



QUIC alapú szállítási réteg-mechanizmus forgalmi tulajdonságai

Prof. Dr. Gál Zoltán
Debreceni Egyetem Informatikai Kar

HUNOG_2 Konferencia
Inárcs
2024. október 9-10.



**DEBRECENI
EGYETEM**



**INFORMATIKAI
KAR**



Tartalom

1. QUIC (Quick UDP Internet Connections) mechanizmus dióhéjban
2. QUIC forgalom mérések és teljesítmény tapasztalások
3. QUIC szolgáltatások a jelenlegi gyakorlatban
4. QUIC demó

1. QUIC (Quick UDP Internet Connections) mechanizmus dióhéjban

► Történet:

- 2013. jún. Google, „[Experimenting with QUIC](#)”
- 2017. aug. Google, SIGCOMM előadás

The QUIC Transport Protocol: Design and Internet-Scale Deployment

Adam Langley, Alistair Riddoch, Alyssa Wilk, Antonio Vicente, Charles Krasic, Dan Zhang, Fan Yang, Fedor Kouranov, Ian Swett, Janardhan Iyengar, Jeff Bailey, Jeremy Dorfman, Jim Roskind, Joanna Kulik, Patrik Westin, Raman Tenneti, Robbie Shade, Ryan Hamilton, Victor Vasiliev, Wan-Teh Chang, Zhongyi Shi *
Google
quic-sigcomm@google.com

ABSTRACT

We present our experience with QUIC, an encrypted, multiplexed, and low-latency transport protocol designed from the ground up to improve transport performance for HTTPS traffic and to enable rapid deployment and continued evolution of transport mechanisms. QUIC has been globally deployed at Google on thousands of servers and is used to serve traffic to a range of clients including a widely-used web browser (Chrome) and a popular mobile video streaming app (YouTube). We estimate that 7% of Internet traffic is now QUIC. We describe our motivations for developing a new transport, the principles that guided our design, the Internet-scale process that we used to perform iterative experiments on QUIC, performance improvements seen by our various services, and our experience deploying QUIC globally. We also share lessons about transport design and the Internet ecosystem that we learned from our deployment.

CCS CONCEPTS

• **Networks** → **Network protocol design; Transport protocols; Cross-layer protocols;**

ACM Reference format:

Adam Langley, Alistair Riddoch, Alyssa Wilk, Antonio Vicente, Charles Krasic, Dan Zhang, Fan Yang, Fedor Kouranov, Ian Swett, Janardhan Iyengar, Jeff Bailey, Jeremy Dorfman, Jim Roskind, Joanna Kulik, Patrik Westin, Raman Tenneti, Robbie Shade, Ryan Hamilton, Victor Vasiliev, Wan-Teh Chang, Zhongyi Shi . 2017. The QUIC Transport Protocol: Design and Internet-Scale Deployment. In *Proceedings of SIGCOMM '17, Los Angeles, CA, USA, August 21-25, 2017*, 14 pages. <https://doi.org/10.1145/3098822.3098842>

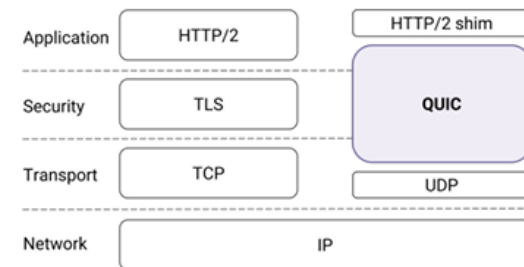


Figure 1: QUIC in the traditional HTTPS stack.

TCP (Figure 1). We developed QUIC as a user-space transport with UDP as a substrate. Building QUIC in user-space facilitated its deployment as part of various applications and enabled iterative changes to occur at application update timescales. The use of UDP allows QUIC packets to traverse middleboxes. QUIC is an encrypted transport: packets are authenticated and encrypted, preventing modification and limiting ossification of the protocol by middleboxes. QUIC uses a cryptographic handshake that minimizes handshake latency for most connections by using known server credentials on repeat connections and by removing redundant handshake-overhead at multiple layers in the network stack. QUIC eliminates head-of-line blocking delays by using a lightweight data-structuring abstraction, *streams*, which are multiplexed within a single connection so that loss of a single packet blocks only streams with data in that packet.

On the server-side, our experience comes from deploying QUIC at Google's front-end servers, which collectively handle billions of

1. QUIC (Quick UDP Internet Connections) mechanizmus dióhéjban

► Történet:

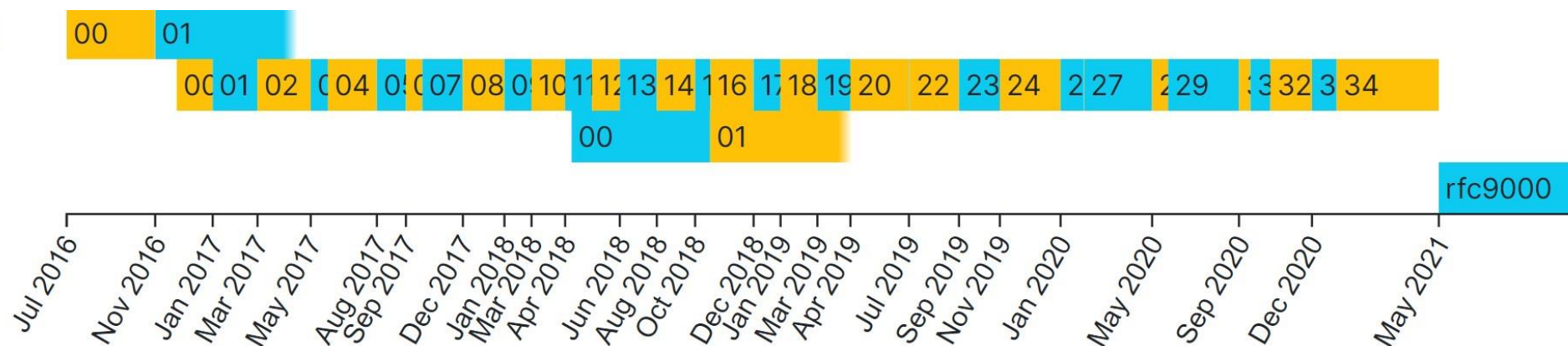
- 2013. jún. Google, „[Experimenting with QUIC](#)”
- 2014. aug. Net-Dev, Field Trial
- 2016. júl. Draft Hamilton QUIC Transport Protocol
- 2016. nov. Draft IETF QUIC Transport
- 2017. aug. Google, SIGCOMM előadás
- 2018. ápr. Draft IETF QUIC Spin Exp.
- 2021. máj. IETF RFC9000: „[QUIC: A UDP-Based Multiplexed and Secure Transport](#)”
- 2022. márc. IETF RFC9221: „[An Unreliable Datagram Extension to QUIC](#)”
- 2023. máj. IETF RFC9369: „[QUIC Version 2](#)”
- ...

draft-hamilton-quic-transport-protocol

draft-ietf-quic-transport

draft-ietf-quic-spin-exp

rfc9000



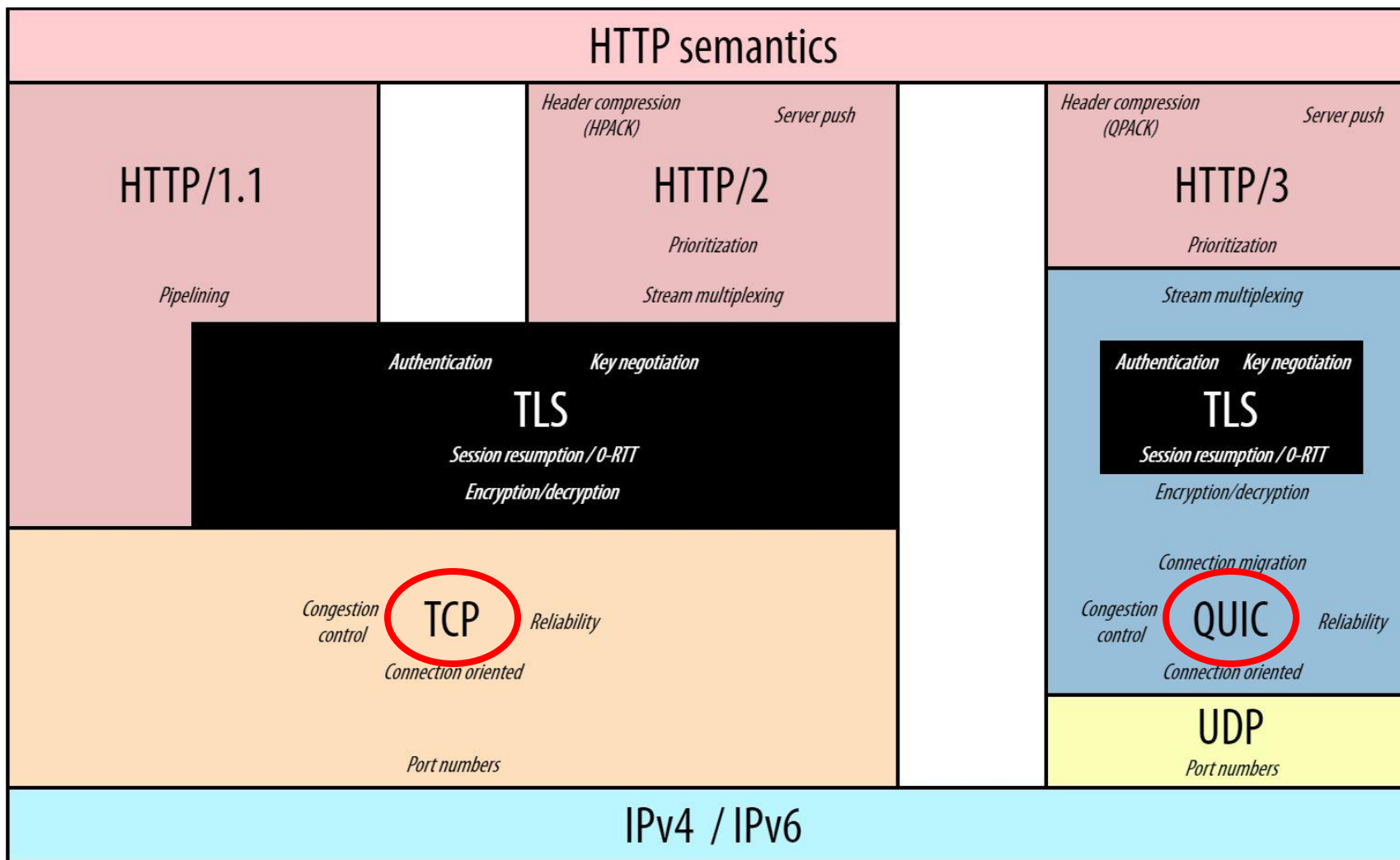
1. QUIC (Quick UDP Internet Connections) mechanizmus dióhéjban

► Összehasonlítás: TCP, UDP QUIC

| Szempont | TCP | UDP | QUIC |
|----------------------------|--------------------------------------|----------------------------|---|
| Réteg a TCP/IP modellben | Transzport | Transzport | Transzport |
| Hely a TCP/IP modellben | IPv4 vagy IPv6 felett | IPv4 vagy IPv6 felett | UDP felett |
| Kapcsolat típus | Kapcsolatorientált | Kapcsolat nélküli/datagram | Kapcsolatorientált |
| Kézbesítési sorrend | Kötött | Nem kötött | Stream-ek között: nem kötött Stream-en belül: kötött |
| Kézbesítési garancia | Van (elveszett szegmens újraküldése) | Nincs | Van (elveszett csomag újraküldése) |
| Handshake mechanizmus | Nem-kriptografikus | Nincs | Kriptografikus kézfogás |
| Titkosítás | Nincs | Nincs | Van |
| Szállított adat azonosítás | Nincs | Nincs | Stream ID-k |

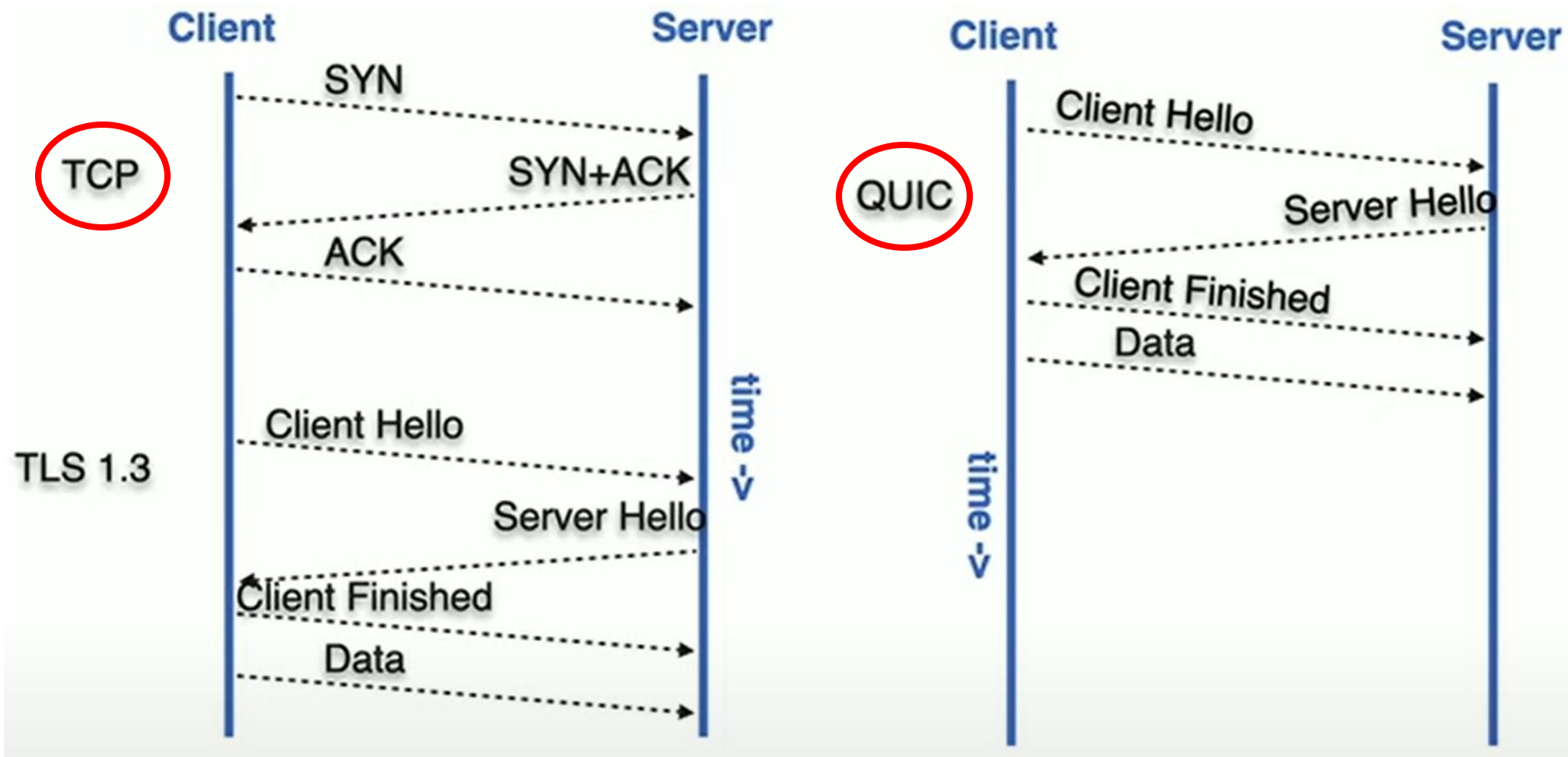
1. QUIC (Quick UDP Internet Connections) mechanizmus dióhéjban

► Protokoll stack: IP, TLS, QUIC, HTTP



1. QUIC (Quick UDP Internet Connections) mechanizmus dióhéjban

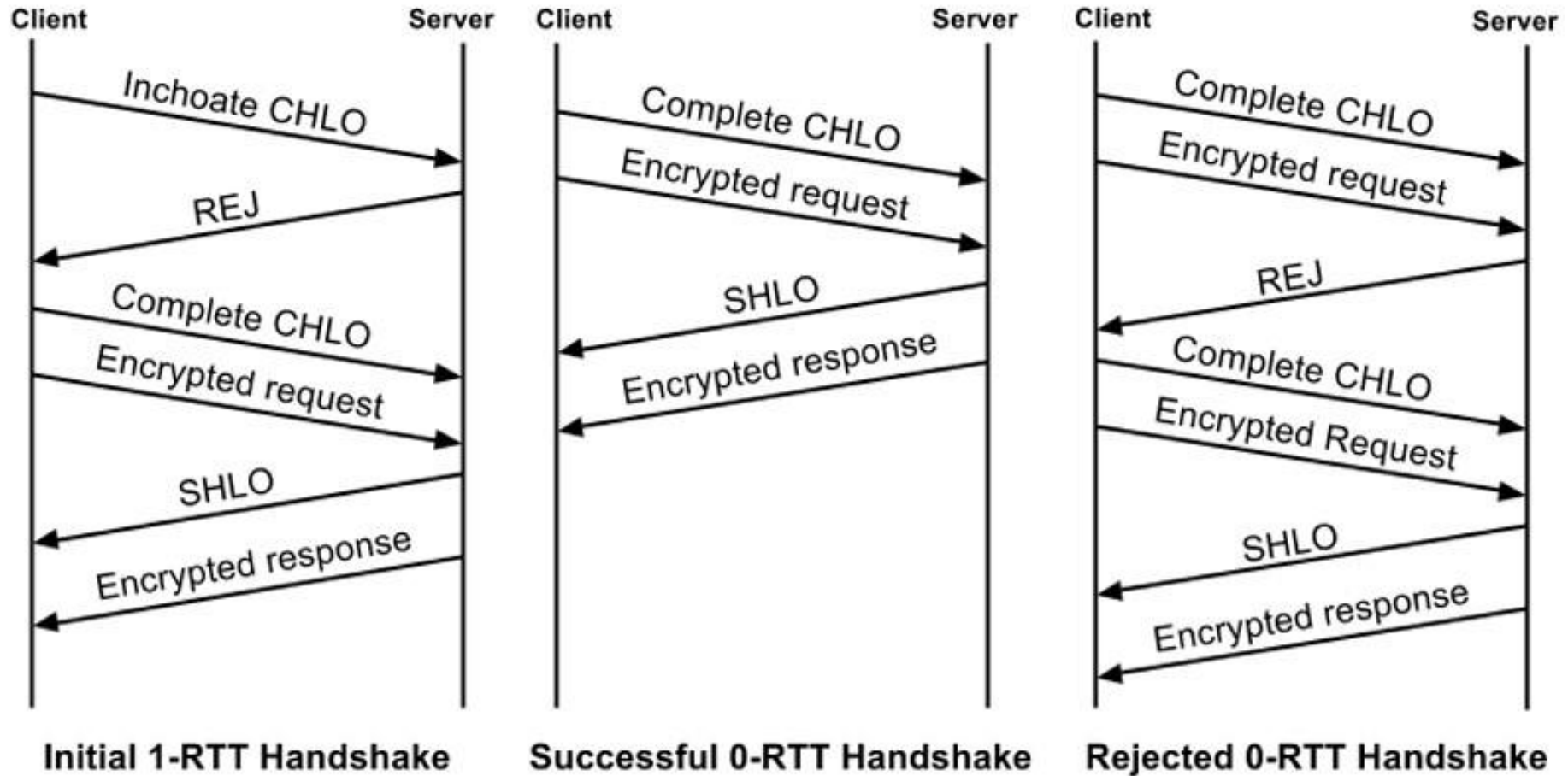
► Kapcsolat felépítés: TCP vs. QUIC



1. QUIC (Quick UDP Internet Connections) mechanizmus dióhéjban

► Kapcsolat felépítés sikeres/sikertelen esetekben: QUIC

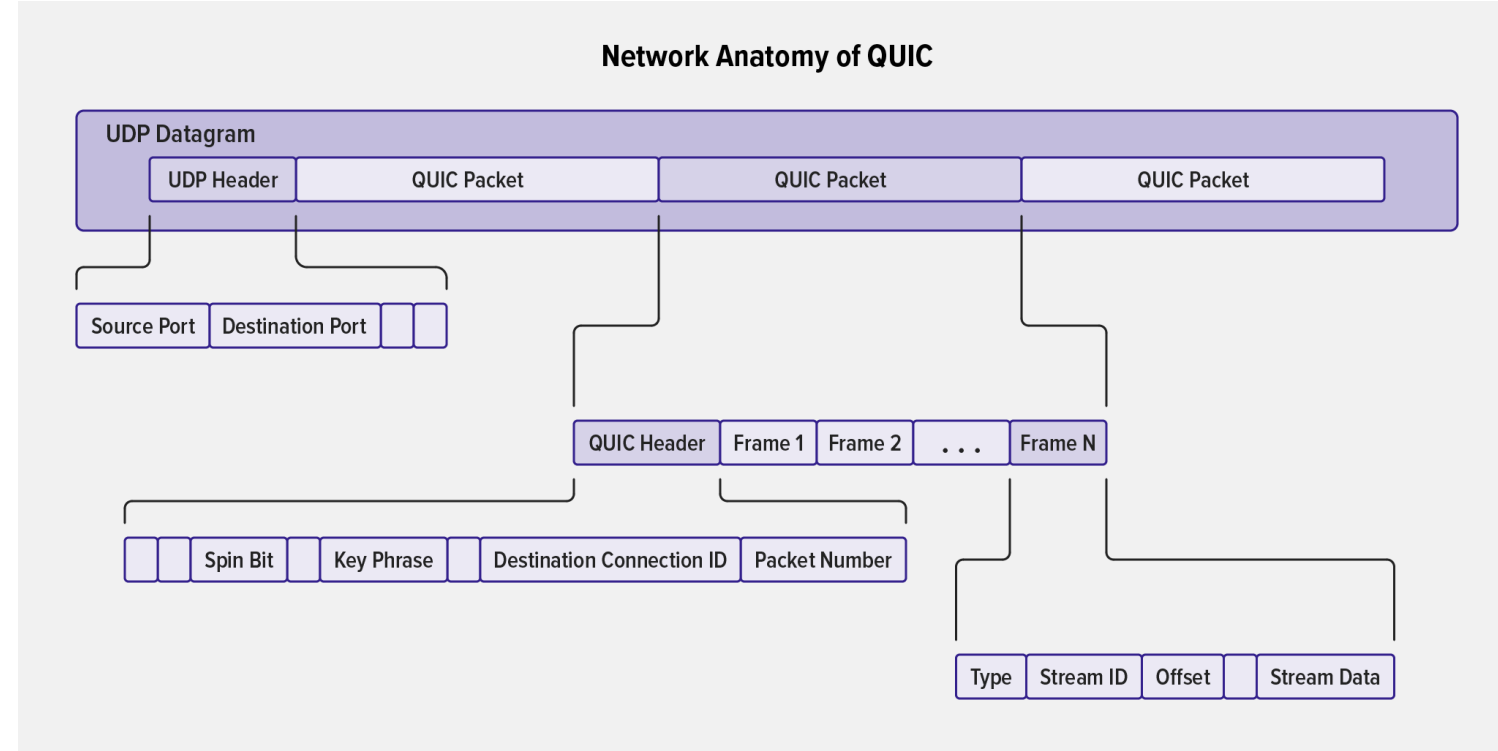
QUIC



1. QUIC (Quick UDP Internet Connections) mechanizmus dióhéjban

► Csomag szerkezete: QUIC

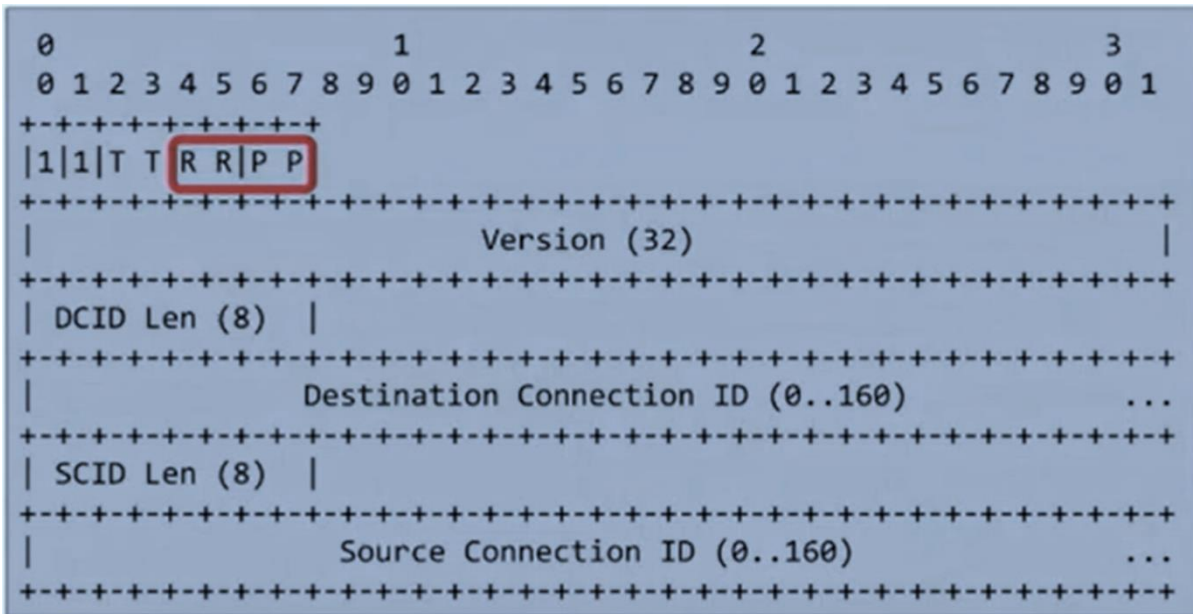
- Header:
 - Long (kapcsolat felépítéshez)
 - Short (adatátvitelhez)
- Frame: adatok tördelve több keretben
- Stream: egyirányú vagy kétirányú adatfolyam
 - 1 session: több független stream
- Connection ID: Source CID, Destination CID
- CID mérete változó: 0, ..., 255 bájt
- QUIC kapcsolat csomagok: eltérő CID értékek lehetnek átvitel közben
- Csomag ID: 62 bit, három térben: initial + handshake + application data



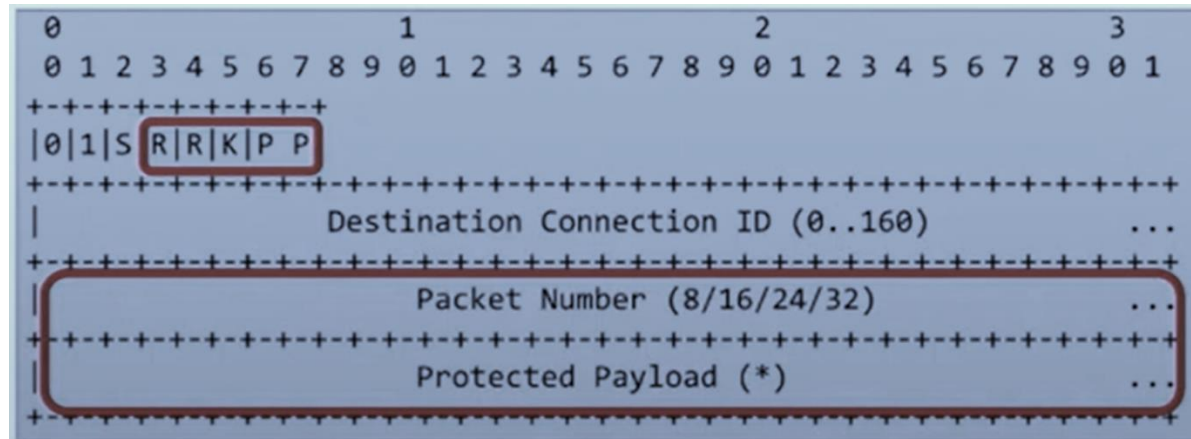
1. QUIC (Quick UDP Internet Connections) mechanizmus dióhéjban

► Csomag Header változatok felépítése: QUIC

Long Header



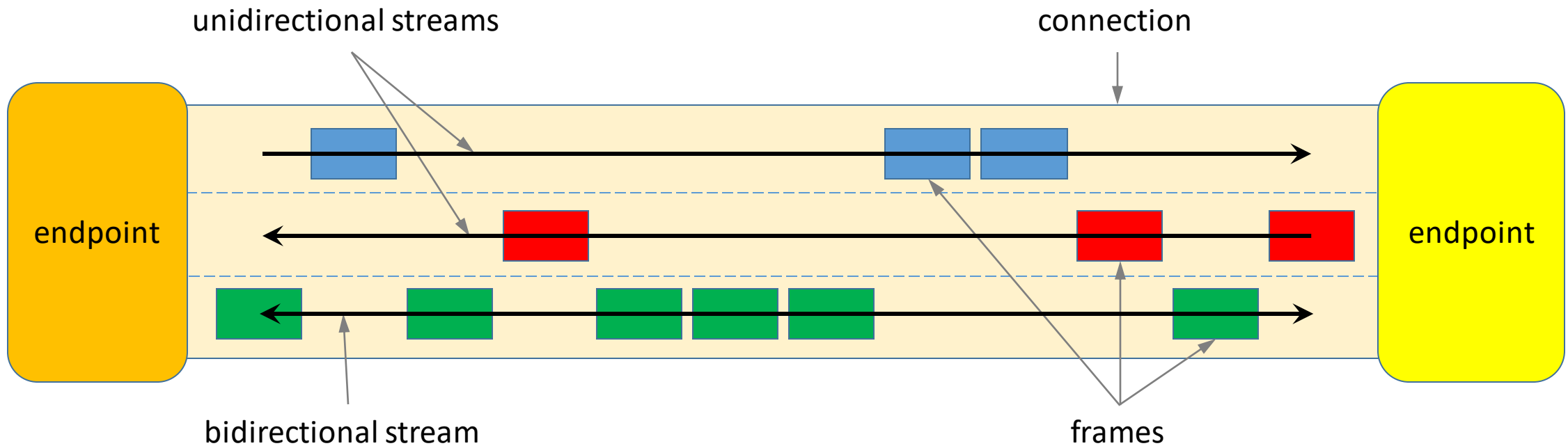
Short Header



1. QUIC (Quick UDP Internet Connections) mechanizmus dióhéjban

► Stream típusok: QUIC

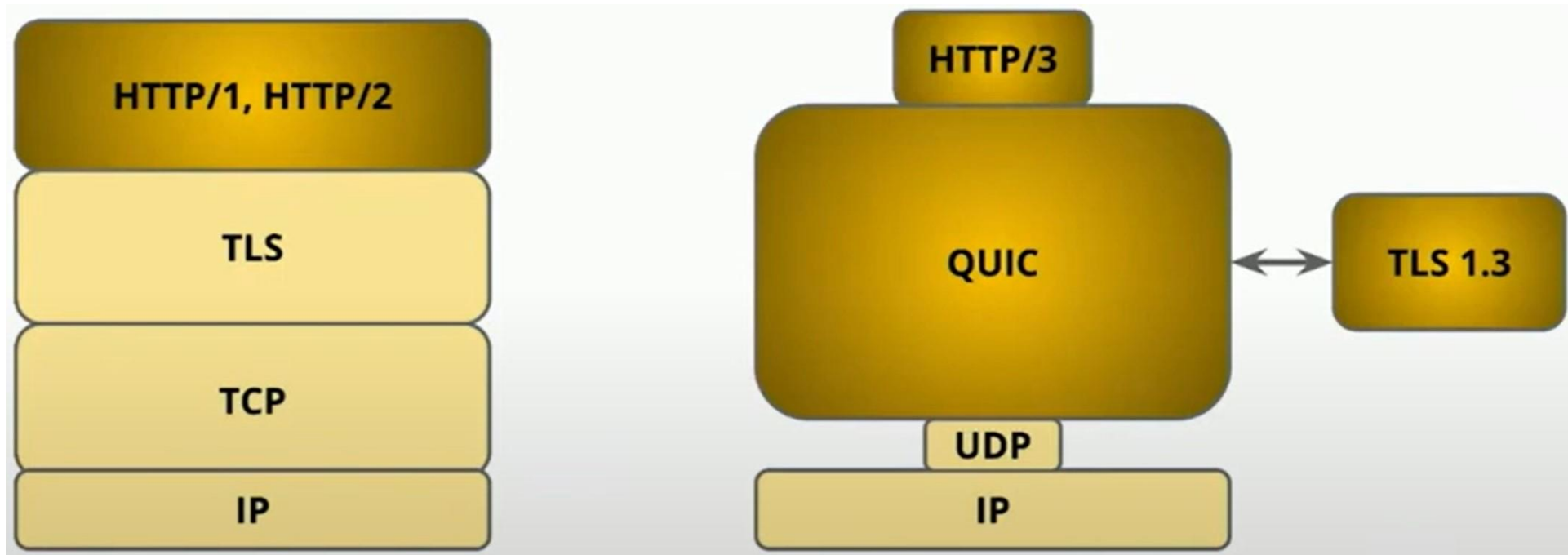
- Stream: keretek sorozata
- Típusok: egyirányú, kétirányú



1. QUIC (Quick UDP Internet Connections) mechanizmus dióhéjban

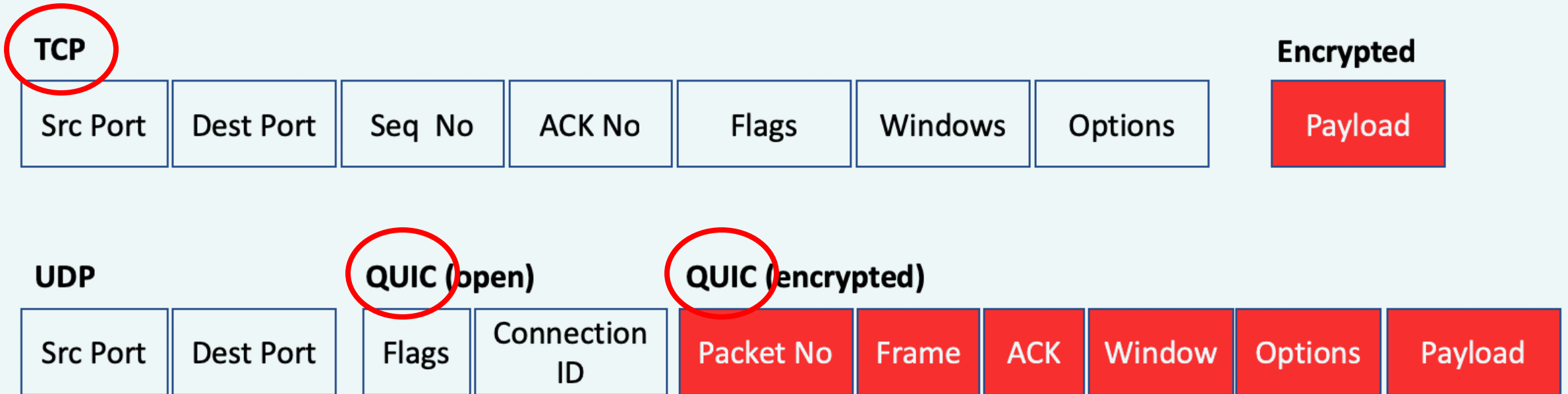
► Titkosítás: TLS és QUIC

- Belső titkosítási mechanizmus TLS v1.3 szerint



1. QUIC (Quick UDP Internet Connections) mechanizmus dióhéjban

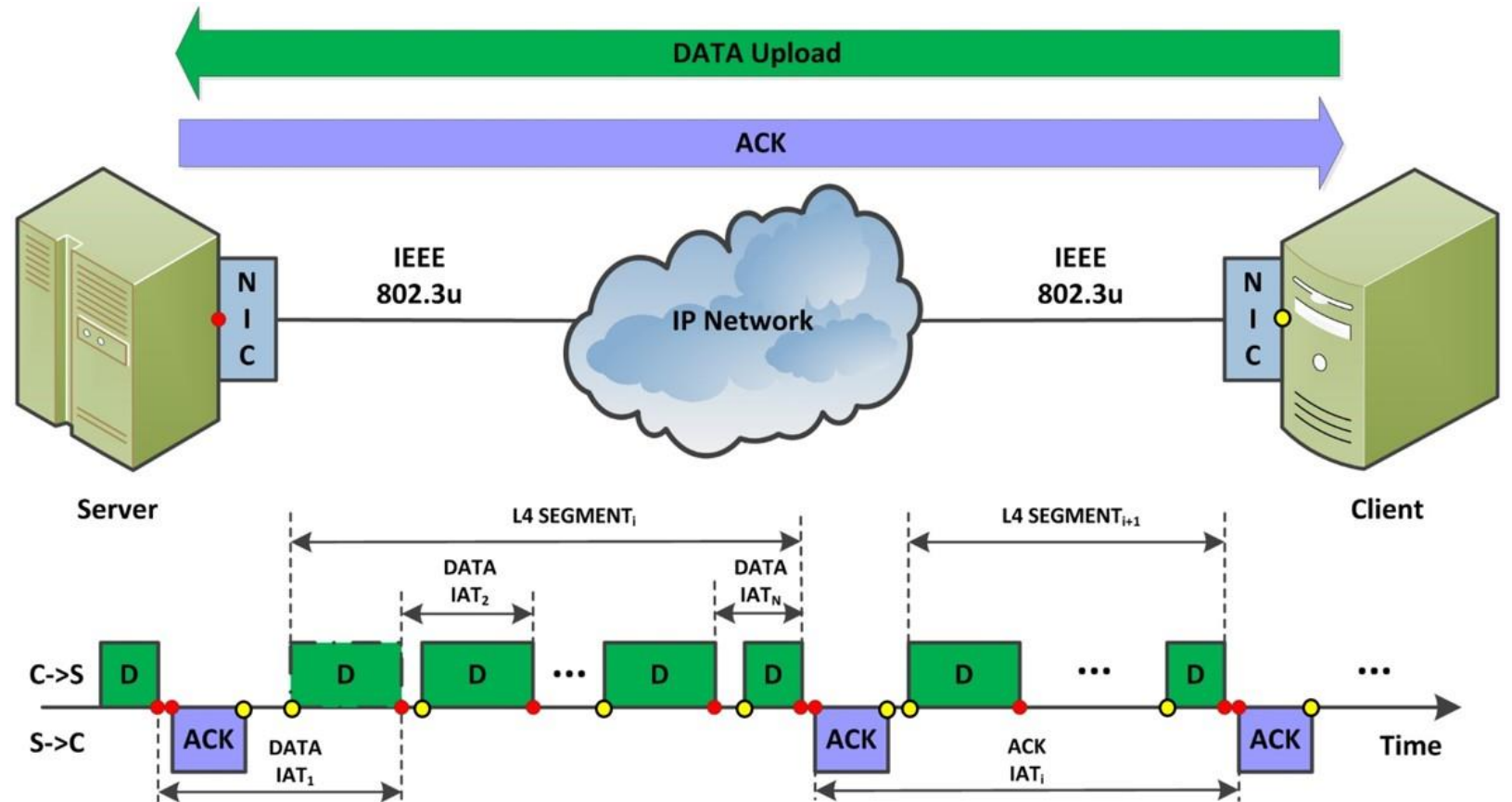
► Tartalom titkosítás: TCP vs. QUIC



2. QUIC forgalom mérések és teljesítmény tapasztalások

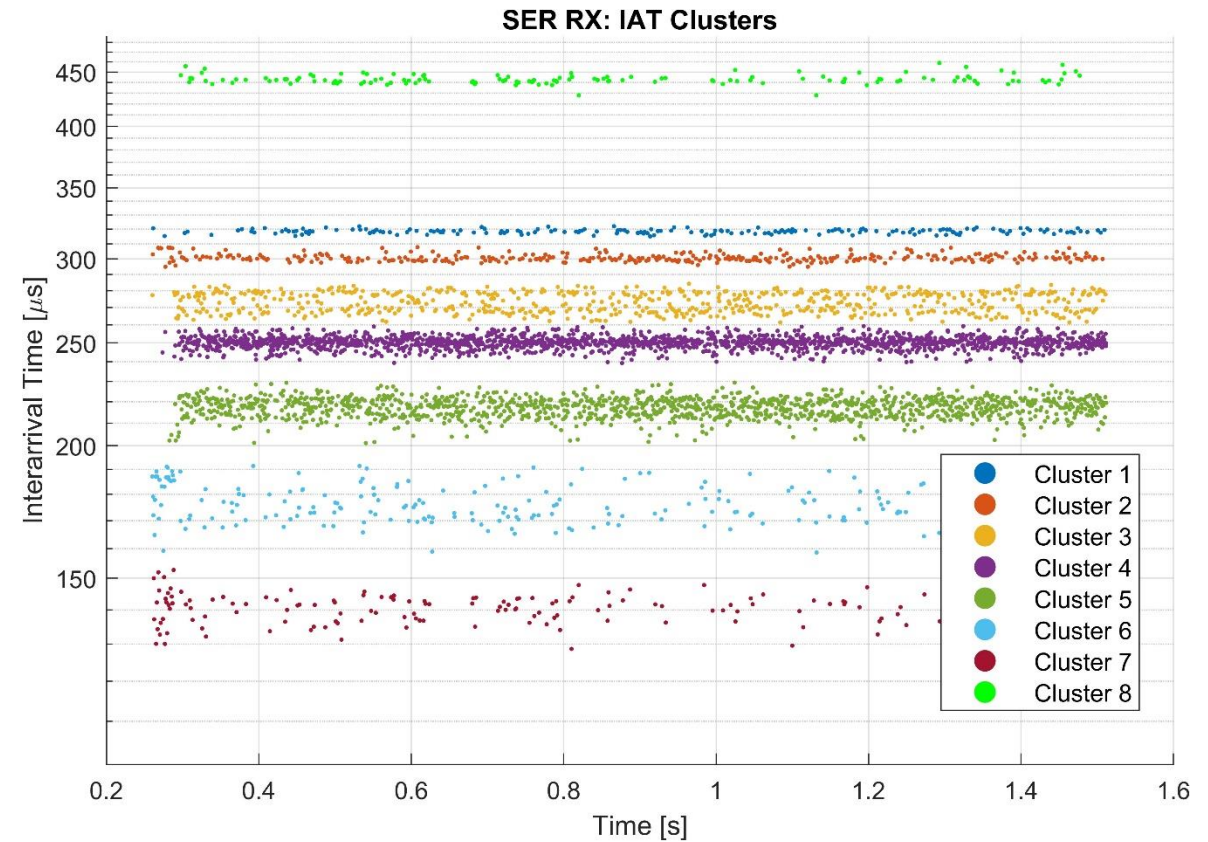
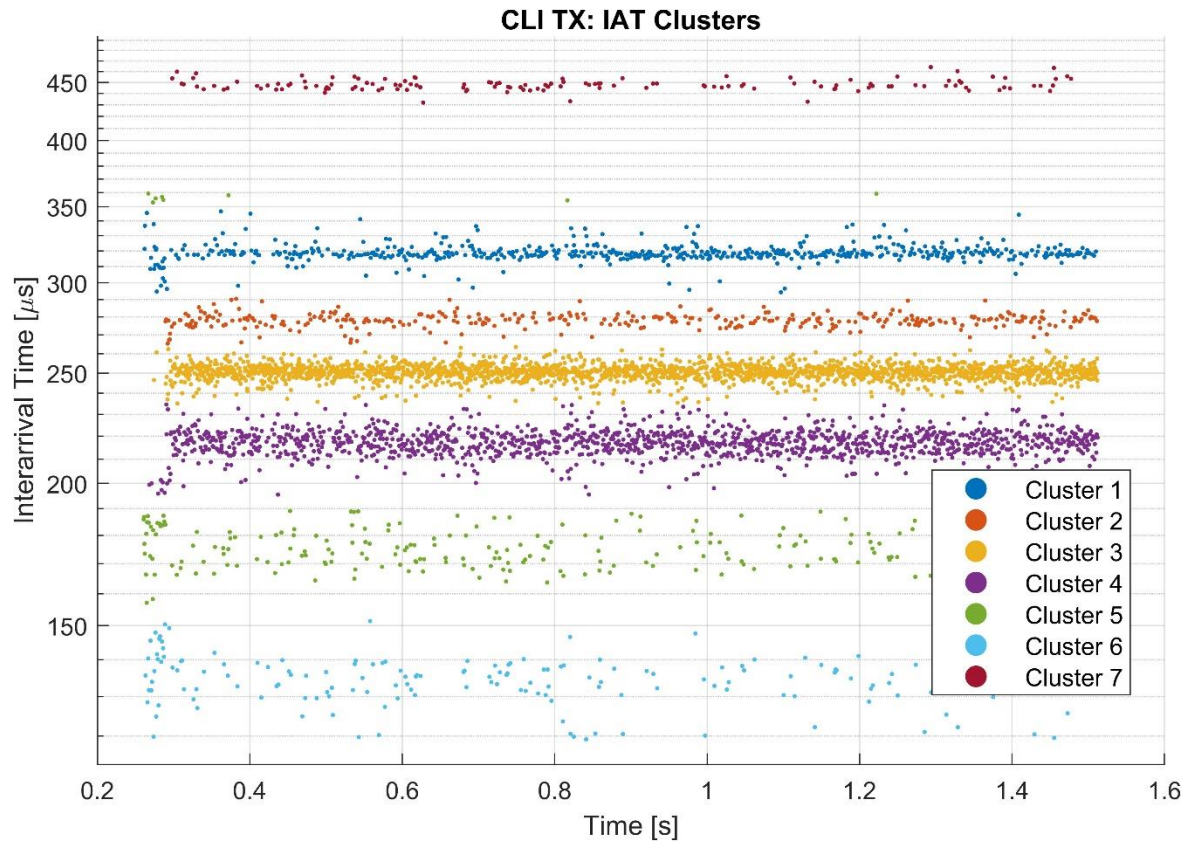
► Mérési scenárió:

- QUIC típus: Picoquic (Linux és Windows, de minimális implementáció)
- Kliensről 10 MB-os fájl feltöltése szerverre
- Független paraméterek: MTU, SSize, Bw
- Mért értékek: keretméret, beérkezési idő
- Elemzett mennyiség: beérkezési időköz (IAT)



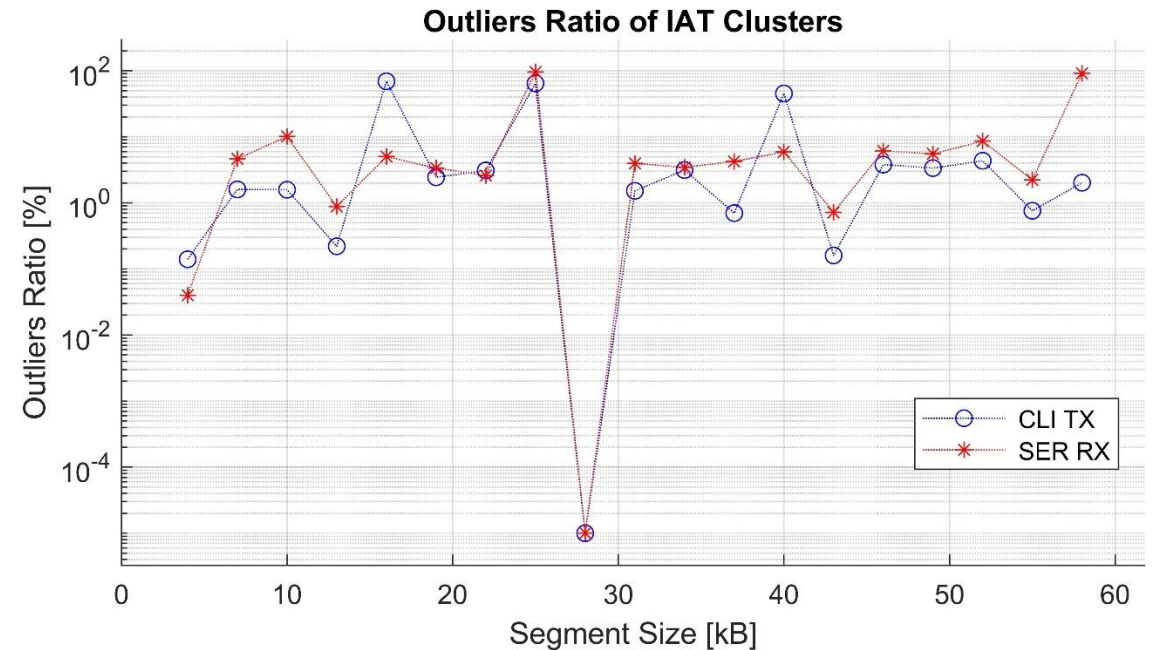
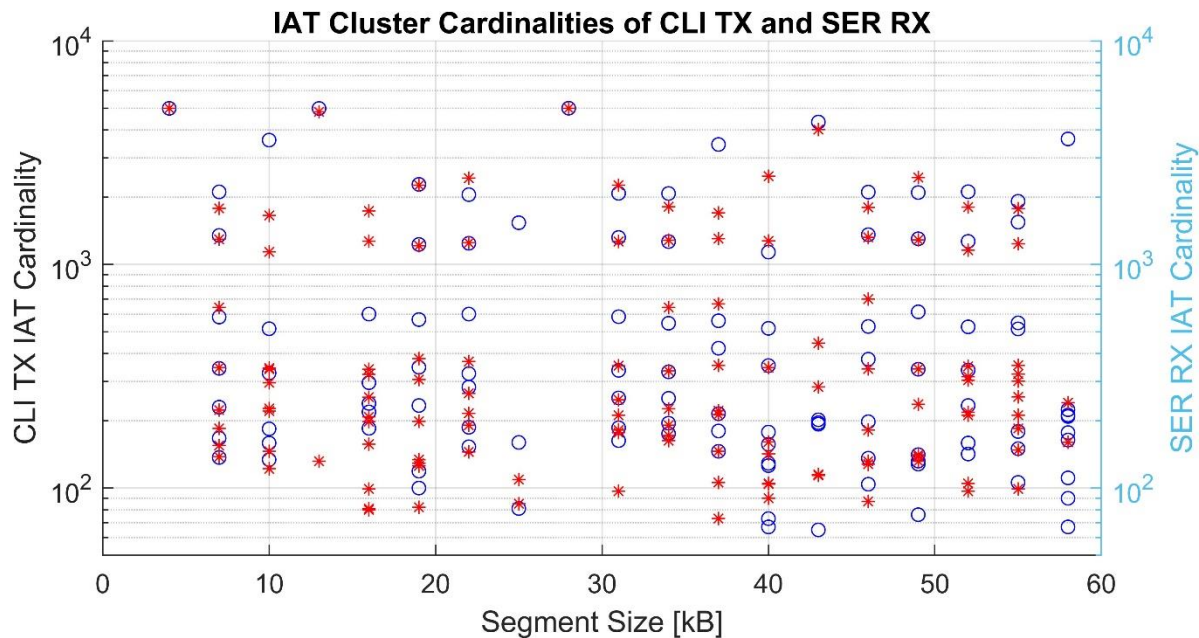
2. QUIC forgalom mérések és teljesítmény tapasztalások

► Az IAT időközök klasztereződése, (MTU, Bw, SSize) = (1500 B, 46 %, 7 kB):



2. QUIC forgalom mérések és teljesítmény tapasztalások

► Az IAT időközök klasztereződése (MTU, Bw) = (1500 B, 46 %): kardinalitás, kiugrók



2. QUIC forgalom mérések és teljesítmény tapasztalások

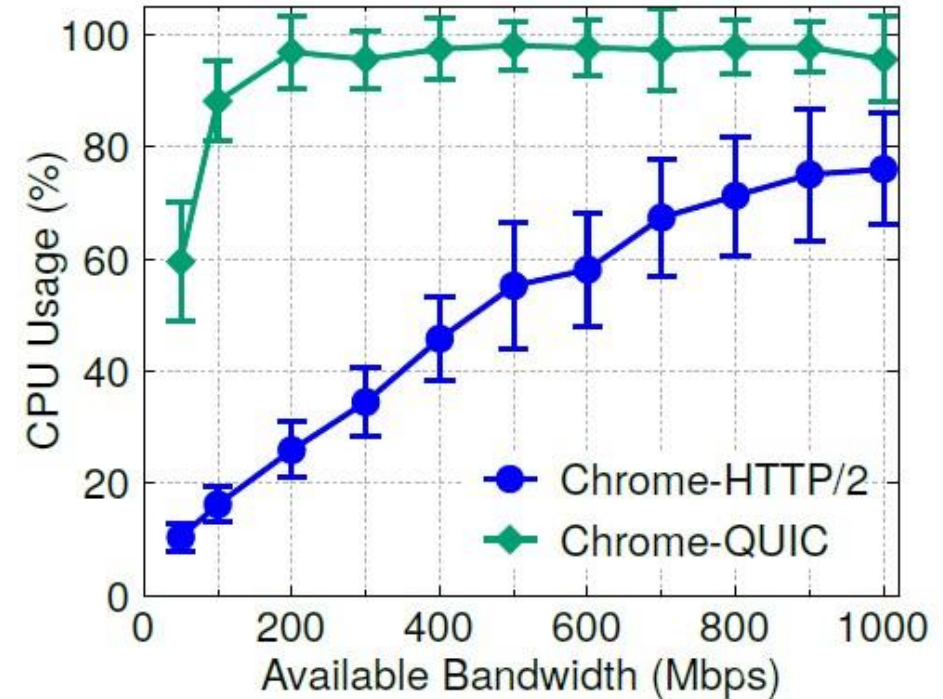
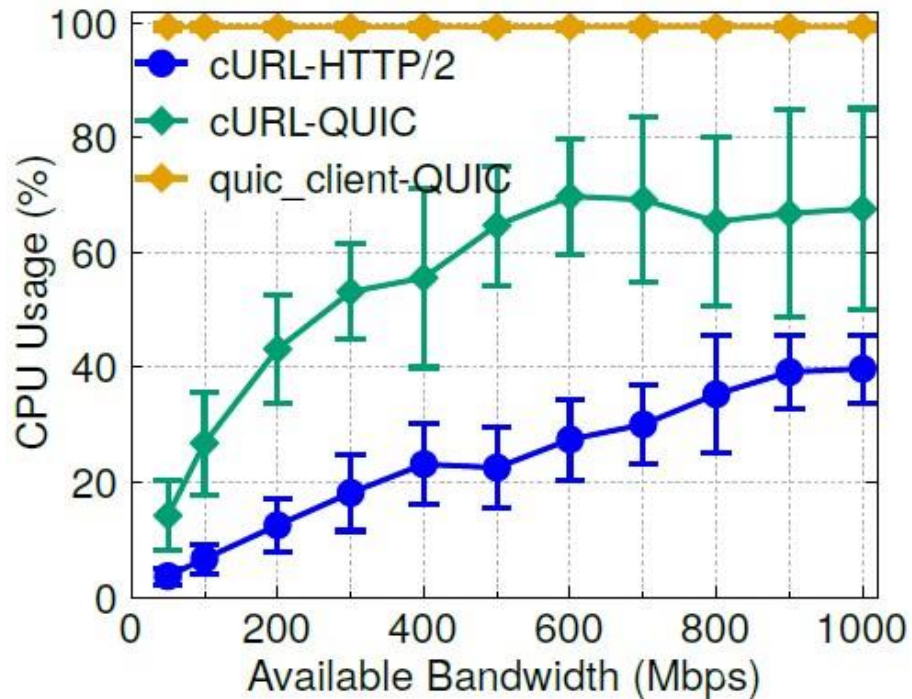
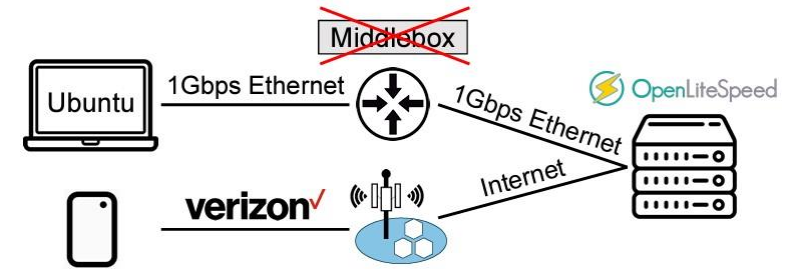
► Performancia jellemzők (2024): QUIC

QUIC is not Quick Enough over Fast Internet

Authors: Xumiao Zhang, Shuowei Jin, Yi He, Ahmad Hassan, Z. Morley Mao, Feng Qian, Zhi-Li Zhang | [Authors Info & Claims](#)

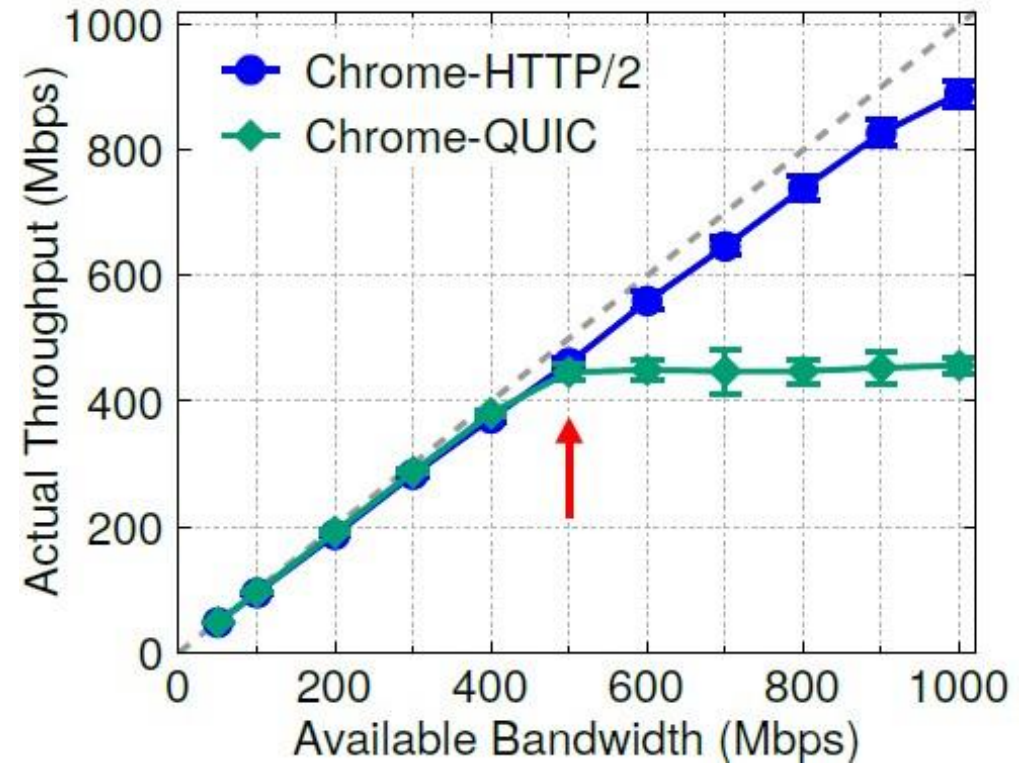
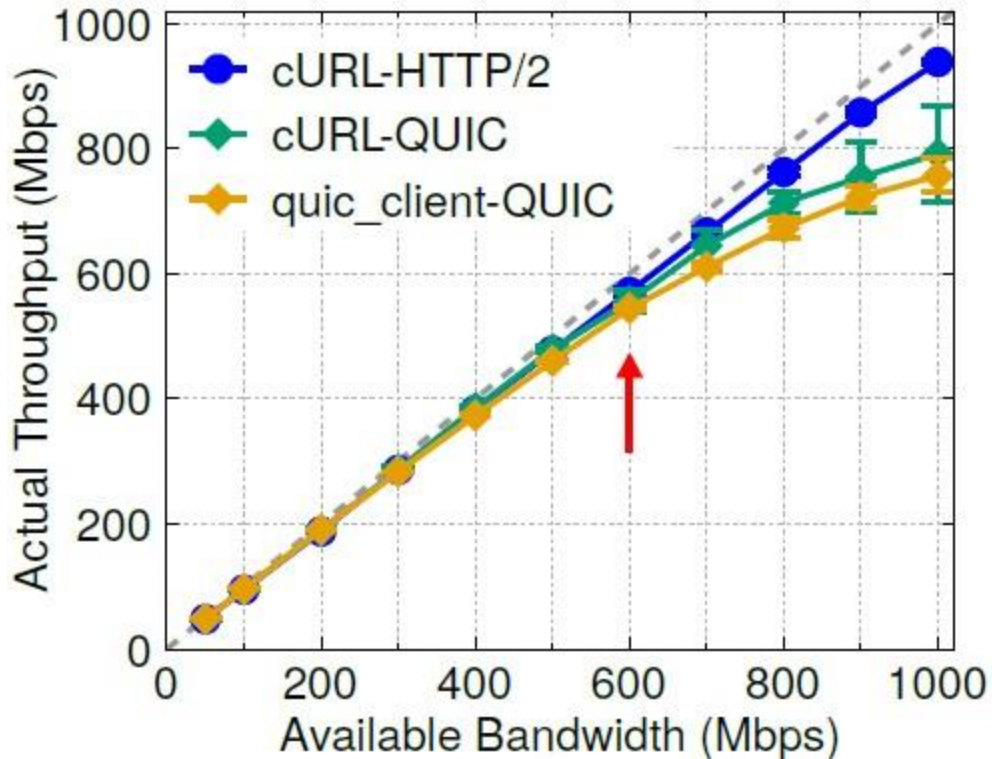
WWW '24: Proceedings of the ACM Web Conference 2024 • Pages 2713 - 2722 • <https://doi.org/10.1145/3589334.3645323>

Published: 13 May 2024 [Publication History](#)



2. QUIC forgalom mérések és teljesítmény tapasztalások

► Performancia jellemzők (2024): QUIC



3. QUIC szolgáltatások a jelenlegi gyakorlatban

► Elterjedtség (2024.09.17.): QUIC, HTTP/3

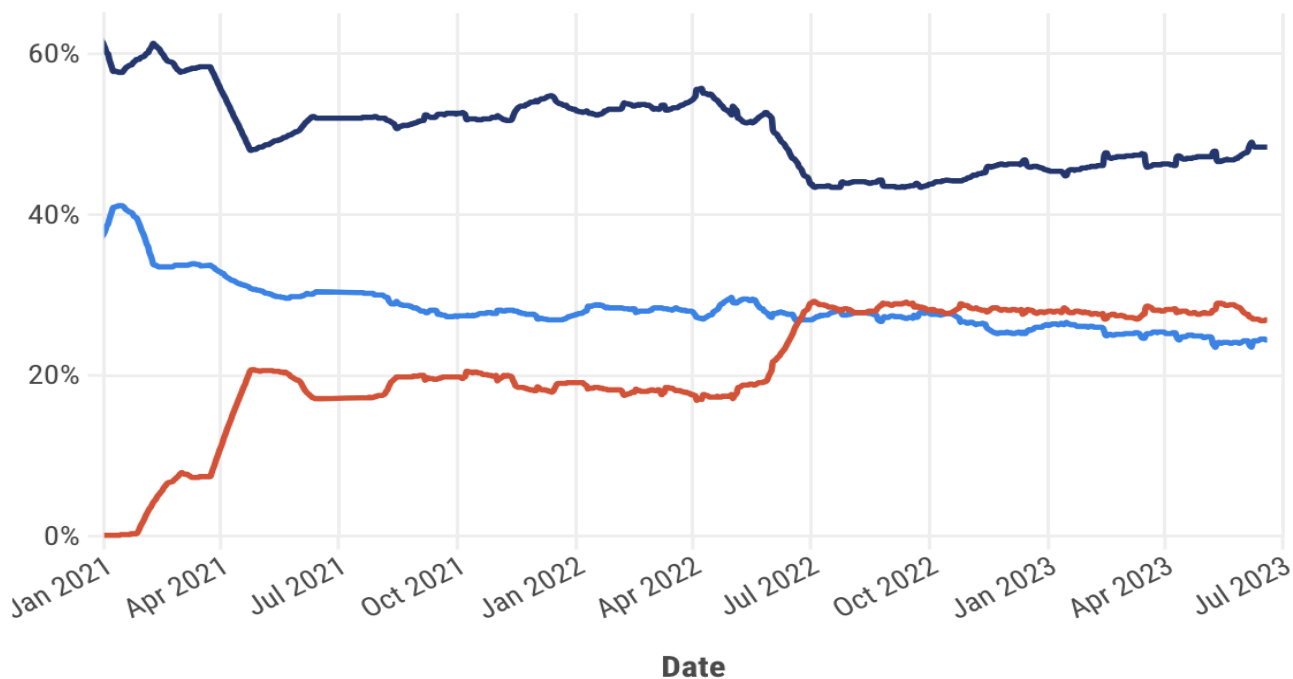
- Szolgáltatók:
 - Google
 - Youtube
 - Uber
 - Whatsapp
 - Facebook, Messenger
 - Stb. (egyre többen)

H/3 Adoption Grows Rapidly

HTTP Versions In Use 2021 - 2023

HTTP Version ■ v1.1 ■ v2.0 ■ v3.0

Percentage



Datasource:
Mozilla

 Internet Society
Pulse

4. QUIC demó

▶ 1. Wireshark capture: QUIC, HTTP/3

The image shows a Wireshark capture of QUIC traffic. The top pane displays a list of packets with columns for No., Time, Delta, Source, Destination, Protocol, Length, and Info. The bottom pane shows the details of a selected packet (No. 764), including Ethernet II, Internet Protocol Version 6, and User Datagram Protocol. The QUIC IETF section is expanded, showing connection information and expert info. The hex data pane on the right shows the raw bytes of the packet.

| No. | Time | Delta | Source | Destination | Protocol | Length | Info |
|-----|----------|----------|-------------------------|-------------------------|----------|--------|--|
| 470 | 1.808736 | 0.000066 | 2001:738:3000:24c0::... | 2a00:1450:400d:806::... | QUIC | | 1292 Initial, DCID=3379fd1a2c92d538, PKN: 1, CRYPTO |
| 471 | 1.808816 | 0.000080 | 2001:738:3000:24c0::... | 2a00:1450:400d:806::... | QUIC | | 1292 Initial, DCID=3379fd1a2c92d538, PKN: 2, CRYPTO |
| 472 | 1.808835 | 0.000019 | 2001:738:3000:24c0::... | 2a00:1450:400d:806::... | QUIC | | 1292 Initial, DCID=3379fd1a2c92d538, PKN: 3, PADDING, CRYPTO, PADDING, PING, CRYPTO, PING, PING, CRYPTO, CRYPTO, PADDING, CRYPTO, PADDING, PING, PING, PADDING |
| 473 | 1.808969 | 0.000134 | 2001:738:3000:24c0::... | 2a00:1450:400d:806::... | QUIC | | 139 0-RTT, DCID=3379fd1a2c92d538 |
| 589 | 1.813735 | 0.000210 | 2a00:1450:400d:806::... | 2001:738:3000:24c0::... | QUIC | | 1292 Initial, SCID=f379fd1a2c92d538, PKN: 1, ACK, PADDING |
| 590 | 1.813895 | 0.000160 | 2a00:1450:400d:806::... | 2001:738:3000:24c0::... | QUIC | | 1292 Initial, SCID=f379fd1a2c92d538, PKN: 2, ACK, PADDING |
| 592 | 1.815046 | 0.000142 | 2001:738:3000:24c0::... | 2a00:1450:400d:806::... | QUIC | | 1292 Initial, DCID=f379fd1a2c92d538, PKN: 6, PADDING, PING, PADDING |
| 760 | 1.826355 | 0.007025 | 2a00:1450:400d:806::... | 2001:738:3000:24c0::... | QUIC | | 1292 Initial, SCID=f379fd1a2c92d538, PKN: 3, ACK, PADDING |

Frame 764: 369 bytes on wire (2952 bits), 369 bytes captured (2952 bits) on interface \Device\NPF_{89E70809-8531-47F7-A9EF-388F797F6113}, id 0
Ethernet II, Src: Cisco_27:8d:3f (30:e4:db:27:8d:3f), Dst: MicroStarINT_d2:3c:9b (04:7c:16:d2:3c:9b)
Internet Protocol Version 6, Src: 2a00:1450:400d:806::200a, Dst: 2001:738:3000:24c0:a586:d745:d916:866b
User Datagram Protocol, Src Port: 443, Dst Port: 59287

QUIC IETF
QUIC Connection information
[Packet Length: 241]
... = Header Form: Long Header (1)
... = Fixed Bit: True
... = Packet Type: Handshake (2)
Version: 1 (0x00000001)
Destination Connection ID Length: 0
Source Connection ID Length: 8
Source Connection ID: f379fd1a2c92d538
Length: 224

[Expert Info (Warning/Decryption): Failed to create decryption context: Secrets are not available]
[Failed to create decryption context: Secrets are not available]
[Severity level: Warning]
[Group: Decryption]
Remaining Payload [...]: 1605ac43d096fb19fac2c05fe423d9e0916a034dc9ce2598585d6c34f17d0a59bc9d1f31ad653dba87ab15169e4332abaa2b64eb05b1677ba371a8e32157cfc95d5c884e413b634a601c

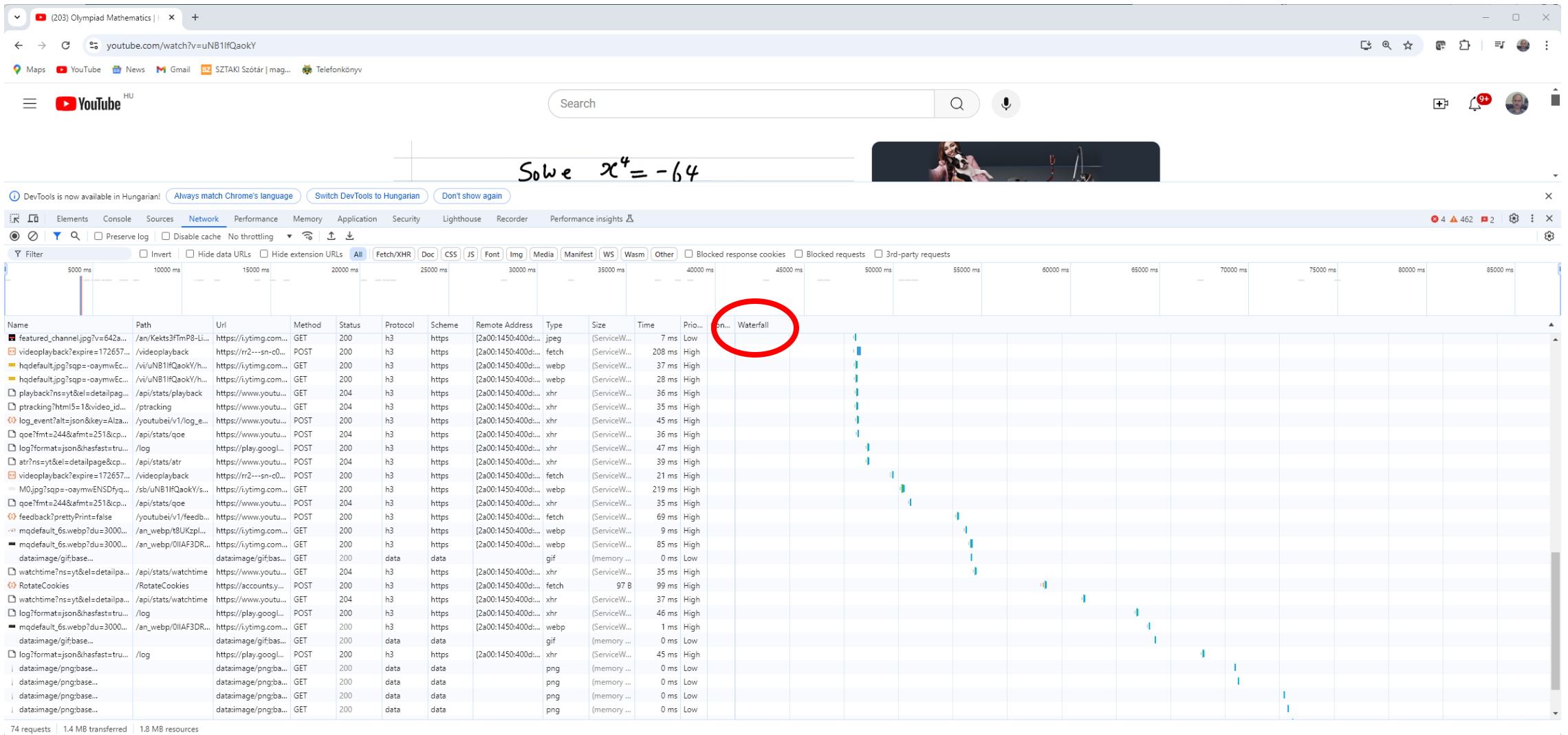
QUIC IETF
QUIC Short Header
[Packet Length: 66]
... = Header Form: Short Header (0)
... = Fixed Bit: True
... = Spin Bit: False

[Expert Info (Warning/Decryption): Failed to create decryption context: Secrets are not available]
[Failed to create decryption context: Secrets are not available]
[Severity level: Warning]
[Group: Decryption]
Remaining Payload: 21b7dcdf399d7fb24ac1b198484911feed8e5781619c0f4b23da73c4d982294c223da5af1c3a1349a267de7280c2722bf7f8811d5c02434238e7613c911a51df43

0000 04 7c 16 d2 3c 9b 30 e4 db 27 8d 3f 86 dd 68 00 | |<0-?~h
0010 00 00 01 3b 11 38 2a 00 14 50 40 0d 08 06 00 00 | ;8*~P@~
0020 00 00 00 20 0a 20 01 07 38 30 00 24 c0 a5 86 | ~~~~80\$~
0030 d7 45 d9 16 86 6b 01 bb e7 97 01 3b 4f b4 e8 00 | E~k~;~;0~
0040 00 00 01 00 08 f3 79 fd 1a 2c 92 d5 38 40 e0 16 | ~~~~~y~;#@~
0050 05 ac 43 d0 96 fb 19 fa c2 c0 5f e4 23 d9 e0 91 | ~C~...~#~
0060 6a 03 4d c9 ce 25 98 58 5d 6c 34 f1 7d 0a 59 bc | j~M~%~X~]14~}~Y~
0070 9d 1f 31 ad 65 3d ba 87 ab 15 16 9e 43 32 ab aa | ~1~e~...~C2~
0080 2b 64 eb 05 b1 67 7b a3 71 a8 e3 21 57 cf c9 5d | +d~g{~q~!W~
0090 5c 88 4e 41 3b 63 4a 60 1c d3 3a e9 47 6a 73 82 | \~NA;c~}~...Gjs~
00a0 b5 a7 19 ac 1c 8b 74 0d 34 ee b6 bb 37 23 ac 0f | ~~~~~t~4~7#~
00b0 0d 5a 9d 81 2e 60 9c d3 62 d7 84 31 85 2d 44 20 | ~Z~...~b~1~D~
00c0 21 6b 68 b2 c4 50 af 42 7c 58 c4 40 6d cd 23 a1 | !kh~P~B~|X~@~#~
00d0 bc 02 a2 c8 b8 48 85 bd d3 a6 2a 63 4d a0 1e bb | ~~~~~H~...*cN~
00e0 8b 4c 68 aa c1 75 d1 db 54 1b d8 1c 22 10 d1 cf | ~Lh~u~T~...~
00f0 1b 64 cd 42 a6 23 7d 83 ab bd 8d c2 e2 3d e1 6e | ~d~B~#~}~...~n~
0100 9a d2 96 54 66 a3 b9 c7 82 cf 4c b2 8b 08 86 d7 | ~...Tf~...~L~...~
0110 55 f1 86 df b4 6f 32 e3 51 69 f9 82 d4 45 c0 26 | U~...o2~Qi~...E&~
0120 28 05 30 f1 b3 8e a1 03 1f ab 1a 54 d0 0f 82 48 | (~0~...~T~...H~
0130 21 b7 dc af 39 9d 7f b2 4a c1 b1 98 48 49 11 fe | !~9~...~J~...HI~
0140 ad 8e 57 81 61 9c 0f 4b 23 da 73 c4 d9 82 29 4c | ~W~a~K~#~s~...~L~
0150 22 3d a5 af 1c 3a 13 49 a2 67 de 72 80 c2 72 2b | ~...~I~g~r~r~+~
0160 f7 f8 81 1d 5c 02 43 42 38 e7 61 3c 91 1a 51 df | ~...~\CB~8~a~<~Q~
0170 43 | C

4. QUIC demó

► 2. Chrome waterfall: QUIC, HTTP3



4. QUIC demó

▶ 3. Web szerver tesztelés: QUIC, HTTP3

The screenshot shows the 'HTTP/3 CHECK' website interface. The URL 'fad12.fad.klte.hu' is entered in the search box. The results section shows two green checkmarks: '✓ QUIC is supported' and '✓ HTTP/3 is supported', both of which are circled in red. Below this, a table displays connection metrics for two different connection IDs.

| CONNECTION ID | PACKET RX | HANDSHAKE DONE |
|---------------|-----------|----------------|
| E012868FBA... | 106.982 | 108.099 |
| 340DC33C61... | 106.727 | 107.124 |

HTTP Header

```
HTTP/1.1 200 OK
server: nginx/1.26.2
date: Tue, 17 Sep 2024 06:49:17 GMT
content-type: text/html
content-length: 1000
last-modified: Wed, 28 Aug 2024 17:07:42 GMT
alt-svc: h3=":443"; ma=86400
```

Certificate Chain

Domain: fad12.fad.klte.hu
Issued By: E5
Expires: Thursday, November 28, 2024 at 11:55:24 AM GMT
✓ This certificate is valid

SUBJECT
Common Name: fad12.fad.klte.hu

ISSUER
Country: US
Organization: Let's Encrypt
Common Name: E5

Serial Number: 309550139080335664085260267806231912297331
Signature Algorithm: ecdsa-with-SHA384
Version:

Public Key Bits: 256
Public Key Type: DSA



QUIC

Köszönöm a figyelmet!

gal.zoltan@inf.unideb.hu

Köszönetnyilvánítás: *Ezt a munkát a Debreceni Egyetem QoS-HPC-IoT Laboratórium támogatta.*