A wide look into RFC9460 apps..

Ralf
Weber
Principal Architect

6.2.2025

Agenda

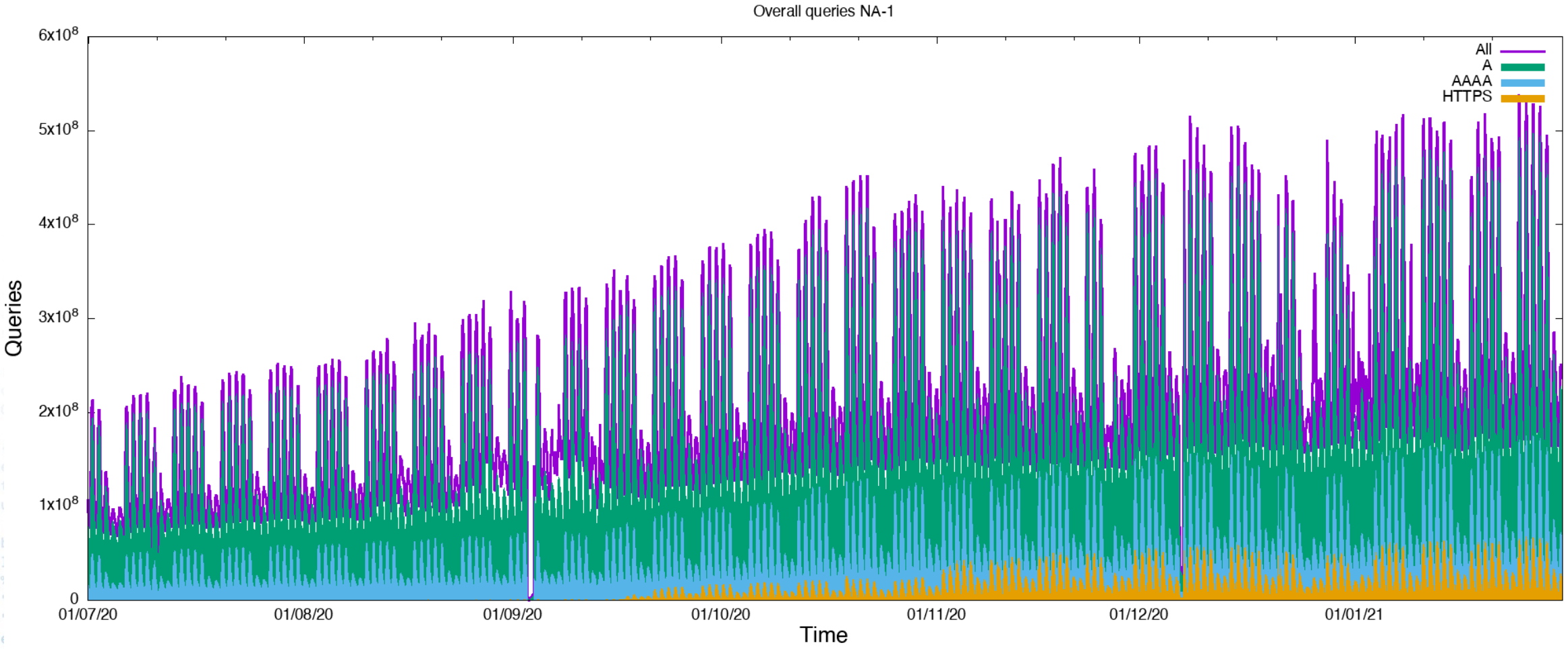
- Motivation
- Data Sources
- Processing
- Data
- Findings
- Questions

Motivation

- First new query type to gain traction in decades
- Can support multiple use cases
  - CNAME at the APEX (if Chrome would support it)
  - Encrypted Client Hello
  - Strict HTTPS/ALPN
  - DELEG
- Wanted to find out what the deployments of those are
  - HTTPS query type use cases/lookups are all done by browsers
- I talked about this before (DNS-OARC 34):

Overview of Traffic Impact

All
A
AAAA
HTTPS



Data sources

- There is a lot of FQDN data out there
  - Wanted to use recursive queries but
    - Interesting data is in the answer. which is stored differently
      - Setting up a pipeline for this proved to difficult for the timeline I had
    - Still got 344 million names from recursive resolvers
- Other sources
  - ICANN Centralized Zone Data Service (https://czds.icann.org/) – 220 million
  - Certificate transparency logs from Merklemap (https://www.merklemap.com) – 735 million
- Merging all this data gives me 1.3 billion – well not really…

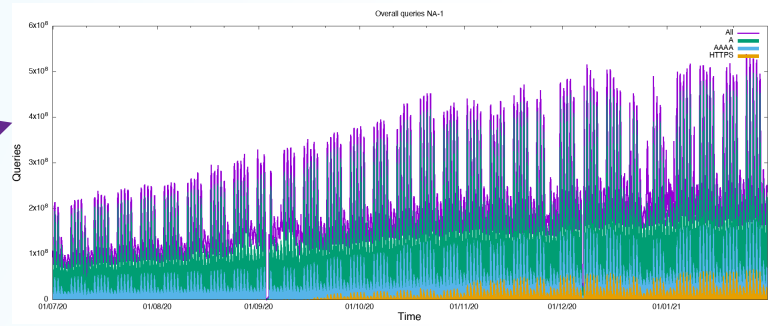
Processing

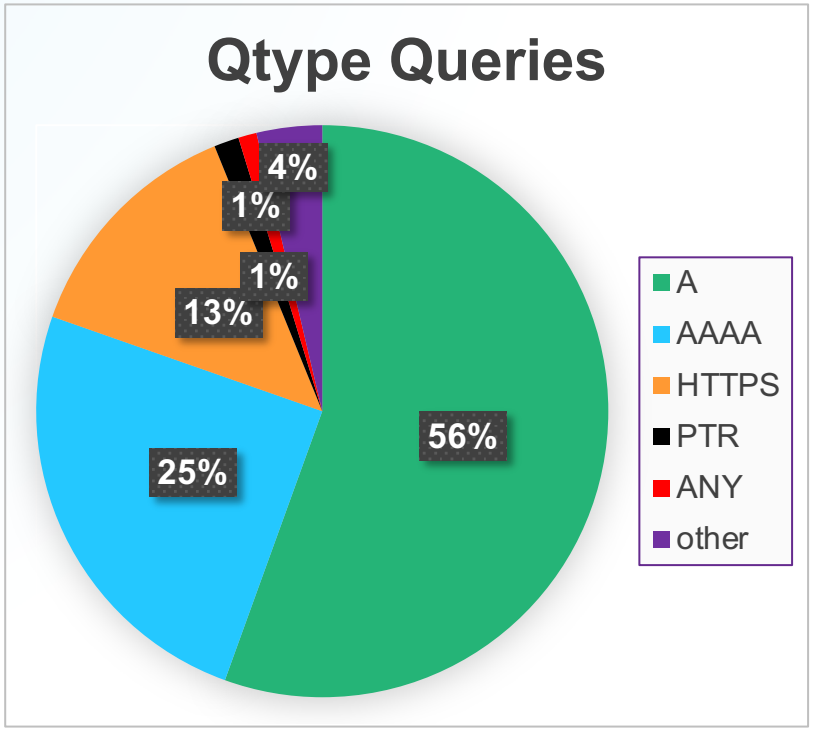
- I’m only interested in positive answers
  - NXDomain or NoData get dropped
- To get more data I prepend everything positive with www and try again
- HTTPS records can live on their own (without A/AAAA). but those will not be found as I need positive answers to continue
- For every FQDN I count the answers for
  - A
  - AAAA
  - HTTPS
- Then examined HTTPS FQDNs further

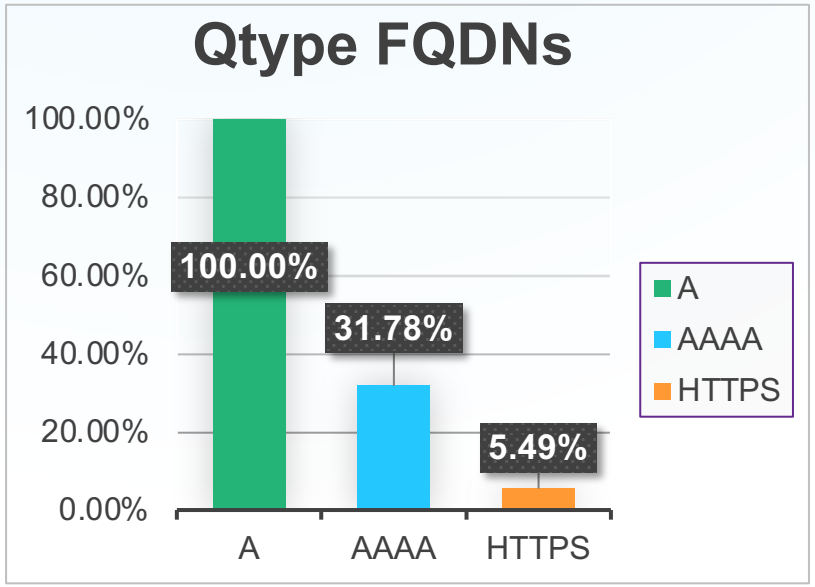
A grain of salt

- HTTPS queries have increased
  - Now Chrom(e|ium) always does them
  - Firefox sometimes
- Looking at number of FQDNs here
  - Not how much they get queried

5-10%

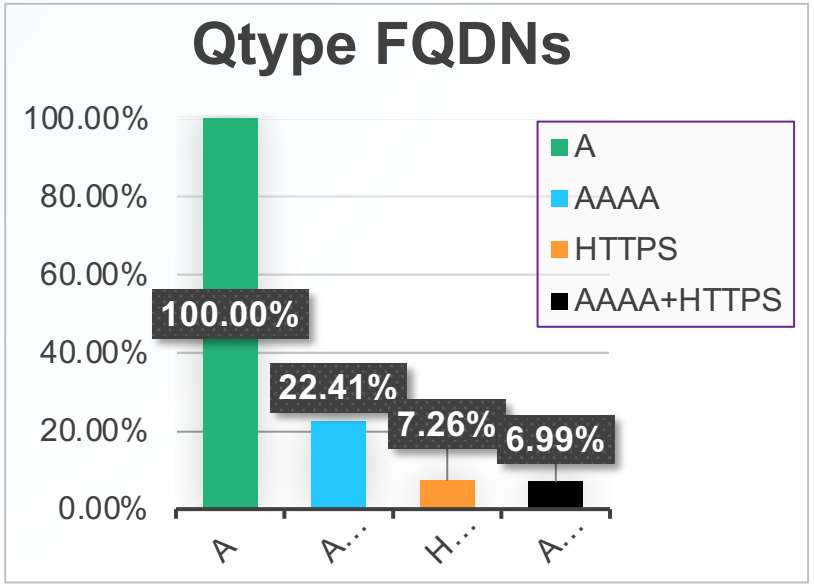






Overview of all FQDNs

- About 1 billion FQDNs reply to an A query (1,058,501,939)
- AAAA is 237 million or 22.41% (237,169,842)
- HTTPS is ~77 million or 7.26% (76,804,616)
  - Post processing eliminated a further 1,061,787
  - Actual inspected records were 75,742,829
  - DNS is dymanic
- FQDNS answer both is ~74 million or 6.99%
  - Absolute 73,971,845
  - 96.31% of HTTPS domains have an AAAA
  - Modern records support modern transports



A quick recap of SVCB/HTTPS responses

```
whitesnake.rwdns.de.    300     IN      HTTPS   1 whitesnake.rw42.de. alpn="h2" ipv4hint=172.232.49.121
whitesnake.rwdns.de.    300     IN      HTTPS   1 . alpn="h3" ipv6hint=2600:3c07::f03c:93ff:feae:2058
```

- Each DNS response can have multiple answers
- Each SVCB/HTTPS record has
  - A priority (with 0 being special indicating an Alias)
  - A target
  - Several SVCB paramaters (SvcParams)
- Common SVCB parameters are:
  - ALPN
  - IPv4/6Hint
  - ECH
  - Dohpath
  - Generics are possible

Answers and Priorites

- Most FQDNs just have one HTTPs record

Answercount	Domains	%
1	75,646,511	99.87284%
2	96,115	0.12690%
3	27	0.00004%
5	82	0.00011%
4	91	0.00012%
8	3	0.00000%

If you have two answers Priorities are usually 1 and 2

- The most used priority is 1

Priority	Count	%
0	30,355	0.0400%
1	75,711,308	99.8308%
2	96,215	0.1269%
other	1,742	0.0023%

Too bad Chrome can't reach these

Targets

- For 75742829 (~76 million) FQDN we got 19161 unique targets
  - Because of multiple answers there were a total of 75839620 HTTPs answers
- 75712041 or 99.83% are using '.' as a target
- Only other outstanding user is ~~Facebook~~ Meta
  - 43 unique targets
  - For 95090 FQDNs (0.12%)
- AWS (242) and Azure (310) FQDNs almost always found because of CNAME to a CDN

SVCB Parameters

- ALPN and IPv4Hint are most common
- IPv6 and ECH follow

SVCB Parameter	Count	%
mandatory	33	0.00004%
alpn	75,521,983	99.58117%
no-default-alpn	170	0.00022%
port	1,806	0.00238%
ipv4hint	75,531,330	99.59350%
ech	64,966,919	85.66356%
ipv6hint	73,437,342	96.83242%
dohpath	9	0.00001%
32768	9	0.00001%

ALPN distributions

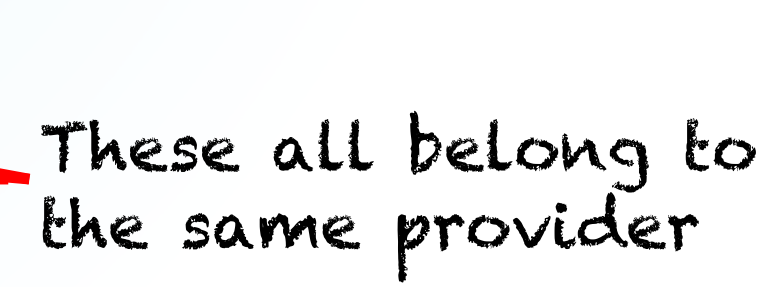
- Mostly h3.h2
  - QUIC preferred
  - Aligns with ECH
    - 97.63% of ECH domains have ALPN h3.h2

ALPN	Count	%
h3.h2	69,697,765	92.29%
h2	5,574,588	7.38%
h2.h3	202,680	0.27%
h3	32,022	0.04%
other	14,928	0.02%

ECH keys

- ECH Keys can and should be reused for deployments
- 65 million domains with ECH
- 151 unique keys

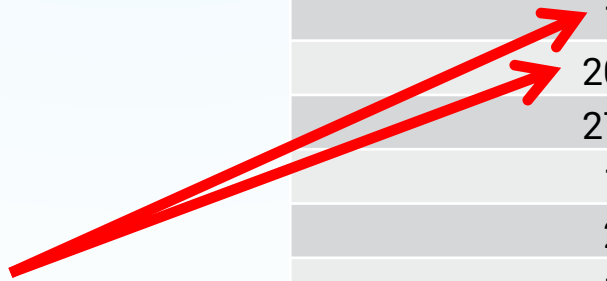
Key	Count	%
Key1	32,850,012	50.56421%
Key2	32,068,053	49.36059%
Key3	48,512	0.07467%
Key4	20	0.00003%
Key5	11	0.00002%
Key6	10	0.00002%
Key7	10	0.00002%
Other	288	0.00044%



Where do all these records point?

- Pretty much all HTTPS records have IP hints (76 million)
  - 307141 different addresses (v4 and v6)
  - At least 246 domains per address
- AS where they run
  - 425 different ASes

AS	Domains	%
13335	73,941,344	97.86%
209242	1,322,074	1.75%
273584	139,634	0.18%
12996	102,776	0.14%
29729	25,583	0.03%
11045	4,247	0.01%
33191	3,410	0.00%
29085	2,110	0.00%
24940	1,510	0.00%
4837	1,334	0.00%



Summary

- HTTPS records are being deployed
  - Unfortunately not all use cases are supported by all browsers
- ECH is being deployed as an RFC9460 application
  - Dominated by one provider
- There’s value in continuing to understand these deployment trends
  - To be continued…

Questions