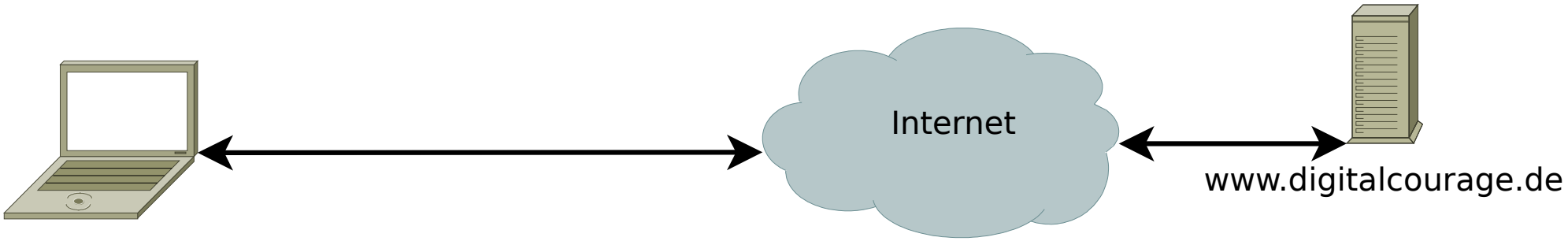
Agenda Samstag

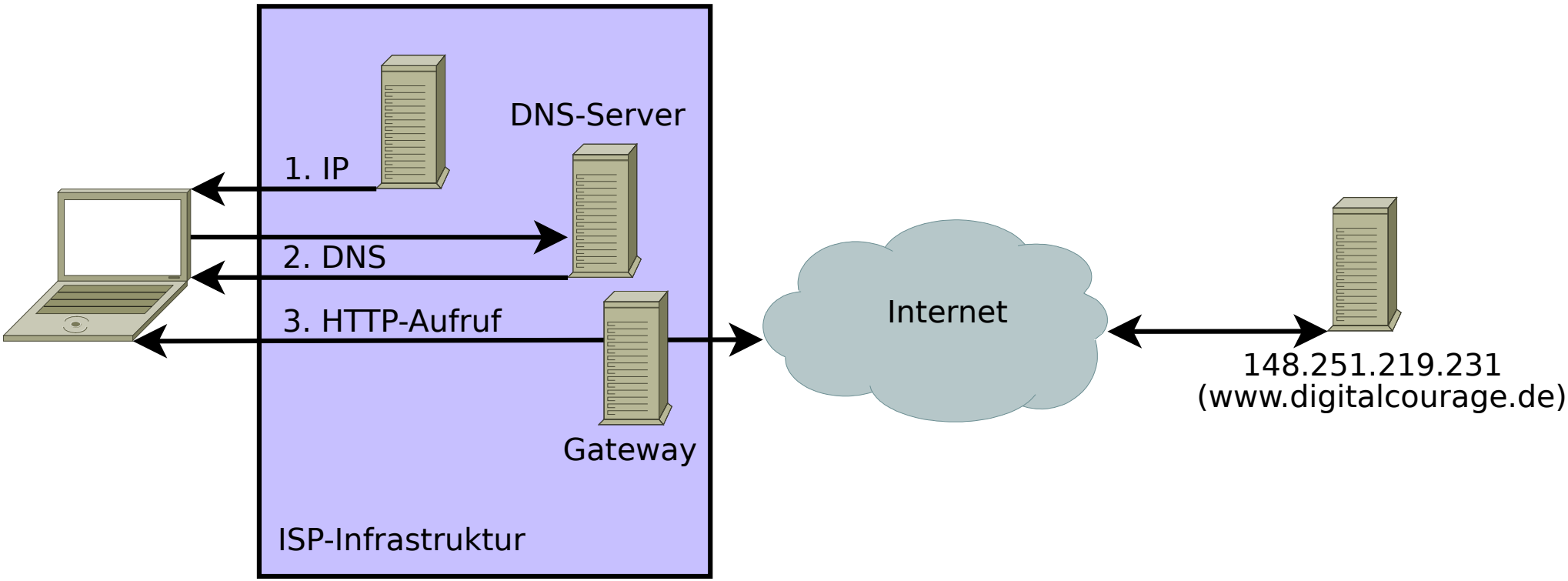
von	bis	Titel
10:00	12:00	Digitale Selbstverteidung II (Browser, Mobilgeräte)
12:00	12:45	- Mittagspause -
12:45	14:00	Praxisteil
14:00	14:15	- Pause -
14:15	16:00	Feedback Praxis, Diskussion
		Open End

Sicheres Surfen mit Privatsphäre

Wie funktioniert der Aufruf einer Webseite?



Was ist technisch *notwendig*?



Wie schrecklich ist die Web-Realität?

Beispiel: www.spiegel.de

Standard-Firefox, Debian 8 GNU/Linux

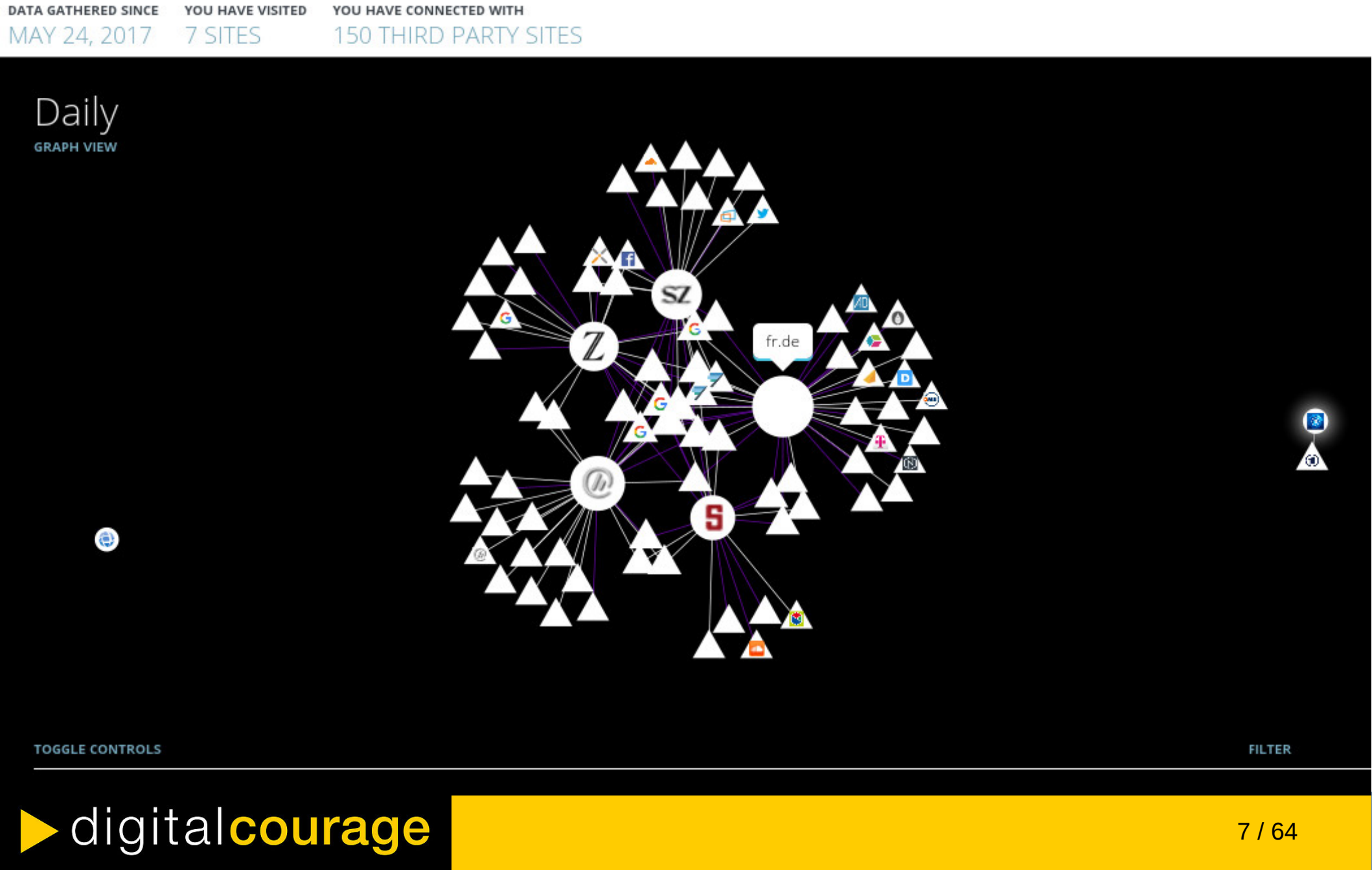
... so schrecklich!

Beispiel: www.spiegel.de

Standard-Firefox, Debian 8 GNU/Linux

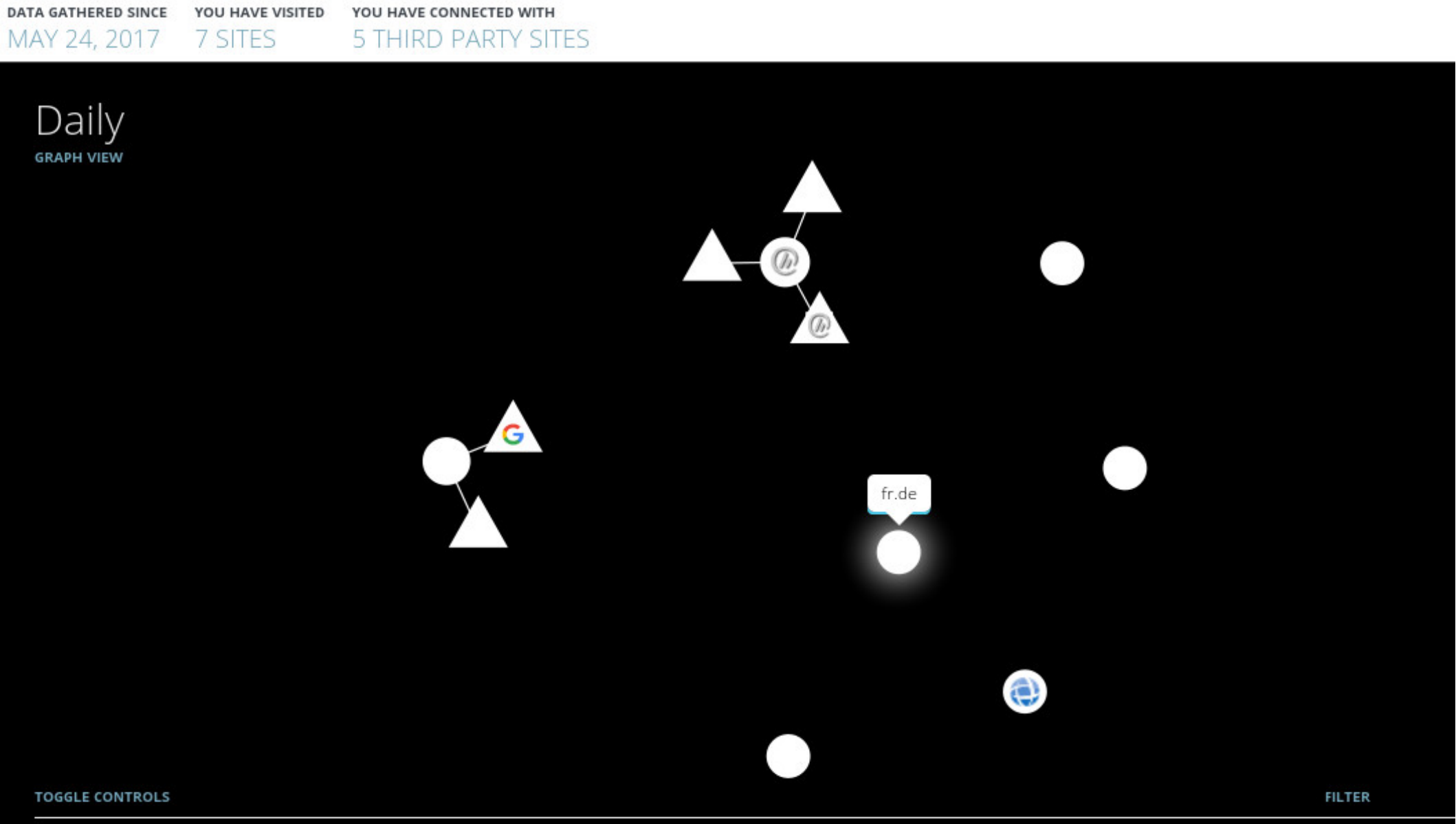
- 136 HTTP-GETs an folgende Domains...
- spiegel.de, meetrics.net, ioam.de, adition.com, yieldlab.net, criteo.com, *flashtalking.com*, exactag.com, parsely.com, meetrics.net, outbrain.com, *atdmt.com, ligatus.com*, doubleclick.net, adform.net, google-analytics.com, *t4ft.de*, *westlottol.com*, *ligadx.com,* googlesyndication.com, *lqm.io*, *soundcloud.com*,
- 1,6 MB; 59 Cookies von 19 Domains
- Ladezeit ca. 17 Sek. (Core i5 M560)

Analyse im Firefox mit Lightbeam

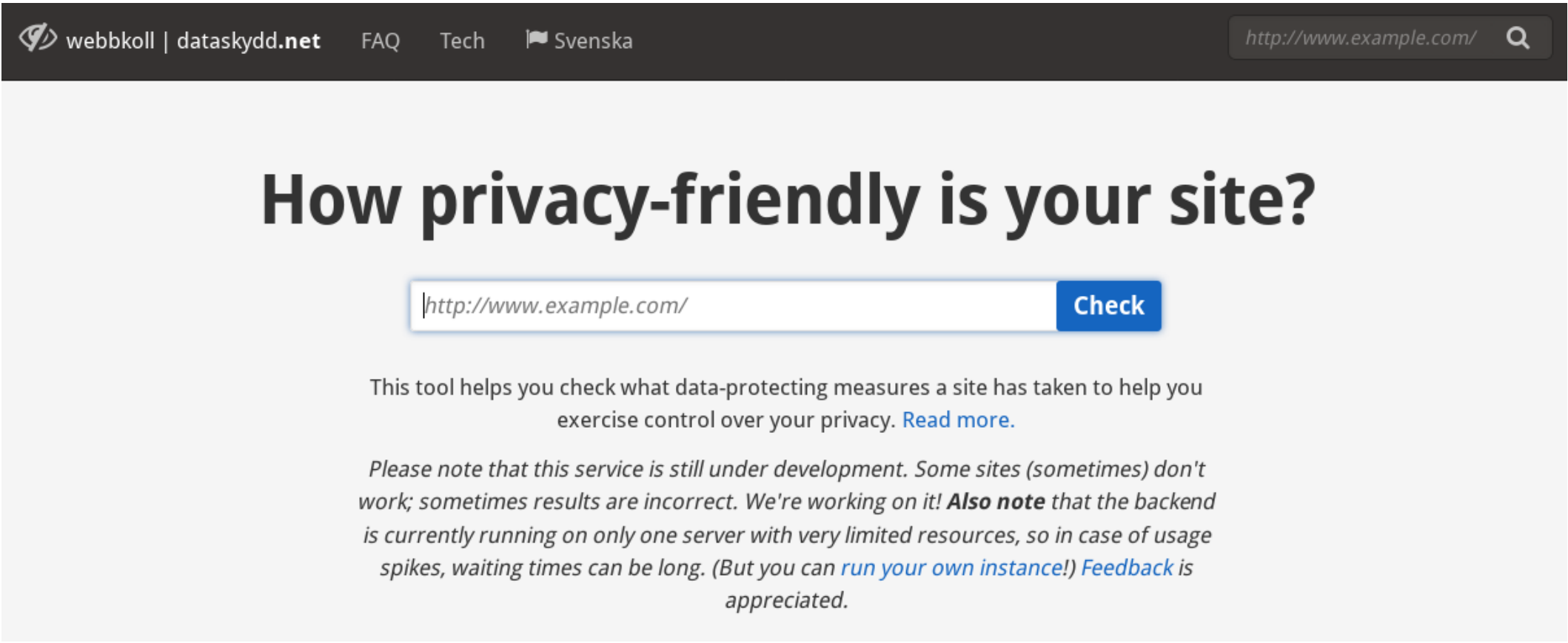


(Bild: CC-BY-2.0: EFF)

Analyse im Firefox mit Lightbeam



Einfach selber Testen mit Webbkoll



https://webbkoll.dataskydd.net/en

"How we take back the Internet?"

– Title of a TED Talk by Edward Snowden

Sicheres Surfen mit Privatsphäre

Ziele:

- Sicherheit:
  - Vertraulichkeit
  - Authentizität
  - Integrität

Sicheres Surfen mit Privatsphäre

Ziele:

- Sicherheit:
  - Vertraulichkeit
  - Authentizität
  - Integrität
- Anonymität
  - Nur teilweise vereinbar mit Authentizität!

Sicheres Surfen mit Privatsphäre

Ziele:

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

Sicheres Surfen mit Privatsphäre

Ziele:

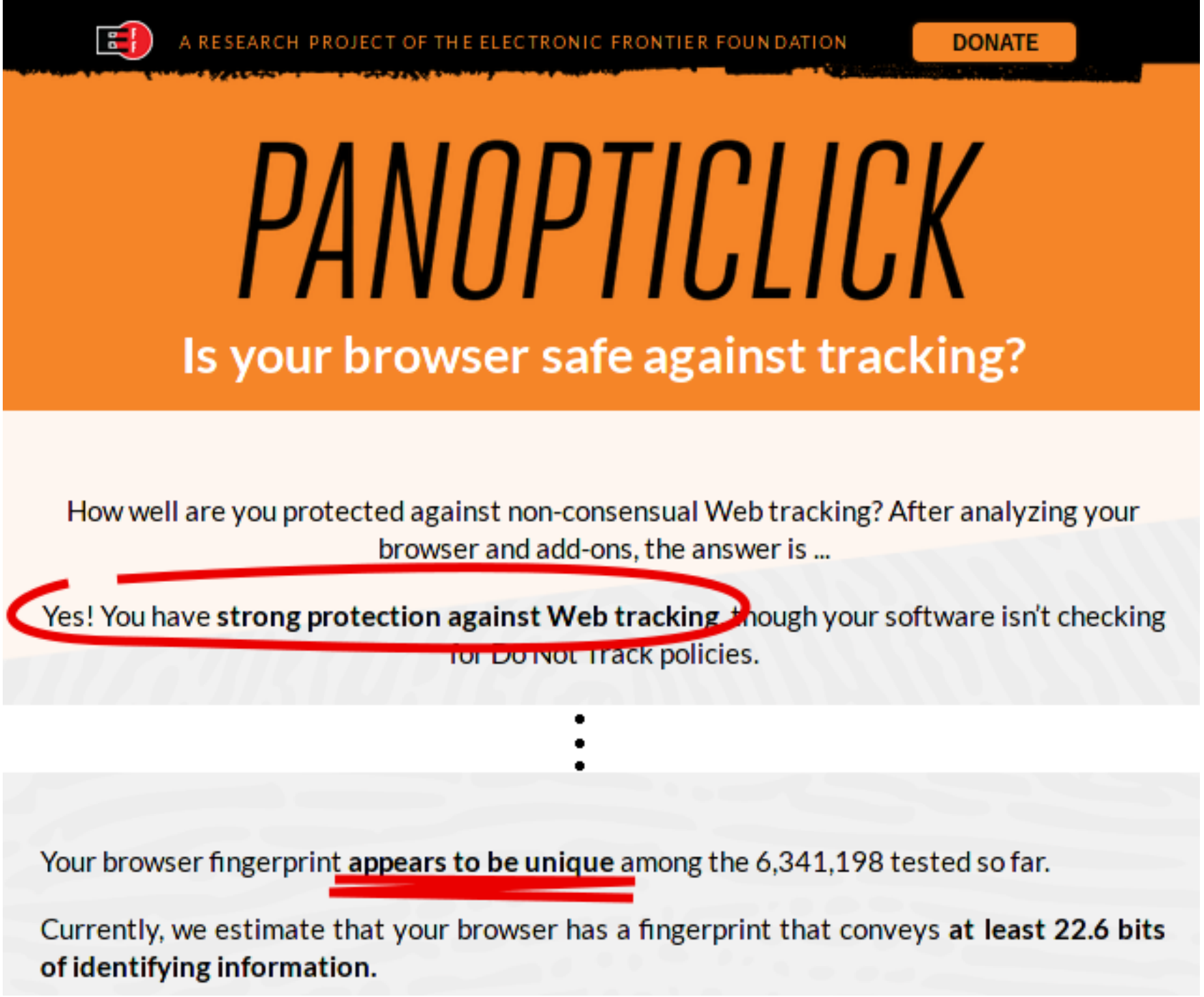
- Sicherheit:
  - Vertraulichkeit → HTTPS (Verschlüsselung)
  - Authentizität → HTTPS (Zertifikate)
  - Integrität → HTTPS
- Anonymität
  - Firefox
  - Tracking blocken → verschiedene Add-ons
  - Nur benötigte Cookies → Cookie-Einstellungen
  - IP-Verschleierung → Tor-Browser

Wie kann ein Webserver mich identifizieren und verfolgen (Tracking)?

- Cookies:
  - kleine Textdateien, die die aufgerufene Webseite im Browser speichern und wieder abrufen kann.
- Passive Merkmale:
  - IP-Adresse, Sprache, Browser, Betriebssystem
- Aktive Merkmale (Javascript, Flash, Java, h264, ...)
  - Schriftarten, Browser-Add-ons, Bildschirmauflösung, uvm.

⇒ Eindeutiger Browser-Fingerabdruck

- siehe https://panopticlick.eff.org/


A RESEARCH PROJECT OF THE ELECTRONIC FRONTIER FOUNDATION
DONATE
PANOPTICLICK
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
  - Do-not-Track Option
  - Benutzerdefinierte Chronik:
    Cookies (für Drittanbieter) deaktivieren
- Suchmaschinen
  - startpage.com, ixquick.eu, DuckDuckGo.com, MetaGer.de, etc.
    (im Gegensatz zu Google auch keine individuellen Ergebnisse)
- Browser-Add-ons! ...

Firefox-Add-ons

- Tracker und Werbung blocken: **uBlock origin**
- Aktive Inhalte blocken: **NoScript**
  - Skripte allgemein erlauben (vom Hersteller nicht empfohlen)
- Webseiten immer verschlüsseln: **HTTPS Everywhere**
- Adobe-Flash am besten entfernen oder deaktivieren!
- Ein Klick statt about:config: **Privacy-Settings**

Etwas komplizierter und aufwendiger:

- Alle Skripte blocken: **NoScript**
- Alle Drittanbieteranfragen blocken: **RequestPolicy Continued**
- Referer blocken: **RefControl** (Vorsicht!)

Kontrolle

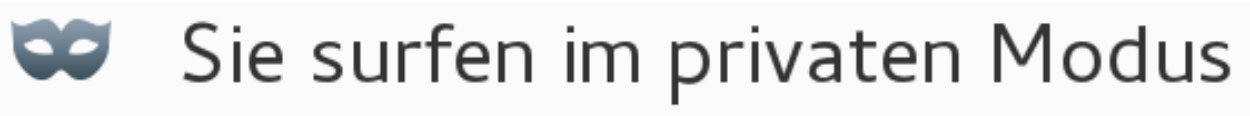
Wirkung von Add-ons und Einstellungen kontrollieren:

- Add-On: **Lightbeam**
- Menü → Extras → Webentwickler → Netzwerk

Weitere Firefox-Funktionen

Privater Modus

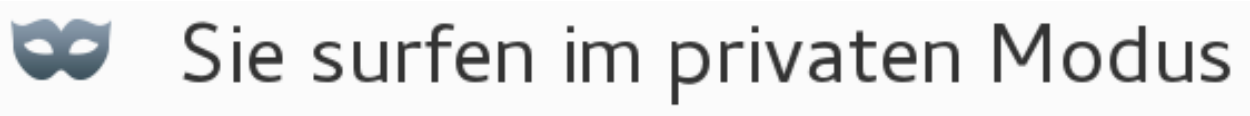
- Keine **lokale** Speicherung von Daten besuchter Webseiten (insb. keine Chronik, keine URL-Vervollständigung, Cookies, etc.)
- Auf dem verwendeten PC verbleiben keine Spuren
- *Keine Anonymität* gegenüber dem Netz



Weitere Firefox-Funktionen

Privater Modus

- Keine **lokale** Speicherung von Daten besuchter Webseiten (insb. keine Chronik, keine URL-Vervollständigung, Cookies, etc.)
- Auf dem verwendeten PC verbleiben keine Spuren
- *Keine Anonymität* gegenüber dem Netz



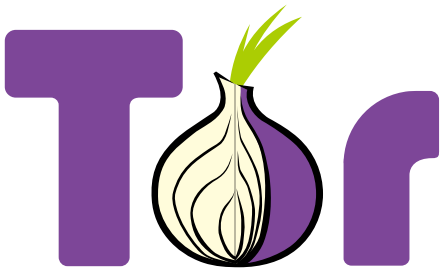
WebRTC (statt Skype)

- Firefox, Opera und Google Chrome
- Video-Telefonie **ohne Anmeldung**
- Aufbau durch Öffnen eines Links
- **Ende-zu-Ende-Verschlüsselung** mit **PFS**
- Keine starke Anonymität
- Läuft in der Amazon-Cloud
- Freie Software; eigenes Hosting möglich!

https://meet.jit.si/

Anonym surfen mit dem Tor-Browser

Tor (von „The Onion Router“)



Was ist Tor?

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

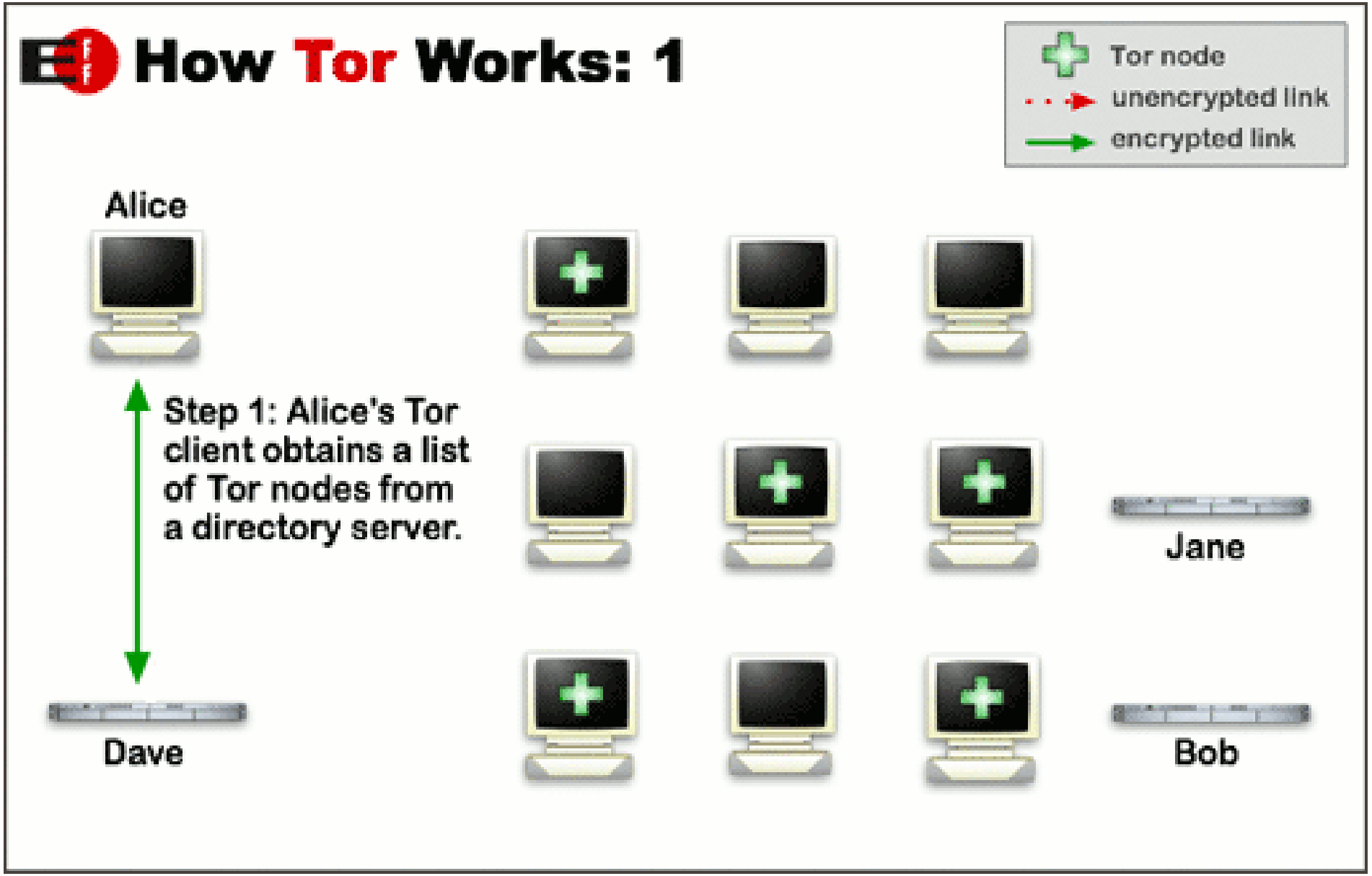
Vorteile

- Freie Software
- Anonymes Surfen

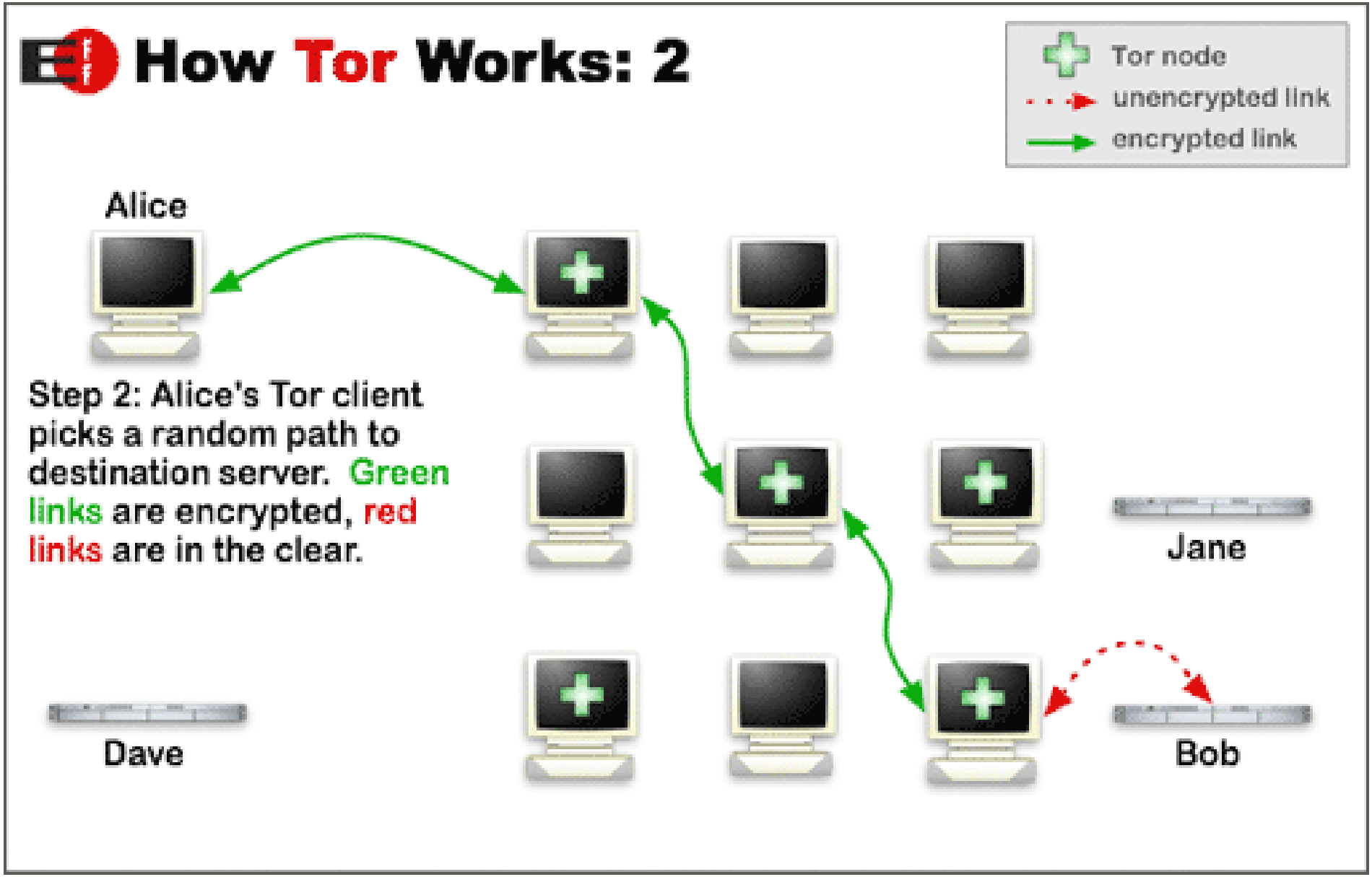
Nachteile

- Login bei personalisierten Seiten nicht sinnvoll
- Latenz ist größer

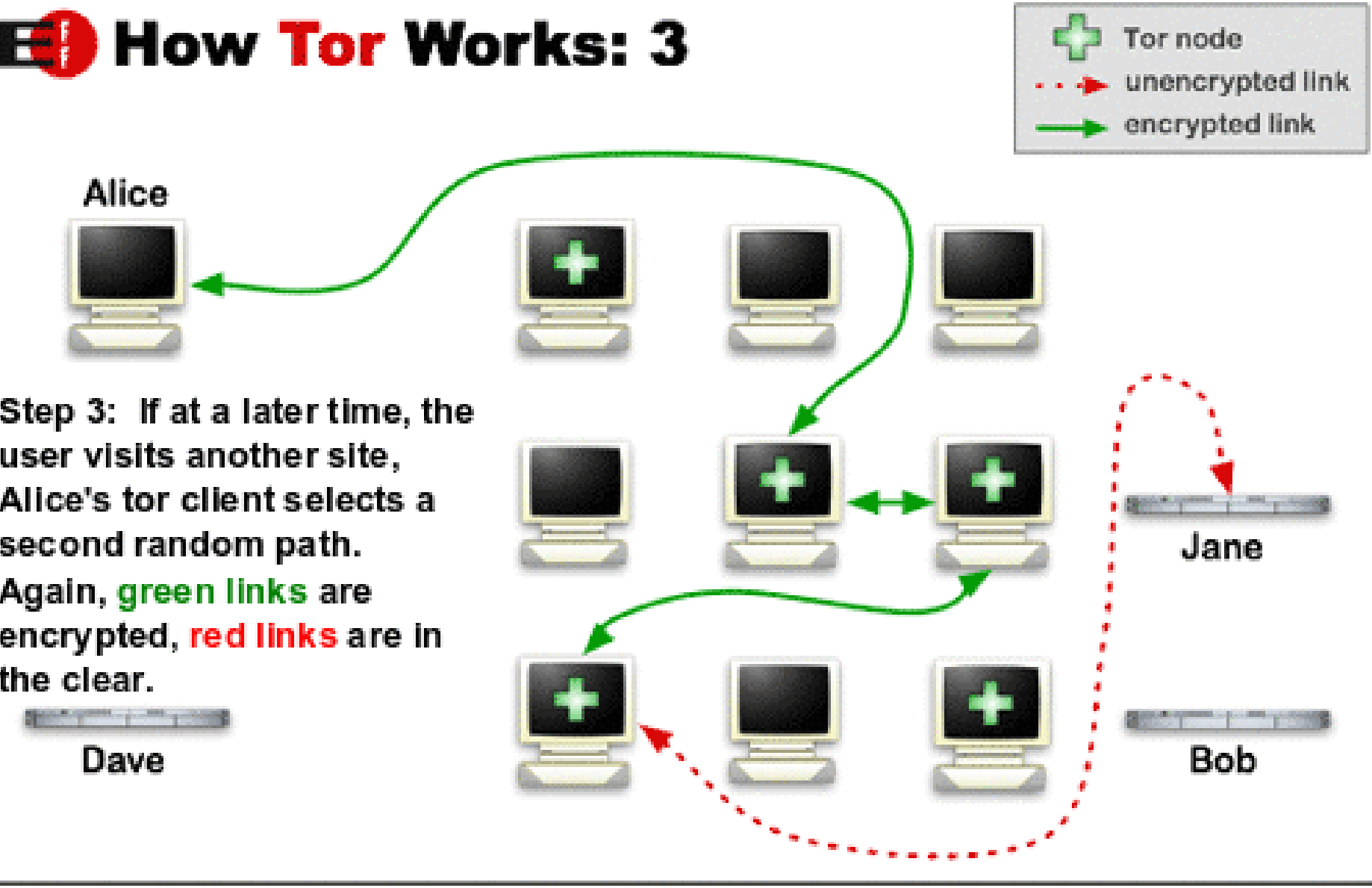
How Tor Works: 1



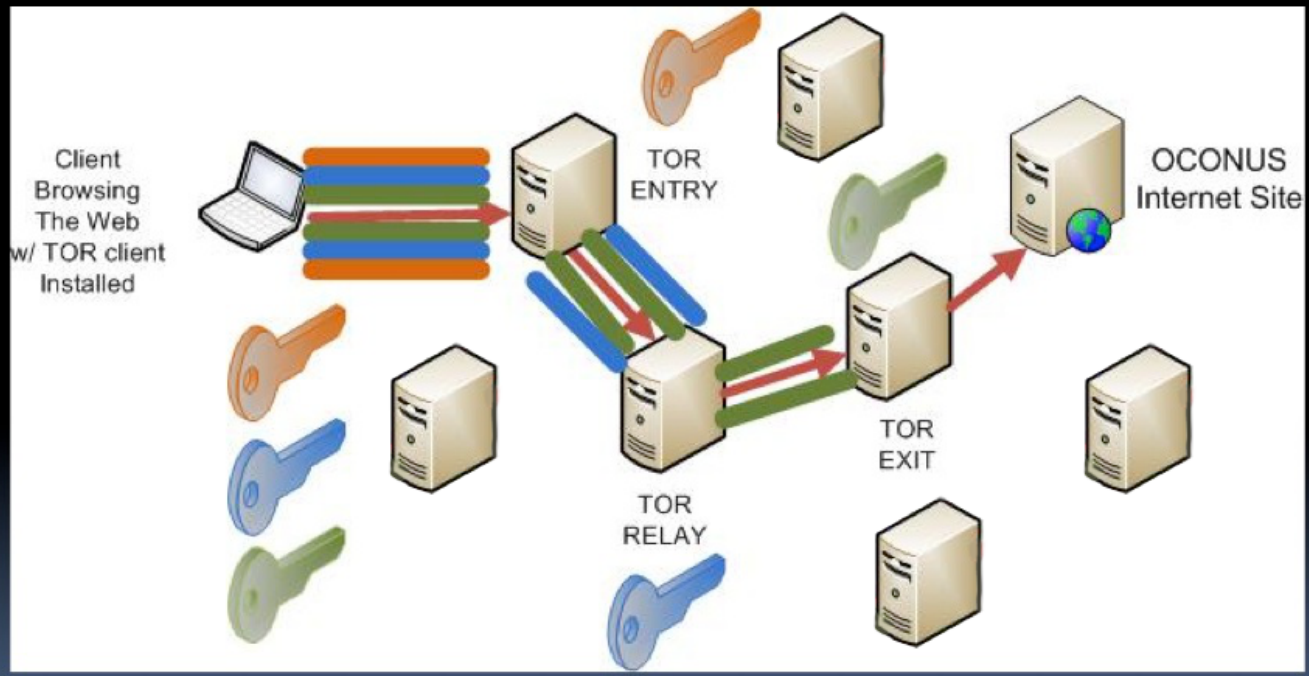
How Tor Works: 2



How Tor Works: 3



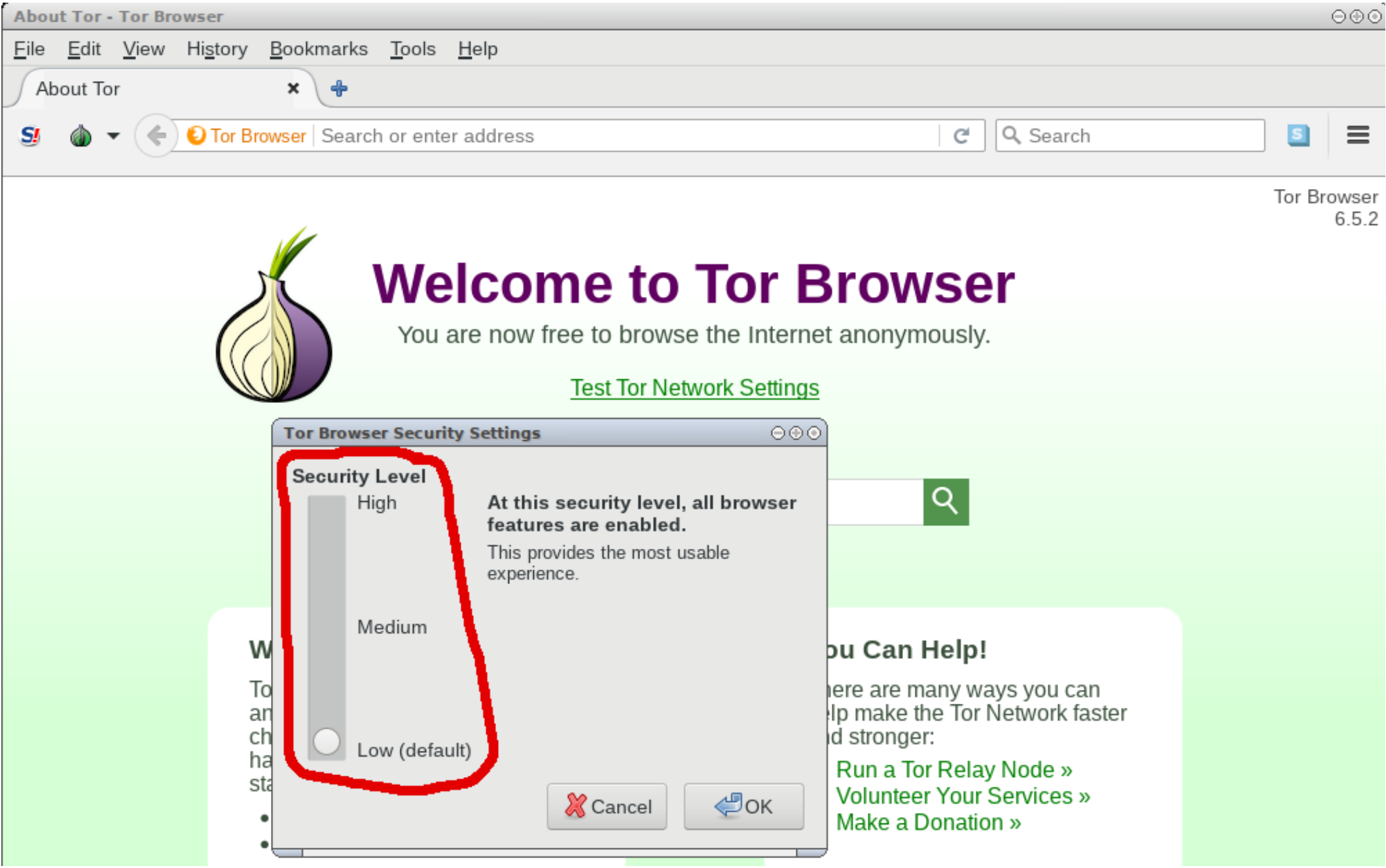
(U) What is TOR?


Client
Browsing
The Web
w/ TOR client
Installed
TOR
ENTRY
TOR
RELAY
TOR
EXIT
OCONUS
Internet Site

TOR-Browser

Firefox + TOR + NoScript + HTTPS-Everywhere

Einstellungsoptionen:


About Tor - Tor Browser
File Edit View History Bookmarks Tools Help
About Tor
Tor Browser
Search or enter address
Search
Tor Browser
6.5.2
Welcome to Tor Browser
You are now free to browse the Internet anonymously.
Test Tor Network Settings
Tor Browser Security Settings
Security Level
High
Medium
Low (default)
At this security level, all browser features are enabled.
This provides the most usable experience.
Cancel
OK
ou Can Help!
here are many ways you can
lp make the Tor Network faster
d stronger:
Run a Tor Relay Node »
Volunteer Your Services »
Make a Donation »

Installation

https://www.torproject.org/projects/torbrowser.html

Tails – ein OS für Tor

The **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

- Das 3-Browser-Konzept von Mike Kuketz https://www.kuketz-blog.de/ (Stichwort "Not my data")
- Disconnect!- und Tails-Broschüre von Capulcu https://capulcu.blackblogs.org/neue-texte/

Mobilgeräte

Überwachung

- Geheimdienste sammeln

  - tägl. rund 5 Milliarden Standortdaten von Mobiltelefonen
  - tägl. Fast 200 Millionen SMS

Überwachung

…und werten sie unter bestimmten Blickwinkeln aus

(Kontaktbeziehungen, Reisedaten, Finanztransfers, …)

…bzw. setzen die gesammelten Daten gezielt ein

(z. B. in der Ukraine Anfang 2014. SMS an Teilnehmer einer Demonstration:

"Sehr geehrter Kunde, sie sind als Teilnehmer eines Aufruhrs registriert.")

Kommerzielle Datensammelungen

- Neuer Markt für optimierte personenbezogene Werbung
- Apps sammeln diverse Nutzerdaten (z. B. Standortdaten)

App-Berechtigungen: Facebook (1)

- Geräte- & App-Verlauf
  - Aktive Apps abrufen
- Identität
  - Konten auf dem Gerät suchen
  - Konten hinzufügen oder entfernen
  - Kontaktkarten lesen
- Kalender
  - Kalendertermine sowie vertrauliche Informationen lesen
  - Ohne Wissen der Eigentümer Kalendertermine hinzufügen oder ändern und E-Mails an Gäste senden
- Kontakte
  - Konten auf dem Gerät suchen
  - Kontakte lesen
  - Kontakte ändern

App-Berechtigungen: Facebook (2)

- Standort
  - Ungefährer Standort (netzwerkbasiert)
  - Genauer Standort (GPS- und netzwerkbasiert)
- SMS
  - SMS oder MMS lesen
- Telefon
  - Telefonnummern direkt anrufen
- Anrufliste lesen
  - Telefonstatus und Identität abrufen
  - Anrufliste bearbeiten
- Fotos/Medien/Dateien
  - USB-Speicherinhalte lesen
  - USB-Speicherinhalte ändern oder löschen
- Speicher
  - USB-Speicherinhalte lesen
  - USB-Speicherinhalte ändern oder löschen

App-Berechtigungen: Facebook (3)

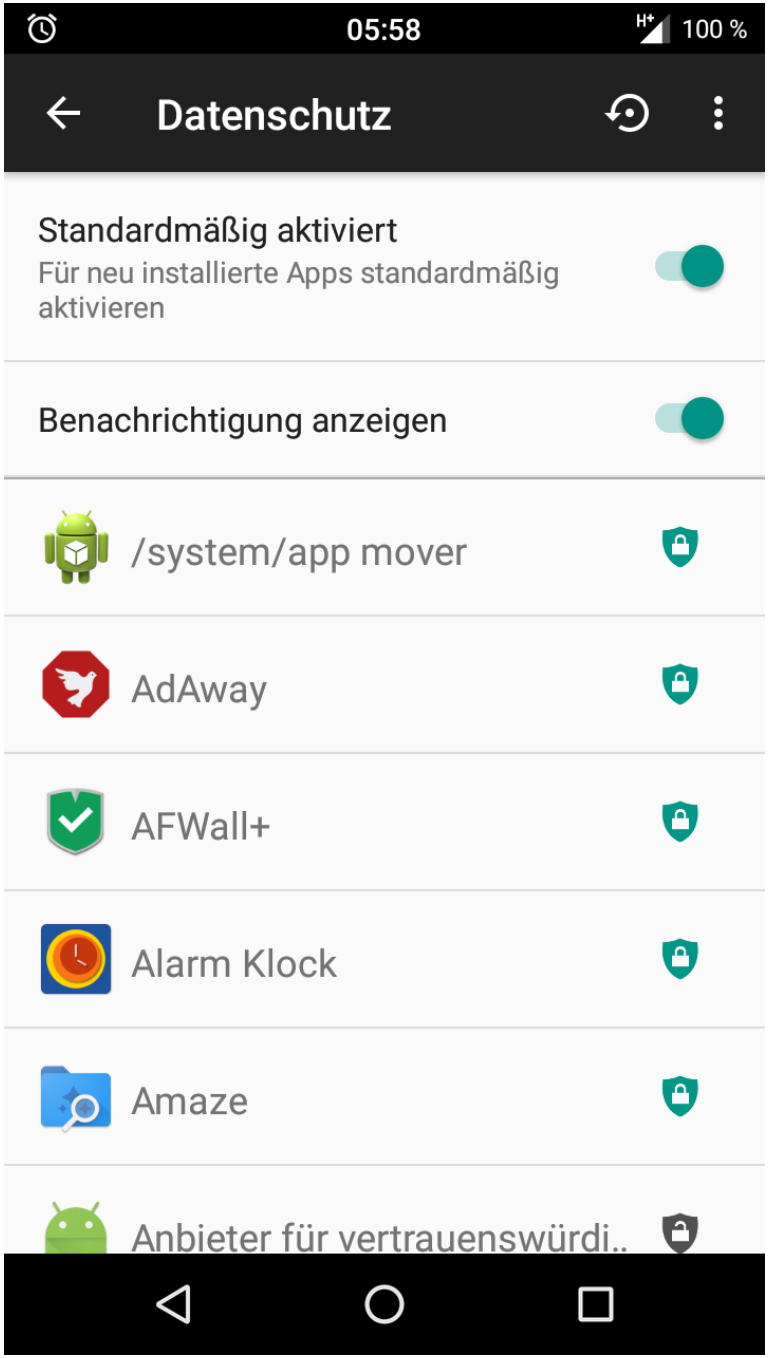
- Kamera
  - Bilder und Videos aufzeichnen
- Mikrofon
  - Ton aufzeichnen
- WLAN-Verbindungsinformationen
  - WLAN-Verbindungen abrufen
- Geräte-ID & Anrufinformationen
  - Telefonstatus und Identität

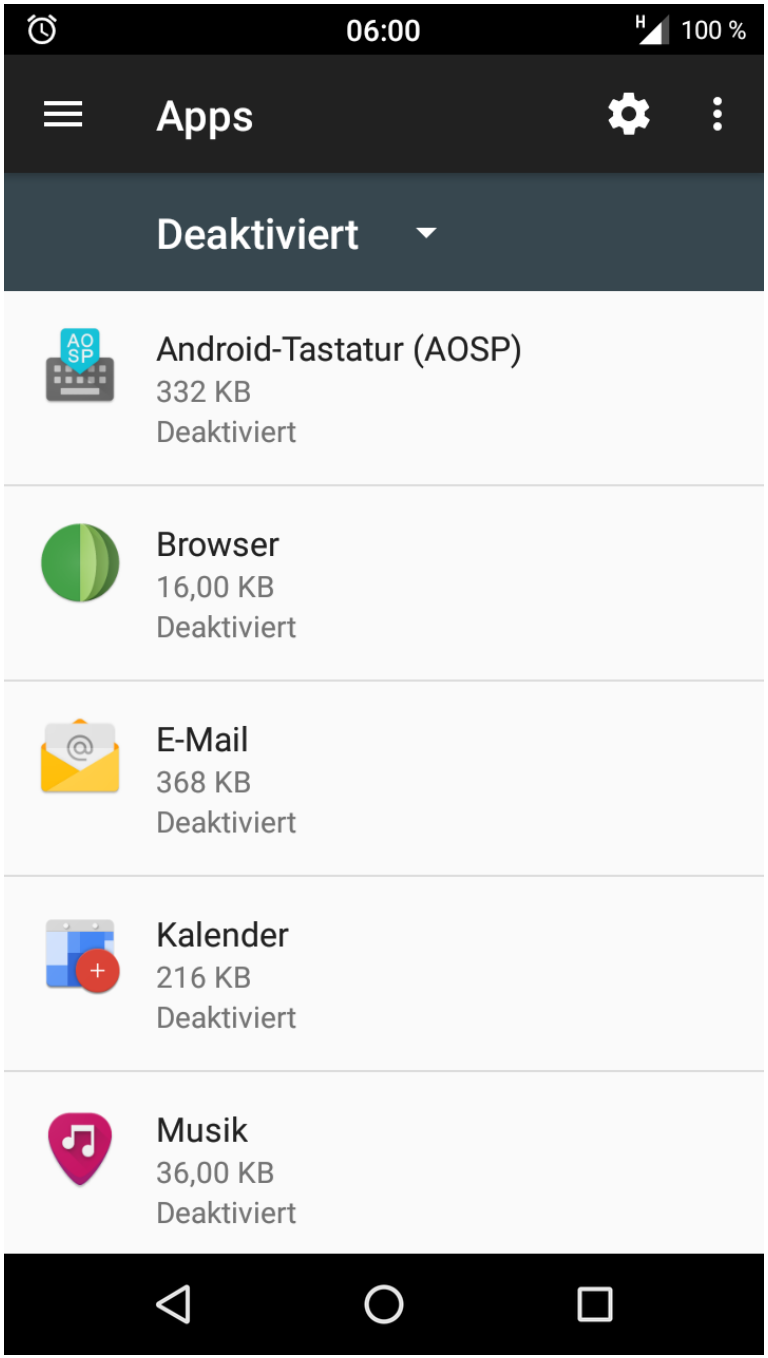
App-Berechtigungen: Facebook (4)

- Sonstige
  - Dateien ohne Benachrichtigung herunterladen
  - Größe des Hintergrundbildes anpassen
  - Daten aus dem Internet abrufen
  - Netzwerkverbindungen abrufen
  - Konten erstellen und Passwörter festlegen
  - Akkudaten lesen
  - dauerhaften Broadcast senden
  - Netzwerkkonnektivität ändern
  - WLAN-Verbindungen herstellen und trennen
  - Statusleiste ein-/ausblenden
  - Zugriff auf alle Netzwerke
  - Audio-Einstellungen ändern
  - Synchronisierungseinstellungen lesen
  - Beim Start ausführen
  - Aktive Apps neu ordnen
  - Hintergrund festlegen
  - Über anderen Apps einblenden
  - Vibrationsalarm steuern
  - Ruhezustand deaktivieren
  - Synchronisierung aktivieren oder deaktivieren
  - Verknüpfungen installieren
  - Google-Servicekonfiguration lesen

App-Berechtigungen

- Sich selbst die immer Frage stellen, ob Apps bestimmte Berechtigungen für ihre Funktion benötigen.
- Einzelne Berechtigungen von Apps entziehen.
- Alternative Apps nutzen, die weniger Berechtigungen benötigen.
- Falls verfügbar: Datenschutzmodus aktivieren!


05:58
100 %
Datenschutz
Standardmäßig aktiviert
Für neu installierte Apps standardmäßig aktivieren
Benachrichtigung anzeigen
/system/app mover
AdAway
AFWall+
Alarm Klock
Amaze
Anbieter für vertrauenswürdi..


06:00
100 %
Apps
Deaktiviert
Android-Tastatur (AOSP)
332 KB
Deaktiviert
Browser
16,00 KB
Deaktiviert
E-Mail
368 KB
Deaktiviert
Kalender
216 KB
Deaktiviert
Musik
36,00 KB
Deaktiviert

Smartphones & Tablets

- Hardware („Super-Wanze“)
  - Mikrofon, Kamera, GPS, Bewegungssensor
- Betriebssystem
  - iOS (Apple) oder Windows Phone/Mobile (Microsoft) = Pest oder Cholera
  - Apps nur aus einer Quelle (zentraler App-Store)
  - Geschlossene Systeme, keine Gerätehoheit
  - Mehr Freiheit durch Jailbreak (Gefängnisausbruch)

Android

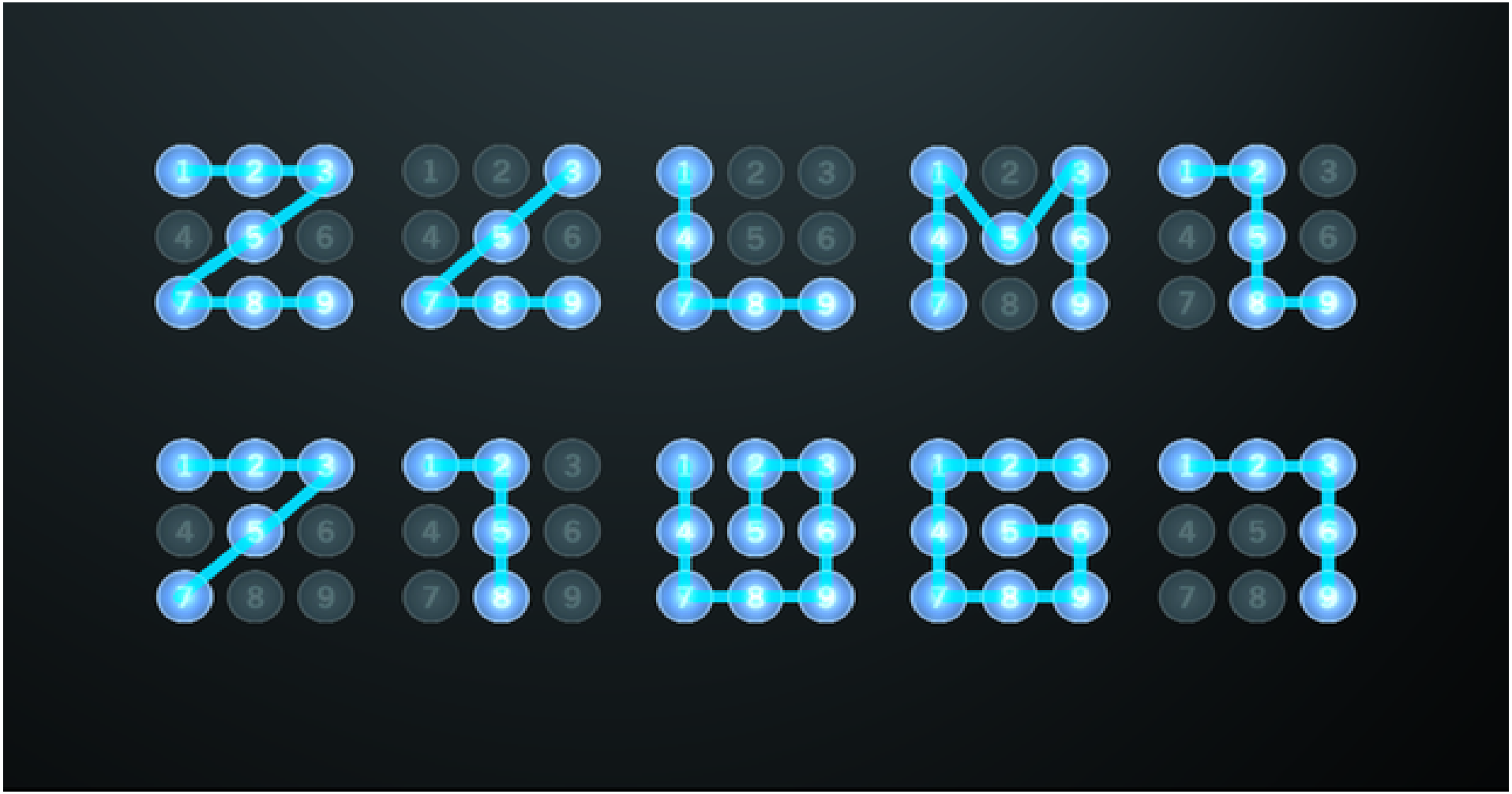
- Theoretisch gute Basis
  - Linux-basiert, Freie Software

- **Aber:** tiefe Integration proprietärer Google-Software
  - Suche, Browser, Gmail, Maps, Kalender- / Kontakte-Sync …
  - Play Store & Google-Dienste
  - Fernzugriff, Datenübermittlung
  - standardmäßig keine Gerätehoheit
  - Je nach Hersteller oft nur zwei Jahre lang Sicherheitsupdates

Erste Schritte: Konfiguration

- Sichere Bildschirmsperre
  - von unsicher zu sicherer:
    Wischgeste, Muster, Biometrisch, PIN, Passwort
- Speicher verschlüsseln
- WLAN, GPS, Bluetooth, etc. ausschalten, wenn nicht genutzt
- Browser (Firefox) gegen Tracking schützen

Typische Wischgesten



Super sichere Iris-Scanner?

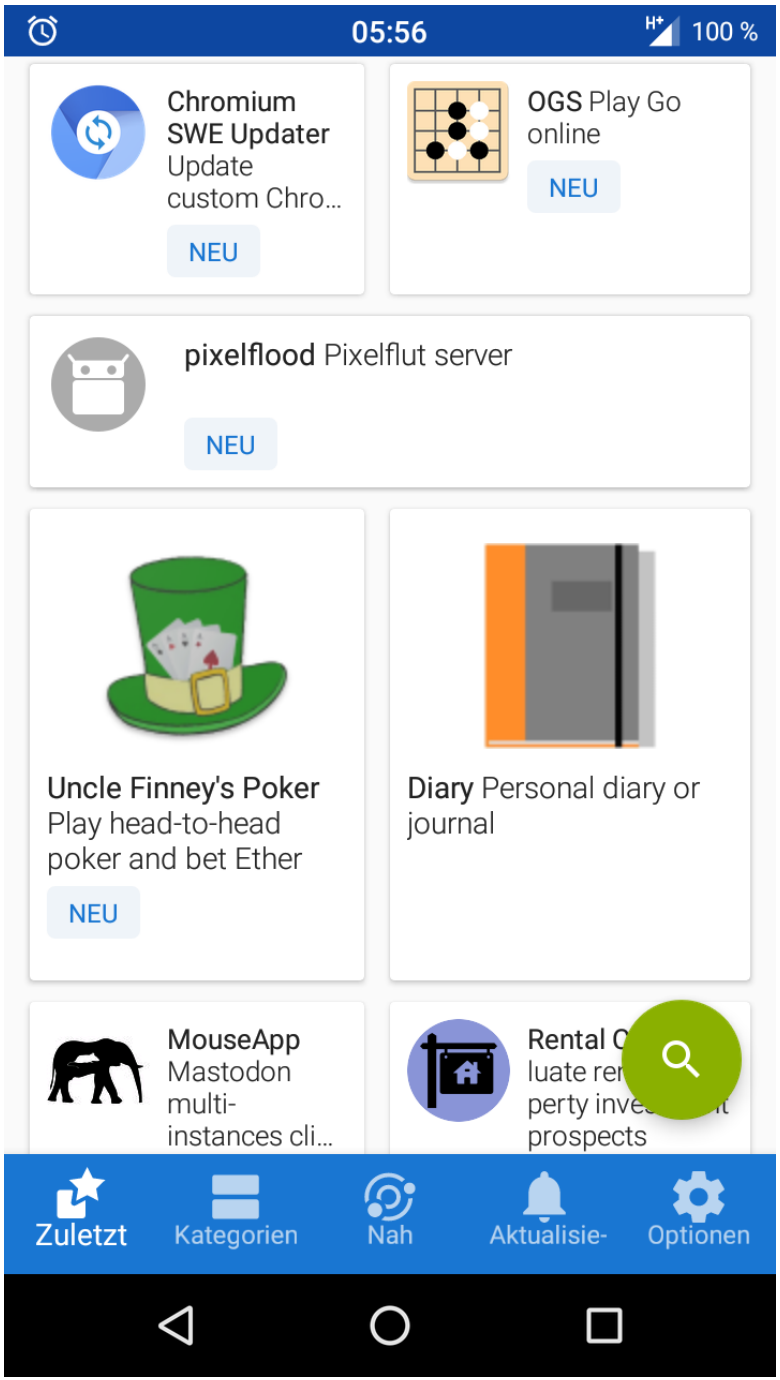
https://media.ccc.de/v/biometrie-s8-iris-fun

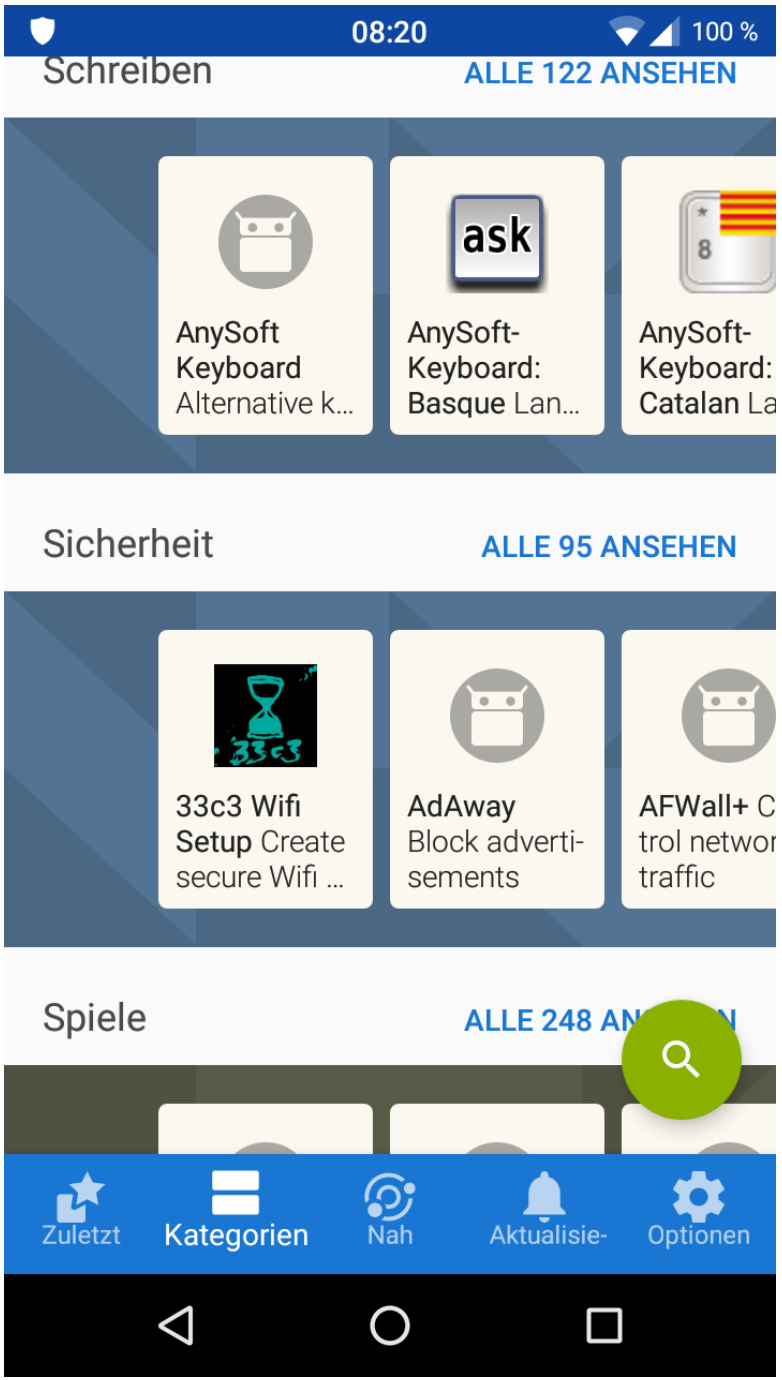
Android ‚entgoogeln‘

1. Unnötiges entfernen
   - Google-Einstellungen (G+, Standort, Suche, Werbe-ID, usw.)
2. Alternativ-Dienste nutzen
   - Browser, Suche, Mail, Sync für Kalender / Kontakte...
3. Play Store löschen / F-Droid nutzen
   - App-Alternativen nutzen
4. Freie Android-Variante installieren
   - z.B. LineageOS, Replicant

Empfehlenswerte Apps: F-Droid

- Alternative/Ergänzung zum Play Store: **F-Droid**
  - **https://f-droid.org/**
- Ausschließlich Software/Apps unter freier Lizenz
- Kein Nutzerkonto erforderlich
- Ergänzungen zum offiziellen F-Droid-Repository können von allen vorgeschlagen werden
- Es ist möglich, private Repositories zur Verfügung zu stellen und einzubinden
- Auch direkter Download von Apps über die Website möglich (dann keine automatischen Updates)


05:56
100 %
Chromium SWE Updater Update custom Chro...
NEU
OGS Play Go online
NEU
pixelflood Pixelflut server
NEU
Uncle Finney's Poker Play head-to-head poker and bet Ether
NEU
Diary Personal diary or journal
MouseApp Mastodon multi-instances cli...
prospects
Zuletzt
Kategorien
Nah
Aktualisie-
Optionen


08:20
100 %
Schreiben
ALLE 122 ANSEHEN
AnySoft Keyboard Alternative k...
AnySoft-Keyboard: Basque Lan...
AnySoft-Keyboard: Catalan La
Sicherheit
ALLE 95 ANSEHEN
33c3 Wifi Setup Create secure Wifi ...
AdAway Block adverti-sements
AFWall+ C trol networ traffic
Spiele
Zuletzt
Kategorien
Nah
Aktualisie-
Optionen

Ansprüche an Messenger

- Für alle gängigen Betriebsysteme verfügbar
- Ende-zu-Ende-Verschlüsselung
- Sicherer Verschlüsselungsalgorithmus (AES)
- Dezentralität / Möglichkeit für eigene Server
- Quelloffen (Überprüfung durch unabhängige Experten)
- Upload von Daten (z.B. Adressbuch) nur mit ausdrücklicher Bestätigung des Nutzers
  - Adressbuch enthält Daten anderer Personen → Upload erlaubt?
- Unabhängige Installation und Betrieb
  - z.B. ohne Google Play Store & Google-Dienste

Messenger-Vergleich

	Signal	Telegram	Surespot	Threema	WhatsApp
Freie Software	ja	teils	ja	nein	nein
Ende-zu-Ende-Verschlüsselung	ja	(ja)	ja	(ja)	(ja)
unabhängiges Audit	ja	ja	nein	(ja)	nein
Adressbuch-Zugriff	ja	ja	nein	(nein)	(nein)
Nicknames (Pseudonyme)	nein	nein	ja	ja	nein
außerhalb Play-Store erhältlich	ja	ja	nein	ja	ja
funktioniert ohne Google-Dienste	ja	ja	nein	ja	nein
Verbreitung	mittel	weit	kaum	mittel	sehr weit

Empfehlenswerte Messenger

- **Conversations** (Android) bzw.

  ChatSecure (iOS)

  - Nutzen das offene **XMPP** (Jabber) als Protokoll, das im Gegensatz zu anderen Messengern dezentrale Kommunikationsstrukturen erlaubt
  - Unterstützen verschlüsselte Chats via OpenPGP, OTR und OMEMO
  - Verfügbar via F-Droid (Conversations) bzw. App Store (ChatSecure)
  - Conversations auch im Play Store, allerdings nicht kostenlos

Alternative zu WhatsApp & Co

- **Signal** (Android, iOS)
  - Freie Software
  - Sicherer Verschlüsselungsalgorythmus
  - Unterstützt verschlüsselte Text- und Sprachnachrichten, Telefonie und SMS.
  - Telefonnummer zwingend erforderlich, zentrale Struktur
  - Kostenlos im Play bzw. App Store, für Android auch als APK:
    - https://signal.org/android/apk/

Empfehlenswerter Browser

- **Mozilla Firefox**
  - Freie Software
  - Auch unter Android und iOS durch Add-ons erweiterbar (uBlock Origin, NoScript, HTTPS Everywhere etc.)
  - Konfiguration ähnlich zur Desktop-Version

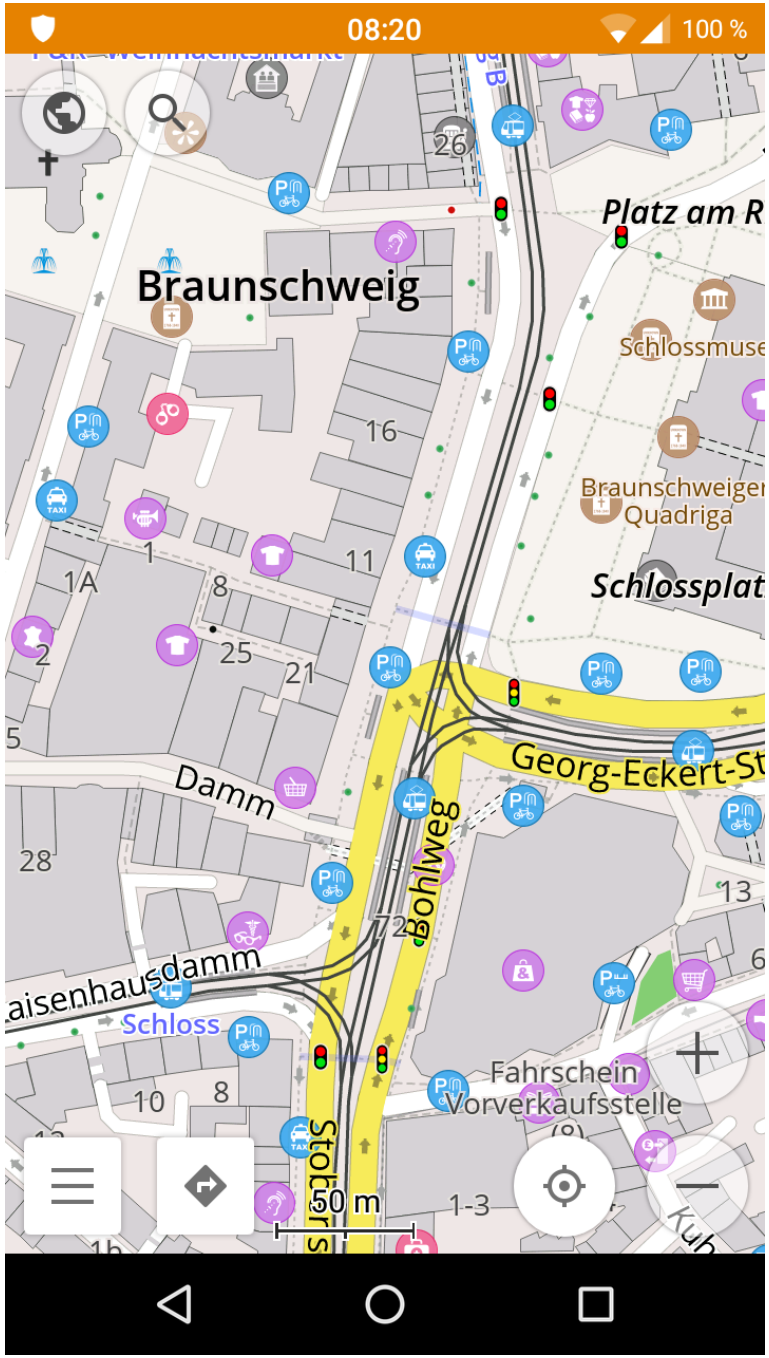
Empfehlenswerter E-Mail-Client

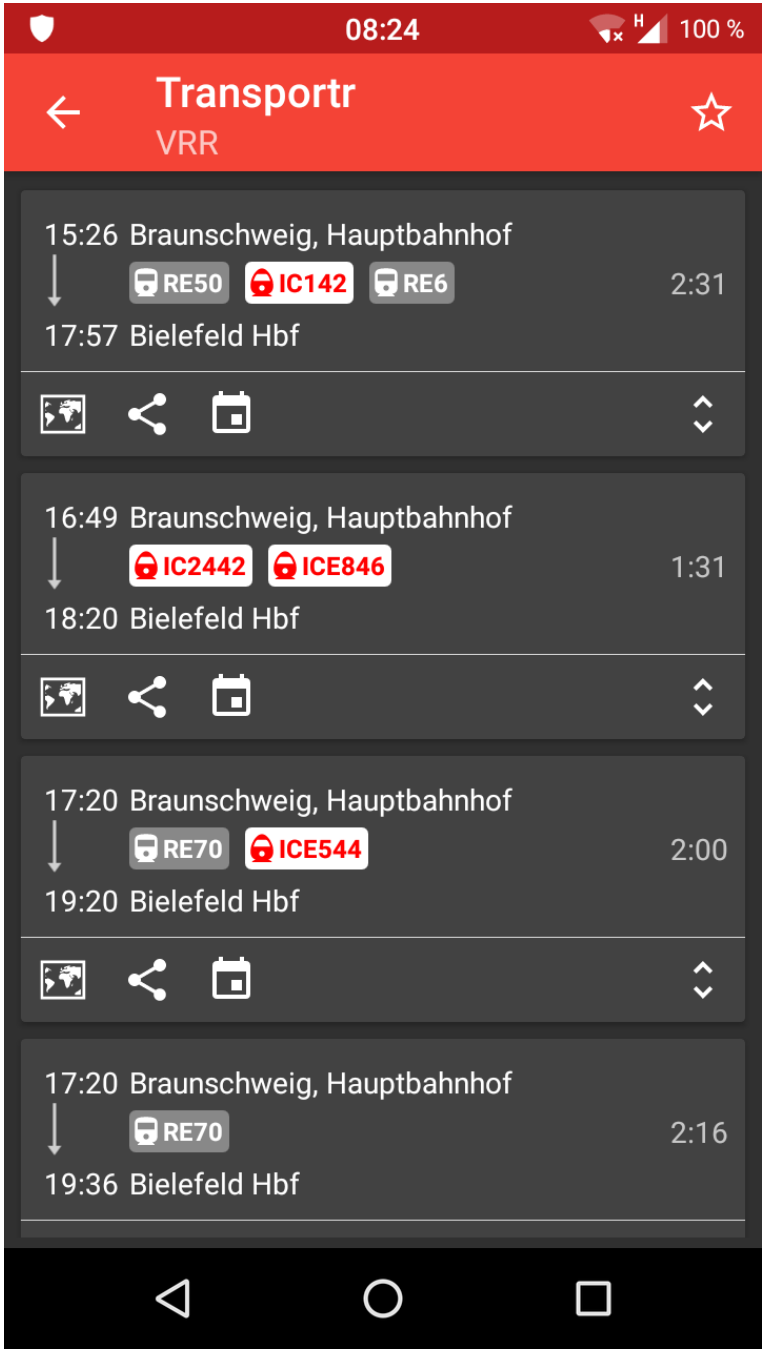
- **K-9 Mail**
  - sehr funktionaler und freier Mail-Client
  - unterstützt IMAP/POP3
  - kann verschlüsselte Mails via PGP/MIME senden und empfangen

- **OpenKeychain**
  - Implementierung von OpenPGP unter Android
  - agiert außerdem als Schlüsselverwaltung
  - Problem: private Schlüssel auf Mobilgerät zu gefährdet?

Weitere empfehlenswerte Apps

- **Transportr**
  - Fahrpläne des öffentlichen Nahverkehrs & Verbindungssuche
- **VLC**
  - Video- und Audioplayer
- **OsmAnd**
  - Karten- und Navigationssoftware auf Basis von OpenStreetMap
  - unterstützt auch Offline-Karten


08:20
100 %
Braunschweig
Platz am R
Schlossmuse
Braunschweiger
Quadriga
Schlossplat
Georg-Eckert-St
Damm
Bohlweg
aisenhausdamm
Schloss
Fahrschein
Vorverkaufsstelle
Stobr s
50 m
1-3
Kuh


08:24
100 %
Transportr
VRR
15:26 Braunschweig, Hauptbahnhof
RE50 IC142 RE6
2:31
17:57 Bielefeld Hbf
16:49 Braunschweig, Hauptbahnhof
IC2442 ICE846
1:31
18:20 Bielefeld Hbf
17:20 Braunschweig, Hauptbahnhof
RE70 ICE544
2:00
19:20 Bielefeld Hbf
17:20 Braunschweig, Hauptbahnhof
RE70
2:16
19:36 Bielefeld Hbf

Links & Literatur

PRISM Break zu Android & iOS

- https://prism-break.org/de/categories/android/
- https://prism-break.org/de/categories/ios/

Mike Kuketz: Your phone Your data – Android ohne Google?!

- https://www.kuketz-blog.de/your-phone-your-data-teil1/

Digitalcourage: Digitale Selbstverteidigung

- https://digitalcourage.de/digitale-selbstverteidigung/mobil

Weitere Projekte

- **PRISM Break:** (https://prism-break.org/de/all/)
  Liste datenschutzfreundlicher Software und Anbieter
- **Digitalcourage: Digitale Selbstverteidigung**
  (https://digitalcourage.de/digitale-selbstverteidigung)
  - Übersichts-Flyer hier im Raum zum Mitnehmen!
- **Cryptopartys!**
  - https://www.cryptoparty.in/ (auf Englisch)

Anlaufstellen in Braunschweig

- **Hackspace Stratum 0 & Freifunk Braunschweig**
  - https://stratum0.org/

- **Digitalcourage: Ortsgruppe Braunschweig**
  - Trifft sich jeden zweiten Donnerstag um 18:30 Uhr (nächstes Treffen am 1. Juni)
  - https://digitalcourage.de/mitmachen/digitalcourage-treffen-vor-ort

Vielen Dank
für die Aufmerksamkeit

Fragen?!