# Assignment - VII

**Problem statement :-**

Write a C/C++ program to analyze following packet format captured through wireshark for wired network.

1) FTP 2) IP 3) TCP 4) UDP

**Objective :-** To understand packet format captured through wireshark for wired network.

**Outcome :-** students will be able to understand captured packet format through wireshark.

**S/W & H/W :-** C/C++ compiler, wireshark, monitor, keyboard.

**Theory :-**

Packet Sniffer

A packet sniffer is a computer program or a piece of computer hardware that can intercept & log traffic passing over a digital network or part of network. A data streams flow across the network the sniffer captures each packet & if required decodes packet's raw data,

showing the values of various fields in the packet & analyze its content A packet sniffer a wire-tap device that plays into computer network & eavesdrops on the network traffic.

FTP:-

File Transfer Protocol is standard network protocol used for the transfer of computer files between a client & server on a computer network.

FTP is built on a client-server model architecture using separate control & data connections between client & server.

IP:-

Internet protocol (IP) is principal communication protocol in internet protocol suite for relaying datagrams across network boundaries. IP has task to deliver packets from source to destination solely based on IP addresses in the packet headers. IP defines packets structures that encapsulate the data to be delivered It also defines addressing methods that are used to label the diagram with source & destination information

GoodLuck | Page No.
Date

TCP :-
TCP segments are sent as internet datagrams. The internet protocol header carries several information fields, including the source & destination host addresses. A TCP header follows the internet header, supplying information specific to TCP. This allows for the existence for the host level protocol other than TCP.

UDP :-
UDP is a connectionless & unreliable transport protocol. The two ports serve to identify the end points within the source & destination machines. User Datagram Protocol is used, in place of TCP, when reliable delivery is not required. However UDP is never used to send important data such as web pages, database information, streaming data / media such as video, audio & others use UDP because it offers speed.

Algorithm :-

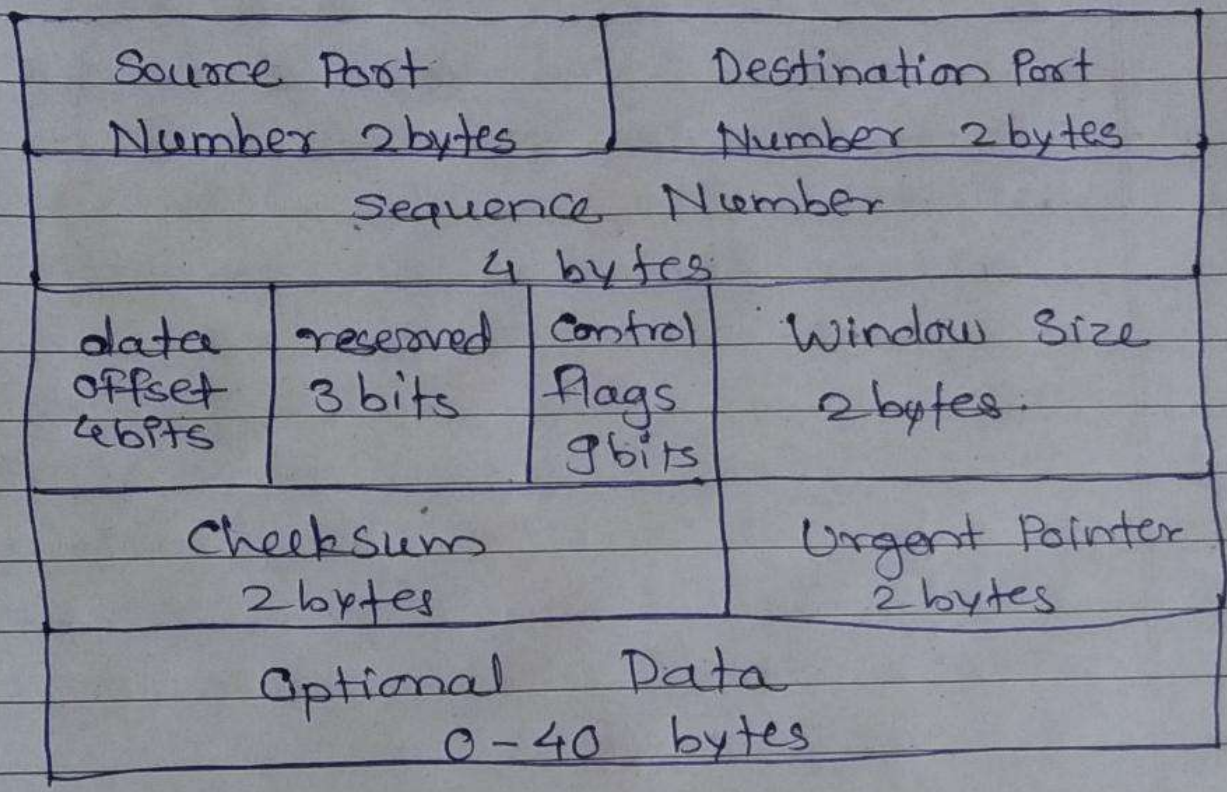
1] Start wireshark.
2] Start capturing packets.
3] Stop capturing packets
4] Export as csv file.
5] Open the csv file in cpp program
6] Ask "which protocol packets"
7] Display the count.
8] Exit.

Test cases :-

| I/P | Expected O/P | Actual O/P | Result |
|---|---|---|---|
| FTP | count: 4 | Count: 4 | Success |
| TCP | count: 17 | count: 17 | Success |
| IP | Count: 7 | Count: 7 | Success |
| UDP | Count: 979 | Count: 979 | Success |

GoodLuck | Page No.
Date

# TCP header




Conclusion:-

We learnt how to analyze packet format using wireshark.