1. What is wireshark used for?
   Ans: Wirehshark is a network packet analyzer which presents captured packets data as much as possible.

2. What is a packet?
   Ans: In networking, a packet is a small segment of larger message. Data sent over computer networks, such as the Internet, is divided into packets, which are then re-combined by the computer or device that receives them.

3. How to filter packets in Wireshark?
   Ans: In wireshark, you can filter packets using the display filter bar at the top of the window. You can enter specific protocols, IP addresses, port numbers, or other criteria to filter the packets displayed. For example, type "http" would display only HTTP packets.

4. What is the difference between TCP and UDP?

Ans: TCP is suitable for applications requiring guaranteed delivery (e.g., file transfers, emails) while UDP is suitable for applications prioritizing speed (e.g., online gaming, video streaming).

5. What is a DNS query packet?
   Ans: A DNS query is a message that client sends to the DNS server. It contains a list of questions that the DNS server answers. A DNS query can contain multiple questions that the server will reply to, but a server might also reply with its own additional information.

6. How can packet capture help in troubleshooting?
   Ans: Packet capture helps in troubleshooting by providing a detailed view of network traffic, allowing administrations to analyze and identify issues such as packet loss, latency, or misconfigures protocols.

7. What is a protocol?
   Ans: In networking, a protocol is a set of rules and standards that governs communication between devices, defining how data is formatted, transmitted, and received.

8. Can Wireshark decrypt encrypted traffic?
   Ans: Wireshark can decrypt certain types of encrypted traffic if the encryption keys are available. For example, it can decrypt SSL/TLS traffic if you have the private key or session keys, but it cannot break strong encryption without keys.