

Das TOR-Netzwerk: Anonym im Internet

Florian Knodt <adlerweb@adlerweb.info>

Was ist Tor

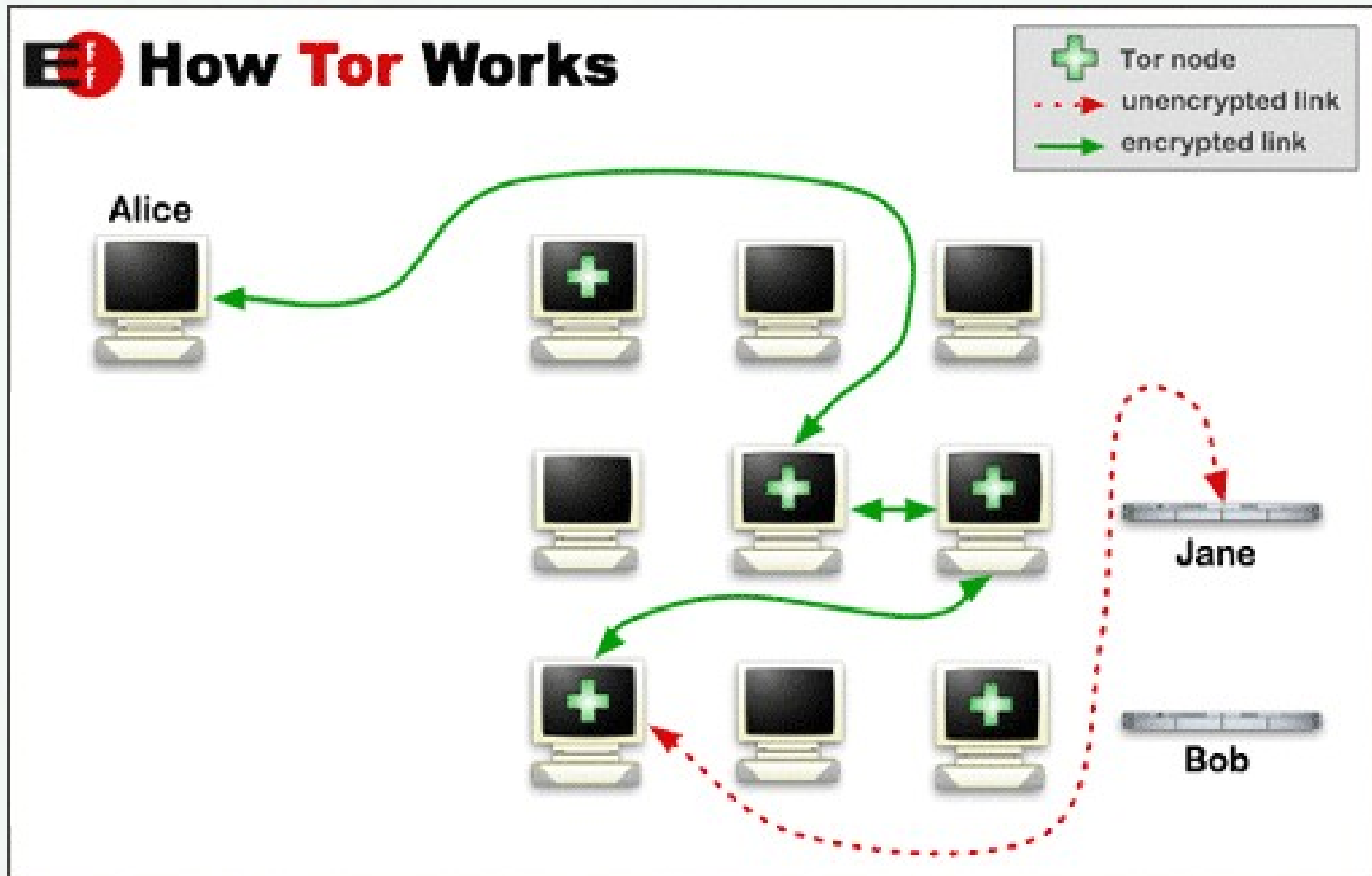
- „The Onion Router“
- Netzwerk zur Anonymisierung von Verbindungsdaten
 - Anonymisiert nicht die Nutzdaten
- Freie Software

Warum Tor?

→ Warum möchte man anonym bleiben?

- Furcht vor Nachteilen durch Meinungsäußerung oder Assoziation
 - Politische Äußerungen: Arabischer Frühling, China
 - Whistleblower: Snowden, Manning
 - Persönliches: Suche nach Krankheiten, Neigungen
- Unwille durch seine Daten Konzerne weiter zu finanzieren
- Zugriff auf zensierte Webseiten

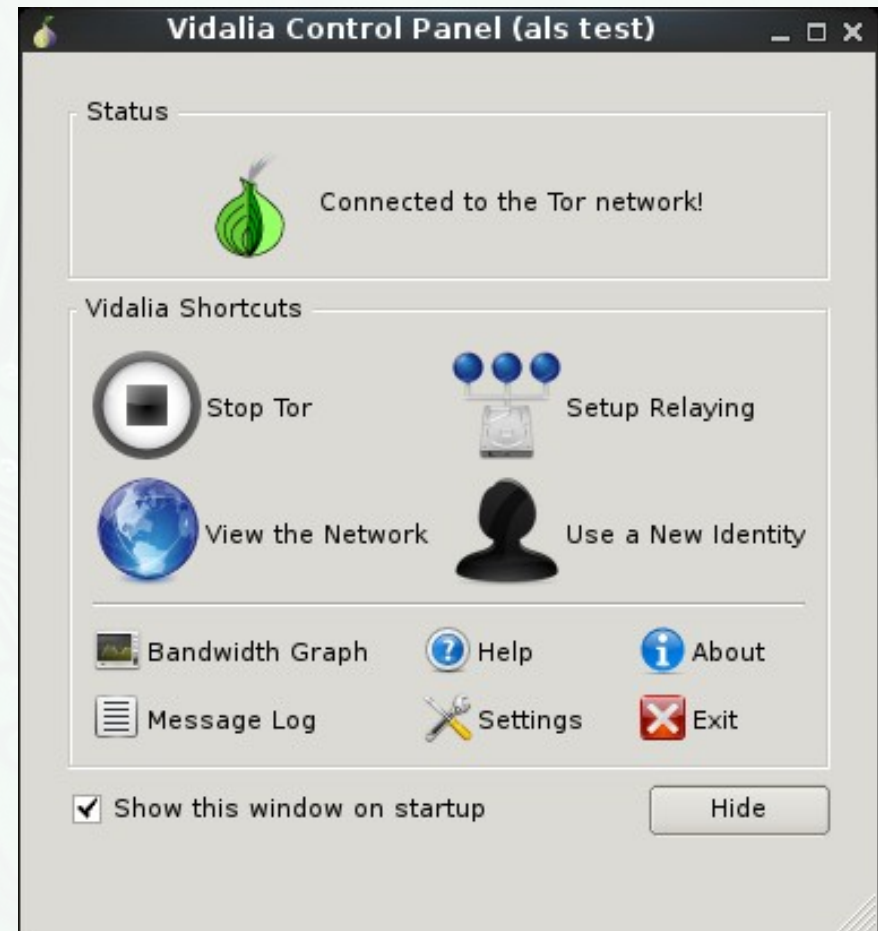
Funktion von Tor



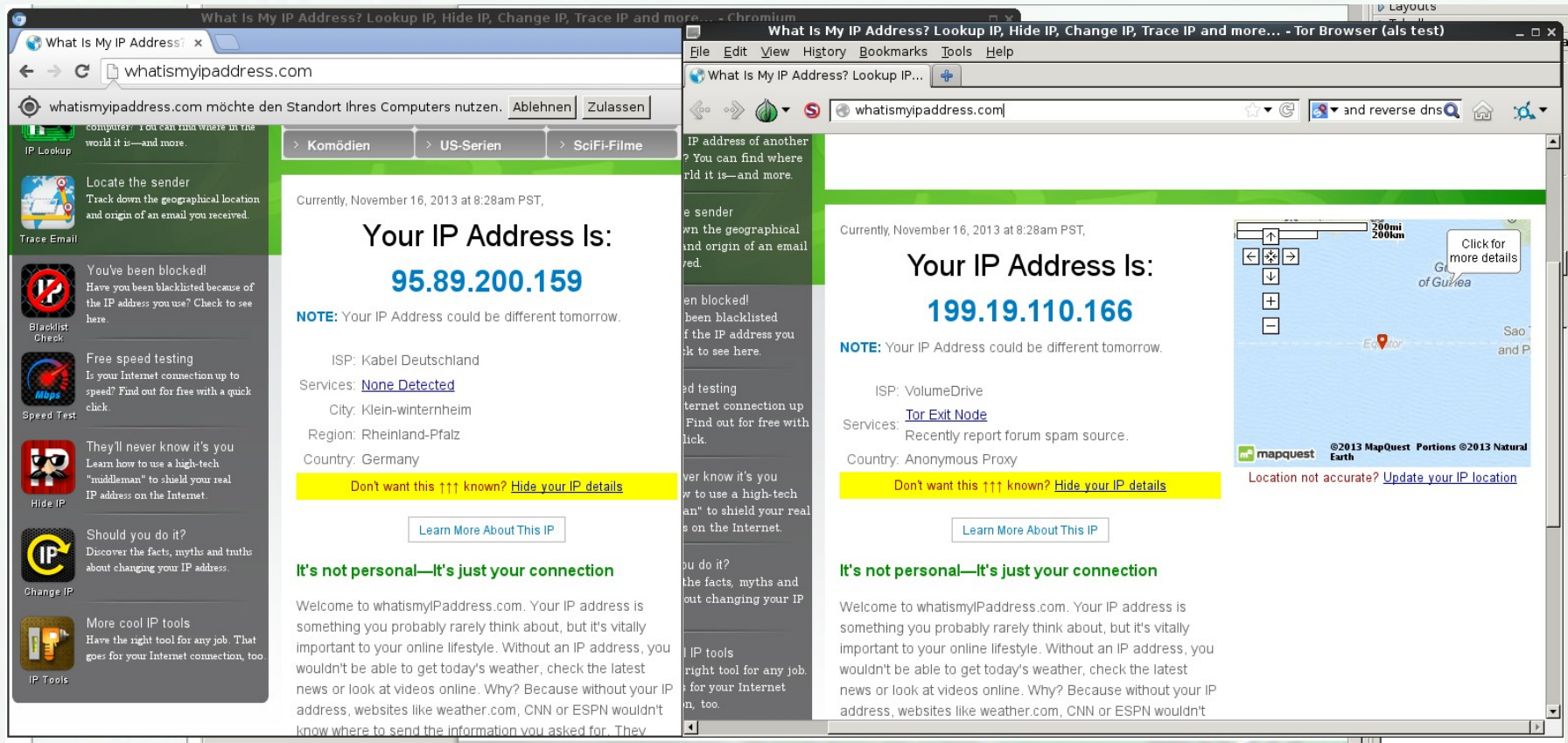
Ursprungsbild: Electronic Frontier Foundation · CC-BY
<https://ssd.eff.org/tech/tor> · <https://www.torproject.org/about/overview.html.en>

Das Browser-Bundle

- Paket mit Tor, GUI und angepasstem Firefox
- Unsichere Elemente wie Javascript oder Flash per default blockiert



Das Browser-Bundle



Ist Tor sicher?

Nope!

Ist Tor sicher?

- Kommunikation zwischen letztem Knoten und dem Ziel ist unverschlüsselt
 - Daten können abgefangen werden, wenn kein SSL (HTTPS o.Ä.) genutzt wird
- Wenn man mehrere Knoten abhört kann man durch zeitliche Zusammenhänge den Pfad nachvollziehen
 - TOR versucht mit absichtlichen Verzögerungen zu kontern
 - Scheint zu funktionieren, denn die NSA sagt: "Tor stinks"
- Angriffe auf den Nutzerrechner selbst, z.B. über Sicherheitslücken im Browser

Weiteres zu Tor

- Kann nicht nur Webseiten
 - Prinzipiell kann alles, was TCP/IP nutzt über Tor getunnelt werden
- Versteckte Dienste
 - Nicht nur der Nutzer sondern auch der Betreiber der Seite bleiben Anonym
 - Bekanntes Beispiel: Silkroad
- Tor-“OS“
 - Virtuelle Maschine welche den gesamten Traffic über Tor tunnelt