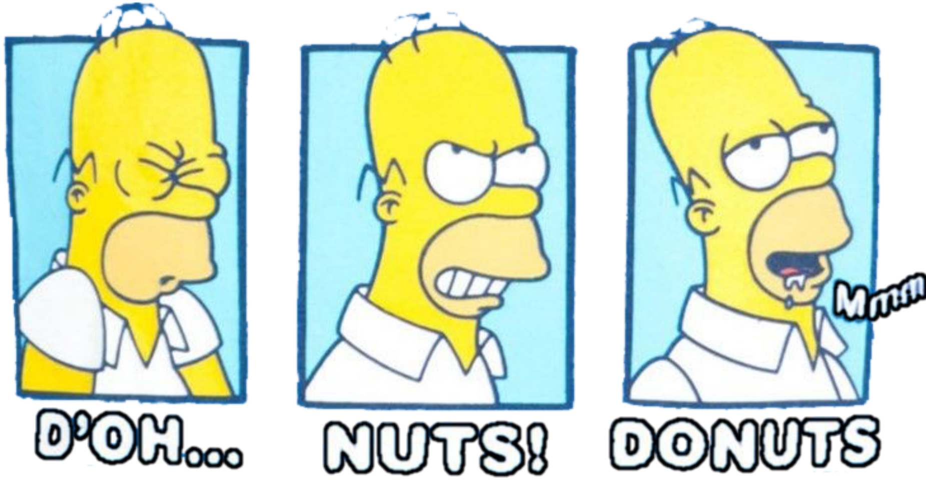
Measuring DNS and DoH



HACKATHON TRACK

AT THE
AFRICA
INTERNET
SUMMIT'19
KAMPALA – UGANDA
19 & 20 JUNE 2019

CHAMPIONS:

Willem Toorop
NLNETLABS

Jasper den Hertog
RIPE NCC
RIPE NETWORK COORDINATION CENTRE

Who are we?

- **Willem Toorop**
- Developer @ NLNETLABS
- Loves doing Hackathons
- Internet measurements with RIPE Atlas

Who are we?

- **Jasper den Hertog**
- Developer @ RIPE NCC RIPE NETWORK COORDINATION CENTRE
- Loves doing Hackathons
- Internet measurements with RIPE Atlas

What is/What does NLNETLABS

- Objective:
  - *To develop* ***Open Source Software*** *and* ***Open Standards*** *for the benefit of the Internet,*

NSD

unbound

getdns

OpenDNSSEC

ROUTINATOR

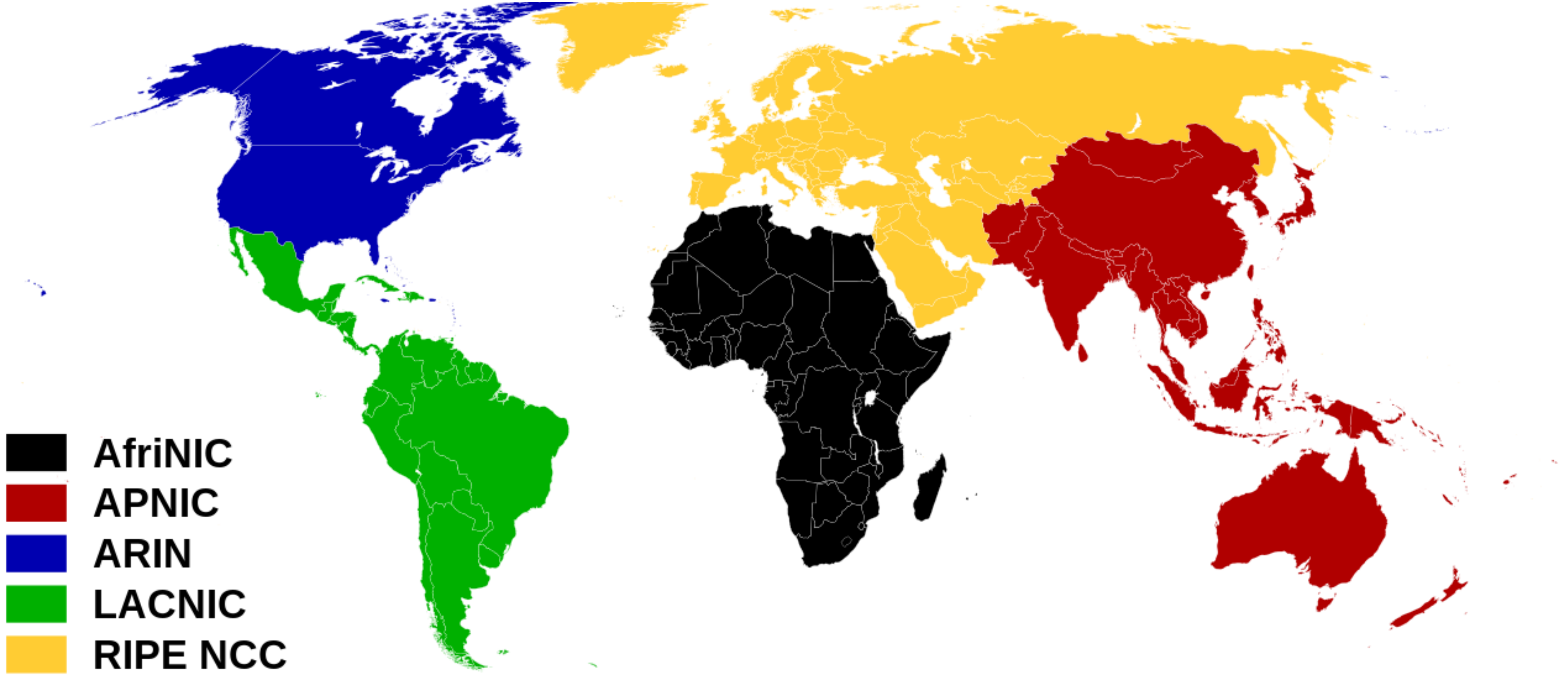
Krill

- ldns
- Net::DNS
- Net::DNS::SEC

What is/What does RIPE NCC

RIPE NETWORK COORDINATION CENTRE

- Regional Internet Registry for Europe, the Middle East and parts of Central Asia

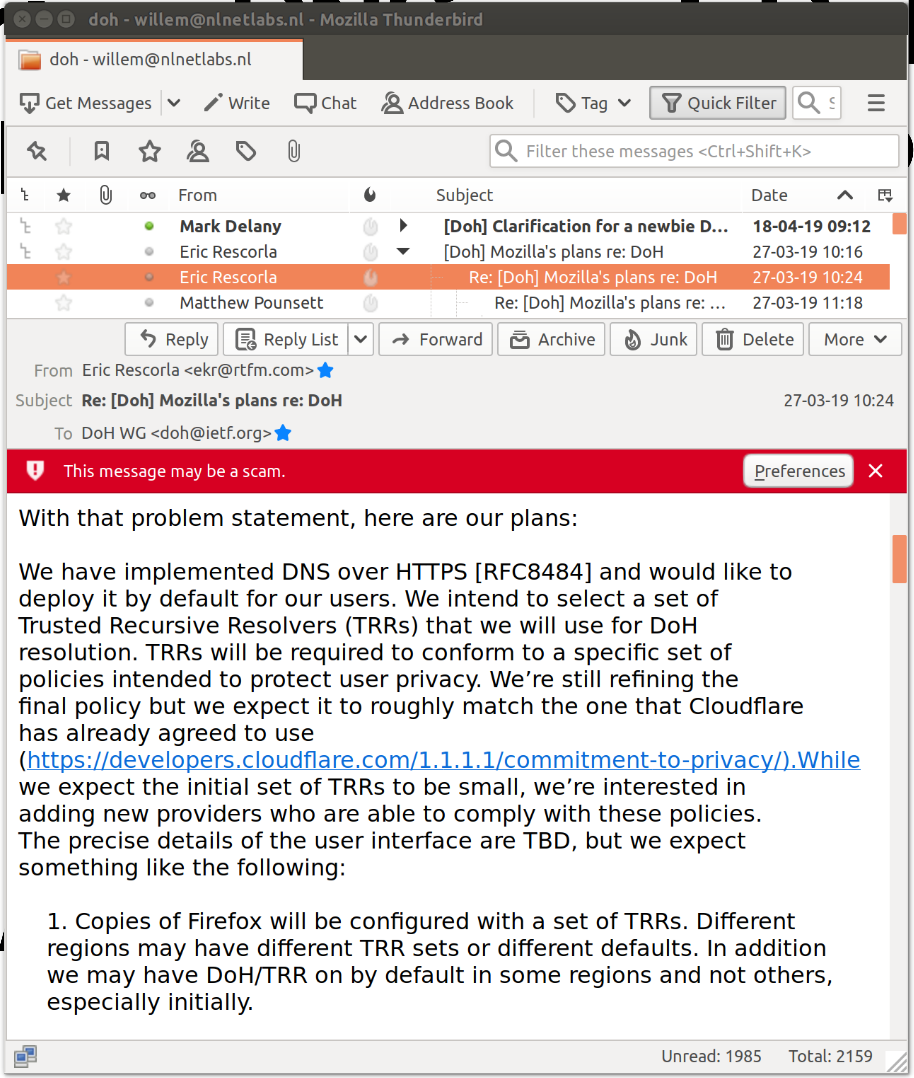


Measuring DNS and DoH
Topics & motivation

- Current trend is DNS resolvers moving to cloud
- 8.8.8.8 9.9.9.9 1.1.1.1
- Not just with the network or user’s consent

Measur… To… …n

- Current trend is DNS res…
- 8.8.8.8 9.9.9.9 1.1.1.1
- Not just with the network…
- *HOW? WHY?*



Privacy

March 2011: I-D
Privacy Considerations for Internet Protocols

June 2013: Snowden Revelations
Morecowbell

July 2013: RFC6973
Privacy Considerations for Internet Protocols

May 2014: RFC7258
Pervasive Monitoring is an Attack

Encryption Everywhere

Ma

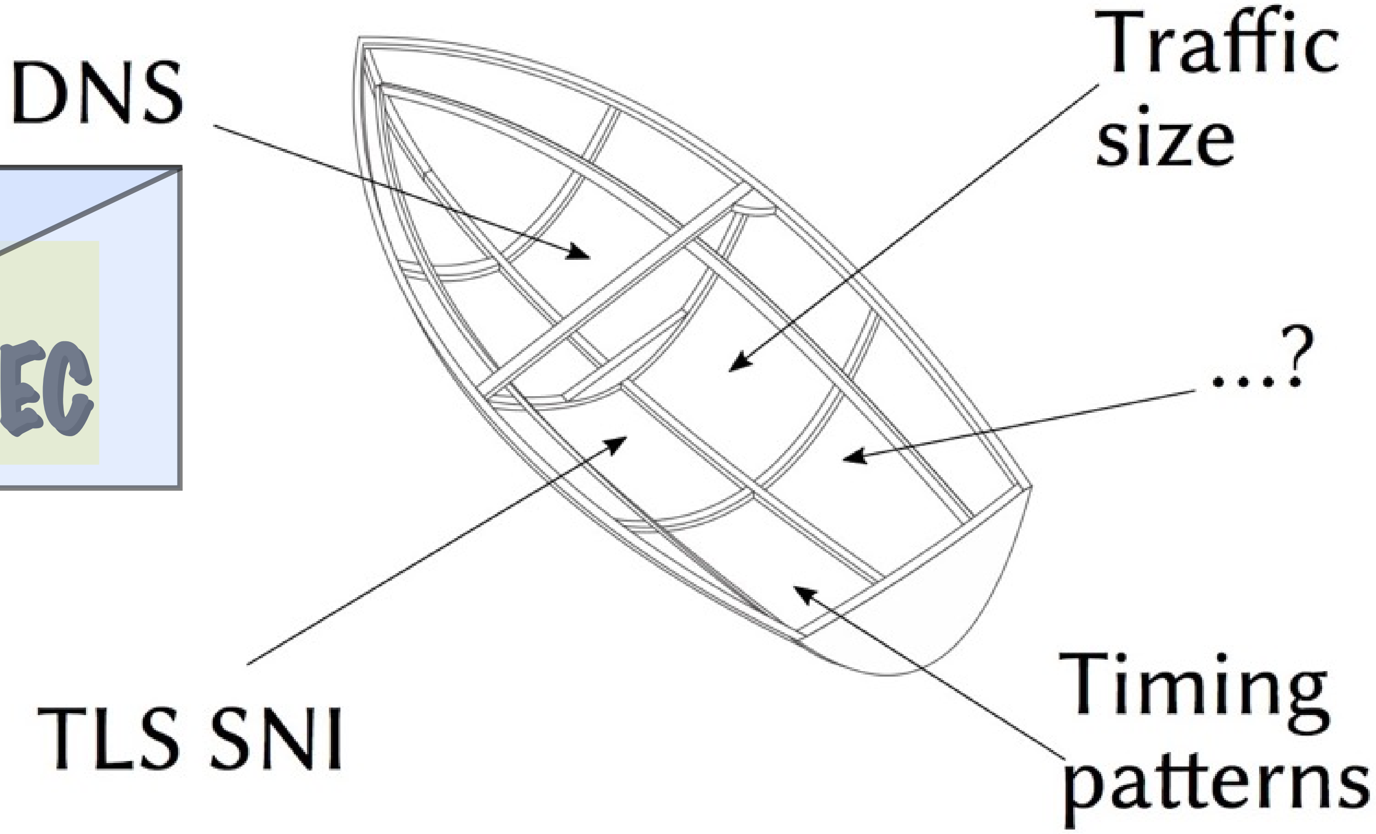
s

June 201 evelations
Morecowbell

July 2013 : RFC6973
Privacy Considerations for Internet Protocols

May 2014: RFC7258
Pervasive Monitoring is an Attack

Privacy



- NSA's Morecowbell on DNS based pervasive monitoring system

ns
cols

May 20
Pervasive Monitoring
is an Attack

May 2016 : RFC7858
DNS-over-TLS (DoT)

October 2018: RFC8484
DNS-over-HTTPS (DoH)

DNS Measurements Hackathon Track
Topics and motivation

- How would centralized cloud provided DNS resolvers impact Internet in the African region?
- Does it have performance implications?
- Does it have other implications? (Political?)
- Is it beneficial and achievable to provide local DoT or DoH resolvers?
- How can this best be achieved/realized?

Measuring DNS and DoH
Topics and motivation

- **Optimal DNS Latency**
  - Compare latency of probes resolvers to cloud resolvers
- **Resolver Jedi**
  - How local are probe resolvers?
    Do they cross country borders?
- **Run your own DoH and/or DoT server**
  - Howto and evaluation of different possibilities
- **DoH with DNS Messages in JSON**
  - Provide DoH which is actually usable for applications

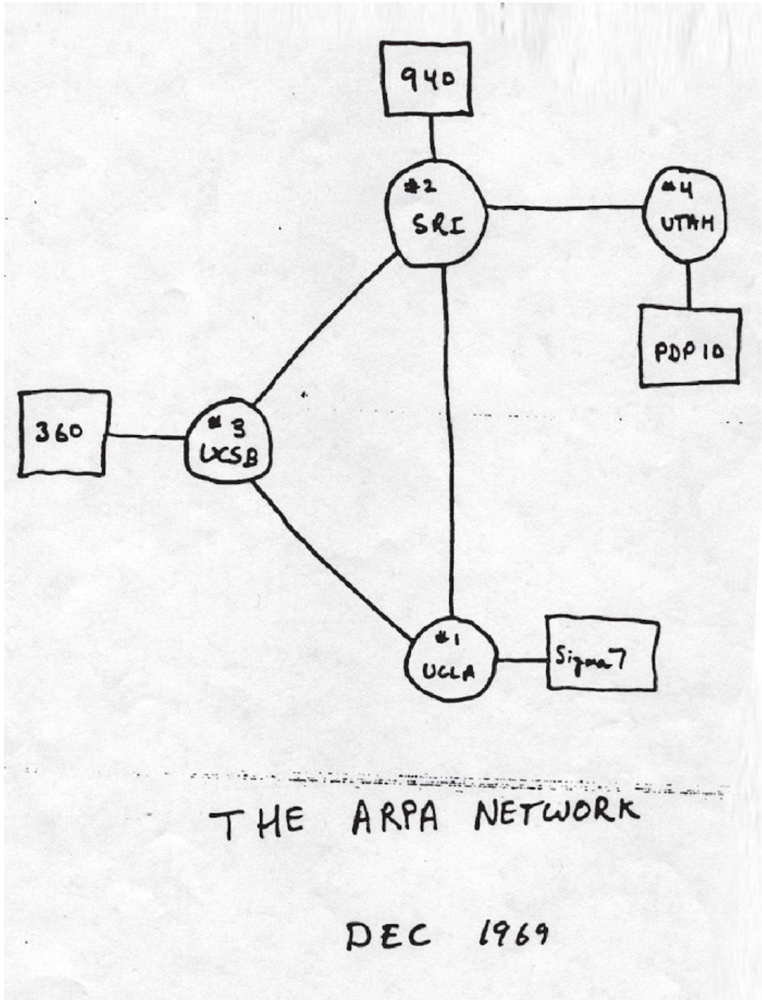
Measuring DNS and DoH Preperation

- A *not so short* introduction to DNS
  - why is it the way it is
  - where did it came from and
  - how did it evolve in response to what

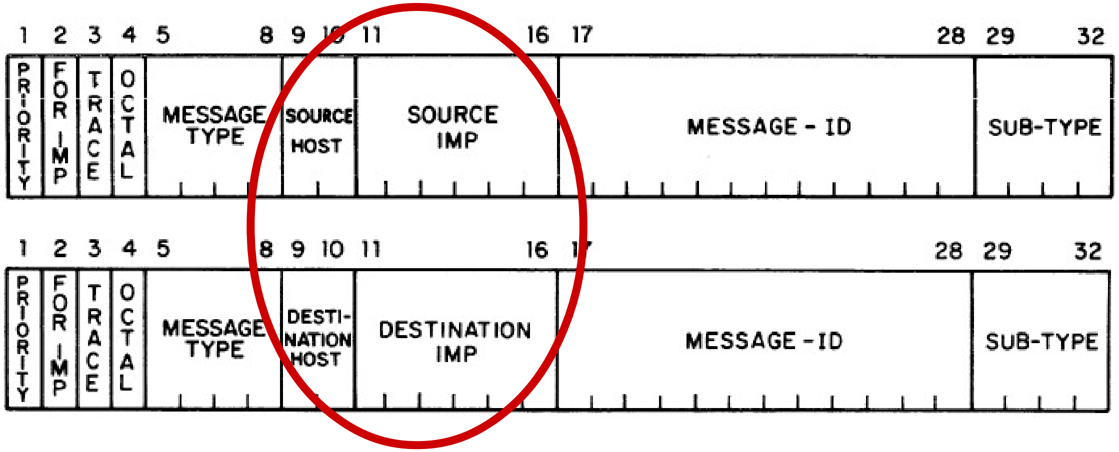
Name Space on the Internet

- Finding IP addresses
  - Start with a domain name (human form)
  - Translating to an IP address (machine form)
- What is the IP address of internetsummit.africa?
  - Client asks server
  - Server responds with answer
  - … case closed?

Name Space on the Internet



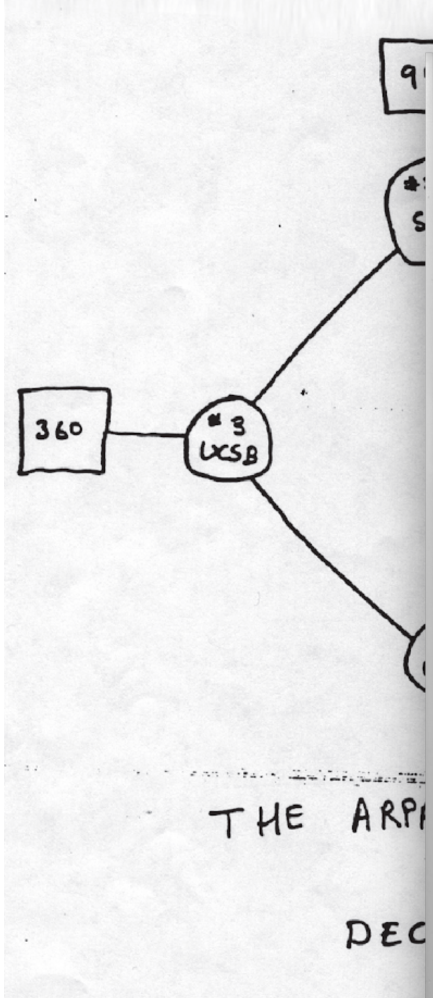
NCP (Network Control Program)

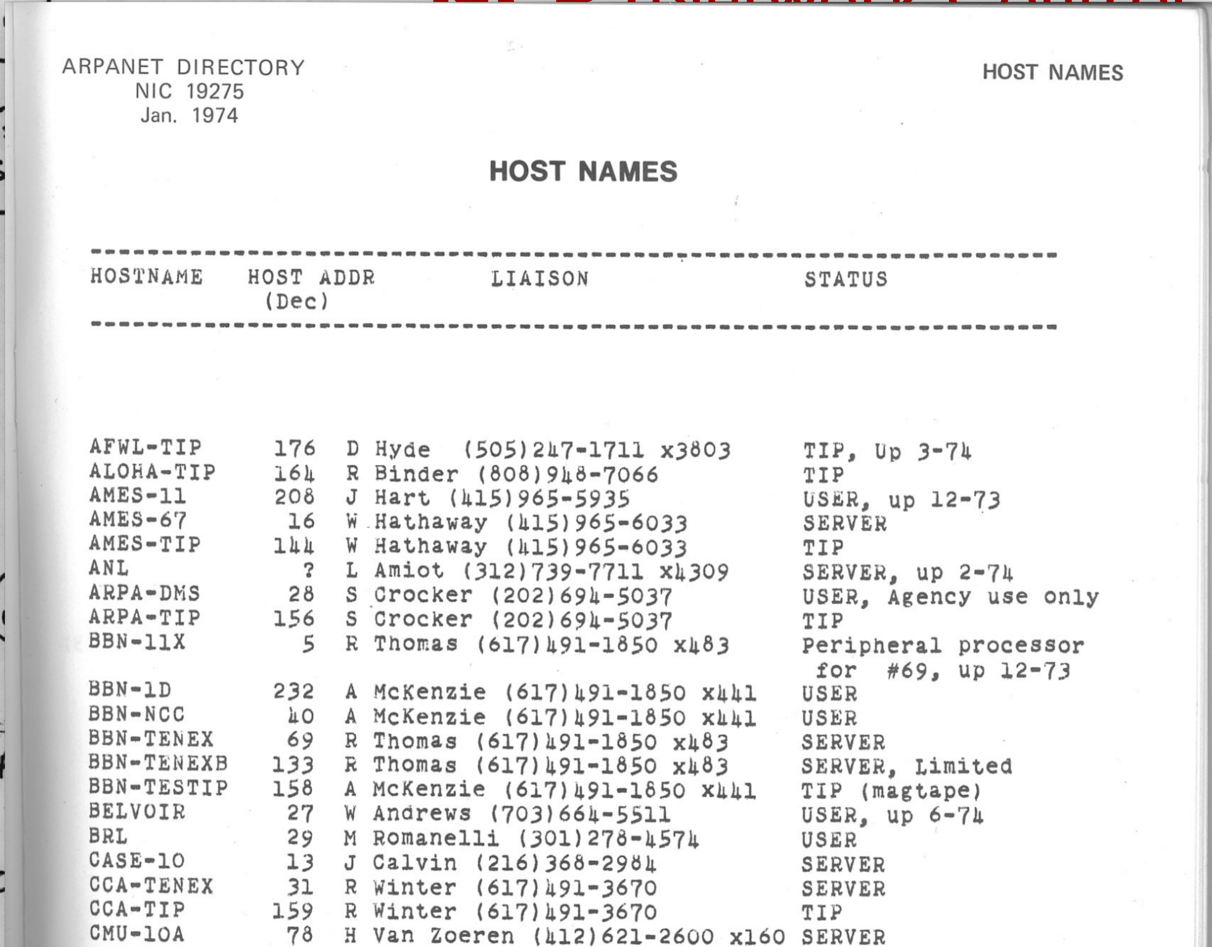


- December 1973 `HOSTS.TXT` (RFC 606)

Namespace on the Internet

NCP (Network Control Program)



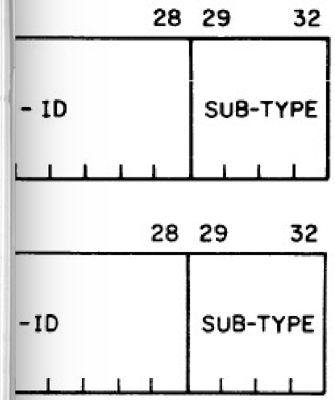


ARPANET DIRECTORY
NIC 19275
Jan. 1974

HOST NAMES

HOST NAMES

HOSTNAME	HOST ADDR (Dec)	LIAISON	STATUS
AFWL-TIP	176	D Hyde (505)247-1711 x3803	TIP, Up 3-74
ALOHA-TIP	164	R Binder (808)948-7066	TIP
AMES-11	208	J Hart (415)965-5935	USER, up 12-73
AMES-67	16	W Hathaway (415)965-6033	SERVER
AMES-TIP	144	W Hathaway (415)965-6033	TIP
ANL	?	L Amiot (312)739-7711 x4309	SERVER, up 2-74
ARPA-DMS	28	S Crocker (202)694-5037	USER, Agency use only
ARPA-TIP	156	S Crocker (202)694-5037	TIP
BBN-11X	5	R Thomas (617)491-1850 x483	Peripheral processor for #69, up 12-73
BBN-1D	232	A McKenzie (617)491-1850 x441	USER
BBN-NCC	40	A McKenzie (617)491-1850 x441	USER
BBN-TENEX	69	R Thomas (617)491-1850 x483	SERVER
BBN-TENEXB	133	R Thomas (617)491-1850 x483	SERVER, Limited
BBN-TESTIP	158	A McKenzie (617)491-1850 x441	TIP (magtape)
BELVOIR	27	W Andrews (703)664-5511	USER, up 6-74
BRL	29	M Romanelli (301)278-4574	USER
CASE-10	13	J Calvin (216)368-2984	SERVER
CCA-TENEX	31	R Winter (617)491-3670	SERVER
CCA-TIP	159	R Winter (617)491-3670	TIP
CMU-10A	78	H Van Zoeren (412)621-2600 x160	SERVER



C 606)

Name Spaces on the Internet

- 1 January 1983 NCP → IP/TCP

  flagday

- max 256 → max 4.294.967.296 hosts
- November 1983 DNS (RFC 882)

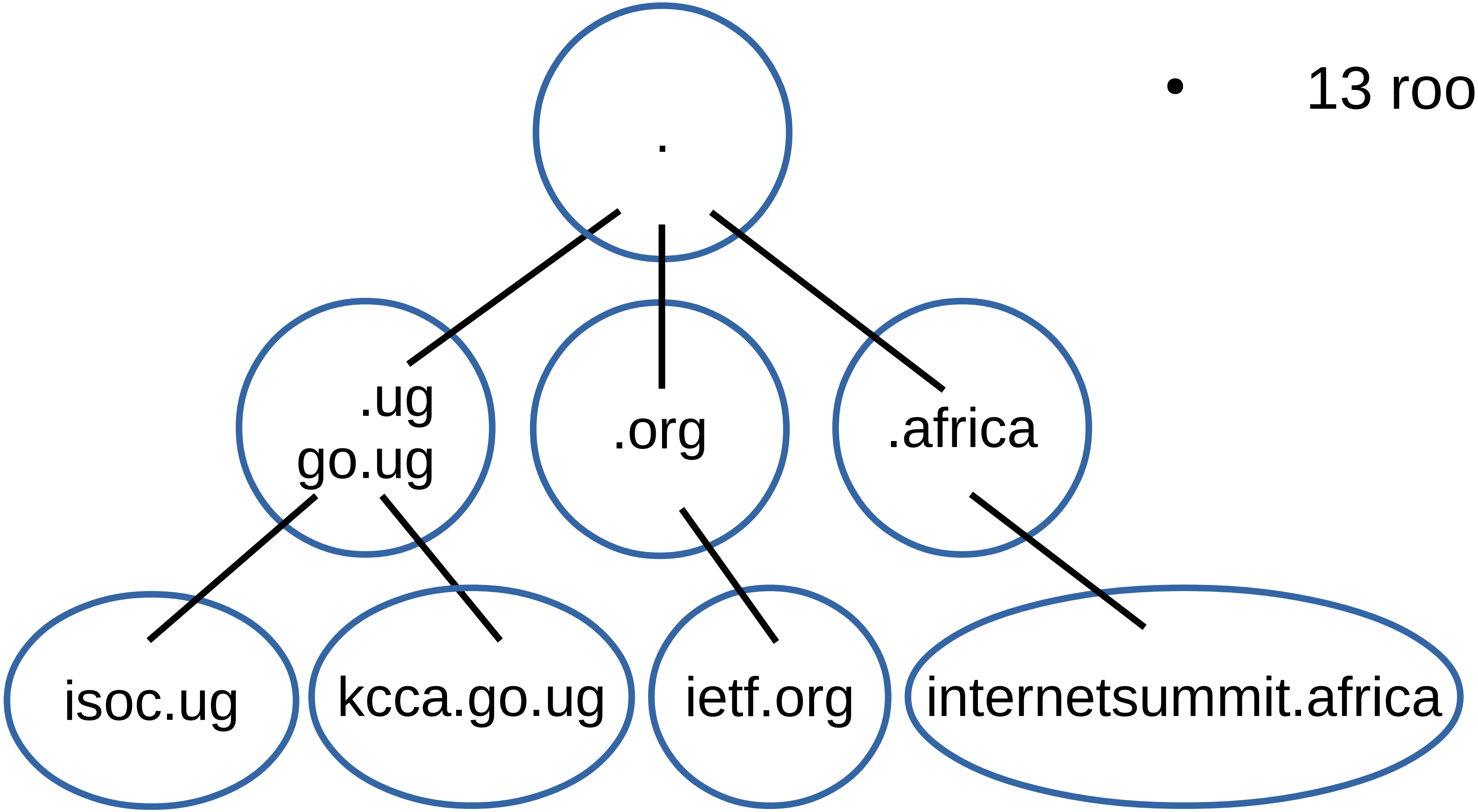
  ***D**omain **N**ame **S**ystem*

- November 1987 STD13

  (RFC 1034 & RFC 1035)

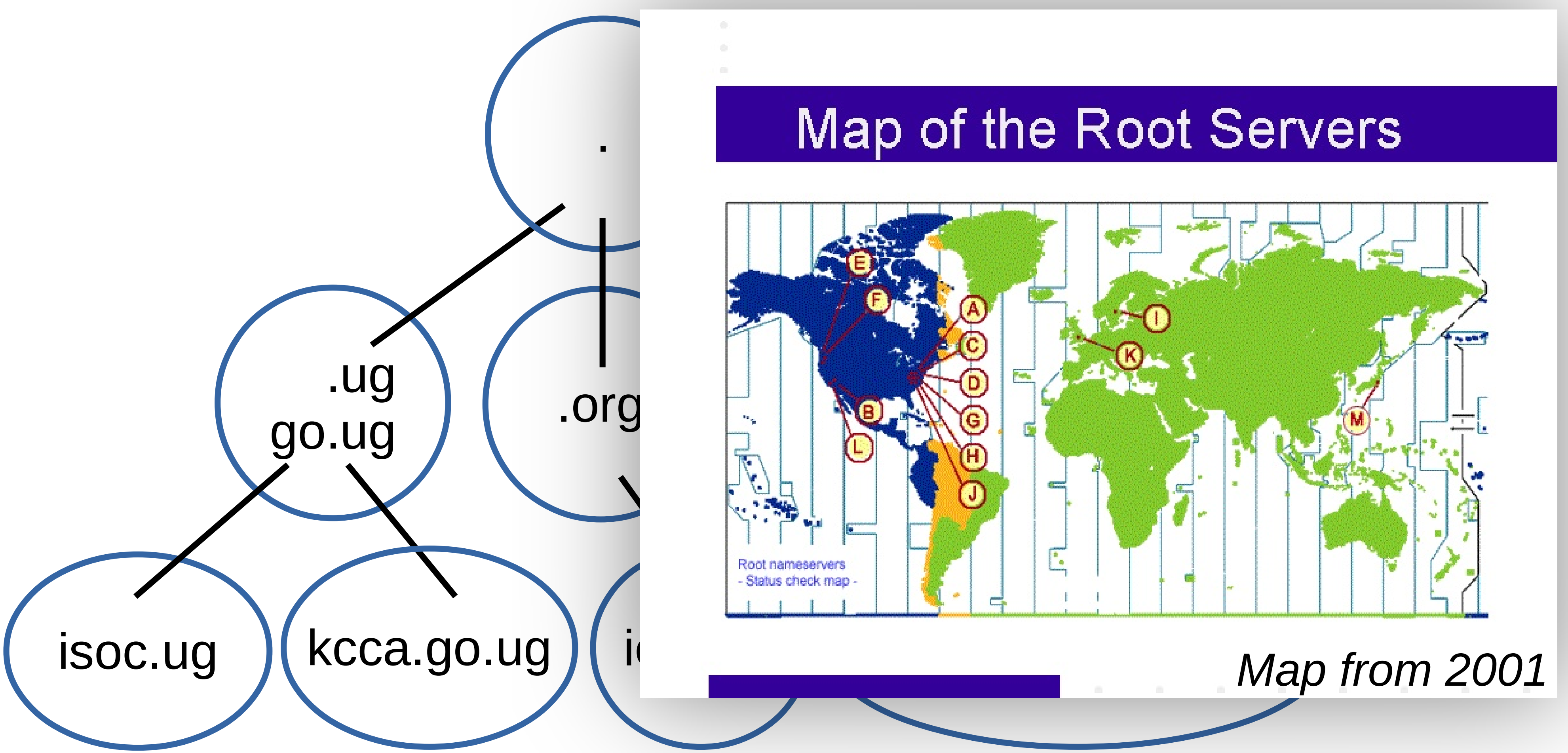
First implementation: https://www.hactrn.net/hacks/jeeves/

Domain Name Space – scale



- 13 root servers

Domain Name Space – scale

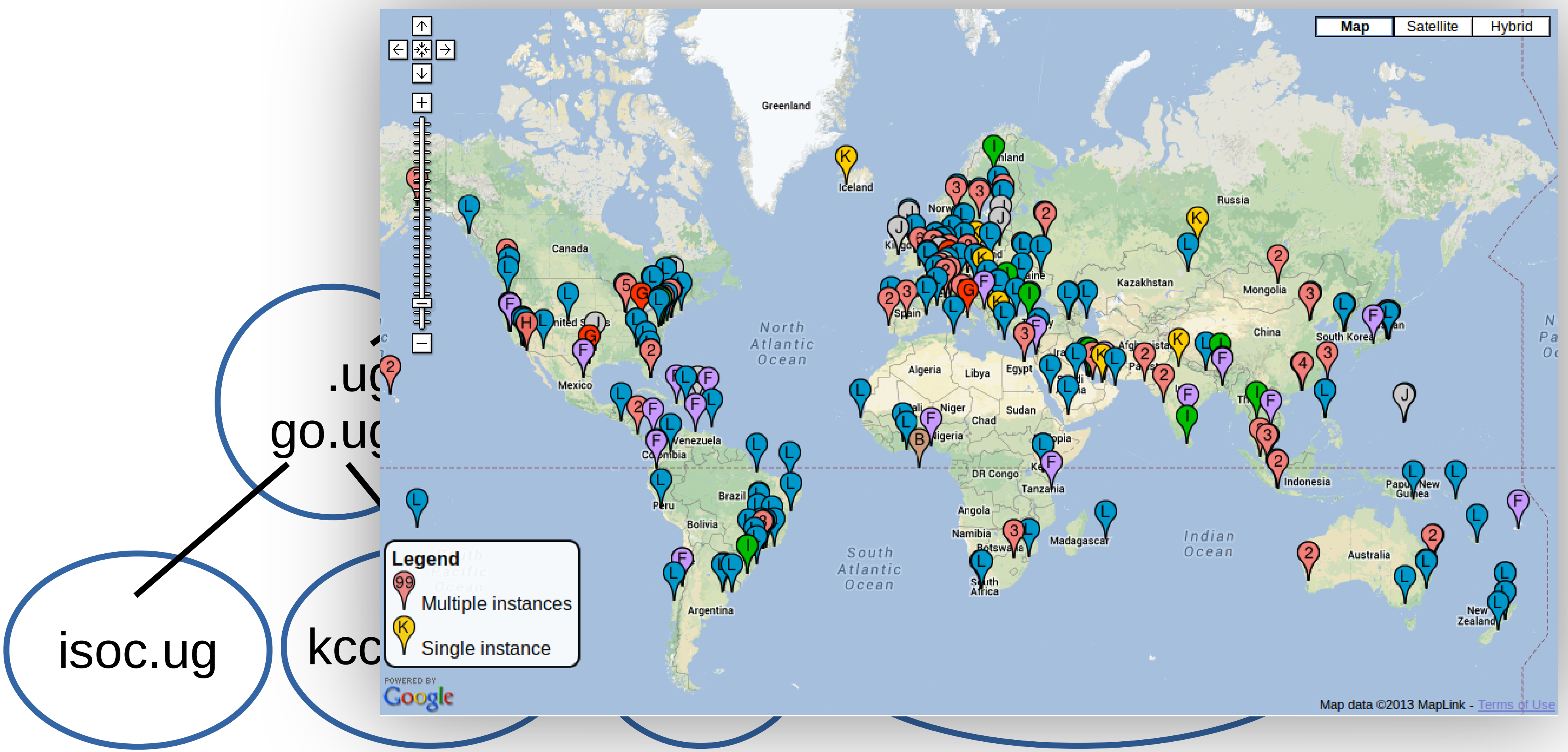


Map from 2001

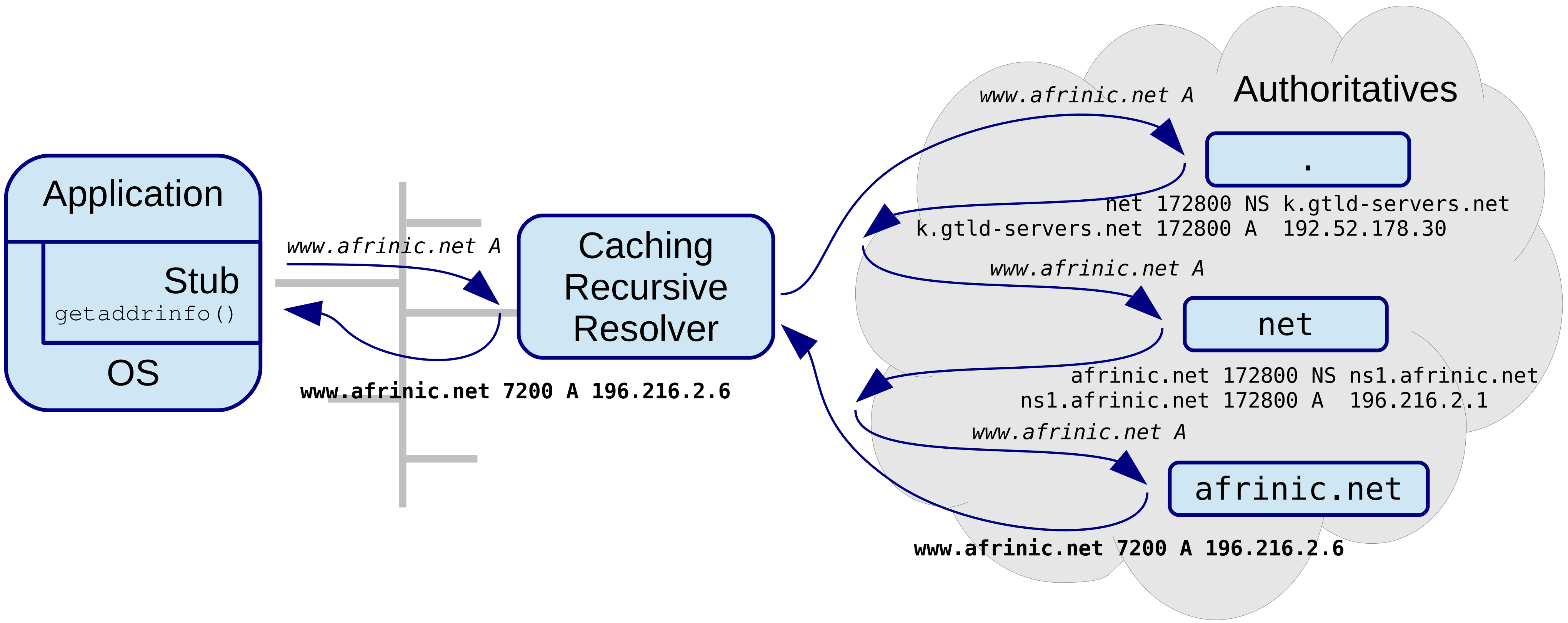
Domain Name Space – scale

A	VeriSign	198.41.0.4 2001:503:BA3E::2:30	**H**	US Army	128.63.2.53 2001:500:1::803f:235
B	USC-ISI	192.228.79.201 2001:478:65::53	**I**	Netnod	192.36.148.17 2001:7fe::53
C	Cogent	192.33.4.12 2001:500:2::c	**J**	VeriSign	192.58.128.30 2001:503:C27::2:30
D	Uni Maryland	199.7.91.13 2001:500:2d::d	**K**	RIPE NCC	193.0.14.129 2001:7fd::1
E	NASA	192.203.230.10 2001:500:a8::e	**L**	ICANN	199.7.83.42 2001:500:3::42
F	ISC	192.5.5.241 2001:500:2f::f	**M**	WIDE Project	202.12.27.33 2001:dc3::35
G	DoD	192.112.36.4 2001:500:12::d0d			

Domain Name Space – scale

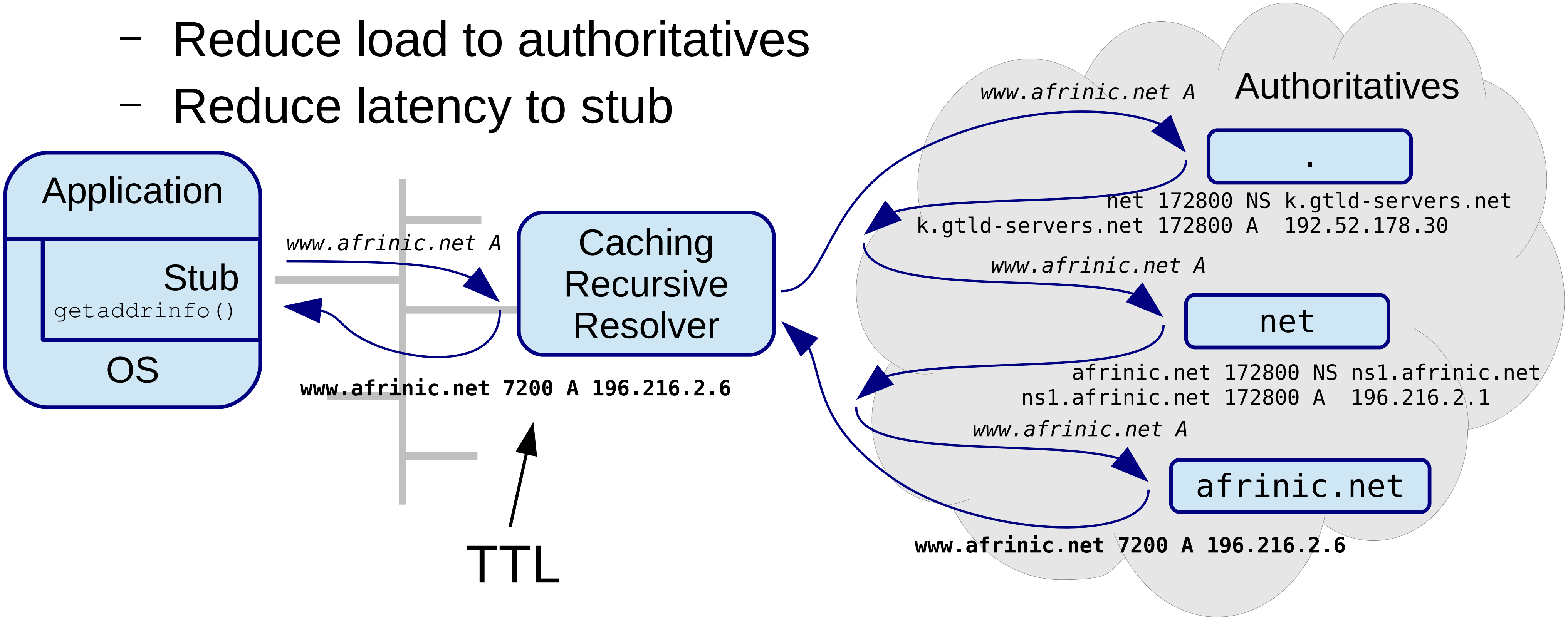


Domain Name System - scale



Domain Name System – scale

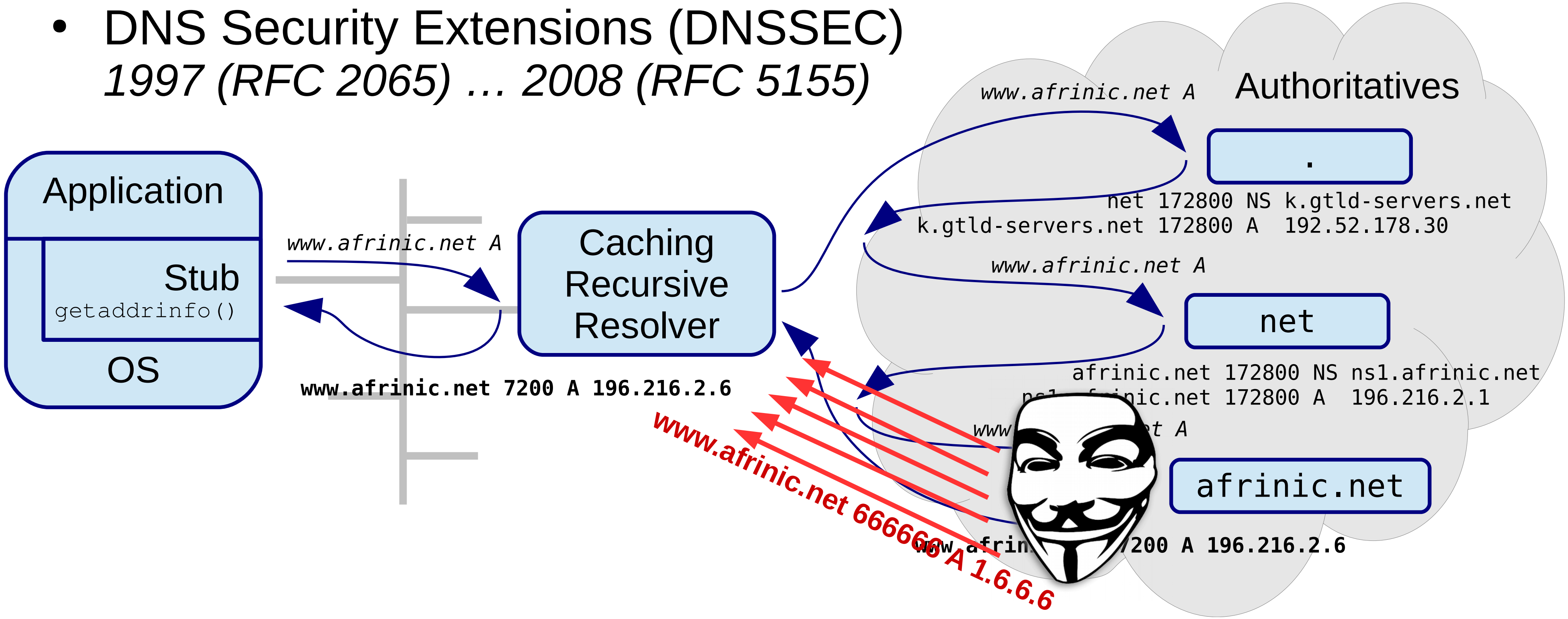
- ***UDP*** = No State on authoritatives
- ***Caching*** Recursive Resolvers:
  - Reduce load to authoritatives
  - Reduce latency to stub



Domain Name System – security

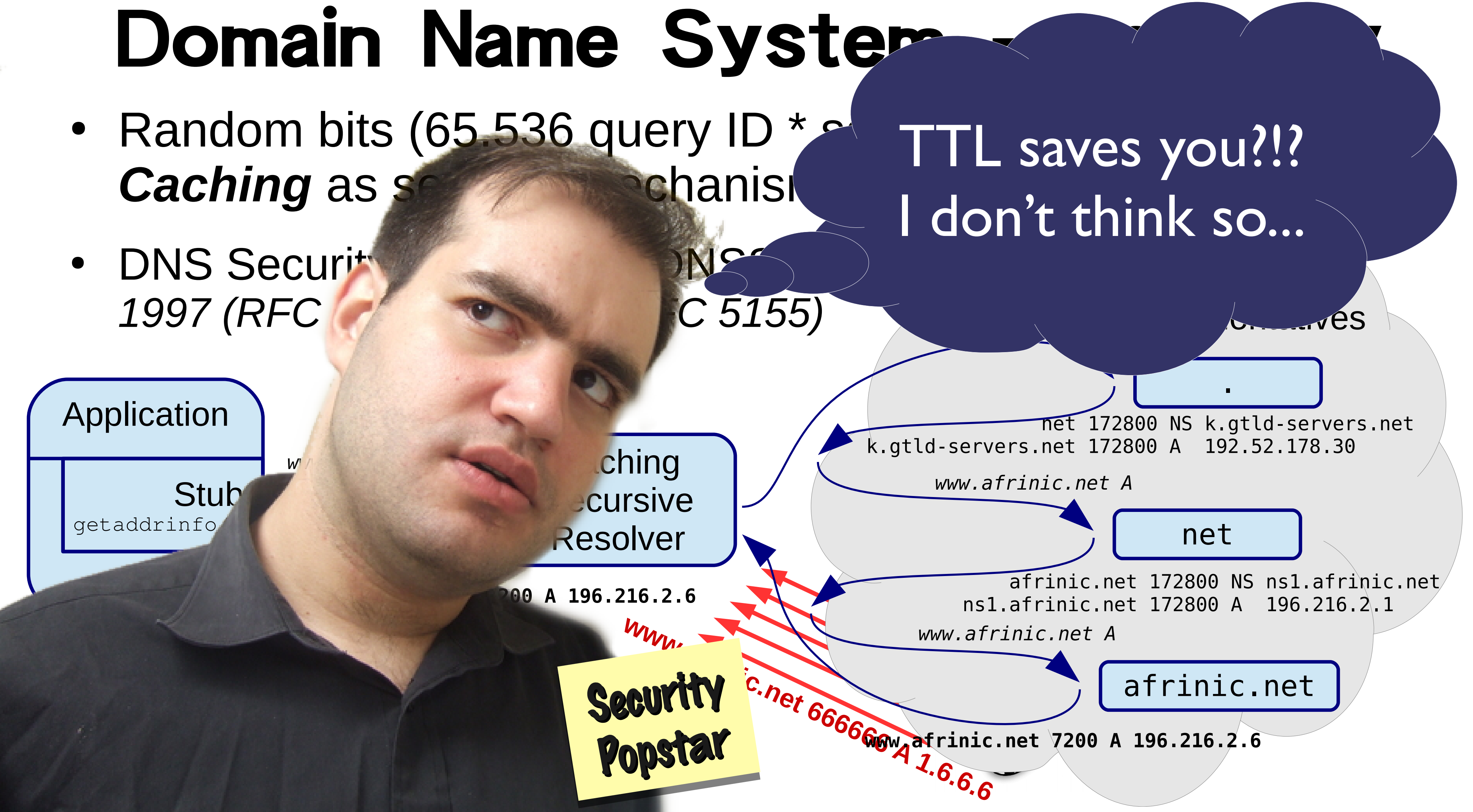
- Random bits (65.536 query ID * source ports) & ***Caching*** as security mechanism

- DNS Security Extensions (DNSSEC)
  1997 (RFC 2065) … 2008 (RFC 5155)

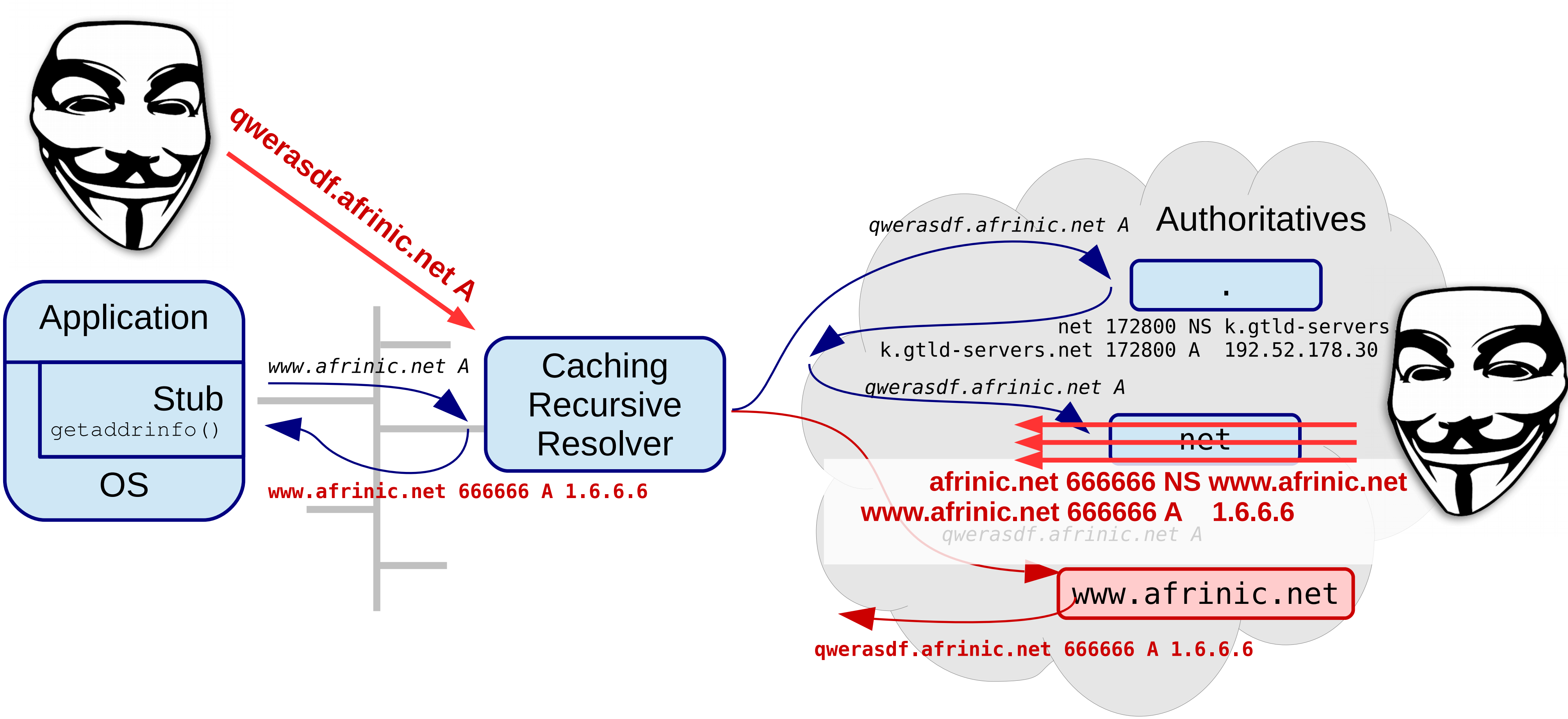


Domain Name System

- Random bits (65.536 query ID * s
Caching as se echanism
- DNS Securit DNSS
1997 (RFC C 5155)



Domain Name System - security

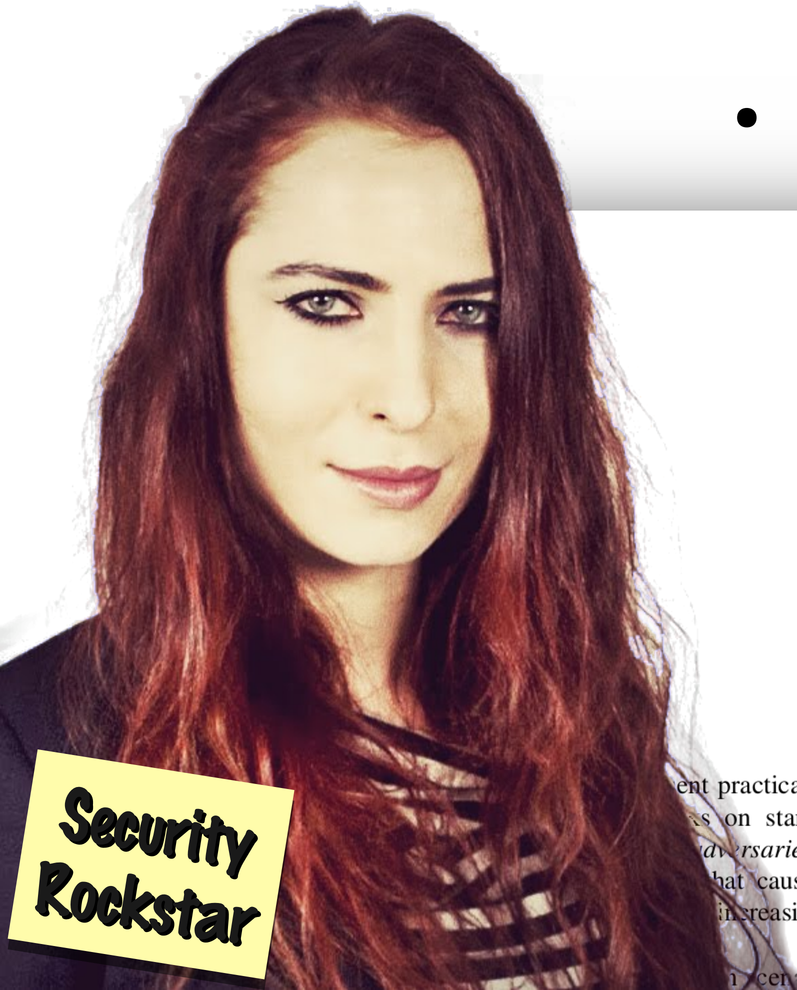


Domain Name System - security

# Bits	50% chance	5% chance	Method
16	10 seconds	1 second	Query ID
26	2.8 hours	17 minute	1024 source ports
34	28 days	2.8 days	All source ports + 2 bits server selection
44	288444 days	2844.4 days	0x20 hack

Domain Name System - security

- Help with spoofing DNS responses



Security Rockstar

Fragmentation Considered Poisonous

Amir Herzberg[†] *and Haya Shulman*[‡]
Dept. of Computer Science, Bar Ilan University
[†]*amir.herzberg@gmail.com,* [‡]*haya.shulman@gmail.com*

Abstract

ent practical *poisoning* and *name-server block-*
s on standard DNS resolvers, by *off-path,*
rsaries. Our attacks exploit large DNS
hat cause IP fragmentation; such long re-
reasingly common, mainly due to the use

cenarios, where DNSSEC is partially or

sary that is able to send spoofed packets (but not to intercept, modify or block packets). The most well known is Kaminsky's DNS poisoning attack [21], which was exceedingly effective against many resolvers at the time (2008). Kaminsky's attack, and most other known DNS poisoning attacks, allows the attacker to cause resolvers to provide incorrect (poisoned) responses to DNS queries of the clients, and thereby 'hijack' a domain name. We

Domain Name System – security

- Help with spoofing DNS responses

attacker ICMP frag needed→ authoritative

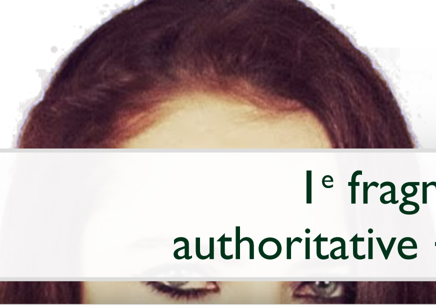
Offsets / Octet	Octet / Bit	0 (bits 0–7)	1 (bits 8–15)	2 (bits 16–23)	3 (bits 24–31)	
0	0	v4 IHL = 20	TOS	Total Length = 56		IP Header
4	32	IPID		x DF MF Frag Offset		
8	64	TTL	Protocol = 1	IP Header Checksum		
12	96	Source IP = 6.6.6.6				
16	128	Destination IP = 2.2.2.2				
20	160	Type = 3	Code = 4	ICMP Checksum		ICMP Header
24	192	Unused		MTU = 100		
28	224	v4 IHL = 20	TOS	Total Length = 76		IP Header
32	256	IPID		x DF MF Frag Offset		
36	288	TTL	Protocol = 17	IP Header Checksum		
40	320	Source IP = 2.2.2.2				
44	352	Destination IP = 7.7.7.7				
48	384	Source Port = 53		Destination Port = 12345		UDP Header
52	416	Length = 56		UDP Checksum = 0		

ent practical
s on stand
adversaries.
hat cause
increasingly common, mainly due to the use
scenarios, where DNSSEC is partially or

poisoning attacks, allows the attacker to cause resolvers to provide incorrect (poisoned) responses to DNS queries of the clients, and thereby 'hijack' a domain name. We

Domain Name System – security

- Help with spoofing DNS responses



1e fragment
authoritative → resolver

Offsets Octet	Octet Bit	0 (bits 0–7)	1 (bits 8–15)	2 (bits 16–23)	3 (bits 24–31)	Section
0	0	v4 · IHL = 20	TOS	Total Length = 85		IP Header
4	32	IPID = 23456		x DF MF Frag Offset = 0		IP Header
8	64	TTL	Protocol = 17	IP Header Checksum		IP Header
12	96	Source IP = 2.2.2.2				IP Header
16	128	Destination IP = 7.7.7.7				IP Header
20	160	Source Port = 53		Destination Port = 12345		UDP Header
24	192	Length = 65		UDP Checksum = 0x14de		UDP Header
28	224	TXID = 76543		QR Opcode = 0 AA TC RD RA	Z RCODE = 0	DNS Header
32	256	Question Count = 1		Answer Record Count = 1		DNS Header
36	288	Authority Record Count = 0		Additional Record Count = 1		DNS Header
40	320	4	m	a	i	Question Section
44	352	l	4	v	i	Question Section
48	384	c	t	2	i	Question Section
52	416	m	0	Type = A		Question Section
56	448	Class = IN		Name (Pointer)		Question Section / Answer Section
60	480	Type = A		Class = IN		Answer Section
64	512	TTL				Answer Section

2e fragment
attacker → resolver

Offsets Octet	Octet Bit	0 (bits 0–7)	1 (bits 8–15)	2 (bits 16–23)	3 (bits 24–31)	Section
0	0	v4 · IHL = 20	TOS	Total Length = 85		IP Header
4	32	IPID = 23456		x DF MF Frag Offset = 48		IP Header
8	64	TTL	Protocol = 17	IP Header Checksum		IP Header
12	96	Source IP = 2.2.2.2				IP Header
16	128	Destination IP = 7.7.7.7				IP Header
20	160	Data Length = 4		IPv4 Address		Answer Section
24	192	= 2.2.2.2		Name = 0	Type	Answer Section / Additional Section
28	224	= OPT	UDP Payload Size = 4096		EXTENDED-RCODE = 0	Additional Section
32	256	Version = 0	DO Z		Data Length	Additional Section
36	288	= 0				Additional Section

server block-
by *off-path,*
it large DNS
uch long re-
due to the use
n cenarios, where DNSSEC is partially or

sary that is able to send spoofed packets (but not to intercept, modify or block packets). The most well known is Kaminsky's DNS poisoning attack [21], which was exceedingly effective against many resolvers at the time (2008). Kaminsky's attack, and most other known DNS poisoning attacks, allows the attacker to cause resolvers to provide incorrect (poisoned) responses to DNS queries of the clients, and thereby 'hijack' a domain name. We

Domain Name System - security

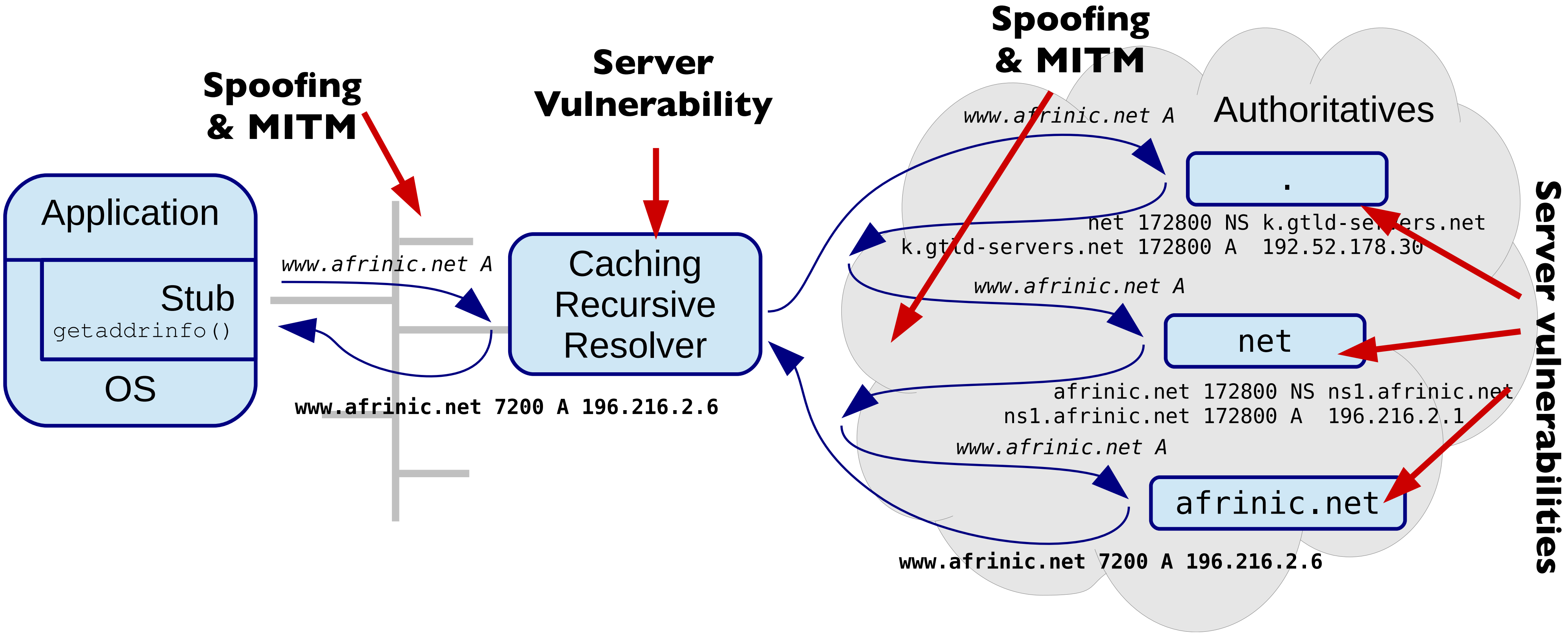
bits	50% chance	5% chance	Method
~~16~~	~~10 seconds~~	~~1 seconde~~	~~Query ID~~
~~26~~	~~2,8 uur~~	~~17 minutes~~	~~1024 source ports~~
2	0 seconds	0 seconds	~~All source ports~~ 2 bits server selection
~~44~~	~~288444 days~~	~~2844.4 days~~	~~0x20 hack~~
5	0 seconds	0 seconds	IP ID

Domain Name System - security

bits	50% chance	5% chance	Method
~~16~~	~~10 seconds~~	~~1 seconde~~	~~Query ID~~
~~26~~	~~2,8 uur~~	~~17 minutes~~	~~1024 source ports~~
2	0 seconds	0 seconds	~~All source ports~~ 2 bits server selection
~~44~~	~~288444 days~~	~~2844.4 days~~	~~0x20 hack~~
5	0 seconds	0 seconds	IP ID
69	2,928,370,544 year	292,837,054 year	IPv6 /64 source address

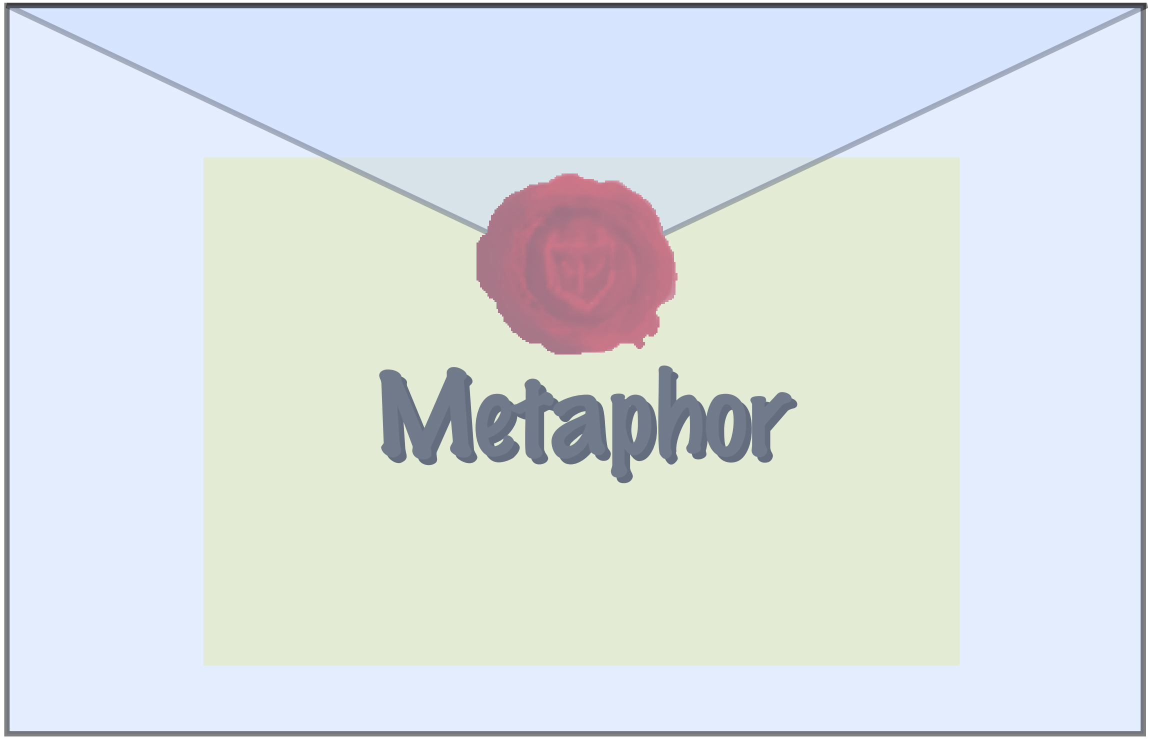
Domain Name System – security

- It's not just spoofing



DNS Security Extensions (DNSSEC)

- end-to-end security on top of DNS

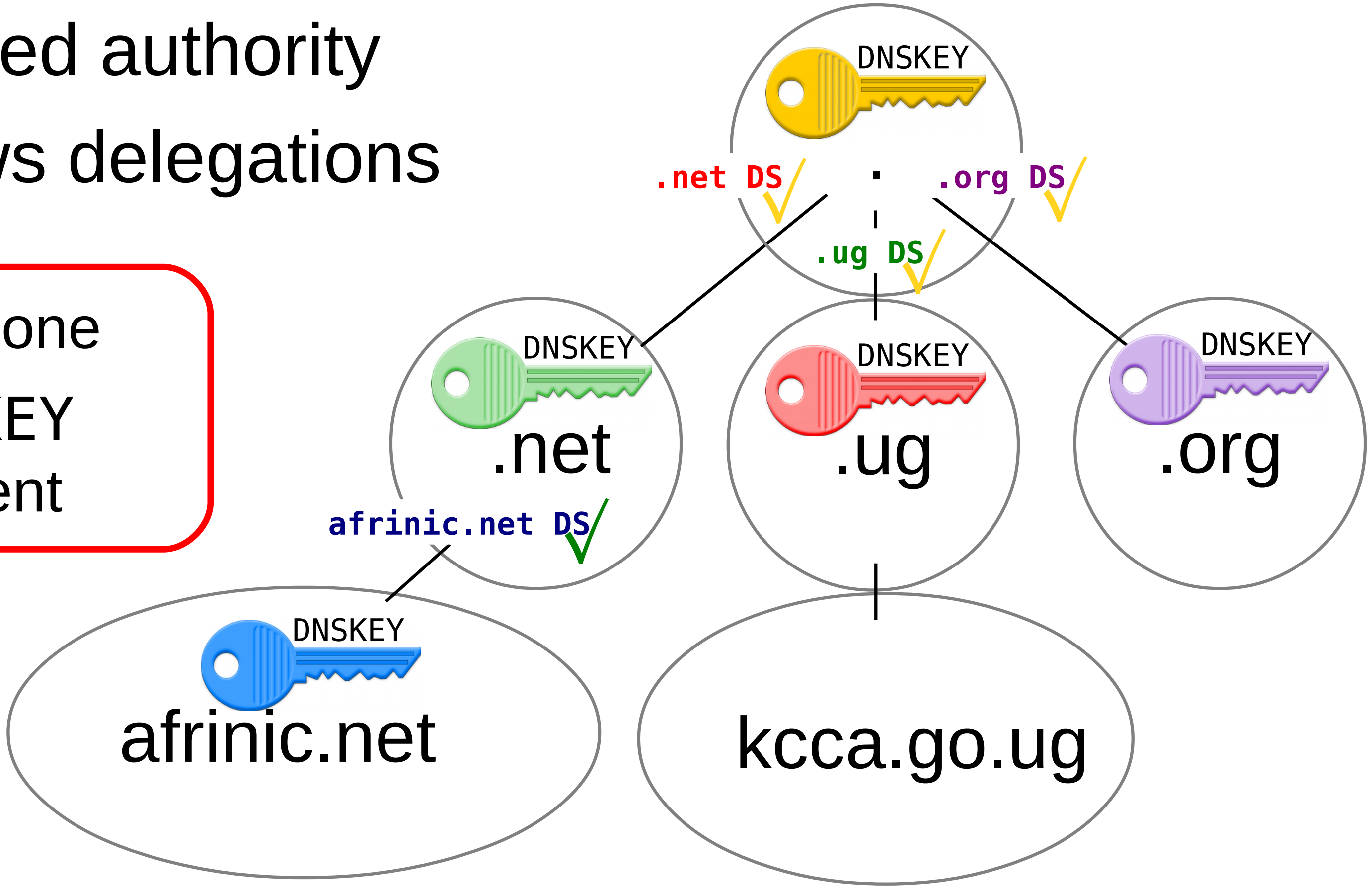


DNS Security Extensions (DNSSEC)

Chain of Trust

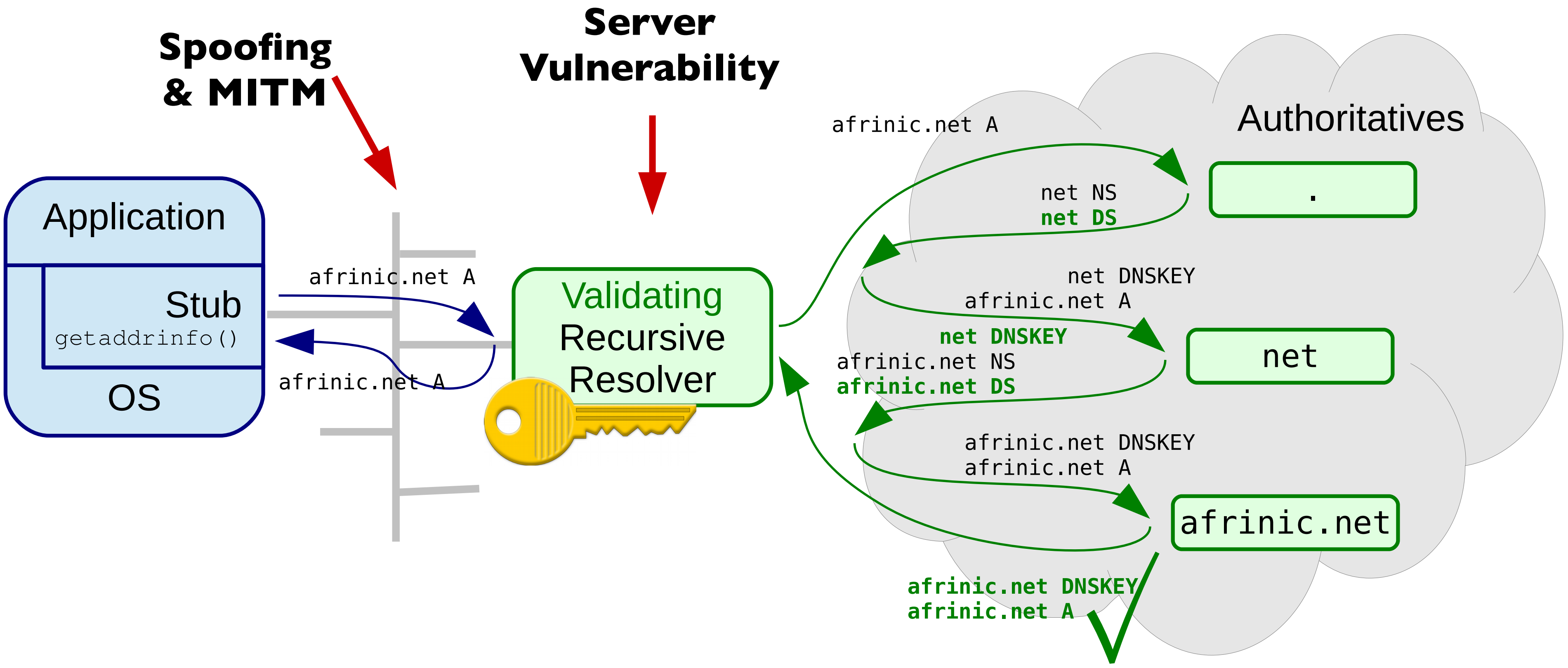
- Zones with distributed authority
- Chain of trust follows delegations

DNSKEY	Public key of zone
DS	Hash of DNSKEY signed by parent



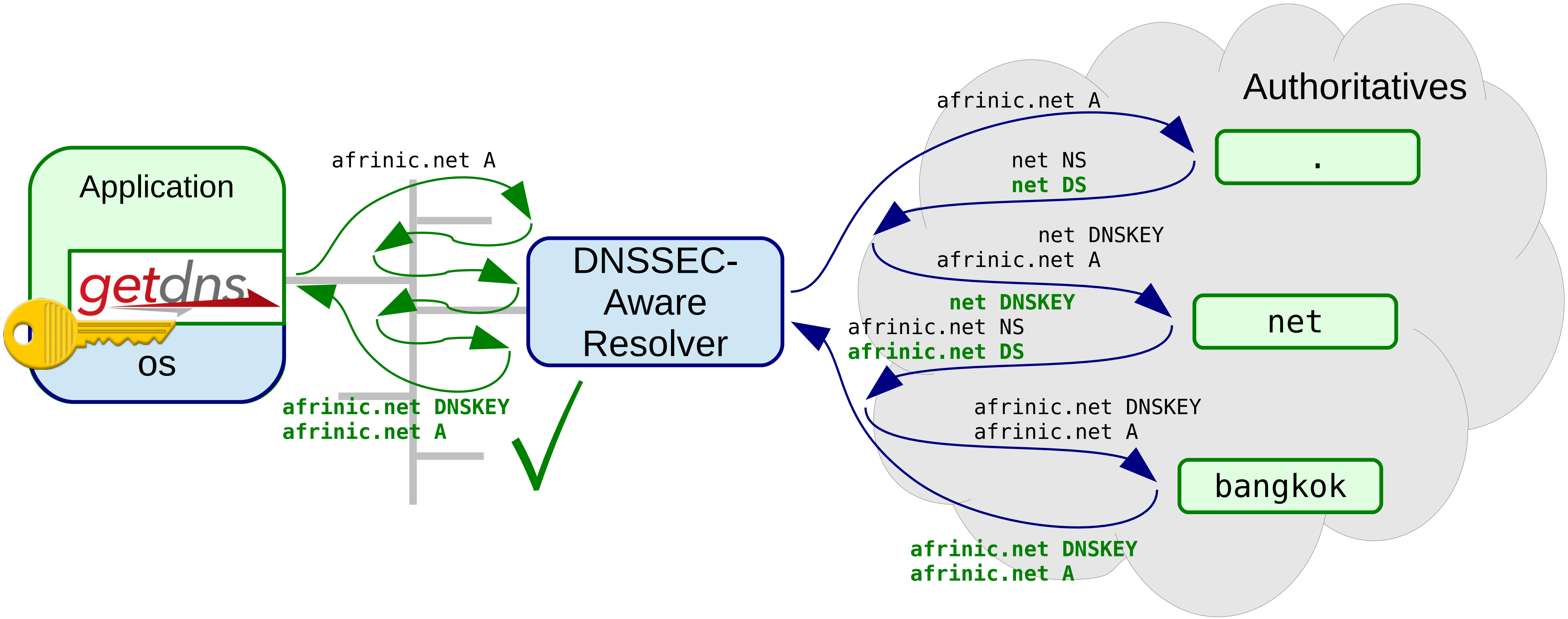
DNS Security Extensions (DNSSEC)

Validation



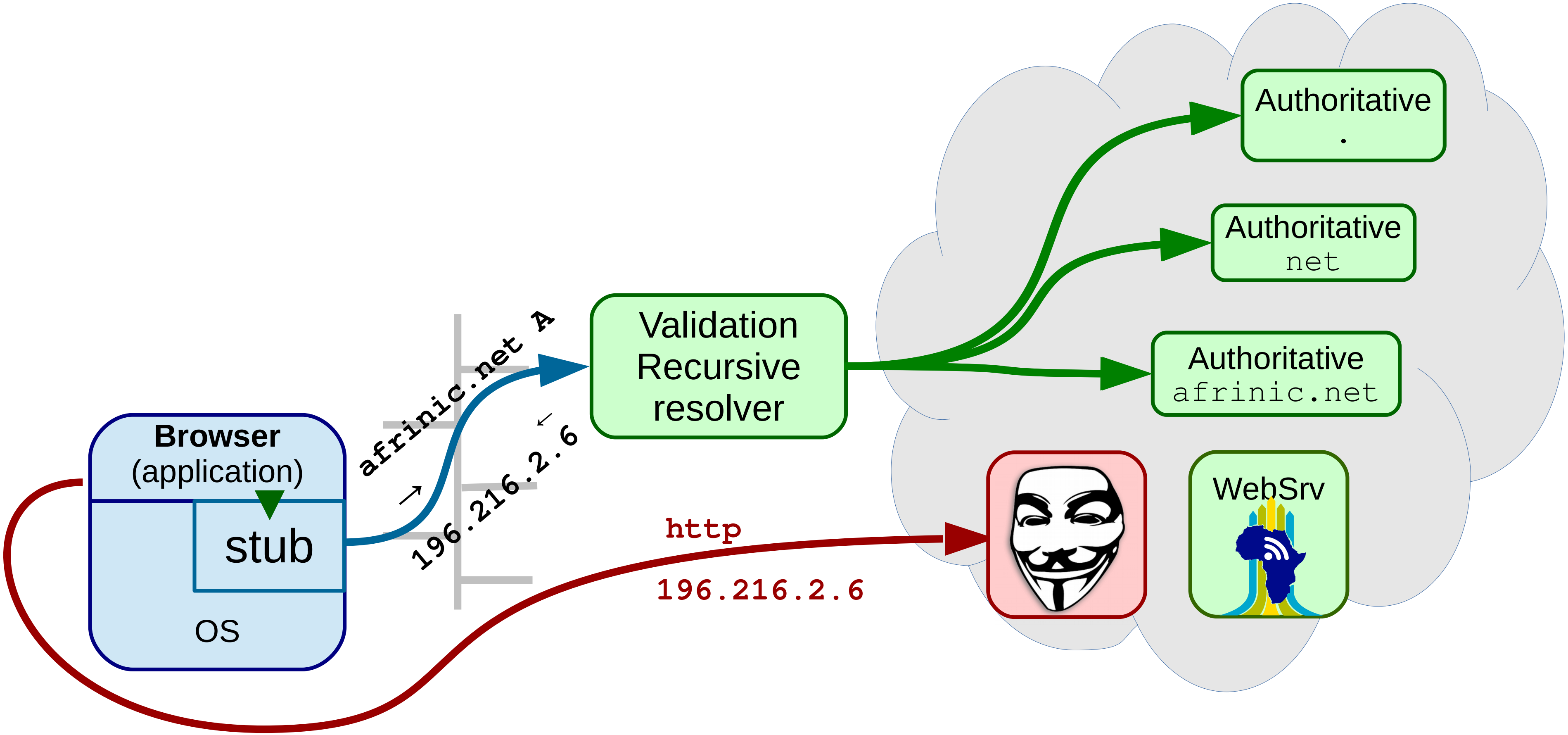
DNS Security Extensions (DNSSEC)

end-to-end validation

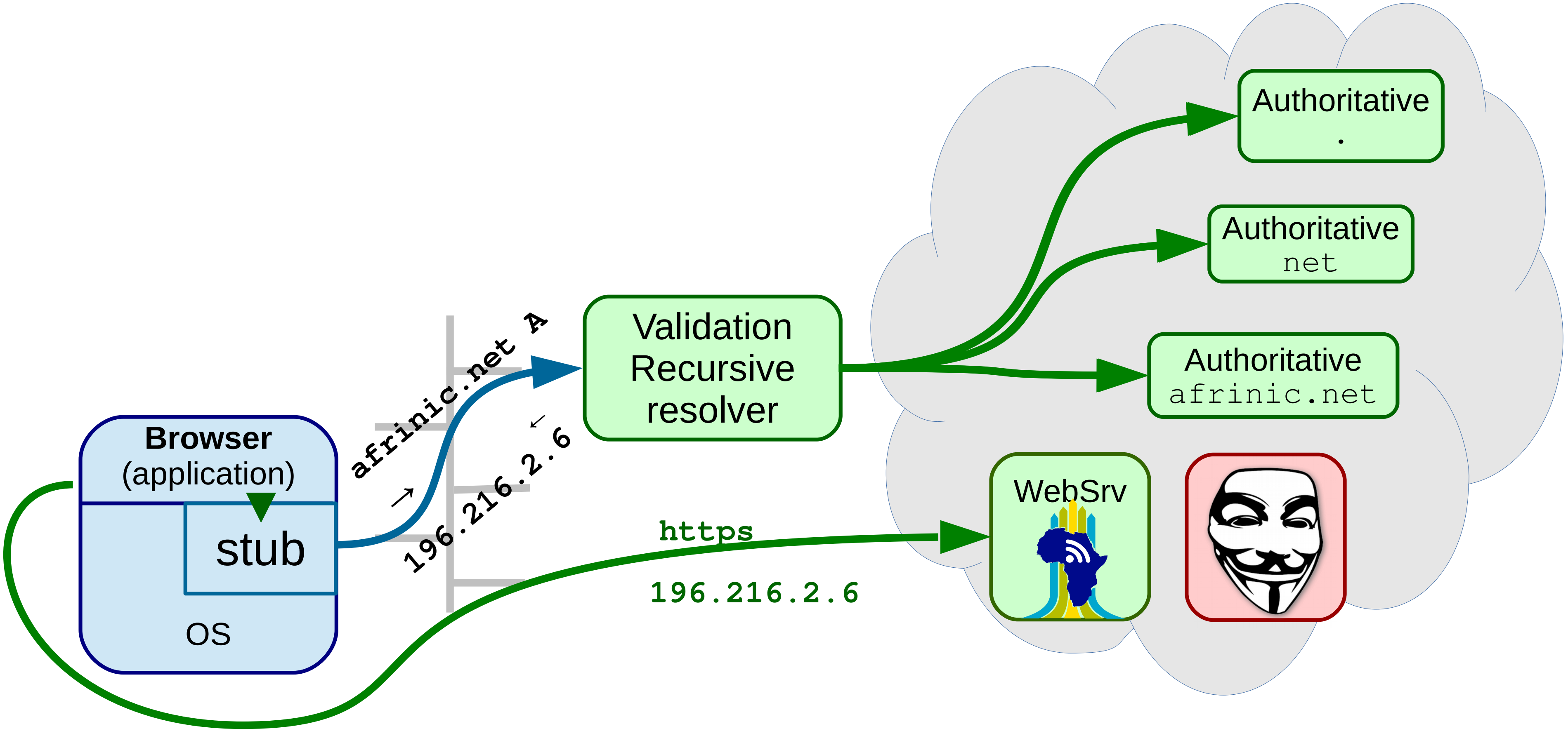


DNS Security Extensions (DNSSEC)

does not protect against MITM

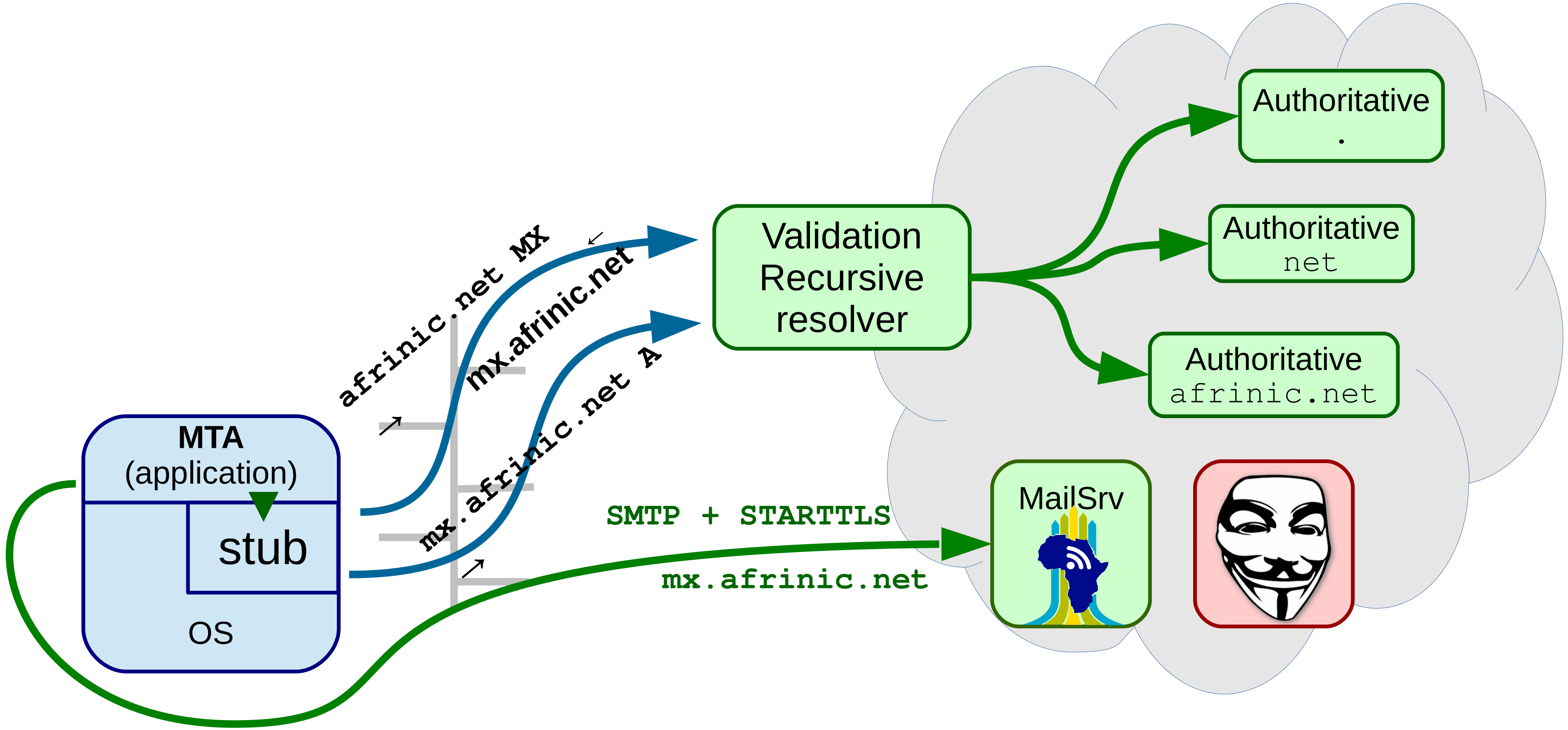


DNS Security Extensions (DNSSEC)
does not protect against MITM – TLS does!



DNS Security Extensions (DNSSEC)

still needed for referrals

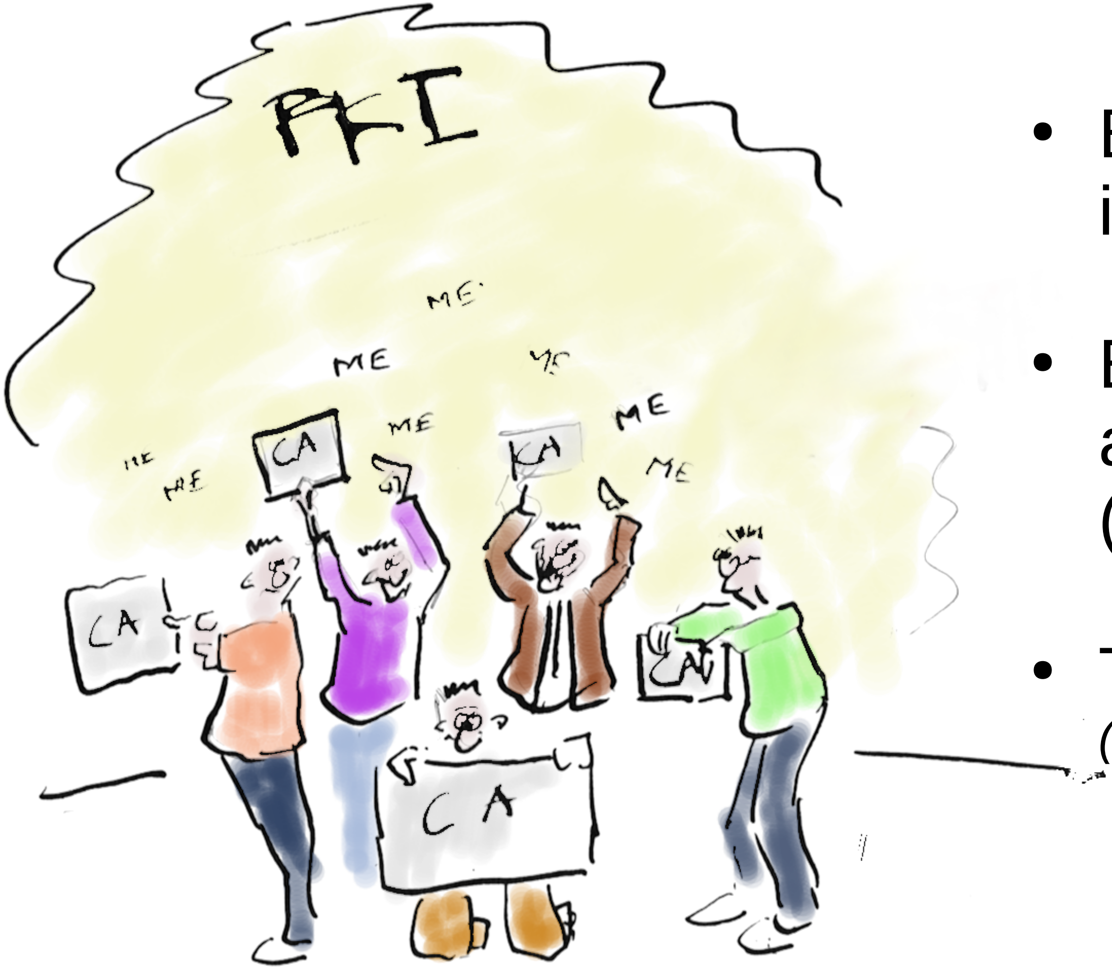


DNSSEC for Applications
voor TLS

- Transport Layer Security (TLS) uses
  both asymmetric and symmetric encryption
- A symmetric key is sent encrypted with remote public key

- How is the remote public key authenticated?

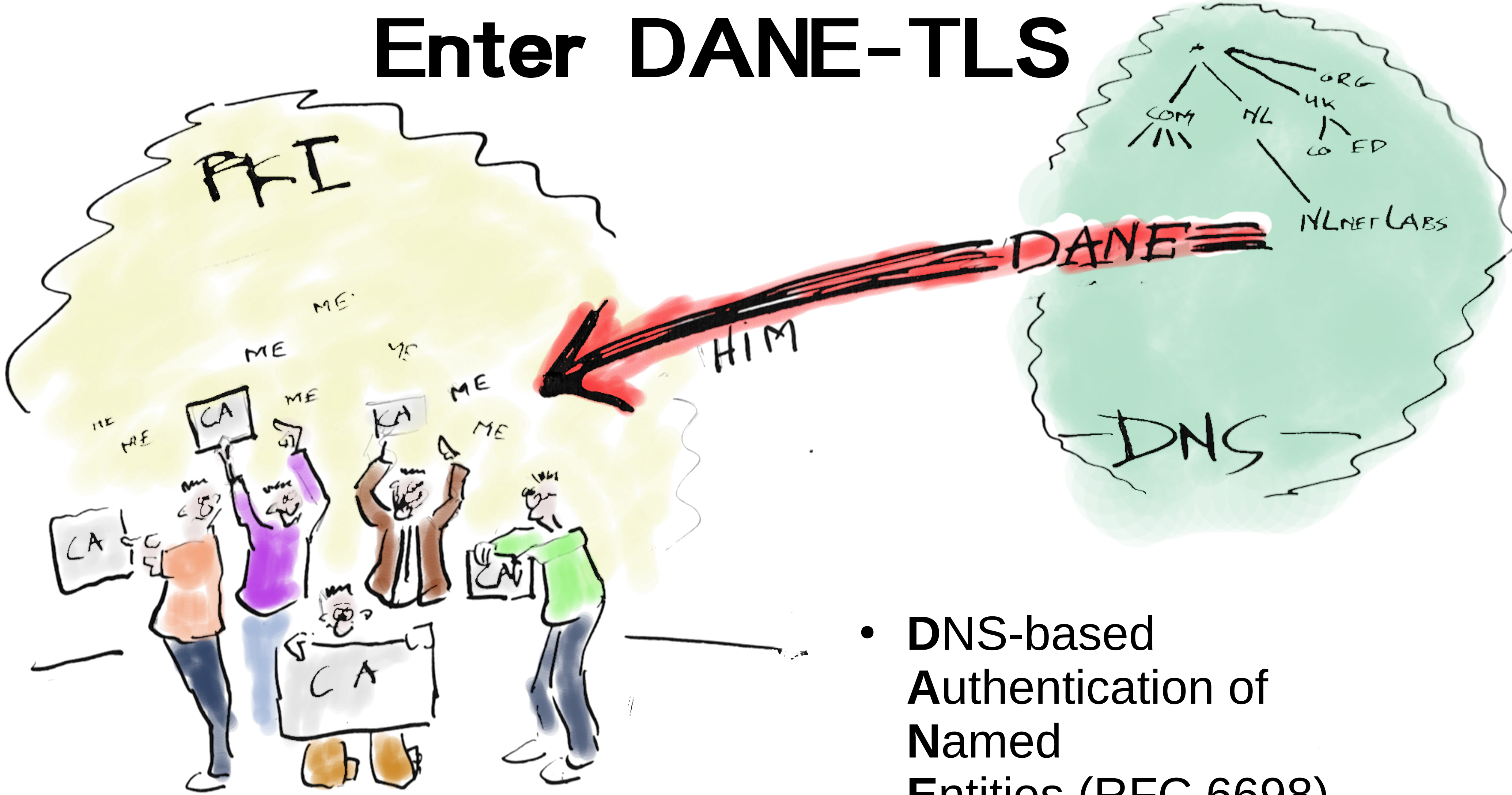
TLS without DNSSEC



Cartoon by Kloot

- By the Certificate Authorities in OS and/or browser
- Each CA is authorized to authenticate for **any** name (weakest link problem)
- There are more than 1500 CAs
  (in 2010, see https://www.eff.org/observatory)

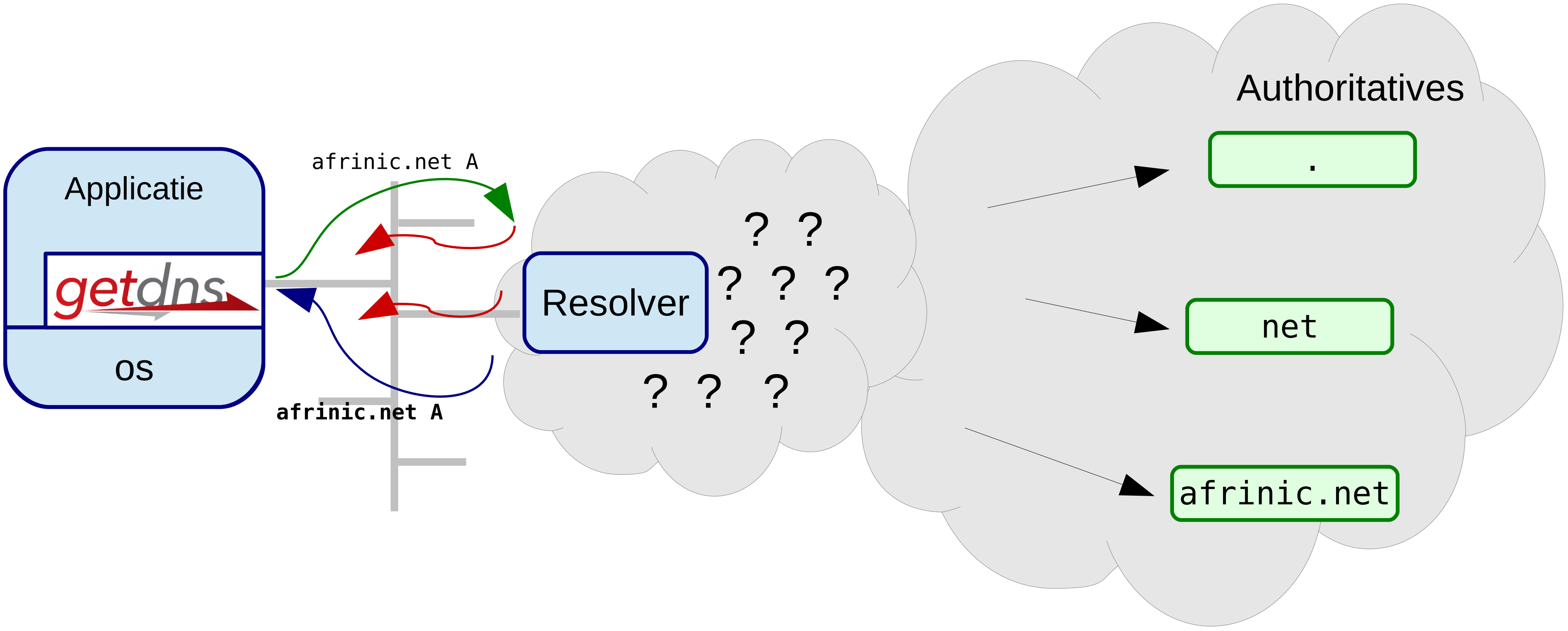
Enter DANE-TLS



Cartoon by Kloot

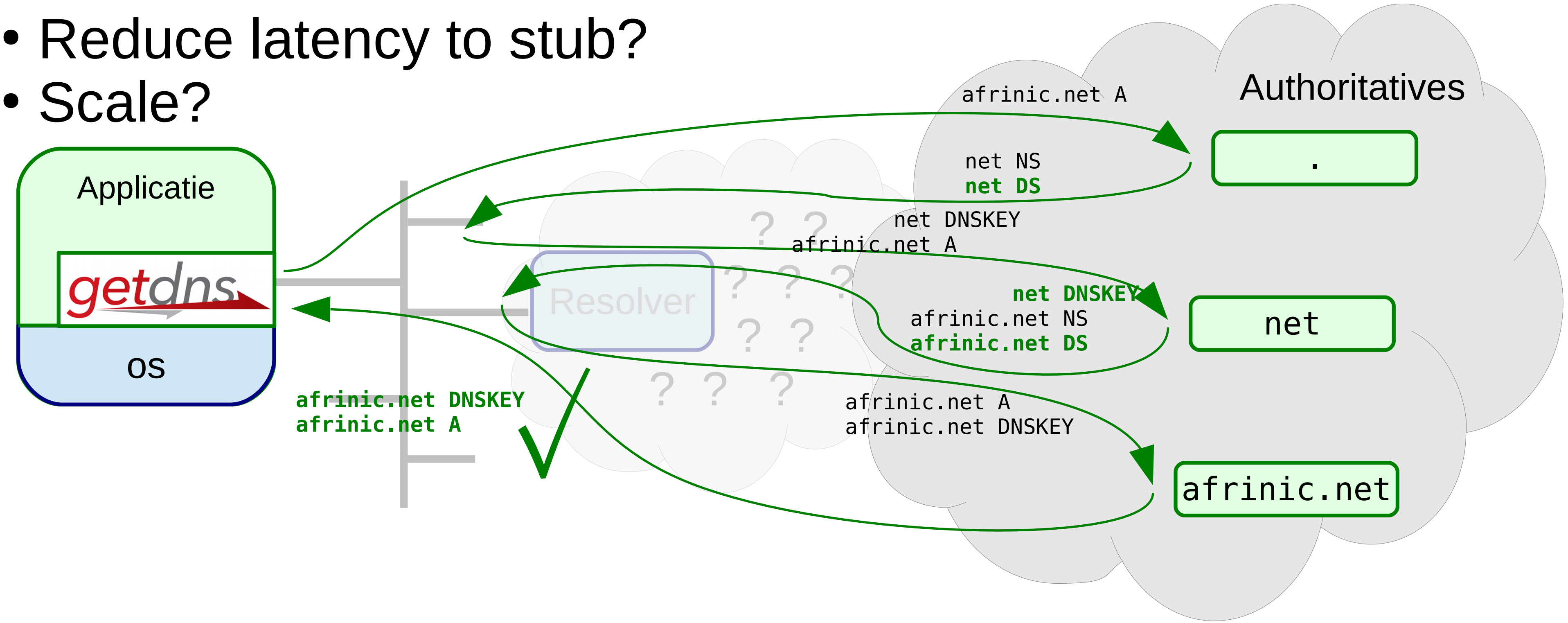
- **D**NS-based **A**uthentication of **N**amed **E**ntities (RFC 6698)

DNS Security Extensions (DNSSEC)
end-to-end validation in practice



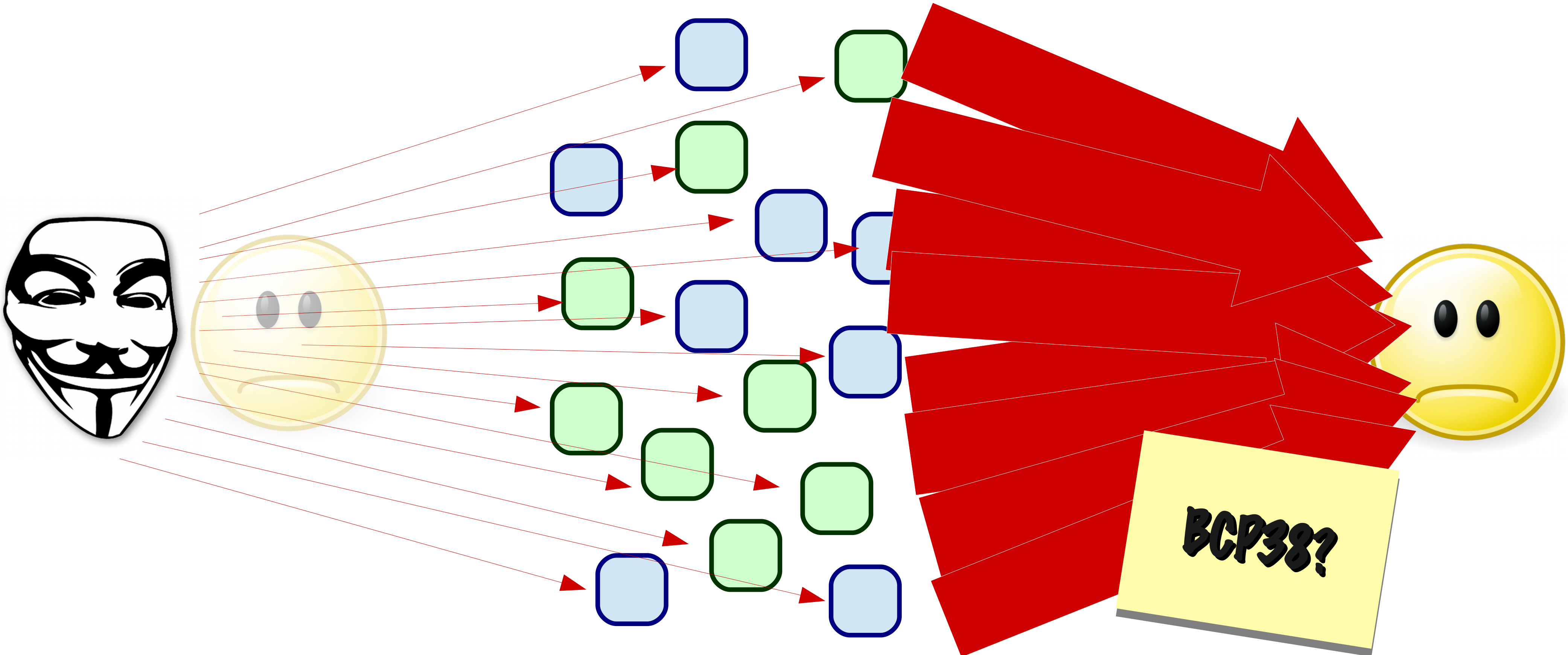
DNS Security Extensions (DNSSEC)
end-to-end validation in practice

- Reduce load to authoritatives?
- Reduce latency to stub?
- Scale?



DNS Security Extensions (DNSSEC)

consequence of UDP, worse with DNSSEC



Privacy

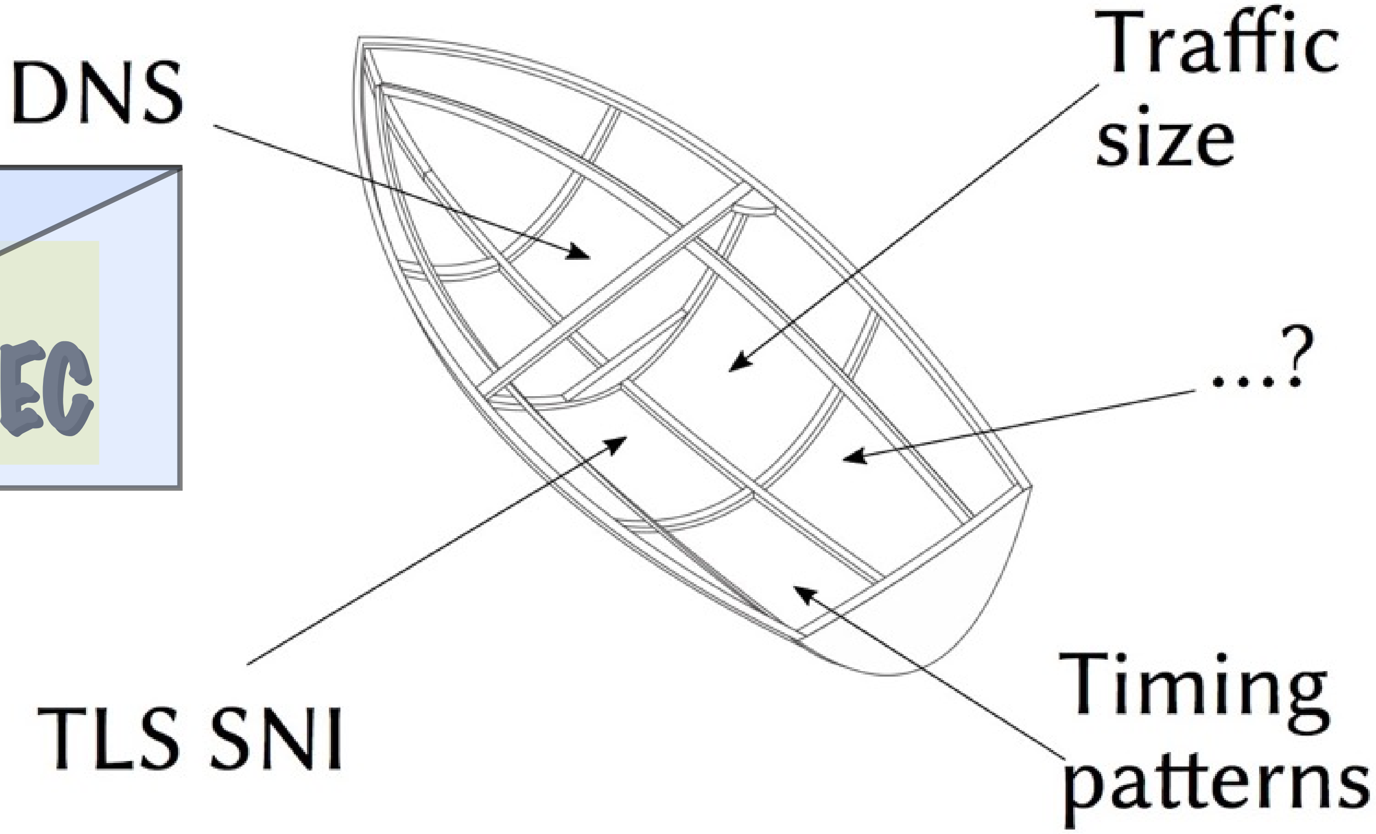
March 2011: I-D
Privacy Considerations
for Internet Protocols

June 2013: Snowden Revelations
Morecowbell

July 2013: RFC6973
Privacy Considerations
for Internet Protocols

May 2014: RFC7258
Pervasive Monitoring
is an Attack

Privacy

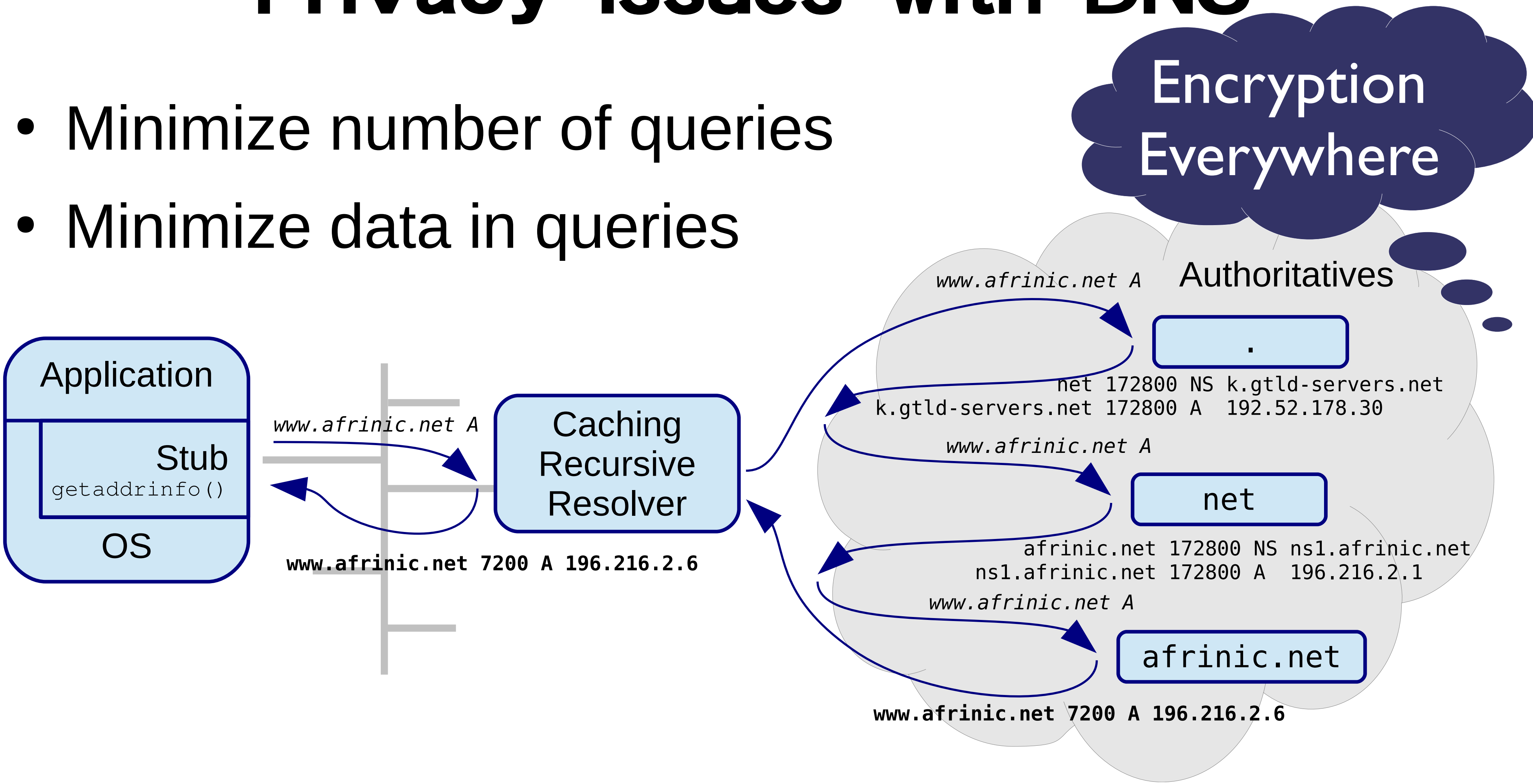


- NSA's Morecowbell on DNS based pervasive monitoring system

Leaky Boat van DKG

Privacy issues with DNS

- Minimize number of queries
- Minimize data in queries



Privacy issues with DNS

minimize # queries – local root

- RFC 7706 -
  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 – 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 – serve stale

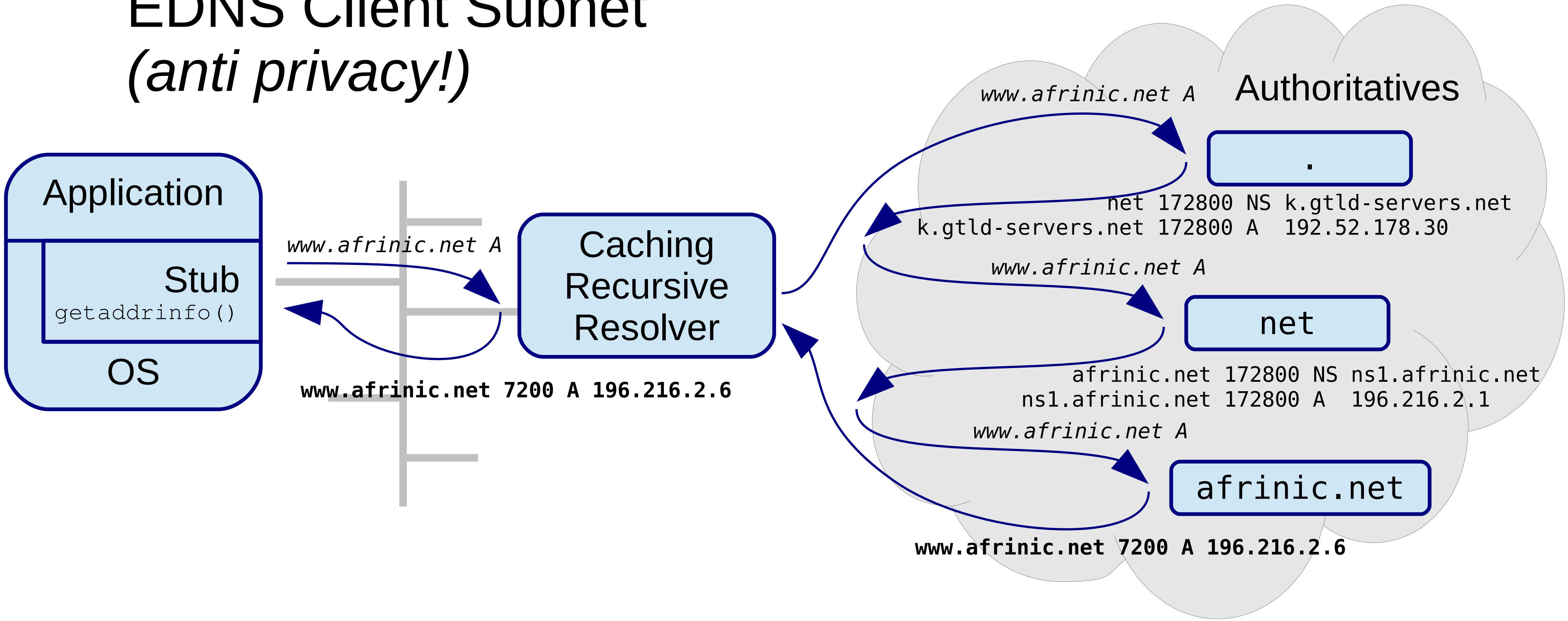
- draft-ietf-dnsop-serve-stale
- Privacy aspect and/or Performance aspect

```
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

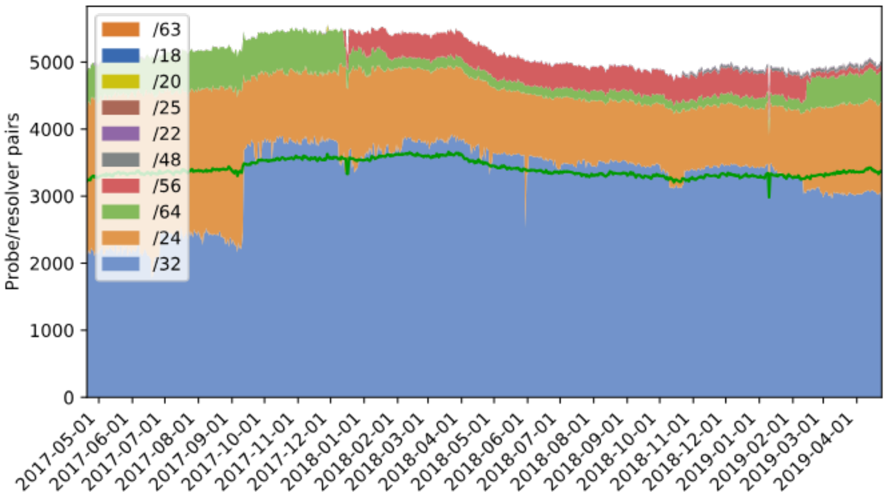
- RFC7871 -
  EDNS Client Subnet
  (anti privacy!)

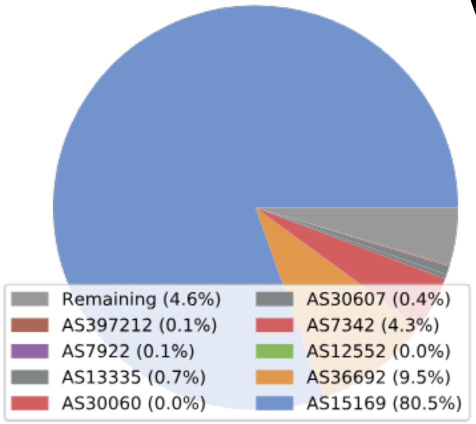


Privacy issues with DNS

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
  section 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** respect it

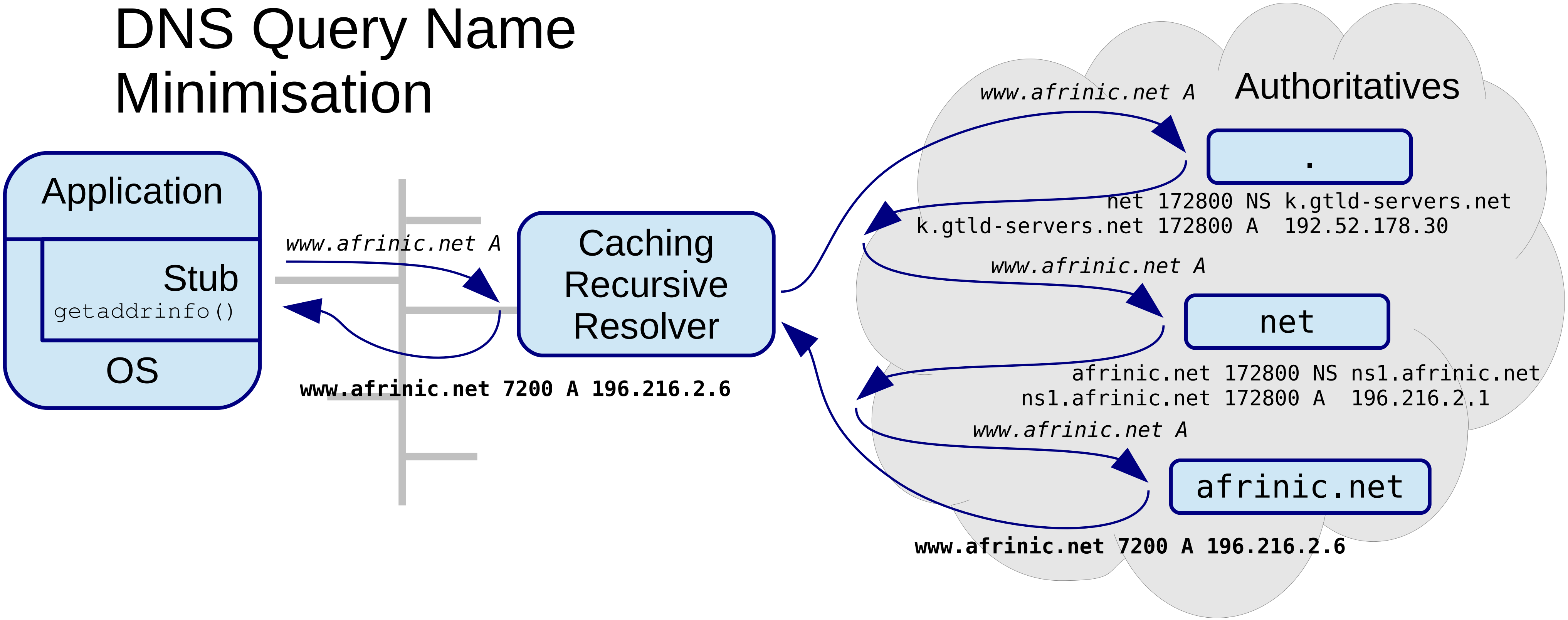
```
# EDNS0 option for ECS client privacy
# as described in Section 7.1.2 of
# https://tools.ietf.org/html/rfc7871

edns_client_subnet_private : 1




"stubby.yml"
```

getdns

Privacy issues with DNS

minimize data in queries – qname min

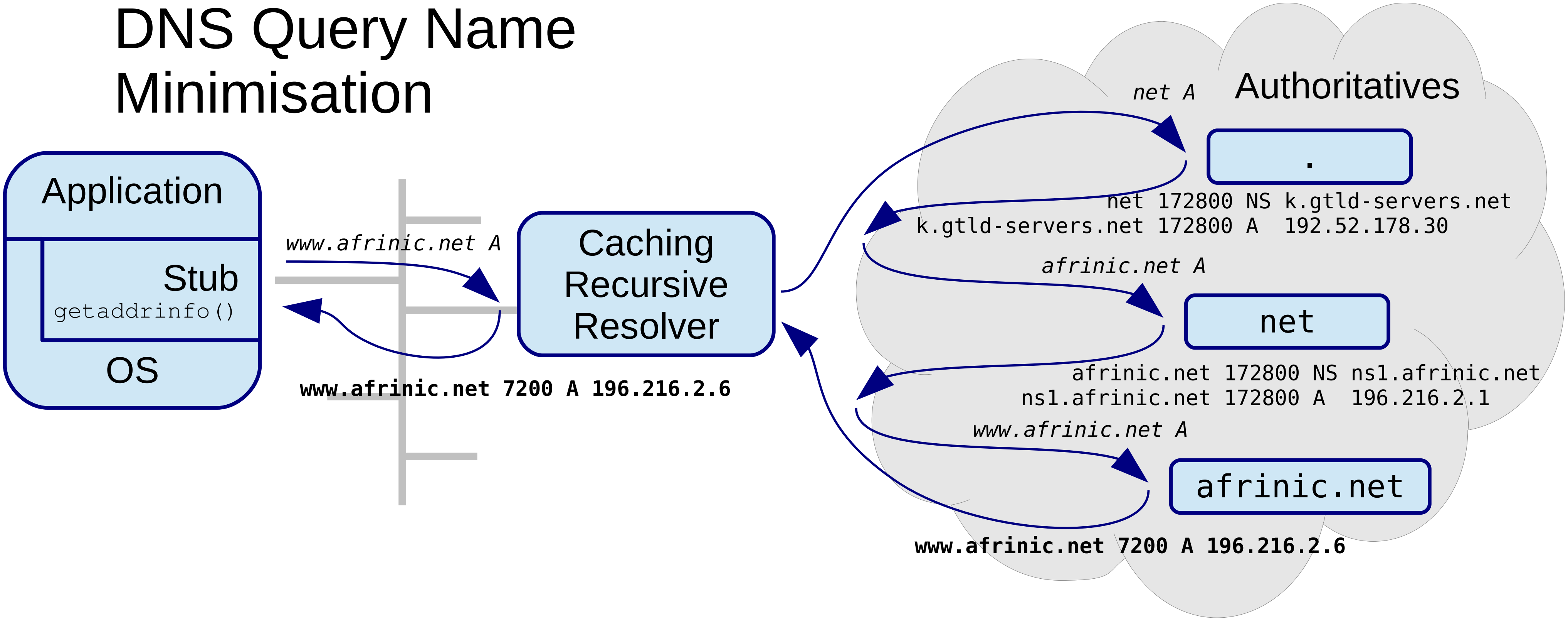
- Without RFC7816 - DNS Query Name Minimisation



Privacy issues with DNS

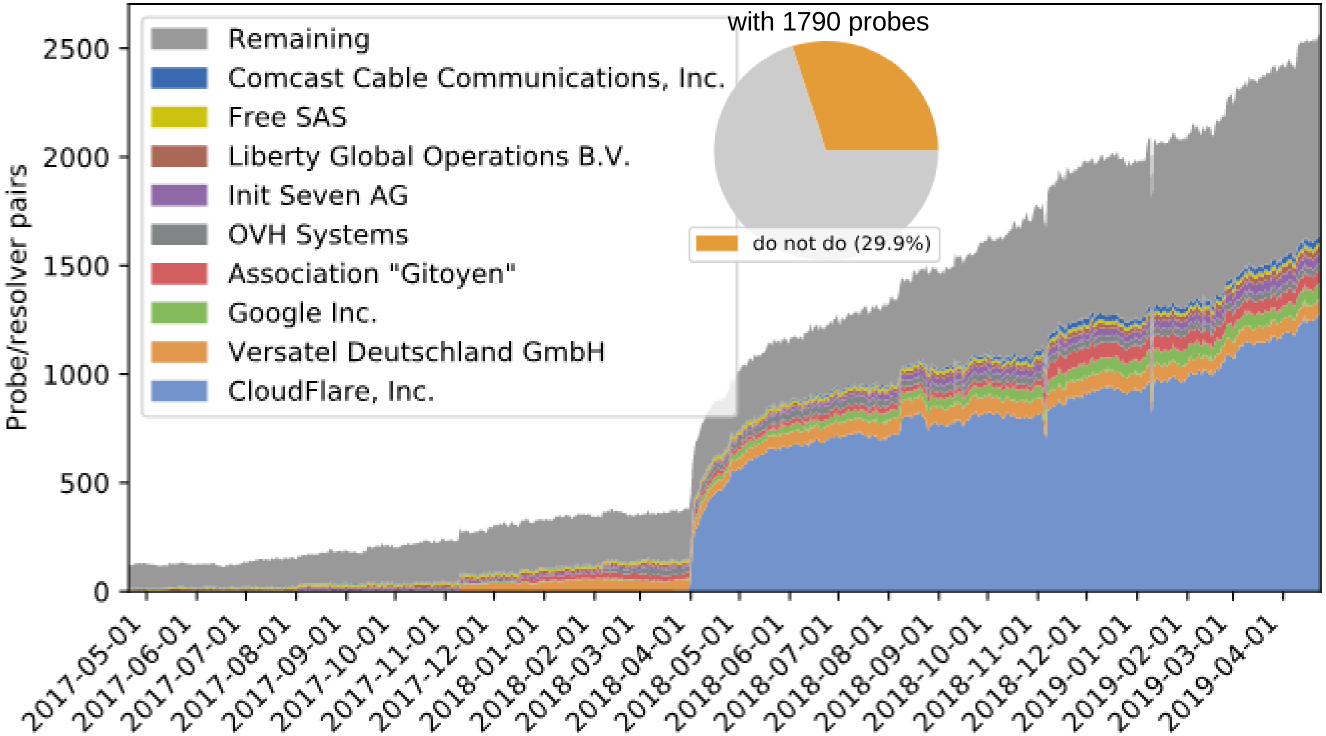
minimize data in queries – qname min

- With RFC7816 - DNS Query Name Minimisation



Privacy issues with DNS
minimize data in queries – qname min

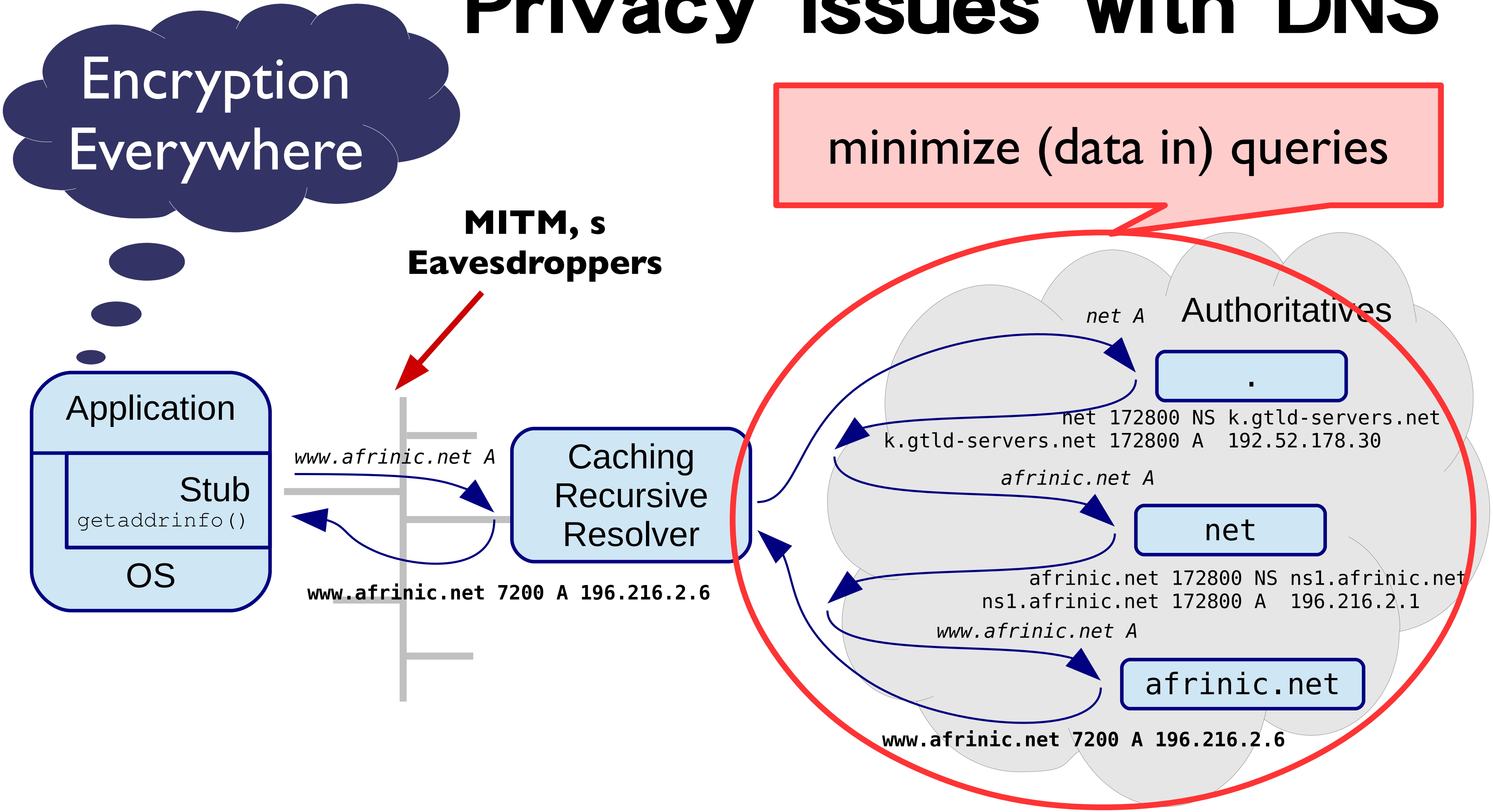
- RFC7816 - DNS Query Name Minimisation



DNSThought

ITHI: 20.6% measured at root

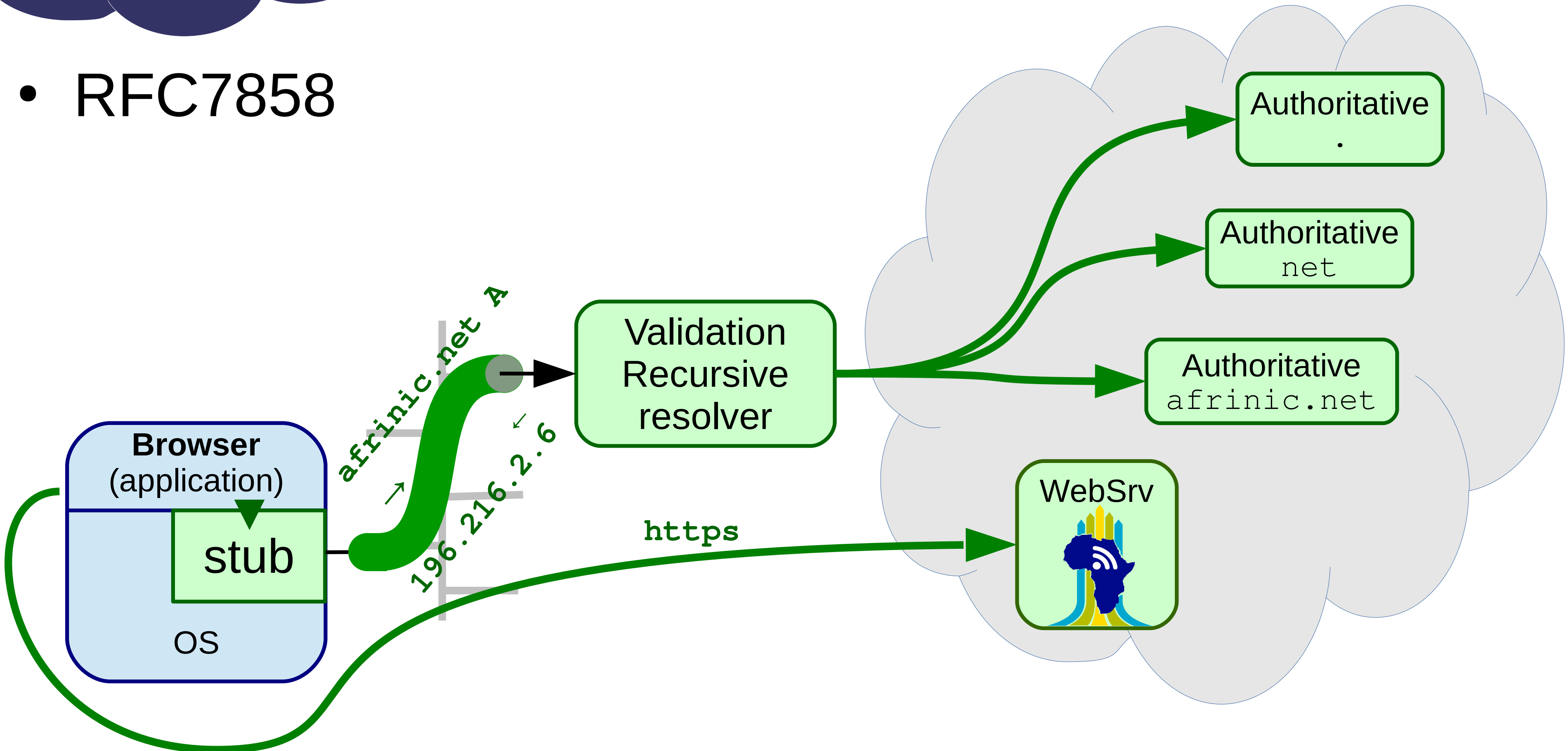
Privacy issues with DNS



Encryption Everywhere

Privacy issues with DNS
DNS over TLS (DoT)

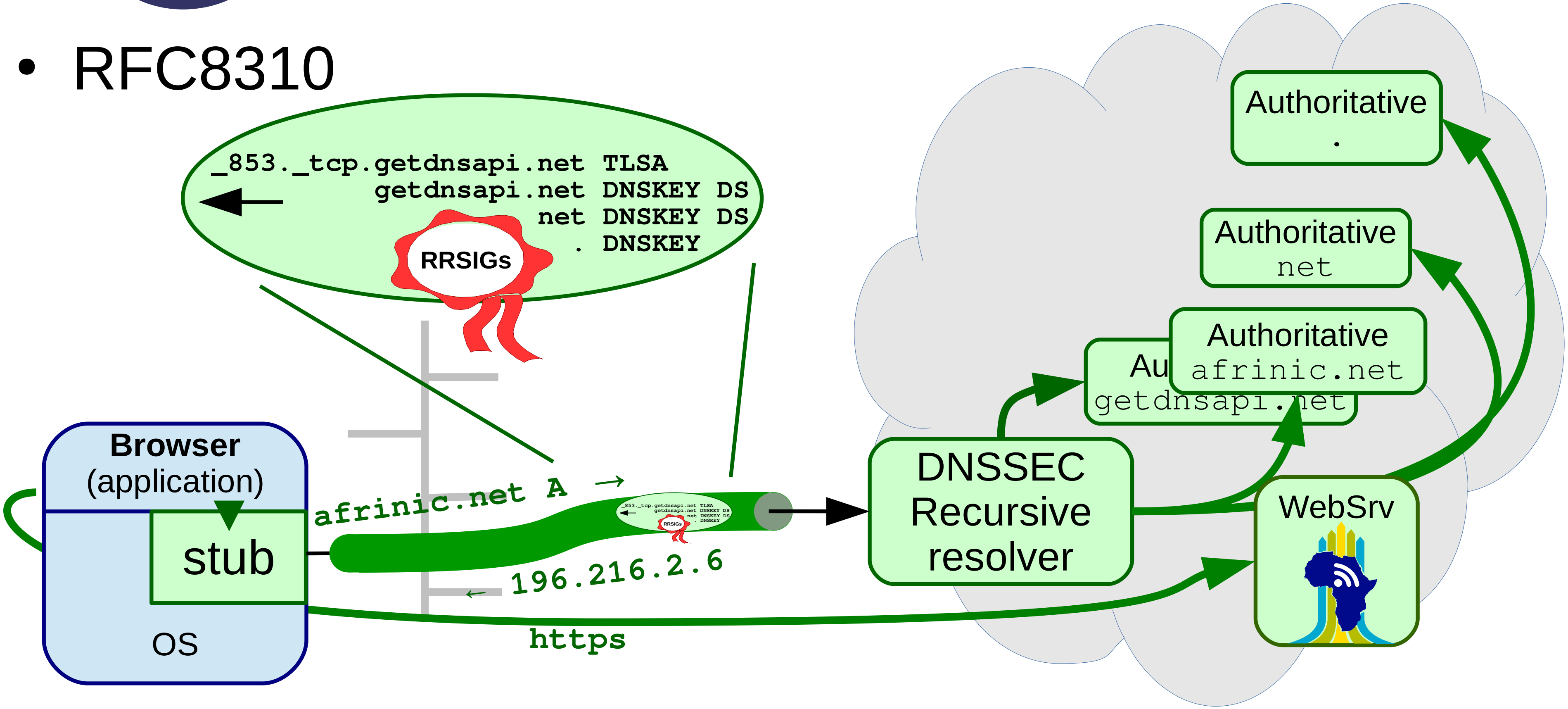
- RFC7858



Encryption Everywhere

Privacy issues with DNS
DNS over TLS (DoT)

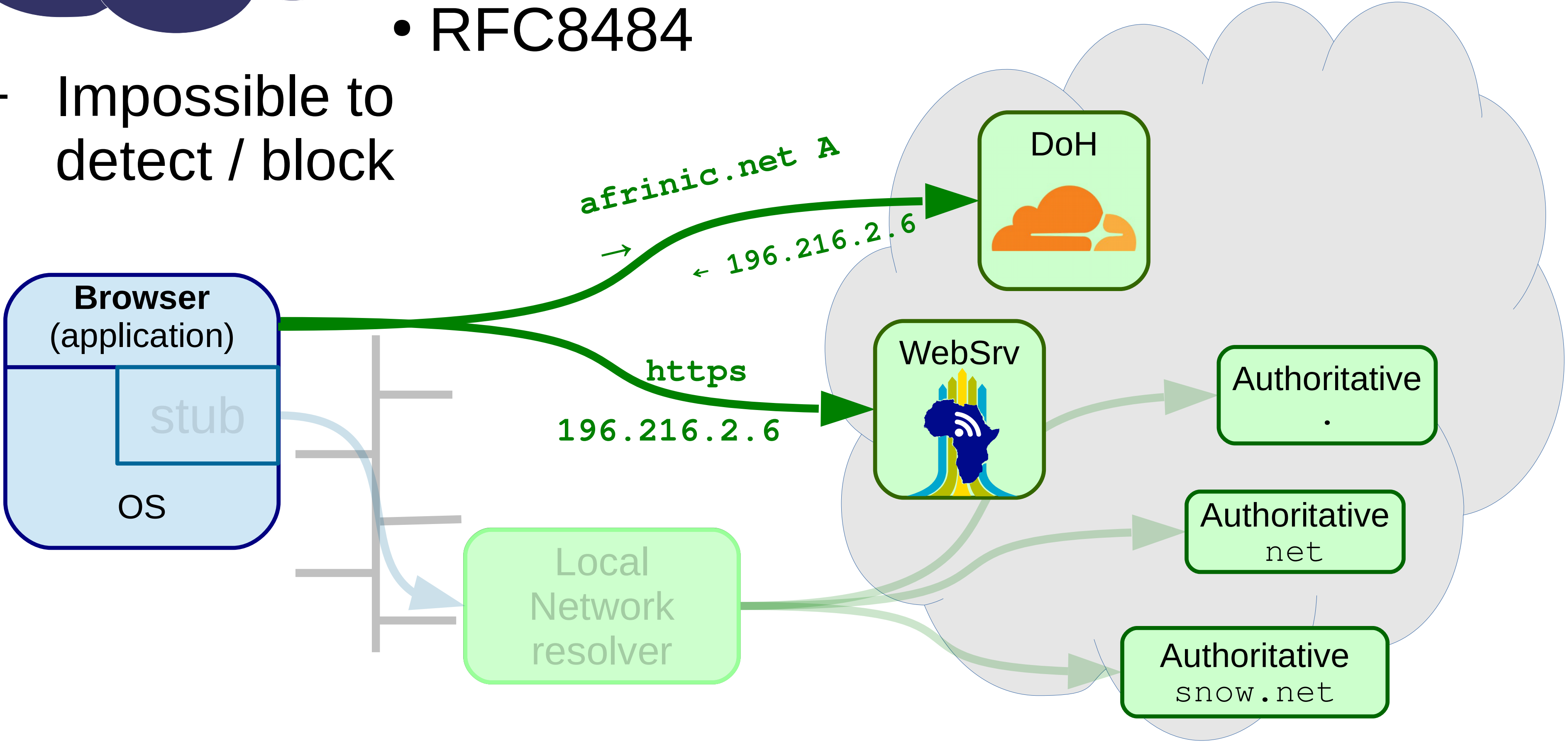
- RFC8310



Privacy issues with DNS

DNS over HTTPS (DoH)

- RFC8484
- \+ Impossible to detect / block

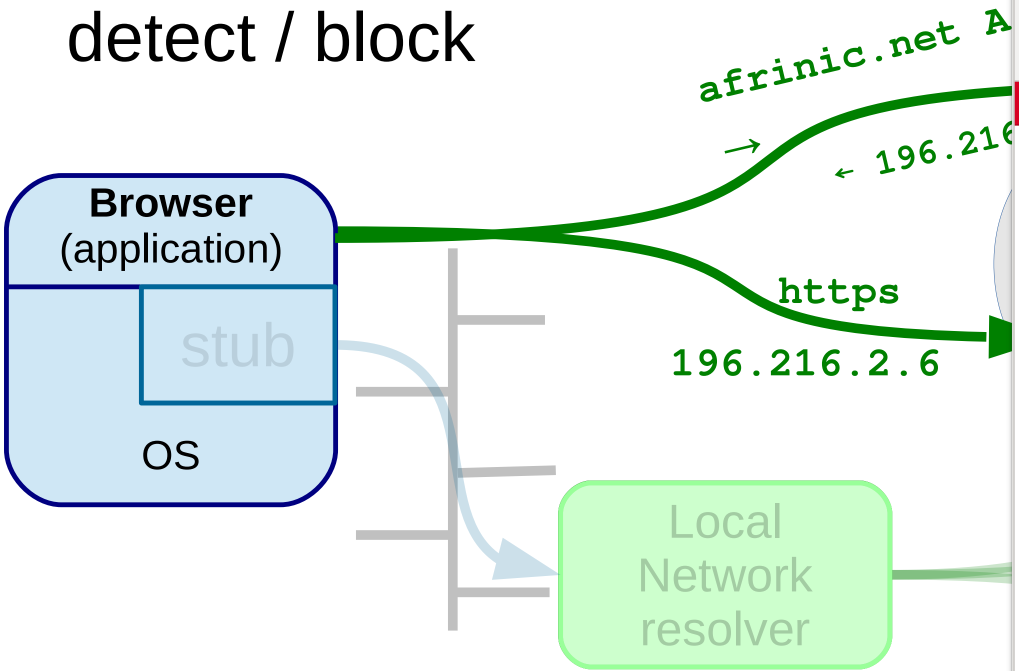


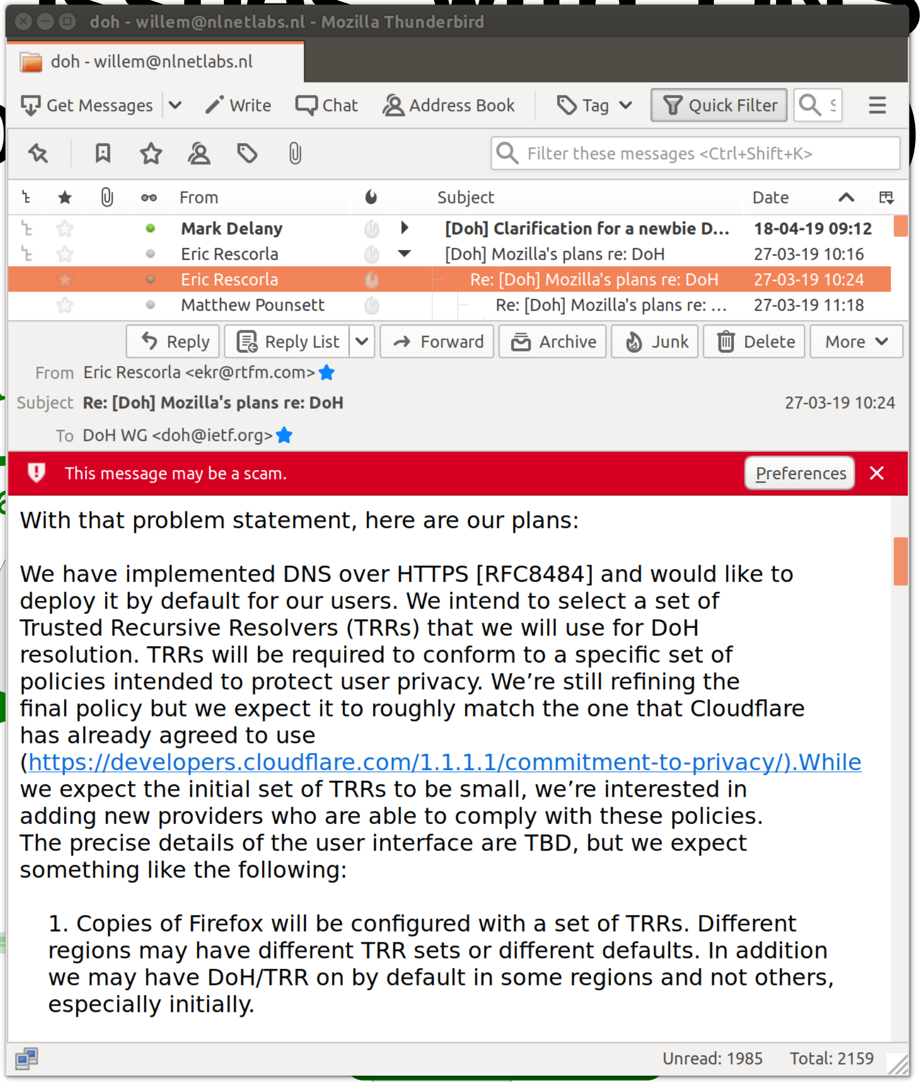
Encryption Everywhere

Privacy issues with DNS

DNS o

- RFC8484
- + impossible to detect / block





doh - willem@nlnetlabs.nl - Mozilla Thunderbird

doh - willem@nlnetlabs.nl

Get Messages | Write | Chat | Address Book | Tag | Quick Filter

Filter these messages <Ctrl+Shift+K>

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

Reply | Reply List | Forward | Archive | Junk | Delete | More

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. Preferences

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:

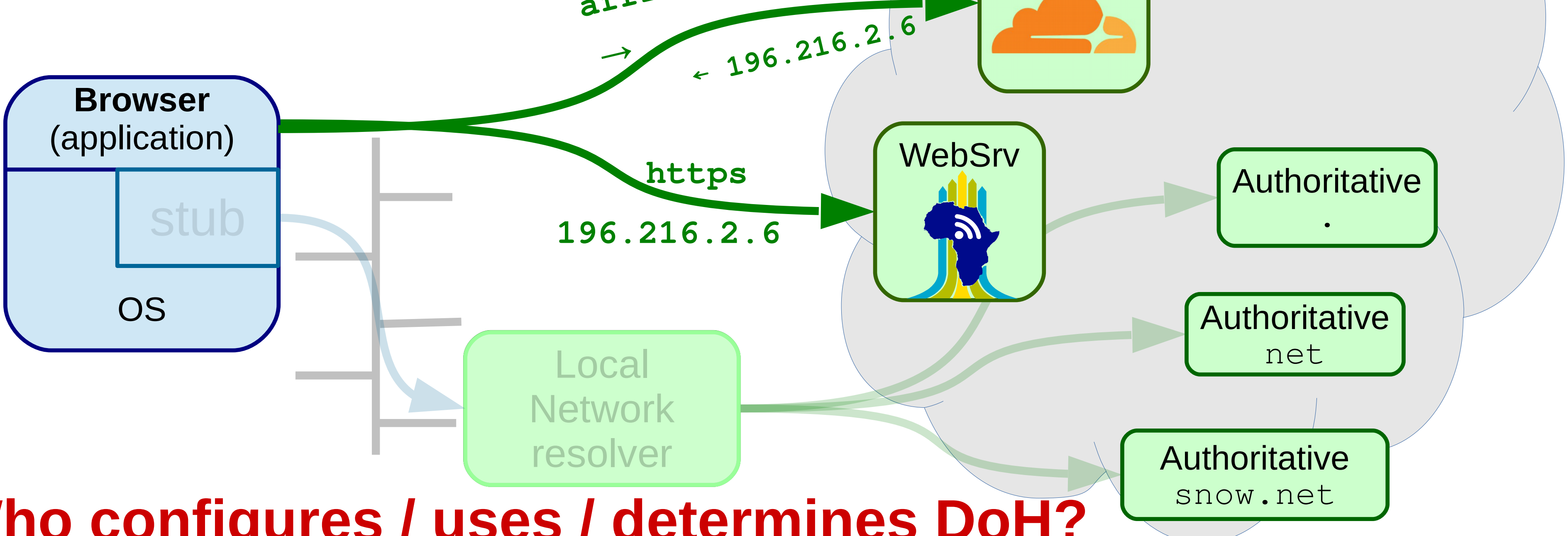
1. Copies of Firefox will be configured with a set of TRRs. Different regions may have different TRR sets or different defaults. In addition we may have DoH/TRR on by default in some regions and not others, especially initially.

Unread: 1985 Total: 2159

Encryption Everywhere

Privacy issues with DNS
DNS over HTTPS (DoH)

- RFC8484
- \+ Impossible to detect / block



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

DNS Measurements Hackathon Track
Topics and motivation

- How would centralized cloud provided DNS resolvers impact Internet in the African region?
- Does it have performance implications?
- Does it have other implications? (Political?)
- Is it beneficial and achievable to provide local DoT or DoH resolvers?
- How can this best be achieved/realized?

Measuring DNS and DoH Topics and motivation

- **Optimal DNS Latency**
  - Compare latency of probes resolvers to cloud resolvers
- **Resolver Jedi**
  - How local are probe resolvers?
    Do they cross country borders?
- **Run your own DoH and/or DoT server**
  - Howto and evaluation of different possibilities
- **DoH with DNS Messages in JSON**
  - Provide DoH which is actually usable for applications
- **Your Idea**

Measuring DNS and DoH
Common resources

- https://hackathon.internetsummitafrica.org/
- Subscribe to Slack hackathon@AIS2019 workspace
  #measuring-dns-and-doh channel Invite link
- Linux command line available with VM on NUC
- ssh to it with OpenSSH or
  putty: https://www.chiark.greenend.org.uk/~sgtatham/putty/

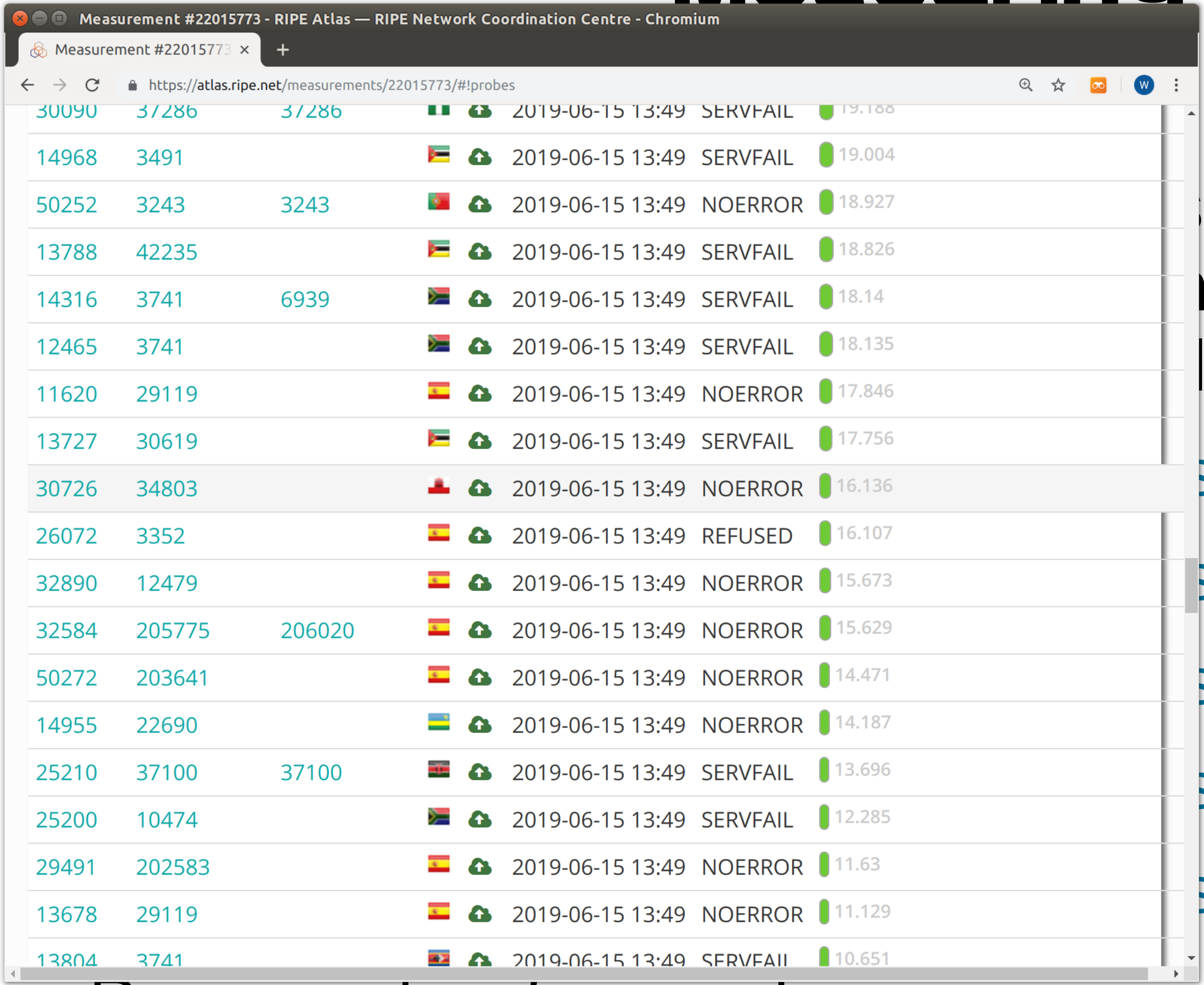
Measuring DNS and DoH Optimal DNS Latency

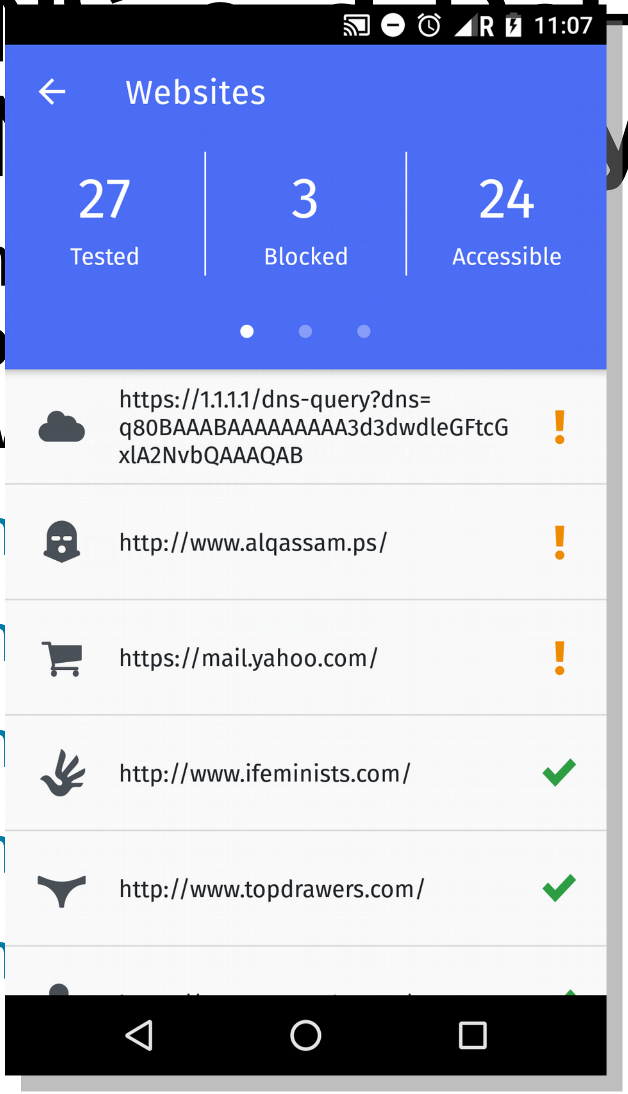
- High level overview: - https://atlas.ripe.net/landing/about/
- Webinar:
  - https://www.ripe.net/support/training/webinars/webinar-recordings/webinar-ripe-atlas
- Documentation:
  - https://atlas.ripe.net/docs/
- Voucher for 5,000,000 credits! Posted on the Slack channel.
  - Thank you Lia! ♥

Measuring DNS and DoH
Optimal DNS Latency

- `i.root-servers.net A` query measurement to 1.1.1.1, 8.8.8.8, 9.9.9.9 **from Africa region probe**s made during Internet Measurements Workshop last weekend
  - 1.1.1.1 https://atlas.ripe.net/measurements/22015773/
  - 8.8.8.8 https://atlas.ripe.net/measurements/22015800/
  - 9.9.9.9 https://atlas.ripe.net/measurements/22015801/
  - Local 1st https://atlas.ripe.net/measurements/22015822/
  - Local 2nd https://atlas.ripe.net/measurements/22015846/
- Reuse probes from earlier measurement

Measuring DN… DN…





- Reuse probes from earlier measurement

Measuring DNS and DoH
Optimal DNS Latency

- WHAT IS GOING ON WITH 1.1.1.1 IN THE AFRICA?
- Is this the same worldwide?
- Where are those measurements going?
  (traceroute to 1.1.1.1)
- Are DNS queries intercepted?
  - send `whoami.akamai.net A` to 8.8.8.8
  - Result should be any of list published at `locations.publicdns.goog. TXT`

Measuring DNS and DoH Optimal DNS Latency

- WHAT IS GOING ON WITH 1.1.1.1 IN THE AFRICA?
- Does DNS-over-TLS to 1.1.1.1 give same results
- **Challenge!**
  DNS-over-TLS available, but not with web interface
- https://atlas.ripe.net/docs/api/v2/reference/
- https://ripe-atlas-cousteau.readthedocs.io/en/latest/
- https://ripe-atlas-tools.readthedocs.io/en/latest/

Measuring DNS and DoH Resolver Jedi

- Adapt IPX-country-jedi for traceroutes to probe IP address
- https://github.com/emileaben/ixp-country-jedi
- Warning!
  Probe resolvers are only mentioned in measurement results

Measuring DNS and DoH
Run your own DoH and/or DoT server

- Try to get a client setup and working
  - https://www.bleepingcomputer.com/news/software/mozilla-firefox-expands-dns-over-https-doh-test-to-release-channel/
  - https://github.com/bromite/bromite/wiki/Enabling-DNS-over-HTTPS
  - https://dnsprivacy.org/wiki/display/DP/DNS+Privacy+Clients
- Test if it is working:
  - https://1.1.1.1/help

Measuring DNS and DoH
Run your own DoH and/or DoT server

- Setup server software on a VM on the NUC
- Resources:
  - Current state of software for DoH and DoT *by Carsten Strotmann*
  - https://doh.defaultroutes.de/implementations.html
  - Operational Experience providing DoH Service

Measuring DNS and DoH
DoH with DNS messages in JSON

- Setup server software on a VM on the NUC
- RFC8427

Measuring DNS and DoH

Your Idea

Measuring DNS and DoH

- Introduction round
  - Who are you?
  - Where are you from?
  - Day job?
  - Experience?
    - Command line? Python? Hobbies?

Happy birthday Gervin!