TASK-5

1. What is Wireshark used for?

→ Wireshark is a free and open-source network protocol analyzer used to capture, inspect, and analyze network packets in real time.
It helps in troubleshooting network issues, monitoring traffic, and detecting security problems.

2. What is a packet?

→ A packet is a small unit of data transmitted over a network.
It contains **header information** (like source and destination IP) and a **payload** (actual data being sent).

3. How to filter packets in Wireshark?

→ You can filter packets using **display filters** in the filter bar at the top of Wireshark.
For example:

- http → shows only HTTP packets
- dns → shows DNS queries and responses
- tcp → shows only TCP packets
- icmp → shows ping packets

4. What is the difference between TCP and UDP?

→ TCP (Transmission Control Protocol) is a **connection-oriented** protocol, which means it establishes a reliable connection between sender and receiver before transmitting data. It ensures that all packets are delivered in order, checks for errors, and retransmits lost packets. Because of this reliability, TCP is used in applications like web browsing (HTTP/HTTPS), email, and file transfer (FTP).

UDP (User Datagram Protocol), on the other hand, is **connectionless** and does not guarantee delivery, order, or error correction. It simply sends packets called datagrams without establishing a connection. This makes it faster but less reliable than TCP. UDP is mainly used in applications that require speed and can tolerate some data loss, such as video streaming, online gaming, and DNS lookups.

5. What is a DNS query packet?

→ A DNS query packet is a request sent by a client to a DNS server asking to resolve a domain name into its IP address.
Example: When you type www.google.com, your computer sends a DNS query to get the IP of Google’s server.

6. How can packet capture help in troubleshooting?

→ Packet capture helps in identifying:

- Network delays or dropped packets
- Misconfigured devices or ports
- Unauthorized access or suspicious traffic
- Application-level issues
  It provides a detailed view of what's happening on the network in real time.

7. What is a protocol?

→ A protocol is a set of rules and conventions that define how data is transmitted and received over a network.
Examples include **TCP**, **UDP**, **HTTP**, **DNS**, and **ICMP**.

8. Can Wireshark decrypt encrypted traffic?

→ Wireshark **cannot decrypt encrypted traffic** (like HTTPS or SSL/TLS) unless you provide the proper **encryption keys or SSL certificates**.
Without keys, it can only show encrypted data but not the actual content.