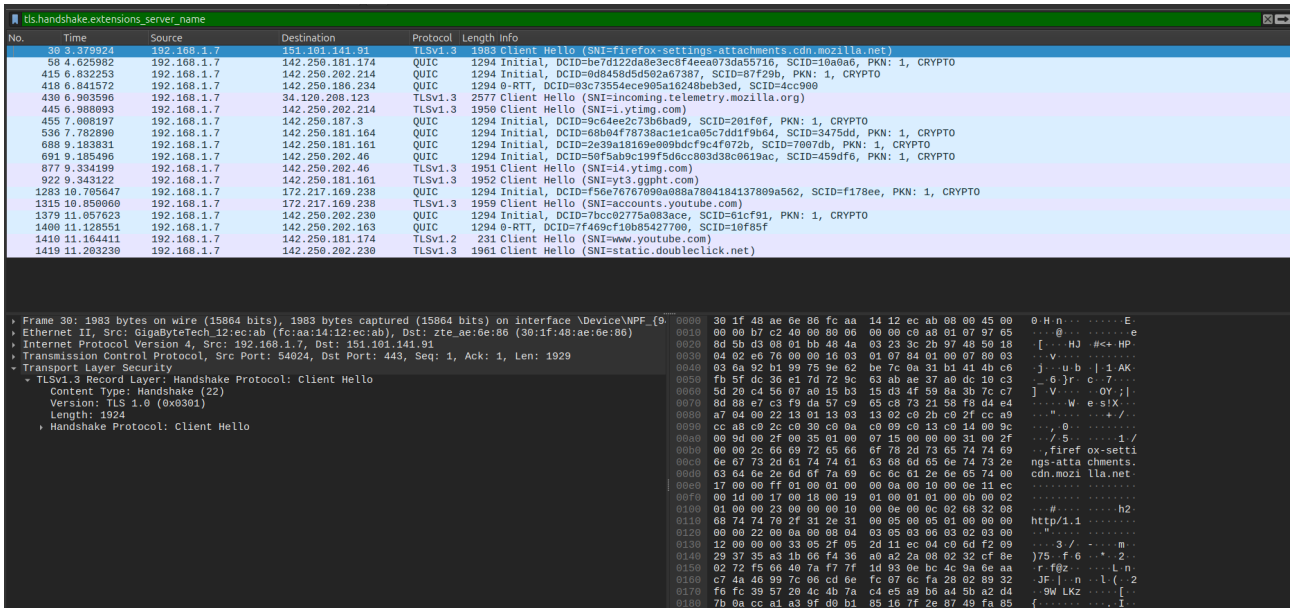
Q1. What is the name of website?
The website is identified from the SNI extension in the ClientHello.
Website: `www.youtube.com`

Q2. Find the packet that contains the Initial QUIC handshake. What information is exchanged here?

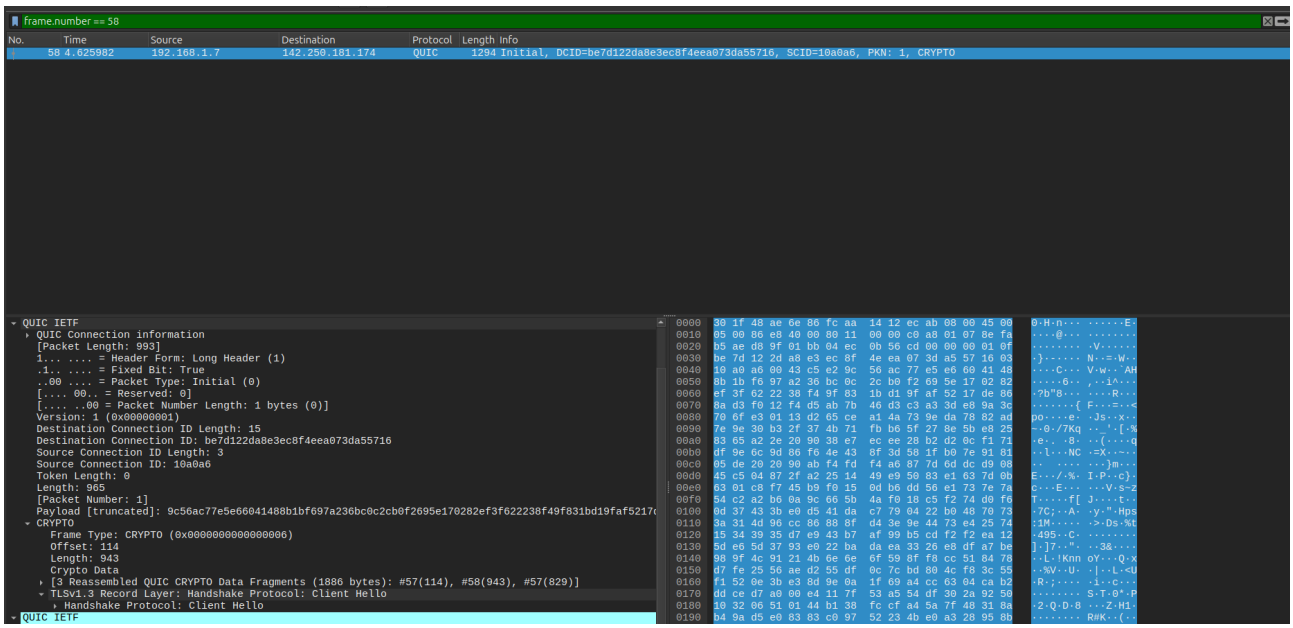
Packet 58

- **Type:** Initial QUIC packet
- **Information exchanged:**
  - TLS **ClientHello**
  - Proposed cipher suites (3 suites offered)
  - Key share values: X25519MLKEM768, x25519, secp256r1
  - Supported version: TLS 1.3
  - QUIC transport parameters
  - Connection IDs (DCID, SCID)



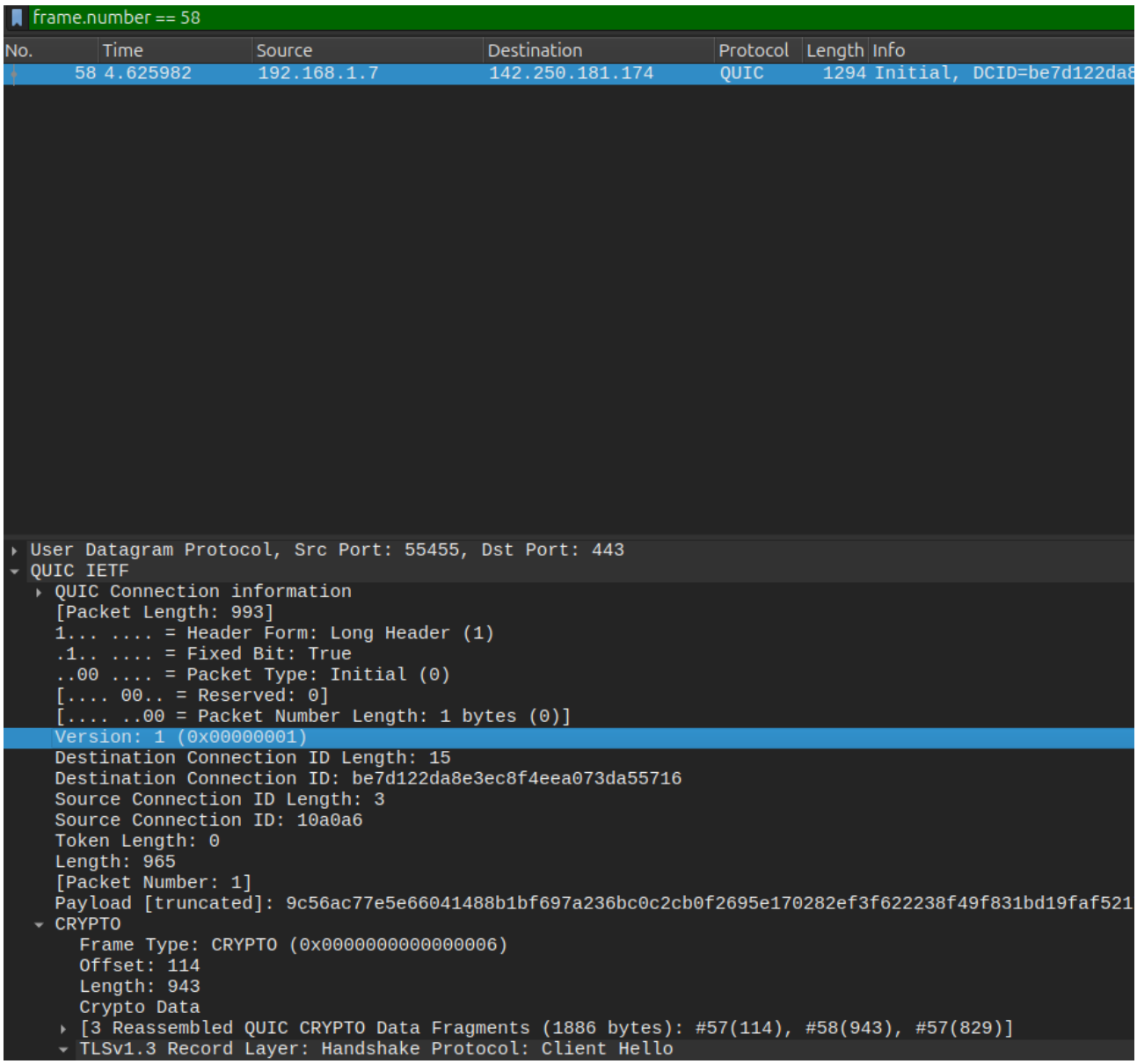
Q3. Identify the QUIC packet that contains the TLS ClientHello.

The TLS ClientHello is embedded inside the Initial QUIC packet:
- **Packet:** 58
- Path: `QUIC → CRYPTO → TLSv1.3 Handshake → Client Hello`



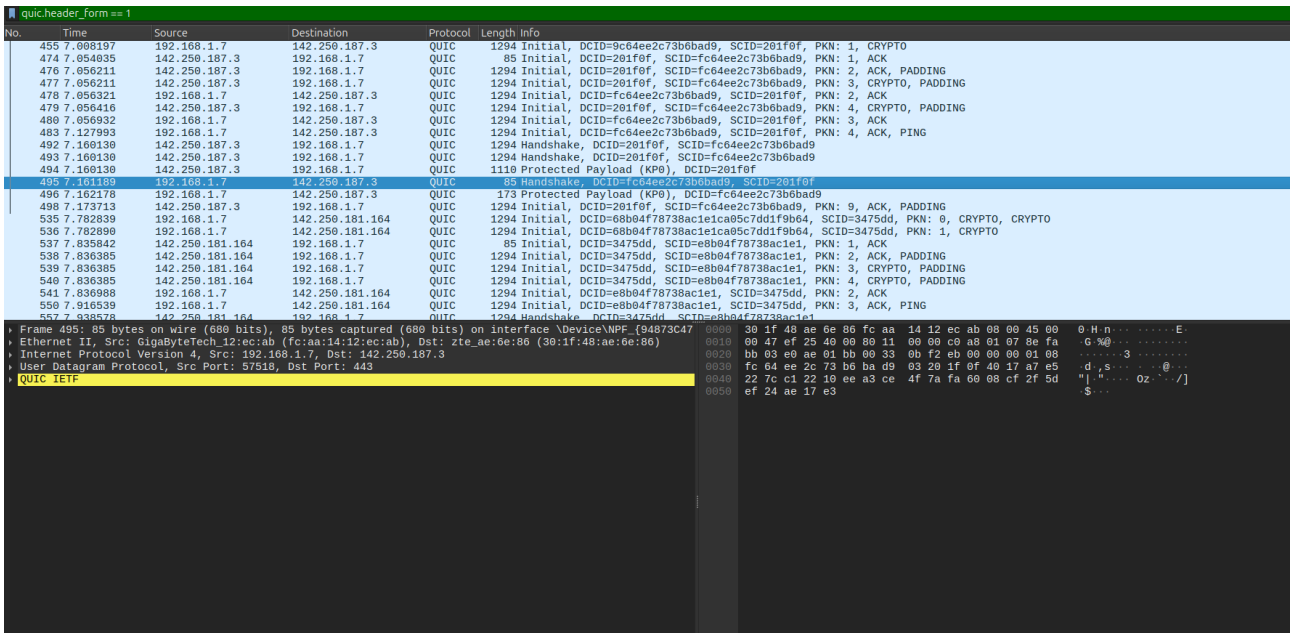
Q4. Which QUIC version is used in your trace?

From the QUIC header in Packet 58:
Version: 1 (0x00000001) → IETF QUIC v1 (used for HTTP/3)



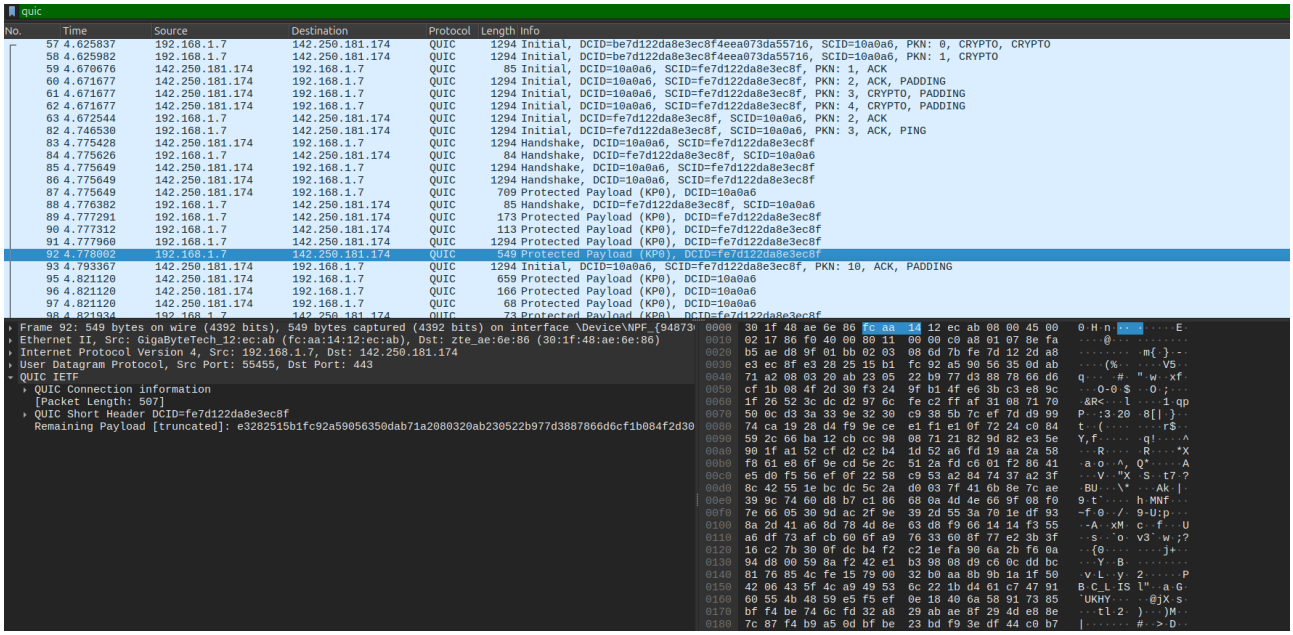
Q5. Locate the packet where 0-RTT or 1-RTT keys are first used.

The first **QUIC 1-RTT Protected** packet marks the start of encrypted communication.
This packet indicates the use of 1-RTT keys for secure application data transfer.



Q6. Find the first packet that carries application data (HTTP/3). How does this differ from HTTP over TCP?

- The first **1-RTT Protected packet with Stream Frame** carries the HTTP/3 application data.



Differences from HTTP over TCP:
- QUIC runs on **UDP** instead of TCP.
- TLS 1.3 encryption is built directly into QUIC.
- Multiplexing streams avoids head-of-line blocking.
- Faster connection setup is possible (0-RTT / 1-RTT).
