



COMPUTER FORENSIC INVESTIGATION GUIDE

Sachin Sathe
FORnSEC Solutions, Nagpur



INDEX

CHAPTER 1 – Introduction & Details about Computer Forensics.....	4
CHAPTER 2 – Types of Computer Crimes.....	18
CHAPTER 3 – Role of Cyber Forensics Investigator	26
CHAPTER 4 – Pointers in Reporting a Cyber Crime	34
CHAPTER 5 – Details about Investigating Computer Crime	35
CHAPTER 6 – Rules of Evidence	44
CHAPTER 7 – Computer Forensics Hardware	46
CHAPTER 8 – Windows Forensics	58
CHAPTER 9 – Network Forensics, Investigating Logs and Investigating Network Traffic	65
CHAPTER 10 – Investigating Wireless Attacks & Forensics	70
CHAPTER 11 – Investigating Web Attacks & Forensics	73
CHAPTER 12 – Tracking Emails and Investigating Email Crimes & Forensics	76
CHAPTER 13 – Mobile Forensics	79
CHAPTER 14 – Cyber Forensic Investigative Reports & Documents	83
CHAPTER 15 – Becoming an Expert Witness.....	93

INTRODUCTION

What is a computer? What is Internet? These questions are very well-known amongst the individuals now a days!! and the answer to these questions can be given by a child too...But with the increase in the advance technology computer crimes are also increasing ,computer crimes such as cyber terrorism , identity theft , hacking and many more. To counteract those computer-related crimes, Computer Forensics plays a very major role.

A Computer Forensic Investigation generally investigates the data that can be extracted from the computer , hard disk or any other digital storage device.

Here with the computer forensic investigation , and to conduct the investigation computer forensic investigators play an important role.They conduct the forensic analysis by using various methodologies (e.g. Static and Dynamic) and tools (e.g. FTK & Encase) to ensure the computer network system is secure in an organization. A successful forensic investigator must be familiar with various laws and regulations related to the computer crimes in their specific country. There are also many more things in cyber forensic investigation so,**I have decided to make a white paper tutorial, this tutorial includes the cyber forensic investigation processes.**

Here in this white paper tutorial, you will get detailed information about the cyber forensic, their subfields , how to conduct an investigation, I have collected and accumulated the data into this one tutorial, which would be beneficial to carry out the investigations.

SO, LET'S GET STARTED!

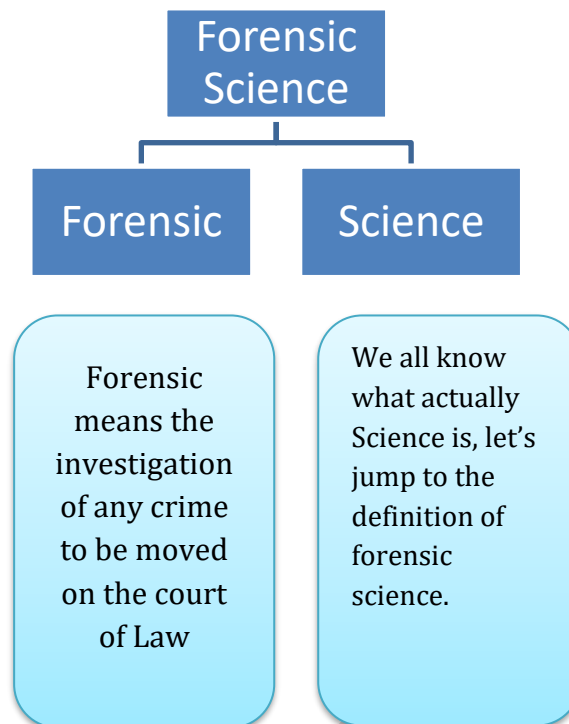
Chapter: 1

“Introduction and Details about Computer Forensics”



Forensic Science

To Understand Forensic Science, First Let's just divide this word as



So here we are, **“Forensic Science is the term which is used to describe the use of various Applications & Techniques to investigate a crime for the purpose of the law.”**

“Let’s Understand Computer Forensic”

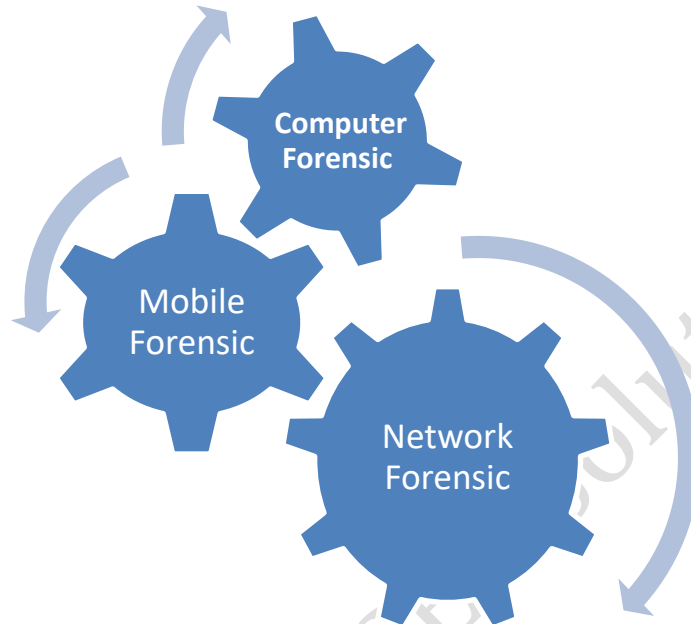
We all know that Forensic science is the investigation of any crime which needs to be proved in the court of law.

So, “**Computer Forensic is the investigation of computer-related crime, more precisely; Computer Forensic is the use of various process and procedures for the investigation that are related to the computers.**”

Let me also tell you that computer forensic is also known as

Cyber Forensic.

Cyber forensic is further divided into three categories:-



Computer Forensic: - Crime that is carried out with the use of computers than the investigation is termed as computer forensic..

Mobile Forensic: - If any crime is carried out using the mobile device then the investigation is specified as mobile forensics.

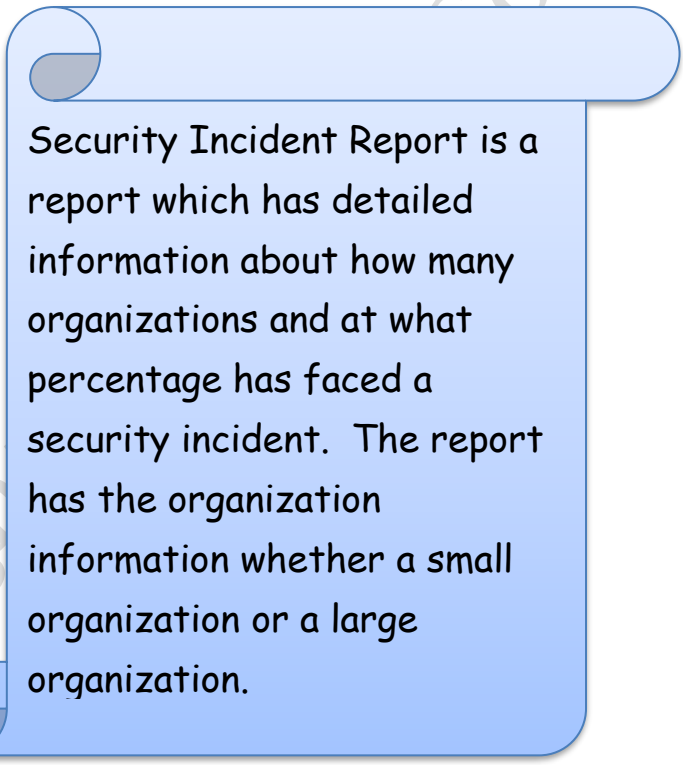
Network Forensic: - The investigation which is carried out to investigate the network logs and network traffics is known as network forensics.

What is a security Incident Report?

First of all, let's understand the security incident.

“An incident which has taken place in an organization harming it's system or data and the protection system has been failed to protect it is termed as a security incident.”

For Example - Hacking company site.



Security Incident Report is a report which has detailed information about how many organizations and at what percentage has faced a security incident. The report has the organization information whether a small organization or a large organization.

Details of the information included in the Security Incident Report are:

- Organization name: - Small and large organizations.
- Percentage of the security incident.
- The number of employees in the organization.
- Type of security incident.

What are the aspects of organizational security?

Aspects of organizational Security are:-

- 1) **Organization:** This stage focuses on the Organizational security policy and its implementation.
- 2) **Employee Security Focus:** This stage focuses on the security awareness of the Employees and their training.
- 3) **Change Management:** This stage focuses on any physical & virtual modifications from a security point of view.
- 4) **Network Security:** This stage focuses on the security related to the Network.
- 5) **Application Security:** This stage focuses on the security related to Applications and Data.
- 6) **System Security:** This stage focuses on how vulnerable the existing system is Identity
- 7) **Management:** This stage focuses on Account & Password management.
- 8) **Event Management:** This stage focuses on Event Monitoring, Incidents & Disaster cases.
- 9) **Asset Security:** This stage focuses on the verification of Hardware from a security point of view.

How do computer forensic evolve?

I think it would be very difficult to point out the evolution of computer forensics.

According to the Computer Forensics recruiter.com most experts agree that the field of computer forensics began to evolve more than 30 years ago. The field began in the United States, in large part, when law enforcement and military investigators started seeing criminals get technical.

Over the next decades, and up to today, the field has exploded. The Law enforcement and the military continue to have a very large presence in the cyber forensics field at the local, state, and also federal level. Various private organizations have been started to investigate the computer related crimes and also to spread awareness related to computer forensic and computer security.



The objective of Computer Forensics

The very first objective of computer forensic is to recover, analyze and preserve the pieces of evidence related to the computers in such a way that it can be presented in the court of law.

The second objective is to identify the perpetrator/hacker/attacker and the loss caused due to the attack.

The third objective is to generate a proper report to be submitted in the court of law.

Urgent need for computer forensics

To maintain data integrity of the organisation system and network.

To protect the data of an organization.

To save the organization from loss.

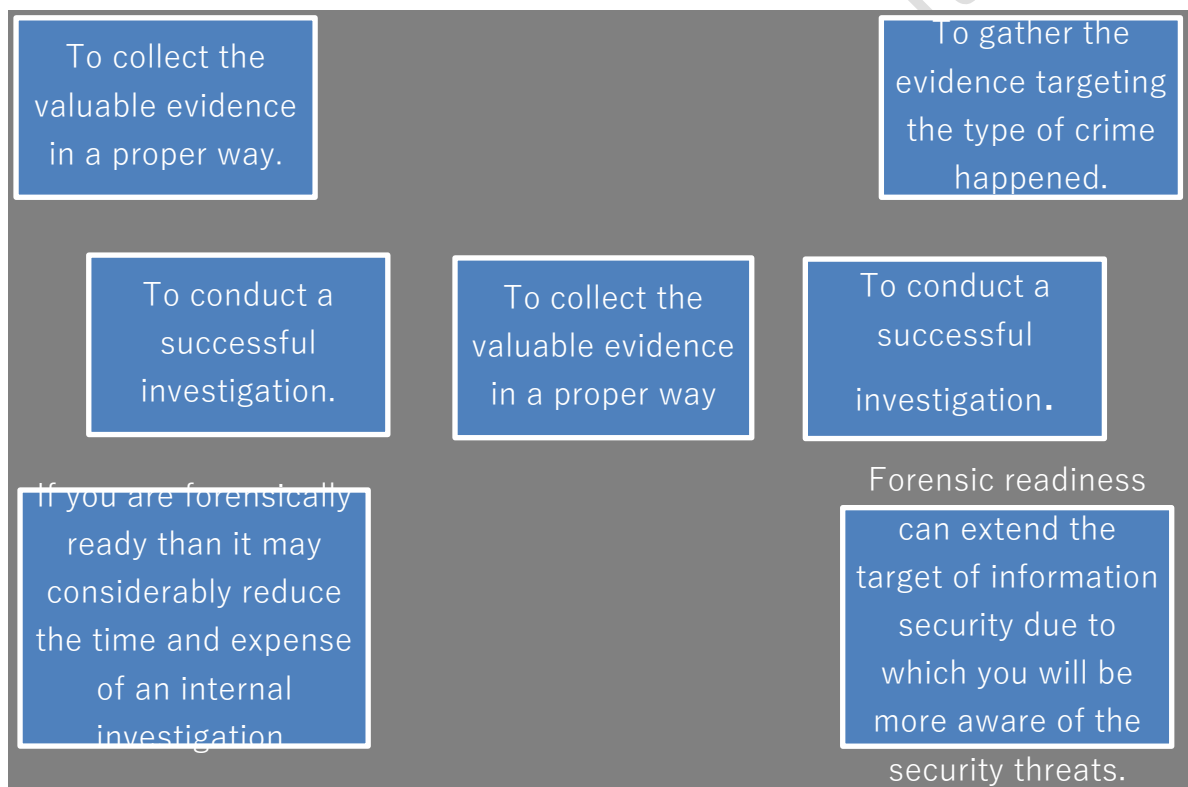
To prove the crime in court of law, maintain chain of custody .

Forensic Readiness....

Forensic readiness is the phenomenon of **getting ready or fully prepared before going on to the cyber forensic investigation.**

To conduct the forensic investigation in a fast and effective manner **“An organization must have the forensic readiness”**

Benefits



Here we have learned about computer forensics, Now, Let's move on to cybercrime...

What is a cybercrime?

“

Cybercrime is defined as any illegal activity which involves the use of computer or network. The computers or network may be used as a tool or the target to commit a crime.”



Mode of Attacks/ Techniques of Cyber Crimes:

- 1) **Computer Viruses and Worms** - Virus is a malicious program that can cause damage to the computer. It can replicate by itself that can produce its own code by attaching copies of itself to other files. The virus can corrupt or delete the data. The worm is a special type of virus that can replicate itself and use memory but cannot attach itself to other programs. It causes the system to slow down. A worm spreads itself into the network, automatically.
- 2) **Phishing / Spoofing** - This attack is the fast-growing online scam. In this type of attack, a cybercriminal creates a fake website page which looks real and is usually sent via email and marks as a trustworthy organization. This technique is called phishing. The cybercriminal may also send you a lottery email and ask for your details like credit card details, bank account details, and other such information.
- 3) **Denial of Service Attack** -This attack is a technique that makes the website or service unavailable. Typically, this is achieved by using multiple computers by repeatedly making requests that make the site or a network down. This type of attack might stop your website from functioning temporarily or permanently and may result in data and financial loss.
- 4) **Social Engineering** - It is a method where cyber criminals make use of emails or phone calls. They try to gain your confidence and assert as a real identity and get the information they need. This information can

be about your bank account details, money, your company or anything that can be useful to cybercriminals.

- 5) **Identity Theft**- The term Identity Theft is used, when a person intends to be some other person to do fraud for financial gains. The most usual source to steal identity information of others is from data breaches of private, government or federal websites that contain financial details.

Computer-Facilitated Crime/Types of Crime

- 1) **Financial Crime** - Financial crimes, as the name suggests, are committed for financial gain.
- 2) **Information Theft**- For any organization, information is the main asset of the company. Theft information can range from revenge to industrial spying. Such thefts are growing phenomenally over the past few years.
- 3) **Cyber Extortion**- Cyber extortion is a crime involving an attack or threat of attack against an enterprise, generally using Denial of Service attacks (DoS) or other kinds of attacks.
- 4) **Harassment** -The virtual harassment has risen up heavily. Thousands of social networking harassment cases are registered every day. Harassment is generally done to women but can also be aimed at a specific group involving race or religion and so on.
- 5) **Cyber Stalking** - Cyberstalking means pursuing a person's movements on the internet and posting email messages, chat rooms, social media and any other online medium that bombard him/her on the sites she

frequently visits. By collecting sufficient personal details about the person, they plan for the harassment.

- 6) **Intellectual Property Theft** - It means the ownership of rights related to software, copyrights, trademarks, and other such intangible assets. When these rights of the owner are deprived of completely or partially, it is said to be an Intellectual Property Rights (IPR).
- 7) **Computer Vandalism** - It leads to any physical computer harm or its parts are called Computer Vandalism.
- 8) **Email Bombing**-Email bombing is the phenomenon of sending huge/bulk emails to the victim in an attempt to overflow the inbox of the victim.
- 9) **Software Piracy:-** Software piracy is the illegal copying, distribution, or use of the software.
- 10) **Phishing /Spoofing:-** Phishing is the fraudulent attempt to obtain sensitive information such as usernames, passwords, and credit card details by disguising as a trustworthy entity in electronic communication.
- 11) **Credit-Card Fraud:-** Credit card fraud is a form of identity theft in which an individual uses someone else's credit card information to charge purchases, or to withdraw funds from the account.

Chapter 2

“Types of Computer Crimes”



Who can be cybercriminals?

“ A criminal who commits a crime with the use of digital devices are termed as cybercriminals.

He can use a mobile phone, internet, computer or any digital device.”

What is an organized cybercrime?

To commit a crime, we need a full proof plan right?

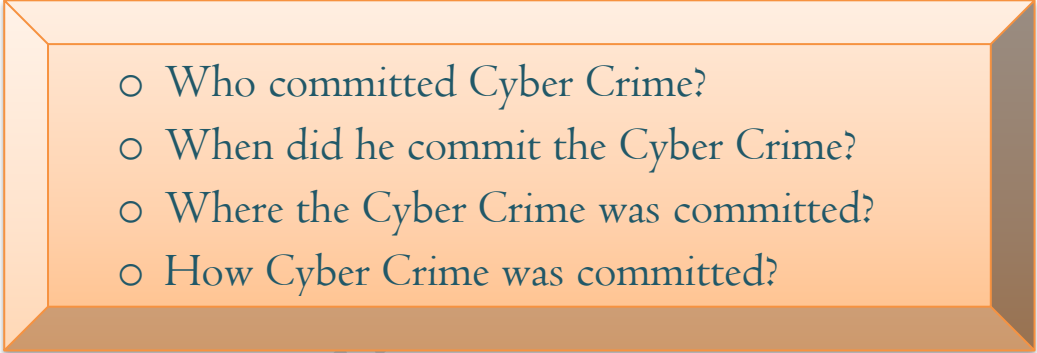
“ So organized cybercrime is a crime which is committed by a group of people or an individual while collecting the victim's information (full information.) More precisely organized cybercrime is committed with the full organization, with a full plan, such as

- ❖ How to commit crimes?
- ❖ When to commit?
- ❖ Where to commit?
- ❖ How serious are different types of incidents?

What is a cyber-crime investigation?

As we have discussed more on cyber-crime, I think we are clear with the concept of Cyber-crime. So here if **cyber-crime has happened** then it is **mandatory to investigate the cybercrime to find out the culprit** behind the crime, This **process is being called Cyber Crime Investigation**.

In Cyber Crime Investigation it is very crucial to find out the answer to these questions:-

- 
- Who committed Cyber Crime?
 - When did he commit the Cyber Crime?
 - Where the Cyber Crime was committed?
 - How Cyber Crime was committed?

“The Cyber Crimes Investigation includes a very detailed procedure, processes to find out the culprit behind the crimes.”

For the investigation process, there are many things which need to be kept in mind such as:

- ✓ Not to destroy the evidence.
- ✓ Collect as much as information.
- ✓ Do the investigation in forensic sound Condition.

The Cyber Crime Investigation is a very crucial and sensitive process where we need to handle evidences in a proper manner. Because the **digital evidence is the only evidence which makes a pull to have a link between crimes, suspect, victims and crime scenes.**

Key steps in the cyber forensic investigation

Step 1.

Collect primary level information from the complainant.

Step 2

Find out the preliminary level evidence, more preciously, collect evidence related to crime for further investigation.

Step 3.

Obtain permission from the higher Officials or Court

Step 4.

Performed the first responder procedure.

Step 5

Calculate the hash value of digital evidence

Step 6

Make bitstream copy of the evidence.

Step 7.

Seize the evidence in a proper manner.

Step 8.

Maintain the chain of custody (Proper Document and Procedure).

Step 9.

Send it secondary copy to the lab for further investigation.

Step 10.

Analysis and Reporting of data.

Step 11

Submit the forensic report.

Step12:

If required testify as an expert witness.

**Additional
Comments for the
steps:-**

Step 3 :-Obtain Search Warrant

(when and Investigating officer can take the permission?- if the IO thinks that he needs to go to the Crime scene for further investigation such as to collect more evidence.)

Step 4:- Performed the first responder procedure.

The first responder procedure is as:

- a. Keep the user away from the computer.
- b. Photograph the crime scene.
- c. Count and label the attached accessories to the computer.

If the computer is in 'ON' state than run the first responder tool to collect the information of the computer.

-If the computer is in 'OFF' state than detach the hard drive from the computer.

Rules of Cyber Forensic Investigation

As mentioned earlier that during the cyber forensic investigation we need to follow various rules procedure and processes.

The rules of Cyber forensic investigation are as follows:

- ✓ The very first rule is not to temper the original evidence.
- ✓ Maintain proper documentation of each and every step taken.
- ✓ Calculate the proper hash value.
- ✓ After the investigation keeps the evidence in a secure condition.
- ✓ Handle the digital evidence with Care, as it is very fragile in nature.

Need for Cyber forensic investigation

- Cyber forensic investigation is a very sensitive procedure which requires only skilled person to do the investigation.
- If the investigation is conducted with a non-technical person then it may result in the tampering of evidence which may directly affect the case.



Chapter 3

“Role of Cyber Forensic Investigator”



Obtain search consent/ warrant to investigate

To conduct a successful investigation it is important to have a warrant because with warrant we can have an investigation in a more precise manner.

We can obtain the search warrant as:-

1. If we want to have an investigation for an ordinary person/organisation then we can get direct permission from the higher authorities.
2. If we want to have an investigation for a big personality/organisation then we need to go to the court with the preliminary evidence to obtain the search warrant.

Computer Forensic Resources:-

Obtaining computer forensic resources would be a very simple task, but it also needs dedication and great research work.

As, we have a very important thing with us, in essence “ **Internet**”, so here we go on we are very first resource.

I. The Internet is the world of information, the Universe of information. With the help of the internet, we can get information related to computer forensics. The Internet is a huge platform related to getting the information related to Cyber Forensic

As it is said that talking therapy is the best to relieve pain or to make someone happy.

So why not use this talking therapy in obtaining information related to computer forensics.

So, the next point here we can say as:

2) Rather than getting information from the internet we can join groups or can take information from our higher authorities. The person who is having numerous knowledge of computer forensics. We can contact them and get the information related to the computer forensics. For this, we can join groups, join the network (a network of higher authorities.)

Role of digital evidence collection and preservation

“The main aim behind cyber-crime investigation is finding the culprit behind the Crime. So to find out the culprit behind the crimes we need evidence.”

“Because in the cyber-crime investigation, digital evidence plays a major role”

Digital evidence creates a link between them



With the digital evidence, we can determine whether -

- ❖ Who committed crimes?
- ❖ When did he commit the Crime?
- ❖ How did he commit the crimes?

Through this, we can understand that digital evidence plays a very important role in detecting crimes.

As we know that digital evidence is very fragile in nature, they may get easily destroyed. Here it is the duty of the cyber forensic investigator to collect the evidence properly and preserve them in a proper way.

Corporate investigation & and understanding computer science.

Corporate investigation: - The word itself provides us with the definition that is the “investigation of Corporates” Now here the question arises why do we need to do the corporate investigation? Here I would like to explain this with a Case Study

Case Study:-

The xyz own a company, he is having a small organization with 50-150 employees. As it is predefined that according to the employee capability, various tasks are assigned to them. But one-day XYZ comes to know his company information from an outsider, he was in doubt that from where his information is transformed. So he decides to contact one of the cyber forensic Investigation Agency to do the forensic investigation of his company. Thereafter the team of cyber forensic investigator visits the company and started with the investigation. They started with the investigation/ looking/ checking the computers of the employees, they checked their email ID's, their OS, browsing history, and many other things. So here they got a clue that one of the company employees was transferring the detail to some other company. Here this particular process is Corporate Investigation

Here we get our simpler definition **for Corporate Investigation that is the process of investigation or scrutinizing the asset of the corporate to find out the culprit behind any crime related to that company.**

What are the instructions for the forensic investigator to approach the cyber scene?

Our main aim to visit the crime scene is collecting the evidence, preserving them and obtaining information, from the evidence.

First of all our duty to provide the material required for the investigation to investigate such as training suit, gloves, badges, tags etc.

Here are some of the instructions to be given to the investigators.

1. Firstly wear the forensic Suite which has gloves, mask, boots etc .
2. Observe the crime scene with an Eagle Eye.
3. Protect the Crime Scene and remove unnecessary people from the Crime scene.
 - ❖ If indoor Crime scene: - then protect the Crime scene with the Crime Scene tapes.
 - ❖ If outdoor Crime scene: - then protect the Crime scene with the barricades or if barricades are not present then we can use vehicles.
4. Have a look to the victim:-
 - ❖ If the victim is dead: - then sketch the body and transport it to the laboratory
 - ❖ If the victim is alive: - immediately give medication to the victims, call the ambulance and admit him to the hospital.
5. Photograph the whole Crime scene.
6. Do not tamper the evidence.
7. Collect the evidence in a proper way with the collection tools.
8. After the collection of evidence transport them in a laboratory for further investigation.

Why and when do you use computer forensics?

If a cyber-crime has happened we need to do the investigation, hence we will use computer forensics to find out the culprit behind the crime.

Enterprise theory of Investigation:-

Criminals commit crime in a group, so the individual commits crime to benefit their enterprise/group. The Enterprise Theory of investigation tell us about to take actions against enterprise/group rather than individual. Because of the ETI , Law enforcement Agency can target and dismantle the entire criminal enterprise/group.

Understanding Legal Issues

When a cyber-forensic investigator investigates crime, he should have the knowledge of legal issues, he should be aware of policies and sections such as IPC, CRPC, IT Act, and Federal rules.

For example: - If cyber forensic investigator is investigating crime and the crime is of computer vandalism then he needs to associate that crime to the particular sections.

How to do reporting of results in compliance with policy and laws.

The report should contain the detailed information such as summary, conclusion, observation.

The report is based on who has accessed the data, what modifications are made , how was it available to investigate.

A perfect investigation report contains:-

- ✓ Summary
- ✓ Method of investigation
- ✓ Tools used during Investigation
- ✓ Comments
- ✓ Graphs
- ✓ Attachments
- ✓ Conclusions

Chapter 4

“Points in Reporting Cyber Crime”



Why you should report Cyber-Crime?

"Do not endure cyber-crime, fight against, cyber-crime"

If a person is a victim of Cyber Crime, he should definitely report cyber-crime as it is said that

- Stop Cyber Crime.
- Fight against Cyber Crime.
- Every criminal who is committing a crime should get to know that what he/she has done to the person.
- While Reporting cyber-crime you will be a step towards stopping cyber-crime.
- If a person is reporting a crime, then he is protecting the lives of others.

When, how, and to whom one should report the computer-related crime.

If you are a victim of cybercrime than:-

- Consult any private cyber forensic investigator.
- Report the crime to the nearest cyber-crime cell.
- Carry the necessary evidence such as screenshots, mobile number etc. with you while reporting the crime to the private investigator or cyber cell if needed.

To whom you can report cyber-crime?

- Firstly you can report to a private cyber forensic investigator.
- A person who is having great knowledge of Cyber forensic investigation such as If reporting to Cyber Cell then there are the people who are having knowledge of Cyber forensic investigation.
- You can also contact the local authority or the police officers as per your jurisdiction.

Copyright-FoRnSEC Solutions

Chapter 5

“The Details about Investigating Computer Crime need to Know Before the Investigation”



How to build a forensic workstation?

While in the previous section we have learned about cyber-crime, cyber-crime investigation, but **going to the investigation is a big task for the**

investigator because they need to be prepared for the investigation, with proper tools policies procedures and many more.

So let's learn about this deeply.

1) Build a workstation

The workstation is all about the place and the computer on which the investigation is to be conducted. The Forensic workstation should be a well-equipped workstation. It should have the forensic software which are required in the investigation process. The Software and Hardware should be able to detect in storage devices, also they should be able to make the bit stream copies of the devices. The workstation should be facilitated with all the necessary software, Hardware's, cables.

2) Building the investigation team

.....that is people to be involved in computer forensics.

Now once we are ready with the workstation, now we need to have an investigating team which will do the investigation computer forensic. There are many members who are in the investigating team.

So now let's identify the people who are involved in computer forensic investigation. We should have the member who is having the knowledge of Cyber forensic investigation and good thinking capability (Person Involved).

3) The person who are involved in an investigating team

1. **Photographer:** - Able to photograph the Crime scene.
2. **Sketcher:** - Able to sketch the Cyber Scene.
3. **Documenters:** - Who can document each and every activity related to the crime scene.
4. **Examiner:** - Who can examine the digital evidence.
5. **Attorney:** - Who can give legal advice.
6. **Evidence Manager:** - Who Manages Evidence.
7. **Cyber forensic expert:** - Gives suggestion about the cyber forensic investigation and can investigate too.
8. **Expert Witness:** - Can do a formal opinion in the court of law.

Now, here if we are having an investigating team than it is important that they should have knowledge of Cyber forensic investigation, but with this, this world also knows the policies and laws related to Cyber forensic investigation.

4) Review policy and laws of Cyber forensic

The cyber forensic investigating Team should be able to understand the laws and policies.

- They should be aware of, the policies such as not to harm or damage any computer or Digital device.
- If they are not aware of the laws, they should consult and legal advisor.
- If in case, some laws and policies are not made then notify decision makers.

5) Notify decision makers

- You can notify the decision makers about an incident.
- Now, who are the decision makers?
- The decision maker is the person who makes policy and procedure which should be applied to an incident.
- If policy or procedure is not made for an incident then you should notify the authorized decision makers.
- After authorization determine the course of the incident which incident took place.
- once the incident is determined the decision makers can start making the policies in respect to the incident
- While making the policies the point which should be kept in mind is just assessment.
- Risk assessment is all about identifying the risk caused by an incident or the problem caused by the incident.
- Once the incident is identified, identify the damage caused by the incident, to which extend the damage has been caused.

{ After, making an investigating team we need to have the
“Computer Investigating Toolkit”. }

6) Computer Investigation Toolkit

- The computer investigating toolkit is provided to the cyber forensic investigator to do the investigation of computer-related crimes.
- The tool kit consists of a laptop, which has all software in it, storage devices such as hard disk, pen drive, CD 's, DVD's, cable connections, hardware, notepads, write protection tools or write protected backup device.
- The cyber forensic investigation toolkit help us to do the investigation in a more precise way

{ When an investigator investigates the crime there are also
some step which the investigator should always keep in
mind }

7) Steps for Computer Forensic Investigation

The steps are as:-

1. The investigator should have the knowledge of Cyber forensic investigation such as how to handle the evidences.
2. Collect all the preliminary evidence present at the Crime scene.
3. Collect information about the computer such as the operating system.
4. Check for each and every file in the computers.
5. Check for stenographic images/ Files.
6. Also, do check for any password protected or encrypted files.
7. Collect the valuable information such as the email addresses or list of account login, this may be valuable in cyber forensic investigation.
8. Maintain or record each and every information such as maintain the chain of custody.

“Let’s have a glance at the Computer Forensic Investigation Methodology.”

8) Methodology for Computer Forensic Investigation

The methodology for cyber-crime investigation is:-

1. Ask for the preliminary information about the case.
2. Collect the primary level evidence.
3. Obtain search warrant.
4. Perform the first responder procedure.
5. Calculate the hash value of digital evidence.
6. Create bit stream copy of evidence.
7. Seize the evidence.
8. Maintain chain of custody.
9. Send to laboratory for investigation.
10. Analyse and reporting of data.
11. Submit forensic report.
12. It requires justify as an expert witness.

Chapter 6

“Rules Of Evidence”



Rule of Evidence

The law of evidence, also known as the rules of evidence, includes the rules and legal principles that govern the proof of facts in a legal proceeding.

These rules help to determine what evidences must or must not be considered in the court of Law. The rules varies depending upon whether the venue is a criminal court, civil court, or family court, and they vary by jurisdiction.

The International Organization on Computer Evidence (IOCE) was formed on 1995 .It provides an international forum for the LEA to exchange information related to the computer evidence.

The Scientific Working Group on Digital Evidence (SWGDE)

This group brings together various organizations which are engaged in the field of computers , digital evidences. SWGDE also provides guidance to the digital forensic community through the publication of standards, guidelines, and best practices on its website. SWGDE also encourages a number of its published documents that can be used by various standard developing organizations such as (e.g. ASTM International).

Chapter 7

“Computer Forensic Lab”



Requirement & steps in setting up a Cyber-Forensic Lab

For Cyber Forensic Investigation we need to have a **Cyber-Forensic lab**.

“The Cyber Forensic is a lab which is equipped with the cyber Forensic tools through which we can commence the investigation. As it is said that conduct the investigation in **“Forensically sound Condition. Forensically Sound condition itself means having investigation in a cyber-forensic lab”**

The requirement for setting up a lab

1. Area / Place (Secured Place).
2. Structural Design.
3. 24-Hour Electricity / Power Backup.
4. 24- Net Connect.
5. Communication.
6. Ambience of Lab.
7. Physical Security.
8. Fire Suppression.
9. CCTV Surveillance
10. Cyber Forensic Investigation Team
11. Obtain License

Steps in setting up a Cyber Forensic Lab.

Step I:- Area / Place

- Firstly, we need to decide a place where we need to set up a Cyber Forensic Lab.
- The Place Should be Secured, it should be situated in a place where there is no danger such as it should not be the area criminals.
- Decide an area which is secured & set up a lab there itself.

Step 2:- Structure Design

- The structured design of a lab is accomplished according to the requirement.

Step 3:- CCTV Surveillance

- Once you have decided a place & had constructed the lab than we need to have the CCTV Surveillance.
- It is very important to have CCTV camera in your building to notice each & every one of your premises & your team.

Step 4:- Fire suppression

- Fire Suppression is one of the major aspects in Cyber forensic lab setting.
- It is also one of the aspect of Security.
- Every lab & office should have fire Suppression.

Step 5: - 24 Hours Electricity/24 Hours Power backup.

- A Cyber Forensic Lab requires 24 hours electricity supply so that the investigations are not disturbed.

Step 6:- 24 Hours Net Connection.

- A Cyber Forensic Lab requires 24 hours net connection because some of the investigation requires high speed net.(this net connection should not be made available to the workstations.)

Step 7:- Communication Lines

- Communication Lines should be available in a cyber-forensic lab to have communication with the other members

Step 8 :- Ambience of Lab.

- As the Cyber Forensic Investigators will be working in the lab, they would be needing a pleasant Environment to work.
- Always keep in mind to have Simple wall Paints, Should not use bright Points.

Step 9:- Physical Security

- Have Security guards in the premises in the entry point and exit point.
- Always have a log book to mention the list of visitors their entry time and exit time.

Step 10:- Obtain License

We need to have a license from the licensing authority to run a lab.

Step 11:- Setting Up a team

The Team will have

- 1) Director.
- 2) Lawyer.
- 3) Investigator.
- 4) Cyber forensic Expert.

The Director will be the main person in the Lab. The Lab Director the lab should have Cyber Forensic Investigator, Cyber Forensic Expert, and a lawyer.

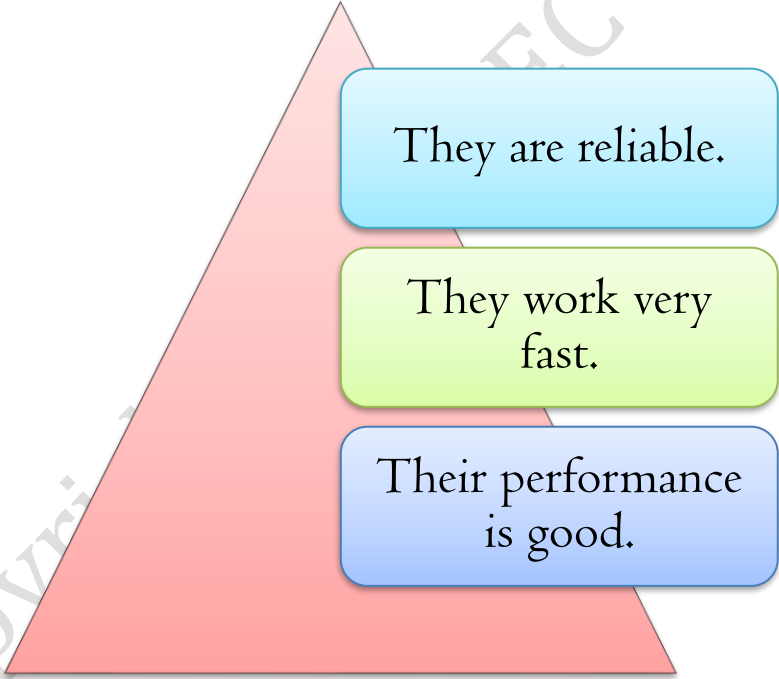
Let's understand the hardware and software that are required in a Cyber Forensic Lab

1) Computer Forensic Hardware

Why do we use Cyber Forensic Hardware?

Computer Forensic Hardware are the tools which we use during the Cyber Forensic Investigation.

The Uses / Advantages of Cyber Forensic Hardware are



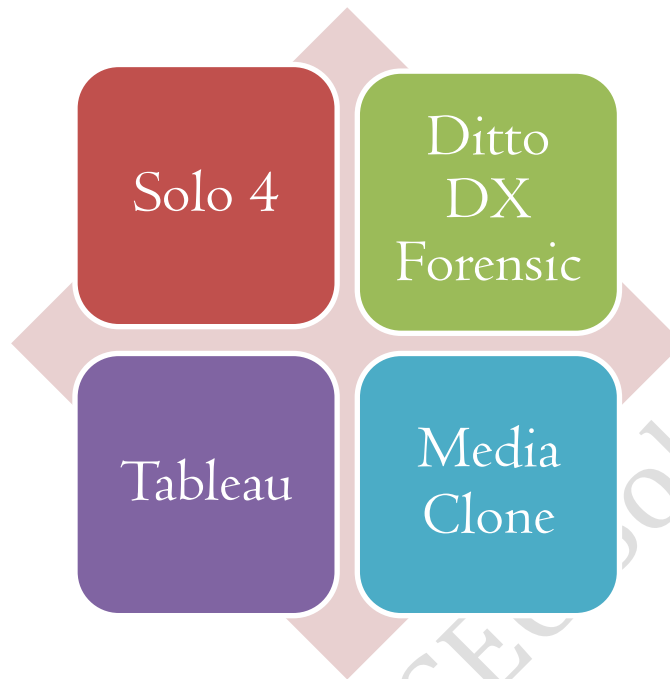
They are reliable.

They work very fast.

Their performance is good.

Types of Cyber Forensic Hardware are

Hard Disk Cloning and imaging Hardware



Hard Disk Overview



“A Hard drive is basically a storage device in which we can store various information. We can store images, videos, audio, and many more.”

Let's begin with starting the parts of a hard drive.

A hard drive has only a few basic parts. The information is stored on the shiny silver platters, there's an arm mechanism that moves a tiny magnet called a read-write head back and forth over the platters to record or store information, and also there's an electronic circuit to control everything and act as a link between the hard drive and the rest of your computer.

Parts of Hard Disk

1. The actuator that moves the read-write arm.
2. A Read-write arm that swings read-write head back and forth across the platter.
3. A Central spindle that allows platter to rotate at high speed.
4. A Magnetic platter that stores information in binary form.
5. Plug connections link hard drive to the circuit board in the personal computer.
6. A Read-write head which is a tiny magnet on the end of the read-write arm.
7. A Circuit board is present underside that controls the flow of data to and from the platter.
8. A Flexible connector is present that carries data from the circuit board to read-write head and platter.
9. A Small spindle that allows the read-write arm to swing across the platter

Structure of Hard disk

As with floppy disks, every platter is divided into thin concentric bands that are known as tracks. There can be more than a thousand tracks on a hard disk. These tracks are further subdivided into sectors. These are the smallest physical storage unit on a hard disk and they are almost 512 bytes long.

A group of tracks which have the same track number, are referred to as a cylinder.

The Tracks are created when the hard disk is formatted. Occasionally there are 1024 tracks on a hard disk, numbered from 0 (at the edge of the disk) to 1023 (near the centre).

One side of the first platter of the hard disk has space reserved for hardware-based track-positioning information which is not available to the operating system.

{Here let us now jump to our next topic that is the types of hard disk or the hard disk interface.}

Hard Disk Interface (Port/ Interface)

Let's start understanding the interfaces of the hard disk.

Parallel ATA (PATA, also called IDE or EIDE):- ATA is a common interface which is used in many personal computers .It is the least expensive of the interfaces.

Serial ATA (SATA): -SATA is basically an advancement of ATA

SCSI (Small computer system interface):- SCSI is commonly used in servers, and more in industrial applications.

Serial Attached SCSI (SAS):- This is an interface which is used for data transfer

Computer Forensic Software

Hard Disk Cloning and Imaging

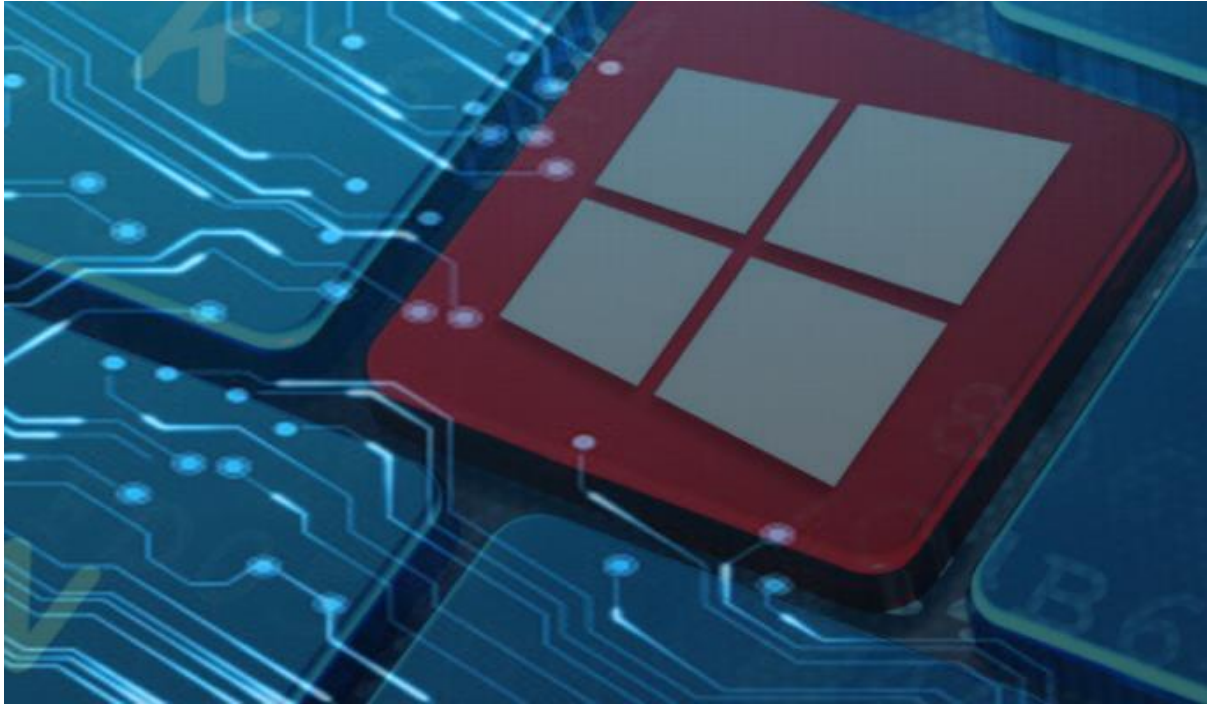
- Prodiscover.
- FTK.
- Encase.
- Forensic Replicator.

Hard Disk Analysis Software

- X-ways Forensics
- IEF
- FTK
- Encase
- P2 Explore
- Sleuth Kit
- Prodiscover

Chapter 8

“Windows forensic”



The question here is what is actually windows forensic?

Let us understand this with a simple definition.

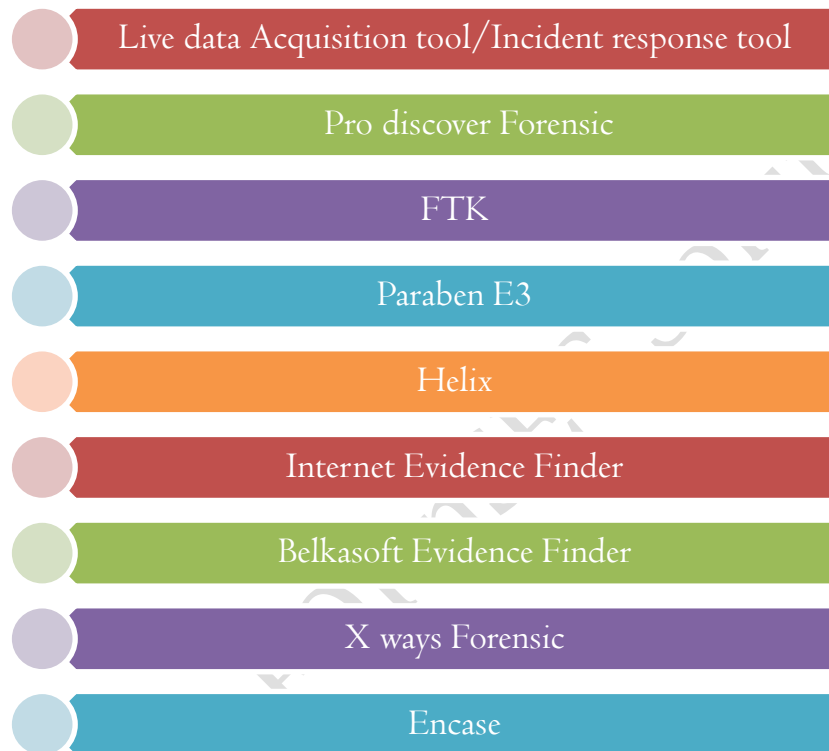
“

The study of computer forensic investigation under the windows platform to perform live analysis, capture volatile data, make an image of media, analyze file system, analyze network traffic, analyze the file, perform memory analysis and also

”

analyze malware.

In windows forensic investigation process we also look towards the cache, cookies and history analysis, Hash value calculation, windows password issue, Event log analysis, metadata investigation, and windows file analysis. For the different type of data investigation, we use various tools some of the tools are:-



Data Acquisition and duplication

{Data Acquisition is the process of gathering information from digital devices, while data duplication is the process of making a bit by bit image or clone of the device.}

Some of the data duplication tools are:-

- Solo 4: Used For Cloning & imaging of Hard Disk.
- Tableau.
- Media Clone.
- Ditto Forensic.

Recovering Deleted Files and Deleted Partitions

Files are one of the most important things for an individual. We have our important documents stored in as files. But, it happens sometimes that we accidentally delete our files and partitions or someone with an intention deletes the files or partitions. So here we are in a clue in how to recover the files.

So let us learn about, **how to recover the deleted files and partitions.**

Firstly, Let's understand how the files are deleted?

- Deleting the files with a habit pressing keys Shift + Delete – through which the files are deleted immediately without going to the recycle bin.
- Deleting the files from Recycle Bin.
- Completely deleting the recycle bin.

- Deleting various files from a USB drive, memory card, external hard disk and so on.
- Sometimes Files are also lost when they are transferred by cutting from one location and pasting into the other (Cut & Paste).

Copyright-FoRnSEC Solutions

Let's begin with the recovering of deleted files

We can Recover Deleted Files and Partitions with Professional Data Recovery Software.

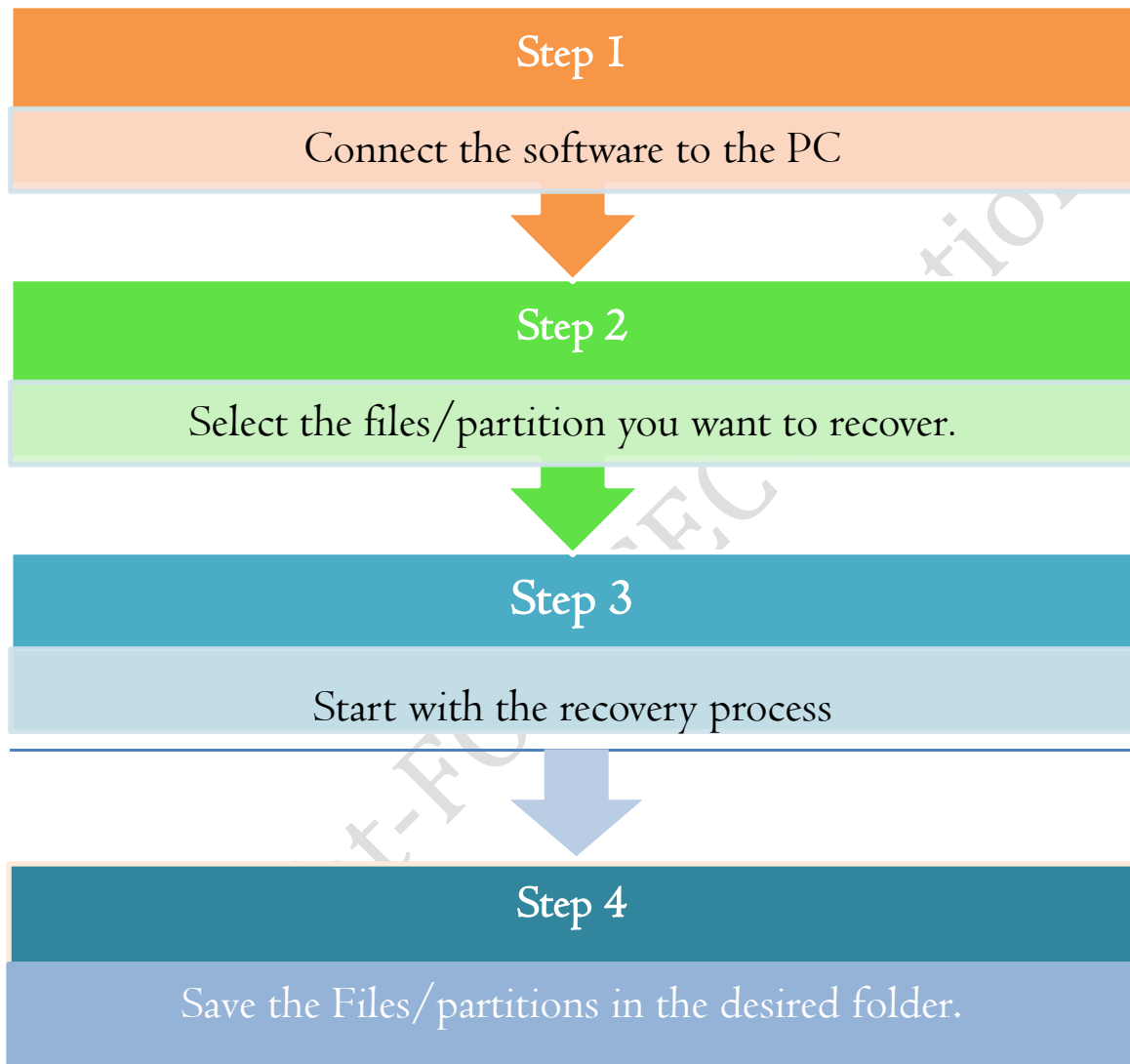
Tools to Recover Deleted Files are:

- Recover My Files.
- EaseUs Data Recovery Wizard.
- Recuva
- Stellar Phoenix Windows Data Recovery

Tools to Recover Deleted Partitions are

- Active BootX
- Helix

Steps to Recover the Deleted Files and Partitions



“And, here your files are recovered”

Usage of Forensic Investigation using Access Data FTK

Cyber Forensic Investigation is a very vital process which includes the collection, analysis, preservation of the data. The digital evidence is very fragile in nature and they can be altered, modified easily which may result in the loss of data. We need to preserve the data in such a way that it can be presented in the court of law.

Access Data FTK (Forensic Toolkit) is a Cyber Forensic Investigation tool which is recognized worldwide. FTK can help you analyze emails, Look for specific characters in files and also crack passwords.

Some of the major capabilities of FTK are:-

Email Analysis: - With FTK forensic Professionals can analyze the emails in a more dedicated way and also search for specific words.

File Decryption: - An another feature of FTK is file Decryption, with this feature one can decrypt the files and can also recover the passwords.

Data Carving: - Yet, another feature of FTK, the professionals can search for the data in a more precise way, where they have the options to search files based on size, data type, and even the pixel size.

How to get Access Data FTK or FTK Imager?

We can download the FTK from the official site of Access Data. We can download it for free or else can also buy the full version.

Chapter 9

“Network Forensic, Investigating logs & Investigating Network Traffic”



What is actually Network Forensic?

Network forensic investigation is the process of recovering and analyzing digital evidence from network sources in such a way that the results must be **reproducible and truthful**. There are various types of network forensics tools, each with different functions, In which some are packet sniffers and others deal with identification, fingerprinting, location, ip address tracking, web services, etc.

For Example:- If a Company is undergoing any network attacks than we need to monitor / Investigate the Network Logs & the Network Traffic to identify From where are the attacks Happening.

What are actually Network Vulnerabilities?

Network vulnerabilities are the weakness in the network through which an attacker has access to the computer system. There are various attacks which are performed by hacker/attacker to hack a website.

Let's discuss some of the attacks.

1)IP Address Spoofing

- IP Address Spoofing is the Phenomenon where an attacker changes it's genuine IP into a fake one.
- This actually is done by the attacker so that his real IP is not visible & he can Spoof anyone.

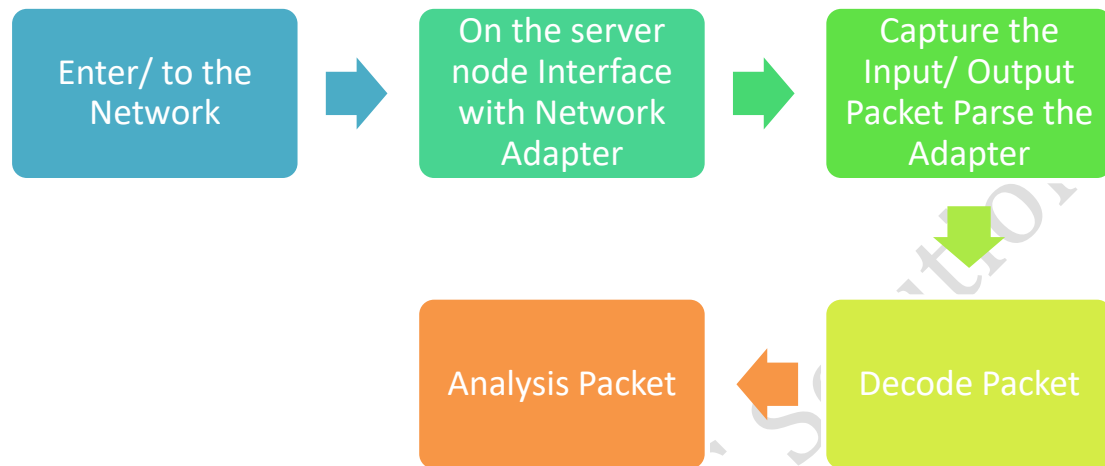
2) Man in the Middle attack

- In this attack, the attacker intrudes into your network, & captures your Packet & monitor messages.

3)Packet Sniffing

- Packet Sniffing is a Process which capture in & out Packets within a network. This is done with the help of a packet sniffing tool.

How does a packet sniffer works?



(Firstly, Connect to the Network & the On the Server Node Interface with the Network Adapter & Capture the input/ Output Packet, & then Decode the Packet, once the Packet is Decoded than the Packet Analysis is been Conducted)

4)Enumeration

- Enumeration is the process through which we can get Username, System Name, Network resource, Shared folder & service from a Network.
- This Process is carried out with use of internet only.

5)Dos Attack

- A DOS Attack is the process in which continue services are bombarded into a victims computer so that the victim is unable to perform the specified task.
- Session Attack
- Firstly let's understand what actually Session is.
- Sessions are nothing but a period of time given to a user while he accessing the website i.e. a session id is generated.

So, what actually session attack is?

The attacker uses a packet sniffer tool & as he is getting the packet, so with the help of packet he can get the session ID & gets unauthorized access to the website.

6)Buffer Overflow

- An attacker uses the empty slack space & injects the malicious code into the slack space & executes the Programmer.

Trojan Horse

- Trojan Horse is a malicious code, through which hacker gets access to the victims Personal Document, deleted files, message & Display Picture.

Chapter 10

“Investigating Wireless Attacks & Forensics”



Let's understand the definition of wireless network.....

“A wireless network is a computer network that uses wireless data connections between network nodes.”

Wireless attacks are being the most common security issue. Wireless attack can be said as an malicious action against any wireless network or the system information.

What are the types of wireless attacks?

- Denial of Service Attacks.
- ARP Poisoning Attacks.
- WEP Key-Cracking.
- MAC Spoofing.
- Man-in-the-Middle Attack

Tools to investigate Wireless Attacks.

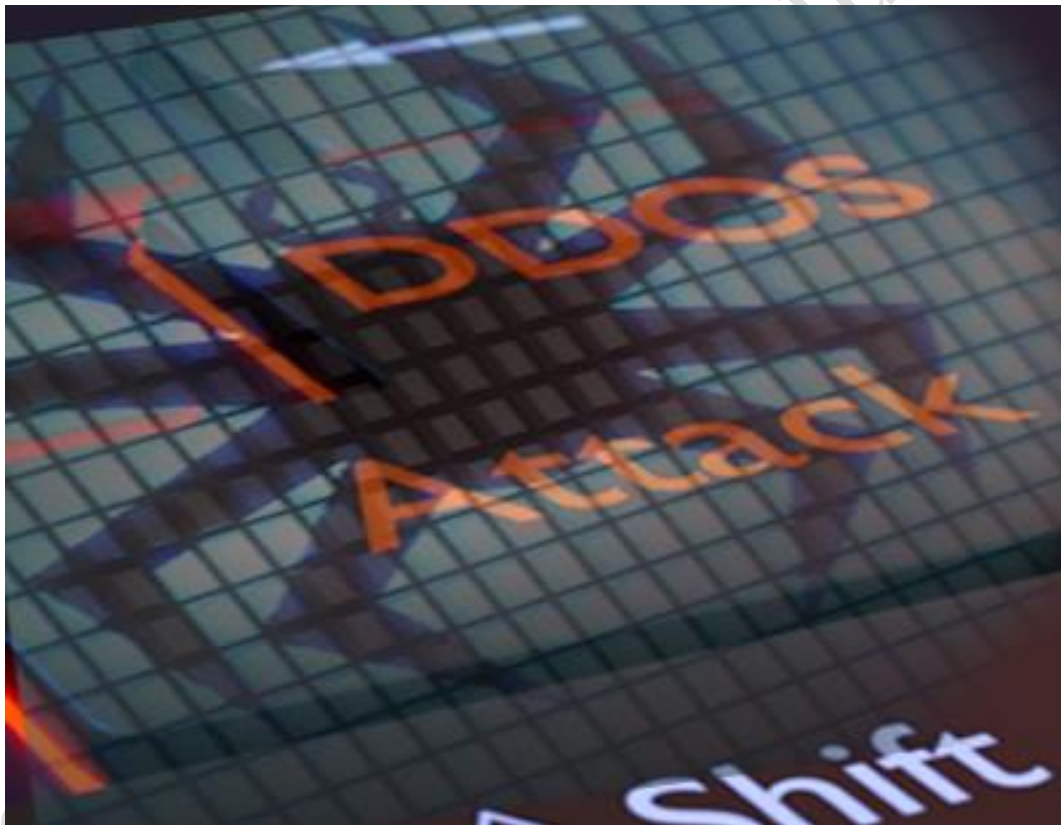
- Wireshark
- Network Miner
- NetSleuth

Steps to investigate Wireless Attacks



Chapter 11

“Investigation web Attacks & Forensic”



{ The attack which is done on a website or web application is termed as website attacks. }

Types of Web Attacks

- Cookie Poisoning
- Denial of Service Attack (DoS)
- Buffer Overflow
- SQL Injection
- Log Tampering.

How to investigate Web Attacks?

- 1) Firstly, visit the crime scene & analyze the web server, FTP & local system Logs.
- 2) Check the log file for the information related to crime, IP address, secure connection resources & status.
- 3) Identify the nature of the attack.
- 4) Identify the source of the attack.
- 5) Analyze firewall & IDS log to locate the source of the attack.
- 6) Block the attack ones you know from where the attack is coming from.
- 7) If you find the system compromised pull it out of the secure & disinfect the system & put it back.
- 8) Its attack is coming from outside identify the IP address & block it & than commence the investigation.

Tools to investigate Web Attacks

- Accunetix Web Vulnerability Scanner
- Burpsuite
- OWASP
- Appscan

Copyright-FoRnSEC Solutions

Chapter 12

Chapter 9 Tracking Email & Investigation emails Attacks



Okay let's begin this with the introduction of Email?

Email, which stands for Electronic Mail, consists of messages which are sent and received using the Internet facility. There are many different types of email services available which allows you to create an email account or send and receive emails & attachments, and also many of which are free. The availability of email, their speed and the anonymity had made it a powerful tool for the cyber criminals. An individual with the help of emails can also commit the crime to harass an individual to cause him some loss, or for personal benefits.

Some of the major email related crimes are:

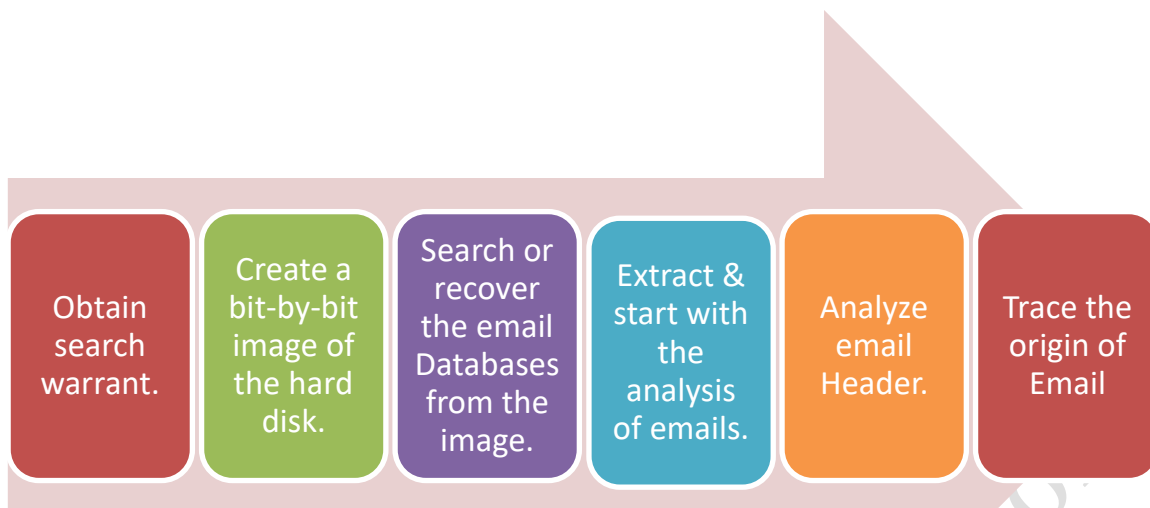
1. Email spoofing
2. Sending malicious codes through email
3. Email bombing
4. Sending threatening emails
5. Defamatory emails
6. Email frauds

Email spoofing-A spoofed email is one that appears to be originated from one source but has been actually emerged from another source.

Spreading Trojans, viruses and worms-Emails are often one of the fastest and easiest ways to circulate malicious code over the Internet.

Email bombing-Email bombing is the process of sending large number of emails to the victim's email account or servers crashing .

Step to investigate Email Crime



Tools to investigate Email Crime

- ✓ eMail Tracker Pro
- ✓ Paraben Mail Examiner
 - ✓ Mail Xaminer
 - ✓ Mail Detective

Chapter 13

“Mobile Forensic”



Copyr

Mobile device forensics is another branch of digital forensics which deals with extracting, recovering and analyzing digital evidence from a mobile device under forensically sound conditions.

In addition, it deals with recovering or accessing the data stored on devices which can include SMS, contacts, call records, photos, videos, documents, application files, browsing history and so on, while recovering the deleted data from devices using various forensic techniques for mobile analysis, mobile malware analysis. It is a vitally important process of recovering or accessing details or data from a device which needs to be admitted in the court of law and also we need to maintain the integrity of the evidence.

{ The Process of Using various tools & techniques to investigate a mobile phone to find out the culprit behind the crime for the sake of law is called Mobile Forensic Investigation. }

Let's understand the mobile forensic investigation process:-

- I) If we are going to the crime scene & we get a mobile phone then:-

- If it is in 'OFF' condition than directly seize the evidence.
- If it is in 'ON' condition than put the evidence in the faraday bag so that the wireless Signal is disabled or it faraday bag is not present than able the airplane mode.

Note: - Mention each & every detail in the chain of custody form.

- 2) Package the evidence properly & transport it to the laboratory.
- 3) Once the investigating team or the laboratory officers get the faraday bag than open the faraday bag in the faraday box itself.
- 4) Connect the device with the computer.
- 5) After connecting take the backup of the data.
- 6) With the help of mobile forensic software/hardware start with the analysis process.
- 7) After the Completion of the analysis generate the report.

Mobile Forensic Hardware

- 1) Cellebrite UFED
- 2) XRY Forensic
- 3) Access Data MPE plus.

Mobile Forensic Software

- 1) MobileEdit Forensic

- 2) MobileEdit Forensic Express
- 3) Oxygen Forensic
- 4) Paraben Device Seizure
- 5) Secure Kit
- 6) Axiom

Copyright-FoRnSEC Solutions

Chapter 14

“Computer Forensic Investigation Report & Documents”



Computer Forensic Report Templates

What is computer Forensic Investigation Report?

- A computer Forensic Investigation Report is a report or a document which has all the detailed finding of the computer-related crime Investigation.

Who makes a Computer Forensic Investigation Report?

- A Computer forensic expert is a person who has the authority to submit the report.

What things are included in the Report?

- A Cyber Forensic Report has each & every detail related to the investigation .
- It is one of the most important reports on which sometimes the whole judgment is depended.

So let's have a look at what thing are included in the report

- 1) **Investigator Details:** - Name, Experience
- 2) **Investigating Company Details:** - Name of Company, Place where it is situated.
- 3) **Date**
- 4) **Time**
- 5) **Location**
- 6) **Short summary about the case.**
- 7) **Evidence collected (Digital Evidence)**
- 8) **Tools used during Investigation**
- 9) **Name & work done by the Investigator.**
- 10) **Observations**
- 11) **If required sample attachments.**
- 12) **Conclusion**
- 13) **Signature, the stamp of the company & the Investigation officer.**

Crime Number: _____	Evidence Number: _____
Laboratory Name: _____	Investigated By: _____

Case Information

Client Name: _____

Date: _____

Time: _____

Location of Crime: _____

Summary about Case: _____

Evidence for Analysis: _____

Tools used for Investigation: _____

Observation: _____

Annexure Attached (If Any): _____

Conclusions : _____

Sign
(Seal of company)

Fig I:- The template of computer forensic Report

Here we have understood about the computer forensic investigation report. But when a cyber-forensic investigator visits a crime scene the needs to fill various forms to fill in the information.

So, now let's discuss the forms:-

- 1) Chain of Custody
- 2) Evidence Collection Forms
- 3) Computer Evidence Form
- 4) Mobile Evidence Form
- 5) Hard drive Evidence Form
- 6) Removable Storage Media

I) Chain of Custody Form:-

The chain of custody form has all the details info about the crime.

Crime Number: _____ Type of Crime: _____

Investigating officer: _____

Type of Evidences: _____

Date/Time Seized: _____ Location of Seizure: _____

Description of Evidence		
Item #	Quantity	Description of Item (Model, Serial , Condition, Marks, Scratches)

+

Chain of Custody				
Item #	Date/Time	Released by (Signature & ID#)	Received by (Signature & ID#)	Comments/Location

Fig 2:- The template of Chain of Custody Form

2) Evidence Collection Form:-

Has detailed information of evidence collected from the crime Scene.

Crime Number: _____	Evidence Number: _____
Laboratory Name: _____	Investigated By: _____
Date : _____	
Type of Crime : _____	
<u>Name & No. of Evidence #:</u>	
1. _____	
2. _____	
3. _____	

Fig 3:- The template of Evidence Collection Form

3) Computer Evidence Worksheet

Crime Number: _____	Evidence Number: _____																								
Laboratory Name: _____	Investigated By: _____																								
Computer Information :																									
<table style="width: 100%; border: none;"> <tr> <td style="width: 50%;">Manufacturer: _____</td> <td style="width: 50%;">Model: _____</td> </tr> <tr> <td colspan="2">Serial Number: _____</td> </tr> <tr> <td colspan="2">Examiner Markings: _____</td> </tr> </table>		Manufacturer: _____	Model: _____	Serial Number: _____		Examiner Markings: _____																			
Manufacturer: _____	Model: _____																								
Serial Number: _____																									
Examiner Markings: _____																									
<table style="width: 100%; border: none;"> <tr> <td style="width: 33%;">Computer Type:</td> <td style="width: 33%;">Desktop</td> <td style="width: 33%;">Laptop</td> <td style="width: 33%;">Other: _____</td> </tr> <tr> <td>Computer Condition:</td> <td>Good</td> <td>Damaged</td> <td></td> </tr> <tr> <td>Number of Hard Drives:</td> <td>_____</td> <td>3.5" Floppy Drive</td> <td>5.25" Floppy Drive</td> </tr> <tr> <td>Modem</td> <td>Network Card</td> <td>Tape Drive</td> <td>Tape Drive Type: _____</td> </tr> <tr> <td></td> <td></td> <td>CD Reader</td> <td>CD Read/Write</td> </tr> <tr> <td>DVD</td> <td>Other: _____</td> <td></td> <td></td> </tr> </table>		Computer Type:	Desktop	Laptop	Other: _____	Computer Condition:	Good	Damaged		Number of Hard Drives:	_____	3.5" Floppy Drive	5.25" Floppy Drive	Modem	Network Card	Tape Drive	Tape Drive Type: _____			CD Reader	CD Read/Write	DVD	Other: _____		
Computer Type:	Desktop	Laptop	Other: _____																						
Computer Condition:	Good	Damaged																							
Number of Hard Drives:	_____	3.5" Floppy Drive	5.25" Floppy Drive																						
Modem	Network Card	Tape Drive	Tape Drive Type: _____																						
		CD Reader	CD Read/Write																						
DVD	Other: _____																								

Fig 4:- The template of computer evidence worksheet

4) Hard Drive Evidence Worksheet

Crime Number: _____	Exhibit Number: _____
Laboratory Name: _____	Location : _____
 <u>No. of Hard Drive #:</u>	
Manufacturer: _____	
Model: _____	
Type: _____	
Serial Number: _____	
Capacity: _____	
Heads: _____	
Condition: _____	

Fig 5:- The template of hard drive evidence collection worksheet

5) Mobile Evidence Worksheet

CASE NUMBER: _____	DATE: _____
Property Tag #: _____	Requested By: _____
Is the Battery Dead or in need of Charging?	YES NO
Picture Phone?	YES NO
Cable Available?	YES NO
Powered ON?	YES NO
PIN Protected? PIN / PUK #: _____	YES NO
Airplane Mode / Radio Off?	YES NO Date/Time: _____
<div style="display: flex; justify-content: space-between;"> <div style="width: 45%;"> CELL PHONE NUMBER: _____ Service Provider: _____ FCC ID #: _____ IMEI: _____ NOTES: _____ </div> <div style="width: 45%;"> Owner: _____ Manufacturer: _____ Model: _____ Serial Number: _____ IMSI: _____ </div> </div>	

Fig 6:- The template of Mobile evidence collection worksheet

6) Removable Media Worksheet

Crime Number: _____ Laboratory Name: _____ Media Type / Quantity _____	Evidenace Number: _____ Investigated By: _____ _____						
<table style="width: 100%;"> <tr> <td style="width: 33%;">Pendrive []</td> <td style="width: 33%;">SD Card []</td> <td style="width: 33%;"></td> </tr> <tr> <td>CD []</td> <td>DVD []</td> <td>Other []</td> </tr> </table> <p>Evidance Description:</p> <div style="border: 1px solid black; height: 100px; margin-top: 5px;"></div>		Pendrive []	SD Card []		CD []	DVD []	Other []
Pendrive []	SD Card []						
CD []	DVD []	Other []					

Fig 7:- The template of Removal Media collection worksheet

Chapter 15

“Becoming an Expert Witness”



What is an Expert Witness?

An expert Witness is a Person who has tremendous Knowledge more than an average person in his Field & can give his opinion in legal matters such as in the court of law.

Roles of an Expert Witness?

- Needs to give his opinion in the court of Law.
- Should be fair, that is he should not give bias opinion.
- Should be able to educate Public & Court.
- Should be able to conduct an investigation if asked by the court.
- Provide Proper Report with Findings.
- Should be concise in his decisions.

Types of Expert Witness

- Computer Forensic Expert,
- Architecture Expert
- Medical & Psychological Expert
- Toxicology Expert
- Ballistic Expert
- Criminal litigation Expert
- Psychology Expert
- Civil litigation Expert

I) Computer Forensic Expert

- Computer Forensic Expert is techno savy Person.
- He is having an expertise in the field of Computer Forensic.

Roles Of Computer Forensic Expert

- A computer forensic expert identifies the incident happened.
- Investigates the incident properly.
- Finds out if any deleted files, then tries to recover it.
- Finds out if any password protected files, and try to recover the password.
- Make proper reports with findings.
- Testifies as an expert witness in the court of law.

2) Architecture Expert

- Architecture Experts is the person who is an expertise in the field of Construction and Architecture.

Role of Architecture Expert

- An Architecture Expert Testifies as an Expert Witness.
- Give opinion in if any accidental case.
- Give opinion in Construction matters if any detects

3) Serology Expert

- Serology Expert is the Person who is an expertise in the field of serology.
- He is having the knowledge of the serological fluids Present in the human body.

4) Medical & Psychological Expert.

- Medical & Psychological experts are the Physicians or their assistants who can describe the physical finding observed in the human body.

Role Of Medical Expert

- Identity the finding in the victim's body.
- Testify as an expert witness.
- Observe the injury caused to a human body.

5) Psychology Expert

- He is an expert who understands the psychology of a human being.

Role of psychological expert

- Conduct interviews & test of the Suspect.
- Provides details report about the suspect.
- Testify as an expert witness.
- Identify human Behaviour.

6) Ballistic Expert

- Ballistic Expert is a person who is having an Expertise in the field of ballistic. Ballistic is an area covering the firearms, types of firearms, usage of firearms, bullets etc. Ballistic expert is having the Knowledge of all firearms

Role of Ballistic Expert

- Testify as an expert witness in the court of law
- Identify the wounds, the bullet entry & exit Points in a Human body.
- Identify whether the Cartridge case & the bullet are same
- Identify whether the bullet is fired from which given.
- Provide information report with findings.

7) Civil Litigation Expert

- He is the person who is an expert in handling civil cases such as divorce cases or family disputes.

Role of civil litigation Expert

- They correct the false assumptions regarding the crime scene shreds of evidence.

8) Criminal Litigation Expert

- He is the person who is having expertise in handling criminal cases such as murder, rape etc.

Role of Criminal Expert

- Handles the criminal cases such as murder, rape etc.
- Testifies as an expert witness in the court of law.

Reference

- 1) https://www.computer-forensics-recruiter.com/home/computer_forensics_history/#context/api/listings/prefilter
- 2) <https://www.pandasecurity.com/mediacenter/panda-security/types-of-cybercrime/>
- 3) <https://www.law.cornell.edu/rules/fre>
- 4) <https://www.swgde.org/>

“End of Chapter”