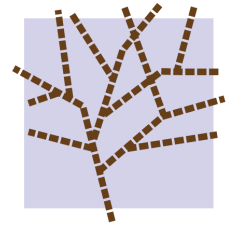




NLNETLABS

Willem Toorop



DNS-OARC 39

23 October 2022

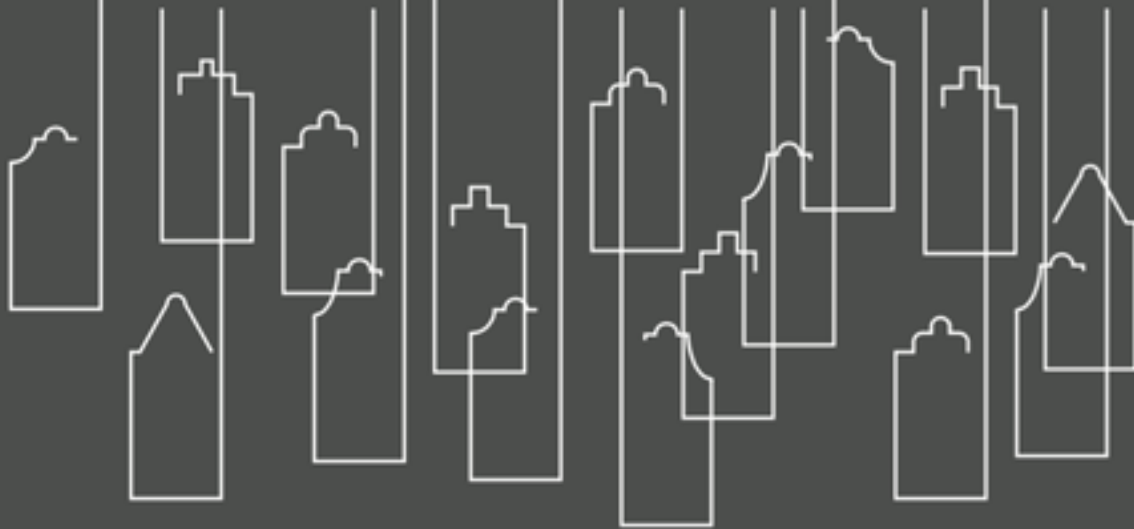
Belgrade, RS

Brushing
up **DNSThought**

*Everything you ever wanted to know
about caching resolvers but were afraid to ask*

AMSTERDAM APRIL 2017
DNS MEASUREMENTS

HACKATHON



Participants:

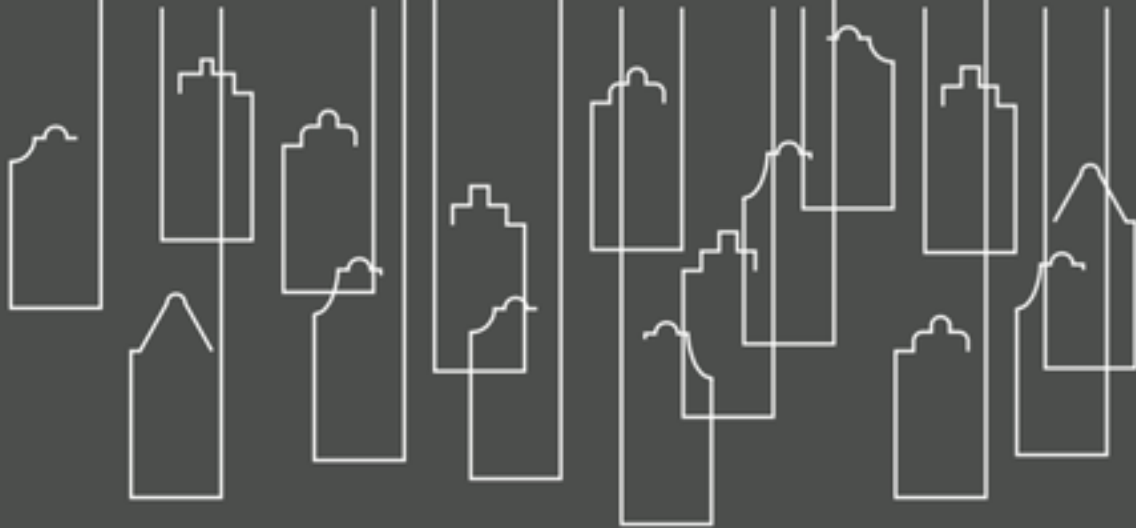
Andrea Barberio,
Petros Gigis,
Jerry Lundström,
Teemu Ryttilähti,
Willem Toorop

Goal:

Provide insight into
caching resolver
capabilities

AMSTERDAM APRIL 2017
DNS MEASUREMENTS

HACKATHON



Capabilities

Basic

IPv6, TCP

Security

DNSSEC validation,
Algorithm support,
TA's Root KSK Sentinel

Privacy

Qname minimization,
EDNS Client Subnet

DNSThought in research

Roll, Roll, Roll your Root: A Comprehensive Analysis of the First Ever DNSSEC Root KSK Rollover [PDF] nsf.gov

..., D Wessels, [W Hardaker](#), [T Chung](#), [W Toorop](#)... - Proceedings of the ..., 2019 - dl.acm.org

The DNS Security Extensions (DNSSEC) add authenticity and integrity to the naming system of the Internet. Resolvers that validate information in the DNS

☆ Save Cite Cited by 12 Related articles All 10 versions

The reality of algorithm agility: Studying the DNSSEC

[M Müller](#), [W Toorop](#), [T Chung](#), [J Jansen](#)... - Proceedings of the ...,

The DNS Security Extensions (DNSSEC) add data origin authentication to the Domain Name System (DNS), the naming system of the Internet

☆ Save Cite Cited by 12 Related articles All 10 versions

The root canary: Monitoring and measuring the DNS

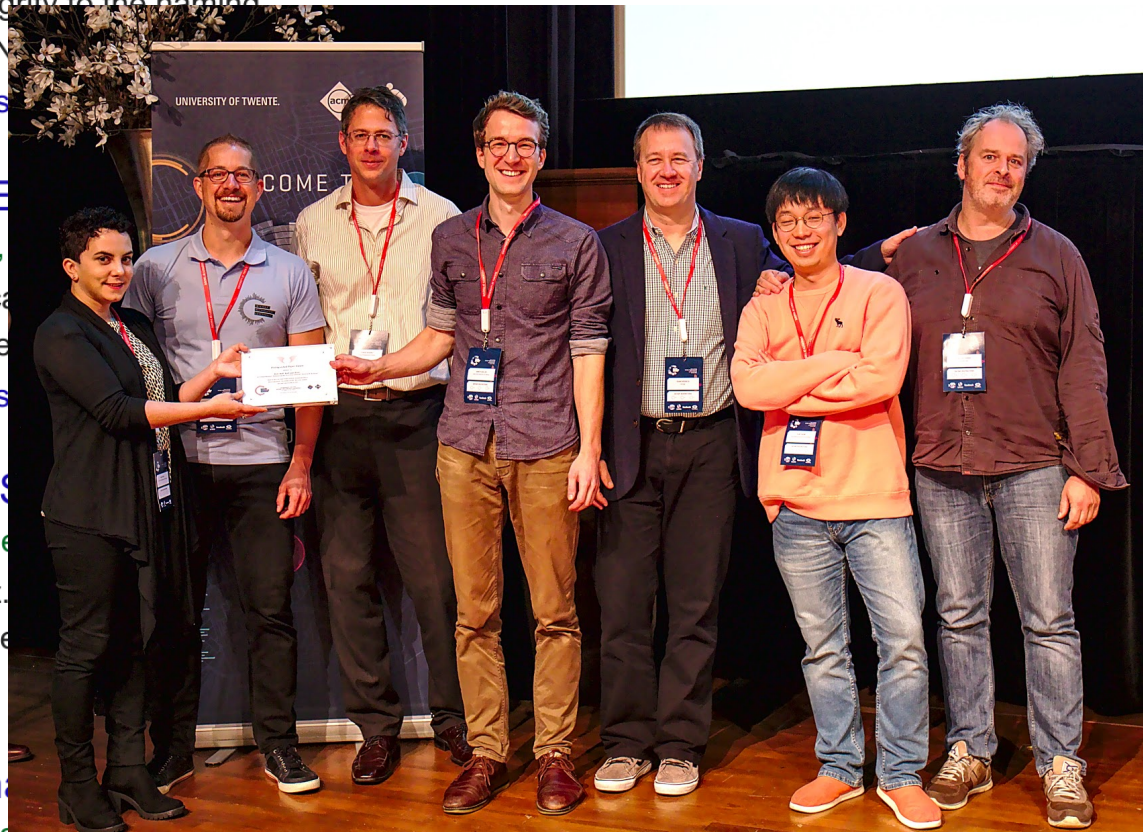
..., [T Chung](#), [D Choffnes](#), [A Mislove](#), [W Toorop](#) - Proceedings of the

The Domain Name System (DNS) is part of the core of the Internet. In the much-needed security features were added to this protocol, with the

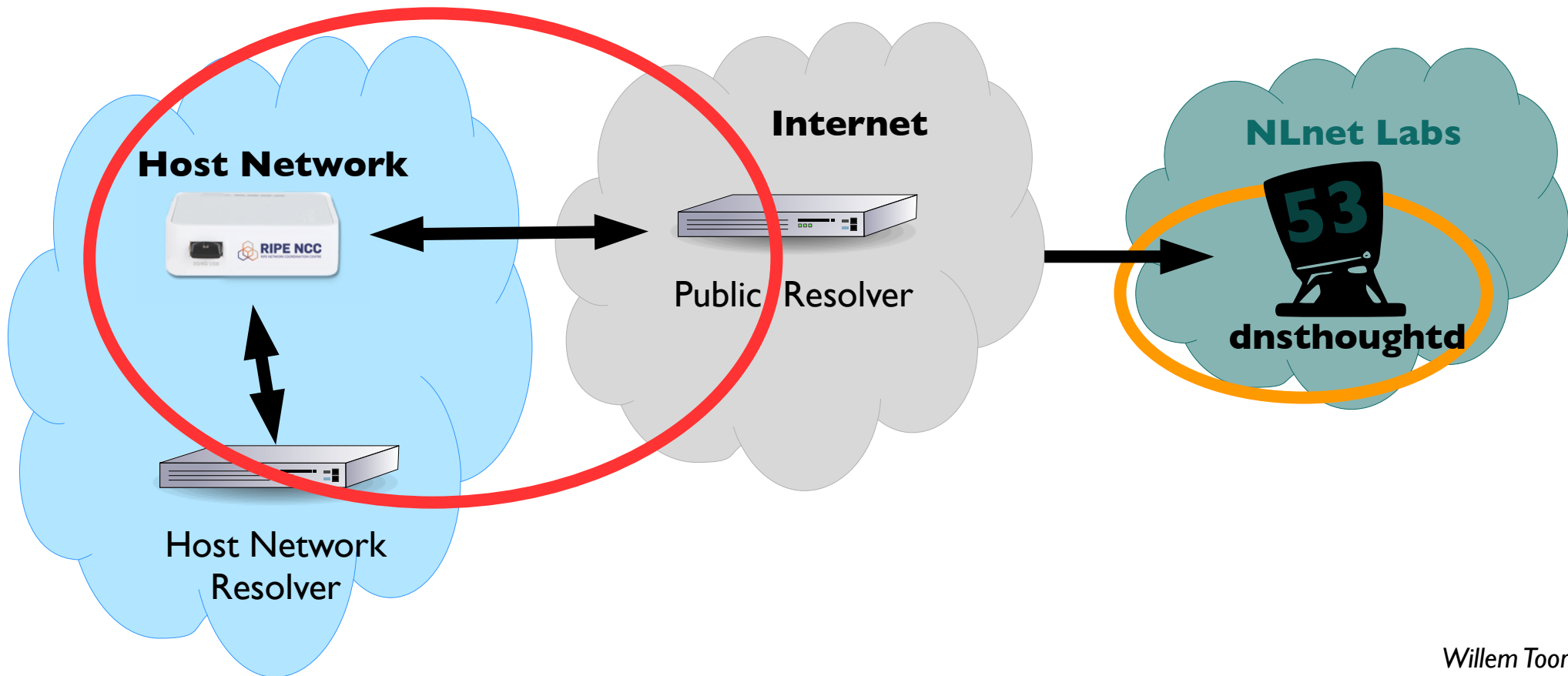
☆ Save Cite Cited by 7 Related articles All 4 versions

A first look at QNAME minimization in the domain name

[WB Vries](#), [Q Scheitle](#), [M Müller](#), [W Toorop](#)... - ... Conference on Pa



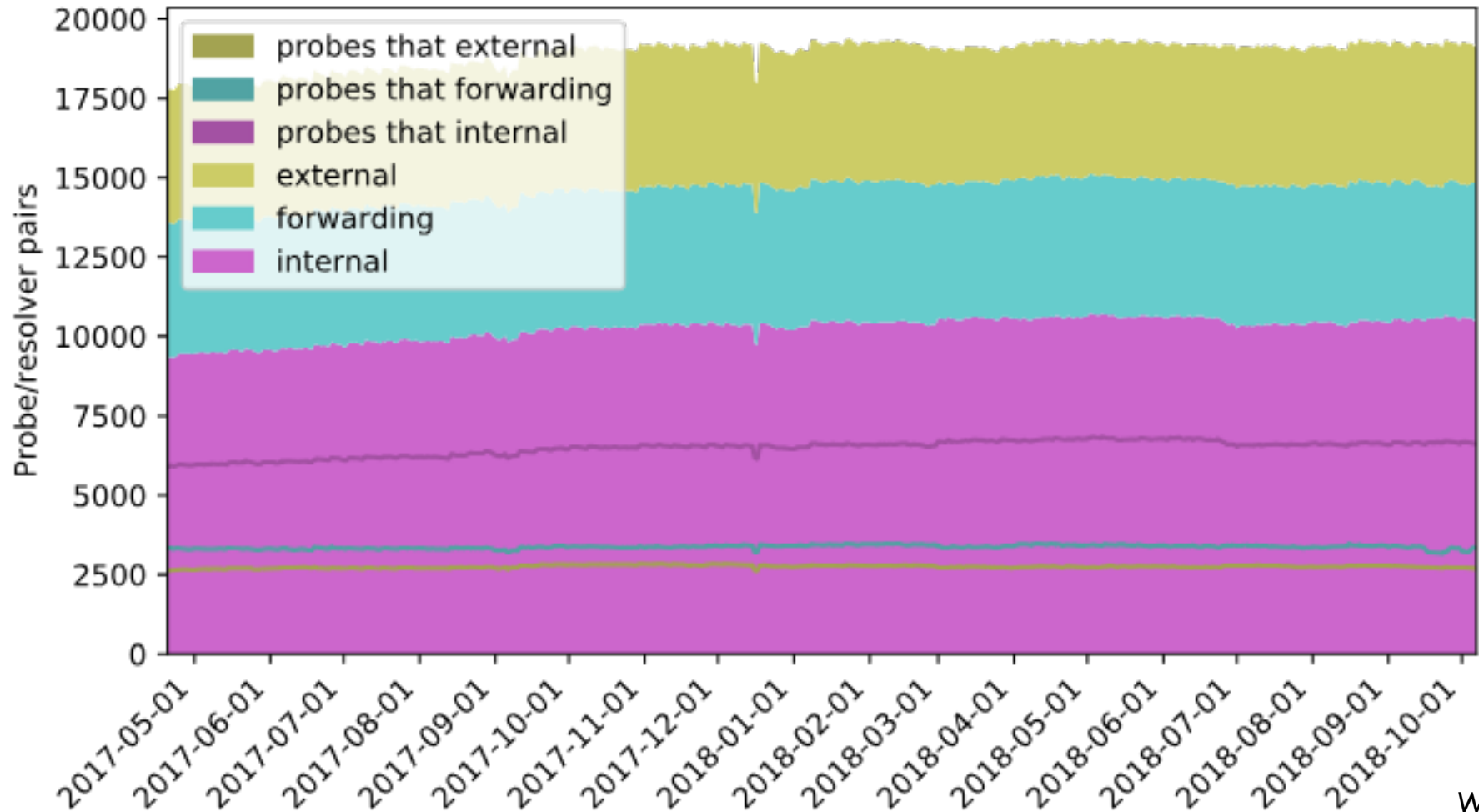
The RIPE Atlas perspective



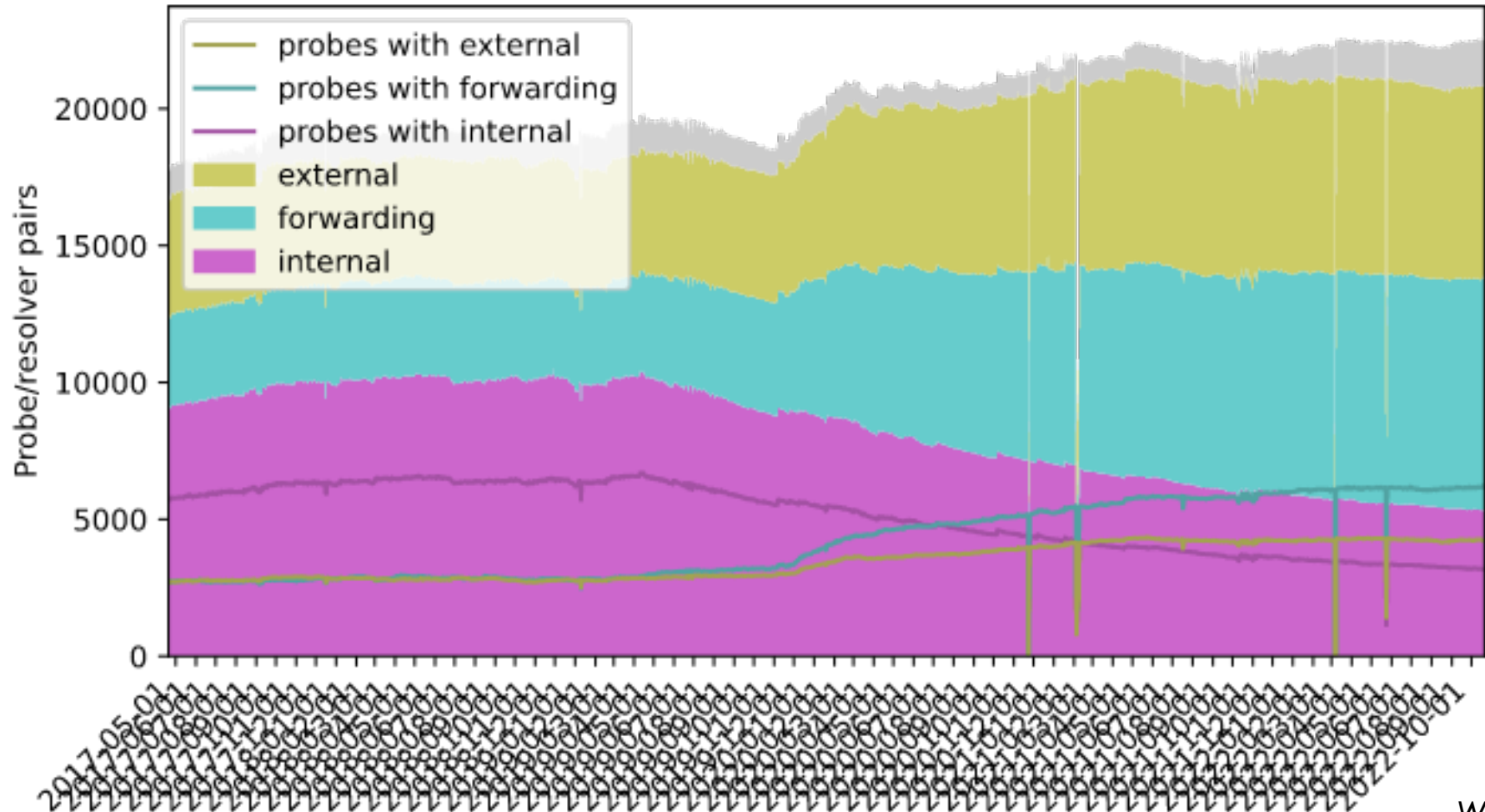
The RIPE Atlas perspective

	Probe ASN	Resolver ASN	Authoritative ASN
Internal	X	=	X
Forwarding	X	X	Z
	X	Y	Z
External	X	Z	Z

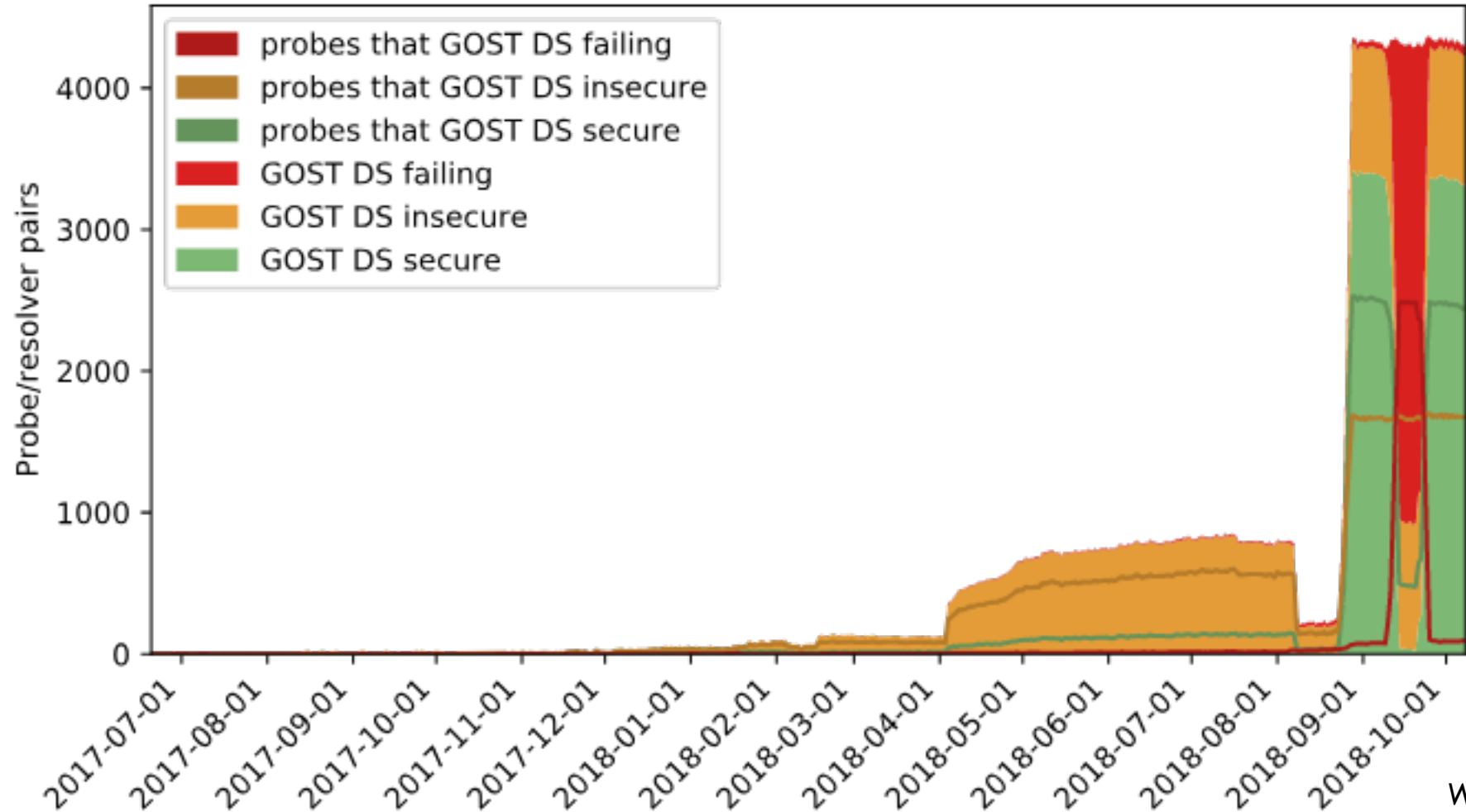
1½ years of measurements



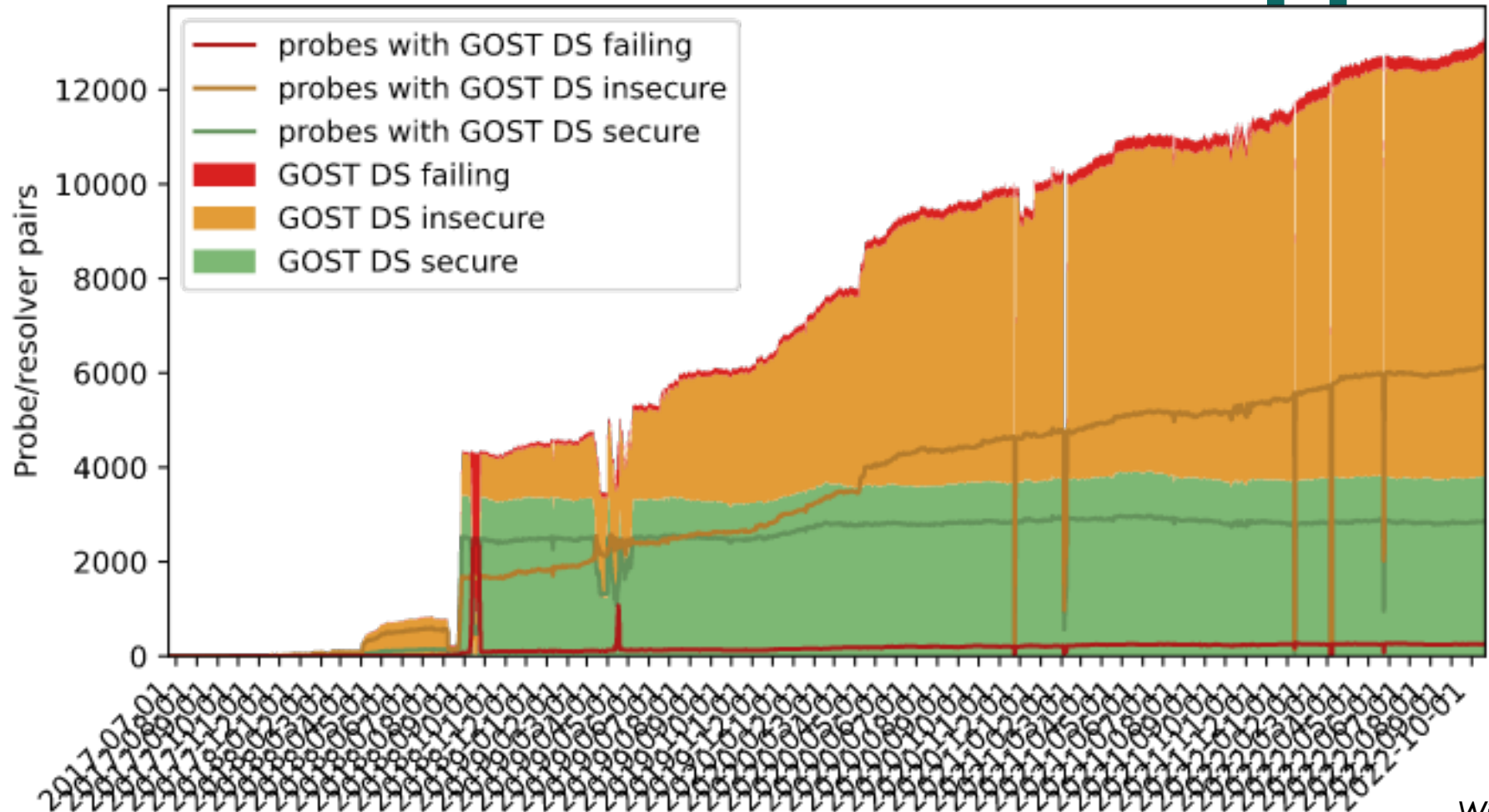
5¹/₂ years of measurements



GOST DS and ED25519 support



GOST DS and ED25519 support



Horrible user interface

Archief Bewerken Weergave Geschiedenis Extra Profielen Help

DNSThought - Resolvers t x +

dnstought.nl/netlabs.nl/can_ed25519/#gost

Report from 2022-10-21 22:00 for 13086 resolver at 7501 probes that validate DNSKEY algorithm ED25519

- [Clear validate DNSKEY algorithm ED25519](#)
- [do not validate DNSKEY algorithm ED25519](#)
- [have broken DNSKEY algorithm ED25519 validation support](#)

[Internal, Forwarding & External](#) | [Top 10 Authoritative ASNs](#) | [Top 10 Resolver ASNs](#) | [Top 10 Probe ASNs](#) | [Qname Minimization](#) | [Flagday](#) | [IPv4 Route origin Validation](#) | [IPv6 Route origin Validation](#) | [Top EDNS Client Subnet masks](#) | [Top 10 NX domain rewriting ASNs](#) | [Root Key Trust Anchor Sentinel for DNSSEC](#) | [DNSKEY Algorithm ED448 support](#) | [DNSKEY Algorithm ED25519 support](#) | [DNSKEY Algorithm ECDSA-P384-SHA384 support](#) | [DNSKEY Algorithm ECDSA-P256-SHA256 support](#) | [DNSKEY Algorithm ECC-GOST support](#) | [DNSKEY Algorithm RSA-SHA512 support](#) | [DNSKEY Algorithm RSA-SHA256 support](#) | [DNSKEY Algorithm RSA-SHA1-NSEC3 support](#) | [DNSKEY Algorithm DSA-NSEC3 support](#) | [DNSKEY Algorithm RSA-SHA1 support](#) | [DNSKEY Algorithm DSA support](#) | [DNSKEY Algorithm RSA-MD5 support](#) | [DS Algorithm GOST DS support](#) | [DS Algorithm SHA-384 DS support](#) | [IPv6](#) | [TCP](#) | [TCP6](#) |

Internal, Forwarding & External



RIPE NCC Community Projects Fund



The RIPE NCC has supported a range of projects and innovative ideas over its 25-year history, and we are now formalising these efforts through the RIPE NCC Community Projects Fund. We know there's no shortage of brilliant minds in the Internet technical community working on groundbreaking projects, but securing funding to support these projects can be challenging.

We started working with a professional data visualiser

DNSThought test visualisations

- ☒ Totals
- ☐ Percentages
- ☐ Percentages without remaining resolvers

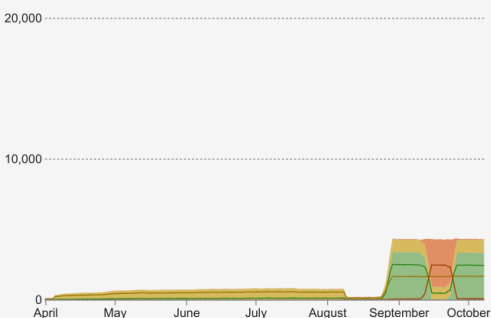
Reset

Compare:

- ☐ Internal, Forwarding & External
- ☐ Qname Minimization
- ☐ Root Key Trust Anchor Sentinel for DNSSEC
- ☐ DNSKEY Algorithm ED448 support
- ☒ DNSKEY Algorithm ED25519 support
- ☐ DNSKEY Algorithm ECDSA-P384-SHA384 support
- ☐ DNSKEY Algorithm ECDSA-P256-SHA256 support
- ☐ DNSKEY Algorithm ECC-GOST support
- ☐ DNSKEY Algorithm RSA-SHA512 support
- ☐ DNSKEY Algorithm RSA-

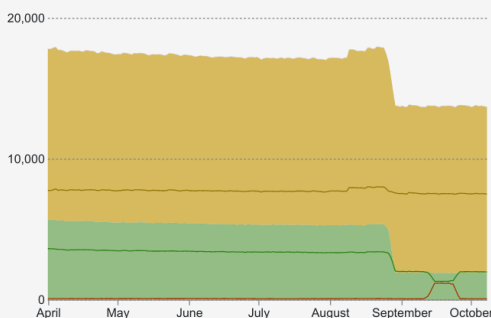
ED25519 secure

DS Algorithm GOST DS support



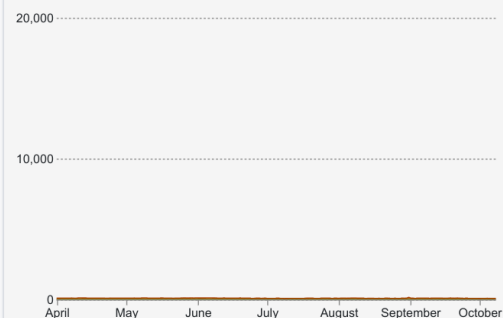
ED25519 insecure

DS Algorithm GOST DS support

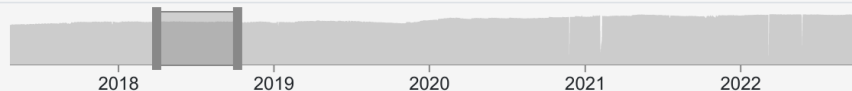


ED25519 failing

DS Algorithm GOST DS support

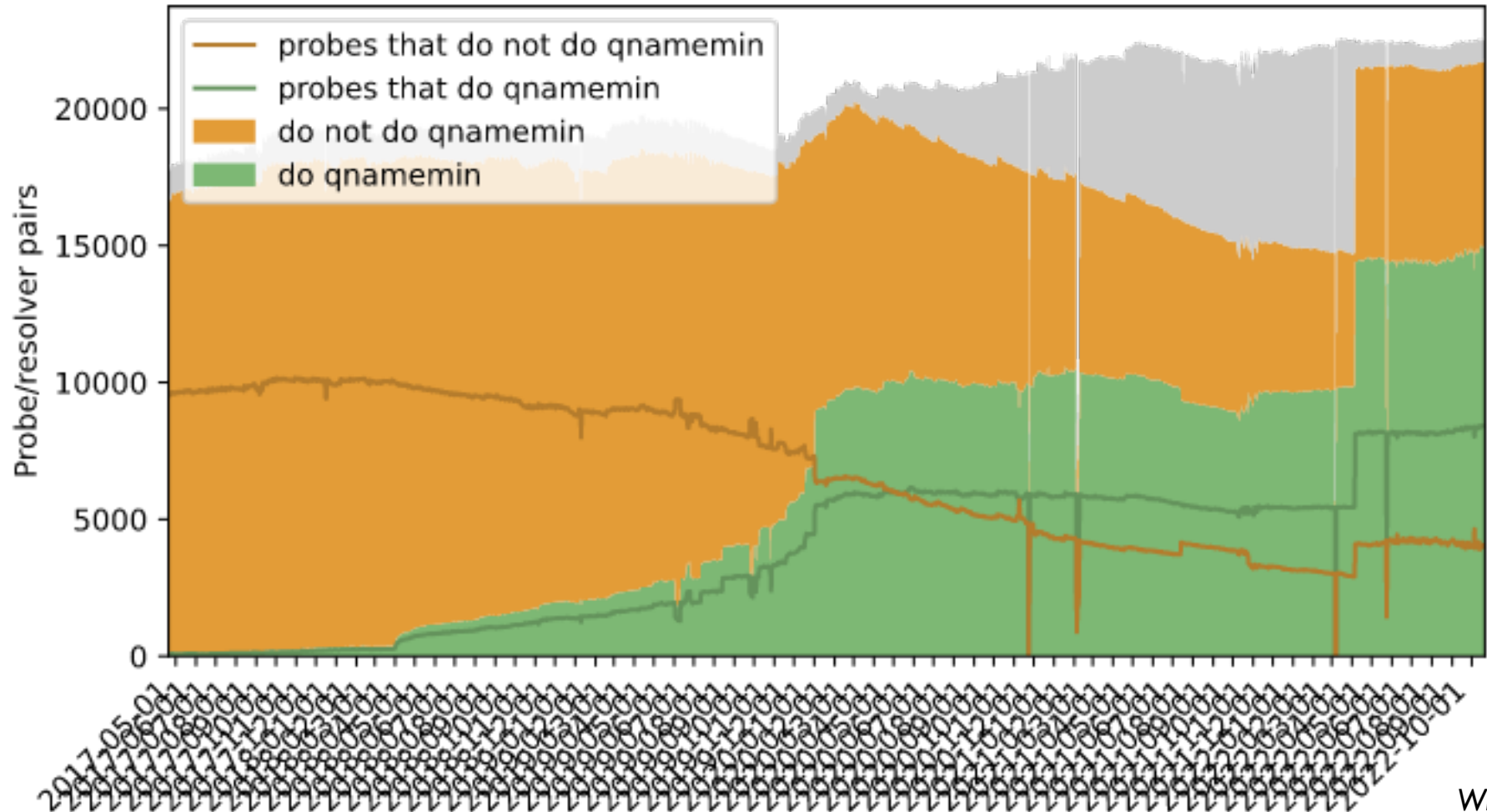


Select time range:



Select and compare

RIPE Atlas bug (qname min)



DNSThought test visualisations

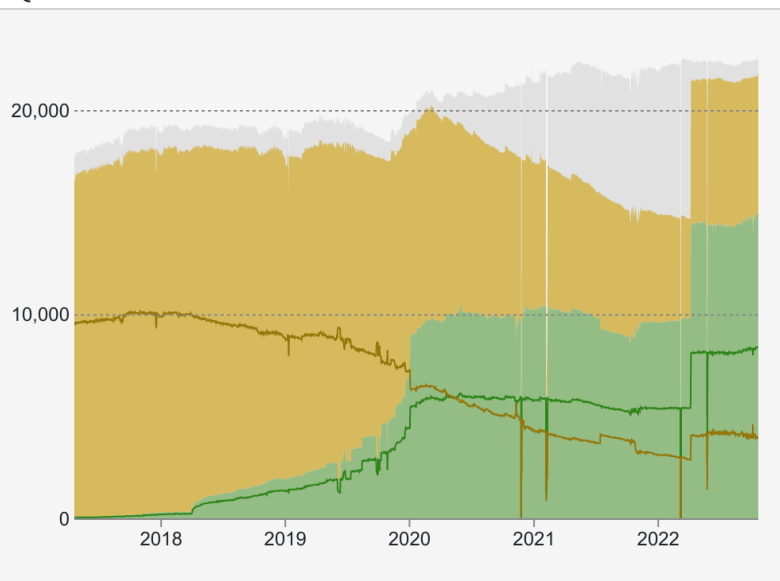
- ☒ Totals
- ☐ Percentages
- ☐ Percentages without remaining resolvers

[Reset](#)

Compare:

- ☐ Internal, Forwarding & External
- ☐ Root Key Trust Anchor Sentinel for DNSSEC
- ☐ DNSKEY Algorithm ED448 support
- ☐ DNSKEY Algorithm ED25519 support
- ☐ DNSKEY Algorithm ECDSA

Qname Minimization



Select time range:

2018

2019

2020

2021

2022

DNSThought test visualisations

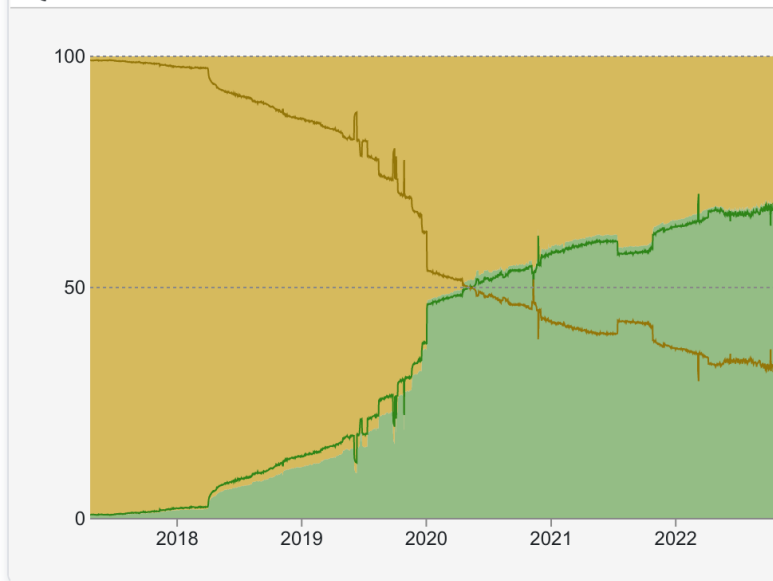
- ☐ Totals
- ☐ Percentages
- ☒ Percentages without remaining resolvers

[Reset](#)

Compare:

- ☐ Internal, Forwarding & External
- ☐ Root Key Trust Anchor Sentinel for DNSSEC
- ☐ DNSKEY Algorithm ED448 support
- ☐ DNSKEY Algorithm ED25519 support
- ☐ DNSKEY Algorithm ECDSA

Qname Minimization



Select time range:

2018

2019

2020

2021

2022

Brushing up **DNSThought**

- Can you take a look?
 - <https://dnsthought.nlnetlabs.nl/vis/test4/>
- Does this make sense (UI wise)?
- How to improve?
- Send it all to me please
 - [Willem Toorop <willem@nlnetlabs.nl>](mailto:willem@nlnetlabs.nl)

