

**Computer Network**

**Task No 03**

Submitted by: **Umair Tariq**

Registration No: **B23F0662AI103**

Submitted to:**Dr. Adnan Iqbal**

Date:**22-09-2025**

https://lh7-rt.googleusercontent.com/docsz/AD_4nXdVQ8OUBR_dhCrOWV1vxlqoLBzyJs70xCYbzvgAIFmfaWpFIdo2pXDaYOKmtp_vrwUYfft8dgX6ZR4ULRPnkssCqn40PP5czpDoNF8Wv8rX95d9oFefvexKWheM6s0jgWZ-dZ4C1u_sld56EN9HgaXiiTc?key=Wa7SeqjkZKC1QT8VhWH50Q **Assignment N0 01**

**Task NO 03:**

**For Quic:**

For the QUIC based website access, answer the following:

1-What is the name of website?

**Solution:**

**Name of website:**

The name of the website is tazeen.com.

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

**Solution:**

The Initial QUIC handshake typically occurs in the first few packets of the connection. In this handshake:

* Connection IDs are exchanged to identify the connection.
* QUIC version information is shared to ensure compatibility.
* Initial cryptographic parameters are established to secure the connection.

3. Identify the QUIC packet that contains the TLS ClientHello (QUIC embeds TLS handshake inside QUIC).

**Solution:**

The TLS ClientHello message is embedded within the Initial QUIC packets. These packets are used to initiate the TLS handshake over QUIC, allowing for secure communication.

4. Which QUIC version is used in your trace?

**Solution:**

The specific QUIC version used would typically be identified in the Initial packets or during the version negotiation process. Without access to the exact packet details, it's challenging to specify the version used.

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

**Solution:**

The 0-RTT or 1-RTT keys are used after the initial handshake is completed and the cryptographic keys are established. These packets would be marked as using 0-RTT or 1-RTT keys, indicating encrypted communication.

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

**Solution:**

The first packet carrying application data (HTTP/3) would typically be after the handshake is completed and the connection is secured. HTTP/3 over QUIC differs from HTTP over TCP in several ways:

**1-Transport Layer:**

QUIC uses UDP, while traditional HTTP uses TCP.

**2-Performance:**

QUIC provides faster connection establishment and better multiplexing capabilities, reducing head-of-line blocking.

**3-Security:**

QUIC integrates TLS 1.3, providing similar security benefits as HTTP over TCP with TLS, but with potentially lower latency.

**Conclusion:**

We can concluded that QUIC protocol is used for secure and efficient communication on tazeen.com. It provides faster connection establishment and better multiplexing compared to traditional HTTP over TCP. QUIC integrates TLS 1.3 for secure data transmission.

**Thank You**