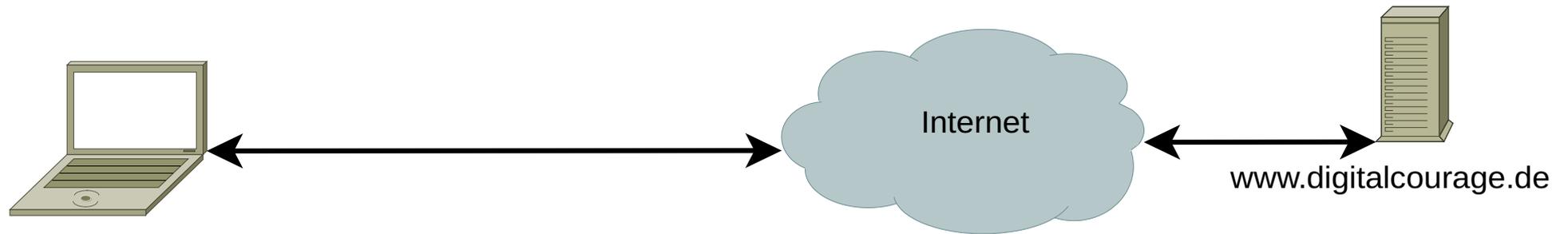
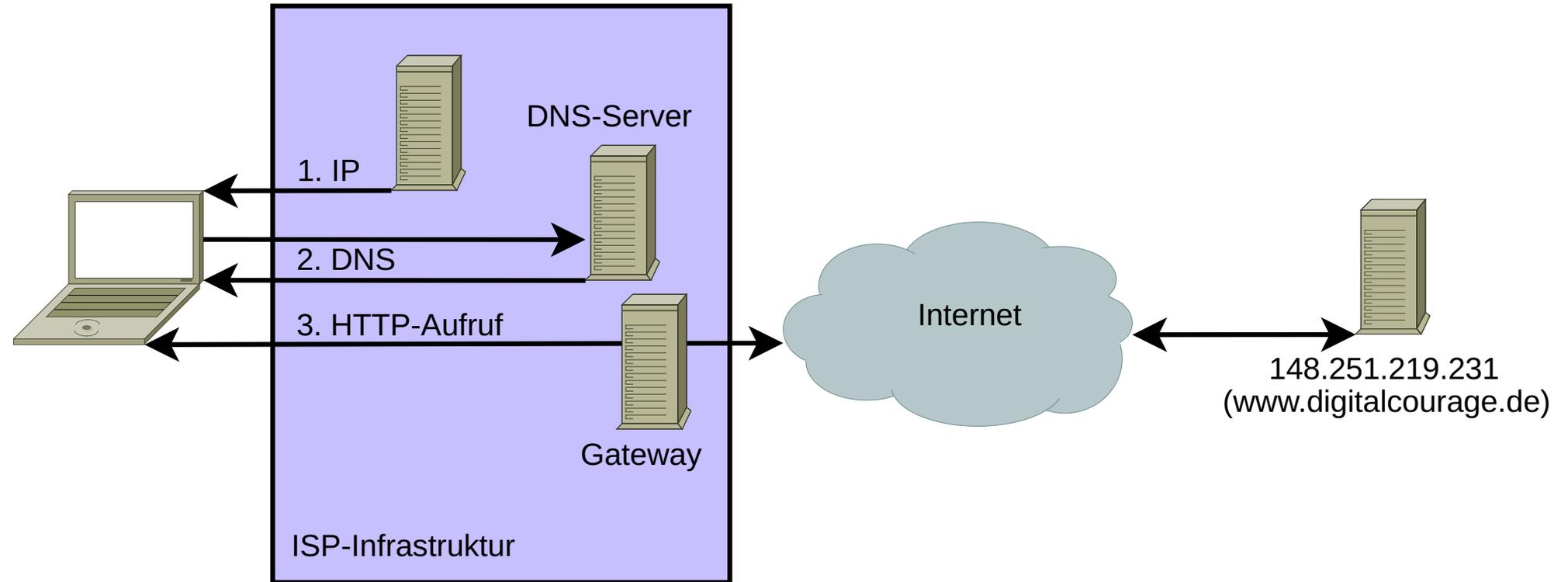


Spurenarmes und anonymes Surfen

Wie funktioniert das Web?



Und technisch?



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

- ▶ Beispiel: <https://www.spiegel.de/> (mit aktuellem Firefox)
- ▶ ca. 380 Anfragen, davon ca. 10 an deutsche Server des Spiegel; Anfragen an 65 externe Domains ...
- ▶ ca. 15 MB; 58 Cookies, 28 von Drittanbietern
- ▶ Ladezeit ca. 15–30 Sek. + Nachladen
weiteres Nachladen bei Interaktion und Scrollen

... 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, ...

VISUALIZATION

Graph

DATA

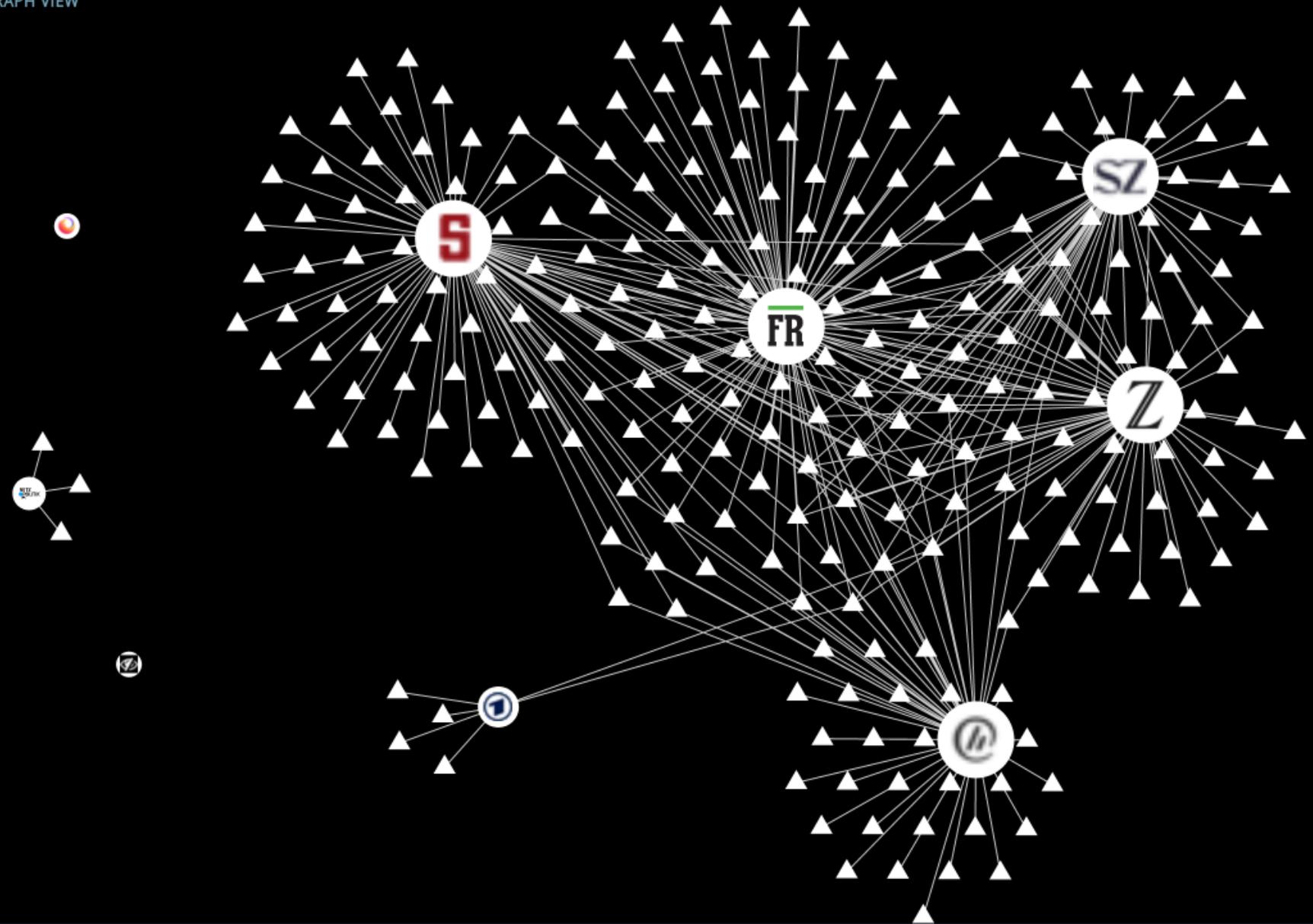
Save Data

Reset Data

Give Us Feedback

Recent Site

GRAPH VIEW



VISUALIZATION

 Graph

DATA

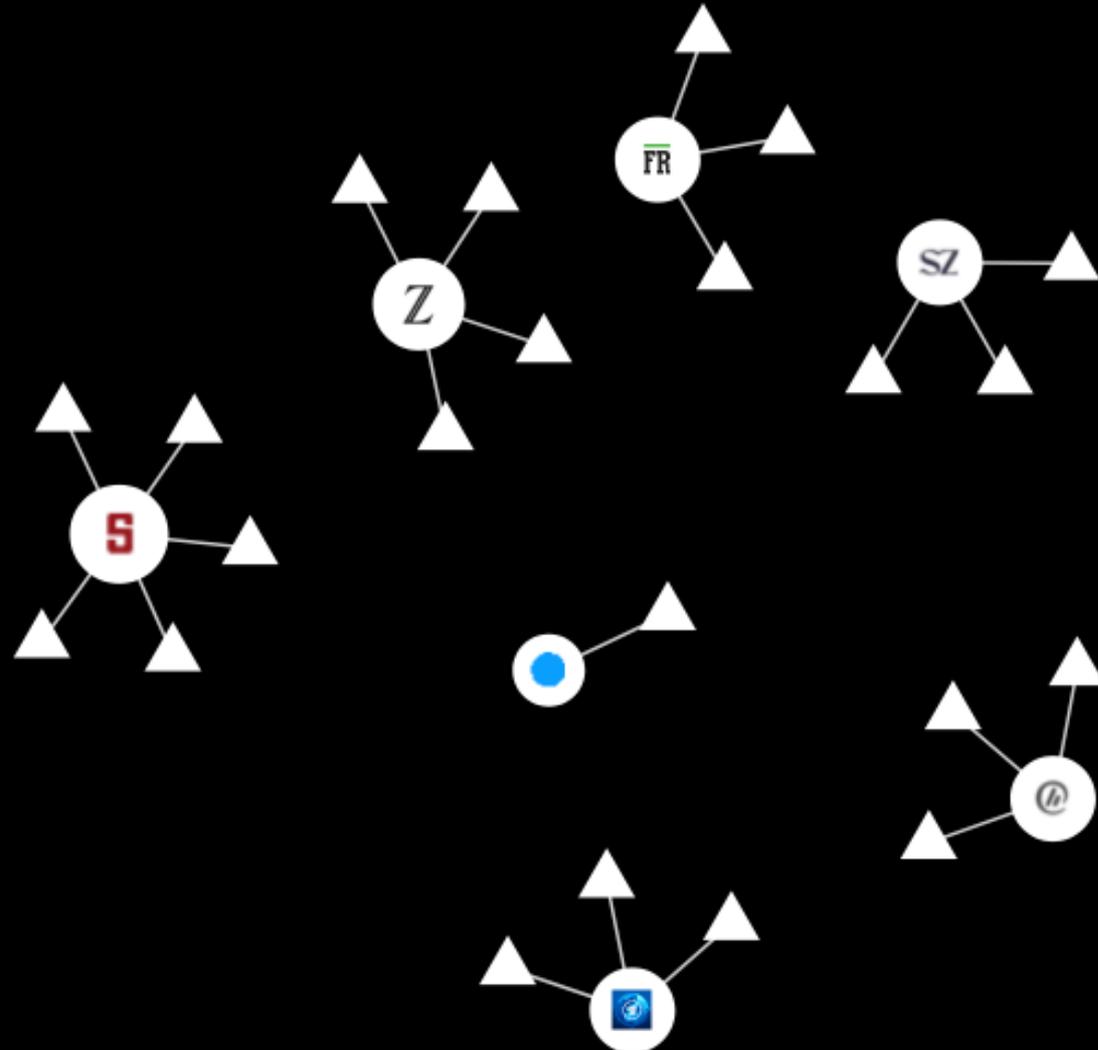
 Save Data

 Reset Data

 [Give Us Feedback](#)

Recent Site

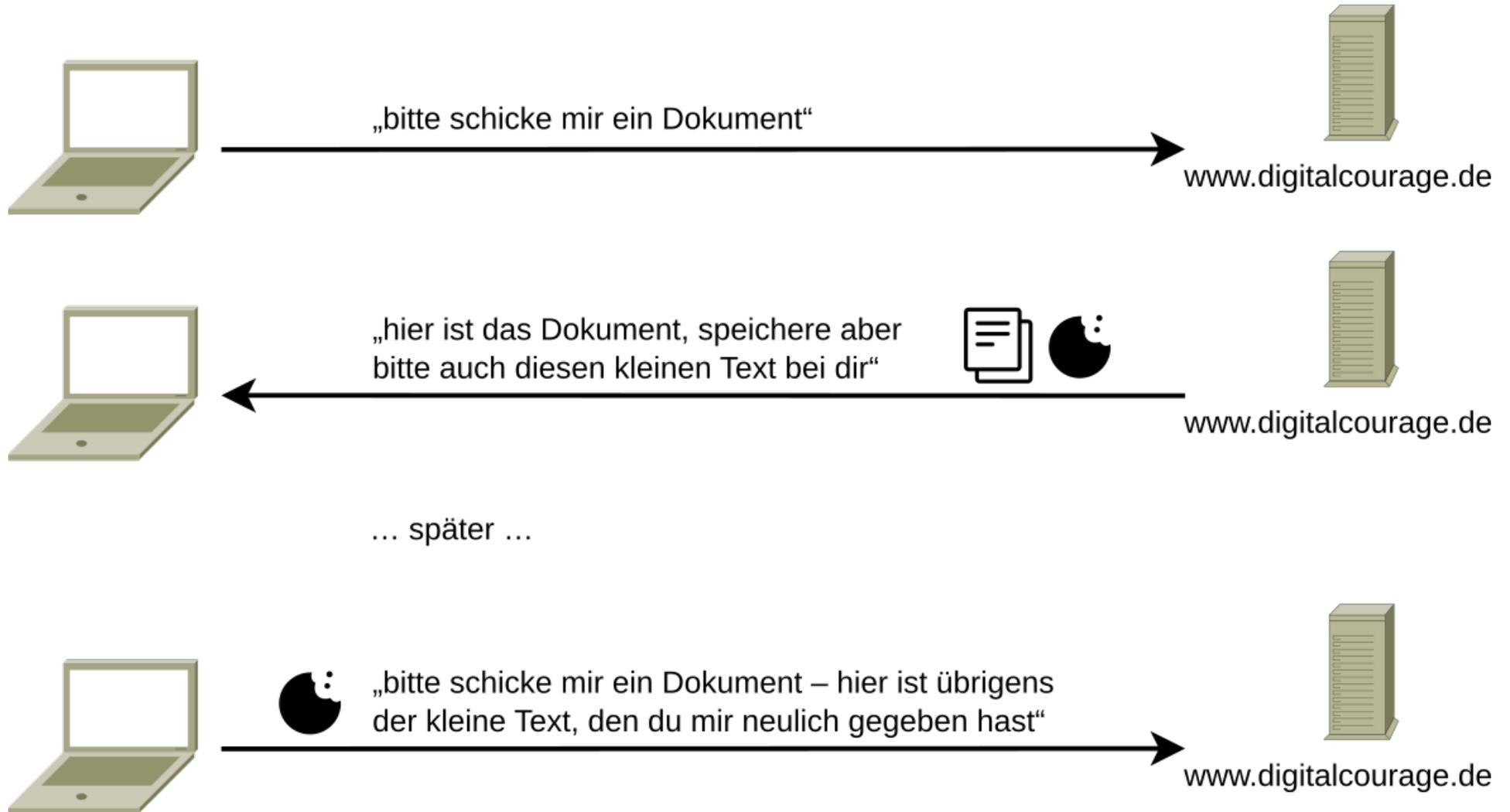
GRAPH VIEW



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://coveryourtracks.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

Tracking nachvollziehen

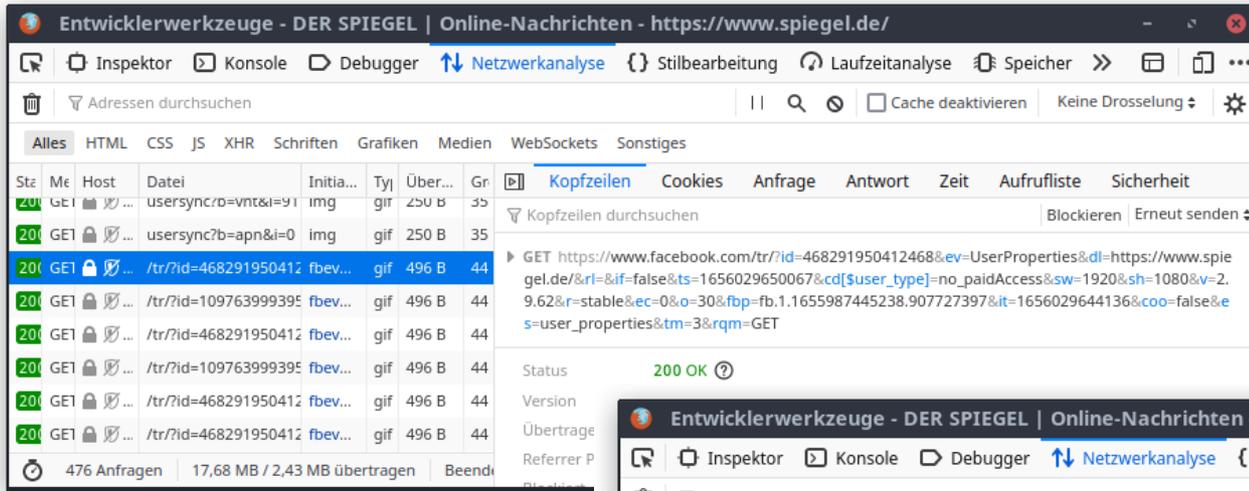
- ▶ Lightbeam: Entwicklung beendet, nur in Demos verwenden (letzter Stand wieder verfügbar gemacht durch Digitalcourage-AG Selbstverteidigung)
- ▶ Web-Entwicklungswerkzeuge in Firefox:
Menü → Weitere Werkzeuge → Werkzeuge für ... (F12)
 - ▷ Reiter Netzwerkanalyse (Umschalt + Strg + E)
 - ▷ Reiter Web-Speicher (Umschalt + F9)
 - Screenshots auf den nächsten zwei Folien
- ▶ Online-Tools wie Webbkoll
 - Screenshot auf der drittnächsten Folie

The screenshot shows the DER SPIEGEL website in a Mozilla Firefox browser. The developer tools network tab is open, displaying a list of network requests. The selected request is a GET request to a Facebook image, which is highlighted in blue. The request details are as follows:

Status	Metho...	Host	Datei	Initiator	Typ	Übertragen	Größe	0 ms
200	GET	usersync.g...	usersync?b=apn&i=0	img	gif	250 B	35 B	48 ms
200	GET	usersync.g...	usersync?b=apn&i=0	img	gif	250 B	35 B	50 ms
200	GET	www.faceb...	/tr?id=468291950412468&ev=UserProperties&dl=f	fbevents.js:24 (i...	gif	496 B	44 B	18 ms
200	GET	www.faceb...	/tr?id=109763999395282&ev=PageView&dl=https://	fbevents.js:24 (i...	gif	496 B	44 B	20 ms
200	GET	www.facebook.com (157.240.210.35:443)	https://	fbevents.js:24 (i...	gif	496 B	44 B	20 ms
200	GET	www.faceb...	/tr?id=109763999395282&ev=ViewHomePage&dl=	fbevents.js:24 (i...	gif	496 B	44 B	20 ms
200	GET	www.faceb...	/tr?id=468291950412468&ev=ViewHomePage&dl=	fbevents.js:24 (i...	gif	496 B	44 B	20 ms
200	GET	www.faceb...	/tr?id=468291950412468&ev=Microdata&dl=https://	fbevents.js:24 (i...	gif	496 B	44 B	19 ms

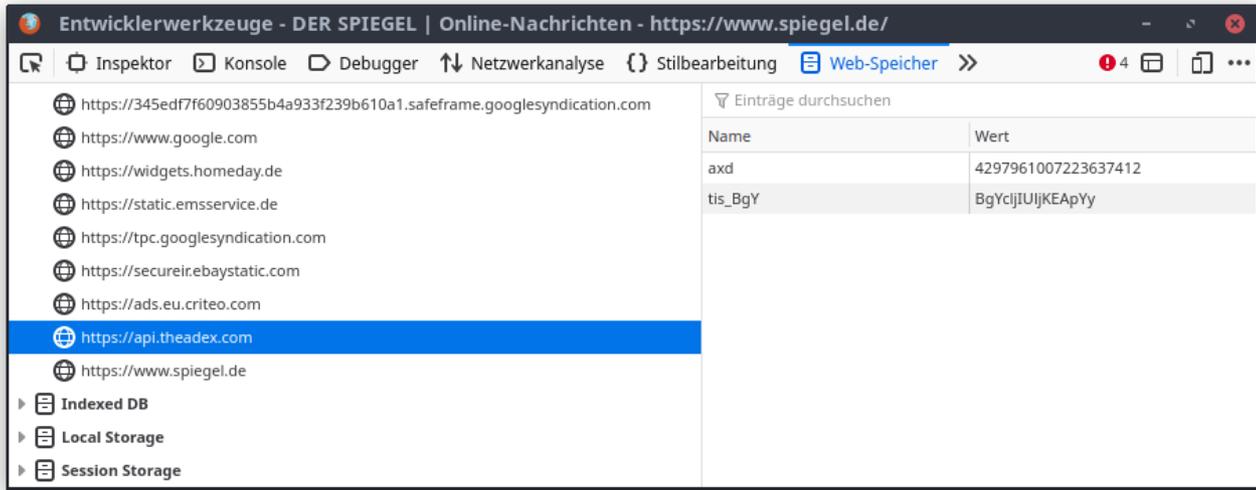
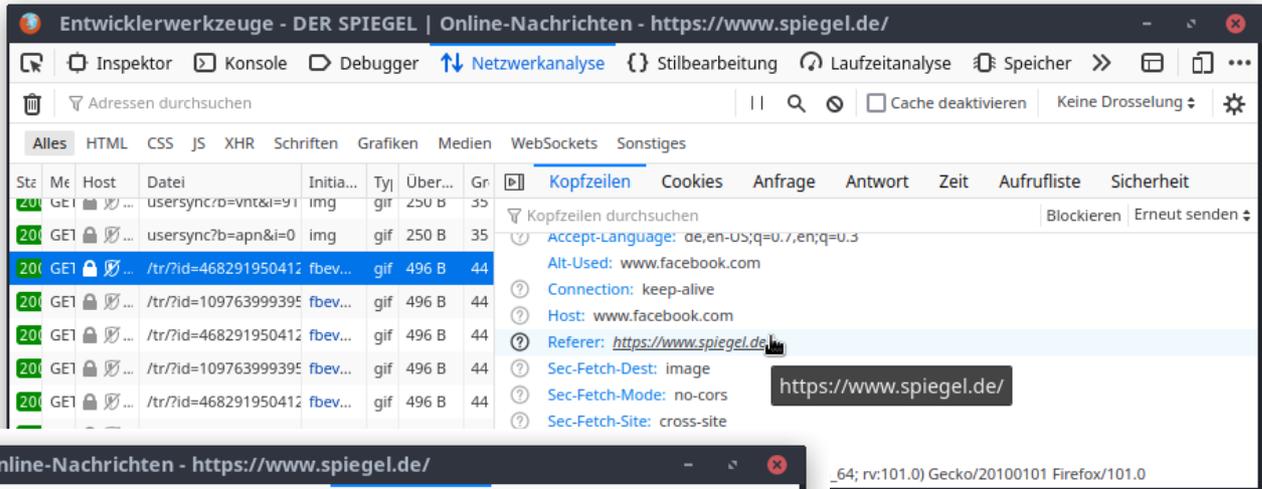
The browser's status bar at the bottom of the developer tools shows: 473 Anfragen | 17,68 MB / 2,43 MB übertragen | Beendet: 1,94 min | DOMContentLoaded: 1,99 s | load: 4,36 s

Abruf eines Bildes von Facebook als Teil der Startseite von spiegel.de



das Facebook-Bild ist sehr klein, die Adresse komplex → wahrscheinlich ein unsichtbares Pixel mit User-Kennung in der Adresse

via HTTP-Referrer wird Facebook mitgeteilt, dass das Bild auf spiegel.de eingebettet ist



_64; rv:101.0) Gecko/20100101 Firefox/101.0

diverse Websites (hier: „theadex“) hinterlassen Cookies mit Kennungen nach Besuch von spiegel.de

Websites prüfen mit Webbkoll



Überprüfe Deine Webseite!

bielefeld.de

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.

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

Feedback? Fragen? info@dataskydd.net

Twitter: [@dataskyddnet](#)

Wie einzigartig bin ich im Web? Browser-Fingerabdruck testen



See how trackers view your browser

[Learn](#)

[About](#)

HOW TO READ YOUR REPORT

You will see a summary of your overall tracking protection. The first section gives you a general idea of what your browser configuration is blocking (or not blocking). Below that is a list of specific browser characteristics in the format that a tracker would view them. We also provide descriptions of how they are incorporated into your fingerprint.

HOW CAN TRACKERS TRACK YOU?

Trackers use a variety of methods to identify and track users. Most often, this includes tracking cookies, but it can also include browser fingerprinting. Fingerprinting is a sneakier way to track users and makes it harder for users to regain control of their browsers. This report measures how easily trackers might be able to fingerprint your browser.

HOW CAN I USE MY RESULTS TO BE MORE ANONYMOUS?

Knowing how easily identifiable you are, or whether you are currently blocking trackers, can help you know what to do next to protect your privacy. While most trackers can be derailed by browser add-ons or built-in protection mechanisms, the sneakiest trackers have ways around even the strongest security. We recommend you use a tracker blocker like [Privacy Badger](#) or use a browser that has fingerprinting protection built in.

Here are your Cover Your Tracks results. They include an overview of how visible you are to trackers, with an index (and glossary) of all the metrics we measure below.

Our tests indicate that you have strong protection against Web tracking, though your software isn't checking for Do Not Track policies.

IS YOUR BROWSER:

Blocking tracking ads?	<u>Yes</u>
Blocking invisible trackers?	<u>Yes</u>
Protecting you from <u>fingerprinting</u> ?	<u>Your browser has a unique fingerprint</u>

Still wondering how fingerprinting works?

[LEARN MORE](#)

Note: because tracking techniques are complex, subtle, and constantly evolving, Cover Your Tracks does not measure all forms of tracking and protection.

Your Results

Your browser fingerprint **appears to be unique** among the 283,282 tested in the past 45 days.

Currently, we estimate that your browser has a fingerprint that conveys **at least 18.11 bits of identifying information.**

„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

Wahl des Browsers: Mozilla Firefox

- ▶ <https://www.mozilla.org/de/firefox/browsers/>
- ▶ Freie Software
- ▶ Für Linux, Windows, macOS verfügbar
 - ▷ auch für Android und iOS, aber dort andere Empfehlungen
- ▶ Der einzige große Browser, der nicht auf Googles Chromium-Projekt aufbaut



Wie kann ich mich in Firefox vor Tracking schützen?

▶ Browser-Einstellungen

- ▷ Seitenelemente blockieren: streng
 - seitenübergreifende Cookies, Inhalte zur Aktivitätenverfolgung überall blockiert
- ▷ Nur-HTTPS-Modus in allen Fenstern aktivieren
- ▷ „Do Not Track“-Information immer senden
- ▷ Cookies, Website-Daten beim Beenden löschen? Entscheidung
- ▷ Passwörter, Kreditkartendaten nicht speichern

▶ Suchmaschinen

- ▷ MetaGer.de, Startpage.com, Duckduckgo.com, Qwant.com

▶ Browser-Add-ons – neuerdings weniger erforderlich

▶ JavaScript ausschalten – eine interessante Option

Firefox-Add-ons (bis Juni 2022)

Zum Einstieg:

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

Die gestrichenen Erweiterungen sind durch das Firefox-Feature „Total Cookie Protection“ ([Version 101](#), Juni 2022) und durch den allgemeinen Trend zu HTTPS weniger wichtig geworden

Firefox-Add-ons (bis Juni 2022)

Für Fortgeschrittene:

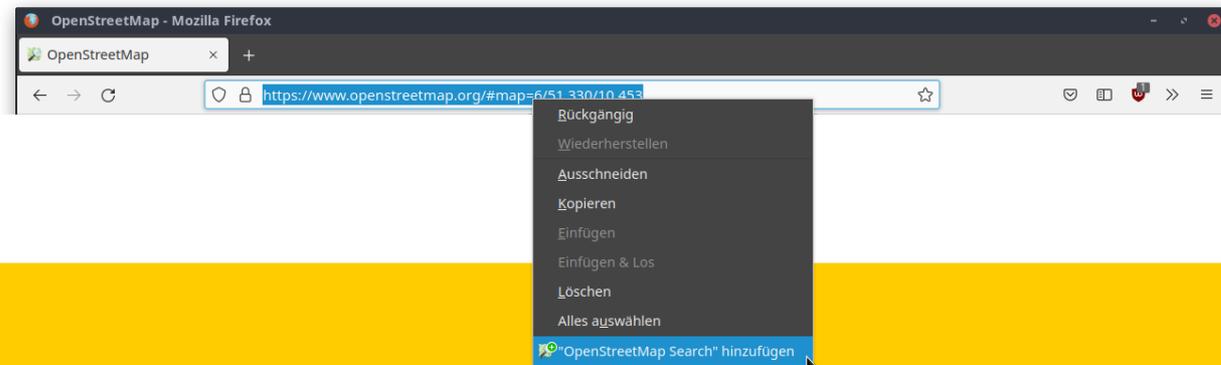
- ▶ ~~Referrer blockieren:~~ **Smart Referer**
- ▶ ~~JavaScript blockieren:~~ **NoScript**
- ▶ ~~Alle Drittanbieteranfragen blocken:~~ **uMatrix**

Der Referrer wird durch Firefox selbst seit [Version 93](#) (Oktober 2021) beschränkt, strengere Beschränkung mit Add-ons Smart Referer oder Toggle Referrer möglich

NoScript und uMatrix können durch erweiterte Funktionen von uBlock Origin weitgehend ersetzt werden

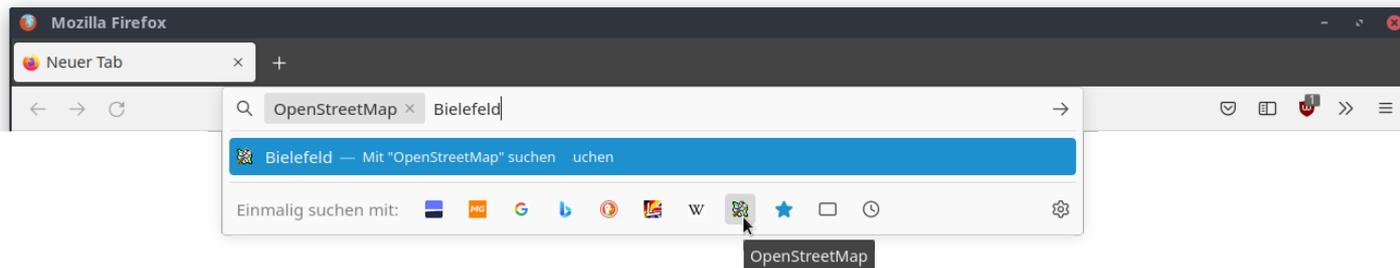
Exkurs zu Suchmaschinen: Google sollte nicht alles wissen!

- ▶ Eine von vielen Alternativen: **MetaGer.de** 
 - ▷ Wird vom SUMA-EV aus Hannover betrieben
 - ▷ eigener Suchindex + Ergebnisse verschiedener Suchmaschinen
 - ▷ Freie Software und datensparsam
 - ▷ Kann als neue Standard-Suchmaschine eingerichtet werden
- ▶ weitere: Startpage.com, DuckDuckGo.com, Qwant.com, ...
 - ▷ Viele Websites können „Suchmaschinen“ werden, Beispiele: OpenStreetMap, Wörterbücher, ... jede Site mit einer Suchfunktion
 - ▷ Hinzufügen via Rechtsklick in Adressleiste oder mycroftproject.com

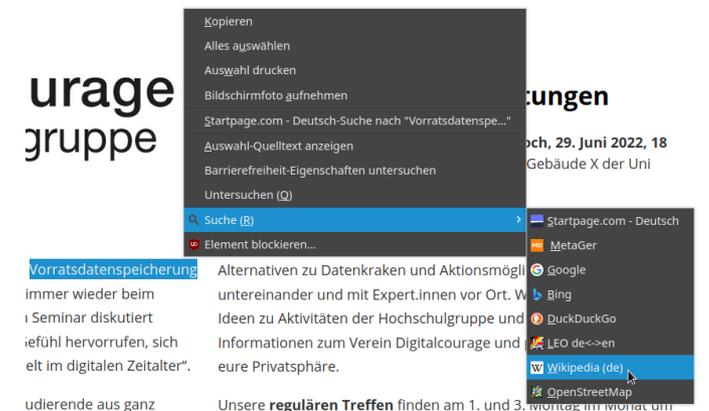


Eigene Suchmaschinen in Firefox nutzen

- ▶ wichtig zum Recherchieren mit Effizienz und Souveränität
- ▶ Suchphrase in Adressleiste eingeben, vor Gebrauch der Enter-Taste die passende Suchmaschine anklicken



- ▶ mit Add-on „Simple Context Search“: Suchwort in einer Seite markieren, Rechtsklick – Submenü zur Suche mit einer der eingestellten Suchmaschinen nutzen



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:

- ▷ Integrität
- ▷ Authentizität
- ▷ Vertraulichkeit

▶ Anonymität

- ▷ Nur teilweise vereinbar mit Authentizität!

▶ Resistenz gegenüber Zensur

Wie bekommen wir das?

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

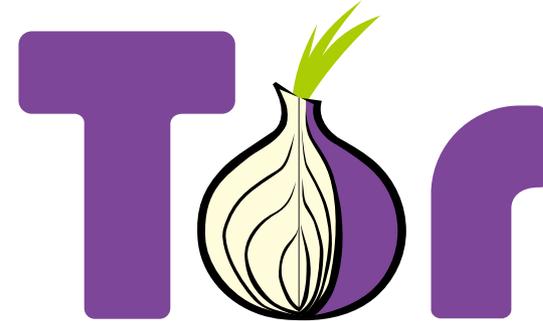
- ▷ mit Firefox → Tracking / Cookies reduzieren
- ▷ besser: Tor-Browser

- ▷ Tor-Browser

Anonym surfen mit dem Tor-Browser

Tor: The Onion Router

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



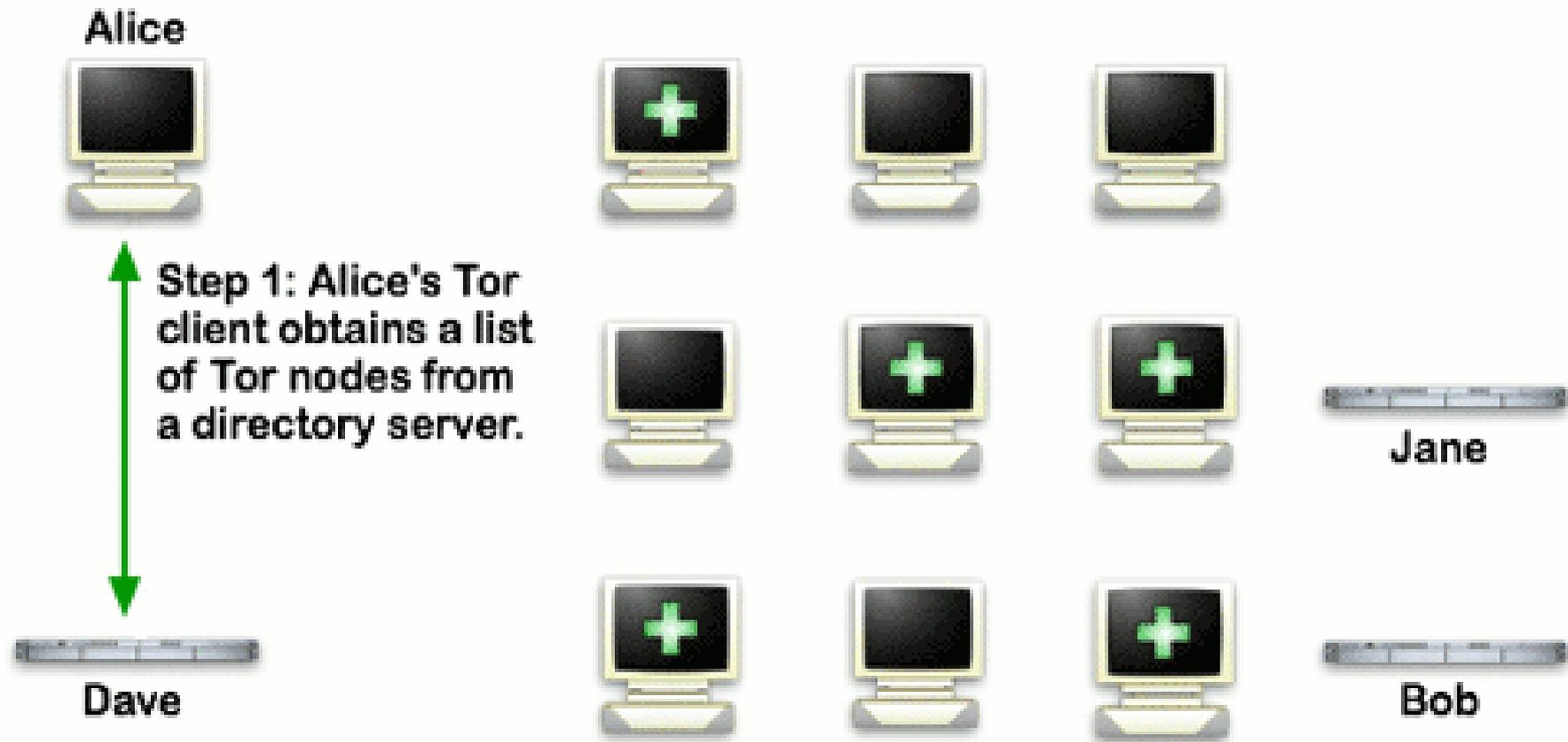
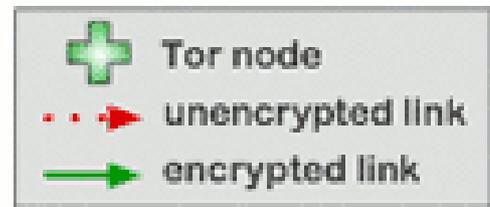
Vorteile

- ▶ quelloffen, freie Software
- ▶ anonymes Surfen

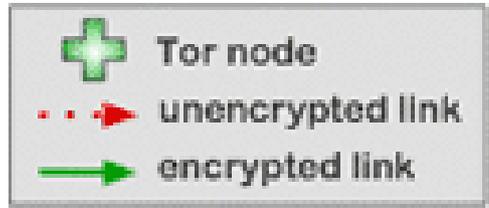
Nachteile

- ▶ 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.

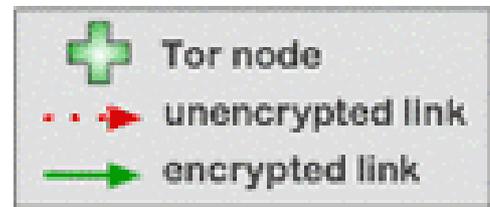


Dave

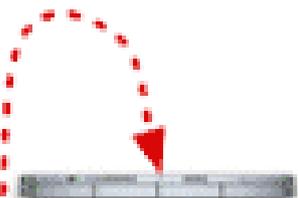
Jane

Bob

E How Tor Works: 3



Alice



Jane



Bob

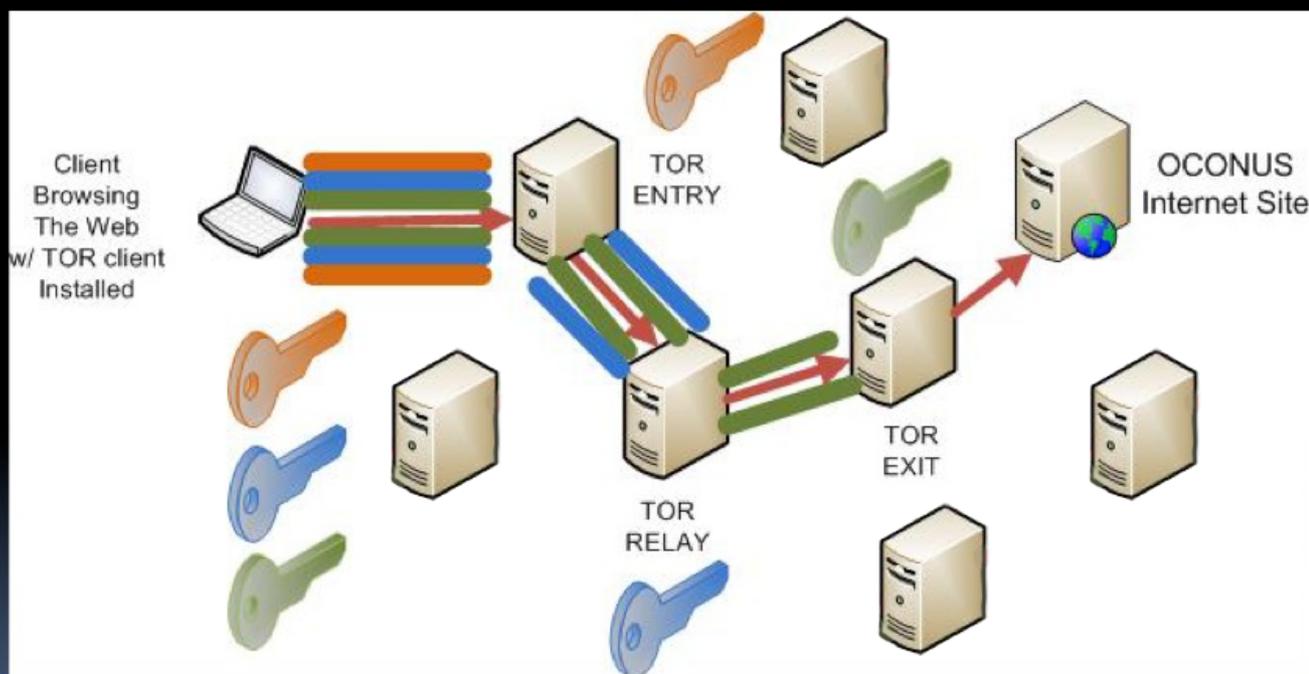
Step 3: If at a later time, the user visits another site, Alice's tor client selects a second random path. Again, **green links** are encrypted, **red links** are in the clear.



Dave



(U) What is TOR?



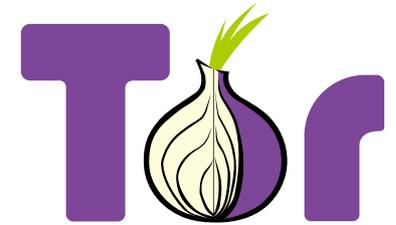
Wie nutze ich Tor?

- ▶ 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:

- ▷ **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>
- ▶ Big-Brother-Award 2021, „was mich wirklich wütend macht“
<https://bigbrotherawards.de/2021>

Vielen Dank fürs Mitmachen!

