DoH vs DoT

Geoff Huston, Joao Damas
APNIC Labs

What's the question again?

- We've seen two efforts to add session encryption in the stub-to-recursive resolution path
  - Use DNS over TLS over TCP
  - Use DNS over HTTPS (collectively that's HTTPS/2 and HTTPS/3)

- Some Android platforms have the ability to configure a "Secure DNS" resolver that then uses DOT to query the recursive resolver
- In some areas Firefox has adopted a "Trusted Recursive Resolver" program that uses DoH

But…

- Only nerds twiddle with the knobs
- So uptake is likely to be small
- Unless it is part of some automated framework where the user is not directly consulted

Can we measure DoT and DoH uptake?

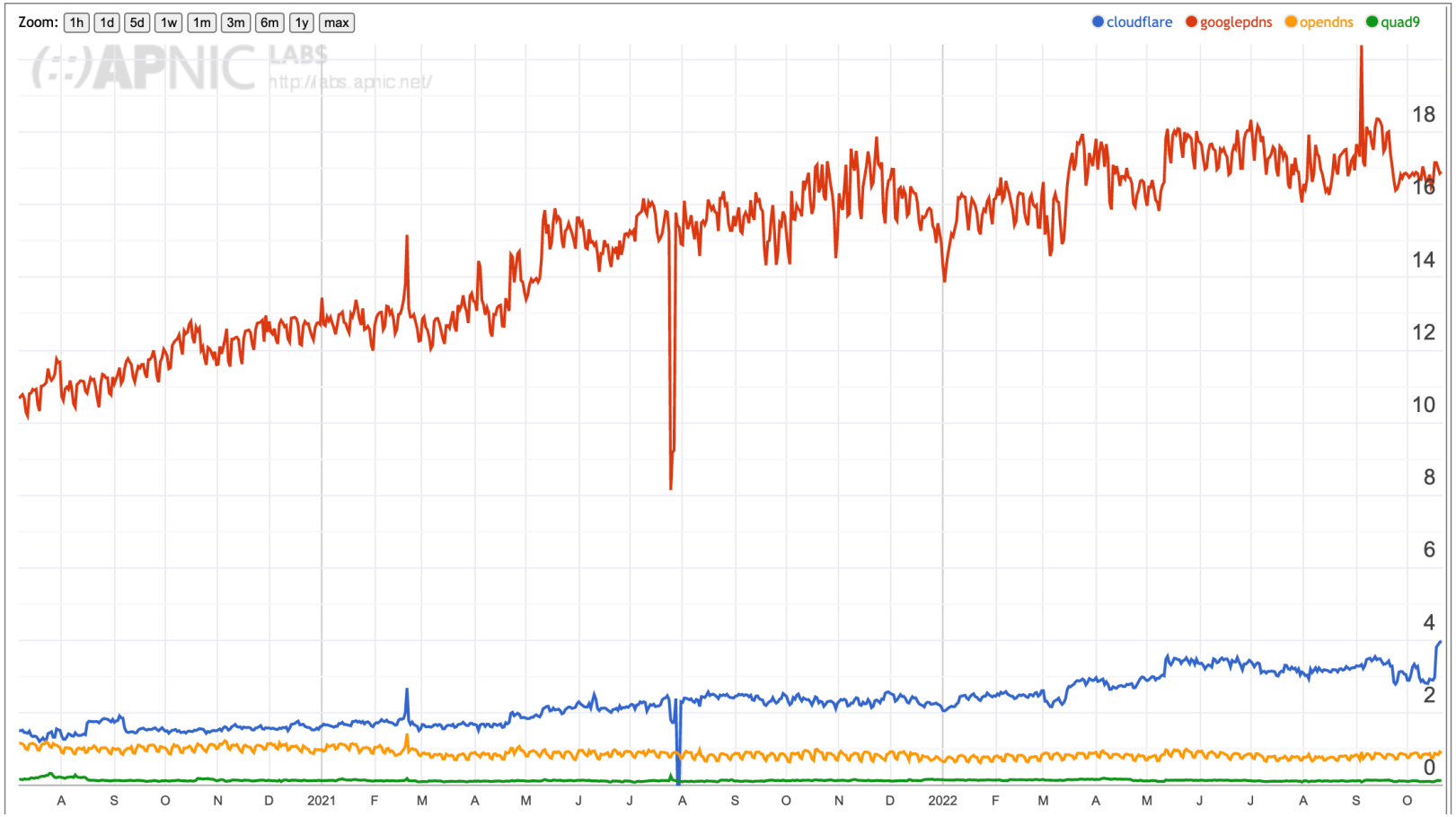
- Authoritative Servers can’t help
- Stub resolver data can’t really help (limited view)
- And recursive data is generally locked away
  - And quite properly so!

Recursive Resolver Data

At APNIC we have limited access to the data relating to the use of the 1.1.1.1 recursive resolver

- We don’t know who is querying, but we do see the query protocol
- The market share of Cloudflare’s open resolver service is around 4% of users which is a non-trivial resolver in the open resolver set (ranked #2 in terms of market share)

Cloudflare's "market share" of Open DNS resolvers



Google

Cloudflare's 1.1.1.1 is used by some 4% of eyeball users

Open DNS (Umbrella)

Quad 9

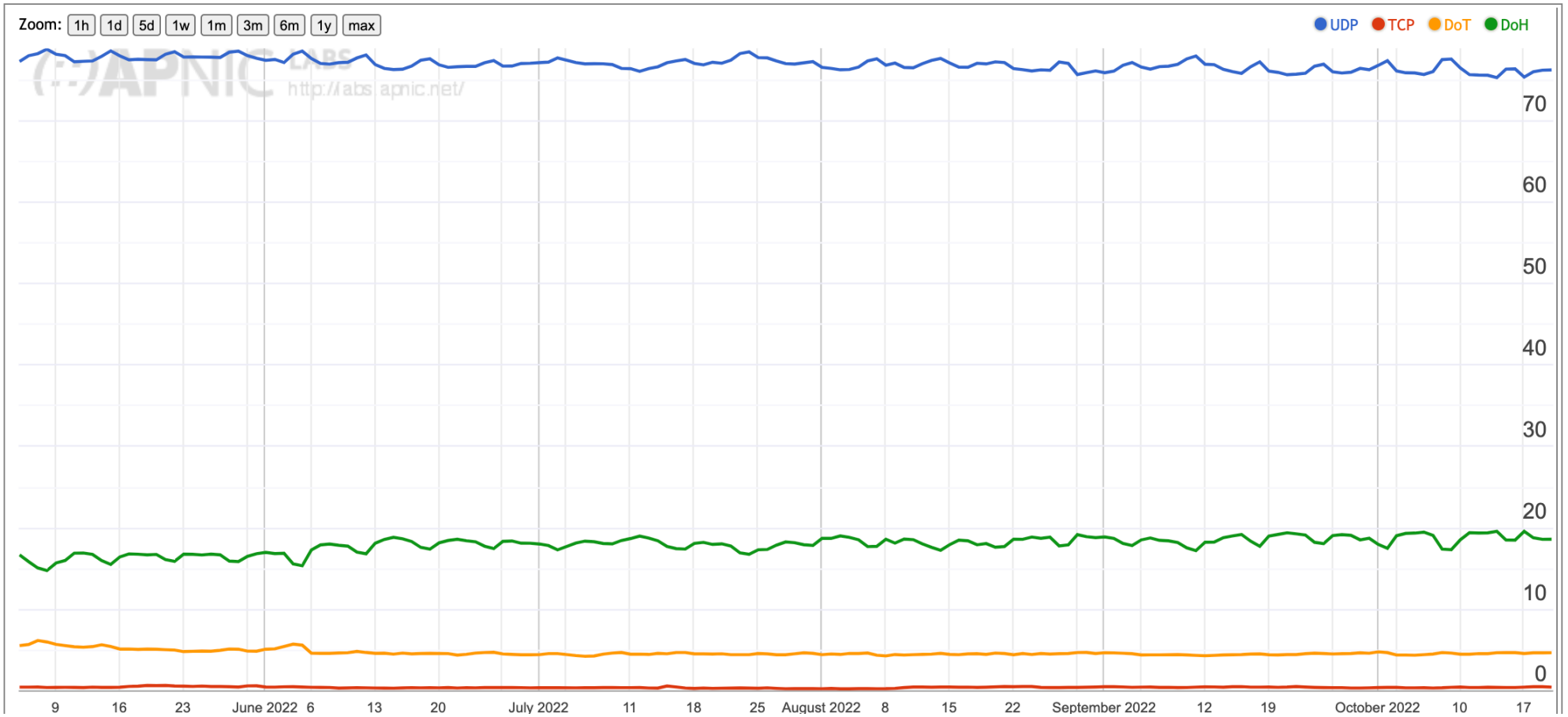
https://stats.labs.apnic.net/rvrs

Recursive Resolver Data

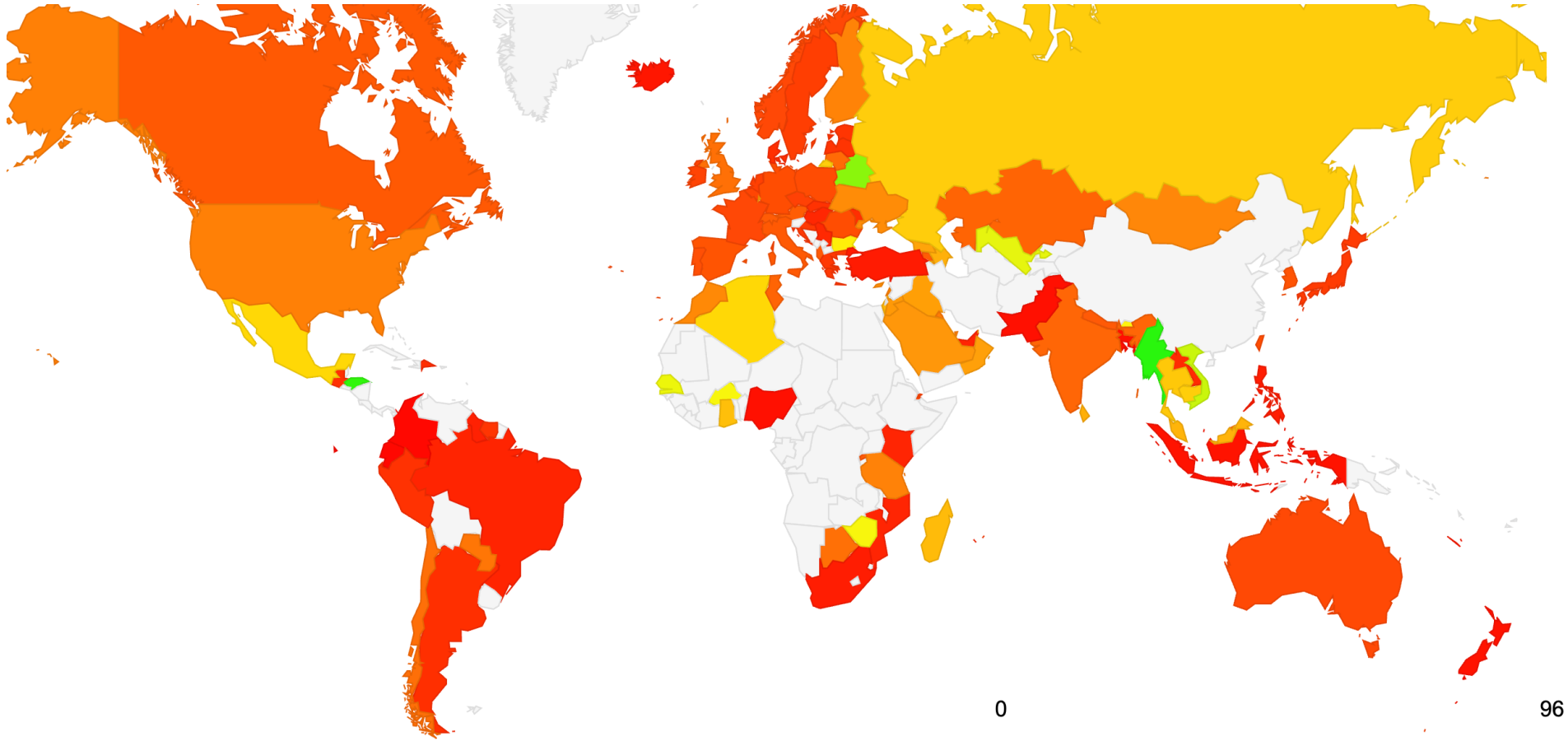
At APNIC we have limited access to the data relating to the use of the 1.1.1.1 recursive resolver

- We don’t know who is querying, but we do see the query protocol
- The market share of Cloudflare’s open resolver service is around 4% of users which is a non-trivial resolver in the open resolver set (ranked #2 in terms of market share)
- It’s a skewed view because it’s a TRR with Firefox

DoH vs DoT vs Do53



Where is DoH used?



DoH Use

- Appears to be correlated to the Firefox Trusted Recursive Resolver use

DNS over HTTPS (Trusted Recursive Resolver)

Terminology

DNS-over-HTTPS (DoH) allows DNS to be resolved with enhanced privacy, secure transfers and comparable performance. The protocol is described in RFC 8484 .

Trusted Recursive Resolver (TRR) is the name of Firefox's implementation of the protocol and the policy that ensures only privacy-respecting DoH providers are recommended by Firefox.

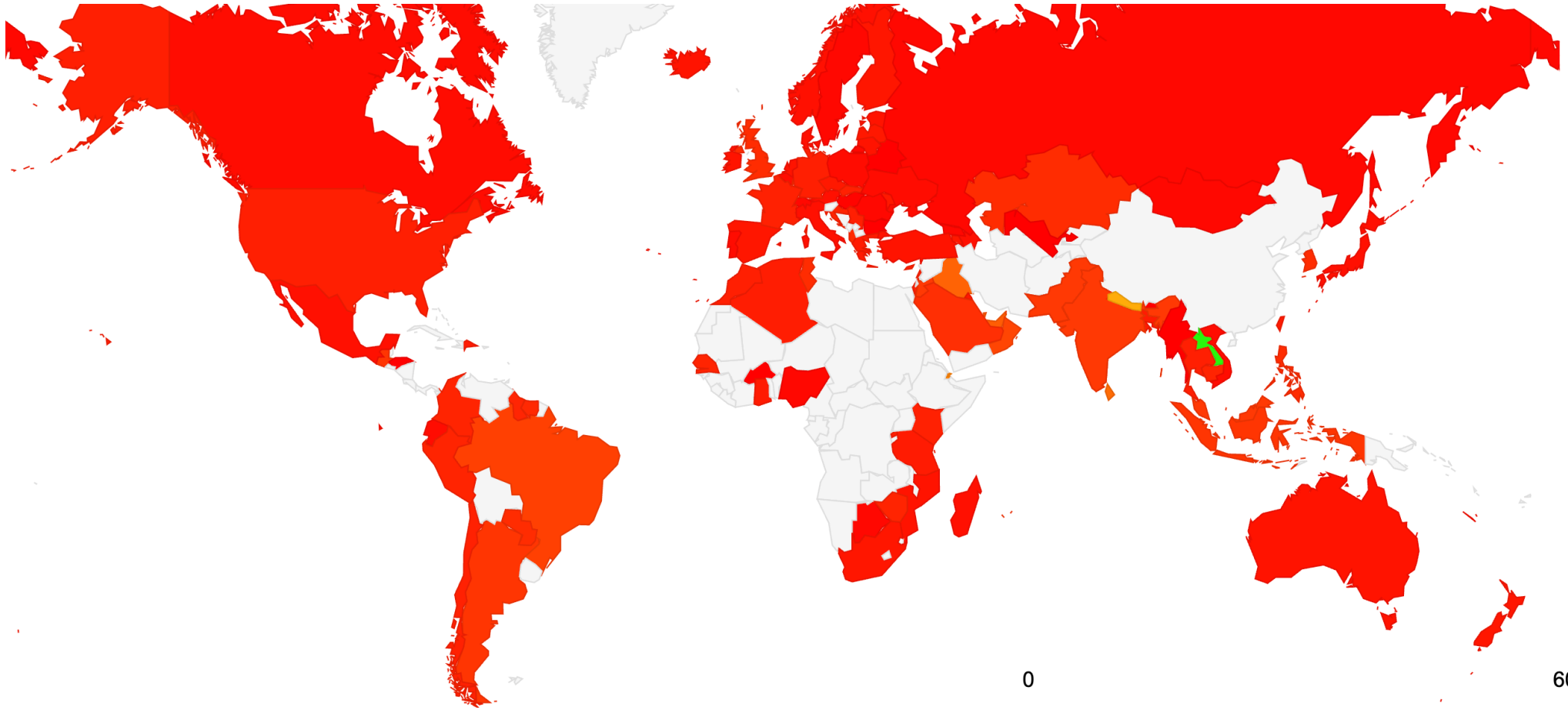
On this page we will use DoH when referring to the protocol, and TRR when referring to the implementation.

Unencrypted DNS (Do53) is the regular way most programs resolve DNS names. This is usually done by the operating system by sending an unencrypted packet to the DNS server that normally listens on port 53.

DoH Rollout

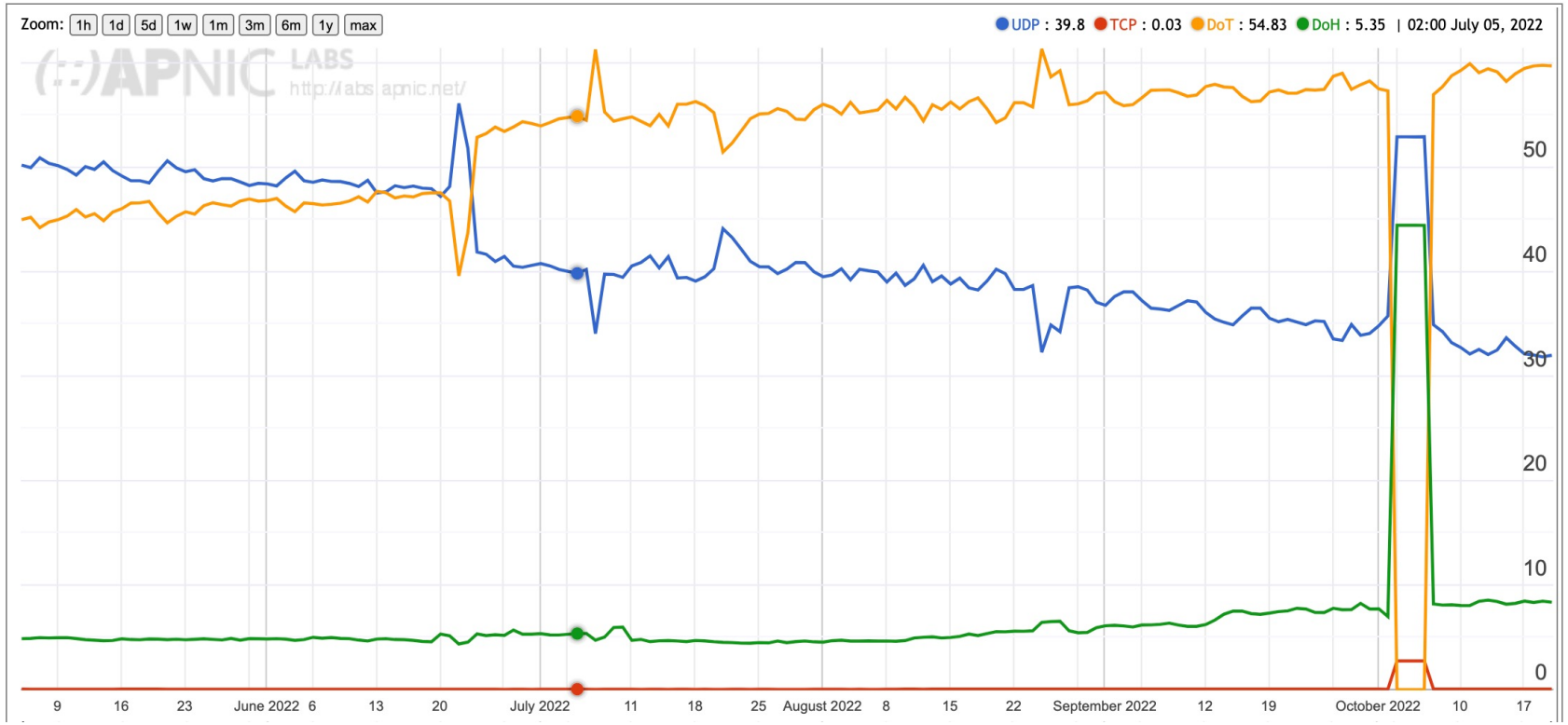
DoH Rollout refers to the frontend code that decides whether TRR will be enabled automatically for users in the rollout population.

Where is DoT used?



Laos!

Cloudflare Open Recursive Resolver DNS Query Profile for Lao People's Democratic Republic (LA)



Average Interval (days) 1

Hide country ASN List
Hide Regional Use
Redraw

Observations

- DoH use appears to be related to browser behaviour (Firefox)
  - Use levels are growing over the past 6 months
  - But its not clear whether this is Firefox-related, or other apps experimenting with DoH or <…>
- DoT use is relatively small with some singular exceptions (Laos)
  - Relative use levels are declining

Thanks!