FORMAL SPECIFICATION AND TESTING OF QUIC

Name : Raghav Gade
Roll no. : 20CS02003
Supervisor : Dr. Srinivas Pinisetty
School of Electrical and Computer Sciences

MOTIVATION

TCP & EVOLUTION

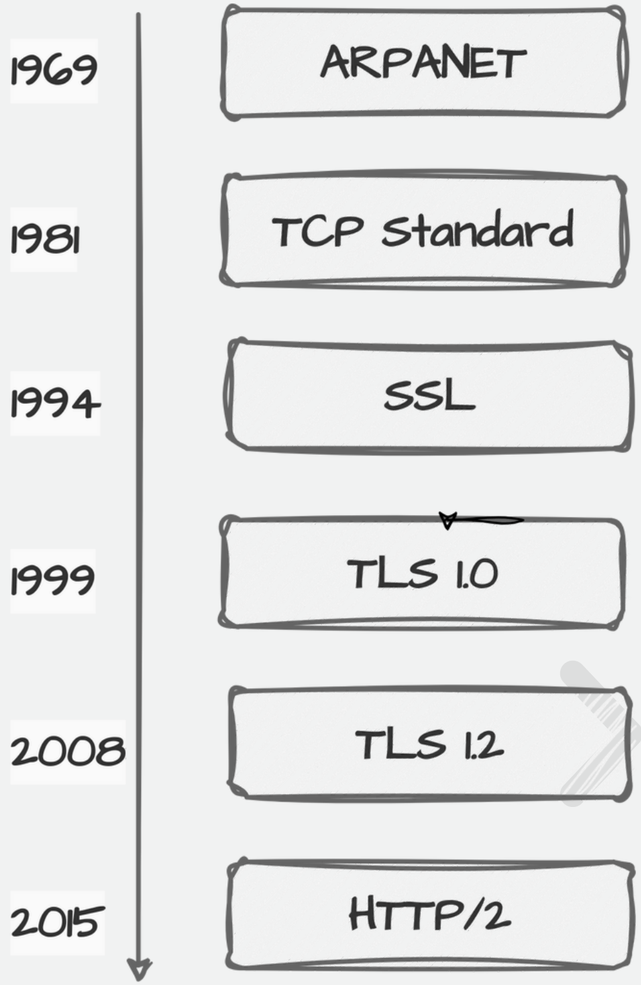
TCP/IP suite has been running the internet since TCP was standardized as RFC 761 in 1980. TCP evolution is slow due to kernel integration requiring widespread OS updates.

WHY QUIC?

QUIC is a new transport protocol that aims to be widely used over the Internet.
It will serve as a basis to HTTP/3.

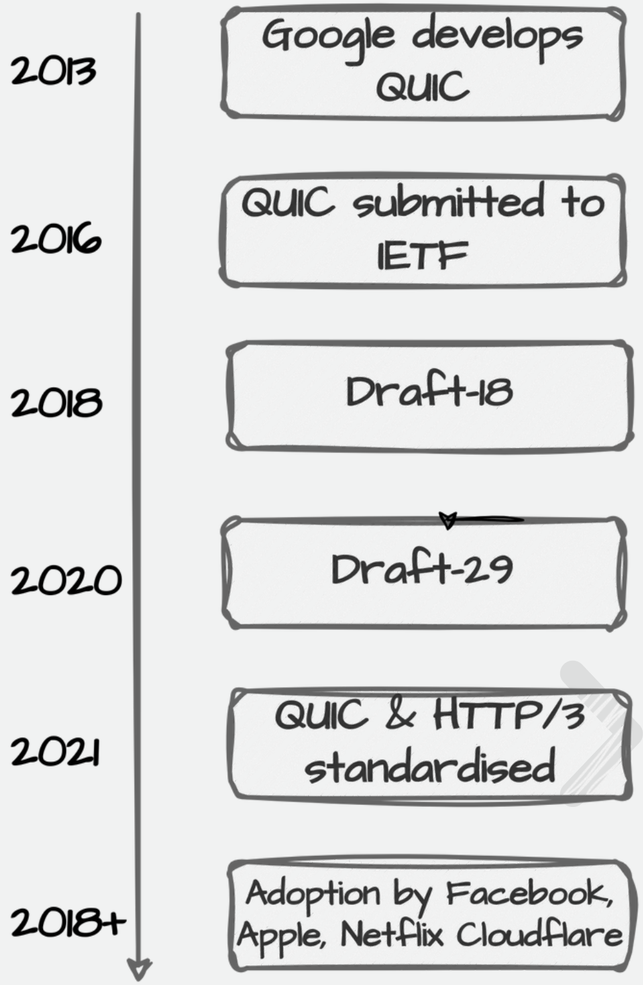
TCP+TLS+HTTP/2 STACK

- TCP provides connection-oriented, ordered communication with guaranteed delivery, retransmissions, and error correction.
- TLS encrypts data transmitted over TCP, ensuring confidentiality, integrity, and authentication.
- HTTP/2 runs over TLS and optimizes web performance by multiplexing multiple streams over a single connection.



QUIC+UDP+HTTP/3 STACK

- QUIC was designed to combine the speed of UDP with the reliability and security features typically associated with TCP, along with the encryption capabilities of TLS-1.3.
- It runs on top of UDP.
- UDP is just IP with ports.
- HTTP/3 runs over QUIC and improves upon HTTP/2 by removing reliance on TCP.



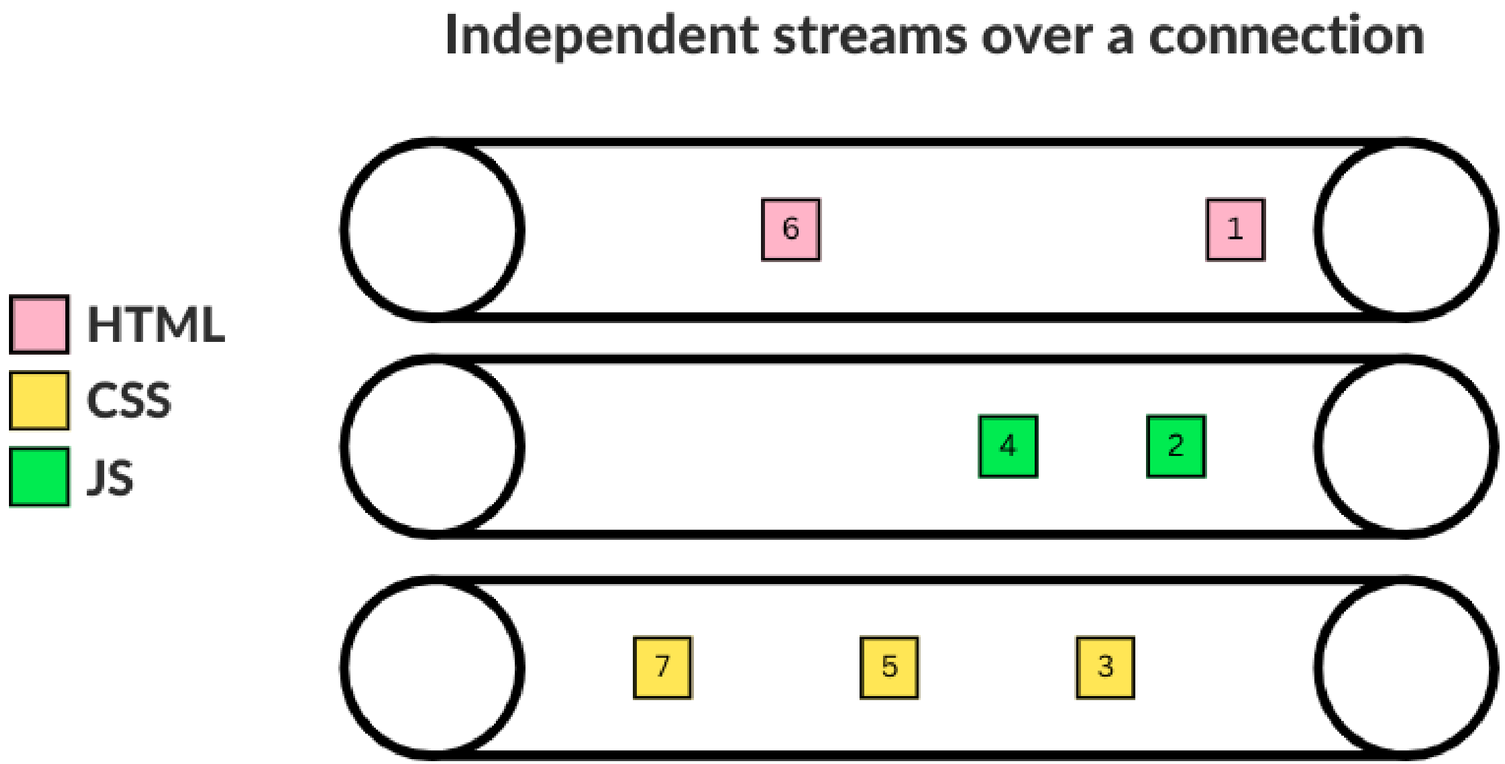
TCP HEAD OF LINE BLOCKING

HTML
CSS
JS

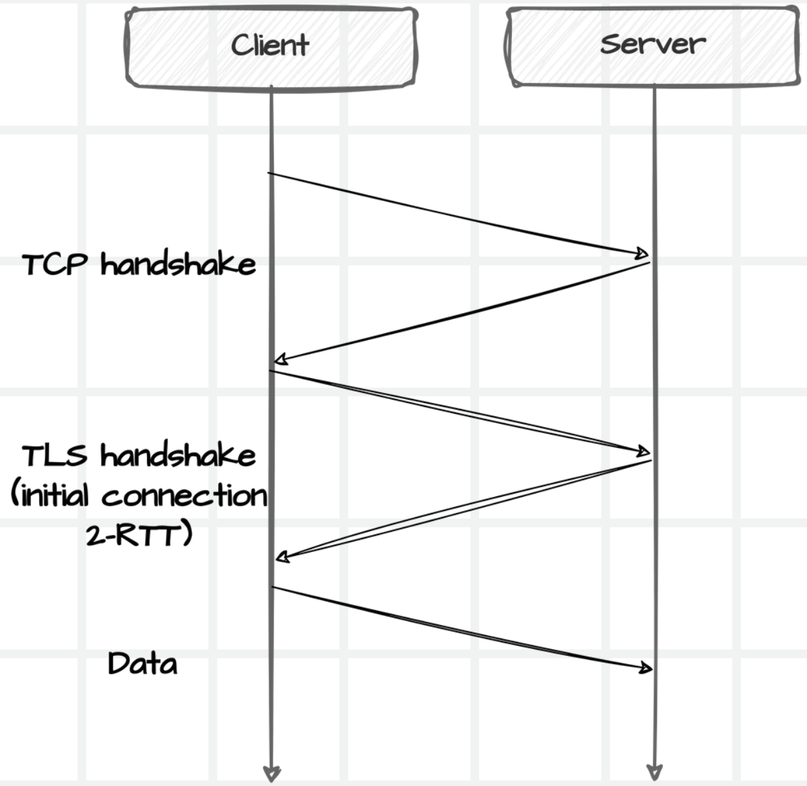
4 to be retransmitted again

3 Dropped

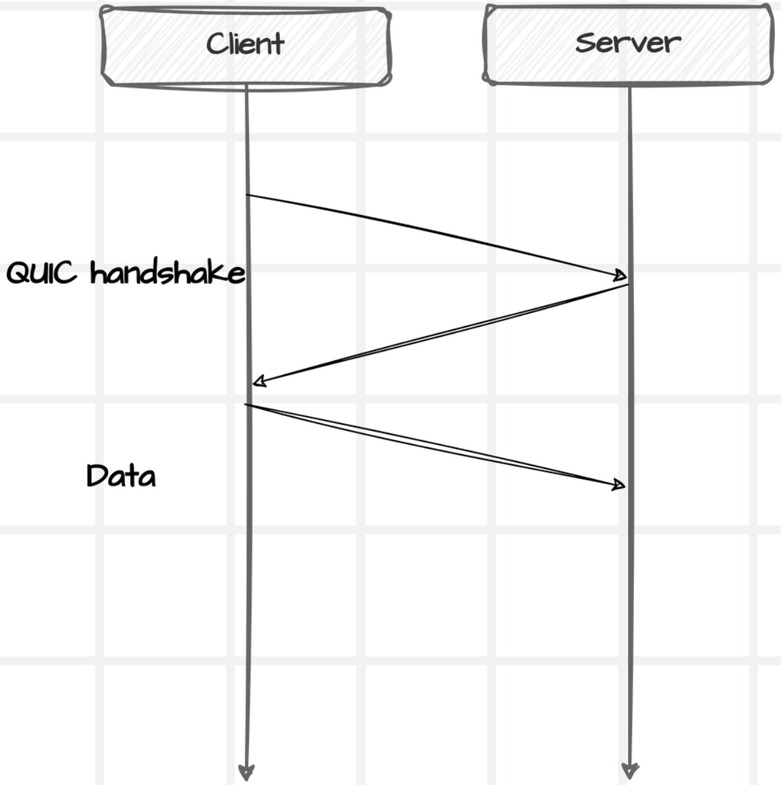
QUIC SOLUTION TO HOL



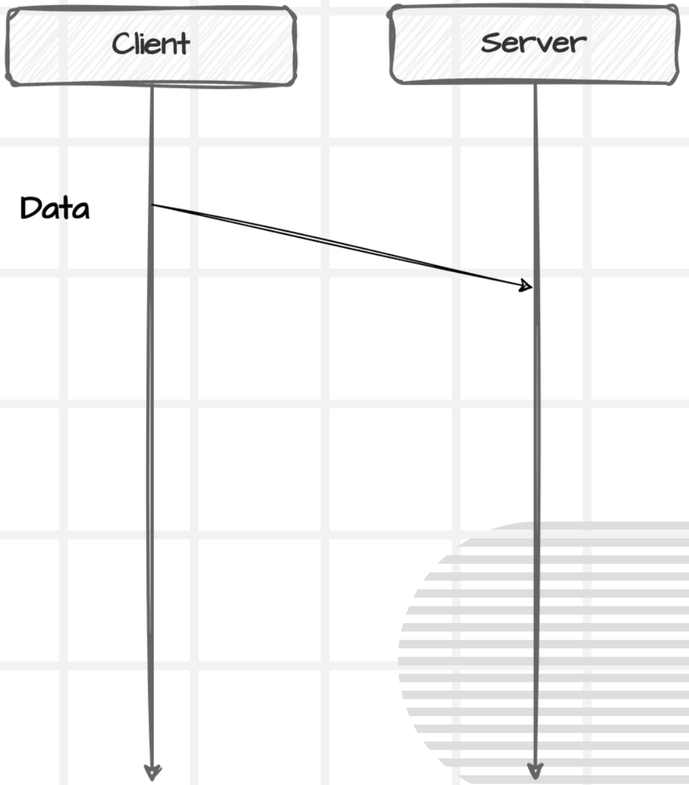
RTT COMPARISON



TCP + TLS 1.2
2 RTT

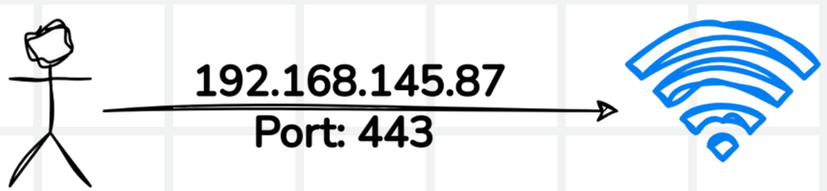


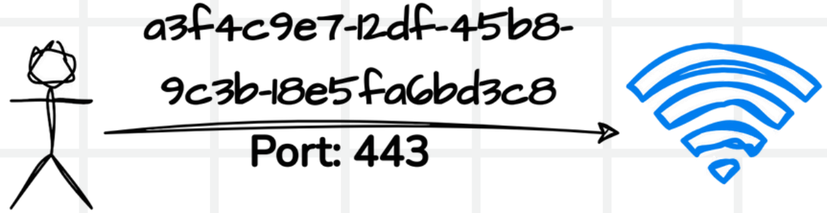
QUIC with TLS 1.3
1 RTT

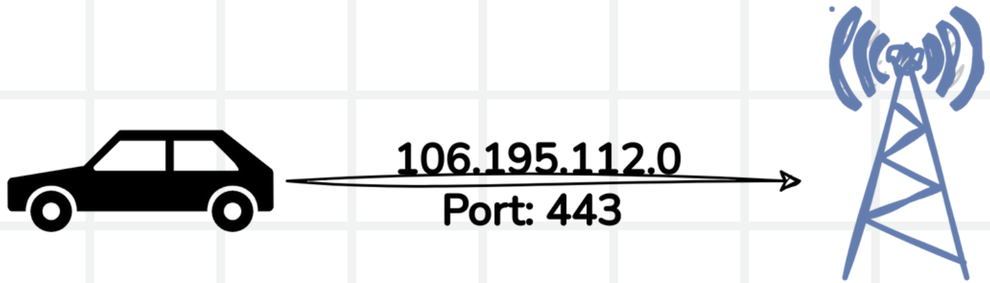


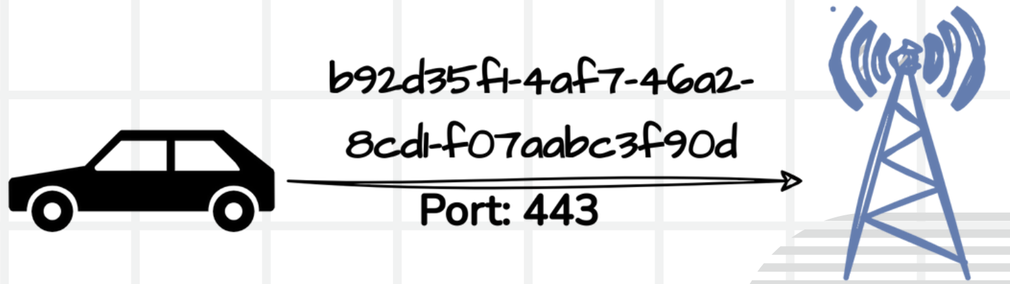
QUIC with TLS 1.3
0 RTT

CONNECTION MIGRATION









QUIC uses connection ID (20 bytes) and UDP allows the client to change its source address without breaking the session while TCP needs to form new.

OTHER FEATURES

- TCP has been integrated into kernel-space since its early implementation in operating systems in the 1980s.
- Updating TCP in kernel space requires OS updates and kernel recompilation, making protocol evolution slow.

- QUIC is implemented in user-space which helps developers to push frequent updates with new features and optimizations without having to wait for kernal updates.
- Therefore, there exist several implementations of QUIC based on one's use case and needs.

PROBLEM STATEMENT

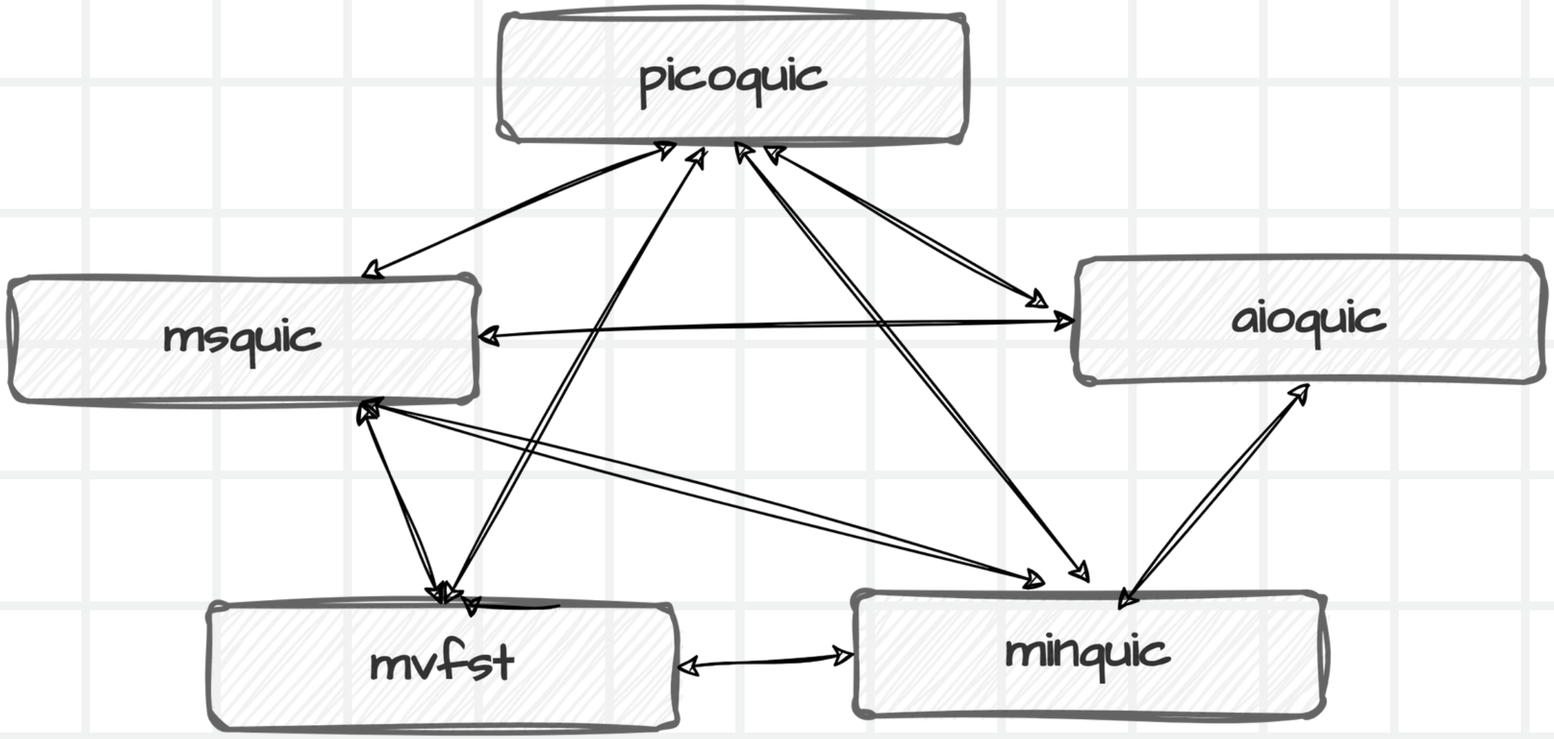
WHY DO WE NEED FORMAL SPECIFICATION?

Isn’t checking interoperability of QUIC implementations enough.

WHAT KIND OF TESTING IS REQUIRED?

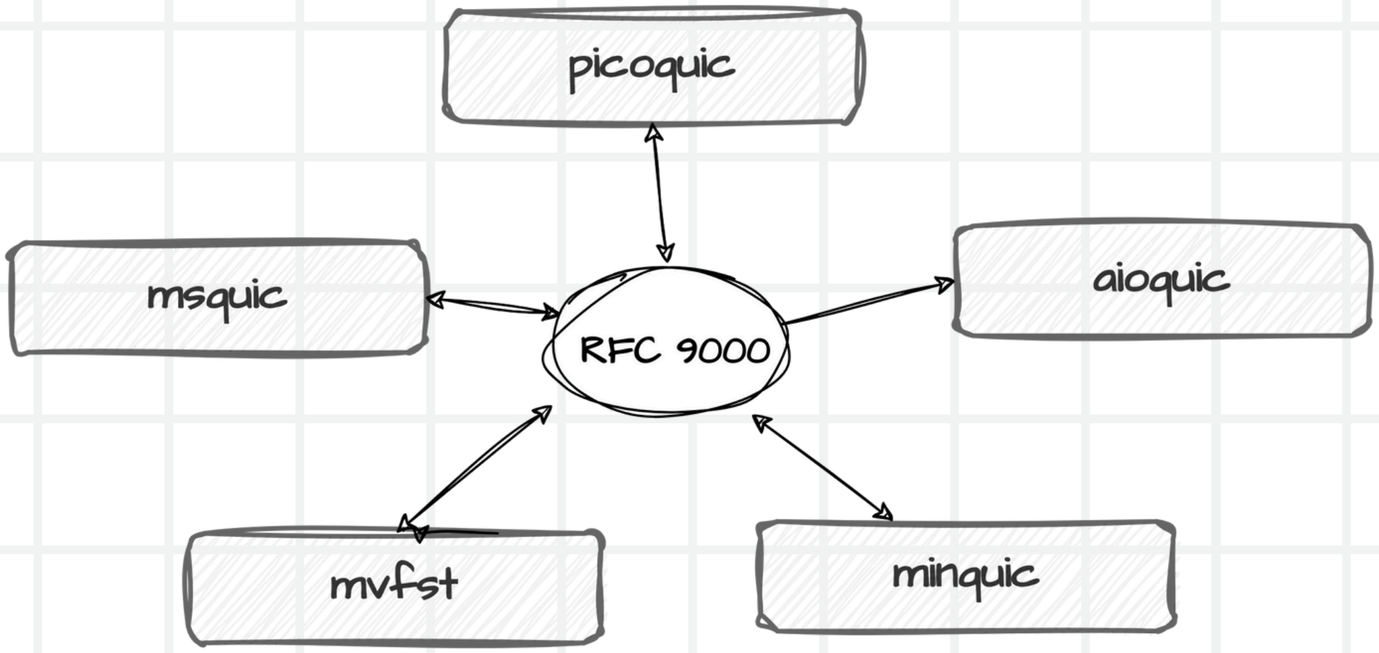
Isn’t checking performance across different conditions with parameters like with parameters like throughput, latency, percentage of packet loss enough.

INTEROPERABILITY



Test QUIC traffic through different network setups with middleboxes, such as corporate firewalls, home routers, mobile networks across different implementations to check compatibility and performance

FORMAL VERIFICATION



- List all properties that can be verified from RFC 9000.
- A network protocol is a high-level abstraction that includes many components: the server, the receivers, the network, etc. To test formally QUIC, split the whole system in several components and see if each of them behaves correctly.
- Needs a checker to see if all the actions are legal.
- Create randomized tests to verify the abstract model and see if implementation conforms to RFC.

LITERATURE SURVERY

TAKING A LONG LOOK AT QUIC (2017)

by M. Kakhki, S. Jero

Performance evaluation and discusses performance comparisons between TCP and QUIC.

FORMAL SPECIFICATION AND TESTING OF QUIC (2019)

by K. L. McMillan and L. D. Zuck,
Verification of QUIC -draft 18 was done by using a
methodology called "Network-centric Compositional testing" using IVy.

VERIFYING QUIC IMPLEMENTATIONS USING IVY(2021)

by C. Crochet, T. Rousseaux

Extension to McMillan’s work by using to same methodology to produce formal model for draft-29 of QUIC

FORMAL ANALYSIS OF QUIC HANDSHAKE PROTOCOL USING SYMBOLIC MODEL CHECKING (2021)

by J. Zhang, X. Gao,

Security analysis of the QUIC handshake protocol based on symbolic model checking using ProVerif and Verifpal

METHODOLOGY

TESTING IMPLEMENTATIONS OF QUIC

Implementation	Language	Description
picoquic + picotls	C	Minimal implementation of QUIC aligned with IETF specifications. One of the best performers in interoperability testing. Needs picotls for encryption.
minquic + mint	go	Minq is a minimal implementation of QUIC which partly implements QUIC draft-05 with TLS 1.3 draft-20 or draft-21.
aioquic	Python	Library featuring an I/O-free API suitable for embedding in both clients and servers.

Given implementations are chosen as they were supposed to work with Ivy Model as mentioned in the paper.

AIOQUIC+PICOQUIC+MINQUIC TERMINAL OUTPUTS

```
❯ python examples/http3_server.py --certificate tests/ssl_cert.pem --private-key tests/ssl_key.pem
2024-11-29 00:27:24,669 INFO quic [5c8549c3e18d0235] Negotiated protocol version 0x00000001 (VERSION_1)
2024-11-29 00:27:24,674 INFO quic [5c8549c3e18d0235] ALPN negotiated protocol hq-interop
2024-11-29 00:27:24,675 INFO quic [5c8549c3e18d0235] HTTP request GET /
2024-11-29 00:27:24,678 INFO quic [5c8549c3e18d0235] Connection close received (code 0x100, reason )
2024-11-29 00:27:33,778 INFO quic [0dfae2e5fb7fc4c7] Negotiated protocol version 0x00000001 (VERSION_1)
2024-11-29 00:27:33,783 INFO quic [0dfae2e5fb7fc4c7] ALPN negotiated protocol h3
2024-11-29 00:27:33,784 INFO quic [0dfae2e5fb7fc4c7] HTTP request GET /
2024-11-29 00:27:33,784 INFO quic [0dfae2e5fb7fc4c7] HTTP request GET /style.css
2024-11-29 00:27:33,787 INFO quic [0dfae2e5fb7fc4c7] Connection close received (code 0x100, reason )
```

```
❯ source aioquic-env/bin/activate
❯ python examples/http3_client.py --ca-certs tests/pycacert.pem --legacy-http https://localhost:4433/
2024-11-29 00:27:24,672 INFO quic [5c8549c3e18d0235] Negotiated protocol version 0x00000001 (VERSION_1)
2024-11-29 00:27:24,674 INFO quic [5c8549c3e18d0235] ALPN negotiated protocol hq-interop
2024-11-29 00:27:24,674 INFO client New session ticket received
2024-11-29 00:27:24,678 INFO client Response received for GET / : 1106 bytes in 0.0 s (2.693 Mbps)
2024-11-29 00:27:24,678 INFO quic [5c8549c3e18d0235] Connection close sent (code 0x100, reason )
❯ python examples/http3_client.py --ca-certs tests/pycacert.pem https://localhost:4433/
2024-11-29 00:27:33,781 INFO quic [0dfae2e5fb7fc4c7] Negotiated protocol version 0x00000001 (VERSION_1)
2024-11-29 00:27:33,782 INFO quic [0dfae2e5fb7fc4c7] ALPN negotiated protocol h3
2024-11-29 00:27:33,783 INFO client New session ticket received
2024-11-29 00:27:33,784 INFO client Response received for GET / : 1196 bytes in 0.0 s (8.251 Mbps)
2024-11-29 00:27:33,785 INFO client Push received for GET /style.css : 0 bytes
2024-11-29 00:27:33,785 INFO quic [0dfae2e5fb7fc4c7] Connection close sent (code 0x100, reason )

~/C/m/impl/aioquic  main ?1                                  ✓ aioquic-env
```

picoquic : picoquicdemo

```
579f4aa3c5bedf5c:     stream 8, offset 1076289, length 1407, fin = 0: 5a5a5a5a5a5a5a5a...

579f4aa3c5bedf5c: T= 0.039795, cwin: 94473,flight: 24480,nb_ret: 0,rtt_min: 61,rtt: 622,rtt_var: 979,ma
x_ack_delay: 0,state: 14
579f4aa3c5bedf5c: Sending 1440 bytes to [0:0:0:0:0:0:0:1]:49363 at T=0.039795 (113111b6e)
579f4aa3c5bedf5c: Sending packet type: 6 (1rtt protected), S0, Q0,
579f4aa3c5bedf5c:     <6e09ac272a35a111>, Seq: 773 (773), Phi: 0,
579f4aa3c5bedf5c:     Prepared 1413 bytes
579f4aa3c5bedf5c:     stream 8, offset 1077696, length 1407, fin = 0: 5a5a5a5a5a5a5a5a...

579f4aa3c5bedf5c: T= 0.039795, cwin: 94473,flight: 25920,nb_ret: 0,rtt_min: 61,rtt: 622,rtt_var: 979,ma
x_ack_delay: 0,state: 14
579f4aa3c5bedf5c: Sending 1440 bytes to [0:0:0:0:0:0:0:1]:49363 at T=0.039795 (113111b6e)
579f4aa3c5bedf5c: Sending packet type: 6 (1rtt protected), S0, Q0,
579f4aa3c5bedf5c:     <6e09ac272a35a111>, Seq: 774 (774), Phi: 0,
579f4aa3c5bedf5c:     Prepared 1413 bytes
```

picoquic : zsh

```
❯ source ~/ivy_env/bin/activate
❯ ./picoquicdemo localhost
Starting Picoquic (v1.1.28.0) connection to server = localhost, port = 4443
Testing scenario: <0:index.html;4:test.html;8:/1234567;12:main.jpg;16:war-and-peace.txt;20:en/latest/;2
4:/file-123K>
Max stream id bidir remote before start = 0 (0)
Starting client connection. Version = 1, I-CID: 579f4aa3c5bedf5c
Max stream id bidir remote after start = -4 (0)
Waiting for packets.
Client port (AF=10): 54208.
Negotiated ALPN: h3
Almost ready!

Connection established. Version = 1, I-CID: 579f4aa3c5bedf5c, verified: 1
Opening stream 0 to GET /index.html
Stream 0 ended after 386 bytes
```

impl : go

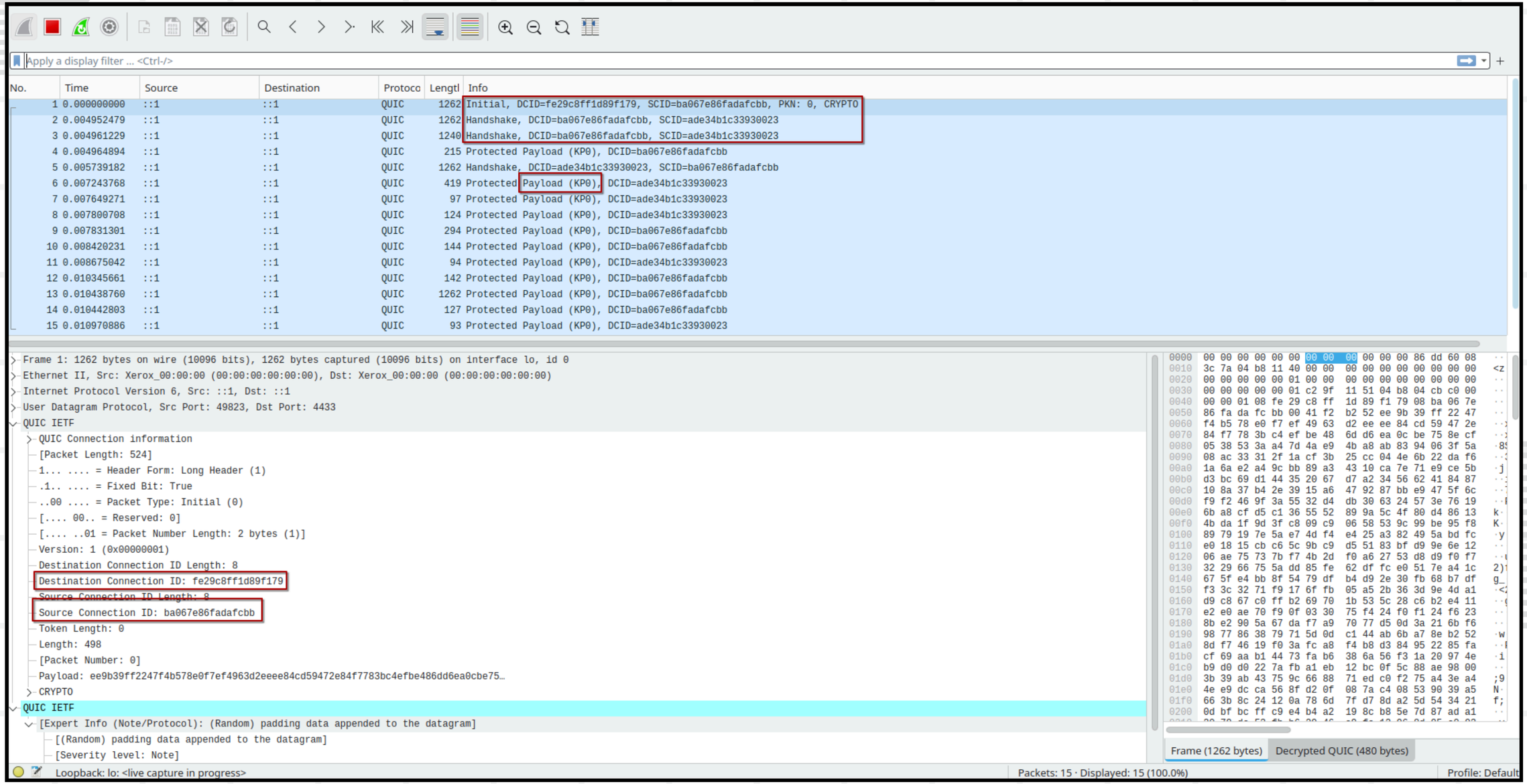
```
❯ go run minq/bin/server/main.go
2024/11/29 11:05:48 New connection
2024/11/29 11:05:48 State changed to  StateEstablished
2024/11/29 11:05:54 State changed to  StateClosing
2024/11/29 11:05:55 State changed to  StateClosed
```

impl : zsh

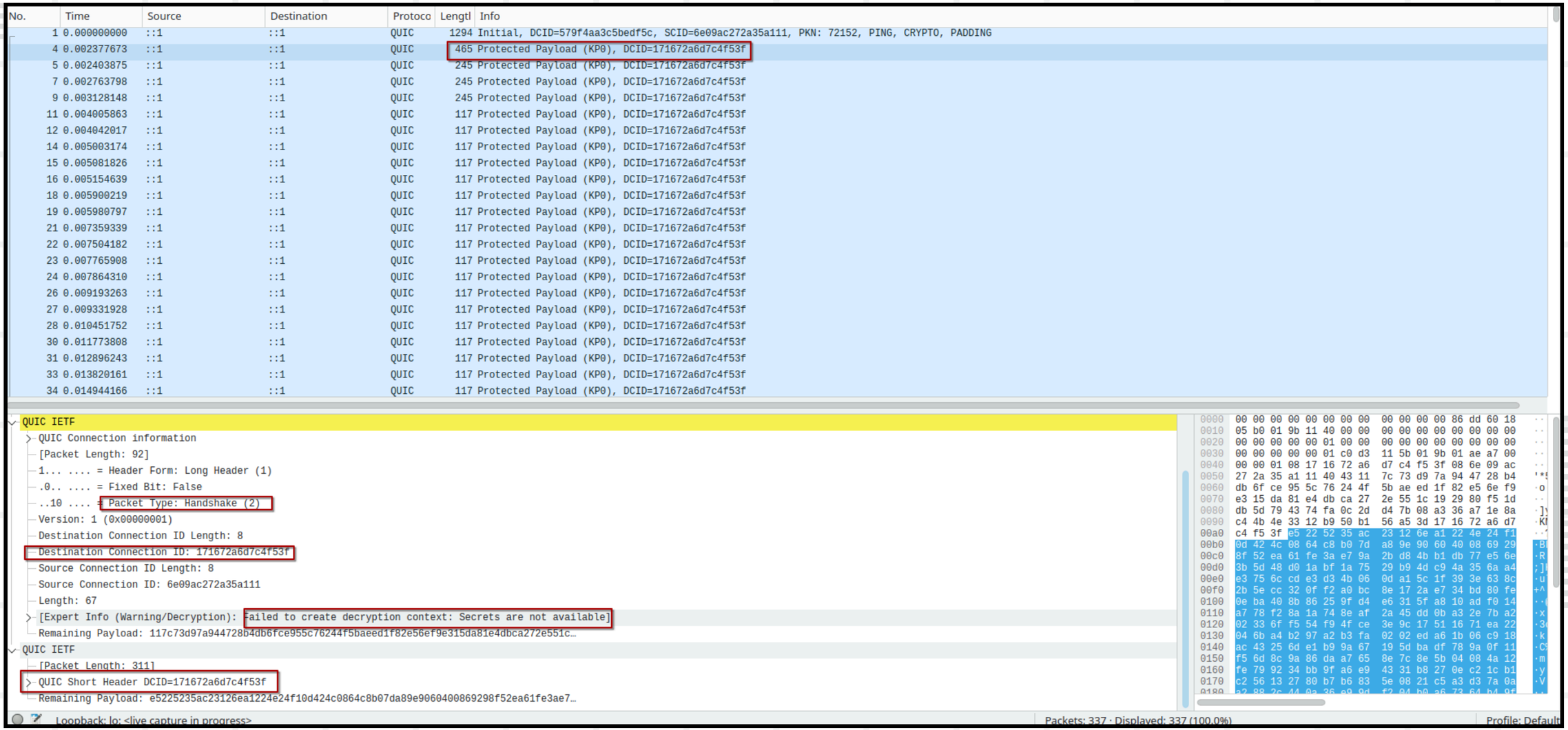
```
❯ go run minq/bin/client/main.go
2024/11/29 11:05:48 PID= 8670
2024/11/29 11:05:48 Client conn id=fba6142dd7
2024/11/29 11:05:48 State changed to  StateWaitServerInitial
2024/11/29 11:05:48 State changed to  StateWaitServerFirstFlight
2024/11/29 11:05:48 State changed to  StateEstablished
2024/11/29 11:05:48 Connection established server CID = 8fd99c249d
2024/11/29 11:05:54 State changed to  StateClosing
2024/11/29 11:05:54 Error Connection is closing

~/Code/mtp/impl                                  ✓ 5s ivy_env
```

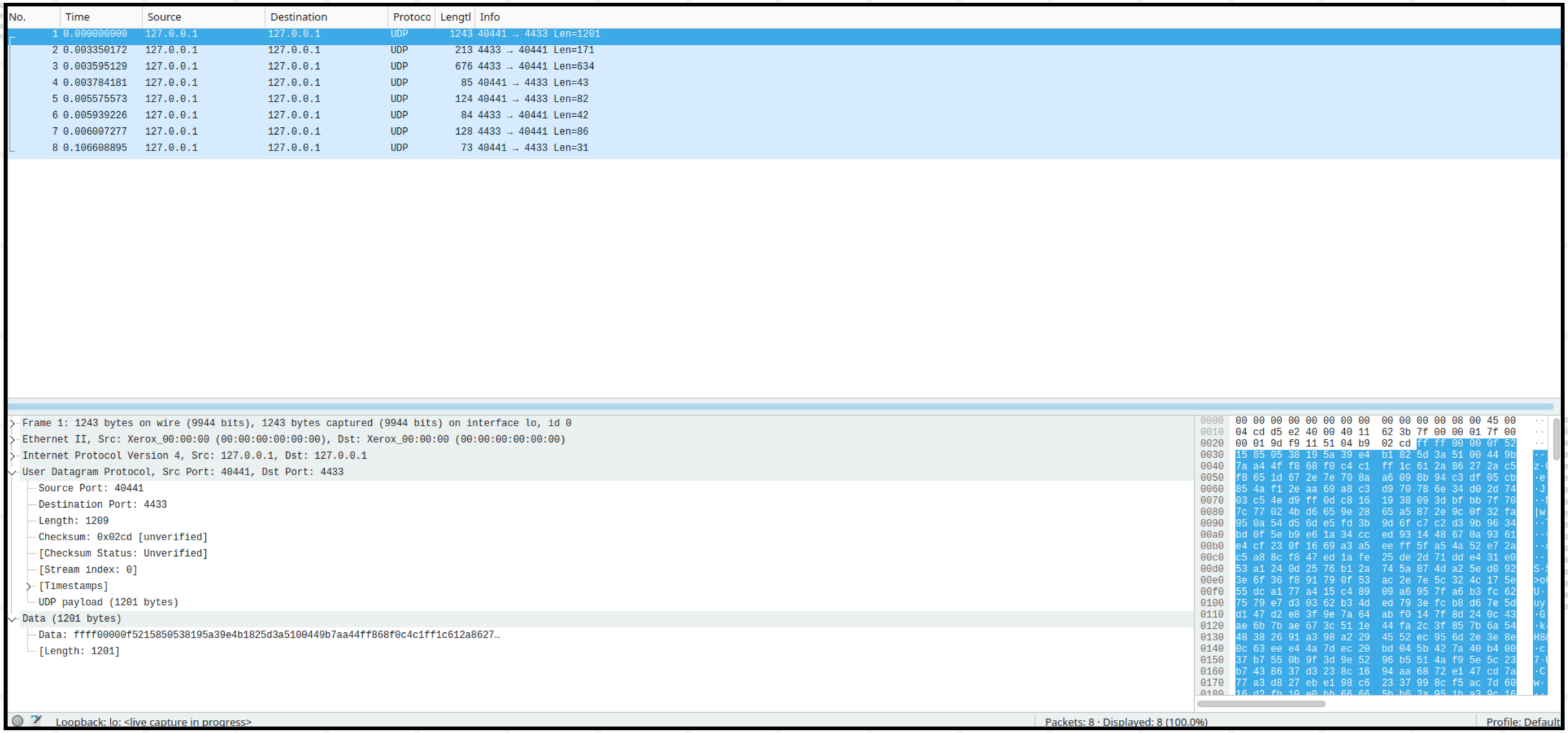
AIOQUIC


Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protoco Lengtl Info
1 0.000000000 ::1 ::1 QUIC 1262 Initial, DCID=fe29c8ff1d89f179, SCID=ba067e86fadafcbb, PKN: 0, CRYPTO
2 0.004952479 ::1 ::1 QUIC 1262 Handshake, DCID=ba067e86fadafcbb, SCID=ade34b1c33930023
3 0.004961229 ::1 ::1 QUIC 1240 Handshake, DCID=ba067e86fadafcbb, SCID=ade34b1c33930023
4 0.004964894 ::1 ::1 QUIC 215 Protected Payload (KP0), DCID=ba067e86fadafcbb
5 0.005739182 ::1 ::1 QUIC 1262 Handshake, DCID=ade34b1c33930023, SCID=ba067e86fadafcbb
6 0.007243768 ::1 ::1 QUIC 419 Protected Payload (KP0), DCID=ade34b1c33930023
7 0.007649271 ::1 ::1 QUIC 97 Protected Payload (KP0), DCID=ade34b1c33930023
8 0.007800708 ::1 ::1 QUIC 124 Protected Payload (KP0), DCID=ade34b1c33930023
9 0.007831301 ::1 ::1 QUIC 294 Protected Payload (KP0), DCID=ba067e86fadafcbb
10 0.008420231 ::1 ::1 QUIC 144 Protected Payload (KP0), DCID=ba067e86fadafcbb
11 0.008675042 ::1 ::1 QUIC 94 Protected Payload (KP0), DCID=ade34b1c33930023
12 0.010345661 ::1 ::1 QUIC 142 Protected Payload (KP0), DCID=ba067e86fadafcbb
13 0.010438760 ::1 ::1 QUIC 1262 Protected Payload (KP0), DCID=ba067e86fadafcbb
14 0.010442803 ::1 ::1 QUIC 127 Protected Payload (KP0), DCID=ba067e86fadafcbb
15 0.010970886 ::1 ::1 QUIC 93 Protected Payload (KP0), DCID=ade34b1c33930023
Frame 1: 1262 bytes on wire (10096 bits), 1262 bytes captured (10096 bits) on interface lo, id 0
Ethernet II, Src: Xerox_00:00:00 (00:00:00:00:00:00), Dst: Xerox_00:00:00 (00:00:00:00:00:00)
Internet Protocol Version 6, Src: ::1, Dst: ::1
User Datagram Protocol, Src Port: 49823, Dst Port: 4433
QUIC IETF
QUIC Connection information
[Packet Length: 524]
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: 8
Destination Connection ID: fe29c8ff1d89f179
Source Connection ID Length: 8
Source Connection ID: ba067e86fadafcbb
Token Length: 0
Length: 498
[Packet Number: 0]
Payload: ee9b39ff2247f4b578e0f7ef4963d2eeee84cd59472e84f7783bc4efbe486dd6ea0cbe75…
CRYPTO
QUIC IETF
[Expert Info (Note/Protocol): (Random) padding data appended to the datagram]
[(Random) padding data appended to the datagram]
[Severity level: Note]
0000 00 00 00 00 00 00 00 00 00 00 00 00 86 dd 60 08
0010 3c 7a 04 b8 11 40 00 00 00 00 00 00 00 00 00 00
0020 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00
0030 00 00 00 00 00 01 c2 9f 11 51 04 b8 04 cb c0 00
0040 00 00 01 08 fe 29 c8 ff 1d 89 f1 79 08 ba 06 7e
0050 86 fa da fc bb 00 41 f2 b2 52 ee 9b 39 ff 22 47
0060 f4 b5 78 e0 f7 ef 49 63 d2 ee ee 84 cd 59 47 2e
0070 84 f7 78 3b c4 ef be 48 6d d6 ea 0c be 75 8e cf
0080 05 38 53 3a a4 7d 4a e9 4b a8 ab 83 94 06 3f 5a
0090 08 ac 33 31 2f 1a cf 3b 25 cc 04 4e 6b 22 da f6
00a0 1a 6a e2 a4 9c bb 89 a3 43 10 ca 7e 71 e9 ce 5b
00b0 d3 bc 69 d1 44 35 20 67 d7 a2 34 56 62 41 84 87
00c0 10 8a 37 b4 2e 39 15 a6 47 92 87 bb e9 47 5f 6c
00d0 f9 f2 46 9f 3a 55 32 d4 db 30 63 24 57 3e 76 19
00e0 6b a8 cf d5 c1 36 55 52 89 9a 5c 4f 80 d4 86 13
00f0 4b da 1f 9d 3f c8 09 c9 06 58 53 9c 99 be 95 f8
0100 89 79 19 7e 5a e7 4d f4 e4 25 a3 82 49 5a bd fc
0110 e0 18 15 cb c6 5c 9b c9 d5 51 83 bf d9 9e 6e 12
0120 06 ae 75 73 7b f7 4b 2d f0 a6 27 53 d8 d9 f0 f7
0130 32 29 66 75 5a dd 85 fe 62 df fc e0 51 7e a4 1c
0140 67 5f e4 bb 8f 54 79 df b4 d9 2e 30 fb 68 b7 df
0150 f3 3c 32 71 f9 17 6f fb 05 a5 2b 36 3d 9e 4d a1
0160 d9 c8 67 c0 ff b2 69 70 1b 53 5c 28 c6 b2 e4 11
0170 e2 e0 ae 70 f9 0f 03 30 75 f4 24 f0 f1 24 f6 23
0180 8b e2 90 5a 67 da f7 a9 70 77 d5 0d 3a 21 6b f6
0190 98 77 86 38 79 71 5d 0d c1 44 ab 6b a7 8e b2 52
01a0 8d f7 46 19 f0 3a fc a8 f4 b8 d3 84 95 22 85 fa
01b0 cf 69 aa b1 44 73 fa b6 38 6a 56 f3 1a 20 97 4e
01c0 b9 d0 d0 22 7a fb a1 eb 12 bc 0f 5c 88 ae 98 00
01d0 3b 39 ab 43 75 9c 66 88 71 ed c0 f2 75 a4 3e a4
01e0 4e e9 dc ca 56 8f d2 0f 08 7a c4 08 53 90 39 a5
01f0 66 3b 8c 24 12 0a 78 6d 7f d7 8d a2 5d 54 34 21
0200 0d bf bc ff c9 e4 b4 a2 19 8c b8 5e 7d 87 ad a1
Frame (1262 bytes)
Decrypted QUIC (480 bytes)
Loopback: lo: <live capture in progress>
Packets: 15 · Displayed: 15 (100.0%)
Profile: Default

PICOQUIC

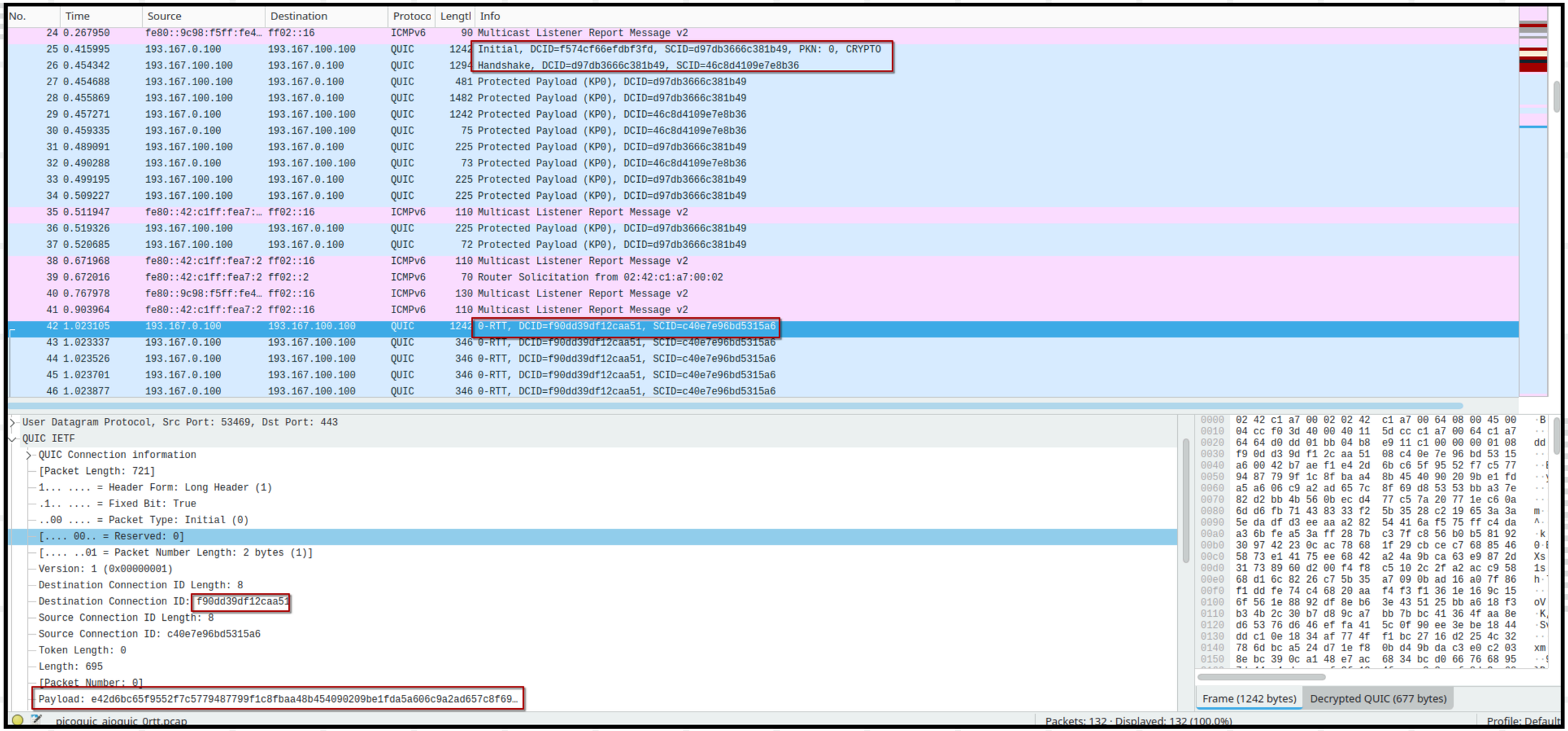

No. Time Source Destination Protoco Lengtl Info
1 0.000000000 ::1 ::1 QUIC 1294 Initial, DCID=579f4aa3c5bedf5c, SCID=6e09ac272a35a111, PKN: 72152, PING, CRYPTO, PADDING
4 0.002377673 ::1 ::1 QUIC 465 Protected Payload (KP0), DCID=171672a6d7c4f53f
5 0.002403875 ::1 ::1 QUIC 245 Protected Payload (KP0), DCID=171672a6d7c4f53f
7 0.002763798 ::1 ::1 QUIC 245 Protected Payload (KP0), DCID=171672a6d7c4f53f
9 0.003128148 ::1 ::1 QUIC 245 Protected Payload (KP0), DCID=171672a6d7c4f53f
11 0.004005863 ::1 ::1 QUIC 117 Protected Payload (KP0), DCID=171672a6d7c4f53f
12 0.004042017 ::1 ::1 QUIC 117 Protected Payload (KP0), DCID=171672a6d7c4f53f
14 0.005003174 ::1 ::1 QUIC 117 Protected Payload (KP0), DCID=171672a6d7c4f53f
15 0.005081826 ::1 ::1 QUIC 117 Protected Payload (KP0), DCID=171672a6d7c4f53f
16 0.005154639 ::1 ::1 QUIC 117 Protected Payload (KP0), DCID=171672a6d7c4f53f
18 0.005900219 ::1 ::1 QUIC 117 Protected Payload (KP0), DCID=171672a6d7c4f53f
19 0.005980797 ::1 ::1 QUIC 117 Protected Payload (KP0), DCID=171672a6d7c4f53f
21 0.007359339 ::1 ::1 QUIC 117 Protected Payload (KP0), DCID=171672a6d7c4f53f
22 0.007504182 ::1 ::1 QUIC 117 Protected Payload (KP0), DCID=171672a6d7c4f53f
23 0.007765908 ::1 ::1 QUIC 117 Protected Payload (KP0), DCID=171672a6d7c4f53f
24 0.007864310 ::1 ::1 QUIC 117 Protected Payload (KP0), DCID=171672a6d7c4f53f
26 0.009193263 ::1 ::1 QUIC 117 Protected Payload (KP0), DCID=171672a6d7c4f53f
27 0.009331928 ::1 ::1 QUIC 117 Protected Payload (KP0), DCID=171672a6d7c4f53f
28 0.010451752 ::1 ::1 QUIC 117 Protected Payload (KP0), DCID=171672a6d7c4f53f
30 0.011773808 ::1 ::1 QUIC 117 Protected Payload (KP0), DCID=171672a6d7c4f53f
31 0.012896243 ::1 ::1 QUIC 117 Protected Payload (KP0), DCID=171672a6d7c4f53f
33 0.013820161 ::1 ::1 QUIC 117 Protected Payload (KP0), DCID=171672a6d7c4f53f
34 0.014944166 ::1 ::1 QUIC 117 Protected Payload (KP0), DCID=171672a6d7c4f53f
QUIC IETF
QUIC Connection information
[Packet Length: 92]
1... .... = Header Form: Long Header (1)
.0.. .... = Fixed Bit: False
..10 .... = Packet Type: Handshake (2)
Version: 1 (0x00000001)
Destination Connection ID Length: 8
Destination Connection ID: 171672a6d7c4f53f
Source Connection ID Length: 8
Source Connection ID: 6e09ac272a35a111
Length: 67
[Expert Info (Warning/Decryption): Failed to create decryption context: Secrets are not available]
Remaining Payload: 117c73d97a944728b4db6fce955c76244f5baeed1f82e56ef9e315da81e4dbca272e551c…
QUIC IETF
[Packet Length: 311]
QUIC Short Header DCID=171672a6d7c4f53f
Remaining Payload: e5225235ac23126ea1224e24f10d424c0864c8b07da89e9060400869298f52ea61fe3ae7…
Loopback: lo: <live capture in progress>
Packets: 337 · Displayed: 337 (100.0%)
Profile: Default

MINQUIC

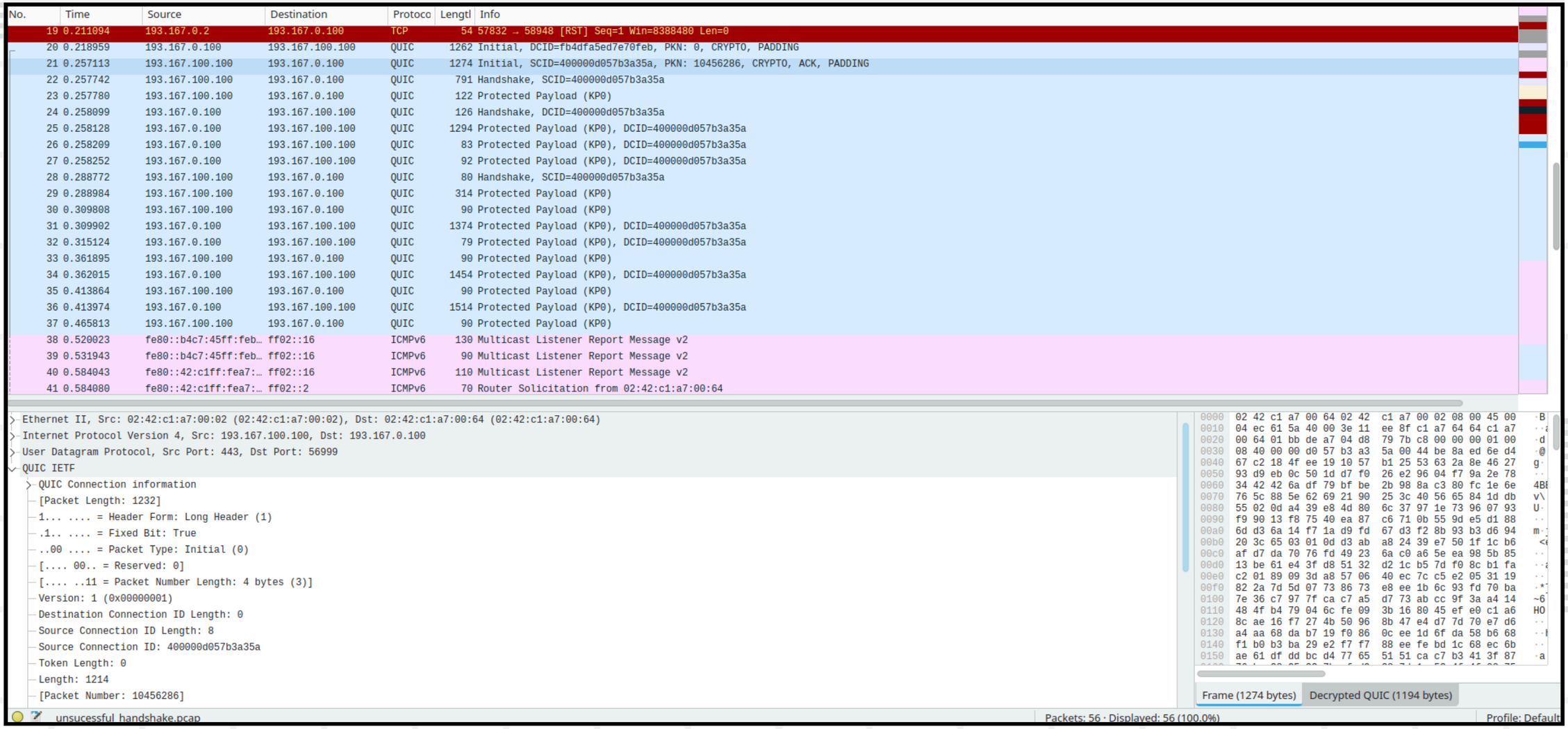

No. Time Source Destination Protoco Lengtl Info
1 0.000000000 127.0.0.1 127.0.0.1 UDP 1243 40441 → 4433 Len=1201
2 0.003350172 127.0.0.1 127.0.0.1 UDP 213 4433 → 40441 Len=171
3 0.003595129 127.0.0.1 127.0.0.1 UDP 676 4433 → 40441 Len=634
4 0.003784181 127.0.0.1 127.0.0.1 UDP 85 40441 → 4433 Len=43
5 0.005575573 127.0.0.1 127.0.0.1 UDP 124 40441 → 4433 Len=82
6 0.005939226 127.0.0.1 127.0.0.1 UDP 84 4433 → 40441 Len=42
7 0.006007277 127.0.0.1 127.0.0.1 UDP 128 4433 → 40441 Len=86
8 0.106608895 127.0.0.1 127.0.0.1 UDP 73 40441 → 4433 Len=31
Frame 1: 1243 bytes on wire (9944 bits), 1243 bytes captured (9944 bits) on interface lo, id 0
Ethernet II, Src: Xerox_00:00:00 (00:00:00:00:00:00), Dst: Xerox_00:00:00 (00:00:00:00:00:00)
Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
User Datagram Protocol, Src Port: 40441, Dst Port: 4433
Source Port: 40441
Destination Port: 4433
Length: 1209
Checksum: 0x02cd [unverified]
[Checksum Status: Unverified]
[Stream index: 0]
[Timestamps]
UDP payload (1201 bytes)
Data (1201 bytes)
Data: ffff00000f5215850538195a39e4b1825d3a5100449b7aa44ff868f0c4c1ff1c612a8627…
[Length: 1201]
0000 00 00 00 00 00 00 00 00 00 00 00 00 08 00 45 00
0010 04 cd d5 e2 40 00 40 11 62 3b 7f 00 00 01 7f 00
0020 00 01 9d f9 11 51 04 b9 02 cd ff ff 00 00 0f 52
0030 15 85 05 38 19 5a 39 e4 b1 82 5d 3a 51 00 44 9b
0040 7a a4 4f f8 68 f0 c4 c1 ff 1c 61 2a 86 27 2a c5
0050 f8 65 1d 67 2e 7e 70 8a a6 09 8b 94 c3 df 05 cb
0060 85 4a f1 2e aa 69 a8 c3 d9 70 78 6e 34 d0 2d 74
0070 03 c5 4e d9 ff 0d c8 16 19 38 09 3d bf bb 7f 70
0080 7c 77 02 4b d6 65 9e 28 65 a5 87 2e 9c 0f 32 fa
0090 95 0a 54 d5 6d e5 fd 3b 9d 6f c7 c2 d3 9b 96 34
00a0 bd 0f 5e b9 e6 1a 34 cc ed 93 14 48 67 0a 93 61
00b0 e4 cf 23 0f 16 69 a3 a5 ee ff 5f a5 4a 52 e7 2a
00c0 c5 a8 8c f8 47 ed 1a fe 25 de 2d 71 dd e4 31 e0
00d0 53 a1 24 0d 25 76 b1 2a 74 5a 87 4d a2 5e d0 92
00e0 3e 6f 36 f8 91 79 0f 53 ac 2e 7e 5c 32 4c 17 5e
00f0 55 dc a1 77 a4 15 c4 89 09 a6 95 7f a6 b3 fc 62
0100 75 79 e7 d3 03 62 b3 4d ed 79 3e fc b8 d6 7e 5d
0110 d1 47 d2 e8 3f 9e 7a 64 ab f0 14 7f 8d 24 0c 43
0120 ae 6b 7b ae 67 3c 51 1e 44 fa 2c 3f 85 7b 6a 54
0130 48 38 26 91 a3 98 a2 29 45 52 ec 95 6d 2e 3e 8e
0140 0c 63 ee e4 4a 7d ec 20 bd 04 5b 42 7a 40 b4 00
0150 37 b7 55 0b 9f 3d 9e 52 96 b5 51 4a f9 5e 5c 23
0160 b7 43 86 37 d3 23 8c 16 94 aa 68 72 e1 47 cd 7a
0170 77 a3 d8 27 eb e1 98 c6 23 37 99 8c f5 ac 7d 60
Loopback: lo: <live capture in progress>
Packets: 8 · Displayed: 8 (100.0%)
Profile: Default

INTEROPERABILITY TESTS

0-RTT TEST BETWEEN AIOQUIC AND PICOQUIC



UNSUCCESSFUL HANDSHAKE TEST BET'N MSQUIC (IMPL BY MICROSOFT) & MVFST (IMPL BY META)



No.	Time	Source	Destination	Protoco	Lengtl	Info
19	0.211094	193.167.0.2	193.167.0.100	TCP	54	57832 → 58948 [RST] Seq=1 Win=8388480 Len=0
20	0.218959	193.167.0.100	193.167.100.100	QUIC	1262	Initial, DCID=fb4dfa5ed7e70feb, PKN: 0, CRYPTO, PADDING
21	0.257113	193.167.100.100	193.167.0.100	QUIC	1274	Initial, SCID=400000d057b3a35a, PKN: 10456286, CRYPTO, ACK, PADDING
22	0.257742	193.167.100.100	193.167.0.100	QUIC	791	Handshake, SCID=400000d057b3a35a
23	0.257780	193.167.100.100	193.167.0.100	QUIC	122	Protected Payload (KP0)
24	0.258099	193.167.0.100	193.167.100.100	QUIC	126	Handshake, DCID=400000d057b3a35a
25	0.258128	193.167.0.100	193.167.100.100	QUIC	1294	Protected Payload (KP0), DCID=400000d057b3a35a
26	0.258209	193.167.0.100	193.167.100.100	QUIC	83	Protected Payload (KP0), DCID=400000d057b3a35a
27	0.258252	193.167.0.100	193.167.100.100	QUIC	92	Protected Payload (KP0), DCID=400000d057b3a35a
28	0.288772	193.167.100.100	193.167.0.100	QUIC	80	Handshake, SCID=400000d057b3a35a
29	0.288984	193.167.100.100	193.167.0.100	QUIC	314	Protected Payload (KP0)
30	0.309808	193.167.100.100	193.167.0.100	QUIC	90	Protected Payload (KP0)
31	0.309902	193.167.0.100	193.167.100.100	QUIC	1374	Protected Payload (KP0), DCID=400000d057b3a35a
32	0.315124	193.167.0.100	193.167.100.100	QUIC	79	Protected Payload (KP0), DCID=400000d057b3a35a
33	0.361895	193.167.100.100	193.167.0.100	QUIC	90	Protected Payload (KP0)
34	0.362015	193.167.0.100	193.167.100.100	QUIC	1454	Protected Payload (KP0), DCID=400000d057b3a35a
35	0.413864	193.167.100.100	193.167.0.100	QUIC	90	Protected Payload (KP0)
36	0.413974	193.167.0.100	193.167.100.100	QUIC	1514	Protected Payload (KP0), DCID=400000d057b3a35a
37	0.465813	193.167.100.100	193.167.0.100	QUIC	90	Protected Payload (KP0)
38	0.520023	fe80::b4c7:45ff:feb…	ff02::16	ICMPv6	130	Multicast Listener Report Message v2
39	0.531943	fe80::b4c7:45ff:feb…	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
40	0.584043	fe80::42:c1ff:fea7:…	ff02::16	ICMPv6	110	Multicast Listener Report Message v2
41	0.584080	fe80::42:c1ff:fea7:…	ff02::2	ICMPv6	70	Router Solicitation from 02:42:c1:a7:00:64

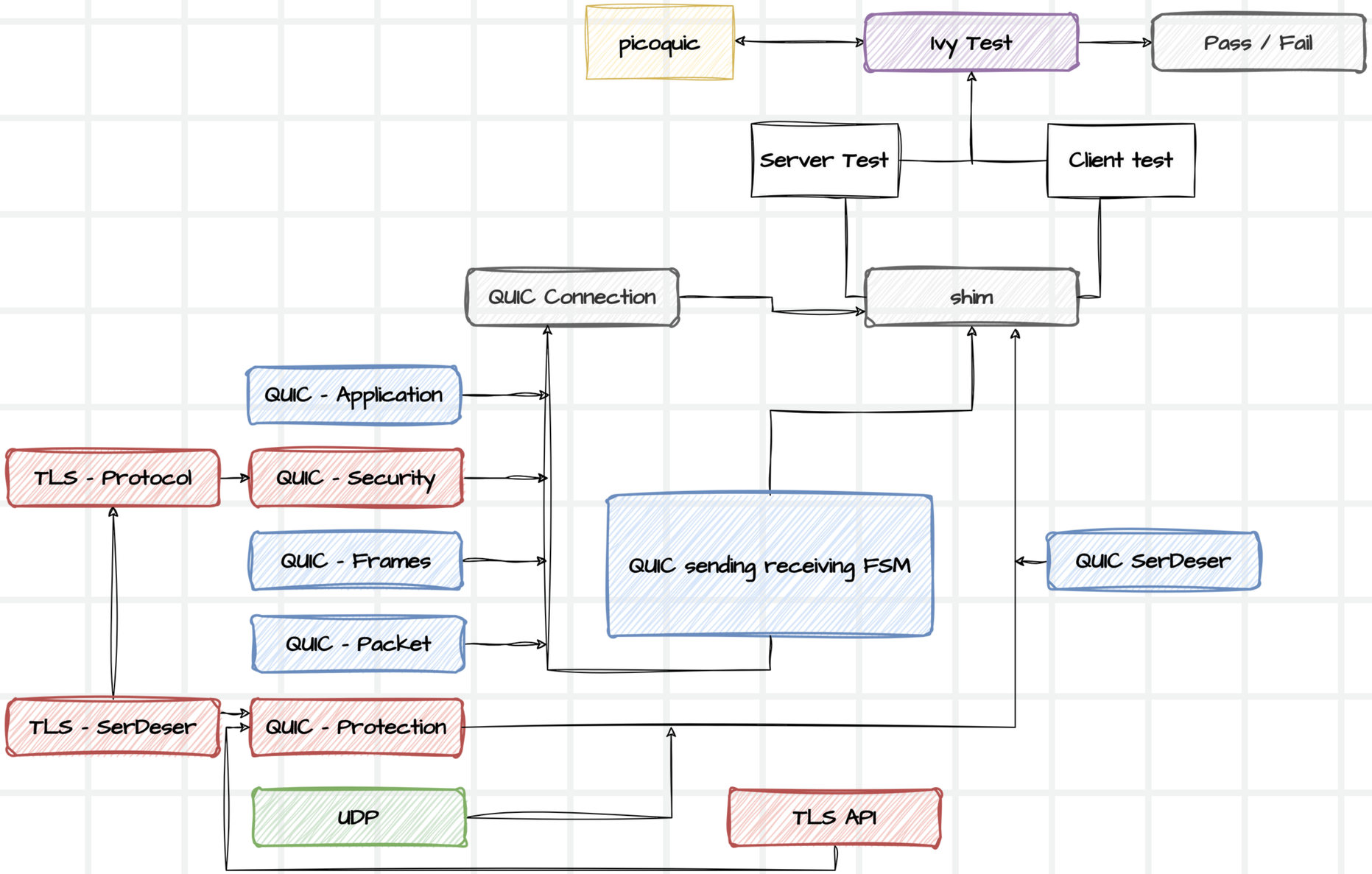
```
> Ethernet II, Src: 02:42:c1:a7:00:02 (02:42:c1:a7:00:02), Dst: 02:42:c1:a7:00:64 (02:42:c1:a7:00:64)
> Internet Protocol Version 4, Src: 193.167.100.100, Dst: 193.167.0.100
> User Datagram Protocol, Src Port: 443, Dst Port: 56999
v QUIC IETF
  > QUIC Connection information
    [Packet Length: 1232]
    1... .... = Header Form: Long Header (1)
    .1.. .... = Fixed Bit: True
    ..00 .... = Packet Type: Initial (0)
    [.... 00.. = Reserved: 0]
    [.... ..11 = Packet Number Length: 4 bytes (3)]
    Version: 1 (0x00000001)
    Destination Connection ID Length: 0
    Source Connection ID Length: 8
    Source Connection ID: 400000d057b3a35a
    Token Length: 0
    Length: 1214
    [Packet Number: 10456286]
```

```
0000  02 42 c1 a7 00 64 02 42  c1 a7 00 02 08 00 45 00   ·B
0010  04 ec 61 5a 40 00 3e 11  ee 8f c1 a7 64 64 c1 a7   ··
0020  00 64 01 bb de a7 04 d8  79 7b c8 00 00 00 01 00   ·d
0030  08 40 00 00 d0 57 b3 a3  5a 00 44 be 8a ed 6e d4   ·@
0040  67 c2 18 4f ee 19 10 57  b1 25 53 63 2a 8e 46 27   g·
0050  93 d9 eb 0c 50 1d d7 f0  26 e2 96 04 f7 9a 2e 78   ··
0060  34 42 42 6a df 79 bf be  2b 98 8a c3 80 fc 1e 6e   4BE
0070  76 5c 88 5e 62 69 21 90  25 3c 40 56 65 84 1d db   v\
0080  55 02 0d a4 39 e8 4d 80  6c 37 97 1e 73 96 07 93   U·
0090  f9 90 13 f8 75 40 ea 87  c6 71 0b 55 9d e5 d1 88   ··
00a0  6d d3 6a 14 f7 1a d9 fd  67 d3 f2 8b 93 b3 d6 94   m·
00b0  20 3c 65 03 01 0d d3 ab  a8 24 39 e7 50 1f 1c b6    <
00c0  af d7 da 70 76 fd 49 23  6a c0 a6 5e ea 98 5b 85   ··
00d0  13 be 61 e4 3f d8 51 32  d2 1c b5 7d f0 8c b1 fa   ··
00e0  c2 01 89 09 3d a8 57 06  40 ec 7c c5 e2 05 31 19   ··
00f0  82 2a 7d 5d 07 73 86 73  e8 ee 1b 6c 93 fd 70 ba   ·*
0100  7e 36 c7 97 7f ca c7 a5  d7 73 ab cc 9f 3a a4 14   ~6
0110  48 4f b4 79 04 6c fe 09  3b 16 80 45 ef e0 c1 a6   HO
0120  8c ae 16 f7 27 4b 50 96  8b 47 e4 d7 7d 70 e7 d6   ··
0130  a4 aa 68 da b7 19 f0 86  0c ee 1d 6f da 58 b6 68   ··
0140  f1 b0 b3 ba 29 e2 f7 f7  88 ee fe bd 1c 68 ec 6b   ··
0150  ae 61 df dd bc d4 77 65  51 51 ca c7 b3 41 3f 87   ·a
```

Frame (1274 bytes) | Decrypted QUIC (1194 bytes)

unsucessful_handshake.pcap | Packets: 56 · Displayed: 56 (100.0%) | Profile: Default

FORMAL SPECIFICATION IN IVY



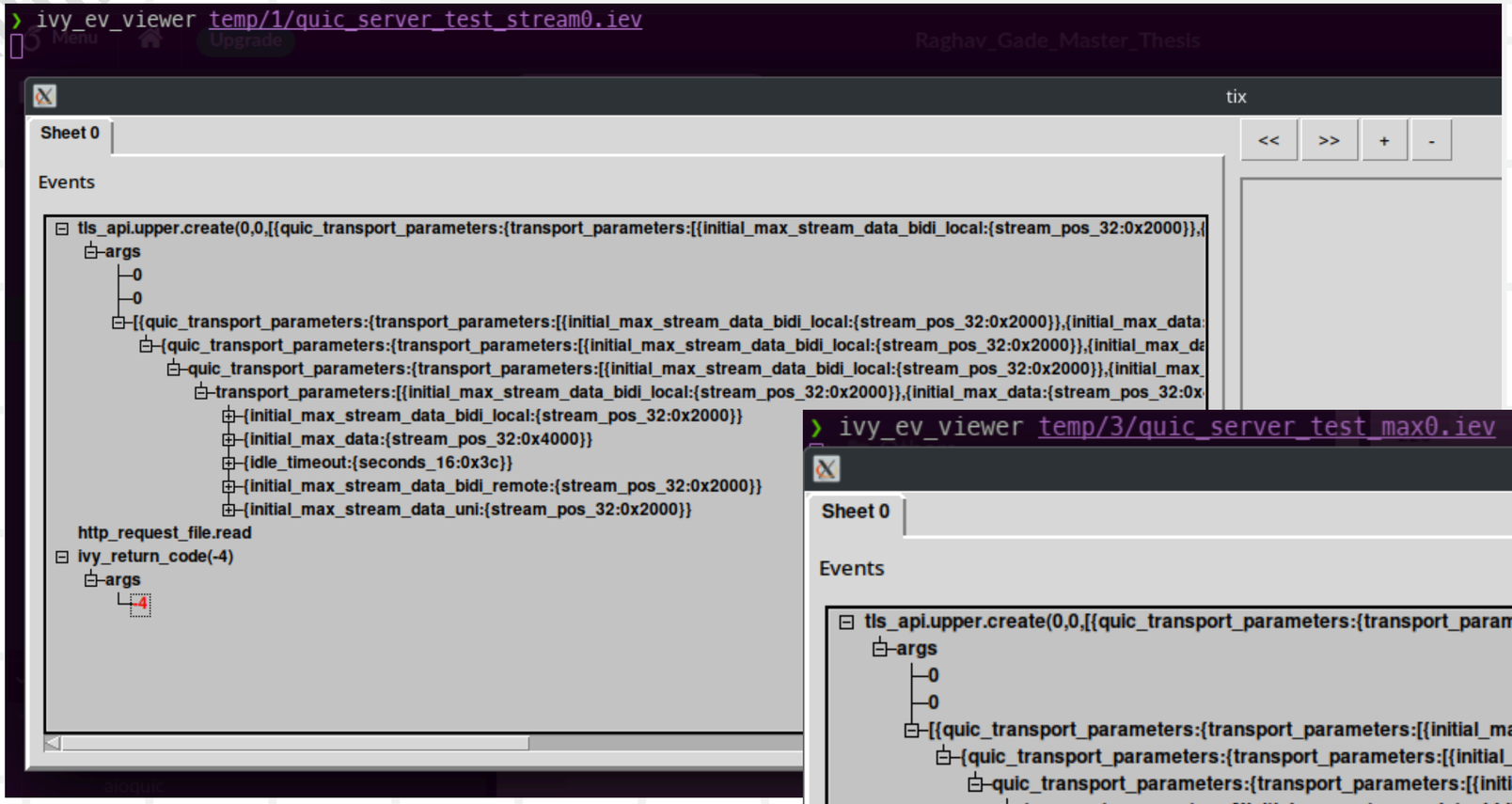
TEST ENVIRONMENT SETUP

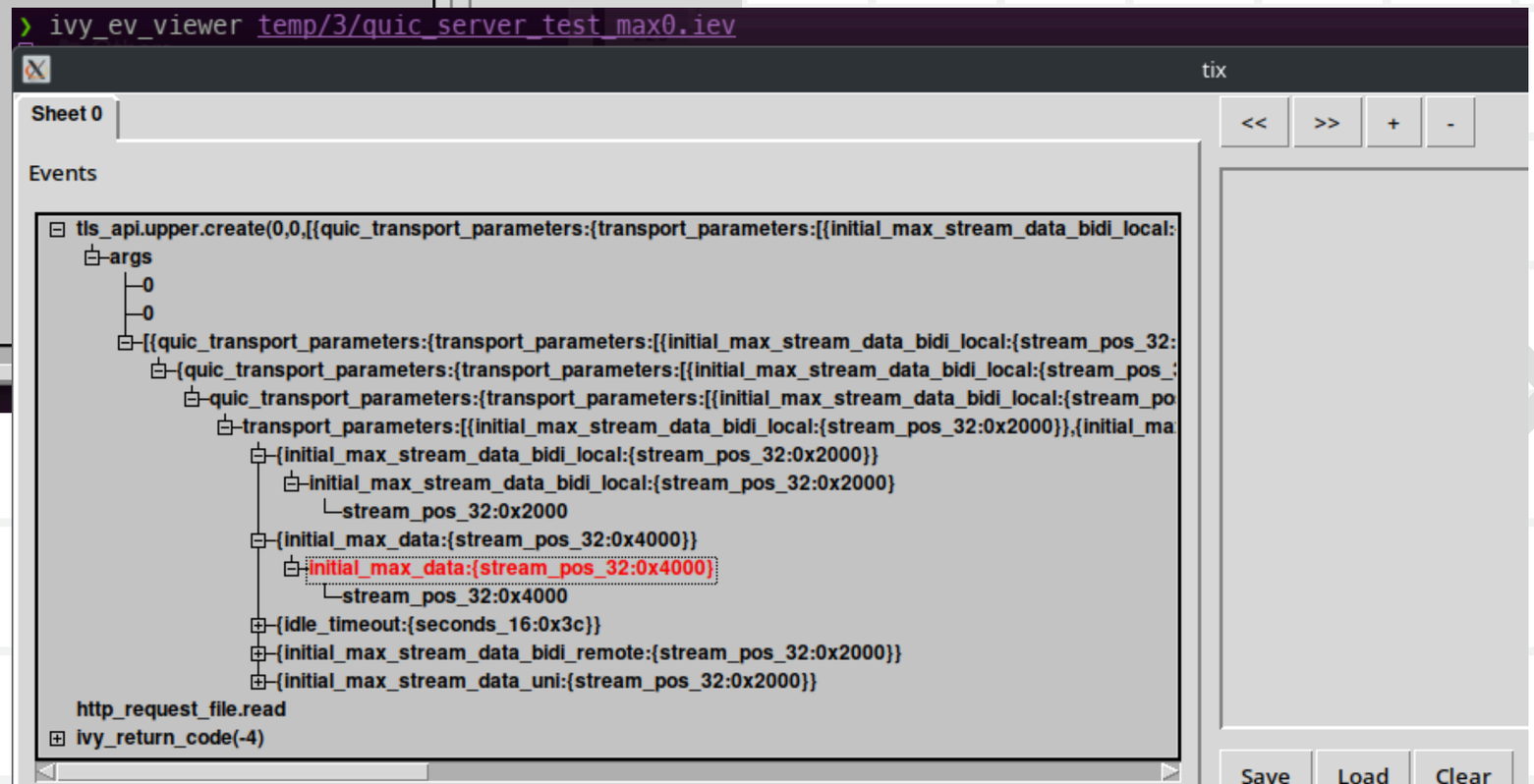
SETUP 1	Arch Linux x86_64 with 45 GB root and 50 GB of /home. Use of python environments wherever necessary.
SETUP 2	Docker container with Ubuntu-18, runs inside setup 1. Takes up 16 GB.

RESULTS SETUP 1

```
❯ python test.py iters=2 server=picoquic test=quic_server_test_stream
output directory: temp/1
implementation directory: /home/huntrag/Code/mtp/new_impl/picoquic
implementation command: ./picoquicdemo -L -l -
../quic_server_test_stream (0) ...
implementation command: ['./picoquicdemo', '-L', '-l', '-']
server pid: 9325
timeout 100 ./build/quic_server_test_stream seed=0 the_cid=0 server_cid=1 client_port=4987 client_port_alt=4988
timeout: the monitored command dumped core
client return code: -4
FAIL
../quic_server_test_stream (1) ...
implementation command: ['./picoquicdemo', '-L', '-l', '-']
server pid: 9334
timeout 100 ./build/quic_server_test_stream seed=1 the_cid=2 server_cid=3 client_port=4989 client_port_alt=4990
timeout: the monitored command dumped core
client return code: -4
FAIL
error: 2 tests(s) failed
❯ python test.py iters=2 server=winquic test=quic_server_test_max
output directory: temp/3
implementation directory: ..
implementation command: true
../quic_server_test_max (0) ...
implementation command: ['true']
server pid: 10408
timeout 100 ./build/quic_server_test_max seed=0 the_cid=0 server_cid=1 client_port=4987 client_port_alt=4988
timeout: the monitored command dumped core
client return code: -4
FAIL
../quic_server_test_max (1) ...
implementation command: ['true']
server pid: 10415
timeout 100 ./build/quic_server_test_max seed=1 the_cid=2 server_cid=3 client_port=4989 client_port_alt=4990
timeout: the monitored command dumped core
client return code: -4
FAIL
error: 2 tests(s) failed
```

OUTPUT SETUP 1





PICOQUIC SERVER TESTS ON SETUP 2

```
Running as user "root" and group "root". This could be dangerous.
Capturing on 'lo'
tshark: cap_set_proc() fail return: Operation not permitted

tshark: cap_set_proc() fail return: Operation not permitted



between random: 82942441
between random: 82942437
between random: 82942441
between random: 28081
"            require f.data = crypto_data(scid,e).segment(f.offset,f.offset+f.length);  # [2]
"
/usr/local/lib/python2.7/dist-packages/ivy/include/1.7/quic_frame.ivy: line 803: error: assumption failed
output directory: temp/13
implementation directory: /quic/picoquic
implementation command: ./picoquicdemo -l - -D -L -q /results/picoquic_qlog
../quic_server_test_crypto_limit_error (0) ...
implementation command: ['./picoquicdemo', '-l', '-', '-D', '-L', '-q', '/results/picoquic_qlog']
quic_process pid: 18614
timeout 100 ./build/quic_server_test_crypto_limit_error seed=495 the_cid=0 server_cid=1 client_port=4987 client_port_alt=498
client return code: 1
FAIL
error: 1 tests(s) failed
test_server.sh: line 94: [: 15: unary operator expected

\Iteration => 15
\Implementation => picoquic
\Test => quic_server_test_crypto_limit_error
```

EXPECTED RESULTS

Test Case	Picoquic	Quant
quic_server_test_stream	614/1000	362/1000
quic_server_test_max	682/1000	306/1000
quic_server_test_connection_close	92/1000	78/1000
quic_client_test_max	133/1000	0/1000

Test Case	Error Code	#
quic_server_test_stream	require ~_generating & ~queued_non_ack(scid) → ack_credit(scid) ¿ 0; [5]	242
	Ran out of values for type cid	121
	require ~path_challenge_pending(dcid,f.data);	24
	bind failed: Address already in use	2
	require conn_seen(dcid) → hi_non_probing_endpoint(dcid,dst); [10]	1
Total		390/1000
quic_server_test_max	require stream_id_allowed(dcid,f.id); [4]	219
	Ran out of values for type cid	102
	require ~path_challenge_pending(dcid,f.data);	8
	require ~_generating & ~queued_non_ack(scid) → ack_credit(scid) ¿ 0; [5]	12
	require conn_total_data(the_cid) ¿ 0;	31
	require conn_seen(dcid) → hi_non_probing_endpoint(dcid,dst); [10]	7
	bind failed: Address already in use	1
Total		380/1000

These are results of 1000 iterations per test. These are the number of tests that passed.

Error code distribution of the tests conducted in setup 1

CONCLUSION

SETUP ERRORS	Compatibilty issue in setup 1 and, space and convenience issue in setup 2. Use virtual machines instead.
RFC 9000 & DRAFT-29	Differences between draft-18, draft-29 and RFC-9000 need to be listed down
ALTERNATIVES TO IVY	No commits regarding development for long time though both papers conclude Ivy is operational for testing. If not Dafny or TLA+ can be explored.

REFERENCES

- K. L. McMillan and L. D. Zuck, “Formal specification and testing of quic,” in Proceedings of the ACM Special Interest Group on Data Communication (SIGCOMM ’19). New York, NY, USA: Association for Computing Machinery,2019, pp. 227–240. [Online]. Available: https://doi.org/10.1145/3341302.3342087
- A. M. Kakhki, S. Jero, D. Choffnes, C. Nita-Rotaru, and A. Mislove, “Taking a long look at quic: An approach for rigorous evaluation of rapidly evolving transport protocols,” in Proceedings of the 2017 Internet Measurement Conference (IMC ’17). New York, NY, USA: Association for Computing Machinery, November 2017, pp. 290–303. [Online]. Available: https://doi.org/10.1145/3131365.3131368
- J. Zhang, X. Gao, L. Yang, T. Feng, D. Li, and Q. Wang, “A systematic approach to formal analysis of quic handshake protocol using symbolic model checking,” Security and Communication Networks, vol. 2021, pp. 1–13, August 2021, academic Editor: Ruhul Amin. [Online]. Available: https://doi.org/10.1155/2021/1630223
- X. Zhang, S. Jin, Y. He, A. Hassan, Z. M. Mao, F. Qian, and Z.-L. Zhang, “Quic is not quick enough over fast internet,” in Proceedings of the ACM Web Conference 2024 (WWW ’24). New York, NY, USA: Association for Computing Machinery, May 2024, pp. 2713–2722. [Online]. Available: https://doi.org/10.1145/3589334.3645323
- C. Crochet, T. Rousseaux, M. Piraux, J.-F. Sambon, and A. Legay, “Verifying quic implementations using ivy,” in Proceedings of the 2021 Workshop on Evolution, Performance and Interoperability of QUIC (EPIQ ’21). New York, NY, USA: Association for Computing Machinery, December 2021, pp. 35–41. [Online]. Available: https://doi.org/10.1145/3488660.3493803

THANK YOU