Crypto-Seminar
Fachhochschule Bielefeld

13. Juni 2019

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/hsgbi)***
  - 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

DONNERSTAG

- **Warum** sollte ich eigentlich **verschlüsseln**?
  - 14:00 bis 15:00
- **Browser**
  - 15:00 bis 16:00
- **Passwörter**
  - 16:10 bis 16:40
  - **Praxis bis 18:00**

FREITAG

- Was ist ein sicheres **Passwort**?
- Wie kann ich meine **E-Mails** verschlüsseln?
- Wie richte ich mein **Smartphone** sicher ein?

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

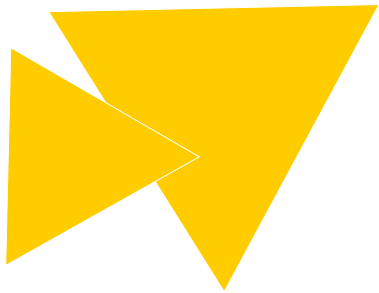
Privatsphäre – was ist das?

- „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

Privatsphäre

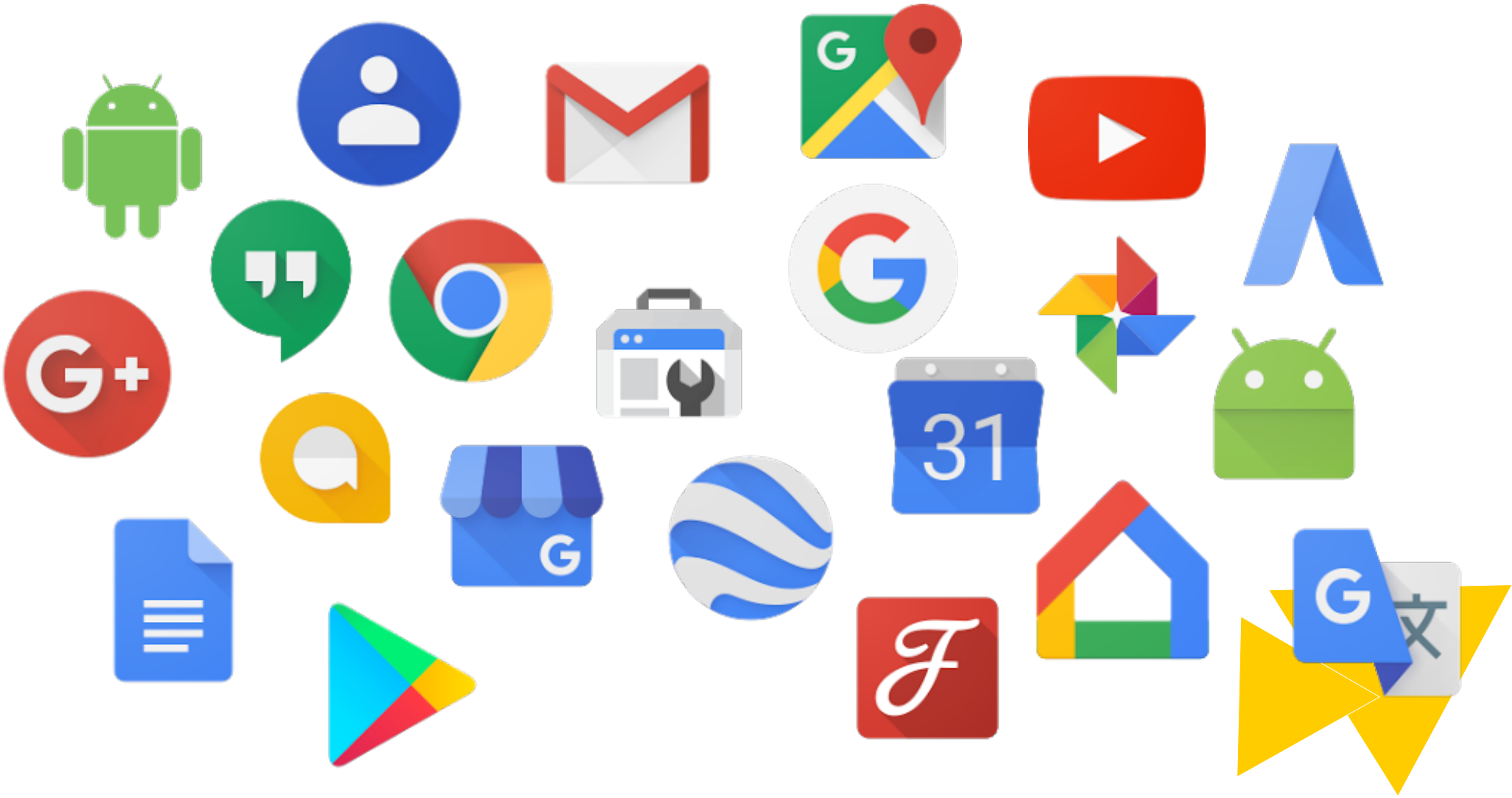
- **analog**
  - Privatsphäre selbstverständlich akzeptiert
  - Einbrüche in Privates meist erkennbar
  - Gesetze zum Schutz der Privatsphäre
    - Unverletzlichkeit der Wohnung
    - Briefgeheimnis
    - Freie Entfaltung der Persönlichkeit
- **digital**
  - neuer Wirtschaftsraum
  - neue technische Mechanismen / Möglichkeiten
  - intransparente Datenerhebung und -nutzung
  - technisches Verständnis häufig notwendig
  - Datenschutzgesetze nicht zeitgemäß, #neuland

Juristischer Ansatz

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

Digitale Identität

Google-Dienste

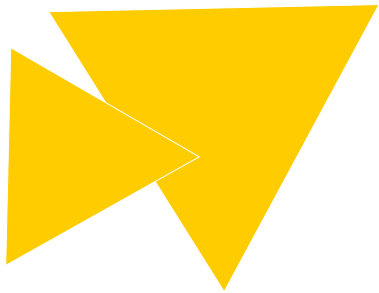


Zu niemandem ist man ehrlicher als zum Suchfeld von Google.

Constanze Kurz, Chaos Computer Club

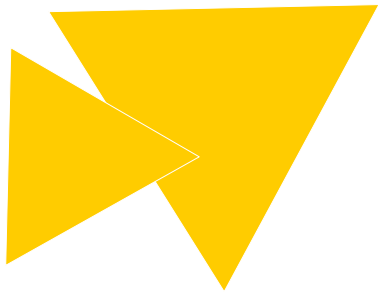
Was weiß Google?

- Suchbegriffe (Search History)
- eingegeben, gesehen, angeklickt
- IP-Adresse
- Sprache
- Datum, Uhrzeit
- Gerät, Betriebssystem, Browser
- Standort (GPS oder Browser)
- https://myactivity.google.com/



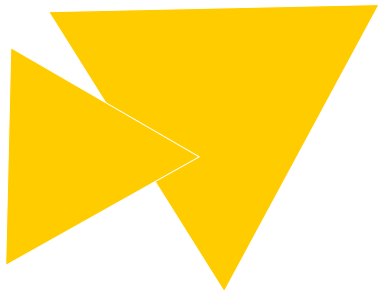
Google Analytics

- Einbindung auf Webseiten
- Statistiken für die Betreiber der Website
- Tracking der Besucher beim Seitenaufruf
  - IP-Adresse, Sprache, Land
  - Datum, Uhrzeit
  - Gerät, Betriebssystem, Browser
  - Bildschirmauflösung
  - Referer (von welcher Webseite gekommen)



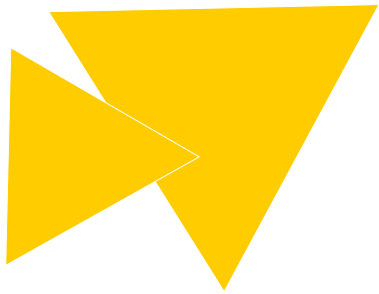
Facebook

- „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

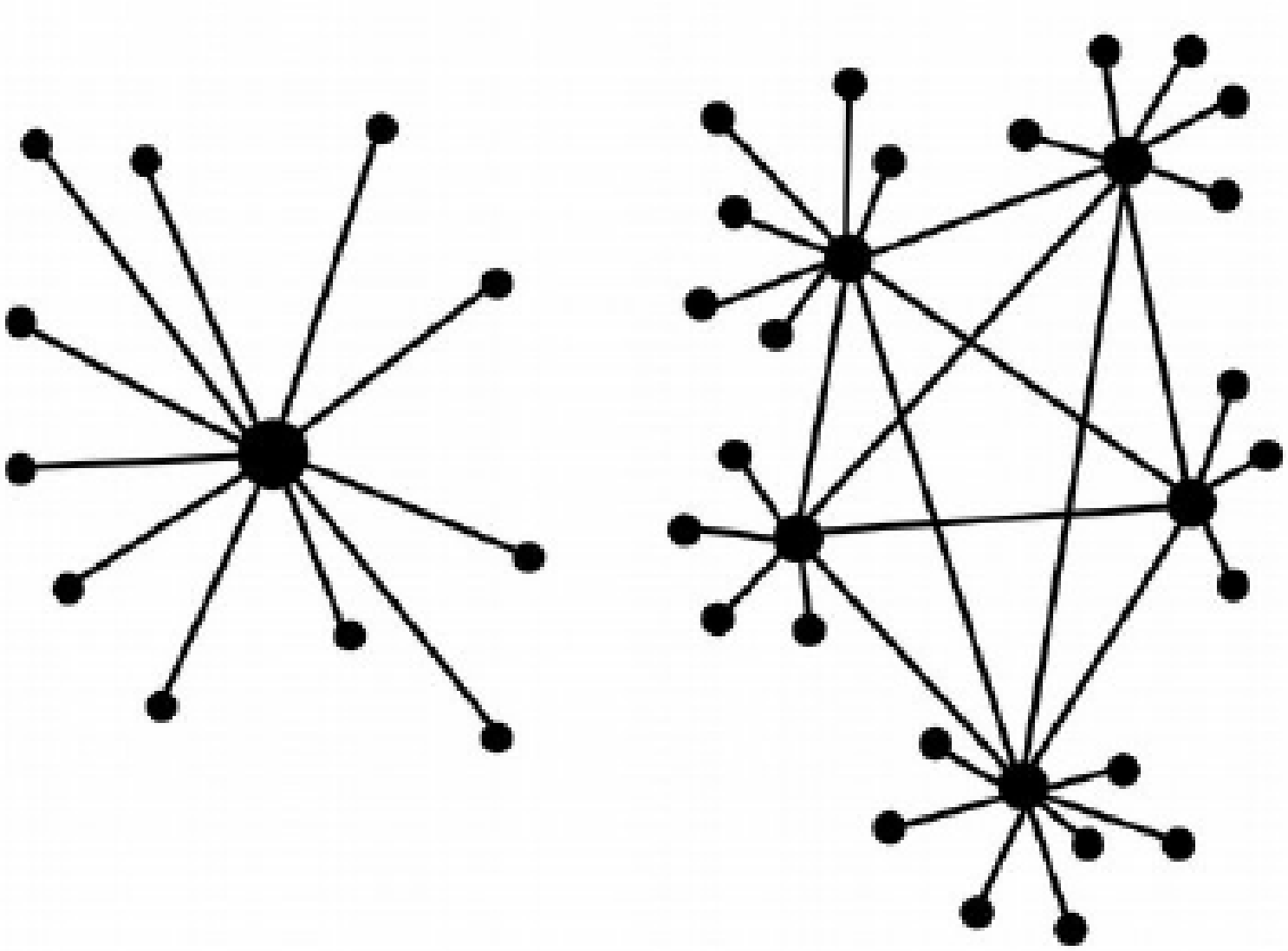
Facebook is watching you!

- Big Brother Award 2019 für *ZEIT ONLINE*, stellvertretend für rund ¾ aller Onlinezeitungen

Name	Startseite	Artikelseite	Aboseite
FAZ	😠	😠	😠
Handelsblatt	😠	😠	😠
taz	✅	✅	✅
Neue Westfälische	✅	✅	✅
Westfalen-Blatt	✅	✅	✅

Quelle: https://netzpolitik.org/2019/konzern-liest-mit-facebook-trackt-nutzer-auf-drei-viertel-aller-deutschen-nachrichtenseiten/

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

Vorratsdatenspeicherung (Historie)

- 2006: EU-Richtlinie
  - Nach und nach von vielen Mitgliedsstaaten umgesetzt
- 2010: Vom Bundesverfassungsgericht als verfassungswiedrig erklärt
- 2014: Vom EuGh wegen Verstoß gegen die Charta der Grundrechte als ungültig erklärt

VDS-Zombie

- 2015 vom Bundestag beschlossen als:
  - „Einführung einer Speicherpflicht und Höchstspeicherfrist für Verkehrsdaten“.
- Anfang 2017: Bundesverfassungsgericht lehnt Klärung im
- Eilrechtsschutzverfahren und Aufschub ab.
- Verfassungsbeschwerden laufen

Neusprech Award 2015

- Vorratsdatenspeicherung
- Mindestspeicherfrist, Mindestspeicherdauer
- Mindestdatenspeicherung
- Speicherpflicht und Höchstspeicherfrist für Verkehrsdaten
- private Vorsorgespeicherung
- Digitale Spurensicherung

VDS: Wer speichert?

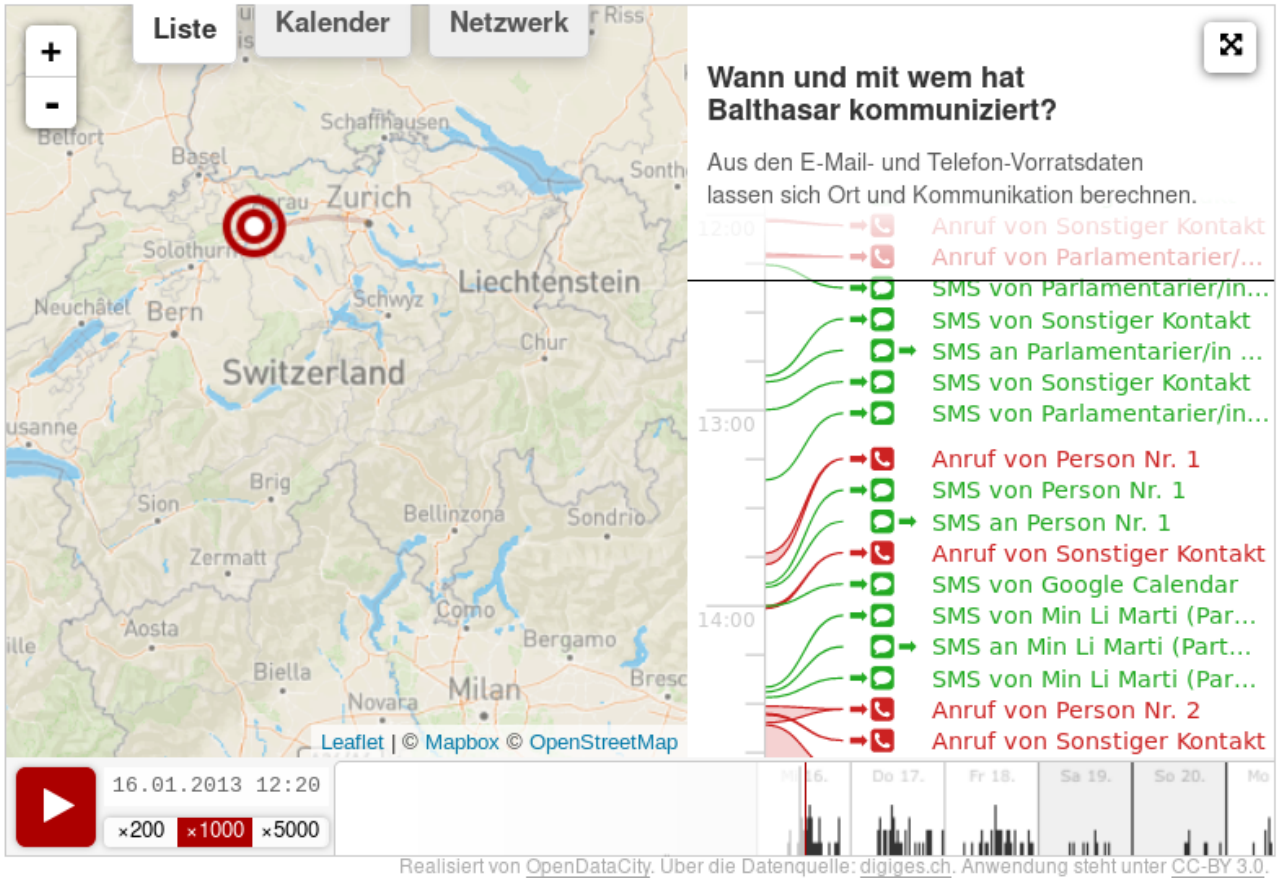
- Telekommunikationsanbieter
  - ISP (Internet-Service-Provider) & Mobilfunkanbieter
  - Outsourcing: VDS as a Service
- Polizeibehörden fordern Daten zur Aufklärung „schwerer Straftaten“ an.

VDS: Was wird gespeichert?

- Standortdaten aller Mobiltelefonate bei Beginn des Telefonats (für 4 Wochen)
- Standortdaten bei Beginn einer mobilen Internetnutzung (für 4 Wochen)
- Rufnummern, Zeit und Dauer aller Telefonate (für 10 Wochen)
- Rufnummern, Sende- und Empfangszeit aller SMS-Nachrichten (für 10 Wochen)
- Zugewiesene IP-Adressen aller Internetnutzer sowie Zeit und Dauer der Internetnutzung (für 10 Wochen)

VDS Visualisierung

- Balthasar Glättli (Grüne, Schweiz): https://www.digitale-gesellschaft.ch/vorratsdatenspeicherung/
- Malte Spitz (Grüne, Deutschland): http://www.zeit.de/datenschutz/malte-spitz-vorratsdaten



Telekommunikationsüberwachung 2015 nach Straftatbeständen

Quelle: https://netzpolitik.org/2015/statistiken-zur-telekommunikationsueberwachung-telefon-und-internet-ueberwachung-weiterhin-meistens-wegen-drogen/

VDS: Ausweitung

- schon vor Inkrafttreten des Gesetzes
- Vorratsdaten auch bei Wohnungseinbrüchen abfragen
- zusätzlich Funkzellenabfrage
- Kritik: Technik erst etablieren, dann ausweiten

Folgen von Massenüberwachung

- alle Bürger sind Verdächtige
- Schere im Kopf → Selbstzensur
- Chilling Effect → Angepasstes Verhalten
- Einschränkung vieler Grundrechte:
  - Meinungsfreiheit,
  - Briefgeheimnis,
  - Freie Entfaltung der Persönlichkeit

Massenüberwachung durch die NSA

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

Leseempfehlungen

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

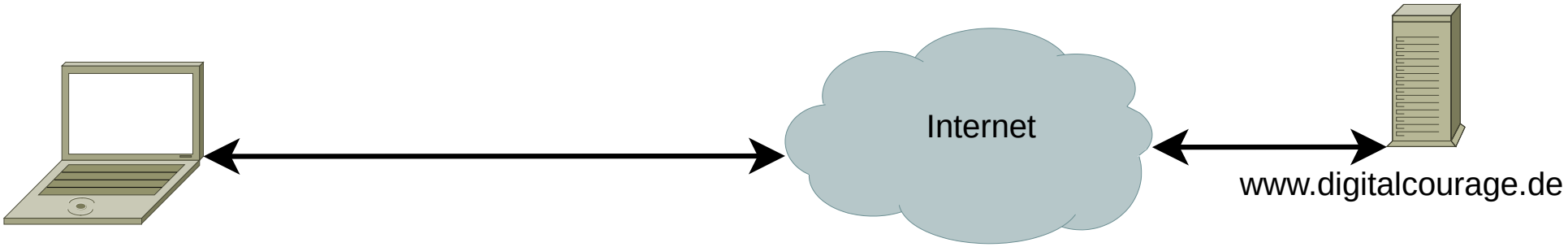
Freie Software

- **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)

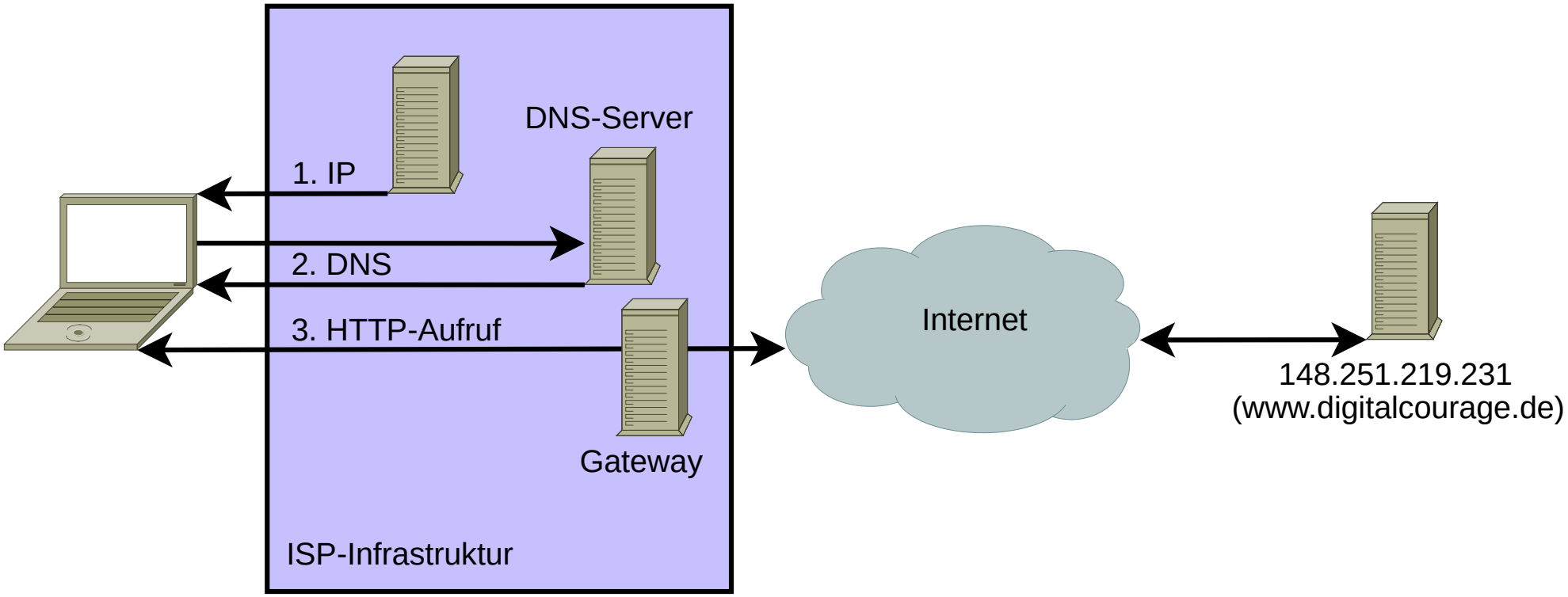
Sicher unterwegs im Web: Browser mit Privatsphäre

Georg

Wie funktioniert das Web?



Und technisch?

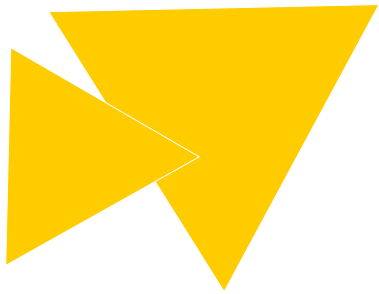


Wie schrecklich ist die Web-Realität (mit Standardeinstellungen)?

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

… so schrecklich!

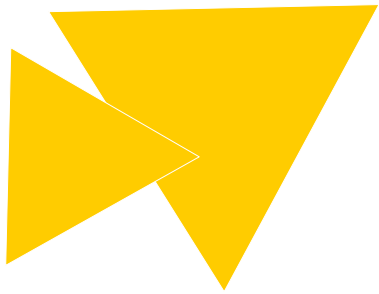
- Beispiel: **https**://www.spiegel.de/ (mit Standard-Firefox 67)
- 424 (nach 20s) Anfragen an mehr als 56 externe Server...
- www.spiegel.de, magazin.spiegel.de, cdn1.spiegel.de, count.spiegel.de, fsm2.spiegel.de, m.spiegel.de



… 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

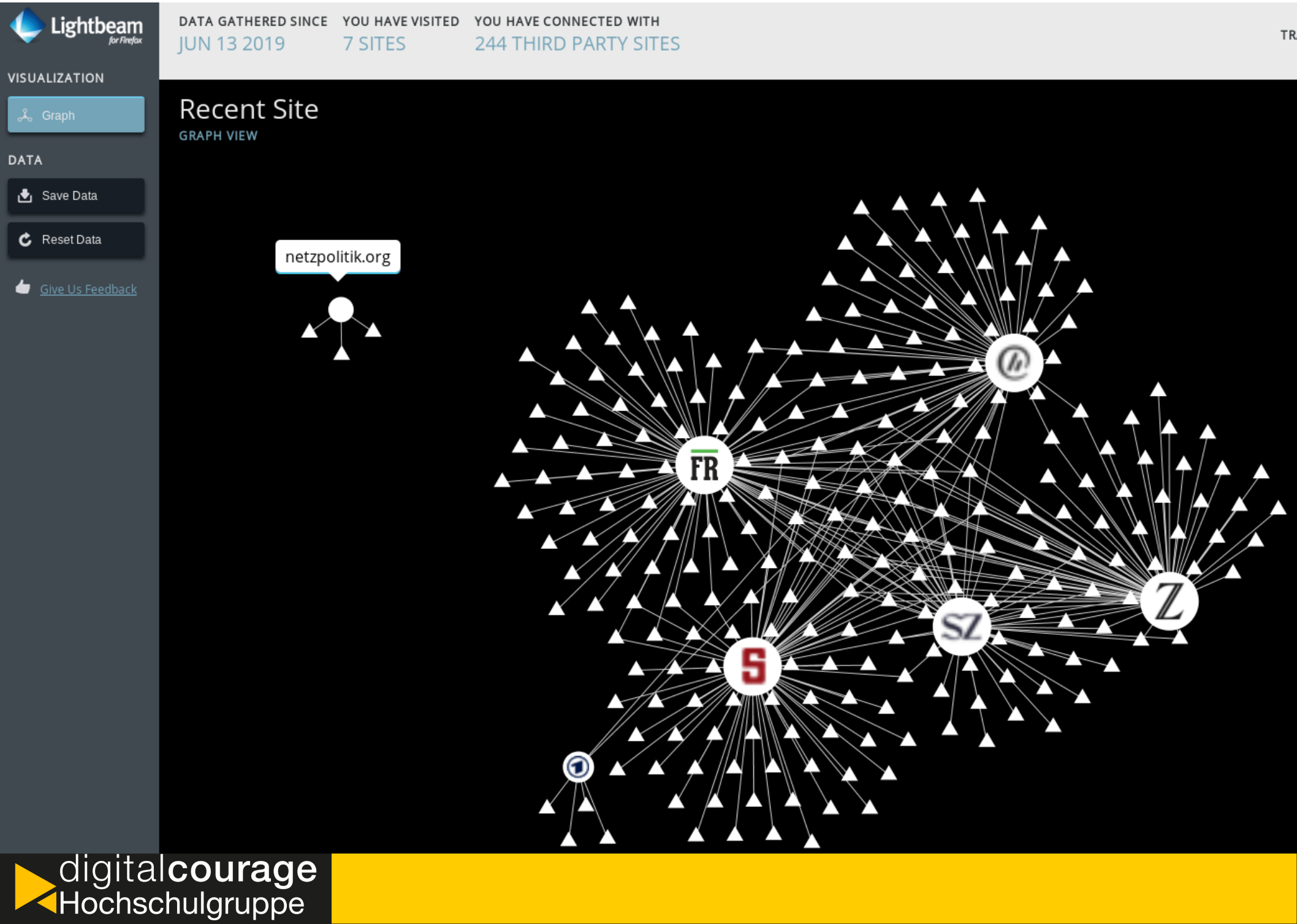


… so schrecklich!

- 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. + Nachladen (Test ohne Interaktion und Scrollen)



digitalcourage
Hochschulgruppe

(Bild: CC-BY-2.0: EFF)

Lightbeam for Firefox

VISUALIZATION

Graph

DATA

Save Data

Reset Data

Give Us Feedback

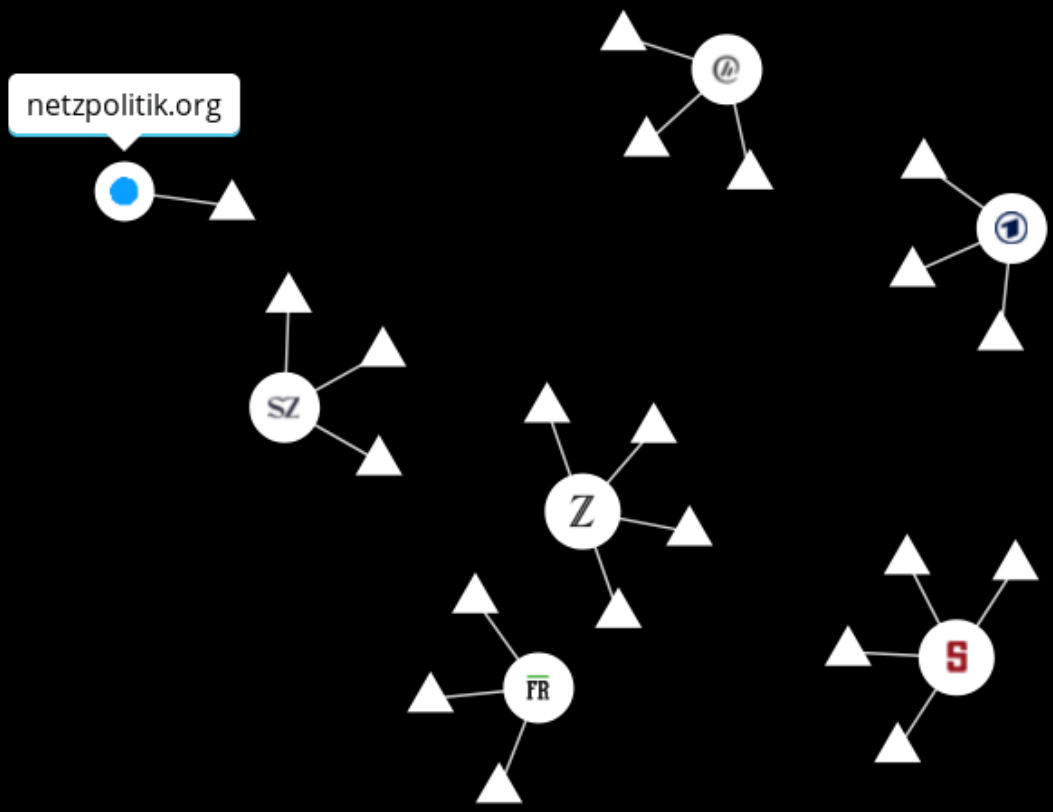
DATA GATHERED SINCE
JUN 13 2019

YOU HAVE VISITED
7 SITES

YOU HAVE CONNECTED WITH
21 THIRD PARTY SITES

Recent Site

GRAPH VIEW



digitalcourage
Hochschulgruppe

https://webbkoll.dataskydd.net/de

digitalcourage Hochschulgruppe

Here’s how we take back the Internet

– title of a TED Talk by Edward Snowden

Sicheres Surfen mit Privatsphäre

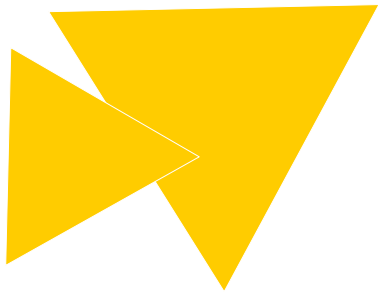
Was wollen wir?

- Sicherheit:
  - Vertraulichkeit
  - Authentiziät
  - Integrität

Sicheres Surfen mit Privatsphäre

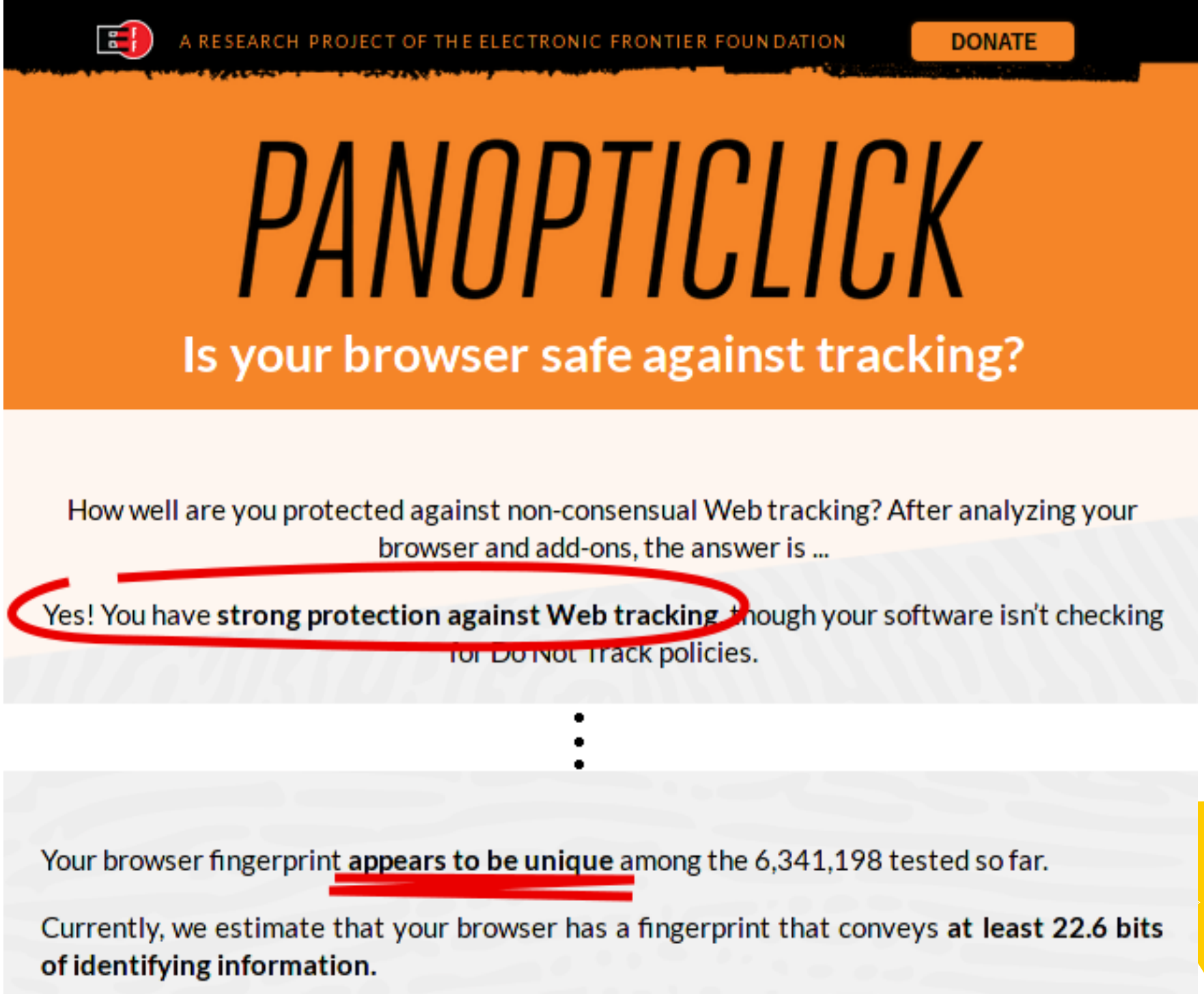
Was wollen wir?

- 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


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, Qwant.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

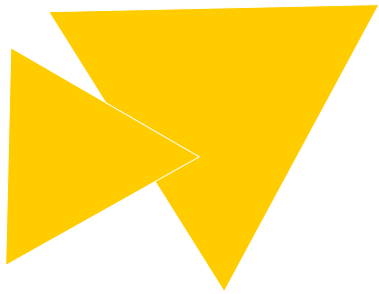
Firefox-Add-ons

für Fortgeschrittene:

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

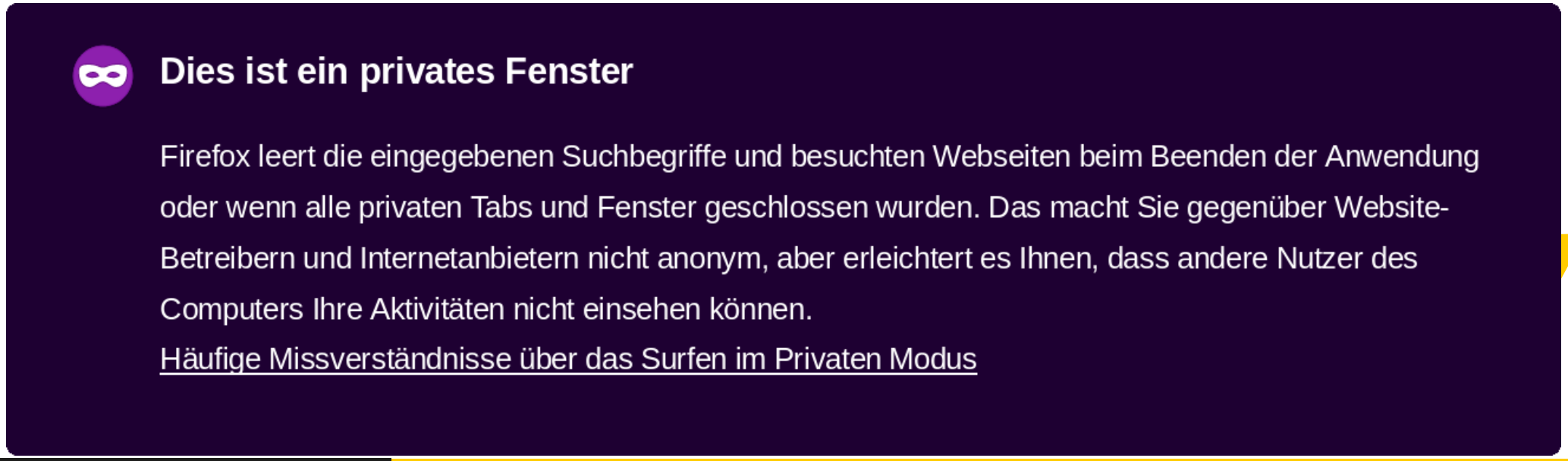
Kontrolle

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



Exkurs: Privater Modus von Firefox

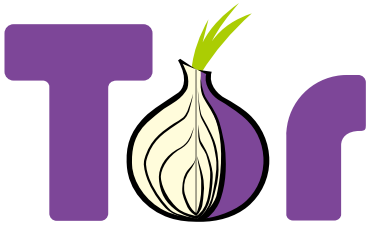
- keine Speicherung von Daten besuchter Webseiten **auf dem eigenen** Computer (insbesondere keine Chronik, keine URL-Vervollständigung, Cookies, etc.)
- auf dem lokalen System verbleiben keine Spuren
- *keine Anonymität* gegenüber dem Netz



Sicheres Surfen mit Privatsphäre

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

Anonym surfen mit dem Tor-Browser



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

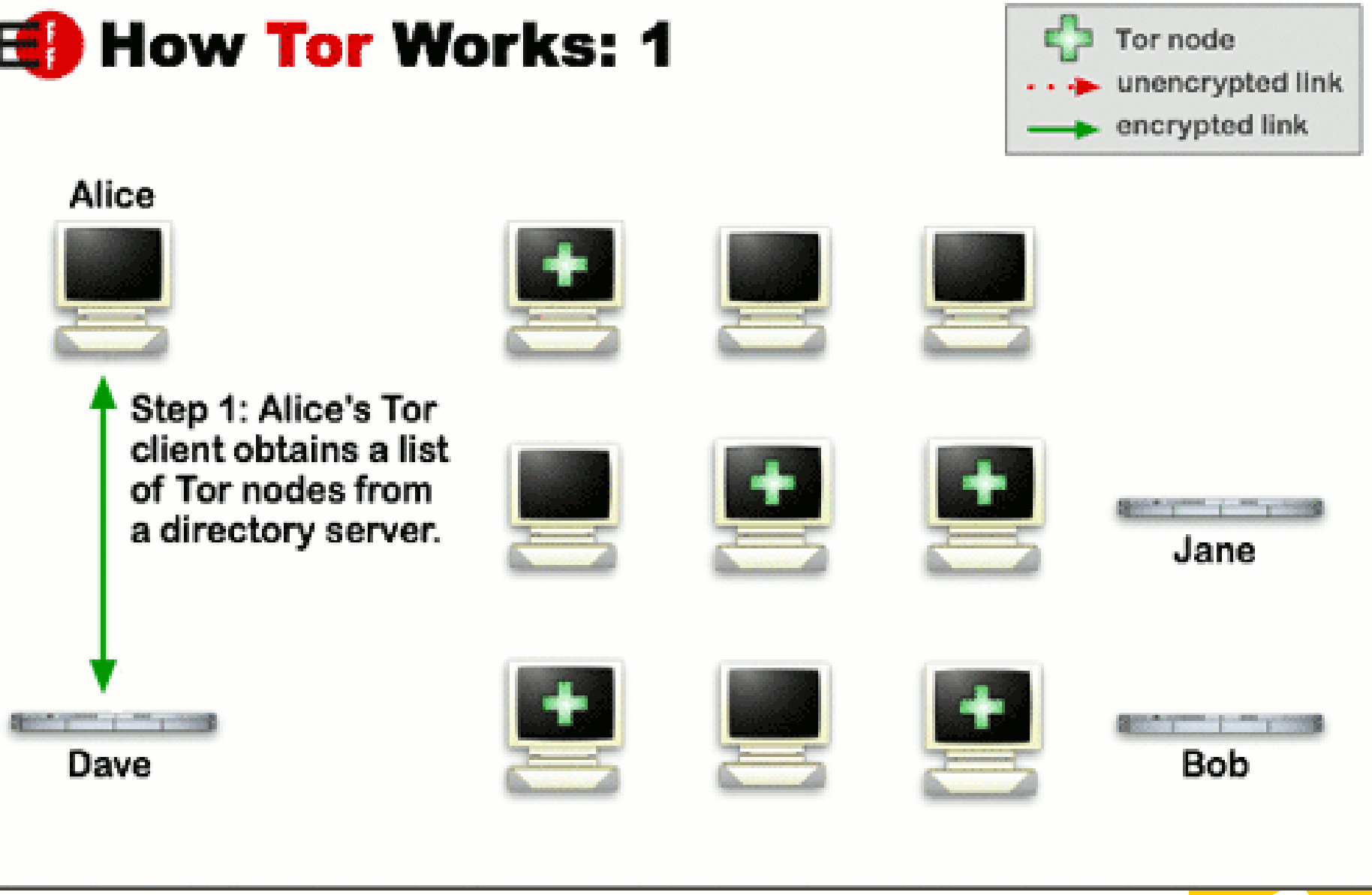
Vorteile

- quelloffen, freie Software
- anonymes Surfen

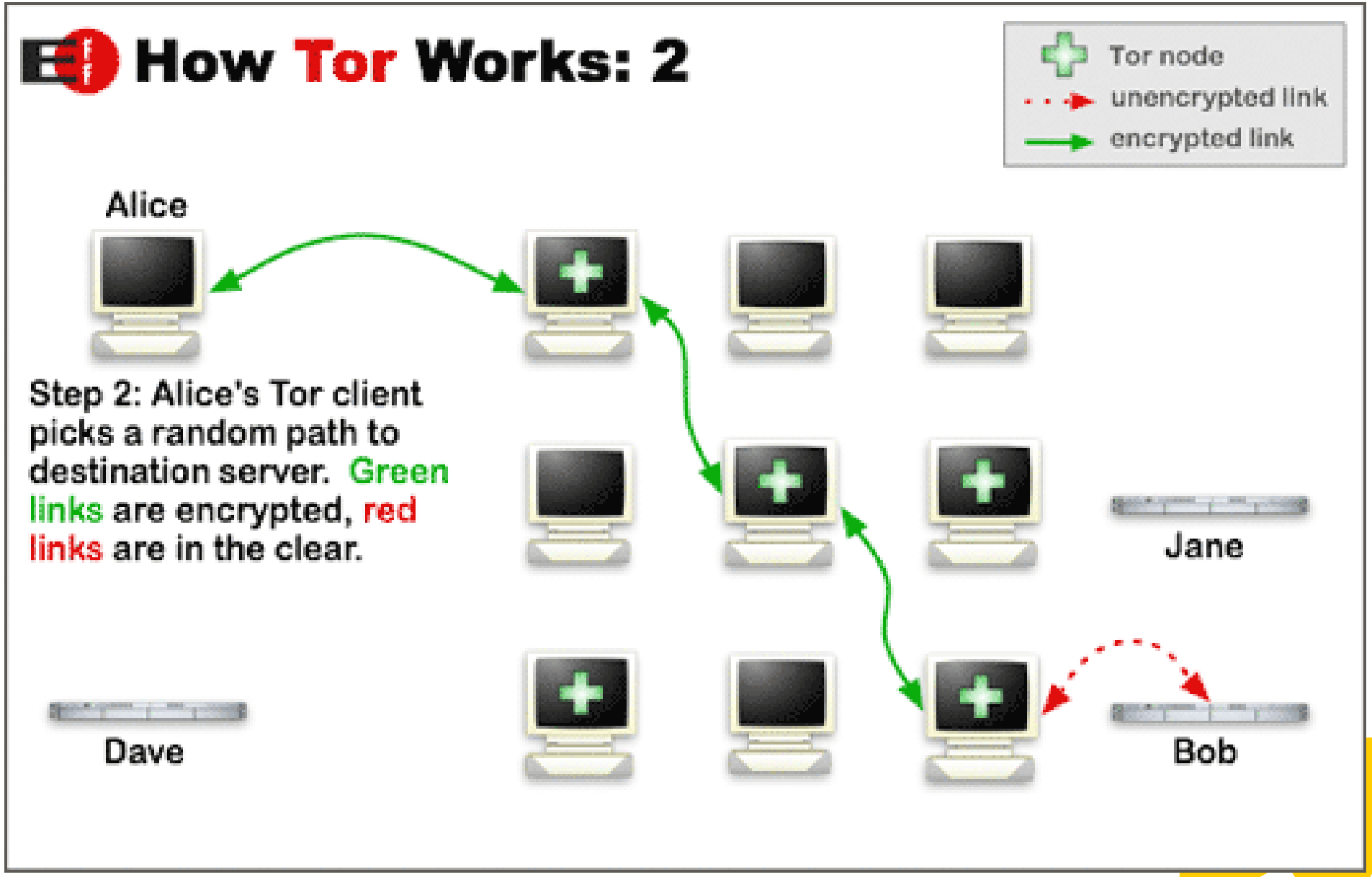
Nachteile

- Login bei personalisierten Seiten nicht sinnvoll
- Latenz ist größer

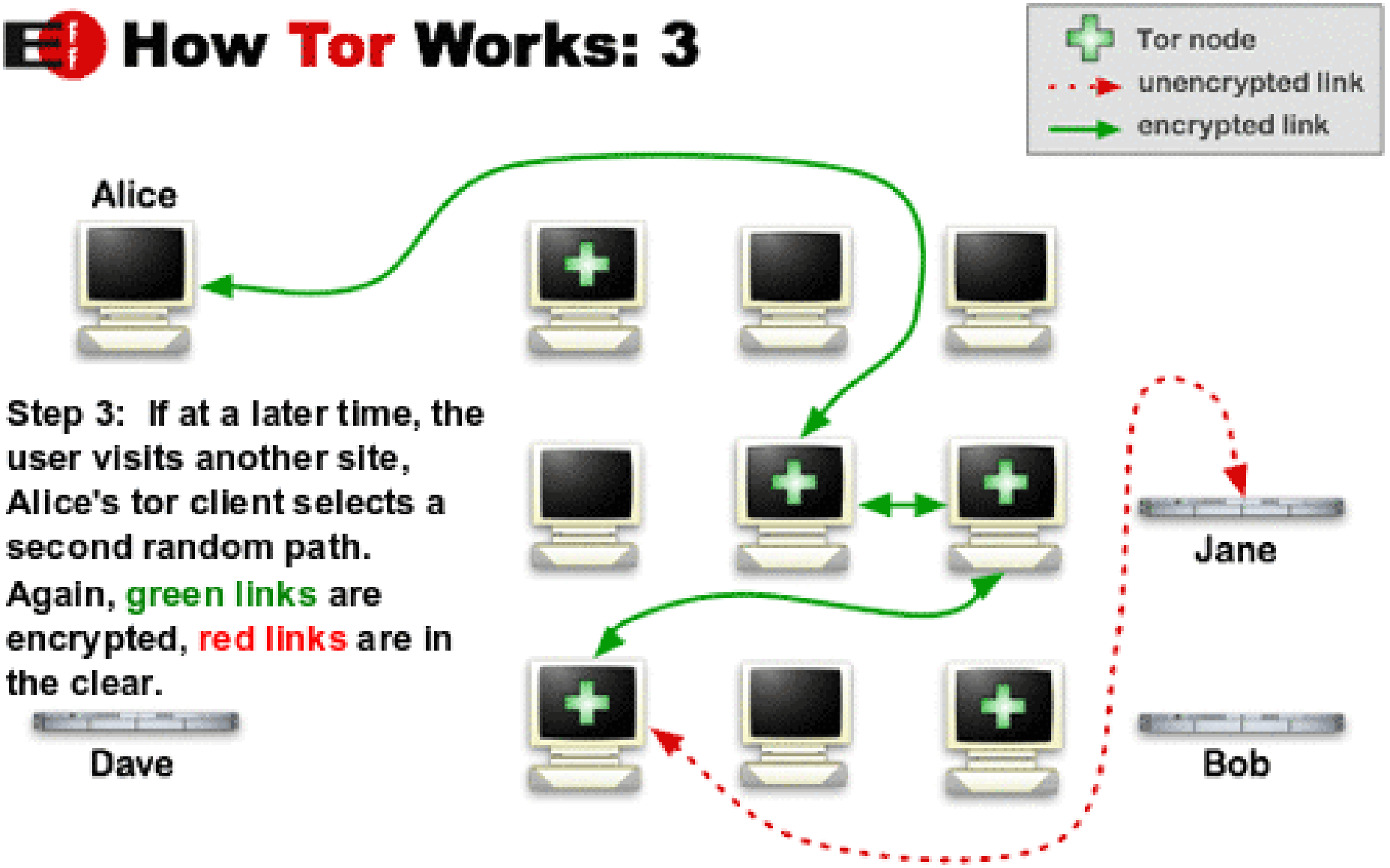
How Tor Works: 1



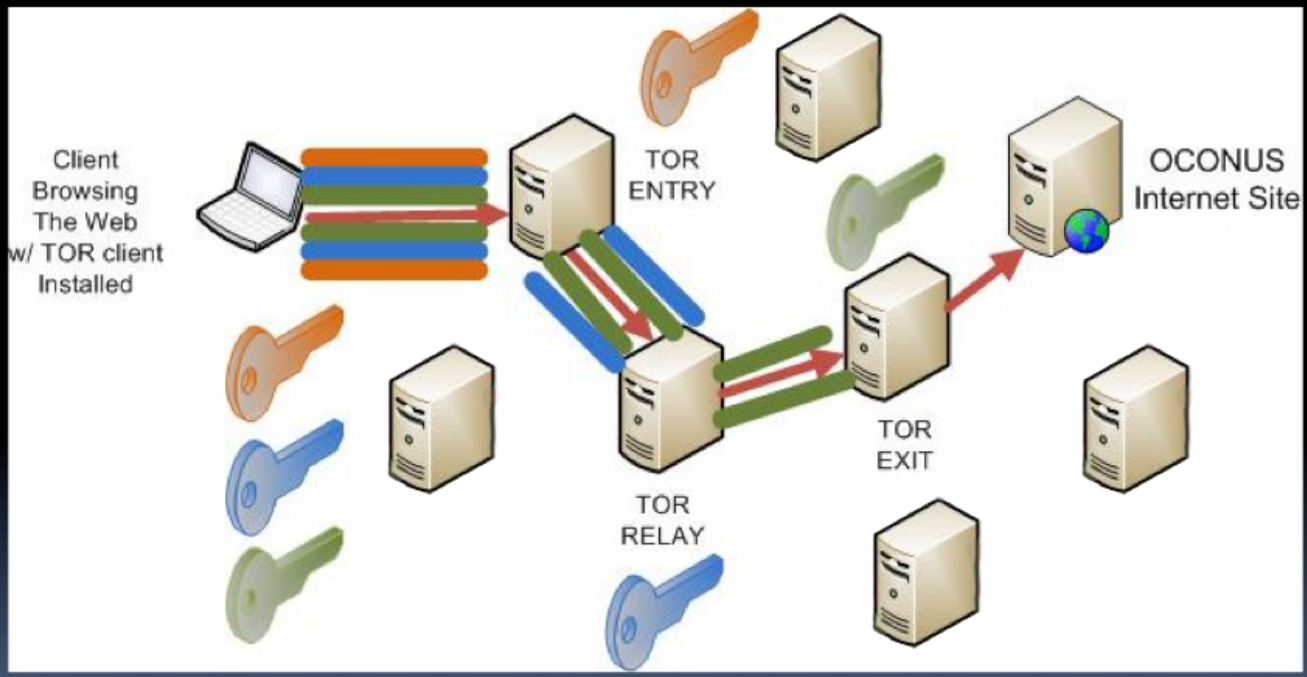
How Tor Works: 2



How Tor Works: 3



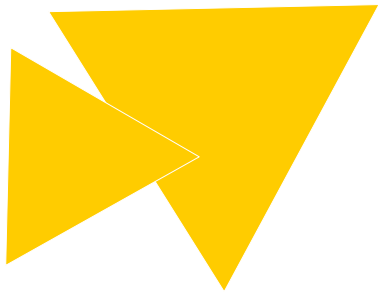
(U) What is TOR?

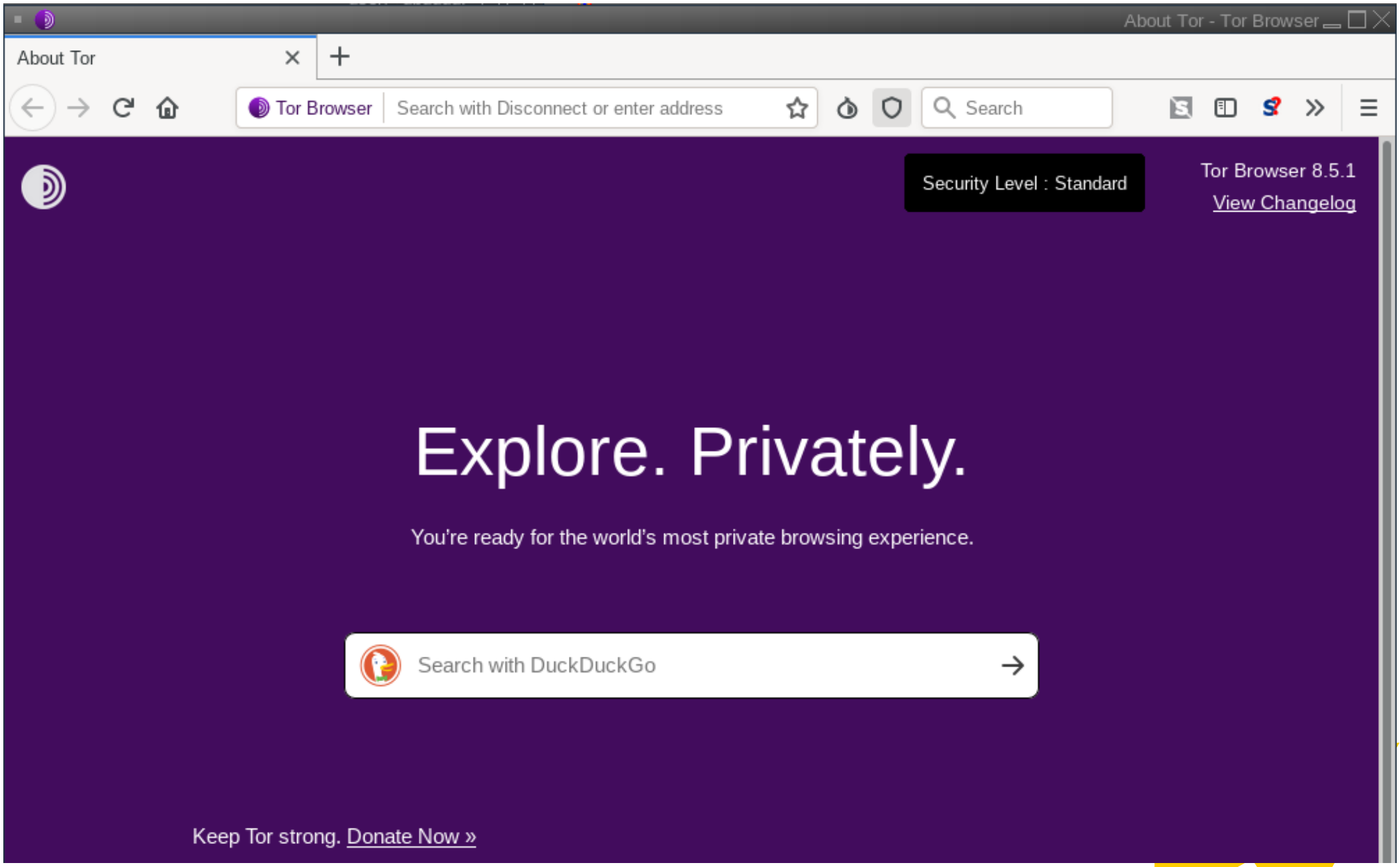


digitalcourage
Hochschulgruppe

Download Tor-Browser

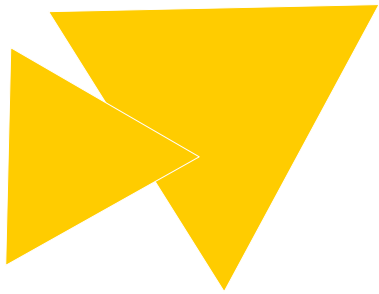
- Firefox + Tor + NoScript + HTTPS-Everywhere
- Download unter: https://www.torproject.org/
- Einstellungsoptionen:




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/

„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.

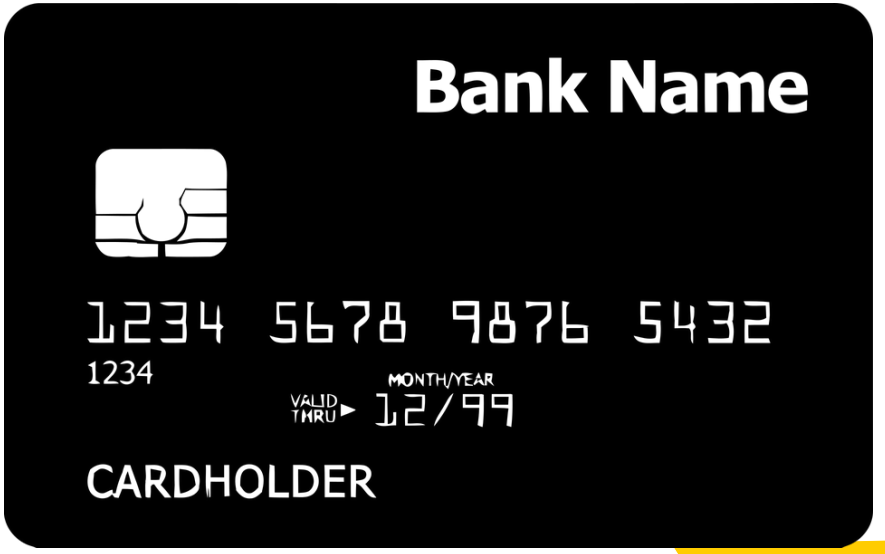
Wie erschwert man das Knacken des Passworts?

- 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

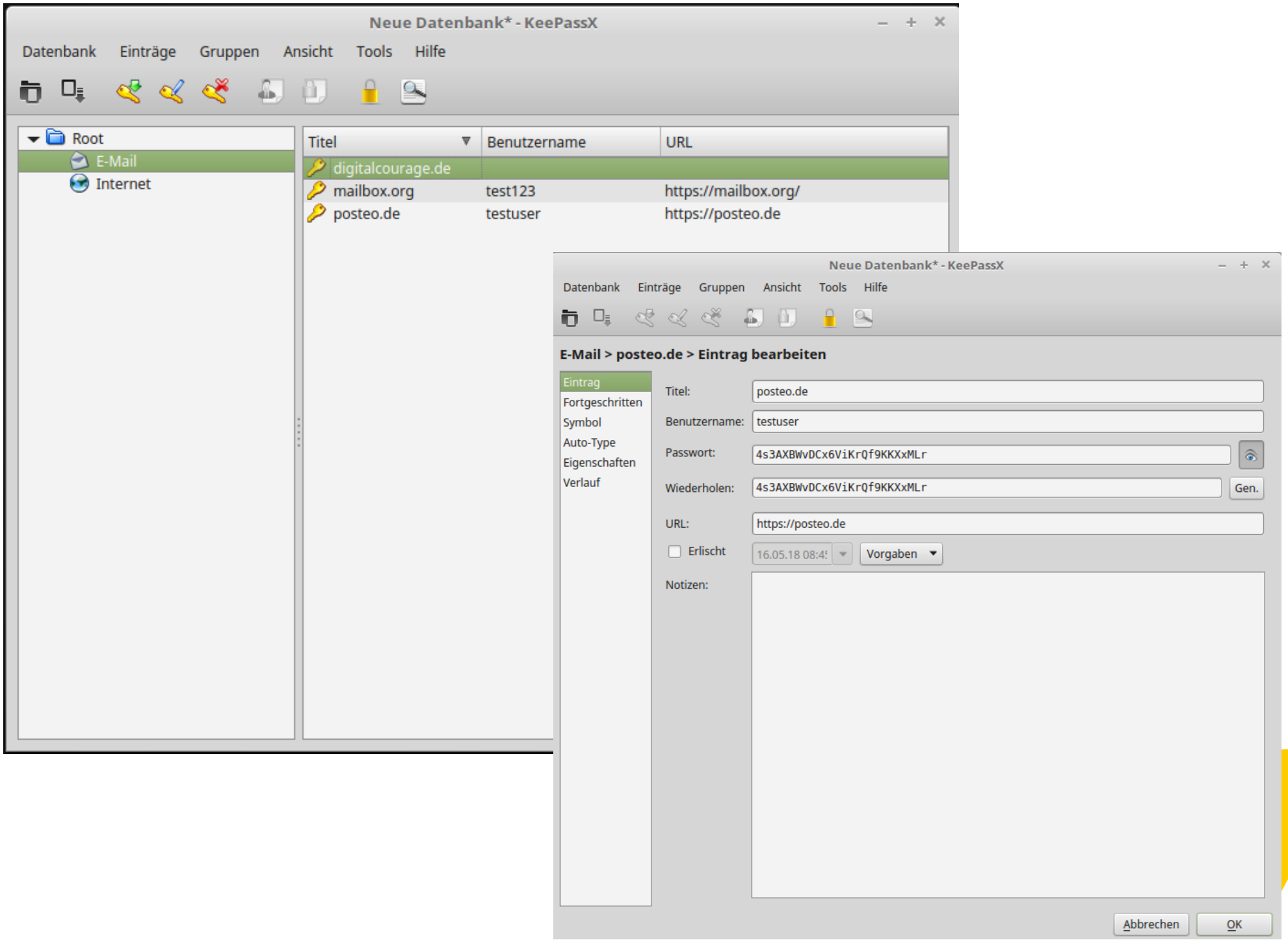
Software: **KeePassX**

Vorteile

- Freie Software
- viele Plattformen
  - Win, Linux, Mac, Android
- 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
16.05.18 08:4
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

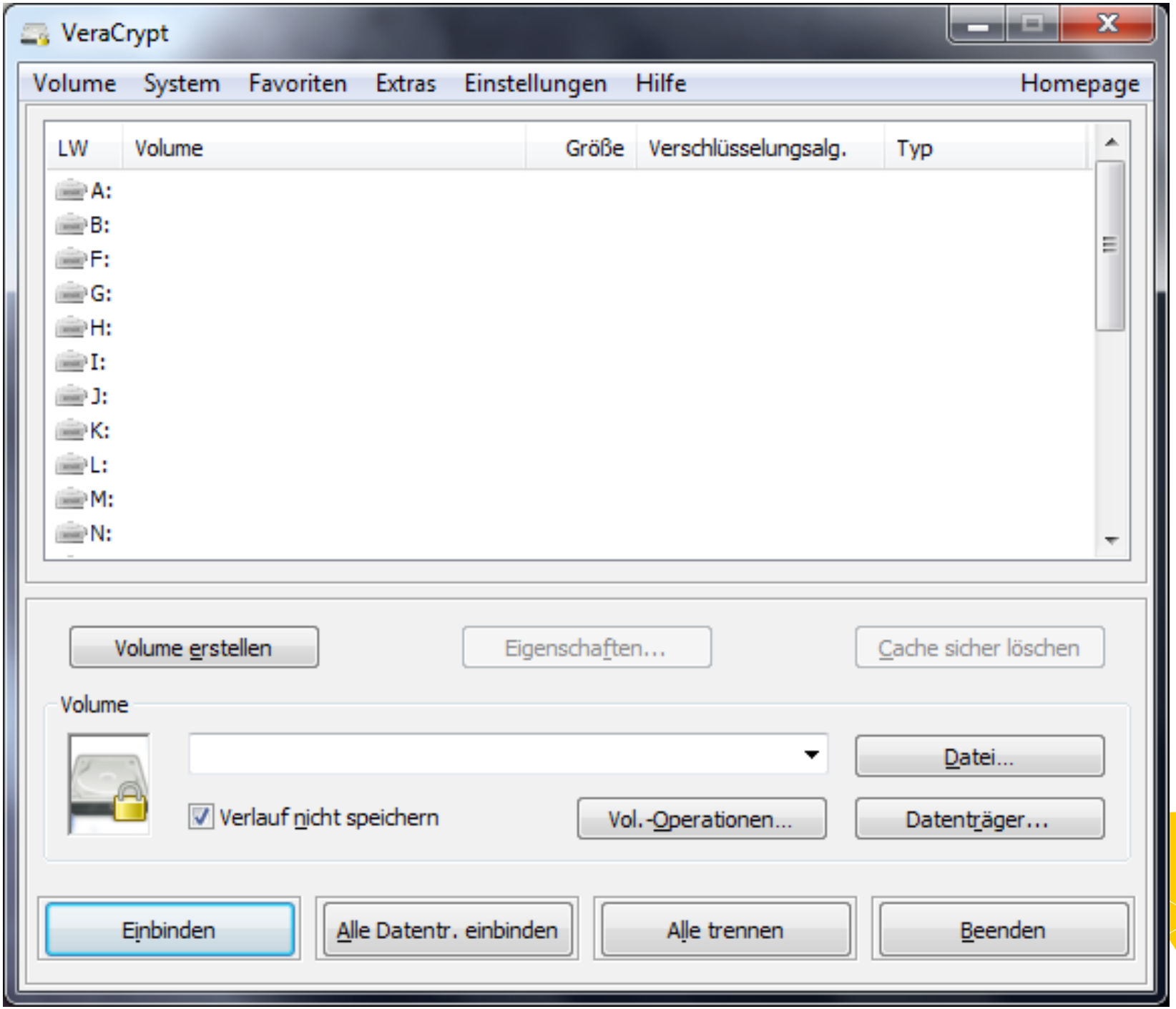
- Weil Ihr ein Grundrecht auf digitale Privat- und Intimsphäre habt!
  - „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“ – sogenanntes IT-Grundrecht
  - Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG

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

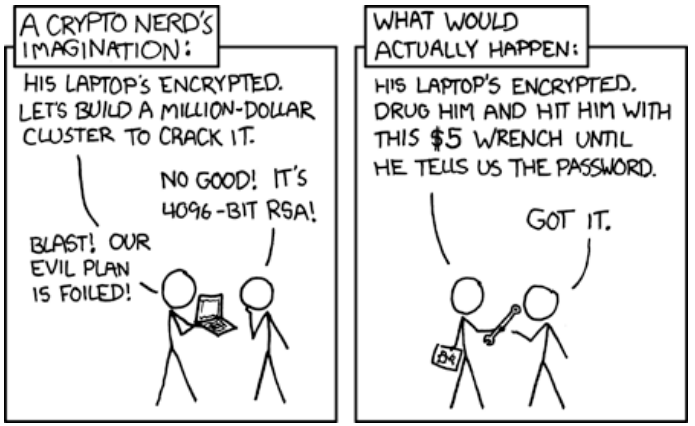
- quelloffen, freie Software
- nachvollziehbare Änderungen am Code
- plattformübergreifend
- auf USB-Stick transportierbar
- unabhängiger Audit

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