1. What is Wireshark used for?

Wireshark is a **network protocol analyzer** used to capture and inspect network traffic in real time. It allows cybersecurity professionals, network administrators, and developers to **analyze packets at a granular level** to troubleshoot connectivity issues, detect anomalies, study protocols, and identify malicious activity or data leaks. Essentially, it provides visibility into what's happening "on the wire."

---

2. What is a packet?

A packet is the **smallest unit of data transmitted over a network**. When large data (like a file or video) is sent, it's broken down into multiple packets, each containing a header (with routing and protocol information) and a payload (the actual data). The packets are reassembled at the destination to reconstruct the original message.

---

3. How to filter packets in Wireshark?

Wireshark offers **display filters** and **capture filters**:

- **Capture filters** (set before starting the capture) limit what traffic is recorded. Example: `tcp port 80` captures only HTTP traffic.

- **Display filters** (applied after capture) refine what's shown in the interface. Example: `ip.addr == 192.168.1.10` shows only packets to or from that IP.
 Filters help focus on relevant traffic and make analysis faster and more efficient.

---

4. What is the difference between TCP and UDP?

- **TCP (Transmission Control Protocol)** is **connection-oriented**, ensuring reliable data transfer with error checking, acknowledgments, and retransmissions. It's used where accuracy matters, like web browsing (HTTP/HTTPS) or email.

- **UDP (User Datagram Protocol)** is **connectionless** and faster, but doesn't guarantee delivery or order. It's used in real-time applications like video streaming, VoIP, and online gaming, where speed is more important than reliability.

---

5. What is a DNS query packet?

A DNS query packet is a **request sent from a client to a DNS server** to resolve a domain name (like `www.example.com`) into an IP address.
It typically includes the query type (e.g., A, AAAA, MX), transaction ID, flags, and the domain name. Wireshark can capture and display these packets to help analyze name resolution issues or detect DNS-based attacks.

---

6. How can packet capture help in troubleshooting?

Packet capture provides **firsthand visibility into network communication**. By analyzing captured traffic, you can:

- Identify **latency issues**, dropped connections, or retransmissions.
- Verify if **requests and responses** are properly exchanged.
- Detect **malicious behavior** like port scanning or unauthorized access.
- Diagnose **application-level issues**, such as misconfigured protocols or DNS failures.
  It's one of the most powerful diagnostic tools for both network and security problems.

---

7. What is a protocol?

A protocol is a **set of standardized rules** that define how data is formatted, transmitted, and received over a network. It ensures devices can communicate effectively.
Examples include **HTTP (web traffic)**, **FTP (file transfer)**, **SMTP (email)**, **TCP/IP (internet communication)**, and **DNS (name resolution)**. Each protocol operates at a specific layer of the OSI model and serves a distinct purpose.

---

8. Can Wireshark decrypt encrypted traffic?

Wireshark **cannot decrypt most encrypted traffic** (like HTTPS, SSL/TLS, or VPN tunnels) unless you provide the necessary **encryption keys** or capture the traffic before encryption occurs.
However, if you have access to **session keys or private keys** (for example, in a lab or debugging scenario), Wireshark can decrypt and analyze the contents. In real-world cases, it's mostly used to inspect **handshake information and metadata** rather than decrypting actual data.