

DNS Privacy

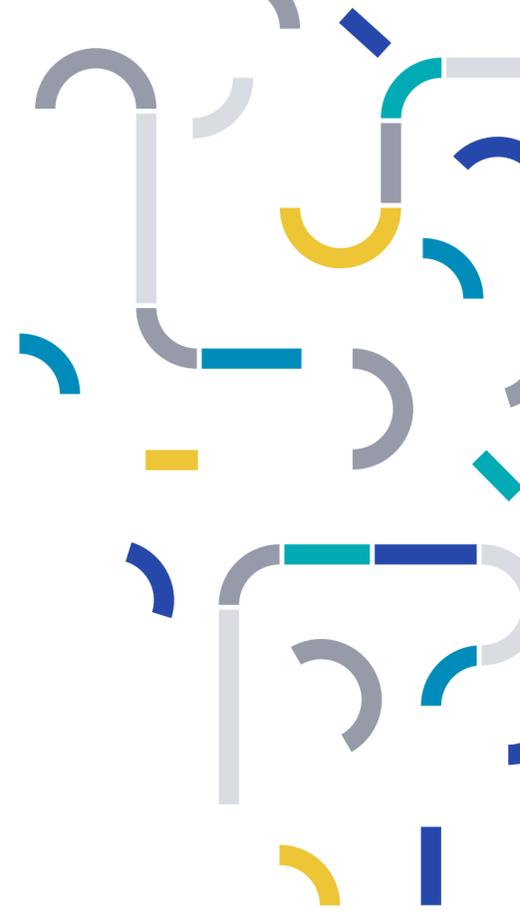
Can DNS-over-HTTPS fix it?

dnsimple

Automating domain management since 2010

 OleMchls  ole@dnsimple.com







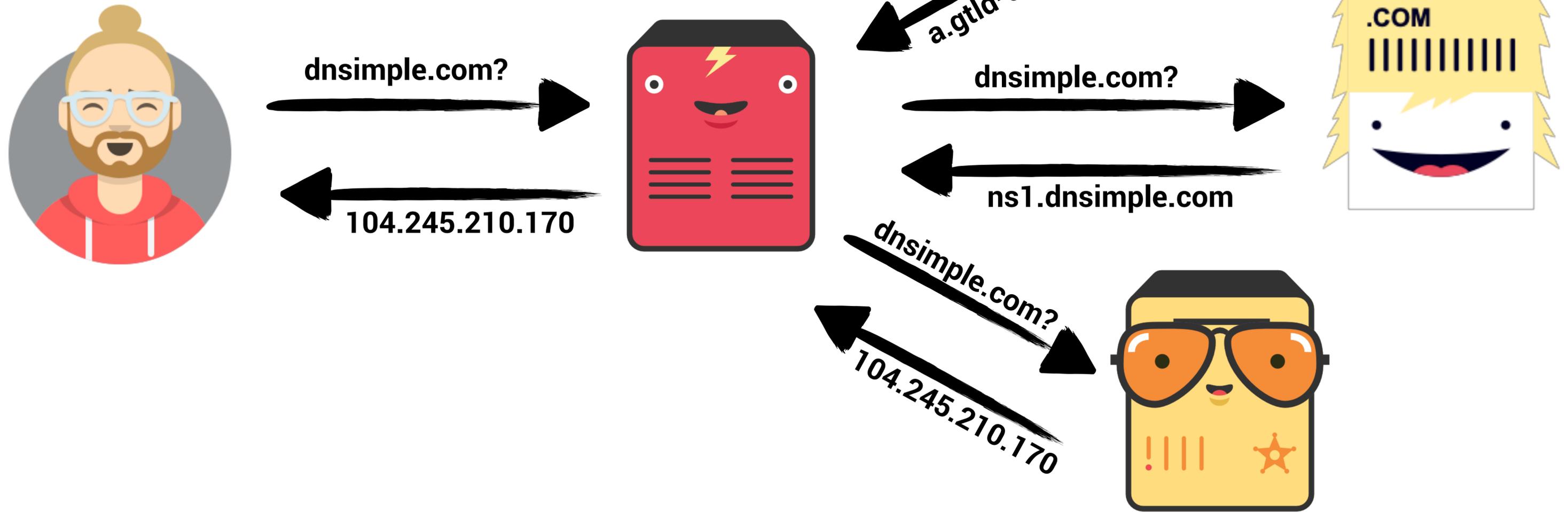
DNS over HTTPS



DNS

DNS Concepts

DNS Concepts

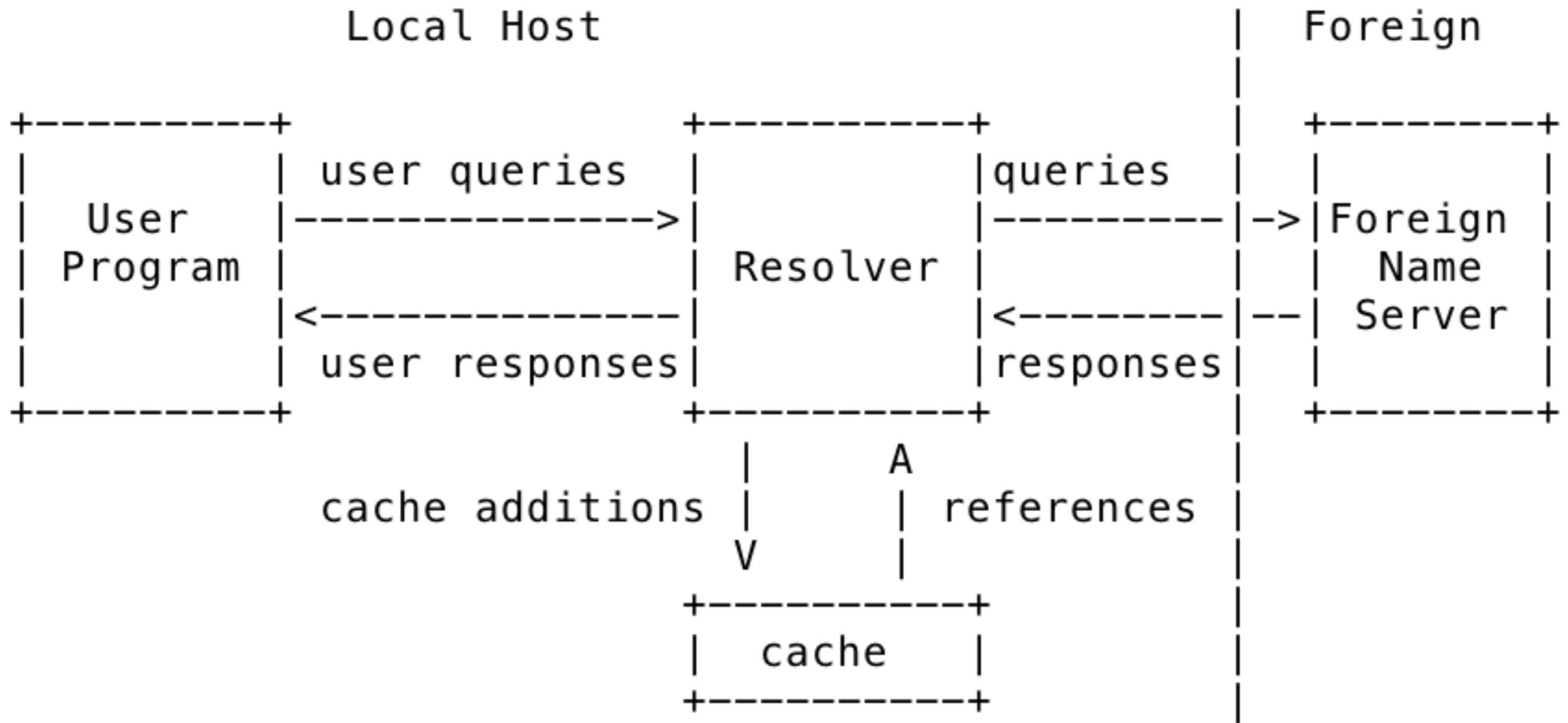


DNS Implementation

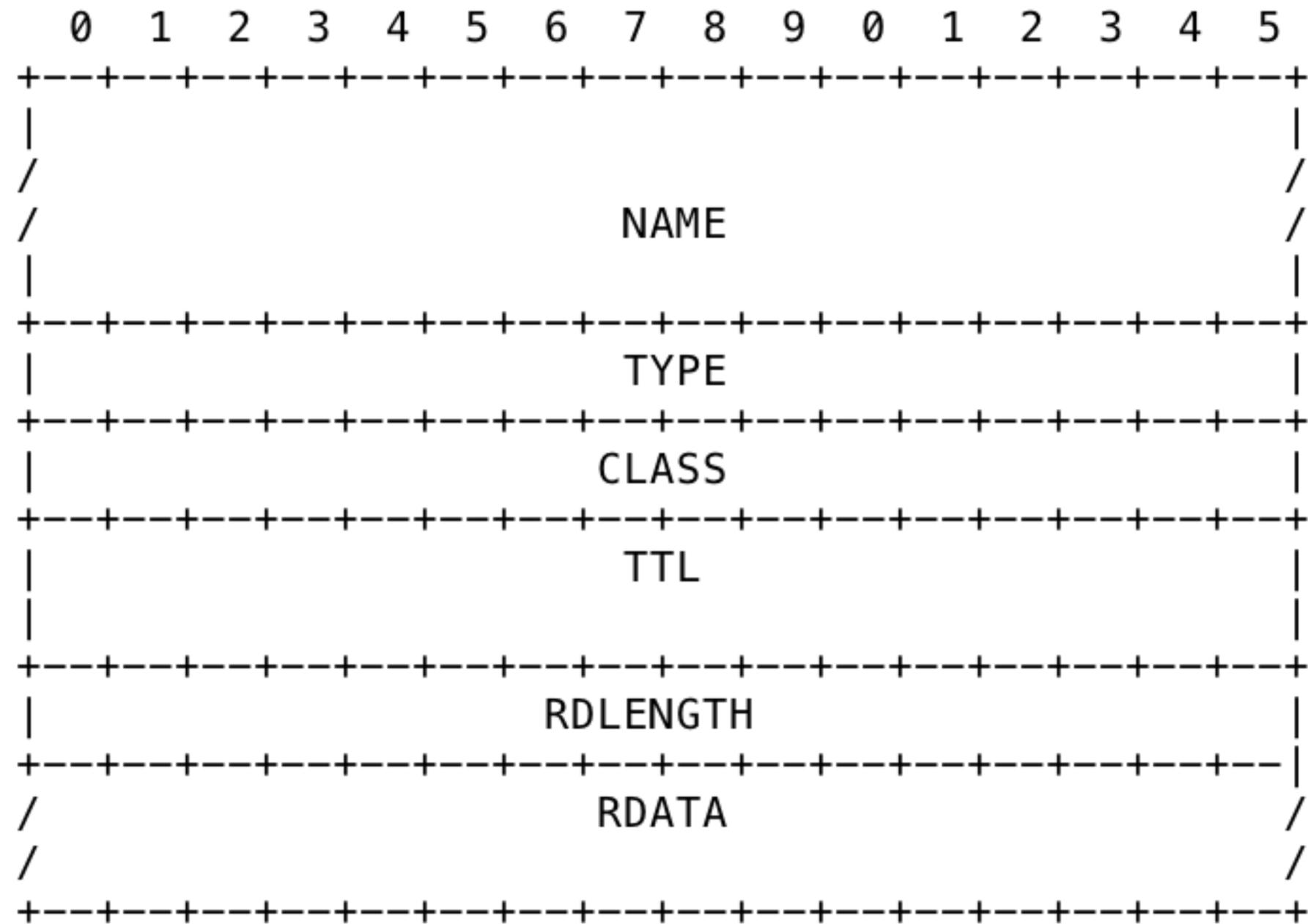
RFC 1035

DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION

🔍 DNS Implementation - Flow



DNS Implementation - Resource Record



DNS Implementation - Messages

+-----+		
	Header	
+-----+		
	Question	the question for the name server
+-----+		
	Answer	RRs answering the question
+-----+		
	Authority	RRs pointing toward an authority
+-----+		
	Additional	RRs holding additional information
+-----+		

DNS Transport

What's DNS transport layer?

 **TCP**

 **UDP**

UDP

Mostly UDP

Mostly UDP ... unless it's TCP



What's wrong with that?

Flaws

```
$~ traceroute 8.8.8.8
```

```
traceroute to 8.8.8.8 (8.8.8.8), 64 hops max, 52 byte packets
```

```
1 fritz.box (192.168.178.1)  2.671 ms  2.655 ms  1.889 ms
2 84.46.106.85 (84.46.106.85)  3.423 ms  4.960 ms  8.916 ms
3 b10.bibo.ipv4.wtnet.de (84.46.106.84)  4.002 ms  5.058 ms  4.091
4 84.46.110.255 (84.46.110.255)  3.619 ms  9.379 ms  6.519 ms
5 108.170.253.33 (108.170.253.33)  4.241 ms
  108.170.253.65 (108.170.253.65)  4.570 ms
  108.170.253.33 (108.170.253.33)  3.912 ms
6 209.85.244.219 (209.85.244.219)  4.729 ms
  216.239.43.123 (216.239.43.123)  4.259 ms
  209.85.244.219 (209.85.244.219)  13.039 ms
7 google-public-dns-a.google.com (8.8.8.8)  4.084 ms  4.068 ms  5.
```



All of these parties can:

1. Intercept
2. Analyze
3. Manipulate

Flaws

```
$~ traceroute 8.8.8.8
```

```
traceroute to 8.8.8.8 (8.8.8.8), 64 hops max, 52 byte packets
```

```
1 fritz.box (192.168.178.1)  2.671 ms  2.655 ms  1.889 ms
2 84.46.106.85 (84.46.106.85)  3.423 ms  4.960 ms  8.916 ms
3 b10.bibo.ipv4.wtnet.de (84.46.106.84)  4.002 ms  5.058 ms  4.091
4 84.46.110.255 (84.46.110.255)  3.619 ms  9.379 ms  6.519 ms
5 108.170.253.33 (108.170.253.33)  4.241 ms
  108.170.253.65 (108.170.253.65)  4.570 ms
  108.170.253.33 (108.170.253.33)  3.912 ms
6 209.85.244.219 (209.85.244.219)  4.729 ms
  216.239.43.123 (216.239.43.123)  4.259 ms
  209.85.244.219 (209.85.244.219)  13.039 ms
7 google-public-dns-a.google.com (8.8.8.8)  4.084 ms  4.068 ms  5.
```

Flaws

```
$~ traceroute 8.8.8.8
```

```
traceroute to 8.8.8.8 (8.8.8.8), 64 hops max, 52 byte packets
```

```
1  fritz.box (192.168.178.1)  2.671 ms  2.655 ms  1.889 ms
2  84.46.106.85 (84.46.106.85)  3.423 ms  4.960 ms  8.916 ms
3  b10.bibo.ipv4.wtnet.de (84.46.106.84)  4.002 ms  5.058 ms  4.091
4  84.46.110.255 (84.46.110.255)  3.619 ms  9.379 ms  6.519 ms
5  108.170.253.33 (108.170.253.33)  4.241 ms
   108.170.253.65 (108.170.253.65)  4.570 ms
   108.170.253.33 (108.170.253.33)  3.912 ms
6  209.85.244.219 (209.85.244.219)  4.729 ms
   216.239.43.123 (216.239.43.123)  4.259 ms
   209.85.244.219 (209.85.244.219)  13.039 ms
7  google-public-dns-a.google.com (8.8.8.8)  4.084 ms  4.068 ms  5.
```

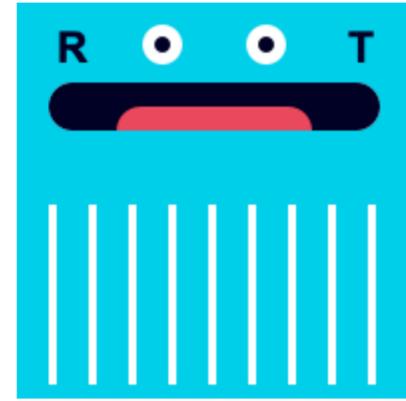
🔥 Flaws



dnsimple.com?
104.245.210.170



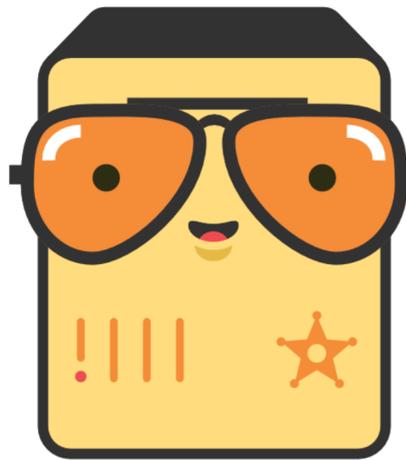
.com?
a.gtld-servers.net



dnsimple.com?
ns1.dnsimple.com

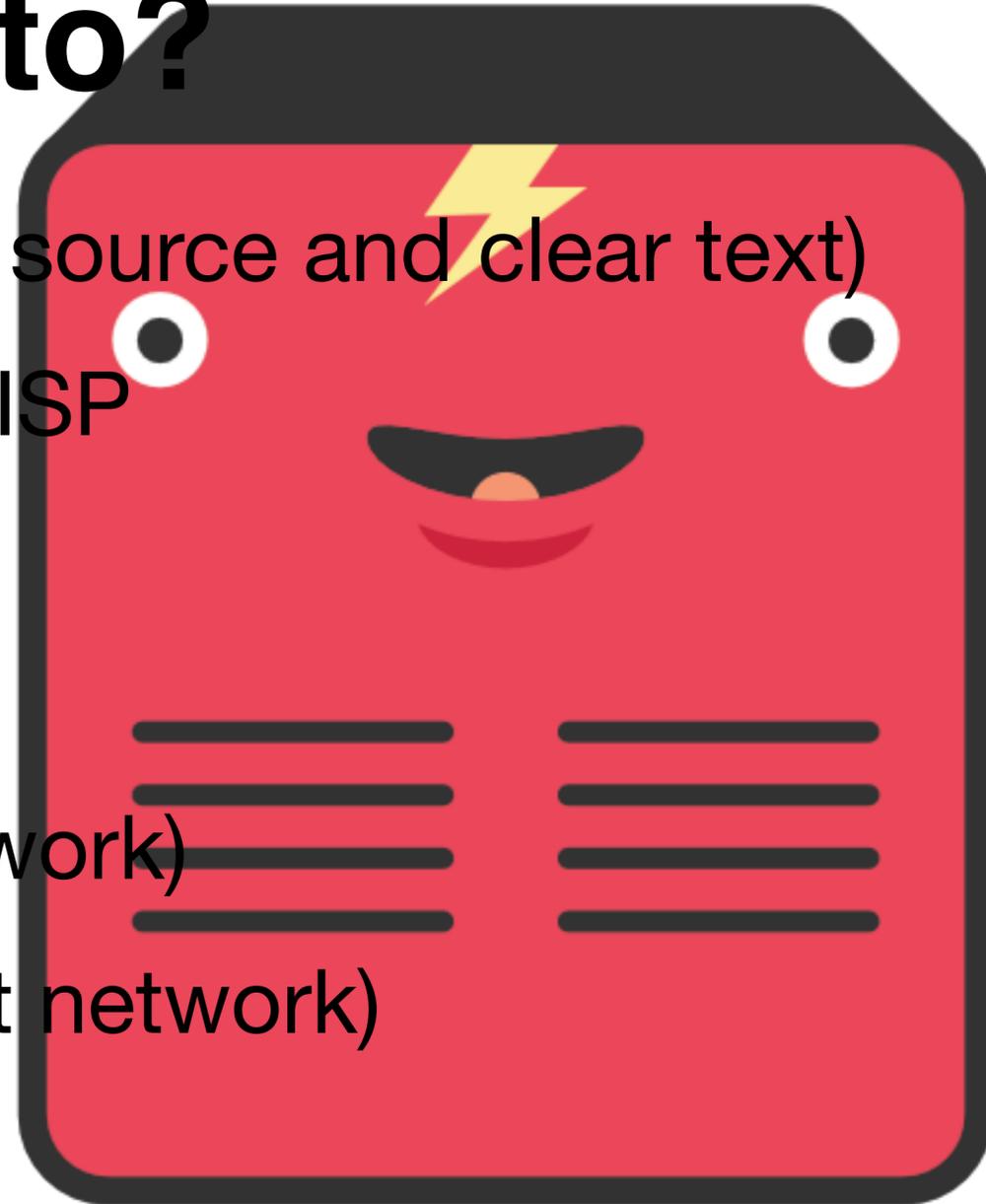


dnsimple.com?
104.245.210.170



Who to talk to?

- 👉 DHCP (unverified source and clear text)
 - 👉 Hopefully, your ISP
- 👉 User configured
 - 👉 8.8.8.8 (Ad Network)
 - 👉 1.1.1.1 (Content network)



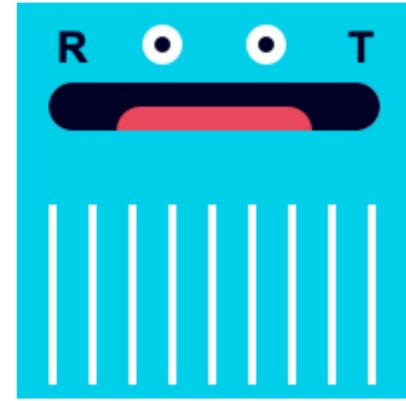
🔥 Flaws



dnsimple.com?
104.245.210.170



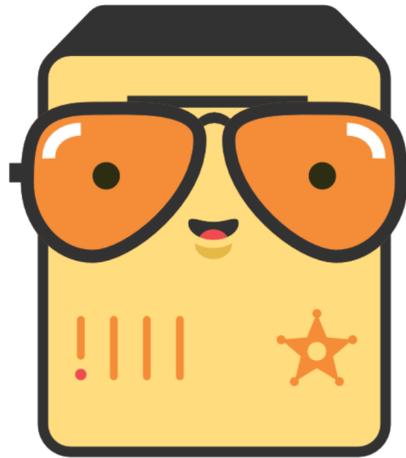
.com?
a.gtld-servers.net



dnsimple.com?
ns1.dnsimple.com



dnsimple.com?
104.245.210.170



🔥 Flaws



ICANN DNS Root servers (managing names)

a.root-servers.net	VeriSign, Inc.
b.root-servers.net	University of Southern California (ISI)
c.root-servers.net	Cogent Communications
d.root-servers.net	University of Maryland
e.root-servers.net	NASA (Ames Research Center)
f.root-servers.net	Internet Systems Consortium, Inc.
g.root-servers.net	US Department of Defense (NIC)
h.root-servers.net	US Army (Research Lab)
i.root-servers.net	Netnod
j.root-servers.net	VeriSign, Inc.
k.root-servers.net	RIPE NCC
l.root-servers.net	ICANN
m.root-servers.net	WIDE Project

TECHNOLOGY

IS ALWAYS

POLITICAL!





Turkish Protesters Are Spray Painting "8.8.8.8" and "8.8.4.4" On Walls — Here's What It Means

By Matt Essert | March 22, 2014



<https://mic.com/articles/85987/turkish-protesters-are-spray-painting-8-8-8-8-and-8-8-4-4-on-walls-here-s-what-it-means#.pqVa0kaGq>

China's great firewall and the war to control the internet

The West thinks China's internet is all about firewalls and censorship, but as a new book shows, the battle for control is full of dubious motives

TECHNOLOGY 12 March 2019



<https://www.newscientist.com/article/mg24132210-400-chinas-great-firewall-and-the-war-to-control-the-internet/>

Regulation

Inside the giant German protest trying to bring down Article 13

Article 17 (formerly Article 13) could become law this week. In Germany, protestors beg to differ



By **MORGAN MEAKER**

Tuesday 26 March 2019



r-internets/

You have nothing to hide?

General Content Warning



You have nothing to hide?

- 👉 aidsinfo.nih.gov
- 👉 suicidepreventionlifeline.org
- 👉 abortion-clinics.eu
- 👉 thercc.org (Rape Crisis Center)
- 👉 nationaleatingdisorders.org
- 👉 womenshelter.org
- 👉 ptsdalliance.org
- 👉 hartziv.org
- 👉 bkms-system.net (BaFin whistle blower portal)
- 👉 verdi.de



DNScrypt

No Multiplexing
No Connection Reuse
No IETF Project
No RFC



DNScrypt



DNS-over-TLS *DoT*

Transport Layer Security

TLS



TCP only?

RFC 4347

Datagram Transport Layer Security

 **This also has Flaws**

Also announced via DHCP

Runs on :853

Only pipelining

Disabled by default



DNS-over-HTTPS

Just looks like HTTP(S)



What if google.com could answer DNS queries?

DNS-over-HTTPS

```
$ sudo tcpdump -i any port 53 or port 443 -w pcap -s 0 &
tcpdump: listening on any, link-type LINUX_SLL (Linux cooked), capture size 262144 bytes

$ curl -s -H 'Host: dns.google.com' 'https://google.com/resolve?name=www.powerdns.com&type=A'
{"Status": 0,"TC": false,"RD": true,"RA": true,"AD": true,"CD": false,"Question":[
{"name": "www.powerdns.com.", "type": 1}], "Answer": [
{"name": "www.powerdns.com.", "type": 1, "TTL": 3485, "data":
"188.166.104.92"}]}

$ fg
^C56 packets captured

$ strings pcap | grep -i dns
$
```



Bert Hubert 
@PowerDNS_Bert



Undetectable and unblockable DNS has arrived. This resolves [google.com](https://www.google.com) & asks for [google.com](https://www.google.com) SNI. Only once encrypted, is the 'Host: [dns.google.com](https://www.google.com)' header sent. This DNS query can't be detected or blocked without MiTM or blocking all of Google.

♡ 140 5:20 PM - Feb 7, 2019

💬 92 people are talking about this



Implementation



RFC 8484

DNS Queries over HTTPS (DoH)



DNS-over-HTTPS

GET /resolve?name=dnsimple.com

host = google.com

:status = 200

content-type = application/dns-message

content-length = 61

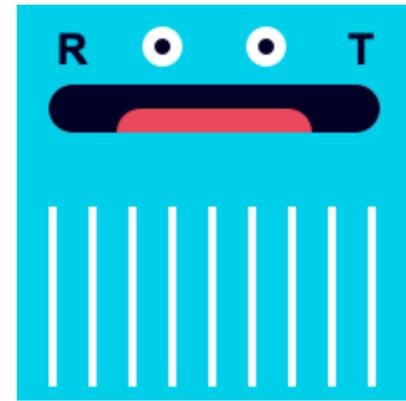
cache-control = max-age=3709

```

+-----+
| <61 bytes represented by the following hex encoding>
+-----+ 01 00 00 00 00 03 77 77 77
| 07 65 75 01 00 70 6c | the question for the name server
+-----+
| 01 c0 0c 00 1c 00 01 | RRs answering the question
| b8 ab cd 00 12 00 01 |
+-----+
| Authority | RRs pointing toward an authority

```

DNS-over-HTTPS





Problems of DNS-over-HTTPS

Problems of DNS-over-HTTPS

Tracking

Resolver still sees every query

Problems of DNS-over-HTTPS

All of HTTP

Centralisation of DNS

 Problems of DNS-over-HTTPS

DNS-over-Cloud *DoC*

WHO DO YOU TRUST?

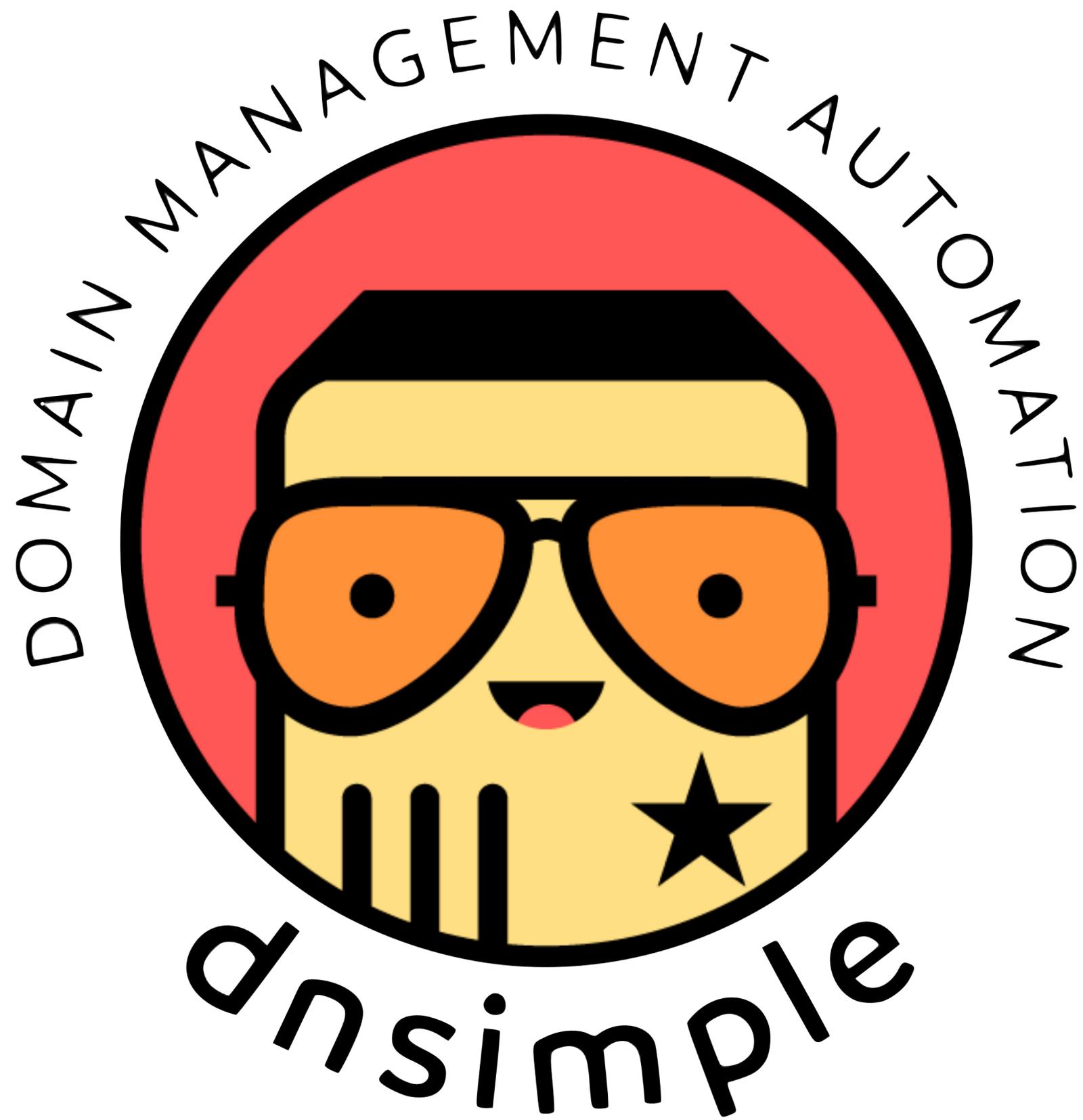




Ole Michaelis

 OleMchls

 ole@dnsimple.com





Questions?

 **OleMchls**

 **ole@dnssimple.com**



Sources and Kudos

1. <https://tools.ietf.org/html/rfc1035>
2. <http://dspace.mit.edu/bitstream/handle/1721.1/6353/AIM-628.pdf?sequence=2>
3. <https://wiki.mozilla.org/Security/DOH-resolver-policy>
4. https://datatracker.ietf.org/doc/draft-ietf-doh-resolver-associated-doh/?include_text=1
5. <https://tools.ietf.org/html/rfc8484#section-5.2>
6. <https://blog.apnic.net/2019/04/08/opinion-what-does-doh-really-mean-for-privacy/>
7. <https://blog.powerdns.com/2019/02/07/the-big-dns-privacy-debate-at-fosdem/>
8. https://video.fosdem.org/2019/Janson/dns_over_http.mp4