

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

Stefan Böcker, Martin Byrenheid, Marius Melzer  
Chaos Computer Club Dresden

20.05.2014

# 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



## NSA-Skandal



Grafik:  Laura Poitras / Praxis Films



# Tempora

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

**SPIEGEL ONLINE NETZWELT**

Login | Registrierung

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

Nachrichten > Netzwerk > Netzpolitik > Überwachung > Internetüberwachung: Tempora ist schlimmer als Prism

## Netz-Spähsystem Tempora: Der ganz große britische Bruder



Hehr als 200 Glasfaserkabel sollen die Briten angezapft haben

DPA/dpa/UKU/ingenitaucher.com

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

Samstag, 22.06.2013 - 20:24 Uhr

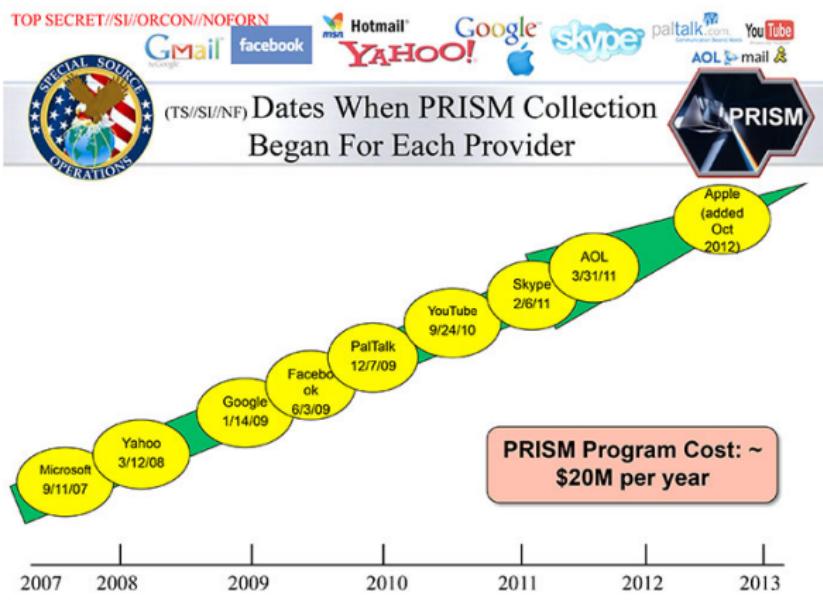
Drucken | Versenden | Merken

Nutzungsrechte | Feedback

Kommentieren | 389 Kommentare

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 Barack is watching you. Doch Brit Brother tut genau dies auch. Und in mancher Hinsicht scheint die Überwachung durch die britischen Netzsperne viel umfassender zu sein als die der Amerikaner.

# Prism



# 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.“

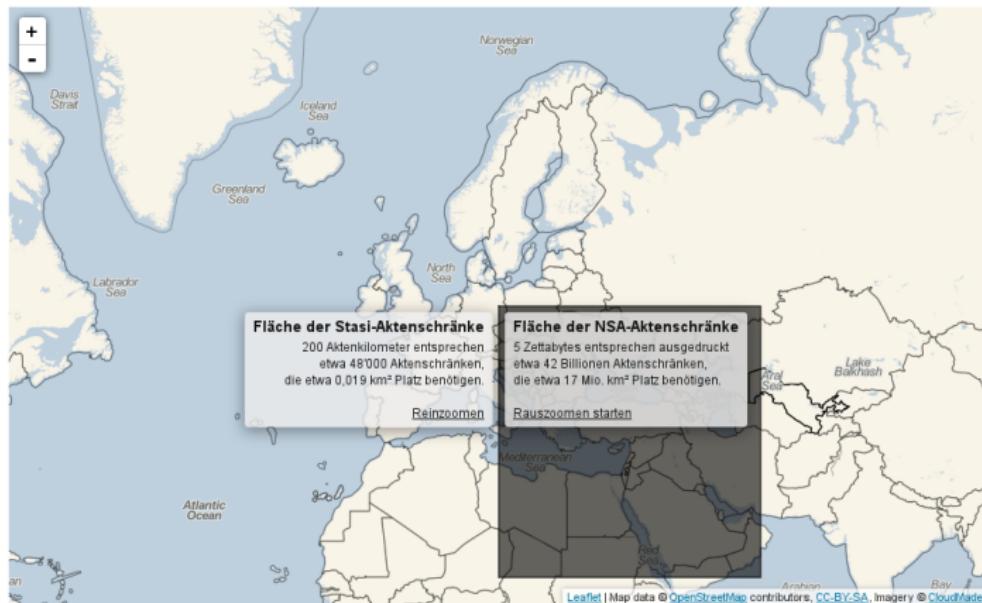
# Stasi vs. NSA



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](#)



Toptthemen: [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**



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 German

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

GröÙe Koalition setzt auf intelligente Stromzähler

[Videos bei heise online](#)



et zockt (Episode 23)

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



heise open

#### Zehn Jahre bei Fedor:

## Bei der Mitarbeit an einer Linux



# Metadaten

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

## Vorratsdatenspeicherung (USA)



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 als eine Art Staubauger 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 Saving 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

Spender

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 

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

 tagesschau.de

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

heise online > News > 2014 > KW 11 > Studie: Was auf Vorrat gespeicherte Verbindungsdaten verraten

14.03.2014 18:59



Anzeige

## Studie: Was auf Vorrat gespeicherte Verbindungsdaten verraten

[MP3 vorlesen / MP3-Download]

Stanford-Forscher haben mithilfe eines Crowdsourcing-Verfahrens von "Metadaten" aus der Telekommunikation relativ einfach sehr intime Details über Nutzer wie etwa deren potentielle Krankheiten herausfinden können.

Verbindungsdaten erlauben offenbar ziemlich umfassende Rückschlüsse auf die Personen, die sie verursachen, wie US-Wissenschaftler herausgefunden haben wollen. Sie seien selbst überrascht gewesen, welch tiefe Einblicke ihnen reine Verbindungsdaten gegeben hätten, schreibt ein Mitglied des wissenschaftlichen Teams in einem [Blogbeitrag](#).

Teilnehmer an der Untersuchung hätten Gespräche mit den Anonymen Alkoholikern, Waffengeschäften, Gewerkschaften, Scheidungsnichtern, auf Sexuaskrankheiten spezialisierte Kliniken oder etwa Strip-Cubs geführt. Bei den Erkenntnissen habe es sich nicht um eine "hypothetische Horrorparade" gehandelt, sondern um einfache Ableitungen aus dem Verhalten echter Telekommunikationsnutzer, halten die Forscher fest.

Für das [Projekt](#) haben Mitarbeiter des Center for Internet and Society der Stanford-Universität Nutzer von Android-Smartphones gebeten, über die [MetaPhone-App](#) ihre Verbindungsdaten beizusteuern. Über einen Abgleich mit 5000 aus dem so generierten Material zufällig ausgewählten Telefonnummern mit Yelp, Facebook und Google Places war es den Forschern bereits [Ende vergangenen Jahres gelungen](#),



Verbindungsdaten aus Telefongesprächen verraten offenbar mehr über eine Person als gedacht. (G)

Bild: dpa, Marc Müller

## Top-News

Fünfjähriger entdeckt Xbox-One-Backdoor  
Metro-Look im Auto: Microsoft verbindet Infotainment und Windows Phone  
Android-TV: Googles nächster Angriff auf den Fernseher  
Britische Regierung kauft 12 Monate XP-Support  
c't zeigt Auswege aus dem Router-Desaster



c't

### Das Router-Desaster

Unbeachtet in einer Ecke oder unter Ihrem Schreibtisch lauert eine Gefahr: der Router für Ihren Internet-Zugang. Ganoven nutzen dessen Sicherheitslücken aus, um Sie zu schädigen.



heise open

### Die Neuerungen von Linux 3.14

Neben einem weiteren Process-Scheduler bringt der neue Kernel eine Reihe von Performance-Optimierungen und Unterstützung für einige kürzlich vorgestellte Grafikkerne.

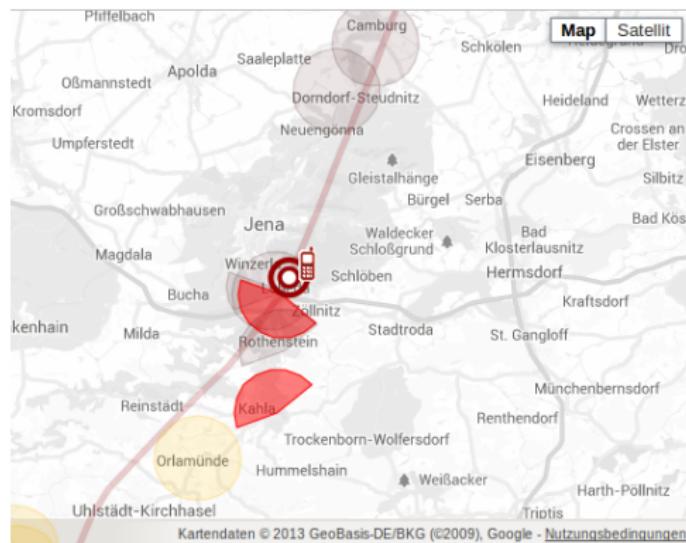


heise security

### Verwurmt, verphishst, verspamt

Echte Firmen-E-Mails sind kaum noch von Phishingmails zu unterscheiden. Täuschen sollten Kunden den Durchblick:

# 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



# Metadaten

golem.de  
IT-NEWS FÜR PROFIS

HOME TICKER

TOP-THEMEN: OnePlus Wearable Android NSA Apple Google mehr

Suchen

EX-NSA-CHEF HAYDEN

## "Wir töten Menschen auf Basis von Metadaten"

Der frühere NSA-Chef Michael Hayden ist für provokante Äußerungen bekannt. Nun bestätigte er freimütig, zu welchen Zwecken Verbindungsdaten genutzt werden können.

Der frühere US-Geheimdienstchef Michael Hayden hat bestätigt, was durch die Enthüllungen von Edward Snowden schon seit längerem diskutiert wird: "Wir töten Menschen auf der Basis von Metadaten", sagte Hayden vor einigen Wochen auf einer Diskussionsveranstaltung der John-Hopkins-Universität (ab Min. 18:00) in Baltimore. In der Debatte hatte ihm der Juraprofessor David Cole, der das Zitat nun bekanntmachte, vorgehalten, dass es alleine mit Verbindungsdaten möglich sei, über das Leben eines Menschen fast alles zu erfahren. Dies sei "absolut korrekt", sagte Hayden. Allerdings würden die Daten, die von US-Amerikanern gesammelt würden, nicht zum Töten von Menschen eingesetzt.



Ex-NSA-Chef Hayden räumt die Tötung von Menschen auf Basis von Metadaten ein. (Bild: Youtube.com/Screenshot: Golem.de)

Datum: 12.5.2014, 13:37

Autor: Friedhelm Greis

Themen: Datenschutz, Edward Snowden, NSA, Prism, Spionage, Verschlüsselung, Whistleblower, Überwachung, Internet, Politik/Recht

Teilen:



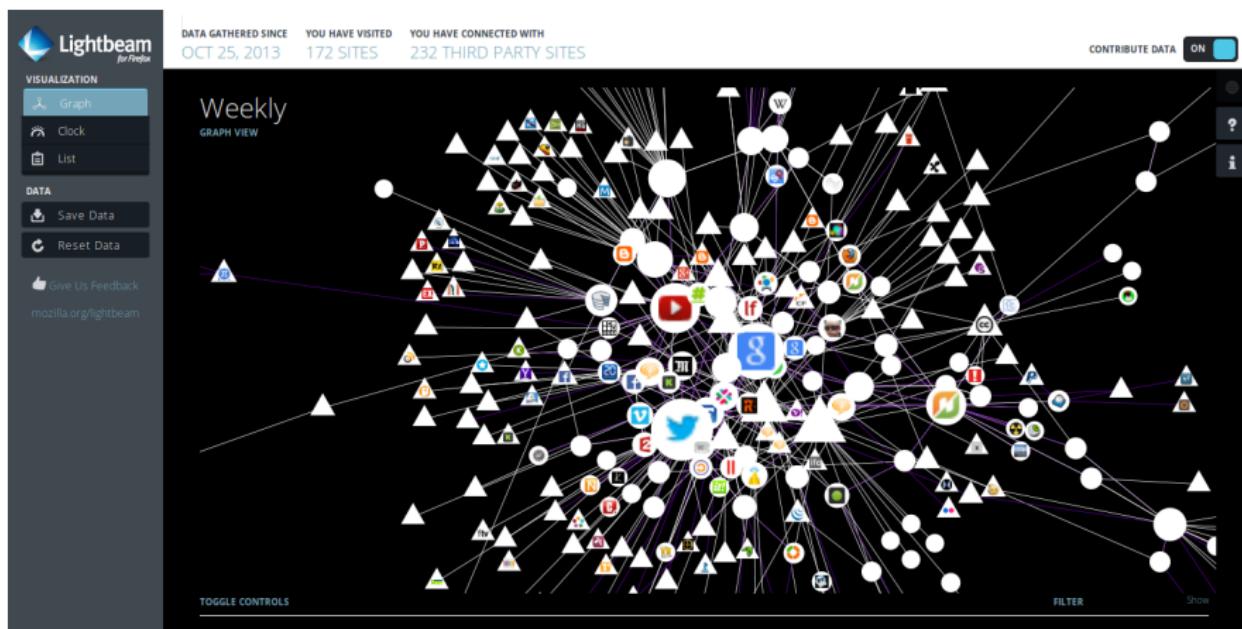
CCC  
000

NSA  
0000000

## Metadaten

## Inhalte

# Metadaten - Lightbeam



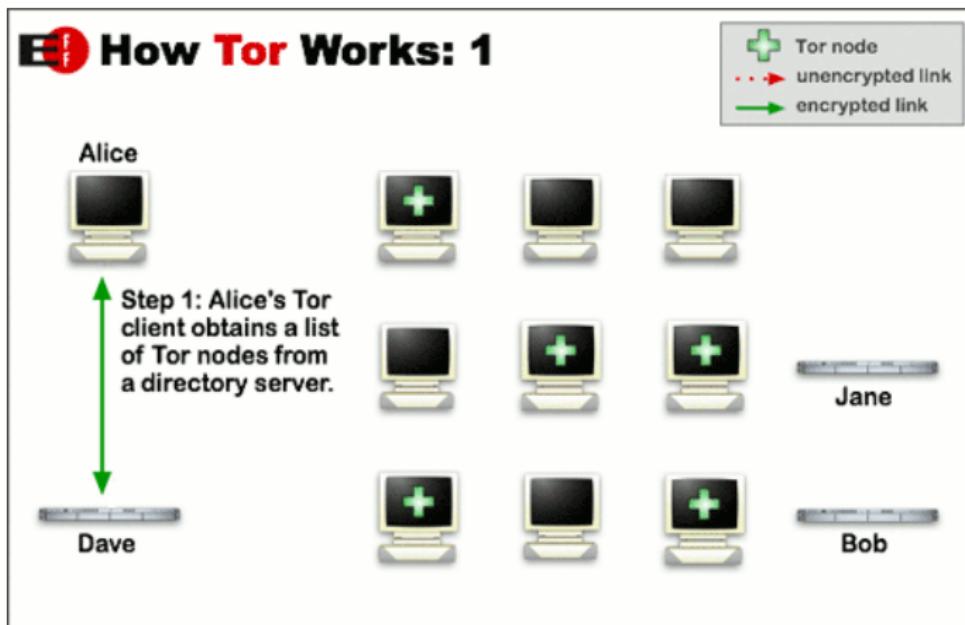
Grafik:  Clint Lalonde



# Metadaten - Disconnect

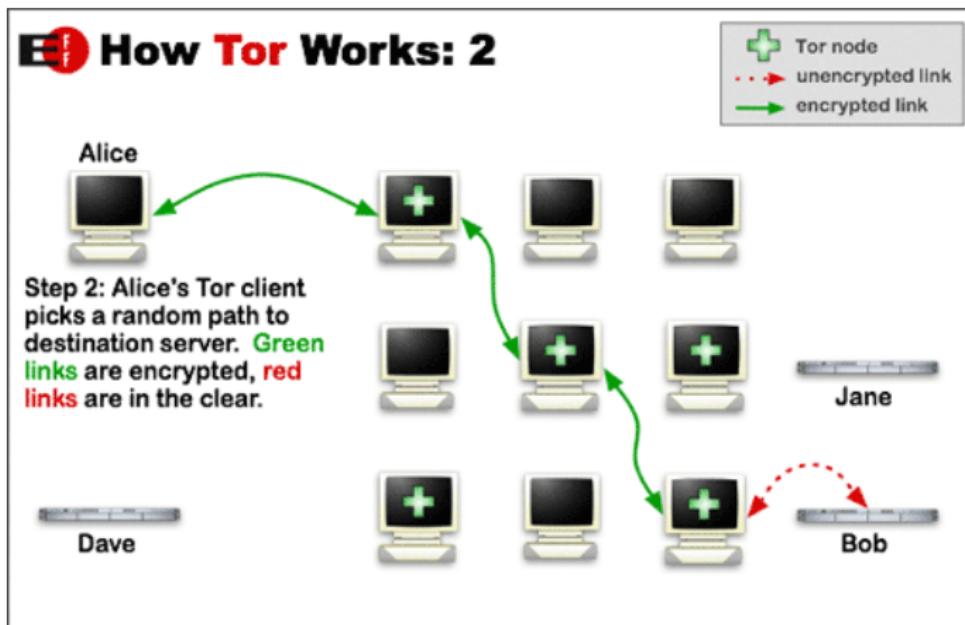


# Tor



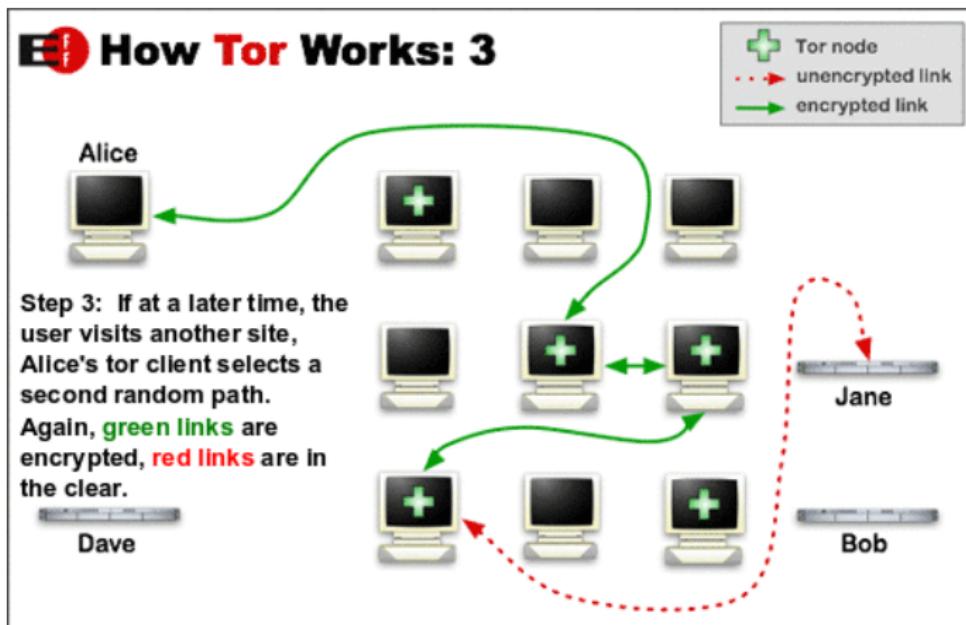
Grafik: The Tor Project

## 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



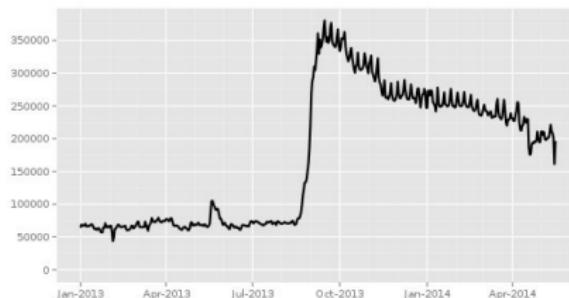
# Tor in Deutschland



## Tor Metrics Portal: Users

### Direct users by country:

Directly connecting users from Germany



The Tor Project - <https://metrics.torproject.org/>

Start date (yyyy-mm-dd):  End date (yyyy-mm-dd):

Source:

# Anonymität unter Vollüberwachung

p. 2

TOP SECRET//COMINT//REL FVEY

## Tor Stinks...<sup>[u]</sup>

- 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



# Datensparsamkeit

- Viele Daten zusammen ergeben Profile
- Werden die Daten gebraucht?
- Werden echte Daten gebraucht?
  - Pseudonymität
  - mailinator.com (Wegwerf-Email-Adresse)
  - frank-geht-ran.de (Wegwerf-Telefonnummer)
  - bugmenot.com (Fake Accounts)

# Verschlüsselung: Analogie



Grafik: Ronald Preuss

CCC  
ooo

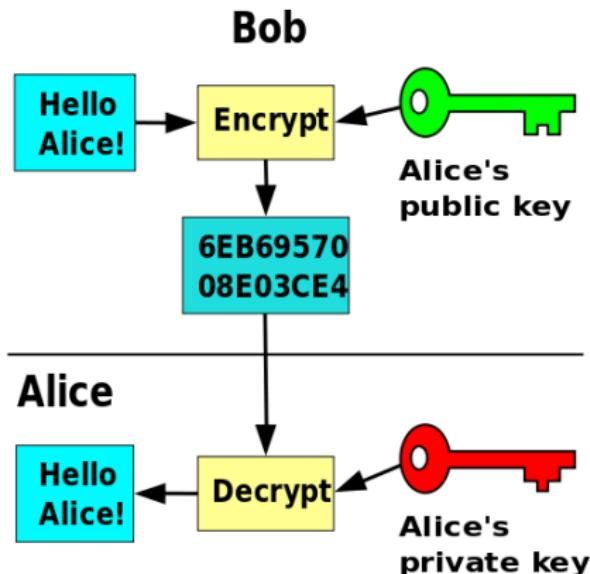
NSA  
oooooooo

Metadaten  
oooooooooooo

Inhalte  
o●oooooooooooo

# Verschlüsselung: Asymmetrische

# Verschlüsselung: Asymmetrische



CCC  
000

NSA  
0000000

## Metadaten

## Inhalte

## SSL / TLS

## SSL / TLS

- SSL = Secure Socket Layer

# SSL / TLS

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

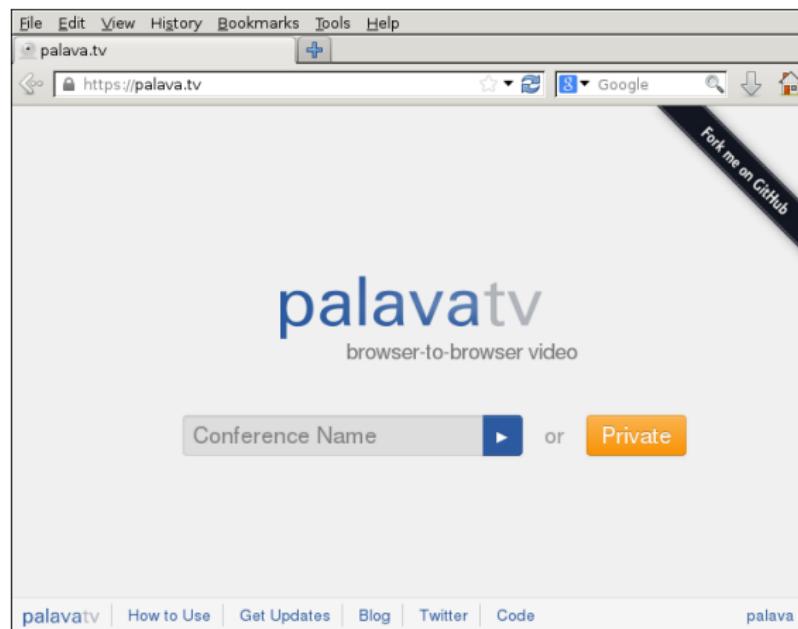
CCC  
ooo

NSA  
oooooooo

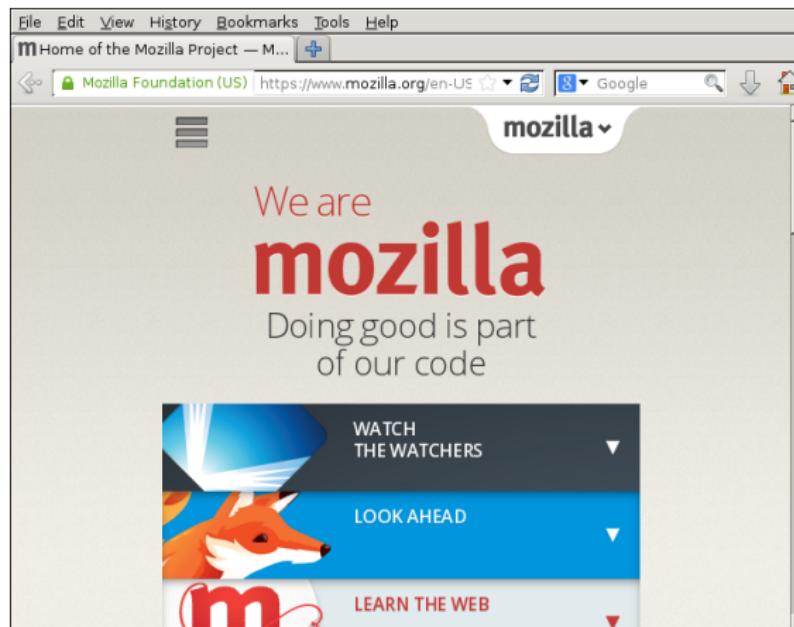
Metadaten  
oooooooooooo

Inhalte  
oooo●oooooooooooo

# SSL im Browser



# SSL im Browser



# SSL im Browser

File Edit View History Bookmarks Tools Help

⚠ Untrusted Connection 

  https://pentapad.c3d2.de    Google  

 **This Connection is Untrusted**

You have asked Iceweasel to connect securely to **pentapad.c3d2.de**, but we can't confirm that your connection is secure.

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.

**What Should I Do?**

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.

[Get me out of here!](#)

▼ **Technical Details**

pentapad.c3d2.de uses an invalid security certificate.

The certificate is not trusted because no issuer chain was provided.  
(Error code: sec\_error\_unknown\_issuer)

► **I Understand the Risks**

CCC  
ooo

NSA  
oooooooo

Metadaten  
oooooooooooo

Inhalte  
oooooooo●oooooooo

# Zertifizierungsstellen

# Zertifizierungsstellen

Zertifikat-Manager

Ihre Zertifikate Personen Server Zertifizierungsstellen Andere

Sie haben Zertifikate gespeichert, die diese Zertifizierungsstellen identifizieren:

Zertifikatsname	Kryptographie-Modul
(c) 2005 TÜRKİSTAN BİLGİ İletişim ve Bilişim Güvenliği Hizmetleri A.Ş.	Default Trust
TÜRKTRUST Elektronik Sertifika Hizmet Sağlayıcısı	Default Trust
A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH	Default Trust
A-Trust+Qual-03	Default Trust
AC Camerfirma S.A.	Default Trust
Chambers of Commerce Root - 2008	Default Trust
Global Chambersign Root - 2008	Default Trust
AC Camerfirma SA CIF A82743287	Default Trust
Chambers of Commerce Root	Default Trust
Global Chambersign Root	Default Trust
Actalis S.p.A./03358520967	Default Trust
Actalis Authentication Root CA	Default Trust
AddTrust AB	Default Trust
AddTrust External CA Root	Default Trust
AddTrust Class 1 CA Root	Default Trust
AddTrust Public CA Root	Default Trust
AddTrust Qualified CA Root	Default Trust
COMODO High-Assurance Secure Server CA	Software-Sicherheitsmodul
COMODO SSL CA	Software-Sicherheitsmodul
COMODO SSL CA 2	Software-Sicherheitsmodul
PositiveSSL CA 2	Software-Sicherheitsmodul
InCommon Server CA	Software-Sicherheitsmodul
AffirmTrust	Default Trust
AffirmTrust Commercial	Default Trust

Ansehen... Vertrauen bearbeiten... Importieren... Exportieren... Löschen oder Vertrauen entziehen...

OK

# 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.

# E-Mail Verschlüsselung



- GNU Privacy Guard
- Verschlüsselungssoftware für Texte und Dateien
- Windows: **GPG4Win** - <http://www.gpg4win.org/>
- Mac OS X: **MacGPG** - <https://gpgtools.org/>
- Android: **APG**

CCC  
ooo

NSA  
oooooooo

Metadaten  
oooooooooooo

Inhalte  
oooooooo●oooo

# E-Mail Verschlüsselung auf dem PC

Mozilla  
Thunderbird mit  
Enigmail-Plugin



# E-Mail Verschlüsselung auf dem PC

Mozilla Firefox  
mit Mailvelope-  
Plugin



CCC  
ooo

NSA  
oooooooo

Metadaten  
oooooooooooo

Inhalte  
oooooooooooo●ooo

# 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

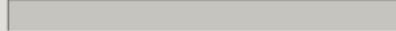
Gemeinsames Geheimnis

Fingerabdruck-Verifizierung

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

Frage:

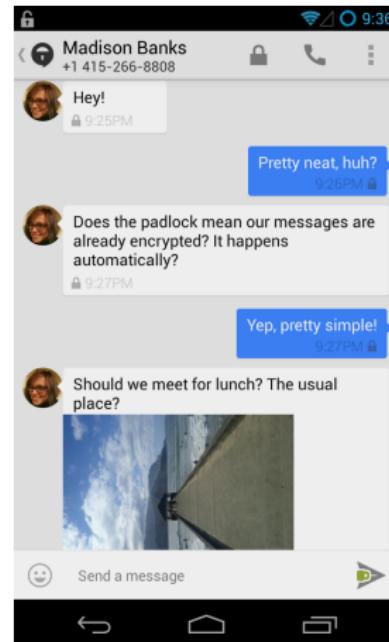
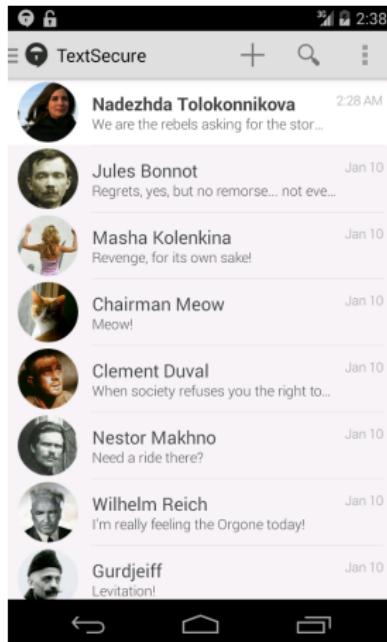
Antwort:

 0%

Abbrechen Authentifizieren



# TextSecure



# Diskussion

## Diskussion

Folien:  Chaos Computer Club Dresden

CMS Dresden: schule@c3d2.de