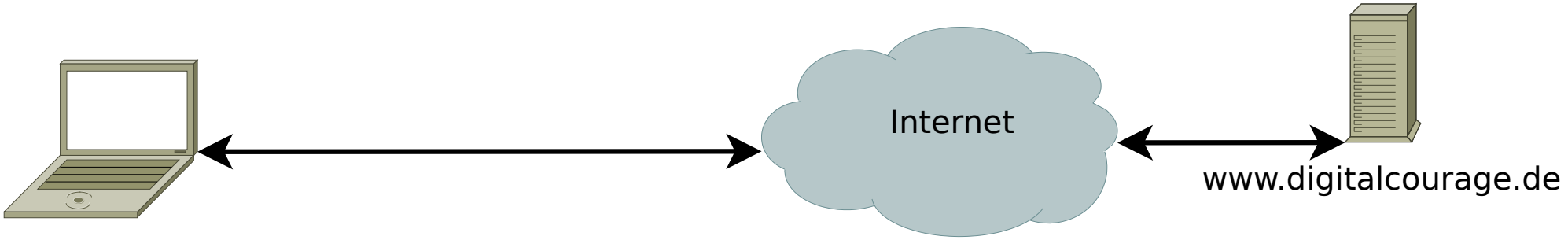
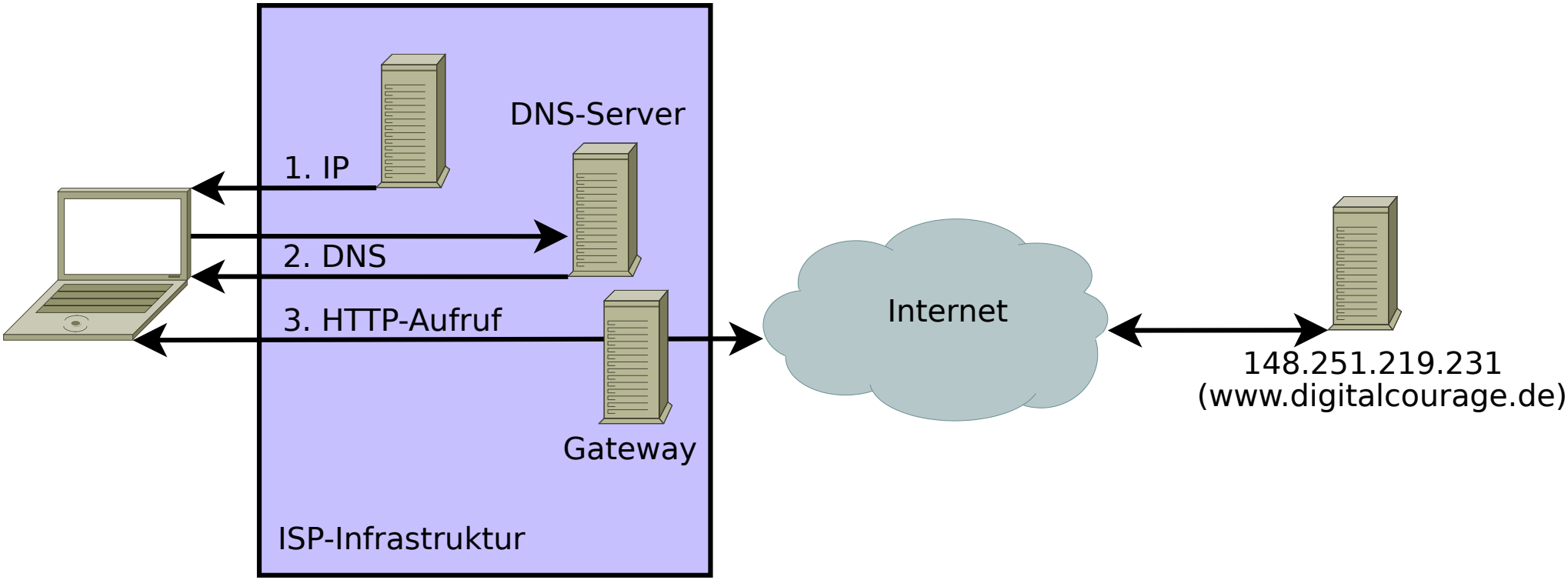
Sicher und anonym unterwegs im Web

Georg

Wie funktioniert das Web?



Und technisch?



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

- Beispiel: **https**://www.spiegel.de/ (mit Standard-Firefox 67)

… so schrecklich!

- Beispiel: **https**://www.spiegel.de/
- 494 (nach 20s) Anfragen, davon 419 an 79 externe Server...
- www.spiegel.de, magazin.spiegel.de, cdn1.spiegel.de, count.spiegel.de, fsm2.spiegel.de, m.spiegel.de

… so schrecklich!

dt.adsafeprotected.com, .research.de.com, .meetrics.net, .**googlesyndication**.com, script.ioam.de, .criteo.net, **googletagmanager**.com,omny.fm, .cloudfront.net, .mxcdn.net, .optimizely.com, w.soundcloud.com, static.emsservice.de, dyn.emetriq.de, optout.adalliance.io, .mxcdn.net, c.amazon-adsystem.com, 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, cdn.adrtx.net, servedby.flashtalking.com, pixel.adsafeprotected.com, tags.bluekai.com, www.omnycontent.com, .2mdn.net, m.exactag.com, widgets.outbrain.com, dnacdn.net, cdn.content-garden.com, www.summerhamster.com, ...

… so schrecklich!

- 8-10 MB; 64 Cookies, 31 von Drittanbietern
- Ladezeit ca. 15-30 Sek. + Nachladen ohne Interaktion und Scrollen

Lightbeam for Firefox

VISUALIZATION

Graph

DATA

Save Data

Reset Data

Give Us Feedback

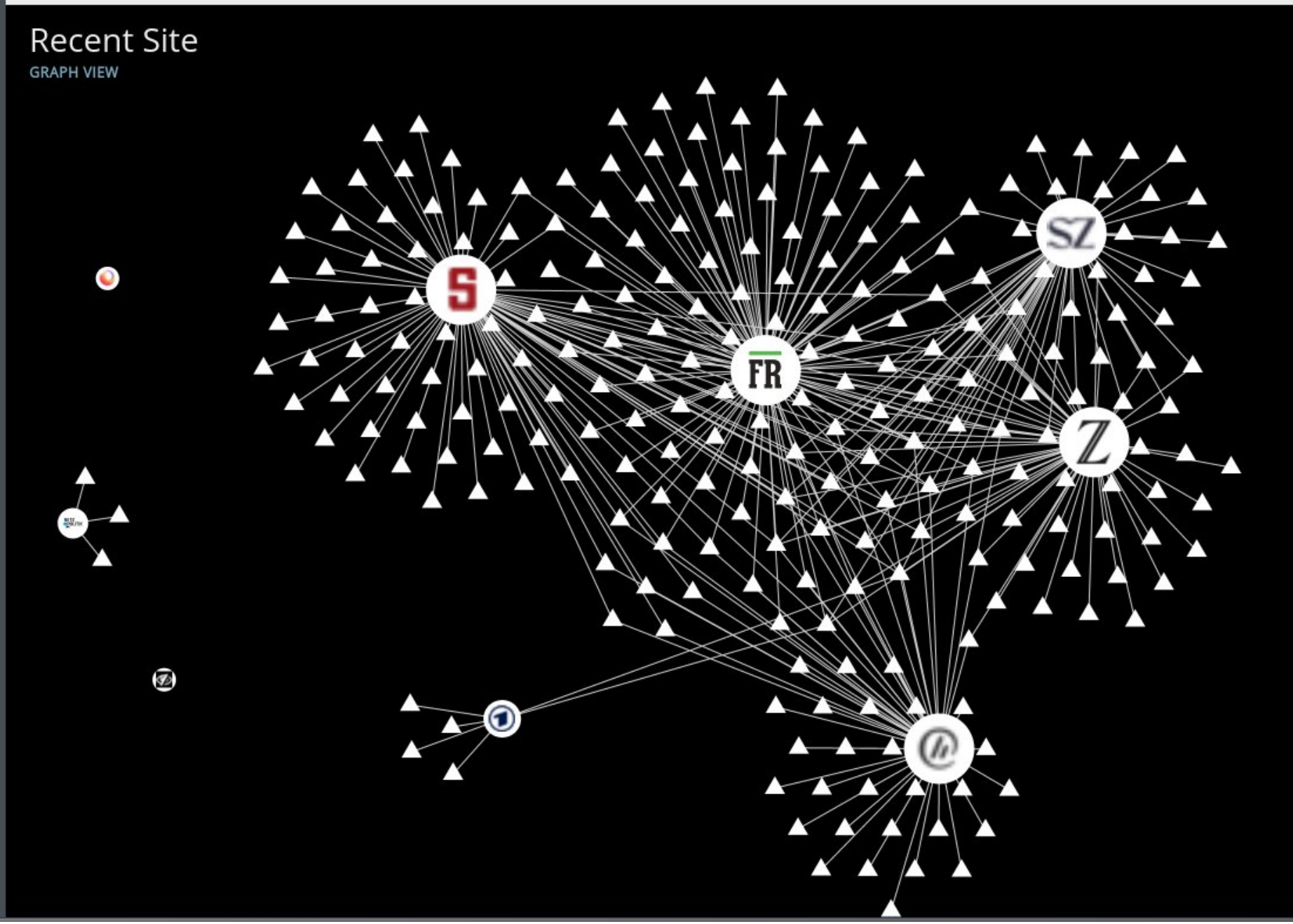
DATA GATHERED SINCE
DEC 12 2019

YOU HAVE VISITED
10 SITES

YOU HAVE CONNECTED WITH
247 THIRD PARTY SITES

Recent Site

GRAPH VIEW



(Bild: CC-BY-2.0: EFF)

Lightbeam for Firefox

VISUALIZATION

Graph

DATA

Save Data

Reset Data

Give Us Feedback

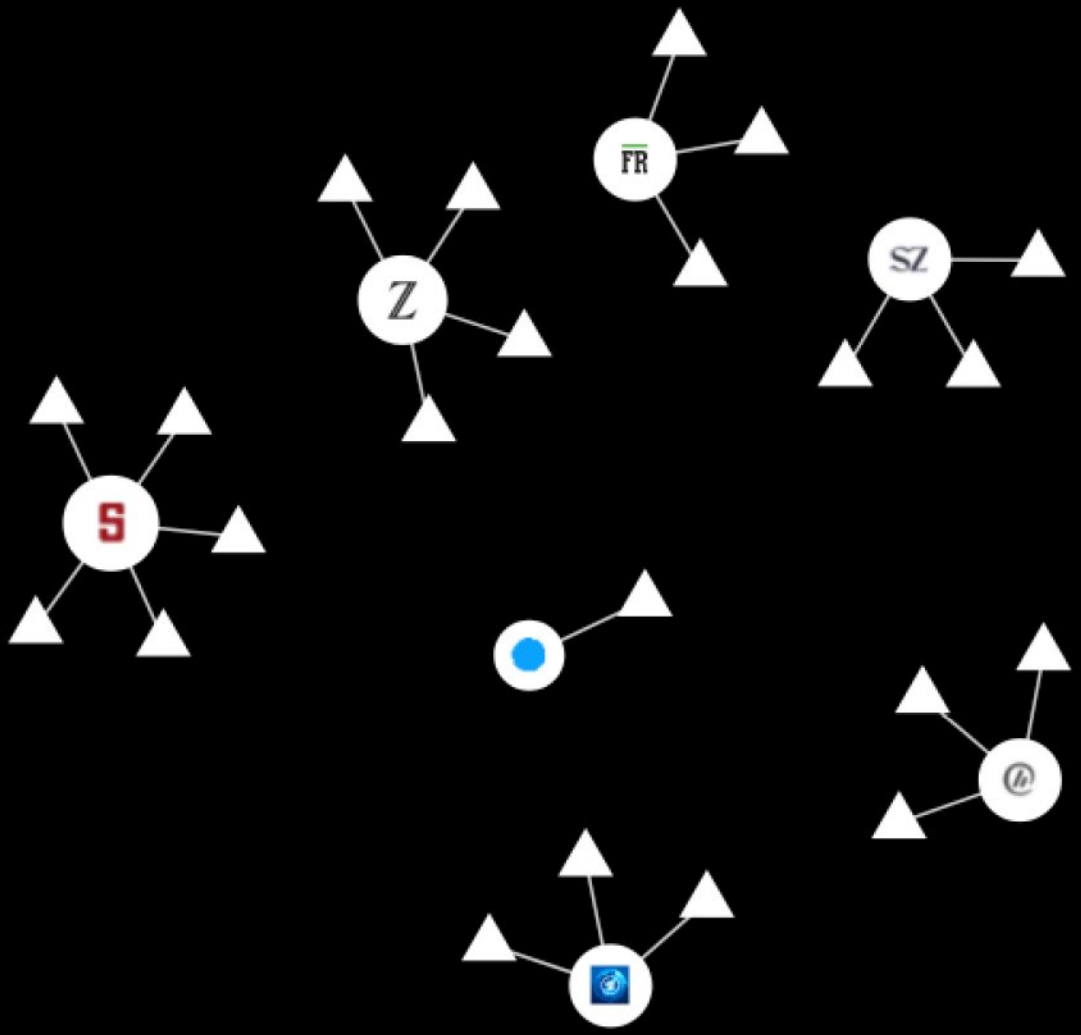
DATA GATHERED SINCE
DEC 12 2019

YOU HAVE VISITED
7 SITES

YOU HAVE CONNECTED WITH
22 THIRD PARTY SITES

Recent Site

GRAPH VIEW



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.

Entwickelt von dataskydd.net.

Der Quellcode ist auf GitHub verfügbar.

Feedback? Fragen? info@dataskydd.net

Twitter: @dataskyddnet

Unterstütze uns

https://webbkoll.dataskydd.net/de

"How we take back the Internet?"

– Title of a TED Talk by Edward Snowden

Sicheres Surfen mit Privatsphäre

Was wollen wir?

- Sicherheit:
  - Vertraulichkeit
  - Authentiziät
  - Integrität

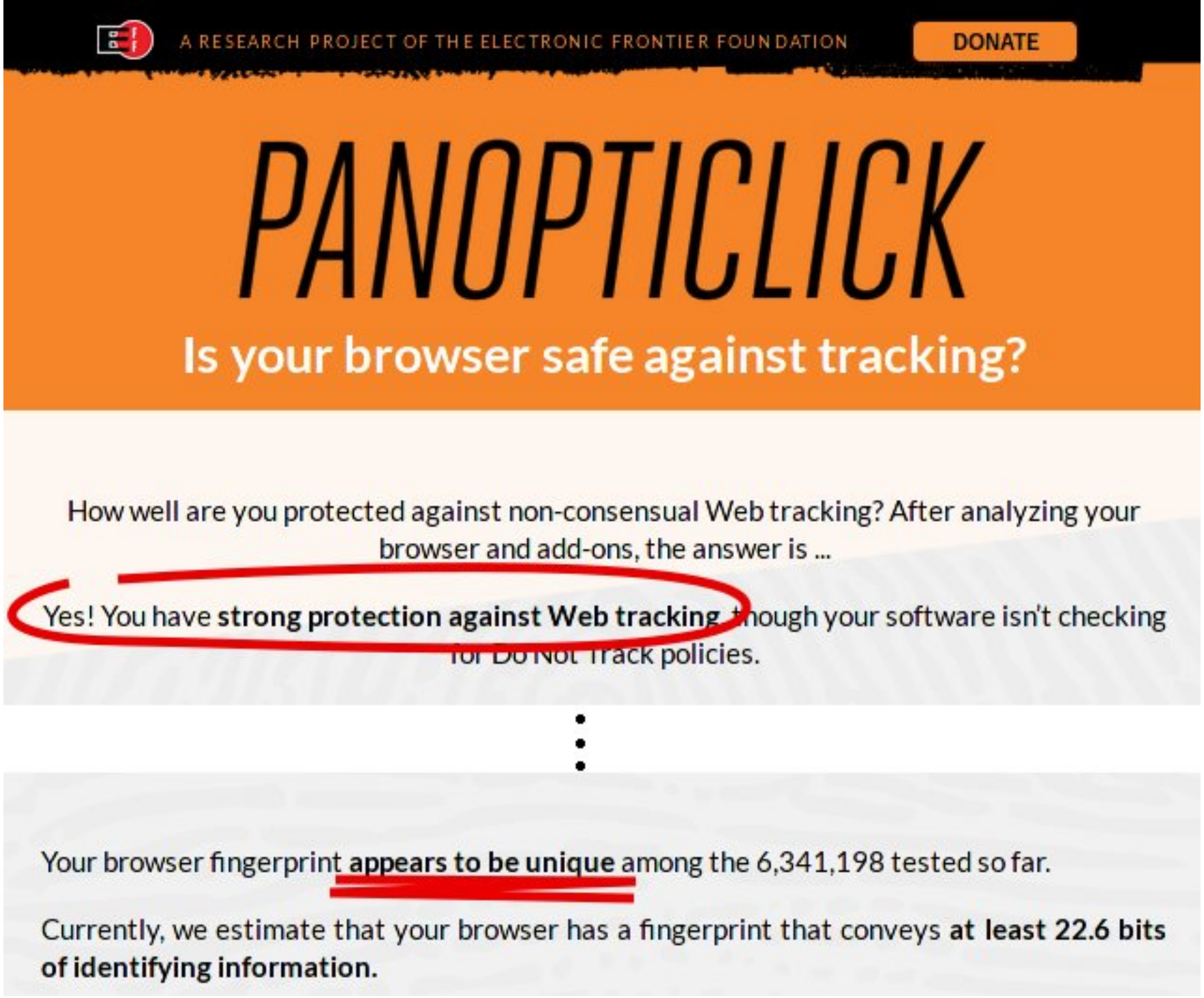
Sicheres Surfen mit Privatsphäre

Was wollen wir?

- Sicherheit:
  - Vertraulichkeit
  - Authentiziät
  - 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 Webseite 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, uvm.
- Externe Merkmale:
  - IP-Adresse
- Eindeutiger Browser-Fingerabdruck:
  - https://panopticlick.eff.org



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:

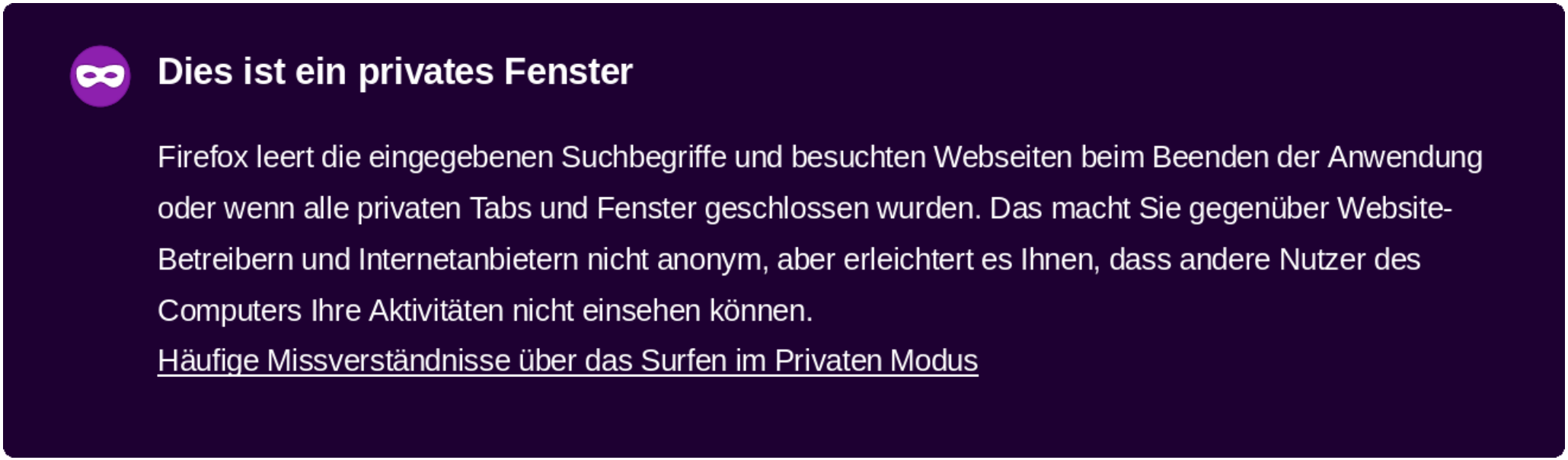
- Referer blockieren: **SmartReferer**
- JavaScript blockieren (Whitelist säubern): **NoScript**
- Alle Drittanbieteranfragen blocken: **uMatrix**

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
- *Keine Anonymität* gegenüber dem Netz



Sicheres Surfen mit Privatsphäre

Was wollen wir?

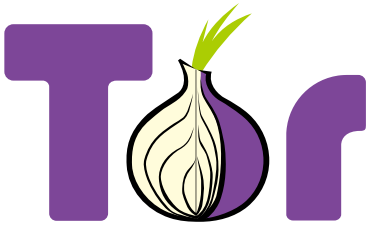
- Sicherheit:
  - Vertraulichkeit
  - Authentiziät
  - Integrität
- Anonymität
  - Nur teilweise vereinbar mit Authentizität!
- Resistenz gegenüber Zensur

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

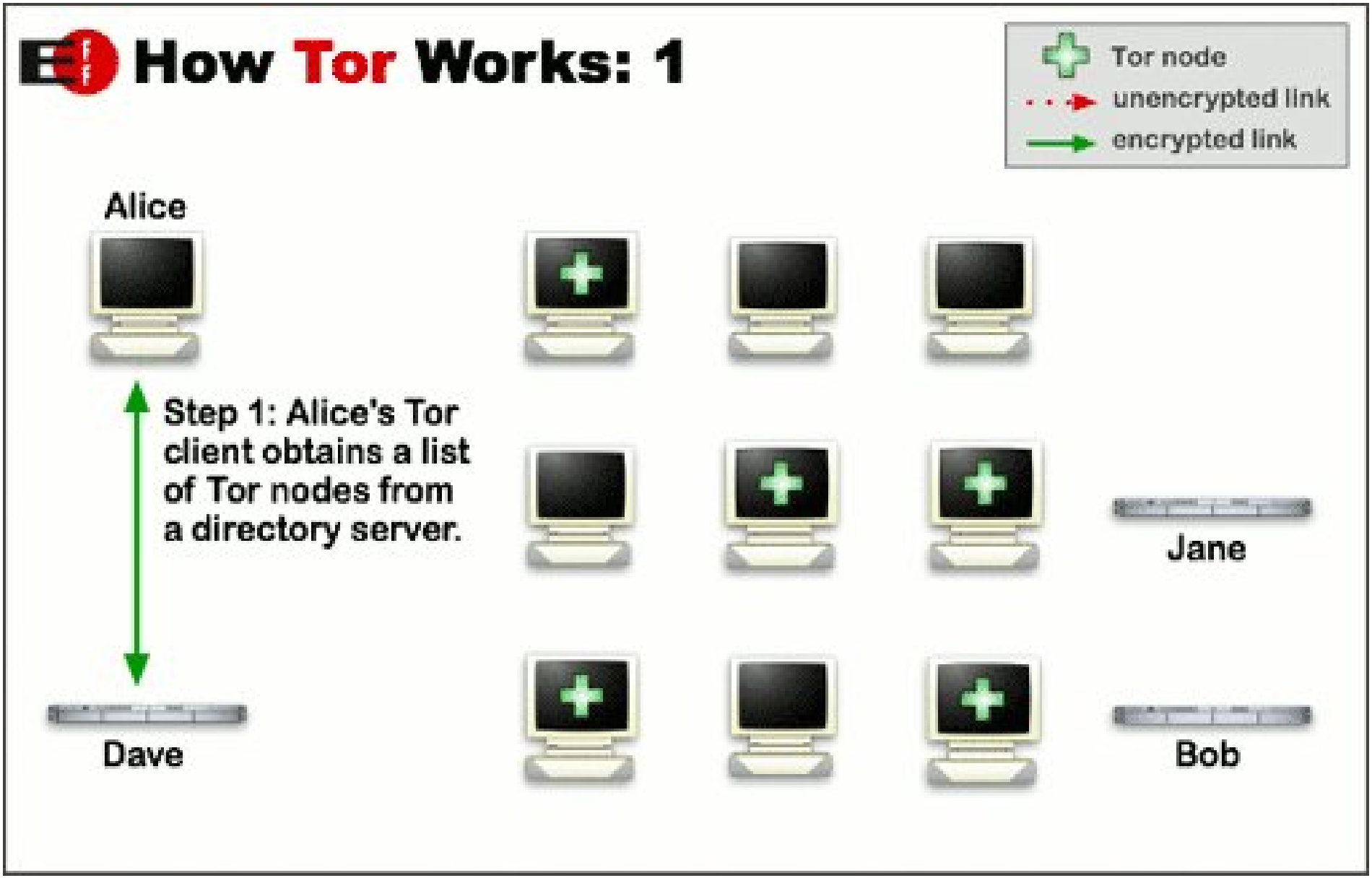
Vorteile

- Quelloffen, freie Software
- Anonymes Surfen

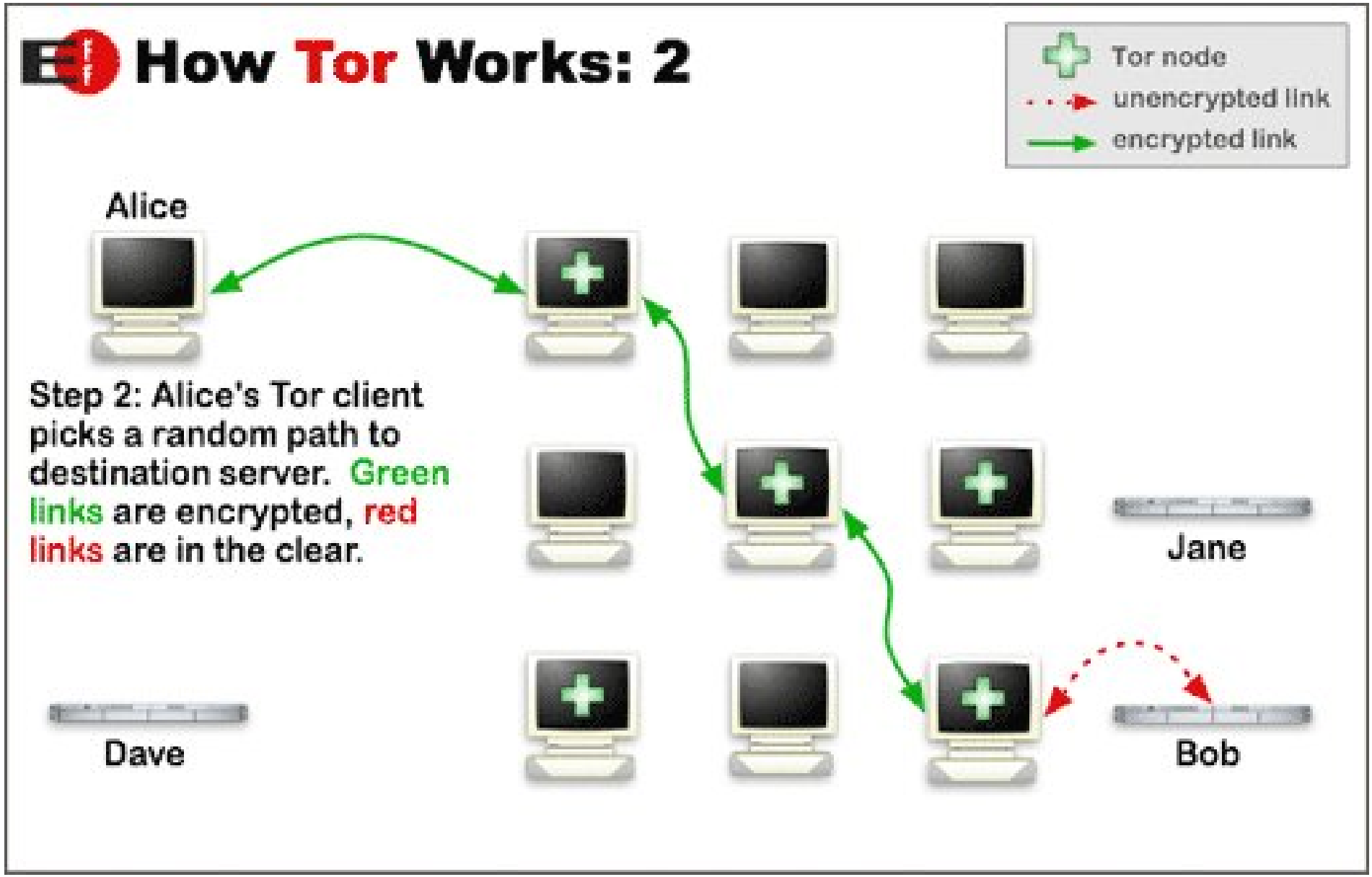
Nachteile

- Login bei personalisierten Seiten nicht sinnvoll
- Latenz ist größer

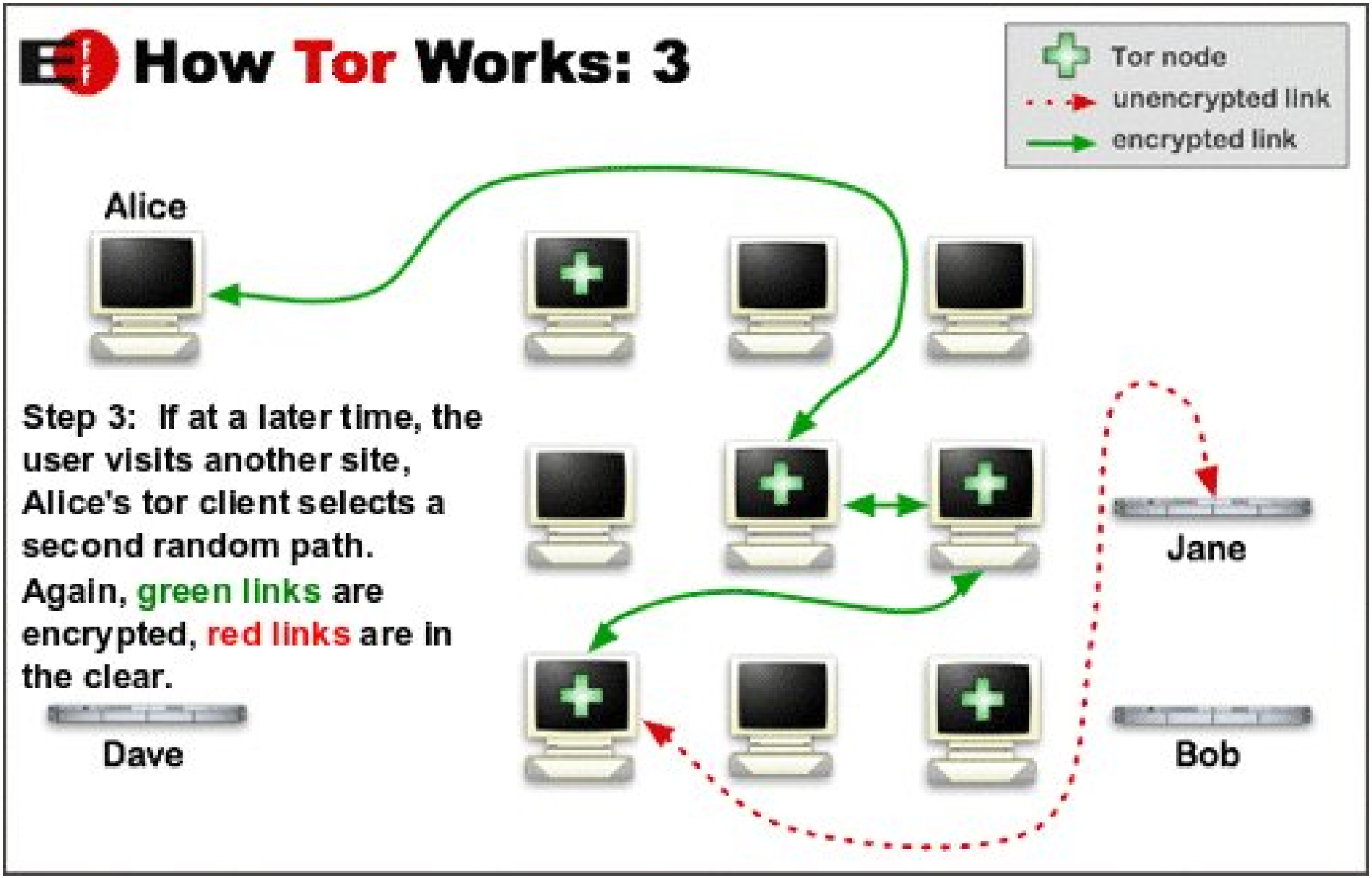
How Tor Works: 1



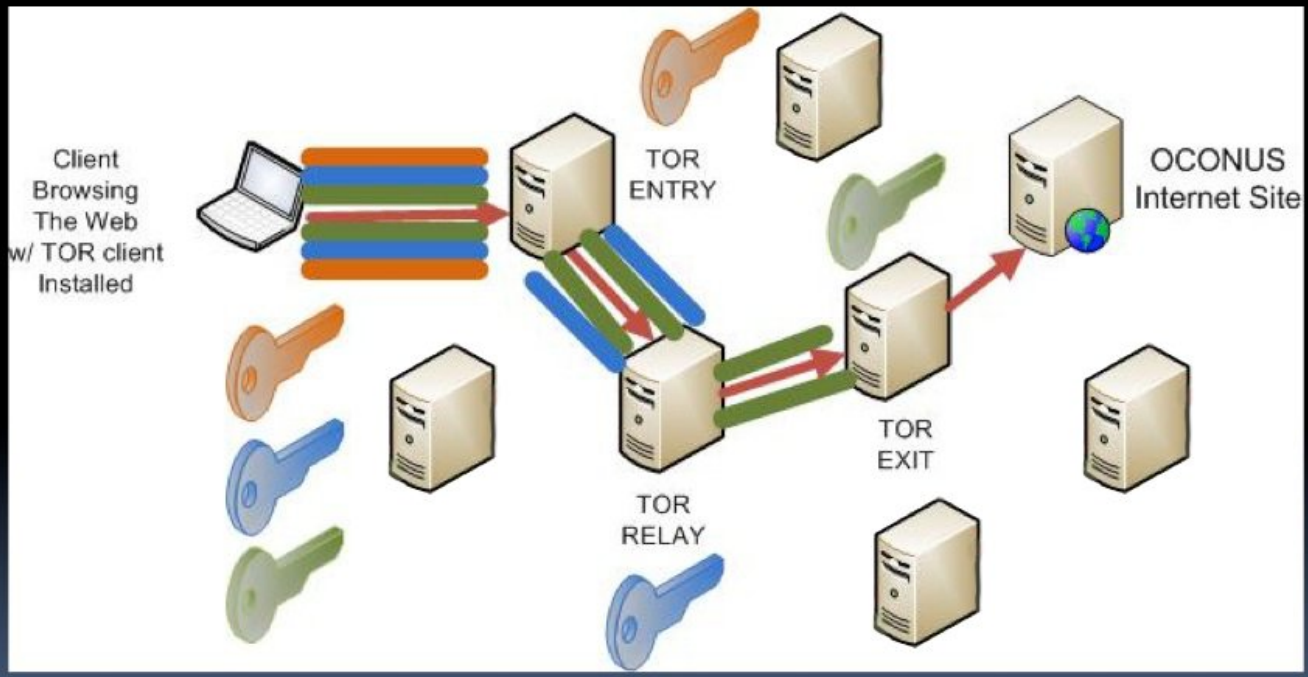
How Tor Works: 2



How Tor Works: 3

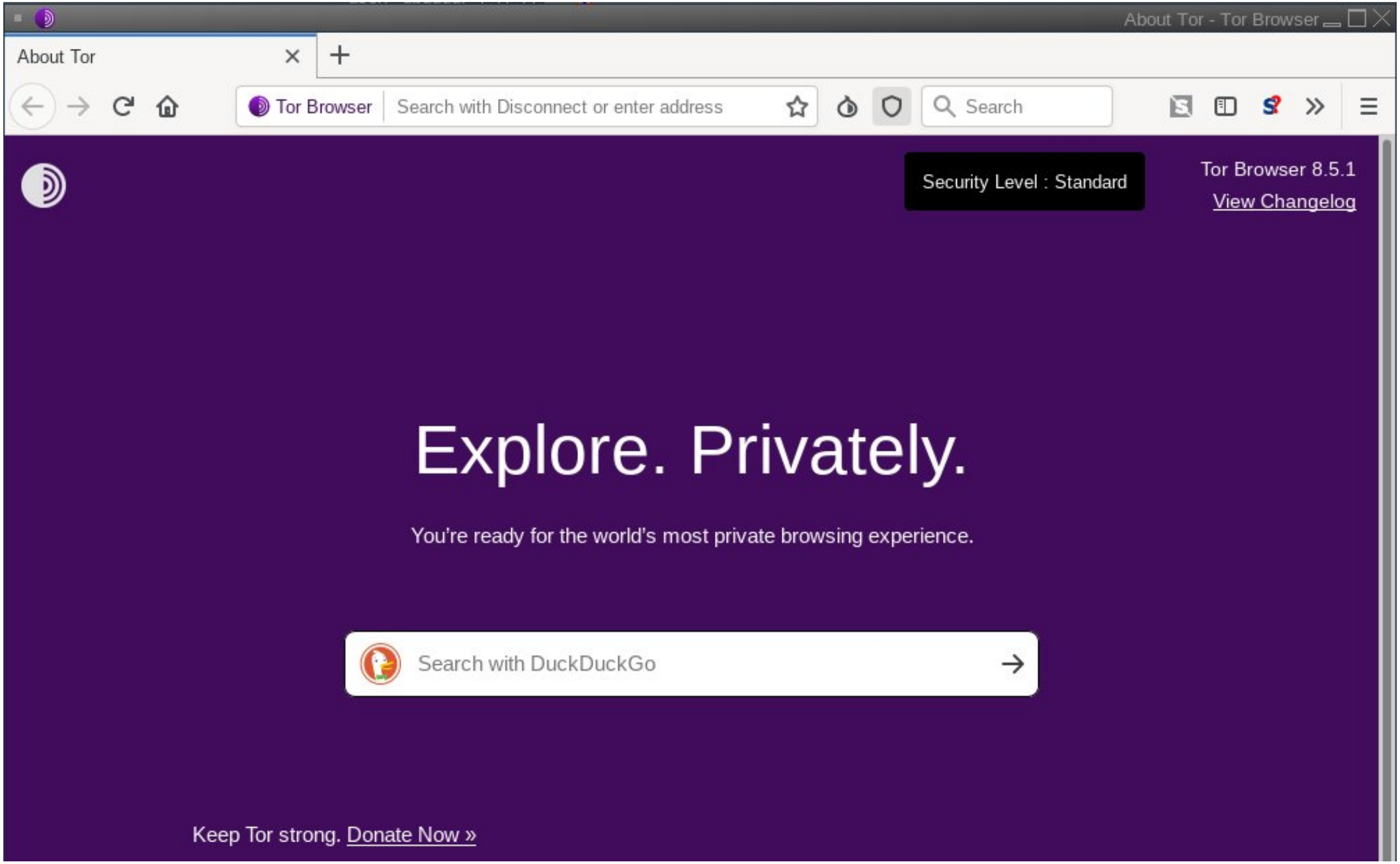


(U) What is TOR?



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

- **T**he **A**mnesic **I**ncognito **L**ive **S**ystem (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 Capulcu https://capulcu.blackblogs.org/

Vielen Dank für‘s Mitmachen!

(Bild: CC-BY-2.0: EFF)