**QUIC PACKETS:**

1. What is the name of website?

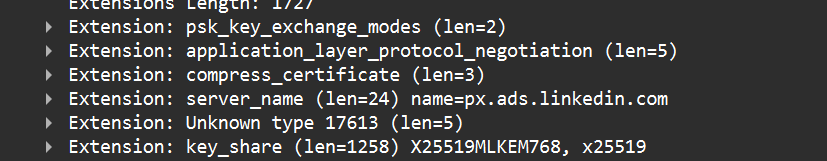
Here the server name represents the name of the server on which site is hosted

A screenshot of a computer

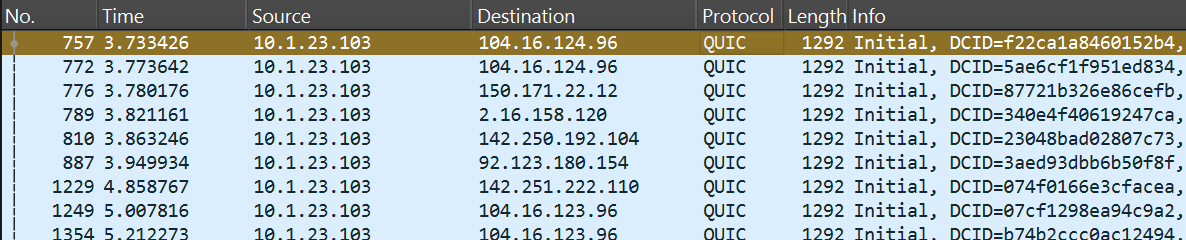
AI-generated content may be incorrect.

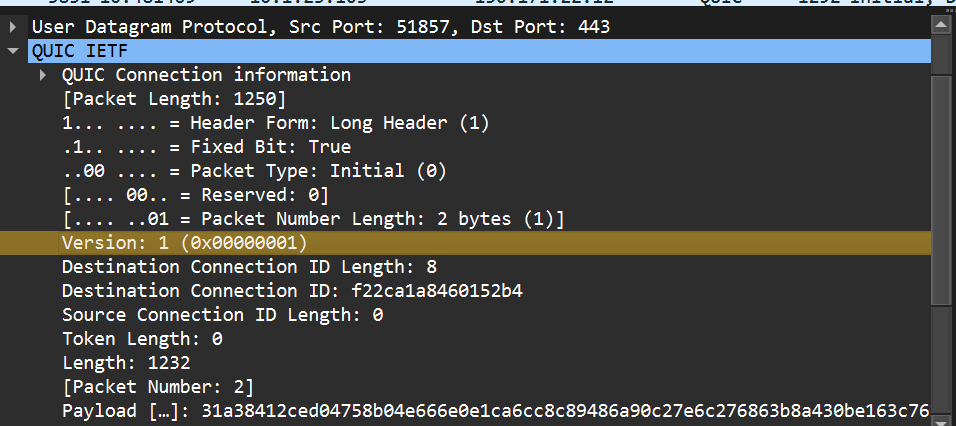
A screen shot of a computer program

AI-generated content may be incorrect.



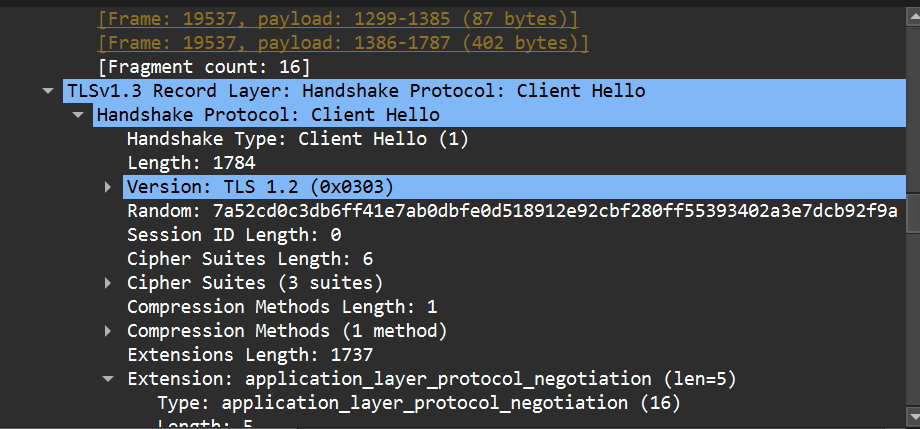
1. Find the packet that contains the Initial QUIC handshake





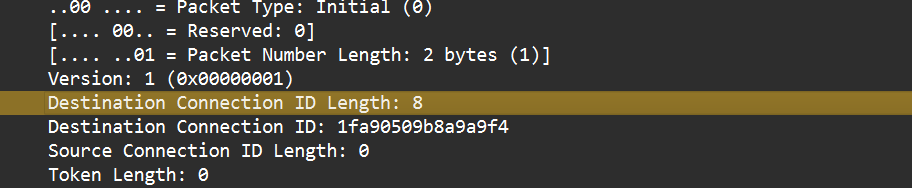
**What information is exchanged in this Initial packet?**

1. **Connection details**
   * QUIC Version (the client proposes one)
   * Source Connection ID & Destination Connection ID
2. **TLS Handshake messages (embedded in QUIC):**
   * **Client → Server (Initial):** contains **TLS ClientHello**
     + Advertises supported TLS version (1.3), cipher suites, key shares, and SNI (server name).
   * **Server → Client (Initial):** contains **TLS ServerHello** and cryptographic parameters needed for key agreement.
3. Identify the QUIC packet that contains the TLS ClientHello (QUIC embeds TLS handshake inside QUIC).



1. Which QUIC version is used in your trace?

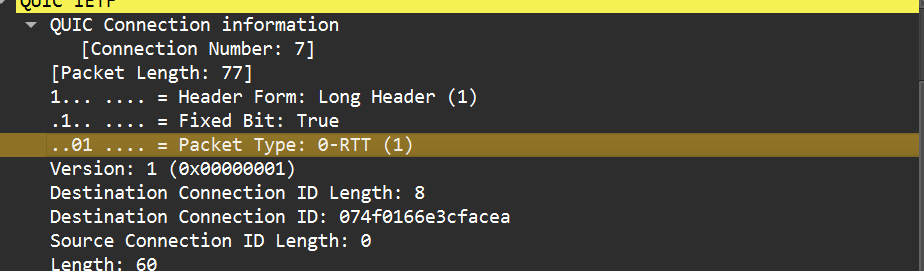
0x00000001 → IETF QUIC version 1 (standardized QUIC v1).



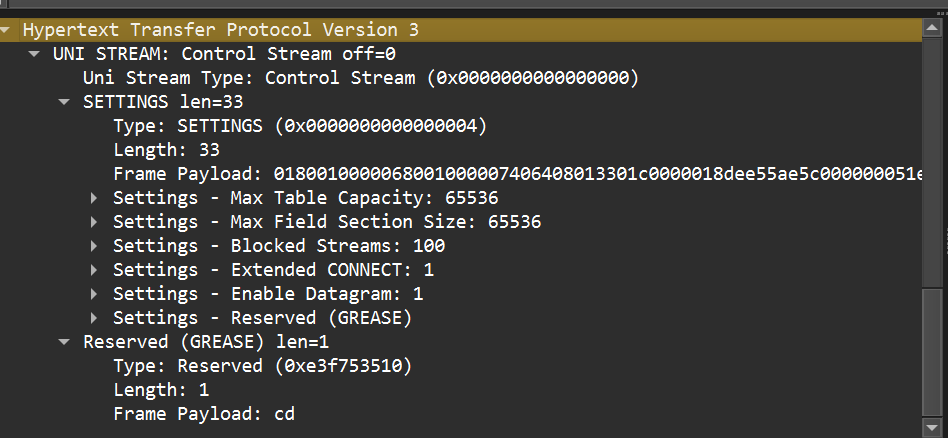
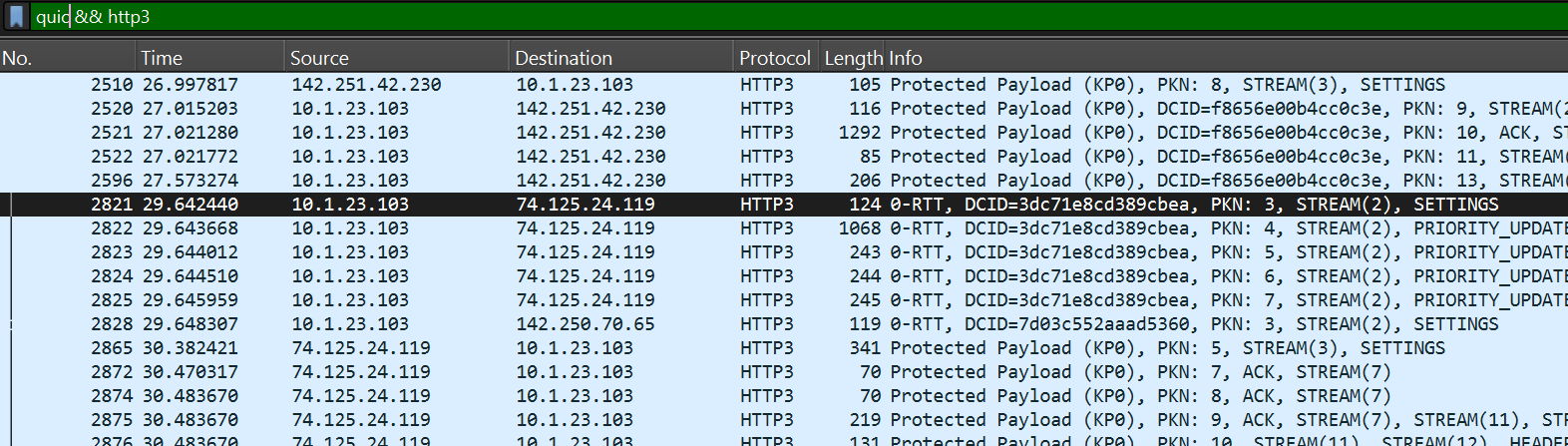
1. Locate the packet where 0-RTT or 1-RTT keys are first used?

 0-RTT packets = rare unless reconnect to the same server with resumption.

 1-RTT = always appears in a fresh session once TLS handshake is done.



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



**How HTTP/3 differs from HTTP over TCP**

* **Transport:**
  + HTTP/3 = runs on **QUIC (UDP)**.
  + HTTP/1.1 & HTTP/2 = run on **TCP**.
* **Encryption:**
  + In QUIC, TLS 1.3 handshake is integrated and encrypted inside QUIC packets.
  + In TCP, TLS handshake is separate and runs above TCP.
* **Multiplexing:**
  + QUIC provides **independent streams** inside a single connection → one stream’s packet loss doesn’t block others.
  + TCP causes **head-of-line blocking** → one lost packet stalls all streams (especially in HTTP/2).
* **Connection migration:**
  + QUIC uses **Connection IDs**, allowing connections to survive IP/port changes.
  + TCP connections break if IP/port changes.