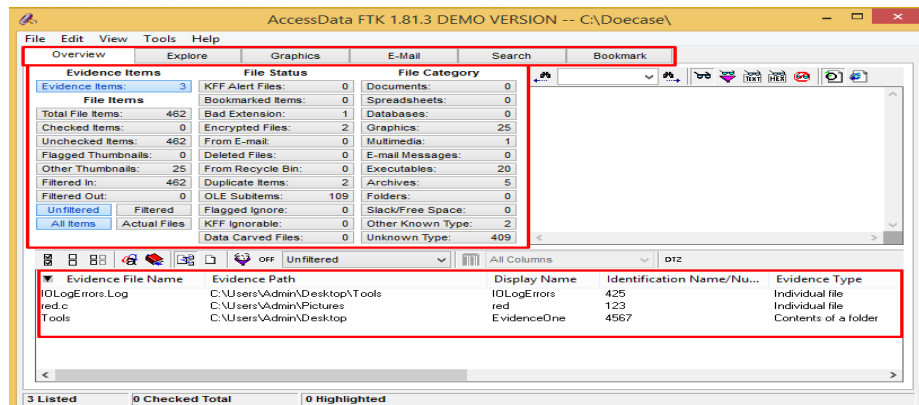
Click OK And Then Next To Proceed .



Hit finish and Done

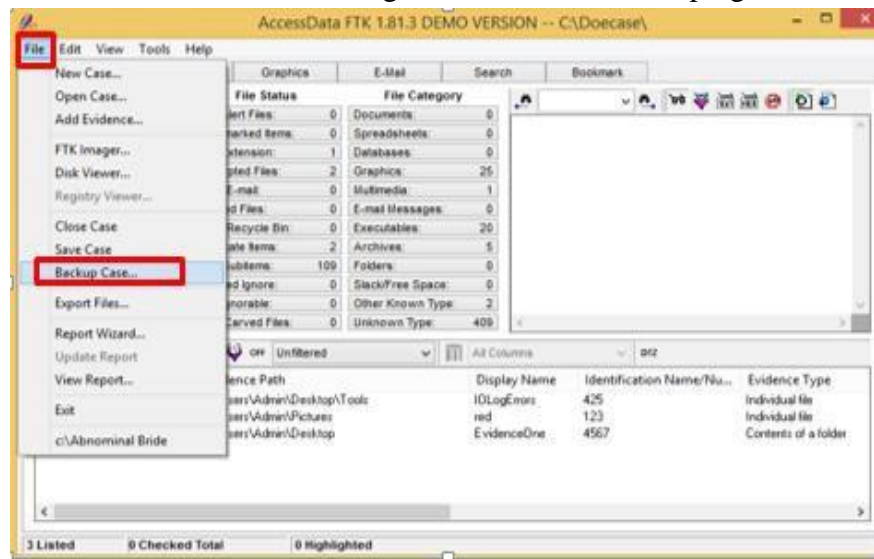


Step-6: We'll Be Presented With Findings From The Evidences Added Into The Case We Can Search, Refine, Examine The Data In The Evidence With The Help Of The Options Provided In The Access Toolkit.

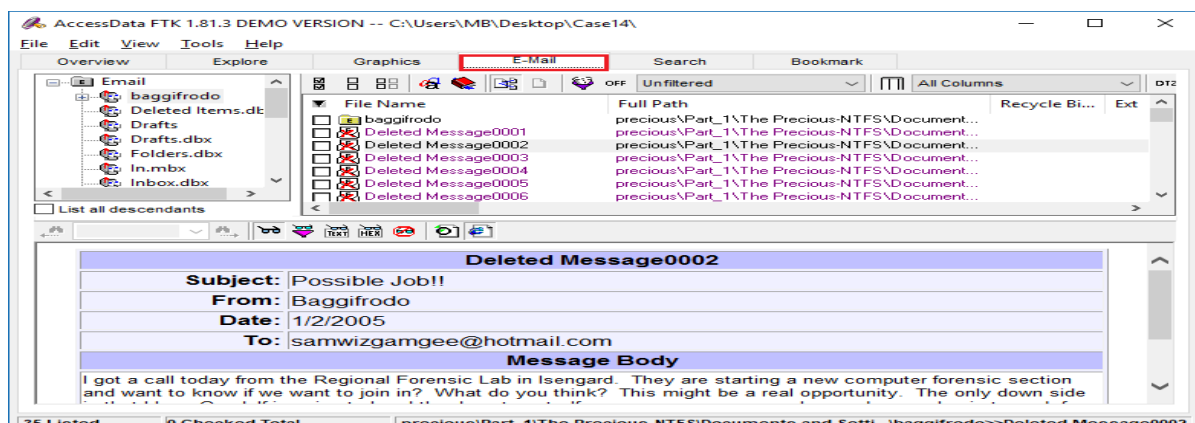


Step-7: We Can Create The Backup Of The Case By Selecting The Backup Case Option In The

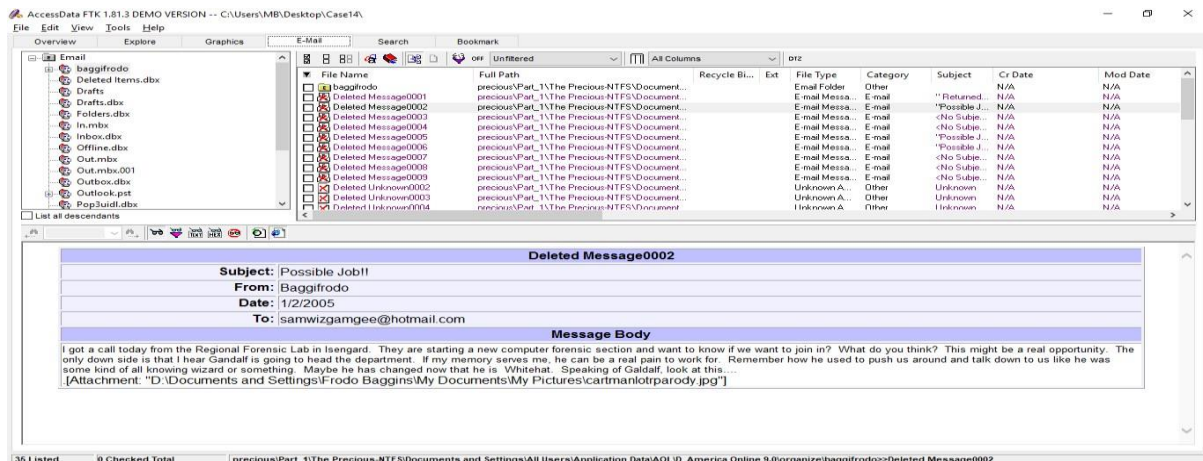
File Menu And Then Providing The Location For Keeping The Backup File.



Step 8: (Email Forensics Using FTK) Checking Email Forensic Navigate to Email tab



Select an email and investigate it

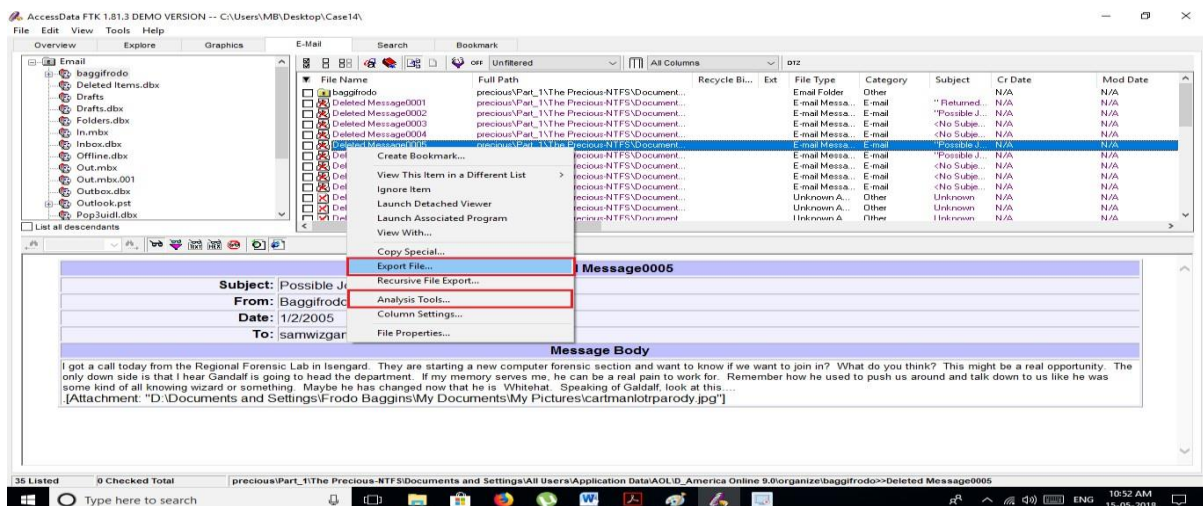


Step-9: Additional Steps Can Be Performed Like,

Exporting The File

Performing Analysis w.r.t SHA,MD5 And Many More.

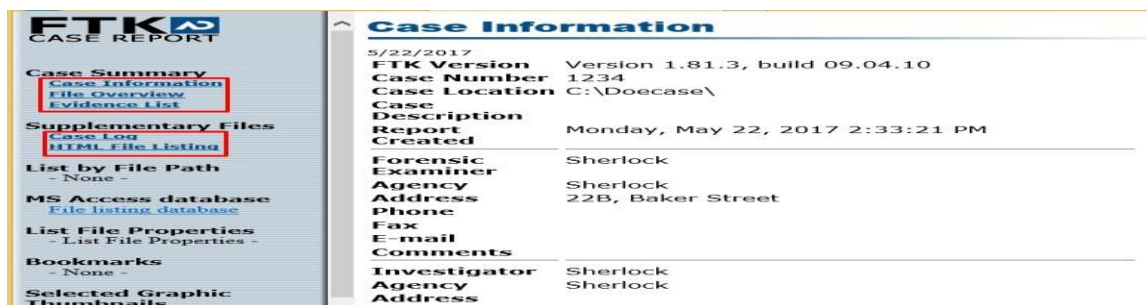
To Do So, Right Click The Desired Email And Select The Required Option.



Step-10: (Generating Report using FTK) 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.



Practical 3

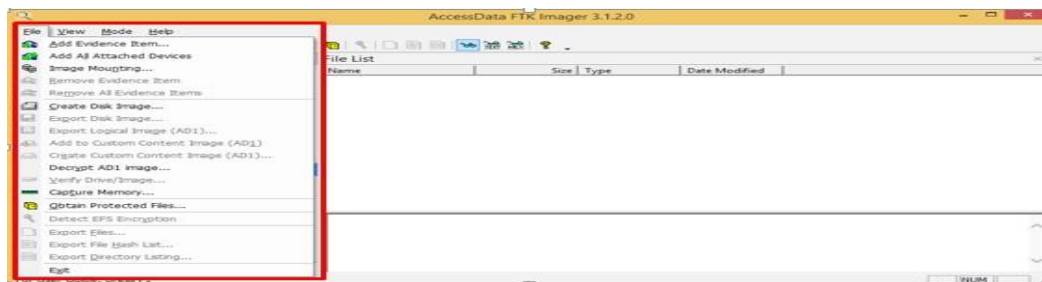
Aim : Using File Recovery Tools [FTK Imager] Creating Image

Step-1: Open Access FTK Imager

Step-2: In The Resulting Application, Many Options Will Be Provided

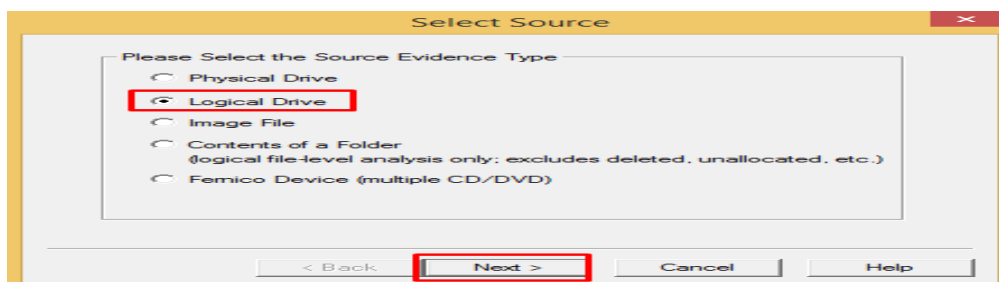
We Will Proceed With Creating A Disk Image Of A Logical Drive.

Select Create Disk Image.

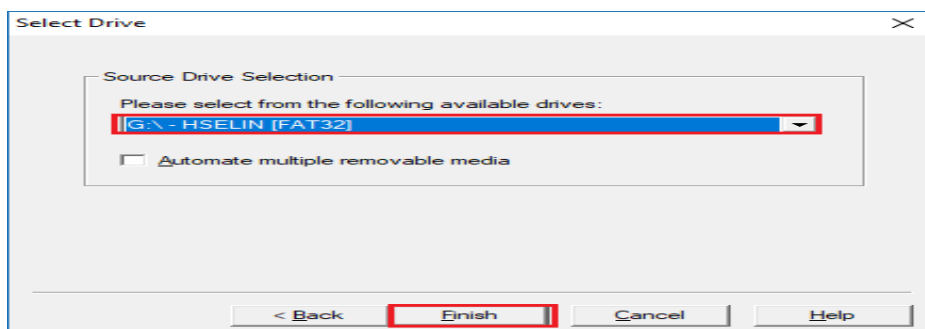


Step-3: In The Resulting Popup,

Select Logical Drive And Click Next.



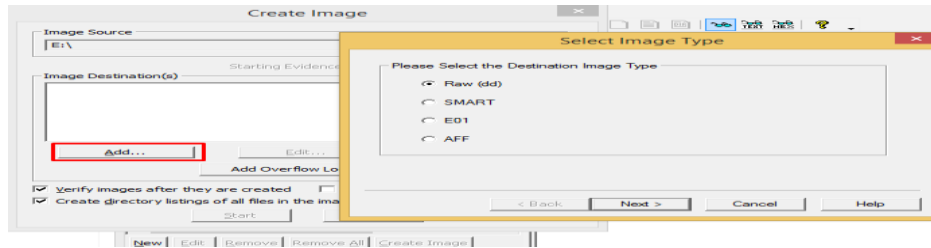
Select A Drive And Click Finish.



Step-4: Creating Image – Configuring Options

In The Resulting Popup, Click Add And Select The Image Type.

We Will Go With Raw Type Here.

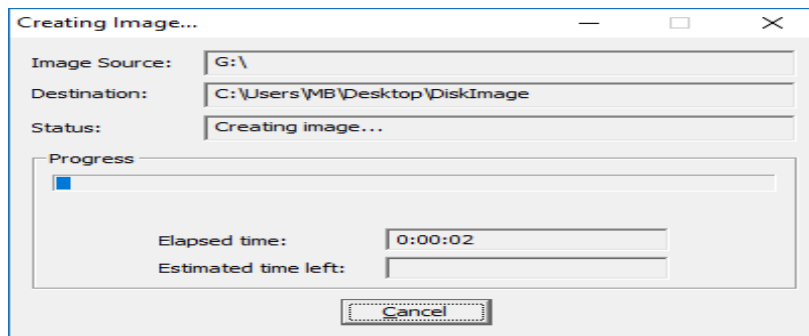


Proceed With Filling The Required Information In The Resulting Popup.

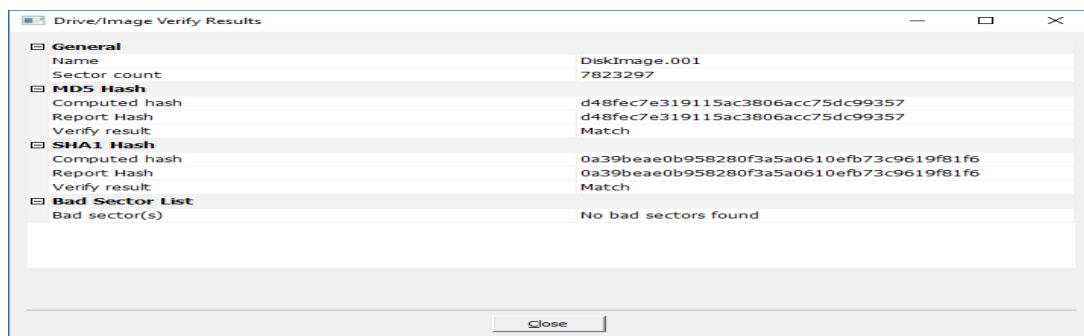
Provide The Location For The Disk Image File To Be Stored.
Click Finish.

Click Start To Proceed With The Creating Of The Image.

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



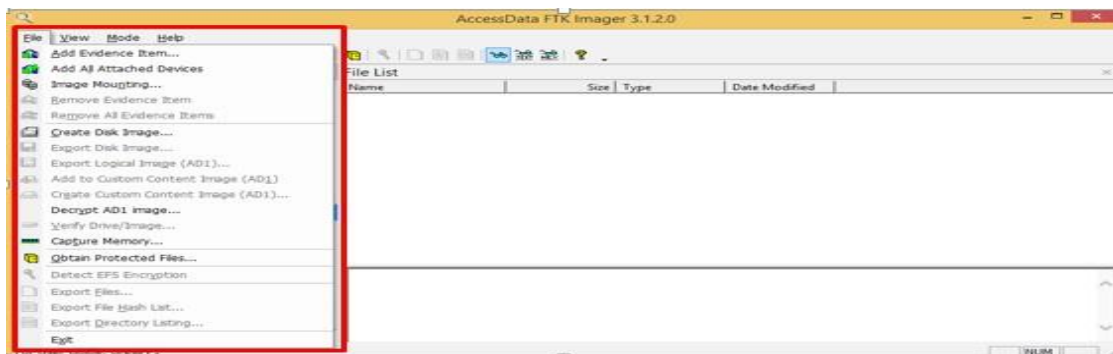
Step-5: After The Processing, A Dialog Box Will Show The Results.



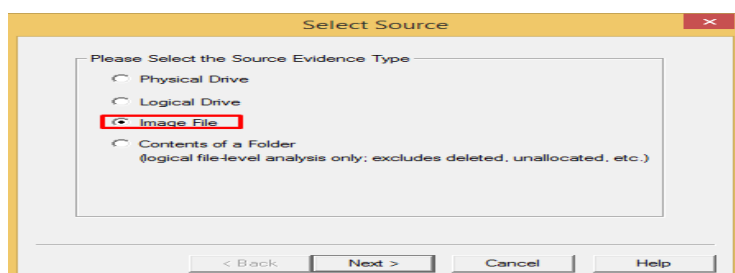
Using File Recovery Tools [FTK Imager] Using Evidence

Step-1: Open Access FTK Imager

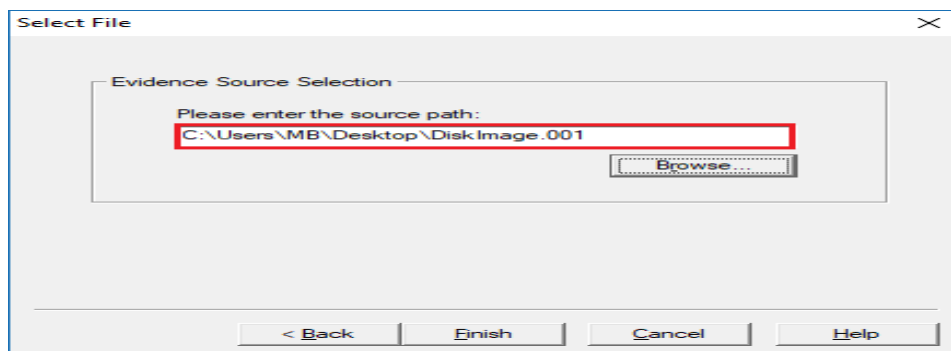
Step-2: In The Resulting Application, Many Options Will Be Provided
We Will Proceed With Adding An Evidence File.
Select Add Evidence Item.



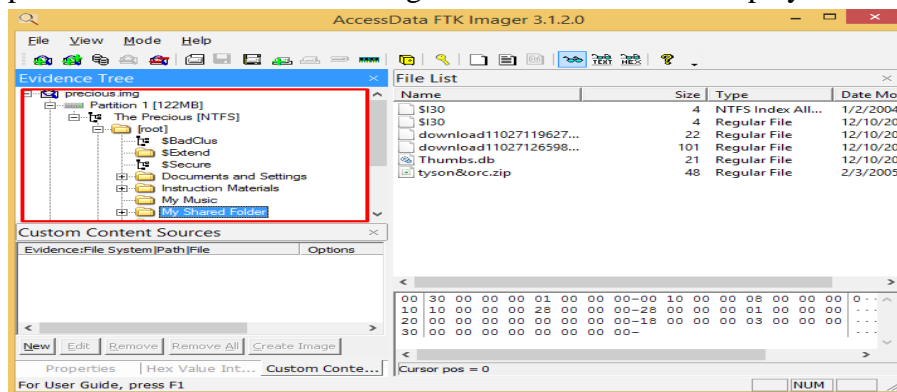
Step-3: In The Resulting Popup Select The Image File Option And Click Next



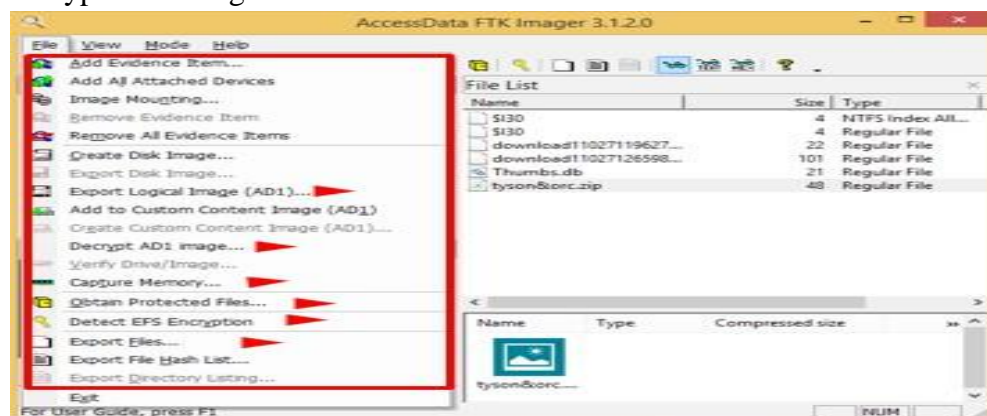
Step-4: Provide The Location Of The Image File To Be Used
Click Finish.



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.

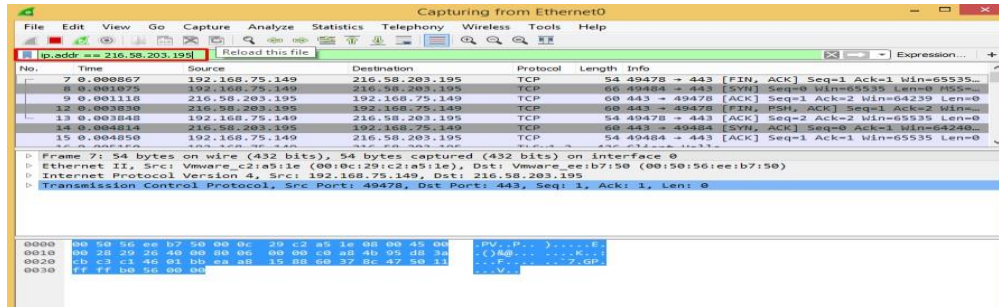
Practical 4

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

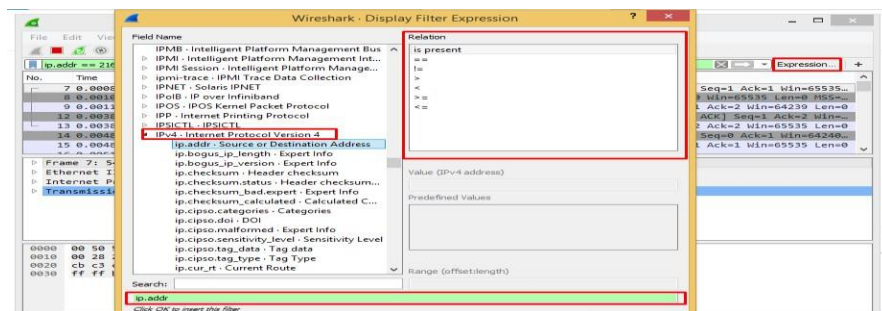
Step-1: Open Wireshark

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.

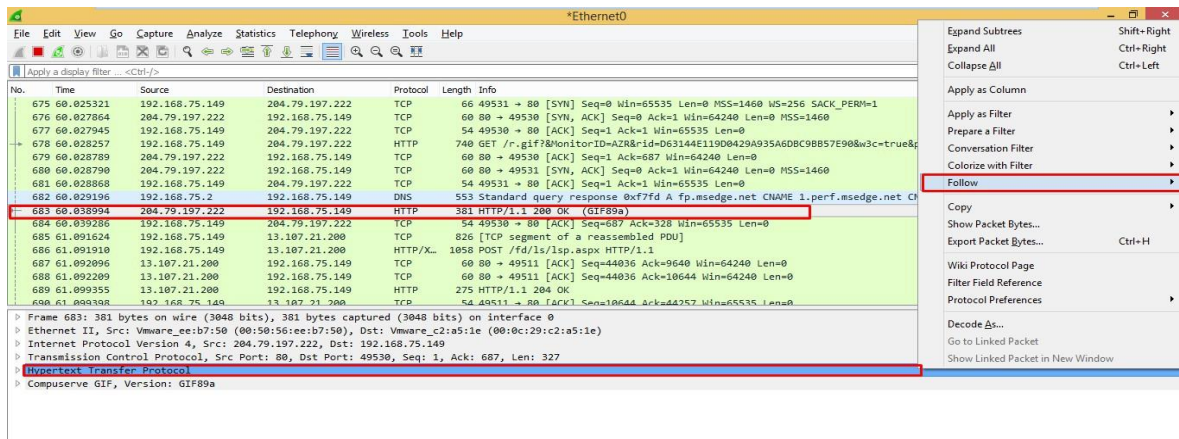


Step-3: Analyzing A Packet.

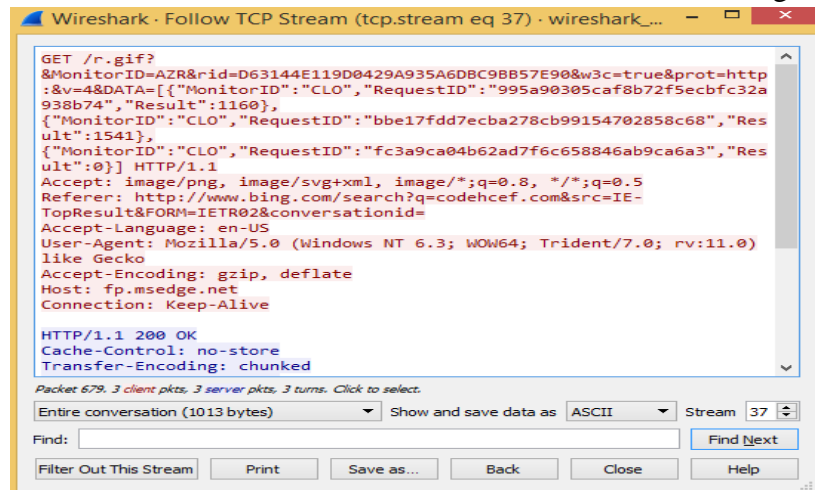
Select A Packet.

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.

```
Frame 683: 381 bytes on wire (3048 bits), 381 bytes captured (3048 bits) on interface 0
  Interface id: 0 (\Device\NPF_{3129A2D4-3C7B-4A80-A3C4-73CD7EAFB22A})
  Encapsulation type: Ethernet (1)
  Arrival Time: May 23, 2017 13:16:10.112844000 India Standard Time
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1495525570.112844000 seconds
  [Time delta from previous captured frame: 0.009798000 seconds]
  [Time delta from previous displayed frame: 0.010205000 seconds]
  [Time since reference or first frame: 60.038994000 seconds]
  Frame Number: 683
  Frame Length: 381 bytes (3048 bits)
  Capture Length: 381 bytes (3048 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: eth:ethertype:ip:tcp:http:data:image-gif]
  [Coloring Rule Name: HTTP]
```

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

Practical 5

Aim: Using Web attack detection tools [Wireshark]

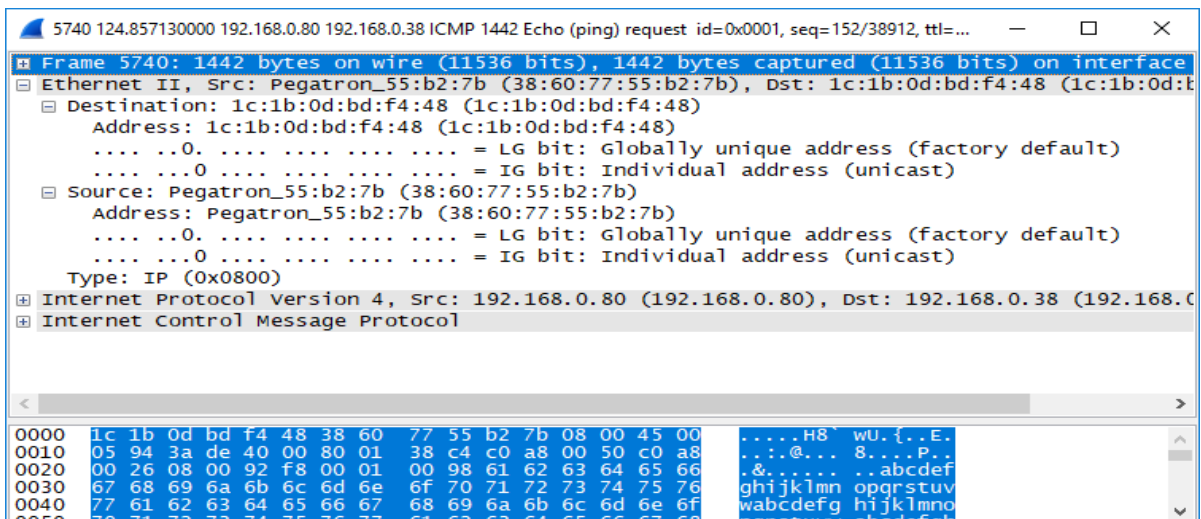
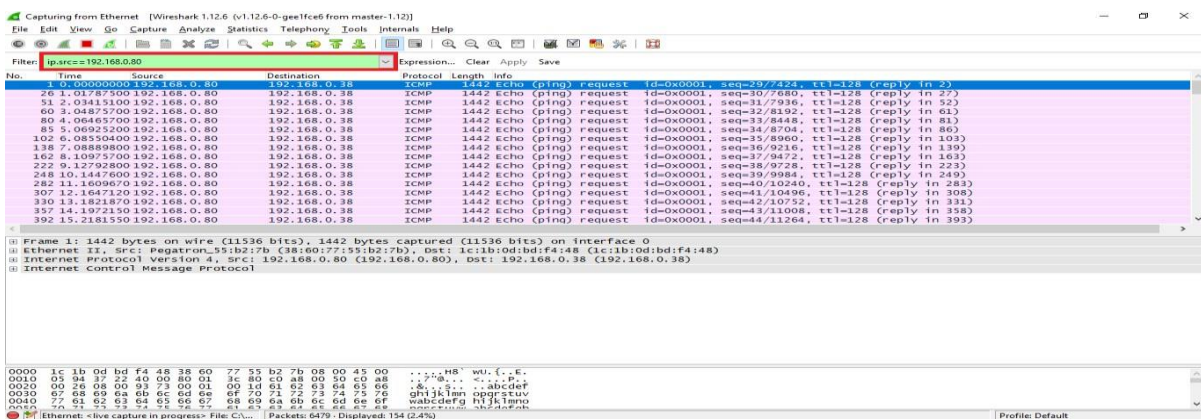
Step-1: Open Wireshark

From 1 computer ping your computer 's IP and monitor it using wireshark

```
Command Prompt - ping 192.168.0.38 -l 1400 -f -t

C:\Users\MCC>ping 192.168.0.38 -l 1400 -f -t

Pinging 192.168.0.38 with 1400 bytes of data:
Reply from 192.168.0.38: bytes=1400 time<1ms TTL=128
Reply from 192.168.0.38: bytes=1400 time<1ms TTL=128
Reply from 192.168.0.38: bytes=1400 time<1ms TTL=128
```

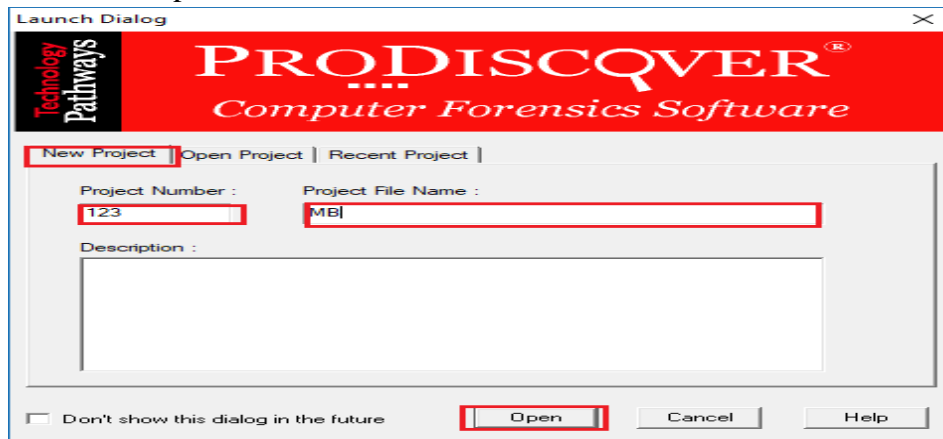


Practical 6

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.

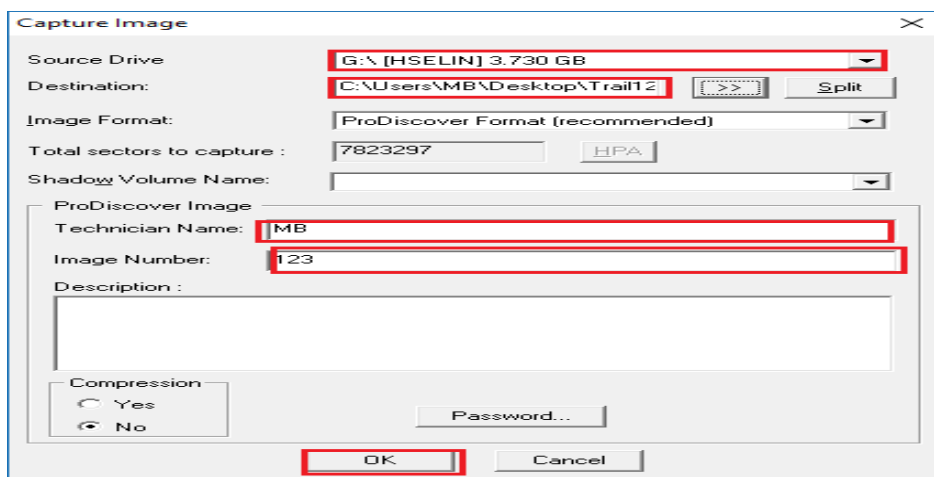


Step-3: To Create An Image For Investigation Purpose,

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. Give a Name for Destination filename and hit OK

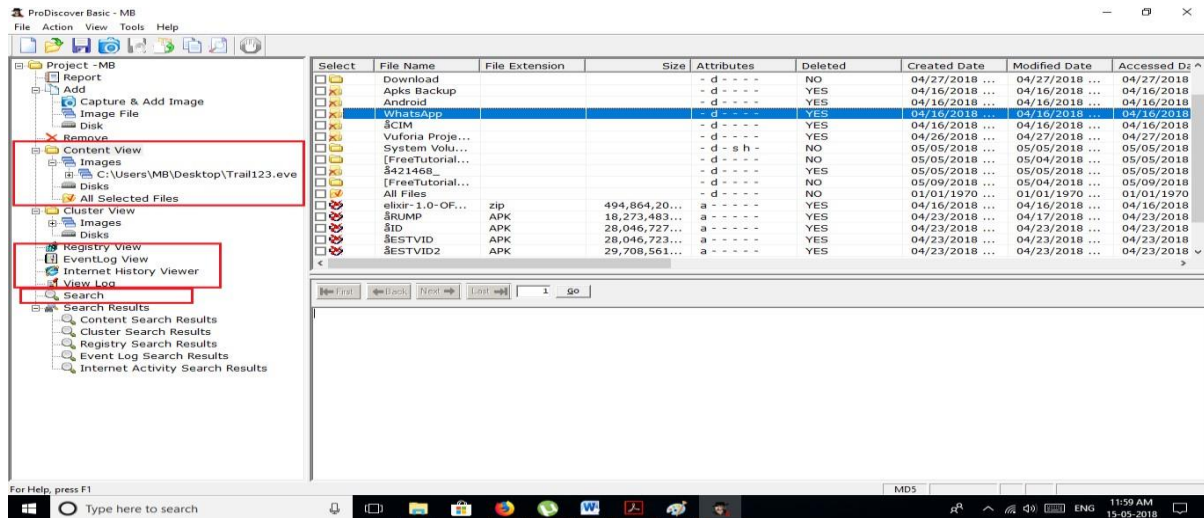
Once Done Filling All The Necessary Information, Click OK.



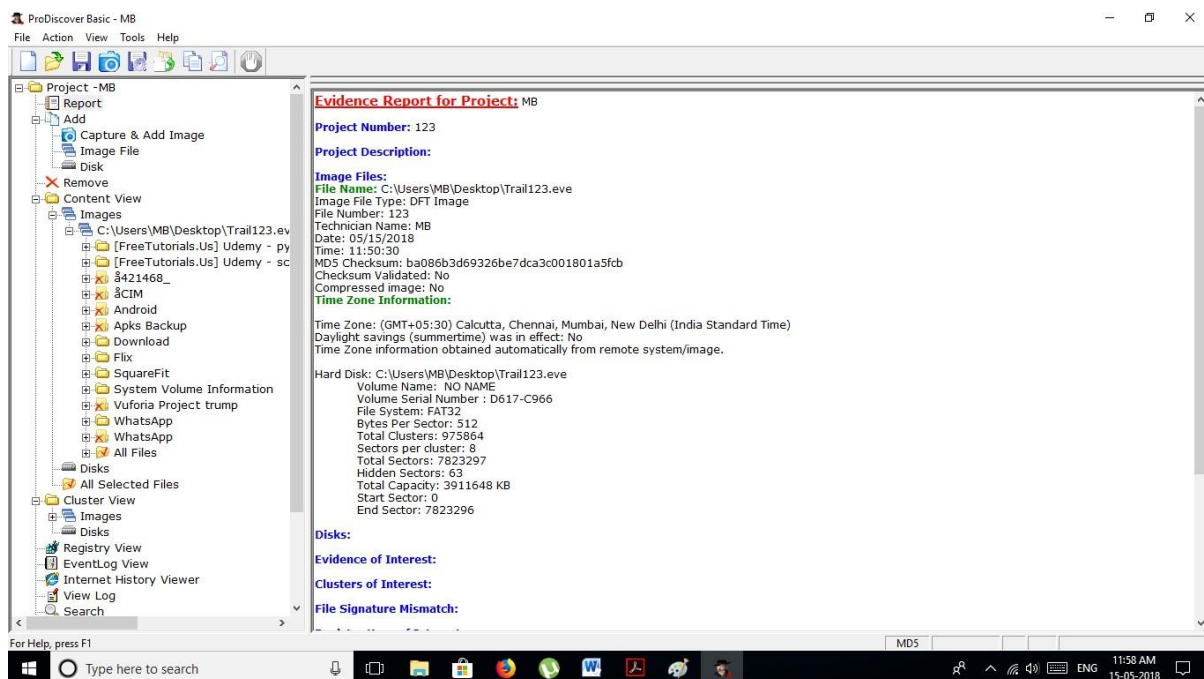
The Tool Will Now Start The Process Of Making An Image From The Given Drive.

Step-4: Now The Image Will Be Processed And The Contents Will be Presented In The Left

The Deleted Files, Registry Files And Many More Data Can Be Viewed.



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



Practical 7

Aim: Using Steganography Tools [S-Tools]

Step-1: Open S-Tools

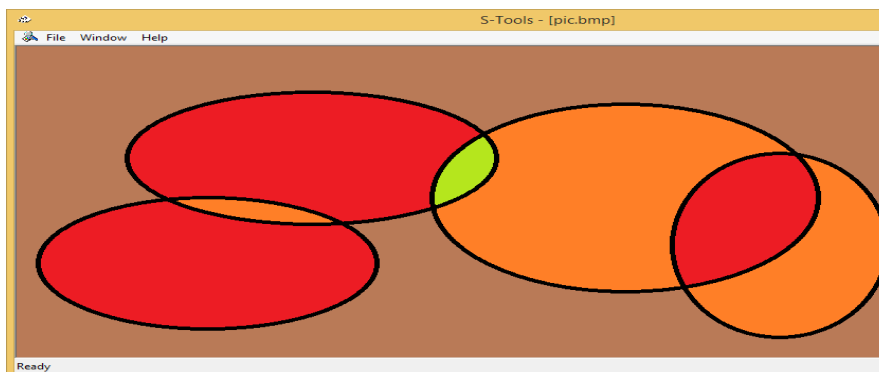
Step-2: Create A .bmp Image File & .txt File

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

Audio - *.wav Image - *.bmp and *.gif

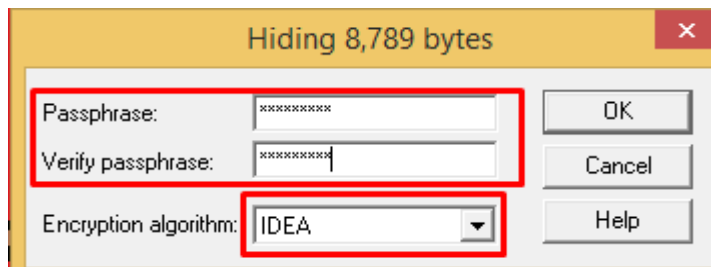
Step-3: Drag & Drop The Two Files (Image & Text)

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.

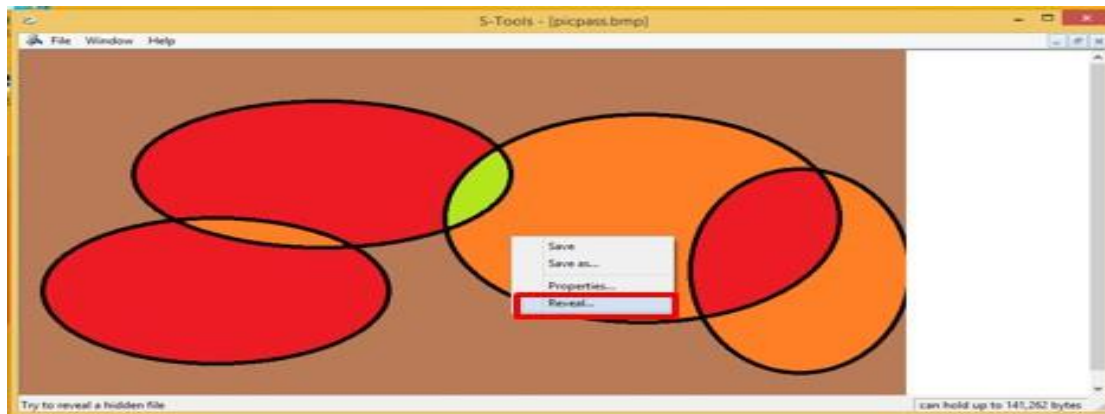


Step-5: Save The Image Into The Desired Location Of Your System.

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.

Revealed files:

Name	Size	
Info.txt	118	
Pic.bmp	1,131,654	

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.

Practical 8

Aim: Performing Password Cracking [Cain & Abel]

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

Step-2: Creating Users

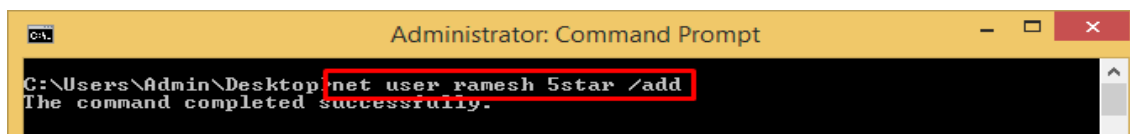
Open Command Line As Administrator

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

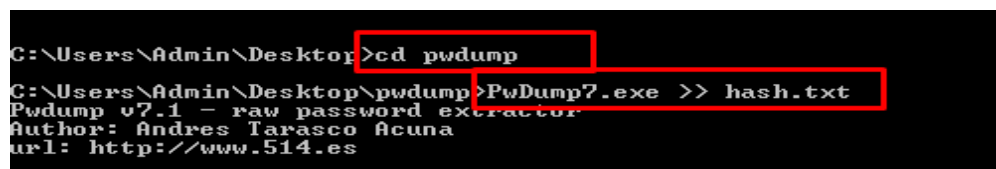
Step-3: Now Navigate To The pwdump Folder Present In Your System.

Type Command,

Pwdump7.exe >> hash.txt

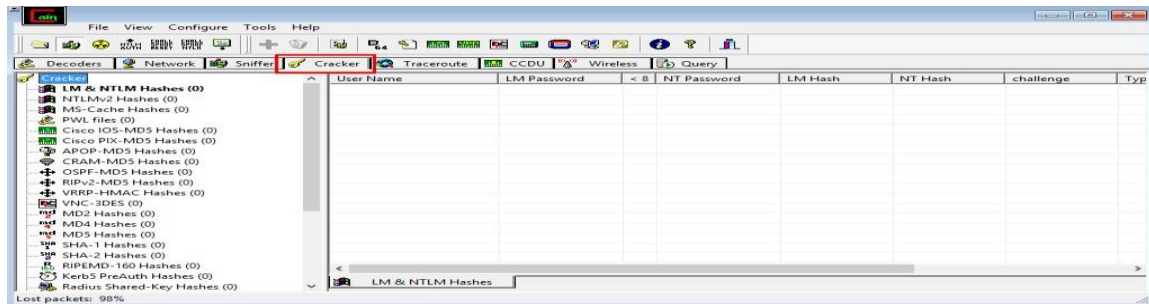
Pwdump7(We have installed The pwdump 7th release)

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

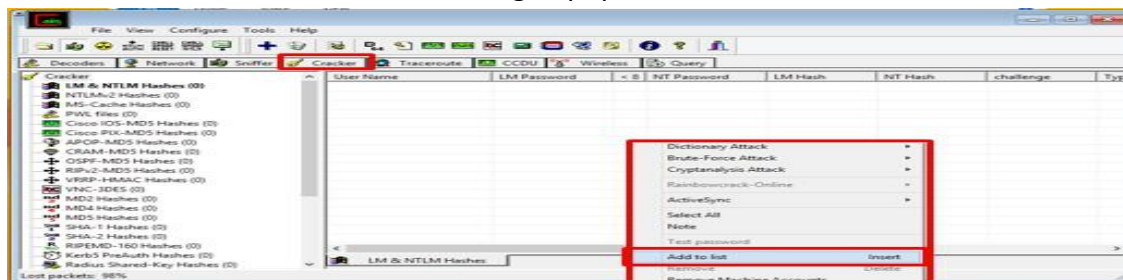


Step-4: Start Cain & Abel As Administrator

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.

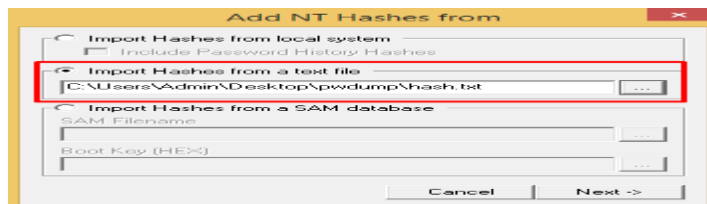


Step-7: In The Resulting Popup,

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.

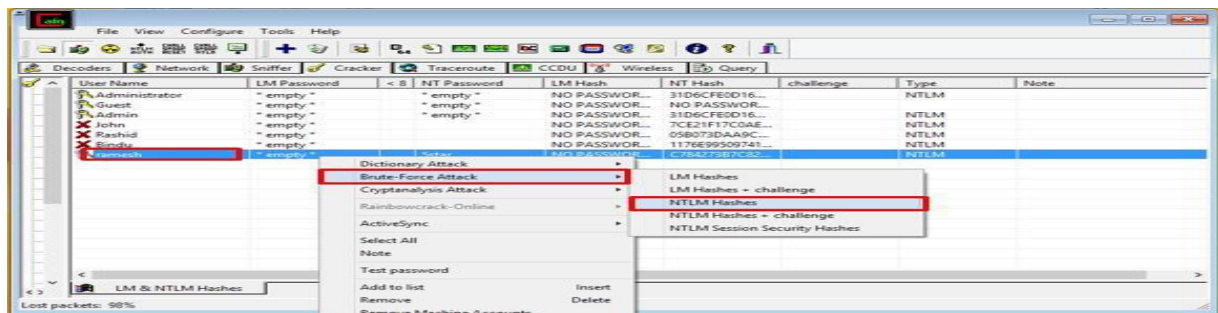
User Name	LM Password	< 8	NT Password	LM Hash	NT Hash	challenge	Type	Note
Administrator	* empty *		* empty *	NO PASSWOR...	31D6CFE0D16...		NTLM	
Guest	* empty *		* empty *	NO PASSWOR...	NO PASSWOR...			
Admin	* empty *		* empty *	NO PASSWOR...	31D6CFE0D16...		NTLM	
John	* empty *			NO PASSWOR...	7CE21F17C0AE...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

Step-9: Select An Account,

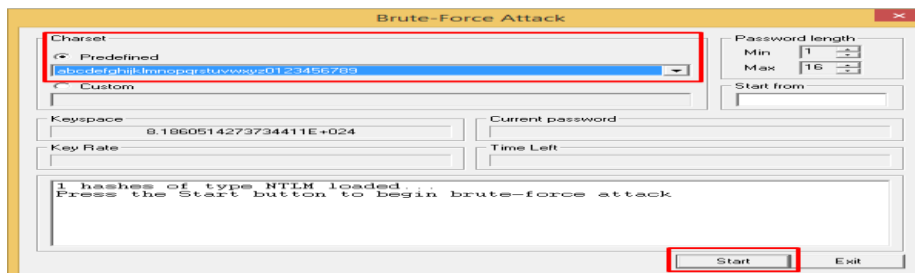
Right Click On That User Account

Select Brute-Force Attack

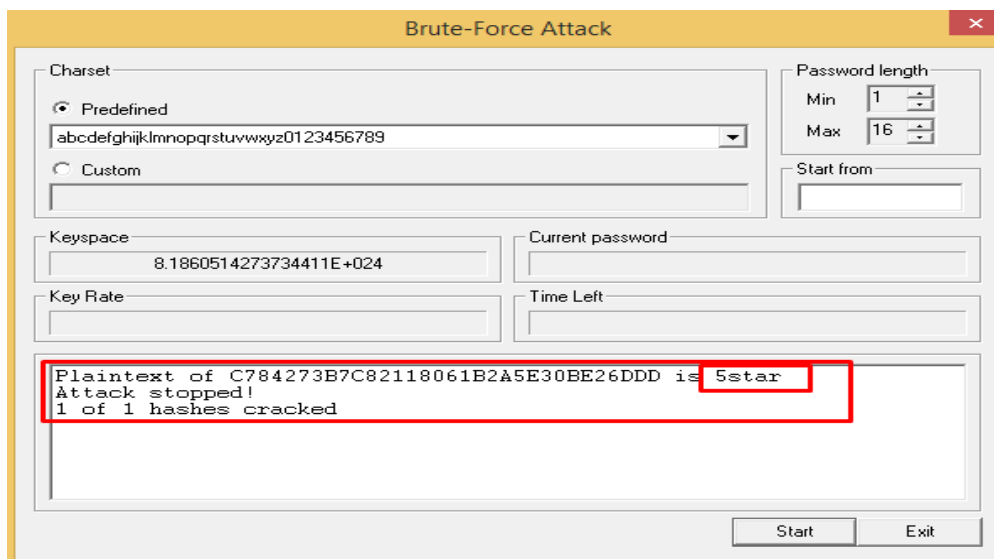
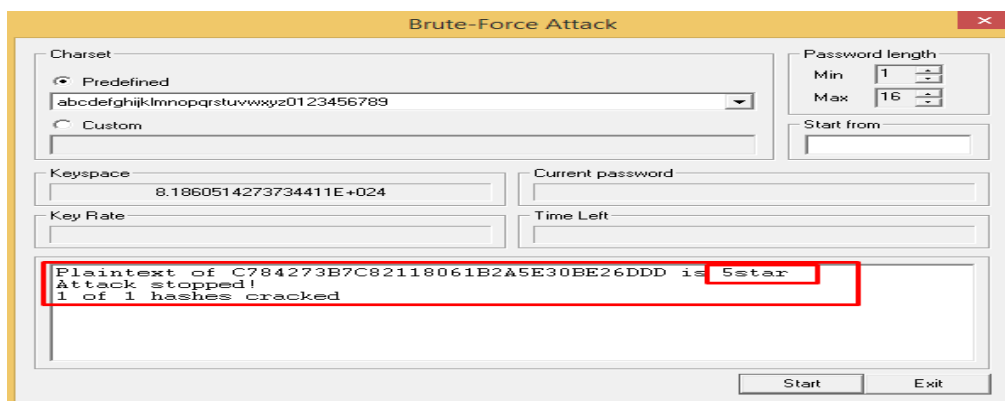
Select NTLM Hashes



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.

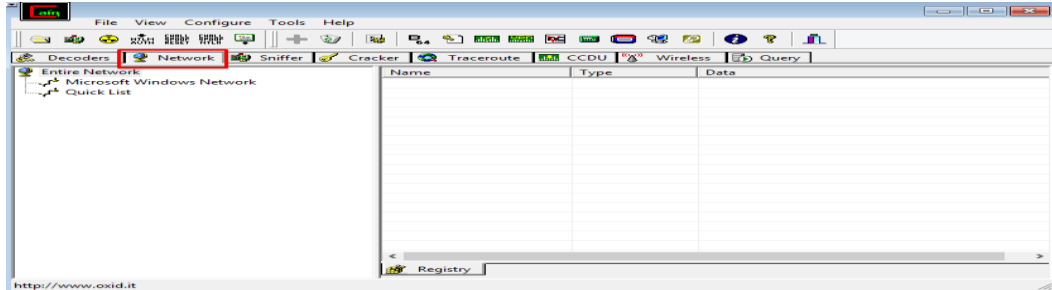


Practical 9

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

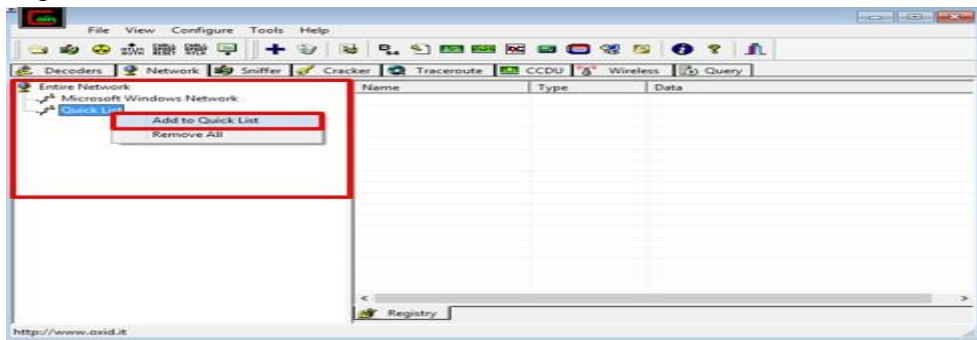
Step-1: Open Cain & Abel As Administrator

Step-2: Go To Network Tab



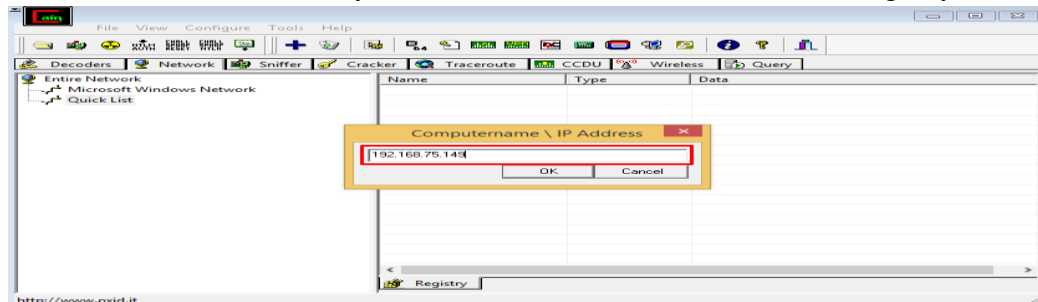
Step-3: Expand Entire Network

Right Click Quick List & Select Add To Quick List.



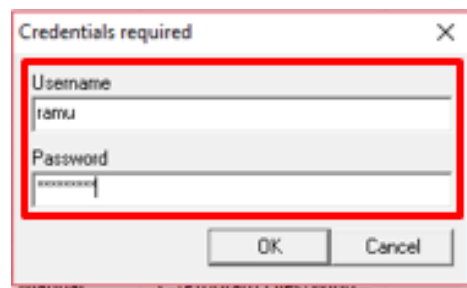
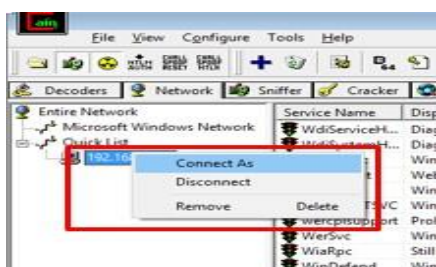
Step-4: In The Resulting Popup Box, Enter The IP Address Of The System You Want To Study

(You Can Use Your Own System's IP Address To Examine Your Registry)



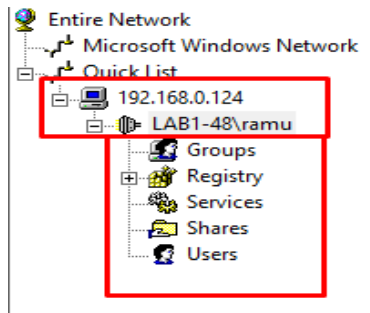
To Access Other System's Registry & Services, Use That System's IP Address

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

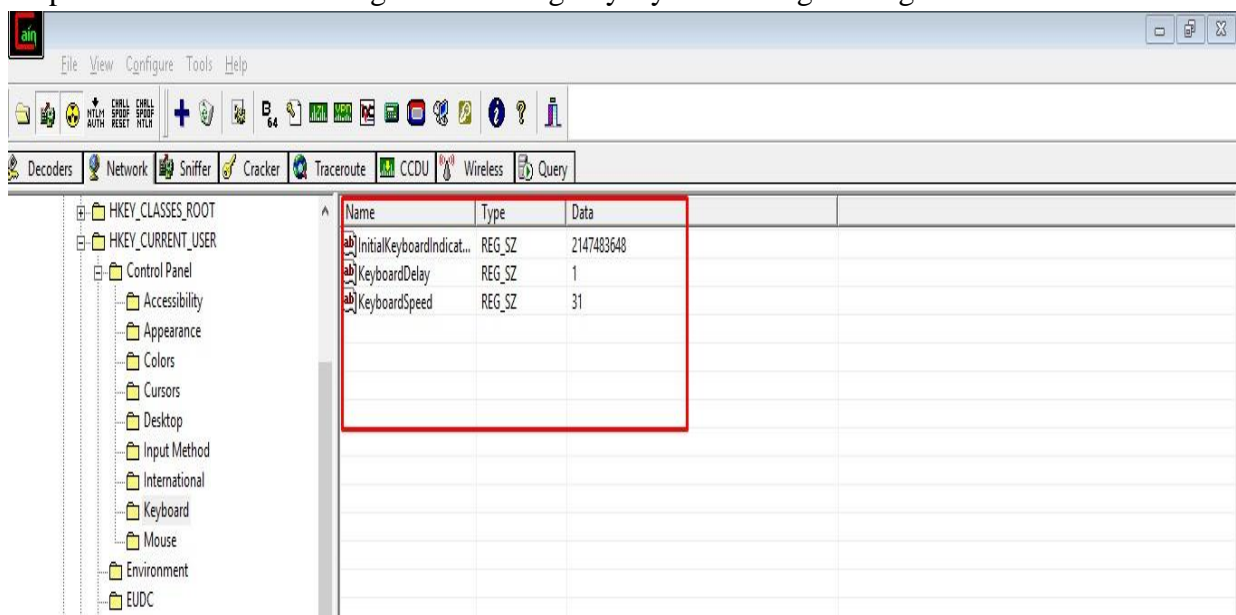
- a. Groups
- b. Registry
- c. Services
- d. Shares
- e. Users



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.

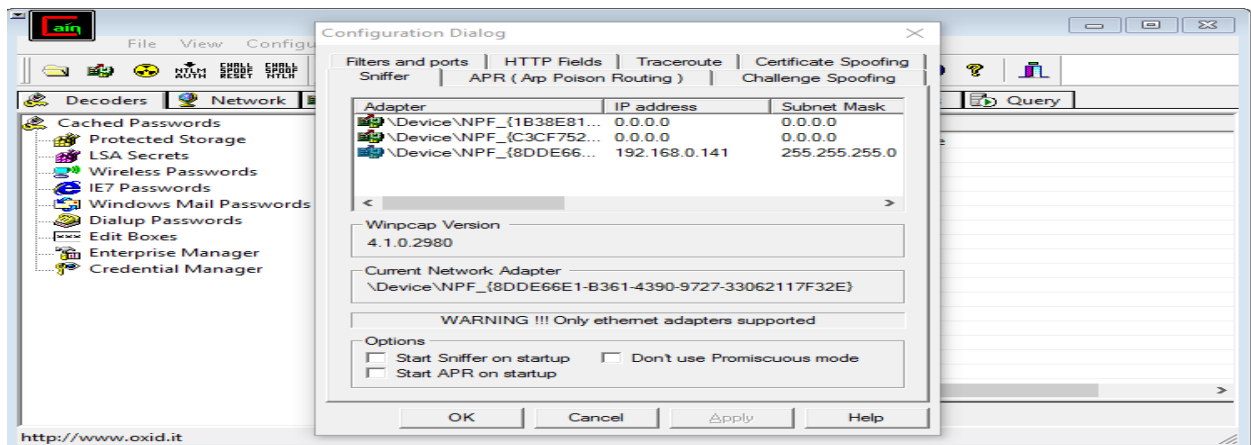
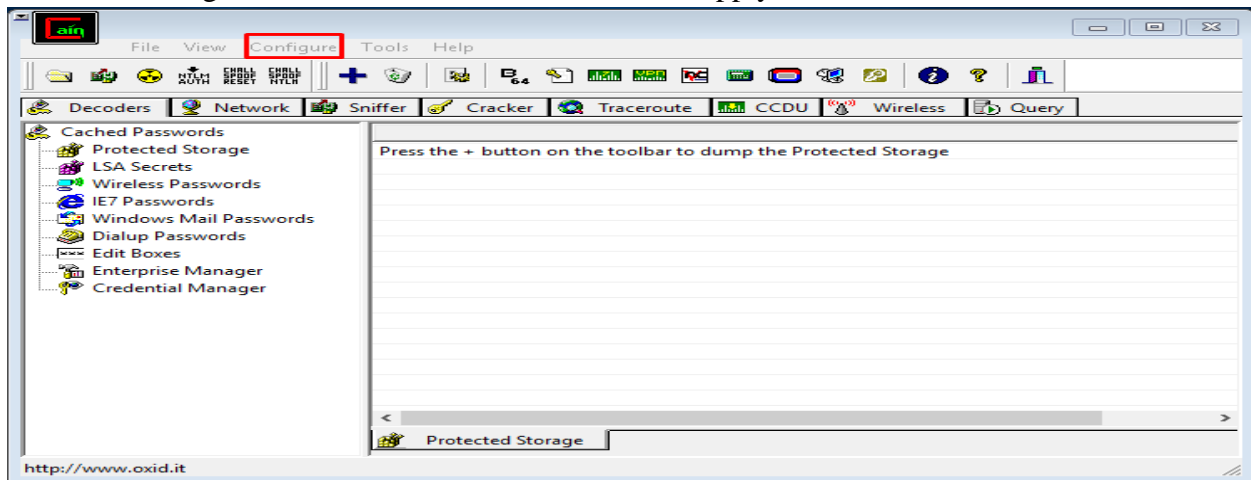
Practical 10

Aim: Performing Sniffing [Cain & Abel]

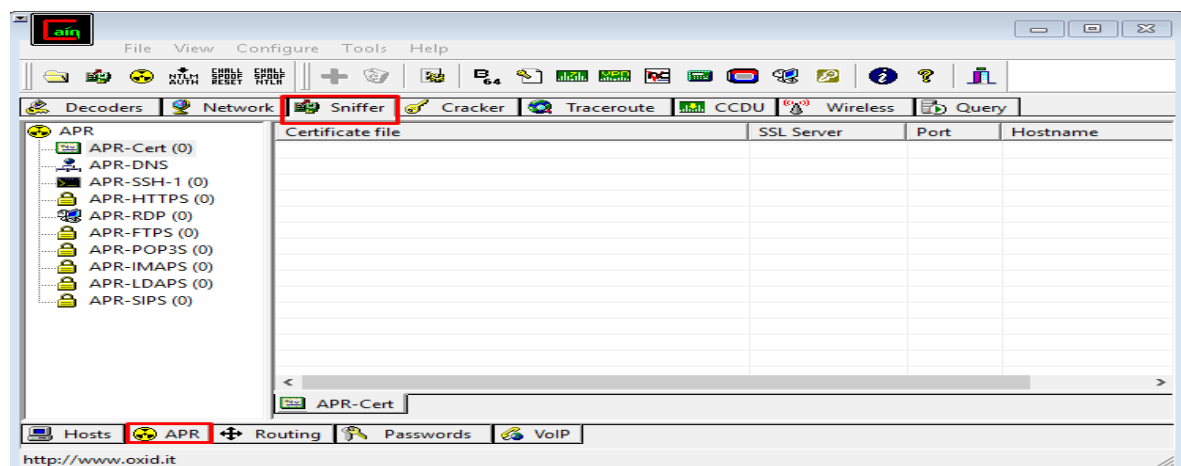
Steps : (Note : Go to command prompt & type ipconfig & note down your IP Address.)

1. Open Cain & Abel By Running It As Administrator. (Note: Firewall Exception Might Occur, Press OK)

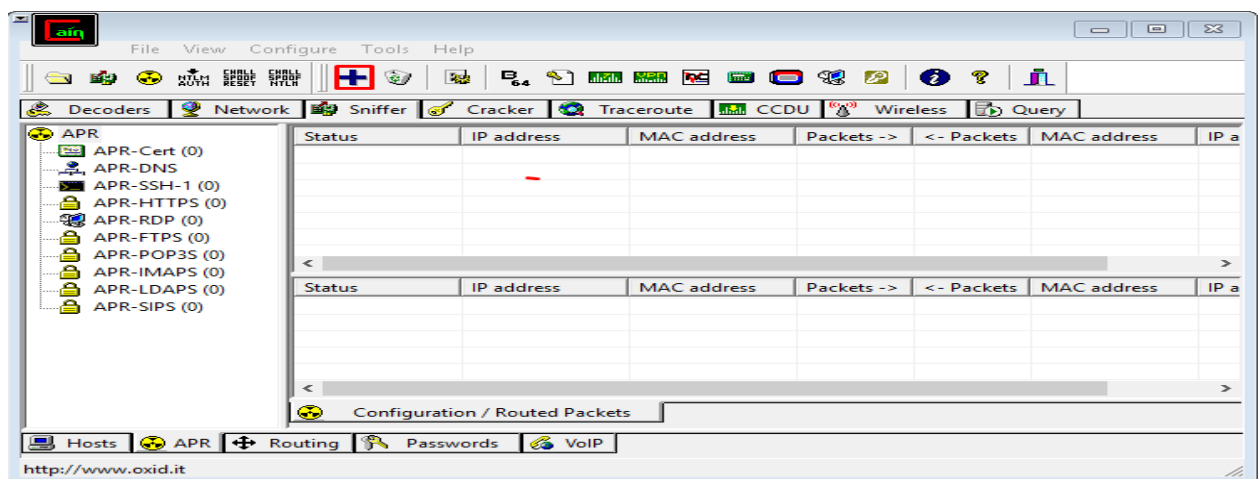
2. Go To Configure & Select Your IP Address, Press Apply & OK.



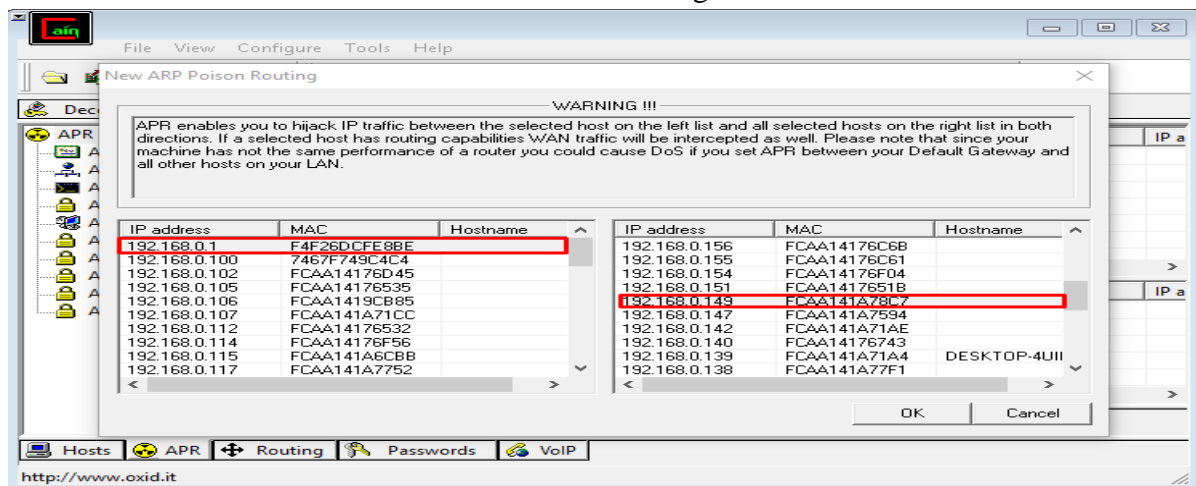
3. Now Go To Sniffer Tab On Top & Select APR Tab From Bottom.



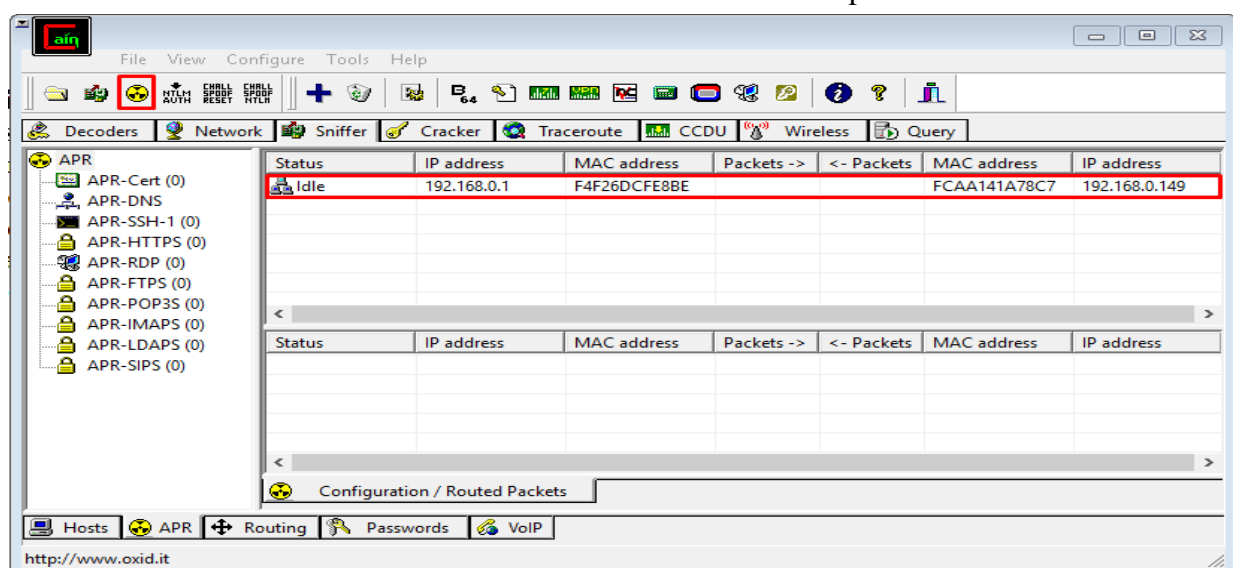
4. Single Click On The Right Above Part Of APR And Then Click On "+" Icon On Top Left.



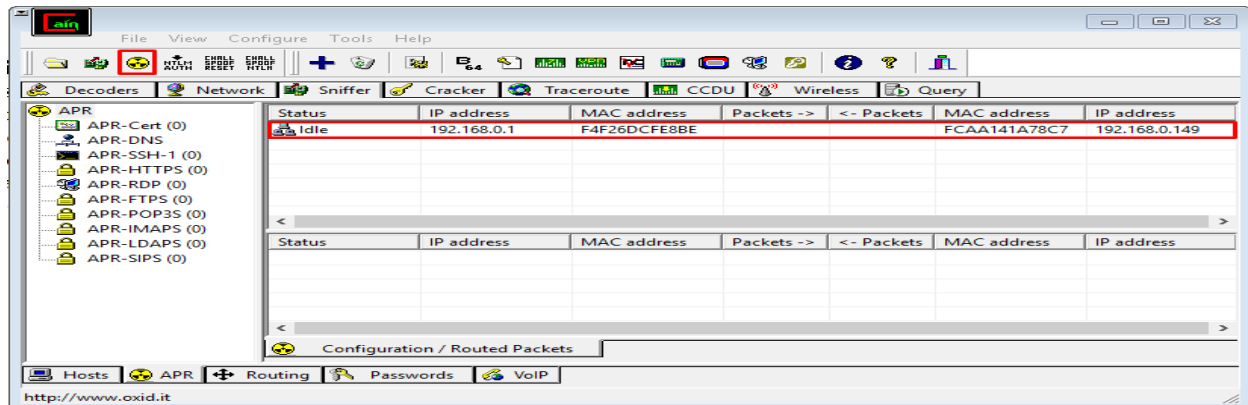
5. Now Select Your Subnet & Machine With The Target IP Address & Press OK.



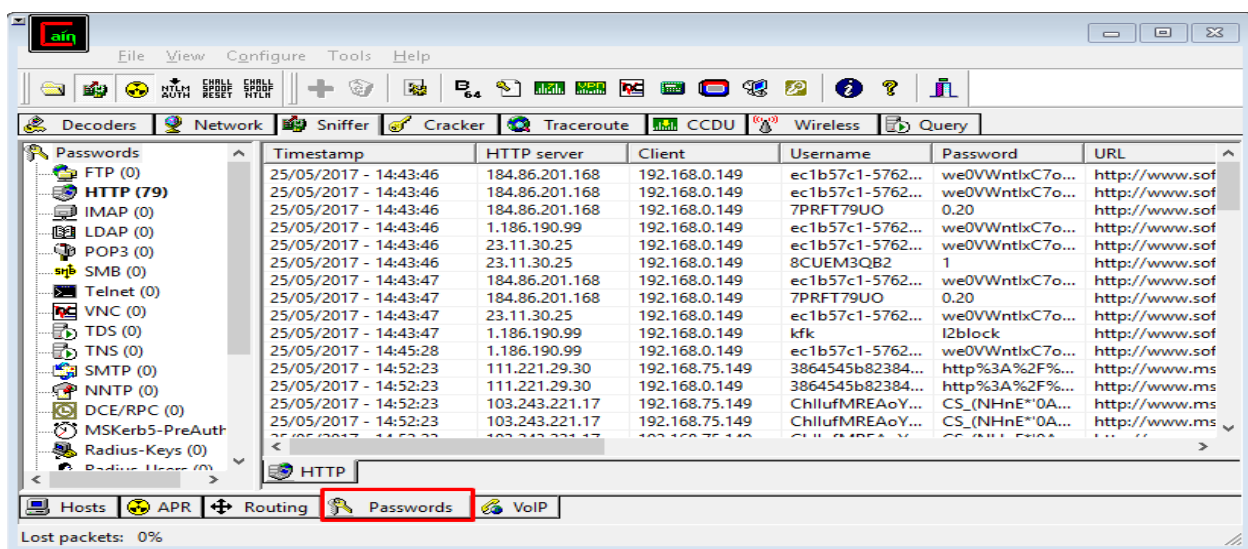
6. Select The Listed Machine & Click On Poison Icon On The Top Left.



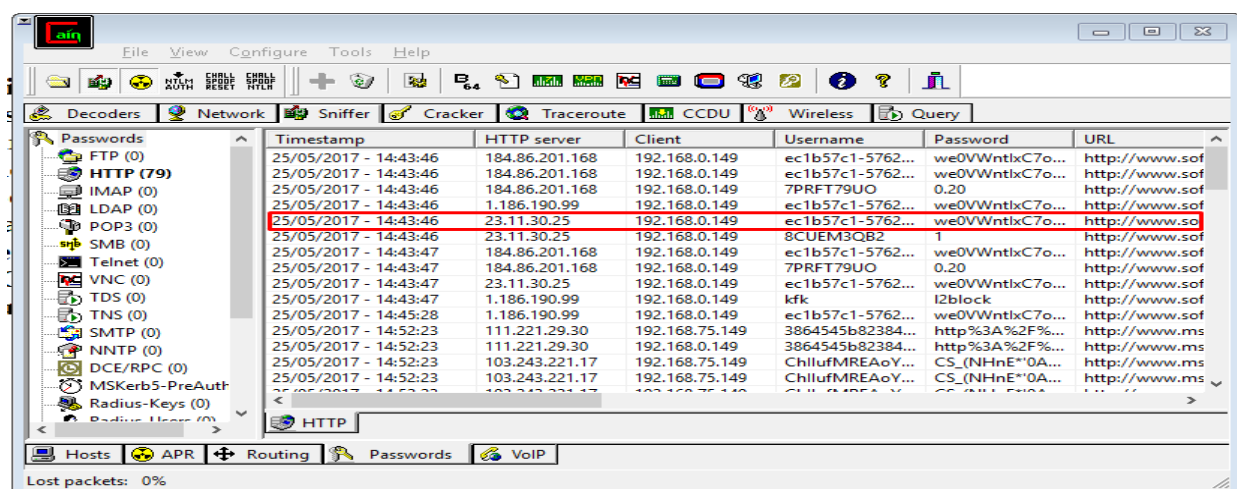
(Note : If You Get AN Exception : "Couldn't bind HTTPS acceptor socket", Press OK)



7. Go To Passwords Tab At The Bottom.



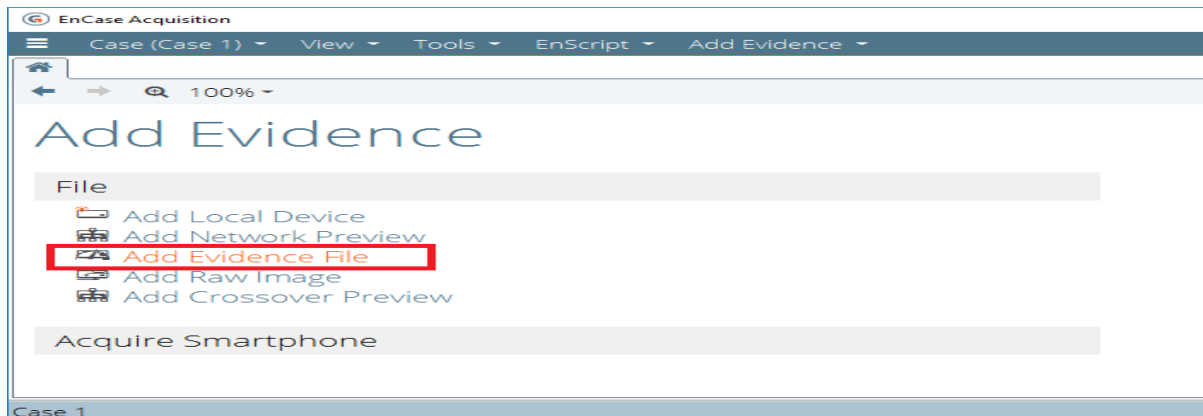
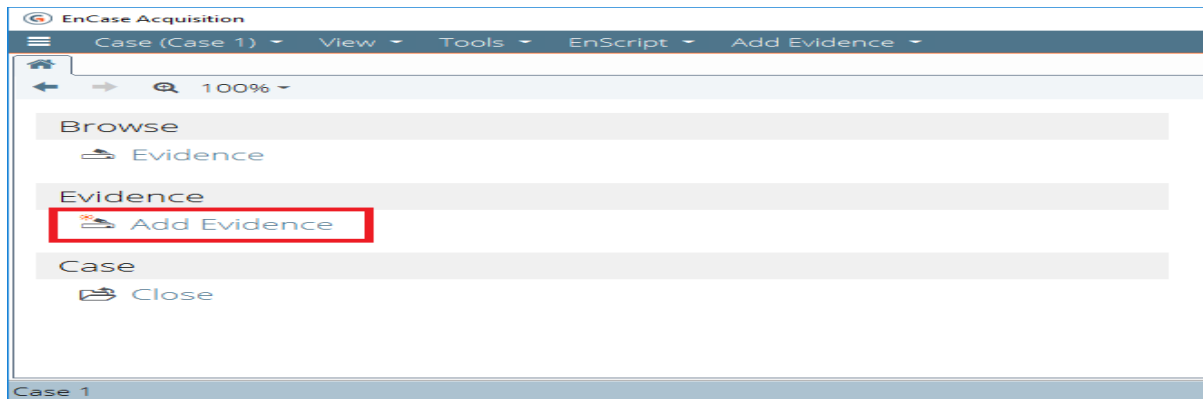
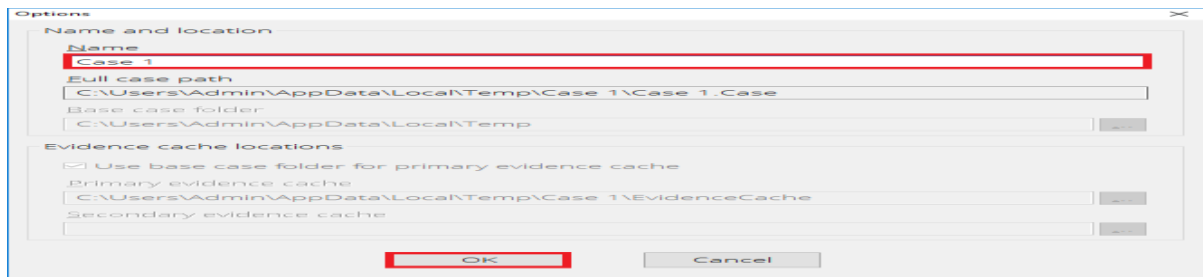
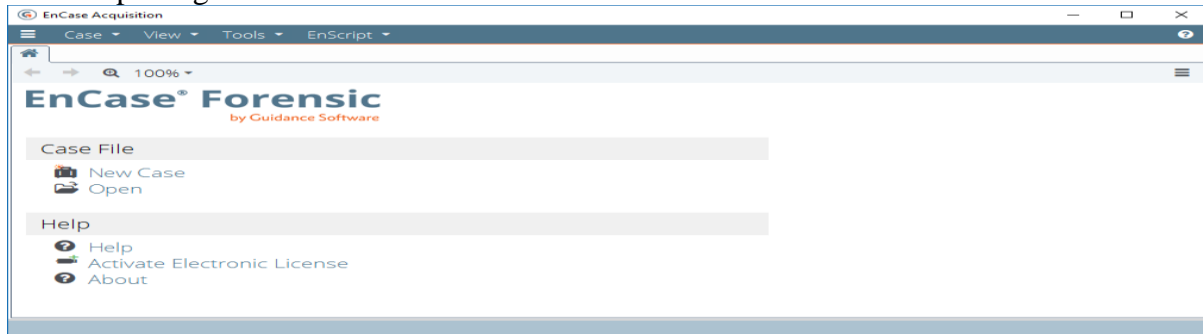
8. Sniffed Logs With All Information With Password Is Now Visible.

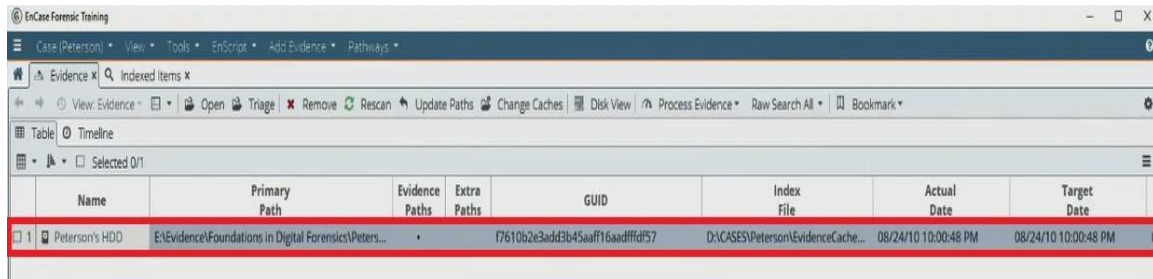
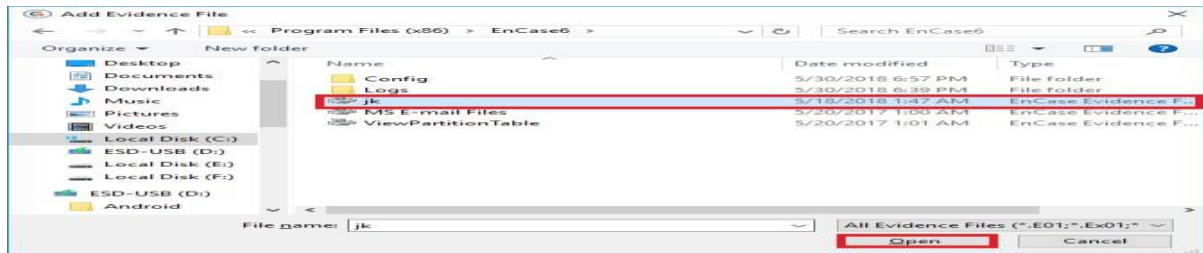


Practical No. 11

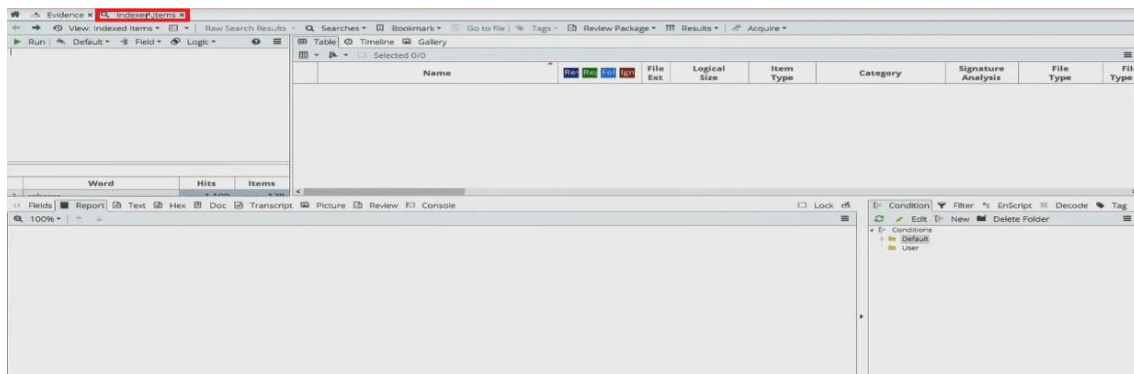
Forensics Investigation Using Encase

Aim: Exploring Encase

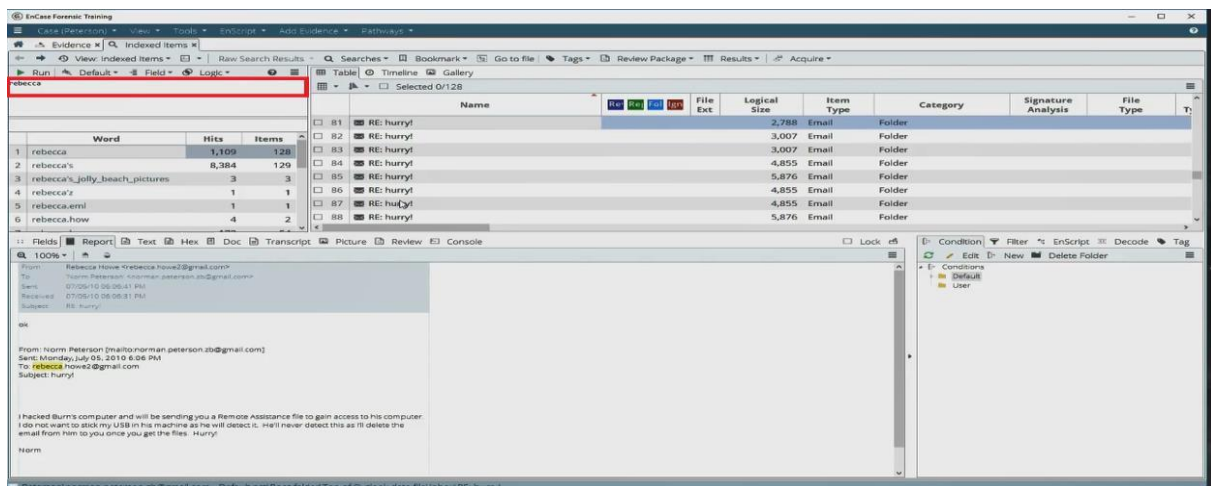




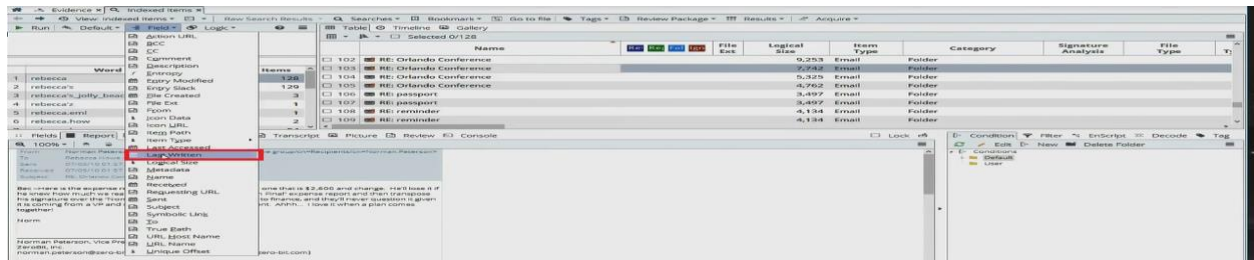
Navigate to Indexed Items



Searching keyword e.g. “Rebecca” and press Enter Key

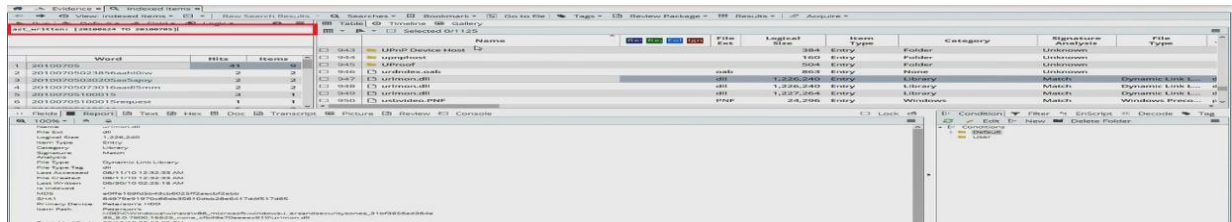


Now click on last written

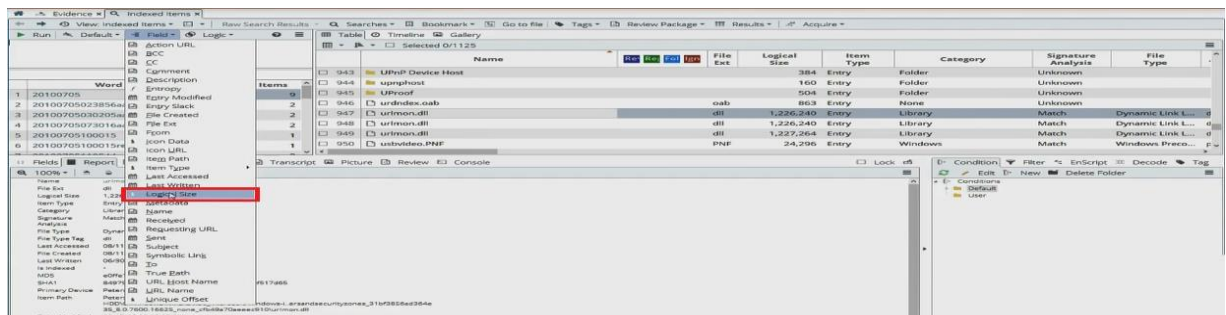


Last_written [20100624 TO 20100705]

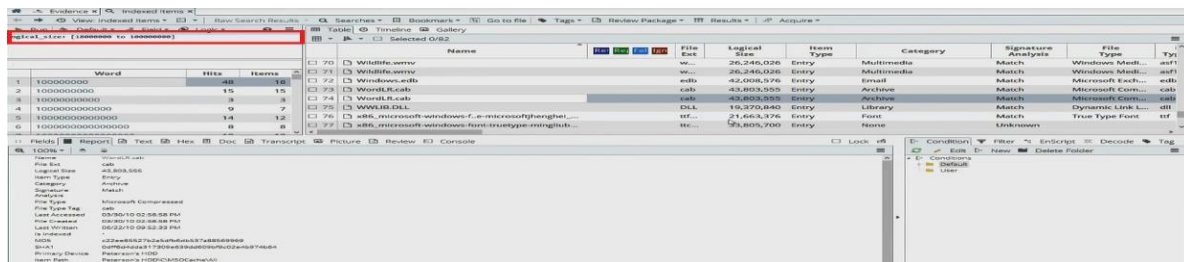
i.e last_witten [yyyymmdd To yyyymmdd] where y is year and m is month and d is day



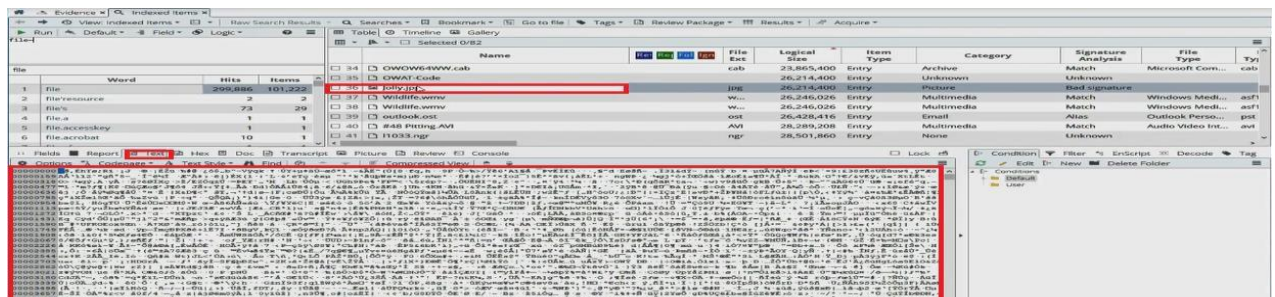
Now lets try Logical Size



Logical_size: [18000000 TO 100000000]



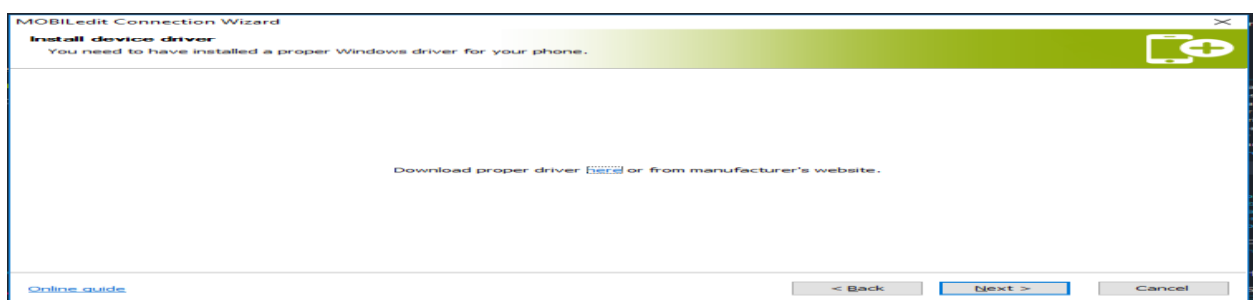
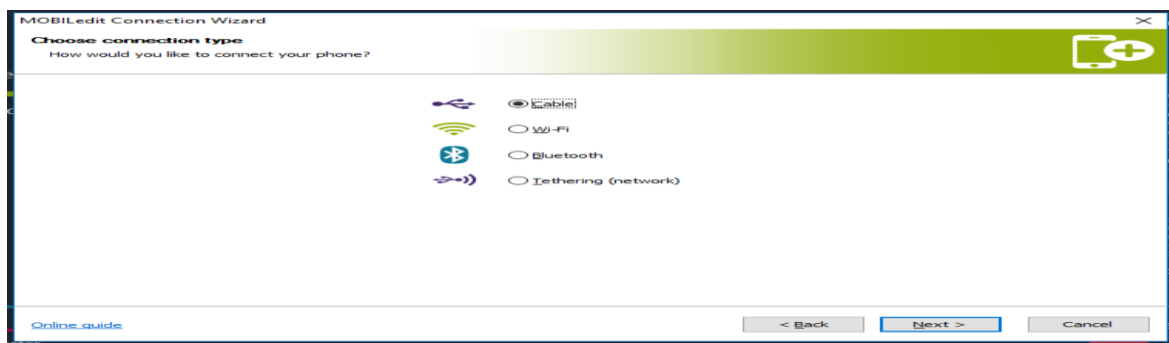
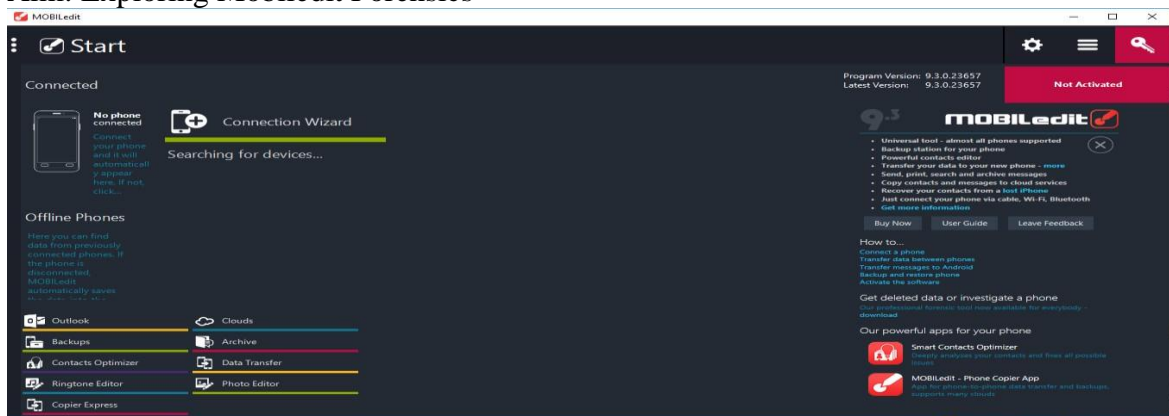
Now checking data on an File

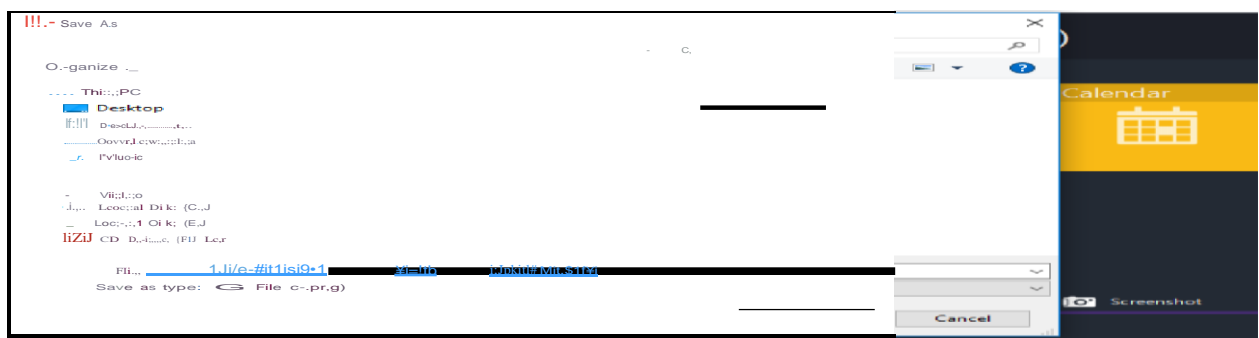
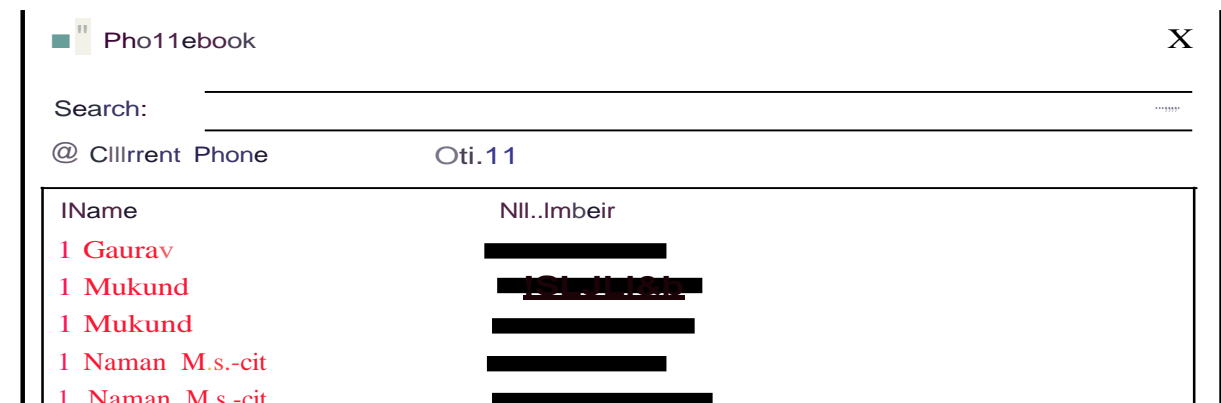
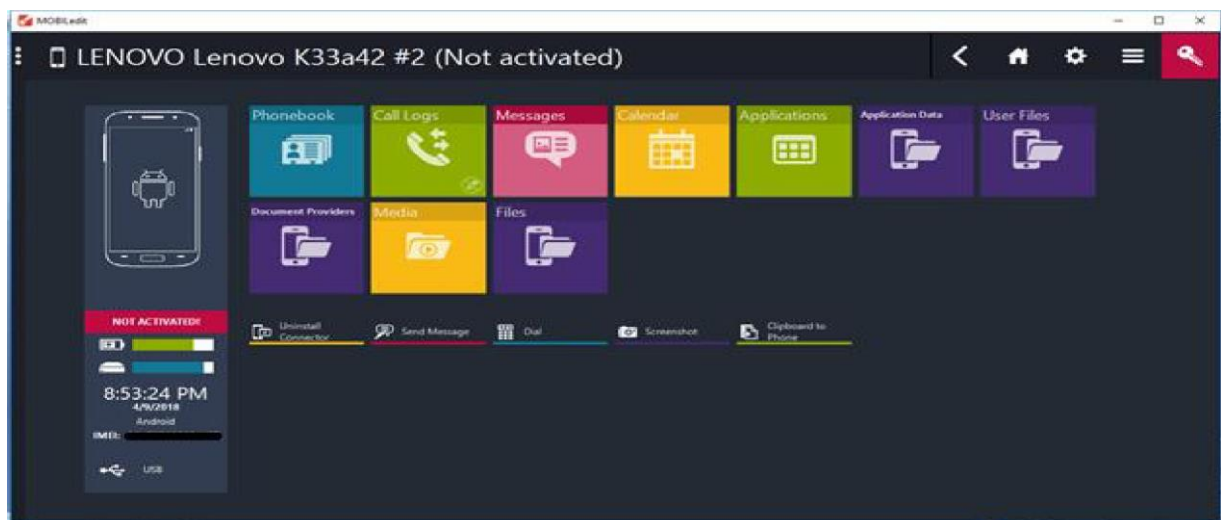
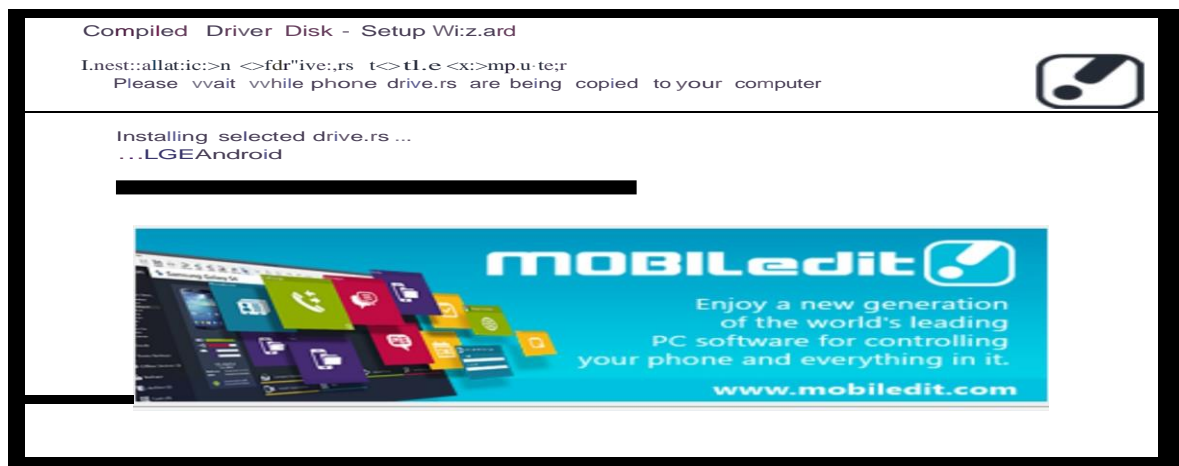


Practical No. 12

Using Mobile Forensics software tools

Aim: Exploring Mobiledit Forensics





De.skto,p

Documents

Downloads

Music

Pictures

Videos

Device,. and drives (5)

Lenovo 6 POWER

Local Disk (E:)

3116 GB free of 5.35, GB

Local Di\sk [C:]

287 GB free of 341 GB

CD Drive.(F:) Lenovo_Suite.

0 bytes free of 41.5 MB

CDF5

DVD,RW Drive (D:)

Send Message

X

To...

Phone:

UNOVQ LenovoK33a42 .t2

v

Message:

25/160(1)

1 Vignesh

Number

GSM

Pack

IJripadc

Sn

Help...

Close