Achieving QUIC's Full Potential:

How a DNS Deployment Gap Is Limiting HTTP/3 Performance

NANOG 95

2-4 Feb 2026

Levente Csikor, Dinil Mon Divakaran

Institute for Infocomm Research (I2R)
A*STAR, Singapore

$ whoami

`name:`	Levi [Leh-VEE]
`background:`	Ph.D. (Hungary), research stints in UK, Brazil, and Singapore.
`role:`	Senior Scientist @ A*STAR, Singapore
`focus:`	Network security and privacy in next-generation networks
`passion:`	Privacy enthusiast → run my entire digital life off the cloud
`track rec.:`	Mostly academic, but a few Industry-focused events: - `Black Hat:` RollBack attack on automotive keyless entry systems - `OVS+OVN:` Algorithmic complexity attack on OVS
`why am i here:`	Traffic analysis → wireshark/PCAP → something was strange...

Motivation

The Fastest Protocol Nobody Can Find

Latency in the Modern Web

The Problem

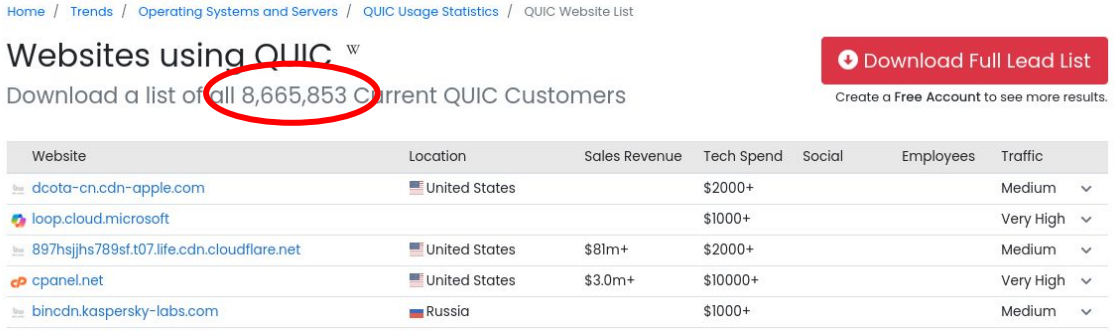
- Surprising number of packets and handshakes required to load a modern web page
- airbnb.com index page: **~6K packets…**
  - *…and it's not because of the media elements!*

The Paradox: it won't be getting any better!

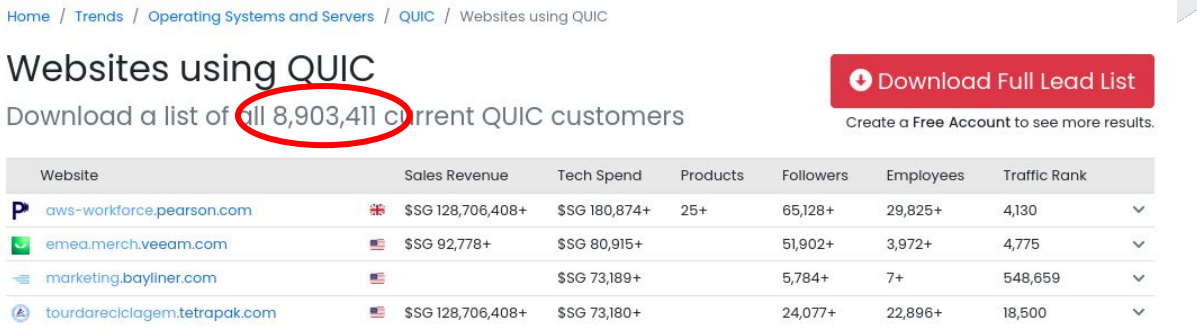
- Adoption of privacy & security-enhancing protocols (e.g., DoH, ECH)
  - more and more layers and handshakes → increased latency
- *How about QUIC?*

Promise and the Rise of QUIC and HTTP/3

- Transforming the web landscape
  - more than 8 million site already (try to) benefit from it*.



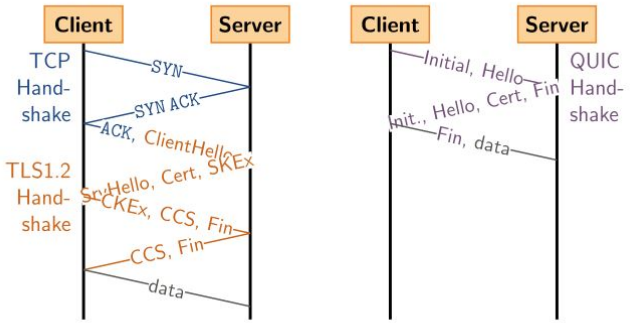
Sept 2025

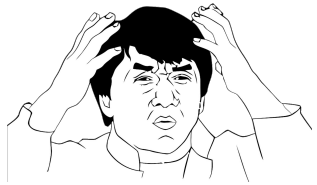


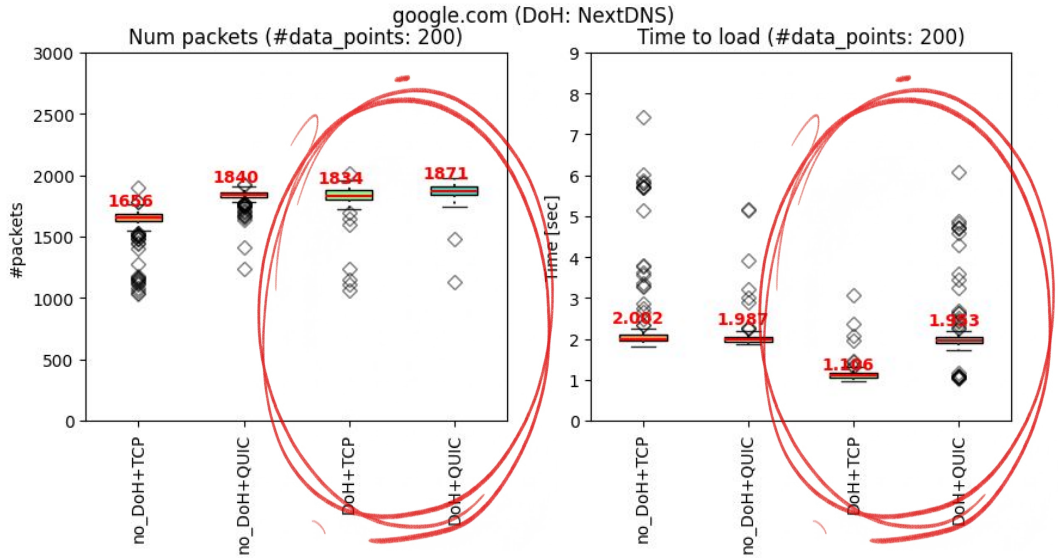
Jan 2026

Key improvements:

- no Head-of-Line blocking
- faster connection establishment
- Default encryption for enhanced security







It's the fastest protocol that's running late

*https://trends.builtwith.com/websitelist/QUIC

Background

Recent evolution of the underlying ecosystem

Enhanced privacy with DoH and ECH

- Along HTTPS evolution, DNS remained plain-text
  - Revealing sensitive information (i.e., the domain being visited)
  - **BUT:** many security/privacy/convenience solutions based on DNS
    - malicious domain block, ads, parental control, etc.

- Let us encrypt DNS:
  - DNS-over-TLS (2016)
  - DNS-over-HTTPS (2018)
  - DNS-over-QUIC / DNS-over-HTTP3 (2022)

There is still a privacy leak

- SNI in the TLS handshake (Client Hello) is still there

Solution

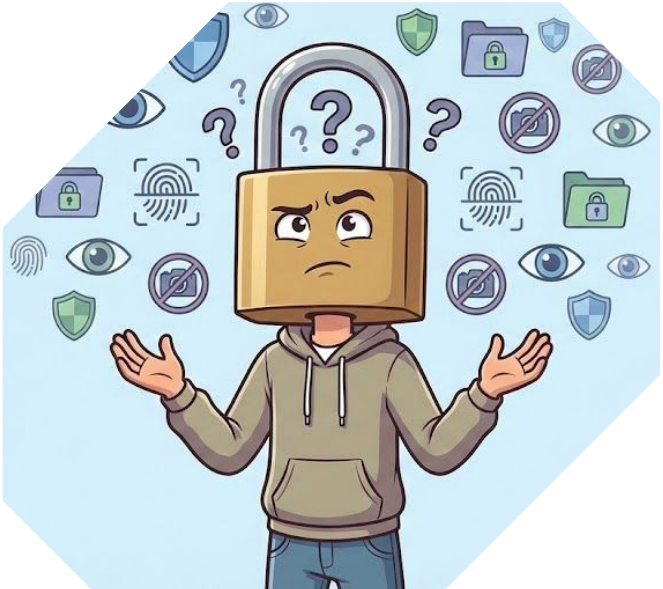
- TLS 1.3 + Encrypted Client Hello (ECH, 2020)
- (first proposed as eSNI in 2018)

Encrypted Client Hello and DNS HTTPS RR

- Encryption requires keys (to be distributed)
- Let's use DNS for that → **DNS HTTPS RR** (RFC 9460 in 2023)
  - (note: ECH for DoH: chicken-and-egg problem)

Nowadays:

- "crazy-privacy" mode in your browser (e.g., DoH, ECH)
  - DNS HTTPS records are queried
- why "crazy privacy"?
  - If you don't encrypt DNS, why use ECH?



Evolution of HTTPS records

- DNS HTTPS records were evolving
- not only for “crazy-privacy” mode but:
  - *“Providing alternative endpoints.”*
  - *“Supporting non-default TCP and UDP ports.”*
  - *“Providing an indication signaling that the "https" scheme should be used.”*
  - ***“Connecting directly to HTTP/3 (QUIC transport)”.***

If the standards are there, why do we need so many packets to be exchanged?

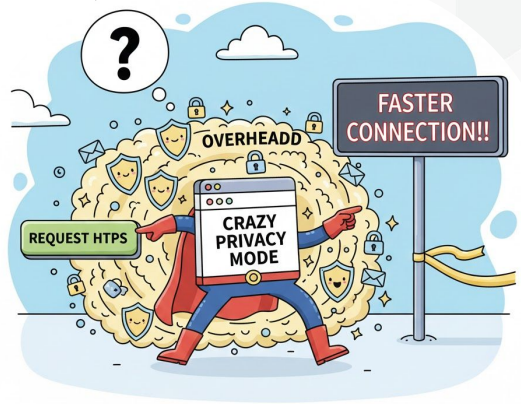
Persistent Challenges in Web Security and Performance

ECH implementation paradox, DNS knowledge gap, QUIC vs TCP, efficiency dilemma

Security vs. Performance

ECH implementation paradox

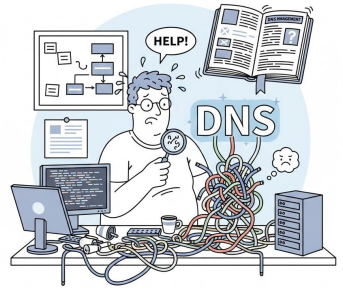
- Ironic twist:
  - browsers request HTTPS records in “crazy privacy” mode *only*
  - additional security and privacy layers introduced
  - **to achieve faster connections ???**



Ironally: More Privacy = More Speed???

DNS knowledge gap

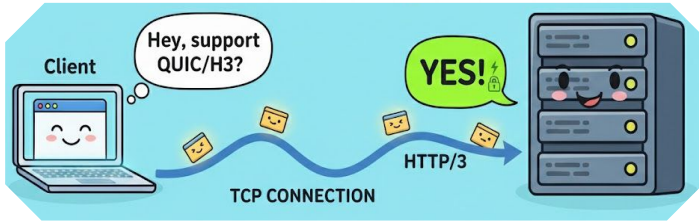
- website administrators often lack expertise in DNS management
- HTTP/3 indicators not received in advance



DNS MANAGEMENT CHALLENGES

QUIC vs TCP Efficiency dilemma

- determining QUIC availability takes longer than simply using TCP and HTTP/2
- Contradicts the primary objective to enhance speed



State-of-the-art

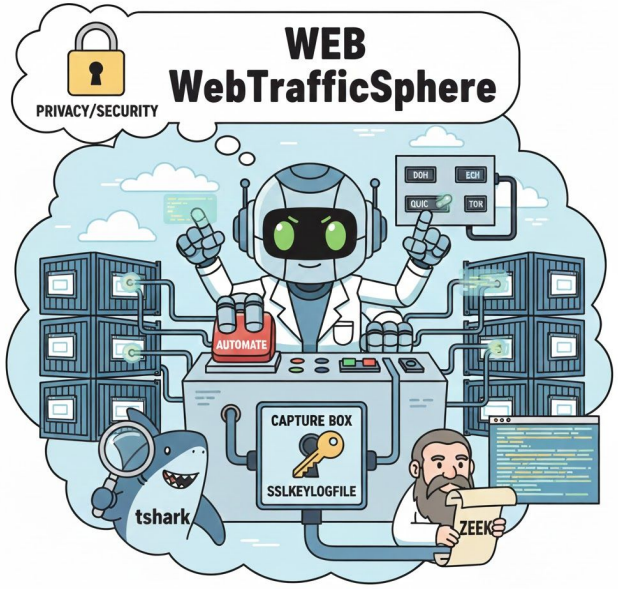
Deep-dive into a packet trace

Introducing WebTrafficSphere

Introducing WebTrafficSphere

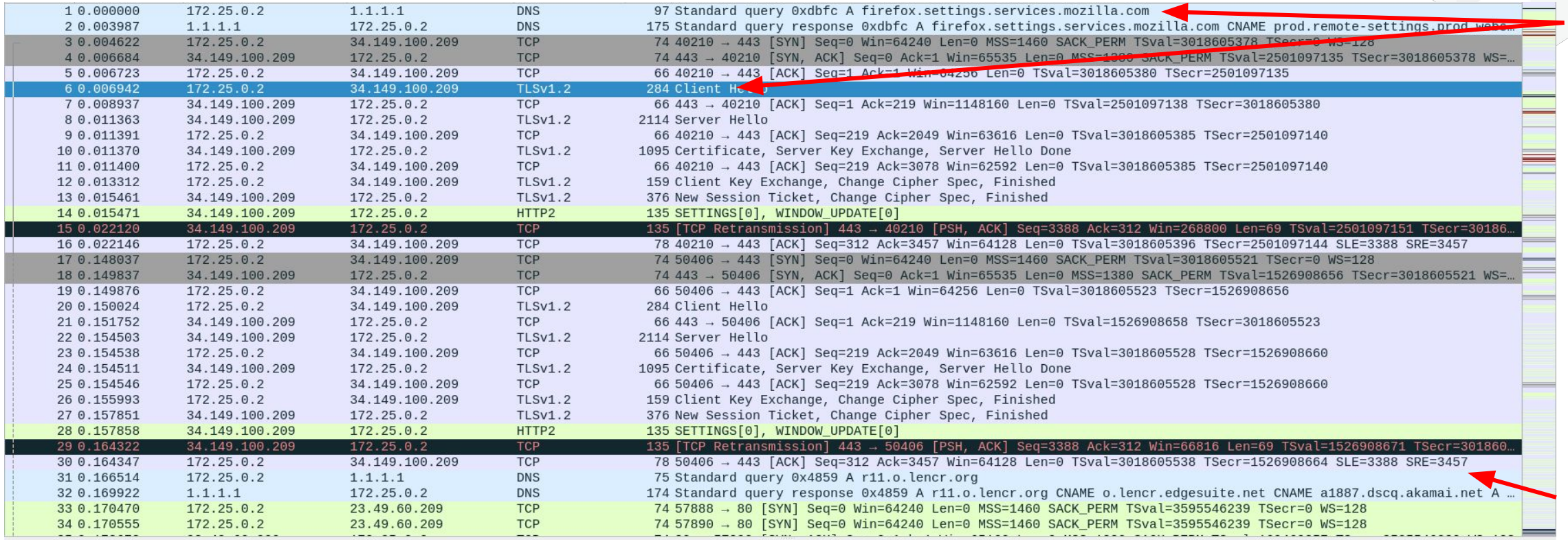
Our *open-source tool* to address the analysis challenge

- Automating website visits with configurable privacy/security settings
- Containerized to eliminate background noise
- Highly configurable (toggle DoH, QUIC, ECH, or even Tor)
- Capture full packet traces with encryption keys
- Process PCAP files with *tshark* and *Zeek*



Traffic trace breakdown: airbnb.com

From a fresh browser start – some examples are highlighted



1	0.000000	172.25.0.2	1.1.1.1	DNS	97 Standard query 0xdbfc A firefox.settings.services.mozilla.com
2	0.003987	1.1.1.1	172.25.0.2	DNS	175 Standard query response 0xdbfc A firefox.settings.services.mozilla.com CNAME prod.remote-settings.prod.webs…
3	0.004622	172.25.0.2	34.149.100.209	TCP	74 40210 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3018605378 TSecr=0 WS=128
4	0.006684	34.149.100.209	172.25.0.2	TCP	74 443 → 40210 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1380 SACK_PERM TSval=2501097135 TSecr=3018605378 WS=…
5	0.006723	172.25.0.2	34.149.100.209	TCP	66 40210 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3018605380 TSecr=2501097135
6	0.006942	172.25.0.2	34.149.100.209	TLSv1.2	284 Client Hello
7	0.008937	34.149.100.209	172.25.0.2	TCP	66 443 → 40210 [ACK] Seq=1 Ack=219 Win=1148160 Len=0 TSval=2501097138 TSecr=3018605380
8	0.011363	34.149.100.209	172.25.0.2	TLSv1.2	2114 Server Hello
9	0.011391	172.25.0.2	34.149.100.209	TCP	66 40210 → 443 [ACK] Seq=219 Ack=2049 Win=63616 Len=0 TSval=3018605385 TSecr=2501097140
10	0.011370	34.149.100.209	172.25.0.2	TLSv1.2	1095 Certificate, Server Key Exchange, Server Hello Done
11	0.011400	172.25.0.2	34.149.100.209	TCP	66 40210 → 443 [ACK] Seq=219 Ack=3078 Win=62592 Len=0 TSval=3018605385 TSecr=2501097140
12	0.013312	172.25.0.2	34.149.100.209	TLSv1.2	159 Client Key Exchange, Change Cipher Spec, Finished
13	0.015461	34.149.100.209	172.25.0.2	TLSv1.2	376 New Session Ticket, Change Cipher Spec, Finished
14	0.015471	34.149.100.209	172.25.0.2	HTTP2	135 SETTINGS[0], WINDOW_UPDATE[0]
15	0.022120	34.149.100.209	172.25.0.2	TCP	135 [TCP Retransmission] 443 → 40210 [PSH, ACK] Seq=3388 Ack=312 Win=268800 Len=69 TSval=2501097151 TSecr=30186…
16	0.022146	172.25.0.2	34.149.100.209	TCP	78 40210 → 443 [ACK] Seq=312 Ack=3457 Win=64128 Len=0 TSval=3018605396 TSecr=2501097144 SLE=3388 SRE=3457
17	0.148037	172.25.0.2	34.149.100.209	TCP	74 50406 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3018605521 TSecr=0 WS=128
18	0.149837	34.149.100.209	172.25.0.2	TCP	74 443 → 50406 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1380 SACK_PERM TSval=1526908656 TSecr=3018605521 WS=…
19	0.149876	172.25.0.2	34.149.100.209	TCP	66 50406 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3018605523 TSecr=1526908656
20	0.150024	172.25.0.2	34.149.100.209	TLSv1.2	284 Client Hello
21	0.151752	34.149.100.209	172.25.0.2	TCP	66 443 → 50406 [ACK] Seq=1 Ack=219 Win=1148160 Len=0 TSval=1526908658 TSecr=3018605523
22	0.154503	34.149.100.209	172.25.0.2	TLSv1.2	2114 Server Hello
23	0.154538	172.25.0.2	34.149.100.209	TCP	66 50406 → 443 [ACK] Seq=219 Ack=2049 Win=63616 Len=0 TSval=3018605528 TSecr=1526908660
24	0.154511	34.149.100.209	172.25.0.2	TLSv1.2	1095 Certificate, Server Key Exchange, Server Hello Done
25	0.154546	172.25.0.2	34.149.100.209	TCP	66 50406 → 443 [ACK] Seq=219 Ack=3078 Win=62592 Len=0 TSval=3018605528 TSecr=1526908660
26	0.155993	172.25.0.2	34.149.100.209	TLSv1.2	159 Client Key Exchange, Change Cipher Spec, Finished
27	0.157851	34.149.100.209	172.25.0.2	TLSv1.2	376 New Session Ticket, Change Cipher Spec, Finished
28	0.157858	34.149.100.209	172.25.0.2	HTTP2	135 SETTINGS[0], WINDOW_UPDATE[0]
29	0.164322	34.149.100.209	172.25.0.2	TCP	135 [TCP Retransmission] 443 → 50406 [PSH, ACK] Seq=3388 Ack=312 Win=66816 Len=69 TSval=1526908671 TSecr=301860…
30	0.164347	172.25.0.2	34.149.100.209	TCP	78 50406 → 443 [ACK] Seq=312 Ack=3457 Win=64128 Len=0 TSval=3018605538 TSecr=1526908664 SLE=3388 SRE=3457
31	0.166514	172.25.0.2	1.1.1.1	DNS	75 Standard query 0x4859 A r11.o.lencr.org
32	0.169922	1.1.1.1	172.25.0.2	DNS	174 Standard query response 0x4859 A r11.o.lencr.org CNAME o.lencr.edgesuite.net CNAME a1887.dscq.akamai.net A …
33	0.170470	172.25.0.2	23.49.60.209	TCP	74 57888 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3595546239 TSecr=0 WS=128
34	0.170555	172.25.0.2	23.49.60.209	TCP	74 57890 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3595546239 TSecr=0 WS=128

```
▸ Frame 6: 284 bytes on wire (2272 bits), 284 bytes captured (2272 bits)
▸ Ethernet II, Src: c2:cf:f0:d2:00:9b (c2:cf:f0:d2:00:9b), Dst: e6:c1:4b:dc:0c:54 (e6:c1:4b:dc:0c:54)
▸ Internet Protocol Version 4, Src: 172.25.0.2, Dst: 34.149.100.209
▸ Transmission Control Protocol, Src Port: 40210, Dst Port: 443, Seq: 1, Ack: 1, Len: 218
▾ Transport Layer Security
  ▾ TLSv1.2 Record Layer: Handshake Protocol: Client Hello
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 213
    ▾ Handshake Protocol: Client Hello
        Handshake Type: Client Hello (1)
        Length: 209
```

```
0000  e6 c1 4b dc 0c 54 c2 cf  f0 d2 00 9b 08 00 45 00   ··K··T·· ·····E·
0010  01 0e 96 e9 40 00 40 06  6f 7f ac 19 00 02 22 95   ····@·@· o·····"·
0020  64 d1 9d 12 01 bb 34 7a  6f 8e 6c 8b a5 c5 80 18   d·····4z o·l·····
0030  01 f6 3d 57 00 00 01 01  08 0a b3 ec 43 44 95 13   ··=W···· ····CD··
0040  b6 af 16 03 01 00 d5 01  00 00 d1 03 03 1b d0 2e   ········ ········.
0050  c4 93 37 29 17 e9 01 7c  6c 53 b4 ba 32 1b 80 fe   ··7)···| lS··2···
0060  cf 41 1c d8 3d b4 9f ed  02 5f ef 7e 6e 00 00 1c   ·A··=··· ·_·~n···
0070  c0 2b c0 2f cc a9 cc a8  c0 2c c0 30 c0 0a c0 09   ·+·/···· ·,·0····
0080  c0 13 c0 14 00 9c 00 9d  00 2f 00 35 01 00 00 8c   ········ ·/·5····
0090  00 00 00 2a 00 28 00 00  25 66 69 72 65 66 6f 78   ···*·(·· %firefox
00a0  2e 73 65 74 74 69 6e 67  73 2e 73 65 72 76 69 63   .setting s.servic
00b0  65 73 2e 6d 6f 7a 69 6c  6c 61 2e 63 6f 6d 00 17   es.mozil la.com··
```

connecting to firefox services

DNS for Let's Encrypt for OCSP

First DNS query and redirection

First DNS query for airbnb.com (#211)

208	1.203253	172.25.0.2	52.24.225.206	TCP	66	48488 → 443 [ACK] Seq=1733 Ack=4937 Win=63616 Len=0 TSval=25136583 TSecr=2481343712
209	1.203524	172.25.0.2	52.24.225.206	TLSv1.2	97	Alert (Level: Warning, Description: Close Notify)
210	1.203566	172.25.0.2	52.24.225.206	TCP	66	48488 → 443 [FIN, ACK] Seq=1764 Ack=4937 Win=64128 Len=0 TSval=25136583 TSecr=2481343712
211	1.205649	172.25.0.2	1.1.1.1	DNS	70	Standard query 0x9e4b A airbnb.com
212	1.209172	1.1.1.1	172.25.0.2	DNS	118	Standard query response 0x9e4b A airbnb.com A 54.243.237.216 A 44.223.197.210 A 34.231.2.231
213	1.209316	172.25.0.2	1.1.1.1	DNS	95	Standard query 0xc246 A tracking-protection.cdn.mozilla.net

Once connected on port 80 → redirected to port 443 (#935)

932	1.461427	54.243.237.216	172.25.0.2	TCP	74	80 → 33368 [SYN, ACK] Seq=0 Ack=1 Win=62643 Len=0 MSS=1380 SACK_PERM TSval=3703402906 TSecr=1167552753 WS=5…
933	1.461466	172.25.0.2	54.243.237.216	TCP	66	33368 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1167553005 TSecr=3703402906
934	1.473784	34.231.2.231	172.25.0.2	TCP	66	80 → 36828 [ACK] Seq=1 Ack=375 Win=62464 Len=0 TSval=4178390682 TSecr=1788683306
935	1.473792	34.231.2.231	172.25.0.2	HTTP	481	HTTP/1.1 301 Moved Permanently (text/html)
936	1.473829	172.25.0.2	34.231.2.231	TCP	66	36828 → 80 [ACK] Seq=375 Ack=416 Win=64128 Len=0 TSval=1788683569 TSecr=4178390682
937	1.477137	172.25.0.2	1.1.1.1	DNS	70	Standard query 0xe3ef A airbnb.com
938	1.480617	1.1.1.1	172.25.0.2	DNS	118	Standard query response 0xe3ef A airbnb.com A 54.243.237.216 A 34.231.2.231 A 44.223.197.210
939	1.481227	172.25.0.2	54.243.237.216	TCP	74	59414 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1167553025 TSecr=0 WS=128
940	1.731453	172.25.0.2	54.243.237.216	TCP	74	59418 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1167553275 TSecr=0 WS=128
941	1.732823	54.243.237.216	172.25.0.2	TCP	74	443 → 59414 [SYN, ACK] Seq=0 Ack=1 Win=62643 Len=0 MSS=1380 SACK_PERM TSval=1960091301 TSecr=1167553025 WS=…
942	1.732857	172.25.0.2	54.243.237.216	TCP	66	59414 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1167553276 TSecr=1960091301
943	1.733531	172.25.0.2	54.243.237.216	TLSv1.2	724	Client Hello
944	1.880845	54.243.237.216	172.25.0.2	TCP	66	443 → 59414 [ACK] Seq=1 Ack=659 Win=1147904 Len=0 TSval=1960091301 TSecr=1167553277
945	1.985687	54.243.237.216	172.25.0.2	TLSv1.2	2802	Server Hello
946	1.985714	172.25.0.2	54.243.237.216	TCP	66	59414 → 443 [ACK] Seq=659 Ack=2737 Win=63232 Len=0 TSval=1167553529 TSecr=1960091554
947	1.985717	54.243.237.216	172.25.0.2	TLSv1.2	2643	Certificate, Server Key Exchange, Server Hello Done
948	1.985723	172.25.0.2	54.243.237.216	TCP	66	59414 → 443 [ACK] Seq=659 Ack=5314 Win=60928 Len=0 TSval=1167553529 TSecr=1960091554
949	1.986930	172.25.0.2	54.243.237.216	TLSv1.2	192	Client Key Exchange, Change Cipher Spec, Finished
950	1.989103	172.25.0.2	1.1.1.1	DNS	77	Standard query 0xf1ef A ocsp.digicert.com
951	1.990540	54.243.237.216	172.25.0.2	TCP	74	443 → 59418 [SYN, ACK] Seq=0 Ack=1 Win=62643 Len=0 MSS=1380 SACK_PERM TSval=1960091559 TSecr=1167553275 WS=…
952	1.990567	172.25.0.2	54.243.237.216	TCP	66	59418 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1167553534 TSecr=1960091559
953	1.991140	172.25.0.2	54.243.237.216	TLSv1.2	724	Client Hello
954	1.993075	1.1.1.1	172.25.0.2	DNS	198	Standard query response 0xf1ef A ocsp.digicert.com CNAME ocsp.edge.digicert.com CNAME cac-ocsp.digicert.com…
955	1.993479	172.25.0.2	23.210.96.161	TCP	74	54670 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3349919916 TSecr=0 WS=128
956	1.995267	23.210.96.161	172.25.0.2	TCP	74	80 → 54670 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1380 SACK_PERM TSval=3411143013 TSecr=3349919916 WS=1…
957	1.995293	172.25.0.2	23.210.96.161	TCP	66	54670 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3349919918 TSecr=3411143013
958	1.995467	172.25.0.2	23.210.96.161	OCSP	495	Request
959	1.997521	23.210.96.161	172.25.0.2	TCP	66	80 → 54670 [ACK] Seq=1 Ack=430 Win=64768 Len=0 TSval=3411143015 TSecr=3349919918
960	2.002392	23.210.96.161	172.25.0.2	OCSP	971	Response
961	2.002418	172.25.0.2	23.210.96.161	TCP	66	54670 → 80 [ACK] Seq=430 Ack=906 Win=64128 Len=0 TSval=3349919925 TSecr=3411143019

```
Frame 935: 481 bytes on wire (3848 bits), 481 bytes captured (3848 bits)
Ethernet II, Src: e6:c1:4b:dc:0c:54 (e6:c1:4b:dc:0c:54), Dst: c2:cf:f0:d2:00:9b (c2:cf:f0:d2:00:9b)
Internet Protocol Version 4, Src: 34.231.2.231, Dst: 172.25.0.2
Transmission Control Protocol, Src Port: 80, Dst Port: 36828, Seq: 1, Ack: 375, Len: 415
Hypertext Transfer Protocol
  HTTP/1.1 301 Moved Permanently\r\n
  Server: nginx\r\n
  Date: Tue, 11 Mar 2025 08:29:49 GMT\r\n
  Content-Type: text/html\r\n
  Content-Length: 162\r\n
  Connection: keep-alive\r\n
  Location: https://airbnb.com/\r\n
  x-airbnb-sureride: i1t1m.Whnf4sqp%%h1\r\n
  X-Server-Name: airbnb.tld\r\n
  \r\n
  [HTTP response 1/1]
```

```
0000  c2 cf f0 d2 00 9b e6 c1  4b dc 0c 54 08 00 45 00   ........ K..T..E.
0010  01 d3 53 65 40 00 ec 06  67 d6 22 e7 02 e7 ac 19   ..Se@... g.".....
0020  00 02 00 50 8f dc cd 0d  5f 34 ba ad 41 01 80 18   ...P.... _4..A...
0030  00 7a 18 07 00 00 01 01  08 0a f9 0d 2e 9a 6a 9d   .z...... ......j.
0040  24 2a 48 54 54 50 2f 31  2e 31 20 33 30 31 20 4d   $*HTTP/1 .1 301 M
0050  6f 76 65 64 20 50 65 72  6d 61 6e 65 6e 74 6c 79   oved Per manently
0060  0d 0a 53 65 72 76 65 72  3a 20 6e 67 69 6e 78 0d   ..Server : nginx.
0070  0a 44 61 74 65 3a 20 54  75 65 2c 20 31 31 20 4d   .Date: T ue, 11 M
0080  61 72 20 32 30 32 35 20  30 38 3a 32 39 3a 34 39   ar 2025  08:29:49
0090  20 47 4d 54 0d 0a 43 6f  6e 74 65 6e 74 2d 54 79    GMT..Co ntent-Ty
00a0  70 65 3a 20 74 65 78 74  2f 68 74 6d 6c 0d 0a 43   pe: text /html..C
00b0  6f 6e 74 65 6e 74 2d 4c  65 6e 67 74 68 3a 20 31   ontent-L ength: 1
00c0  36 32 0d 0a 43 6f 6e 6e  65 63 74 69 6f 6e 3a 20   62..Conn ection:
00d0  6b 65 65 70 2d 61 6c 69  76 65 0d 0a 4c 6f 63 61   keep-ali ve..Loca
00e0  74 69 6f 6e 3a 20 68 74  74 70 73 3a 2f 2f 61 69   tion: ht tps://ai
00f0  72 62 6e 62 2e 63 6f 6d  2f 0d 0a 78 2d 61 69 72   rbnb.com /..x-air
0100  62 6e 62 2d 73 75 72 65  72 69 64 65 3a 20 69 31   bnb-sure ride: i1
```

Redirect to HTTPS

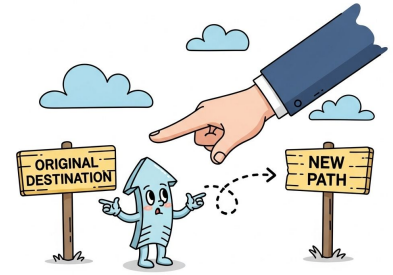
DNS query again

TLS handshake

OCSP and certificate checks for airbnb.com start here — DNS, TCP handshake, OCSP messages

Redirections continue

Redirect to **www.**airbnb.com (#970)



970	2.489172	54.243.237.216	172.25.0.2	HTTP	587 HTTP/1.1 301 Moved Permanently (text/html)
971	2.490586	172.25.0.2	54.243.237.216	TCP	66 59418 → 443 [FIN, ACK] Seq=785 Ack=5314 Win=64128 Len=0 TSval=1167554034 TSecr=1960091819
972	2.492057	172.25.0.2	1.1.1.1	DNS	74 Standard query 0x5c76 A www.airbnb.com
973	2.503692	1.1.1.1	172.25.0.2	DNS	181 Standard query response 0x5c76 A www.airbnb.com CNAME san.airbnb.com.edgekey.net CNAME e118243.a.akamaiedge…
974	2.504254	172.25.0.2	23.209.46.162	TCP	74 32934 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=213584854 TSecr=0 WS=128
975	2.505969	23.209.46.162	172.25.0.2	TCP	74 443 → 32934 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1380 SACK_PERM TSval=2591550602 TSecr=213584854 WS=1…
976	2.505996	172.25.0.2	23.209.46.162	TCP	66 32934 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=213584855 TSecr=2591550602
977	2.506690	172.25.0.2	23.209.46.162	TLSv1.3	728 Client Hello
978	2.510132	54.243.237.216	172.25.0.2	TLSv1.2	324 New Session Ticket, Change Cipher Spec, Finished
979	2.510163	172.25.0.2	54.243.237.216	TCP	54 59418 → 443 [RST] Seq=735 Win=0 Len=0
980	2.514316	23.209.46.162	172.25.0.2	TLSv1.3	1422 Server Hello, Change Cipher Spec, Encrypted Extensions
981	2.514341	172.25.0.2	23.209.46.162	TCP	66 32934 → 443 [ACK] Seq=663 Ack=1357 Win=64128 Len=0 TSval=213584864 TSecr=2591550610
982	2.514343	23.209.46.162	172.25.0.2	TCP	94 [TCP Previous segment not captured] 443 → 32934 [PSH, ACK] Seq=4069 Ack=663 Win=64128 Len=28 TSval=25915506…
983	2.514348	172.25.0.2	23.209.46.162	TCP	78 [TCP Dup ACK 981#1] 32934 → 443 [ACK] Seq=663 Ack=1357 Win=64128 Len=0 TSval=213584864 TSecr=2591550610 SLE…
984	2.514349	23.209.46.162	172.25.0.2	TCP	1422 [TCP Out-Of-Order] 443 → 32934 [PSH, ACK] Seq=1357 Ack=663 Win=64128 Len=1356 TSval=2591550610 TSecr=213584…
985	2.514354	172.25.0.2	23.209.46.162	TCP	78 32934 → 443 [ACK] Seq=663 Ack=2713 Win=62848 Len=0 TSval=213584864 TSecr=2591550610 SLE=4069 SRE=4097
986	2.514355	23.209.46.162	172.25.0.2	TCP	1422 [TCP Out-Of-Order] 443 → 32934 [ACK] Seq=2713 Ack=663 Win=64128 Len=1356 TSval=2591550610 TSecr=213584856 […
987	2.514360	172.25.0.2	23.209.46.162	TCP	66 32934 → 443 [ACK] Seq=663 Ack=4097 Win=61568 Len=0 TSval=213584864 TSecr=2591550610
988	2.515708	23.209.46.162	172.25.0.2	TLSv1.3	1185 Certificate, Certificate Verify, Finished
989	2.515727	172.25.0.2	23.209.46.162	TCP	66 32934 → 443 [ACK] Seq=663 Ack=5216 Win=64128 Len=0 TSval=213584865 TSecr=2591550612
990	2.517885	172.25.0.2	23.209.46.162	TLSv1.3	146 Change Cipher Spec, Finished
991	2.518394	172.25.0.2	23.209.46.162	HTTP2	158 Magic, SETTINGS[0], WINDOW_UPDATE[0]
992	2.518457	172.25.0.2	23.209.46.162	HTTP2	419 HEADERS[3]: GET /, WINDOW_UPDATE[3]
993	2.519257	23.209.46.162	172.25.0.2	TCP	66 443 → 32934 [ACK] Seq=5216 Ack=743 Win=64128 Len=0 TSval=2591550615 TSecr=213584867
994	2.519827	23.209.46.162	172.25.0.2	TCP	66 443 → 32934 [ACK] Seq=5216 Ack=835 Win=64128 Len=0 TSval=2591550616 TSecr=213584868
995	2.519840	23.209.46.162	172.25.0.2	TCP	66 443 → 32934 [ACK] Seq=5216 Ack=1188 Win=64128 Len=0 TSval=2591550616 TSecr=213584868

```
▸ Frame 970: 587 bytes on wire (4696 bits), 587 bytes captured (4696 bits)
▸ Ethernet II, Src: e6:c1:4b:dc:0c:54 (e6:c1:4b:dc:0c:54), Dst: c2:cf:f0:d2:00:9b (c2:cf:f0:d2:00:9b)
▸ Internet Protocol Version 4, Src: 54.243.237.216, Dst: 172.25.0.2
▸ Transmission Control Protocol, Src Port: 443, Dst Port: 59414, Seq: 5572, Ack: 1292, Len: 521
▾ Transport Layer Security
  ▾ TLSv1.2 Record Layer: Application Data Protocol: Hypertext Transfer Protocol
      Content Type: Application Data (23)
      Version: TLS 1.2 (0x0303)
      Length: 516
      Encrypted Application Data: a190645e5b68053ab3ec5da01e95ee2c384b05a1e3f437399379e393b29f882a782c57a8…
      [Application Data Protocol: Hypertext Transfer Protocol]
▾ Hypertext Transfer Protocol
  ▸ HTTP/1.1 301 Moved Permanently\r\n
```

```
0000  48 54 54 50 2f 31 2e 31  20 33 30 31 20 4d 6f 76   HTTP/1.1  301 Mov
0010  65 64 20 50 65 72 6d 61  6e 65 6e 74 6c 79 0d 0a   ed Perma nently··
0020  53 65 72 76 65 72 3a 20  6e 67 69 6e 78 0d 0a 44   Server:  nginx··D
0030  61 74 65 3a 20 54 75 65  2c 20 31 31 20 4d 61 72   ate: Tue , 11 Mar
0040  20 32 30 32 35 20 30 38  3a 32 39 3a 35 30 20 47    2025 08 :29:50 G
0050  4d 54 0d 0a 43 6f 6e 74  65 6e 74 2d 54 79 70 65   MT··Cont ent-Type
0060  3a 20 74 65 78 74 2f 68  74 6d 6c 0d 0a 43 6f 6e   : text/h tml··Con
0070  74 65 6e 74 2d 4c 65 6e  67 74 68 3a 20 31 36 32   tent-Len gth: 162
0080  0d 0a 43 6f 6e 6e 65 63  74 69 6f 6e 3a 20 6b 65   ··Connec tion: ke
0090  65 70 2d 61 6c 69 76 65  0d 0a 4c 6f 63 61 74 69   ep-alive ··Locati
00a0  6f 6e 3a 20 68 74 74 70  73 3a 2f 2f 77 77 77 2e   on: http s://www.
00b0  61 69 72 62 6e 62 2e 63  6f 6d 2f 0d 0a 78 2d 61   airbnb.c om/··x-a
00c0  69 72 62 6e 62 2d 73 75  72 65 72 69 64 65 3a 20   irbnb-su reride:
00d0  69 31 74 31 6d 2e 39 63  5a 55 53 79 66 66 25 25   i1t1m.9c ZUSyff%%
```

DNS for www. subdomain

TCP+TLS Handshakes

First meaningful query byte (#992) - HTTP GET /

Repeat for CDN

1004	2.530895	172.25.0.2	1.1.1.1	DNS	75	Standard query 0x122e A a0.muscache.com
1005	2.535390	1.1.1.1	172.25.0.2	DNS	182	Standard query response 0x122e A a0.muscache.com CNAME san.airbnb.com.edgekey.net
1006	2.535927	172.25.0.2	23.209.46.157	TCP	74	39262 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2324635230 TSecr=0
1007	2.537527	23.209.46.157	172.25.0.2	TCP	74	443 → 39262 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1380 SACK_PERM TSval=2679463
1008	2.537559	172.25.0.2	23.209.46.157	TCP	66	39262 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2324635232 TSecr=2679463026
1009	2.538169	172.25.0.2	23.209.46.157	TLSv1.3	729	Client Hello
1010	2.540415	23.209.46.157	172.25.0.2	TLSv1.3	1422	Server Hello, Change Cipher Spec, Encrypted Extensions
1011	2.540431	172.25.0.2	23.209.46.157	TCP	66	39262 → 443 [ACK] Seq=664 Ack=1357 Win=64128 Len=0 TSval=2324635235 TSecr=267946302
1012	2.540433	23.209.46.157	172.25.0.2	TCP	1450	[TCP Previous segment not captured] 443 → 39262 [PSH, ACK] Seq=2713 Ack=664 Win=641
1013	2.540439	172.25.0.2	23.209.46.157	TCP	78	[TCP Dup ACK 1011#1] 39262 → 443 [ACK] Seq=664 Ack=1357 Win=64128 Len=0 TSval=23246
1014	2.540440	23.209.46.157	172.25.0.2	TCP	1422	[TCP Out-Of-Order] 443 → 39262 [PSH, ACK] Seq=1357 Ack=664 Win=64128 Len=1356 TSval
1015	2.540446	172.25.0.2	23.209.46.157	TCP	66	39262 → 443 [ACK] Seq=664 Ack=4097 Win=61440 Len=0 TSval=2324635235 TSecr=267946302
1016	2.541734	23.209.46.157	172.25.0.2	TLSv1.3	1185	Certificate, Certificate Verify, Finished
1017	2.541744	172.25.0.2	23.209.46.157	TCP	66	39262 → 443 [ACK] Seq=664 Ack=5216 Win=64128 Len=0 TSval=2324635236 TSecr=267946303
1018	2.543527	172.25.0.2	23.209.46.157	TLSv1.3	146	Change Cipher Spec, Finished
1019	2.543755	172.25.0.2	23.209.46.157	HTTP2	158	Magic, SETTINGS[0], WINDOW_UPDATE[0]
1020	2.543778	172.25.0.2	23.209.46.157	HTTP2	429	HEADERS[3]: GET /airbnb/static/airbnb-dls-web/build/fonts/cereal-variable/AirbnbCer
1021	2.544748	23.209.46.157	172.25.0.2	TCP	66	443 → 39262 [ACK] Seq=5216 Ack=744 Win=64128 Len=0 TSval=2679463033 TSecr=232463523
1022	2.544757	23.209.46.157	172.25.0.2	TCP	66	443 → 39262 [ACK] Seq=5216 Ack=836 Win=64128 Len=0 TSval=2679463033 TSecr=232463523
1023	2.544985	23.209.46.157	172.25.0.2	TCP	66	443 → 39262 [ACK] Seq=5216 Ack=1199 Win=64128 Len=0 TSval=2679463033 TSecr=232463523
1024	2.547071	23.209.46.157	172.25.0.2	TLSv1.3	353	New Session Ticket
1025	2.547079	23.209.46.157	172.25.0.2	TLSv1.3	353	New Session Ticket
1026	2.547331	172.25.0.2	23.209.46.157	TCP	66	39262 → 443 [ACK] Seq=1199 Ack=5790 Win=64128 Len=0 TSval=2324635242 TSecr=267946303
1027	2.547430	23.209.46.157	172.25.0.2	HTTP2	127	SETTINGS[0]
1028	2.547433	23.209.46.157	172.25.0.2	HTTP2	97	SETTINGS[0]
1029	2.547454	172.25.0.2	23.209.46.157	HTTP2	97	SETTINGS[0]
1030	2.554541	23.209.46.157	172.25.0.2	HTTP2	841	HEADERS[3]: 200 OK
1031	2.554564	23.209.46.157	172.25.0.2	TCP	8202	443 → 39262 [ACK] Seq=6657 Ack=1230 Win=64128 Len=8136 TSval=2679463043 TSecr=23246

```
Header: access-control-max-age: 0
Header: x-amz-replication-status: COMPLETED
Header: last-modified: Mon, 05 Aug 2024 20:29:25 GMT
Header: etag: "2d9d32865ef1262644c455b3ead871e9"
Header: x-amz-server-side-encryption: AES256
Header: x-amz-version-id: s37i7xogUfgqeggXin9.Xx6qHFoa6.qL
Header: accept-ranges: bytes
Header: content-type: font/woff2
Header: server: AmazonS3
Header: content-length: 67300
Header: cdn-cache-h: HIT
Header: cache-control: public, max-age=31536000
Header: expires: Wed, 11 Mar 2026 08:29:50 GMT
Header: date: Tue, 11 Mar 2025 08:29:50 GMT
Header: alt-svc: h3=":443"; ma=93600
    Name Length: 7
    Name: alt-svc
    Value Length: 19
    Value: h3=":443"; ma=93600
    [Unescaped: h3=":443"; ma=93600]
    Representation: Literal Header Field never Indexed - New Name
```

```
0100  27 99 43 2e 99 df 27 9b  84 b3 76 2c d3 7e 1a a7
0110  d7 fc f2 e7 8c 78 4e 37  17 ed 9f 1f 03 84 8f d2
0120  4a 8f 1f 10 88 94 f5 25  8f 07 96 51 7f 1f 27 86
0130  86 91 fb 3d 5b 99 1f 0d  84 71 d6 40 0f 10 88 24
0140  95 2c 41 92 72 ad 3f 03  48 49 54 1f 09 92 ae d8
0150  e8 31 3e 94 a4 7e 56 1c  c5 81 90 b6 cb 80 00 3f
0160  1f 15 96 e4 59 3e 94 08  54 d0 3b 14 10 04 e2 80
0170  7a e0 9f b8 d8 14 c5 a3  7f 1f 12 96 df 69 7e 94
0180  08 54 d0 3b 14 10 04 da  80 7a e0 9f b8 d8 14 c5
0190  a3 7f 10 85 1d 09 59 1d  c9 90 9d 98 3f 9b 8d 34
01a0  cf f3 f6 a5 23 81 f6 5c  00 3f 10 8c 1f 51 d2 33
01b0  2d 61 7b 5a 54 25 68 c9  ad ff d8 e0 13 2b b4 f2
01c0  e1 74 4b bb f5 1c 01 7d  b0 b4 c8 5d 00 7e 89 04
01d0  df 55 41 bb 14 51 6e c9  a7 14 3a f5 6d c1 f4 78
01e0  04 07 da 07 ff 3f 10 8d  f2 b0 cd 64 75 46 b2 2d
01f0  b0 b6 1a 42 ff 9c 20 46  12 2e 05 c0 e8 c8 c8 02
0200  ea e1 75 a0 b8 f0 5d 7c  0b ba d3 60 74 81 6d 55
0210  67 0f 10 88 20 c9 39 50  91 a6 d4 7f 84 20 c9 39
0220  7f 10 8a 41 6c ee 5b 16  49 a9 35 53 7f b3 24 95
0230  2c 41 92 72 fd a9 21 50  48 31 e4 df f4 49 2a 5a
0240  73 d6 8f b9 0a 82 40 1f  a5 0b 24 c5 fb 52 4b 6c
0250  80 3f 4a 1e c3 4c 6a be  d4 92 db 20 e1 a7 76 0d
```

DNS query for CDN

TCP + TLS handshake with CDN

HTTP OK from CDN
ALT-SVC header: h3

CDN Server

QUIC to CDN + regional redirect

```
1043 2.555891   172.25.0.2      23.209.46.157   TCP       66 39262 → 443 [ACK] Seq=1230 Ack=44759 Win=58752 Len=0 TSval=2324635250 TSecr=2679463044
1044 2.555927   23.209.46.157   172.25.0.2      TLSv1.3 13626 Application Data, Application Data
1045 2.555936   172.25.0.2      23.209.46.157   TCP       66 39262 → 443 [ACK] Seq=1230 Ack=58319 Win=47232 Len=0 TSval=2324635250 TSecr=2679463044
1046 2.556248   23.209.46.157   172.25.0.2      TCP    10914 443 → 39262 [PSH, ACK] Seq=58319 Ack=1230 Win=64128 Len=10848 TSval=2679463045 TSecr=2324635249 [TCP
1047 2.556253   172.25.0.2      23.209.46.157   TCP       66 39262 → 443 [ACK] Seq=1230 Ack=69167 Win=56448 Len=0 TSval=2324635251 TSecr=2679463045
1048 2.556497   172.25.0.2      23.209.46.157   QUIC    1399 Initial, DCID=d8db3eedbaf9f033, SCID=3ebfcd, PKN: 0, CRYPTO
1049 2.556759   23.209.46.157   172.25.0.2      TLSv1.3 5099 Application Data, Application Data, Application Data
1050 2.556765   172.25.0.2      23.209.46.157   TCP       66 39262 → 443 [ACK] Seq=1230 Ack=74200 Win=61184 Len=0 TSval=2324635251 TSecr=2679463045
1051 2.570116   172.25.0.2      23.209.46.162   TCP       66 32934 → 443 [ACK] Seq=1219 Ack=6107 Win=64128 Len=0 TSval=213584920 TSecr=2591550625
1052 2.850905   23.209.46.162   172.25.0.2      HTTP2   3260 HEADERS[3]: 307 Temporary Redirect
1053 2.850930   172.25.0.2      23.209.46.162   TCP       66 32934 → 443 [ACK] Seq=1219 Ack=9301 Win=62592 Len=0 TSval=213585200 TSecr=2591550947
1054 2.855772   172.25.0.2      23.209.46.157   QUIC    1399 Initial, DCID=d8db3eedbaf9f033, SCID=3ebfcd, PKN: 1, CRYPTO
1055 2.858308   23.209.46.162   172.25.0.2      HTTP2/JSON  308 DATA[3], JavaScript Object Notation
1056 2.858328   172.25.0.2      23.209.46.162   TCP       66 32934 → 443 [ACK] Seq=1219 Ack=9543 Win=64128 Len=0 TSval=213585208 TSecr=2591550954
1057 2.861862   172.25.0.2      23.209.46.162   QUIC    1399 Initial, DCID=ce61bfba075d39eb0167c9a5a0f3, SCID=1dee7a, PKN: 0, CRYPTO
1058 2.863093   172.25.0.2      1.1.1.1         DNS       77 Standard query 0xc5d4 A www.airbnb.com.sg
1059 2.866691   1.1.1.1         172.25.0.2      DNS      184 Standard query response 0xc5d4 A www.airbnb.com.sg CNAME san.airbnb.com.edgekey.net CNAME e118243.a.
1060 2.867229   172.25.0.2      23.209.46.162   TCP       74 32938 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=213585217 TSecr=0 WS=128
1061 2.868687   23.209.46.162   172.25.0.2      TCP       74 443 → 32938 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1380 SACK_PERM TSval=2591550965 TSecr=2135852
1062 2.868711   172.25.0.2      23.209.46.162   TCP       66 32938 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=213585218 TSecr=2591550965
1063 2.869858   172.25.0.2      23.209.46.162   TLSv1.2   731 Client Hello
1064 2.875429   23.209.46.162   172.25.0.2      TLSv1.2  1422 [TCP Previous segment not captured] , Ignored Unknown Record
1065 2.875445   172.25.0.2      23.209.46.162   TCP       78 [TCP Dup ACK 1062#1] 32938 → 443 [ACK] Seq=666 Ack=1 Win=64256 Len=0 TSval=213585225 TSecr=259155096
1066 2.875447   23.209.46.162   172.25.0.2      TCP     2778 [TCP Out-Of-Order] 443 → 32938 [PSH, ACK] Seq=1 Ack=666 Win=64128 Len=2712 TSval=2591550971 TSecr=2
1067 2.875455   172.25.0.2      23.209.46.162   TCP       66 32938 → 443 [ACK] Seq=666 Ack=4097 Win=61952 Len=0 TSval=213585225 TSecr=2591550971
1068 2.875456   23.209.46.162   172.25.0.2      TLSv1.2   94 Ignored Unknown Record
1069 2.875460   172.25.0.2      23.209.46.162   TCP       66 32938 → 443 [ACK] Seq=666 Ack=4097 Win=61952 Len=0 TSval=213585225 TSecr=2591550971
1070 2.876698   23.209.46.162   172.25.0.2      TLSv1.2 1185 Ignored Unknown Record
1071 2.876706   172.25.0.2      23.209.46.162   TCP       66 32938 → 443 [ACK] Seq=666 Ack=5216 Win=64128 Len=0 TSval=213585226 TSecr=2591550973
1072 2.878525   172.25.0.2      23.209.46.162   TLSv1.2  146 Change Cipher Spec, Application Data
1073 2.878875   172.25.0.2      23.209.46.162   TLSv1.2  158 Application Data
1074 2.878923   172.25.0.2      23.209.46.162   TLSv1.2  460 Application Data
```

```
▾ Header: status: 307 Temporary Redirect
    Name Length: 6
    Name: status
    Value Length: 22
    Value: 307 Temporary Redirect
    [Unescaped: 307 Temporary Redirect]
    Representation: Literal Header Field never Indexed - New Name
▸ Header: expires: Thu, 01 Jan 1970 00:00:00 GMT
▸ Header: x-kraken-loop-name: core-guest-loop
▸ Header: location: https://www.airbnb.com.sg/?_set_bev_on_new_domain=1741681790_EAYjU3YzUwOWYzMz
▸ Header: cache-control: no-store, max-age=0, private, must-revalidate
▸ Header: accept-ch-lifetime: 31536000
▸ Header: content-security-policy: default-src 'nonce-cb94e40ae460cc2394f640df009d5afe' 'self' https:;…
▸ Header: x-frame-options: SAMEORIGIN
▸ Header: x-envoy-upstream-service-time: 75
▸ Header: x-xss-protection: 1; mode=block
▸ Header: accept-ch: Sec-CH-Device-Memory, Sec-CH-DPR, ECT, Sec-CH-UA-Platform-Version, Sec-CH-Viewpor…
▸ Header: x-content-type-options: nosniff
▸ Header: x-airbnb-internal-trace-id: u6XD8zN2UZ9BRSD3fDNsSg==
▸ Header: strict-transport-security: max-age=10886400; includeSubdomains
▸ Header: x-server-name: www.airbnb.com
▸ Header: content-length: 211
▸ Header: date: Tue, 11 Mar 2025 08:29:50 GMT
▸ Header: set-cookie: _user_attributes=%7B%22curr%22%3A%22SGD%22%7D; Path=/; Domain=.airbnb.com; Expir…
▸ Header: set-cookie: bev=1741681790_EAYjU3YzUwOWYzMz; Path=/; Domain=.airbnb.com; Expires=Thu, 11-Sep…
▸ Header: set-cookie: bev=1741681790_EAYjU3YzUwOWYzMz; Path=/; Domain=.airbnb.com; Expires=Thu, 11-Mar…
▸ Header: set-cookie: everest_cookie=1741681790.EAMTkzZDMxODI2NWNmMT.pX7AtWqdi37p6Yo1p6OKV-4qKx9CRdSHo…
▸ Header: set-cookie: bev=1741681790_EAYjU3YzUwOWYzMz; expires=Thu, 11-Mar-2027 08:29:50 GMT; path=/; …
▸ Header: set-cookie: country=SG; path=/; domain=.airbnb.com; secure
▸ Header: set-cookie: cdn_exp_5d4847f312830318=control; expires=Sat, 10-May-2025 08:29:50 GMT; path=/…
▸ Header: set-cookie: cdn_exp_d12d391c391[illegible]cc6a=treatment; expires=Sat, 10-May-2025 08:29:50 GMT; path…
▾ Header: alt-svc: h3=":443"; ma=93600
    Name Length: 7
    Name: alt-svc
```

```
0050  86 b2 da aa 35 53 7f 10  84 42 46 9[illegible] 51 90 64 0e   ····5S·· ·BF·Q·d·
0060  a9 bc b4 d6 7[illegible] 07 67 a5  3[illegible] 96 42 58 52 27 1f 15   ····[illegible]g· 6·CXR'··
0070  96 df 3d bf 4a 60 2a 65  1d [illegible] 05 f7 40 a0 01 70   ··=·J`*e ·J··@··p
0080  00 b8 00 29 8b 46 [illegible] 10  8e f2 b[illegible] 5b 07 d4 b5 2d   ···)·F·· ··[····-
0090  41 cf 5a d5 0e 92 ff [illegible] 21 ec 2a d[illegible] 5a 54 25 6a   A·Z····· !·*·ZT%j
00a0  0e 7a ff 1f 1f bb [illegible] 29  ad 17 18 63 [illegible] 8f 0b 8c   ·z·····) ···c····
00b0  d6 47 54 6b 90 [illegible] ae 89  [illegible] ff 22 41 53 [illegible] 65 ef   ·GTk···· ··"AS·e·
00c0  11 ea 8a a2 [illegible] 8a 43 d2  33 [illegible] 00 5d 68 2e [illegible] 17   ·····C· 3U·]h.<··
00d0  5f 04 58 [illegible] e7 d3 83 3c  fd f0 [illegible] ab 97 3f 7a [illegible]   _·X!···< ·····?z=
00e0  ff 1f [illegible] a1 a8 eb 21 27  b0 bf 4a 52 3f 2b 0e 62   ·····!' ··JR?+·b
00f0  c0 [illegible] a5 2b b0 dd c6 92  fd 29 4d a[illegible] 4a d6 17 b8   ···+···· ·)M·J···
0100  e8 34 83 49 7f 10 8d 19  08 5a d2 b1 [illegible] 5a 83 4a   ·4·I···· ·Z··'Z·J
0110  54 9a 92 ff 86 64 2d b2  e0 00 0f 10 90 [illegible] ea 49   T····d-· ·····!·I
0120  6a 4a c8 29 2d b0 c9 f4  b5 67 a0 c4 f5 ff [illegible] 05   jJ·)-··· ·g·····
0130  90 b2 8e da 12 b2 2c 22  9f ea a3 d4 42 ac 48 df   ·····," ····B·H·
0140  68 ad 00 65 69 c0 10 82  65 f6 a5 71 a0 49 28 0e   h··ei··· e··q·I(·
0150  fc 8d 8e 52 ff a5 3f d2  0b 44 bf e9 49 d2 9a d1   ···R··?· ·D··I···
0160  73 ed 42 1e aa 8a 44 ac  8b 08 a7 fa 41 68 97 fd   s·B···D· ····Ah··
0170  29 3a 53 5a 2e 29 e1 08  b8 c3 1e 10 b8 cd 64 75   ):SZ.)·· ······du
0180  46 b9 0f 4f da 86 a6 65  91 61 14 ff 48 2d 12 ff   F··O···· ·a··H-··
0190  a5 27 4a 6b 45 c5 24 1a  47 73 ed 4a 4b 21 86 b2   ·'JkE·$· Gs·JK!··
01a0  2c 22 9f e9 05 a2 5f f4  a4 e9 4d 68 b9 f6 a4 a7   ,"····_· ··Mh····
01b0  a9 2b 22 c2 29 fe 90 5a  25 ff 4a 48 34 8e e2 93   ·+"·)··Z %·JH4···
01c0  a5 35 a2 e7 da 92 d8 3a  4a b2 2c 22 9f 3f 6a 20   ·5·····: J·,"·?j·
01d0  96 1a b4 ac 8b 08 a7 fa  a8 f5 10 ab 12 37 da 2b   ········ ·····7·+
01e0  40 19 5a 70 04 20 99 7d  a9 5c 68 12 4a 00 3f 23   @·Zp· ·} ·\h·J·?#
01f0  63 94 bf e9 4f f4 82 d1  2f fa 52 74 a6 b4 5c 53   c···O··· /·Rt··\S
0200  fd 5b 52 07 29 56 2f 71  d1 fe 94 ff 48 9c 62 6d   ·[R·)V/q ····H·bm
0210  c5 ac 86 97 f5 3d 97 5f  ee 74 ec a6 47 9a f7 a2   ·····=·_ ·t··G···
0220  ff b9 d1 89 be cc b7 95  04 c1 bb cf 92 0f 0e 77   ········ ·······w
0230  7f dd fb e4 83 fd 29 fe  91 38 c4 db 8b 75 46 73   ······)· ·8···uFs
0240  5e ee 34 e5 c6 8c de ac  13 3f 96 0f 66 4a fc 67   ^·4····· ·?··fJ·g
0250  3d 44 d1 9b b4 d6 63 d1  cb 0e 8b cd 23 c7 b8 60   =D····c· ····#··`
0260  ff 4a 7f a4 4e 31 36 e2  d7 bf 6a e4 09 fb e7 d9   ·J··N16· ··j·····
```

Frame (3260 bytes) | Decrypted TLS (3172 bytes) | Decompressed Header (4474 bytes)

QUIC Initial to CDN

Regional redirect to `.sg` (#1052)

"Btw., I support QUIC"

DNS query for regional domain

TCP handshake to regional domain

TLS handshake to regional domain

CDN again for the regional domain

1085	2.891277	172.25.0.2	1.1.1.1	DNS	75	Standard query 0xbb1e A a0.muscache.com
1086	2.902950	1.1.1.1	172.25.0.2	DNS	182	Standard query response 0xbb1e A a0.muscache.com CNAME a0.airbnb.com.edgekey.net CN
1087	2.903543	172.25.0.2	23.209.46.151	TCP	74	42702 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=378274923 TSecr=0 W
1088	2.905196	23.209.46.151	172.25.0.2	TCP	74	443 → 42702 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1380 SACK_PERM TSval=32412813
1089	2.905212	172.25.0.2	23.209.46.151	TCP	66	42702 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=378274925 TSecr=324128130
1090	2.905818	172.25.0.2	23.209.46.151	TLSv1.3	729	Client Hello
1091	2.907385	23.209.46.151	172.25.0.2	TCP	66	443 → 42702 [ACK] Seq=1 Ack=664 Win=1140160 Len=0 TSval=324128132 TSecr=378274925
1092	2.908077	23.209.46.151	172.25.0.2	TLSv1.3	2802	Server Hello, Change Cipher Spec, Encrypted Extensions
1093	2.908093	172.25.0.2	23.209.46.151	TCP	66	42702 → 443 [ACK] Seq=664 Ack=2737 Win=63232 Len=0 TSval=378274927 TSecr=324128133
1094	2.908095	23.209.46.151	172.25.0.2	TCP	1426	443 → 42702 [PSH, ACK] Seq=2737 Ack=664 Win=64512 Len=1360 TSval=324128133 TSecr=378
1095	2.908099	172.25.0.2	23.209.46.151	TCP	66	42702 → 443 [ACK] Seq=664 Ack=4097 Win=61952 Len=0 TSval=378274927 TSecr=324128133
1096	2.908100	23.209.46.151	172.25.0.2	TLSv1.3	1185	Certificate, Certificate Verify, Finished
1097	2.908104	172.25.0.2	23.209.46.151	TCP	66	42702 → 443 [ACK] Seq=664 Ack=5216 Win=60928 Len=0 TSval=378274927 TSecr=324128133
1098	2.909960	172.25.0.2	23.209.46.151	TLSv1.3	146	Change Cipher Spec, Finished
1099	2.910211	172.25.0.2	23.209.46.151	HTTP2	158	Magic, SETTINGS[0], WINDOW_UPDATE[0]
1100	2.910234	172.25.0.2	23.209.46.151	HTTP2	433	HEADERS[3]: GET /airbnb/static/airbnb-dls-web/build/fonts/cereal-variable/AirbnbCere
1101	2.911395	23.209.46.151	172.25.0.2	TLSv1.3	353	New Session Ticket
1102	2.911411	23.209.46.151	172.25.0.2	TLSv1.3	353	New Session Ticket
1103	2.911627	23.209.46.151	172.25.0.2	TCP	66	443 → 42702 [ACK] Seq=5790 Ack=1203 Win=64128 Len=0 TSval=324128137 TSecr=378274930
1104	2.911640	23.209.46.151	172.25.0.2	HTTP2	127	SETTINGS[0]
1105	2.911643	23.209.46.151	172.25.0.2	HTTP2	97	SETTINGS[0]
1106	2.911764	172.25.0.2	23.209.46.151	HTTP2	97	SETTINGS[0]
1107	2.916183	23.209.46.151	172.25.0.2	HTTP2	842	HEADERS[3]: 200 OK
1108	2.916204	23.209.46.151	172.25.0.2	TCP	8274	443 → 42702 [ACK] Seq=6658 Ack=1234 Win=64128 Len=8208 TSval=324128141 TSecr=378274
1109	2.916248	23.209.46.151	172.25.0.2	TCP	2802	443 → 42702 [PSH, ACK] Seq=14866 Ack=1234 Win=64128 Len=2736 TSval=324128141 TSecr=3
1110	2.916253	23.209.46.151	172.25.0.2	TLSv1.3	5528	[TLS segment of a reassembled PDU]
1111	2.916255	23.209.46.151	172.25.0.2	HTTP2	1434	DATA[3]
1112	2.916277	172.25.0.2	23.209.46.151	TCP	66	42702 → 443 [ACK] Seq=1234 Ack=24432 Win=49536 Len=0 TSval=378274936 TSecr=324128141
1113	2.916492	23.209.46.151	172.25.0.2	TCP	2802	443 → 42702 [PSH, ACK] Seq=24432 Ack=1234 Win=64128 Len=2736 TSval=324128142 TSecr=3
1114	2.916505	172.25.0.2	23.209.46.151	TCP	66	42702 → 443 [ACK] Seq=1234 Ack=27168 Win=61952 Len=0 TSval=378274936 TSecr=324128142
1115	2.917291	23.209.46.151	172.25.0.2	TLSv1.3	13746	DATA[3]
1116	2.917407	23.209.46.151	172.25.0.2	TCP	6906	443 → 42702 [PSH, ACK] Seq=40848 Ack=1234 Win=64128 Len=6840 TSval=324128143 TSecr=3
1117	2.917412	23.209.46.151	172.25.0.2	TCP	1434	443 → 42702 [ACK] Seq=47688 Ack=1234 Win=64128 Len=1368 TSval=324128143 TSecr=378274
1118	2.917519	23.209.46.151	172.25.0.2	TLSv1.3	13746	DATA[3]
1119	2.917675	172.25.0.2	23.209.46.151	TCP	66	42702 → 443 [ACK] Seq=1234 Ack=62736 Win=64128 Len=0 TSval=378274937 TSecr=324128143
1120	2.917741	23.209.46.151	172.25.0.2	TCP	2802	443 → 42702 [PSH, ACK] Seq=62736 Ack=1234 Win=64128 Len=2736 TSval=324128143 TSecr=3
1121	2.917748	172.25.0.2	23.209.46.151	TCP	66	42702 → 443 [ACK] Seq=1234 Ack=65472 Win=69632 Len=0 TSval=378274937 TSecr=324128143
1122	2.917885	23.209.46.151	172.25.0.2	TCP	5538	443 → 42702 [PSH, ACK] Seq=65472 Ack=1234 Win=64128 Len=5472 TSval=324128143 TSecr=3
1123	2.917891	172.25.0.2	23.209.46.151	TCP	66	42702 → 443 [ACK] Seq=1234 Ack=70944 Win=80512 Len=0 TSval=378274937 TSecr=324128143
1124	2.918711	23.209.46.151	172.25.0.2	TLSv1.3	3323	DATA[3]
1125	2.918723	172.25.0.2	23.209.46.151	TCP	66	42702 → 443 [ACK] Seq=1234 Ack=74201 Win=87040 Len=0 TSval=378274938 TSecr=324128144
1126	2.918950	172.25.0.2	23.209.46.151	QUIC	1399	Initial, DCID=793fe56ffd177ad583d89b, SCID=a2b6dd, PKN: 0, CRYPTO
1127	2.930116	172.25.0.2	23.209.46.162	TCP	66	32938 → 443 [ACK] Seq=1263 Ack=6107 Win=64128 Len=0 TSval=213585280 TSecr=2591550986

DNS query for CDN

TCP + TLS handshake

QUIC support in ALT-SVC

QUIC to CDN

First QUIC to airbnb.com

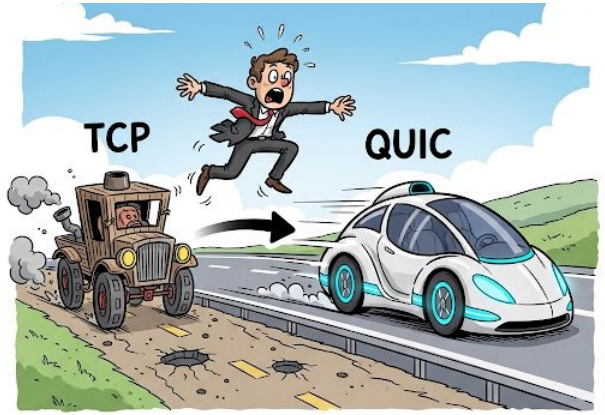
First QUIC packet (#1134)

```
3.213146    172.25.0.2      23.209.46.162   TCP     66 32938 → 443 [ACK] Seq=1263 Ack=11339 Win=64128 Len=0 TSval=213585563 TSecr=2591551309
1134 .215759    172.25.0.2      23.209.46.162   QUIC    1399 Initial, DCID=0ea008ec5c53615c, SCID=a2d36e, PKN: 0, CRYPTO
1136 3.265330   23.209.46.162   172.25.0.2      TLSv1.2  187 Application Data
```

```
▸ Compression Methods (1 method)
  Extensions Length: 461
▾ Extension: server_name (len=22)
    Type: server_name (0)
    Length: 22
  ▾ Server Name Indication extension
      Server Name list length: 20
      Server Name Type: host_name (0)
      Server Name length: 17
      Server Name: www.airbnb.com.sg
```

```
0040  77 77 77 2e 61 69 72 62  6e 62 2e 63 6f 6d 2e 73   www.airb nb.com.s
0050  67 00 17 00 00 ff 01 00  01 00 00 0a 00 0a 00 08   g······ ········
0060  00 1d 00 17 00 18 00 19  00 10 00 05 00 03 02 68   ········ .......h
0070  33 00 05 00 05 01 00 00  00 00 00 22 00 0a 00 08   3······ ···"····
0080  04 03 05 03 06 03 02 03  00 33 00 6b 00 69 00 1d   ········ ·3·k·i··
0090  00 20 12 80 f8 ab 7a f1  de 69 24 ff 11 d2 13 27   · ····z· ·i$····'
00a0  46 0e 01 77 c1 8a b5 9c  f1 ab 2d 6b dd e2 fa 5e   F··w···· ··-k···^
00b0  8c 5c 00 17 00 41 04 a1  04 e0 c6 2a 40 7d bd 73   ·\···A·· ···*@}·s
00c0  dd 20 b8 8a 85 6f 1c 40  c4 d8 c2 96 b2 70 72 fd   · ···o·@ ·····pr·
00d0  ba 55 2a d2 de f3 5f 4c  b1 c1 25 91 b0 86 6a a1   ·U*···_L ··%···j·
```

- First DNS packet to airbnb.com is #211
- First relevant QUIC packet is #1134
- **923 packets** were exchanged to reach this stage



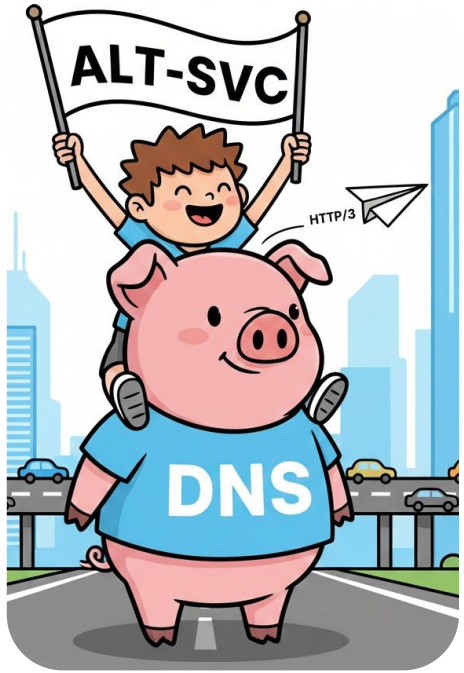
Mostly due to backward compatibility and not being aware of alternative services (i.e., QUIC) in time

How is it supposed to work?

Utilize HTTPS records, but what if they are missing?

Rely on DNS HTTPS records (RFC 9460)

- Inform the browser about HTTP/3 in the first DNS response
  - …after the `A` record
- Browser can straight away initiate QUIC connection
- Significantly reduce packet exchanges
  - UDP → **no TCP handshakes**
  - encrypted by default
    - no **port 80 → port 443 redirect**!
    - **TLS handshake “baked-in”**
- **SOTA:** *Cloudflare* knows this very well
  - they set these records for all their customers [1]




```
[CARBON-X1]  lele ~/git
↳ ♻  $ dig cloudflare.com HTTPS +short
1 . alpn="h3,h2" ipv4hint=104.16.132.229,104.16.133.229 ipv6hint=2606:4700::6810:84e5,2606:4700::6810:85e5
```

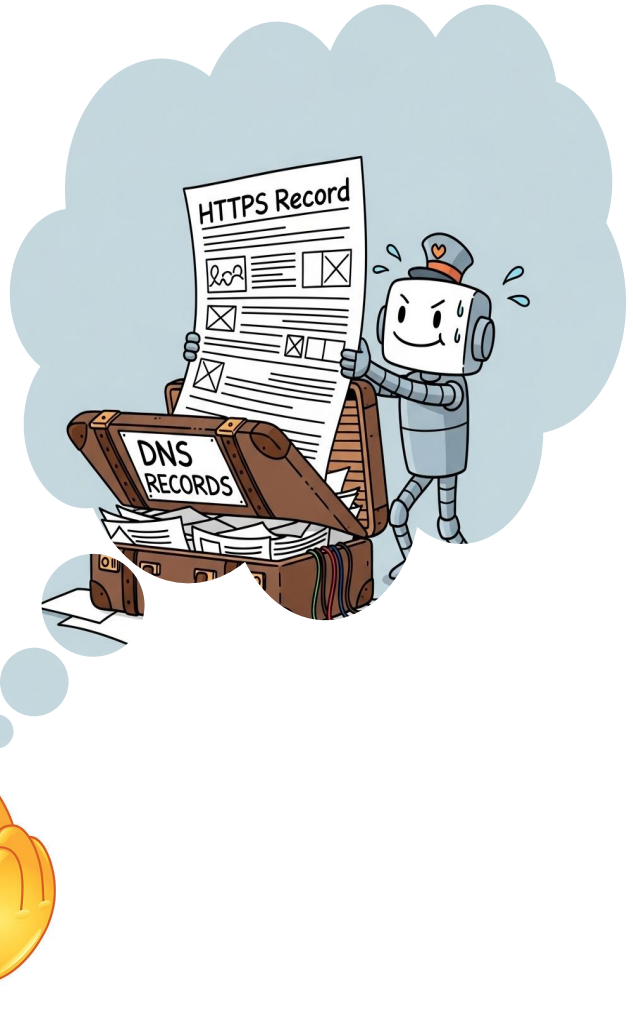

[1] https://blog.cloudflare.com/speeding-up-https-and-http-3-negotiation-with-dns/

What can I do for those not set?

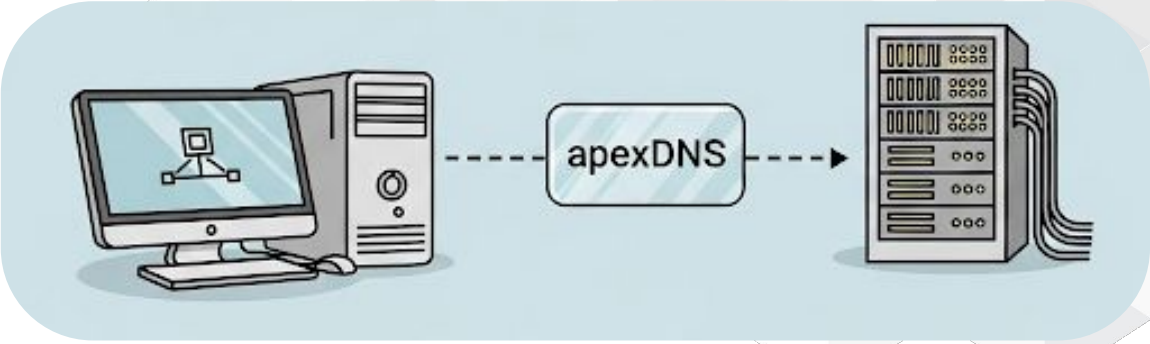
- Wait for the whole Internet to catch up?

nuh uh.

- The problem is clear…
- Augment DNS responses on-the-fly?



ApexDNS



- **Aims:**
  - *Augment DNS responses on-the-fly*
  - Locally - do not interfere with the DNS ecosystem

  - Do not run a modified local DNS server (overhead+mgmt)
  - Avoid inconsistency →Do not tamper with original records (e.g., A, AAAA, CNAME)

  - Gather intel about websites in advance
  - Transparent - no client addons or extra requirements

ApexDNS

DNSDist proxy

- PowerDNS-based proxy for load-balancing
  - as a stub
- Provides encrypted access to upstream
  - Privacy preserved with DoH to recursive resolvers like 8.8.8.8
- Provides encrypted access to downstream
  - Your browser can send DoH queries to this stub resolver
  - (important for the “crazy-privacy” mode)
- Scriptable via a Lua-interface
  - Not just a simple proxy - can manipulate messages!

ApexDNS - Two approaches

Naive

- Matching on HTTPS records of main domains
  - e.g., augment response for www.airbnb.com

Advanced

- Matching on HTTPS records from third-party CDNs too
  - e.g., augment a0.muscache.com too

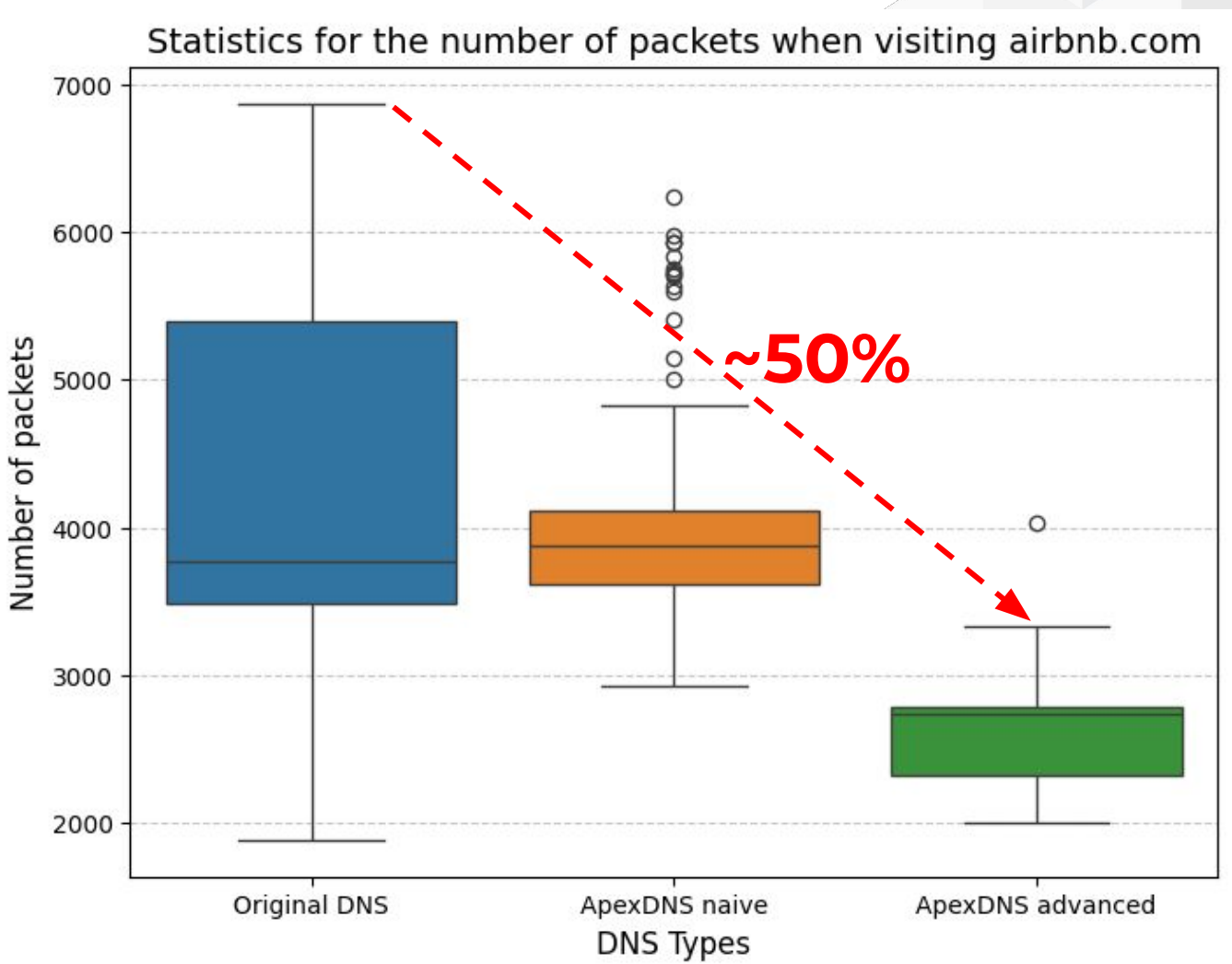
```
$ sudo pdnsutil raw-lua-from-content HTTPS '1 . alpn="h3,h2" ipv4hint=23.48.224.103'
"\000\001\000\000\001\000\006\002h\051\002h\050\000\004\000\004\023\048\224g"
```

```
addAction(AndRule({
  QNameRule('www.airbnb.com.'), QTypeRule(DNSQType.HTTPS)}),
  SpoofRawAction({"\000\001\000\000\001\000\006\002h\051\002h\050\000\004\000\004\023\048\224g"}))

addAction(AndRule({
  QNameRule('airbnb.com.'), QTypeRule(DNSQType.HTTPS)}),
  SpoofRawAction({"\000\001\000\000\001\000\003\002h\050"}))

addAction(AndRule({
  QNameRule('a0.muscache.com.'), QTypeRule(DNSQType.HTTPS)}),
  SpoofRawAction({"\000\001\000\000\001\000\006\002h\051\002h\050\000\004\000\004\023\032\039\139"}))
```

Evaluation - #packets

- #Visits = ~100
- ~50% reduction in the number of packets

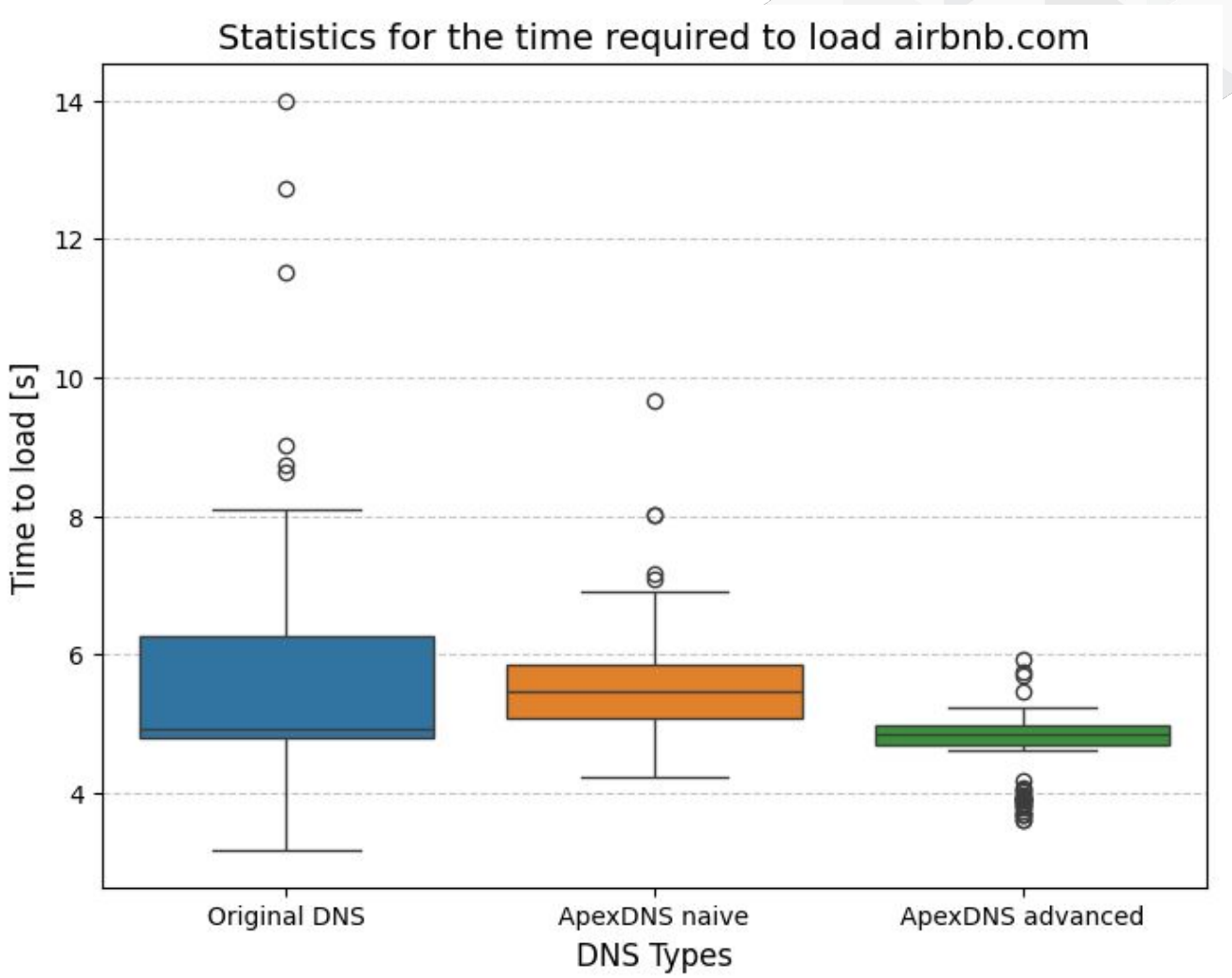
- First QUIC packet ~20% earlier



Note: I had to use VPN as UDP (i.e., QUIC) was dropped at the firewall → introduced some extra bias once in a while

Evaluation - time to load

- #Visits = ~100
- First QUIC packet ~20% earlier → **~20-35% faster page load times**



Note: I had to use VPN as UDP (i.e., QUIC) was dropped at the firewall → introduced some extra bias once in a while

Current state (Jan 2026)

- Is everyone doing it wrong (except Cloudflare)?

FUN FACTS (FUN?)

```
$ cat ipv4hints_providers.txt|uniq
cruz.ns.cloudflare.com.
ns1.dcloud.co.id.
ns1.intellispace.net.
cruz.ns.cloudflare.com.
darl.ns.cloudflare.com.
cruz.ns.cloudflare.com.
rdns1.hostiservices.com.
pri.authdns.ripe.net.
darl.ns.cloudflare.com.
rdns1.frantech.ca.
cruz.ns.cloudflare.com.
pri.authdns.ripe.net.
z.arin.net.
```

6 out of 13 providers are **Cloudflare**

TRANCO LIST OF TOP DOMAINS (2025)	QUIC SUPPORT	HTTPS RECORDS	"H3" IN HTTPS RECORDS	70% OF QUIC-ENABLED SITES
Top 5000 domains	25% → 1254 domains	56.2% → 705 domains	30% → 375 domains	Zero benefit

GOOGLE CRUX LIST OF TOP DOMAINS (2026)	QUIC SUPPORT	HTTPS RECORDS	"H3" IN HTTPS RECORDS	33.5% OF QUIC-ENABLED SITES
Top 5000 domains	39% → 1956 domains	172% → 3371 domain	66.5% → 1302 domains	Zero benefit

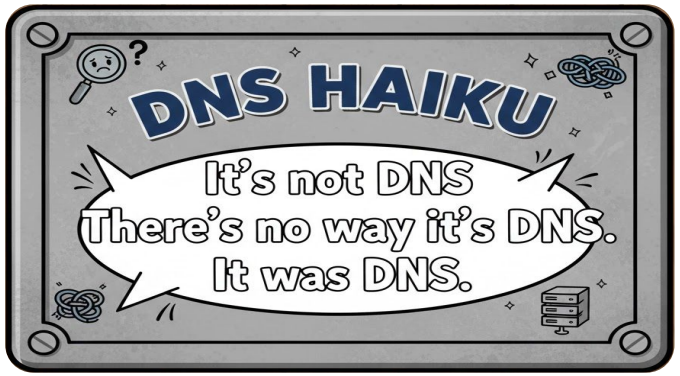
Future work

- **ApexDNS** is just a Proof-of-concept
  - bunch of scripts to
    - make your “own Internet faster”
    - Do evaluations and gather intel
  - No pre-loaded HTTPS records for all domains
    - must be done regionally to hard-code the best IPs
- **Plan:** Automating the whole process

Main takeaways

⚠️ **The Problem**: QUIC is only "Quick" if the client knows it exists before the handshake.

- Missing DNS records = wasted protocol overhead.



📢 **Network operators and service providers**:

- Adopt DNS HTTPS Resource Records globally.
- It is the modern standard for protocol discover.

📣 **Customers (whose service providers are not here)**:

- Bridge the Gap with ApexDNS
- Use ApexDNS to ensure you always find the "fast path."
- Update your browser → query HTTPS without crazy-privacy, enforce HTTPS

SCAN ME

ApexDNS

SCAN ME

WebTrafficSphere

Thank you

Levente Csikor (csikor_levente@a-star.edu.sg)

Dinil Mon Divakaran (dinil_divakaran@a-star.edu.sg)

Several images were made with Google Gemini's Nano banana. Thank you AI :)