

Spurenarmes und anonymes Surfen

▶ **digitalcourage**
Hochschulgruppe
Bayreuth ◀

Digitalcourage e.V.

- ▶ Gemeinnütziger Verein für Datenschutz und Bürgerrechte
 - ▷ "Für eine lebenswerte Welt im digitalen Zeitalter"
 - ▷ Big Brother Awards
 - ▷ Aktionen zu aktuellen Themen

- ▶ Orts- und Hochschulgruppen
 - ▷ <https://digitalcourage.de/treffen-vor-ort>
 - ▷ HSG Bayreuth: <https://digitalcourage.de/hsg-bt>

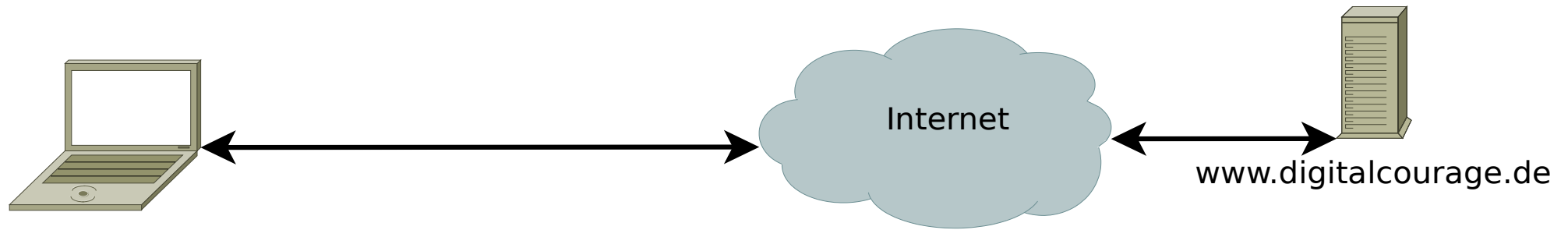
Hochschulgruppe Bayreuth

- ▶ Wir freuen uns über Eure Teilnahme via BigBlueButton; abonniert unsere Mailing-Liste!

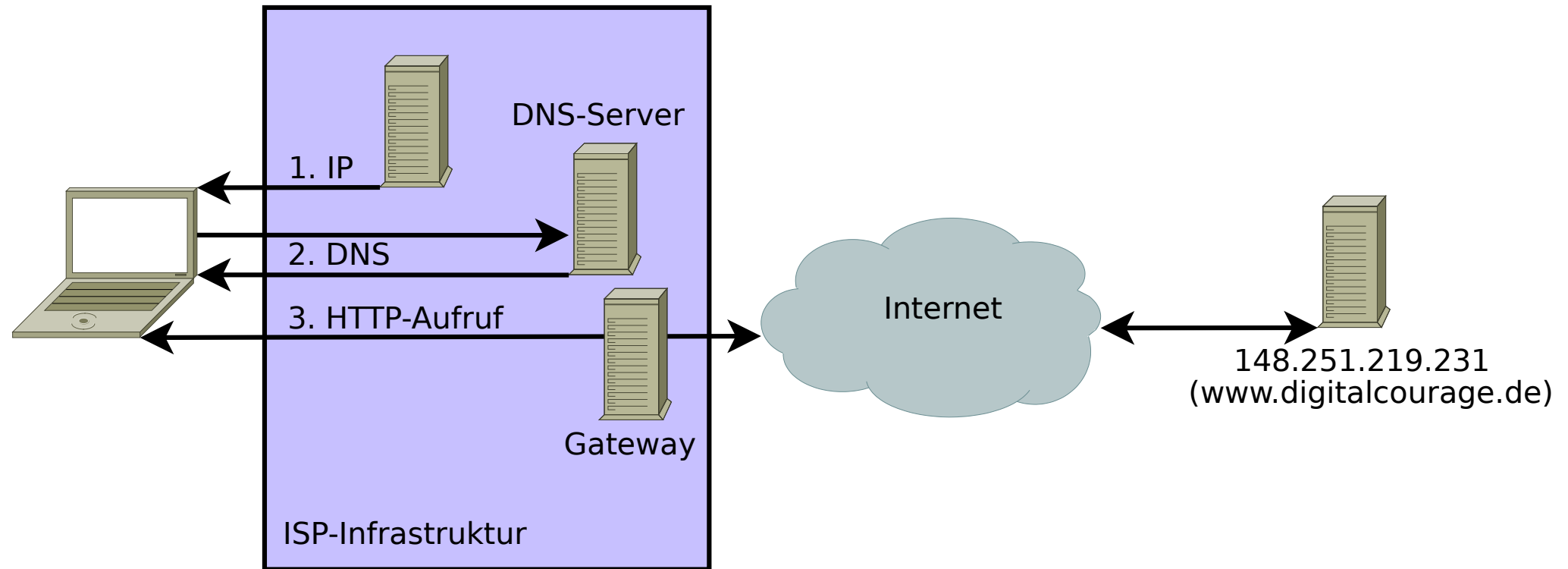
<https://mail.digitalcourage.de/cgi-bin/mailman/listinfo/dc-hsg-bayreuth>

- ▶ Livestream der BigBrotherAwards:
 - ▷ Freitag, 18. September 2020, 17:30 Uhr
 - ▷ Black Box im RW21 (UG)
Richard-Wagner-Straße 21
95444 Bayreuth

Wie funktioniert das Web?



Und technisch?



Wie schrecklich ist die Web-Realität (mit Standardeinstellungen)?

- ▶ Beispiel: <https://www.spiegel.de/> (mit aktuellem Firefox)

... so schrecklich!

- ▶ Beispiel: **https://www.spiegel.de/**
- ▶ ca. 380 Anfragen, davon ca. 10 an deutsche Server des Spiegel; insgesamt Anfragen an 65 externe Domains ...
- ▶ **www.spiegel.de, cdn.prod.www.spiegel.de, sams.spiegel.de, spiegel-de.spiegel.de, sats.spiegel.de**

... so schrecklich!

bat.bing.com, facebook.com, tracking.adalliance.io,
admixer.net, .amazon-adsystem.com, .meetrics.net,
.googlesyndication.com, adobedtm.com,
script.ioam.de, .criteo.net, **googletagmanager.com**,
omny.fm, .cloudfront.net, .mxcdn.net, .mxcdn.net, .optimizely.
com, static.emsservice.de, dyn.emetriq.de,
optout.adalliance.io, .sparwelt.click,
ajax.**googleapis.com**, .config.parse.ly.com, bidder.criteo.com,
dpm.demdex.net, de.ioam.de, ad.**doubleclick.net**, **google-**
analytics.com, ad.yieldlab.net, ups.xplosion.de, js-
agent.newrelic.com, .cloudfront.net, bam.nr-data.net,
xpl.theadex.com, adservice.**google.de**, pippio.com,
cdn.adrtx.net, .flashtalking.com, pixel.adsafeprotected.com,
tags.bluekai.com, .2mdn.net, m.exactag.com, dnacdn.net,
widgets.outbrain.com, cdn.content-garden.com, ...

... so schrecklich!

- ▶ 8–15 MB; 58 Cookies, 28 von Drittanbietern
- ▶ Ladezeit ca. 15-30 Sek. + Nachladen ohne Interaktion und Scrollen

VISUALIZATION

Graph

DATA

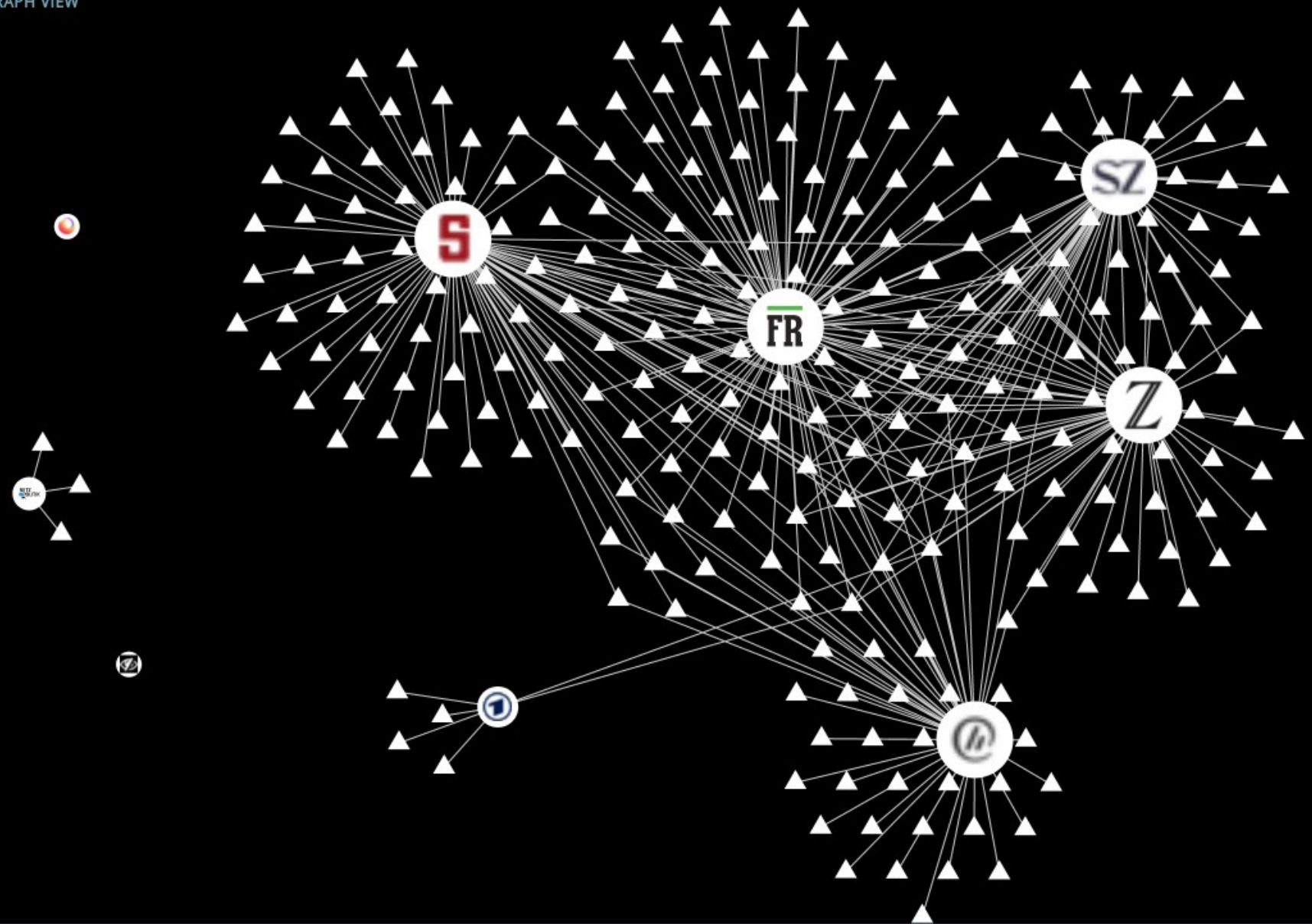
Save Data

Reset Data


[Give Us Feedback](#)

Recent Site


GRAPH VIEW





VISUALIZATION

 Graph

DATA

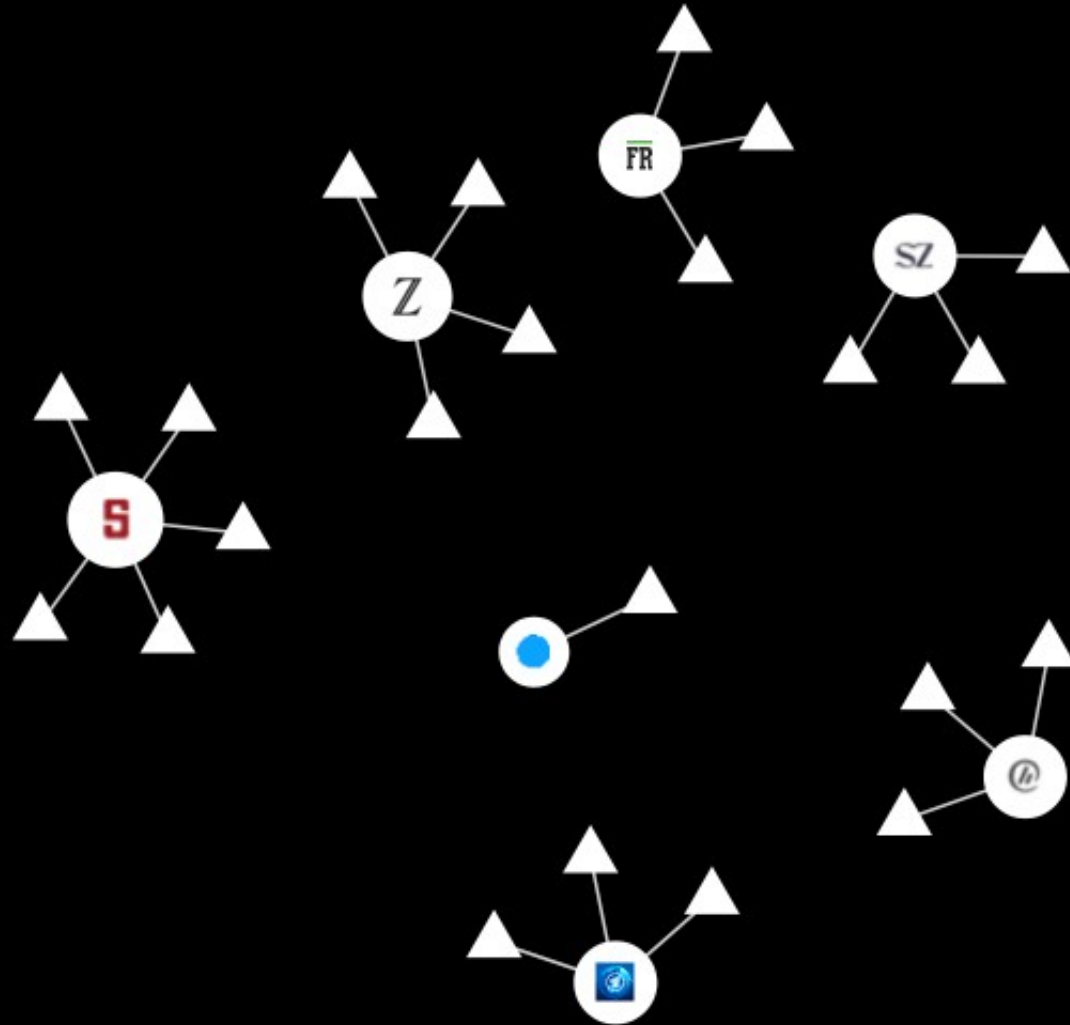
 Save Data

 Reset Data

 [Give Us Feedback](#)

Recent Site

GRAPH VIEW



Überprüfe Deine Webseite!

Check

Webbkoll hilft Dir festzustellen, welche datenschutzrechtlichen Maßnahmen eine Website ergriffen hat, um Dir die Kontrolle über Deine Privatsphäre zu geben.

Bitte beachte:

1. Dieses Tool simuliert einen normalen Browser mit ausgeschalteter "Do Not Track" Funktion (ist bei den meisten die Standardeinstellung) und ohne Erweiterungen.
2. Auch wenn Du `https://` eingibst, prüfen wir `http://` und ob es automatisch auf eine `https://` Seite weiter leitet (Weiterleitungen wird gefolgt).
3. Im Allgemeinen sollte alles funktionieren, manchmal kann es jedoch vorkommen, dass einzelne Seiten aus den verschiedensten Gründen nicht funktionieren.
4. Das Back-End läuft derzeit auf einem einzelnen Server mit begrenzten Ressourcen. In Spitzenzeiten kann ein Durchlauf daher etwas dauern. (Wenn Du willst, kannst Du [Webbkoll in einer eigenen Instanz](#) betreiben!)
5. Feedback ist willkommen: Sende uns eine [Email](#) oder [berichte einen Fehler](#).

Testergebnisse werden auf unserem Servern für 24 Stunden im Arbeitsspeicher gehalten. Wir zeigen keine Liste von zuletzt getesteten URLs. Wir verwenden keine URLs oder Testergebnisse. Wir loggen keine IP Adressen. Wir verwenden keine Cookies.

Entwickelt von [dataskydd.net](#).

Der [Quellcode](#) ist auf [GitHub](#) verfügbar.

Feedback? Fragen? info@dataskydd.net

Twitter: [@dataskyddnet](#)

[Unterstütze uns](#)

<https://webbkoll.dataskydd.net/de>
(Websites auf Tracker überprüfen)

„Here’s how we take back the Internet“

– Titel eines TED-Vortrags von Edward Snowden

Sicheres Surfen mit Privatsphäre

Was wollen wir?

- ▶ Sicherheit:
 - ▷ Vertraulichkeit
 - ▷ Authentizität
 - ▷ Integrität

Sicheres Surfen mit Privatsphäre

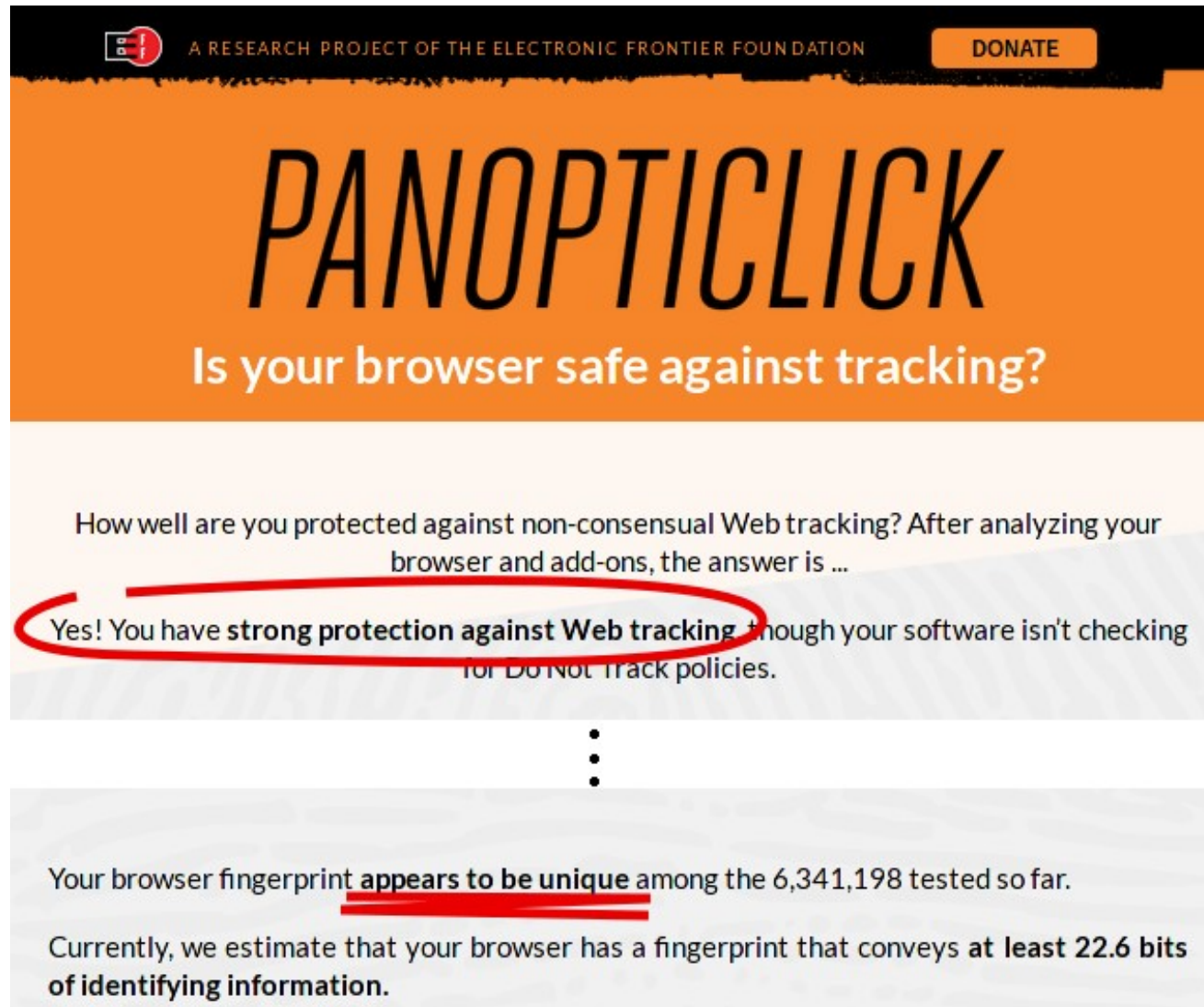
Was wollen wir?

- ▶ Sicherheit:
 - ▷ Vertraulichkeit
 - ▷ Authentizität
 - ▷ Integrität
- ▶ Anonymität
 - ▷ Nur teilweise vereinbar mit Authentizität!
- ▶ Resistenz gegenüber Zensur

Wie kann ein Webserver mich identifizieren und verfolgen (Tracking)?

- ▶ Cookies
 - ▷ Kleine Textdateien, die die aufgerufene Website im Browser speichern und wieder abrufen kann.
- ▶ Browser- und Betriebssystem-Merkmale:
 - ▷ Browsertyp und -version, Betriebssystem, Sprache
 - ▷ Schriftarten, Browser-Add-ons (Noscript, Flash, ...), Browser-Fenstergröße, Font-Rendering, u.v.m.
- ▶ Externe Merkmale:
 - ▷ IP-Adresse
- ▶ Eindeutiger Browser-Fingerabdruck:
 - ▷ <https://panopticklick.eff.org>

Wie einzigartig bin ich im Web? Browser-Fingerabdruck testen



The screenshot shows the Panopticlick website interface. At the top, there is a black header with the EFF logo, the text "A RESEARCH PROJECT OF THE ELECTRONIC FRONTIER FOUNDATION", and a "DONATE" button. Below the header is a large orange banner with the title "PANOPTICCLICK" and the question "Is your browser safe against tracking?". The main content area is white with a light gray background pattern. It contains the text: "How well are you protected against non-consensual Web tracking? After analyzing your browser and add-ons, the answer is ...". Below this, a red circle highlights the text: "Yes! You have strong protection against Web tracking, though your software isn't checking for Do Not Track policies." A vertical ellipsis follows. At the bottom, it states: "Your browser fingerprint appears to be unique among the 6,341,198 tested so far." and "Currently, we estimate that your browser has a fingerprint that conveys at least 22.6 bits of identifying information."

EFF A RESEARCH PROJECT OF THE ELECTRONIC FRONTIER FOUNDATION DONATE

PANOPTICCLICK

Is your browser safe against tracking?

How well are you protected against non-consensual Web tracking? After analyzing your browser and add-ons, the answer is ...

Yes! You have strong protection against Web tracking, though your software isn't checking for Do Not Track policies.

⋮

Your browser fingerprint appears to be unique among the 6,341,198 tested so far.

Currently, we estimate that your browser has a fingerprint that conveys at least 22.6 bits of identifying information.

Wie kann ich mich vor Tracking schützen?

- ▶ Browser-Wahl: Firefox
- ▶ Browser-Einstellungen
 - ▷ Seitenelemente blockieren: Benutzerdefiniert
 - Elemente zur Aktivitätsverfolgung in allen Fenstern blockieren
 - Alle Cookies von Drittanbieter blockieren
 - Identifizierer (Fingerprinter) blockieren
 - ▷ „Do Not Track“-Information immer senden
- ▶ Suchmaschinen
 - ▷ MetaGer.de, Startpage.com, Duckduckgo.com, Qwant.com
(im Gegensatz zu Google auch keine individualisierten Ergebnisse)
- ▶ JavaScript abschalten, wenn möglich
- ▶ Browser-Add-ons!

Wahl des Browsers: Mozilla Firefox



- ▶ <https://www.mozilla.org/de/firefox/browsers/>
- ▶ Freie Software
- ▶ Für Linux, Windows, macOS, Android und iOS (hier mit Einschränkungen) verfügbar
- ▶ Der einzige große Browser, der nicht auf Googles Chromium-Projekt aufbaut

Firefox-Add-ons

Für Einsteiger:

- ▶ Tracker und Werbung blocken: **uBlock Origin**
- ▶ JavaScript-Bibliotheken ersetzen: **LocalCDN**
- ▶ Webseiten immer verschlüsseln: **HTTPS Everywhere**
- ▶ Cookies automatisch löschen: **Cookie AutoDelete**

Firefox-Add-ons

Für Fortgeschrittene:

- ▶ Referrer blockieren: **SmartReferer**
- ▶ JavaScript blockieren:
(nach Installation Whitelist säubern) **NoScript**
- ▶ Alle Drittanbieteranfragen blocken: **uMatrix**

Kontrolle

- ▶ Wirkung von Add-ons und Einstellungen kontrollieren:
 - ▷ Add-on: Lightbeam 3.0
 - ▷ Menü → Web-Entwickler → Netzwerkanalyse (Umschalt + F12)

Exkurs zu Suchmaschinen: Google sollte nicht alles wissen!

- ▶ Zahlreiche Alternativen verfügbar

metaGer

- ▶ Eine davon: **MetaGer.de**

- ▷ Wird vom SUMA-EV aus Hannover betrieben
- ▷ Eigener Suchindex & Ergebnisse verschiedener Suchmaschinen
- ▷ Freie Software
- ▷ Arbeitet datensparsam
- ▷ Kann als neue Standard-Suchmaschine im Browser eingerichtet werden

- ▶ Noch mehr Alternativen: StartPage.com, DuckDuckGo.com, Qwant.com

Exkurs: Privater Modus von Firefox

- ▶ Keine Speicherung von Daten besuchter Webseiten **auf dem eigenen** Computer (insb. keine Chronik, keine URL-Vervollständigung, Cookies, etc.)
- ▶ auf dem lokalen System verbleiben keine Spuren
- ▶ aber: **keine Anonymität gegenüber dem Netz**



Dies ist ein privates Fenster

Firefox leert die eingegebenen Suchbegriffe und besuchten Webseiten beim Beenden der Anwendung oder wenn alle privaten Tabs und Fenster geschlossen wurden. Das macht Sie gegenüber Website-Betreibern und Internetanbietern nicht anonym, aber erleichtert es Ihnen, dass andere Nutzer des Computers Ihre Aktivitäten nicht einsehen können.

[Häufige Missverständnisse über das Surfen im Privaten Modus](#)

Sicheres Surfen mit Privatsphäre

Was wollen wir?

▶ Sicherheit:

- ▷ Vertraulichkeit
- ▷ Authentizität
- ▷ Integrität

▶ Anonymität

- ▷ Nur teilweise vereinbar mit Authentizität!

▶ Resistenz gegenüber Zensur

Wie bekommen wir das?

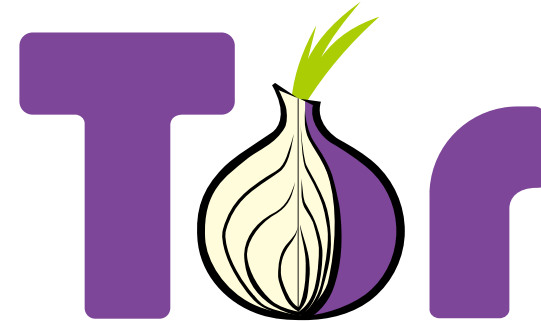
- ▷ HTTPS (Verschlüsselung)
- ▷ HTTPS (Zertifikate)
- ▷ HTTPS

- ▷ Firefox
- ▷ Tracking blocken
- ▷ nur benötigte Cookies
- ▷ Tor-Browser

Anonym surfen mit dem Tor-Browser

Tor: The Onion Router

- ▶ Netzwerk zur Anonymisierung von Verbindungsdaten
- ▶ IP-Adresse wird verschleiert



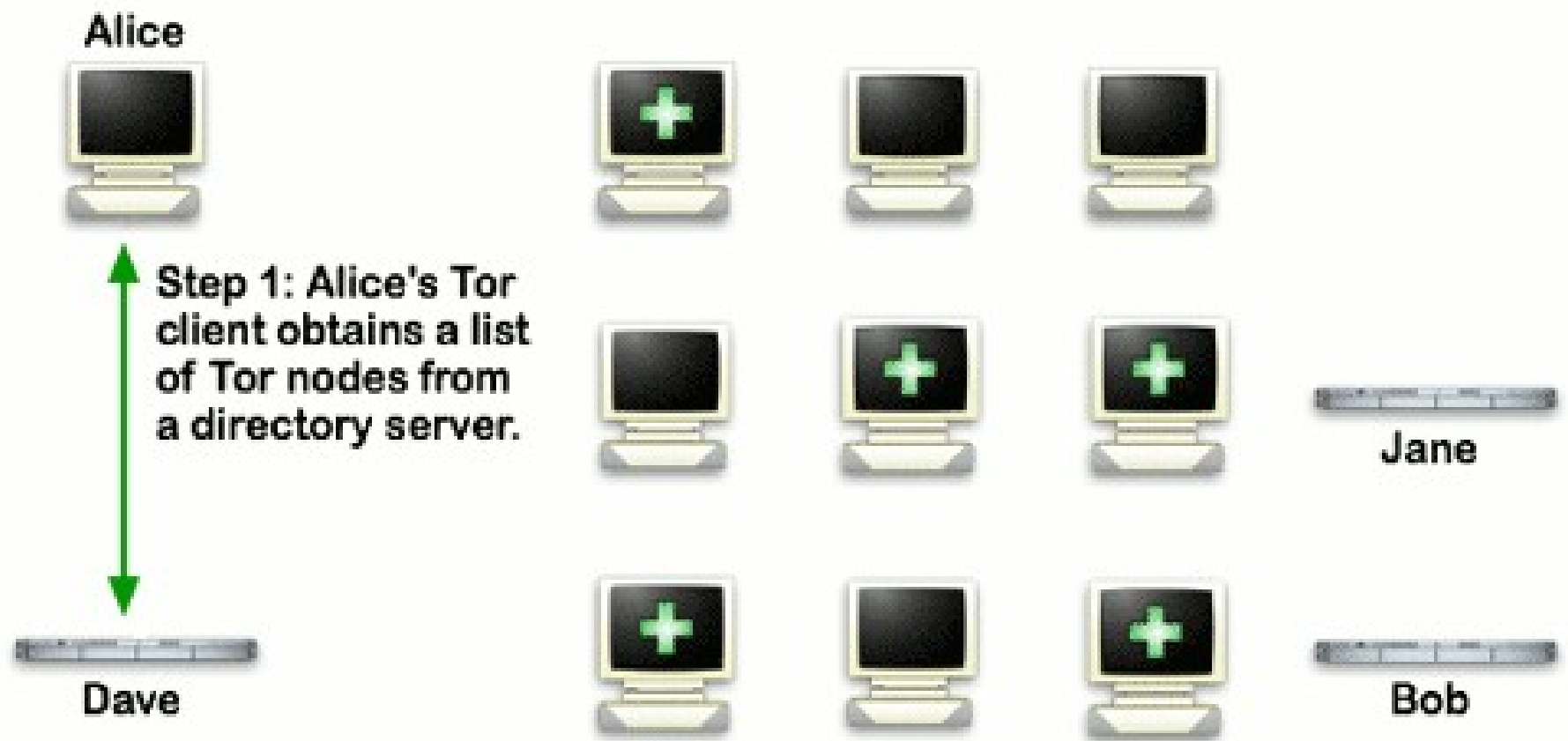
Vorteile

- ▶ quelloffen, freie Software
- ▶ anonymes Surfen

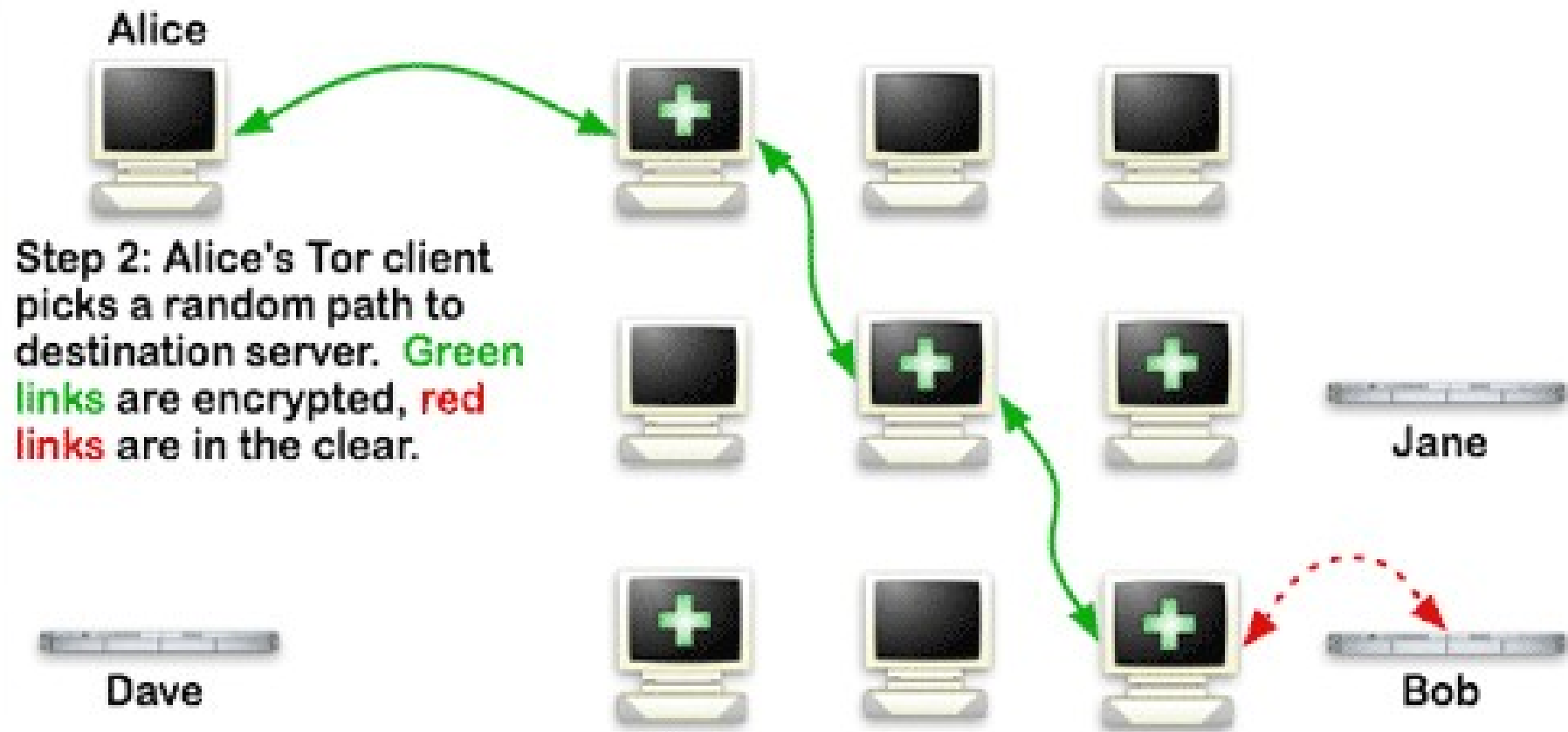
Nachteile

- ▶ Login bei personalisierten Seiten nicht sinnvoll
- ▶ Latenz ist größer

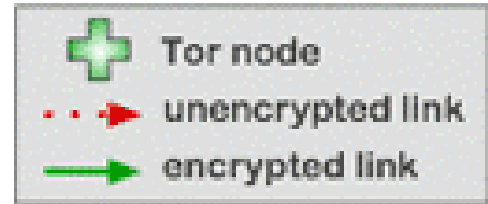
How Tor Works: 1



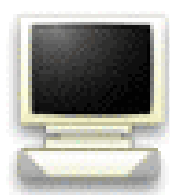
How Tor Works: 2



E How Tor Works: 3



Alice



Jane



Bob

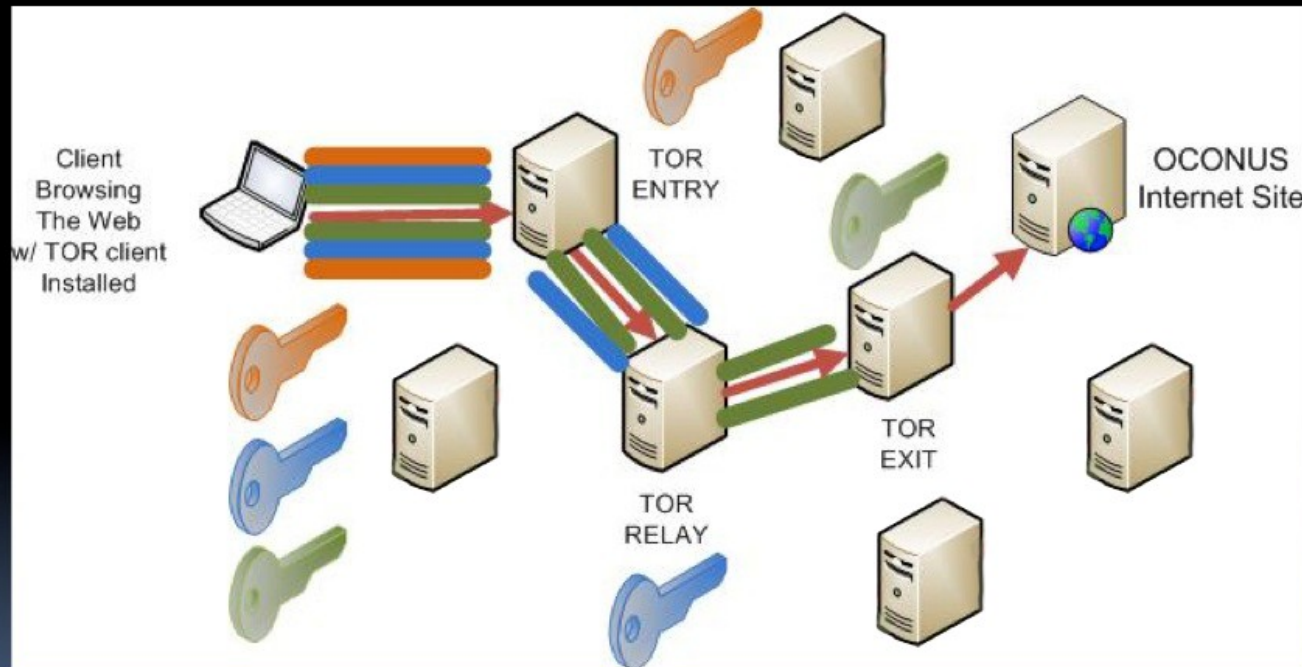
Step 3: If at a later time, the user visits another site, Alice's tor client selects a second random path. Again, **green links** are encrypted, **red links** are in the clear.



Dave



(U) What is TOR?



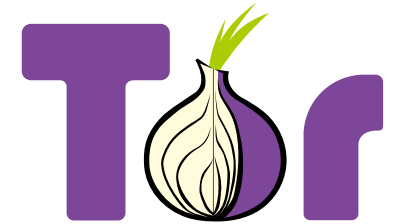
Wie nutze ich Tor?

- ▶ Tor-Browser installieren
 - ▷ Modifizierter Firefox mit mehreren Addons (NoScript, HTTPS Everywhere, Torbutton und TorLauncher)
 - ▷ <https://www.torproject.org/download/>
- ▶ Hinweis zur Zielgruppe:
 - ▷ Nutzung ist vor allem bei exponierten Personen sinnvoll (Investigativjournalisten, innerhalb bestimmter Länder mit zensierten Internet oder anderweitiger Unterdrückung, ...)
 - ▷ Für den Normalanwender ist oftmals die Verwendung von Werbeblockern und ggf. weiteren Addons ausreichend

Anonym Surfen mit Tor (The Onion Router)

▶ Normales Surfen

- ▷ Beide Seiten sehen ihr Gegenüber direkt



▶ Surfen mit Tor

- ▷ Sämtlicher Datenverkehr geht über das Tor-Netzwerk
- ▷ Nur der Einstiegsknoten des Tor-Netzwerks "kennt" mich
- ▷ Die angesurfte Internetseite hat keine Möglichkeit, meine Herkunft (IP-Adresse) herauszufinden

▶ Vorteile

- ▷ Quelloffen, freie Software
- ▷ Anonymes Surfen


▶ Nachteile

- ▷ Login bei personalisierten Seiten nicht sinnvoll
- ▷ Langsamer

Über Tor - Tor-Browser

Über Tor x +


← → ↻ Tor-Browser Suche oder Adresse eingeben ☆ 🛡️ 🔧 ☰

 Nutzen Sie Tor-Browser das erste Mal? Schauen Sie sich diese kleine Einführung an.

Tor-Browser 9.5
[Änderungsprotokoll anzeigen](#)


Entdecken. Privat.

Du bist bereit für das privateste Browsing-Erlebnis der Welt.

 Mit DuckDuckGo suchen →

Tor ist aufgrund von Spenden von Leuten wie dir frei nutzbar. [Spende jetzt »](#)

Fragen? [Schau unser Tor Browser Handbuch an »](#)

 Erhalte die neuesten Nachrichten von Tor direkt in den Posteingang. [Tor-Nachrichten abonnieren. »](#)

Projekt Tor ist eine in den USA als "The Tor Project" US 501(c)(3) registrierte nicht-kommerzielle Organisation für Menschenrechte und Freiheit, die freie und

Tails – ein OS für Tor

- ▶ The Amnesic Incognito Live System (Tails)

- ▷ <https://tails.boum.org/>

- ▶ Live-Linux (via USB oder DVD)

- ▶ Anonymität als erstes Designprinzip

- ▶ Viele Tools:

- ▷ **Pidgin** (Chats via XMPP und IRC)

- ▷ **Electrum** (Bitcoin-Wallet)

- ▷ **MAT2** (Metadaten von Dateien entfernen)

- ▷ **KeePassXC** (Passwortverwaltung)



Weiterführende Literatur

- ▶ Firefox-Kompendium von Mike Kuketz:
<https://www.kuketz-blog.de/artikelserien/#firefox>
- ▶ Spurenarm Surfen im Privacy-Handbuch:
https://www.privacy-handbuch.de/handbuch_21.htm
- ▶ Tails-Broschüre von Çapulcu
<https://capulcu.blackblogs.org/neue-texte/bandi/>
- ▶ Digitale Selbstverteidigung bei Digitalcourage:
<https://digitalcourage.de/digitale-selbstverteidigung>

Weitere Vorträge

- ▶ Online-Crypto-Seminar der HSG Bielefeld:
<https://digitalcourage.de/blog/2020/online-crypto-seminar-vom-24-juni-bis-zum-2-juli-2020>
 - ▷ Mi, 1. Juli, 18 Uhr: E-Mail-Verschlüsselung
 - ▷ Do, 2. Juli, 18 Uhr: Datenschutz auf Mobilgeräten
- ▶ Infos über Nachholtermine der HSG Bayreuth:
<https://digitalcourage.de/hochschulgruppe-bayreuth>
- ▶ CryptoParties weltweit:
<https://www.cryptoparty.in/index>

Vielen Dank fürs Mitmachen!

