

# **Computer Forensics**

# **Contents**

Sr.NO	Name	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 (MobiEdit Forensics)	

# Practical 1

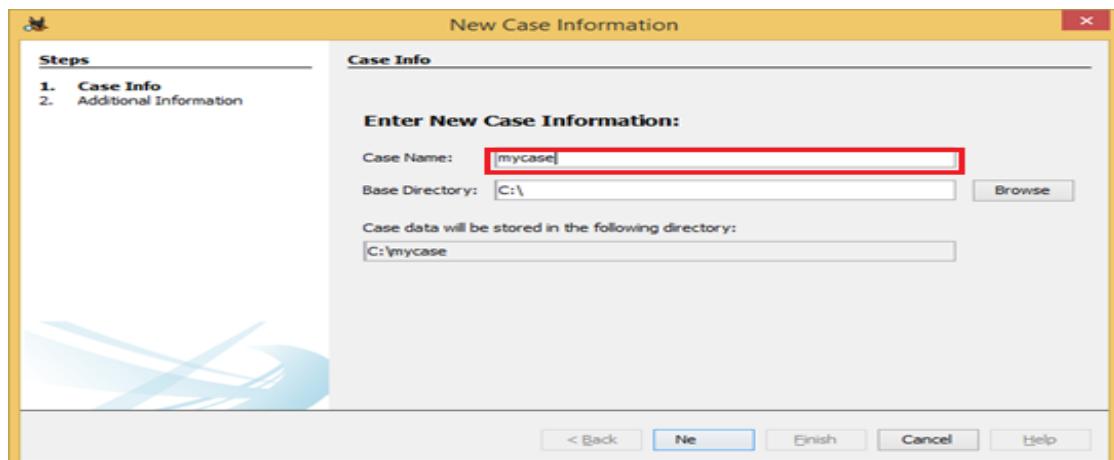
Aim: **File System Analysis [Autopsy]**

Step-1: Start Autopsy Tool

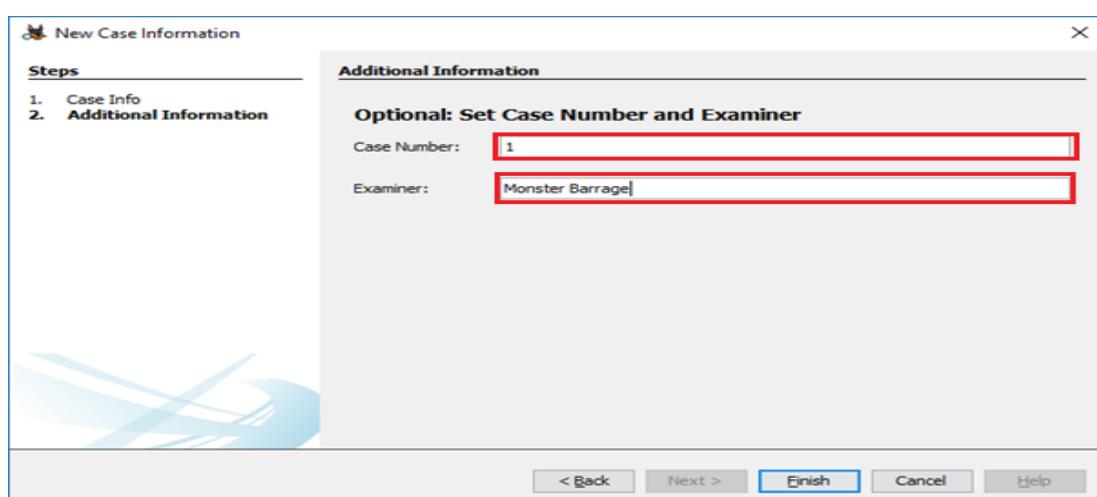
Step-2: Click Create New Case



Step-3: Enter The Details



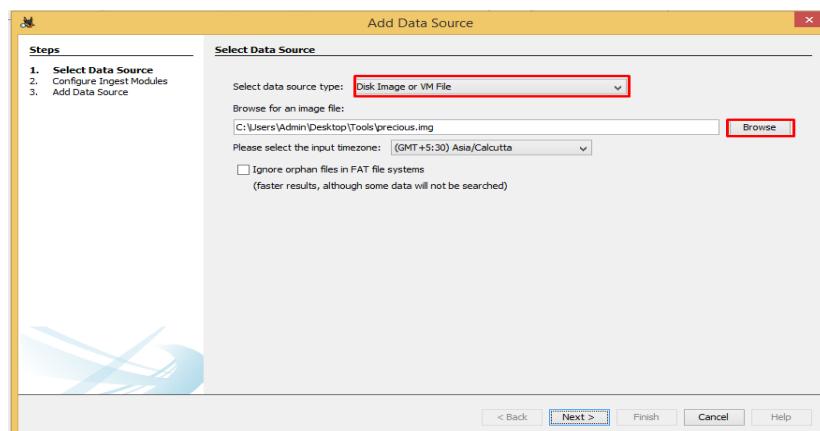
Step-4: Enter The Case Name & Case Examiner Name



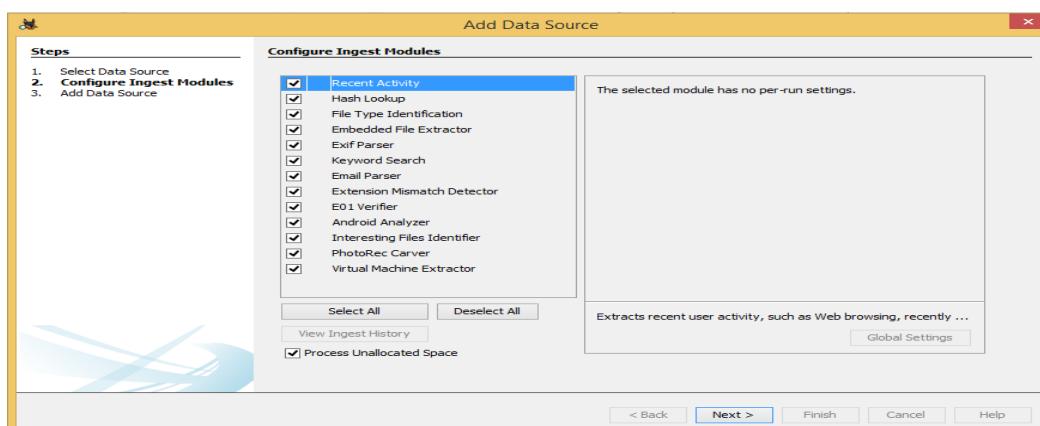
Step-5: After Clicking The Finish Button In The Above Window,

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

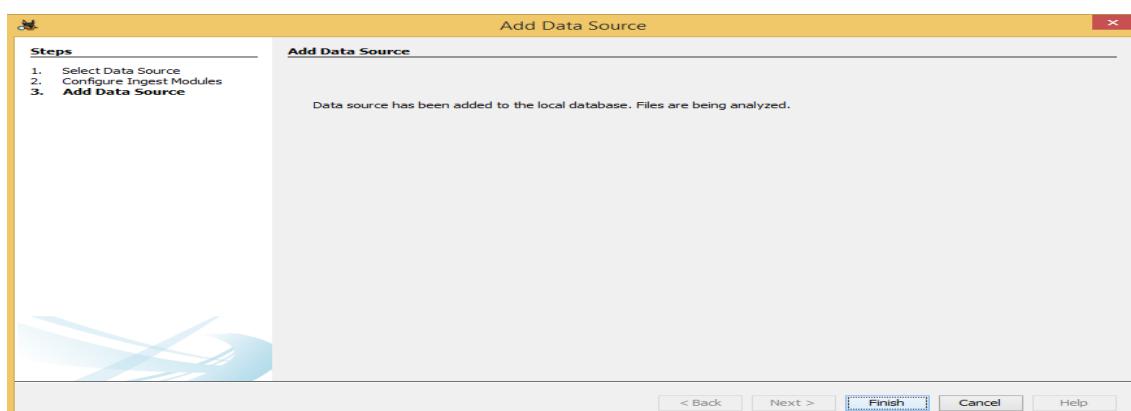
Then Browse The .img File Present In The Directory  
Click Next



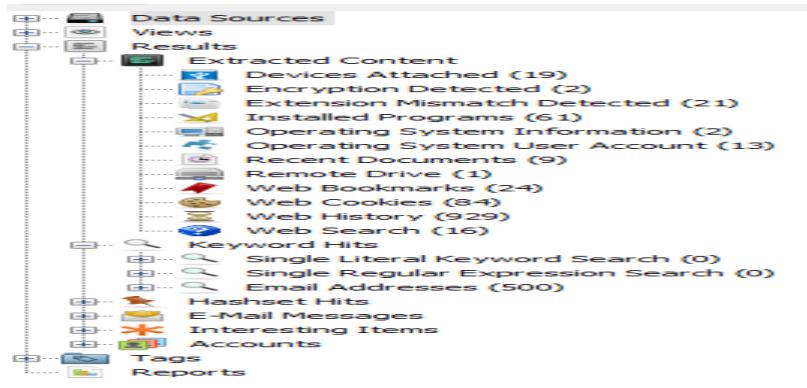
Step-6: The Next Step Provides A Ingest Wizard Panel Which Aims At Increasing The Search Capability. Select As Desired And Proceed To The Next Step.



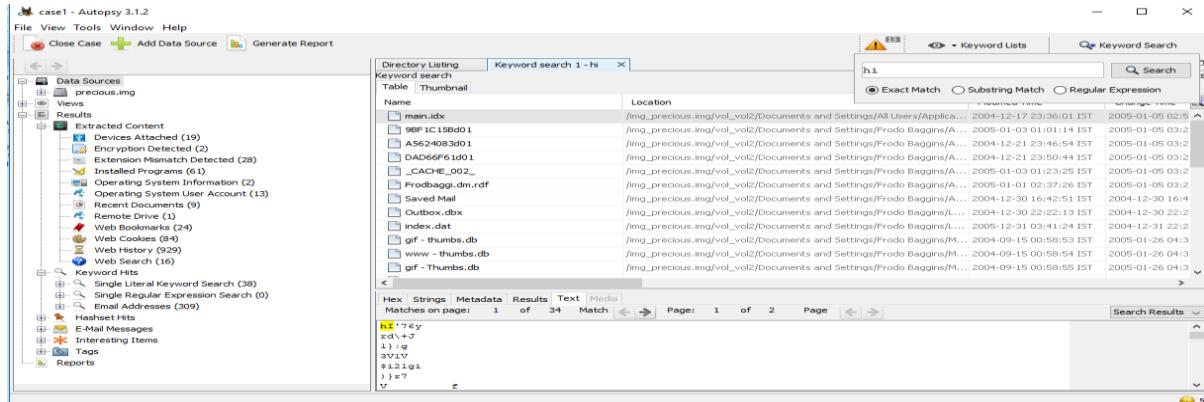
Step-7: In The Resulting Window, You'll Be Notified That The Files Are Being Analyzed. Proceed To Finish.



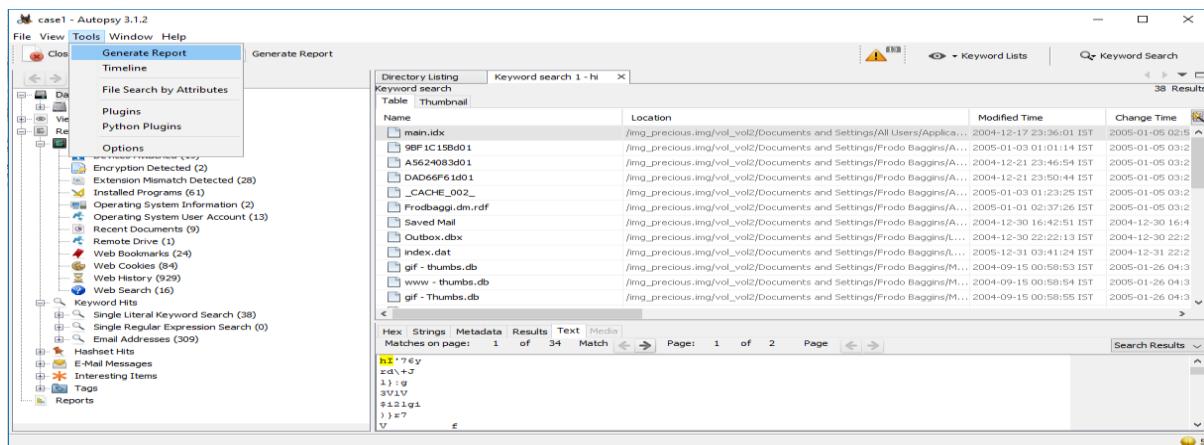
Step-8: After The Image Is Indexed The Tree Will Be Populated By The File System, Extracted Content, Keyword Searches, And The Hash List (If Any Were Used). This Tree Can Be To Retrieve The Information About The Image File Under Observation.

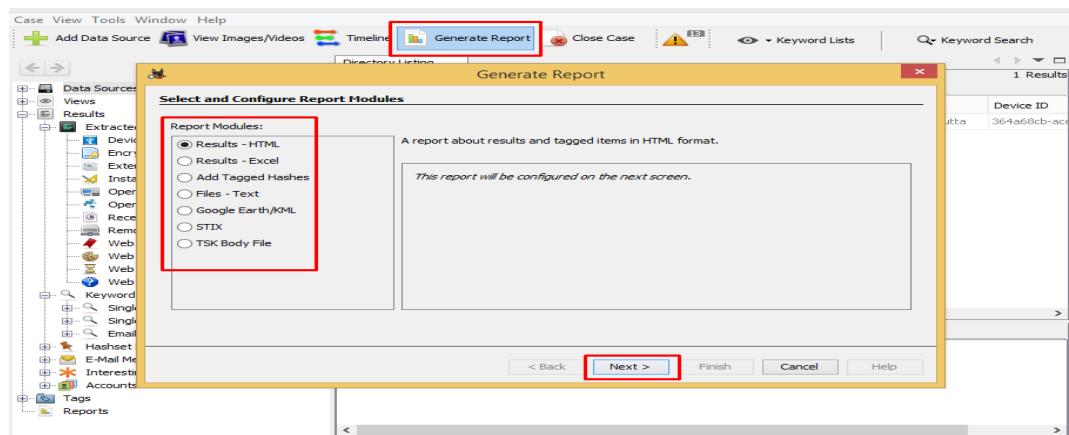


The Investigator can also Search by keyword



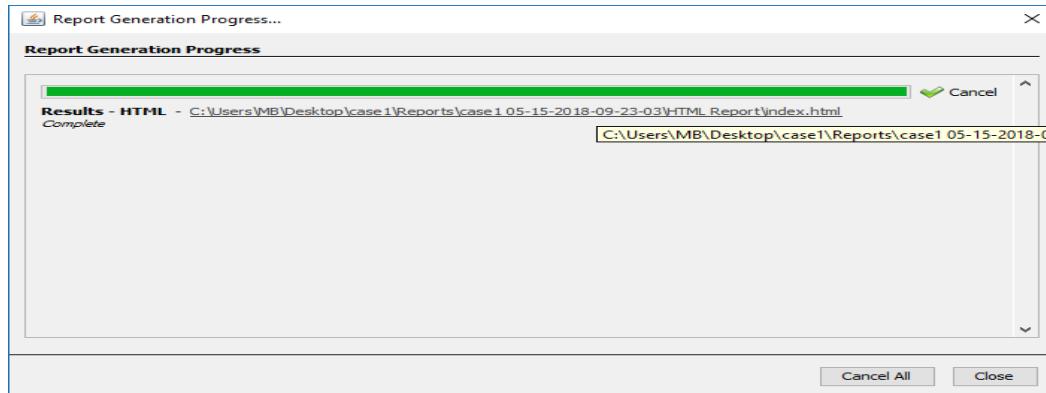
Should Generate A Report. This Will Allow The Investigator To Have An Idea Of What Type Of Information Is Available And What To Expect.



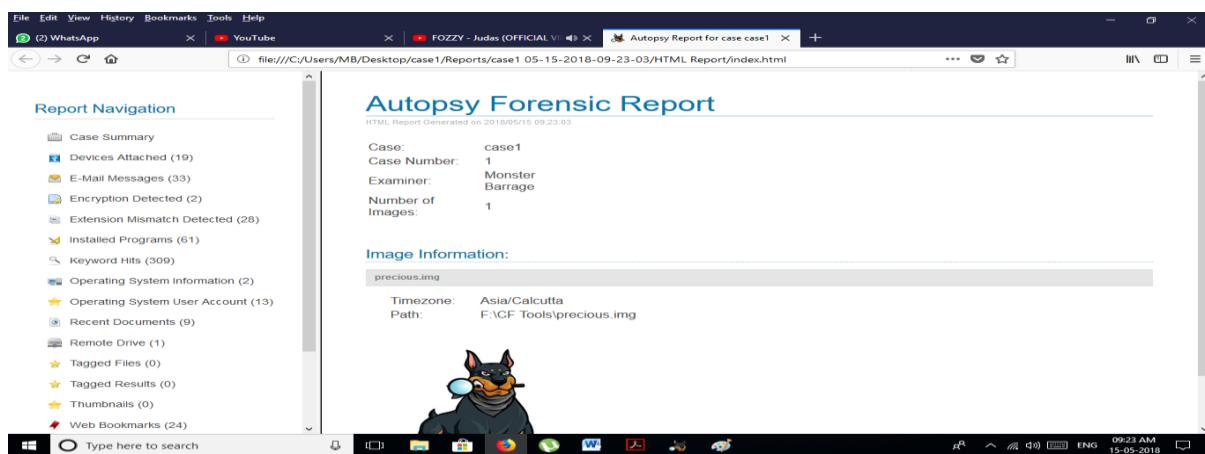


Click Next And Then Finish

.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

Case Information

Investigator Name:	MB
Case Number:	1
Case Name:	CASE12
Case Path:	C:\Users\MB\Desktop\
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\ Case Folder: C:\Users\MB\Desktop\Case12
Case Description:	

Next > Cancel

FTK Report Wizard - Case Information

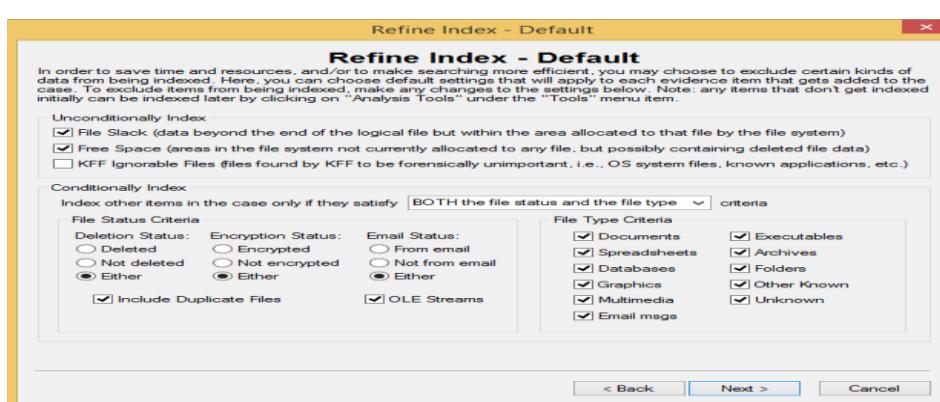
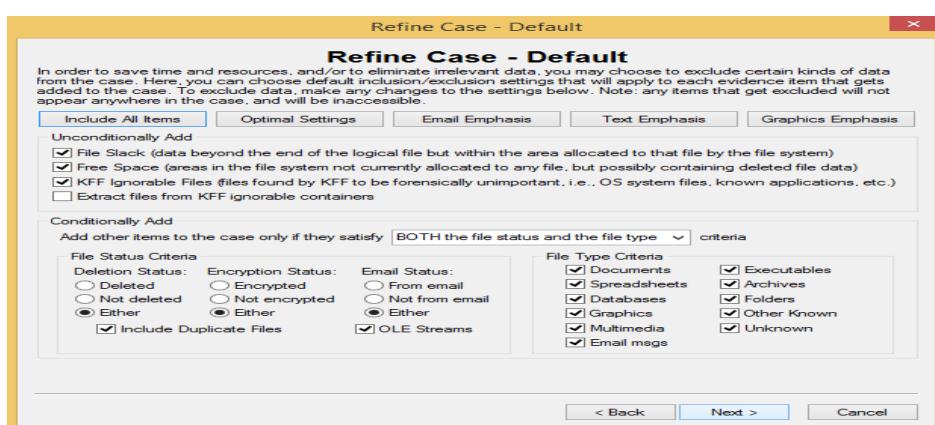
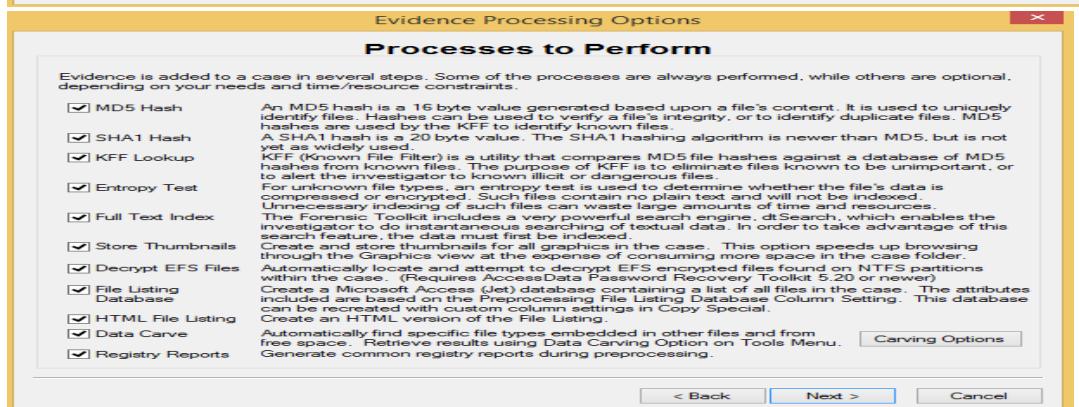
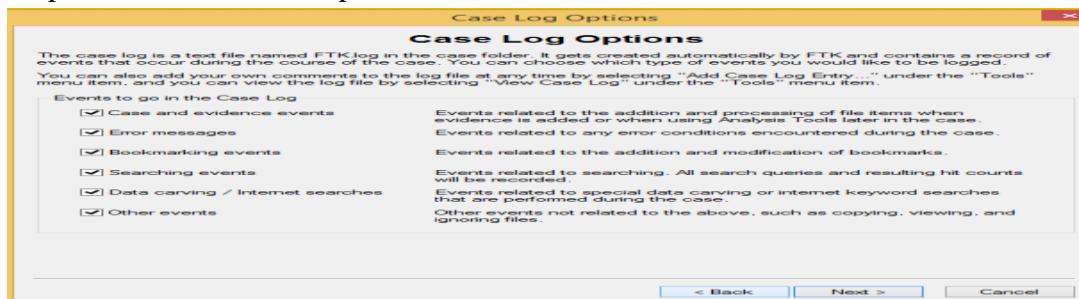
**Forensic Examiner Information**

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:	

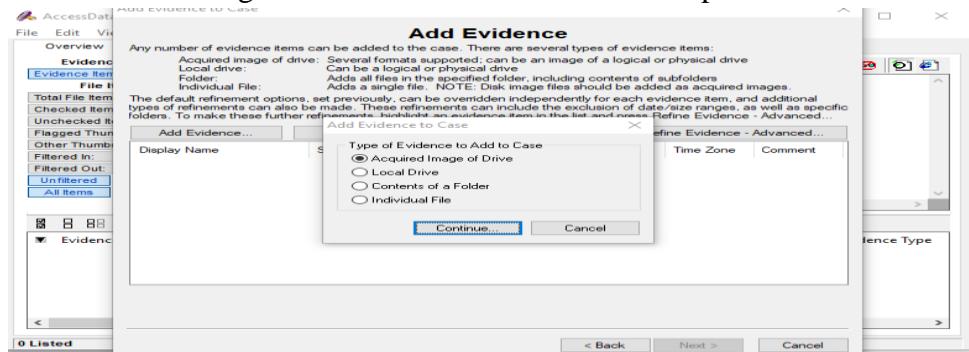
< Back Next > Cancel

## Step-4: Select Relevant Options And Proceed.

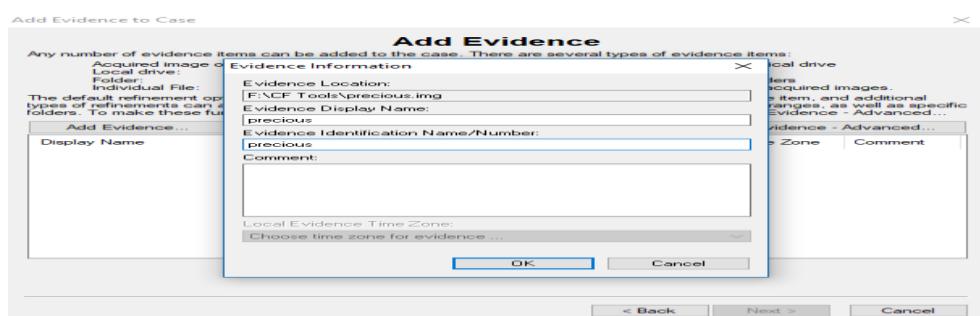


## Step-5: Adding Evidence.

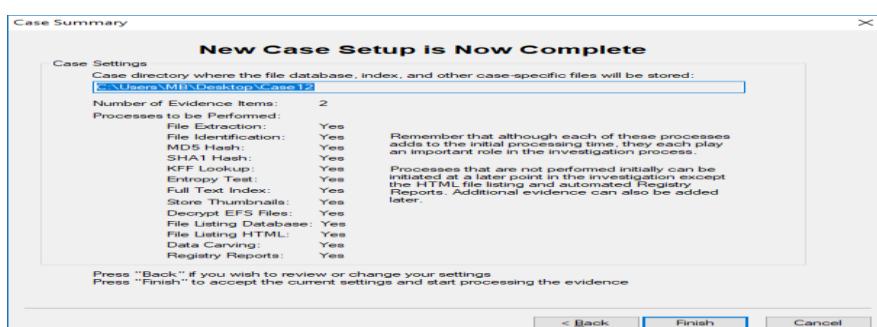
We Can Add Evidence Now Or Later Via The File Menu. The Evidence Can Be In The Form Of Accquired Image Of Drive Local Drive Contents Of A Folder Individual File According To The Option Selected We Will Be Presented With The Relevant Popup Screen. For Now We Will Be Going With The Contents Of A Folder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



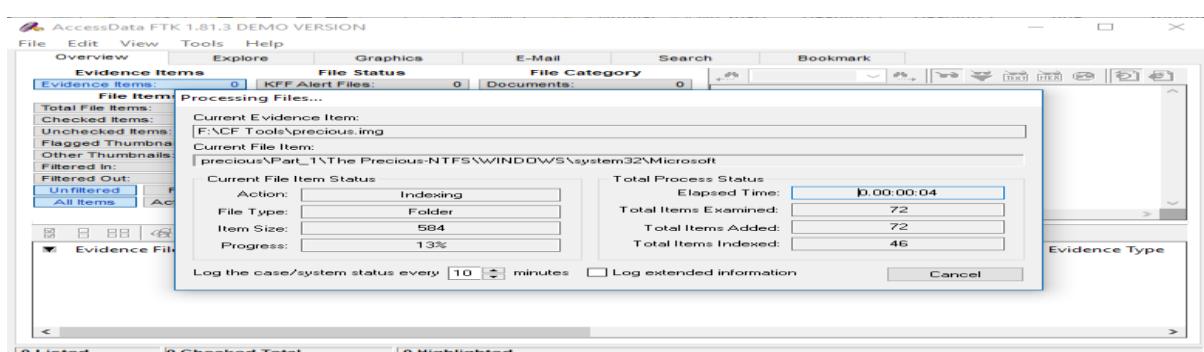
Select The Image File



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.

The screenshot shows the AccessData FTK interface with the following details:

- Evidence Items:** 3 (highlighted)
- File Status:**
  - Total File Items: 462
  - Checked Items: 0
  - Unchecked Items: 462
  - Flagged Thumbnails: 0
  - Other Thumbnails: 25
  - Filtered In: 462
  - Filtered Out: 0
  - Unfiltered: All Items
  - Actual Files
- File Category:**

Documents:	0
Spreadsheets:	0
Databases:	0
Graphics:	25
From E-mail:	0
Deleted Files:	0
From Recycle Bin:	0
Executables:	20
Archives:	5
Folders:	0
Slack/Free Space:	0
Other Known Type:	2
Unknown Type:	409
- Evidence File Name:** IOLogErrors.Log, red.c, Tools
- Evidence Path:** C:\Users\Admin\Desktop\Tools, C:\Users\Admin\Pictures, C:\Users\Admin\Desktop
- Display Name:** IOLogErrors, red, EvidenceOne
- Identification Name/Number:** 425, 123, 4567
- Evidence Type:** Individual file, Individual file, Contents of a folder

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.

The screenshot shows the AccessData FTK interface with the following details:

- File Menu:** New Case..., Open Case..., Add Evidence..., FTK Imager..., Disk Viewer..., Registry Viewer..., Close Case, Save Case, **Backup Case...** (highlighted), Export Files..., Report Wizard..., Update Report, View Report..., Exit, c:\Abnormal Bride
- Evidence Items:** 3 (highlighted)
- File Status:**
  - Total File Items: 462
  - Checked Items: 0
  - Unchecked Items: 462
  - Flagged Thumbnails: 0
  - Other Thumbnails: 25
  - Filtered In: 462
  - Filtered Out: 0
  - Unfiltered: All Items
  - Actual Files
- File Category:**

Documents:	0
Spreadsheets:	0
Databases:	0
Graphics:	25
From E-mail:	0
Deleted Files:	0
From Recycle Bin:	0
Executables:	20
Archives:	5
Folders:	0
Slack/Free Space:	0
Other Known Type:	2
Unknown Type:	409
- Evidence File Name:** IOLogErrors.Log, red.c, Tools
- Evidence Path:** C:\Users\Admin\Desktop\Tools, C:\Users\Admin\Pictures, C:\Users\Admin\Desktop
- Display Name:** IOLogErrors, red, EvidenceOne
- Identification Name/Number:** 425, 123, 4567
- Evidence Type:** Individual file, Individual file, Contents of a folder

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

The screenshot shows the AccessData FTK interface with the following details:

- Email Tab:** Deleted Items.dbx
- Deleted Items:**
  - Deleted Message0001
  - Deleted Message0002
  - Deleted Message0003
  - Deleted Message0004
  - Deleted Message0005
  - Deleted Message0006
- Message Preview:**

**Deleted Message0002**

**Subject:** Possible Job!!  
**From:** Baggifrodo  
**Date:** 1/2/2005  
**To:** samwizgamgee@hotmail.com

**Message Body:**

I got a call today from the Regional Forensic Lab in Isengard. They are starting a new computer forensic section and want to know if we want to join in? What do you think? This might be a real opportunity. The only down side

Select an email and investigate it

**Deleted Message0002**

**Subject:** Possible Job!!  
**From:** Baggifrodo  
**Date:** 1/2/2005  
**To:** samwizgamgee@hotmail.com

**Message Body**

I got a call today from the Regional Forensic Lab in Isengard. They are starting a new computer forensic section and want to know if we want to join in? What do you think? This might be a real opportunity. The only down side is that I hear Gandalf is going to head the department. If my memory serves me, he can be a real pain to work for. Remember how he used to push us around and talk down to us like he was some kind of all knowing wizard or something. Maybe he has changed now that he is Whitehat. Speaking of Gandalf, look at this... [Attachment: "D:\Documents and Settings\Frodo Baggins\My Documents\My Pictures\cartmanlotrparody.jpg"]

## 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.

**Subject:** Possible Job!!  
**From:** Baggifrodo  
**Date:** 1/2/2005  
**To:** samwizgar

**Message Body**

I got a call today from the Regional Forensic Lab in Isengard. They are starting a new computer forensic section and want to know if we want to join in? What do you think? This might be a real opportunity. The only down side is that I hear Gandalf is going to head the department. If my memory serves me, he can be a real pain to work for. Remember how he used to push us around and talk down to us like he was some kind of all knowing wizard or something. Maybe he has changed now that he is Whitehat. Speaking of Gandalf, look at this... [Attachment: "D:\Documents and Settings\Frodo Baggins\My Documents\My Pictures\cartmanlotrparody.jpg"]

## 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.

Case Information	
5/22/2017	Version 1.81.3, build 09.04.10
FTK Version	Version 1.81.3, build 09.04.10
Case Number	1234
Case Location	C:\Doecase\
Case Description	Monday, May 22, 2017 2:33:21 PM
Report Created	Sherlock
Forensic Examiner	Sherlock
Agency	Sherlock
Address	22B, Baker Street
Fax	
E-mail	
Comments	
Investigator	Sherlock
Agency	Sherlock
Address	

# Practical 3

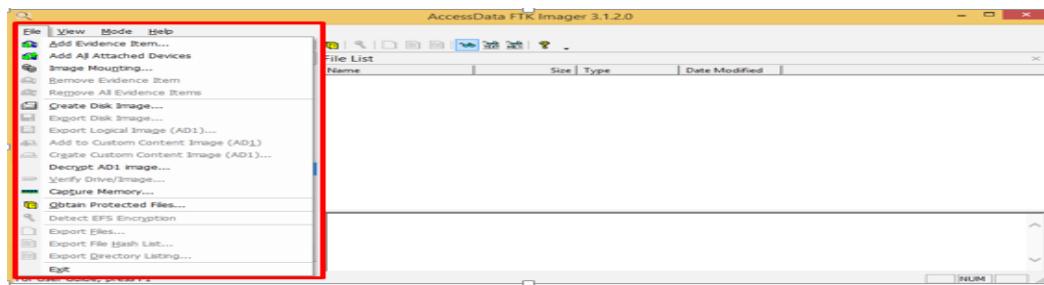
Aim : **Using File Recovery Tools [FTK Imager] Creating Image**

Step-1: Open Access FTK Imager

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

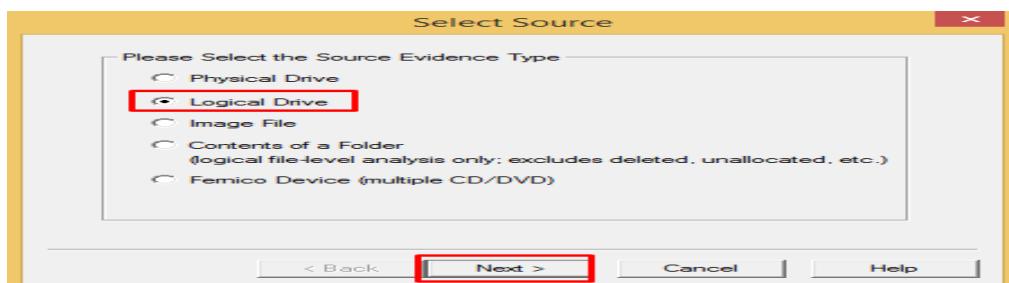
We Will Proceed With Creating A Disk Image Of A Logical Drive.

Select Create Disk Image.

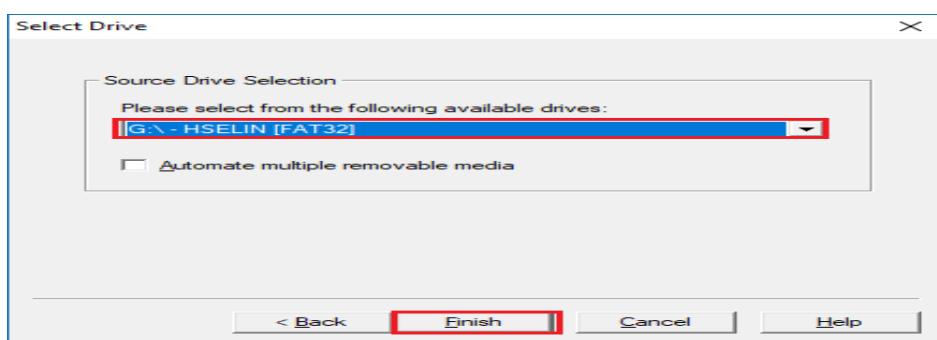


Step-3: In The Resulting Popup,

Select Logical Drive And Click Next.



Select A Drive And Click Finish.



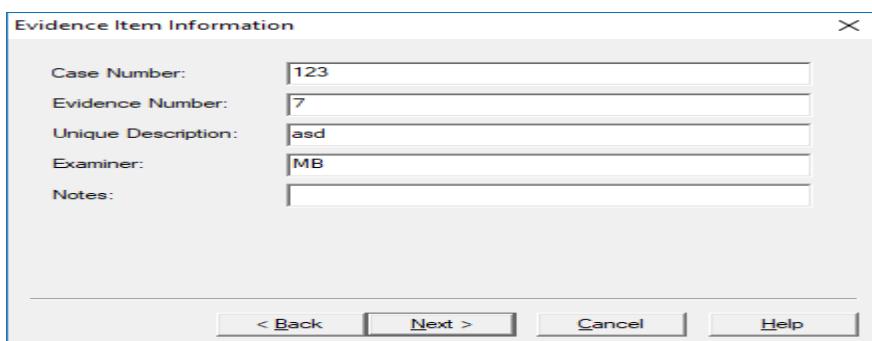
Step-4: Creating Image – Configuring Options

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

We Will Go With Raw Type Here.

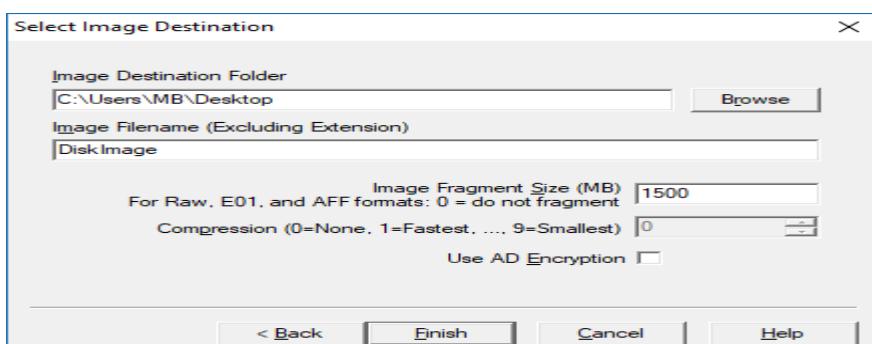


Proceed With Filling The Required Information In The Resulting Popup.

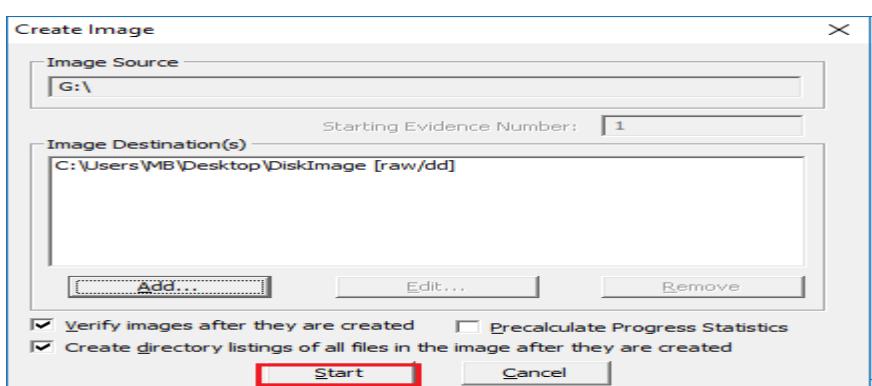


Provide The Location For The Disk Image File To Be Stored.

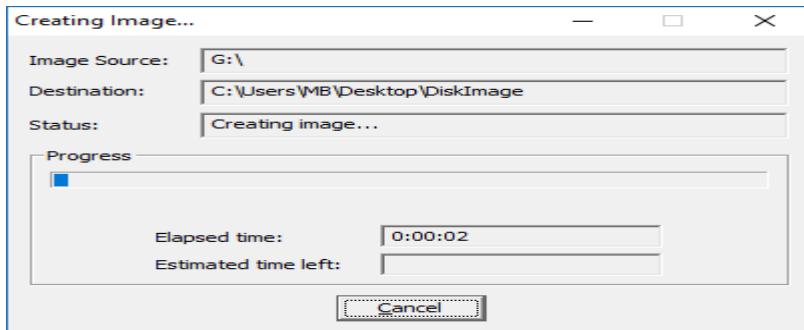
Click Finish.



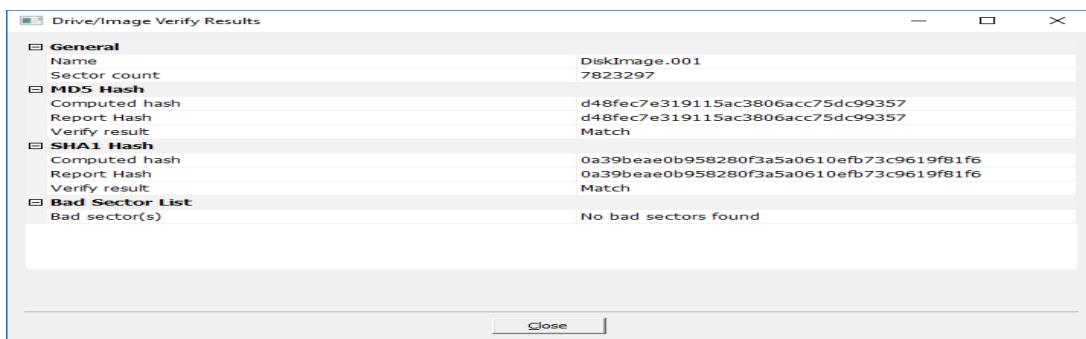
Click Start To Proceed With The Creating Of The Image.



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



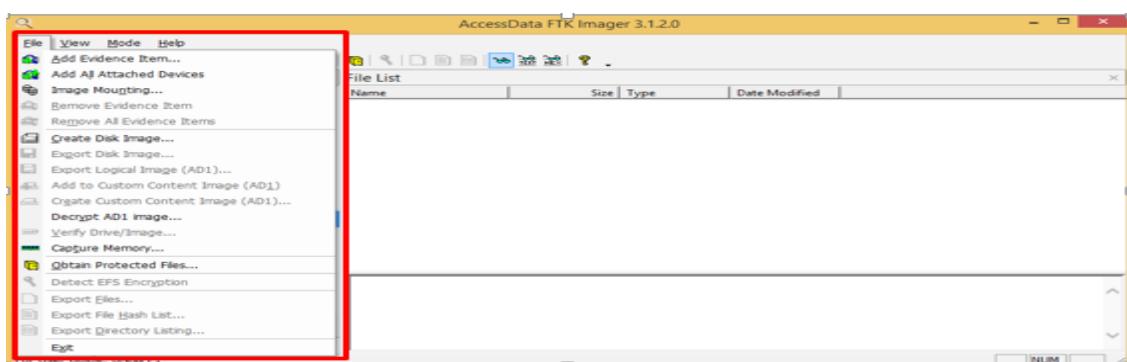
Step-5: After The Processing, A Dialog Box Will Show The Results.



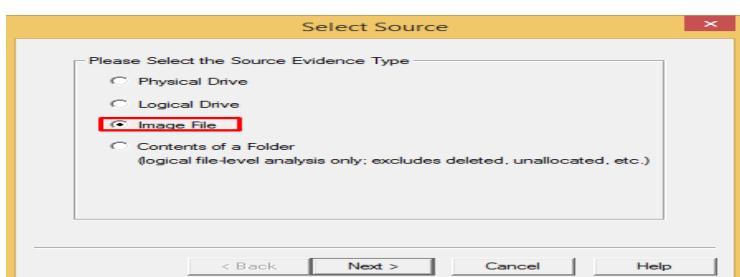
## Using File Recovery Tools [FTK Imager] Using Evidence

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.

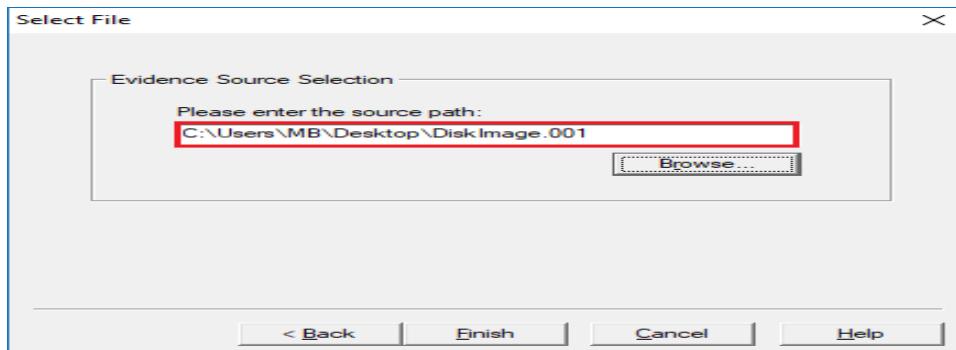


Step-3: In The Resulting Popup Select The Image File Option And Click Next

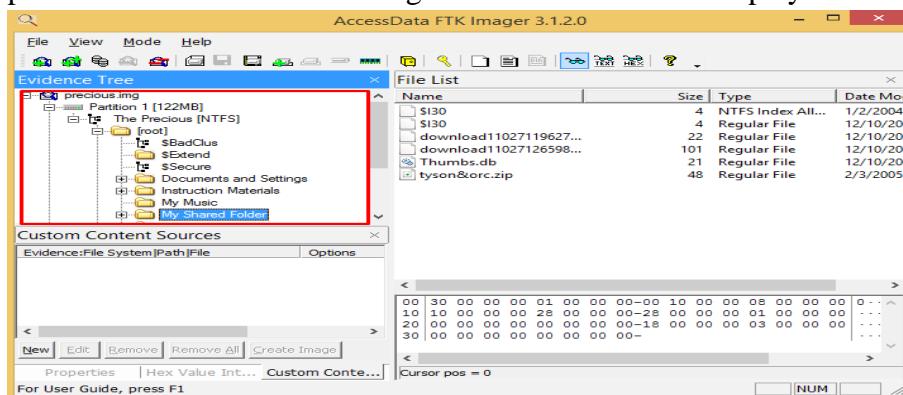


Step-4: Provide The Location Of The Image File To Be Used

Click Finish.



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

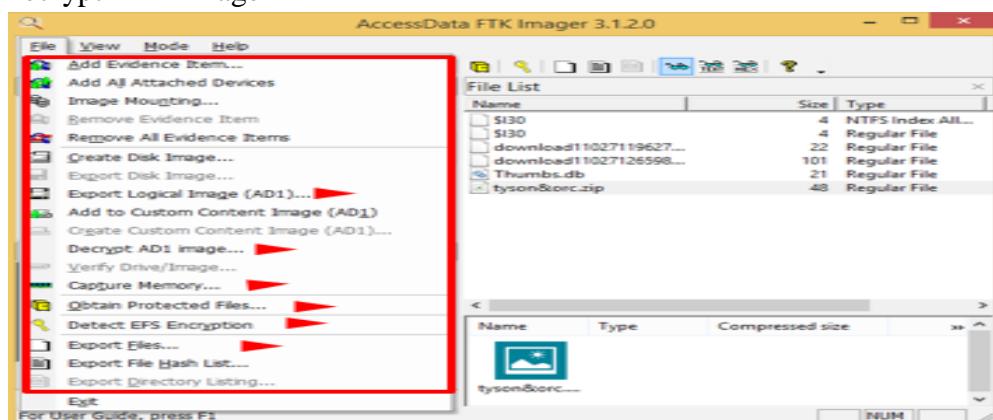


Step-6: In The File Menu, There Are Various Options That Can Be Used

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.

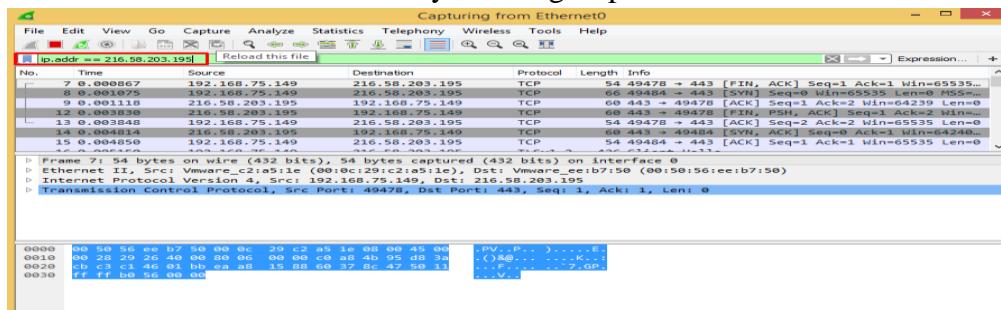
# Practical 4

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

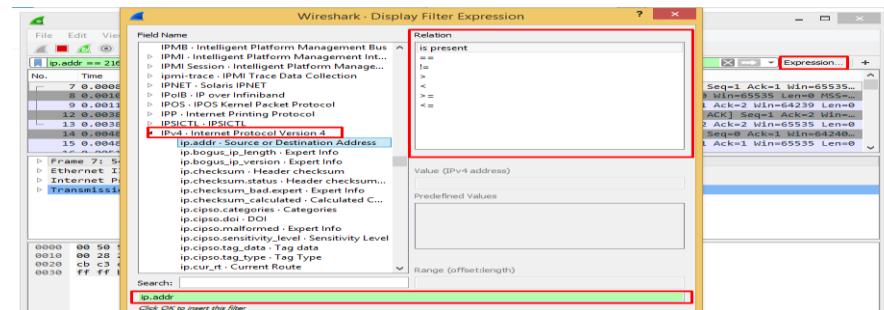
Step-1: Open Wireshark

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.

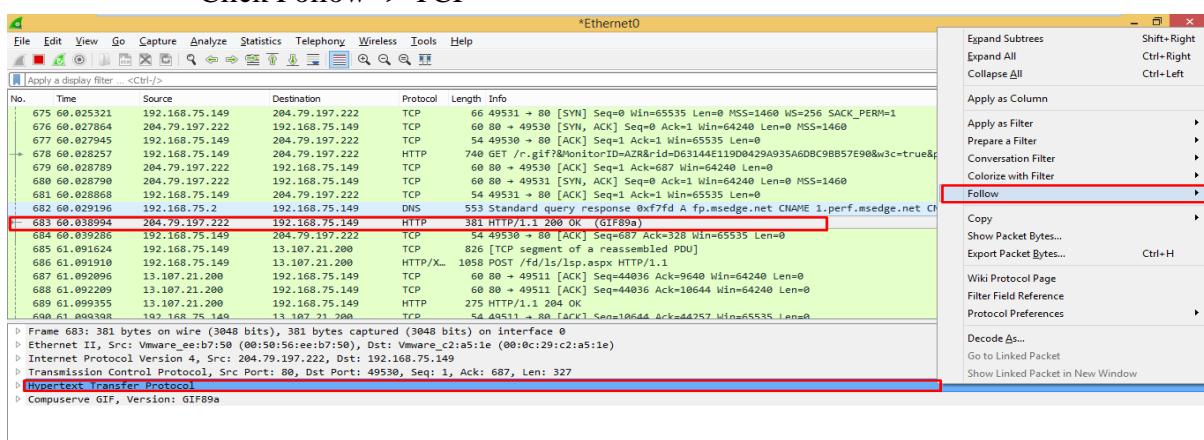


Step-3: Analyzing A Packet.

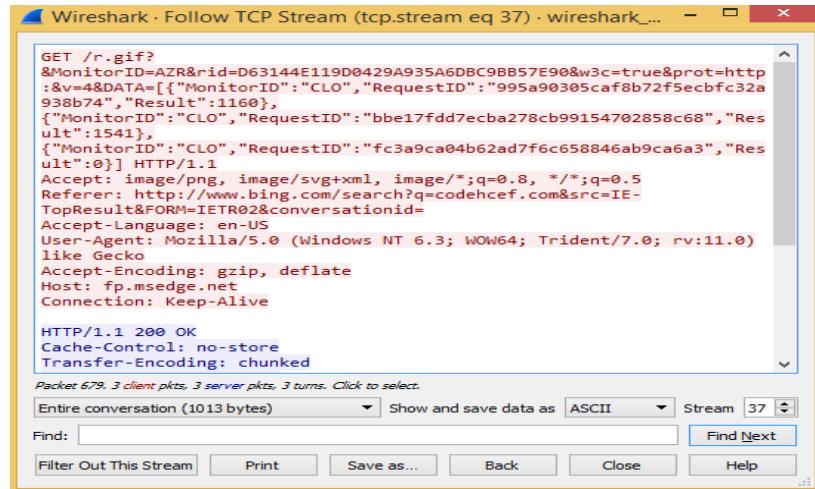
Select A Packet.

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: 0.00000000 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]
```

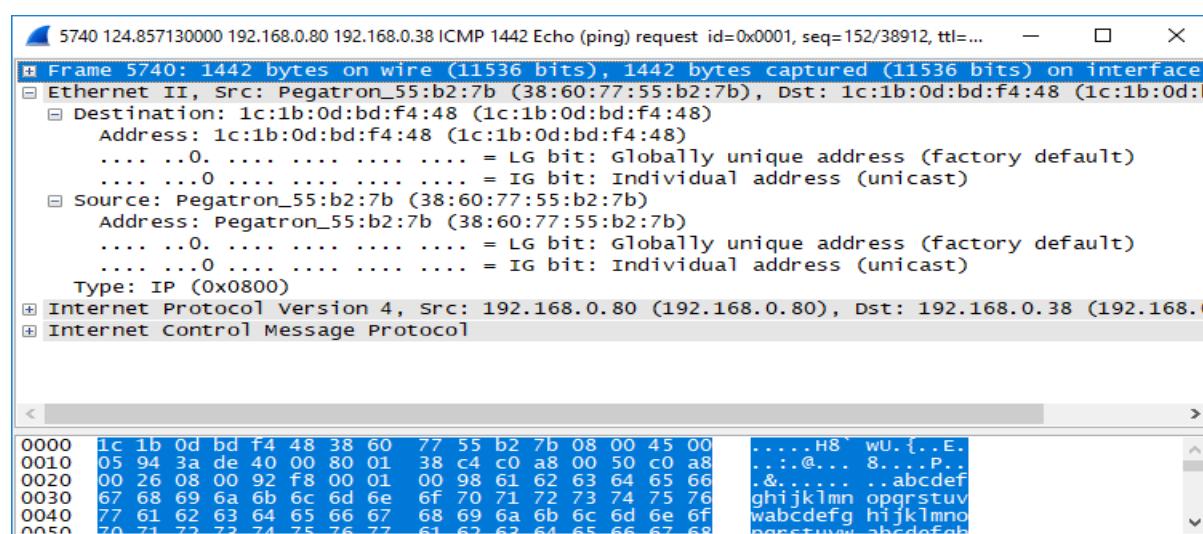
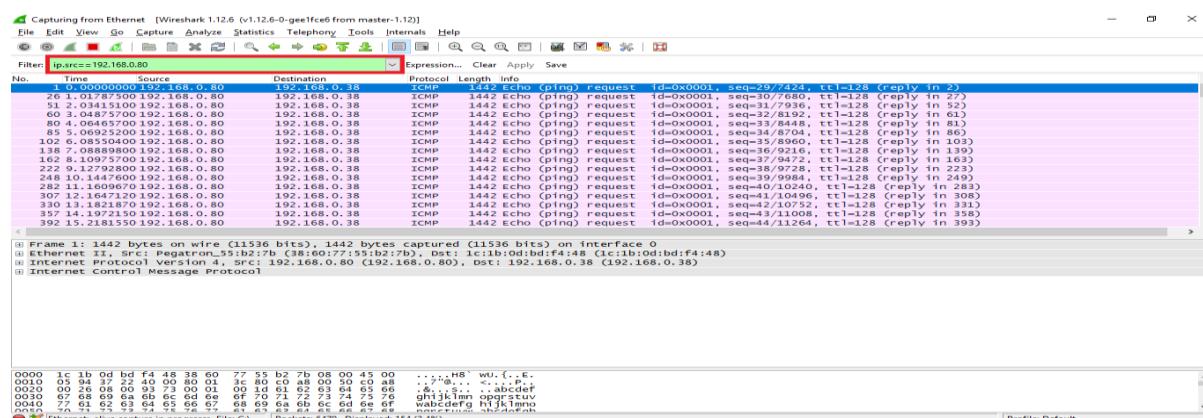
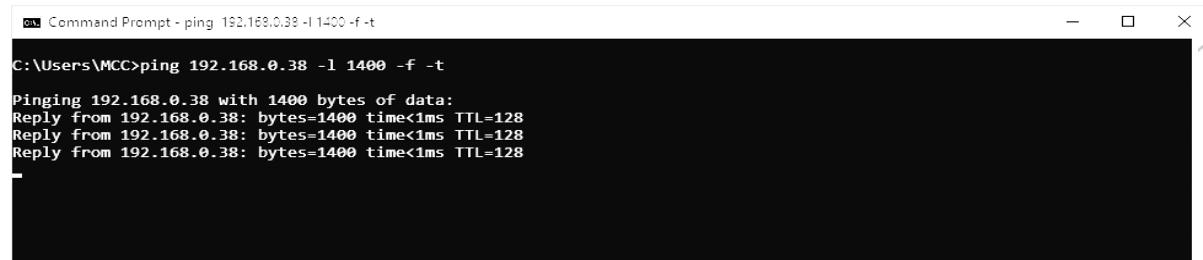
Step-5: Depending On The Analysis More Filters Can Be Added And Inspected.

# 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



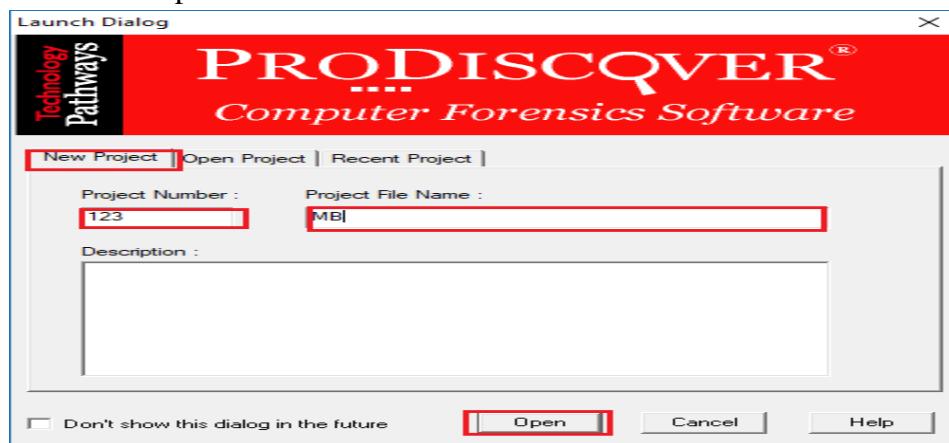
# Practical 6

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.

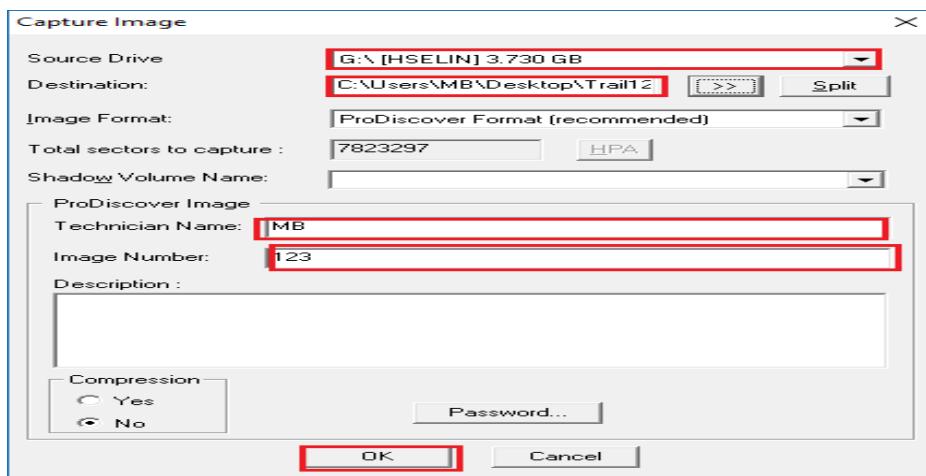


Step-3: To Create An Image For Investigation Purpose,

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.

Select	File Name	File Extension	Size	Attributes	Deleted	Created Date	Modified Date	Accessed Date
	Download			- d - - -	NO	04/27/2018 ...	04/27/2018 ...	04/27/2018
	Apks Backup			- d - - -	YES	04/16/2018 ...	04/16/2018 ...	04/16/2018
	Android			- d - - -	YES	04/16/2018 ...	04/16/2018 ...	04/16/2018
	WhatsApp			- d - - -	YES	04/16/2018 ...	04/16/2018 ...	04/16/2018
	3CIM			- d - - -	YES	04/16/2018 ...	04/16/2018 ...	04/16/2018
	Vufona Proj...			- d - - -	YES	04/16/2018 ...	04/16/2018 ...	04/16/2018
	System Volu...			- d - a h -	NO	05/05/2018 ...	05/05/2018 ...	05/05/2018
	[FreeTutorial...			- d - - -	NO	05/05/2018 ...	05/04/2018 ...	05/05/2018
	3421468_			- d - - -	YES	05/05/2018 ...	05/05/2018 ...	05/05/2018
	[FreeTutorial...			- d - - -	YES	05/09/2018 ...	05/04/2018 ...	05/09/2018
	APK			- d - - -	NO	01/16/2018 ...	01/16/2018 ...	01/16/2018
	Alvir-1.0-OF...	zip	494,864,20...	a - - - -	YES	04/16/2018 ...	04/16/2018 ...	04/16/2018
	8RUMP	APK	18,273,483...	a - - - -	YES	04/23/2018 ...	04/17/2018 ...	04/23/2018
	8ID	APK	28,046,727...	a - - - -	YES	04/23/2018 ...	04/23/2018 ...	04/23/2018
	8ESTVID	APK	28,046,723...	a - - - -	YES	04/23/2018 ...	04/23/2018 ...	04/23/2018
	8ESTVID2	APK	29,708,561...	a - - - -	YES	04/23/2018 ...	04/23/2018 ...	04/23/2018

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

**Evidence Report for Project: MB**

**Project Number:** 123

**Project Description:**

**Image File:**

- File Name: C:\Users\MB\Desktop\Trail123.eve
- Image File Type: DFT Image
- File Number: 123
- Technician Name: MB
- Date: 05/15/2018
- Time: 11:59 AM
- MD5 Checksum: ba086b3d69326be7dca3c001801a5fc
- Checksum Validated: No
- Compressed image: No
- Time Zone Information:

  - Time Zone: (GMT+05:30) Calcutta, Chennai, Mumbai, New Delhi (India Standard Time)
  - Daylight savings (summertime) was in effect: No
  - Time Zone information obtained automatically from remote system/image.

**Hard Disk:** C:\Users\MB\Desktop\Trail123.eve

- Volume Name: NO NAME
- Volume Serial Number : D617-C966
- File System: FAT32
- Bytes Per Sector: 512
- Total Clusters: 975864
- Sectors per cluster: 8
- Total Sectors: 7823297
- Hidden Sectors: 63
- Total Capacity: 3911648 KB
- Start Sector: 0
- End Sector: 7823296

**Disks:**

**Evidence of Interest:**

**Clusters of Interest:**

**File Signature Mismatch:**

# Practical 7

Aim: Using Steganography Tools [S-Tools]

Step-1: Open S-Tools

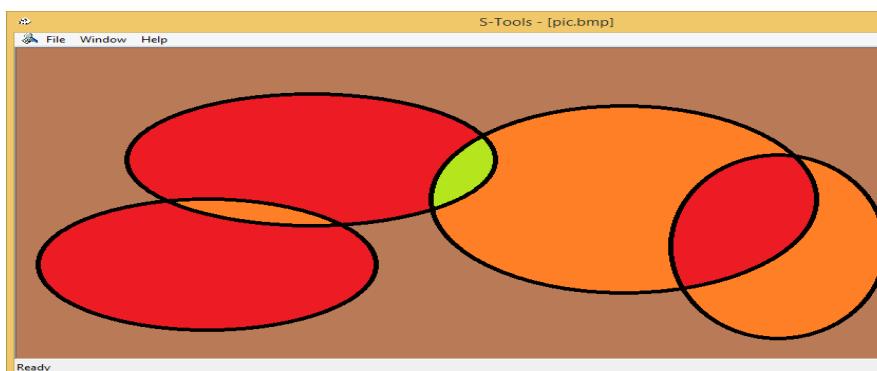
Step-2: Create A .bmp Image File & .txt File

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

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

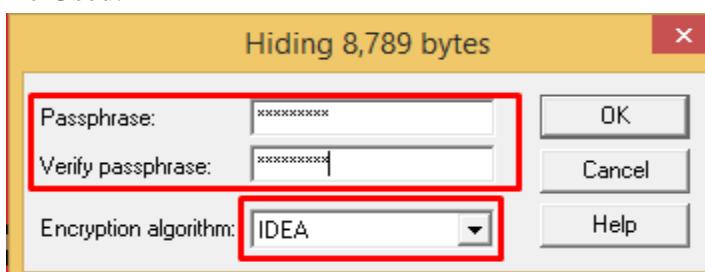
Step-3: Drag & Drop The Two Files (Image & Text)

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.

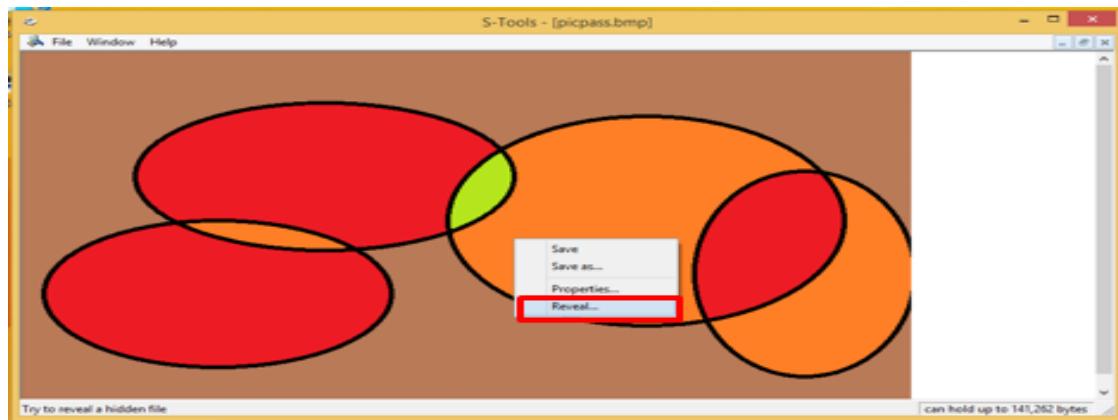


Step-5: Save The Image Into The Desired Location Of Your System.

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.



```
C:\Users\Admin\Desktop>net user ramesh 5star /add
The command completed successfully.
```

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

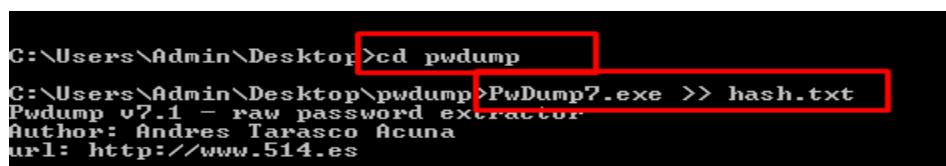
Step-3: Now Navigate To The pwdump Folder Present In Your System.

Type Command,

```
Pwdump7.exe >> hash.txt
```

Pwdump7(We have installed The pwdump 7<sup>th</sup> release)

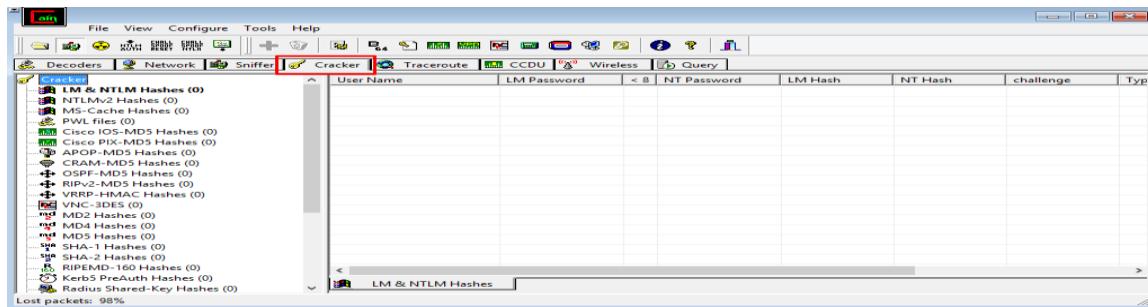
This Will Create The Hashes Of The Passwords Of The User Accounts & Store It In File Named hash.txt In The Same Folder.



```
C:\Users\Admin\Desktop>cd pwdump
C:\Users\Admin\Desktop\pwdump>PwDump7.exe >> hash.txt
PwDump v7.1 - raw password extractor
Author: Andres Tarasco Acuna
url: http://www.514.es
```

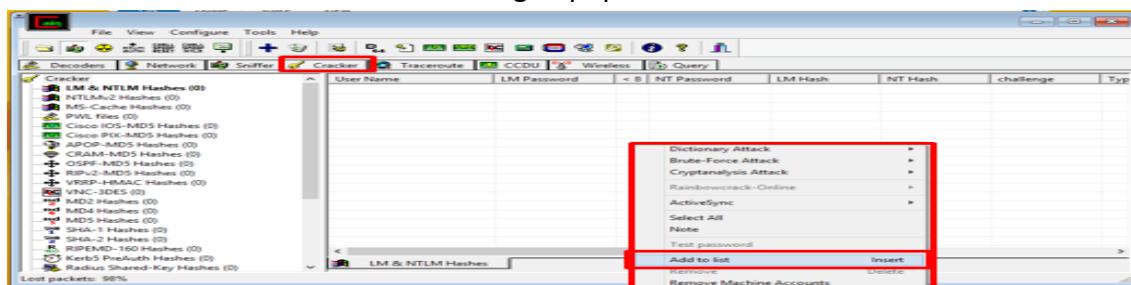
Step-4: Start Cain & Abel As Administrator

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.

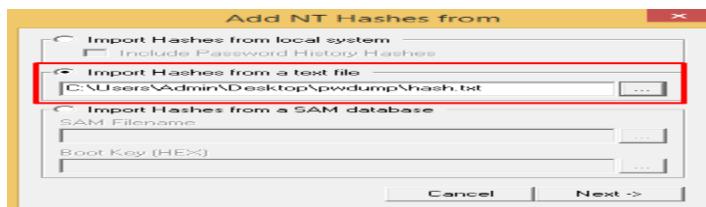


Step-7: In The Resulting Popup,

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.

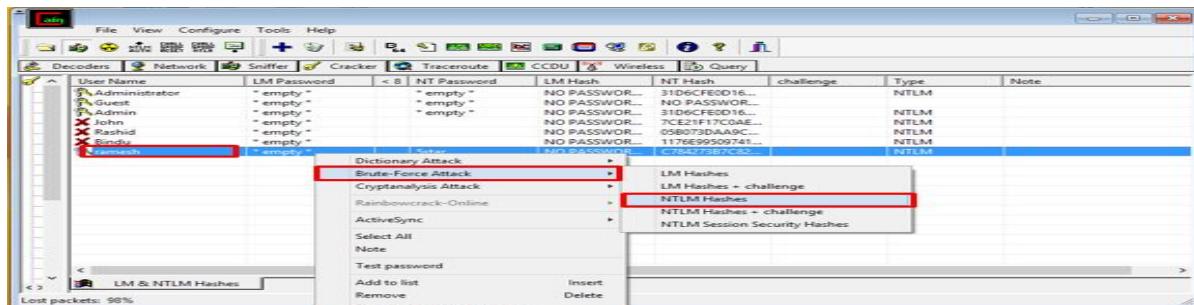
User Name	LM Password	< 8	NT Password	LM Hash	NT Hash	challenge	Type	Note
Administrator	* empty *		* empty *	NO PASSWOR...	31D6CFE0D1...		NTLM	
Guest	* empty *		* empty *	NO PASSWOR...	NO PASSWOR...		NTLM	
Admin	* empty *		* empty *	NO PASSWOR...	31D6CFE0D1...		NTLM	
X John	* empty *			NO PASSWOR...	7CE21F17C0AE...		NTLM	
X Rashid	* empty *			NO PASSWOR...	05B073DAA9C...		NTLM	
X Bindu	* empty *			NO PASSWOR...	1176E99509741...		NTLM	
X ramesh	* empty *			NO PASSWOR...	C784273B7C82...		NTLM	

Step-9: Select An Account,

Right Click On That User Account

Select Brute-Force Attack

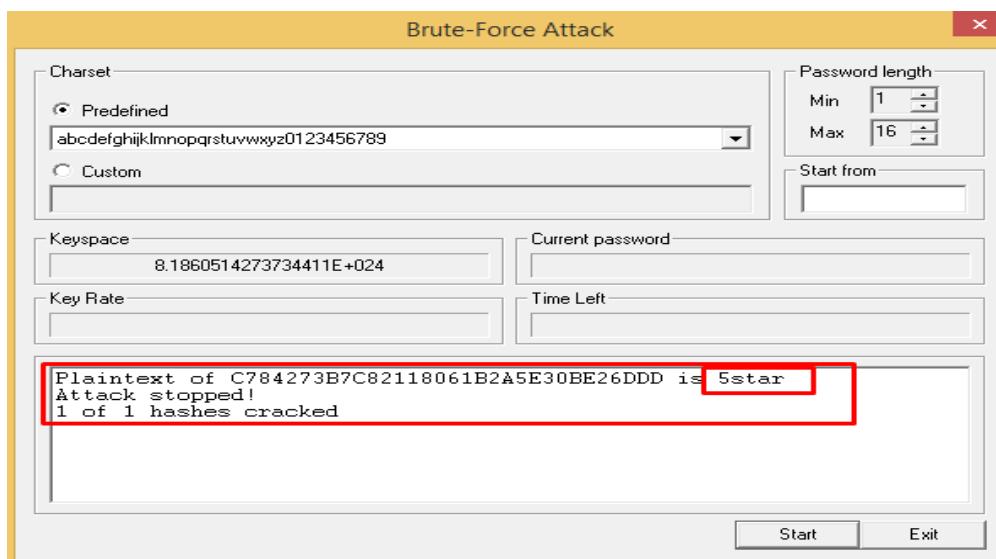
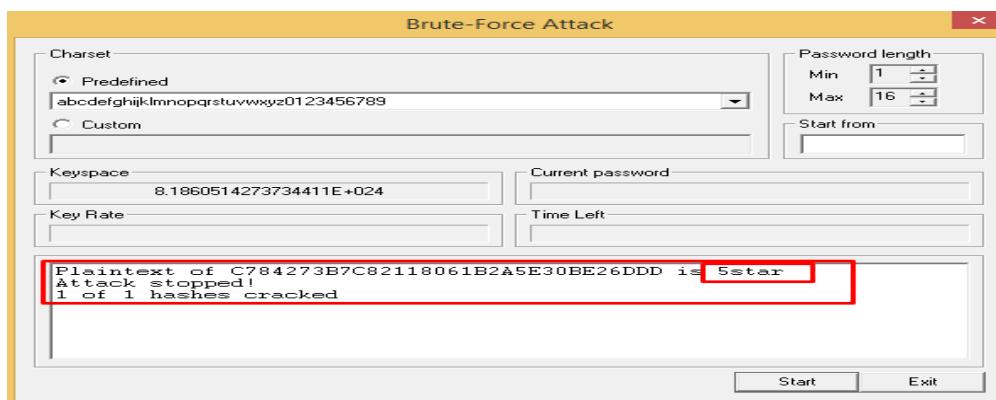
Select NTLM Hashes



#### 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.

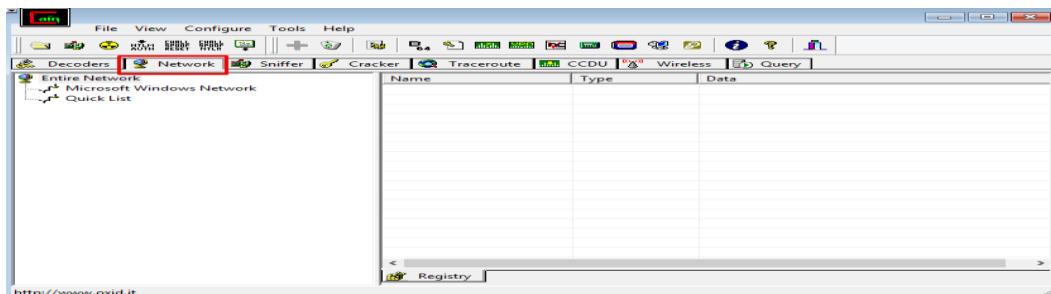


# Practical 9

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

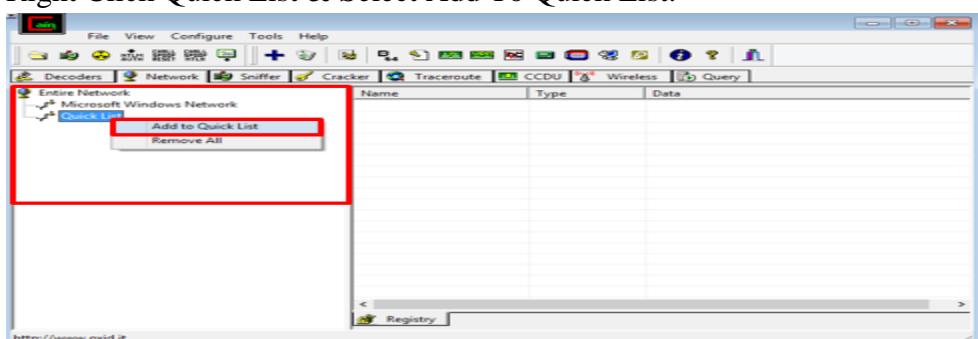
Step-1: Open Cain & Abel As Administrator

Step-2: Go To Network Tab



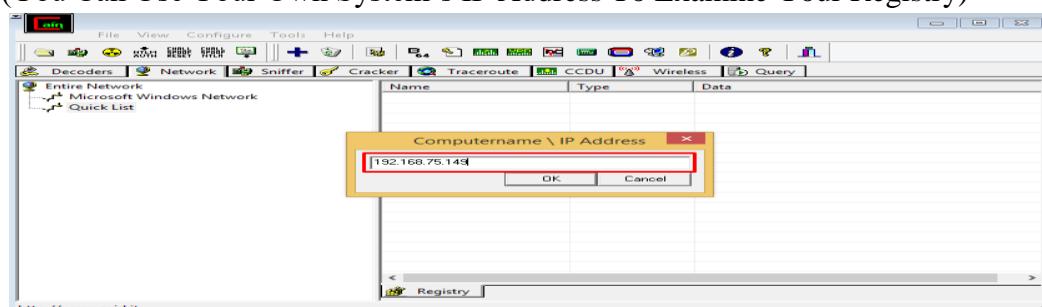
Step-3: Expand Entire Network

Right Click Quick List & Select Add To Quick List.



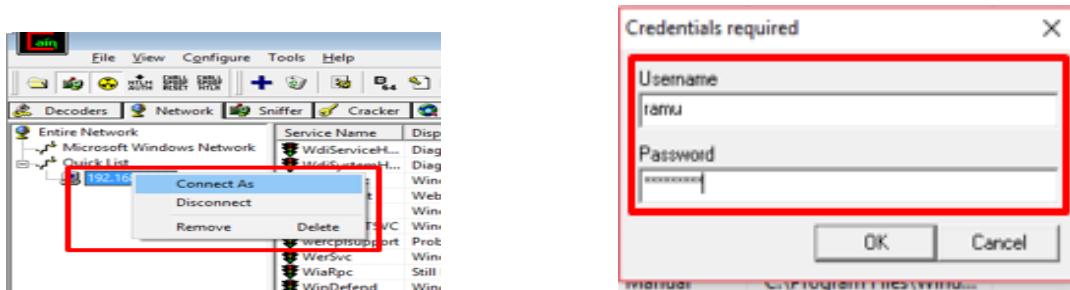
Step-4: In The Resulting Popup Box, Enter The IP Address Of The System You Want To Study

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



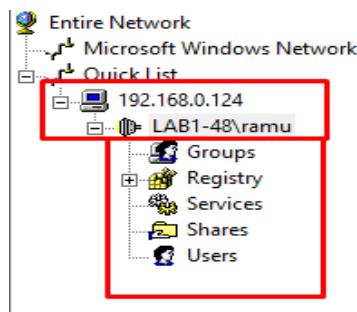
To Access Other System's Registry & Services, Use That System's IP Address

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

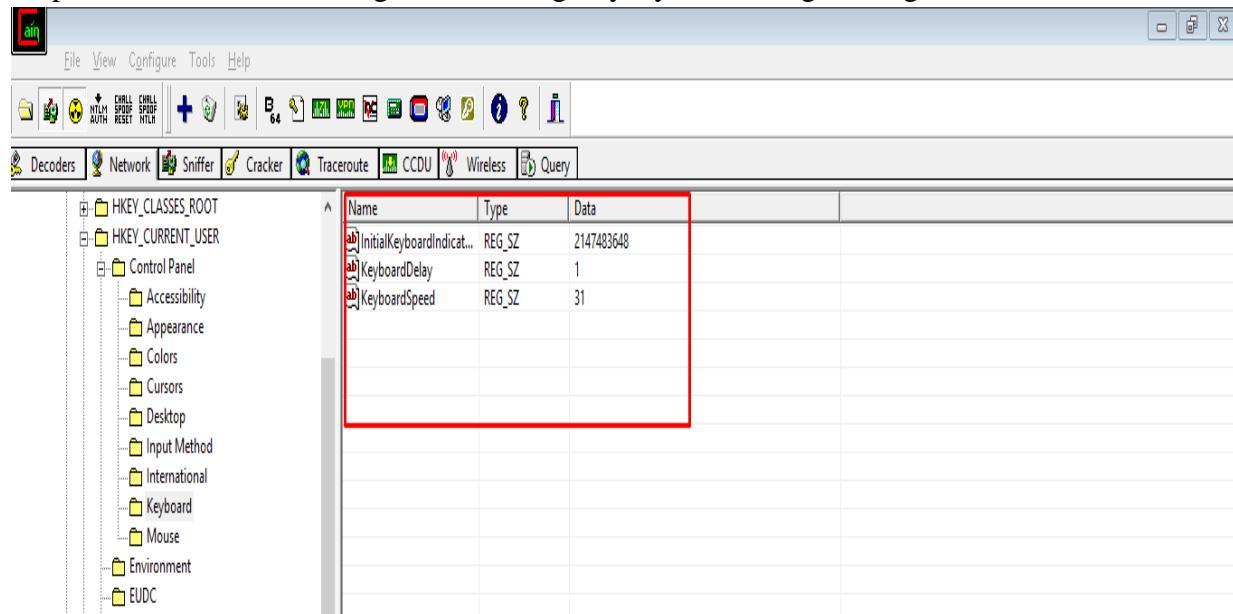


Step-6 Make Sure To Start ‘Remote Registry’ Service In Both The PCs,

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.

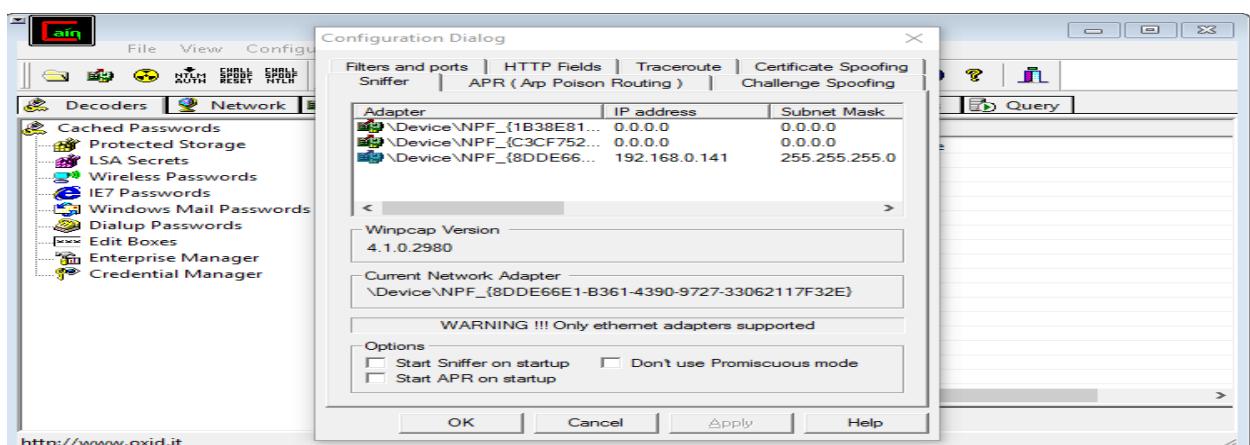
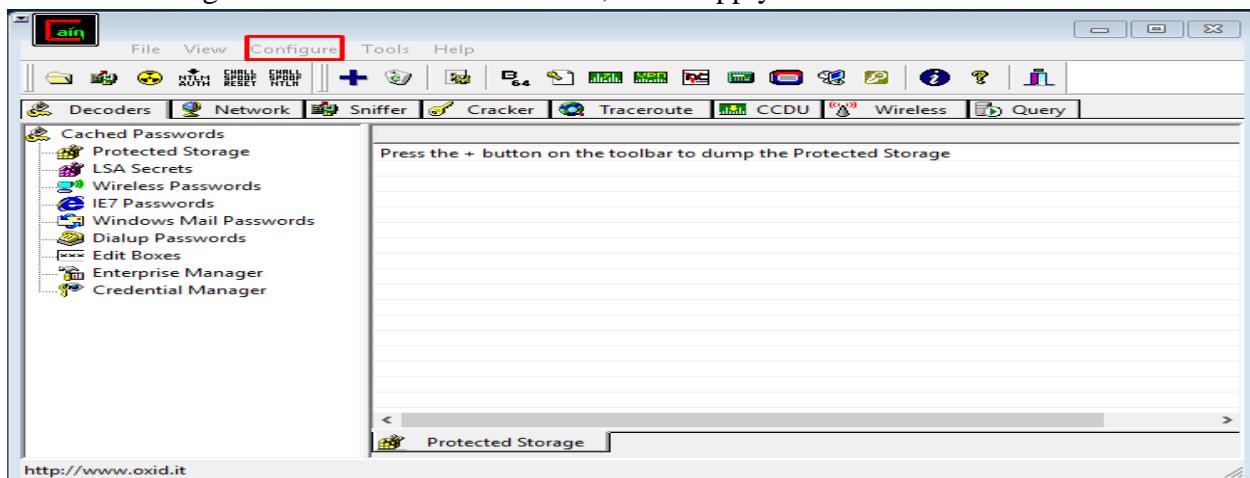
# Practical 10

Aim: Performing Sniffing [Cain & Abel]

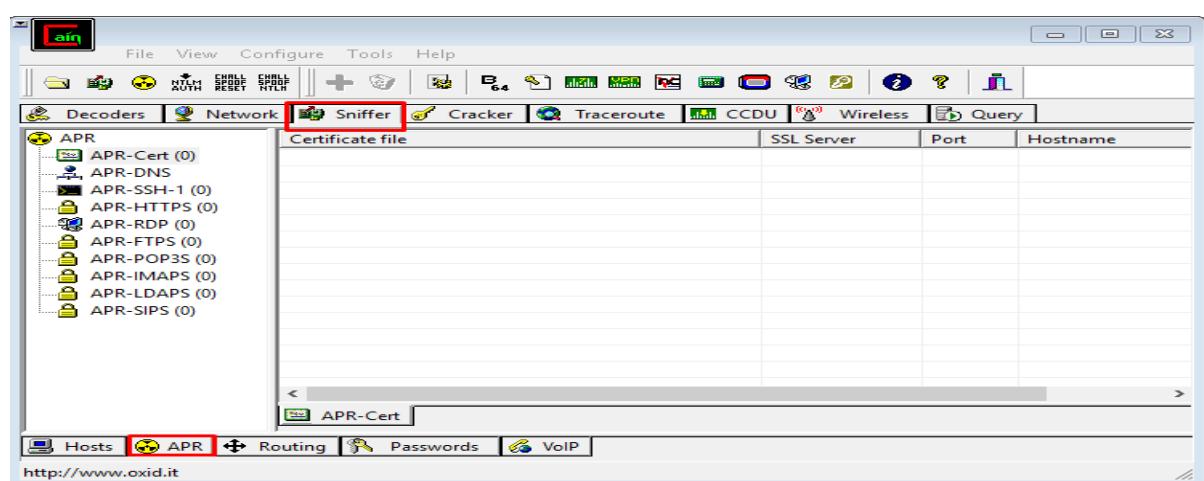
Steps : (Note : Go to command prompt & type ipconfig & note down your IP Address.)

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

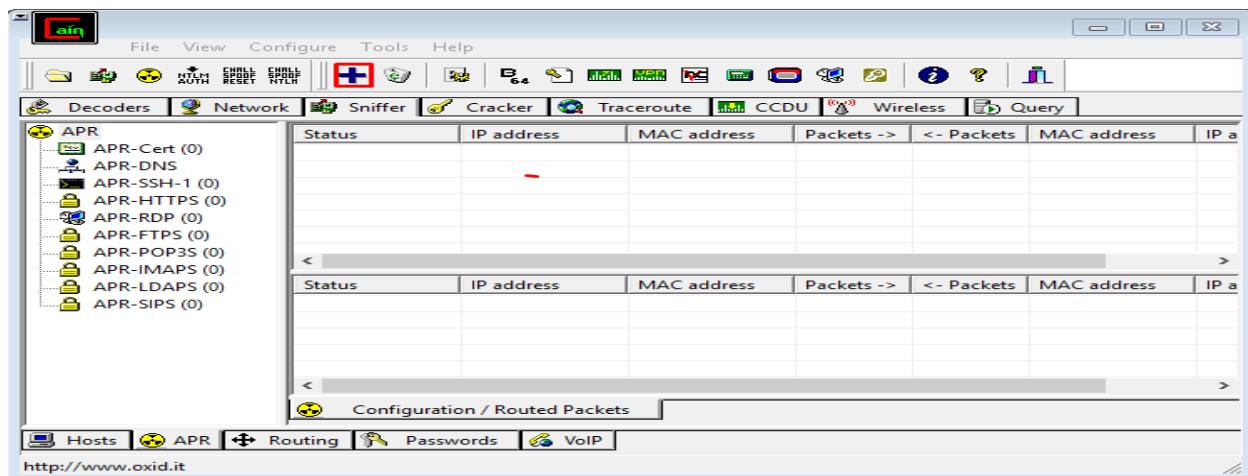
2. Go To Configure & Select Your IP Address, Press Apply & OK.



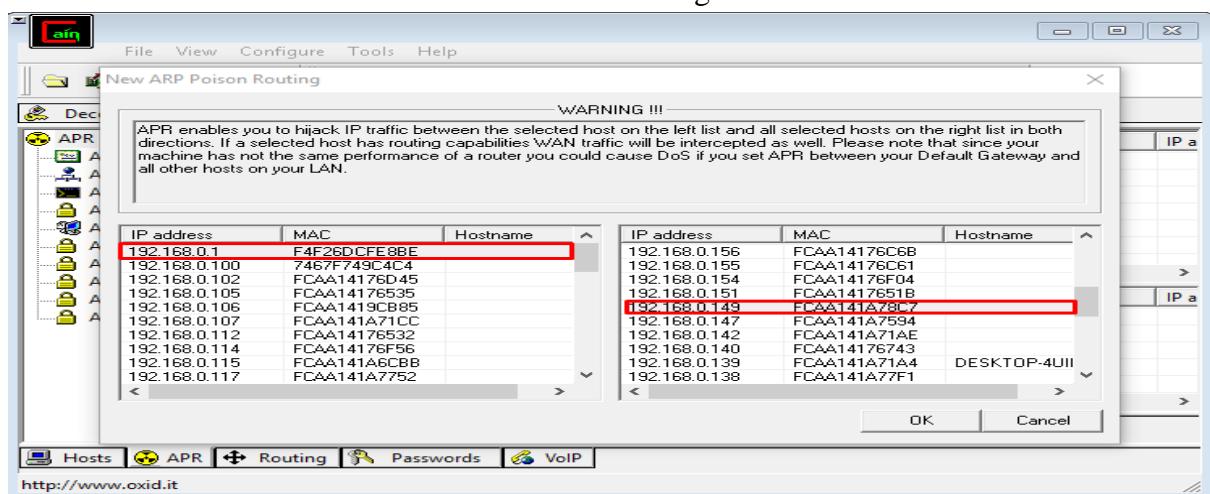
3. Now Go To Sniffer Tab On Top & Select APR Tab From Bottom.



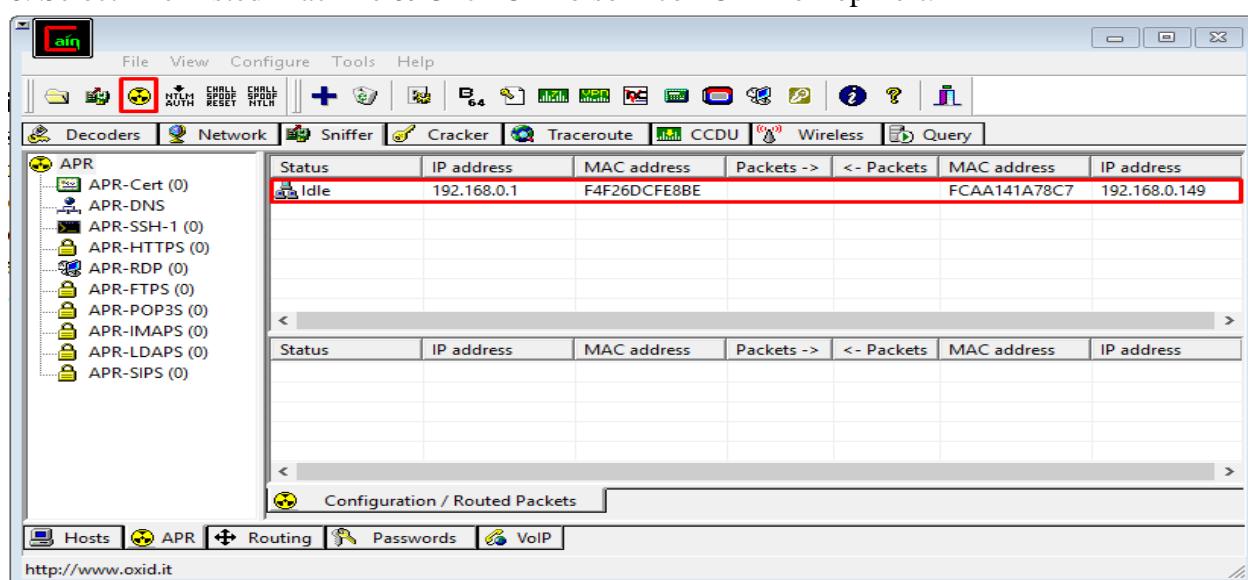
4. Single Click On The Right Above Part Of APR And Then Click On "+" Icon On Top Left.



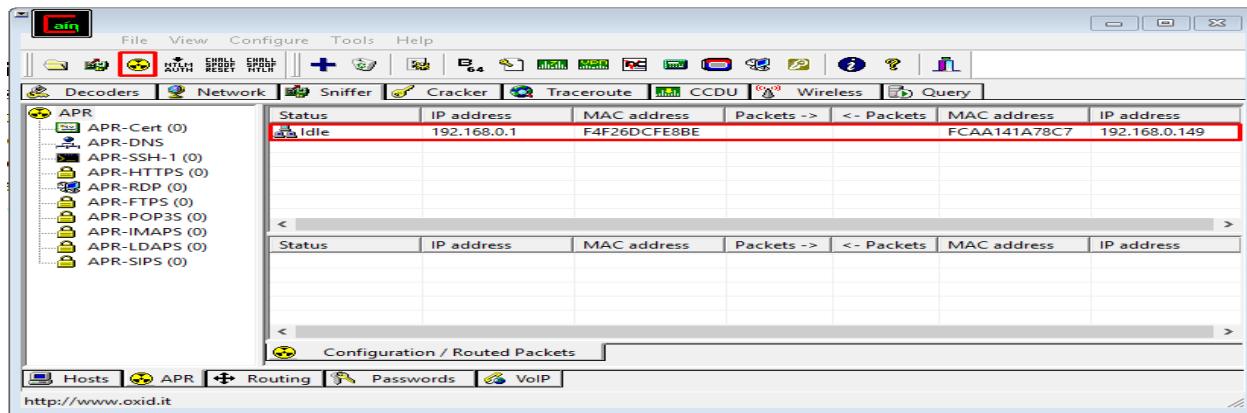
5. Now Select Your Subnet & Machine With The Target IP Address & Press OK.



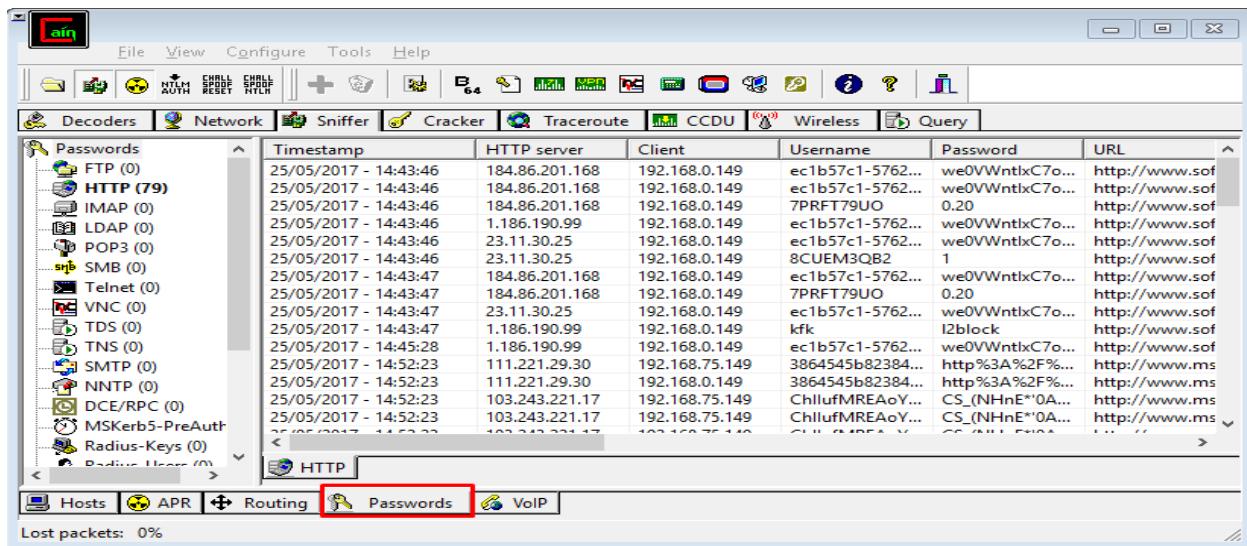
6. Select The Listed Machine & Click On Poison Icon On The Top Left.



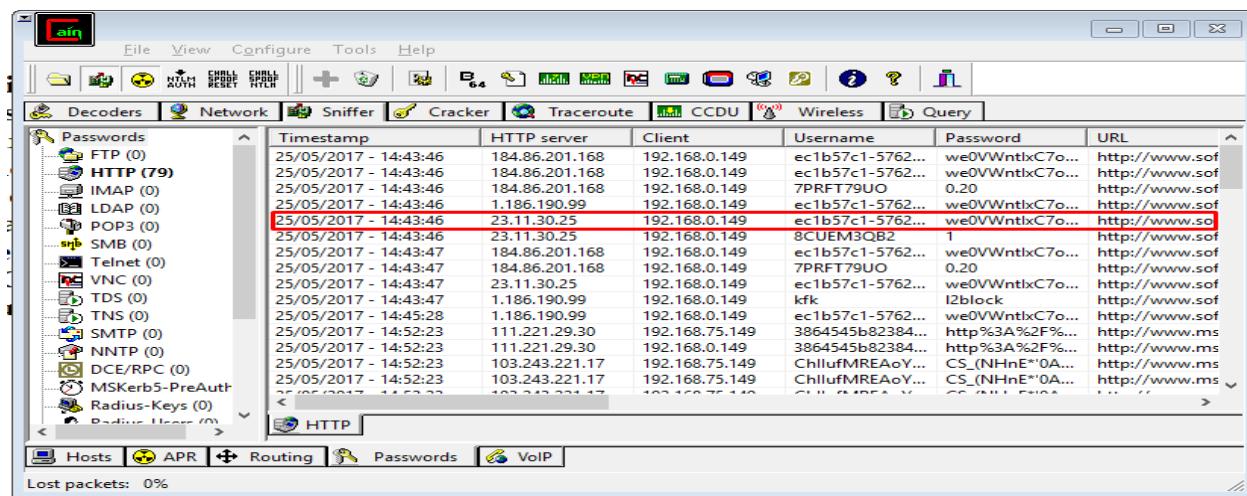
(Note : If You Get AN Exception : "Couldn't bind HTTPS acceptor socket", Press OK)



## 7. Go To Passwords Tab At The Bottom.



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



# Practical No. 11

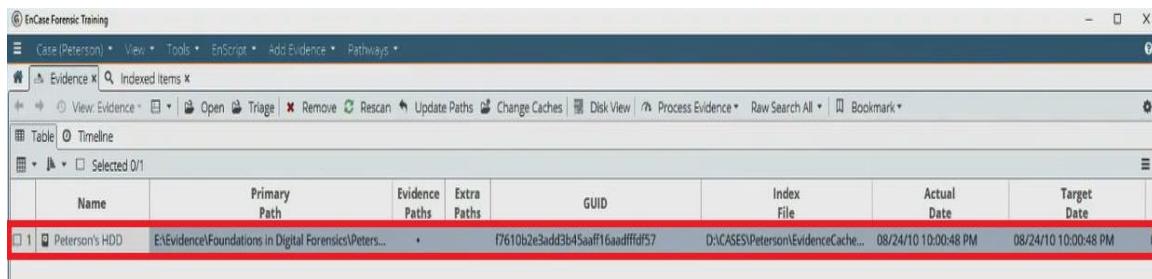
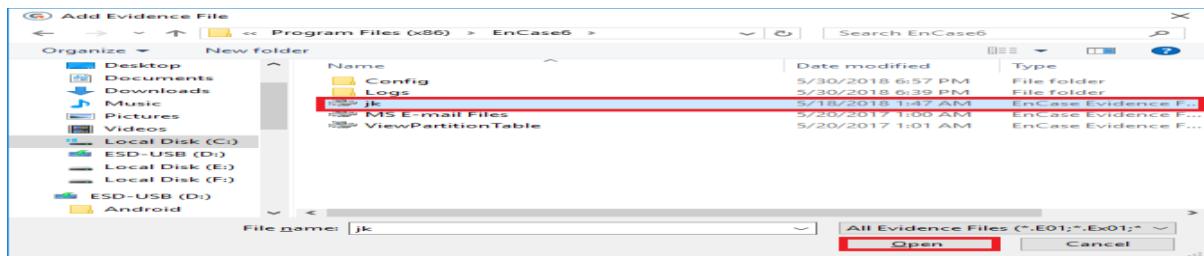
Forensics Investigation Using EnCase  
Aim: Exploring EnCase

The image consists of three vertically stacked screenshots of the EnCase Forensic software interface.

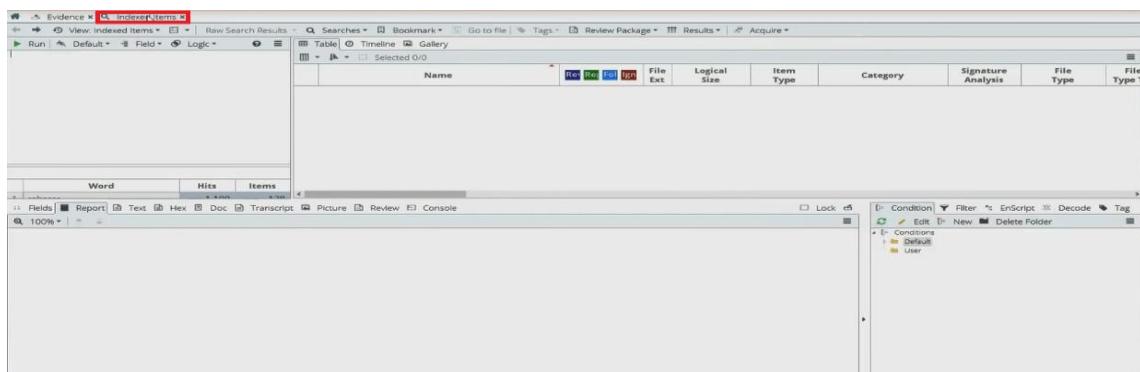
**Screenshot 1: Case Creation**  
The main window shows the "EnCase® Forensic" logo. The "Case File" menu is open, displaying "New Case" and "Open". The "Help" menu is also open, showing "Help", "Activate Electronic License", and "About". A modal dialog box titled "Options" is displayed, containing fields for "Name and location" (Name: "Case 1", Full case path: "C:\Users\Admin\AppData\Local\Temp\Case 1\Case 1.Case") and "Evidence cache locations" (Primary evidence cache: "C:\Users\Admin\AppData\Local\Temp\Case 1\EvidenceCache"). The "OK" button is highlighted with a red box.

**Screenshot 2: Main Window**  
The main window title bar reads "Case (Case 1)". The menu bar includes "Case (Case 1)", "View", "Tools", "EnScript", and "Add Evidence". The left sidebar has "Browse" (Evidence), "Evidence" (Add Evidence highlighted with a red box), and "Case" (Close). The bottom status bar shows "Case 1".

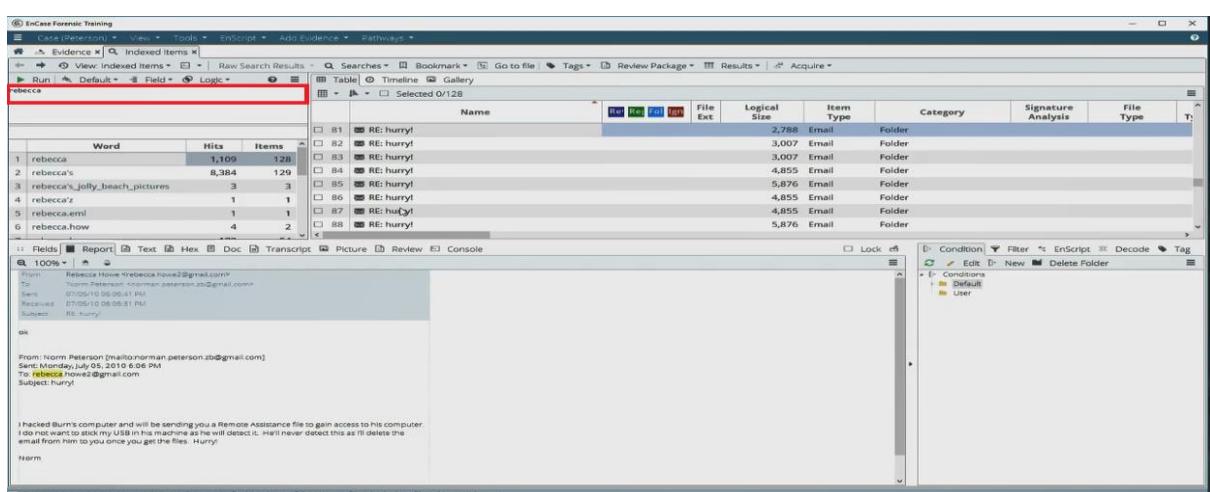
**Screenshot 3: Add Evidence Dialog**  
A modal dialog box titled "Add Evidence" is shown. The "File" section contains options: "Add Local Device", "Add Network Preview", "Add Evidence File" (highlighted with a red box), "Add Raw Image", and "Add Crossover Preview". Below this is a section for "Acquire Smartphone". The bottom status bar shows "Case 1".



## Navigate to Indexed Items



Searching keyword e.g. "Rebecca" and press Enter Key



Now click on last written

Search Results for 'Last\_Written'

Word	Hits	Items
1 rebecca	100	100
2 rebeccas	2	2
3 rebeccas...	2	2
4 rebeccas...	1	1
5 rebeccal...	1	1
6 zoom...	1	1
7 zoom...	2	2

Results Table:

Name	File Ext	Logical Size	Item Type	Category	Signature Analysis	File Type
102 RE: Orlando Conference	eml	9,253	Email	Folder	Match	Text
103 RE: Orlando Conference	eml	4,762	Email	Folder	Match	Text
104 RE: Orlando Conference	eml	3,449	Email	Folder	Match	Text
105 RE: Orlando Conference	eml	3,097	Email	Folder	Match	Text
106 RE: reminder	eml	4,134	Email	Folder	Match	Text
107 RE: passport	eml	4,134	Email	Folder	Match	Text
108 RE: reminder	eml	4,134	Email	Folder	Match	Text
109 RE: reminder	eml	4,134	Email	Folder	Match	Text

Last\_written [20100624 TO 20100705]

i.e. last\_written [yyyyymmdd To yyyyymmdd] where y is year and m is month and d is day

Search Results for 'Last\_Written'

Word	Hits	Items
1 20100705...	1	1
2 20100705032356...	2	2
3 20100705032356...	2	2
4 20100705073016...	2	2
5 20100705073016...	1	1

Results Table:

Name	File Ext	Logical Size	Item Type	Category	Signature Analysis	File Type
104-3 UPnP Device Host	txt	1	Text	Folder	Unknown	Text
943 URN:uuid:...	cab	384	Entry	Folder	Unknown	Unknown
944 URN:uuid:...	cab	160	Entry	Folder	Unknown	Unknown
945 URN:uuid:...	cab	256	Entry	Folder	Match	Dynamic Link Lib...
946 URN:uuid:...	cab	863	Entry	None	Unknown	Unknown
947 URN:uuid:...	dll	1,226,240	Entry	Library	Match	Dynamic Link Lib...
948 URN:uuid:...	cab	1,226,240	Entry	Library	Match	Dynamic Link Lib...
949 URN:uuid:...	cab	1,226,240	Entry	Library	Match	Dynamic Link Lib...
950 URN:uuid:...	PNF	24,296	Entry	Windows	Match	Windows Preco...

Now lets try Logical Size

Search Results for 'Logical Size'

Word	Hits	Items
1 20100705...	1	1
2 20100705032356...	2	2
3 20100705073016...	2	2
4 20100705073016...	1	1
5 20100705073016...	1	1

Results Table:

Name	File Ext	Logical Size	Item Type	Category	Signature Analysis	File Type
943 UPnP Device Host	txt	384	Entry	Folder	Unknown	Text
944 URN:uuid:...	cab	160	Entry	Folder	Unknown	Unknown
945 URN:uuid:...	cab	256	Entry	Folder	Match	Dynamic Link Lib...
946 URN:uuid:...	cab	863	Entry	None	Unknown	Unknown
947 URN:uuid:...	dll	1,226,240	Entry	Library	Match	Dynamic Link Lib...
948 URN:uuid:...	cab	1,226,240	Entry	Library	Match	Dynamic Link Lib...
949 URN:uuid:...	cab	1,226,240	Entry	Library	Match	Dynamic Link Lib...
950 URN:uuid:...	PNF	24,296	Entry	Windows	Match	Windows Preco...

Logical\_size: [18000000 TO 10000000]

Search Results for 'Logical\_size: [18000000 TO 10000000]'

Word	Hits	Items
1 00000000...	15	15
2 0000000000...	3	3
3 0000000000...	9	9
4 0000000000...	14	12
5 0000000000...	8	8

Results Table:

Name	File Ext	Logical Size	Item Type	Category	Signature Analysis	File Type
70 Wildfire.wmv	wmv	26,246,026	Entry	Multimedia	Match	Windows Medi...
71 Wildfire.wmv	wmv	26,246,026	Entry	Multimedia	Match	Windows Medi...
72 Wildfire.wmv	wmv	26,246,026	Entry	Multimedia	Match	Windows Medi...
73 WordArt.cab	cab	42,008,976	Entry	Archive	Match	Microsoft Com...
74 WordArt.cab	cab	43,803,555	Entry	Archive	Match	Microsoft Com...
75 WordArt.cab	cab	21,663,376	Entry	Library	Match	Dynamic Link Lib...
76 xbl.microsoft-windows-f.e-microsofthighghe...	inf	23,805,700	Entry	Font	Match	True Type Font
77 xbl.microsoft-windows-font-truetype-mingl...	ttc	23,805,700	Entry	Font	Match	True Type Font

Now checking data on an File

File Details for 'C:\DOC\DWAT\Code\bolly.jpg'

Word	Hits	Items
1 file	295,856	101,222
2 file/resource	2	2
3 file/a	73	29
4 file.a	1	1
5 file.acceskey	1	1
6 file.acrobat	10	1

File Properties:

- File Path: C:\DOC\DWAT\Code\bolly.jpg
- File Type: Picture
- File Size: 29,864,400
- Logical Size: 29,864,400
- Item Type: Unknown
- Category: Archive
- Signature Analysis: Bad signature
- File Type: Microsoft Com... cab

# Practical No. 12

Using Mobile Forensics software tools

Aim: Exploring MobiEdit Forensics

