

NSA, Prism und co - Wie schützt man sich vor Überwachung?

Marius Melzer
Chaos Computer Club Dresden

23.04.2014

Chaos Computer Club



Chaos Computer Club



Chaos Computer Club

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

Chaos Computer Club

- Chaos Computer Club Dresden (<http://c3d2.de>)
 - Datenspuren: 13./14.09.2014 <http://datenspuren.de>

Chaos Computer Club

- Chaos Computer Club Dresden (<http://c3d2.de>)
 - Datenspuren: 13./14.09.2014 <http://datenspuren.de>
 - Podcasts (<http://pentamedia.de>)



Chaos Computer Club

- Chaos Computer Club Dresden (<http://c3d2.de>)
 - Datenspuren: 13./14.09.2014 <http://datenspuren.de>
 - Podcasts (<http://pentamedia.de>)
 - Chaos macht Schule



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.“

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](#).



Merkels Handy

News Newsticker 7-Tage-News Archiv Foren



Topthemen: NSA Xbox Playstation 4 Windows 8.1 VDSL iPad iPhone Android Google Nexus

heise online > News > 2013 > KW 48 > NSA-Affäre: Merkel angeblich von fünf Geheimdiensten abgehört

26.11.2013 09:43

« Vorige | Nächste »

NSA-Affäre: Merkel angeblich von fünf Geheimdiensten abgehört

vorlesen / MP3-Download

Angela Merkel wurde in ihrer Amtszeit als Bundeskanzlerin nicht nur von der NSA, sondern auch den Geheimdiensten Russlands, Chinas, Nordkoreas und Großbritanniens abgehört. [Das berichtete](#) der Focus am Sonntag unter Berufung auf eine nicht näher erläuterte Analyse deutscher Sicherheitsbehörden. Hilfreich bei den Angriffen [auf das ungesicherte Handy](#) der Kanzlerin sei das weitläufige Regierungsviertel in Berlin, das sich hervorragend für die Funkspionage eigne, wird ein hochrangiger Sicherheitsbeamter zitiert.

Dem Bericht zufolge arbeiten alleine für Russland 120 Geheimdienstler in Deutschland und spähen die Bundesrepublik aus. Offiziell eingesetzt würden sie von der russischen Botschaft. Weiterhin hätten ausländische Geheimdienste in den vergangenen Jahren versucht, mehr als 100 deutsche Politiker, Beamte, Militärs, Manager und Wissenschaftler als Quellen anzuwerben. Das sei aber nur die Zahl derer, die sich danach bei deutschen Behörden gemeldet hätten, die tatsächliche Dunkelziffer sei unbekannt, aber wohl beträchtlich.

Top-News

Rätselhafte Entführungen im Internet

Ungewisse Zukunft für Windows RT

Satelliten made in Germany

NSA soll 75 Millionen US-Dollar zum Schutz vor Whistleblowing erhalten

Große Koalition setzt auf intelligente Stromzähler

Videos bei heise online

1 2 3 4 5

ct zockt (Episode 23)

Diesmal: Tower-Defense-Spiel "Kingdom", Japan-Gruseler "Run into the Dark" und "Code Combat".



heise open

Zehn Jahre bei Fedora

Bei der Mitarbeit an einer Linux-



Wem nützen meine Daten?

Wem nützen meine Daten?

- ### • Unternehmen

Wem nützen meine Daten?

- Unternehmen
 - (Zielgerichtete) Werbung

Wem nützen meine Daten?

- Unternehmen
 - (Zielgerichtete) Werbung
 - Tracking

Wem nützen meine Daten?

- Unternehmen
 - (Zielgerichtete) Werbung
 - Tracking
- Staat, Geheimdienste

Wem nützen meine Daten?

- Unternehmen
 - (Zielgerichtete) Werbung
 - Tracking
- Staat, Geheimdienste
 - Terrorismusbekämpfung? Kinderpornographie?

Wem nützen meine Daten?

- Unternehmen
 - (Zielgerichtete) Werbung
 - Tracking
- Staat, Geheimdienste
 - Terrorismusbekämpfung? Kinderpornographie?
 - => Kontrolle, Wirtschaftsspionage

Wem nützen meine Daten?

- Unternehmen
 - (Zielgerichtete) Werbung
 - Tracking
- Staat, Geheimdienste
 - Terrorismusbekämpfung? Kinderpornographie?
 - => Kontrolle, Wirtschaftsspionage
- Meine Mitmenschen

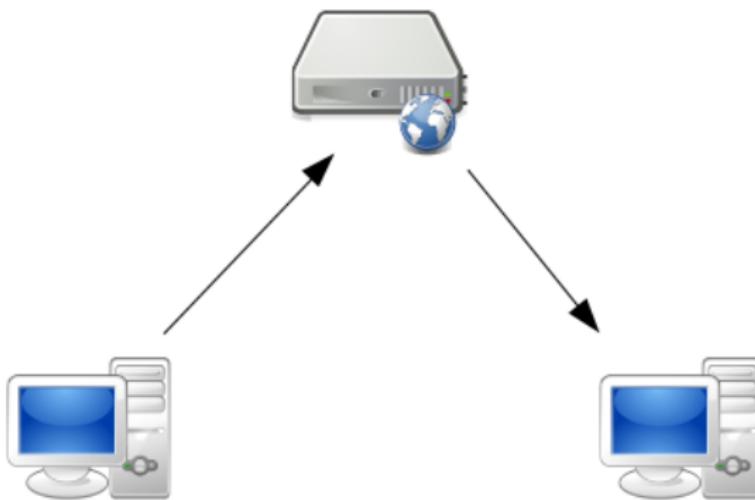
Wie schütze ich mich?

- technisch

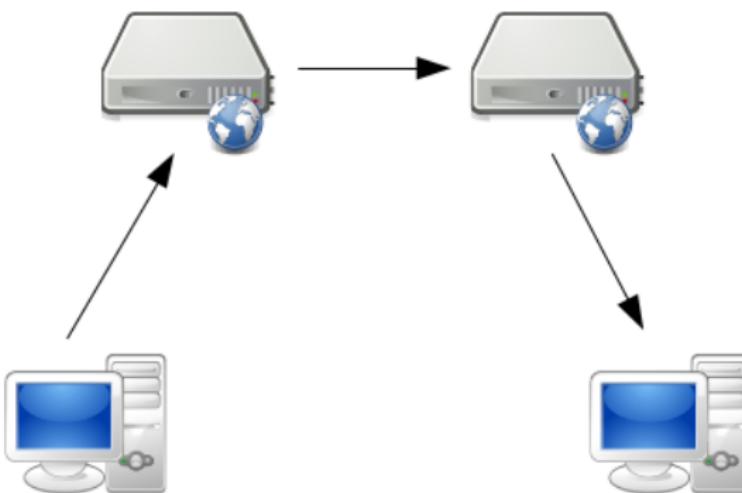
Wie schütze ich mich?

- technisch
- Verhalten

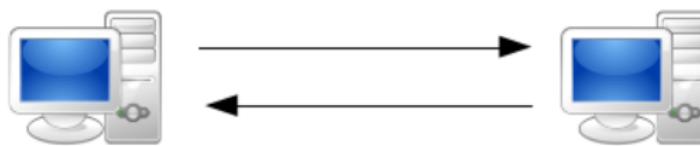
Wie kommunizieren wir im Internet?



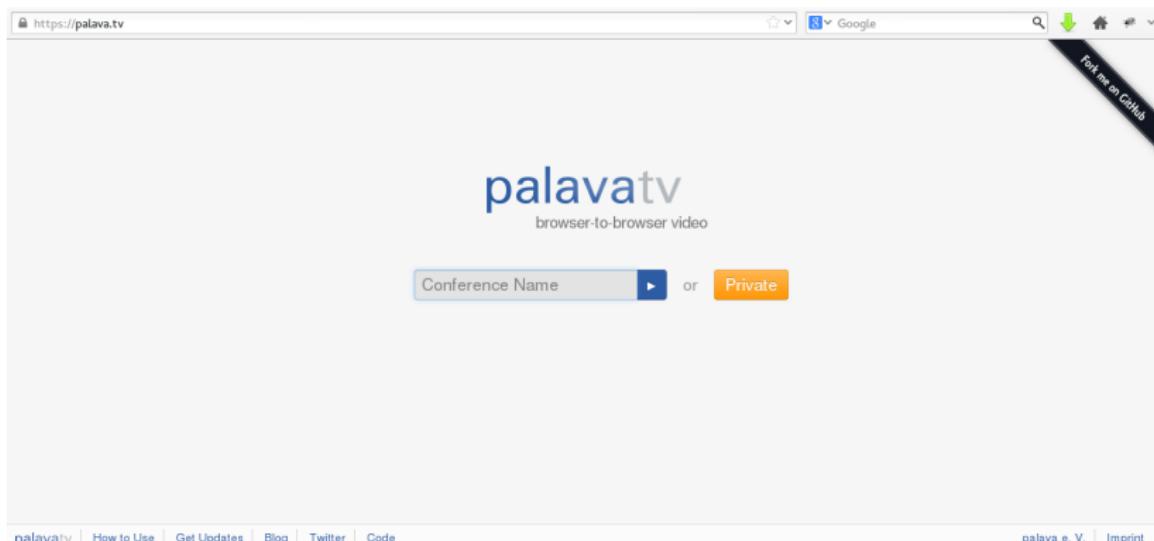
Föderation



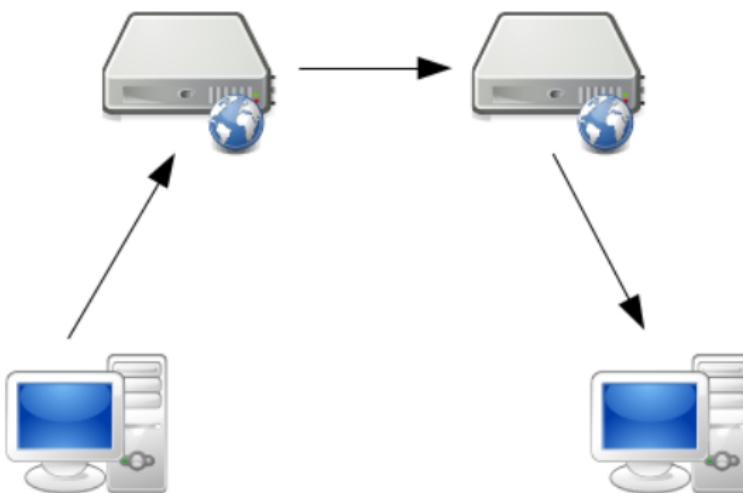
P2P



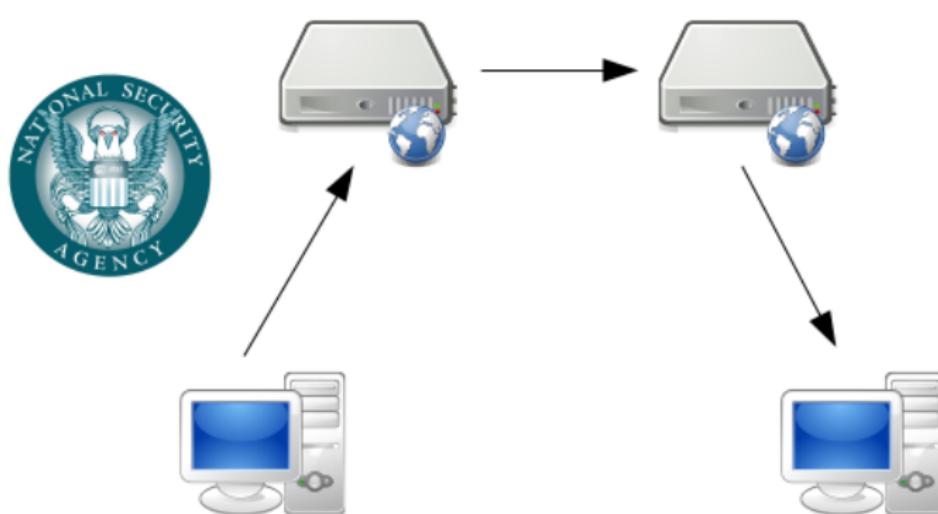
P2P: Praxis-Beispiel: <https://palava.tv>



Was ist zu schützen?



Was ist zu schützen?



Tempora

Home | Video | Themen | Forum | English | DER SPIEGEL | SPIEGEL TV | Abo | Shop | Schlagzeilen | Wetter | TV-Programm | mehr ▾

Login | Registrierung

SPIEGEL ONLINE NETZWELT

Politik | Wirtschaft | Panorama | Sport | Kultur | Netzpolit. | Wissenschaft | Gesundheit | einestages | Karriere | Uni | Schule | Reise | Auto

Nachrichten > Netzpolit. > Netzpolitik > Überwachung > Internetüberwachung: Tempora ist schlimmer als Prism

Netz-Spähsystem Tempora: Der ganz große britische Bruder



Mehr als 200 Glasfaserkabel sollen die Briten angezapft haben

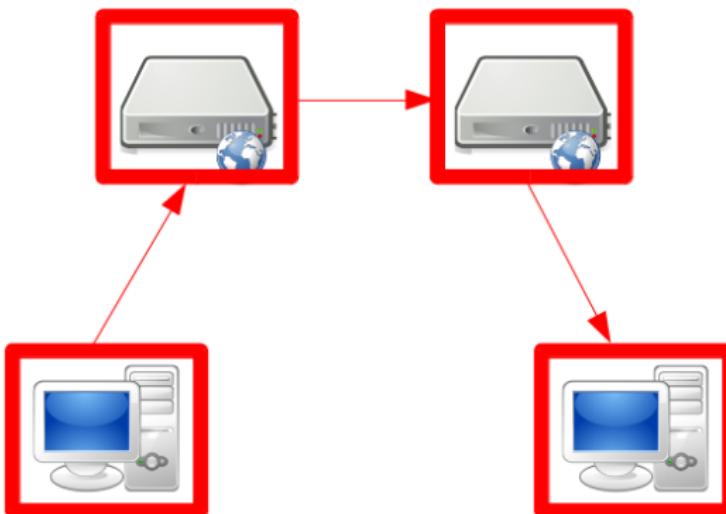
© DPA/dpa/VRK/Regenttaucher.com

Das umstrittene US-Spähprogramm Prism? Ist harmlos im Vergleich dazu, in welchem Umfang ein britischer Geheimdienst unter dem Codenamen Tempora weltweit das Internet ausspiioniert - und damit auch deutsche Nutzer. Doch selbst Datenschutzaaktivisten halten das Vorgehen für legal.

Hamburg/London - Die Aufregung war riesig, als bekannt wurde, dass die National Security Agency (NSA) im Rahmen ihres unter US-Präsident Barack Obama initiierten Spähprogramms Prism die Kunden von Telefon- und Internetfirmen ausleuchtet - Big Brother is watching you. Doch Brit Brother tut genau das auch. Und in mancher Hinsicht scheint die Überwachung durch die britischen Netzspione viel umfassender zu sein als die der Amerikaner.



Was ist zu schützen?



Wie schütze ich meinen Computer?

- (VirensScanner)
- Firewall
- Aktuelle und vertrauenswürdige Software

Wie schütze ich mein Smartphone?

- Permissions
- Firewall (z.B. AFwall+: <https://f-droid.org/repository/browse/?fdid=dev.ukanth.ufirewall>)
- Aktuelle und vertrauenswürdige Software
- Alternativer Appstore: f-droid.org

Vertrauenswürdige Software?

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

Open Source Software



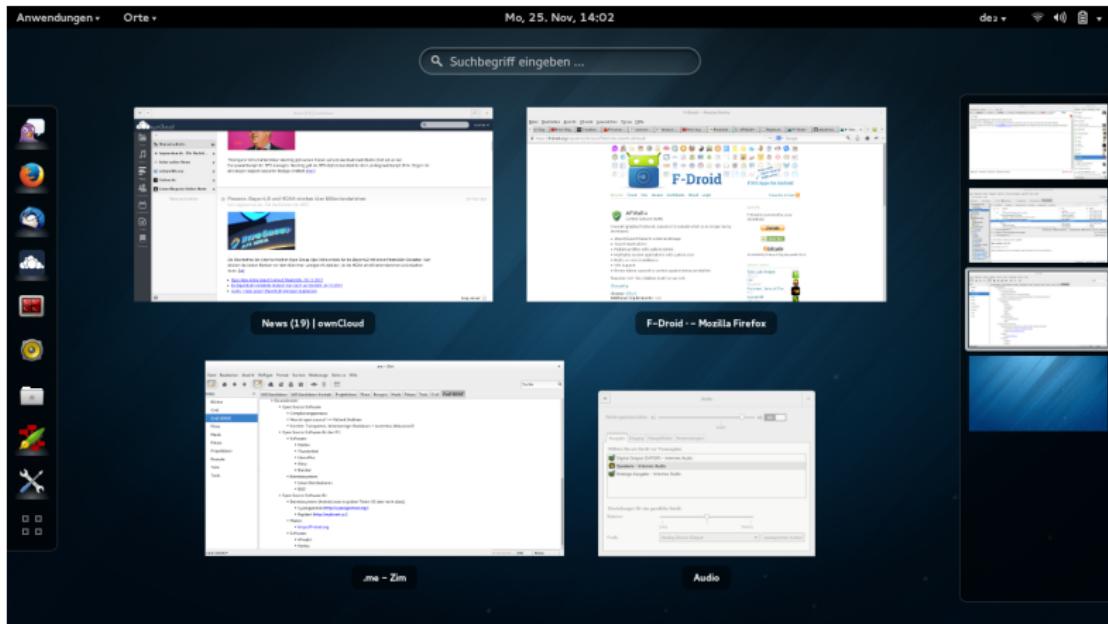
Foto: Anders Brenna



Freie Software

- Firefox
- Thunderbird
- LibreOffice
- Pidgin
- Evince/Okular
- Gimp
- VLC

Freie Software



Freie Software

https://prism-break.org/en/  Google

PRISM ↳ BREAK Platforms Protocols

Mobile	 Android	>
	 iOS	>
Computer	 BSD	>
	 GNU/Linux	>
	 OS X	>
	 Windows	>
Network	 Routers	>
	 Servers	>

Opt out of global programs like PRISM Tempora.
Stop governments from your communications at proprietary services.



Freie Software

https://prism-break.org/en/categories/android/

Operating Systems

Proprietary	Free Recommendations
BlackBerry	CyanogenMod Aftermarket firmware for Android devices.
Google Android	Replicant Fully free Android distribution based o...
Microsoft Windows Phone	Firefox OS Open source operating system for And...

Productivity

Proprietary	Free Recommendations
Doodle	dudle A free online poll with an optional priva... Web Service
Evernote	EtherCalc Multi-user spreadsheet server. Web Service
Microsoft Office Web A...	Etherpad Self-hosted, real-time collaborative doc... Web Service
Zoho Office Suite	ProtectedText Free online encrypted notepad. Web Service
	Riseup Secure communication tools for peop... Web Service

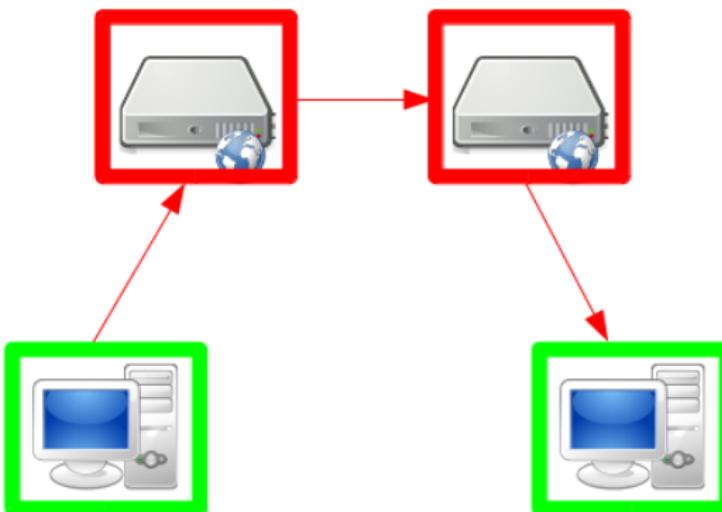
Categories

- Anonymizing Networks
- App Store
- DNS
- Email Accounts
- Email Clients
- Email Encryption
- File Storage & Sync
- Finance
- Instant Messaging
- Media Publishing
- Mesh Networks
- Operating Systems
- Productivity
- Social Networks
- Video & Voice
- VPN Accounts
- VPN Clients
- Web Browser Addons
- Web Browsers
- Web Hosting
- Web Search
- World Maps

Zusammenfassung

- Computer/Handy absichern
- Open Source Software verwenden

Was ist zu schützen?



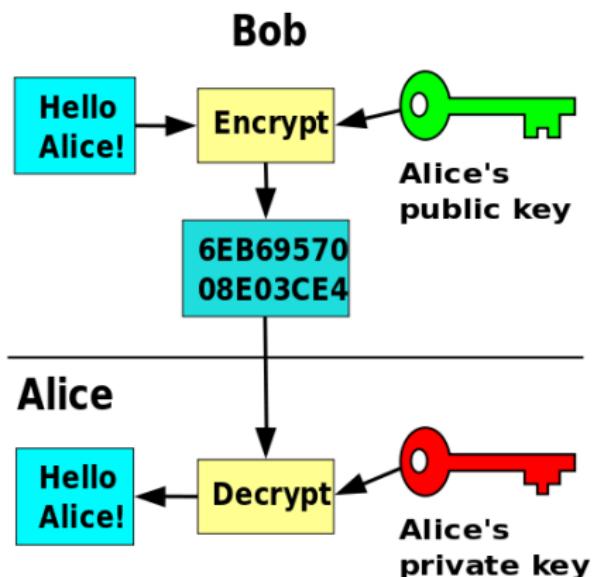
Verschlüsselung: Analogie



Grafik: Ronald Preuss

Verschlüsselung: Asymmetrische

Verschlüsselung: Asymmetrische



SSL / TLS

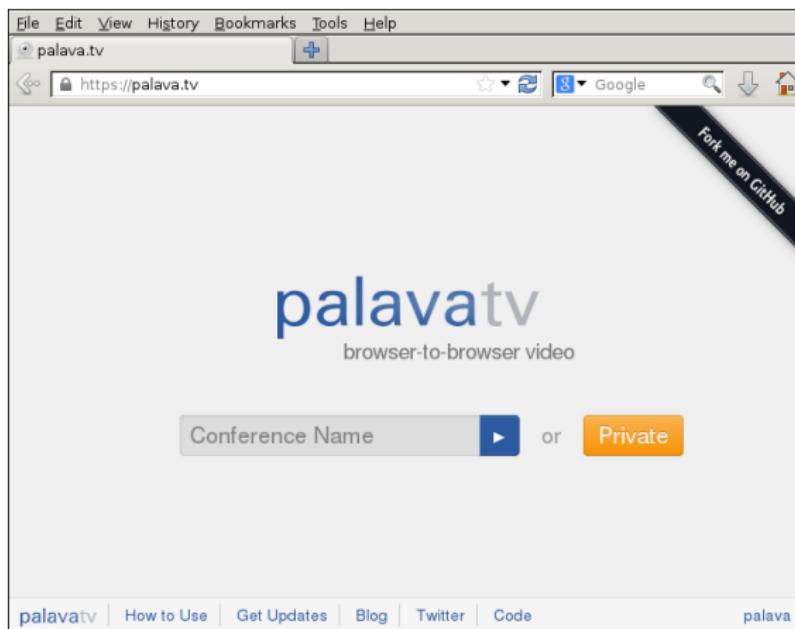
SSL / TLS

- SSL = Secure Socket Layer

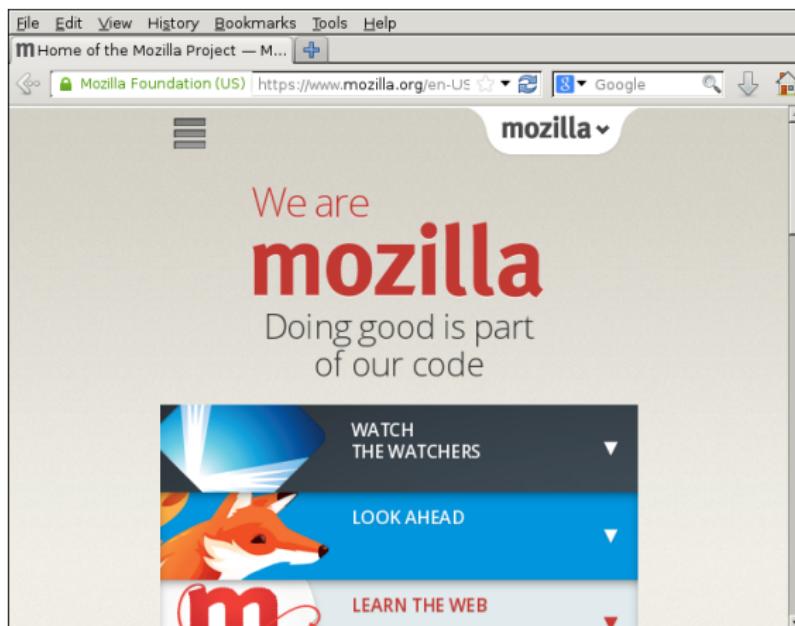
SSL / TLS

- SSL = Secure Socket Layer
- eingesetzt im Web, Mail, ...

SSL im Browser



SSL im Browser



SSL im Browser

The screenshot shows a web browser window with the following details:

- Address Bar:** https://pentapad.c3d2.de
- Warning Message:** "This Connection is Untrusted".
- Icon:** A yellow icon of a person with a question mark.
- Description:** You have asked iceweasel to connect securely to pentapad.c3d2.de, but we can't confirm that your connection is secure.
- Note:** Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.
- Section:** **What Should I Do?**
- Description:** If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.
- Button:** Get me out of here!
- Section:** ▾ **Technical Details**
- Description:** pentapad.c3d2.de uses an invalid security certificate.
- Description:** The certificate is not trusted because no issuer chain was provided.
- Description:** (Error code: sec_error_unknown_issuer)
- Section:** ▶ **I Understand the Risks**

CCC
ooo

Datenschutz
oooooo

Kommunikation
oooooooo

Geräte
oooooooo

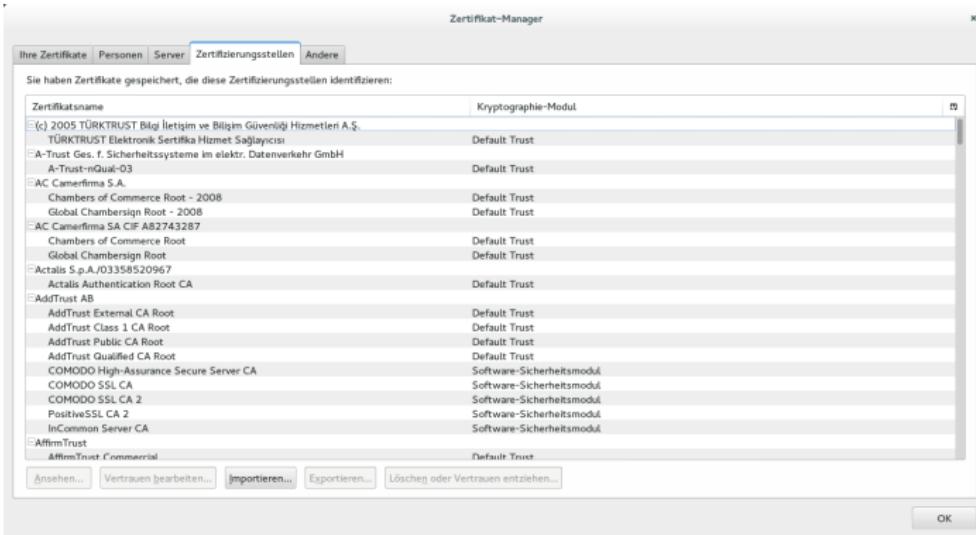
Verschlüsselung I
oooooooo●○

Anonymität
oooooooooooo

Unternehmen
oooooooooooo

Zertifizierungsstellen

Zertifizierungsstellen



HTTPS Everywhere

 ELECTRONIC FRONTIER FOUNDATION
DEFENDING YOUR RIGHTS IN THE DIGITAL WORLD

SEARCH

[HOME](#) [ABOUT](#) [OUR WORK](#) [DEEPLINKS BLOG](#) [PRESS ROOM](#) [TAKE ACTION](#) [SHOP](#)

 **HTTPS Everywhere**

[HTTPS Everywhere](#) [FAQ](#) [Report Bugs / Hack On The Code](#) [Creating HTTPS Everywhere Rulesets](#) [How to Deploy HTTPS Correctly](#)

HTTPS Everywhere is a Firefox, Chrome, and Opera extension that encrypts your communications with many major websites, making your browsing more secure. **Encrypt the web: Install HTTPS Everywhere today.**

[Install in Firefox Version 3 Stable](#) [Install in Chrome Beta Version](#) [Install in Opera Beta Version](#)

Donate to EFF 

Stay in Touch

Email Address
Postal Code (optional)
[SIGN UP NOW](#)

NSA Spying

 eff.org/nsa-spying

EFF is leading the fight against the NSA's illegal mass surveillance programs. Learn more about what the program is, how it works, and what you can do.

Vorratsdatenspeicherung (USA)



Home Über uns Kontakt Podcast Netzpolitik: TV Facebook Youtube Twitter RSS

VERMARKTET VON
ZEIT ONLINE

US-Geheimdienst NSA der geheimen Vorratsdatenspeicherung überführt

Von Markus Beckedahl | Veröffentlicht: 06.06.2013 um 7:51h | 1 Antwort

Was der US-Geheimdienst National Security Agency (NSA) alles überwacht, ist in der Regel Spekulation. Weil dieser im Geheimen agiert. Es wird vermutet, dass die NSA in einer Art Staubsauger sehr viele öffentlich im Netz fluktuierende Daten sammelt und speichert. Aber da die NSA im geheimen operiert, fällt es in der Regel schwer, etwas zu beweisen.

Der Journalist Glenn Greenwald schreibt im britischen Guardian über eine als geheim klassifizierte [Verordnung des Foreign Intelligence Surveillance Court \(FISC\)](#), die der Guardian auch veröffentlicht hat: [NSA collecting phone records of millions of Americans daily – revealed](#). In dieser wird der US-Provider Verizon angewiesen, eine Vorratsdatenspeicherung für drei Monate durchzuführen. Und zwar für lokale, nationale und ausländische Verbindungen mit allem, was dazu gehört. Es wird spekuliert, dass eine solche Verordnung regelmäßig erneuert und zudem nicht nur an Verizon verschickt wird.

Die Electronic Frontier Foundation (EFF) berichtet darüber: [Confirmed: The NSA is Spying on Millions of Americans](#).

Suchen

Suchtext eingeben

Über uns

netzpolitik.org ist ein Blog und eine politische Plattform für Freiheit und Offenheit im digitalen Zeitalter.

Blog abonnieren

[netzpolitik.org Blog Feed](#)

Spenden

netzpolitik.org produziert eine Reihe kostenloser Inhalte. Eine Spende erhält das Projekt am Leben und ermöglicht uns einen Ausbau der Redaktion.

[Unser Bank-Konto \(ohne Gebühren\)](#)

Inhaber: netzpolitik.org e. V.

Vorratsdatenspeicherung (Deutschland)

ARD Home Nachrichten Sport Börse Ratgeber Wissen Kultur Kinder ARD Intern Fernsehen Radio ARD Mediathek **ARD** 

Suche in tagesschau.de 

tagesschau.de

Startseite Videos & Audios Inland Ausland Wirtschaft Wahlarchiv Wetter Ihre Meinung Kontakt & Mehr



Nicht mit EU-Recht vereinbar

EuGH kippt Vorratsdatenspeicherung

Die Speicherung von Kommunikationsdaten ohne Verdacht auf Straftaten ist nicht mit EU-Recht vereinbar. Das hat der Europäische Gerichtshof (EuGH) in Luxemburg entschieden und damit die EU-Richtlinie zur Sicherung von Telefon- und E-Mail-Informationen gekippt. Die Richtlinie muss nun reformiert und die verdachtlose Speicherung von Verbindungsdaten von Telefon, Internet und E-Mails künftig "auf das absolut Notwendige beschränkt" werden.

Die Regelung "beinhaltet einen Eingriff von großem Ausmaß und besonderer Schwere in die Grundrechte auf Achtung des Privatlebens und auf den Schutz

VIDEO



Gigi Deppe, SWR, über das EuGH-Urteil zur Vorratsdatenspeicherung
tagesschau24 11:15 Uhr, 08.04.2014 | [video](#)

AUDIO

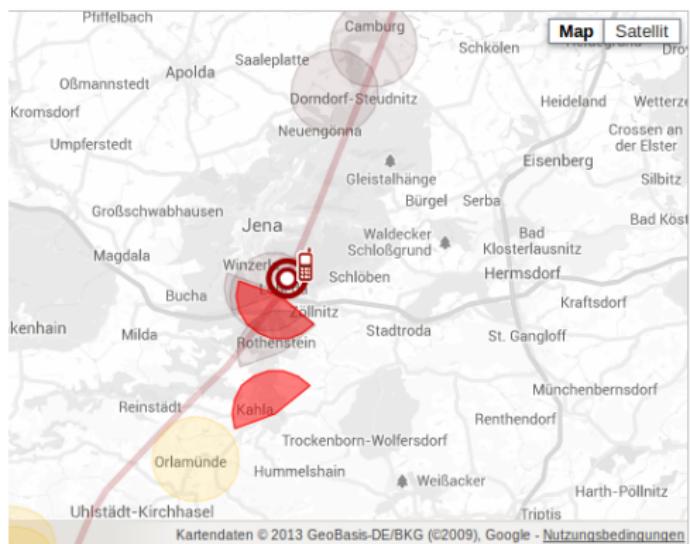
[EuGH kippt Vorratsdatenspeicherung - Reaktionen gespalten, Malte Pieper, ARD Berlin, 08.04.14 12:42 Uhr | audio](#)

LINKS

[Das EuGH-Urteil zur Vorratsdatenspeicherung \(pdf\)](#)



Metadaten



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



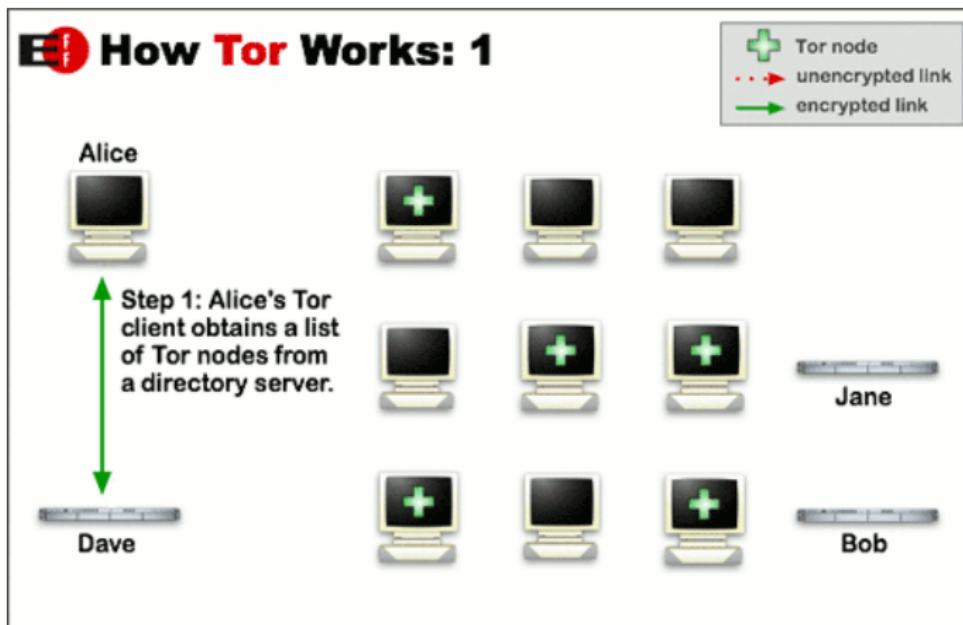
duration of internet connection:
21h 17min 25s



Download Data

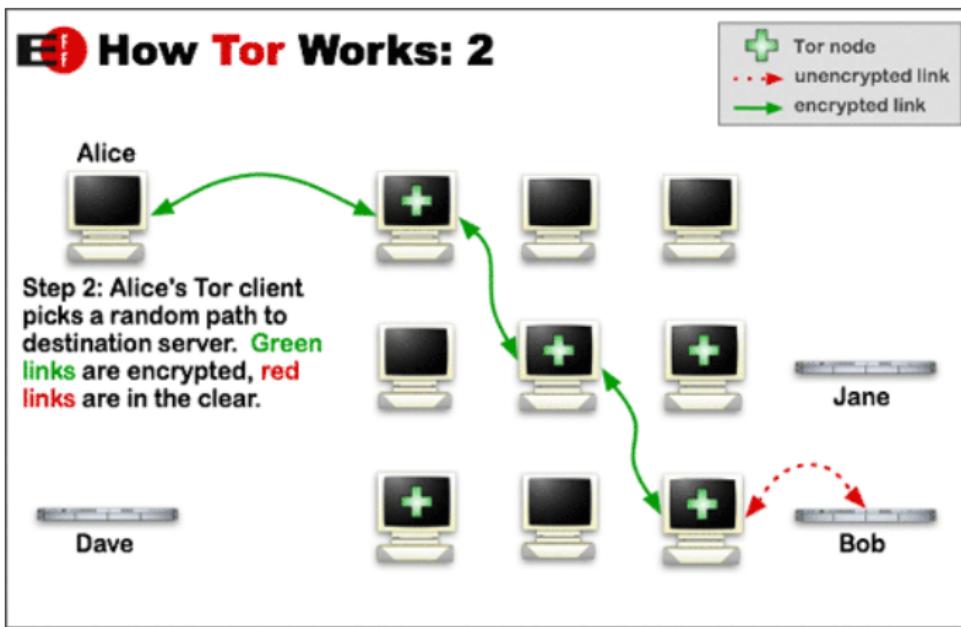


Tor



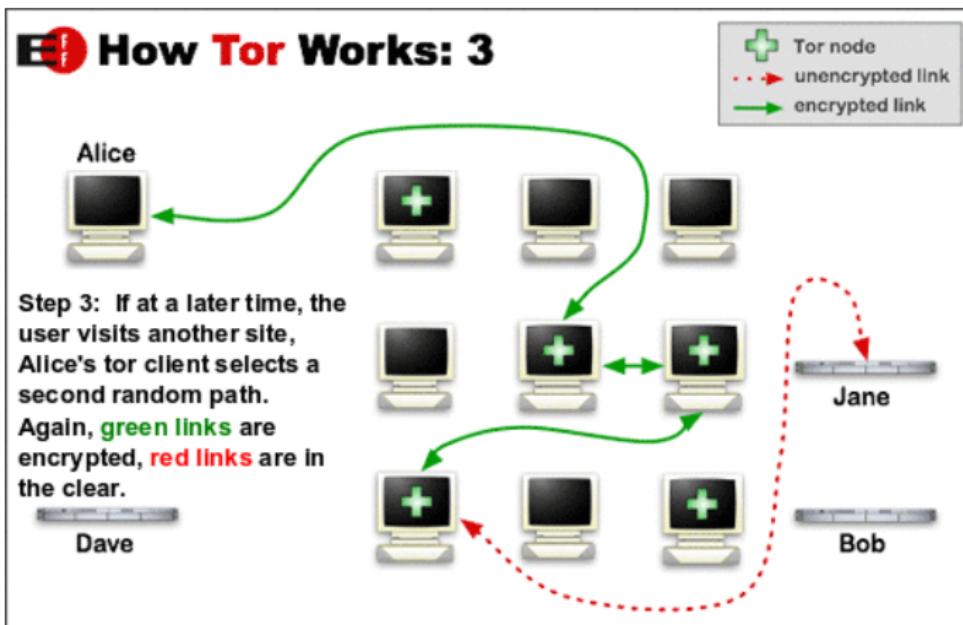
Grafik: The Tor Project

Tor



Grafik: The Tor Project

Tor



Grafik: The Tor Project

Tor

Anonymity Online

Protect your privacy. Defend yourself against network surveillance and traffic analysis.

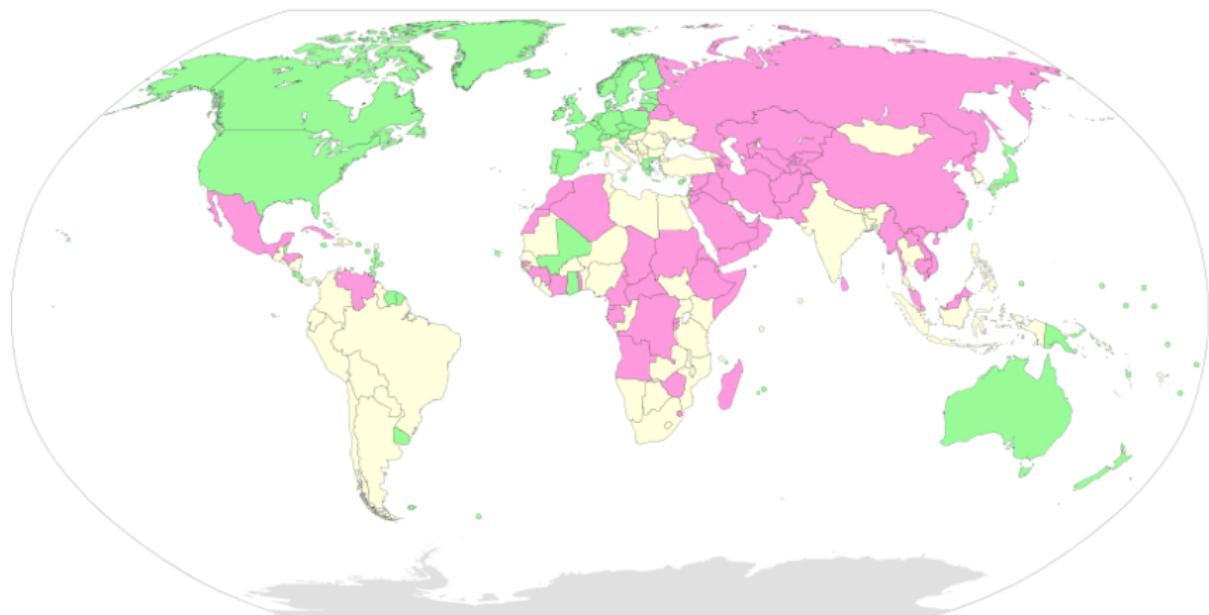


Download Tor

- ▶ Tor prevents people from learning your location or browsing habits.
- ▶ Tor is for web browsers, instant messaging clients, and more.
- ▶ Tor is free and open source for Windows, Mac, Linux/Unix, and Android



Zensur



Grafik: Jeff Ogden (W163)

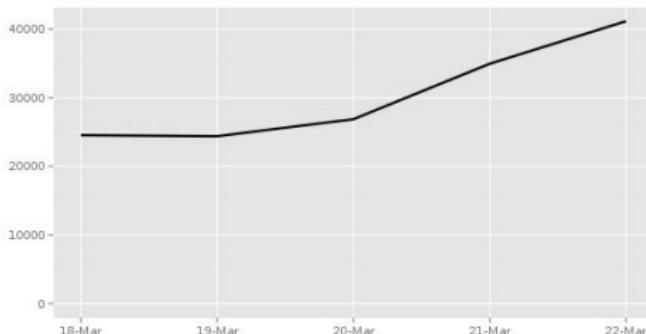
Tor in der Türkei



Tor Metrics Portal: Users

Direct users by country:

Directly connecting users from Turkey



Anonymität unter Vollüberwachung

p. 2

TOP SECRET//COMINT//REL FVEY

Tor Stinks...^[u]

- We will never be able to de-anonymize all Tor users all the time.
- With manual analysis we can de-anonymize a **very small fraction** of Tor users, however, **no** success de-anonymizing a user in response to a TOPI request/on demand.

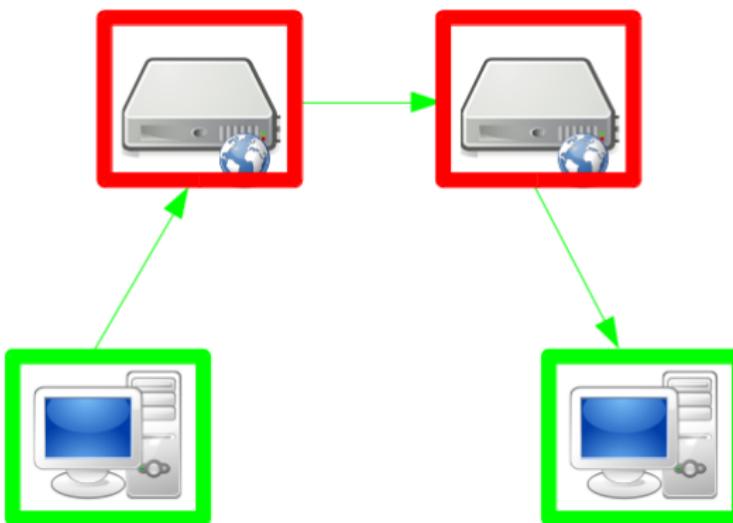
TOP SECRET//COMINT//REL FVEY



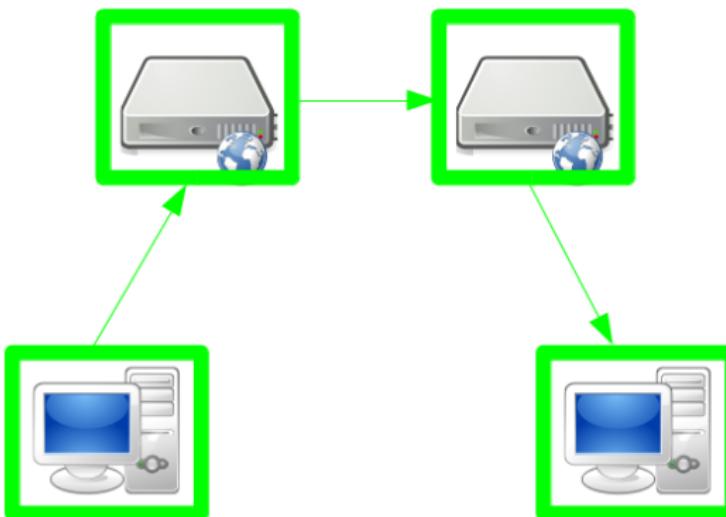
Zusammenfassung

- SSL nutzen (mit HTTPS Everywhere)
- Anonymität wahren (mit Tor)

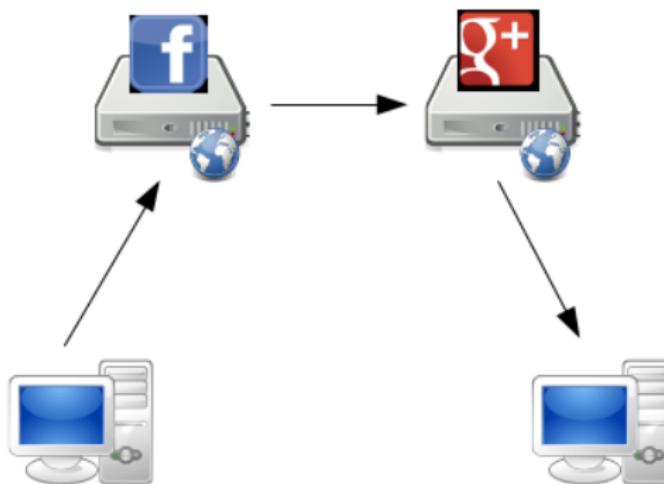
Was ist zu schützen?



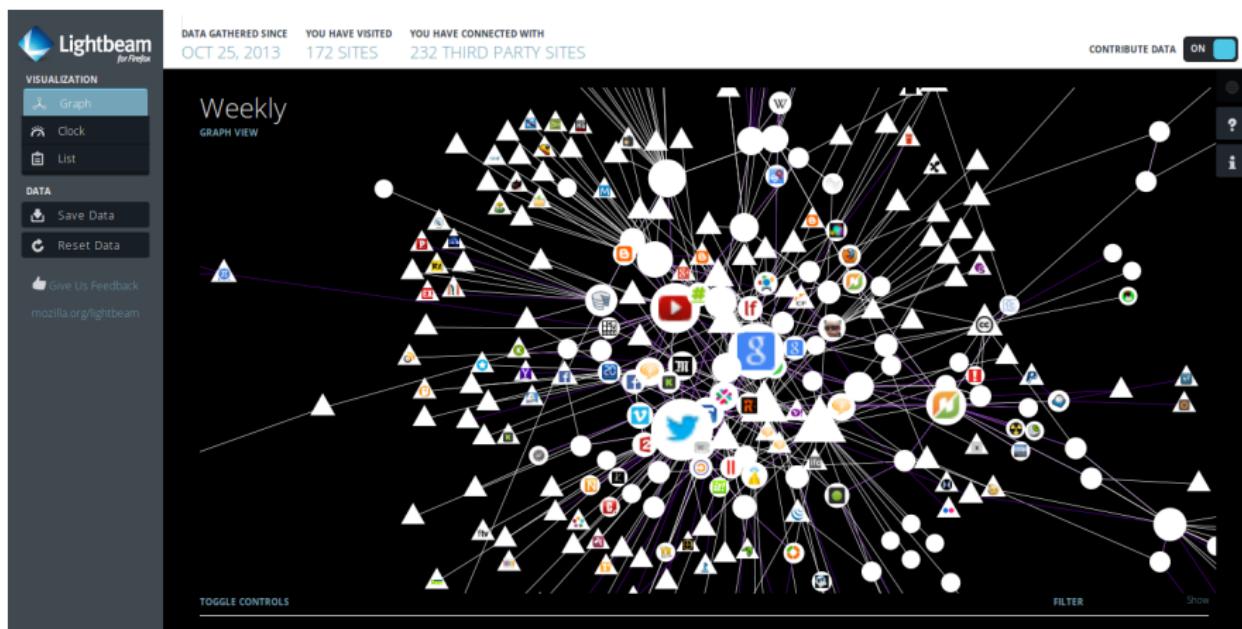
Was ist zu schützen?



Was ist zu schützen?



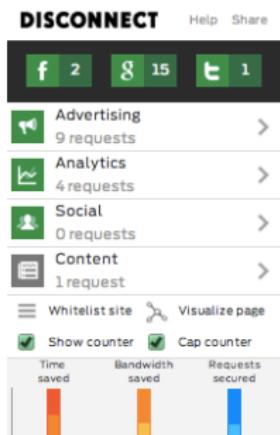
Metadaten - Lightbeam



Grafik: Clint Lalonde



Ich will etwas vom Server I



Disconnect.me

Ich will etwas vom Server II

Ich will etwas vom Server II

- Datensparsamkeit

Ich will etwas vom Server II

- Datensparsamkeit
- Werden echte Daten gebraucht?

Ich will etwas vom Server II

- Datensparsamkeit
- Werden echte Daten gebraucht?
 - Pseudonymität

Ich will etwas vom Server II

- Datensparsamkeit
- Werden echte Daten gebraucht?
 - Pseudonymität
 - mailinator.com (Wegwerf-Email-Adresse)

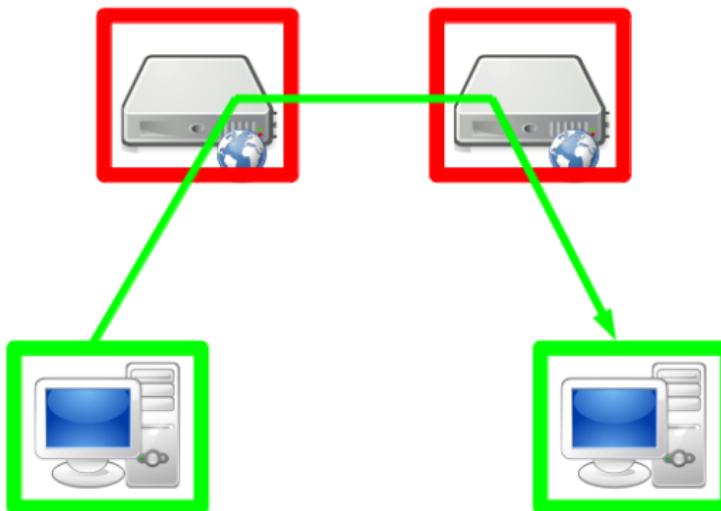
Ich will etwas vom Server II

- Datensparsamkeit
- Werden echte Daten gebraucht?
 - Pseudonymität
 - mailinator.com (Wegwerf-Email-Adresse)
 - frank-geht-ran.de (Wegwerf-Telefonnummer)

Ich will etwas vom Server II

- Datensparsamkeit
- Werden echte Daten gebraucht?
 - Pseudonymität
 - mailinator.com (Wegwerf-Email-Adresse)
 - frank-geht-ran.de (Wegwerf-Telefonnummer)
 - bugmenot.com (Fake Accounts)

Ich will etwas von einem anderen Nutzer



Ende-zu-Ende-Verschlüsselung I

- Email: GPG = Gnu Privacy Guard
- Thunderbird: Enigmail
- Outlook: Gpg4win
- Apple Mail: GPGTools
- Web: Mailvelope (Firefox, Chrome)

Ende-zu-Ende-Verschlüsselung II

Ende-zu-Ende-Verschlüsselung II

- OTR für Jabber:

- Pidgin mit OTR-Plugin für Linux und Windows
- GibberBot oder Xabber für Android
- Adium für Mac, ChatSecure für iOS

Ende-zu-Ende-Verschlüsselung II

- OTR für Jabber:
 - Pidgin mit OTR-Plugin für Linux und Windows
 - GibberBot oder Xabber für Android
 - Adium für Mac, ChatSecure für iOS
- palava.tv für Videotelefonie

Ende-zu-Ende-Verschlüsselung II

- OTR für Jabber:
 - Pidgin mit OTR-Plugin für Linux und Windows
 - GibberBot oder Xabber für Android
 - Adium für Mac, ChatSecure für iOS
- palava.tv für Videotelefonie
- Redphone für Handytelefone (Android)

Ende-zu-Ende-Verschlüsselung II

- OTR für Jabber:

- Pidgin mit OTR-Plugin für Linux und Windows
- GibberBot oder Xabber für Android
- Adium für Mac, ChatSecure für iOS
- palava.tv für Videotelefonie
- Redphone für Handytelefonate (Android)
- TextSecure für Nachrichten (Android)

Authentifizierung

Frage und Antwort

Frage und Antwort

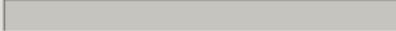
Gemeinsames Geheimnis

Fingerabdruck-Verifizierung

Stellen Sie eine Frage dessen Antwort nur Sie und thammi@debianforum.de kennen.

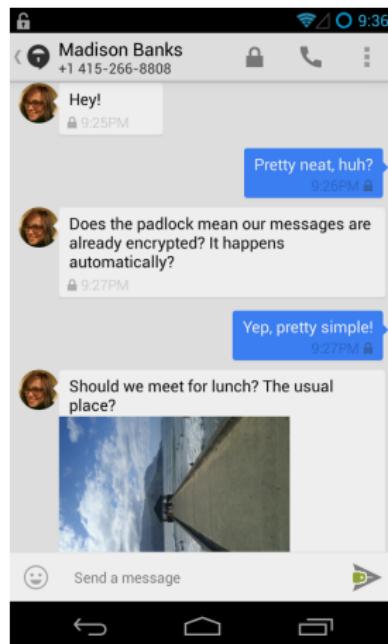
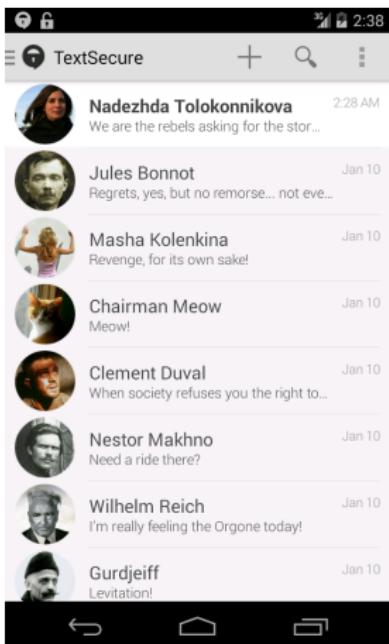
Frage:

Antwort:

 0%

[Abbrechen](#) [Authentifizieren](#)

TextSecure



Zusammenfassung

- Tracking-Daten loswerden mit Disconnect
- Datensparsamkeit / falsche Daten
- Ende-zu-Ende-Verschlüsselung

Diskussion

Diskussion

Folien:  Marius Melzer

Twitter: @faraoso, Email und Jabber: marius@rasumi.net
GPG-Fingerprint: 52DEFC3E

CMS Dresden: schule@c3d2.de