



ଓଡ଼ିଶା ରାଜ୍ୟ ମୁକ୍ତ ବିଶ୍ୱବିଦ୍ୟାଳୟ, ସମ୍ବଲପୁର, ଓଡ଼ିଶା  
**Odisha State Open University, Sambalpur, Odisha**  
Established by an Act of Government of Odisha.

## **M.Sc. in Cyber Security** **(MSCS)**

### **CSPL-18: Computer Forensics Laboratory**

#### **LAB MANUAL**

##### **Course Writers**

**Aseem Kumar Patel**

Academic Consultant

Odisha State Open University, Sambalpur

---

#### **Material Production**

**Dr. Manas Ranjan Pujari**

Registrar

Odisha State Open University, Sambalpur



(CC) OSOU, 2020. *Promoting Use and Contribution of Open Education Resources* is made available under a Creative Commons Attribution- ShareAlike4.0

<http://creativecommons.org/licences/by-sa/4.0>

# **CSPL-18 Computer Forensics Laboratory**

## **LIST OF EXPERIMENTS**

<b>S.L. No.</b>	<b>Experiment</b>	<b>Page No.</b>
<b>1</b>	<b>Study of Computer Forensics and different tools used for forensic investigation</b>	<b>02</b>
<b>2</b>	<b>How to Recover Deleted Files using Forensics Tools</b>	<b>07</b>
<b>3</b>	<b>Study the steps for hiding and extract any text file behind an image file/ Audio file using Command Prompt.</b>	<b>12</b>
<b>4</b>	<b>How to Extract Exchangeable image file format (EXIF) Data from Image Files using Exifreader Software</b>	<b>17</b>
<b>5</b>	<b>How to make the forensic image of the hard drive using EnCase Forensics.</b>	<b>19</b>
<b>6</b>	<b>How to Restoring the Evidence Image using EnCase Forensics</b>	<b>25</b>
<b>7</b>	<b>How to Collect Email Evidence in Victim PC</b>	<b>28</b>
<b>8</b>	<b>How to Extracting Browser Artifacts</b>	<b>31</b>
<b>9</b>	<b>How to View Last Activity of Your PC</b>	<b>33</b>
<b>10</b>	<b>Find Last Connected USB on your system (USB Forensics)</b>	<b>34</b>
<b>11</b>	<b>Comparison of two Files for forensics investigation by Compare IT software</b>	<b>35</b>
<b>12</b>	<b>Live Forensics Case Investigation using Autopsy</b>	<b>37</b>

---

# EXPERIMENT-01

---

## 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.

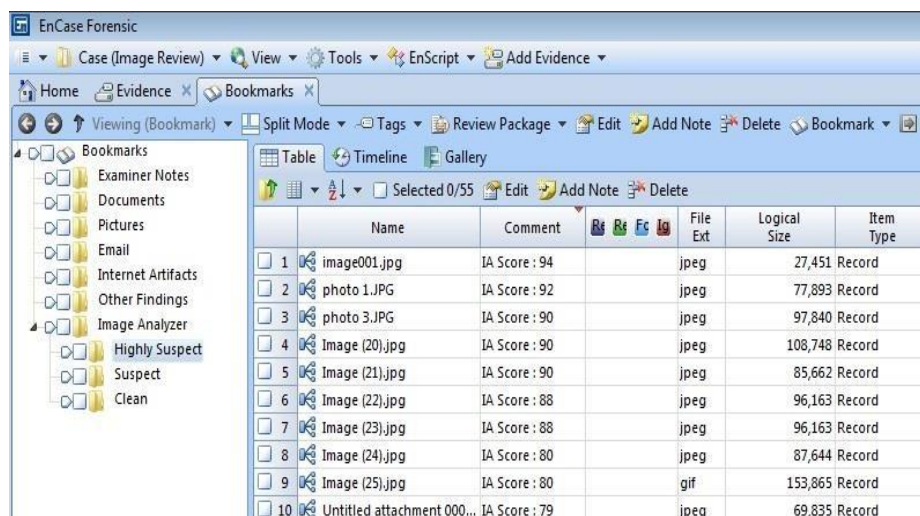
It relies upon the fundamental concept that whenever a digital intrusion or crime is committed, the perpetrator inadvertently leaves a bit of themselves behind for the investigator to find. These "bits" could be entries in log files, changes to the registry, hacking software, malware, remnants of deleted 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
- 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's 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 so on.

---

## EXPERIMENT-02

---

### Aim of the Experiment:

How to Recover Deleted Files using Forensics Tools

#### Step-01: Create a File

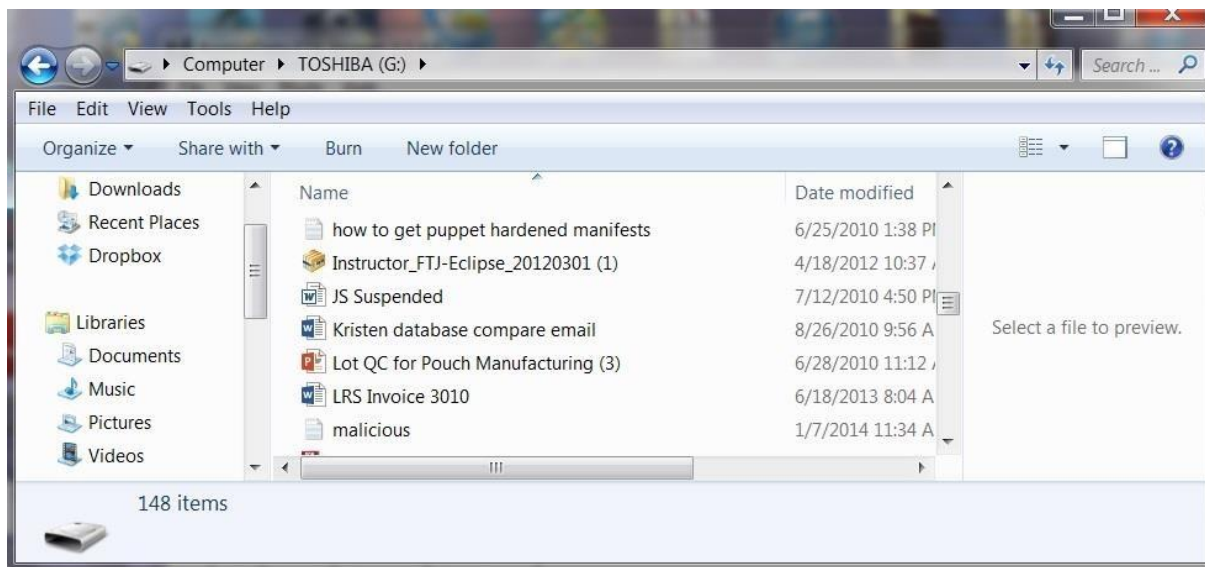
To demonstrate how to recover deleted files, let's create a malicious document. We will call this document "Malicious" and create it with Notepad in Windows.



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

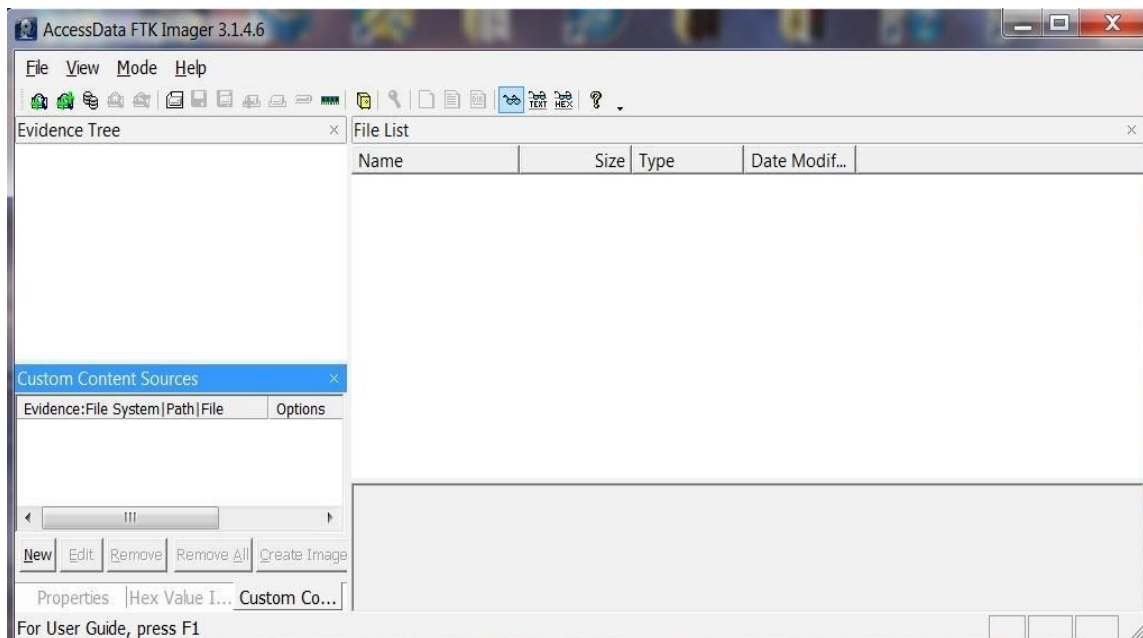
The first step a forensic investigator will do when examining your computer is to make a bit-by-bit copy of your hard drive or in this case your flash drive. There are numerous tools that can do this and in Linux, we have the dd command that does an excellent job of making bit-by-bit copies (it's on 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.



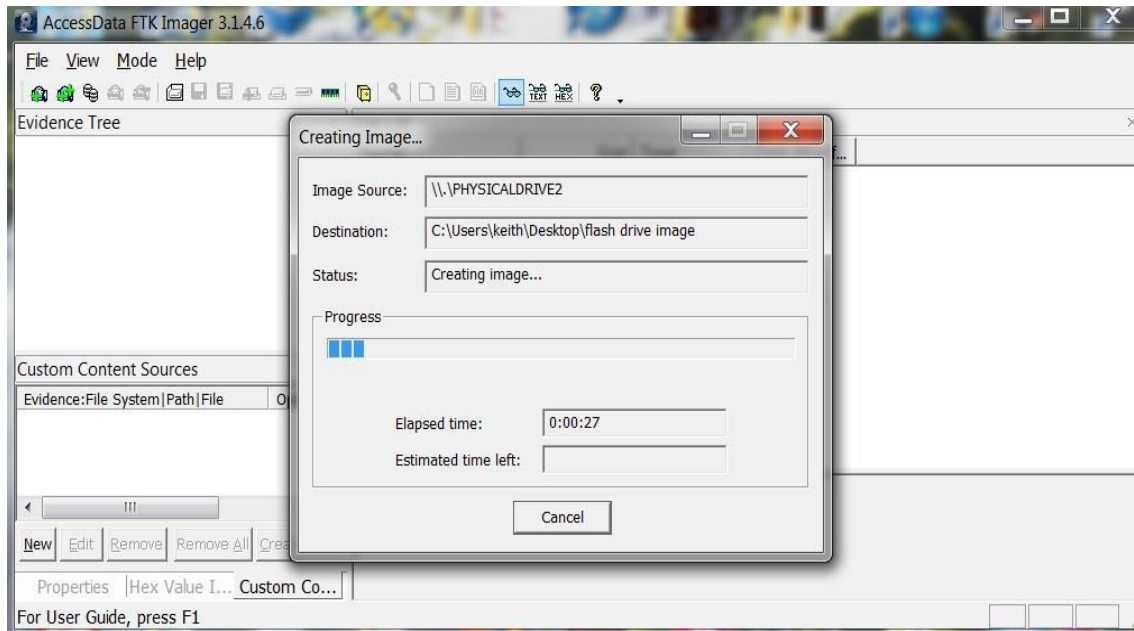
Go to the menu at the top of the application and select:

- **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.



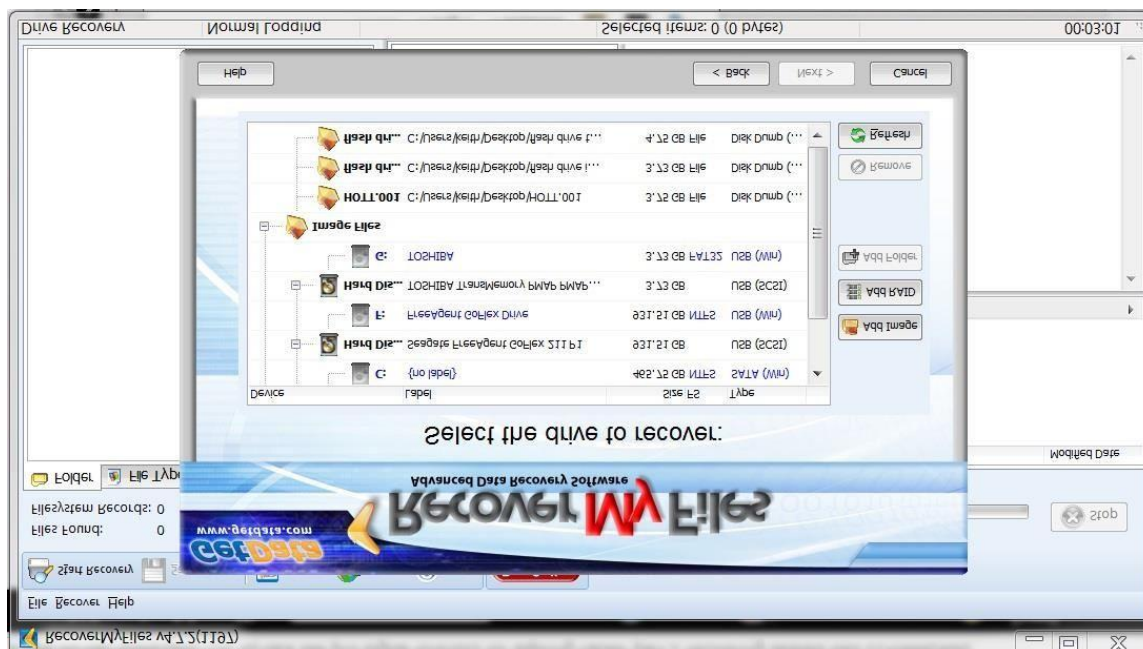
Now that we've created an image of the flash drive, we are ready to recover the deleted files.

#### **Step 4: Recover Deleted Files**

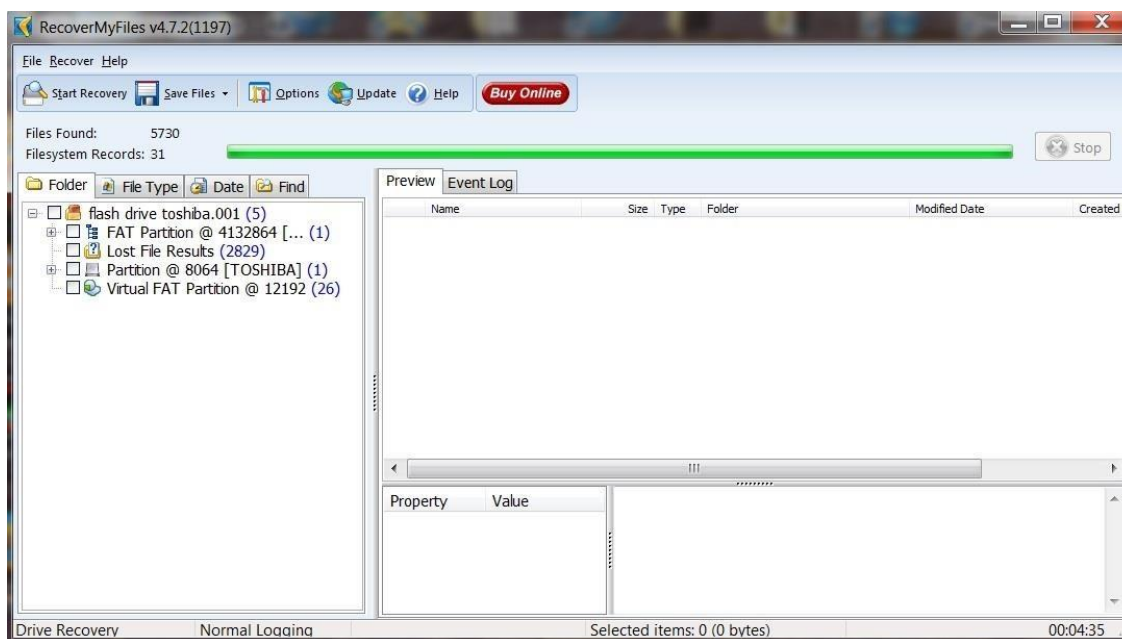
There are many tools on the market to recover deleted files and all of them are adequate to do the job. Deleted file recovery is probably the simplest of forensic tasks. Here, I will be using a trial version of RecoverMyFiles.

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.

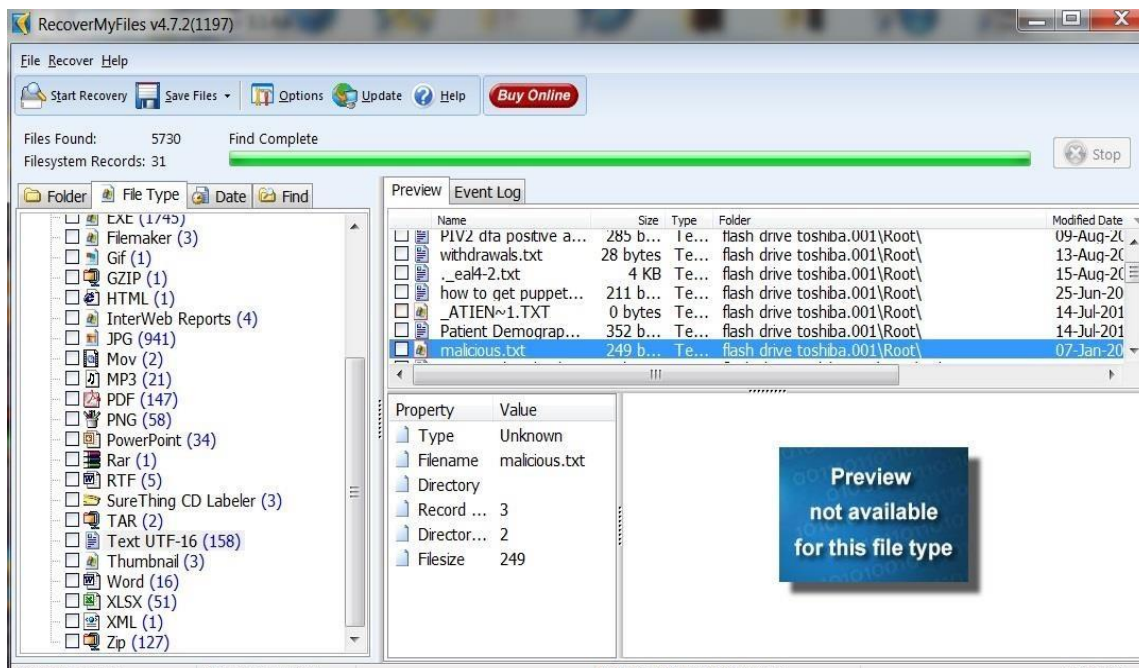


Once you select an image file, start the automatic file recovery. When the recovery is completed, you will see a screen similar to the one below.



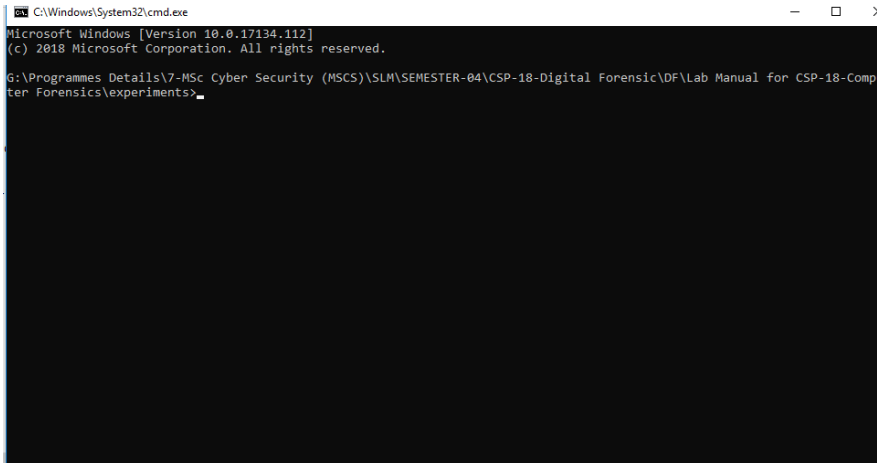
I then selected the File Type tab above the Explorer window to categorize the files by type.

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.





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**

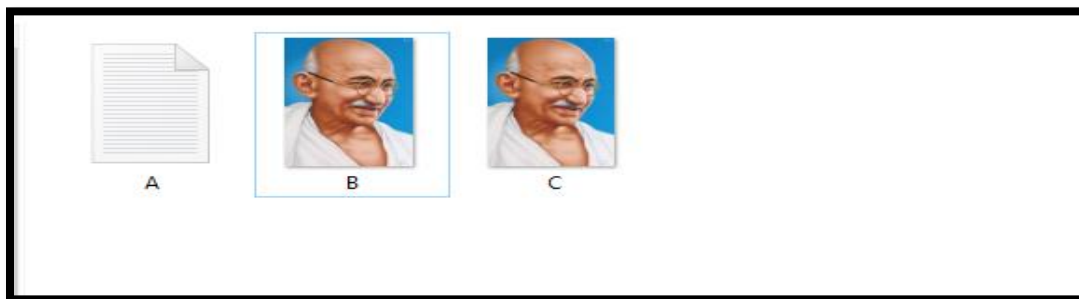
```
G:\Programmes Details\7-MSc Cyber Security (MSCS)\SLM\SEMESTER-04\CSP-18-Digital Forensic\DF\Lab Manual for CSP-18-Computer Forensics\experiments>copy /b B.jpg + A.txt C.jpg
```

**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 for CSP-18-Computer 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 for CSP-18-Computer Forensics\experiments>
```

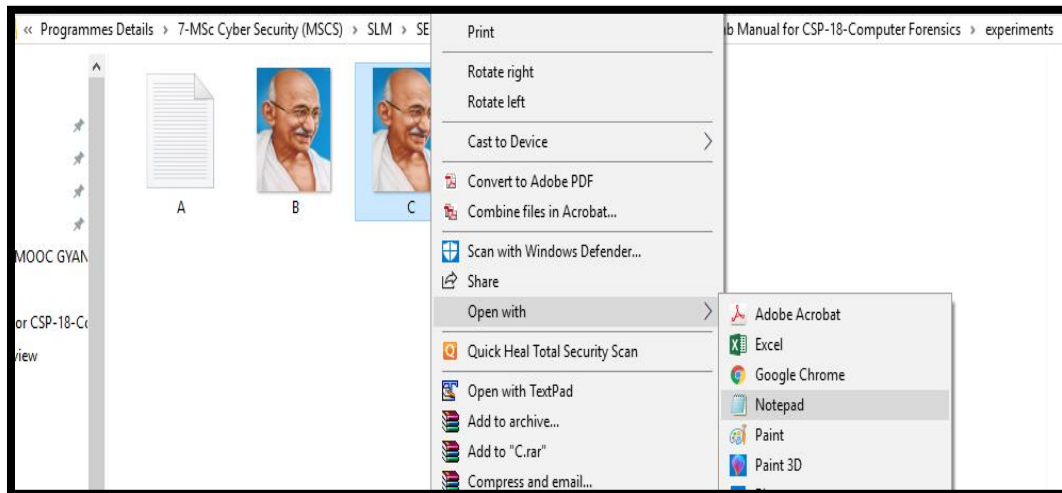
**"C.jpg" is the output image inside this out image our file is hidden**





## 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 :

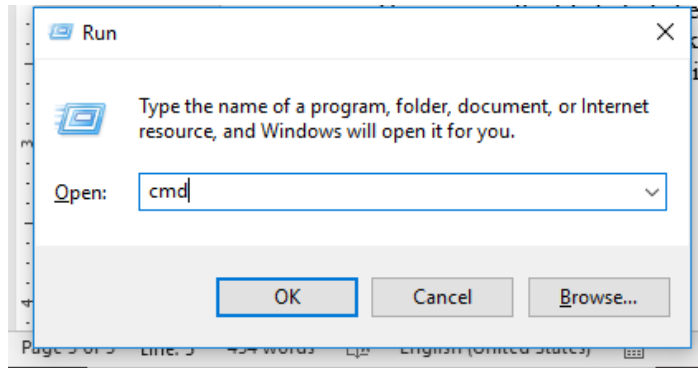
**echo "Your Message">>"image.jpg"**

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**

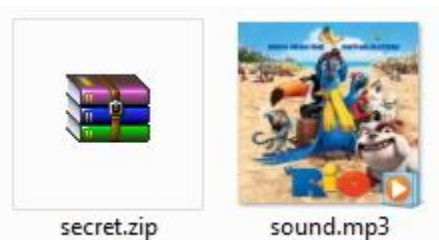
Here a.rar is the file to hide behind the image file (b.jpg) and the output file is **c.jpg**.

**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:

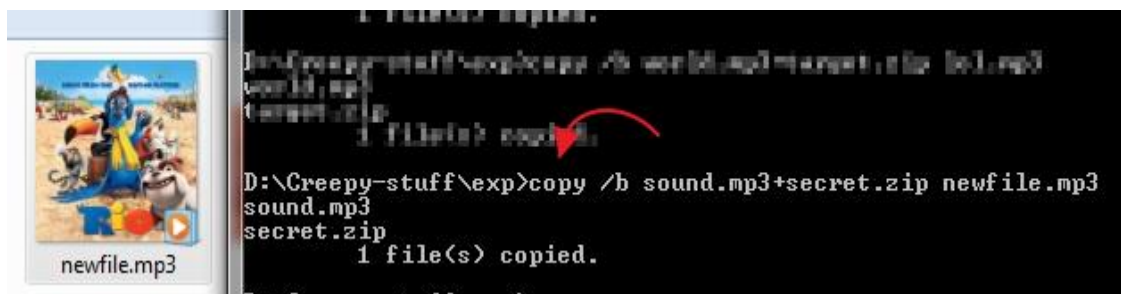
```
copy /b secret.zip + sound.mp3 newfile.mp3
```

## Linux

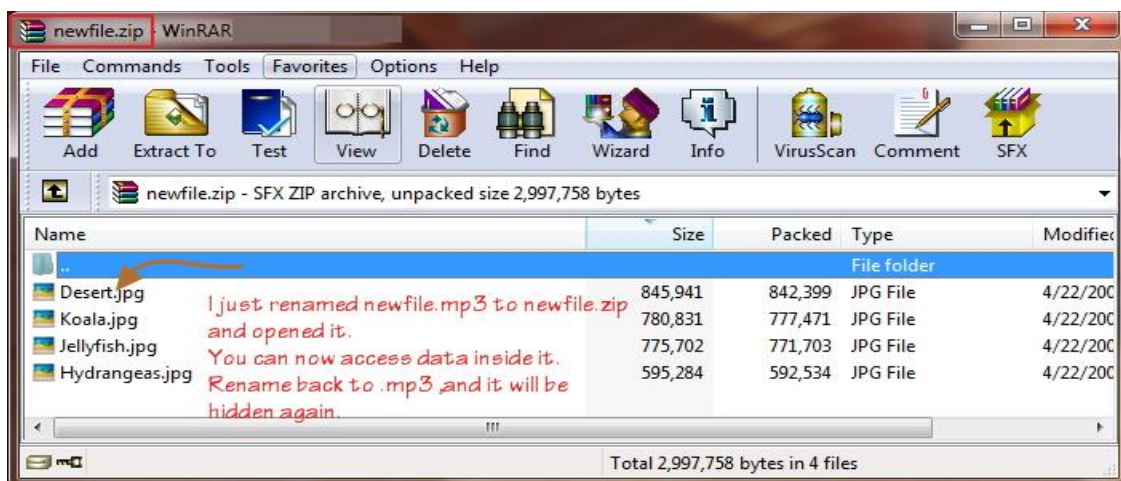
### Code:

```
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-04

---

**Aim of the Experiment:** How to Extract Exchangeable image file format (EXIF) Data from Image Files using **Exifreader** Software.

### Introduction:

In many cases when a computer, phone, or mobile device is seized for evidence, the system will have graphic images that might be used as evidence. Obviously, in some cases, these graphic images may be evidence such as in child pornography cases.

Most digital devices "stamp" information on these graphic images that can tell us a lot about the who, what, when, and where the pictures were taken. This information is known as **EXIF data** and can very often be useful to the forensic investigator.

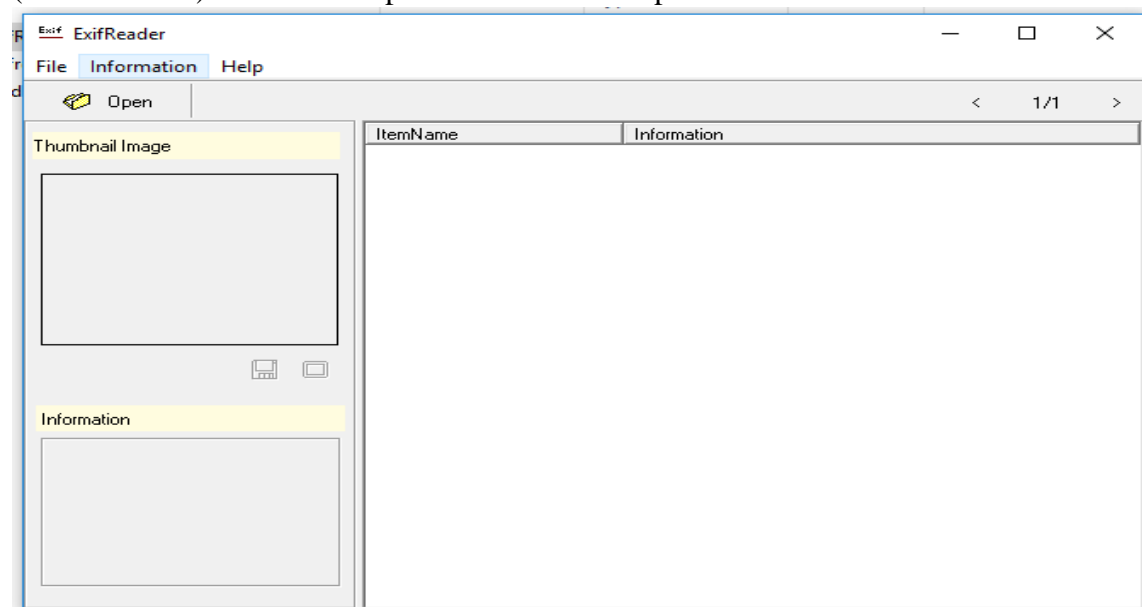
Exchangeable image file format (EXIF) is a standard set by the digital camera industry to identify formats for digital images and sound files. This information includes camera settings, time, date, shutter speed, exposure, whether a flash was used, compression, the name of the camera, and other information critical to viewing and editing the image in image-editing software. This information can be useful to the forensic investigator.

There are numerous applications that can extract this EXIF data from graphic files. Nearly every one of the major forensic suites (EnCase, FTK, Oxygen, etc.) has this capability built-in. For this lab, we will be using a simple, Windows-based tool called [ExifReader](#) (free).

### Extract EXIF Data from Image Files

#### Step-01:

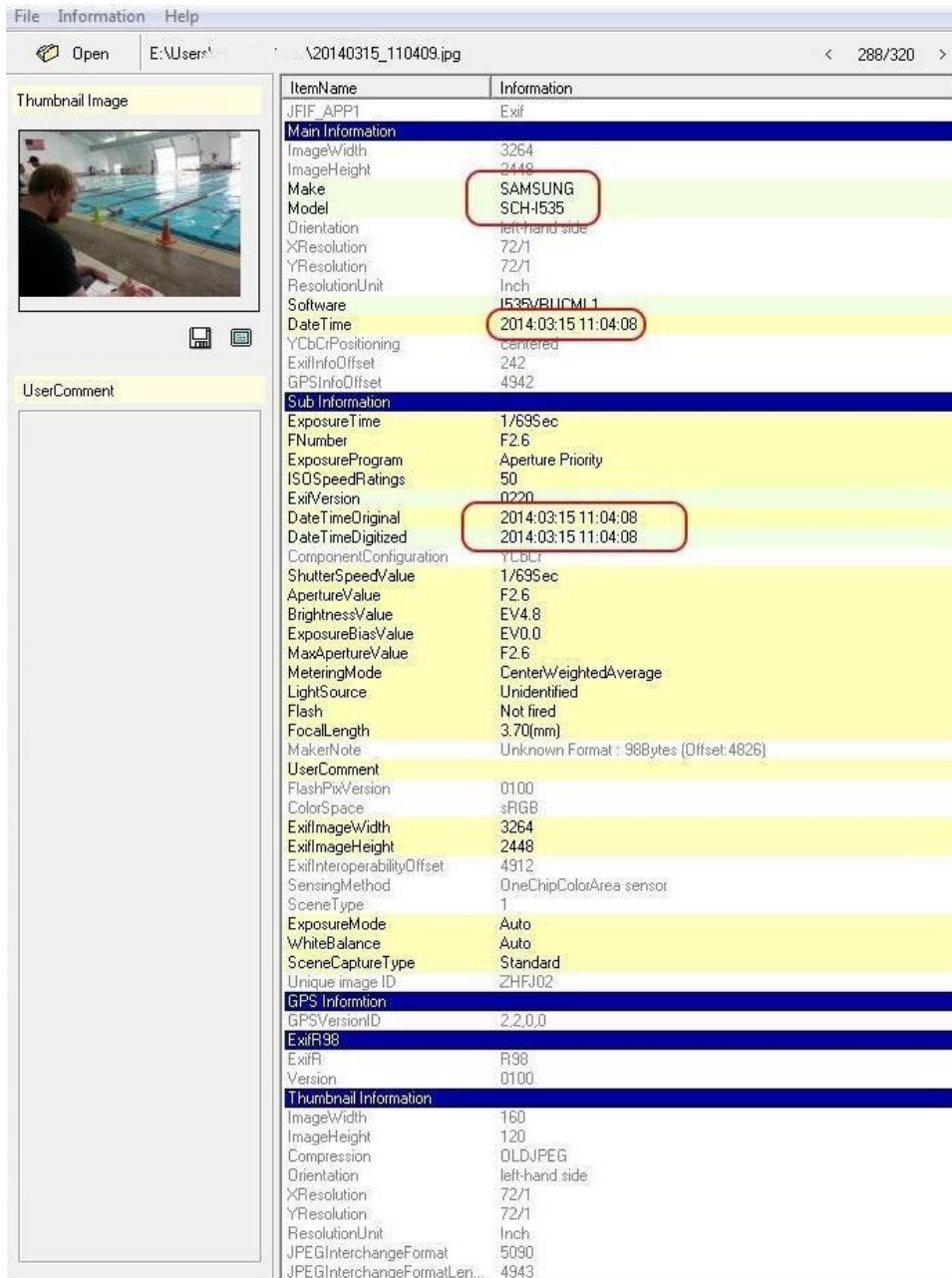
Download the ExifReader from the above link and click on the .exe file (ExifRead.exe) and it will open a clean and simple GUI Wizard as shown below:



Now, simply click on the **"Open"** button and browse to the pictures from the system or media. Normally, JPEG and JPG contain the maximum information, so let's use a JPEG file.

## Step-02: Open a Picture File

Once the selected picture opens the picture, it will load the picture into the thumbnail to the left and display the EXIF data to the right down the page as shown below.



The screenshot displays a software window with a menu bar (File, Information, Help) and a toolbar (Open, Save, Print). The main area is divided into three sections: a 'Thumbnail Image' on the left, a 'UserComment' section below it, and a large table of EXIF data on the right. The thumbnail shows a person in a swimming pool. The EXIF data table is organized into sections: Main Information, Sub Information, GPS Information, and Thumbnail Information. Several fields are highlighted with red boxes, including 'Make' (SAMSUNG), 'Model' (SCH-I535), 'DateTime' (2014:03:15 11:04:08), 'DateTimeOriginal' (2014:03:15 11:04:08), 'DateTimeDigitized' (2014:03:15 11:04:08), and 'Flash' (Not fired).

ItemName	Information
JFIF_APP1	Exif
<b>Main Information</b>	
ImageWidth	3264
ImageHeight	2448
Make	SAMSUNG
Model	SCH-I535
Orientation	left-hand side
XResolution	72/1
YResolution	72/1
ResolutionUnit	Inch
Software	1535/BLICM1.1
DateTime	2014:03:15 11:04:08
YCbCrPositioning	centered
ExifInfoOffset	242
GPSInfoOffset	4942
<b>Sub Information</b>	
ExposureTime	1/695sec
FNumber	F2.6
ExposureProgram	Aperture Priority
ISO Speed Ratings	50
ExifVersion	0220
DateTimeOriginal	2014:03:15 11:04:08
DateTimeDigitized	2014:03:15 11:04:08
ComponentConfiguration	YCbCr
ShutterSpeedValue	1/695sec
ApertureValue	F2.6
BrightnessValue	EV4.8
ExposureBiasValue	EV0.0
MaxApertureValue	F2.6
MeteringMode	CenterWeightedAverage
LightSource	Unidentified
Flash	Not fired
FocalLength	3.70(mm)
MakerNote	Unknown Format : 988bytes (Offset:4826)
<b>UserComment</b>	
FlashPixVersion	0100
ColorSpace	sRGB
ExifImageWidth	3264
ExifImageHeight	2448
ExifInteroperabilityOffset	4912
SensingMethod	OneChipColorArea sensor
SceneType	1
ExposureMode	Auto
WhiteBalance	Auto
SceneCaptureType	Standard
Unique image ID	ZHFJ02
<b>GPS Information</b>	
GPSVersionID	2.2.0.0
<b>ExifR98</b>	
ExifR	R98
Version	0100
<b>Thumbnail Information</b>	
ImageWidth	160
ImageHeight	120
Compression	OLDJPEG
Orientation	left-hand side
XResolution	72/1
YResolution	72/1
ResolutionUnit	Inch
JPEGInterchangeFormat	5090
JPEGInterchangeFormatLen...	4943

There are lots of information you can collect in the EXIF data, but most are related to the technical specifications of the camera and photography. GPS coordinates of where the picture was taken. Most of this is of limited value to the forensic investigator.

---

## EXPERIMENT-05

---

**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 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.

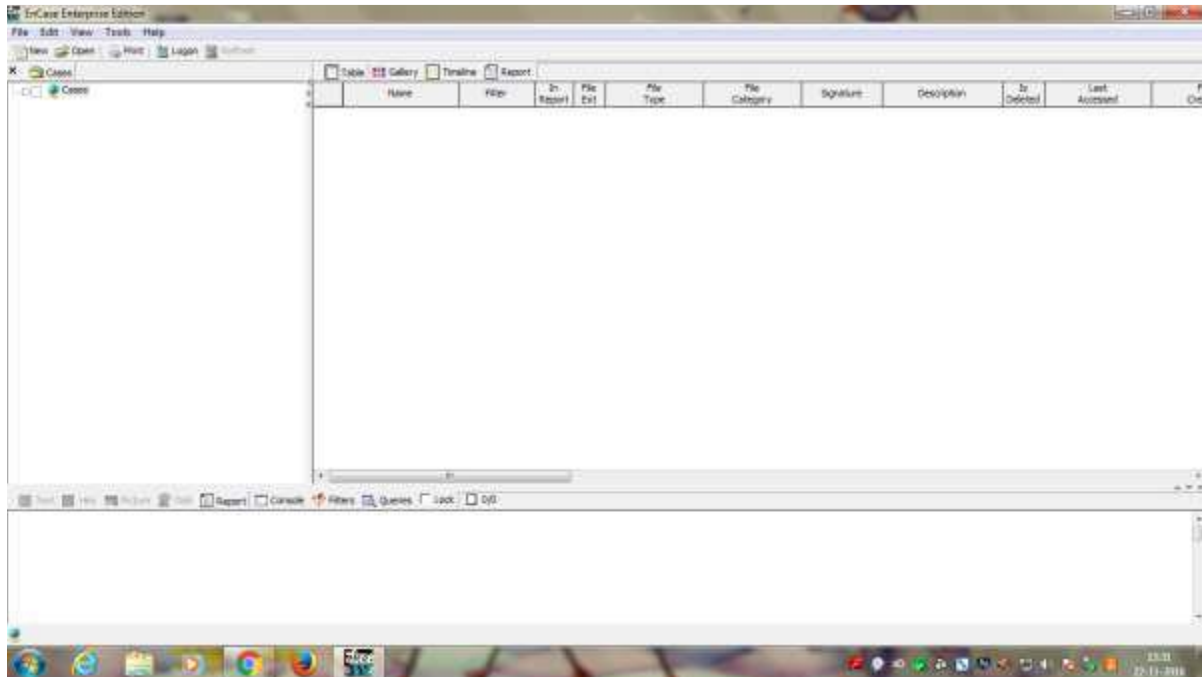
**Scenario:** Mr. X is suspected to be involved in selling his company's confidential data to the competitors, but without any evidence, no action could be taken against him. To get into reality and proof Mr. X guilty, the company has requested the forensic services and have come to know all the relevant 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.

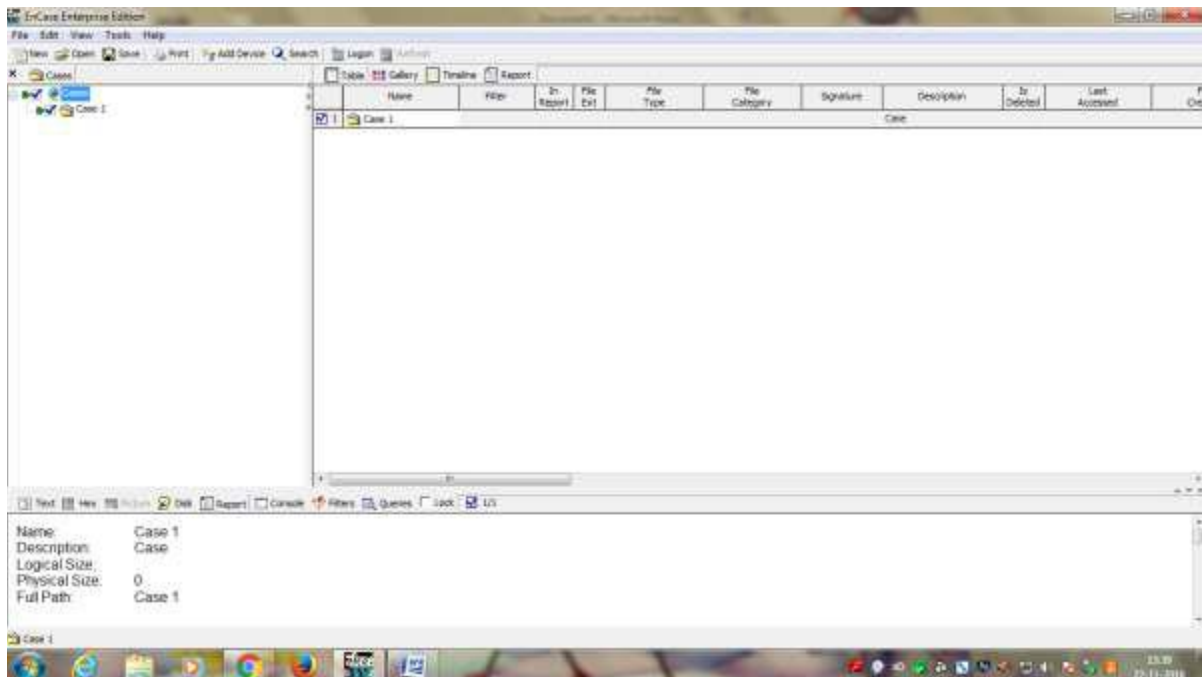


**Step 2:** Click On New For Creating A New Case. Fill the labels.

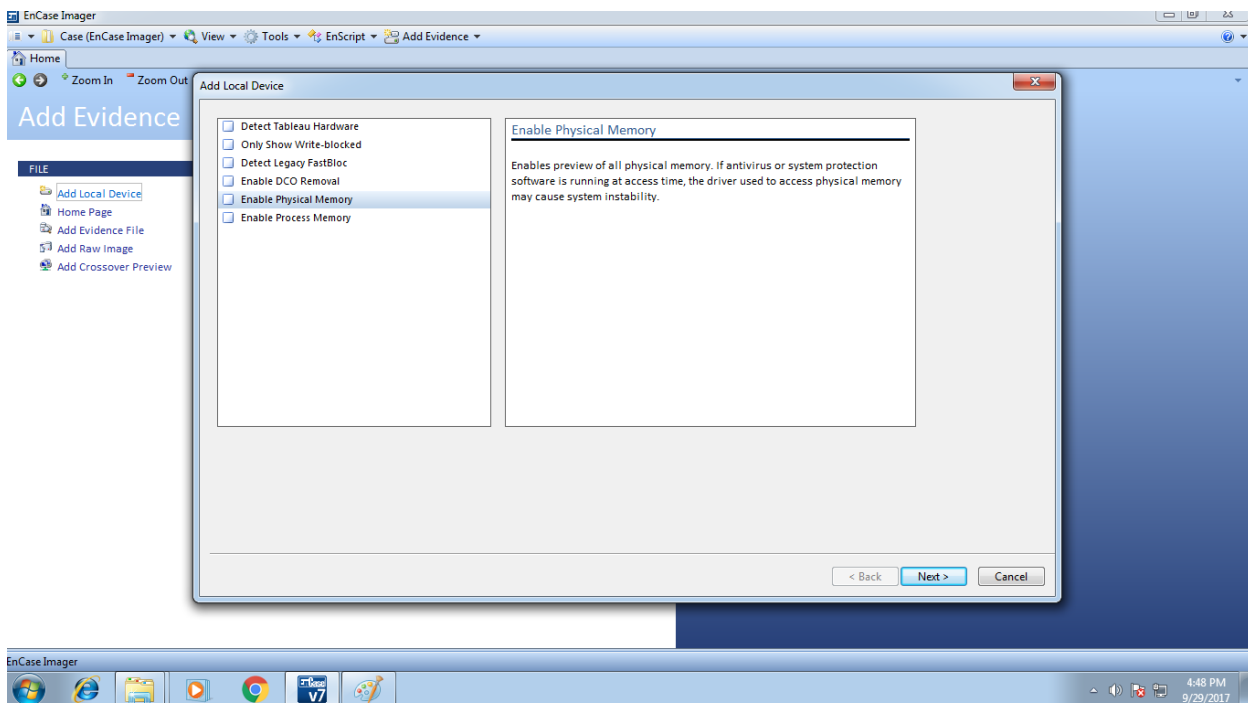
A screenshot of the 'Case Options' dialog box in Encase. The dialog box has a title bar with a close button (X). It contains four text input fields: 'Name' with the value 'Case 1', 'Examiner Name' with the value 'abcd', 'Default Export Folder' with the value 'C:\Program Files\EnCase4', and 'Temporary Folder' with the value 'C:\Users\Administrator\AppData\Local\Temp'. Each folder field has a browse button (three dots). At the bottom of the dialog box are three buttons: '< Back', 'Finish', and 'Cancel'.

Click On Finish.

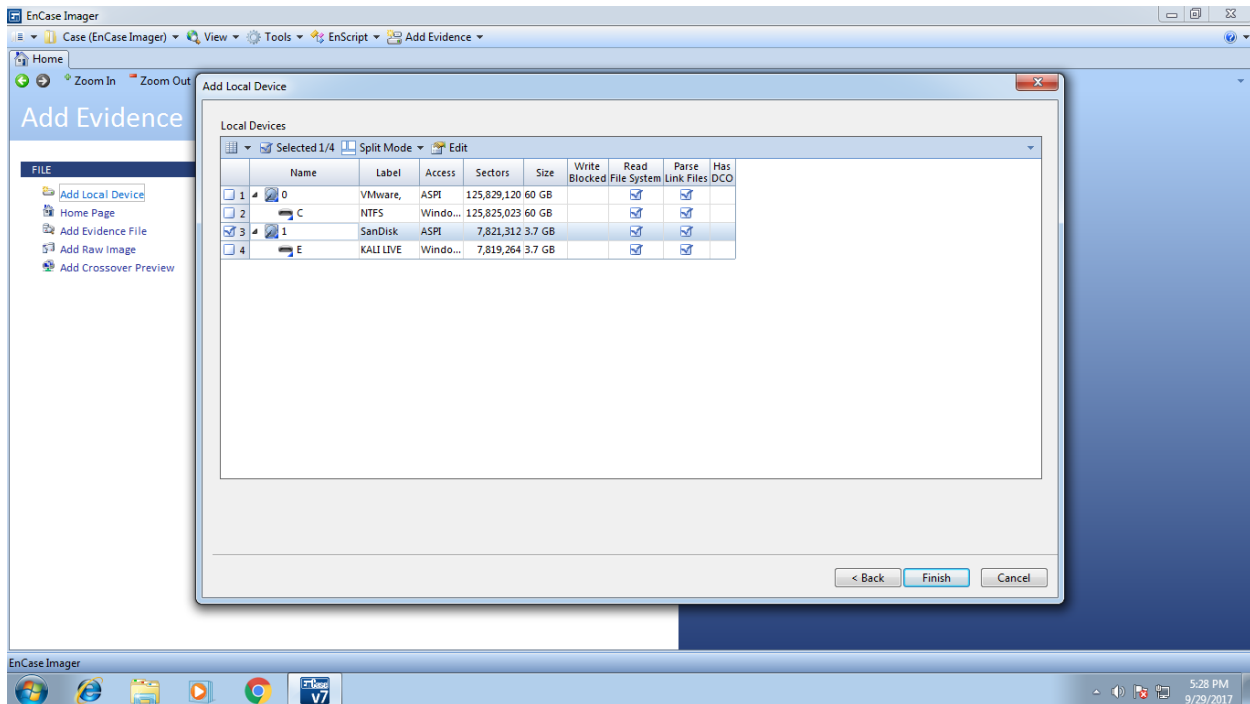
**Step 3: View the Case by Clicking On Case 1 <Case Name>**



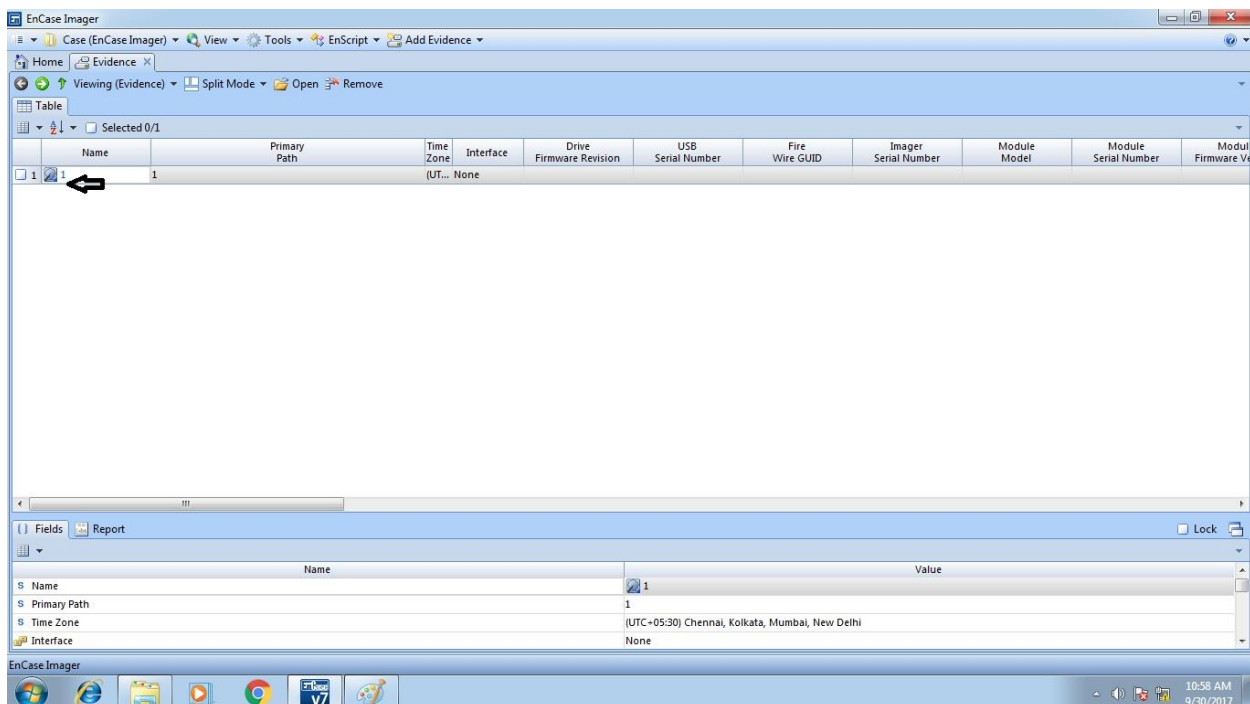
**Step 4: Click on add local device for Adding Devices to Your Case. If there is any write blocker attached with the machine and digital device then tick to 1,2 and 5 option otherwise untick to all and click on **Next** button.**

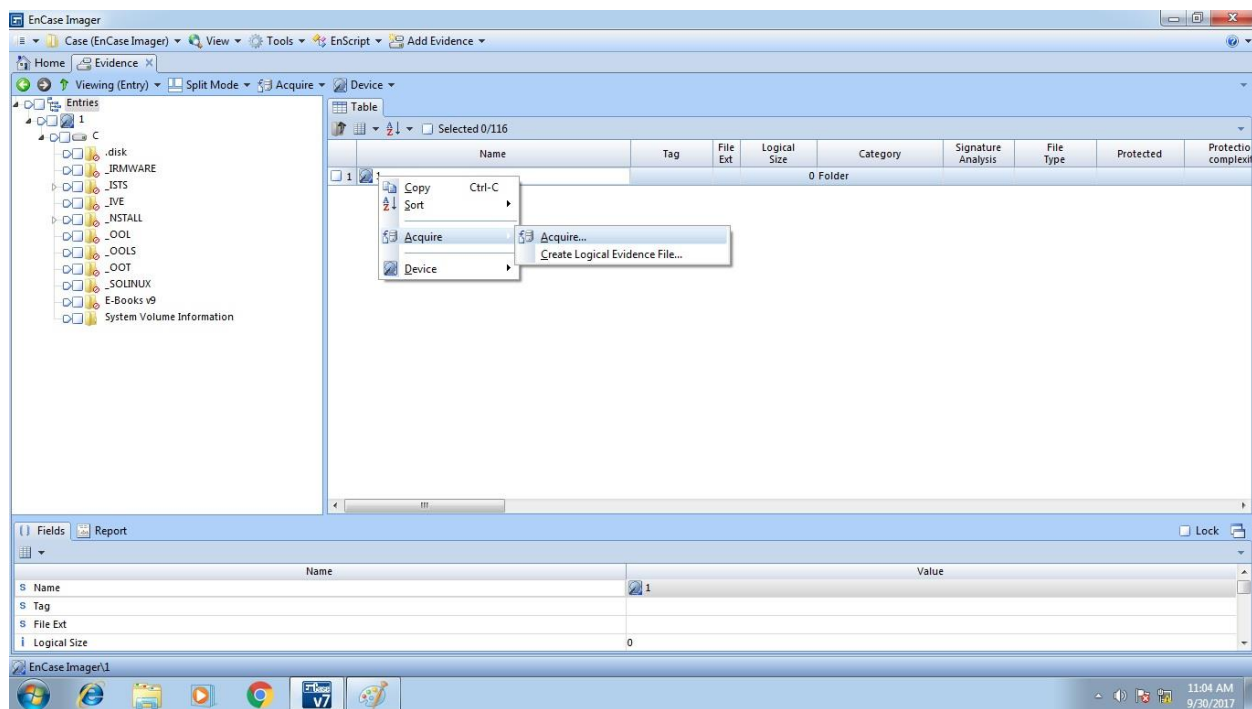


**Step 5:** Tick in the box of name column which shows the connected device name or label like (1,2,3 or any numeric number) and click on the **finish** button.



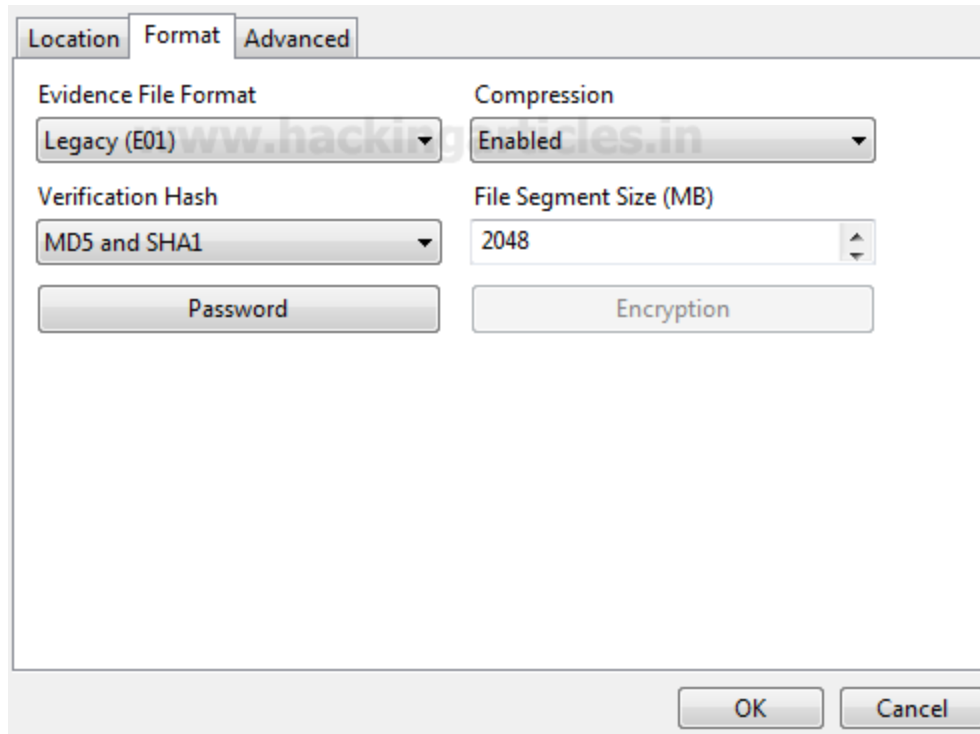
**Step-06:** Now to open evidence click on label number of the device which shows in “name” column and again right-click on label number and choose **acquire** the option.



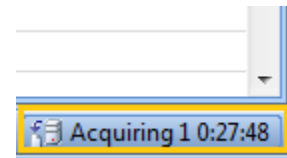


**Step-07:** Then a pop up will appear with three tabs. In the **location tab**, fills all the fields. In **format tab** if you want to encrypt the evidence file then enable the Compression field otherwise disable it. In Verification Hash field value should be chosen MD5 and SHA1 after it click on **OK 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).



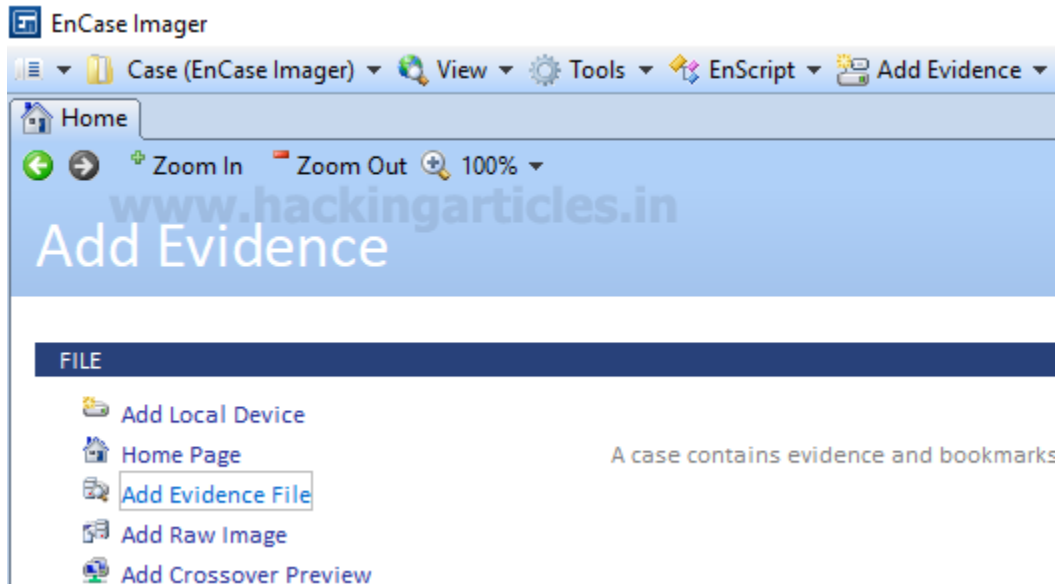
**Step-09:** Device will automatically disconnect after creating the image. The image will save in the folder which we set the path earlier. Once the acquisition is complete the image will get saved to the output folder (refer below image).

1.E01	1/24/2018 7:09 PM	E01 File
1.E02	1/24/2018 7:12 PM	E02 File
1.E03	1/24/2018 7:16 PM	E03 File
1.E04	1/24/2018 7:19 PM	E04 File
1.E05	1/24/2018 7:21 PM	E05 File
1.E06	1/24/2018 7:23 PM	E06 File
1.E07	1/24/2018 7:24 PM	E07 File

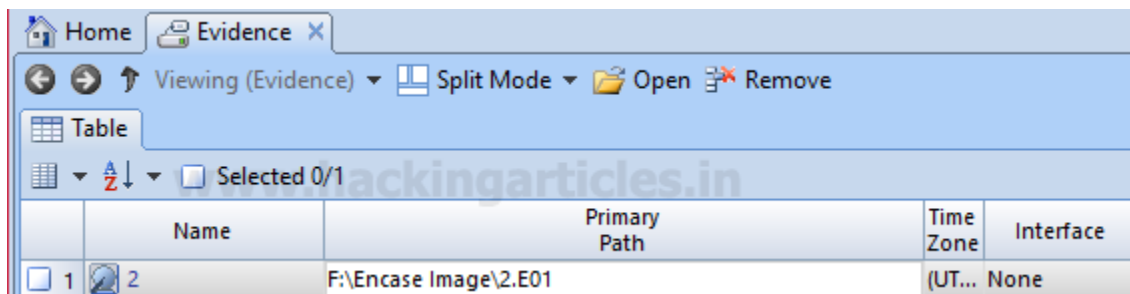
## EXPERIMENT-06

**Aim of the Experiment:** How to Restoring the Evidence Image using EnCase Imager

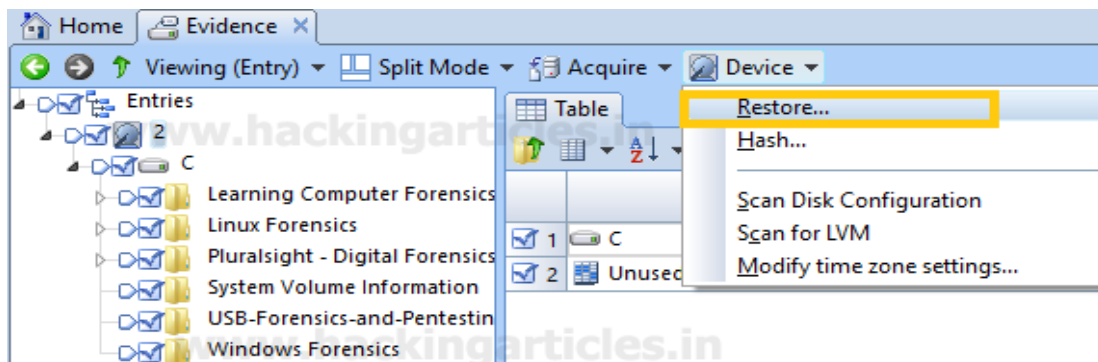
Open Encase Imager and add the evidence to Encase imager



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



Double click on the image, select the 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.

#### Restore 2

Local Devices							
Split Mode Edit							
	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.

#### Drives

☐ Wipe remaining sectors on target

☒ Verify wiped sectors

Wipe character (hex)

00

☒ Verification MD5    ☒ Verification SHA1

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.

Drives

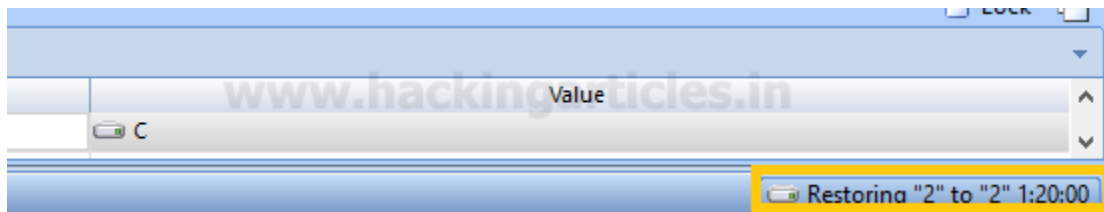
This will destroy all information on "Device: 2, Label: SanDisk".

Continue? Type the word "Yes"

Yes

OK Cancel

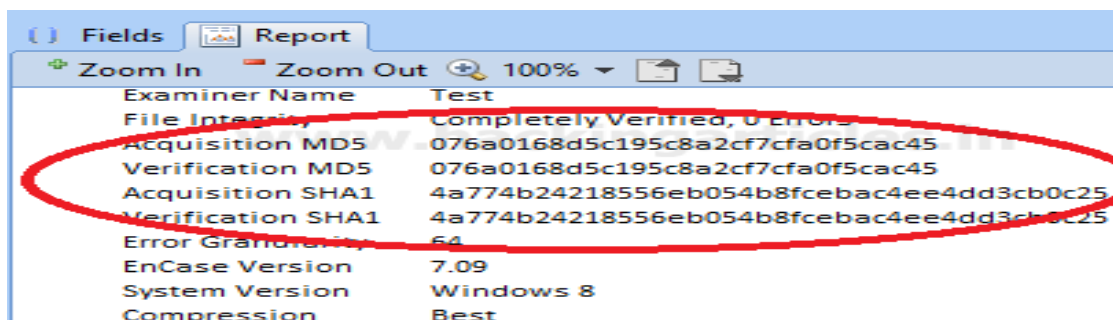
Image Restoration will start, we can check the progress on the lower right corner of the window.



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

Name	Date modified
Learning Computer Forensics	1/22/2018 1:01 PM
Linux Forensics	1/22/2018 1:03 PM
Pluralsight - Digital Forensics Tools in Kal...	1/22/2018 1:03 PM
USB-Forensics-and-Pentesting	1/22/2018 1:04 PM
Windows Forensics	1/22/2018 1:04 PM
1-Basic Networking	1/17/2018 8:47 PM
2.1-OSI LAYERS	1/17/2018 8:47 PM
2.2-TCP IP LAYER (1)	1/17/2018 8:47 PM
2.2-TCP IP LAYER	1/17/2018 8:47 PM

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.

---

## EXPERIMENT-07

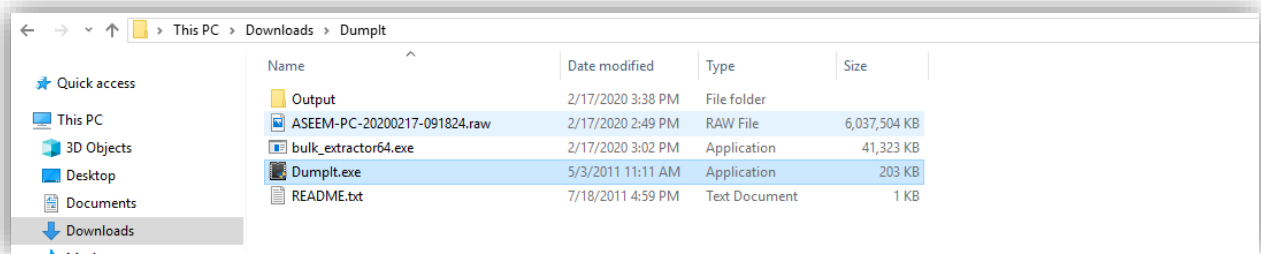
---

### Aim of the Experiment: How to Collect Email Evidence in Victim PC

To collect email evidence from Victim PC the first step is to capture the victim's RAM. This can be possible using **dumpit** tool.

This utility is used to generate a physical memory dump of Windows machines. It works with both x86 (32-bits) and x64 (64-bits) machines. The raw memory dump is generated in the current directory, only a confirmation question is prompted before starting. Perfect to deploy the executable on USB keys, for quick incident responses needs.

Run **Dumplt.exe** file the raw memory dump will be generated and save to the same directory



```
C:\Users\OSOU-18\Downloads\Dumplt\Dumplt.exe

DumpIt - v1.3.2.20110401 - One click memory memory dumper
Copyright (c) 2007 - 2011, Matthieu Suiche <http://www.msuiche.net>
Copyright (c) 2010 - 2011, MoonSols <http://www.moonsols.com>

Address space size:      6182404096 bytes ( 5896 Mb)
Free space size:        59016699904 bytes ( 56282 Mb)

* Destination = \\?\C:\Users\OSOU-18\Downloads\DumpIt\ASEEM-PC-20200217-105827.raw

--> Are you sure you want to continue? [y/n]
```

Write 'Y' for processing

```
C:\Users\OSOU-18\Downloads\Dumplt\Dumplt.exe

DumpIt - v1.3.2.20110401 - One click memory memory dumper
Copyright (c) 2007 - 2011, Matthieu Suiche <http://www.msuiche.net>
Copyright (c) 2010 - 2011, MoonSols <http://www.moonsols.com>

Address space size:      6182404096 bytes ( 5896 Mb)
Free space size:        59016699904 bytes ( 56282 Mb)

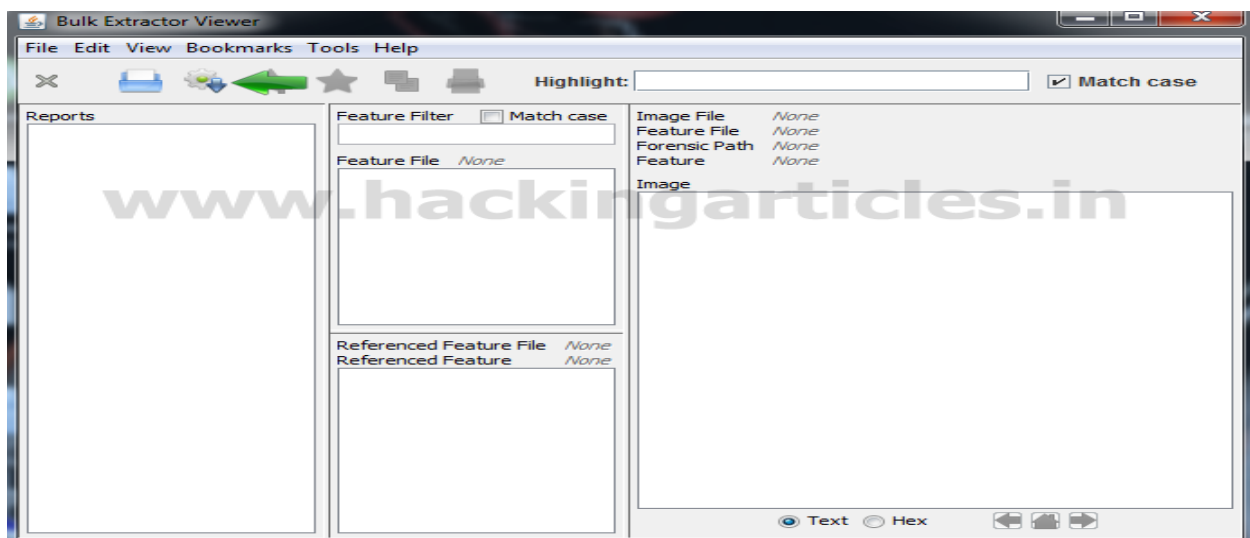
* Destination = \\?\C:\Users\OSOU-18\Downloads\DumpIt\ASEEM-PC-20200217-105827.raw

--> Are you sure you want to continue? [y/n] y
+ Processing...
```

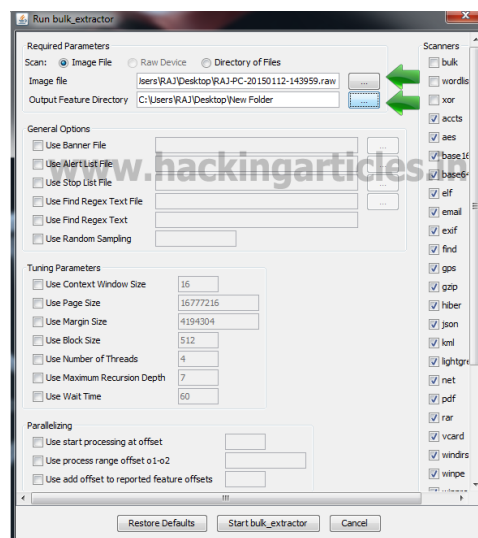
The output .RAW file will be as follows

Name	Date modified	Type	Size
Output	2/17/2020 3:38 PM	File folder	
ASEEM-PC-20200217-105827.raw	2/17/2020 4:29 PM	RAW File	6,037,504 KB
bulk_extractor64.exe	2/17/2020 3:02 PM	Application	41,323 KB
Dumplt.exe	5/3/2011 11:11 AM	Application	203 KB
README.txt	7/18/2011 4:59 PM	Text Document	1 KB

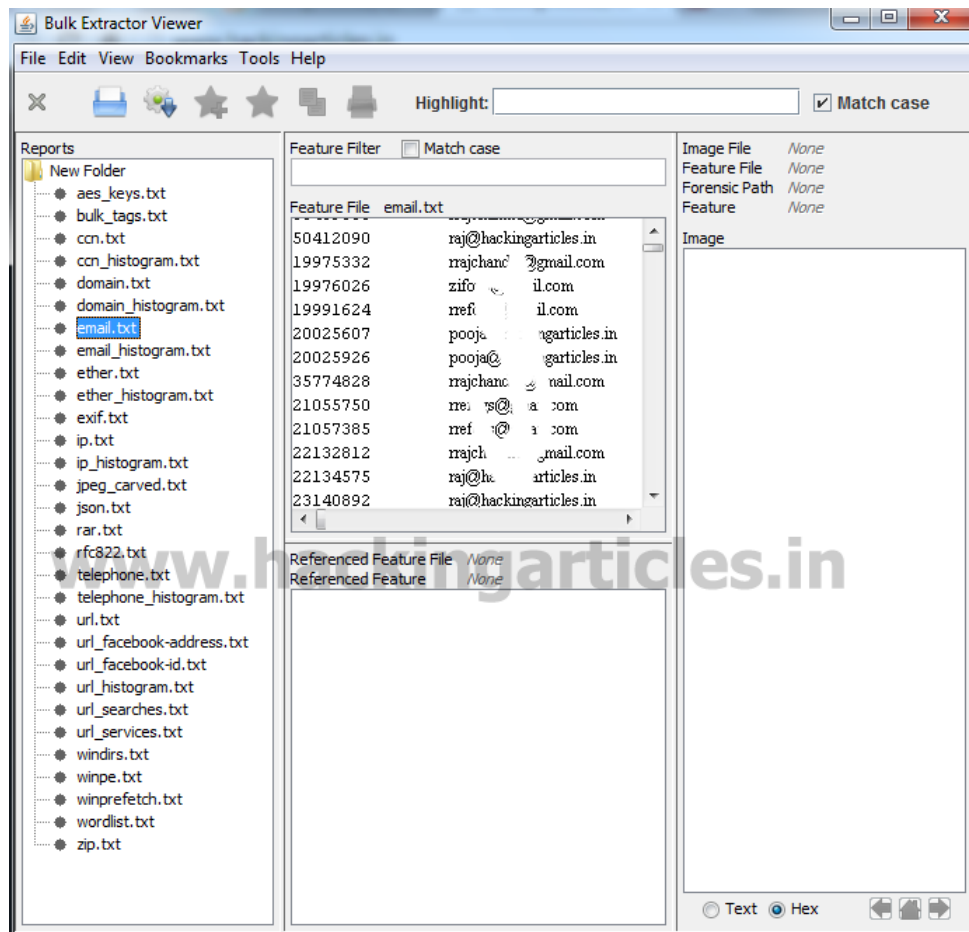
Then Download **bulk extractor viewer** from GitHub and install it in your PC. Now open bulk extractor viewer and click on to **generate report**.



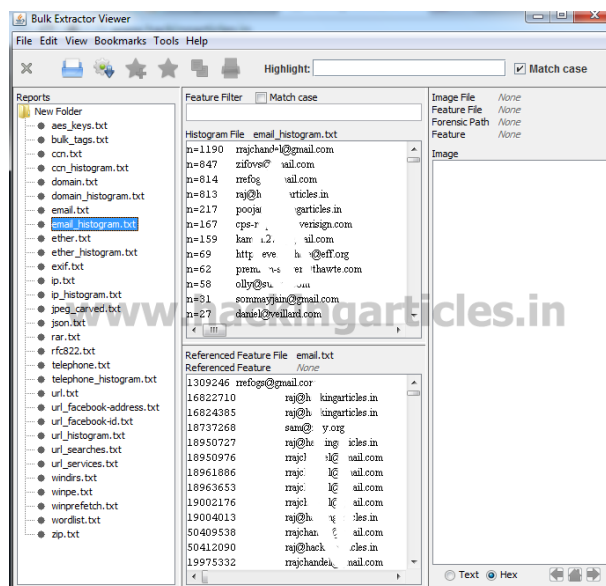
Now select the dump it image file and select an output folder for the report and click on start bulk extractor as seen below



Now in order to investigate the victim saved information of Email ID Click on email.txt as seen below



And also click on email\_histogram.txt

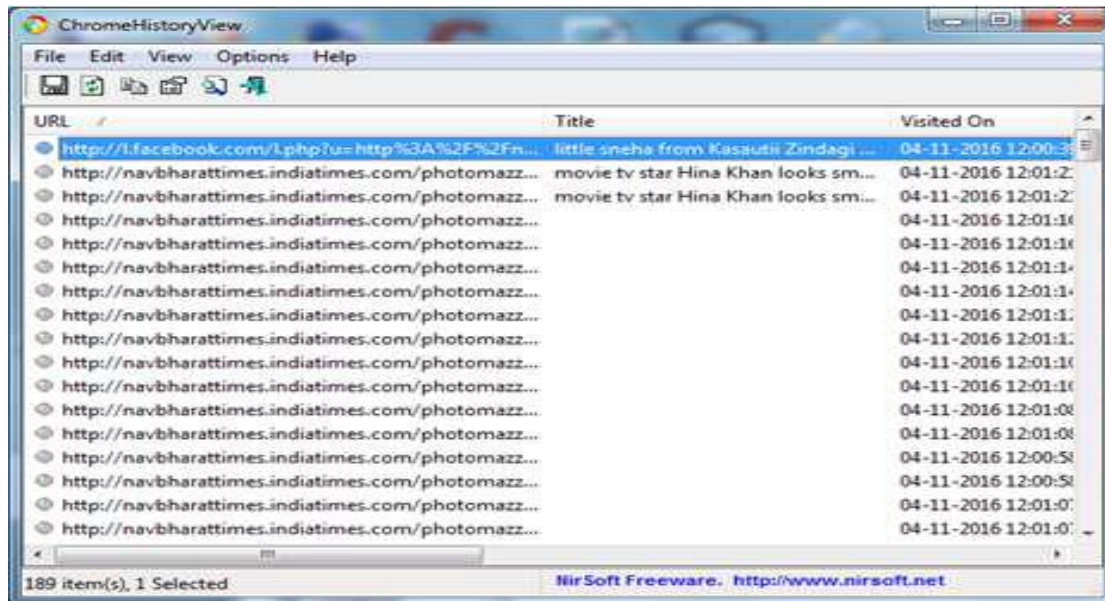




## EXPERIMENT-08

**Aim of the Experiment:** How to Extracting Browser Artifacts

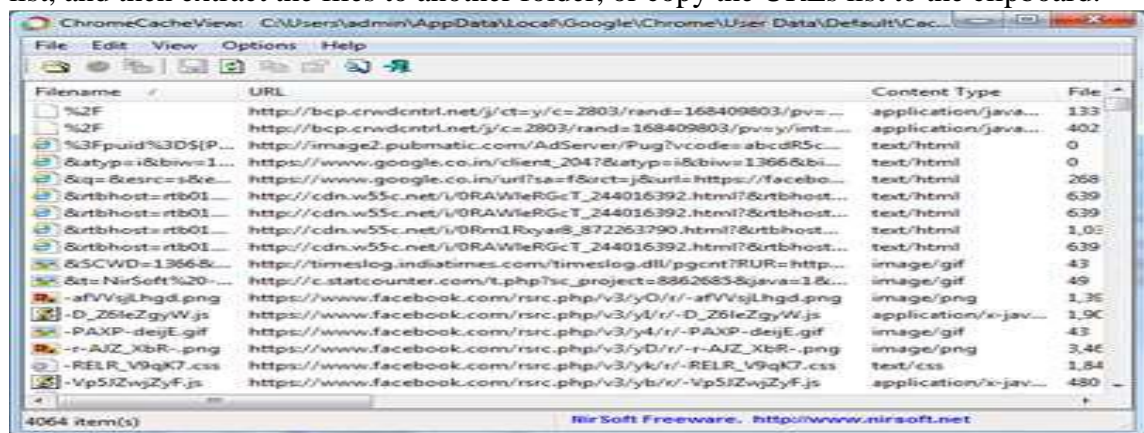
**ChromeHistoryView:** is a small utility that reads the history data file of Google Chrome Web browser, and displays the list of all visited Web pages in the last days. For each visited Webpage, the following information is displayed: URL, Title, Visit Date/Time, Number of visits, number of times that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

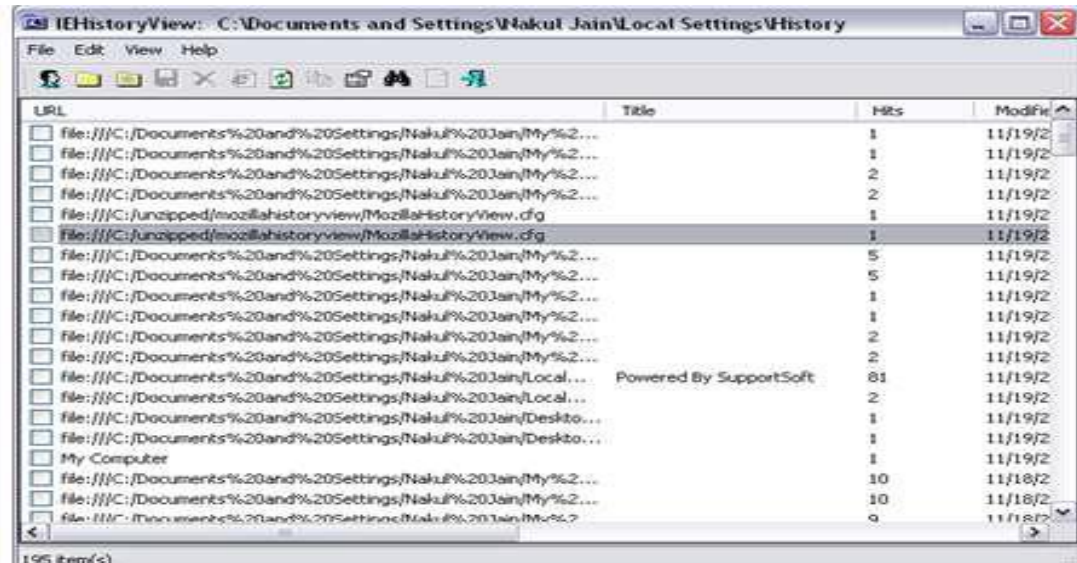
For each cache file, the following information is displayed:

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.

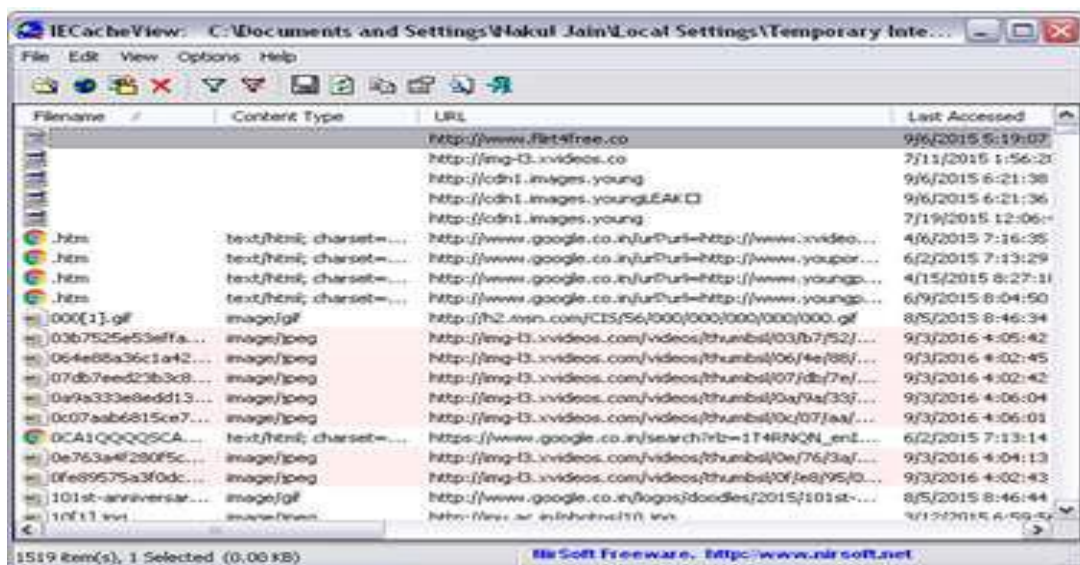




**IEHistoryView:** This utility reads all information from the history file on your computer, and displays the list of all URLs that you have visited in the last few days. It also allows you to select one or more URL addresses, and then remove them from the history file or save them into text, HTML or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



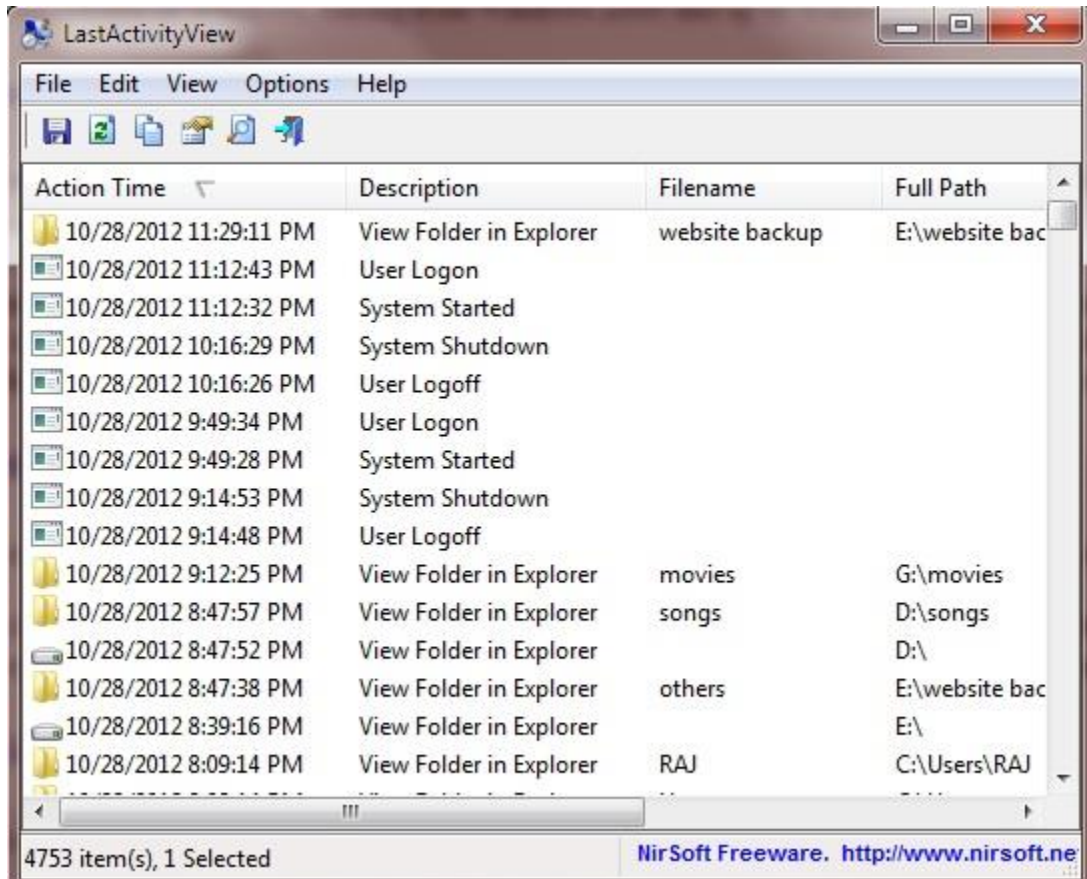
---

## EXPERIMENT-09

---

**Aim of the Experiment:** How to View Last Activity of Your PC

LastActivityView is a tool for Windows operating system that collects information from various sources on a running system, and displays a log of actions made by the user and events occurred on this computer.



---

## EXPERIMENT-10

---














**Aim of the Experiment:** 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

---

## EXPERIMENT-11

---

**Aim of the Experiment:** Comparison of two Files for forensics investigation by Compare IT software

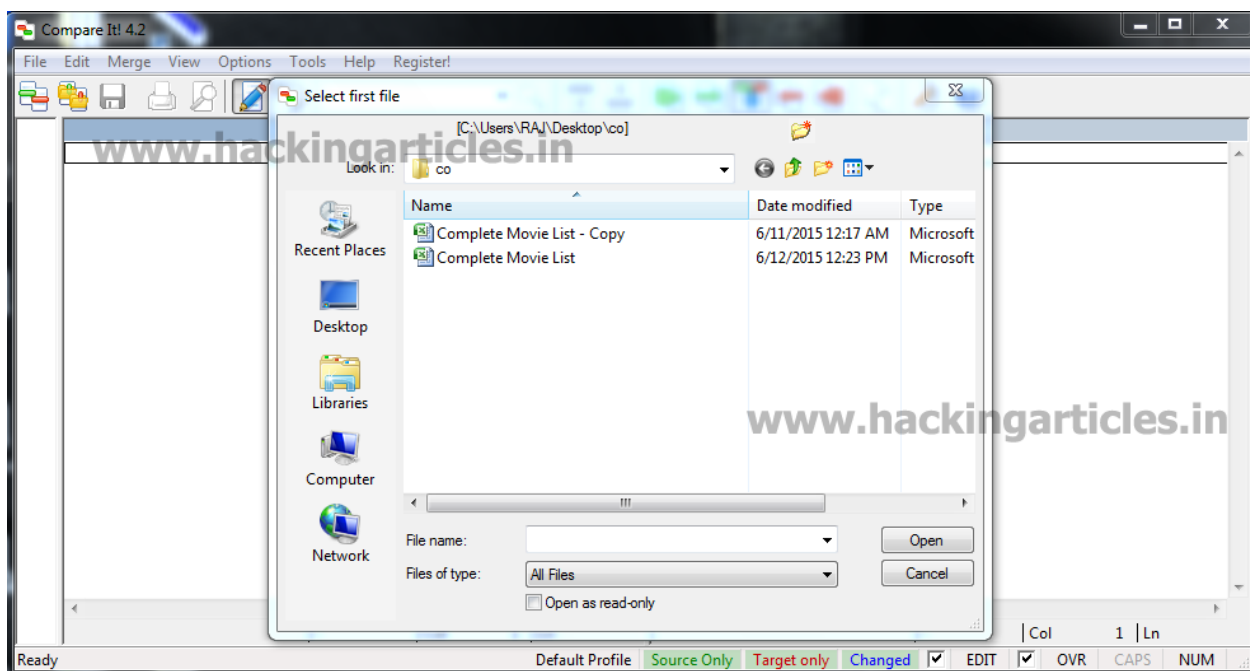
Compare It is a software that displays 2 files side by side, with colored differences sections to simplify analyzing. You can move changes between files with a single mouse click or keystroke, and of course, you have the ability to edit files directly in comparison window. It can make colored printout of differences report, exactly as it's on the screen.

First of all, install the Compare It from the Link given below.

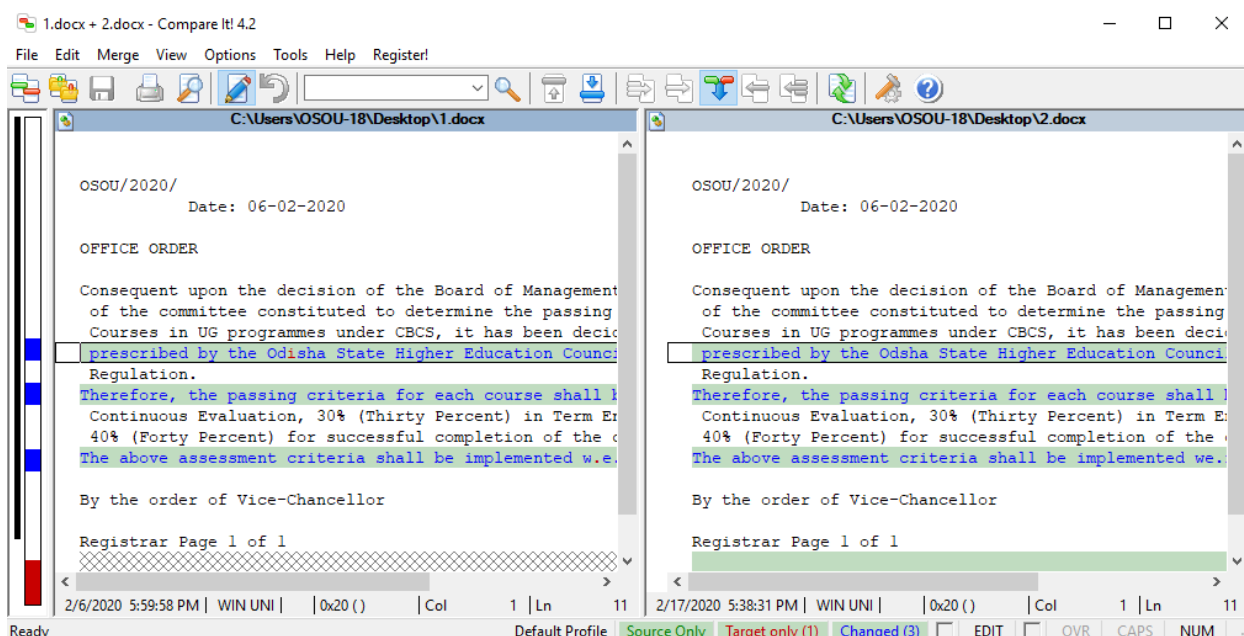
**<http://www.grigsoft.com/wincmp3.htm> it is a 1.7 Mb Software package**

Click on Compare It Tool, It will show a window to select the files to be compared.

First, select the first file and click on open and then select the second file and click on open.



Now it will show us the changes in the highlighted bar.



It also gives you Print report of the difference in the file as follows

2/17/2020 5:54:13 PM			
C:\Users\OSOU-18\Desktop\1.docx		C:\Users\OSOU-18\Desktop\2.docx	
1		1	
2		2	
3	OSOU/2020/	3	OSOU/2020/
4	Date: 06-02-2020	4	Date: 06-02-2020
5		5	
6	OFFICE ORDER	6	OFFICE ORDER
7		7	
8	Consequent upon the decision of the Board of Management (BOM) and the resolution	8	Consequent upon the decision of the Board of Management (BOM) and the resolution
9	of the committee constituted to determine the passing criteria in different	9	of the committee constituted to determine the passing criteria in different
10	Courses in UG programmes under CBCS, it has been decided to adopt the criteria	10	Courses in UG programmes under CBCS, it has been decided to adopt the criteria
11	prescribed by the Odisha State Higher Education Council (OSHEC) under Model Regulation.	11	prescribed by the Odsha State Higher Education Council (OSHEC) under Model Regulation.
12	Therefore, the passing criteria for each course shall be 40% (Forty Percent) in	12	Therefore, the passing criteria for each course shall be 30% (Forty Percent) in
13	Continuous Evaluation, 30% (Thirty Percent) in Term End Examination and overall	13	Continuous Evaluation, 30% (Thirty Percent) in Term End Examination and overall
14	40% (Forty Percent) for successful completion of the course.	14	40% (Forty Percent) for successful completion of the course.
15	The above assessment criteria shall be implemented w.e.f. TEE-Dec 2019.	15	The above assessment criteria shall be implemented we.f. TEE-Dec 2019.
16		16	
17	By the order of Vice-Chancellor	17	By the order of Vice-Chancellor
18		18	
19	Registrar Page 1 of 1	19	Registrar Page 1 of 1
20		20	
		21	
		22	



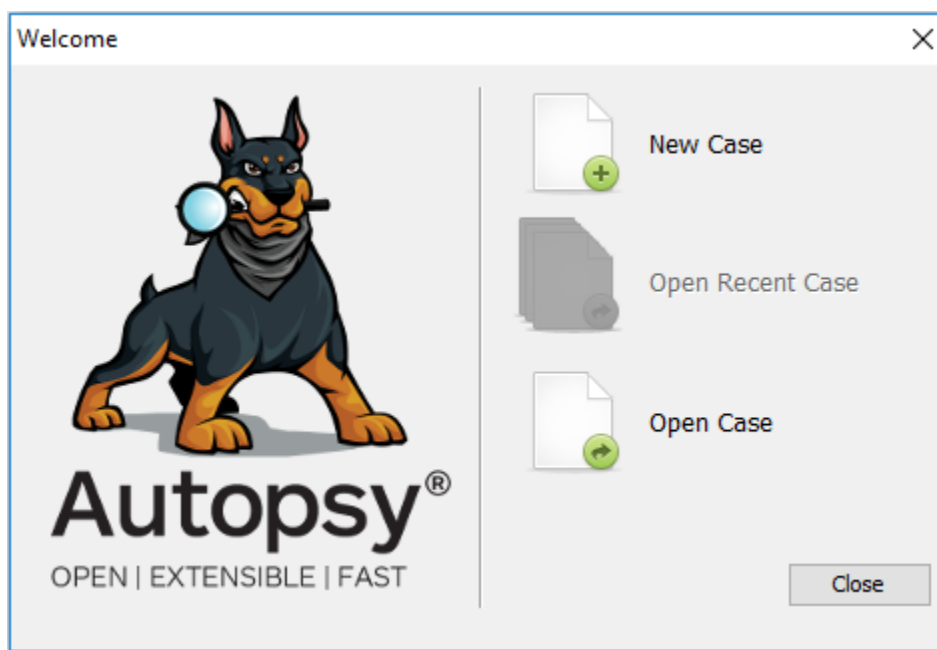
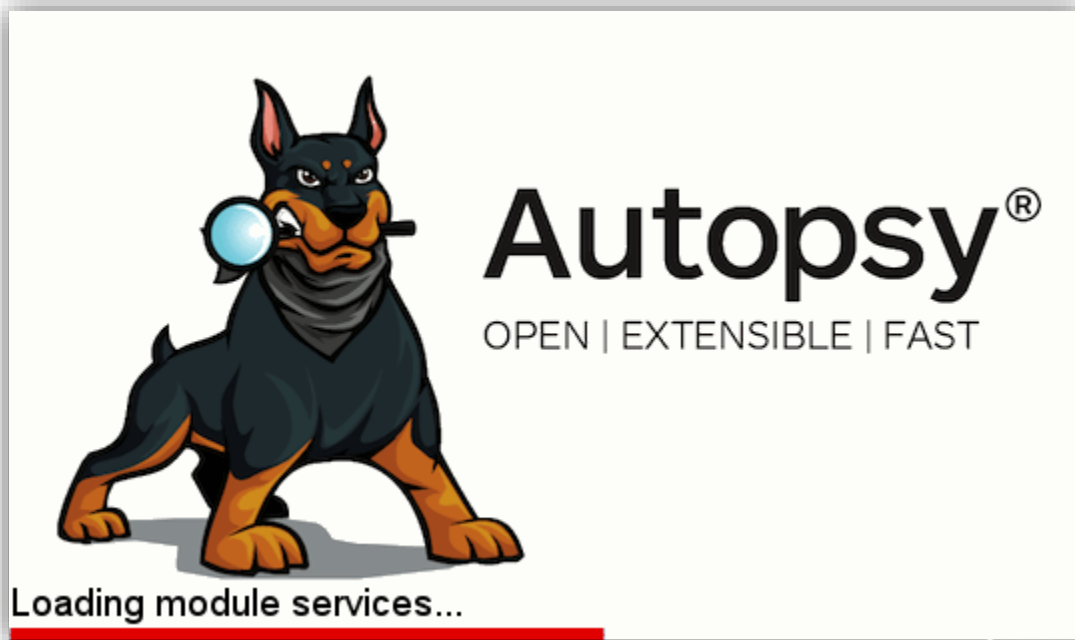
---

## EXPERIMENT-12

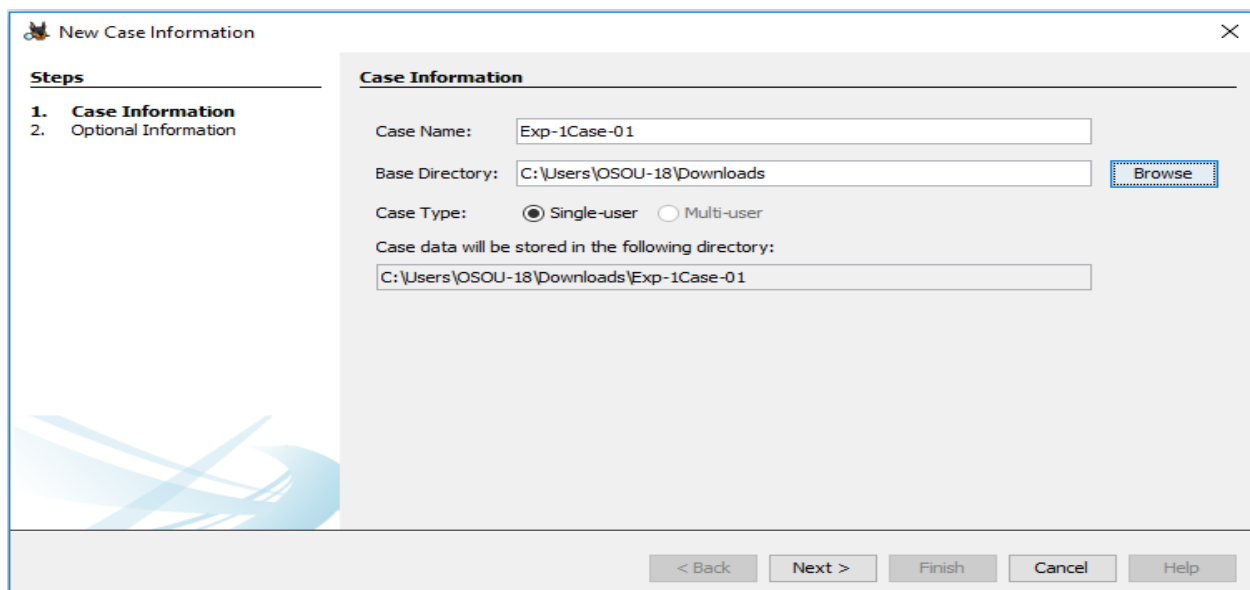
---

**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.

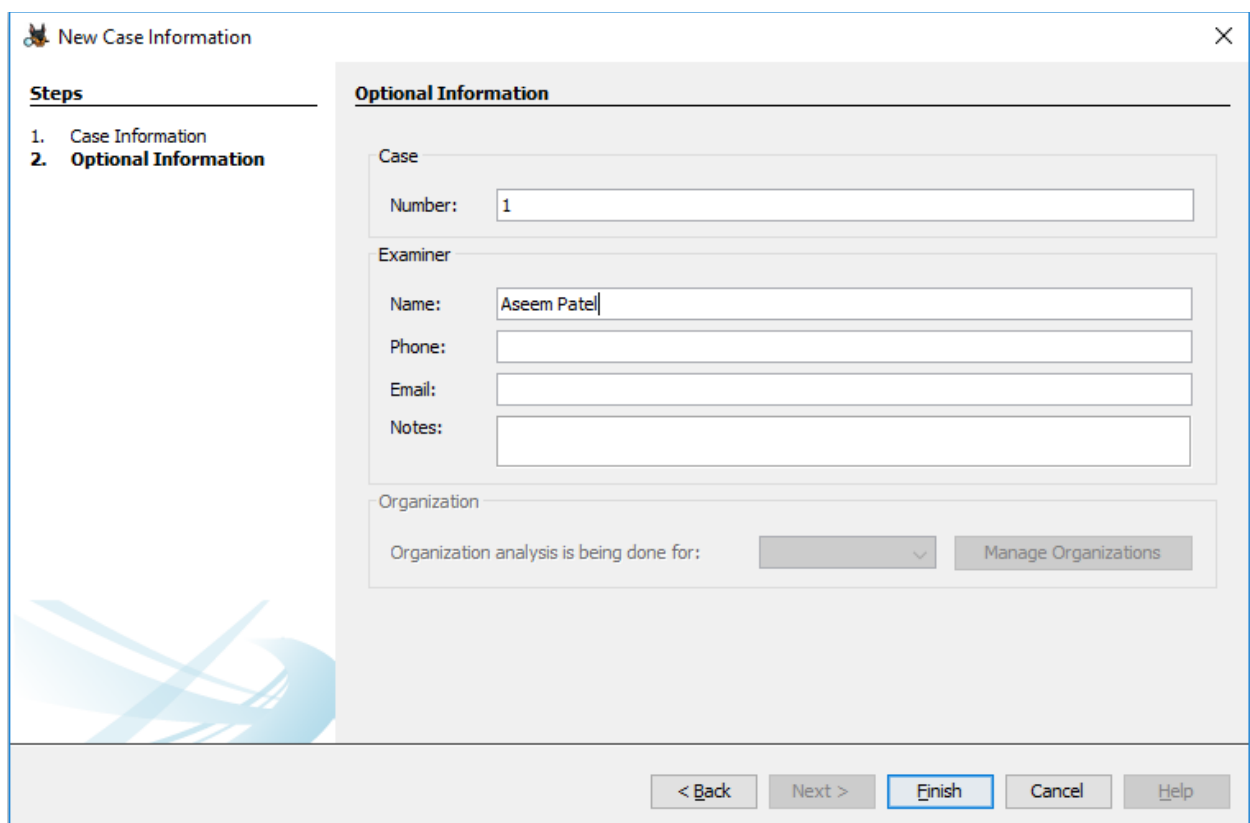


The dialog box is titled "New Case Information" and has a close button (X) in the top right corner. On the left, a "Steps" panel shows two steps: "1. Case Information" (which is bolded) and "2. Optional Information". The main area is titled "Case Information" and contains the following fields and controls:

- Case Name:** A text box containing "Exp-1Case-01".
- Base Directory:** A text box containing "C:\Users\OSOU-18\Downloads". To its right is a "Browse" button.
- Case Type:** Two radio buttons: "Single-user" (which is selected) and "Multi-user".
- Case data will be stored in the following directory:** A text box containing "C:\Users\OSOU-18\Downloads\Exp-1Case-01".

At the bottom of the dialog, there are five buttons: "< Back", "Next >", "Finish", "Cancel", and "Help".

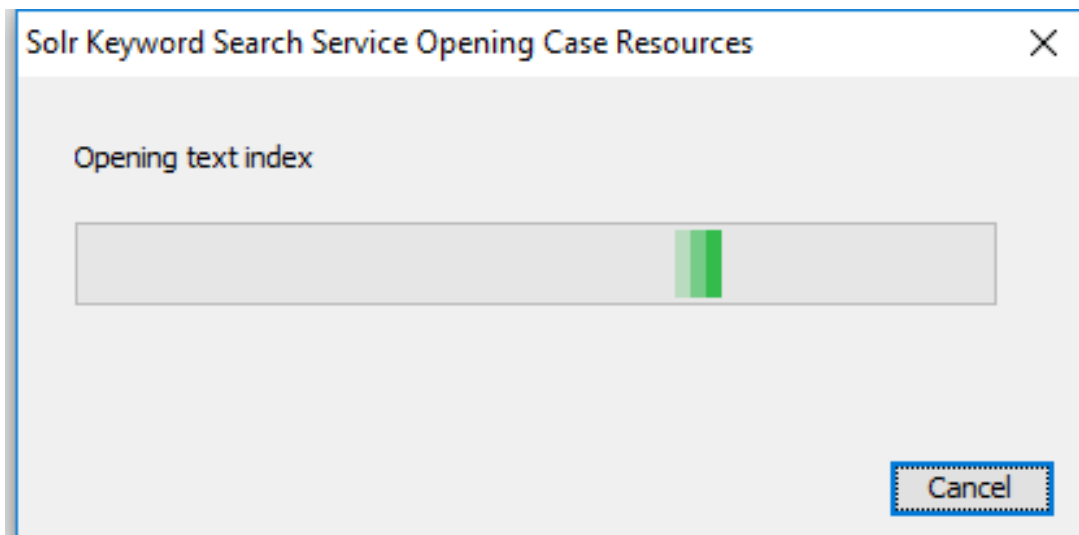
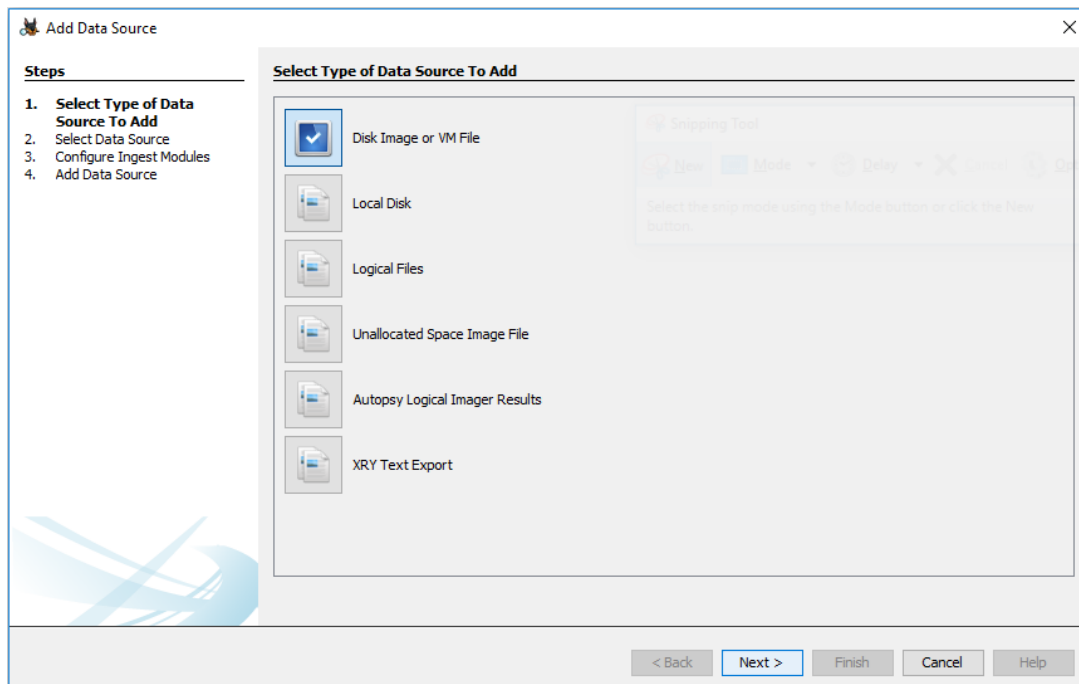
Here in the next step, you have to enter the case number and Examiner details and click on finish to proceed to the next step.



The dialog box is titled "New Case Information" and has a close button (X) in the top right corner. On the left, a "Steps" panel shows two steps: "1. Case Information" and "2. Optional Information" (which is bolded). The main area is titled "Optional Information" and contains the following fields and controls:

- Case:** A section containing a "Number:" label and a text box with the value "1".
- Examiner:** A section containing four labels and text boxes: "Name:" (with "Aseem Patel"), "Phone:", "Email:", and "Notes:".
- Organization:** A section containing a label "Organization analysis is being done for:" followed by a dropdown menu and a "Manage Organizations" button.

At the bottom of the dialog, there are five buttons: "< Back", "Next >", "Finish" (which is highlighted with a blue border), "Cancel", and "Help".



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.



**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 Data Source**

Path:

☒ Ignore orphan files in FAT file systems

Time zone:

Sector size:

Hash Values (optional):

MD5:

SHA-1:

SHA-256:

NOTE: These values will not be validated when the data source is added.

< Back   Next >   Finish   Cancel   Help

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.

**Add Data Source**

**Steps**

1. Select Type of Data Source To Add
2. Select Data Source
- 3. Configure Ingest Modules**
4. Add Data Source

**Configure Ingest Modules**

Run ingest modules on:

- ☒ Recent Activity
- ☒ Hash Lookup
- ☒ File Type Identification
- ☒ Extension Mismatch Detector
- ☒ Embedded File Extractor
- ☒ Exif Parser
- ☒ Keyword Search
- ☒ Email Parser
- ☒ Encryption Detection
- ☒ Interesting Files Identifier
- ☒ Correlation Engine
- ☒ PhotoRec Carver
- ☒ Virtual Machine Extractor
- ☒ Data Source Integrity

Select All   Deselect All   History

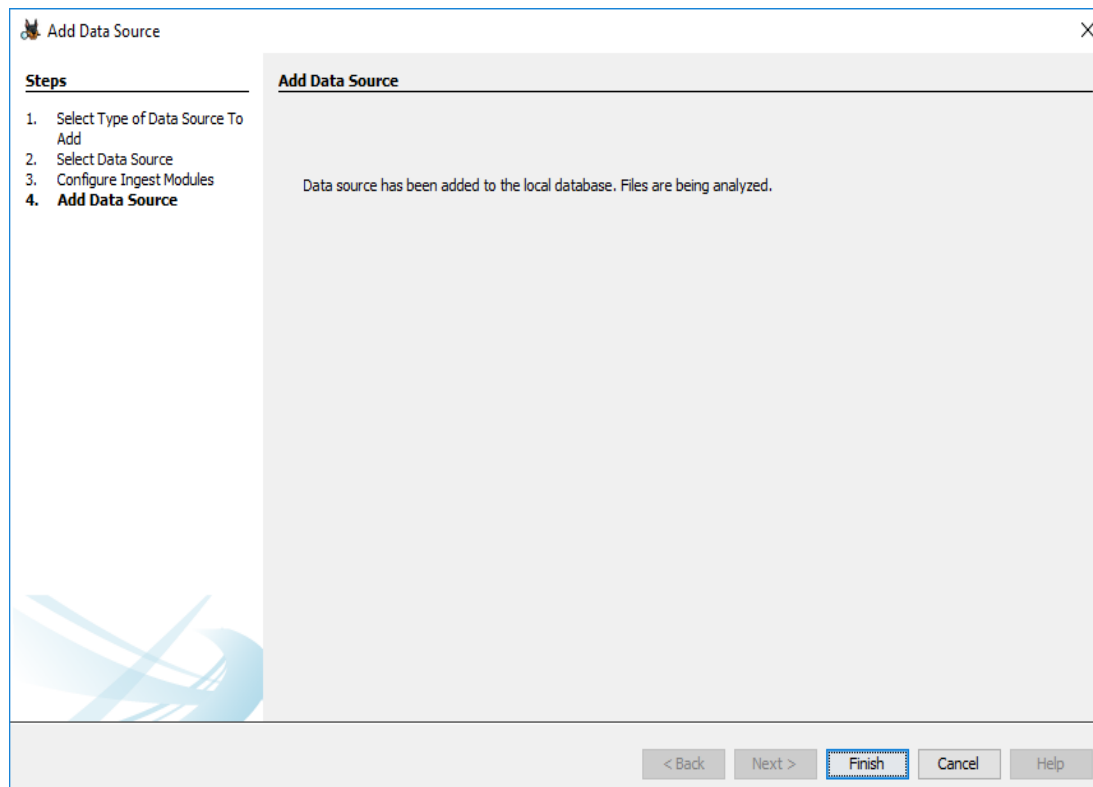
The selected module has no per-run settings.

Extracts recent user activity, such as Web browsing, recently us...

Global Settings

< Back   **Next >**   Finish   Cancel   Help

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/>