1. What is Wireshark used for?

Wireshark is a powerful network analysis tool used to capture and inspect data packets traveling through a network. It helps monitor network traffic, detect problems, and understand protocol behavior.

2. What is a packet?

A packet is a small unit of data sent across a network. It contains both control information (like source, destination, and type) and the actual data being transmitted between devices.

3. How to filter packets in Wireshark?

You can filter packets in Wireshark using display filters. For example, filters like 'ip.addr == 192.168.1.1' or 'tcp.port == 80' show only relevant packets for easier analysis.

4. What is the difference between TCP and UDP?

TCP is a reliable, connection-oriented protocol that ensures data delivery with acknowledgments and retransmissions. UDP is faster but connectionless, with no guarantee of packet delivery.

5. What is a DNS query packet?

A DNS query packet is a request sent by a client to a DNS server to translate a domain name into its corresponding IP address, enabling access to websites and services.

6. How can packet capture help in troubleshooting?

Packet capture helps diagnose issues like network delays, packet loss, or misconfigurations. By analyzing packets, you can pinpoint where and why communication errors occur.

7. What is a protocol?

A protocol is a standardized set of rules that define how data is formatted, transmitted, and received over a network. Common examples include HTTP, TCP, UDP, and DNS.

8. Can Wireshark decrypt encrypted traffic?

Wireshark can decrypt encrypted traffic if the necessary encryption keys are available. For instance, HTTPS traffic can be decrypted using SSL/TLS session keys for analysis.