**TASK 2**

**QUIC PACKET TRACING :**

**QUESTION 1 :**

What is the name of website?

**ANSWER 1 :**

The website is www.cloudflare.com.

**QUESTION 2 :**

Find the packet that contains the Initial QUIC handshake. What information is exchanged here?

**ANSWER 2 :**

Packet 70 is an Initial QUIC packet. It carries the TLS 1.3 ClientHello, which exchanges supported QUIC versions, cipher suites,

**QUESTION 3:**

Identify the QUIC packet that contains the TLS ClientHello.

**ANSWER 3 :**

The TLS ClientHello is contained inside the Initial QUIC packet (e.g., Packet 70). Wireshark shows this under the QUIC and then the CRYPTO frame as “TLSv1.3 Record Layer: Handshake Protocol: Client Hello (fragment).”

**QUESTION 4 :**

Which QUIC version is used in your trace?

**ANSWER 4 :**

The QUIC version in the Initial packet is QUIC v1 (0x00000001).

**QUESTION 5 :**

Locate the packet where 0-RTT or 1-RTT keys are first used.

**ANSWER 5 :**

The first packet labeled as “0-Rs.TT Protected” is packet no **(72)**  and the first packet labeled as 1-Rs-TT is packet n**o (101)**

**QUESTION 6 :**

Find the first packet that carries application data (HTTP/3). How does this differ from HTTP over TCP?

**ANSWER 6 :**

Packet 101, labeled as Protected Payload, is also the first application data packet. It carries HTTP/3 traffic encrypted inside QUIC. HTTP/3 differs from HTTP over TCP because it runs on QUIC (UDP), integrates TLS into the transport layer, and avoids TCP’s head-of-line blocking, allowing faster and more efficient communication.