Crypto-Seminar
Fachhochschule Bielefeld

14. Juni 2019

digitalcourage
Hochschulgruppe

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
  (www.digitalcourage.de/hsg)
  - 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

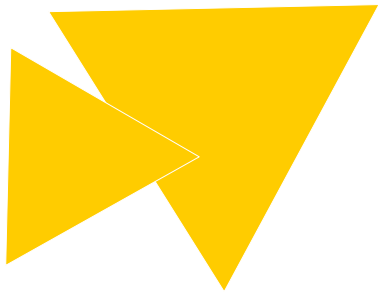
DONNERSTAG

- **Warum** sollte ich eigentlich **verschlüsseln**?
- **Browser**
- **Passwörter**
- **Praxis**

FREITAG

- Wie kann ich meine **E-Mails** verschlüsseln?
  - 14:00 bis 15:00 Uhr
- Wie richte ich mein **Smartphone** sicher ein?
  - 15:00 bis 16:00 Uhr
- **Praxis**
  - bis 17:00 Uhr (oder länger)

E-Mail-Verschlüsselung



Alternativen zu „kostenlosen“ E-Mail-Anbietern

- **Posteo.de** oder **mailbox.org**
- 24h-Einmal-E-Mail-Adresse, gratis: anonbox.net (CA-Cert)

Vorteile

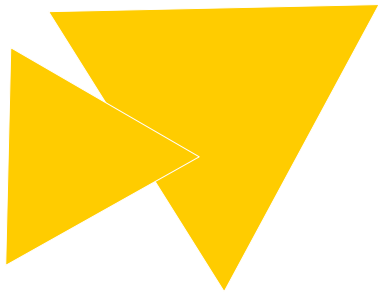
- Standort in Deutschland
- Datensparsamkeit
- keine Inhaltsanalyse
- keine Werbung
- anonyme Nutzung möglich
- Datenschutz hat Priorität

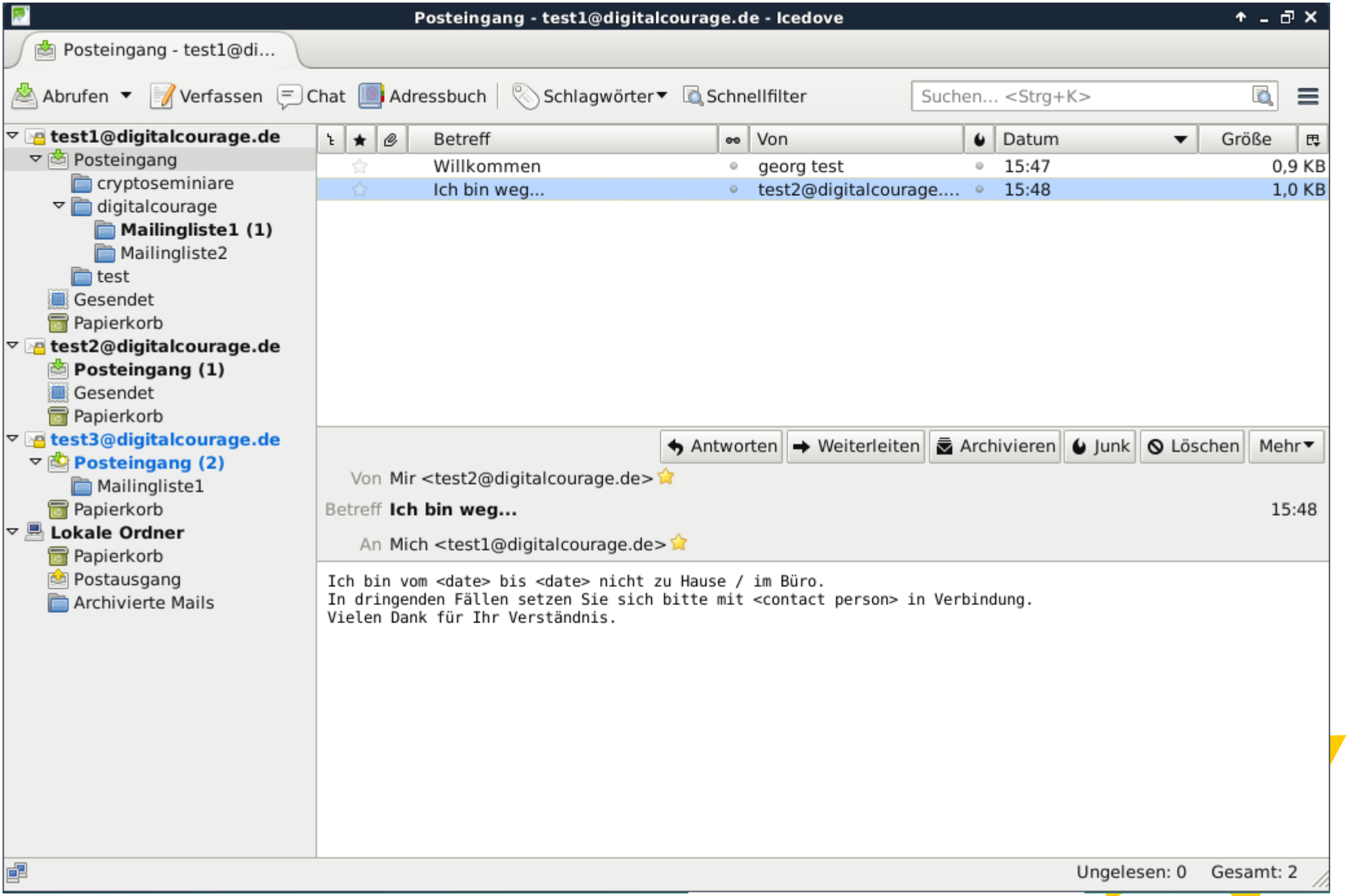
Nachteile

- posteo.de und mailbox.org kosten 1 € pro Monat

E-Mail-Verwaltung

- Software: **Mozilla Thunderbird**
  - Freie Software
  - mehrere Mail-Konten möglich
  - Verwaltung mit Filtern und Ordnern
  - HTML abschalten möglich
  - Mails offline lesen, speichern und durchsuchen
  - Add-ons: Kalender, Massenmails, **Verschlüsselung**




Posteingang - test1@digitalcourage.de - Icedove
Posteingang - test1@di...
Abrufen
Verfassen
Chat
Adressbuch
Schlagwörter
Schnellfilter
Suchen... <Strg+K>
test1@digitalcourage.de
Posteingang
cryptoseminiare
digitalcourage
Mailingliste1 (1)
Mailingliste2
test
Gesendet
Papierkorb
test2@digitalcourage.de
Posteingang (1)
Gesendet
Papierkorb
test3@digitalcourage.de
Posteingang (2)
Mailingliste1
Papierkorb
Lokale Ordner
Papierkorb
Postausgang
Archivierte Mails
Betreff
Von
Datum
Größe
Willkommen
georg test
15:47
0,9 KB
Ich bin weg...
test2@digitalcourage....
15:48
1,0 KB
Antworten
Weiterleiten
Archivieren
Junk
Löschen
Mehr
Von Mir <test2@digitalcourage.de>
Betreff Ich bin weg...
15:48
An Mich <test1@digitalcourage.de>
Ich bin vom <date> bis <date> nicht zu Hause / im Büro.
In dringenden Fällen setzen Sie sich bitte mit <contact person> in Verbindung.
Vielen Dank für Ihr Verständnis.
Ungelesen: 0
Gesamt: 2

E-Mail-Verschlüsselung (PGP / GnuPG)

Vorteile

- Inhalt Ende-zu-Ende-verschlüsselt
- Absender[1] & Empfängerin werden eindeutig
  ([1] mit PGP-Signatur)

Nachteile

- Metadaten (von, an, Betreff[2] etc). bleiben unverschlüsselt
  ([2] Enigmail ab 2.0 kann Betreff verschlüsseln)
- Absender & Empfängerin müssen PGP nutzen

Benötigte Software:

- E-Mail Programm: Thunderbird
- Add-on: **Enigmail**
  - **p≡p** (Pretty Easy Privacy) nutzen wir noch nicht (ggf. deaktivieren)

Verschlüsselung – was ist das eigentlich?

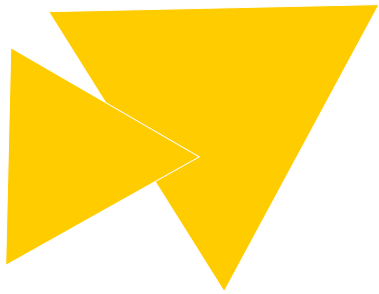
- Alice schreibt an Bob, Eve will mithören (eavesdrop) / Mallory (malicious) will manipulieren → man in the middle

- Beispiele und Grundprinzipien
  - meist gibt es ein **Verfahren** mit **Schlüssel**
  - Caesar-Verschlüsselung: einheitliche Verschiebung, 3 Positionen – wurde tatsächlich von Caesar und lange danach eingesetzt
  - ab 16. Jahrhundert komplexere Verfahren, noch im 1. Weltkrieg handschriftlich, 2. Weltkrieg Enigma – entscheidende Misserfolge
  - Vertrauen in moderne Kryprographie beruht darauf, dass das **Verfahren offen**, der **Schlüsselraum sehr groß** und als Angriff eigentlich **nur brute force** (alle Schlüssel probieren) bekannt ist

Unterschied symmetrische / asymmetrische Verschlüsselung

Symmetrische Verschlüsselung

- **derselbe Schlüssel** zum Ver- und Entschlüsseln
- alle Beteiligten brauchen diesen (geheimen) Schlüssel
- Problem: um Nachrichten (auf unsicheren Kanälen) zu senden, muss zuerst der Schlüssel (auf sicherem Kanal) verteilt werden



Unterschied symmetrische / asymmetrische Verschlüsselung

Asymmetrische Verschlüsselung → PGP

- **Schlüsselpaar:** was **ein** Schlüssel **ver**schlüsselt, muss mit dem **anderen** Schlüssel **ent**schlüsselt werden
- Alle Beteiligten erzeugen ein eigenes Schlüsselpaar

- Öffentlicher Schlüssel
  - kann und muss verteilt werden (an alle, über unsichere Kanäle)

- Privater Schlüssel
  - bleibt privat – gut schützen und sichern, niemals herausgeben!

- Zentrale Voraussetzungen
  - private Schlüssel können von niemand sonst benutzt werden
  - öffentliche Schlüssel sind unverfälscht und korrekt zugeordnet

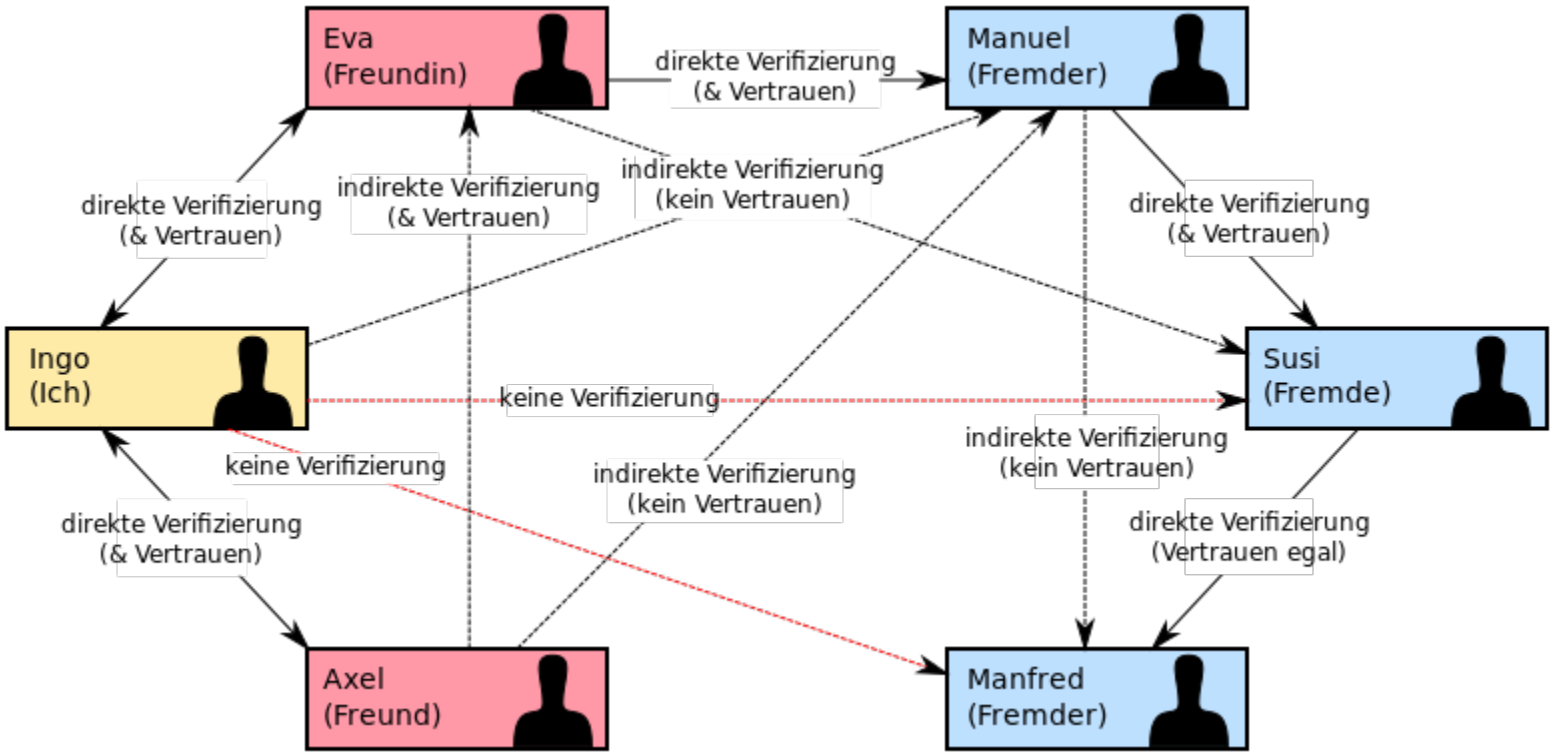
E-Mails verschlüsseln und signieren

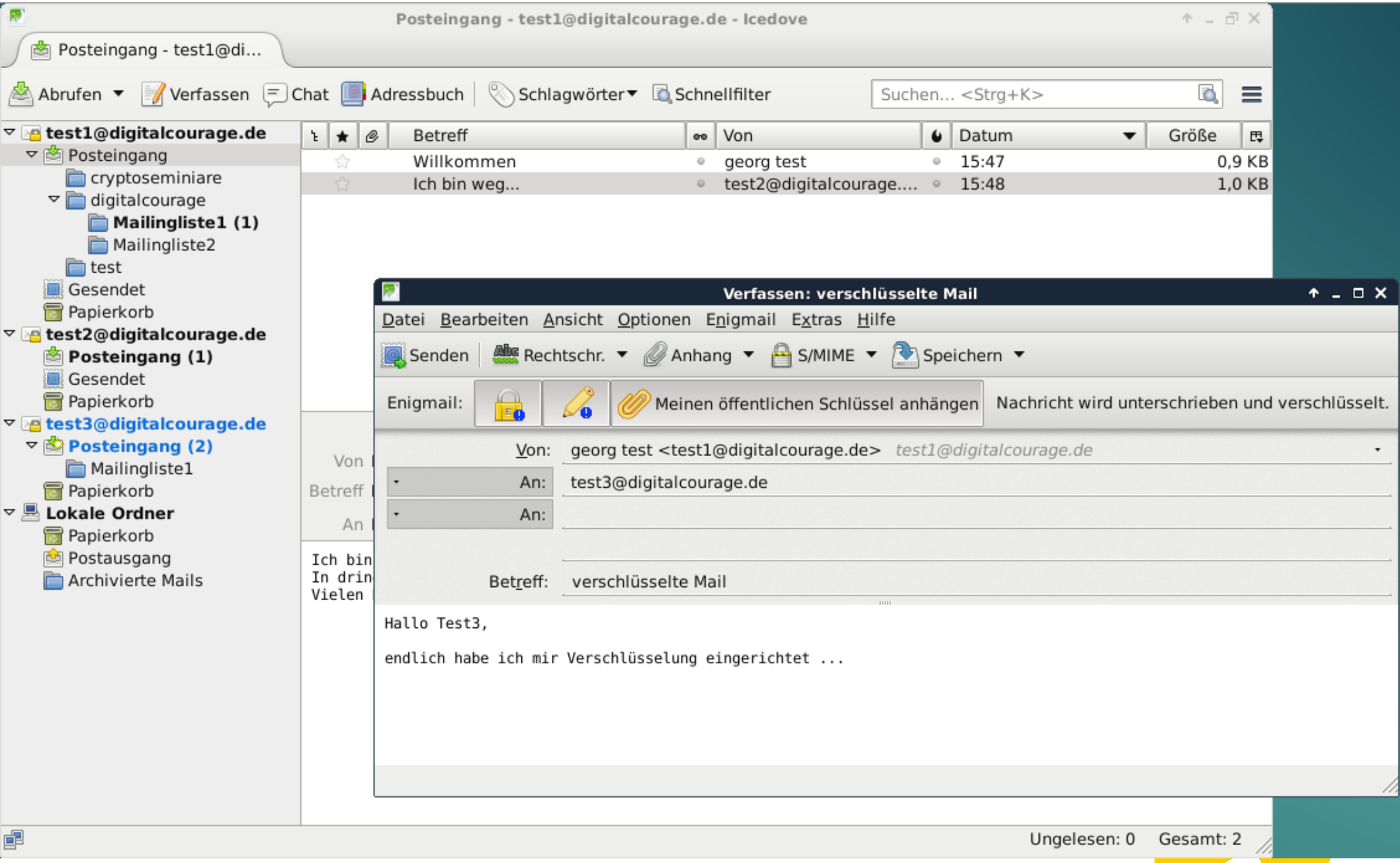
- Verschlüsseln
  - sichert Vertraulichkeit der Nachricht
  - verwendet den **öffentlichen Schlüssel des Empfängers**
    (nur der Empfänger kann mit privatem Schlüssel entschlüsseln)
- Signieren
  - sichert Unverfälschtheit der Nachricht und wer sie verfasste
  - nicht verwechseln mit Unterschrift und Fußzeile („Signatur“)
  - ein Fingerabdruck der Nachricht wird verschlüsselt und angehängt
  - verwendet den **privaten Schlüssel der Absenderin**
    (niemand anders konnte diesen Schlüssel einsetzen)
- Verschlüsseln und Signieren sind unabhängig voneinander

öffentliche PGP-Schlüssel austauschen

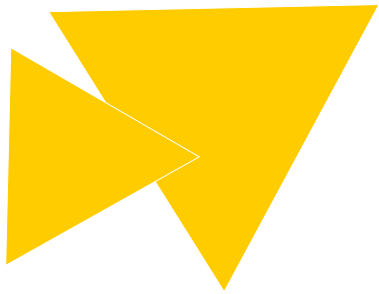
- E-Mail-Anhang
  - zur Verteilung im privaten Kreis
- Key-Server
  - bequem durchsuchbar
  - E-Mail-Adresse öffentlich einsehbar
- Habe ich den richtigen Schlüssel bekommen?
  - komplexes Thema → Schlüssel signieren, „Web of Trust“
  - pragmatische Lösung: Schlüssel auf mehreren Wegen finden (z.B. von persönlicher Website); Fingerprints austauschen und vergleichen (Visitenkarte, Telefon, Website, „Signatur“ unter Mails)

Web of Trust




Posteingang - test1@digitalcourage.de - Icedove
Posteingang - test1@di...
Abrufen
Verfassen
Chat
Adressbuch
Schlagwörter
Schnellfilter
Suchen... <Strg+K>
test1@digitalcourage.de
Posteingang
cryptoseminiare
digitalcourage
Mailingliste1 (1)
Mailingliste2
test
Gesendet
Papierkorb
test2@digitalcourage.de
Posteingang (1)
Gesendet
Papierkorb
test3@digitalcourage.de
Posteingang (2)
Mailingliste1
Papierkorb
Lokale Ordner
Papierkorb
Postausgang
Archivierte Mails
Betreff
Von
Datum
Größe
Willkommen
georg test
15:47
0,9 KB
Ich bin weg...
test2@digitalcourage....
15:48
1,0 KB
Verfassen: verschlüsselte Mail
Datei Bearbeiten Ansicht Optionen Enigmail Extras Hilfe
Senden
Rechtschr.
Anhang
S/MIME
Speichern
Enigmail:
Meinen öffentlichen Schlüssel anhängen
Nachricht wird unterschrieben und verschlüsselt.
Von:
georg test <test1@digitalcourage.de>
test1@digitalcourage.de
An:
test3@digitalcourage.de
An:
Betreff:
verschlüsselte Mail
Hallo Test3,
endlich habe ich mir Verschlüsselung eingerichtet ...
Ungelesen: 0
Gesamt: 2

Mobilgeräte



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 …

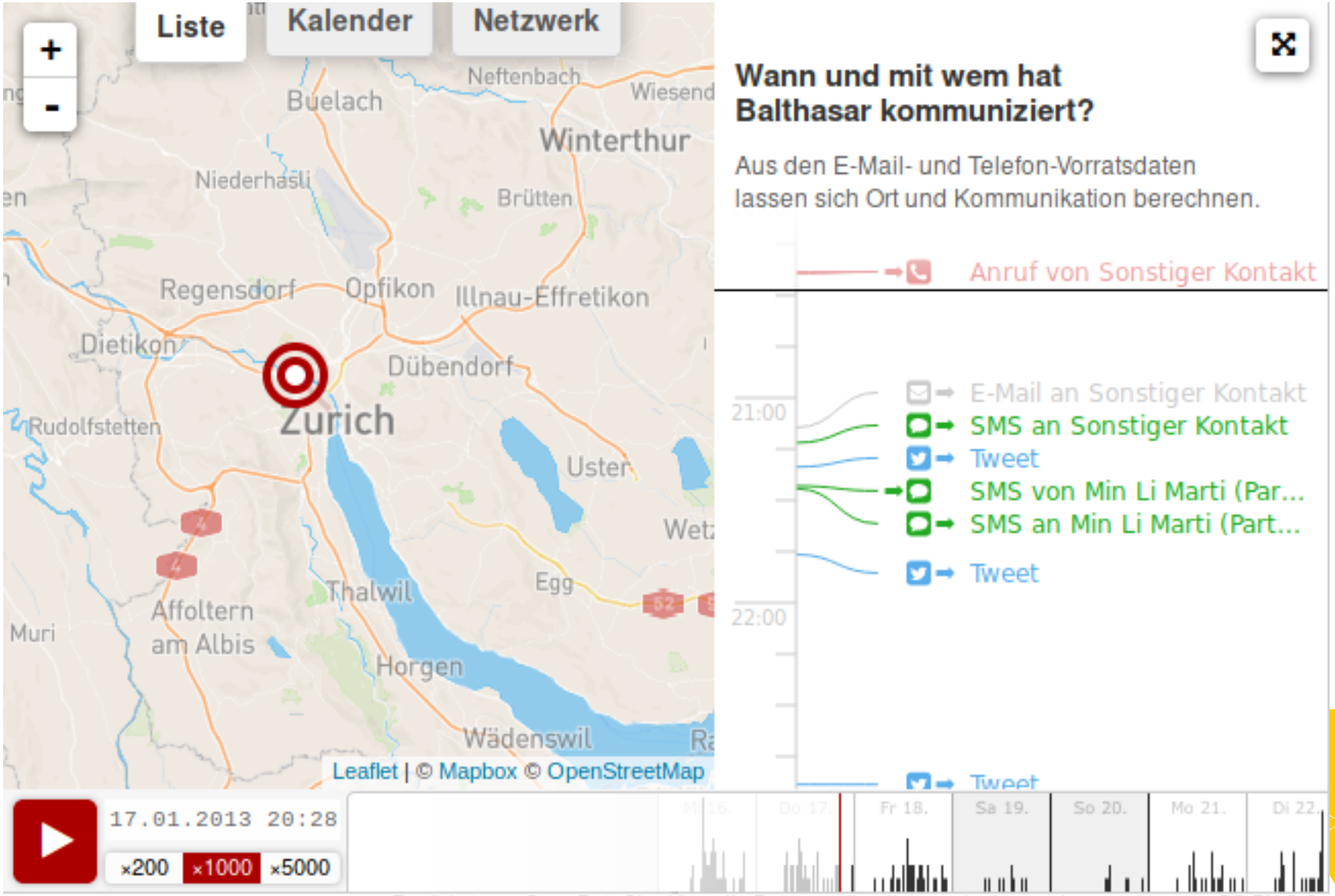
  (Kontaktbeziehungen, Reisedaten, Finanztransfers, …)

- … 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

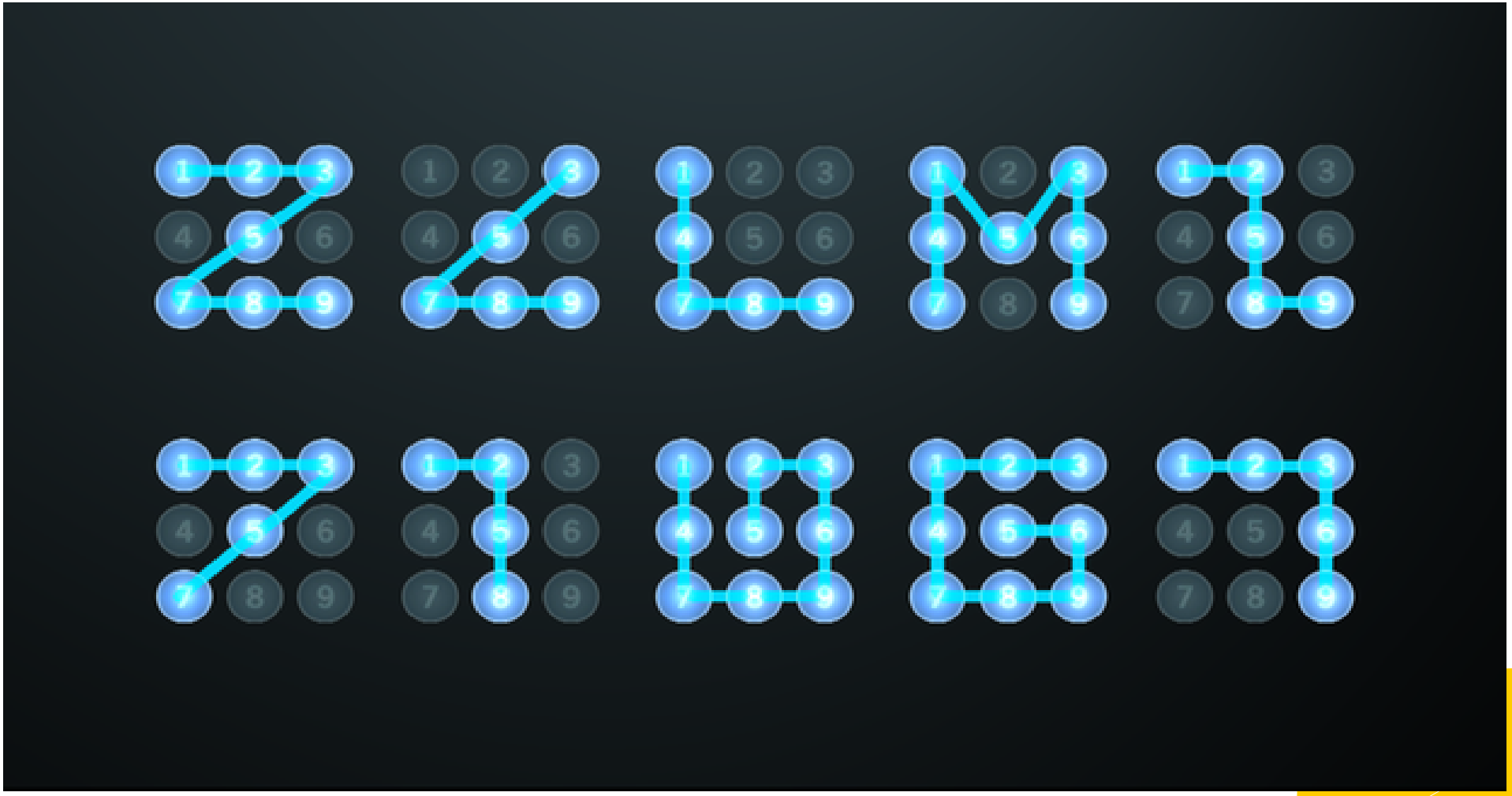
- Betriebssystem: Goldener Käfig iOS (Apple)
  - Apps nur aus einer Quelle (zentraler App-Store)
  - geschlossenes System, keine Gerätehoheit
  - mehr Freiheit durch Jailbreak (Gefängnisausbruch)
  - massives Tracking durch Apps aus dem App-Store:
    - https://www.washingtonpost.com/technology/2019/05/28/its-middle-night-do-you-know-who-your-iphone-is-talking/

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)

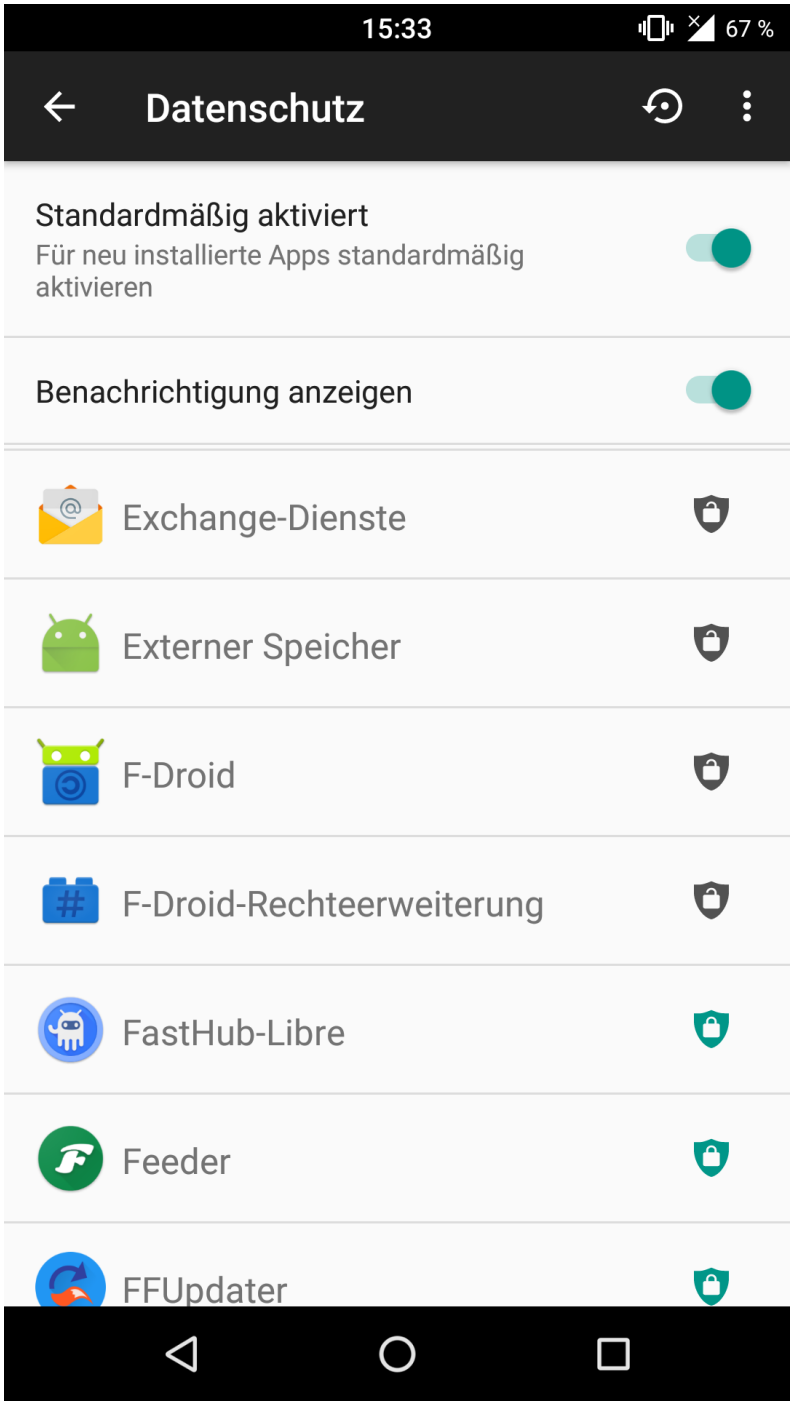
ACCESS_NETWORK_STATE (android.permission)
View Network Connections

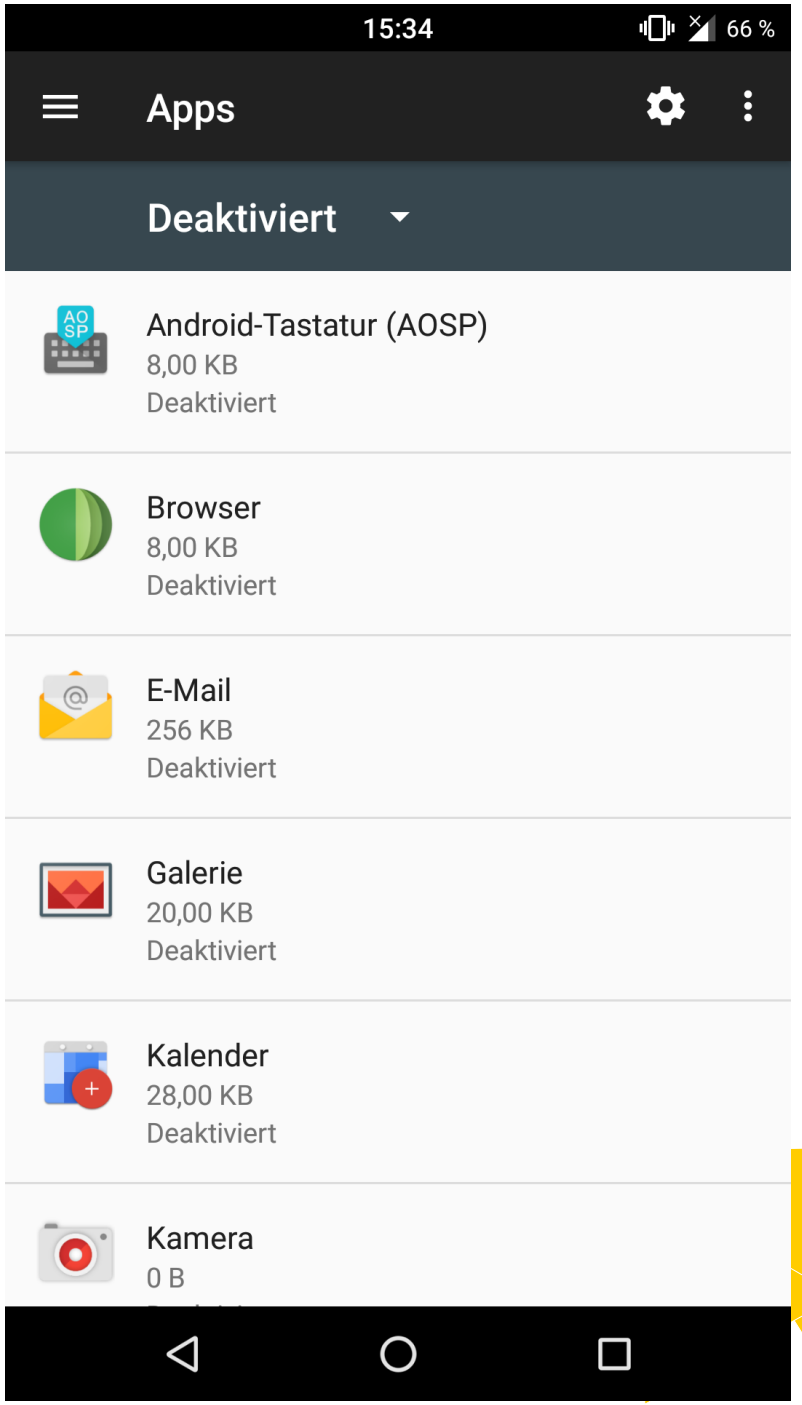
ACCESS_WIFI_STATE (android.permission)
View Wi-Fi Connections

INTERNET (android.permission)
Have Full Network Access

Apps immer kritisch begegnen!

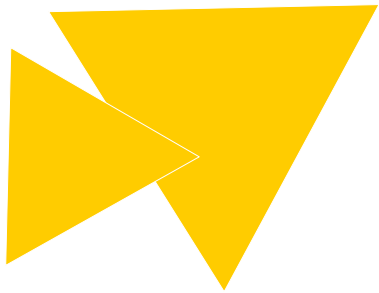
- „kostenlose“ Apps im App/Play Store verdienen häufig mit Datensammelei und Werbung an den Nutzer.innen
- immer hinterfragen: Braucht App XY diese oder jene Berechtigung für ihre Funktion überhaupt?
- einzelne Berechtigungen von Apps entziehen
- falls verfügbar: Datenschutzmodus aktivieren!
- alternative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

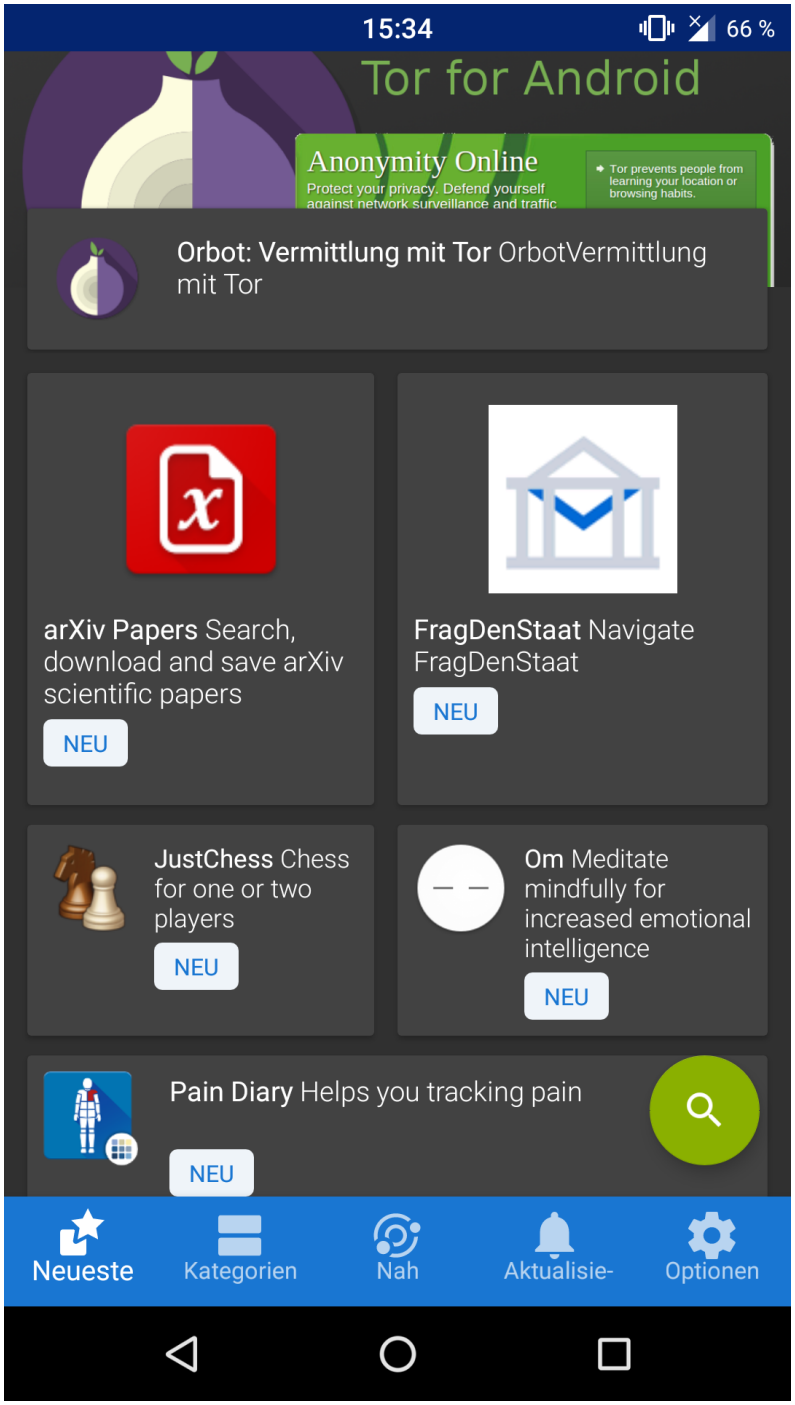
Android „entgoogeln“

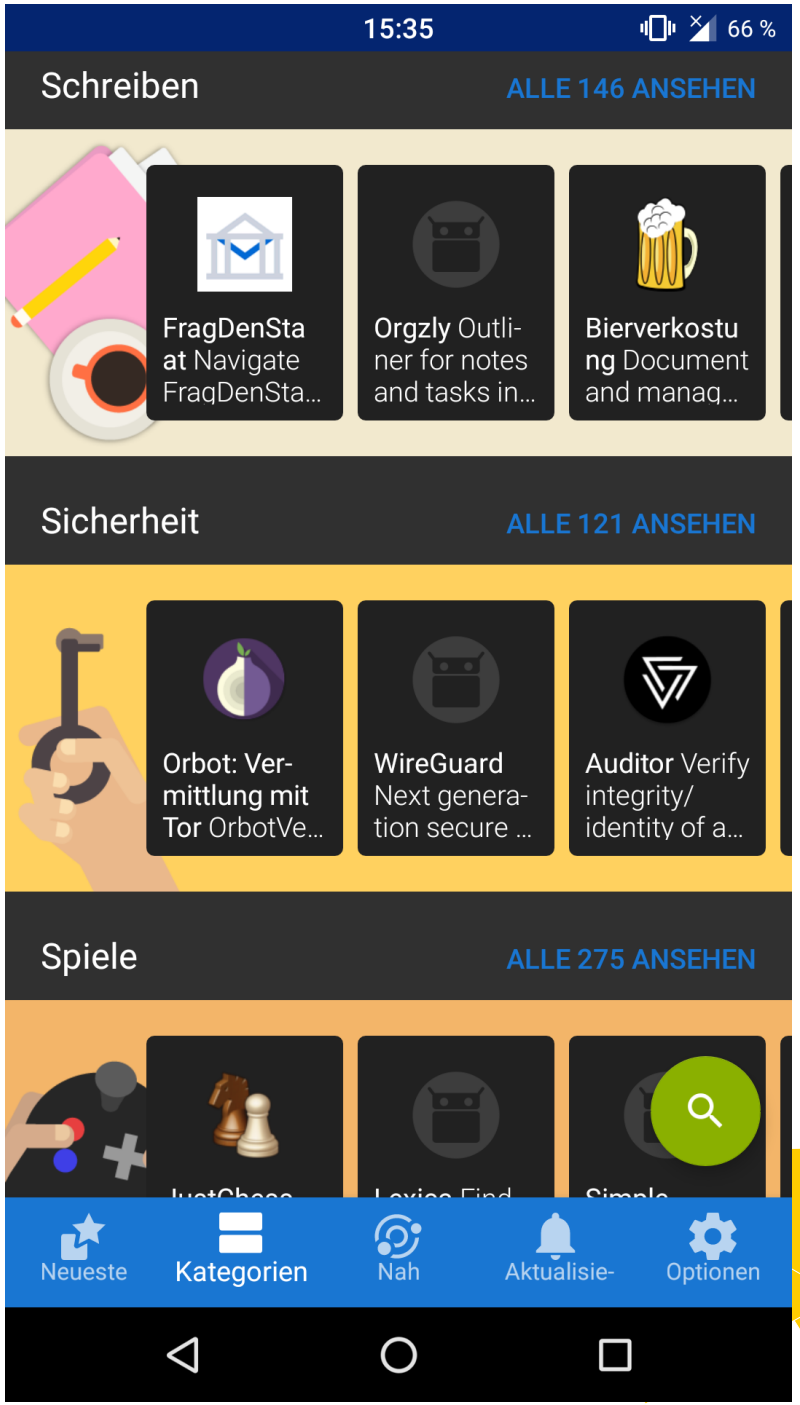
1. Apps und Dienste von Google deaktivieren/deinstallieren
   - Google-Einstellungen (G+, Standort, Suche, Werbe-ID, usw.)
2. Alternativ-Dienste nutzen
   - Browser, Suche, Mail, Sync für Kalender / Kontakte …
3. Play Store deaktivieren / F-Droid nutzen
   - App-Alternativen nutzen
4. Freie Android-Variante 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
Protect your privacy. Defend yourself against network surveillance and traffic
Tor prevents people from learning your location or browsing habits.
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 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 (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)

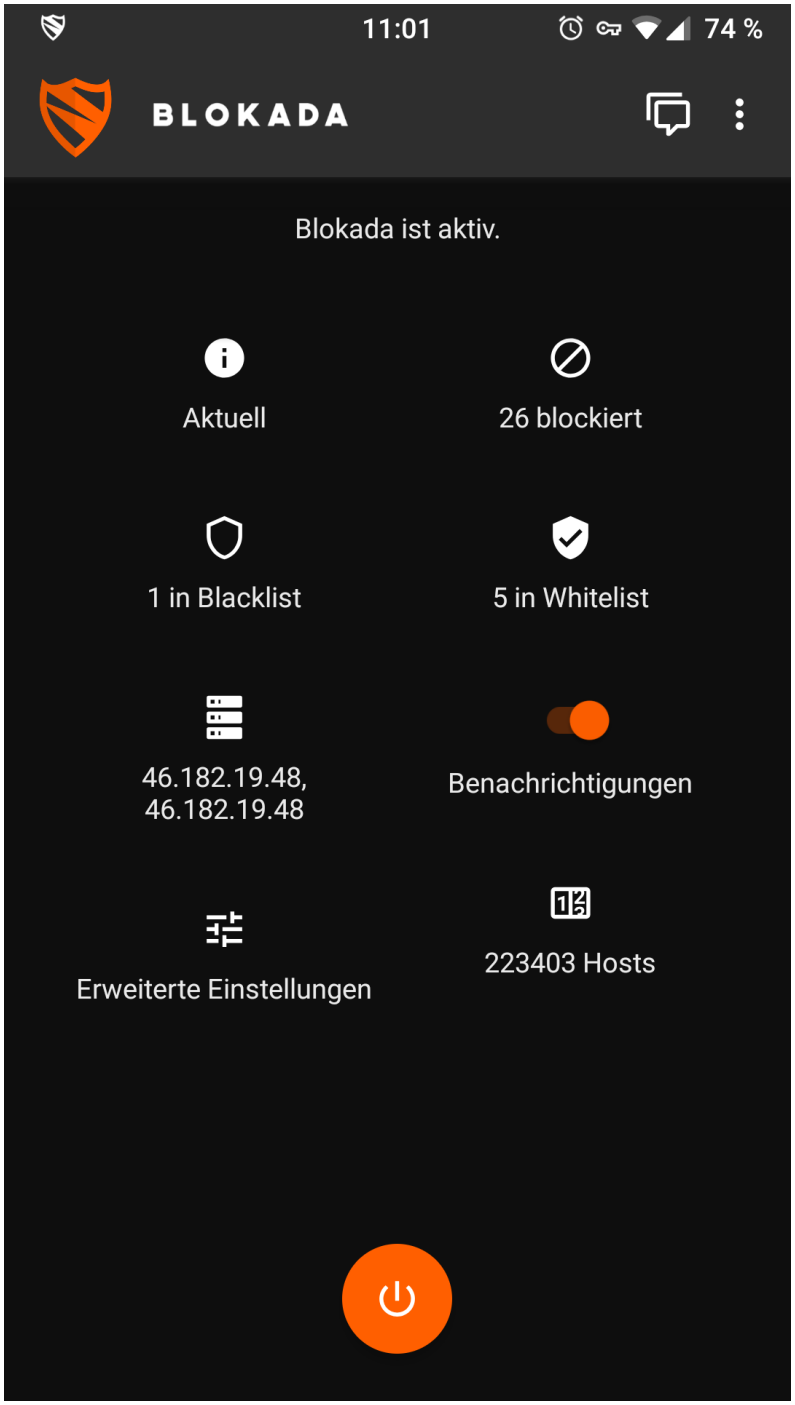
  - nutzen das offene Protokoll **XMPP** (Jabber), das im Gegensatz zu anderen Messengern dezentrale Kommunikationsstrukturen erlaubt
  - unterstützen Ende-zu-Ende-verschlüsselte Chats via OpenPGP, OTR und OMEMO
  - verfügbar via F-Droid (Conversations) bzw. App Store (ChatSecure)
  - als Conversations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

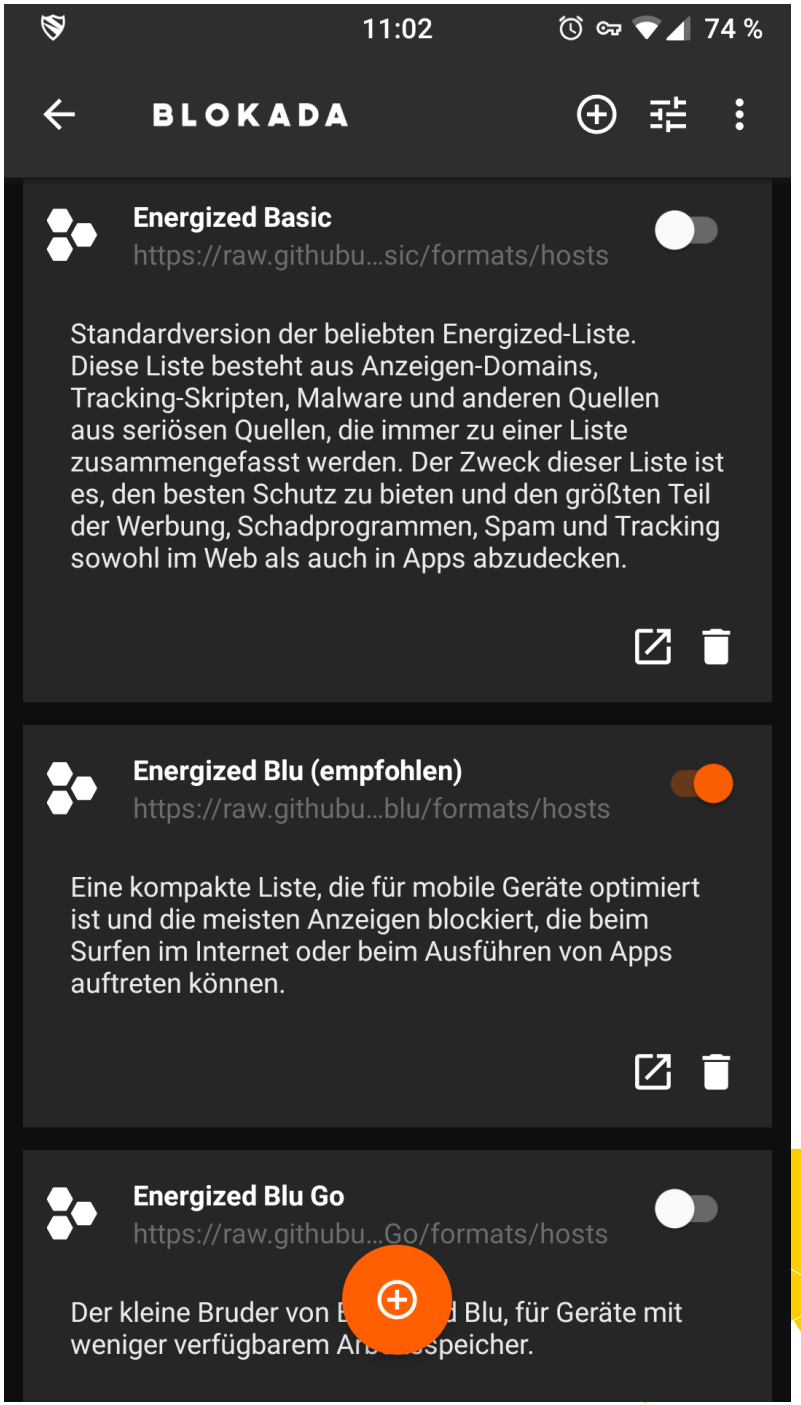
Empfehlenswerte Browser

- **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
Der kleine Bruder von E d Blu, für Geräte mit weniger verfügbarem Ar speicher.

Empfehlenswerter E-Mail-Client

- **K-9 Mail**

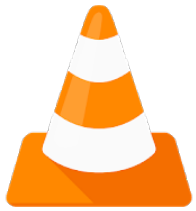
  - umfangreicher, freier Mail-Client
  - unterstützt IMAP/POP3
  - kann verschlüsselte Mails via PGP/MIME senden und empfangen

- **OpenKeychain**

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

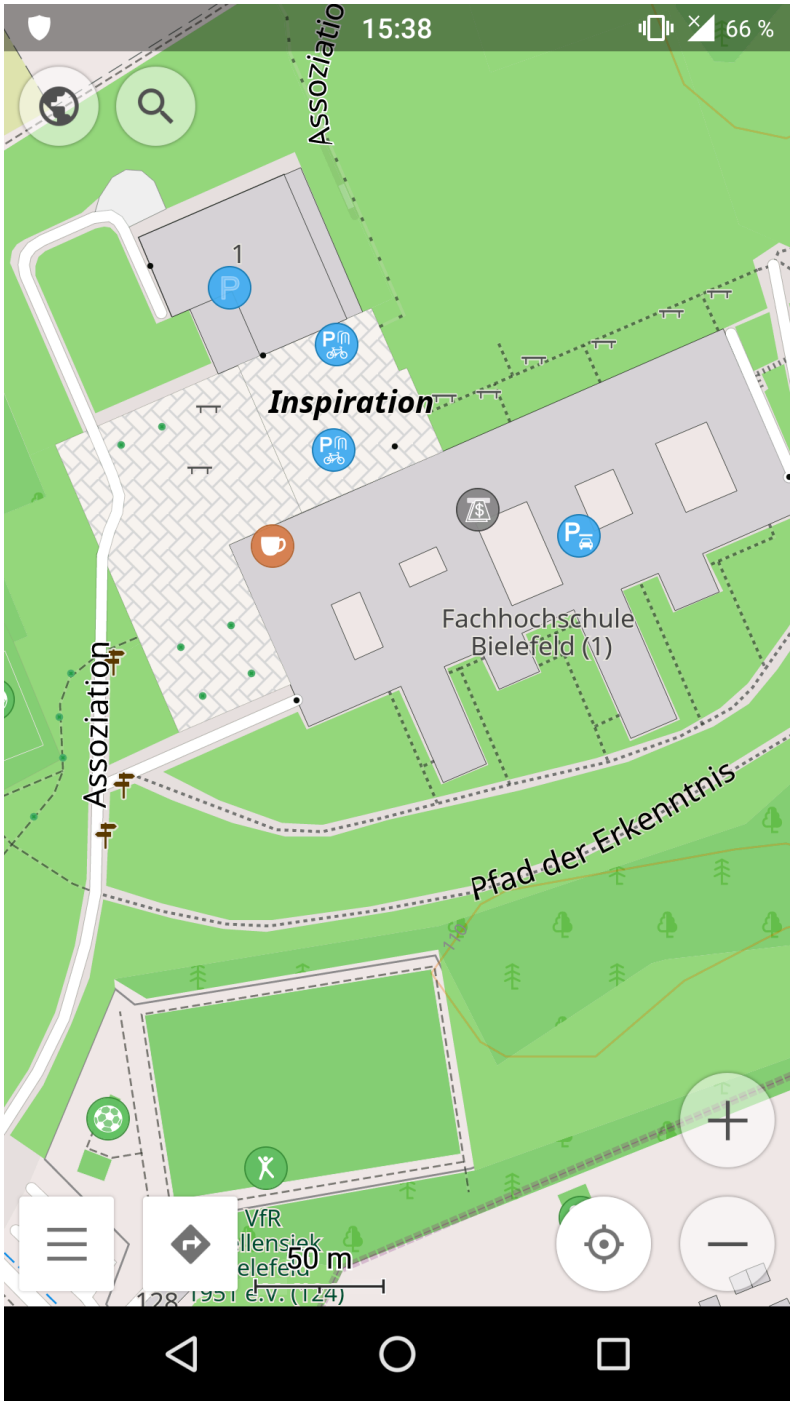
Weitere empfehlenswerte Apps

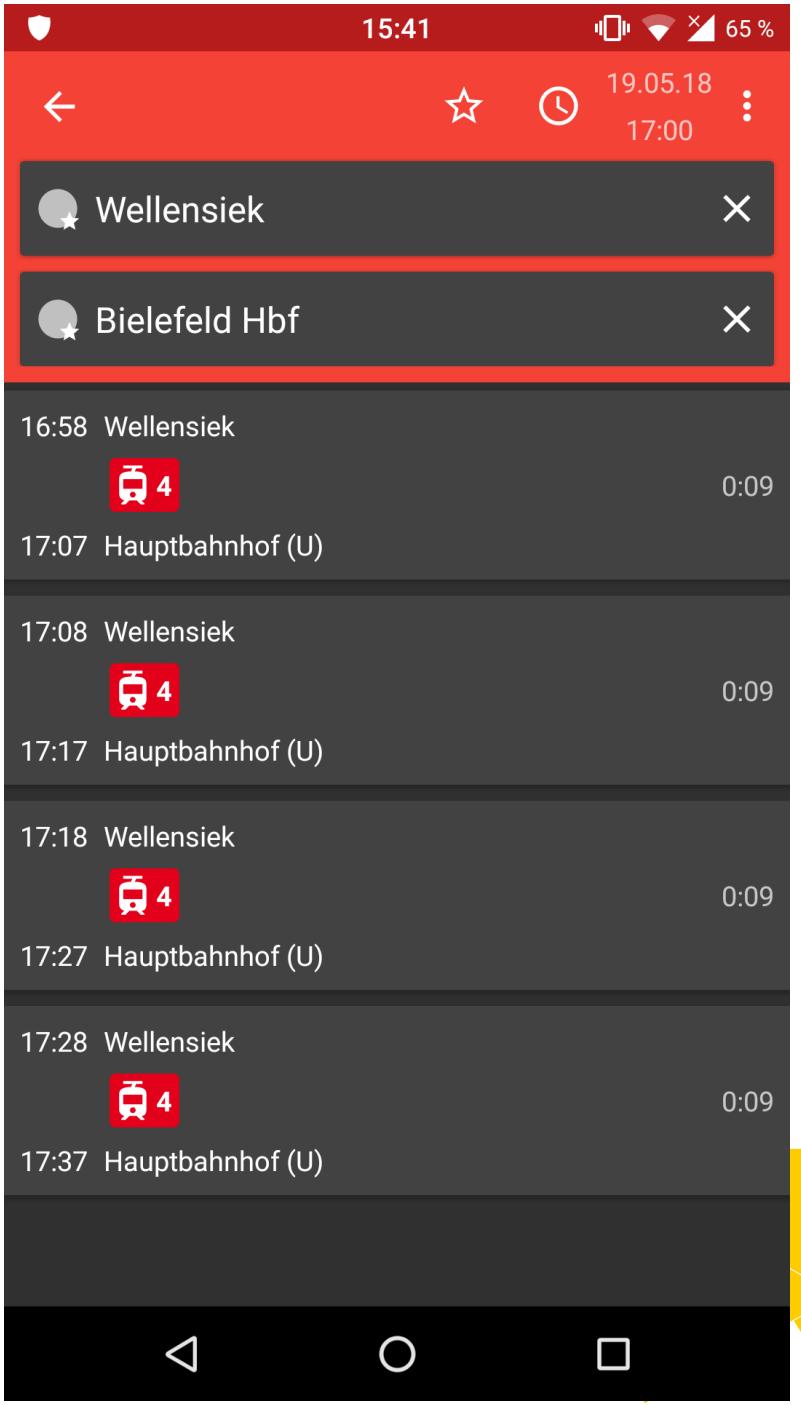
- **Transportr**
  - Fahrpläne des öffentlichen Nah-/Fernverkehrs & Verbindungssuche



- **VLC**
  - Video- und Audioplayer

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


15:38
66 %
Assoziatio
1
Inspiration
Fachhochschule
Bielefeld (1)
Assoziation
Pfad der Erkenntnis
50 m

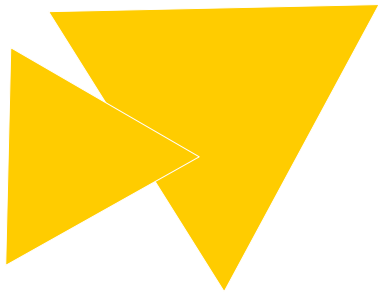

15:41
65 %
19.05.18
17:00
Wellensiek
Bielefeld Hbf
16:58 Wellensiek
4
0:09
17:07 Hauptbahnhof (U)
17:08 Wellensiek
4
0:09
17:17 Hauptbahnhof (U)
17:18 Wellensiek
4
0:09
17:27 Hauptbahnhof (U)
17:28 Wellensiek
4
0:09
17:37 Hauptbahnhof (U)

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?!



Digitalcourage in der Nähe

- **Digitalcourage-Hochschulgruppe**
  - Treffen an jedem ersten und dritten Montag im Monat um 18:00 Uhr im SozCafé (X-C2-116, X-Gebäude Uni Bielefeld).
  - https://digitalcourage.de/hochschulgruppe-bielefeld

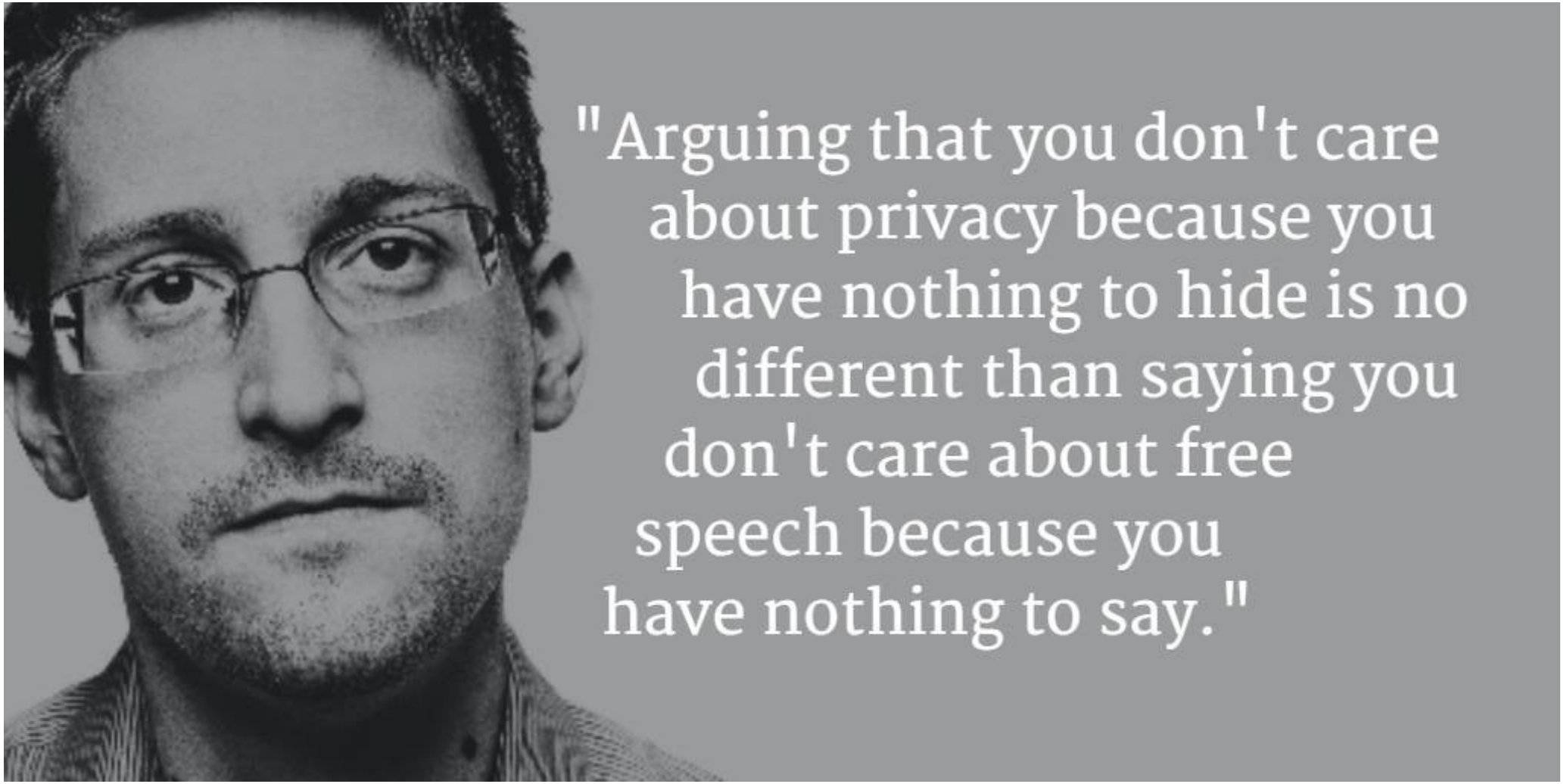
- **Digitalcourage e.V.**
  - Offenes Treffen jeden Dienstag ab ca. 20:30 Uhr im TaverNio (Niederwall 23).
  - https://digitalcourage.de/treffen-vor-ort

Weitere Veranstaltungen

- CryptoParty in der Stadtbibliothek Bielefeld
  - 9. Juli 2019 (Dienstag) ab 18 Uhr im Veranstaltungssaal S02

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 -