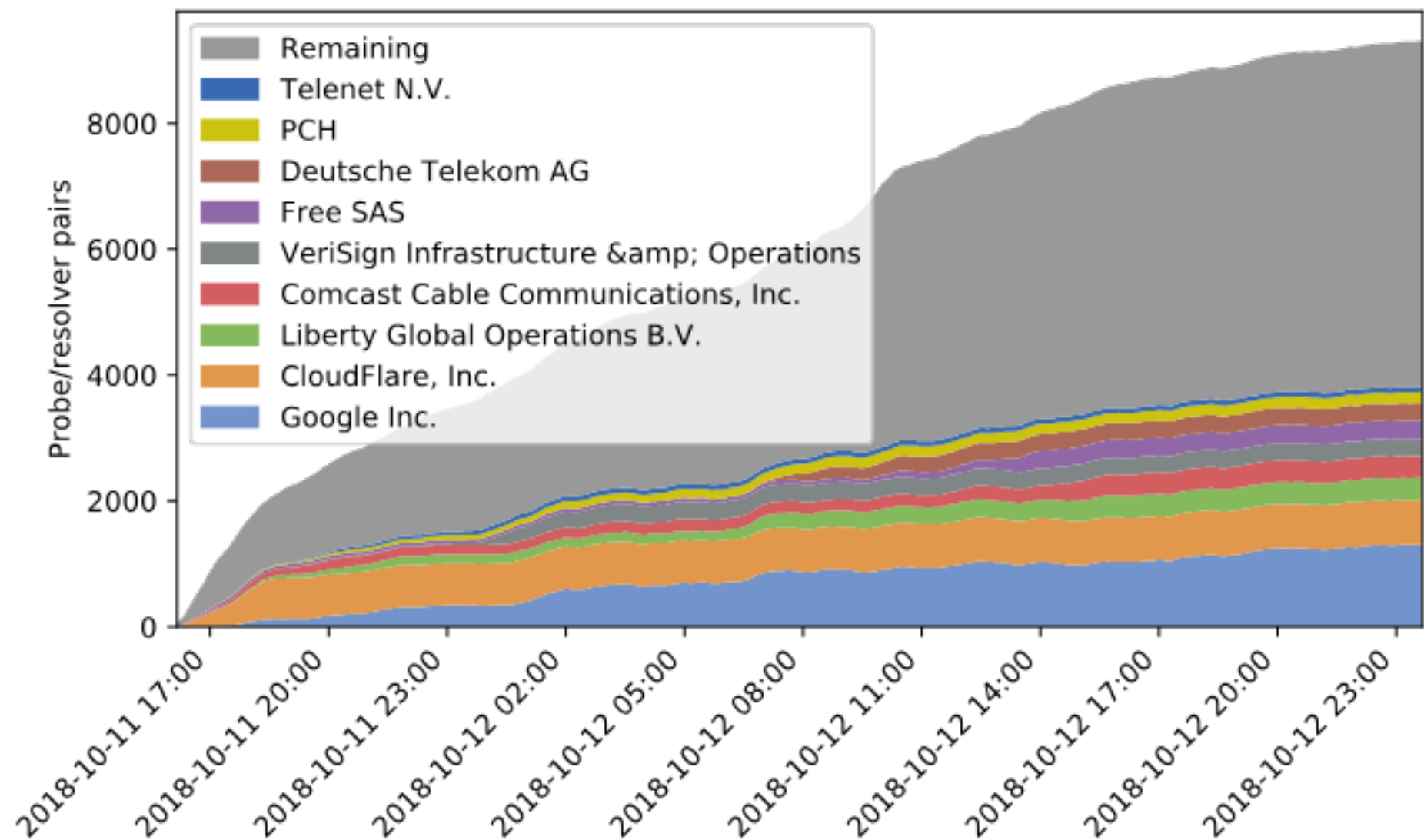
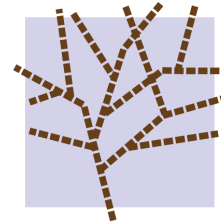






NLNETLABS
Willem Toorop



DNS-OARC 29

13 October 2018
Amsterdam

*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 & properties

Basic : IPv6, TCP, TCP over IPv6

Security: DNSSEC validation, Algorithm support,
TA's Root KSK Sentinel, NXdomain rewrite

Privacy : Qname minimization, EDNS Client Subnet

AMSTERDAM APRIL 2017
DNS MEASUREMENTS
HACKATHON

Some msms need just a zone

IPv6, DNSSEC validation, NXdomain rewriting

Some need authoritative perspective

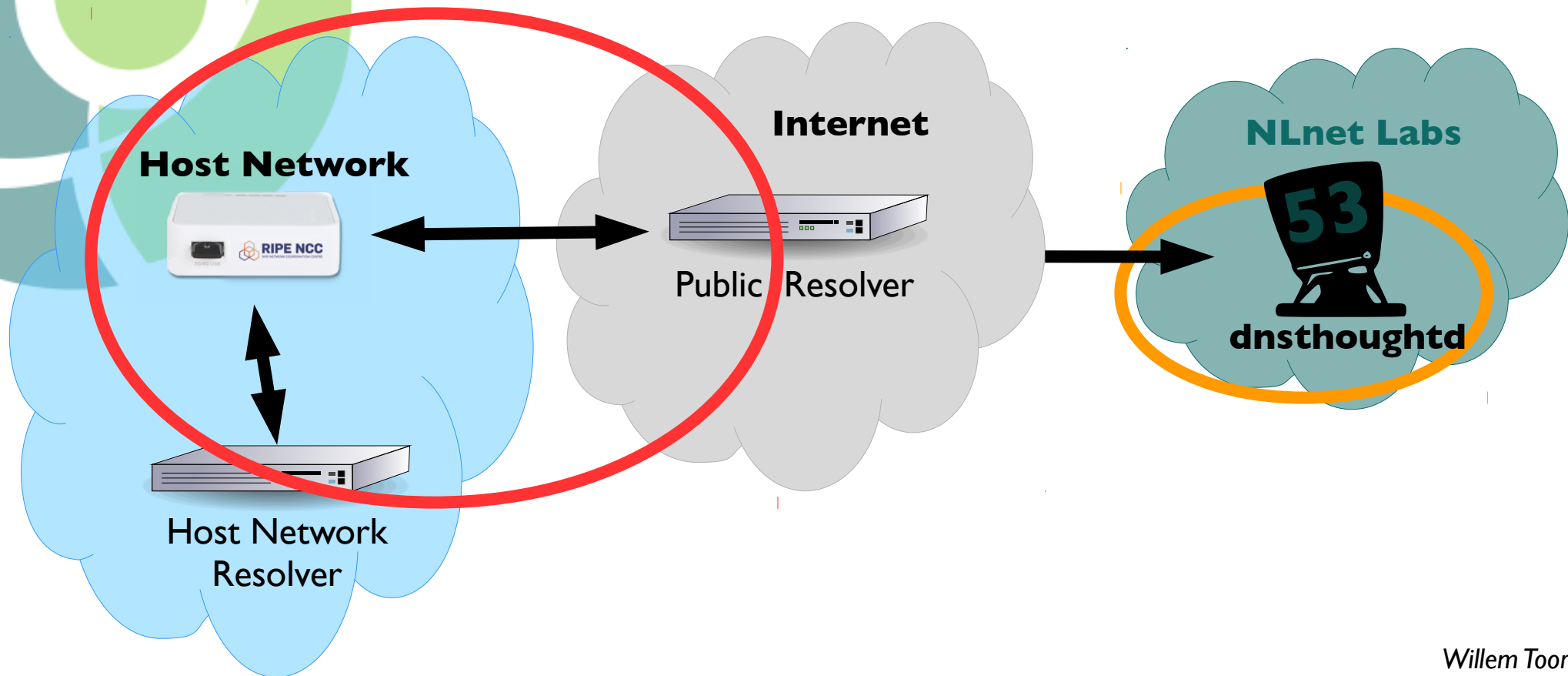
TCP, Qname minimization, EDNS Client subnet

dnsthoughtd

dnsthoughtd

```
willem@makaak: ~  
willem@makaak:~$ dig @9.9.9.9 tc.ripe-hackathon6.nlnetlabs.nl AAAA  
; <<>> DiG 9.11.0-P2 <<>> @9.9.9.9 tc.ripe-hackathon6.nlnetlabs.nl AAAA  
; (1 server found)  
;; global options: +cmd  
;; Got answer:  
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 61711  
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1  
  
;; OPT PSEUDOSECTION:  
; EDNS: version: 0, flags:; udp: 4096  
;; QUESTION SECTION:  
;tc.ripe-hackathon6.nlnetlabs.nl. IN      AAAA  
  
;; ANSWER SECTION:  
tc.ripe-hackathon6.nlnetlabs.nl. 0 IN      AAAA      2620:171:f9:f0::8  
  
;; Query time: 15 msec  
;; SERVER: 9.9.9.9#53(9.9.9.9)  
;; WHEN: Mon Oct 08 15:10:12 CEST 2018  
;; MSG SIZE rcvd: 88  
  
willem@makaak:~$ dig -x 2620:171:f9:f0::8 +short  
res110.ams.rdns.pch.net.  
willem@makaak:~$
```

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

Qname minimization

```
willem@makaak: ~  
willem@makaak:~$ dig @1.1.1.1 qnamemintest.internet.nl TXT  
;  
<<>> DiG 9.11.0-P2 <<>> @1.1.1.1 qnamemintest.internet.nl TXT  
; (1 server found)  
;; global options: +cmd  
;; Got answer:  
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 33167  
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1  
  
;; OPT PSEUDOSECTION:  
; EDNS: version: 0, flags:; udp: 1452  
;; QUESTION SECTION:  
;qnamemintest.internet.nl.      IN      TXT  
  
;; ANSWER SECTION:  
qnamemintest.internet.nl. 10      IN      CNAME    a.b.qnamemin-test.internet.nl.  
a.b.qnamemin-test.internet.nl. 10 IN      TXT      "HOORAY - QNAME minimisation is enabled on your resolver :)"  
  
;; Query time: 20 msec  
;; SERVER: 1.1.1.1#53(1.1.1.1)  
;; WHEN: Mon Oct 08 15:26:41 CEST 2018  
;; MSG SIZE rcvd: 157  
  
willem@makaak:~$
```

AMSTERDAM APRIL 2017

Measurements for all probes every hour

query	msm ID
<prb_id>.<time>.ripe-hackathon6.nl netlabs.nl AAAA	8310366
<prb_id>.<time>.tc.ripe-hackathon4.nl netlabs.nl A	8310360
<prb_id>.<time>.tc.ripe-hackathon6.nl netlabs.nl AAAA	8310364
qnamemintest.internet.nl TXT	8310250
nxdomain.ripe-hackathon2.nl netlabs.nl A	8311777
whoami.akamai.net A	8310245
o-o.myaddr.l.google.com TXT	8310237
secure.ripe-hackathon2.nl netlabs.nl A	8311760
bogus.ripe-hackathon2.nl netlabs.nl A	8311763

Thank you Emile Aben! ❤️

Willem Toorop

DNSThought @OARC29 10/39

DNSThought | Dashboard x

sg-pub.ripe.net/petros/dnsthought/per_probe.html?probe_id=31568#

W

DNSThought

Enter probe id... Q

MAIN NAVIGATION

Home

Per probe

Per resolver

QNAME Map

Global Map

About

Per probe | Overview of probe 31568 Prototype

Home > Per probe

Overview: - x

The probe can connect to a name server ✓

The probe resolver is able to perform DNS IPv4 TCP ✓

The probe resolver is able to perform DNS IPv6 TCP ✓

The probe resolver have IPv6 capability ✓

The probe resolver offers QNAME minimization ✓

The probe resolver does not deliver edns subnet info ✗

Availability per DNS Resolver - x

Resolver IP	Last Hour	Last 6h
192.87.36.36	1	1
195.169.124.124	1	1

Capabilities per DNS Resolver - x

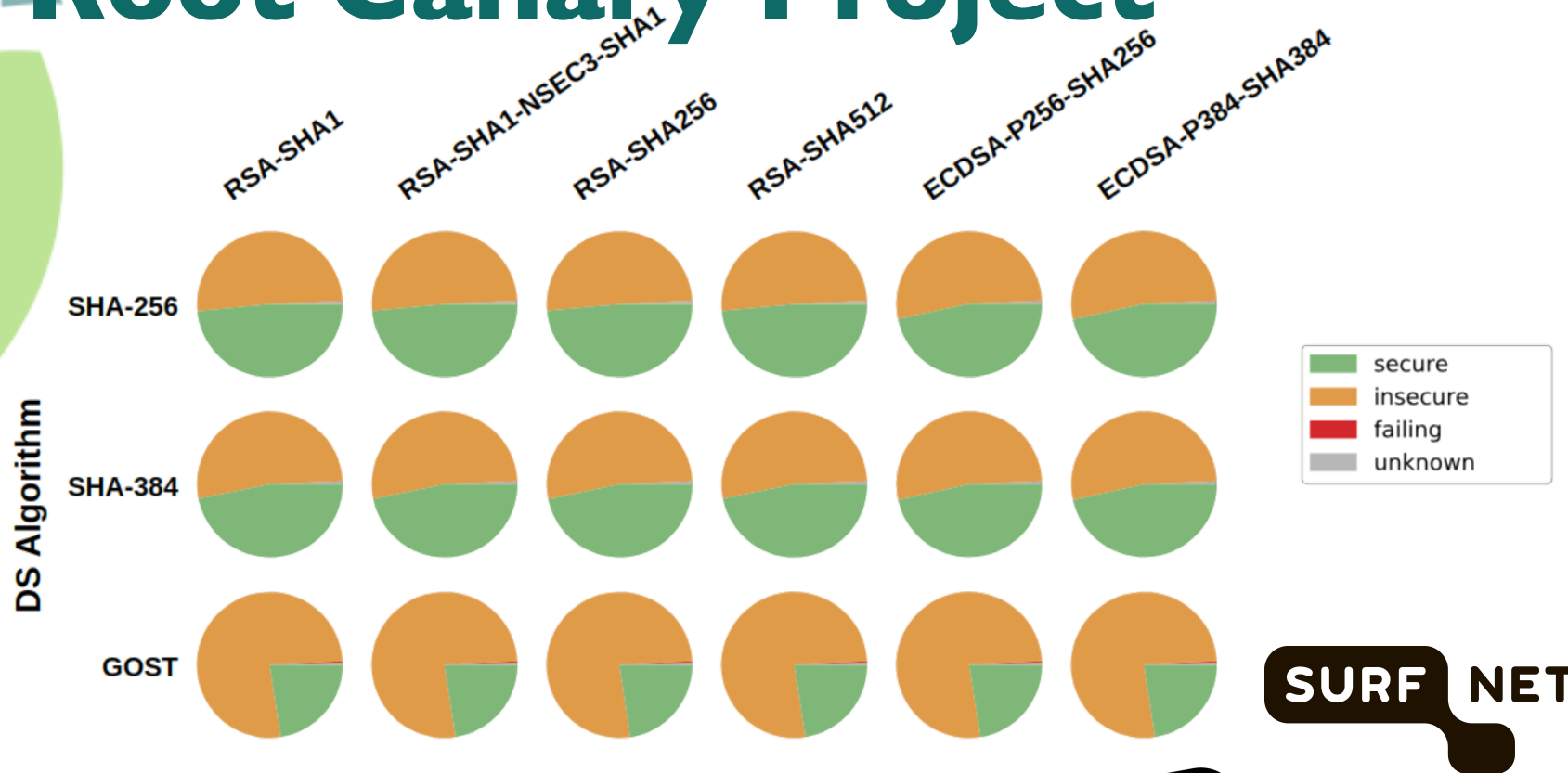
resolver IP	resolver net	resolver ASN	edns0 client subnet	IPv6 capability	IPv4 TCP	IPv6 TCP	QNAME minimization
195.169.124.124	195.169.0.0/16	1103	No	Yes	Yes	Yes	Yes
192.87.36.36	192.87.0.0/16	1103	No	Yes	Yes	Yes	Yes

Probe Map of AS v4: 1103 | v6: 1103 - x

+

-

Root Canary Project



- Participation with Roland van Rijswijk - Deij
- Measurements started 20 June 2017



More measurements

- Moritz Muller joined too
- Root KSK Sentinel msms since 19 July 2018



query	msm ID
root-key-sentinel-not-ta-19036.d2a8n3.rootcanary.net A	15283670
root-key-sentinel-not-ta-20326.d2a8n3.rootcanary.net A	15283671

With validating resolvers we have three situations:

- 1. Key 20326 has not been picked up (yet)*
- 2. Key 20326 is a valid TA, and key 19036 is still a valid TA*
- 3. Key 20326 is a valid TA, and key 19036 is removed*

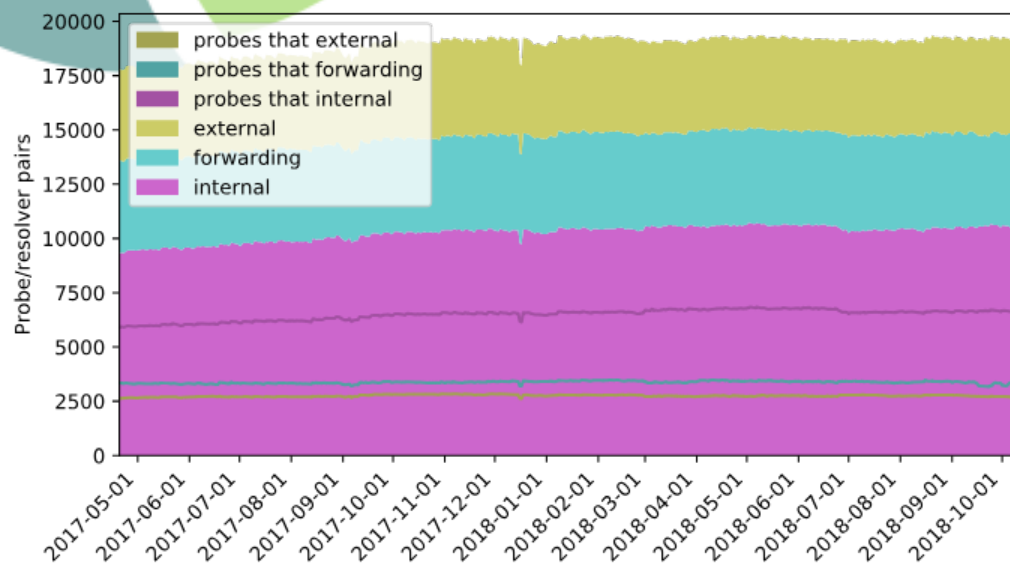
For these situations (1, 2,3), measurements for:

- (not-ta-19036 is-ta-20326) results in 1: (S S), 2: (S A), 3: (A A)*
- (is-ta-19036 is-ta-20326) results in 1: (A S), 2: (A A), 3: (S A)*
- (not-ta-19036 not-ta-20326) results in 1: (S A), 2: (S S), 3: (A S)*
- (is-ta-19036 not-ta-20326) results in 1: (A A), 2: (A S), 3: (S S)*

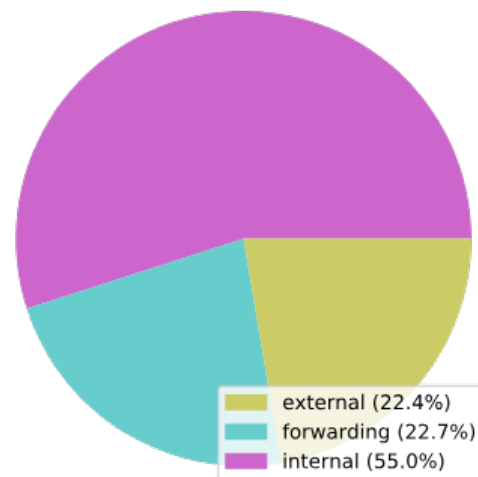
1½ years of measurements

Internal, Forwarding & External

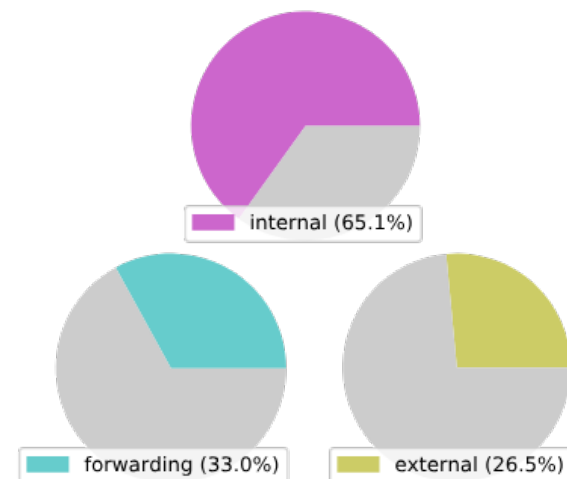
https://dnsthought.nl/netlabs.nl/#int_fwd_ext



with 19082 resolvers



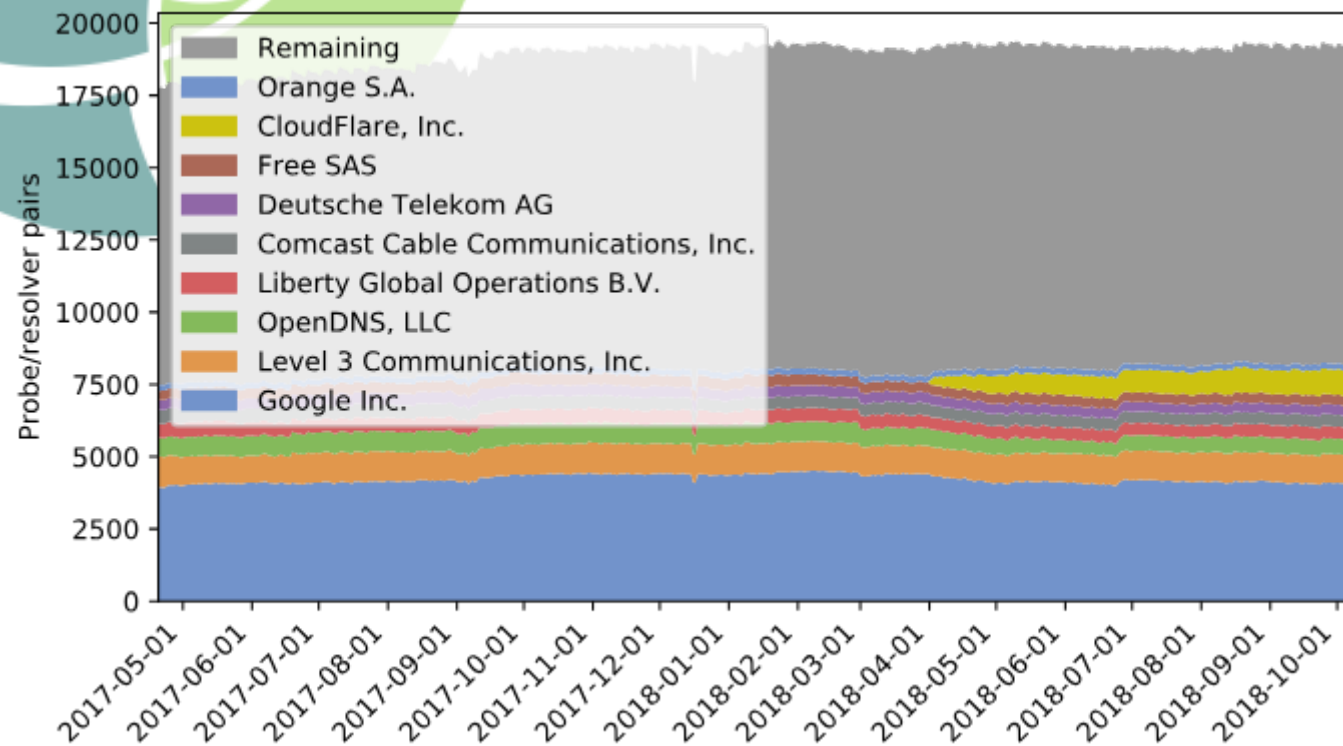
with 10155 probes



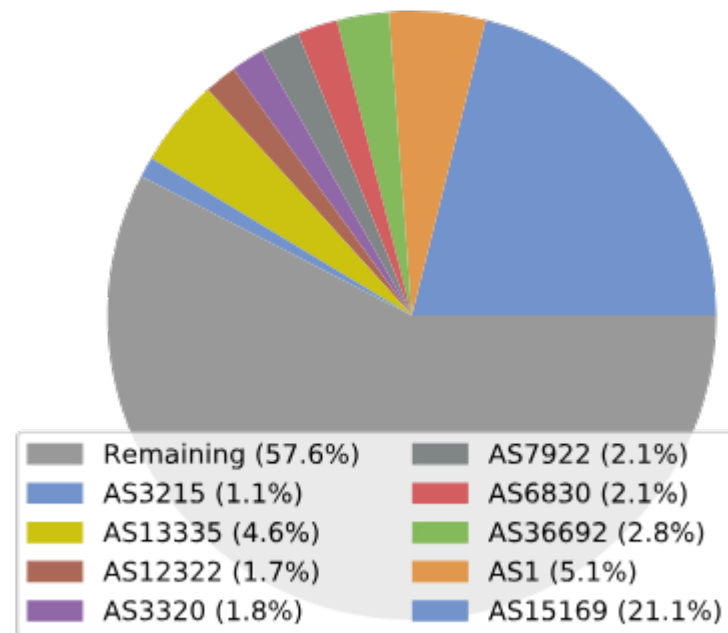
1½ years of measurements

Top 10 ASNs seen @ authoritative

https://dnsthought.nlnetlabs.nl/#top_auth_asns



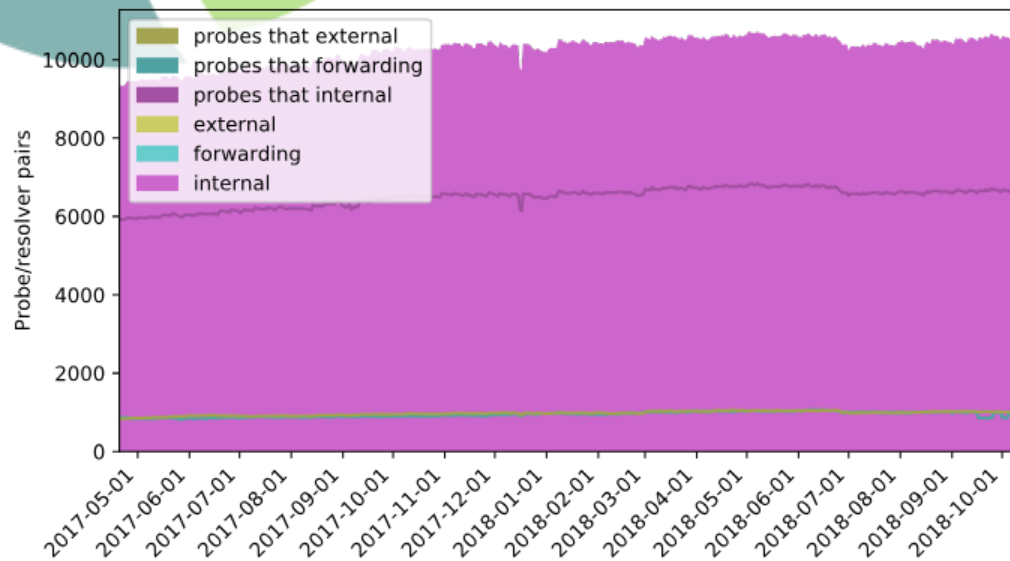
with 19082 resolvers



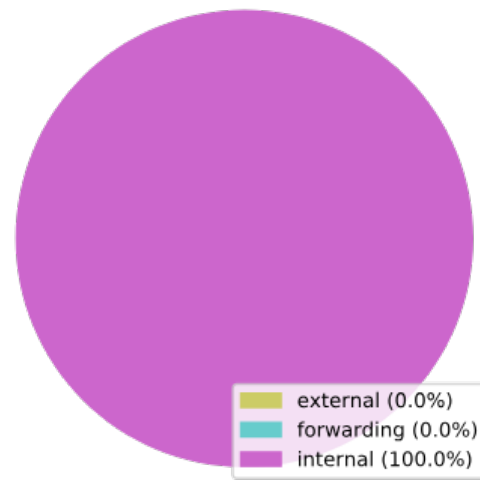
have the same ASN as the probe (internal)

https://dnsthought.nl/netlabs.nl/is_internal/#int_fwd_ext

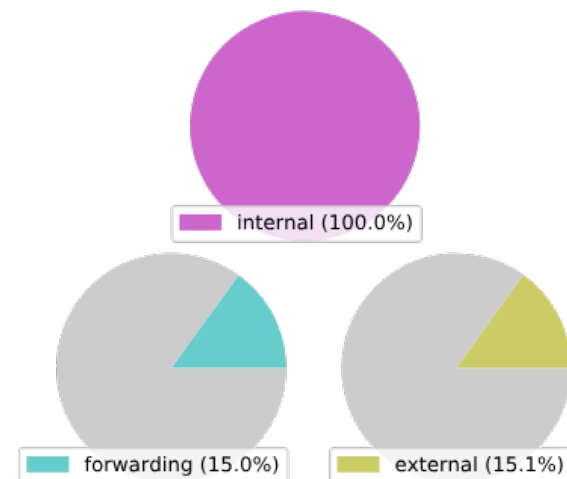
Internal



with 10490 resolvers



with 6611 probes



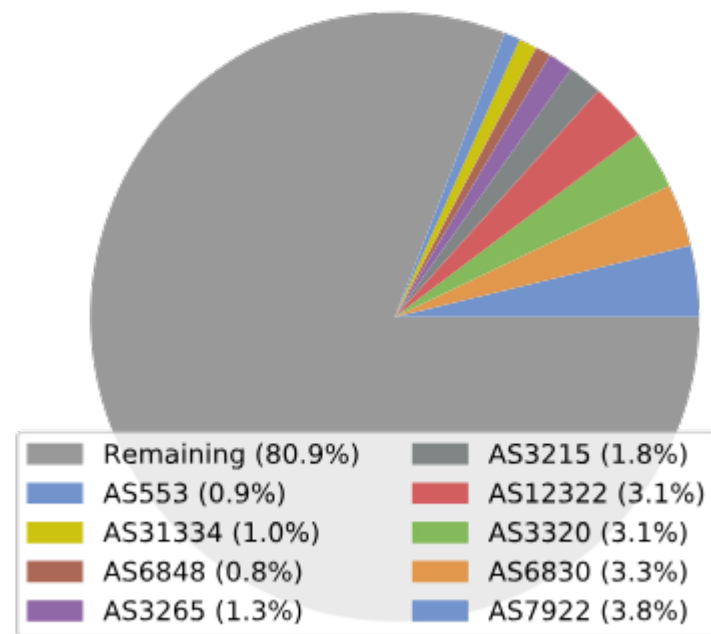
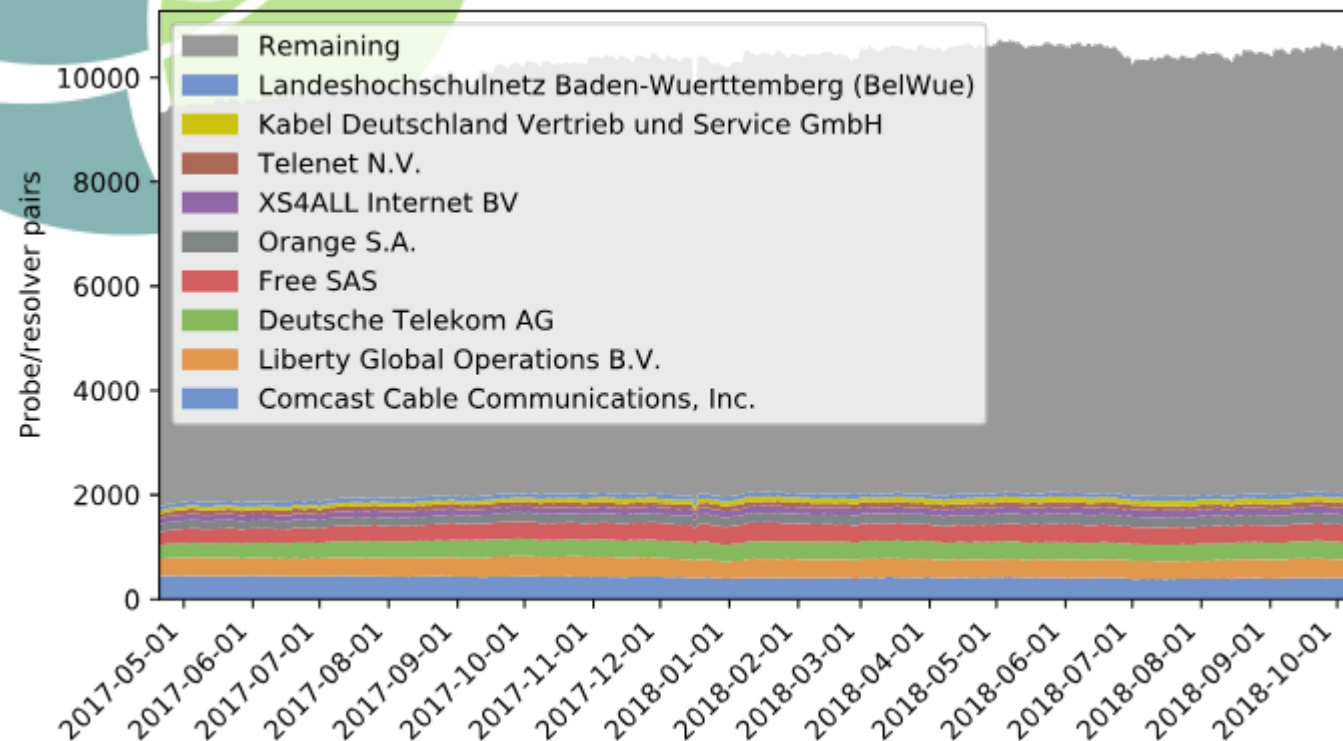
Willem Toorop

DNSThought @OARC29 16/39

have the same ASN as the probe (internal)
https://dnsthought.nl/netlabs.nl/is_internal/#top_auth_asns

Top 10 ASNs seen @ authoritative

with 10490 resolvers



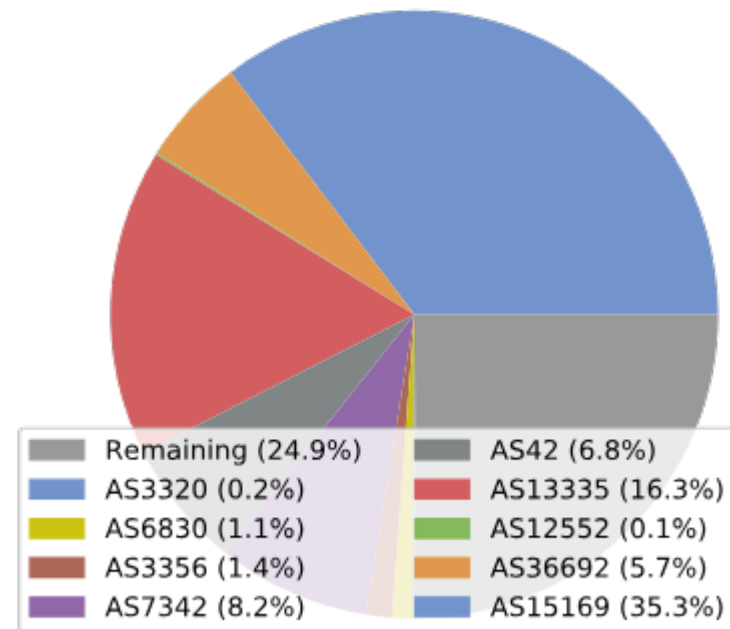
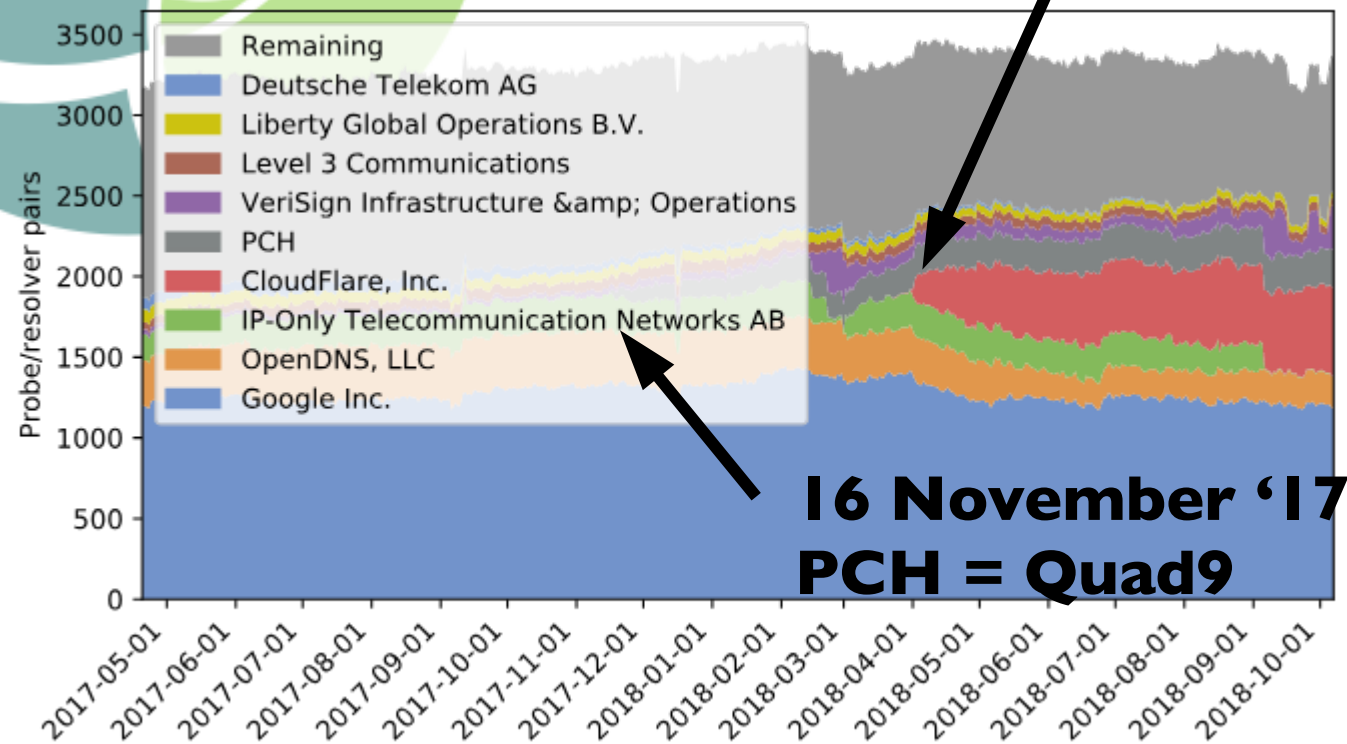
forwarding to a resolver with a different ASN
https://dnstthought.nl/netlabs.nl/is_forwarding/#top_auth_asns

Forwarding

Top 10 ASNs seen @ authoritative

1st April 2018

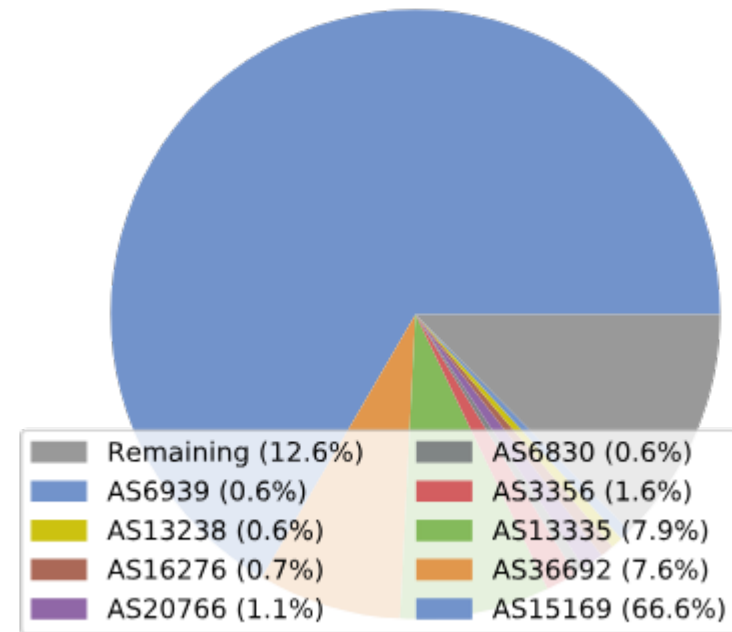
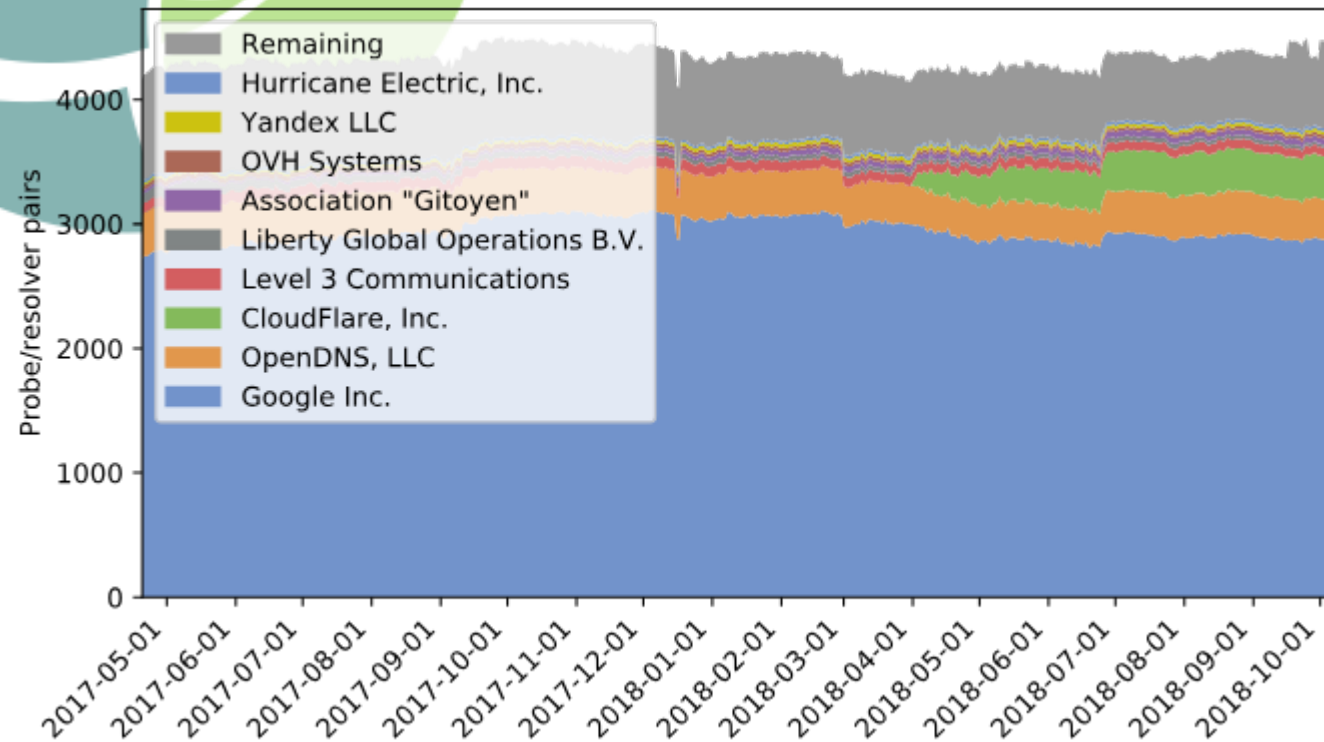
with 3351 resolvers



have a ASN different from the probe ASN
https://dnsthought.nl/netlabs.nl/is_external/#top_auth_asns

Top 10 ASNs seen @ authoritative

with 4266 resolvers





Internal, Forwarding, External

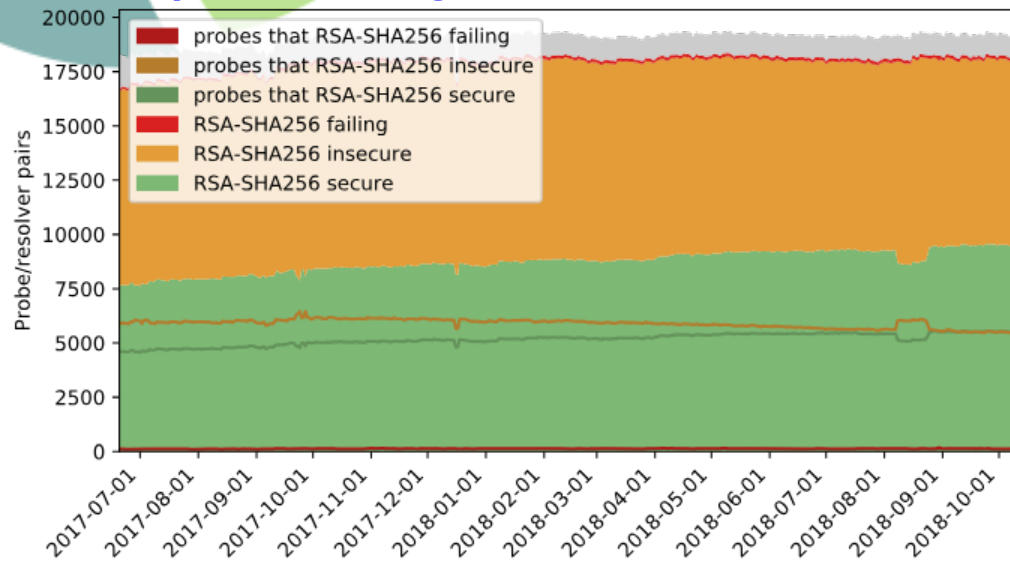


Diversity

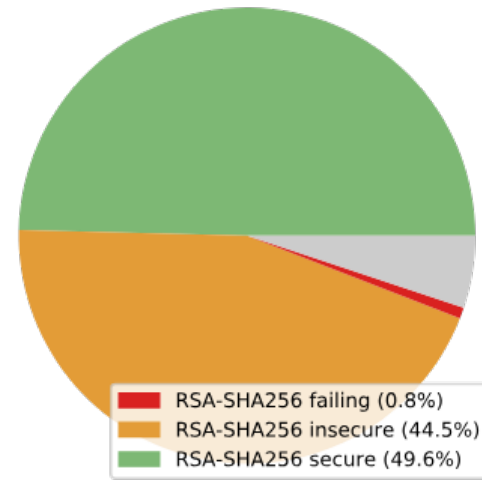
DNSSEC

RSA-SHA256 support

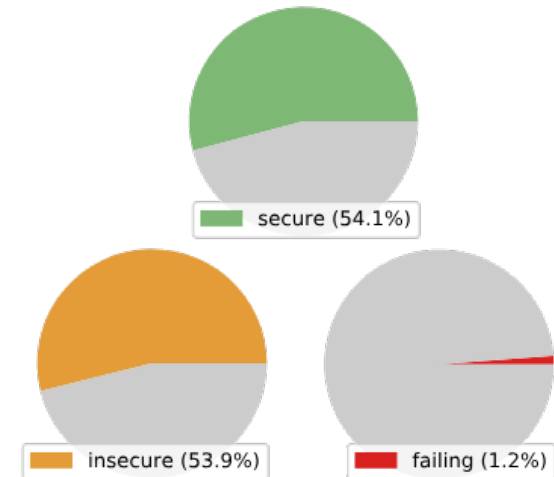
<https://dnsthought.nlnetlabs.nl/#rsasha256>



with 19135 resolvers



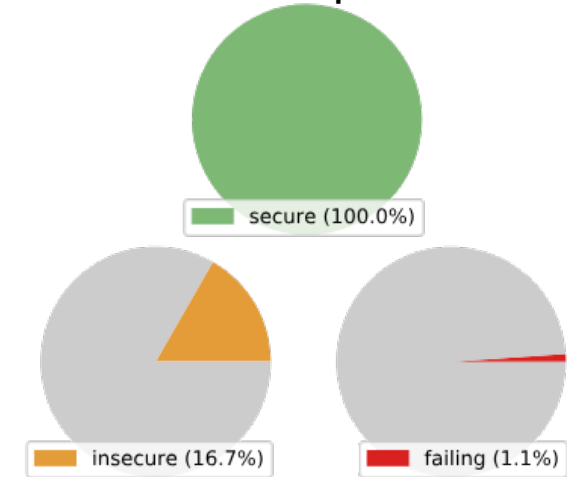
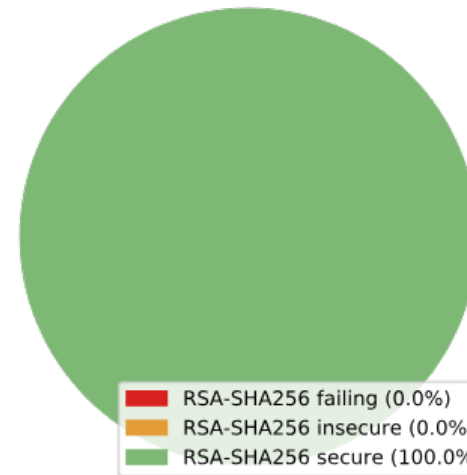
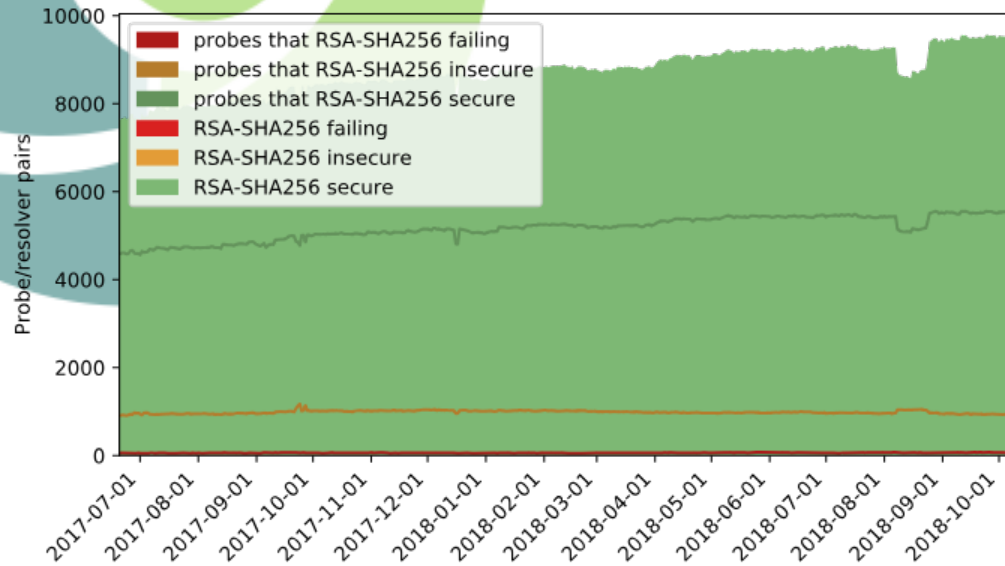
with 10178 probes



RSA-SHA256 support

with 9493 resolvers

with 5508 probes

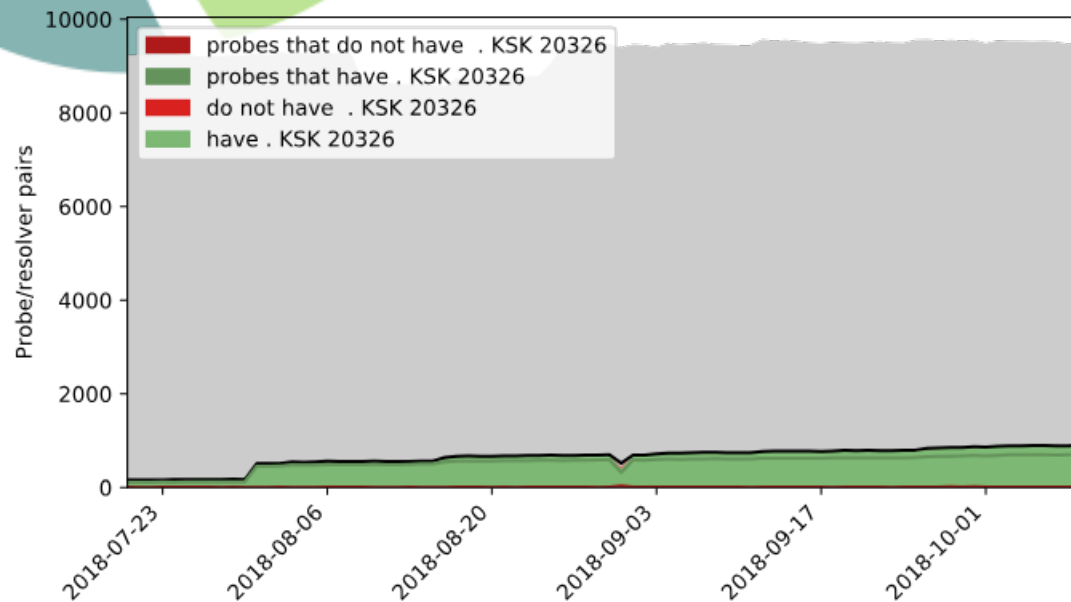


- 54.1% of probes has validating resolver
- 16.7% of those have a non validating resolver too
- So realistically only 45.1% of probes is protected

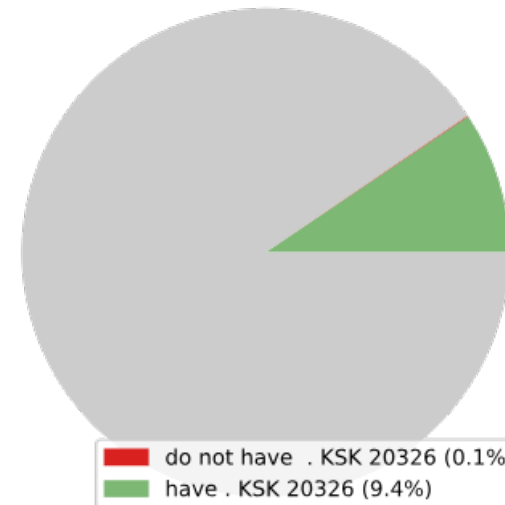
validate DNSKEY algorithm RSA-SHA256
https://dnsthought.nl/netlabs.nl/can_rsasha256/#ta_20326

DNSSEC

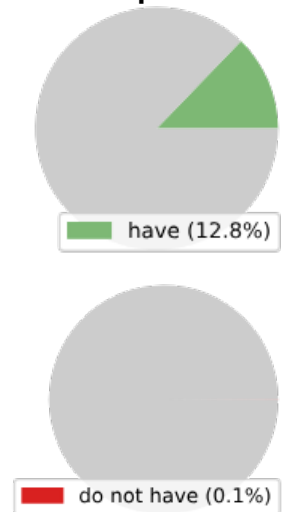
Root Key Trust Anchor Sentinel



with 9493 resolvers



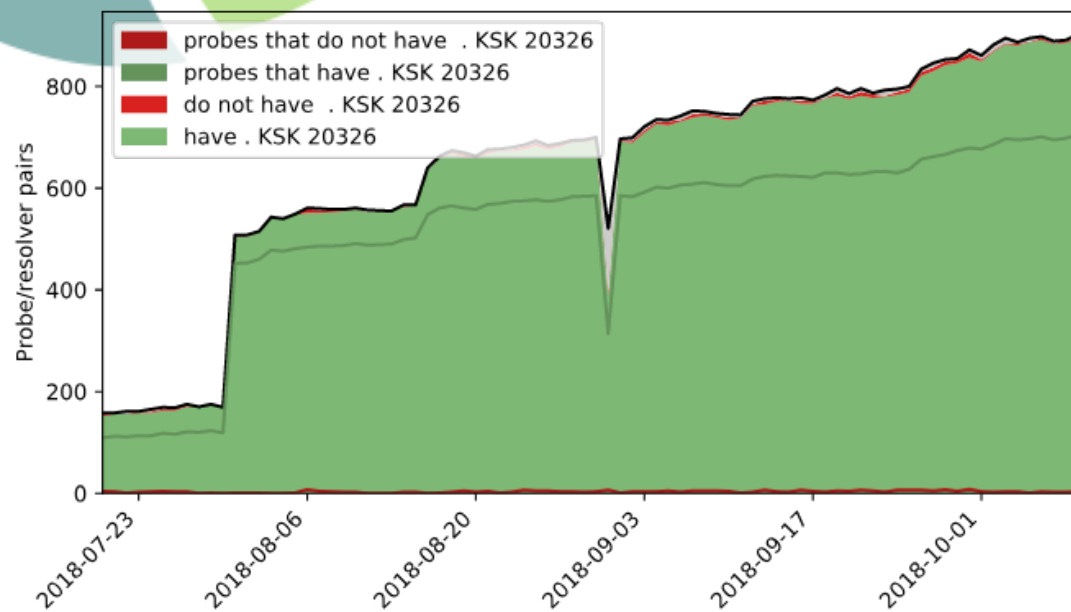
with 5508 probes



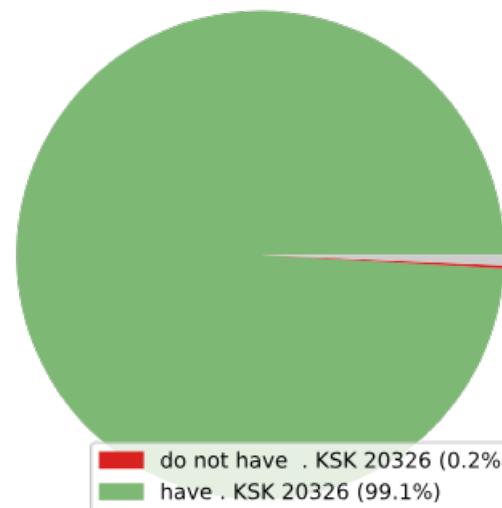
root KSK sentinel support
https://dnsthought.nl/netlabs.nl/has_ta_19036/#ta_20326

DNSSEC

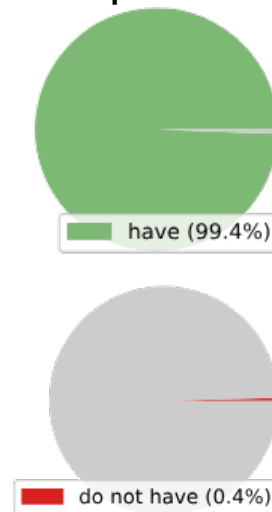
Root Key Trust Anchor Sentinel



with 902 resolvers



with 709 probes



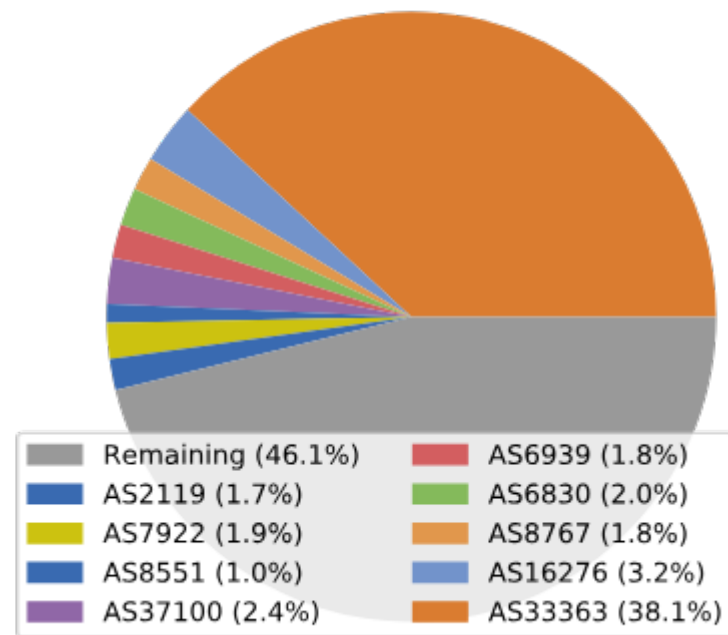
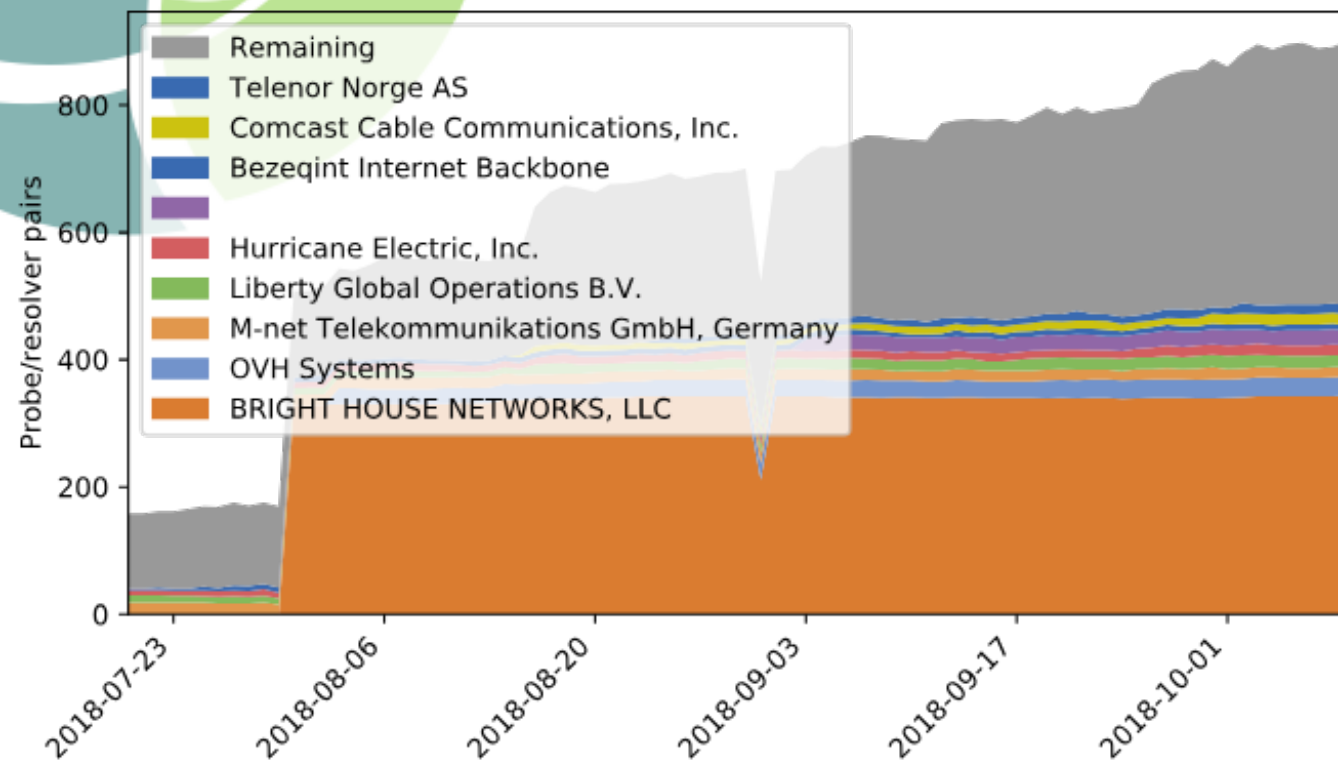
root KSK sentinel support

https://dnsthought.nl/netlabs.nl/has_ta_19036/#top_resolver_asns

DNSSEC

Root Key Trust Anchor Sentinel

with 902 resolvers
In 709 probes



Willem Toorop

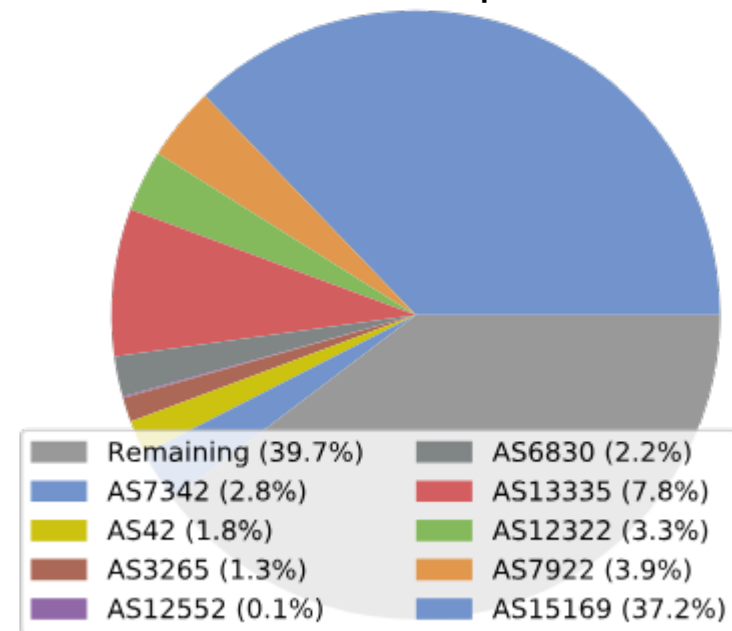
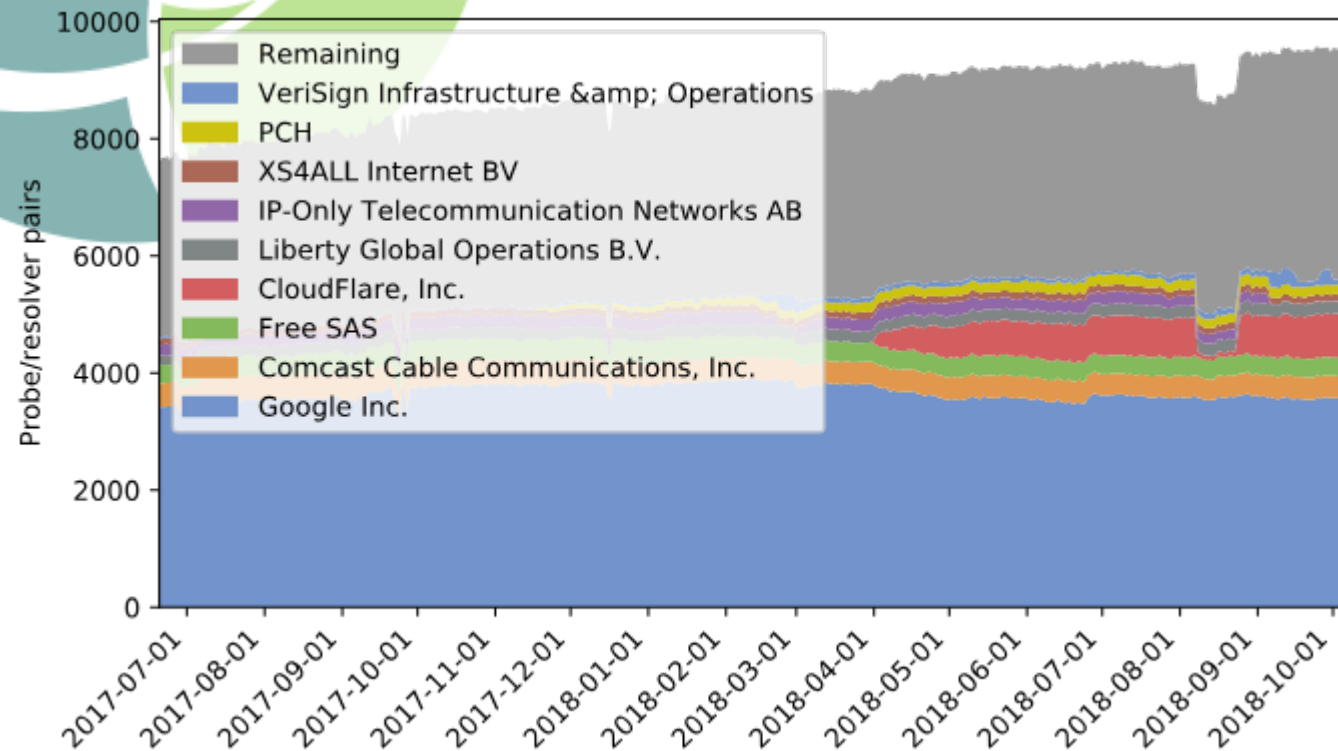
DNSThought @OARC29 25/39

validate DNSKEY algorithm RSA-SHA256
https://dnsthought.nl/netlabs.nl/can_rsasha256/#top_auth_asns

DNSSEC

Strange dent in August

with 9493 resolvers
In 5508 probes

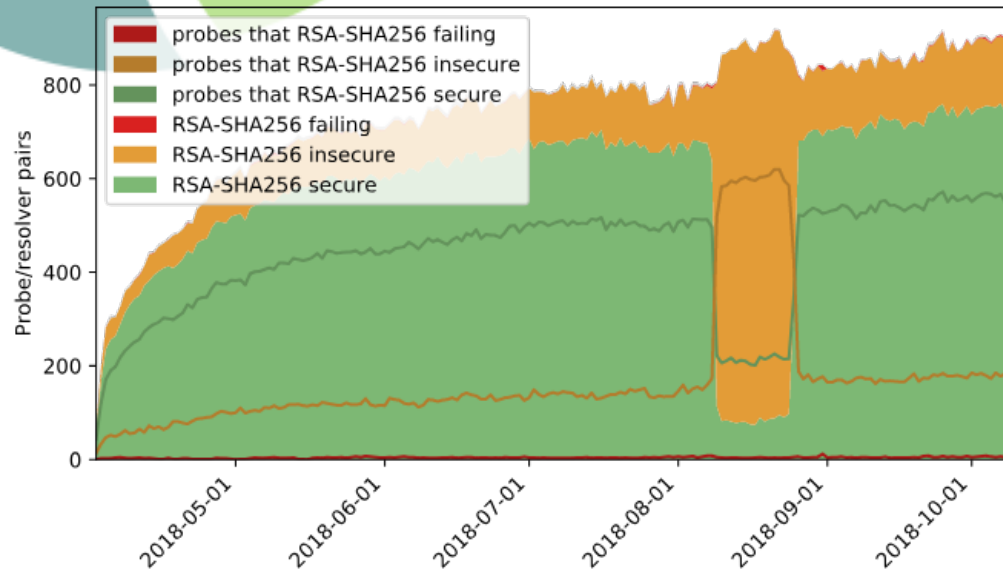


coming from AS13335

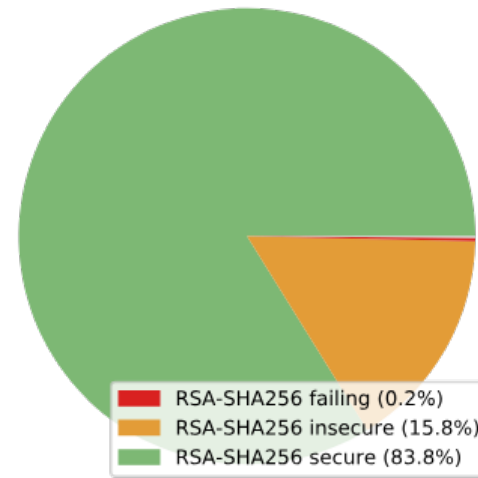
https://dnsthought.nl/netlabs.nl/auth_AS13335/#rsasha256

DNSSEC

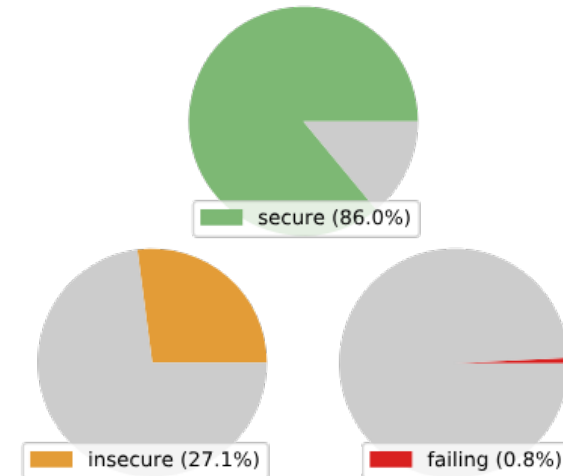
Strange dent in August



with 897 resolvers



with 650 probes



Willem Toorop

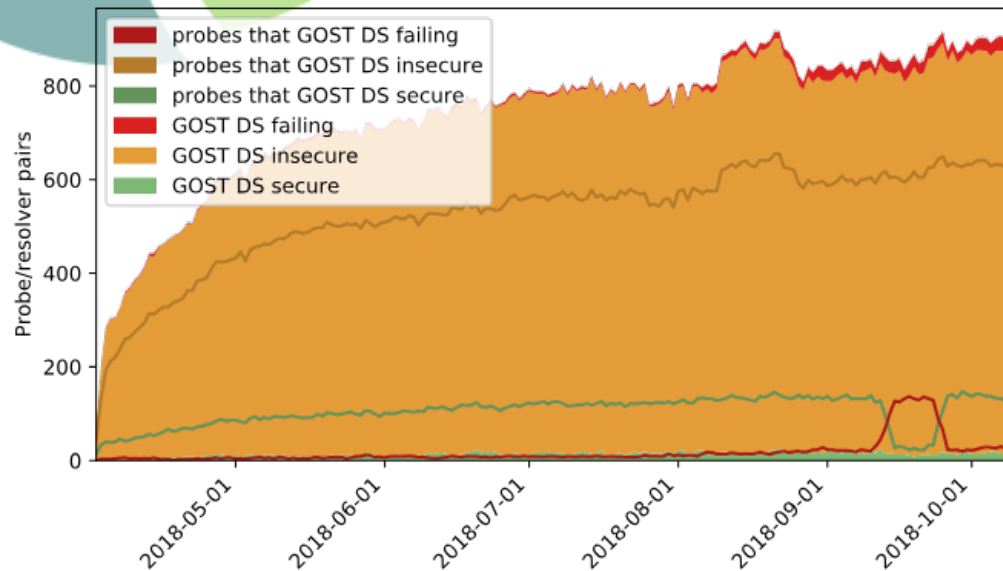
DNSThought @OARC29 27/39

coming from AS13335

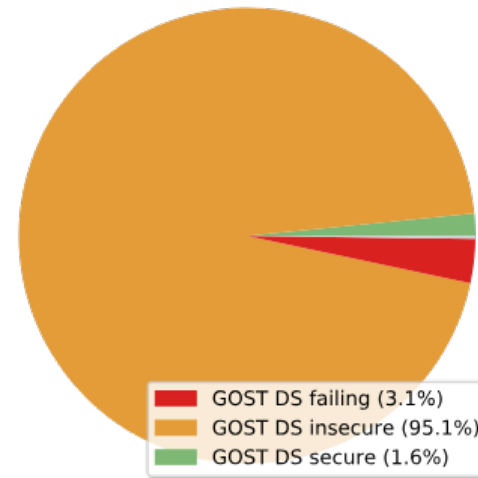
https://dnsthought.nl/netlabs.nl/auth_AS13335/#gost

DNSSEC

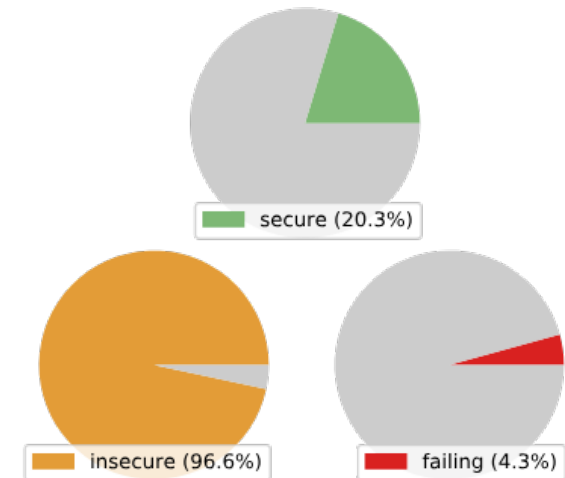
Strange broken GOST DS in September



with 897 resolvers



with 650 probes

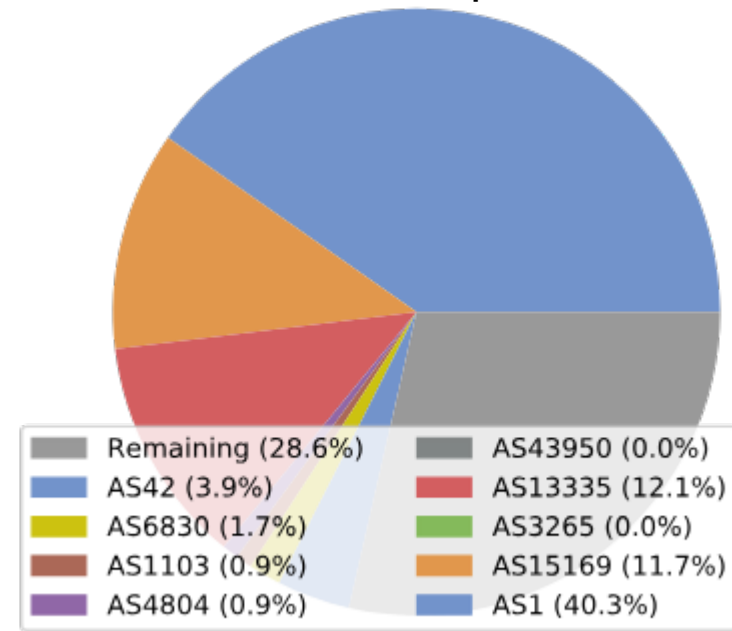


broken DS algorithm GOST validation support
https://dnsthought.nl/netlabs.nl/broken_gost/#top_auth_asns

DNSSEC

Strange broken GOST DS in September

with 231 resolvers
in 185 probes



Willem Toorop

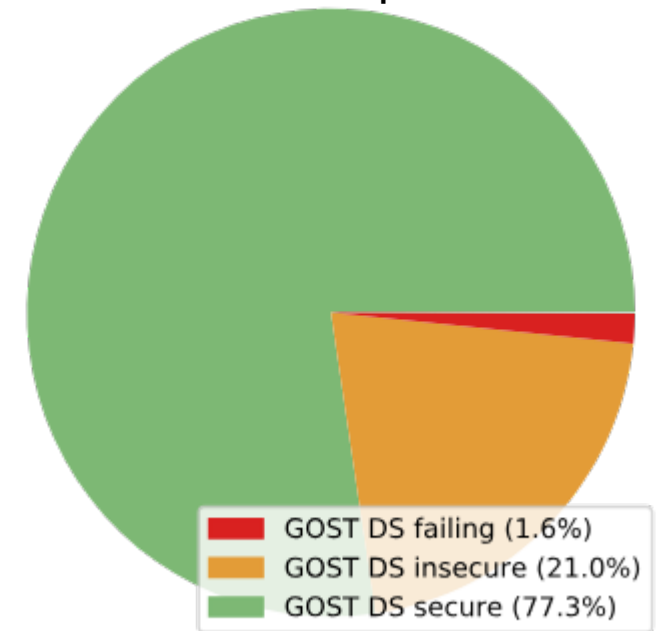
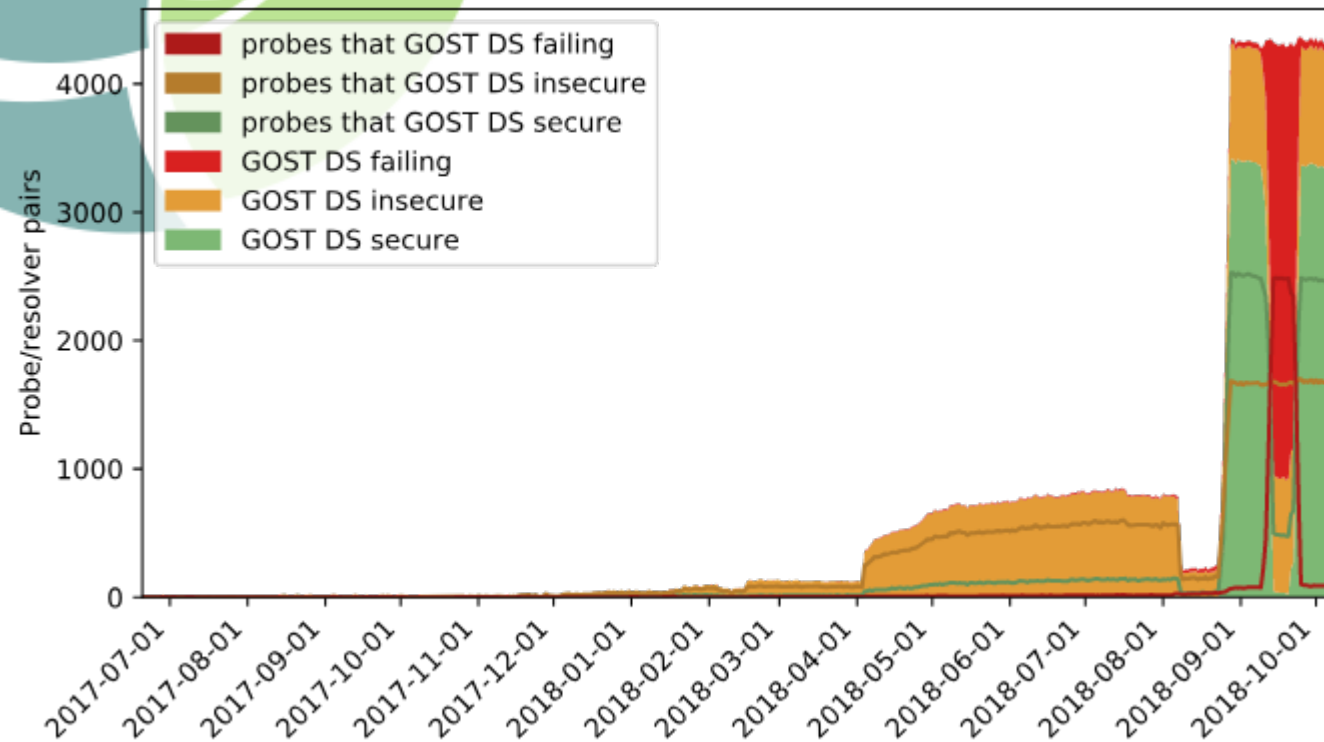
DNSThought @OARC29 29/39

validate DNSKEY algorithm ED25519
https://dnsthought.nl/netlabs.nl/can_ed25519/#gost

DNSSEC

The two incidents side by side

with 4304 resolvers
in 3025 probes



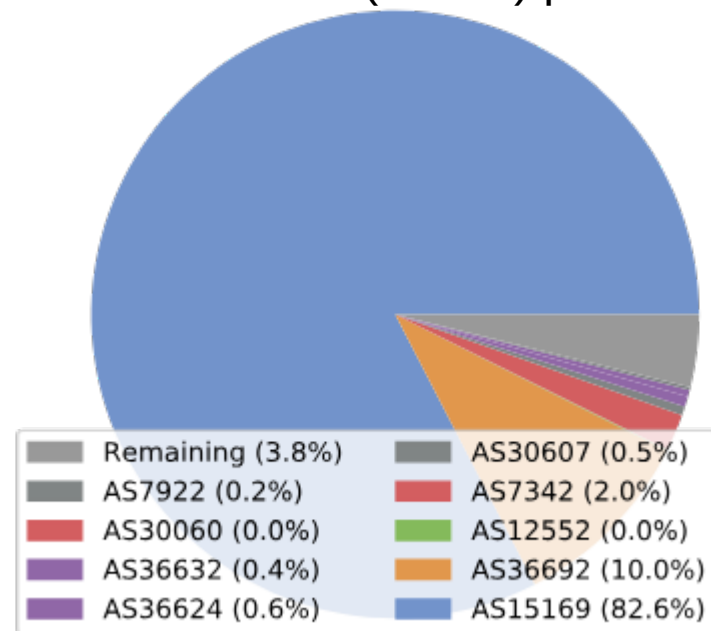
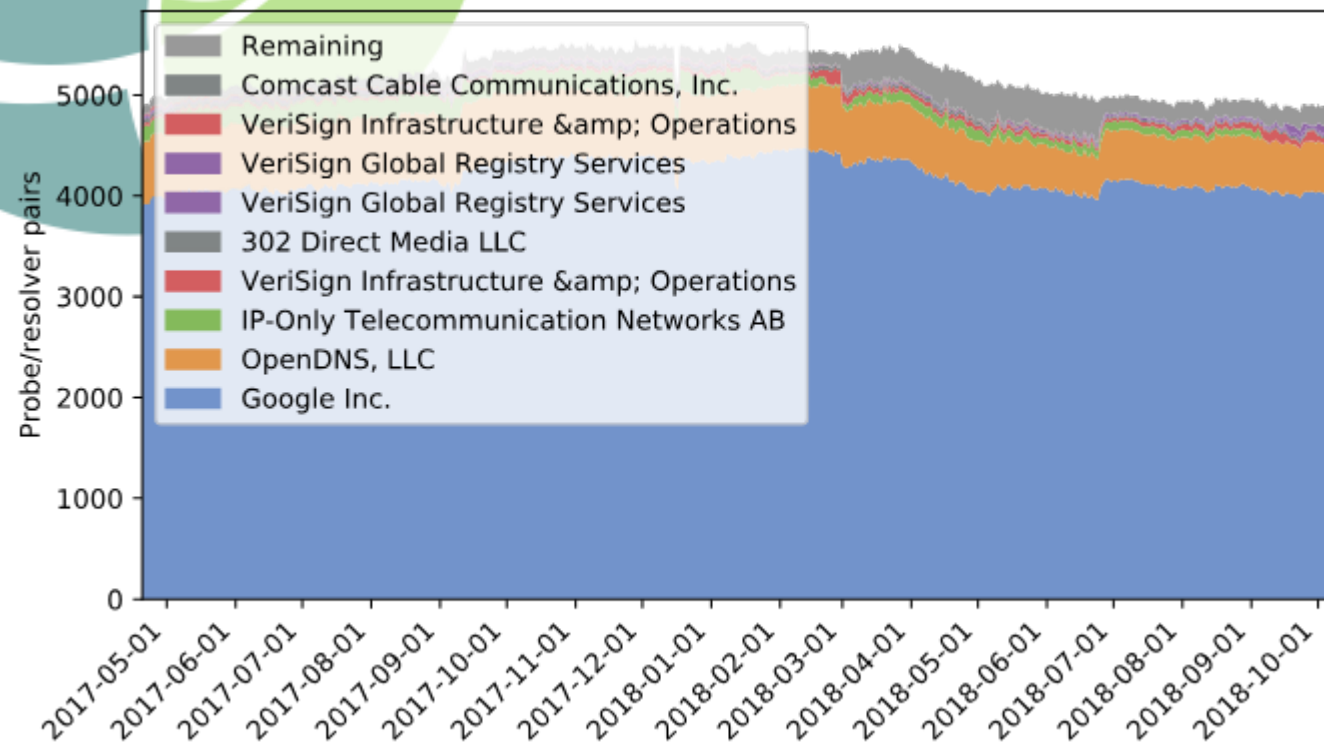
send an EDNS Client Subnet option

https://dnstthought.nl/netlabs.nl/does_ecs/#top_auth_asns

Send an EDNS Client Subnet option

Privacy

With 4832 (25.3%) resolvers
in 3283 (32.3%) probes



Willem Toorop

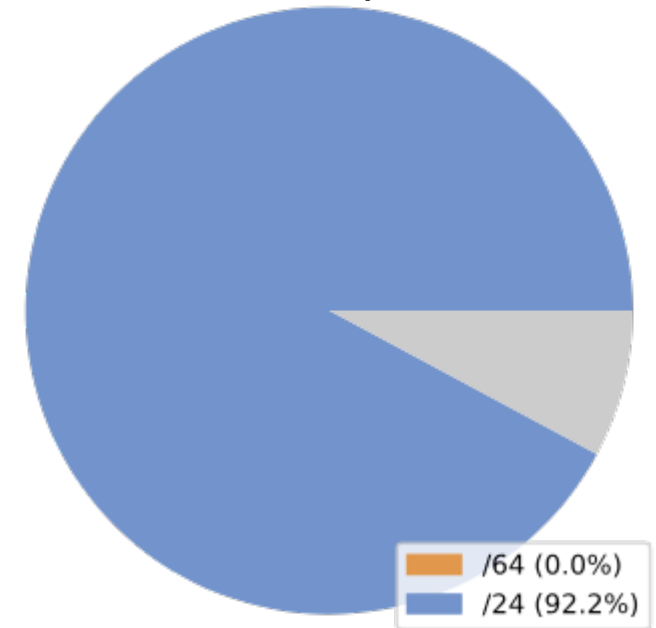
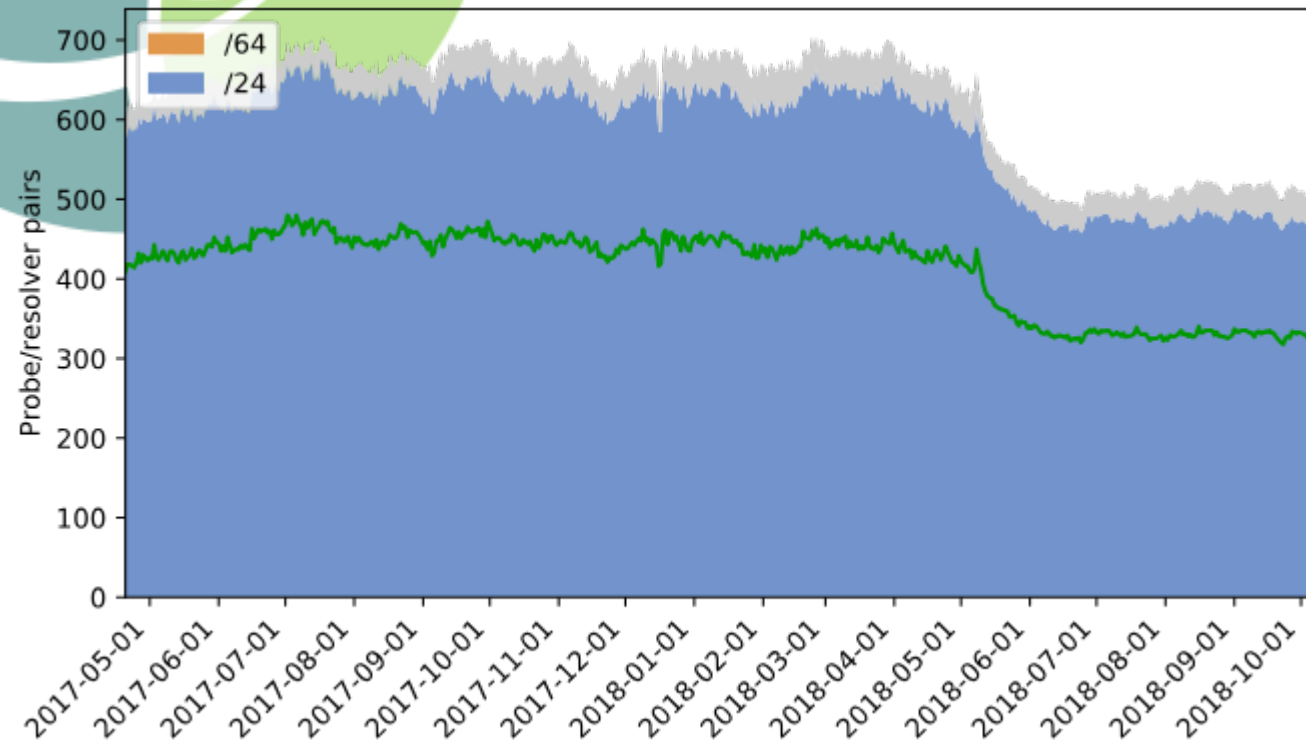
DNSThought @OARC29 31/39

coming from AS36692

https://dnstthought.nl/netlabs.nl/auth_AS36692/#ecs_masks

Send an EDNS Client Subnet option

With 498 resolvers
in 338 probes



Willem Toorop

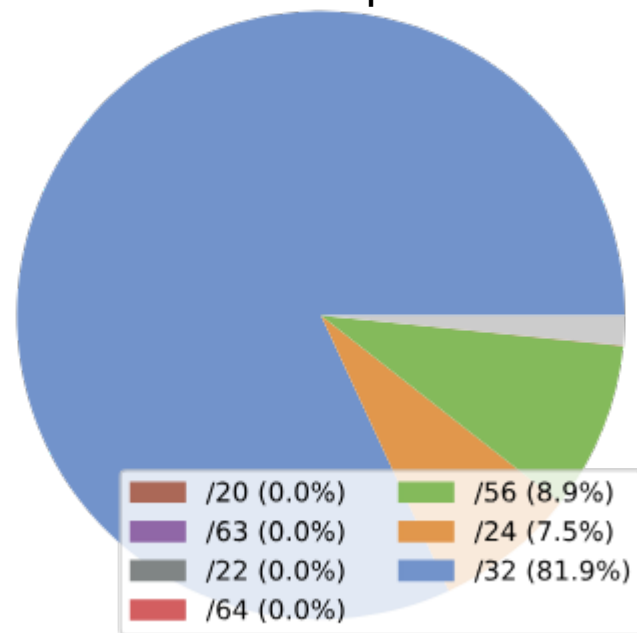
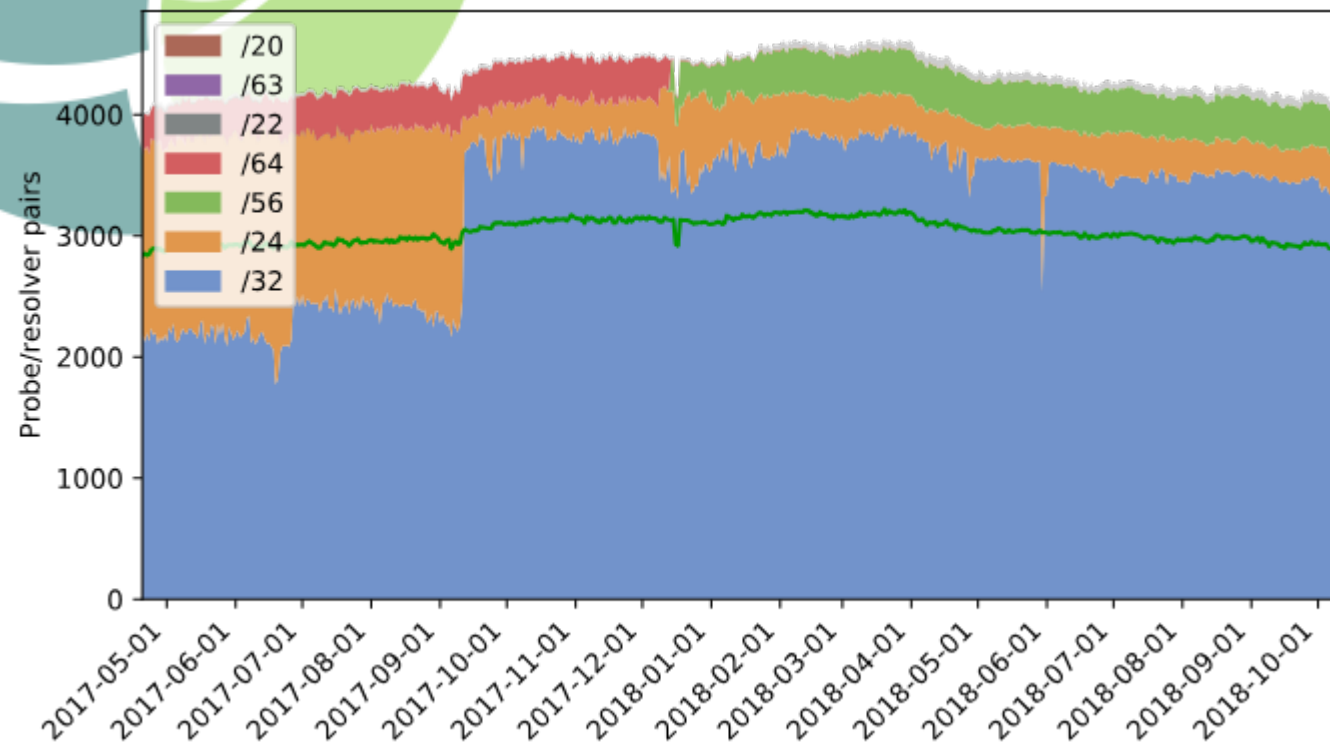
DNSThought @OARC29 32/39

coming from AS15169

https://dnstthought.nl/netlabs.nl/auth_AS15169/#ecs_masks

Send an EDNS Client Subnet option

With 4129 resolvers
in 2963 probes



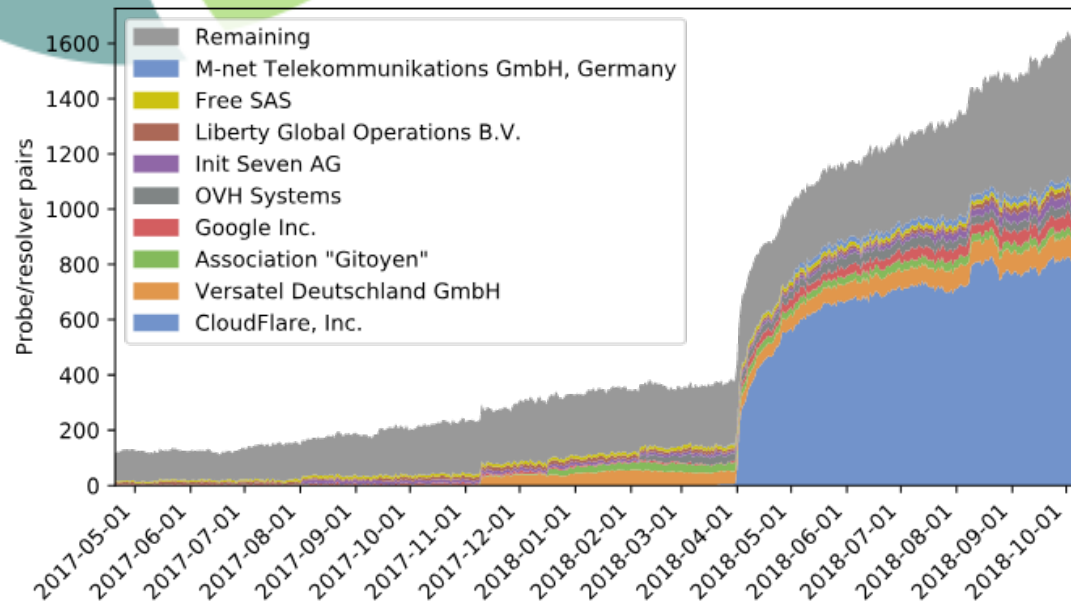
Willem Toorop

DNSThought @OARC29 33/39

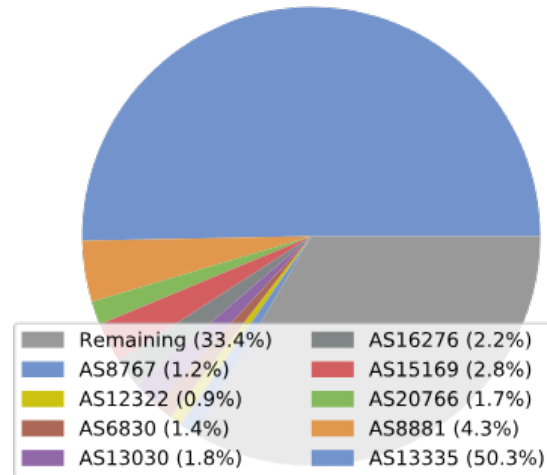
do QNAME Minimization

https://dnsthought.nl/netlabs.nl/does_qnamemin/#top_auth_asns

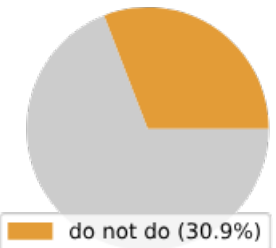
Privacy QNAME Minimization



With 1624 (8.5%) resolvers
in 1140 (11.2%) probes



with 1140 probes



do QNAME Minimization

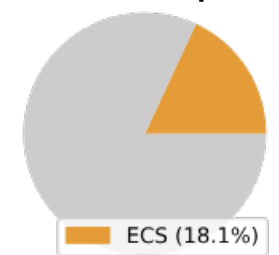
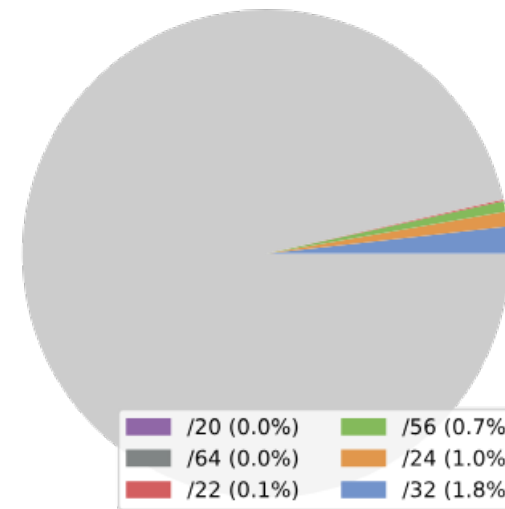
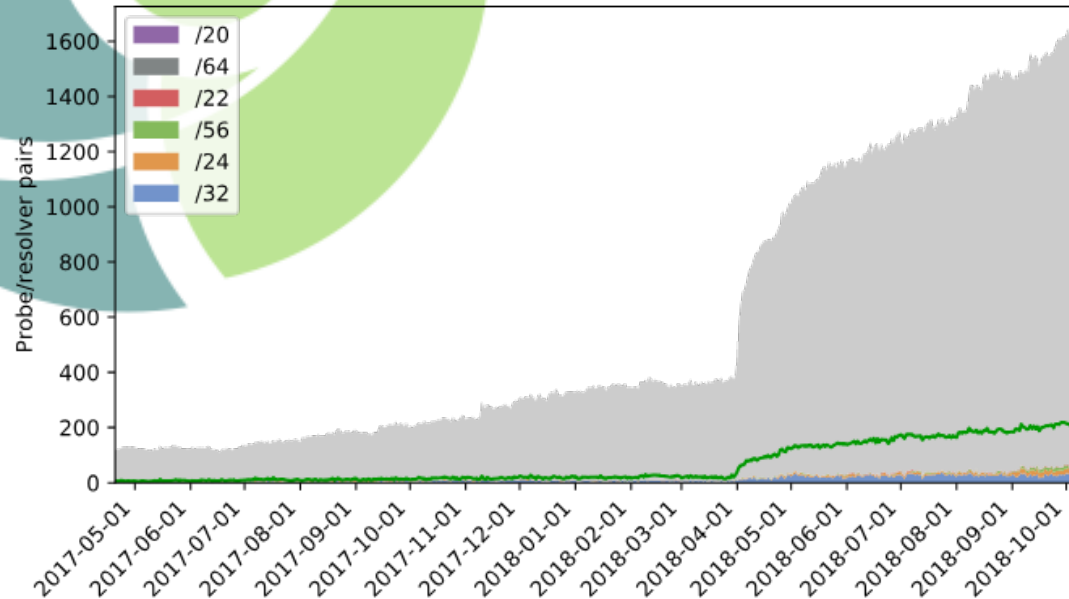
https://dnsthought.nl/netlabs.nl/does_qnamemin/#ecs_masks

Privacy

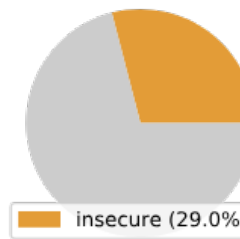
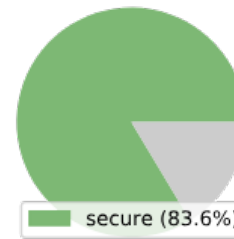
QNAME Minimization

with 1624 resolvers

with 1140 probes



- Also zero NX domain rewriting
- Also high % DNSSEC validation:



Willem Toorop

DNSThought @OARC29 35/39

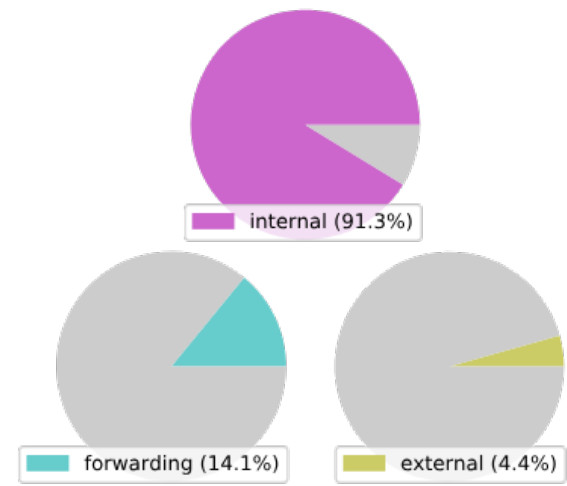
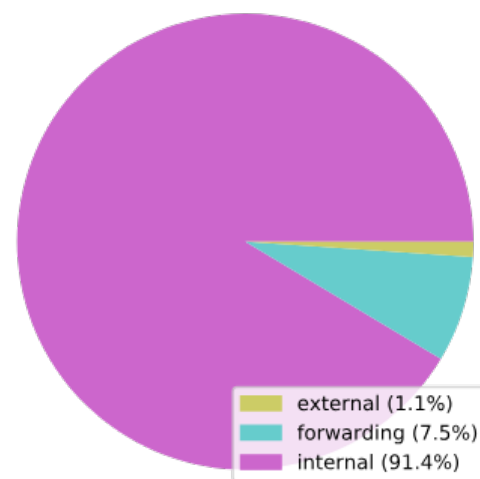
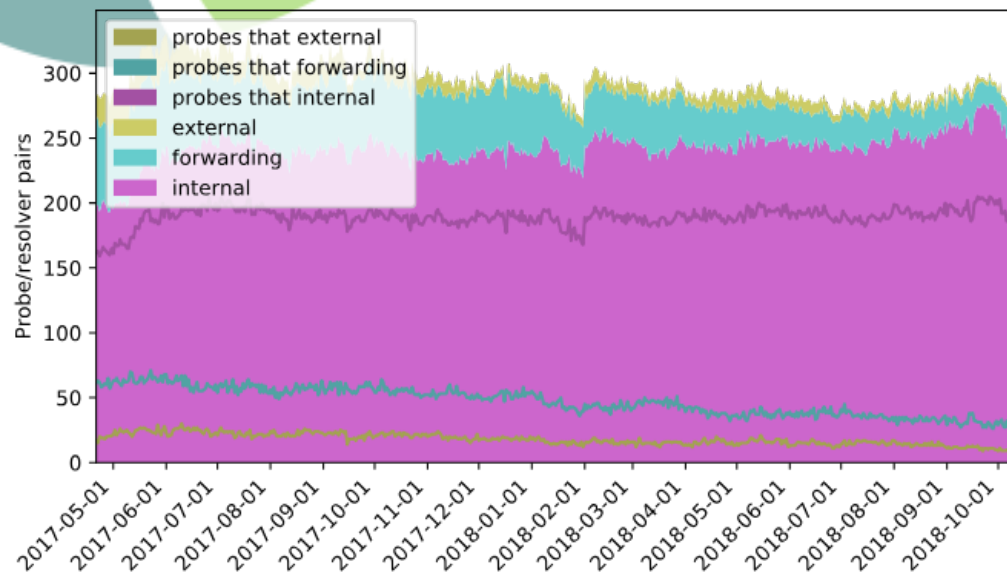
do NX domain rewriting

https://dnstought.nl/netlabs.nl/does_nxdomain/#int_fwd_ext

Privacy/Security NX domain rewriting

With 279 (1.5%) resolvers

With 206 (2.0%) probes



Willem Toorop

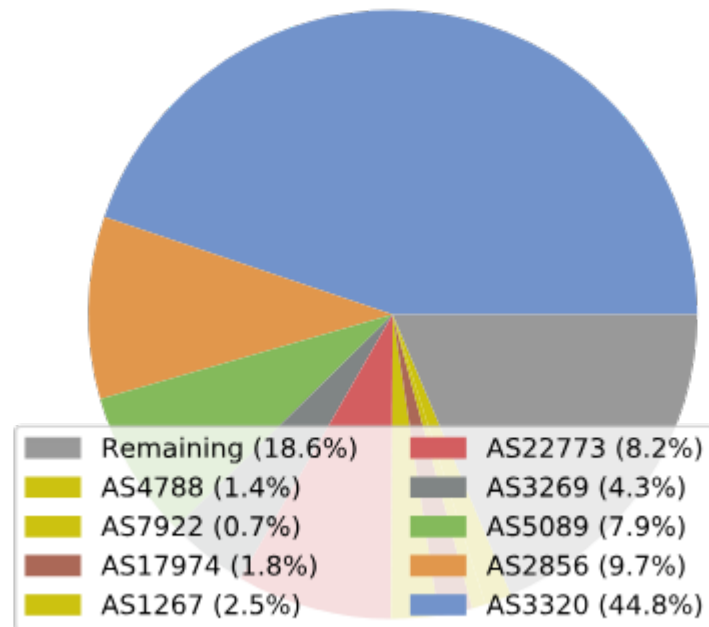
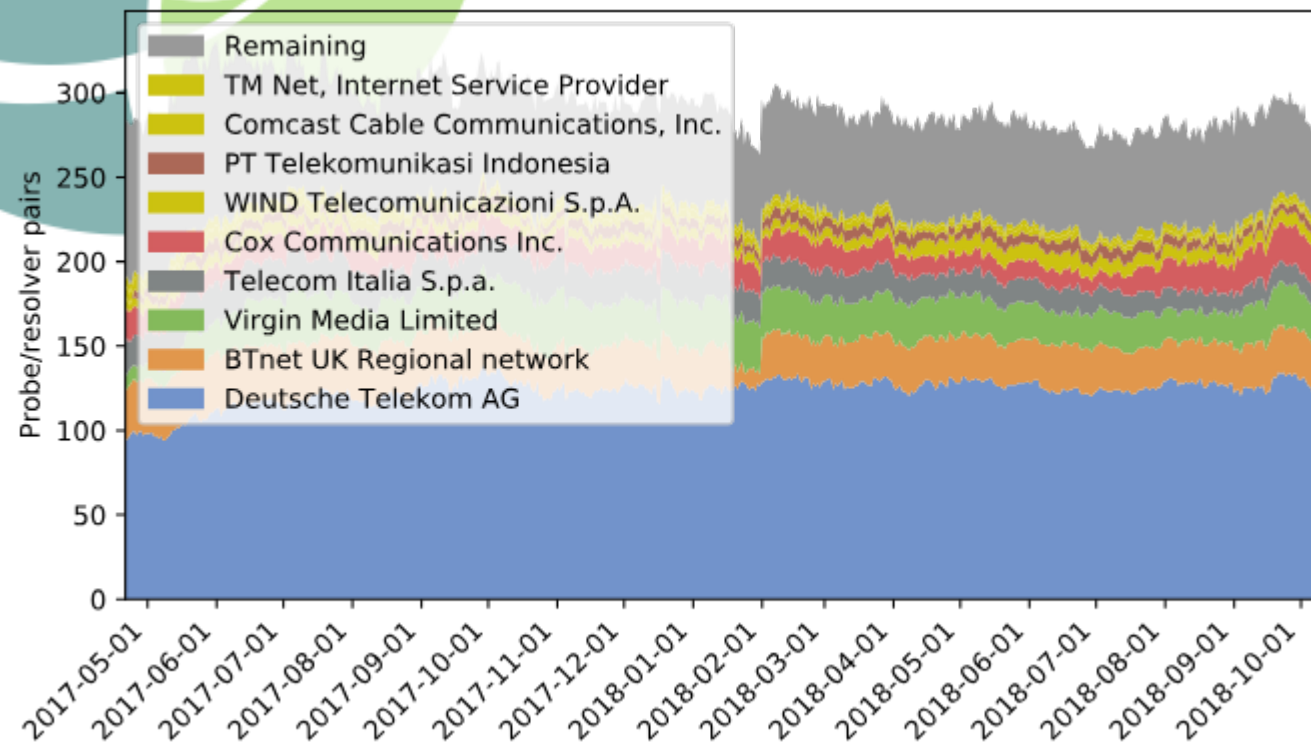
DNSThought @OARC29 36/39

do NX domain rewriting

https://dnsthought.nl/netlabs.nl/does_nxdomain/#top_auth_asns

Privacy/Security NX domain rewriting

Top 10 Probe ASNs == Top 10 Resolver ASNs == Top 10 Authoritative ASNs



Willem Toorop

DNSThought @OARC29 37/39

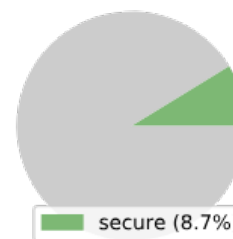
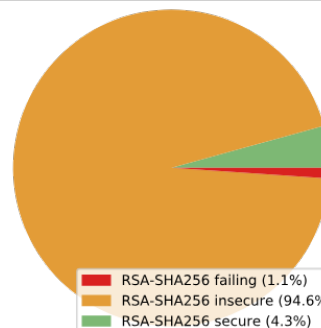
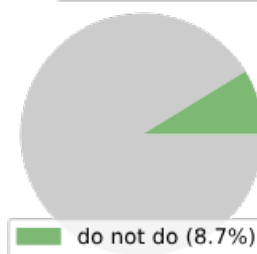
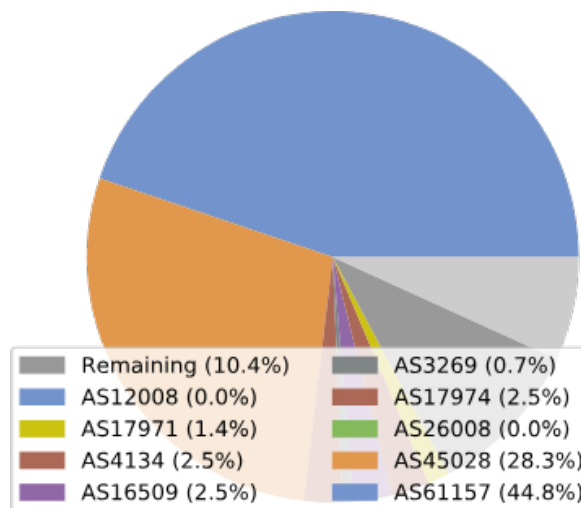
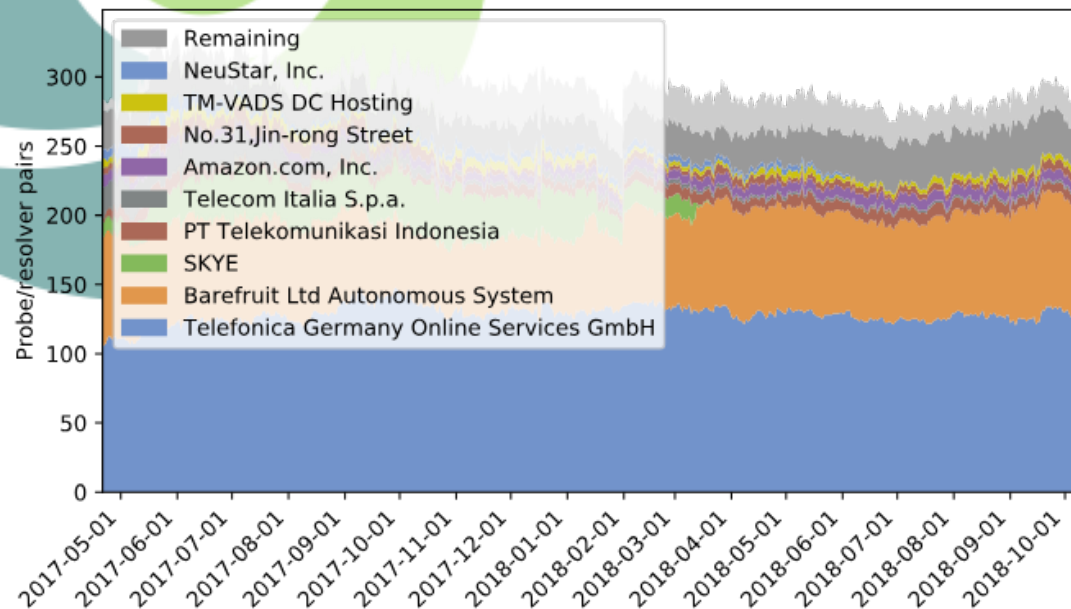
do NX domain rewriting

https://dnsthought.nl/netlabs.nl/does_nxdomain/#top_nxhj_asns

Privacy/Security NX domain rewriting

with 279 resolvers

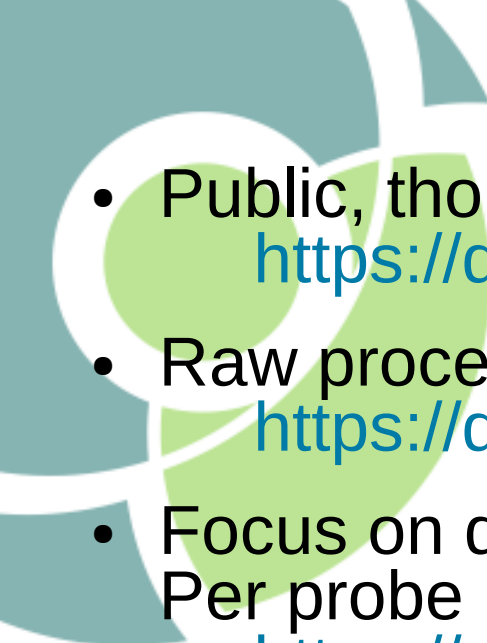
with 206 probes



- Also only 4.3% DNSSEC validation:

Willem Toorop

DNSThought @OARC29 38/39



DNSThought

- Public, though rough, interface to data available
<https://dnsthought.nlnetlabs.nl/>
- Raw processed data available too
<https://dnsthought.nlnetlabs.nl/raw>
- Focus on development of properties over time
Per probe properties & capabilities with RIPE Atlas Probe Tags
<https://atlas.ripe.net/docs/probe-tags/>
- Lots to improve
 - Dynamic (zoomable) plots
 - IPv4 & IPv6 ECS detection
 - Better DS algorithm detection
 - Fragment dropping / Path MTU

Questions ?
Suggestions ●