

DoH Bench: Measuring Public DoH Resolvers from the User's Browser



Jhannes Reimann



Robert Richter



Vaibhav Bajpai

*Chair of Data-Intensive Internet Computing
Hasso Plattner Institute, University of Potsdam*

Try DoH Bench



<https://dns.diic-hpi.org>

**Design IT.
Create Knowledge.**

www.hpi.de



How to make an Informed Decision what Recursive Resolver to use?

Problem Statement



<https://dns.diic-hpi.org>



The User's DNS Problem

- Every page access requires a lot of DNS queries
- Public DoH adds security and hygienic features (e.g., add blocking)
- But a decision for a public resolver depends on the individual machine



Requirements of Good Measurement Tooling?

- Ease of measurement
- No installation of random tooling
- No payments
- No tracking
- Unbiased methodology

What is the most fitting resolver for the user's concrete setup?

DoH Bench runs a set of measurements to come up with a **concrete resolver recommendation**

How to make an Informed Decision what Recursive Resolver to use?

Available Tools

CLI / Desktop

- **Accurate, but installation requirements create a high barrier**
⇒ in enterprises often not an option as arbitrary tooling not always allowed
- **Often Do53 (DNS over UDP) focused**

Server-Side Benchmarks

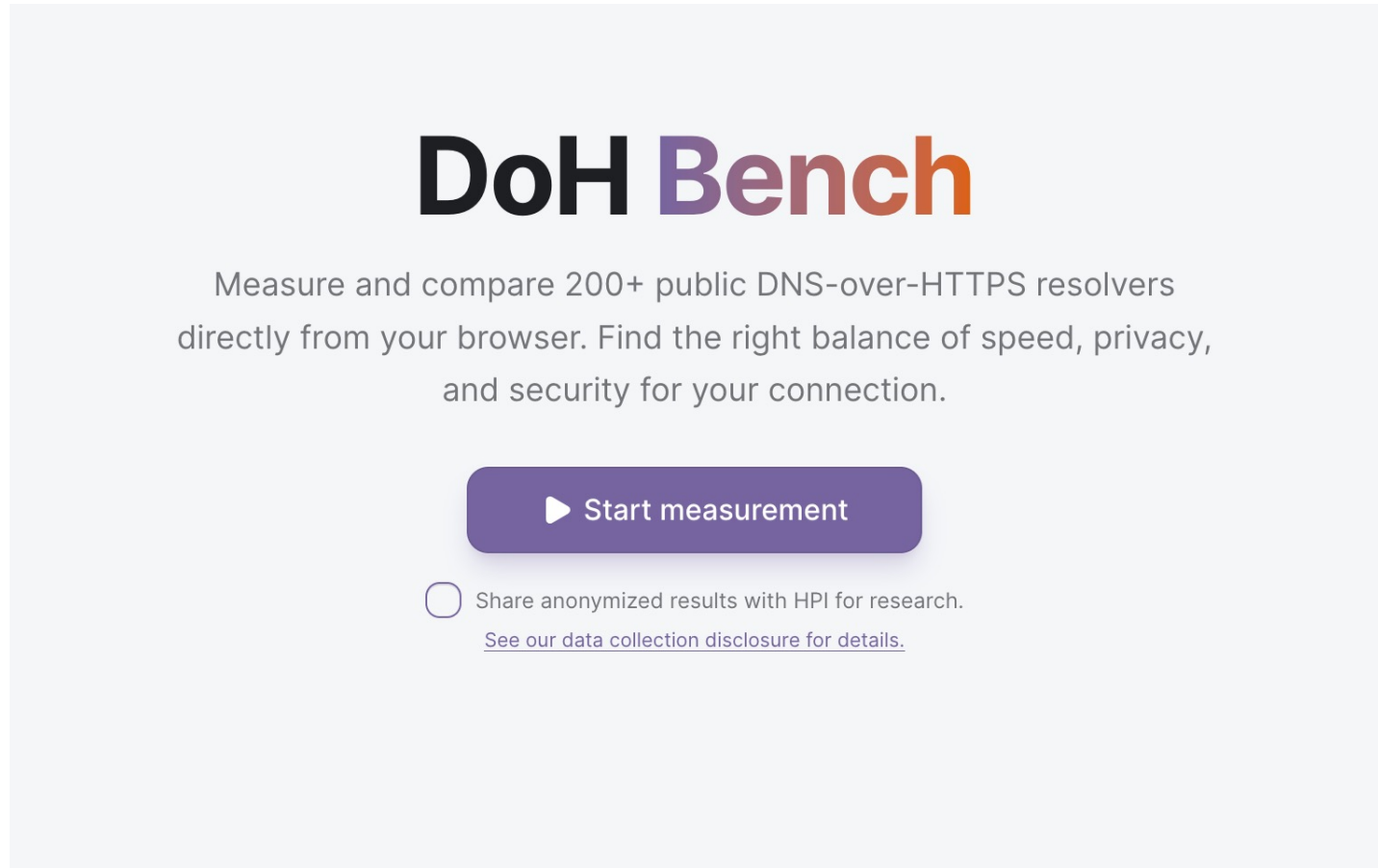
- **Hard to account for the user's setup (browser, network connection, ...)**

Browser Measurement

- **Low-barrier as access is easy**
- **Limitations apply:**
CORS verification
Only DoH
No ISP-operated resolvers

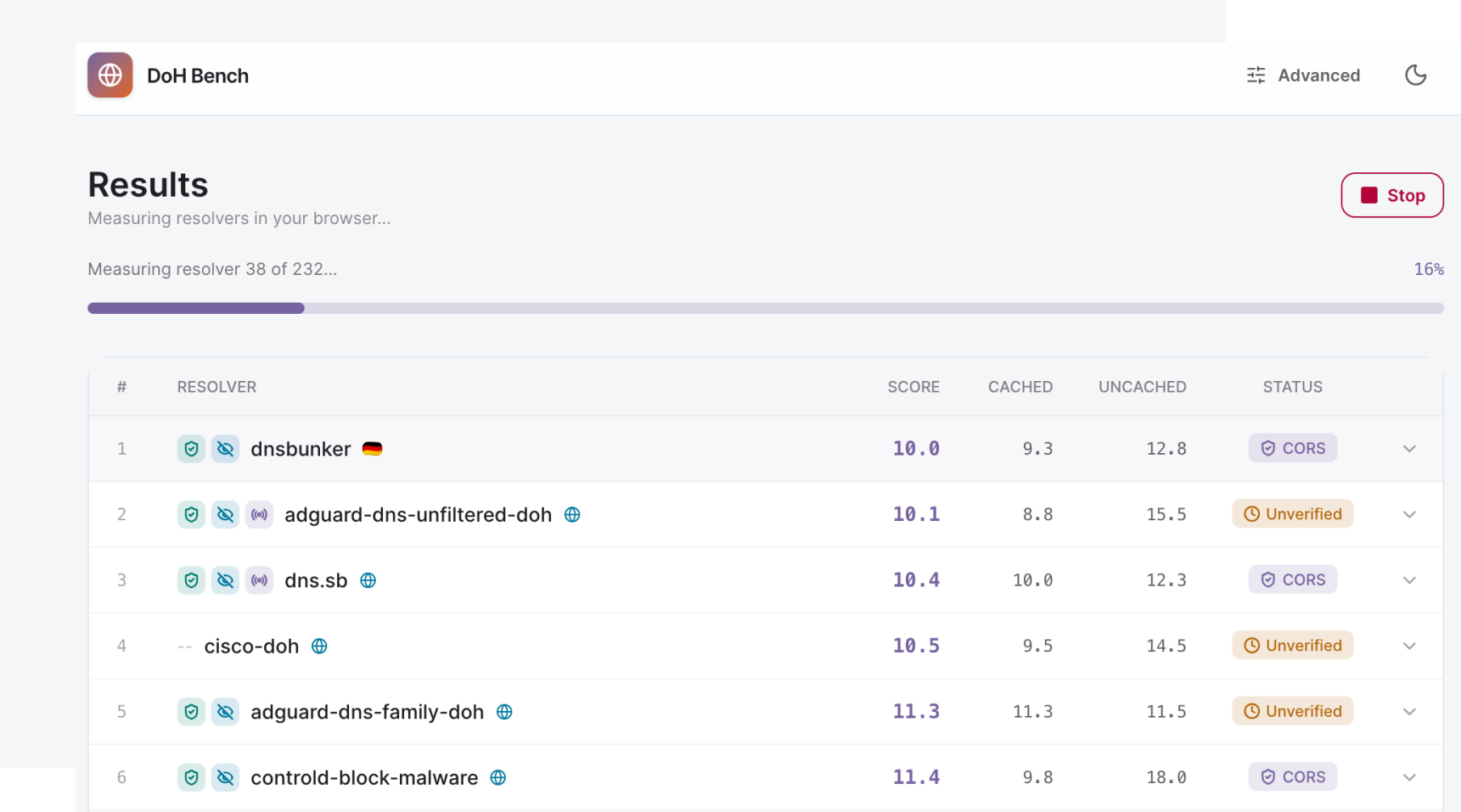
How to make an Informed Decision what Recursive Resolver to use?

Our tool: DoH Bench



How to make an Informed Decision what Recursive Resolver to use?

Our tool: DoH Bench



How to make an Informed Decision what Recursive Resolver to use?

Our tool: DoH Bench



DoH Bench

Advanced

Run again

Results

179 measurable · 53 offline

Measuring

Measuring

RECOMMENDED

Canary

mullvad-family-doh

DNSSEC

No-logs

SCORE	CACHED	UNCACHED
8.6 _{ms}	7.8 _{ms}	12.0 _{ms}

✓ Among the fastest measured

✓ DNSSEC validation

✓ No-logs policy

✓ Verified via canary log

USE THIS RESOLVER (DOH URL)

https://family.dns.mullvad.net/dns-query

Copy

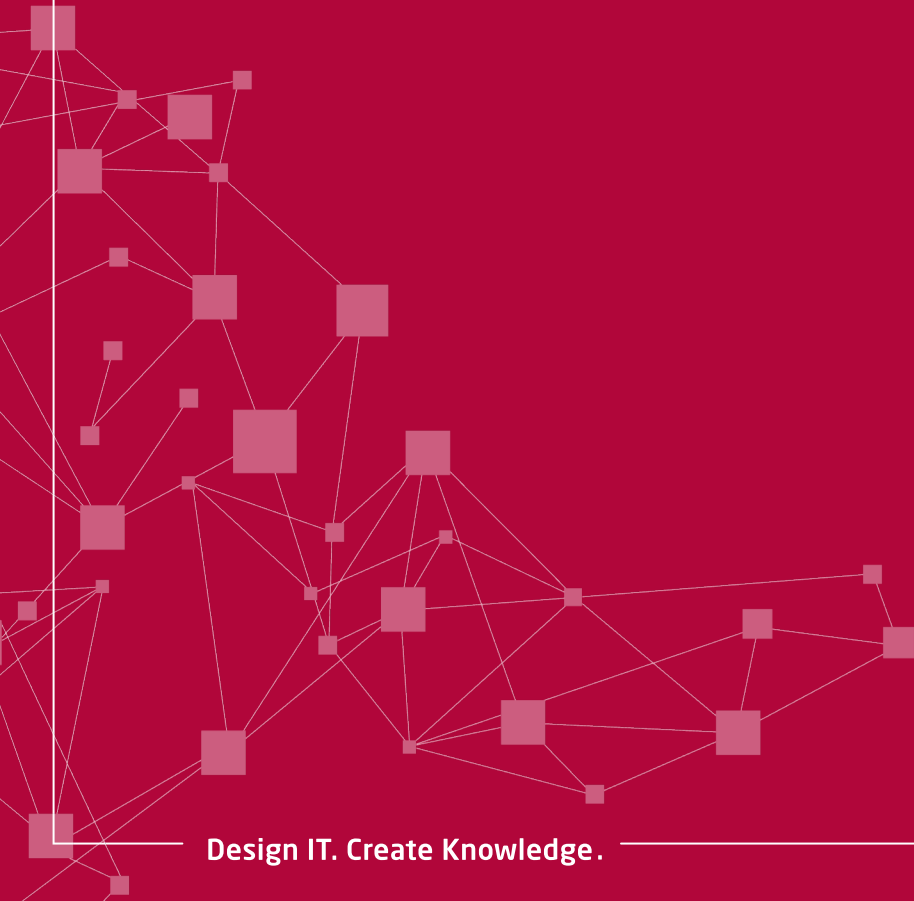
System IP

194.242.2.6

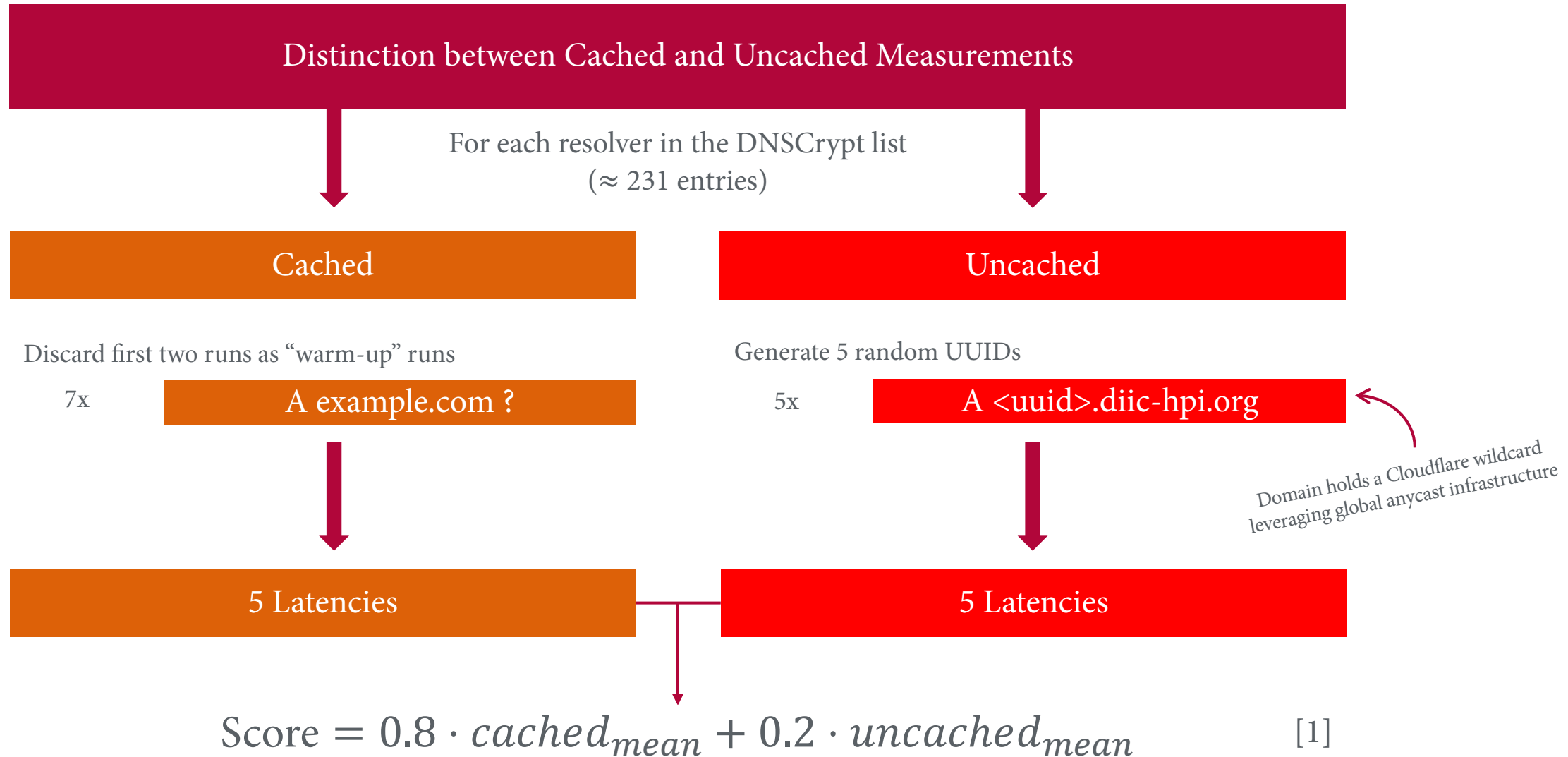
Copy

Paste the DoH URL into your browser's Secure DNS setting, or use the IP in your system network settings.

DNS Measurement Methodology



Measurement Sequence

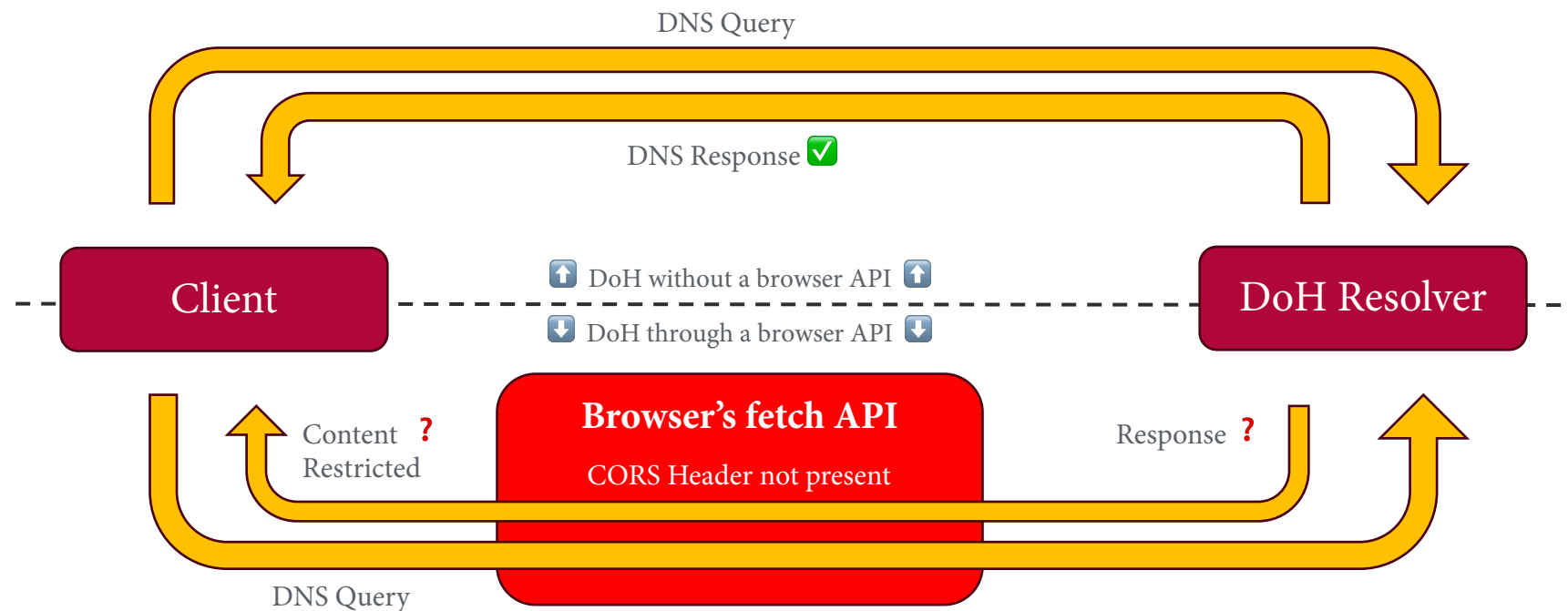
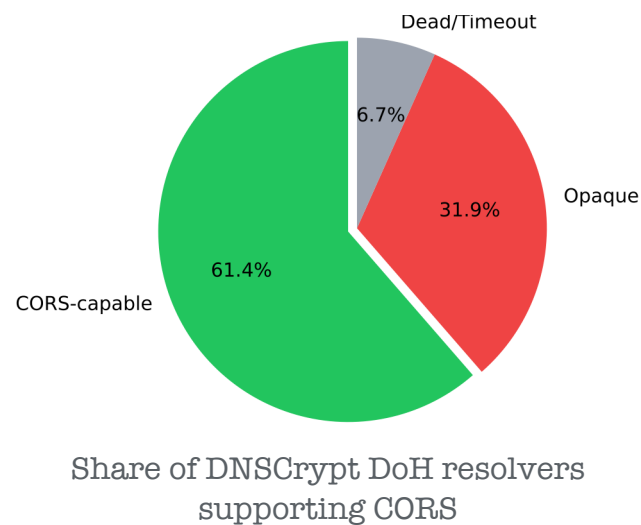


The CORS Problem

- CORS (Cross-Origin Resource Sharing) is a browser security mechanism that allows a client to access a resource (*RFC 6454*)
- The server sends an HTTP header that allows access.

How to verify the DNS response was valid if CORS header is missing?

HPI



Three-Tier Verification Architecture



Problem: How to verify the expected queries have actually been made?

⇒ Three steps to verify responses, even if CORS headers are not set!

1

DNS Response Validation

- Does the response contain a hard-coded fixed IP address?
- Fails if CORS headers are not set

2

Canary Logs

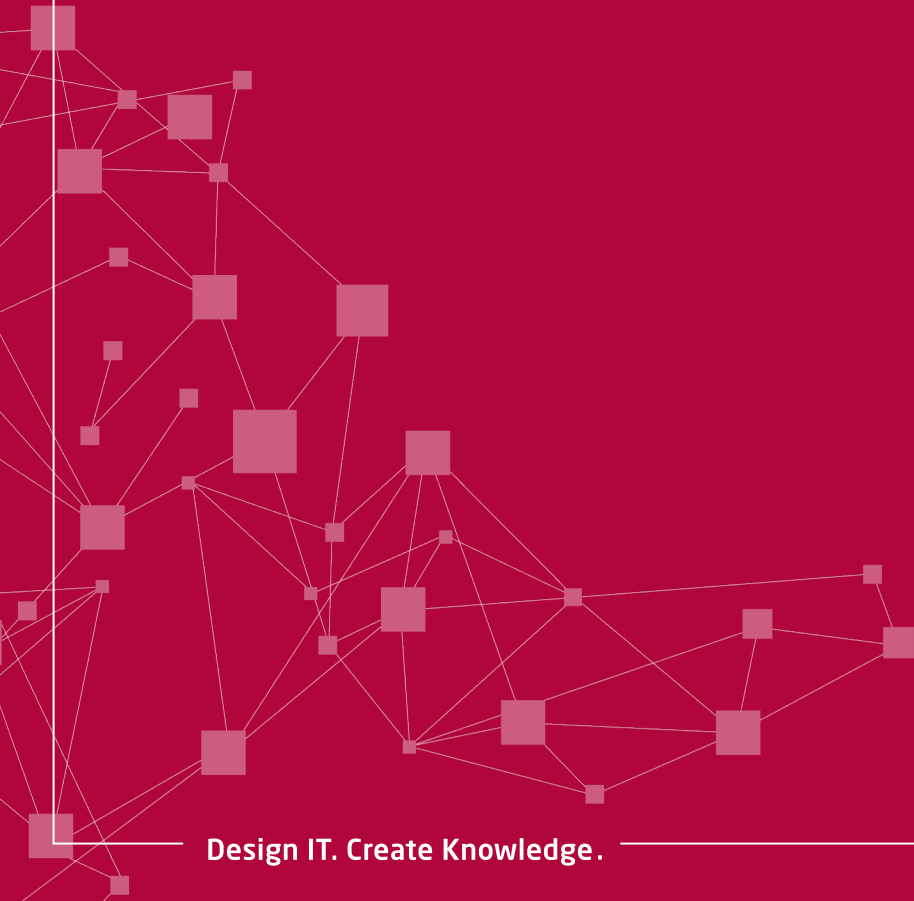
- Parallel authoritative Bind9 server that logs queries
- Parallel (untimed) DNS query to resolver for `<uuid>.verify.diic-hpi.org`
- Resolver is verified if log contains uuid

3

Cloudflare Query Logging (Fallback)

- Polling Cloudflare backend for their authoritative logs
- BUT:
 - Highly rate-limited
 - Adaptive sampling in CF causes false negatives

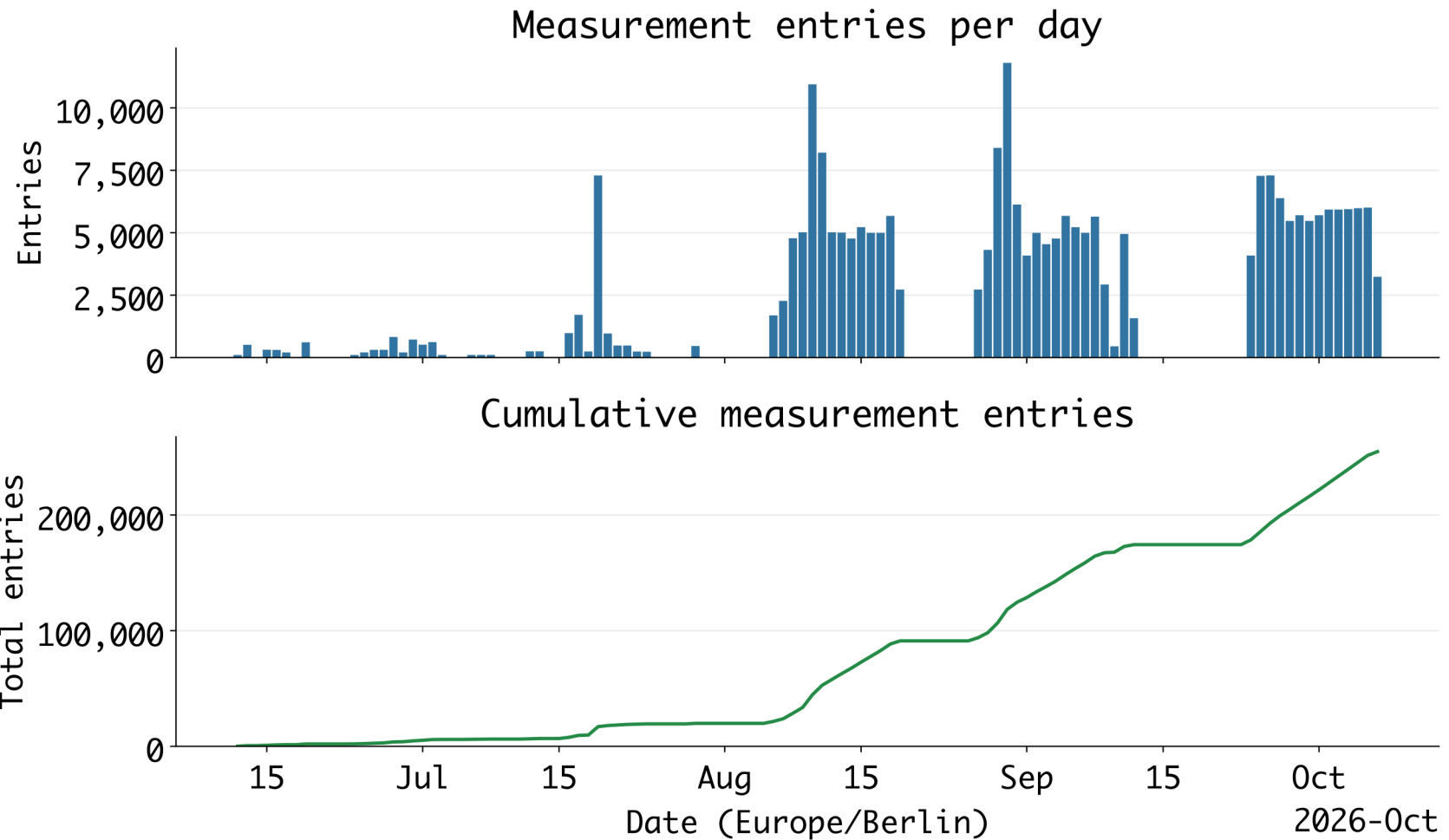
Preliminary Results



Number of Measurements

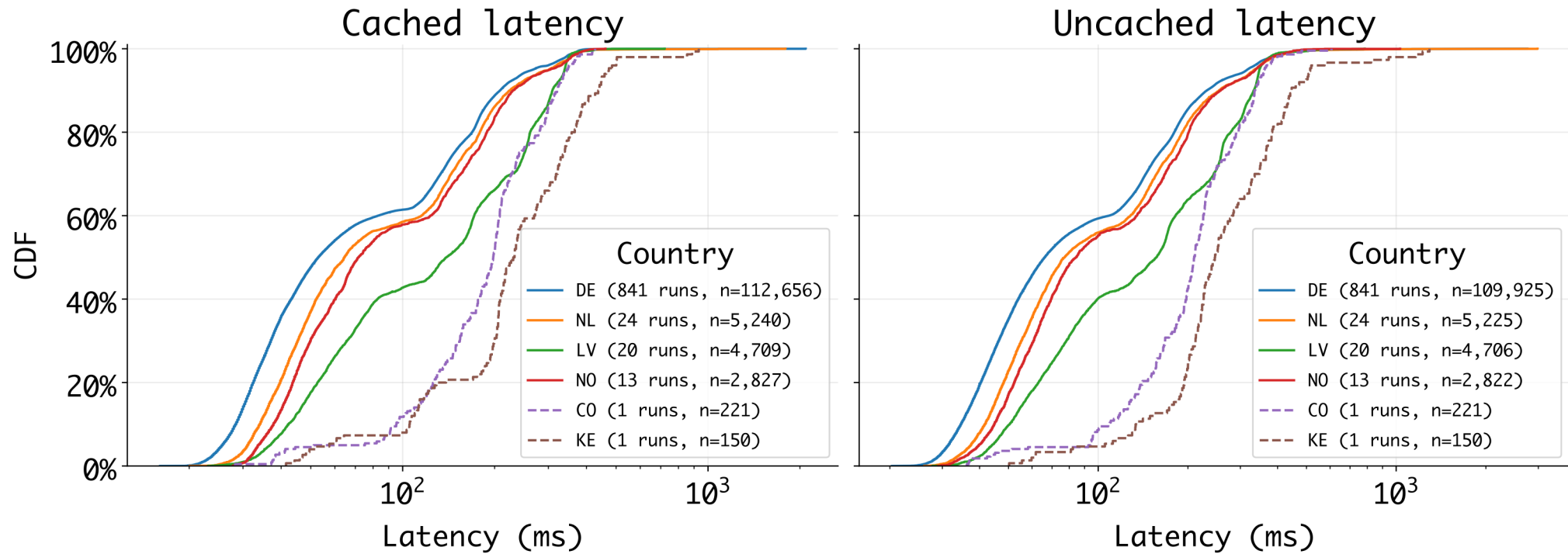


Total **286,910** individual resolver measurements from **1,296** measurement runs



80 ASes covered in **27** countries

Case Study – Starlink Latencies across Countries



- Most measurement points for European countries (Germany, Netherlands, Latvia, and Norway)
- Those countries also show lowest latency

Case Study – Starlink Latencies across the Top Resolvers



Plenty of
alternatives to CF



cisco-doh
cloudflare
controld-block-malware-ad
dnsbunker
dnscry.pt-doh-frankfurt-ipv4
dnscry.pt-doh-frankfurt02-ipv4
dnscry.pt-doh-nuremberg-ipv4
doh-cleanbrowsing-family
doh-cleanbrowsing-security
mullvad-extend-doh
mullvad-family-doh
quad9-doh-ip4-port443-nofilter-ecs-pri
quad9-doh-ip4-port443-nofilter-pri

Cached latency

Uncached latency

cisco-doh	29.0 ms n=553	37.1 ms n=24	41.0 ms n=13	35.1 ms ☹️ n=20	35.8 ms n=552	45.1 ms n=24	42.8 ms n=13	46.2 ms n=20
cloudflare	30.2 ms n=571	34.9 ms n=24	39.5 ms n=13	37.3 ms n=20	35.6 ms n=570	35.4 ms ☹️ n=24	46.2 ms n=13	43.7 ms ☹️ n=20
controld-block-malware-ad	31.5 ms n=568	33.0 ms n=24	37.0 ms ☹️ n=13	52.0 ms n=20	35.8 ms n=563	40.5 ms n=24	41.2 ms ☹️ n=13	55.7 ms n=20
dnsbunker	28.8 ms n=533	34.6 ms n=24	40.8 ms n=13	256.5 ms n=20	33.2 ms n=530	36.9 ms ☹️ n=24	41.0 ms ☹️ n=13	257.9 ms n=20
dnscry.pt-doh-frankfurt-ipv4	26.8 ms ☹️ n=505	31.8 ms ☹️ n=24	37.8 ms n=13	33.6 ms ☹️ n=20	33.0 ms n=498	38.2 ms ☹️ n=24	44.0 ms n=13	45.3 ms n=20
dnscry.pt-doh-frankfurt02-ipv4	27.0 ms ☹️ n=515	31.6 ms ☹️ n=24	37.8 ms n=13	56.9 ms n=20	34.0 ms n=512	39.9 ms n=24	45.8 ms n=13	64.1 ms n=20
dnscry.pt-doh-nuremberg-ipv4	29.2 ms n=503	31.2 ms ☹️ n=24	47.2 ms n=13	39.2 ms n=20	43.5 ms n=504	45.5 ms n=24	61.5 ms n=13	56.7 ms n=20
doh-cleanbrowsing-family	28.5 ms n=537	36.4 ms n=24	38.8 ms n=13	38.4 ms n=20	32.8 ms n=532	41.9 ms n=24	41.0 ms ☹️ n=13	42.9 ms ☹️ n=20
doh-cleanbrowsing-security	28.0 ms n=545	33.1 ms n=24	37.8 ms n=13	37.2 ms ☹️ n=20	32.0 ms ☹️ n=539	42.9 ms n=24	43.5 ms n=13	45.3 ms n=20
mullvad-extend-doh	27.0 ms n=508	33.1 ms n=24	41.2 ms n=13	38.3 ms n=20	32.0 ms ☹️ n=508	40.6 ms n=24	48.0 ms n=13	44.0 ms n=20
mullvad-family-doh	26.5 ms ☹️ n=501	32.9 ms n=24	37.8 ms n=12	38.1 ms n=20	32.0 ms ☹️ n=496	44.9 ms n=24	44.5 ms n=12	41.5 ms ☹️ n=20
quad9-doh-ip4-port443-nofilter-ecs-pri	29.0 ms n=457	39.8 ms n=19	35.2 ms ☹️ n=13	38.8 ms n=20	37.9 ms n=378	40.6 ms n=18	48.2 ms n=13	48.0 ms n=20
quad9-doh-ip4-port443-nofilter-pri	29.2 ms n=491	37.5 ms n=24	36.8 ms ☹️ n=13	37.9 ms n=17	44.0 ms n=414	54.0 ms n=23	45.8 ms n=12	47.1 ms n=18

Median latency (ms)



Germany 841 runs Netherlands 24 runs Norway 13 runs Latvia 20 runs Germany 841 runs Netherlands 24 runs Norway 13 runs Latvia 20 runs

Supporting the Project

Data is soon going to be published regularly.

- Most data is collected from periodic measurements from probes
- A probe is a Docker container executing the following image:
<https://hub.docker.com/r/richterrobert/dnsrr-headless-probe>
 - Spins up headless Firefox with Selenium, clicks on opt-in, and then runs the measurement until its finished
- Currently 6 probes running, including four probes from **LEOScope** [1]

[1] Fadaei, Saeed et al. "Leoscope: Building a global testbed for low-earth orbit satellite networks." *ACM SIGCOMM Computer Communication Review* 55.2 (2025)

Looking for a PhD position?
⇒ <https://hpi.de/bajpai>

