Wireshark interview Question & Answers

1. What is Wireshark used for?

Wireshark is a widely-used network protocol analyzer. It lets you capture and interactively browse the traffic running on a computer network. It's used for network troubleshooting, analysis, software and communications protocol development, and education.

2. What is a packet?

A packet is a small segment of a larger message. Data sent over computer networks, like the internet, is broken down into these smaller pieces. Each packet contains a portion of the user data plus control information like the source and destination IP addresses, protocol, and sequencing numbers.

3. How to filter packets in Wireshark?

You can filter packets in Wireshark by typing a filter expression into the "Apply a display filter" bar at the top of the window and pressing Enter. For example, you can filter by protocol (

`tcp`), IP address (`ip.addr == 8.8.8.8`), or port number (`tcp.port == 443`).

4. What is the difference between TCP and UDP?

TCP (Transmission Control Protocol) and **UDP (User Datagram Protocol)** are two core internet protocols. The main difference is reliability.

- **TCP**: Is **connection-oriented** and **reliable**. It establishes a connection before sending data and includes error-checking and packet sequencing to guarantee that all data arrives in the correct order. It's used for web Browse (HTTP/S), email, and file transfers.
- **UDP**: Is **connectionless** and **unreliable**. It sends data without establishing a connection or guaranteeing delivery. It's much faster but packets can be lost or arrive out of order. It's used for time-sensitive applications like video streaming, DNS, and online gaming.

5. What is a DNS query packet?

A DNS query packet is a request sent from a user's computer to a DNS server when the user tries to go to a website. Its purpose is to ask the server for the IP address associated with a specific domain name (e.g., "What is the IP address for www.google.com?").

6. How can packet capture help in troubleshooting?

Packet capture allows network administrators to see exactly what is happening on their network at a low level. It helps in troubleshooting by:

- **Identifying Errors**: Spotting malformed packets or protocol errors.
- **Analyzing Performance**: Diagnosing slow network speeds by identifying latency, packet loss, or unnecessary traffic.
- **Security Analysis**: Detecting suspicious activity like malware communications or unauthorized scans.

7. What is a protocol?

A protocol is a set of established rules that determine how data is transmitted between different devices in a network. It ensures that computers can communicate with each other in an orderly and efficient manner. Examples include TCP, IP, HTTP, and DNS.

8. Can Wireshark decrypt encrypted traffic?

It depends. Wireshark can decrypt encrypted traffic (like TLS/SSL, used in HTTPS)

only if you have the appropriate encryption keys. For example, if you have the server's private key or a pre-master secret key from the client, you can configure Wireshark to use them to decrypt the session. However, without these keys, the traffic will remain unreadable.