

**Assignment : 01**

**Submitted by: Abdullah Aslam**

**Registration no:B23F0754AI129**

**Instructor : Sir Adnan**

**Department: BSAI Red**

**Date: 24th Sep ,2025**

**Group members: Rehab Gul, Umer Khan and Abdullah Aslam**

***Part 03 and 06:***

**Task 05:**

For the HTTPS based website access, answer the following:

**Question :01:**

What is the name of website?

**Answer:**

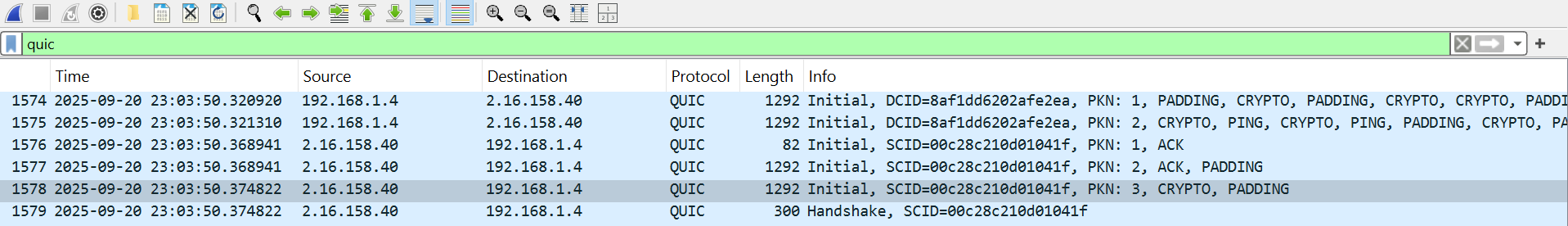
The name of the website is [www.google.com](http://www.google.com)

**Question :02:**

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

**The packets that contain the Initial QUIC handshake are:**

* **Packet 1574** (Client to Server)
* **Packet 1575** (Client to Server)
* **Packet 1576** (Server to Client, ACK)
* **Packet 1577** (Server to Client, ACK + PADDING)
* **Packet 1578** (Server to Client, CRYPTO frame with TLS ServerHello)
* **Packet 1579** (Server to Client, Handshake packet with TLS extensions)

****

**Information exchanged in the Initial handshake:**

* **Connection IDs (CIDs):**

Client uses **Destination Connection ID (DCID):** 8af1dd6202afe2ea (in packets 1574, 1575) to tell the server how to reach it.

Server provides **Source Connection ID (SCID):** 86c28c21e601041f (in packet 1576) for the client to use in future packets.

* **Packet Numbers (PKN):** Used for ordering and reliability (e.g., PKN: 1, 2, 3).
* **CRYPTO Frames:** These contain the actual **TLS handshake messages** (the ClientHello is in the client's CRYPTO frames, and the ServerHello/certificate is in the server's CRYPTO frames).
* **ACK Frames:** For acknowledging received packets (e.g., packet 1576 is an ACK for the client's initial packets).
* **PADDING Frames:** Used to increase the packet size for security and reliability.
* **PING Frames:** To check liveness of the connection.

The Initial handshake establishes the secure connection using TLS 1.3, negotiates encryption keys, and sets up the connection IDs for the rest of the session.

**Question :03:**

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

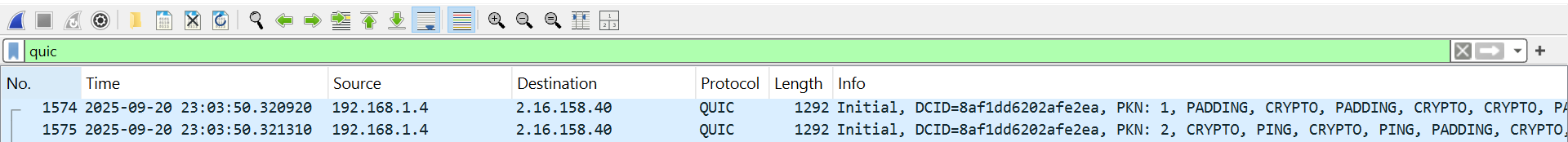
**Answer:**

The **TLS ClientHello** is contained within the **CRYPTO frames** of the **Initial QUIC packets** sent by the client.

Specifically, it is found in:

* **Packet 1574** (Initial, DCID=8af1dd6202afe2ea, PKN: 1, CRYPTO)
* **Packet 1575** (Initial, DCID=8af1dd6202afe2ea, PKN: 2, CRYPTO)

These packets carry the TLS ClientHello message as part of the QUIC CRYPTO frames, which is the first step in the TLS 1.3 handshake embedded within QUIC.

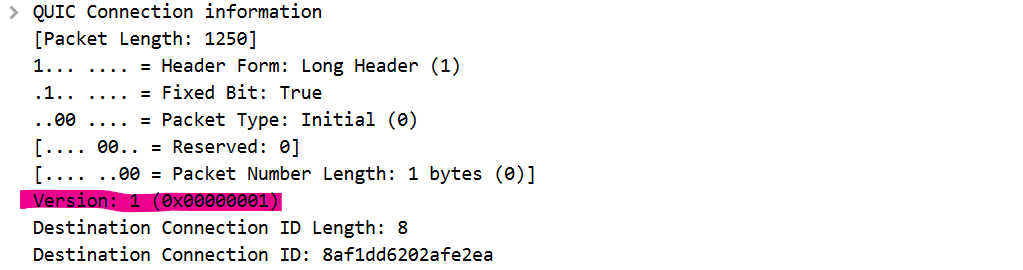


**Question :04:**

Which QUIC version is used in your trace?

**Answer:**

The QUIC version used in your trace is **1 (0x00000001)**, which is the standardized IETF QUIC version 1.



**Question :05:**

Locate the Certificate message. Extract the server’s certificate information (issuer, subject, validity dates).

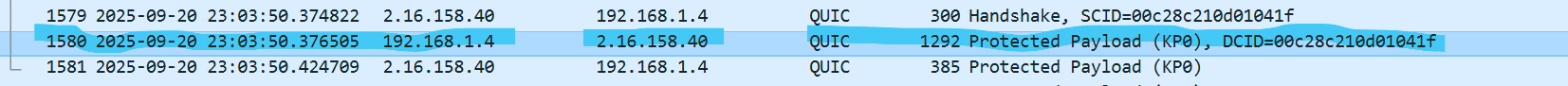
**Answer:**

The **1-RTT keys** are first used in **packet 1580**.

**Evidence:**

* Packet 1580 is labeled: Protected Payload (KP0).
* KP0 stands for **Key Phase 0**, which indicates the first generation of 1-RTT encryption keys.
* This packet is sent by the client (**192.168.1.4**) to the server (**2.16.158.40**) after the handshake is complete, meaning it is encrypted with the 1-RTT keys negotiated during the TLS handshake.

There is no **0-RTT** data in this capture, as all early data packets would be labeled 0-RTT Protected , which is not present here.



**Question :06:**

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

**Answer:**

**The first packet that carries application data (HTTP/3) is packet 1580.**  
It is labeled: Protected Payload (KP0), indicating it is encrypted with 1-RTT keys and contains application data (HTTP/3 frames).

### **How this differs from HTTP over TCP:**

1. **Transport Protocol:**

* **HTTP/3 over QUIC** uses **UDP** (port 443).
* **HTTP over TCP** uses **TCP** (port 80 or 443).

1. **Encryption:**

* **HTTP/3** encrypts **all data**, including headers and payload, at the transport layer (QUIC handles encryption).
* **HTTP over TCP** relies on TLS over TCP (HTTPS) for encryption, which is a separate layer.

1. **Head-of-Line (HOL) Blocking:**

* **HTTP/3** eliminates HOL blocking because each stream is independent; packet loss in one stream doesn’t block others.
* **HTTP over TCP** suffers from HOL blocking; packet loss delays all subsequent packets in the connection.

1. **Connection Establishment:**

* **HTTP/3** uses **QUIC’s combined transport and cryptographic handshake** (often 0-RTT or 1-RTT).
* **HTTP over TCP** requires a TCP handshake (3-way) + TLS handshake (1-2 RTT), resulting in slower startup.

1. **Connection Migration:**

* **HTTP/3** supports connection migration using Connection IDs (e.g., switching networks without dropping the connection).
* **HTTP over TCP** cannot easily migrate connections; IP/port changes break the connection.

1. **Packet Headers:**

* **QUIC headers are encrypted** (except for the initial handshake).
* **TCP headers are unencrypted** (metadata is visible).