1. **What is Wireshark used for?**
   It's a "packet sniffer" or network protocol analyzer. It's used to capture and look at the network traffic going in and out of a computer, which is essential for troubleshooting network problems and for security analysis.

2. **What is a packet?**
   A packet is a small piece of data sent over a network. Think of it like a digital envelope that has a "to" address (destination IP), a "from" address (source IP), and the actual message or data inside.

3. **How to filter packets in Wireshark?**
   You use the **"Apply a display filter"** bar at the top of the window. You can type in the name of a protocol (like dns, http, or tcp) and press Enter to see only the packets that match that protocol.

4. **What is the difference between TCP and UDP?**

   - **TCP** is like a **phone call**. It's reliable—it establishes a connection first and makes sure all the data arrives in the correct order. It's used for web browsing and emails.

   - **UDP** is like sending a **postcard**. It's faster but unreliable—it just sends the data without checking if it all arrived. It's used for video streaming or online gaming where speed is more important than perfect accuracy.

5. **What is a DNS query packet?**
   It's a packet your computer sends to a DNS server that essentially asks a question, like: "What is the IP address for www.google.com?"

6. **How can packet capture help in troubleshooting?**
   It lets you see exactly what's happening on the network. If a website isn't loading, you can use Wireshark to see if your computer is even sending out a request, or if the server is responding, or if there are errors in the communication. It provides definitive proof of where the problem is.

7. **What is a protocol?**
   A protocol is a set of rules that computers use to communicate with each other. Just like humans use languages to understand one another, computers use protocols like TCP, IP, and HTTP to manage their conversations.

8. **Can Wireshark decrypt encrypted traffic?**
   No, not by itself. If traffic is encrypted with protocols like HTTPS (TLS/SSL),

Wireshark will just show it as scrambled, unreadable data. The only way to decrypt it is if you have access to the private decryption keys, which you normally would not.