Assignment A7

- Title : Study of wireshark & header format of Ethernet IP, TCP & UDP.

- Problem statement : Write a program to analyze following packet formats captured through wireshark for wired network 1. Ethernet 2. IP 3. TCP 4. UDP

- Objectives :
  1. To learn & understand header format of ethernet, IP, TCP & UDP.
  2. To learn concept of wireshark

- Theory :
  1. Wireshark :
     We use a packet sniffer called wireshark. It is a free packet sniffer/ analyzer which is available for both UNIX & windows os.

     It captures packet from a network interface & displays them with detailed protocol information. It only captures packet without manipulate them, It neither sends packets to the network nor does other active operation.

     Main window :
        Wireshark window is made of 7 sections Title bar, menu bar, filter bar, packet list panel, packet detail panel, packet byte pane & status bar.

Title bar : Like any GUI shows, the title of window, the closing, max & minimizing icons.

Menu bar : Several pulldown menus & tool bars used in most GUI's.

Filter bar : Allows us to display packet we are interested in while hiding the rest.

Packet List Pane : Displays line summary for each captured packet. Summary includes packet, number, time, source

Packet Details Pane : It shows detailed analysis for each frame. The info is limited for one frame

Packet Byte Pane : It shows entire current frame in hexdump format & As CII format no. in left field shows effect in packet data. Hexdump of packet is shown in middle field.

Status Bar : It shows current protocol, total number of packets captured & so on.

• IP protocol Header format
    IP being a layer -3 protocol (OSI) takes data segment from layer 4 (transport) & divides it into packet IP packet encapsulator data unit recieved from above layers and add to its own header information

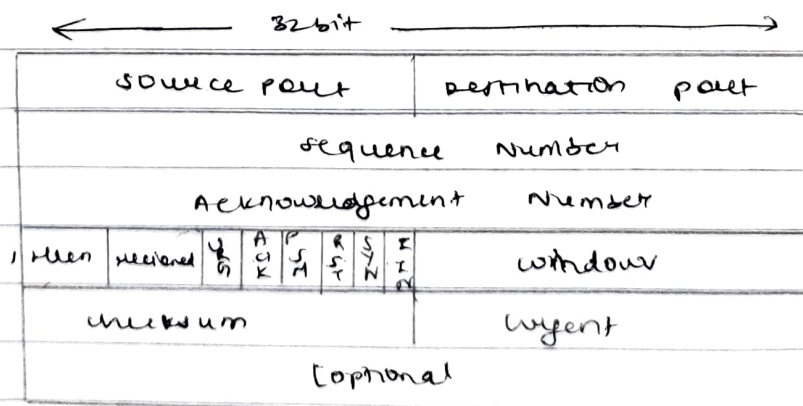| IP header	Layer -4 data
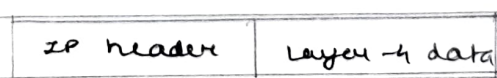
IP encapsulation.

IP header includes many relevant info, including version number, while in the context, is 4

i) Version : version no. of Internet Protocol (IP) used (eg. IPv4)

ii) IHL : Internet Header Length, length of entire IP header

iii) DSCP : Differentiated Services Code Point : this is type of service

iv) ECN : Explicit Congestion Notification info about congestion in route

v) Total length : length of entire IP packet.

vi) Identification : If IP packet is fragmented during the transmission, all fragments contain same identification no. to identify original IP packet they belong to.

vii) Flags : As required by network resources, these flags tells if packets can be fragmented or not if are too large

viii) Fragment offset : Tells exact position of packet of fragment in IP

ix) Time to live : At each hop, value is decremented by one.

x) Protocol : Tells about protocol to which packet belongs

xi) Header checksum : used to check if packet recieved error free

xii) Source address : 32 bit address of sender.

xiii) Destination Address : 32 bit address of reciever

TCP Header format :

←——— 32 bit ———→

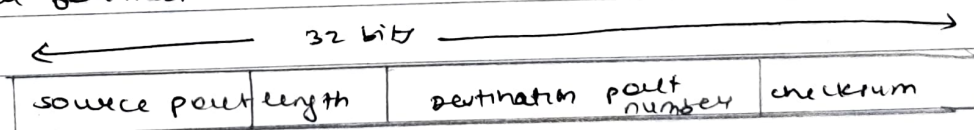| Source Port						Destination Port	
Sequence Number							
Acknowledgement Number							
Hlen	reserved	U R G	A C K	P S H	R S T	S Y N	F I N	Window
Checksum						Urgent	
Optional							

TCP Header format

Each TCP Header has 10 required fields totally 20 bytes (160 bits) in size. They can also optionally include one additional data section upto 40 bytes in size.

Layout of TCP headers.

i) Source TCP Port Number (2 byte)

ii) Destination TCP Port Number (2 bytes)

iii) Sequence number (4 bytes)

iv) Acknowledgement Number (4 bytes)

v) TCP data effort (4 bits)

vi) Reserved data (3 bits)

vii) Control flags (0-9 bytes)

viii) Window size (2 bytes)

ix) TCP checksum (2 bytes)

x) Urgent pointer (2 bytes)

xi) TCP optional data (0-40 bytes)

TCP inserts header fields into message stream

UDP Header format

$\longleftarrow$ 32 bit $\longrightarrow$

Source port	length	Destination port number	checksum

UDP Header format

A UDP header contains 8 bytes, divided into follows 4 field

i.) Source port number (2 byte)   ii.) Destination port no. (2 bytes)

iii.) Length of data (2 bytes)   iv.) UDP checksum (2 bytes)

- conclusion :

we studied and implemented program to analyze following packet format captured through wireshark
1. Ethernet   2. IP   3. TCP   4. UDP.