Crypto-Seminar Dörentrup

3. Juli 2019

Kurze Vorstellung

- Georg Gottleuber
- Jan Schötteldreier

Digitalcourage e.V.

- Gemeinnütziger Verein für Datenschutz und Bürgerrechte
  - „für eine lebenswerte Welt im digitalen Zeitalter“
  - Big Brother Awards
  - Aktionen zu aktuellen Themen

- Digitalcourage-Hochschulgruppe Bielefeld ***(digitalcourage.de/hsg-bi)***
  - CryptoPartys, Backup-Partys, Linux-Install-Partys
  - regelmäßige Treffen an der Uni

CryptoParty

- Digitale Selbstverteidigung
- Schutz vor Massenüberwachung
- einsteigerfreundlich
- öffentlich, nicht-kommerziell, weltweit
- von AnwenderInnen für AnwenderInnen
- Mach mit und werde Teil der CryptoParty-Bewegung!

- https://cryptoparty.in

Das Seminar im Überblick

- **Warum sollte ich eigentlich verschlüsseln?**
  - Vortrag: 10:00 bis 10:45 Uhr
- **Browser**
  - Vortrag: 10:45 bis 11:30 Uhr
  - Praxis: bis 12:30 Uhr
- **Passwörter & Dateiverschlüsselung**
  - Vortrag: 14:00 bis 14:45 Uhr
- **Smartphones**
  - Vortrag: 14:45 bis 15:45 Uhr
  - Praxis bis 17:00 Uhr

Datenhandel und -verwertung

- Doku: Der gläserne Deutsche

Welche Daten nutzt Facebook?

- Ort; Alter; Geschlecht; Bildungsniveau; Einkommen und Eigenkapital;
- Hausbesitz und Hauswert; Grundstücksgröße; Hausgröße in Quadratmetern;
- Nutzer, die frisch verheiratet sind; Beziehungsstatus;
- Nutzer, die planen, ein Auto zu kaufen (welche Art/Marke, und wann);
- Betriebssystem, Emailanbieter, Art der Internetverbindung;
- Nutzer, die Browserspiele spielen;
- Nutzer, die eine Facebook-Veranstaltung erstellt haben;
- Anzahl der Kredite;
- Nutzer, die aktiv eine Kreditkarte benutzen;
- Arten von Kleidung, die der Haushalt des Nutzers kauft;
- Die Zeit im Jahr, in der der Haushalt des Nutzers am meisten einkauft;
- **Nutzer, die „sehr viel“ Bier, Wein oder Spirituosen kaufen;**
- **Nutzer, die Medikamente gegen Allergien und Schnupfen/Grippe, Schmerzmittel und andere nicht-verschreibungspflichtige Arzneimittel einkaufen;**
- **Nutzer, die „empfänglich“ [sind] für [Werbung zu] Online-Autoversicherungen, Hochschulbildung oder Hypotheken, Prepaid-Debitkarten und Satellitenfernsehen;**
- Wie lange der Nutzer sein Haus bereits bewohnt;
- Nutzer, die wahrscheinlich bald umziehen;
- etc.

Privatsphäre

Privatsphäre – was ist das?

Juristische Perspektive:

- „Datenschutz beobachtet, beurteilt und gestaltet die asymmetrischen Machtbeziehungen zwischen mächtigen **Organisationen** (Risikogebern) und im Grundsatz selbstständig agierenden **Personen** (Risikonehmer).“
  - Abwehr der Machtasymmetrie zum Schutz des Individuums!

Privatsphäre – was ist das?

Philosophische Perspektive:

- „Privat ist etwas genau dann, wenn man den Zugang dazu kontrollieren kann.“ (Rössler, 2001)

Quelle: Rössler, Beate (2001): Der Wert des Privaten. Frankfurt: Suhrkamp

Warum brauchen wir Privatsphäre?

- „the right to be left alone“
- Freie Entfaltung der Persönlichkeit
- Kontrolle über die Folgen des eigenen Handelns
- Selbstbestimmung (wer weiß was von mir)
- Schutz vor Kritik und Diskriminierung
- Sicherheit (Passwörter, Eigentum, ...)
- Freiheit
- Intimität?
  - **WICHTIG FÜR DAS INDIVIDUUM**

Warum brauchen wir Privatsphäre?

- Wichtig für die Gesellschaft:
- essentiell für Demokratie und Rechtsstaat:
  - Verschwiegenheitspflicht (Medizin, Recht, Beratung, ...)
  - Journalismus (Quellenschutz)
  - Abwehrrecht gegen die Staatsmacht
- soziale Rollen (unterschiedliches Verhalten)
- Fortschritt ermöglichen (Opposition zulassen)
  - sobald Offenlegung sich zur sozialen Norm entwickelt, wird das Gegenteil zum Stigma
  - **WICHTIG FÜR DIE GESELLSCHAFT**

Was ist, wenn die Privatsphäre verletzt wird?

- Erpressbarkeit
- Chilling Effects: Selbstbeschränkung der Meinungsfreiheit
- Konformes Verhalten
- ...

Digitale Identität

Google-Dienste

Zu niemandem ist man ehrlicher als zum Suchfeld von Google.

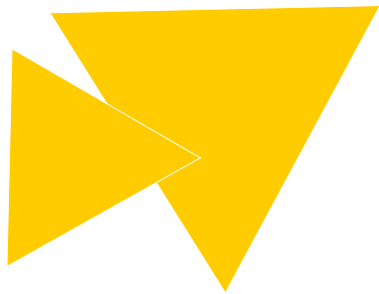
Constanze Kurz, Chaos Computer Club

Facebook

- „kostenlos“
- Datenschutzeinstellungen werden immer schwieriger
- Klarnamenpflicht
- Rechte an den Daten
- Intransparenz bei der Weitergabe
- Lock-In (kein Profil-Export)

Datenwirtschaft

- „kostenlose“ Angebote
  - Daten sind eine neue Währung
  - Datenhändler kaufen Profile und verkaufen sie an die Werbeindustrie, Versicherungen, Schufa, etc.
- Geschlossene Systeme
  - proprietäre Software
  - keine offenen Schnittstellen
- Big Data
  - Zusammenführung, Analyse und Auswertung großer Datenmengen

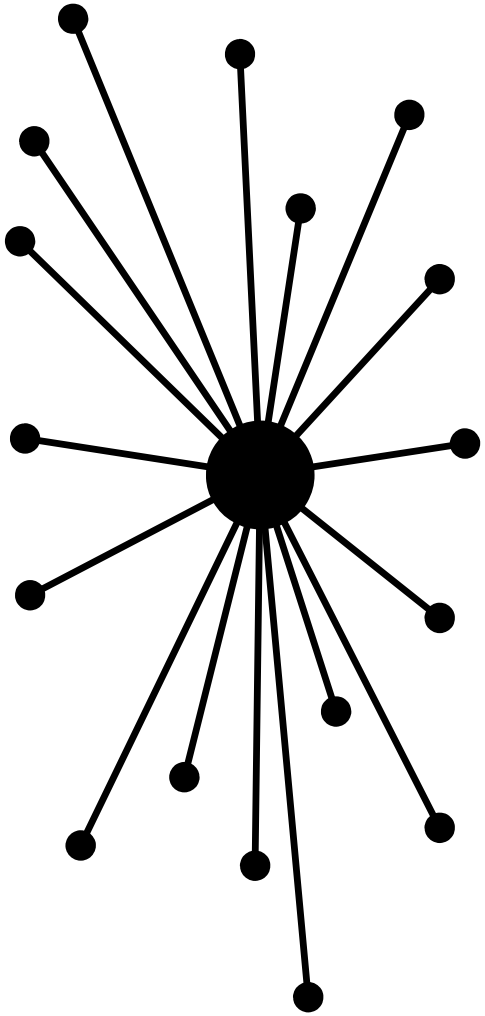


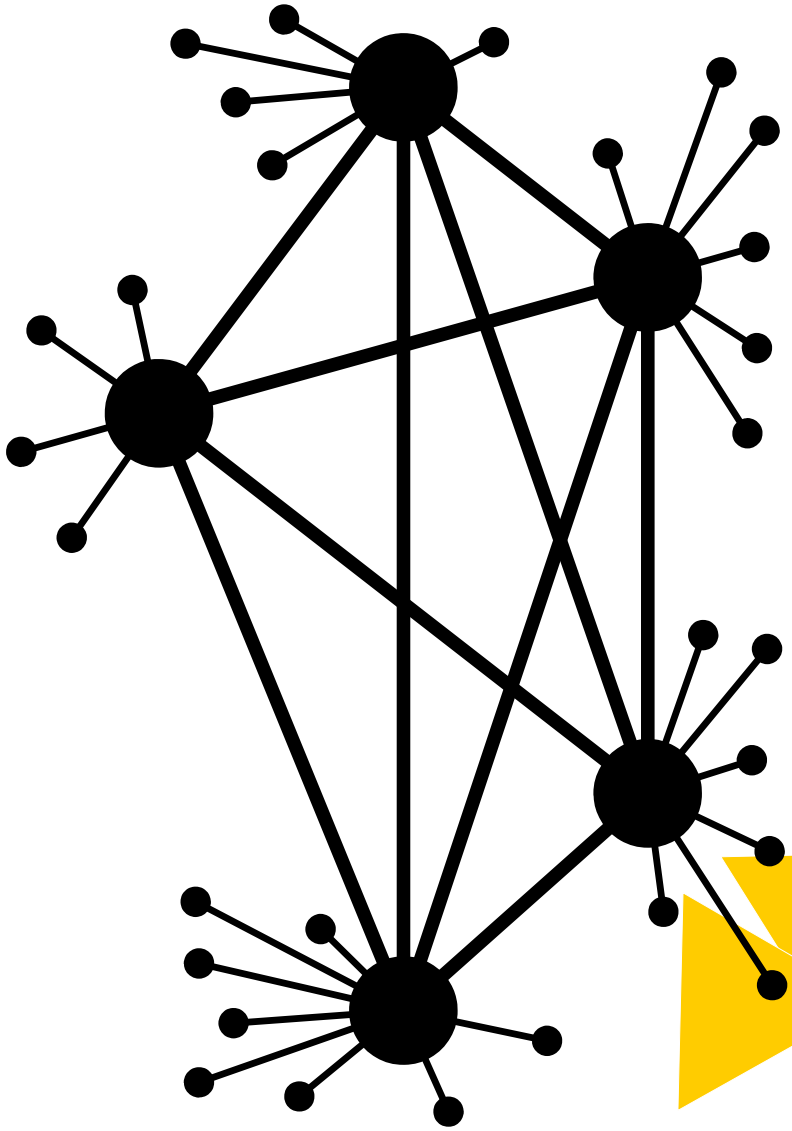
Datenwirtschaft

- Sicherheit
  - Bedeutet Aufwand = Kosten
- Datenschutz
  - Weniger Daten für das Unternehmen
  - Weniger Rohmaterial zum Analysieren und Verkaufen
  - Privatsphäre "überholt"?
- Die DSGVO hat Datenschutz in Europa wieder stark gemacht

Wichtige Begriffe und Begebenheiten

zentral vs. dezentral





Begriff: Metadaten

- Inhalt
- Metadaten (Nachricht)
  - Absender, Empfänger
  - Datum, Uhrzeit
  - IP-Adresse / Mobilfunknetz
- Metadaten (Foto)
  - Auflösung
  - Blende, Belichtungszeit
  - GPS Koordinaten

Metadaten

- In der Telekommunikation häufig Verbindungsdaten genannt.
- Kleine Datenmenge
- Leicht zu analysieren (im Gegensatz zu Inhalt)
- Schwierig zu verschlüsseln, da notwendig um die Kommunikation zu ermöglichen
- **Metadaten eignen sich perfekt zur Datenanalyse und Massenüberwachung!**

Metadaten – wo ist das Problem?

- **Kleine Datenmenge, aber sehr viel Wissen** über Nutzer.innen:
  - Interessen, Krankheiten, sexuelle Vorlieben, Bewegungsprofil, …
- leicht zu **analysieren** (im Gegensatz zu Inhalt)
- **Zusammenführung** von Daten verschiedener Quellen
  - Suche, YouTube, Gmail, Analytics, AdWords, Android, …
- **Big Data**: Suchtrends (regional, weltweit)
- **Datenhandel**: Werbung, Kreditwürdigkeit, Versicherungen …
- schwierig zu verschlüsseln, da **notwendig**, um die Kommunikation zu ermöglichen

We Kill People Based on Metadata

General Michael Hayden, Ex-Chef von NSA und CIA

Massenüberwachung findet in gigantischem Ausmaß statt

- Flächenvergleich Stasi vs. NSA: https://apps.opendatacity.de/stasi-vs-nsa/

Leseempfehlungen

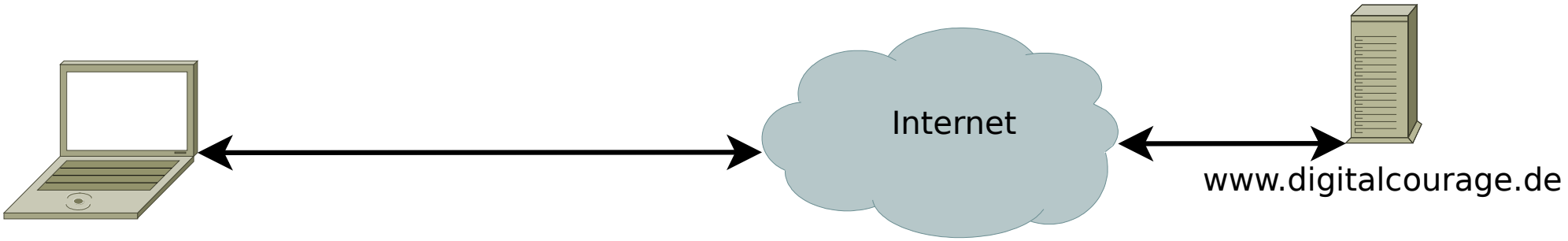
- Buch: „Die globale Überwachung“ (Glenn Greenwald)
- https://netzpolitik.org
- Buch: „was Google wirklich will“ (Thomas Schulz)
- Videos: http://www.alexanderlehmann.net/

Sicher unterwegs im Web: Browser mit Privatsphäre

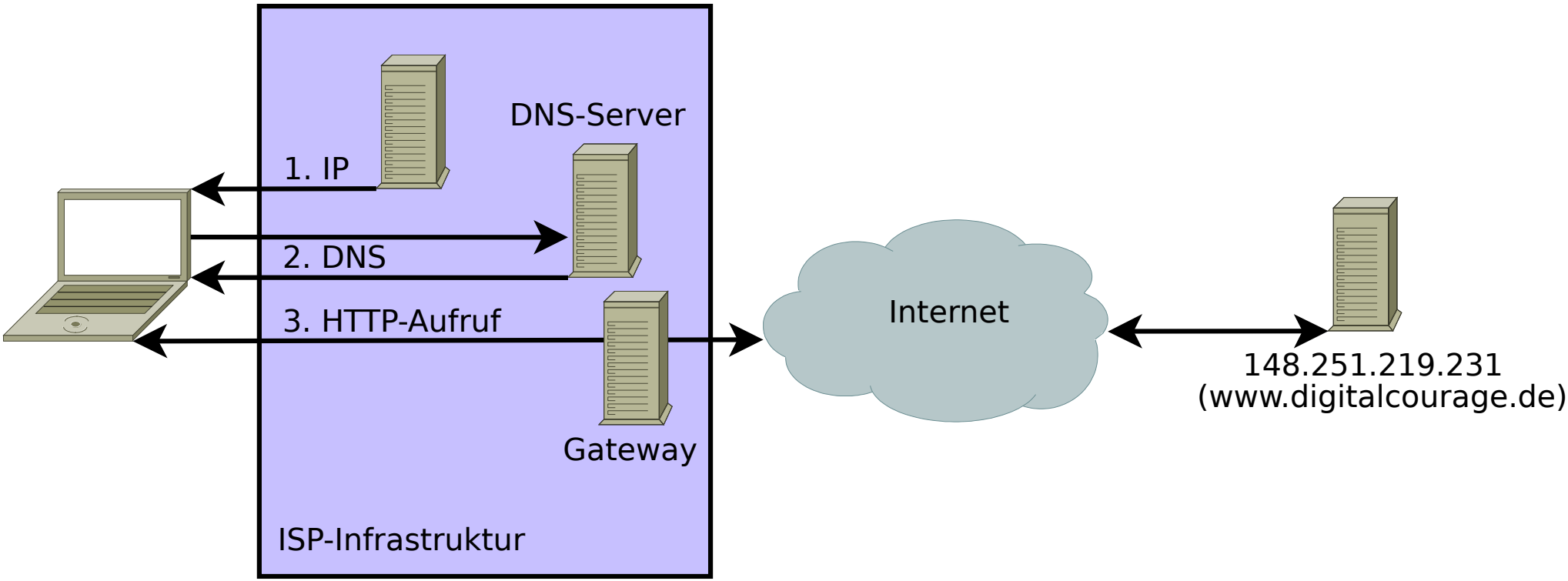
Freie Software

- **Freiheit 0**: Die Freiheit, das Programm auszuführen, wie man möchte, für *jeden Zweck.*
- **Freiheit 1**: Die Freiheit, die Funktionsweise des Programms zu untersuchen und eigenen Bedürfnissen der Datenverarbeitung anzupassen.
- **Freiheit 2**: Die Freiheit, das Programm weiterzuverbreiten und damit seinen Mitmenschen zu helfen.
- **Freiheit 3**: Die Freiheit, das Programm zu verbessern und diese Verbesserungen der Öffentlichkeit freizugeben, damit die gesamte Gemeinschaft davon profitiert.
- ⇒ viel mehr als Open Source (Quelltexte offenlegen)

Wie funktioniert das Web?



Und technisch?

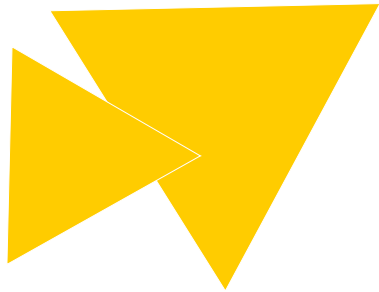


Wie schrecklich ist die Web-Realität (mit Standardeinstellungen)?

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

… so schrecklich!

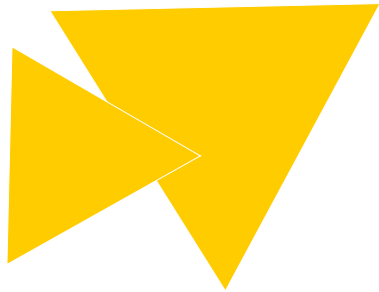
- Beispiel: **https**://www.spiegel.de/ (mit Standard-Firefox 67)
- 424 (nach 20s) Anfragen an mehr als 56 externe Server...
- www.spiegel.de, magazin.spiegel.de, cdn1.spiegel.de, count.spiegel.de, fsm2.spiegel.de, m.spiegel.de



… so schrecklich!

- Beispiel: **https**://www.spiegel.de/ (mit Standard-Firefox 67)
- 424 (nach 20s) Anfragen an mehr als 56 externe Server...
- www.spiegel.de, magazin.spiegel.de, cdn1.spiegel.de, count.spiegel.de, fsm2.spiegel.de, m.spiegel.de

fsm2.spiegel.de => dqdhughtuysrk.cloudfront.net

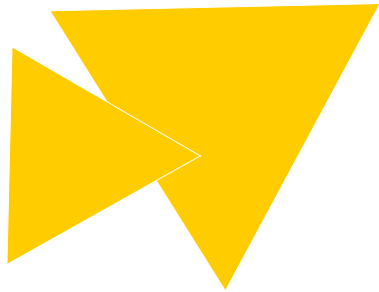


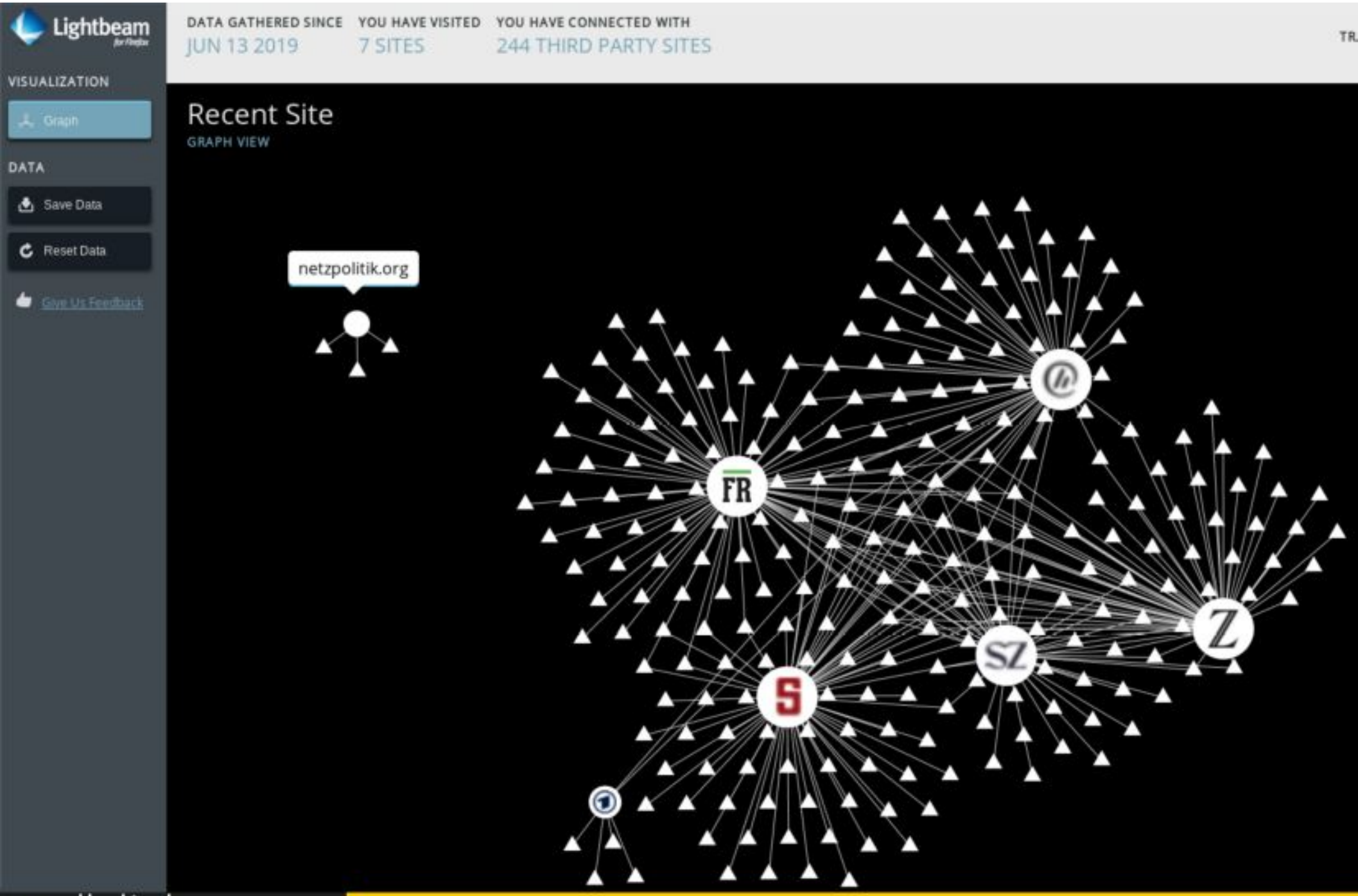
… so schrecklich!

- ioam.de, **google**tagmanager.com, omny.fm, cloudfront.net, mxcdn.net, optimizely.com, soundcloud.com, demdex.net, adalliance.io, emsservice.de, emetriq.de, criteo.net, s79.research.de.com, meetrics.net, omtrdc.net, criteo.com, **doubleclick**.net, hotjar.com, **google**-analytics.com, **google**tagservices.com, yieldlab.net, everesttech.net, xplosion.de, **google**apis.com, ampcid.**google**.com, adservice.**google**.de, ampcid.**google**.de, srv-2019-06-13-05.pixel.parsely.com, theadex.com, newrelic.com, adrtx.net, nr-data.net, ligatus.com, ligadx.com, summerhamster.com, zemanta.com, scorecardresearch.com, outbrain.com, **google**syndication.com, csi.**gstatic**.com, … (ohne Subdomains!)

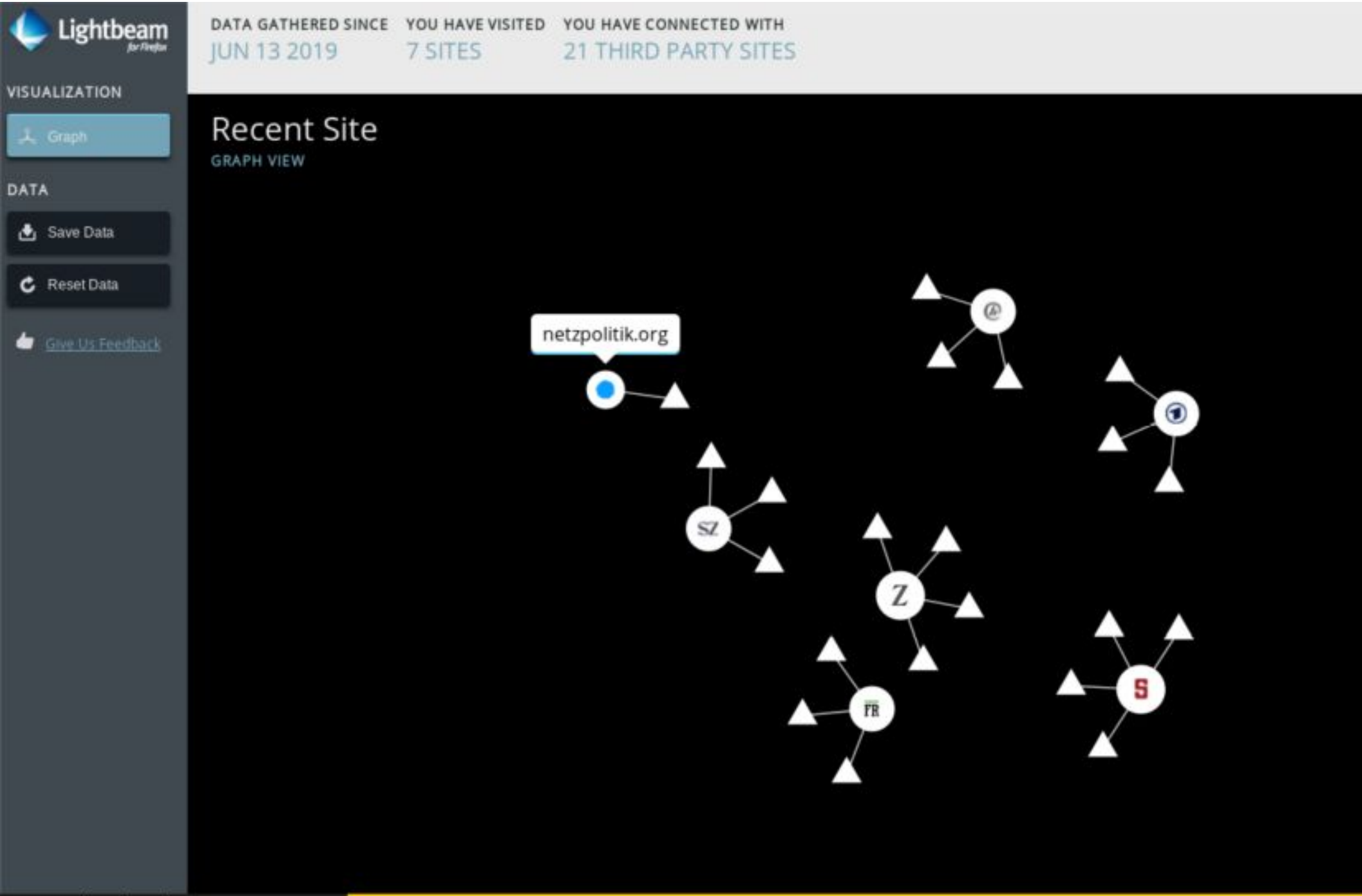
… so schrecklich!

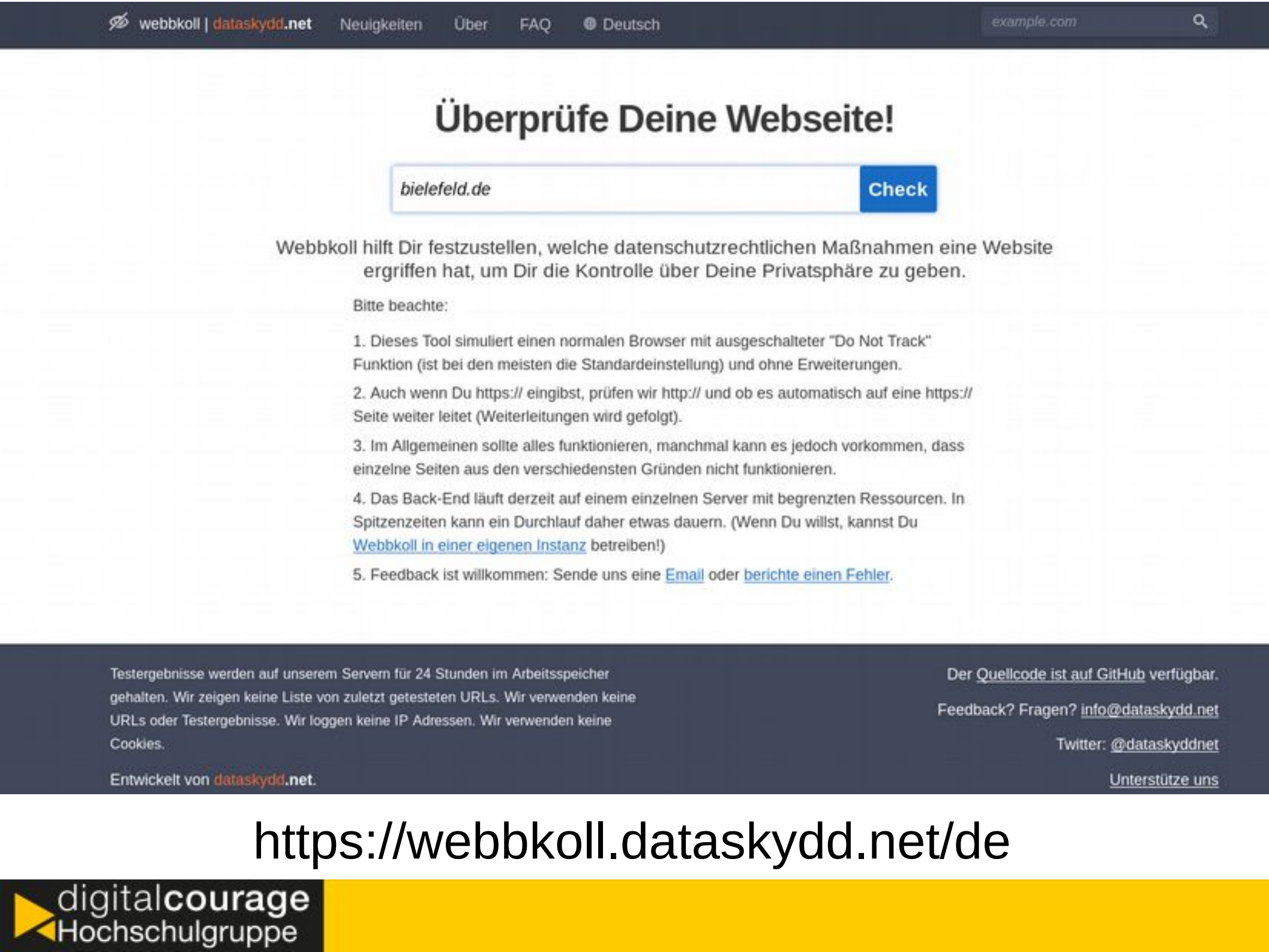
- 8–10 MB; 49 Cookies, min. 20 davon von Drittanbietern
- Ladezeit ca. 15–30 Sek. (Test ohne Interaktion und Scrollen)




Lightbeam
DATA GATHERED SINCE
JUN 13 2019
YOU HAVE VISITED
7 SITES
YOU HAVE CONNECTED WITH
244 THIRD PARTY SITES
VISUALIZATION
Graph
DATA
Save Data
Reset Data
Give Us Feedback
Recent Site
GRAPH VIEW
netzpolitik.org
FR
SZ
Z
S

(Bild: CC-BY-2.0: EFF)



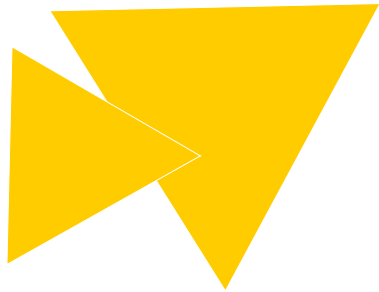


https://webbkoll.dataskydd.net/de

Sicheres Surfen mit Privatsphäre

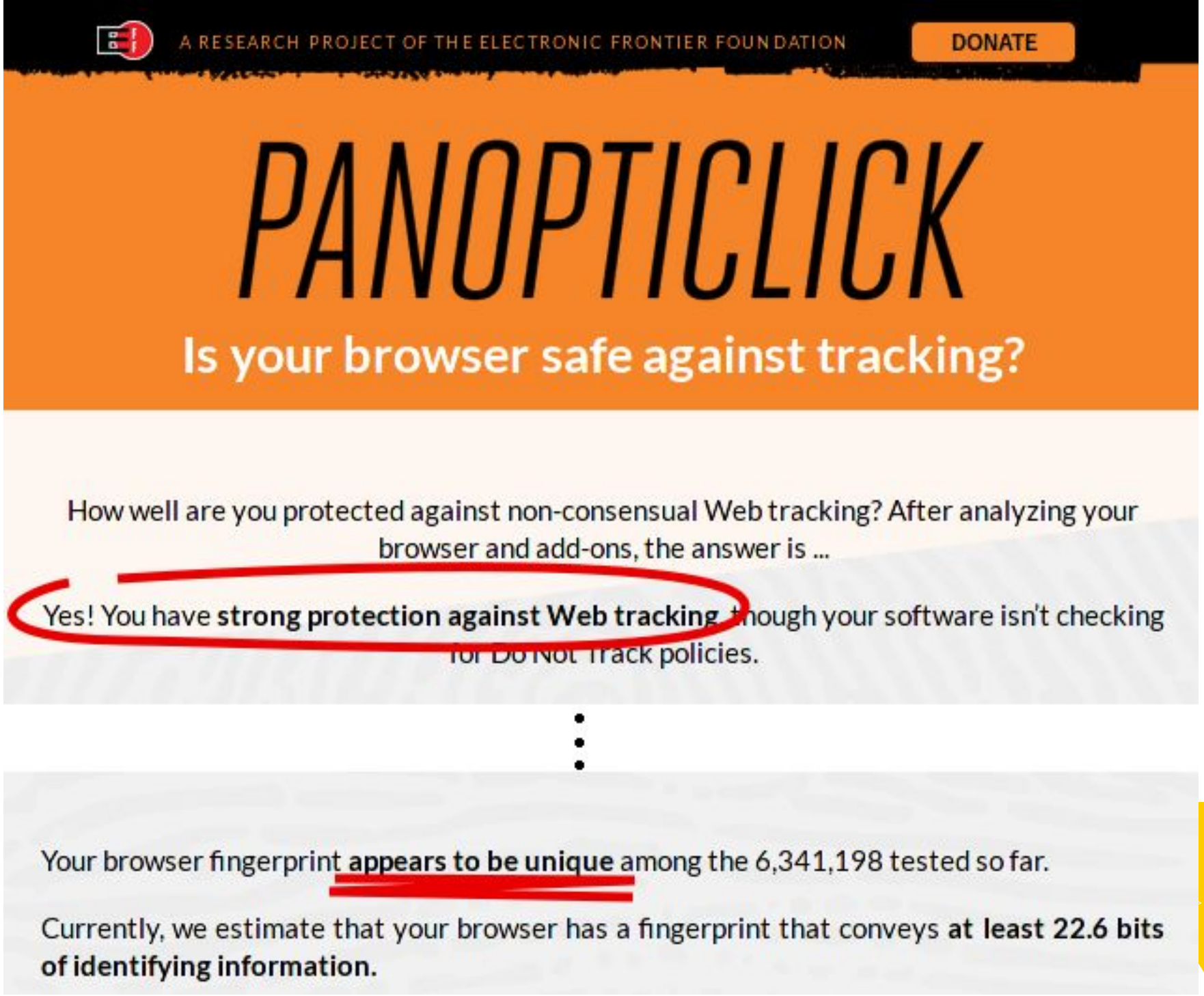
Was wollen wir?

- 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


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
  - 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
  - Startpage.com, MetaGer.de (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!
- aktive Inhalte blocken: **NoScript**
  - alles außer Java-Script erlauben

Firefox-Add-ons

für Fortgeschrittene:

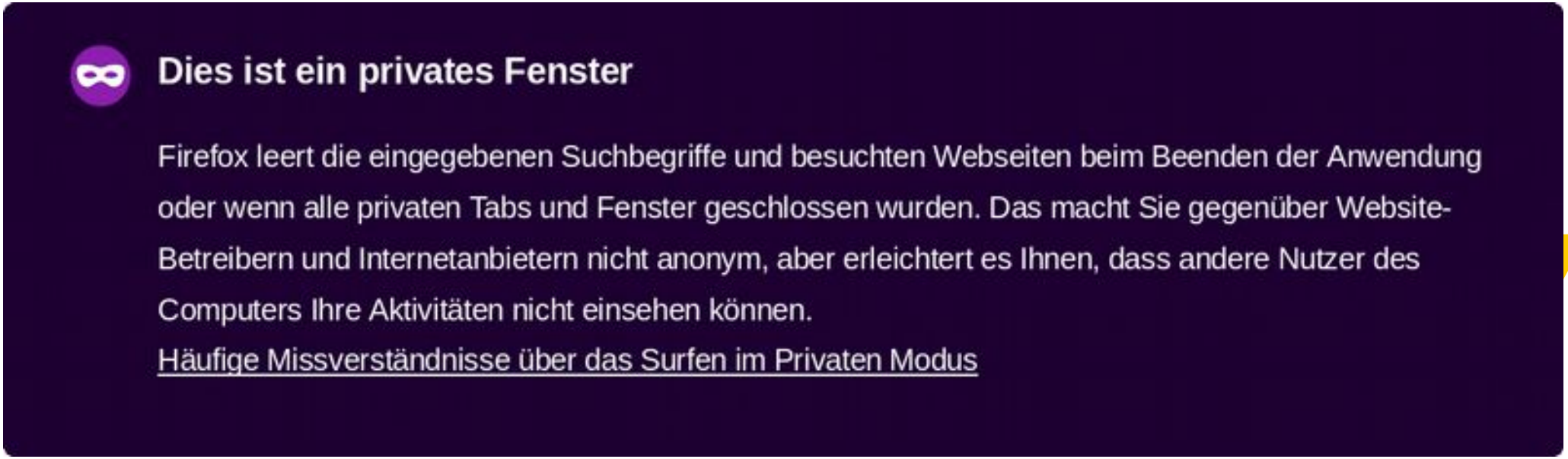
- Referer blockieren: **SmartReferer**
- alles blocken (Whitelist säubern): **NoScript**
- alle Drittanbieteranfragen blocken: **uMatrix**

Kontrolle

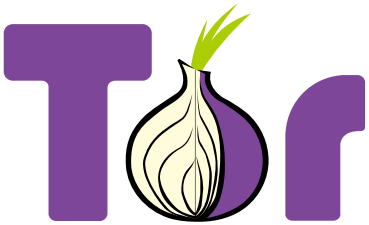
- Wirkung von Add-ons und Einstellungen kontrollieren:
  - Add-On: Lightbeam
  - Menü → Web-Entwickler → Netzwerkanalyse

Exkurs: Privater Modus von Firefox

- keine Speicherung von Daten besuchter Webseiten **auf dem eigenen** Computer (insbesondere keine Chronik, keine URL-Vervollständigung, Cookies, etc.)
- auf dem lokalen System verbleiben keine Spuren
- *keine Anonymität* gegenüber dem Netz



Anonym surfen mit dem Tor-Browser



- Tor: The Onion Router
  - Netzwerk zur Anonymisierung von Verbindungsdaten
  - IP-Adresse wird verschleiert

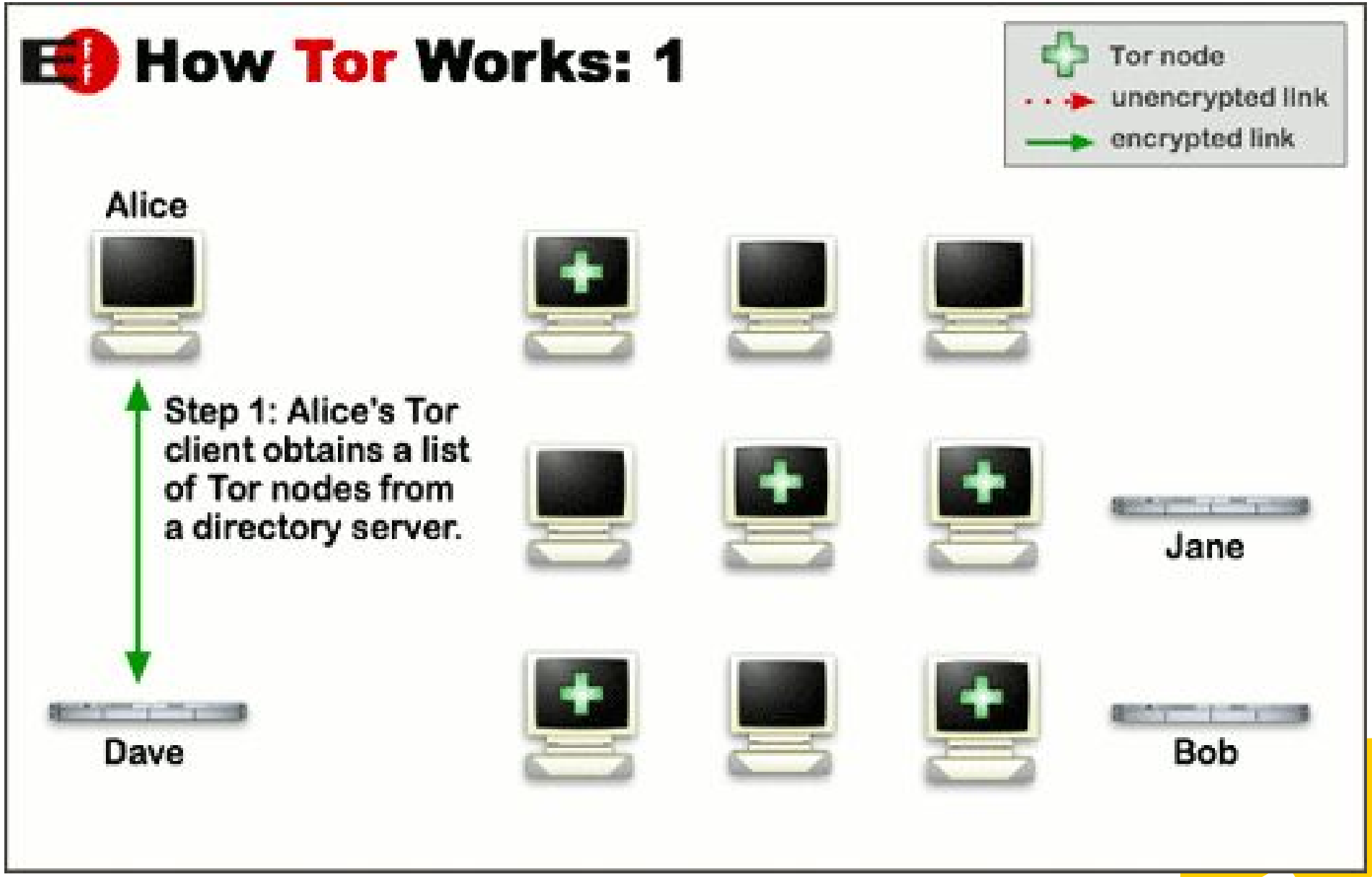
Vorteile

- quelloffen, freie Software
- anonymes Surfen

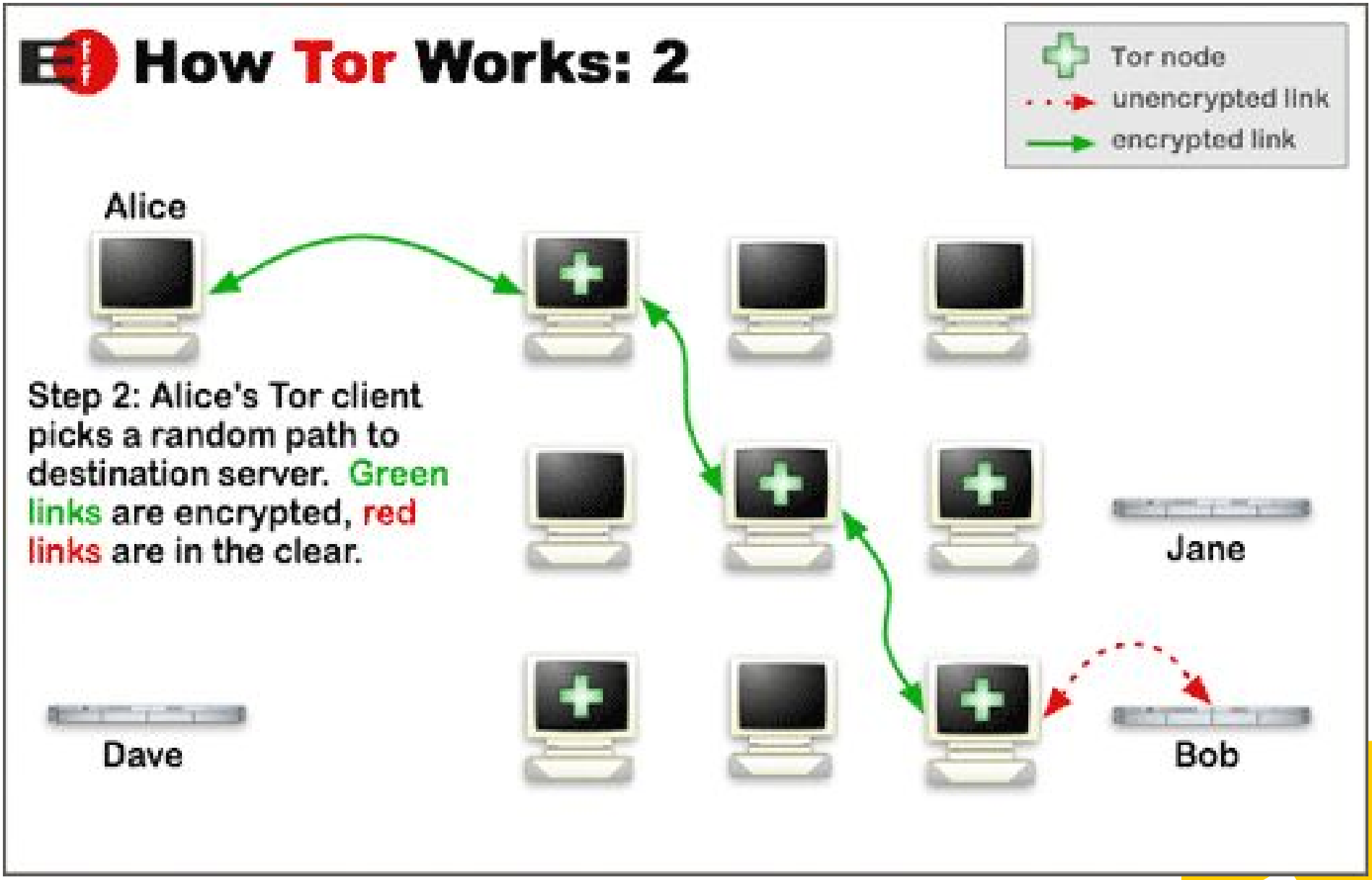
Nachteile

- Login bei personalisierten Seiten nicht sinnvoll
- Latenz ist größer

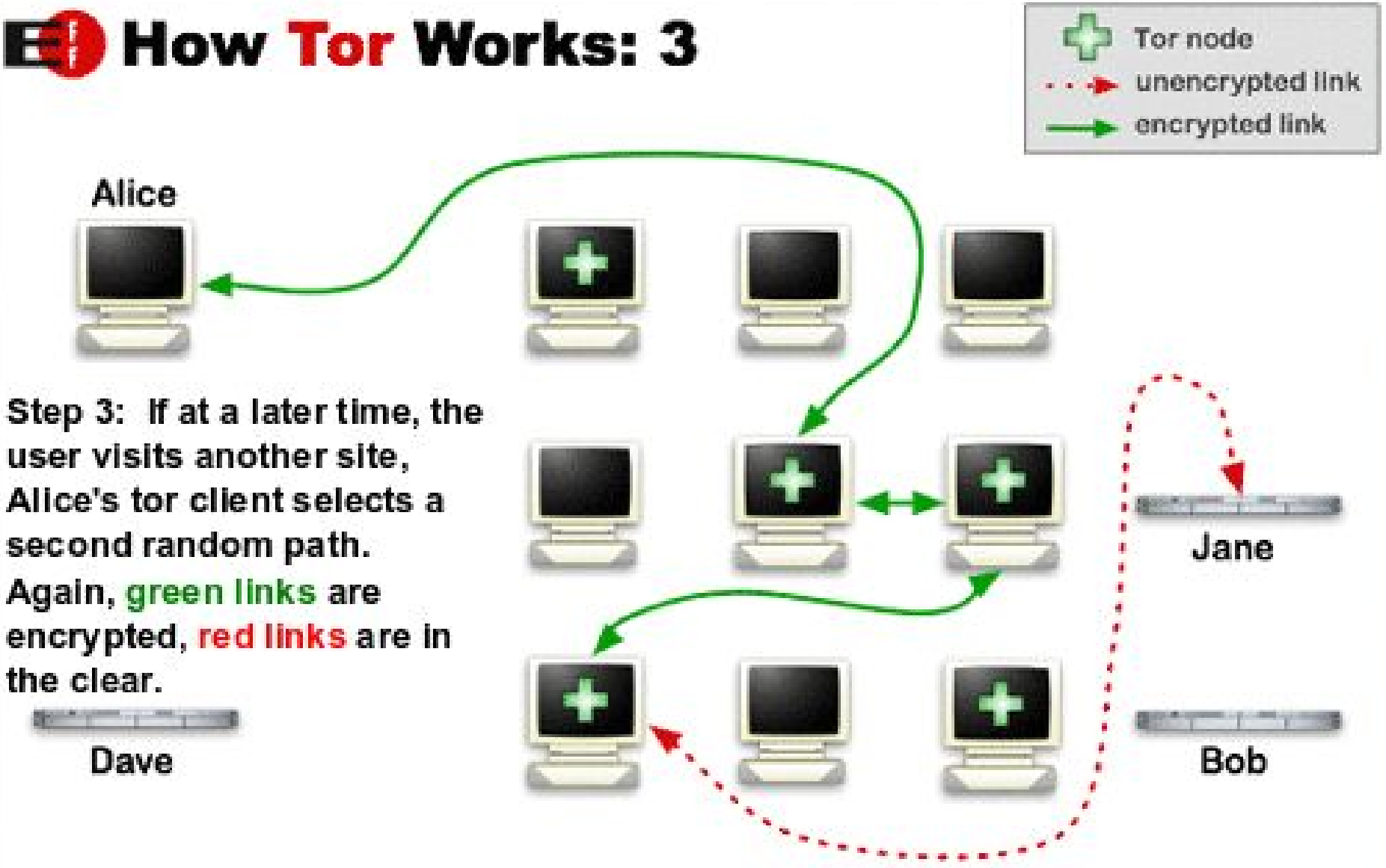
How Tor Works: 1



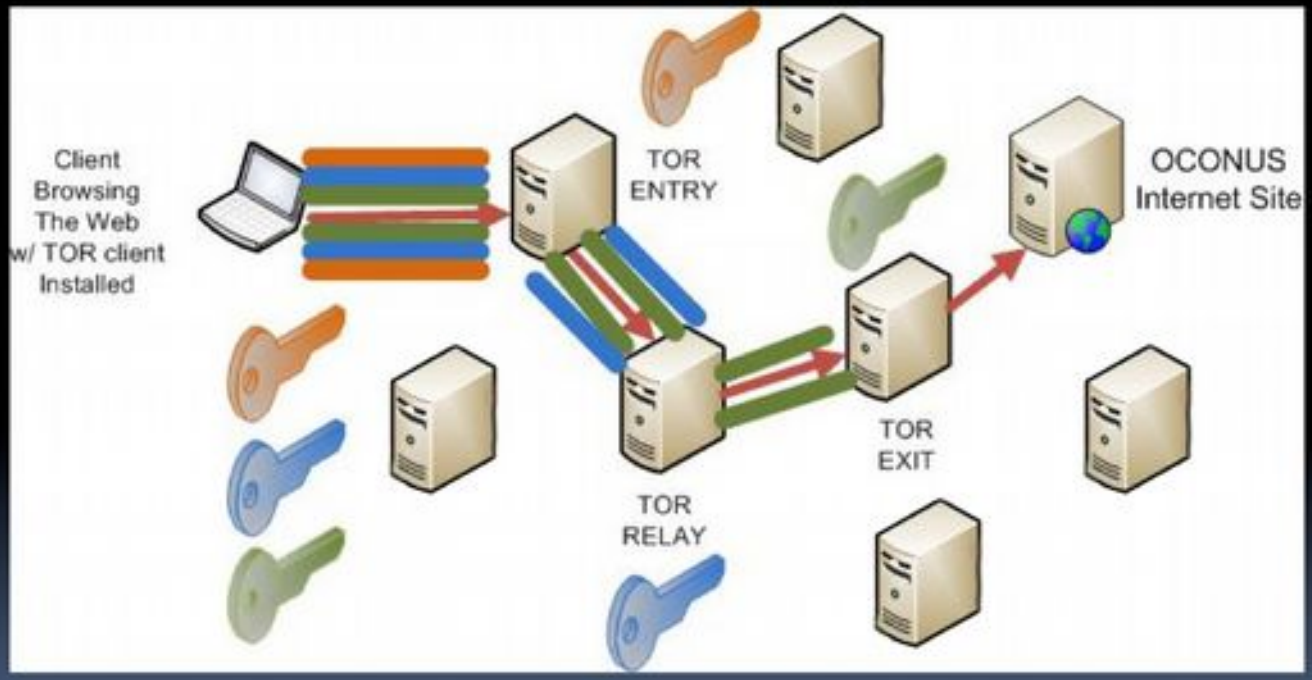
How Tor Works: 2



How Tor Works: 3

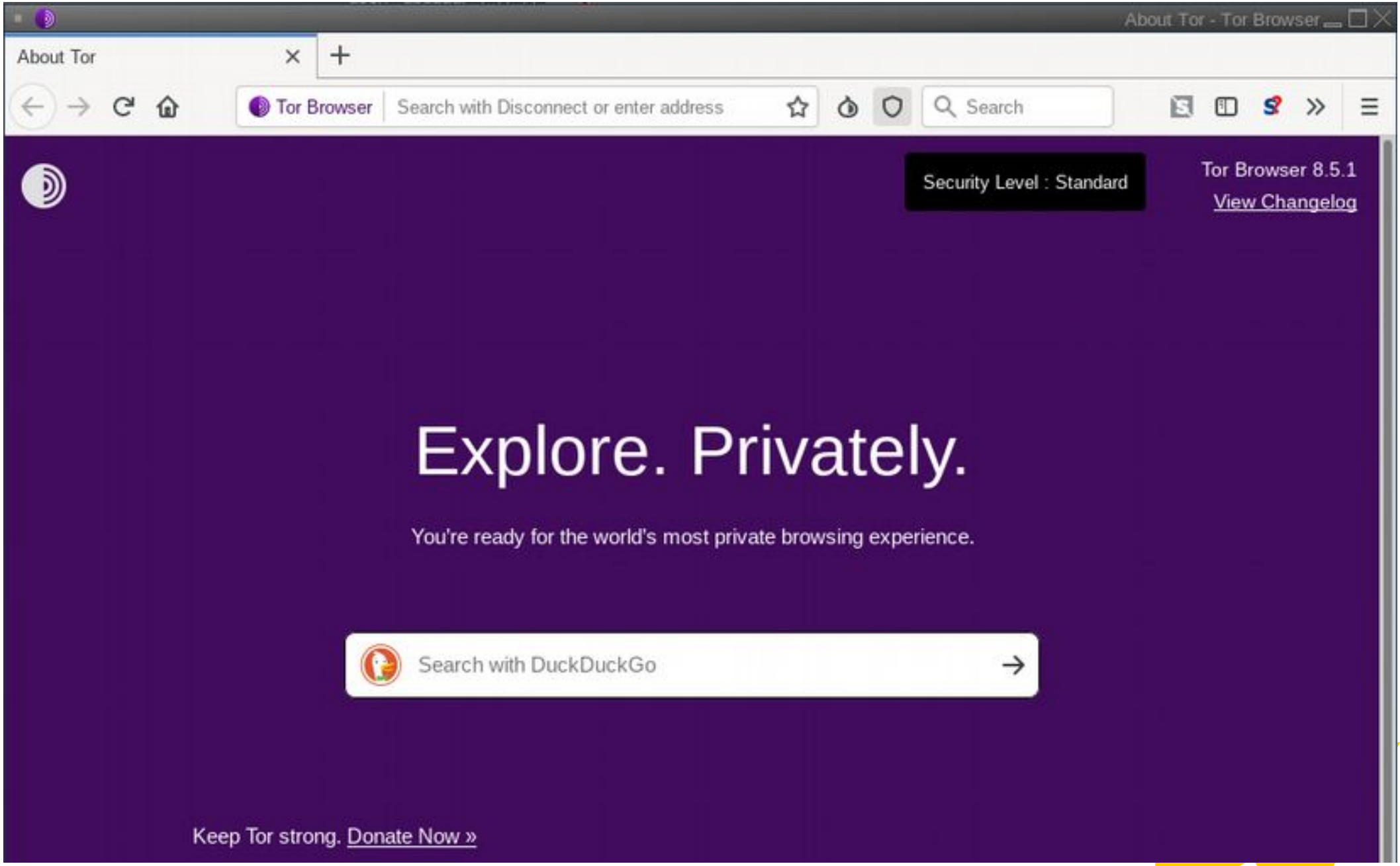


(U) What is TOR?



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")
- Broschüre zu Disconnect! und Tails von Capulcu https://capulcu.blackblogs.org/

- Praxis -

„Sichere“ Passwörter

Wie werden Passwörter geknackt?

- Brute Force
  - alle möglichen Kombinationen ausprobieren
- Listen / Wörterbuch-Angriffe
  - alle Wörter aus einer Liste oder einem Wörterbuch ausprobieren
- Social Engineering
  - Phishing, Person austricksen um Passwort zu erfahren
  - gerne auch durch Facebook, LinkedIn etc.

Wie erschwert man das Knacken des Passworts?

- Brute Force
  - Länge ≥ 10 Zeichen
  - verschiedene Zeichentypen (Groß- und Kleinbuchstaben, Zahlen, Sonderzeichen)
- Listen / Wörterbuch-Angriffe
  - kein einzelnes Wort als Passwort verwenden
  - keine Wörter aus dem persönlichen Umfeld verwenden (Namen, Geburtsdaten etc.)
- Social Engineering
  - Niemandem das Passwort verraten!

Starke Passwörter finden

- Wichtig:
  - für jeden Dienst ein anderes Passwort verwenden!
  - Passwörter in regelmäßigen Abständen austauschen/ändern
- DBiR&dSd90M!
  - Merksatz: »**D**er **B**all **i**st **R**und **&** **d**as **S**piel **d**auert **90** **M**inuten**!**«
- HausLocherTasteMeloneBagger
  - Wortreihung
- 2UrN47oCfK6jAZ8xuKHiop4upPsI73
  - Passwort-Generator

Zwei-Faktor-Authentifizierung

= Kombination zweier unterschiedlicher und insbesondere unabhängiger Komponenten (Faktoren).

HowTo: Starke Passwörter merken?!

Passwortverwaltung

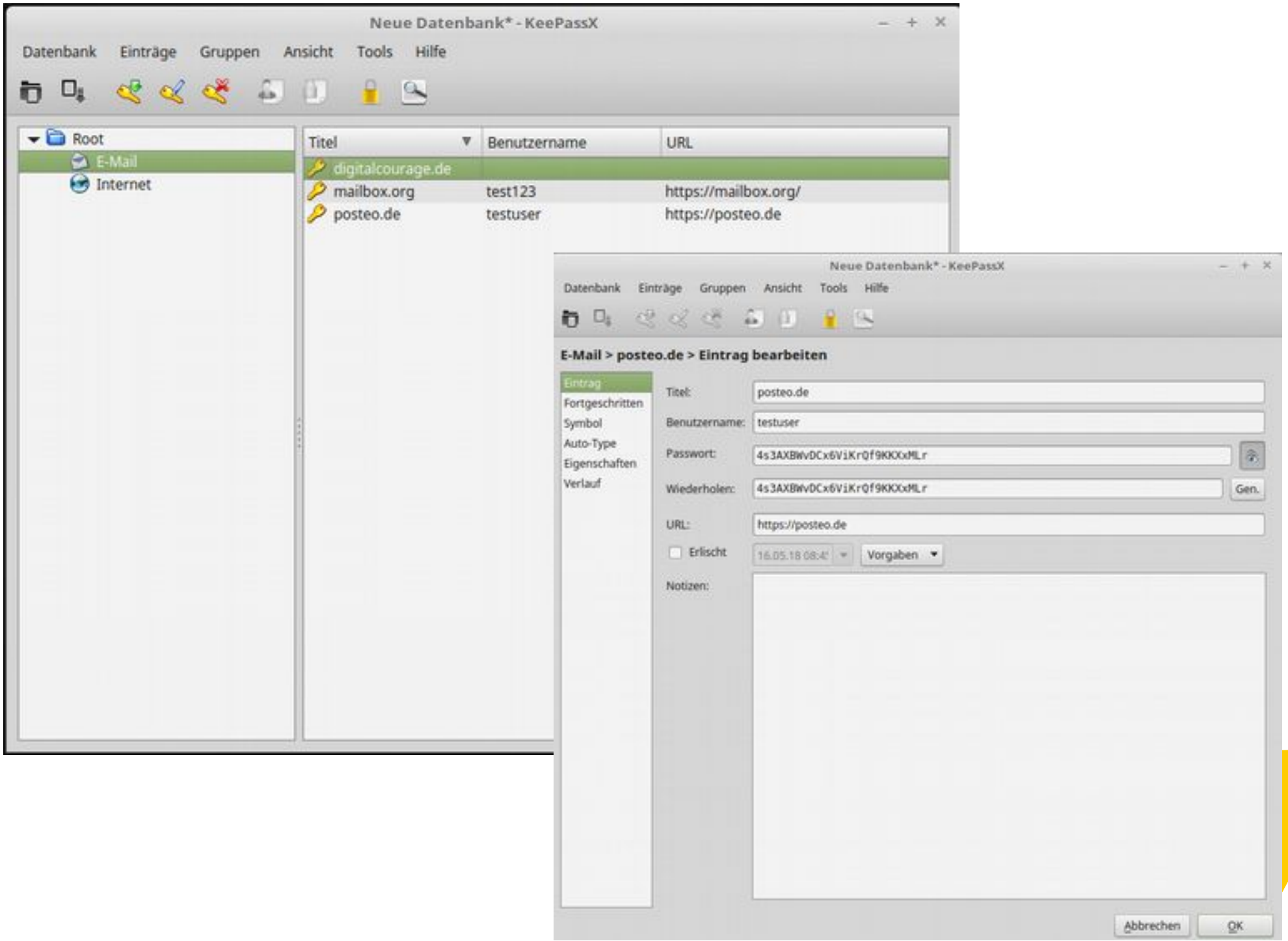
Software: **KeePassX**

Vorteile

- Freie Software
- viele Plattformen
  - Win, Linux, Mac
- Passwortgenerator
- verschlüsselt gespeichert

Nachteile

- Masterpasswort
  - darf nicht vergessen oder geknackt werden!
- Gefahr bei Verlust
  - „setzt alles auf eine Karte“: PW-Datenbank gut sichern!
- Komfort
  - kein Sync zwischen verschiedenen Geräten


Neue Datenbank* - KeePassX
Datenbank
Einträge
Gruppen
Ansicht
Tools
Hilfe
Root
E-Mail
Internet
Titel
Benutzername
URL
digitalcourage.de
mailbox.org
test123
https://mailbox.org/
posteo.de
testuser
https://posteo.de
Neue Datenbank* - KeePassX
Datenbank
Einträge
Gruppen
Ansicht
Tools
Hilfe
E-Mail > posteo.de > Eintrag bearbeiten
Eintrag
Fortgeschritten
Symbol
Auto-Type
Eigenschaften
Verlauf
Titel:
posteo.de
Benutzername:
testuser
Passwort:
4s3AXBWvDCx6ViKrQf9KKXxMLr
Wiederholen:
4s3AXBWvDCx6ViKrQf9KKXxMLr
Gen.
URL:
https://posteo.de
Erlischt
Vorgaben
Notizen:
Abbrechen
OK

Starkes Masterpasswort finden

- Passwörter würfeln mithilfe einer Passwortliste
- Warum? → Entropie!
- Vorteil: nur dieses Passwort muss man sich merken
- mind. 6 Wörter würfeln

Dateiverschlüsselung

Warum überhaupt verschlüsseln?

- Genereller Schutz sensibler und vertraulicher Daten
  - Bei Verlust/Diebstahl des Laptops oder USB-Stick
  - Alle, die personenbezogene Daten speichern

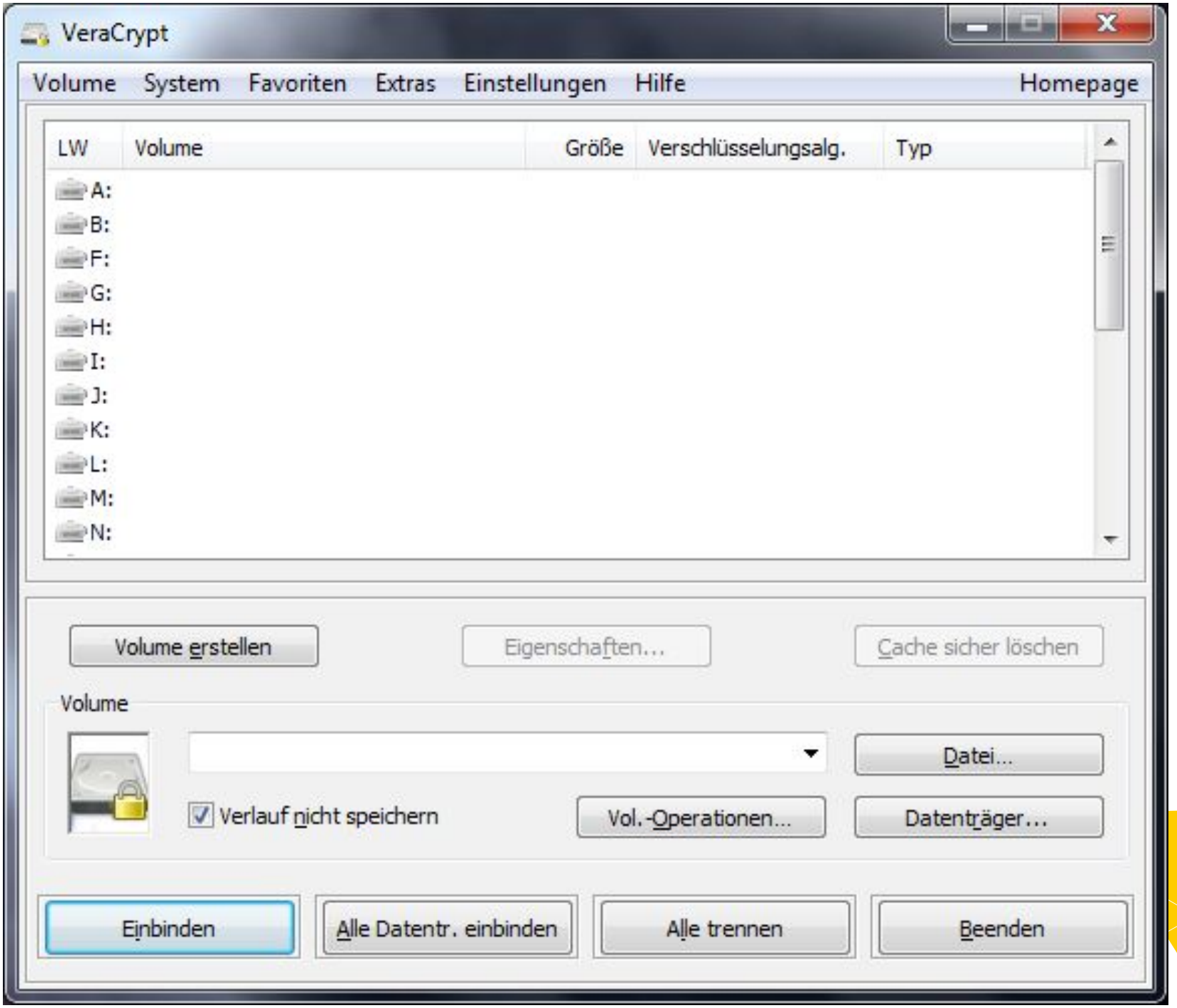
- Weil Ihr ein Grundrecht auf digitale Privat- und Intimsphäre habt!
  - „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“ – sogenanntes IT-Grundrecht
  - Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG

VeraCrypt

- Software zur Dateiverschlüsselung
- quelloffen und auf allen gängigen Plattformen verfügbar
- Freie Software

Was kann ich mit VeraCrypt verschlüsseln?

- Container (verschlüsselte Ordner)
- Datenträger:
  - Festplatten/SSDs
  - CDs, DVDs … (Container)
  - USB-Sticks
- Systempartition


VeraCrypt
Volume
System
Favoriten
Extras
Einstellungen
Hilfe
Homepage
LW
Volume
Größe
Verschlüsselungsalg.
Typ
A:
B:
F:
G:
H:
I:
J:
K:
L:
M:
N:
Volume erstellen
Eigenschaften...
Cache sicher löschen
Volume
Datei...
Verlauf nicht speichern
Vol.-Operationen...
Datenträger...
Einbinden
Alle Datentr. einbinden
Alle trennen
Beenden

Über VeraCrypt

Vorteile

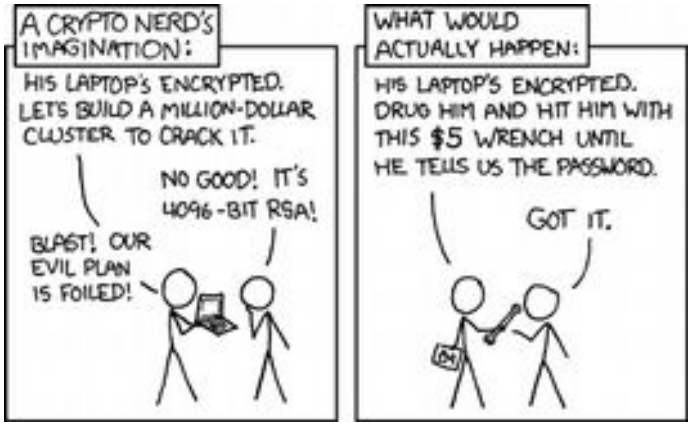
- quelloffen, freie Software
- nachvollziehbare Änderungen am Code
- plattformübergreifend
- auf USB-Stick transportierbar
- unabhängiger Audit

Nachteile

- Komfortverlust
- Passwortverlust = Datenverlust

Umgang mit VeraCrypt

- Was will ich verschlüsseln?
- Starkes Passwort wählen
- Adminrechte notwendig
- Vorsicht bei fremden Geräten!
- Generell: Benutzerhandbuch zu VeraCrypt lesen
- Größtes Sicherheitsrisiko sind fast immer die Menschen! Eventuell unfreiwillig:



Alternativen

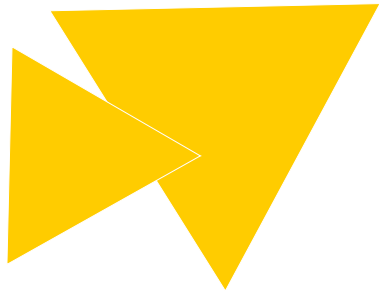
- **dm-crypt** (Teil des Linux-Kernels ab Version 2.6)
  - z.B. Ubuntu und Mint erlauben Systemverschlüsselung bei Installation
- **7-Zip**: freie Software, unterstützt AES256-Verschlüsselung für 7z-Archive

- Nicht vertrauenswürdig, da nicht quelloffen:
  - Windows: **BitLocker** (ab Vista, nur bei teuren Windows-Versionen)
  - MacOS: **FileVault**
  - zahllose weitere kommerzielle Produkte

Rechtliches

- Deutschland: Kein Zwang zur Herausgabe eines Passworts/Schlüssels bei möglicher Selbstbelastung
- Vorsicht im Ausland:
  - Großbritannien: Pflicht zur Herausgabe (→ RIPA), auch Beugehaft möglich!
  - USA: Ein- und Ausreise mit verschlüsselten Datenträgern problematisch

Mobilgeräte



Noch einmal zu den Metadaten…

- Was sind Metadaten?
  - „Informationen über Informationen“
  - Beispiel SMS: u.a. Länge der Nachricht, Zeitpunkt, Ort (Funkzelle), Ursprung und Ziel
  - Metadaten verraten häufig mehr über Menschen als die eigentlichen Inhalte

→ Für Geheimdienste besonders interessant

- BND speicherte 2015 täglich 220 Millionen Metadaten

Überwachung

- Geheimdienste werten Metadaten unter bestimmten Blickwinkeln aus …

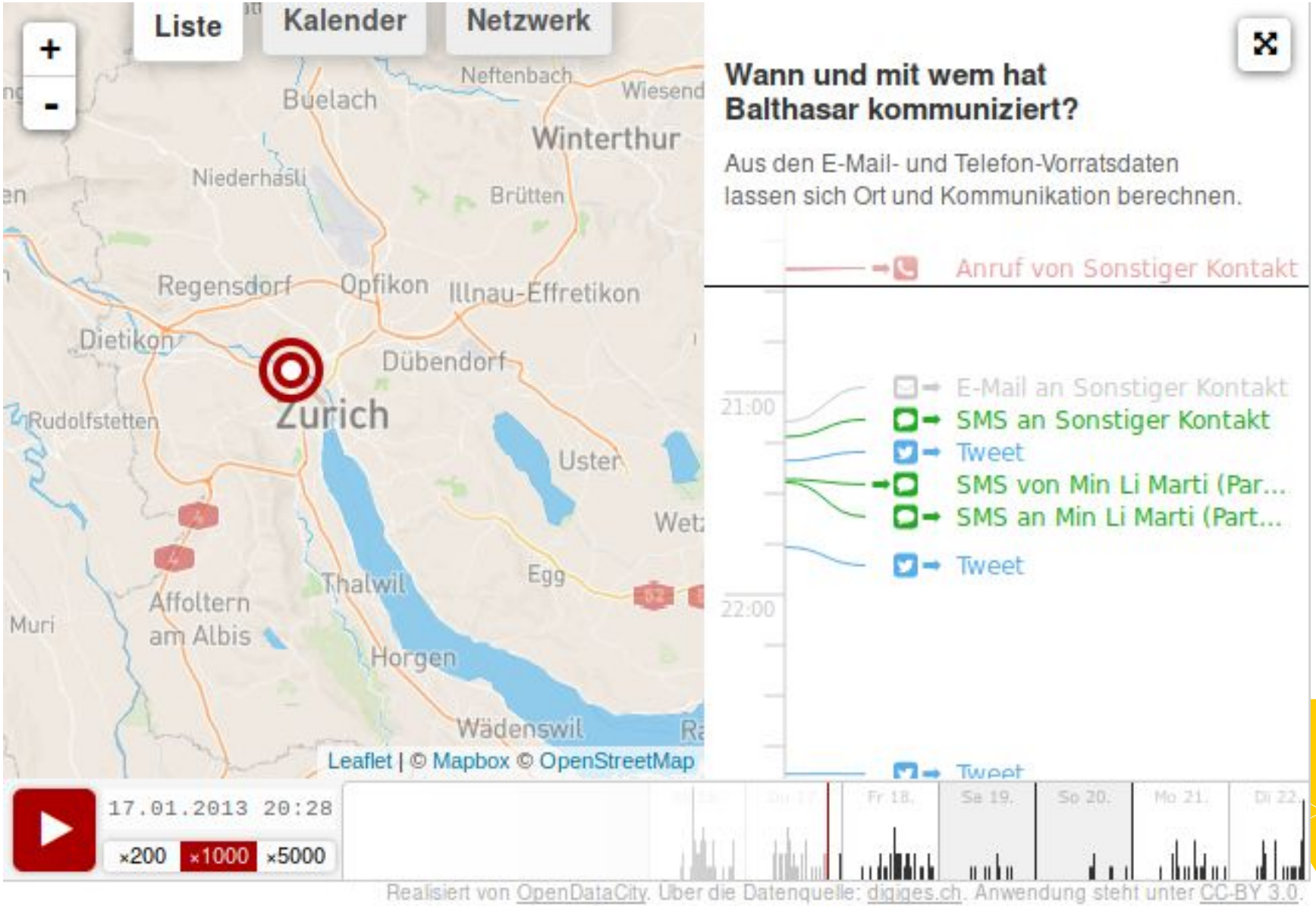
  (Kontaktbeziehungen, Reisedaten, Finanztransfers, …)

- … 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.“)

Verräterisches Telefon



Kommerzielle Datensammlungen

- Markt für optimierte personenbezogene Werbung
- Apps sammeln diverse Nutzerdaten (z. B. Standortdaten) und leiten diese weiter
- Beispiel: Die Diabetiker-App **mySugr** übermittelte in einem Test von Mike Kuketz u.a. folgende Daten an das US-Unternehmen Mixpanel
  - E-Mail-Adresse
  - Vor- und Nachname der Person
  - Diabetes-Typ
  - Art der Therapie (Spritze oder Pumpe)

Smartphones: Hardware & Betriebssystem

- Hardware („Super-Wanze“)
  - Mikrofon, Kamera, GPS, Bewegungssensor

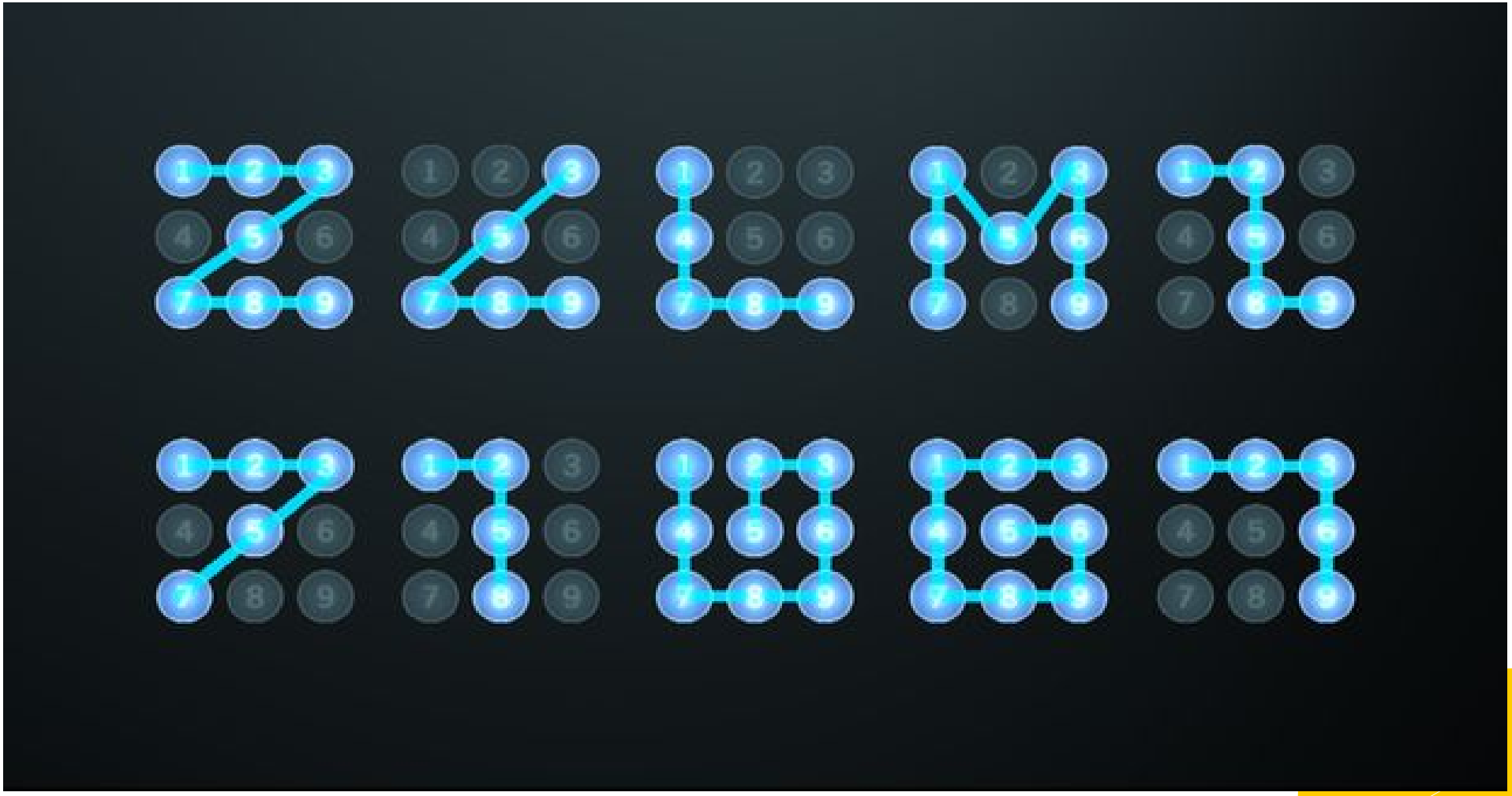
- Betriebssystem: Goldener Käfig iOS (Apple)
  - Apps nur aus einer Quelle (zentraler App-Store)
  - geschlossenes System, keine Gerätehoheit
  - mehr Freiheit durch Jailbreak (Gefängnisausbruch)
  - massives Tracking durch Apps aus dem App-Store:
    - https://www.washingtonpost.com/technology/2019/05/28/its-middle-night-do-you-know-who-your-iphone-is-talking/

Android

- Theoretisch gute Basis …
  - Linux-basiert, freie Software

- **Aber:**
  - Google-Dienste bei Neugeräten fest integriert: Suche, Browser, Gmail, Maps, Kalender- / Kontakte-Sync …
  - Play Store & Google-Dienste
  - Fernzugriff, Datenübermittlung
  - standardmäßig keine Gerätehoheit
  - oft unzureichende Versorgung mit Sicherheitsupdates durch den Hersteller, starke Abhängigkeit von Google

Typische Wischgesten



Erste Schritte: Konfiguration

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

Super sichere Iris-Scanner?

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
  - Telefonstatus und Identität abrufen
- Anrufliste lesen
  - 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

10
trackers

26
permissions

Lieferando.de - Order Food

Version: **6.1.4**
Creator: **Takeaway.com**
Downloads: **5,000,000+ downloads**

Other versions | On Google Play | APK fingerprint

This report was automatically issued on **May 8, 2019, 6:12 a.m.**.
This report was automatically updated on **May 8, 2019, 6:12 a.m.**.

S
Finger
Issuer:
Subjec
Serial:

10 Trackers

We have found **code signature** of the following trackers in the application:

- Ad4Screen
- Adjust
- Facebook Analytics
- Facebook Login
- Facebook Places
- Facebook Share
- Google Analytics
- Google CrashLytics
- Google Firebase Analytics
- HockeyApp

26 Permissions

We have found the following permissions in the application: (2 Special 2 Dangerous)

ACCESS_COARSE_LOCATION (android.permission)
Access Approximate Location (Network-based)

ACCESS_FINE_LOCATION (android.permission)
Access Precise Location (GPS And Network-based)

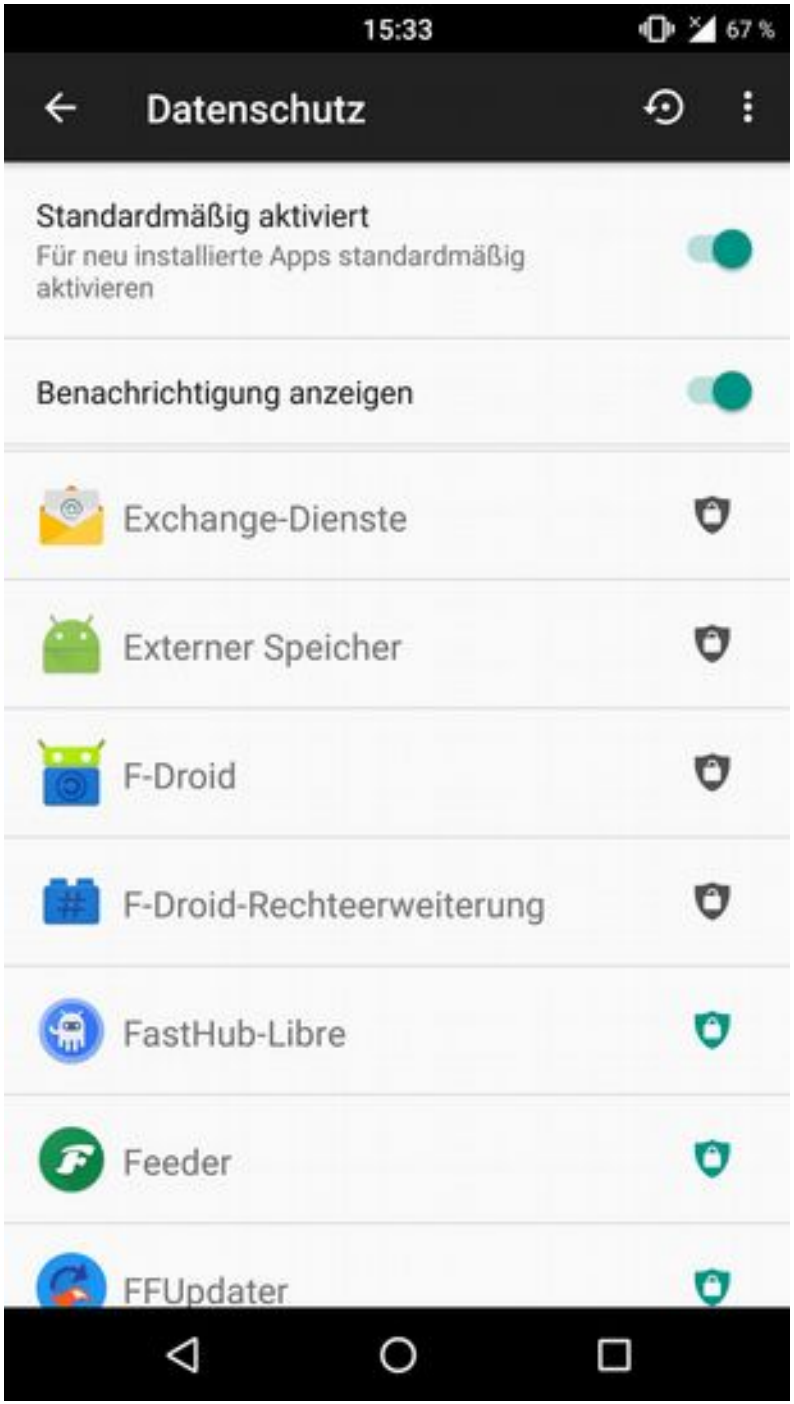
ACCESS_NETWORK_STATE (android.permission)
View Network Connections

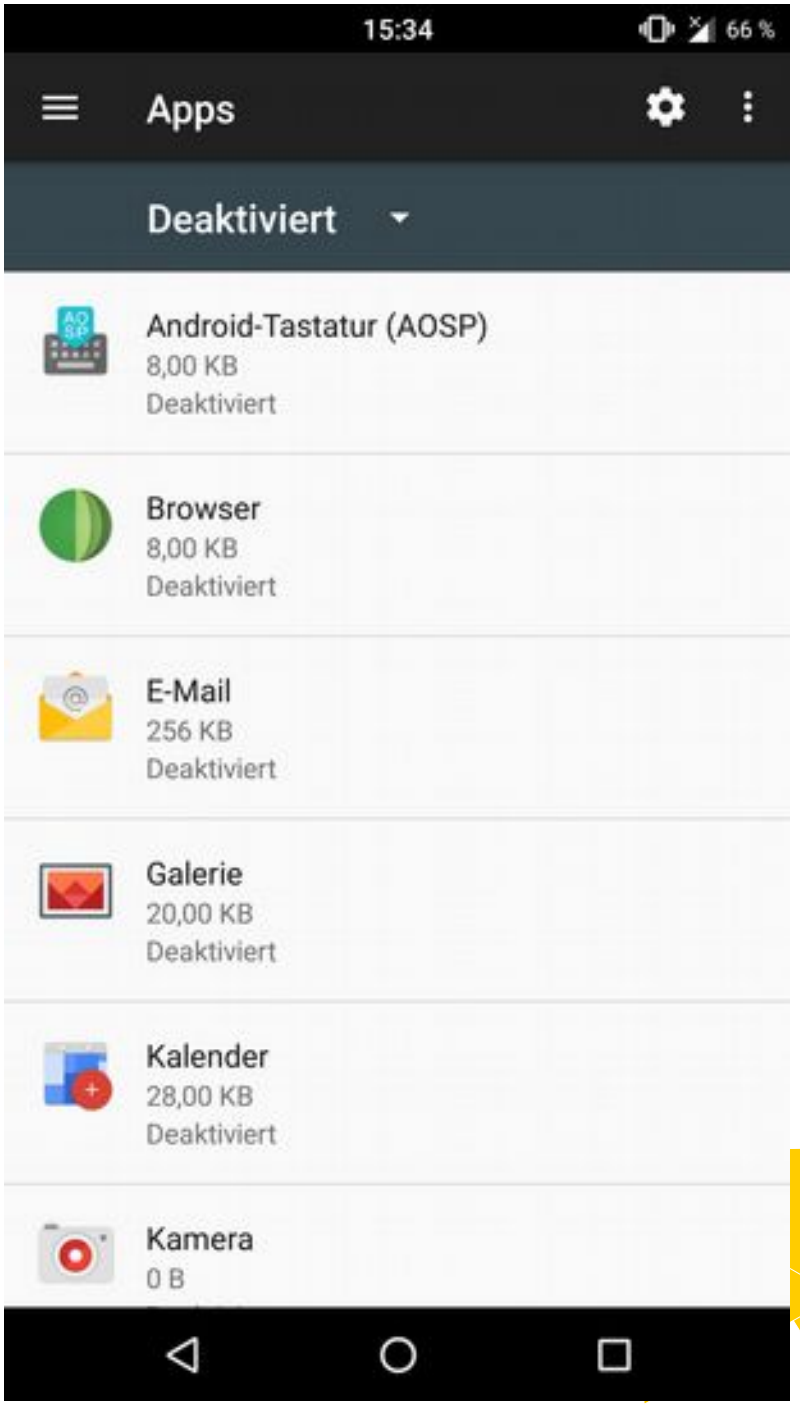
ACCESS_WIFI_STATE (android.permission)
View Wi-Fi Connections

INTERNET (android.permission)
Have Full Network Access

Apps immer kritisch begegnen!

- „kostenlose“ Apps im App/Play Store verdienen häufig mit Datensammelei und Werbung an den Nutzer.innen
- immer hinterfragen: Braucht App XY diese oder jene Berechtigung für ihre Funktion überhaupt?
- einzelne Berechtigungen von Apps entziehen
- falls verfügbar: Datenschutzmodus aktivieren!
- alternative Apps nutzen, die weniger Berechtigungen benötigen


15:33
67 %
Datenschutz
Standardmäßig aktiviert
Für neu installierte Apps standardmäßig aktivieren
Benachrichtigung anzeigen
Exchange-Dienste
Externer Speicher
F-Droid
F-Droid-Rechteerweiterung
FastHub-Libre
Feeder
FFUpdater

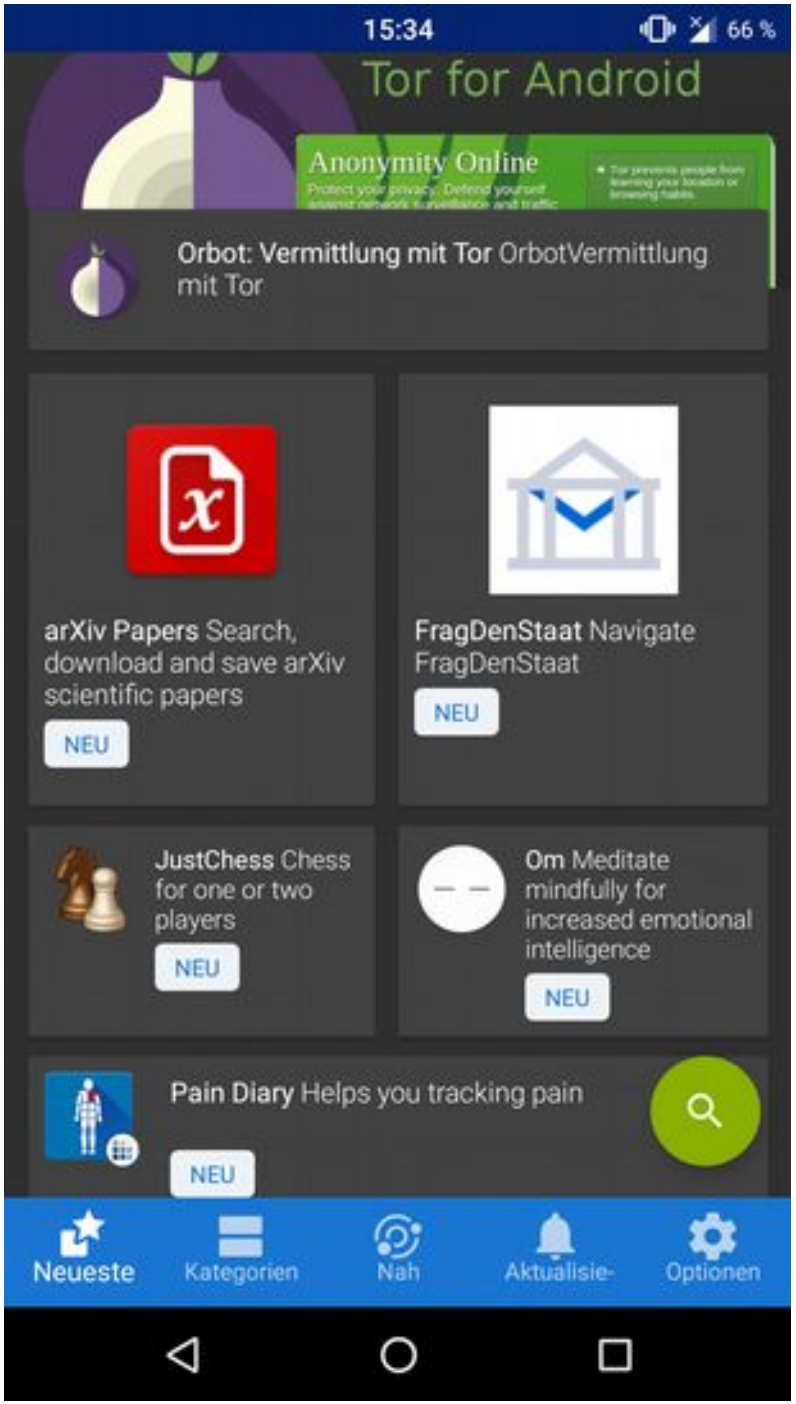

15:34
66 %
Apps
Deaktiviert
Android-Tastatur (AOSP)
8,00 KB
Deaktiviert
Browser
8,00 KB
Deaktiviert
E-Mail
256 KB
Deaktiviert
Galerie
20,00 KB
Deaktiviert
Kalender
28,00 KB
Deaktiviert
Kamera
0 B

Android „entgoogeln“

1. Apps und Dienste von Google deaktivieren/deinstallieren
   - Google-Einstellungen (G+, Standort, Suche, Werbe-ID, usw.)
2. Alternativ-Dienste nutzen
   - Browser, Suche, Mail, Sync für Kalender / Kontakte …
3. Play Store deaktivieren / 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)


15:34
66 %
Tor for Android
Anonymity Online
Orbot: Vermittlung mit Tor OrbotVermittlung mit Tor
arXiv Papers Search, download and save arXiv scientific papers
NEU
FragDenStaat Navigate FragDenStaat
NEU
JustChess Chess for one or two players
NEU
Om Meditate mindfully for increased emotional intelligence
NEU
Pain Diary Helps you tracking pain
NEU
Neueste
Kategorien
Nah
Aktualisie-
Optionen


15:35
66 %
Schreiben
ALLE 146 ANSEHEN
FragDenSta at Navigate FragDenSta...
Orgzly Outli- ner for notes and tasks in...
Bierverkostu ng Document and manag...
Sicherheit
ALLE 121 ANSEHEN
Orbot: Ver- mittlung mit Tor OrbotVe...
WireGuard Next genera- tion secure ...
Auditor Verify integrity/ identity of a...
Spiele
ALLE 275 ANSEHEN
Neueste
Kategorien
Nah
Aktualisie-
Optionen

Ansprüche an Messenger

- für alle gängigen Betriebssysteme 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 (Android)

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

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/

Empfehlenswerte Messenger

- **Conversations (Legacy)** (Android)

  bzw. ChatSecure (iOS)

  - nutzen das offene Protokoll **XMPP** (Jabber), das im Gegensatz zu anderen Messengern dezentrale Kommunikationsstrukturen erlaubt
  - unterstützen Ende-zu-Ende-verschlüsselte Chats via OMEMO
  - verfügbar via F-Droid (Conversations) bzw. App Store (ChatSecure)
  - als Conversations Legacy auch kostenlos im Play Store

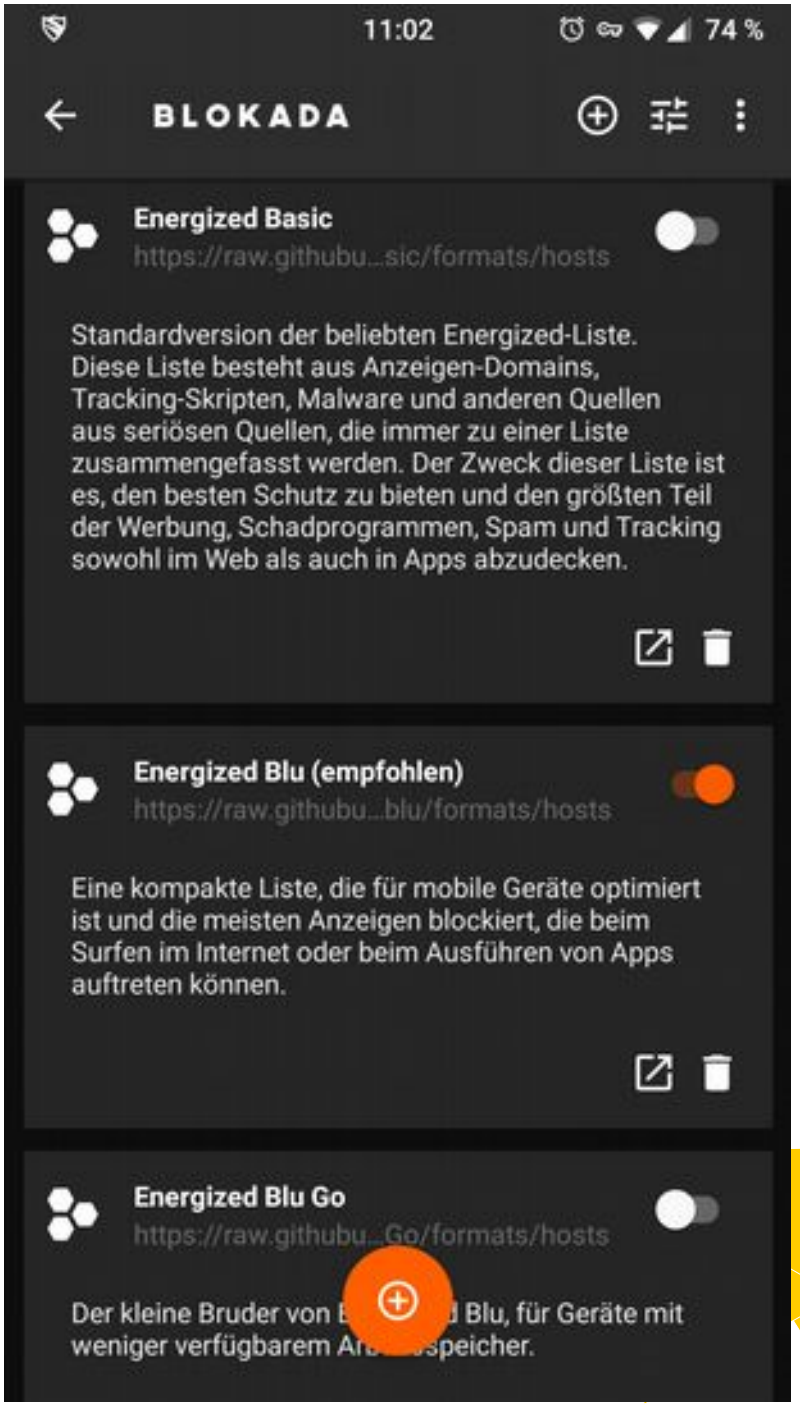
Empfehlenswerte Browser

- **Mozilla Firefox / Fennec F-Droid**
  - Freie Software
  - unter Android durch Add-ons erweiterbar (uBlock Origin, NoScript, HTTPS Everywhere etc.)
  - Konfiguration ähnlich zur Desktop-Version
  - iOS-Version stark eingeschränkt
- **Tor Browser** nun auch (stabil) für Android verfügbar

Blokada: Werbung und Tracking blockieren

- systemweites Blockieren von Werbung und Trackern via VPN-Schnittstelle
- alternativen DNS-Server einstellen
- Freie Software
- nicht im Play Store, sondern in **F-Droid** erhältlich
- https://blokada.org/
- **Achtung:** Nicht mit Tor oder anderen Apps kompatibel, die die VPN-Schnittstelle von Android nutzen


11:01
74 %
BLOKADA
Blokada ist aktiv.
Aktuell
26 blockiert
1 in Blacklist
5 in Whitelist
46.182.19.48,
46.182.19.48
Benachrichtigungen
Erweiterte Einstellungen
223403 Hosts


11:02
74 %
BLOKADA
Energized Basic
https://raw.githubu...sic/formats/hosts
Standardversion der beliebten Energized-Liste. Diese Liste besteht aus Anzeigen-Domains, Tracking-Skripten, Malware und anderen Quellen aus seriösen Quellen, die immer zu einer Liste zusammengefasst werden. Der Zweck dieser Liste ist es, den besten Schutz zu bieten und den größten Teil der Werbung, Schadprogrammen, Spam und Tracking sowohl im Web als auch in Apps abzudecken.
Energized Blu (empfohlen)
https://raw.githubu...blu/formats/hosts
Eine kompakte Liste, die für mobile Geräte optimiert ist und die meisten Anzeigen blockiert, die beim Surfen im Internet oder beim Ausführen von Apps auftreten können.
Energized Blu Go
https://raw.githubu...Go/formats/hosts

Empfehlenswerter E-Mail-Client

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

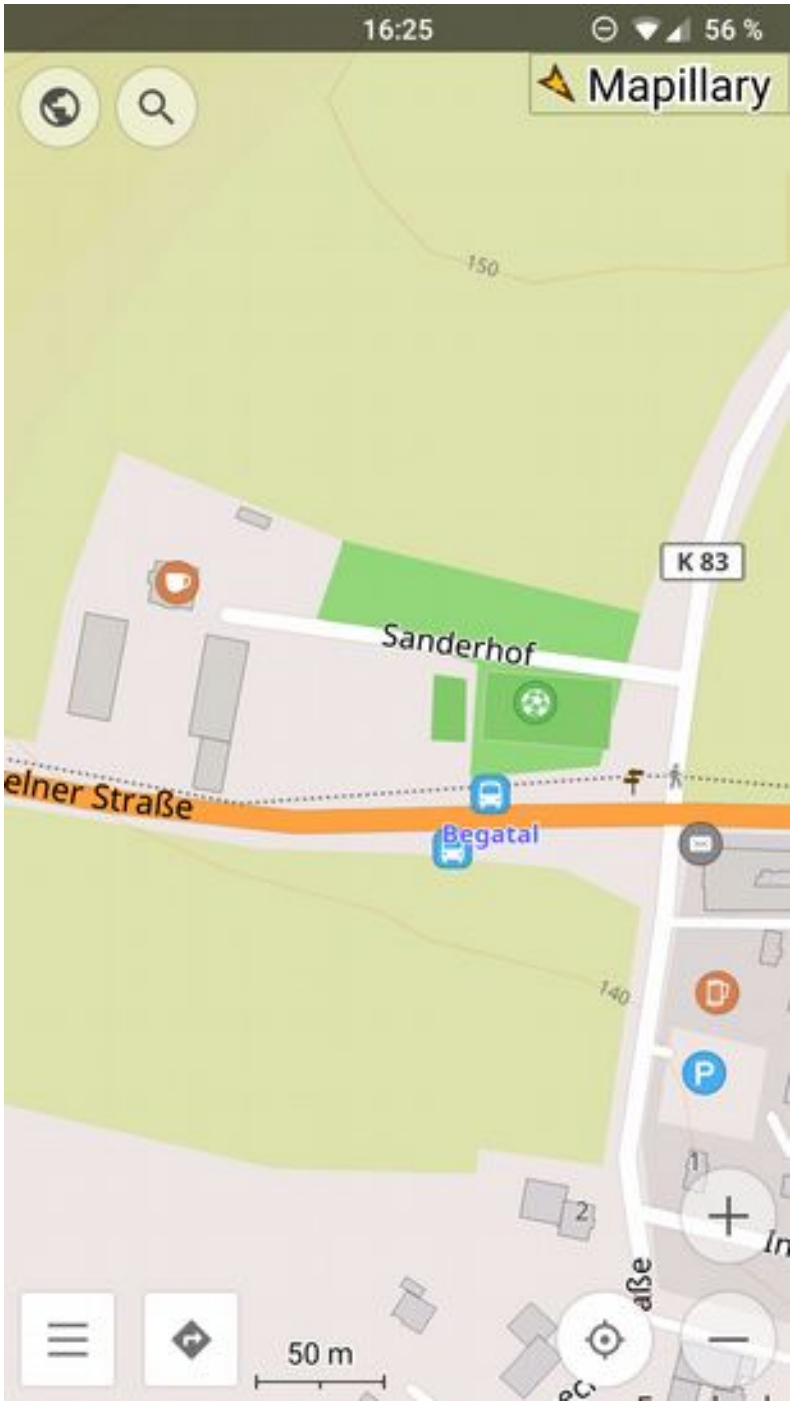
- **OpenKeychain**
  - Implementierung von OpenPGP unter Android
  - agiert außerdem als Schlüsselverwaltung
  - Problem: private Schlüssel auf Mobilgerät zu gefährdet?

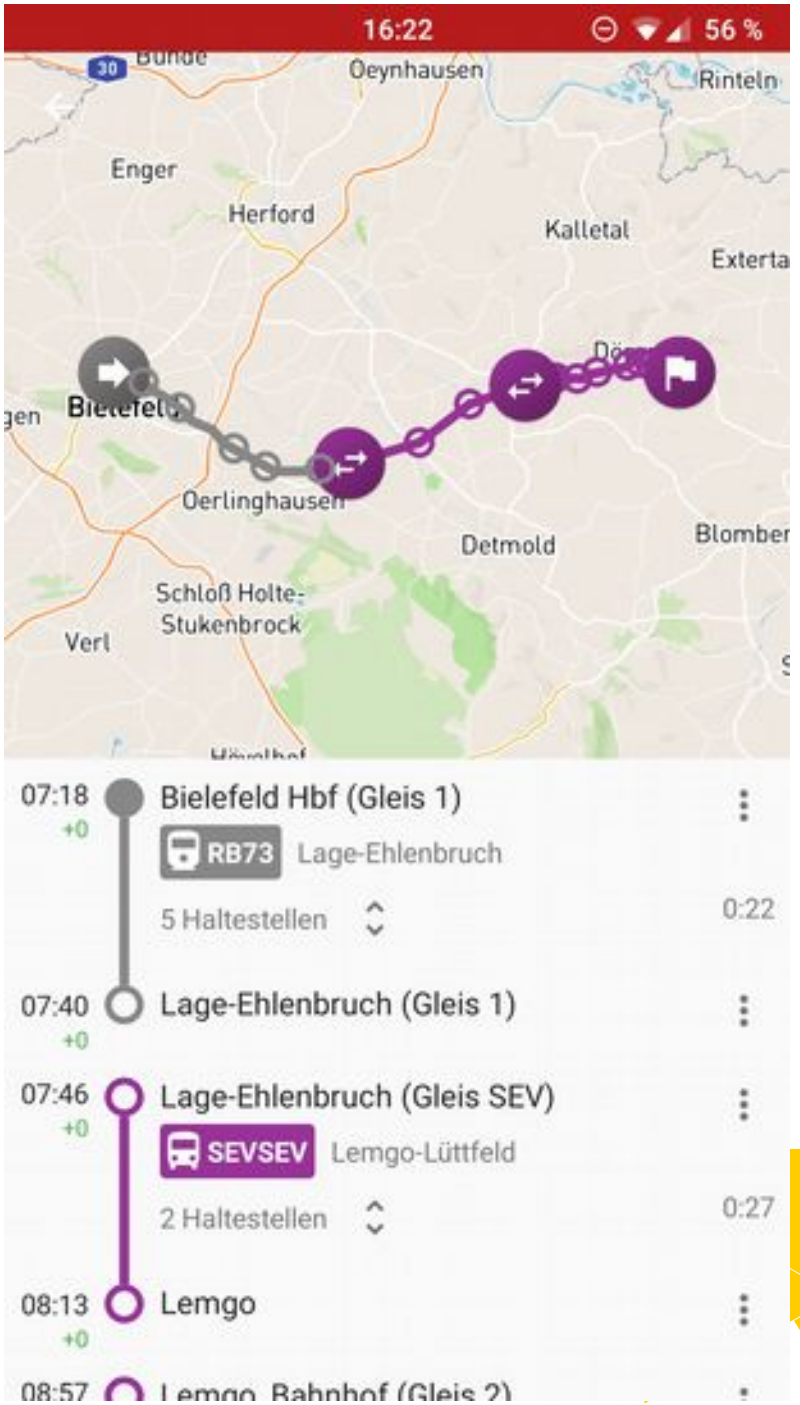
Weitere empfehlenswerte Apps

- **Transportr**
  - Fahrpläne des öffentlichen Nah-/Fernverkehrs & Verbindungssuche

- **VLC**
  - Video- und Audioplayer

- **OsmAnd+**
  - Karten- und Navigationssoftware auf Basis von OpenStreetMap
  - unterstützt auch Offline-Karten


16:25
56 %
Mapillary
150
K 83
Sanderhof
elner Straße
Begatal
140
50 m

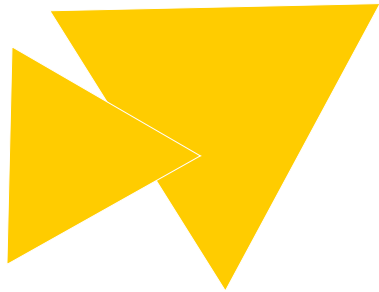

16:22
56 %
30
Bünde
Oeynhausen
Rinteln
Enger
Herford
Kalletal
Bielefeld
Oerlinghausen
Detmold
Schloß Holte-
Stukenbrock
Verl
07:18
+0
Bielefeld Hbf (Gleis 1)
RB73
Lage-Ehlenbruch
5 Haltestellen
0:22
07:40
+0
Lage-Ehlenbruch (Gleis 1)
07:46
+0
Lage-Ehlenbruch (Gleis SEV)
SEVSEV
Lemgo-Lüttfeld
2 Haltestellen
0:27
08:13
+0
Lemgo

Links & Literatur

- **PRISM Break zu Android & iOS**
  - https://prism-break.org/de/categories/android/
  - https://prism-break.org/de/categories/ios/
- **Artikelreihen zu Android von Mike Kuketz**
  - https://www.kuketz-blog.de/android-ohne-google-take-back-control-teil1/
  - https://www.kuketz-blog.de/your-phone-your-data-light-android-unter-kontrolle/
- **Digitalcourage: Digitale Selbstverteidigung**
  - https://digitalcourage.de/digitale-selbstverteidigung/mobil

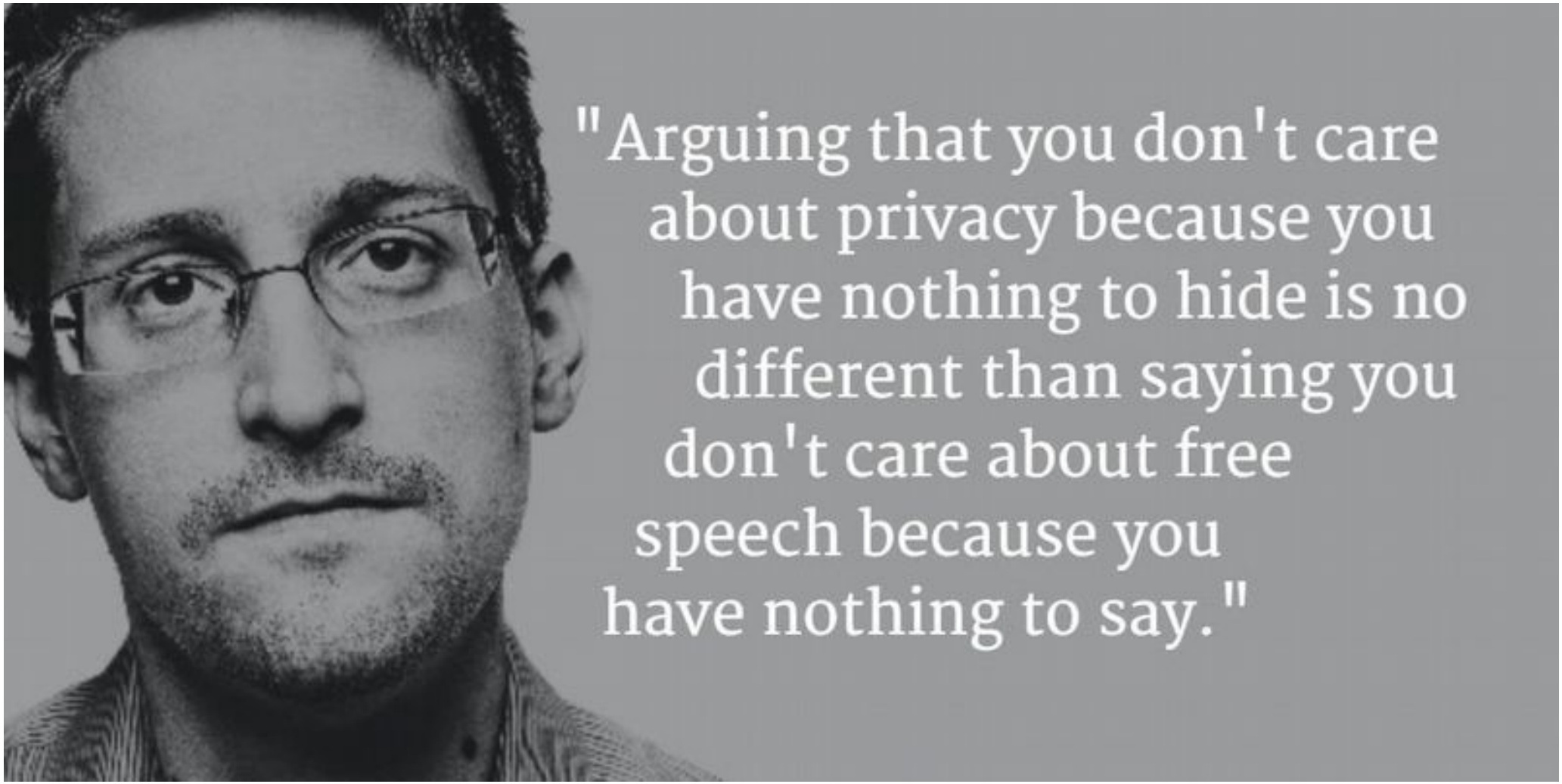
Vielen Dank
für die Aufmerksamkeit

Fragen?!



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 weltweit!**
  - https://www.cryptoparty.in/ (auf Englisch)
- **Freifunk Bielefeld**
  - https://www.freifunk-bielefeld.de/


"Arguing that you don't care about privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say."

- Praxis -