Computer Forensics

Contents

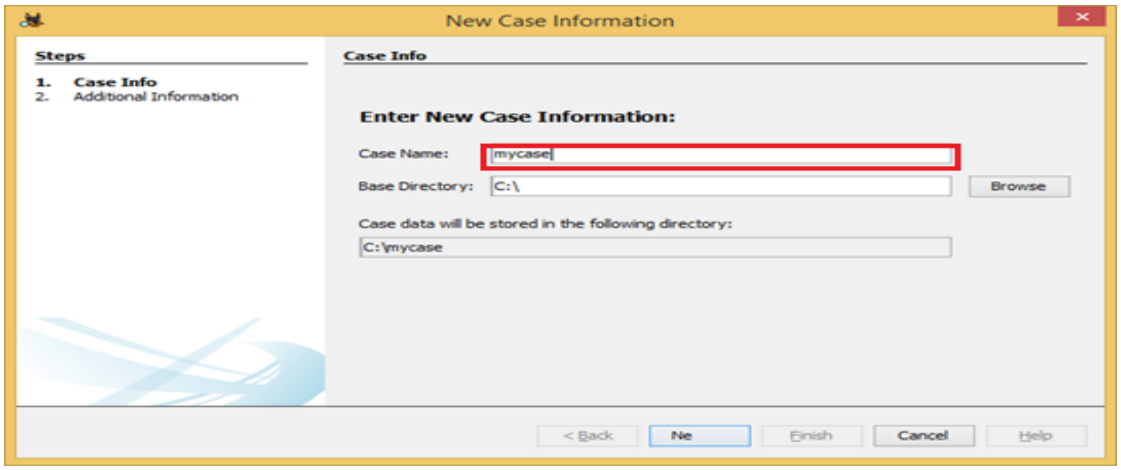
Practical 1

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

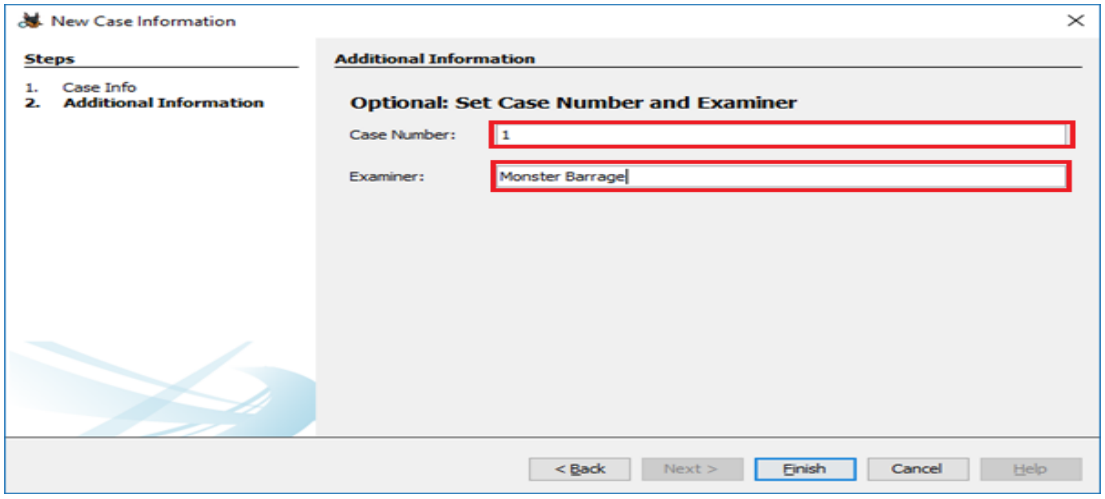
Step-1: Start Autopsy Tool

Step-2: Click Create New Case

Step-3: Enter The Details

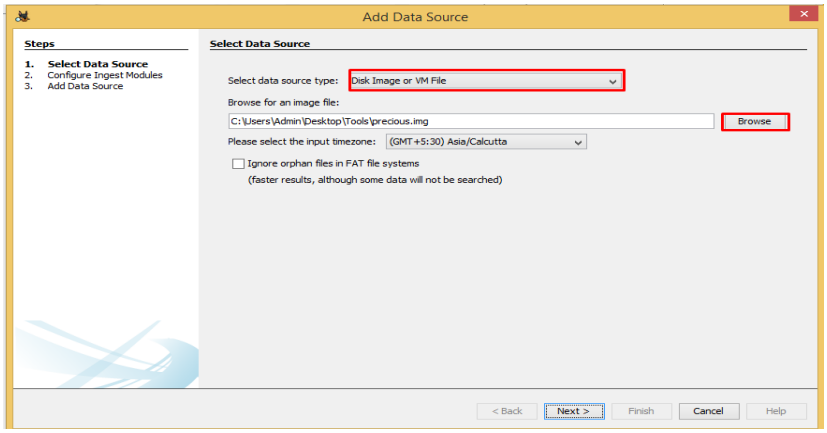


Step-4: Enter The Case Name & Case Examiner Name

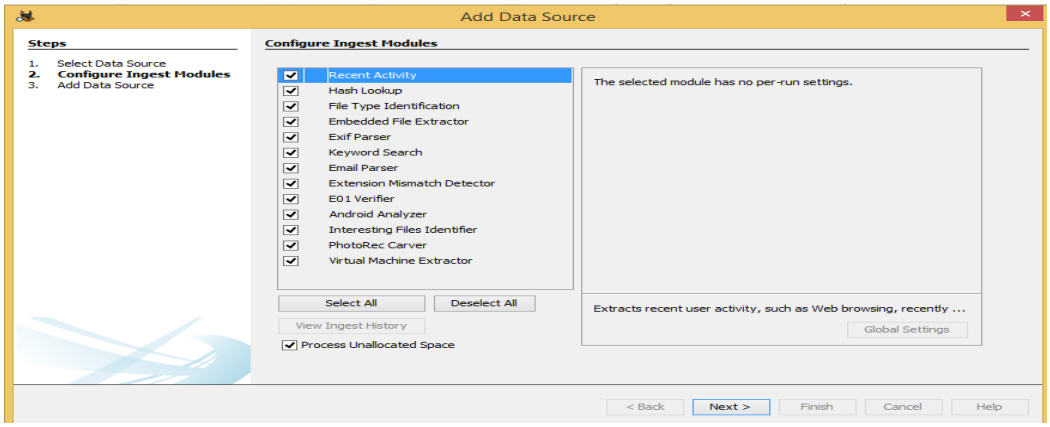


Step-5: After Clicking The Finish Button In The Above Window,

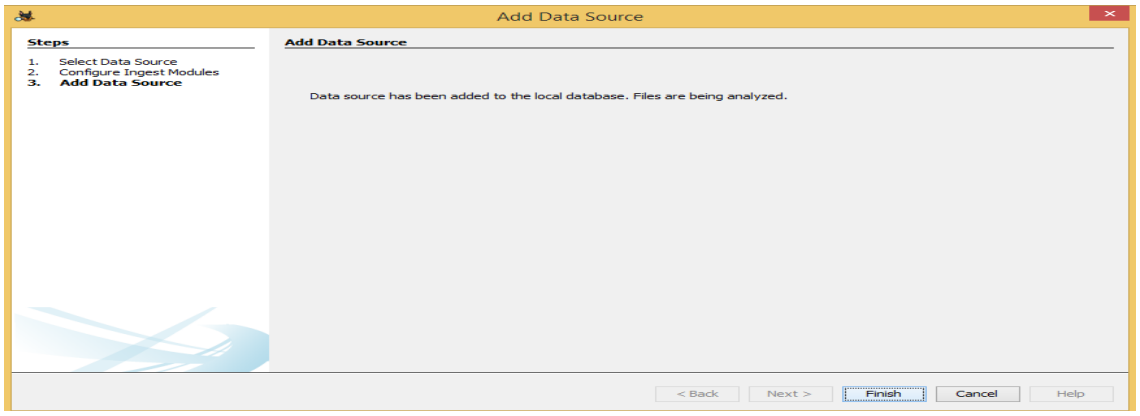
A New Window Will Open For Retrieving The Datasource,
Select Disk Image or VM File
Then Browse The .img File Present In The Directory
Click Next



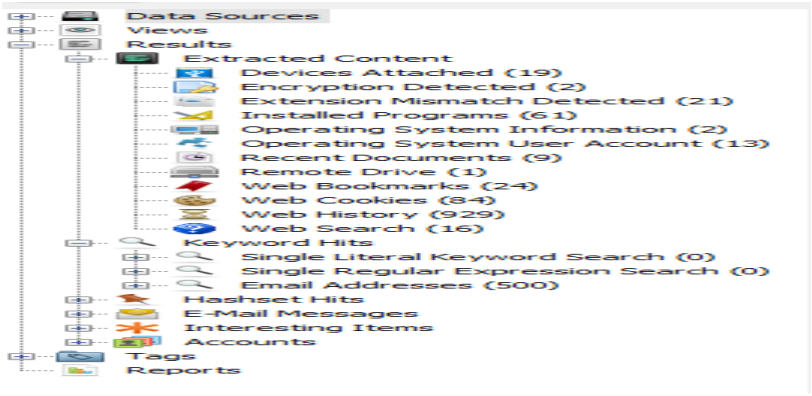
Step-6: The Next Step Provides A Ingest Wizard Panel Which Aims At Increasing The Search Capability. Select As Desired And Proceed To The Next Step.



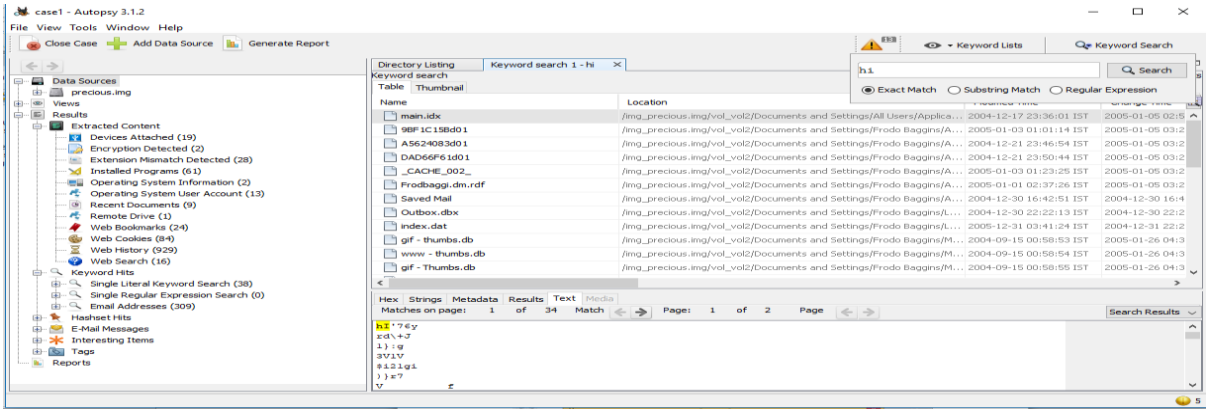
Step-7: In The Resulting Window, You'll Be Notified That The Files Are Being Analyzed. Proceed To Finish.



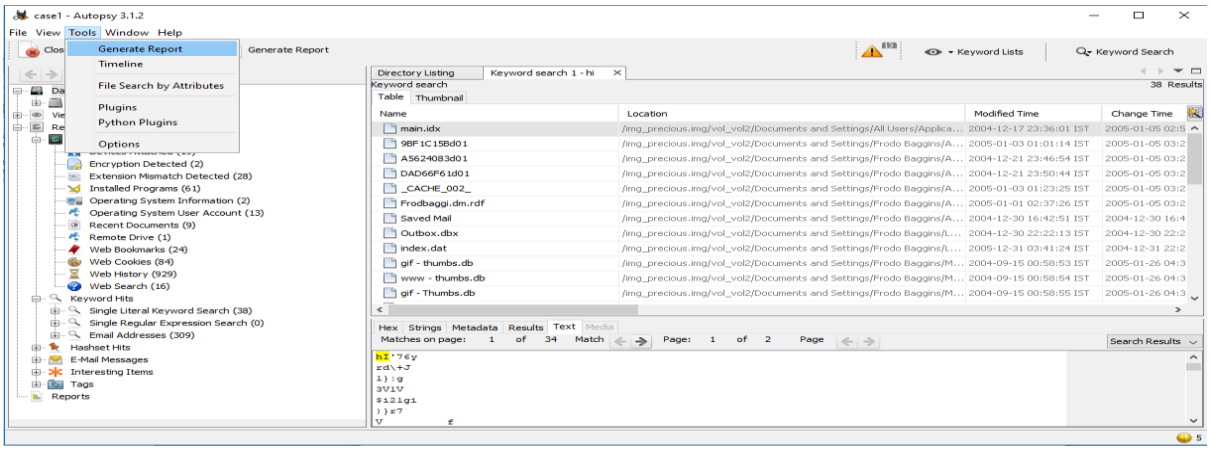
Step-8: After The Image Is Indexed The Tree Will Be Populated By The File System, Extracted Content, Keyword Searches, And The Hash List (If Any Were Used). This Tree Can Be To Retrieve The Information About The Image File Under Observation.

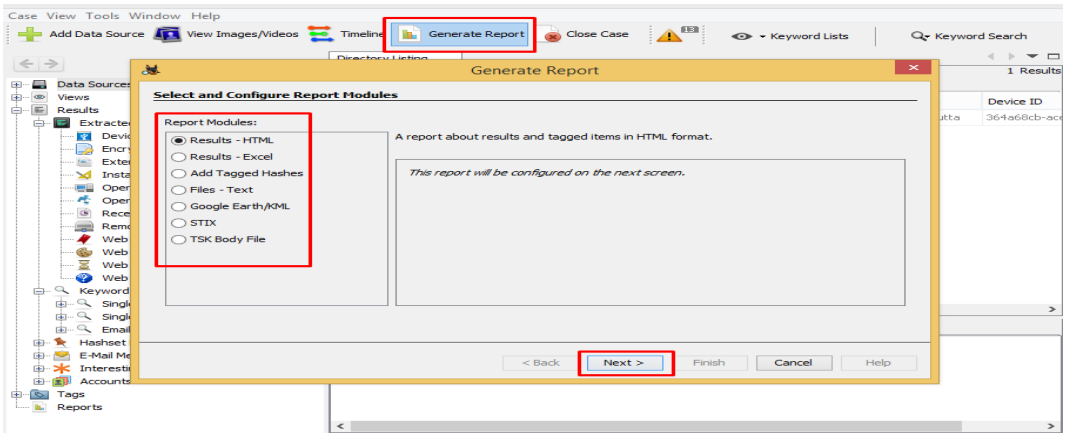


The Investigator can also Search by keyword



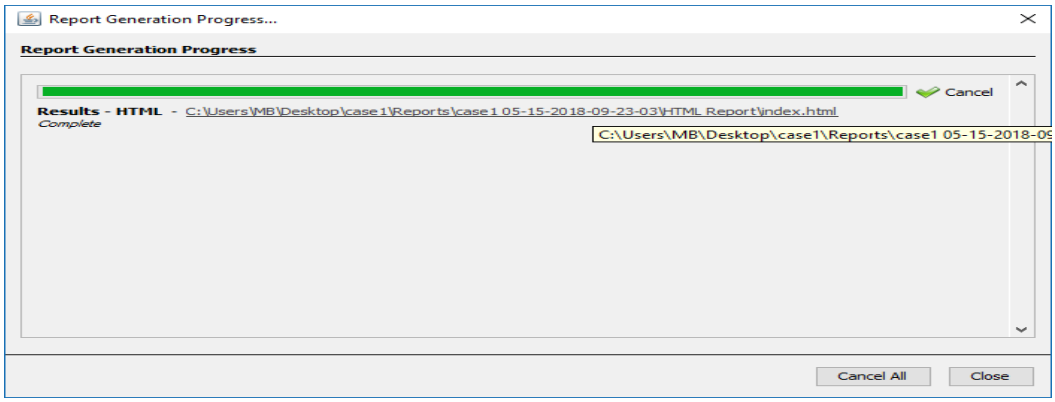
Should Generate A Report. This Will Allow The Investigator To Have An Idea Of What Type Of Information Is Available And What To Expect.



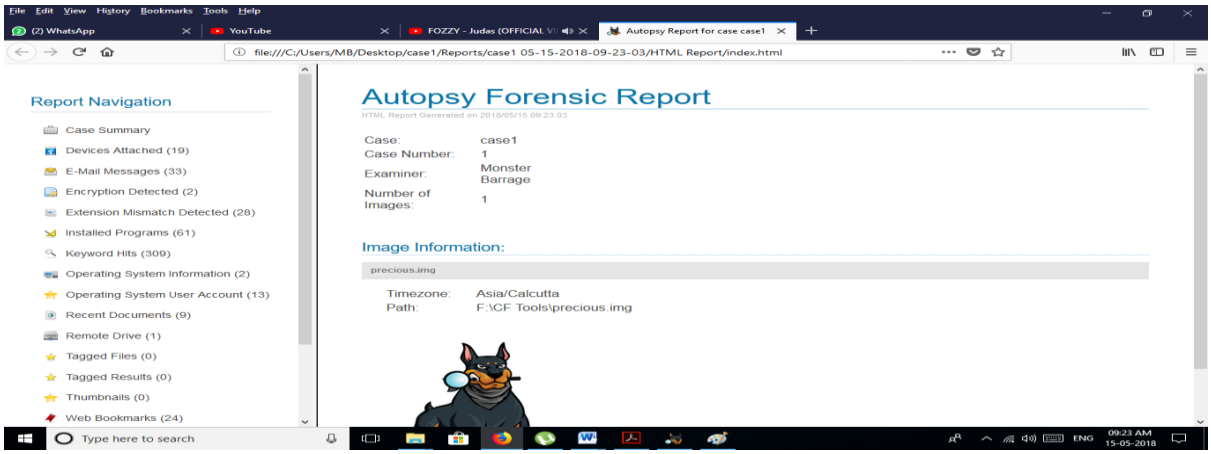


Click Next And Then Finish

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



Click On the Link

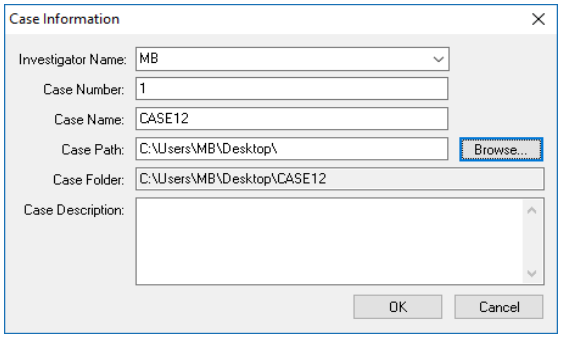


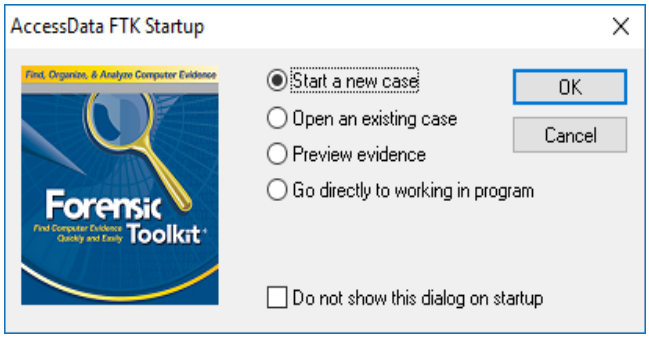
Practical 2

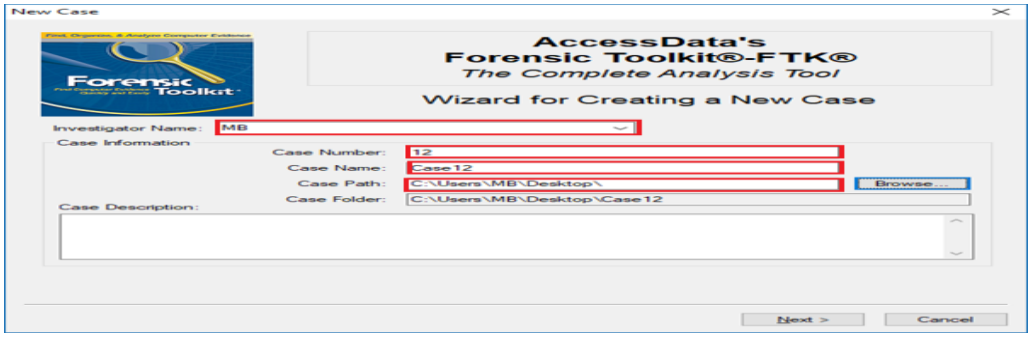
Aim: Using Forensic Toolkit (FTK) **&** Writing report using FTK **(AccessData FTK)**

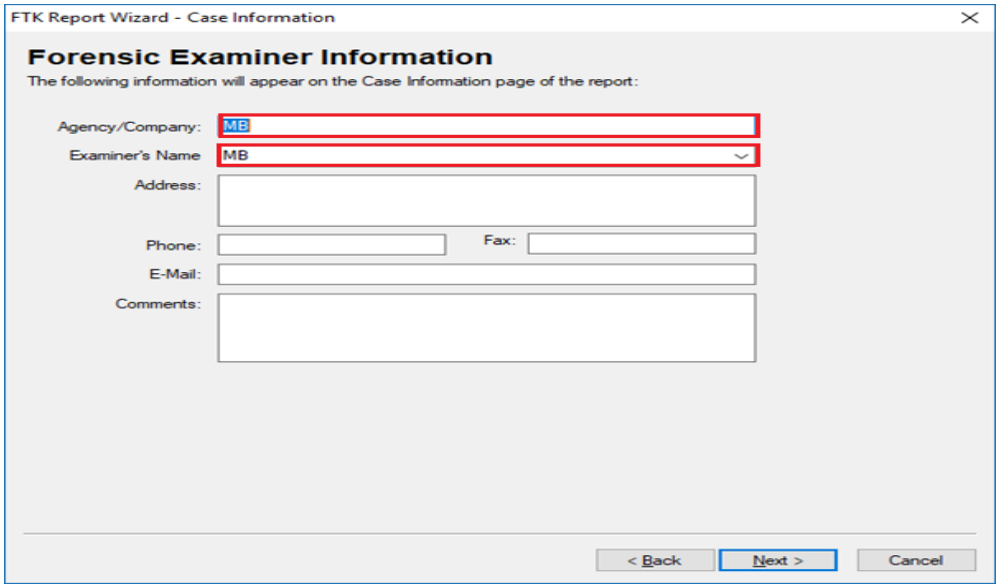
Step-1: Open Forensic Toolkit

Step-2: We can

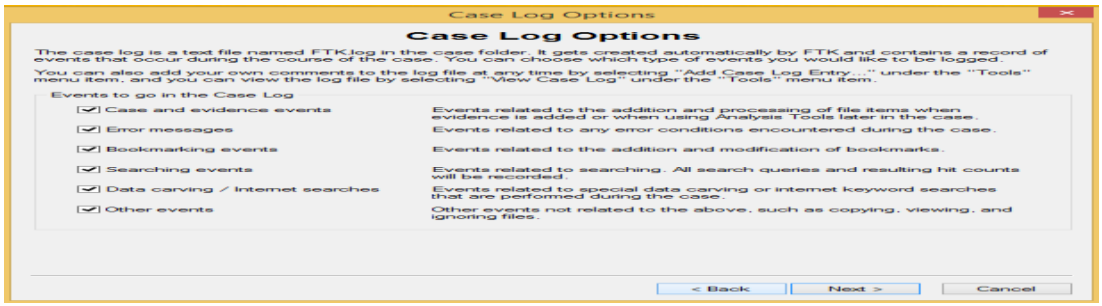


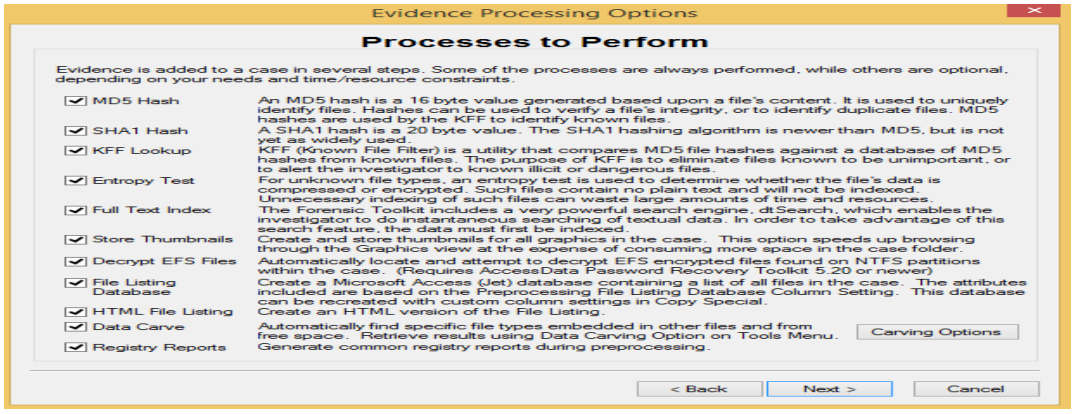


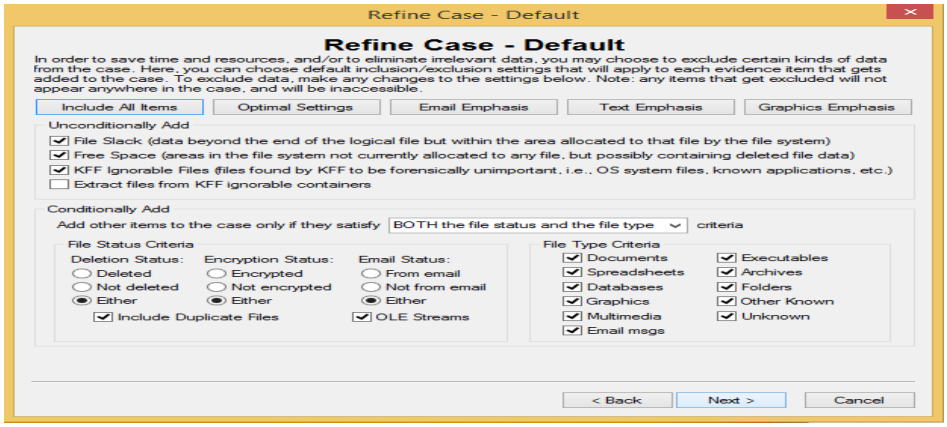


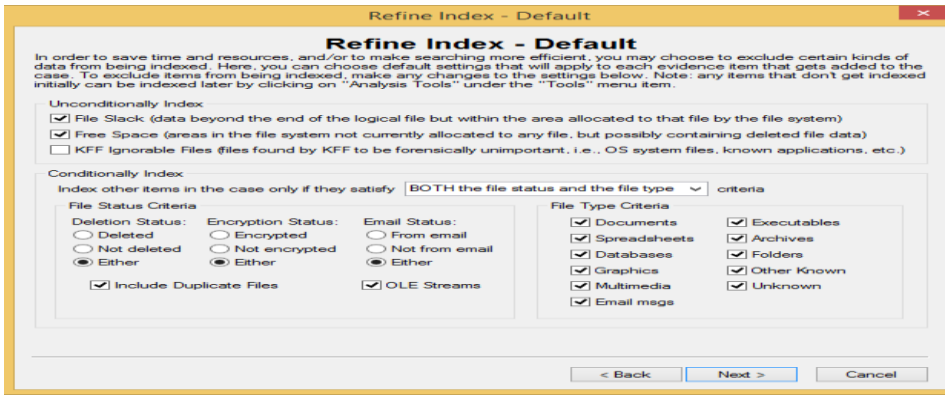


Step-4: Select Relevant Options And Proceed.



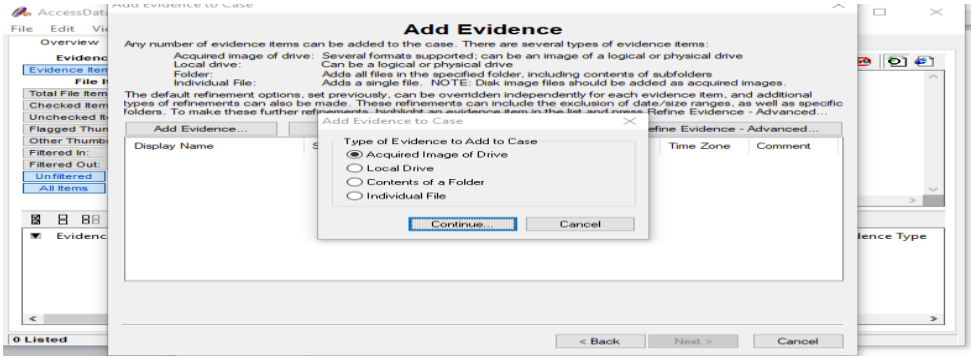




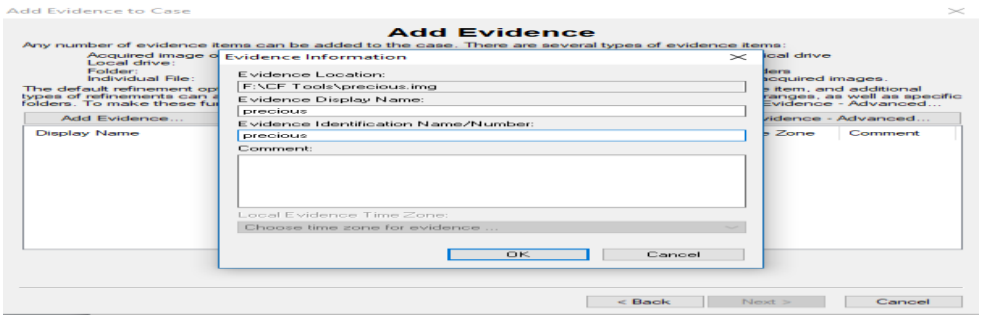


Step-5: Adding Evidence.

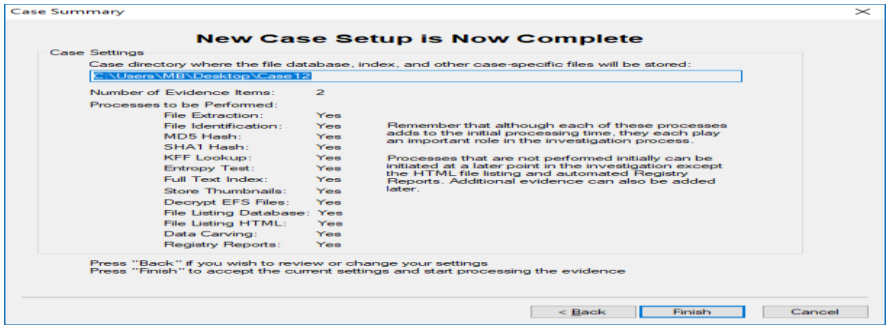
We Can Add Evidence Now Or Later Via The File Menu. The Evidence Can Be In The Form Of Accquired Image Of Drive Local Drive Contents Of A Folder Individual File According To The Option Selected We Will Be Presented With The Relevant Popup Screen. For Now We Will Be Going With The Contents Of A Folder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



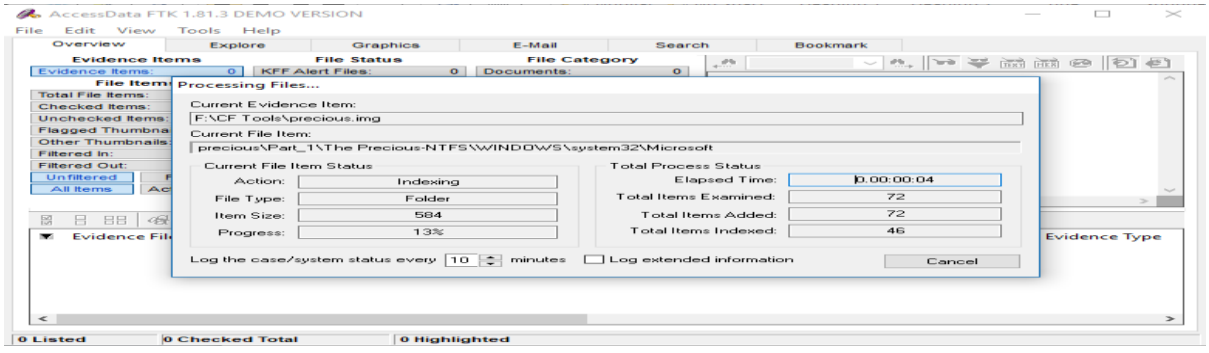
Select The Image File



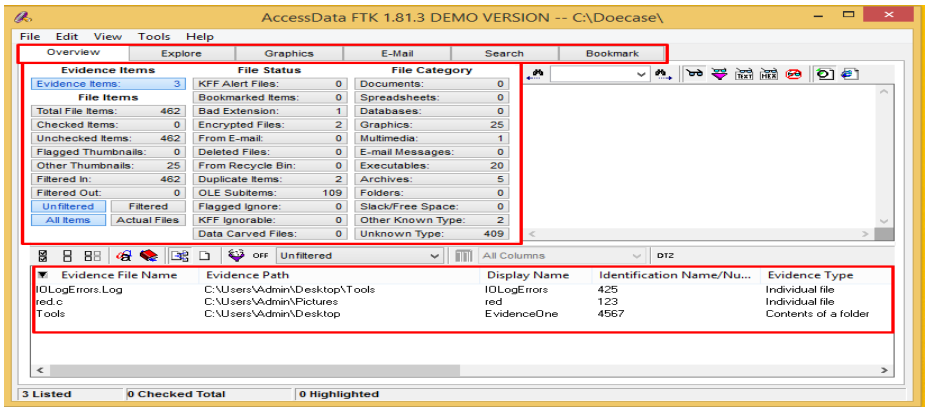
Click OK And Then Next To Proceed .



Hit finish and Done

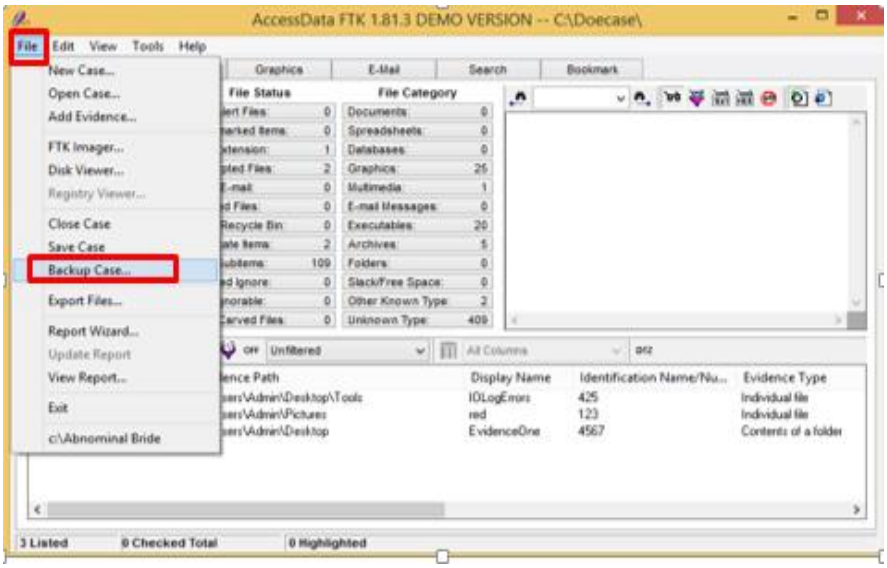


Step-6: We'll Be Presented With Findings From The Evidences Added Into The Case We Can Search, Refine, Examine The Data In The Evidence With The Help Of The Options Provided In The Access Toolkit.

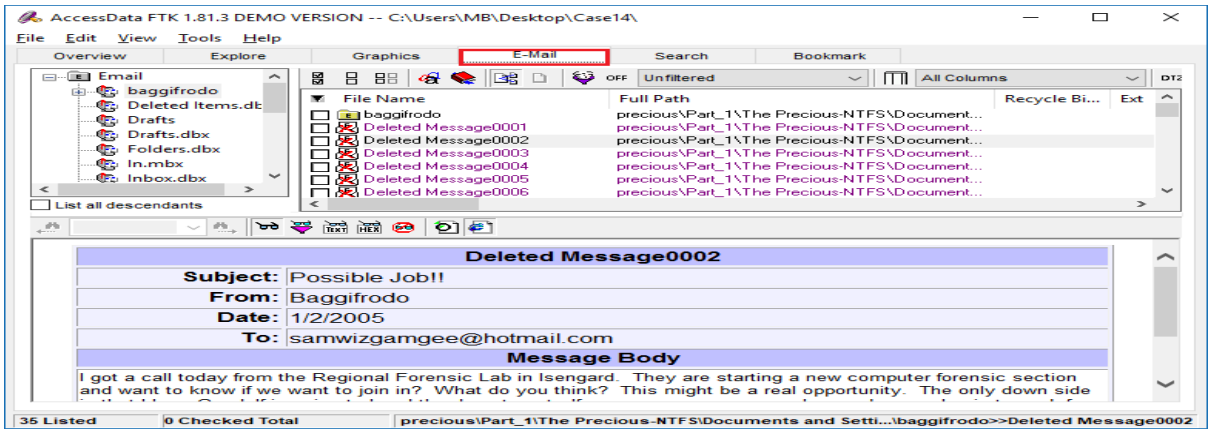


Step-7: We Can Create The Backup Of The Case By Selecting The Backup Case Option In The

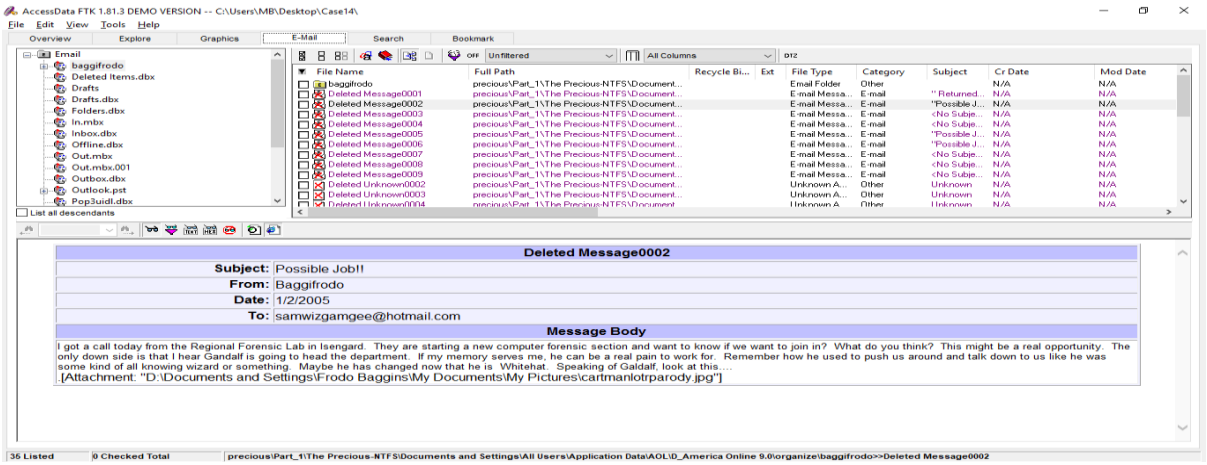
File Menu And Then Providing The Location For Keeping The Backup File.



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



Select an email and investigate it

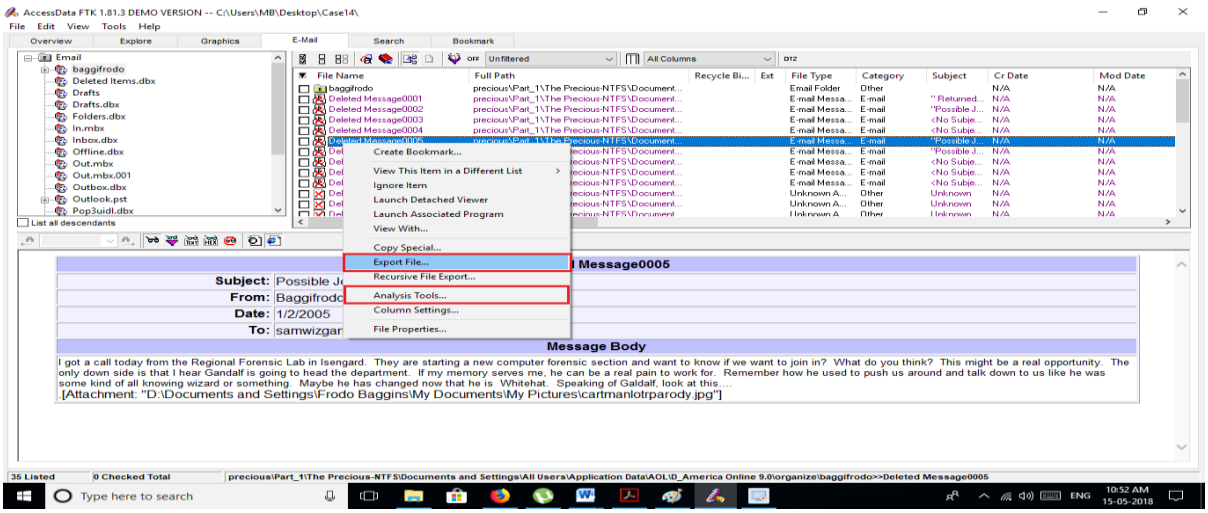


Step-9: Additional Steps Can Be Performed Like,

Exporting The File

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

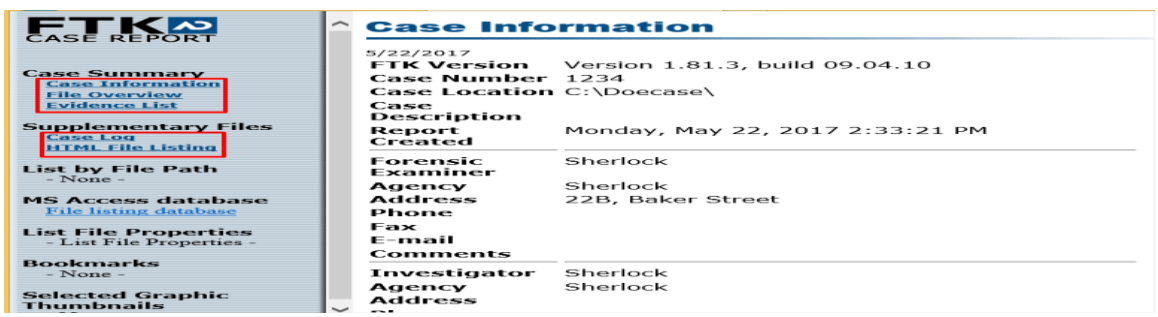
To Do So, Right Click The Desired Email And Select The Required Option.



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

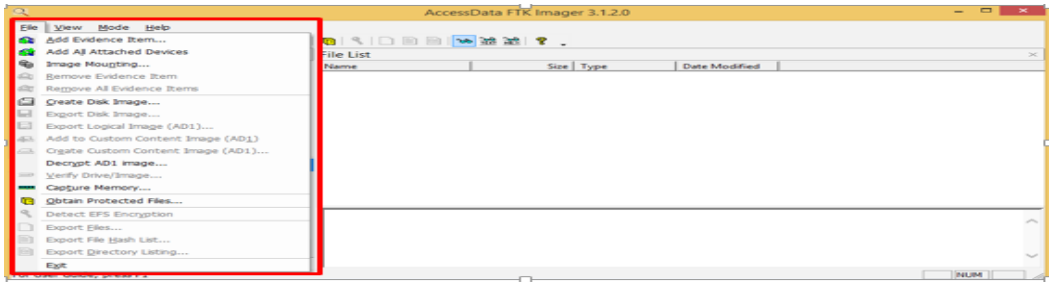
Aim : **Using File Recovery Tools [FTK Imager] Creating Image**

Step-1: Open Access FTK Imager

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

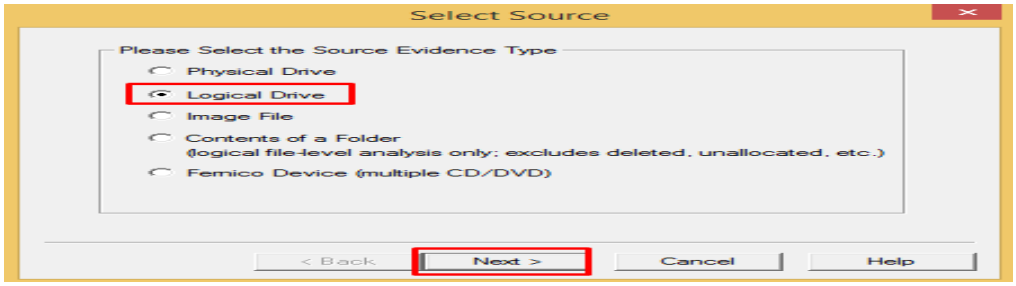
We Will Proceed With Creating A Disk Image Of A Logical Drive.

Select Create Disk Image.

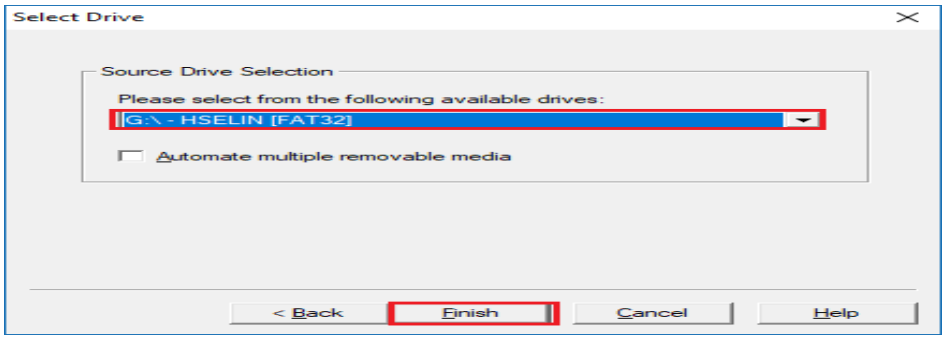


Step-3: In The Resulting Popup,

Select Logical Drive And Click Next.



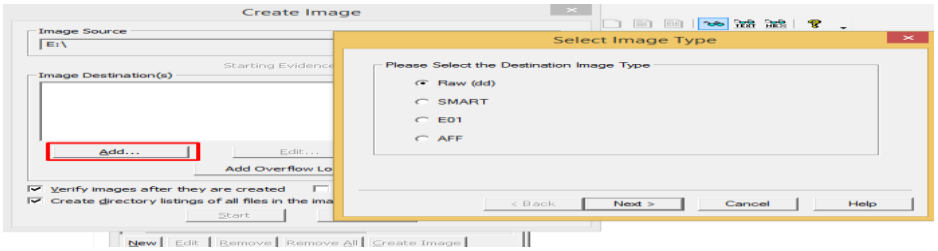
Select A Drive And Click Finish.



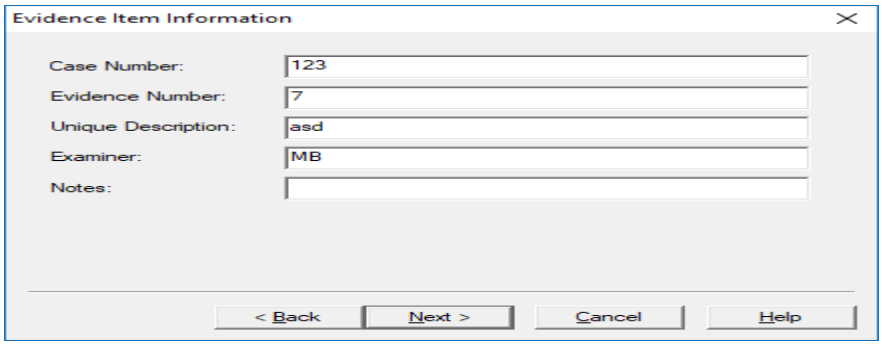
Step-4: Creating Image – Configuring Options

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

We Will Go With Raw Type Here.

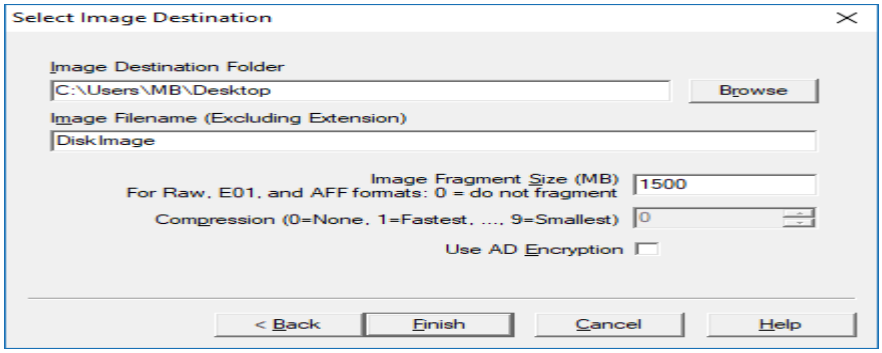


Proceed With Filling The Required Information In The Resulting Popup.

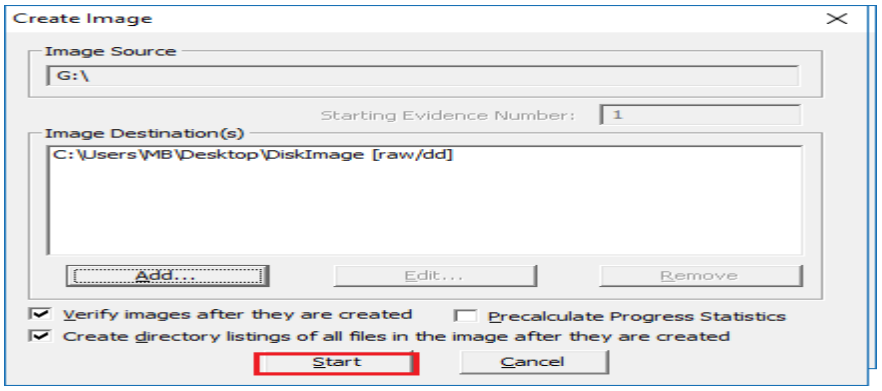


Provide The Location For The Disk Image File To Be Stored.

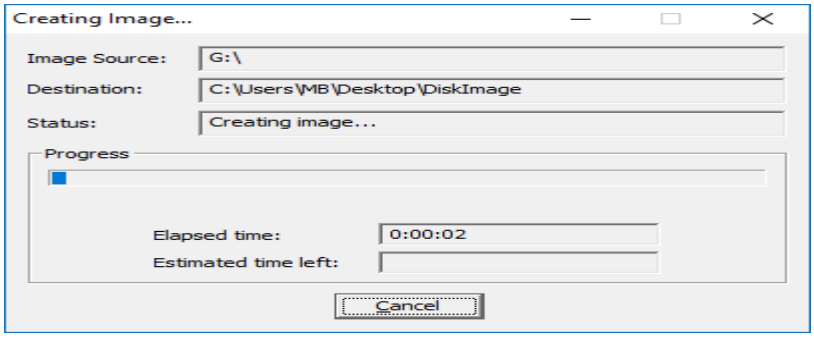
Click Finish.



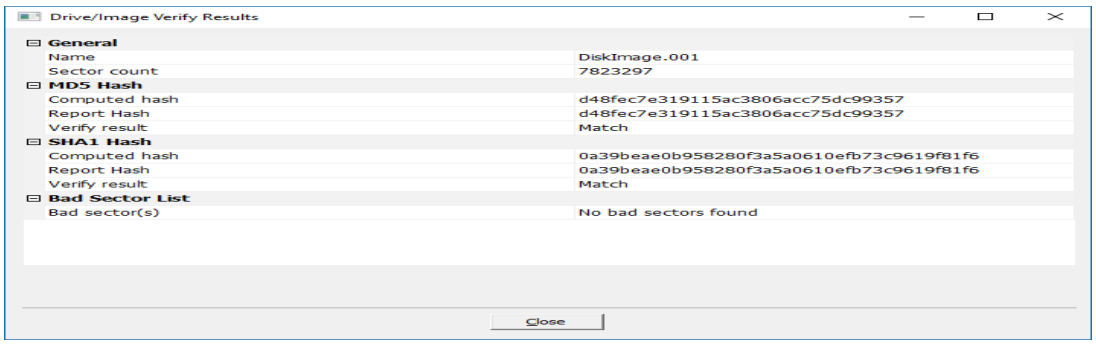
Click Start To Proceed With The Creating Of The Image.



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



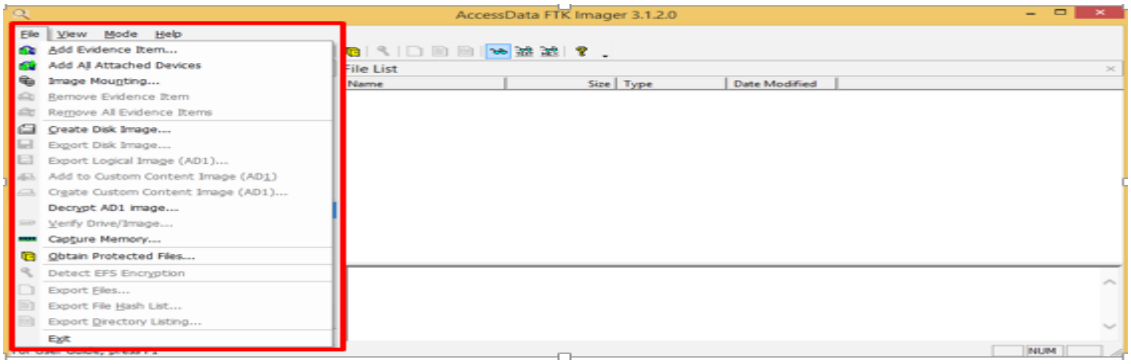
Step-5: After The Processing, A Dialog Box Will Show The Results.



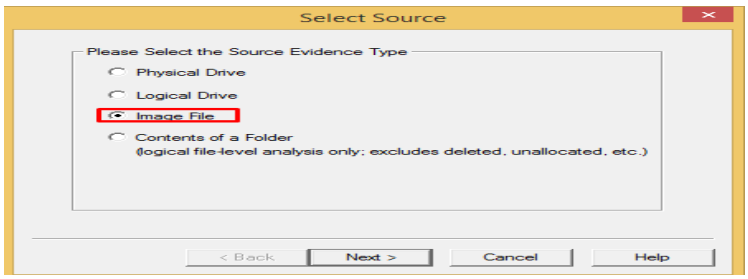
Using File Recovery Tools [FTK Imager] Using Evidence

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.

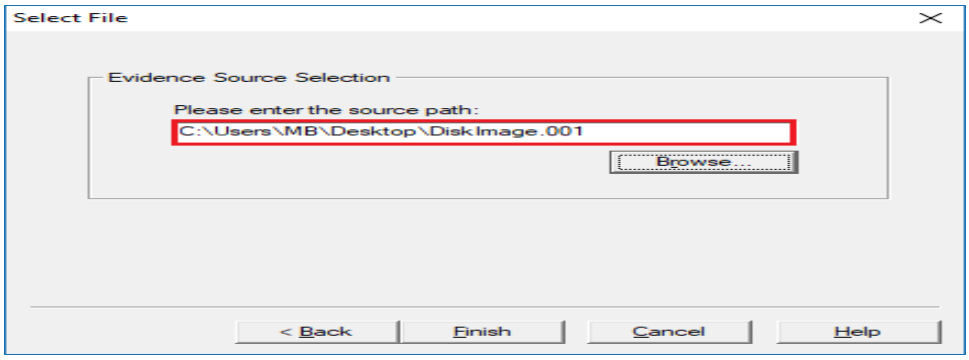


Step-3: In The Resulting Popup Select The Image File Option And Click Next

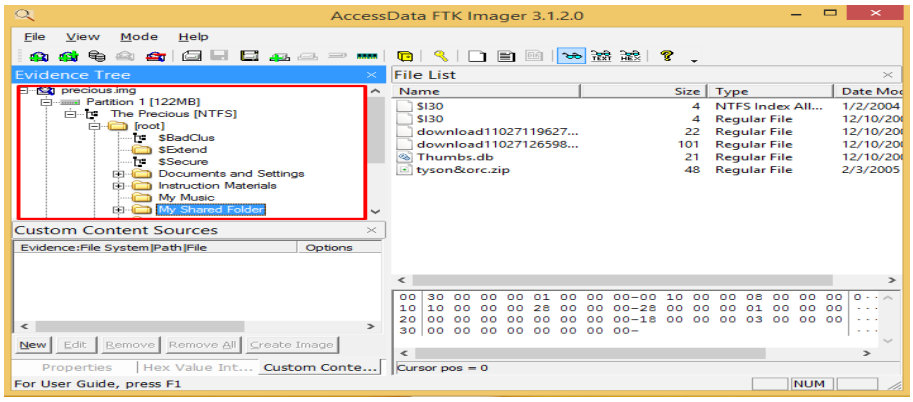


Step-4: Provide The Location Of The Image File To Be Used

Click Finish.



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

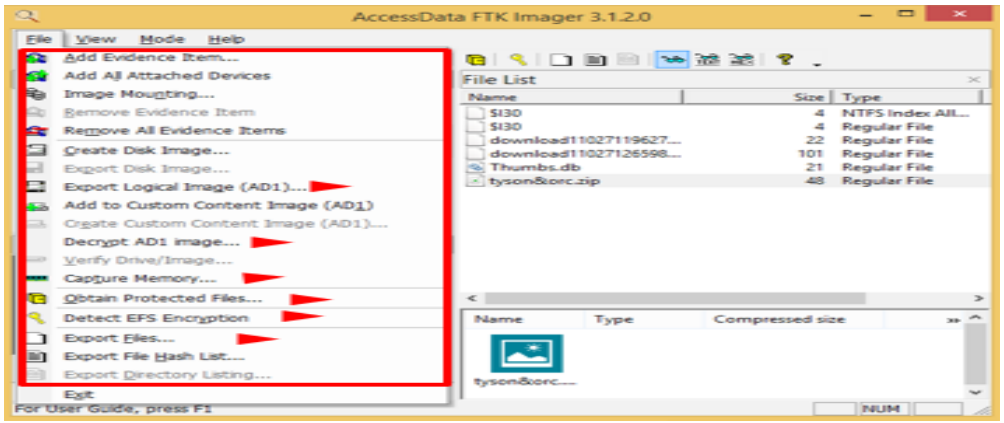


Step-6: In The File Menu, There Are Various Options That Can Be Used

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.

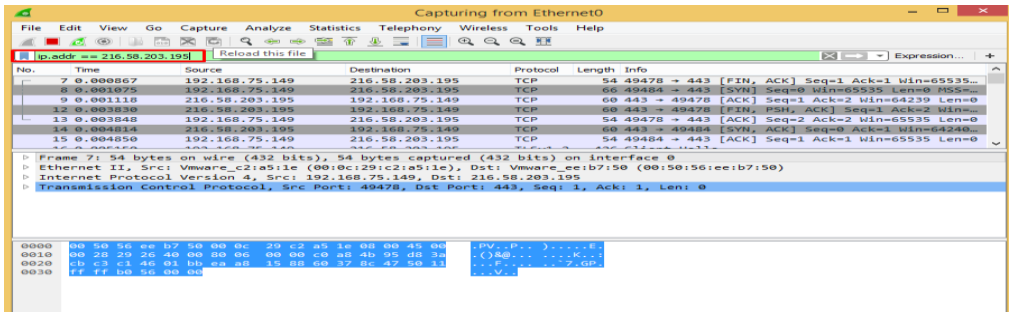
Practical 4

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

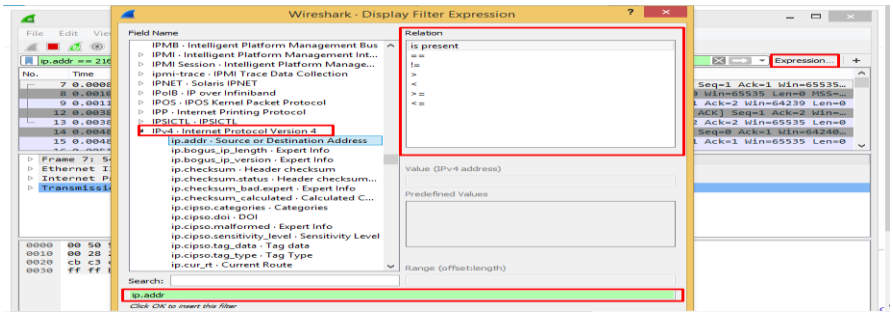
Step-1: Open Wireshark

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.

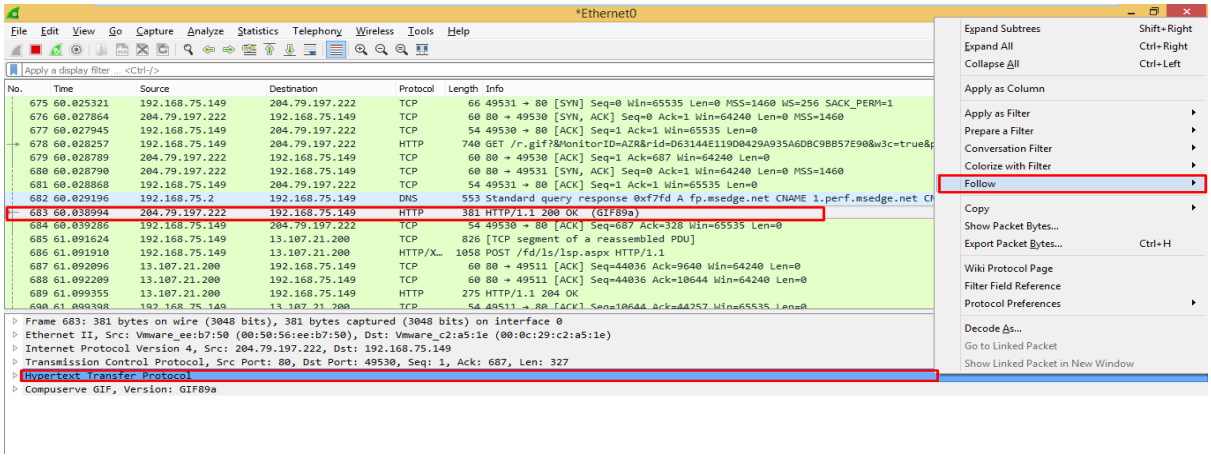


Step-3: Analyzing A Packet.

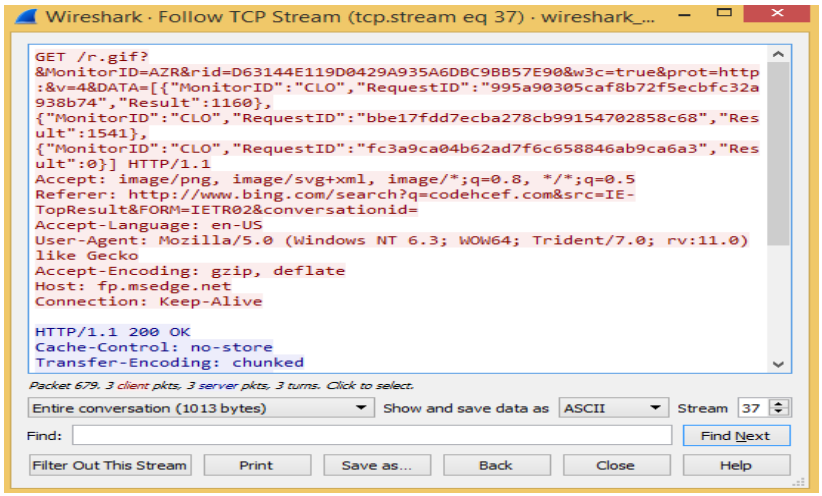
Select A Packet.

Right Click On The Packet Data Available Below

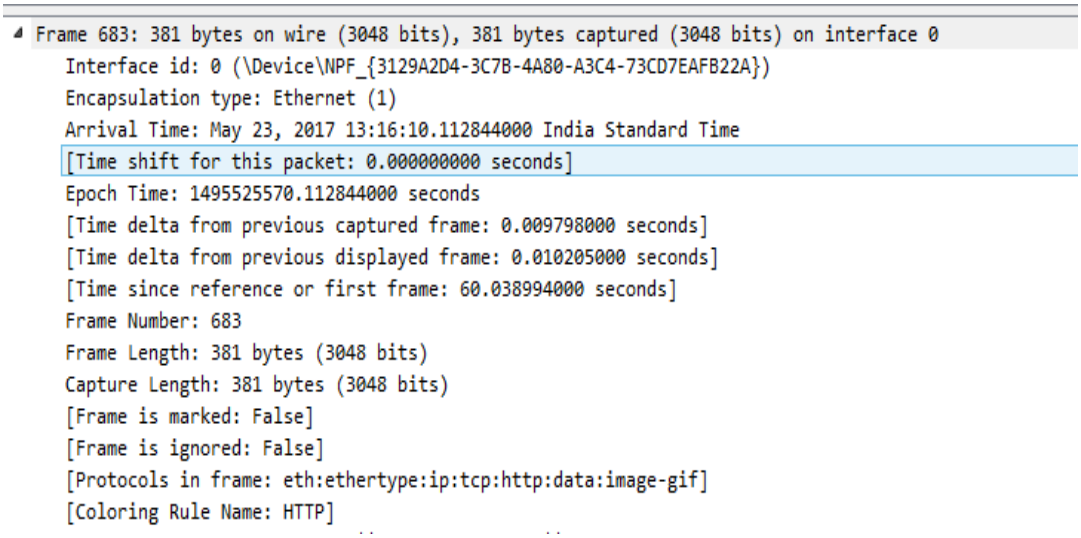
Click Follow -> TCP



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.



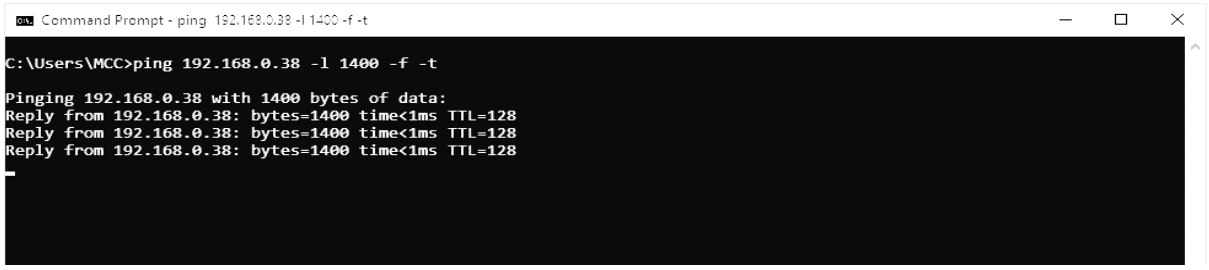
Step-5: Depending On The Analysis More Filters Can Be Added And Inspected.

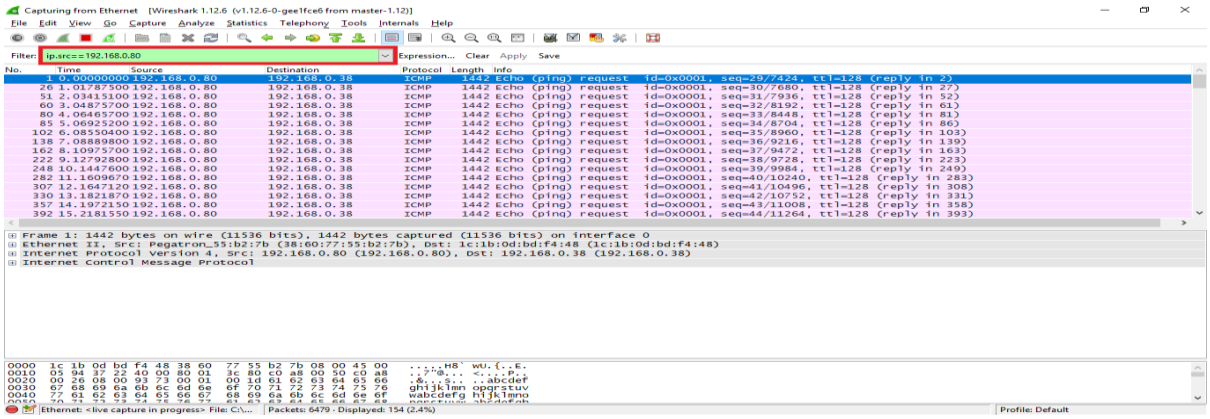
Practical 5

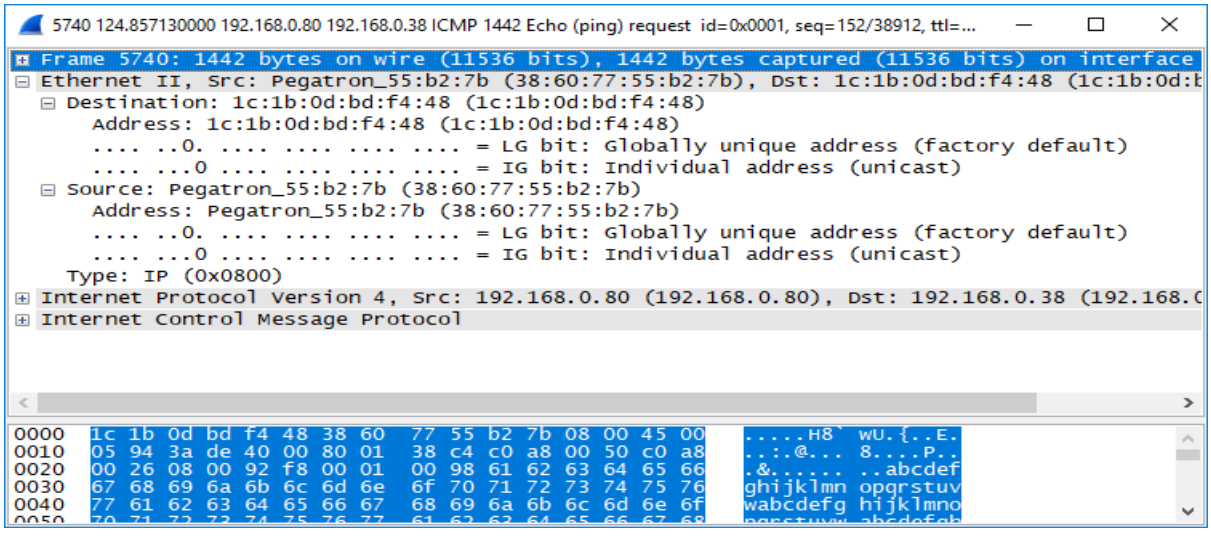
Aim: Using Web attack detection tools [Wireshark]

Step-1: Open Wireshark

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





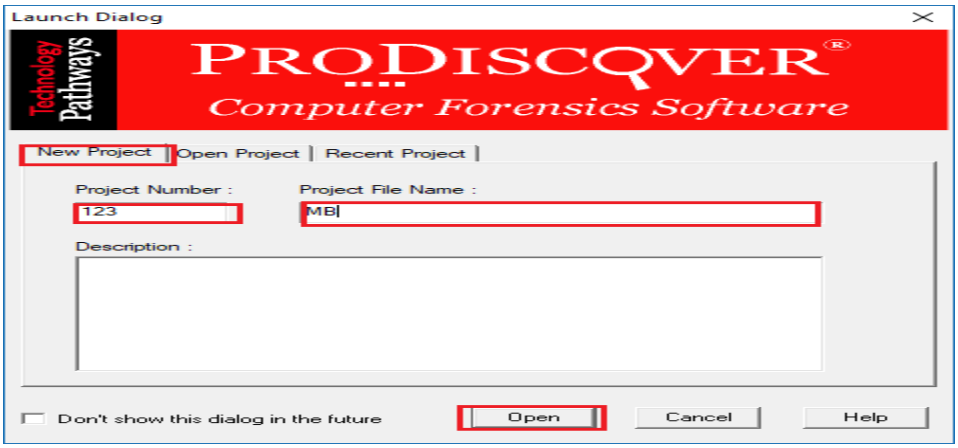


Practical 6

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.

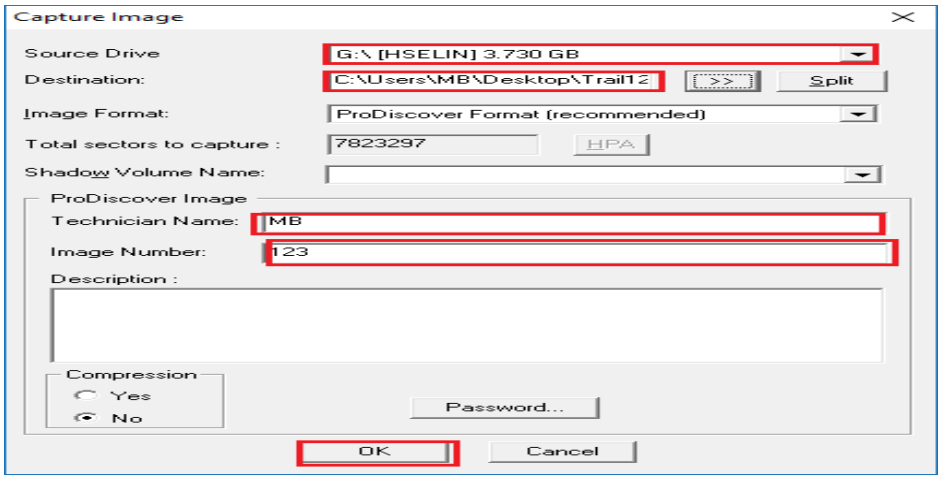


Step-3: To Create An Image For Investigation Purpose,

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.

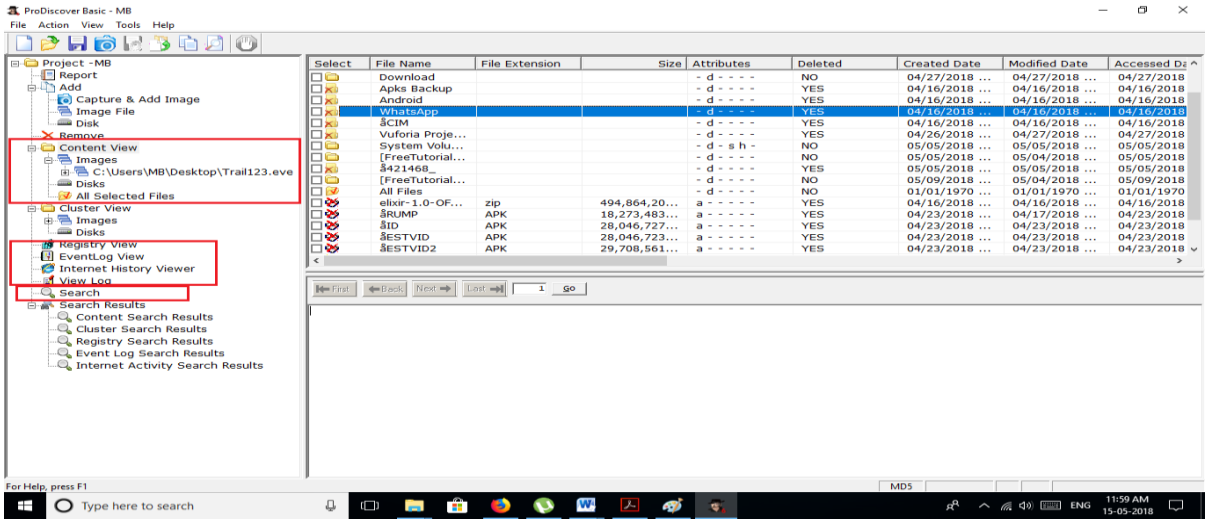


The Tool Will Now Start The Process Of Making An Image From The Given Drive.

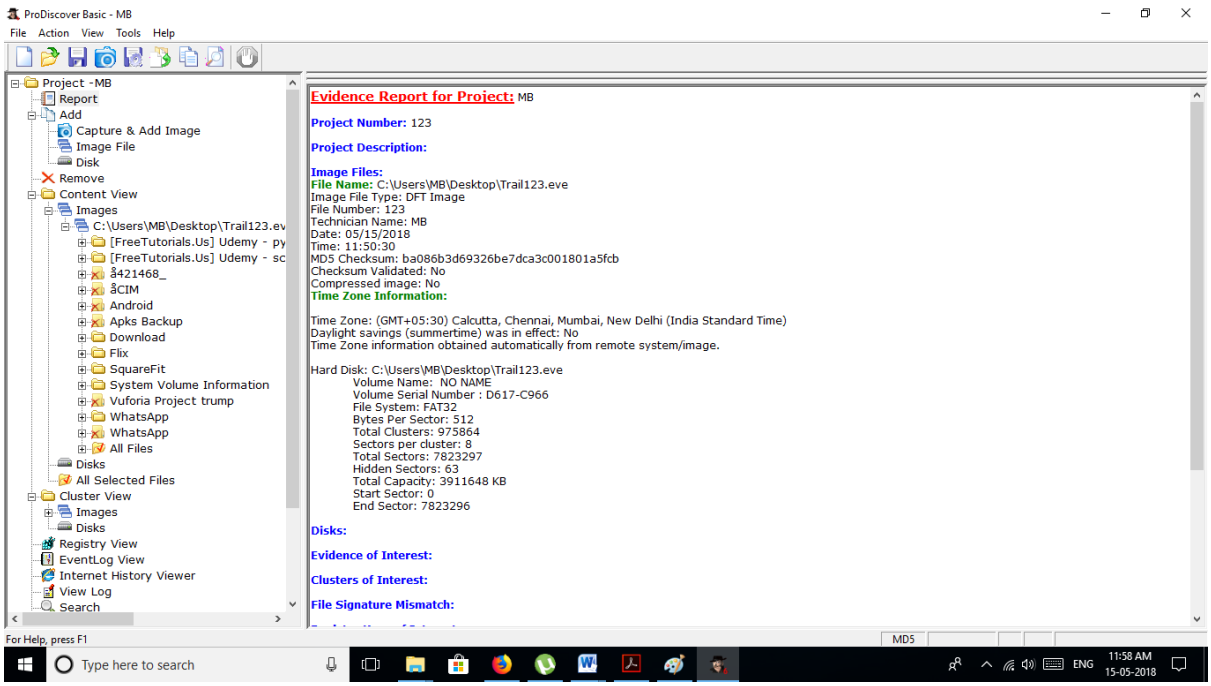
Step-4: Now The Image Will Be Processed And The Contents Will be Presented In The Left

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



Practical 7

Aim: Using Steganography Tools [S-Tools]

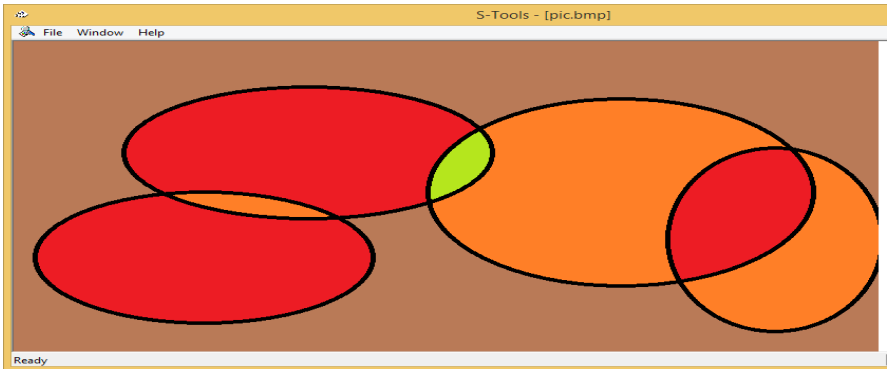
Step-1: Open S-Tools

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

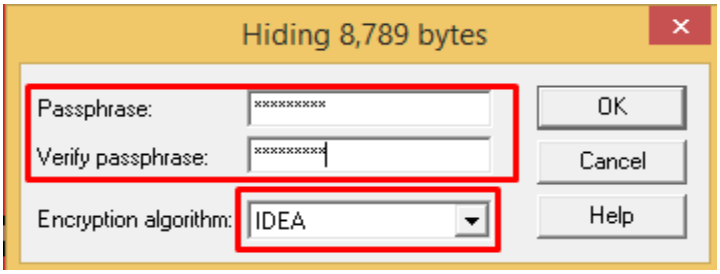
Step-3: Drag & Drop The Two Files (Image & Text)

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.

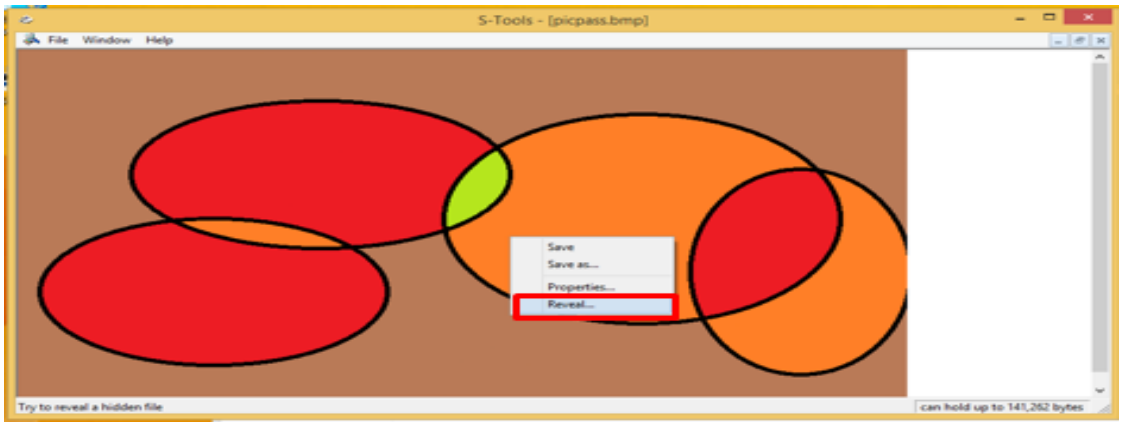


Step-5: Save The Image Into The Desired Location Of Your System.

Step-6: To Obtain The Hidden Text. Open The Saved Image File,

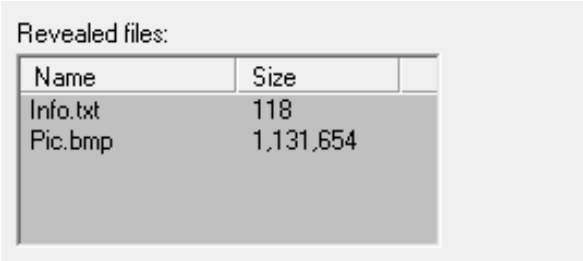
Right Click On the Image File

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.



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

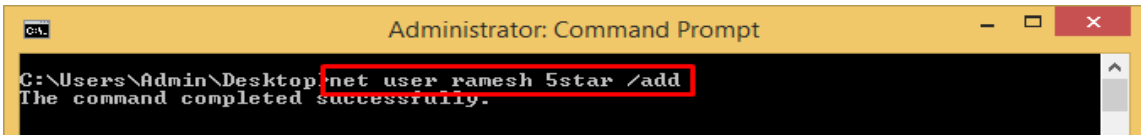
Open Command Line As Administrator

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

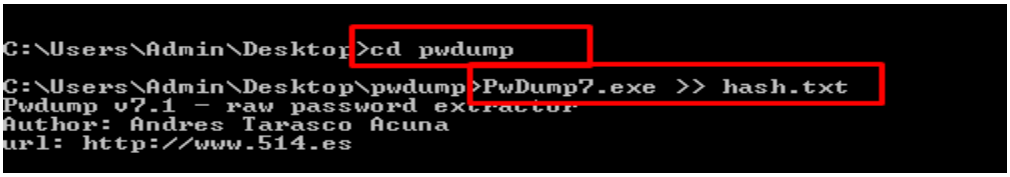
Step-3: Now Navigate To The pwdump Folder Present In Your System.

Type Command,

Pwdump7.exe >> hash.txt

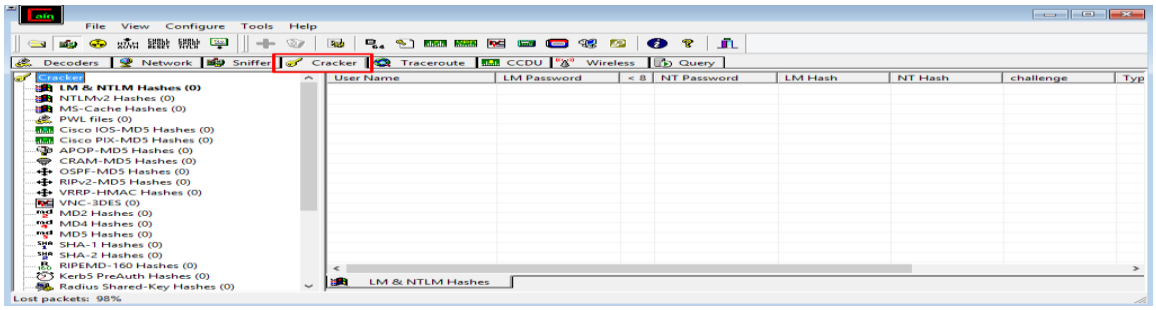
Pwdump7(We have installed The pwdump 7th release)

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



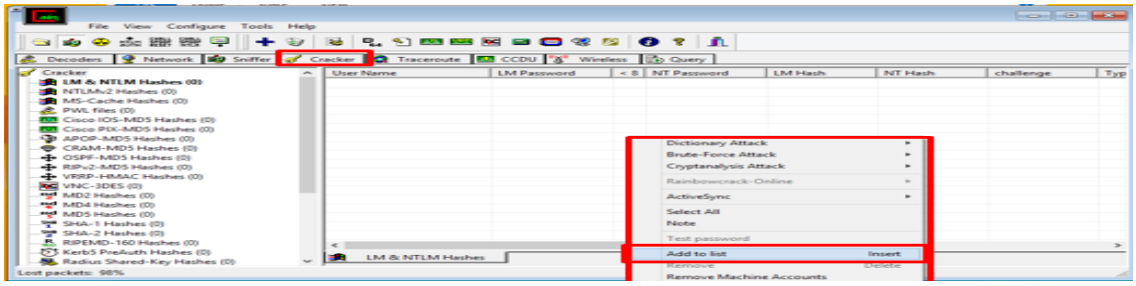
Step-4: Start Cain & Abel As Administrator

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.

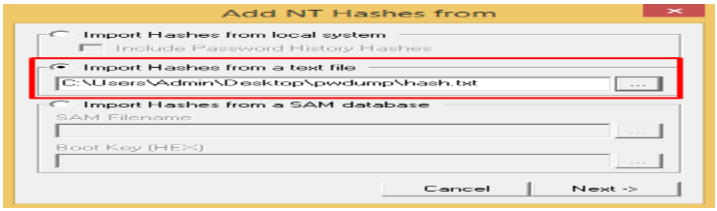


Step-7: In The Resulting Popup,

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.

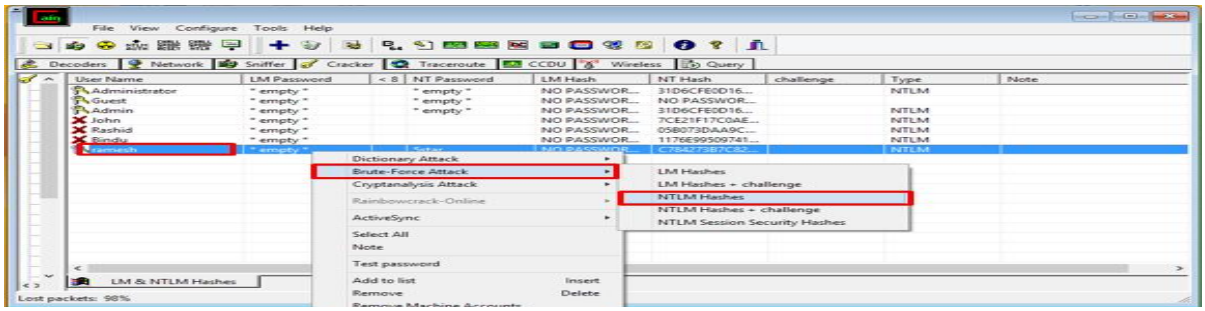
User Name	LM Password	< 8	NT Password	LM Hash	NT Hash	challenge	Type	Note
Administrator	* empty *		* empty *	NO PASSWOR...	31D6CFE0D16...		NTLM	
Guest	* empty *		* empty *	NO PASSWOR...	NO PASSWOR...			
Admin	* empty *		* empty *	NO PASSWOR...	31D6CFE0D16...		NTLM	
John	* empty *			NO PASSWOR...	7CE21F17C0AE...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

Step-9: Select An Account,

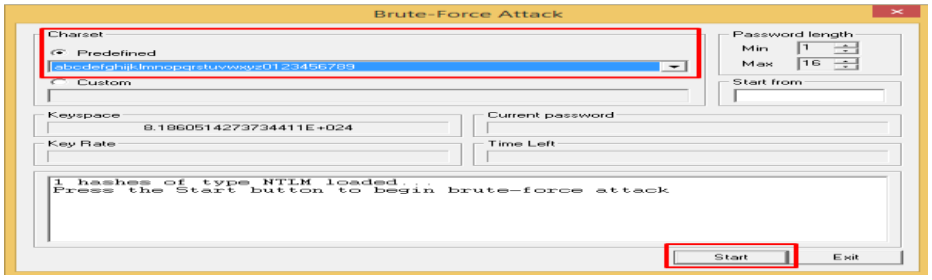
Right Click On That User Account

Select Brute-Force Attack

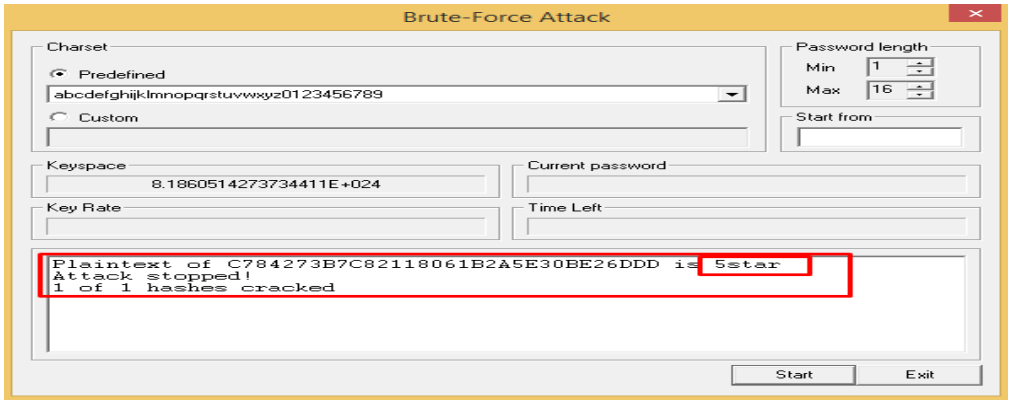
Select NTLM Hashes

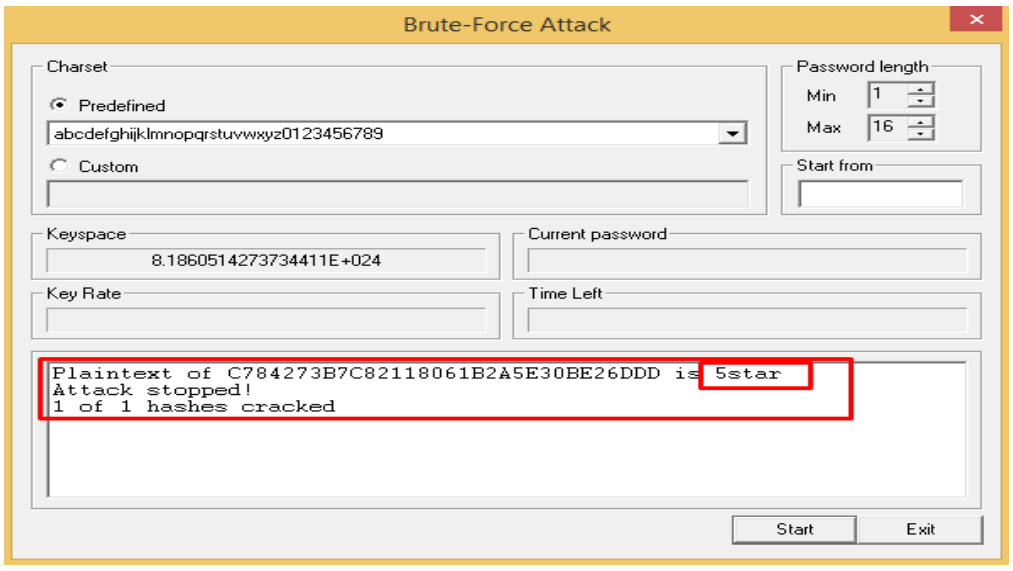


Step-10: Select Relevant Charset & Click Start



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



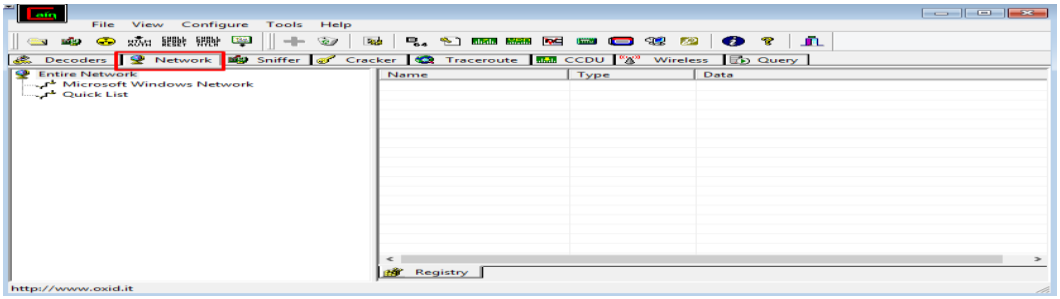


Practical 9

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

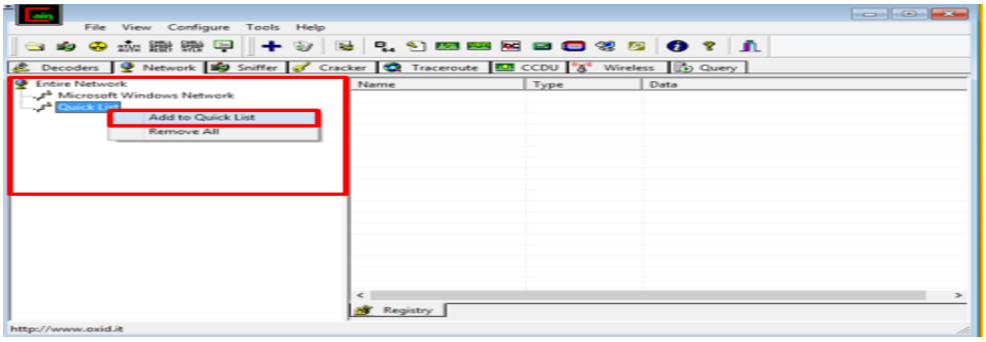
Step-1: Open Cain & Abel As Administrator

Step-2: Go To Network Tab



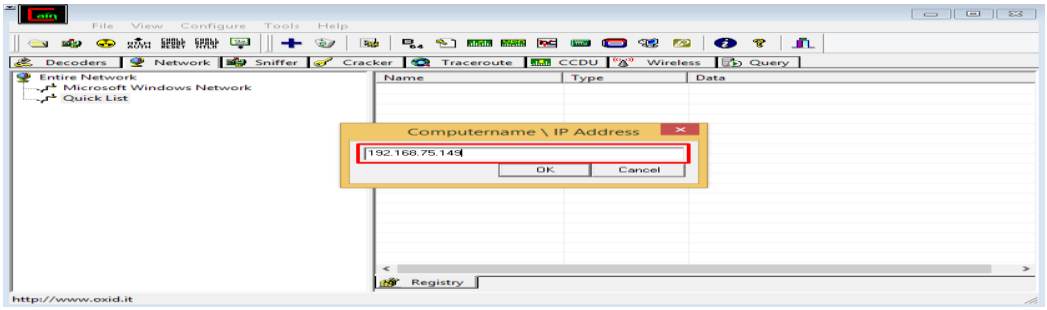
Step-3: Expand Entire Network

Right Click Quick List & Select Add To Quick List.



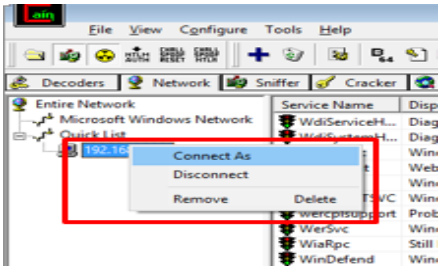
Step-4: In The Resulting Popup Box, Enter The IP Address Of The System You Want To Study

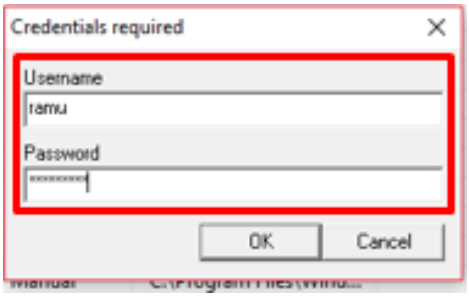
(You Can Use Your Own System's IP Address To Examine Your Registry)



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

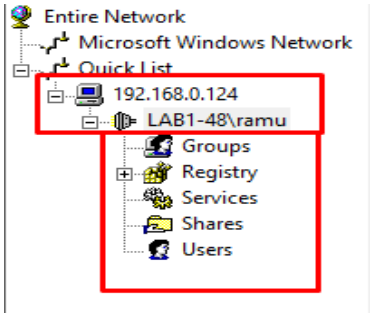
Right Click On The Account And Enter User Credentials (Necessary Only If Using Accessing Other System)





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

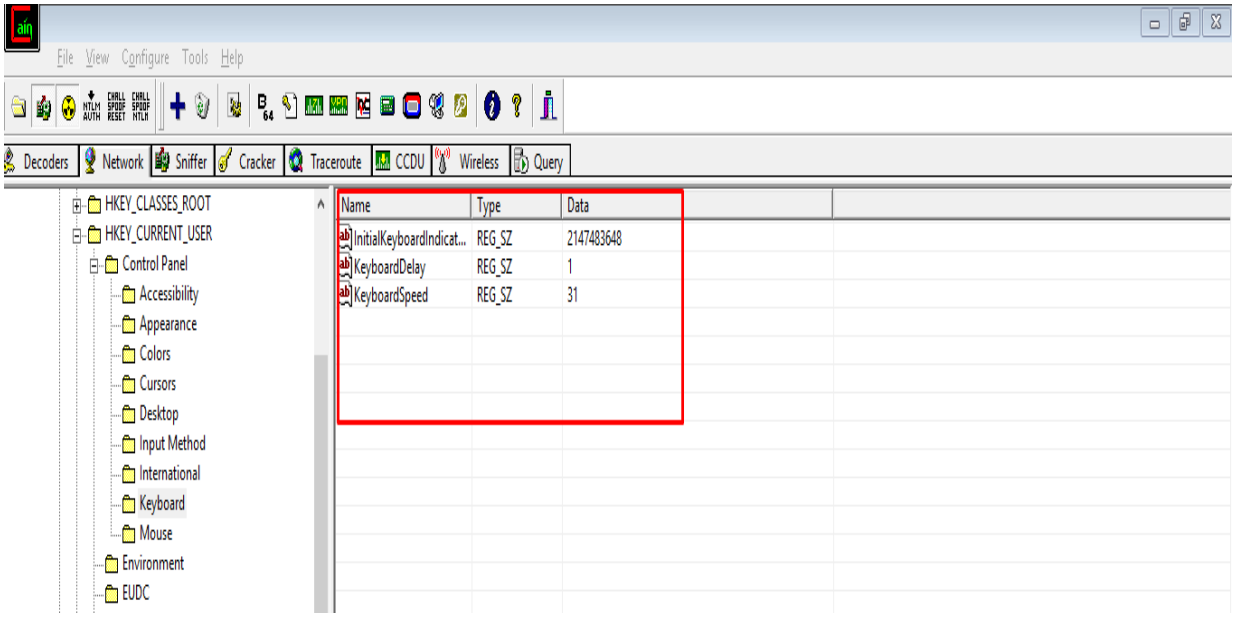
a. Groups
b. Registry
c. Services
d. Shares
e. Users



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.

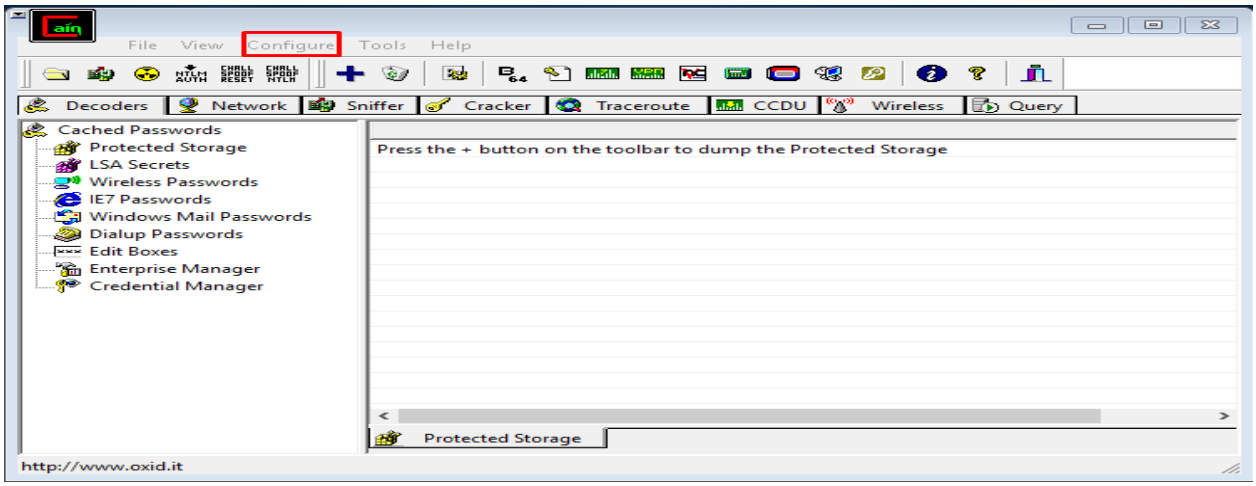
Practical 10

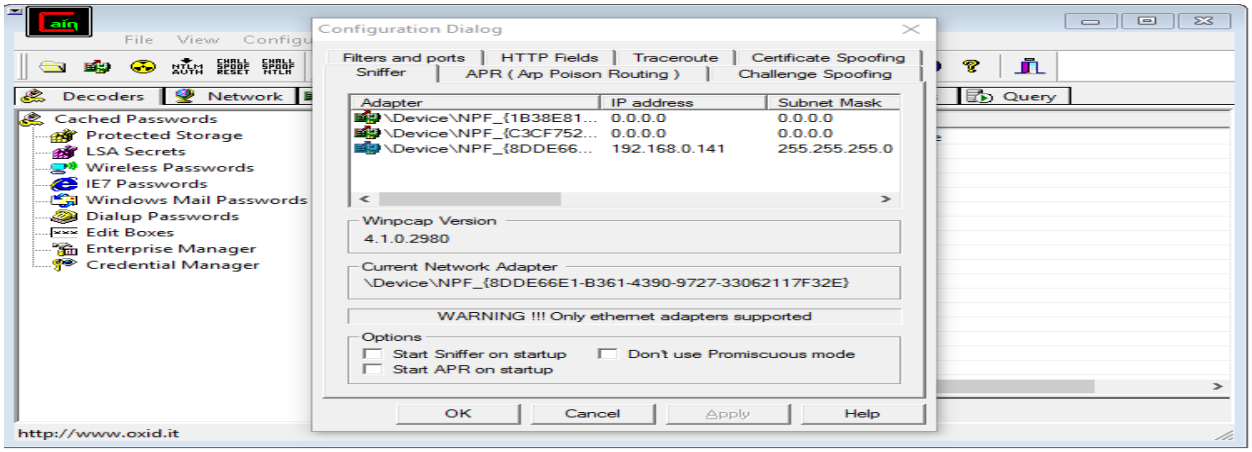
Aim: Performing Sniffing [Cain & Abel]

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

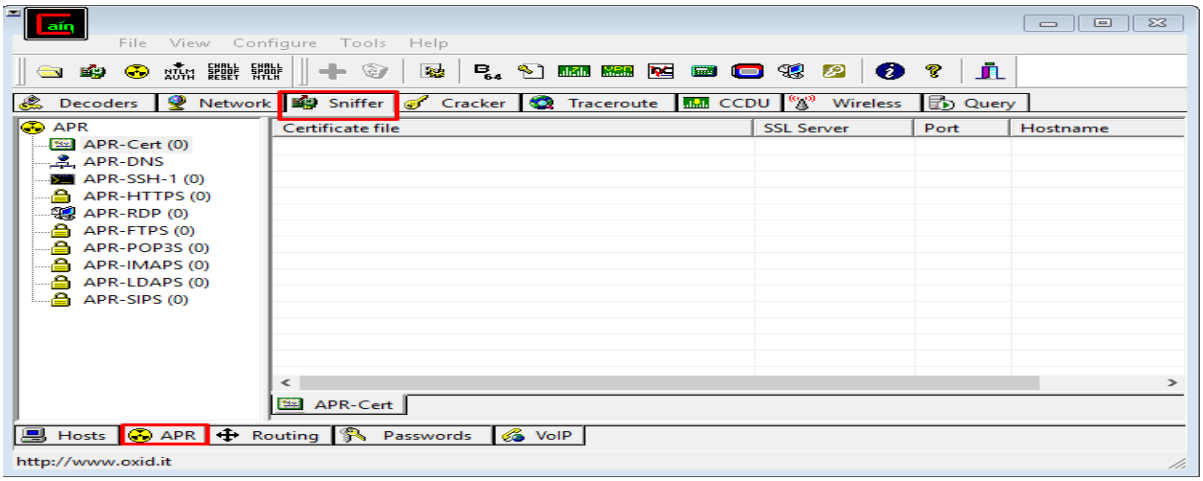
1. Open Cain & Abel By Running It As Administrator. (Note: Firewall Exception Might Occur, Press OK)

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

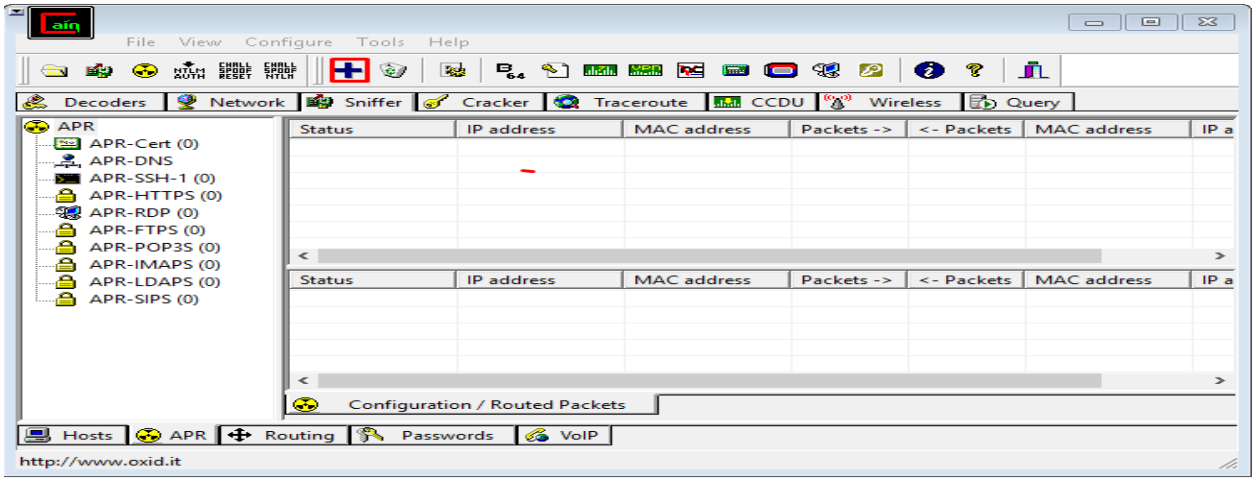




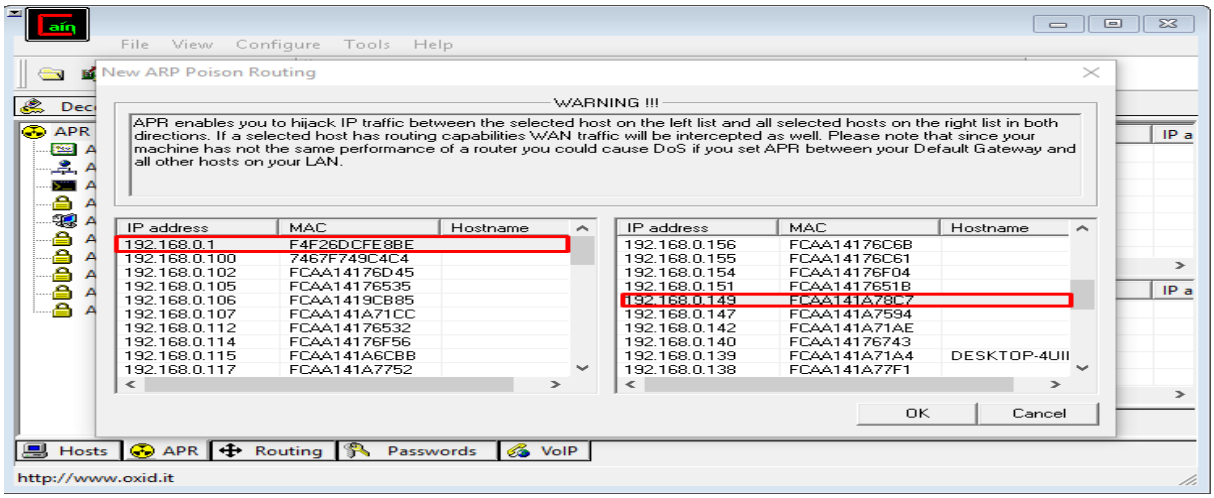
3. Now Go To Sniffer Tab On Top & Select APR Tab From Bottom.



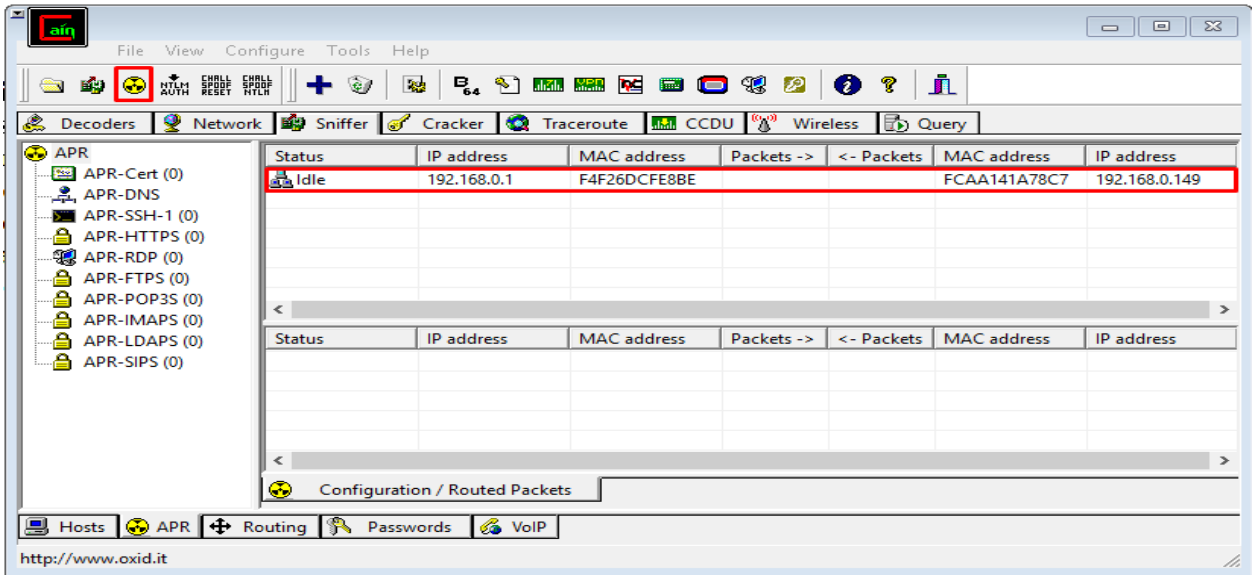
4. Single Click On The Right Above Part Of APR And Then Click On "+" Icon On Top Left.



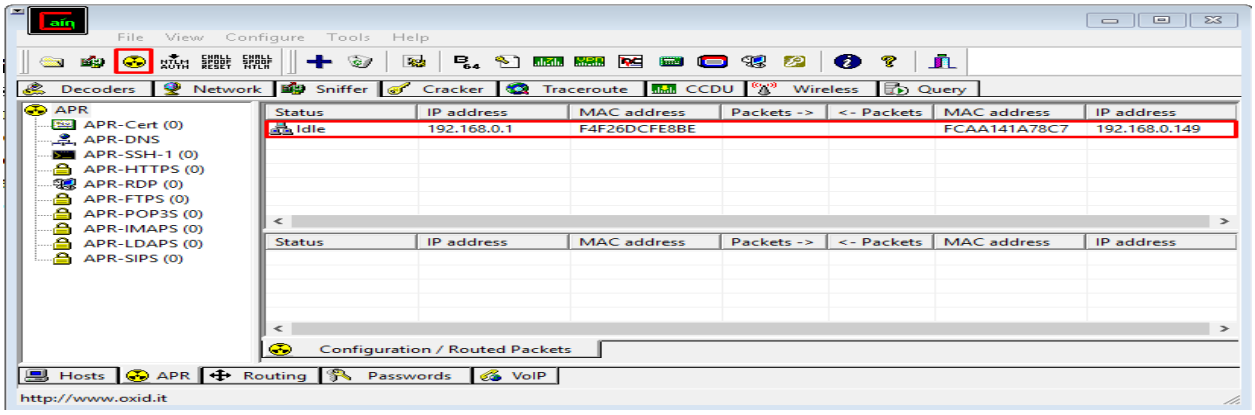
5. Now Select Your Subnet & Machine With The Target IP Address & Press OK.



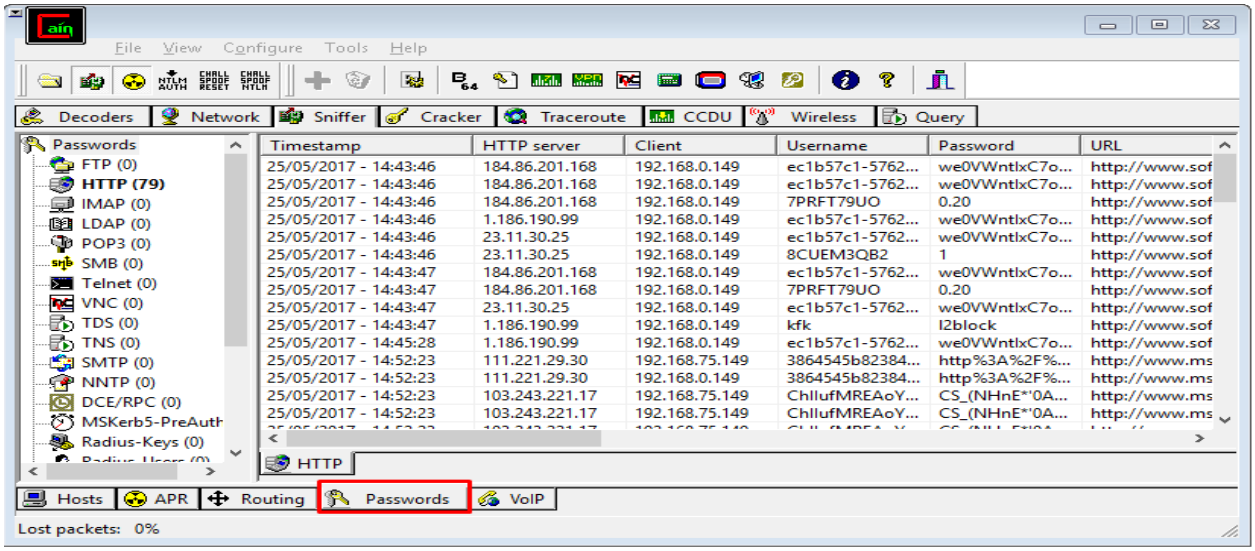
6. Select The Listed Machine & Click On Poison Icon On The Top Left.



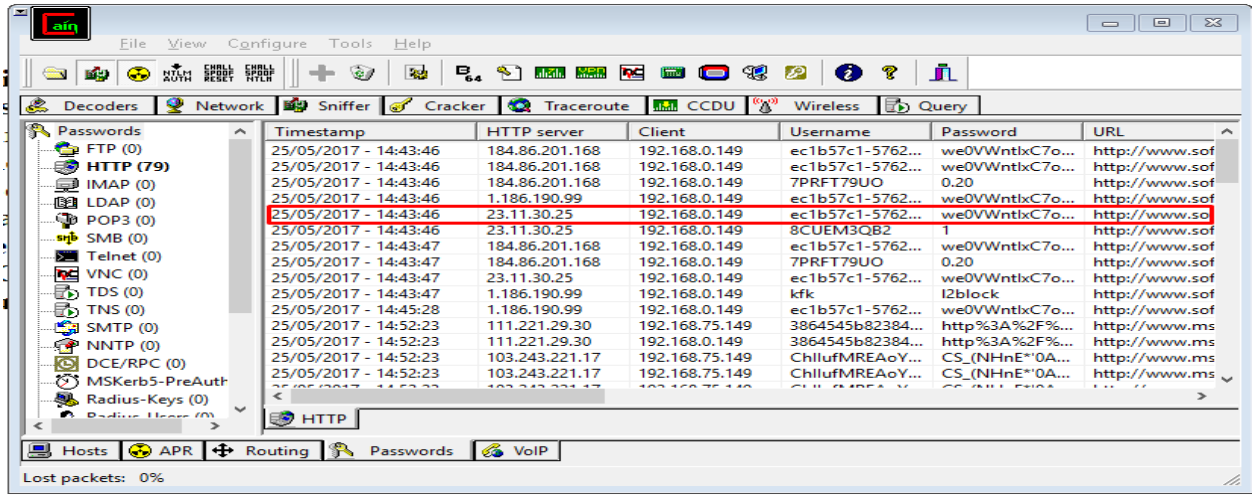
(Note : If You Get AN Exception : "Couldn't bind HTTPS acceptor socket", Press OK)



7. Go To Passwords Tab At The Bottom.



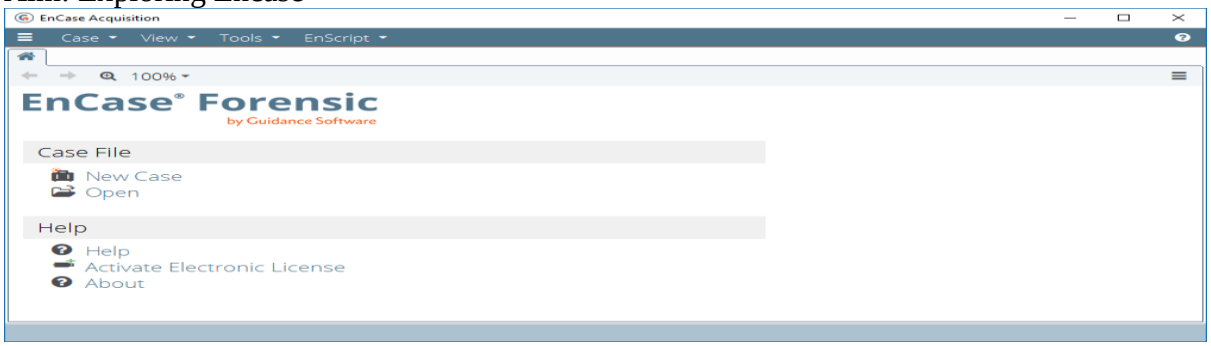
8. Sniffed Logs With All Information With Password Is Now Visible.

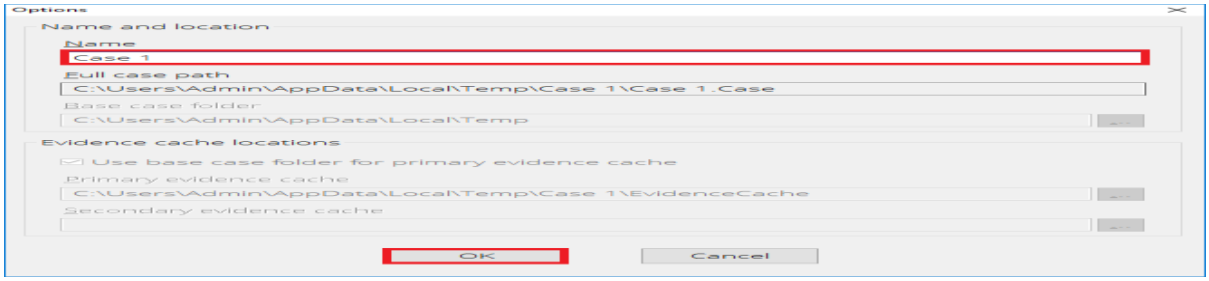


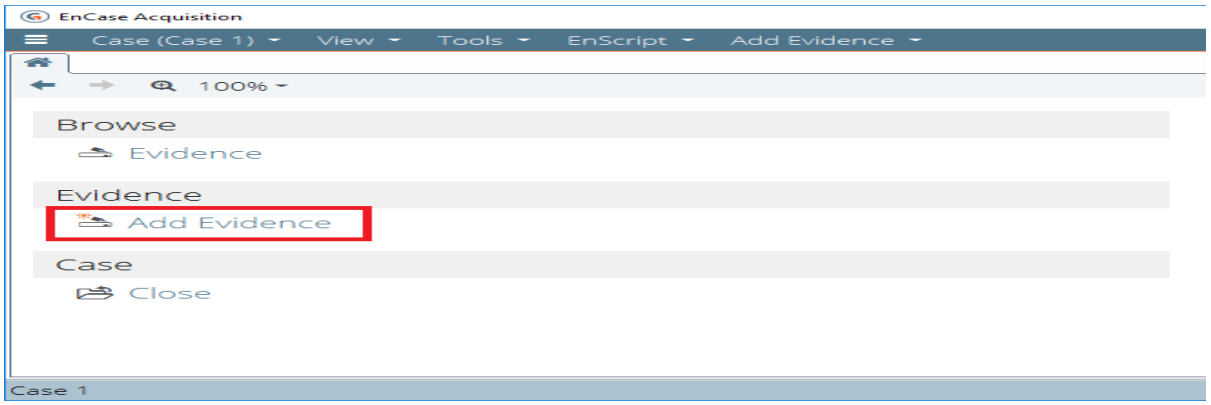
Practical No. 11

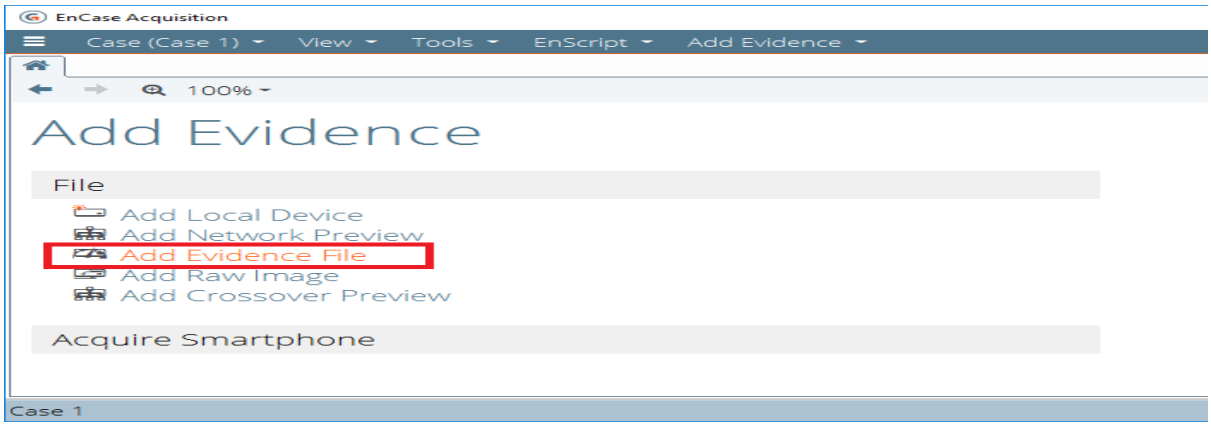
Forensics Investigation Using Encase

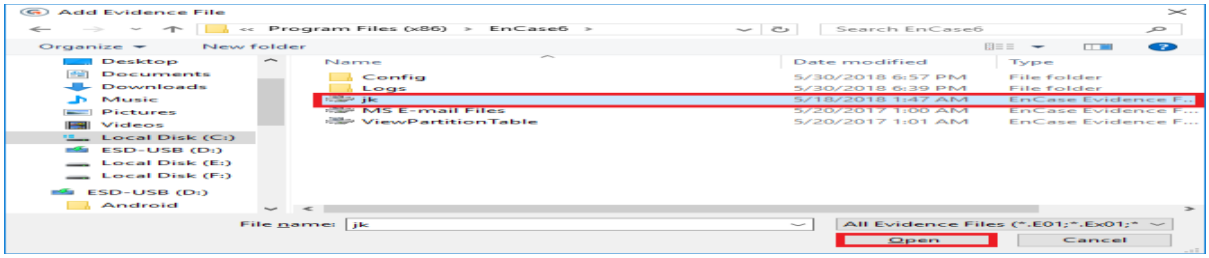
Aim: Exploring Encase

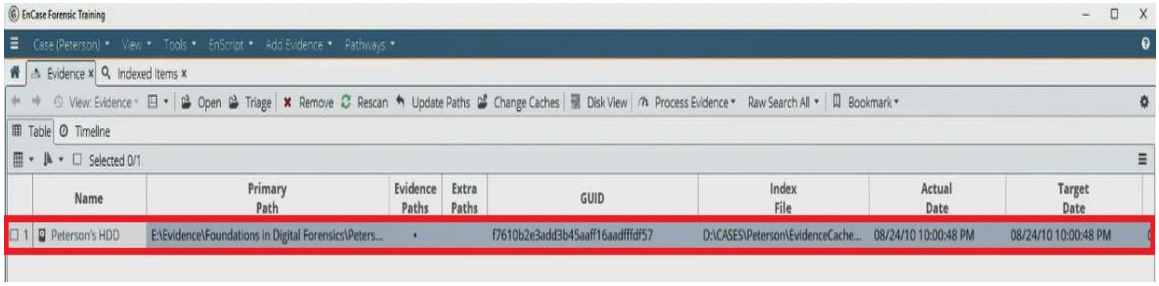




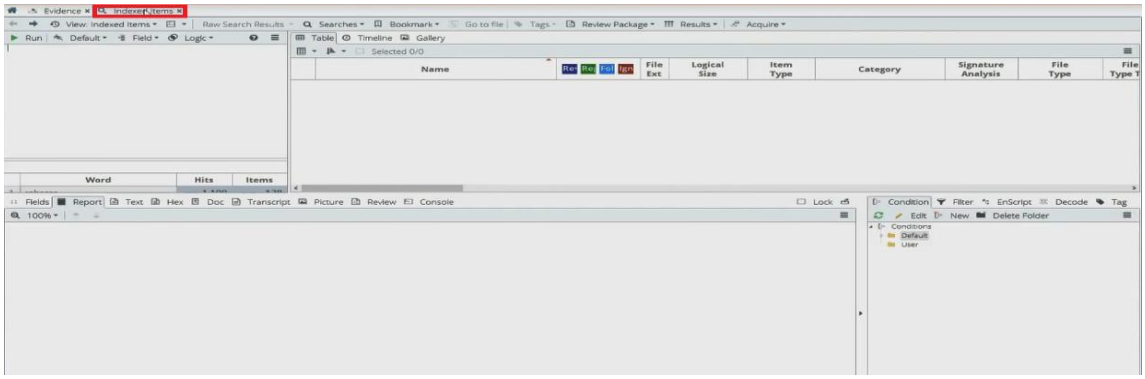




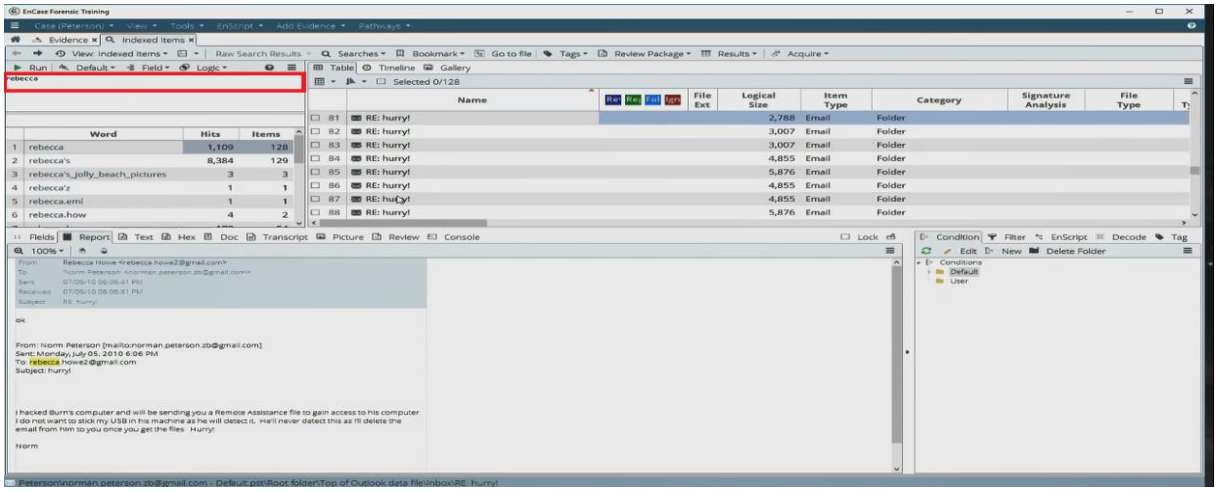




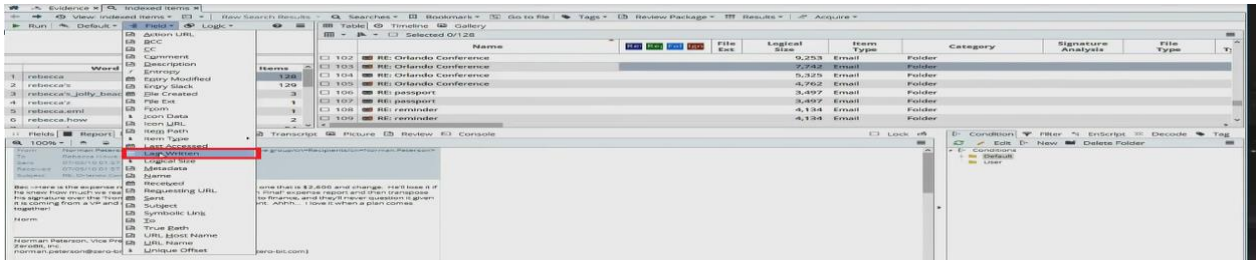
Navigate to Indexed Items



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

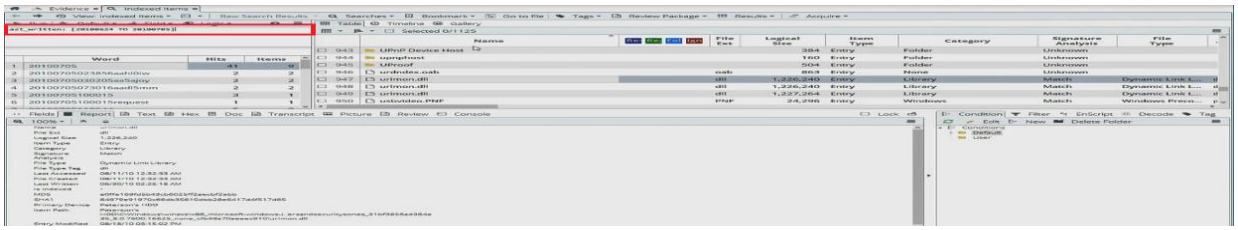


Now click on last written

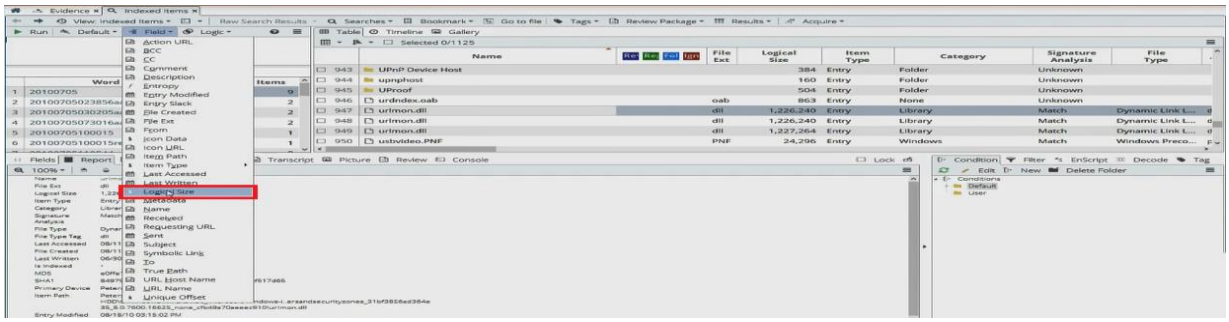


Last_written [20100624 TO 20100705]

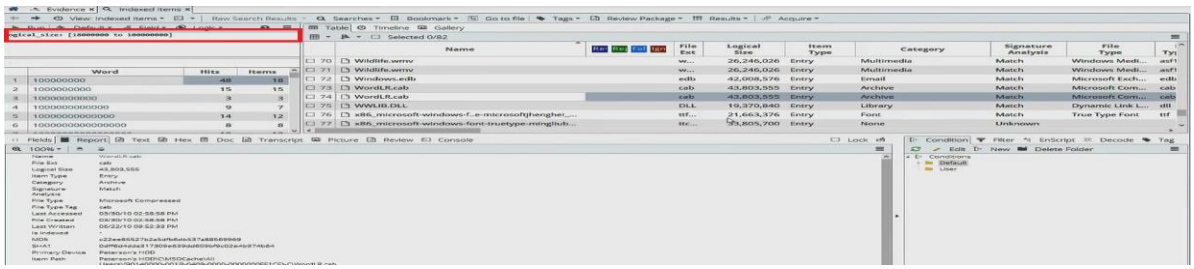
i.e last_witten [yyyymmdd To yyyymmdd] where y is year and m is month and d is day



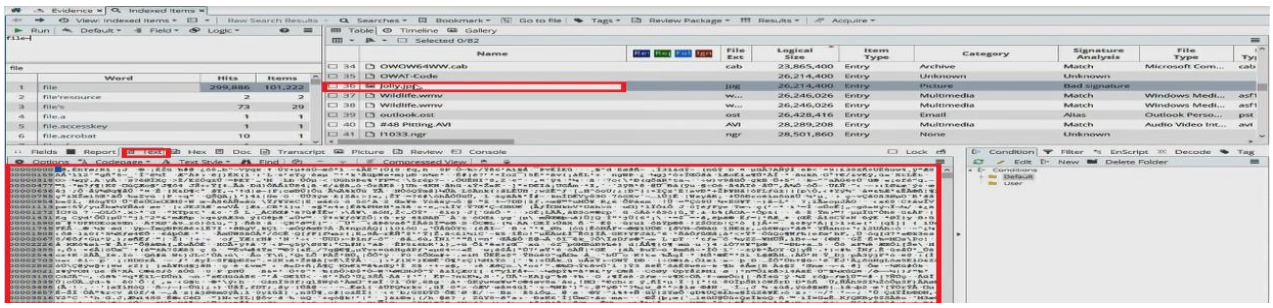
Now lets try Logical Size



Logical_size: [18000000 TO 10000000]



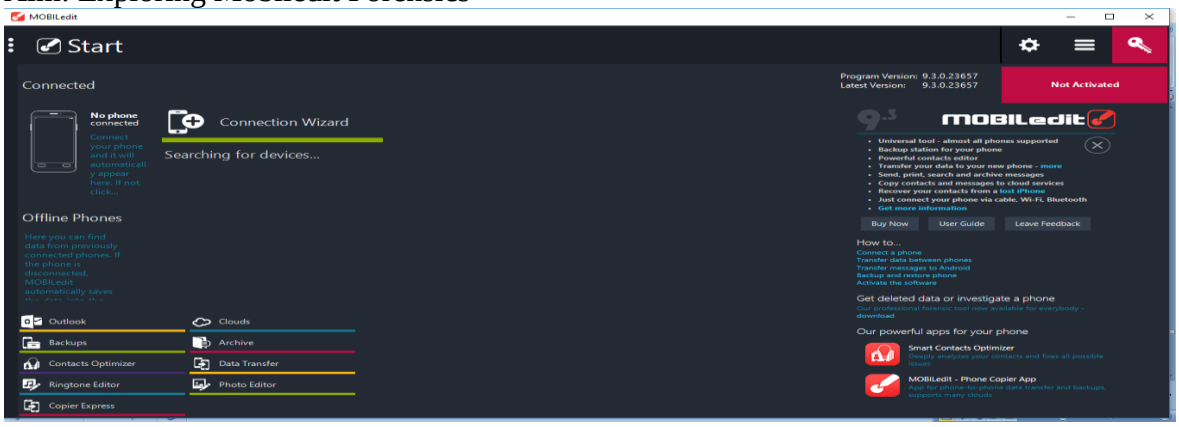
Now checking data on an File

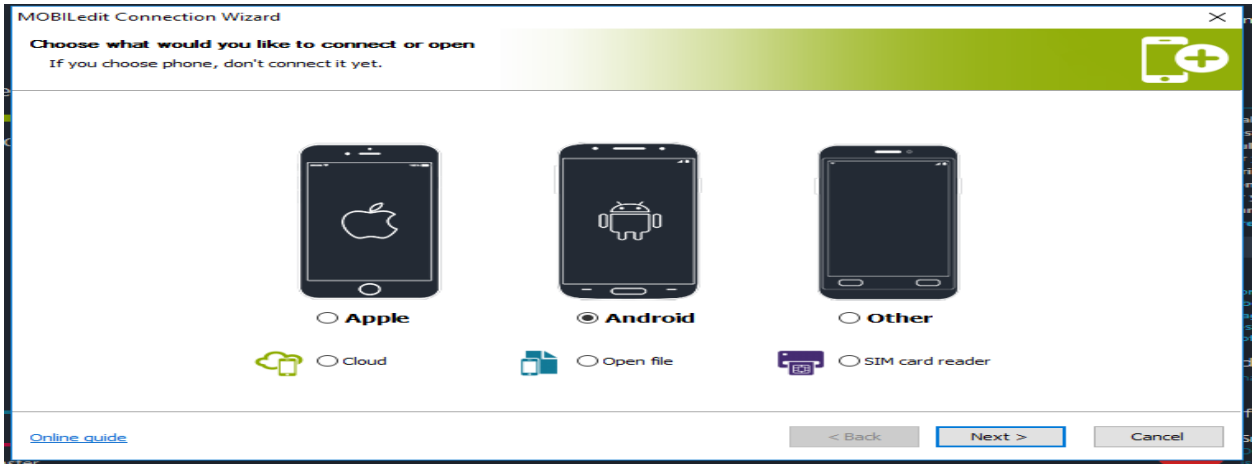


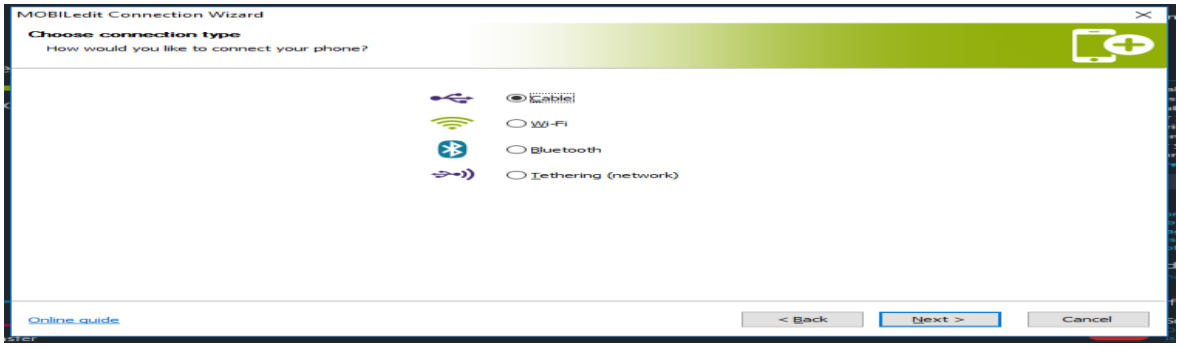
Practical No. 12

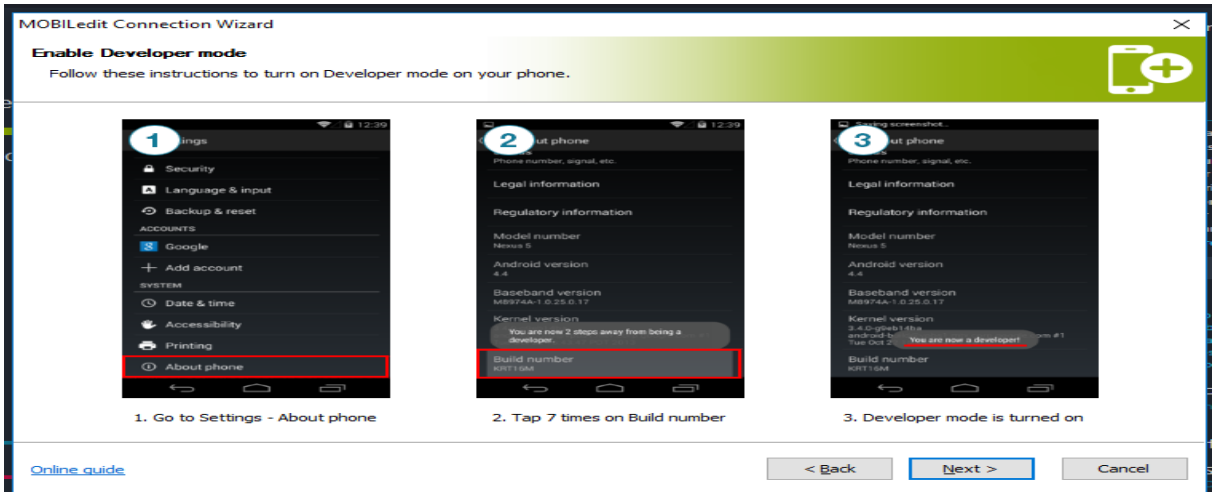
Using Mobile Forensics software tools

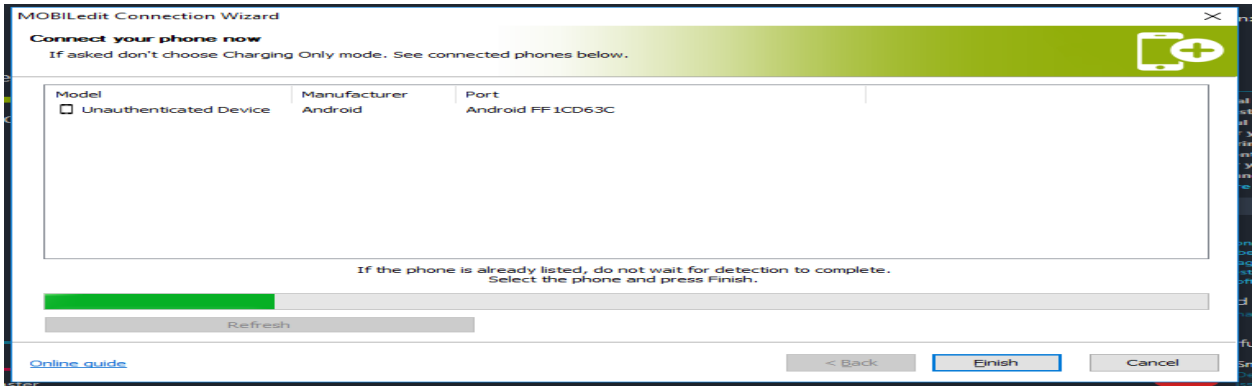
Aim: Exploring Mobiledit Forensics

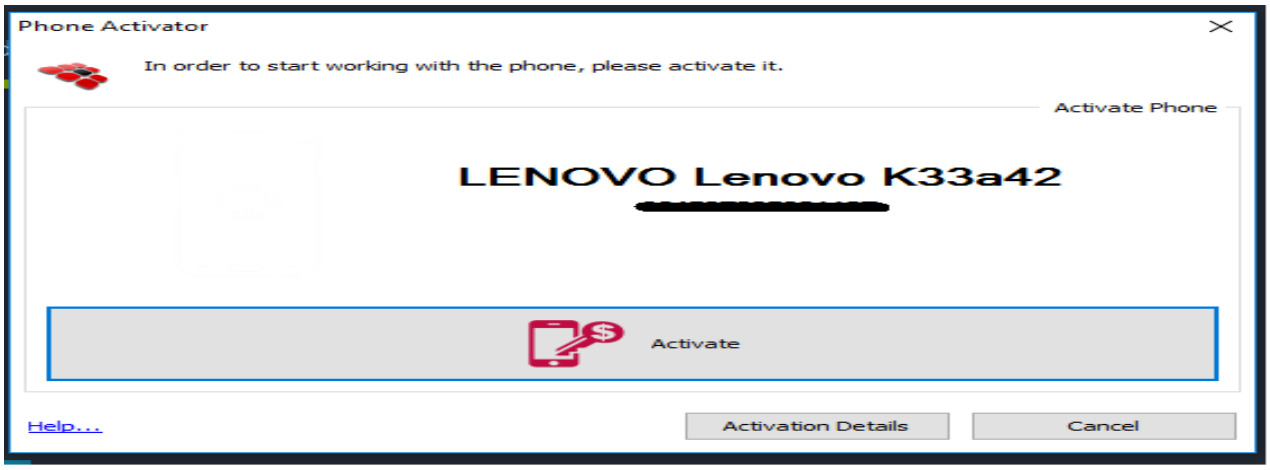


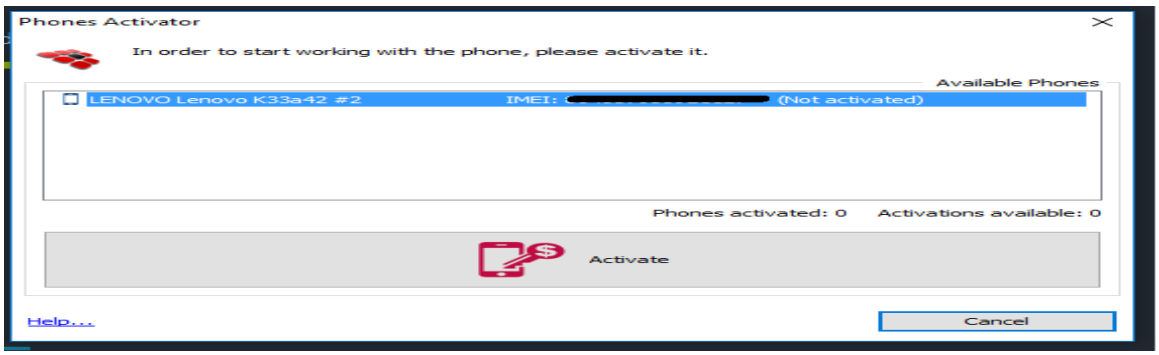


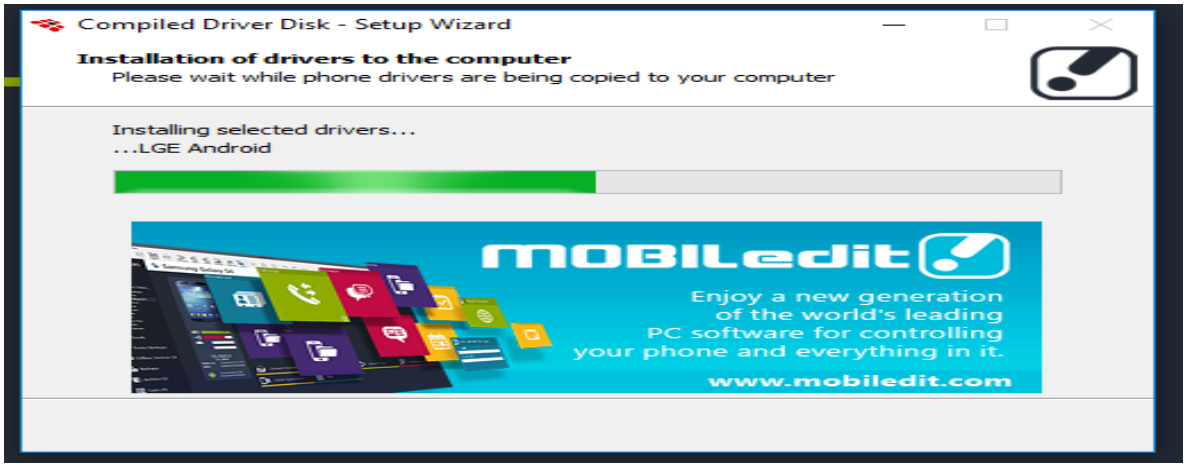


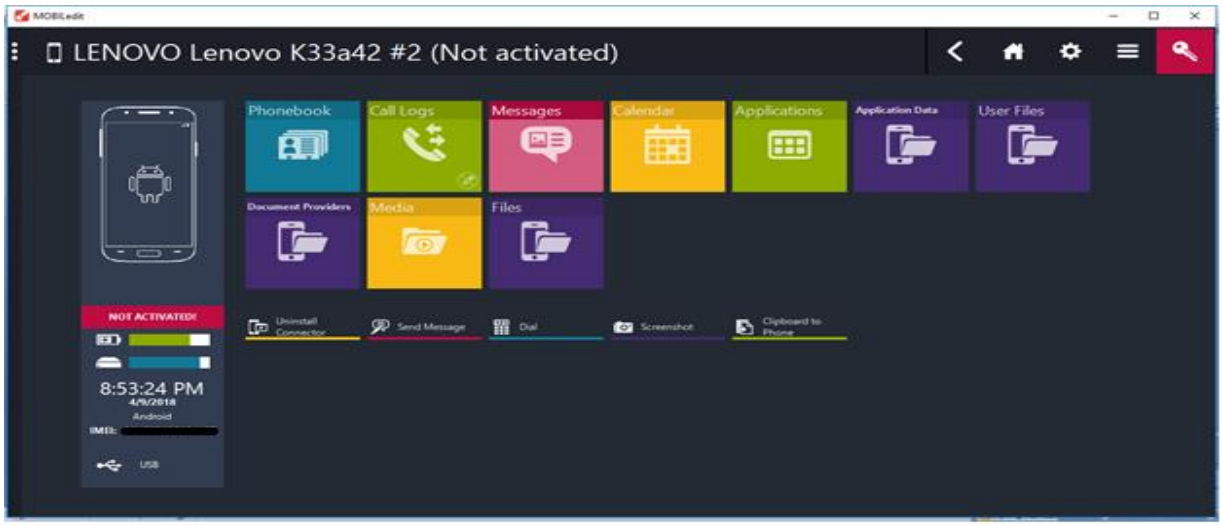

MOBILedit Connection Wizard
Enable Developer mode
Follow these instructions to turn on Developer mode on your phone.
1
Security
Language & input
Backup & reset
ACCOUNTS
Google
Add account
SYSTEM
Date & time
Accessibility
Printing
About phone
2
Legal information
Regulatory information
Model number
Android 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

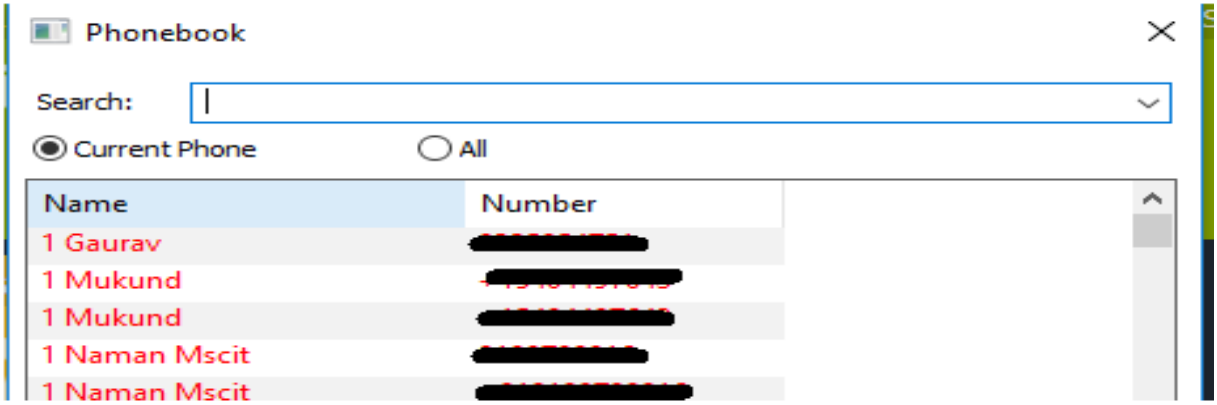

MOBILedit Connection Wizard
Connect your phone now
If asked don't choose Charging Only mode. See connected phones below.
Model
Manufacturer
Port
Unauthenticated Device
Android
Android FF1CD63C
If the phone is already listed, do not wait for detection to complete.
Select the phone and press Finish.
Refresh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

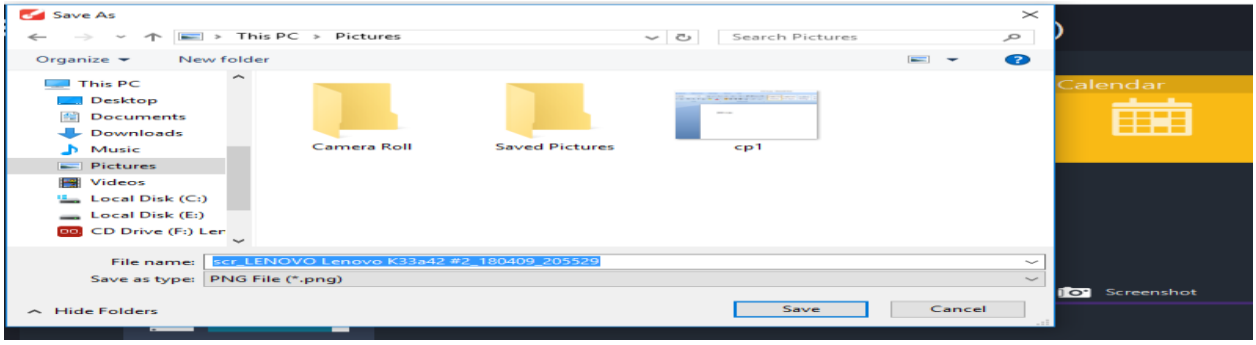

Phone Activator
In order to start working with the phone, please activate it.
Activate Phone
LENOVO Lenovo K33a42
[redacted]
Activate
Help...
Activation Details
Cancel

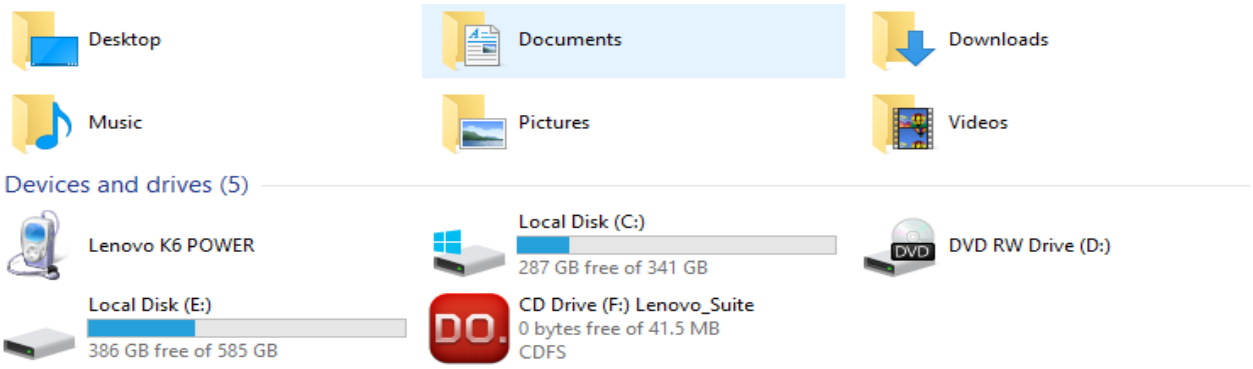

Phones Activator
In order to start working with the phone, please activate it.
Available Phones
LENOVO Lenovo K33a42 #2
IMEI: [redacted]
(Not activated)
Phones activated: 0
Activations available: 0
Activate
Help...
Cancel

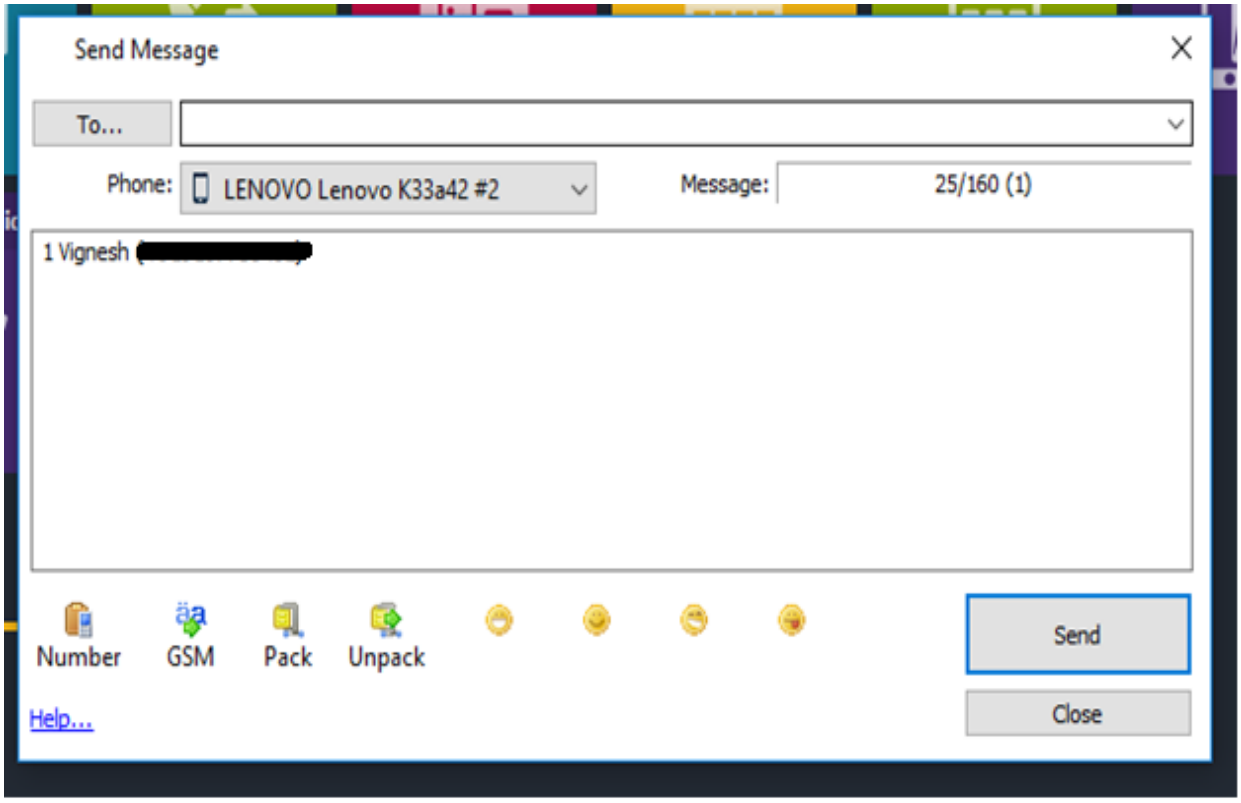

Compiled Driver Disk - Setup Wizard
Installation of drivers to the computer
Please wait while phone drivers are being copied to your computer
Installing selected drivers...
...LGE Android
MOBILedit
Enjoy a new generation of the world's leading PC software for controlling your phone and everything in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


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...