

# Digitale Anonymität

vmann & mike

# Anonymität

Was ist Anonymität?

- ▶ Mensch ist anonym, wenn es nicht identifiziert werden kann
- ▶ Identitäten sind schwer komplett zu trennen

Warum ist das wichtig?

- ▶ Antirepression
- ▶ Weil es niemanden etwas angeht wo du grade bist und was du gerade tust!

# Wer will eins identifizieren?

Der Staat

- ▶ Strafverfolgung
- ▶ Überblick über politische Bewegungen

Konzerne

- ▶ Personalisierte Werbung
- ▶ Arbeiten manchmal mit Staaten zusammen

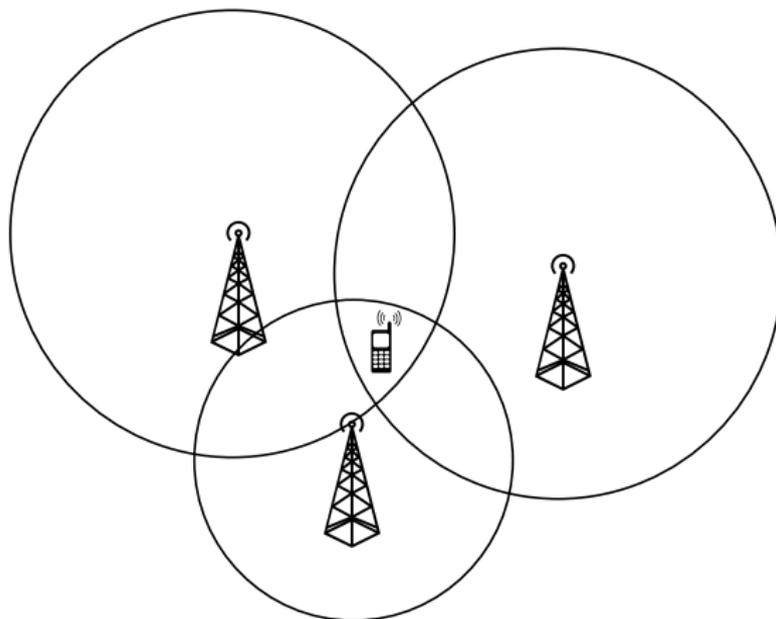
Nicht alles, was technisch möglich ist, ist auch legal oder wird gemacht.

Auch Nazis oder Stalker wollen eins vielleicht identifizieren - werden aber hier nicht behandelt.

# Handys - IMSI und IMEI

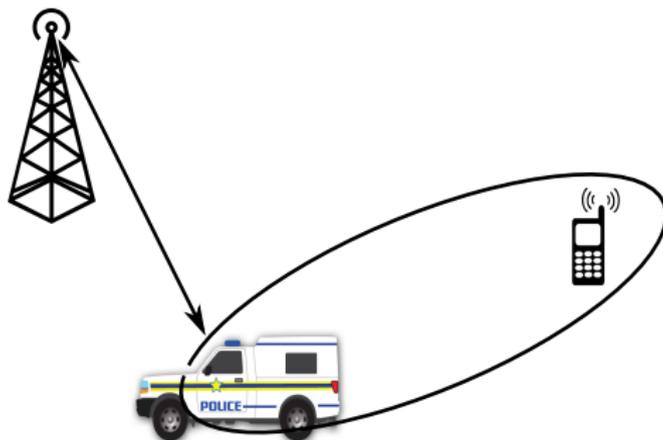
- ▶ IMEI - International Mobile Equipment Identity, eindeutige Nr des Handys
- ▶ IMSI - International Mobile Subscriber Identity, eindeutige Nr der SIM-Karte
- ▶ Seit 2017 Klarnamens-Pflicht für SIM-Karten, aber anonym bei "kleinen" Shops erhältlich

# Handys - Funkzellenabfrage



- ▶ Funkzelle zeichnet Zeit, IMSI, IMEI, groben Standort und Gesprächspartner auf

# Handys - IMSI-Catcher

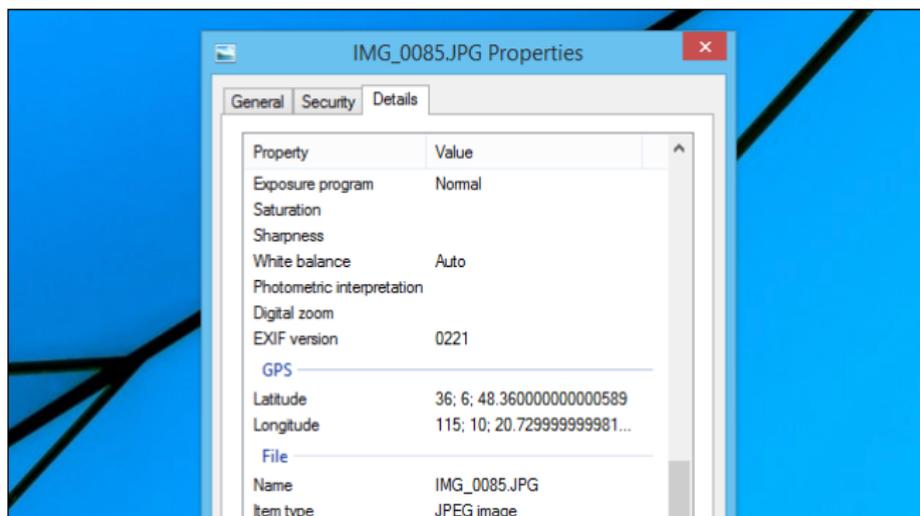


- ▶ Fake-Funkzelle
- ▶ Ermöglicht genauere Ortung und Abhören
- ▶ Manchmal an ungewöhnlich gutem Empfang oder anderer/unterdrückter Nr bei ausgehenden Anrufen erkennbar

# Aktions-Handys

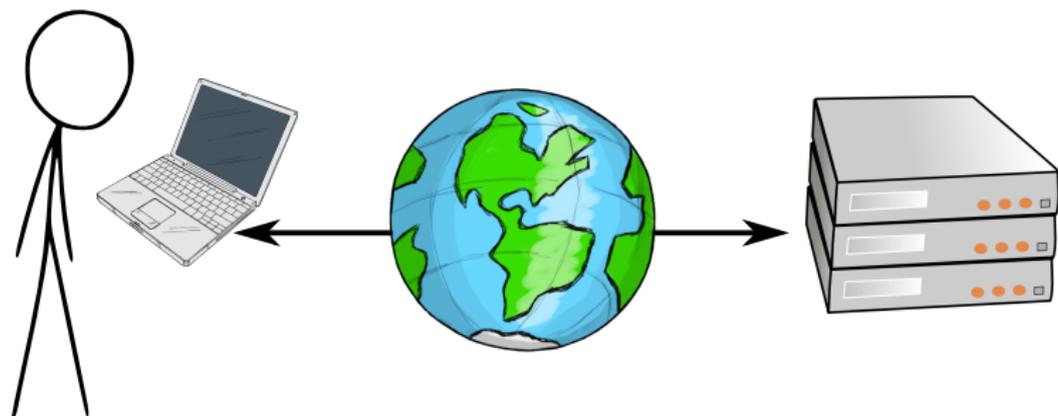
- ▶ Wiederverwendung von SIM **oder** Handy ermöglicht Zuordnung
- ▶ Jede Nutzung ist ein Datenpunkt der Eingrenzung ermöglicht
- ▶ “Alltags-Handy aus - Aktions-Handy ein” ist ein sehr auffälliges Pattern

# Veröffentlichungen



- ▶ Bild-Metadaten - Kamera, Zeit, Ort, ...
- ▶ Netzbrummen in Audio/Video-Aufnahmen
- ▶ Autoren-Analyse

# Tracking im Internet



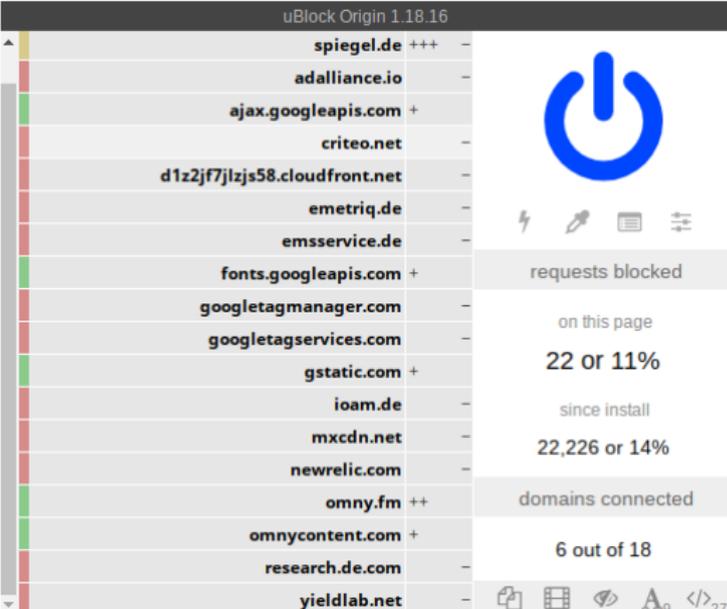
- ▶ IP-Adresse
- ▶ Cookies - Daten die Websites in eurem Browser ablegen
- ▶ Browser/Betriebssystem-“Fingerabdruck”  
(<https://panopticlick.eff.org/>)

# Tracking im Internet - Soziale Netze



- ▶ Beziehungen, Mail-Adresse, Handy-Nr., Klarnamen
- ▶ Tracking von Nutzer-Verhalten
- ▶ Nach Möglichkeit nicht und wenn dann nur im Private Browsing Mode benutzen (und Browser nach Benutzung wieder schließen)

# Tracking im Internet - Werbenetzwerke



The screenshot shows the uBlock Origin 1.18.16 interface. On the left, a list of domains is displayed with their respective status (e.g., blocked, allowed) and a color-coded bar. On the right, a large blue power button icon is visible, along with a summary of blocked requests: 22 or 11% on this page, and 22,226 or 14% since install. Below this, it shows 6 out of 18 domains connected. At the bottom right, there are icons for copy, list, refresh, font size, and code view.

Domain	Status
spiegel.de	+++ -
adalliance.io	-
ajax.googleapis.com	+
criteo.net	-
d1z2jf7jlzjs58.cloudfront.net	-
emetriq.de	-
emsservice.de	-
fonts.googleapis.com	+
googletagmanager.com	-
googletagservices.com	-
gstatic.com	+
ioam.de	-
mxcdn.net	-
newrelic.com	-
omny.fm	++
omnycontent.com	+
research.de.com	-
yieldlab.net	-

requests blocked

on this page  
22 or 11%

since install  
22,226 or 14%

domains connected

6 out of 18

- ▶ Nicht nur Anonymitäts-, sondern auch Sicherheitsrisiko
- ▶ Benutzt Ad-Blocker! (uBlock Origin)



Was ist Tor?

- ▶ Kurz für "The Onion Router"
- ▶ Tor-Browser (wie Firefox/Chrome/...) hilft anonym zu sein
- ▶ (außerdem gibt es Websites, die man nur mit diesem Browser erreichen kann)
- ▶ Kann man herunterladen auf <https://www.torproject.org/> und einfach starten

Wie funktioniert es?

# Wie Tor funktioniert: 1



## **E!** Wie Tor funktioniert: 2



Alice



Schritt 2: Nachdem der Torclient von Alice die Liste erhalten hat, weiß er, welche Rechner benutzt werden können.



Dave



Jane



Bob

## Wie Tor funktioniert: 3



Alice



Schritt 3: Der Torclient von Alice wählt einen zufälligen Pfad zum Zielserver.

Grüne Verbindungen sind verschlüsselt, rote Verbindungen nicht.



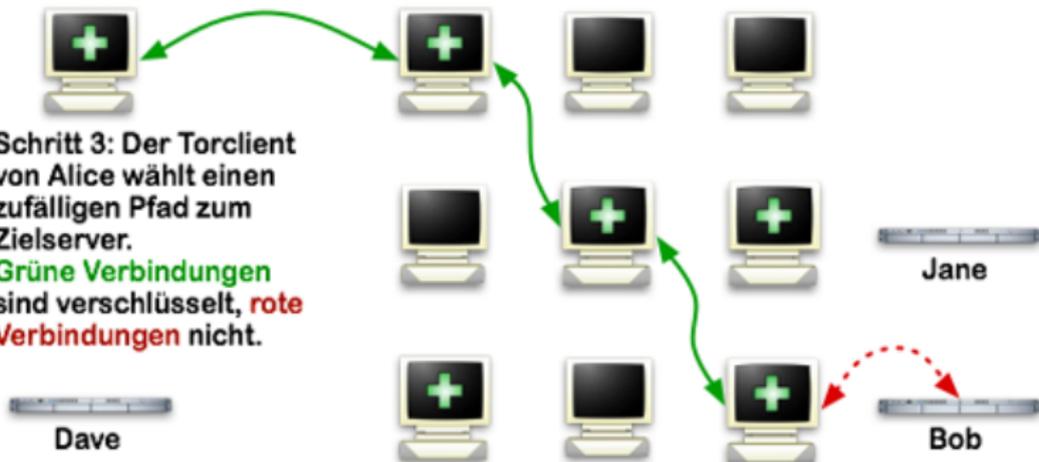
Dave



Jane



Bob



## Wie Tor funktioniert: 4



Alice



Schritt 4: Wenn der Nutzer auf eine andere Seite zugreifen möchte, wählt der Torclient von Alice einen zweiten zufälligen Pfad. Wiederum sind **grüne Verbindungen** verschlüsselt und **rote** nicht.



Dave



Jane



Bob

## Was ist das?

- ▶ TAILS ist ein Betriebssystem, das zum Ziel hat, anonymes Verhalten im Internet sicher und einfach zu machen.
- ▶ Kann man an alle möglichen PCs anstecken; beim Hochfahren im Boot Menü auswählen
- ▶ Sämtlicher Traffic wird über das Tor-Netzwerk geleitet
- ▶ Tor-Browser und andere Werkzeuge vorinstalliert
- ▶ Speichert keinerlei Daten - aber Encrypted Persistent Storage möglich

# Workshop!

Jetzt seid ihr dran!

Fragen?

Braucht ihr Hilfe bei der Installation oder beim Benutzen?

Wir sind für euch da :)

Danke fürs zuhören!