Einführung in DNS Privacy Protokolle

PrivacyWeek 2019

Foundation for Applied Privacy

Foundation for Applied Privacy

- Non-profit Privacy Infrastruktur Provider
- Privacy Enhancing Technology Dienste für die Öffentlichkeit
- 2018 gegründet
- Top 3 Tor Exit Relay Operator (weltweit)
- > 2500 Terabyte monatlicher Netzwerkverkehr
- AS 208323

Foundation for
Applied Privacy

Vereinszweck

- Betrieb kostenlos nutzbarer **technischer Privacy Infrastruktur** für die Öffentlichkeit

- Förderung von freier Software für:
  - **Sichere Kommunikation**
  - **Schutz der Privatsphäre**

Foundation for Applied Privacy

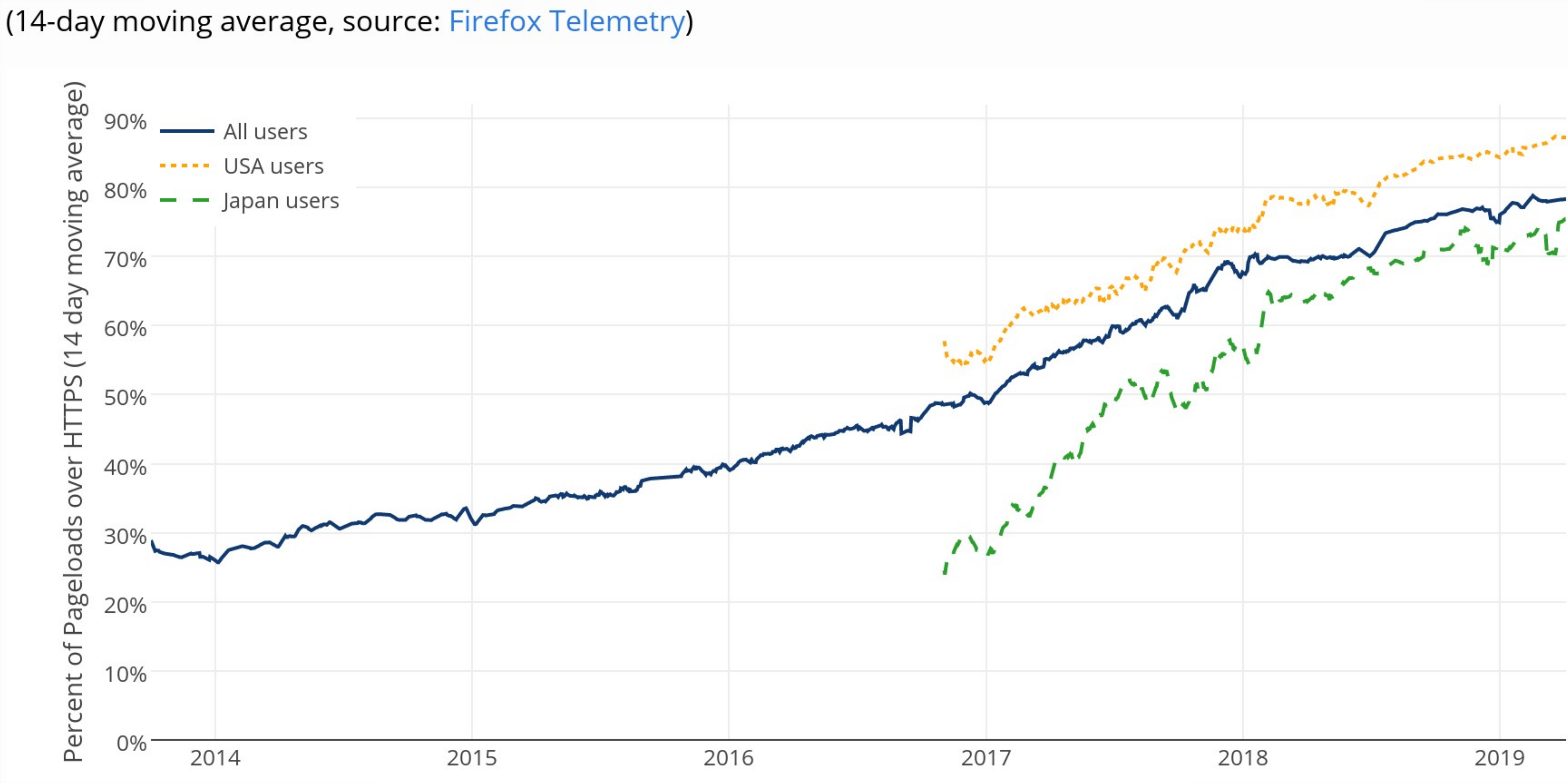
Ziele dieses Vortrags

- Welches Problem lösen DNS Privacy Protokolle?
- Was ist DoT und DoH?
- Welche Software unterstützt dies Protokolle?
- Wie kann ich DoT und DoH verwenden?

Foundation for Applied Privacy

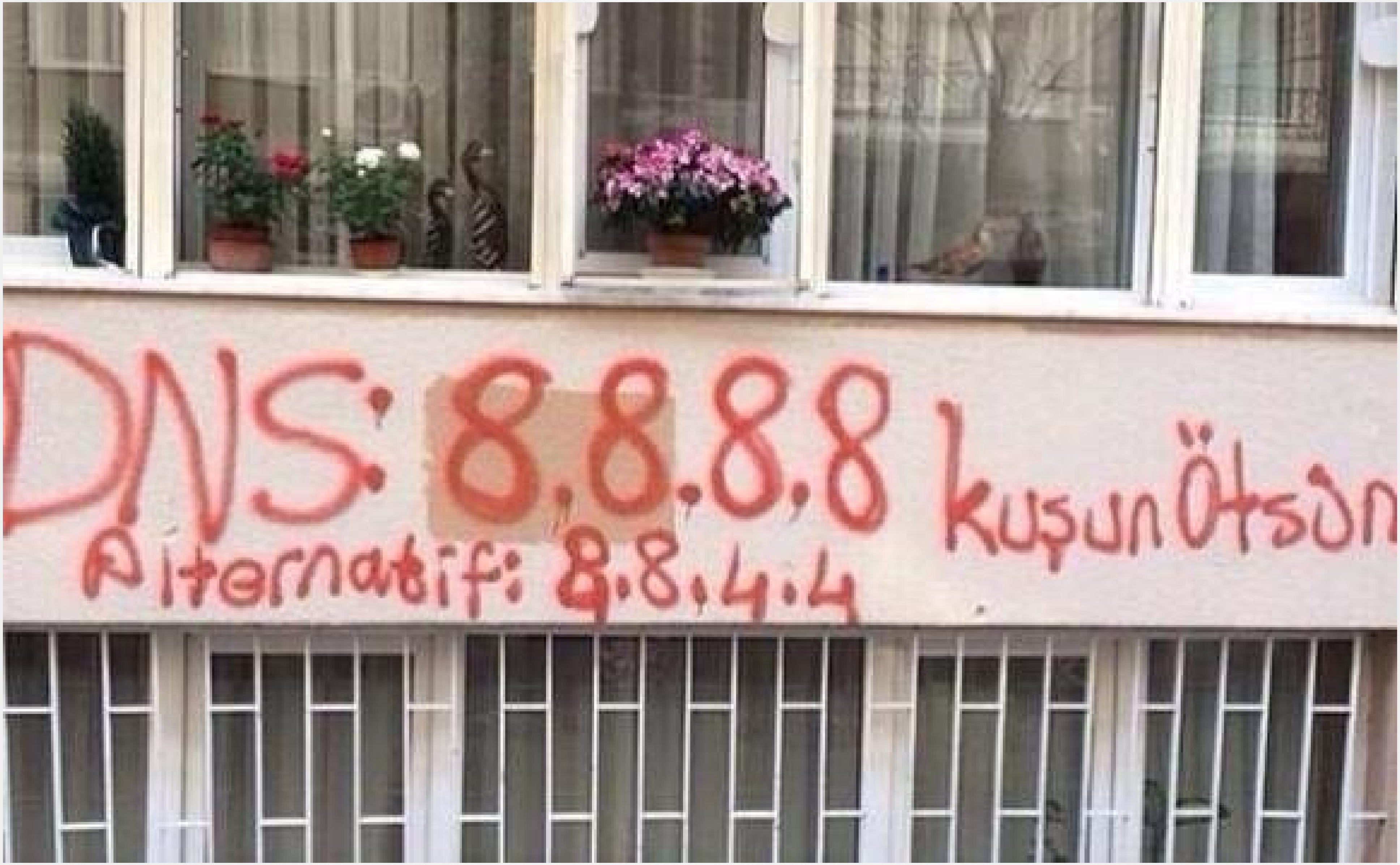
Warum DNS Privacy?

Foundation for Applied Privacy



(14-day moving average, source: Firefox Telemetry)

Foundation for Applied Privacy

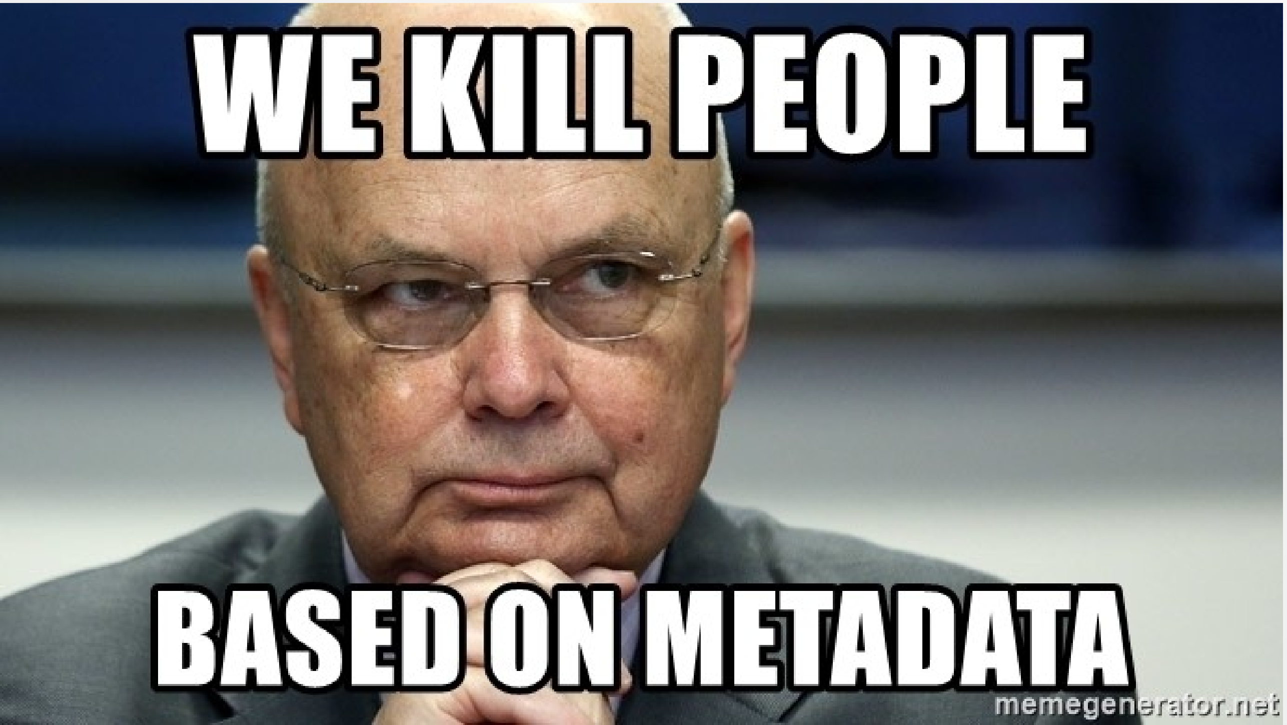

DNS: 8.8.8.8 kuşun Ötsün
Alternatif: 8.8.4.4

Ziel

Schutz von Metadaten (Hostname)

Warum ist das wichtig?

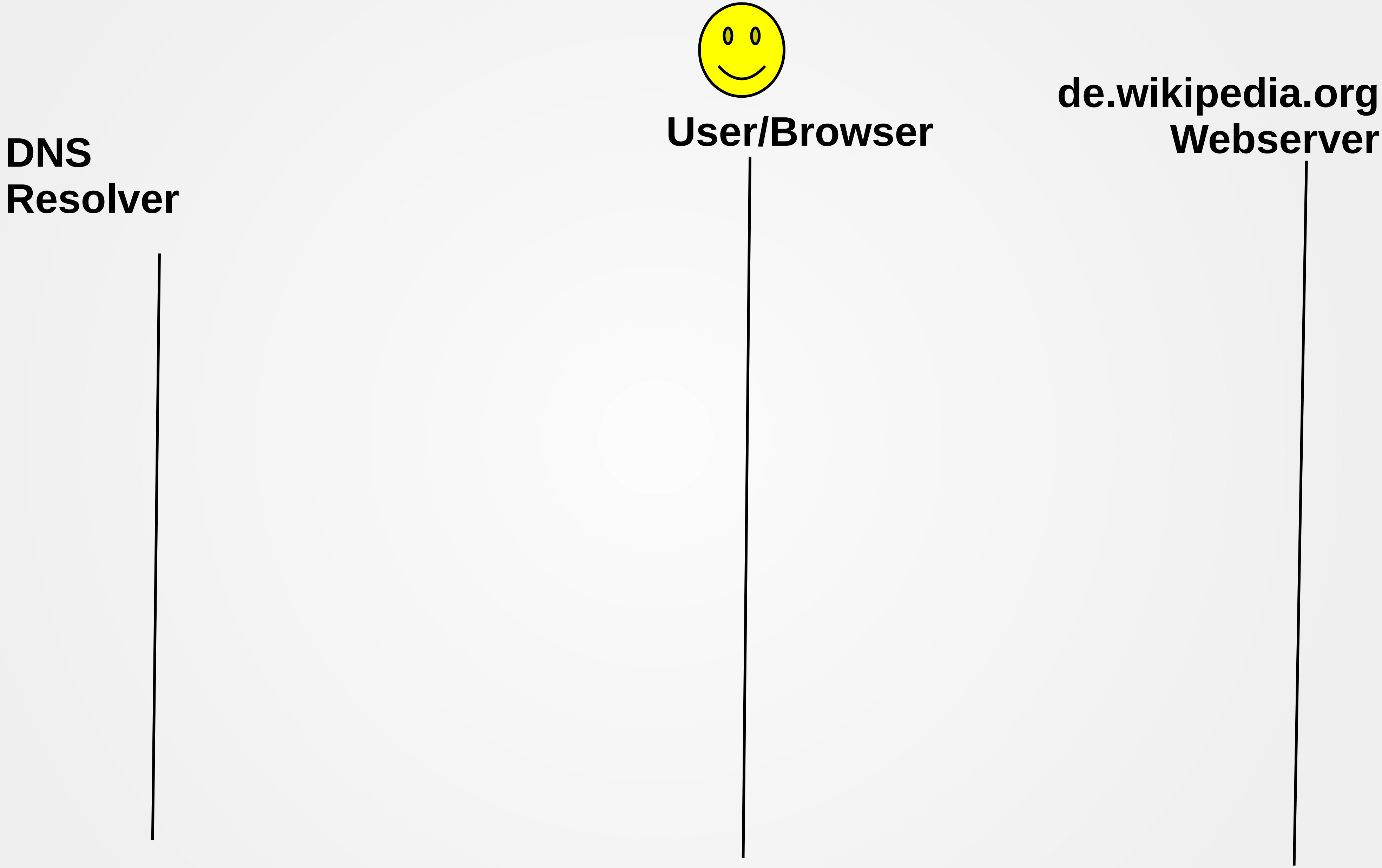
- Ermöglicht privateres Internet surfen
- Erschwert Zensur
- Erschwert Massenüberwachung



Foundation for Applied Privacy

Warum ist das aktuell noch nicht möglich?

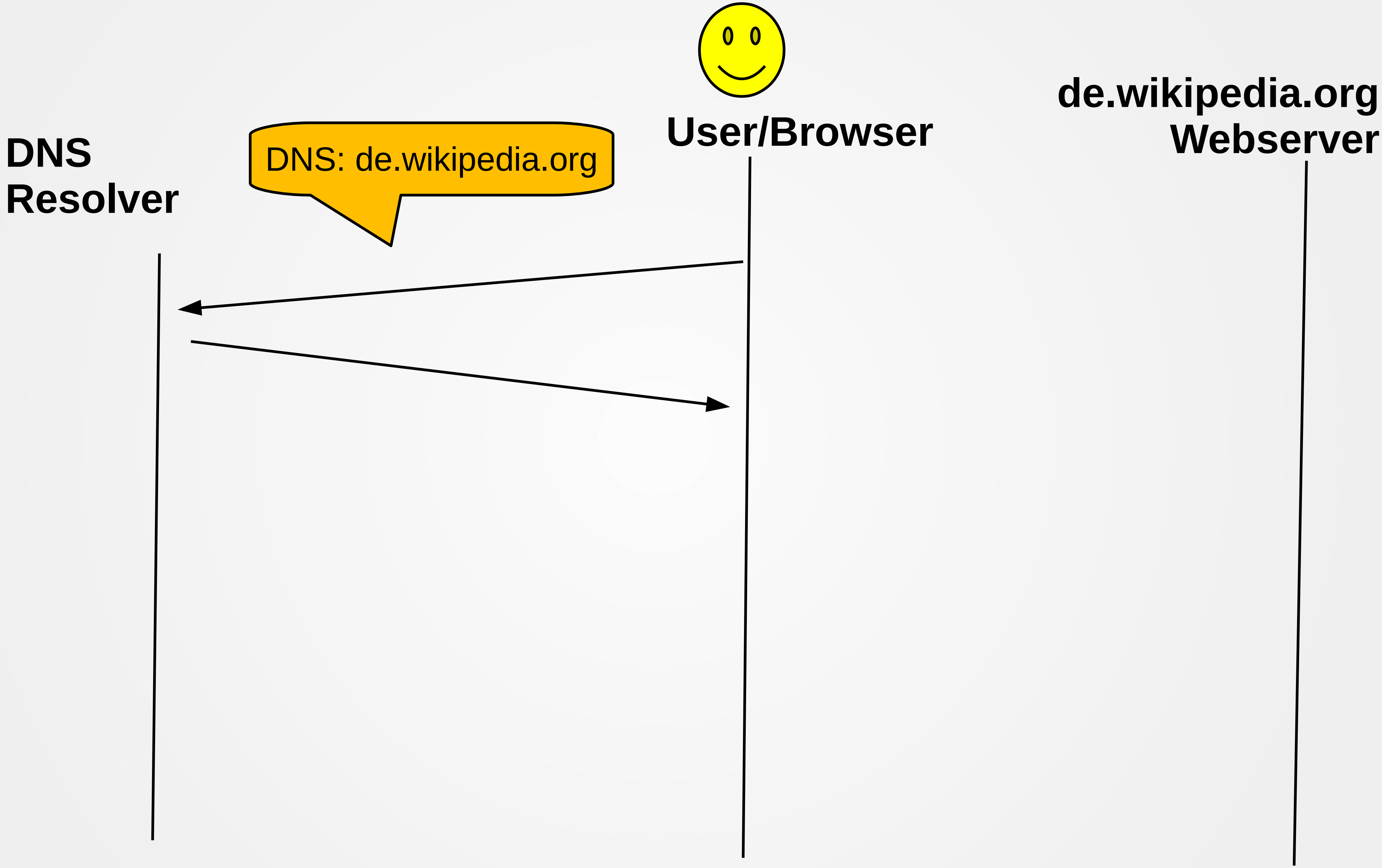
(ohne Torbrowser)



DNS
Resolver

User/Browser

de.wikipedia.org
Webserver



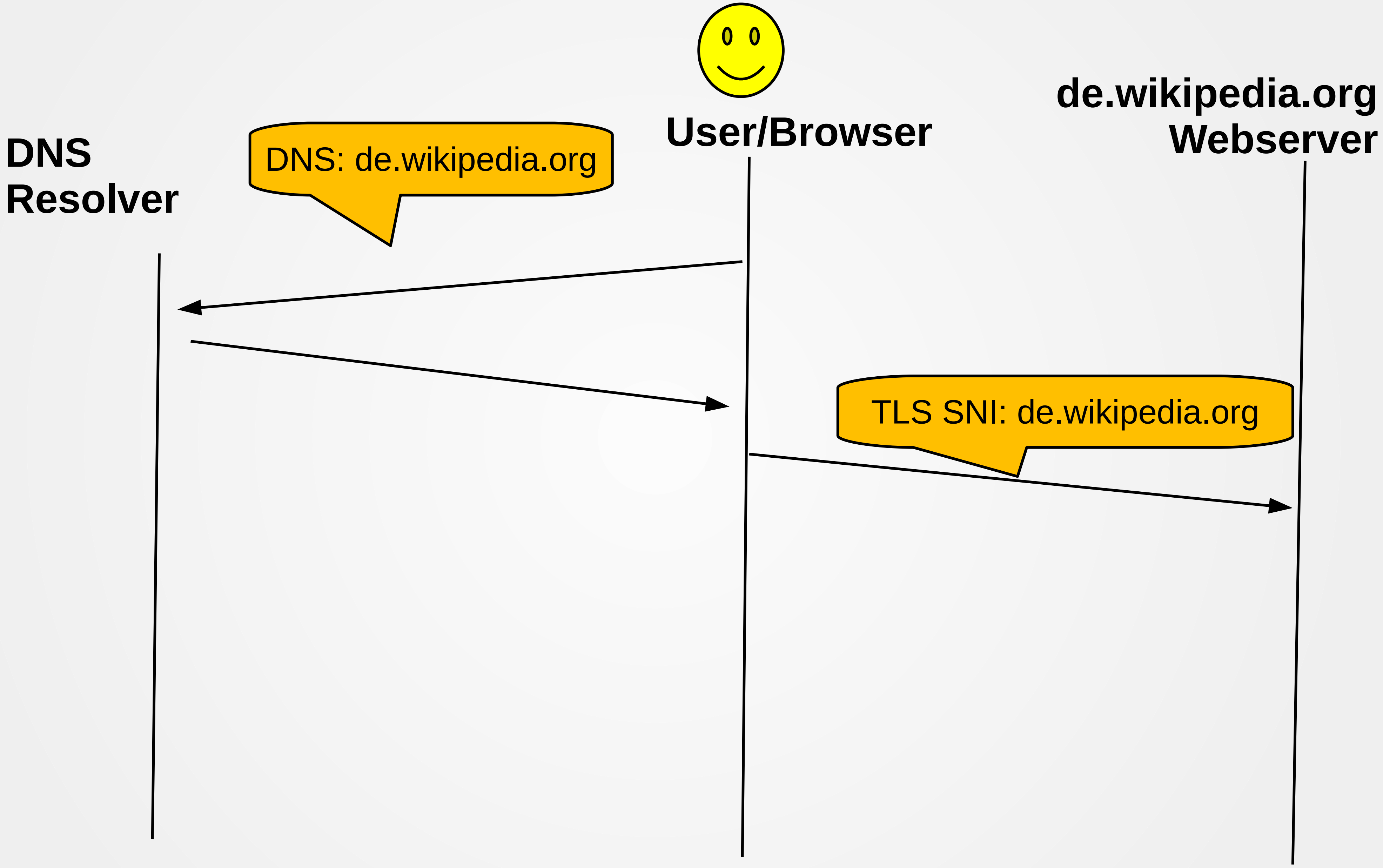
DNS
Resolver

DNS: de.wikipedia.org

User/Browser

de.wikipedia.org
Webserver

Foundation for
Applied Privacy



DNS Resolver

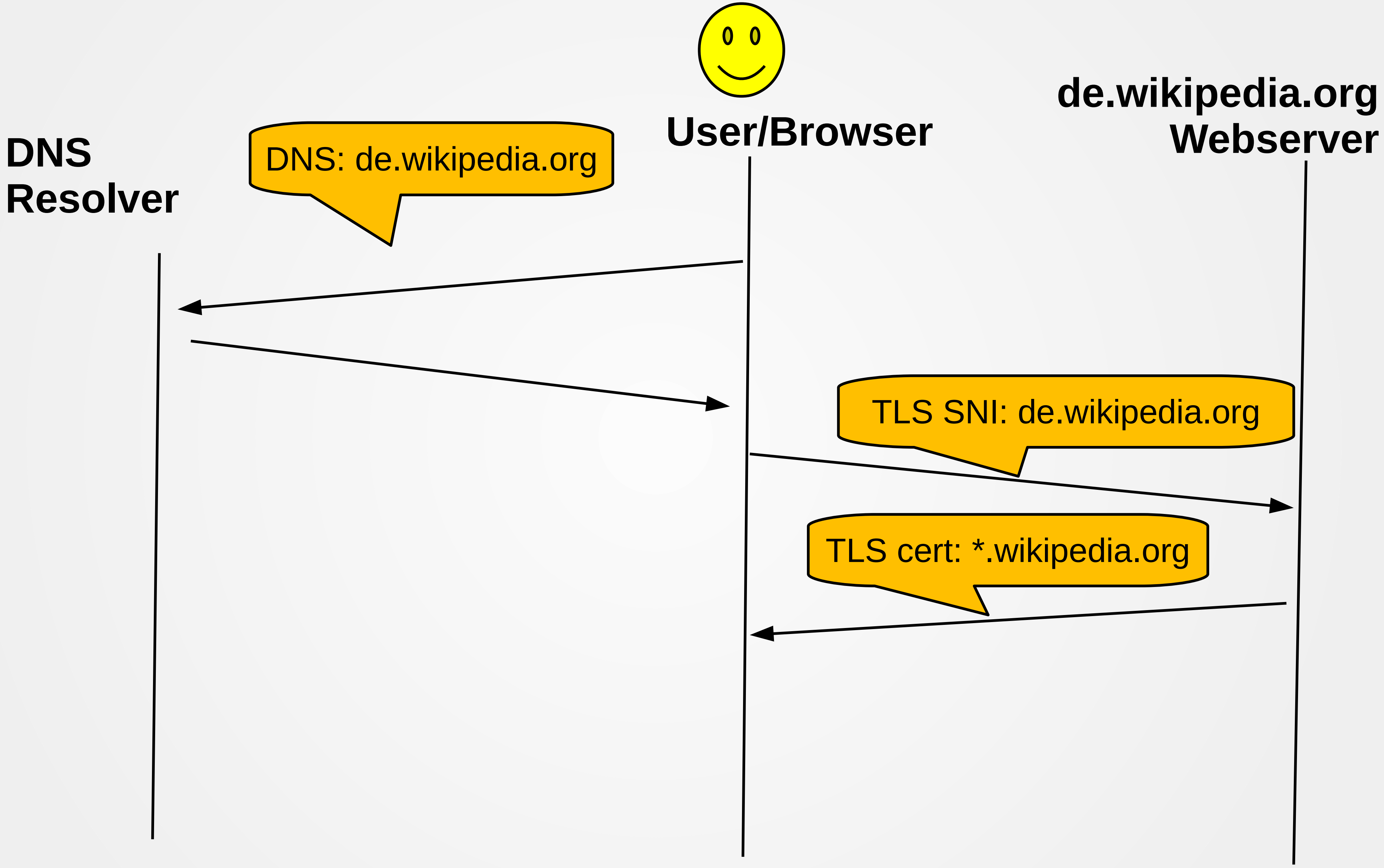
User/Browser

de.wikipedia.org Webserver

DNS: de.wikipedia.org

TLS SNI: de.wikipedia.org

Foundation for Applied Privacy



User/Browser

DNS Resolver

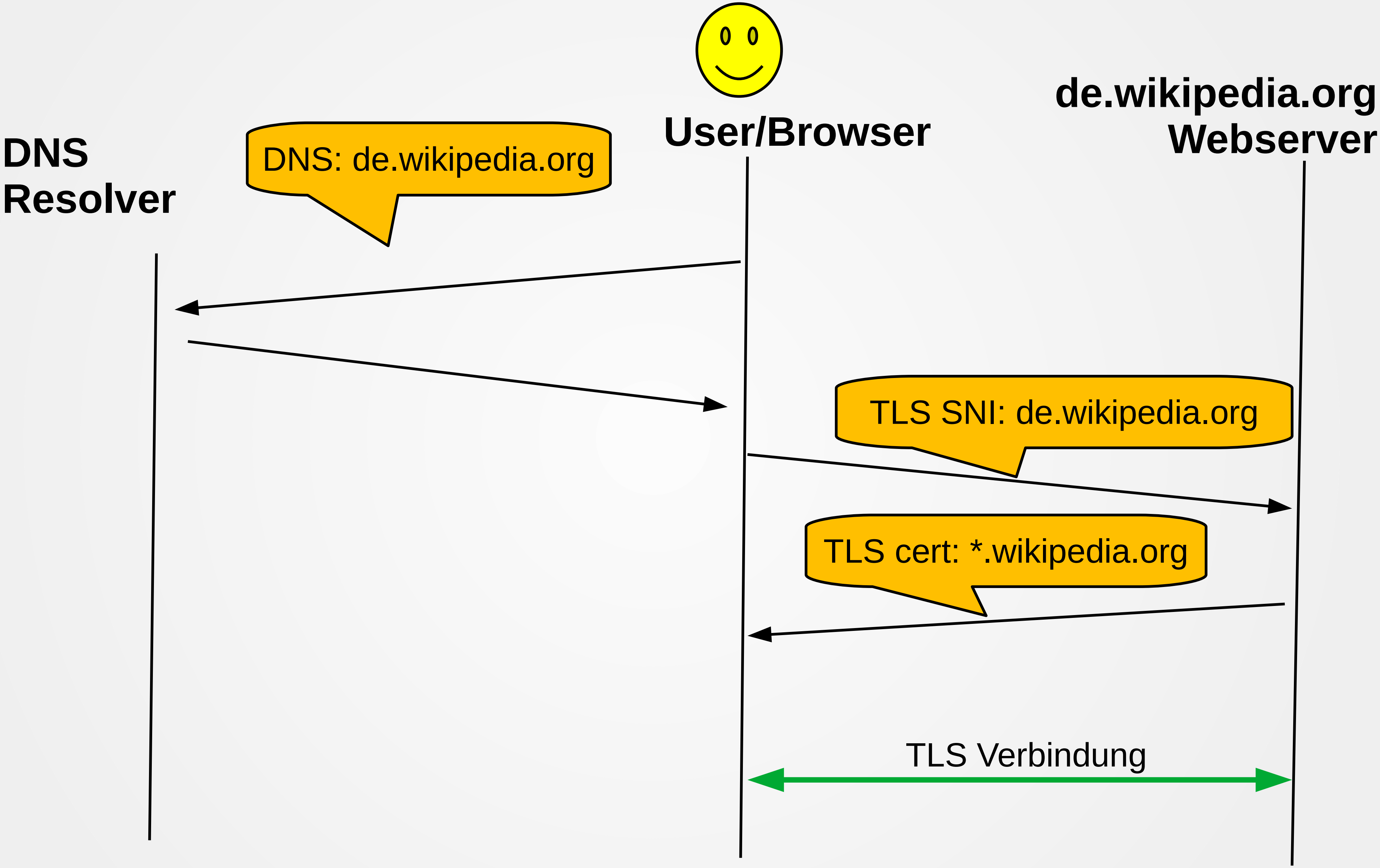
de.wikipedia.org Webserver

DNS: de.wikipedia.org

TLS SNI: de.wikipedia.org

TLS cert: *.wikipedia.org

Foundation for Applied Privacy



DNS Resolver

User/Browser

de.wikipedia.org Webserver

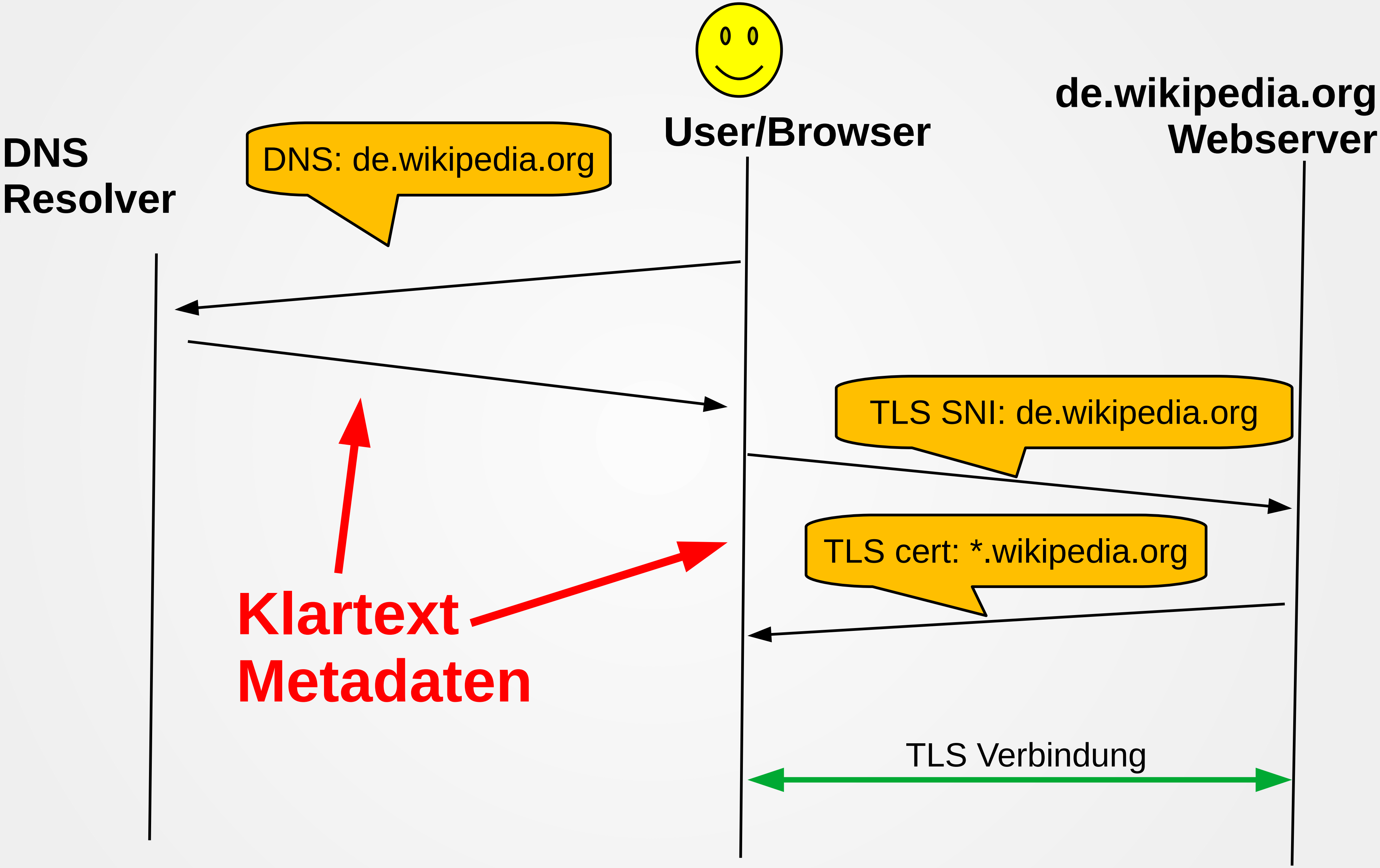
DNS: de.wikipedia.org

TLS SNI: de.wikipedia.org

TLS cert: *.wikipedia.org

TLS Verbindung

Foundation for Applied Privacy



DNS Resolver

DNS: de.wikipedia.org

User/Browser

de.wikipedia.org Webserver

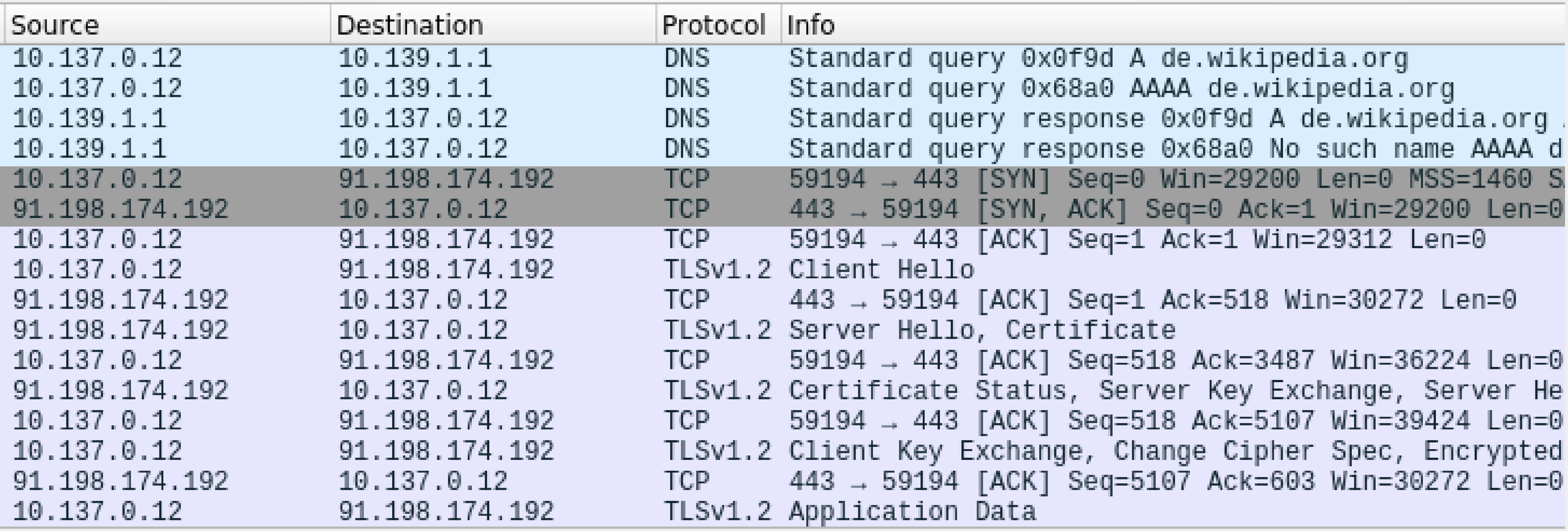
TLS SNI: de.wikipedia.org

TLS cert: *.wikipedia.org

Klartext Metadaten

TLS Verbindung

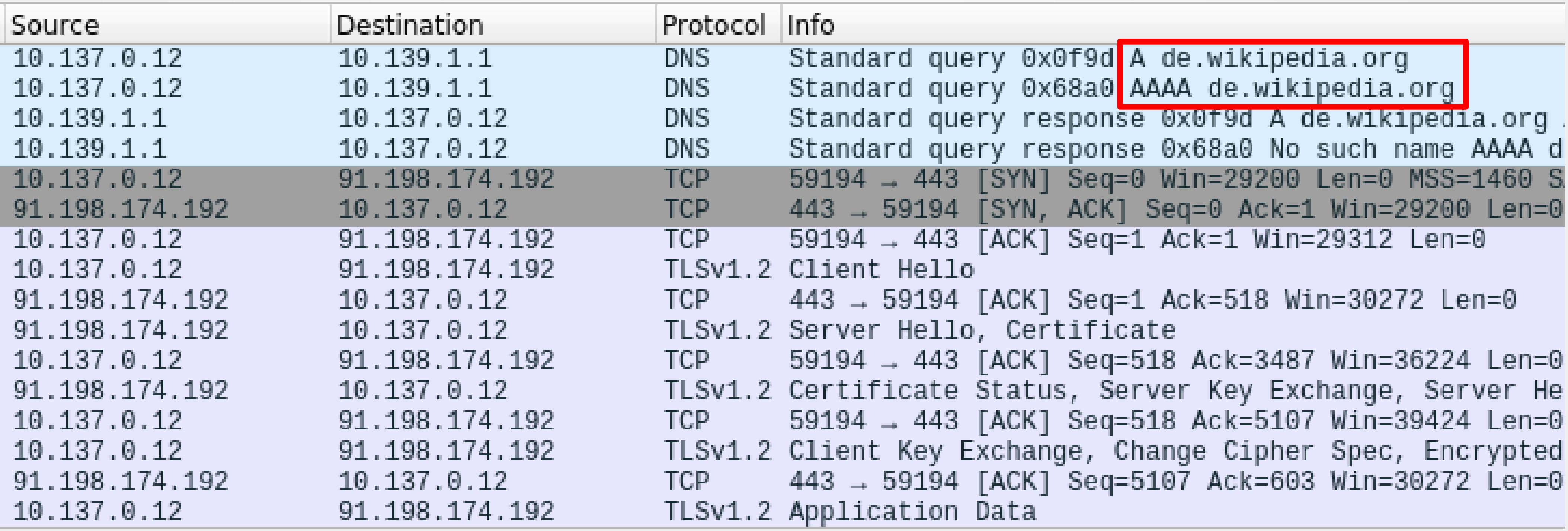
Foundation for Applied Privacy



```
Source          Destination     Protocol Info
10.137.0.12     10.139.1.1      DNS      Standard query 0x0f9d A de.wikipedia.org
10.137.0.12     10.139.1.1      DNS      Standard query 0x68a0 AAAA de.wikipedia.org
10.139.1.1      10.137.0.12     DNS      Standard query response 0x0f9d A de.wikipedia.org .
10.139.1.1      10.137.0.12     DNS      Standard query response 0x68a0 No such name AAAA d
10.137.0.12     91.198.174.192  TCP      59194 → 443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 S
91.198.174.192  10.137.0.12     TCP      443 → 59194 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0
10.137.0.12     91.198.174.192  TCP      59194 → 443 [ACK] Seq=1 Ack=1 Win=29312 Len=0
10.137.0.12     91.198.174.192  TLSv1.2  Client Hello
91.198.174.192  10.137.0.12     TCP      443 → 59194 [ACK] Seq=1 Ack=518 Win=30272 Len=0
91.198.174.192  10.137.0.12     TLSv1.2  Server Hello, Certificate
10.137.0.12     91.198.174.192  TCP      59194 → 443 [ACK] Seq=518 Ack=3487 Win=36224 Len=0
91.198.174.192  10.137.0.12     TLSv1.2  Certificate Status, Server Key Exchange, Server He
10.137.0.12     91.198.174.192  TCP      59194 → 443 [ACK] Seq=518 Ack=5107 Win=39424 Len=0
10.137.0.12     91.198.174.192  TLSv1.2  Client Key Exchange, Change Cipher Spec, Encrypted
91.198.174.192  10.137.0.12     TCP      443 → 59194 [ACK] Seq=5107 Ack=603 Win=30272 Len=0
10.137.0.12     91.198.174.192  TLSv1.2  Application Data
```

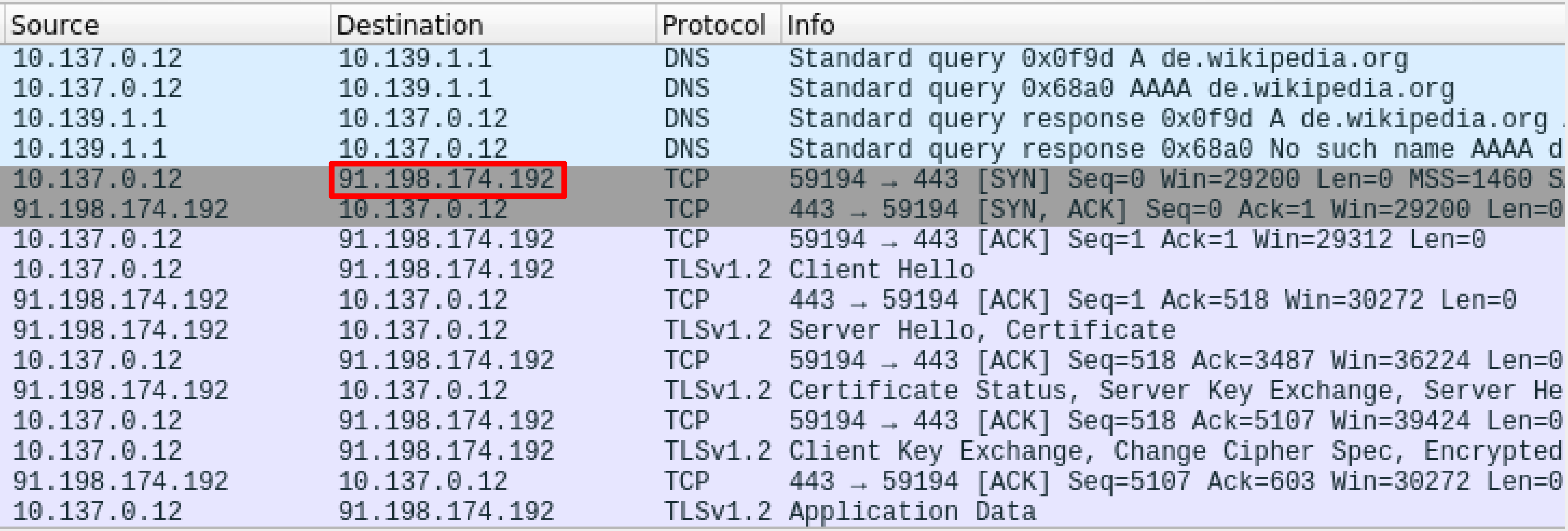
Foundation for Applied Privacy

DNS Anfrage



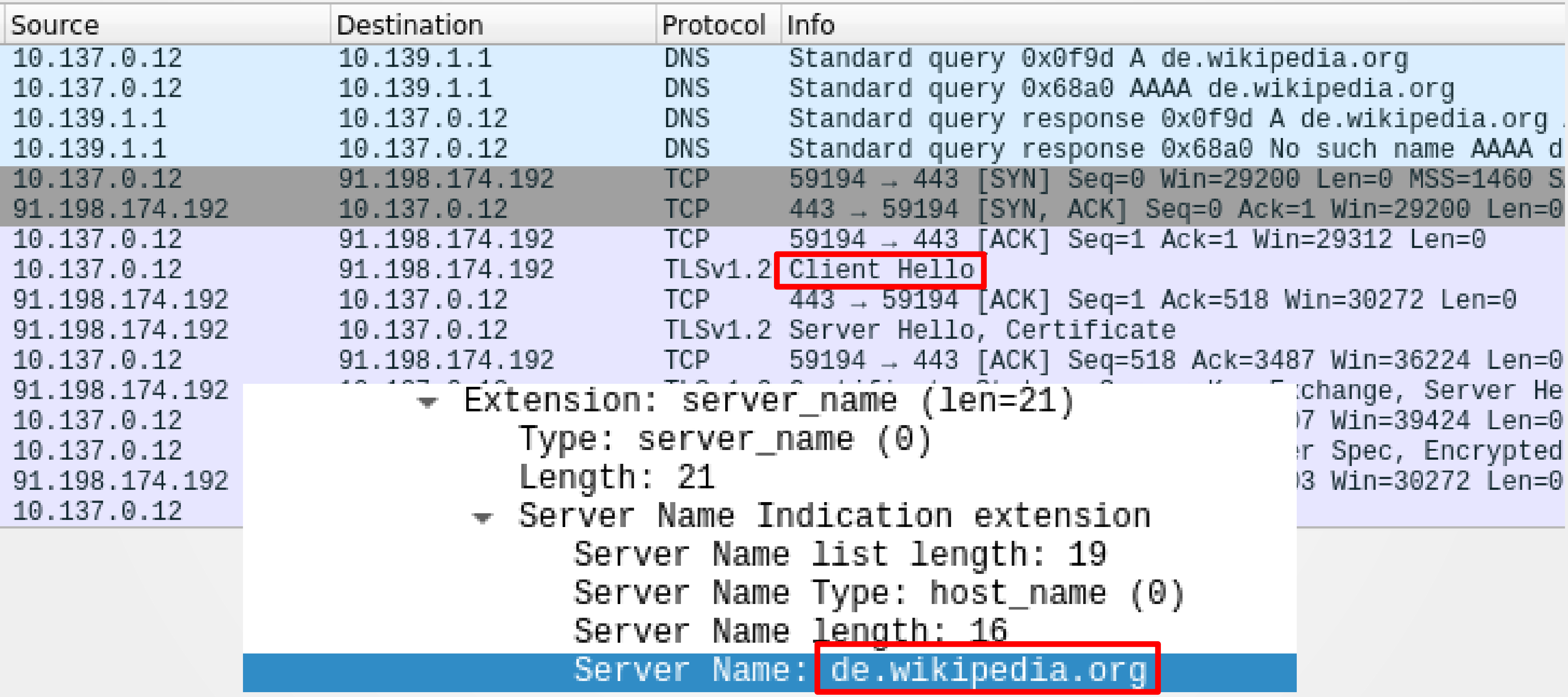
Source	Destination	Protocol	Info
10.137.0.12	10.139.1.1	DNS	Standard query 0x0f9d A de.wikipedia.org
10.137.0.12	10.139.1.1	DNS	Standard query 0x68a0 AAAA de.wikipedia.org
10.139.1.1	10.137.0.12	DNS	Standard query response 0x0f9d A de.wikipedia.org
10.139.1.1	10.137.0.12	DNS	Standard query response 0x68a0 No such name AAAA d
10.137.0.12	91.198.174.192	TCP	59194 → 443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 S
91.198.174.192	10.137.0.12	TCP	443 → 59194 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0
10.137.0.12	91.198.174.192	TCP	59194 → 443 [ACK] Seq=1 Ack=1 Win=29312 Len=0
10.137.0.12	91.198.174.192	TLSv1.2	Client Hello
91.198.174.192	10.137.0.12	TCP	443 → 59194 [ACK] Seq=1 Ack=518 Win=30272 Len=0
91.198.174.192	10.137.0.12	TLSv1.2	Server Hello, Certificate
10.137.0.12	91.198.174.192	TCP	59194 → 443 [ACK] Seq=518 Ack=3487 Win=36224 Len=0
91.198.174.192	10.137.0.12	TLSv1.2	Certificate Status, Server Key Exchange, Server He
10.137.0.12	91.198.174.192	TCP	59194 → 443 [ACK] Seq=518 Ack=5107 Win=39424 Len=0
10.137.0.12	91.198.174.192	TLSv1.2	Client Key Exchange, Change Cipher Spec, Encrypted
91.198.174.192	10.137.0.12	TCP	443 → 59194 [ACK] Seq=5107 Ack=603 Win=30272 Len=0
10.137.0.12	91.198.174.192	TLSv1.2	Application Data

Ziel IP Adresse



Source	Destination	Protocol	Info
10.137.0.12	10.139.1.1	DNS	Standard query 0x0f9d A de.wikipedia.org
10.137.0.12	10.139.1.1	DNS	Standard query 0x68a0 AAAA de.wikipedia.org
10.139.1.1	10.137.0.12	DNS	Standard query response 0x0f9d A de.wikipedia.org .
10.139.1.1	10.137.0.12	DNS	Standard query response 0x68a0 No such name AAAA d
10.137.0.12	91.198.174.192	TCP	59194 → 443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 S
91.198.174.192	10.137.0.12	TCP	443 → 59194 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0
10.137.0.12	91.198.174.192	TCP	59194 → 443 [ACK] Seq=1 Ack=1 Win=29312 Len=0
10.137.0.12	91.198.174.192	TLSv1.2	Client Hello
91.198.174.192	10.137.0.12	TCP	443 → 59194 [ACK] Seq=1 Ack=518 Win=30272 Len=0
91.198.174.192	10.137.0.12	TLSv1.2	Server Hello, Certificate
10.137.0.12	91.198.174.192	TCP	59194 → 443 [ACK] Seq=518 Ack=3487 Win=36224 Len=0
91.198.174.192	10.137.0.12	TLSv1.2	Certificate Status, Server Key Exchange, Server He
10.137.0.12	91.198.174.192	TCP	59194 → 443 [ACK] Seq=518 Ack=5107 Win=39424 Len=0
10.137.0.12	91.198.174.192	TLSv1.2	Client Key Exchange, Change Cipher Spec, Encrypted
91.198.174.192	10.137.0.12	TCP	443 → 59194 [ACK] Seq=5107 Ack=603 Win=30272 Len=0
10.137.0.12	91.198.174.192	TLSv1.2	Application Data

Hostname im TLS SNI

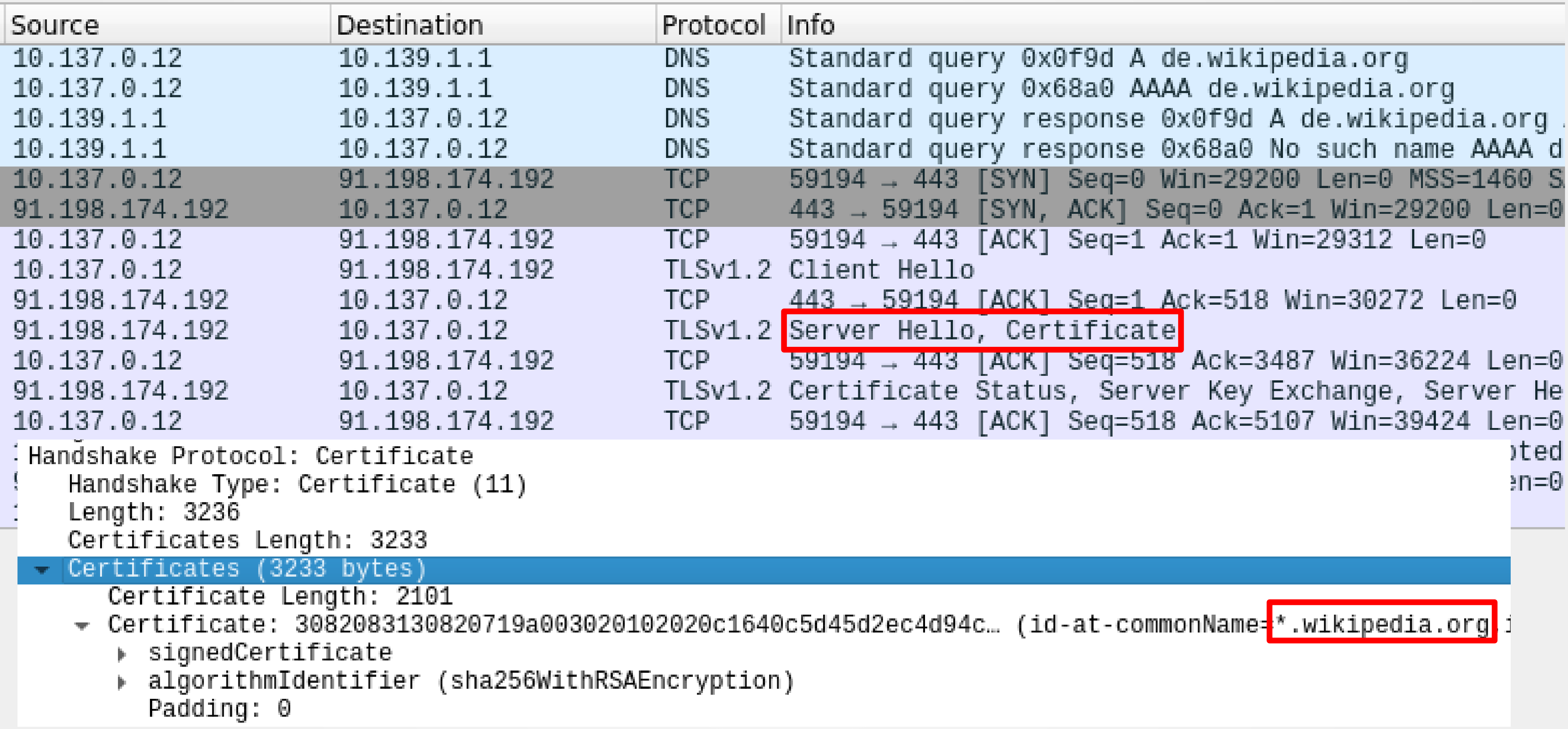


```
Source          Destination     Protocol Info
10.137.0.12     10.139.1.1      DNS      Standard query 0x0f9d A de.wikipedia.org
10.137.0.12     10.139.1.1      DNS      Standard query 0x68a0 AAAA de.wikipedia.org
10.139.1.1      10.137.0.12     DNS      Standard query response 0x0f9d A de.wikipedia.org
10.139.1.1      10.137.0.12     DNS      Standard query response 0x68a0 No such name AAAA d
10.137.0.12     91.198.174.192  TCP      59194 → 443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 S
91.198.174.192  10.137.0.12     TCP      443 → 59194 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0
10.137.0.12     91.198.174.192  TCP      59194 → 443 [ACK] Seq=1 Ack=1 Win=29312 Len=0
10.137.0.12     91.198.174.192  TLSv1.2  Client Hello
91.198.174.192  10.137.0.12     TCP      443 → 59194 [ACK] Seq=1 Ack=518 Win=30272 Len=0
91.198.174.192  10.137.0.12     TLSv1.2  Server Hello, Certificate
10.137.0.12     91.198.174.192  TCP      59194 → 443 [ACK] Seq=518 Ack=3487 Win=36224 Len=0
91.198.174.192                                                  change, Server He
10.137.0.12                                                     7 Win=39424 Len=0
10.137.0.12                                                     r Spec, Encrypted
91.198.174.192                                                  3 Win=30272 Len=0
10.137.0.12
```

```
▾ Extension: server_name (len=21)
    Type: server_name (0)
    Length: 21
  ▾ Server Name Indication extension
      Server Name list length: 19
      Server Name Type: host_name (0)
      Server Name length: 16
      Server Name: de.wikipedia.org
```

Foundation for Applied Privacy

Hostname im TLS Zertifikat



```
Source          Destination     Protocol Info
10.137.0.12     10.139.1.1      DNS      Standard query 0x0f9d A de.wikipedia.org
10.137.0.12     10.139.1.1      DNS      Standard query 0x68a0 AAAA de.wikipedia.org
10.139.1.1      10.137.0.12     DNS      Standard query response 0x0f9d A de.wikipedia.org
10.139.1.1      10.137.0.12     DNS      Standard query response 0x68a0 No such name AAAA d
10.137.0.12     91.198.174.192  TCP      59194 → 443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 S
91.198.174.192  10.137.0.12     TCP      443 → 59194 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0
10.137.0.12     91.198.174.192  TCP      59194 → 443 [ACK] Seq=1 Ack=1 Win=29312 Len=0
10.137.0.12     91.198.174.192  TLSv1.2  Client Hello
91.198.174.192  10.137.0.12     TCP      443 → 59194 [ACK] Seq=1 Ack=518 Win=30272 Len=0
91.198.174.192  10.137.0.12     TLSv1.2  Server Hello, Certificate
10.137.0.12     91.198.174.192  TCP      59194 → 443 [ACK] Seq=518 Ack=3487 Win=36224 Len=0
91.198.174.192  10.137.0.12     TLSv1.2  Certificate Status, Server Key Exchange, Server He
10.137.0.12     91.198.174.192  TCP      59194 → 443 [ACK] Seq=518 Ack=5107 Win=39424 Len=0
```

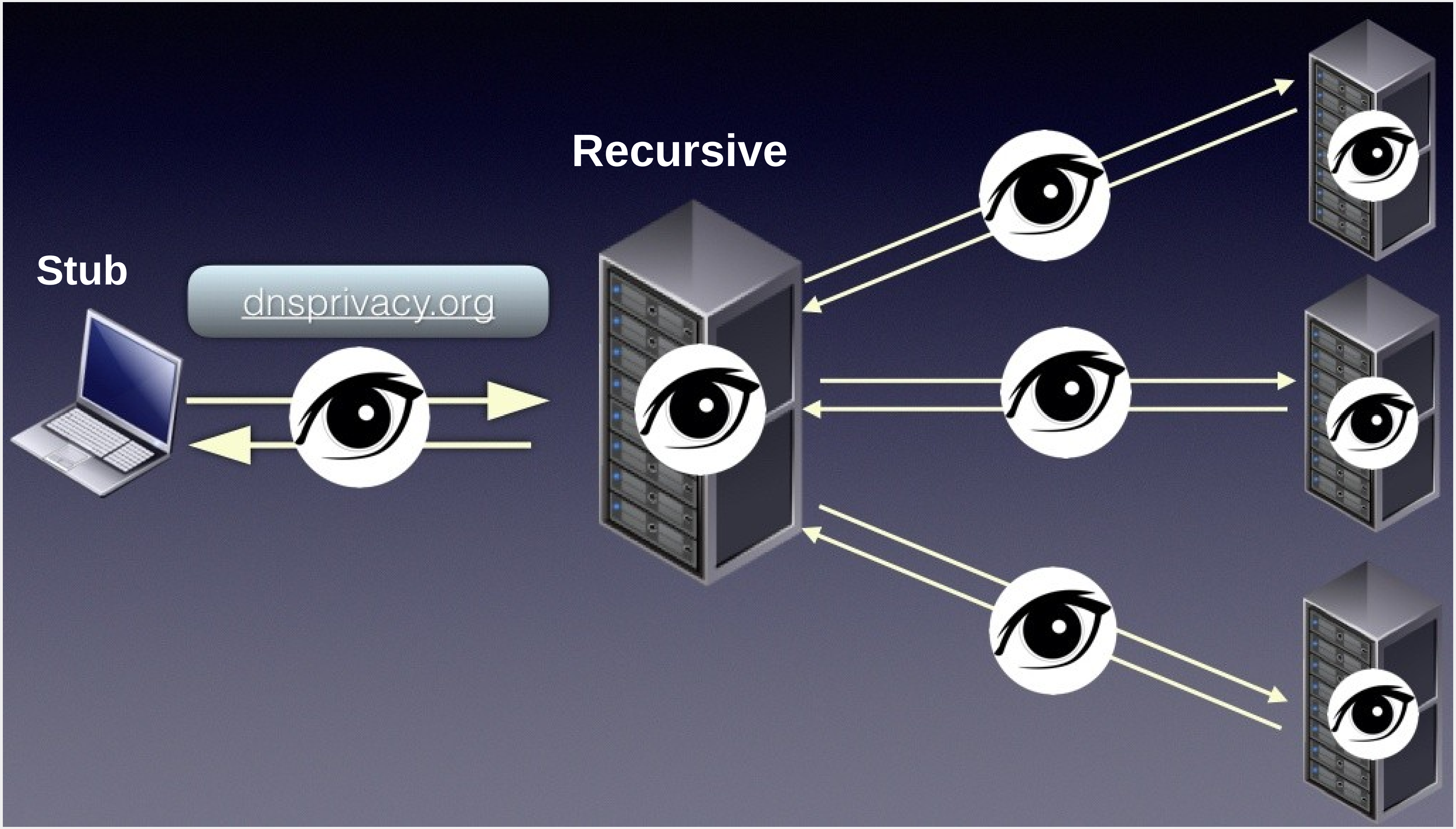
```
Handshake Protocol: Certificate
    Handshake Type: Certificate (11)
    Length: 3236
    Certificates Length: 3233
  ▾ Certificates (3233 bytes)
        Certificate Length: 2101
      ▾ Certificate: 3082083130820719a003020102020c1640c5d45d2ec4d94c… (id-at-commonName=*.wikipedia.org,i
          ▸ signedCertificate
          ▸ algorithmIdentifier (sha256WithRSAEncryption)
            Padding: 0
```

Klartext Metadaten	Lösung
IP Adresse	CDN/vHosts/Tor
TLS SNI	Work in Progress: Encrypted SNI (ESNI)
TLS Zertifikat	TLS 1.3
OCSP	OCSP Stapling
DNS	DoH/DoT/...

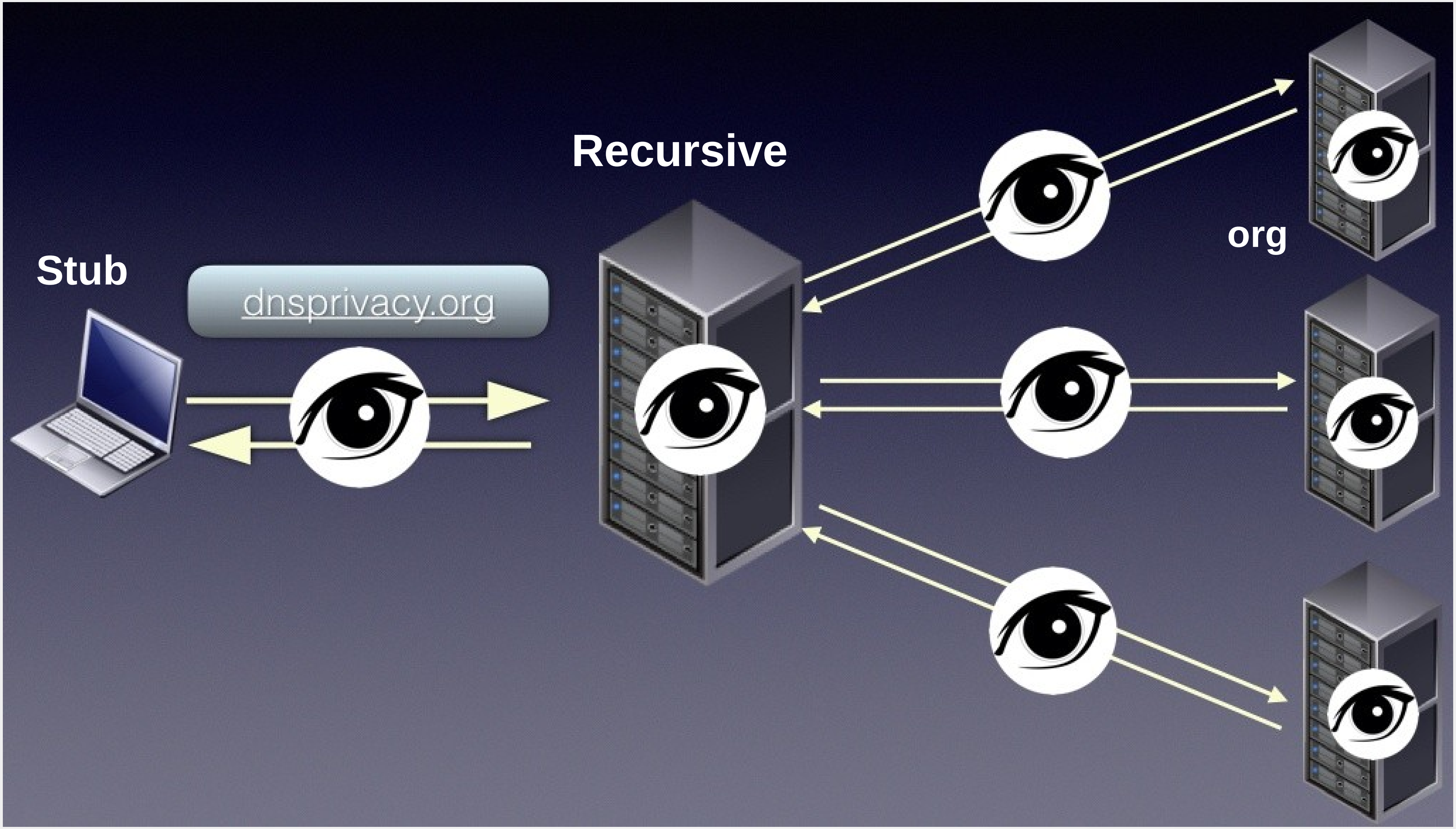
Klartext Metadaten	**Lösung**
IP Adresse	CDN/vHosts/Tor
TLS SNI	Work in Progress: Encrypted SNI (ESNI)
TLS Zertifikat	TLS 1.3
OCSP	OCSP Stapling
DNS	**DoH/DoT/...**

DNS

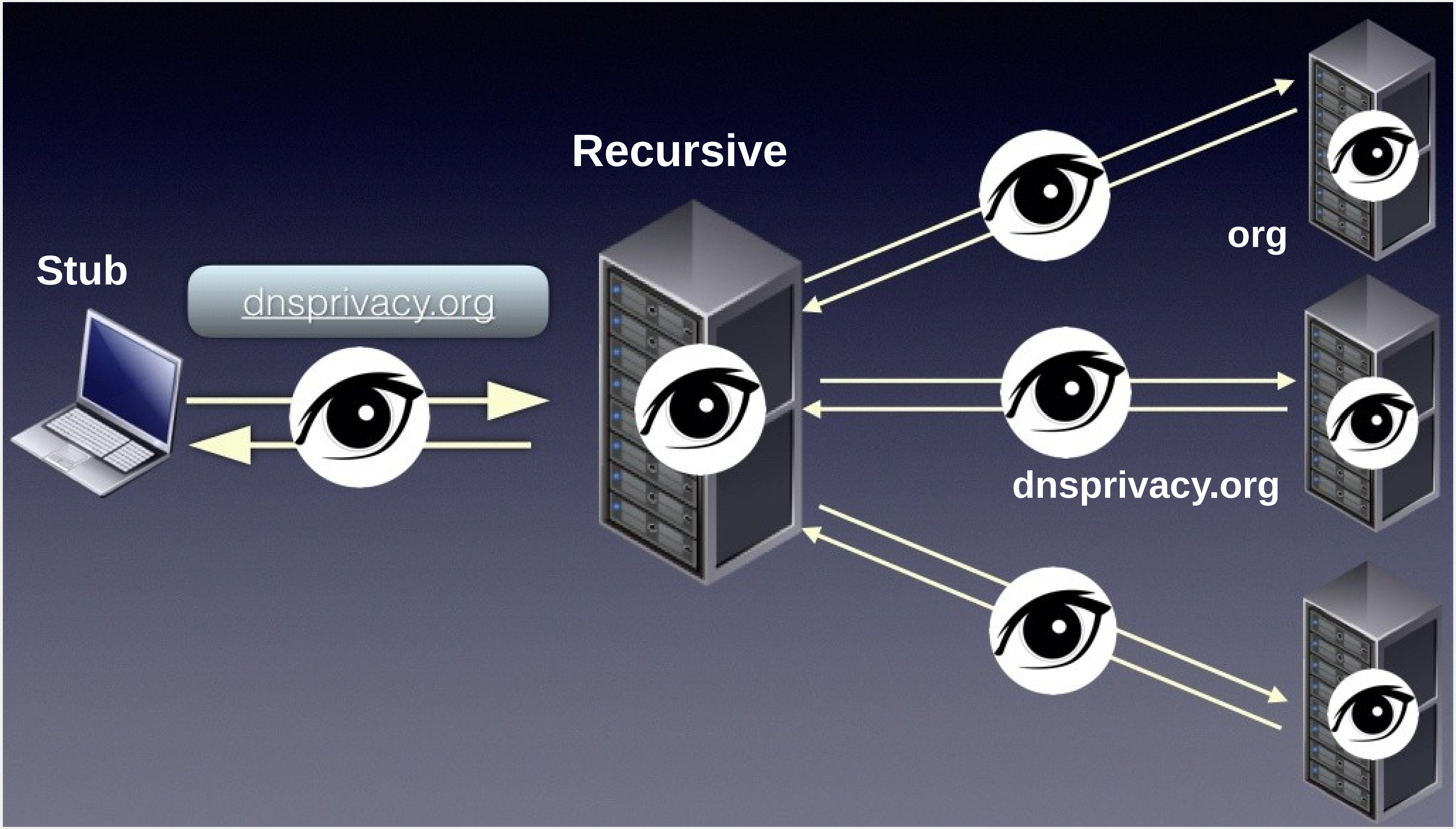
Foundation for Applied Privacy



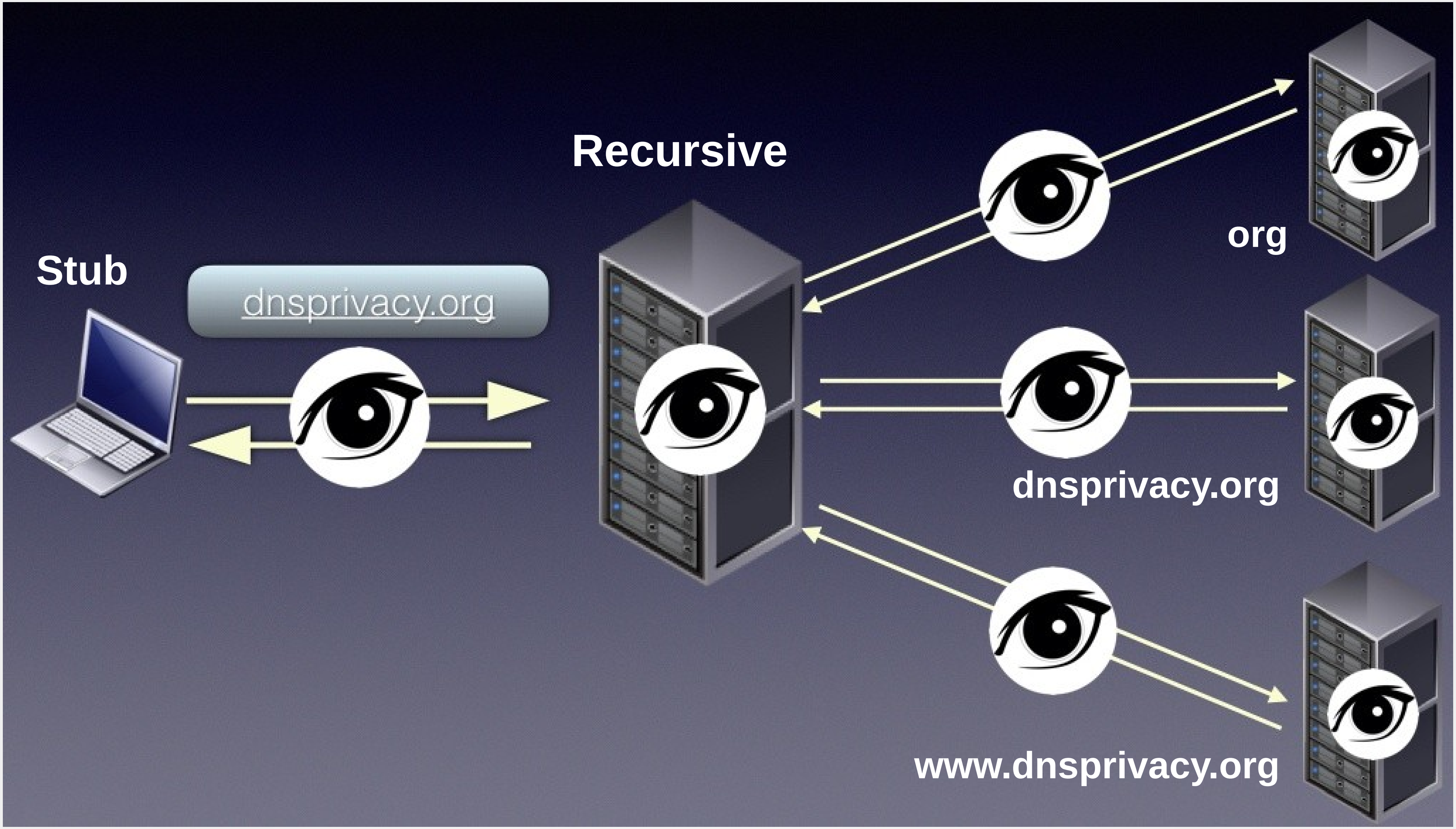
Quelle: dnsprivacy.org



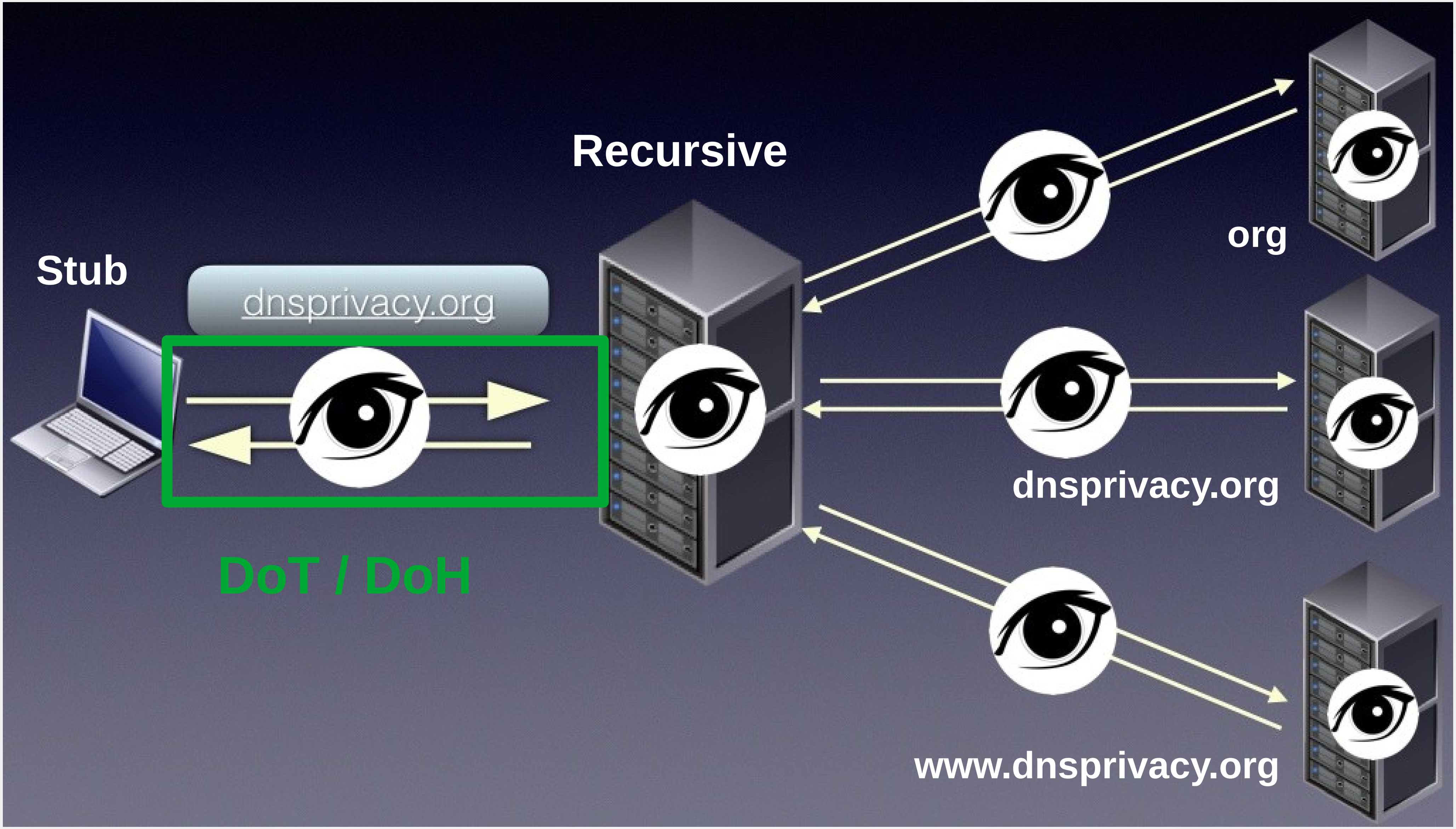
Foundation for Applied Privacy



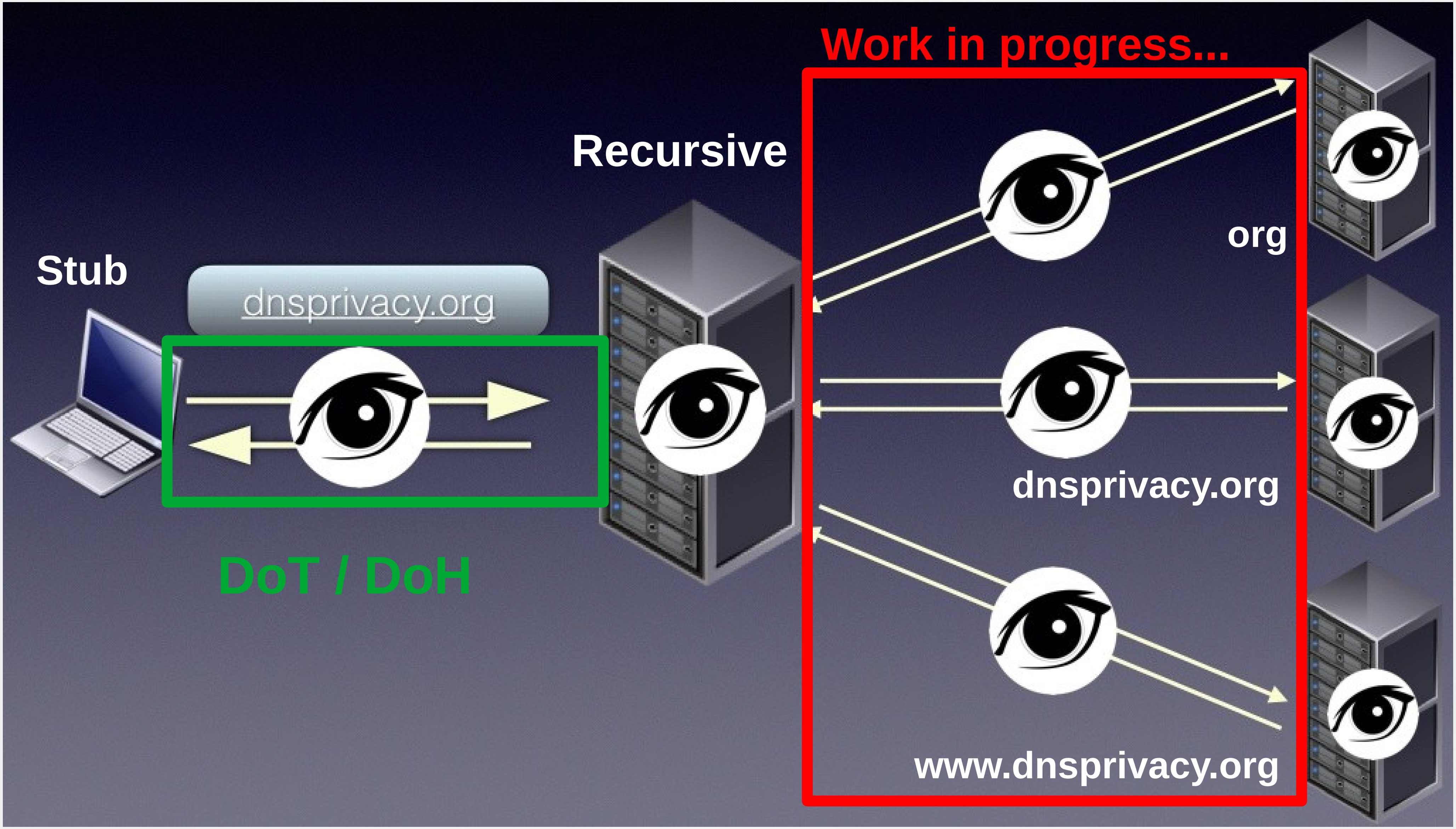
Foundation for Applied Privacy



Foundation for Applied Privacy



Foundation for Applied Privacy



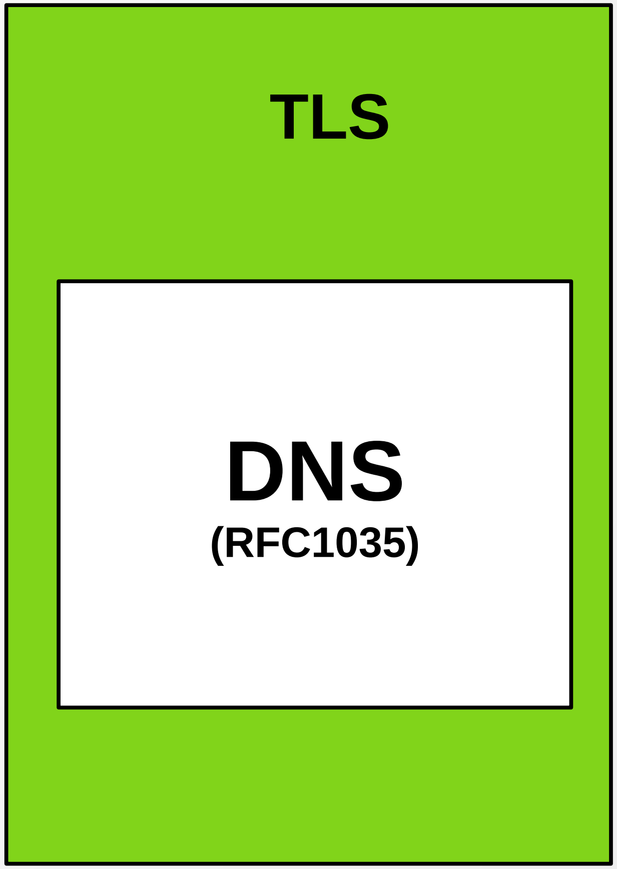
Foundation for Applied Privacy

DNS-over-TLS (DoT)

RFC7858 (Mai 2016)
RFC8310 (März 2018)

DoT

- >=TLS 1.2
- TCP Port 853
- Inoffiziell auch beliebt: Port 443



DoT Profile

- Opportunistisch

DoT Profile

- Opportunistisch

- Strikt
  - PKIX
  - SPKI Pins
  - DANE/TLSA

DoT Implementierungen (Client)

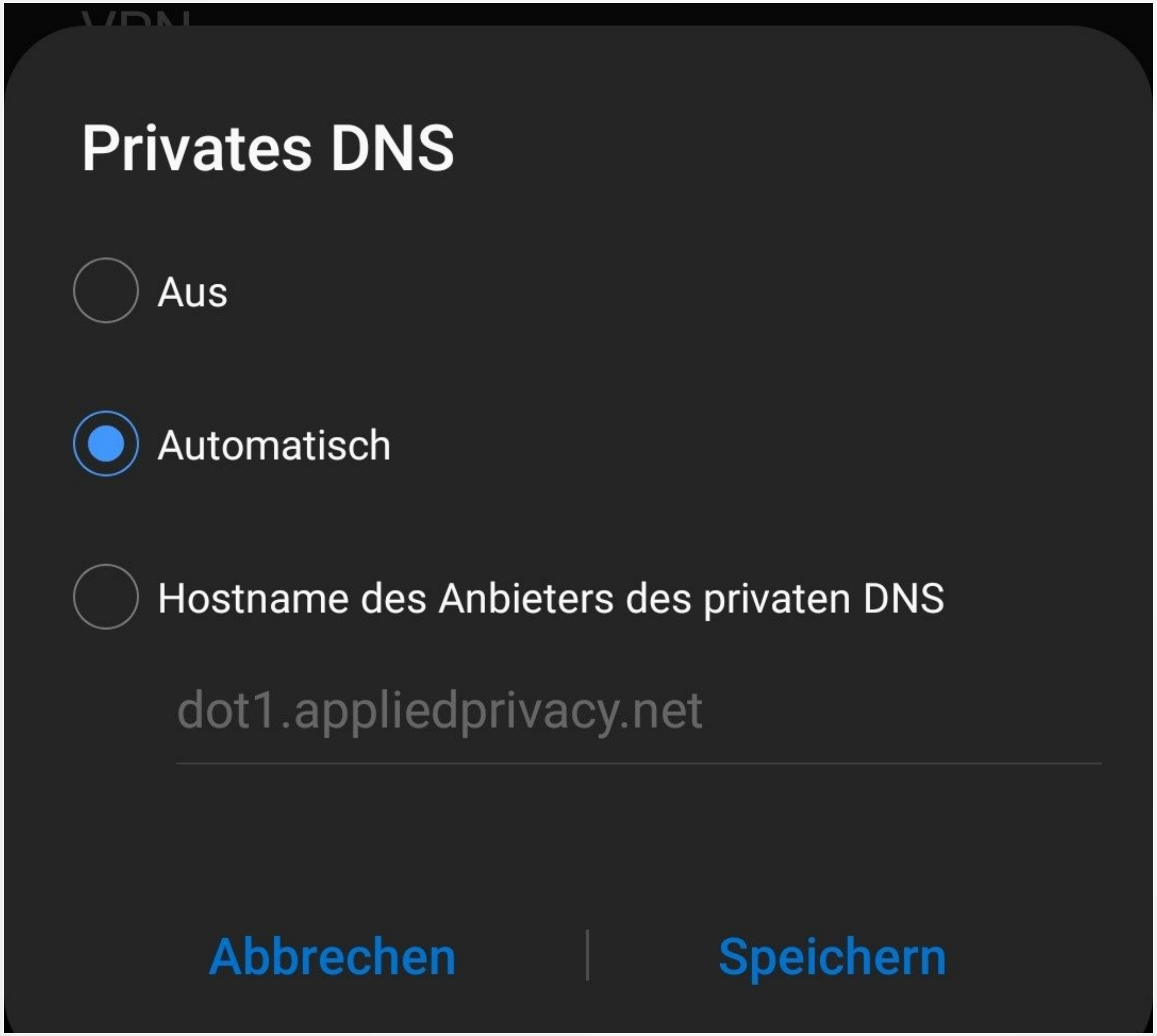
- **Stubby** (macOS, Windows, Linux)
- Android 9
- Knot-Resolver
- Unbound
- systemd-resolved

DoT Unbound (Client)

DoT Unbound (Client)

ONE FULL TLS HANDSHAKE
PER DNS QUERY
imgflip.com

Android 9 “Automatisch” (default)



Privates DNS

○ Aus

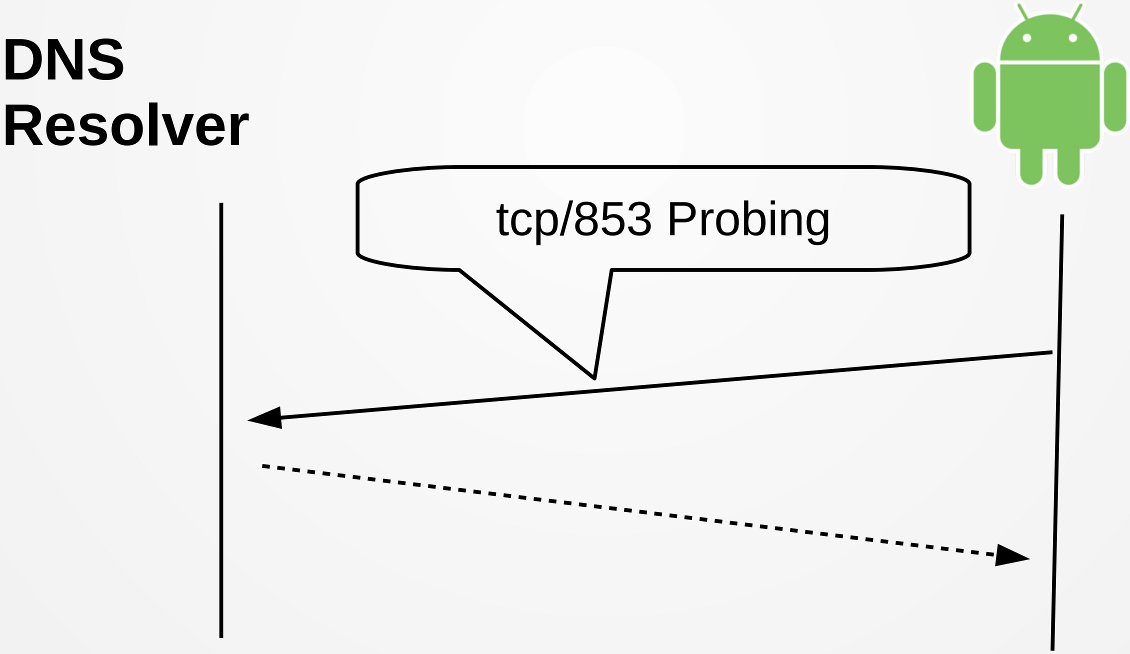
● Automatisch

○ Hostname des Anbieters des privaten DNS

dot1.appliedprivacy.net

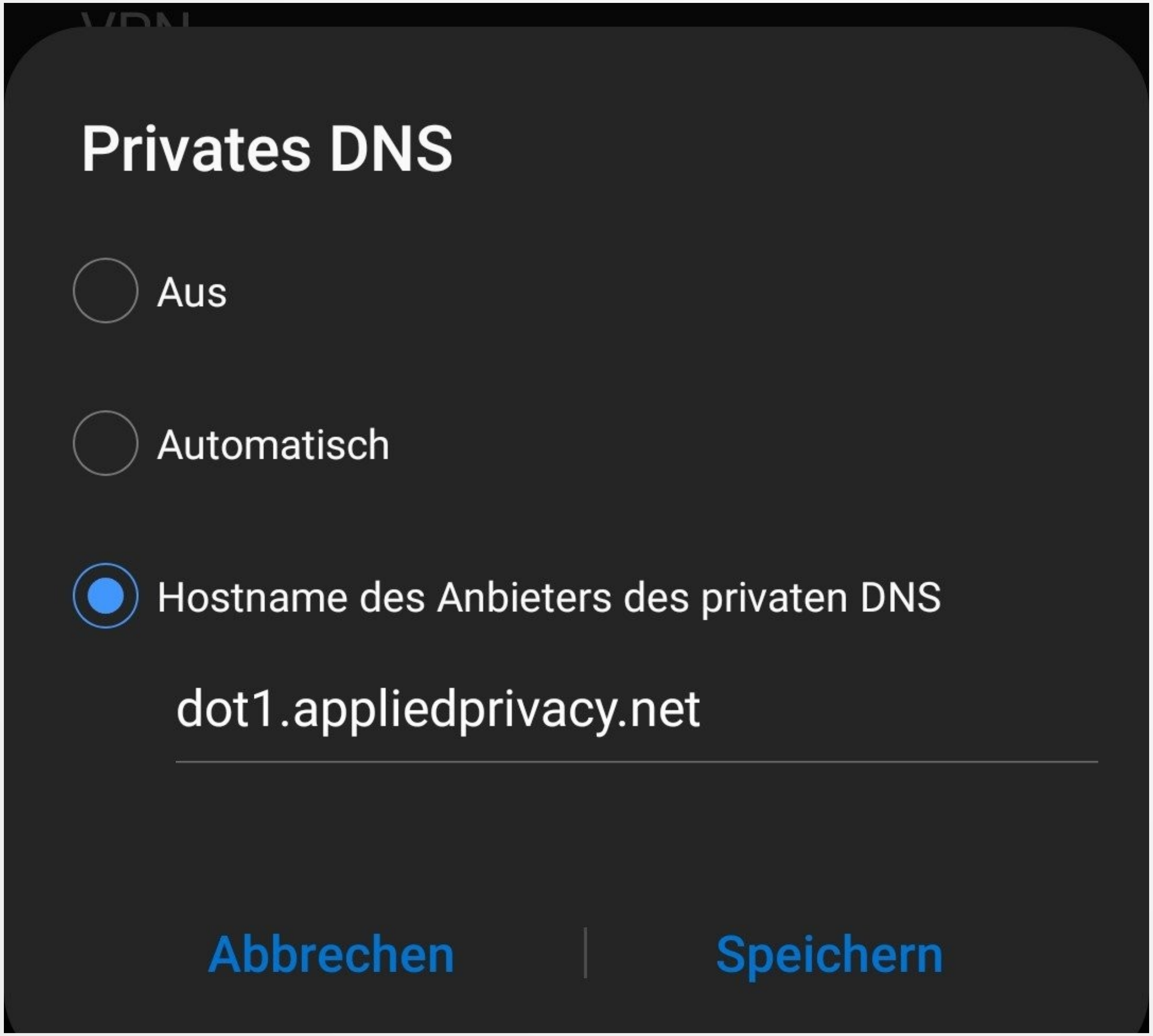
Foundation for Applied Privacy

Android 9 "Automatisch" (default)



Foundation for Applied Privacy

Android 9 strikt Mode



Privates DNS

○ Aus

○ Automatisch

● Hostname des Anbieters des privaten DNS

dot1.appliedprivacy.net

Foundation for Applied Privacy

DoT Client Stubby

- **Opportunistisch oder strikt Mode**
- **TLS Connection Re-use**
- Pipelining, Out-of-Order Responses
- Explizites deaktivieren von EDNS Client Subnet
- DNS Padding, DNSSEC

DNS-over-HTTPS (DoH)

RFC8484 (Okt 2018)

Foundation for Applied Privacy

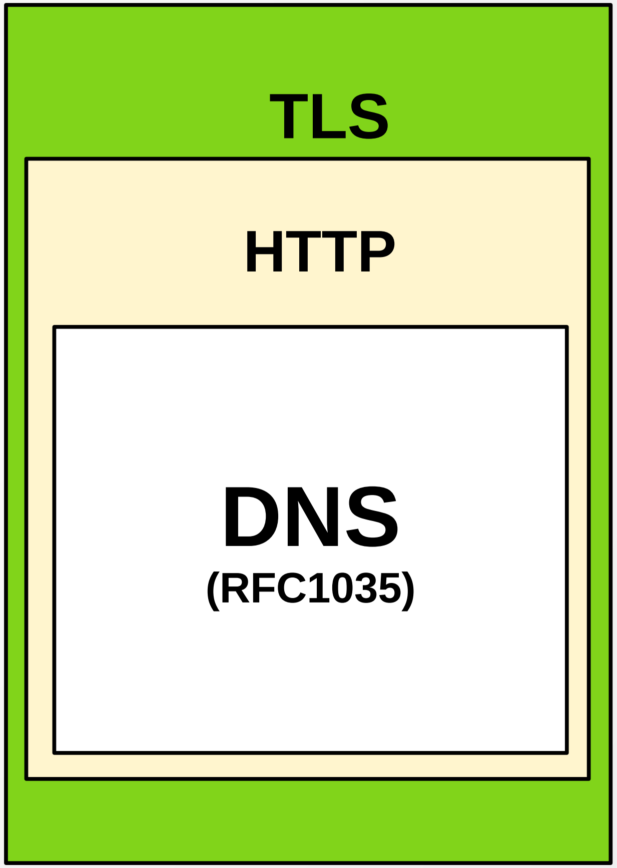
DoH - Motivation

- DNS Traffic vertraulich übertragen
- und vor Manipulation schützen
- soll auch in restriktiven Netzen funktionieren (in denen zB. nur 53/80/443 erlaubt ist)
- vor allem von Browsern getrieben

Foundation for Applied Privacy

DoH

- HTTPS (443)
- **POST**
- oder GET (base64url)
- HTTP/2 (empfohlen)
- Content Type: application/dns-message

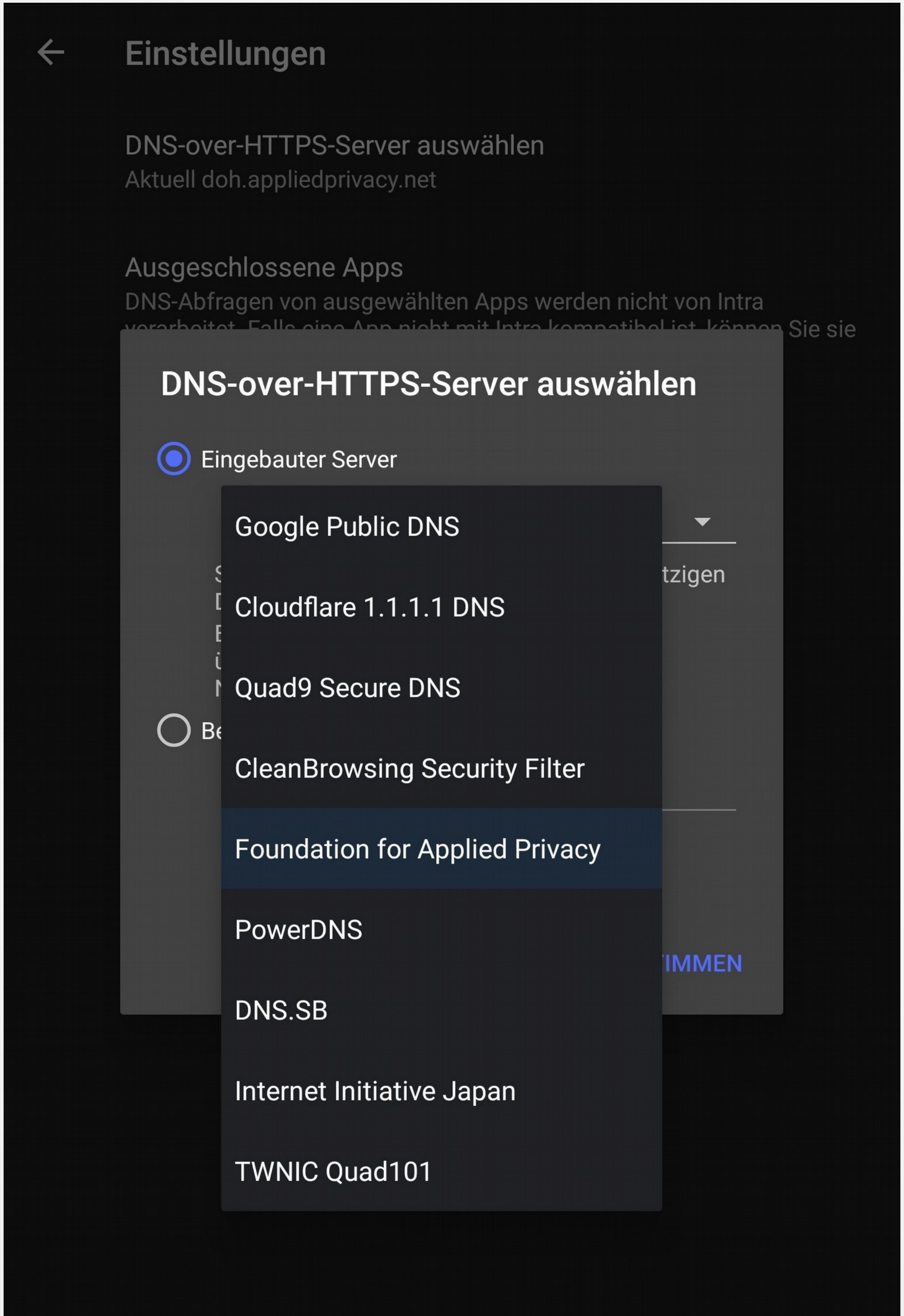


Foundation for Applied Privacy

DoH Client Software

- Jigsaw Intra (Android)
- dnscrypt-proxy
  - DNSCloak (iOS)
  - Simple DNSCrypt (Windows)
- **Firefox**
- Chrome https://blog.chromium.org/2019/09/experimenting-with-same-provider-dns.html
- Opera https://blogs.opera.com/desktop/2019/09/opera-65-0-3430-0-developer-update/

Jigsaw Intra (Android)



Einstellungen

DNS-over-HTTPS-Server auswählen
Aktuell doh.appliedprivacy.net

Ausgeschlossene Apps
DNS-Abfragen von ausgewählten Apps werden nicht von Intra verarbeitet. Falls eine App nicht mit Intra kompatibel ist, können Sie sie

DNS-over-HTTPS-Server auswählen

● Eingebauter Server

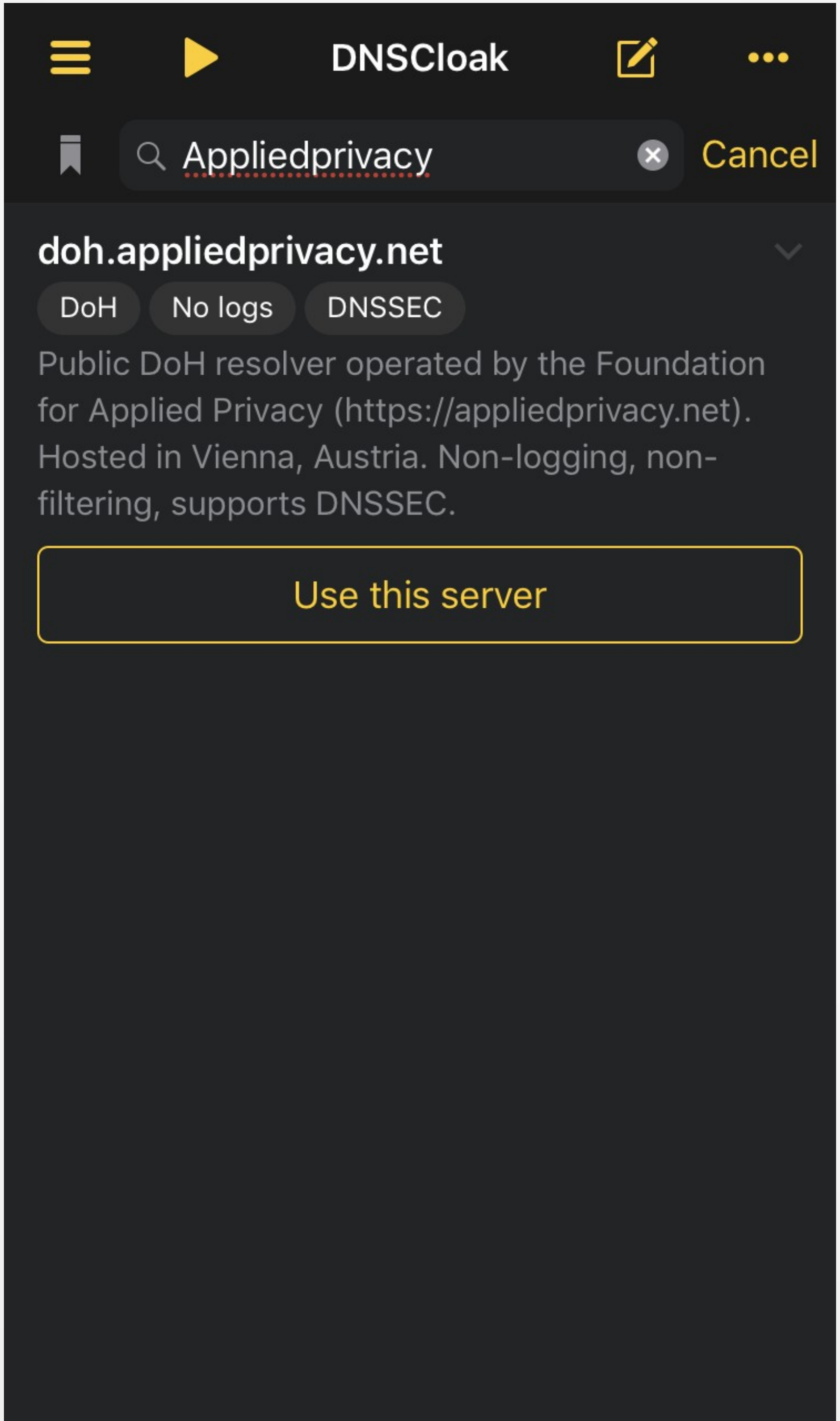
- Google Public DNS
- Cloudflare 1.1.1.1 DNS
- Quad9 Secure DNS
- CleanBrowsing Security Filter
- Foundation for Applied Privacy
- PowerDNS
- DNS.SB
- Internet Initiative Japan
- TWNIC Quad101

S tzigen
D
E
ü
N

○ Be

Foundation for Applied Privacy

DNSCloak (iOS)

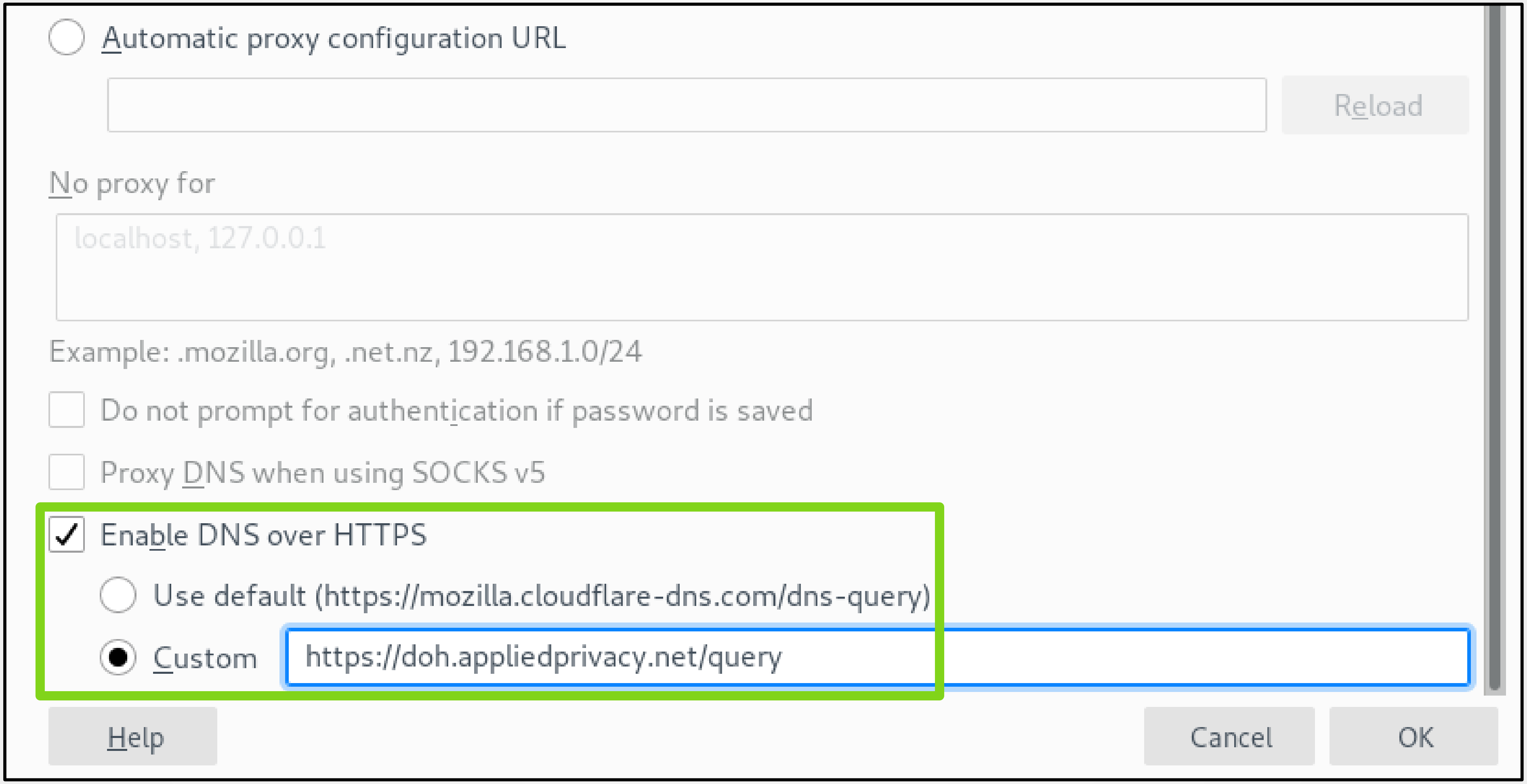


doh.appliedprivacy.net

Public DoH resolver operated by the Foundation for Applied Privacy (https://appliedprivacy.net). Hosted in Vienna, Austria. Non-logging, non-filtering, supports DNSSEC.

Foundation for Applied Privacy

DoH mit Firefox nutzen



○ Automatic proxy configuration URL

No proxy for

localhost, 127.0.0.1

Example: .mozilla.org, .net.nz, 192.168.1.0/24

□ Do not prompt for authentication if password is saved

□ Proxy DNS when using SOCKS v5

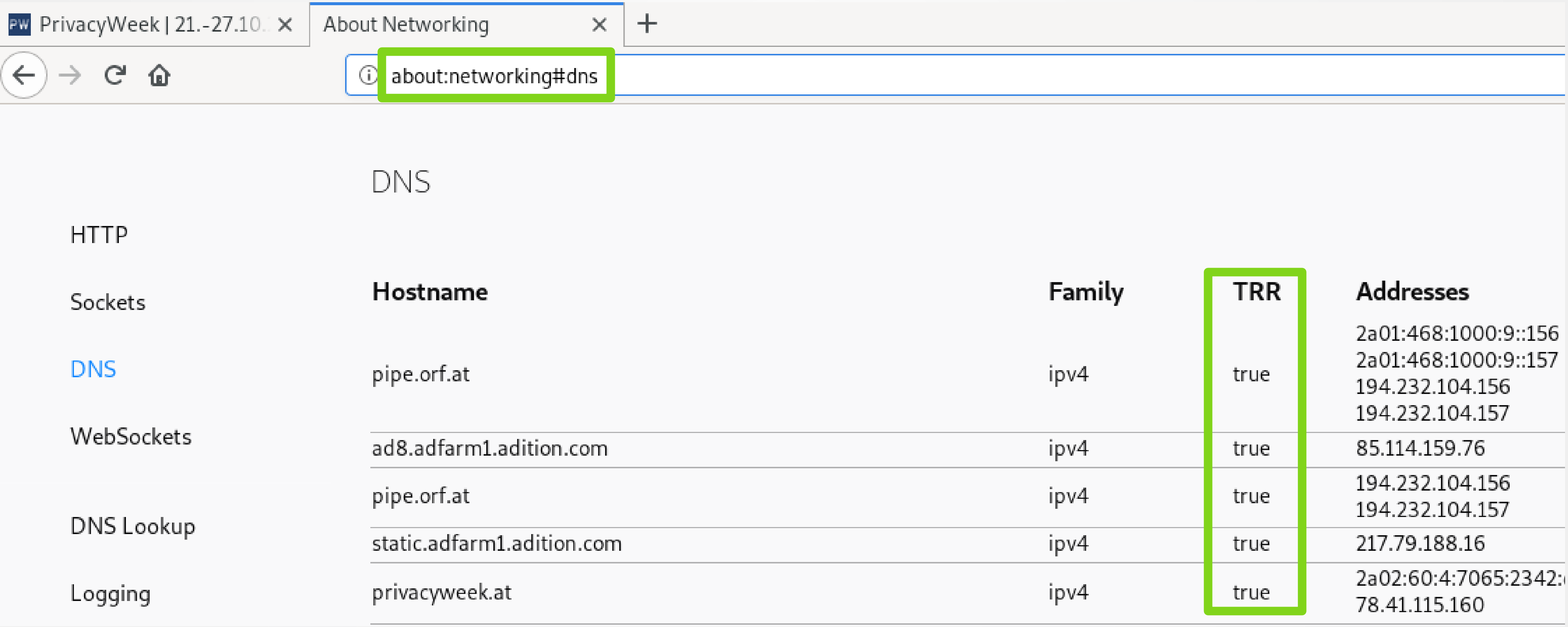
☑ Enable DNS over HTTPS

○ Use default (https://mozilla.cloudflare-dns.com/dns-query)

● Custom https://doh.appliedprivacy.net/query

Foundation for Applied Privacy

DoH mit Firefox nutzen



about:networking#dns

DNS

Hostname	Family	TRR	Addresses
pipe.orf.at	ipv4	true	2a01:468:1000:9::156 2a01:468:1000:9::157 194.232.104.156 194.232.104.157
ad8.adfarm1.adition.com	ipv4	true	85.114.159.76
pipe.orf.at	ipv4	true	194.232.104.156 194.232.104.157
static.adfarm1.adition.com	ipv4	true	217.79.188.16
privacyweek.at	ipv4	true	2a02:60:4:7065:2342: 78.41.115.160

Foundation for Applied Privacy

DoH -Firefox Modi

network.trr.mode:

2: “TRR first” - Fallback auf Klartext

3: “TRR only” - kein Fallback

+“network.trr.bootstrapAddress”

https://daniel.haxx.se/blog/2018/06/03/inside-firefoxs-doh-engine/

DoH Server Discovery in Chrome 79

- Automatisches Upgrade zu DoH sofern unterstützt

- Statische Liste im Browser (Resolver IP -> DoH URI)

DoH Server Software

- dnsdist
- Knot Resolver

POWERDNS

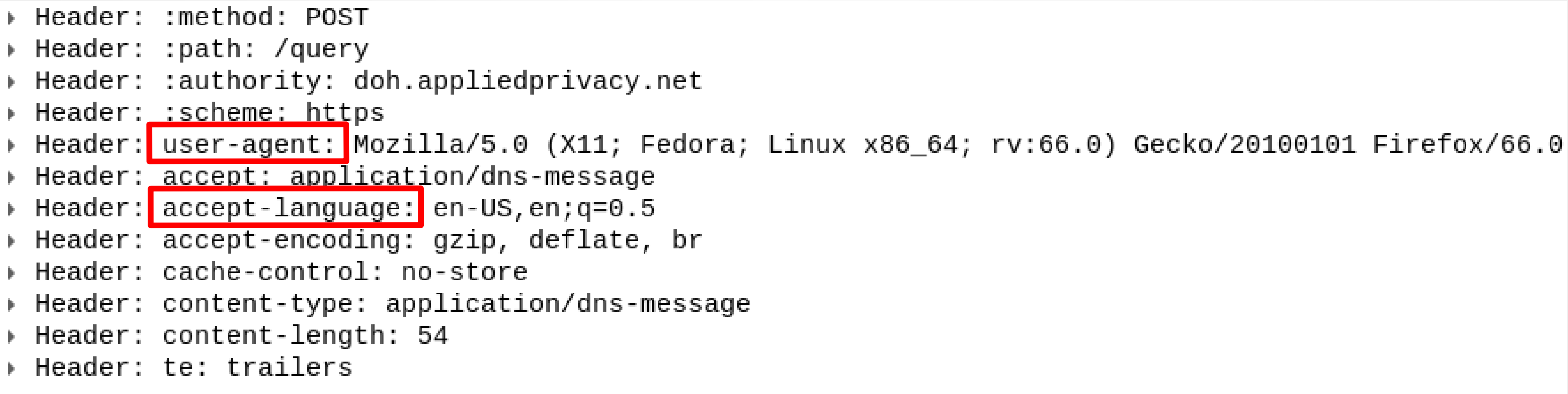
cz.nic

Foundation for Applied Privacy

DoH Kritik: HTTP Metadaten

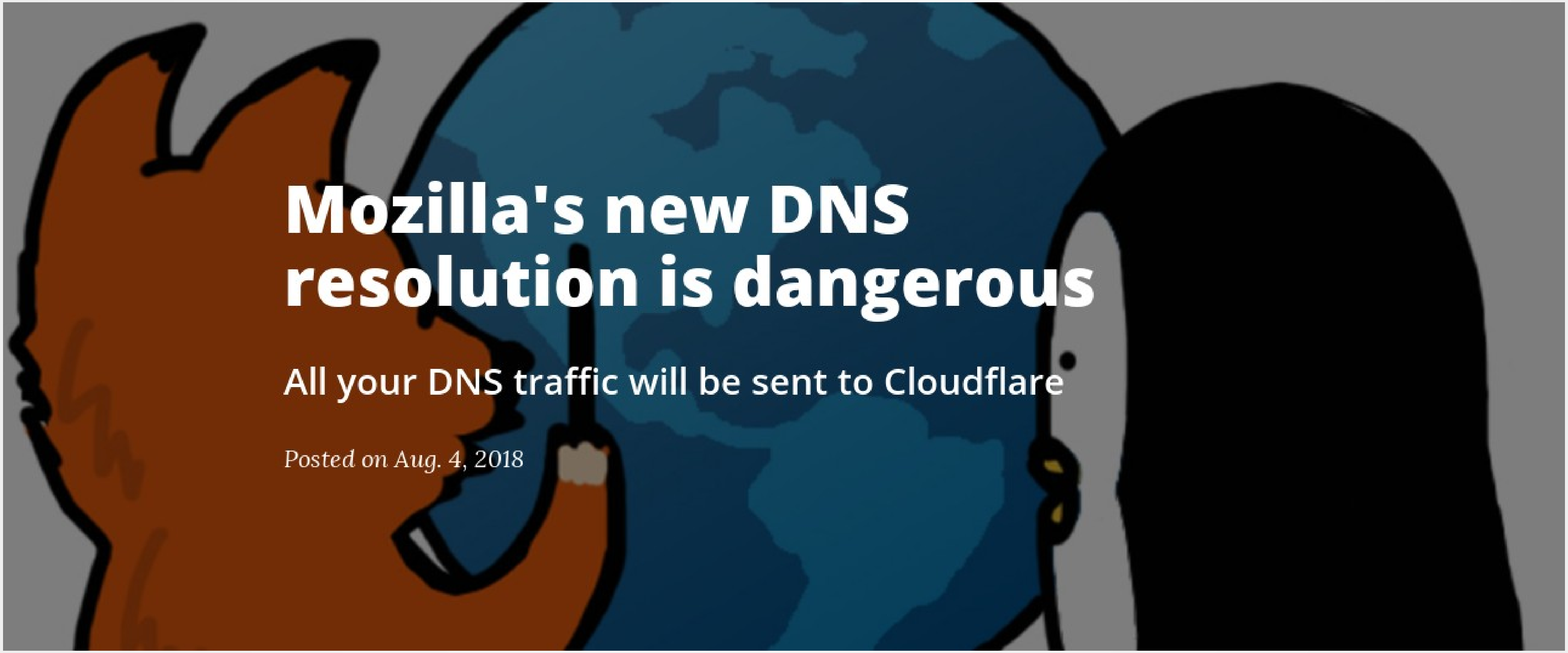
Foundation for Applied Privacy

DoH Kritik: HTTP Metadaten



```
Header: :method: POST
Header: :path: /query
Header: :authority: doh.appliedprivacy.net
Header: :scheme: https
Header: user-agent: Mozilla/5.0 (X11; Fedora; Linux x86_64; rv:66.0) Gecko/20100101 Firefox/66.0
Header: accept: application/dns-message
Header: accept-language: en-US,en;q=0.5
Header: accept-encoding: gzip, deflate, br
Header: cache-control: no-store
Header: content-type: application/dns-message
Header: content-length: 54
Header: te: trailers
```

Mozilla / Cloudflare Kritik



Mozilla's new DNS resolution is dangerous

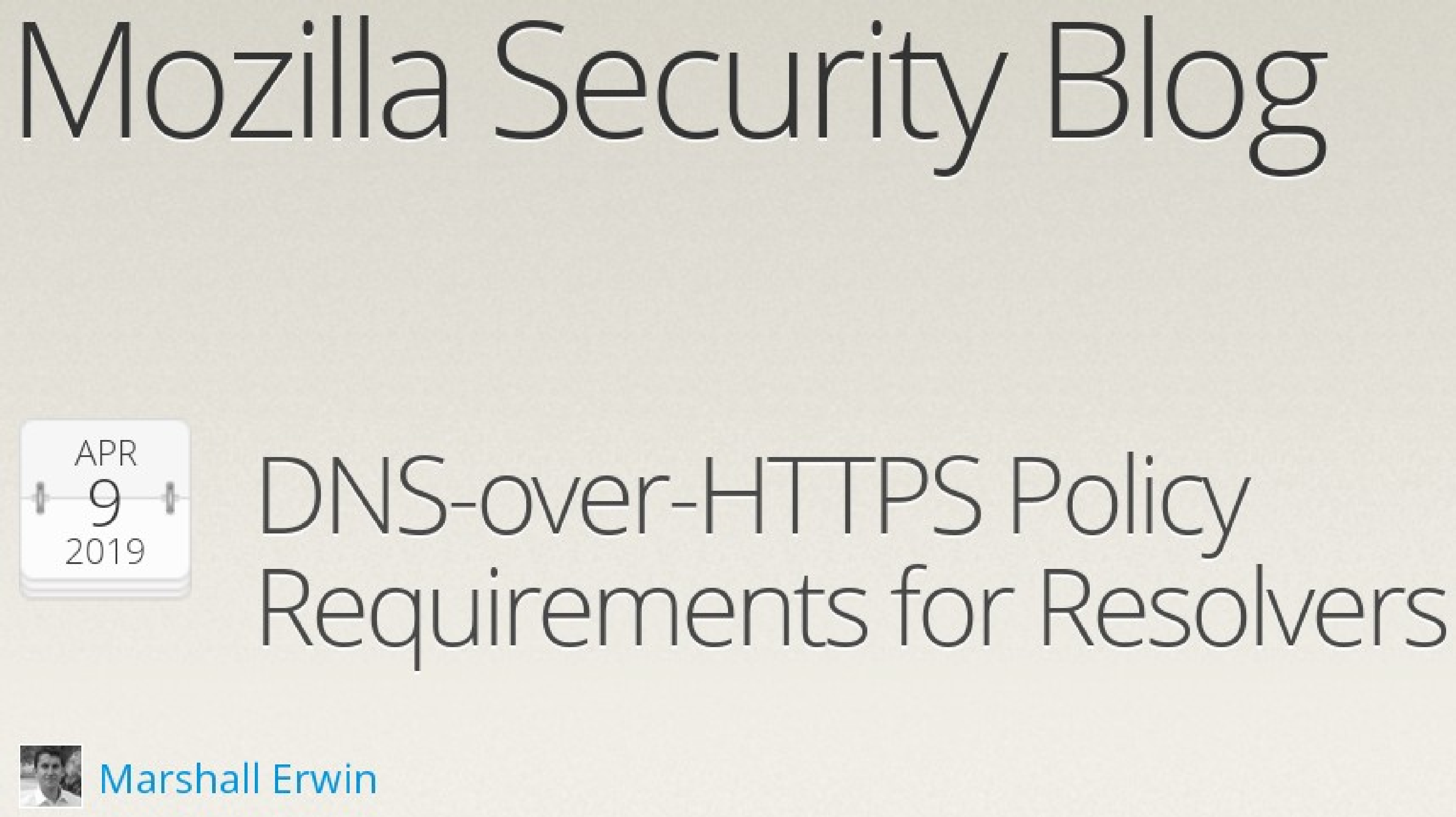
All your DNS traffic will be sent to Cloudflare

Posted on Aug. 4, 2018

Quelle: https://ungleich.ch

Foundation for Applied Privacy

Mozilla / Cloudflare Kritik



Mozilla Security Blog

APR 9 2019

DNS-over-HTTPS Policy Requirements for Resolvers

Marshall Erwin

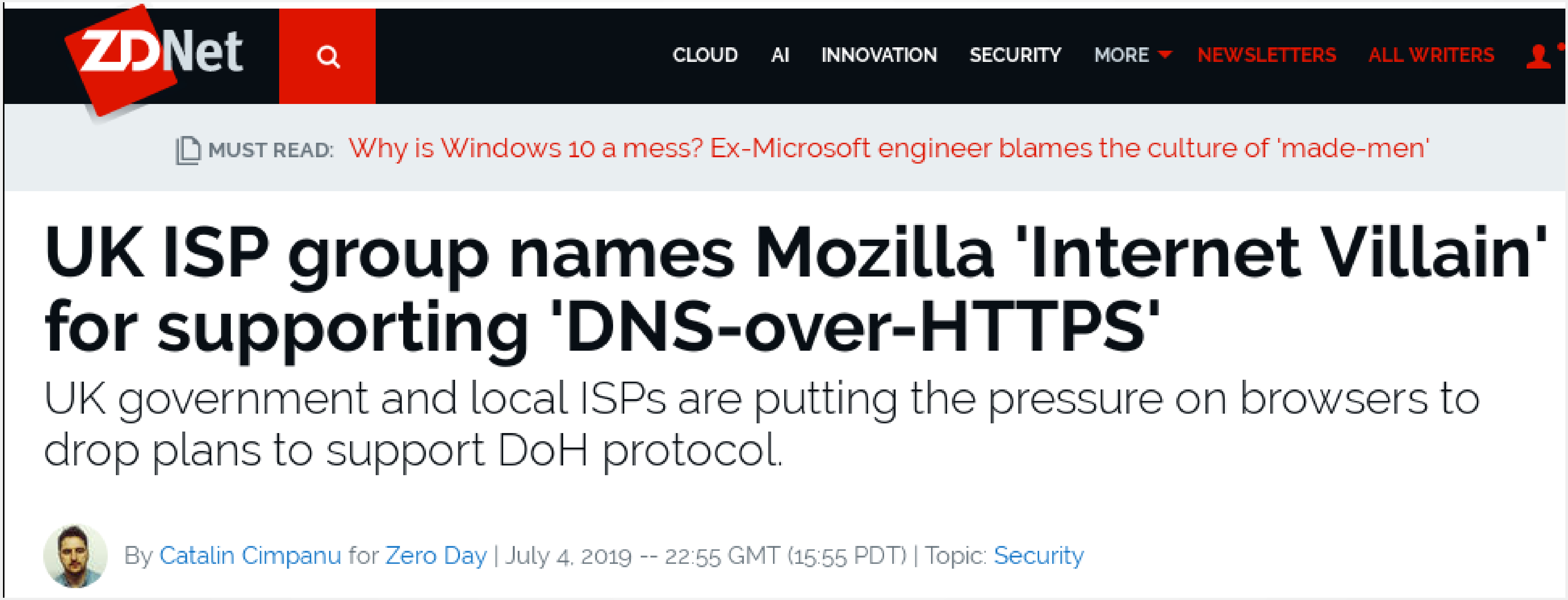
Foundation for Applied Privacy

Mozilla / Cloudflare Kritik

https://dnscrypt.info/public-servers/

https://github.com/curl/curl/wiki/DNS-over-HTTPS

Mozilla / ISPA UK Kritik



MUST READ: Why is Windows 10 a mess? Ex-Microsoft engineer blames the culture of 'made-men'

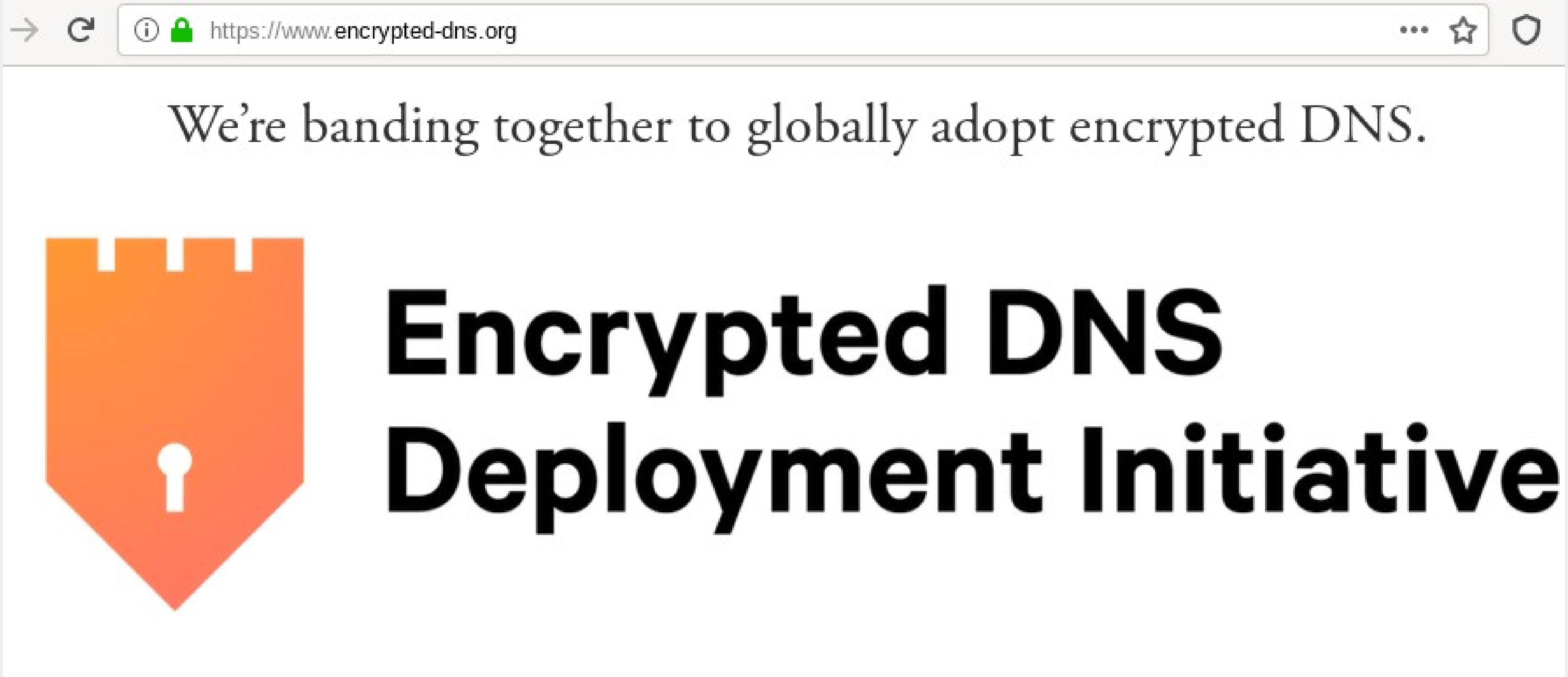
UK ISP group names Mozilla 'Internet Villain' for supporting 'DNS-over-HTTPS'

UK government and local ISPs are putting the pressure on browsers to drop plans to support DoH protocol.

By Catalin Cimpanu for Zero Day | July 4, 2019 -- 22:55 GMT (15:55 PDT) | Topic: Security

Quelle:
https://www.zdnet.com/article/uk-isp-group-names-mozilla-internet-villain-for-supporting-dns-over-https/

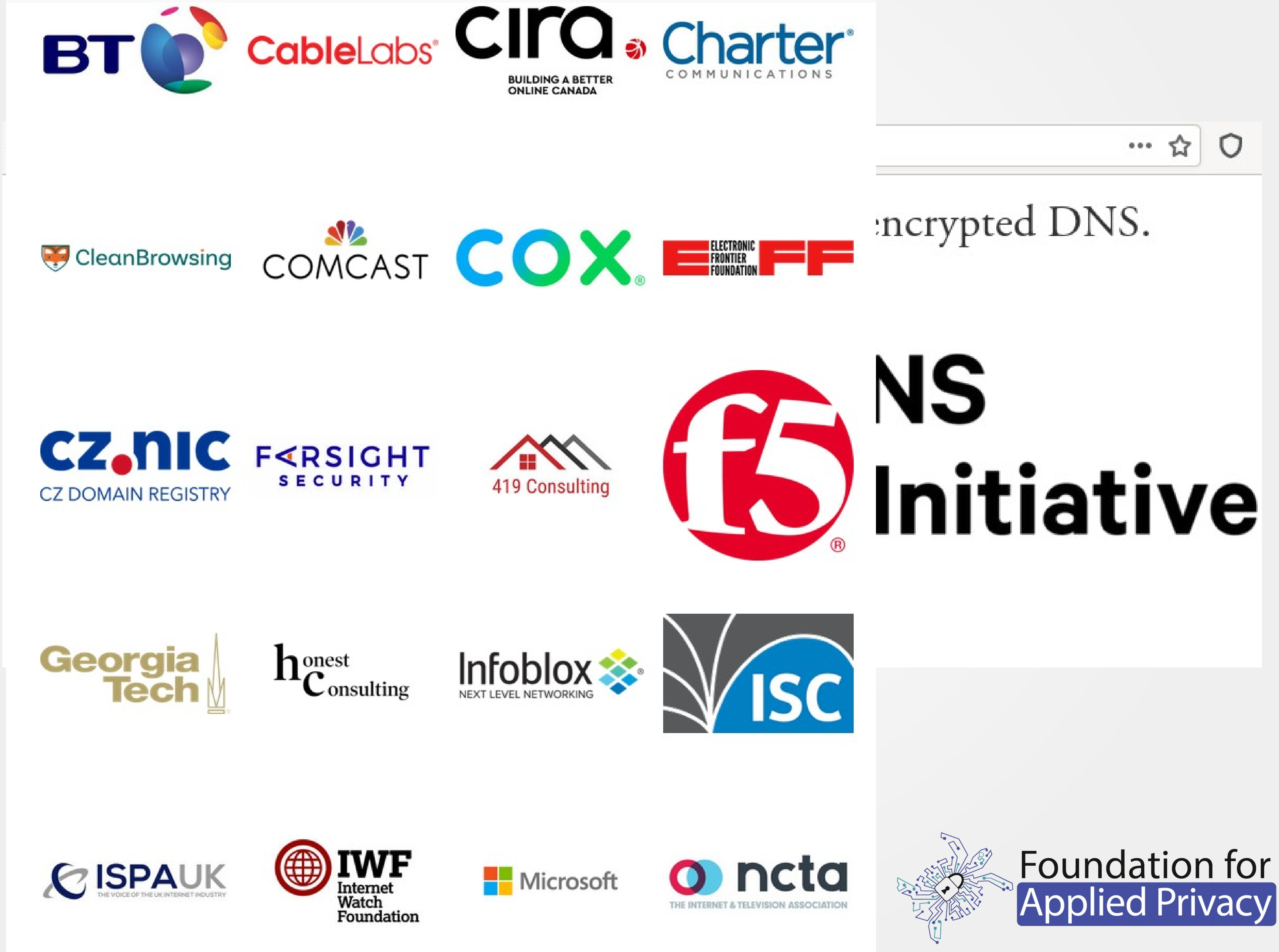
Foundation for Applied Privacy



https://www.encrypted-dns.org

We’re banding together to globally adopt encrypted DNS.

Encrypted DNS Deployment Initiative



ncrypted DNS.

NS Initiative

DoT vs. DoH

	DoT	DoH
Zensurresistenter	-	+
mit ESNI in Firefox kompatibel	-	+
wenig Metadaten für den Resolver	+	-
Server Software Verfügbarkeit	+	~
Einfaches einrichten (Client)	~	+

DoH / DoT – DNSSEC?

- Löst unterschiedliche Probleme
- Am besten in Kombination eingesetzt

DNS Privacy - Zukunft

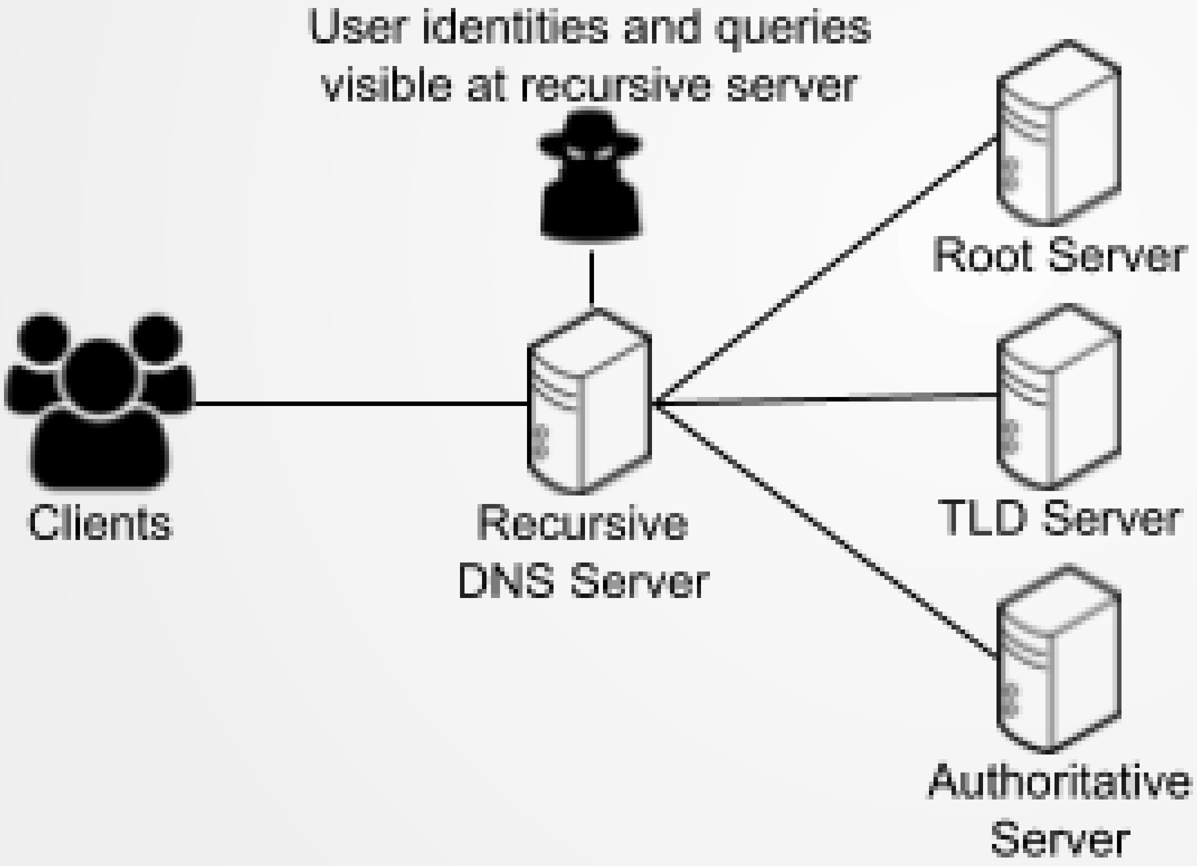
- DoH/DoT Server Discovery Protokolle
- Verschlüsselung zu authoritative Server
- Oblivious DNS

Oblivious DNS

PRINCETON UNIVERSITY

Foundation for Applied Privacy

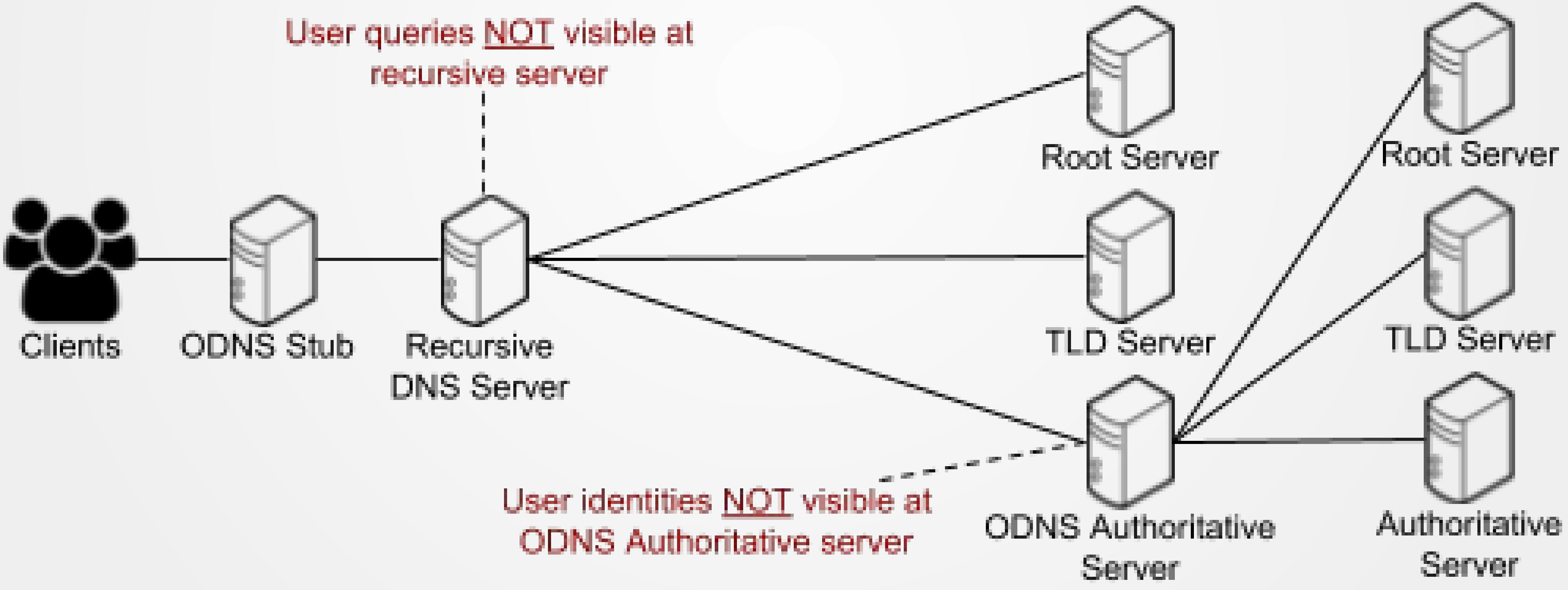
Klassisches DNS



Quelle: https://odns.cs.princeton.edu/

Foundation for Applied Privacy

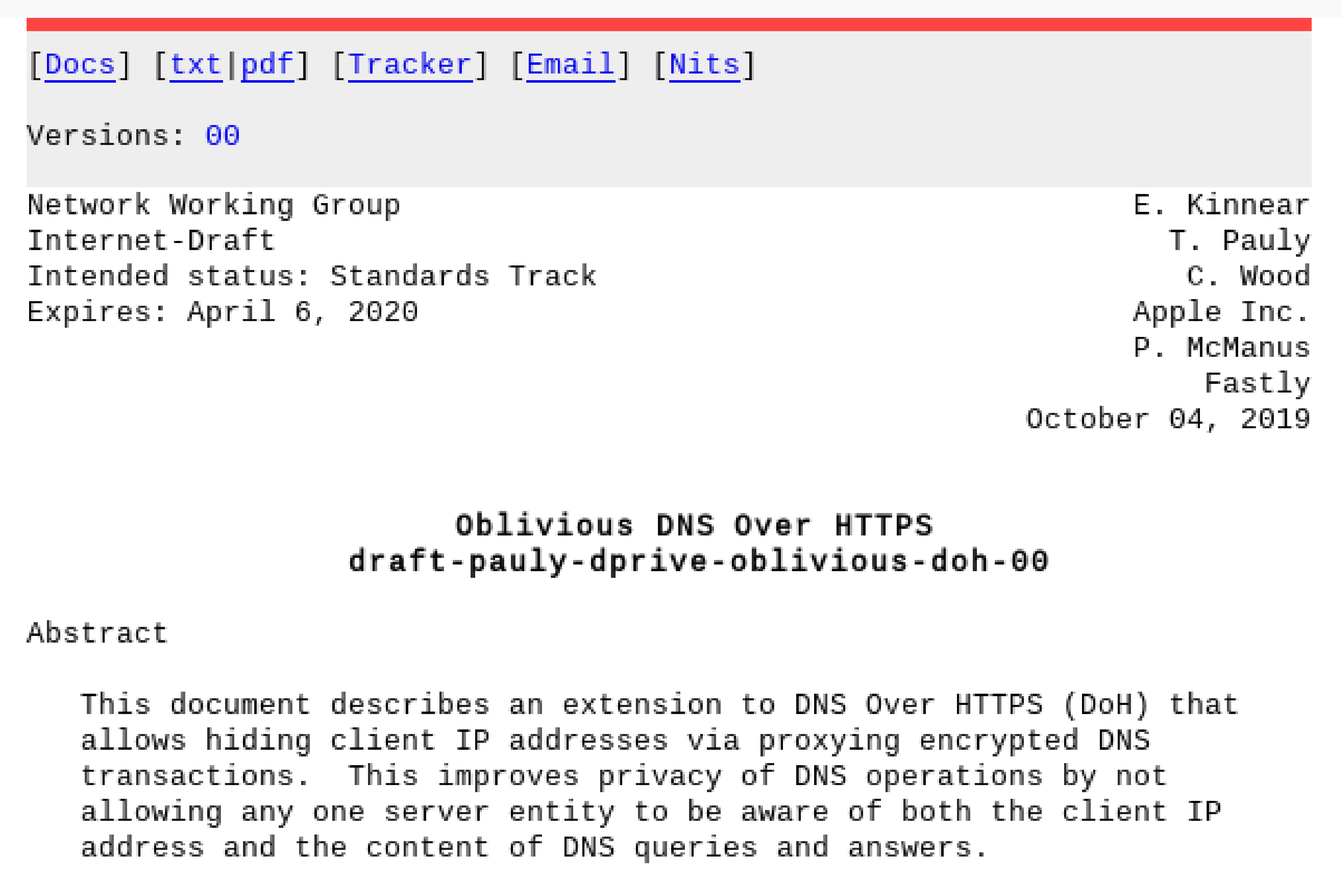
Oblivious DNS


User queries NOT visible at recursive server
Root Server
Root Server
Clients
ODNS Stub
Recursive DNS Server
TLD Server
TLD Server
User identities NOT visible at ODNS Authoritative server
ODNS Authoritative Server
Authoritative Server

Quelle: https://odns.cs.princeton.edu/

Foundation for Applied Privacy

Oblivious DNS-over-HTTPS



[Docs] [txt|pdf] [Tracker] [Email] [Nits]

Versions: 00

```
Network Working Group                                         E. Kinnear
Internet-Draft                                                  T. Pauly
Intended status: Standards Track                                 C. Wood
Expires: April 6, 2020                                        Apple Inc.
                                                              P. McManus
                                                                  Fastly
                                                        October 04, 2019
```

Oblivious DNS Over HTTPS
draft-pauly-dprive-oblivious-doh-00

Abstract

This document describes an extension to DNS Over HTTPS (DoH) that allows hiding client IP addresses via proxying encrypted DNS transactions. This improves privacy of DNS operations by not allowing any one server entity to be aware of both the client IP address and the content of DNS queries and answers.

Foundation for
Applied Privacy

Fazit (1/3)

DoT und DoH haben dieselben Kernziele

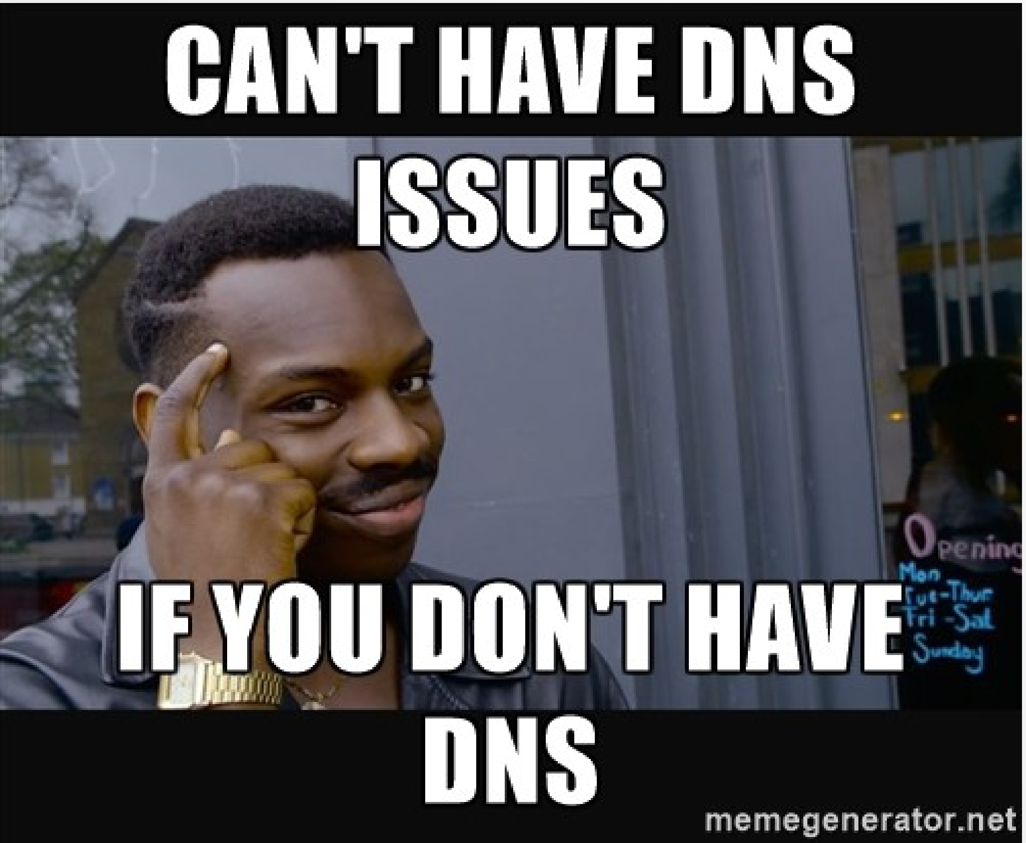
Foundation for Applied Privacy

Fazit (2/3)

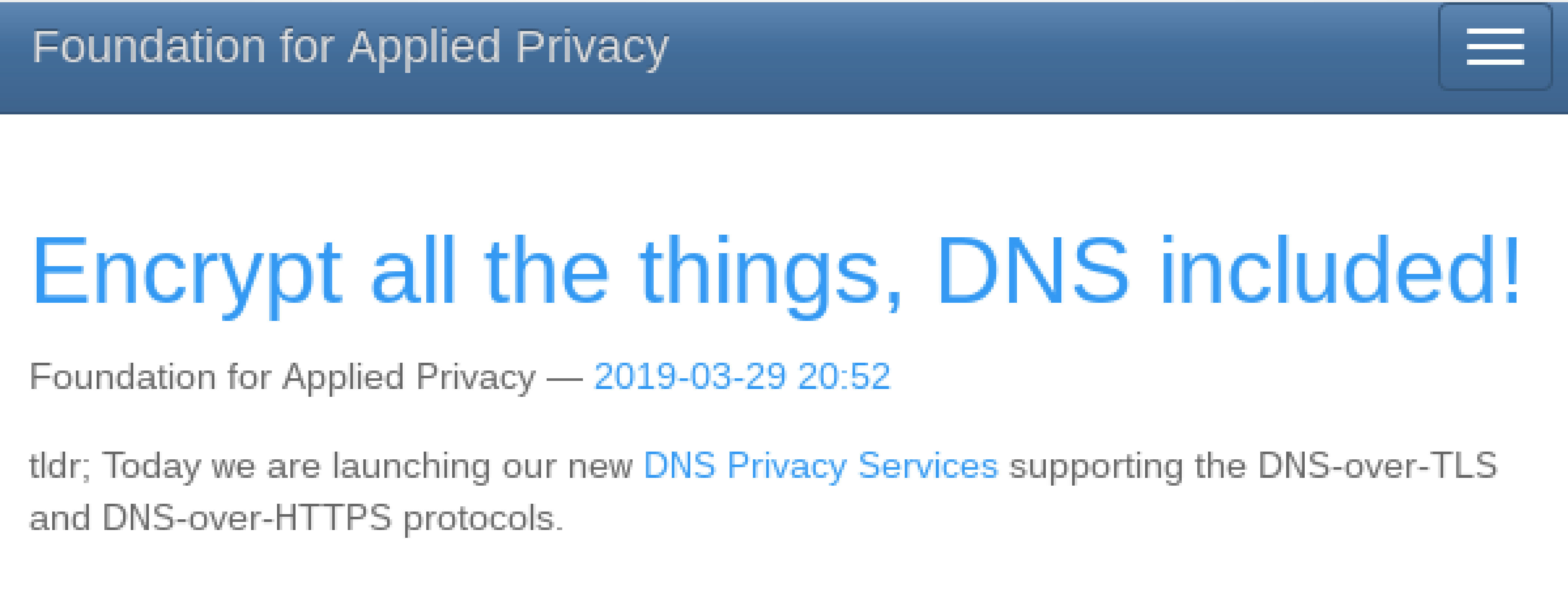
- Trotz DoH/DoT sind Metadaten von HTTPS Verbindungen sichtbar (ESNI erforderlich!)
- DoT gibt weniger Metadaten preis als DoH
- Verschlüsselt euren DNS Traffic!
  (es ist sehr einfach)

Fazit (3/3)

Verwende (weiterhin) **Tor Browser** für die stärksten Privacyeigenschaften



Foundation for Applied Privacy



Foundation for Applied Privacy

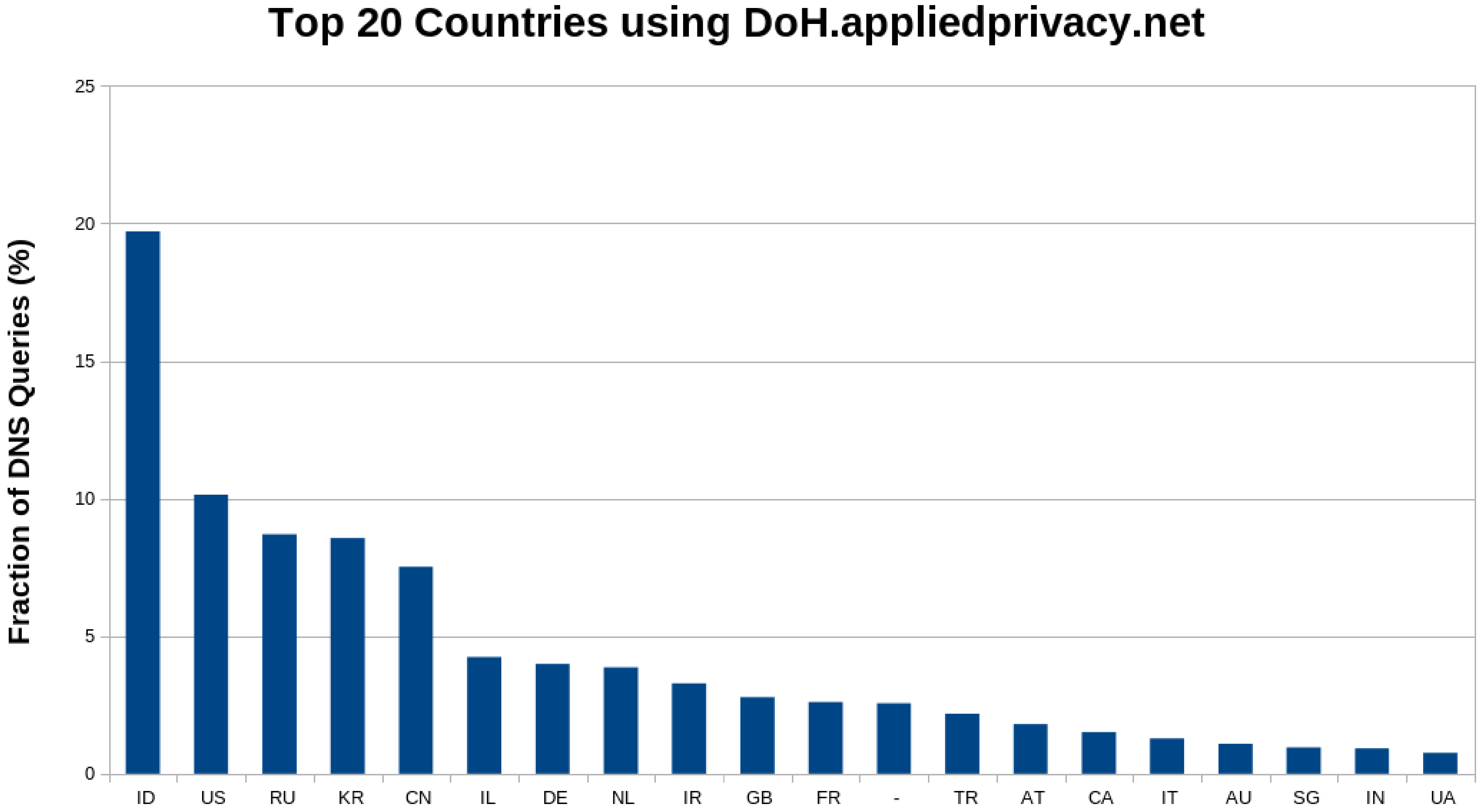
Encrypt all the things, DNS included!

Foundation for Applied Privacy — 2019-03-29 20:52

tldr; Today we are launching our new DNS Privacy Services supporting the DNS-over-TLS and DNS-over-HTTPS protocols.

https://appliedprivacy.net/posts/dns-privacy-services-launch/

Foundation for Applied Privacy



Foundation for Applied Privacy

Unsere DNS Privacy Resolver

https://applied-privacy.net/services/dns/

Foundation for Applied Privacy

Fragen?

✉ contact@appliedprivacy.net

@applied_privacy

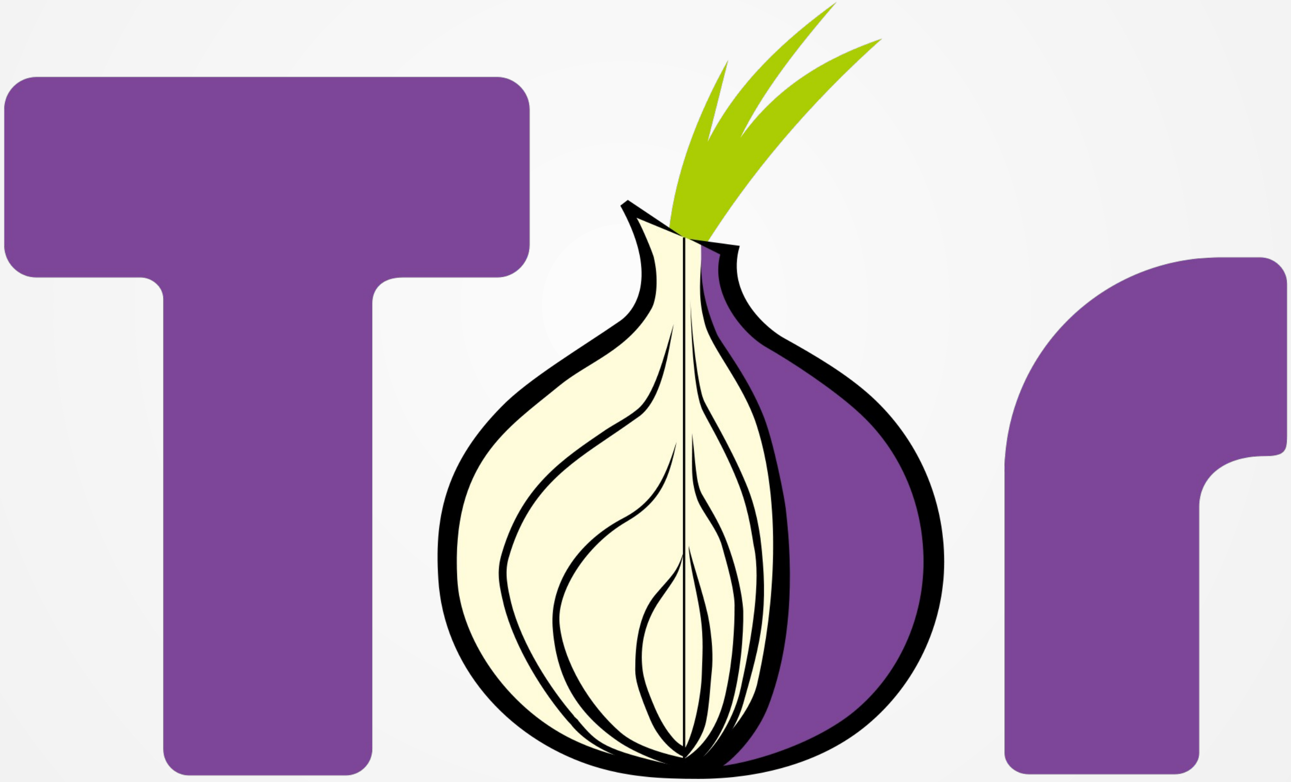
https://mastodon.social/@applied_privacy

https://applied-privacy.net

Foundation for
Applied Privacy

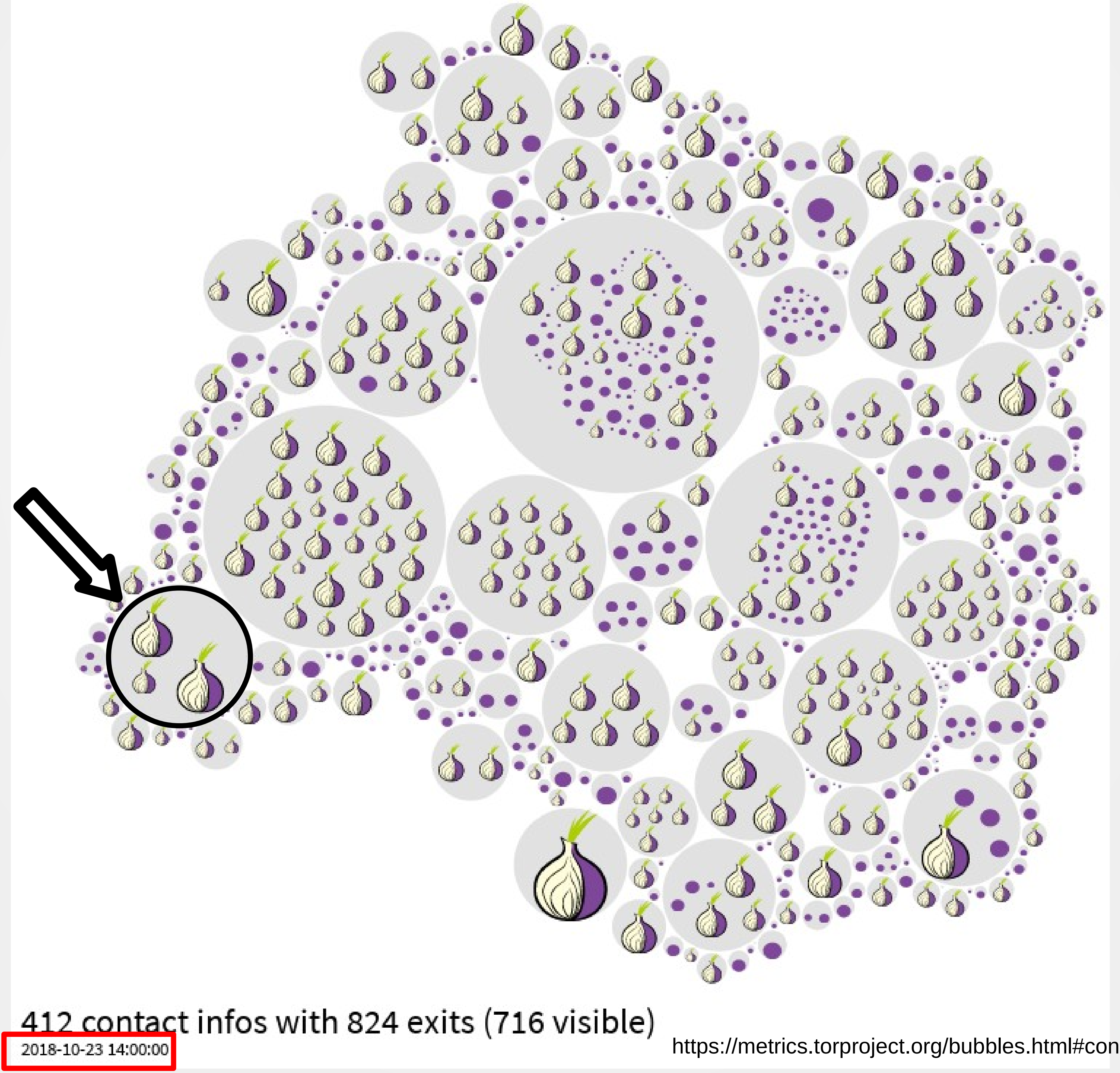
STICKERS!!!!!11

Bonus Slides Unlocked



Foundation for
Applied Privacy

PW18

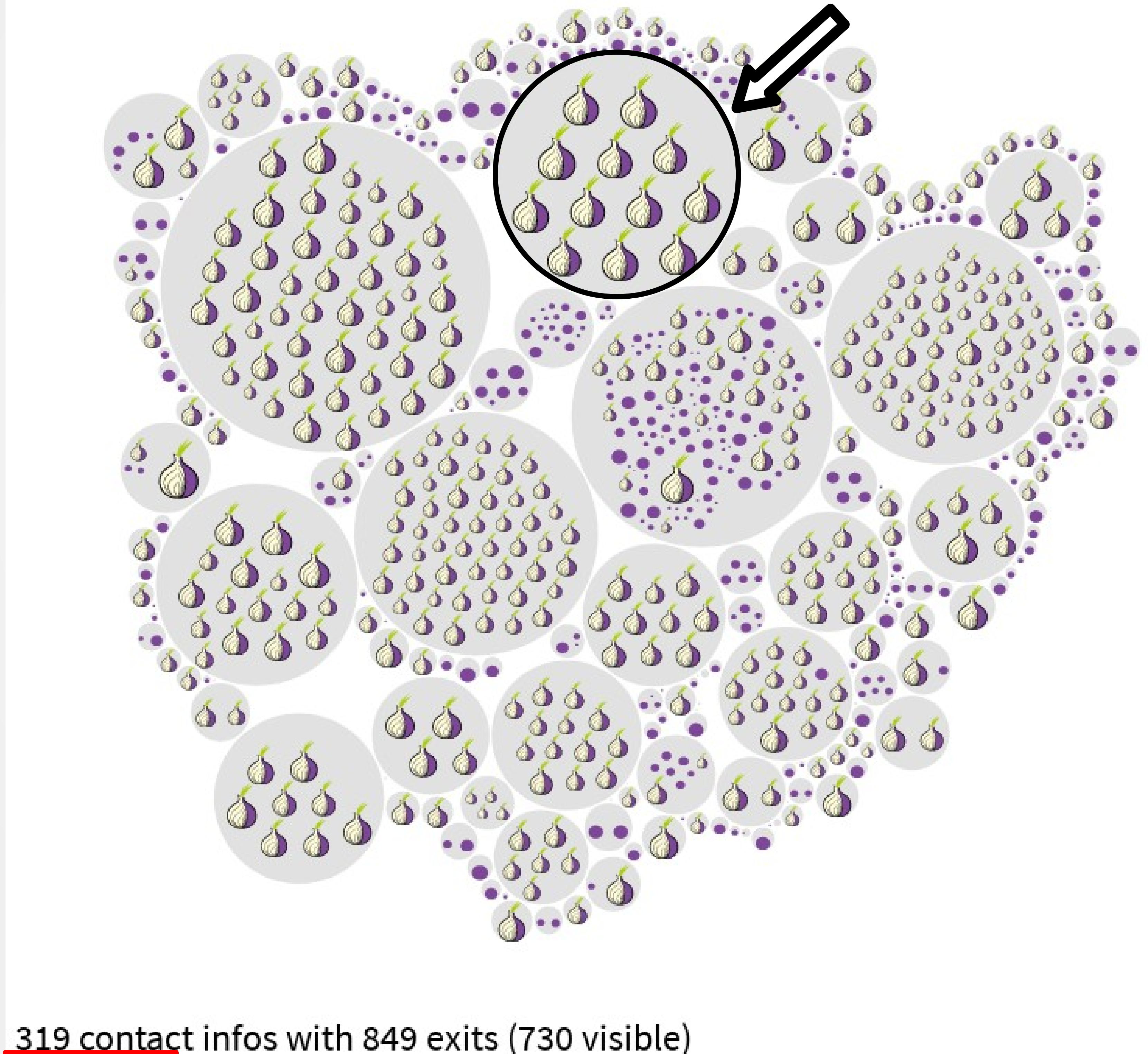


412 contact infos with 824 exits (716 visible)

2018-10-23 14:00:00

https://metrics.torproject.org/bubbles.html#contact-exits-only

PW19

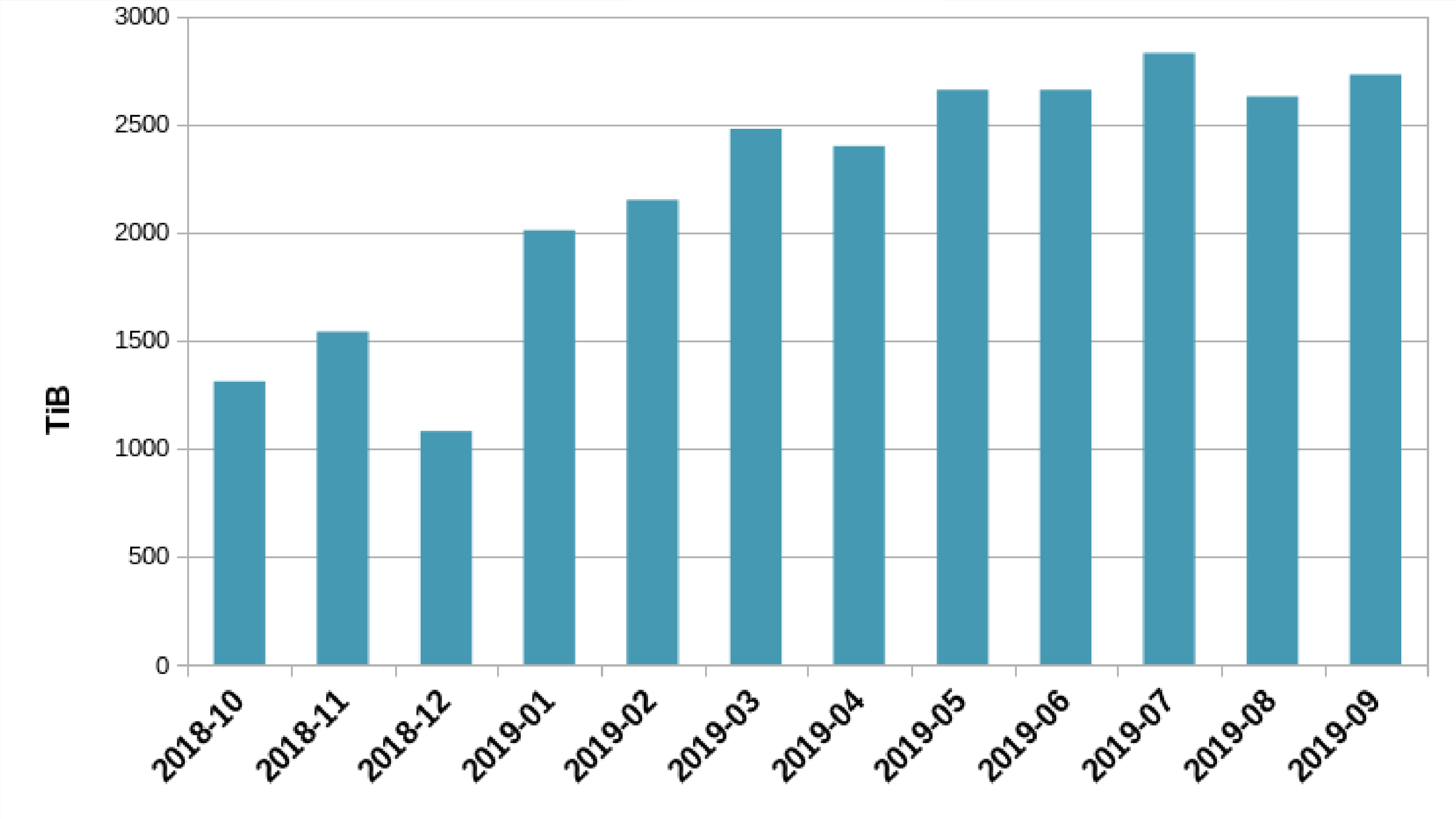


319 contact infos with 849 exits (730 visible)

2019-10-24 11:00:00

https://metrics.torproject.org/bubbles.html#contact-exits-only

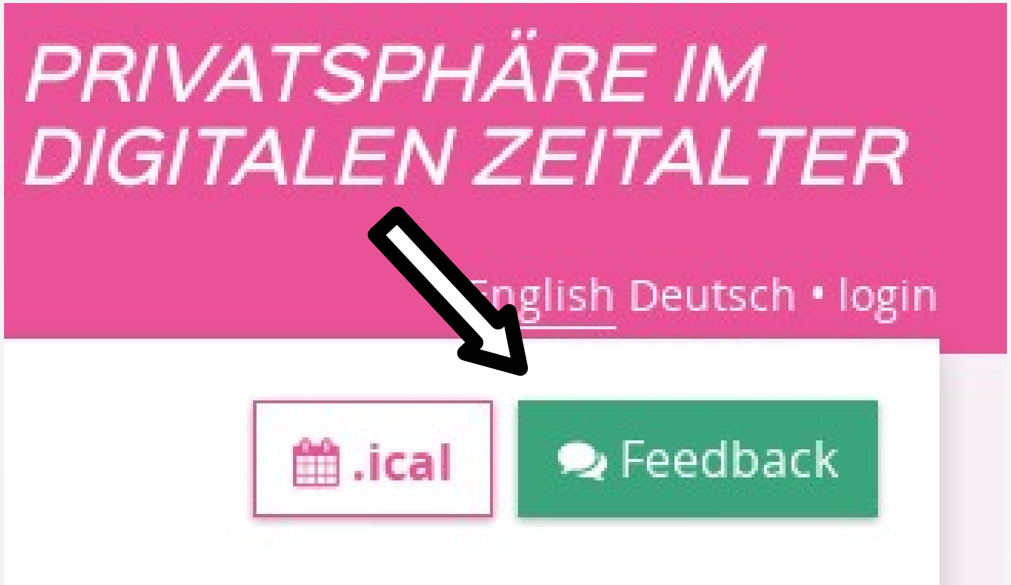
Monatliche Traffic Stats



Foundation for Applied Privacy

~24 Petabibyte Traffic

01.09.2018 - 31.08.2019


PRIVATSPHÄRE IM DIGITALEN ZEITALTER
English Deutsch • login
.ical
Feedback