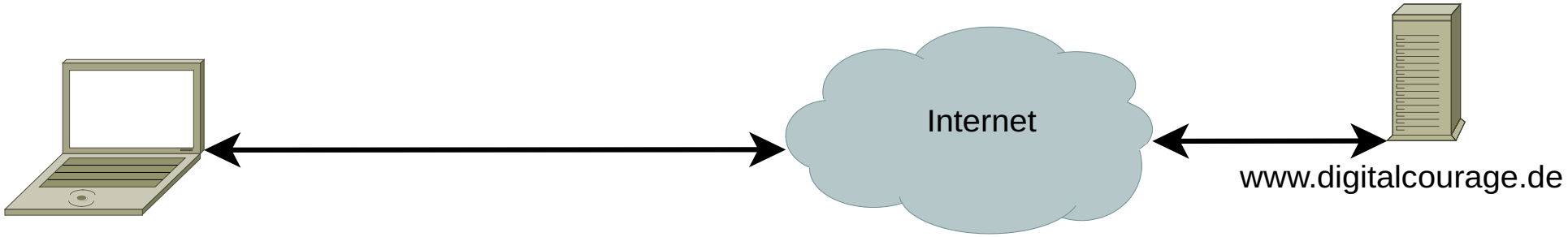
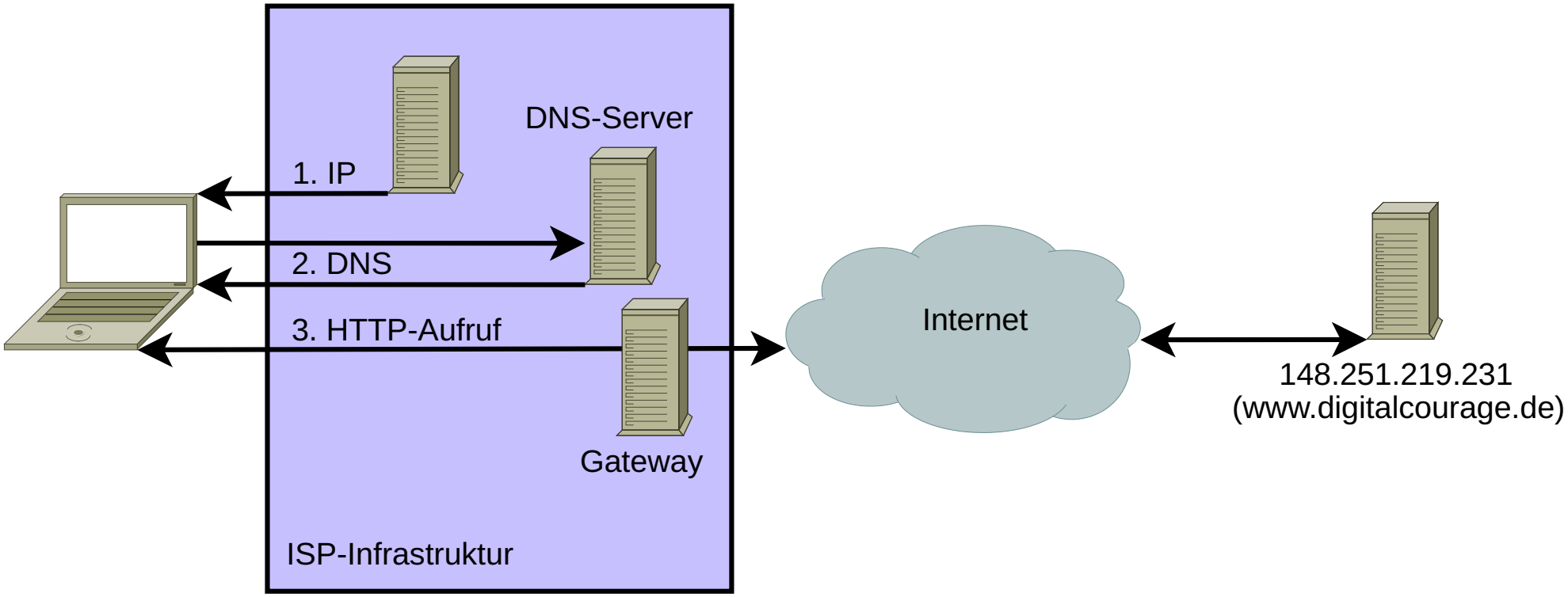
Spurenarmes und anonymes Surfen

digitalcourage
Hochschulgruppe

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.parsely.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, ...

Lightbeam for Firefox

VISUALIZATION

Graph

DATA

Save Data

Reset Data

Give Us Feedback

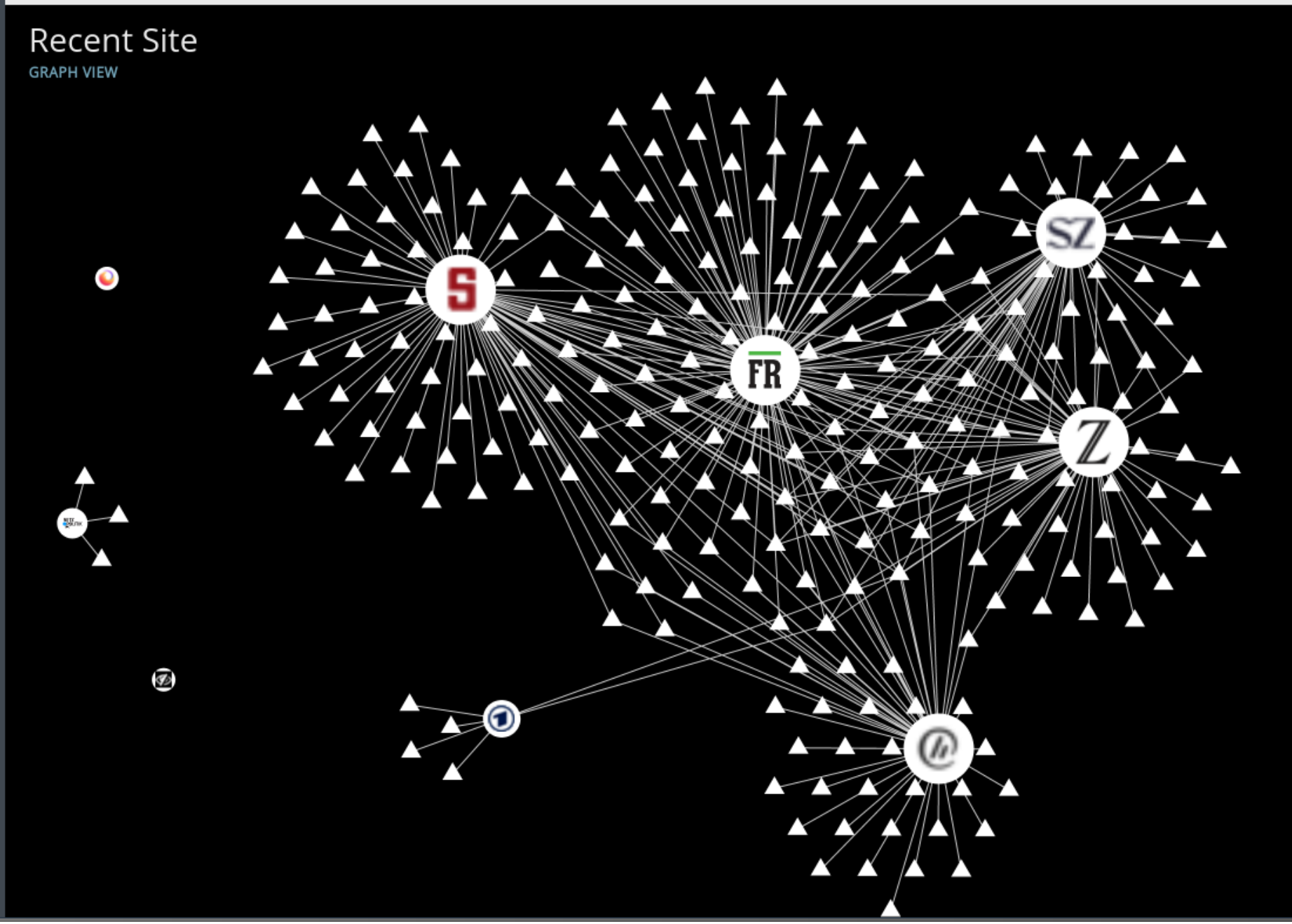
DATA GATHERED SINCE
DEC 12 2019

YOU HAVE VISITED
10 SITES

YOU HAVE CONNECTED WITH
247 THIRD PARTY SITES

Recent Site

GRAPH VIEW



Lightbeam for Firefox

VISUALIZATION

Graph

DATA

Save Data

Reset Data

Give Us Feedback

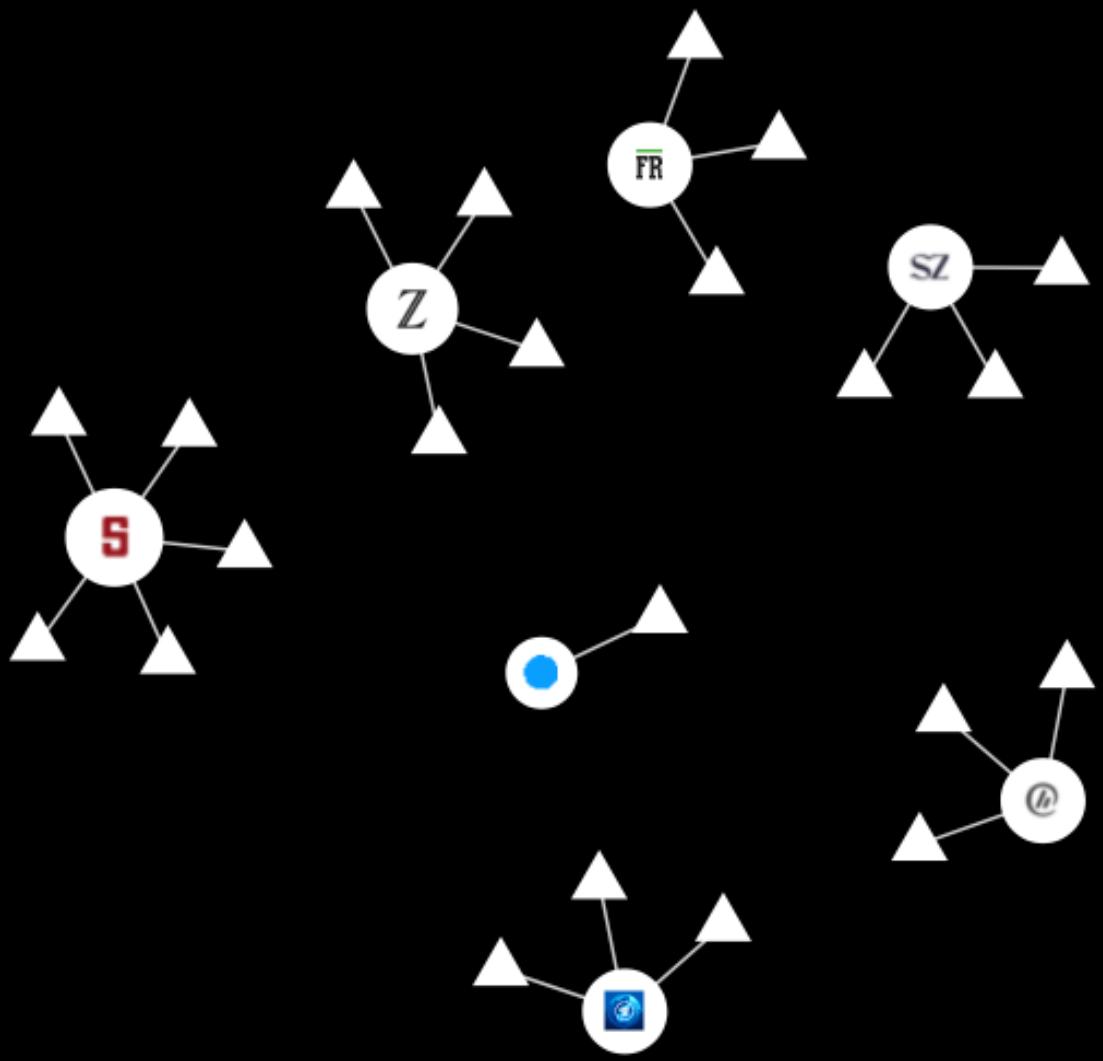
DATA GATHERED SINCE
DEC 12 2019

YOU HAVE VISITED
7 SITES

YOU HAVE CONNECTED WITH
22 THIRD PARTY SITES

Recent Site

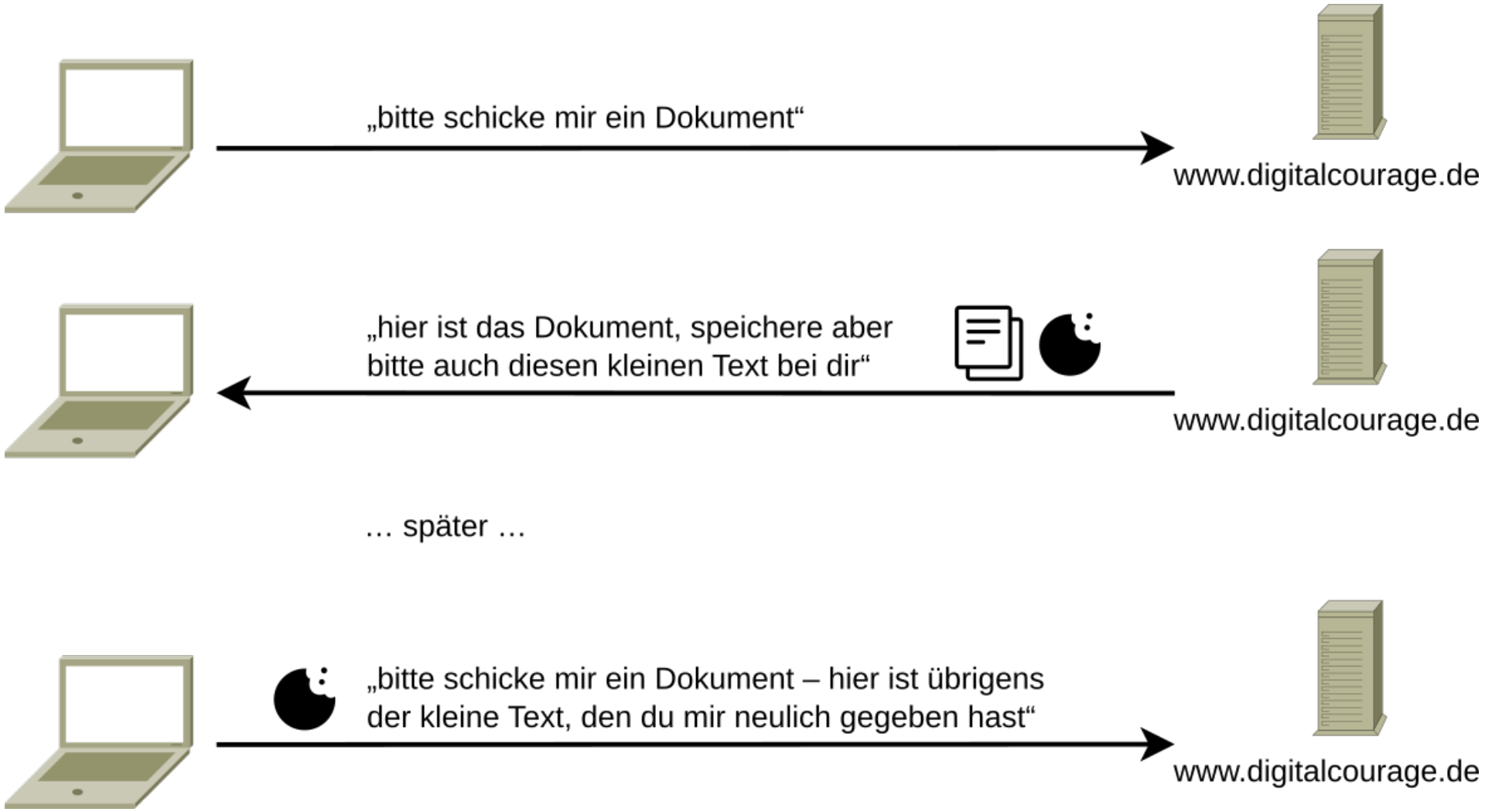
GRAPH VIEW



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?

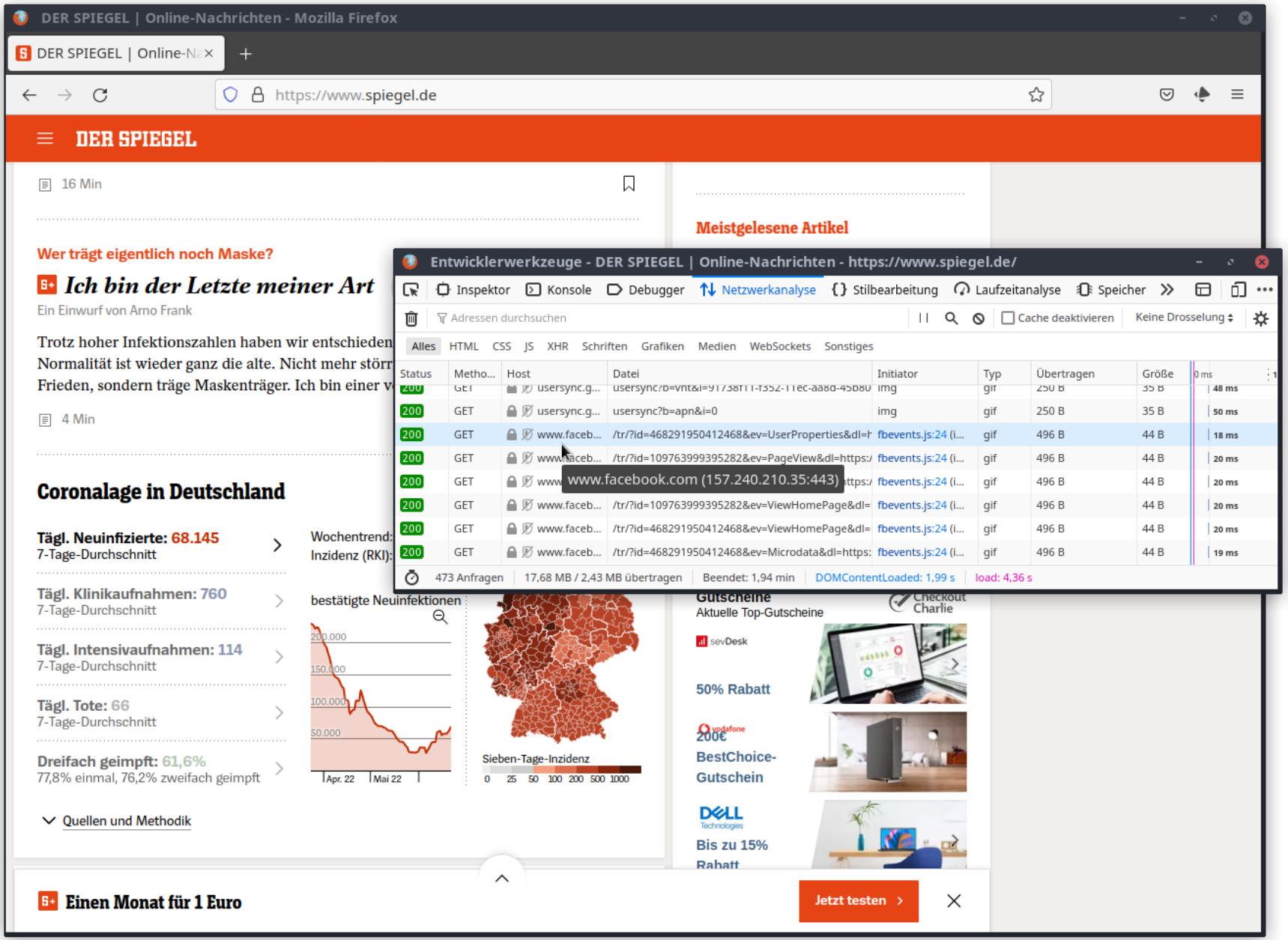
- sie lösen das Problem, dass HTTP „kein Gedächtnis“ hat
- Speichern von vorübergehenden Einstellungen:
  - bevorzugte Sprache, vielleicht auch regionale Präferenzen
  - meine Cookie-Präferenzen :-)
- Speichern, dass ich mich eingeloggt habe
- typisch: Zuweisung einer zufällig erzeugten, aber eindeutigen 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

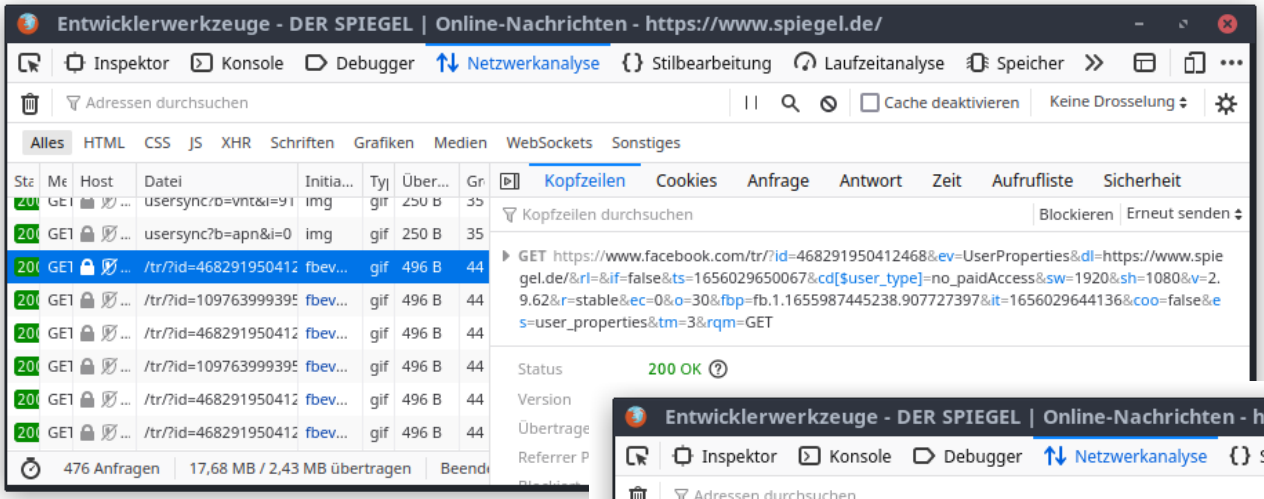
- Lightbeam: Entwicklung beendet, nur in Demos verwenden (letzter Stand wieder verfügbar gemacht durch Digitalcourage-AG Selbstverteidigung)
- Web-Entwicklungswerkzeuge in Firefox:
  Menü → Weitere Werkzeuge → Werkzeuge für … (F12)
  - Reiter Netzwerkanalyse (Umschalt + Strg + E)
  - Reiter Web-Speicher (Umschalt + F9)

  → Screenshots auf den nächsten zwei Folien
- Online-Tools wie Webbkoll

  → Screenshot auf der drittnächsten Folie

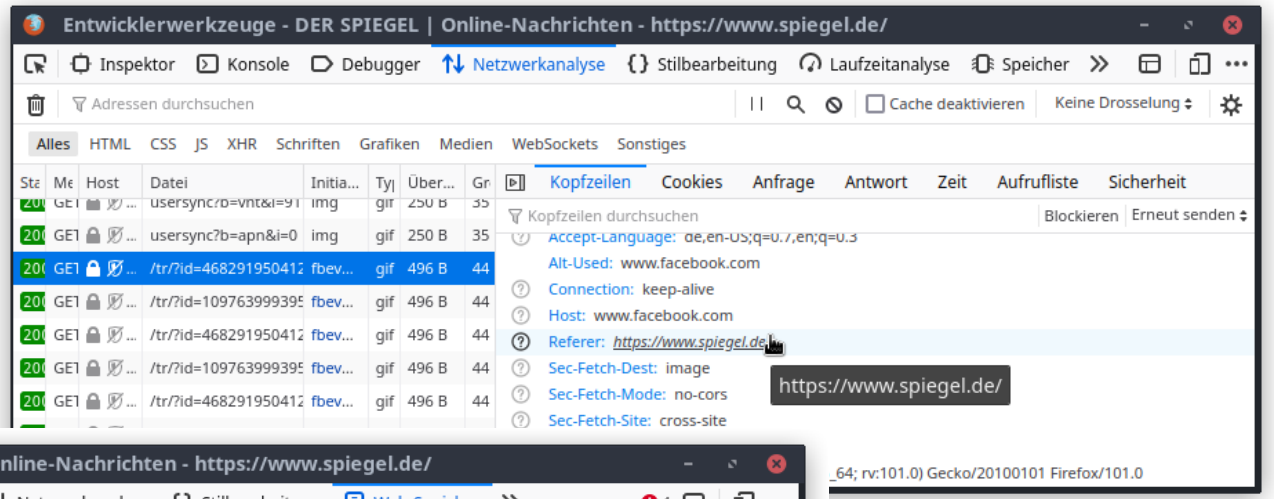


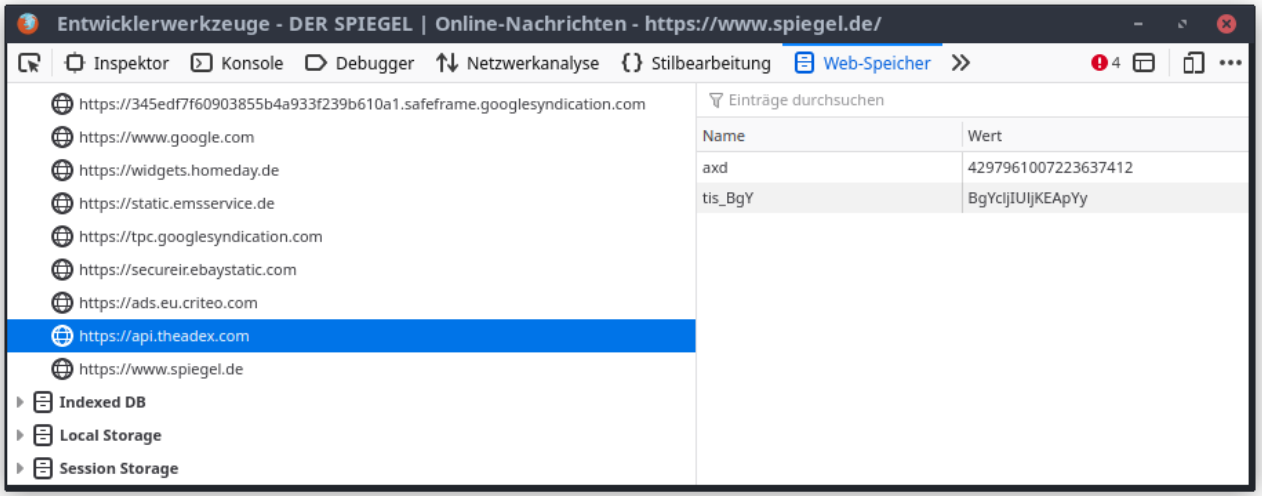
Abruf eines Bildes von Facebook als Teil der Startseite von spiegel.de



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

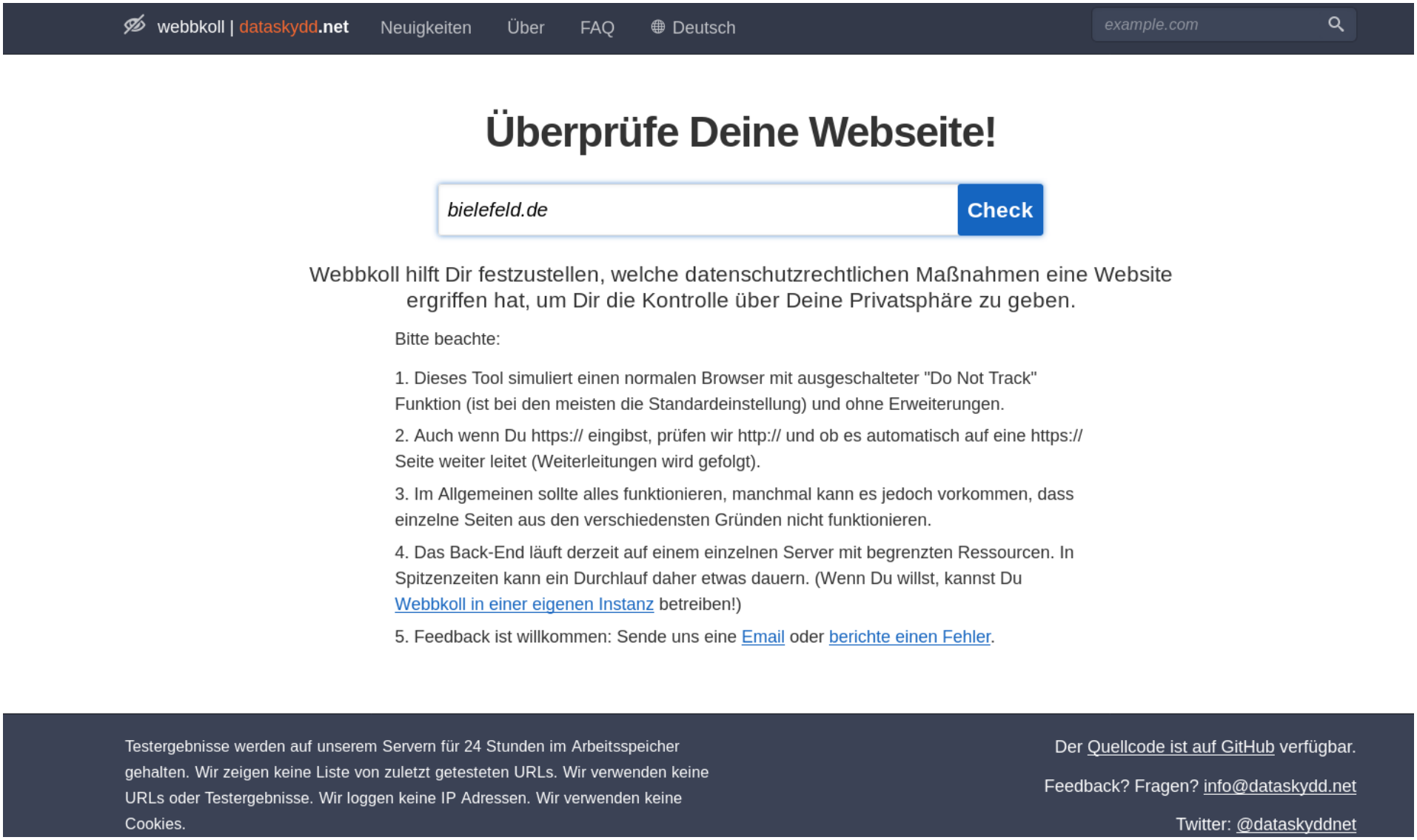
via HTTP-Referrer wird Facebook mitgeteilt, dass das Bild auf spiegel.de eingebettet ist



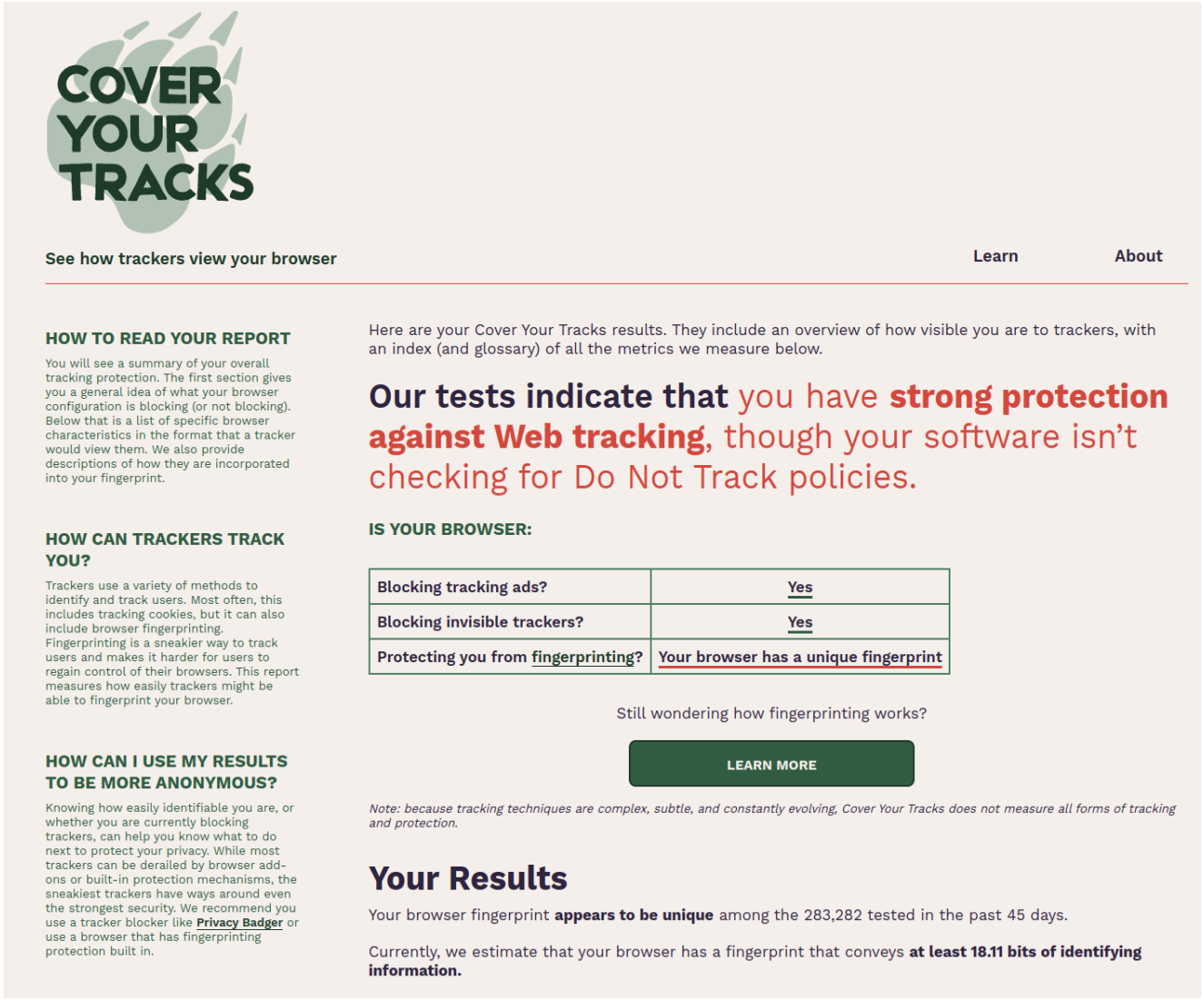


diverse Websites (hier: „theadex“) hinterlassen Cookies mit Kennungen nach Besuch von spiegel.de

Websites prüfen mit Webbkoll



Wie einzigartig bin ich im Web? Browser-Fingerabdruck testen



„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:

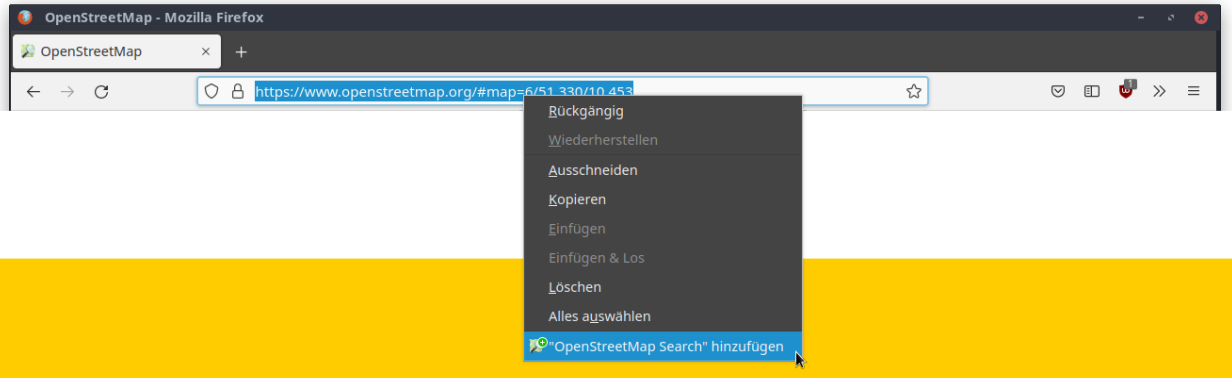
- ~~Referrer blockieren:~~ **~~Smart Referer~~**
- ~~JavaScript blockieren:~~ **~~NoScript~~**
- ~~Alle Drittanbieteranfragen blocken:~~ **~~uMatrix~~**

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

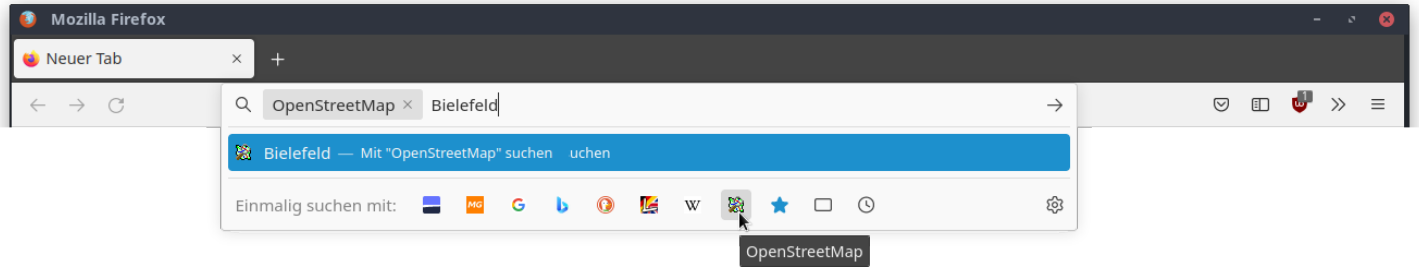
Exkurs zu Suchmaschinen: Google sollte nicht alles wissen!

- 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

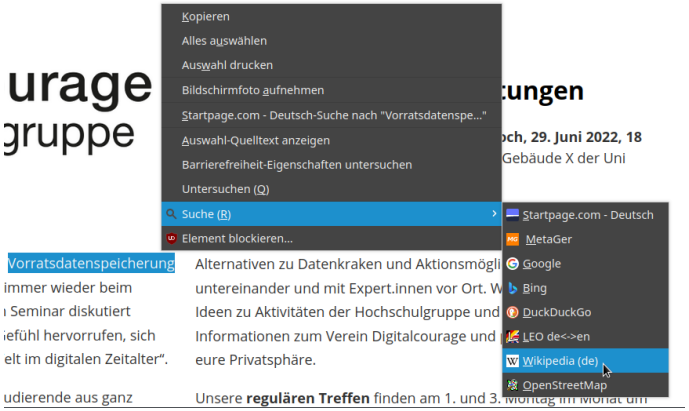


Eigene Suchmaschinen in Firefox nutzen

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

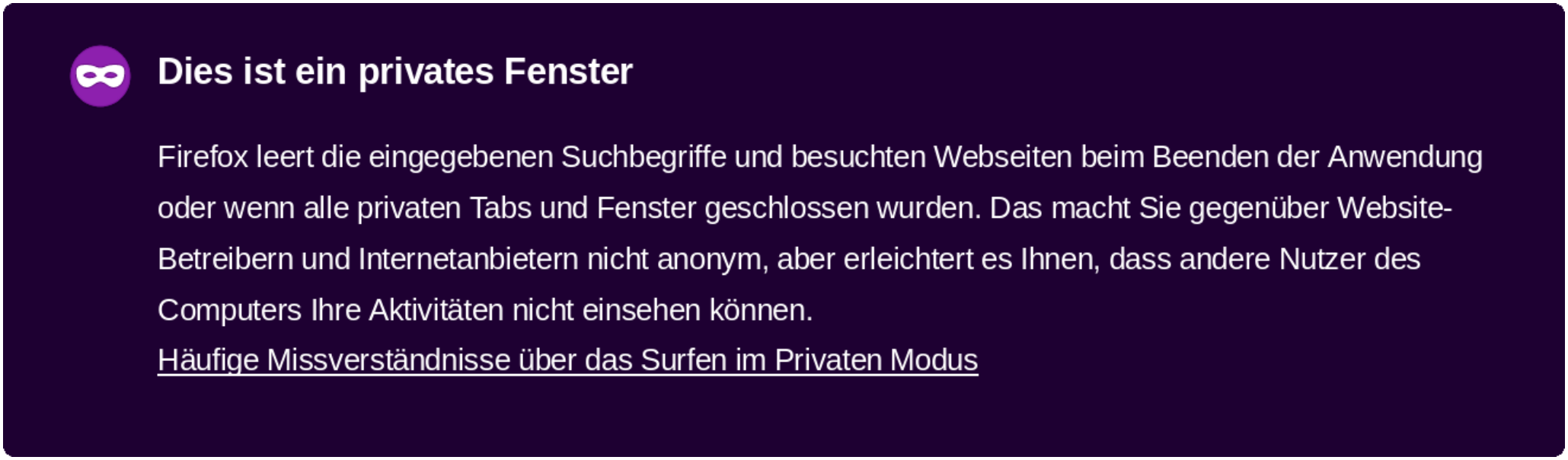


- mit Add-on „Simple Context Search“: Suchwort in einer Seite markieren, Rechtsklick – Submenü zur Suche mit einer der eingestellten Suchmaschinen nutzen



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**



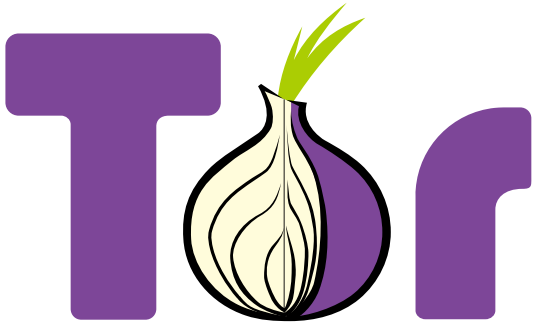
Sicheres Surfen mit Privatsphäre

Was wollen wir?	Wie bekommen wir das?
Sicherheit:	
▷ Integrität	▷ HTTPS
▷ Authentiziät	▷ HTTPS (Zertifikate)
▷ Vertraulichkeit	▷ HTTPS (Verschlüsselung)
Anonymität	
▷ Nur teilweise vereinbar mit Authentizität!	▷ mit Firefox → Tracking / Cookies reduzieren
	▷ besser: Tor-Browser
Resistenz gegenüber Zensur	▷ Tor-Browser

Anonym surfen mit dem Tor-Browser

Tor: The Onion Router

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



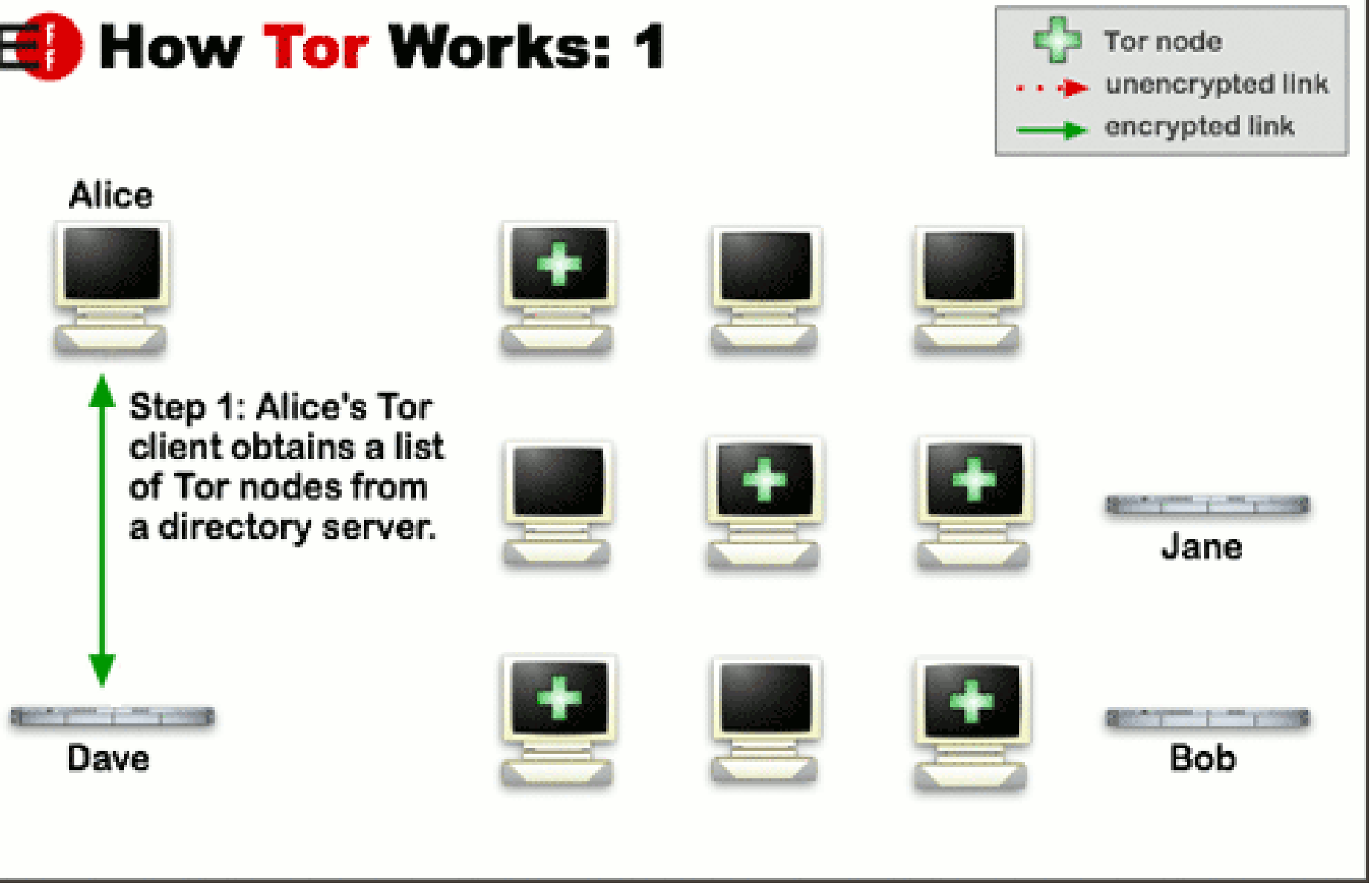
Vorteile

- quelloffen, freie Software
- anonymes Surfen

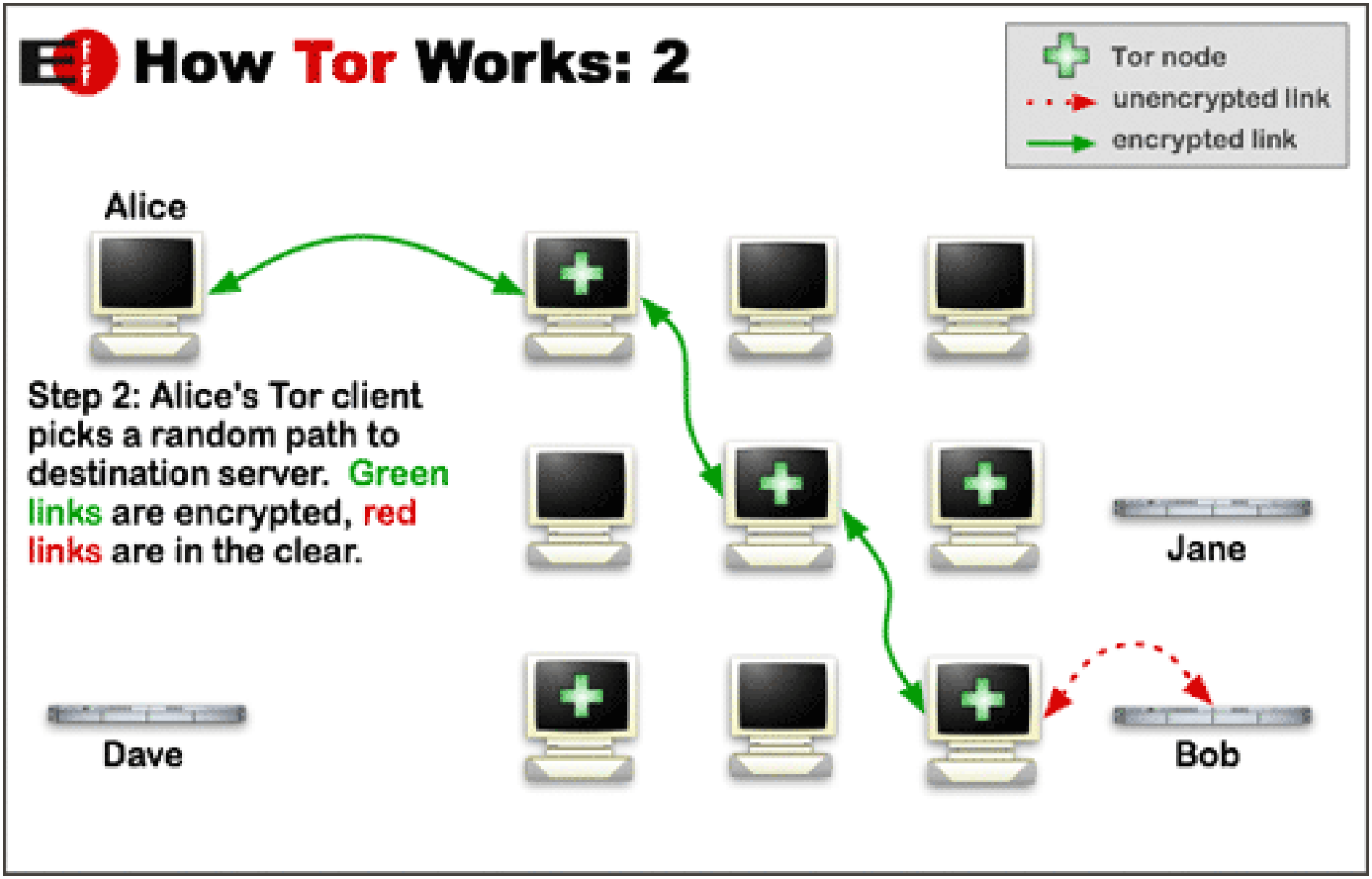
Nachteile

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

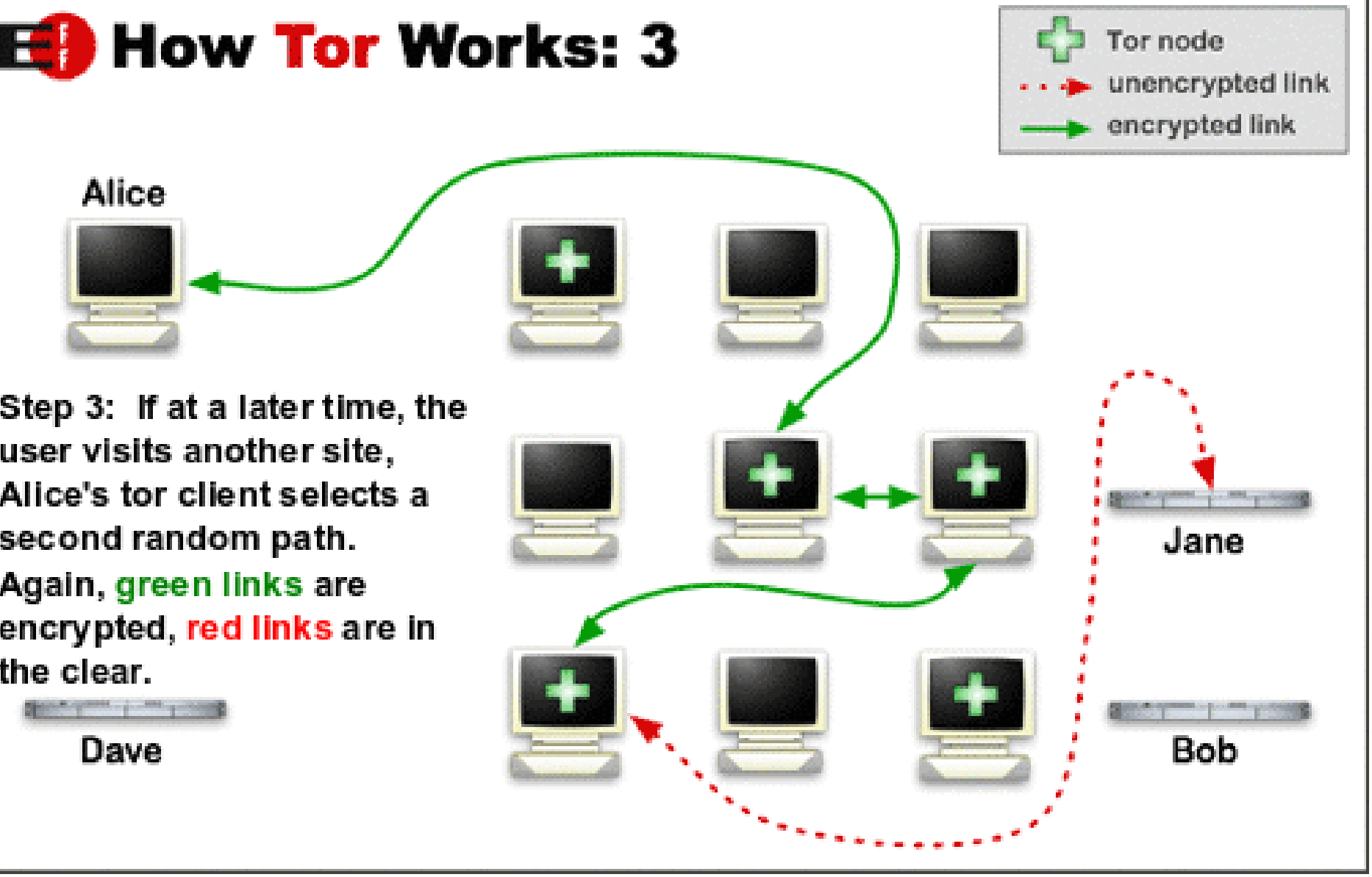
How Tor Works: 1



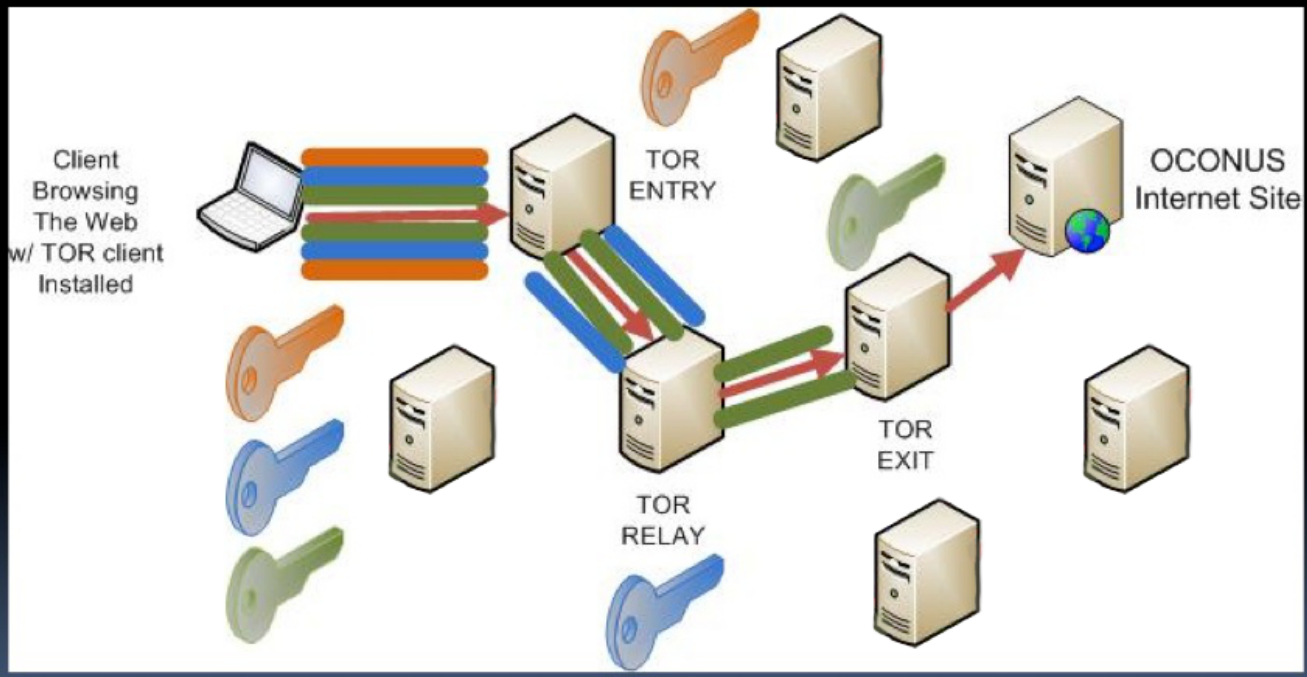
How Tor Works: 2



How Tor Works: 3



(U) What is TOR?

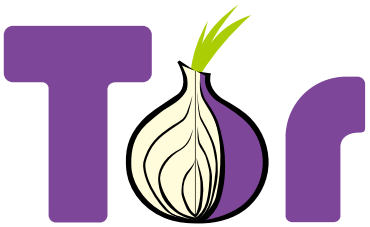


Wie nutze ich Tor?

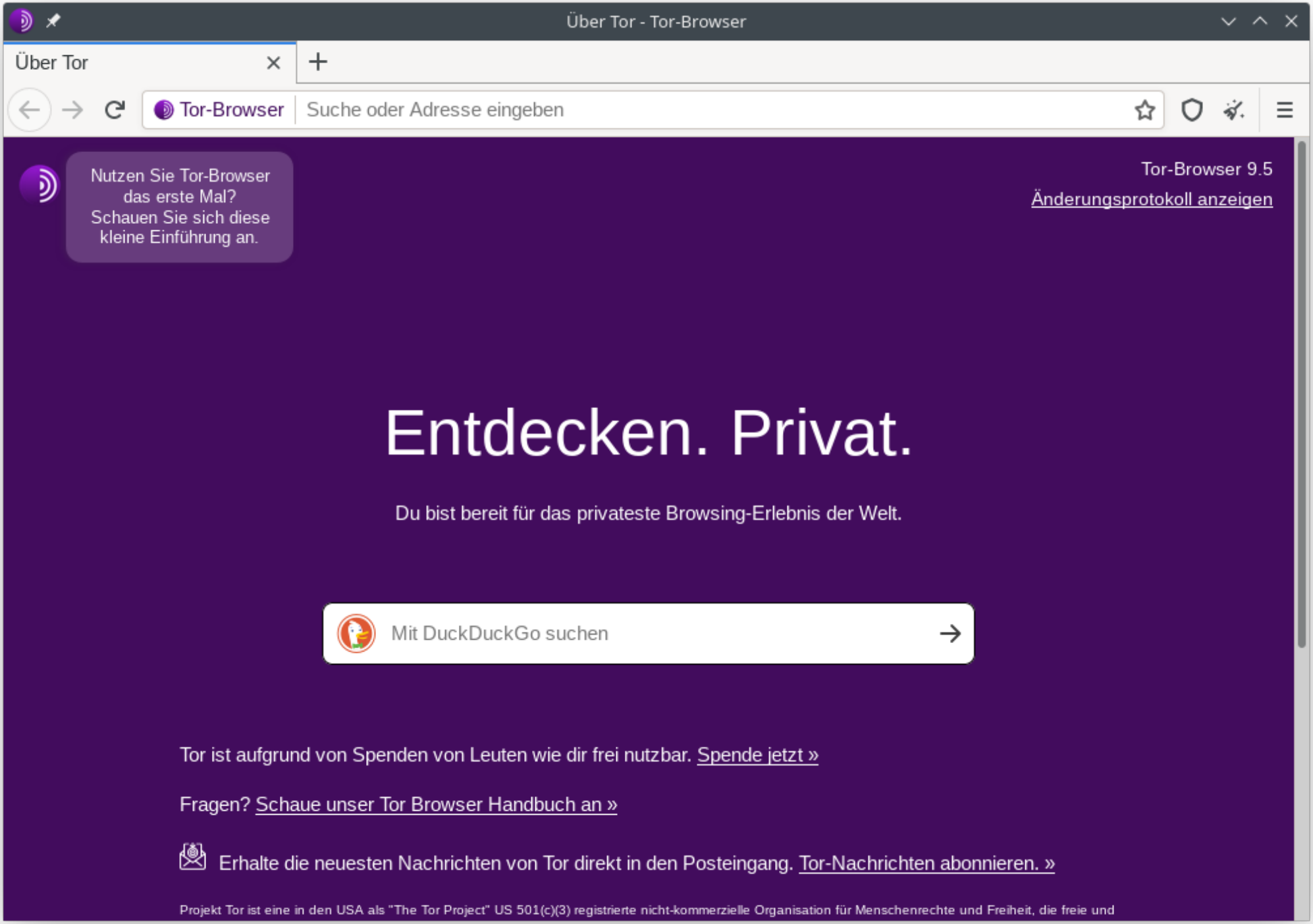
- Tor-Browser installieren
  - Modifizierter Firefox mit mehreren Addons (NoScript, HTTPS Everywhere, Torbutton und TorLauncher)
  - https://www.torproject.org/download/
- Hinweis zur Zielgruppe:
  - Nutzung ist vor allem bei exponierten Personen sinnvoll (Investigativjournalisten, innerhalb bestimmter 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



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!

(Bild: CC-BY-2.0: EFF)