

Tor

Anonym surfen

Kire

Swiss Privacy Foundation

Inhaltsverzeichnis

- ▶ Browser-Spuren - technisch und rechtlich
- ▶ Tor - der Zwiebelrouter
 - ▶ Übersicht
 - ▶ Client installieren
 - ▶ Tor Browser Bundle
 - ▶ Anleitungen für viele andere Programme
 - ▶ Hidden Services
 - ▶ Tor-Serverknoten
- ▶ Schluss

Browser-Spuren - technisch und rechtlich

Server-Logfiles

- ▶ Webserver
 - ▶ IP-Adresse, Browser, Betriebssystem, Referrer, Datum
- ▶ Mailserver
- ▶ Nameserver (DNS)

Aufbewahrungspflicht der IP-Zuordnungen

- ▶ CH: 6 Monate durch Provider
- ▶ EU: 6 - 24 Monate

Browser-Spuren - technisch und rechtlich

Eindeutige Merkmale

- ▶ MAC-Adresse
- ▶ „Einwahl“
- ▶ Cookies & IDs

Lokaler Computer

- ▶ Cache & Browser-History

Genauere Informationen und täglicher Umgang

- ▶ <http://www.privacyfoundation.ch/de/service/browserspuren.html>


Tor - der Zwiebelrouter

Übersicht

- ▶ Anonymisierendes Netzwerk
- ▶ 8 Vollzeitentwickler
- ▶ Opensource
- ▶ Vorkompiliert für Windows, Mac OS X, Linux, *BSD
- ▶ Fixfertige Browser Bundles für Windows, Mac OS X, Linux
- ▶ Client wählt Route über drei Server
- ▶ Peer-to-Peer-Netz: über 2'000 Server & über 300 MB/s Exit-Traffic
- ▶ Verschlüsselung bis zum Exit-Node
- ▶ Hidden Services für anonyme Webserver

Wie Tor funktioniert: 1

Legend:

-  Torknoten
-  unverschlüsselte Verbindung
-  verschlüsselte Verbindung



E! Wie Tor funktioniert: 2

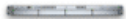
+

•••➔

➔

Torknoten
unverschlüsselte
Verbindung
verschlüsselte
Verbindung

Alice



Schritt 2: Der Torclient von Alice wählt einen zufälligen Pfad zum Zielserver.
Grüne Verbindungen sind verschlüsselt, rote Verbindungen nicht.



Dave

Jane

Bob

E! Wie Tor funktioniert: 3



Alice



Schritt 3: Wenn der Nutzer auf eine andere Seite zugreifen möchte, wählt der Torclient von Alice einen zweiten zufälligen Pfad. Wiederum sind **grüne Verbindungen** verschlüsselt und **rote** nicht.

Dave



Jane



Bob

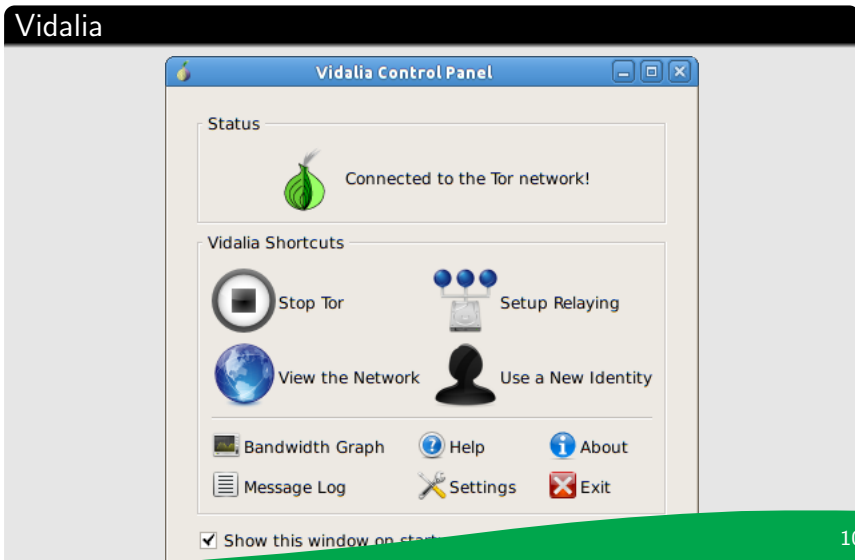


Client installieren

Tor Browser Bundle

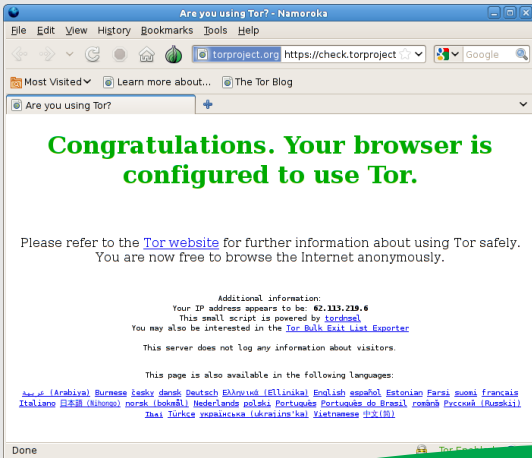
- ▶ Fixfertiges Paket mit
 - ▶ Tor
 - ▶ Vidalia (grafische Benutzeroberfläche)
 - ▶ Polipo (lokaler Proxy)
 - ▶ Firefox
 - ▶ Torbutton
- ▶ `https://www.torproject.org/projects/torbrowser.html.en`
- ▶ Entpacken und mit „Start Tor Browser“ aufrufen

Tor Browser Bundle



Tor Browser Bundle

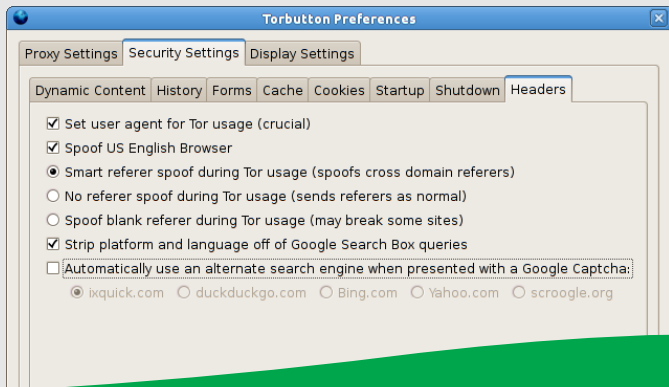
Vidalia



Tor Browser Bundle

Torbutton Feintuning

- ▶ „Automatically use an alternate search engine when presented with a Google Captcha“ ausschalten
 - ▶ Oder z.B. etools.ch verwenden



Tor Browser Bundle

Firefox Feintuning

- ▶ Nur mit aktiviertem Tor-Button verwenden
 - ▶ Cookies, JavaScript etc. werden gemäss aktuellen Einstellungen nur im aktivierten Modus geblockt
- ▶ Suchmaschinen nach Gusto hinzufügen
- ▶ Auch Extensions
 - ▶ Tab Mix Plus
 - ▶ Adblock Plus
- ▶ jedoch **nicht**
 - ▶ User Agent Switcher
 - ▶ RefControl
 - ▶ QuickJava
 - ▶ Flashblock

Weitere Anwendungen

Anleitungen für viele andere Programme

- ▶ <https://wiki.torproject.org/noreply/TheOnionRouter/TorifyHOWTO>
 - ▶ SSH
 - ▶ Pidgin
 - ▶ Fetchmail
 - ▶ FileZilla

Hidden Services

- ▶ Tor-Netzwerk mit Webserver verknüpfen
- ▶ Kommunikation über Rendezvous-Punkt
- ▶ sehr langsam

Tor-Serverknoten

- ▶ Exit-Node nicht zuhause betreiben
- ▶ Entry-, Middle-Nodes und Bridges schon
- ▶ Root-Server
 - ▶ AMD Opteron 2.0 GHz, 1 GB RAM
 - ▶ 6 TB Daten/Monat, 24 Mbit/s
 - ▶ CHF 1000.-/Jahr
- ▶ Zusammenschluss von Administratoren
 - ▶ German/Swiss Privacy Foundation
 - ▶ 8 Tor-, 6 DNS- & 2 I2P-Server, PrivacyBox etc.
- ▶ Oder Spenden an
 - ▶ The Tor Project, CCC, FoeBuD

Danke fürs Mitmachen!

Slides

Die Slides werden unter <http://www.privacyfoundation.ch/> zum Download angeboten.

Lizenz



<http://creativecommons.org/licenses/by-sa/2.5/ch/deed.de>

Kontakt

Anregungen werden gerne per Mail entgegen genommen.
<http://www.privacyfoundation.ch/de/kontakt.html>