Bayero University, Kano - Nigeria

B.Sc. in Cyber Security

Computer Forensics Laboratory

CBS3201: Introduction to Digital Forensics Laboratory

LIST OF EXPERIMENTS

No.	Experiment	Page No.
1	Study of various Tools used in Computer Forensics for forensic investigation	
2	Using Forensics Tools to Recover Deleted Files	
3	Study the steps for hiding and extract any text file behind an image file/ Audio file using Command Prompt.	
4	How to make the forensic image of the hard drive using Encase Forensics	
5	Live Forensics Case Investigation using Autopsy	

EXPERIMENT ONE

Aim of the Experiment:

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.

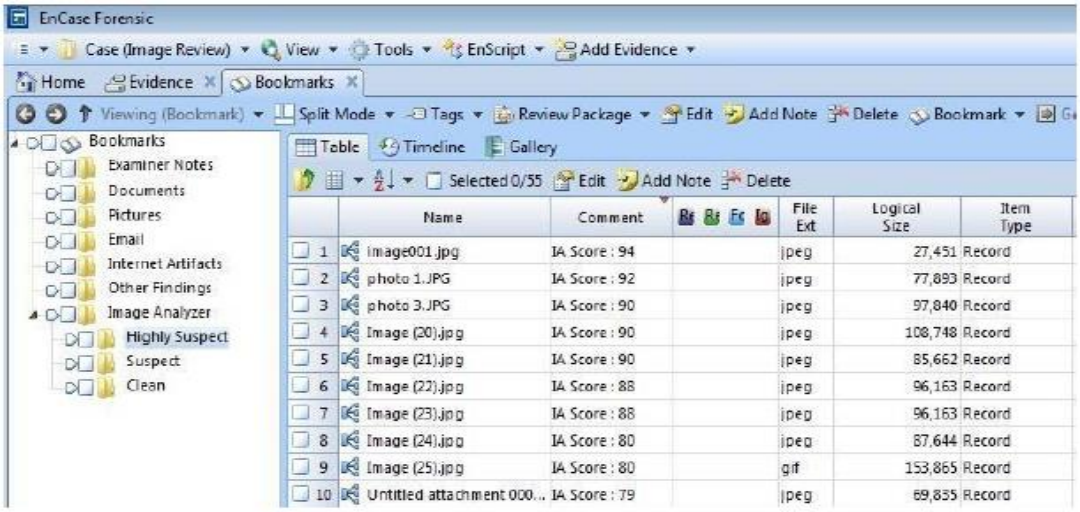
It relies upon the fundamental concept that whenever a digital intrusion or crime is committed, the perpetrator inadvertently leaves a bit of themselves behind for the investigator to find. These "bits" could be entries in log files, changes to the registry, hacking software, malware, remnants of deleted 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
- autopsy
- ptk
- fatback
- driftnet
- truecrypt
- iphoneanalyzer
- exiftool
- scalpel
- timestomp
- hexedit
- rifiuti2
- evtparse.pl
- dc3dd

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 tools

- **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 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**

  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 Honey net 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, and 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 so on.

EXPERIMENT TWO

Aim of the Experiment:

How to Recover Deleted Files using Forensics Tools

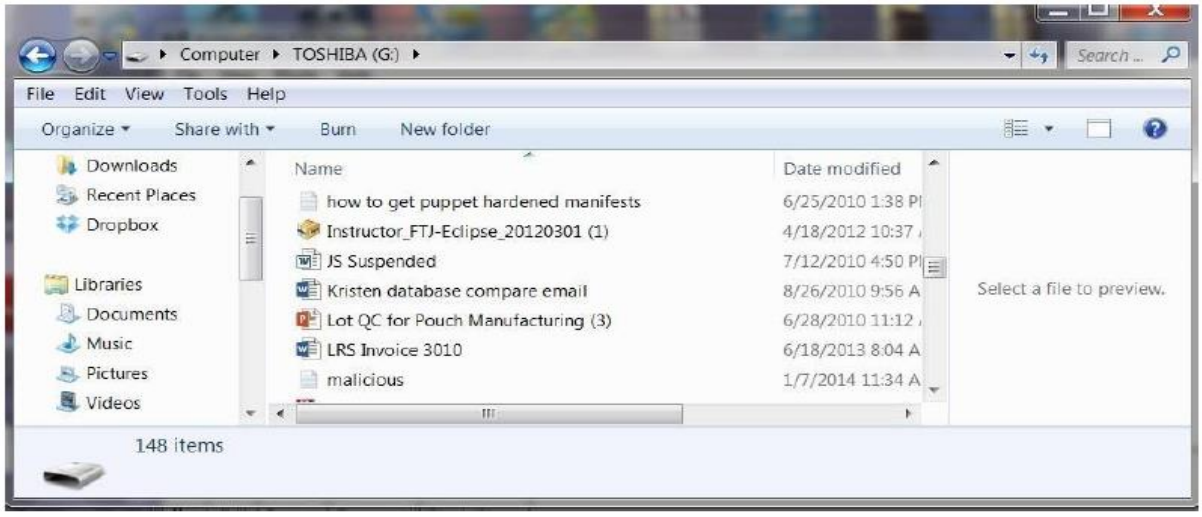
First Step: Create a File

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.

Second Step: 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.

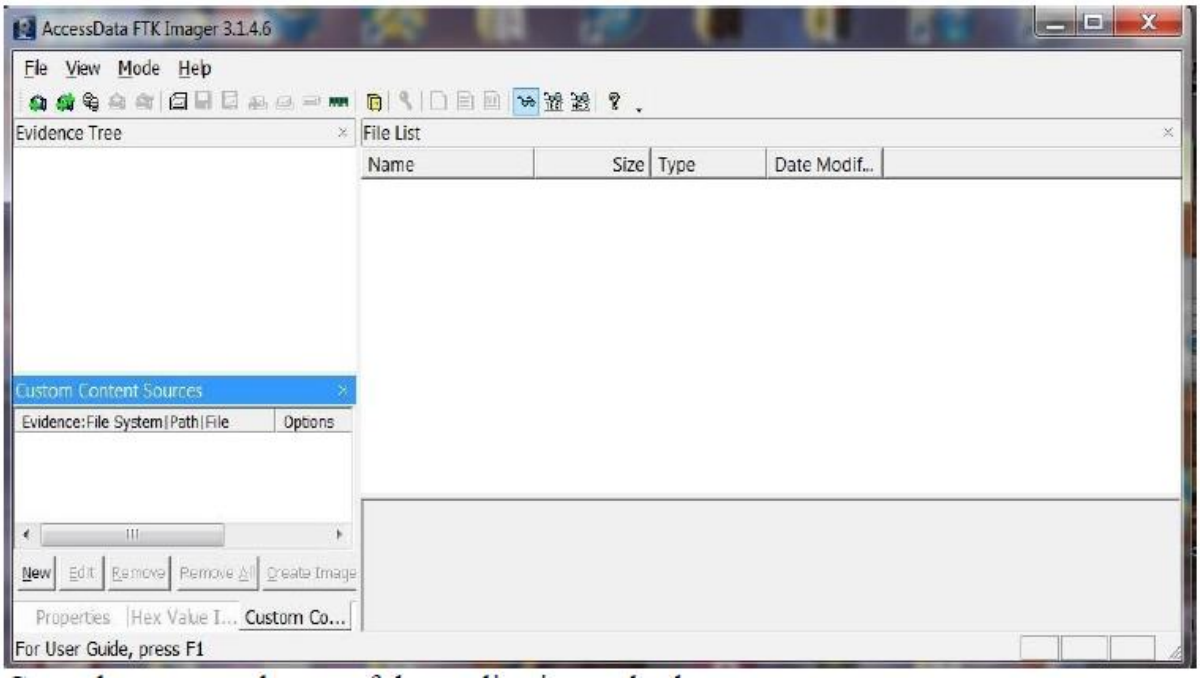
Third Step: Create an Image

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 Back Track). 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.

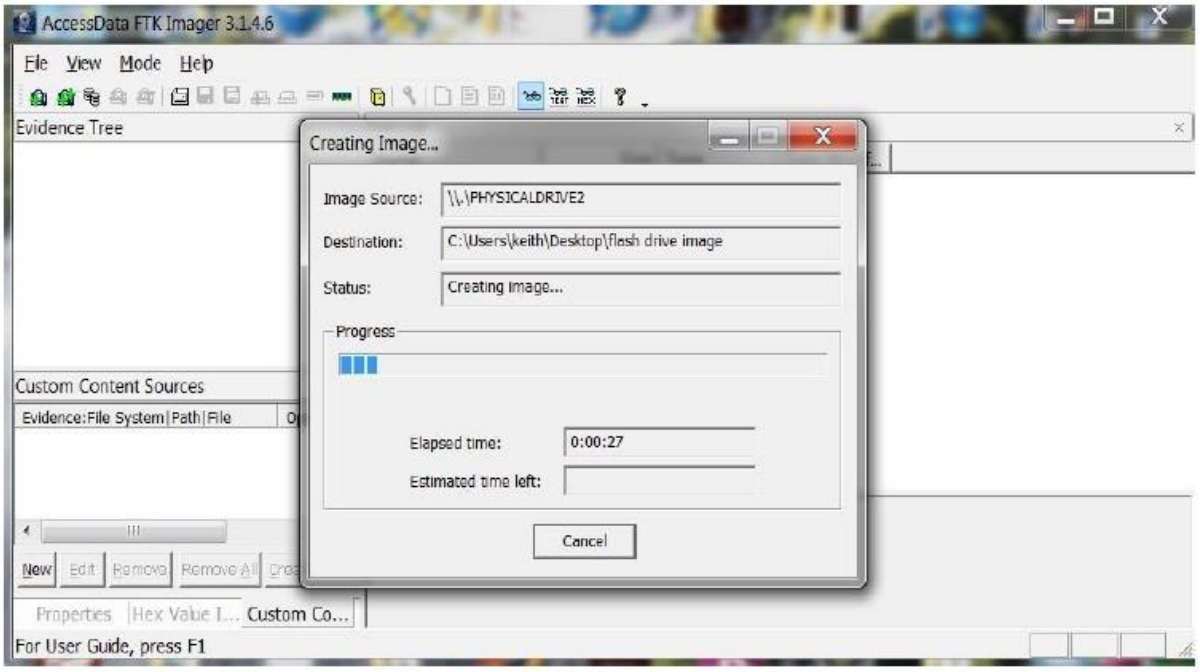
Now that have downloaded the FTK imager, we need to create a bit-by-bit image of the flash drive.



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.

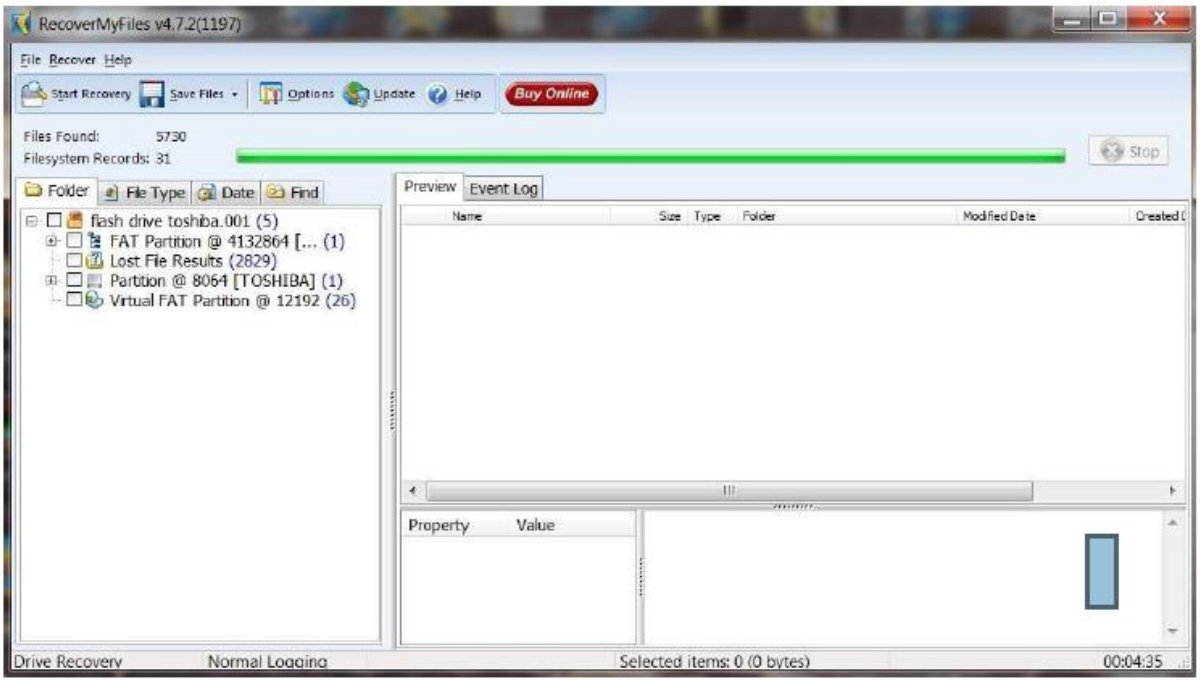
Fourth Step: Recover Deleted Files
There are many tools on the market to recover deleted files and all of them are adequate to do the job. Deleted file recovery is probably the simplest of forensic tasks. Here, I will be using a trial version of RecoverMyFiles.

You can download a trial version.

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

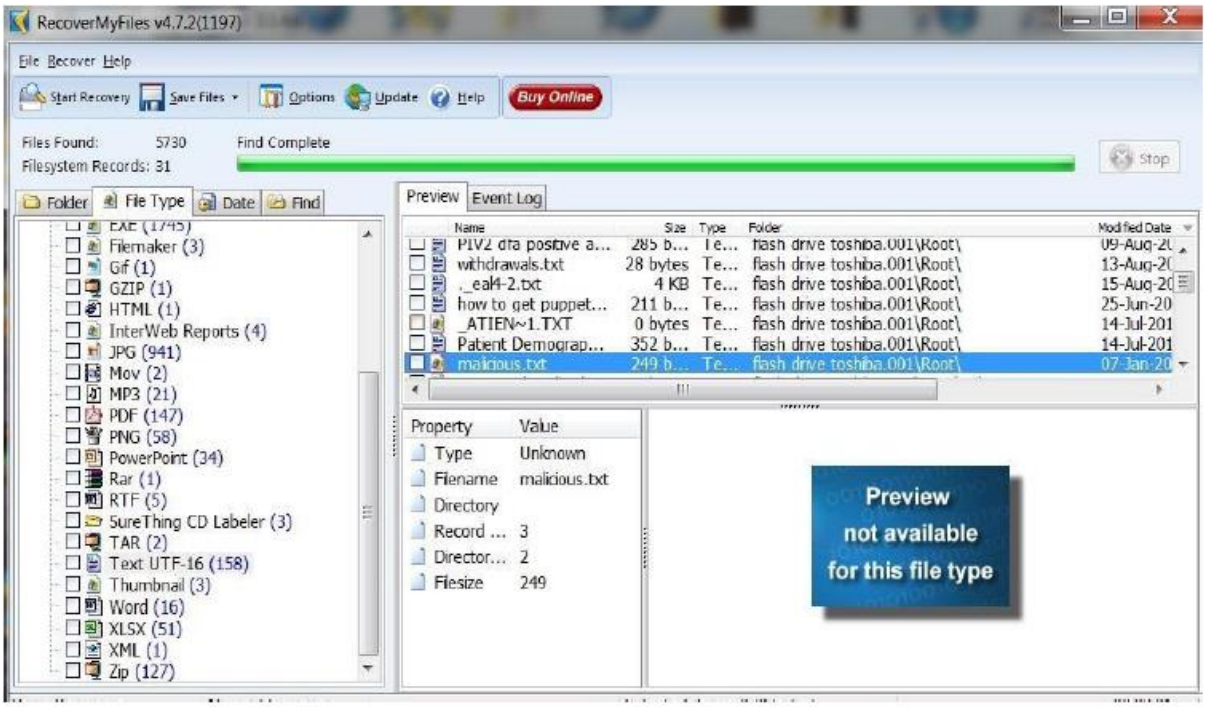
the screenshot below. Since we are using a forensic image, select Add Image button to the right. You will need to provide a path to your image file created with FTK.

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!



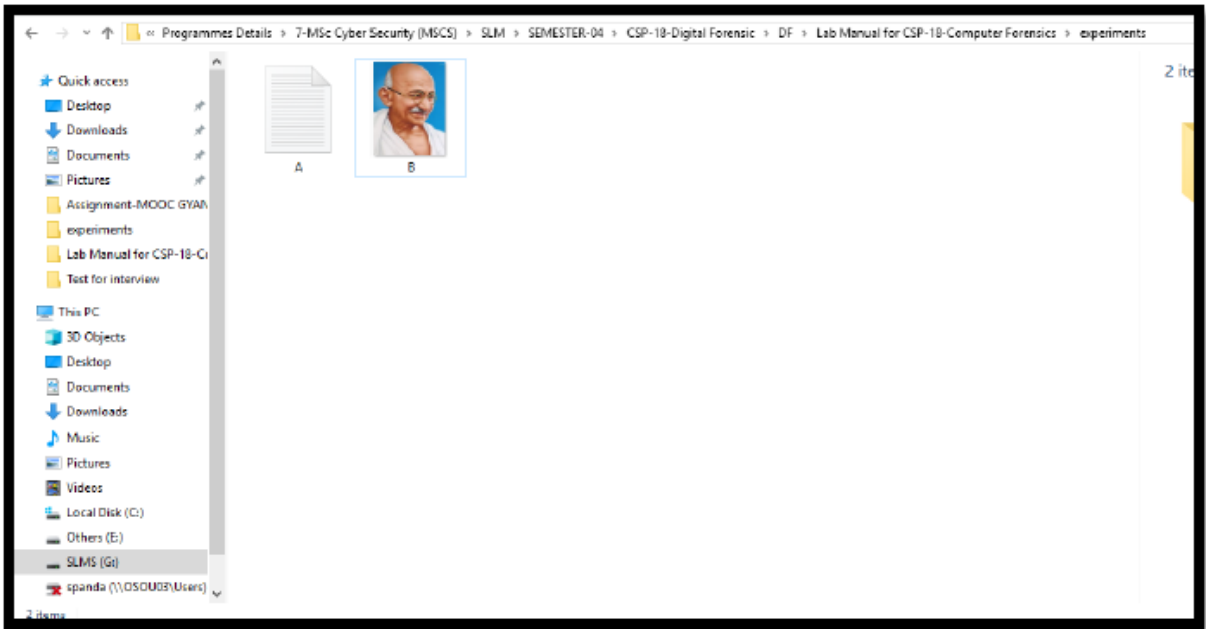
I'm hoping that this tutorial clearly showed you how simple it is for a forensic investigator to recover the files you have deleted. This should be a lesson that you need to be exceedingly cautious and when possible, overwrite any deleted files to remove evidence. In some cases, even that may not be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

EXPERIMENT THREE

Aim of the Experiment:

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:

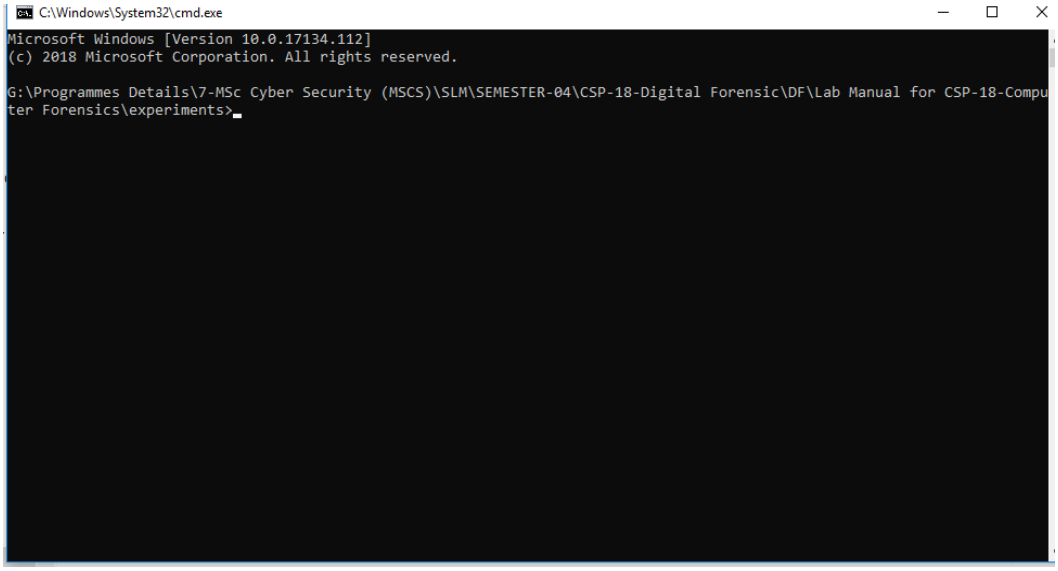
1. Copy the file, you need to hide, to desktop (for our tutorial let us assume the file to be "A.txt")

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:

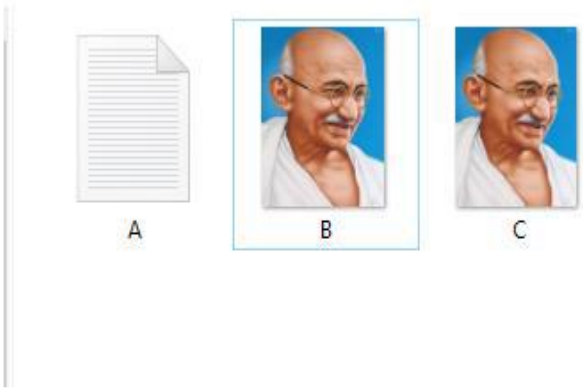
> Copy /b B.jpg + A.txt C.jpg

```
G:\Programmes Details\7-MSc Cyber Security (MSCS)\SLM\SEMESTER-04\CSP-18-Digital Forensic\DF\Lab Manual for CSP-18-Co
ter Forensics\experiments>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*

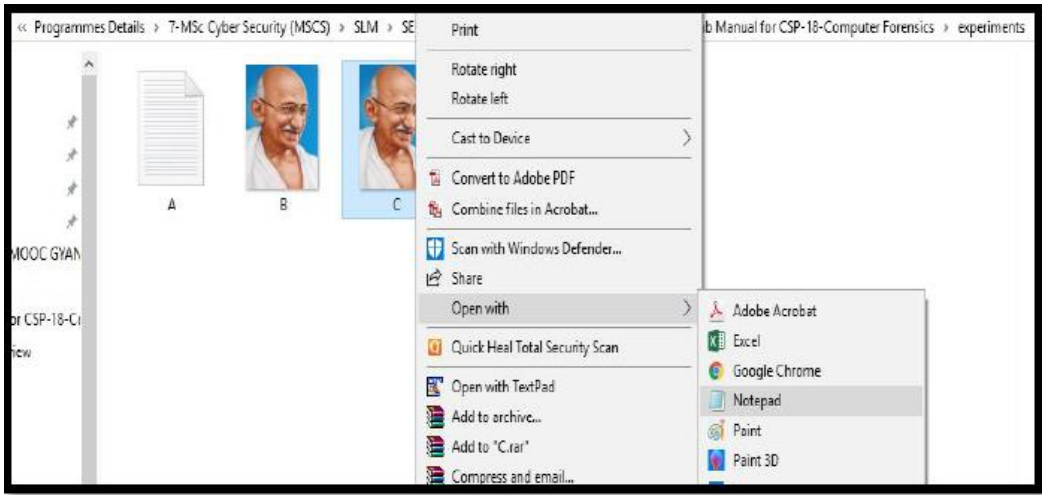
```
G:\Programmes Details\7-MSc Cyber Security (MSCS)\SLM\SEMESTER-04\CSP-18-Digital Forensic\DF\Lab Manual fo
ter Forensics\experiments>copy /b B.jpg + A.txt  C.jpg
B.jpg
A.txt
       1 file(s) copied.

G:\Programmes Details\7-MSc Cyber Security (MSCS)\SLM\SEMESTER-04\CSP-18-Digital Forensic\DF\Lab Manual fo
ter Forensics\experiments>
```

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

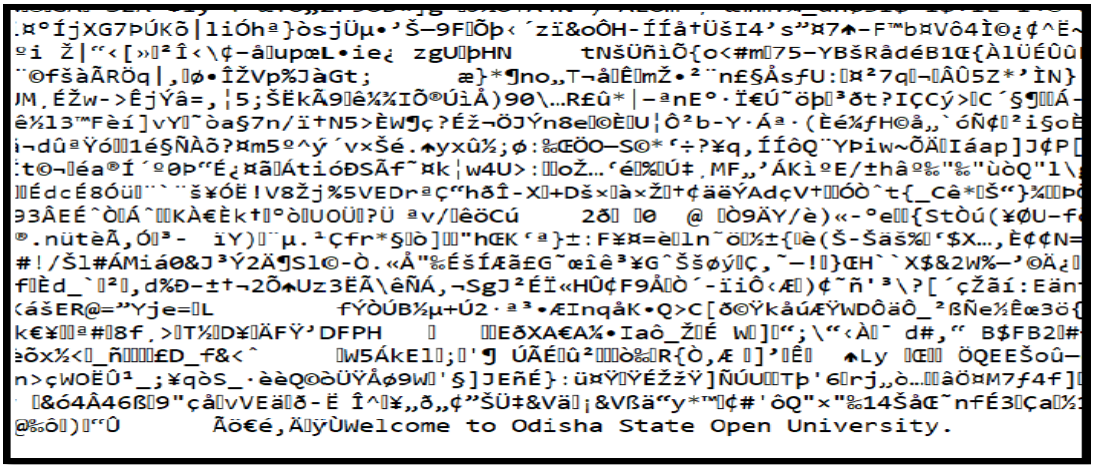


How to retrieve the file?

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



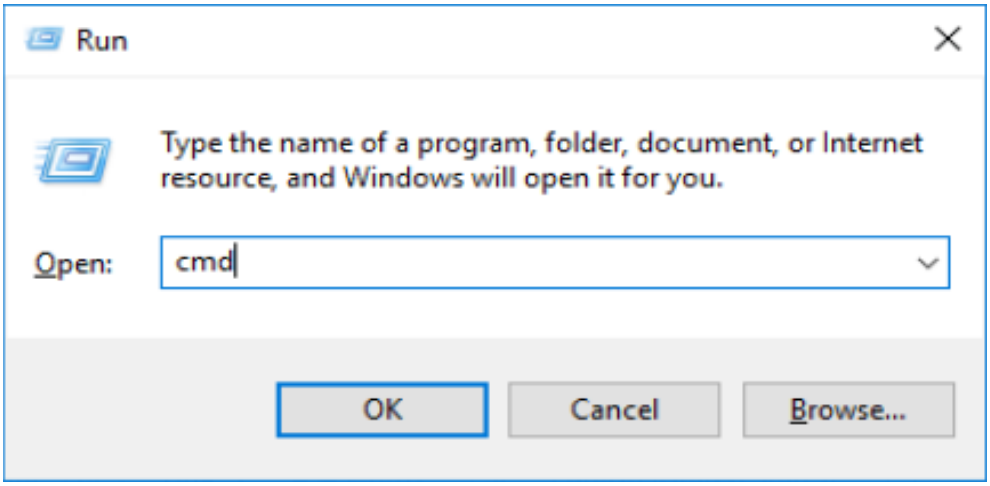
Done! Successfully opened! In the last of the notepad, you'll find the content of the text file.



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**

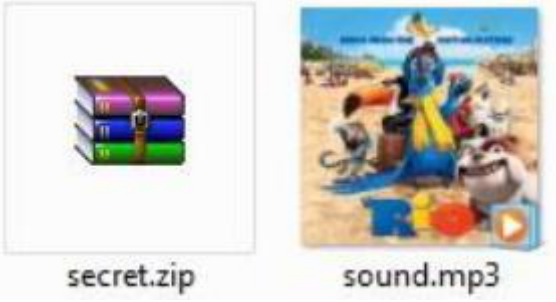


3. Enter the directory where you have your files.
4. Then type the command:
>> Copy /b B.jpg + A.rar C.jpg
Here a.rar is the file to hide behind the image file (b.jpg) and the output file is **c.jpg**.

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:

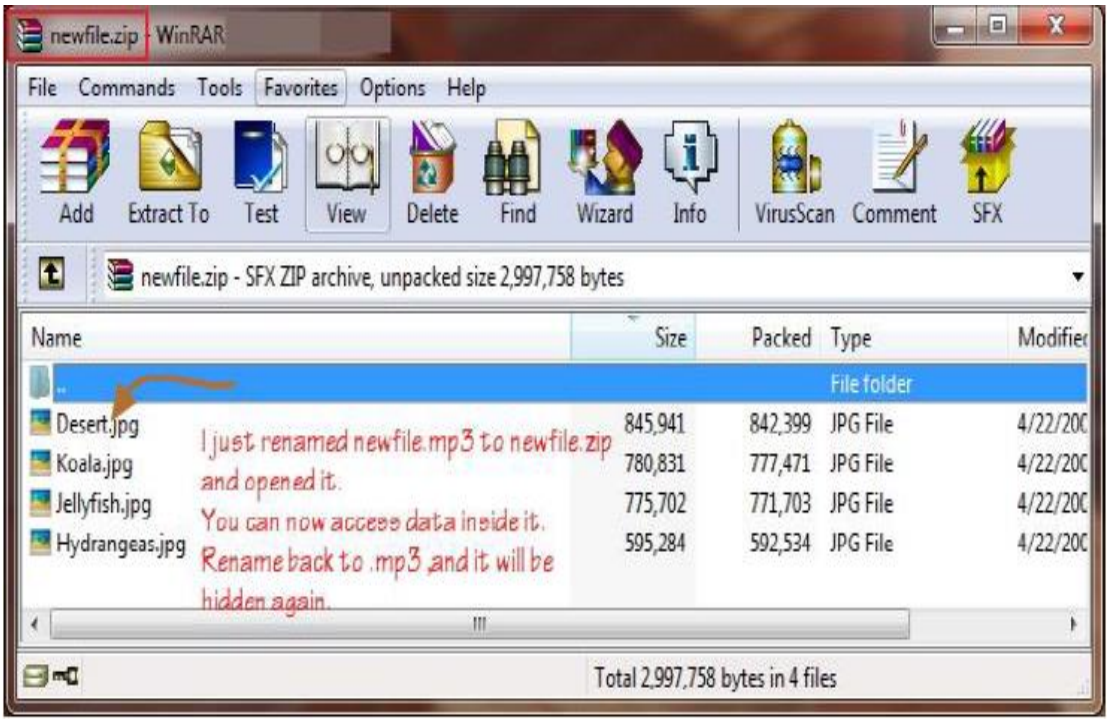
Copy /b secret.zip + sound.mp3 newfile.mp3

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.



EXPERIMENT FOUR

Aim of the Experiment:

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

2. Introduction

In solving computer crime cases, computer forensics is used to gather evidence, which will be analysed 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."

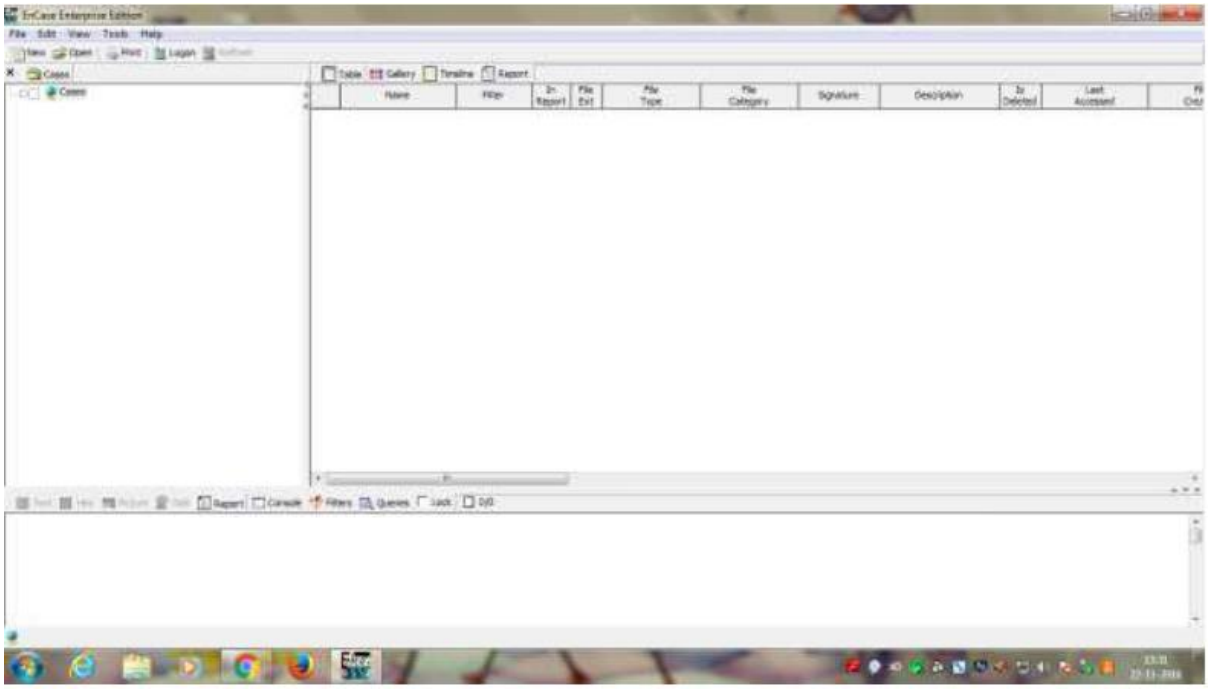
Disk imaging is also one of the approaches for backup except that backup only copies the active file. In backup, ambient data will not be copied. This is an area where the most important source for the evidence could be found. Ambient data is a data stored in Windows swap file, unallocated space and 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.

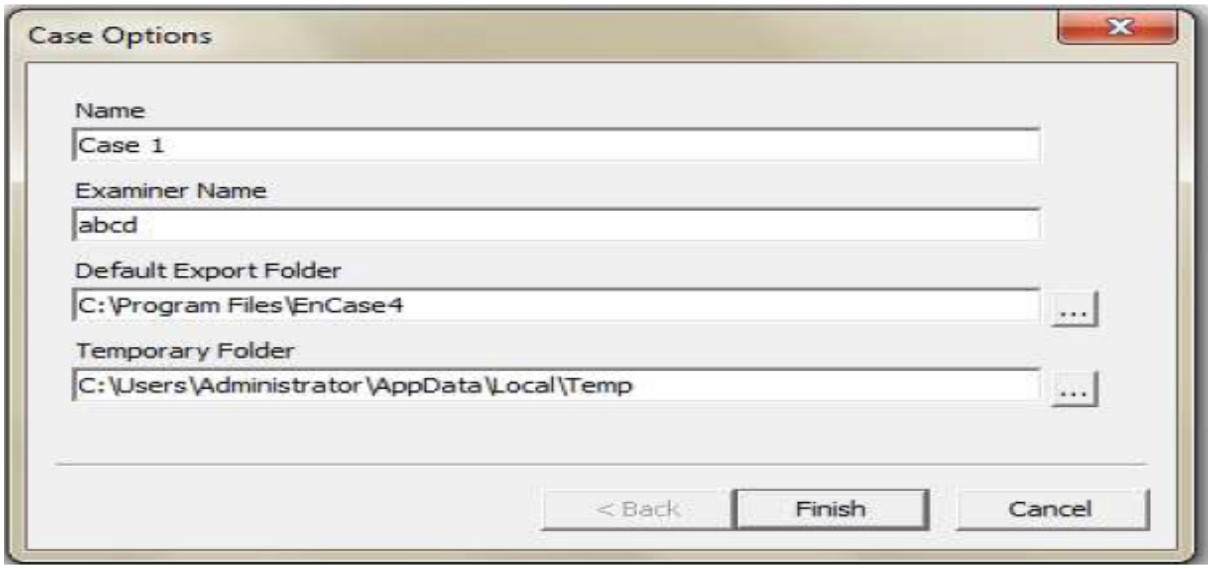
Since it is never advised to work with the original evidence because we may lose some relevant data accidentally, so we will create an image of the original

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 One:
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.

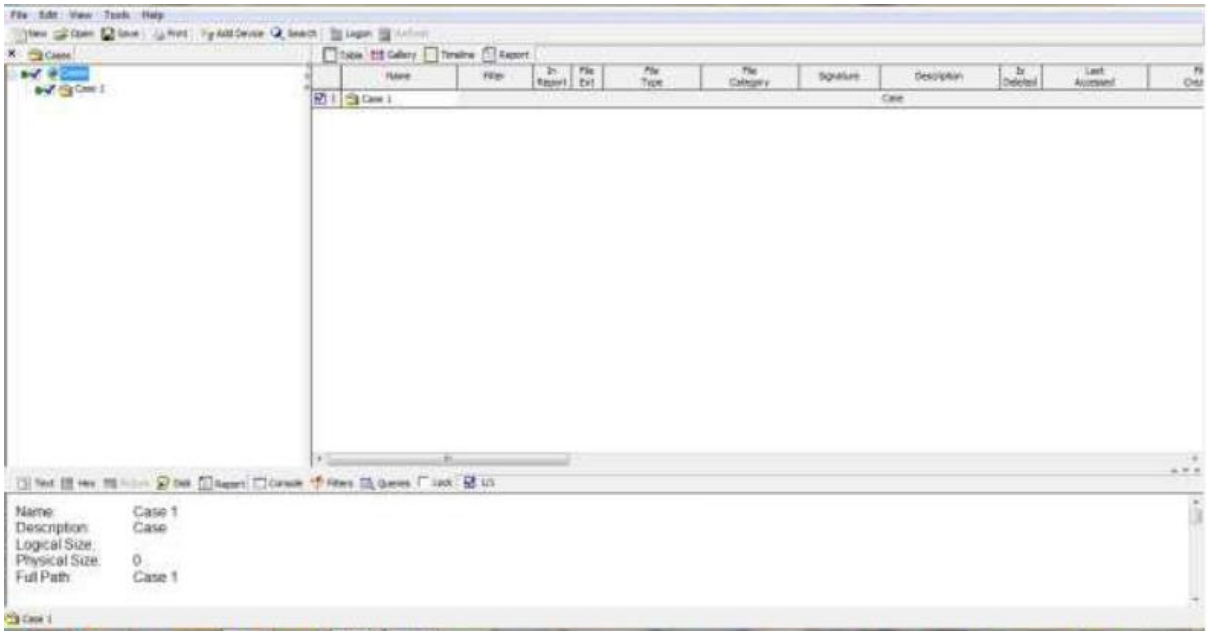


Step Two: Click On New For Creating A New Case. Fill the labels.

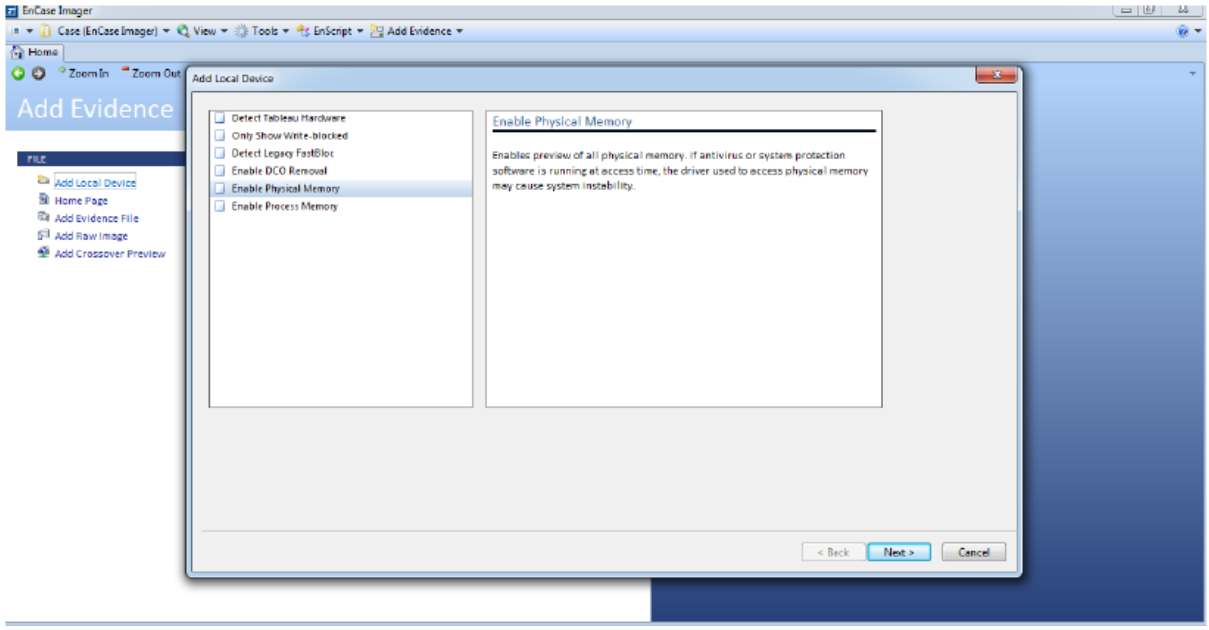


Click On **Finish.**

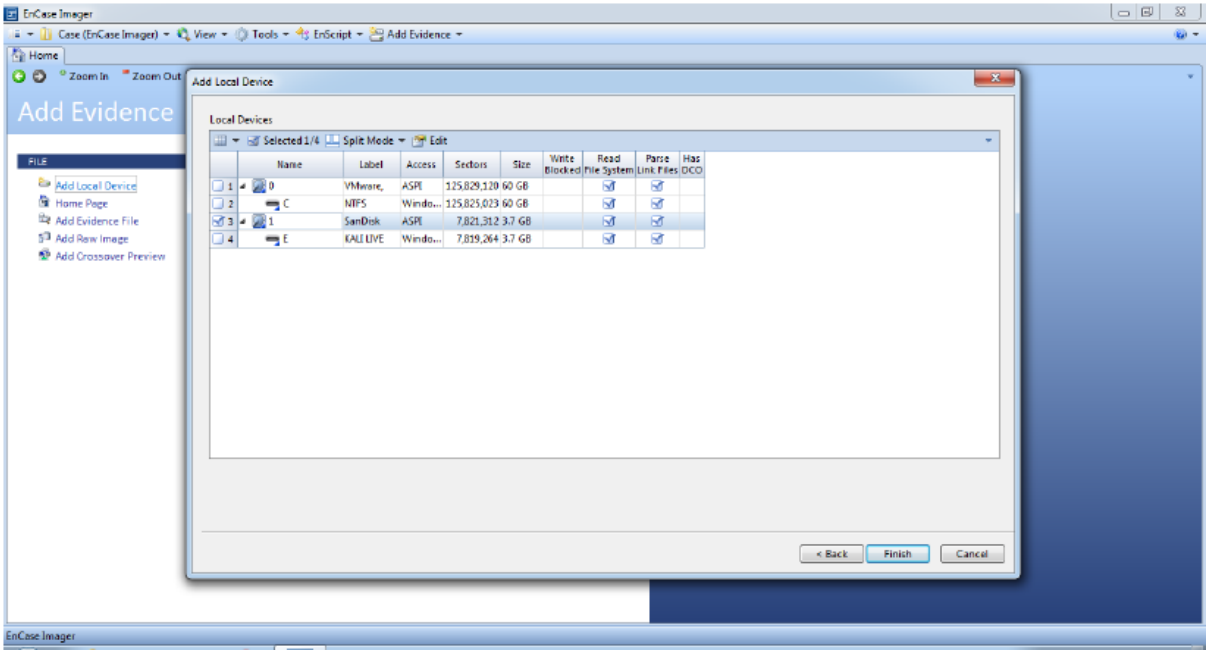
Step Three: View the Case by Clicking On Case 1 <Case Name>



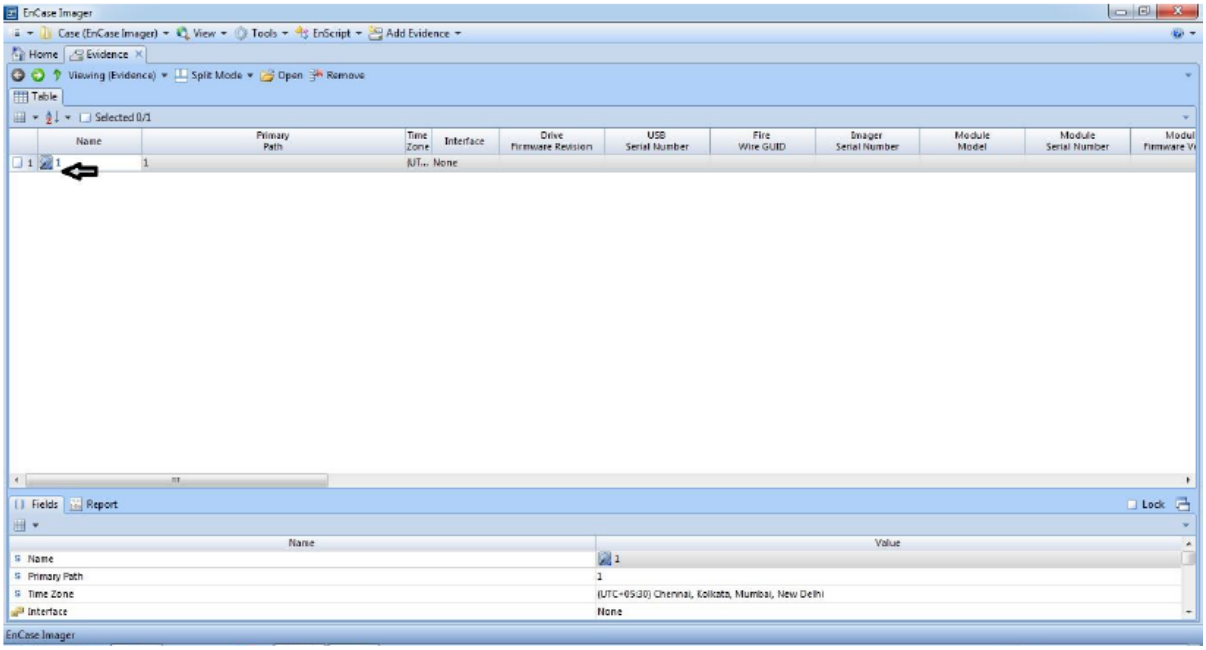
Step Four: Click on add local device for Adding Devices to Your Case. If there is any write blocker attached with the machine and digital deice then tick to 1, 2 and 5 option otherwise untick to all and click on **Next button**.

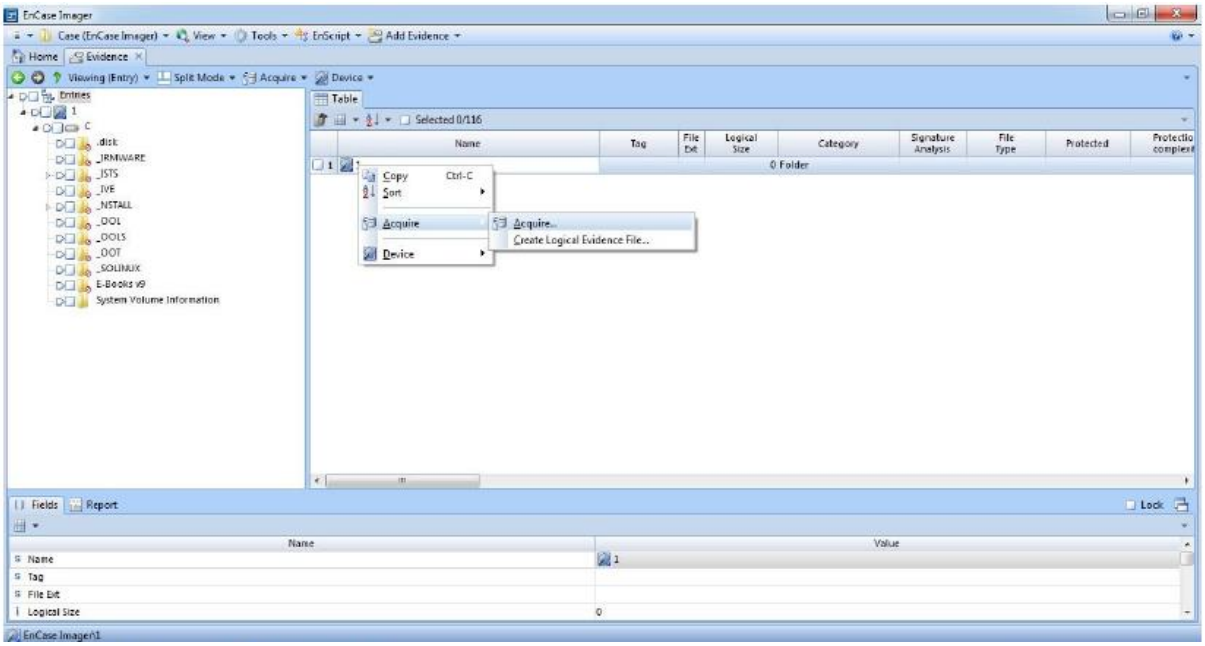


Step Five: Tick in the box of name column which shows the connected device name or label like (1, 2, 3 or any numeric number) and click on the **finish button**.

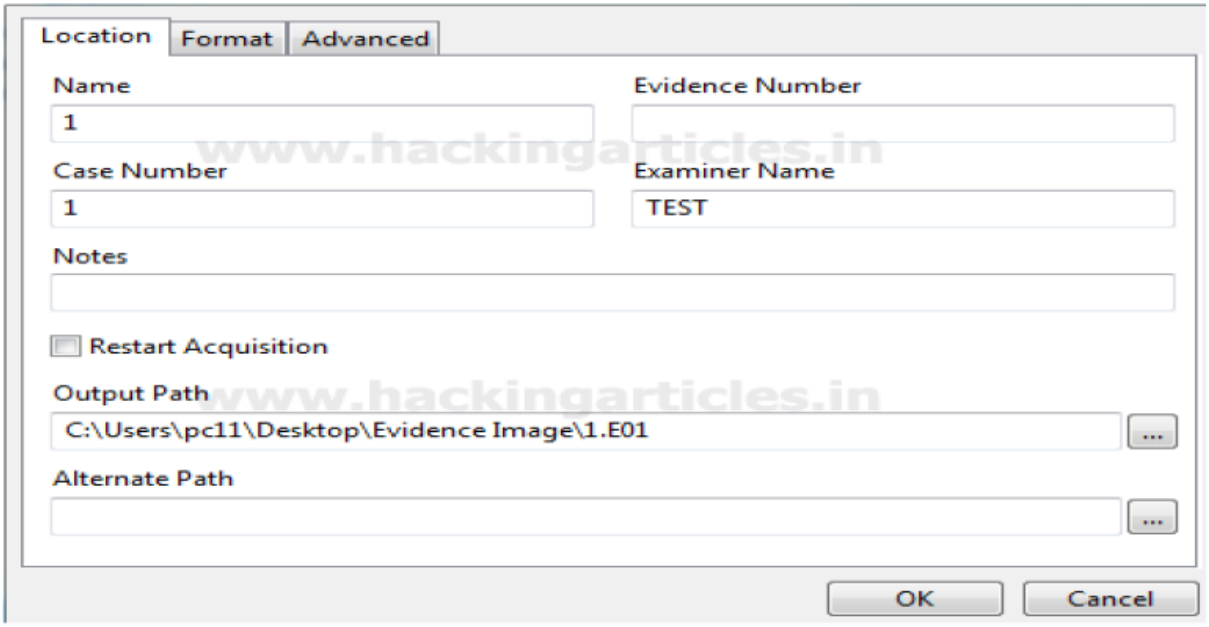


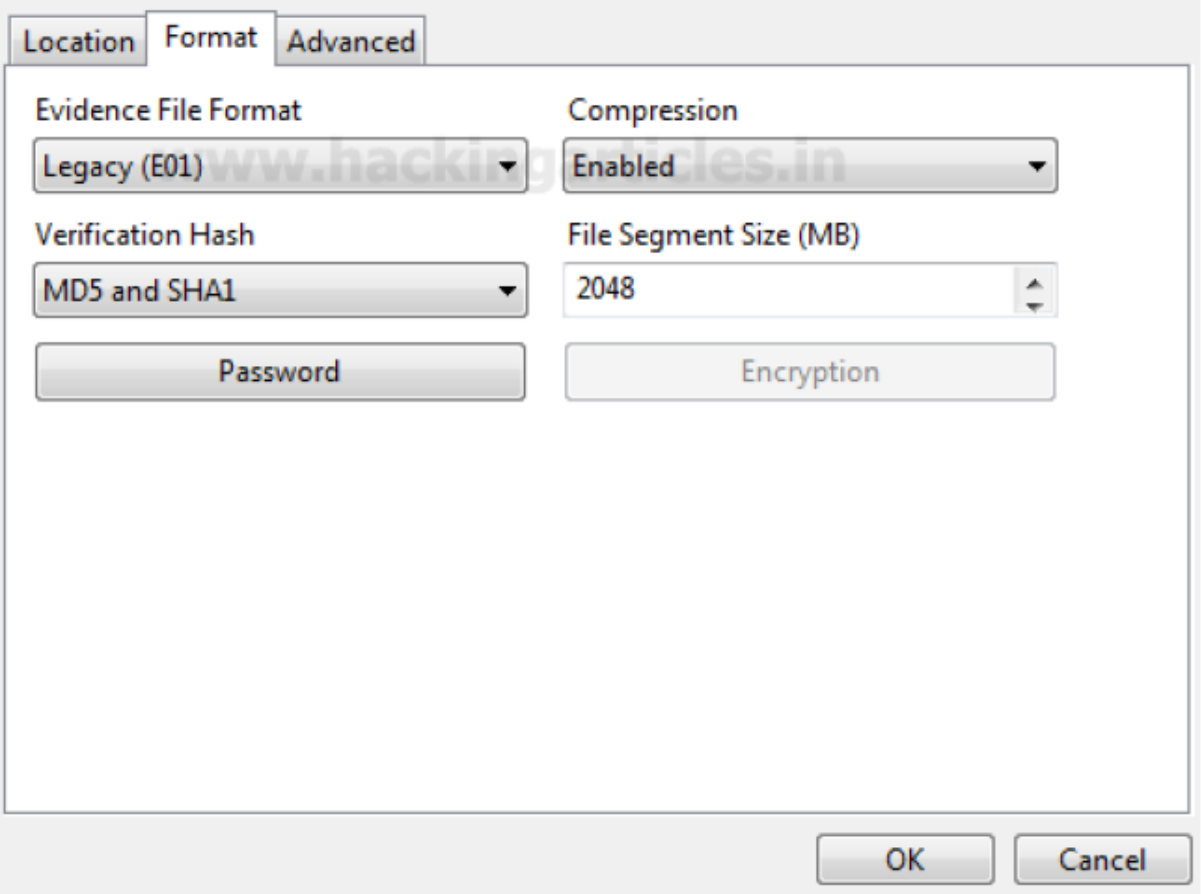
Step Six: Now to open evidence click on label number of the device which shows in “name” column and again right-click on label number and choose **acquire the option**.



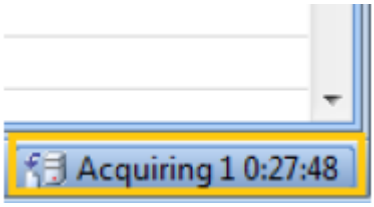


Step Seven: Then a pop up will appear with three tabs. In the **location tab**, fills all the fields. In **format tab** if you want to encrypt the evidence file then enable the Compression field otherwise disable it. In Verification Hash field value should be chosen MD5 and SHA1 after it click on **OK 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 Eight: 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 Nine: 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).

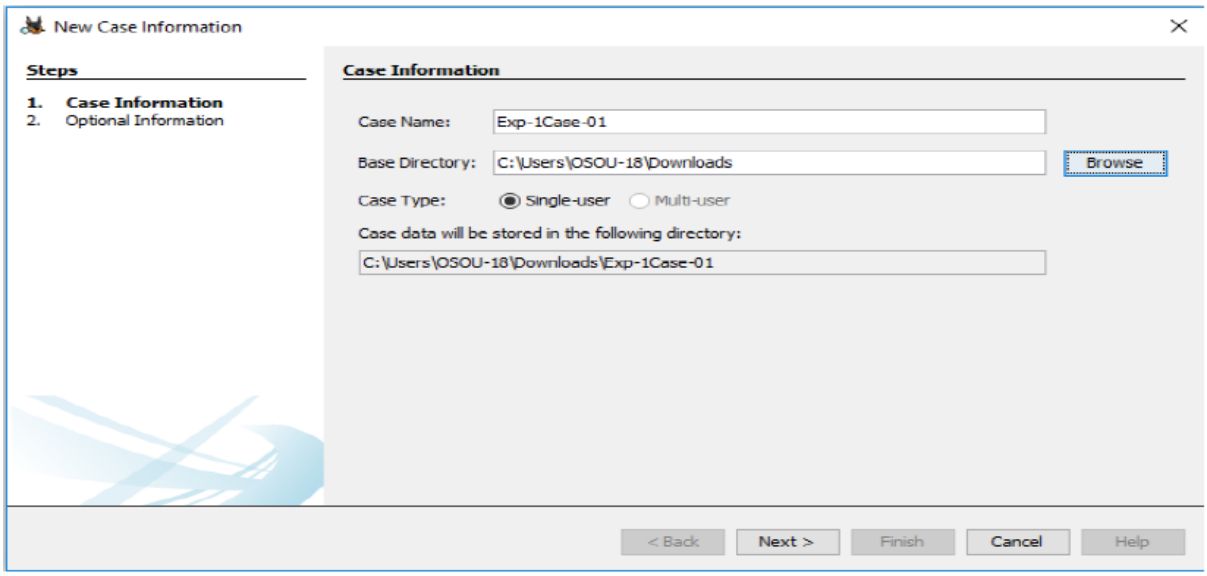
EXPERIMENT FIVE

Aim of the Experiment:

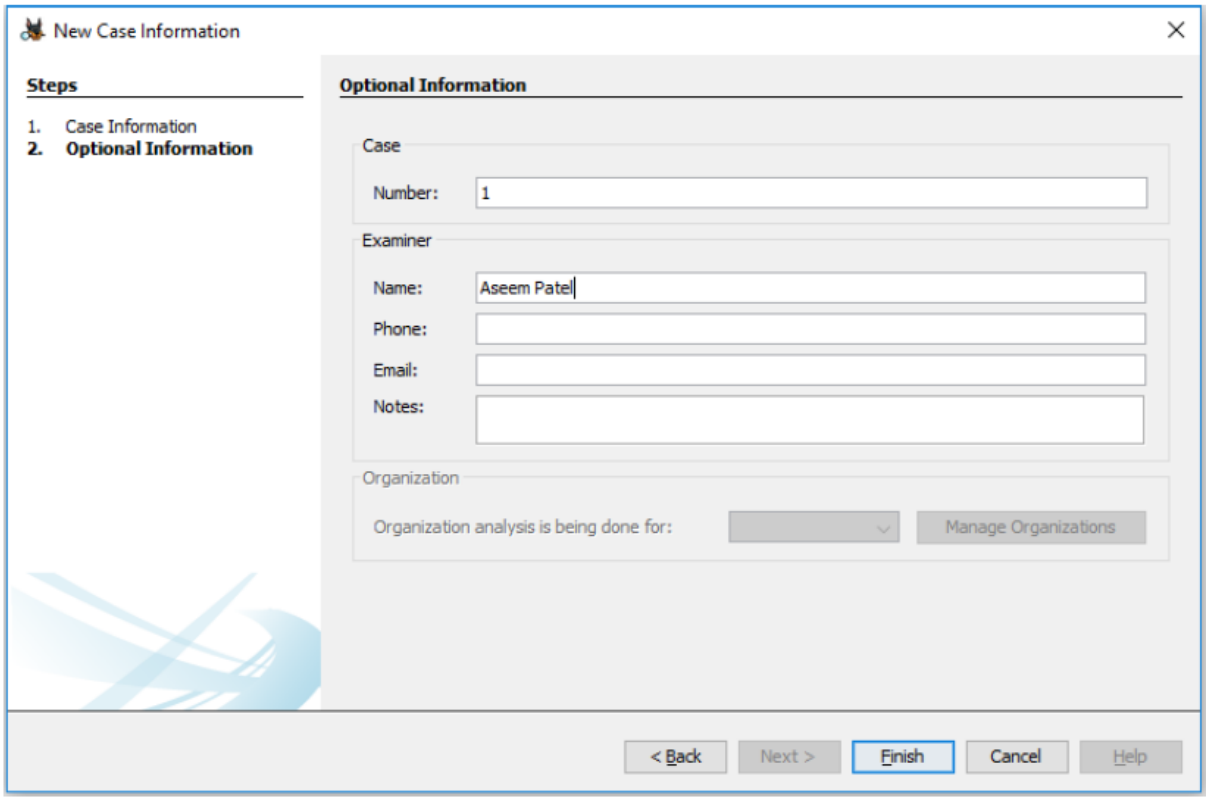
Live Forensics Case Investigation using Autopsy

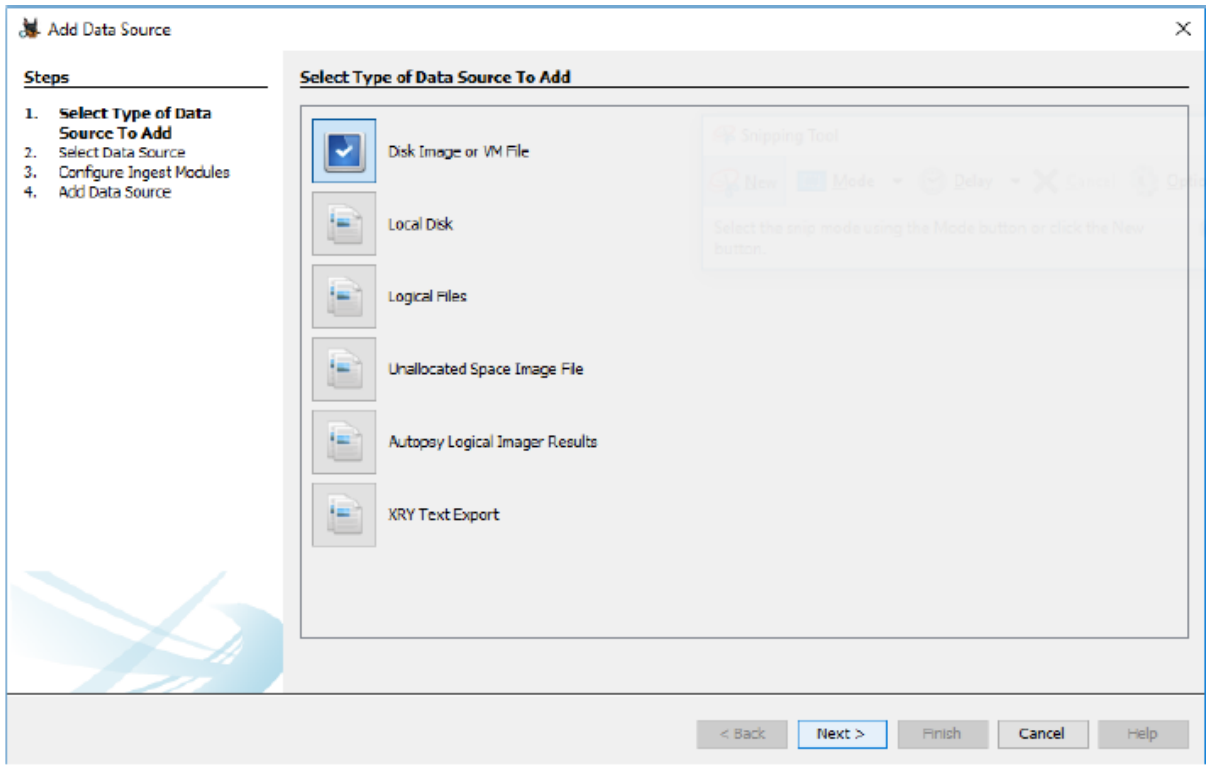
First Download autopsy from here and install in your pc. Click '**New Case**' option.

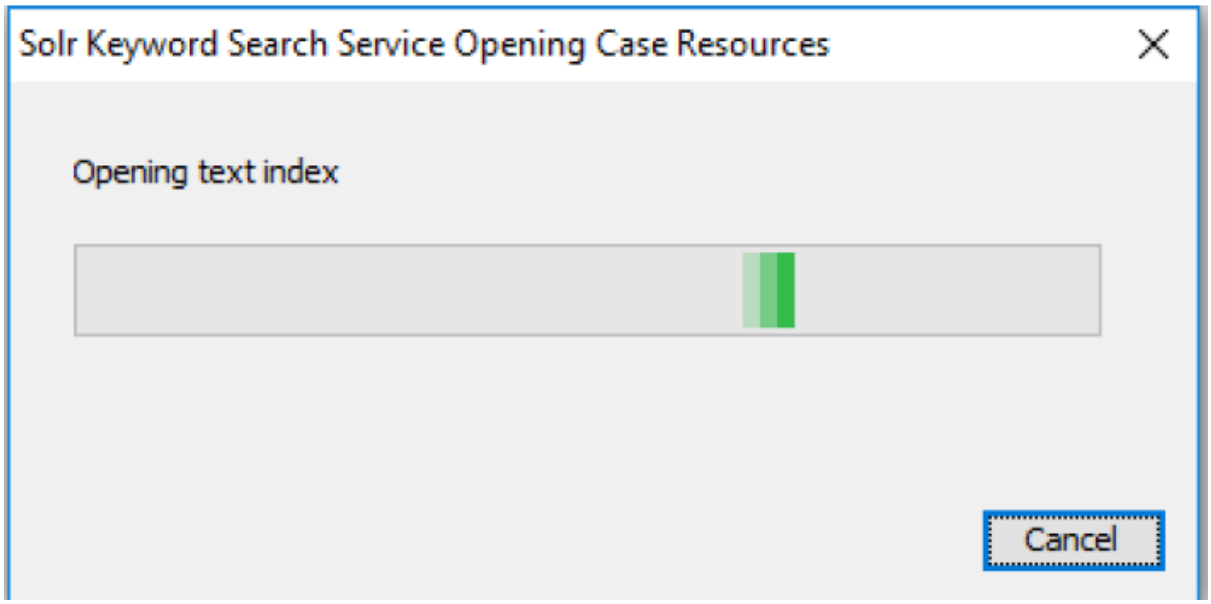
A new page will open. Enter the details in **'Case Name'** and **'Base Directory'** and choose the location to save the report e.g.: Autoreport. Then click on next to proceed to the next step.



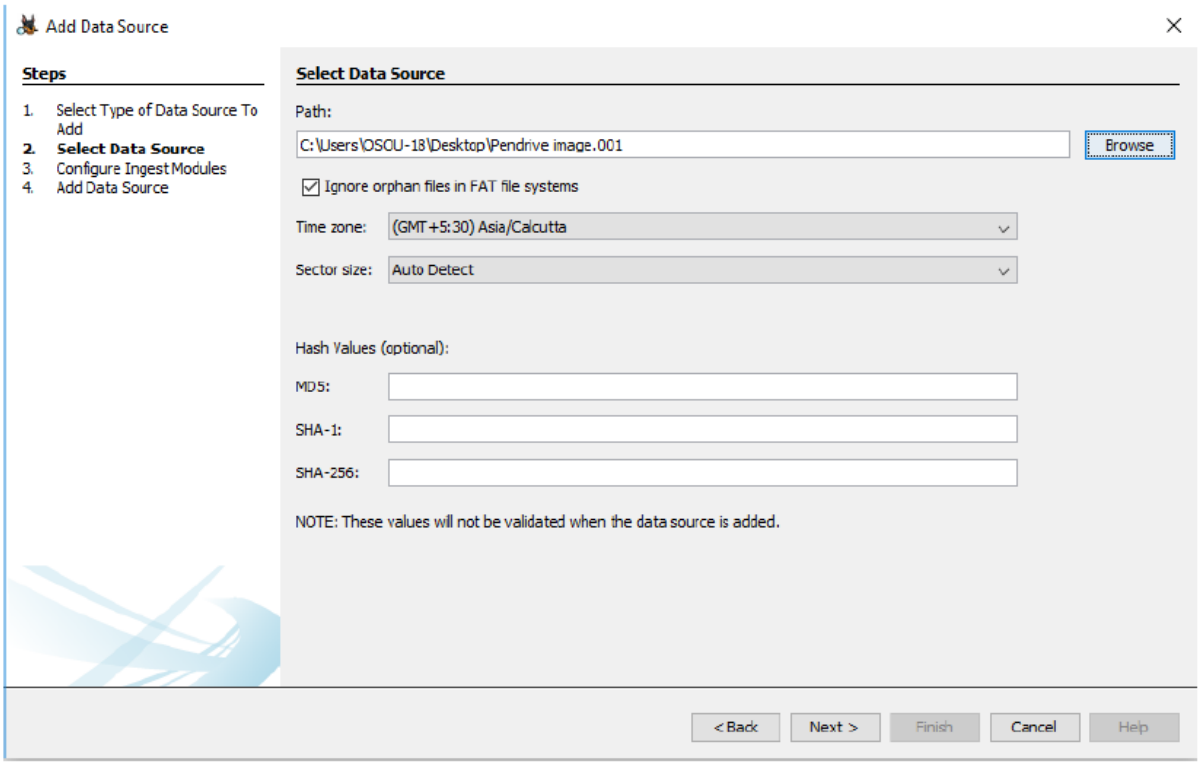
Here in the next step, you have to enter the case number and Examiner details and click on finish to proceed to the next step.


New Case Information
Steps
1. Case Information
2. Optional Information
Optional Information
Case
Number: 1
Examiner
Name: Aseem Patel
Phone:
Email:
Notes:
Organization
Organization analysis is being done for:
Manage Organizations
< Back
Next >
Finish
Cancel
Help

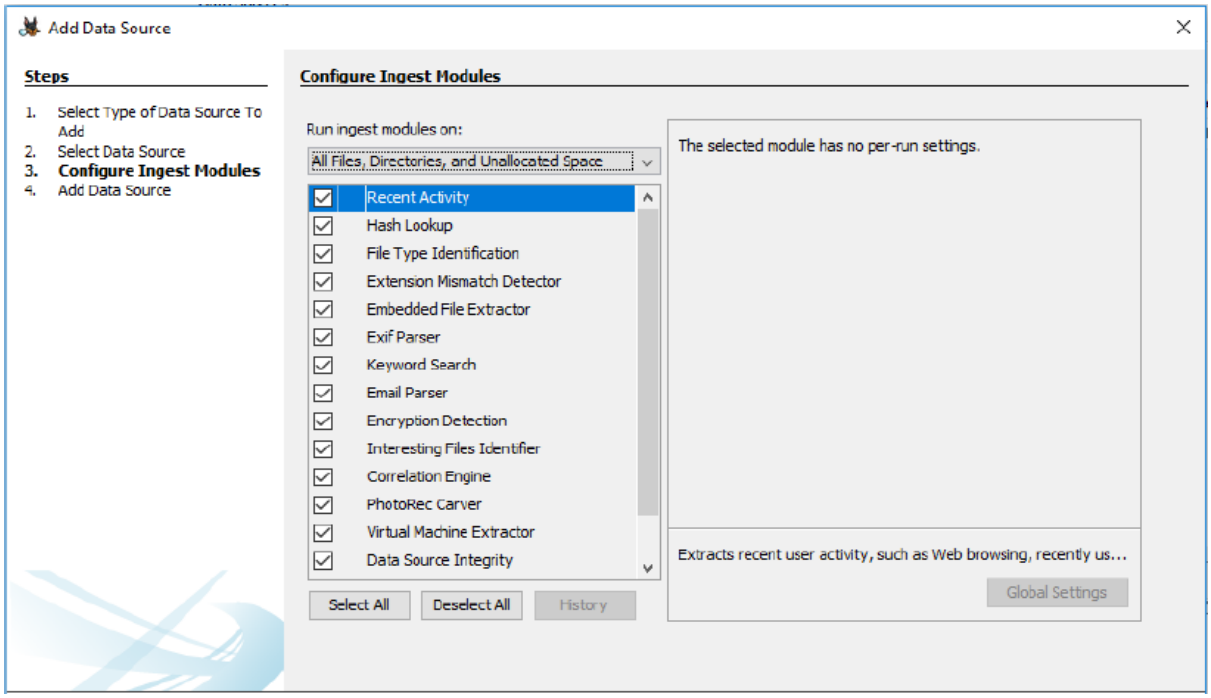

Add Data Source
Steps
1. Select Type of Data Source To Add
2. Select Data Source
3. Configure Ingest Modules
4. Add Data Source
Select Type of Data Source To Add
Disk Image or VM File
Local Disk
Logical Files
Unallocated Space Image File
Autopsy Logical Imager Results
XRY Text Export
< Back
Next >
Finish
Cancel
Help



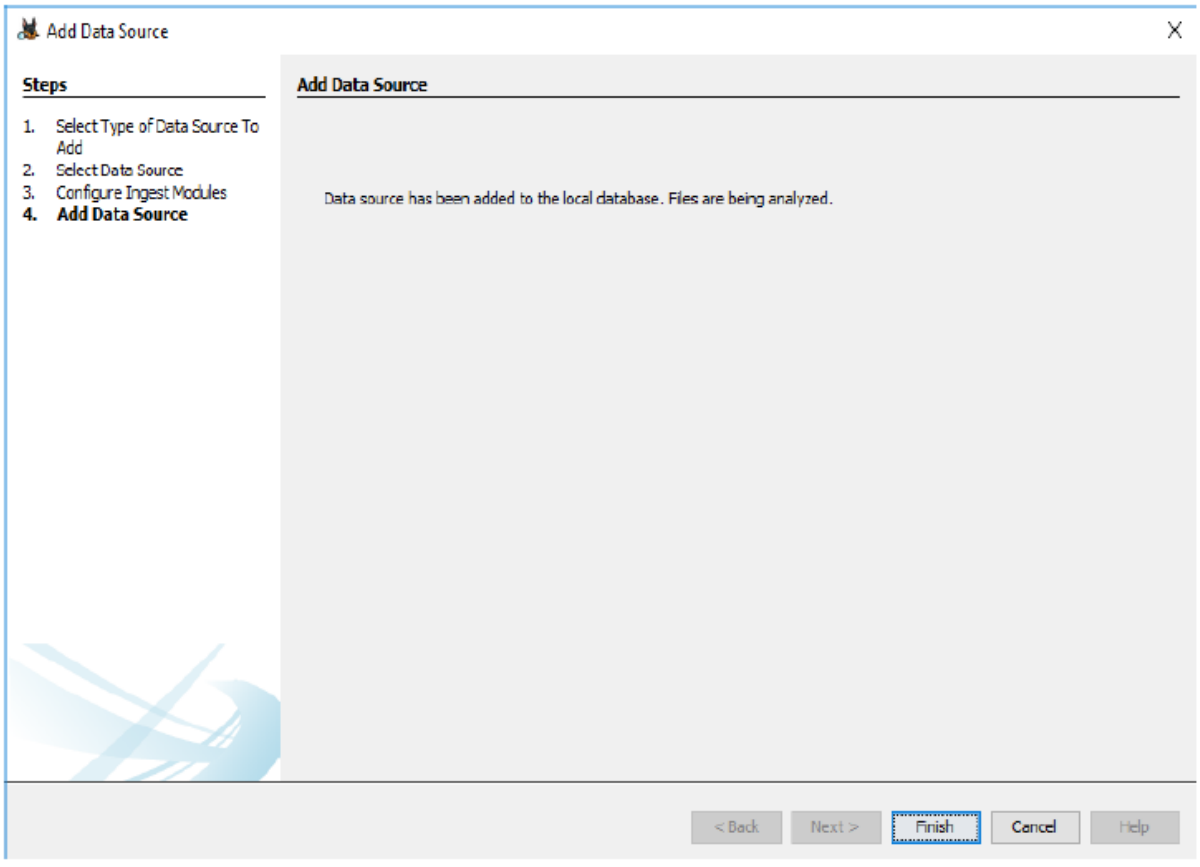
A new window will open. It will ask for the add data source in **Step One**. Select source type to add & browse the file Path and click on NEXT option to proceed further.



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.

References

1. https://www.noxcivis.com/forensics/
2. https://null-byte.wonderhowto.com/how-to/hack-like-pro-digital-forensics-for-aspiring-hacker-part-3-recovering-deleted-files-0149868/