Hands on **DNS** Privacy

Online for NOMINET

20-24 September 2021

Privacy

March 2011 : I-D
Privacy Considerations
for Internet Protocols

June 2013 : [redacted] Revelations
Morecowbell

July 2013 : RFC6973
Privacy Considerations
for Internet Protocols

May 2014 : RFC7258
Pervasive Monitoring
is an Attack

Privacy
Folk Singer

Picture © (CC BY 3.0) Laura Poitras

Encryption Everywhere

tions
tocols

June 2013 : [redacted] Revelations
Morecowbell

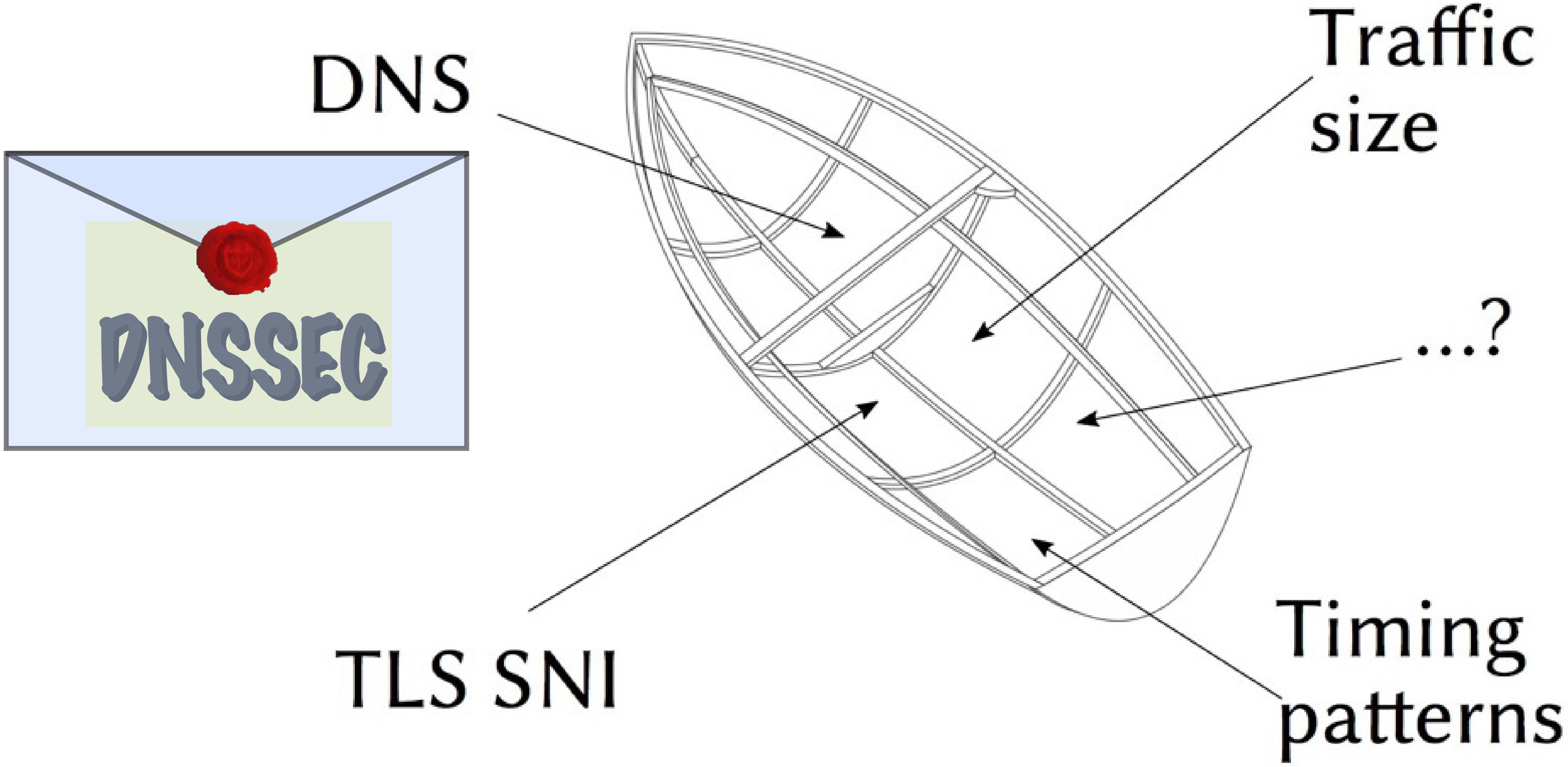
July 2013 : RFC6973
Privacy Considerations
for Internet Protocols

May 2014 : RFC7258
Pervasive Monitoring
is an Attack

Privacy Folk Singer

Picture © (CC BY 3.0) Laura Poitras

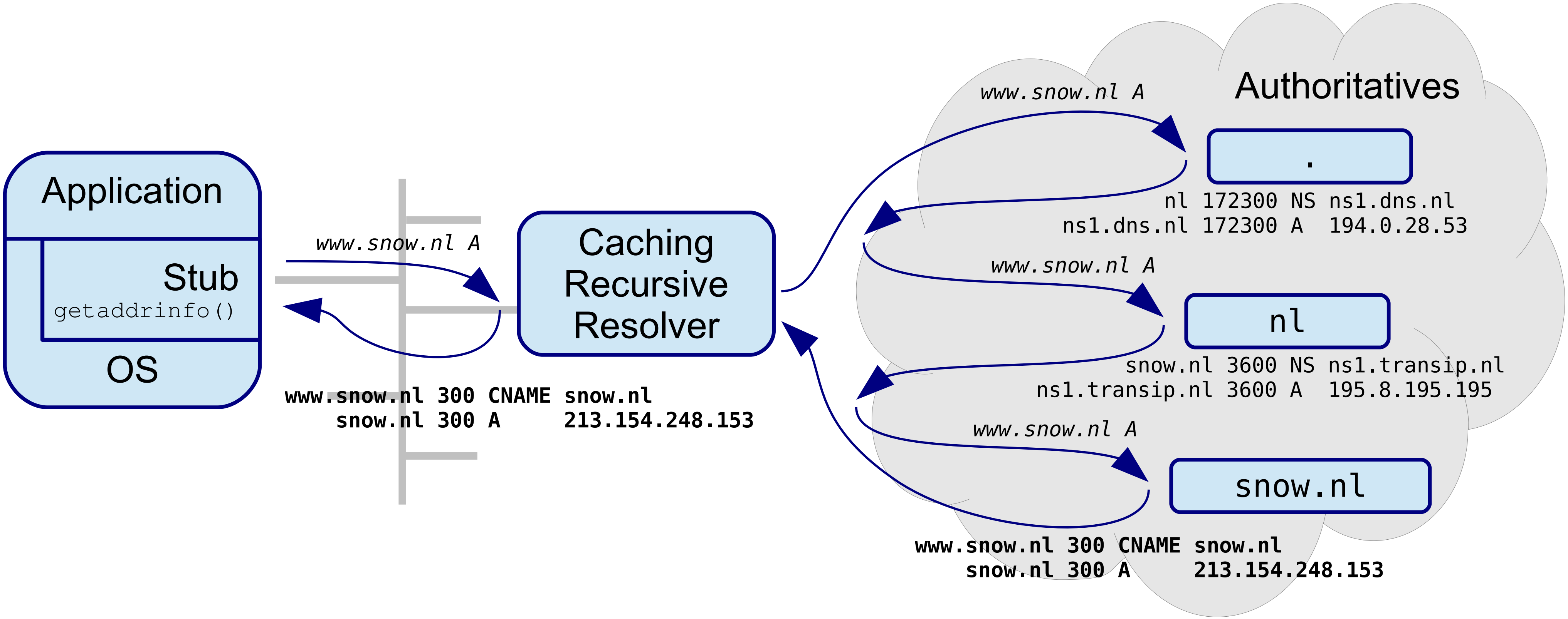
Privacy



- NSA's Morecowbell: an on DNS based monitoring system

Leaky Boat van DKG

Privacy issues with DNS



```
www.snow.nl 300 CNAME snow.nl
    snow.nl 300 A     213.154.248.153
```

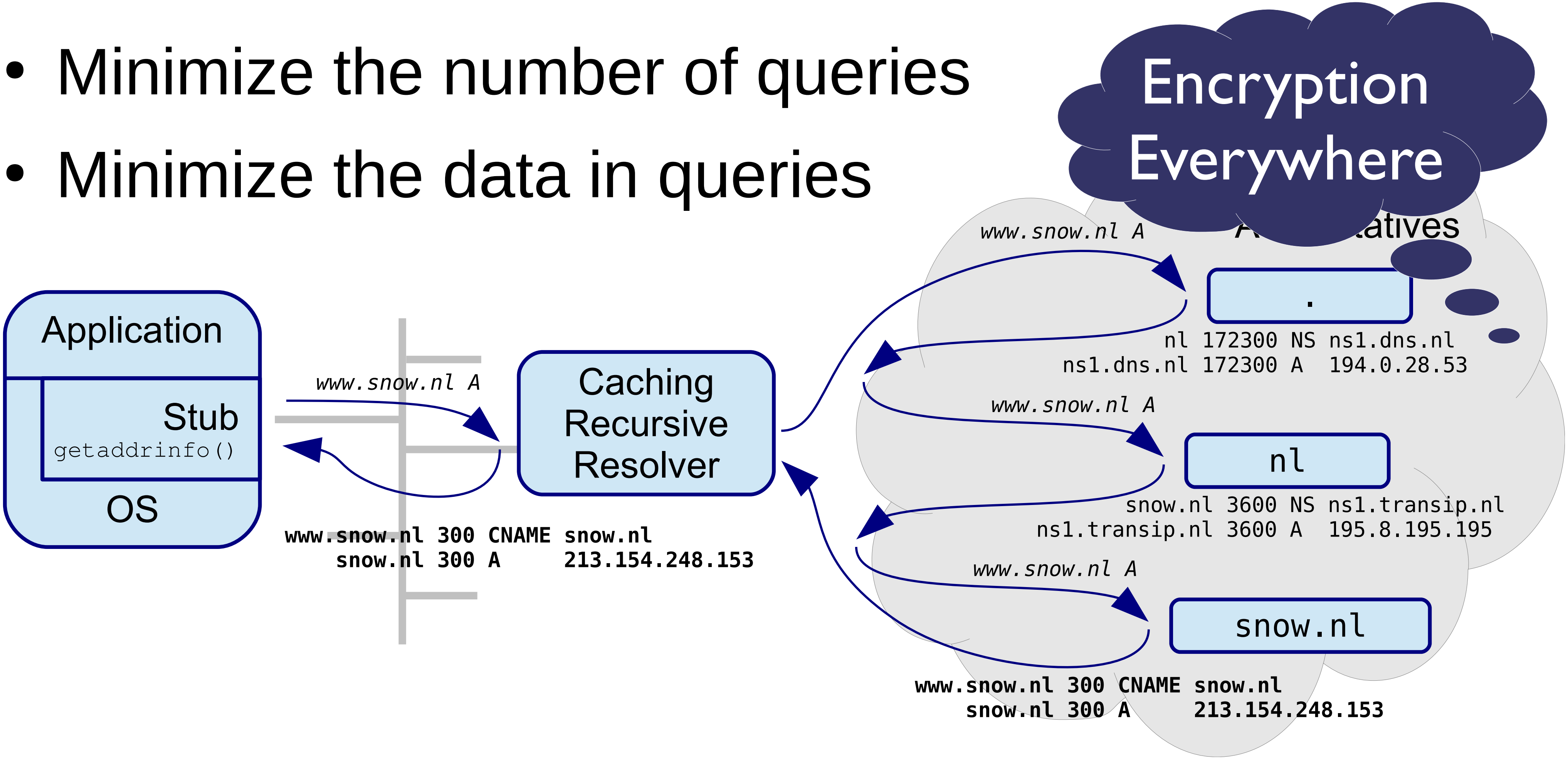
```
         nl 172300 NS ns1.dns.nl
ns1.dns.nl 172300 A  194.0.28.53
```

```
       snow.nl 3600 NS ns1.transip.nl
ns1.transip.nl 3600 A  195.8.195.195
```

```
www.snow.nl 300 CNAME snow.nl
    snow.nl 300 A     213.154.248.153
```

Privacy issues with DNS

- Minimize the number of queries
- Minimize the data in queries



```
                  nl 172300 NS ns1.dns.nl
          ns1.dns.nl 172300 A  194.0.28.53
```

```
            snow.nl 3600 NS ns1.transip.nl
     ns1.transip.nl 3600 A  195.8.195.195
```

```
www.snow.nl 300 CNAME snow.nl
    snow.nl 300 A     213.154.248.153
```

```
www.snow.nl 300 CNAME snow.nl
    snow.nl 300 A     213.154.248.153
```

Privacy issues with DNS

minimize # queries – local root

- RFC 8806 - Running a Root Server Local to a Resolver

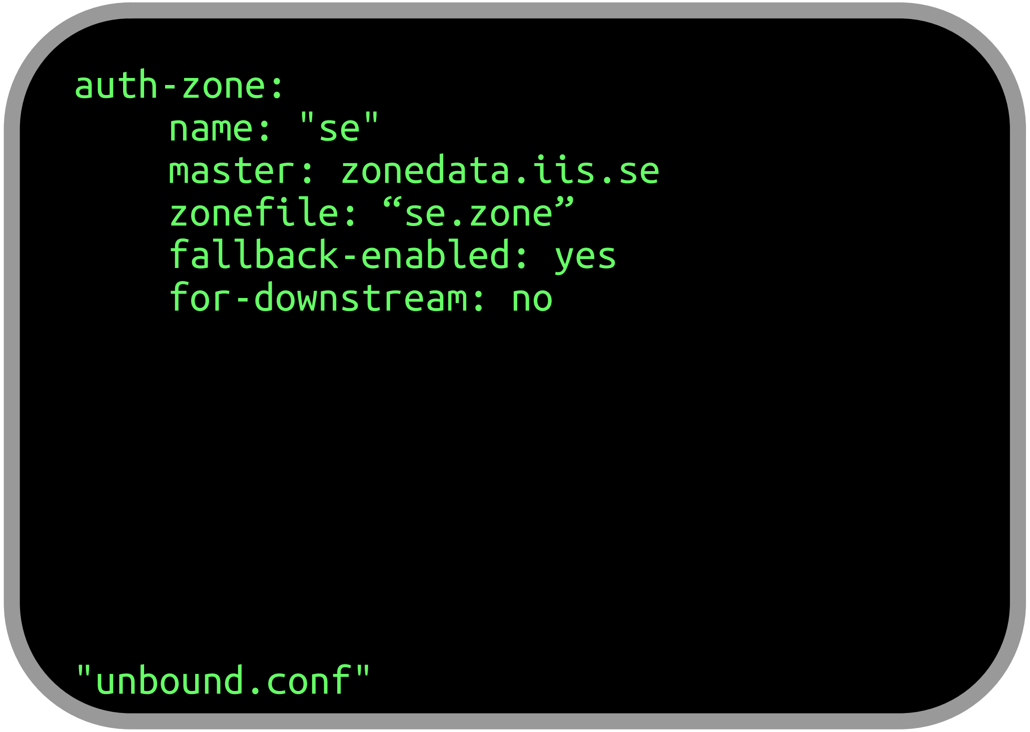
```
auth-zone:
    name: "."
    master: 199.9.14.201
    master: 192.33.4.12
    master: 199.7.91.13
    master: 192.5.5.241
    master: 192.112.36.4
    master: 193.0.14.129
    master: 192.0.47.132
    master: 192.0.32.132
    fallback-enabled: yes
    for-downstream: no
    for-upstream: yes

"unbound.conf"
```

unbound

Privacy issues with DNS

minimize # queries – local auth zone

- RFC 8806 -
  Running a Root Server Local to a Resolver
- Not just for the root



```
auth-zone:
     name: "se"
     master: zonedata.iis.se
     zonefile: “se.zone”
     fallback-enabled: yes
     for-downstream: no
```

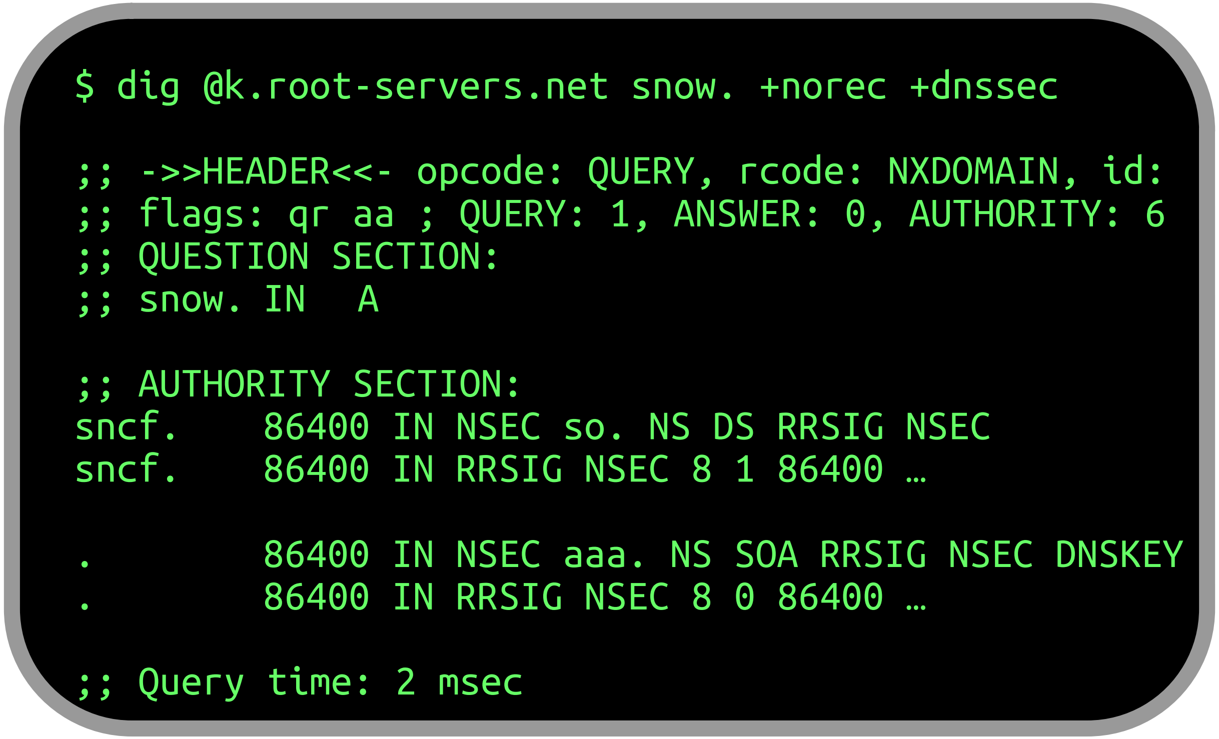
"unbound.conf"

unbound

Privacy issues met DNS

mimize # queries – aggressive NSEC

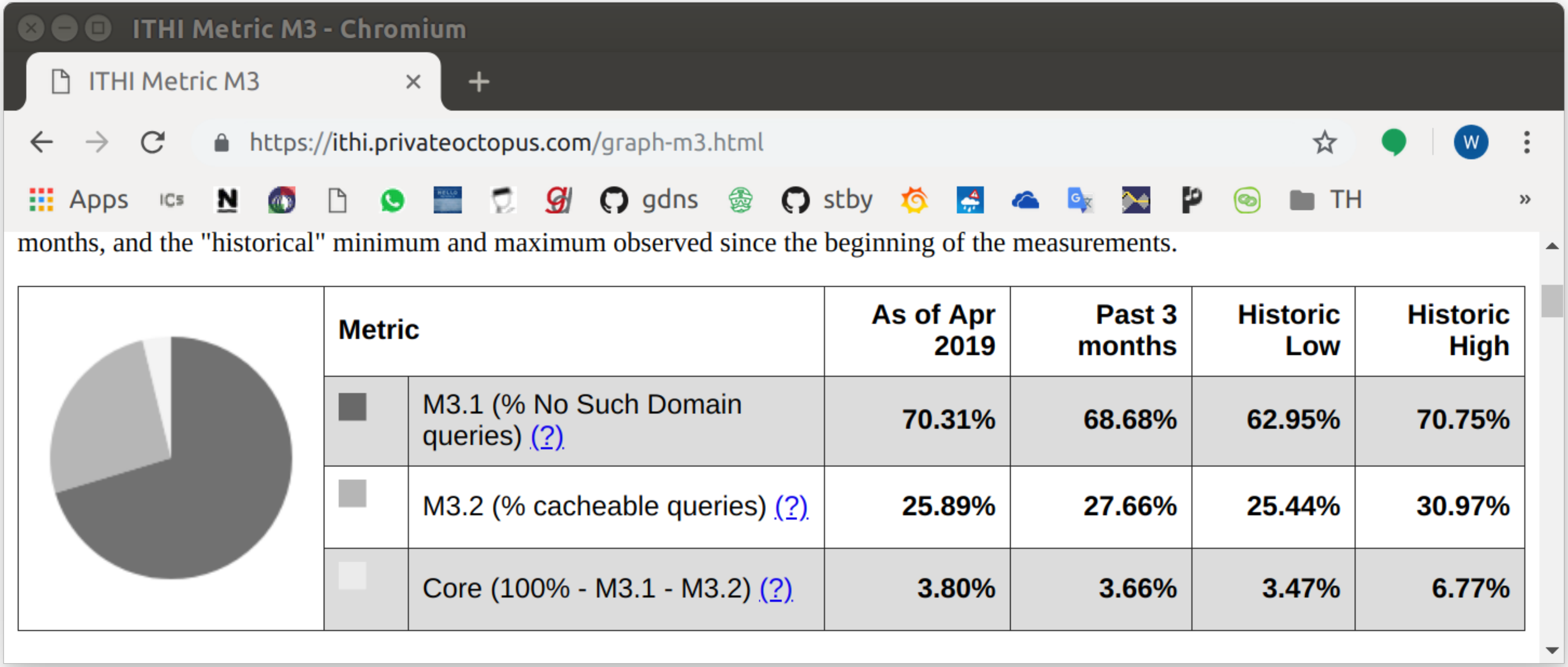
- RFC8198 - Aggressive NSEC



```
$ dig @k.root-servers.net snow. +norec +dnssec

;; ->>HEADER<<- opcode: QUERY, rcode: NXDOMAIN, id:
;; flags: qr aa ; QUERY: 1, ANSWER: 0, AUTHORITY: 6
;; QUESTION SECTION:
;; snow. IN   A

;; AUTHORITY SECTION:
sncf.    86400 IN NSEC so. NS DS RRSIG NSEC
sncf.    86400 IN RRSIG NSEC 8 1 86400 …

.        86400 IN NSEC aaa. NS SOA RRSIG NSEC DNSKEY
.        86400 IN RRSIG NSEC 8 0 86400 …

;; Query time: 2 msec
```

Privacy issues with DNS

minimize # queries – aggressive NSEC


ITHI Metric M3 - Chromium
ITHI Metric M3
https://ithi.privateoctopus.com/graph-m3.html
Apps
gdns
stby
TH

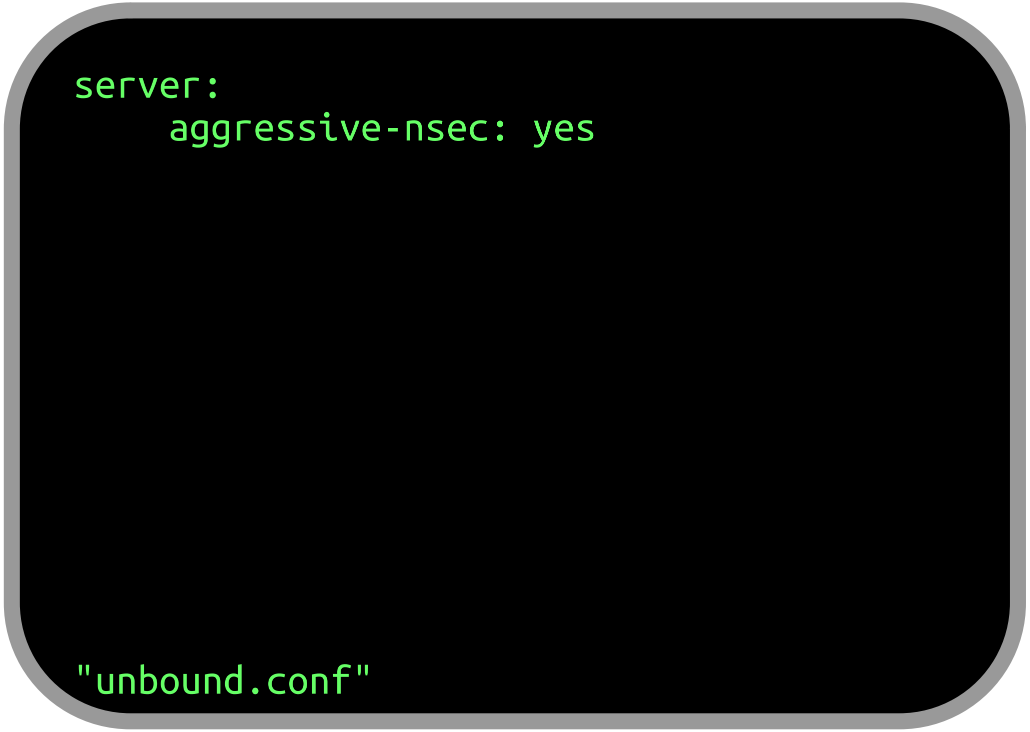
months, and the "historical" minimum and maximum observed since the beginning of the measurements.

	Metric		As of Apr 2019	Past 3 months	Historic Low	Historic High
	■	M3.1 (% No Such Domain queries) (?)	70.31%	68.68%	62.95%	70.75%
	▩	M3.2 (% cacheable queries) (?)	25.89%	27.66%	25.44%	30.97%
	□	Core (100% - M3.1 - M3.2) (?)	3.80%	3.66%	3.47%	6.77%

Privacy issues with DNS

minimize # queries – aggressive NSEC

- RFC8198 - Aggressive NSEC



```
server:
    aggressive-nsec: yes
```

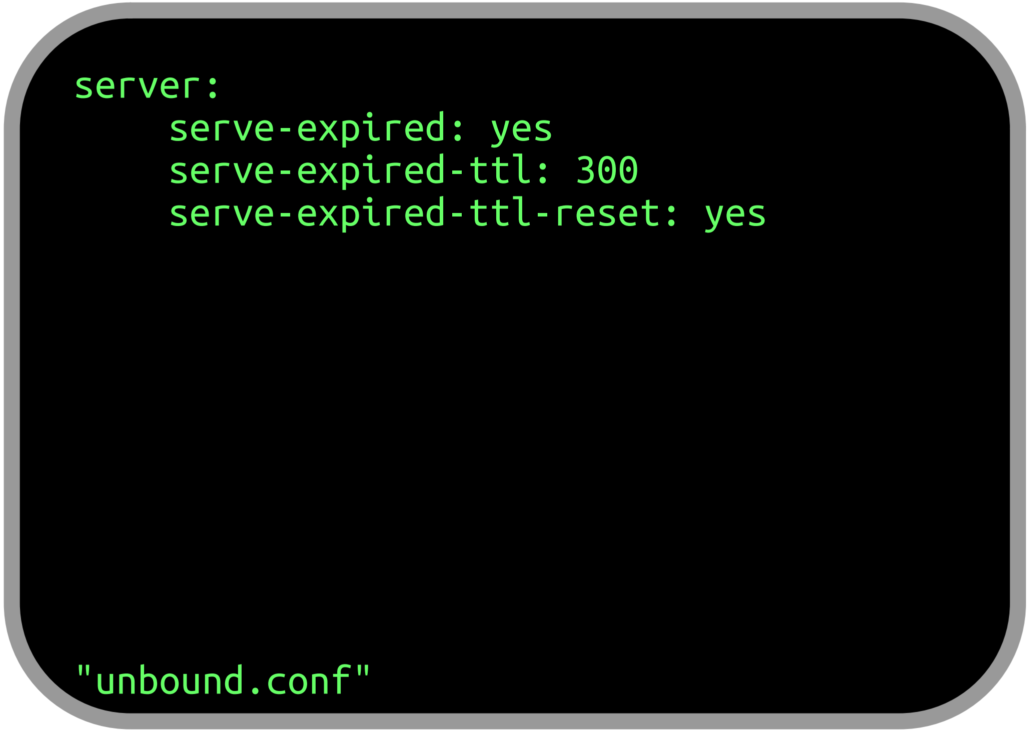
```
"unbound.conf"
```

unbound

Privacy issues with DNS

minimize # queries – serve stale

- RFC8767
- Better Privacy
  and better Performance



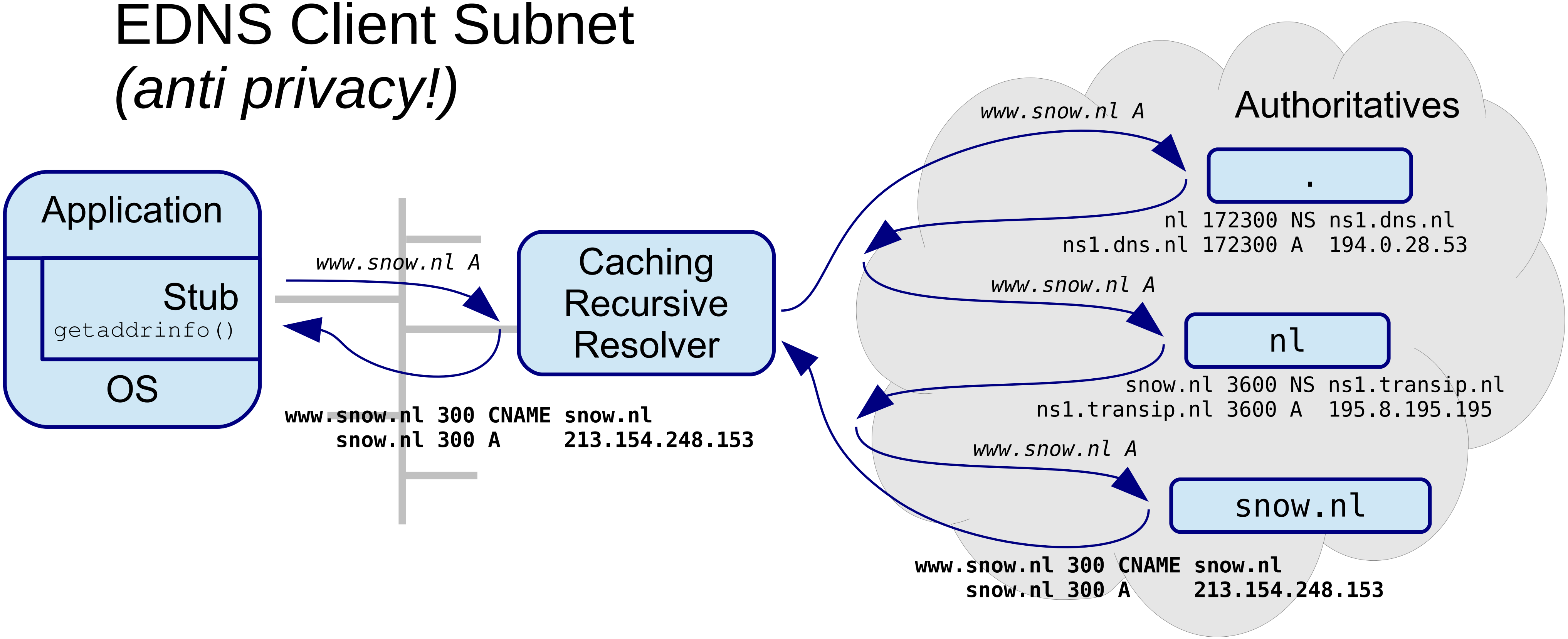
```
server:
     serve-expired: yes
     serve-expired-ttl: 300
     serve-expired-ttl-reset: yes





"unbound.conf"
```

unbound

Privacy issues with DNS

minimize *data* in queries – ECS

- RFC7871 -
  EDNS Client Subnet
  (anti privacy!)



```
www.snow.nl 300 CNAME snow.nl
    snow.nl 300 A     213.154.248.153
```

```
     nl 172300 NS ns1.dns.nl
ns1.dns.nl 172300 A  194.0.28.53
```

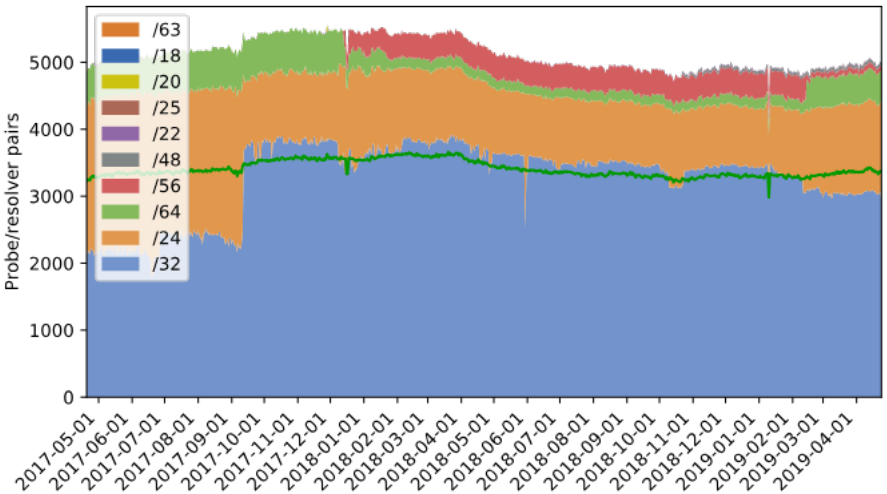
```
     snow.nl 3600 NS ns1.transip.nl
ns1.transip.nl 3600 A  195.8.195.195
```

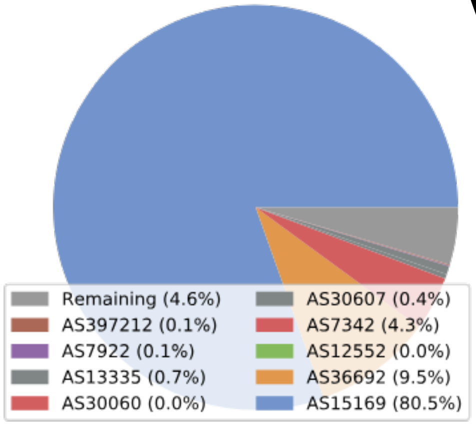
```
www.snow.nl 300 CNAME snow.nl
    snow.nl 300 A     213.154.248.153
```

Privacy issues with DNS

minimize data in queries – ECS

- RFC7871 -
  EDNS Client Subnet
  (anti privacy!)





DNSThought

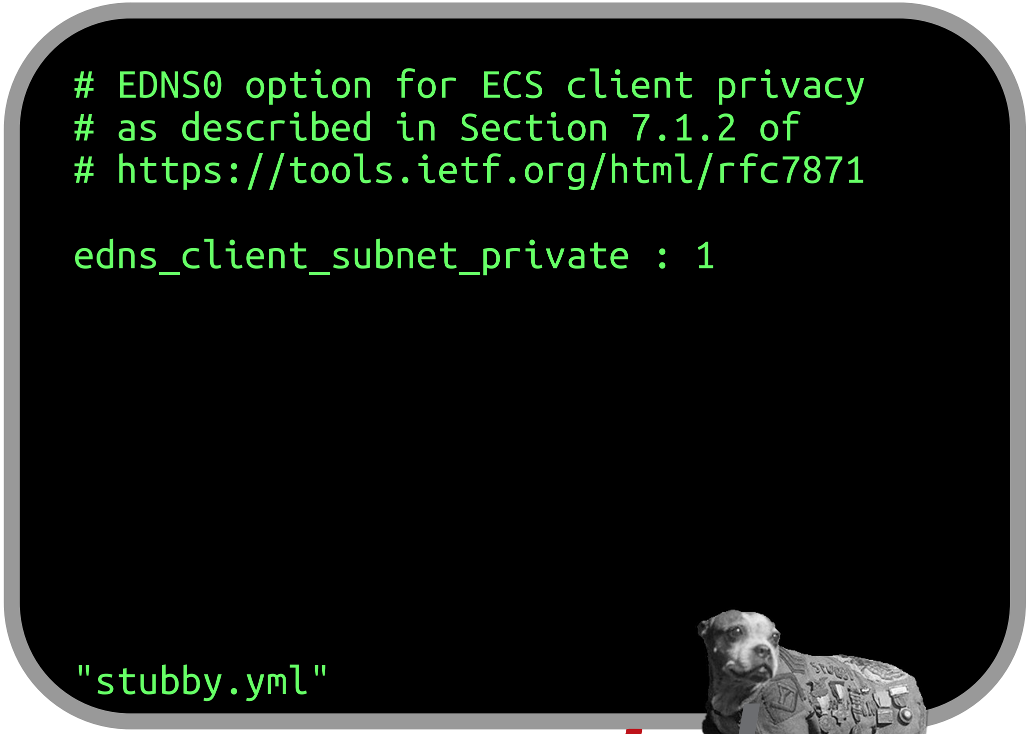
Privacy issues with DNS

minimize *data* in queries – ECS priv.

- RFC7871 - EDNS Client Subnet sectie 7.1.2:

  “ A SOURCE PREFIX-LENGTH value of 0 means that the Recursive Resolver MUST NOT add the client's address information to its queries. ”

- unbound respects this
- Google respects this
- OpenDNS does not



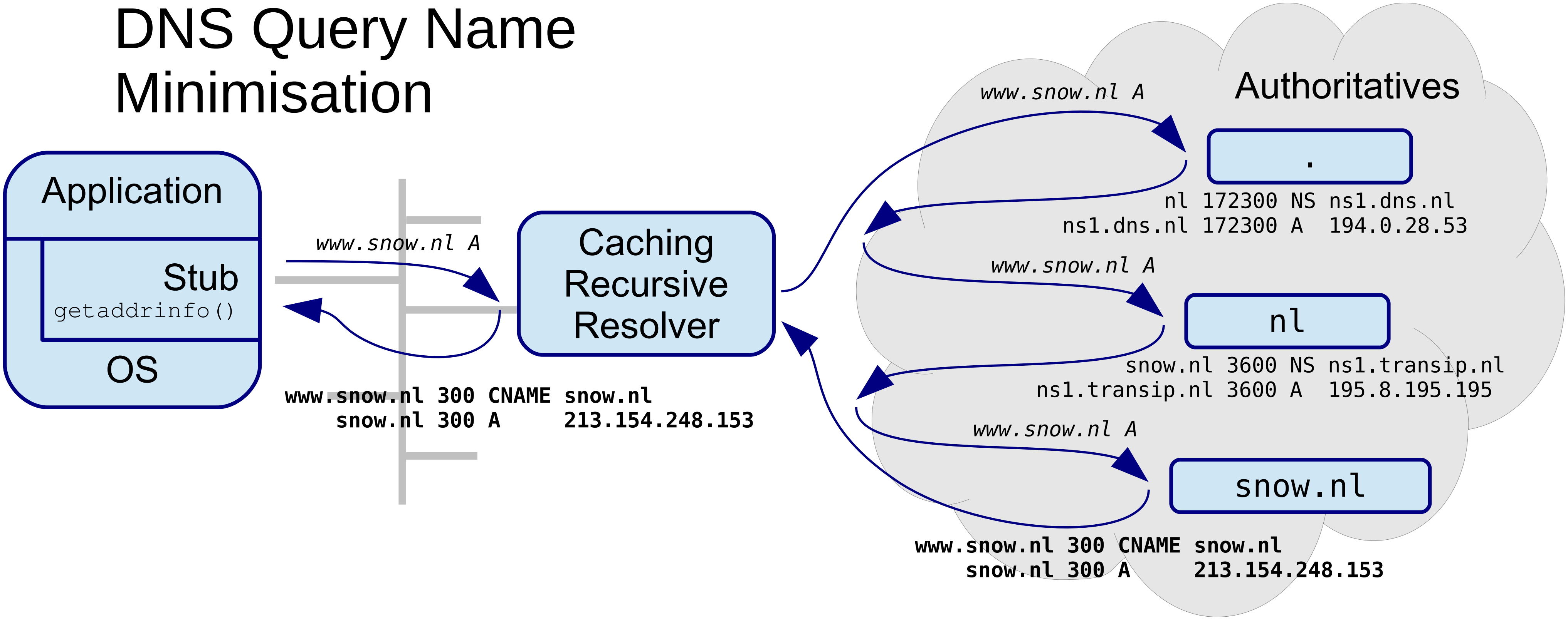
```
# EDNS0 option for ECS client privacy
# as described in Section 7.1.2 of
# https://tools.ietf.org/html/rfc7871

edns_client_subnet_private : 1
```

"stubby.yml"

Privacy issues with DNS

minimize data in queries – qname min

- Without RFC7816bis - DNS Query Name Minimisation



```
         nl 172300 NS ns1.dns.nl
 ns1.dns.nl 172300 A  194.0.28.53
```

```
       snow.nl 3600 NS ns1.transip.nl
ns1.transip.nl 3600 A  195.8.195.195
```

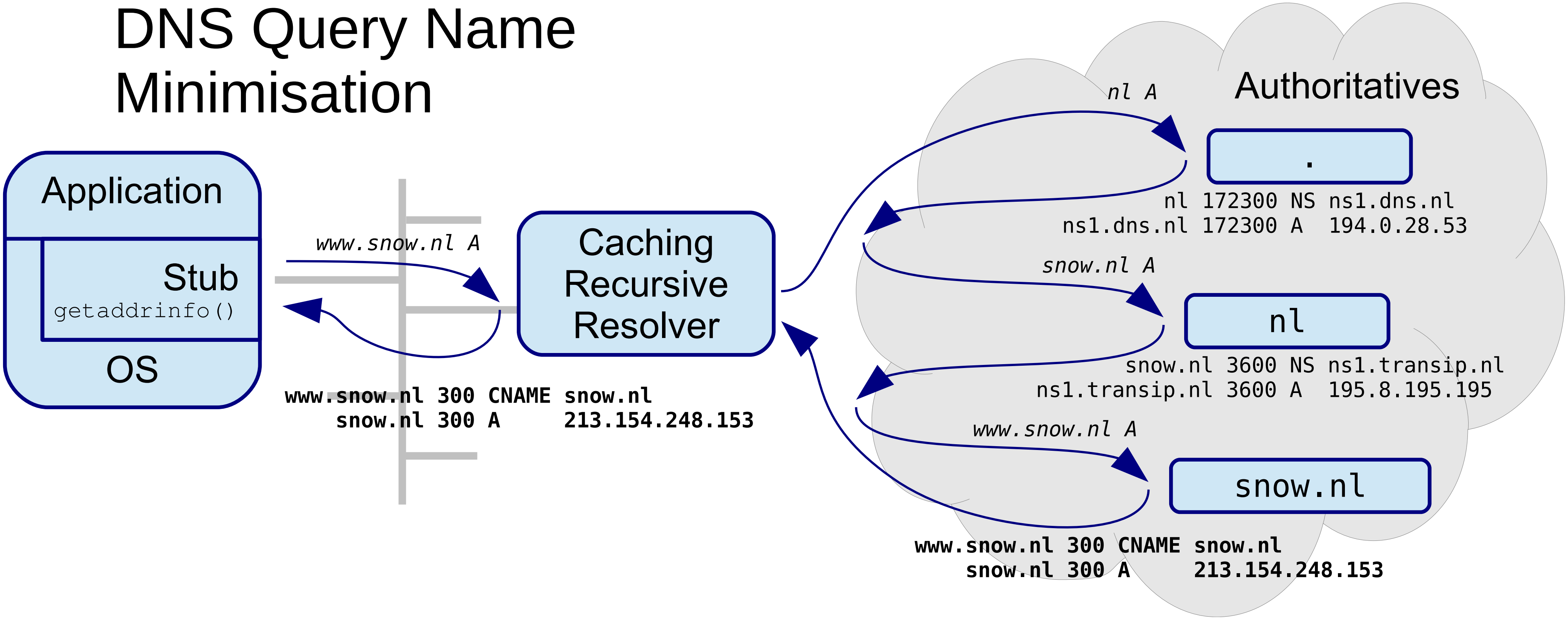
```
www.snow.nl 300 CNAME snow.nl
    snow.nl 300 A     213.154.248.153
```

```
www.snow.nl 300 CNAME snow.nl
    snow.nl 300 A     213.154.248.153
```

Privacy issues with DNS

minimize data in queries – qname min

- With RFC7816bis - DNS Query Name Minimisation


Authoritatives
Application
Stub
getaddrinfo()
OS
www.snow.nl A
Caching Recursive Resolver
nl A
.
nl 172300 NS ns1.dns.nl
ns1.dns.nl 172300 A 194.0.28.53
snow.nl A
nl
snow.nl 3600 NS ns1.transip.nl
ns1.transip.nl 3600 A 195.8.195.195
www.snow.nl A
snow.nl

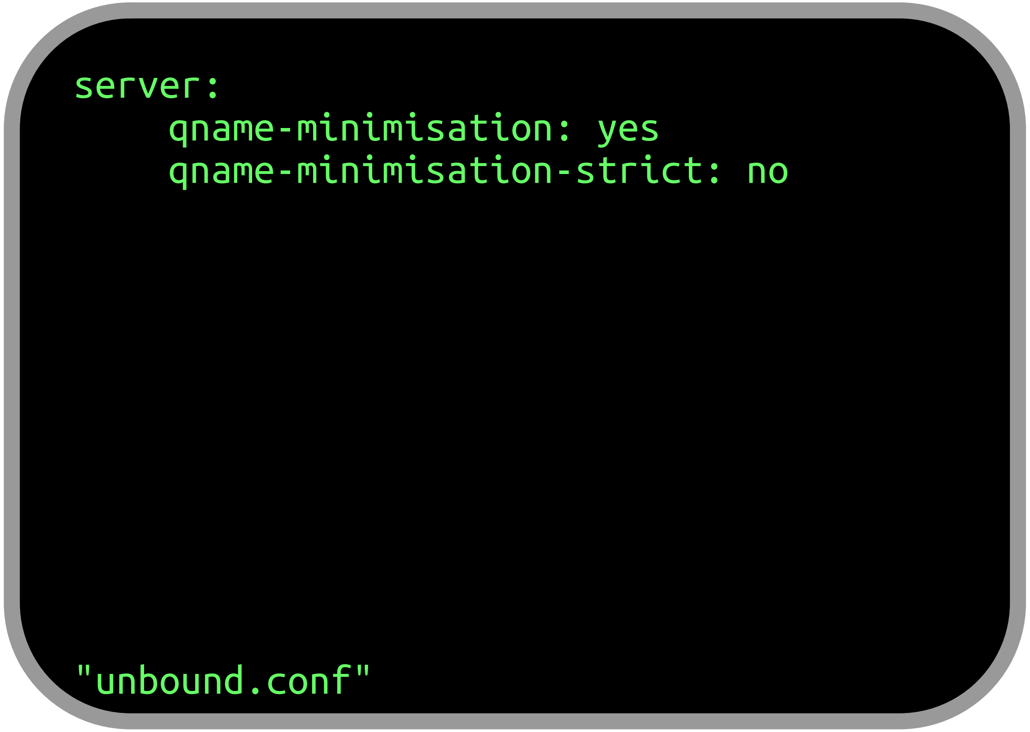
```
www.snow.nl 300 CNAME snow.nl
    snow.nl 300 A     213.154.248.153
```

```
www.snow.nl 300 CNAME snow.nl
    snow.nl 300 A     213.154.248.153
```

Privacy issues with DNS

minimize data in queries – qname min

- RFC7816bis - DNS Query Name Minimisation



```
server:
    qname-minimisation: yes
    qname-minimisation-strict: no
```

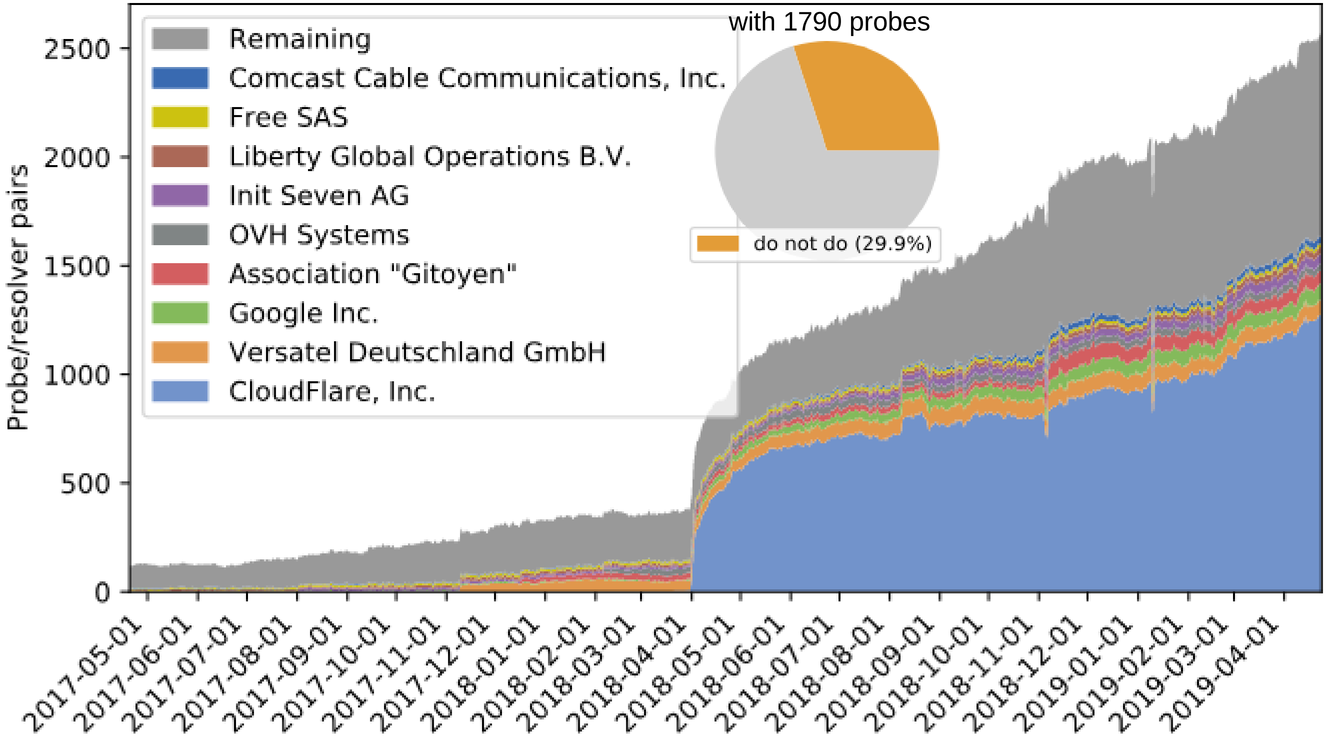
"unbound.conf"

unbound

Privacy issues with DNS

minimize data in queries – qname min

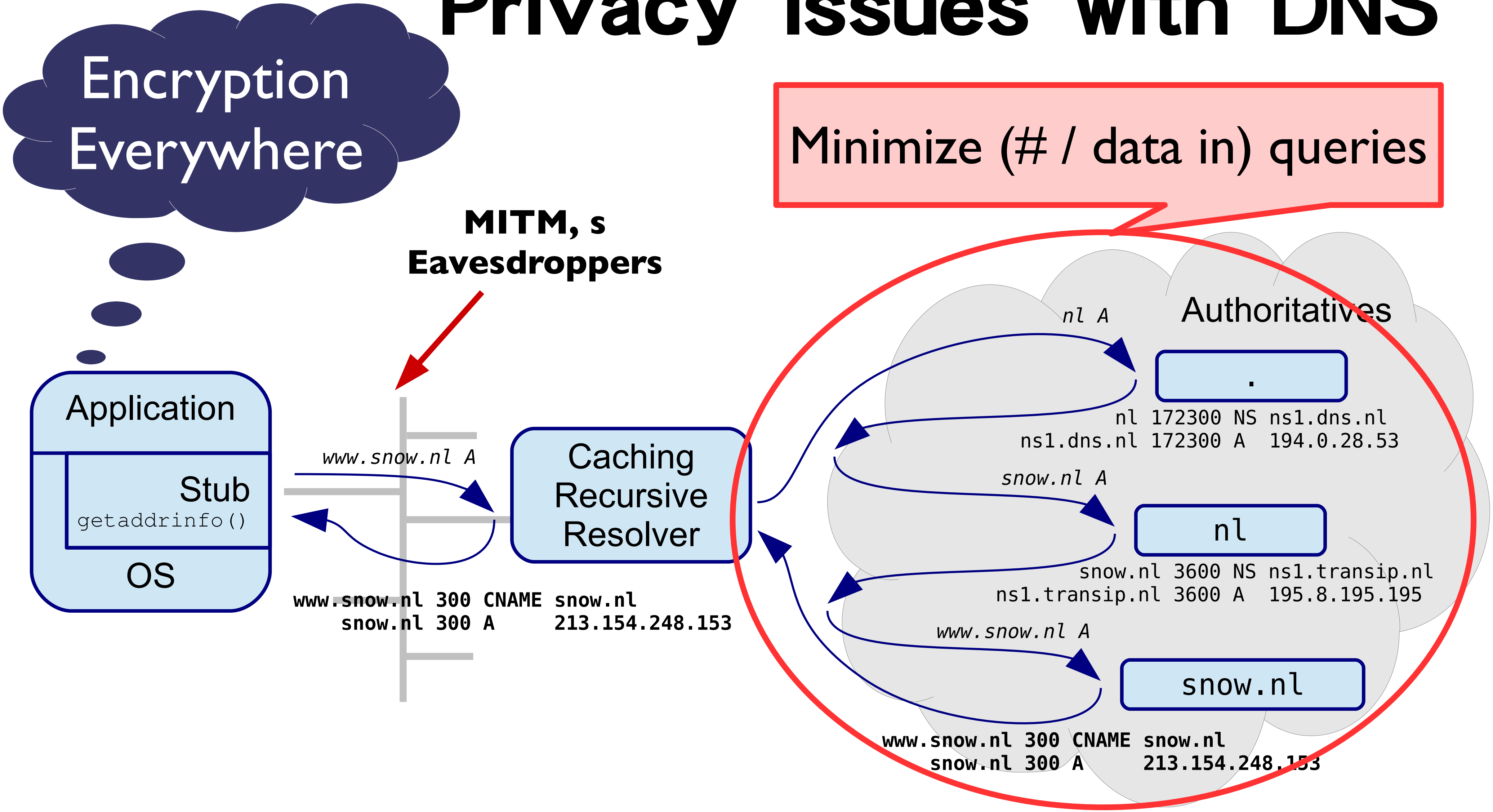
- RFC7816bis - DNS Query Name Minimisation



DNSThought

ITHI: 35% measured on the root

Privacy issues with DNS



Encryption Everywhere

Minimize (# / data in) queries

MITM, s Eavesdroppers

Application

Stub
getaddrinfo()

OS

www.snow.nl A

Caching Recursive Resolver

```
www.snow.nl 300 CNAME snow.nl
    snow.nl 300 A     213.154.248.153
```

Authoritatives

nl A

.

```
         nl 172300 NS ns1.dns.nl
ns1.dns.nl 172300 A  194.0.28.53
```

snow.nl A

nl

```
     snow.nl 3600 NS ns1.transip.nl
ns1.transip.nl 3600 A  195.8.195.195
```

www.snow.nl A

snow.nl

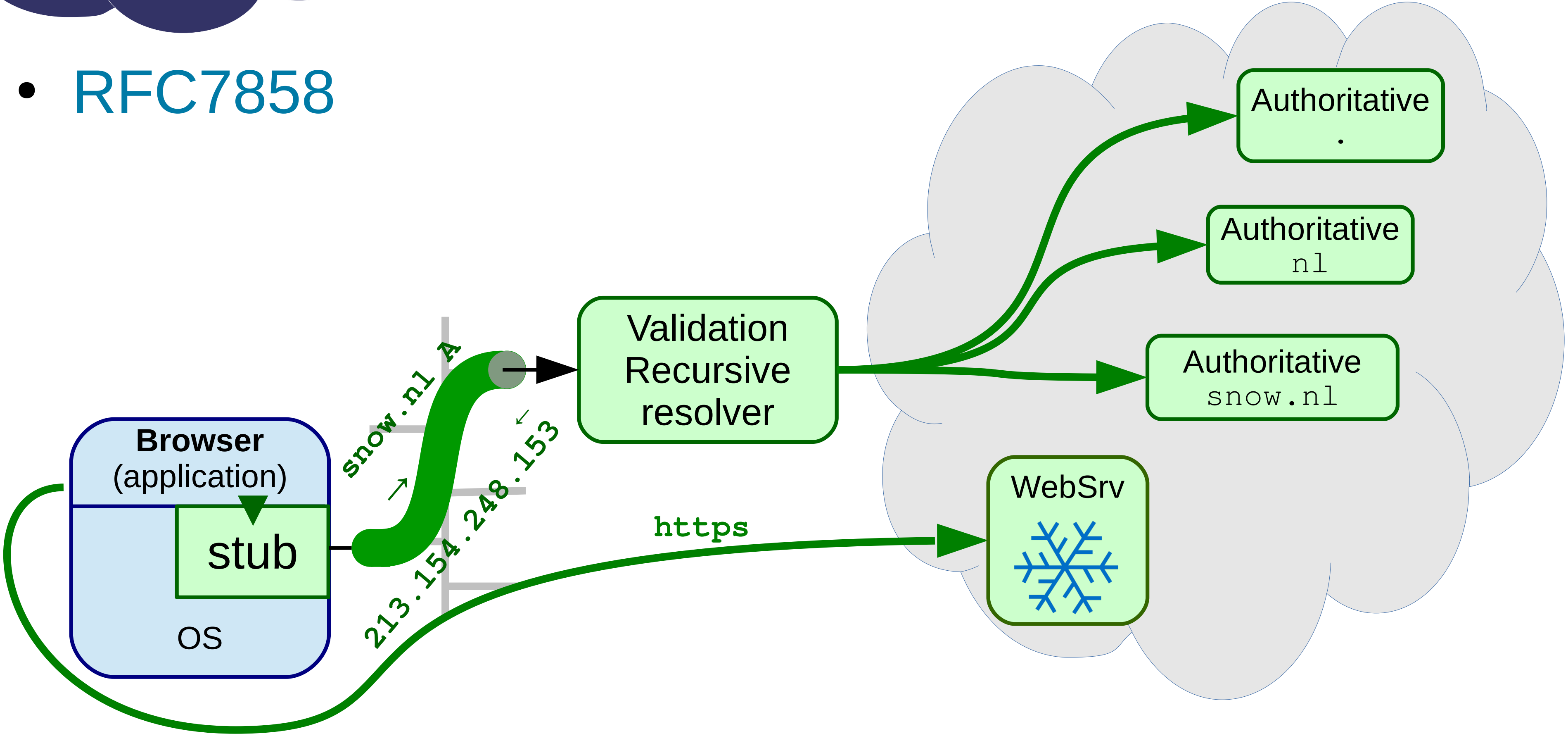
```
www.snow.nl 300 CNAME snow.nl
    snow.nl 300 A     213.154.248.153
```

Encryption Everywhere

Privacy issues with DNS

DNS over TLS (DoT)

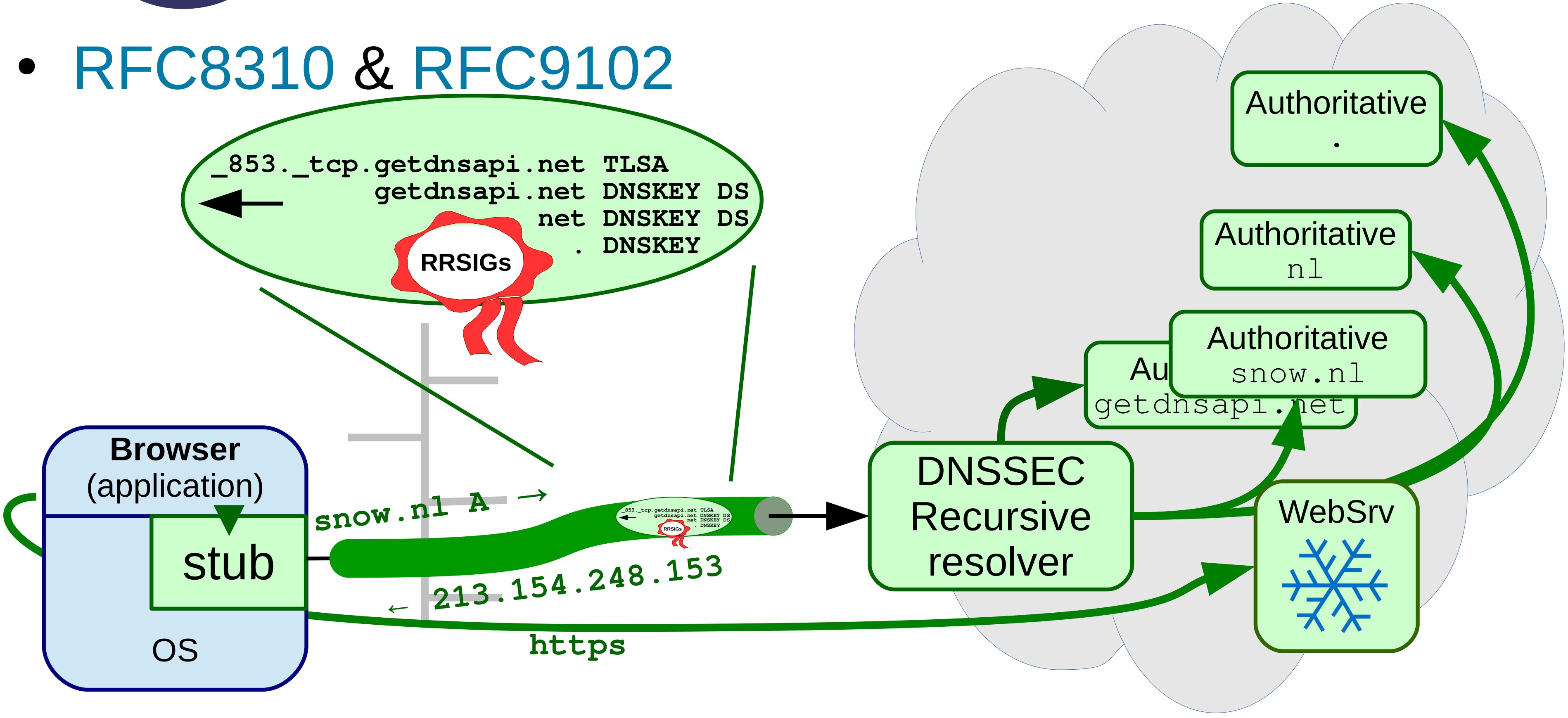
- RFC7858



Encryption Everywhere

Privacy issues with DNS
DNS over TLS (DoT)

- RFC8310 & RFC9102



Encryption Everywhere

Privacy issues with DNS

DNS over TLS (DoT)

```
server:
    tls-service-key: "privkey.pem"
    tls-service-pem: "fullchain.pem"
    tls-port: 853
```

"unbound.conf"

```
round_robin_upstreams: 1

upstream_recursive_servers:
## Quad 9
  - address_data: 9.9.9.9
    tls_auth_name: "dns.quad9.net"
## Cloudflare
  - address_data: 1.1.1.1
    tls_auth_name: "cloudflare-dns.com"
## Google
  - address_data: 8.8.8.8
   tls_auth_name: "dns.google"
```

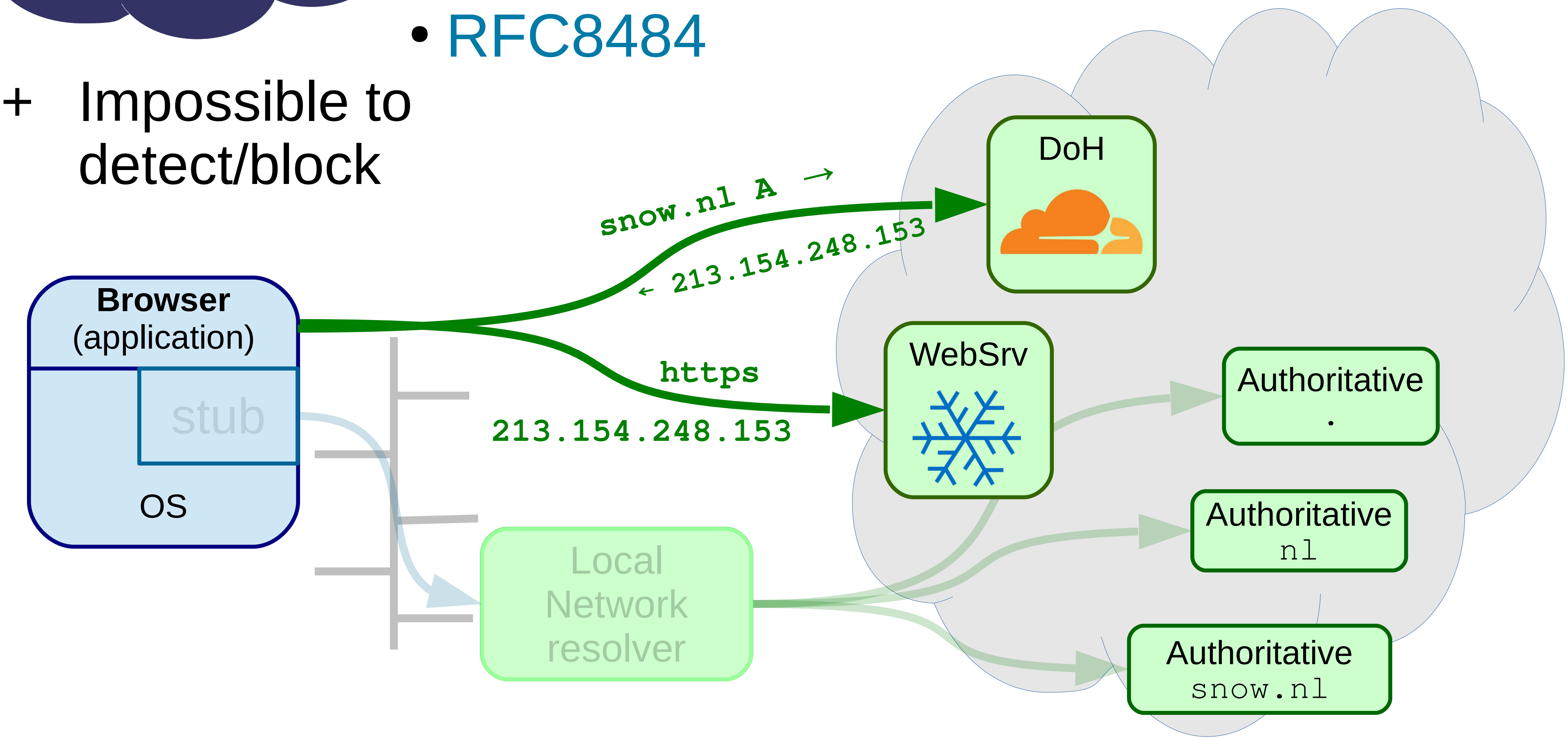
"stubby.yml"

unbound

getdns

Privacy issues with DNS
DNS over HTTPS (DoH)

- RFC8484
- + Impossible to detect/block



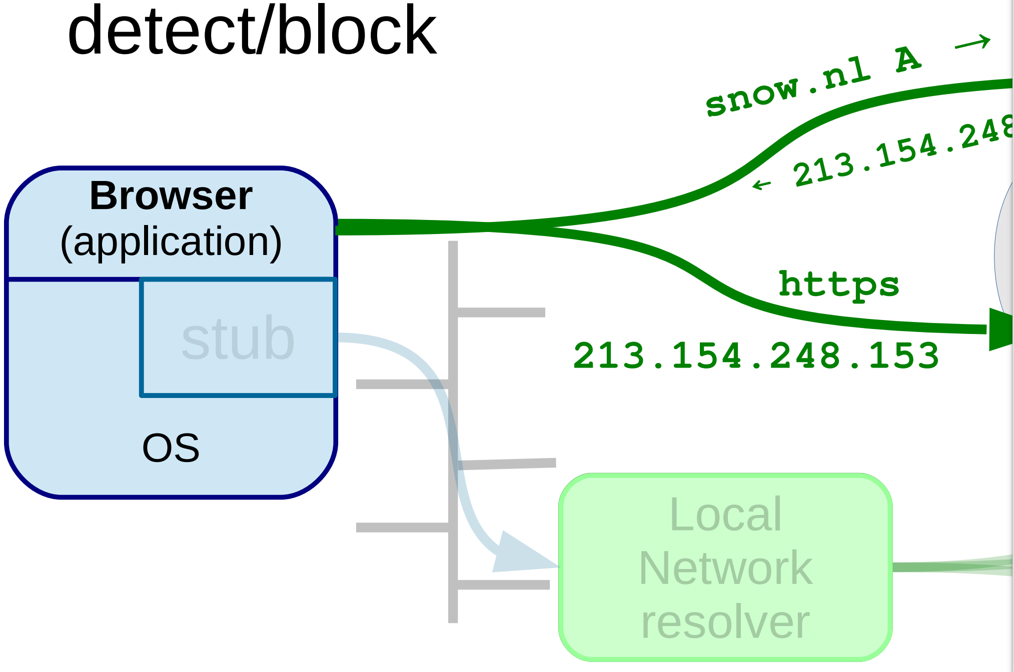
Encryption Everywhere

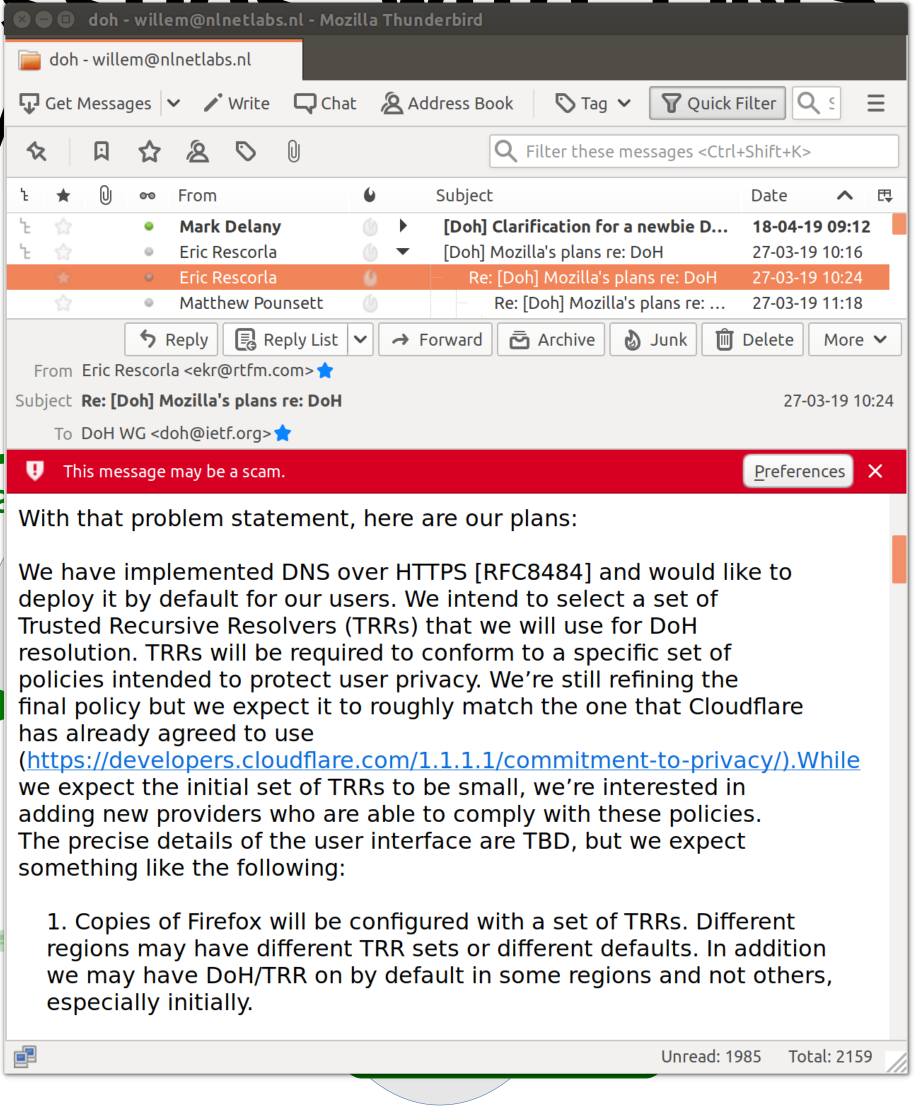
Privacy issues with DNS

DNS ov

- RFC8484

- + Impossible to detect/block





From	Subject	Date
Mark Delany	[Doh] Clarification for a newbie D...	18-04-19 09:12
Eric Rescorla	[Doh] Mozilla's plans re: DoH	27-03-19 10:16
Eric Rescorla	Re: [Doh] Mozilla's plans re: DoH	27-03-19 10:24
Matthew Pounsett	Re: [Doh] Mozilla's plans re: ...	27-03-19 11:18

From Eric Rescorla <ekr@rtfm.com>
Subject **Re: [Doh] Mozilla's plans re: DoH** 27-03-19 10:24
To DoH WG <doh@ietf.org>

This message may be a scam.

With that problem statement, here are our plans:

We have implemented DNS over HTTPS [RFC8484] and would like to deploy it by default for our users. We intend to select a set of Trusted Recursive Resolvers (TRRs) that we will use for DoH resolution. TRRs will be required to conform to a specific set of policies intended to protect user privacy. We’re still refining the final policy but we expect it to roughly match the one that Cloudflare has already agreed to use (https://developers.cloudflare.com/1.1.1.1/commitment-to-privacy/).While we expect the initial set of TRRs to be small, we’re interested in adding new providers who are able to comply with these policies. The precise details of the user interface are TBD, but we expect something like the following:

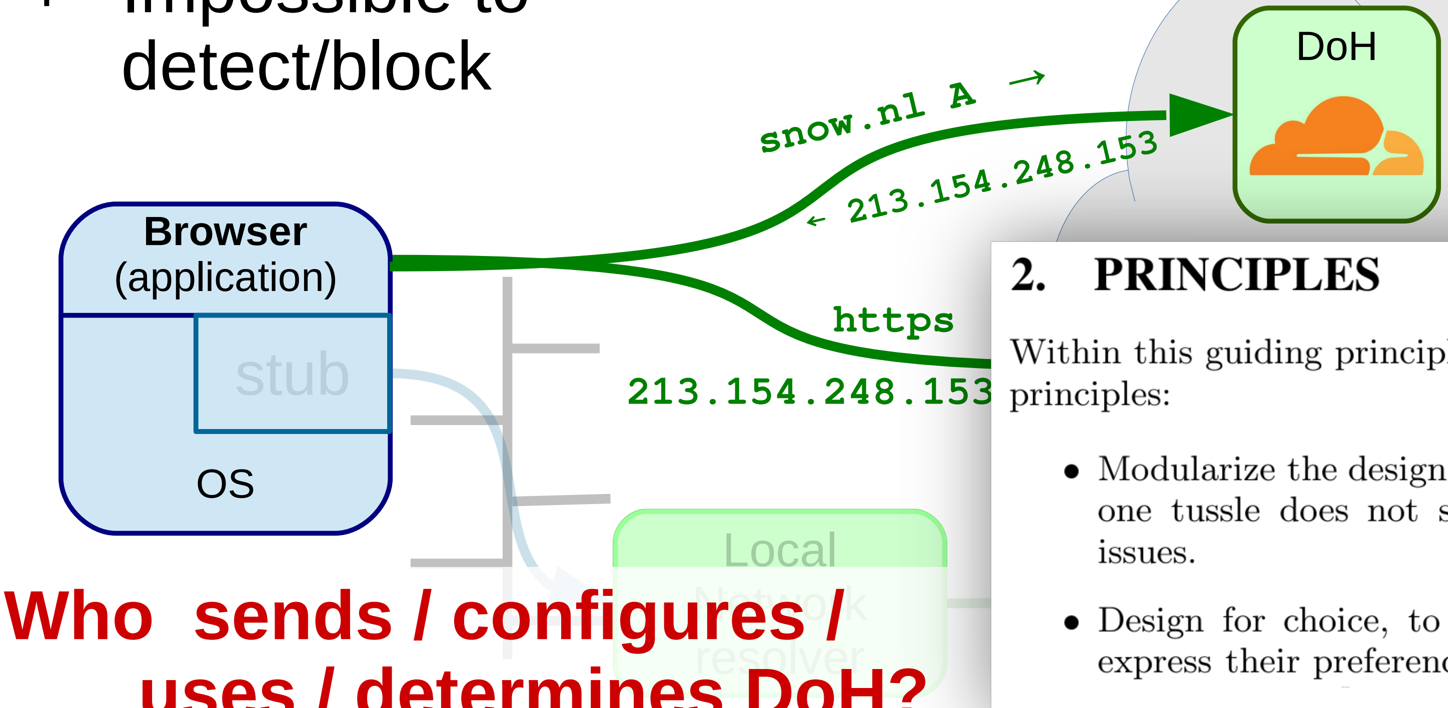
1. Copies of Firefox will be configured with a set of TRRs. Different regions may have different TRR sets or different defaults. In addition we may have DoH/TRR on by default in some regions and not others, especially initially.

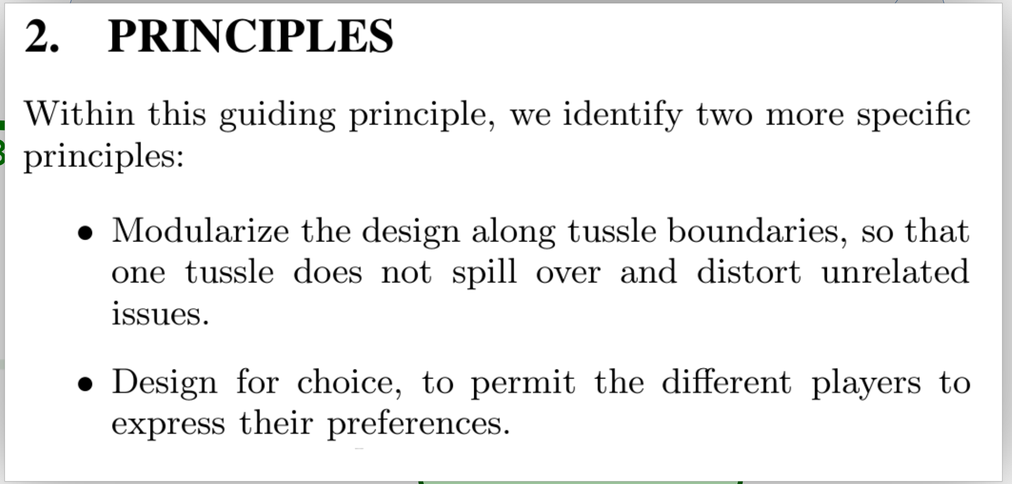
Encryption Everywhere

Privacy issues with DNS

DNS over HTTPS (DoH)

- RFC8484
- + Impossible to detect/block





2. PRINCIPLES

Within this guiding principle, we identify two more specific principles:

- Modularize the design along tussle boundaries, so that one tussle does not spill over and distort unrelated issues.
- Design for choice, to permit the different players to express their preferences.

- **Who sends / configures / uses / determines DoH?**

Encryption Everywhere

Privacy issues with DNS
DNS over HTTPS (DoH)

- RFC8484 - DNS over HTTPS (DoH)
- How to configure DoH in your browser

```
server:
     https-port: 443
     http-endpoint: “/dns-query”

     http-max-streams: 100
     http-query-buffer-size: 4m
     http-response-buffer-size: 4m
     http-nodelay: yes

     # Disable use of TLS for the downstream
     # DNS-over-HTTP connections. Useful for
     # local back end servers. Default is no
     #
     http-notls-downstream: no
```

unbound

Lab time!

- Hands on: https://dnslab.uk/
- 6. DNS Privacy lab

Photo by Alex Kondratiev on Unsplash