**TASK 5**

**INTERVIEW QUESTION**

**1. What is Wireshark used for?**

Wireshark is a network protocol analyzer used to capture and inspect data packets traveling through a network.  
It helps in network troubleshooting, performance analysis, security monitoring, and protocol development by showing detailed information about each packet.

**2. What is a packet?**

A packet is the smallest unit of data transmitted over a network.  
It contains two parts:

* Header – includes source and destination addresses, protocol type, etc.
* Payload – the actual data being sent.  
  Packets are sent and reassembled at the destination to complete communication.

**3. How to filter packets in Wireshark?**

You can filter packets using the Display Filter Bar in Wireshark.  
Example filters:

* http → show only HTTP packets
* dns → show DNS packets
* tcp.port == 80 → show packets using TCP port 80
* ip.addr == 8.8.8.8 → show packets involving a specific IP address

Filters make analysis faster and more focused.

**4. What is the difference between TCP and UDP?**

|  |  |  |
| --- | --- | --- |
| Feature | TCP (Transmission Control Protocol) | UDP (User Datagram Protocol) |
| Connection | Connection-oriented | Connectionless |
| Reliability | Reliable (acknowledges delivery, retransmits lost packets) | Unreliable (no retransmission) |
| Speed | Slower due to error checking | Faster but less reliable |
| Use Cases | Web browsing (HTTP/HTTPS), email, file transfer | Streaming, gaming, VoIP |

**5. What is a DNS query packet?**

A DNS query packet is a request sent by your computer to a DNS server to resolve a domain name (like google.com) into an IP address.  
In Wireshark, you can identify these packets using the filter dns.  
They usually appear as Standard query (A) or Standard query response (A) packets.

**6. How can packet capture help in troubleshooting?**

Packet capture helps identify:

* Network delays or dropped connections
* Misconfigured devices
* Unauthorized traffic or security threats
* Protocol errors  
  By analyzing captured packets, administrators can pinpoint where communication fails or why performance is poor.

**7. What is a protocol?**

A protocol is a set of rules that defines how data is transmitted and received over a network.  
Examples include:

* HTTP/HTTPS – web communication
* TCP/UDP – transport layer
* DNS – domain name resolution
* ICMP – ping and error reporting

Each protocol ensures devices can understand and exchange data correctly.

**8. Can Wireshark decrypt encrypted traffic?**

Wireshark can decrypt some encrypted traffic only if the decryption keys are available.  
For example:

* It can decrypt SSL/TLS (HTTPS) if you provide the session keys or private key.
* However, it cannot decrypt end-to-end encrypted traffic (like WhatsApp or Signal messages) because those keys are not accessible.