AKTU NEXTGEN ENGINEERING

WHATSAPP GRP

1 & 2 YR

3 & 4 YR

FREE COURSES

UNIT-1

CYBER SECURITY

ONE SHOT VIDEO

JOIN TELEGRAM FOR NOTES

Q Explain how the term 'cybercrime' originated state few cyber crimes.

Sol Cybercrime is the use of a computer as a weapon for committing crimes such as commiting fraud, identity theft, or breaching privacy

⇒ The word "cybercrime" is made up of two parts "cyber" and "crime"

⇒ "cyber" comes from "cybernetics", which was a term created in the 1940s.

⇒ Cybernetics is the study of how animals and machines communicate and control themselves

⇒ Over time "cyber" started to refer to thing related to computers and the internet.

⇒ "crime" means activities that break the law

⇒ When we put "cyber" and "crime" together, it means illegal activities involving computers and the internet

⇒ The term "cybercrime" became popular in the late 20th century as more people used the internet and digital devices

⇒ Few examples of Cyber crimes:

① Hacking: Unauthorized access to computer systems or network.

② Phishing: Fraudulent attempts to obtain sensitive information by pretending to be a trustworthy entity in electronic communication.

③ Identity Theft: Stealing someone's personal information to commit fraud

④ Denial of Service (DOS): Overloading a network or website to make it unavailable to users

Q. Who are Cyber Criminals?

Sol Cyber criminals :-

① Cyber criminals are individual or groups who engage in illegal activities in the digital realm, using technology and the internet to commit various forms of cybercrime

② They exploit vulnerabilities in computer systems, networks and online platforms for financial gain, personal motives, or to disrupt and harm other

Q What are the types of cybercrime?

Sol Ransomware :- locking someone's computer files and demanding money to unlock them

① Child Exploitation :- Using the internet to harm or exploit children

② Intellectual Property :- Stealing ideas, designs or inventions from their rightful owners

③ Cyberbullying :- Bullying someone through online message or social media.

Q Explain term information security?

Sol Protecting data and information system from being accessed or used by unauthorized people.

. Key Principle

① Confidentiality :- Making sure only the right people can see or use the information

② Integrity :- Ensuring Information is accurate and hasn't been changed without permission

⊙ Availability :- Ensuring that information and resources are available when needed by those who are authorized.

⇒ Key Aspects :→

- Risk Management :- Finding and reducing risks to information by using security measure.
- Access Control :- Limiting access to information through password, biometrics and permissions
- Network Security :- Protecting networks with firewalls, intrusion detection system.

Q Survival Mantra for the Neitizens

Sol Basically There are 5P netizen mantra for online security is :-

- Precaution: Take steps to avoid danger or problems before they happen. This mean being careful about what you click on and who you share information with online.

- Prevention :- Act to stop threats from affecting you. This include using strong password, keeping your software updated, and enabling two-factor authentication
- Protection :- Use tools and methods to defend yourself against cyber threats (installing antivirus)
- Preservation :- Keep your data safe and intact. Regularly backup important files and use encrypt to protect sensitive information
- Perseverance :- Stay consistent, continously learn about new threats, update your security practices, and be vigilant in protecting your information

Q What is the fuel of cybercrime.

Sol Botnet is the fuel of cybercrime.

① A botnet is a network of computers that have been infected with malware.

② These infected computers, called "bots" or "zombies" are controlled by a cybercriminal.

③ The cybercriminal uses a central server or a

set of servers to issue commands to the bots.

- Computers become part of a botnet through method like phishing emails, malicious downloads, or security vulnerabilities.

⇒ Botnets can be used for various illegal activities such as:

- DDos Attacks
- Spam
- Data theft :- like card Details

⇒ A botnet can consist of a few to millions of infected computers.

⇒ often, the computer owners are unaware that their machines are part of a botnet.

Q How may a criminal plan cybercrime?

Sol Steps are following :-

① Reconnaissance :

→ This the first step of cyberattack is "Reconnaissance"

- This is the information-gathering stage
- The attacker quietly collect data about the target
- It's considered a passive attack because it doesn't directly harm the system.
- The attacker might look at public information such as websites and social media to learn about the target.

① Scanning and Scruthinization!-

→ The attacker examines the collected data closely.
→ They use tools to scan the target's systems and networks.
→ The goal is to identify weaknesses or vulnerabilities that can be exploited.
→ This is basically used to find the pinpoint specific security gaps.

① Launching the Attack!-

→ The attacker gains access to the system using the identified vulnerabilities.
→ They might use malware, phishing, or other techniques to break in.

→ The attacker might take control of the system, steal data, or cause damage.

Q. Explain Wireless devices with example.

Sol Mobile devices like smartphones and laptops are very important for business.

→ They provide internet access outside the office.

→ In 2023, there are over 11.856 billion mobile connections worldwide.

→ Many of these devices can connect to the internet

→ IT departments have challenges managing these devices remotely.

→ They need to ensure security and support productivity

→ More employees are bringing their own smartphone to work.

→ This increases the variety of devices IT departments must change.

→ These changes create new security challenges for companies globally

Q What are the security challenges faced by wireless devices?

Sol The security challenges faced by wireless devices are following :-

1. Devices Outside Controlled Environments :-

- Mobile and hand-held devices, like smartphones and laptop, are portable.
- People carry these devices outside secure places like offices or homes.
- This means sensitive information can be exposed to less secure environment

2. Remote Access to Secure Networks :-

- Mobile devices often need to connect to corporate or protected network from afar
- This remote access is necessary for people to work and use resources when they are not in the office.
- Ensuring this access is secure is a major challenges, as it opens up potential vulnerabilities

Q. Explain the security measure and policies taken for mobile devices.

Sol. The widespread use of mobile devices makes cybersecurity more challenging.

- People, especially young ones, store sensitive information on their phones
- This include credit card details, password, emails and work data.
- Losing or having a phone stolen can expose this information and harm business
- This can lead to PR disasters and legal problems
- If data can't be protected on stolen devices, don't store important information on them
- Teaching people about there risks can be effective.
- Avoiding storage of sensitive data on risky devices reduces theft or loss risks.

Q State some attacks on Mobile devices.

Sol There are the following attacks on mobile devices :-

- Phishing : Fake messages or emails trick you into giving away personal info.
- Malware : Harmful software that can mess up your phone or steal your data
- Main-in-the-Middle (MitM) : Hackers intercept your communication to steal information
- SIM Swapping : Hackers trick your phone company to take over your phone number
- Ransomware : Software that locks your phone and demands money to unlock it.
- Network Spoofing : Fake wifi networks that steal your information when you connect
- Bluetooth Attacks : Hackers use Bluetooth to access your phone without permission
- Jailbreaking / Rooting : Modifying your phone to remove limits, which can make it easier to hack

Q What are the security implications for organizations.

Sol Managing Diversity and Proliferation of Hand-held Devices:

- Cyber security is a top priority for most organizations.
- Many organizations forget to keep track of who owns mobile devices long-term
- All employee mobile devices should be listed in the company's asset register.
- It's important to monitor how these devices are used
- When an employee leaves, their access to company networks must be revoked.

Unconventional / stealth Storage Devices:-

- USB drivers and similar devices used by employees can be a cyber security risk.
- These devices are getting smaller and more varied with new technology
- They are hard to detect, posing a big security concern
- Their small size makes them easy to hide.
- It's best to ban these devices to prevent viruses and data loss.

Threats through Lost and stolen Devices:

- Lost and stolen devices are a growing cyber security concern.
- people often lose their mobile devices while travelling.
- Lost devices are a big security risk for companies.
- The threat is worse because mobile devices often have weak security
- The devices value is small concerned to the important data it holds
- Lost devices with wireless access to company networks are a major security problem

Q Discuss credit card frauds in mobile and wireless computing era.

Sol Credit card frauds have become increasingly prevalent in the mobile and wireless computing era due to the widespread use of smartphones and wireless technologies.

Types of Credit Card Frauds:

⇒ Phishing:- fraudsters sends fake message or emails that appears to be form legitimate source to trick use to stole data.

- Smishing :- Similar to phishing but uses SMS message to devive users into provide personal and financial information.

- Card Skimming :- Devive are attached to card readers (e.g. ATMs, POS terminals) to steal card information during transactions.

and many more ways to create credit card frauds are present.

Q Factors Contributing to Mobile and Wireless Credit Card Frauds ?

Sol
- Increased use of Mobile payments.
- Public Wi-Fi networks.
- Lack of Awareness
- Weak Security Measure.

Q How to prevent it ?

Sol
- Two - Factor Authentication
- Use of Secure Network
- Regular Networking
- Strong Password and Biometrics
- Updating software.
- Education and Awareness

UNIT-2

COMPLETE

THANK YOU

SUBSCRIBE CHANNEL

@MULTIATOMST

UNIT - 3

CYBER SEQURITY

ONE SHOT VIDEO

SUBSCRIBE MUHTI ATOMS T

JOIN TELEGRAM FOR NOTES

⇒ 7 TOOLS USED IN CYBER CRIME

. Malware :
-> It is a Bad software
-> Steal info, locks data for ransom, or message up your device.

. Phishing Kits :
-> Fake Websites and emails.
-> Tricks you into giving personal info like passwords and credit card numbers

. Key loggers :
-> Tools that record everything you type.
-> Steals your password and other typed information.

. Botnets :
-> Networks of hacked devices controlled by cyber criminals
-> Sends spam, attacks website or spread malware

RATs (Remote Access Trojans) :
-> Software that lets hackers control your computer
-> Spies on you, steals info, and changes your system setting

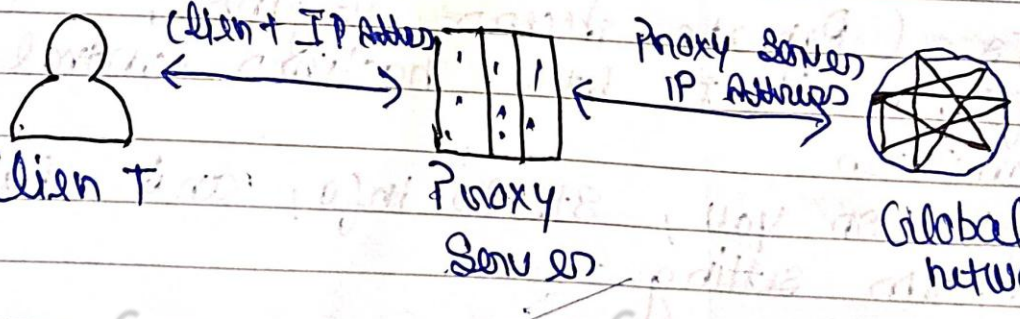
- Exploit kits:
  -> Packs of tools that exploit security holes in software.
  -> Help hackers inject your device with malware.

- Denial of Service (DoS) Tools:
  -> Tools that flood a website or network with too many requests.
  -> Make website or service crash or became unavailable.

PROXY SERVER

- A proxy server is an intermediate server that sits between a user's device and the internet.

- When a user make a request to access a website, the request first goes to the proxy server, which then forward the request to the website.

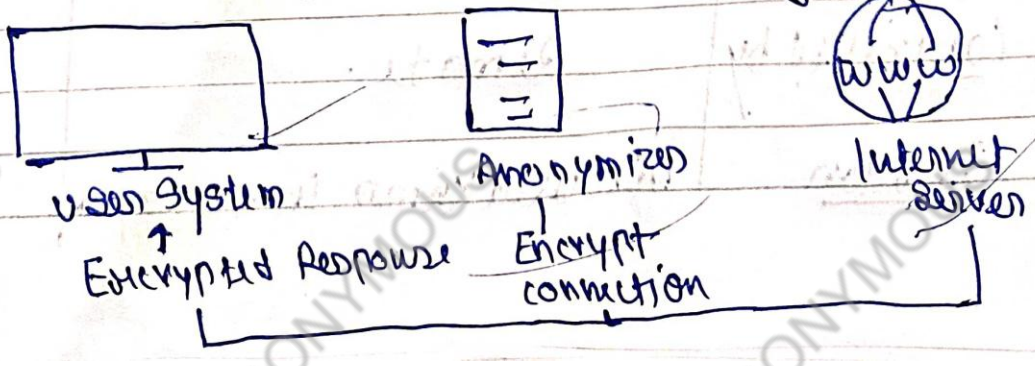


Types of Proxy Servers

- Forward Proxy: The client sends a request to the forward proxy, which then sends the request to the internet on behalf of the client.
- Reverse proxy: The reverse proxy receives requests from the internet and then forwards those requests to the appropriate server.
- Transparent Proxy: Transparent proxies are often used in corporate environments to monitor and control access to the internet.
- Anonymous Proxy: An anonymous proxy is a proxy that hides the user IP address, providing an additional layer of privacy.

ANONYMIZERS

- An anonymizer is a tool that is used to hide a user's identity when accessing the internet.



VIRUS VS WORMS

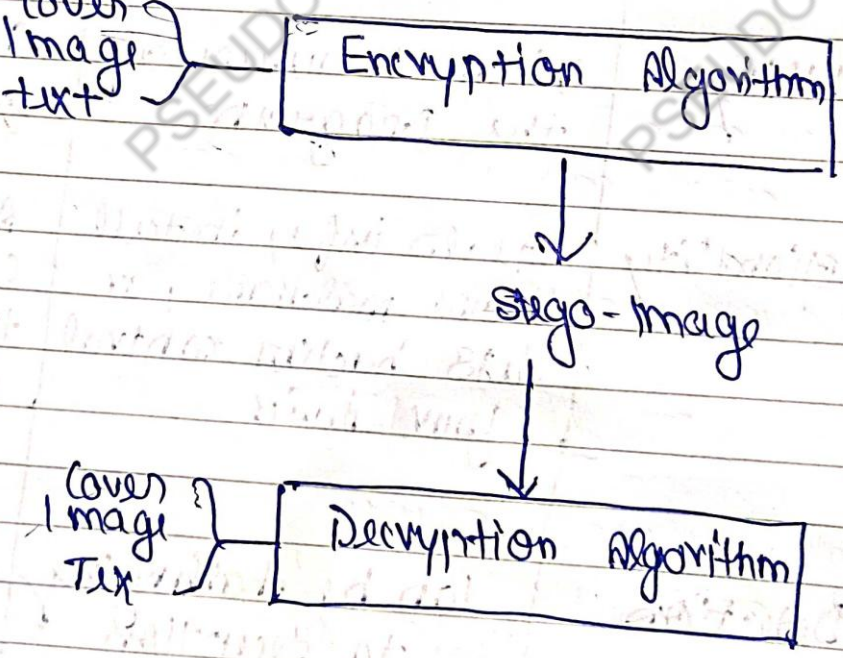
Basics	Worms	Virus
Definition	A worm is a form of malware that replicate itself and can spread to different computers via network.	A virus is a malicious executable code attached to another executable file which can be harmless or can modify the data.
Objective	The main objective of worms is to eat the system	The main objective of viruses is to modify the information
Host	It doesn't need a host to replicate from one computer to another	It requires a host to spread
Harmful	less Harmful	More harmful
Detection and Protection	By Antivirus and firewall	Antivirus softwares
Controlled by	Remote.	Not remotely
Execution	via weakness in the system	Via executable file

TROJAN HORSE Vs BACKDOOR

S.NO	Aspect	Trojan Horse	Backdoor
1.	Purpose	Bad software pretending to be something good	Secret ways to get into a system without normal password.
2	Works	You download and run it, thinking its safe.	Hackers or developers put it there without you knowing
3	Visibility	Victim is aware of the program	Often hidden from the user
4.	Functionality	Steals info, install more malware, or lets hacker control your device	Allow hackers to come and go as they please, stealing info or causing harm
5.	Detection	Can be challenging due to deception	Can be detected through monitoring
6.	Example	Zeus	Netcat

=> STEGANOGRAPHY

- Steganography is like hiding a secret messa in plain sight.
- Instead of encrypting the message, you hide within another seemingly innocent file like an image audio file or even a text document.
- The goal is to hide the existance of the messag making it difficult for other to detect.



techniques :-

- Image Steganography :- Embedding data within images by subtly altering pixel values
- Audio Steganography :- Hide information within audio files by modifying certain components such as the amplitude or frequency
- Text Steganography :- Hiding information within text by using techniques like white space manipulation, word or letter arrangement
- Video Steganography :- Embedding data within video files
- File Steganography :- Hiding data within seemingly innocuous files such as document or executable files

SQL INJECTION

- SQL Injection is a code-based vulnerability that allows an attacker to read and access sensitive data from the database.
- A successful SQL injection attacks can badly

affect websites or web application using relational databases such as MYSQL, Oracle or SQL server.

IDENTITY THEFT

- Identity theft also called Identity fraud is a crime that is being committed by a huge number nowdays
- Identity theft happens when someones steals your personal information to commit fraud.
- This theft is committed in many ways by gathering personal information such as transactional information of another person to make another transaction

=> Techniques of Identity theft :-

- Pretext calling :- Thieves pretending to be an employee of a company over phone asking for financial information.
- Mail theft :- This is a technique in which credit card information with transactional data is extracted from the public mailbox.

- **Phishing :-** This is a technique in which emails pertaining to be from banks are sent to a victim with malware in it.

- **Card Verification Value Code :-** The card verification value number is located at the back of your debit cards. This number is used to ahance transaction security but Several attackers ask for this number while pretending as a bank official.

=> **Prevention**

- Two-factor Authentication
- Strong Password
- Update Software
- change your PIN and Password Regularly
- check your account daily.
- Don't install random software from the Internet
- Do not disclose your information over the phone

COMPLETE THANK YOU

SUBSCRIBE MULTI ATOMS+

Join TELEGRAM FOR NOTES

Cyber Security

UNIT-4 ONE SHOT with PYQs.

Topics:

→ Introduction, Digital forensics Science.

→ The need for Computer forensics.

→ Cybir forensics & Digital Evidince. [2023-24]

→ forensics Analysis of E-mail. [2023-24]

→ Digital forensics life Cycle. [2023-24]

→ Chain of Custody Concept & Network forensics.

→ Approaching a Computer forensics Investigation.

→ Forensics & Social Networking sites:

~~The Network~~

* The Security / Privacy Threats, [2023-24].
* Challenges in Computer forensics.

Page No.
Date / /

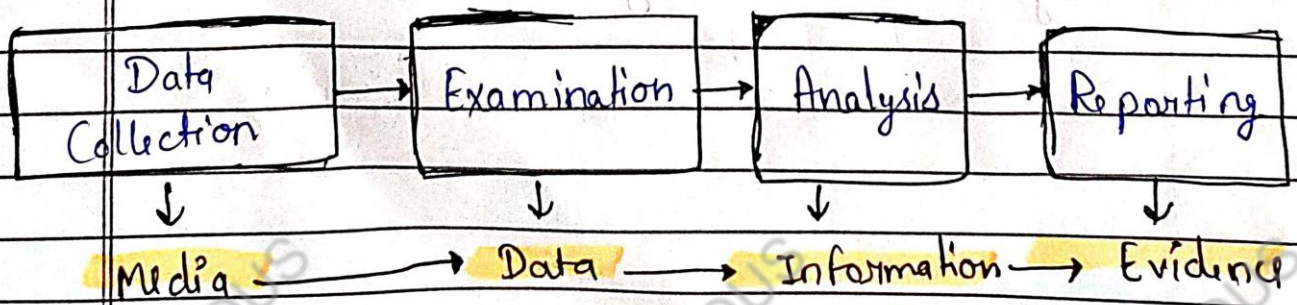
Digital Evidence [2023-24] [2 marks]

Information stored or transmitted in digital form that can be used in a court of law.

It includes a wide range of data types and sources, all of which must be handled with care to ensure their integrity & admissibility.

Types of Digital Evidence

1. Files & Documents:-
   Text documents, images & videos.
2. Emails & Communications:
   Emails, chat logs, SMS and social media Comm°
3. System logs & Meta data:
   access logs, time stamps.
4. Browser History & Cache:
   URLs visited, cookies
5. Database Records:
   Entries in databases, queries.



Process of Collection Digital Evidence.

[AKTU - 2023-24] [7 marks]

Forensics Analysis of E-mail :

→ Email forensics involves the analysis of email messages to uncover relevant information is an investigation.

→ This include identifying the sender & recipient, analyzing the content, attachments and headers & tracing the email's origin & path.

→ There are many tools available that help create fake mails. but forensics Analysis of E-mail helps in authenticity of an E-mail when suspected.

→ Mail Server Software is a network server software that control the flow of E-mail

→ The mail client software helps each user to read, send & delete messages.

→ E-mail tracking is done by examing the header information

• Header Analysis of e-mails.

- Information about Senders of an e-mails.
- path through which e-mails have travelled.
- Information about Spoofing.

Page No..
Date / /

Link Analysis

→ Used to identifying the links between the suspects.
→ Graphical data analysis method.

Bait Tactics

- Extracts IP address of the culprit.
- Email with http: <img src> tag is sent to the suspect.
- IP address of recipient is recorded.

Mail forensic Tools

- eMail TrackerPro
  - Can locate the position of IP address
  - Misuse reporting.

- Ad complain
  - Robotically identify the message
  - Compute misuse report

- FINAL eMAIL
  → Can recover the e-mail database file.
  → locates lost e-mails.

[AKTU - 2023-24] [7 marks]

Digital forensics Lifecycle

→ firstly you have to write about Digital forensics.

The Digital forensics life cycle consists of several stages: aimed at identifying, collecting, analysing & preserving digital evidence.

① **Identification**: Determining what digital evidence is relevant to the investigation.

② **Preservation**: Ensuring the integrity of the evidence by creating exact copies and protecting the original data.

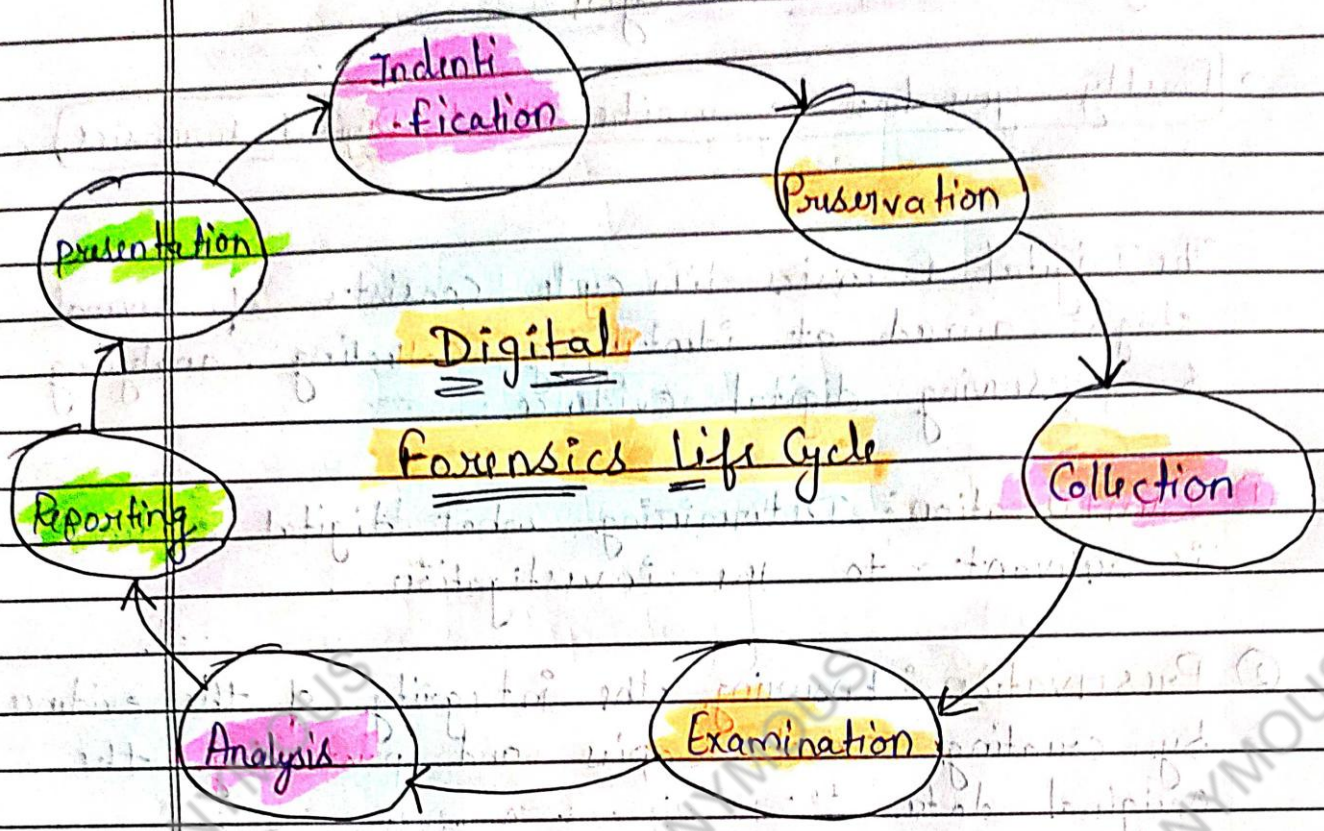
③ **Collection**: Gathering the digital evidence from various sources.

④ **Examination**: Analyzing the data to extract relevant information.

⑤ **Analysis**: Interpreting the extracted data to build a case

⑥ **Reporting**: Presenting the findings in a clear & concise manner.

⑦ **Presentation**: providing the evidence and findings in a court of law.



Chain Of Custody Concept

→ The chain of custody is a critical in digital forensics. It refers to the documentation & handling process of evidence from the moment it is collected untill it is presented in court.

→ Maintaining an unbroken chain of custody ensures that the evidence has not been tampered with & is admissible in legal proceedings

→ protects evidence from alteration, loss ~~or Communicatio~~

→ details of who handled the evidence, when, where & why.

→ Each transfer of evidence is verified & recorded.

process same as Collection Digital Evidence

Network forensics

→ Network forensics involves monitoring and analyzing computer network traffic to identify & investigate security breaches, cyberattacks & other network-related incidents.

→ This field requires specialized tools & techniques to capture & examine network packets.

Techniques:

- Packet Analysis: Examining network packets using tools like wireshark to identify suspicious activities.
- Traffic Monitoring: Using network monitoring tools to detect unusual traffic patterns.
- Flow Analysis: Analyzing network flow data to identify communication patterns.

Page No..
Date / /

Steps in Network forensics

1. Data Collection
2. Data Preservation
3. Data Analysis
4. Incident Reconstruction
5. Reporting

- **Approaching a Computer Forensics Investigation.**

→ Secure the subject system

→ Quickly & effectively responding to the incident to mitigate damage and preserve evidence.

→ Identify & recover all files

→ Examining the data to uncover evidence and build a case.

→ Documenting the findings & p

Preparation (1) — Incident Response (2) — Data Acquisition (3) — Data Analysis (4) — Reporting (5)

Page No.:
Date: / /

Forensics & Social Networking Sites:

→ It involves the application of digital forensic techniques to investigate & analyze activities, behaviours, & data on data on social media platforms.

→ It is a critical aspect of modern digital investigations.

→ Analyze evidence while respecting user's privacy & maintaining data integrity.

[AKTU - 2023-24] [7 marks]

Q. what are privacy threats? what are the challenges faced?

* The Security / privacy Threats.

→ Security & Privacy threats on social networking sites are diverse & evolving.

→ Users & Organizations must remain robust Security practices, such as strong passwords, two-factor authentication, and regular monitoring of accounts.

→ Additionally, social networking platforms must continuously enhance their security measures to protect user data and maintain trust.

→ Data Breaches:
Unauthorized access to personal data, leading to fraud.

→ Malware Distribution:
Malicious links or files infect devices with malware.

→ Cyberbullying & Harassment:
online bullying & threats causing emotional harm.

→ Impersonation & fake Accounts:
Creation of fake profiles for fraud & mis information.

→ Challenges in Computer Forensics

1. Data Volume & Variety:
Handling and analyzing large amounts of different types of data.

2. Encryption & Privacy Protection:
Accessing data protected by encryption & respecting privacy laws.

3. Rapid Data Deletion:
Recovering Data that is quickly deleted or disappears.

4. Anonymity & Pseudonymity:
Identifying users who use fake or anonymous profiles.

Page No.:
Date: / /

5. Jurisdictional Issues:
Dealing with different legal rules across various regions.

6. Evolving Technologies:
Keeping up with constant changes in technology & platforms.

Unit-4 Complete

Subscribe

Multi Atoms &

Multi Atoms Plus

Date : __ / __ / ____

UNIT-05 (CSS)

- Need For an information Security Policy
- Indian Cyber Law
- Digital Personal data Protection Act 2023
- Intellectual Property Issues
- Patent, Copyright, Trademarks

Date : __/__/____

Information Security Policy :-

- An Information Security Policy is a set of rules and guidelines that an Organization creates to protect its information and technology
- It Outlines how employees and System should handle and protect sensitive data
- A Security Policy is a written document in an Organization Outlining how to protect the Organization from threats

Why is it Important :-

1. Protection of Data :-
   - Helps keep important information safe from unauthorized access, use.
   - This includes Customer data, Company secrets and Financial information.

2. Risk Management :-
   - Identifies Potential Security threats and Provides measure to Prevent them
   - This reduce the risk of data breaches or Cyber attacks

3. Compliance :-
   - Ensures the Organization Follows Laws and regulations related to data Protection.

Date : __/__/____

4. Consistency :-
- Provides a clear Framework for everyone in the Organization to Follow, ensuring that all employees handle data in a secure and Consistent manner

5. Trust :-
- Builds trust with customers, partners and stockholders by demonstrating a commitment to protecting their data.

Key Components of a Security Policy

1. Access Control
2. Data Protection
3. Employee Responsibilities
4. Training and Awareness

Indian Cyber Law :-

Cyber Law :-

→ Cyber Law is a set of rules and regulations that govern how people use the Internet and digital devices

→ In India, Cyber laws are designed to protect users from online crime and ensure safe and

Date : __/__/____

secure use of the internet.

Importance of Cyber Law :-

1. Protect Individuals and Organizations
2. Protect Safe Online Transactions
3. Regulates Digital Content

- The Primary Law governing Cyber activities in India is the IT Act 2000 (Information Technology Act).

- Legal Recognition of electronic Transaction
→ IT Act recognizes electronic contracts and digital signatures making online transactions legally valid.

- Cyber Crime Provisions :-
→ Define Various Cyber Crimes such as hacking, Unauthorized access to computer System

- Data Protection :-
→ Establishes guidelines For the Protection of Personal data and privacy Online

- Government Powers :-
→ Block websites and monitor online activity.

Date : __/__/____

Advantages of Cyber Law:

- Organizations are now able to carry out e-commerce using the legal infrastructure provided by the Act.
- Cyber Law provides both hardware and Software security
- Digital Signature have been given Legal Validity

Digital Personal Data Protection Bill 2023:

- Is to establish a Comprehensive Framework For the Protection of Personal data

Features:

1. Applicability:
   - → Collected Online
   - → Collected offline and is digitised
   - → It will also apply to the Processing of Personal data Outside India if it is For Offering goods or Services in India

Date : __/__/____

2. Consent :-

→ Personal data may be processed only for a lawful purpose after obtaining the consent of the individuals.

3. Rights and duties of data principle (Individual)

→ An individual whose data is being processed will have to right

1. Obtain information about processing
2. Seek correction and erase (erasure of personal data
3. Nominate another person to exercise rights in the event of death

4. Obligations of data fiduciaries

→ Reasonable efforts

→ Erase personal data

Data Protection Board of India :-

→ The central government will establish the data protection Board of India.

Key Functions :

(i) Monitoring compliance and imposing penalties

(ii) directing data fiduciaries to take

Date : __/__/____

necessary measures in the event of a data breach.

(iii) hearing grievances made by affected persons

Tenure of Board :-

→ Two years (member)

→ no of members of the board and the selection process

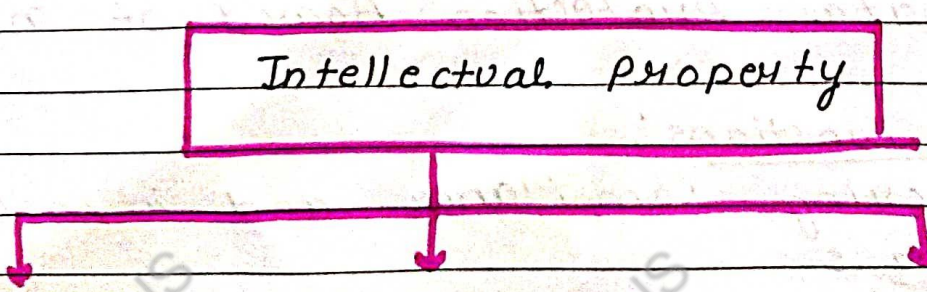
Intellectual Property :-

↓
Creation of mind

- Intellectual Property refers to Creations of the mind, such as inventions, literary and artistic works, designs, symbols.

- Intellectual Property is Protected in Law by, For example Patent, Copyrights and trademarks.

Intellectual → Creativity, Idea
Property → owned or Registered



1. Patent 2 Copyright 3 trademarks

Date : __ / __ / ____

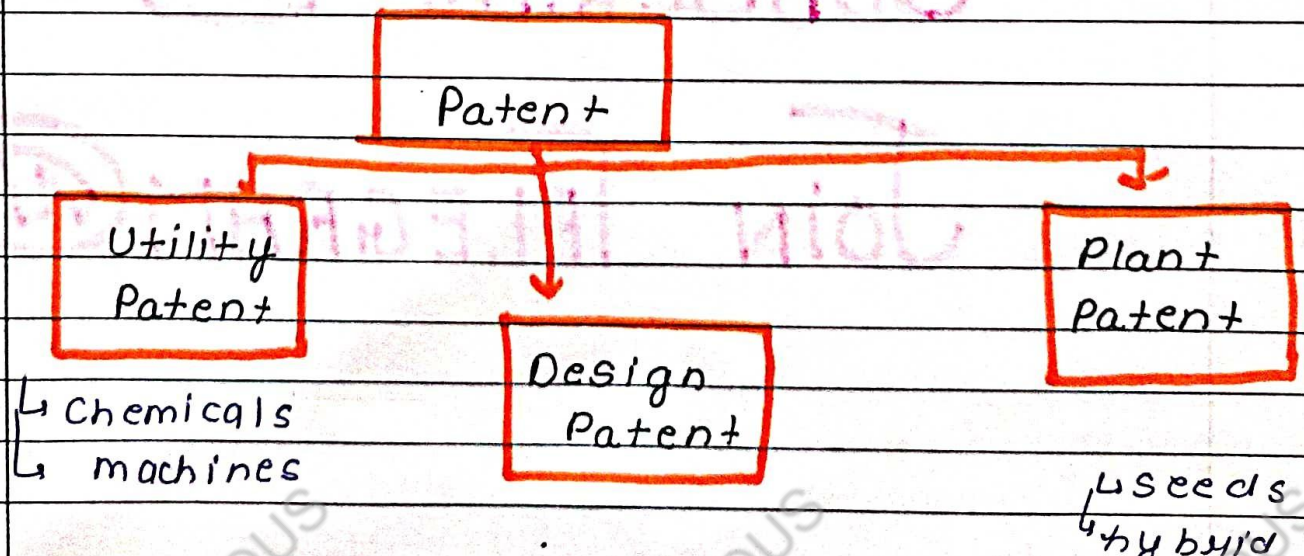
Patent :-

→ A Patent is granted as an exclusive right by the government to a true and First inventor For a limited Period of time In exchange For the Public disclosure of an invention

→ Valid of a Certain Period of time [20 Year] after Free For Public

Objectives :-

1. To encourage Inventions by Providing Protection to investors From infringement of theory inventions
2. To Provide maximum benefits of Inventions to the ~~Securit~~ Society by Securing the working



Date : __/__/____

Copyright :-

→ It is a Form of legal right
→ given to the Creator who has ownership in literacy, musical or any other artistic work
→ Sound, recording etc

Trademark :-

→ any word, Phrases, symbol, design, identifies the source of your goods or services

→ Provide legal Protection For your brand.

AKTU NEXTGEN ENGINEERING

WHATSAPP GRP

1 & 2 YR

3 & 4 YR

FREE COURSES