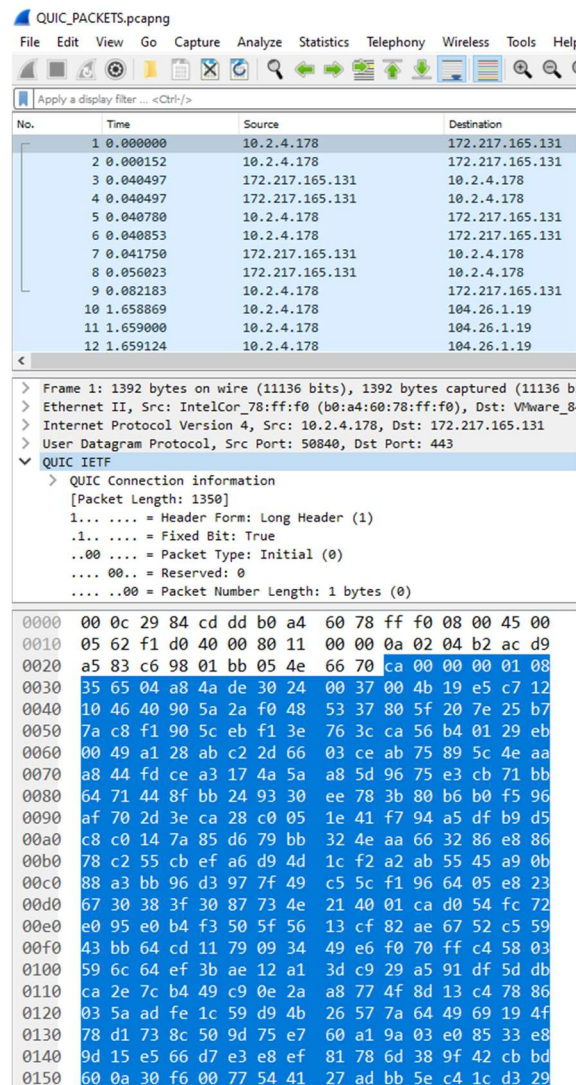


## QUIC Wireshark

The QUIC packets were captured via Wireshark when browsing the internet. Wireshark was activated upon opening a YouTube video and filtering the packets specifically for QUIC packets. A quick Wireshark test before opening YouTube was done to make sure my computer wasn't using an existing connection that involved QUIC before doing the packet capture on YouTube.

- On Wireshark, the QUIC packets were found using quic in the Wireshark filter.
- A sudden burst of QUIC packets were also received upon loading the YouTube comments section and other recommended videos were loaded.
- When bringing up YouTube's sidebar, an influx of QUIC packets were detected as well.
- The packet being read in this assignment will be the initial packet used to establish the first connection with YouTube.
- The packet capture was recording while the YouTube video was being played, so more packets were captured as the video kept playing and more sections of the video were buffered and loaded.



Packet Header captured (in Hexadecimal)	The type and meaning
0xca 00	<p>Converts to 11001010 in binary. (8-bit Header)</p> <p>Marks this packet to have the QUIC Long Header, uses fixed bits, that this is the initial packet type, that there are no reserved packets, and that this will be packet number 0.</p>
0x08	ID Length 8 (in Hexadecimal)
0x35 65 04 a8 4a de 30 24	<p>Converts to 0011 0101 0110 0101 0000 0100 1010 1000 0100 1010 1101 1110 0011 0000 0010 0100 in binary (Connection ID header)</p> <p>This is the 64-bit connection ID randomly chosen by the client. This is used to help create the initial packet being captured.</p>
0x00 00 00 01	<p>Converts to 0000 0000 000 0001 (16-bits) (Version header)</p> <p>Lists version 1 as a supported version to be used during negotiation. Uncertain why the Version header is 16-bits instead of 32-bits.</p>
0xce	<p>Converts to 1100 1110 in binary (Packet Number header)</p> <p>Identifies this packet as the first packet being used in the QUIC exchange.</p> <p>It is also 8-bits instead of the expected 32-bits.</p>
0x00 4b 19 e5 c7 12 10 46 40 90 5a 2a f0 48 53 37 80 5f 20 7e 25 b7 7a c8 f1 90 5c eb f1 3e 76 3c ca 56 b4 01 29 eb 00 49 a1 28 ab c2 2d 66 03 ce ab 75 89 5c 4e aa a8	Server Token being used to establish a 0-RTT connection

## Brandon Vo

Apply a display filter ... <Ctrl-/>	
:	
..00 .... = Packet Type: Initial (0)	
0060	00 49 a1 28 ab c2 2d 66 03 ce ab 75 89 5c 4e aa
0070	a8 44 fd ce a3 17 4a 5a a8 5d 96 75 e3 cb 71 bb
0080	64 71 44 8f bb 24 93 30 ee 78 3b 80 b6 b0 f5 96
0090	af 70 2d 3e ca 28 c0 05 1e 41 f7 94 a5 df b9 d5
00a0	c8 c0 14 7a 85 d6 79 bb 32 4e aa 66 32 86 e8 86
00b0	78 c2 55 cb ef a6 d9 4d 1c f2 a2 ab 55 45 a9 0b
00c0	88 a3 bb 96 d3 97 7f 49 c5 5c f1 96 64 05 e8 23
00d0	67 30 38 3f 30 87 73 4e 21 40 01 ca d0 54 fc 72
00e0	e0 95 e0 b4 f3 50 5f 56 13 cf 82 ae 67 52 c5 59
00f0	43 bb 64 cd 11 79 09 34 49 e6 f0 70 ff c4 58 03
0100	59 6c 64 ef 3b ae 12 a1 3d c9 29 a5 91 df 5d db
0110	ca 2e 7c b4 49 c9 0e 2a a8 77 4f 8d 13 c4 78 86
0120	03 5a ad fe 1c 59 d9 4b 26 57 7a 64 a9 69 19 4f
0130	78 d1 73 8c 50 9d 75 e7 60 a1 9a 03 e0 85 33 e8
0140	9d 15 e5 66 d7 e3 e8 ef 81 78 6d 38 9f 42 cb bd
0150	60 0a 30 f6 00 77 54 41 27 ad bb 5e c4 1c d3 29
0160	b1 89 cc ef 8d 47 b5 a6 7a 39 bb 04 6c 2b 9a e1
0170	2e ea 1e 1a 4e eb 2f 9f db 15 70 0b 4e b5 22 a6
0180	96 4d ff a8 46 9e 06 f0 aa 2f 5d 43 9a 08 82 d4
0190	82 35 99 11 ca a2 a0 59 0c c8 61 74 fe 65 fe d1
01a0	d6 e2 3a 32 ad da 81 ed fc 14 9a 55 2c 78 24 65
01b0	7c 40 dc fb ac 48 9c 86 06 84 e9 be 0b ff 8f 12
01c0	f8 dc 37 e9 51 23 d0 14 42 ee 91 5a d6 58 3b 0f
01d0	f3 10 c1 5c ce 4e fe ee d8 95 32 0b 8e 72 c7 00
01e0	fa fa 88 05 14 de 53 e7 d7 68 f5 f9 c4 d6 9a d6
01f0	da 03 4c 24 a7 ea b1 fb 88 df 3f 9c 40 62 8c 2d
0200	7d 60 41 f1 21 b6 d5 ae 3b 14 63 7f f7 4a 7c 82
0210	5e ce 0f d9 27 c9 b8 c1 3b e5 84 81 b9 90 82 ca
0220	c7 0a 9c be d0 86 ad 8f 43 6e 94 78 77 ac f1 2e
0230	a6 00 f1 60 21 ff f8 98 86 ca 74 a1 10 56 08 9b
0240	c1 7e a3 7f da 00 7c e2 89 be 09 cf 97 d8 1f 72
0250	86 ed ba 72 d7 05 9b ba fc 21 fb d6 b7 54 4f 1c
0260	47 e2 ef 60 b0 3d b8 b8 a3 a1 2c 74 fa 73 25 c9
0270	b7 7c 63 4d b6 b0 e5 30 02 43 f2 1c 88 80 e3 77
0280	70 ba 16 ee c3 ef e6 dd 4d 90 22 c1 ee 61 53 dc
0290	92 ef 2a 57 6c 15 5e bb 0f d7 7a 8b 88 0a 0c a4
02a0	61 45 ae 75 7b 4c 03 39 ae 3c 03 44 99 32 ab ad
02b0	6a 51 c3 79 c5 33 01 53 fc de b7 a8 eb fa 7d 96
02c0	55 2c 31 17 25 43 7e b1 7c 91 f2 b3 26 68 9f c1
02d0	17 45 94 4a 41 8c f1 77 bb 76 4d 19 b5 df b0 ec
02e0	dd 34 3c 17 36 ff d8 67 b6 10 37 27 2f 41 39 28
02f0	0e 20 70 b1 77 6e 4e 6b d6 27 ec 16 71 92 76 21

..00 .... = Packet Type: Initial (0)	
d0	17 45 94 4a 41 8c f1 77 bb 76 4d 19 b5 df b0 ec
e0	dd 34 3c 17 36 ff d8 67 b6 10 37 27 2f 41 39 28
f0	0e 20 70 b1 77 6e 4e 6b d6 27 ec 16 71 92 76 21
00	07 18 1f 4c c4 cc 21 62 59 3d 76 4b 50 0a b6 30
10	08 d5 51 0b 0d 82 88 ab fb 8f f7 b8 bf 59 63 52
20	f4 f8 82 85 f8 19 a0 59 d9 b1 97 c9 09 a9 5f dc
30	ee 07 1d d9 61 1c 18 d5 f9 9a 99 97 44 aa 07 cb
40	3d d3 33 e9 88 1a 3f 6f 59 54 ba fb 6a cc f8 00
50	29 e6 f2 de 1a a2 48 11 68 c6 64 0b de 8f 3c d0
60	85 b3 e3 b6 ff 17 26 21 b1 84 de 2b 38 38 36 87
70	88 63 f9 de 6d d9 d3 4d 17 0e 4f b7 8d 54 7d 1a
80	bc 23 5a 3c 9c 0f b7 89 84 1a 13 42 6b 1a 51 20
90	3f 02 36 39 2b 4c 7b 89 ab 94 8b 8f 2a 27 de 27
ao	23 9d 45 d1 62 68 60 ff 7b 83 ad 85 28 23 05 a3
b0	6f 52 94 ea bd 08 f4 1a 2f 9d c6 d1 81 42 34 c0
c0	1d 10 31 05 4c 70 eb 05 64 09 94 69 65 0c 37 fb
d0	40 9b 6a 81 9c be e2 ad 59 62 95 e8 44 86 fe 26
e0	1a 80 24 f2 ba 40 5c f5 32 5c 01 13 c2 6d 93 a6
f0	75 c7 6d 0f b7 3a 79 b3 92 a7 31 7e 5d 18 36 e5
00	88 eb 7f ad bd 7f 3f 38 e6 49 99 22 40 ee e9 f9
10	64 62 3c 5b c9 e8 44 44 24 f6 95 1a ab 60 6b ab
20	10 1d 0b dc 69 53 26 0f 68 40 c4 3e c0 8d fc e7
30	36 4f 6d 4b 94 fe 7f 58 63 05 d7 39 ee 35 73 37
40	50 02 7a f1 2c 48 37 76 44 49 ae 7d 42 43 e1 8f
50	05 4d 53 65 18 63 f1 ec 6b 88 14 ac 65 59 33 b7
60	b6 7e 8e e7 f6 77 b5 c0 93 99 9b 3b ce 4a d8 ee
70	b7 66 4f be b8 07 22 d5 1b 26 00 91 6f b6 f8 e5
80	40 45 07 dc c1 36 47 66 76 e5 b3 cf 6e 45 a1 3e
90	15 ef 1f ad ce 21 56 85 13 6c 88 ff 6e a1 1f 20
ao	f5 fb c0 0e 45 d9 14 fd c8 4a f0 f1 91 81 0a ae
b0	8f cb 45 aa 08 17 83 20 e2 c4 bd 72 06 82 5e e4
c0	d8 db b1 fe d3 ac 28 98 98 6f 75 ab 3d 6a 5b 9c
d0	e0 b7 3b 51 bf 73 06 6e 07 6b 2a 93 e8 8a 18 53
e0	c3 14 d5 97 7f ce 43 54 50 84 65 3e 2a 1f 1a 95
f0	08 c9 4b ab 0f 93 6c 09 07 f2 f6 49 39 ac 6c 03
00	c5 a5 a9 6f 6c 01 69 84 5d 8c 87 87 fc 35 0d 46
10	5c f2 12 ba 3d 59 b5 ac 27 43 b9 dd 59 9c ff e2
20	f4 80 dd 4a 53 76 fe 4c c8 31 3f 22 66 93 ea 21
30	b3 e8 10 9d 96 53 95 80 fd 40 6f 0b 8d ba 1f fc
40	64 0f 38 e7 47 99 db 0d dd 89 ad b7 b0 7b d7 48
50	3f 02 02 80 f3 ee 25 29 99 6b 8d d9 fd cf 06 a3
60	fa 53 f0 cb c9 f2 30 54 16 5d e7 7e b7 ca 49 fc

The rest is just the QUIC protected payload which was too large to include in the description table. It sends the payload through TLSv1.3 while sending a series of Frames. The Frames found in the initial exchange are PADDING and PING using 0x00 and 0x01 respectively.

Apply a display filter ... <Ctrl-/>				
No.	Time	Source	Destination	Protocol
1	0.000000	10.2.4.178	172.217.165.131	QUIC
2	0.000152	10.2.4.178	172.217.165.131	QUIC
Destination Connection ID: 356504a84ade3024 Source Connection ID Length: 0 Token Length: 55 Token: 004b19e5c712104640905a2af0485337805f207e25b77ac8f1905cebf13e763cca56b401... Length: 1277 Packet Number: 1 Payload: a3174a5aa85d9675e3cb71bb6471448fbb249330ee783b80b6b0f596af702d3eca28c005...				
> TLSv1.3 Record Layer: Handshake Protocol: Server Hello (fragment) > TLSv1.3 Record Layer: Handshake Protocol: Multiple Handshake Messages > PADDING Length: 138 > TLSv1.3 Record Layer: Handshake Protocol: Multiple Handshake Messages > PADDING Length: 208 > TLSv1.3 Record Layer: Handshake Protocol: Multiple Handshake Messages > TLSv1.3 Record Layer: Handshake Protocol: Multiple Handshake Messages > PING > PING > PADDING Length: 206 > TLSv1.3 Record Layer: Handshake Protocol: Multiple Handshake Messages > TLSv1.3 Record Layer: Handshake Protocol: Multiple Handshake Messages > TLSv1.3 Record Layer: Handshake Protocol: Multiple Handshake Messages > PADDING Length: 10 > TLSv1.3 Record Layer: Handshake Protocol: Multiple Handshake Messages ✓ TLSv1.3 Record Layer: Handshake Protocol: Multiple Handshake Messages Frame Type: CRYPTO (0x0000000000000006) Offset: 57 Length: 5 Crypto Data Handshake Protocol: Server Hello (fragment) ✓ TLSv1.3 Record Layer: Handshake Protocol: Multiple Handshake Messages Frame Type: CRYPTO (0x0000000000000006) Offset: 0 Length: 1 Crypto Data Handshake Protocol: Server Hello (fragment) ✓ PING Frame Type: PING (0x0000000000000001)				
3220	3d ac 92 aa	00 00 00 00	00 00 00 00	00 00 00 00
3230	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
3240	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
3250	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
3260	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
3270	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
3280	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
3290	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
32a0	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
32b0	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
32c0	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
32d0	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
32e0	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00



The packet below was recorded while the YouTube video from before continued playing. After the initial QUIC packet was exchanged between my computer and the server, my computer transitioned to using QUIC short header packets for a more light-weight exchange. The packet shown below is a QUIC packet using the Short Header.

Data captured (Hexadecimal)	Header meaning
0x4b	0100 1011 (8-bit Header)  Identifies that this packet will be using the short header since we've already established a connection.  Also labels this as packet number 4
<b>No Connection ID Present</b>	
The rest of the data is just the protected payload contained in the short frames. Unlike the long header, there is no Connection ID or version number found in QUIC's short header.	

QUIC\_PACKETS.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-F>

No.	Time	Source	Destination
1	0.000000	10.2.4.178	172.217.165.131
2	0.000152	10.2.4.178	172.217.165.131
3	0.040497	172.217.165.131	10.2.4.178
4	0.040497	172.217.165.131	10.2.4.178
5	0.040780	10.2.4.178	172.217.165.131
6	0.040853	10.2.4.178	172.217.165.131
7	0.041750	172.217.165.131	10.2.4.178
8	0.056023	172.217.165.131	10.2.4.178
9	0.082183	10.2.4.178	172.217.165.131
10	1.658869	10.2.4.178	104.26.1.19

< Frame 4: 664 bytes on wire (5312 bits), 664 bytes captured (5312 bits) on interface 0  
 > Ethernet II, Src: VMware\_S4:cd:dd (00:0c:29:84:cd:dd), Dst: IntelCor\_78:ff:ff  
 > Internet Protocol Version 4, Src: 172.217.165.131, Dst: 10.2.4.178  
 > User Datagram Protocol, Src Port: 443, Dst Port: 50840

▼ QUIC IETF

- ▼ QUIC Connection information
  - [Connection Number: 0]
  - [Packet Length: 622]
- ▼ QUIC Short Header
  - 0... .. = Header Form: Short Header (0)
  - ... .. = Fixed Bit: True
  - ..0. .... = Spin Bit: False

Remaining Payload: e4a7babf39031da49ffa4280650fb2efe3b4a2b9376345155b2f

```

0020 04 b2 01 bh c6 98 02 76 0f a7 dh e4 a7 ha hf 30
0030 03 1d a4 9f fa d2 80 65 0f b2 ef e3 ha a2 b9 37
0040 53 d5 15 5b 2f 04 6e bd 78 bf 16 ef 53 00 6e e2
0050 cc 27 11 1e e0 0e 80 50 14 eb 35 e8 df 38 e7 dc
0060 f1 12 22 18 5b 93 ee f9 7a 2e 30 2f 35 3c 34 20
0070 8e 94 h6 d1 37 47 c5 a1 9f a9 6b 6f 34 37 8f e6
0080 ac 6c af d1 d4 74 06 8e a7 32 hd 52 79 17 79 9a
0090 20 fd 85 66 20 3f cd 64 56 f9 d2 cf ac ea 91 67
00a0 a9 d6 86 93 76 f5 46 5c 26 65 d3 31 16 7c h1 92
00b0 h1 27 e6 1c e2 a1 19 63 82 e5 63 f9 c2 4e 71 95
00c0 1d 05 2a 91 8c 09 fa e8 75 48 38 1e 19 f1 98 e3
00d0 3d cd df 21 07 ae 10 49 58 df c8 b6 9e 88 44 1d
00e0 2f 91 fb 02 h1 98 84 31 1f 5e ab 2c 4f 70 3f d0
00f0 2d 21 83 ec ac d1 75 d1 90 92 e8 b9 96 02 17 bf
0100 a1 10 f6 c8 77 e3 c6 fa 7b cc 2e 5a 19 a5 27 e4
0110 5d 7f cc b8 27 44 90 09 8e cb 8a e4 41 f3 6d 79
0120 52 96 4a c3 ac cd 9e 0c 3d dd 2d 34 a2 9a 03 67
0130 eh 6a 80 1h c5 5d 23 h3 87 45 7f 3d 73 96 h2 38
0140 94 13 ch f5 6c 06 2a 2e 71 f1 56 ab 3d 65 af 1f
0150 f3 19 53 15 f2 37 99 0d 55 ha f6 7f 8b 05 d1 60
0160 64 f5 ab 15 96 36 f0 2h c4 c3 c9 e4 9b 07 5c 04
0170 8f 29 ca 02 c2 87 96 dd e4 48 de a7 45 d2 85 d6
0180 3f 83 c4 c6 64 52 6f d5 6e d8 38 09 c5 00 72 a6
0190 50 59 e4 02 0d d6 e0 98 32 9b 69 8a 95 5a 8e 76
01a0 3c ce 05 4c 8c c0 a6 15 9e h0 c1 12 ee 24 fe 67
01b0 ea 53 e2 fa c9 5a f9 6f 21 c6 e0 e9 95 06 9a 96
01c0 25 68 2e h7 0d 05 77 88 29 f4 a3 22 0b 26 h5 2h
01d0 e0 e4 f6 04 76 9d 69 db c6 94 2e aa 14 b0 63 a7
  
```