DATE: __/__/____
PAGE: _____

Cyber forensics

The preservation, identification, extraction & interpretation ~~and anal~~ of computer media for evidentiary or/and a root cause analysis is called cyber forensics.

Digital forensic science

The use of scientifically derived and proven methods towards the preservation collection validation analysis interpretation documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal or helping to anticipate unauthorized actions shown to be disruptive to planned operations.

Types of computer or cyber forensics.

i) Disk forensics :-

It deals with extracting raw data from the primary or secondary storage of the device by searching active, modified or deleted files.

ii) Network forensics :-

It is a sub-branch of computer forensics that involves monitoring and analyzing the computer network traffic.

iii) Database forensics :-

It deals with study and examination of database and their related metadata.

Good Write

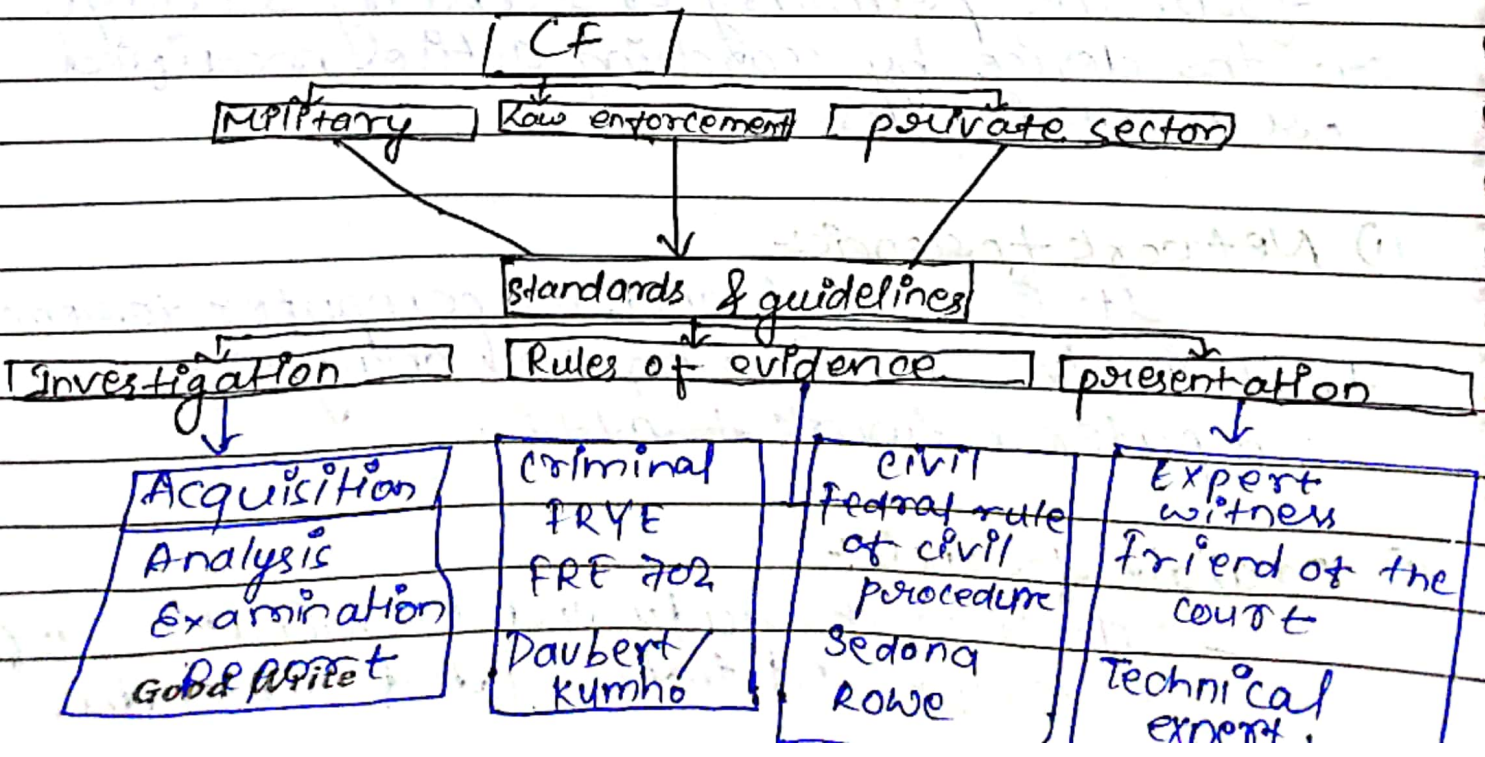
Malware forensics:-
Deals with the identification of suspicious code and studying viruses and worms.

Email forensics:-
Deals with emails and their recovery and analysis including deleted emails calenders and contacts.

Memory forensics:-
Deals with collecting data from system memory in raw form and then analyzing it for further investigations.

Mobile phone forensics:-
Deals with the examination and analysis of phone and smartphones and helps to retrive contacts, call logs, incoming, outgoing SMS etc and other data present in it

Fundamentals of CF



There at least 3 distinct communities within digital forensics

- Law Enforcement
- Military
- Business & industry

Digital forensics science

- Law Enforcement (courts)
- Military (Information welefare)
- Business & Industry (critical infrastructure protection)

Cyber forensics includes
Networks
small scale Digital Devices
Storage media
Code Analysis

Skills required for becoming cyber forensic investigator.

Reverse Steganography :-
It's a method of hiding important data inside the digital file image etc so cyber forensic experts do reverse steganography to analyze the data and find a relationship with the case.

Stochastic forensics :-
The experts analyze and reconstruct digital activity without using digital artifact

Cross drive analysis :-
the info found on multiple computer drives is correlated and cross-references to analyze and preserve info that is relevant to the investigation.

Live analysis :-
the computer of criminals is analyzed from within the OS in running mode. It aims at the volatile data of RAM to get some valuable information.

Deleted file recovery :-
Searching for memory to find fragments of a partially deleted file in order to recover it for evidence purpose.

Effective communication abilities
pay close attention to the details.
Technical aptitude
Analytical skills

Computer Forensic Requirements

Hardware :-

- familiarity with all internal and external devices / components of a computer.
- Thorough understanding of hard drives and settings.
- Understanding motherboards and the various chipsets used.
- power connections
- Memory.

Basic input output system (BIOS)

- Understanding how the BIOS works
- Familiarity with the various settings and limitations of the BIOS.

Operation Systems

- Windows 3.1 / 95 / 98 / ME / NT / 2000 / 2003 / XP
- DOS
- UNIX
- LINUX
- VAX / VMS

Software

- Familiarity with most popular software packages such as Office.

Good Write

Forensic Tools

familiarity with computer forencis techniques and the software packages that could be used.

Admissibility of Evidence

Legal rules which determine whether potential evidence can be considered by a court.

Must be obtained in a manner which ensures the authenticity and validity and that no tampering had taken place.

Handling evidences.

Establishing and maintaining a continuing chain of custody.

Initiating an investigation

Donot begin by exploring files on system. randomly.

Establish evidence custodian.

collect email, DNS, and other network service logs.

Capture exhaustive external TCP and UDP port scans of the host.

Contact security personnel, management and local enforcement.

DATE: __/__/____
PAGE: _____

Incidence Response

- Identify, designate or become evidence custodian
- Review any existing journal if some case has been done with the system.
- Begin new or maintain existing journal.
- Install monitoring tools.
- Without rebooting or affecting running processes, perform a copy of physical disk.
- Capture network information.
- Capture processes and files in use.
- Capture config information.
- Receipt and signing of data.

Handling Information

- Information and data being sought after and collected in the investigation must be properly handled.
- Volatile info
  - ↳ Network info
  - ↳ Active processes
  - ↳ Logged-on Users
  - ↳ open files.

DATE: __/__/____
PAGE: _____

Non-volatile info:-

- This includes information, configuration settings, system files and registry settings that are available after reboot.

- This information should investigated and reviewed from a backup copy.

- Accessed through drive mappings from system.

Cyber forensics activities

- secure collection of computer data
- Identification of suspect data
- examination
- presentation to the courts of law.
- application of a countrys law to computer practice.

Methodology for Cyber forensics :-

- Acquire :- evidence without altering or damaging the original.

- Authenticate the image

- Analyze :-
  the data without modifying it.

Cyber crime :-

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

Locard's principle applies when a person commits a crime something is always left at the scene of the crime that was not present when the person arrived.

Digital evidence :-

Digital data that establish that a crime has been committed, can provide a link between a crime and its victim or can provide a link between a crime and the perpetrator.

Digital crime scene :-

Electronic environment where digital evidence can potentially exist

Principle of cyber forensics :-

1. When dealing with digital evidence, all of the general forensic and procedural princip must be applied.
2. Upon seizing digital evidence actions taken should not change that evidence

3. When it is necessary for a person to access original digital evidence, that person should be trained for the purpose.

4. All activity relating to the seizure access, storage or transfer of digital evidence must be fully documented preserved and available for review.

5. An individual is responsible for all actions taken with respect to digital evidence while the digital evidence is in their possession.

6. An agency which is responsible for seizing, accessing, storing or transferring digital evidence is responsible for compliance with these principles.

Computer forensics is a four step process:-

- Acquisition
- Identification
- Evaluation
- Presentation

Process / phases:-

- Identification
- collection
  - Bag & Tag
- preservation
- Examination
- Analysis
- Presentation

Good Write

We can demonstrate that the Image is true or unaltered by using MD5 or SHA 256 algorithms.
It helps to find authenticity & integrity of the data

Examination of evidence can be done by the following ways:-

(i) Examine directory tree
(ii) Perform keyword searches
(iii) Search for relevant evidence types.
(iv) Look for obvious first.

Issues:-
Lack of certification for tools
Lack of standars.
Rapid change in tech
Immature scientific discipline.

Evidence processing guidelines

Step 1:- Shut down the computer

Step 2:- Document hardware configuration

Step 3:- Transport the computer system to secure location.

Step 4 : Back ups of Hard Disk and floppy disks.

DATE : / /
PAGE :

Step 5
Mathematically authenticate Data on all storage device.

Step 6 :-
Document the system date & time.

Step 7
Mak a list of key search words

Step 8:
Evaluate the windows Swap file

Step 9:- Evaluate file slack

Step 10:- Evaluate Unallocated Space

Step 11: Search files, file slack and unallocated space for keywords

Step 12 : Document file names date and time.

Step 13: Identify file, program and storage anammolies

Step 14: Evaluate program functionality

Step 15: Document your findings

Step 16:- Retain copies of software used.

Good Write

DATE: __/__/____
PAGE: _____

Methods of data hiding :-

- Covert channels
- Steganography
  The art of hiding information in such a way that the existence of the information is hidden.
- Water marking
- Hard drive / File system manipulation
- Manipulating HTTP requests by changing order of element.
- Encryption

Steganalysis :-

art of detecting and decoding hidden data.

Methods are :-

- Human observation
- Software analysis
- Statistical analysis
- Frequency scanning

DATE: / /
PAGE:

Cyber space :-

Environment that involves interaction between people, software and services. For example computer, networks, storage devices, emails, phones, atm machine. Its also a virtual medium based on bits and bytes.

Cyber security :-

It denotes the technologies and procedure to safeguard resources from unlawful admittance through the internet.

ISO 27001 (international cyber security standard for managing IS management system

Cyber security policy :-

- An authority framework that defines and guard the activities associated with the security of cyber space.
- provide an outline to effectively protect information, information system and networks.
- manages the entire field of ICT users and providers.

DATE : __/__/____
PAGE : _____

Cyber crime :-

Computer crime normally refers to a criminal activity where computer or network is used as a target or as a tools.

Computer as a tool

when individual is main target.
(cyber stalking, cyber theft)

Computer as a target

web defacement, cyber terrorism

Category of cyber crimes

- Cyber crime against a person
- Cyber crimes against property
- Cyber crime against government / firm
- Cyber crime against society

Kinds of Cyber crimes :-

- Unathorized access / hacking
- Virus, Worm & Trojan Attack
- Cyber stalking
- Email related crimes
- Internet Relay chat relating crimes
- Sale of illegal article
- Online gambling
- phishing
- IPR crime
- web defacement

DATE : __/__/____
PAGE : _____

Cyber Laws :-

The I.T Act 2000 defines the terms

- access in computer network in section 2(a)
- computer section 2(i)
- computer network in section (2,j)
- data in section 2(o)
- information in section 2(v)

PAGE :

THE OSI Model

Established in 1947, ISO is a multinational body dedicated to cover all aspects of network communication.

ISO is organization
OSI is a model

Application
presentation
session
transfer layer
Network layer
data link layer
Physical layer

Pysical layer :-

- transmit raw bit stream over physical medium
- Establishing physical connection between devices.

Data link layer :-

Node to node delivery of message.
Define format of data on network.

Network layer :-

- Determine best route for the packets (Data) to travel.
- converts logical address into physical address.

Transport layer
Delivers message from process to process and provides error checking so that no error occurs during transfer of data. error recovery.

session layer
Used to establish manage and terminate the sessions.

Presentation layer:-
responsible for translation compression encryption.

Application:-
provide service to the user.

TCP/IP
compatible with all os and used by private computer for networking.
Remote login

	SMTP FTP HTTP	
Application	process	Specific address
Transport	TCP UDP	port address
	ARP RARP	
Network	IP and other protocols	Logical Address
Data link + physical	underlying physical network	physical address

Good Write

Physical / Mac address - used to identify hops and
Logical or IP address - identify src & dest
port :- label assigned to a process is called endpoints.
specific :- user friendly address that are
designed for specific address.
- Defines the recipient of an email
- use to find a document on the
network.

port address is 16 bits address represented as one single number.

position of IP in TCP/IP protocol suite.

Datagrams

Packets in the network layer are called datagrams.

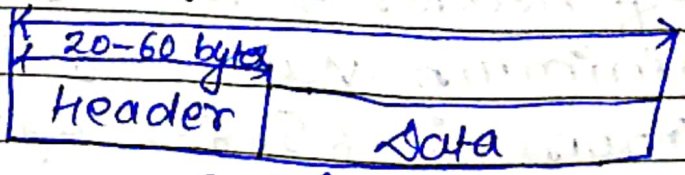
It is variable length packet consisting of two parts

header and data

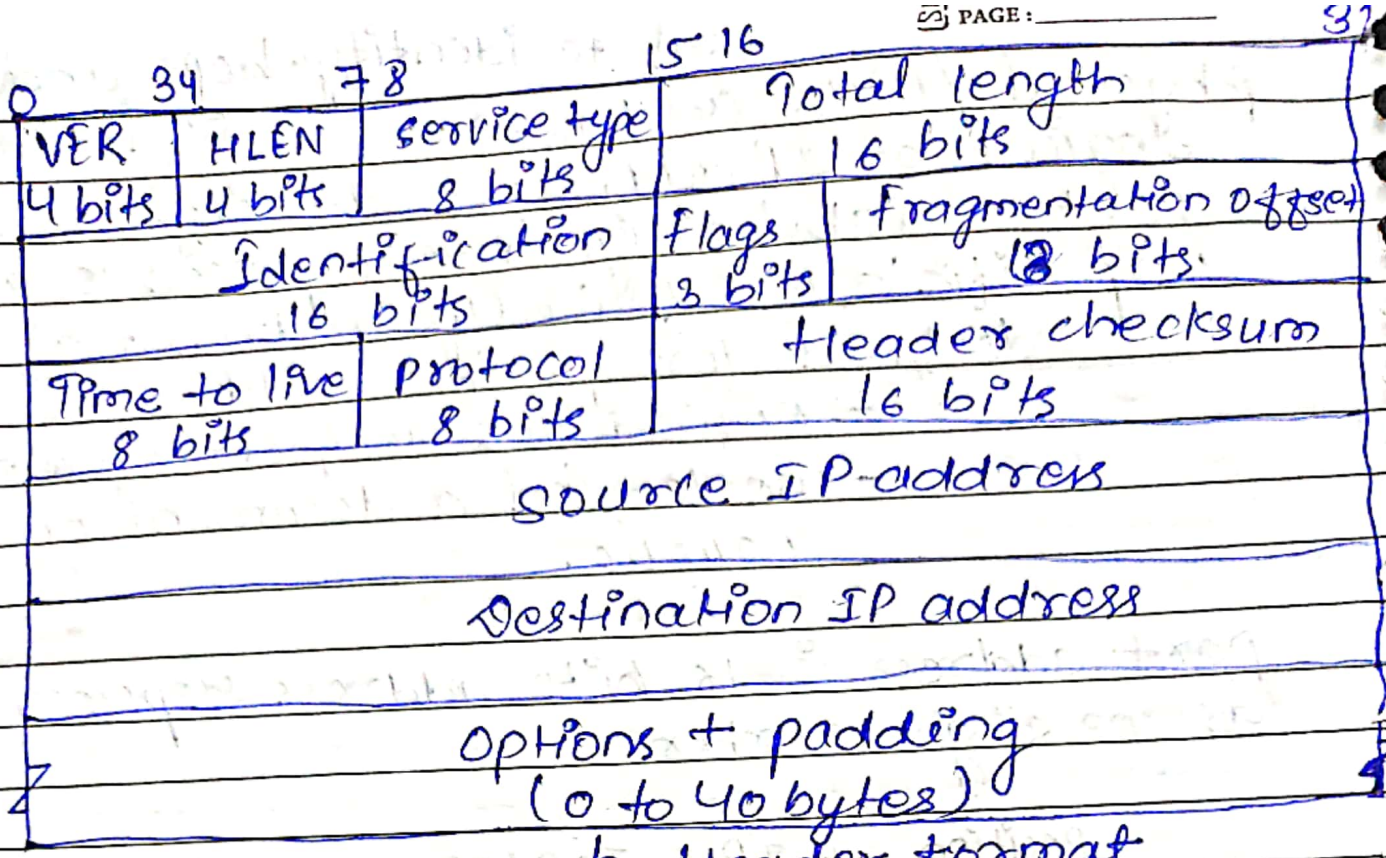
Header is 20 to 60 bytes in length and contains information essential to routing & delivery.

show header in 4 byte section.

IP datagram



a. IP datagram



b. Header format

version (VER) :-
Version of IP protocol (4 bits)

HLEN :- stores IP header length information

Type of service :-
Low Delay
High throughput
Reliability
provide network service parameters

Total length :-
Length of header + Data (16 bits)
which has a minimum value of 20 bytes and the maximum is 65,535 bytes.

Identification :-
Unique packet Id for identifying the group of fragments of a single IP datagram.

Flags :- 3 flags of 1 bit each
reversed bit (must be zero)
do not fragment flag
more fragments flag.

Fragmentation offset :-
Fragment identification via offset value.

Time to live :-
contains the total number of routers allowing packet pass through.

Protocol
This 8-bit field contains header transport packet information.

Header checksum :- checks and monitors communication errors.

Source address :- stores source IP address

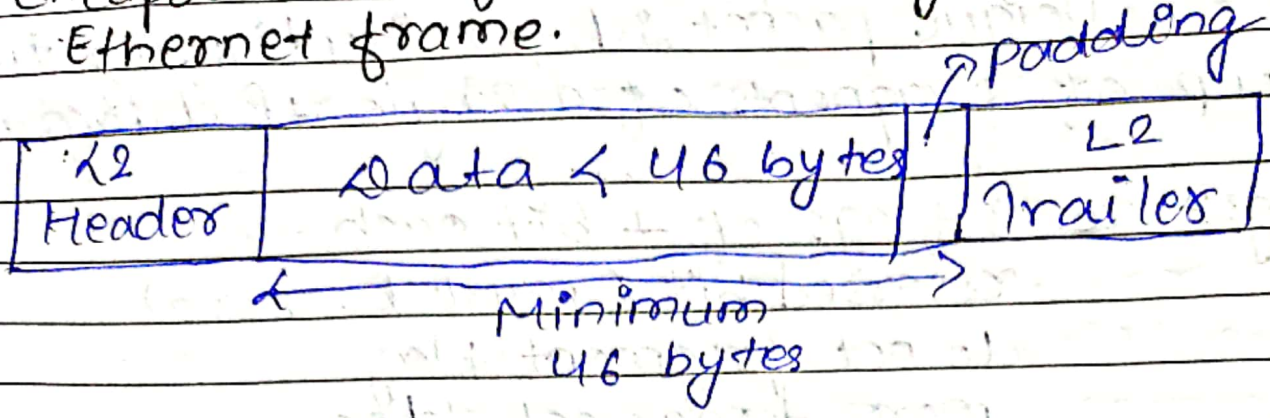
Destination address :-
Stores destination IP address

Options :- Optional info such as router, record route used by Network administrator to check weather path is working or not.

Good Write

DATE: __/__/____
PAGE: _____

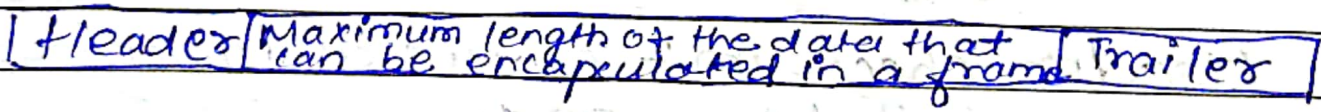
Encapsulation of a small datagram in an Ethernet frame.



Fragmentation

A datagram can travel through different networks. Each router decapsulates the IP datagram from the frame it receives, processes it and then encapsulates it in another frame, whose format and size depends on the protocol used by the physical network through which it travels.

Maximum Transfer Unit



Only data in a datagram is fragmented

Checksum

One of the most reliable method for error detection.

Divide data into equal subunits each of 16 bits length.

These subunits are added togheth using 1st complement method

Scanned with CamScanner

getting sum of n bits. The resultant bit is further complemented. This complemented sum which is called checksum is appended to the end of original data unit and then transmitted.

Same process is perform by checksum checker, if resultant is zero, then the data is error free or it is erroneous.

Sum:-T Sum = T-T = 0
checksum:- -T

checksum in IP covers only the header not the data

Each packet of data consists of 3 parts:-

Header control info at start
Payload:- actual data
Trailer:- control info at end point

Note
Not all ~~packets~~ parts in all packets.

purpose of header:-
Contains information to support protocol operation.
Sender include information in header so the receiver can correctly receive the data and optionally respond.

DATE: __/__/____
PAGE: _____

Although packets are just sequence of bits for convenience headers and header field often drawn row by row

Ethernet

Its a traditional technology for connecting devices in a wired LAN or WLAN which enable devices to communicate with each other via a protocol.

Ethernet cable is the medium over which the data travels.

Advantage

I) relatively low cost
II) backward compaciblity
III) Reliability
IV) good data transfer quality.

Disadvantage

I) limited mobility
II) use of longer cables can create crosstalk.

Ethernet	wifi
• transmits data over a cable	tranmits data through wireless signals rather than over a cable.
• limited mobility	better mobility
• more speed	not as fast as ethernet.
consistent speed	more convenient
No data encryption	require data encryption

Good Write

DATE: __/__/____
PAGE: _____

Ethernet frame format

Basic frame format which is required for all MAC implementation is defined in IEE 802.3 standards.

PREMBLE	SFD	DESTINATION ADDRESS	Source Address	Length	Data	CRC
7 byte	1 Byte	6 Byte	6 Bytes	0 Bytes	46-1500 byte	4 bytes.

1) 7 byte starting bits stream of 0's & 1's to indicate the receiver that frame is coming and allow the receiver to lock onto the data stream before the actual frame

2. SFD ⇒ start of frame delimiter warns stations that this is the last chance for synchronization.

3. Destination :- 6 bytes, contain MAC address of destination machi

4. Source :- 6 bytes, contain MAC address of source machine.

5. Length :- indicates length of ethernet frame.

6. Data :- place where actual data is inserted.

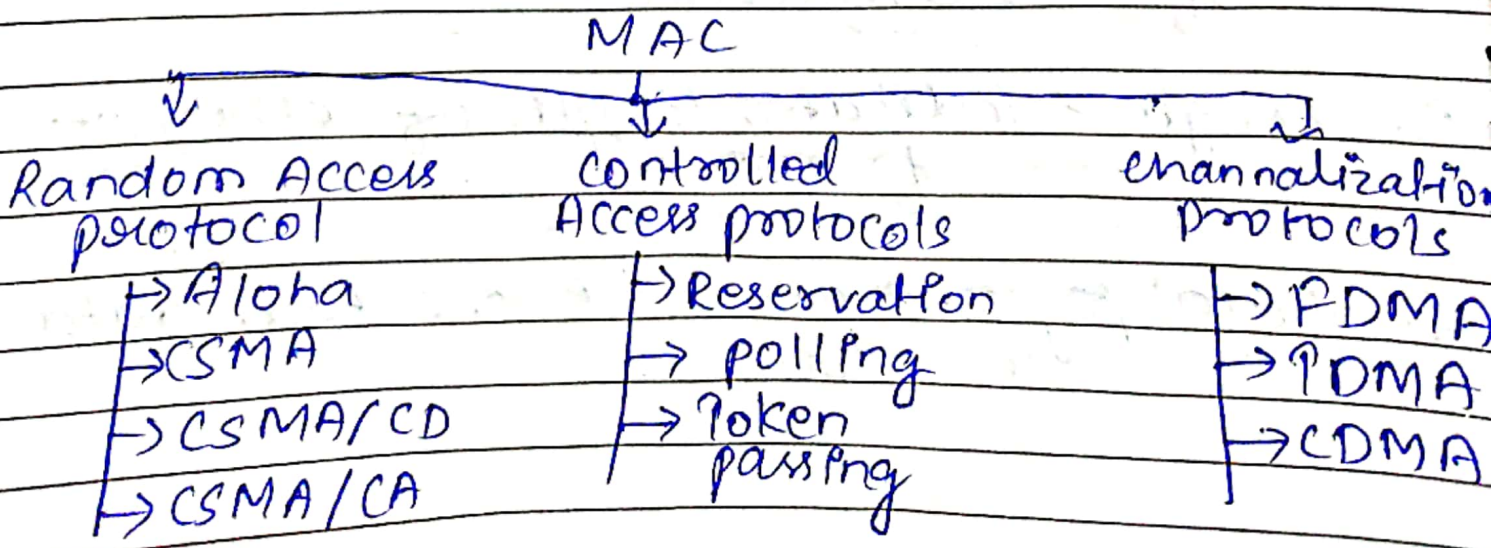
7. Cyclic Redundency check :- 4 byte field for error detection.

Multiple Access control

Data link layer is responsible for transmission of data between two nodes.

transmission of data by using techiques called
framing
error control
and flow control

If dedicated link is given between src and dest, then data link control layer is sufficient, however if there is no such link then Multiple Access control comes into action to decrease collission and avoid cross talk.



DATE: __/__/____
PAGE: _____

Aloha

Pure Aloha

a station sends data, if it not get acknowledgement ~~with~~ in alloted time, then it wait for random amount of time and resend the data.

Vunerable time = 2 * frame transmission time

Throughput = $G e^{-2G}$

Maxi throughput = 0.1841 for $G = 0.5$

Slotted aloha

similar to pure aloha, except that we divide time into slots and sending of data is only allowed at the beginning of these slots.

Vulnerable time = frame transmission time

Throughput = $G \exp^{-G}$

Maxi throughput = 0.368 for $G = 1$

b) CSMA, first sense the medium before transmitting data.

CSMA models are :-

- 1-persistent :- continuously keeps on checking the medium for being idle and then transmit data.

- Non-persistent :- It checks medium after the random amount of time.

Good Write

DATE : __/__/____
PAGE : _____

P- persistent :- node sends the medium for being idle and then sends data with p probability.

O- persistent :-
Superiority of nodes is decided beforehand and transmission occurs in that order.

c) CSMA/CD
Stations can terminate transmission of data if collision is detected.

d) CSMA/CA
CSMA/CA is used in wireless LAN.

collission can be avoid by
- Interframe spacing
- Contention windole
- Acknowledgement.

controlled access
Access is given to certain for transm

i) Reservation :- Just like train reservation
ii) ~~clarification~~
ii) polling :- Its like roll calling
iii) Tokenization :- routers are in ring and one having token can send data.

3. Channelization:-
available bandwidth of the link is shared in time, frequency and code to multiple stations to access channel.
- FDMA
- TDMA
- CDMA

Ethernet addressing
Every interface has unique 48 bits address. that are assigned to vendors by a central authority.

If address doesnot match the hardware address, then frame is discarded.

IP address consists of two components to which the host belongs
i) Network Id ⇒ identifies the network segment
ii) Host Id ⇒ identifies an individual host on specific host on specific network segment

class A 0-127
Default mask 255.000.000.000
Network bits = 8 bits
Host bits = 24 bits
No. of network Id = 2^7
No. of host Id = 2^{24}
reserved for loop back and diagnostic function.

Good Write

DATE:
PAGE:

Class B 128-191

Default mask = 255.255.000.000
Reserved bits = 10
No. of host bits = 16 bits
No. of network bits = 16 bits
No. of address = 2^4
Address per network = 2^{16}
Total address = 2^{30}

helps you to identify the HOt network host.

Class C 192-223

Default mask = 255.255.255.000
Resered bits = 110
Size of network bits = 24 bits
" " host bits = 8 bits
No. of network address = 2^{21}
Address per network = 2^8

•local area network used class C IP address to connect with the network.

Class D :- 224-239

Used for multicasting applicatation
Reserved bits = 1110
Default mask = 255.255.255.255

All the value within the range are used to identify multicast groups uniquely therefore no requirement for extra host address from IP address.

Good Write

PAGE:

Class E Network (240-255)
starting four bits address as 1.
Many network implementations discard these addresses as undefined or illegal.
Used for military purpose.

Mapping of IP address to hardware address.
The process of finding the hardware address of a host given the IP address is called address resolution.

ARP
It is used by sender host when it knowns the IP address of the destination but needs the MAC address.
send
ARP request to every host by broading casting.

After that the right one respond with its mac or Ethernet addrss.

ICMP:- Internet control message protocol
Its used for exchanging control messag

ICMP messages are generally generated and processed by the IP software.

User Datagram Protocol (UDP)

The UDP helps to establish low-latency and loss-tolerating connections establish over the network.

~~ports~~

UDP

- Datagram delivery
- Connectionless
- Unreliable
- Minimal

UDP Datagram format

Source port	Destination port
Length	checksum
Data	

TCP

I) connection-oriented
II) Reliable (transmission of data is acknowledged by the receiver)
III) Full-duplex
IV) Byte-stream

Stream means that the connection is treated as a stream of bytes.

User application doesn't need to package data in individual datagrams.

Buffering

TCP is responsible for buffering. It is possible for an application to tell TCP to send the data it has buffered without waiting for a buffer to

Good Write

DATE: __/__/____
PAGE: _____

TCP segments:-

The chunk of data that TCP asks IP to deliver is called a TCP segment.

Each segment contains:-

- data bytes from the byte stream
- control info that identifies the data bytes.

TCP Segment Format

Source port	Destination port
Sequence Number	
Request Number	
offset | Reser. control	Window
Checksum	Urgent pointer
options (if any)	
Data	