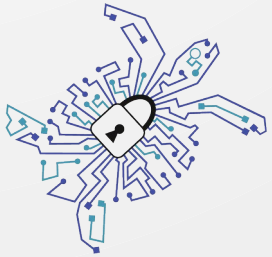
DoH, DoT, what?

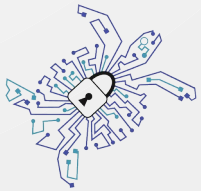
Eine Einführung in die DNS Privacy Protokolle DoH und DoT.



Foundation for Applied Privacy

Foundation for Applied Privacy

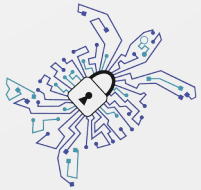
- Non-profit Privacy Infrastruktur Provider
- PETS Dienste für die Öffentlichkeit
- 2018 gegründet
- Top 3 Tor Exit Relay Operator (weltweit)
- > 2000 Terabyte monatlicher Netzwerkverkehr



Foundation for
Applied Privacy

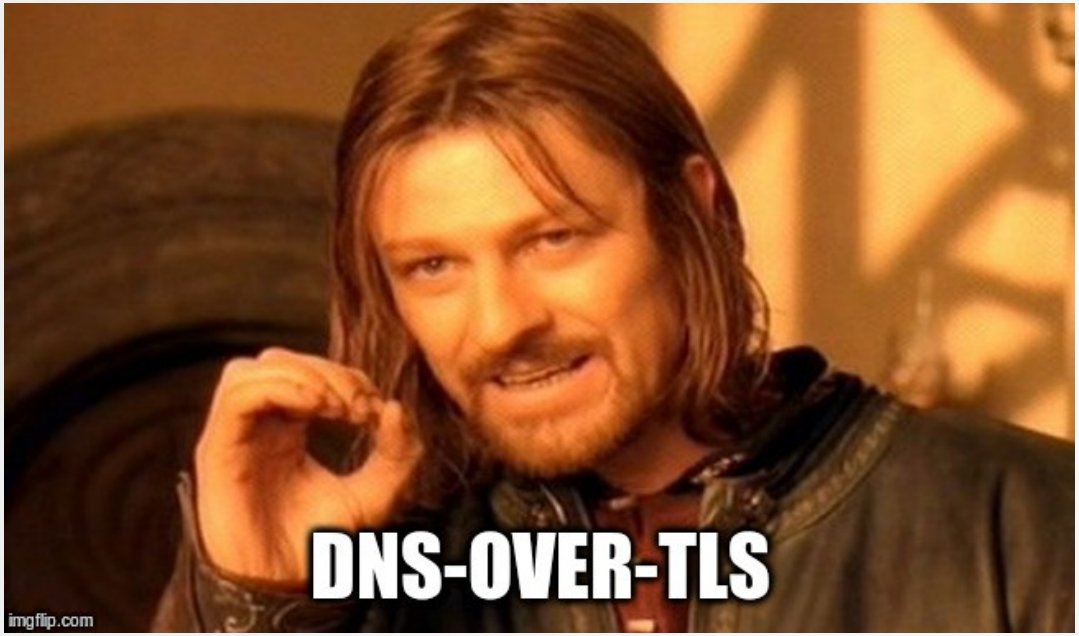
Ziele dieses Vortrags

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



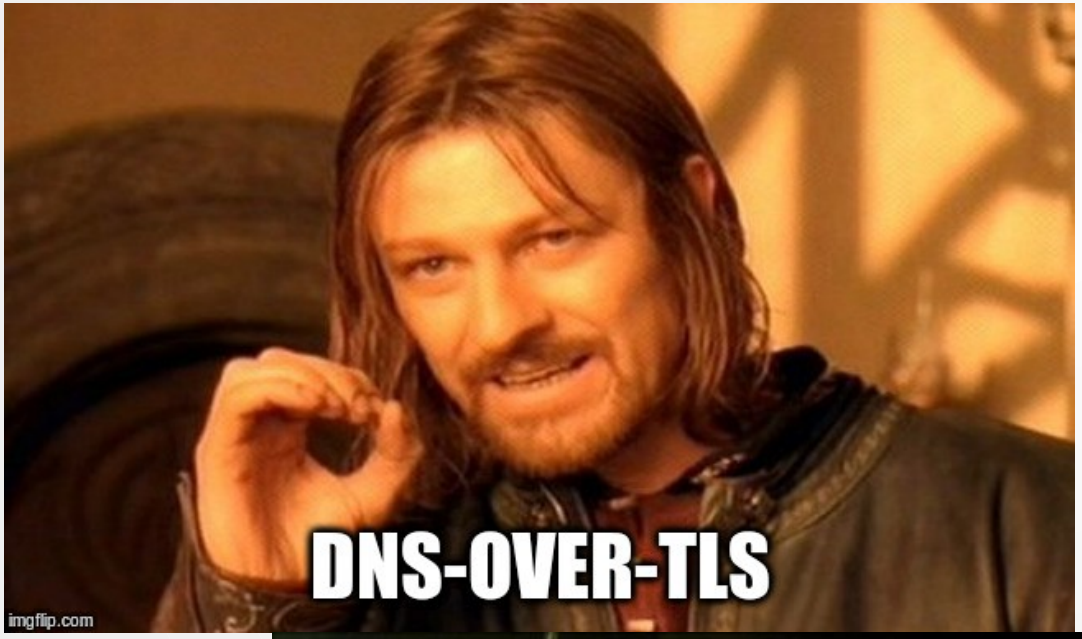
Foundation for
Applied Privacy

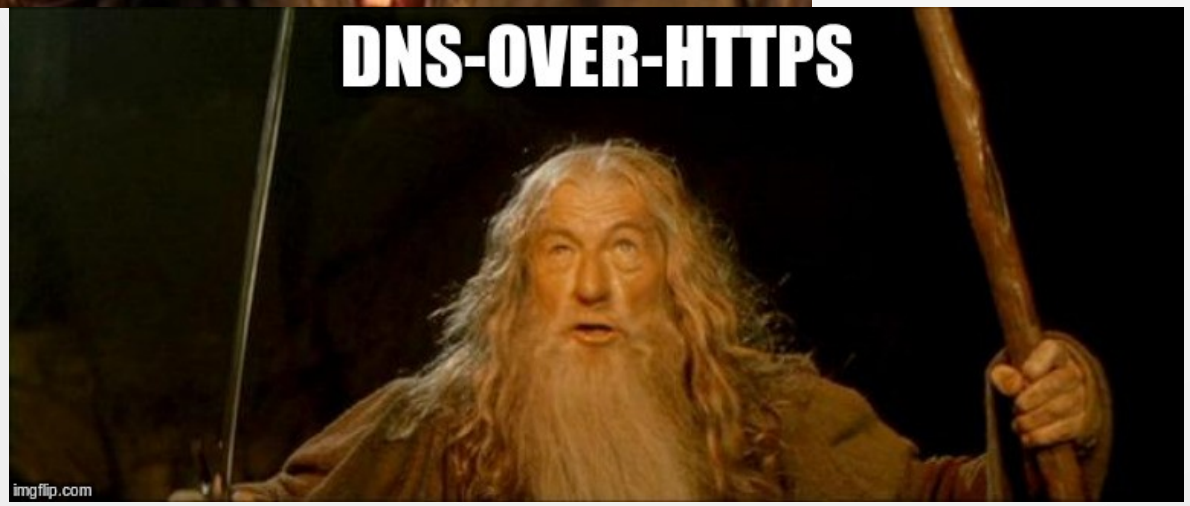
Ziele dieses Vortrags



Foundation for Applied Privacy

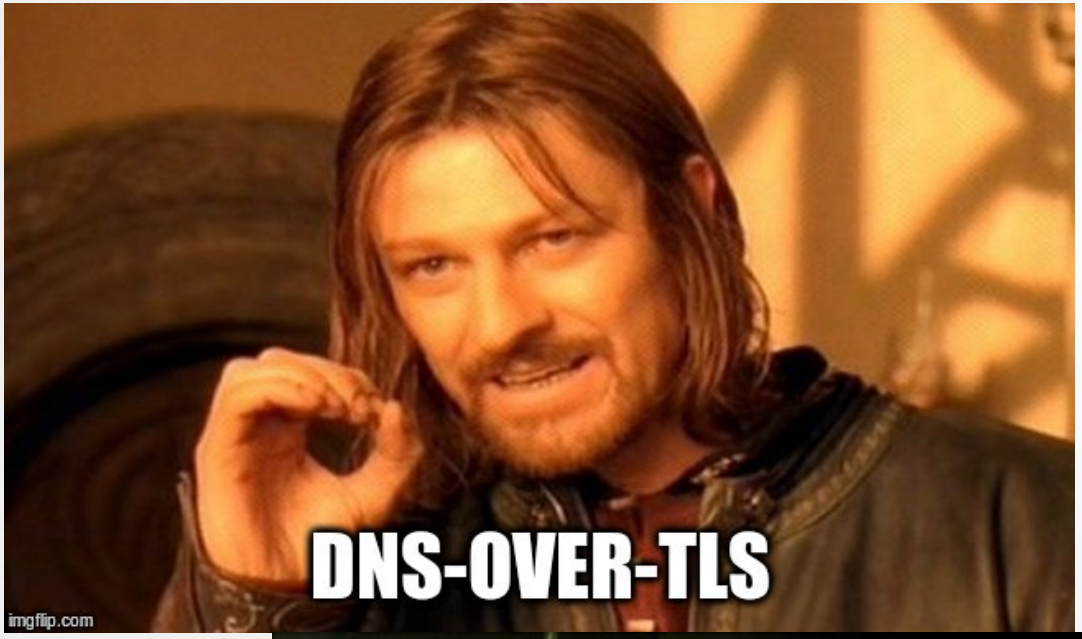
Ziele dieses Vortrags

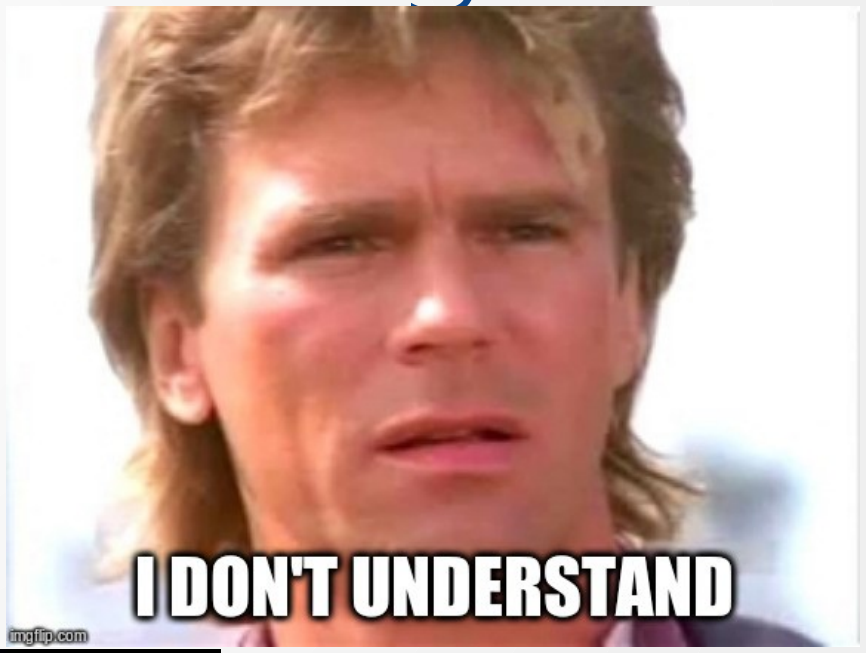


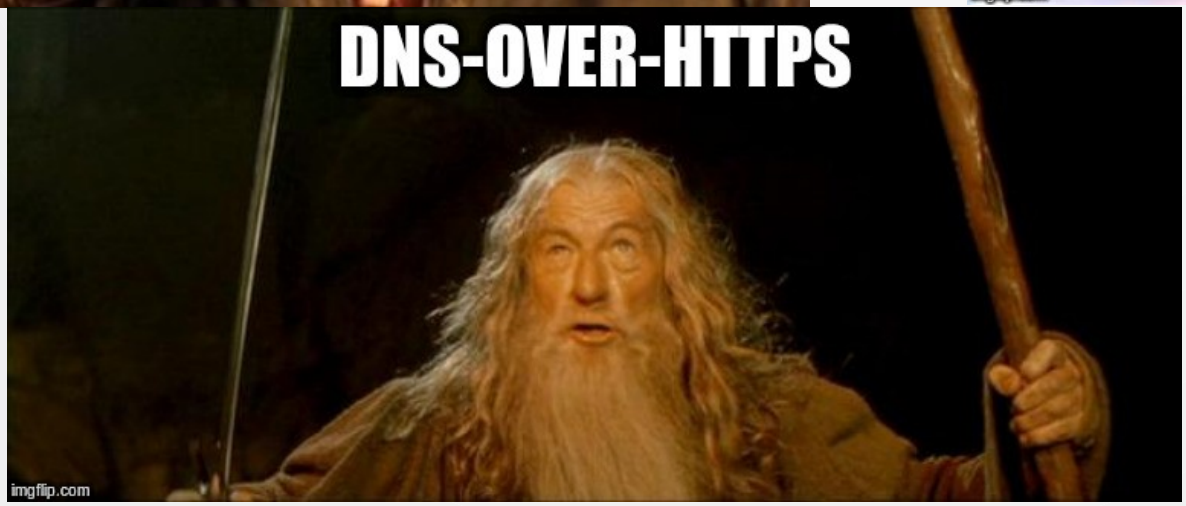


Foundation for Applied Privacy

Ziele dieses Vortrags

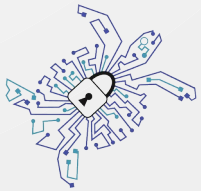






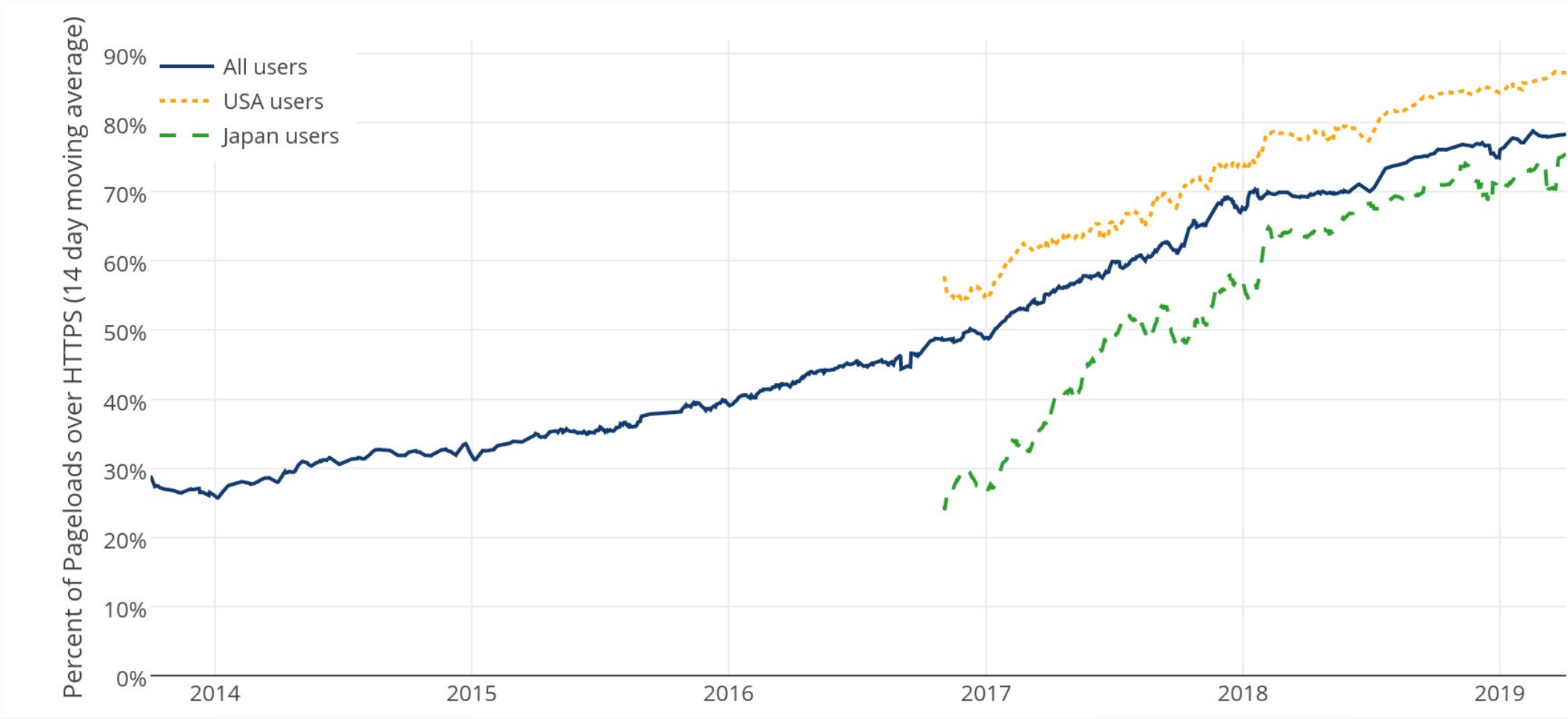
Foundation for Applied Privacy

Warum DNS Privacy?



Foundation for
Applied Privacy

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

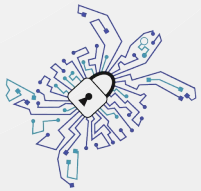


Foundation for Applied Privacy

Foundation for
Applied Privacy

Ziel

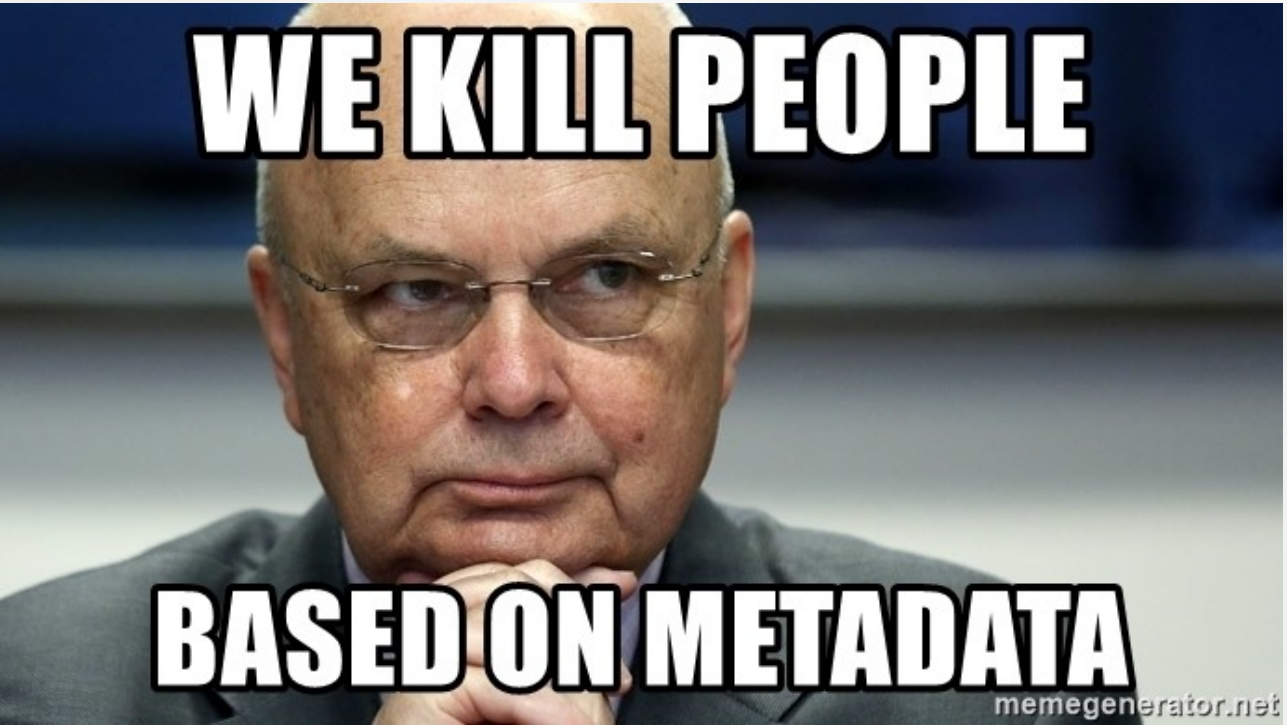
Schutz von Metadaten (Hostname)



Foundation for Applied Privacy

Warum ist das wichtig?

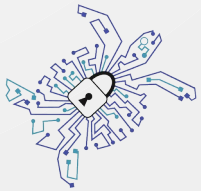
- Ermöglicht privateres browsen
- Erschwert Zensur
- Erschwert Massenüberwachung



Foundation for Applied Privacy

Warum ist das aktuell noch nicht möglich?

(ohne Torbrowser)



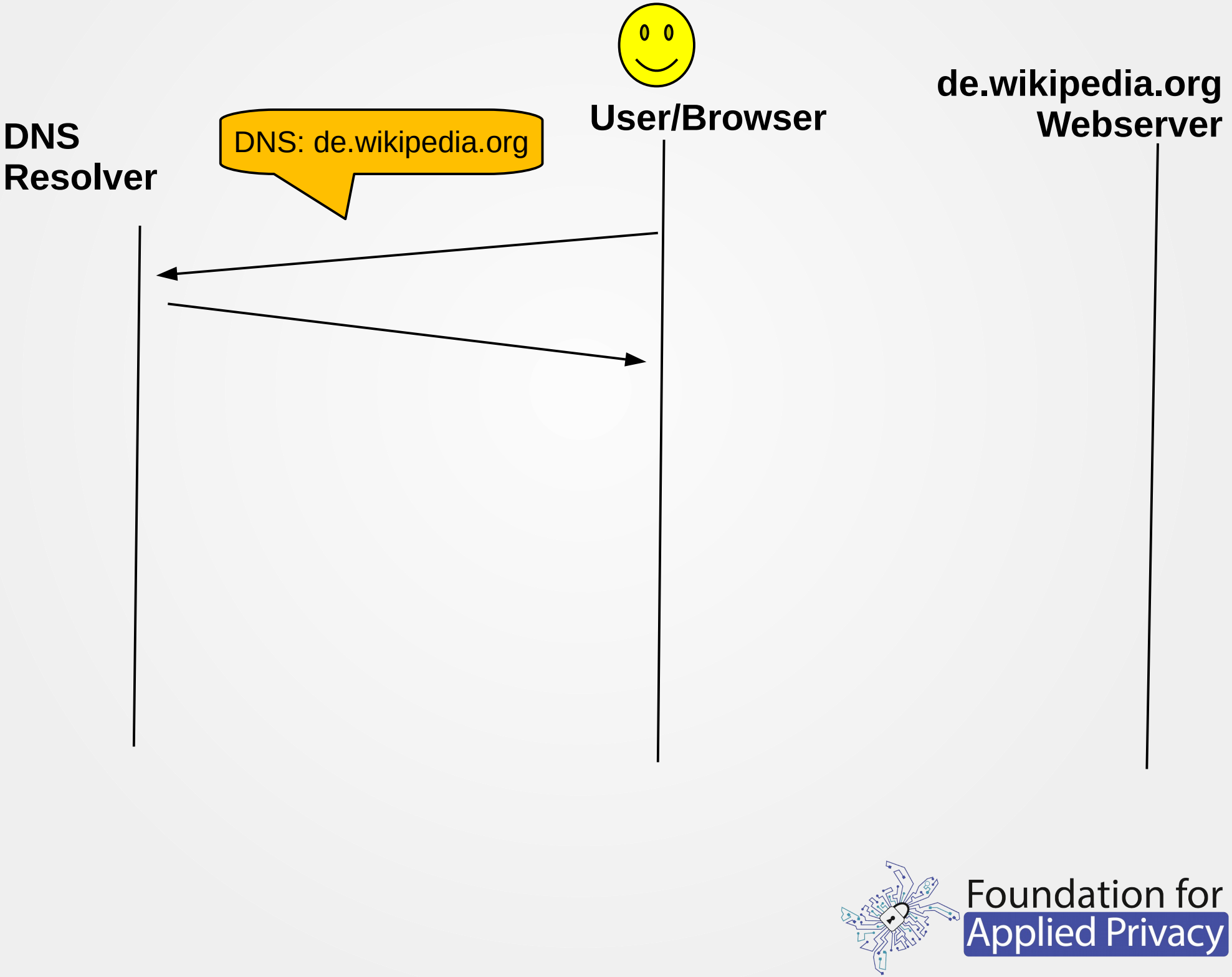
Foundation for Applied Privacy

User/Browser

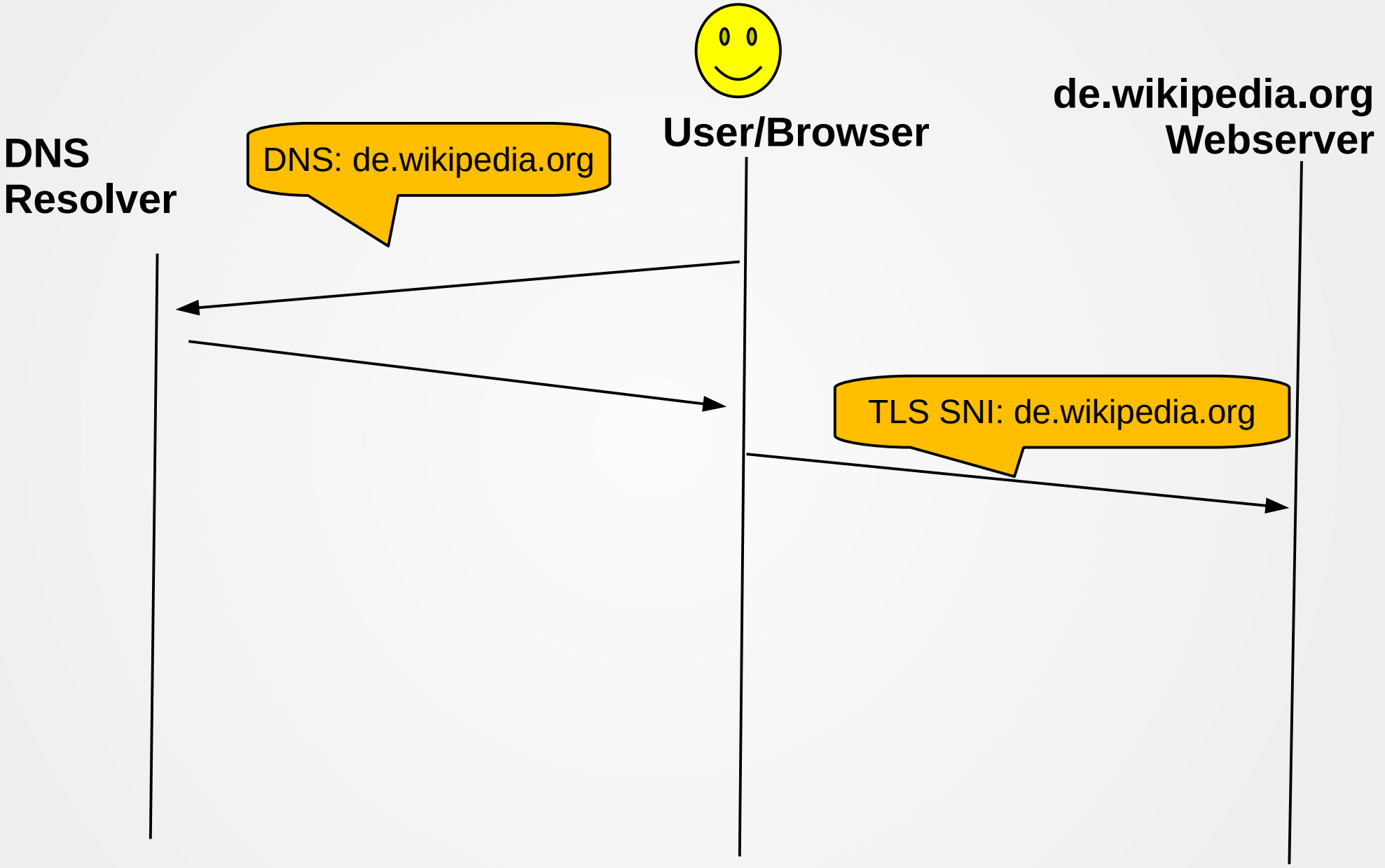
de.wikipedia.org
Webserver

DNS
Resolver

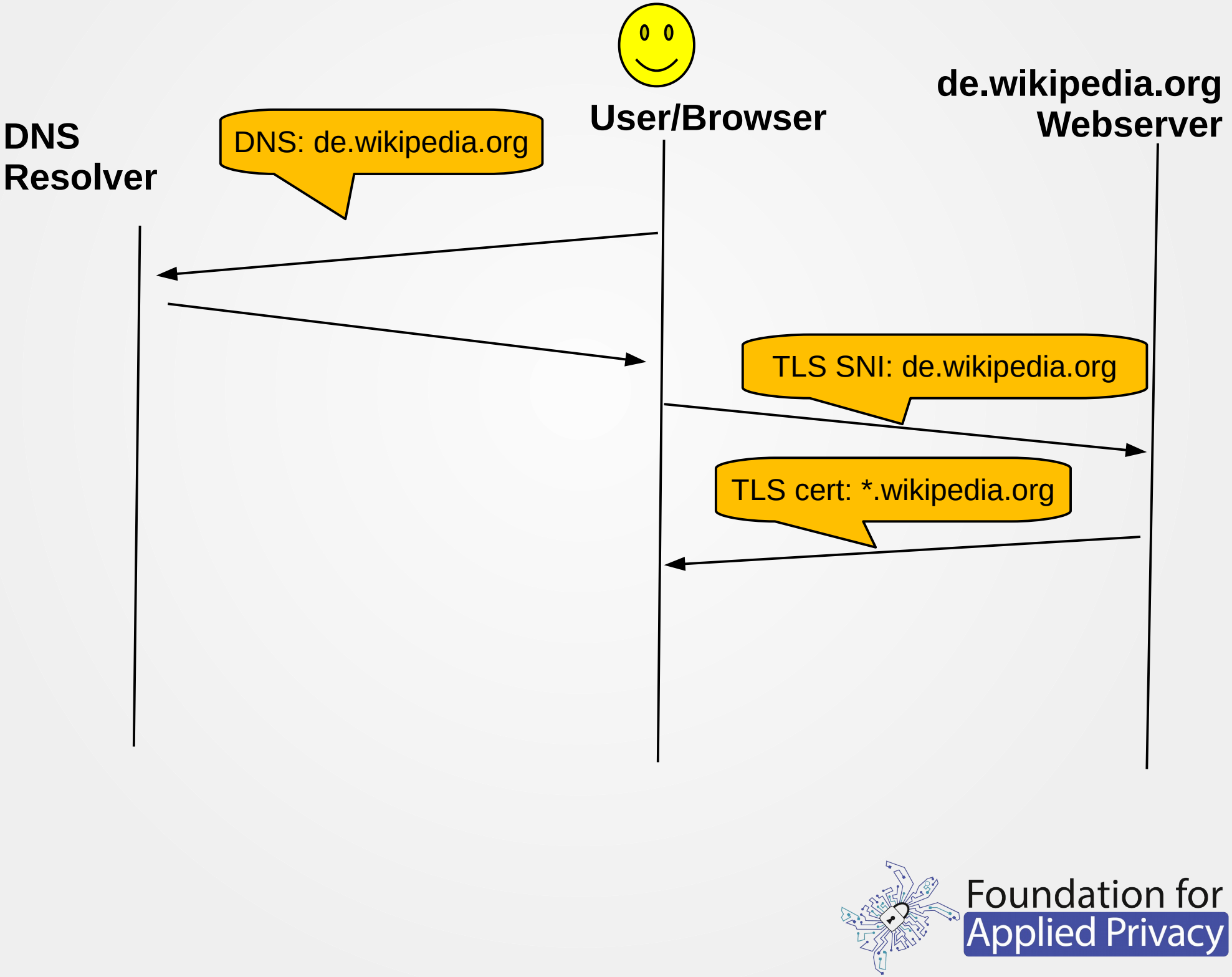
Foundation for
Applied Privacy



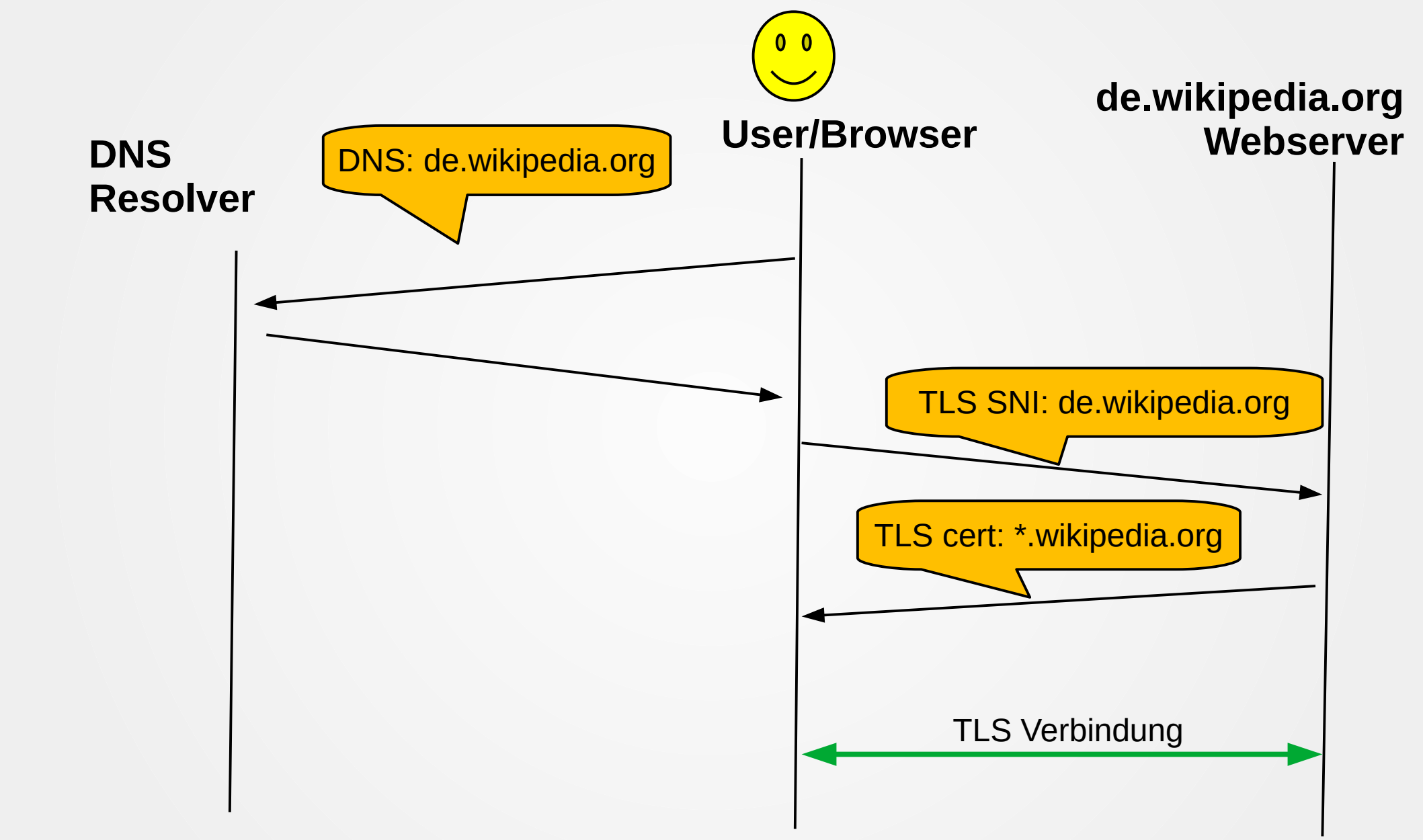
Foundation for Applied Privacy



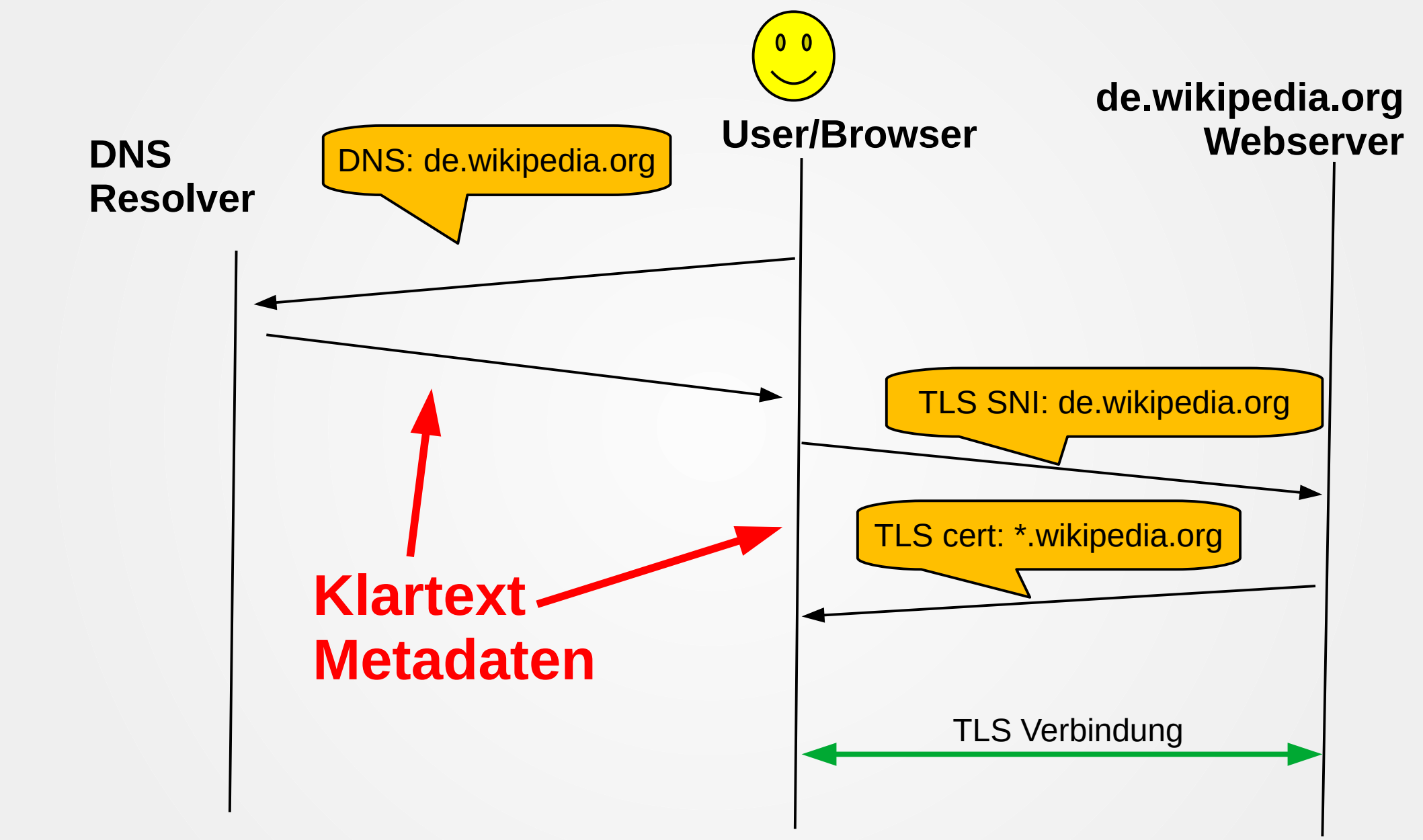
Foundation for Applied Privacy



Foundation for Applied Privacy

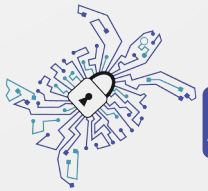


Foundation for Applied Privacy



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

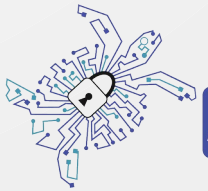


Foundation for Applied Privacy

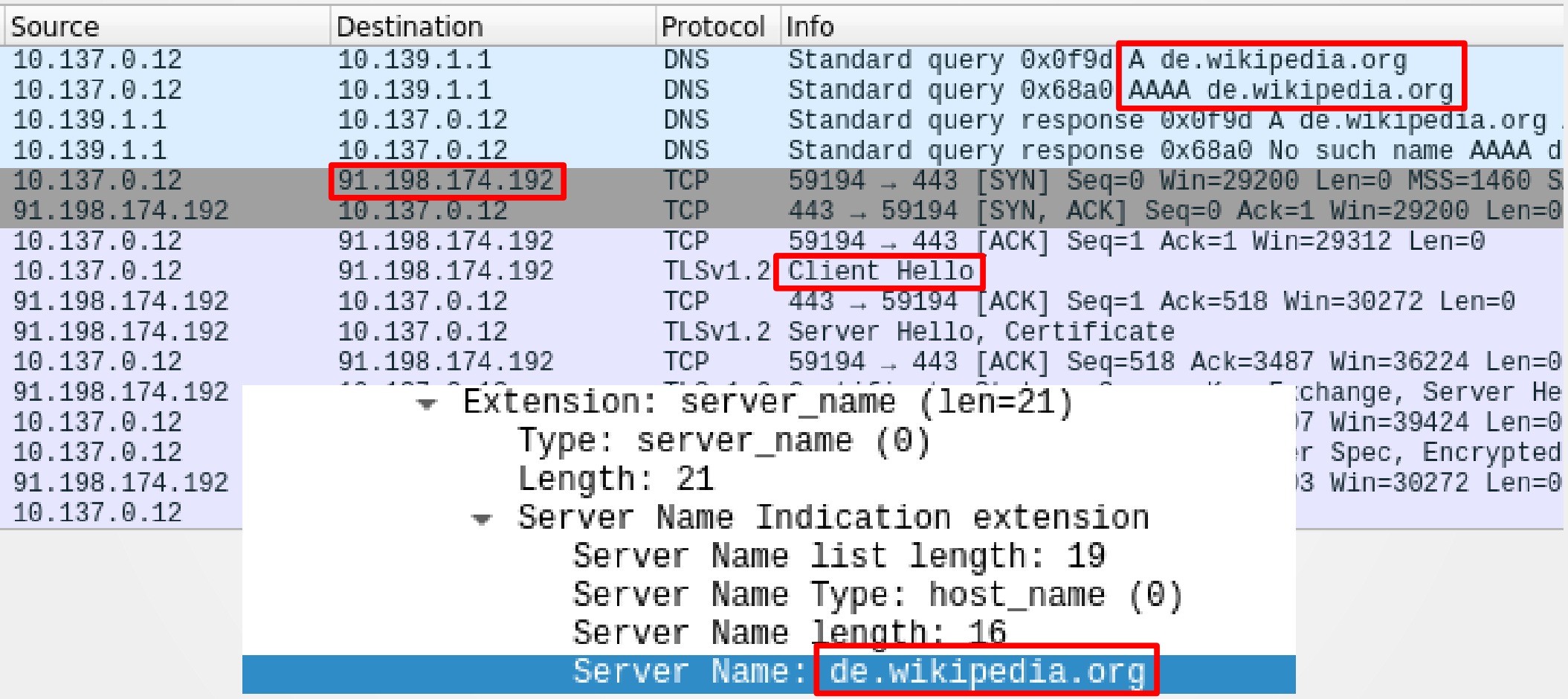
Source	Destination	Protocol	Info
10.137.0.12	10.139.1.1	DNS	Standard query 0x0f9d A de.wikipedia.org
10.137.0.12	10.139.1.1	DNS	Standard query 0x68a0 AAAA de.wikipedia.org
10.139.1.1	10.137.0.12	DNS	Standard query response 0x0f9d A de.wikipedia.org
10.139.1.1	10.137.0.12	DNS	Standard query response 0x68a0 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

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



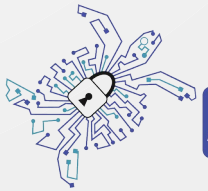
Foundation for
Applied Privacy



Foundation for Applied Privacy

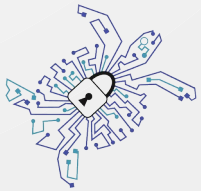
Source	Destination	Protocol	Info
10.137.0.12	10.139.1.1	DNS	Standard query 0x0f9d A de.wikipedia.org
10.137.0.12	10.139.1.1	DNS	Standard query 0x68a0 AAAA de.wikipedia.org
10.139.1.1	10.137.0.12	DNS	Standard query response 0x0f9d A de.wikipedia.org
10.139.1.1	10.137.0.12	DNS	Standard query response 0x68a0 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

```
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,
      ▸ signedCertificate
      ▸ algorithmIdentifier (sha256WithRSAEncryption)
        Padding: 0
```



Foundation for Applied Privacy

Problem/Leak	Lösung	Aufwand für Webseitbetreiber

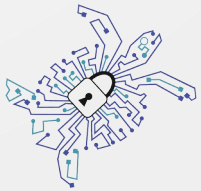


Foundation for Applied Privacy

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

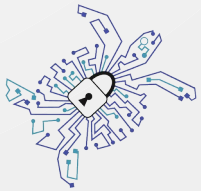
Foundation for Applied Privacy

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



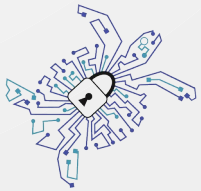
Foundation for Applied Privacy

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



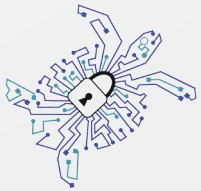
Foundation for Applied Privacy

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)



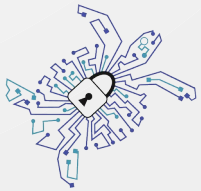
Foundation for Applied Privacy

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)

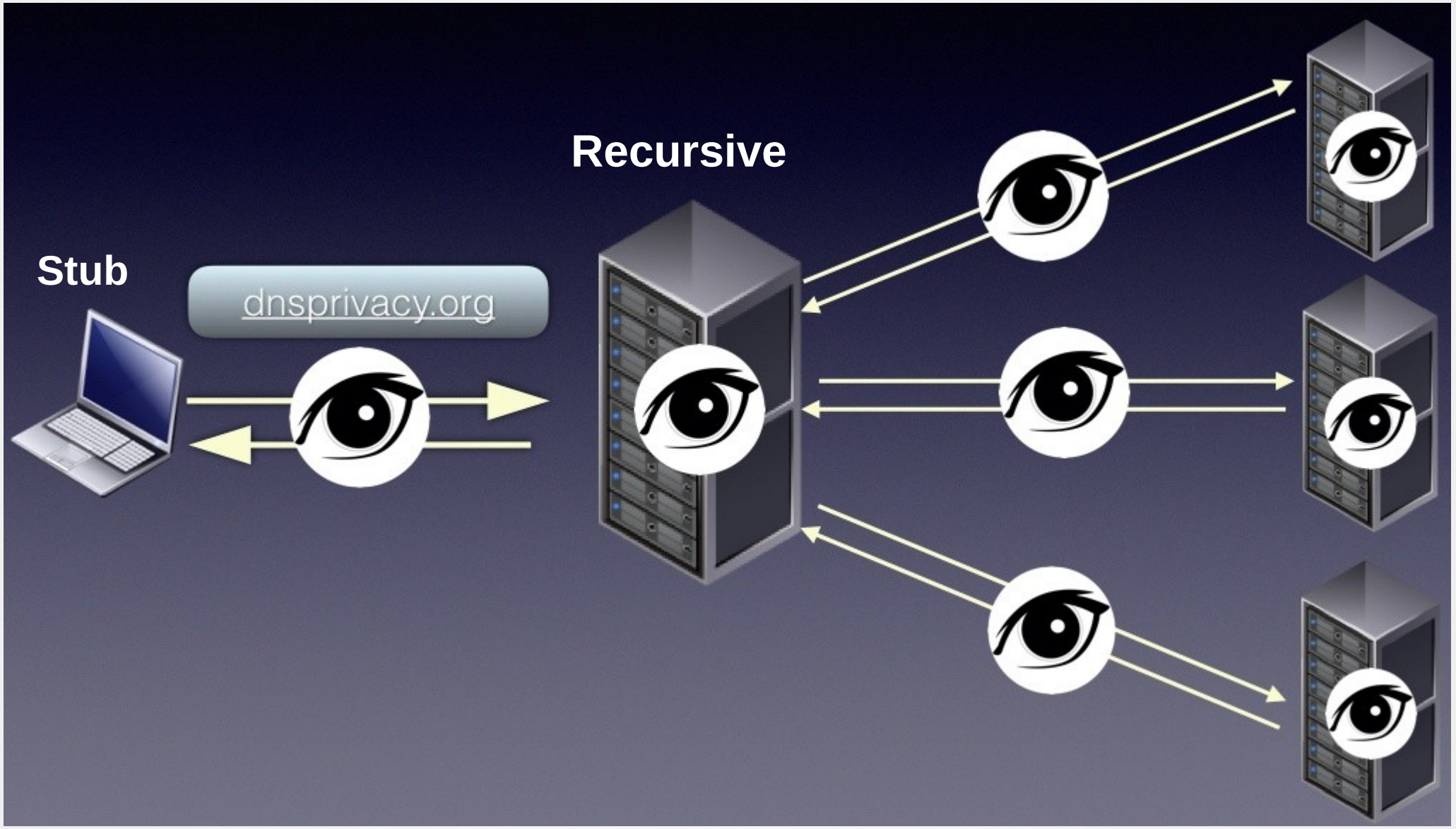


Foundation for Applied Privacy

DNS

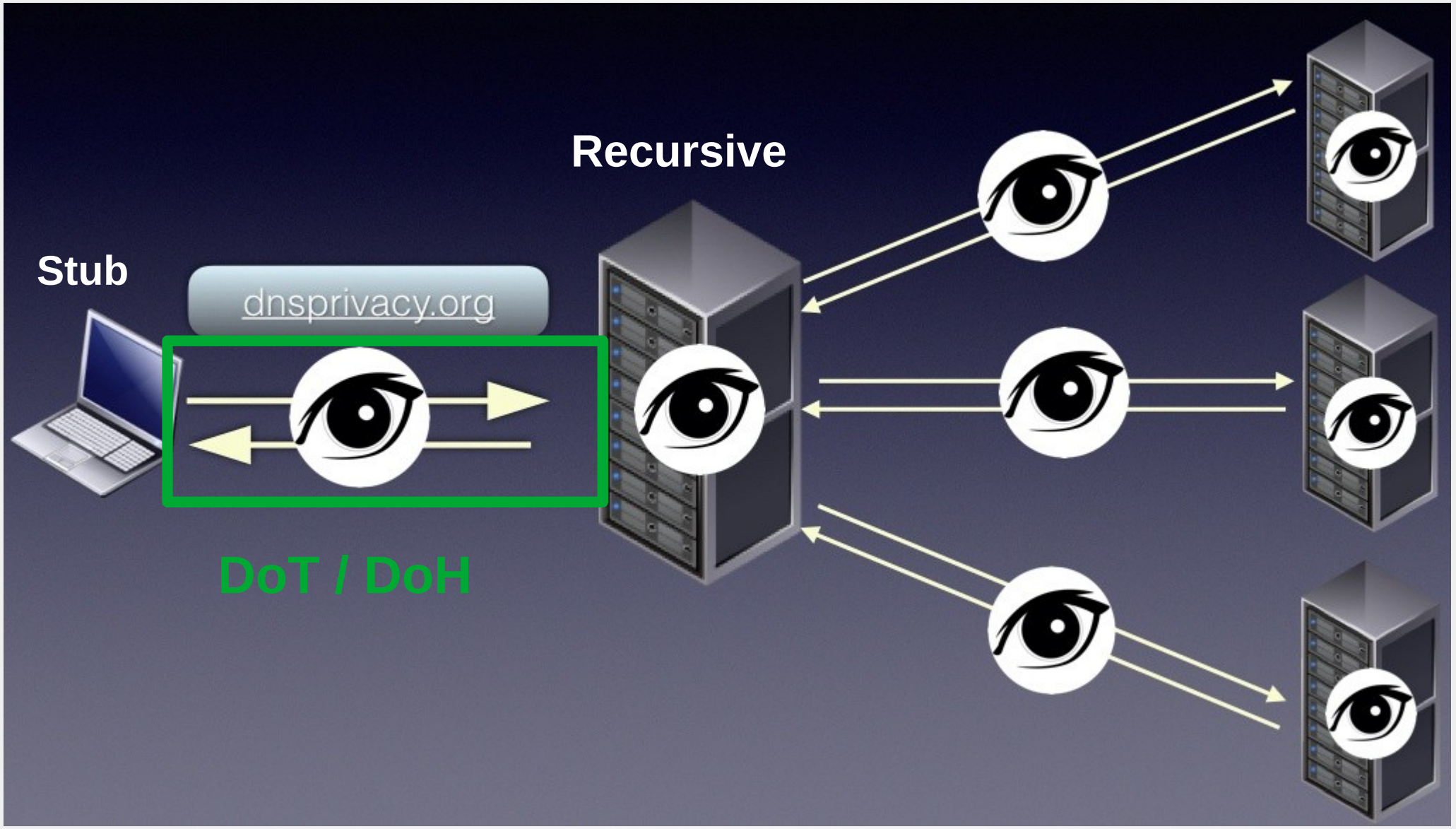


Foundation for
Applied Privacy



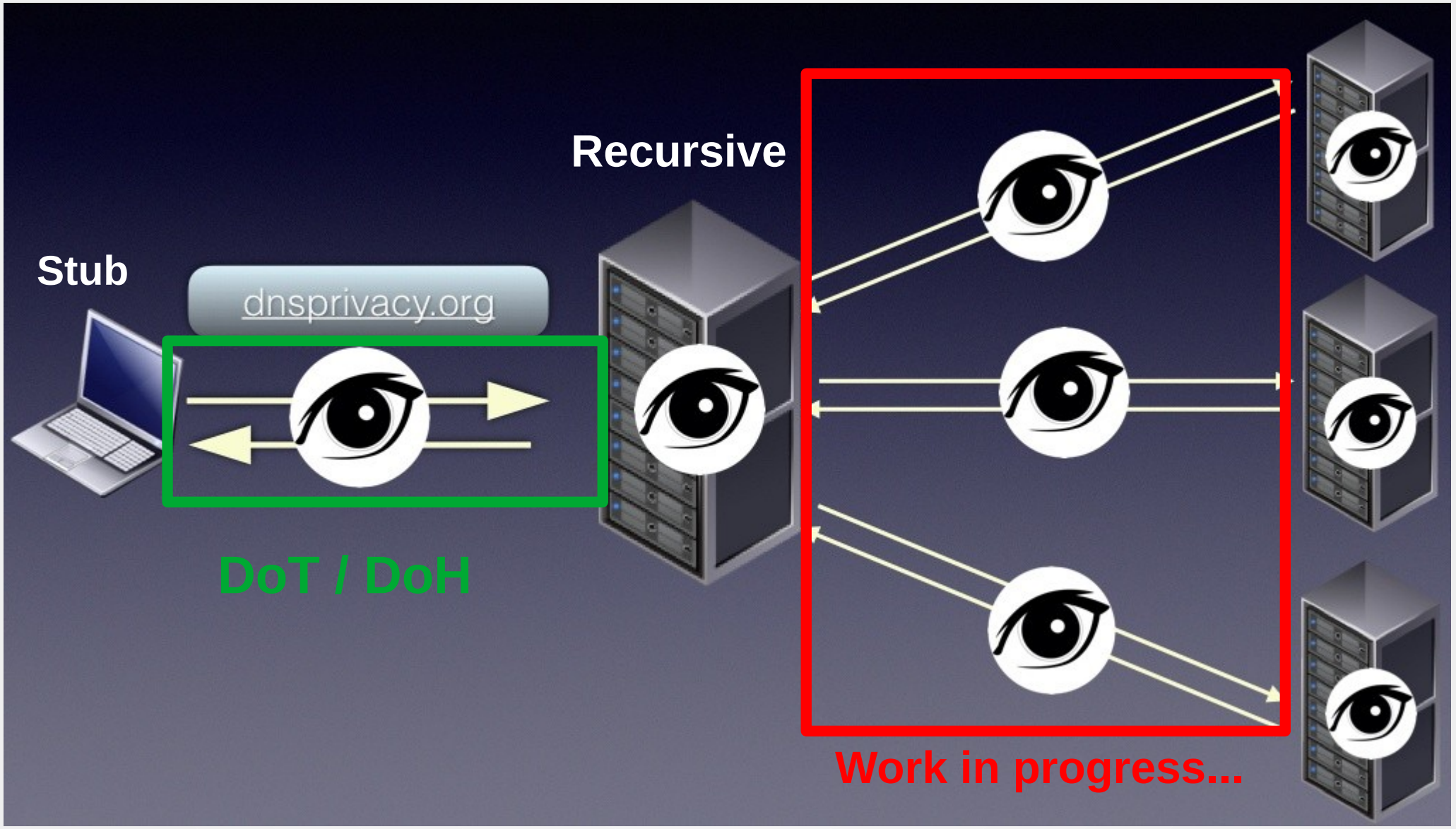
Quelle: dnsprivacy.org

Foundation for Applied Privacy



Quelle: dnsprivacy.org

Foundation for Applied Privacy

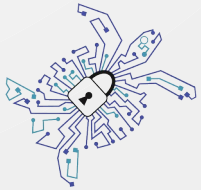


Quelle: dnsprivacy.org

Foundation for Applied Privacy

DNS-over-TLS (DoT)

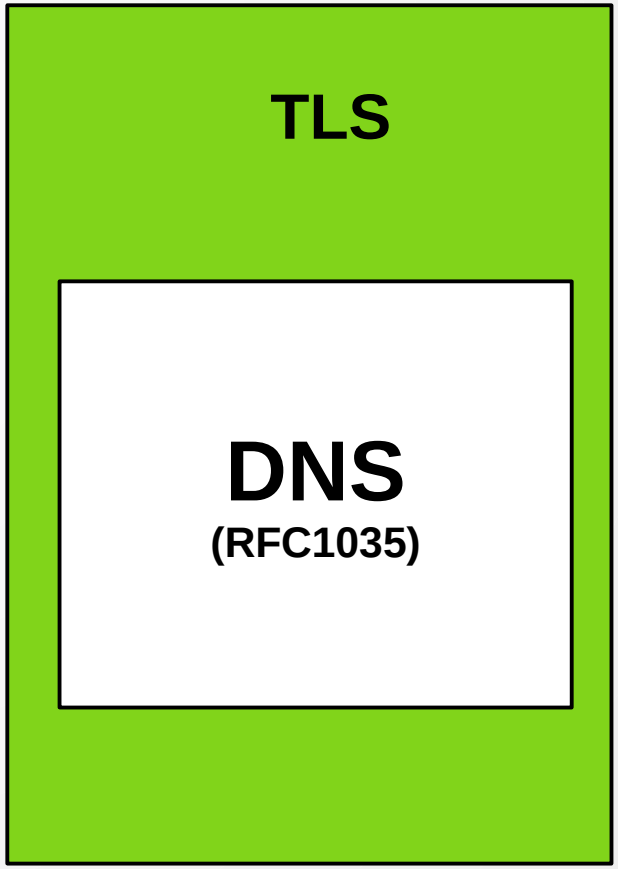
RFC7858 (Mai 2016)
RFC8310 (März 2018)



Foundation for
Applied Privacy

DoT

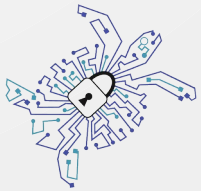
- >=TLS 1.2
- TCP Port 853
- inoffiziell auch beliebt: Port 443



Foundation for Applied Privacy

DoT Profile

- Opportunistisch

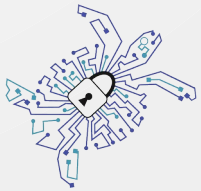


Foundation for
Applied Privacy

DoT Profile

- Opportunistisch

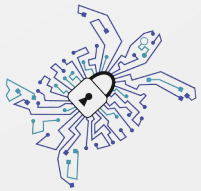
- Strikt
  - SPKI Pins
  - PKIX
  - DANE/TLSA



Foundation for
Applied Privacy

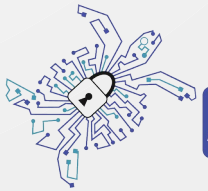
DoT Implementierungen (Client)

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



Foundation for Applied Privacy

DoT Unbound (Client)

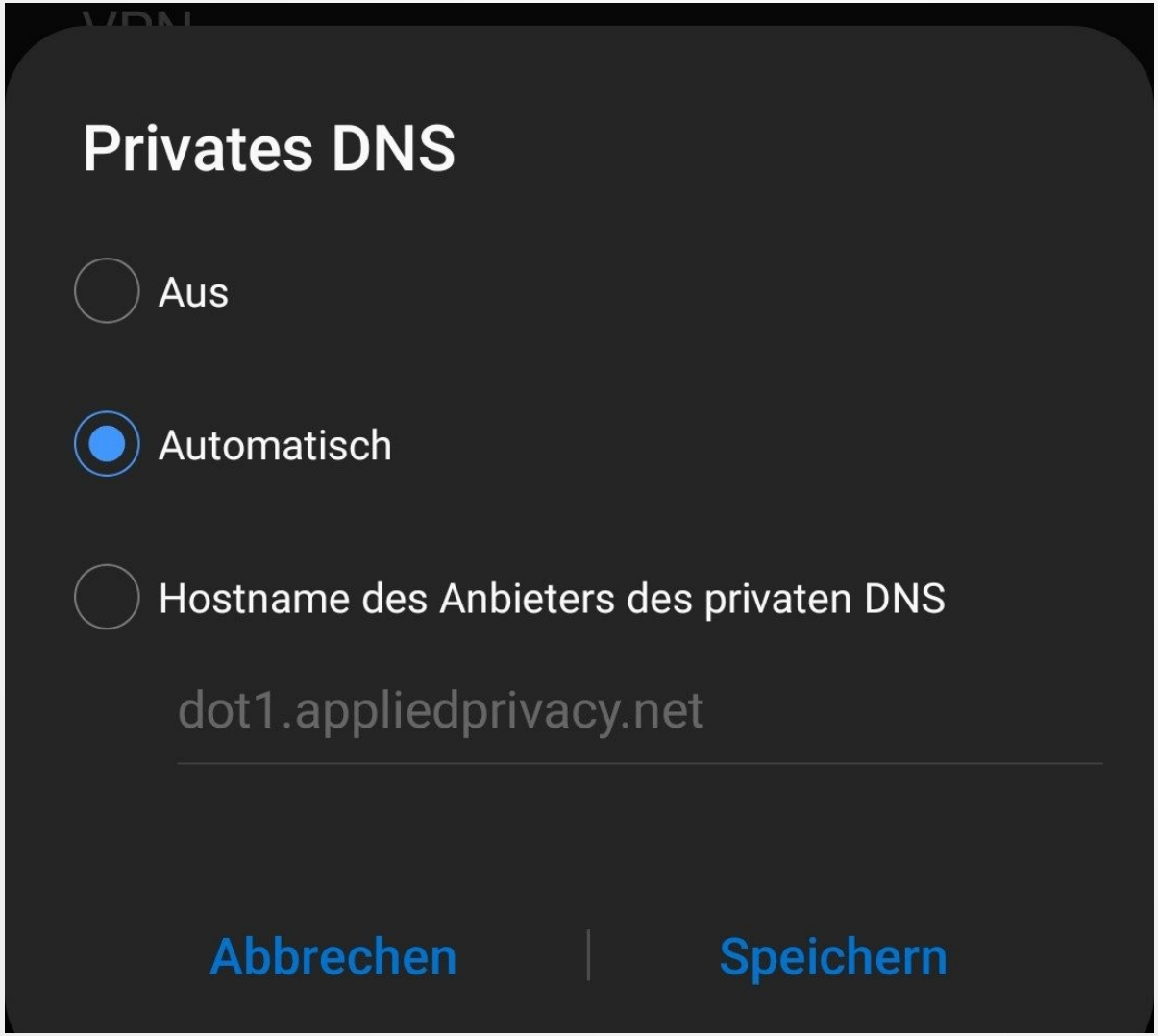


Foundation for
Applied Privacy

DoT Unbound (Client)

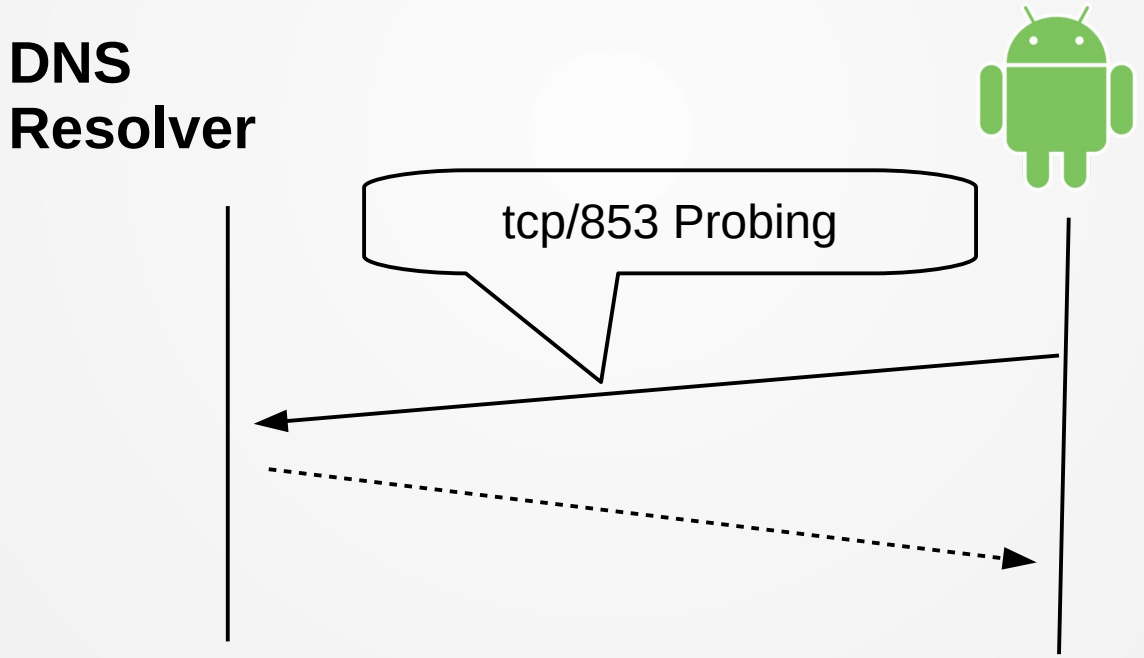
Foundation for Applied Privacy

Android 9 “Automatisch” (default)



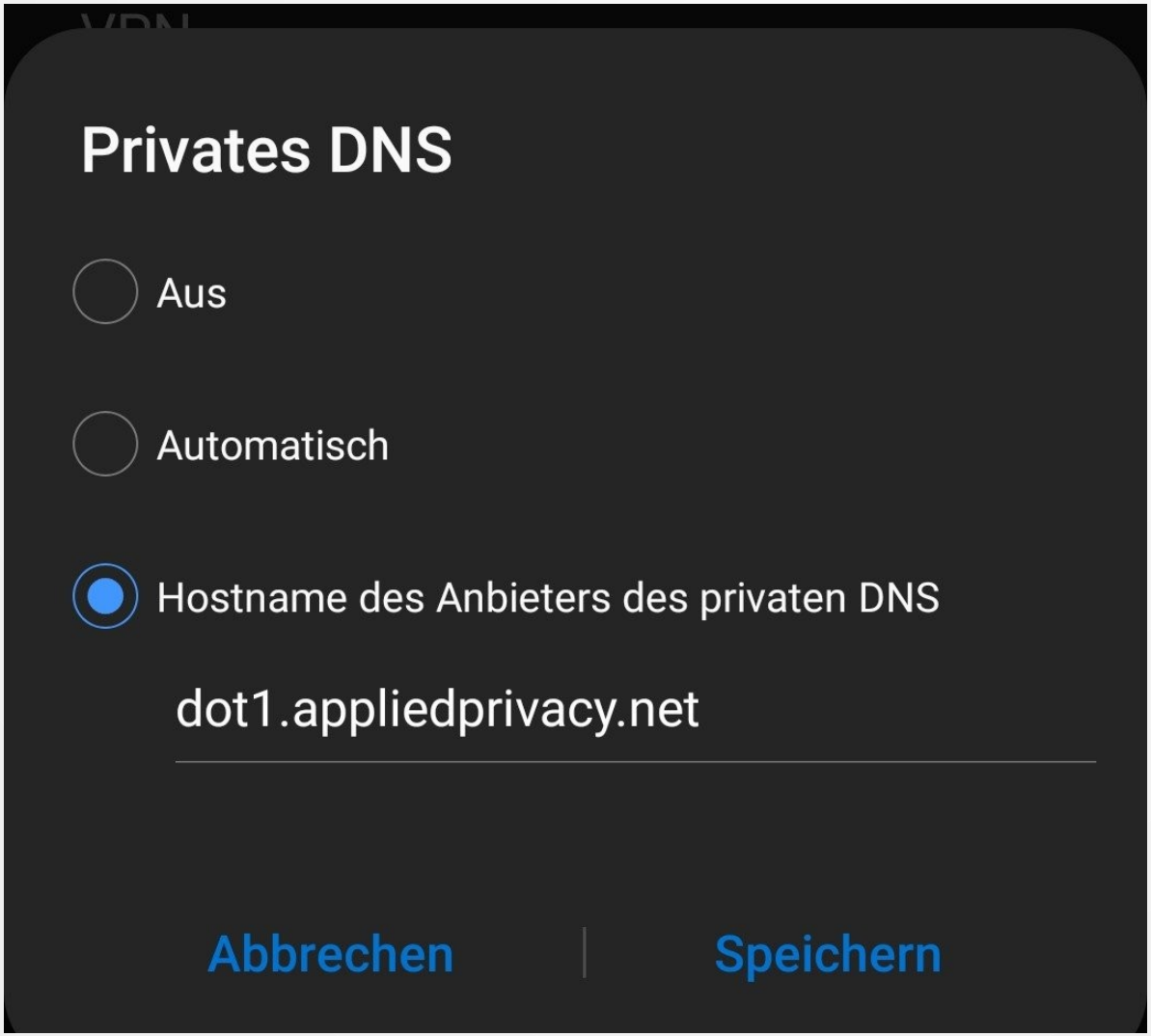
Foundation for Applied Privacy

Android 9 "Automatisch" (default)



Foundation for Applied Privacy

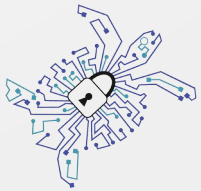
Android 9 strikt Mode



Foundation for Applied Privacy

DoT Client Stubby

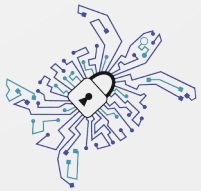
- **Opportunistisch oder strikt Mode**
- **TLS Connection Re-use**
- Pipelining, Out-of-Order Responses
- Explizites deaktivieren von EDNS Client Subnet
- DNS Padding, DNSSEC



Foundation for Applied Privacy

DoT Implementierungen (Server)

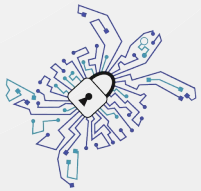
- Knot-Resolver (Padding)
- Unbound
- dnsdist
- BIND mit stunnel (Padding)



Foundation for Applied Privacy

DNS-over-HTTPS (DoH)

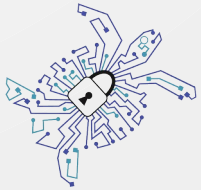
RFC8484 (Okt 2018)



Foundation for
Applied Privacy

DoH - Motivation

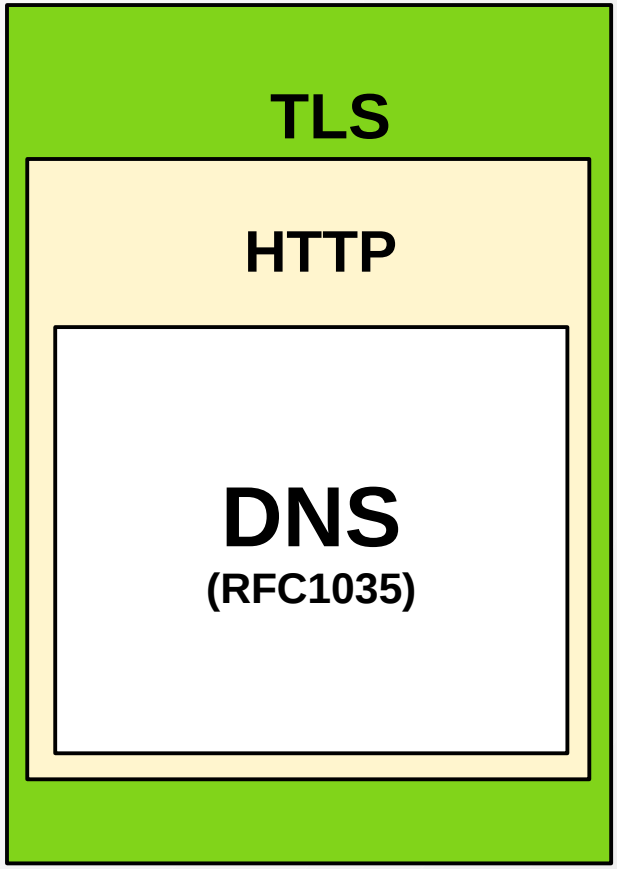
- DNS gegen Middleboxen wappnen
- DNS Anfragen von Web Applikationen
- Proxy kompatibel
- Vor allem von Browser getrieben



Foundation for
Applied Privacy

DoH

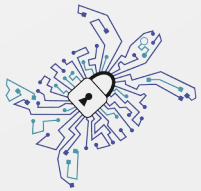
- HTTPS (443)
- **POST**
- oder GET (base64url)
- HTTP/2 (empfohlen)
- Content Type: application/dns-message



Foundation for Applied Privacy

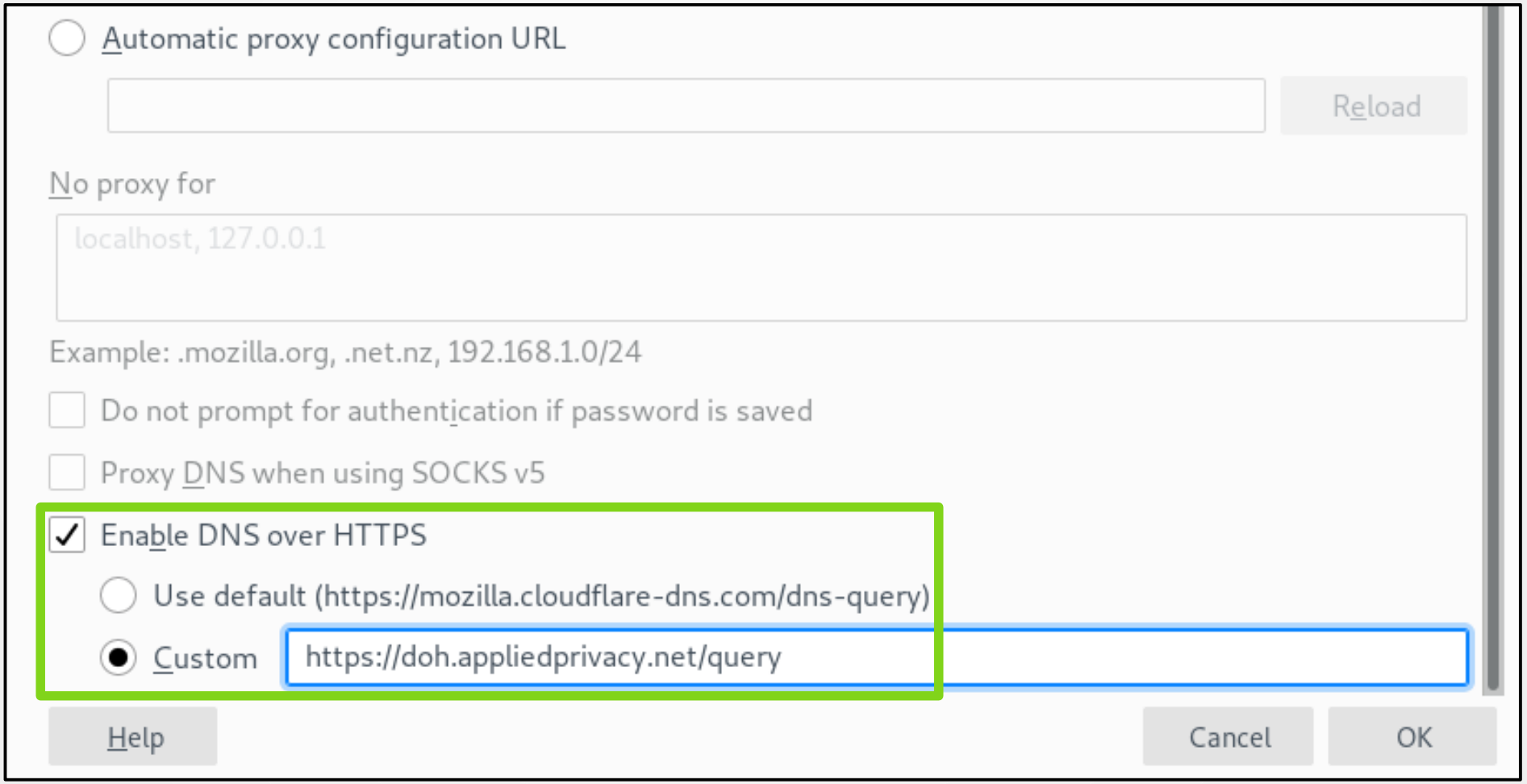
DoH Client Software

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



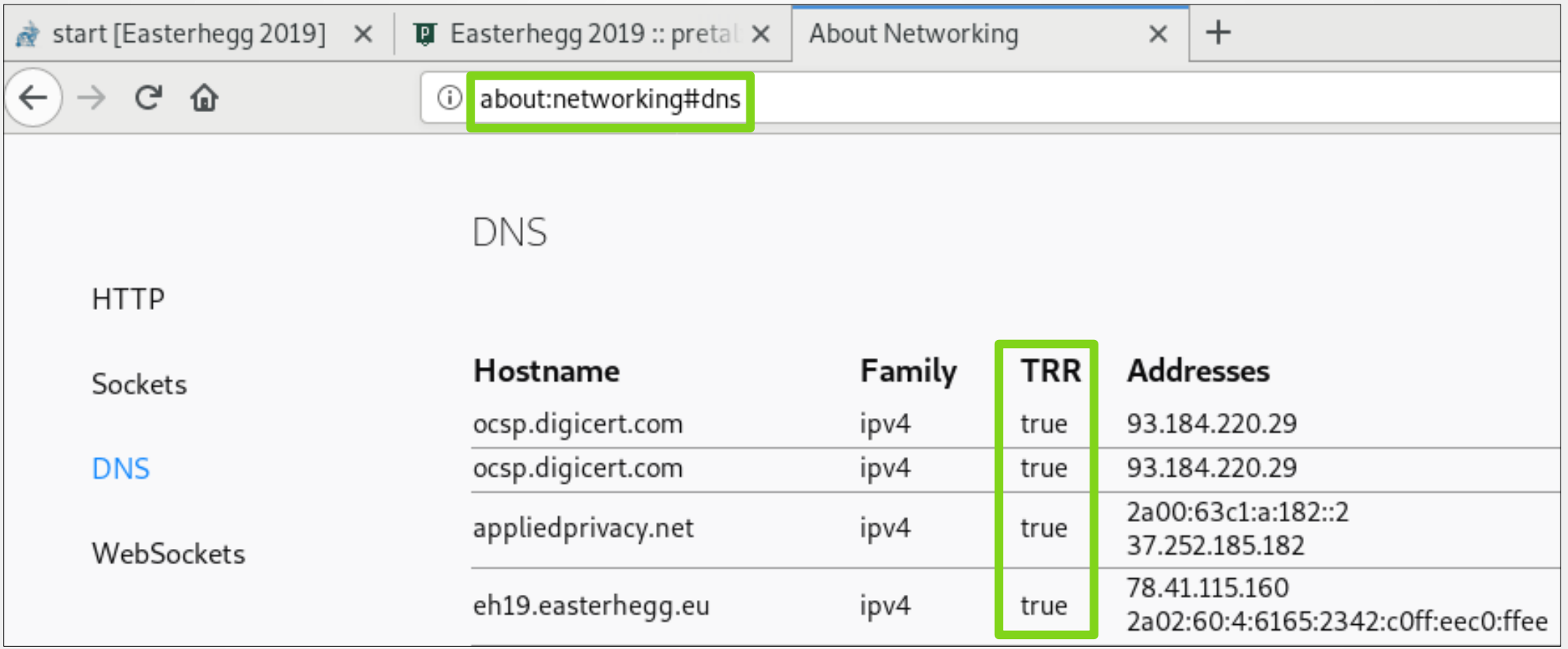
Foundation for Applied Privacy

DoH mit Firefox nutzen



Foundation for Applied Privacy

DoH in Firefox



Foundation for Applied Privacy

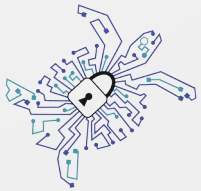
DoH -Firefox Modi

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/

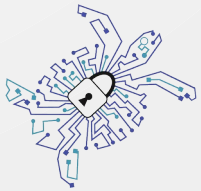


Foundation for Applied Privacy

DoH Server Discovery in Chrome (angekündigt)

- Automatisches Upgrade zu DoH sofern unterstützt

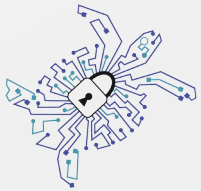
- Statische Liste im Browser (Resolver IP -> DoH URI)



Foundation for Applied Privacy

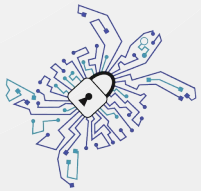
DoH Server Software

- Knot-Resolver 4.0.0
- Experimentell: doh-httpproxy, ...



Foundation for
Applied Privacy

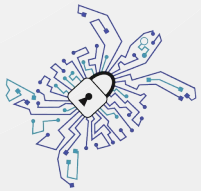
DoH Kritik: HTTP Metadaten



Foundation for Applied Privacy

DoH Kritik: HTTP Metadaten

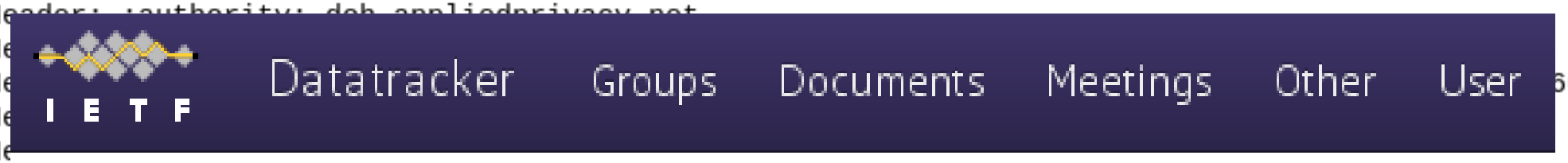
```
Header: :method: POST
Header: :path: /query
Header: :authority: doh.appliedprivacy.net
Header: :scheme: https
Header: user-agent: Mozilla/5.0 (X11; Fedora; Linux x86_64; rv:66.0) Gecko/20100101 Firefox/66.0
Header: accept: application/dns-message
Header: accept-language: en-US,en;q=0.5
Header: accept-encoding: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



Foundation for Applied Privacy

DoH Kritik: HTTP Metadaten

- Header: :method: POST
- Header: :path: /query
- Header: :authority: doh.appliedprivacy.net
- He
- He
- He
- He
- He
- He
- He
- He



66.0

DoHPE: DoH with Privacy Enhancements

draft-dickinson-doh-dohpe-00

Foundation for Applied Privacy

Mozilla / Cloudflare Kritik

Quelle: https://ungleich.ch

Foundation for Applied Privacy

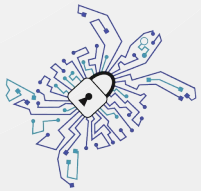
Mozilla / Cloudflare Kritik

Foundation for Applied Privacy

Mozilla / Cloudflare Kritik

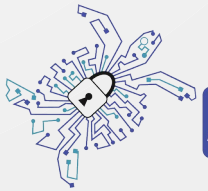
https://dnscrypt.info/public-servers/

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



Foundation for
Applied Privacy

DoH / ISP Kritik



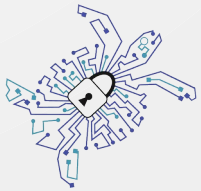
Foundation for
Applied Privacy

DoH / ISP Kritik

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

M. Antonakakis
Georgia Institute of Technology
J. Livingood
Comcast
B. Sleigh
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

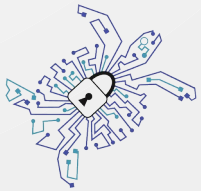
A. Fidler
BT plc
B. Hubert
OpenXchange
J. Livingood
Comcast
J. Reid
RTFM llp
N. Leymann
Deutsche Telekom AG
March 10, 2019

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

Foundation for Applied Privacy

DoH / ISP Kritik

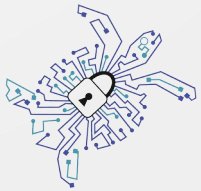
> This will have two unwelcome results. First, threat intelligence and reputation services will have fewer data to analyse and therefore have a significantly less complete perspective of end users' DNS behaviour. Second, the quality and effectiveness of the data provided by threat intelligence and reputation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



Foundation for Applied Privacy

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

DoT vs. DoH

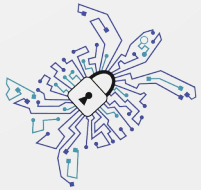
	DoT	DoH
Zensurresistenter	-	+
mit ESNI in Firefox kompatibel	-	+
wenig Metadaten für den Resolver	+	-
Server Software Verfügbarkeit	+	~
Easy Setup (Client)	~	+

Foundation for Applied Privacy

DoH / DoT – DNSSEC?

- Löst unterschiedliche Problem

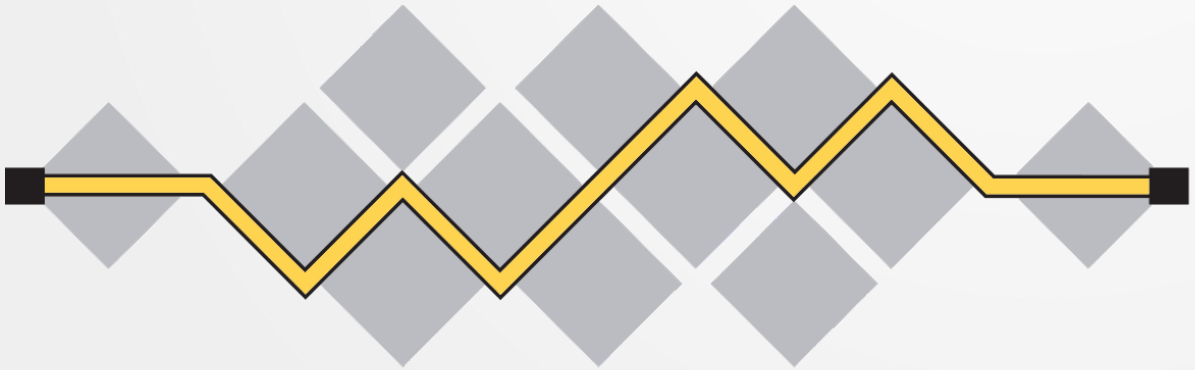
- Am besten in Kombination eingesetzt



Foundation for
Applied Privacy

DNS Privacy - Zukunft

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

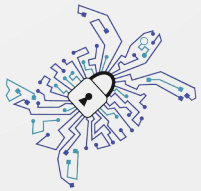


I E T F®

Foundation for Applied Privacy

Fazit

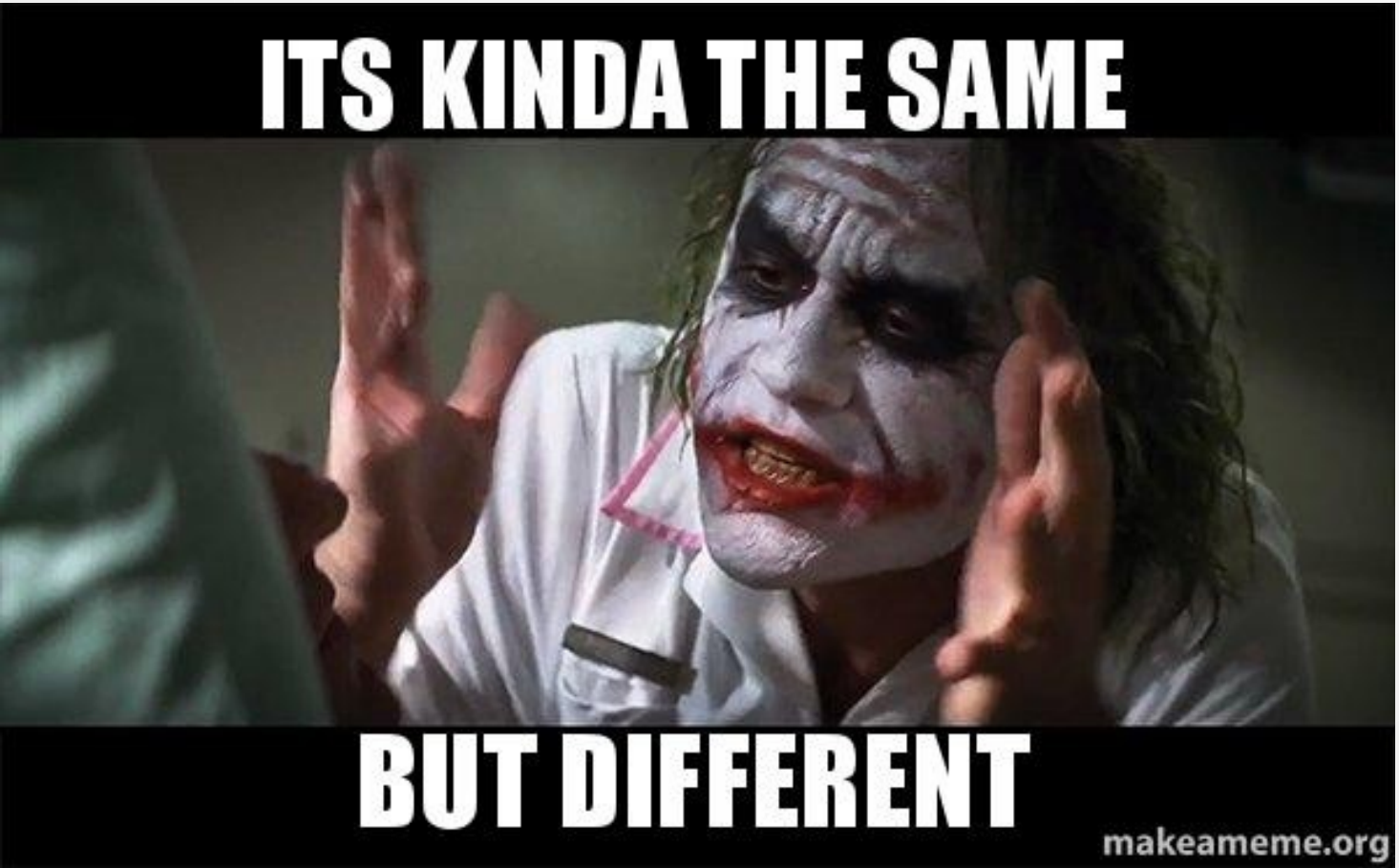
- Verschlüsselt euren DNS Traffik!
- Auch mit DoH/DoT sind Metadaten (zB Hostname) sichtbar (ESNI erforderlich!)
- DoH: pot. schnelle Verbreitung durch Firefox



Foundation for Applied Privacy

Fazit

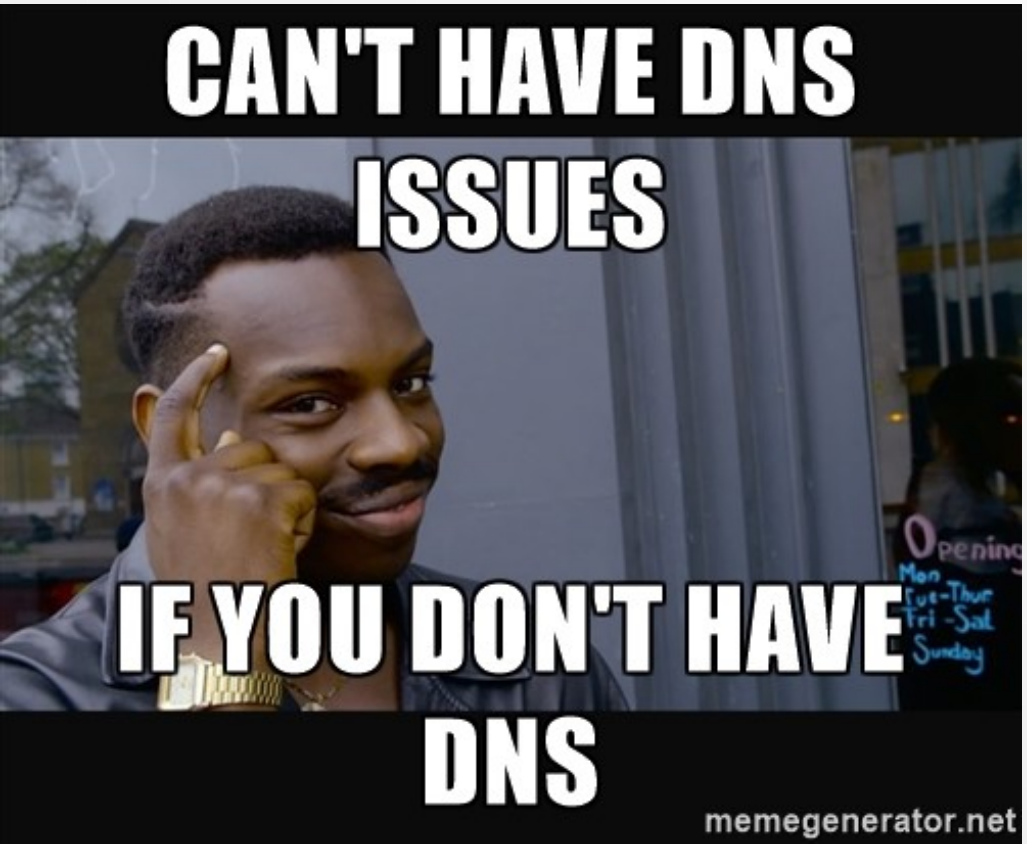
DoT und DoH haben die selben Kernziele



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

gdbr6pm66tzpavenstxove4ftwil52onqmhwioyb7dffojc6h56saoqd.onion

Foundation for Applied Privacy

Fragen?

contact@appliedprivacy.net

@applied_privacy
https://mastodon.social/@applied_privacy

https://appliedprivacy.net

Foundation for Applied Privacy