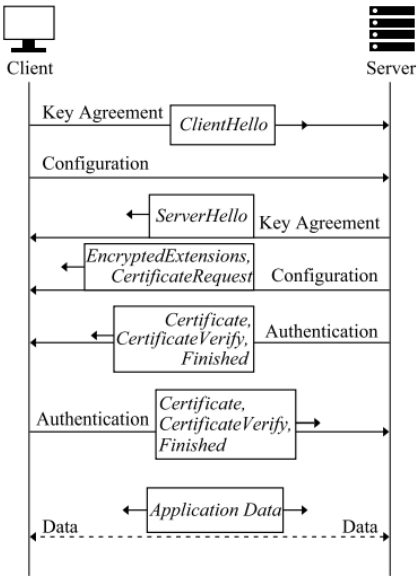
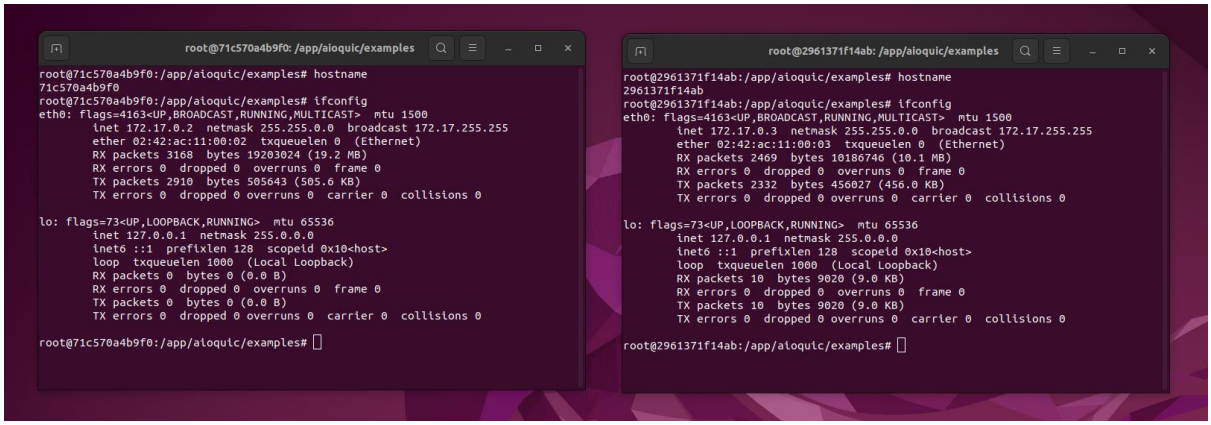
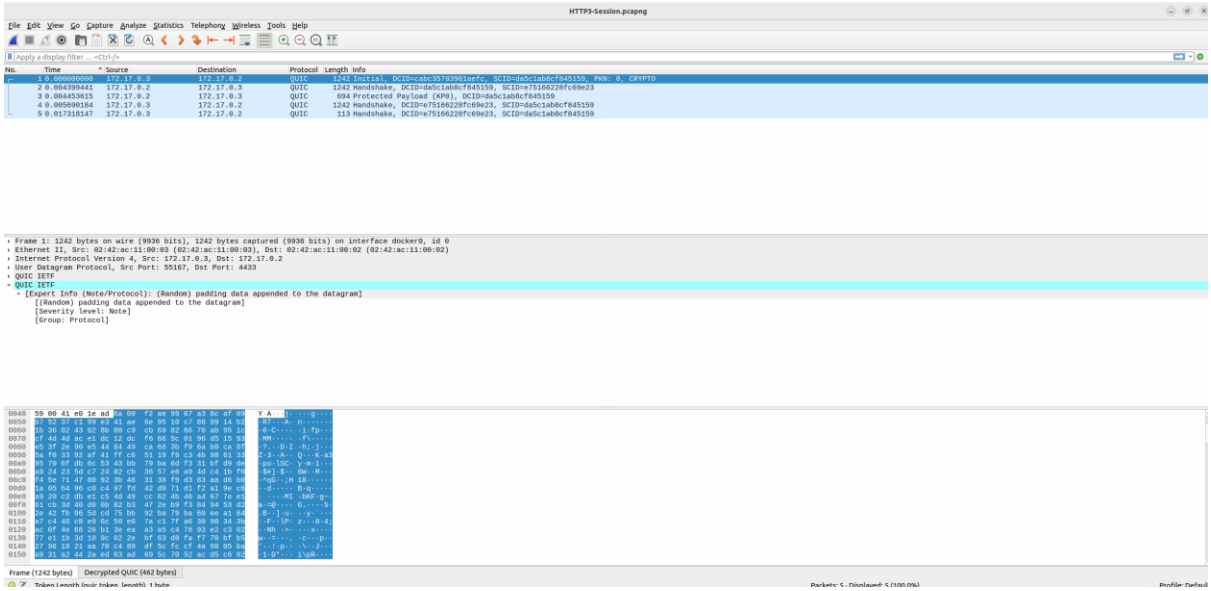
HTTP3 Session Establishment - Two Machines (Docker)





First packet: Client -> Server (Client Hello)



```
Destination Connection ID Length: 8
Destination Connection ID: cabc35783961aefc
Source Connection ID Length: 8
Source Connection ID: da5c1ab8cf845159
```

🔐 DCID and SCID for 0-RTT Resumption

When a client attempts a 0-RTT connection:

The client sends a CRYPTO frame in the Initial packet using the previously established DCID.

If the server recognizes the DCID from a previous session, it allows the client to send encrypted data immediately without waiting for a full handshake.

The server validates the client's session ticket and resumes the connection using the saved session parameters (like cipher suites and keys).

```
QUIC IETF
  QUIC Connection information
  [Packet Length: 506]
  1... .... = Header Form: Long Header (1)
  .1.. .... = Fixed Bit: True
  ..00 .... = Packet Type: Initial (0)
  .... 00.. = Reserved: 0
  .... ..01 = Packet Number Length: 2 bytes (1)
  Version: 1 (0x00000001)
```

Header Form: Long Header (1) connection establishment | Short Header (0) Data sending.

Fixed Bit: Identify if the protocol is QUIC (True -> QUIC | False -/> QUIC)

Packet Type: Initial (0x00) | 0-RTT (0x01) | Handshake (0x02) | Retry (0x03)

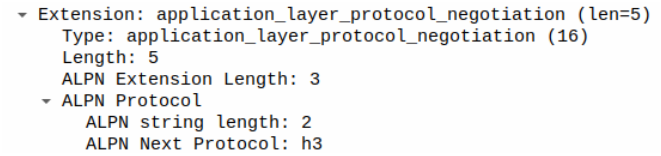
Reserved: Not in use ATM but changes are incoming.

Version: Version of QUIC (Version 2 is out)

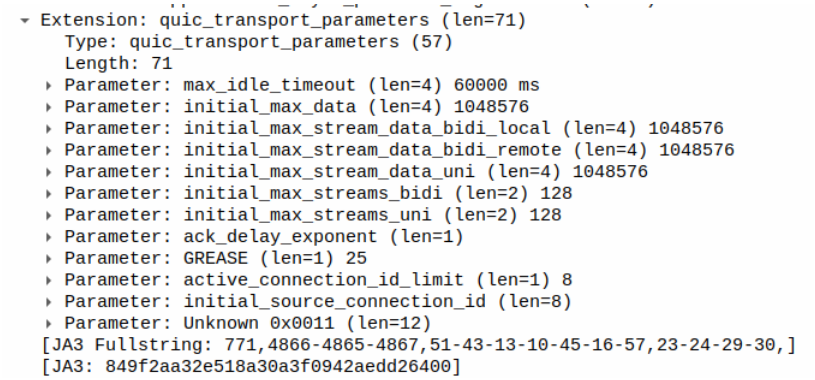
TLSv1.3 Record Layer: Handshake Protocol: Client Hello

```
TLSv1.3 Record Layer: Handshake Protocol: Client Hello
  Handshake Protocol: Client Hello
    Handshake Type: Client Hello (1)
    Length: 454
    Version: TLS 1.2 (0x0303)
    Random: 83fc98f2fbc370db48c64b7b8c42c42758e1492514ec3d61337555e4c6cdbca7
    Session ID Length: 0
    Cipher Suites Length: 6
    Cipher Suites (3 suites)
      Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)
      Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)
      Cipher Suite: TLS_CHACHA20_POLY1305_SHA256 (0x1303)
    Compression Methods Length: 1
    Compression Methods (1 method)
    Extensions Length: 407
    Extension: key_share (len=268)
    Extension: supported_versions (len=3)
    Extension: signature_algorithms (len=20)
    Extension: supported_groups (len=10)
```

The **Key Share Extension** in the **ClientHello** is used to perform the Diffie-Hellman key exchange in **TLS 1.3**, allowing both the client and server to agree on a shared encryption key in fewer round trips. The extension contains the client's **public key** and the **key exchange group** used for the secure handshake.

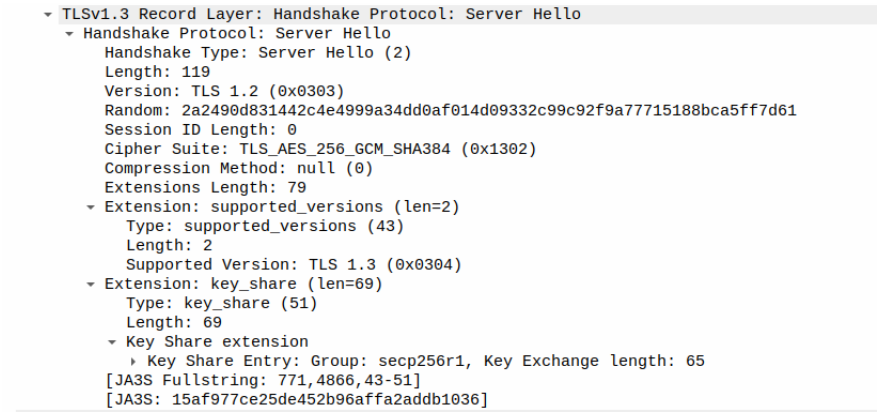


Lists the protocols the client supports at the **application layer**, like **HTTP/3** or **HTTP/2**.
Example: h3, h2.



It contains QUIC-specific parameters, such as connection IDs, initial flow control limits, and maximum packet sizes. It ensures the client and server agree on **transport-level settings** for the QUIC protocol.

Server Hello:



Supported version: The server supports TLSv1.3.

original_destination_connection_id (len=8)

The original connection ID from the client to maintain the connection context.

max_idle_timeout (len=4)

The maximum allowed idle time before the connection is closed, in this case, 60000 ms (60 seconds).

stateless_reset_token (len=16)

A token used for stateless resets to close a connection without maintaining state.

initial_max_data (len=4)

The initial maximum amount of data the peer is allowed to send, 1048576 bytes (1MB).

initial_max_stream_data_bidi_local (len=4)

The initial maximum amount of data for locally initiated bidirectional streams, 1048576 bytes.

initial_max_stream_data_bidi_remote (len=4)

The initial maximum amount of data for remotely initiated bidirectional streams, 1048576 bytes.

initial_max_stream_data_uni (len=4)

The initial maximum amount of data for unidirectional streams, 1048576 bytes.

initial_max_streams_bidi (len=2)

The initial maximum number of bidirectional streams, 128 streams.

initial_max_streams_uni (len=2)

The initial maximum number of unidirectional streams, 128 streams.

ack_delay_exponent (len=1)

Defines the exponent for the acknowledgment delay, controlling how soon ACKs are sent after receiving data.

GREASE (len=1)

A value used for "Grease" to ensure future protocol flexibility and to avoid potential attacks.

active_connection_id_limit (len=1)

The maximum number of connection IDs the peer can hold, in this case, 8.

initial_source_connection_id (len=8)

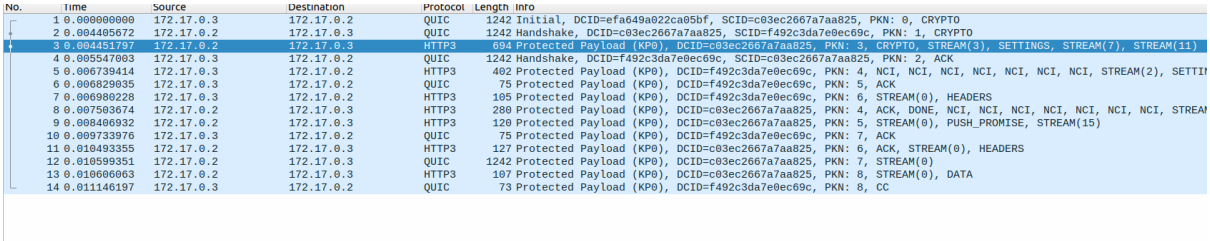
The connection ID for the source to initiate the connection, which helps route traffic correctly.

Unknown 0x0011 (len=12)

An unknown parameter type with a length of 12 bytes, representing proprietary or experimental extensions.

max_datagram_frame_size (len=4)

The maximum size of datagram frames, in this case, 65536 bytes (64 KB).



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	172.17.0.3	172.17.0.2	QUIC	1242	Initial, DCID=efa649a022ca05bf, SCID=c03ec2667a7aa825, PKN: 0, CRYPTO
2	0.004405672	172.17.0.2	172.17.0.3	QUIC	1242	Handshake, DCID=c03ec2667a7aa825, SCID=f492c3da7e0ec69c, PKN: 1, CRYPTO
3	0.004451797	172.17.0.2	172.17.0.3	HTTP3	694	Protected Payload (KP0), DCID=c03ec2667a7aa825, PKN: 3, CRYPTO, STREAM(3), SETTINGS, STREAM(7), STREAM(11)
4	0.005547003	172.17.0.3	172.17.0.2	QUIC	1242	Handshake, DCID=f492c3da7e0ec69c, SCID=c03ec2667a7aa825, PKN: 2, ACK
5	0.006739414	172.17.0.3	172.17.0.2	HTTP3	402	Protected Payload (KP0), DCID=f492c3da7e0ec69c, PKN: 4, NCI, NCI, NCI, NCI, NCI, NCI, STREAM(2), SETTI
6	0.006829035	172.17.0.3	172.17.0.2	QUIC	75	Protected Payload (KP0), DCID=f492c3da7e0ec69c, PKN: 5, ACK
7	0.006980228	172.17.0.3	172.17.0.2	HTTP3	105	Protected Payload (KP0), DCID=f492c3da7e0ec69c, PKN: 6, STREAM(0), HEADERS
8	0.007503674	172.17.0.2	172.17.0.3	HTTP3	280	Protected Payload (KP0), DCID=c03ec2667a7aa825, PKN: 4, ACK, DONE, NCI, NCI, NCI, NCI, NCI, NCI, NCI, STREA
9	0.008406932	172.17.0.2	172.17.0.3	HTTP3	120	Protected Payload (KP0), DCID=c03ec2667a7aa825, PKN: 5, STREAM(0), PUSH_PROMISE, STREAM(15)
10	0.009733976	172.17.0.3	172.17.0.2	QUIC	75	Protected Payload (KP0), DCID=f492c3da7e0ec69c, PKN: 7, ACK
11	0.010493355	172.17.0.2	172.17.0.3	HTTP3	127	Protected Payload (KP0), DCID=c03ec2667a7aa825, PKN: 6, ACK, STREAM(0), HEADERS
12	0.010599351	172.17.0.2	172.17.0.3	QUIC	1242	Protected Payload (KP0), DCID=c03ec2667a7aa825, PKN: 7, STREAM(0)
13	0.010606063	172.17.0.2	172.17.0.3	HTTP3	107	Protected Payload (KP0), DCID=c03ec2667a7aa825, PKN: 8, STREAM(0), DATA
14	0.011146197	172.17.0.3	172.17.0.2	QUIC	73	Protected Payload (KP0), DCID=f492c3da7e0ec69c, PKN: 8, CC

```
..10 .... = Packet Type: Handshake (2)
.... 00.. = Reserved: 0
.... ..01 = Packet Number Length: 2 bytes (1)
Version: 1 (0x00000001)
Destination Connection ID Length: 8
Destination Connection ID: c03ec2667a7aa825
Source Connection ID Length: 8
Source Connection ID: f492c3da7e0ec69c
Length: 474
Packet Number: 2
Payload: 6e8216f9c15a49883cf5b26b127f461ed546b3c283a59bc954b1d467660ef106f71dbcec…
▾ CRYPTO
    Frame Type: CRYPTO (0x0000000000000006)
    Offset: 976
    Length: 451
    Crypto Data
  ▾ TLSv1.3 Record Layer: Handshake Protocol: Multiple Handshake Messages
      Handshake Protocol: Certificate (last fragment)
    ▸ [2 Reassembled Handshake Fragments (987 bytes): #2(852), #3(135)]
    ▾ Handshake Protocol: Certificate
        Handshake Type: Certificate (11)
        Length: 983
        Certificate Request Context Length: 0
        Certificates Length: 979
      ▸ Certificates (979 bytes)
    ▾ Handshake Protocol: Certificate Verify
        Handshake Type: Certificate Verify (15)
        Length: 260
      ▸ Signature Algorithm: rsa_pss_rsae_sha256 (0x0804)
        Signature Length: 256
        Signature: 666e010de7dd63c61883879f1c8b0772dc755f10ce5ac6c134b20e0a526261db9ab94049…
    ▾ Handshake Protocol: Finished
        Handshake Type: Finished (20)
        Length: 48
        Verify Data
▾ QUIC IETF
```

Summary of Protocol Actions:

Certificate: The server is sending its certificate, proving its identity.

Certificate Verify: The server is proving ownership of the certificate's private key.

Finished: The server confirms that the handshake is complete from its side.

New Session Ticket: The server offers the client the option to resume the session later without a full handshake.

Stream Data: The server initiates QUIC streams to transmit application data.

0.000000000	60241	Initial, DCID=efa649a022ca05bf, SCID=c03ec2667a7aa825, PKN: 0, CRYPTO	4433
0.004405672	60241	Handshake, DCID=c03ec2667a7aa825, SCID=f492c3da7e0ec69c, PKN: 1, CRYPTO	4433
0.004451797	60241	Protected Payload (KP0), DCID=c03ec2667a7aa825, PKN: 3, CRYPTO, STREAM(3), SETTINGS, STREAM(7), STREAM(11)	4433
0.005547003	60241	Handshake, DCID=f492c3da7e0ec69c, SCID=c03ec2667a7aa825, PKN: 2, ACK	4433
0.006739414	60241	Protected Payload (KP0), DCID=f492c3da7e0ec69c, PKN: 4, NCI, NCI, NCI, NCI, NCI, NCI, STREAM(2), SETTINGS, MAX_PUSH_ID, STREAM(6), STREAM(10)	4433
0.006829035	60241	Protected Payload (KP0), DCID=f492c3da7e0ec69c, PKN: 5, ACK	4433
0.006980228	60241	Protected Payload (KP0), DCID=f492c3da7e0ec69c, PKN: 6, STREAM(0), HEADERS	4433
0.007503674	60241	Protected Payload (KP0), DCID=c03ec2667a7aa825, PKN: 4, ACK, DONE, NCI, NCI, NCI, NCI, NCI, NCI, STREAM(7)	4433
0.008406932	60241	Protected Payload (KP0), DCID=c03ec2667a7aa825, PKN: 5, STREAM(0), PUSH_PROMISE, STREAM(15)	4433
0.009733976	60241	Protected Payload (KP0), DCID=f492c3da7e0ec69c, PKN: 7, ACK	4433
0.010493355	60241	Protected Payload (KP0), DCID=c03ec2667a7aa825, PKN: 6, ACK, STREAM(0), HEADERS	4433
0.010599351	60241	Protected Payload (KP0), DCID=c03ec2667a7aa825, PKN: 7, STREAM(0)	4433
0.010606063	60241	Protected Payload (KP0), DCID=c03ec2667a7aa825, PKN: 8, STREAM(0), DATA	4433
0.011146197	60241	Protected Payload (KP0), DCID=f492c3da7e0ec69c, PKN: 8, CC	4433