Page No.
Date

Assignment - 07

* 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 operations.

Main Window:
Wireshark window is made of 4 sections. Title bar, menu bar, filter bar, packet list panel, packet detail pane, packet byte pane & status bar.

Teacher's Sign.: _____

Page No.
Date

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

Menu bars: 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 one 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 hex-dump format & ASCII format. No. in left field shows offset 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 encapsulates data unit received from above layer & add to its own header information.

IP Header	Layer-4 Data

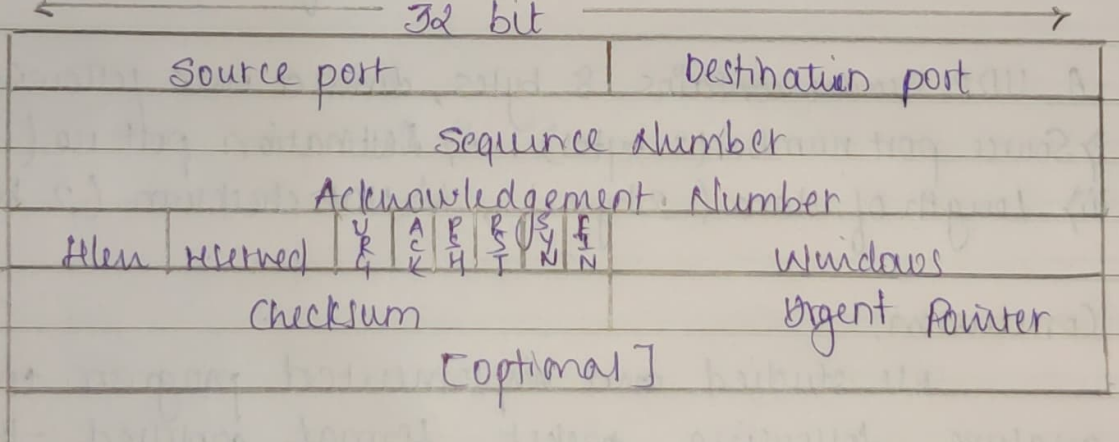
IP Encapsulation

Teacher's Sign.

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

i) Version: version no of Internet protocol 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 received error free
xii) Source address: 32 bit address of sender.
xiii) Destination Address: 32 bit address of receiver

TCP header format:



TCP header format

Teacher's Sign.:

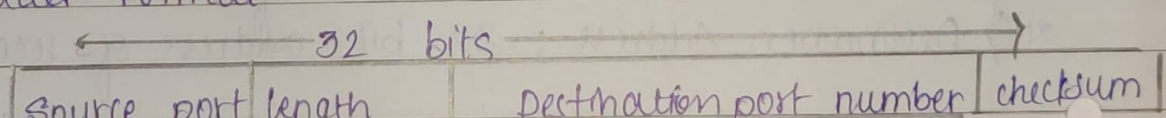
Each TCP header has 10 required fields totalling 20 bytes (160 bits) in size. They can also optionally include one additional data section upto 40 bytes in size

Layout of TCP headers

i) Source TCP Port Number (2 bytes)
ii) Destination TCP port Number (2 bytes)
iii) Sequence Number (4 bytes)
iv) Acknowledgement Number (4 bytes)
v) TCP data offset (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



UDP Header format

A UDP header contains 8 bytes, divided into following 4 fields:
i) Source port number (2 bytes), 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.

Teacher's Sign.: _____