DATE: __/__/____
PAGE: _____

TCP/IP: Transmission Control Protocol / Internet Protocol.
4 layers of TCP/IP model ⇒

i) Application layer: Process to Process. Synchronizing various encoding systems, encryption, decryption & creating and maintaining data generation.

ii) Transport layer: Host to host. TCP, UDP, SMTP. deciding connection oriented or connectionless transmission.

iii) Internet layer: Source to destination., IP addressing in header of source or destination

iv) Physical layer: Node to node. How to transmit data from one node to another (Network access layer)

TCP Header: Segment = Header + Data generated

TCP header

Source Port (16)				Destination Port (16)				→ 4B
Sequence Number (32)								→ 4B
Acknowledgement No. (32)								→ 4B
Header length (4)	Reserved bit (4)	URG	ACK	PSH	RST	SYN	FIN	Window Size (16) → 4B
			Flag bit (occupying one bit each) Flag field					
Checksum (16) identifying the error						Urgent Pointer (16)		→ 4B
Options (0-40 B)								→ 20B

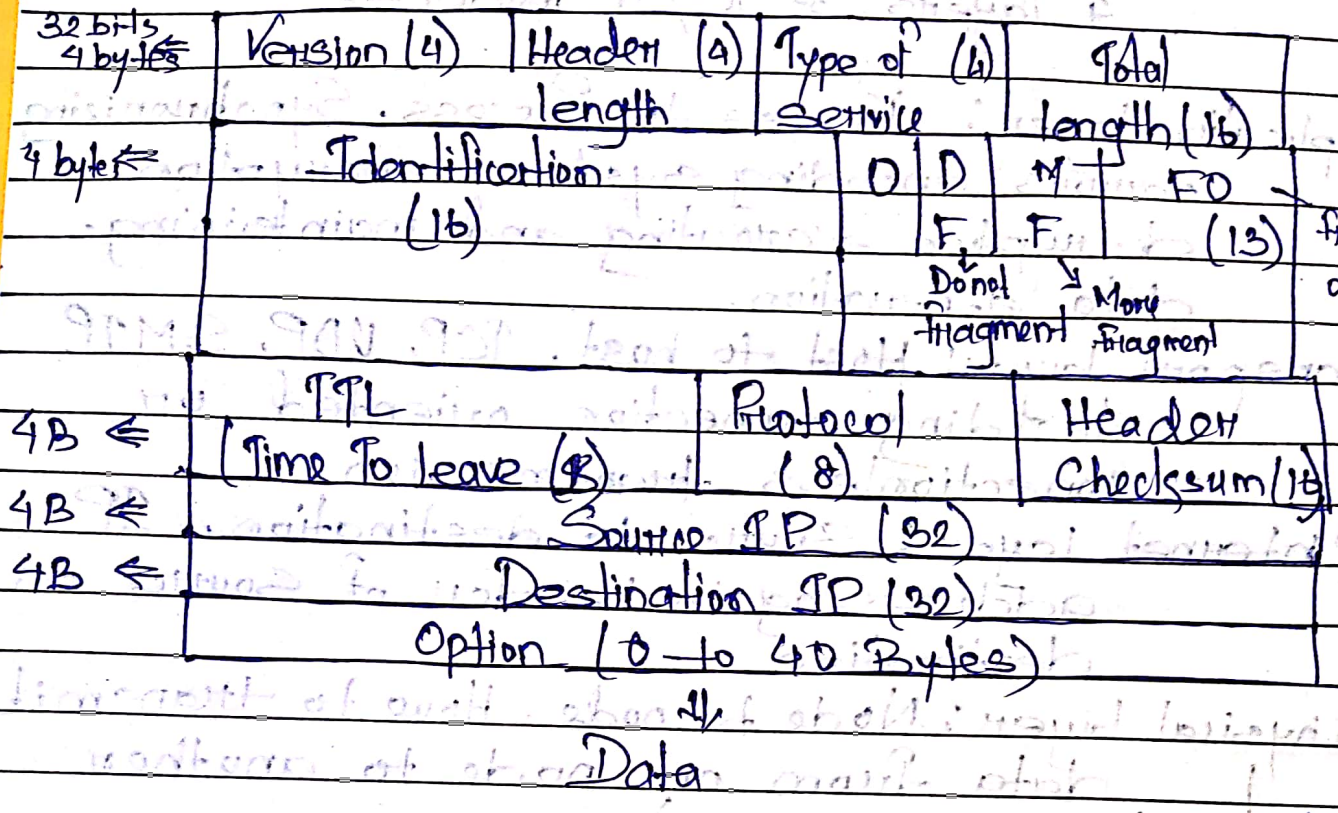
Data

Minimum = 20B
Maximum = 60B.

Good Write

DATE: __/__/____
PAGE: _____

IP header:



Cyber Forensic:

The preservation, identification, extraction, documentation and interpretation of computer media for evidentiary and/or root cause analysis is called cyber forensic.

Cyber attacks: Most common cyber attacks-

i) Blocks access to key components of the network.
ii) Install malware or additional harmful software.
iii) Covertly obtains information by transmitting data from the hard drive

Good Write

iv) Disrupts certain components and renders the system inoperable.

Cyber Security:

Denotes the technologies and procedures to safeguard resources from unlaw

Cyber Security Policy ⇒

⇒ An authority framework that defines and guides the activity associated with the security of cyberspace.

⇒ Provides an outline to effectively protect information, information systems and networks.

⇒ Manages the entire field of ICT users & providers.

Cyber Crimes:

⇒ Crimes directed at a computer or a computer network.

⇒ Cyber crime normally refers to a criminal activity where computer or network is used as a tool or target of a crime.

DATE: __/__/____
PAGE: _____

⇒ Computer as a tool: When individual is the main target of the crime committed by the offenders then the computer can be described as a tool and not the target.
example: cyber stalking, cyber theft.

⇒ Computer as a target: These crimes are comitted by a selected groups of people with technical knowledge by comitting a series of acts in the planned manner.
example: web defacement, cyber terrorism.

☒ Categories:

i) Cyber crimes against person: Include harrassment of someone with the use of a computer.

ii) Cyber crimes against property: Intellectual property crimes, cyber vandalism.

iii) Cyber crimes against government/firm/company: Cyber terrorism, pyrated software distribution

iv) Cyber crime against society: Online gambling, selling illegal articles.

DATE: __/__/____
PAGE: _____

Kinds of Cyber Crime:

i) Unauthorised Access and hacking
ii) Virus, Worms and Trojan Attack
iii) E-mail related crimes
iv) Internet Relay Chat relating crimes.
v) Sale of Illegal Articles.
vi) Online Gambling
vii) Phishing
viii) Intellectual Property Crimes
ix) Web defacement
x) Cyber Stalking

i) Unauthorised Access and Hacking: Refers to any kind access without seeking the permission of either the true owner or person in charge of a computer. Hacking/Cracking is a crime for gaining unauthorized access to the data stored in system. Purpose: personal monetary gain.

ii) Virus, Worms and Trojan Attack: Virus is a program that is capable of infecting other program and making copies of itself.

Worms is a program that multiply like viruses but spread from one computer to another. Not required to attach themselves to a host programme.

Trojan attacks is a program which functions from inside what looks like unauthorized program, thereby concealing what it is actually doing.

Good Write

DATE: __/__/____
PAGE: _____

iii) Email related crimes:

- Email spoofing ⇒ a fraudulent email activity with intent to cheat the other party.
- Email spamming ⇒ refers to sending of bulk mails to thousands and thousands of users by an identified or unidentified source. It results in reduction of productivity and wastage of time.
- Email bombing ⇒ Sending huge volumes of e-mails to a particular address which results in crashing of victim's e-mail account or mail servers. Blocks inbox continuously with numerous identical emails.

iv) Sale of illegal article: Sale of narcotics drugs, weapons and wild life etc. Websites, auction websites and bulletins board may be used for posting such information.

v) Phishing: Cracking sensitive information such as username, password, credit card details, account data etc. by disguising as a trustworthy entity.

vi) Intellectual property crimes: Distribution of pirated software, copyright infringement, trade violations

DATE: __/__/____
PAGE: _____

vii) Web Defacement: Substitution of the original homepage of a ~~weeb~~ website with another page by a hacker or a cracker. The substituted page contains pornographic or defamatory material.

viii) Cyber Stalking: Use of internet, e-mail or other electronic communication devices to stalk, or threatens another person by making harassing phone calls, leaving written messages or objects.

ix) Cyber vandalism: It refers to damaging or destroying the data or property rather than stealing or misusing them.

Digital forensic: Digital forensic is used to supplement investigations.

Digital Forensic Science: The use of scientifically derived and proven methods towards the preservation, collection, validation, identification analysis, interpretation, documentation and presentation of digital evidence derived from digital sources to find the criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operation.

DATE: __/__/____
PAGE: _____

- Communities: There are at least 3 distinct communities within Digital Forensic.
  - ⇒ Law Enforcement = Courts
  - ⇒ Military = Information welfare
  - ⇒ Business Industry = Critical Infrastructure Protection.

- Cyber forensic include:

1) Network forensic: A subcategory of digital forensic that essentially deals with examination of network and its traffic going across a network that is suspected to be involved in malicious activities.

Processes involved in Network forensic:

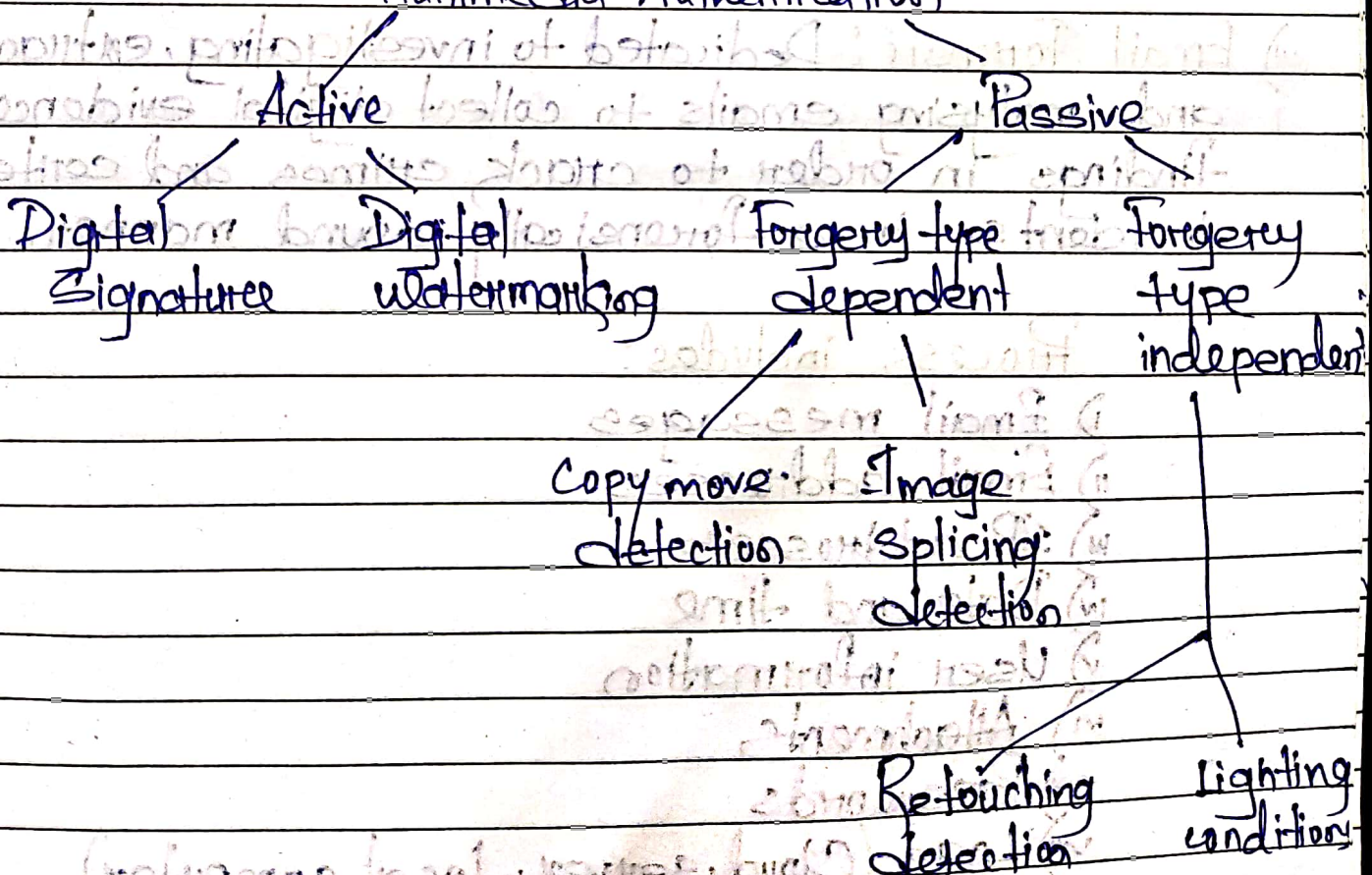
1. Identification: Investigators identify and evaluate the incident based on network pointers.
2. Safeguarding: Investigators preserve and secure the data so that the tempering can be prevented
3. Accumulation: A detailed report of the crime scene is documented and all the collected digital shreds of evidence are duplicated.
4. Observation: All the visible data is tracked along with the metadata.
5. Investigation: A final conclusion is drawn from the collected shreds of evidence.
6. Documentation: All shreds of evidence, reports are documented and presented in court.

Good Write

DATE: __/__/____
PAGE: _____

Challenges in Network forensic:
i) Manage the data generated by the process
ii) Intrinsic anonymity of the IP.
iii) Address spoofing.

ii) Media Forensic: Media forensic is the use of scientifically derived and proven methods towards the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from the digital sources for the purpose of facilitation or furthering the reconstruction of events found to be criminal



DATE: __/__/____
PAGE: _____

- Active Image Authentication: A known authentication code is embedded in the image at the time of image generation & sent with the image for accessing its integrity at the receiving end. Verifying this code authenticates the originality of the image.

- Passive Image Authentication: Uses the only image with no prior information for accessing the integrity of the image. Passive works on the assumption that even though tampering with the image may not leave any visual trace but they are likely to alter the underlying statistics.

iii) Email Forensic: Dedicated to investigating, extracting and analysing emails to collect digital evidence as findings in order to crack crimes and certain incidents in a forensically sound manner.

Process includes:

i) Email messages
ii) Email addresses
iii) IP addresses
iv) Date and time
v) User information
vi) Attachments
vii) Passwords
viii) Logs (Cloud, server, local computer)

DATE: __/__/____
PAGE: _____

- Major investigative extraction working directions of email forensic:

i) Local Computer-based emails;
ii) Server based emails
iii) Web-based emails

- Email tracing and investigation: The victim's email should be examined carefully.

Sometimes, criminals may be use proxy servers to send emails in order to mislead the investigation. The cooperation of the email service provider is required to obtain the postal address of the corresponding IP addresses used to carry out the offence.

Sometimes, the investigation may lead to cyber cafe or open wifi or other public computer.