

DoH, DoT, what?

**Eine Einführung in die DNS Privacy
Protokolle DoH und DoT.**



Foundation for
Applied Privacy

Foundation for Applied Privacy

- Non-profit Privacy Infrastruktur Provider
- PETS Dienste für die Öffentlichkeit
- 2018 gegründet
- Top 3 Tor Exit Relay Operator (weltweit)
- > 2000 Terabyte monatlicher Netzwerkverkehr



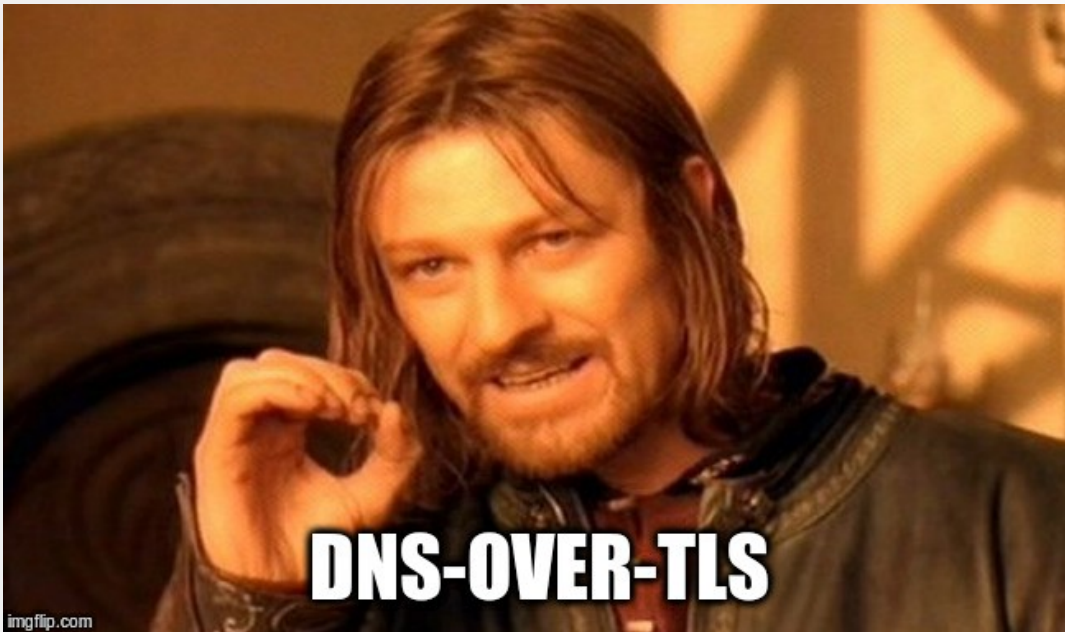
Foundation for
Applied Privacy

Ziele dieses Vortrags

- Welches Problem lösen DoH/DoT?
- Wie ist DoT und DoH aufgebaut?
- Welche Software gibts?
- Kritikpunkte

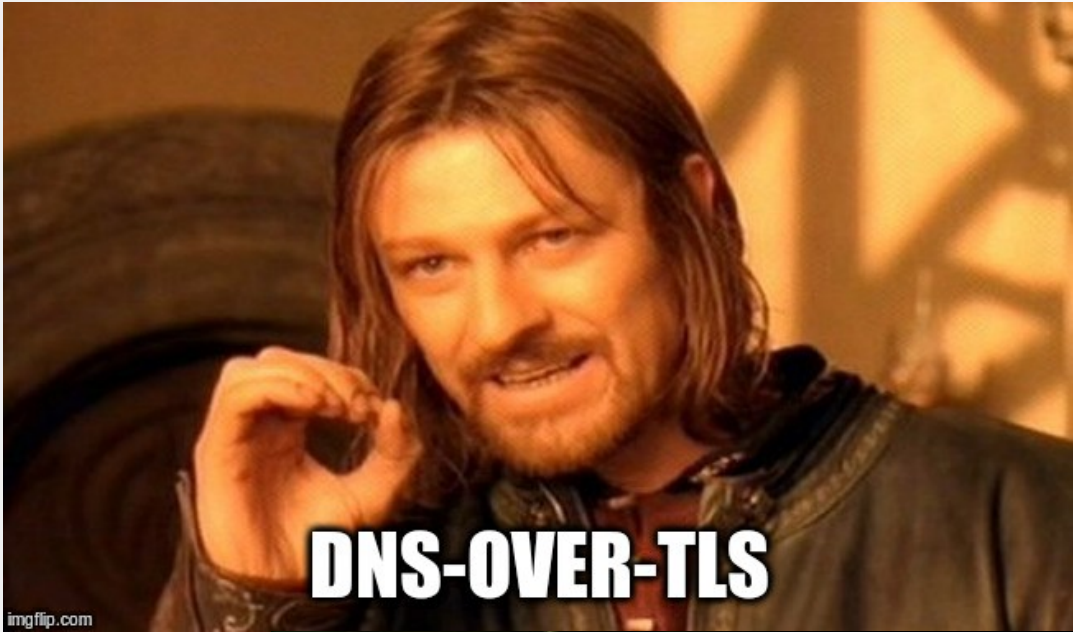


Ziele dieses Vortrags



Foundation for
Applied Privacy

Ziele dieses Vortrags

A meme featuring Legolas from The Lord of the Rings. He is shown from the chest up, with long brown hair and a slight smile, looking towards the camera. The background is a warm, golden light. The text "DNS-OVER-TLS" is overlaid in white, bold, sans-serif font at the bottom.

DNS-OVER-TLS

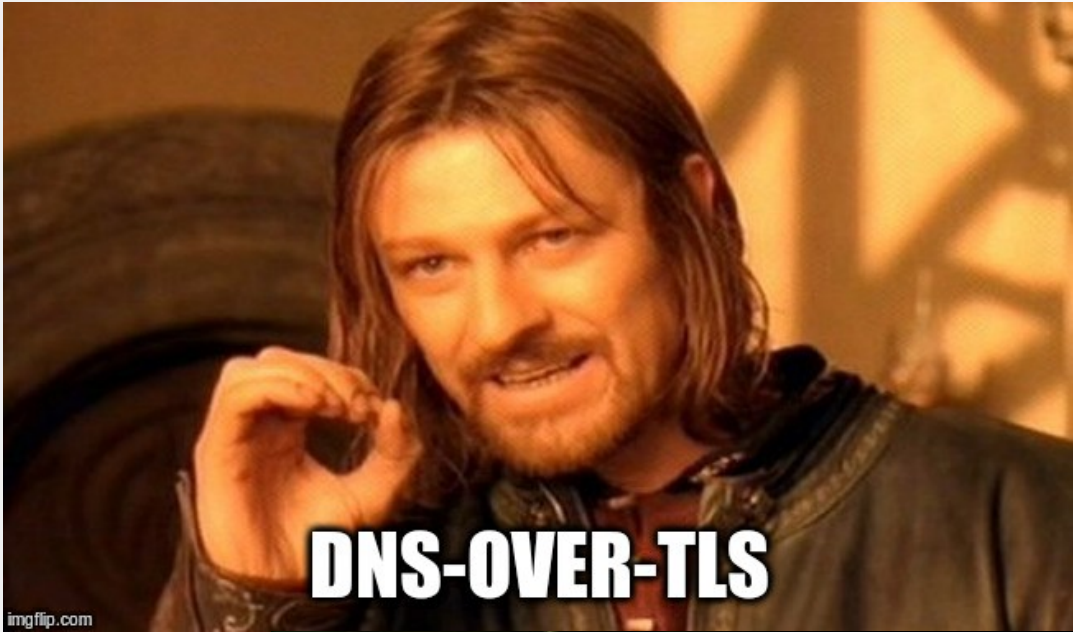
A meme featuring Gandalf the White from The Lord of the Rings. He is shown from the chest up, with long white hair and a long white beard, holding a wooden staff. The background is dark. The text "DNS-OVER-HTTPS" is overlaid in white, bold, sans-serif font at the top.

DNS-OVER-HTTPS

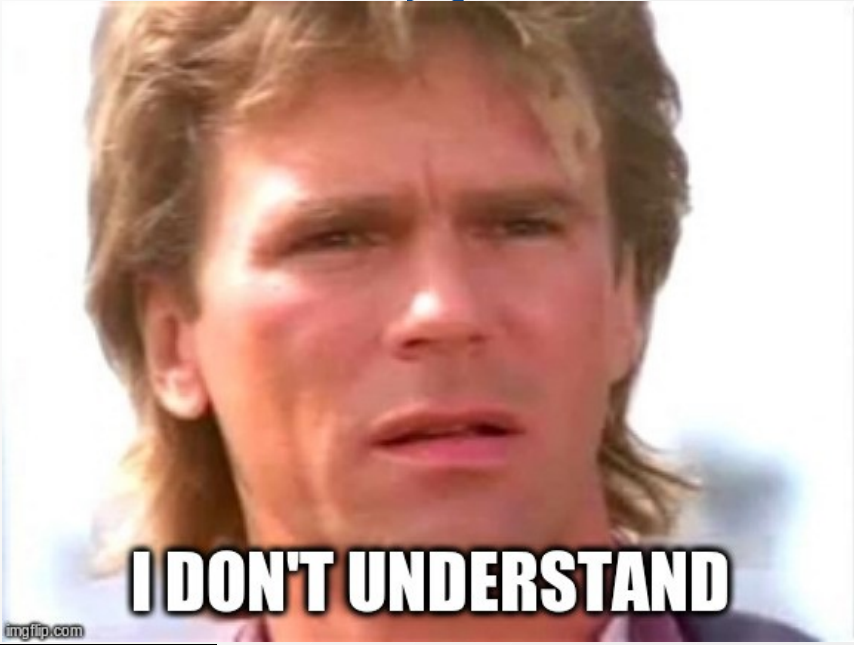


Foundation for
Applied Privacy

Ziele dieses Vortrags

A meme featuring Aragorn from The Lord of the Rings. He has long brown hair and a beard, looking slightly to the side with a faint smile. The text "DNS-OVER-TLS" is overlaid in white, bold, sans-serif font at the bottom.

DNS-OVER-TLS

A meme featuring a man with light brown hair, looking directly at the camera with a confused expression. The text "I DON'T UNDERSTAND" is overlaid in white, bold, sans-serif font at the bottom.

I DON'T UNDERSTAND

A meme featuring Gandalf the White from The Lord of the Rings. He has a long white beard and hair, holding a wooden staff. The text "DNS-OVER-HTTPS" is overlaid in white, bold, sans-serif font at the top.

DNS-OVER-HTTPS



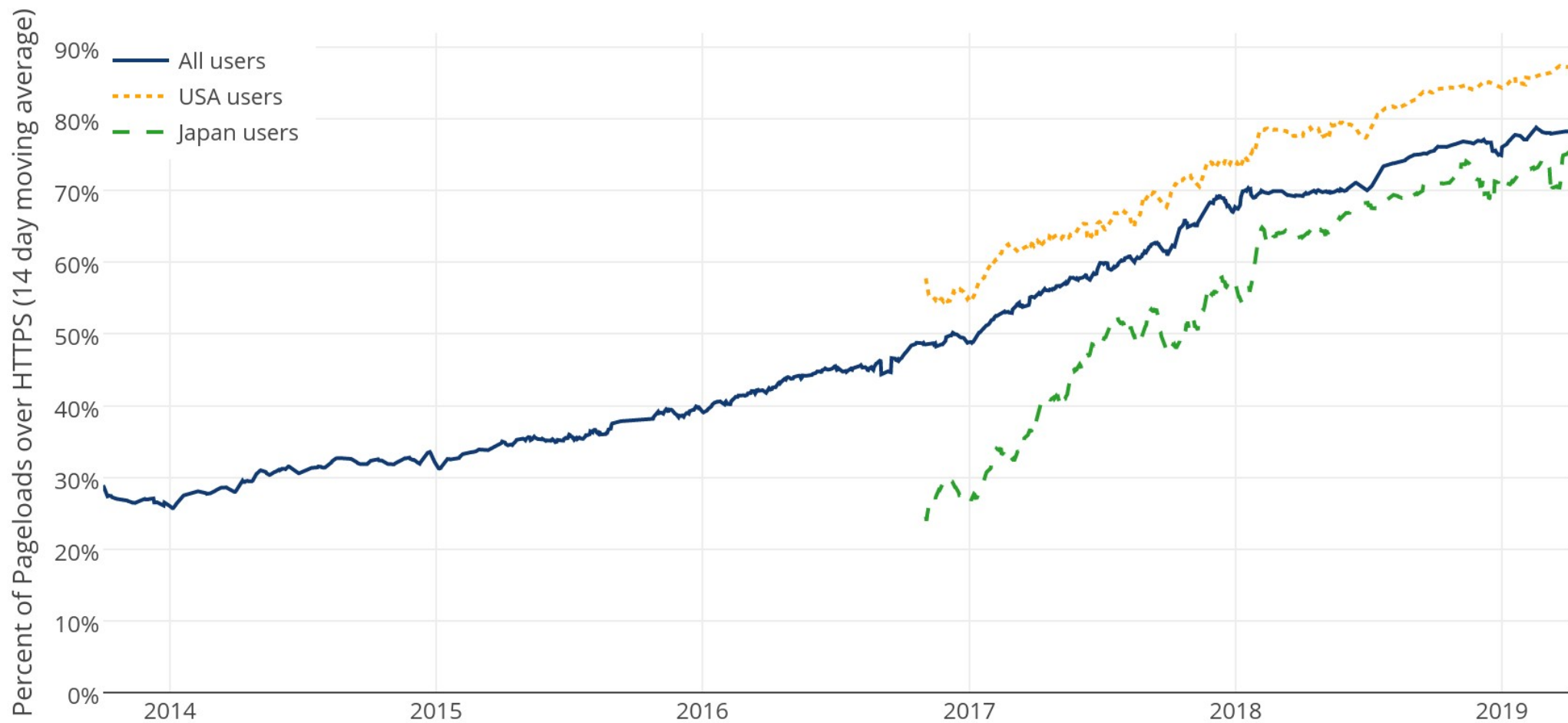
Foundation for
Applied Privacy

Warum DNS Privacy?



Foundation for
Applied Privacy

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



Foundation for
Applied Privacy



Foundation for
Applied Privacy

Ziel

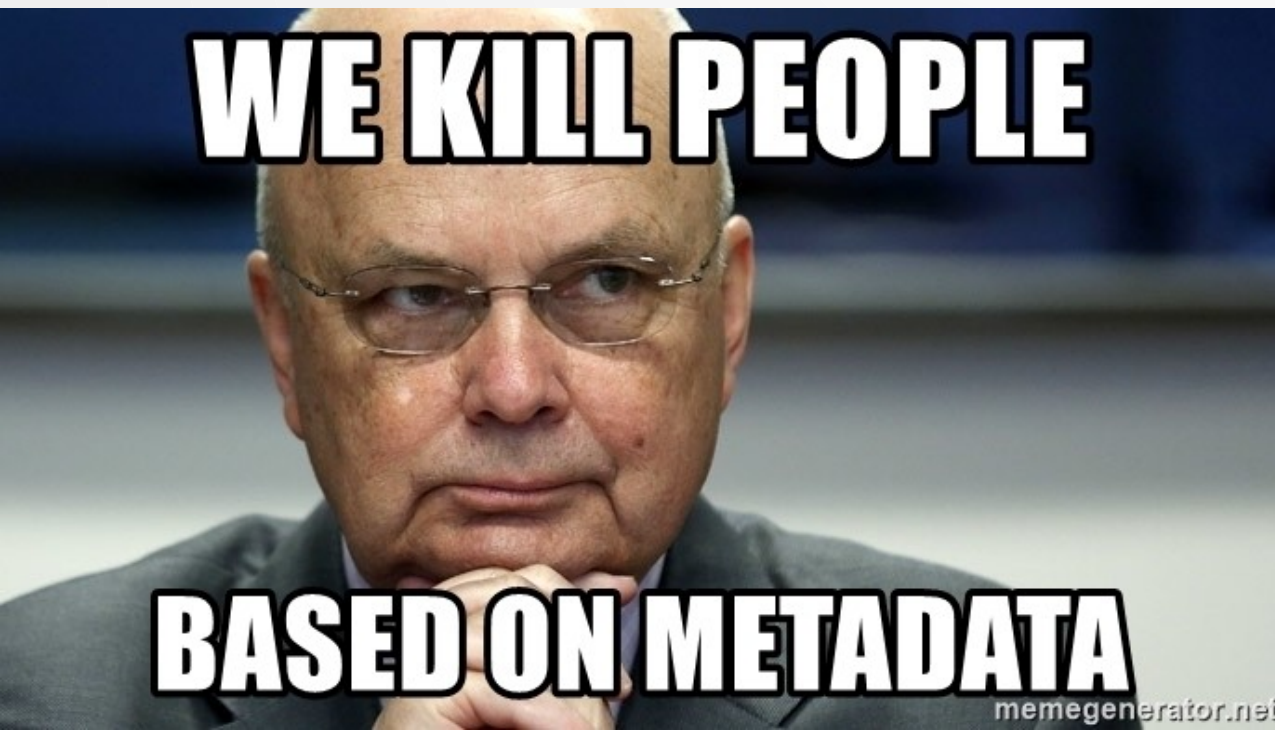
Schutz von Metadaten (Hostname)



Foundation for
Applied Privacy

Warum ist das wichtig?

- Ermöglicht privateres browsen
- Erschwert Zensur
- Erschwert Massenüberwachung



Foundation for
Applied Privacy

Warum ist das aktuell noch nicht möglich?

(ohne Torbrowser)



Foundation for
Applied Privacy



User/Browser

de.wikipedia.org
Webserver

DNS
Resolver



Foundation for
Applied Privacy

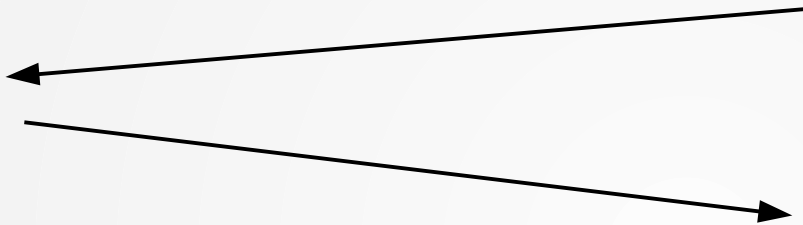


User/Browser

de.wikipedia.org
Webserver

DNS
Resolver

DNS: de.wikipedia.org



Foundation for
Applied Privacy



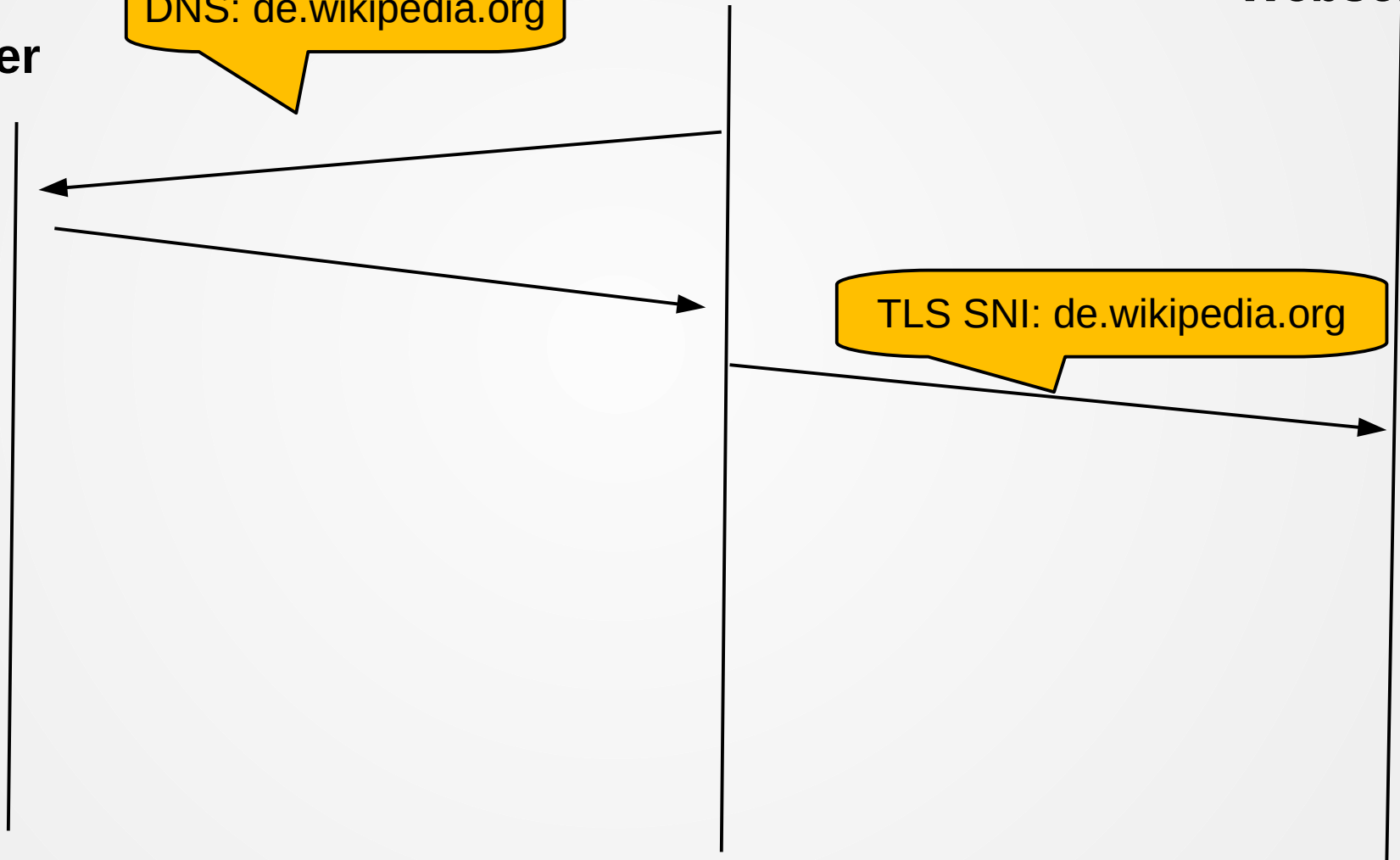
User/Browser

de.wikipedia.org
Webserver

DNS
Resolver

DNS: de.wikipedia.org

TLS SNI: de.wikipedia.org



Foundation for
Applied Privacy



User/Browser

de.wikipedia.org
Webserver

DNS
Resolver

DNS: de.wikipedia.org

TLS SNI: de.wikipedia.org

TLS cert: *.wikipedia.org



Foundation for
Applied Privacy



User/Browser

de.wikipedia.org
Webserver

DNS
Resolver

DNS: de.wikipedia.org

TLS SNI: de.wikipedia.org

TLS cert: *.wikipedia.org

TLS Verbindung



Foundation for
Applied Privacy



User/Browser

de.wikipedia.org
Webserver

DNS
Resolver

DNS: de.wikipedia.org

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



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



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



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			oted
Handshake Type: Certificate (11)			en=0
Length: 3236			
Certificates Length: 3233			
▼ Certificates (3233 bytes)			
Certificate Length: 2101			
▼ Certificate: 3082083130820719a003020102020c1640c5d45d2ec4d94c... (id-at-commonName=*.wikipedia.org)			
▶ signedCertificate			
▶ algorithmIdentifier (sha256WithRSAEncryption)			
Padding: 0			

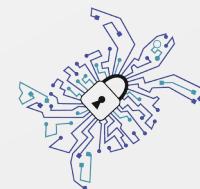


Problem/Leak	Lösung	Aufwand für Webseitbetreiber
---------------------	---------------	---

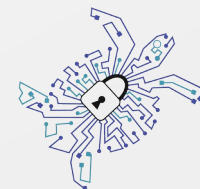


**Foundation for
Applied Privacy**

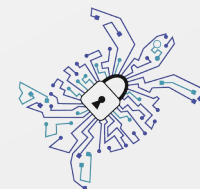
Problem/Leak	Lösung	Aufwand für Webseitbetreiber
IP Adresse	CDN/vHosts	~



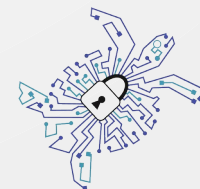
Problem/Leak	Lösung	Aufwand für Webseitbetreiber
IP Adresse	CDN/vHosts	~
TLS SNI	Work in Progress: Encrypted SNI (ESNI)	Aufwand gross (Webserver + DNS)



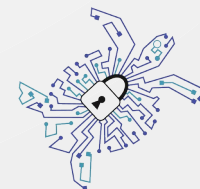
Problem/Leak	Lösung	Aufwand für Webseitbetreiber
IP Adresse	CDN/vHosts	~
TLS SNI	Work in Progress: Encrypted SNI (ESNI)	Aufwand gross (Webserver + DNS)
TLS Zertifikat	TLS 1.3	TLS 1.3 ausrollen



Problem/Leak	Lösung	Aufwand für Webseitbetreiber
IP Adresse	CDN/vHosts	~
TLS SNI	Work in Progress: Encrypted SNI (ESNI)	Aufwand gross (Webserver + DNS)
TLS Zertifikat	TLS 1.3	TLS 1.3 ausrollen
DNS	DoH/DoT/...	Kein Aufwand (Betreiber nicht involviert)



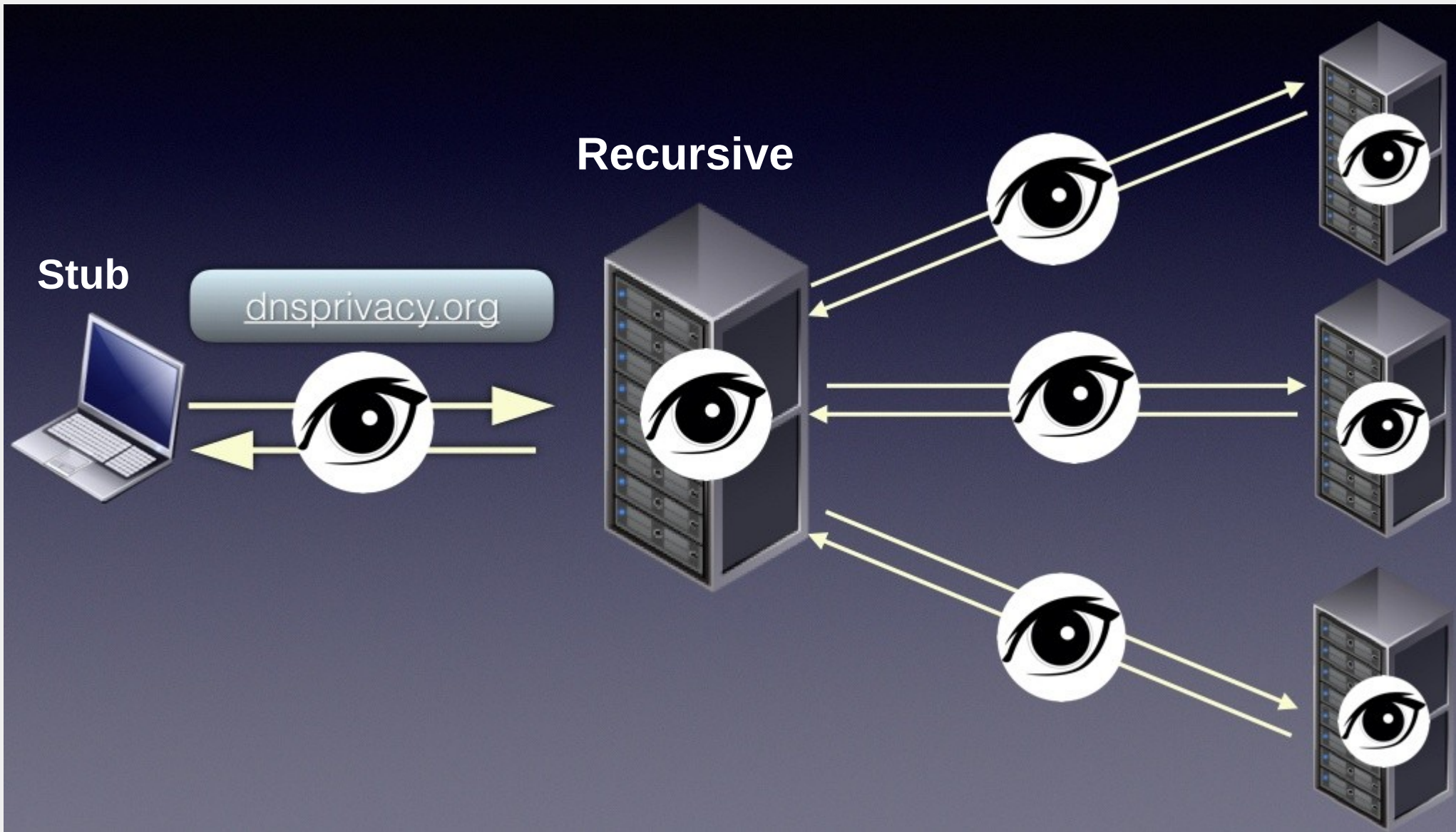
Problem/Leak	Lösung	Aufwand für Webseitbetreiber
IP Adresse	CDN/vHosts	~
TLS SNI	Work in Progress: Encrypted SNI (ESNI)	Aufwand gross (Webserver + DNS)
TLS Zertifikat	TLS 1.3	TLS 1.3 ausrollen
DNS	DoH/DoT/...	Kein Aufwand (Betreiber nicht involviert)



DNS



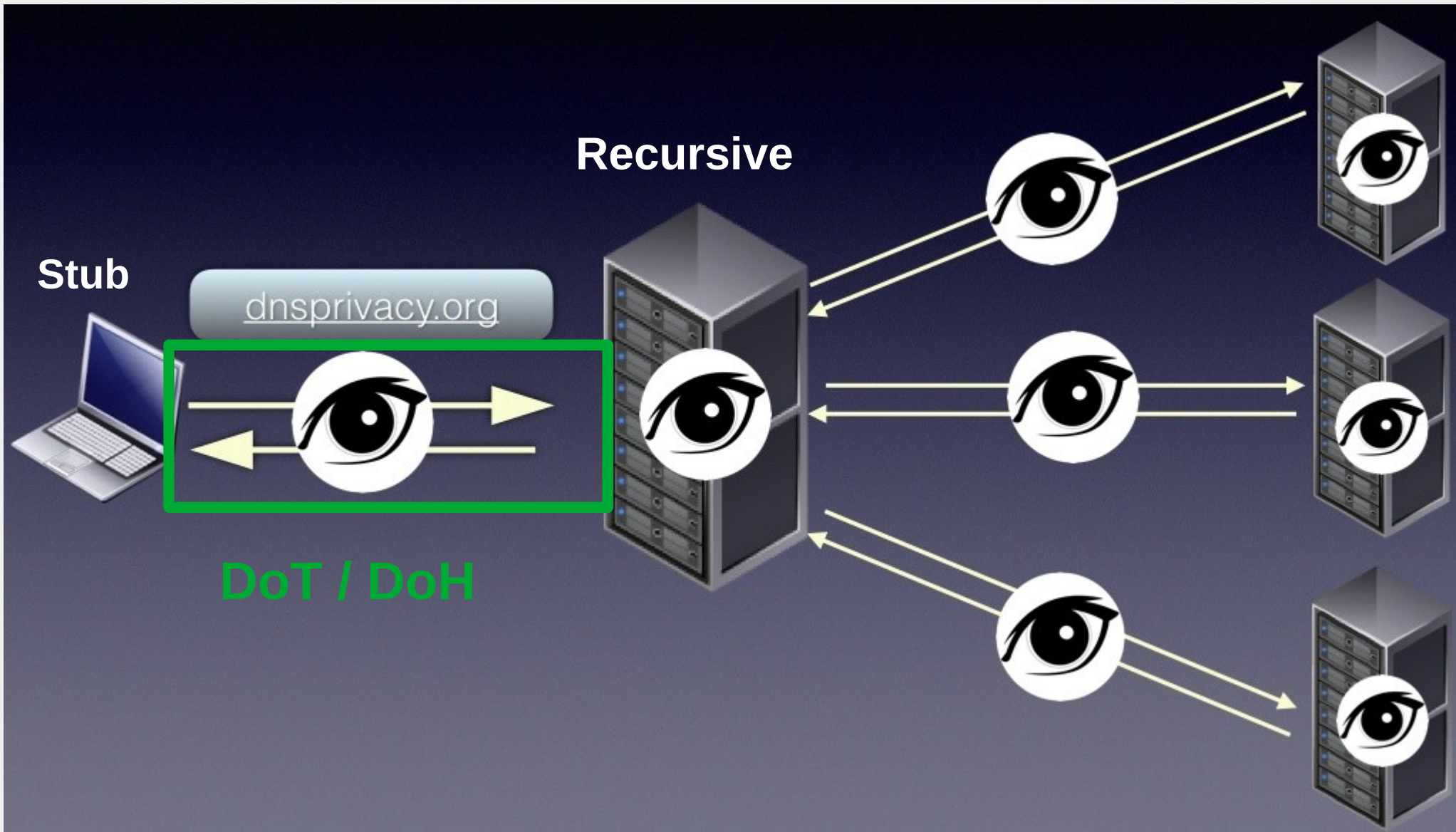
Foundation for
Applied Privacy



Quelle: dnsprivacy.org



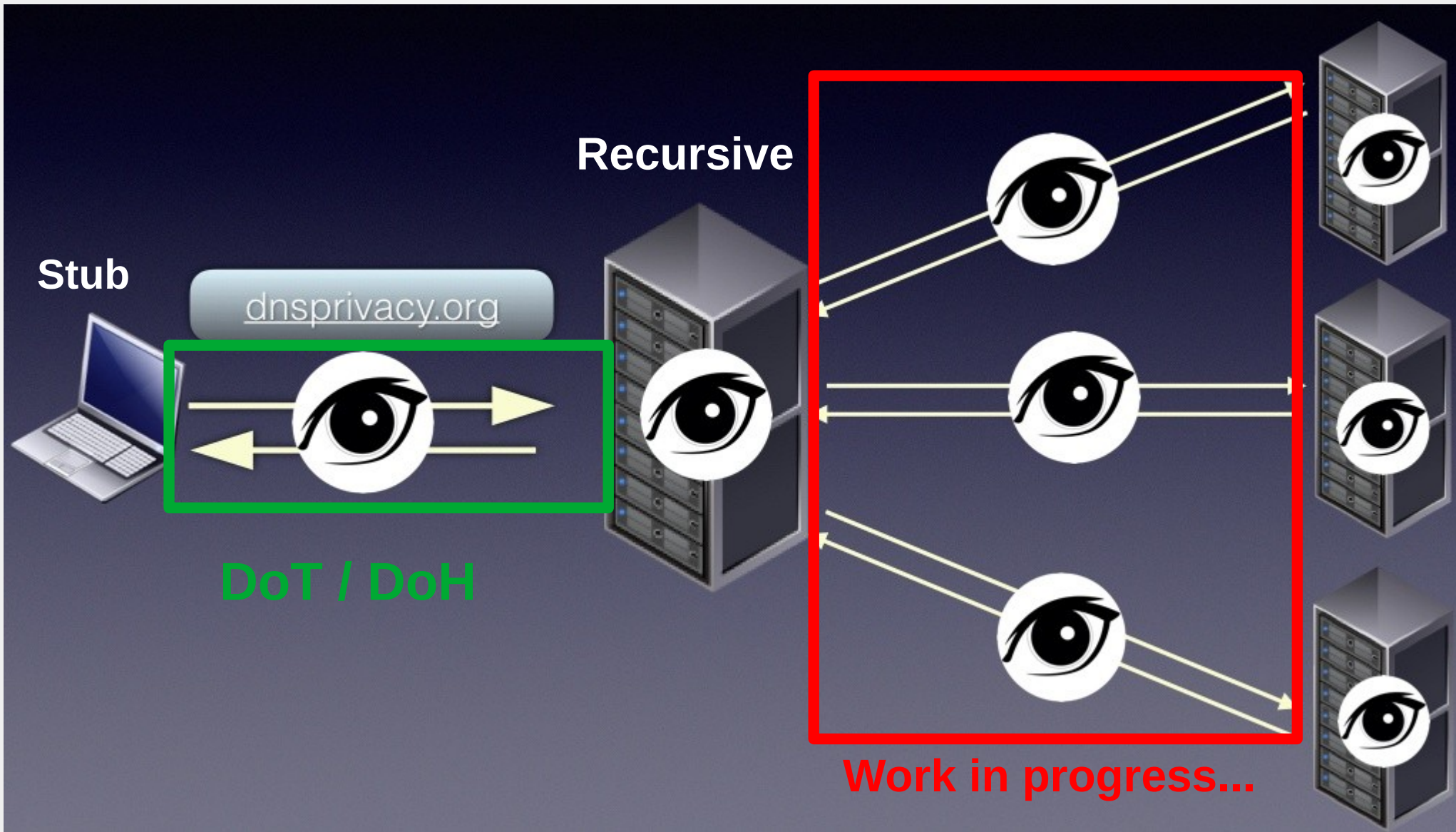
Foundation for
Applied Privacy



Quelle: dnsprivacy.org



Foundation for
Applied Privacy



Quelle: dnsprivacy.org



Foundation for
Applied Privacy

DNS-over-TLS (DoT)

RFC7858 (Mai 2016)

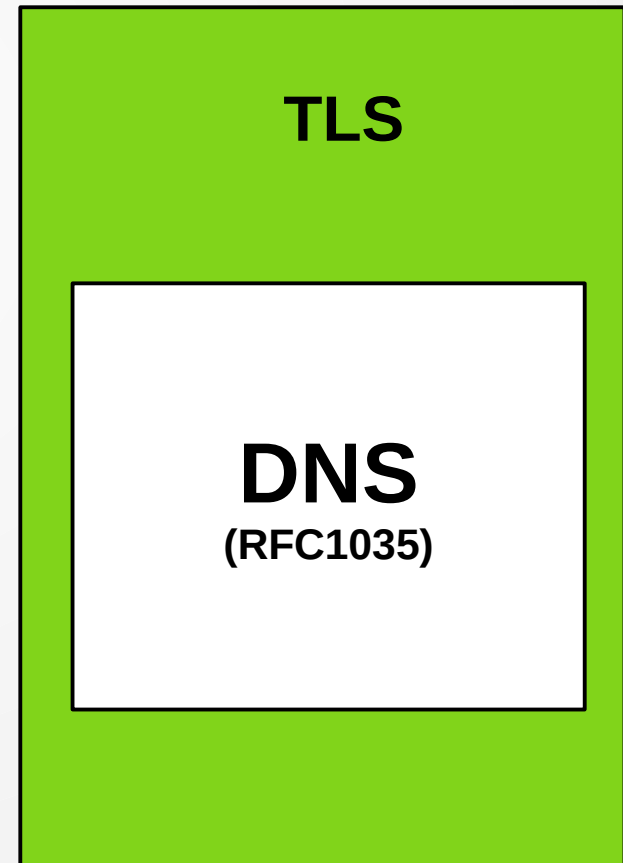
RFC8310 (März 2018)



Foundation for
Applied Privacy

DoT

- $\geq$ TLS 1.2
- TCP Port 853
- inoffiziell auch beliebt:
Port 443



DoT Profile

- Opportunistisch



Foundation for
Applied Privacy

DoT Profile

- Opportunistisch
- Strikt
 - SPKI Pins
 - PKIX
 - DANE/TLSA



DoT Implementierungen (Client)

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



DoT Unbound (Client)



Foundation for
Applied Privacy

DoT Unbound (Client)



Foundation for
Applied Privacy

Android 9 "Automatisch" (default)

Privates DNS

☐ Aus

☒ Automatisch

☐ Hostname des Anbieters des privaten DNS

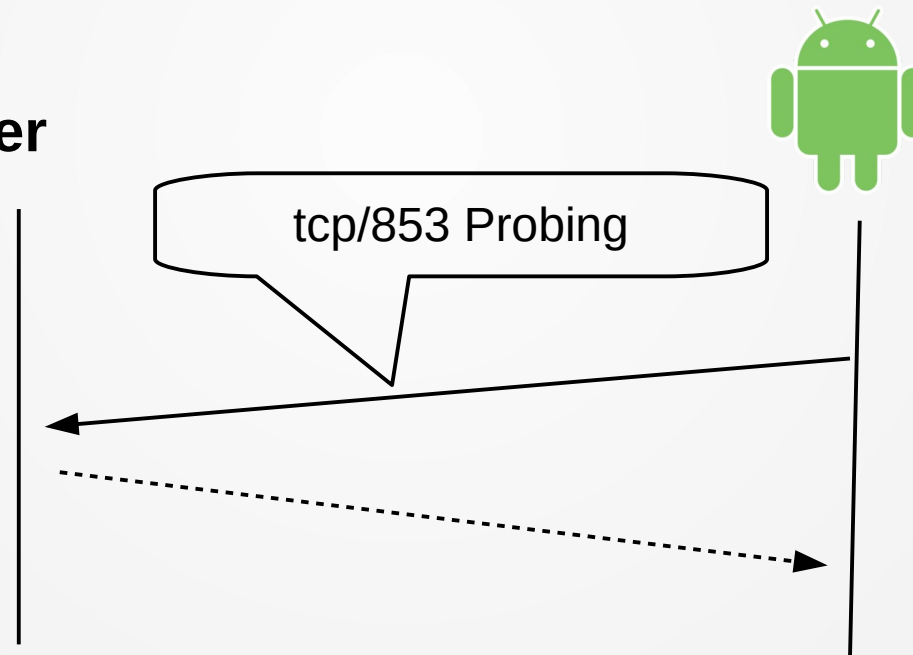
dot1.appliedprivacy.net

Abbrechen | **Speichern**



Android 9 “Automatisch” (default)

**DNS
Resolver**



Foundation for
Applied Privacy

Android 9 strikt Mode

Privates DNS

☐ Aus

☐ Automatisch

☒ Hostname des Anbieters des privaten DNS

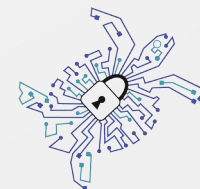
dot1.appliedprivacy.net

Abbrechen | Speichern



DoT Client Stubby

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



DoT Implementierungen (Server)

- Knot-Resolver (Padding)
- Unbound
- dnsmist
- BIND mit stunnel (Padding)



DNS-over-HTTPS (DoH)

RFC8484 (Okt 2018)



Foundation for
Applied Privacy

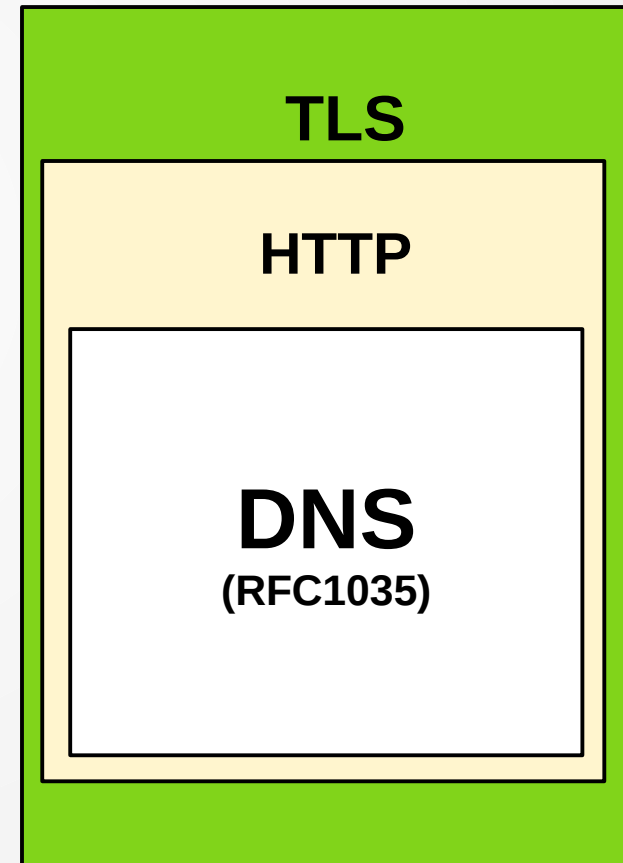
DoH - Motivation

- DNS gegen Middleboxen wappnen
- DNS Anfragen von Web Applikationen
- Proxy kompatibel
- Vor allem von Browser getrieben



DoH

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



DoH Client Software

- Firefox
- Bromite (Android)
- Chrome (noch keine UI)
- dnscrypt-proxy (kann auch DoH)
 - DNSCloak (iOS)
 - Simple DNSCrypt (Windows)
- curl, ...



DoH mit Firefox nutzen

☐ Automatic proxy configuration URL

Reload

No proxy for

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

☐ Do not prompt for authentication if password is saved

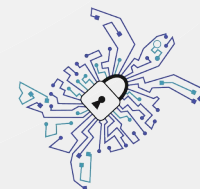
☐ Proxy DNS when using SOCKS v5

☒ Enable DNS over HTTPS

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

☒ Custom

Help Cancel OK



DoH in Firefox

start [Easterhegg 2019] x Easterhegg 2019 :: pretal x About Networking x +

← → ↻ 🏠 ⓘ about:networking#dns

DNS

HTTP

Sockets

DNS

WebSockets

Hostname	Family	TRR	Addresses
ocsp.digicert.com	ipv4	true	93.184.220.29
ocsp.digicert.com	ipv4	true	93.184.220.29
appliedprivacy.net	ipv4	true	2a00:63c1:a:182::2 37.252.185.182
eh19.easterhegg.eu	ipv4	true	78.41.115.160 2a02:60:4:6165:2342:c0ff:eec0:ffee



DoH -Firefox Modi

network.trr.mode:

2: “TRR first” - Fallback auf Klartext

3: “TRR only” - kein Fallback

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



Foundation for
Applied Privacy

DoH Server Discovery in Chrome (angekündigt)

- Automatisches Upgrade zu DoH sofern unterstützt
- Statische Liste im Browser (Resolver IP -> DoH URI)



DoH Server Software

- Knot-Resolver 4.0.0
- Experimentell: doh-http-proxy, ...



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
```



DoH Kritik: HTTP Metadaten

```

▶ Header: :method: POST
▶ Header: :path: /query
▶ Header: :authority: deb-appliedprivacy.net

```



Datatracker

Groups

Documents

Meetings

Other

User

66.0

DoHPE: DoH with Privacy Enhancements

draft-dickinson-doh-dohpe-00



Foundation for
Applied Privacy

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



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>



Foundation for
Applied Privacy

DoH / ISP Kritik



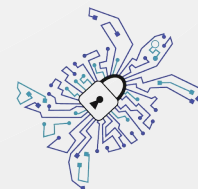
Foundation for
Applied Privacy

DoH / ISP Kritik

DOH
Internet-Draft
Intended status: Informational
Expires: September 9, 2019

M. Antonakakis
Georgia Institute of Technology
J. Livingood
Comcast
B. Sleight
BT Plc
A. Winfield
Sky
March 8, 2019

Centralized DNS over HTTPS (DoH) Implementation Issues and Risks
draft-livingood-doh-implementation-risks-issues-00



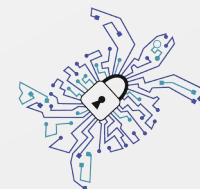
Foundation for
Applied Privacy

DoH / ISP Kritik

DoH
Internet-Draft
Intended status: Informational
Expires: September 11, 2019

A. Fidler
BT plc
B. Hubert
OpenXchange
J. Livingood
Comcast
J. Reid
RTFM llp
N. Leymann
Deutsche Telekom AG
March 10, 2019

DNS over HTTPS (DoH) Considerations for Operator Networks
draft-reid-doh-operator-00



Foundation for
Applied Privacy

DoH / ISP Kritik

This will have two unwelcome results. First, threat intelligence and reputation services will have fewer data to analyse and therefore have a significantly less complete perspective of end users' DNS behaviour. Second, the quality and effectiveness of the data provided by threat intelligence and reputation services will be



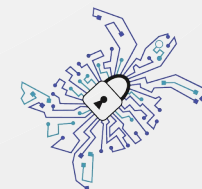
DoT vs. DoH

	DoT	DoH
Zensurresistenter	-	+
mit ESNi in Firefox kompatibel	-	+
wenig Metadaten für den Resolver	+	-
Server Software Verfügbarkeit	+	~
Easy Setup (Client)	~	+



DoT vs. DoH

	DoT	DoH
Zensurresistenter	-	+
mit ESNi in Firefox kompatibel	-	+
wenig Metadaten für den Resolver	+	-
Server Software Verfügbarkeit	+	~
Easy Setup (Client)	~	+



Foundation for
Applied Privacy

DoH / DoT – DNSSEC?

- Löst unterschiedliche Problem
- Am besten in Kombination eingesetzt



DNS Privacy - Zukunft

- DoH/DoT Server Discovery Protokolle
- Verschlüsselung zu authoritative Server
- DNS over QUIC



I E T F[®]



Foundation for
Applied Privacy

Fazit

- Verschlüsselt euren DNS Traffic!
- Auch mit DoH/DoT sind Metadaten (zB Hostname) sichtbar (ESNI erforderlich!)
- DoH: pot. schnelle Verbreitung durch Firefox



Fazit

DoT und DoH haben die selben Kernziele

ITS KINDA THE SAME



BUT DIFFERENT

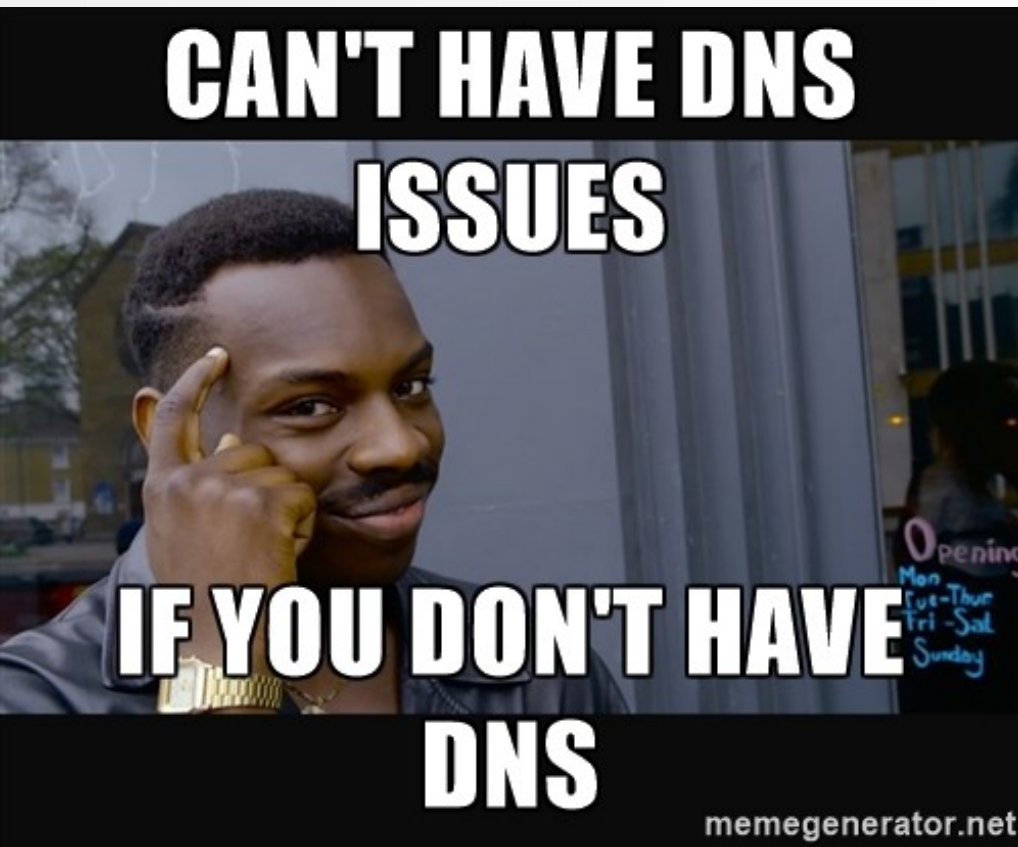
makeameme.org



Foundation for
Applied Privacy

Fazit

Verwende (weiterhin) **Torbrowser** für die stärksten Privacyeigenschaften



Foundation for
Applied Privacy

Unsere DNS Privacy Resolver

<https://doh.appliedprivacy.net/query>

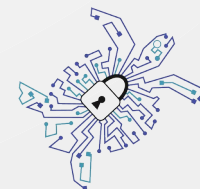
dot1.appliedprivacy.net

dot2.appliedprivacy.net

Kein Logging der IP Adresse / Query

QNAME Minimzation, DNSSEC

gdb6r6pm66tzpavenstxove4ftwil52onqmhwiob7dffojc6h56saoqd.onion



Foundation for
Applied Privacy

Fragen?

contact@appliedprivacy.net

[@applied_privacy](https://mastodon.social/@applied_privacy)

https://mastodon.social/@applied_privacy

<https://appliedprivacy.net>



Foundation for
Applied Privacy