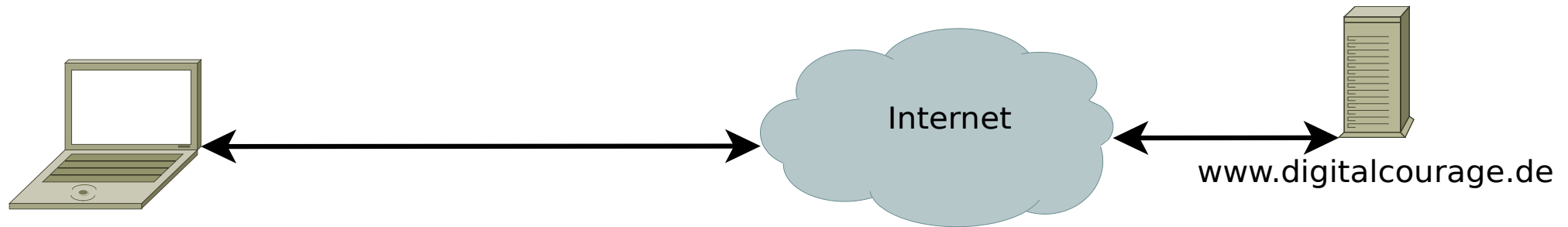


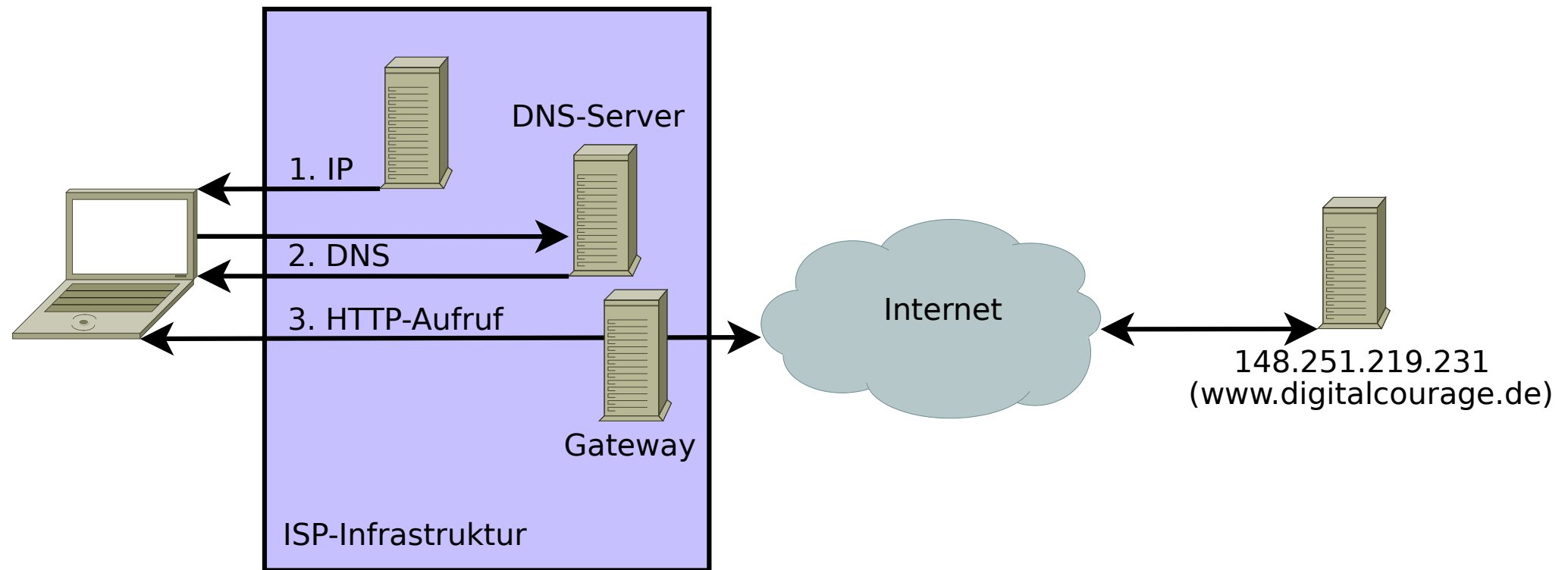
Sicher und anonym im World Wide Web



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. 490 Anfragen (nach 37 Sek.) an 94 externe Domains ...
- ▶ **www.spiegel.de**, **cdn.prod.www.spiegel.de**, **sams.spiegel.de**, **sats.spiegel.de**

... so schrecklich!

- ▶ Beispiel: **https://www.spiegel.de/**
- ▶ ca. 490 Anfragen (nach 37 Sek.) an 94 externe Domains ...
- ▶ **www.spiegel.de**, **cdn.prod.www.spiegel.de**, **sams.spiegel.de**, **sats.spiegel.de**
 - ▷ **www.spiegel.de** → Link11 GmbH (DE)
 - ▷ **cdn.prod.www.spiegel.de** → Level 3 Parent (USA)
 - ▷ **sams.spiegel.de** → Amazon (FR)
 - ▷ **sats.spiegel.de** → Amazon (IE)

... so schrecklich!

- ▶ adalliance.io, addition.com, adnxs.com, adobedtm.com, adrtx.net, adsafeprotected.com, adsrvr.org, amazon-adsystem.com, ampproject.org, atdmt.com, bidswitch.net, bing.com, casalemedia.com, cloudflare.com, cloudfront.net, conative.de, createjs.com, criteo.com, criteo.net, de.com, demdex.net, digitru.st, **doubleclick.net**, emetriq.de, emsservice.de, exactag.com, facebook.com, facebook.net, googleapis.com, **google.com**, **google.de**, **googlesyndication.com**, **googletagmanager.com**, **googletagservices.com**, imgix.net, imrworldwide.com, ioam.de, jsdelivr.net, krxn.net, mathtag.com, meetrics.net, mookie1.com, mxcdn.net, opecloud.com, openx.net, outbrain.com, privacy-mgmt.com, semasio.net, smartadserver.com, sparwelt.click, spiegel.de, technical-service.net, theadex.com, xplosion.de, yahoo.com, yieldlab.net

... so schrecklich!

- ▶ 8–15 MB; 51 Cookies, 21 von Drittanbietern
- ▶ Ladezeit ca. 25–37 Sek. + Nachladen ohne Interaktion und Scrollen

VISUALIZATION

 Graph

DATA

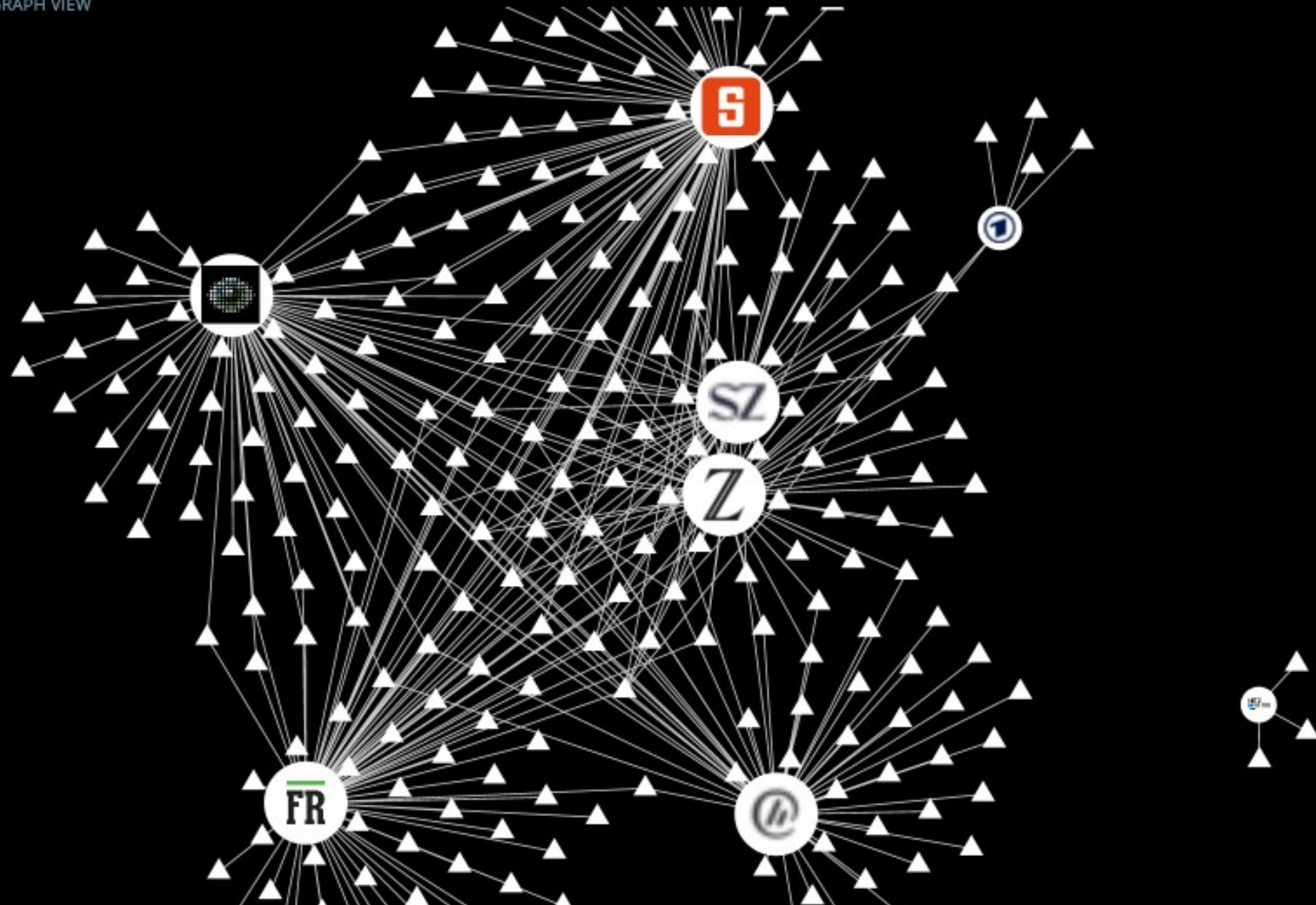
 Save Data

 Reset Data

 [Give Us Feedback](#)

Recent Site

GRAPH VIEW





VISUALIZATION

 Graph

DATA

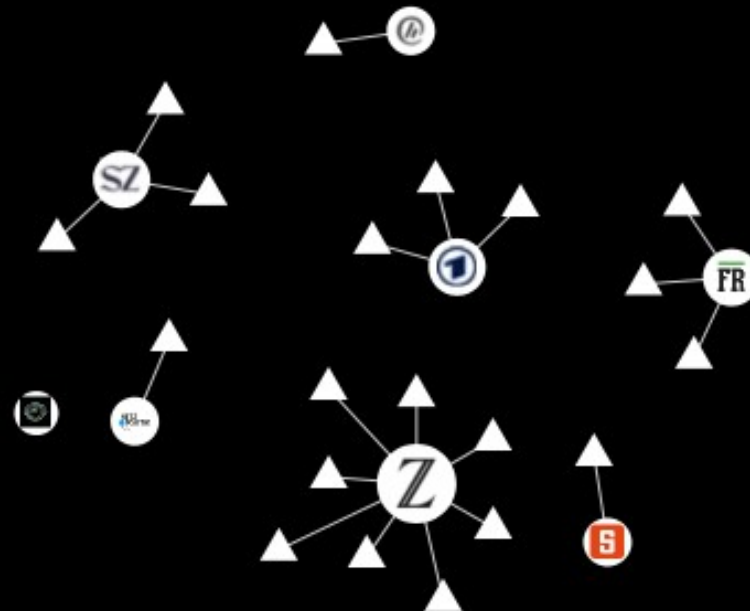
 Save Data

 Reset Data

 [Give Us Feedback](#)

Recent Site

GRAPH VIEW



VISUALIZATION

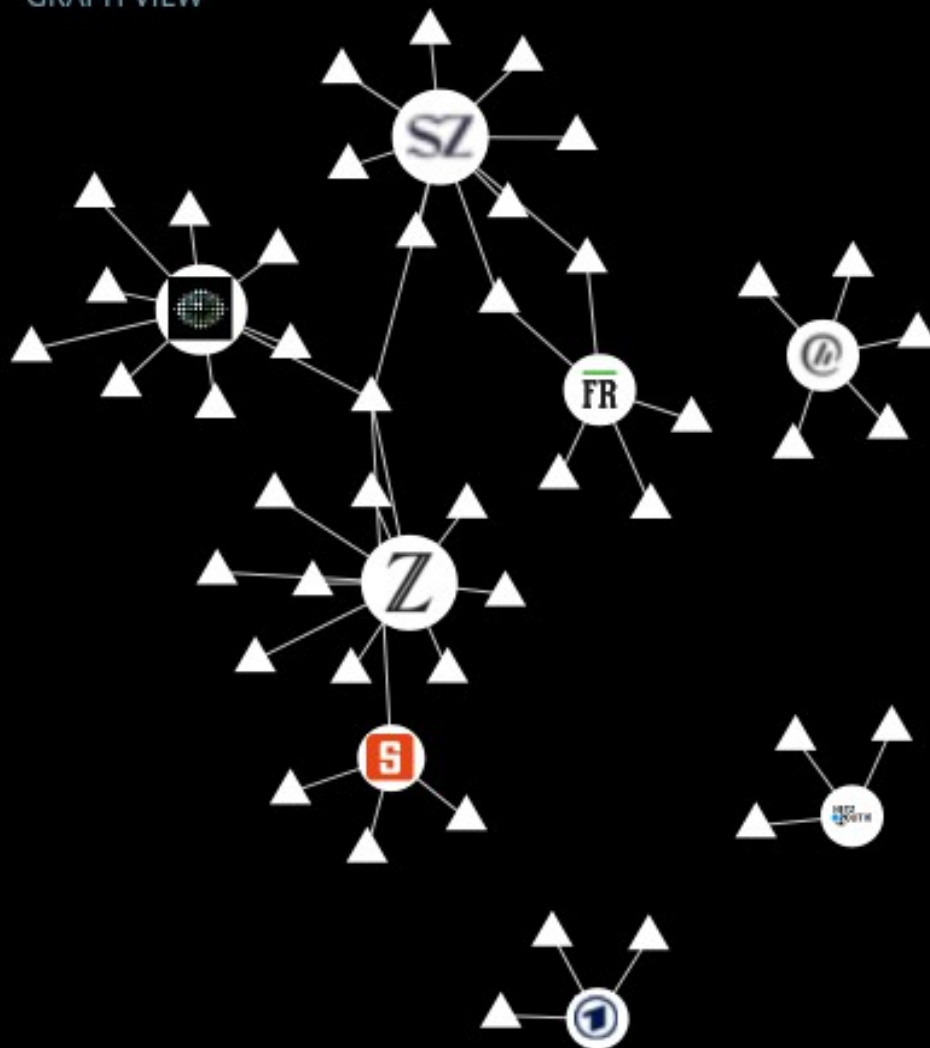
 Graph

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>
(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.

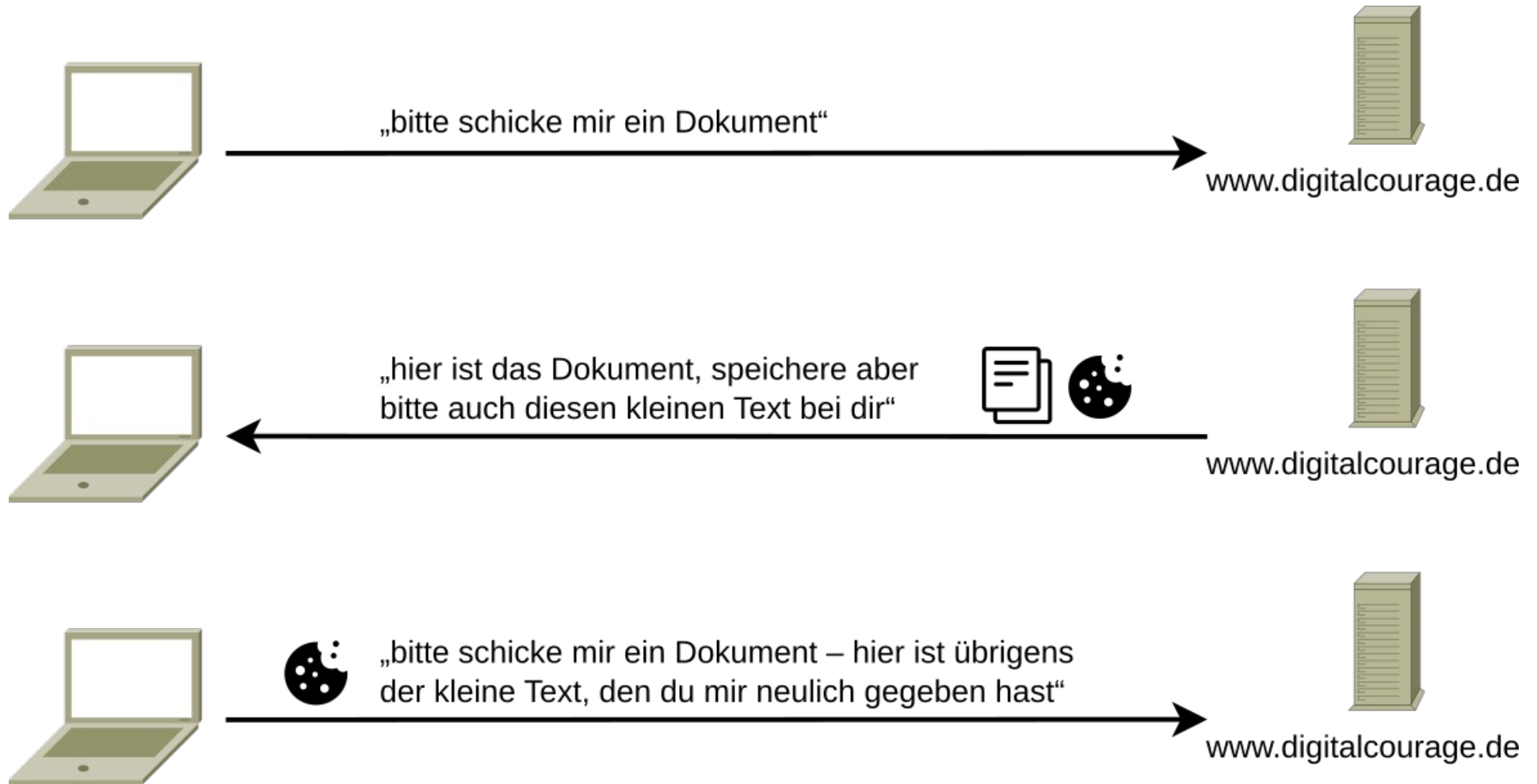
▶ Externe Merkmale:

- ▷ IP-Adresse

▶ Eindeutiger Browser-Fingerabdruck:

- ▷ <https://panopticlick.eff.org>

Was sind Cookies?

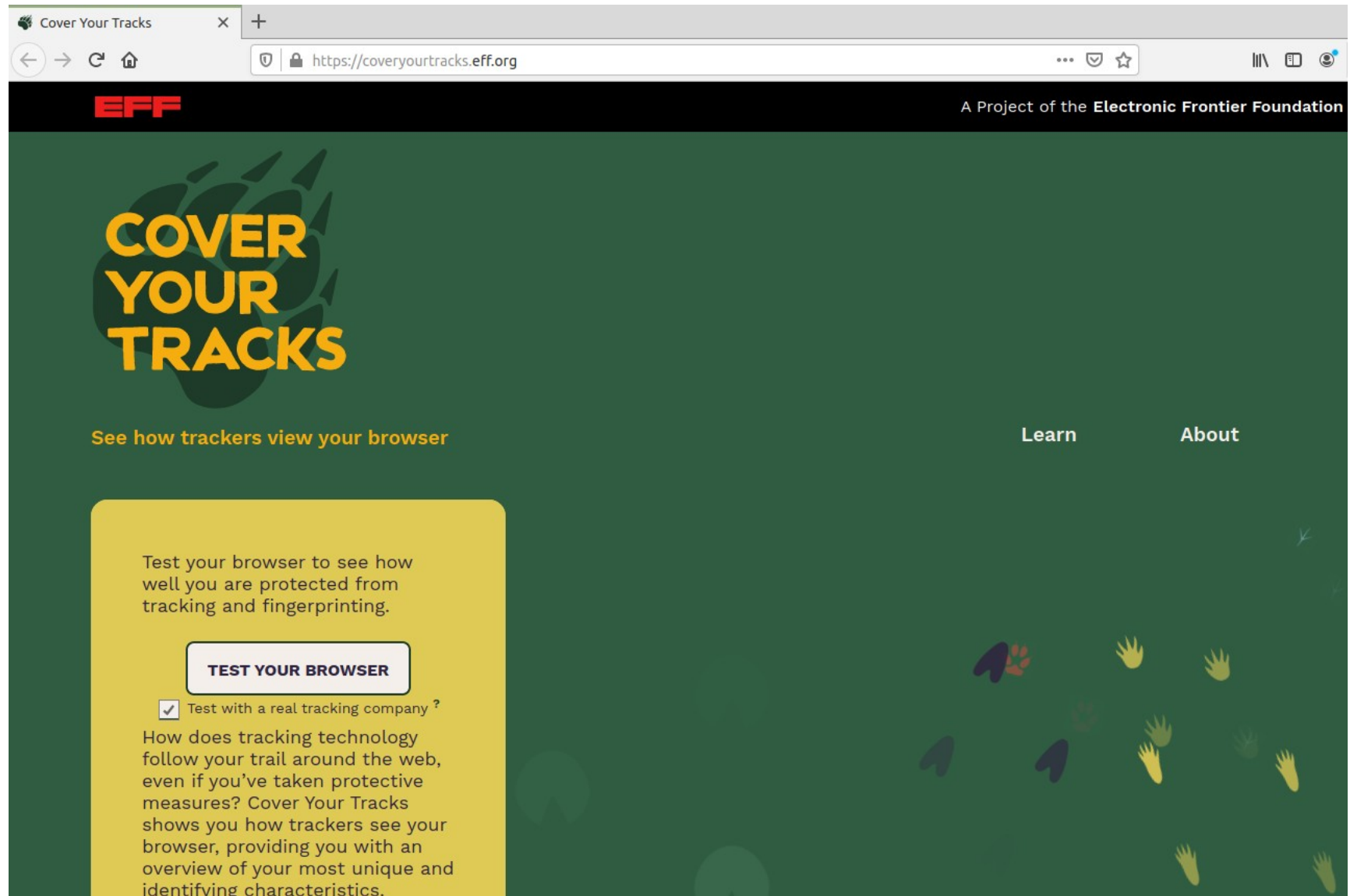


Was machen Cookies?

- ▶ sie lösen das Problem, dass HTTP „kein Gedächtnis“ hat
- ▶ Speichern von 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



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: **LocalCDN**
- ▶ 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~~
uBlock Origin

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

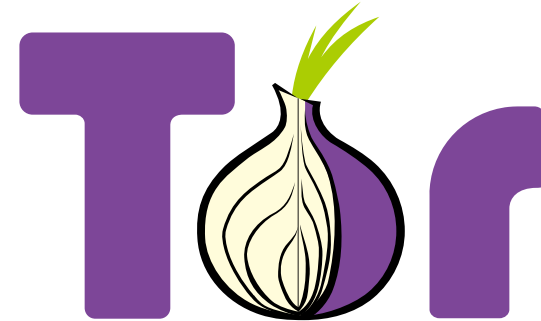
Wie bekommen wir das?

- ▷ 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



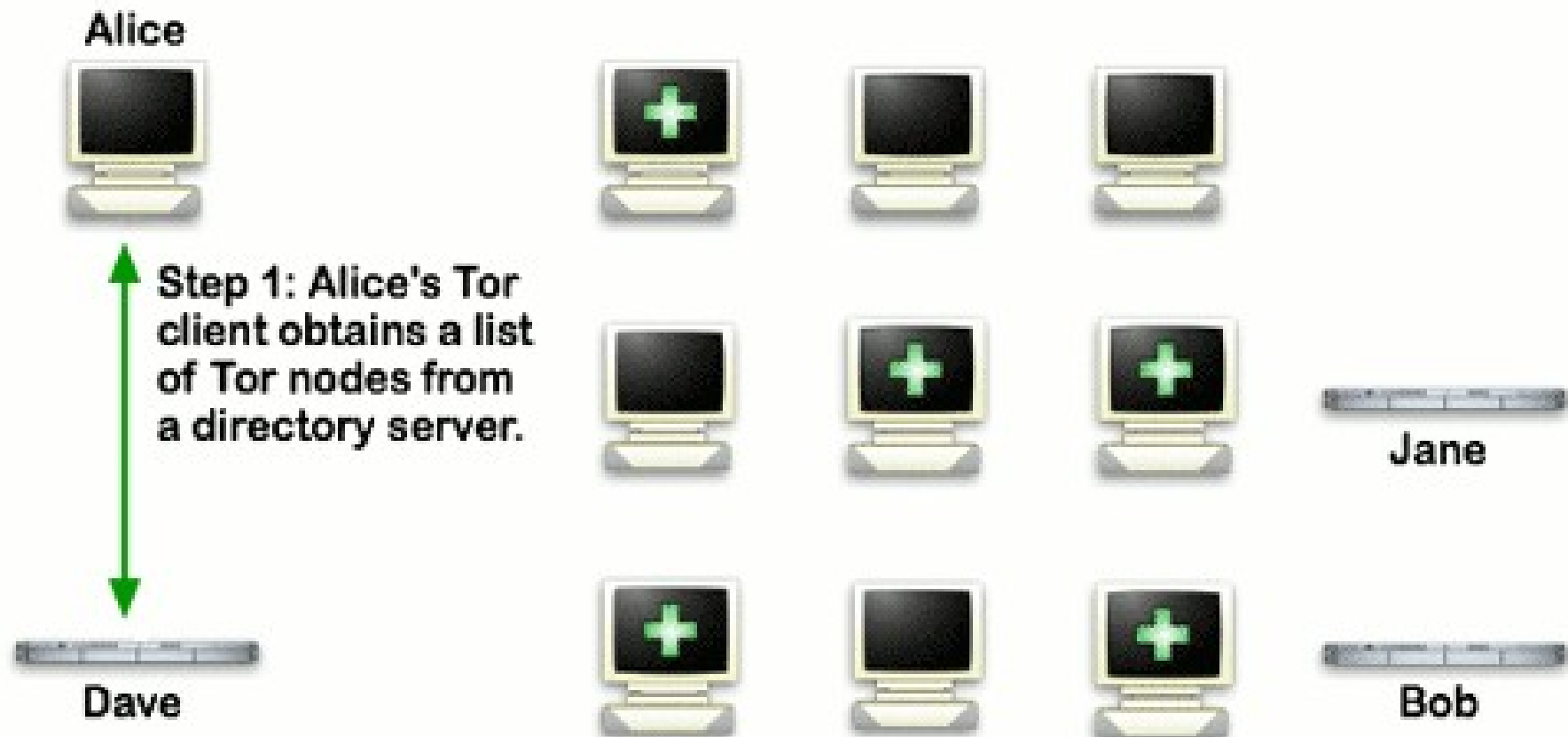
Vorteile

- ▶ quelloffen, freie Software
- ▶ anonymes Surfen

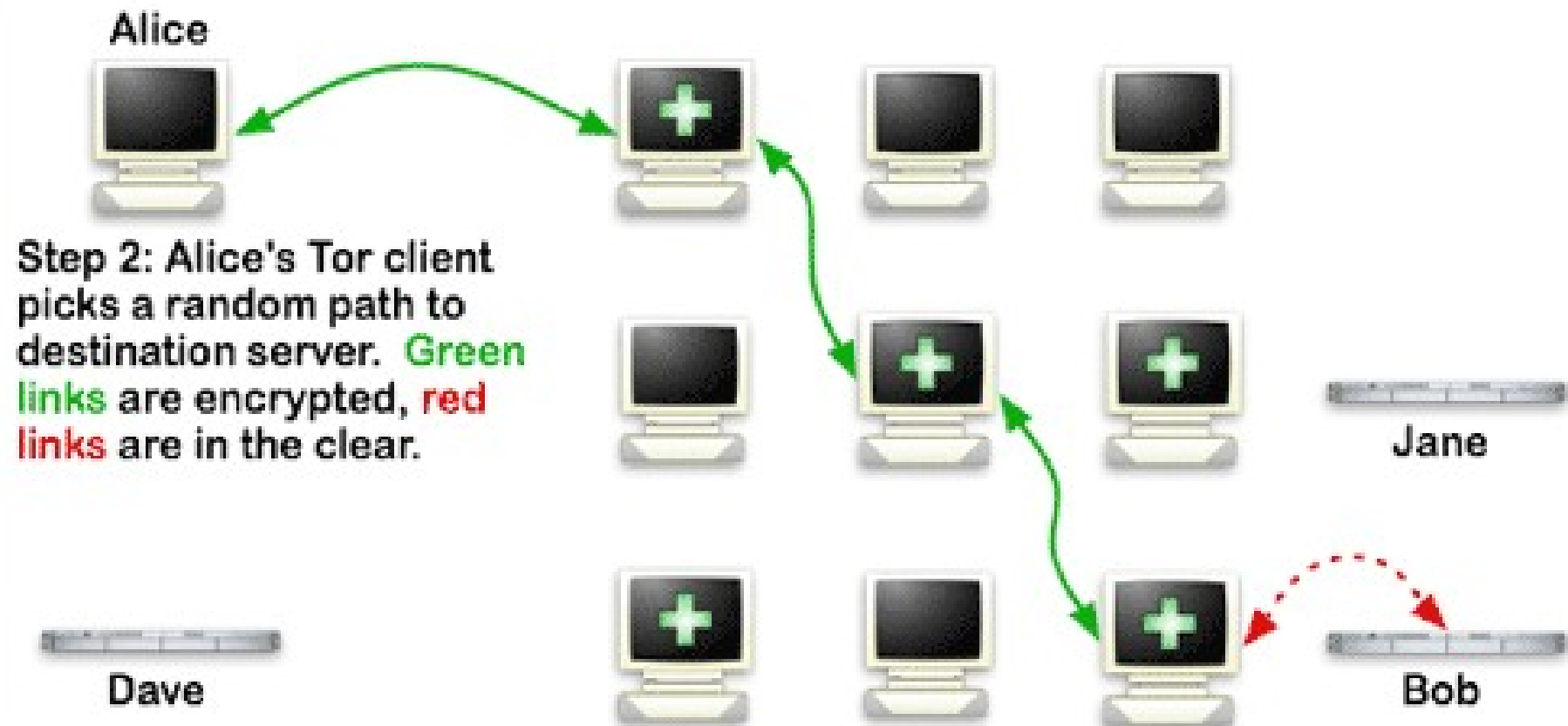
Nachteile

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

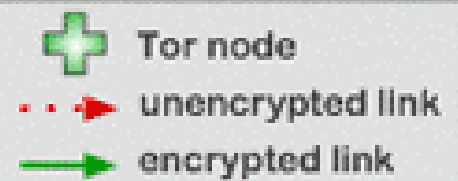
How Tor Works: 1



How Tor Works: 2



E How Tor Works: 3



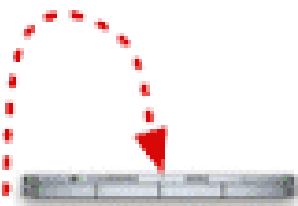
Alice



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



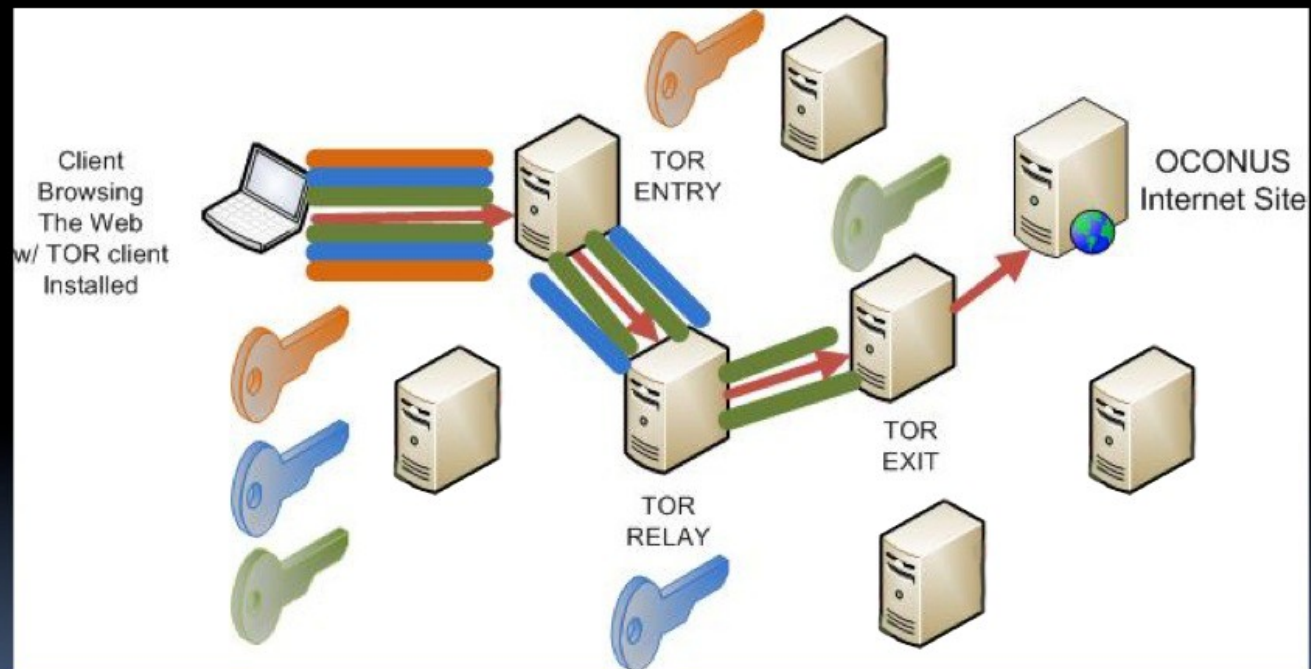
Jane



Bob

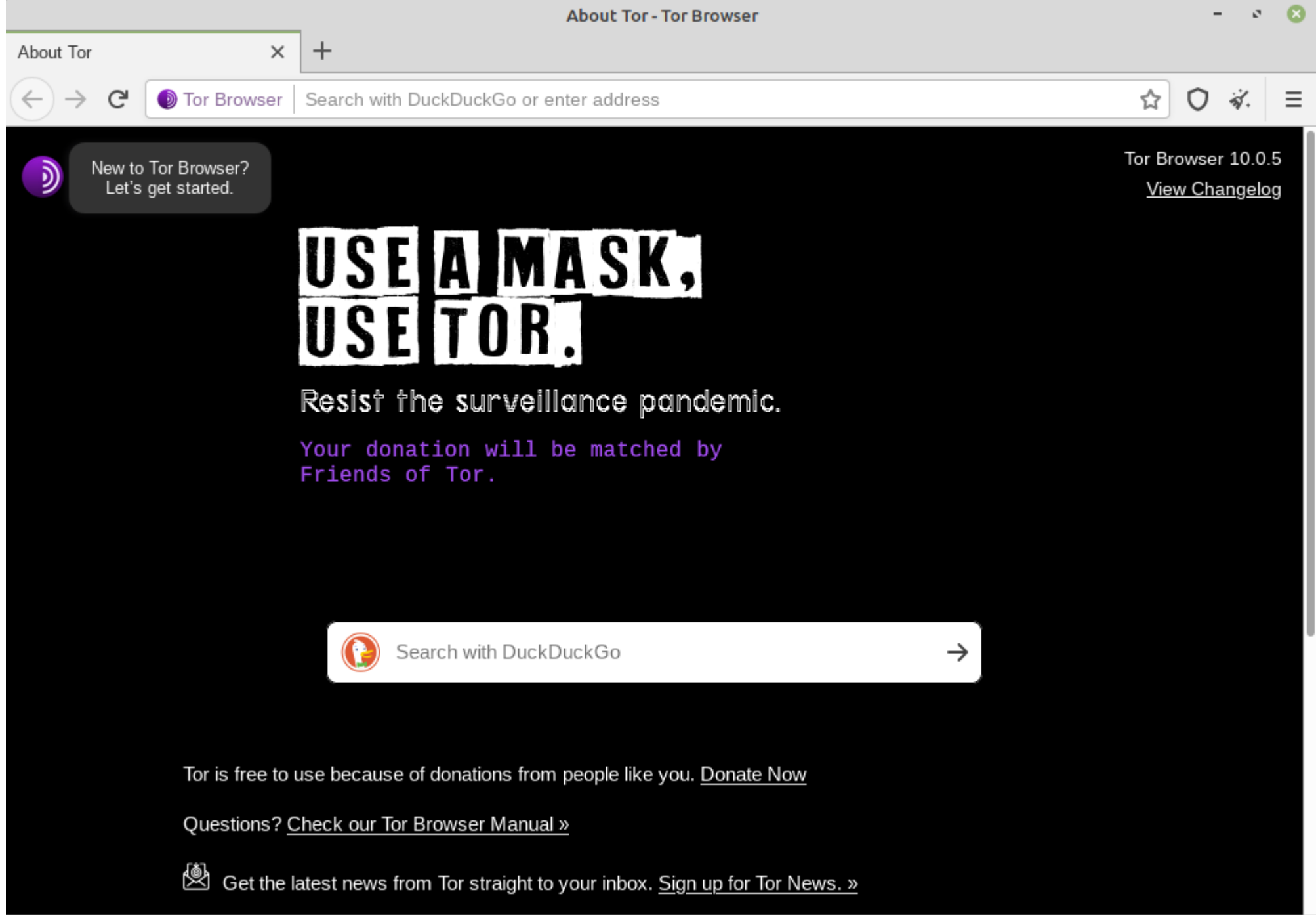


(U) What is TOR?



Download Tor-Browser

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



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 (Band I & II)
<https://capulcu.blackblogs.org/>

– Ende –