SSM INSTITUTE OF ENGINEERING AND TECHNOLOGY

(An Autonomous Institution)
Approved by AICTE, New Delhi and Affiliated to Anna University, Chennai
Sindalagundu Post, Palani Road, Dindigul – 624 002
Ph: 0451 – 2448800 – 2448899 (100 lines) Fax: 0451 – 2557755
E-mail: info@ssmiet.com, website: www.ssmiet.com

CB3601 - CYBER FORENSICS

RECORD NOTEBOOK

NAME	
REGISTER NUMBER	
YEAR	III
SEMESTER	VI
DEPARTMENT	Computer Science and Engineering (Cyber Security)
ACADEMIC YEAR	2025 – 2026 (Even semester)

SSM INSTITUTE OF ENGINEERING AND TECHNOLOGY

(An Autonomous Institution)
Approved by AICTE, New Delhi and Affiliated to Anna University, Chennai
Sindalagundu Post, Palani Road, Dindigul – 624 002
Ph: 0451 – 2448800 – 2448899 (100 lines) Fax: 0451 – 2557755
E-mail: info@ssmiet.com, website: www.ssmiet.com

PRACTICAL RECORD BONAFIDE CERTIFICATE

REGISTER NUMBER | |

Certified that this is the bonafide record work done by

*Mr./Miss……**Reg. No**……*

*Fifth Semester, **Computer Science and Engineering(Cyber Security)** branch during the*

*Academic year **2025 - 2026** in the **CB3601 - CYBER FORENSICS***

Staff in-Charge ***Head of the Department***

Submitted for the Semester End Practical Examination held on ……..

Internal Examiner ***External Examiner***

SSM INSTITUTE OF ENGINEERING AND TECHNOLOGY (Autonomous)
AICTE Approved / Affiliated to Anna University / Accredited by NAAC (2029) & NBA (2025)
Dindigul – Palani Highway, Dindigul 624 002.

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING (CYBER SECURITY)

VISION

To develop skilled cyber security professionals equipped to secure digital landscapes, address emerging cyber challenges, and contribute to society with strong technical expertise, entrepreneurial skills, and ethical values.

MISSION

- Foster self-discipline and critical thinking in students through robust teaching and learning.
- Empower students to become proficient cyber security professionals and responsible citizens.
- Strengthen industry partnerships by establishing specialized centres for advanced skill development and practical exposure.
- Deliver knowledge for secure and innovative solutions, contributing to sustainable and ethical technology advancement.

PROGRAM EDUCATIONAL OBJECTIVES (PEOs)

PEO1	Graduates can apply their technical competence in computer science to solve real world problems, with technical and people leadership.
PEO2	Graduates Conduct cutting edge research and develop solutions on problems of social relevance.
PEO3	Graduates will Work in a business environment, exhibiting team skills, work ethics, adaptability and lifelong learning.

PROGRAM OUTCOMES (POs)

Graduate Attribute

1. **Engineering knowledge:** Apply the knowledge of mathematics, science, engineering fundamentals, and an engineering specialization to the solution of complex engineering problems.
2. **Problem analysis:** Identify, formulate, review research literature, and analyse complex engineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.
3. **Design/development of solutions:** Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations.
4. **Conduct investigations of complex problems:** Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.
5. **Modern tool usage:** Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modelling to complex engineering activities with an understanding of the limitations.
6. **The engineer and society:** Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to the professional engineering practice.
7. **Environment and sustainability:** Understand the impact of the professional engineering solutions in societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.
8. **Ethics:** Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering practice.
9. **Individual and team work:** Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.
10. **Communication:** Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive clear instructions.

11. **Project management and finance:** Demonstrate knowledge and understanding of the engineering and management principles and apply these to one's own work, as a member and leader in a team, to manage projects and in multidisciplinary environments.
12. **Life-long learning:** Recognize the need for, and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change.

PROGRAM SPECIFIC OUTCOMES (PSOs)

The Students will be able to

- Exhibit design and programming skills to build and automate business solutions using cutting edge technologies.
- Strong theoretical foundation leading to excellence and excitement towards research, to provide elegant solutions to complex problems.
- Ability to work effectively with various engineering fields as a team to design, build and develop system applications

SSM INSTITUTE OF ENGINEERING AND TECHNOLOGY (Autonomous)
AICTE Approved / Affiliated to Anna University / Accredited by NAAC (2029) & NBA (2025)
Dindigul – Palani Highway, Dindigul 624 002.

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
(CYBER SECURITY)

Do's and Don'ts

Laboratory Rules &Regulation:

- Students are instructed to maintain silence inside the Lab.
- Students have to sign the log-book, while entering and leaving the Lab and also they have to mention the time in and time out.
- Students have to enter and leave the Lab in their scheduled time otherwise they will be marked absent.
- Students should come with proper Lab uniform and with shoes.
- The students should properly shut down the Computer Systems before they leave the Lab.
- Students are not allowed to use CD's & DVD's, USB DRIVE etc. lf required prior permission of Laboratory in-charge is needed.
- All students will be responsible for keeping the Lab clean.
- Students should refrain from dislocating, shifting and damaging with any parts of the computer or any other device in the Lab.
- The students should not load or delete any software from the computer.
- The students should not use computers in the Lab for any personal work.
- Browsing of Internet will not be allowed in the lab beyond the stipulated hour as per time table.
- The Instructor/Lecturer will be the sole authority to judge the disciplinary behavior inside the laboratory. For violation of any of the above rules, the department reserves the right to take appropriate disciplinary action.
- Browsing of non-academic Internet sites will not be allowed in the Lab.
- Before downloading any materials please consult your instructor and save the downloaded files as per instruction given by the laboratory in- charge.

- Because of security problems, downloading software and music etc. from the Internet is strictly prohibited. Any such file found in the hard disk will be deleted without warning.
- Students should arrange the chairs properly while leaving the LAB hours.
- Students should not allow to work inside the LAB other than LAB hours. If required prior permission of Laboratory in-charge and Department in charge is needed.

CB3601	CYBER FORENSICS	L T P C
		3 0 2 4

COURSE OBJECTIVES:

- To learn cyber crime and forensics
- To become familiar with forensics tools
- To learn to analyze and validate forensics data
- To understand cyber laws and the admissibility of evidence with case studies
- To learn the vulnerabilities in network infrastructure with ethical hacking

PRACTICAL EXERCISES: **30 PERIODS**

1) Study and Explore the following forensic tools:

(a) FTK Imager (b) Autopsy (c)EnCase Forensic Imager (d) LastActivityView (e) USBDeview

2. Recover deleted files using FTKImager

3. Acquire forensic image of hard disk using EnCase Forensics Imager and also perform integrity checking/validation

4. Restore the Evidence Image using EnCase Forensics Imager.

5. Study the following:

   (a) Collect Email Evidence in Victim PC.

   (b) Extract Browser Artifacts (ChromeHistory view for Google Chrome)

6. Use USBDeview to find the last connected USB to the system

7. Perform Live Forensics Case Investigation using Autopsy

8. Study Email Tracking and EmailTracing and write a report on them.

COURSE OUTCOMES:

CO1: Understand the basics of cyber crime and computer forensics
CO2: Apply a number of different computer forensic tools to a given scenario
CO3: Analyze and validate forensics data
CO4: Understand Admissibility of evidence in India with Cyber laws and Case Studies
CO5: Identify the vulnerabilities in a given network infrastructure
CO6: Implement real-world hacking techniques to test system security

S.NO	DATE	NAME OF EXPERIMENT	PAGE NO	REMARKS
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				

EX NO:1	STUDY AND EXPLORE THE FOLLOWING FORENSIC TOOLS
DATE:	

Aim:

Study of Computer Forensics and different tools used for forensic investigation

What Is Digital Forensics?

Digital forensics is the field of determining who was responsible for a digital intrusion or other computer crime. It uses a wide range of techniques to gain attribution to the perpetrator.

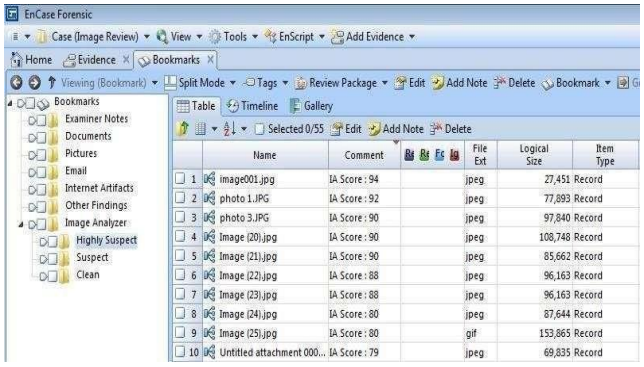
It relies upon the fundamental concept that whenever a digital intrusion or crime is committed, the perpetrator inadvertently leaves a bit of themselves behind for the investigator to find. These "bits" could be entries in log files, changes to the registry, hacking software, malware, remnants of deleted files, etc. All of these can provide clues and evidence to determine their identity and lead to the capture and arrest of the hacker.

As a hacker, the more you know and understand about digital forensics, the better you can evade the standard forensic techniques and even implement anti-forensic measures to throw off the investigator.

The Digital Forensic Tools

Just like in hacking, there are a number of software tools for doing digital forensics. For the hacker, becoming familiar with these tools and how they work is crucial to evading them. Most digital forensic investigators rely upon three major commercial digital forensic suites.

1. Guidance Software's EnCase Forensic
2. Access Data's Forensic Tool Kit (FTK)
3. Prodiscover



These three suites are comprised of multiple tools and reporting features and can be fairly expensive. While these suites are widely used by law enforcement, they use the same or similar techniques as the free open-source suites without the fancy interfaces.

By using the open-source and free suites, we can come to understand how such tools as EnCase work without the expense. EnCase is the most widely used tool by law enforcement, but not necessarily the most effective and sophisticated. These tools are designed for user-friendliness, efficiency, certification, good training, and reporting.

There are a number of the free, open-source forensic suites, including the following three.

1. The Sleuthkit Kit (TSK)
2. Helix
3. Knoppix

The Forensic Tools Available in BackTrack

In addition, there are a large number of individual tools that are available for digital forensics, some of which are available in our BackTrack and Kali distributions.

Some of the better tools in BackTrack include the following, among many others.

- sleuthkit
- truecrypt
- hexedit
- autopsy
- iphoneanalyzer
- rifiuti2
- ptk
- exiftool
- evtparse.pl
- fatback
- scalpel
- dc3dd
- driftnet
- timestomp

What Can Digital Forensics Do?

Digital forensics can do many things, all of which the aspiring hacker should be aware of. Below is a list of just some of the things.

- Recovering deleted files, including emails
- Determine what computer, device, and/or software created the malicious file, software, and/or attack
- Trail the source IP and/or MAC address of the attack
- Track the source of malware by its signature and components
- Determine the time, place, and device that took a picture
- Track the location of a cell phone enabled device (with or without GPS enabled)
- Determine the time a file was modified, accessed or created (MAC)
- Crack passwords on encrypted hard drives, files, or communication
- Determine which websites the perpetrator visited and what files he downloaded
- Determine what commands and software the suspect has utilized
- Extract critical information from volatile memory
- Determine who hacked the wireless network and who the unauthorized users are

And that' just some of the things you can do with digital forensics!

What Is Anti-Forensics?

Anti-forensics are techniques that can be used to obfuscate information and evade the tools and techniques of the forensic investigator. Some of these techniques include the following.

- **Hiding Data:** Hiding data can include such things as encryption and steganography.
- **Artefact wiping:** Every attack leaves a signature or artefact behind. Sometimes it's wise to attempt to wipe these artefacts from the victim machine so as to leave no tell-tale trail for the investigator.
- **Trail Obfuscation:** A decent forensic investigator can trail nearly any remote attack to an IP address and/or MAC address. Trail obfuscation is a technique that leads them to another source of the attack, rather than the actual attack.
- **Change the timestamp:** Change the file timestamp (modify, access, and change) to evade detection by forensic tools.

List of Forensic tool

Forensics Field Tools

Forensics Field Tools

FTKImager

Forensic disk imager and file recovery.

Log Parser Lizard GUI

Flexible and powerful log file parser. It also does much much more.

Noxcivis Field Toolkit

The Noxcivis Field Toolkit (NFT) is a free and open interface that allows forensic examiners and collection teams to collect information from a computer.

Active@ Partition Recovery

Recover deleted partitions.

Autopsy

Forensics tool. Autopsy is a digital forensics platform and graphical interface to The Sleuth Kit® and other digital forensics tools. It can be used by law enforcement, military, and corporate examiners to investigate what happened on a computer. You can even use it to recover photos from your camera's memory card.

CAINE (Computer Aided Investigative Environment)

CAINE (Computer Aided Investigative Environment) is an Italian GNU/Linux live distribution created as a project of Digital Forensics. CAINE represents fully the spirit of the Open Source philosophy because the project is completely open, everyone could take the legacy of the previous developer or project manager. The distro is open source, the Windows side (Wintaylor) is open source and, the last but not the least, the distro is installable, so giving the opportunity to rebuild it in a new brand version, so giving a long life to this project.

Capture-BAT Download Page | The Honeynet Project

Capture-BAT Download Page Capture BAT is a behavioural analysis tool of applications for the Win32 operating system family. Capture BAT is able to monitor the state of a system during the execution of applications and processing of documents, which provides an analyst with insights on how the software operates even if no source code is available. Capture BAT monitors state changes on a low kernel level and can easily be used across various Win32 operating system versions and configurations.

cFAIR Technologies Tools

cFAIR Technologies Tools for forensics and eDiscovery

Digital Forensics Framework (DFF)

Open Source Digital investigation software DFF (Digital Forensics Framework) is a free and Open Source computer forensics software built on top of a dedicated Application Programming Interface (API). It can be used both by professional and non-expert people in order to quickly and easily collect, preserve and reveal digital evidence without compromising systems and data.

EnCase Forensic Imager

FREE software to capture a forensically sound copy of data.

Explorer Suite

Suite of executable file forensics utilities.

File and Partition Recovery Software

Free download Partition Recovery Software, Deleted Partition Recovery, Active Partition Recovery Software. Realize partition data recovery with Free Partition Recovery Software, Free Active Partition Recovery Software, Free Disk Partition Recovery Tool, Free NTFS Partition Recovery Tool, Recovery Partition, Hard Disk Recovery, Drive Partition Recovery, Deleted Partition Recovery and Hard Drive Partition Recovery Tool. Support FAT12, FAT16, FAT32, VFAT, NTFS, NTFS5 and Windows 2000 Professional/XP/Vista/7/8 and soon.

EX NO:2	RECOVER DELETED FILES USING FTK IMAGER
DATE:	

Aim:

How to Recover Deleted Files using Forensics Tools.

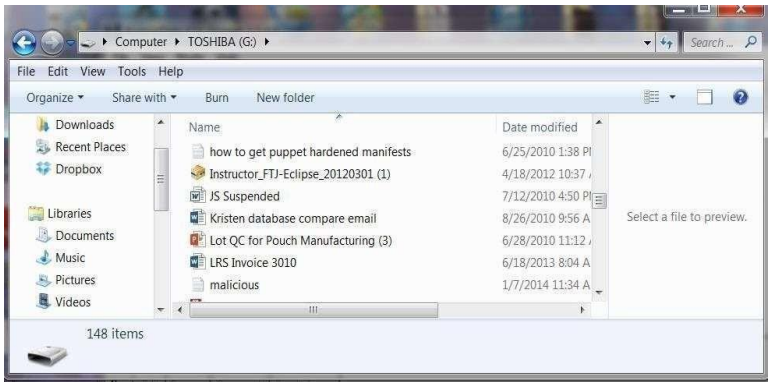
Step-01: Create a File

To demonstrate how to recover deleted files, let's create a malicious document. We will call this document "Malicious" and create it with Notepad in Windows.

This sounds like a sound, albeit ambitious plan.

Step 2: Delete the File

Next, now that we have completed our plans to take over the world, let's delete the file because we no longer need it and we don't want to leave behind any evidence of our malicious plans.



Right-click on the malicious file and select delete. If you put the file in the Recycle Bin, you have made it even easier for the forensic investigator to recover. The Recycle Bin is actually simply a folder where the files are moved until you empty the Recycle Bin. Nothing is deleted until you empty the Recycle Bin.

Step 3: Create an Image

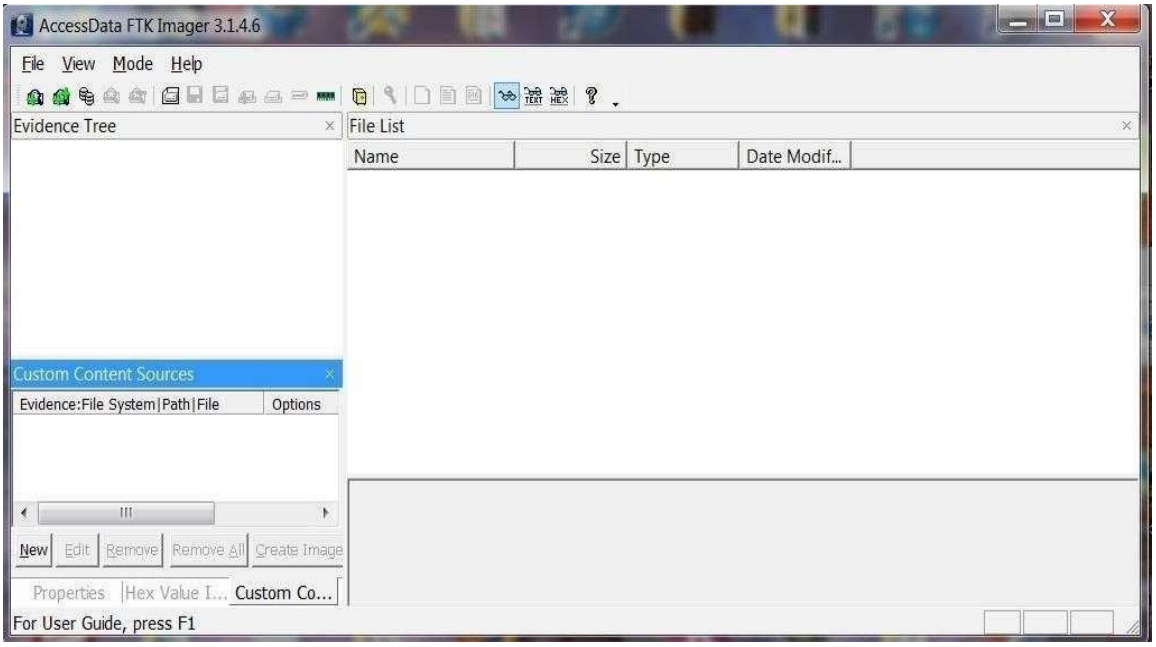
The first step a forensic investigator will do when examining your computer is to make a bit-by-bit copy of your hard drive or in this case your flash drive. There are numerous tools that can do this and in Linux, we have the dd command that does an excellent job of making bit-by-bit copies (it's on all Linux distributions including BackTrack). File backups and copies are not forensically sound as they will not copy deleted files and folders and in many cases will actually change the data.

Most forensic investigators use commercial tools. The two most popular being Encase by Guidance Software and Forensic Tool Kit by Access Data.

FTK, as it is commonly known in the industry, has a free imager that creates a bit-by-bit copy of the drive. This imager is probably the most widely used in the industry and its price is right, so let's use it.

You can download it **here.**

Now that have downloaded the FTK imager, we need to create a bit-by-bit image of the flash drive.



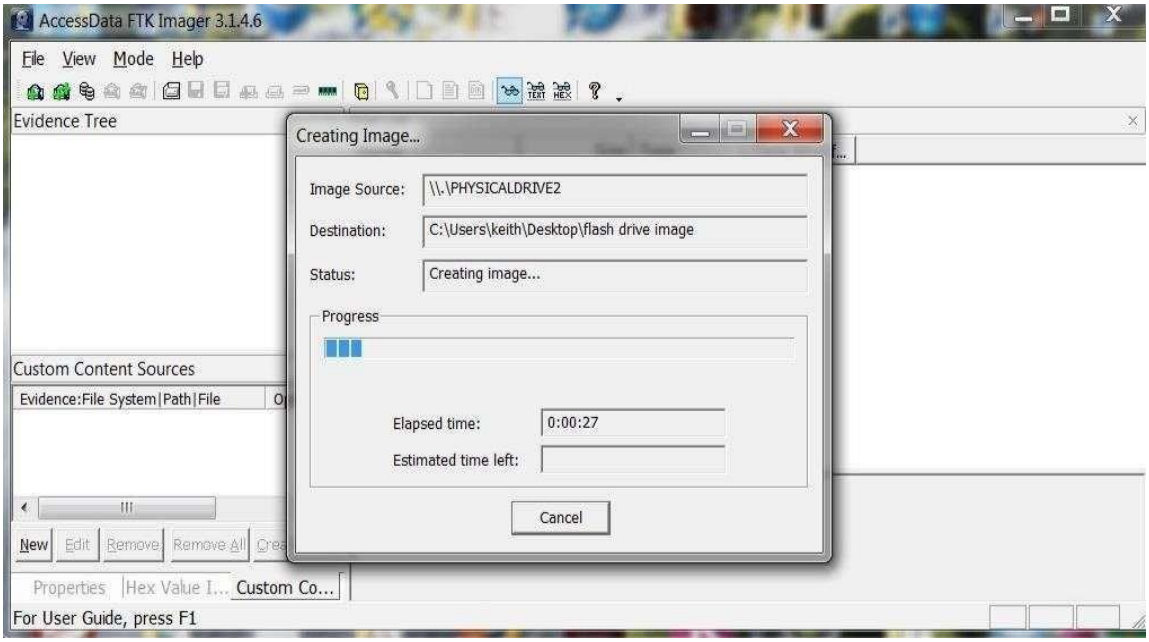
Go to the menu at the top of the application and select:

- **File -> Create Image**

It will open a wizard that will walk you through the process of opening a case and ask you for a case number, evidence number, examiner name, etc. Obviously, this software

was designed for law enforcement and all evidence needs to be categorized and labelled.

Finally, it will ask for a location of the physical drive you want to image, a destination directory and a name for the image file. When you are done with all these administrative tasks, FTK Imager will begin the process of creating a forensically sound bit-by-bit image of your drive.



Now that we've created an image of the flash drive, we are ready to recover the deleted files.

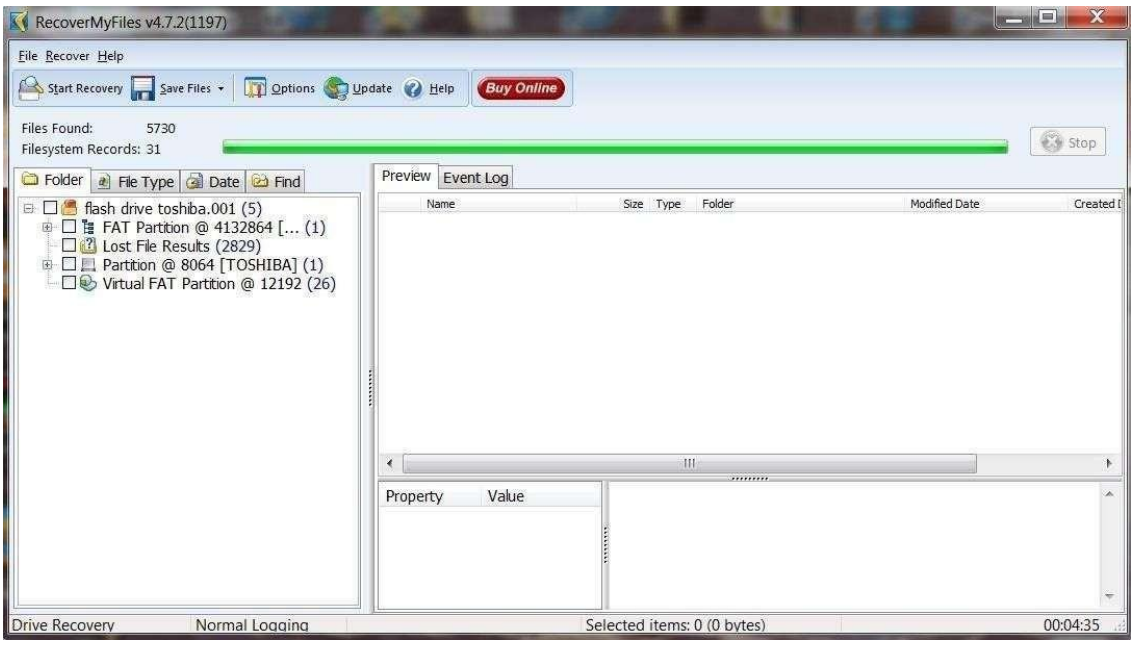
Step 4: Recover Deleted Files

There are many tools on the market to recover deleted files and all of them are adequate to do the job. Deleted file recovery is probably the simplest of forensic tasks. Here, I will be using a trial version of RecoverMyFiles.

You can download a trial version **here.**

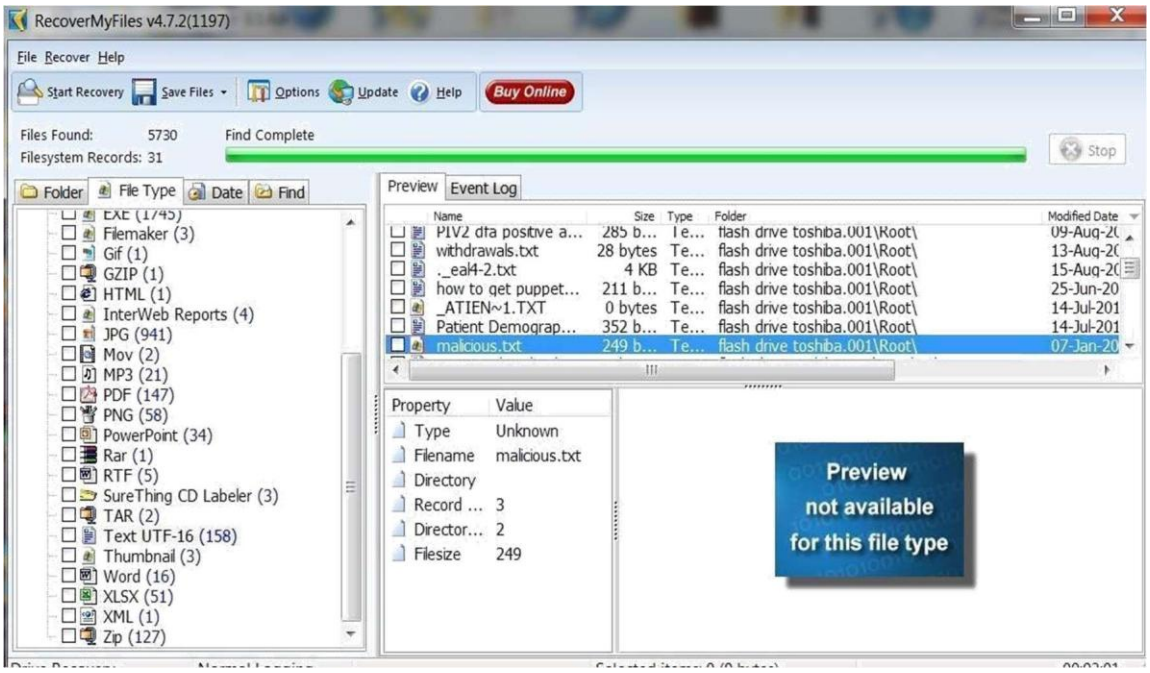
Once you have installed RecoverMyFiles, select the Start Recovery icon in the upper left corner. It will ask you to select either Recover Files or Recover Drive. Select Recover a Drive. It will then search and display all your drives like that in the screenshot below. Since we are using a forensic image, select Add Image button to the right. You will need to provide a path to your image file created with FTK.

Once you select an image file, start the automatic file recovery. When the recovery is completed, you will see a screen similar to the one below.



I then selected the File Type tab above the Explorer window to categorize the files by type.

As you can see, there are numerous file types recovered from this flash drive. Since our malicious document was a .txt, I have selected the TXT UTF-16 file type. It then puts all 158 .txt files on display in the upper right window. As you can see, it has recovered our malicious.txt file and everything on it. Busted!



I'm hoping that this tutorial clearly showed you how simple it is for a forensic investigator to recover the files you have deleted. This should be a lesson that you need to be exceedingly cautious and when possible, overwrite any deleted files to remove evidence. In some cases, even that may not be enough to keep your files from a skilled forensic investigator.

EX NO:3	ACQUIRE FORENSIC IMAGE OF HARD DISK USING ENCASE FORENSICS IMAGER AND ALSO PERFORM INTEGRITY CHECKING/VALIDATION
DATE:	

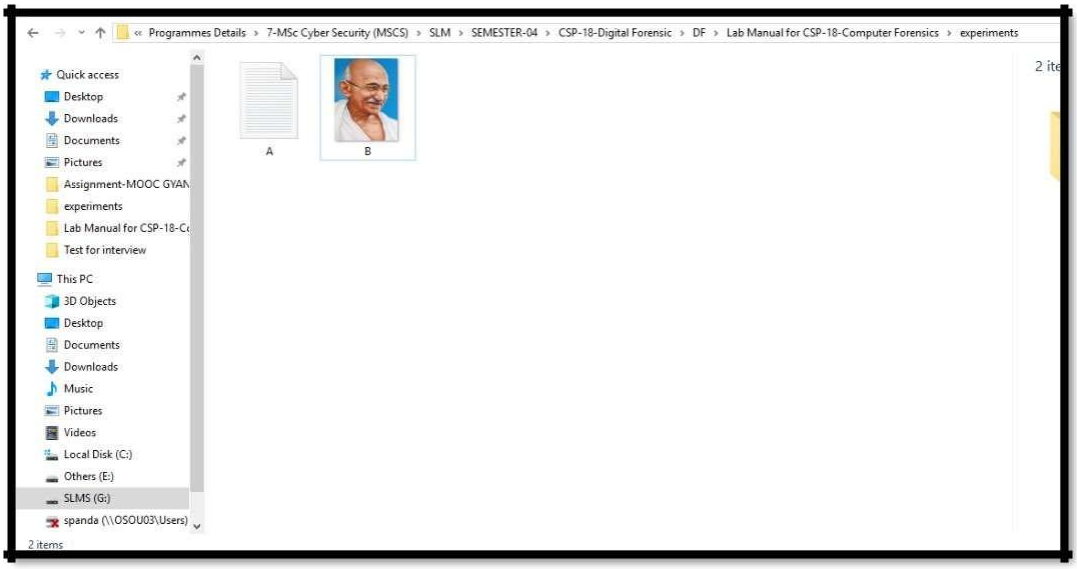
Aim:

To study the steps for hiding and extract any text file behind an image file/ Audio file using Command Prompt.

Any file like .rar .jpg .txt or any file can be merged inside another file. In a simple way, we shall learn how to hide a text file inside an image file using the Command Prompt.

How to Hide the FILE?

Suppose you have to hide a text file “A.txt” with the image file “B.jpg” and combine them in a new file as “C.jpg”.Where “C.jpg” is our output file which contains the text hidden in the image file.

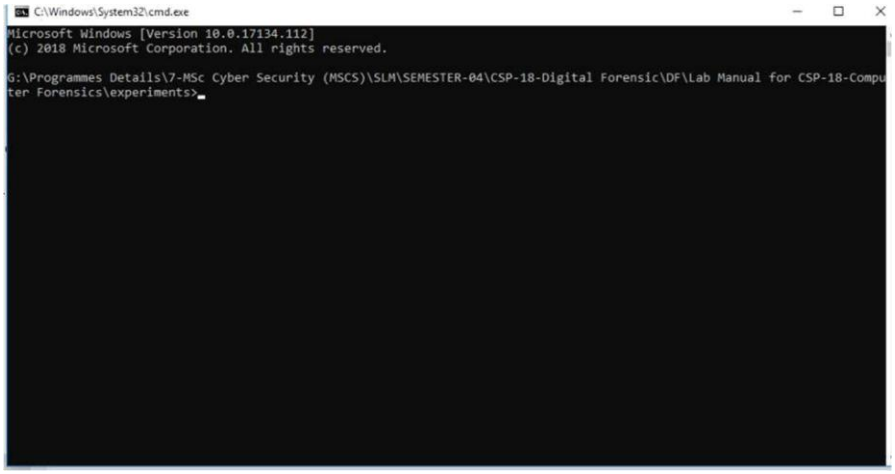


Follow the steps:

1. copy the file,u need to hide, to desktop(for our tutorial let us assume the file to be "A.txt")
2. copy the image, within which you need to hide the file, to desktop (let it be "B.jpg")
3. now open the cmd:

   >ctrl+r

   >type: **cmd** and hit **enter**



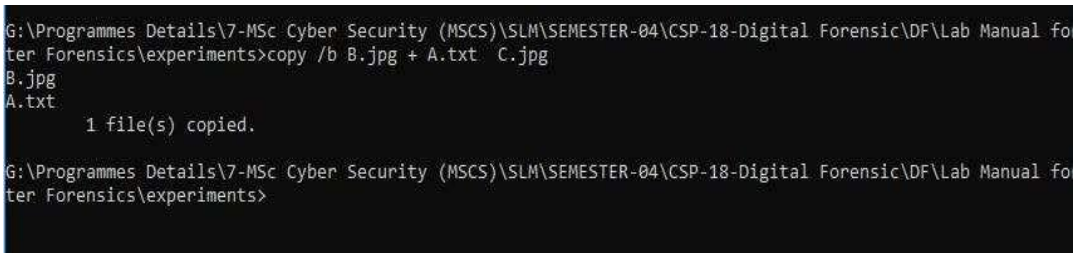
4. in cmd first type the code as follows:

   >**cd desktop**

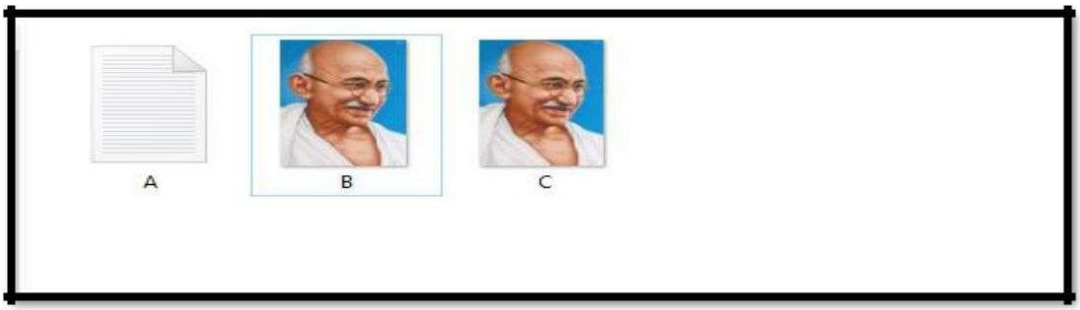
   NOTE: this code is for assigning the location on cmd to desktop
5. Now type the following code:

> copy /b B.jpg + A.txt C.jpg

Syntax: *copy /b Name-of-file-containing-text-you-want-to-hide.txt + Name-of-initial-image.jpg Resulting-image-name.jpg*

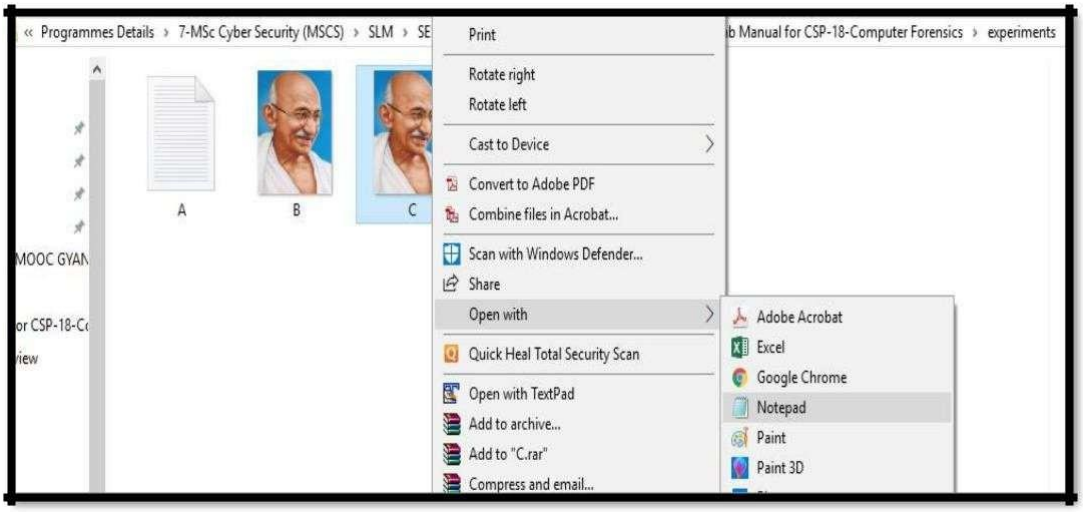


"C.jpg" is the output image inside this out image our file is hidden



How to retrieve the file?

1. locate C.jpg file from where you want to retrieve text data
2. Right-click and open with notepad



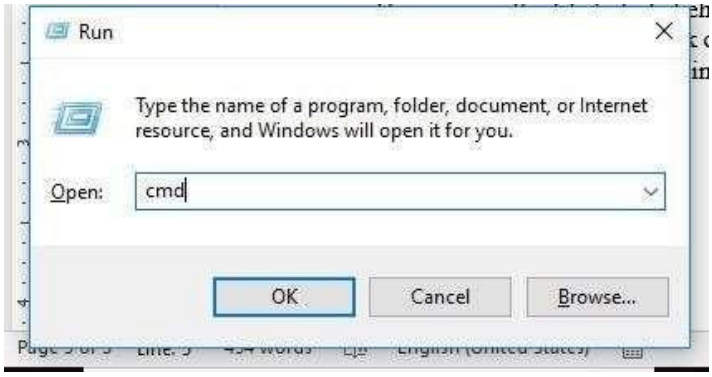
Done! Successfully opened! In the last of the notepad, you'll find the content of the text file.

Hide A Message Into Image:
Open Run command window by pressing **win + r**.
Open command prompt by typing **cmd** and press **OK**
Enter the directory where you have your files. Then type the command :

echo "Your Message">>"image.jpg"
Now the message is successfully hidden in the image file.
To view the message: Open with Notepad, at last, you'll find the Your Message

Another Method

1. Open Run command window by pressing **win + r**.
2. Open command prompt by typing **cmd** and press OK



3. Enter the directory where you have your files.
4. Then type the command :

>> copy /b B.jpg + A.rar C.jpg

Here a.rar is the file to hide behind the image file (b.jpg) and the output file is **c.jpg**.

To view the RAR file: right-click on the output image (here, c.jpg) and open with WinRAR. You'll find the file inside the image.

Hide File and text behind Audio File

Firstly get hold of a sound file you want to hide the data in (example sound.mp3), then gather all your files you want to hide and put them in a ZIP (example secret.zip).

Our chosen Sound and zip file:

Windows 7/10: Shift+right click in the folder containing the files will open the command prompt in that directory Windows: Open command prompt (start->run cmd), then use cd to get to the folder where the files are stored.

Linux: You know what to do, open terminal and move to the directory containing files.

We now need to merge these files together, but we want to use a binary merge to keep the two files intact. With Windows copy command this uses the /B switch. (Binary Data)

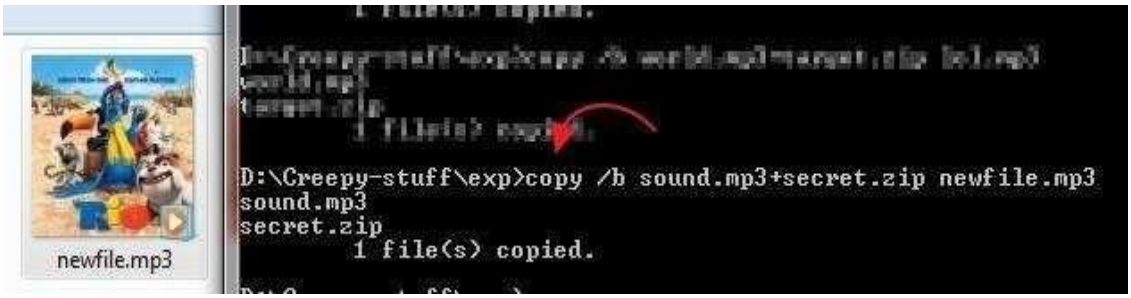
Windows
Code:

copy /b secret.zip + sound.mp3 newfile.mp3

Linux
Code:

cat sound.mp3 secret.zip > newfile.mp3

You should now have gained a new file called newfile.mp3. This should look identical to the sound you started with when opened with a media player, but with a secret payload hidden within. Here is the example sound containing a ZIP:



The two simplest ways to get your data back out of these files is to either change the extension from .mp3 to .zip or to open your chosen ZIP program and open newfile.mp3 within that. You should now be presented with your original files.

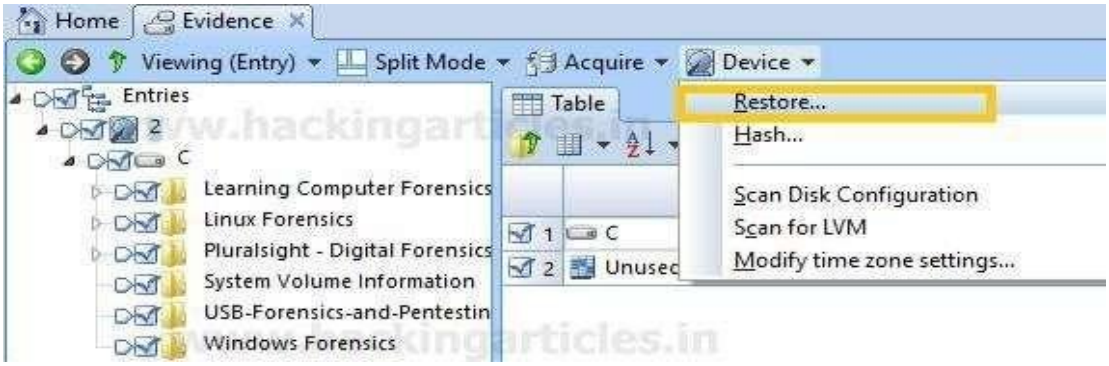
EX NO:4	RESTORE THE EVIDENCE IMAGE USING ENCASE FORENSICS IMAGER
DATE:	

Aim:

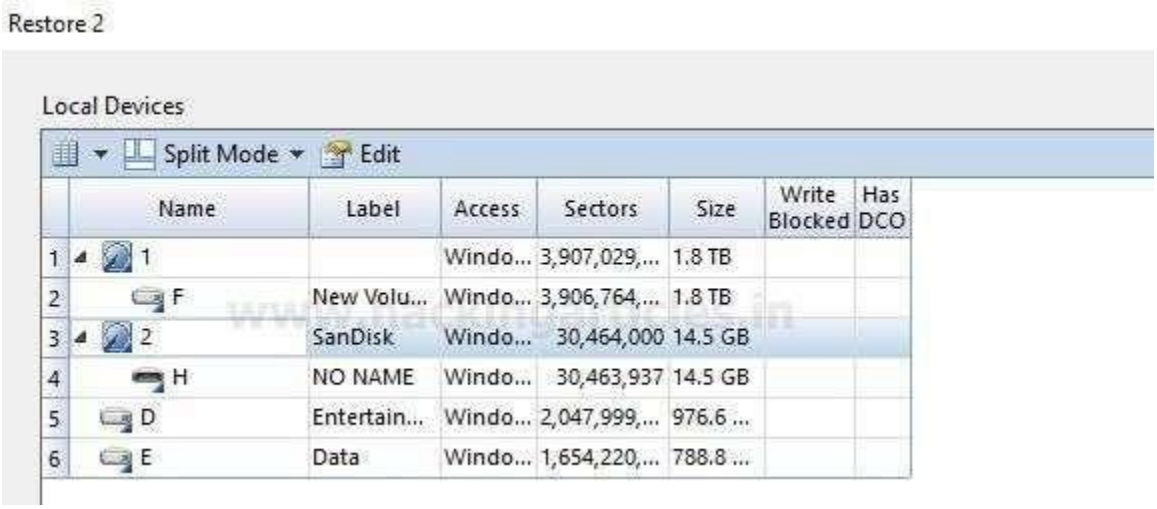
How to Restoring the Evidence Image using EnCase Imager Open Encase Imager and add the evidence to Encase imager

Browse to the image (.E01) file and add it to the case. The evidence added will get listed

Double click on the image, select he files to be restored and select the restore option located under Device option.



When we click on restore, connect the drive where we want to restore the image and click next. All the drives will be read. All the drives will be displayed, select the drive where the image is to be restored. Use the blank drive for restoring the image as the existing data will be wiped.



	Name	Label	Access	Sectors	Size	Write Blocked	Has DCO
1	1		Windo...	3,907,029,...	1.8 TB		
2	F	New Volu...	Windo...	3,906,764,...	1.8 TB		
3	2	SanDisk	Windo...	30,464,000	14.5 GB		
4	H	NO NAME	Windo...	30,463,937	14.5 GB		
5	D	Entertain...	Windo...	2,047,999,...	976.6 ...		
6	E	Data	Windo...	1,654,220,...	788.8 ...		

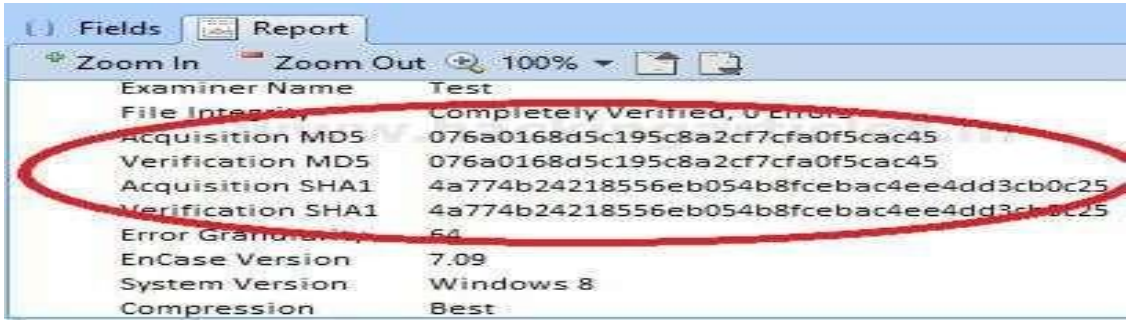
If required we can verify the Hash values and click on finish.

Type “Yes” in the text box and click on OK this will wipe the existing data on the drive and start with the image restoration.

Image Restoration will start, we can check the progress on the lower right corner of the window.

Once the restoration is complete, we can see the data in the drive we have selected.

To ensure the integrity of the data, we can see the report section on the bottom pane and check the hash values. The hash values should be the same as of the image (we can check the original hash value in the image report.)



If required we can copy and save the report in any text / word file for any future reference.

EX NO:5A	STUDY THE FOLLOWING: (A) COLLECT EMAIL EVIDENCE IN VICTIM PC
DATE:	

Aim

How to make the forensic image of the hard drive using EnCase Forensics.

Introduction

In solving computer crime cases, computer forensics is used to gather evidence, which will be analyzed and presented to a court of law to prove the illegal activity.

It is important that when doing computer forensics, no alteration, virus introduction, damages or data corruption occurs.

In order to do a good analysis, the first step is to do a secure collection of computer evidence. Secure collection of evidence is important to guarantee the evidential integrity and security of information.

The best approach for this matter is to use a disk imaging tool. Choosing and using the right tool is very important in computer forensics investigation.

Disk imaging

Disk imaging as defined by Jim Bates, Technical Director of Computer Forensics Ltd, refers to:

"An image of the whole disk was copied. This was regardless of any software on the disk and the important point was that the complete content of the disk was copied including the location of the data.

Disk imaging takes sector-by-sector copy usually for forensic purposes and as such it will contain some mechanism (internal verification) to prove that the copy is exact and has not been altered.

It does not necessarily need the same geometry as the original as long as arrangements are made to simulate the geometry if it becomes necessary to boot into the acquired image."

Disk imaging is also one of the approaches for backup except that backup only copies the active file.

In backup, ambient data will not be copied. This is an area where the most important

source for the evidence could be found. Ambient data is a data stored in Windows swap file, unallocated space and file slack.

Scenario: Mr. X is suspected to be involved in selling his company's confidential data to the competitors, but without any evidence, no action could be taken against him.

To get into reality and proof Mr. X guilty, the company has requested the forensic services and have come to know all the relevant data is present inside the desktop provided to him.

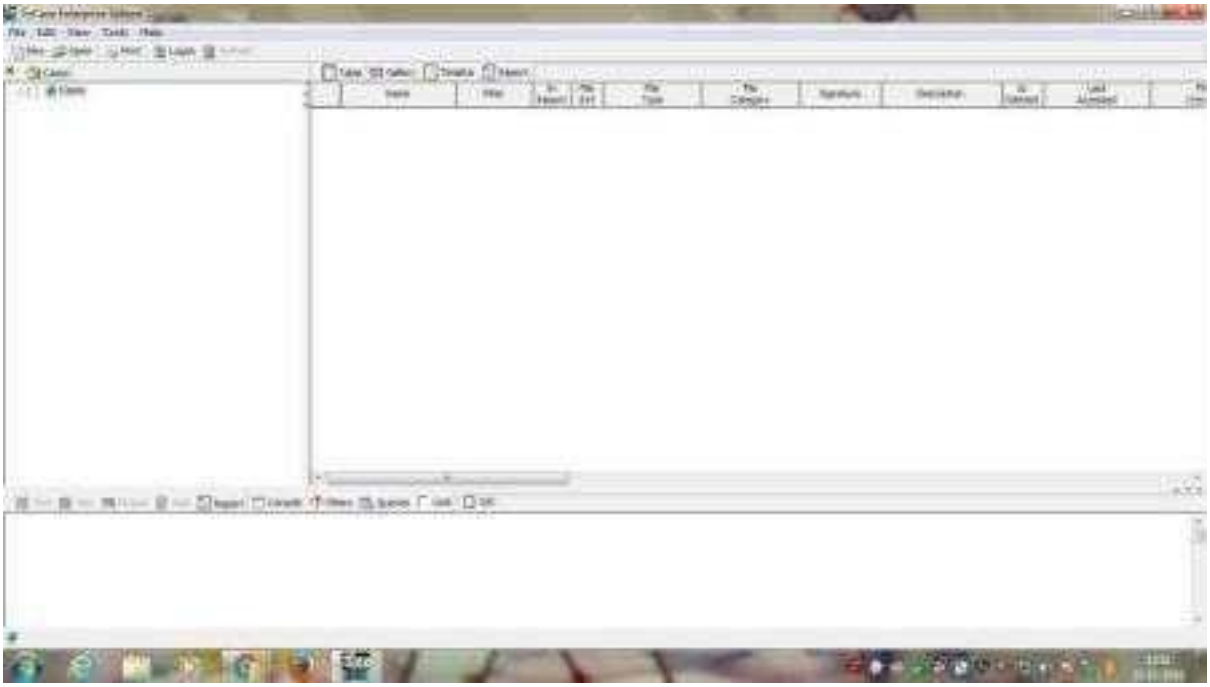
Since it is never advised to work with the original evidence because we may lose some relevant data accidentally, so we will create an image of the original evidence and work on it further.

This way the original evidence is safe and the integrity and authenticity of the evidence could be proved through hash values

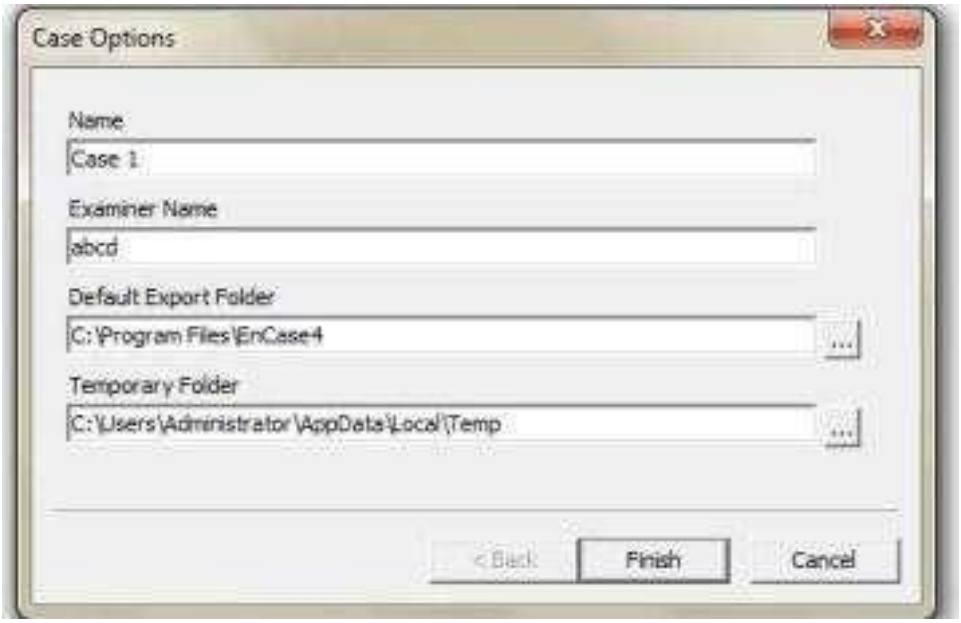
Step-01:

To image the computer hard drive, we will use **Encase Imager**. EnCase Imager is a software which is bundled with numerous features which aid in all the four phases of forensic investigation i.e. Collection, Preservation, Filtering and Report.

First, download the Encase Imager demo from here and install in your computer. Once it is installed, Initialize the Software in Enterprise Mode.

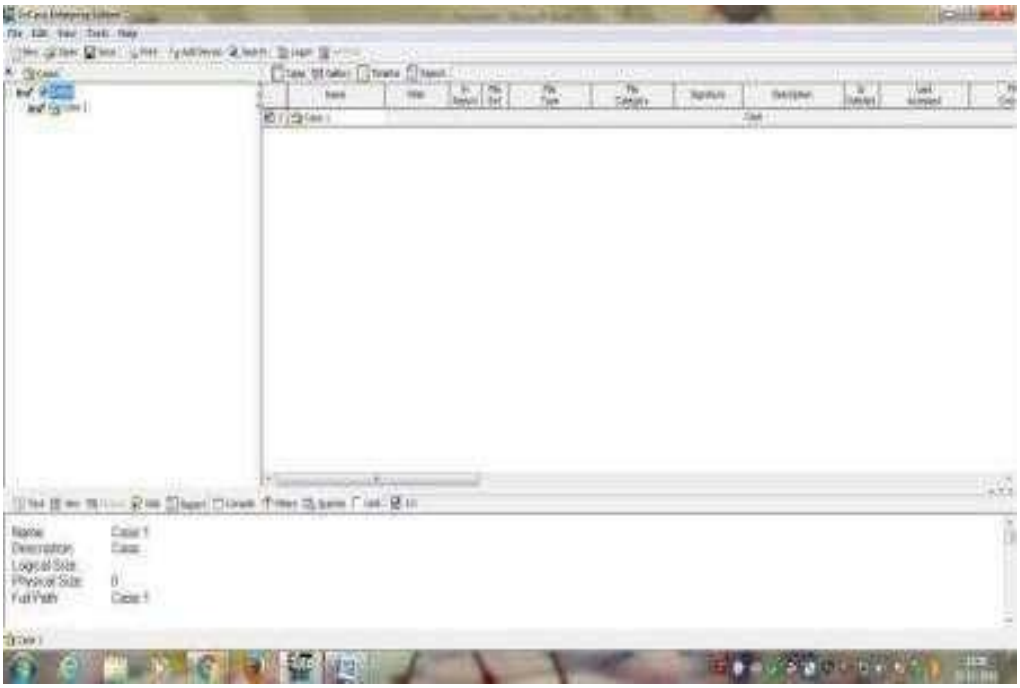


Step 2: Click On New For Creating A New Case. Fill the labels.

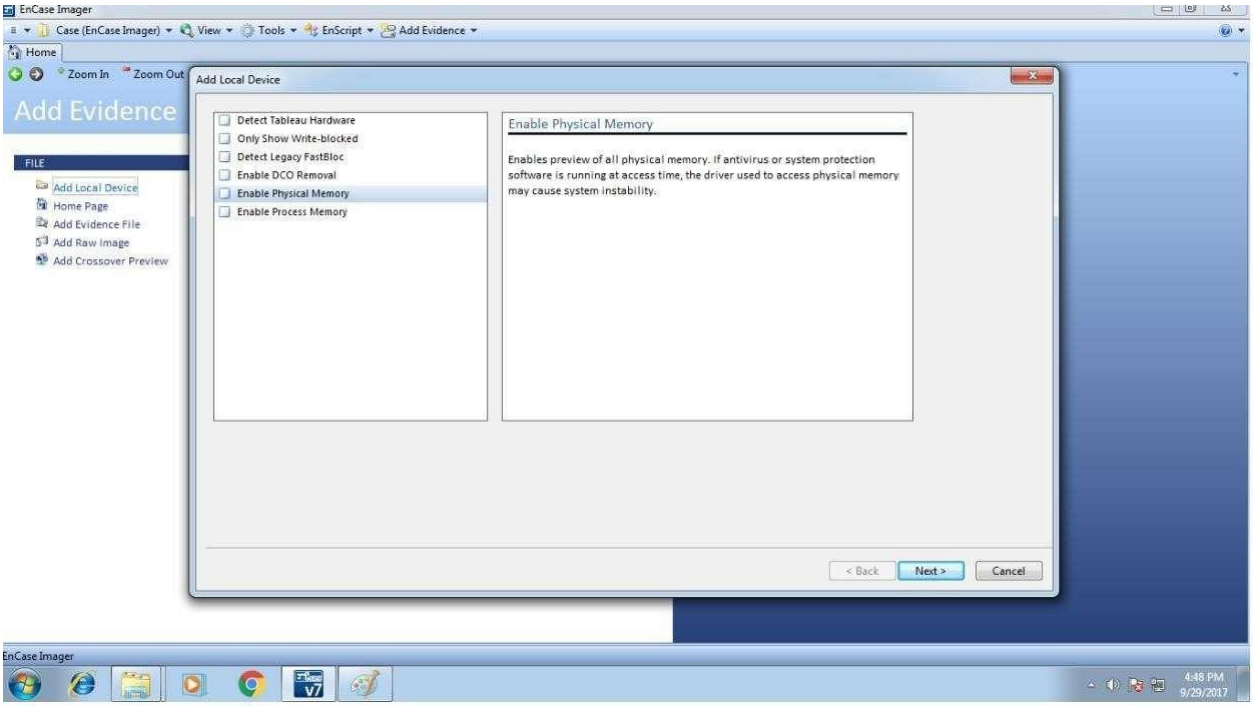


Click On Finish.

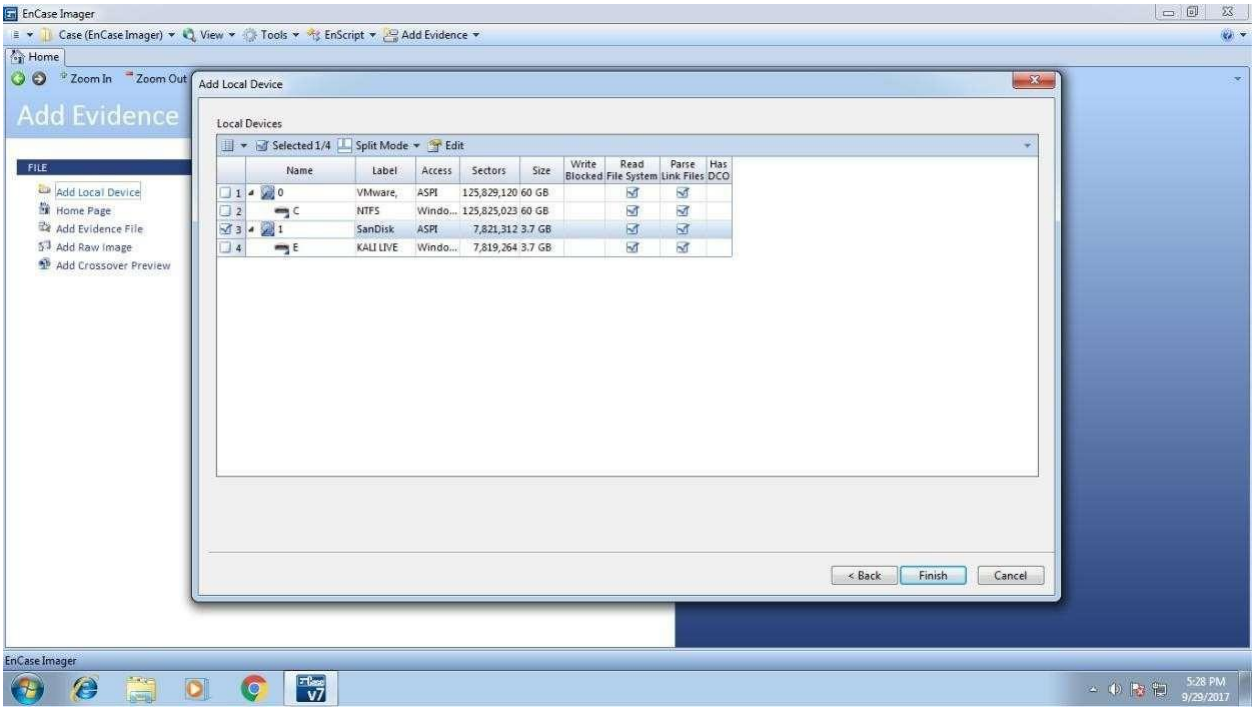
Step 3: View the Case by Clicking On Case 1 <Case Name>



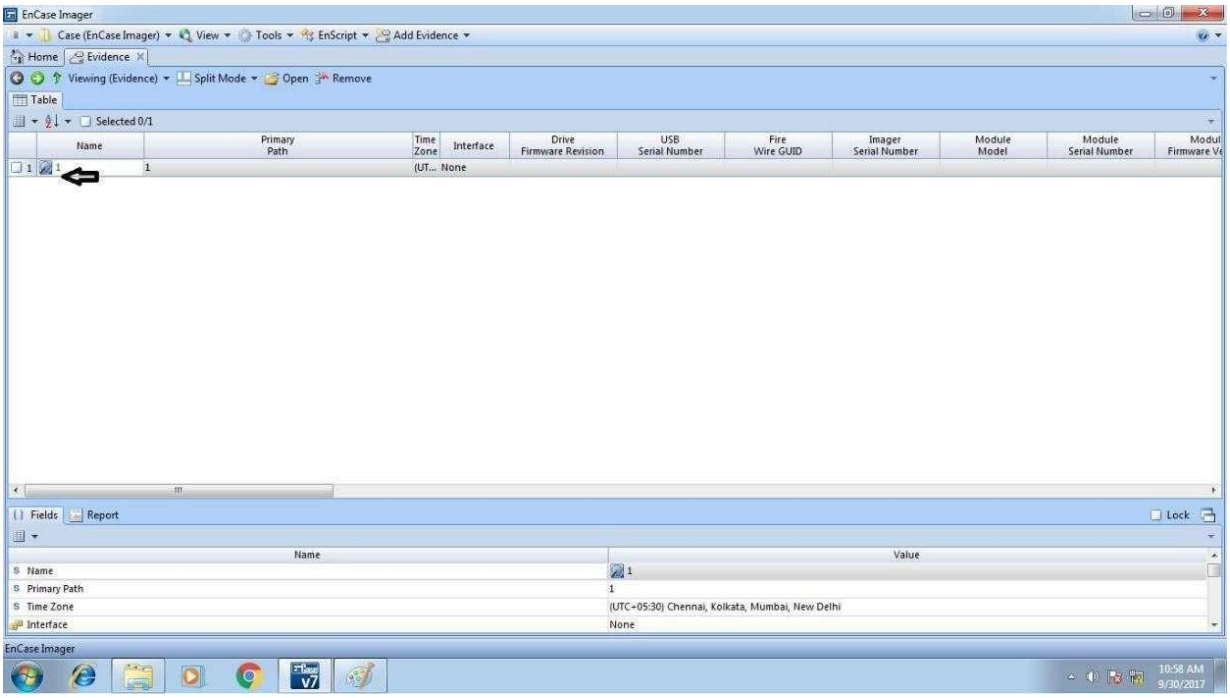
Step 4: Click on add local device for Adding Devices to Your Case. If there is any write blocker attached with the machine and digital deice then tick to 1,2 and 5 option otherwise untick to all and click on **Next button**.

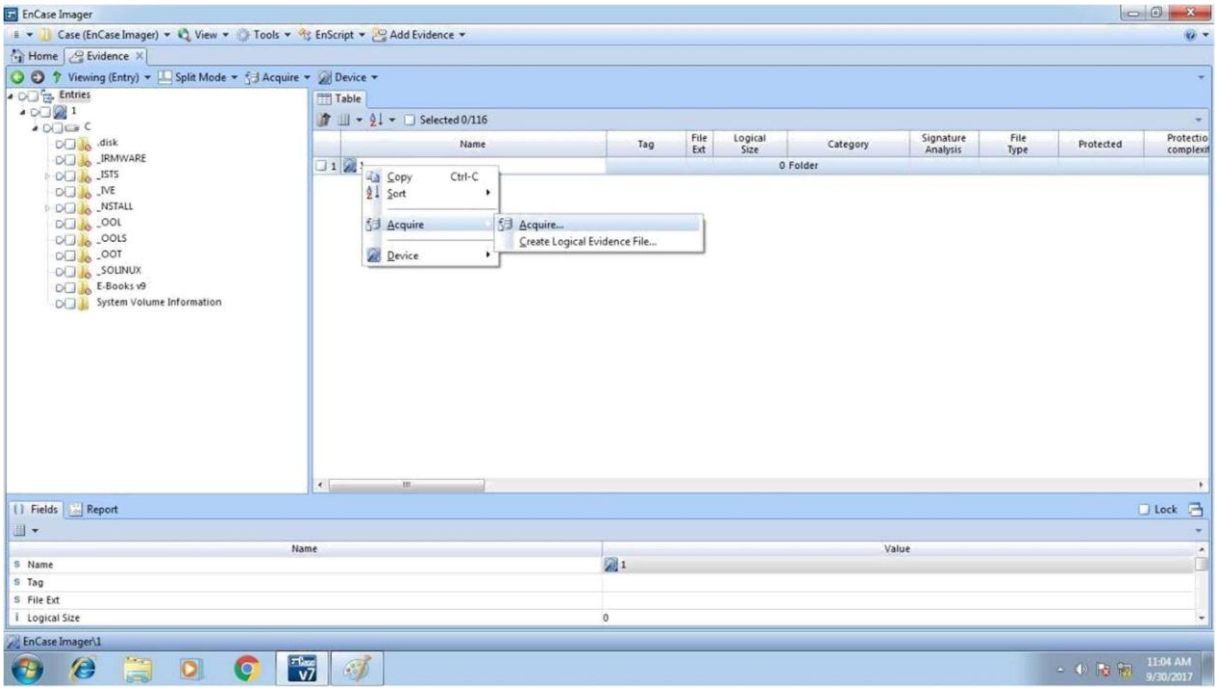


Step 5: Tick in the box of name column which shows the connected device name or label like (1,2,3 or any numeric number) and click on the **finish button**.

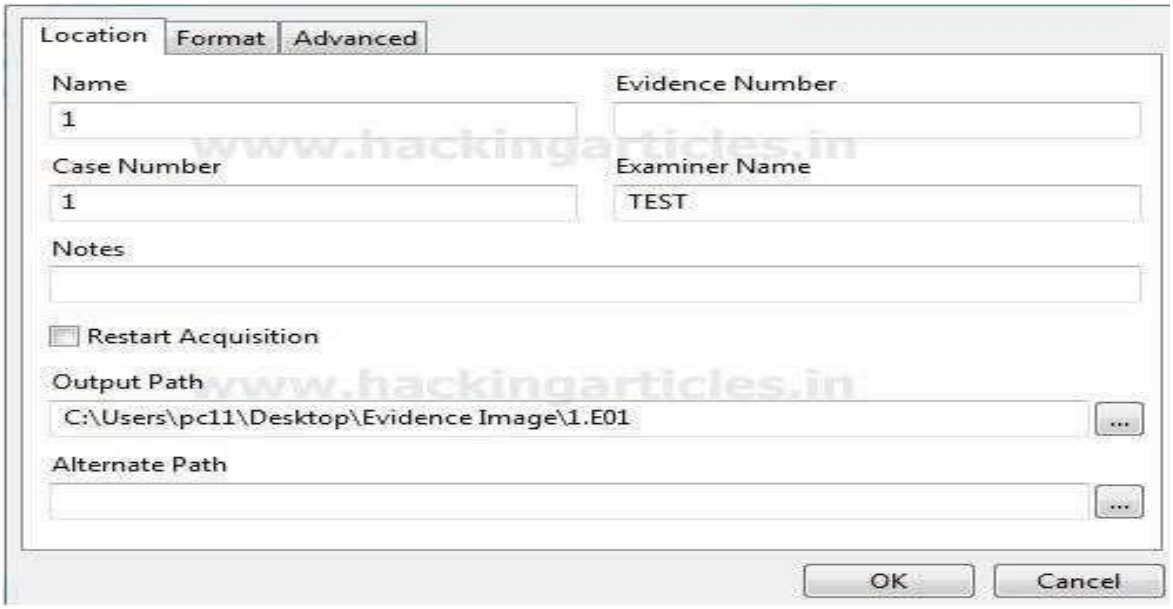


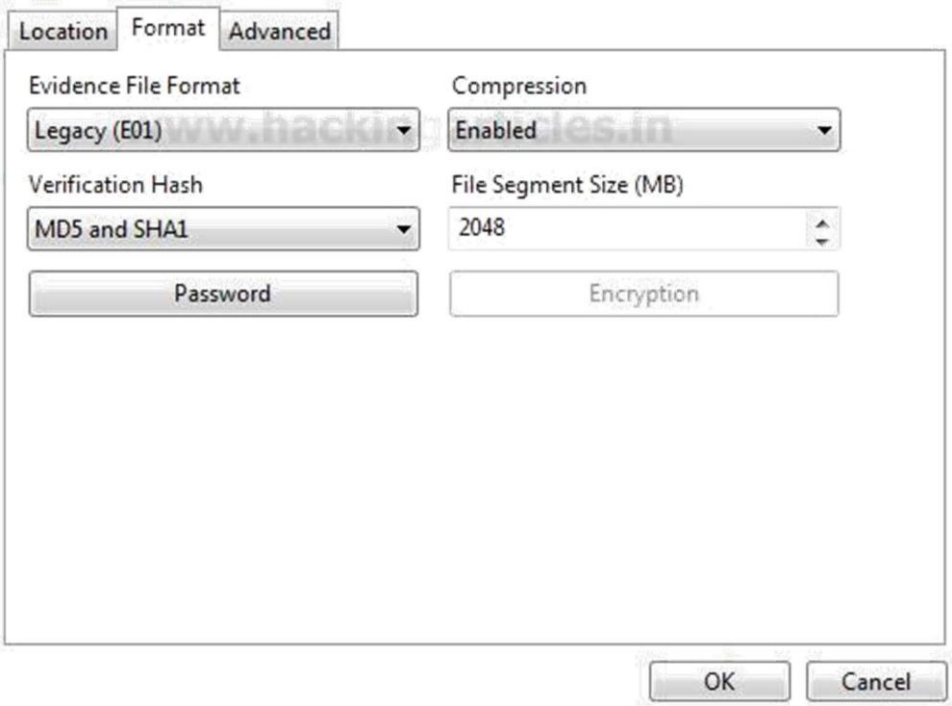
Step-06: Now to open evidence click on label number of the device which shows in "name" column and again right-click on label number and choose **acquire the option**.



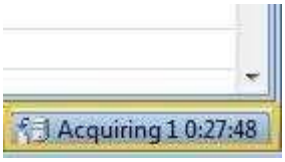


Step-07: Then a pop up will appear with three tabs. In the **location tab**, fills all the fields. In **format tab** if you want to encrypt the evidence file then enable the Compression field otherwise disable it. In Verification Hash field value should be chosen MD5 and SHA1 after it click on **OK button.** File format selected here is **E01** as this is supported by multiple tools and is suitable for further analysis. If we want to password protect/encrypt our image we can do this at this stage.





Step-08: After it, image creation will be start and time taken to create the image will be shown on the right side of the bottom. you can check the status of image acquisition on the same window at the lower right corner along with the time remaining (refer below image).



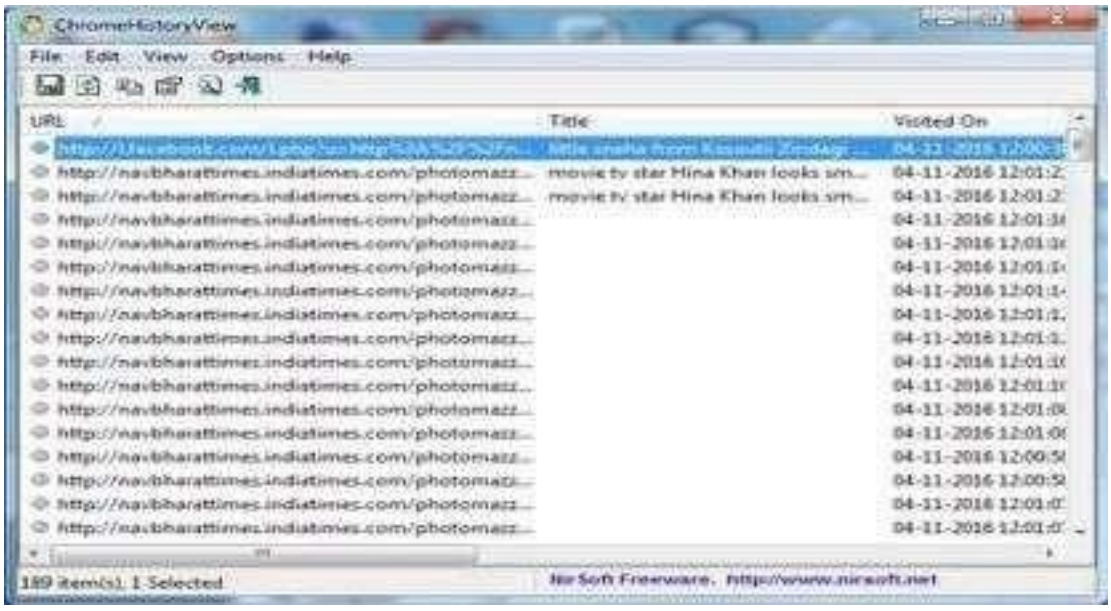
Step-09: Device will automatically disconnect after creating the image. The image will save in the folder which we set the path earlier. Once the acquisition is complete the image will get saved to the output folder (refer below image).

EX NO:5B	(B) EXTRACT BROWSER ARTIFACTS (CHROMEHISTORY VIEW FOR GOOGLE CHROME)
DATE:	

Aim:

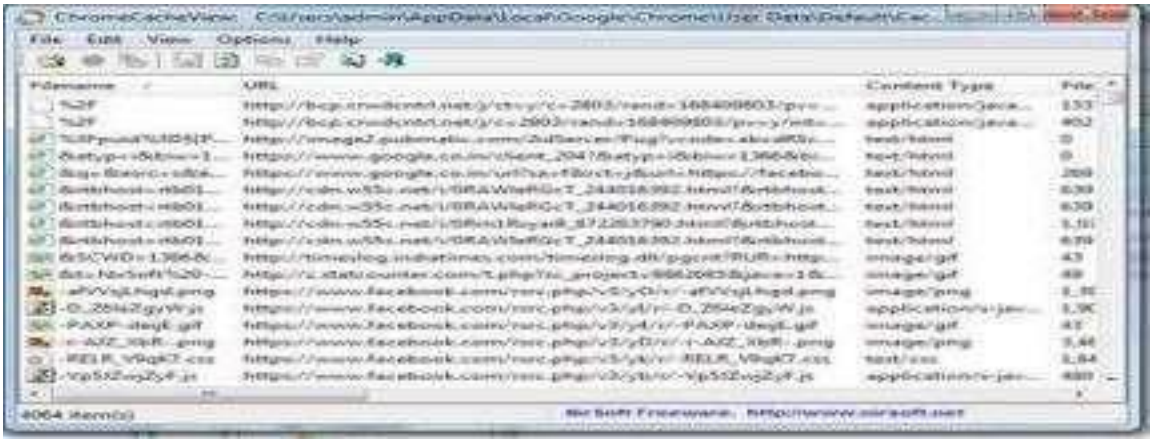
How to Extracting Browser Artifacts

ChromeHistoryView: is a small utility that reads the history data file of Google Chrome Web browser, and displays the list of all visited Web pages in the last days. For each visited Webpage, the following information is displayed: URL, Title, Visit Date/Time, Number of visits, number of times that the user typed this address (Typed Count), Referrer, and Visit ID.

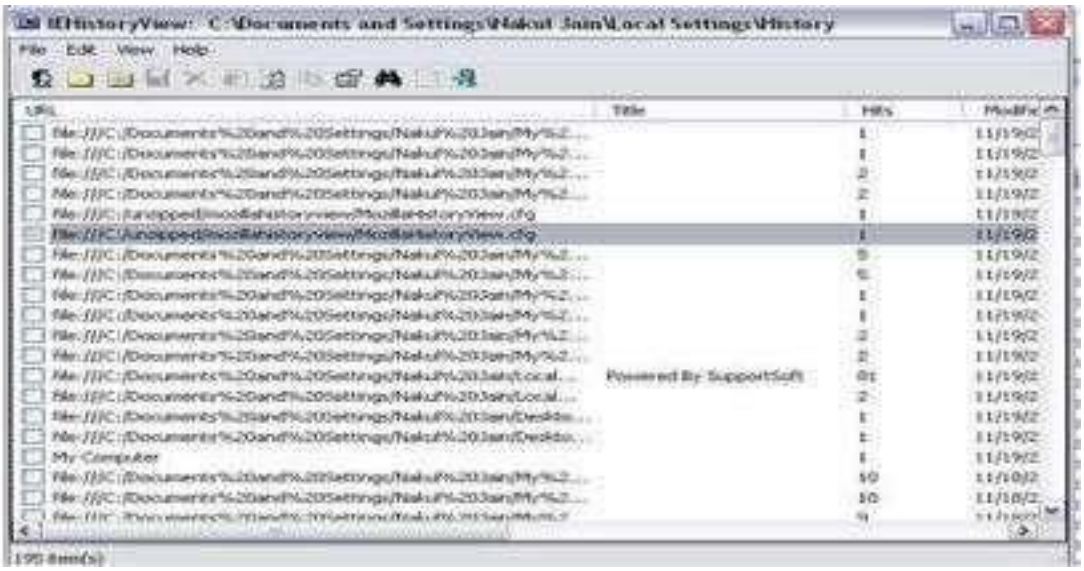


ChromeCacheView: Chromecacheview is a small utility that reads the cache folder of Google Chrome Web browser, and displays the list of all files currently stored in the cache.

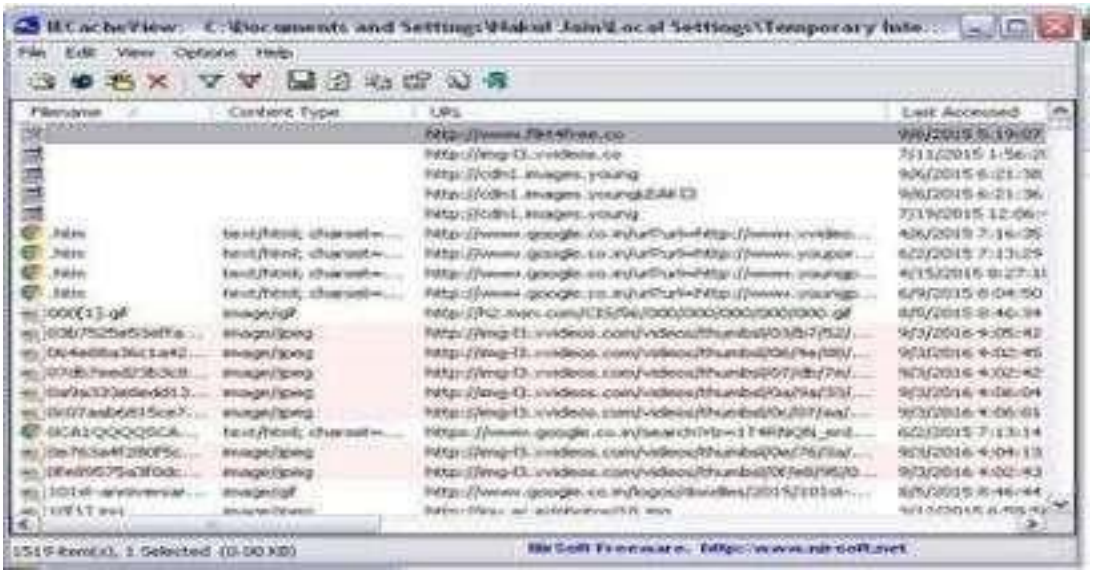
For each cache file, the following information is displayed:
URL, Content type, File size, Last accessed time, Expiration time, Server name, Server response, and more. You can easily select one or more items from the cache list, and then extract the files to another folder, or copy the URLs list to the clipboard.



IEHistoryView: This utility reads all information from the history file on your computer, and displays the list of all URLs that you have visited in the last few days. It also allows you to select one or more URL addresses, and then remove them from the history file or save them into text, HTML or XML file.



IECacheView: IECacheView is a small utility that reads the cache folder of Internet Explorer, and displays the list of all files currently stored in the cache. For each cache file, the following information is displayed: Filename, Content Type, URL, Last Accessed Time, Last Modified Time, Expiration Time, Number of Hits, File Size, Folder Name, and full path of the cache filename.


IECacheView - C:\Documents and Settings\Bakul Jain\Local Settings\Temporary Inte...
File Edit View Options Help
Filename
Content Type
URL
Last Accessed
1519 item(s), 1 Selected (0.00 KB)
NirSoft Freeware. http://www.nirsoft.net

EX NO:6	USE USBDEVIEW TO FIND THE LAST CONNECTED USB TO THE SYSTEM
DATE:	

Aim:

Find Last Connected USB on your system (USB Forensics)

USBDeview is a small utility that lists all USB devices that currently connected to your computer, as well as all USB devices that you previously used.

For each USB device, extended information is displayed: Device name/description, device type, serial number (for mass storage devices), the date/time that device was added, VendorID, ProductID, and more…

USBDeview also allows you to uninstall USB devices that you previously used, disconnect USB devices that are currently connected to your computer, as well as to disable and enable USB devices.

You can also use USBDeview on a remote computer, as long as you log in to that computer with admin user.

Device Na...	Description	Device Type	Safe...	Conne...	Last Plug/Unplug ...	VendorID
	Nokia 7210 Supern...	Communication	No	No	7/26/2011 5:49:04 ...	0421
0000.001d.00...	HUAWEI Mobile C...	Vendor Specific	Yes	No	8/1/2011 8:54:29 PM	12d1
0000.001d.00...	HUAWEI Mobile C...	Vendor Specific	Yes	No	8/1/2011 8:54:27 PM	12d1
0000.001d.00...	HUAWEI Mobile C...	Vendor Specific	Yes	No	8/1/2011 8:54:26 PM	12d1
0000.001d.00...	USB Mass Storage ...	Mass Storage	Yes	No	8/1/2011 8:54:23 PM	12d1
0000.001d.00...	HUAWEI Mobile C...	Vendor Specific	Yes	No	8/5/2011 9:44:46 AM	12d1
0000.001d.00...	HUAWEI Mobile C...	Vendor Specific	Yes	No	8/5/2011 9:44:46 AM	12d1
0000.001d.00...	HUAWEI Mobile C...	Vendor Specific	Yes	No	8/5/2011 9:44:46 AM	12d1
0000.001d.00...	USB Mass Storage ...	Mass Storage	Yes	No	8/5/2011 9:44:46 AM	12d1
0000.001d.00...	HUAWEI Mobile C...	Vendor Specific	Yes	No	8/1/2011 9:59:58 AM	12d1
0000.001d.00...	HUAWEI Mobile C...	Vendor Specific	Yes	No	8/1/2011 9:59:58 AM	12d1
0000.001d.00...	HUAWEI Mobile C...	Vendor Specific	Yes	No	8/1/2011 9:59:58 AM	12d1
0000.001d.00...	USB Mass Storage ...	Mass Storage	Yes	No	8/1/2011 9:59:58 AM	12d1

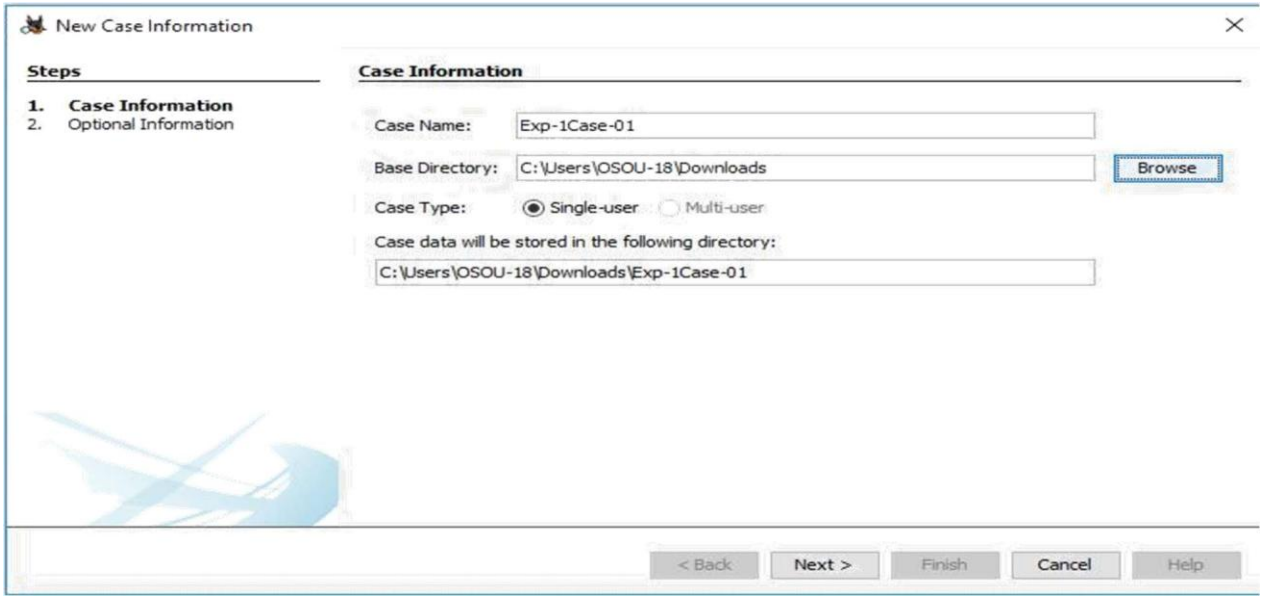
EX NO:7	PERFORM LIVE FORENSICS CASE INVESTIGATION USING AUTOPSY
DATE:	

Aim:

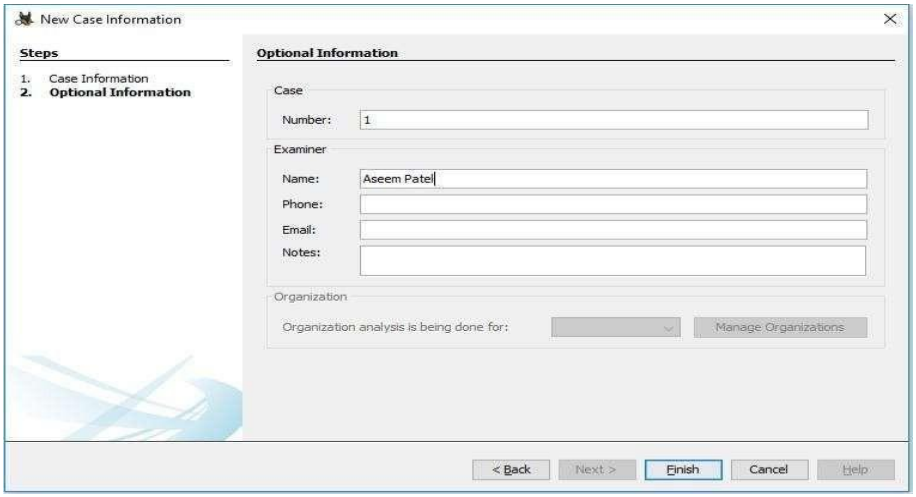
Live Forensics Case Investigation using Autopsy

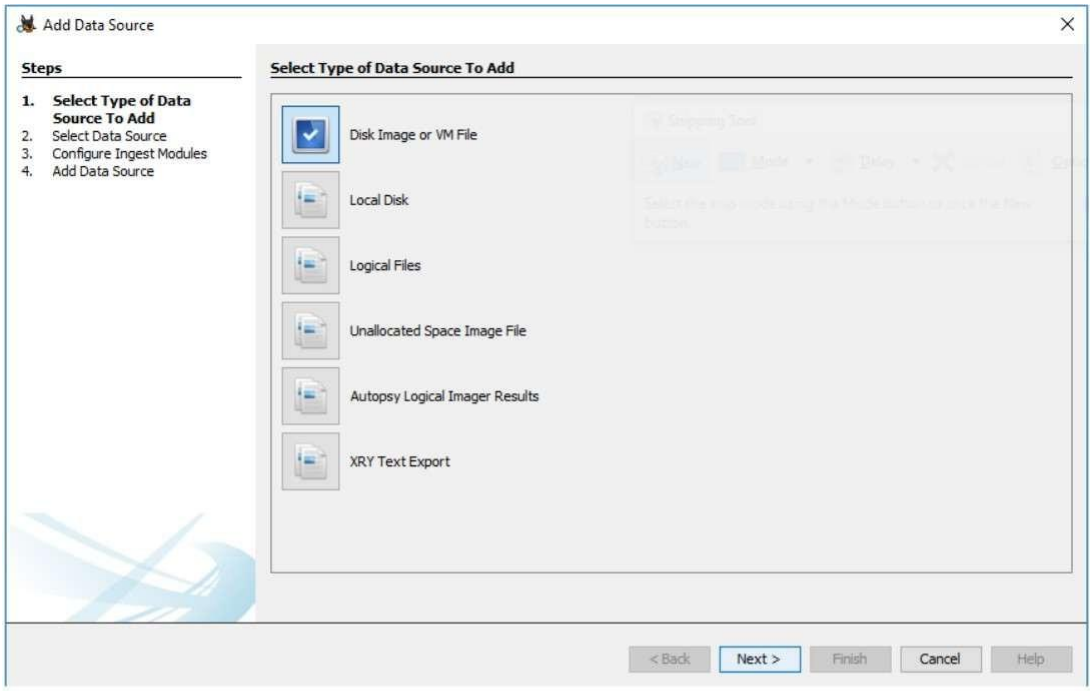
First Download autopsy from here and install in your pc. Click '**New Case**' option.

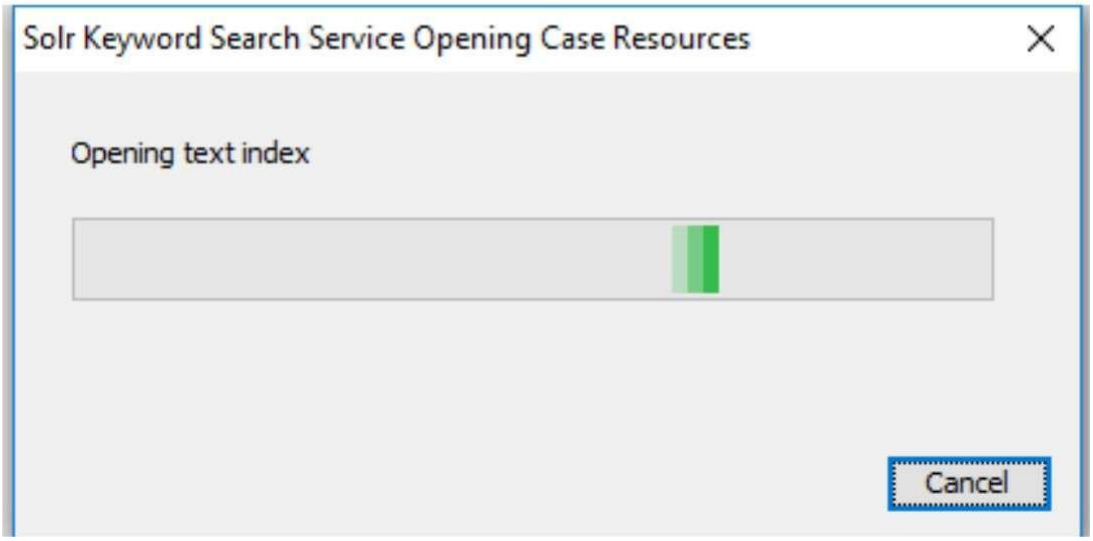
A new page will open. Enter the details in **'Case Name'** and **'Base Directory'** and choose the location to save the report e.g. :Autoreport. Then click on next to proceed to the next step.



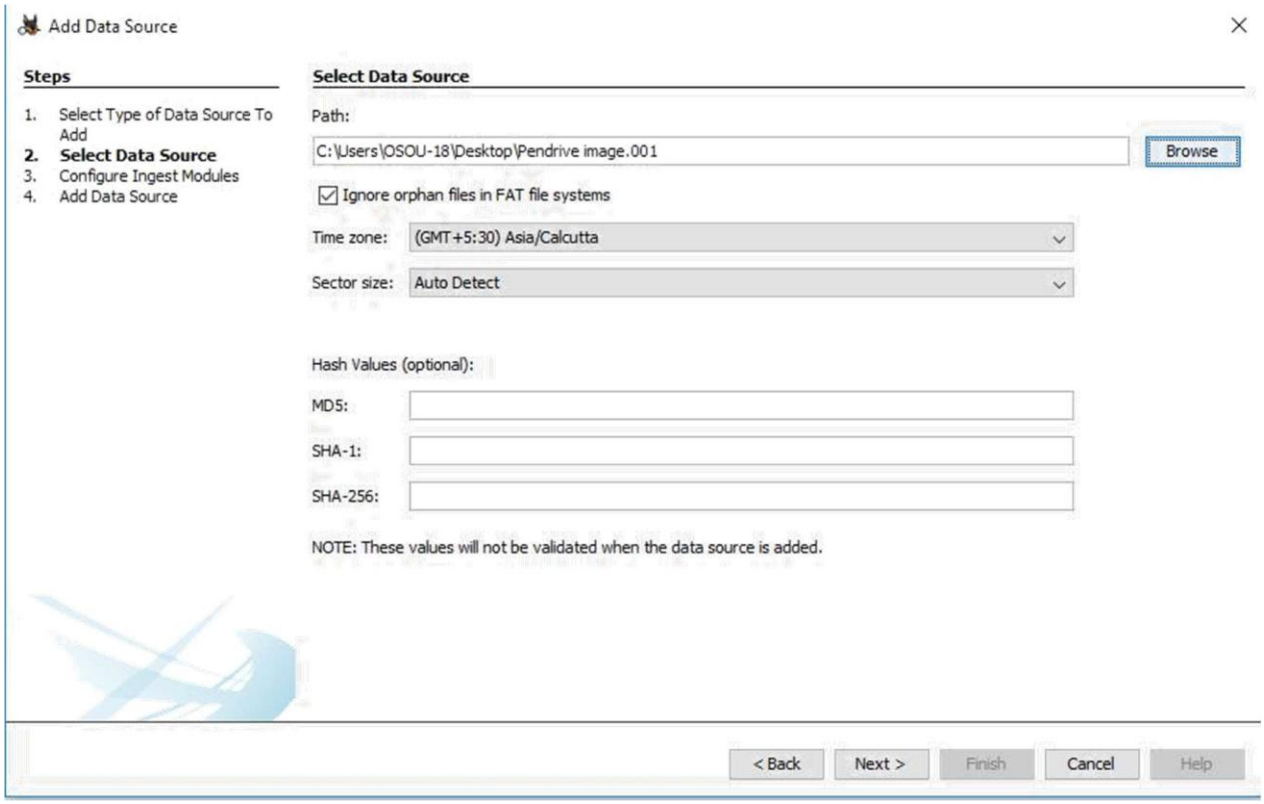
Here in the next step, you have to enter the case number and Examiner details and click on finish to proceed to the next step.





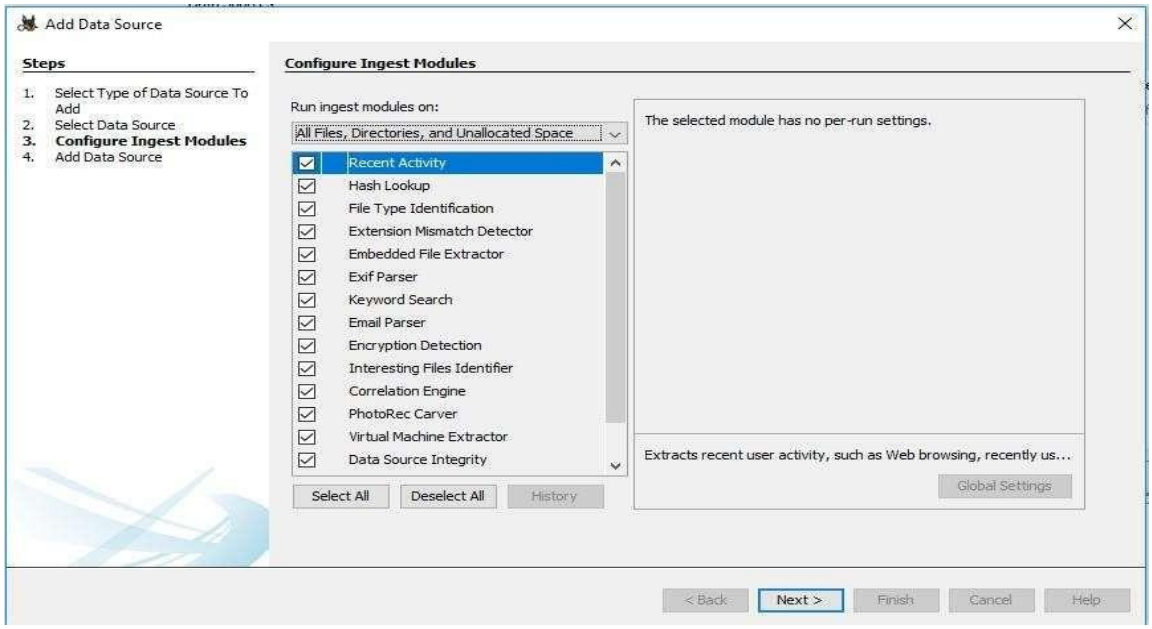


A new window will open. It will ask for the add data source in Step 1. Select source type to add & browse the file Path and click on NEXT option to proceed further

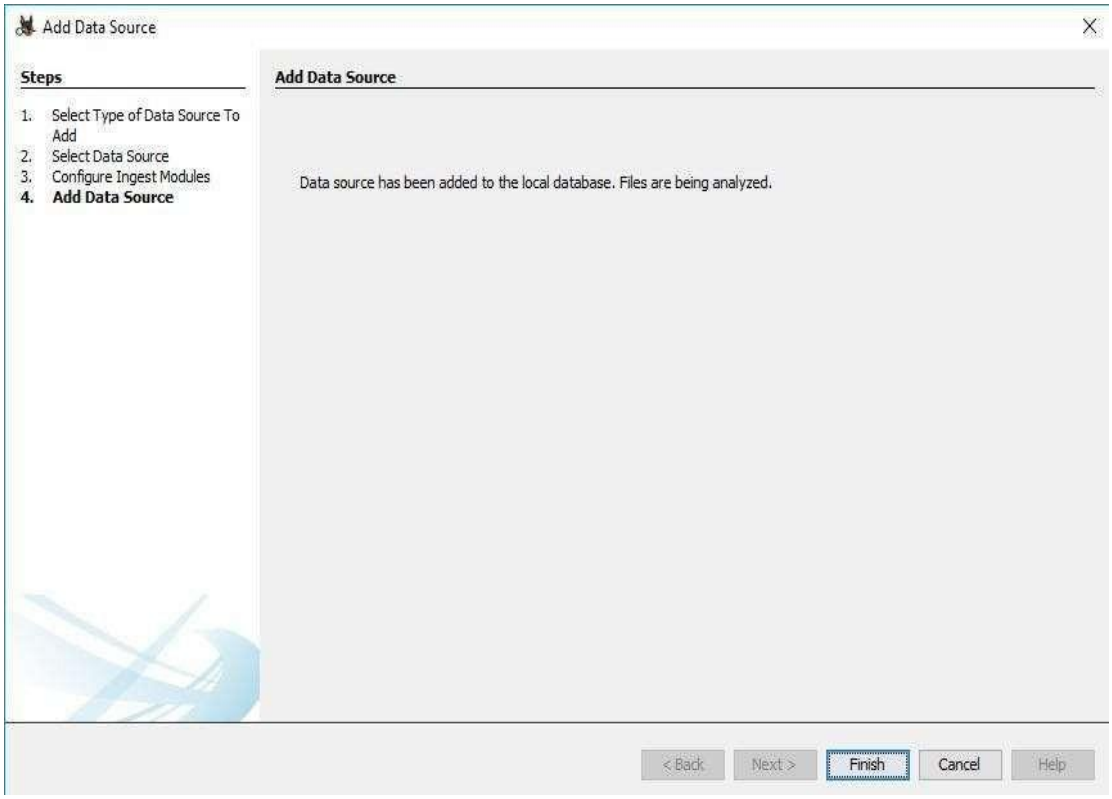


.

Configure ingest Modules I have chosen all the modules as I am looking for complete information on evidence device or disk or system etc. and click next to proceed further.



In Add Data Source just click on Finish to generate the report of the device and you can perform complete investigate on the victim device or system or any other disk. It will process the data Source and add it to the local database.



After Process completion, it will show the Forensic Investigation Report. Now click on Devices Attached option, it will show the list of the attached device with the system.

Now click on EXIF Metadata (Exchangeable image file format for images, sound used by Digital Camera, Smartphone and scanner), click on Installed Programs to see the entire installed programs in the system, Click Operating System Information. It will show the entire operating system list, Now Select Operating System User Account Option. It will Display the name of all the user Accounts, Now click on Recent Documents Option, it will display the latest created or opened documents, Click Web Bookmarks Option to see all the bookmarks by system users in different browsers, To see web cookies, select web cookies option, To See Web Downloads, Click on Web Downloads option, To check internet History, click on Web History Option, To see the history of internet search, click on Web Search Option, To see the list of all email ids in the system, click on email address.

And try to explore other option in autopsy.

EX NO:8	STUDY EMAIL TRACKING AND EMAILTRACING AND WRITE A REPORT ON THEM.
DATE:	

Aim

To study and understand the concepts, methodologies, applications, and ethical considerations of email tracking and email tracing, highlighting their significance in communication, marketing, cybersecurity, and investigative processes.

Introduction

Email communication is a vital aspect of modern personal and professional interactions. With the growing reliance on email, understanding how to monitor and analyze email activities has become increasingly important. Email tracking and email tracing are two related but distinct techniques that serve this purpose. This report explores the concepts, methodologies, applications, and ethical considerations of email tracking and tracing.

Exercise 1: Email Tracking Setup

1. **Objective**:
   - Learn to implement email tracking using tracking pixels and link tracking.
2. **Procedure**:
   1. Select a tool such as Mailtrack or HubSpot for email tracking.
   2. Compose an email and embed a tracking pixel within the content. For example, if using HubSpot, enable the "track email opens" option before sending.
   3. Add a hyperlink in the email (e.g., "Click here to visit our website") and enable click tracking.
   4. Send the email to a test recipient or group.
   5. Monitor the tool's dashboard to observe metrics like open rates and click-through rates.
3. **Expected Outcome**:
   - Gain insights into recipient engagement, such as knowing if the email was opened or links were clicked.

Exercise 2: Analyzing Email Headers

1. **Objective**:
   - Understand how to extract and analyze email headers to identify metadata.
2. **Procedure**:
   1. Open an email in your email client (e.g., Gmail, Outlook).
   2. Locate the email header. In Gmail, click the three-dot menu on the email and select "Show original."
   3. Copy the header content.

4. Paste it into an Email Header Analyzer tool, such as MXToolbox Header Analyzer.
5. Analyze the decoded metadata, including sender's IP, mail servers, and timestamps. For example, identify the "Received" lines to trace the path.

3. **Expected Outcome**:
    - Successfully trace the route of the email through its originating IP and mail servers.

Exercise 3: Tracing the Origin of an Email

1. **Objective**:
    - Learn to trace an email's source using IP and DNS lookup tools.
2. **Procedure**:
    1. Extract the IP address of the sender from the email header. For example, look for the last "Received" line containing an IP address.
    2. Use a reverse DNS lookup tool, such as MXToolbox, to find the domain name associated with the IP address.
    3. Utilize an IP geolocation tool (e.g., IP Tracker) to map the IP address to its geographic location.
    4. Document the findings, including the sender's approximate location and domain details. For instance, trace an email from "example@phishy.com" to its originating IP and identify its location.
3. **Expected Outcome**:
    - Determine the sender's approximate location, ISP, and domain details.

Exercise 4: Ethical Considerations in Email Monitoring

1. **Objective**:
    - Reflect on the ethical implications of email tracking and tracing.
2. **Procedure**:
    1. Research privacy laws such as GDPR and CCPA.
    2. Identify real-world scenarios where email tracking or tracing might raise ethical concerns. For example, consider the use of tracking in unsolicited marketing emails.
    3. Discuss findings with peers or document them in a report.
    4. Propose guidelines for ethical practices in email monitoring, such as obtaining user consent.
3. **Expected Outcome**:
    - Develop a clear understanding of responsible practices, including when and how tracking should be disclosed.