31201

BRUNO | Page No.
Date / /

Assignment A-7

Title → Write a program in C/C++ to analyze following packet formats captured through wireshark for wired network.
1) FTP 2) IP 3) TCP 4) UDP.

Objective →
Analyze of Ethernet, TCP, UDP and IP Packet Format.

Outcome →
Demonstrate the various fields in header structure of TCP/UDP and ethernet packets.

S/w & H/w req: PC, keyboard, mouse, wireshark, Packet Analyzer

Theory

1) A packet analyzer is a computer program or computer hardware such as Packet capture application that can interrupt & log traffic that passes over a computer network or parts of network. It is a process of interception and logging the file as data stream flow across network.

The software captures each packet & if needed decodes the packets raw data having the values of various field in packet and analyzis its content

① Header Format.

Field length (in bytes)

8	6	6	2	76-1500	4
Preamble	Dest addr	src-addr	type	Data	FCS

② IP Header Format

Version	length	types & Service	Total length
Identification			Flags / Flag offsets
Time to live	Protocol		Header Checksum
src_address			
Dest_address			
options			
Data			

③ TCP Header Format

Source Port	Destination Port
Sequence Number	
Acknowledgement Number	
Data offset / Received Code	Window
CheckSum	urgent pointer / padding
Options	
Data	

④ UDP is significantly more limited in compatibility than TCP, its headers are much smaller.

A UDP header contains 8 bytes divided into 4 fields

- Source Port number (2 bytes)
- Destination Port number (2 bytes)
- length of data (2 bytes)
- UDP checksum (2 bytes)

Conclusion

We were able to demonstrate various fields in header structure / format & also analyze the packet captured through wireshark for wired network