DIGITAL FORENSICS NOTES

Adwait Sharma

@lastmomenttuitions.com

sharma.adwait04@gmail.com

(CLICK TO NAVIGATE)

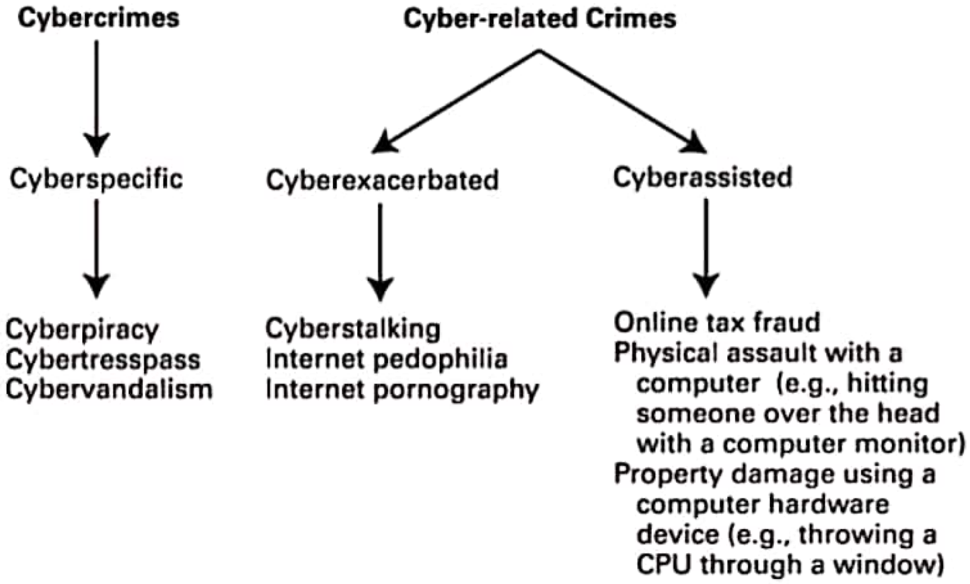
MODULE 01 – INTRODUCTION

Q. What is cybercrime? Explain the cybercrime in detail

Ans.

" Cybercrime wo criminal activity hai jo ek criminal perform karta hai using a computer ya fir internet ke through | Inka main focus hota hai unn systems ko exploit ya hack karna that has a loophole like a broken software aur iske do types hai cybercrime and cyber-realted crime."

1. Cybercrime is any criminal activity done by a person using the computer system or a network.
2. It can also be defined as an act of criminality done via or over the internet.
3. Cybercrime mainly focuses to exploit the broken / hackable software.
4. The crimes performed are either cybercrime or cyber-related crimes.


Cybercrimes
Cyber-related Crimes
Cyberspecific
Cyberexacerbated
Cyberassisted
Cyberpiracy
Cybertresspass
Cybervandalism
Cyberstalking
Internet pedophilia
Internet pornography
Online tax fraud
Physical assault with a computer (e.g., hitting someone over the head with a computer monitor)
Property damage using a computer hardware device (e.g., throwing a CPU through a window)

a. Cybercrimes:

These crimes are related or usually done via the internet. They are further classified as cyberspecific.

i. Cyberspecific –

1. Cyberpiracy: The act of providing copyrighted content over the internet.
Eg: torrents for movies and cracked software.

2. Cybertrespass: The act of accessing sites or webpages which the user doesn't have the rights or access to.
Eg: Browsing paid webpages through fake login id.

3. Cyber-Vandalism: Cyber-Vandalism accounts to the act of damaging someone's data from the computer that in a way disrupts the victim's business or image due to editing the data into something invasive, embarrassing or absurd.

Eg: Editing informative sites like Wikipedia and putting absurd or wrong data.

b. **Cyber-related Crimes: These crimes do not directly qualify in being a cybercrime but partially violates the cyber security. These are partially done using computer systems by a user to create a bad situation or assistance in something illegal.**

i. Cyberexacerbated: Act of a user committing nuisance using a computer system and violating legal cyber laws.

1. Cyberstalking: Act of revisiting a individual's or an organization's profile for self-gain
Eg: Stalking company's recent upgradations / Stalking profiles on social sites.

2. Internet Pedophilia: Act of sexual abuse of children over the internet.
Eg: Stalking / harassing minors over the internet.

3. Internet Pornography: Act of browsing illegal websites and streaming disturbing or arousing videos.
Eg: Browsing over video streaming websites that are banned in a country.

ii. Cyberassisted: Act of assisting the computer system and perform a particular crime.

Eg: Hitting someone using a monitor.
Physical assault using a computer.

Q. Compare Traditional criminal activity with cybercrime

Ans.

1. Traditional crimes are nothing but physically performed crimes like burglary, murder, etc.
2. Cybercrimes include identity theft, stalking, phishing, data stealing, etc.

Parameters	Traditional Crime	Cybercrime
1. Evidence	Traditional criminals usually leave traces of a crime, through either fingerprints or other physical evidences	Cybercriminals rely on the Internet via which they commit their crimes, and it leaves very little evidence about the cybercrime.
2. Identity Forging	It is quite difficult for traditional criminals to fake their gender, race, or age.	Forensic investigators usually experience great difficulty in gathering evidence that could lead to the conviction of cybercriminals since these criminals can freely change their identities.
3. Duration of Investigation	Traditional crimes take shorter time period to investigate because the criminals usually leave evidence that can be used to spot them.	Cybercrime involves criminals using falsified names and working from remote locations, it usually takes longer to identify the real cybercriminals and apprehend them.
4. Protection using Constitution	There is no such amendment against traditional crimes as there are other witness or evidences.	Cybercriminals can use the Constitution to protect themselves from prosecution. The Fifth Amendment points out that nobody can be forced to become a witness against himself in any criminal case. They are the only witness of the crime.
5. Physical force required	Most of the traditional crimes (such as murder and burglary) involve the use of excessive physical force that results in physical injury and trauma on the victims.	Cybercrimes do not require the use of any physical force since the criminals merely use the identities of their victims to steal from them.

Ticket to remember the difference: PD PIE (sounds like pewdiepie)

Protection using constitution

Duration of Investigation

Physical force required

Identity Forging

Evidence

Q. Classification of Cybercrimes / Types of Cybercrimes / Categories of Cybercrimes

Ans.

The cybercrime is categorized as follows:

1. Violent or Potentially Violent Cybercrimes
2. Nonviolent Cybercrimes

1. Violent or Potentially Violent Cybercrimes:

These crimes pose a physical threat to the individual and/or group of individuals. Violent or probably violent crimes are:

a. Cyber Terrorism:

1. Cyber Terrorism is any planned activity in cyberspace via internet or computer networks to create terror in the social space of individuals.

2. It also includes the recruitment of young people in the terrorist's organizations by convincing them to perform violent activities.

3. Usage of e-mails to communicate with team members of the terrorist group is also a part of cyber terrorism.

4. Other examples are:

i. Aircraft crashes are done by controlling the airplane's computer systems.
ii. Hacking into medical database to alter the patient details like its treatment plan, leading to death.
iii. Disrupting electrical power grid to create nuisance and inconvenience among folks.

b. Assault by threat:

1. This is the act of giving threat to someone's life or asking for ransom to ensure loved one's safety, through e-mails.

c. Cyberstalking:

1. It is the act of frequent revisiting of an individual's or organization's profile for self-gain and to plan further criminal conspiracy.

Eg: Stalking company's recent upgradations / Stalking profiles on social sites.

d. Child Pornography:

1. Online streaming of sexual videos having minors as a part of them is a cybercrime as it is against the rights of children and highly illegal.

2. Nonviolent Cybercrimes:

These crimes do not pose a physical threat to the individual and/or group of individuals. Types of non-violent crimes are:

a. Cybertheft:

1. Cybertheft is stealing data / password / login credentials / copyrighted content over the internet. Cyberthefts include:

i. Embezzlement
ii. Unlawful appropriation
iii. Business espionage
iv. Plagiarism
v. Piracy
vi. Identity theft
vii. DNS Cache poisoning

b. Cybertrespass:

1. Cybertrespass is a form of sniffing data in a computer system without actually altering or deleting it. The trespasser is interested in your private data like e-mails and documents uploaded or sent via the internet.

c. Cyberfraud:

1. Cyberfraud is the act of selling fake things over the internet by gaining the trust of the victim and offering goods at cheaper prices to attract them.
2. Cyberfraud also includes the act where the victim voluntarily pays the criminal a hefty sum to obtain services like jobs, trips, lottery, jackpots, etc.
3. Examples are:

i. "Work from home'' fraud
ii." iPhone 64gb@ $10" fraud

d. Destructive Cybercrimes:

1. This cybercrime is used to damage the network, delete data or steal them for misusing.
2. The destructive cybercrimes are:

i. Introduce virus and/or worms into the system.
ii. Cybervandalism. (destroying data rather than stealing)

e. Other non-violent crimes:

1. **Internet gambling** and fooling people to be a part of it.
2. **Selling illegal drugs** / narcotics online without medical prescription.
3. **Cyber laundering** of black money.
4. **Advertising/**soliciting sexually abusive illegal advertisements.

Q. Types of Cybertheft

Ans.

Cybertheft is stealing data / password / login credentials / copyrighted content over the internet. Cyberthefts include the following types:

i. Embezzlement: Misusing someone else's money given with trust for specific purpose for personal benefits.
Eg: Using the trip money for self-use given by others in context of the trip expense.

ii. Unlawful appropriation: The attacker gets access to the data that is not meant to be given with trust to him and misuses it.
Eg: Changing document's author name

iii. Business espionage (spying): The act of spying through the company's network and sharing company's data through a group of spies inside the organization.
Eg: Financial information for sabotaging a tender deal

iv. Plagiarism: The act of stealing someone else's written document over the internet which is meant for private use only.
Eg: Sharing **Last moment tuition's** notes to people who haven't paid for it.

v. Piracy: Copying/Downloading copyrighted movies or software online.
Eg: Movie downloading through pirated sites and not through legal hosts.

vi. Identity theft: Impersonating an individual and gaining access to his privacy through illegal manner.
Eg: Using else's login id and password to browse through a webpage.

vii. DNS Cache poisoning: The cache for Domain Name Servers are hacked and the data may be redirected to the attacker's servers.

Q. Short note on: Internet spawns' crime

Ans.

1. Internet spawn crimes refer to the crimes done through/on the internet
2. Internet is the weapon for such crimes
3. These crimes are hard to detect and investigate as cyber criminals wash off the trails from the internet. For e.g. An IP address
4. Impact may lead to high loss

The following are the types:

i) Copyright privacy: Stealing somebody else's registered stuffs

ii) Information transfer theft: Eavesdropping (listening) the electronic conversation between parties for self-gain

iii) Data transfer theft: Stealing data packets from the public as well as private networks

iv) PC output theft: Travelling back to the victim's computer for private data using mail records, client records, etc.

v) Desktop forgery: Includes forging of organization's letterheads, challans, cash memos, etc.

vi) Password trafficking: Selling victim's credentials online

vii) Computer intrusion: Exploiting the system's firewall and trespassing through the system for confidential data

viii) Internet fraud: Fraud done using honeypot offers and victimizing greedy customers through spam mails

ix) Internet harassment: Stalking or intercepting victim's social space continuously leading to mental stress

Ticket to remember: CID PD PC I I (CID Got a PenDrive, they connected it to a PC and they investigated an Internet fraud & an Internet Harassment Case)

Q. Short note on: Worms, Virus & Differentiate Worms vs Virus

Ans.

i. Worms:

1. A worm is a code that replicates itself over a system in order to consume resources such as disk space and CPU memory.
2. Worm does not basically affect files and folders, in fact it is concerned mainly with memory and slowing a system or crashing it due to overload.
3. Worm replicates itself in a computer network by exploiting the loopholes in the network.
4. Worm spreads faster than virus.
5. It can easily replicate itself without any human intervention.
6.Worms don't require a host to trigger them into action. They are self-executable.

Types of Worms are:

a. Instant messaging worms:

This type of worms spread through messaging apps and infect your contact's system through malicious links.

b. Internet relay chat (IRC) worms:

It targets channels over the network to exploit and introduce malware in them.

c. Internet worms:

These worms find the vulnerable machines over the internet that usually don't have a firewall or similar security and replicates themselves onto such system.

d. File-sharing network worms:

The FTP server is used as a channel to introduce the replicative code and infect other systems in the FTP network.

ii. Viruses:

1. Virus is also a piece of self-replicating code, but it requires a host to trigger its action.
2. These hosts are program files or software executable files (.exe).
3. Virus codes are embedded in these host program files.
4. Virus can be spread through internet, FTP servers through which these hosts are transferred.
5. Virus can alter a file's location, modifies the content or corrupts them.
6. They are slower than worms.

Types of viruses are:

a. Resident program infector:

These viruses trigger upon executing through their host and is responsible to infect every other executable file in the memory. This is done until the user reboots the system. It will affect each .exe file that is being executed on the system.

b. Boot sector infector:

This virus infects the master boot record of the hard disk which leads to infecting other floppy disk's boot sector thereby crashing the system boot process.

c. Multi-Partite virus:

It is a combination of file infector as well as the boot sector virus.

d. File Infector:

This virus code is placed at the starting of the .exe file. Whenever the file is executed the virus code is triggered and it replicates itself to the next .exe file and infects it. This process repeats and all the .exe files gets corrupted.

e. Polymorphic virus codes:

These codes are usually based on encryption and they easily disguise themselves from the scanner and usually goes undetected. It is a form of stealth virus.

Difference Between Virus & Worm

Parameters	Worms	Virus
1. Definition	A worm is a malicious program that spreads automatically on its own.	A virus is a piece of code that attaches itself to legitimate program and uses the program as a host.
2. Modification of codes	Does not modify other program codes.	Modifies other program codes
3. Replication	Replicates itself.	Does not replicate itself.
4. Destructiveness	Non-destructive nature.	Destructive nature
5. Used for	Worm is used to make computer or network unusable.	Virus is used to infect the code or program stored on computer system.
6. Infecting nature	Worm does not infect other files occupies memory space replication.	Virus can infect other files.
7. Trigger	Worm does not need any trigger.	Virus may need a trigger for execution.

Ticket to remember: MR UD^{2}IT

Modification of codes

Replication

Used for

Destructiveness

Definition

Infecting nature

Trigger

Q. Explain: Digital Forensics

Ans.

"Digital forensic is collection, preservation, analysis and presentation of computer/cyber - related evidences."

"Digital forensic wo domain hai jisme cyber related jo crimes hotey hai aur unse related jo evidences hotey hai unko collect karna, unko examine karna aur fir finally unpe ek report banana ki kya hua thha aur kaise hua thha | Ye report waisa hi hota hai jaisa hum ek incident pe banate hai."

1. Digital forensics is more interested in providing reports done in the past.
2. It determines the attack on the system, analyses its fact and then prepares a report.
3. It is a process for examining the volatile components of the computer system, for example hard disks, and other media.
4. It is a process that learns and upgrades its immunity from future attacks.

Importance of Digital Forensic

1. Digital forensics is concerned not only with "detective work" but also it aims to scramble information in such a way that it must be un-readable to the attacker.

For this, we have two methods:

a. *Encryption:* This domain is more concerned with hiding the data in a format that is intended to be read only by the authorized recipients. Eg: Encrypting and scrambling an e-mail with 128-bit SSL

b. *Steganography:* This domain uses larger files like photographs to hide a relatively small data into it. Eg: Message "Hi" hidden inside a photo.

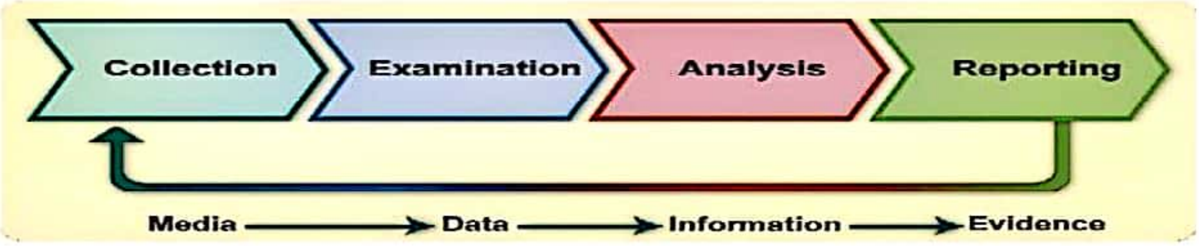
2. Digital forensics also provides:

- Handling sensitive confidential data.
- Prevents data corruption if any, during the detective phase.
- Following prescribed regulations and guidelines.
- Maintains integrity and correctness of the data concerned.

Process of Digital Forensics:

1. For forensic investigation we have following four steps:

a. Collection
b. Examination
c. Analysis
d. Reporting



Detailed Digital Forensics Process:

i. **Collection:**

- It is the first phase in the investigation process
- In this phase, data is firstly identified, labelled for reference and then finally collected
- The physical evidences are also collected

ii. **Examination:**

- This is the second phase in the chain process
- In this phase, the data collected is taken into consideration and relevant information is concluded from them
- This information is extracted using proper forensics tools
- The integrity of the evidences is maintained so that it doesn't get sabotaged or corrupted.

iii. **Analysis:**

- This is the third and the most important phase of the investigation
- The relevant information extracted from the analysis phase is examined thoroughly to get a pattern, information about the criminal, leads on the case, etc.
- This phase leads to the solving of the case, usually

iv. **Reporting:**

- This is the final phase of the process
- This phase describes the final report of the case that includes points like,
    - ✓ Information relevant to the case
    - ✓ Actions performed
    - ✓ Further actions/procedures
    - ✓ Advocated(legal) enhancements

Q. Evidence

Ans.

"Evidence is any set of information of supporting value, that proves/indicates something or helps to prove/indicate something relevant/concluding to the case"

"Evidence digital forensics ke saboot hai jinko hum kisi point ko prove karne ke liye use kar sakte hain"

Types Of Evidences

1. **Real Evidences:** These evidences are those that can be taken into the courtroom, where they prove something on their own. These are self-implacable things. These are therefore termed as real evidences. They are the most powerful evidence. Eg: The criminal's computer/laptop with evidences.

2. **Documentary Evidence:** These are the evidences in the written form. There are chances that such evidences can be faked to falsify the testimonial. Eg: Server logs, e-mails, database documents, etc.
3. **Testimonial Evidence:** These evidences are testimonials of a witness under oath taken in a court. (*main jo bhi kahunga, sach kahunga....*). These evidences are based on commitments basically. A witness may or may not tell the truth even after taking the oath. Eg: Self-surrendering testimony of a criminal.

4. **Demonstrative Evidence:** These evidences are used to prove other evidence that has been proved previously. These evidences are mainly used to explain technical terms to non-technical people.
Eg: Demonstrating a cyber-related attack in the court.

Characteristics of an Evidence:

1. **Admissible:** The evidence must be acceptable. Any irrelevant evidence is not admissible. Certain guidelines are followed in the process of collecting relevant evidences. Eg: If a dog barks at a person doesn't prove that he is thief in the court, so this evidence is not admissible.

2. **Authentic:** It must be from the same context as the crime occurred. Authenticity of an evidence proves if it is relevant to the case/investigation or not. Eg: If a person is poor doesn't prove the fact that he uses crime to earn money. Both are different contexts.

3. **Believable:** The evidence should not be a sort of something unbelievable in real-time world. The evidence must be acceptable to the court and must be under the prescribed guidelines. Eg: Speaking of cybercrime act by a ghost is not believable

4. **Reliable:** The evidence must sustain its matter of fact, that is it must be reliable and should not change with time. It must indicate/highlight the same point as done previously. Eg: The IP address is not reliable as an evidence in whole because it can be spoofed.

5. **Complete:** The evidence must be complete in itself. It should not be partial in the sense of proving something. It should be a complete set and not just randomly collected data that doesn't prove something fully.

Ethical Issues / Factors of Evidences:

1. ***Objectivity:*** The investigator must maintain objectivity. The respected investigator must stick to the points that are objective to the case and not other than that. If done so, it misleads the court into some matter of irrelevancy.

2. ***Decision making:*** It is not the investigator's job to judge the culprit on being innocent or a criminal. He should only focus on proving the case.

3. ***Responsibility:*** It is the responsibility of the investigator to collect relevant facts/evidences and put them forth with a report.

4. ***Confidentiality:*** The investigator must maintain strict privacy in discussing the leads and sharing the facts regarding the case with anyone. He must keep the data to himself privately.

Q. Incident

Ans.

"Computer security incident is any unlawful, unauthorized, or unsuitable activity that includes a computer system or a network"

"Incident wo ghatna hai cyber security mein jab ek crime detect hota hai"

Events:

1. **M**isuse of authority (Extortion)
2. **U**nlawful intrusion into a private system
3. **D**oS attack on a network
4. **E**mbezzlement (theft of money)
5. **S**pam e-mails
6. **T**heft of confidential data and/or secrets

Ticket to Remember: MUDEST (sounds like the word related to honesty, i.e MODEST but a criminal has dirty hands so incidents are MUDEST, just relate it to remember easily).

Goals of Incident Response:

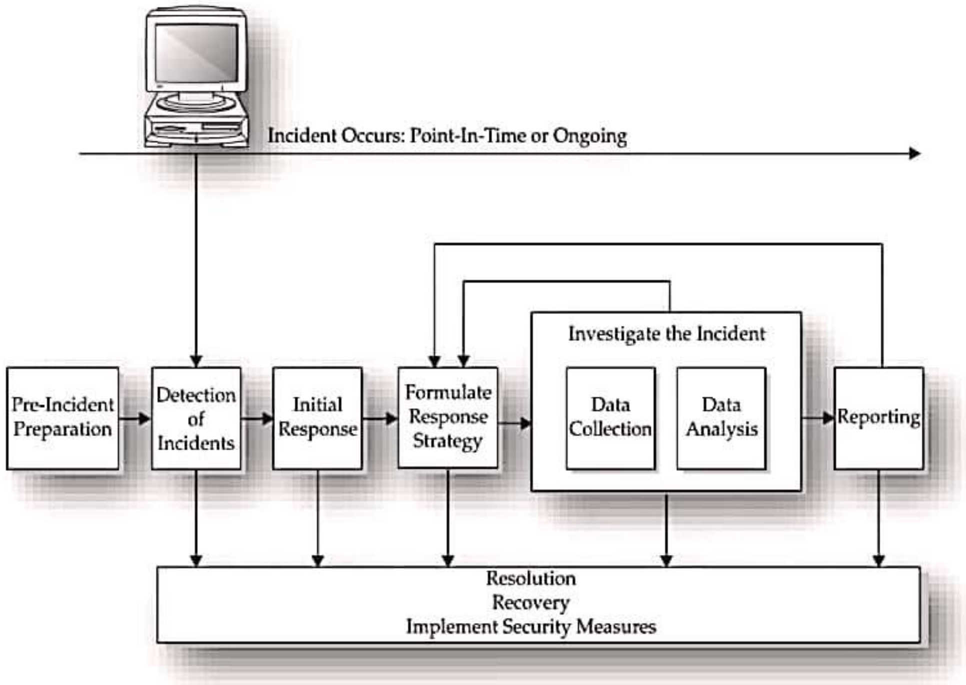
a. Prevents a disjointed/random response (which could be disastrous)
b. Confirms whether an incident occurred
c. Promotes collection of accurate information
d. Controls proper retrieval and handling of evidence
e. Protects privacy rights as per law
f. Minimizes disruption to business
g. Action is taken against perpetrators
h. Provides accurate reports
i. Provides rapid detection
j. Minimizes compromise of proprietary data
k. Protects the organization's reputation
l. Educates senior management
m. Promotes rapid detection and/or prevention of such incidents in the future, via lessons learned

Q. Incident Response Methodology

Ans.

1. Computer incidents are complicated, fragile nd must be handled precisely and with caution.
2. To achieve this precision, we use the approach of dividing incident resolution into component steps and test the input and output.

The figure below illustrates this process:



So, the steps to incident response can be broadly classified as:

1. Pre-incident preparation
2. Detection of incident
3. Initial response
4. Formulate response strategy 5. Investigate the incidents

a. Data Collection

b. Data Analysis

6.Reporting

i. Pre-incident preparation:

1. This phase deals with preparing the organization with proper workforce and management before the incident.
2. It is done before the incident occurs.
3. This phase includes:

A) Preparing the organization: This deals with making the organization immune to the attack.
Some measures taken are:
a. Apply host and network security
b. Hire IDS
c. Perform timely vulnerability test

B) Preparing the CSIRT (Computer Security Incident response team): The organization assembles a CSIRT team responsible for handling the attack. They are provided with necessary training along with desired software and hardware

ii. Detection of incidents:

1. The most critical phase of the process
2. This phase starts when any illegal or unauthorized event occurs
3. The detection can be done by:

A) End user (customer)
B) System admin
C) IDS

4. End users file their complaint through contacting help desk
5. Whereas admins contact their immediate supervisor
6. IDS alarm the information security personnel

iii. Initial Response:

1. First step towards the investigation process
2. In this phase, the CSIRT members are gathered along with data from intrusion and determines the type of attack
3. Further, its impact is assessed
4. The CSIRT are the lead players in the process
5. If any other entity gets any information it must share it with the CSIRT
6. Some other tasks are:

A) Interviewing system admins
B) Reviewing IDS reports

iv. Formulate response strategy:

1. This phase is responsible to propose a strategy for appropriate responses
2. It must consider the factors like,

    A) legal
    B) political
    C) technical
    D)business

3. The objectives of this phase are:

    a. Considering the totality of circumstances
    b. Considering appropriate responses
    c. Taking legal and/or administrative action against the incident

v. Investigate the incident:

1. This phase determines:

    A) Who did it?
    B) When it happened?
    C) What happened?
    D) Why it happened?
    E) How it happened?

2. It gathers evidences regarding the incident

3. There are major two sub-phases:

    i) Data collection
    ii) Forensic analysis

i) Data collection:

a. The aim is to gather electronic information in forensically stable way
b. It gathers:

a) HOST BASED INFORMATION: Like date, time, applications, networks regarding host
b) NETWORK BASED INFORMATION: This information is gathered through IDS logs, router logs and firewall logs.

ii) Forensic analysis:

a. This is the crucial sub-phase
b. It reviews all the collected data

c. Both software and hardware evidences are reviewed and investigation steps are carried out
d. It also takes into account the electronically deleted data in forms of fragments

vi. Reporting:

1. The most difficult phase in the process
2. The challenge is to create reports that precisely describe details on incident
3. The guidelines that must be followed are:

a) Document immediately
b) Write concisely and clearly
c) Use a standard format
d) Use editors which can edit the document so that is understood to the non-technical folks

Q. Explain: Computer roles in crimes

Ans.

Computer crime – Computer crime is any criminal offense, activity or issue that involves computers. Computer is used in illegal activities; child pornography, threatening letters, e-mails spam or harassment, extortion, fraud and theft.
Categorizing computer related crime:

1) Computers serve in several different roles related to criminal activity.
2) The three generally accepted categories speaking in terms of computers *as communications tools, as targets, and as storage devices:*

a) Computer as a communication tool:
It presents the computer as the object used to commit the crime. This category includes traditional offenses such as fraud committed through the use of a computer

b) Computer as a target:
A computer can also be the target of criminal activity, as seen when hackers obtain unauthorized access to department of defense sites.

c) Computer as a storage device:
A computer can also be tangential to crime when, for example, it is used as a storage place for criminal records. For example, a business engaged in illegal activity may be using a computer o store its records.