INDEX

Practical 1

File System Analysis using The SleuthKit

1. **fsstat**

   fsstat displays the details associated with a file system. The output of this command is file system specific. At a minimum, the range of meta-data values (inode numbers) and content units (blocks or clusters) are given. Also given are details from the Super Block, such as mount times and features. For file systems using groups (FFS and EXT2FS), the tool lists the layout of each group.

   fsstat – Display general details of a file system.

2. **istat**

   istat displays the uid, gid, mode, size, link number, modified, accessed, changed times, and all the disk units a structure has allocated.

   istat – Display details of a meta-data structure (i.e. inode)

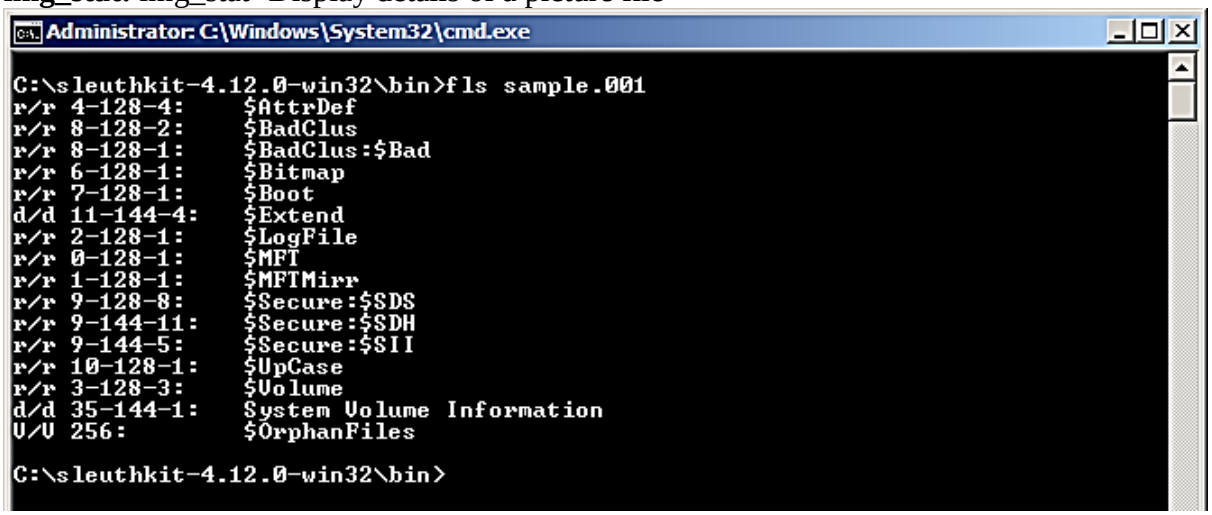
3. **fls**

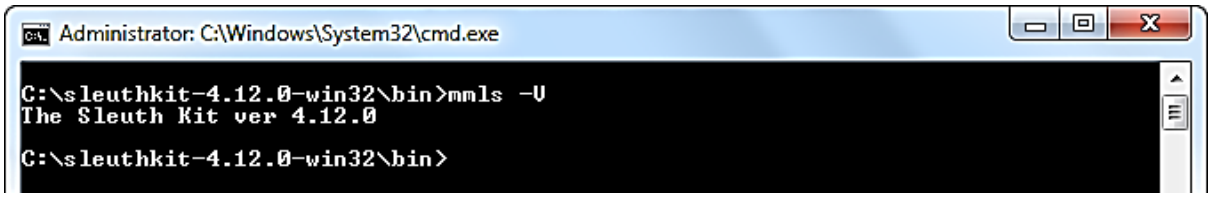
   fls lists the files and directory names within the image and may display file names of recently deleted files for the directory using the given mode.

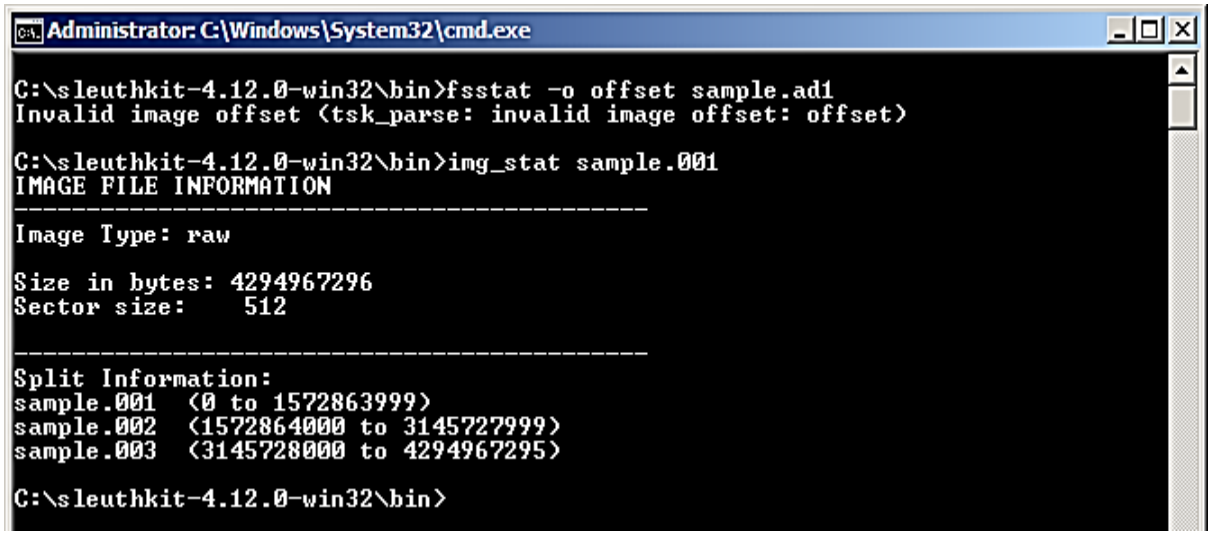
   fls: fls-List file and directory names in a disk image.

4. **img_stat**

   img_stat displays the small print related to a picture file. The output of this command is image format specific.
   img_stat: img_stat- Display details of a picture file



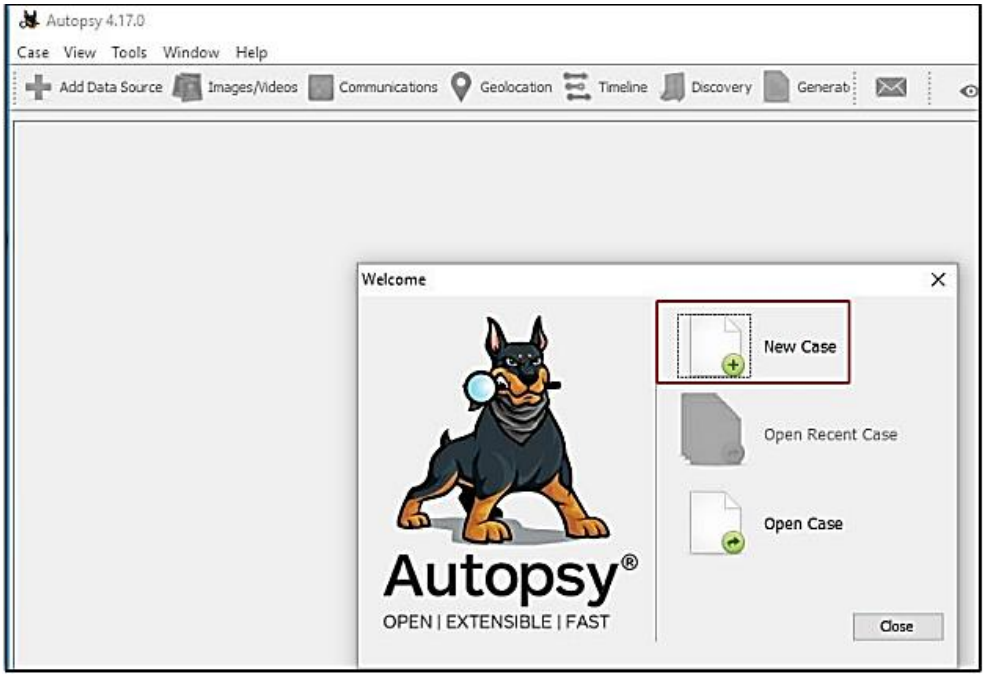




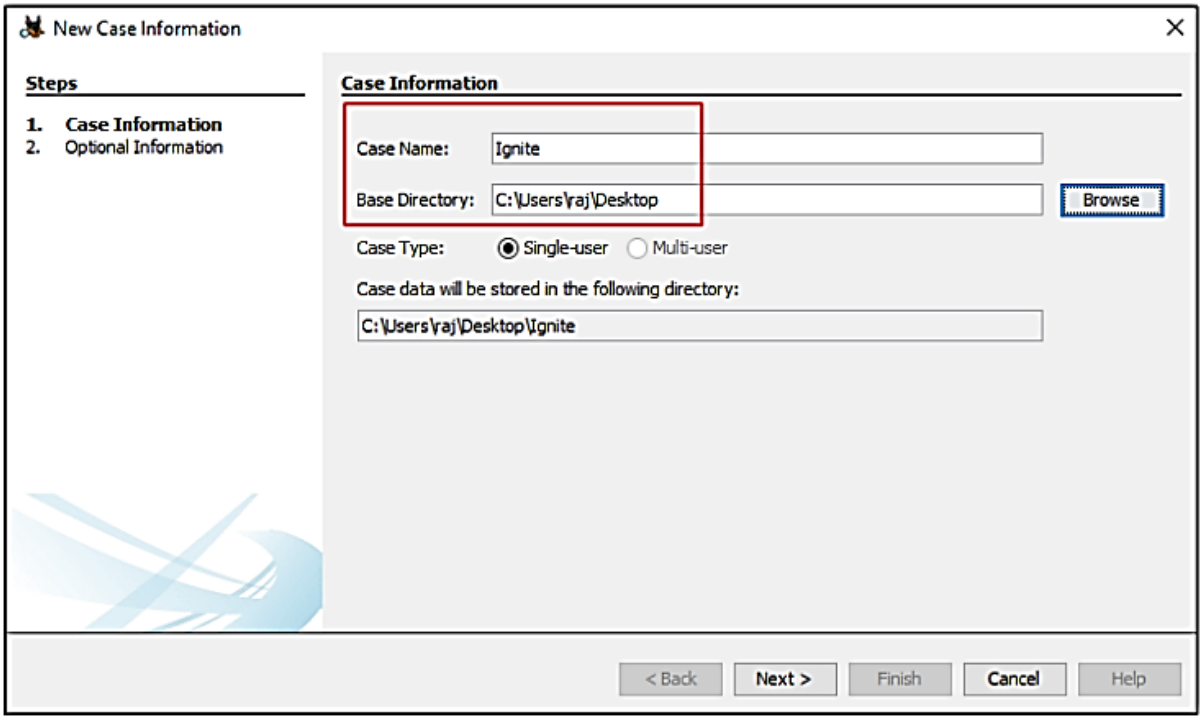
5. Autopsy

File System Analysis Using Autopsy is a digital forensics platform and graphical interface to The Sleuth Kite and other digital forensics tools. Autopsy is an end-to-end platform with modules that come with it out of the box and others that are available from third parties.

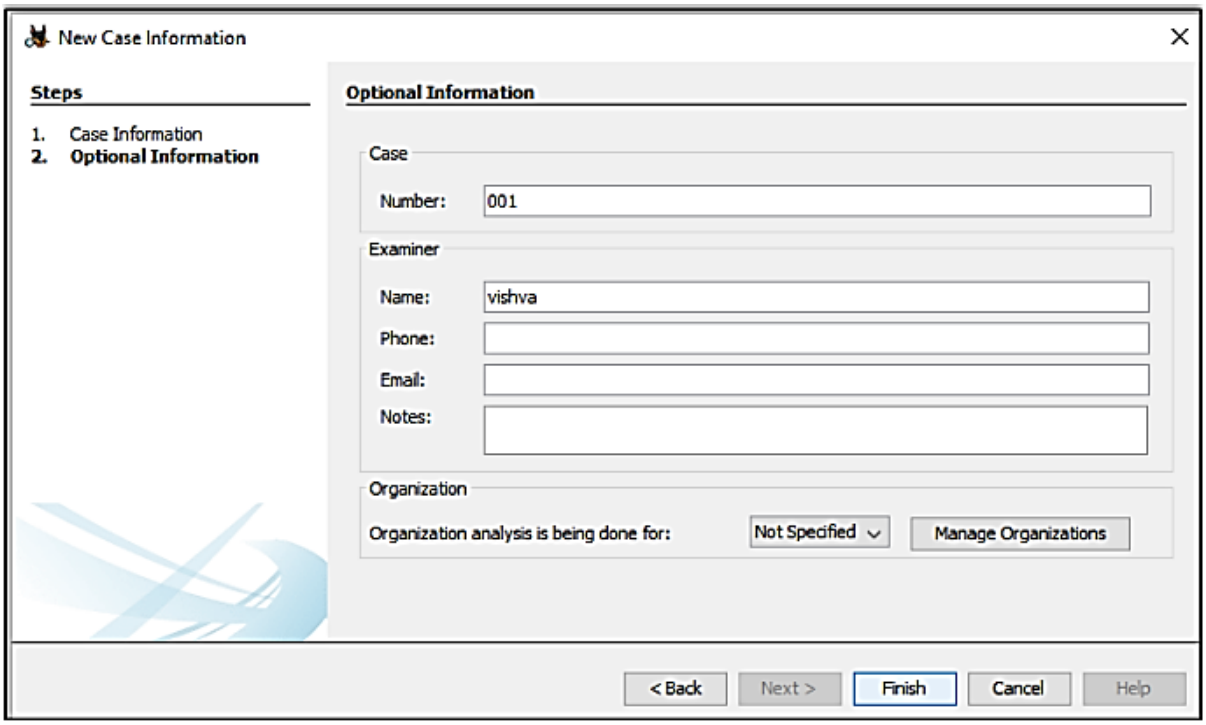
Run the Autopsy tool on your Windows Operating System and click on “New Case” to create a new case.



Then fill in all the necessary case information like the case name and choose a base directory to save all the case data in one place.



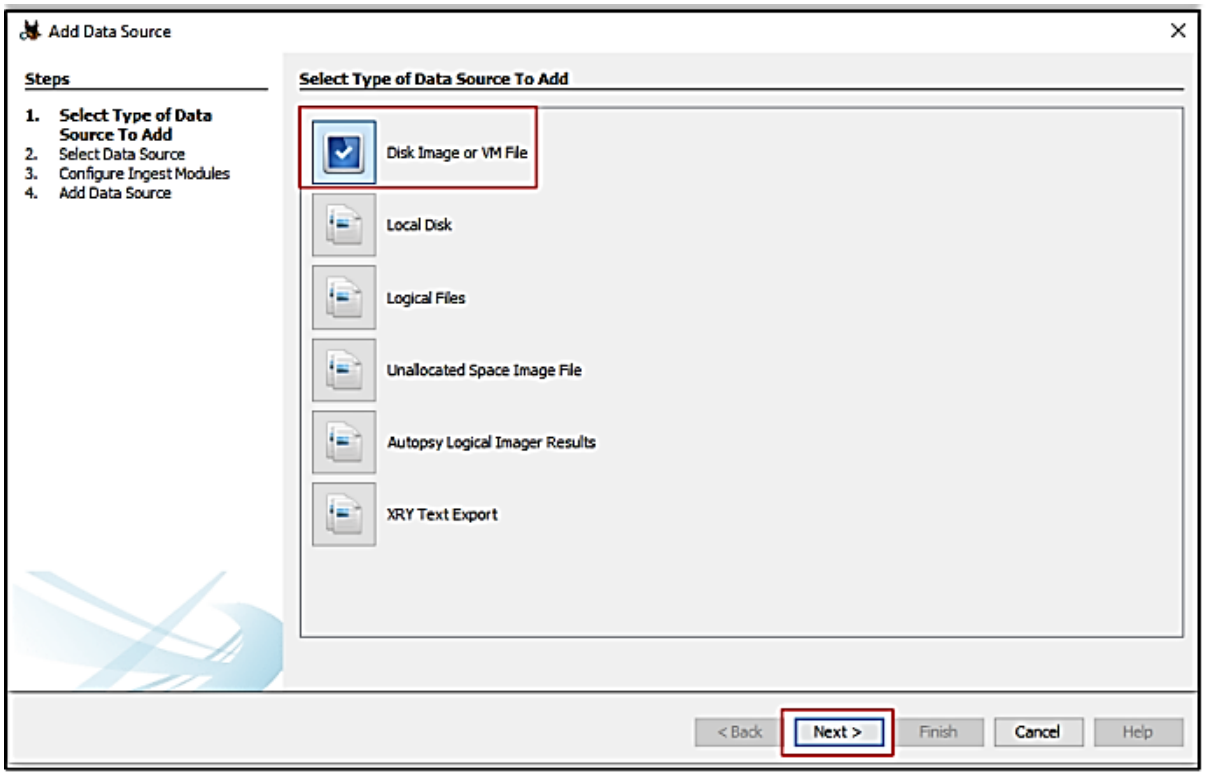
You can also add additional optional information about the case if required.



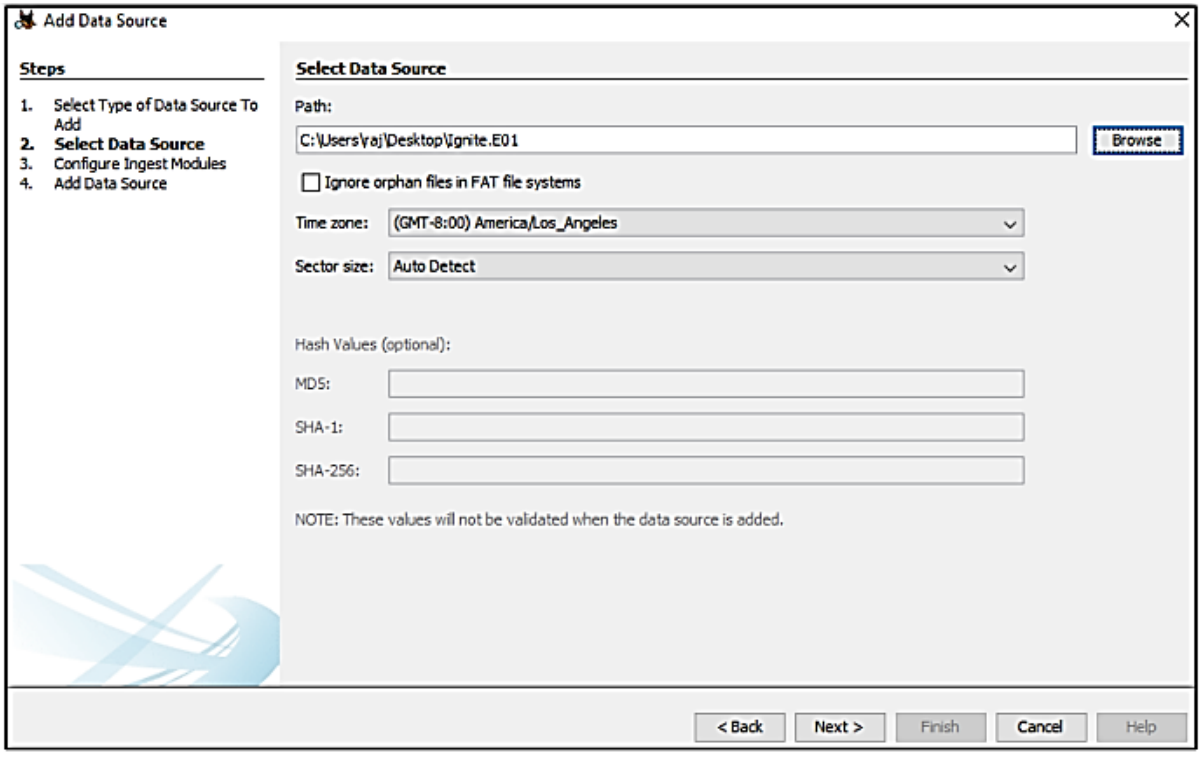
Now let us add the type of data source. There are various types to choose from.

- Disk Image or VM file: This includes the image file which can be an exact copy of a hard drive, media card, or even a virtual machine.
- Local Disk: This option includes devices like Hard disk, Pen drives, memory cards, etc.
- Logical Files: It includes the image of any local folders or files.

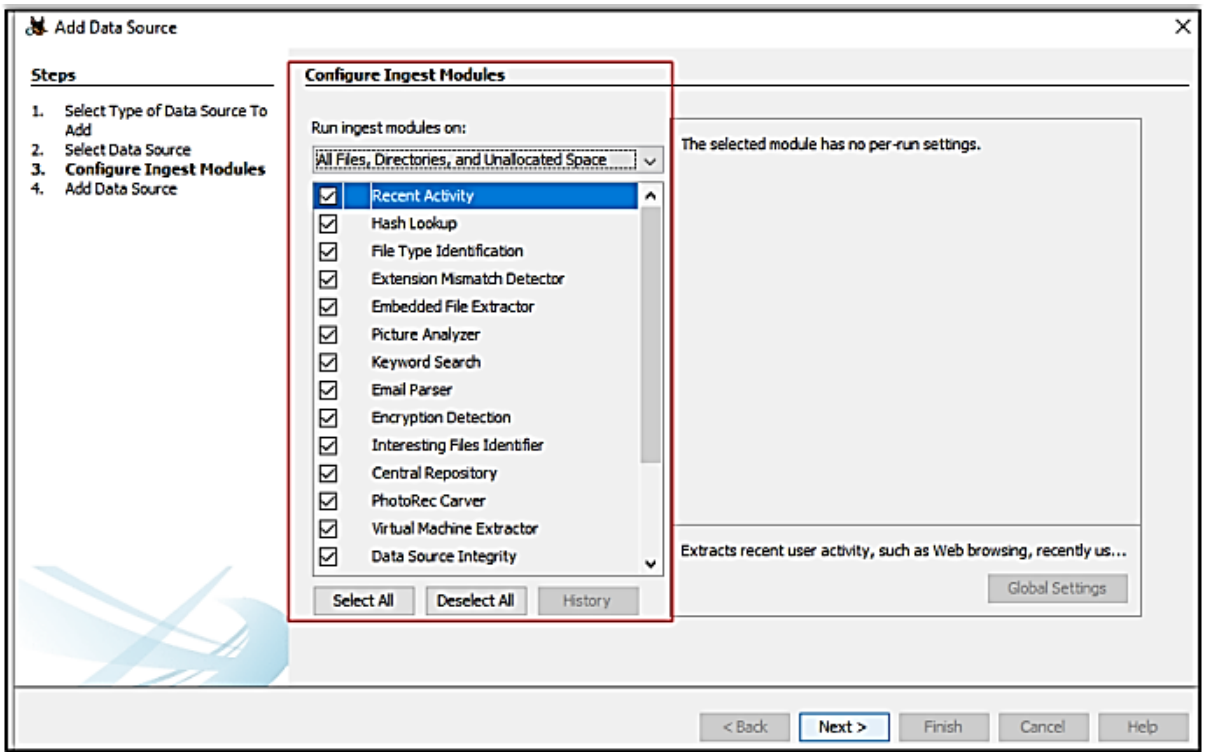
- Unallocated Space Image File: They include files that do not contain any file system and run with the help of the ingest module.
- Autopsy Logical Imager Results: They include the data source from running the logical imager.
- XRY Text Export: This includes the data source from exporting text files from XRY.



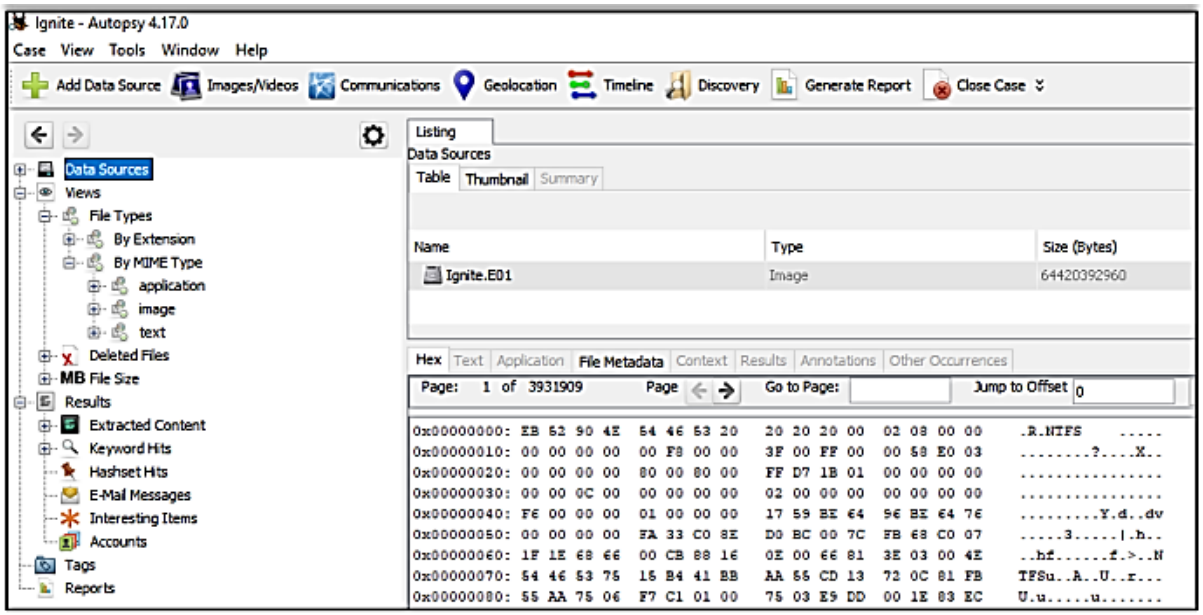
Now let us add the data source. Here we have a previously created image file, so we will add the location of that file.



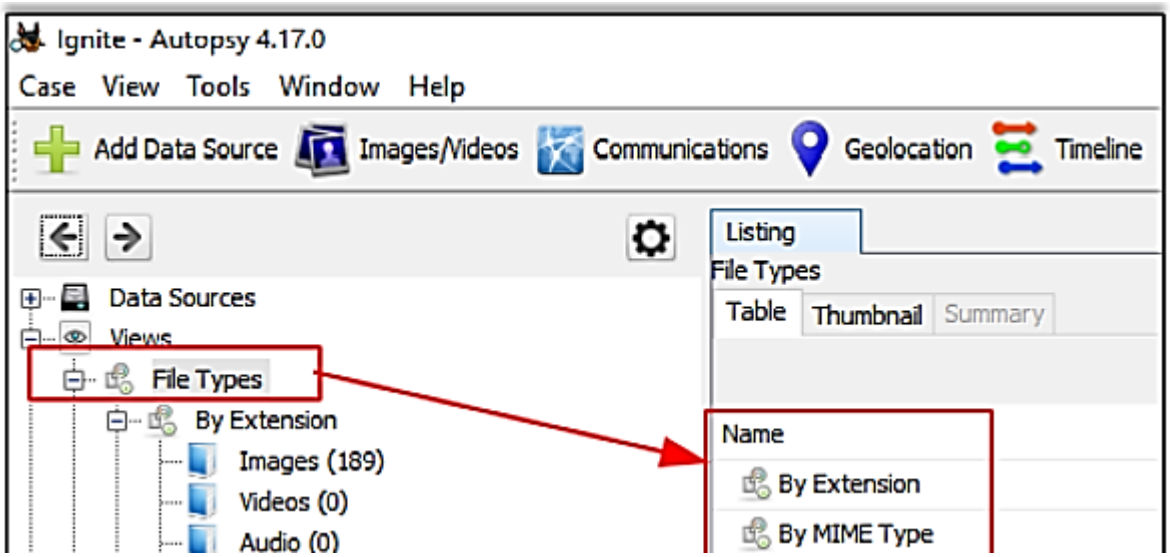
Next, you will be prompted to Configure the Ingest Module.



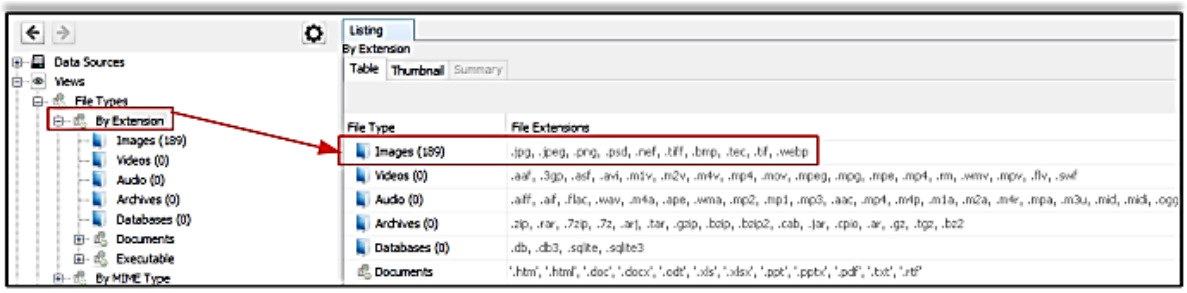
Data Source information displays basic metadata. Its detailed analysis is displayed at the bottom. It can be extracted one after the other.



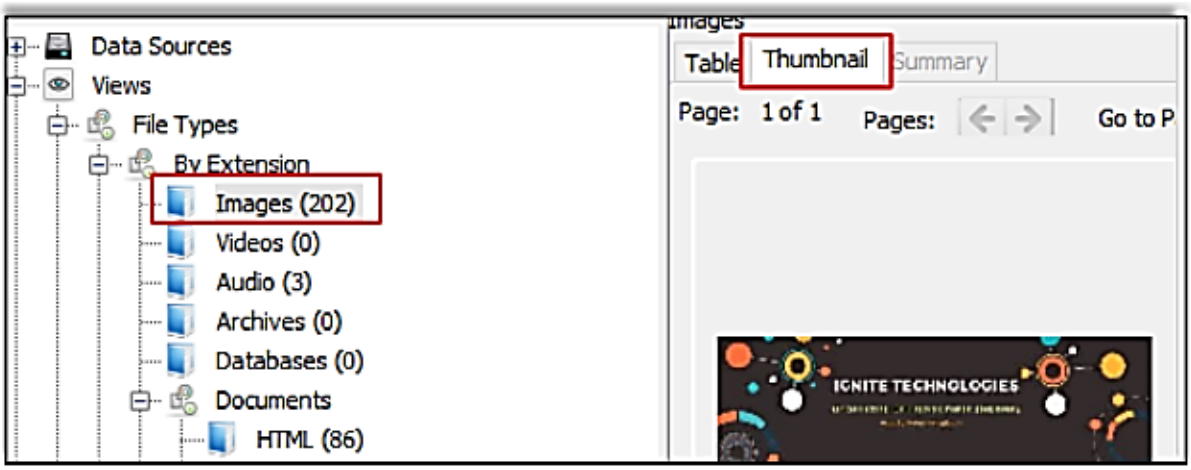
File Type: It can be classified in the form of File extension or MIME type. It provides information on file extensions that are commonly used by the OS whereas MIME types are used by the browser to decide what data to represent. It also displays deleted files.



By Extension In the category Filetypes by extension and you can see that this has been sub-divided into file types like images, video, audio, archives, databases, etc.



We can also view the thumbnail of the images

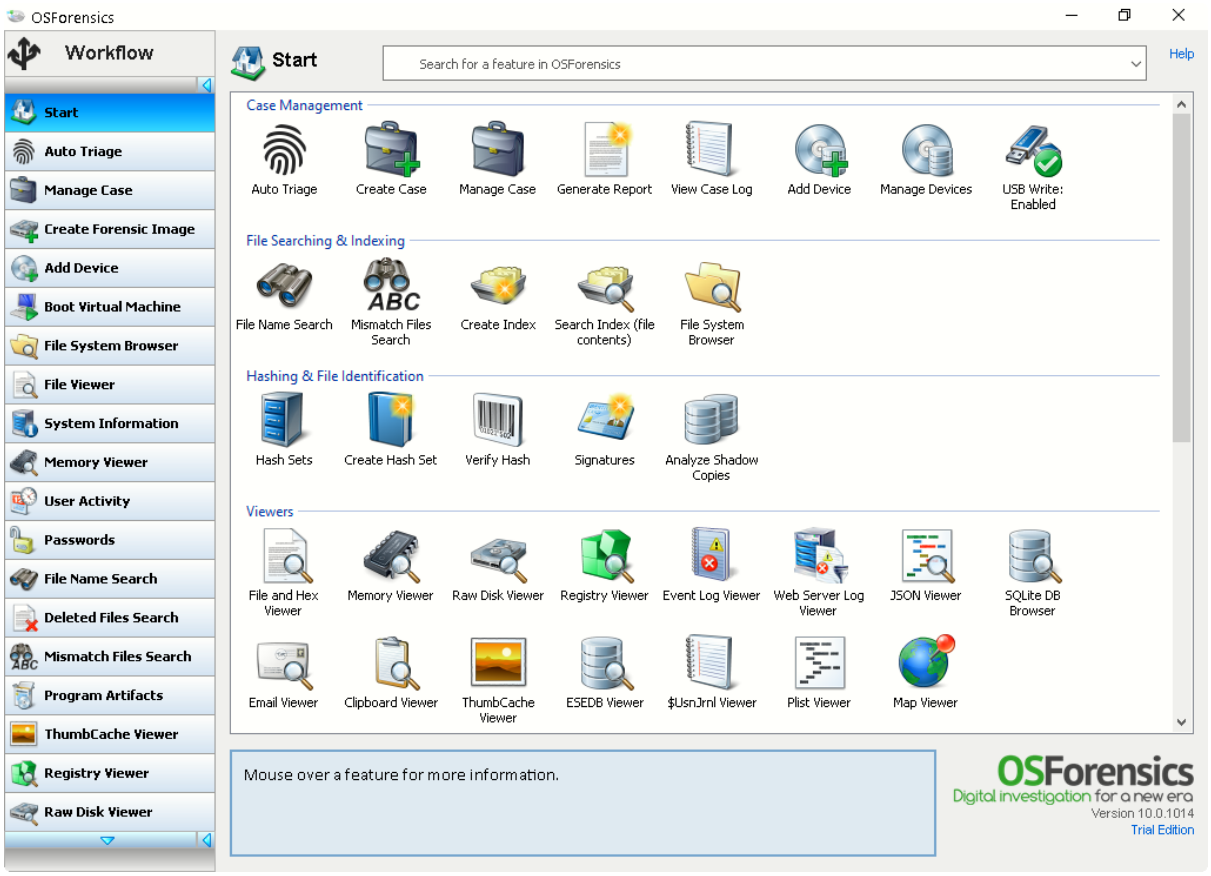


On viewing the thumbnail, you can view the file metadata and details about the image.

Practical 2

a) Explore Windows forensic tools (OSForensics)

OSForensics is organized into multiple feature modules for discovering, identifying and managing digital forensics artifacts. OSForensics Interface: The OSForensics interface gives you access to the following parts of the main menu with 1 click:



OSForensics contains a collection of modules for searching, collecting, analyzing and recovering digital artifacts that can be used as legal evidence in court. The main features of OSForensics are outlined as follows.

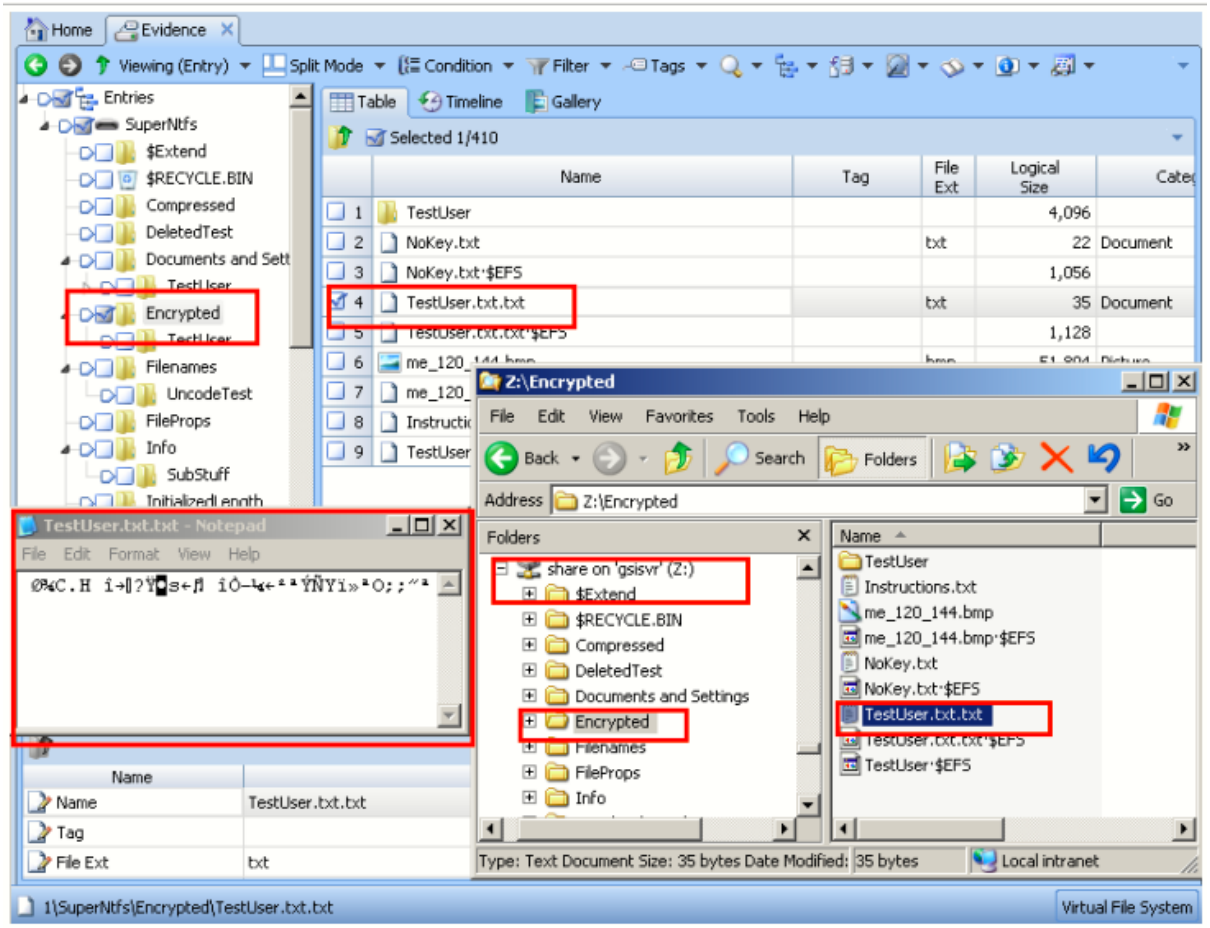
- **Android Artifacts:** Scan Android case devices and backups for evidence of user activity, such as accessed call logs, websites, messages, and contacts.
- **Auto Triage:** Automate common forensic tasks in order to triage the most relevant evidence data in time-limited situations. Auto Triage allows non-forensics trained personnel to acquire intelligence on-site which can be volatile and high-risk.
- **Boot Virtual Machine:** Boot a disk image containing a functional operating system on a virtual machine, recreating the live desktop environment of the system of interest.
- **Case Management:** Manage evidence obtained from OSForensic modules into a single *Case*. Generate HTML and PDF reports to summarize forensic analysis results.
- **Clipboard Viewer:** Display the contents stored in the clipboard on the live system, including the clipboard history and pinned items if available.
- **Deleted Files Search:** Search for and recover files that have been recently deleted from the hard drive.

- **Drive Preparation:** Perform byte pattern verification tests on fixed and removable drives attached to the system.
- **Email Viewer:** Browse and analyze e-mail files including orphaned and deleted e-mails.
- **ESE Database Viewer:** Navigate and search the tables, fields and records contained within ESE database files. Various Microsoft applications including Windows Search and Microsoft Exchange Server store data with potential forensics value in the ESE database file format.
- **Event Log Viewer:** View Windows Event Logs. Scan, search, filter, export and time-line analysis can be performed on the Event Logs.
- **File Name Search:** Search for files/directories based on name and other file attributes such as size, attributes, and time.
- **File System Browser:** Display the file system of all devices added to a case in an explorer-like view. In addition to standard file system attributes such as file size and file times, other forensic-related metadata is displayed.
- **Forensic Imaging:** Create exact, bit-by-bit duplicates of a disk into an image file. Restore an image file back to the disk. Create a forensically sound logical image of files/directories of interest, preserving file dates, attributes and owners.
- **Hash Sets:** Identify known safe or known suspected files using *Hash Sets* to reduce the need for further time-consuming analysis.
- **Image Analysis:** Performs deep learning image analysis on image files for face detection or illicit image detection.
- **Indexing:** Scan and search for text strings within the contents of a file. Also capable of searching within email archives and pulling text out of unallocated disk sectors.
- **Internal Viewer:** View and analyze files within OSForensics without needing to open an external application. This can be used for files in devices added to the Case such as disk images, which cannot be opened normally in the operating system.
- **Map Viewer:** Search, import and plot location-based evidence on a world map. This includes IP addresses in e-mail headers and server logs, and GPS coordinates in EXIF metadata.
- **Memory Viewer:** Collect and analyze digital evidence in volatile memory storage. Due to the non-persistent nature of memory, some digital evidence may only be available on a live system.
- **Mismatch Search:** Identify files that may show evidence of tampering due to having a file extension that is different from what the contents of the file suggests. Eg. A .jpeg file renamed to a .txt file.
- **Passwords:** Recover and decrypt passwords from various sources.
- **Plist Viewer:** View the contents of Plist (property list) files which are commonly used by OSX and iOS to store settings and properties.
- **Program Artifacts:** Collect traces of Prefetch and AmCache hive artifacts left by applications. The Prefetch Viewer displays the information stored by the operating system's Prefetcher, which includes when and how often an application is run. The AmCache Viewer shows information from the AmCache hive that contains meta information on program executables and installation.
- **Raw Disk Viewer:** Open and view raw sectors of a disk. Data hidden in the sectors outside the file system can be identified and analyzed with this module.
- **Registry Viewer:** View Windows Registry Hives, including the live system where files can be locked / in use

- **Signatures:** Create a snapshot of a system's directory structure at specific point in time using *Signatures*. *Signatures* can be compared in order to identify files that have been added, deleted and changed.
- **SQLite Database Browser:** Navigate and search the tables, fields and records of SQLite database files.
- **System Information:** View and export hardware, platform and operating system details which can be used for evidence inventory management.
- **ThumbCache Viewer:** Extract thumbnail images stored in Windows' thumbnail cache files for viewing. Thumbnail cache files may contain evidence of images that have been deleted on the system.
- **User Activity:** Scan the system for evidence of user activity such as accessed websites, USB drives, wireless networks, and recent downloads.
- **Verify/Create Hash:** Create hashes (SHA1, MD5, CRC32) of files or entire hard disk.
- **Web Browser:** Provide a basic web viewer with forensics capabilities. This includes the ability to save screen captures of web pages and add them to the currently opened case.
- **Web Server Log Viewer:** Extract and analyze log data generated by Apache, IIS, NGINX or other custom web server logs. About - Information about the software and the active license.
- **Exit** - Closes the application.

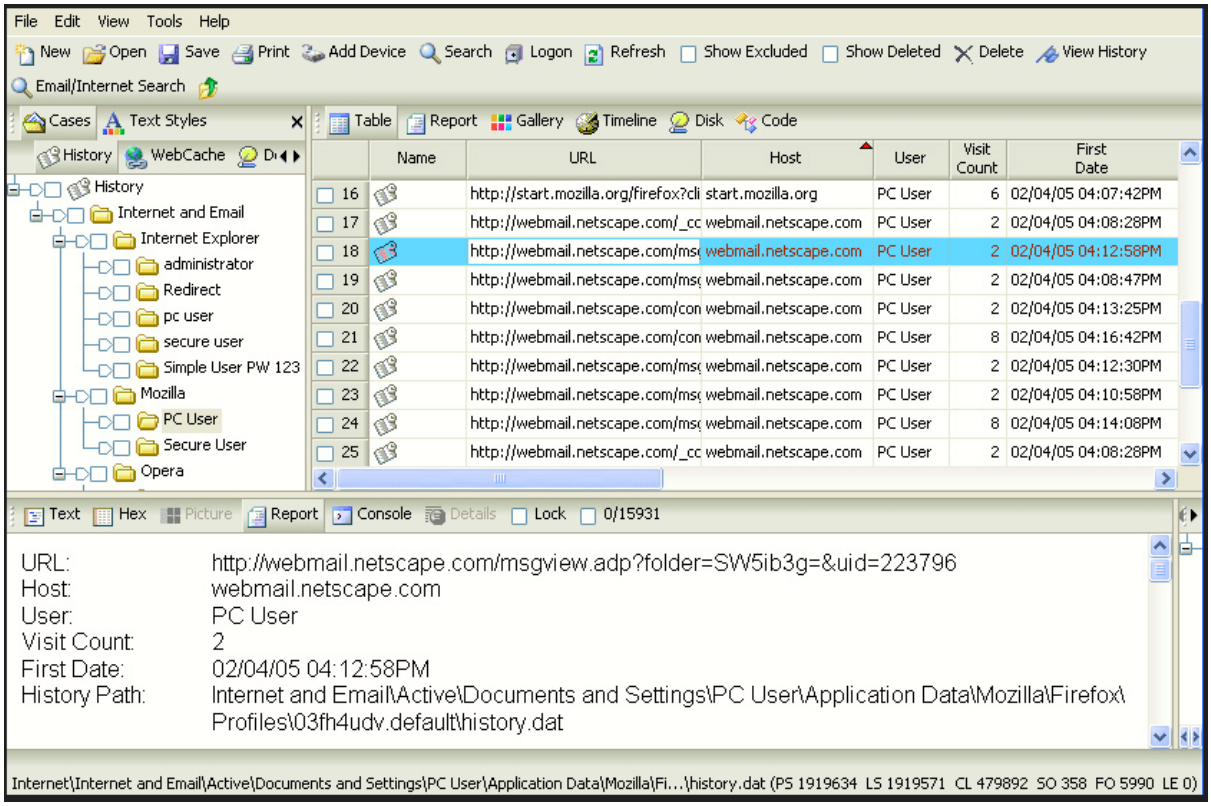
b) Forensics Investigation Using Encase

The powerful and effective features of EnCase® Forensic have made it the trusted standard in corporate and criminal investigation. No other product offers the same degree of functionality, acceptance, and performance.



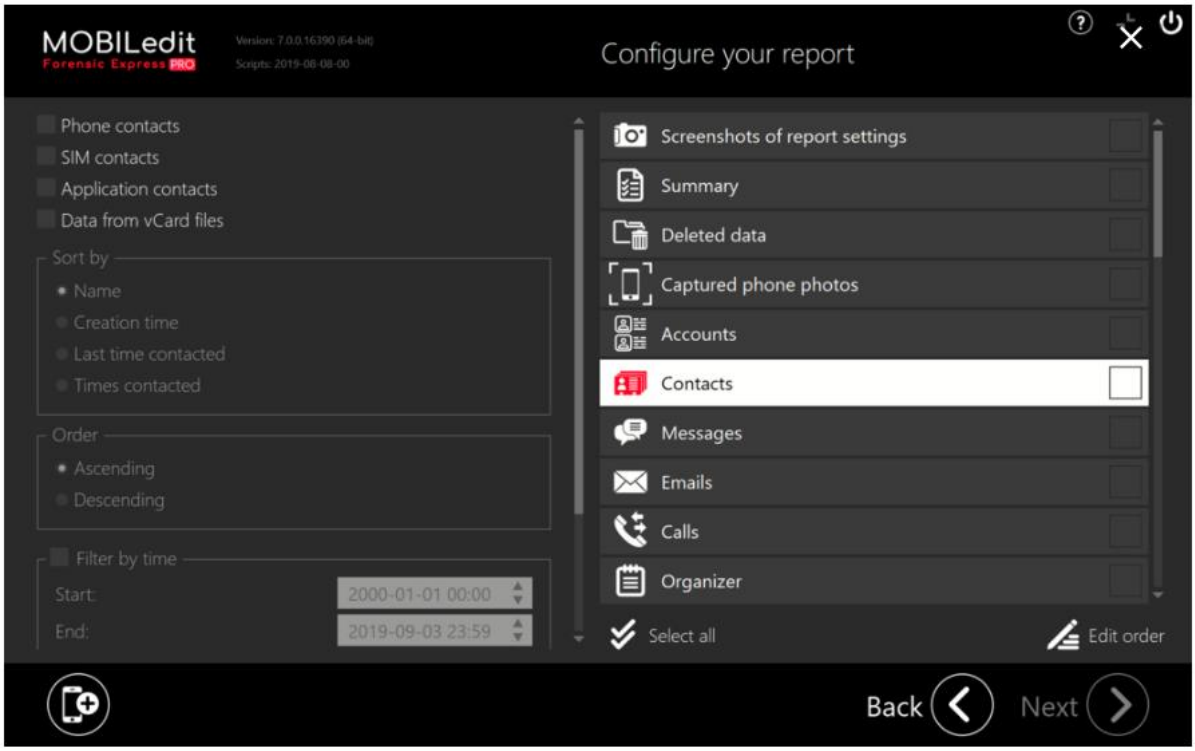
- **Acquire from Almost Anywhere:** Acquire data from disk or RAM, documents, images, e-mail, webmail, Internet artifacts, Web history and cache, HTML page reconstruction, chat sessions, compressed files, backup files, encrypted files, RAIDs, workstations, servers, and with Version 7: smartphones and tablets.
- **Forensically Sound Acquisition:** EnCase® Forensic produces an exact binary duplicate of the original drive or media, then verifies it by generating MD5 hash values for related image files and assigning CRC values to the data. These checks and balances reveal when evidence has been tampered with or altered, helping to keep all digital evidence forensically sound for use in court proceedings or internal investigations.
- **Advanced Analysis:** Recover files and partitions, detect deleted files by parsing event logs, file signature analysis, and hash analysis, even within compounded files or unallocated disk space.
- **Improved Productivity:** Examiners can preview results while data is being acquired. Once the image files are created, examiners can search and analyze multiple drives or media simultaneously.

- **Automated de-NISTing Capabilities:** The National Software Reference Library (NSRL) is provided in the EnCase hash library format, allowing user to easily de-NIST their evidence, eliminating thousands of known files from their evidence set. This reduces the time and amount of data that needs to be analyzed significantly.
- **Multiple File Viewer Support:** View hundreds of file formats in native form, built-in Registry viewer, integrated photo viewer, see results on a timeline/calendar.
- **Customizable and Extensible with Apps from EnCase App Central:** EnCase® Forensic features EnScript® programming capabilities. EnScript®, an object-oriented programming language similar to Java or C++, allows users create to custom programs to help them automate time-consuming investigative tasks, such as searching and analyzing specific document types or other labor-intensive processes and procedures. Dozens of these productivity enhancing programs or Apps are available on EnCase App Central.
- **Automatic Reports:** Export reports with lists of all files and folders along with detailed list of URLs, with dates and time of visits. Provide hard drive information and details related to the acquisition, drive geometry, folder structure, etc.
- **Actionable Data:** Once investigators have identified relevant evidence, they can create a comprehensive report for presentation in court, to management or stakeholders in the outcome of the investigation.
- **Integration to Passware Kit Forensic:** Use the Evidence Processor to automate the detection of encrypted files. Once the files are decrypted by Passware Kit Forensic* they can be easily integrated back into EnCase Forensic for further analysis.



c) Exploring Mobiledit Forensics tool

MOBILedit Forensic can retrieve messages, call logs, pictures, contacts, apps, calendar events, emails, passwords, media, file systems, deleted data, and much more. You can even select specific data which you want to extract from the device. By connecting a phone via USB cable, Wi-Fi or Bluetooth you can perform individual examinations of most mobile devices and generate reports in multiple formats (PDF, HTML, Excel, etc.) for a variety of needs.



Main Functions:

- **Messages** – Messages are fully retrieved for analysis and presented in the Messages Report, including deleted messages when available.

- **Conversations** – Efficiently read through entire uninterrupted conversation streams. The Conversations Reports separates entire conversations by contact and are ordered by time sequence.

- **Call Logs** – The Calls Report provides details of all mobile service and applications-based phone calls, including deleted calls. Pin-point the time and date of when the suspect made or received calls, the duration of the call, the source (mobile, Facebook, WhatsApp etc.) and the contact and phone number associated with each call.

- **Emails** – Emails are fully retrieved for analysis and presented in the Emails Report, including deleted messages when available. Customize the report and sort by contact, timeline, conversation view, or both.

- **Applications** – Perform an advanced applications analysis. All applications are listed and fully analyzed for their detailed data, including deleted applications data where available, and presented in the Applications Report.

- **Integrate** – We understand an investigator may use many tools in an investigation. We've designed our software with the ability to integrate with other forensic tools in your lab.

- **Deleted Data** – Deleted data is often the key information in an investigation. Deleted data details are presented in a special comprehensive Deleted Data Report, and also displayed within each individual analysis report.

- **Passwords** – The Passwords Report will reveal passwords from many types of accounts and applications. In iOS devices all system passwords and most application passwords are managed through dedicated and encrypted Keychain.

- **Wi-Fi Networks** – This section contains detailed data about all Wi-Fi networks saved in a device. The Wi-Fi Networks Report displays the history of Wi-Fi connections in time sequential order, including the Wi-Fi network name, the last joined time and date, the last auto-joined time and date etc.

- **Images** – The Images Report will contain images from the phone file system. This includes application images – images retrieved from applications data, which might also include images stored in temporary files or caches that have been detected as potential images.

- **Photos** – The Photos Report retrieves all device and applications photos taken by the phone, usually in the DCIM folder. iPhone deleted photos can be recovered if they were sent via MMS or from a supported application.

- **Cell Towers** – Data about cell towers that the subject phone was connected to can be obtained. Obtained cell tower locations can be individually viewed on the map through the provided link.

- **Audio Files** – Audio files are copied from the device and its applications. The Audio Files Report allows you to play an audio file simply by clicking on it in the report. The report also details the file path, the created and modified time, the duration of the audio file and the size of the audio file.

- **Video Files** – Video files are also copied from the device and its applications. The Video Files Report allows you to play a video file by clicking on it in the report. The report also details the file path, the created, modified, encoded and tagged time, the duration of the video, the size of the video file as well as the frame rate, height and width.

- **Documents** – Extract and preview most common document formats.

- **GPS Locations** – Knowing when and where a suspect has been is key in every investigation. The GPS Locations Report contains all possible GPS location data from the device and applications.

- **Cookies** – The Cookies Report compiles the history of cookies in a device. System cookies are only obtainable from iOS devices. Application specific cookies are analyzed for every installed application. Cookies contain information about web domain as well as their creation, accessed and expiration time, and if the displayed cookie has been deleted.

- **Web Browsing History** – The Web Browsing History Report contains a consolidated web browsing history from all analyzed browser applications. Each web browsing history entry consists of the visited URL as well as time of the visit.

- **Bluetooth Pairings** – Bluetooth pairing history can be discovered on both Android and iOS devices and is presented in the Bluetooth Pairings Report. In the report you will find the name of the Bluetooth connection, the Bluetooth address of the pairing device, the status, and on iOS- the date and time of the last connection.

- **Contact Analysis** – Contact analysis is a section with analyzed relationships between contacts and the way they were used in various modes of communication. It is also possible to skip contacts that have rarely been communicated with on that mobile phone.

- **System Logs** – The System Logs Report contains system logs and dumpsys files that can be extracted from Android phones. The Android system keeps these files for debugging and monitoring purposes and they contain system data such as recent locations, recent connected Wi-Fi networks, running applications, recently launched applications, recent cell locations and signal info, current Bluetooth MAC address and name etc. These files are listed in the System Logs section within the HTML and PDF reports and can be directly opened by clicking on their filenames. Their content is analyzed and presented in various reports such as Wi-Fi Networks, GPS Locations, Notifications etc.

- **File System** – The File System Report is divided in three section according their source. Internal – which includes raw file system. Then Application File System which contains application data files. The third is the Extra File System, which contains information about files that are not physically present on device but are available to be extracted. This includes all files from iTunes backup on iOS devices. On Android devices, Content Providers, System Logs and DumpSys fall into this category.

- **Timelines** – The Timeline Report provides insight into all device activity exactly as it occurred. The report aggregates all extracted items that contain time and date information and displays it in chronological order. Exact parameters of a generated timeline can be customized to specific function; for example, you can select to configure a timeline of calls and messages only.

- **Photo Recognizer** – This module automatically locates and recognizes suspicious content in photos such as weapons, drugs, nudity, currency and documents. Photo Recognizer utilizes artificial intelligence and deep machine learning to quickly analyze an unlimited number of photos, and is designed to eliminate countless hours that would be spent manually searching for key evidence in huge databases of photos. Each photo is placed in its own specific category so the investigator can keep the case well-organized and easily present the suspicious content in a fine-tuned report.

Practical 3

a. Using File Recovery Tools [FTK Imager] Creating Image

Install FTK Imager to a local hard drive when you intend to attach evidence hardware to that computer for previewing and imaging evidence.

To install FTK Imager

1. Execute the setup file by double-clicking it.
2. On the Welcome screen, click Next.
3. Read and accept the License Agreement, then click Next.
4. Do one of the following:
   - Accept the default installation location.
   - Browse to a different destination folder.
5. Click Next.
6. In the Ready to Install screen, click Next.
7. Do one of the following:
   - Mark the Launch AccessData FTK Imager box to force Imager to run immediately after the install is complete.
   - Leave the box unmarked to run the newly installed program at a later time.
8. You must manually run FTK Imager after installation.
9. Click Finish to complete the installation and close the wizard.

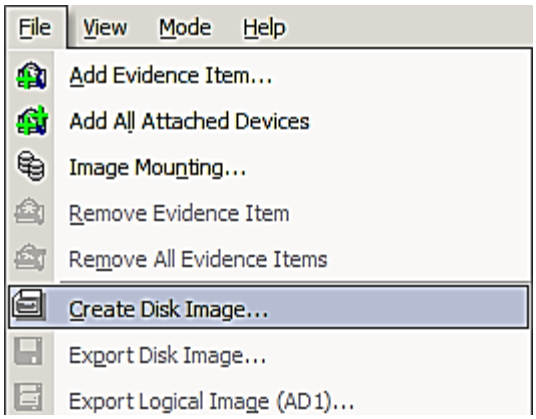
Running FTK Imager

FTK Imager can be run in a variety of ways:

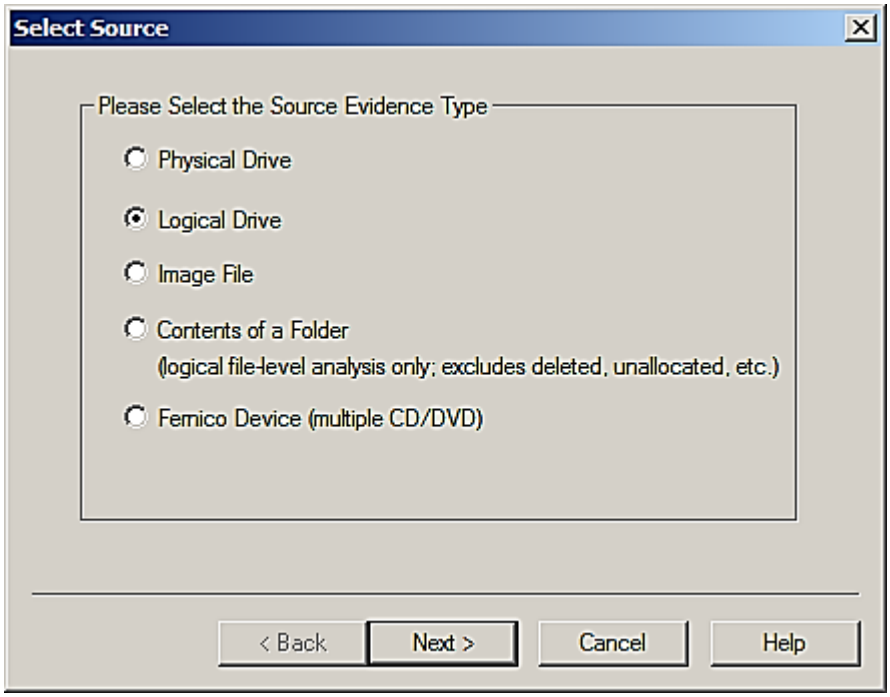
- Double-click on the desktop icon.
- Execute the FTK Imager.exe file from a thumb drive.
- Click Start > Run > Browse. Browse to and select FTK

To create a forensic image

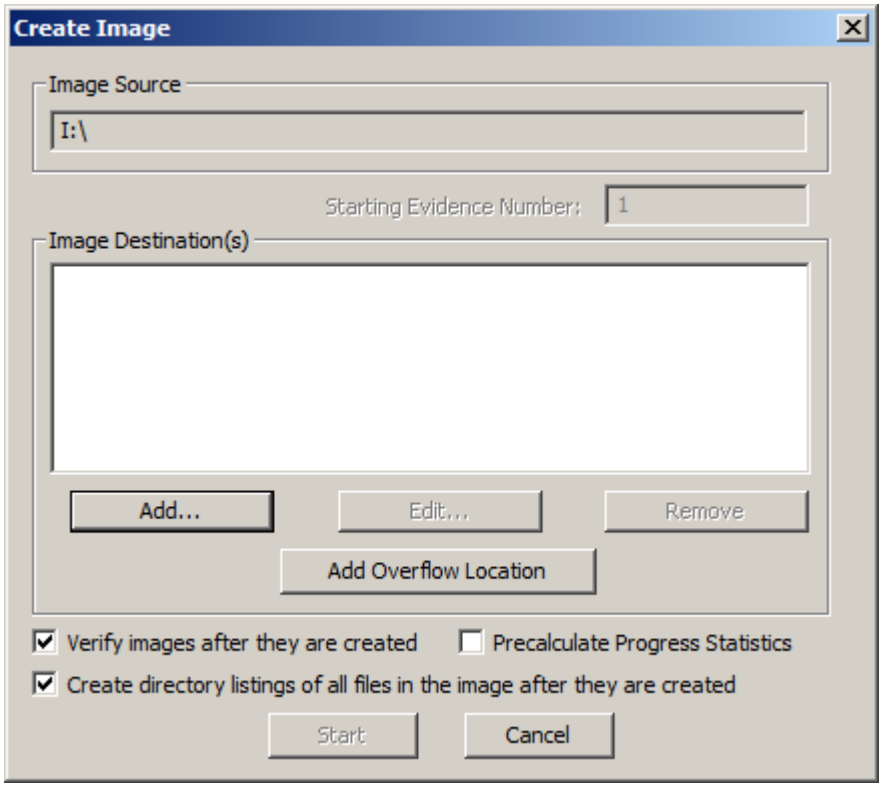
1. Do one of the following: Click File > Create Disk Image.
2. Click the Create Disk Image button on the Toolbar.



In the Select Source dialog box, select the source you want to make an image of.

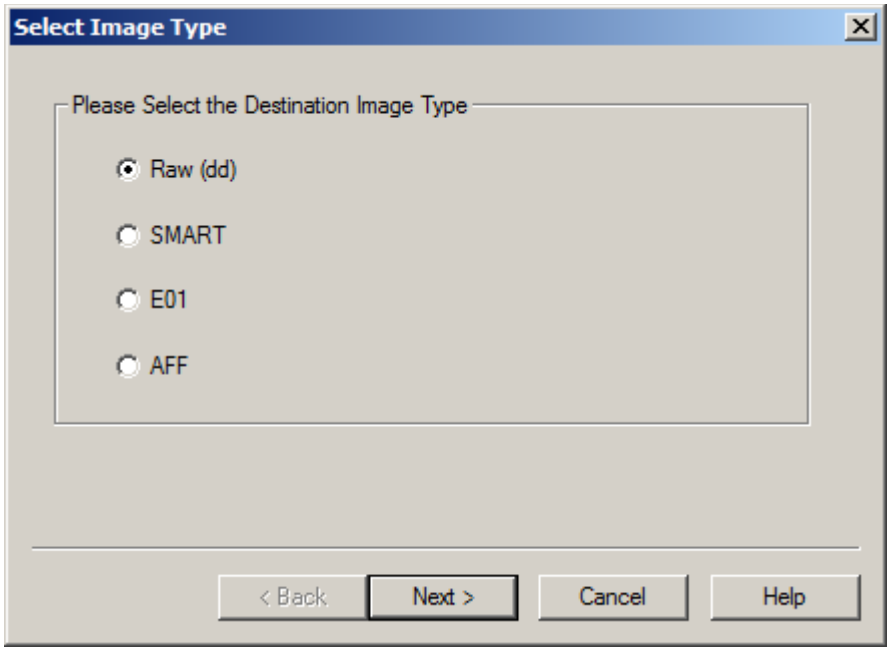


3. Click Next.
4. If you select Logical Drive and need to select a floppy or CD as a source, you can check the Automate multiple removable media box to create groups of images. Imager will automatically increment the case numbers with each image, and if something interrupts the process, you may assign case number manually.
5. Select the drive or browse to the source of the image you want, and then click Finish
6. In the Create Image dialog, click Add.

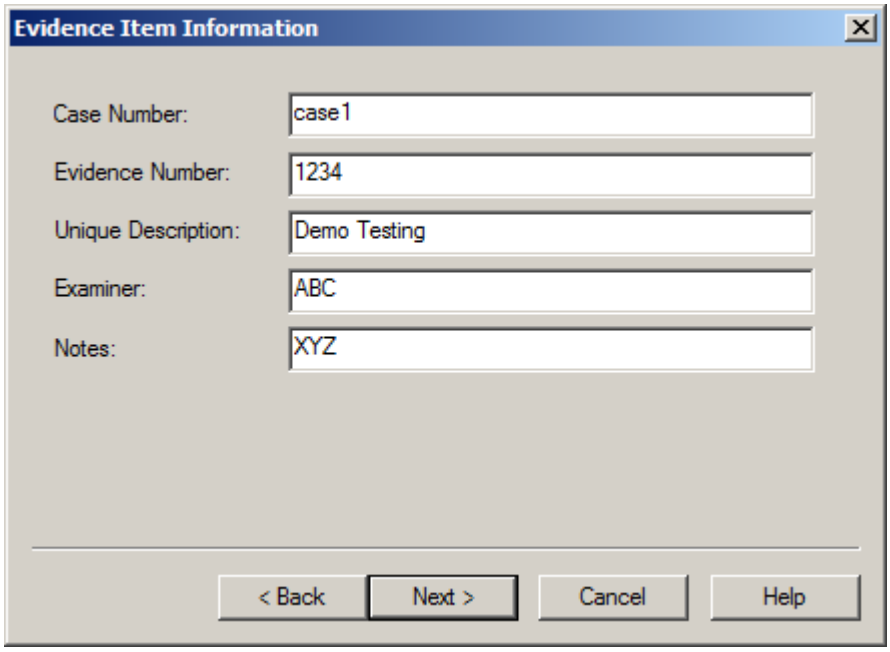


Select the type of image you want to create.

If you are creating an AFF image type, choose AFF. The Image Destination Folder dialog box you see will be different than that seen when selecting ay other image type. Click Next.



Specify Evidence Item Information. All Evidence Item Information is optional, but it is helpful to have the information easily accessible in case it is called into question at any time after creation. Complete the fields in the Evidence Item Information dialog

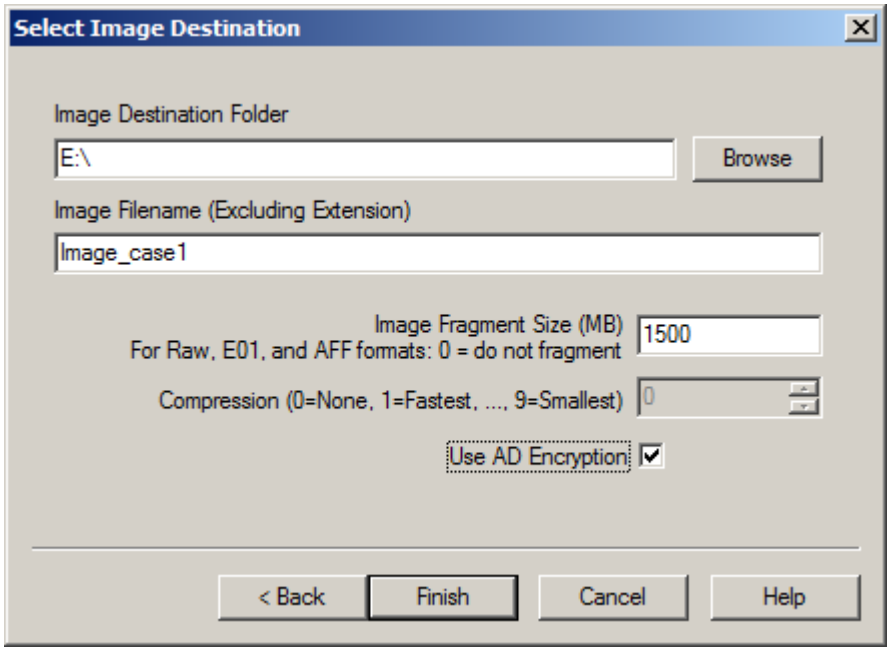


Click Next.

In the Image Destination Folder field, do one of the following:

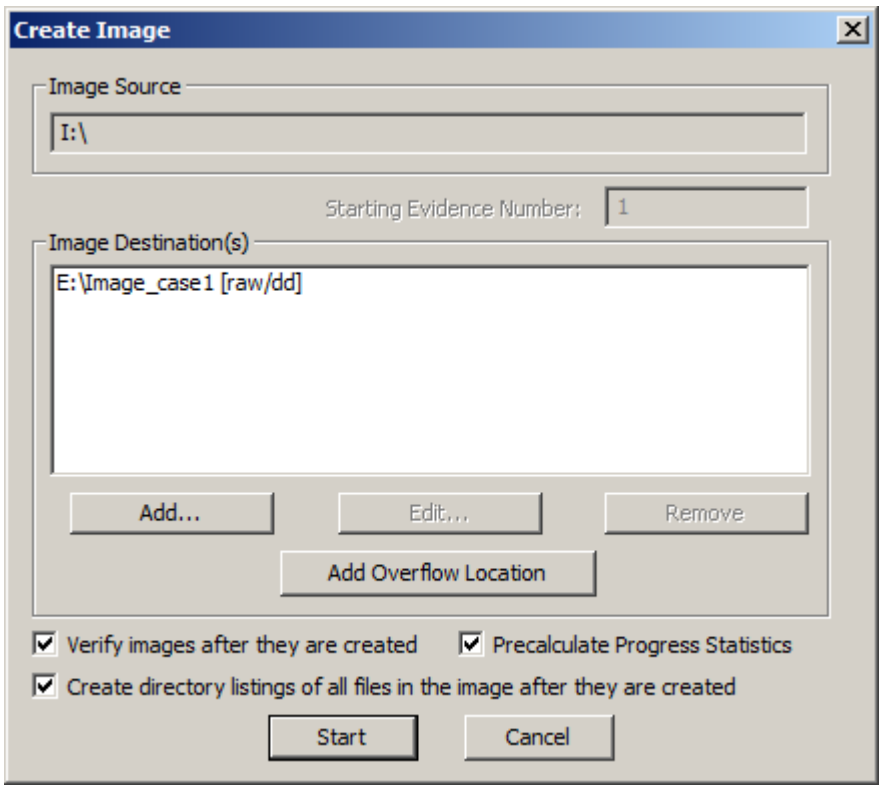
Type the location path where you want to save the image file.

Click Browse to find and select the desired location.



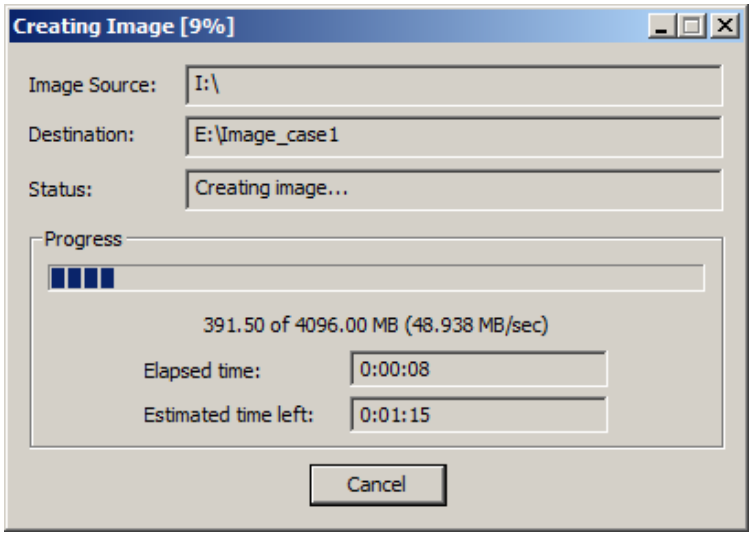
To encrypt the new image with AD Encryption, mark the Use AD Encryption box. Click Finish.

When AD Encryption is selected, you can choose between encrypting with a password, or encrypting with a certificate.



Click Start to begin the imaging process.

A progress dialog appears that shows the following:



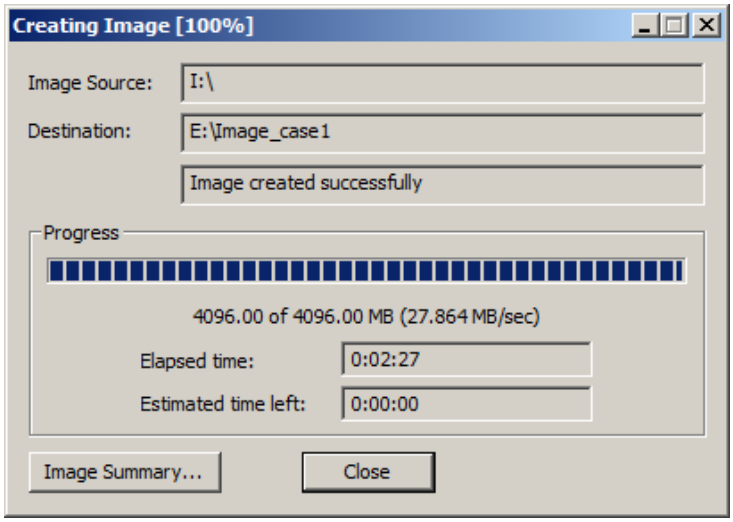
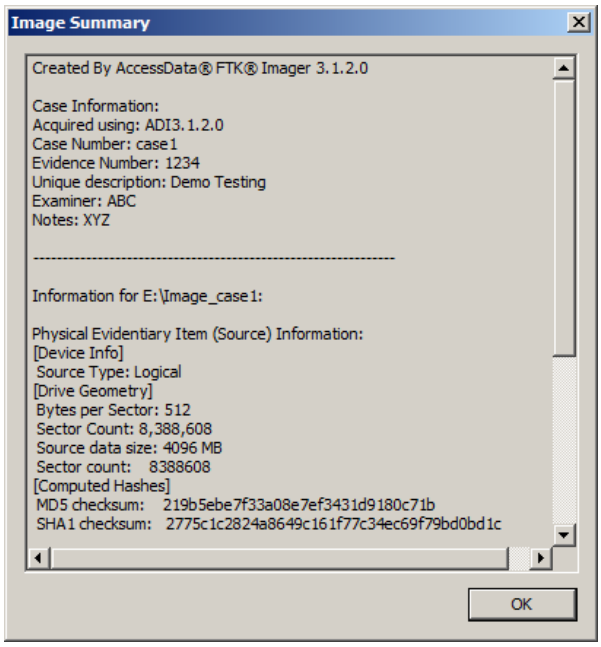
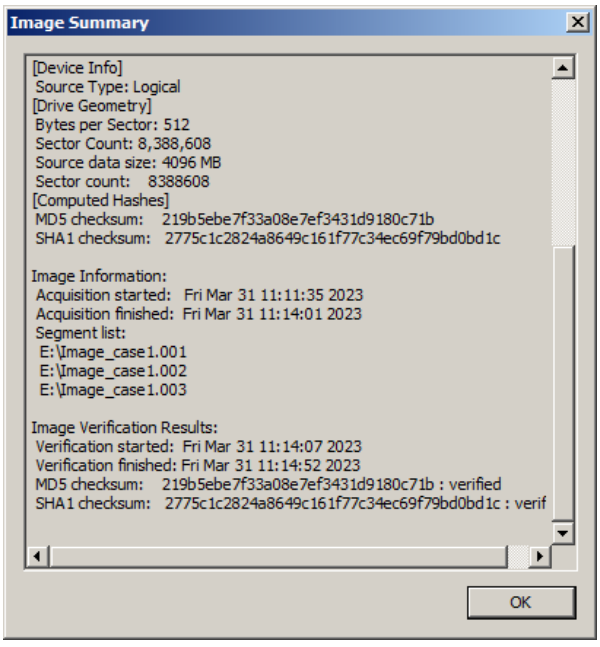


Image Summary button. Click it to open the Image Summary window as shown below:



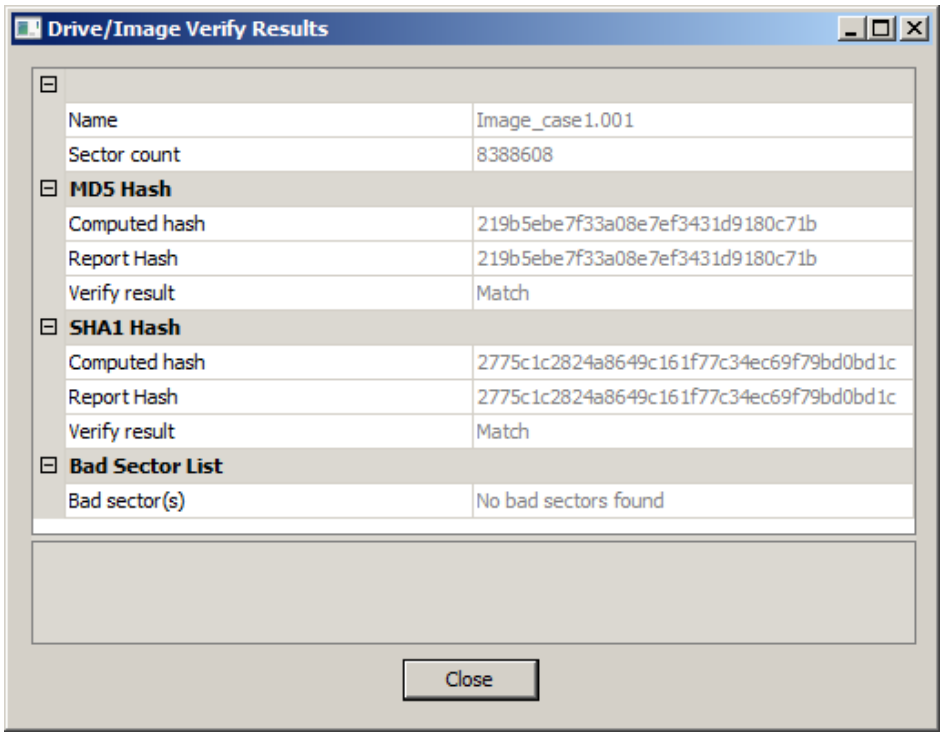


Click OK to close the Image Summary.

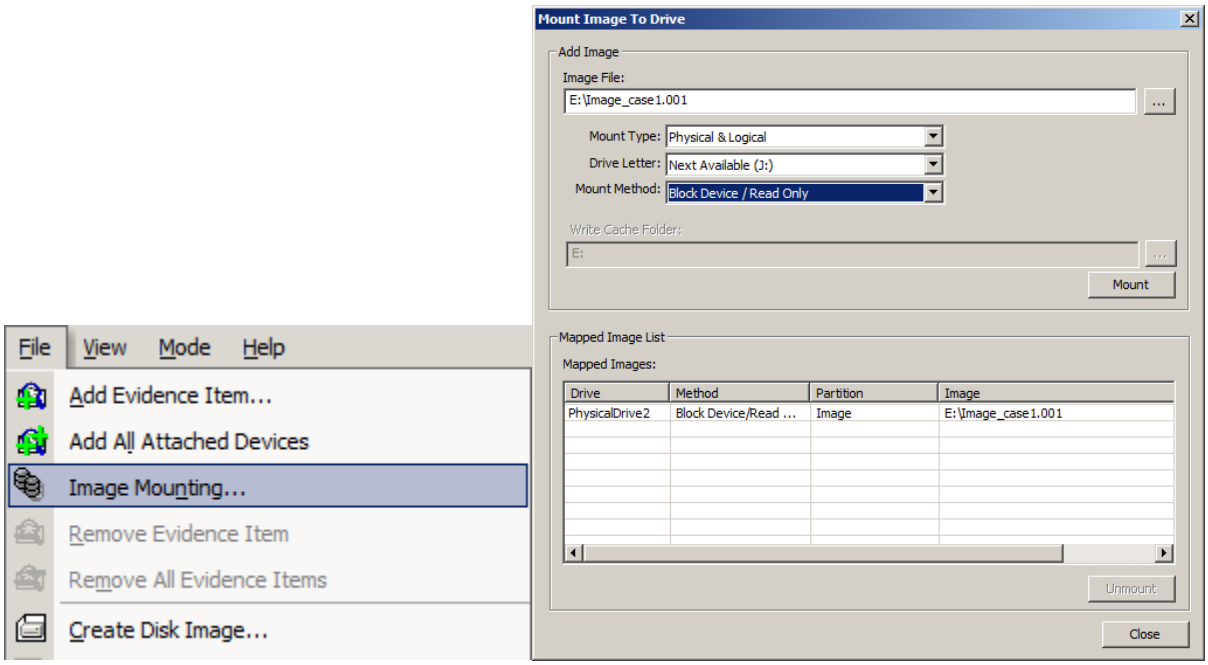
Click OK to return to the Creating Image dialog.

Click Close to exit back to Imager.

After the images are successfully created, the Drive/Image Verify Results box shows detailed image information, including MD5 and SHA1 check sums, and bad sectors.



File - > image Mount to access created image file



b. Using Forensic Toolkit (FTK) &Writing report using FTK (Access Data FTK)

This is a sample forensic report of Volatile Memory using the tool "**FTK Imager Lite** by **AccessData**". This procedure is used by investigating agencies to log each step in evidence acquisition process, and the report is presented in the court for the hearing.

1. Introduction

The purpose of this report is to present the findings of the digital forensic investigation conducted using the Forensic Toolkit (FTK) in relation to the hacking incident on PCno 35 in computer lab. This investigation aimed to identify the extent of the intrusion, the methods employed by the attacker, and any potential damage caused. The report outlines the methodology followed, the evidence collected, and the results of the analysis using FTK.

2. Case Details

2.1 Case Background On 13th March 2023, it was reported that PCno35 had been compromised in a hacking incident. The investigation focused on identifying the unauthorized access, understanding the attack vectors employed, and assessing the impact on the system's security. The goal was to determine the scope of the breach and gather evidence for potential legal actions.

2.2 Digital Evidence The digital evidence collected for analysis using FTK includes the following sources:

Source 1: Server logs

Source 2: Network traffic capture

3. Methodology

The investigation followed a standard digital forensic methodology, consisting of the following steps:

3.1 Evidence Identification and Collection The digital evidence was identified and collected using best practices to preserve its integrity. The server logs (Source 1) were obtained from the affected system, while the network traffic capture (Source 2) was acquired from network monitoring devices. The acquisition process ensured the collection of comprehensive and unaltered evidence.

3.2 Evidence Examination using FTK FTK was employed to examine the collected evidence. FTK's specialized features for analysing network traffic and log files were utilized to identify potential indicators of compromise (IOCs), trace the attacker's activities, and reconstruct the attack timeline.

4. Evidence Analysis

4.1 Source 1: Server Logs Analysis

The analysis of the server logs focused on identifying abnormal activities, unauthorized access attempts, and any signs of compromise. FTK's log analysis capabilities were employed to extract relevant information, including log entries related to the intrusion. Noteworthy findings include:

- Numerous failed login attempts from suspicious IP addresses.
- Successful logins using unauthorized user credentials.
- Unusual outbound network connections from the compromised system.

4.2 Source 2: Network Traffic Capture Analysis

The examination of the network traffic capture aimed to identify any malicious activities or communication associated with the hacking incident. FTK's network analysis features were utilized to dissect the captured traffic and extract valuable information. Key findings from the analysis include:

- Outbound connections to known command and control (C&C) servers.
- Evidence of data exfiltration through encrypted channels.
- Unusual network traffic patterns indicative of lateral movement within the network.

Results and Interpretation Based on the analysis conducted using FTK, the following conclusions can be drawn:

- The server logs indicate multiple failed login attempts and successful logins using unauthorized credentials, suggesting a successful intrusion.
- The presence of outbound connections to known C&C servers indicates command-driven activities by the attacker.
- Evidence of data exfiltration and abnormal network traffic patterns suggest lateral movement and potential compromise of other systems within the network.

5. Conclusion

The analysis of the digital evidence using FTK has provided crucial insights into the hacking incident on Pcno35. The findings reveal a successful intrusion, unauthorized access, and potential data exfiltration, indicating a significant security breach. These findings serve as valuable evidence for further investigation, mitigation efforts, and legal actions against the attacker.

Chain of Custody

CASE NO: C001

DESCRIPTION OF EVIDENCE			
DEVICE TYPE	**DEVICE NAME**	**STATE**	**CONNECTIVITY**
PC	DESKTOP-B2CFDA0	ON	WIRELESS PRESENT

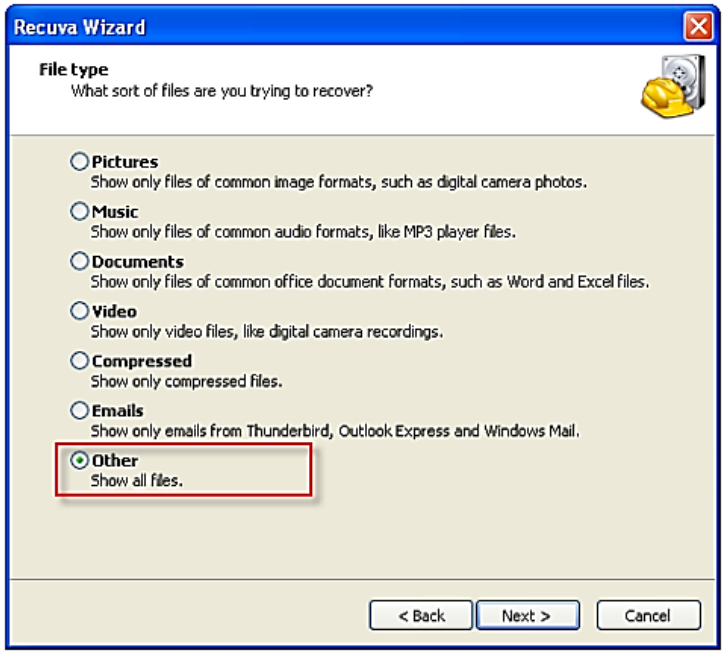
DESCRIPTION OF DEVICE				
LABEL #	**MANUFACTURER**	**OS**	**RAM**	**ARCHITECTURE**
1	HP	WINDOWS 10	4GB	X64

Practical 4

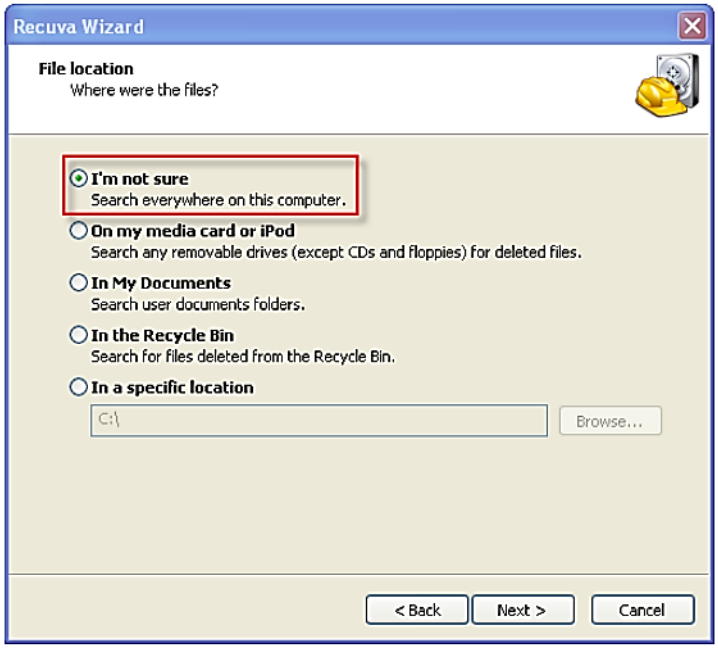
Recover Deleted files using

a) Recuva

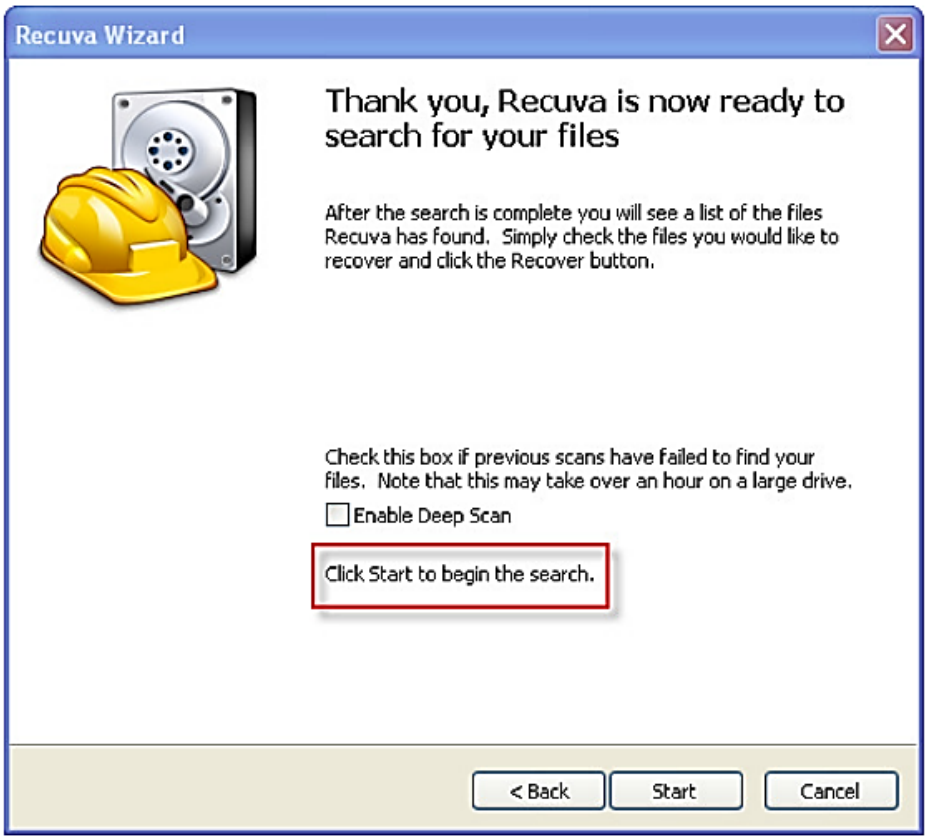
In the initial Recuva pop-up, we read how the tool can help us. Let's use the wizard and see what it can do. Click Next.



Again, here we select the option which gives us the largest possible list of possibilities, for the sake of this demonstration. The "I'm not sure" option will begin a search that is not limited to any particular location on the computer. In your particular situation, it may be more appropriate to select "In My Documents", or "In the Recycle Bin", for example. Click Next.



Here we note that there is another option: Enable Deep Scan. Recuva will usually locate your file without using the Deep Scan option, but if it doesn't, try again using this option. The main difference here is time. If you're in a hurry, don't select the option. If the file is not found, or if time is not an issue, select the Deep Scan option for the most accurate and comprehensive result. Click Start.



Recuva then makes a couple of passes over the computer storage to locate missing files:

b) PC Inspector File Recovery

When you delete a file in Windows, the file is moved to the Recycle Bin. If you open the Recycle Bin, you will see it there. The file can be moved out of the Recycle Bin either by dragging it to a location or Restoring it to the old location. If you Empty the Recycle Bin, for all practical purposes, the file is then deleted. If you delete a file from a diskette or flash drive, the file does not go to the Recycle Bin.

Formatting drives

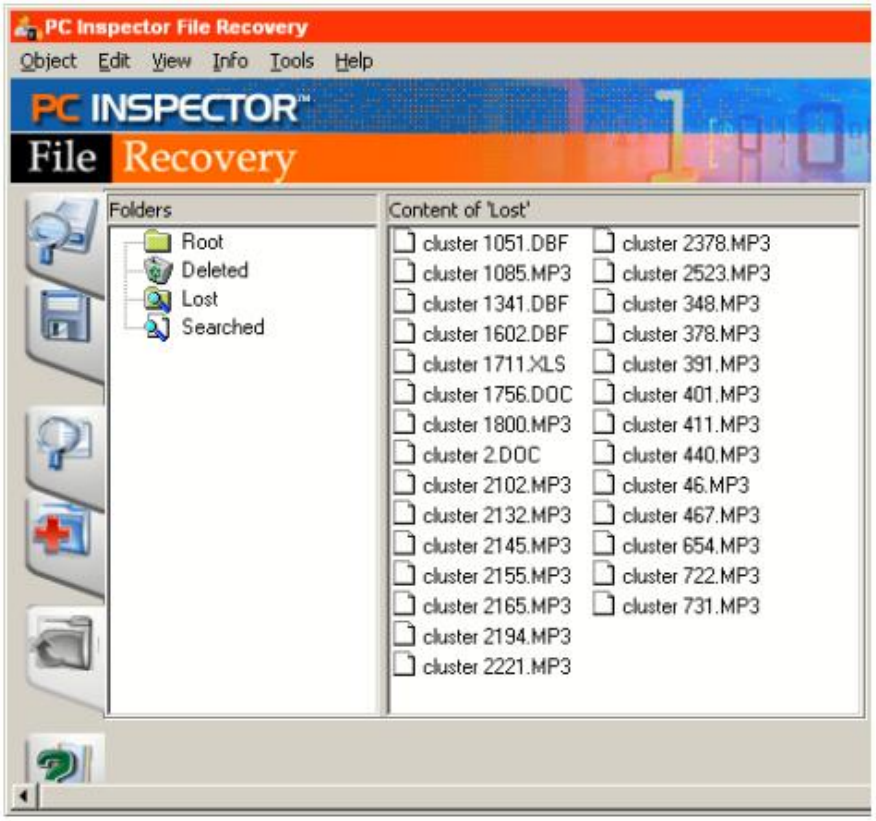
Open MyComputer. Right-click the drive letter for the device you want to format. In the pop-up menu, choose Format…. If you want a low-level format, check the Quick Format box. If you want the full format, leave the box unchecked. Click Start. When the warning box appears, click OK. When the format is complete, click OK. Click Close.

Recovering deleted files

The freeware program use for deleted file recovery is PC Inspector File Recovery. There are many others. These programs can "look behind the scenes" to see if files still exist and if so, attempt to recover them. Businesses that specialize in "data disaster" recovery use tools such as this. After running the program, the results are shown in Figure 1 on the next page. All the files shown have been "deleted" and do not show up in Windows file listing.

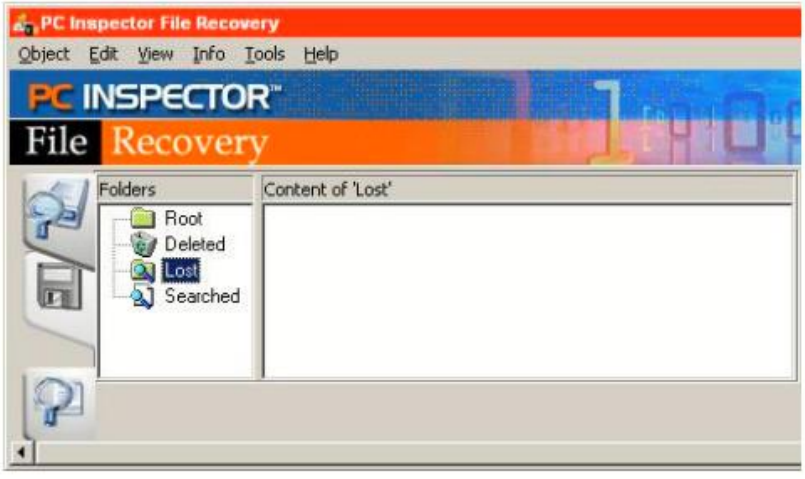
Quick format

After using the Quick Format option in Windows, the files still have not been erased on either a diskette or a flash drive. However, the FAT (file allocation table) has been deleted. The operating system thus cannot read the list of files on the disk. It might be more difficult to recover these "cluster" files.



Full format

In the Full format mode (Quick format box is not checked), the files really are gone on a diskette! (Well, not really, but only intensive data recovery efforts will bring them back.) A flash drive cannot be full-formatted – at least not by the method used for diskettes. If you want to be sure there is no trace of files on either a flash drive or a diskette, use a Wipe program.)



c) Recover My Files

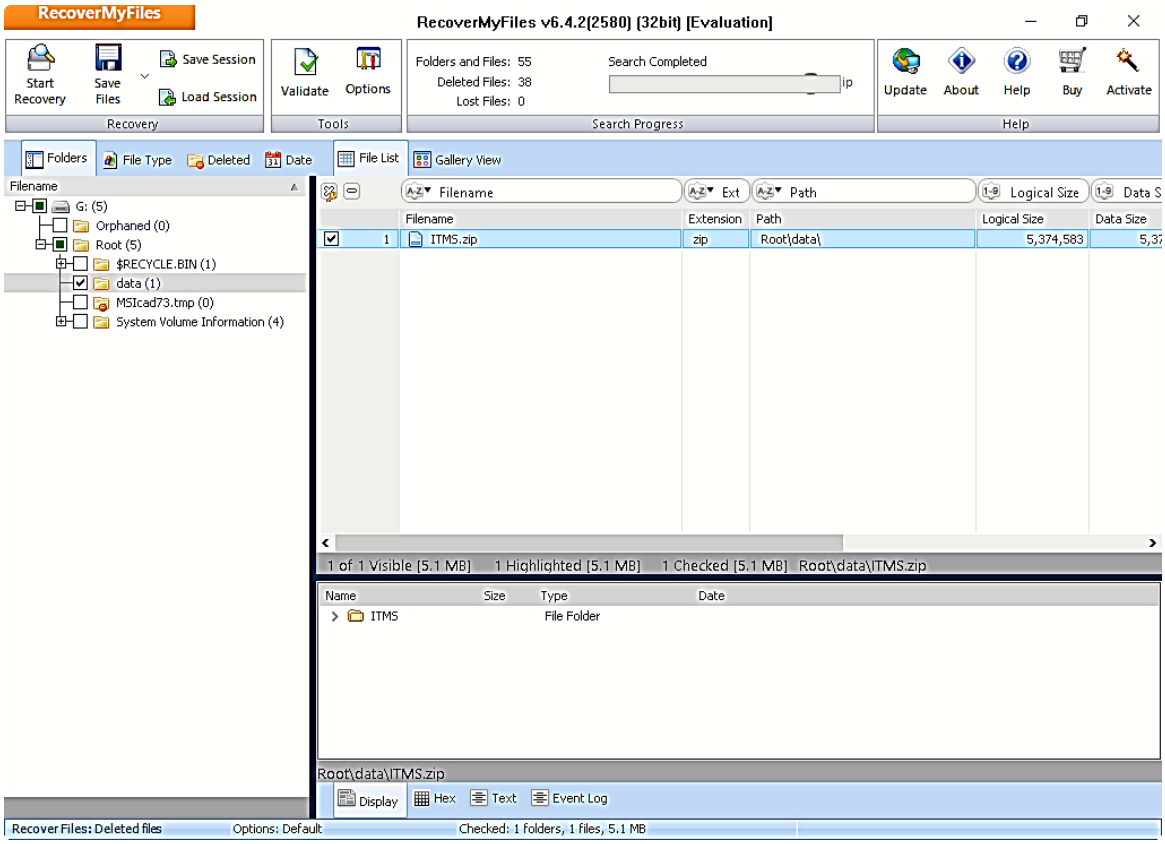
Run Recover My Files. In the wizard, click the "Recover Files" icon (if the Wizard screen is not open, click the Start icon in the toolbar) and click the Next button:

In the drive selection window highlight the drive letter from which the files are missing and click Next.

Select the File Recovery options:

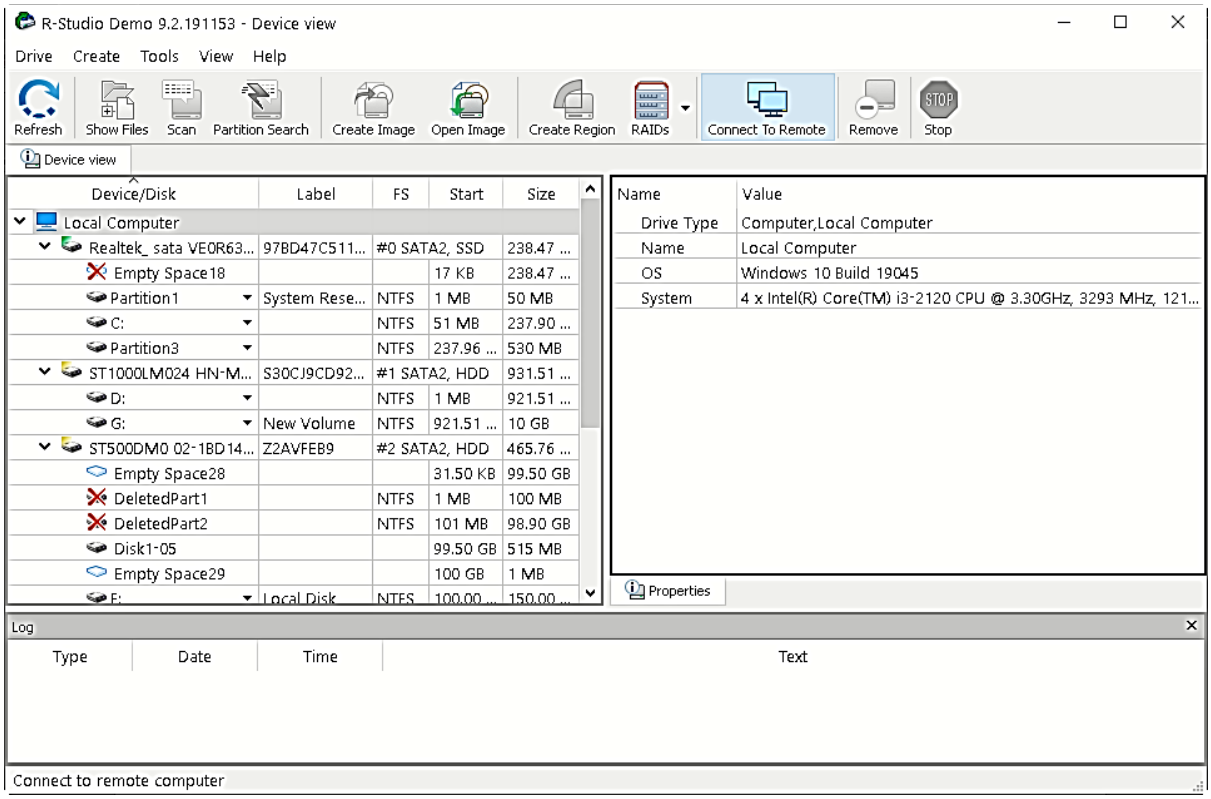
To search for deleted files: 1. Select the “Search for deleted files.” option; 2. Click the Start button.

Click the icon in the search results screen to expand folders. Use the different data view and sort and filter functions to determine if the missing files have been located.



d) R Studio

Basic file recovery can be made for deleted files that has resided on an existing logical disk visible to the operating system. In all other cases, Advanced Data Recovery is required.



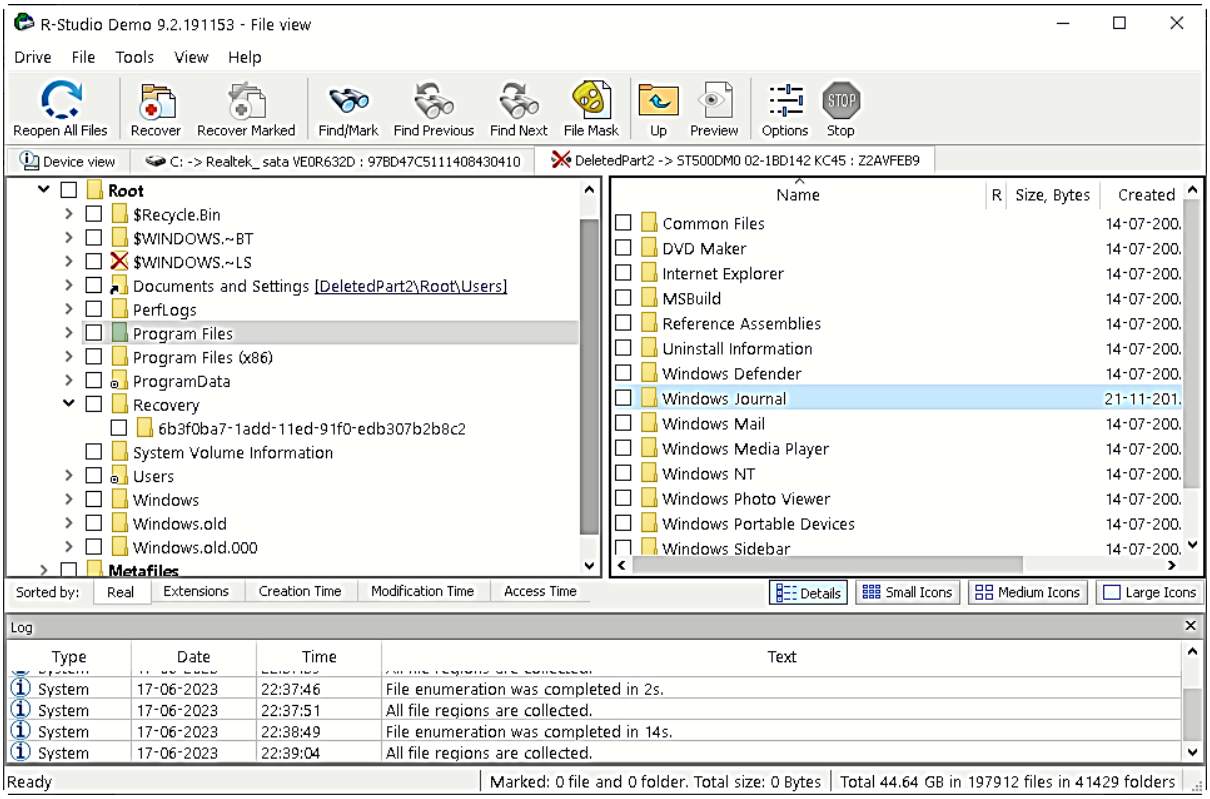
To recover deleted files from a logical disk (recognized partition),

1. Double-click a logical disk in the R-Studio's Drives panel to enumerate files on the disk
2. Other ways to enumerate files

- Select the disk and click the Open Drive Files button, or
- Right-click the selected disk and select Open Drive Files on the shortcut menu, or
- Select the disk and press the F5 key. or
- Select Open Drive Files on the Drive menu

3. If you try to enumerate files on a drive or another object without a valid file system on it, a Double-click a logical disk... message will appear.
4. Select a logical disk on the object or scan the object.
5. R-Studio will change its panel showing the disk's folders/?files structure.
6. R-Studio analyzes data on the object and displays all files for which records have been found in the analysed tables.

If files have not been found, that means that their records have been deleted. To find such files, Advanced Data Recovery is required.

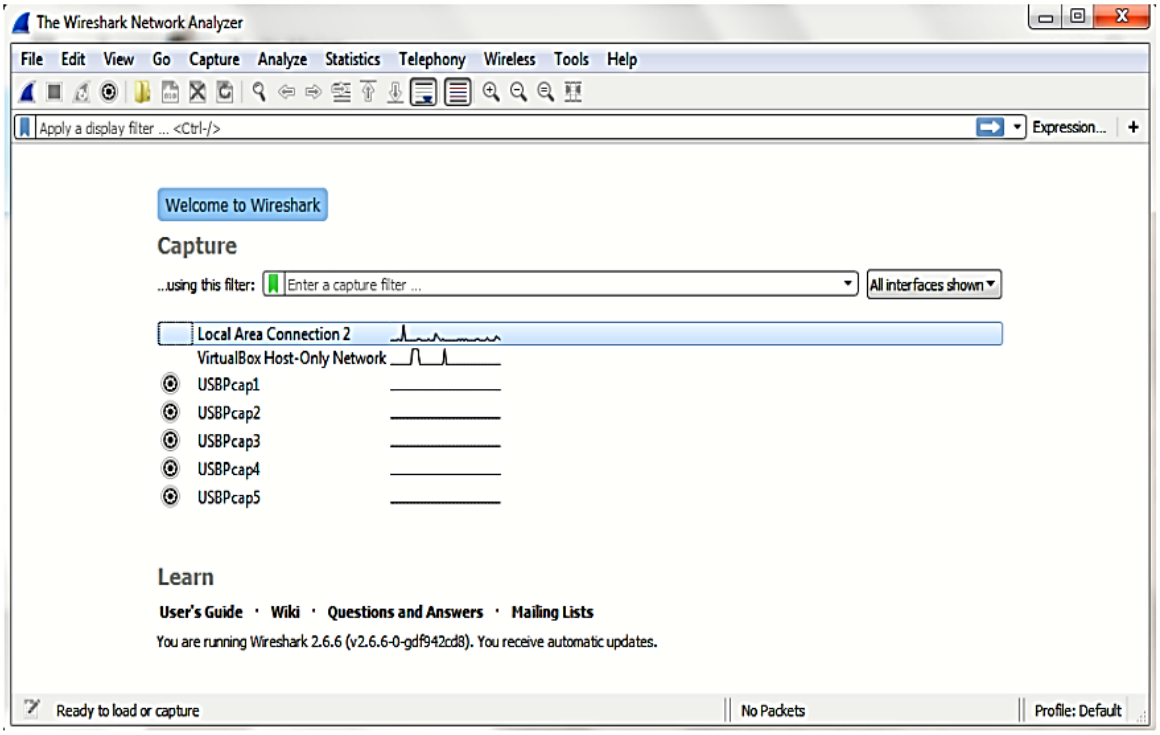

R-Studio Demo 9.2.191153 - File view
Drive File Tools View Help
Reopen All Files
Recover
Recover Marked
Find/Mark
Find Previous
Find Next
File Mask
Up
Preview
Options
Stop
Device view
C: -> Realtek_ sata VE0R632D : 97BD47C5111408430410
DeletedPart2 -> ST500DM0 02-1BD142 KC45 : Z2AVFEB9
Root
$Recycle.Bin
$WINDOWS.~BT
$WINDOWS.~LS
Documents and Settings [DeletedPart2\Root\Users]
PerfLogs
Program Files
Program Files (x86)
ProgramData
Recovery
6b3f0ba7-1add-11ed-91f0-edb307b2b8c2
System Volume Information
Users
Windows
Windows.old
Windows.old.000
Metafiles
Name
R
Size, Bytes
Created
Common Files 14-07-200.
DVD Maker 14-07-200.
Internet Explorer 14-07-200.
MSBuild 14-07-200.
Reference Assemblies 14-07-200.
Uninstall Information 14-07-200.
Windows Defender 14-07-200.
Windows Journal 21-11-201.
Windows Mail 14-07-200.
Windows Media Player 14-07-200.
Windows NT 14-07-200.
Windows Photo Viewer 14-07-200.
Windows Portable Devices 14-07-200.
Windows Sidebar 14-07-200.
Sorted by:
Real
Extensions
Creation Time
Modification Time
Access Time
Details
Small Icons
Medium Icons
Large Icons
Log
Type
Date
Time
Text
System 17-06-2023 22:37:46 File enumeration was completed in 2s.
System 17-06-2023 22:37:51 All file regions are collected.
System 17-06-2023 22:38:49 File enumeration was completed in 14s.
System 17-06-2023 22:39:04 All file regions are collected.
Ready
Marked: 0 file and 0 folder. Total size: 0 Bytes
Total 44.64 GB in 197912 files in 41429 folders

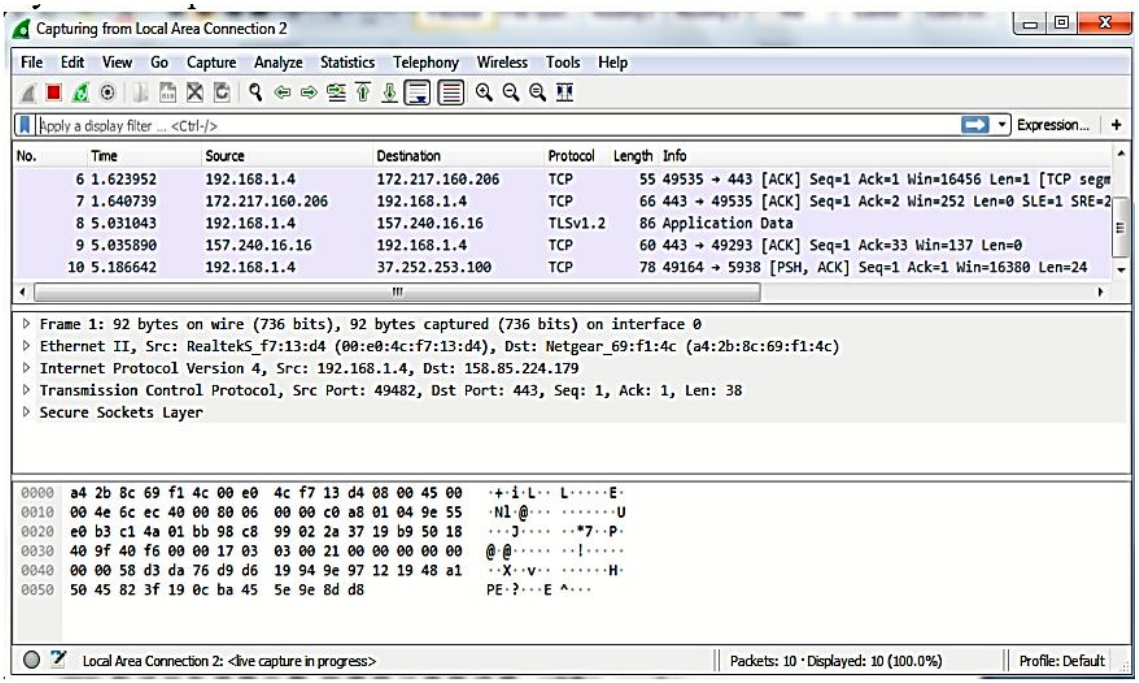
Practical 5

a) Using Log & Traffic Capturing & Analysis Tools [Wireshark]

Capturing Packets

Capture traffic on your wireless network, click your wireless interface. You can configure advanced features by clicking Capture > Options, but this isn't necessary for now.





As soon as you single-click on your network interface's name, you can see how the packets are working in real time.

Wireshark will capture all the packets going in and out of our systems. Promiscuous mode is the mode in which you can see all the packets from other systems on the network and not only the packets send or received from your network adapter.

Promiscuous mode is enabled by default. To check if this mode is enabled, go to Capture and Select Options. Under this window check, if the checkbox is selected and activated at the bottom of the window. The checkbox says "Enable promiscuous mode on all interfaces".

The red box button "STOP" on the top left side of the window can be clicked to stop the capturing of traffic on the network.

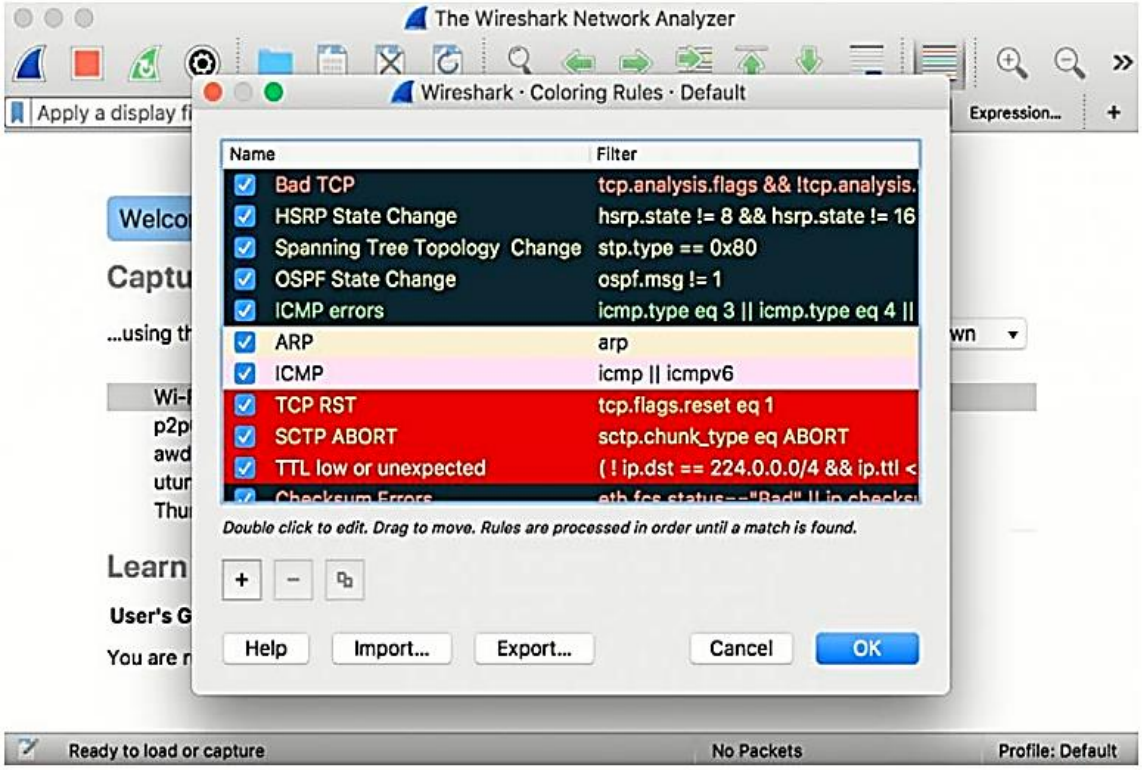
Color Coding

Different packets are seen highlighted in various different colors. This is Wireshark's way of displaying traffic to help you easily identify the types of it.

Default colors are:

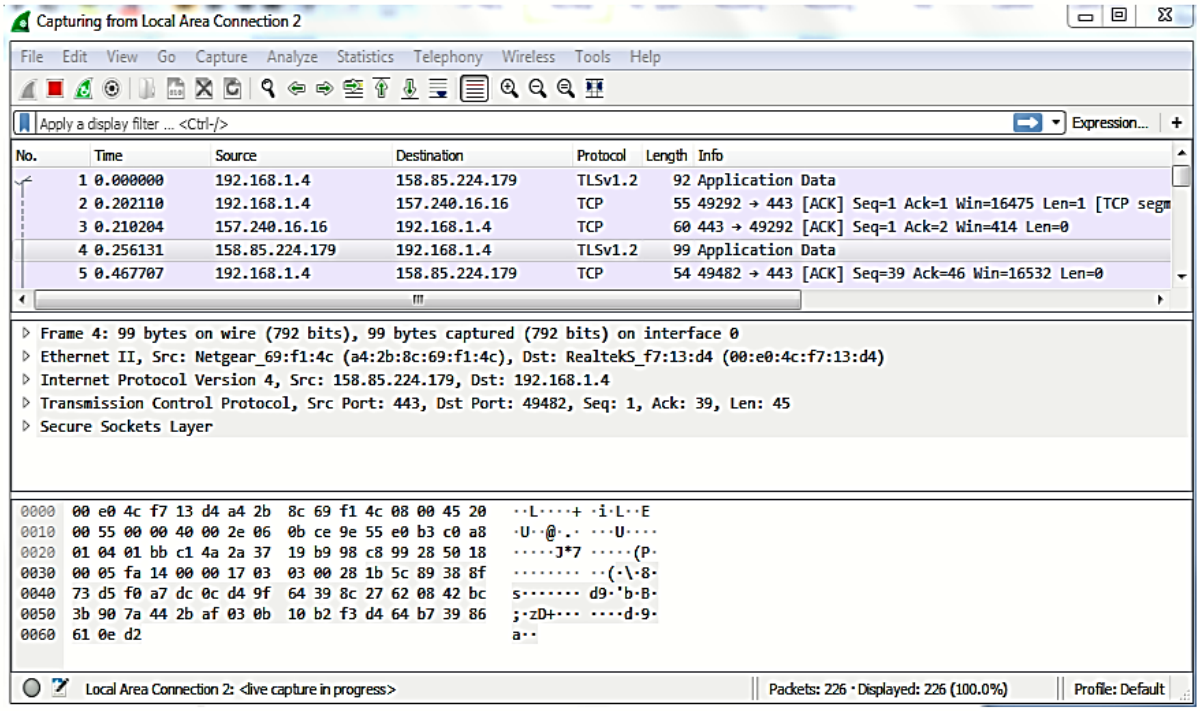
- Light Purple color for TCP traffic
- Light Blue color for UDP traffic
- Black color identifies packets with errors – example these packets are delivered in an unordered manner.

To check the color coding rules click on View and select Coloring Rules. These color coding rules can be customized and modified to fit your needs.

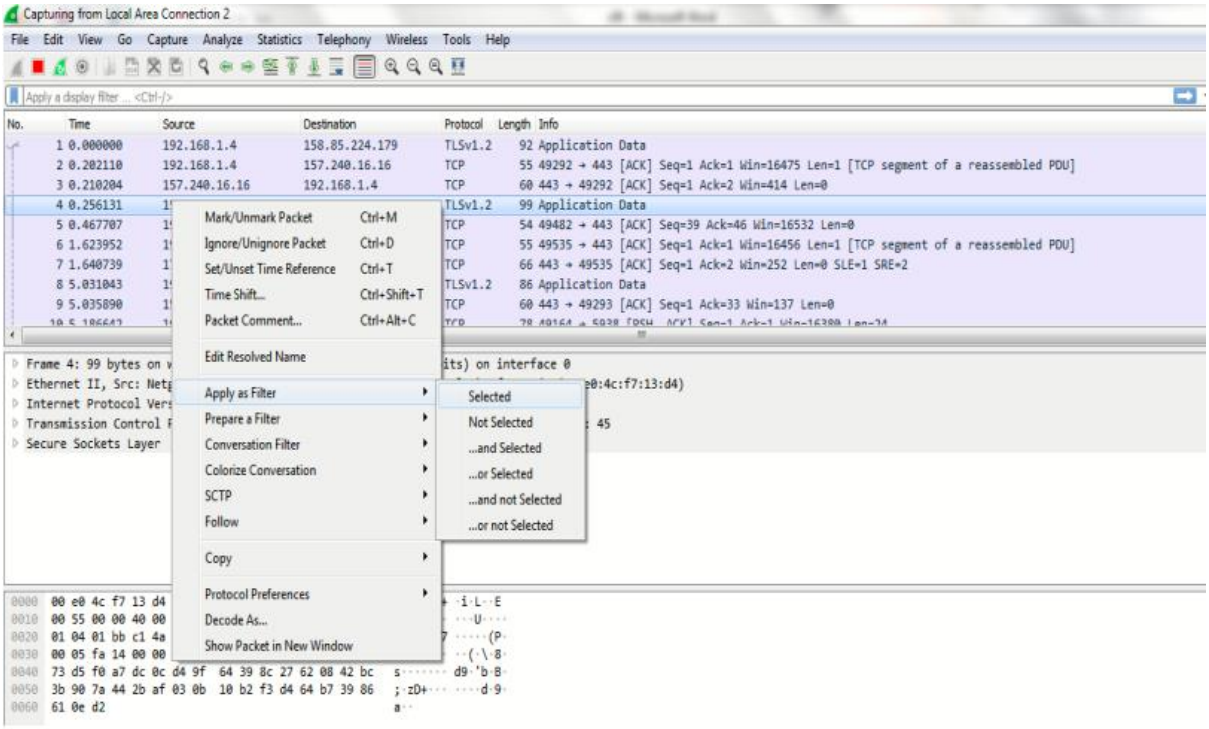


Analyse the captured Packets:

First of all, click on a packet and select it. Now, you can scroll down to view all its details.

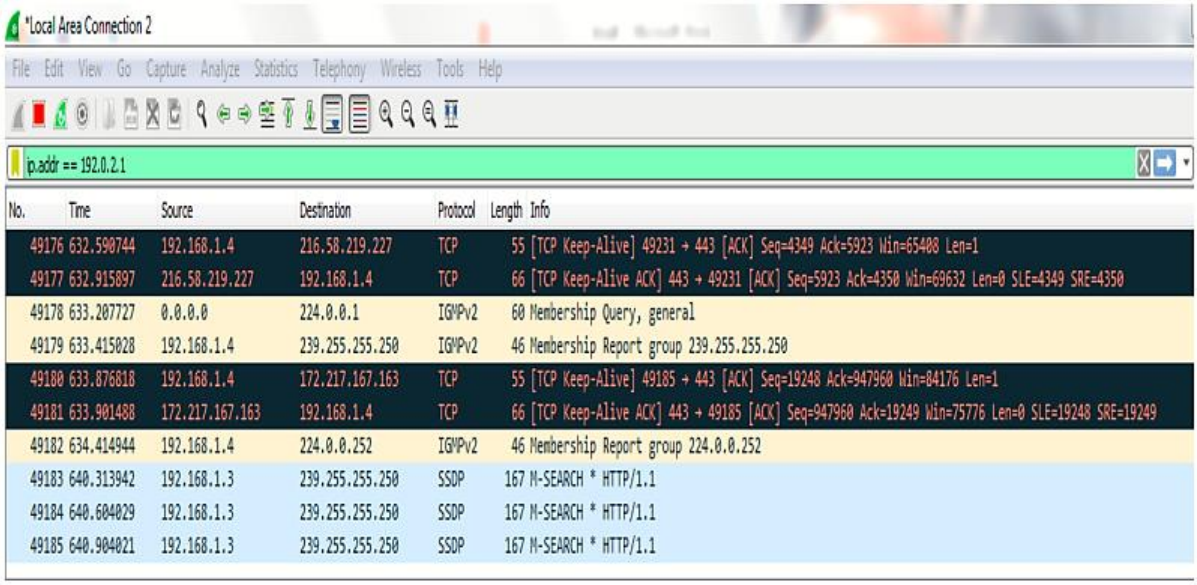


Filters can also be created from here. Right-click on one of any details. From the menu select Apply as Filter drop-down menu so filter based on it can be created.

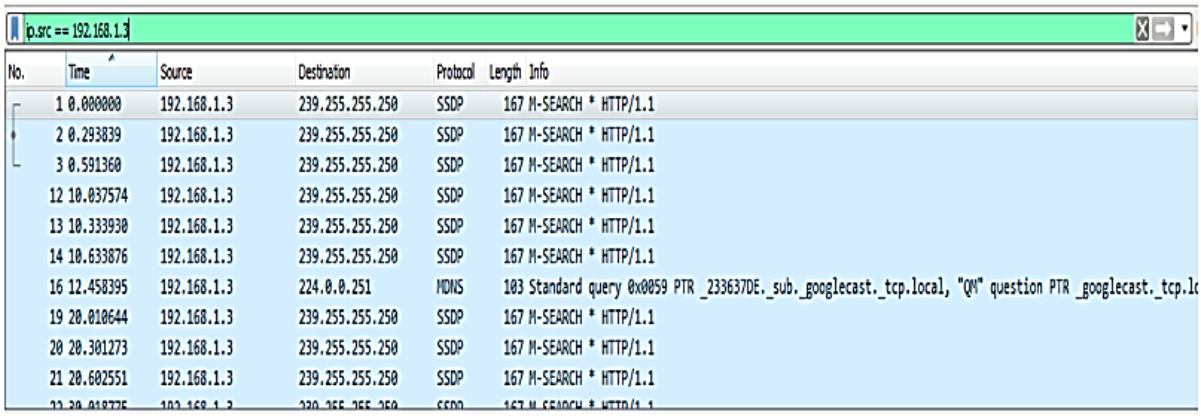


Display filter command –

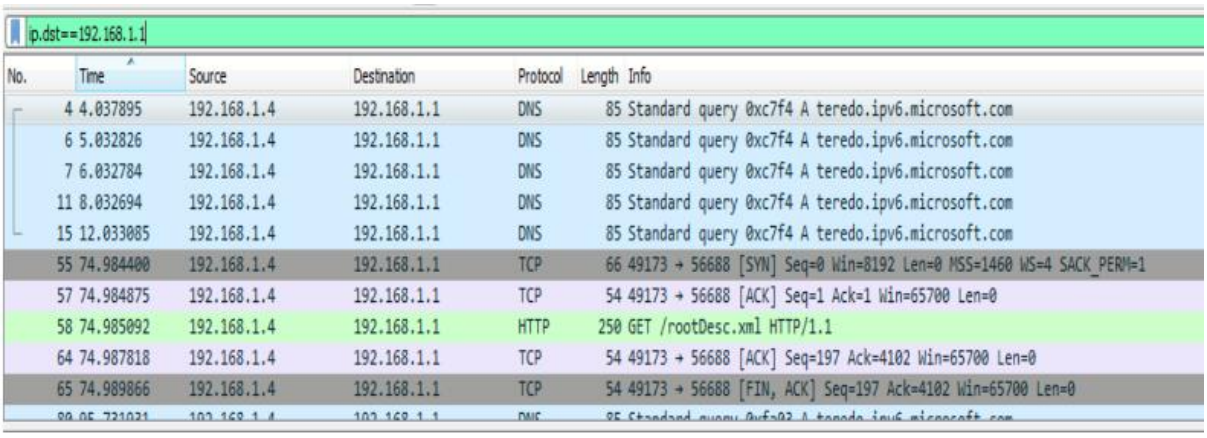
1. Display packets based on specific IP-address ¬ ip.addr == 192.0.2.1



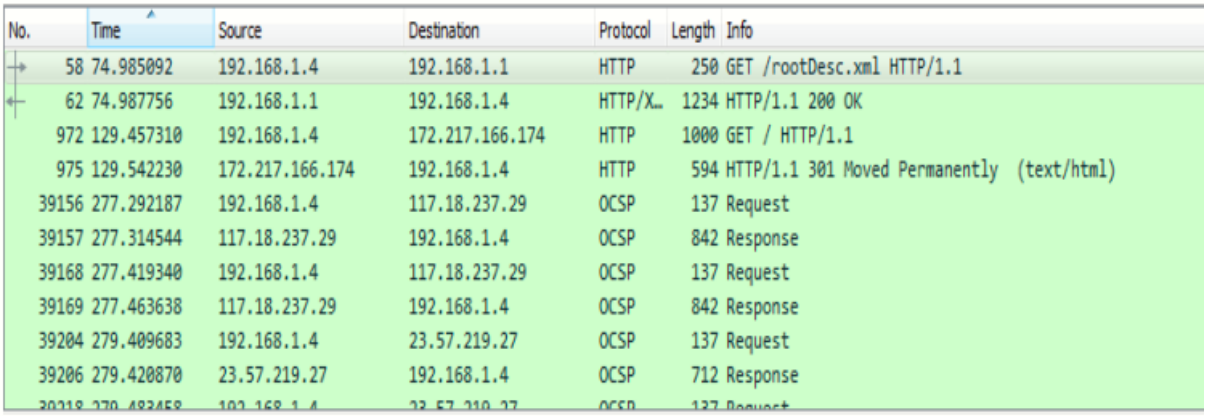
2. Display packets which are coming from specific IP-address ¬ ip.src == 192.168.1.3



3. Display packets which are having specific IP-address destination ¬ ip.dst == 192.168.1.1

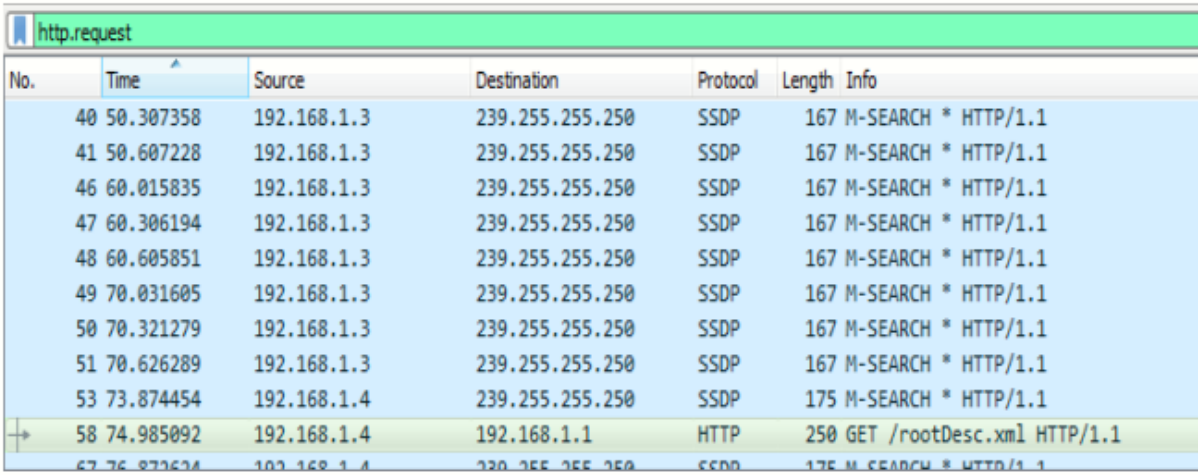


4. Display packets which are using http protocol ¬ http



No.	Time	Source	Destination	Protocol	Length	Info
58	74.985092	192.168.1.4	192.168.1.1	HTTP	250	GET /rootDesc.xml HTTP/1.1
62	74.987756	192.168.1.1	192.168.1.4	HTTP/X…	1234	HTTP/1.1 200 OK
972	129.457310	192.168.1.4	172.217.166.174	HTTP	1000	GET / HTTP/1.1
975	129.542230	172.217.166.174	192.168.1.4	HTTP	594	HTTP/1.1 301 Moved Permanently (text/html)
39156	277.292187	192.168.1.4	117.18.237.29	OCSP	137	Request
39157	277.314544	117.18.237.29	192.168.1.4	OCSP	842	Response
39168	277.419340	192.168.1.4	117.18.237.29	OCSP	137	Request
39169	277.463638	117.18.237.29	192.168.1.4	OCSP	842	Response
39204	279.409683	192.168.1.4	23.57.219.27	OCSP	137	Request
39206	279.420870	23.57.219.27	192.168.1.4	OCSP	712	Response

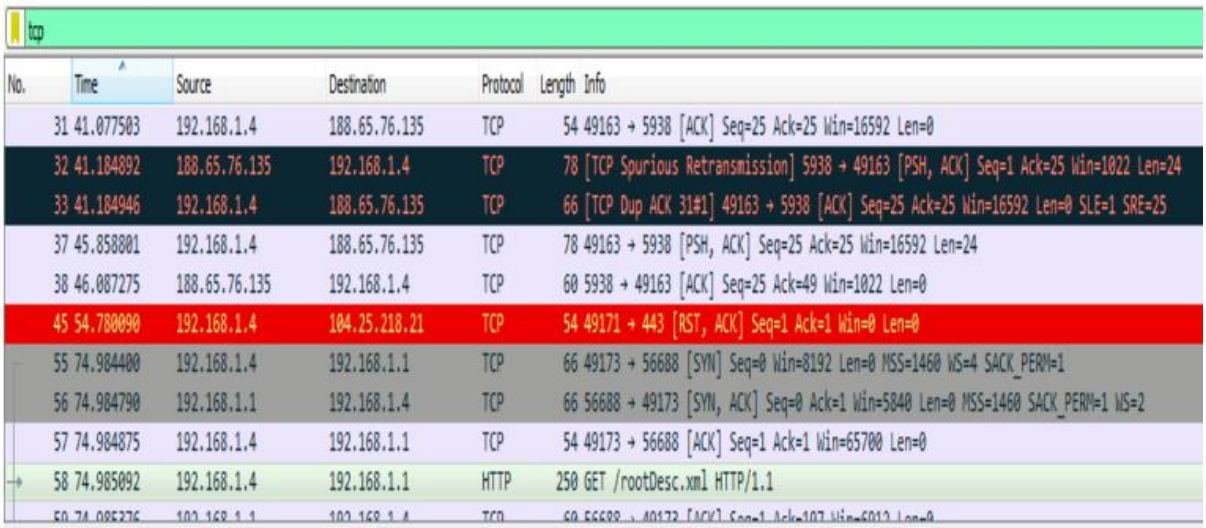
5. Display packets which are using http request ¬ http.request



http.request

No.	Time	Source	Destination	Protocol	Length	Info
40	50.307358	192.168.1.3	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
41	50.607228	192.168.1.3	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
46	60.015835	192.168.1.3	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
47	60.306194	192.168.1.3	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
48	60.605851	192.168.1.3	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
49	70.031605	192.168.1.3	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
50	70.321279	192.168.1.3	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
51	70.626289	192.168.1.3	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
53	73.874454	192.168.1.4	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
58	74.985092	192.168.1.4	192.168.1.1	HTTP	250	GET /rootDesc.xml HTTP/1.1

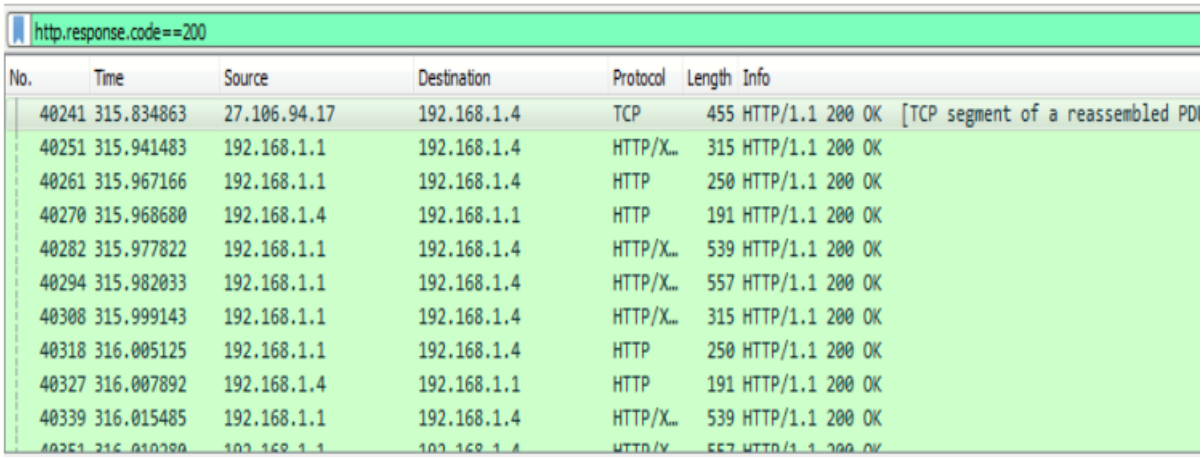
6. Display packets which are using TCP protocol ¬ tcp



tcp

No.	Time	Source	Destination	Protocol	Length	Info
31	41.077503	192.168.1.4	188.65.76.135	TCP	54	49163 → 5938 [ACK] Seq=25 Ack=25 Win=16592 Len=0
32	41.184892	188.65.76.135	192.168.1.4	TCP	78	[TCP Spurious Retransmission] 5938 → 49163 [PSH, ACK] Seq=1 Ack=25 Win=1022 Len=24
33	41.184946	192.168.1.4	188.65.76.135	TCP	66	[TCP Dup ACK 31#1] 49163 → 5938 [ACK] Seq=25 Ack=25 Win=16592 Len=0 SLE=1 SRE=25
37	45.858801	192.168.1.4	188.65.76.135	TCP	78	49163 → 5938 [PSH, ACK] Seq=25 Ack=25 Win=16592 Len=24
38	46.087275	188.65.76.135	192.168.1.4	TCP	60	5938 → 49163 [ACK] Seq=25 Ack=49 Win=1022 Len=0
45	54.780090	192.168.1.4	104.25.218.21	TCP	54	49171 → 443 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
55	74.984400	192.168.1.4	192.168.1.1	TCP	66	49173 → 56688 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
56	74.984790	192.168.1.1	192.168.1.4	TCP	66	56688 → 49173 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1 WS=2
57	74.984875	192.168.1.4	192.168.1.1	TCP	54	49173 → 56688 [ACK] Seq=1 Ack=1 Win=65700 Len=0
58	74.985092	192.168.1.4	192.168.1.1	HTTP	250	GET /rootDesc.xml HTTP/1.1

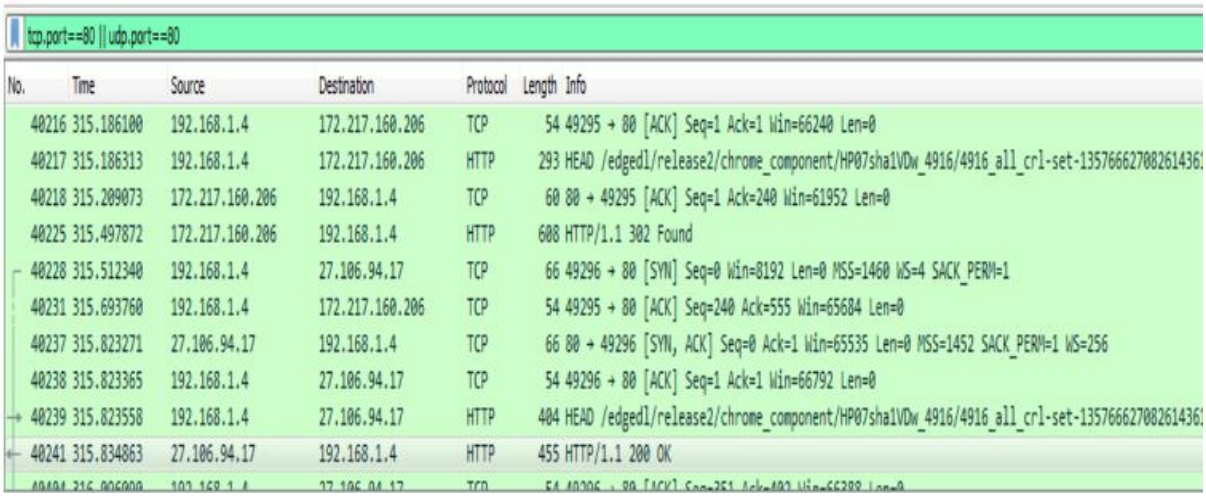
7. Display packets having no error connecting to server ¬ http.response.code==200



http.response.code==200

No.	Time	Source	Destination	Protocol	Length	Info
40241	315.834863	27.106.94.17	192.168.1.4	TCP	455	HTTP/1.1 200 OK [TCP segment of a reassembled PDU
40251	315.941483	192.168.1.1	192.168.1.4	HTTP/X…	315	HTTP/1.1 200 OK
40261	315.967166	192.168.1.1	192.168.1.4	HTTP	250	HTTP/1.1 200 OK
40270	315.968680	192.168.1.4	192.168.1.1	HTTP	191	HTTP/1.1 200 OK
40282	315.977822	192.168.1.1	192.168.1.4	HTTP/X…	539	HTTP/1.1 200 OK
40294	315.982033	192.168.1.1	192.168.1.4	HTTP/X…	557	HTTP/1.1 200 OK
40308	315.999143	192.168.1.1	192.168.1.4	HTTP/X…	315	HTTP/1.1 200 OK
40318	316.005125	192.168.1.1	192.168.1.4	HTTP	250	HTTP/1.1 200 OK
40327	316.007892	192.168.1.4	192.168.1.1	HTTP	191	HTTP/1.1 200 OK
40339	316.015485	192.168.1.1	192.168.1.4	HTTP/X…	539	HTTP/1.1 200 OK

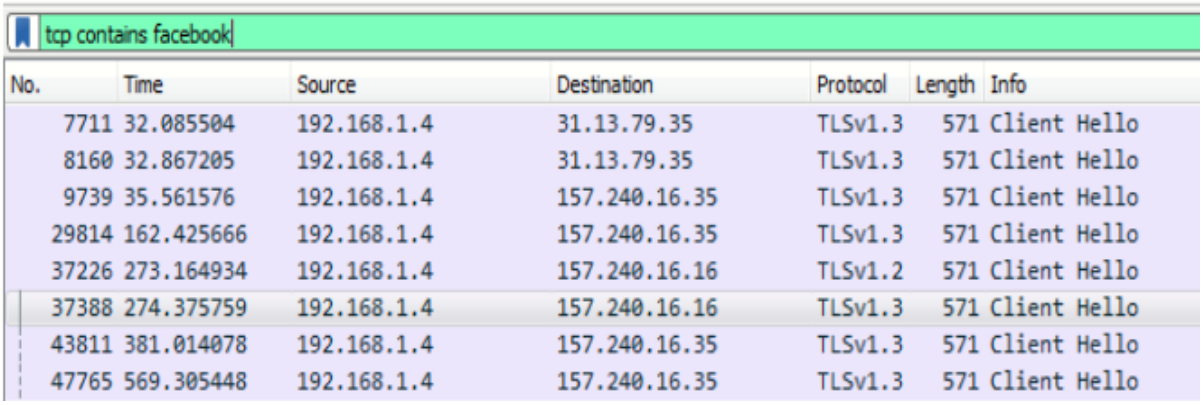
8. Display packets having port number 80 ¬ tcp.port==80 || udp.port==80



tcp.port==80 || udp.port==80

No.	Time	Source	Destination	Protocol	Length	Info
40216	315.186100	192.168.1.4	172.217.160.206	TCP	54	49295 → 80 [ACK] Seq=1 Ack=1 Win=66240 Len=0
40217	315.186313	192.168.1.4	172.217.160.206	HTTP	293	HEAD /edgedl/release2/chrome_component/HP07sha1VDw_4916/4916_all_crl-set-13576662708261436
40218	315.209073	172.217.160.206	192.168.1.4	TCP	60	80 → 49295 [ACK] Seq=1 Ack=240 Win=61952 Len=0
40225	315.497872	172.217.160.206	192.168.1.4	HTTP	608	HTTP/1.1 302 Found
40228	315.512340	192.168.1.4	27.106.94.17	TCP	66	49296 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
40231	315.693760	192.168.1.4	172.217.160.206	TCP	54	49295 → 80 [ACK] Seq=240 Ack=555 Win=65684 Len=0
40237	315.823271	27.106.94.17	192.168.1.4	TCP	66	80 → 49296 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1452 SACK_PERM=1 WS=256
40238	315.823365	192.168.1.4	27.106.94.17	TCP	54	49296 → 80 [ACK] Seq=1 Ack=1 Win=66792 Len=0
40239	315.823558	192.168.1.4	27.106.94.17	HTTP	404	HEAD /edgedl/release2/chrome_component/HP07sha1VDw_4916/4916_all_crl-set-13576662708261436
40241	315.834863	27.106.94.17	192.168.1.4	HTTP	455	HTTP/1.1 200 OK

9. Display packets which that contains keyword facebook ¬ tcp contains facebook



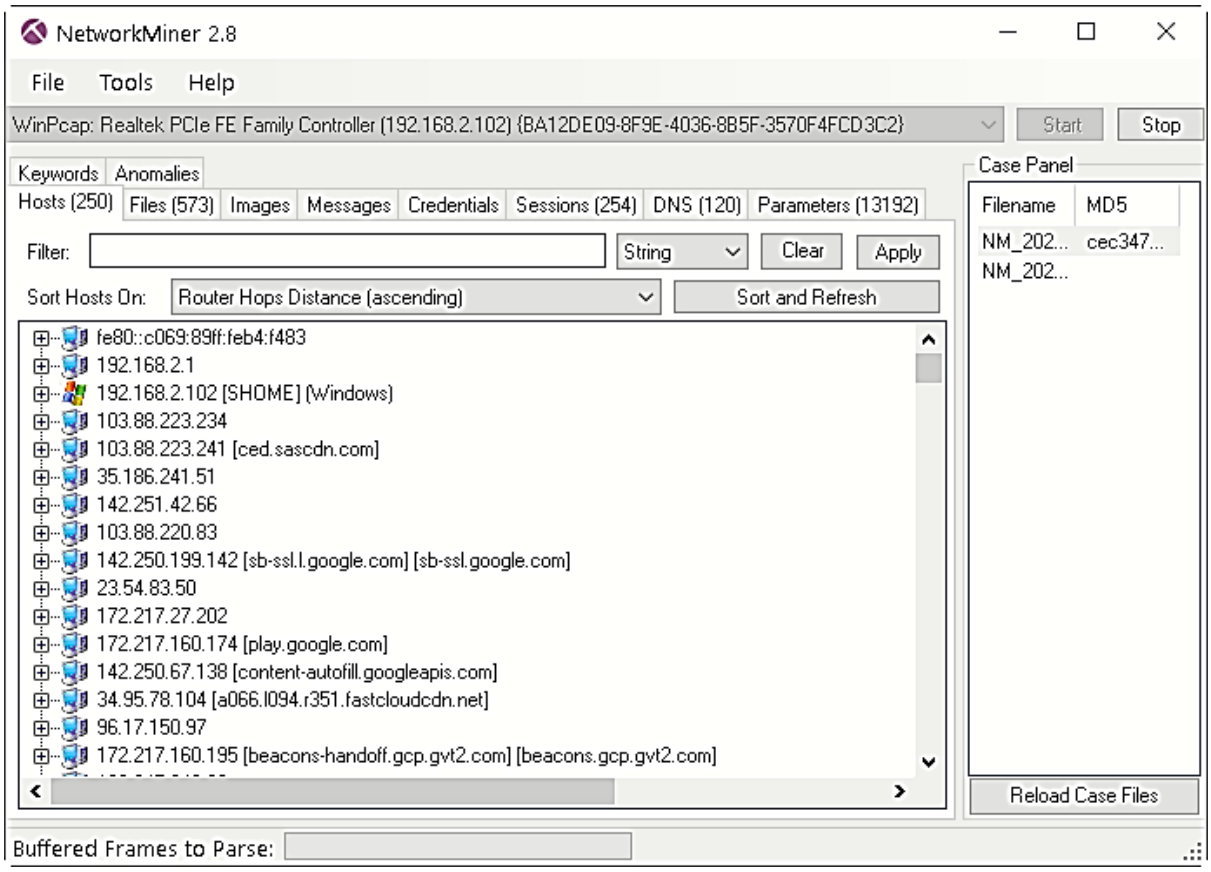
tcp contains facebook

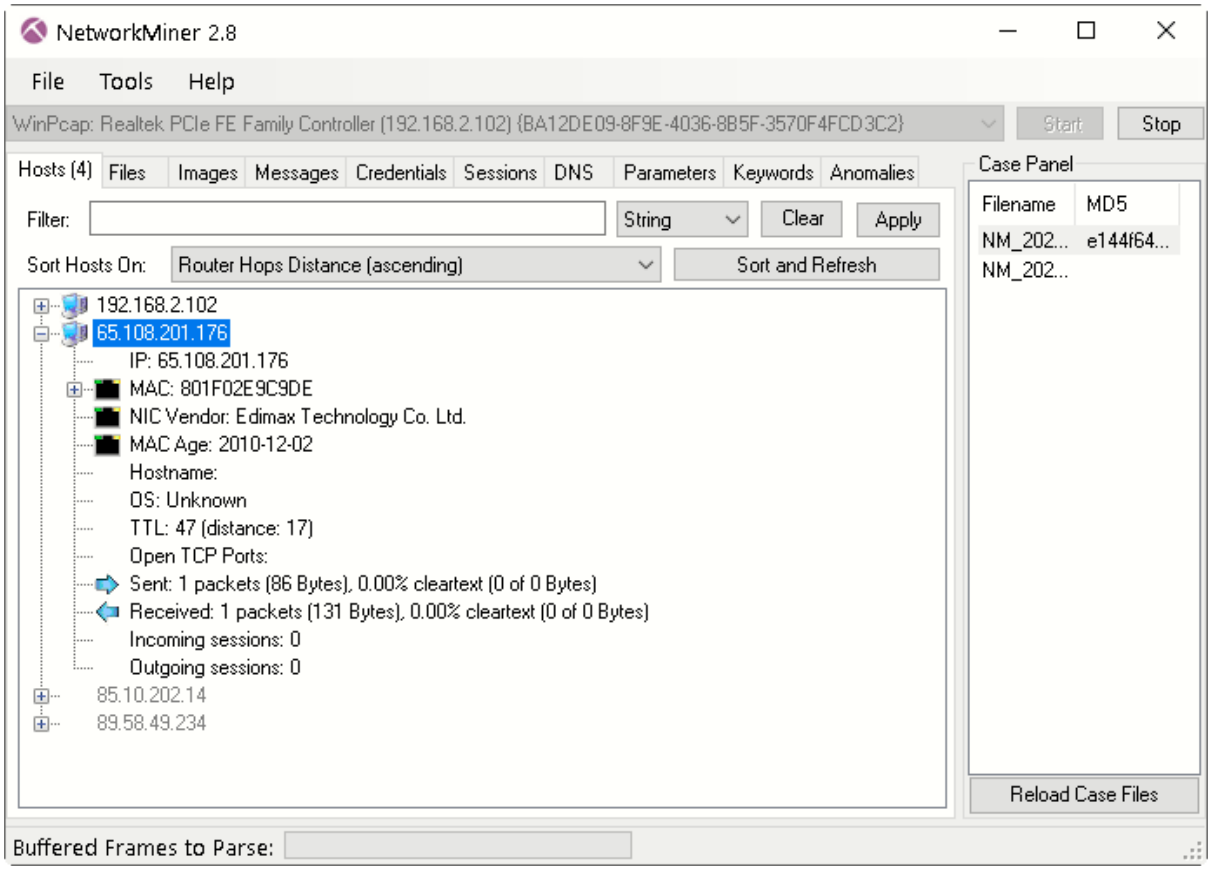
No.	Time	Source	Destination	Protocol	Length	Info
7711	32.085504	192.168.1.4	31.13.79.35	TLSv1.3	571	Client Hello
8160	32.867205	192.168.1.4	31.13.79.35	TLSv1.3	571	Client Hello
9739	35.561576	192.168.1.4	157.240.16.35	TLSv1.3	571	Client Hello
29814	162.425666	192.168.1.4	157.240.16.35	TLSv1.3	571	Client Hello
37226	273.164934	192.168.1.4	157.240.16.16	TLSv1.2	571	Client Hello
37388	274.375759	192.168.1.4	157.240.16.16	TLSv1.3	571	Client Hello
43811	381.014078	192.168.1.4	157.240.16.35	TLSv1.3	571	Client Hello
47765	569.305448	192.168.1.4	157.240.16.35	TLSv1.3	571	Client Hello

b) Using Network Forensic Analysis Tool (Network Miner)

NetworkMiner is an open source network forensics tool that extracts artifacts, such as files, images, emails and passwords, from captured network traffic in PCAP files. NetworkMiner can also be used to capture live network traffic by sniffing a network interface. Detailed information about each IP address in the analyzed network traffic is aggregated to a network host inventory, which can be used for passive asset discovery as well as to get an overview of which devices that are communicating. NetworkMiner is primarily designed to run in Windows, but can also be used in Linux.

You can use NetworkMiner in order to perform ”live sniffing”, i.e. to capture network traffic from a network interface to a pcap file on disk. Simply select the desired network interface in the drop-down list at the top of the GUI and click the green ”play” button or hit he F5 key to start sniffing.



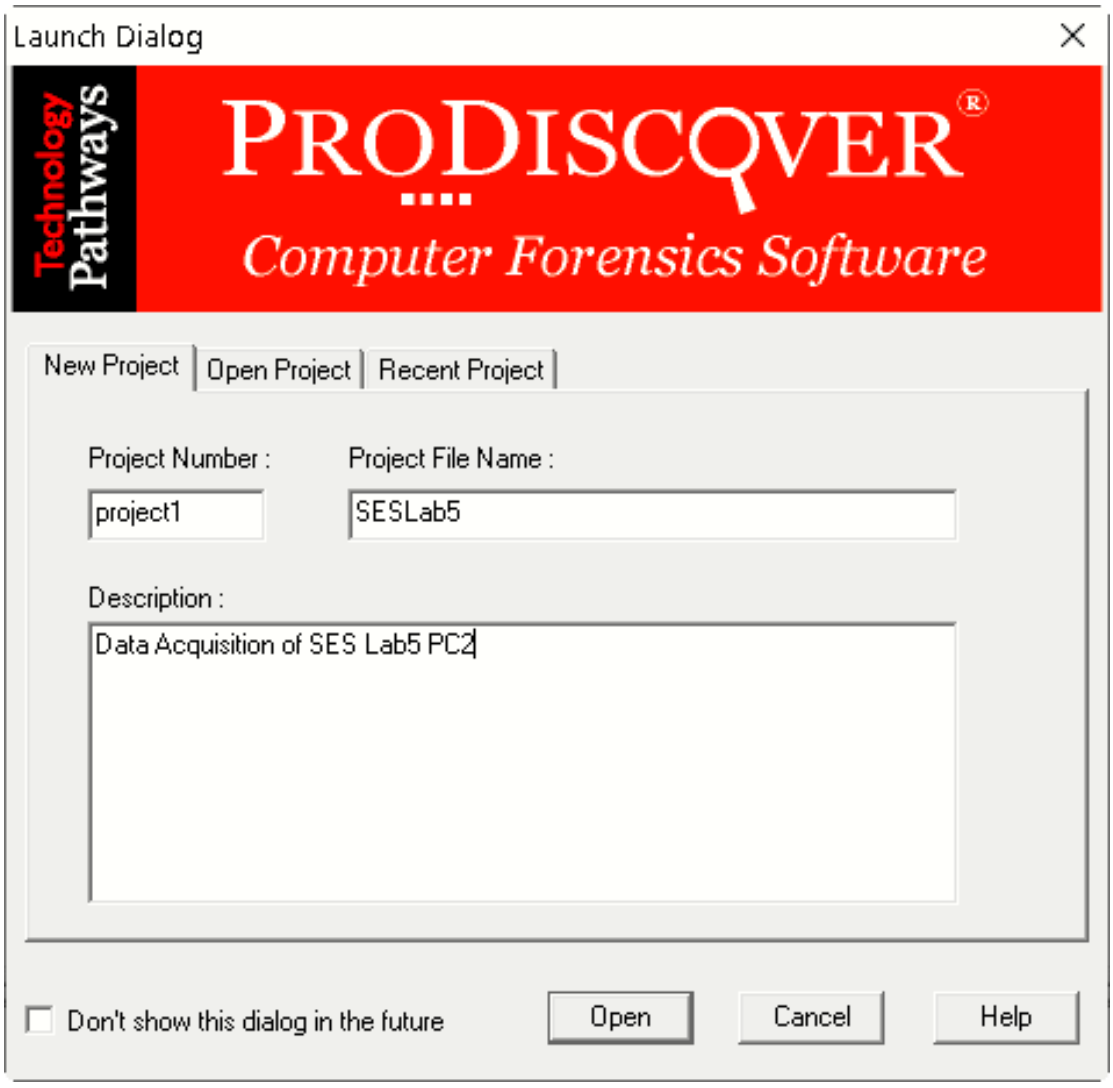

NetworkMiner 2.8
File
Tools
Help
WinPcap: Realtek PCIe FE Family Controller (192.168.2.102) {BA12DE09-8F9E-4036-8B5F-3570F4FCD3C2}
Start
Stop
Hosts (4)
Files
Images
Messages
Credentials
Sessions
DNS
Parameters
Keywords
Anomalies
Filter:
String
Clear
Apply
Sort Hosts On:
Router Hops Distance (ascending)
Sort and Refresh
192.168.2.102
65.108.201.176
IP: 65.108.201.176
MAC: 801F02E9C9DE
NIC Vendor: Edimax Technology Co. Ltd.
MAC Age: 2010-12-02
Hostname:
OS: Unknown
TTL: 47 (distance: 17)
Open TCP Ports:
Sent: 1 packets (86 Bytes), 0.00% cleartext (0 of 0 Bytes)
Received: 1 packets (131 Bytes), 0.00% cleartext (0 of 0 Bytes)
Incoming sessions: 0
Outgoing sessions: 0
85.10.202.14
89.58.49.234
Case Panel
Filename
MD5
NM_202...
e144f64...
NM_202...
Reload Case Files
Buffered Frames to Parse:

Practical 6

Using Data Acquisition Tools [ProDiscover]

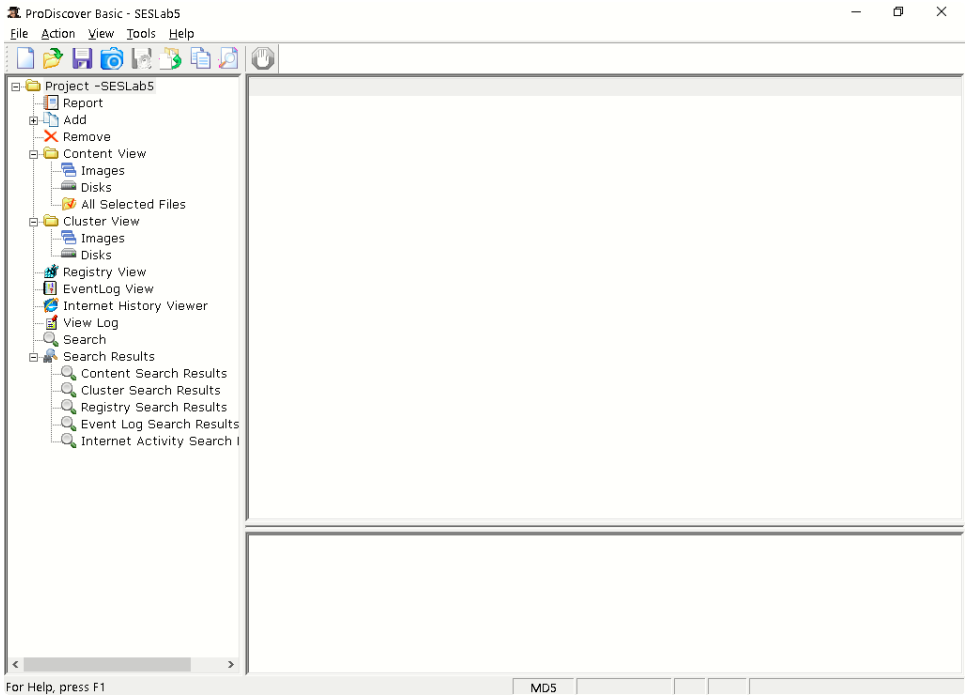
ProDiscover Forensics is a comprehensive digital forensics software that empowers investigators to capture key evidence from computer systems. ProDiscover has capabilities to handle all aspects of an in-depth forensic investigation to collect, preserve, filter, and analyze evidence.

Just double click on Prodiscover icon which is there in system. Following screen will appear. Left click on "Project Number"

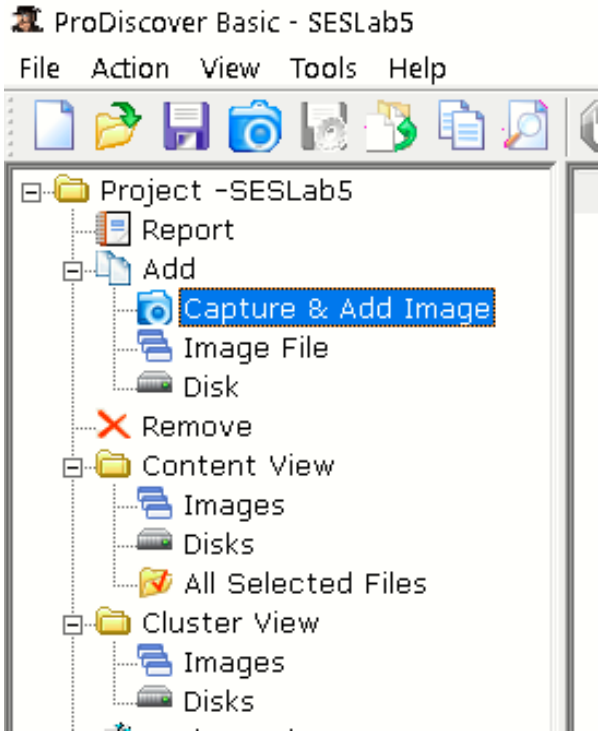


Click open button to start forensics case in prodiscover.

After opening case in prodiscover it will show three pane view with case name as title now please select file menu from PIR to get preference



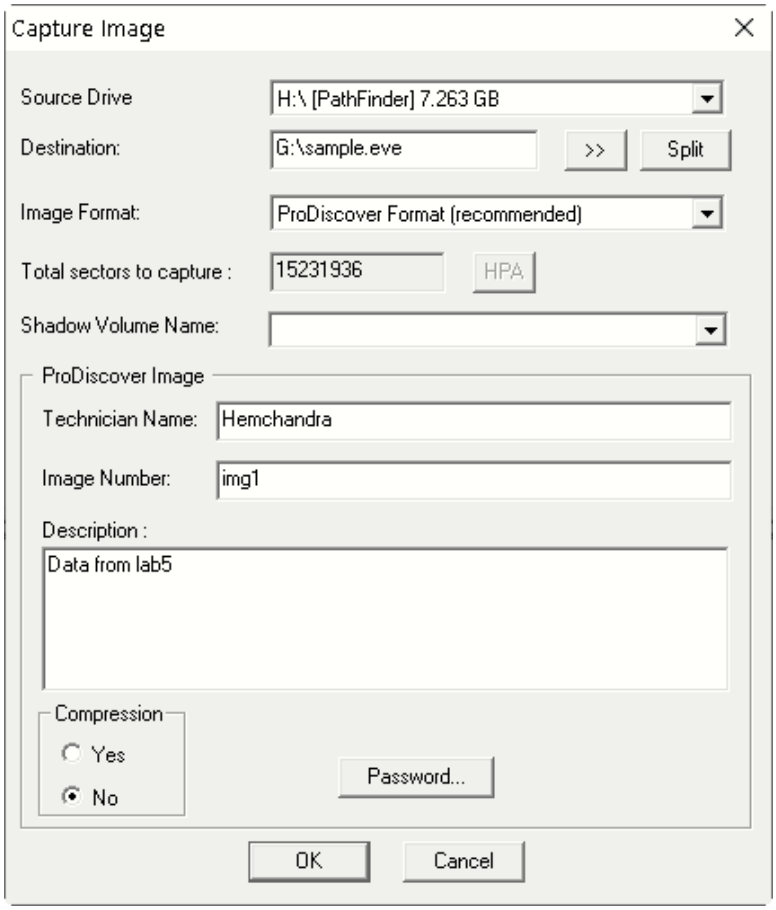
In main window click on **Capture & Add Image**



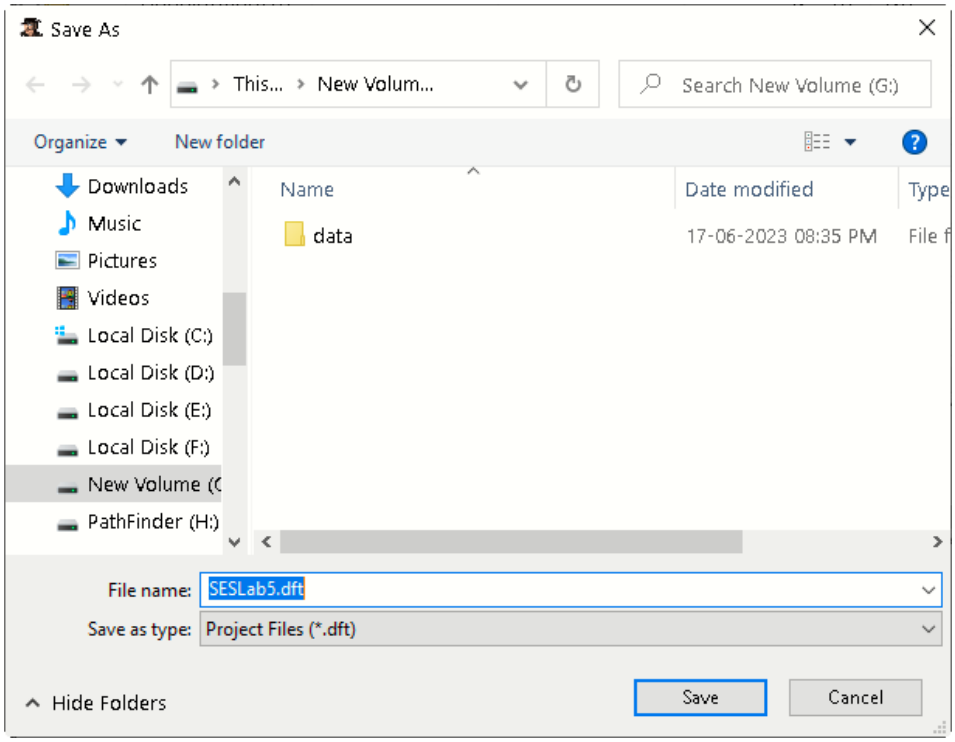
Now select the source drive that we want to capture, this could be a USB Drive or physical Drive.In my case I select drive **Physical Drive 1** which is my USB drive.

Now set the destination of the image file where we want to store it and named the image folder as pd and the name of the image which is to be saved in desired folder is PD.EVE .

Now enter the '**Technician Name'**, '**Image Number'** and '**description'** Now Click on ok.

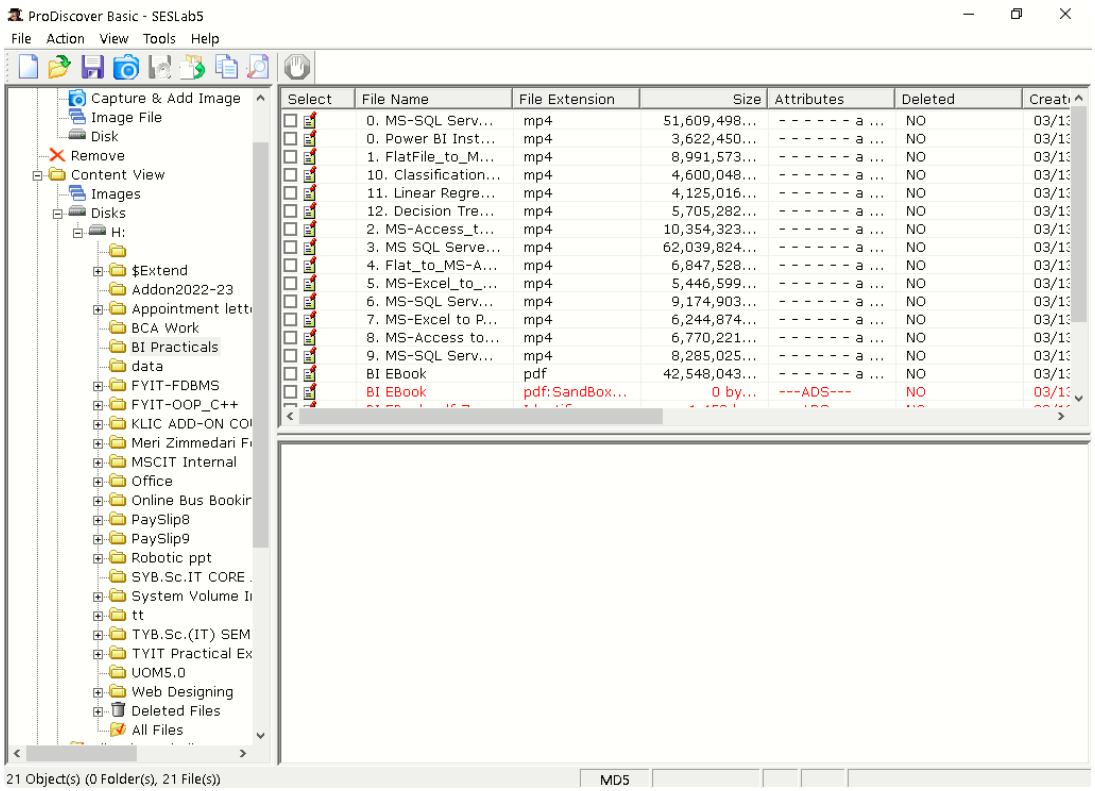


After finishing the following steps, windows will appear. After imaging the drive close the **prodiscover** program then it will ask you to save your project.



Now starts prodiscover program again and click on **open project** and browser your project image select it and click **open**

Now the project will open & go to the left menu and click on **Content View.** Then it will show you all the contents of evidence image.



To generate the automatic report click on **report** tab under the **view** menu. Then it will show you Evidence Report.

Evidence Report for Project: SESLab5

Project Number: p1

Project Description: Data Acquisition from Lab5 Pc

Image Files:

Disks:
Disk Name: H: [lab5]

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 from preferences settings.

Hard Disk: H:
Drive Type: DRIVE_REMOVABLE
Volume Name: PathFinder
Volume Serial Number : 2685-3048
File System: NTFS
Bytes Per Sector: 512
Total Clusters: 1903992
Sectors per cluster: 8
Total Sectors: 15231936
Hidden Sectors: 63
Total Capacity: 7615968 KB
Start Sector: 0
End Sector: 0

Evidence of Interest:

Clusters of Interest:

File Signature Mismatch:

Registry Keys of Interest:

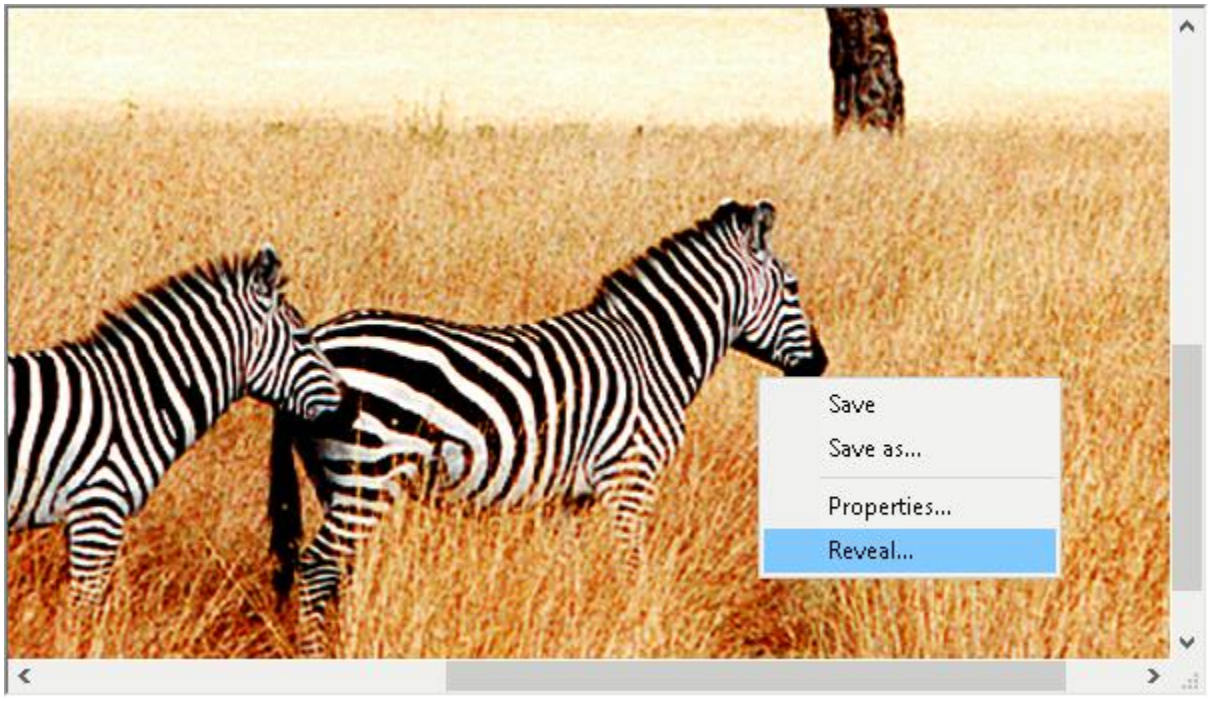
Event Log Entries of Interest:

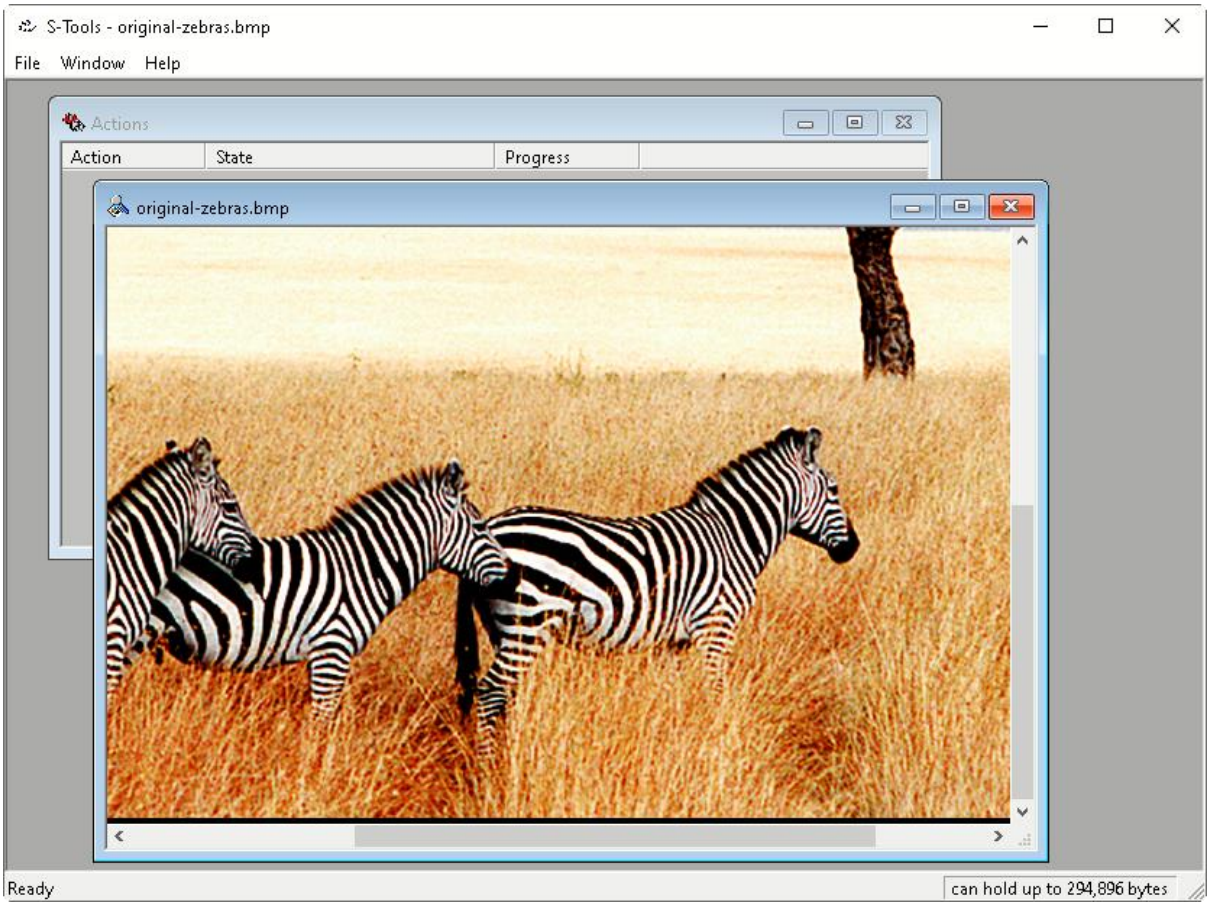
Internet Activity Information:

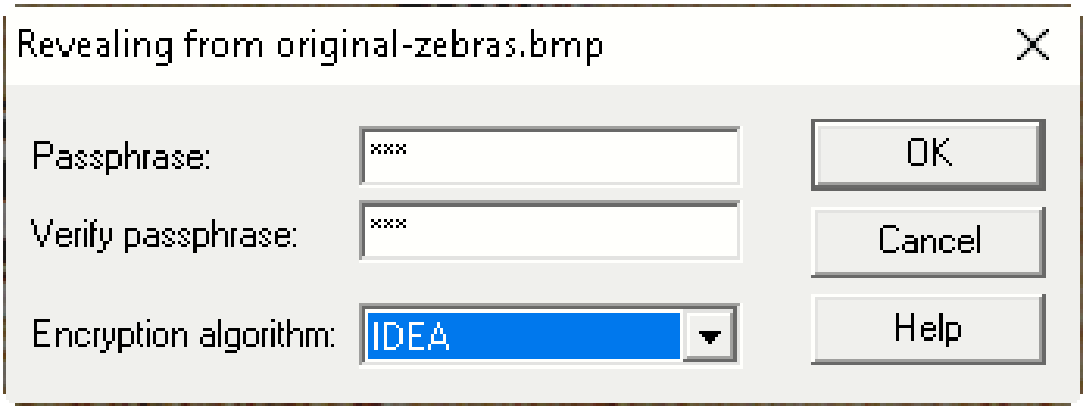
Practical 7

Using Steganography Tools [S-Tools]

1. Download and save the zip file containing the steganography tools and image files.
2. Unzip the file *steg.zip* into an empty directory. If you do not have the *unzip* program already.
3. Put a shortcut to *S-tools.exe* on your desktop by dragging it from Windows Explorer.
4. Drag the *zebras.bmp* file to your desktop. Do not make a shortcut. The file itself must be moved there.
5. Start *S-tools.exe* by double clicking on the icon on the desktop. A window will appear.
6. Drag the *zebras.bmp* file to the S-tools window.
7. Right click on the zebras pictures and select Reveal from the menu.
8. Fill in the 3-character pass phrase 'abc' (without the quotes) in two places. Leave IDEA as the encryption algorithm. Click on OK.
9. Wait until the Revealed Archive dialog box appears. This may take a minute or two.
10. Right click on any item and select Save As to save the file. Repeat for the other ones. These are the hidden files.
11. The file *original-zebras.bmp* is the file before the steganography was done, in case you wish to compare the 'before' and 'after' images.




S-Tools - original-zebras.bmp
File Window Help
Actions
Action
State
Progress
original-zebras.bmp
Ready
can hold up to 294,896 bytes

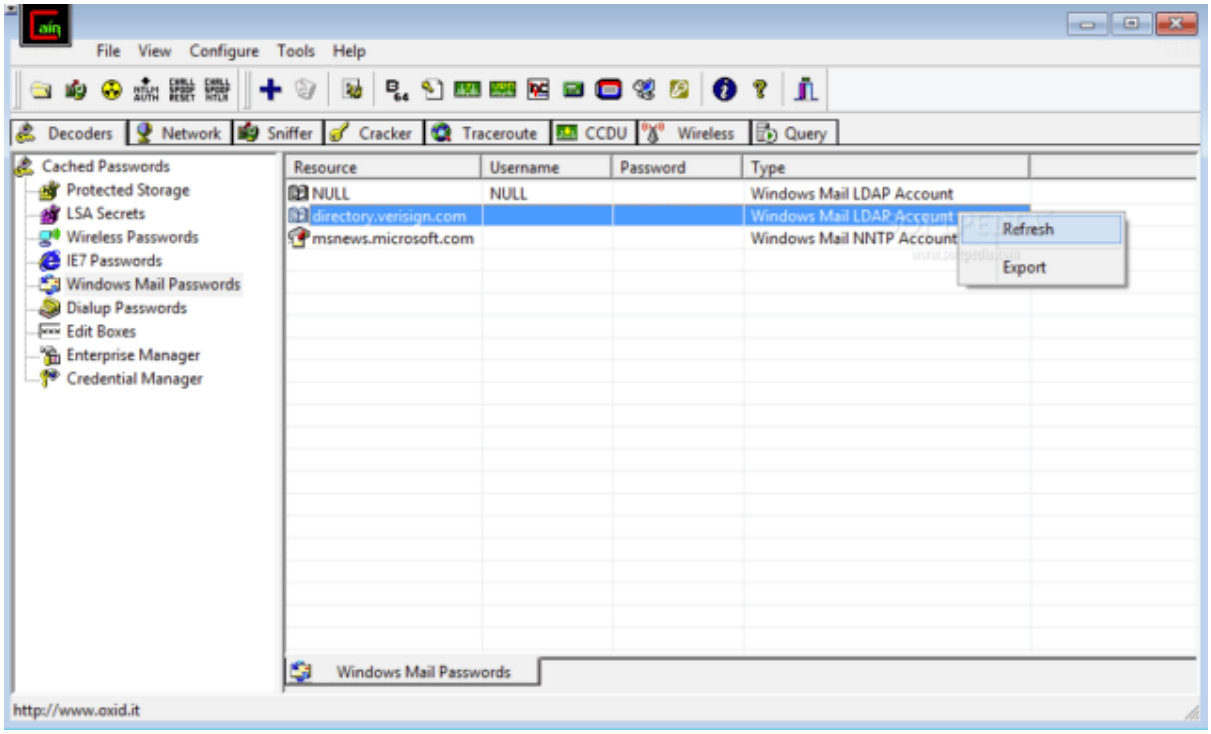

Revealing from original-zebras.bmp
Passphrase:
***
Verify passphrase:
***
Encryption algorithm:
IDEA
OK
Cancel
Help

Practical 8

Performing Password Cracking [Cain & Abel]

Cain & Abel is a password recovery tool for Microsoft Operating Systems. It allows easy recovery of various kind of passwords by sniffing the network, cracking encrypted passwords using Dictionary, Brute-Force and Cryptanalysis attacks, recording VoIP conversations, decoding scrambled passwords, recovering wireless network keys, revealing password boxes, uncovering cached passwords and analysing routing protocols.

Before you use this tool, you need to have a Rainbow table which is a large database of passwords that are needed, also known as a wordlist dictionary. You need to download the free XP rainbow tables and extract files to a folder on your desktop.



Follow to below steps to learn how to crack passwords with Cain and Abel:

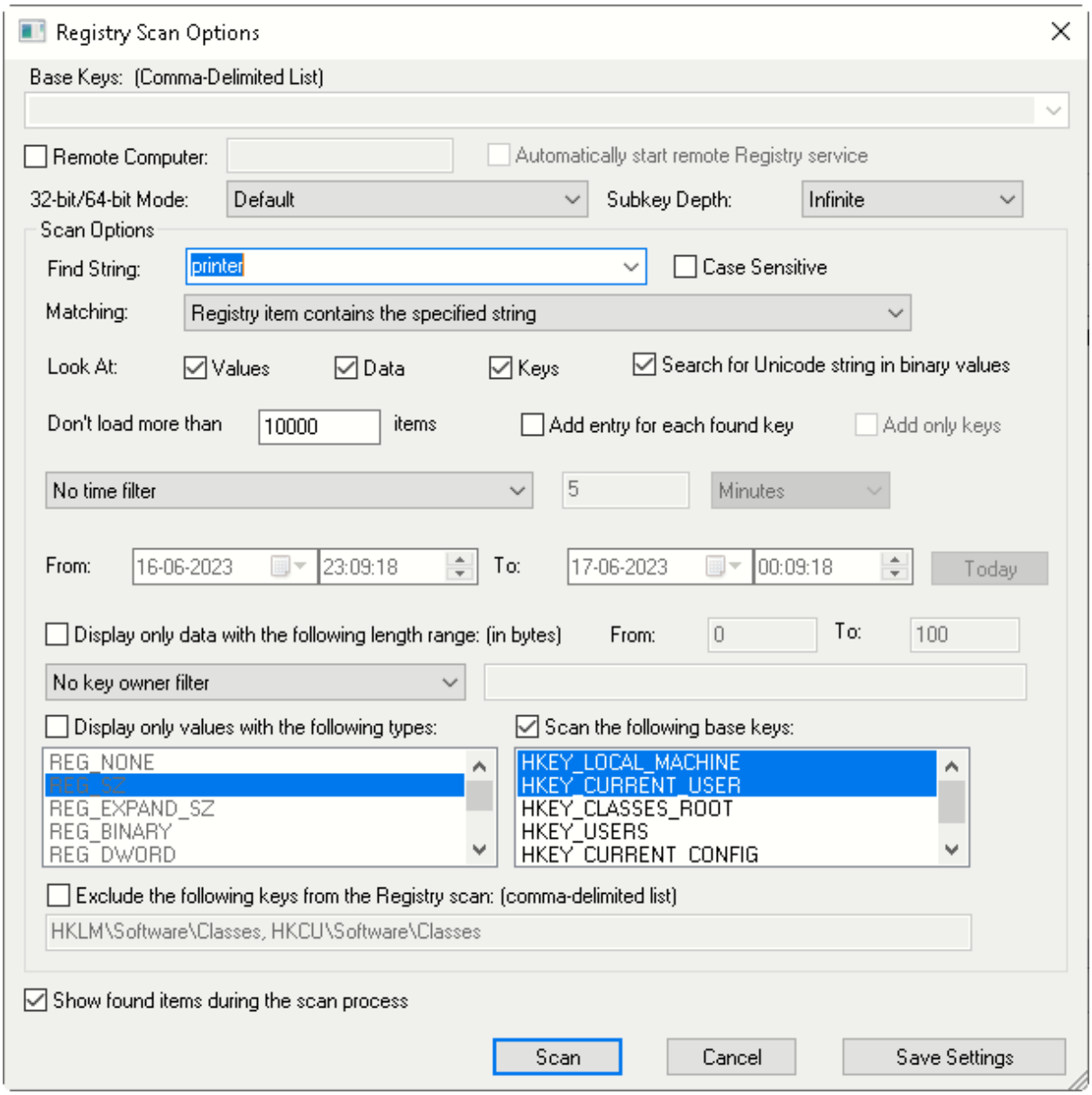
1. Begin by opening the "**Cain and Abel**" program.
2. After this click on the "**Cracker**" tab.
3. From the left side, you need to choose "**LM and LTLM Hashes**".
4. After this select the "**big blur plus sign**" there on the Cain toolbar.
5. You need to be sure that the "**Import Hashed from local System**" is checked.
6. Click on "**Next**".
7. All the user accounts shall be loaded to the right.

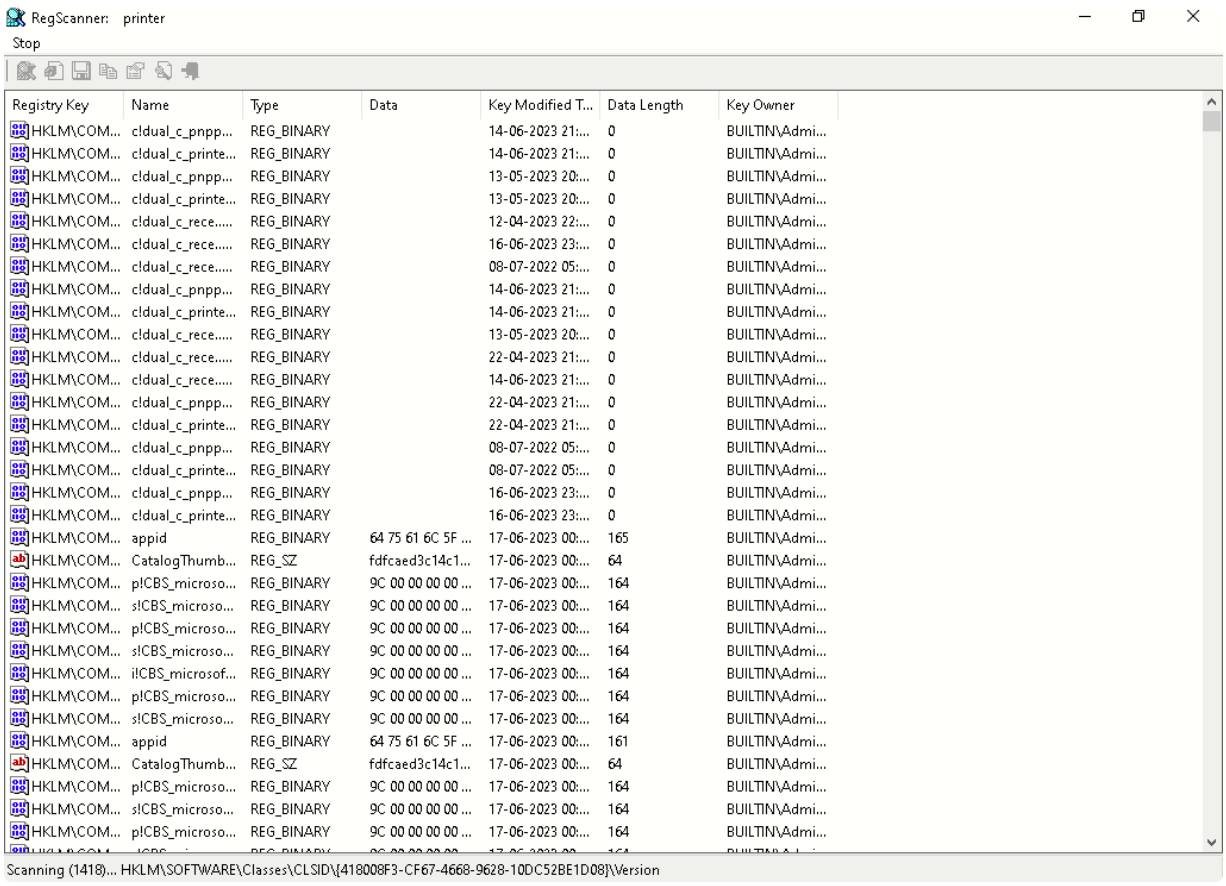
8. Click right on the username that you require the password for.
9. Click on **cryptanalysis attack** > **LM Hashes** > via **RainbowTables** (OphCrack).
10. In LM Hashes Cryptanalysis window, choose the … window and click on the folder you extracted the rainbow tables to.
11. Click on "**OK**" and then "**Start**".
12. Done.

Practical 9

a. Scan Registry using RegScanner

RegScanner is a small free utility that allows you to scan the registry, find the desired Registry values that match the specified search criteria, and display them in one list. In addition to the standard string search (Like in RegEdit), RegScanner can also find Registry values by data length, value type (REG_SZ, REG_DWORD, and so on) modified date of the key. After finding the Registry values, you can quickly jump to the correct value in RegEdit by double-clicking the desired Registry item. You can also export the found Registry values into a .reg file used in RegEdit.




RegScanner: printer
Stop
Registry Key
Name
Type
Data
Key Modified T...
Data Length
Key Owner
HKLM\COM... c!dual_c_pnpp... REG_BINARY 14-06-2023 21:... 0 BUILTIN\Admi...
HKLM\COM... c!dual_c_printe... REG_BINARY 14-06-2023 21:... 0 BUILTIN\Admi...
HKLM\COM... c!dual_c_pnpp... REG_BINARY 13-05-2023 20:... 0 BUILTIN\Admi...
HKLM\COM... c!dual_c_printe... REG_BINARY 13-05-2023 20:... 0 BUILTIN\Admi...
HKLM\COM... c!dual_c_rece..... REG_BINARY 12-04-2023 22:... 0 BUILTIN\Admi...
HKLM\COM... c!dual_c_rece..... REG_BINARY 16-06-2023 23:... 0 BUILTIN\Admi...
HKLM\COM... c!dual_c_rece..... REG_BINARY 08-07-2022 05:... 0 BUILTIN\Admi...
HKLM\COM... c!dual_c_pnpp... REG_BINARY 14-06-2023 21:... 0 BUILTIN\Admi...
HKLM\COM... c!dual_c_printe... REG_BINARY 14-06-2023 21:... 0 BUILTIN\Admi...
HKLM\COM... c!dual_c_rece..... REG_BINARY 13-05-2023 20:... 0 BUILTIN\Admi...
HKLM\COM... c!dual_c_rece..... REG_BINARY 22-04-2023 21:... 0 BUILTIN\Admi...
HKLM\COM... c!dual_c_rece..... REG_BINARY 14-06-2023 21:... 0 BUILTIN\Admi...
HKLM\COM... c!dual_c_pnpp... REG_BINARY 22-04-2023 21:... 0 BUILTIN\Admi...
HKLM\COM... c!dual_c_printe... REG_BINARY 22-04-2023 21:... 0 BUILTIN\Admi...
HKLM\COM... c!dual_c_pnpp... REG_BINARY 08-07-2022 05:... 0 BUILTIN\Admi...
HKLM\COM... c!dual_c_printe... REG_BINARY 08-07-2022 05:... 0 BUILTIN\Admi...
HKLM\COM... c!dual_c_pnpp... REG_BINARY 16-06-2023 23:... 0 BUILTIN\Admi...
HKLM\COM... c!dual_c_printe... REG_BINARY 16-06-2023 23:... 0 BUILTIN\Admi...
HKLM\COM... appid REG_BINARY 64 75 61 6C 5F ... 17-06-2023 00:... 165 BUILTIN\Admi...
HKLM\COM... CatalogThumb... REG_SZ fdfcaed3c14c1... 17-06-2023 00:... 64 BUILTIN\Admi...
HKLM\COM... p!CBS_microso... REG_BINARY 9C 00 00 00 00 ... 17-06-2023 00:... 164 BUILTIN\Admi...
HKLM\COM... s!CBS_microso... REG_BINARY 9C 00 00 00 00 ... 17-06-2023 00:... 164 BUILTIN\Admi...
HKLM\COM... p!CBS_microso... REG_BINARY 9C 00 00 00 00 ... 17-06-2023 00:... 164 BUILTIN\Admi...
HKLM\COM... s!CBS_microso... REG_BINARY 9C 00 00 00 00 ... 17-06-2023 00:... 164 BUILTIN\Admi...
HKLM\COM... i!CBS_microsof... REG_BINARY 9C 00 00 00 00 ... 17-06-2023 00:... 164 BUILTIN\Admi...
HKLM\COM... p!CBS_microso... REG_BINARY 9C 00 00 00 00 ... 17-06-2023 00:... 164 BUILTIN\Admi...
HKLM\COM... s!CBS_microso... REG_BINARY 9C 00 00 00 00 ... 17-06-2023 00:... 164 BUILTIN\Admi...
HKLM\COM... appid REG_BINARY 64 75 61 6C 5F ... 17-06-2023 00:... 161 BUILTIN\Admi...
HKLM\COM... CatalogThumb... REG_SZ fdfcaed3c14c1... 17-06-2023 00:... 64 BUILTIN\Admi...
HKLM\COM... p!CBS_microso... REG_BINARY 9C 00 00 00 00 ... 17-06-2023 00:... 164 BUILTIN\Admi...
HKLM\COM... s!CBS_microso... REG_BINARY 9C 00 00 00 00 ... 17-06-2023 00:... 164 BUILTIN\Admi...
HKLM\COM... p!CBS_microso... REG_BINARY 9C 00 00 00 00 ... 17-06-2023 00:... 164 BUILTIN\Admi...
Scanning (1418)... HKLM\SOFTWARE\Classes\CLSID\{418008F3-CF67-4668-9628-10DC52BE1D08}\Version

b. Study Registry Viewer tool (Alien Registry Viewer)

Alien Registry Viewer is similar to the RegEdit application included into Windows, but unlike RegEdit, it works with standalone registry files. While RegEdit shows the contents of the system registry, Alien Registry Viewer works with registry files copied from other computers. Alien Registry Viewer allows you to explore registry files, search for specific key names and values, export registry data into a .REG file and bookmark registry keys as favorites.

Alien Registry Viewer shows all the keys available in the registry files, for example, you can explore the contents of the SAM hive. If you use RegEdit, many keys are unavailable due to security restrictions.