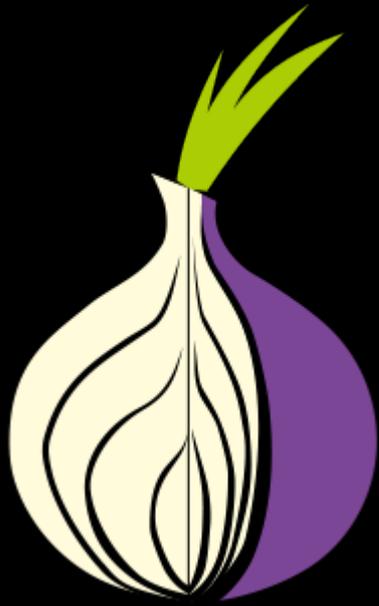
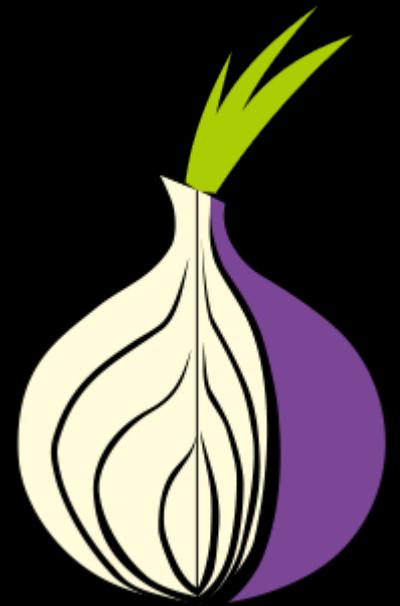


Welcome to the darknet



We
have
onions



V 0.1 180702 Köln

Jochim Selzer - js@crypto.koeln

6AA4 89F9 9E1F DCBA FF00 F291 8A97 4A5C 0970 E0CF

Aufbau

- Was ist „das Darknet“?
- Wie funktioniert Onion-Routing?
- Wovor schützt Tor?
- Wovor schützt Tor nicht?
- Und was heißt das politisch?

Disclaimer

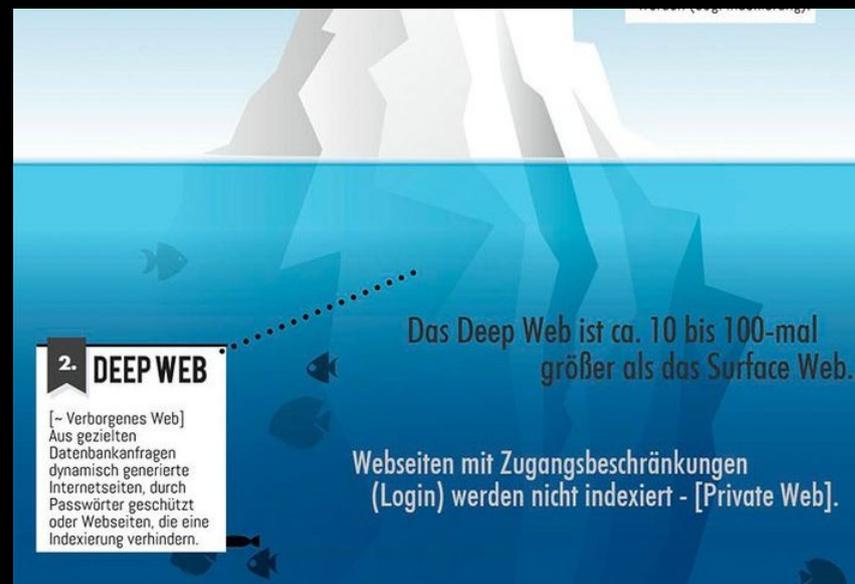
- Das ist ein Einstiegsvortrag.
- Warum nicht I2P, JonDonym, GNUnet, Freenet, Retroshare, Goldbug, Bitmessage <name your favorite tool here>?
- Zum Einwand: Tor ist langsam!
- Zum Einwand: Tor ist gefährlich!

Drei Fragen zur Sicherheit

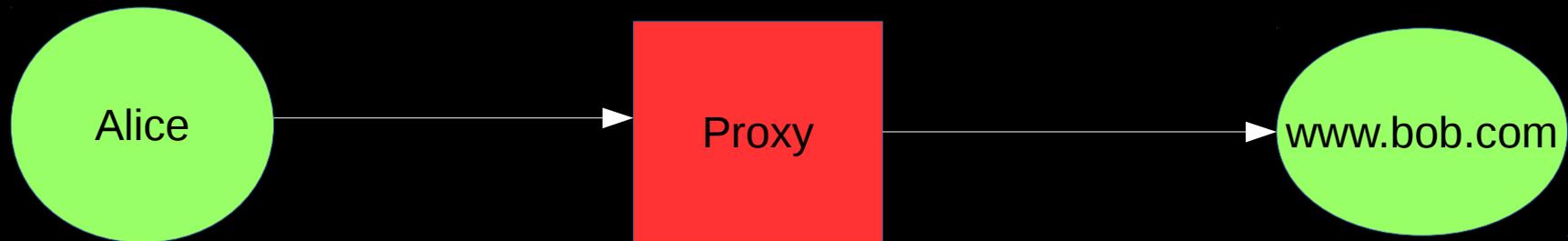
- Wovor will ich mich schützen?
- Wem muss, wem will ich vertrauen?
- Was bin ich zu investieren bereit?

Einige Angebervokabeln

- „Clearnet“, „Surface Web“ – kennen wir
- „Deep Web“ – nicht von Suchmaschinen erfasst
- „Darknet“ – anonym, nur mit Zusatzsoftware ansprechbar

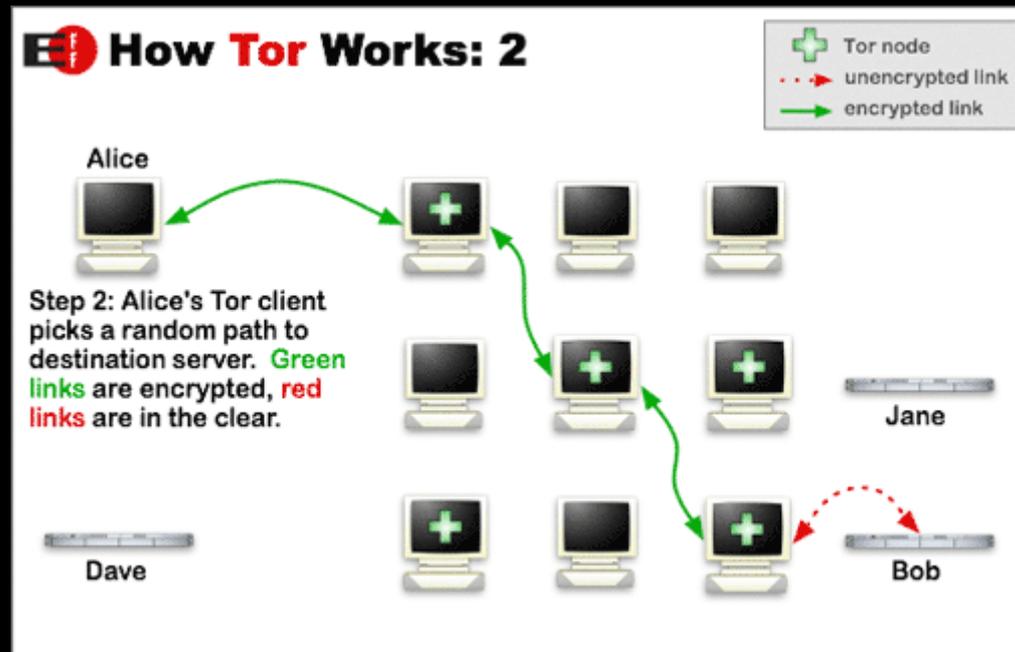


Warum kein VPN-Proxy?

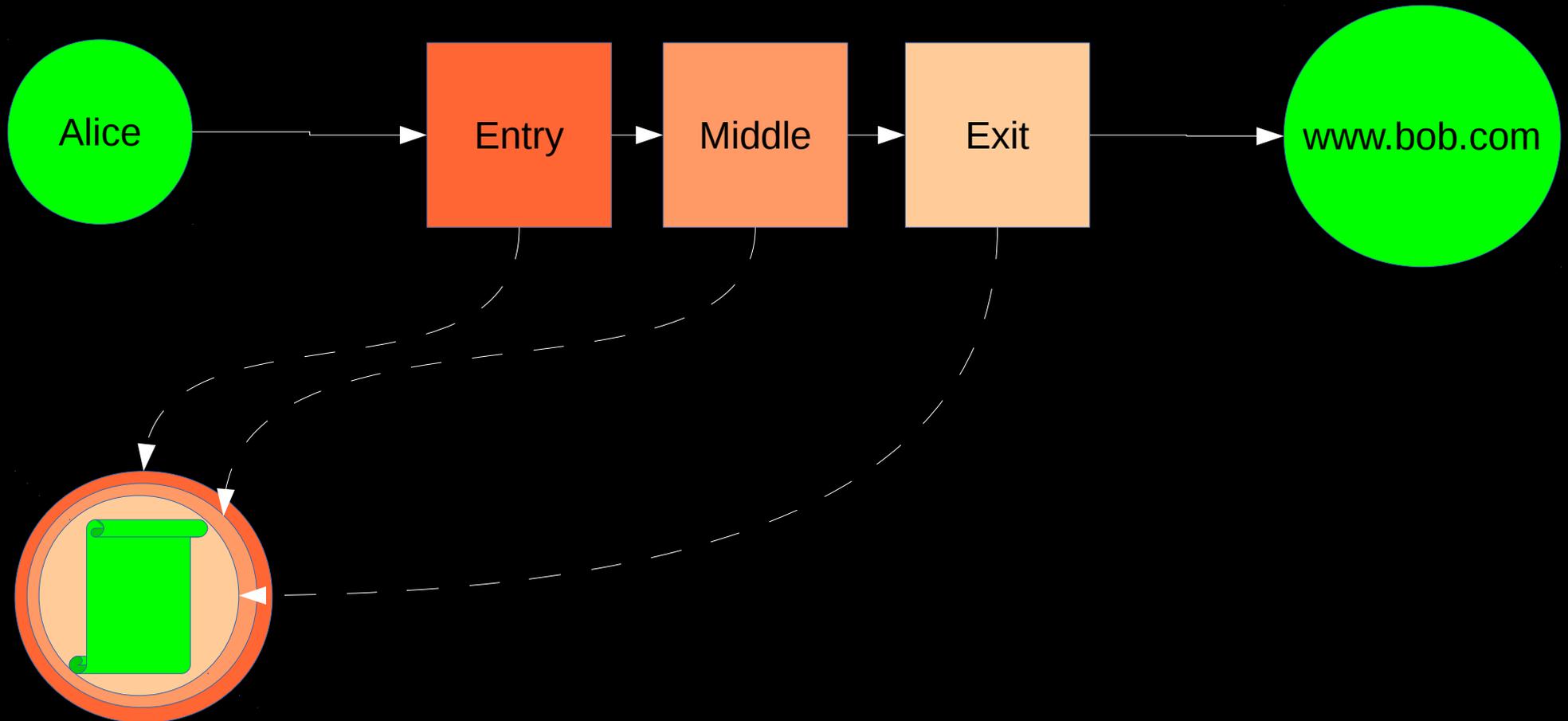


Anonymisierung mit Tor

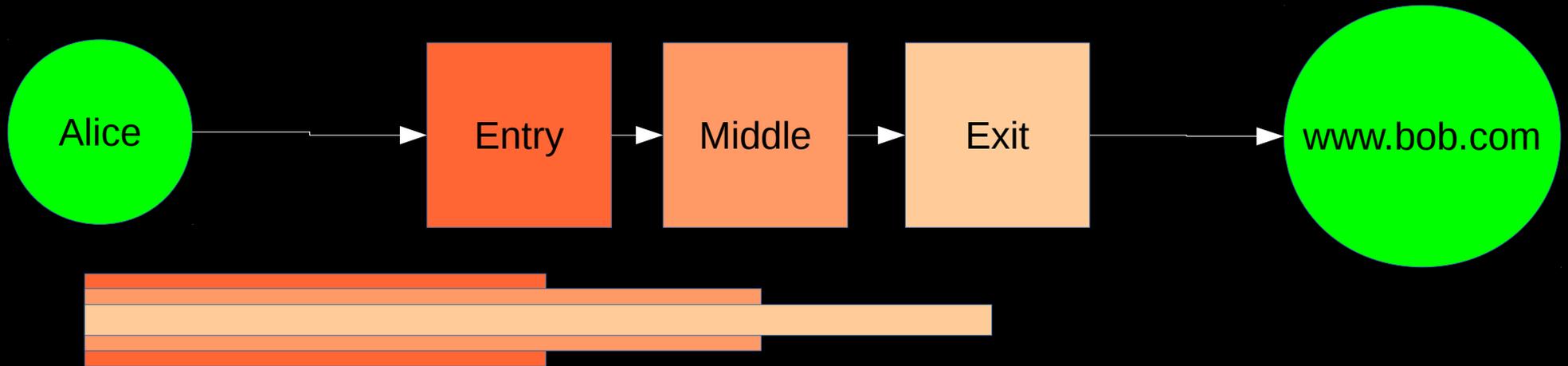
- <https://www.torproject.org/>
- Anonymisierung
- Anti-Zensur-Werkzeug



Tor - prinzipielle Funktionsweise



Tor – prinzipielle Funktionsweise



Was kann Tor?

- Tor verbirgt die Client-IP.

Was kann Tor ein bisschen?

- Tor verschleiert den Browser-Fingerprint.

Was kann Tor nicht?

- Tor ändert nicht
 - Ihren Wach-Schlaf-Rhythmus
 - Ihre Interessen und Gewohnheiten
- Tor schützt nicht vor
 - Schadsoftware
 - Eigener Dummheit (namentliche Logins, Informationen in Postings, Fehler im Analogleben)
- Tor verschleiern nicht dass, nur mit wem Sie kommunizieren.

Schwachstellen

- 7000 Knoten weltweit, davon 60 % in den Ländern Deutschland (1.300), Frankreich, den Niederlanden und USA.
- Tor-Knoten sind bekannt.
- Korrelationsanalysen sind möglich.
- Der Tor-Browser ist etwas veraltet.

Alles ganz schlimm

- Sex!
- Bombenbauanleitungen!
- Nazis!
- Drogen!
- Urheberrechtlich geschütztes Material!

Einstieg über ein hidden Wiki

Marketplace Commercial Services

<http://6w6vcynl6dumn67c.onion/> – Tor Market Board – Anonymous Marketplace Forums
<http://wvk32thojn4gpp4.onion/> – Project Evil
<http://5mvm7cg6bgklftp.onion/> – Discounted electronics goods
<http://lw4ipk5choakk5ze.onion/raw/evbLewgkDSVkifzv8zAo/> – Unfriendlysolution – Legit hitman service
<http://nr6juudpp4as4gjjg.onion/torgirls.html> – Tor Girls
<http://tuu66yxvrnn3of7l.onion/> – UK Guns and Ammo
<http://nr6juudpp4as4gjjg.onion/torguns.htm> – Used Tor Guns
<http://ucx7bkbi2dtia36r.onion/> – Amazon Business
<http://nr6juudpp4as4gjjg.onion/tor.html> – Tor Technology
<http://hbetshipq5yhhrsd.onion/> – Hidden BetCoin
<http://cstoreav7i44h2lr.onion/> – CStore Carded Store
<http://tfwdi3izigxlure.onion/> – Apples 4 Bitcoin
<http://e2qizoerj4d6ldif.onion/> – Carded Store
<http://jvrnuue4bvbftiby.onion/> – Data-Bay
<http://bgkitnugq5ef2cpi.onion/> – Hackintosh
<http://vlp4uw5ui22ljl7.onion/> – EuroArms
<http://b4vqxw2j36wf2bqa.onion/> – Advantage Products
<http://ybp4oezfkhk24hxmb.onion/> – Hitman Network
<http://mts7hqqqeogujc5e.onion/> – Marianic Technology Services
<http://mobil7rab6nuf7vx.onion/> – Mobile Store
<http://54flq67kqr5wvjqf.onion/> – MSR Shop
<http://lyth5q7zdmqlycbcz.onion/> – Old Man Fixer's Fixing Services
http://matrixtxri745dfw.onion/neo/uploads/MATRIXtxri745dfwONION_130827231336IPA_pc.png – PC Shop
<http://storegsq3o5mfxiz.onion/> – Samsung StorE
<http://sheep5u64fi457aw.onion/> – Sheep Marketplace
<http://nr6juudpp4as4gjjg.onion/betcoin.htm> – Tor BetCoin
<http://qizriiqwmeq4p5b.onion/> – Tor Web Developer
<http://vfqnd6mieccqyit.onion/> – UK Passports
<http://en35tuzqmn4lofbk.onion/> – US Fake ID Store
<http://xfnwyig7olypdq5r.onion/> – USA Citizenship
<http://uybu3melulmoljnd.onion/> – iLike Help Guy
<http://dbmv53j45pcv534x.onion/> – Network Consulting and Software Development
<http://lw4ipk5choakk5ze.onion/raw/4585/> – Quick Solution (Hitman)
<http://nr6juudpp4as4gjjg.onion/tynermsr.htm> – Tyner MSR Store

Ein Ausflug ins Darknet

The screenshot shows a web browser window with the address bar displaying `mmgh3rqeswrlgzdr.onion`. The page content is a seizure notice with a dark blue background and a network diagram. The main text reads: "THIS HIDDEN SITE HAS BEEN SEIZED and controlled since June 20" followed by a paragraph detailing the seizure by Dutch National Police, Bundeskriminalamt, Lietuvos Policija, and others. Below the text is a red silhouette of a sailing ship. At the bottom, logos for HANSA and AlphaBay Market are visible, along with logos for the Dutch Ministry of Justice (OPENBAAR MINISTERIE POLITIE) and Europol.

Notice

THIS HIDDEN SITE HAS BEEN SEIZED

and controlled since June 20

by the Dutch National Police in conjunction with the Bundeskriminalamt, Lietuvos Policija, Federal Bureau of Investigation and Europol, under the authority of the Dutch National Prosecutor's Office and the Attorney General's office of the Federal State of Hesse (Germany).

The Dutch National Police have located Hansa Market and taken over control of this marketplace since June 20, 2017. We have modified the source code, which allowed us to capture passwords, PGP-encrypted order information, IP-addresses, Bitcoins and other relevant information that may help law enforcement agencies worldwide to identify users of this marketplace. For more information about this operation, please consult our hidden service at politepost22.asi.onion.

This seizure was part of Operation Bayonet, which includes the takeover of Hansa Market by the National Police of the Netherlands and the takedown of AlphaBay Market by the Federal Bureau of Investigation of the United States of America on July 4, 2017.

HANSA **AlphaBay Market**

OPENBAAR MINISTERIE **POLITIE** **EUROPOL**

Ein Zerrbild

- Hidden Wikis sind veraltet.
- Die Suchmaschinen leisten im Vergleich zu Google wenig.
- Was Sie sehen, sind diejenigen, die gesehen werden wollen.
- Die Polizei ist nicht machtlos.

Auch das ist im Darknet

Facebook, Inc. (US) | https://www.facebookcorewwwi.onion/?_fb_noscript=1 Search

facebook

Email or Phone Password

[Forgot account?](#)

Sign Up

It's free and always will be.

JavaScript is disabled on your browser.
Please enable JavaScript on your browser or upgrade to a JavaScript-capable browser to register for Facebook.

Birthday

[Why do I need to provide my birthday?](#)

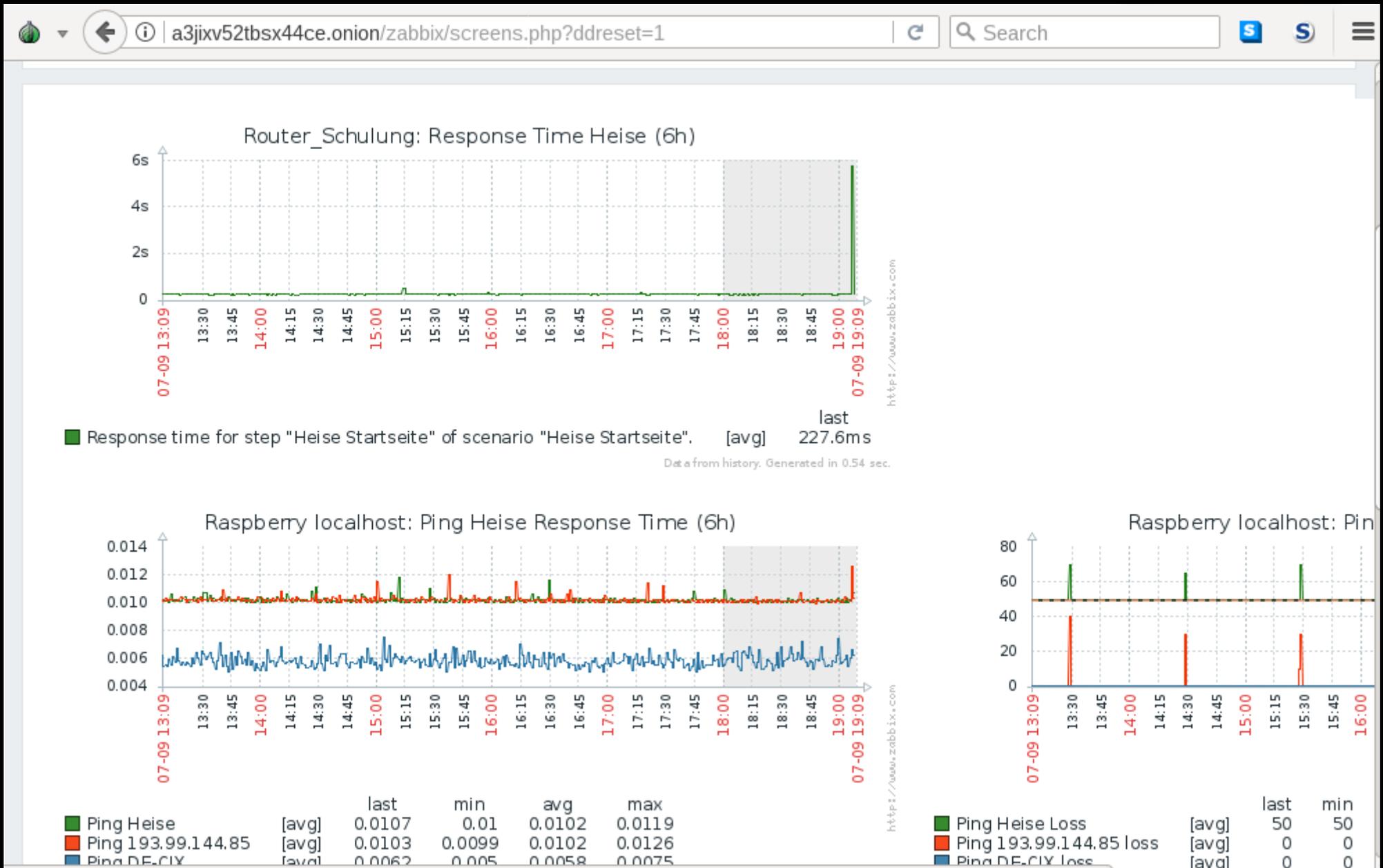
Female Male

By clicking Sign Up, you agree to our [Terms](#), [Data Policy](#) and [Cookies Policy](#). You may receive SMS Notifications from us and can opt out any time.

Connect with friends and the world around you on Facebook.

-  **See photos and updates** from friends in News Feed.
-  **Share what's new** in your life on your Timeline.
-  **Find more** of what you're looking for with Facebook Search.

The real hidden Darknet



Wie wäre es mit ein bisschen Zensur?

- Tor gibt es ganz oder gar nicht.

Weiterführende Links

- Tor-Projektseite mit Software und Dokumentation
- 9 Darknet-Fragen, die sich jeder stellt, aber niemand zu fragen traut
- Polizisten gehen rabiāt gegen Tor-Aktivistēn vor, als sie chemische Formeln in seinem Büro entdecken
- Themenseite Darknet bei der bpb
- Browser-Fingerprinting
 - Panopticlick
 - Studie der FAU Erlangen
 - Am I unique?
- Waffen im Darknet kaufen? Gar nicht so einfach - Chip
- Reportage von Tom Ockers
- Cryptoparty Köln-Bonn