# Assignment - 7

**Title** - Packet Analysis for wired network.

**Objective** - To demonstrate data flow at various layers.

**Problem Statements** -

Write a program to analyze following packet formats captured through Wireshark for wired network.

1. Ethernet 2. IP 3. TCP 4. UDP

**Outcome** -

Student will be able to demonstrate data flow from top-to-down and down-to-up for various protocol stacks at various layers and propose protocol model / frame work for future network requirements.

**Tools Required** -

1. Transport layer : Roles, Protocols (TCP, UDP)
2. Network layer : Roles, Protocols (IP)
3. C/C++ Programming Syntax
4. Wireshark Tool.

• Theory -

Packet sniffer / Packet Analyzer -

A packet analyzer (also known as a network analyzer, protocol analyzer or packet sniffer) is a computer program or a piece of computer that can intercept and log traffic passing over a digital network or part of a network. As data streams own across the network, the sniffer captures each packet and, if needed, decodes the packet's raw data, showing the values of various fields in the packet, and analyzes its content according to the appropriate RFC or other specifications.

→ Different Types of Packets -

1. TCP :

- The Transmission Control Protocol (TCP) is one of the core protocols of the Internet Protocol suite (IP), an is so common that the entire suite is often called TCP/IP.
- TCP provides reliable, ordered and error-checked delivery (or notification of failure to deliver) of a stream of octets between programs running on computers connected to a local area network, intranet or public Internet.
- It resides at the transport layer.
- TCP provides a communication service at an intermediate level between an application

program and the Internet Protocol (IP).

2. UDP :

- The User Datagram Protocol (UDP) is one of the core members of the Internet Protocol Suite.
- UDP uses a simple connectionless transmission model with a minimum of protocol mechanism.
- It has no handshaking dialouges and thus exposes any unreliability of the underlying network protocol to the user's program. There is no guarantee of delivery, ordering or duplicate protection.
- UDP is suitable for purposes where error checking and correction is either not necessary or is performed in the application, avoiding the overhead of such processing at the network interface level.
- Time-sensitive applications often use UDP because dropping packets is preferable to waiting for delayed packets, which may not be an option in a real-time systems.

3. ICMP :

- The Internet Control Message Protocol is one of the main protocols of the Internet Protocol Suite.
- It is used by network devices, like routers, to send error messages indicating that a required service is not available or that a host or

router could not be reached.

- IGMP differs from transport protocols such as TCP and UDP in that, it is not typically used to exchange data b/w systems, nor is it regularly employed by end-user network applications.
- ICMP messages are typically used for diagnostics or control purposes or generated in response to errors in IP operations.

4. IGMP :

- The Internet Group Management Protocol (IGMP) is a communications protocols used by hosts and adjacent routers on IP networks to establish multicast group memberships.
- IGMP can be used for one-to-many networking applications such as online streaming video and gaming, and allows more efficient use of resources when supporting these types of applications.
- IGMP messages are carried in bare IP packets with IP protocol.
- There is no transport layer used with IGMP messaging, similar to the Internet Control Message Protocol.

- <u>Conclusions</u> -

Hence, we implemented analyzed packet formats of Ethernet, IP, UDP/TCP captured through Wireshark.