

Digitale Selbstverteidigung

Marius Melzer (CCC Dresden)

08.06.2016

Chaos Computer Club



- Verein wurde 1981 gegründet (<https://ccc.de>)

Chaos Computer Club



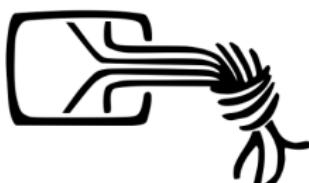
- Verein wurde 1981 gegründet (<https://ccc.de>)
- Aktuell > 6000 Mitglieder

Chaos Computer Club



- Verein wurde 1981 gegründet (<https://ccc.de>)
- Aktuell > 6000 Mitglieder
- Technologie zum gesellschaftlichen Nutzen (und nicht ihrem Schaden)

Chaos Computer Club



- Verein wurde 1981 gegründet (<https://ccc.de>)
- Aktuell > 6000 Mitglieder
- Technologie zum gesellschaftlichen Nutzen (und nicht ihrem Schaden)
- Betreibt u.a. Öffentlichkeitsarbeit und Politikberatung



Chaos Computer Club



- Chaos Computer Club Dresden (<https://c3d2.de>)

Chaos Computer Club



- Chaos Computer Club Dresden (<https://c3d2.de>)
- Datenspuren: Herbst 2016 (<https://datenspuren.de>)



Chaos Computer Club



- Chaos Computer Club Dresden (<https://c3d2.de>)
- Datenspuren: Herbst 2016 (<https://datenspuren.de>)
- Podcasts (<https://c3d2.de/radio.html>)



Chaos Computer Club



- Chaos Computer Club Dresden (<https://c3d2.de>)
- Datenspuren: Herbst 2016 (<https://datenspuren.de>)
- Podcasts (<https://c3d2.de/radio.html>)
- IT4Refugees

Chaos Computer Club



- Chaos Computer Club Dresden (<https://c3d2.de>)
- Datenspuren: Herbst 2016 (<https://datenspuren.de>)
- Podcasts (<https://c3d2.de/radio.html>)
- IT4Refugees
- Chaos macht Schule (<https://c3d2.de/schule.html>)

Bundespräsident Gauck zur NSA-Überwachung

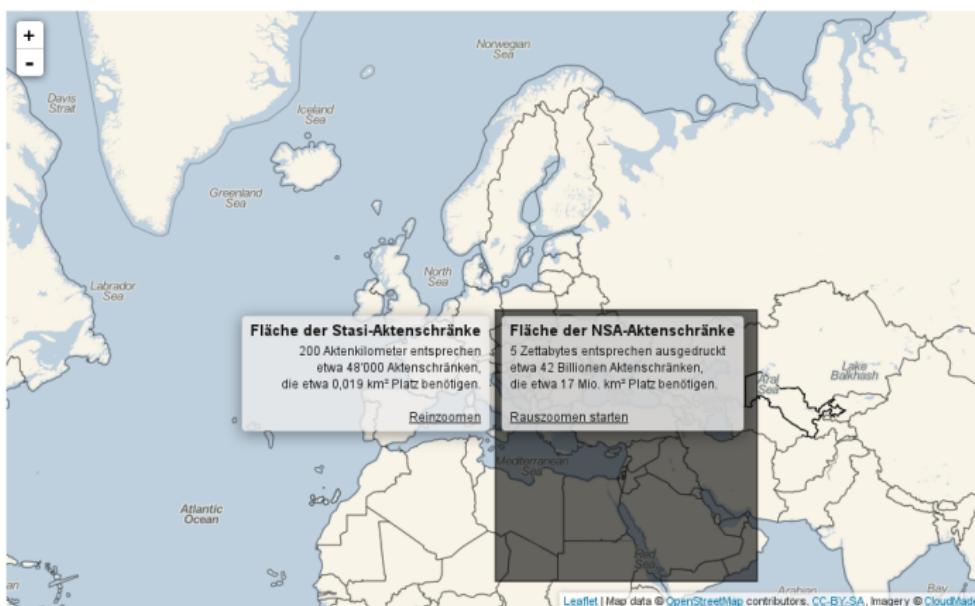
“Wir wissen z.B., dass es nicht so ist, wie bei der Stasi und dem KGB, dass es dicke Aktenbände gibt, wo unsere Gesprächsinhalte alle aufgeschrieben und schön abgeheftet sind. Das ist es nicht.” (Gauck, 30.06.2013 im ZDF-Sommerinterview)

Stasi vs. NSA



Realisiert von [OpenDataCity](#). Anwendung steht unter CC-BY 3.0.

Stasi vs. NSA



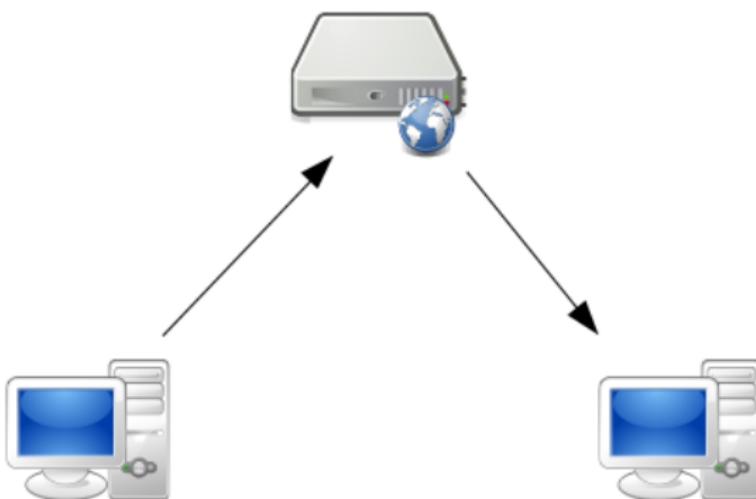
Samsung vs. 1984

Recognition features to you. In addition, Samsung may collect and your device may capture voice commands and associated texts so that we can provide you with Voice Recognition features and evaluate and improve the features. Please be aware that if your spoken words include personal or other sensitive information, that information will be among the data captured and transmitted to a third party through your use of Voice Recognition.

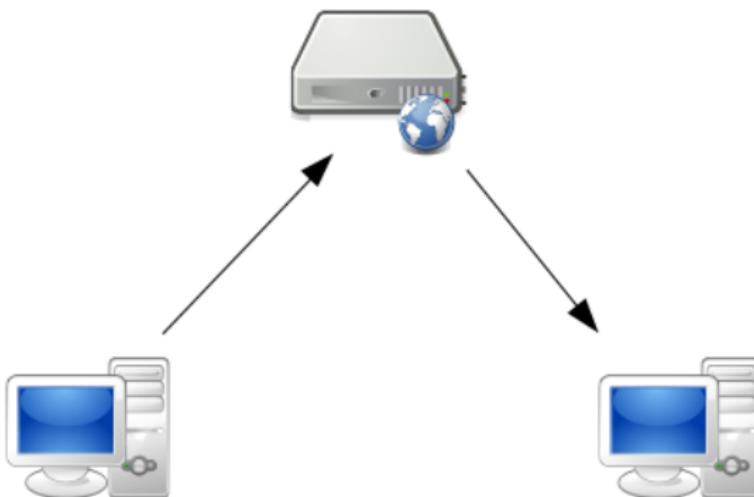
If you do not enable Voice Recognition, you will not be able to use interactive voice recognition features, although you may be able to control your TV using certain predefined voice commands. While Samsung will not collect your spoken word, Samsung may still collect associated texts and other usage data so that

Behind Winston's back the voice from the telescreen was still babbling away about pig-iron and the overfulfilment of the Ninth Three-Year Plan. The telescreen received and transmitted simultaneously. Any sound that Winston made, above the level of a very low whisper, would be picked up by it, moreover, so long as he remained within the field of vision which the metal plaque commanded, he could be seen as well as heard. There was of course no way of knowing whether you were being watched at any given moment. How often, or on what system, the Thought Police plugged in on any individual wire was guesswork. It was even conceivable that they watched everybody all the time. But at any rate they could plug in your wire whenever they wanted to. You had to live--did live, from habit that became instinct--in the assumption that every sound you made was overheard, and, except in darkness, every movement scrutinized.

Wie kommunizieren wir im Internet?



Was ist zu schützen?



Unerwünschte Funktionalität

The screenshot shows the Windows Settings interface under 'DATENSCHUTZ' (Data Protection). The left sidebar lists categories: Allgemein, Position, Kamera, Mikrofon, Spracherkennung, Freihand und Eingabe, Kontoinformationen, Kontakte, Kalender, Messaging, Funkempfang, Weitere Geräte, Feedback und Diagnose, and Hintergrund-Apps. The 'Allgemein' tab is selected. On the right, under 'Datenschutzoptionen ändern', several options are listed with toggle switches:

- Apps die Verwendung der Werbungs-ID für App-übergreifende Erfahrungen erlauben (bei Deaktivierung wird Ihre ID zurückgesetzt)
Aus (switched off)
- SmartScreen-Filter einschalten, um von Windows Store-Apps verwendete Webinhalte (URLs) zu überprüfen
Ein (switched on)
- Informationen zu meinem Schreibverhalten an Microsoft senden, um die Eingabe- und Schreibfunktionen in Zukunft zu verbessern.
Aus (switched off)
- Websites den Zugriff auf die eigene Sprachliste gestatten, um die Anzeige lokal relevanter Inhalte zu ermöglichen
Aus (switched off)
- [Microsoft-Werbung und andere Personalisierungsinfos verwalten](#)
- [Datenschutzbestimmungen](#)

Unerwünschte Funktionalität

App name	iPhone	Android				
	Username Password	Contacts	Age, Gender	Location	Phone ID	Phone number
0.03 Seconds Pro	■	■	■	■	■	■
Age My Face	■	■	■	■	■	■
Angry Birds	■	■	■	■	■	■
Angry Birds Lite	■	■	■	■	■	■
Aurora Feint II: Lite	■■■	■	■	■	■	■
Barcode Scanner (BahnTech)	■	■	■	■	■	■
Bejeweled 2	■	■	■	■	■	■
Best Alarm Clock Free	■	■	■	■	■	■
Bible App (LifeChurch.tv)	■	■	■	■	■	■
Bump	■	■	■	■	■	■
CBS News	■	■	■	■	■	■
0.03 Seconds	■	■	■	■	■	■
Dictionary.com	■	■	■	■	■	■

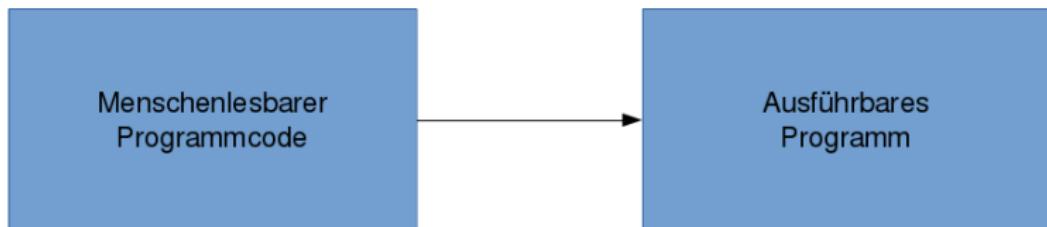
Wie schütze ich meine Geräte?

- Rechte von Applikationen einschränken (Permissions, Firewall)
- Aktuelle und vertrauenswürdige Software

Vertrauenswürdige Software?

Einer Software, die nicht quelloffen ist, kann man nicht vertrauen

Kompilierung von Software



Freie Software auf Computern



Firefox



Thunderbird



LibreOffice



VLC Media Player

Freie Software auf dem Smartphone

F-Droid

Android-Appstore für freie Software



iOS Open Source Apps

[https://github.com/dkhamsing/
open-source-ios-apps](https://github.com/dkhamsing/open-source-ios-apps)

Cyanogenmod, Replicant

- basiert auf Open Source Teil von Android
- ersetzt teilweise die proprietären Apps durch freie
- **Problem:** Verlust der Garantie bei Installation



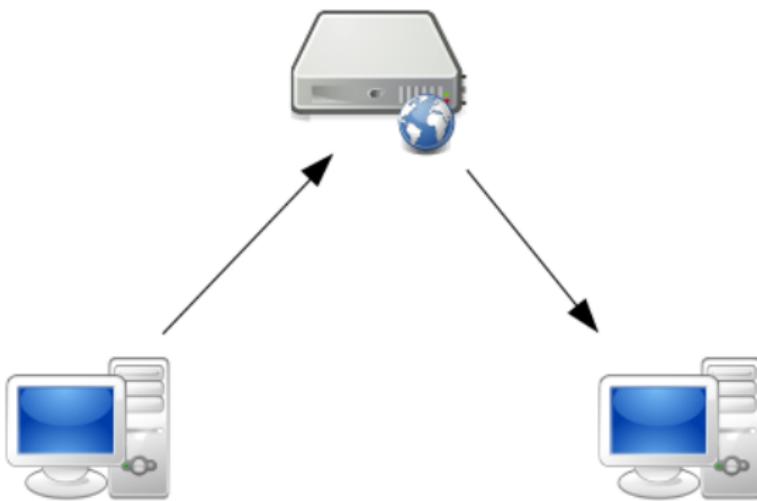
cyanogenmod

Ubuntu Phone, Sailfish OS



Geräteverschlüsselung

Was ist zu schützen?

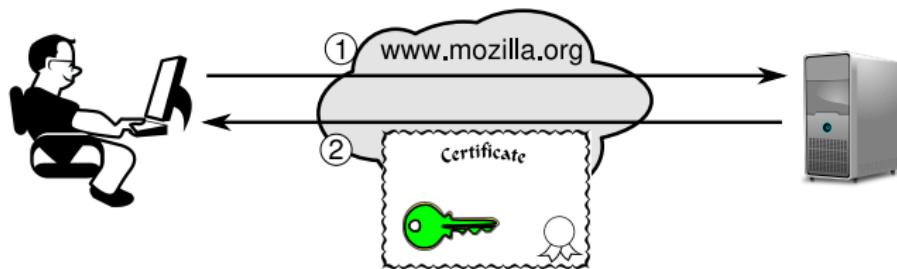


Angreifer im eigenen Netz

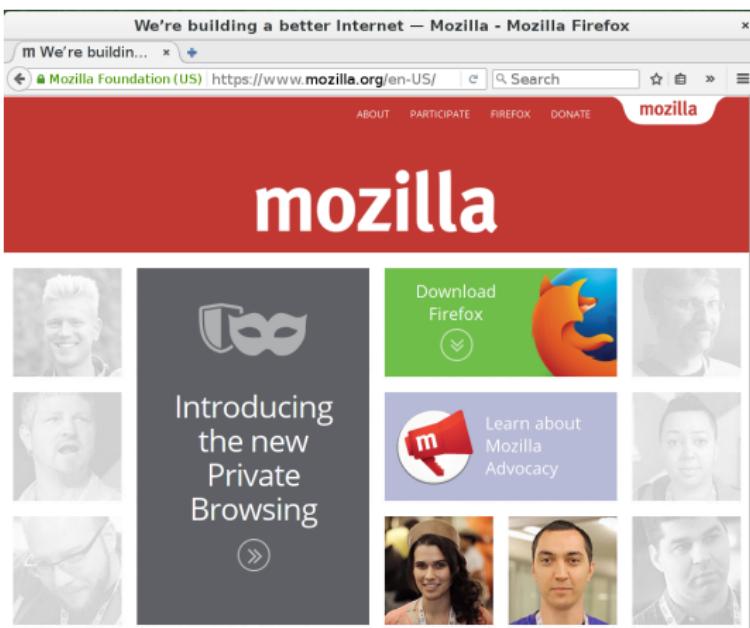


Transportwegverschlüsselung

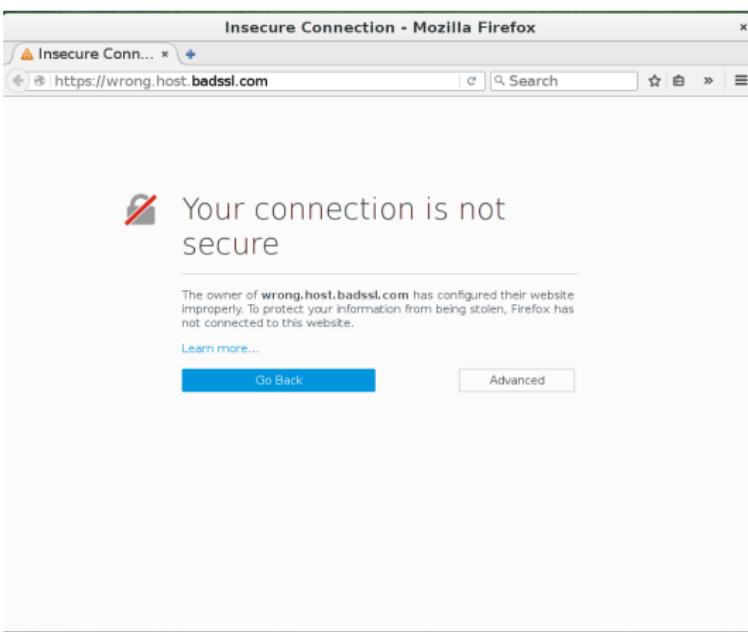
SSL = Secure Socket Layer / TLS = Transport Layer Security



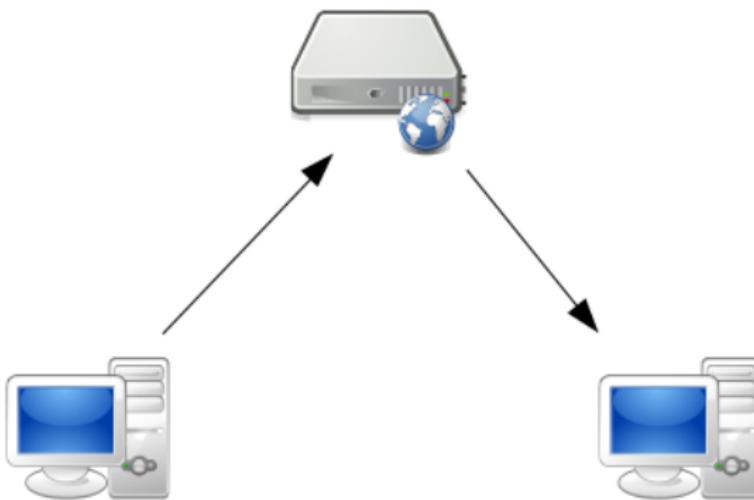
SSL im Browser



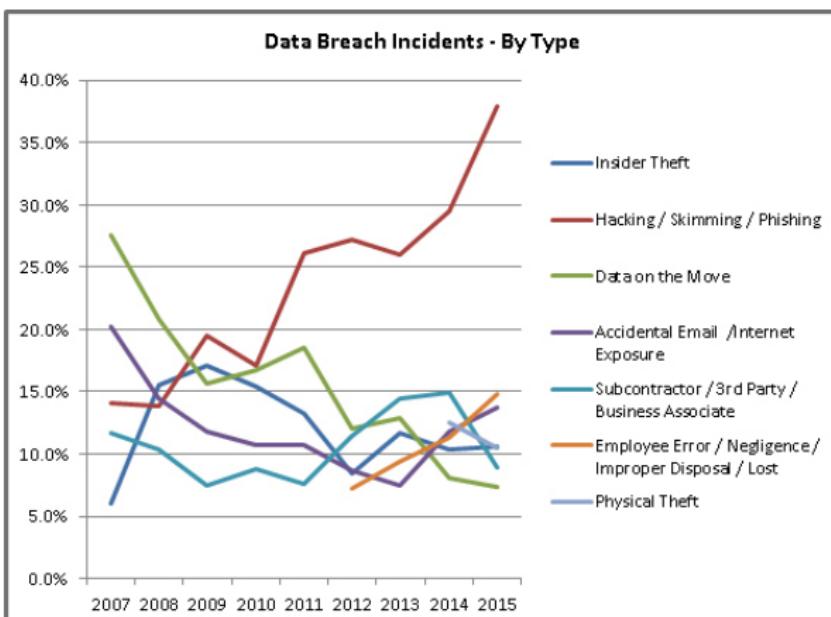
Ungültiges Zertifikat



Was ist zu schützen?



Informationsleaks



<http://www.idtheftcenter.org/ITRC-Surveys-Studies/2015databreaches.html>

Ende-zu-Ende-Verschlüsselung

- PGP für E-Mails

Ende-zu-Ende-Verschlüsselung

- PGP für E-Mails
- OTR/OMEMO für Jabber:
 - Pidgin für Linux und Windows
 - Conversations oder ChatSecure für Android
 - Adium für Mac, ChatSecure für iOS

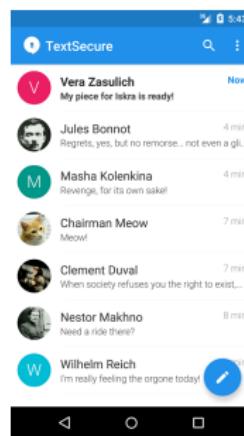
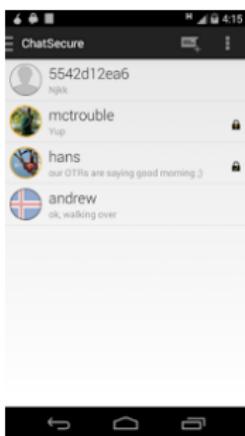
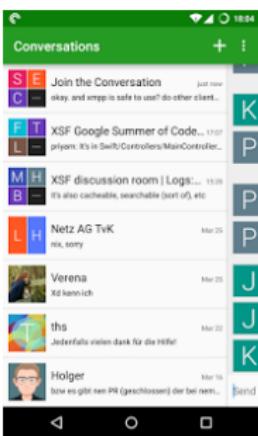
Ende-zu-Ende-Verschlüsselung

- PGP für E-Mails
- OTR/OMEMO für Jabber:
 - Pidgin für Linux und Windows
 - Conversations oder ChatSecure für Android
 - Adium für Mac, ChatSecure für iOS
- palava.tv, Tox, Linphone für Videotelefonie

Ende-zu-Ende-Verschlüsselung

- PGP für E-Mails
- OTR/OMEMO für Jabber:
 - Pidgin für Linux und Windows
 - Conversations oder ChatSecure für Android
 - Adium für Mac, ChatSecure für iOS
- palava.tv, Tox, Linphone für Videotelefonie
- Signal

Alternative Messenger



<https://xmpp.net/directory.php>

Aktuelle Cryptowelle

Facebook, Google and WhatsApp plan to increase encryption of user data

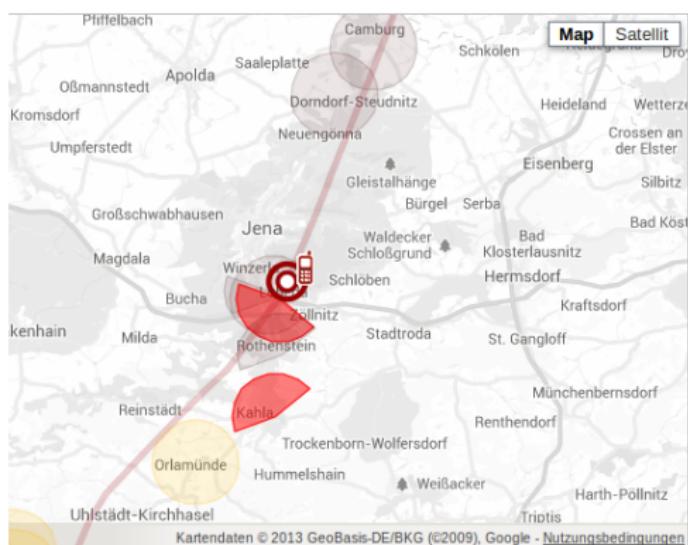
Spurred on by Apple's battles against the FBI, some of tech's biggest names are to expand encryption of user data in their services, the Guardian can reveal



Work on new encryption projects began before Apple entered a court battle with US authorities over the San Bernardino killer's iPhone. Photograph: Philippe Huguen/AFP/Getty Images



Metadaten - VDS



Monday, 31 August 2009

Malte Spitz gives a speech to the Greens in Erfurt against internet censorship.
(source: [Parteiwebsite](#))

6 incoming calls
21 outgoing calls
total time: 1h 16min 8s

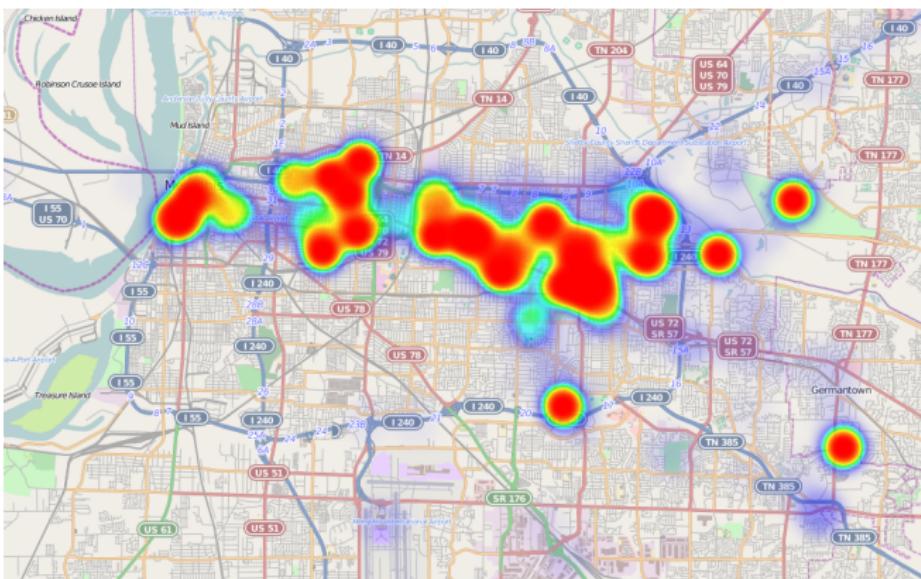
34 incoming messages
29 outgoing messages

duration of internet connection:
21h 17min 25s

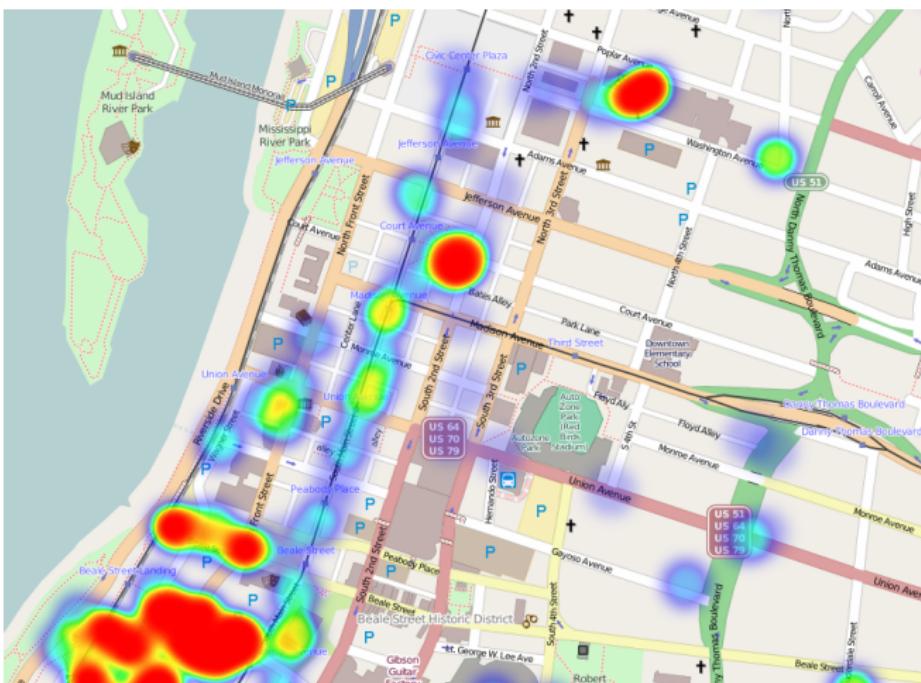
Download Data



Google Takeout



Google Takeout



Zeitstempel

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
0	●	●	●	●	●	●	●	●	●	●	
1	●	●	●	●	●	●	●	●	●	●	
2	●	●	●	●	●	●	●	●	●	●	
3	●	●	●	●	●	●	●	●	●	●	
4	●	●	●	●	●	●	●	●	●	●	
5	
6	

Alan, Microblogging



Zeitstempel

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
0	●	●	●	•						•	•	•			●	•	•	•	●	•	●	•	●	•
1	●	●			•	•	•				•		•	•	•	●	●	●	●	●	●		●	●
2	●		•	•	•	•							•		●	●	●	●	●	●	●	●	●	●
3	●												•			●	●	●	●	●	●	●		●
4	●				•	•	•	•	•	•		•	•			●	●	●		●	●		●	●
5	●	●			•	•										●	●	●	●	●	●	●	●	●
6	●	●	●	●	●	●	●	●	●						●	●	●	●	●	●	●	●	●	●

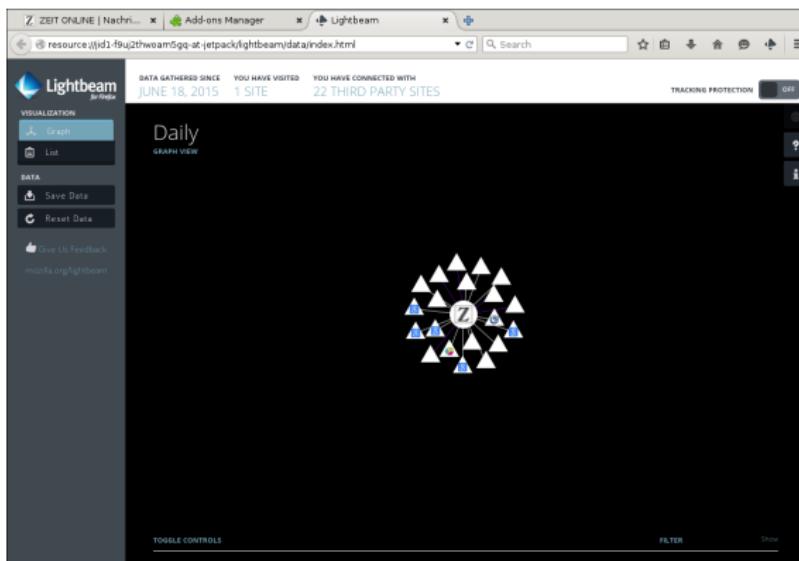
Bob, Microblogging

Zeitstempel

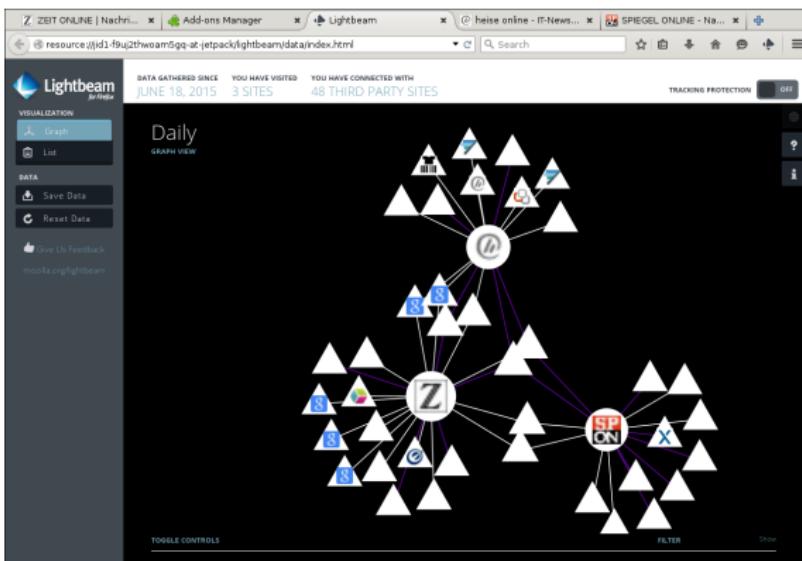
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
0	•	•													•	•						•		•
1		•	•											•	•	•			•		•	•	•	•
2		•			•											•		•					•	
3														•	•	•	•	•	•	•	•	•	•	•
4		•	•	•											•	•	•	•	•	•	•	•	•	•
5	•	•	•	•	•	•								•	•	•	•	•	•	•	•	•	•	•
6	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•

Charlie, Github

Metadaten im WWW



Metadaten im WWW



Tor

About Tor – Tor Browser

The green onion menu now has a security slider which lets you adjust your security level. Check it out!

Open security settings

Tor Browser 5.0.1

Congratulations!

This browser is configured to use Tor.

You are now free to browse the Internet anonymously.

Test Tor Network Settings

Search securely with Disconnect

What Next?

Tor is NOT all you need to browse anonymously! You may need to change some of your browsing habits to ensure your identity stays safe.

Tips On Staying Anonymous »

You Can Help!

There are many ways you can help make the Tor Network faster and stronger:

- Run a Tor Relay Node »
- Volunteer Your Services »
- Make a Donation »

The Tor Project is a US 501(c)(3) non-profit dedicated to the research, development, and education of online anonymity and privacy. [Learn more about The Tor Project »](#)

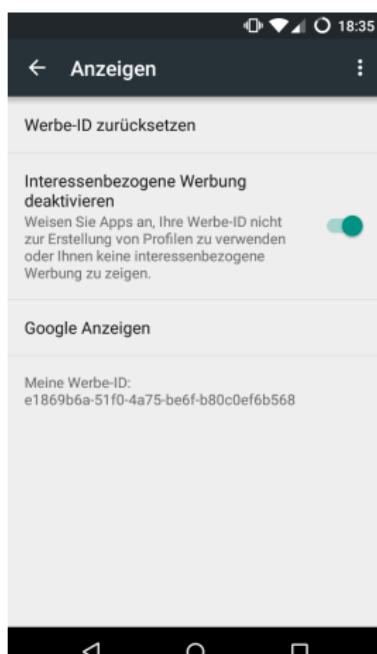
Antitracking auf dem Handy

Android: Google AdID

Google-Einstellungen -> Anzeigen ->
Anzeigen

iOS: Apple IDFA

Settings -> General -> About ->
Advertising



Dezentrale Dienste

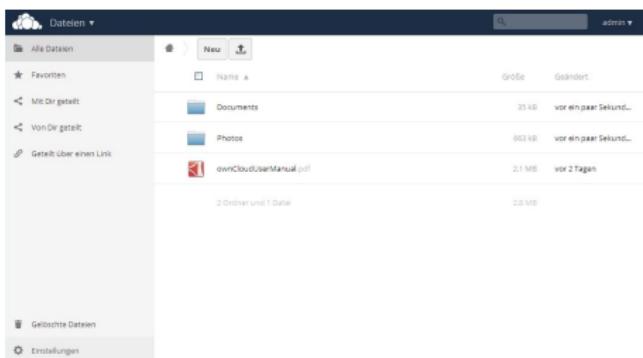


E-Mail



Owncloud

Plattformübergreifende
Synchronisierung von
Dateien, Dokumenten,
Kalendern, Kontakten,
Notizen und News.



Owncloud als Ersatz für Dropbox

The screenshot shows the OwnCloud web interface. The top navigation bar includes a logo, the text "Dateien ▾", a search bar, and a user dropdown set to "admin ▾". On the left, there's a sidebar with links for "Alle Dateien", "Favoriten", "Mit Dir geteilt", "Von Dir geteilt", "Geteilt über einen Link", "Gelöschte Dateien", and "Einstellungen". The main content area displays a list of files and folders:

Name	Größe	Geändert
Documents	35 kB	vor ein paar Sekund...
Photos	663 kB	vor ein paar Sekund...
ownCloudUserManual.pdf	2,1 MB	vor 2 Tagen

Below the list, it says "2 Ordner und 1 Datei" with a total size of "2,0 MB".



Owncloud als Ersatz für Google/Apple-Sync

Calendar

Week 11 of 2016

Day Week Month Today

+ New Calendar

ownCloud

Private

contact_birthdays

Meetings(user4)

Subscriptions

3and(gig)(user3)

Settings

Sun 3/6 Mon 3/7 Tue 3/8 Wed 3/9 Thu 3/10 Fri 3/11 Sat 3/12

all-day 7am 8am 9am 10am 11am 12pm 1pm 2pm 3pm 4pm 5pm 6pm 7pm 8pm 9pm 10pm 11pm

Meeting with Jos

ownCloud

starts 03/10/2016 ends 03/10/2016

02:00 PM 05:00 PM

All day Event

Location

Description

When shared show full event

Attendees Reminders

E-Mail address of attendee

Add

Jos Poortvliet

Delete Cancel Export Update

Meeting with Jos

ownCloud

starts 03/10/2016 ends 03/10/2016

02:00 PM 05:00 PM

All day Event

Location

Description

When shared show full event

Attendees Reminders

E-Mail address of attendee

Add

Jos Poortvliet

Delete Cancel

Export

Update



Owncloud als Ersatz für Google/Apple-Sync

The screenshot shows the OwnCloud Contacts application interface. At the top, there's a navigation bar with icons for file operations (New, Open, Save, etc.) and search. Below the header, the title "Contacts" is displayed next to a cloud icon. On the left, a sidebar lists "All contacts" with icons and names: Franz Liszt (orange), Ludwig van Beethoven (green), Pyotr Tchaikovsky (pink), and Wolfgang Amadeus Mozart (purple). The contact for Wolfgang Amadeus Mozart is currently selected and shown in a detailed view on the right. The view includes fields for email (wolfgang@mozart.at), work phone number (Work), address (Post Office B., Address: Mozartplatz, Postal Code: 5010, City: Salzburg), state/province (State or pro...), country (Country: Austria), birthday (01/27/1756), and a dropdown for Composers. There are also buttons for "Add field ..." and a trash bin icon. At the bottom of the sidebar, there's a "Settings" icon.

Owncloud als Ersatz für Google Docs

The screenshot shows a web browser window with the ownCloud interface. The title bar reads "Format" with various styling options like bold, italic, underline, font size 10.4pt, and a text body button. The main content area is titled "ownCloud Example Document". It contains a paragraph about ownCloud being a self-hosted file sync and share solution, followed by a section about its mobile and desktop client support. A sidebar on the right shows a user profile for "Rosa Luxemburg" with an orange "A" icon and a small photo.

Below the main content, there's a comment section:

- A comment from "admin" (2015-06-24T08:34:11Z) with 0.288Z likes:

I find this entirely non-offensive! It can use improvements.
- A reply from "Rosa Luxemburg" (2015-06-24T08:34:33Z) with 8.408Z likes:

I don't like control unless it is mine.

At the bottom of the document view, there's a note: "(All example pictures & music are licensed under Creative Commons Attribution.)"

Passwörter

Passwörter

- Keine einfachen Wörter

Passwörter

- Keine einfachen Wörter
- Groß-, Kleinbuchstaben, Ziffern, Sonderzeichen

Passwörter

- Keine einfachen Wörter
 - Groß-, Kleinbuchstaben, Ziffern, Sonderzeichen
 - Beispiele:

Passwörter

- Keine einfachen Wörter
- Groß-, Kleinbuchstaben, Ziffern, Sonderzeichen
- Beispiele:
 - dragon

Passwörter

- Keine einfachen Wörter
- Groß-, Kleinbuchstaben, Ziffern, Sonderzeichen
- Beispiele:
 - dragon
 - (nCuAj.§Tsm!f

Passwörter

- Keine einfachen Wörter
- Groß-, Kleinbuchstaben, Ziffern, Sonderzeichen
- Beispiele:
 - dragon
 - (nCuAj.§Tsm!f
 - IchLiebeDich

Passwörter

- Keine einfachen Wörter
- Groß-, Kleinbuchstaben, Ziffern, Sonderzeichen
- Beispiele:
 - dragon
 - (nCuAj.§Tsm!f
 - IchLiebeDich
 - dadada

Passwörter

- Keine einfachen Wörter
- Groß-, Kleinbuchstaben, Ziffern, Sonderzeichen
- Beispiele:
 - dragon
 - (nCuAj.§Tsm!f
 - IchLiebeDich
 - dadada
 - qwerty

Passwörter

- Keine einfachen Wörter
- Groß-, Kleinbuchstaben, Ziffern, Sonderzeichen
- Beispiele:
 - dragon
 - (nCuAj.§Tsm!f
 - IchLiebeDich
 - dadada
 - qwerty
 - Mks?o/.u,1Psw!

Passwörter

- Keine einfachen Wörter
- Groß-, Kleinbuchstaben, Ziffern, Sonderzeichen
- Beispiele:
 - dragon
 - (nCuAj.§Tsm!f
 - IchLiebeDich
 - dadada
 - qwerty
 - Mks?o/.u,1Psw!

Passwörter

- Keine einfachen Wörter
- Groß-, Kleinbuchstaben, Ziffern, Sonderzeichen
- Beispiele:
 - dragon
 - (nCuAj.§Tsm!f
 - IchLiebeDich
 - dadada
 - qwerty
 - Mks?o/.u,1Psw!
- Verschiedene Passwörter nutzen!

Passwörter

- Keine einfachen Wörter
- Groß-, Kleinbuchstaben, Ziffern, Sonderzeichen
- Beispiele:
 - dragon
 - (nCuAj.§Tsm!f
 - IchLiebeDich
 - dadada
 - qwerty
 - Mks?o/.u,1Psw!
- Verschiedene Passwörter nutzen!
- Passwort-Manager verwenden
(z.B. Keepass, Password Safe)

“Ich hab ja nichts zu verbergen”

“Arguing that you don't care about the right to 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.” (Edward Snowden, 21.05.2015 auf Reddit)

Fazit

- Verschlüsselung nutzen (Signal, Conversations, ChatSecure)
- Dezentrale Dienste nutzen (Email, Jabber, Owncloud)
- Endgeräte schützen (Permissions, Freie Software, Geräteverschlüsselung)



Folien: Chaos Computer Club Dresden

CMS Dresden: schule@c3d2.de

Vortragender: Marius Melzer (marius@rasumi.net,

PGP-Fingerprint: 6730 E691 36B9 9BB8 FFB1 2662 A97B
F176 52DE FC3E)

