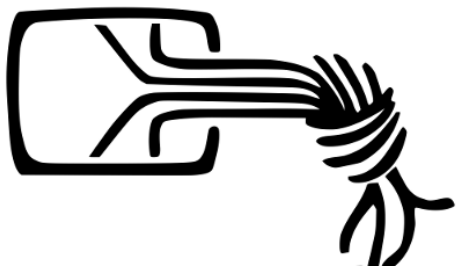
Wie schütze ich mich vor Überwachung?

Marius Melzer
Chaos Computer Club Dresden

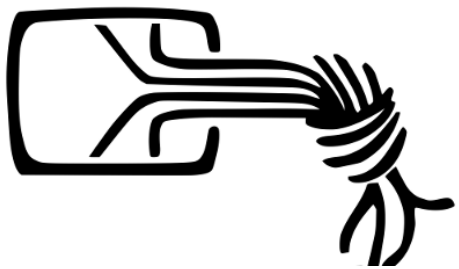
24.11.2015

Chaos Computer Club



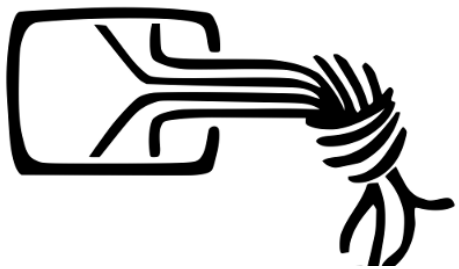
- Verein wurde 1981 gegründet (`https://ccc.de`)

Chaos Computer Club



- Verein wurde 1981 gegründet (`https://ccc.de`)
- Aktuell ca. 4500 Mitglieder

Chaos Computer Club



- Verein wurde 1981 gegründet (`https://ccc.de`)
- Aktuell ca. 4500 Mitglieder
- Betreibt u.a. Öffentlichkeitsarbeit und Politikberatung

Chaos Computer Club

Chaos Computer Club

Chaos Computer Club

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

Chaos Computer Club

- Chaos Computer Club Dresden (`https://c3d2.de`)
- Datenspuren: 24./25. Oktober 2015 (`https://datenspuren.de`)

Chaos Computer Club

- Chaos Computer Club Dresden (`https://c3d2.de`)
- Datenspuren: 24./25. Oktober 2015 (`https://datenspuren.de`)
- Podcasts (`https://c3d2.de/radio.html`)

Chaos Computer Club

- Chaos Computer Club Dresden (`https://c3d2.de`)
- Datenspuren: 24./25. Oktober 2015 (`https://datenspuren.de`)
- Podcasts (`https://c3d2.de/radio.html`)
- Chaos macht Schule (`https://c3d2.de/schule.html`)

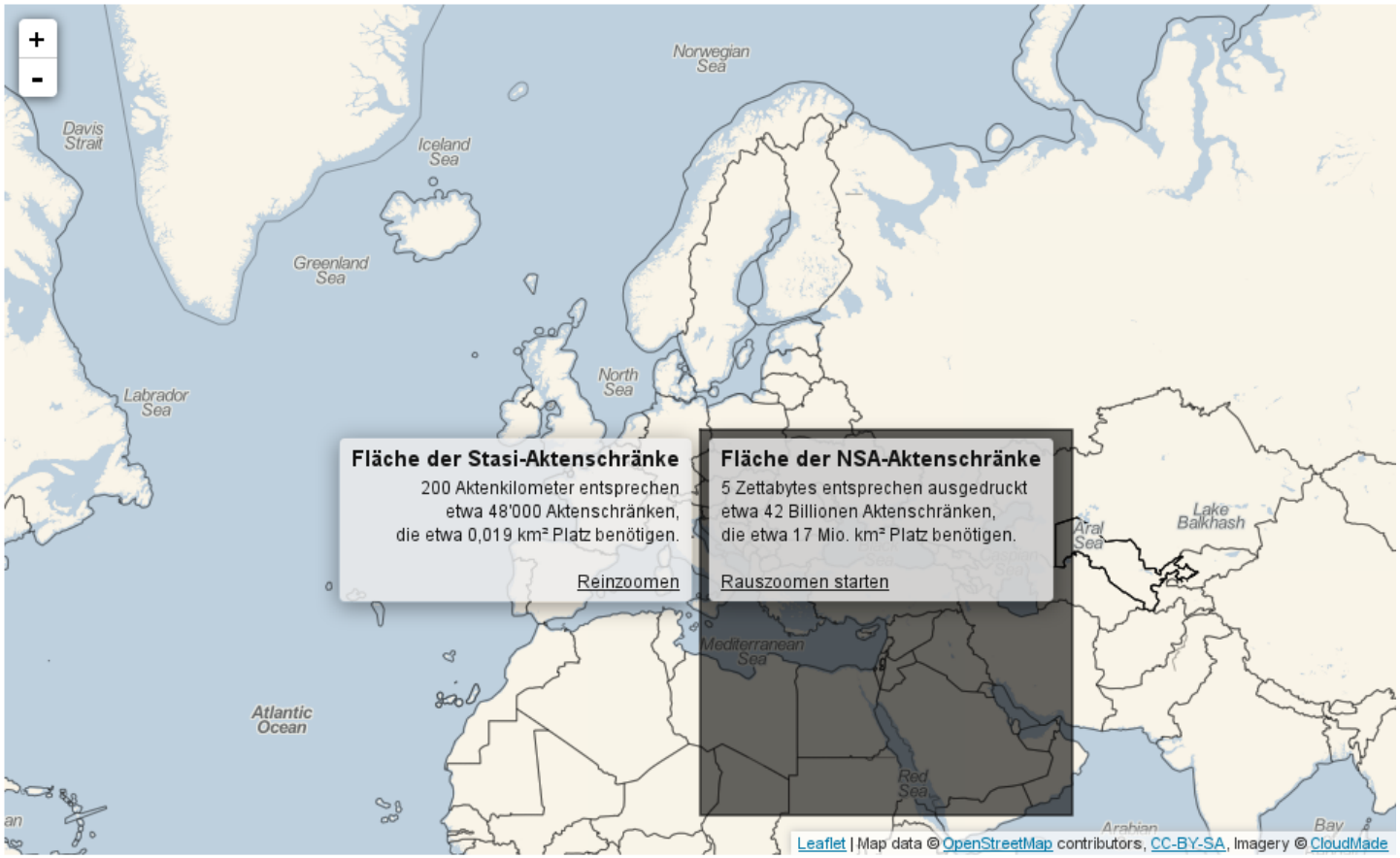
Bundespräsident Gauck zur NSA-Überwachung

"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



Realisiert von OpenDataCity. Anwendung steht unter CC-BY 3.0.

Wer sind potenzielle Angreifer?

- Andere Nutzer eines Dienstes

Wer sind potenzielle Angreifer?

- Andere Nutzer eines Dienstes
- Fremde (“Hacker”)

Wer sind potenzielle Angreifer?

- Andere Nutzer eines Dienstes
- Fremde (“Hacker”)
- Dienstanbieter

Wer sind potenzielle Angreifer?

- Andere Nutzer eines Dienstes
- Fremde (“Hacker”)
- Dienstanbieter
- staatliche Institutionen, Netzbetreiber

Was ist zu schützen?

- Kommunikation

Was ist zu schützen?

- Kommunikation
- Verhalten von Software/Endgeräten

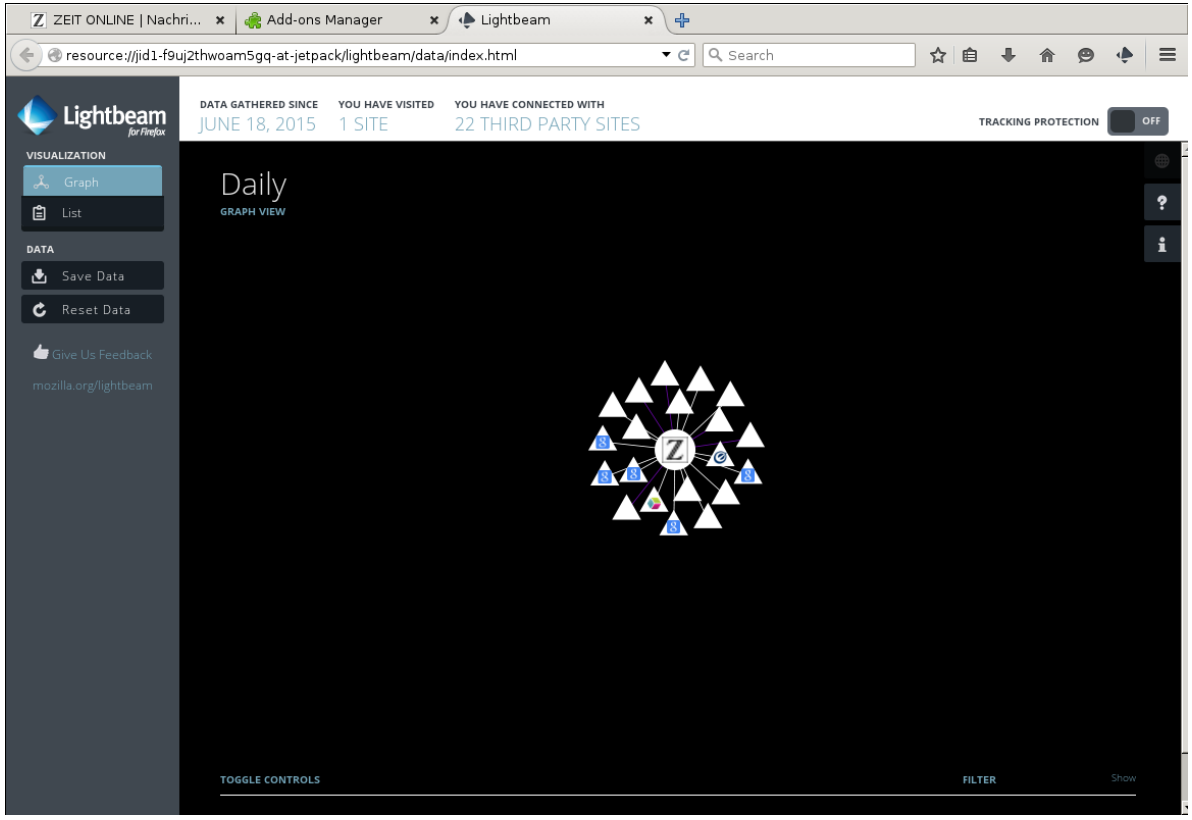
Was ist zu schützen?

- Kommunikation
  - Wer? (Nutzer-Nutzer, Nutzer-Dienst, Dienst-Dienst)
- Verhalten von Software/Endgeräten

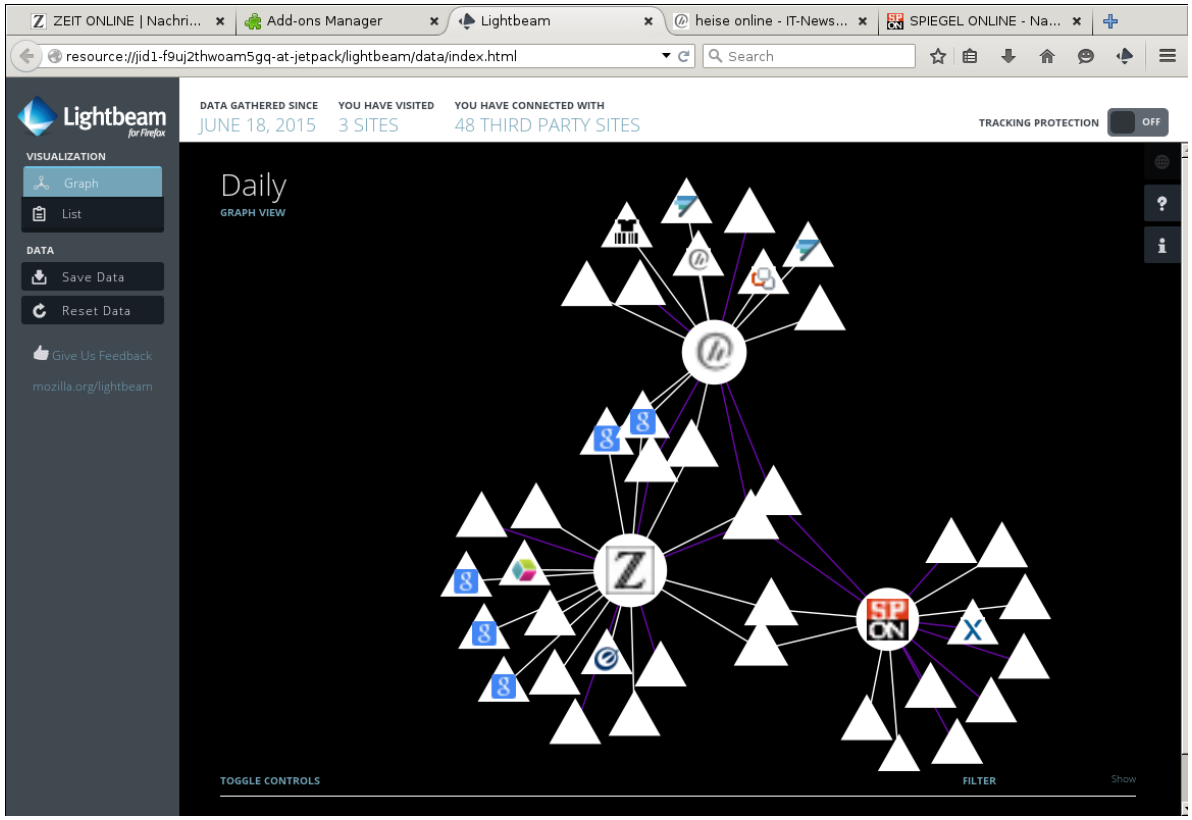
Was ist zu schützen?

- Kommunikation
  - Wer? (Nutzer-Nutzer, Nutzer-Dienst, Dienst-Dienst)
  - Was? (Inhalte, Metadaten)
- Verhalten von Software/Endgeräten

Metadaten im WWW



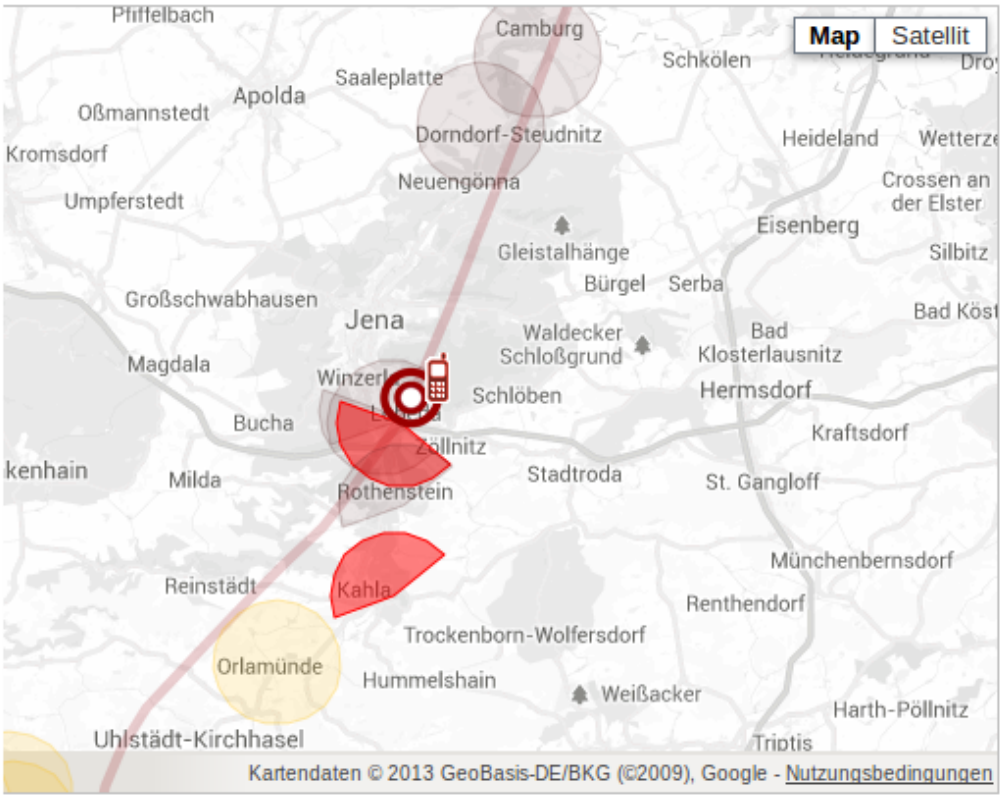
Metadaten im WWW



Metadaten - VDS

- Handynetz
  - Telefonnummern
  - Zeitpunkt und Dauer (Telefonate, SMS)
  - Funkzelle (Ort)
- Internet
  - IP-Adresse (= ungefährer Ort)
  - Alle Verbindungen
  - Email: Adressen von Sender und Empfänger, Zugriff

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

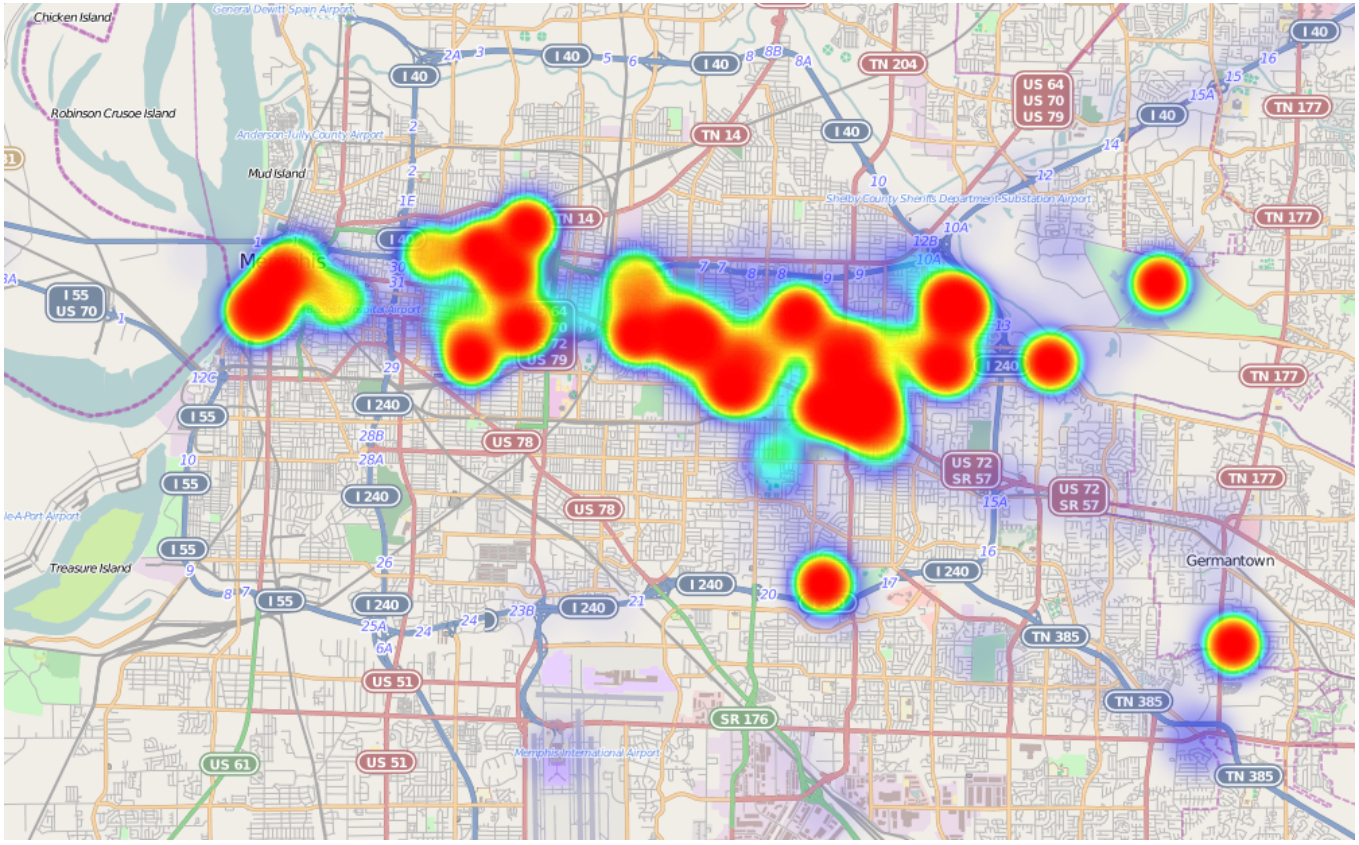
Speed

31 Aug 09 15:30

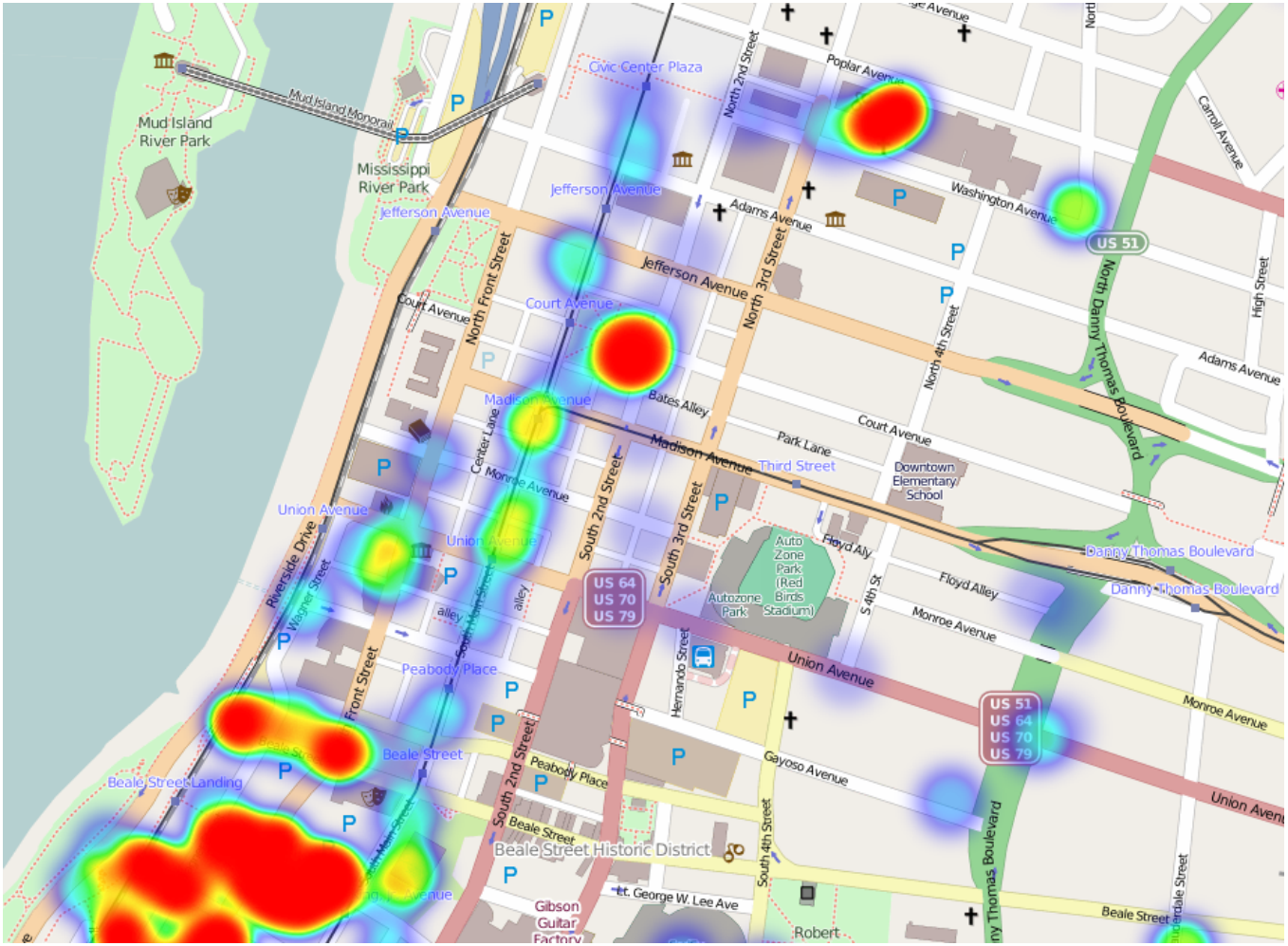
Show the points in time, Malte Spitz was in the selected map segment, too

Download Data

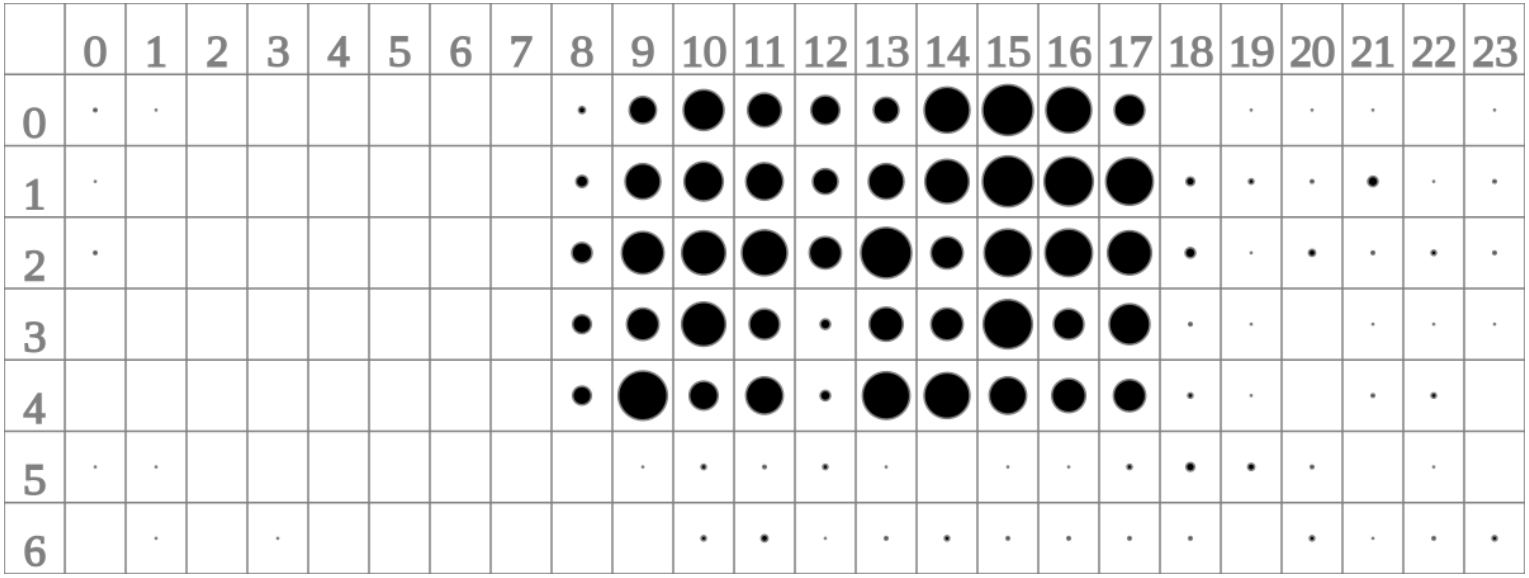
Google Takeout



Google Takeout

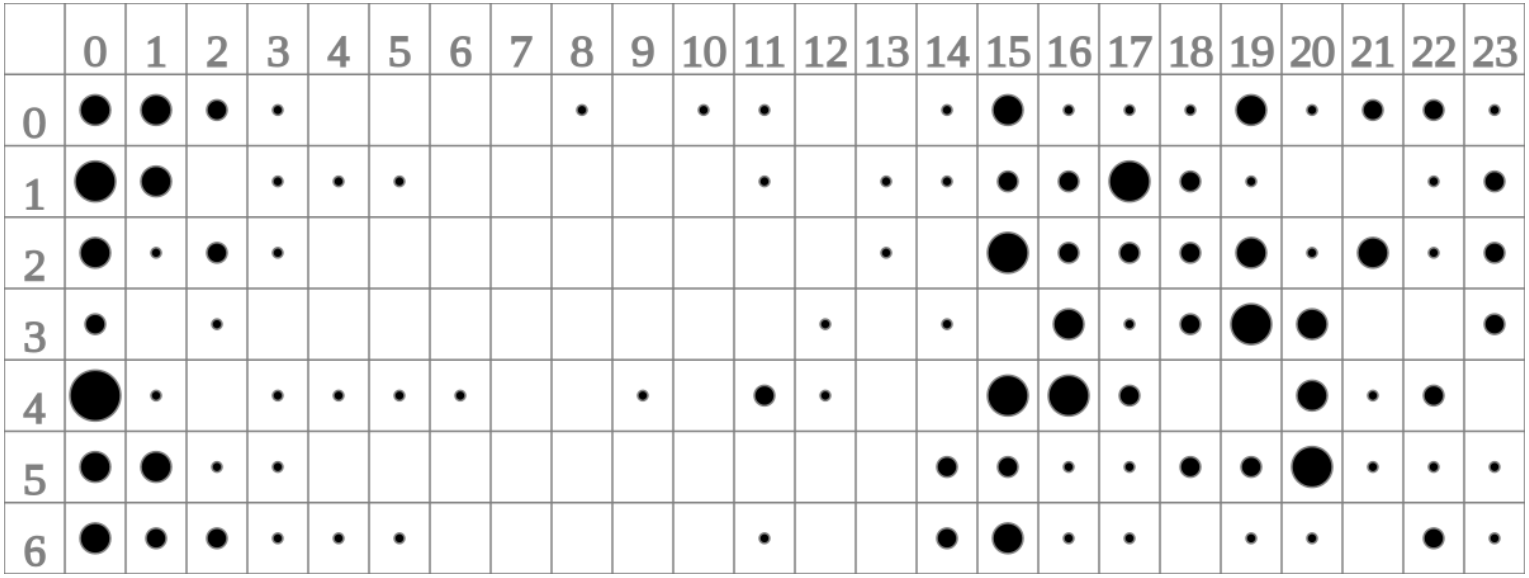


Zeitstempel



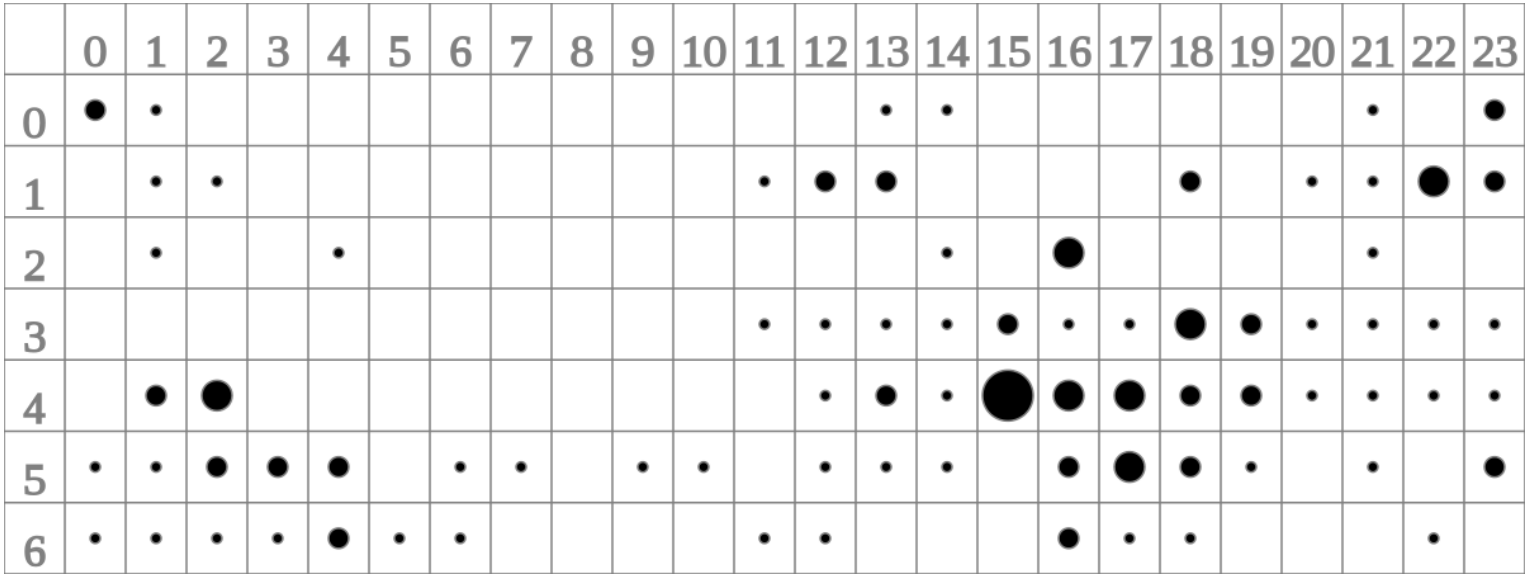
Alan, Microblogging

Zeitstempel



Bob, Microblogging

Zeitstempel



Charlie, Github

Was ist zu schützen?

- Kommunikation
  - Wer? (Nutzer-Nutzer, Nutzer-Dienst, Dienst-Dienst)
  - Was? (Inhalte, Metadaten)
- Verhalten von Software/Endgeräten

Was ist zu schützen?

- Kommunikation
  - Wer? (Nutzer-Nutzer, Nutzer-Dienst, Dienst-Dienst)
  - Was? (Inhalte, Metadaten)
- Verhalten von Software/Endgeräten
  - Schwachstellen

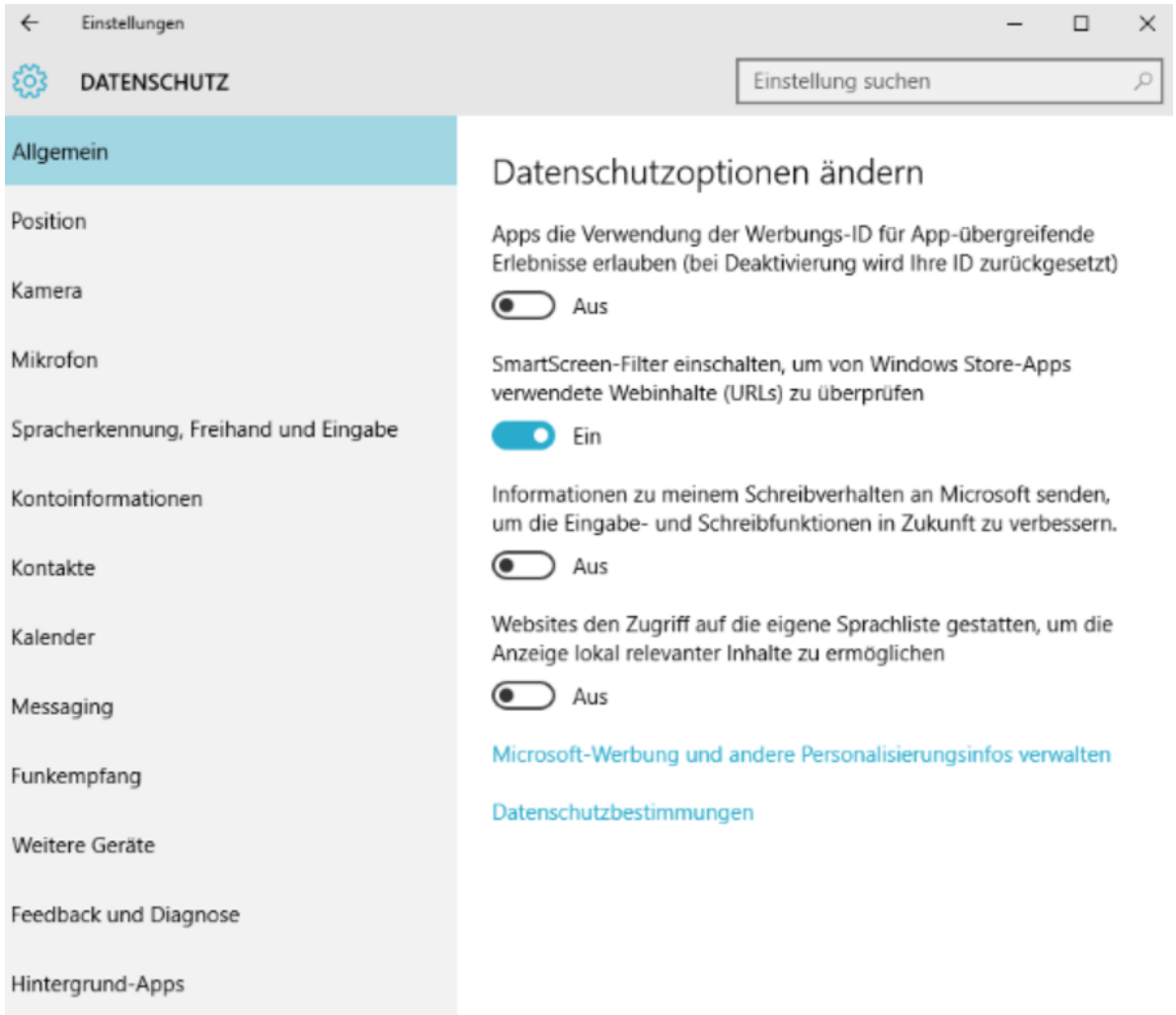
Was ist zu schützen?

- Kommunikation
  - Wer? (Nutzer-Nutzer, Nutzer-Dienst, Dienst-Dienst)
  - Was? (Inhalte, Metadaten)
- Verhalten von Software/Endgeräten
  - Schwachstellen
  - Backdoors

Was ist zu schützen?

- Kommunikation
  - Wer? (Nutzer-Nutzer, Nutzer-Dienst, Dienst-Dienst)
  - Was? (Inhalte, Metadaten)
- Verhalten von Software/Endgeräten
  - Schwachstellen
  - Backdoors
  - Offizielle Funktionalität

Schadhafte Funktionalität



Was tun? (4 Punkte)

- Verschlüsselung nutzen (Inhalte)

Verschlüsselung zum Dienst: SSL

Browser-Plugin: HTTPS Everywhere

Ende-zu-Ende-Verschlüsselung

- GPG für E-Mails

Ende-zu-Ende-Verschlüsselung

- GPG für E-Mails
- OTR für Jabber:
  - Pidgin mit OTR-Plugin für Linux und Windows
  - ChatSecure oder Xabber für Android
  - Adium für Mac, ChatSecure für iOS

Ende-zu-Ende-Verschlüsselung

- GPG für E-Mails
- OTR für Jabber:
  - Pidgin mit OTR-Plugin für Linux und Windows
  - ChatSecure oder Xabber für Android
  - Adium für Mac, ChatSecure für iOS
- palava.tv, talky.io, Tox, Linphone für Videotelefonie

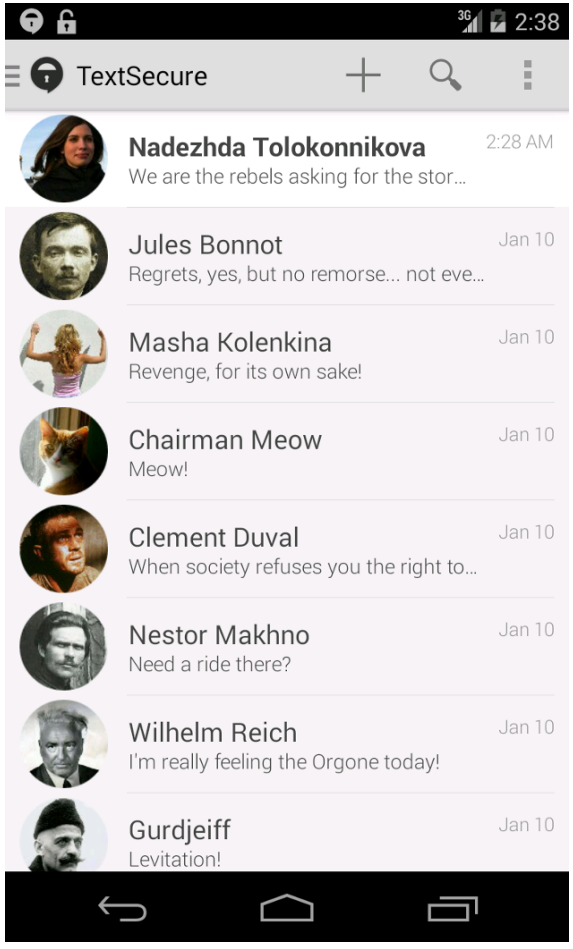
Ende-zu-Ende-Verschlüsselung

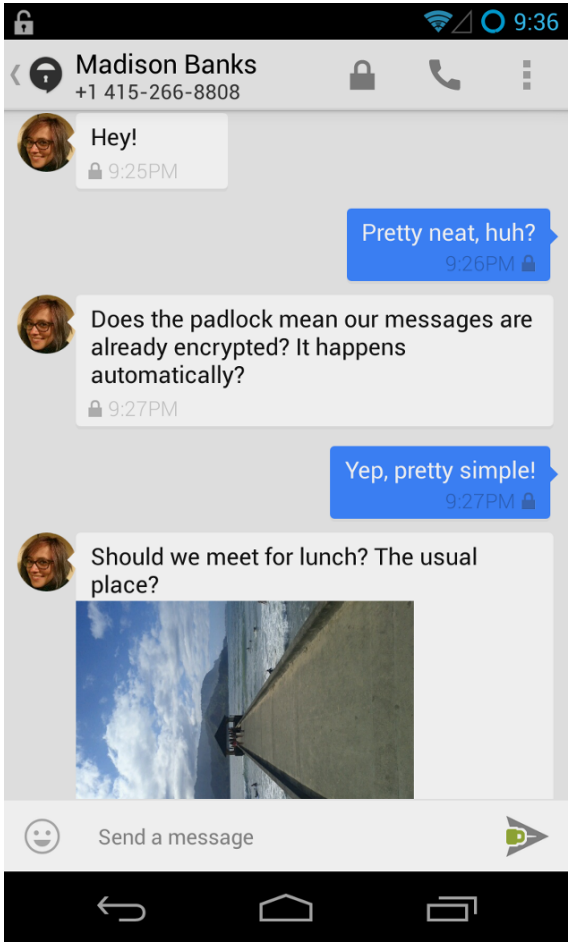
- GPG für E-Mails
- OTR für Jabber:
  - Pidgin mit OTR-Plugin für Linux und Windows
  - ChatSecure oder Xabber für Android
  - Adium für Mac, ChatSecure für iOS
- palava.tv, talky.io, Tox, Linphone für Videotelefonie
- Signal

E-Mail-Selbstverteidigung

- https://emailselfdefense.fsf.org/de/

Signal

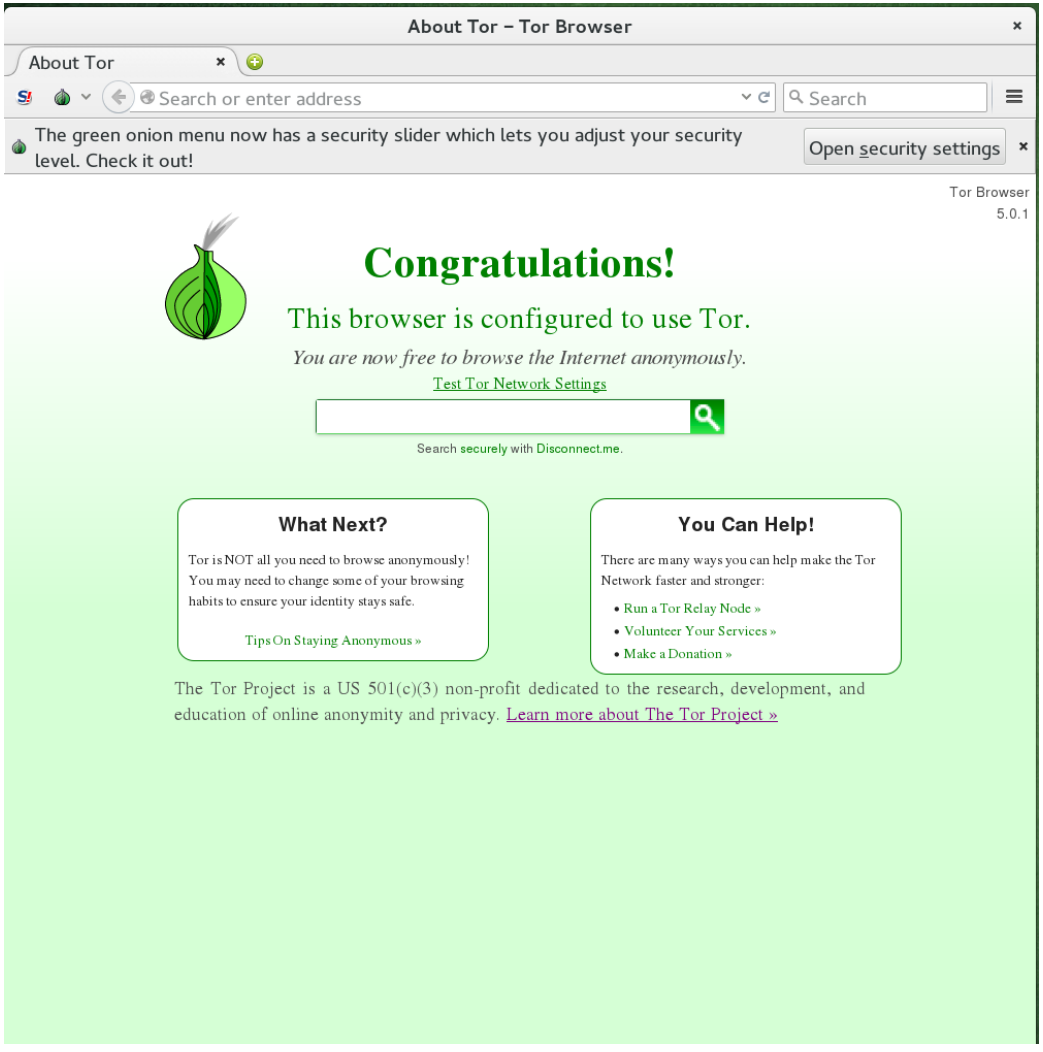

2:38
TextSecure
Nadezhda Tolokonnikova
2:28 AM
We are the rebels asking for the stor...
Jules Bonnot
Jan 10
Regrets, yes, but no remorse... not eve...
Masha Kolenkina
Jan 10
Revenge, for its own sake!
Chairman Meow
Jan 10
Meow!
Clement Duval
Jan 10
When society refuses you the right to...
Nestor Makhno
Jan 10
Need a ride there?
Wilhelm Reich
Jan 10
I'm really feeling the Orgone today!
Gurdjeiff
Jan 10
Levitation!


9:36
Madison Banks
+1 415-266-8808
Hey!
9:25PM
Pretty neat, huh?
9:26PM
Does the padlock mean our messages are already encrypted? It happens automatically?
9:27PM
Yep, pretty simple!
9:27PM
Should we meet for lunch? The usual place?
Send a message

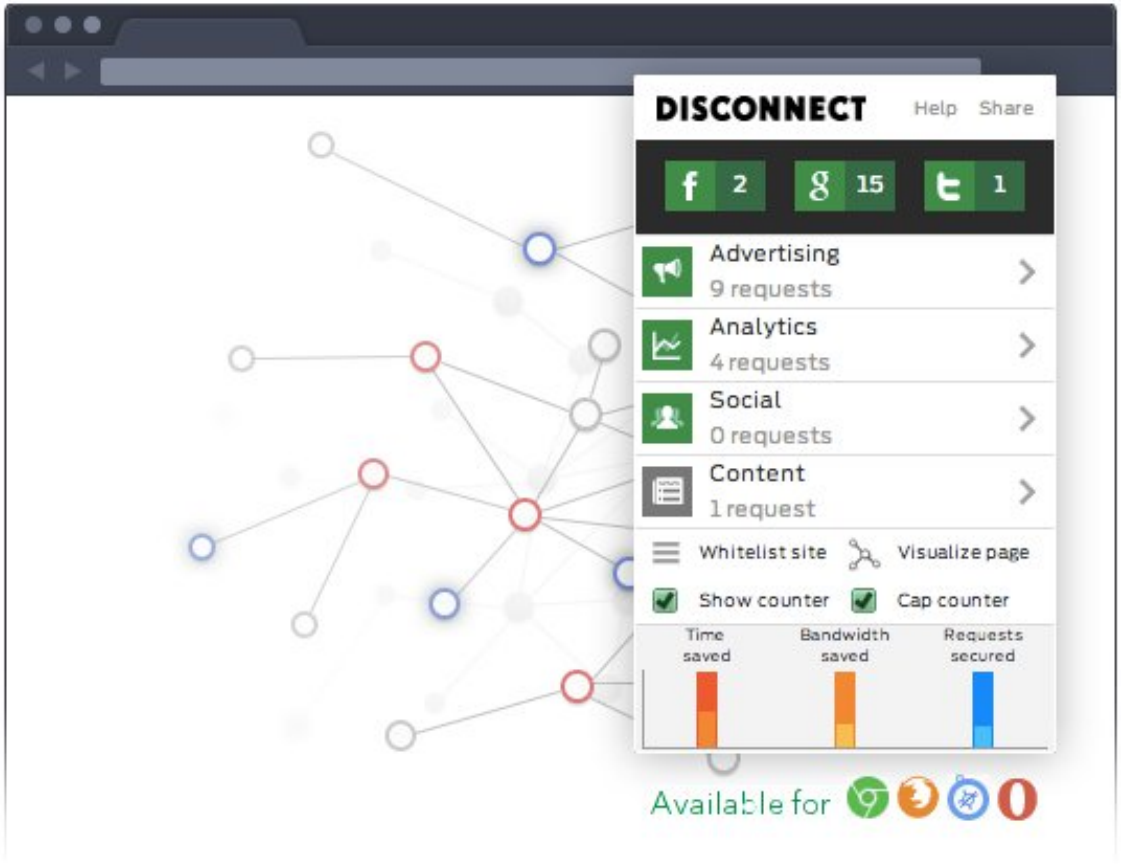
Was tun? (4 Punkte)

- Verschlüsselung nutzen (Inhalte)
- Anonymisieren (Metadaten)

Tor Browser


About Tor – Tor Browser
About Tor
Search or enter address
Search
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.me.
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 »

Disconnect (zum Verstecken der Websiteaufrufe)



Was tun? (4 Punkte)

- Verschlüsselung nutzen (Inhalte)
- Anonymisieren (Metadaten)
- Eigene Dienste betreiben (Inhalte + Metadaten)

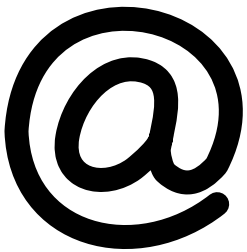
Dezentralisierung

- Idee:
  - Nutzerdaten nicht an Drittdienste abgeben

Dezentralisierung

- Idee:
  - Nutzerdaten nicht an Drittdienste abgeben
  - Kein zentraler Ort für Daten

Dezentrale Dienste



E-Mail

Was tun? (4 Punkte)

- Verschlüsselung nutzen (Inhalte)
- Anonymisieren (Metadaten)
- Eigene Dienste betreiben (Inhalte + Metadaten)
- Endgeräte schützen

Geräte schützen

- Grundlagen IT-Sicherheit (Passwörter, Medienverständnis)

Geräte schützen

- Grundlagen IT-Sicherheit (Passwörter, Medienverständnis)
- Aktuelle Software

Geräte schützen

- Grundlagen IT-Sicherheit (Passwörter, Medienverständnis)
- Aktuelle Software
- Vertrauenswürdige Software

Geräte schützen

- Grundlagen IT-Sicherheit (Passwörter, Medienverständnis)
- Aktuelle Software
- Vertrauenswürdige Software
  - Open Source ist transparenter, anpassbarer und funktional oft ebenbürtig

Geräte schützen

- Grundlagen IT-Sicherheit (Passwörter, Medienverständnis)
- Aktuelle Software
- Vertrauenswürdige Software
  - Open Source ist transparenter, anpassbarer und funktional oft ebenbürtig
  - verhindert Abhängigkeiten

Fazit

- Verschlüsselung nutzen (Inhalte)
- Anonymisieren (Metadaten)
- Eigene Dienste betreiben (Inhalte + Metadaten)
- Endgeräte schützen

CMS Dresden: schule@c3d2.de

Fazit

- Verschlüsselung nutzen (Inhalte)
- Anonymisieren (Metadaten)
- Eigene Dienste betreiben (Inhalte + Metadaten)
- Endgeräte schützen
- ...mit gutem Vorbild vorangehen

CMS Dresden: schule@c3d2.de