

```
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?

```
- **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)
```

— — —

The TLS ClientHello is embedded inside the Initial QUIC packet:

```
- **Packet:** 58
- Path: `QUIC → CRYPTO → TLSv1.3 Handshake → Client Hello`
```


frame.number == 58						
No.	Time	Source	Destination	Protocol	Length	Info
58	4.625982	192.168.1.7	142.250.181.174	QUIC	1294	Initial, DCID=be7d122da8
User Datagram Protocol, Src Port: 55455, Dst Port: 443 QUIC IETF QUIC Connection information [Packet Length: 993] 1... = Header Form: Long Header (1) .1.. = Fixed Bit: True ..00 = Packet Type: Initial (0) [.... 00.. = Reserved: 0] [.... ..00 = Packet Number Length: 1 bytes (0)] Version: 1 (0x00000001) Destination Connection ID Length: 15 Destination Connection ID: be7d122da8e3ec8f4eea073da55716 Source Connection ID Length: 3 Source Connection ID: 10a0a6 Token Length: 0 Length: 965 [Packet Number: 1] Payload [truncated]: 9c56ac77e5e66041488b1bf697a236bc0c2cb0f2695e170282ef3f622238f49f831bd19faf521 CRYPTO Frame Type: CRYPTO (0x0000000000000006) Offset: 114 Length: 943 Crypto Data [3 Reassembled QUIC CRYPTO Data Fragments (1886 bytes): #57(114), #58(943), #57(829)] TLSv1.3 Record Layer: Handshake Protocol: Client Hello						

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.

No.	Time	Source	Destination	Protocol	Length	Info
455	7.808197	192.168.1.7	142.250.187.3	QUIC	1294	Initial, DCID=9c64ee2c73b6bad9, SCID=281f0f, PKN: 1, CRYPTO
474	7.054035	142.250.187.3	192.168.1.7	QUIC	85	Initial, DCID=281f0f, SCID=fc64ee2c73b6bad9, PKN: 1, ACK
476	7.056211	142.250.187.3	192.168.1.7	QUIC	1294	Initial, DCID=281f0f, SCID=fc64ee2c73b6bad9, PKN: 2, ACK, PADDING
477	7.056211	142.250.187.3	192.168.1.7	QUIC	1294	Initial, DCID=281f0f, SCID=fc64ee2c73b6bad9, PKN: 3, CRYPTO, PADDING
478	7.056321	192.168.1.7	142.250.187.3	QUIC	1294	Initial, DCID=fc64ee2c73b6bad9, SCID=281f0f, PKN: 2, ACK
479	7.056416	142.250.187.3	192.168.1.7	QUIC	1294	Initial, DCID=281f0f, SCID=fc64ee2c73b6bad9, PKN: 4, CRYPTO, PADDING
480	7.056932	192.168.1.7	142.250.187.3	QUIC	1294	Initial, DCID=fc64ee2c73b6bad9, SCID=281f0f, PKN: 3, ACK
483	7.127993	192.168.1.7	142.250.187.3	QUIC	1294	Initial, DCID=fc64ee2c73b6bad9, SCID=281f0f, PKN: 4, ACK, PING
492	7.160130	142.250.187.3	192.168.1.7	QUIC	1294	Handshake, DCID=281f0f, SCID=fc64ee2c73b6bad9
493	7.160130	142.250.187.3	192.168.1.7	QUIC	1294	Handshake, DCID=281f0f, SCID=fc64ee2c73b6bad9
494	7.160130	142.250.187.3	192.168.1.7	QUIC	1110	Protected Payload (KP0), DCID=281f0f
495	7.161189	192.168.1.7	142.250.187.3	QUIC	85	Handshake, DCID=fc64ee2c73b6bad9, SCID=281f0f
496	7.162178	192.168.1.7	142.250.187.3	QUIC	173	Protected Payload (KP0), DCID=fc64ee2c73b6bad9
498	7.173713	142.250.187.3	192.168.1.7	QUIC	1294	Initial, DCID=281f0f, SCID=fc64ee2c73b6bad9, PKN: 9, ACK, PADDING
535	7.782839	192.168.1.7	142.250.181.164	QUIC	1294	Initial, DCID=68b04f78738ac1e1ca95c7dd1f9b64, SCID=3475dd, PKN: 0, CRYPTO, CRYPTO
536	7.782890	192.168.1.7	142.250.181.164	QUIC	1294	Initial, DCID=68b04f78738ac1e1ca95c7dd1f9b64, SCID=3475dd, PKN: 1, CRYPTO
537	7.835842	142.250.181.164	192.168.1.7	QUIC	85	Initial, DCID=3475dd, SCID=e8b04f78738ac1e1, PKN: 1, ACK
538	7.836305	142.250.181.164	192.168.1.7	QUIC	1294	Initial, DCID=3475dd, SCID=e8b04f78738ac1e1, PKN: 2, ACK, PADDING
539	7.836385	142.250.181.164	192.168.1.7	QUIC	1294	Initial, DCID=3475dd, SCID=e8b04f78738ac1e1, PKN: 3, CRYPTO, PADDING
540	7.836385	142.250.181.164	192.168.1.7	QUIC	1294	Initial, DCID=3475dd, SCID=e8b04f78738ac1e1, PKN: 4, CRYPTO, PADDING
541	7.836988	192.168.1.7	142.250.181.164	QUIC	1294	Initial, DCID=e8b04f78738ac1e1, SCID=3475dd, PKN: 2, ACK
550	7.916539	192.168.1.7	142.250.181.164	QUIC	1294	Initial, DCID=e8b04f78738ac1e1, SCID=3475dd, PKN: 3, ACK, PING
557	7.938578	142.250.181.164	192.168.1.7	QUIC	1294	Handshake, DCID=3475dd, SCID=e8b04f78738ac1e1
* Frame 495: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on interface \Device\NPF_{94873C47-0000-301F-48AE-6E86}FC AA 14 12 EC AB 08 00 45 00 0 H N E * Ethernet II, Src: GigabyteTech-12:ec:ab (fc:aa:14:12:ec:ab), Dst: zte_ae:6e:86 (30:1f:48:ae:6e:86) 0010 00 47 ef 25 40 00 00 11 00 00 c0 a8 01 07 8e fa 0 H N E * Internet Protocol Version 4, Src: 192.168.1.7, Dst: 142.250.181.74 0020 bb 03 e0 ae 01 b0 00 33 00 f2 eb 00 00 01 08 0 H N E * User Datagram Protocol, Src Port: 57518, Dst Port: 443 0030 fc 64 ee 2c 73 b6 ba d9 03 20 1f 0f 40 17 a7 e5 d, s @ * QUIC IETF 0040 22 7c c1 22 18 ee a3 ce 4f 7a fa 60 08 cf 2f 5d " " Oz / 0050 ef 24 ae 17 e3 \$						

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.

No.	Time	Source	Destination	Protocol	Length	Info
57	4.625837	192.168.1.7	142.250.181.174	QUIC	1294	Initial, DCID=be7d122da8e3ec8f4dea073da55716, SCID=10a0a6, PKN: 0, CRYPTO, CRYPTO
58	4.625882	192.168.1.7	142.250.181.174	QUIC	1294	Initial, DCID=be7d122da8e3ec8f4dea073da55716, SCID=10a0a6, PKN: 1, CRYPTO
59	4.670676	142.250.181.174	192.168.1.7	QUIC	85	Initial, DCID=10a0a6, SCID=fe7d122da8e3ec8f, PKN: 1, ACK
60	4.671677	142.250.181.174	192.168.1.7	QUIC	1294	Initial, DCID=10a0a6, SCID=fe7d122da8e3ec8f, PKN: 2, ACK, PADDING
61	4.671677	142.250.181.174	192.168.1.7	QUIC	1294	Initial, DCID=10a0a6, SCID=fe7d122da8e3ec8f, PKN: 3, CRYPTO, PADDING
62	4.671677	142.250.181.174	192.168.1.7	QUIC	1294	Initial, DCID=10a0a6, SCID=fe7d122da8e3ec8f, PKN: 4, CRYPTO, PADDING
63	4.672544	192.168.1.7	142.250.181.174	QUIC	1294	Initial, DCID=fe7d122da8e3ec8f, SCID=10a0a6, PKN: 2, ACK
82	4.746530	192.168.1.7	142.250.181.174	QUIC	1294	Initial, DCID=fe7d122da8e3ec8f, SCID=10a0a6, PKN: 3, ACK, PING
83	4.775428	142.250.181.174	192.168.1.7	QUIC	1294	Handshake, DCID=10a0a6, SCID=fe7d122da8e3ec8f
84	4.775626	192.168.1.7	142.250.181.174	QUIC	84	Handshake, DCID=fe7d122da8e3ec8f, SCID=10a0a6
85	4.775649	142.250.181.174	192.168.1.7	QUIC	1294	Handshake, DCID=10a0a6, SCID=fe7d122da8e3ec8f
86	4.775649	142.250.181.174	192.168.1.7	QUIC	1294	Handshake, DCID=10a0a6, SCID=fe7d122da8e3ec8f
87	4.775649	142.250.181.174	192.168.1.7	QUIC	789	Protected Payload (KP0), DCID=10a0a6
88	4.776382	192.168.1.7	142.250.181.174	QUIC	85	Handshake, DCID=fe7d122da8e3ec8f, SCID=10a0a6
89	4.777291	192.168.1.7	142.250.181.174	QUIC	173	Protected Payload (KP0), DCID=fe7d122da8e3ec8f
90	4.777312	192.168.1.7	142.250.181.174	QUIC	113	Protected Payload (KP0), DCID=fe7d122da8e3ec8f
91	4.777960	192.168.1.7	142.250.181.174	QUIC	1294	Protected Payload (KP0), DCID=fe7d122da8e3ec8f
92	4.821092	142.250.181.174	192.168.1.7	QUIC	450	Protected Payload (KP0), DCID=fe7d122da8e3ec8f
93	4.793367	142.250.181.174	192.168.1.7	QUIC	1294	Initial, DCID=10a0a6, SCID=fe7d122da8e3ec8f, PKN: 10, ACK, PADDING
95	4.821120	142.250.181.174	192.168.1.7	QUIC	659	Protected Payload (KP0), DCID=10a0a6
96	4.821120	142.250.181.174	192.168.1.7	QUIC	166	Protected Payload (KP0), DCID=10a0a6
97	4.821120	142.250.181.174	192.168.1.7	QUIC	68	Protected Payload (KP0), DCID=10a0a6
98	4.821934	192.168.1.7	142.250.181.174	QUIC	73	Protected Payload (KP0), DCID=fe7d122da8e3ec8f
* Frame 92: 549 bytes on wire (4392 bits), 549 bytes captured (4392 bits) on interface \Device\NPF_{94873C47-0000-301F-48AE-6E86}FC AA 14 12 EC AB 08 00 45 00 0 H N E * Ethernet II, Src: GigabyteTech-12:ec:ab (fc:aa:14:12:ec:ab), Dst: zte_ae:6e:86 (30:1f:48:ae:6e:86) 0010 02 17 86 f0 40 00 00 11 00 00 c0 a8 01 07 8e fa m() * Internet Protocol Version 4, Src: 192.168.1.7, Dst: 142.250.181.174 0020 e3 ec 8f e3 28 25 15 b1 fc 92 a5 98 56 35 0d ab % V5.. * User Datagram Protocol, Src Port: 55455, Dst Port: 443 0030 71 a2 08 03 20 ab 23 05 22 b9 7f 83 88 78 66 d6 q # w x f * QUIC IETF 0040 cf 1b 08 4f 2d 39 f3 24 9f b1 4f e6 3b c3 e8 9c 0-0 \$ 0 ; * QUIC Connection information 0050 1f 20 52 2c dc d2 97 6c fc c2 ff af 33 90 71 70 &R l 1 qp * [Packet Length: 507] 0060 50 8c d3 3a 33 9e 32 0c c9 38 5b 7c ef 7d 09 93 P 3 20 8[] * QUIC Short Header DCID=fe7d122da8e3ec8f 0070 74 ca 19 28 d4 f9 9e ce e1 f1 e1 0f 72 24 00 84 t (..... r \$ * Remaining Payload [truncated]: e3282515bfc92a59956350dab71a2080320ab230522b977d3887866dcfb084f2d30 0080 59 2c 66 ba 12 cb cc 98 08 71 21 82 9d 82 e3 5e Y, f q A 0090 90 1f a1 52 cf d2 c2 b4 1d 52 a0 fd 19 aa 2a 38 .. R R X 00a0 f0 61 e8 6f 9e cd 5e 2c 51 2a fd c6 02 f2 86 41 a o A, Q A 00b0 e5 0d f5 56 ef 0f 22 58 c9 53 a2 84 74 37 a2 3f .. v X S t 7 ? 00c0 8c 42 55 1e bc dc 5c 2a d0 03 7f 41 6b 8e 7c ae BU ^ Ak 00d0 39 9c 74 60 d8 b7 c1 86 68 0a 4d 4e 66 9f 08 f0 9 t r M N F 00e0 7e 66 05 30 0d ac 2f 0e 39 2d 55 3a 70 1e df 93 .. f 0 / 0-0 p 00f0 8a 2d 41 a0 8d 78 4d 8e 63 d8 f9 66 14 14 f3 55 .. A x m c f U 0100 a6 df 73 af cb 60 6f a9 76 33 60 8f 77 e2 3b 3f .. s o v w ? 0110 16 c2 7b 30 0f dc b4 f2 c2 1e fa 90 6a 2b f6 0a .. (..... 0 j + 0120 94 08 00 59 ba f2 42 e1 b3 98 08 09 c0 0c dd bc .. Y B 0130 81 76 85 4c fe 15 70 00 32 b0 aa 8b 9b 1a 1f 90 v L y 2 P 0140 42 06 43 5f 4c a9 49 53 6c 22 1b d4 61 c7 47 91 B C L IS l a G 0150 60 55 4b 48 59 e5 f5 ef 0e 18 40 6a 58 91 73 85 .. UKHY : @ j x s 0160 bf f4 be 74 6c fd 32 a8 29 ab ae 8f 29 4d e8 8e .. t t 2) M 0170 7c 87 f4 b9 a5 9d bf be 23 bd f9 5e df 44 c0 b7 : # > D						

****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).
