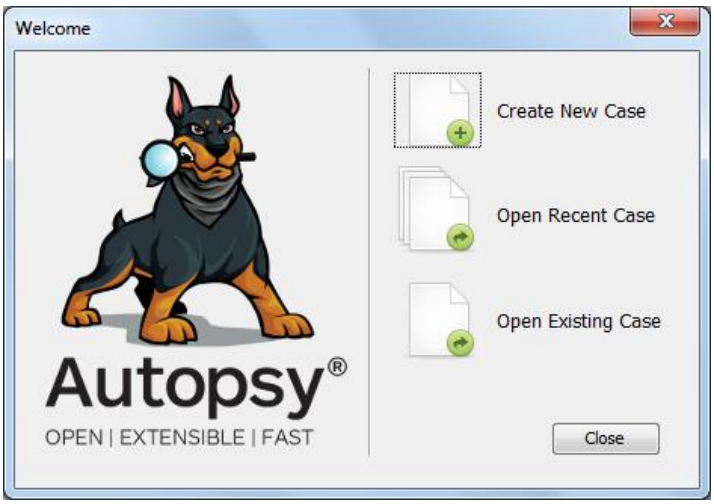
Index

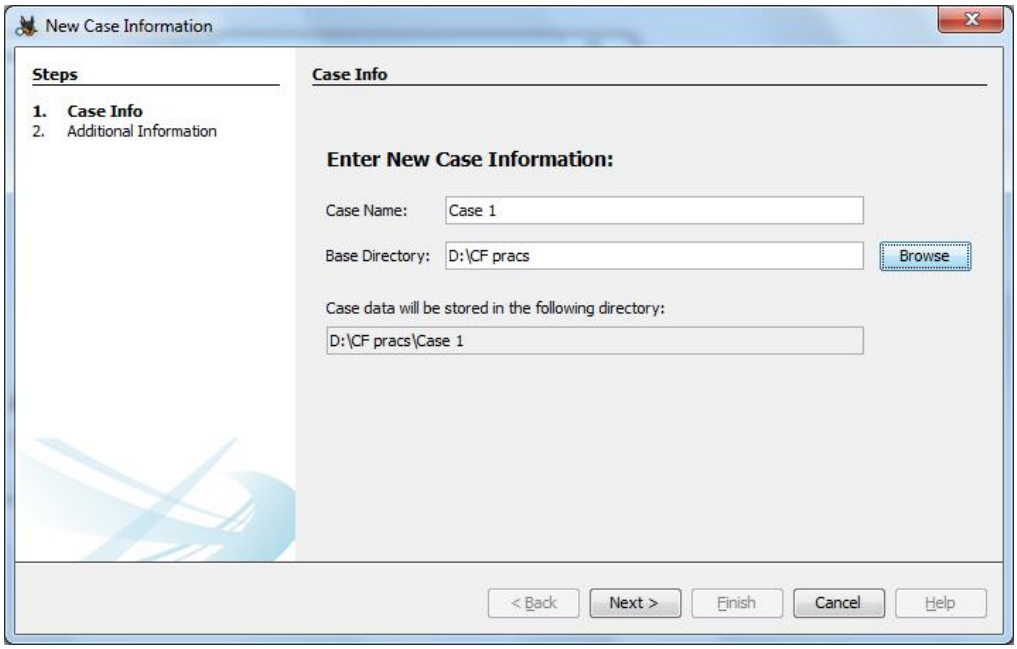
Practical No: 01

How to Start a Case.

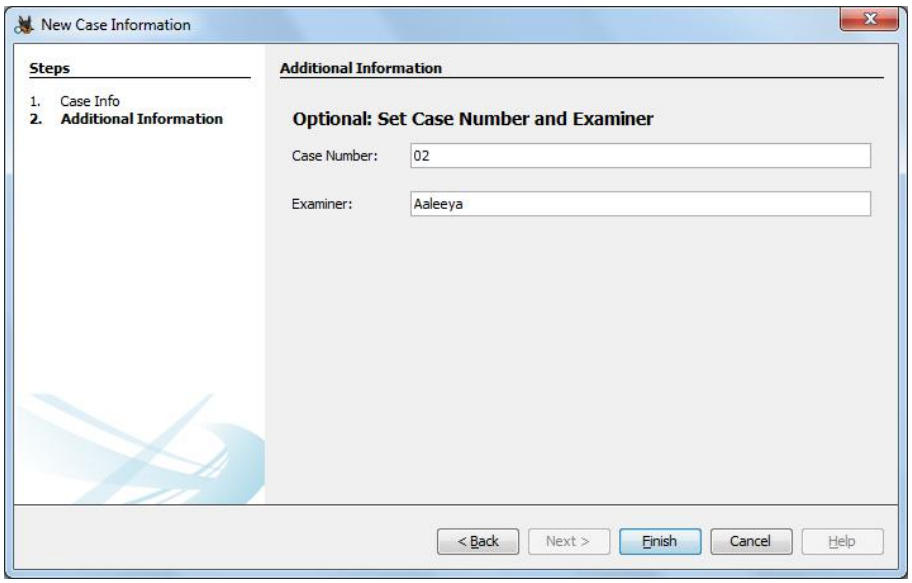
Upon starting Autopsy 3.1.2, a window will open with three selections to make: create a new case, open existing case, or to open a recent case.



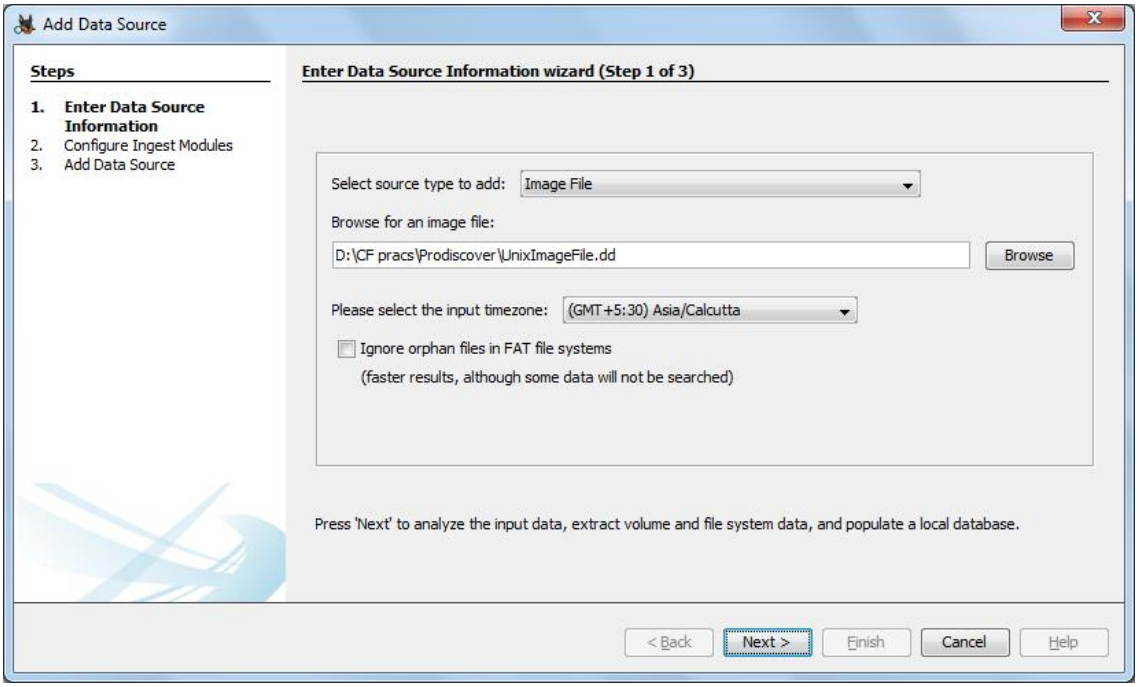
Step 1) Select the "Create New Case" option and be directed to a new window that will have information to fill in, we will be naming the case "Test."



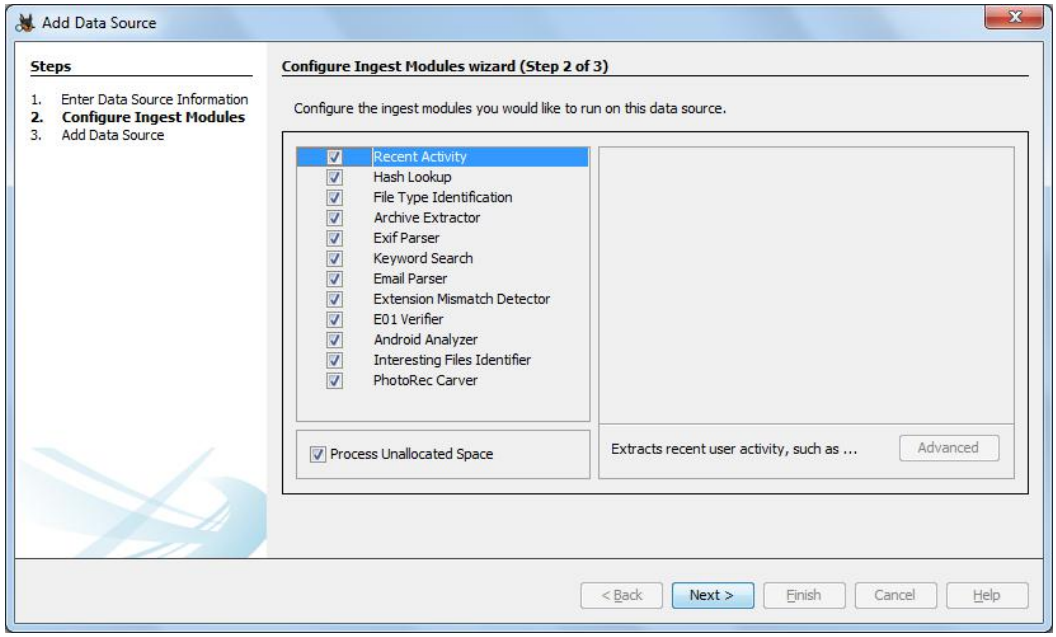
Step 2) After the information has been filled in select the next button. The next window will allow the investigator to fill in the case number and examiner name. This is for the purpose of creating better documentation and logging. After the information is filled in select the finish button to continue.



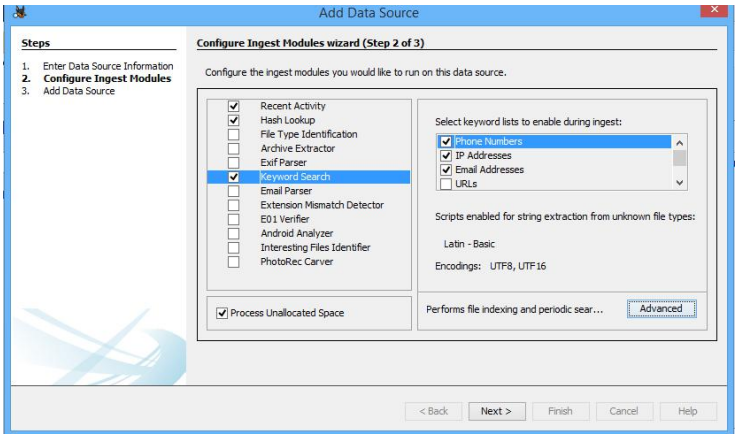
Step 3) The next step in the investigation will be to add an image file to the case. The image file can be chosen from a wide variety of formats including: img, dd, 001, aa, and e01. Use the browse button to find the image that is desired to work with and select add. Options to choose the timezone of where the image came from as well as to ignore orphan files in FAT file systems are available to be selected based on the investigators preference and situation.



Step 4) After selecting the next button the image will be added to the case and the next button should be selected again if there are no errors.

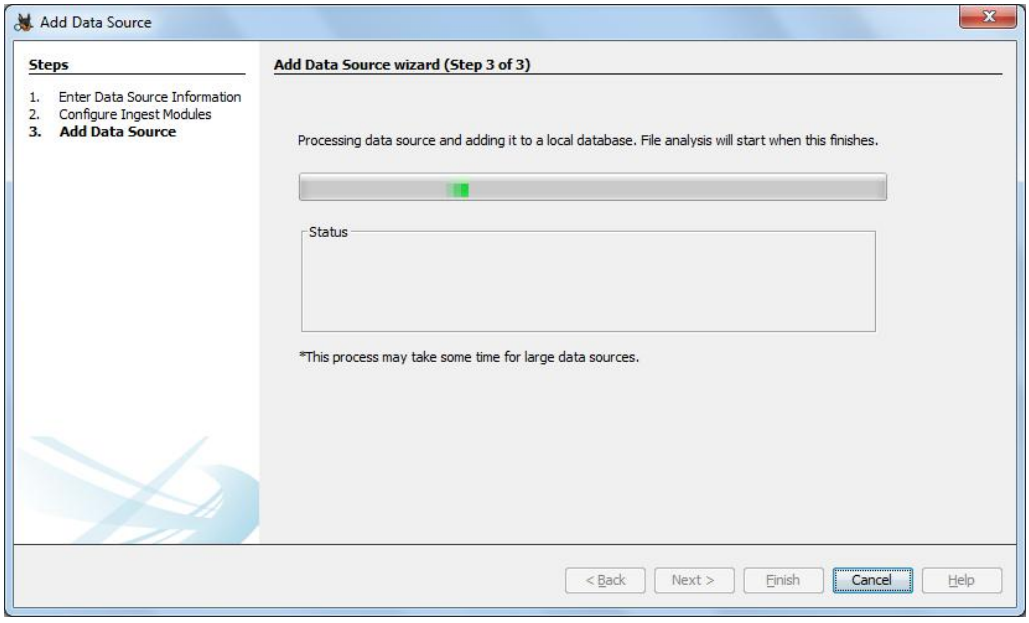


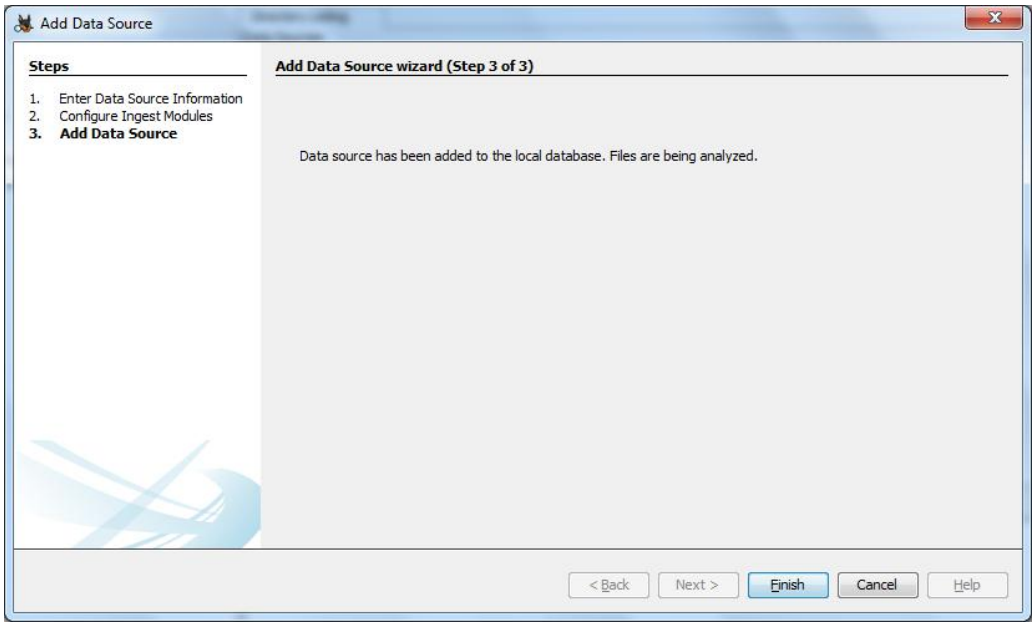
Step 5) The following window will bring the investigator to the Ingest wizard panel, which is one of the new features offered in Autopsy. There are three options in the first box: Recent Activity, Hash lookup, and Keyword Searches.

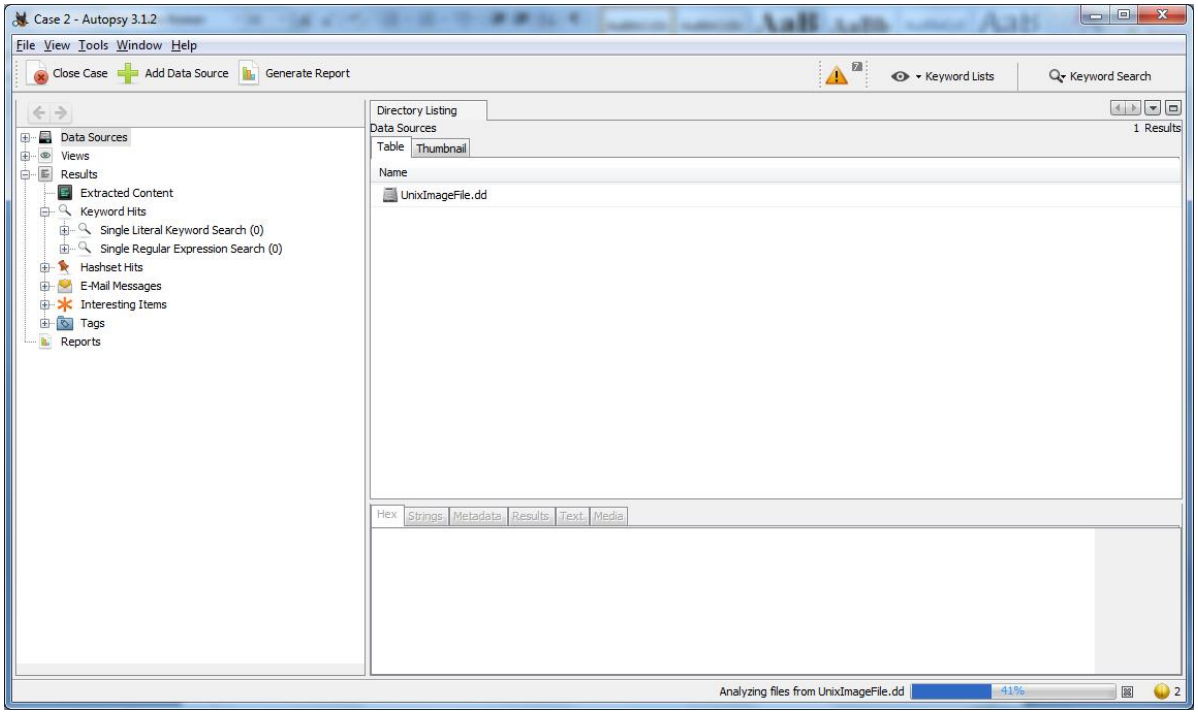


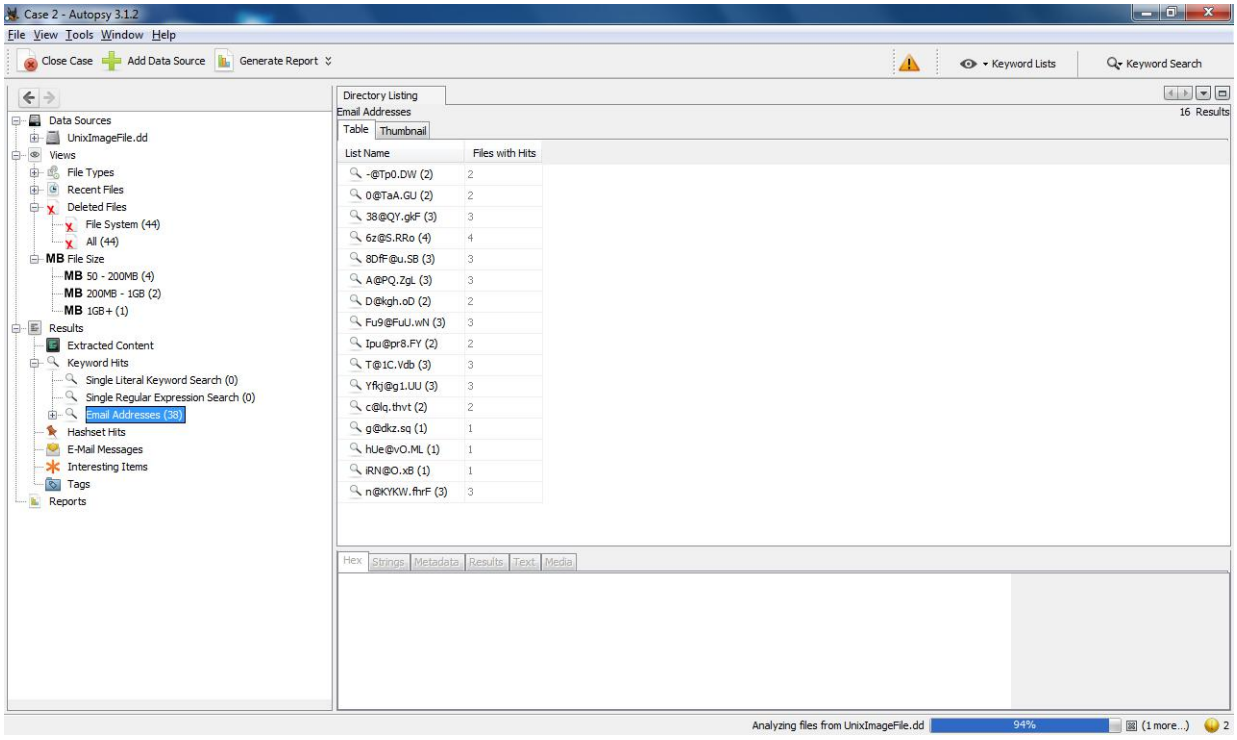
By selecting any of the options advanced settings can be set to increase the capabilities of the search. Under the Hash Lookup option there is the advanced option to add databases of known hashes.

Under the Keyword Search option are many different lists that can be used to search for information. By default, Phone Numbers, IP Addresses, Email Addresses, and URL's are available. Select the Advanced button and a Keyword List Configuration window will open. In this new window select New List and type the name that is desired for the list. This makes it easier to search by subject matter or other organizational methods. For now the list Test keywords will be used to create a list. In the adjacent pane there is a blank section with a word bar and an Add button next to it. Type the keyword desired (case sensitive) and select Add to add the word to the list. There is also the option to select Regular Expression. This allows the investigator to further narrow the field to search in by selecting what the keyword is that is being searched for including: passwords, emails, text file name, domains, and many more options.

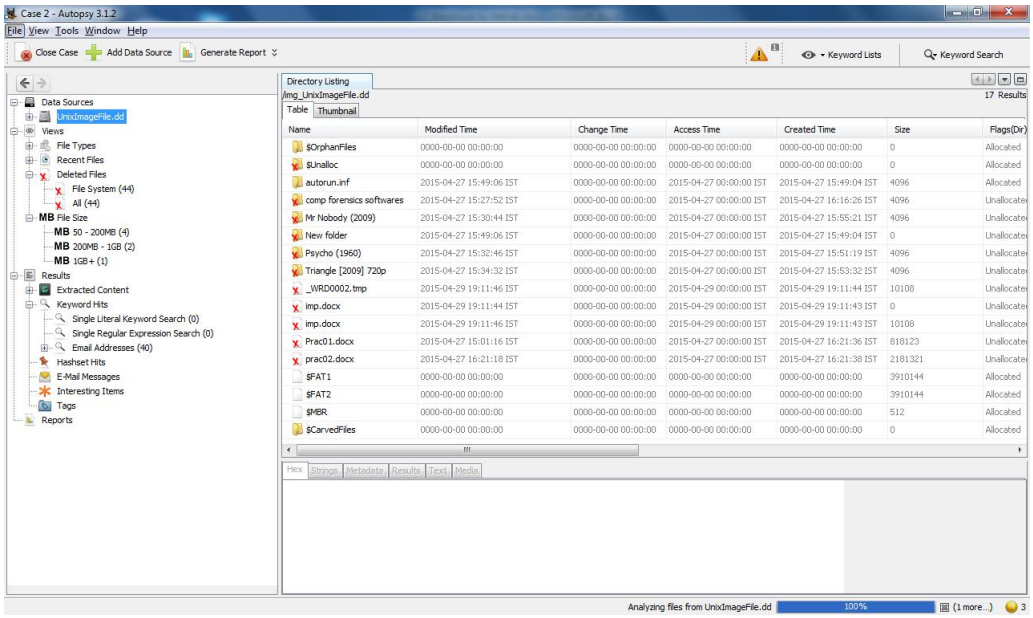

Add Data Source
Steps
1. Enter Data Source Information
2. Configure Ingest Modules
3. Add Data Source
Add Data Source wizard (Step 3 of 3)
Processing data source and adding it to a local database. File analysis will start when this finishes.
Status
*This process may take some time for large data sources.
< Back
Next >
Finish
Cancel
Help


Add Data Source
Steps
1. Enter Data Source Information
2. Configure Ingest Modules
3. Add Data Source
Add Data Source wizard (Step 3 of 3)
Data source has been added to the local database. Files are being analyzed.
< Back
Next >
Finish
Cancel
Help

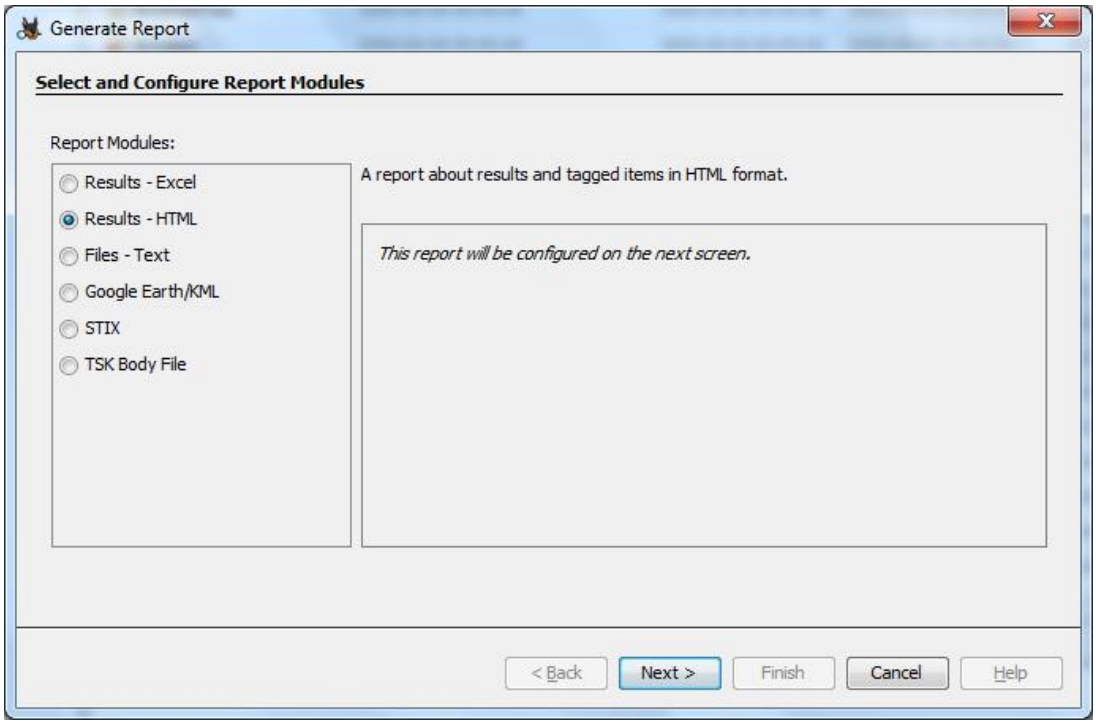

Case 2 - Autopsy 3.1.2
File View Tools Window Help
Close Case
Add Data Source
Generate Report
Keyword Lists
Keyword Search
Data Sources
Views
Results
Extracted Content
Keyword Hits
Single Literal Keyword Search (0)
Single Regular Expression Search (0)
Hashset Hits
E-Mail Messages
Interesting Items
Tags
Reports
Directory Listing
Data Sources
1 Results
Table
Thumbnail
Name
UnixImageFile.dd
Hex
Strings
Metadata
Results
Text
Media
Analyzing files from UnixImageFile.dd
41%

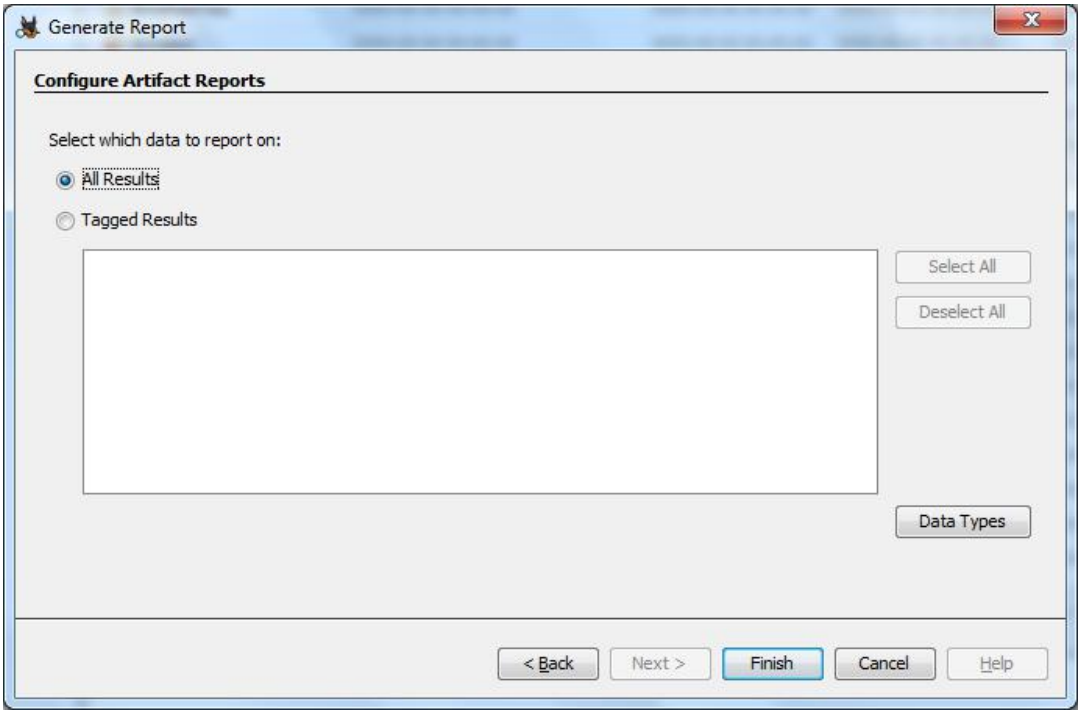

Case 2 - Autopsy 3.1.2
File View Tools Window Help
Close Case
Add Data Source
Generate Report
Keyword Lists
Keyword Search
Data Sources
UnixImageFile.dd
Views
File Types
Recent Files
Deleted Files
File System (44)
All (44)
File Size
50 - 200MB (4)
200MB - 1GB (2)
1GB+ (1)
Results
Extracted Content
Keyword Hits
Single Literal Keyword Search (0)
Single Regular Expression Search (0)
Email Addresses (38)
Hashset Hits
E-Mail Messages
Interesting Items
Tags
Reports
Directory Listing
Email Addresses
16 Results
Table
Thumbnail
List Name
Files with Hits
-@Tp0.DW (2) 2
0@TaA.GU (2) 2
38@QY.gkF (3) 3
6z@S.RRo (4) 4
8DfF@u.SB (3) 3
A@PQ.ZgL (3) 3
D@kgh.oD (2) 2
Fu9@FuU.wN (3) 3
Ipu@pr8.FY (2) 2
T@1C.Vdb (3) 3
Yfkj@g1.UU (3) 3
c@lq.thvt (2) 2
g@dkz.sq (1) 1
hUe@vO.ML (1) 1
iRN@O.xB (1) 1
n@KYKW.fhrF (3) 3
Hex
Strings
Metadata
Results
Text
Media
Analyzing files from UnixImageFile.dd
94%
(1 more...)

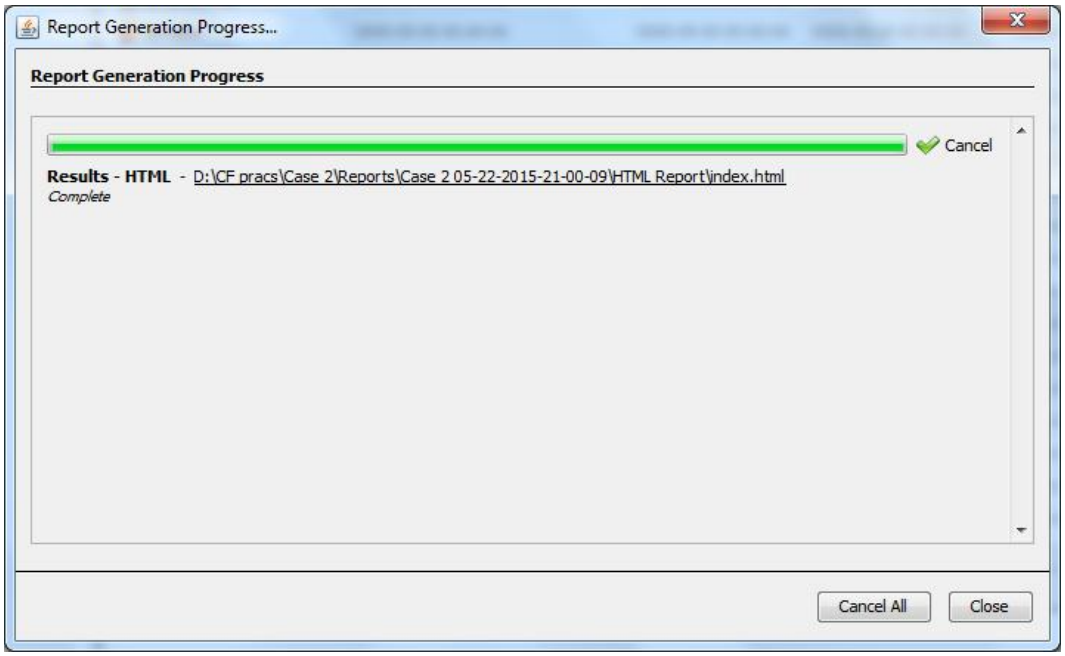
Step 6) After finishing the keyword parameters the screen will be laid out for the user.



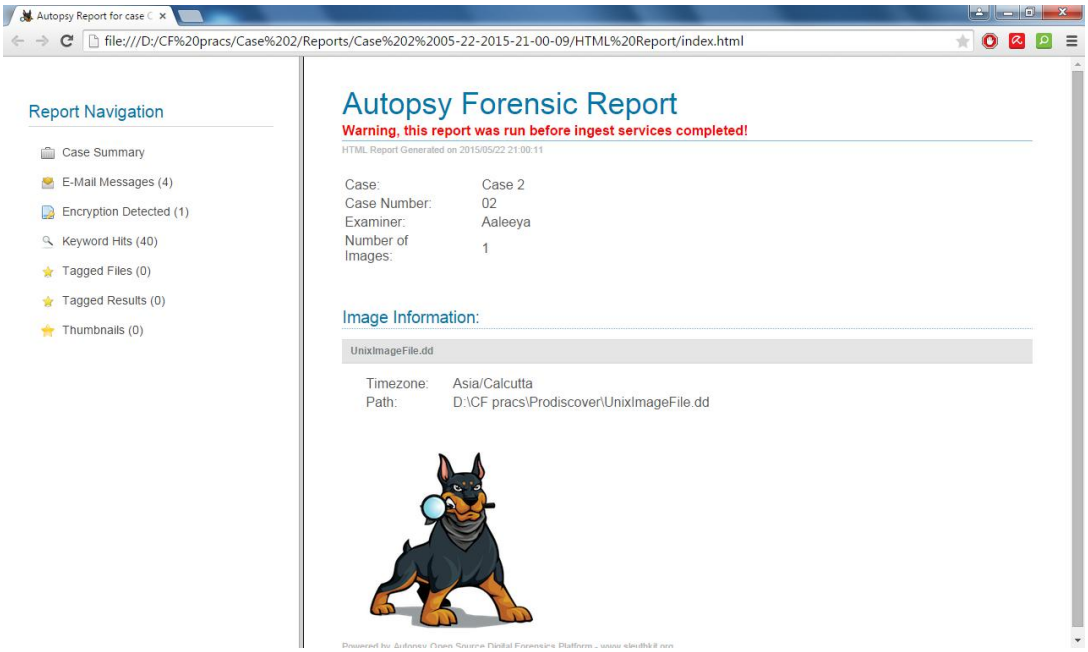
Step 7) After the image is indexed the tree will be populated by the file system, extracted content, keyword searches, and the hash list (if any were used).
the investigator should generate a report. This will allow the investigator to have an idea of what type of information is available and what to expect. The report can be generated in three formats: Excel, XML, and HTML. It also has the ability to select what information to display with choices that can be seen in the image below.



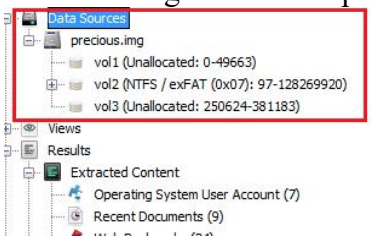

Generate Report
Configure Artifact Reports
Select which data to report on:
All Results
Tagged Results
Select All
Deselect All
Data Types
< Back
Next >
Finish
Cancel
Help


Report Generation Progress...
Report Generation Progress
Cancel
Results - HTML - D:\CF pracs\Case 2\Reports\Case 2 05-22-2015-21-00-09\HTML Report\index.html
Complete
Cancel All
Close

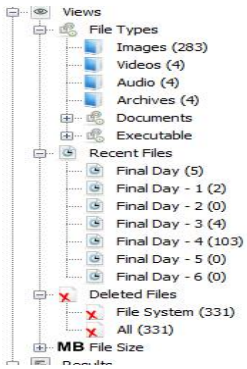
Step 8) With the report on hand the investigator will have an idea of what to expect as well as a list of programs that are installed on the machine. This can help investigators gather all the evidence they need to perform a complete investigation.



Looking at the tree, the top selection is titled “Data Sources” this is where the acquired image is located and the bulk of the investigation, will take place. If the Images tab is expanded the investigator will see each image that was added to the investigation. By expanding an images tab the volumes of the image will be seen including the file system and unallocated space. Expanding the tab that contains the Operating System will give the investigator a look at the root directory and the tree that contains most of the relevant information. This is the same as if the investigator would open the default drive when browsing through a system.

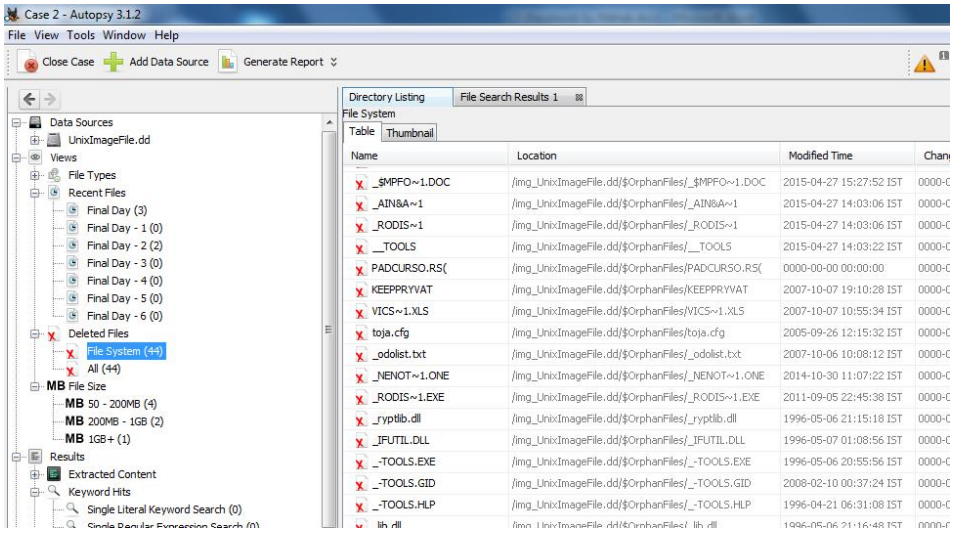


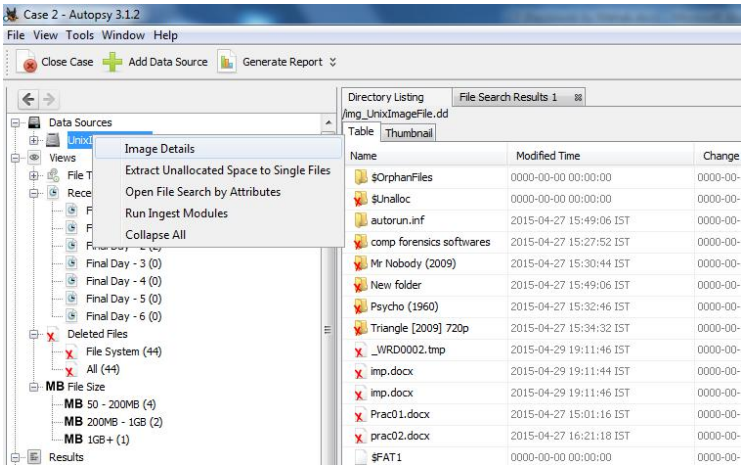
Below the Images tab is the “Views” tab that will allow the investigator to separate the information in the image into different categories such as by file types and by recent documents. The file type can be broken down into: images, video, audio, and documents which includes the major text formats. Another section in the Views tab is a new feature in Autopsy 3, the Recent Files tab. This tab allows the investigator to get a rough outline of what happened in the last 6 days of use by the suspect. The results include registry files, documents opened, and programs run.



The next tab that is seen is the Results tab, this is a new feature that displays all the information from the ingest process. This uses the program BEViewer to look for certain information inside of the data and separate it into sections that make it easier to search for specific data instead of going through all of the information manually. Although this simplifies the investigation process, it does not mean that this is all of the information that is able to be gained through an investigation.

There are 4 main categories when separating the Results tab: Extracted Content, Keyword Hits, Hashset Hits, and E-mail Messages. Each of these sections has subsections that allow for more specific information divisions. In the Extracted Content tab there are sections for: Bookmarks, Cookies, Web History, Downloads, Recent Documents, Installed Programs, and Device Attached.




Case 2 - Autopsy 3.1.2
File View Tools Window Help
Close Case
Add Data Source
Generate Report
Directory Listing
File Search Results 1
/img_UnixImageFile.dd
Table
Thumbnail
Name
Modified Time
Change
Data Sources
Views
Image Details
Extract Unallocated Space to Single Files
Open File Search by Attributes
Run Ingest Modules
Collapse All
Final Day - 3 (0)
Final Day - 4 (0)
Final Day - 5 (0)
Final Day - 6 (0)
Deleted Files
File System (44)
All (44)
MB File Size
MB 50 - 200MB (4)
MB 200MB - 1GB (2)
MB 1GB+ (1)
Results
$OrphanFiles
$Unalloc
autorun.inf
comp forensics softwares
Mr Nobody (2009)
New folder
Psycho (1960)
Triangle [2009] 720p
_WRD0002.tmp
imp.docx
imp.docx
Prac01.docx
prac02.docx
$FAT1

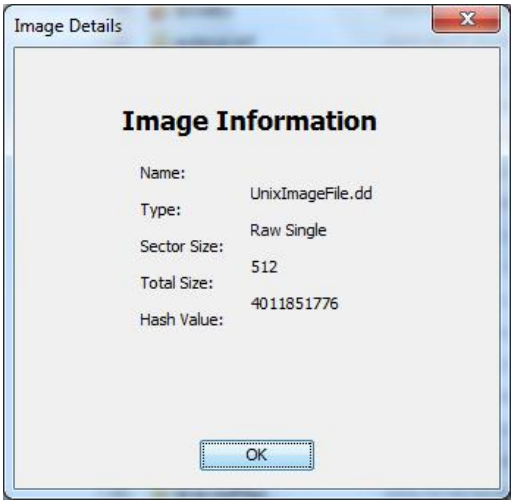
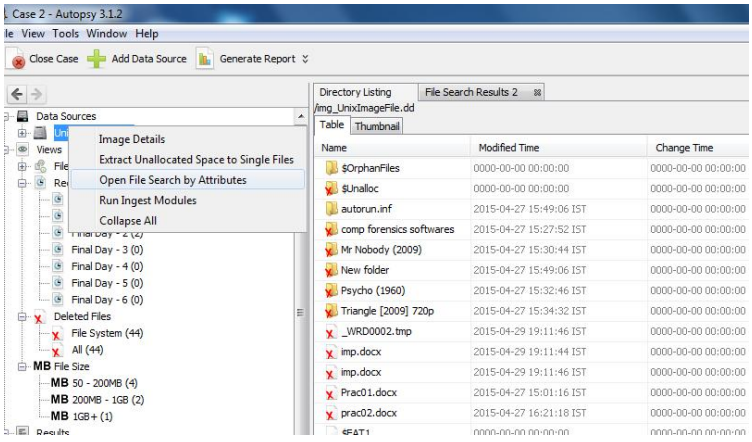
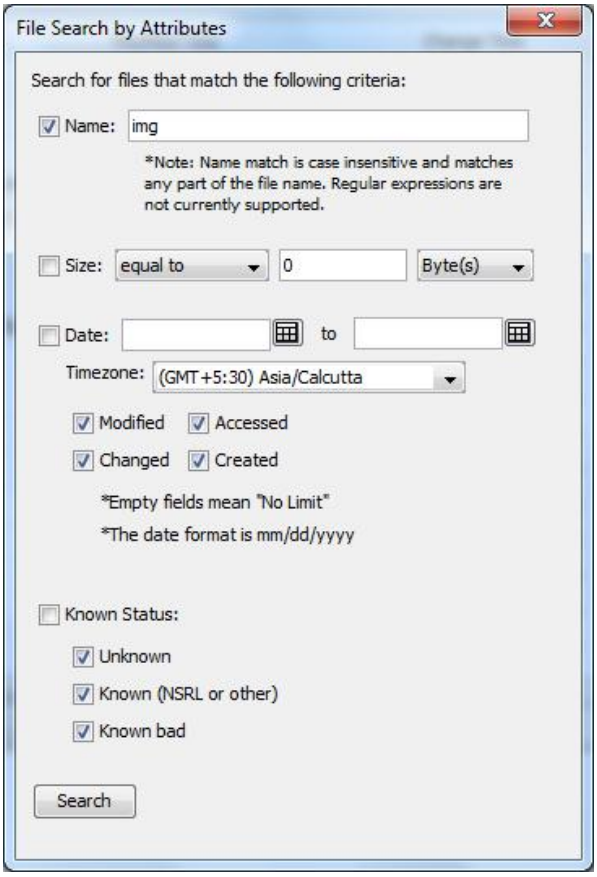
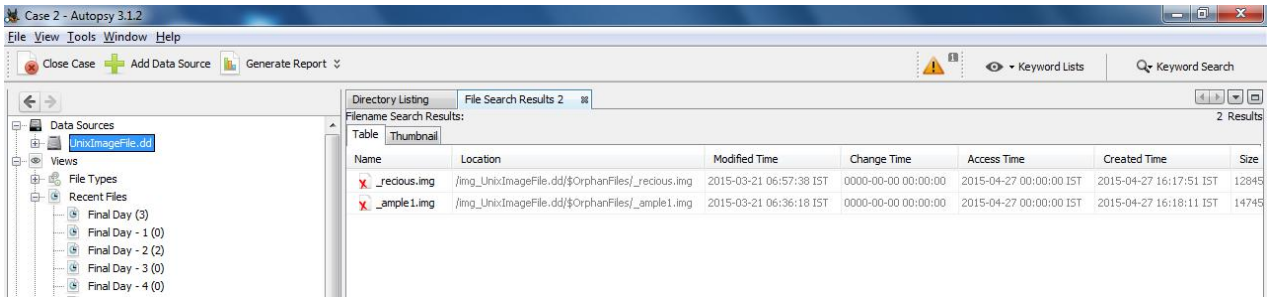
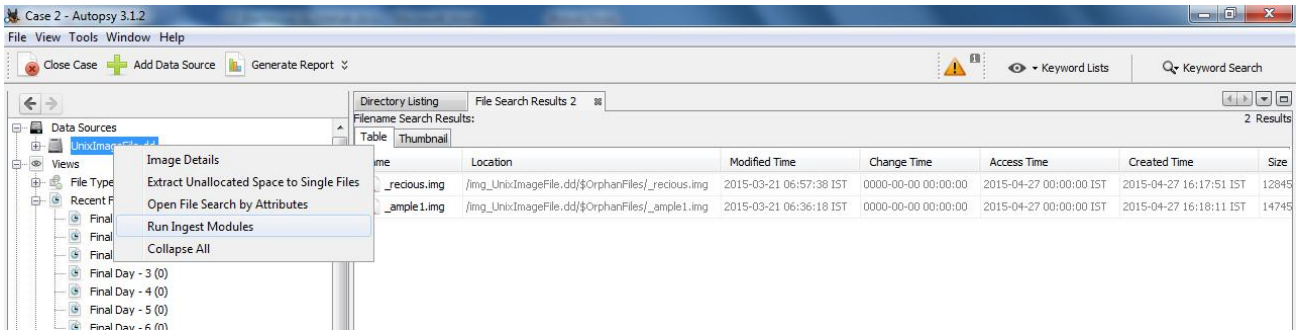


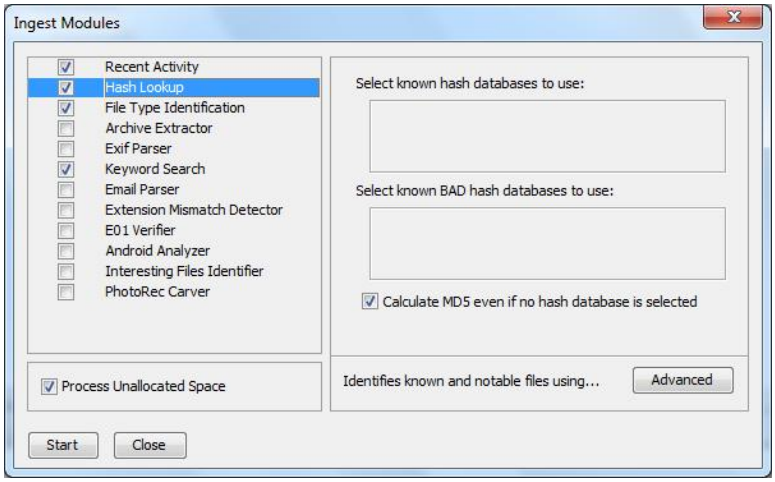
Image Details
Image Information
Name:
UnixImageFile.dd
Type:
Raw Single
Sector Size:
512
Total Size:
4011851776
Hash Value:
OK

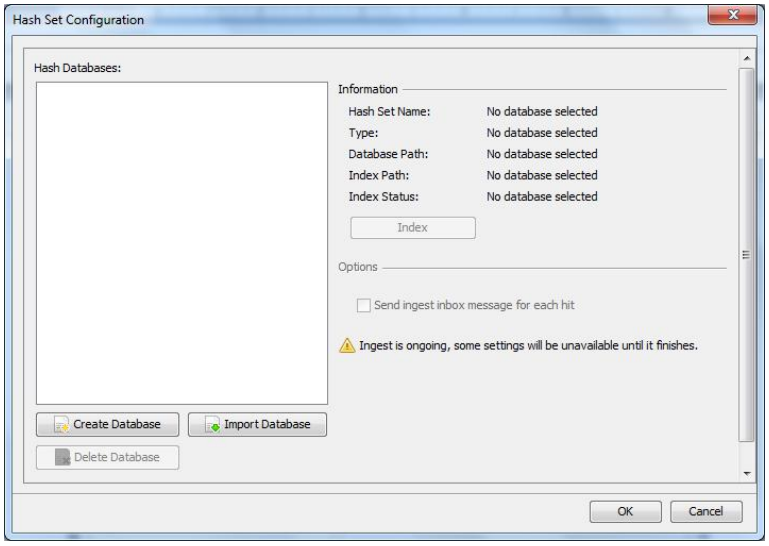

Case 2 - Autopsy 3.1.2
Close Case
Add Data Source
Generate Report
Directory Listing
File Search Results 2
/img_UnixImageFile.dd
Table
Thumbnail
Name
Modified Time
Change Time
Image Details
Extract Unallocated Space to Single Files
Open File Search by Attributes
Run Ingest Modules
Collapse All

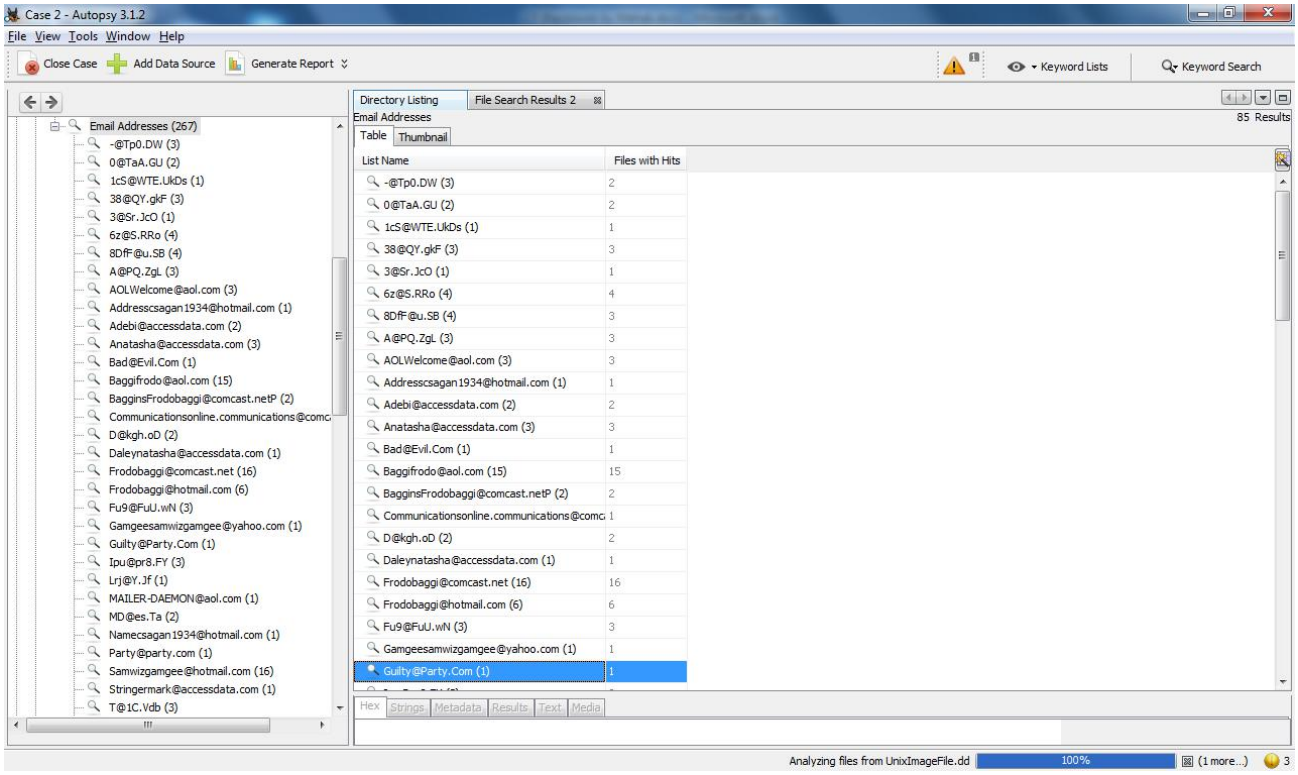

File Search by Attributes
Search for files that match the following criteria:
Name: img
*Note: Name match is case insensitive and matches any part of the file name. Regular expressions are not currently supported.
Size: equal to 0 Byte(s)
Date: to
Timezone: (GMT+5:30) Asia/Calcutta
Modified Accessed
Changed Created
*Empty fields mean "No Limit"
*The date format is mm/dd/yyyy
Known Status:
Unknown
Known (NSRL or other)
Known bad
Search

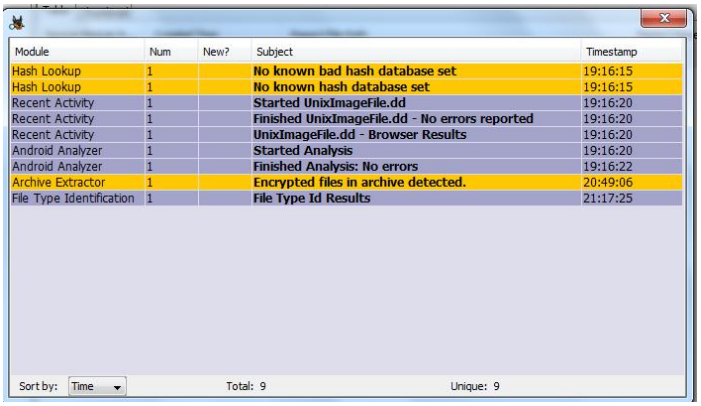

Case 2 - Autopsy 3.1.2
File View Tools Window Help
Close Case
Add Data Source
Generate Report
Keyword Lists
Keyword Search
Directory Listing
File Search Results 2
Filename Search Results:
2 Results
Table
Thumbnail
Name
Location
Modified Time
Change Time
Access Time
Created Time
Size
_recious.img
/img_UnixImageFile.dd/$OrphanFiles/_recious.img
2015-03-21 06:57:38 IST
0000-00-00 00:00:00
2015-04-27 00:00:00 IST
2015-04-27 16:17:51 IST
_ample1.img
/img_UnixImageFile.dd/$OrphanFiles/_ample1.img
2015-03-21 06:36:18 IST
2015-04-27 16:18:11 IST
Data Sources
UnixImageFile.dd
Views
File Types
Recent Files
Final Day (3)
Final Day - 1 (0)
Final Day - 2 (2)
Final Day - 3 (0)
Final Day - 4 (0)

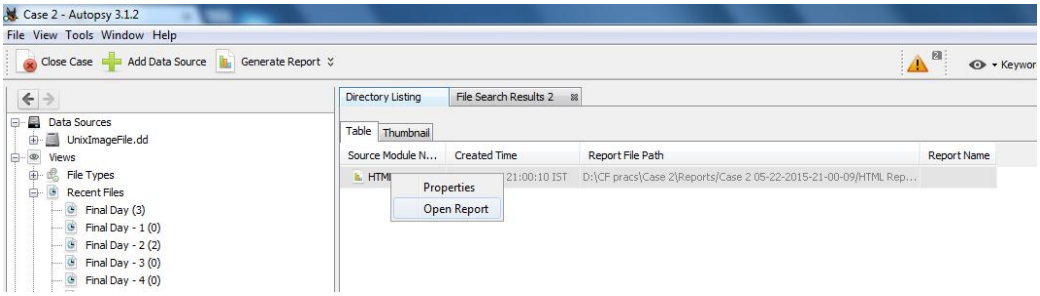

Case 2 - Autopsy 3.1.2
File View Tools Window Help
Close Case
Add Data Source
Generate Report
Keyword Lists
Keyword Search
Directory Listing
File Search Results 2
Filename Search Results:
2 Results
Table
Thumbnail
Location
Modified Time
Change Time
Access Time
Created Time
Size
_recious.img
/img_UnixImageFile.dd/$OrphanFiles/_recious.img
2015-03-21 06:57:38 IST
0000-00-00 00:00:00
2015-04-27 00:00:00 IST
2015-04-27 16:17:51 IST
_ample1.img
/img_UnixImageFile.dd/$OrphanFiles/_ample1.img
2015-03-21 06:36:18 IST
2015-04-27 16:18:11 IST
Data Sources
Views
File Type
Recent F
Image Details
Extract Unallocated Space to Single Files
Open File Search by Attributes
Run Ingest Modules
Collapse All
Final Day - 3 (0)
Final Day - 4 (0)
Final Day - 5 (0)

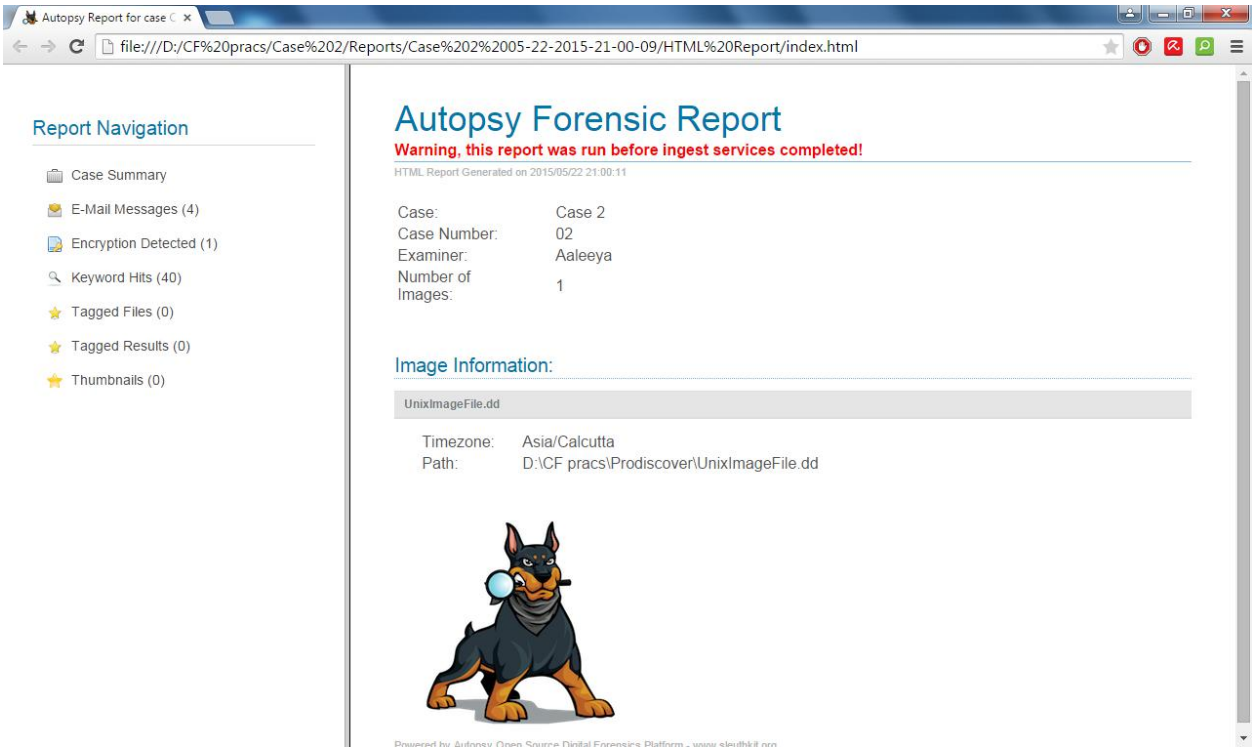

Ingest Modules
Recent Activity
Hash Lookup
File Type Identification
Archive Extractor
Exif Parser
Keyword Search
Email Parser
Extension Mismatch Detector
E01 Verifier
Android Analyzer
Interesting Files Identifier
PhotoRec Carver
Select known hash databases to use:
Select known BAD hash databases to use:
Calculate MD5 even if no hash database is selected
Process Unallocated Space
Identifies known and notable files using...
Advanced
Start
Close


Hash Set Configuration
Hash Databases:
Information
Hash Set Name: No database selected
Type: No database selected
Database Path: No database selected
Index Path: No database selected
Index Status: No database selected
Index
Options
Send ingest inbox message for each hit
Ingest is ongoing, some settings will be unavailable until it finishes.
Create Database
Import Database
Delete Database
OK
Cancel


Case 2 - Autopsy 3.1.2
File View Tools Window Help
Close Case
Add Data Source
Generate Report
Keyword Lists
Keyword Search
Email Addresses (267)
Directory Listing
File Search Results 2
Email Addresses
85 Results
Table
Thumbnail
List Name
Files with Hits
Analyzing files from UnixImageFile.dd
100%


Module Num New? Subject Timestamp
Hash Lookup 1 No known bad hash database set 19:16:15
Hash Lookup 1 No known hash database set 19:16:15
Recent Activity 1 Started UnixImageFile.dd 19:16:20
Recent Activity 1 Finished UnixImageFile.dd - No errors reported 19:16:20
Recent Activity 1 UnixImageFile.dd - Browser Results 19:16:20
Android Analyzer 1 Started Analysis 19:16:20
Android Analyzer 1 Finished Analysis: No errors 19:16:22
Archive Extractor 1 Encrypted files in archive detected. 20:49:06
File Type Identification 1 File Type Id Results 21:17:25
Sort by: Time
Total: 9
Unique: 9

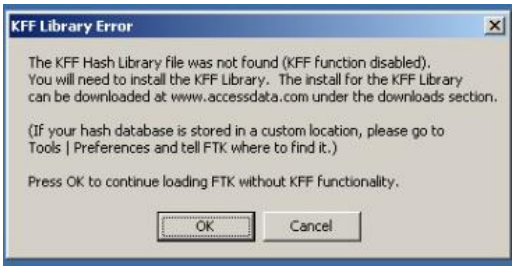

Case 2 - Autopsy 3.1.2
File View Tools Window Help
Close Case
Add Data Source
Generate Report
Directory Listing
File Search Results 2
Table
Thumbnail
Source Module N...
Created Time
Report File Path
Report Name
Data Sources
UnixImageFile.dd
Views
File Types
Recent Files
Final Day (3)
Final Day - 1 (0)
Final Day - 2 (2)
Final Day - 3 (0)
Final Day - 4 (0)
Properties
Open Report


Autopsy Report for case
file:///D:/CF%20pracs/Case%202/Reports/Case%202%2005-22-2015-21-00-09/HTML%20Report/index.html
Report Navigation
Case Summary
E-Mail Messages (4)
Encryption Detected (1)
Keyword Hits (40)
Tagged Files (0)
Tagged Results (0)
Thumbnails (0)
Autopsy Forensic Report
Warning, this report was run before ingest services completed!
HTML Report Generated on 2015/05/22 21:00:11
Case: Case 2
Case Number: 02
Examiner: Aaleeya
Number of Images: 1
Image Information:
UnixImageFile.dd
Timezone: Asia/Calcutta
Path: D:\CF pracs\Prodiscover\UnixImageFile.dd

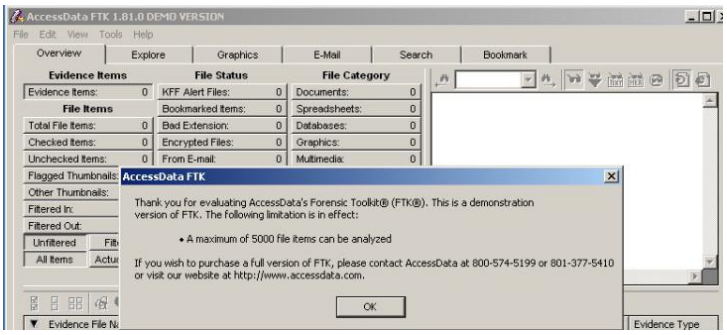
Practical No: 2 A

Step 1: Start Forensic Toolkit.

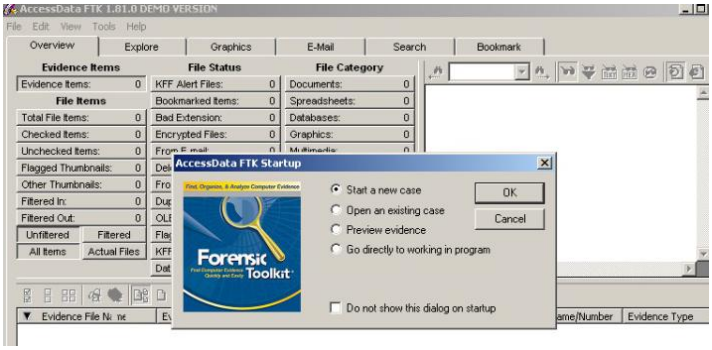
Step 2: Here, prompted with a warning dialog box, click on OK to continue.



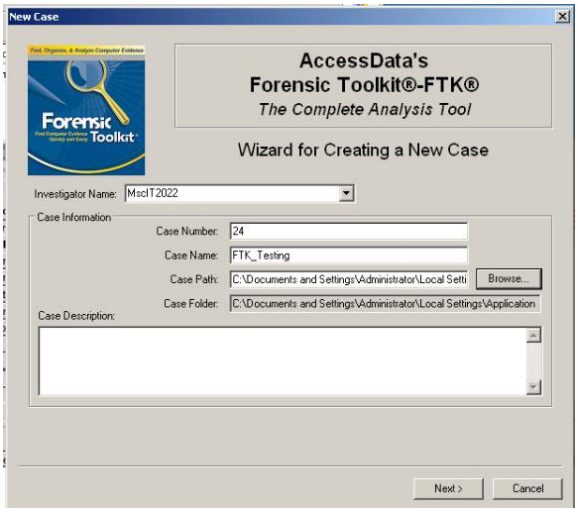
Step 3: click on OK button.



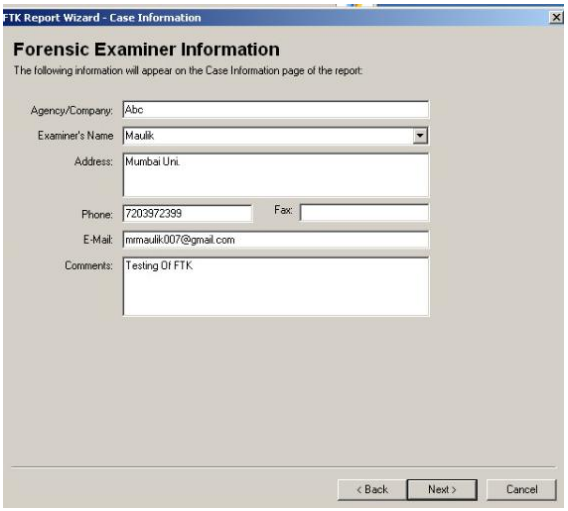
Step 4: Now select Start New Case option and click on ok.



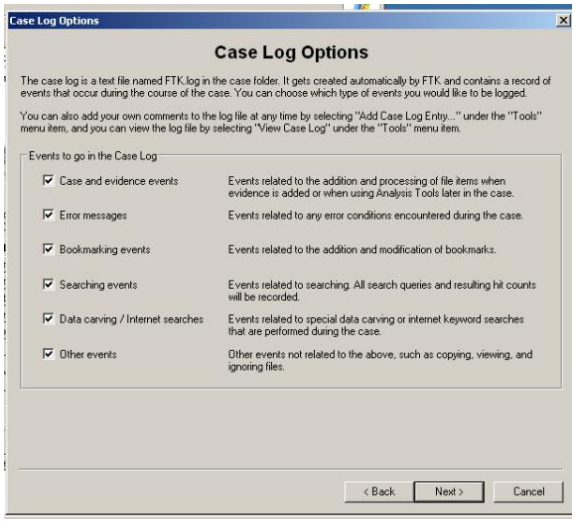
Step 5: Enter the detail for a New case.



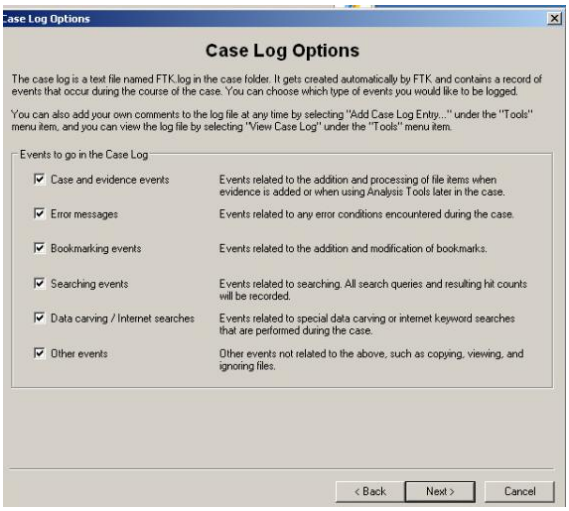
Step 6: Fill the information in Forensic Examiner Information dialog box.



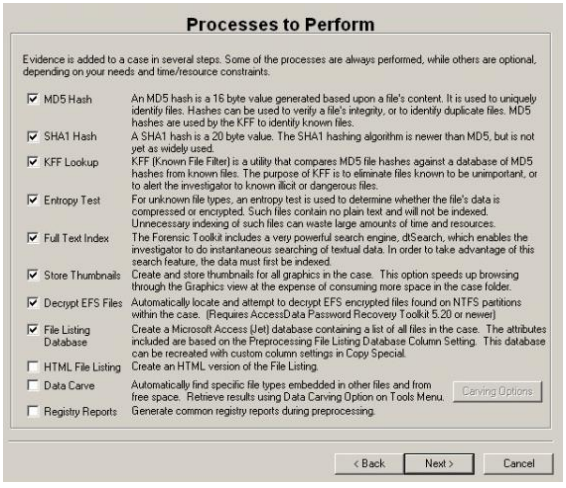
Step 7: leave the default settings and click on next.



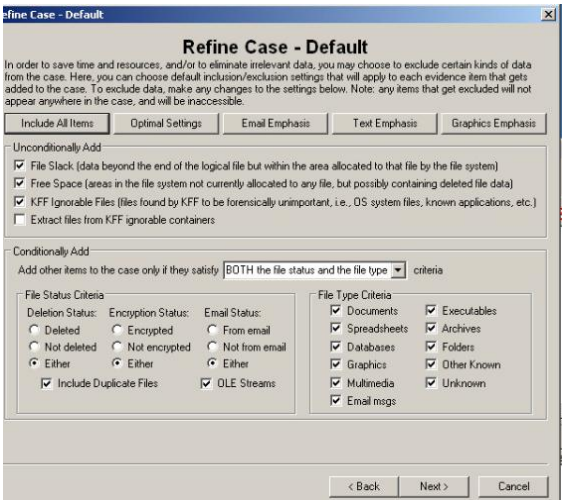
Step 8: Now again leave the default settings and click on next.



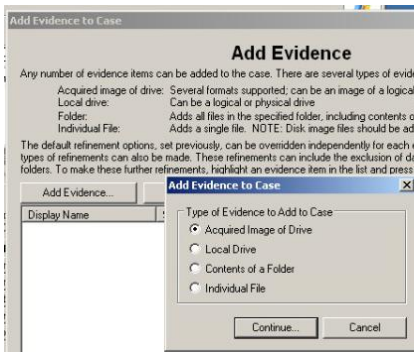
Step 9: In the Refine Case-Default, click the Include All items button and then click Next.



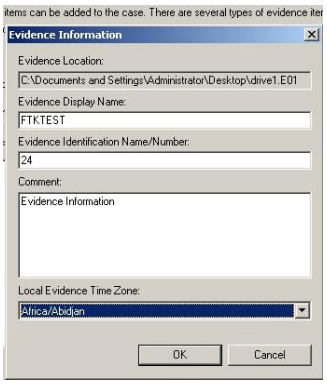
Step 10: In Refine Index-Default, accept the default settings and click Next.



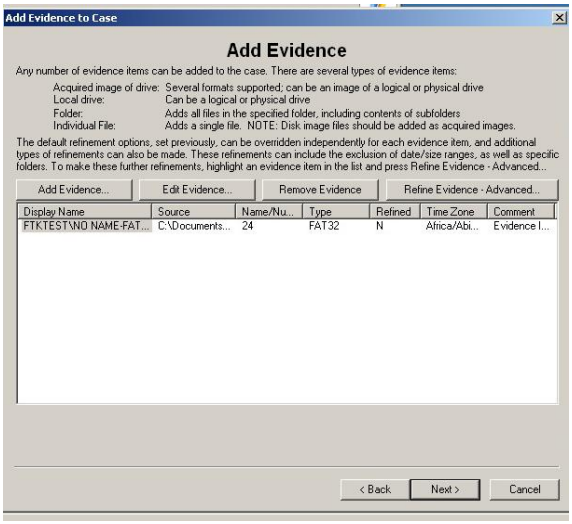
Step 11: Now here Click on add Evidence button.



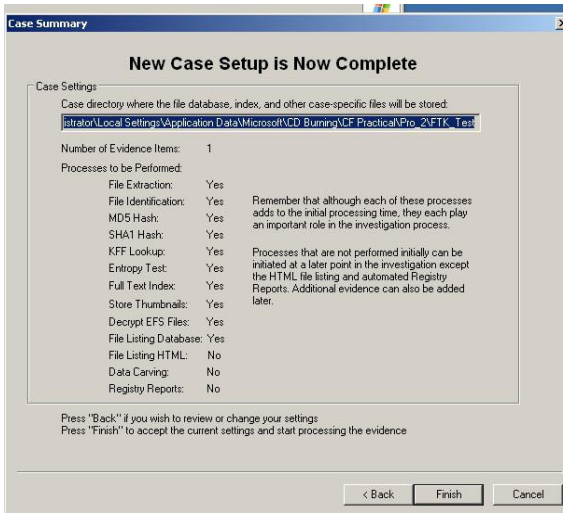
Step 12: Enter Evidence Information and click on OK button.



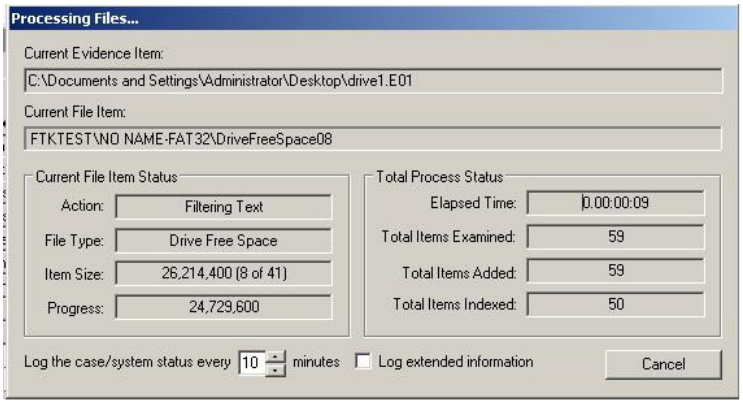
Step 13: Now click on Next.



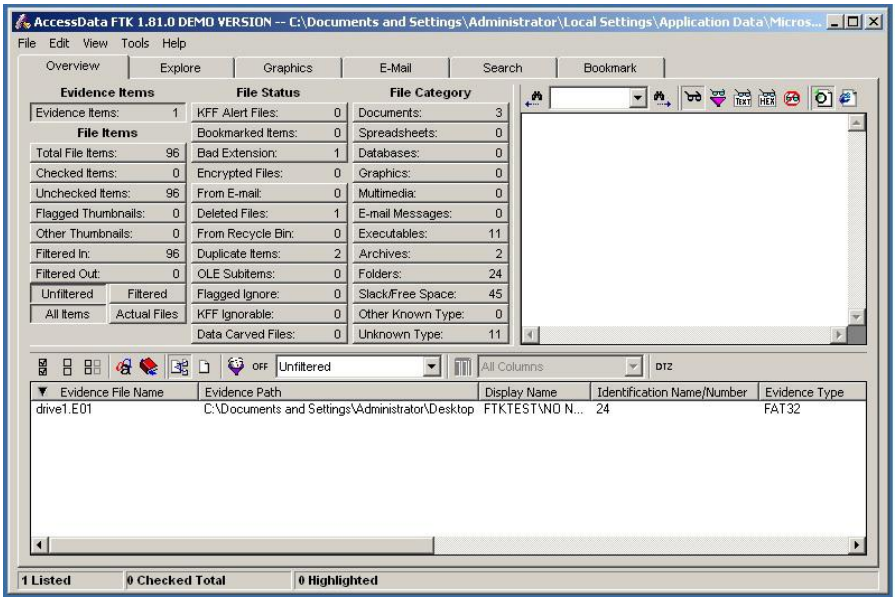
Step 14: Click on Finish to initiate the analysis.



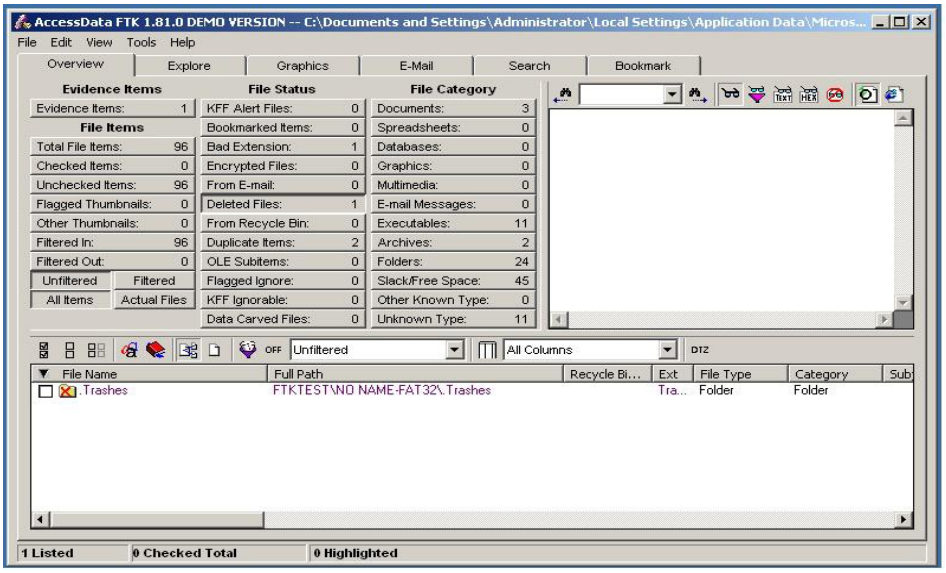
Step 15: Now Processing Will Start.



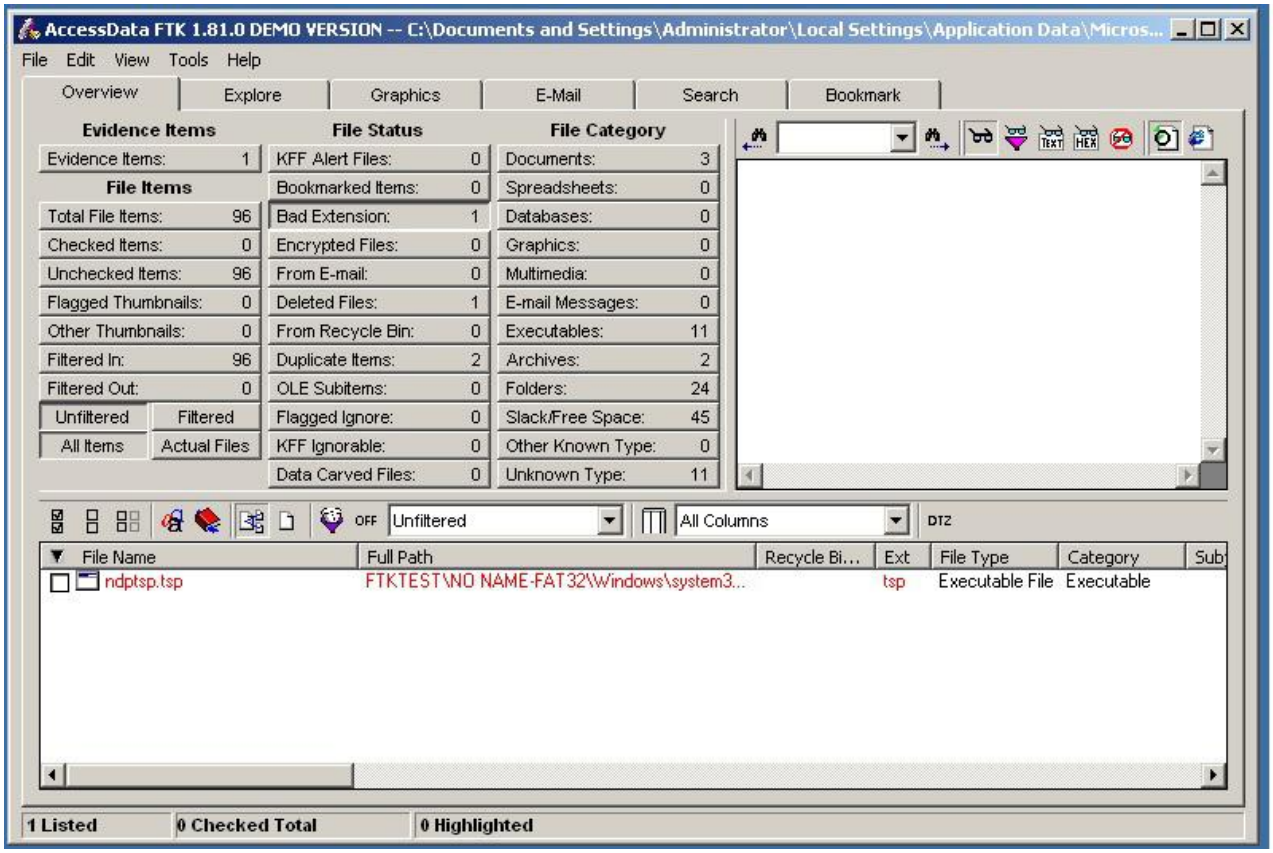
Step 16: when FTK finishes the processing part, the FTK window opens to the Overview tab.



Step 17: Select Deleted Files option to explore the evidence items.



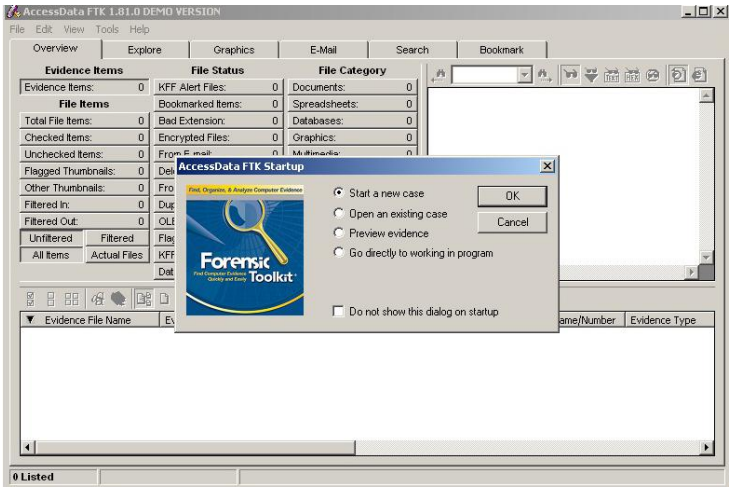
Step 18: Select Bad Extension Files to view.



Practical No: 3

Aim: Using Forensic Toolkit FTK & Write a report using FTK(AccessData FTK).

Step 1: First we need to Create a Case.



To provide the new case information:

1 In the Investigator Name field, type the name of the investigator. The drop-down list contains the name of investigators that have been entered in prior cases. If the investigator has worked on other cases in FTK, select the name from the list.

2: In the Case Number field, enter the case number for reference.

3 In the Case Name field, enter the name of the case. The name cannot contain the following characters: " > ? / : \ | < The case name also becomes the name of the folder where all case information will be stored.

4 Next to the Case Path field, click Browse to select the path where the evidence will be stored. By default, all FTK cases are stored in that directory.

5 Verify that the Case Folder field lists the folder where you want the case to be stored. Each case is stored in a separate folder and should be kept distinct from other cases. The Case Folder field is based on the Case Name and Case Path fields. To make changes to the Case Folder, change the Case Name and Case Path fields.

6 (Optional) In the Case Description field, add information that will be helpful to the analysis of the case. This field is particularly useful if several people work on the case. This field is included in the report created at the end of the case investigation. Click Next.

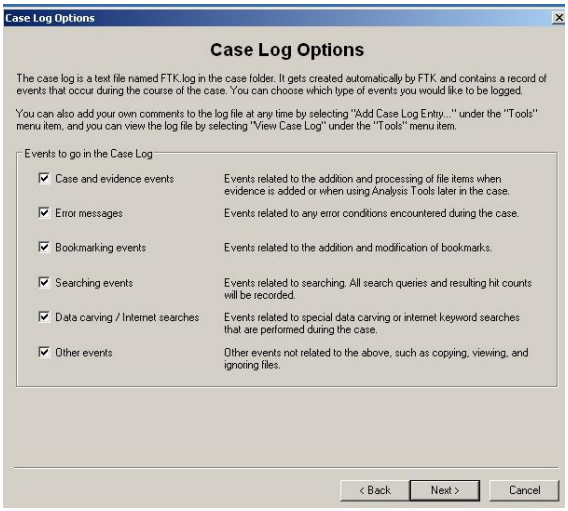
Entering Forensic Examiner Information:

Selecting Case Log Options:

The Case Log Options form allows you to select which events you want FTK to log for the current case. FTK maintains a log file of FTK events such as bookmarking items, searches, and error messages for each case.

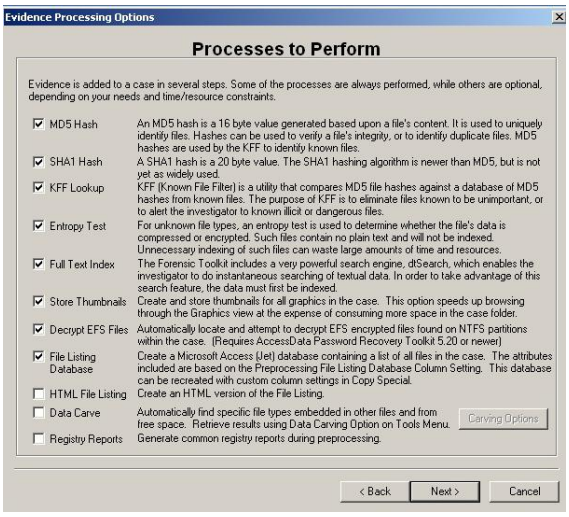
The following table outlines the Case Log Options form:

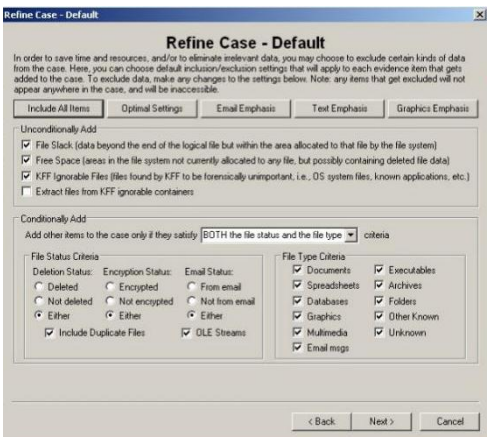
Option	Description
Bookmarking Events	Events related to the addition and modification of bookmarks.
Case and Evidence Events	Events related to the addition and processing of file items when evidence is added or when using the Analysis Tools.
Data Carving/Internet Searches	Events related to data carving or Internet keyword searches that are performed during the case.
Error Messages	Events related to any errors encountered during the case.
Other Events	The following events: • Copy special • Exporting files • Viewing items in the detached viewer • Ignoring and unignoring files
Searching Events	All search queries and resulting hit counts.



Selecting Evidence Processes:

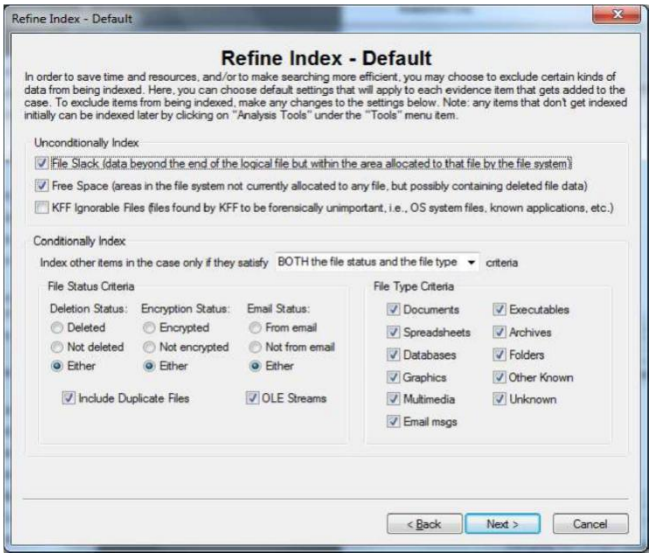
The Evidence Processing Options form allows you to select which processes you want to perform on the current evidence. You only need to select those processes that are relevant to the evidence you are adding to the case. For example, if your case is primarily a graphics case, there is no need to index the evidence.





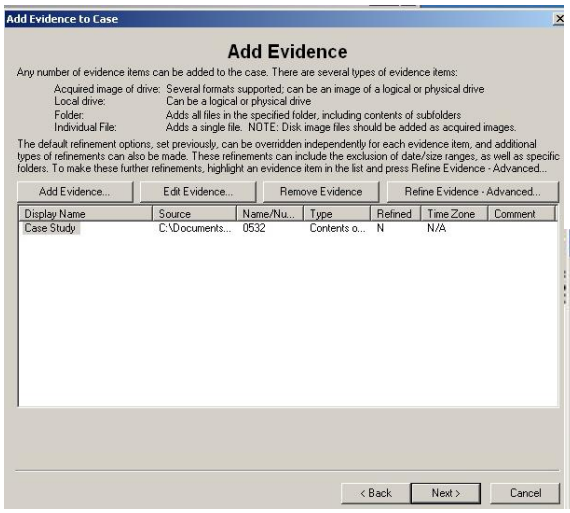
Refining the Index:

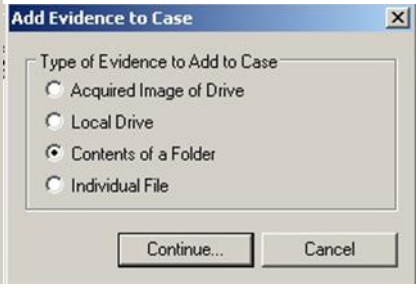
The Refine Index form allows you to specify types of data that you do not want to index. You might choose to exclude data to save time and resources and to increase searching efficiency.

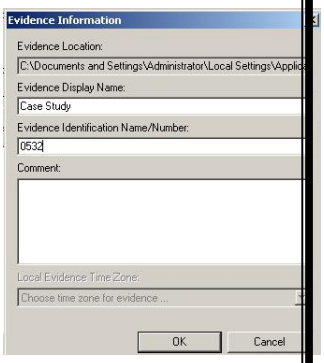


Managing Evidence :

As your investigation progresses, you will want to edit the information you entered for your evidence. Evidence is managed through the Add Evidence forms.

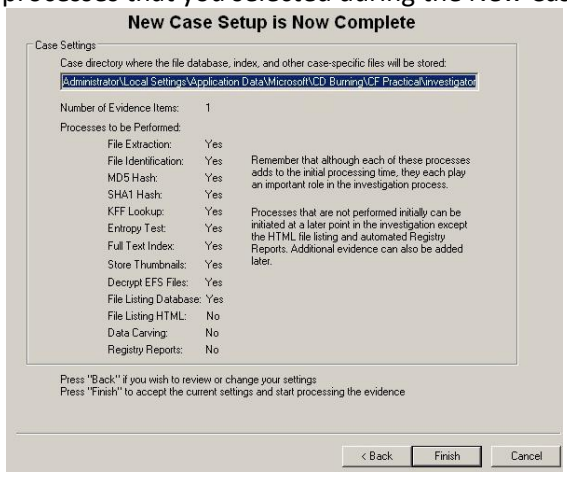






Reviewing Case Summary:

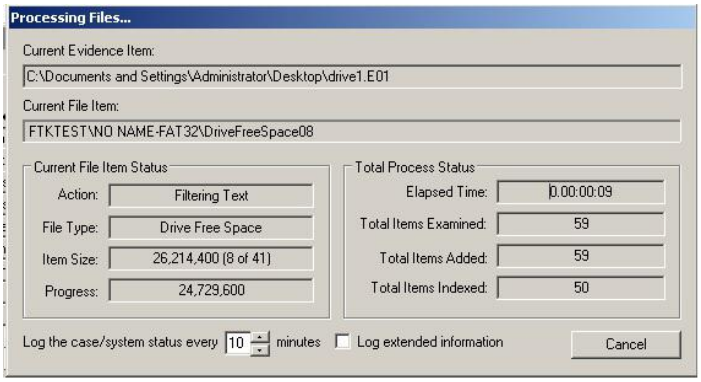
The Case Summary form allows you to review the evidence directory, number of evidence items, and evidence processes that you selected during the New Case Wizard.

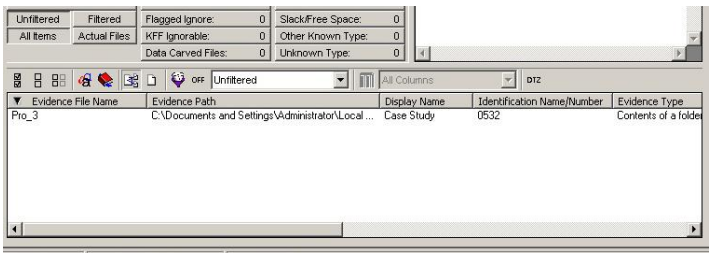


Processing the Evidence :

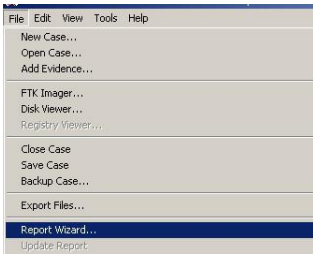
After you click Finish, the Processing Files form appears and displays the status of the processes you selected in the wizard.

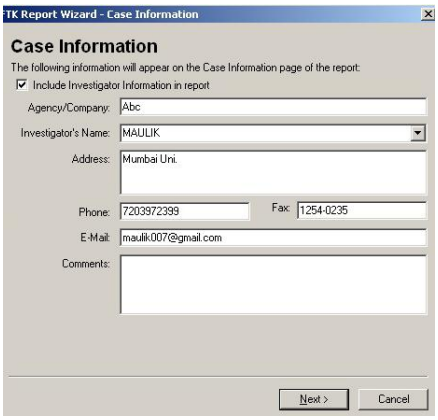
1.From the menu, select Report, and then Generate Report or click the button on the toolbar.



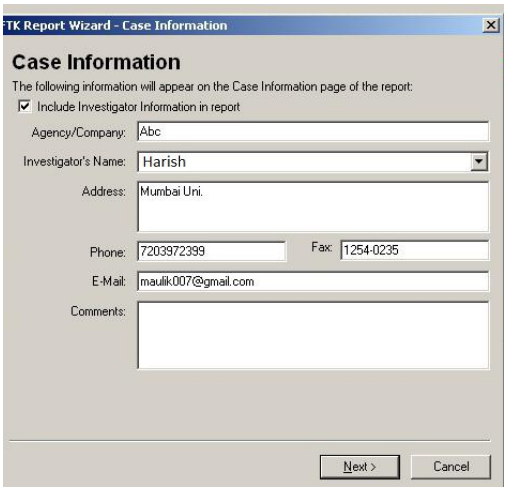


2.The Case Information dialog appears.

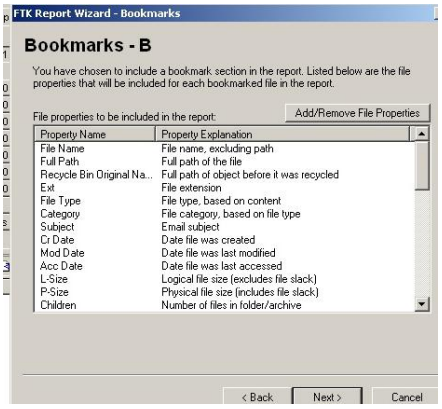




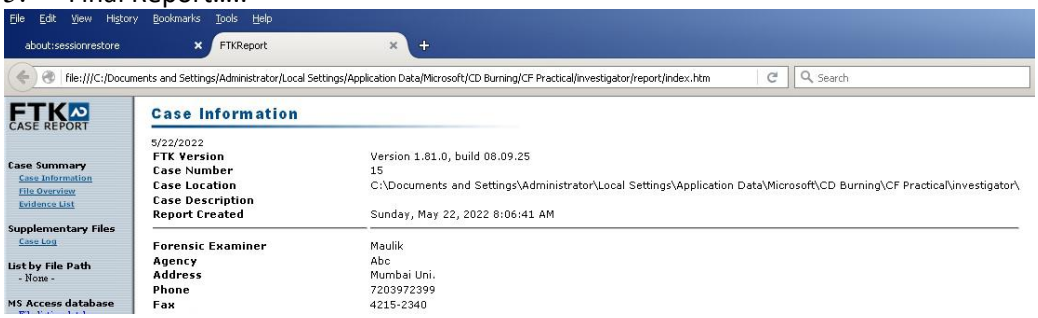
3. The Bookmarks-A dialog appears.



4. The Bookmarks-B dialog appears



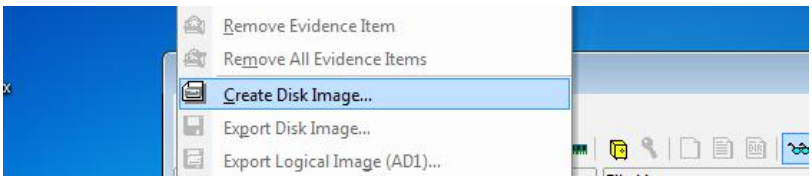
5. Final Report…..



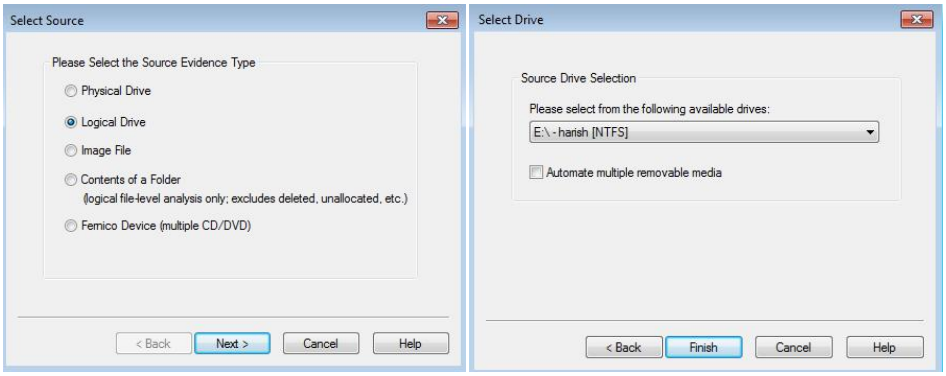
Practical No. 4A

Step 1:Download and install Accessdata FTK Imager on windows virtual machine.

Step 2: Click On File > Create Disk Image



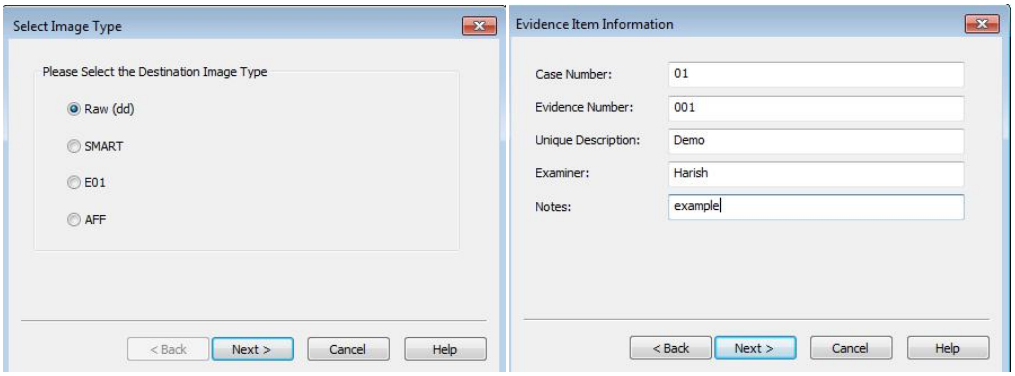
Step 3: Select logical Drive and Select the drive.

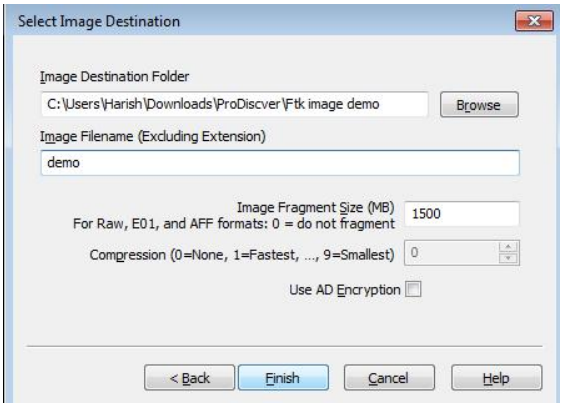


Step 4: Select the Destination for image file to be saved.In that Choose the appropriate destination image type. For our guide, we'll be deploying 'dd' which stands for disk dump.

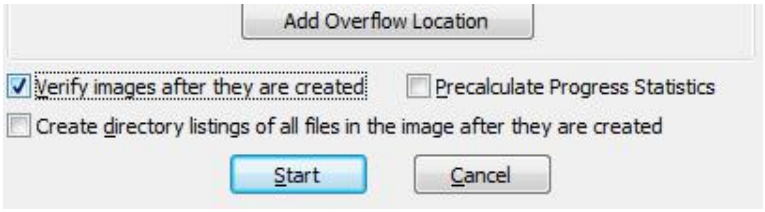
After that we need to enter the case number and other details as show below.

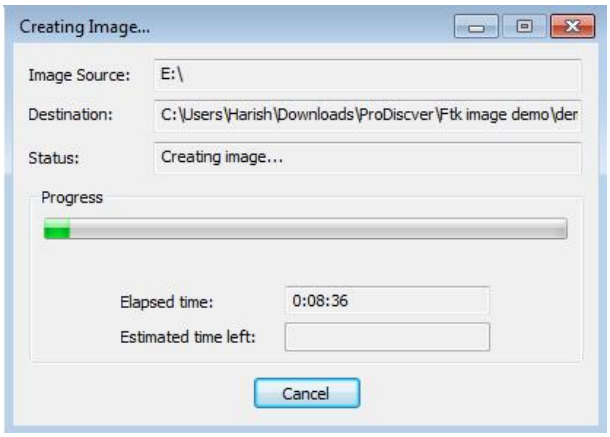
At last select the destination for saving the file.





Step 5: At last we need to select the checkbox for checking the image file after creating. Then start creating Image.





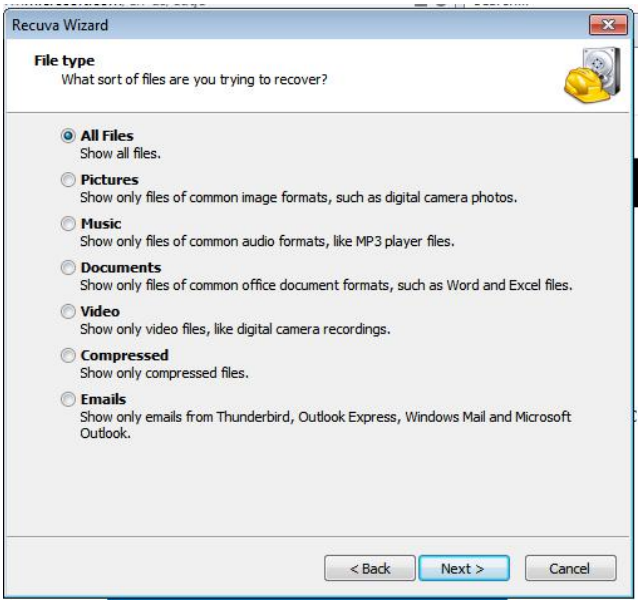
Practical No. 4B

Using Recuva

Step 1: Open the Recuva Software.

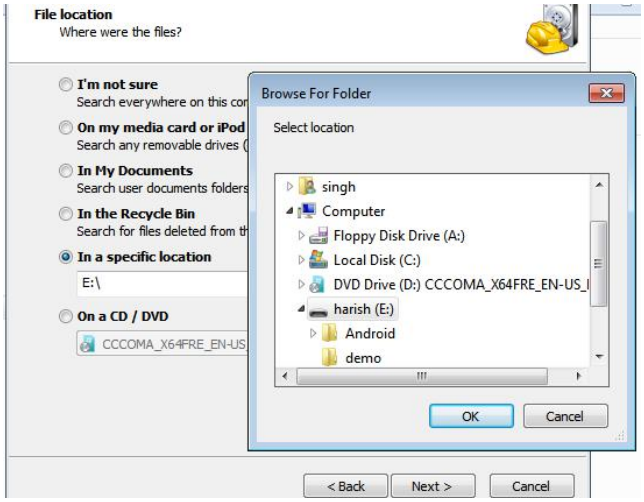
Step 2: click on next.

Step 3: Select the type of files you want to recover.

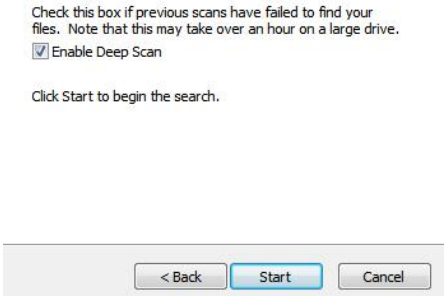


Step 4: Click the next button.

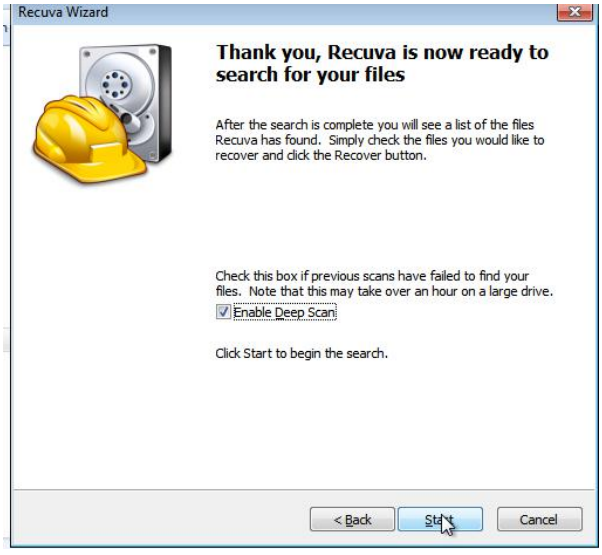
Step 5: Select the drive which we want to recover.



Step 6: check for deep scan for files.

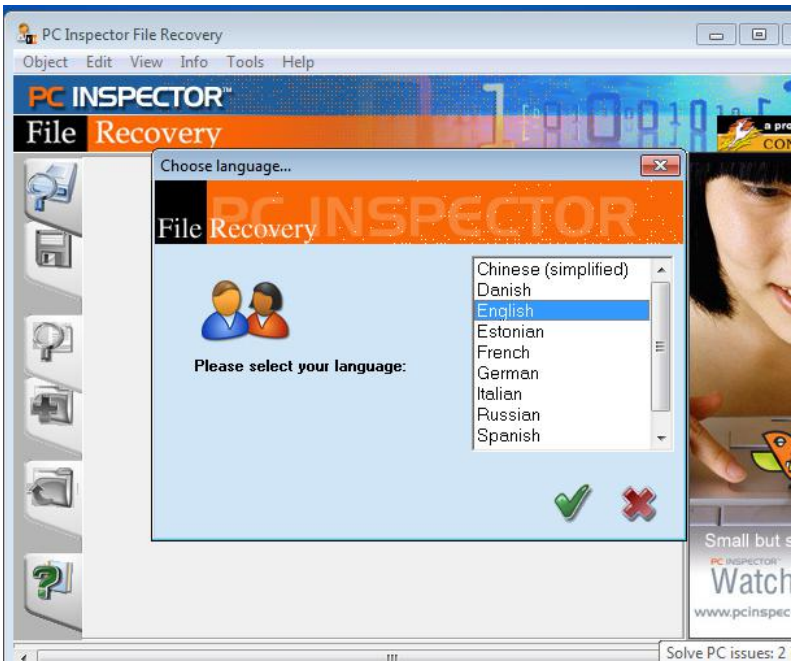


Step 7:Click start Button. It will start recovering deleted files.

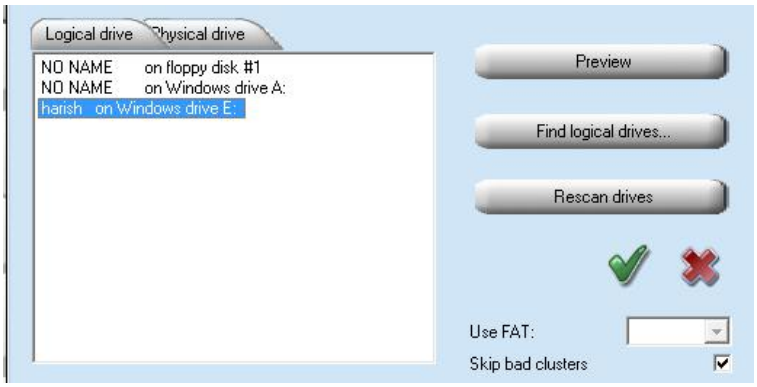


Using PC Inspector File Recovery

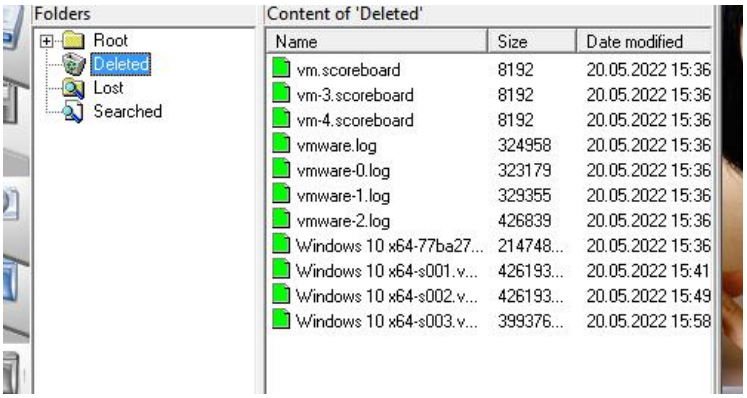
Step 1:Download and install PC inspector and open it.



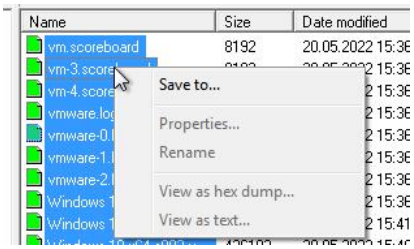
Step 2: Select the drive you want to recover files from. Ensure you've selected the right drive.

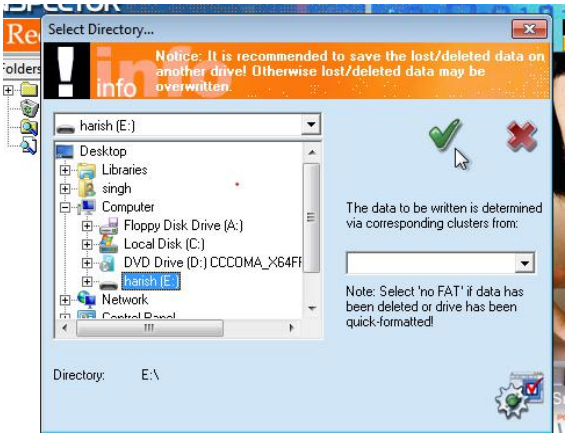


Step 3: Scan the selected drive for deleted files.



Step 4: Sort through the potentially recoverable files.And save the deleted file.

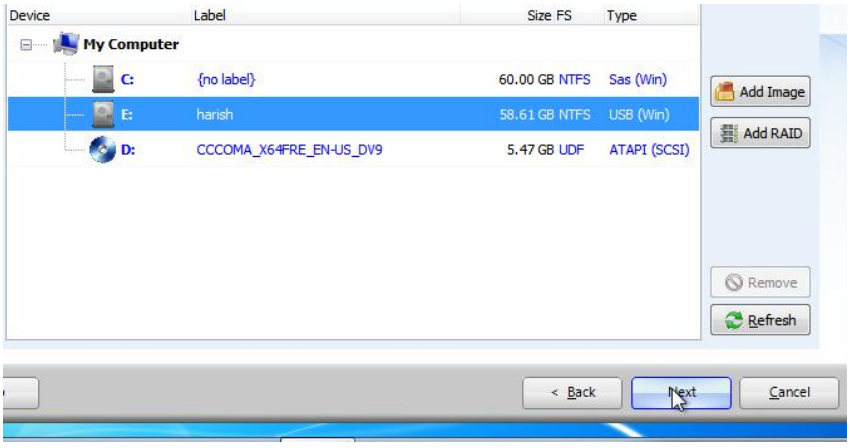




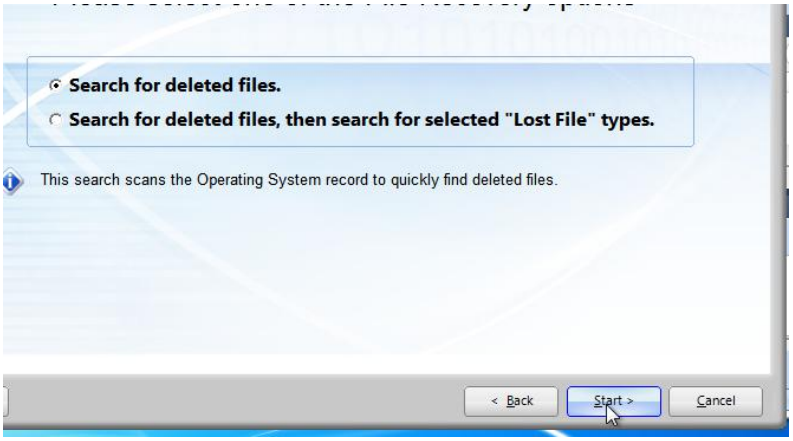
Using Recover my file.

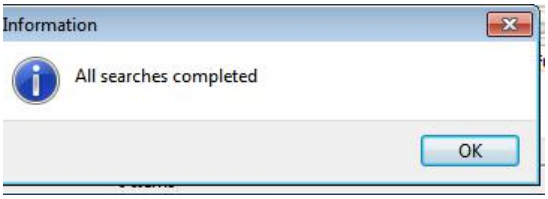
Step 1:Download and install the tool and open then select the type of file you want to recover.

Step 2: Select the file or drive you want to recover.

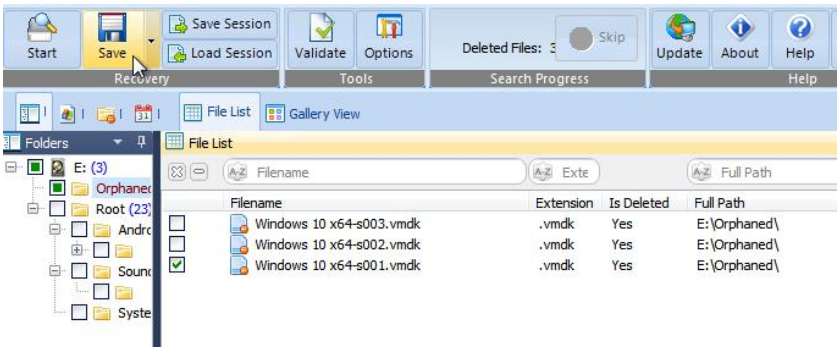


Step 3: Start search for deleted file.



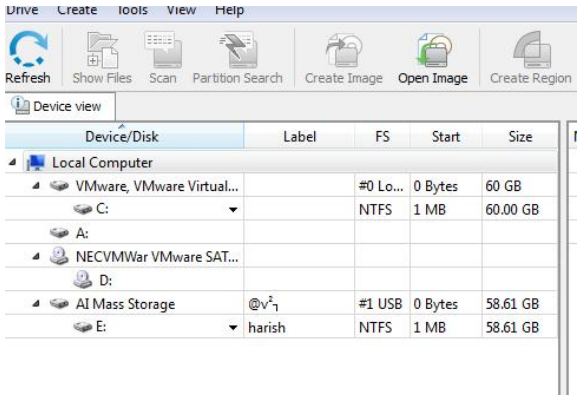


Step 4: Now you can view and recover the deleted file. Then save that original file.

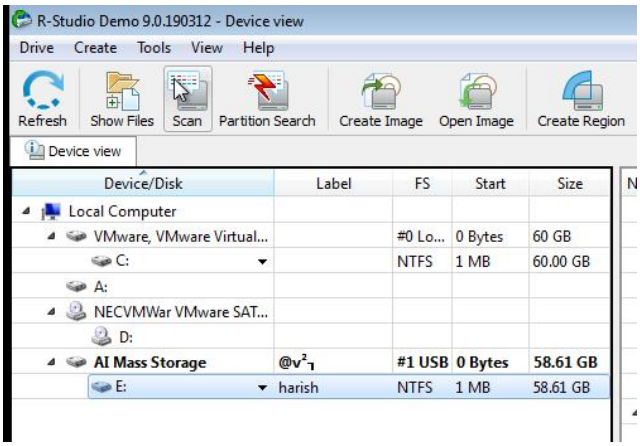


Using R-studio

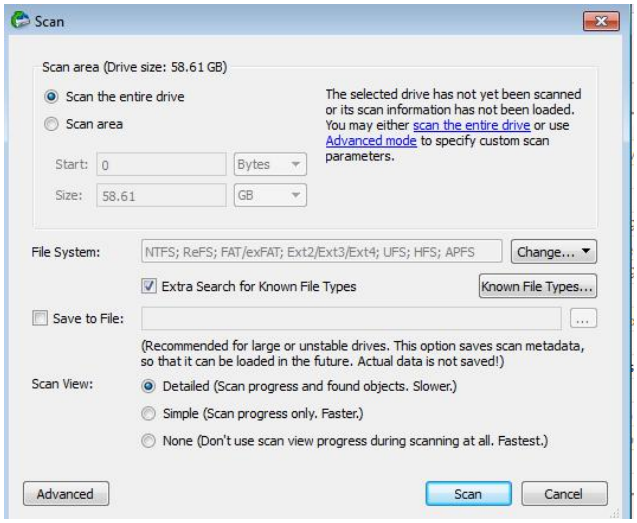
Step 1: Start R-Studio and locate the damaged disk.



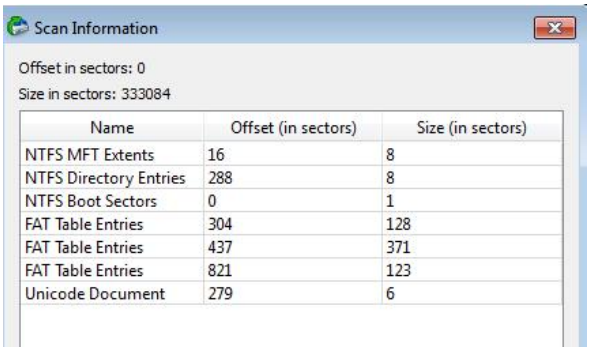
Step 2: Scan the damaged disk.



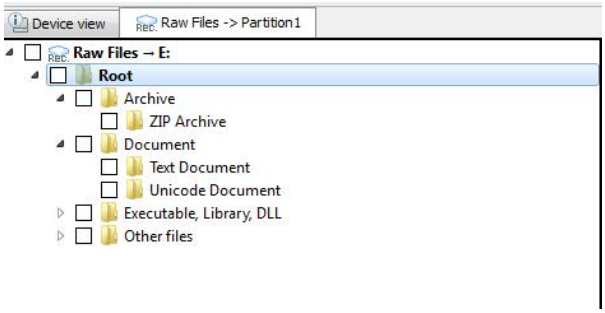
Step 3: View the search results.



Step 4: Double-click the partition to browse its contents.

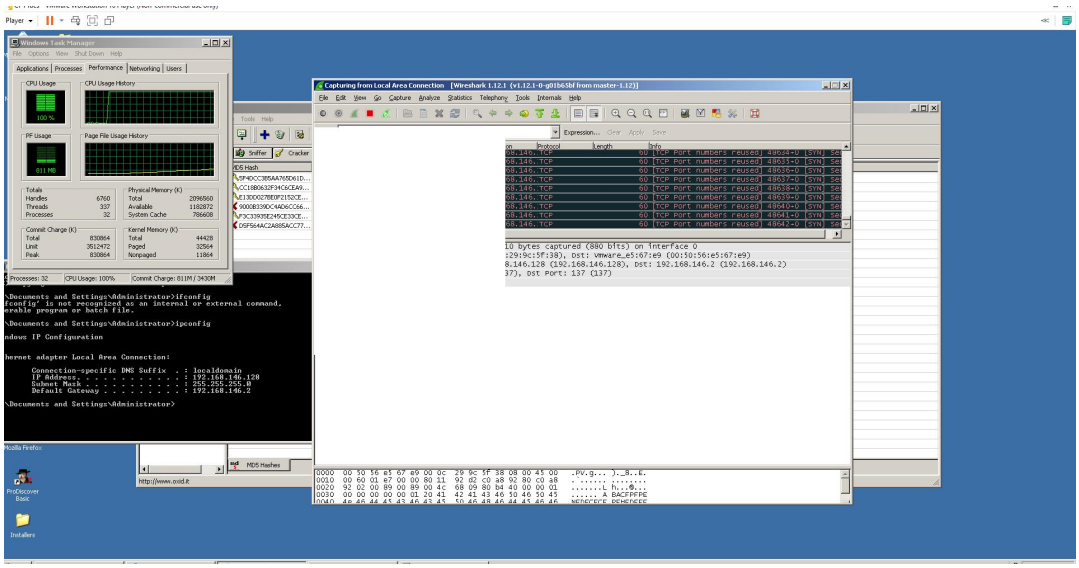


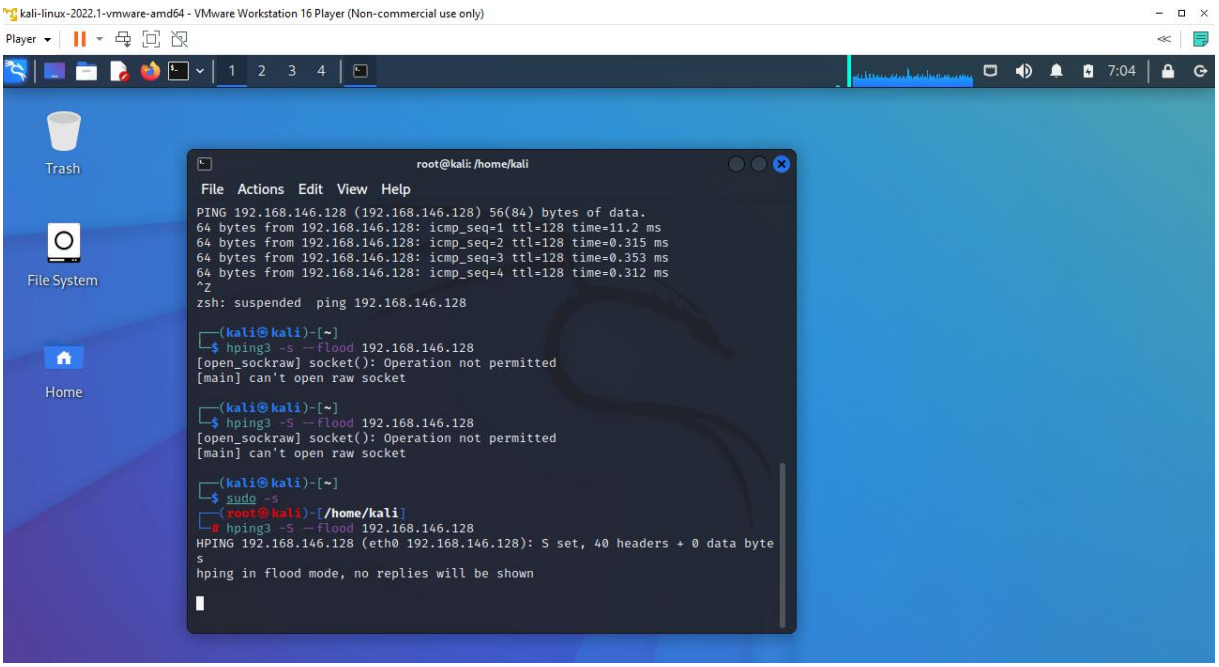
Step 5: Preview the files by double-clicking them.



Practical No. 5A

Step 1: check the ip address of virtual testing pc. And open the Wireshark Network Analyser tool.
Step 2: open another virtual installed kali linux on it.
Step 3: write command to do a Dos attack by network flood.
Step 4: sudo apt-get install hping3
Step 5: hping3 -c 15000 -d 120 -S -w 64 -p 80 --flood --rand-source 192.168.1.159

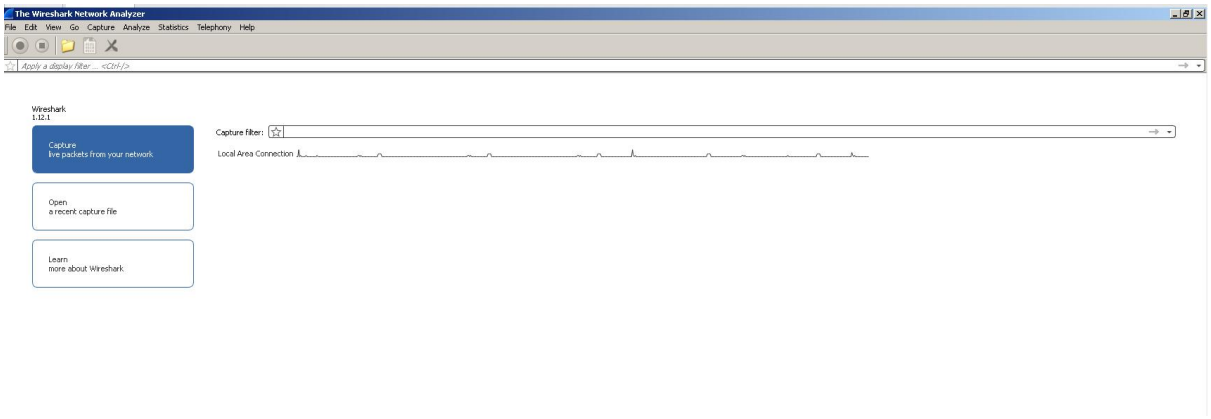




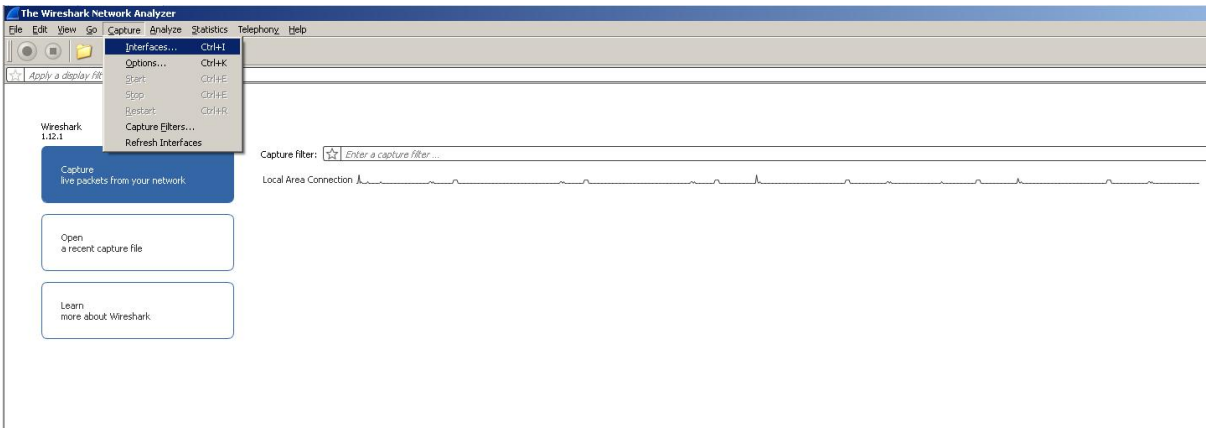
Practical No. 5B

Aim: Using Traffic Capturing and Analysis tools . [wireshark]

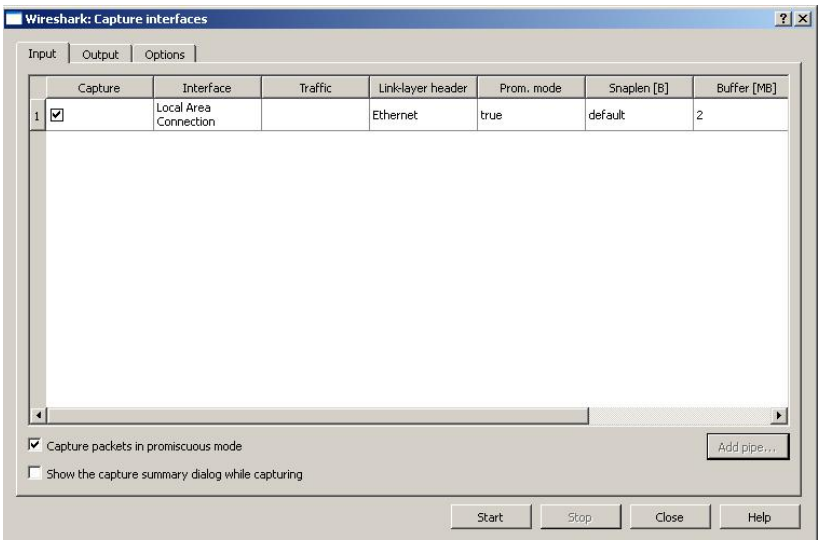
Step 1: open the wireshark

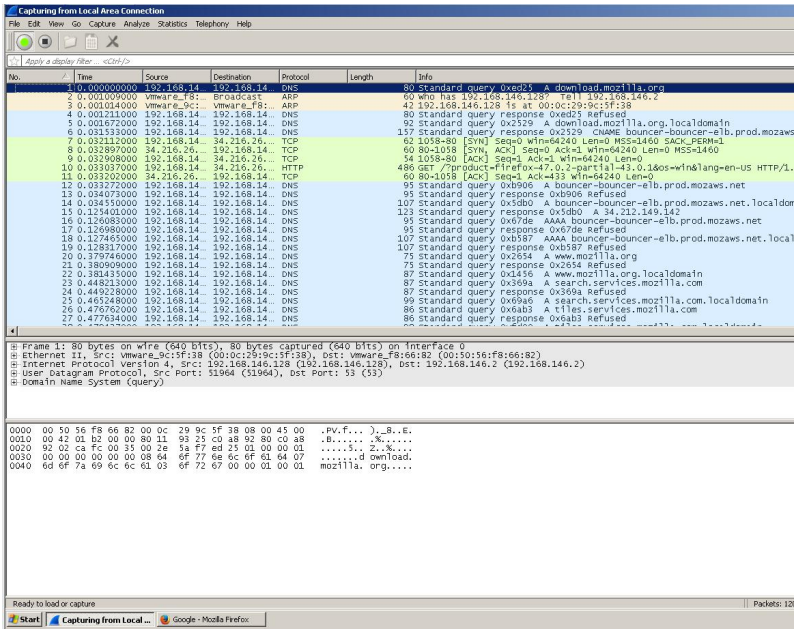


Step 2: On menu bar select Capture. Select interfaces.

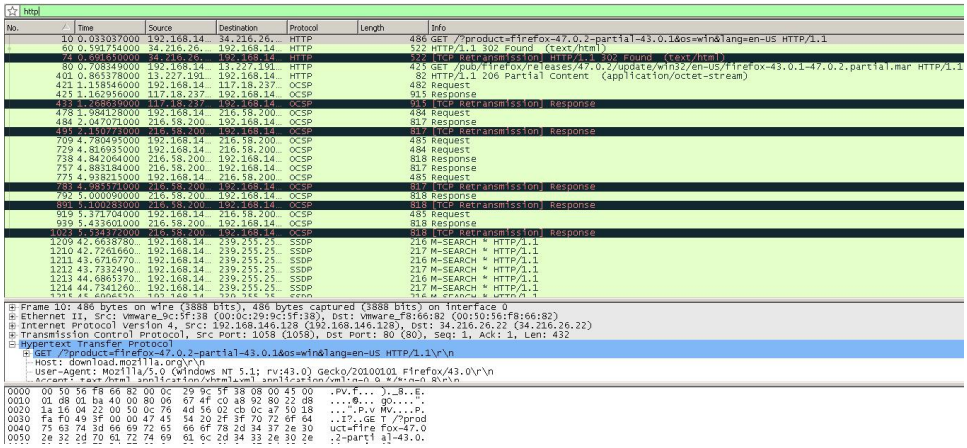


Step 3: Select Once you click on start, then Wireshark starts to capture the packets on that interface.

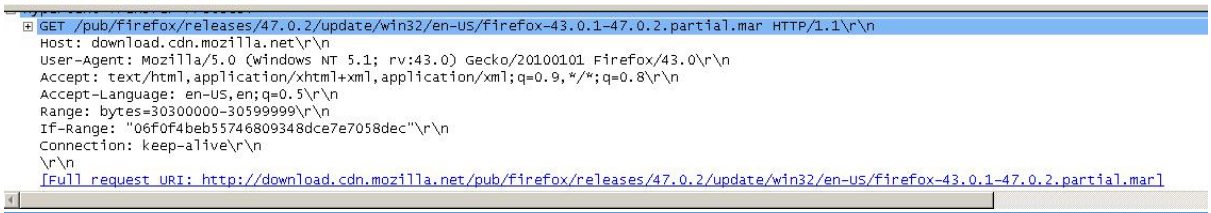




Step 4: Filter packets with HTTP protocol.

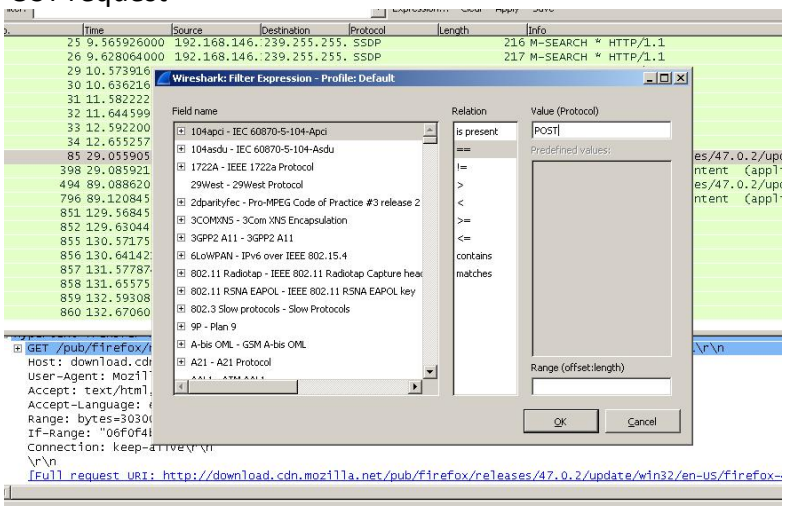


Step 5: A file with only text:
https://vulms.vu.edu.pk/Courses/SOC101/Downloads/Introduction%20to%20Sociology%20-%20SOC101.pdf



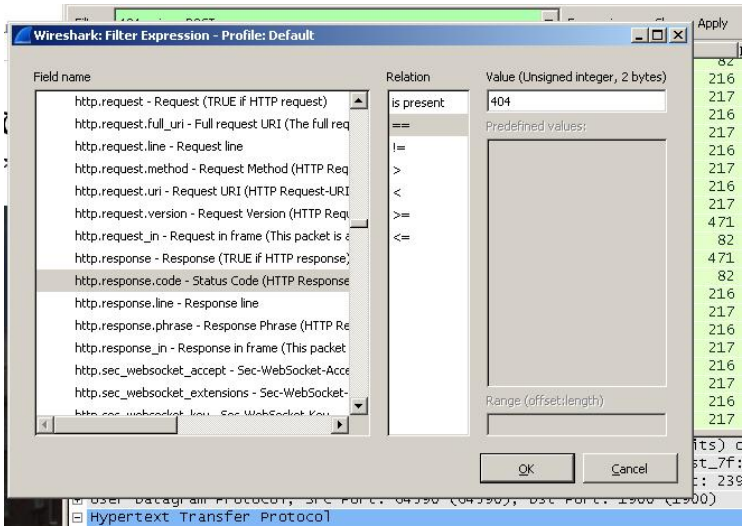
Step 6: Applying different filters using expressions.

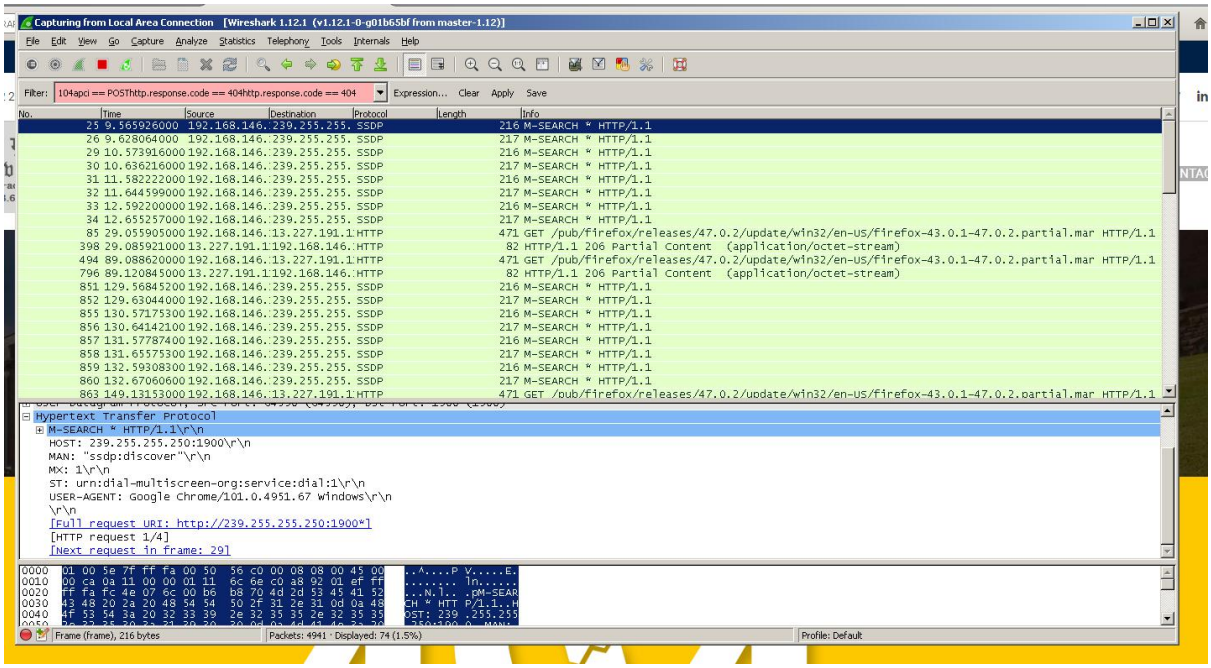
1) Filtering HTTP POST request

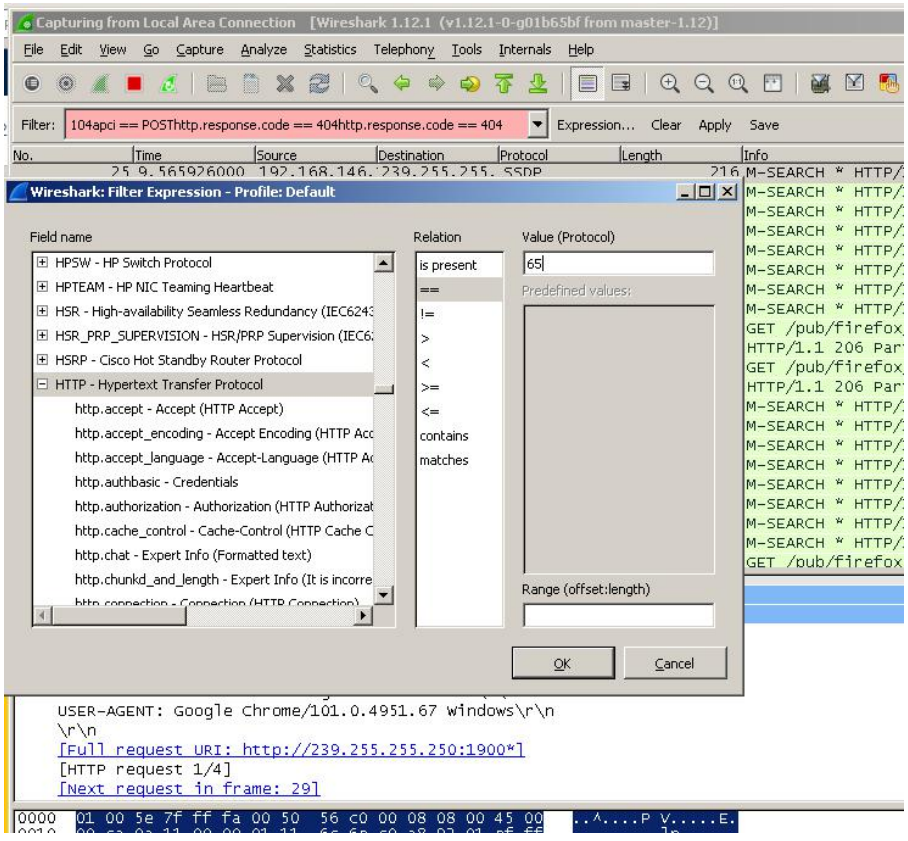


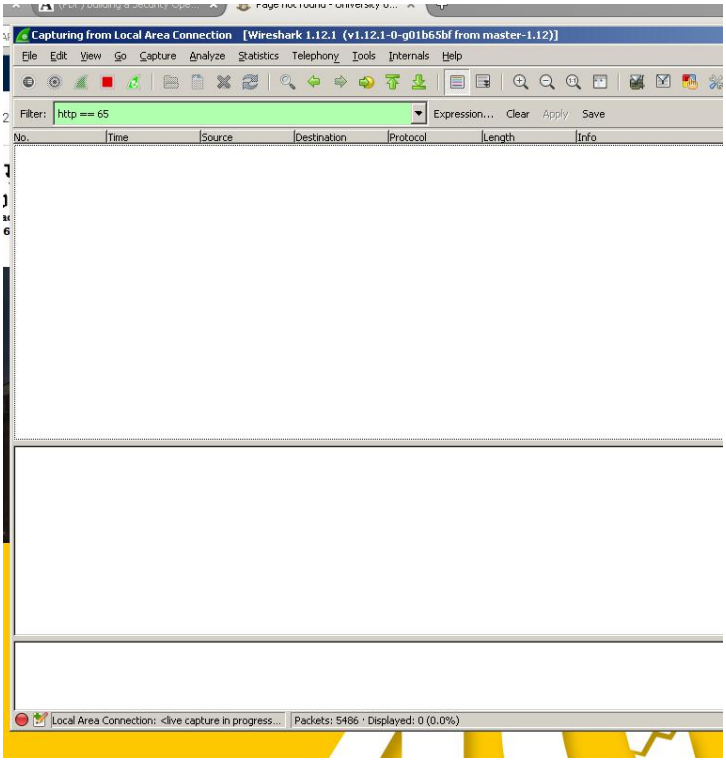
2) Filtering 404 not found error

Same under expression go to HTTP and expand that and select the status code.




Capturing from Local Area Connection [Wireshark 1.12.1 (v1.12.1-0-g01b65bf from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: 104apci == POSThttp.response.code == 404http.response.code == 404
Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
25 9.565926000 192.168.146.239.255.255.255. SSDP 216 M-SEARCH * HTTP/1.1
26 9.628064000 192.168.146.239.255.255.255. SSDP 217 M-SEARCH * HTTP/1.1
29 10.573916000 192.168.146.239.255.255.255. SSDP 216 M-SEARCH * HTTP/1.1
30 10.636216000 192.168.146.239.255.255.255. SSDP 217 M-SEARCH * HTTP/1.1
31 11.582222000 192.168.146.239.255.255.255. SSDP 216 M-SEARCH * HTTP/1.1
32 11.644599000 192.168.146.239.255.255.255. SSDP 217 M-SEARCH * HTTP/1.1
33 12.592200000 192.168.146.239.255.255.255. SSDP 216 M-SEARCH * HTTP/1.1
34 12.655257000 192.168.146.239.255.255.255. SSDP 217 M-SEARCH * HTTP/1.1
85 29.055905000 192.168.146.13.227.191.1 HTTP 471 GET /pub/firefox/releases/47.0.2/update/win32/en-US/firefox-43.0.1-47.0.2.partial.mar HTTP/1.1
398 29.085921000 13.227.191.1 192.168.146. HTTP 82 HTTP/1.1 206 Partial Content (application/octet-stream)
494 89.088620000 192.168.146.13.227.191.1 HTTP 471 GET /pub/firefox/releases/47.0.2/update/win32/en-US/firefox-43.0.1-47.0.2.partial.mar HTTP/1.1
796 89.120845000 13.227.191.1 192.168.146. HTTP 82 HTTP/1.1 206 Partial Content (application/octet-stream)
851 129.56845200 192.168.146.239.255.255.255. SSDP 216 M-SEARCH * HTTP/1.1
852 129.63044000 192.168.146.239.255.255.255. SSDP 217 M-SEARCH * HTTP/1.1
855 130.57175300 192.168.146.239.255.255.255. SSDP 216 M-SEARCH * HTTP/1.1
856 130.64142100 192.168.146.239.255.255.255. SSDP 217 M-SEARCH * HTTP/1.1
857 131.57787400 192.168.146.239.255.255.255. SSDP 216 M-SEARCH * HTTP/1.1
858 131.65575300 192.168.146.239.255.255.255. SSDP 217 M-SEARCH * HTTP/1.1
859 132.59308300 192.168.146.239.255.255.255. SSDP 216 M-SEARCH * HTTP/1.1
860 132.67060600 192.168.146.239.255.255.255. SSDP 217 M-SEARCH * HTTP/1.1
863 149.13153000 192.168.146.13.227.191.1 HTTP 471 GET /pub/firefox/releases/47.0.2/update/win32/en-US/firefox-43.0.1-47.0.2.partial.mar HTTP/1.1
Hypertext Transfer Protocol
M-SEARCH * HTTP/1.1\r\n
HOST: 239.255.255.250:1900\r\n
MAN: "ssdp:discover"\r\n
MX: 1\r\n
ST: urn:dial-multiscreen-org:service:dial:1\r\n
USER-AGENT: Google Chrome/101.0.4951.67 Windows\r\n
\r\n
[Full request URI: http://239.255.255.250:1900*]
[HTTP request 1/4]
[Next request in frame: 29]
0000 01 00 5e 7f ff fa 00 50 56 c0 00 08 08 00 45 00 ..^....P V.....E.
0010 00 ca 0a 11 00 00 01 11 6c 6e c0 a8 92 01 ef ff .... ln.....
0020 ff fa fc 46 07 6c 00 b6 b8 70 4d 20 53 45 41 52 ...N.l.. .pM-SEAR
0030 43 48 20 2a 20 48 54 54 50 2f 31 2e 31 0d 0a 48 CH * HTT P/1.1..H
0040 4f 53 54 3a 20 32 33 39 2e 32 35 35 2e 32 35 35 OST: 239 .255.255
Frame (frame), 216 bytes
Packets: 4941 · Displayed: 74 (1.5%)
Profile: Default


Capturing from Local Area Connection [Wireshark 1.12.1 (v1.12.1-0-g01b65bf from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: 104apci == POSThttp.response.code == 404http.response.code == 404
Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
Wireshark: Filter Expression - Profile: Default
Field name
Relation
Value (Protocol)
HPSW - HP Switch Protocol
HPTEAM - HP NIC Teaming Heartbeat
HSR - High-availability Seamless Redundancy (IEC624
HSR_PRP_SUPERVISION - HSR/PRP Supervision (IEC6
HSRP - Cisco Hot Standby Router Protocol
HTTP - Hypertext Transfer Protocol
http.accept - Accept (HTTP Accept)
http.accept_encoding - Accept Encoding (HTTP Acc
http.accept_language - Accept-Language (HTTP A
http.authbasic - Credentials
http.authorization - Authorization (HTTP Authorizat
http.cache_control - Cache-Control (HTTP Cache C
http.chat - Expert Info (Formatted text)
http.chunkd_and_length - Expert Info (It is incorre
is present
==
!=
>
<
>=
<=
contains
matches
65
Predefined values:
Range (offset:length)
OK
Cancel
USER-AGENT: Google Chrome/101.0.4951.67 Windows\r\n
\r\n
[Full request URI: http://239.255.255.250:1900*]
[HTTP request 1/4]
[Next request in frame: 29]
0000 01 00 5e 7f ff fa 00 50 56 c0 00 08 08 00 45 00 ..^....P V.....E.

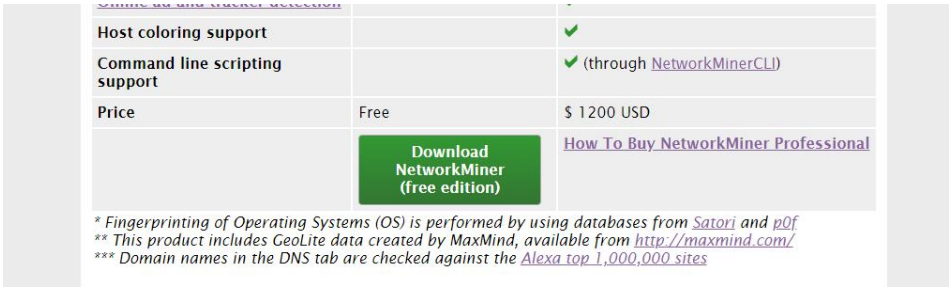

Capturing from Local Area Connection [Wireshark 1.12.1 (v1.12.1-0-g01b65bf from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: http == 65
Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
Local Area Connection: <live capture in progress...
Packets: 5486 · Displayed: 0 (0.0%)

Practical No. 5C

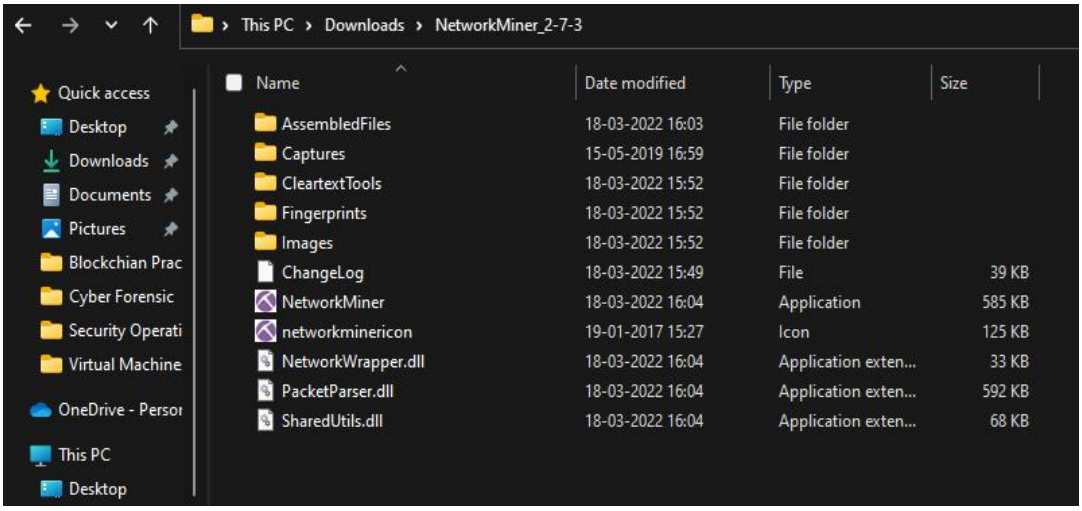
Aim: Using Network Forensic Analysis Tool NetworMiner

Part 1: Install NetworkMiner.

Step 1: download the zip file from the official web link: https://www.netresec.com/?page=NetworkMiner

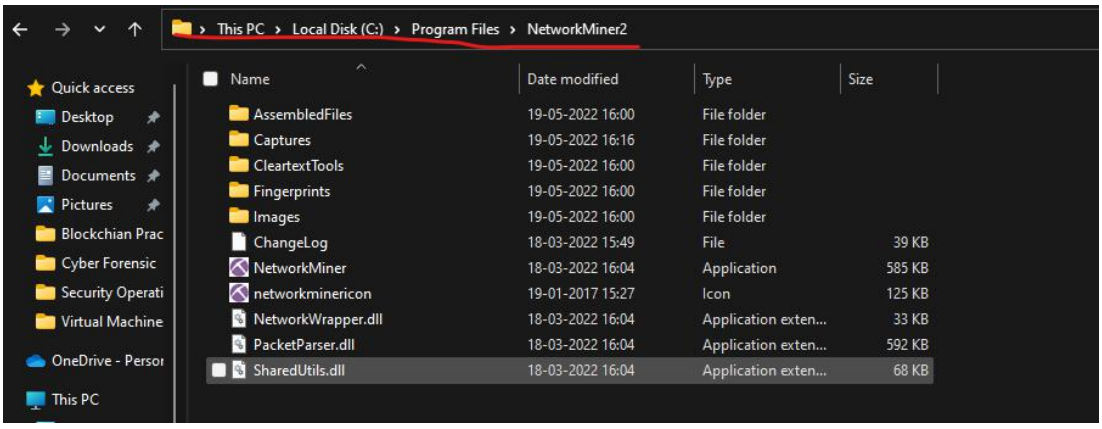


Step 2: after download we need to extract the file.subfiles look like this

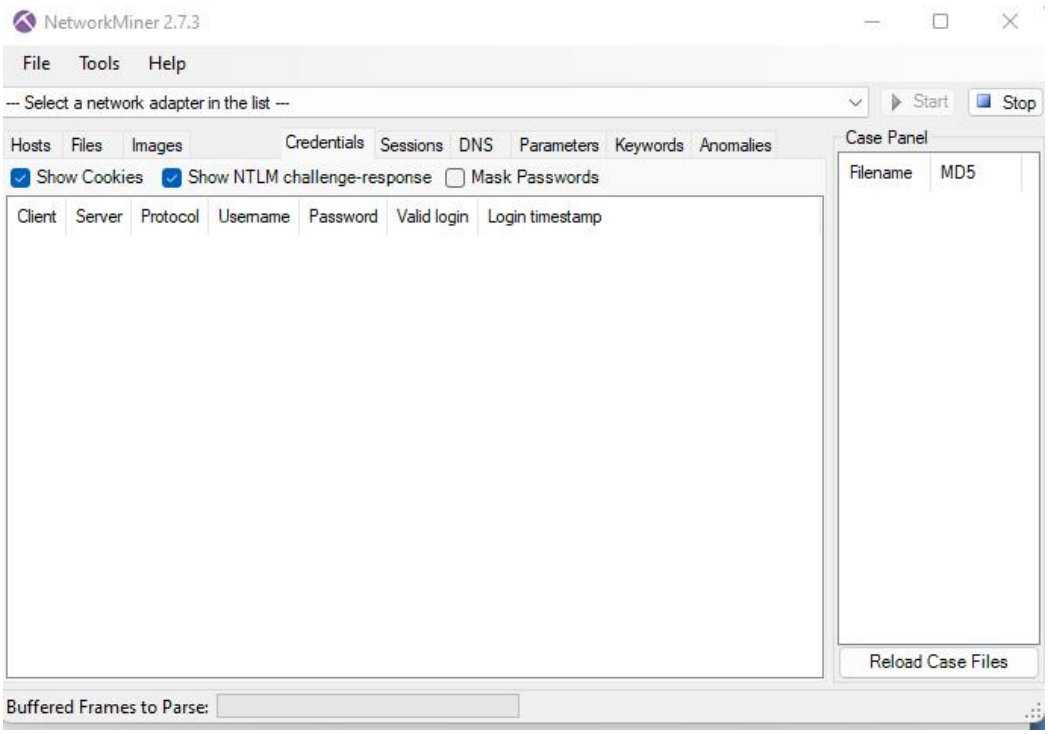


Step 3: Now we need to copy all the files and copy the move to the

C:\Program Files\NetworkMine2 (Create new folder name NetwoekMiner) and paste it that folder.

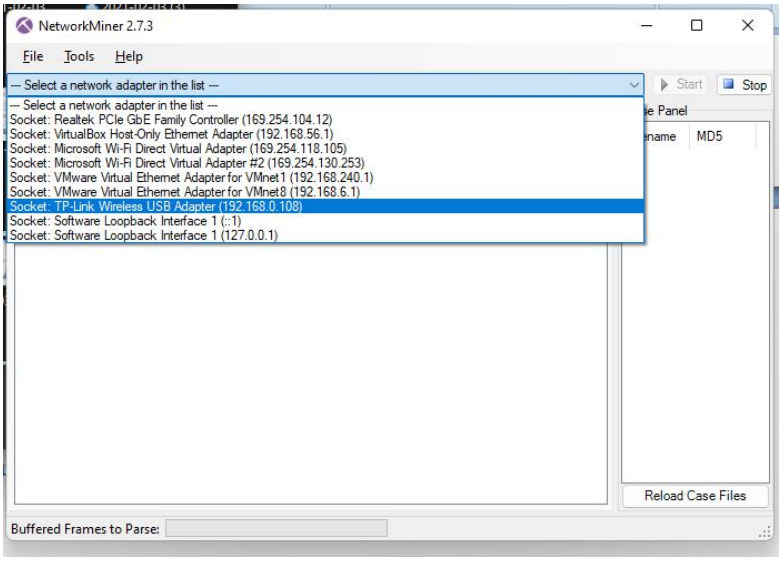


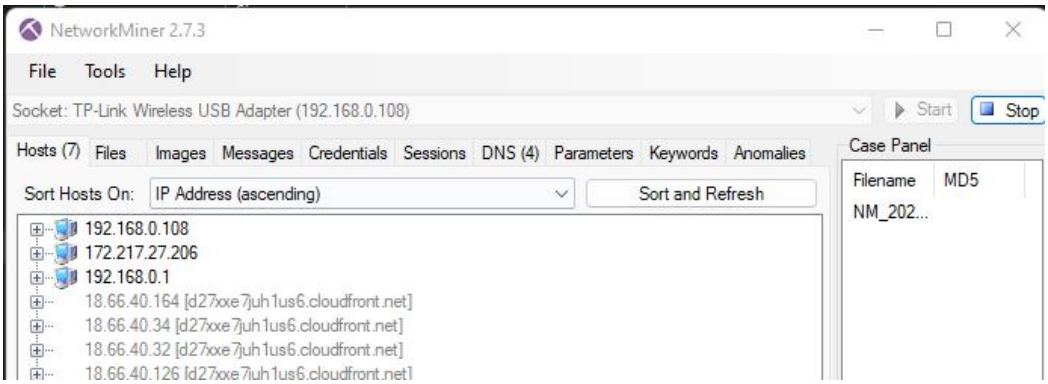
Step 4: Now open the application with open as Admin and interface look ike this.



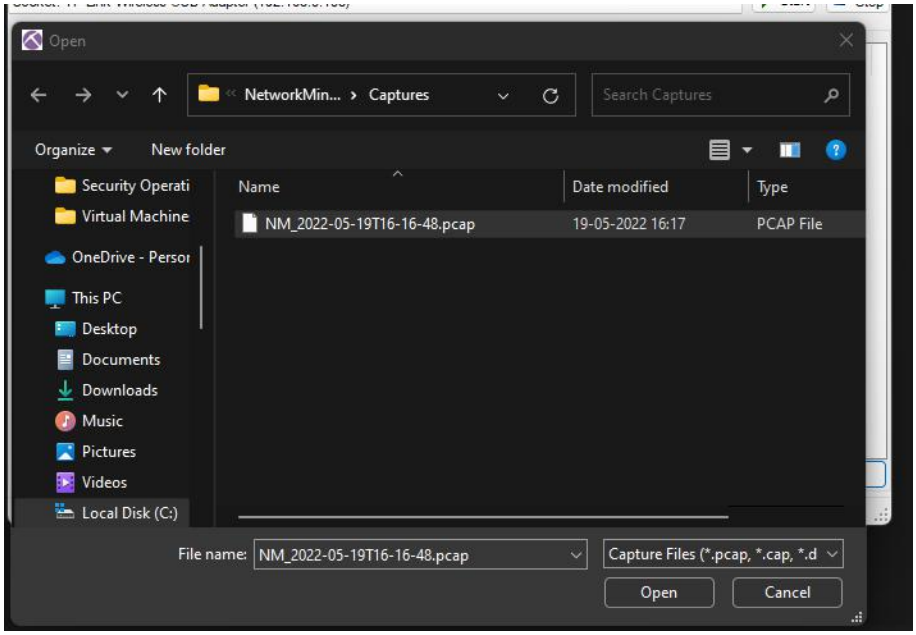
Part 2: Using the NetworkMiner for 1st use.

Step1: choose your network adapter from the top of the window.

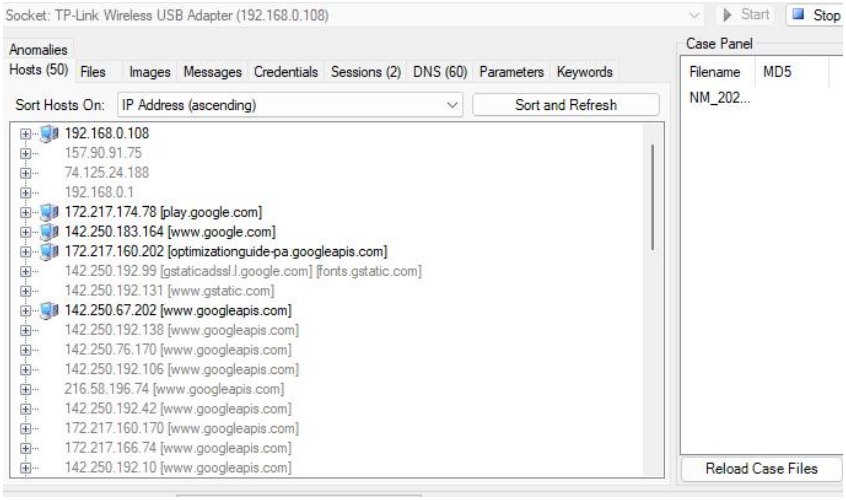




Step 2: Or if you want to open the previous packet captured so open the pcap file.



Step 3: after open the pcap file it will load all packet information which is captured.



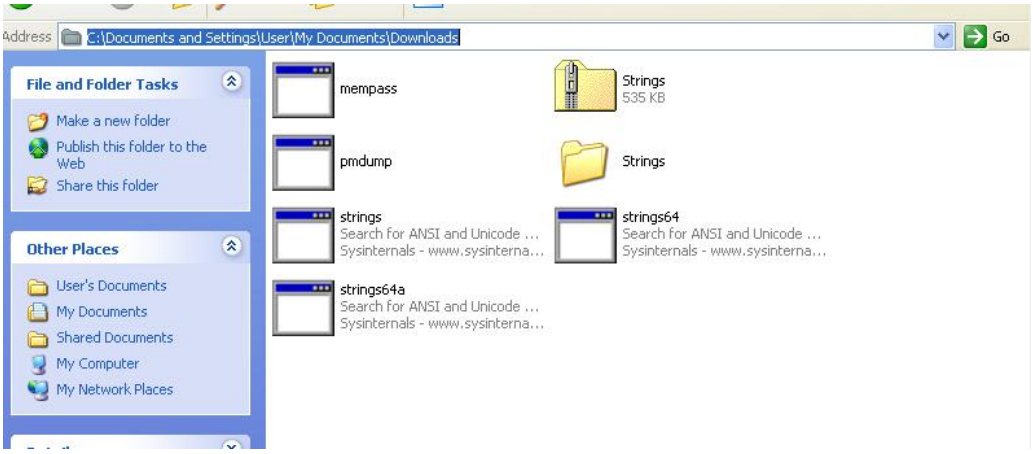
Practical No. 6

Aim: Dump Memory contents using PMdump.

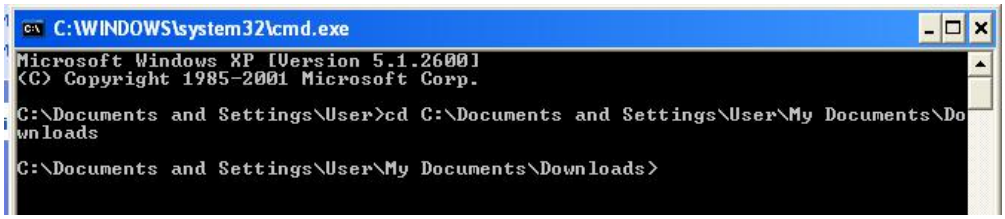
Step 1: Download all the required files. Links are given bellow:

Pmdump – https://dl.packetstormsecurity.net/Win2k/pmdump.exe
Mempass - http://code.securitytube.net/mempass.exe
Strings - https://download.sysinternals.com/files/Strings.zip

Step 2: Save all the files in same folder.

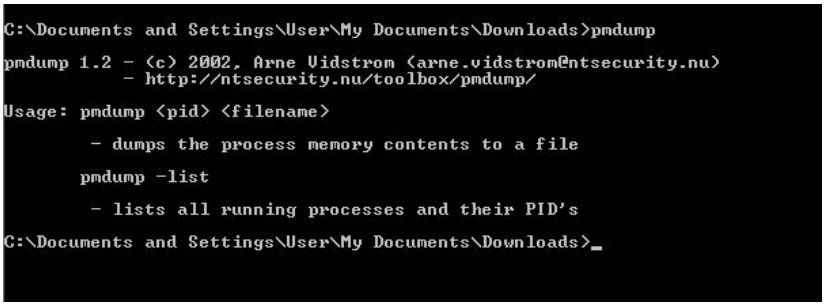


Step 3: open cmd and go to the folder were you have downloaded all the files.



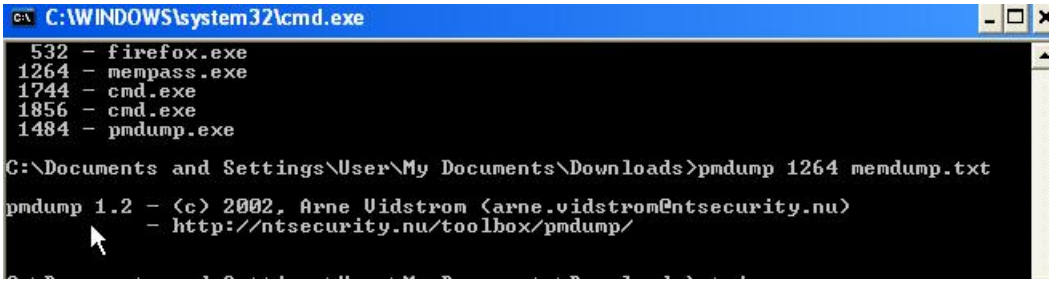
Step 4: run the command “mempass.exe” and create password

Step 5: then type pmdump

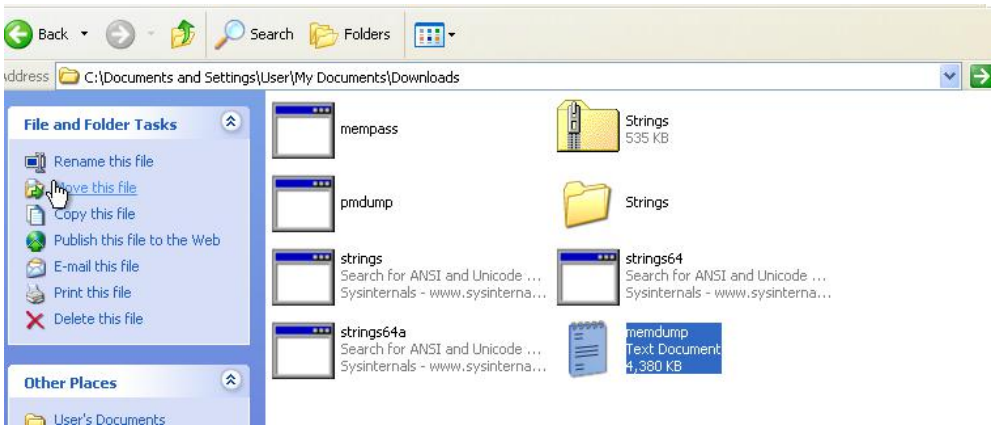


Step 6: type “pmdump –list” and chech for the process id for mempass.exe

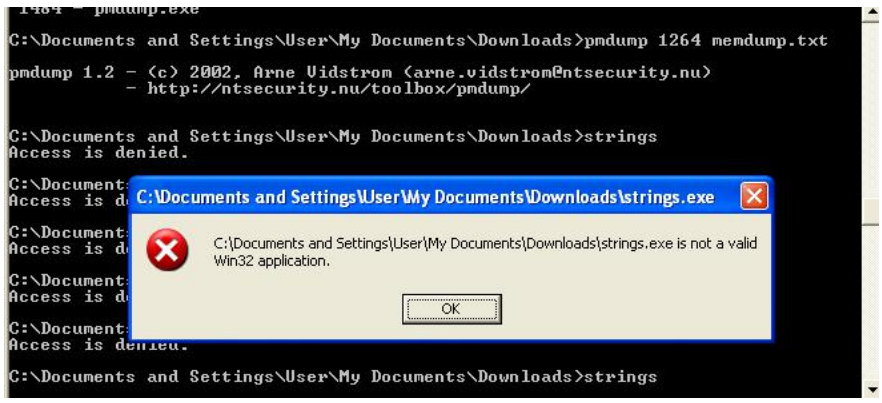
Step 7: type “pmdump 1264 memdump.txt” it will save the log into text file.



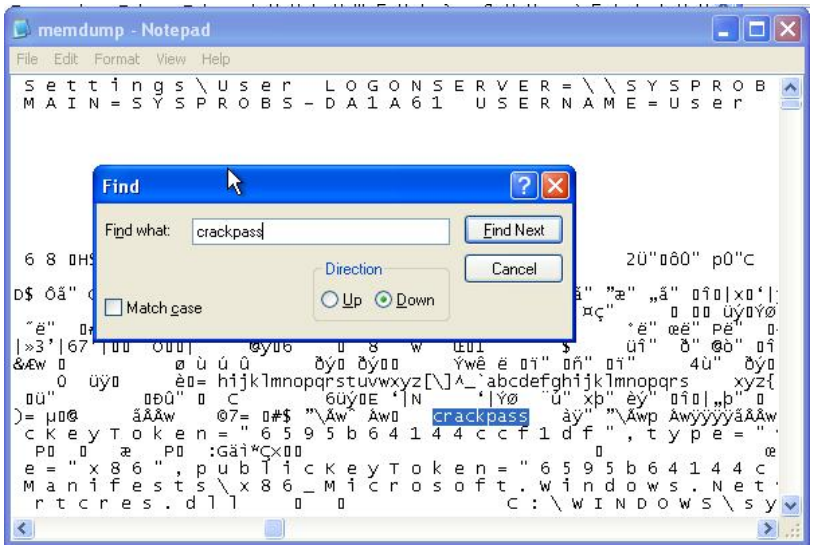
Step 8: txt file is saved in local drive.



Step 9: now we run the strings command but here we are getting some error. It is not possible to go with this process.



Step 10: So simply we open the txt file and search for the password we createdat the time of mempass.exe file running in cmd.

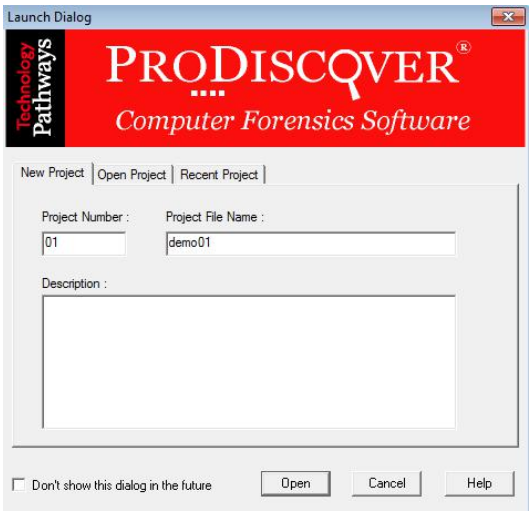


Practical No. 7

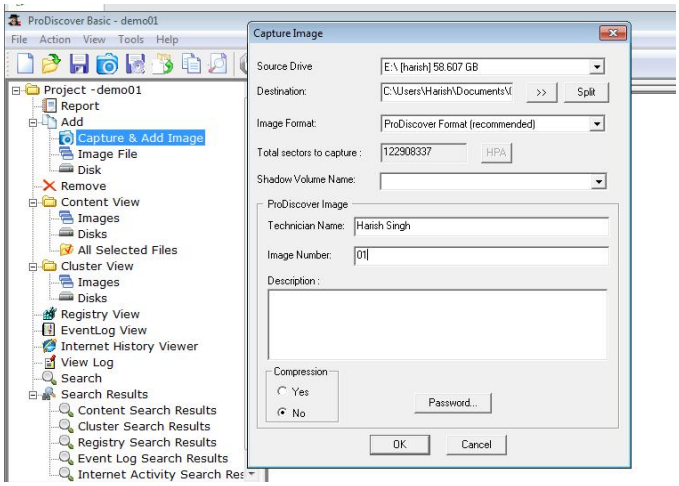
Aim: Using Data Acquisition Tools [ProDiscover Pro]

Solution:

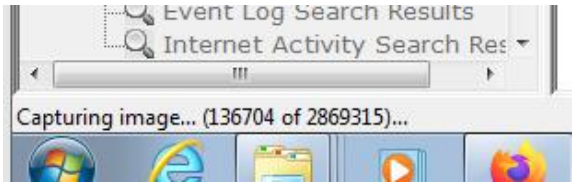
Step 1: open the ProDiscover and add the case number and name.

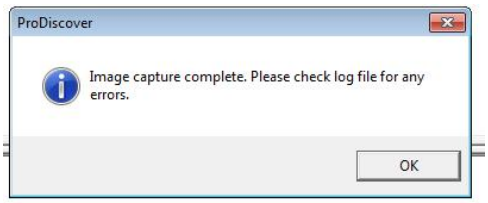


Step 2:open the project and click on Add then select the capture&Add image.fil all the detail as shown in the snap.

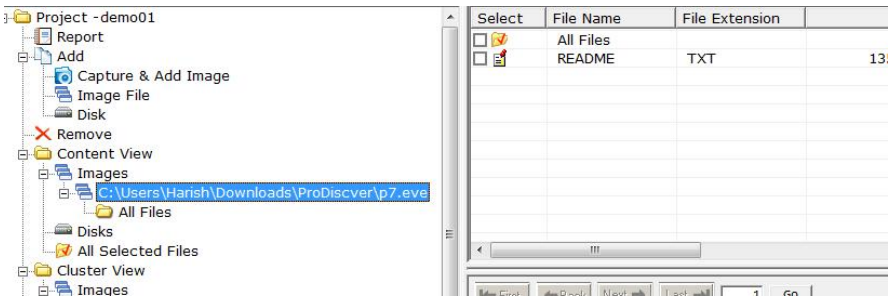


Step 3: After clicking ok image should be created.

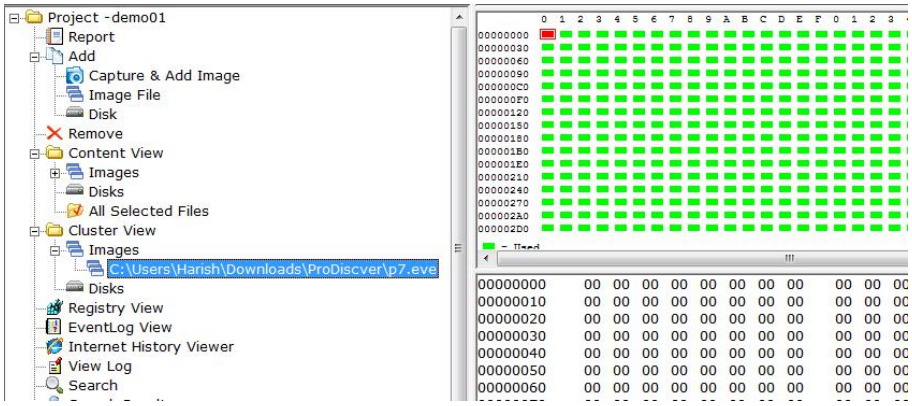




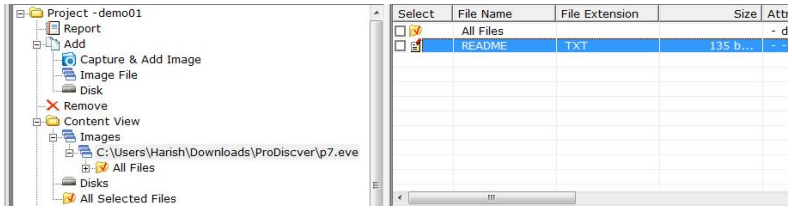
Step 4: After complete of image creation. please check the log file for any error. For that go to content view and click image.



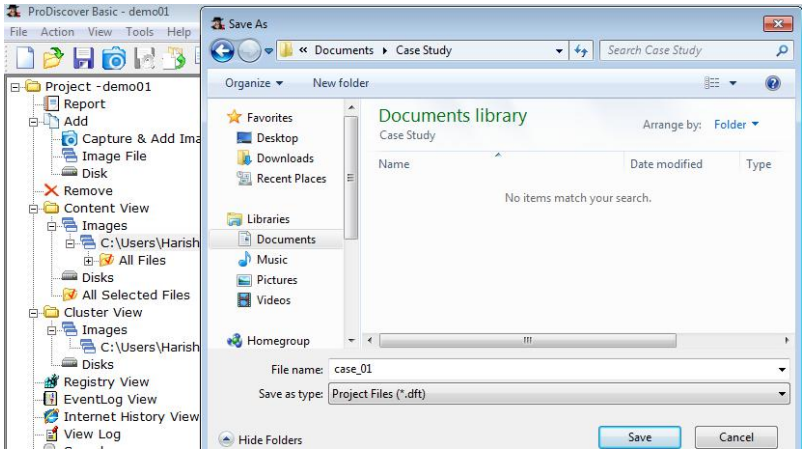
Step 5: you can also see the cluster view file has been created.



Step 6: we can view the file of PanDrive as we created he image.



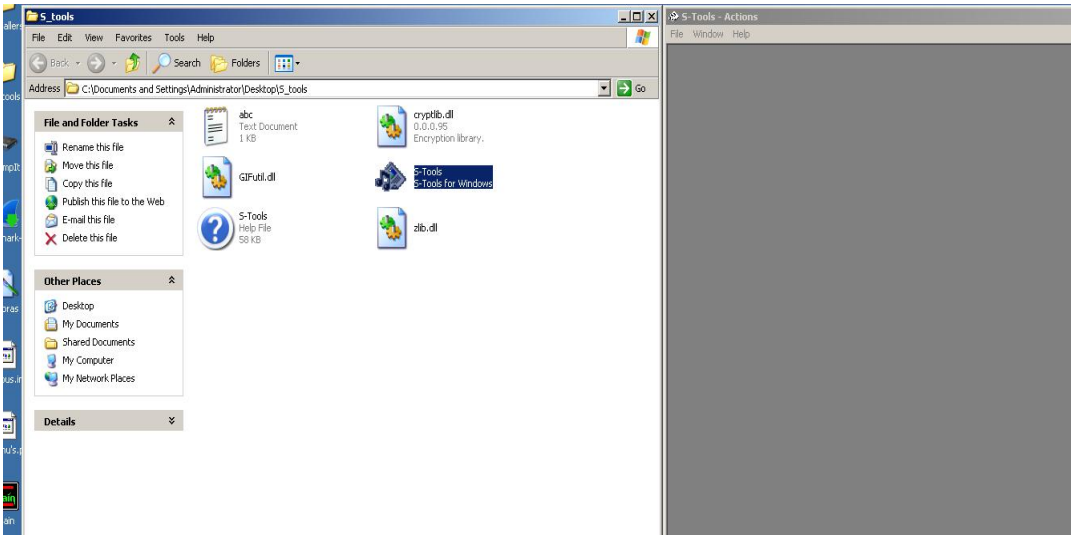
Step 7: At last we need to save the CaseFile.



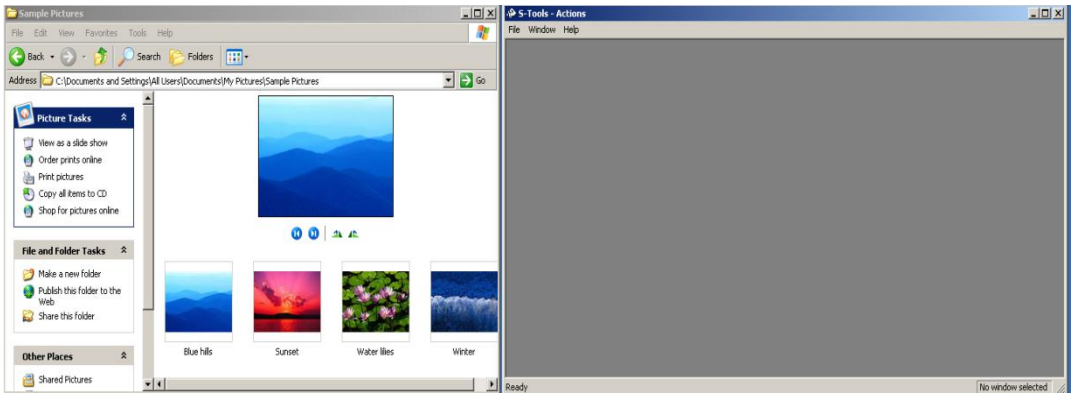
Practical No. 8 A

Following steps Show how to use freeware S-Tools utility to hide and reveal files inside pictures

Step 1) Select the S-Tools.exe file and open the steganography software tool.



Step 2) With both the working directory and the S-Tools program open minimize both windows and place side-by-side



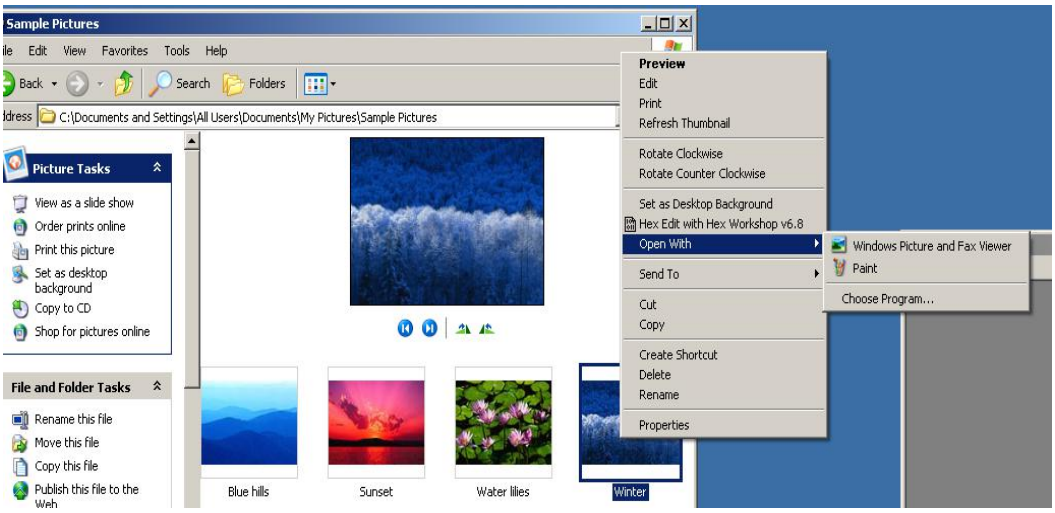
The S-Tools program is a drag and drop software. The files used to create the steganography file can be dragged from the directory into the S-Tools program.

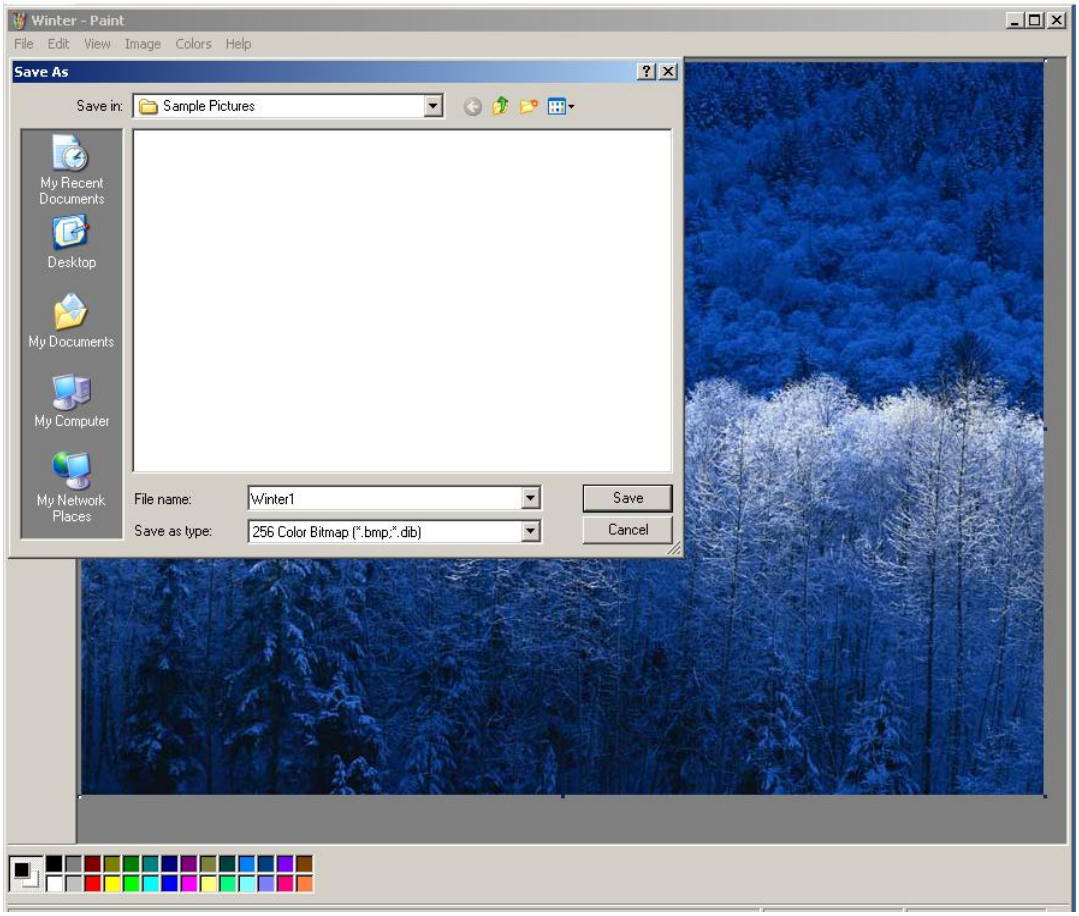
Step 3) Select the file from the directory and drag it over the S-Tools main window and release the file.

A dialogue box appears indicating that the file type is unknown. Supported file types for audio and image files are shown below:

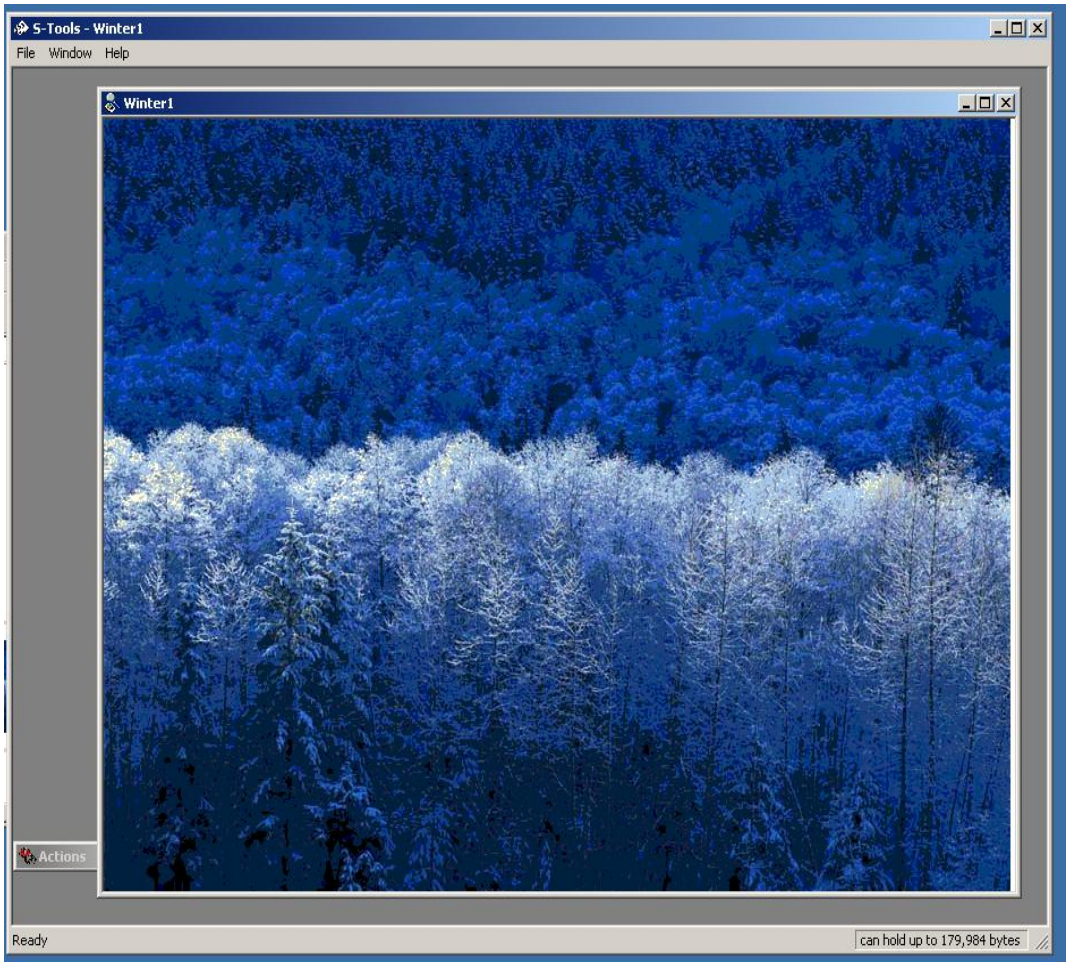
- Audio - *.wav
- Image - *.bmp and *.gif

If your image is in .jpg format, convert it to .bmp format by doing the following steps using Paint:

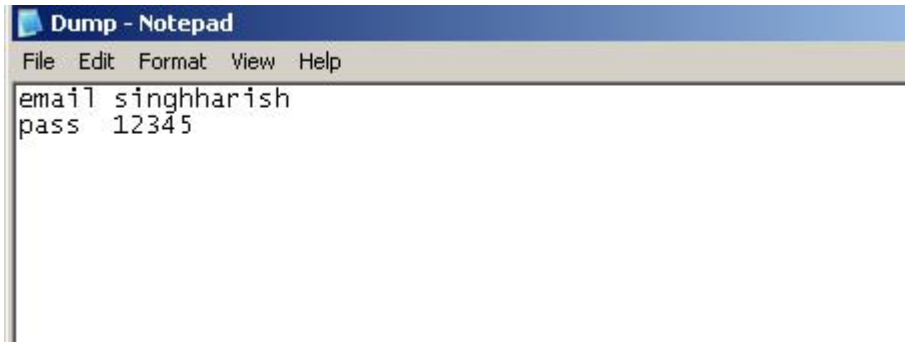




Step 4) Select a valid audio file or image as the base file for the steganography file. The Winter1.bmp was selected and dragged onto the main window of the S-Tools program. The image is opened.

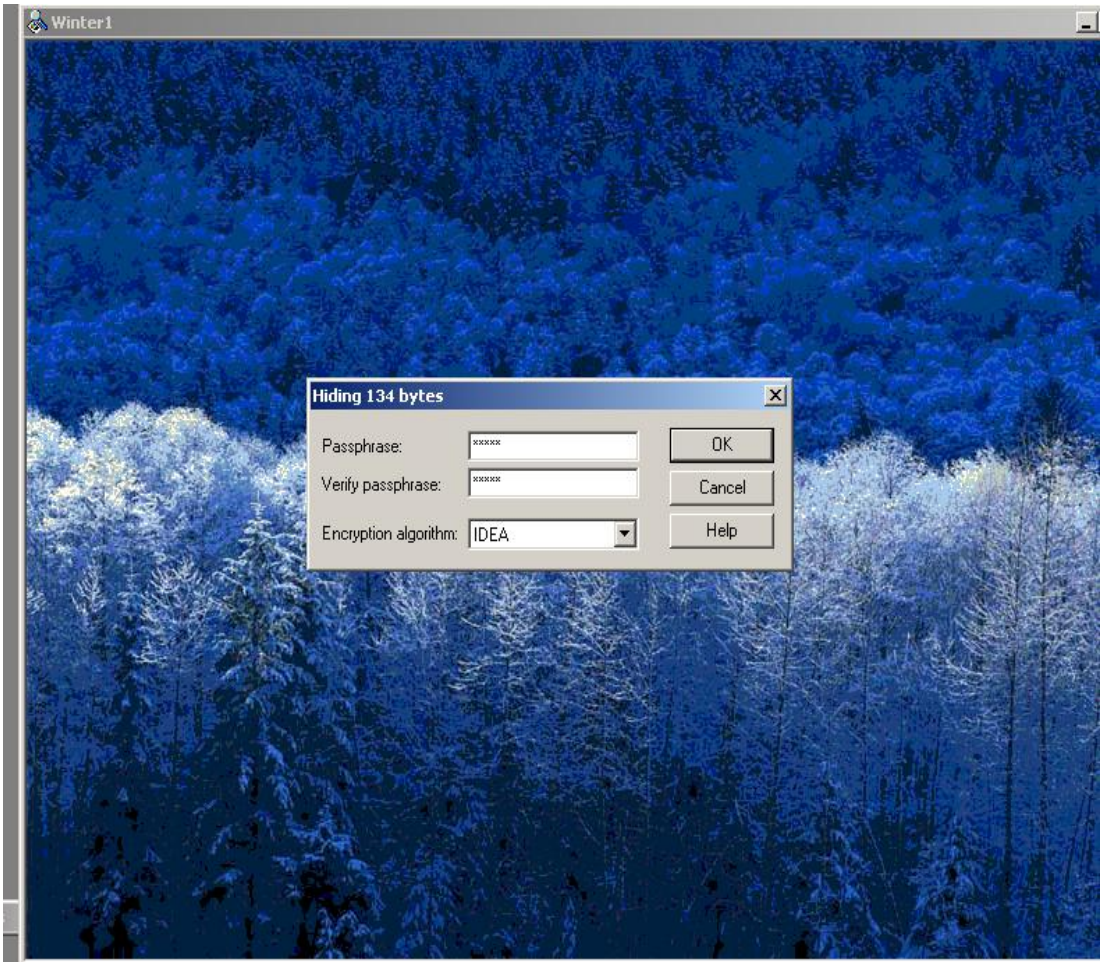


Step 5) Select a file to hide within the base file. If it's not there, create a txt file and Save the file.



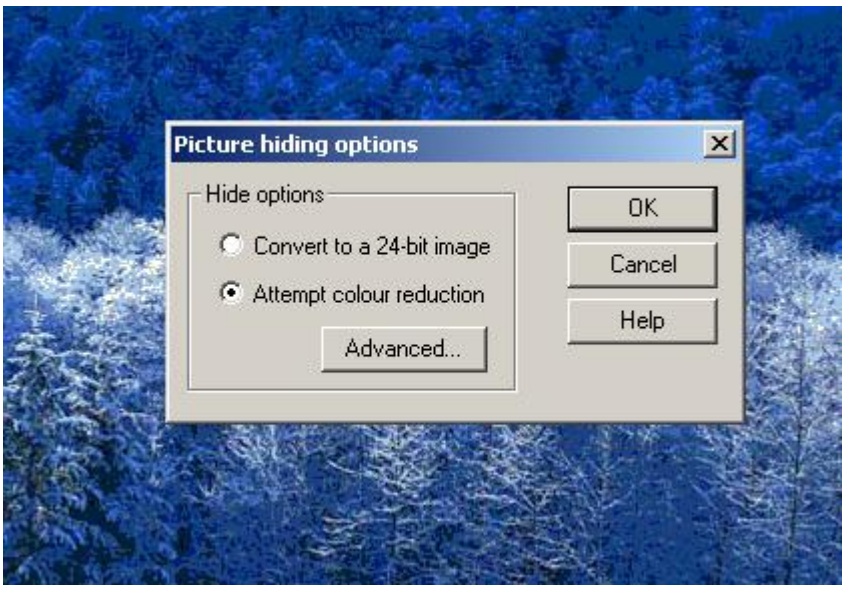
Step 6) The *.txt text file is selected and dragged on top of the base image. Release the file while the cursor is still on top of the base file.

Step 7) A dialogue box will appear asking the user to enter and verify a passphrase. Additionally, the user will have to select an encryption algorithm.

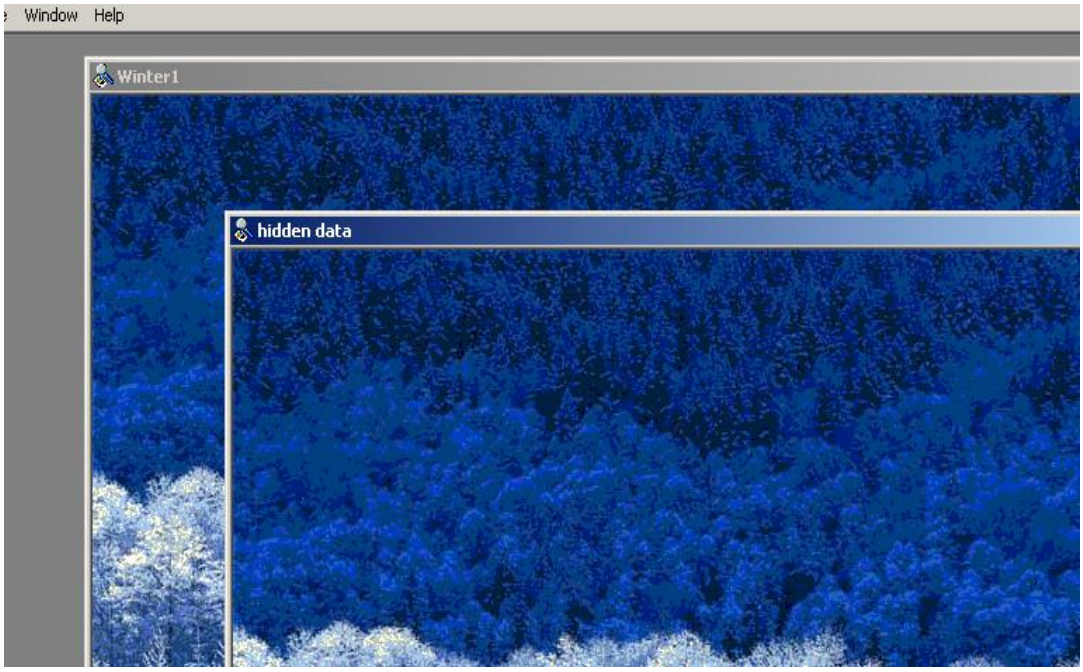


Step 8) Enter a passphrase in both the passphrase and verify passphrase text boxes. If the same passphrase is not entered in both text boxes the 'OK' button will be grayed out and the user will not be able to proceed to creating the steganography file.

Step 9) Select the 'OK' button after entering a valid passphrase.

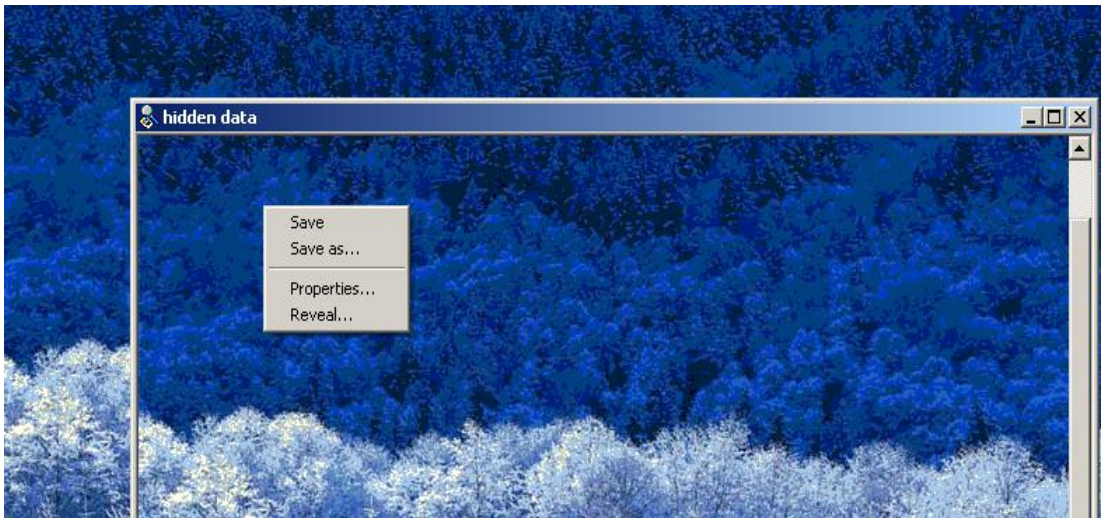


Step 10) The S-Tools main window will appear and a new file will be visible. The name of the file will be called hidden_data by default.



Step 11) Place the cursor on top of the hidden data image and select the right mouse button. The user will
have four options available to them:

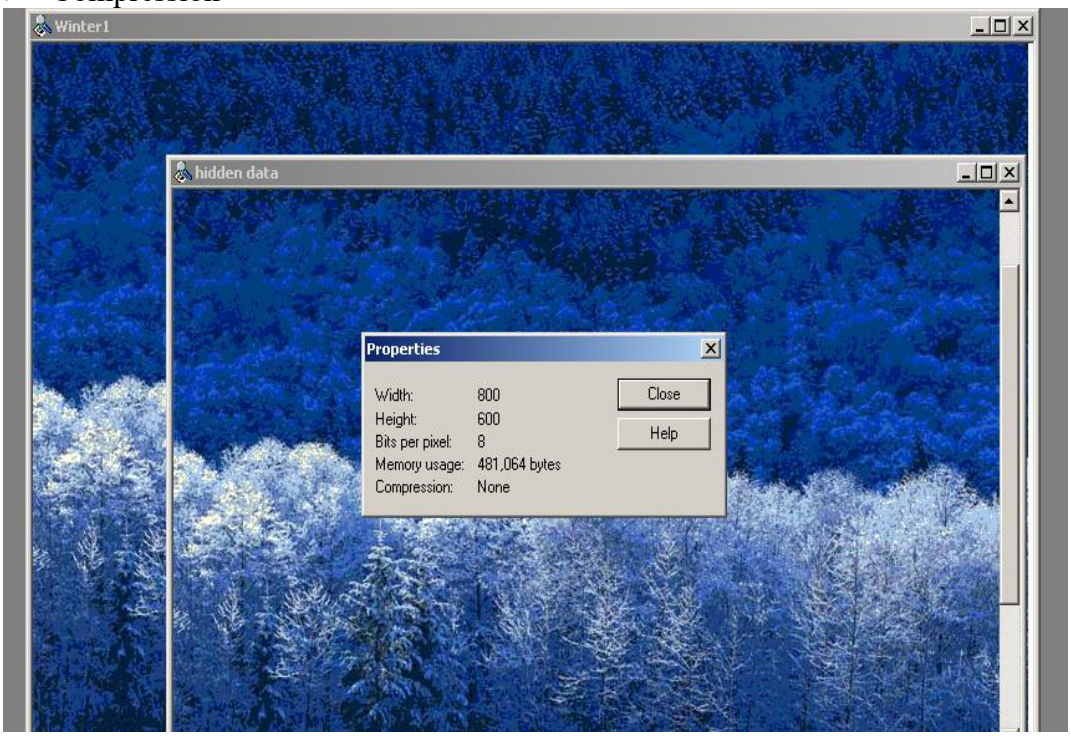
- Save
- Save As
- Properties
- Reveal



Step 12) Selecting the 'Properties' button while the cursor is over any image will display the following properties:

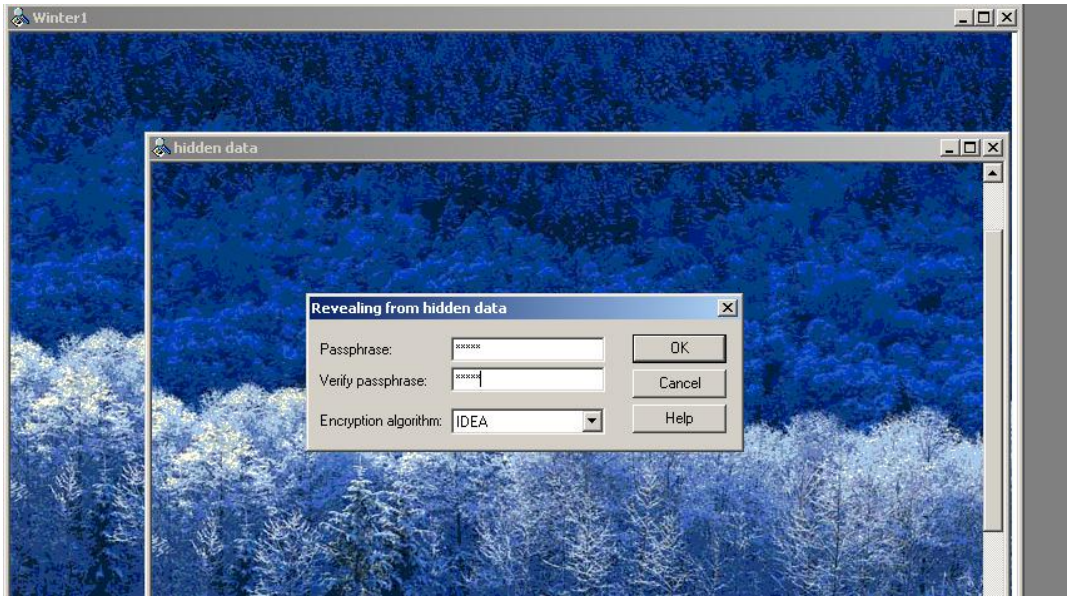
- Width and Height of the image

- Bits per pixel
- Memory Usage (file size in bytes)
- Compression

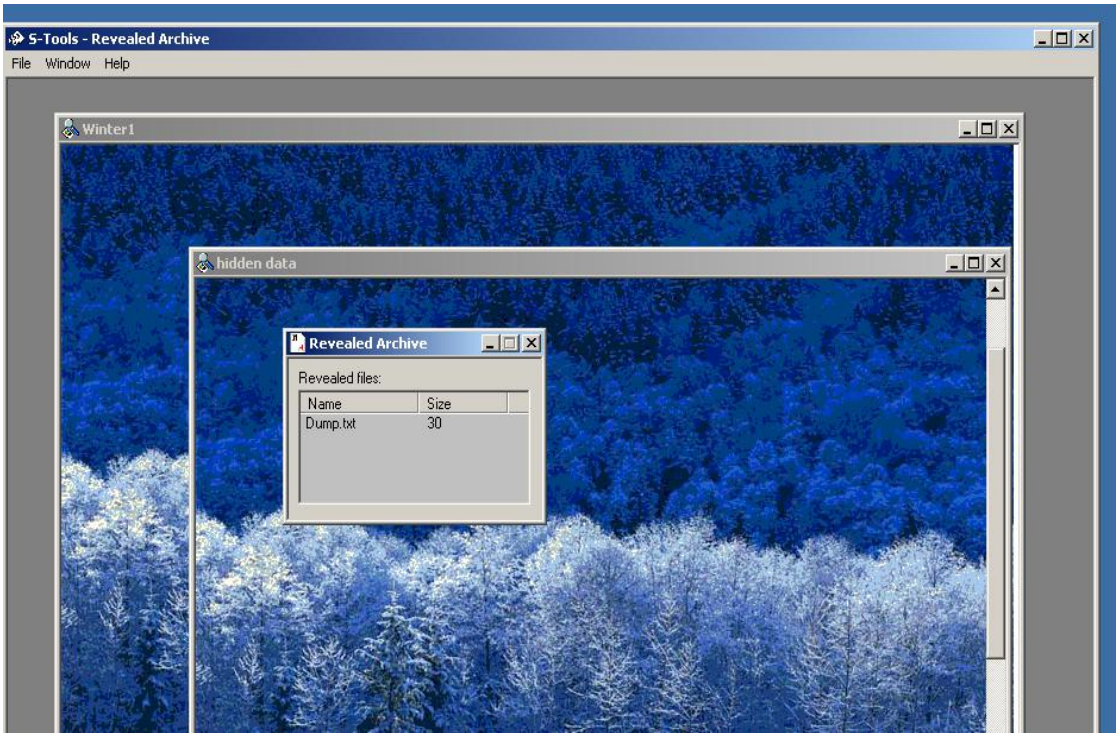


Step 13) Selecting the 'Reveal' button will display a passphrase dialogue box. A passphrase must be entered twice in the dialogue box and the correct encryption algorithm must be selected.
Notice that the title of the dialogue box has changed to 'Revealing from Tulips.bmp'

Step 14) Enter a passphrase twice, select the encryption algorithm, and select the 'OK' button.



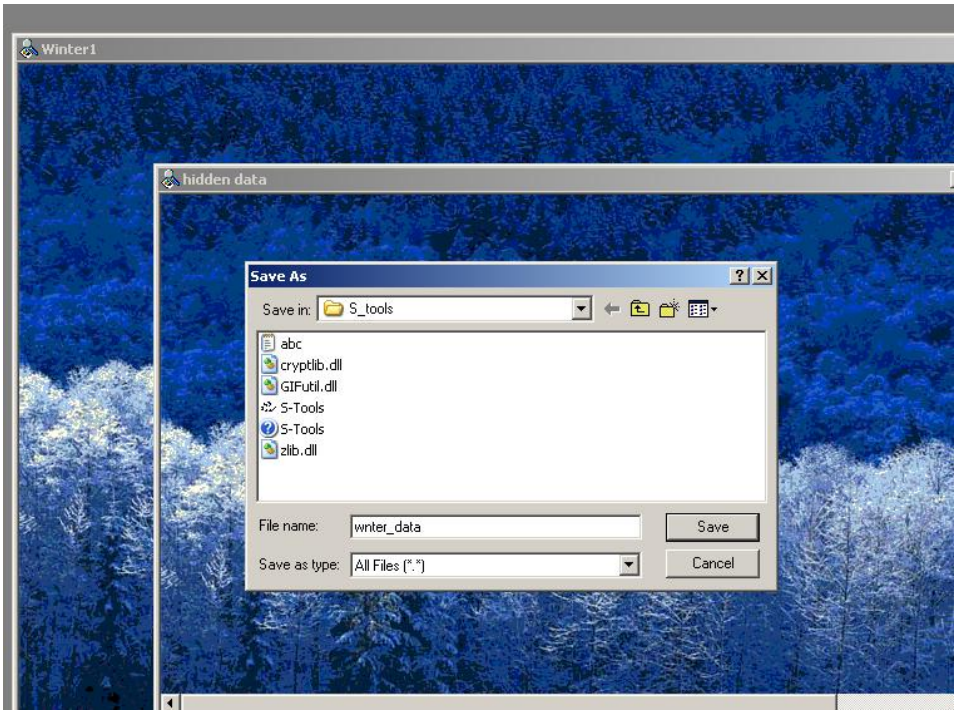
Step 15) A ‘Revealed Archive’ dialogue box will display which contains the file name and size of the hidden file.



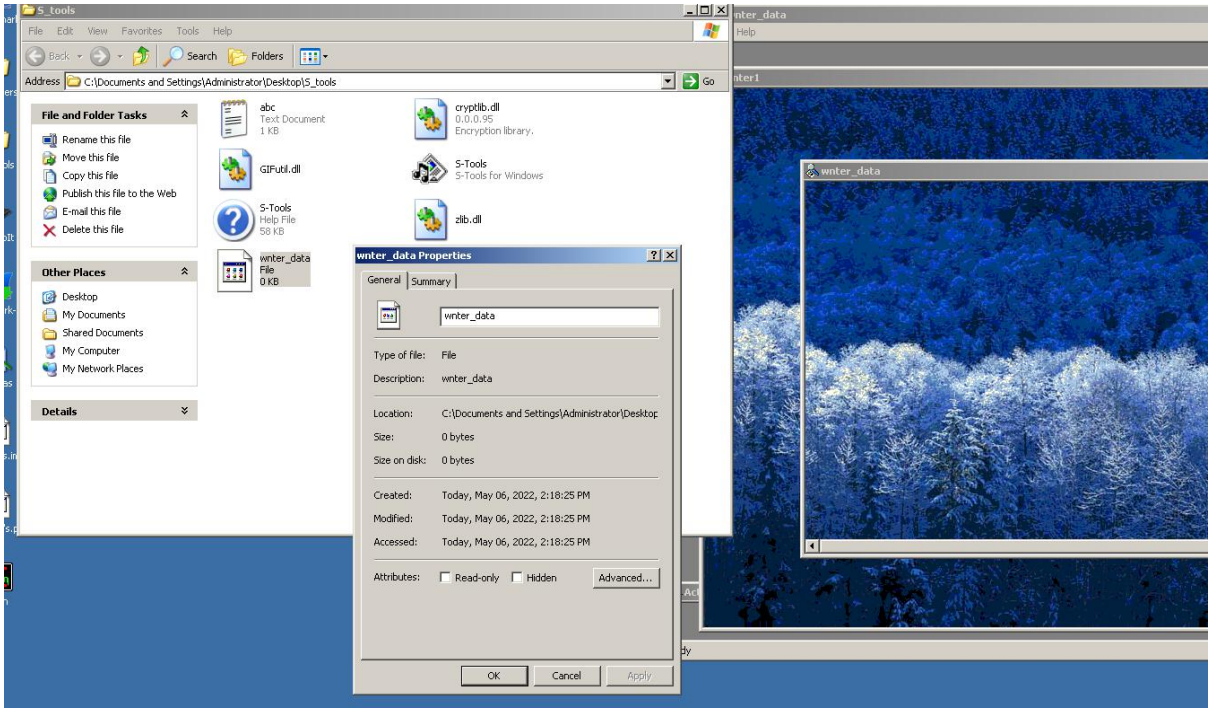
Step 16) Select the ‘Save As’ button.

Step 17) A ‘Save As’ dialogue box will appear. Enter a valid file name, select the working directory and select the ‘Save’ button.

Step 18) Locate the files in the working directory.



Step 19) Open the files using a multimedia software program and ensure that the files were extracted from the steganography file successfully.

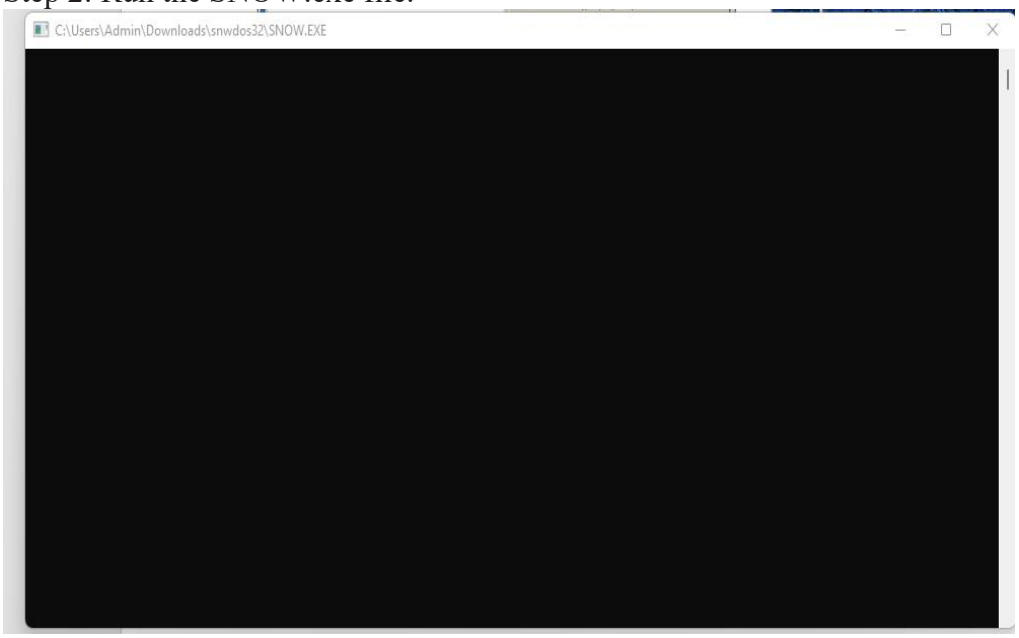


Practical No. 8B

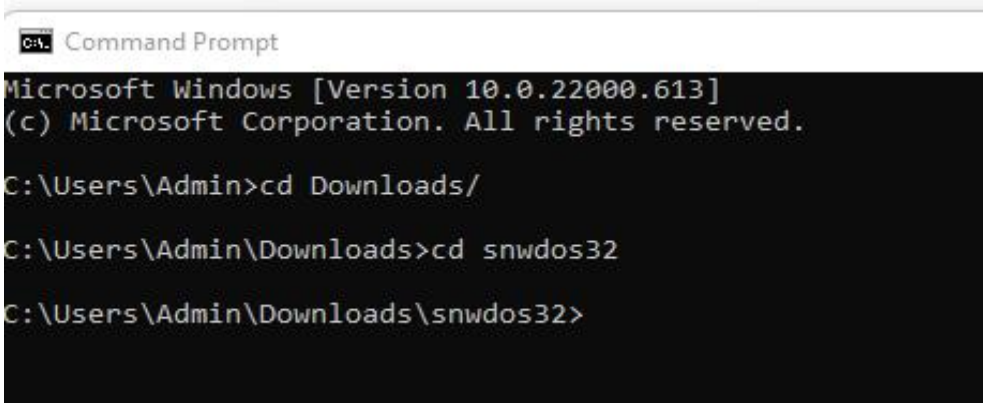
Aim: Stegnography tool SNOW.exe

SNOW is a tool that is the abbreviation of Steganographic Nature Of Whitespace which uses ICE encryption algorithm. SNOW is a whitespace steganography tool that is used to embed hidden messages in ASCII format by extending the whitespace to the end of lines.

Step 1: Open the uncompressed file.
Step 2: Run the SNOW.exe file.



Step 3: Open CMD and reach the file that you want to hide the message within.



Step 4: Put this command on cmd
“SNOW.EXE -C -p 1234 -m "hidden message" input.txt output.txt”

```
Microsoft Windows [Version 10.0.22000.613]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Admin>cd Downloads/

C:\Users\Admin\Downloads>cd snwdos32

C:\Users\Admin\Downloads\snwdos32>SNOW.EXE -C -p 1234 -m "hidden message" input.txt output.txt
Compressed by 44.64%
Message exceeded available space by approximately 1.#J%.
An extra 3 lines were added.

C:\Users\Admin\Downloads\snwdos32>
```

Step 5: to extract the hidden message type the following command
"SNOW.EXE -C -p 1234 output.txt"

```
C:\Users\Admin\Downloads\snwdos32>SNOW.EXE -C -p 1234 -m "hidden message" input.txt output.txt
Compressed by 44.64%
Message exceeded available space by approximately 1.#J%.
An extra 3 lines were added.

C:\Users\Admin\Downloads\snwdos32>SNOW.EXE -C -p 1234 output.txt
hidden message
C:\Users\Admin\Downloads\snwdos32>
```

Practical No. 9A

Aim: Password Cracking using Cain and Abel.

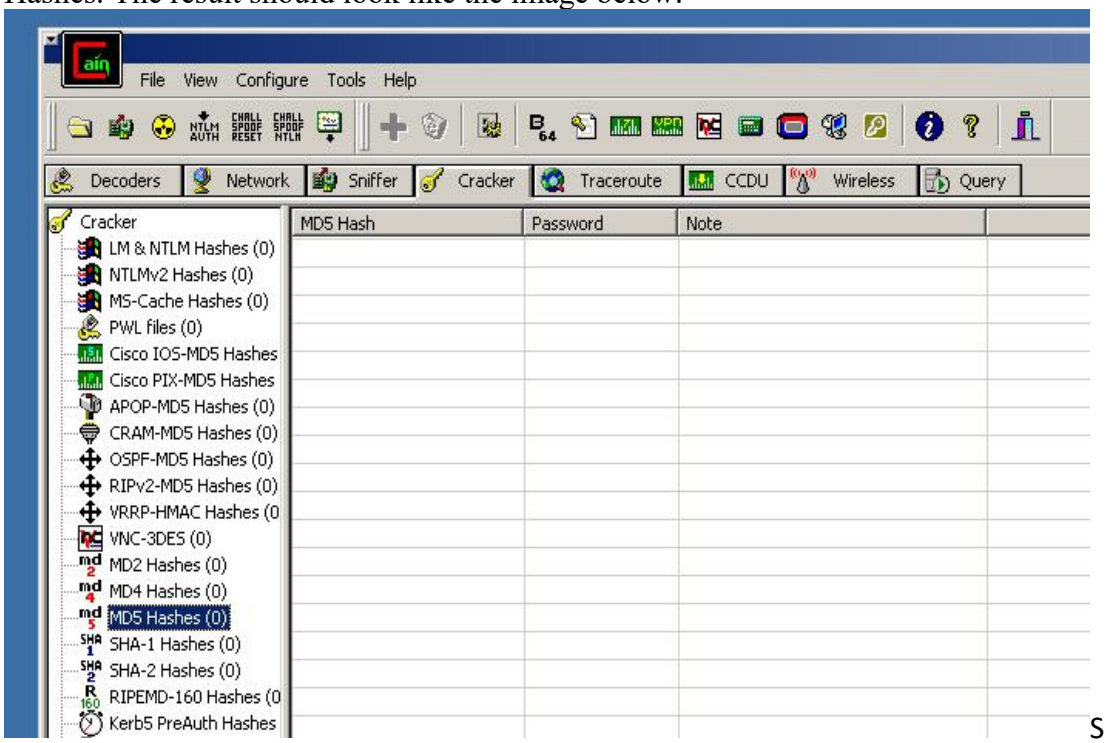
This exercise demonstrates how password could be cracked through various methods, specifically regarding MD5 encrypted passwords

Part 1: Dictionary attack - Dictionary attack uses a predetermined list of words from a dictionary to generate possible passwords that may match the MD5 encrypted password. This is one of the easiest and quickest way to obtain any given password.

Step 1: Start Cain & Abel via the Desktop Shortcut 'Cain' or Start menu . a. (Start > Programs > Cain > Cain).

Step 2: Choose 'Yes' to proceed when a 'User Account Control' notification pops up regarding software authorization

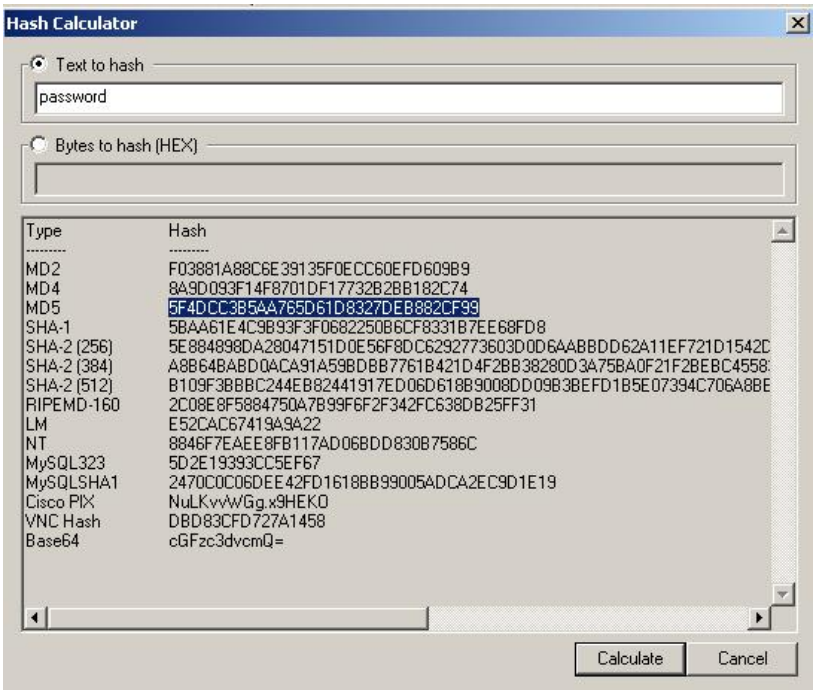
Step 3: Once on, select the 'Cracker' tab with the key symbol, then click on MD5 Hashes. The result should look like the image below.



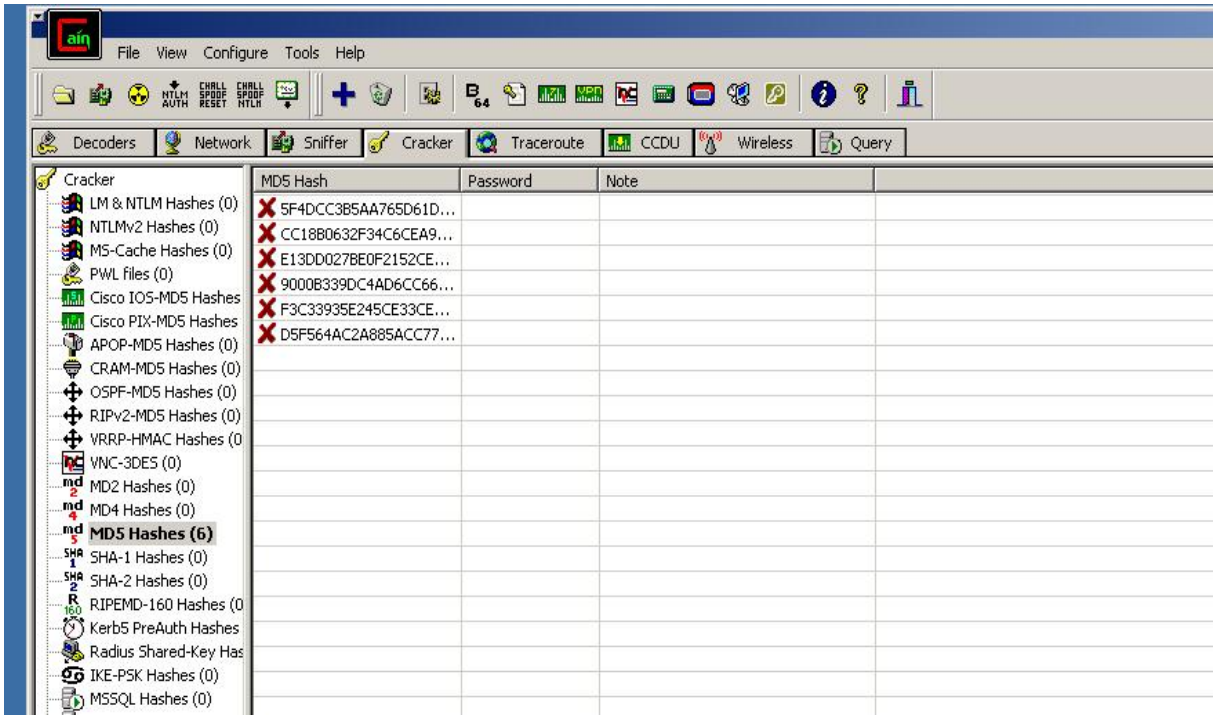
S

tep 4: As you might have noticed we don't have any passwords to crack, thus for the next few steps we will create our own MD5 encrypted passwords. First, locate the Hash Calculator among a row of icons near the top. Open it.

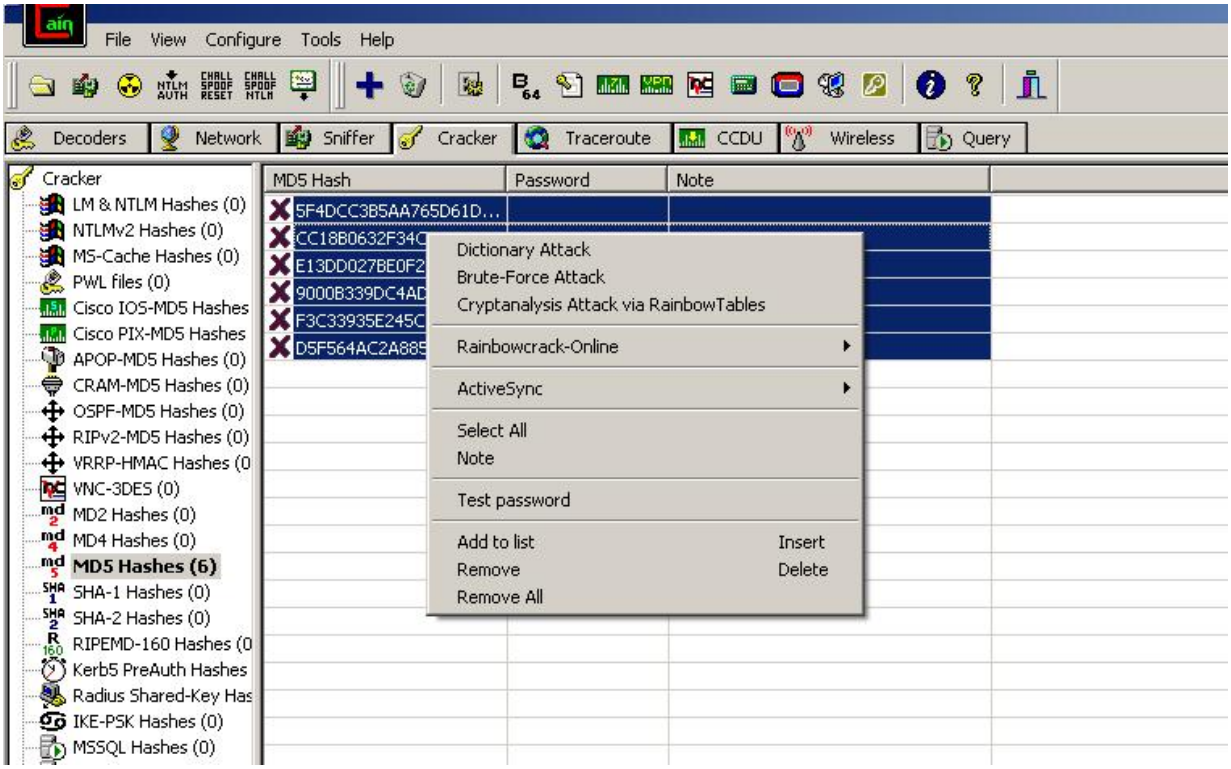
Step 5: Next, type into 'Text to Hash' the word password. It will generate a list of hashes pertaining to different types of hash algorithms. We will be focusing on MD5 hash so copy it. Then exit calculator by clicking 'Cancel'



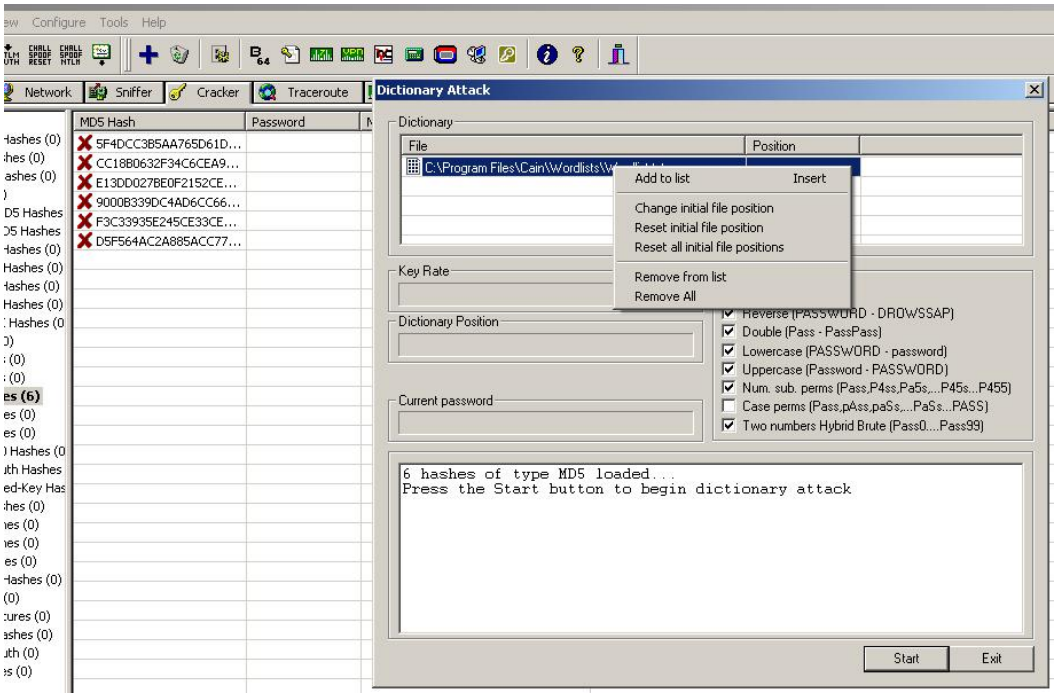
Step 6: After you exit, right click and select 'Add to list' , paste your hash then click OK . Your first encrypted password! But don't stop there, add the following MD5 hashes from the words PaSS , 13579, 15473 , sunshine89, and c@t69



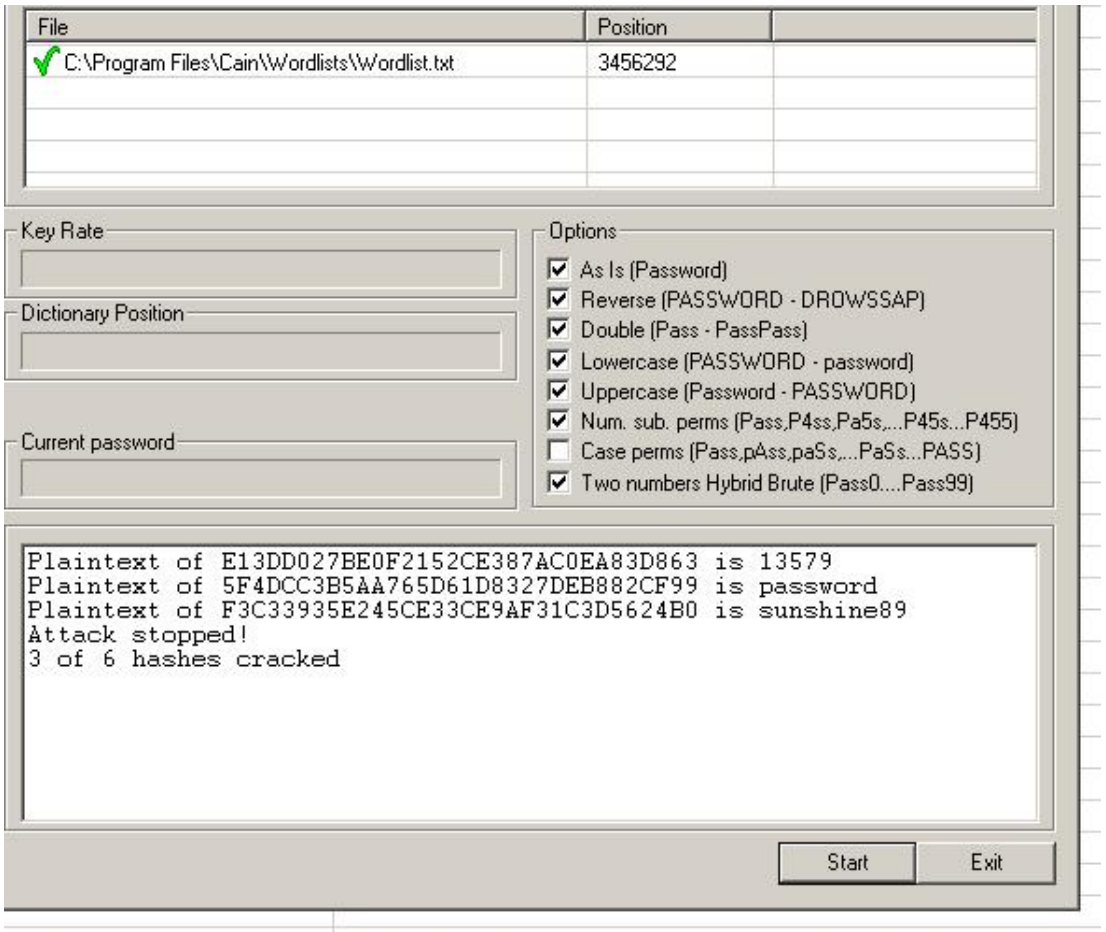
Step 7: With all the encrypted MD5 passwords on hand, we can finally start! Move your cursor and select all six passwords, then right click and press 'Dictionary Attack'.



Step 8: Once the window opens, go up to the dictionary and select 'Wordlist.txt' , right click and select 'Reset initial file position'. You'll know you've resetted when there's nothing under the position column. Note: Make sure to do this every time you want to restart a dictionary attack!

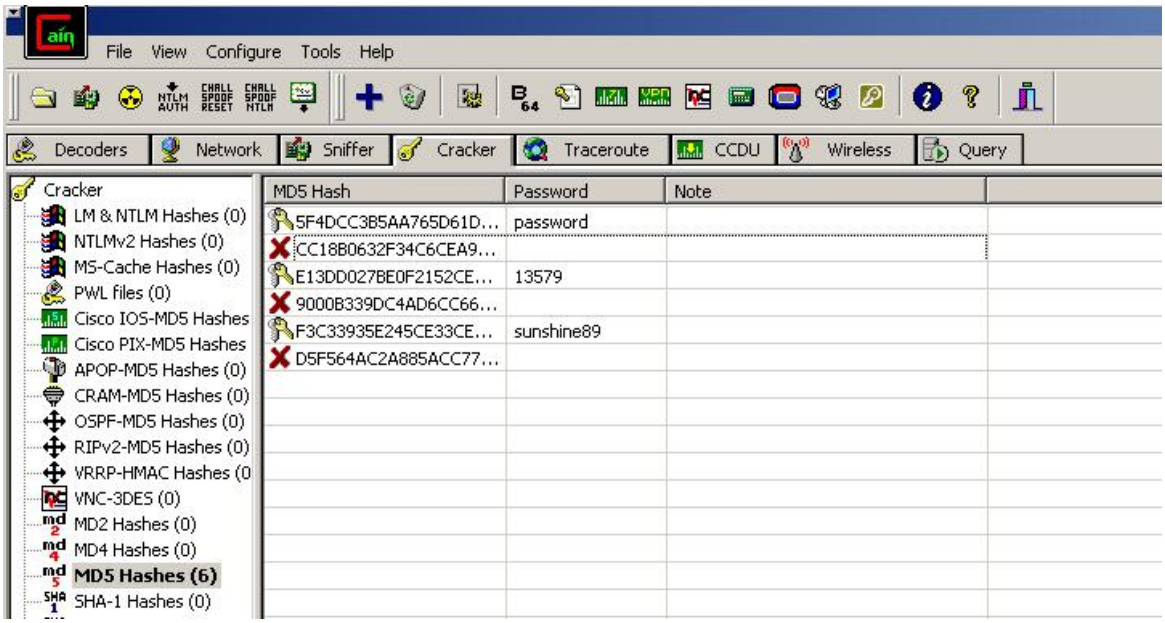


Step 9: Click ‘start’ and watch the magic happens before your eyes! Once it ends ‘exit’ . Your result should be the same as below.

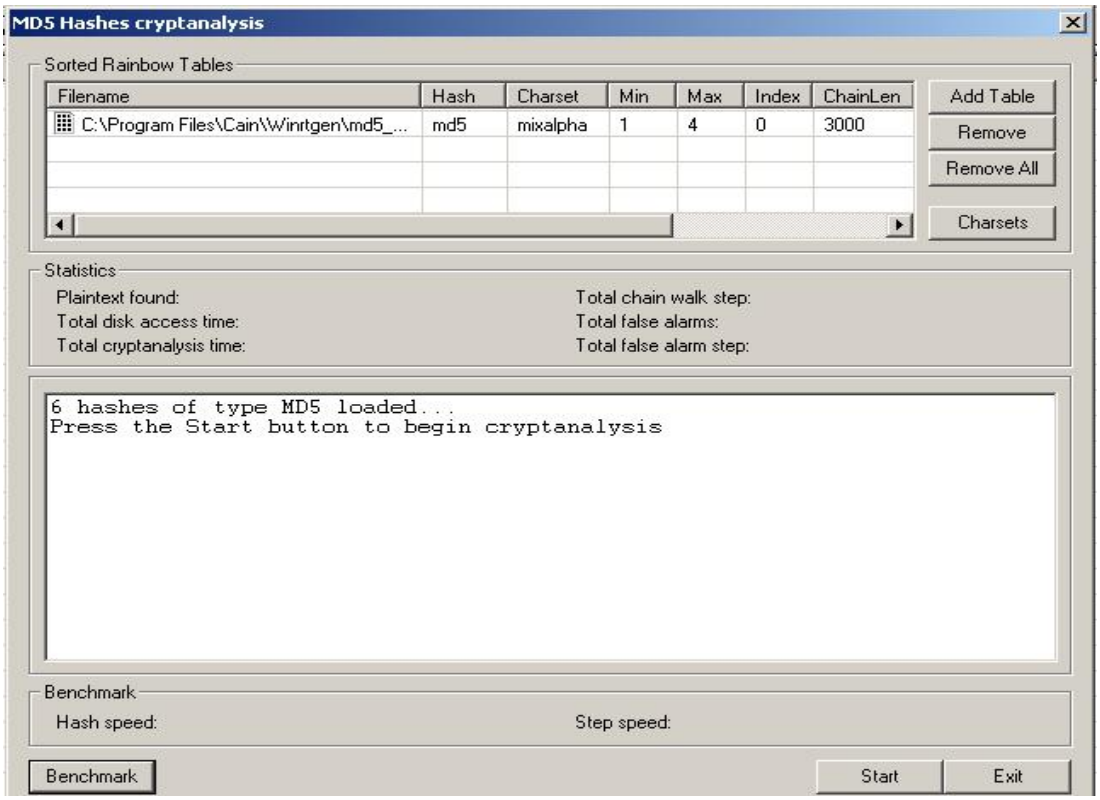


Part 2 : Rainbow Tables - Rainbow tables use pre-calculated MD5 hashes sorted on a table(s) to compare to encrypted MD5 files in order to find a match thus cracking the password. This type of password cracking trades time and storage capacity.

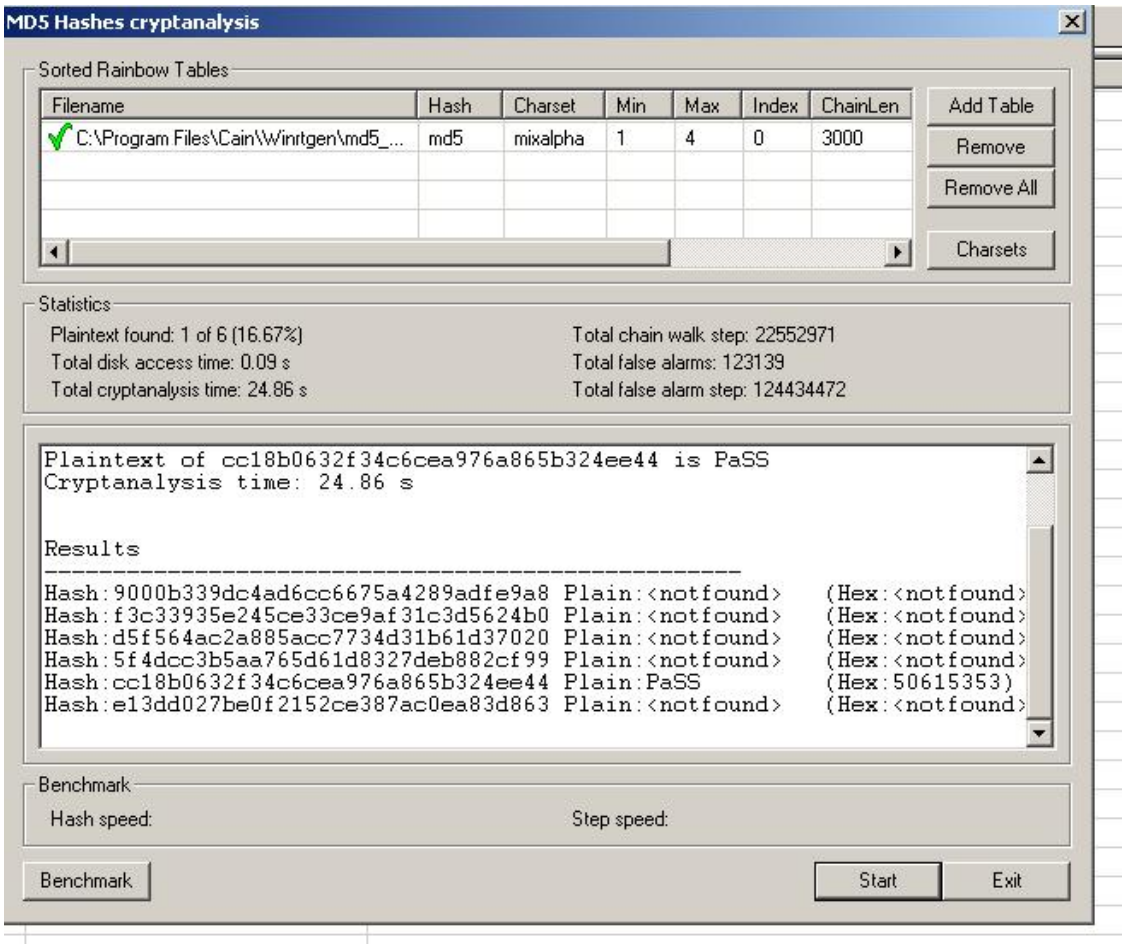
Step 1: Continuation from the previous 'Dictionary Attack' section. Cain & Abel should already be opened with following MD5 encrypted passwords.



Step 2: Now with the other half of the passwords still encrypted, we will be using rainbow table attacking to see if we can finally crack them. Select all six passwords, right click, and select 'Cryptanalysis Attack via RainbowTables'.

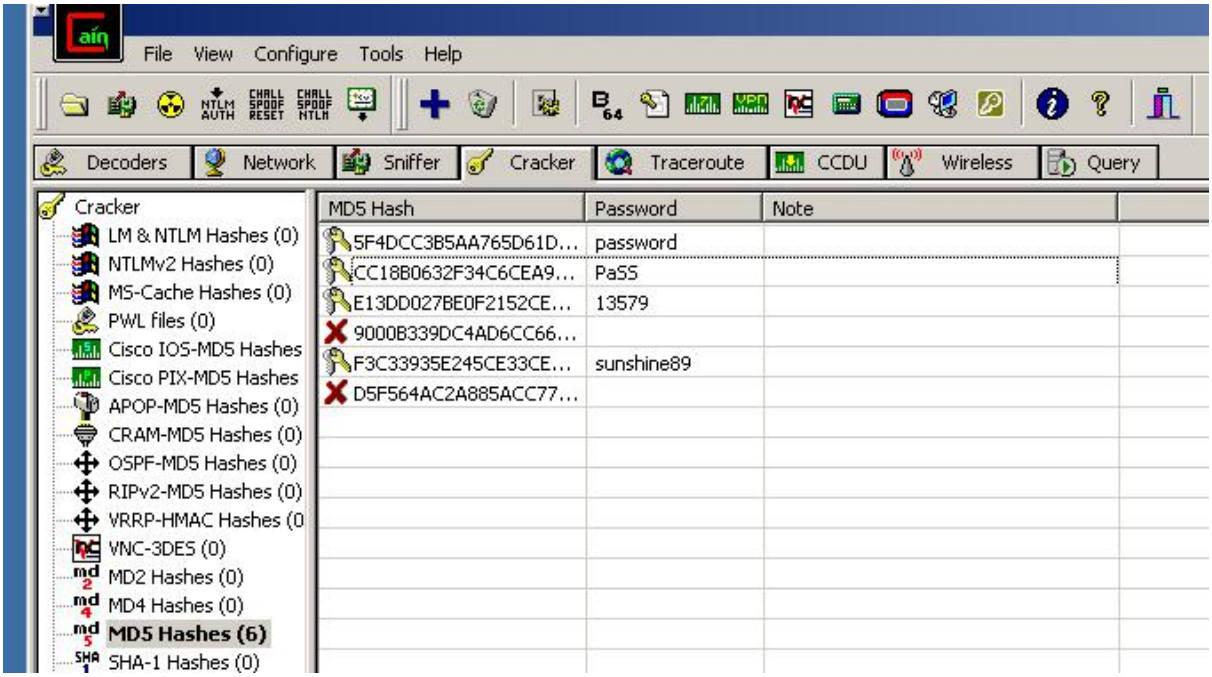


Step 3: A window will pop up and you could see under 'Sorted Rainbow Tables' there is already a MD5 rainbow table already added. Notice the specifications for that specific rainbow table. Click 'Start' when ready. 'Exit' when done.

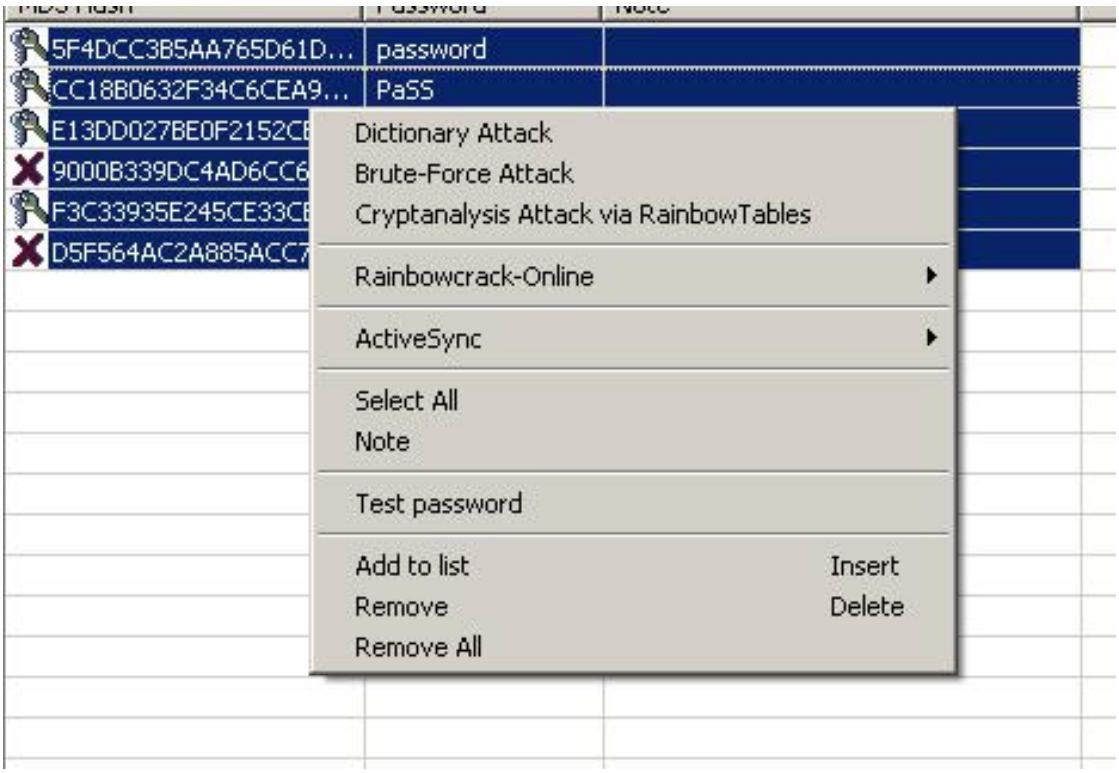


Part 3: Brute Force - Brute force attacks uses a finite but enormous number of combinations involving alphabet, numbers, and symbols in order to crack a password. This type of password cracking is usually used as a last resort as it's the most time consuming overall.

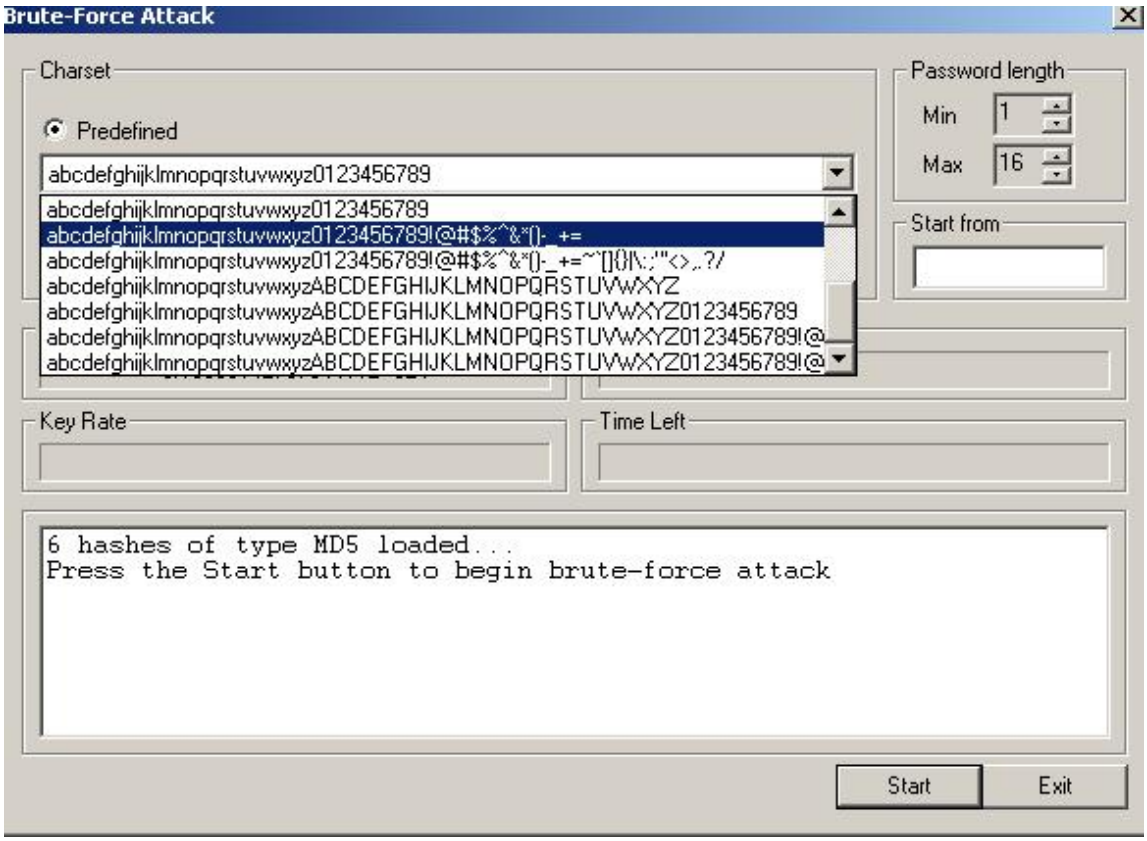
Step 1: Continuation from the previous 'Rainbow Tables' section. Cain & Abel should already be opened with the following MD5 encrypted passwords.



Step 2: Now with only two more passwords still encrypted, we will be using brute force attack to see if we can finally crack them. Select all six passwords, right click, and select 'Brute-Force Attack'.



Step 3 : Once a window appears we will have to adjust some settings to fit our requirements. Under Charset and Predefined selected, open the drop down bar and select the one below the initially selected one. Next, under Password length turn Max down to 5.



Step 4: When ready click 'Start'. Once it's done calculating 'Exit' . Your final results should be the same as below. All of them should be cracked! Yay!