

# Adoption and Implementation of QNAME Minimization in DNS

Jonathan Magnusson

Karlstad University

[jonathan.magnusson@kau.se](mailto:jonathan.magnusson@kau.se)



# \$ whoami

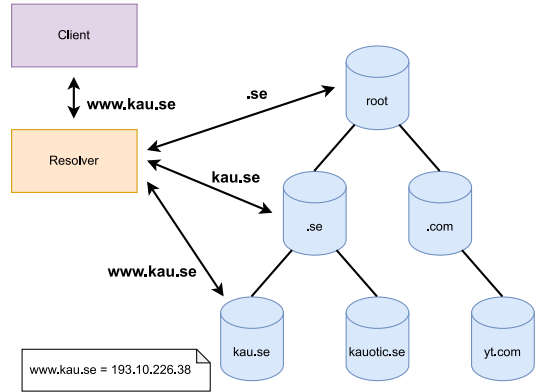
## Jonathan Magnusson

- PhD Student:
  - Karlstad University
  - Internetstiftelsen (.se & .nu)
  - Cybersecurity and Network Analysis of DNS
- Founder of KAUotic Hacking Club
- Cyber Range Development



# Query Name Minimization

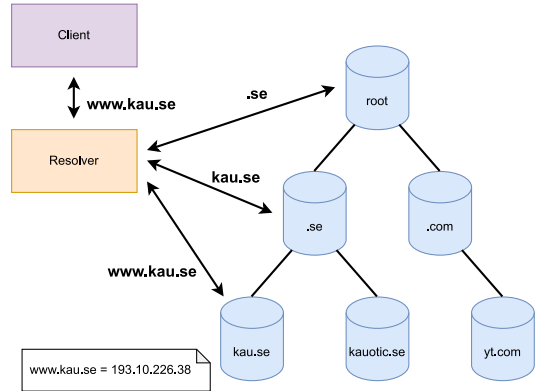
Data Minimization



# Query Name Minimization

## Data Minimization

- Various resource records
- Minimization depth limit
- Plethora of implementations



# Study 1: Adoption of QNAME Minimization



# Adoption

## A Second Look at DNS QNAME Minimization (PAM 2023)

Jonathan Magnusson, Moritz Müller, Anna Brunstrom, Tobias Pulls

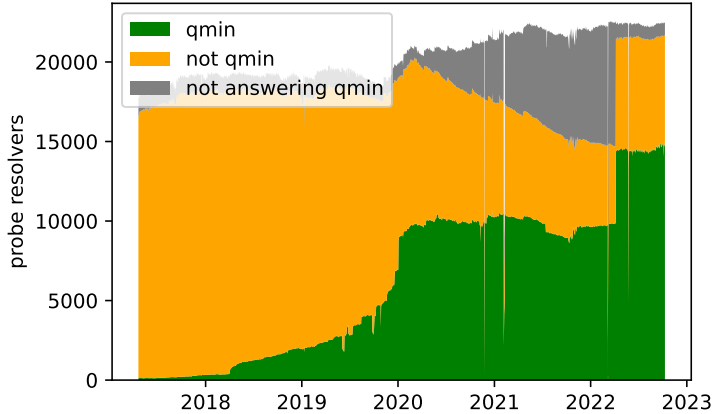
- Active measurements
  - `$ dig a.b.qnamemintest.net TXT → "HOORAY"/"NO"`
  - **Extended** analysis of RIPE Atlas probes
  - Query open resolvers, **100** queries {**nvirginia,tokyo,frankfurt**}
- Passive measurements
- Controlled experiments

Extended work from "A First Look at QNAME Minimization in the Domain Name System"



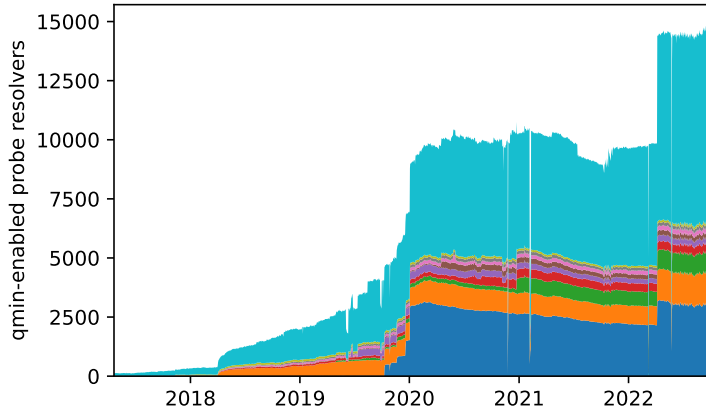
# Adoption Measurements

## RIPE Atlas Probes



# Adoption Measurements

RIPE Atlas Probes



Cloudflare, AS13335

Google, AS15169





# Adoption Measurements

## Open Resolvers

year	geo	#resolv	#queries	resp	noerr	correct	qmin
2018	netherlands	8M	8M	64%	32%	72%	1.6%
2022	nvirginia	6M	600M	70.82%	19.46%	78.12%	16.43%
2022	tokyo	6M	600M	70.71%	19.45%	78.32%	16.42%
2022	frankfurt	6M	600M	70.78%	19.45%	78.21%	16.42%

Table: Categorized responses from open resolvers



# Adoption Measurements

Google Public DNS behavior:

```
dig @8.8.8.8 a.b.qnamemin-test.nl netlabs.nl TXT +short
"NO - QNAME minimisation is NOT enabled on your resolver :("

dig @8.8.8.8 a.b.qnamemin-test.internet.nl TXT +short
"HOORAY - QNAME minimisation is enabled on your resolver :)"

dig @8.8.8.8 a.b.qnamemintest.net TXT +short
"NO - QNAME minimisation is NOT enabled on your resolver :("
```



# Study 2: Implementation of QNAME Minimization



# Implementation

## Fingerprinting DNS Resolvers using Query Patterns from QNAME Minimization (Under submission)

Jonathan Magnusson

Query Representation:<sup>1</sup>

- www.kau.se NS → 3NS
- L4.L3.example.com A → 4A

<sup>1</sup> A First Look at QNAME Minimization in the Domain Name System



# Implementation

## Fingerprinting DNS Resolvers using Query Patterns from QNAME Minimization (Under submission)

Jonathan Magnusson

### Query Representation:<sup>1</sup>

- `www.kau.se NS`  $\rightarrow$  `3NS`
- `L4.L3.example.com A`  $\rightarrow$  `4A`

`fpdns.se` responds to ANY subdomain:

```
dig L24...L4.nonce1.fpdns.se @resolver1
```

1. `nonce1.fpdns.se A`  $\rightarrow$  `3A`
2. `L4.nonce1.fpdns.se A`  $\rightarrow$  `4A`
3. `L5.L4.nonce1.fpdns.se A`  $\rightarrow$  `5A`
4. `L6.L5.L4.nonce1.fpdns.se A`  $\rightarrow$  `6A`

<sup>1</sup> A First Look at QNAME Minimization in the Domain Name System



# Implementation

## Fingerprinting DNS Resolvers using Query Patterns from QNAME Minimization (Under submission)

Jonathan Magnusson

fpdns.se responds to ANY subdomain:

```
dig L24...L4.nonce1.fpdns.se @resolver1
```

1. nonce1.fpdns.se A  $\rightarrow$  3A
2. L4.nonce1.fpdns.se A  $\rightarrow$  4A
3. L5.L4.nonce1.fpdns.se A  $\rightarrow$  5A
4. L6.L5.L4.nonce1.fpdns.se A  $\rightarrow$  6A

resolver1  $\rightarrow$  3A-4A-5A-6A... (Pattern/Signature)

Query Representation:<sup>1</sup>

- www.kau.se NS  $\rightarrow$  3NS
- L4.L3.example.com A  $\rightarrow$  4A

<sup>1</sup> A First Look at QNAME Minimization in the Domain Name System



# Implementation Measurements

## Establishing Signatures

	Signature
No qmin	24A
RFC 7816	3NS-4NS-5NS-...-22NS-23NS-24NS-24A
RFC 9156	3A-4A-5A-6A-9A-12A-15A-18A-21A-24A
Bind 9.18.14	4A-5A-6A-7A-24A
Bind 9.14.0	3NS-4NS-5NS-6NS-24A
Knot Resolver 5.6.0	3NS-4NS-5NS-...-22NS-23NS-24A
Knot Resolver 3.0.0	3NS-4NS-5NS-...-22NS-23NS-24A
PowerDNS 4.8.4	3A-4A-5A-6A-9A-12A-15A-18A-21A-24A
PowerDNS 4.4.0	3A-4A-5A-6A-7A-10A-13A-16A-19A-22A-24A
Unbound 1.17.1	3A-4A-5A-6A-9A-12A-15A-18A-22A-24A
Unbound 1.8.0	3A-4A-5A-6A-9A-12A-15A-18A-22A-24A



# Implementation Measurements

## Establishing Signatures: Unbound

Cache	Unbound Signature
none	3A-4A-7A-10A-13A-16A-20A-24A
TLD	3A-4A-5A-8A-11A-14A-17A-21A-24A
SLD	3A-4A-5A-6A-9A-12A-15A-18A-22A-24A





# Implementation Measurements

## Ingress Patterns

PATTERN	Count
NON-MINIMIZING	2089738
INCOMPLETE	473563
3A-24A	74566
3A-24A-24A	24909
3A-3A-24A	20402
3A-3A-24A-24A	9486
24A-3A	7172
3A-24A-24A-24A	7161
<b>24A-3A-24A</b>	6997
3A-4A-24A	5553
4A-5A-6A-7A-24A	5355
3A-3A-3A-24A	5200
3A-24A-3A-24A	4459
3A-24A-3A	4156
<b>24A-3A-24A-24A</b>	3075
3A-4A-5A-6A-9A-12A-15A-18A-22A-24A	3062
3A-3A-24A-24A-24A	3002
3A-3A-3A-24A-24A	2918
3A-24A-24A-24A-24A	2554
3A-4A-5A-24A	2084
OTHER	611831



# Implementation Measurements

## Ingress Patterns

PATTERN	Count
NON-MINIMIZING	2089738
INCOMPLETE	473563
3A-24A	74566
3A-24A-24A	24909
3A-3A-24A	20402
3A-3A-24A-24A	9486
24A-3A	7172
3A-24A-24A-24A	7161
<b>24A-3A-24A</b>	6997
3A-4A-24A	5553
4A-5A-6A-7A-24A	5355
3A-3A-3A-24A	5200
3A-24A-3A-24A	4459
3A-24A-3A	4156
<b>24A-3A-24A-24A</b>	3075
3A-4A-5A-6A-9A-12A-15A-18A-22A-24A	3062
3A-3A-24A-24A-24A	3002
3A-3A-3A-24A-24A	2918
3A-24A-24A-24A-24A	2554
3A-4A-5A-24A	2084
OTHER	611831

Minimizing **and** Non-Minimizing resolver!



# Implementation Measurements

## Egress Signatures

Signature	Likely Resolver	Public	Probes
4A-5A-6A-7A-24A	Bind	109,366	83
3A-4A-5A-6A-9A-12A-15A-18A-22A-24A	Unbound (SLD)	43,071	90
3NS-4NS-5NS-6NS-24A	Old Bind	8,661	60
3A-4A-5A-8A-11A-14A-17A-21A-24A	Unbound (TLD)	5,664	139
3A-4A-5A-6A-9A-12A-15A-18A-21A-24A	PowerDNS	1,966	141
3NS-4NS-5NS-...-22NS-23NS-24A	Knot	1,003	114
3A-4A-5A-6A-7A-10A-13A-16A-19A-22A-24A	Old PowerDNS	970	24
3A-4A-7A-10A-13A-16A-20A-24A	Unbound	239	24



# Discussion

- The future of QNAME Minimization  
<https://dnsthought.nlnetlabs.nl/#qnamemin>
- Help and speed up adoption
- Age of resolvers
  - Increase granularity
  - Extend scope

