

Anonym surfen

Kire

Swiss Privacy Foundation
www.privacyfoundation.ch

Swiss Privacy Foundation

Der gemeinnützige Verein Swiss Privacy Foundation setzt sich für den Schutz der digitalen Privatsphäre, für Meinungs- und Versammlungsfreiheit und den ungehinderten Informationszugang ein.

Dazu werden praxisorientierte Workshops, Anleitungen und entsprechende Dienste zur freien Nutzung angeboten.

Inhaltsverzeichnis

- ▶ Browser-Spuren - technisch und rechtlich
- ▶ Anonymität im Netz
- ▶ Tor - der Zwiebelrouter
 - ▶ Übersicht
 - ▶ Client installieren
 - ▶ Tor Browser Bundle
 - ▶ Weitere Anwendungen
 - ▶ Tor Hidden Services
 - ▶ Tor Server
- ▶ 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

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

Lokaler Computer

- ▶ Cache & Browser-History

Genauere Informationen und täglicher Umgang

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

Anonymität im Netz

Anonymisierendes Netzwerk

- ▶ Via Proxy (Stellvertreter)
- ▶ Betreiber darf Anonymität nicht aufheben können
 - ▶ Verwendung von Kaskaden
- ▶ Alle Ebenen müssen berücksichtigt sein
 - ▶ Netzwerk-Verbindungen
 - ▶ Applikation
 - ▶ DNS
- ▶ Tor, JonDonym, I2P

Tor - der Zwiebelrouter

Übersicht

- ▶ Opensource-Projekt
- ▶ Spendenfinanziert
- ▶ 8 Vollzeitentwickler
- ▶ Vorkompiliert für Windows, Mac OS X, Linux, *BSD, Android
- ▶ Fixfertige Browser Bundles
- ▶ Über 2'000 Server & über 300 MB/s Exit-Traffic
- ▶ Komplette verschlüsselt (bis zum Exit-Node!)

Wie Tor funktioniert: 1



Wie Tor funktioniert: 2

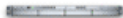


Alice



Schritt 2: Der Torclient von Alice wählt einen zufälligen Pfad zum Zielserver.

Grüne Verbindungen sind verschlüsselt, rote Verbindungen nicht.



Dave



Jane



Bob

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)
 - ▶ Firefox
 - ▶ Torbutton
- ▶ `https://www.torproject.org/projects/torbrowser.html.en`
- ▶ Entpacken und mit „Start Tor Browser“ aufrufen

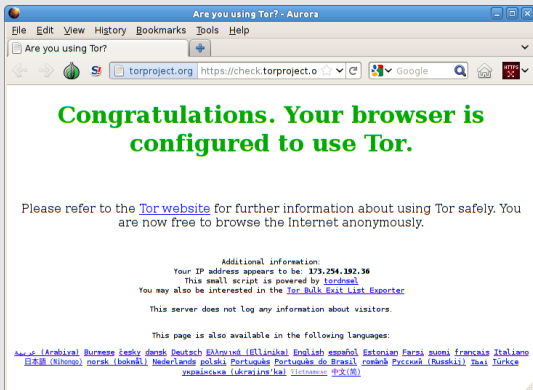
Tor Browser Bundle

Vidalia



Tor Browser Bundle

Firefox

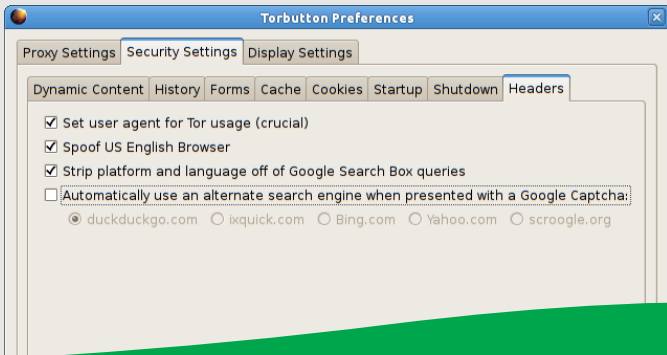


The screenshot shows a Firefox browser window titled "Are you using Tor? - Aurora". The address bar displays "torproject.org" and "https://check.torproject.o". The main content area features a large green heading: "Congratulations. Your browser is configured to use Tor." Below this, a paragraph reads: "Please refer to the [Tor website](#) for further information about using Tor safely. You are now free to browse the Internet anonymously." Further down, it provides "Additional information:" including the IP address "173.254.192.36", a note that the script is powered by "torndns", and a link to "Tor Bulk Exit List Exporter". It also states "This server does not log any information about visitors." At the bottom, it lists available languages: العربية (Arabic), Бурмese тeкyи, deutsch, ελληνικά (Greek), English, español (Spanish), Estonian, Eesti keel, suomi (Finnish), français (French), Italiano, 日本語 (Japanese), norsk (Norwegian), norsk (bokmål) (Norwegian Bokmål), Nederlands, polski (Polish), Português, Português do Brasil (Portuguese Brazilian), română (Romanian), Pусский (Russian), Thai, Türkçe, українська (Ukrainian), and 中文 (Chinese).

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
 - ▶ (Super-)Cookies, JavaScript etc. werden gemäss aktuellen Einstellungen nur im aktivierten Modus geblockt
- ▶ Suchmaschinen nach Gusto hinzufügen
- ▶ Auch Extensions
 - ▶ RefControl
 - ▶ Tab Mix Plus
 - ▶ Adblock Plus
- ▶ jedoch **nicht**
 - ▶ User Agent Switcher
 - ▶ QuickJava
 - ▶ Flashblock

Weitere Anwendungen

Voraussetzung

- ▶ Tor-Client installieren („Expert“ Bundle)
 - ▶ `https://www.torproject.org/download/download.html.en`
- ▶ Stellt Tor via lokalen SOCKS-Proxy zur Verfügung
 - ▶ Host 127.0.0.1, Port 9050
- ▶ Vorsicht bei der Verwendung von Hostnamen
- ▶ Anleitungen für viele Programme
 - ▶ `https://wiki.torproject.org/noreply/TheOnionRouter/TorifyHOWTO`

Weitere Anwendungen

SSH

- ▶ `torify ssh [parameter] $(tor-resolve [host])`

Pidgin

- ▶ SOCKS-Proxy in den Einstellungen hinterlegen
- ▶ Sicherheitshalber per IP-Adresse verbinden

FileZilla

- ▶ Generic-Proxy (SOCKS 5, Host/Port) hinterlegen

Fetchmail

- ▶ `torify fetchmail -p pop3 -P 995 --ssl --sslcommonname
privacybox.de -u kire 94.75.228.20`

Tor Hidden Services

Zensurresistent publizieren

- ▶ Tor-Netzwerk mit z.B. Webserver verknüpfen
- ▶ Kommunikation über Rendezvous-Punkt
- ▶ Beide Kommunikations-Partner sind unbekannt
- ▶ Braucht etwas Geduld

Tor Server

Selber zum Netz beitragen

- ▶ Exit-Node nicht zuhause betreiben
- ▶ Entry-, Middle-Nodes und Bridges schon
 - ▶ IP-Adresse sollte nicht täglich wechseln
- ▶ Root-Server
 - ▶ Intel P4 3.0 GHz (2 Cores), 2 GB RAM
 - ▶ 10 TB Daten/Monat, 40 Mbit/s FD
- ▶ Zusammenschluss von Administratoren
 - ▶ German/Swiss Privacy Foundation
 - ▶ 8 Tor-, 5 DNS- & 1 I2P-Server, PrivacyBox etc.
- ▶ Das Netzwerk lebt von Deiner Spende

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>