1. What is Wireshark used for?

Wireshark is a network protocol analyzer used to capture, inspect, and analyze data packets traveling over a network. It helps in troubleshooting network issues, monitoring network activity, and learning about network protocols.

2. What is a packet?

A packet is a small unit of data transmitted over a network. It typically contains a header (with control information like source, destination, and protocol) and a payload (the actual data being sent).

3. How to filter packets in Wireshark?

In Wireshark, you can use display filters to show only the packets you need. For example, 'http' shows HTTP traffic, 'tcp' shows TCP packets, and 'ip.addr == 192.168.1.1' shows packets to/from a specific IP address.

4. What is the difference between TCP and UDP?

TCP (Transmission Control Protocol) is connection-oriented, reliable, and ensures data delivery in order. UDP (User Datagram Protocol) is connectionless, faster, but does not guarantee delivery or order of data.

5. What is a DNS query packet?

A DNS query packet is a request sent from a client to a DNS server asking for the IP address corresponding to a domain name.

6. How can packet capture help in troubleshooting?

Packet capture allows network administrators to see exactly what data is being transmitted, identify delays, detect errors, spot security threats, and pinpoint the source of network problems.

7. What is a protocol?

A protocol is a set of rules that defines how data is formatted, transmitted, and processed between devices in a network.

8. Can Wireshark decrypt encrypted traffic?

Yes, Wireshark can decrypt some encrypted traffic (like HTTPS, WPA/WPA2) if the necessary encryption keys or certificates are provided. Without keys, encrypted traffic remains unreadable.