1. What is the duration of the capture file in seconds? What about the start and end time of the capture expressed in hh:mm:ss?

   start: 12:12:54

   end: 12:13:06

   duration: 12 seconds

2. How many protocols do you see in the protocol window? List the names of some of these protocols. You can find information about the protocols from the “protocol” field. You can sort on this field or any other field in the review window. You can also add or delete fields from the list.

   DNS, QUIC, TCP, TLSv1.2, TLSv1.3

   5 protocols

3. How many IPv4 conversations do you have in your capture? You can get these if you investigate Statistics -> Conversations.

   28

4. What is the IP address of the DNS server you are connecting to? To minimize the search time, you should search for a specific string, in this case “google” since we ended up typing www.google.com in the web browser and it is what the system needs to resolve with DNS to get to the appropriate IP address of the Google server servicing your search request. To find a string within a packet, click on Edit > Find Packet. Under "Find By:" select "string" and enter your search string in the text entry box.

   10.17.21.2

5. What is the IP address of the Google server? Once you locate DNS query within all captured packets, you will be able to easily find this address as well.

   142.251.40.196

6. Type udp.port in Apply a Display Filter ... <Ctrl-/>? field and click Enter. List the protocols in the “Protocol” field that you see.

   QUIC

7. What is the Checksum field in the UDP header used for and can it be used for reliable data delivery?

   It is used for error detection. .It verifies if the UDP packet was altered during the transmission.

   It cannot be used for reliable data delivery because 1.UDP does not retransmit packets and simply drop the error one. 2. There is no ACK field. 3. in IPv4 the checksum is optional.

8. What is the TOS field in the IP header used for and can it be used for reliable data delivery?

   The TOS field indicates how packets should be handled to achieve packet prioritization and quality of service. It does not ensure reliable data delivery because IP is an unreliable, best-effort protocol. reliability needs to be achieved by the upper layer.

9. What is the Sequence Number field in the TCP header used for?

   It tracks data order, handles lost or duplicate packets, and ensure reliable transmission together with ACK numbers.

10. What is the timestamp field in the PDU header used for?

    It is used for tracking the time a packet was sent or received. (tracking round trip time, latency, and maintaining packet ordering).

11. Elaborate how the router uses TCP acknowledgment for reliable packet delivery?

    Routers prioritizes and forwards TCP ACKs so that ACK packets are forwarded efficiently. If the router detects congestion, it uses active queue management techniques like Random Early Detection to drop packets early, and it also prompts TCP to reduce transmission speed. Some advanced routers can reorder out-of-order packets to improve efficiency.