

## Task 6:

### QUIC based questions

#### 1. What is the name of website?

- google

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

- Packet no 2

The image displays two screenshots from the Wireshark network protocol analyzer. The top screenshot shows the packet list pane with packet 2 selected, which is a QUIC Initial packet. The packet details pane shows the 'QUIC IETF' section expanded, revealing the 'QUIC Connection information' and 'Version: 1 (0x00000001)'. The packet bytes pane shows the raw data of the packet. The bottom screenshot shows the 'Packet 2 - QUIC trace.pcapng' window, which provides a detailed view of the packet structure, including the 'QUIC Connection information' and the 'Version: 1 (0x00000001)' field. The packet details pane also shows the 'QUIC IETF' section expanded, revealing the 'QUIC Connection information' and 'Version: 1 (0x00000001)' field. The packet bytes pane shows the raw data of the packet.

Wireshark - Packet 2 - QUIC trace.pcapng

Frame 2: 1292 bytes on wire (10336 bits), 1292 bytes captured (10336 bits) on interface \Device\NPF\_{DF77F61D-0DA1-470F-9FED-ECBE05406A71}

Ethernet II, Src: d6:93:3e:ac:e2:03 (d6:93:3e:ac:e2:03), Dst: HuaweiTechno\_f6:d6:47 (a0:1c:8d:f6:d6:47)

Internet Protocol Version 4, Src: 10.1.37.200, Dst: 162.159.61.3

User Datagram Protocol, Src Port: 59086, Dst Port: 443

QUIC IETF

QUIC Connection information

[Packet Length: 1250]

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)

Destination Connection ID Length: 20

Destination Connection ID: 01c7d6435df7245ae6c5334349f7027df4906a0c

Source Connection ID Length: 0

Token Length: 0

Length: 1250

[Expert Info (Warning/Decryption): Failed to create decryption context: Decryption (checktag) failed: Checksum error]

Remaining Payload [-]: 87266a9f98eba0ded8189062f827ee67536be37e68998b14f640831ac7986f006c91da385549483177a39b902b52635951d659b0651

QUIC IETF (quic), 1250 bytes

Show packet bytes Layout: Vertical (Stacked)

Close Help

Exchanged informations:

- Source connection id
- Destination connection id
- Destination connection id length
- Version
- Token length

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

- Frame 6

No.	Time	Source	Destination	Protocol	Length	Info
6	0.108423	10.1.37.200	162.159.61.3	TLSv1.2	1821	Client Hello (SNI=chrome.cloudflare-dns.com)
16	1.034664	10.1.37.200	172.64.41.3	QUIC	1292	Initial, DCID=c932945b5bf5fc1f, PKN: 2, CRYPTO, PADDING, CRYPTO, CRYPTO, CRYPTO, PADDING, C...
21	1.202744	10.1.37.200	172.64.41.3	TLSv1.2	1885	Client Hello (SNI=chrome.cloudflare-dns.com)
30	1.394967	10.1.37.200	172.64.41.3	TLSv1.2	1789	Client Hello (SNI=chrome.cloudflare-dns.com)
34	1.569640	10.1.37.200	162.159.61.3	QUIC	1292	Initial, DCID=51ea003bdc17b07, PKN: 2, CRYPTO, CRYPTO, PADDING, PING, PING, PING, PI...
44	1.787631	10.1.37.200	162.159.61.3	TLSv1.2	1853	Client Hello (SNI=chrome.cloudflare-dns.com)
53	1.981461	10.1.37.200	162.159.61.3	TLSv1.2	1885	Client Hello (SNI=chrome.cloudflare-dns.com)
56	1.991978	10.1.37.200	162.159.61.3	TLSv1.2	1885	Client Hello (SNI=chrome.cloudflare-dns.com)
68	2.321066	10.1.37.200	162.159.61.3	TLSv1.2	1821	Client Hello (SNI=chrome.cloudflare-dns.com)
73	2.481069	10.1.37.200	172.64.41.3	TLSv1.2	1789	Client Hello (SNI=chrome.cloudflare-dns.com)
100	3.914508	10.1.37.200	172.64.41.3	TLSv1.2	1853	Client Hello (SNI=chrome.cloudflare-dns.com)
176	4.536002	10.1.37.200	74.125.130.101	QUIC	1292	Initial, DCID=51a2d36f314d8943, PKN: 2, CRYPTO, PING, CRYPTO, PADDING, CRYPTO, PING, CRYPTO...
225	4.751187	10.1.37.200	142.251.10.94	QUIC	1292	Initial, DCID=33c99a4fc47685f9, PKN: 2, CRYPTO, PADDING, CRYPTO, CRYPTO, PING, PING, PADDIN...
230	4.756907	10.1.37.200	64.233.170.113	QUIC	1292	Initial, DCID=a2a1a4ed80d14ba3, PKN: 2, CRYPTO, PING, CRYPTO, CRYPTO, PADDING, CRYPTO, PING, ...

> Frame 6: 1821 bytes on wire (14568 bits), 1821 bytes captured (14568 bits) on interface  
> Ethernet II, Src: d6:93:3e:ac:e2:03 (d6:93:3e:ac:e2:03), Dst: HuaweiTechno\_f6:d6:47 (a  
> Internet Protocol Version 4, Src: 10.1.37.200, Dst: 162.159.61.3  
> Transmission Control Protocol, Src Port: 54641, Dst Port: 443, Seq: 1, Ack: 1, Len: 17  
> Transport Layer Security

0000 a0 1c 8d f6 d6 47 d6 93 3e ac e2 03 00 00 45 00 .....G.....E  
0010 00 00 0a 85 40 00 80 06 00 00 0a 01 25 c8 a2 9f .....@.....%  
0020 3d 03 d5 71 01 bb 7e 47 1c 76 ff d9 50 16 50 18 .....q...V...P:P  
0030 01 00 0f 72 00 00 16 03 01 06 e2 01 00 06 de 03 .....T:4:h-1->  
0040 03 04 c5 54 c9 83 34 00 68 ec a3 6c 9f 10 3e f0 .....T:4:h-1->  
0050 f5 6a 52 49 8a 67 ed 15 1c 06 1c bb e4 3a 53 ec .....jRI g .....:S  
0060 d4 20 21 e9 a1 82 51 a5 f1 82 ed 1f ff e5 c2 c2 .....Q.....+/  
0070 12 a2 34 17 0d e5 46 19 fe 6a a2 e0 cd 98 83 93 .....4...F...j  
0080 11 98 00 20 fa 13 01 13 02 13 03 c0 2b c0 2f .....0.....+/  
0090 c0 2c c0 30 cc a9 cc a8 c0 13 c0 14 00 9c 00 9d .....0.....  
00a0 00 2f 00 35 01 00 06 75 9a 9a 00 00 ff 01 00 01 ...../5...u.....  
00b0 00 00 0b 00 02 01 00 00 00 0e 1e 0c 00 00 19 .....chrome.c loudflar  
00c0 63 68 72 6f 6d 65 2e 63 6c 6f 75 64 66 6c 61 72 .....e-dns.co m #  
00d0 65 2d 64 6e 73 2e 63 6f 6d 00 23 00 00 17 00 .....D.....h2.....  
00e0 00 44 cd 00 05 00 03 02 68 32 00 12 00 00 0a .....-22.....  
00f0 00 00 0a 7a 7a 11 6c 00 1d 00 17 00 18 00 05 .....+.....  
0100 00 05 01 00 00 00 00 2b 07 05 aa aa 03 04 .....+.....  
0110 03 03 00 10 00 0e 00 0c 02 68 32 08 68 74 74 70 .....h2 http

### 4. Which QUIC version is used in your trace?

No.	Time	Source	Destination	Protocol	Length	Info
2	0.035841	10.1.37.200	162.159.61.3	QUIC	1292	Initial, DCID=01c7d6435df7245a6c5334349f7027df4906a0c
9	0.340325	162.159.61.3	10.1.37.200	QUIC	1242	Handshake, SCID=01c7d6435df7245a6c5334349f7027df4906a0c
10	0.340325	162.159.61.3	10.1.37.200	QUIC	966	Handshake, SCID=01c7d6435df7245a6c5334349f7027df4906a0c
12	0.445062	10.1.37.200	172.64.41.3	QUIC	1292	Initial, DCID=016ee8d5b78f0db226c0dd5f88f2ba8f525ea4
13	0.938697	10.1.37.200	172.64.41.3	QUIC	1292	Initial, DCID=67a1a9888f29f59, PKN: 8, PING, PADDING, CRYPTO, PADDING, CRYPTO, PADDING, PI...
15	1.034537	10.1.37.200	172.64.41.3	QUIC	1292	Initial, DCID=c932945b5bf5fc1f, PKN: 1, PADDING, PING, PADDING, CRYPTO, CRYPTO, CRYPTO, CR...
16	1.034664	10.1.37.200	172.64.41.3	QUIC	1292	Initial, DCID=c932945b5bf5fc1f, PKN: 2, CRYPTO, PADDING, CRYPTO, CRYPTO, CRYPTO, PADDING, C...
18	1.191179	172.64.41.3	10.1.37.200	QUIC	1242	Initial, SCID=0133c16e5d941d7e9f30276e1294195530272536, PKN: 1, ACK, CRYPTO
22	1.202932	10.1.37.200	172.64.41.3	QUIC	1292	Initial, DCID=0133c16e5d941d7e9f30276e1294195530272536, PKN: 3, ACK, PADDING
26	1.348005	10.1.37.200	172.64.41.3	QUIC	1292	Initial, DCID=0133c16e5d941d7e9f30276e1294195530272536, PKN: 5, PADDING, PING, PADDING
31	1.395558	10.1.37.200	162.159.61.3	QUIC	1292	Initial, DCID=01c7d6435df7245a6c5334349f7027df4906a0c
33	1.569512	10.1.37.200	162.159.61.3	QUIC	1292	Initial, DCID=51ea003bdc17b07, PKN: 1, CRYPTO, CRYPTO, PING, CRYPTO, CRYPTO, CRYPTO, CRYPTO...
34	1.569640	10.1.37.200	162.159.61.3	QUIC	1292	Initial, DCID=51ea003bdc17b07, PKN: 2, CRYPTO, CRYPTO, PADDING, PING, PING, PING, PI...
37	1.783248	162.159.61.3	10.1.37.200	QUIC	966	Handshake, SCID=01a70b315e142bb6d439f0b0e1a821d0b1a56

> Frame 2: 1292 bytes on wire (10336 bits), 1292 bytes captured (10336 bits) on interface  
> Ethernet II, Src: d6:93:3e:ac:e2:03 (d6:93:3e:ac:e2:03), Dst: HuaweiTechno\_f6:d6:47 (a  
> Internet Protocol Version 4, Src: 10.1.37.200, Dst: 162.159.61.3  
> User Datagram Protocol, Src Port: 59086, Dst Port: 443  
✓ QUIC IETF  
> QUIC Connection Information  
[Packet Length: 1250]  
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)  
Destination Connection ID Length: 20

0000 a0 1c 8d f6 d6 47 d6 93 3e ac e2 03 00 00 45 00 .....G.....E  
0010 04 fe 0a 83 40 00 80 11 00 00 0a 01 25 c8 a2 9f .....@.....%  
0020 3d 03 e6 ce 01 bb 0a ea 14 67 c5 00 00 00 01 14 .....D .....  
0030 01 c7 d6 43 5d f7 24 5a e6 c5 33 43 49 f7 02 7d .....[C] S2 [C] I  
0040 fa 9a 6a 0c 00 00 44 c4 07 26 6a 9f 9a e0 a0 90 .....j D [C] I  
0050 03 03 00 10 00 0e 00 0c 07 51 0b 0a 37 e0 80 90 .....h2 http  
0060 b1 4f 64 08 31 ac 79 86 8f 00 0c 91 da 38 55 40 .....Od-1-y...-1-BUT  
0070 48 31 77 a3 9b 90 2b 52 63 59 51 d6 59 b0 65 18 .....Hlw...+R cVQ-Y-e  
0080 01 77 4a 99 04 94 31 de 01 fe a5 37 52 71 ec f3 .....wJ-1...-7Rq  
0090 73 2f 55 00 75 71 8e 4c 9e 50 4b 80 53 eb f7 57 .....3U-urL PK-S-m  
00a0 2e a0 1f 95 13 68 d4 c5 cf 89 ee aa f9 f3 2b 11 .....h.....  
00b0 aa 9a fe c3 99 a0 a1 9e d8 6b 98 6d b1 e8 ec df .....k:m.....  
00c0 35 8f c8 7b c0 09 dc 1a e1 09 a9 25 f0 5a 7f 92 .....S.....%2-  
00d0 6f 15 12 48 e0 29 c4 35 1b bb 63 7a 4c c5 08 46 .....p...}06...c-L-h  
00e0 aa c1 7f 35 c4 51 2d 63 aa e6 62 40 06 00 15 42 .....h-S-Q-c-b6...  
00f0 f7 03 a5 83 2a ba be 7d d7 8a f1 d3 00 aa f8 f2 .....k-i.....  
0100 29 6b ad 16 69 a4 a5 27 0f ee f8 de 06 ca 92 03 .....k-i.....  
0110 ba 5e de 2a 96 8b df 8f 00 22 50 5a 13 02 fd 3f .....h2 http

- Packet no: 2
- Quic version :1
- Found in the QUIC Long Header of the Initial packet. The client proposes this version during the handshake.

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

- 0-RTT: packet 1201
- 1-RTT: Packet 327
- This is the first packet encrypted with early (0-RTT) or final (1-RTT) keys, marking the transition from handshake to secure data exchange.

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

In **HTTP/3 (QUIC)**:

- No TCP handshake.
- TLS is built into QUIC.
- First application packet appears **immediately after 1-RTT keys** are established.

In **HTTP over TCP**:

- Must first complete **TCP handshake + TLS handshake** before sending any HTTP request.
- More round trips → slower startup compared to QUIC.