

# Tor

Anonym surfen

Kire

Swiss Privacy Foundation

# Inhaltsverzeichnis

- ▶ Browser-Spuren - technisch und rechtlich
- ▶ Tor - der Zwiebelrouter
  - ▶ Übersicht
  - ▶ Client installieren und konfigurieren
  - ▶ Ubuntu Linux
  - ▶ Firefox
  - ▶ 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/service/browserspuren.html>



# Tor - der Zwiebelrouter

## Übersicht

- ▶ Anonymisierendes Netzwerk
- ▶ 8 Vollzeitentwickler
- ▶ Opensource
- ▶ Vorkompiliert für Windows, Mac OS X, Linux, \*BSD
- ▶ Client wählt Route über drei Server
- ▶ Peer-to-Peer-Netz: über 1'500 Server & über 300 MB/s
- ▶ Verschlüsselung bis zum Exit-Node
- ▶ Hidden Services für anonyme Webserver

# Wie Tor funktioniert: 1

Legend:

-  Torknoten
-  unverschlüsselte Verbindung
-  verschlüsselte Verbindung



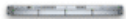
## **E!** Wie Tor funktioniert: 2

+

•••→ unverschlüsselte Verbindung

→ verschlüsselte Verbindung

Alice



Jane



Bob

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

Grüne Verbindungen sind verschlüsselt, rote Verbindungen nicht.



Dave

## **E!** Wie Tor funktioniert: 3



Alice



Jane



Bob

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

# Client installieren und konfigurieren

## Windows

- ▶ Installations-Paket mit
  - ▶ Tor
  - ▶ Vidalia (grafische Benutzeroberfläche)
- ▶ Oder allenfalls installationsfreie Version; zusätzlich mit
  - ▶ Firefox
  - ▶ Torbutton
- ▶ <https://www.torproject.org/easy-download.html>

## Mac OS X

- ▶ Installations-Paket
  - ▶ Analog Windows

# Ubuntu Linux

## Tor-Repository hinzufügen

- ▶ Synaptic Package Manager
  - ▶ Menü Settings - Repositories
  - ▶ Tab "Other Software" - Add
  - ▶ `deb http://deb.torproject.org/torproject.org karmic main`
    - ▶ karmic passt für 9.10 und 10.04
- ▶ Im Terminal (auch je eine Zeile)
  - ▶ `gpg --keyserver keys.gnupg.net --recv 886DDD89`
  - ▶ `gpg --export A3C4F0F979CAA22CDBA8F512EE8CBC9E886DDD89 | sudo apt-key add -`

## Per Synaptic installieren: Tor

- ▶ benötigt polipo, socat, tor-geoipdb und tsocks

# Firefox

## ProfileSwitcher Extension

- ▶ Installieren und konfigurieren
  - ▶ <https://nic-nac-project.org/~kaosmos/profileswitcher-en.html>
  - ▶ Menü File - Open Profile Manager - No
  - ▶ Create Profile - Next - "Tor" - Finish



# Firefox

## ProfileSwitcher Extension II

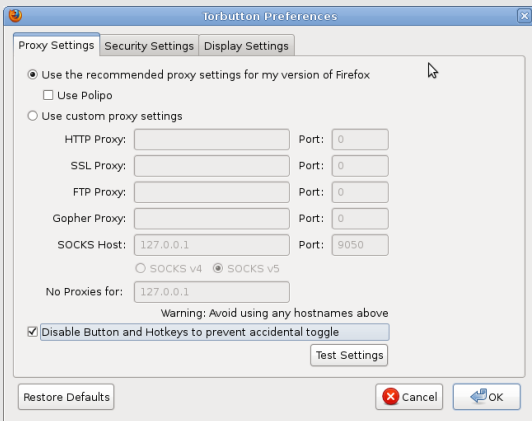
- ▶ Rechte Maustaste auf Profile Manager unten rechts
  - ▶ Launch another Profile - Refresh list - Tor - No
- ▶ Im Profil "Tor" können nun vom täglichen Surfen getrennte Einstellungen vorgenommen werden
  - ▶ ProfileSwitcher Extension auch in diesem Profil installieren...

## Torbutton Extension

- ▶ Installieren und konfigurieren
  - ▶ <https://www.torproject.org/torbutton/index.html>
  - ▶ Rechte Maustaste auf Torbutton unten rechts - Preferences:
    - ▶ "Use Polipo" abhaken
    - ▶ "Disable Button and Hotkeys..." anhaken

# Firefox

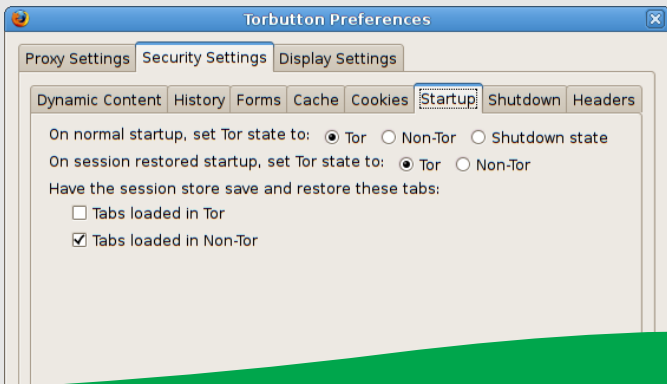
## Torbutton Extension II



# Firefox

## Torbutton Extension III

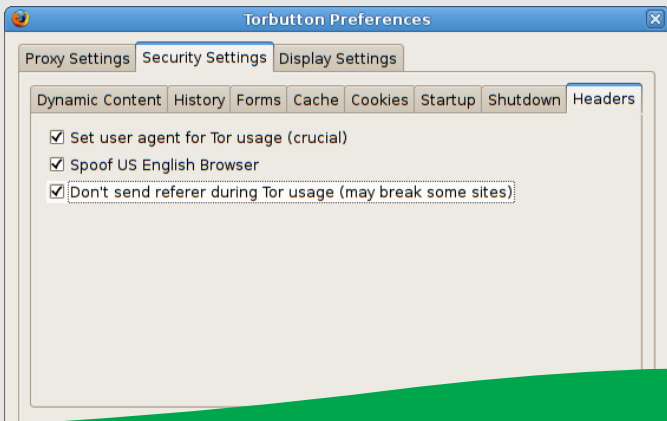
- ▶ Unter Security Settings - Startup
  - ▶ On normal startup, set Tor state to: Tor
  - ▶ On session restored startup, set Tor state to: Tor



# Firefox

## Torbutton Extension IV

- ▶ Und allenfalls unter Security Settings - Headers
  - ▶ “Don't send referer...” anhaken



# Firefox

## Restarten und testen

- ▶ `https://check.torproject.org/?lang=de`
- ▶ `http://centralops.net/asp/co/BrowserMirror.vbs.asp`



# Firefox

- ▶ Tor-Profil nur mit aktiviertem Tor verwenden
  - ▶ Cookies, History, Cache etc. werden gemäss aktuellen Einstellungen nur im aktivierten Modus geblockt
- ▶ Suchmaschinen nach Gusto hinzufügen
- ▶ Auch Extensions
  - ▶ Tab Mix Plus
  - ▶ Adblock Plus
  - ▶ RefControl (anstatt "Don't send referer...")
- ▶ jedoch **nicht**
  - ▶ NoScript
  - ▶ User Agent Switcher
  - ▶ 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
    - ▶ Top-Twenty-Server
    - ▶ CHF 1000.-/Jahr
- ▶ Zusammenschluss von Administratoren
  - ▶ German/Swiss Privacy Foundation
- ▶ 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-nc-sa/2.5/ch/>

## Kontakt

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