No Port 53, Who Dis?

A Year of DNS over HTTPS over Tor

@alecmuffett, February 2021 — v2.0 final

Conclusion

My partner and I have exclusively used
DNS over HTTPS over Tor (DoHoT)
at home for 1 year

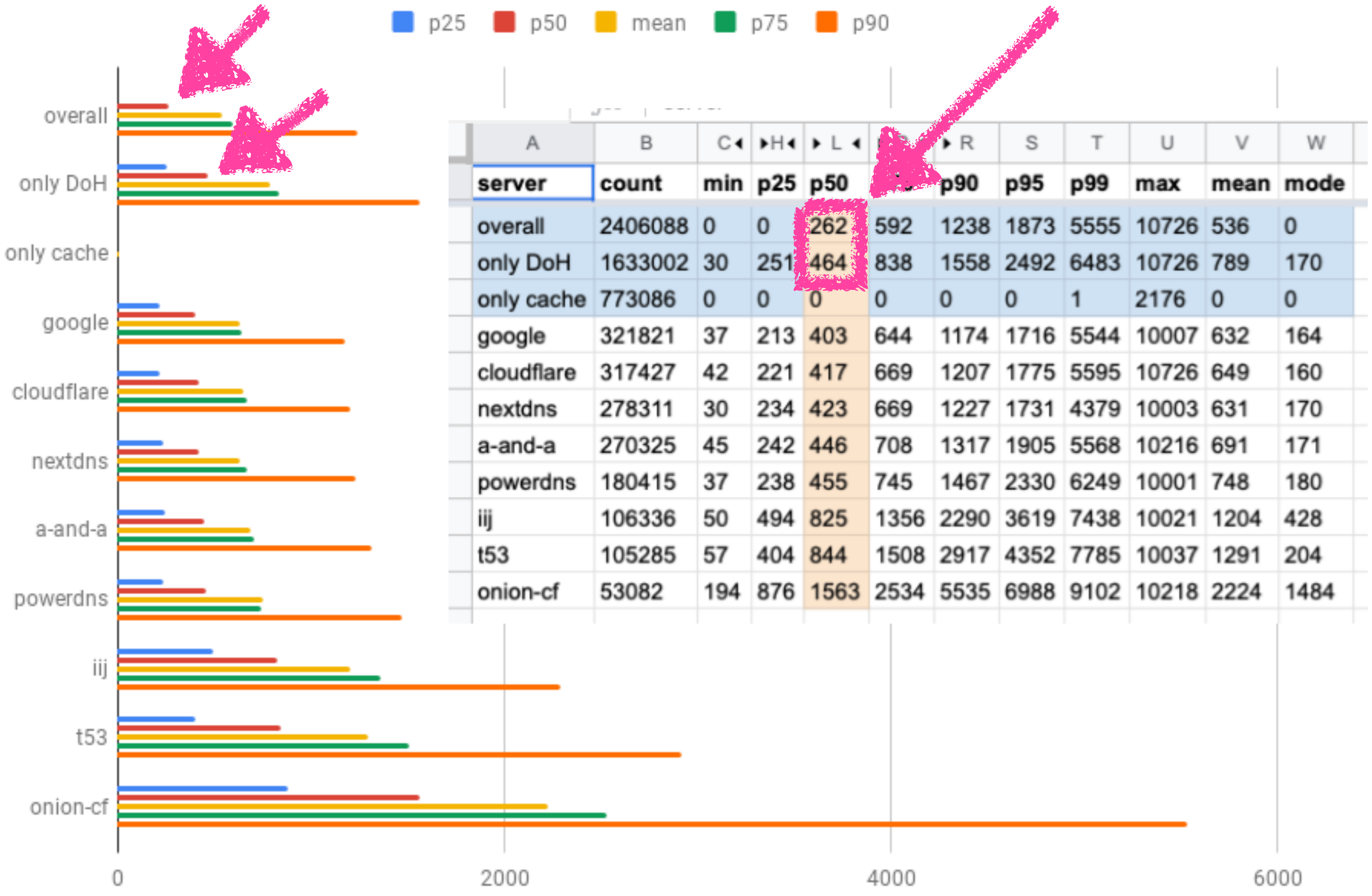
It worked fine

It worked so well that **I set it up and forgot about it from February to July**, because suddenly lockdown

Everything I'd read about this,
told me to **expect disaster**

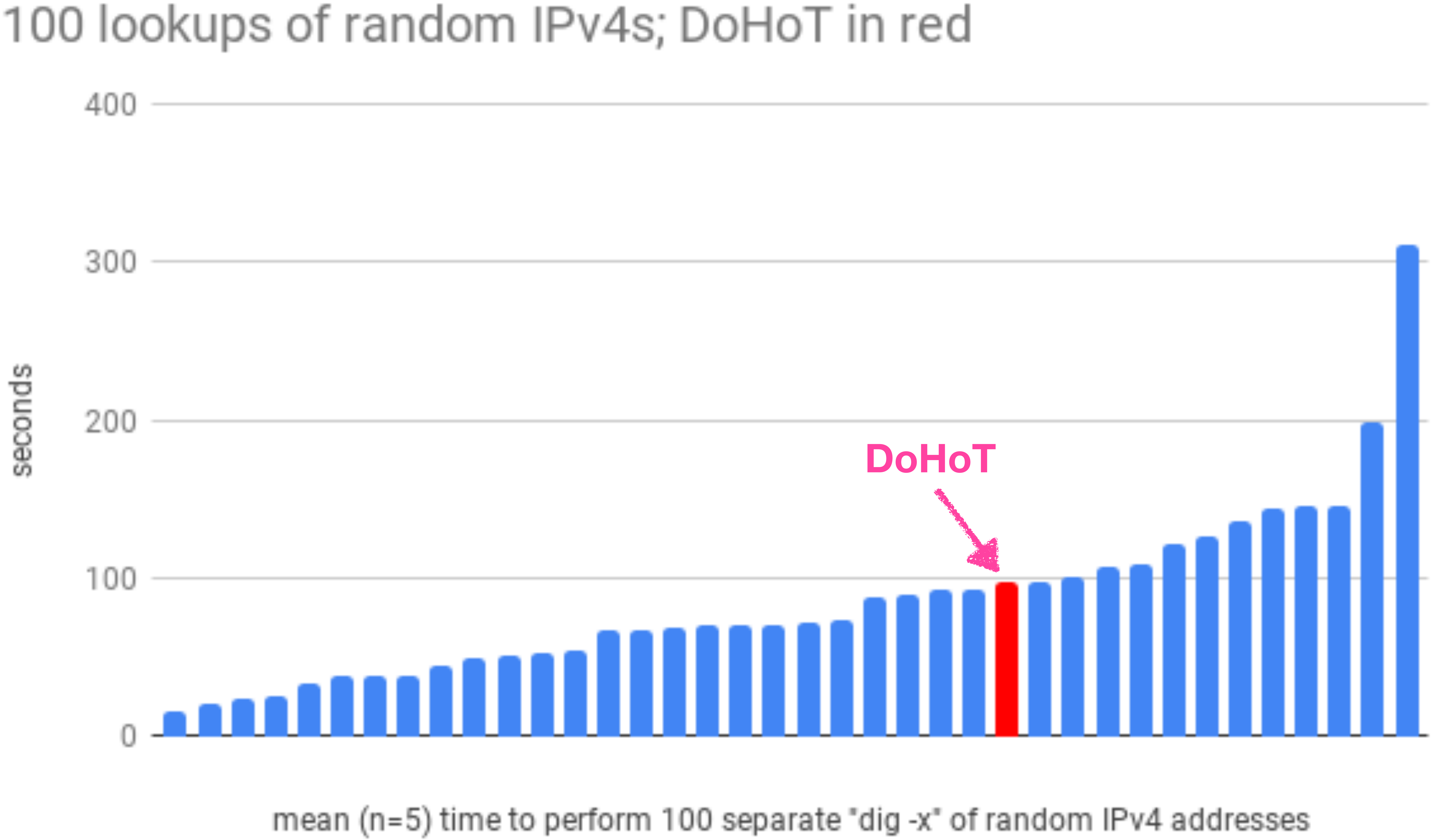
Everything I'd read about this, was and is **wrong**

It turns out that it's **not bad** to live with a median DNS latency of 250 to 500ms



server	count	min	p25	p50	p75	p90	p95	p99	max	mean	mode
overall	2406088	0	0	262	592	1238	1873	5555	10726	536	0
only DoH	1633002	30	251	464	838	1558	2492	6483	10726	789	170
only cache	773086	0	0	0	0	0	0	1	2176	0	0
google	321821	37	213	403	644	1174	1716	5544	10007	632	164
cloudflare	317427	42	221	417	669	1207	1775	5595	10726	649	160
nextdns	278311	30	234	423	669	1227	1731	4379	10003	631	170
a-and-a	270325	45	242	446	708	1317	1905	5568	10216	691	171
powerdns	180415	37	238	455	745	1467	2330	6249	10001	748	180
iij	106336	50	494	825	1356	2290	3619	7438	10021	1204	428
t53	105285	57	404	844	1508	2917	4352	7785	10037	1291	204
onion-cf	53082	194	876	1563	2534	5535	6988	9102	10218	2224	1484

It turns out that **some people live with worse** performance, day-in, day-out


100 lookups of random IPv4s; DoHoT in red
400
300
200
100
0
seconds
DoHoT
mean (n=5) time to perform 100 separate "dig -x" of random IPv4 addresses

It turns out that some people choose latency to **obtain value** more

Some people filter their DNS, who knew?

24	dr1a		30	myself	125	104	51	84	82	51	125	89.2	74
25													34
26													26
27	am1a	20	70	dohot	122	88	103	106	66	66	122	97	56
28	db1a	20	200	pihole-cloudflare	89	84	108	80	125	80	125	97.2	45
29	jr1d	100	1000	cloudflare	115	94	101	82	111	82	115	100.6	33
30	le1h				102	158	109	110	57	57	158	107.2	101
31	jr1f	100	1000	cloudflare	92	91	125	113	123	91	125	108.8	34
32	jr1b	100	1000	quad9_unfiltered	117	155	137	125	71	71	155	121	84
33	db1b	20	200	pihole-quad9	212	87	101	178	52	52	212	126	160
34	ya1a	10	100	cloudflare	132	133	151	129	135	129	151	136	22

It turns out that presuming to argue
5ms vs 50ms vs: 500ms DNS latency,
is a presumptuous act of **tech privilege**

minimum latency isn't everything

latency is only a fraction of the user experience and value proposition

... albeit one that's easy to measure and compare

... which probably explains why we are so hung up about it

If you accept this perspective,
why not invest the **latency budget**
in order to pursue better **privacy value**?

DoHoT Rationale

Assume for simplicity that ...

In a domestic context, or similar ...

- **ISP blocks/allows are by port**, or by **tuples of {ip, net} address & port**
- **HTTPS** is not "wildcard" blockable (cf: "`port 53 and not host A.B.C.D`")
  - ... as it is the "raison d'être" of modern communication ...
- **Tor** is **"hard" to globally surveil**, and **resistant to block, collusion or subpoena**
  - ... Tor's relay cloud & "triple-hop" system greatly complicates correlation ...
  - ... bad actors can run bad relays, but Tor actively hunts / resists them ...
- **HTTPS** adequately assures identity via certificates

DoHoT was designed to address ...

a **privacy-invasive threat model** based around actors who ...

1. may **surveil my network links**
2. **block my queries** to my chosen proxies or resolvers
3. **tamper** with those queries
4. **block responses** from my chosen proxies or resolvers
5. **tamper** with those responses
6. **pretend to be** my chosen proxies or resolvers
7. may **learn that my identity is/was associated with** particular queries or responses
8. may **surveil the path to and beyond** my chosen proxy and resolver, pursuing 7. (e.g. correlation attack)
9. may **collude with, or** FISA / **subpoena logs from**, my proxies or resolvers, pursuing 7.

Comparative Analysis

According to the DoHoT threat model ...

- **Do53** risks all of these;
  egregiously insecure yet somehow ubiquitous

- **DoT** risks 2, 4, 7, 7+8, 7+9;
  port blocks, second-party surveillance, third-party surveillance or collusion

- **DoH** risks 7, 7+8, 7+9;
  second-party surveillance, third-party surveillance or collusion

- **ODNS** risks *2, *4, 7+8, 7+9
  ***maybe** port blocks, third-party surveillance or collusion

- **ODoH** risks 7+8, 7+9
  third-party surveillance or collusion; proper use requires an informed user

- **DoHoT** risks ... arguably **none of the above**, unless Tor relays become severely compromised

ODxx (ODNS and ODoH) are interesting

but suffer from issues that Tor actively works to address

- Designers appear to have made choices primarily to minimise **latency** impact
- Choices include: tiers of **single-layer proxies** that may be open to:
    - **selective ip-blocks** (cf: Russia/AWS, Iran/Signal, vs: Tor bridges, obs4proxy, ...)
    - **"both sides" surveillance** with timing & metadata, to **synthesise collusion**
- (ODoH) user *may* accidentally choose proxy that is run by the same organisation which runs their resolver, yielding unintentional self-collusion:
    - "*Choose a different proxy orgo from your resolver orgo, or bad things may happen*"
    - User education is **hard** and **expensive** and **easy to miss or mess up**

Consequently ...

If **you need strong DNS privacy**, then **deploy DoHoT**

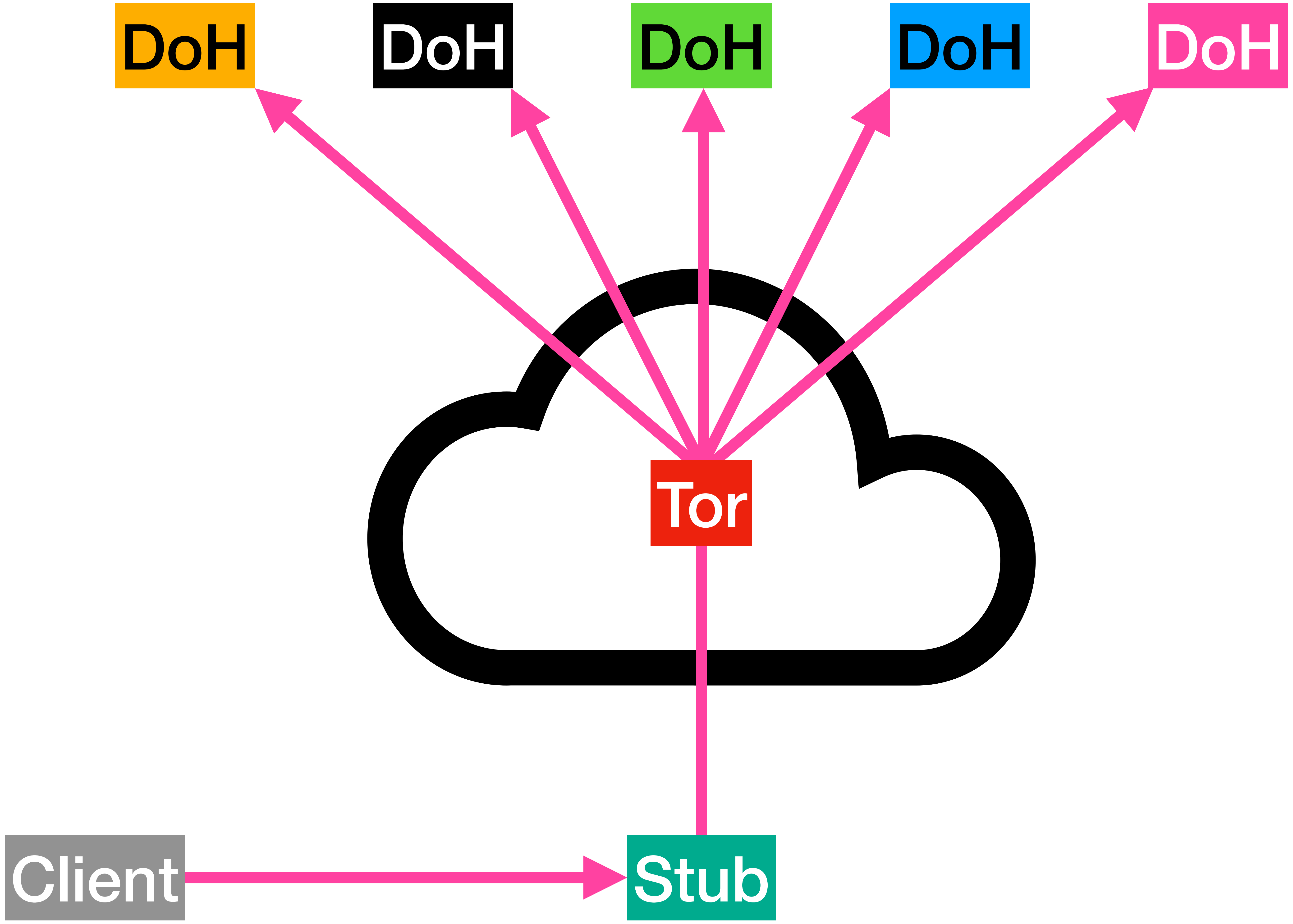
- It's **free**, it **exists**, it requires **no new tooling**, and it's **easy**
  - **You are in control**, you can **roll your own**
- It's an **operational practise** rather than a protocol
  - downside: less opportunity for publication in research journals
    - maybe some **research on cache-tuning**, but maybe "why bother?"
    - some "standardisation" would be good to **increase uniformity of queries**
- If **performance is on par with Pi-hole**, there are already privacy-centric communities who would **value the latency-privacy tradeoff**

Architecture

Obligatory Architecture Slide

- I set up a copy of **dnscrypt-proxy** configured as a **stub resolver**
  - presented to the LAN as a DHCP Do53 DNS Service, enforced by firewall
  - configured to **make all resolution requests over Tor** (via SOCKS5)
  - attempting to **minimise fingerprintable metadata** (e.g. session tix, ciphers)
  - into a **load-balanced pool of public DoH servers**
  - which are **chosen to offer both DNSSEC and** a promise of "**no filters**"
- ... **and that's all**.

Terrible Network Diagram



Rhetorical Question

If we can address the entire **threat model** within a reasonable **latency budget**, why address a **mere subset** of it?

Utter Strawman Answers ...

We should **solve privacy centrally**, not on the client-side ...

Every solution suggests at least client code-changes, if not use of proxy or stub resolvers.
Also: isn't DNS meant to be a "distributed" protocol? Doesn't that also involve the clients?

We need to **solve this for everyone**, so we need a privacy solution that scales ...

That's admirable, but what's your baseline threat model and value proposition? Latency?

If DNS "goes dark" then "the authorities" will be forced to regulate it more tightly ... (e.g. TLS1.3 vs: ETS/eTLS)

The capabilities of democratic states today will be those of totalitarian despots tomorrow.
Personally, I feel that we should plan for, and proactively mitigate the latter.

We reject this "**NSA-inspired**" threat model as being {**unrealistic, impolitic, illegal, ...**}

Fine, it'll be incumbent upon you to explain to people what you're NOT defending against, and why.

Your stats are **inadequate** / don't stack up!

Awesome, go measure and publish. We need diverse, holistic, value-centric user experience data.

Other?

I'd love to see fresh consideration.

If you only remember 1 slide ...

Please stop thinking of **latency** as **cost**

Please consider it a **budget** to **offer value**

`github.com/alecmuffett/dohot`