ASSIGNMENT # 01

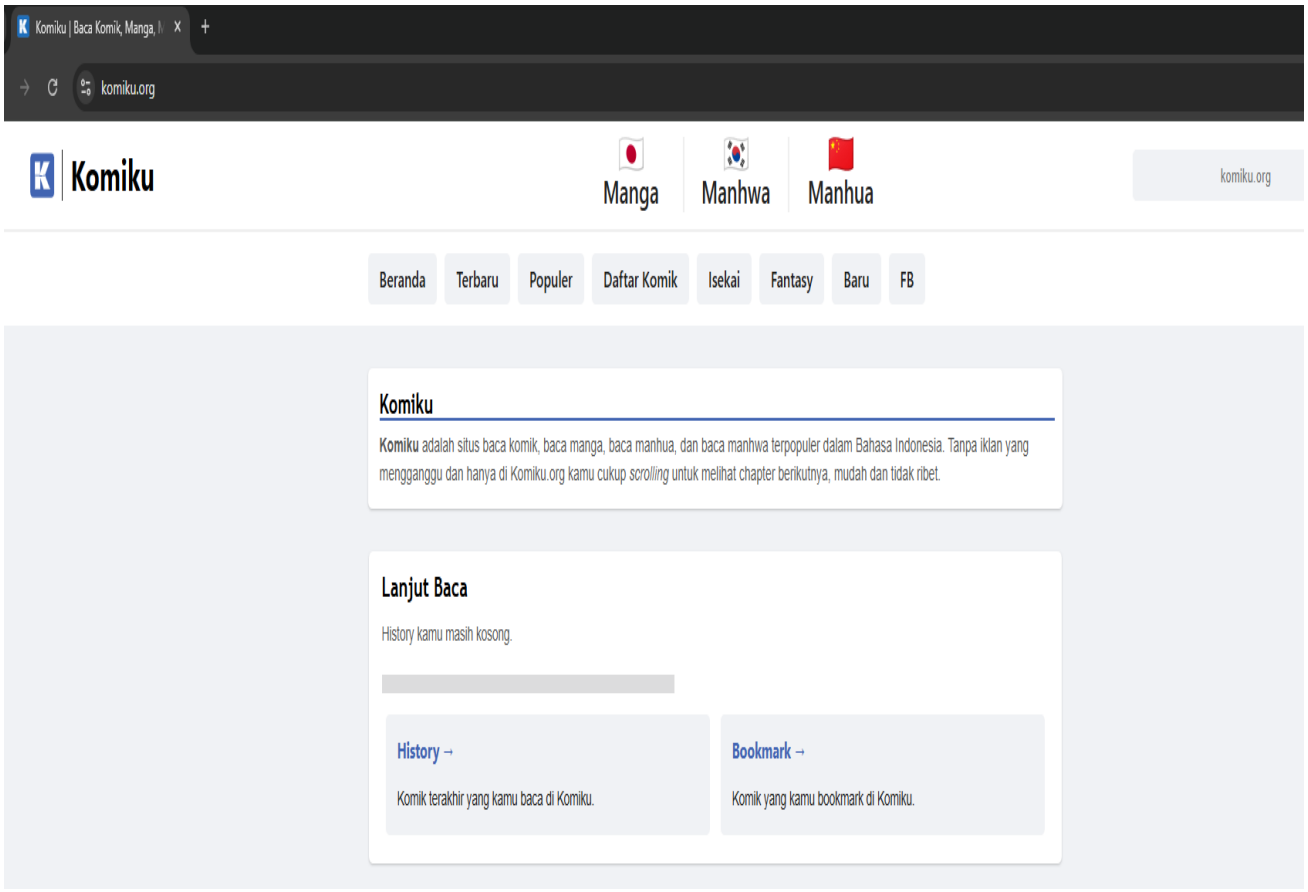
SUBMITTED BY	**Muhammad Azhan** **Omair Ahmad** **Sudais Aziz**
SUBMITTED TO	**Dr Adnan Iqbal**
REGISTRATION NO.	**B23F0001AI059** **B23F0001AI058** **B23F0344AI084**

TASK # 06:

For the QUIC based website access

1. What is the name of website?

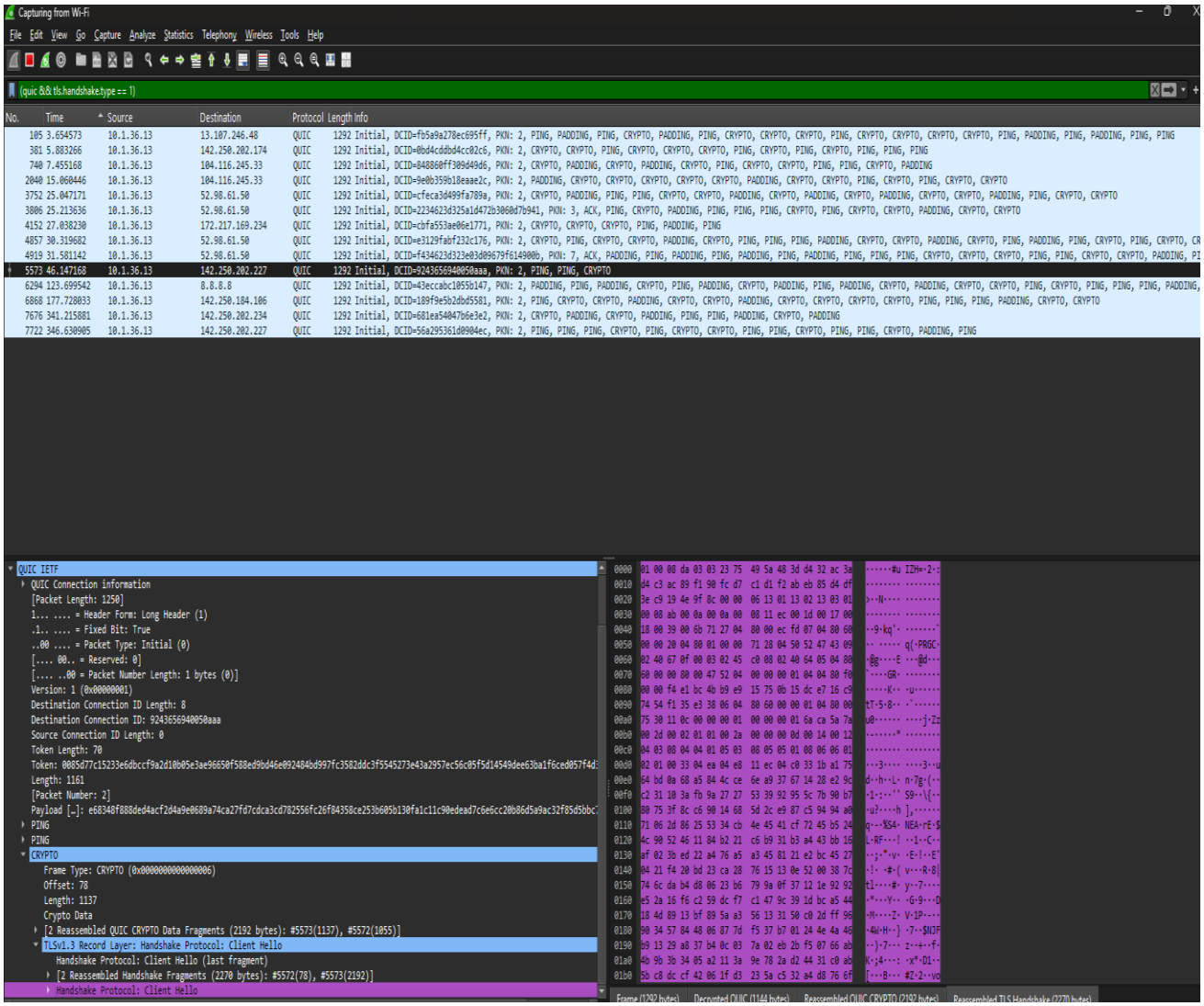
From the TLS ClientHello inside QUIC, the SNI (Server Name Indication) shows the website name I visited. In my trace, it is https://komiku.org/ .



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

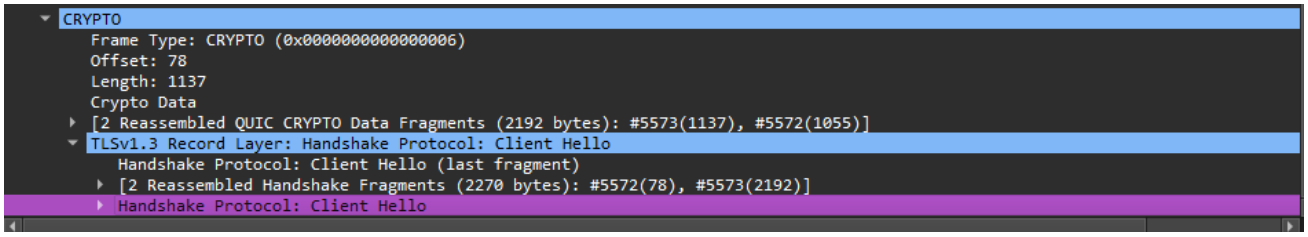
This packet exchanges important setup information:

- QUIC Version proposed by the client.
- Source and Destination Connection IDs (used to identify the connection).
- A CRYPTO frame carrying the TLS ClientHello, which contains supported TLS versions, cipher suites, and extensions.



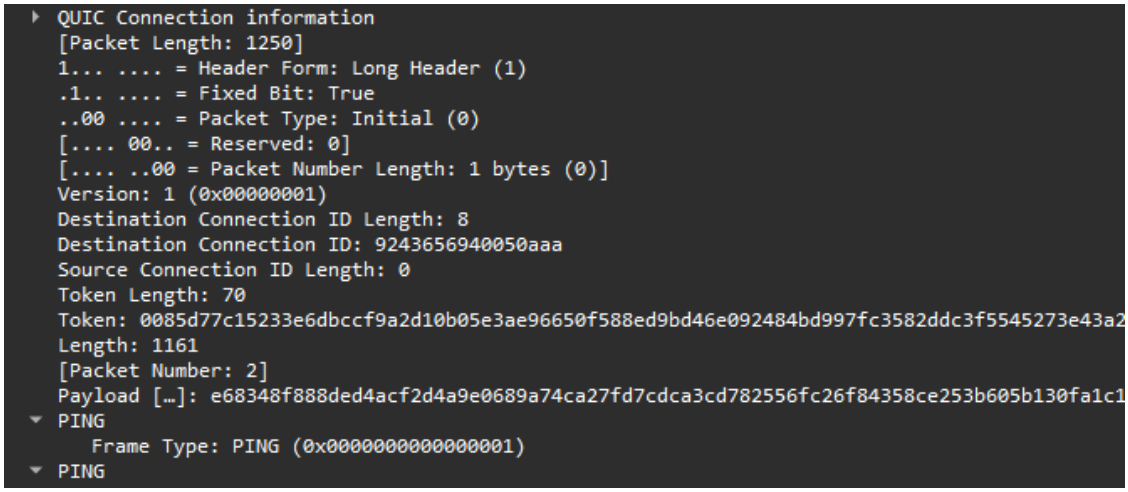
3. Identify the QUIC packet that contains the TLS ClientHello (QUIC embeds TLS handshake inside QUIC).

The TLS ClientHello itself is inside the **CRYPTO frame** of the Initial packet . This is where the client tells the server which TLS version it supports, what cipher suites it can use, and the target website name (SNI).



4. Which QUIC version is used in your trace?

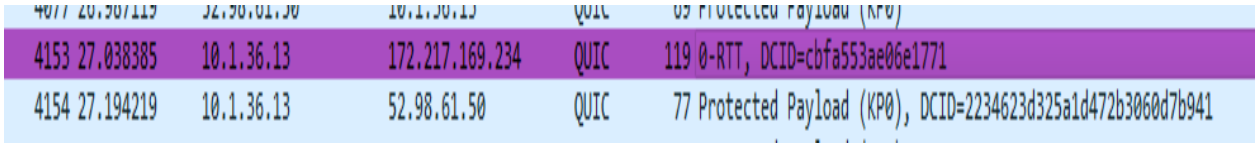
Version 1



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

After the Initial and Handshake packets, Wireshark shows the first protected packets.

- This indicates that the client and server have derived encryption keys, and from this point all QUIC traffic is protected.

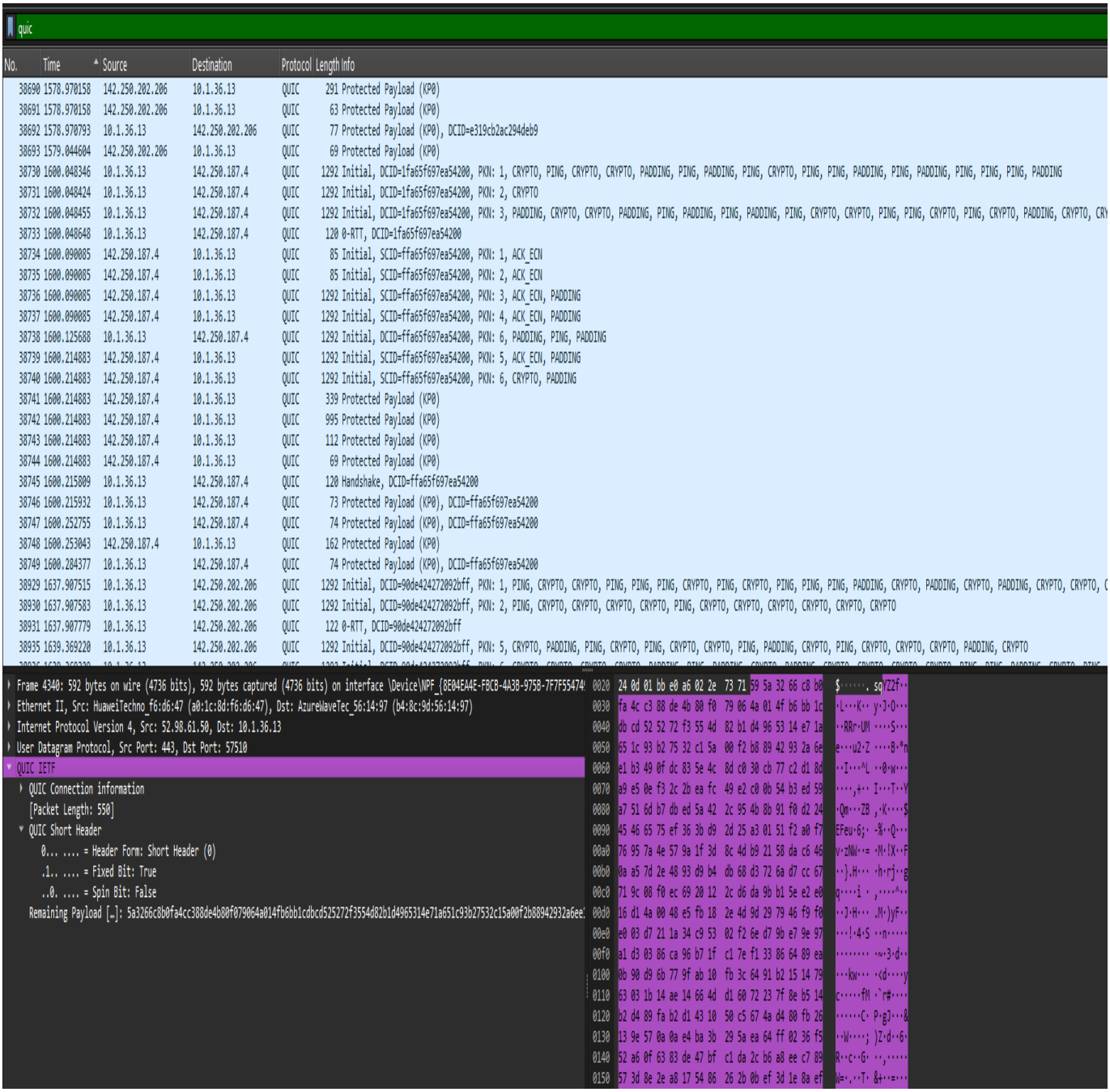


6. Find the first packet that carries application data (HTTP/3). How does this differ from HTTP over TCP?

This shows the actual web content being sent.

Difference from HTTP over TCP:

- HTTP/3 runs on QUIC over UDP, not on TCP.
- QUIC integrates the TLS handshake into the transport itself.
- It supports parallel streams without TCP's "head-of-line blocking."
- QUIC can also use 0-RTT to send data faster on repeated connections.


quic
No. Time Source Destination Protocol Length Info
38690 1578.970158 142.250.202.206 10.1.36.13 QUIC 291 Protected Payload (KP0)
38691 1578.970158 142.250.202.206 10.1.36.13 QUIC 63 Protected Payload (KP0)
38692 1578.970793 10.1.36.13 142.250.202.206 QUIC 77 Protected Payload (KP0), DCID=e319cb2ac294deb9
38693 1579.044604 142.250.202.206 10.1.36.13 QUIC 69 Protected Payload (KP0)
38730 1600.048346 10.1.36.13 142.250.187.4 QUIC 1292 Initial, DCID=1fa65f697ea54200, PKN: 1, CRYPTO, PING, CRYPTO, CRYPTO, PADDING, PING, PADDING, PING, CRYPTO, PING, PING, PADDING, PING, PADDING, PING, PING, PING, PADDING
38731 1600.048424 10.1.36.13 142.250.187.4 QUIC 1292 Initial, DCID=1fa65f697ea54200, PKN: 2, CRYPTO
38732 1600.048455 10.1.36.13 142.250.187.4 QUIC 1292 Initial, DCID=1fa65f697ea54200, PKN: 3, PADDING, CRYPTO, CRYPTO, PADDING, PING, PADDING, PING, PADDING, PING, CRYPTO, CRYPTO, PING, PING, CRYPTO, PING, CRYPTO, PADDING, CRYPTO, CRY
38733 1600.048648 10.1.36.13 142.250.187.4 QUIC 120 0-RTT, DCID=1fa65f697ea54200
38734 1600.090085 142.250.187.4 10.1.36.13 QUIC 85 Initial, SCID=ffa65f697ea54200, PKN: 1, ACK_ECN
38735 1600.090085 142.250.187.4 10.1.36.13 QUIC 85 Initial, SCID=ffa65f697ea54200, PKN: 2, ACK_ECN
38736 1600.090085 142.250.187.4 10.1.36.13 QUIC 1292 Initial, SCID=ffa65f697ea54200, PKN: 3, ACK_ECN, PADDING
38737 1600.090085 142.250.187.4 10.1.36.13 QUIC 1292 Initial, SCID=ffa65f697ea54200, PKN: 4, ACK_ECN, PADDING
38738 1600.125688 10.1.36.13 142.250.187.4 QUIC 1292 Initial, DCID=ffa65f697ea54200, PKN: 6, PADDING, PING, PADDING
38739 1600.214883 142.250.187.4 10.1.36.13 QUIC 1292 Initial, SCID=ffa65f697ea54200, PKN: 5, ACK_ECN, PADDING
38740 1600.214883 142.250.187.4 10.1.36.13 QUIC 1292 Initial, SCID=ffa65f697ea54200, PKN: 6, CRYPTO, PADDING
38741 1600.214883 142.250.187.4 10.1.36.13 QUIC 339 Protected Payload (KP0)
38742 1600.214883 142.250.187.4 10.1.36.13 QUIC 995 Protected Payload (KP0)
38743 1600.214883 142.250.187.4 10.1.36.13 QUIC 112 Protected Payload (KP0)
38744 1600.214883 142.250.187.4 10.1.36.13 QUIC 69 Protected Payload (KP0)
38745 1600.215809 10.1.36.13 142.250.187.4 QUIC 120 Handshake, DCID=ffa65f697ea54200
38746 1600.215932 10.1.36.13 142.250.187.4 QUIC 73 Protected Payload (KP0), DCID=ffa65f697ea54200
38747 1600.252755 10.1.36.13 142.250.187.4 QUIC 74 Protected Payload (KP0), DCID=ffa65f697ea54200
38748 1600.253043 142.250.187.4 10.1.36.13 QUIC 162 Protected Payload (KP0)
38749 1600.284377 10.1.36.13 142.250.187.4 QUIC 74 Protected Payload (KP0), DCID=ffa65f697ea54200
38929 1637.907515 10.1.36.13 142.250.202.206 QUIC 1292 Initial, DCID=90de424272092bff, PKN: 1, PING, CRYPTO, CRYPTO, PING, PING, PING, CRYPTO, PING, CRYPTO, PING, PING, PING, PADDING, CRYPTO, PADDING, CRYPTO, PADDING, CRYPTO, CRYPTO,
38930 1637.907583 10.1.36.13 142.250.202.206 QUIC 1292 Initial, DCID=90de424272092bff, PKN: 2, PING, CRYPTO, CRYPTO, CRYPTO, CRYPTO, PING, CRYPTO, CRYPTO, CRYPTO, CRYPTO, CRYPTO, CRYPTO
38931 1637.907779 10.1.36.13 142.250.202.206 QUIC 122 0-RTT, DCID=90de424272092bff
38935 1639.369220 10.1.36.13 142.250.202.206 QUIC 1292 Initial, DCID=90de424272092bff, PKN: 5, CRYPTO, PADDING, PING, CRYPTO, PING, CRYPTO, CRYPTO, PING, PADDING, CRYPTO, PING, CRYPTO, CRYPTO, CRYPTO, PADDING, CRYPTO
Frame 4340: 592 bytes on wire (4736 bits), 592 bytes captured (4736 bits) on interface \Device\NPF_{8E04EA4E-FBCB-4A38-975B-7F7F55474
Ethernet II, Src: HuaweiTechno_f6:d6:47 (a0:1c:8d:f6:d6:47), Dst: AzureWaveTec_56:14:97 (b4:8c:9d:56:14:97)
Internet Protocol Version 4, Src: 52.98.61.50, Dst: 10.1.36.13
User Datagram Protocol, Src Port: 443, Dst Port: 57510
QUIC IETF
QUIC Connection information
[Packet Length: 550]
QUIC Short Header
0... .... = Header Form: Short Header (0)
.1.. .... = Fixed Bit: True
..0. .... = Spin Bit: False
Remaining Payload […]: 5a3266c8b0fa4cc388de4b80f079064a014fb6bb1cdbcd525272f3554d82b1d4965314e71a651c93b27532c15a00f2b88942932a6ee
0020 24 0d 01 bb e0 a6 02 2e 73 71 59 5a 32 66 c8 b0
0030 fa 4c c3 88 de 4b 80 f0 79 06 4a 01 4f b6 bb 1c
0040 db cd 52 52 72 f3 55 4d 82 b1 d4 96 53 14 e7 1a
0050 65 1c 93 b2 75 32 c1 5a 00 f2 b8 89 42 93 2a 6e
0060 e1 b3 49 0f dc 83 5e 4c 8d c0 30 cb 77 c2 d1 8d
0070 a9 e5 0e f3 2c 2b ea fc 49 e2 c0 0b 54 b3 ed 59
0080 a7 51 6d b7 db ed 5a 42 2c 95 4b 8b 91 f0 d2 24
0090 45 46 65 75 ef 36 3b d9 2d 25 a3 01 51 f2 a0 f7
00a0 76 95 7a 4e 57 9a 1f 3d 8c 4d b9 21 58 da c6 46
00b0 0a a5 7d 2e 48 93 d9 b4 db 68 d3 72 6a d7 cc 67
00c0 71 9c 08 f0 ec 69 20 12 2c d6 da 9b b1 5e e2 e0
00d0 16 d1 4a 00 48 e5 fb 18 2e 4d 9d 29 79 46 f9 f0
00e0 e0 03 d7 21 1a 34 c9 53 02 f2 6e d7 9b e7 9e 97
00f0 a1 d3 03 86 ca 96 b7 1f c1 7e f1 33 86 64 89 ea
0100 0b 90 d9 6b 77 9f ab 10 fb 3c 64 91 b2 15 14 79
0110 63 03 1b 14 ae 14 66 4d d1 60 72 23 7f 8e b5 14
0120 b2 d4 89 fa b2 d1 43 10 50 c5 67 4a d4 80 fb 26
0130 13 9e 57 0a 0a e4 ba 3b 29 5a ea 64 ff 02 36 f5
0140 52 a6 0f 63 83 de 47 bf c1 da 2c b6 a8 ee c7 89
0150 57 3d 8e 2e a8 17 54 86 26 2b 0b ef 3d 1e 8a ef