Measuring Open Resolvers Negative Caching

Yehuda Afek*, Anat Bremler-Barr †, Neta Peleg†

*Tel Aviv University †Reichman University

Research Goals

- Percentage of NXDomain (Non-Existent Domain, NX) requests in the Internet increases from 2018 to 2021 two-fold, 40% → 80%
- We investigate NXDomain response caching on nine large open DNS resolvers. How long have they been cached?
- Measuring on - Adguard, Cloudflare, Comodo, Dyn, Google, Opendns, Quad9, Verisign, Yandex Open Resolvers.

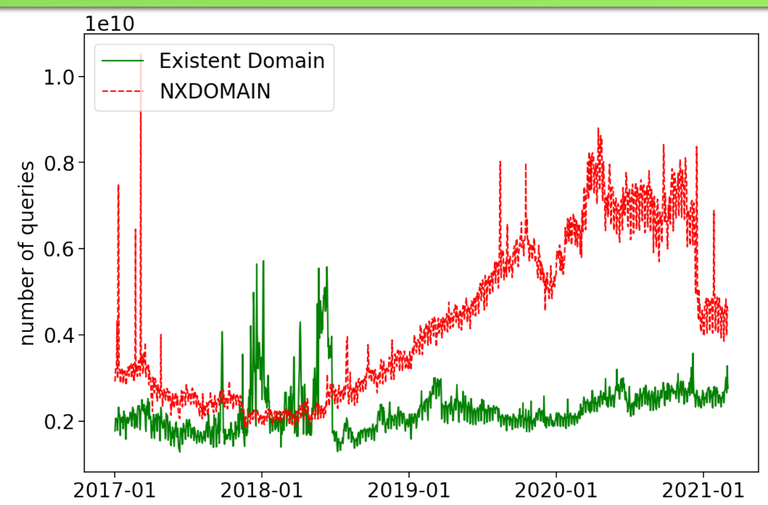

Fig. 1: Count of daily query responses by NX or Existent code in A-Root server over the years Based on RSSAC002 Data

Measurement Setup

• Authoritative server under our control, and monitoring. Set SOA record with TTL 21600.

• At Time 0: Fill up caches by 10 NX "A" queries to hot.ours.xyz (Hot Query) and 10 * 216 queries to nh-T.ours.xyz, T=100,200,…,21600 (Non-Hot Queries)

• At Time T=100, 200,...,21600 secs:
5 NX "A" queries hot.ours.xyz and 5 NX "A" queries nh-T.ours.xyz. Record TTL values on response SOA records.

• Infer longest caching time by observing shortest TTL returned in the SOA records.

❖ Repeated measurement for Existent domain

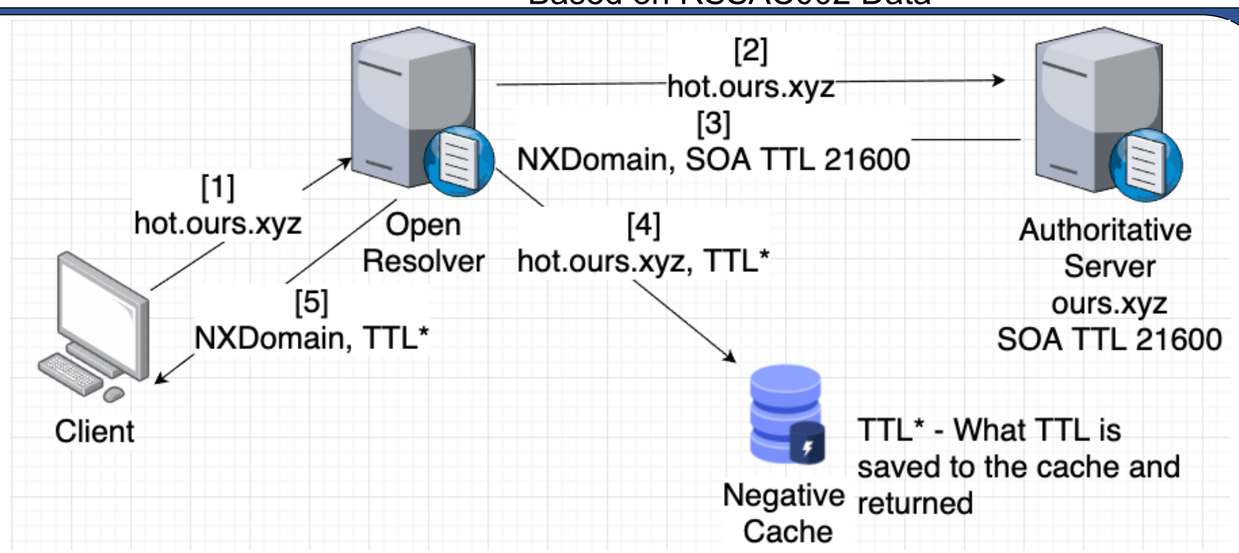

Fig. 2: DNS Topology and query process

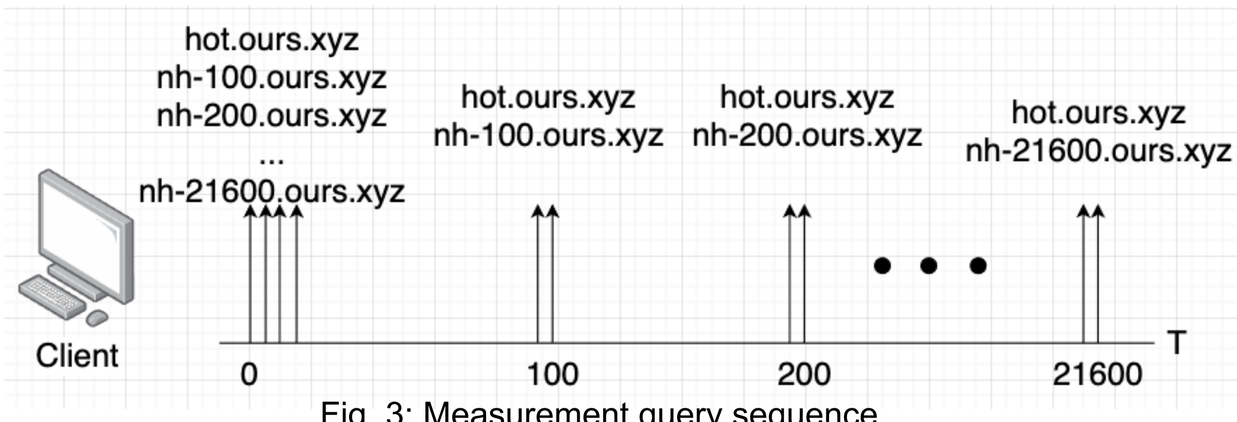

Fig. 3: Measurement query sequence

Result & Key Observations

- TTL Truncation – Most resolvers truncate the negative TTL to less than 1 hour. Google, serving 36% of the DNS traffic, sets the TTL to 30 minutes.
- Caching Time - Records are cached for the entire duration of the TTL, except Cloudflare, since it caches negative responses for less than the TTL it sets to.
- "Hot" vs "Non Hot" Queries – Similar negative caching behavior in most resolvers. Cloudflare caches "Hot queries" for longer than the ”Non-Hot" queries. Might imply cache is filling up and evicting cold records.
- Existent vs NXDomain – TTL of existent usually not truncated. Caching times of Hot vs Non-Hot queries are different. Google has counter intuitive results; non-hot queries are cached for a longer duration than hot queries.

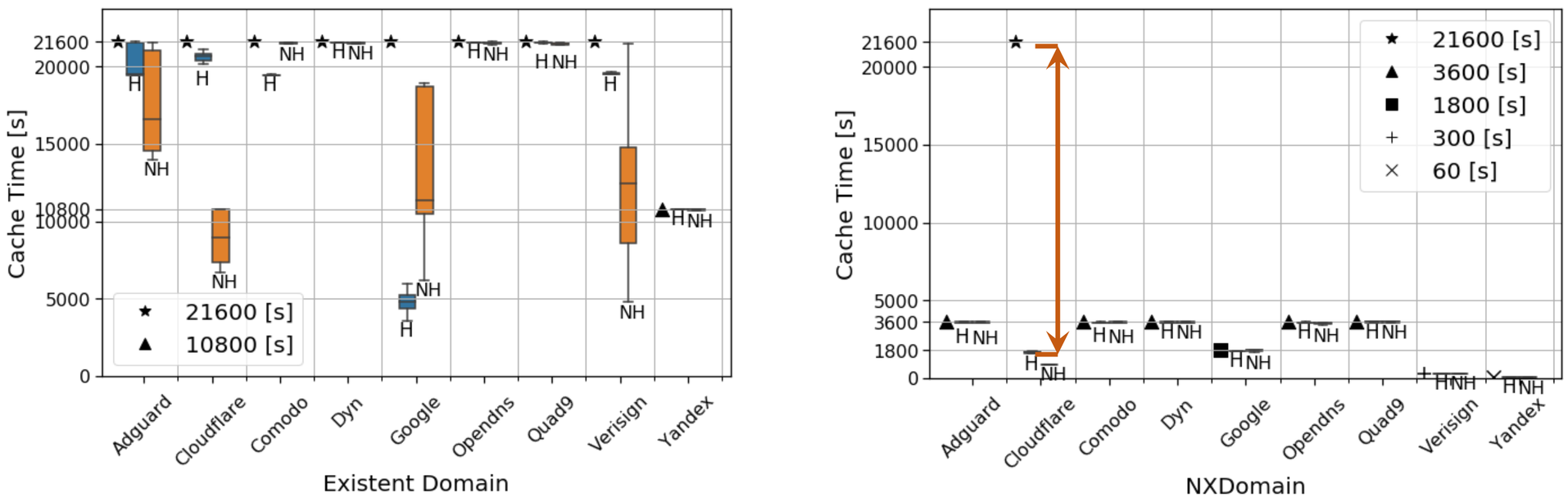

Fig. 4: Cache time observed in seconds per resolver for TTL value of 6 hours. H - Hot Query, NH - Non-Hot Query. Each Resolver has a marker to the left of the H/NH plots indicating the TTL as truncated by the resolver, values are presented in the marker legend ★▲■+×.

neta.peleg@post.idc.ac.il