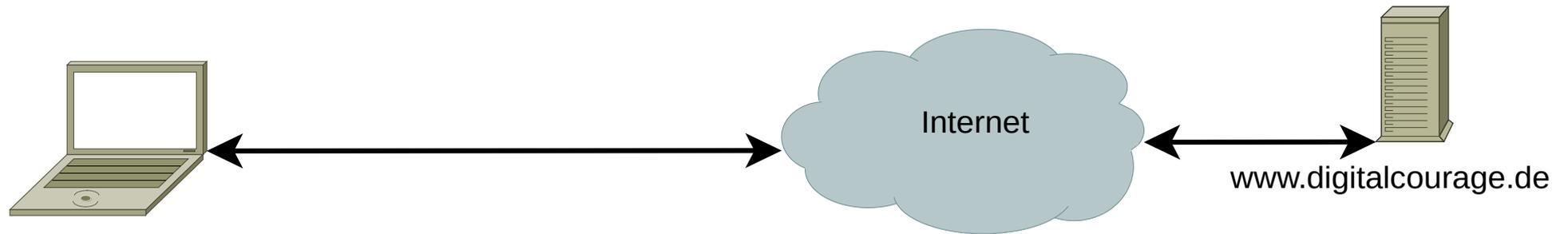


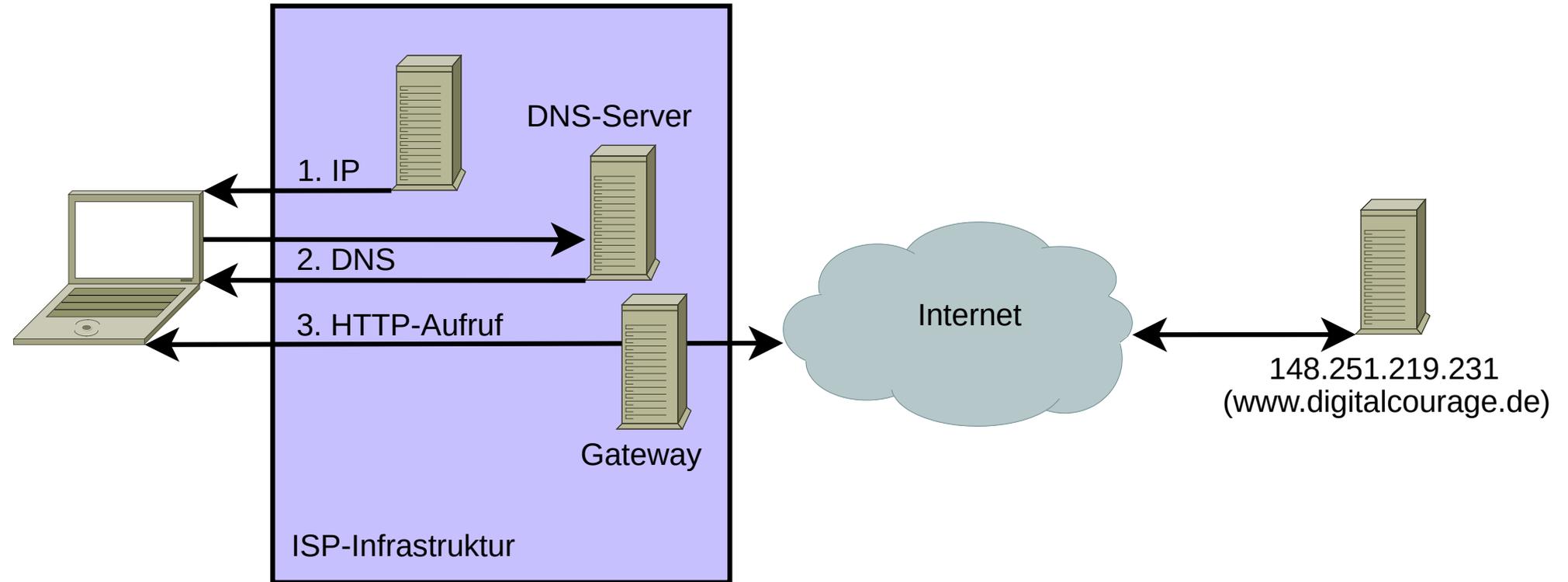
Sicher und anonym im World Wide Web



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

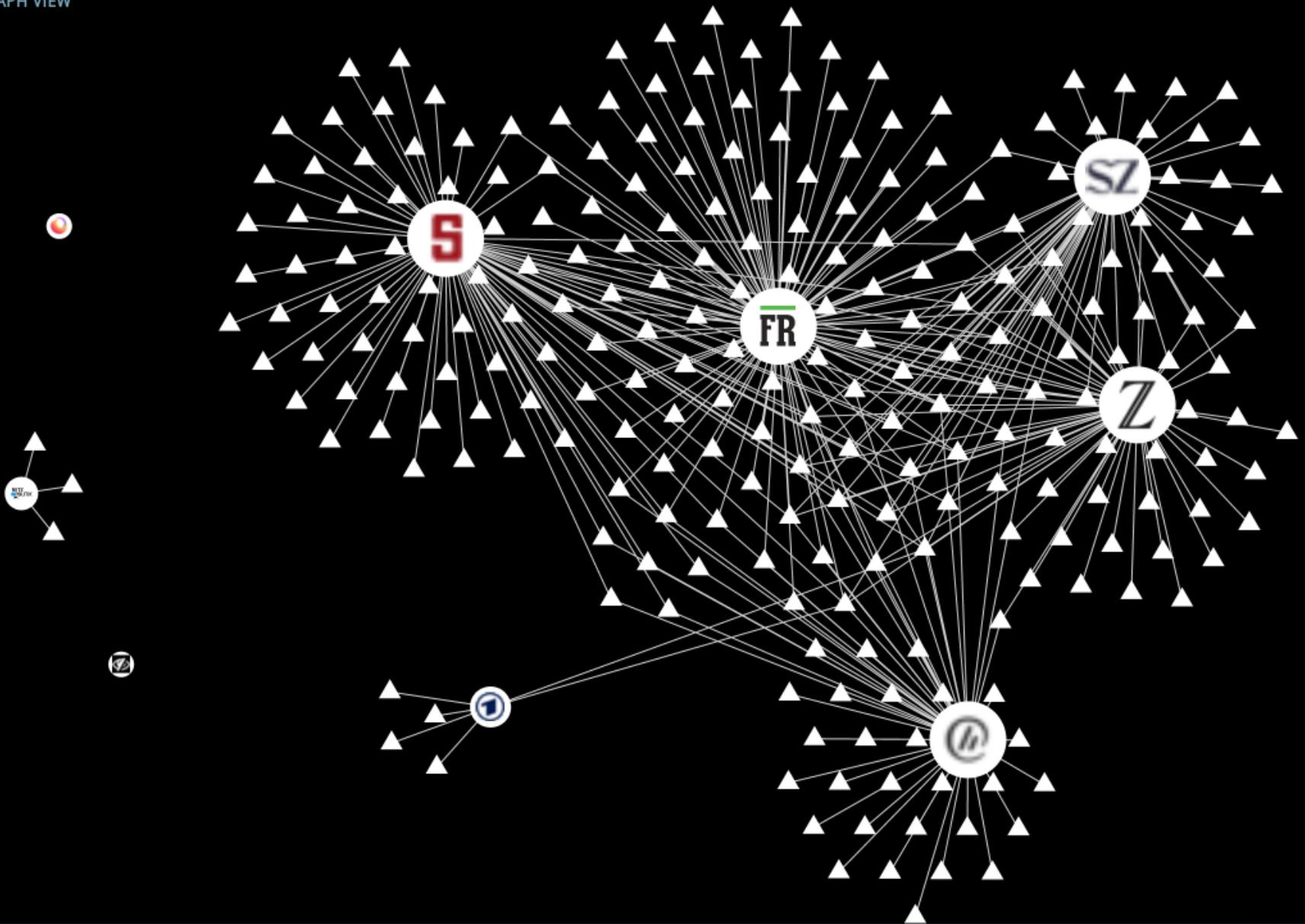
Save Data

Reset Data

[Give Us Feedback](#)

Recent Site

GRAPH VIEW





VISUALIZATION

 Graph

DATA

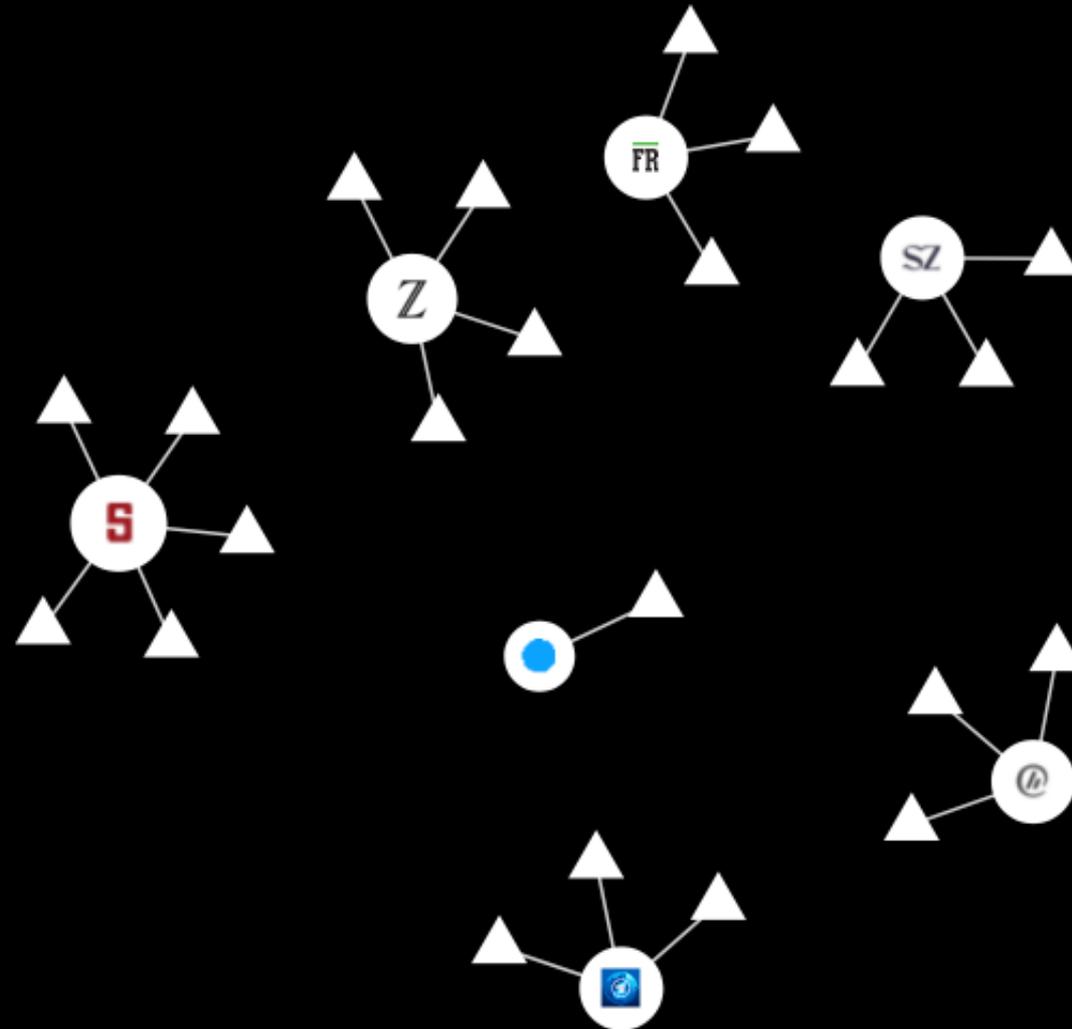
 Save Data

 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](https://twitter.com/dataskyddnet)

[Unterstütze uns](#)

<https://webbkoll.dataskydd.net/de>
(schwed. Web-Track · Datenschutz)

„Here’s how we take back the Internet“

– Titel eines TED-Vortrags von Edward Snowden

Sicheres Surfen mit Privatsphäre

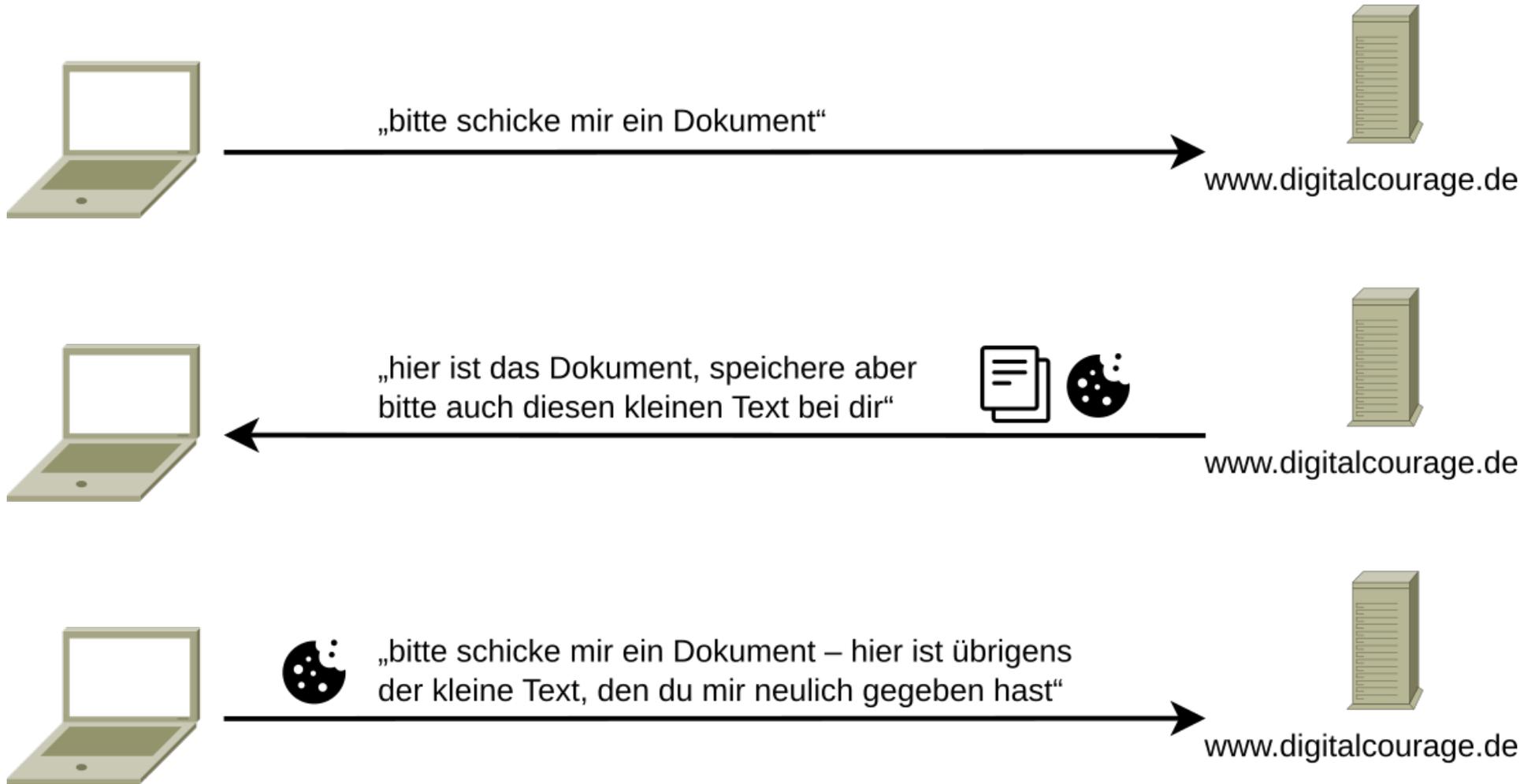
Was wollen wir?

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

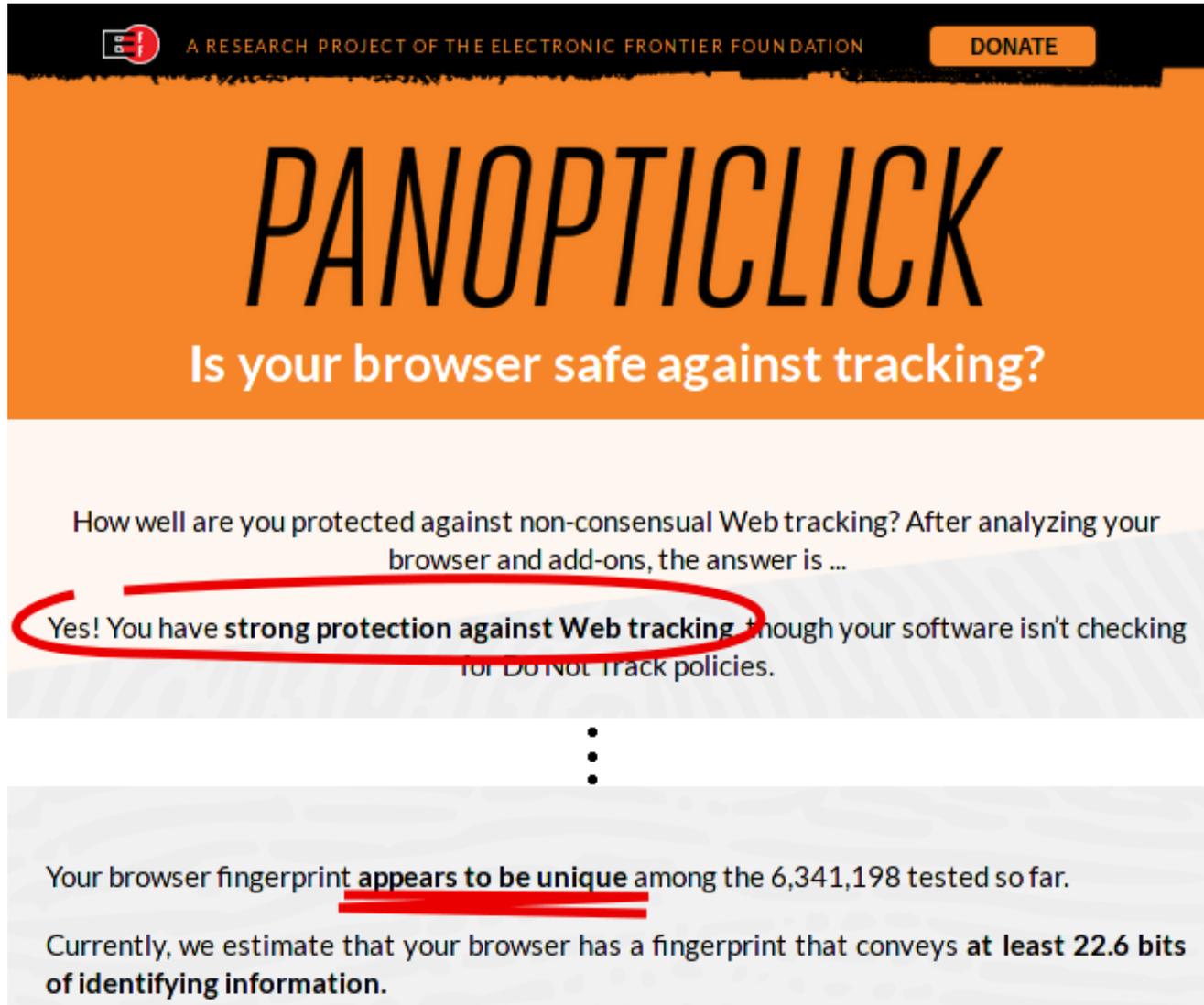
Was sind Cookies?



Was machen Cookies?

- ▶ sie lösen das Problem, dass HTTP „kein Gedächtnis“ hat
- ▶ Speichern von vorübergehenden Einstellungen:
 - ▷ bevorzugte Sprache, vielleicht auch regionale Präferenzen
 - ▷ meine Cookie-Präferenzen :-)
- ▶ Speichern, dass ich mich eingeloggt habe
- ▶ typisch: Zuweisung einer zufällig erzeugten, aber eindeutigen Kennung, um mich zu „identifizieren“
 - ▷ auch wenn ich mich nicht eingeloggt habe
 - ▷ Tracking – wenn das Cookie einem Drittanbieter gehört, der auf vielen Sites eingebunden ist: Tracking über alle diese Sites

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 on the left, the text "A RESEARCH PROJECT OF THE ELECTRONIC FRONTIER FOUNDATION" in the center, and a "DONATE" button on the right. Below the header is a large orange banner with the word "PANOPTICCLICK" in a large, black, serif font. Underneath the banner, the question "Is your browser safe against tracking?" is displayed in white text. The main content area has a light gray background with a subtle 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 oval 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 of three dots is centered below this text. At the bottom of the main content area, there is another text block: "Your browser fingerprint appears to be unique among the 6,341,198 tested so far." Below this, it states: "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, lite.qwant.com
(im Gegensatz zu Google auch keine individualisierten Ergebnisse)
- ▶ JavaScript abschalten, wenn möglich
- ▶ Browser-Add-ons!

Firefox-Add-ons

Für Einsteiger:

- ▶ Tracker und Werbung blocken: **uBlock origin**
- ▶ Java-Script-Bibliotheken ersetzen: **Decentraleyes**
- ▶ Webseiten immer verschlüsseln: **HTTPS Everywhere**
- ▶ Cookies automatisch löschen: **Cookie AutoDelete**
- ▶ Adobe Flash am besten entfernen oder deaktivieren!

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

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

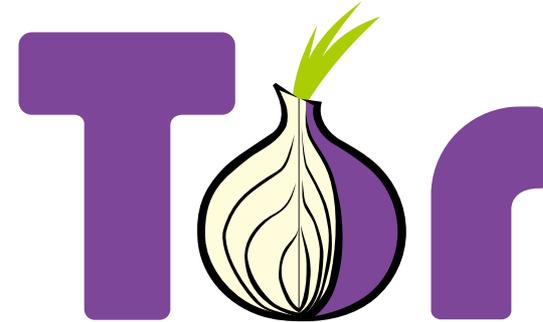
Wie bekommen wir das?

- ▷ HTTPS (Verschlüsselung)
- ▷ HTTPS (Zertifikate)
- ▷ HTTPS
- ▷ Firefox
- ▷ Tracking / Cookies reduzieren
- ▷ Tor-Browser

Anonym surfen mit dem Tor-Browser

Tor: The Onion Router

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



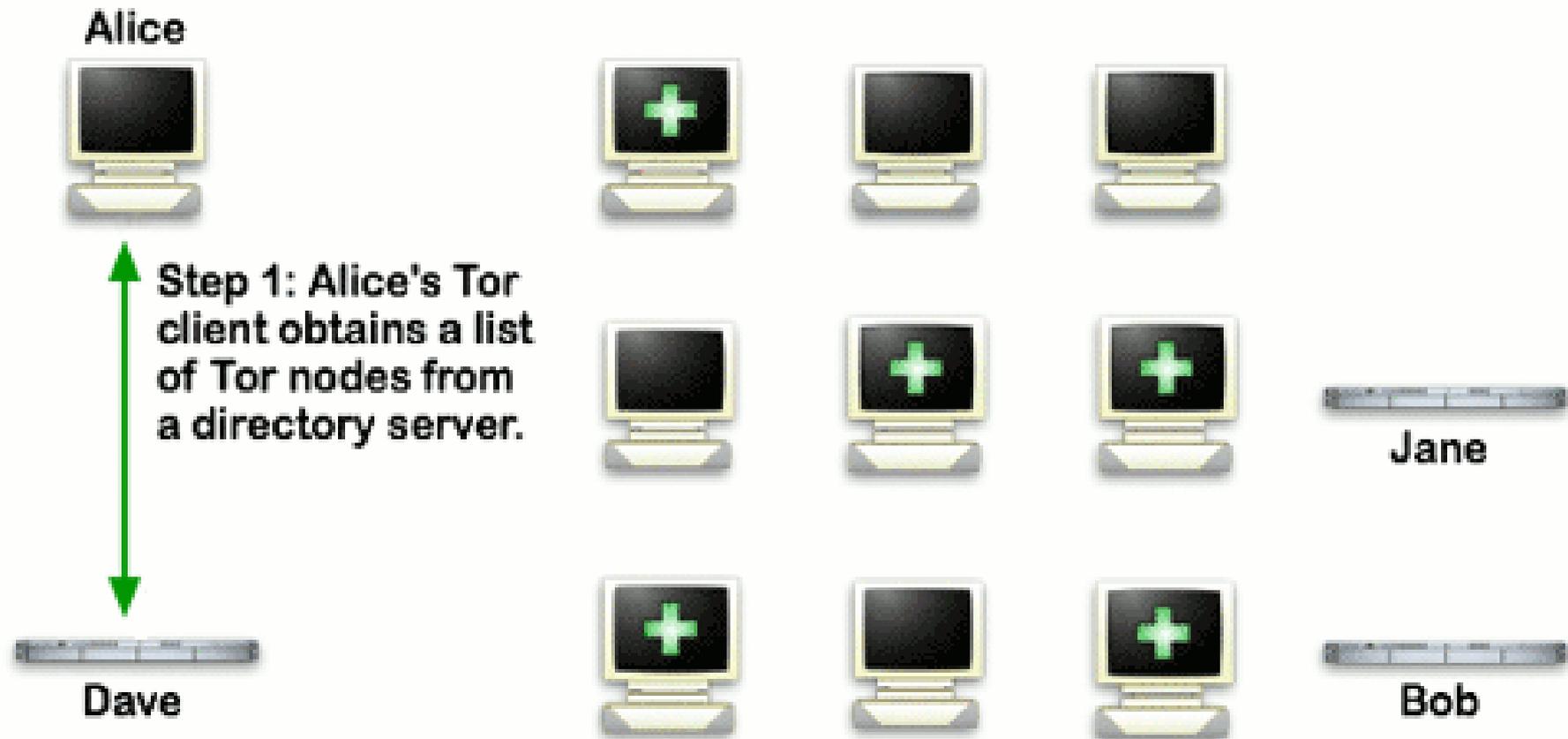
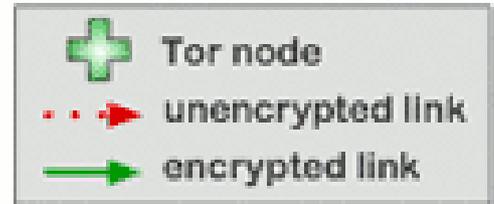
Vorteile

- ▶ quelloffen, freie Software
- ▶ anonymes Surfen

Nachteile

- ▶ Latenz ist größer
- ▶ Hinweis: Nutzung von Tor auf Sites mit persönlichem Login ist nicht sinnvoll

How Tor Works: 1



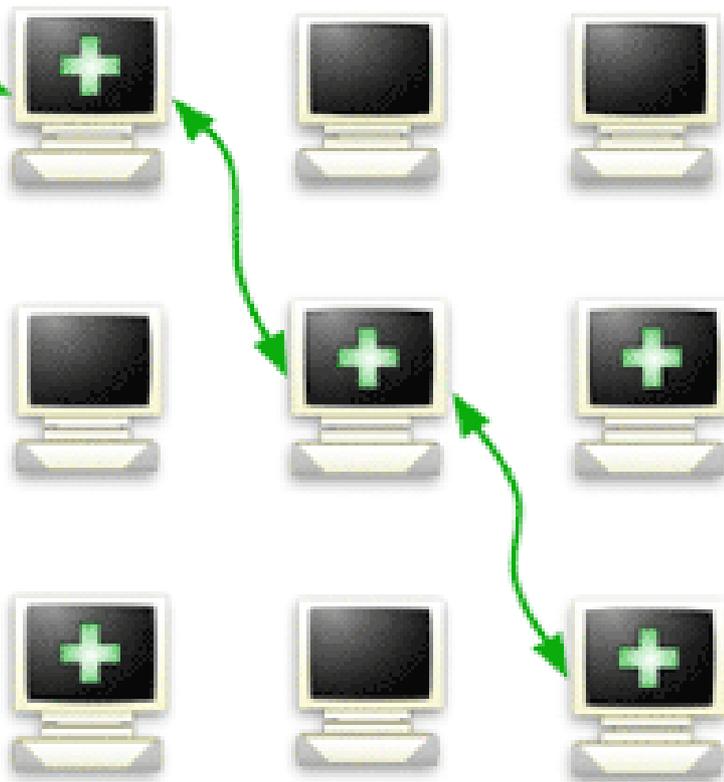
How Tor Works: 2



Alice



Step 2: Alice's Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.



Dave

Jane

Bob

E How Tor Works: 3

-  Tor node
-  unencrypted link
-  encrypted link

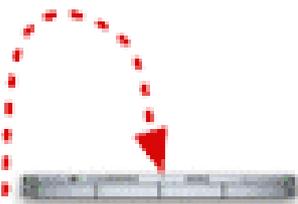
Alice



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



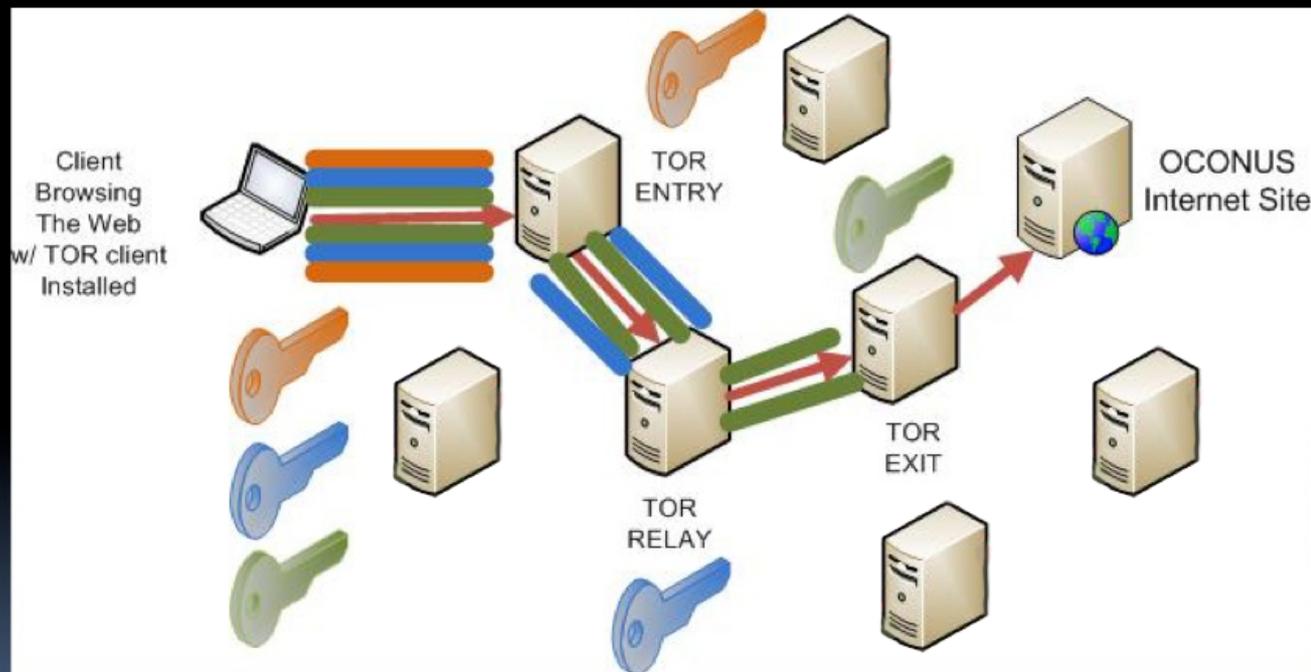
Jane



Bob



(U) What is TOR?



Download Tor-Browser

- ▶ Firefox + Tor + NoScript + HTTPS-Everywhere
- ▶ Download unter: <https://www.torproject.org/>
- ▶ Einstellungsoptionen:

About Tor - Tor Browser

About Tor

Tor Browser Search with Disconnect or enter address

Search

Security Level : Standard

Tor Browser 8.5.1
[View Changelog](#)

Explore. Privately.

You're ready for the world's most private browsing experience.

 Search with DuckDuckGo →

Keep Tor strong. [Donate Now](#) »

Tails – ein OS für Tor

- ▶ The Amnesic Incognito Live System (Tails)
- ▶ Live-Linux-DVD / USB
- ▶ Anonymität als erstes Designprinzip
- ▶ Viele Tools
 - ▷ Pidgin
 - ▷ Electrum
 - ▷ MAT
 - ▷ KeePassX

Weiterführende Literatur

- ▶ 10-teilige Artikelserie von Mike Kuketz:
<https://kuketz-blog.de/> (Suche „Firefox-Kompendium“)
- ▶ Disconnect!- und Tails-Broschüre von Çapulcu
<https://capulcu.blackblogs.org/>

– Ende –