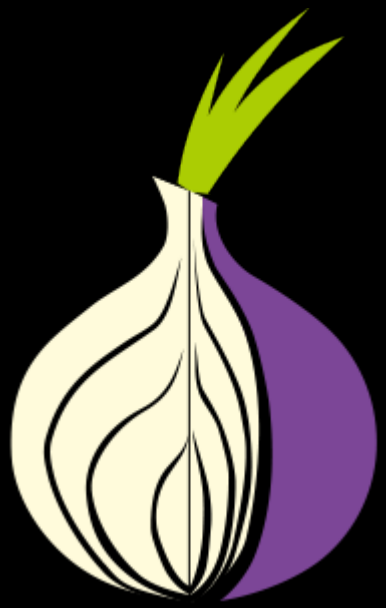
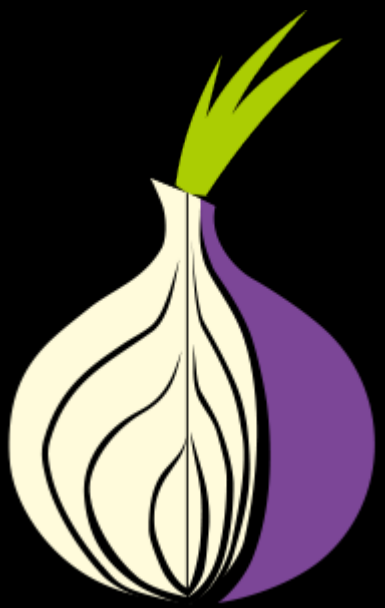
Welcome to the darknet



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!

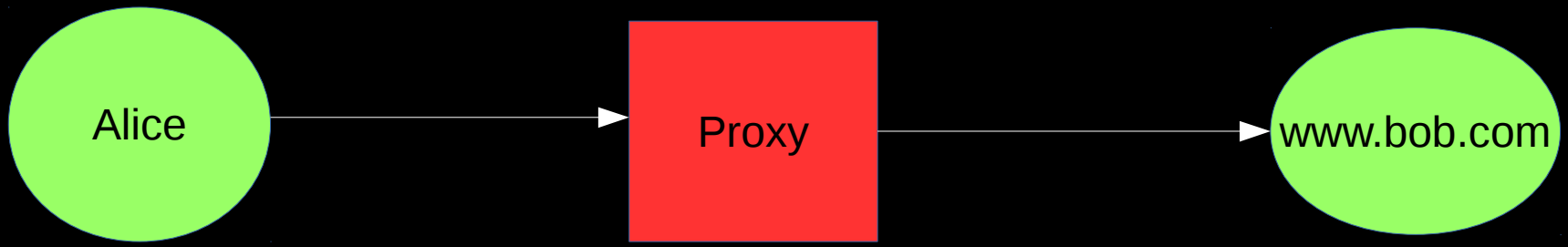
Drei Fragen zur Sicherheit

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

Einige Angebervokabeln

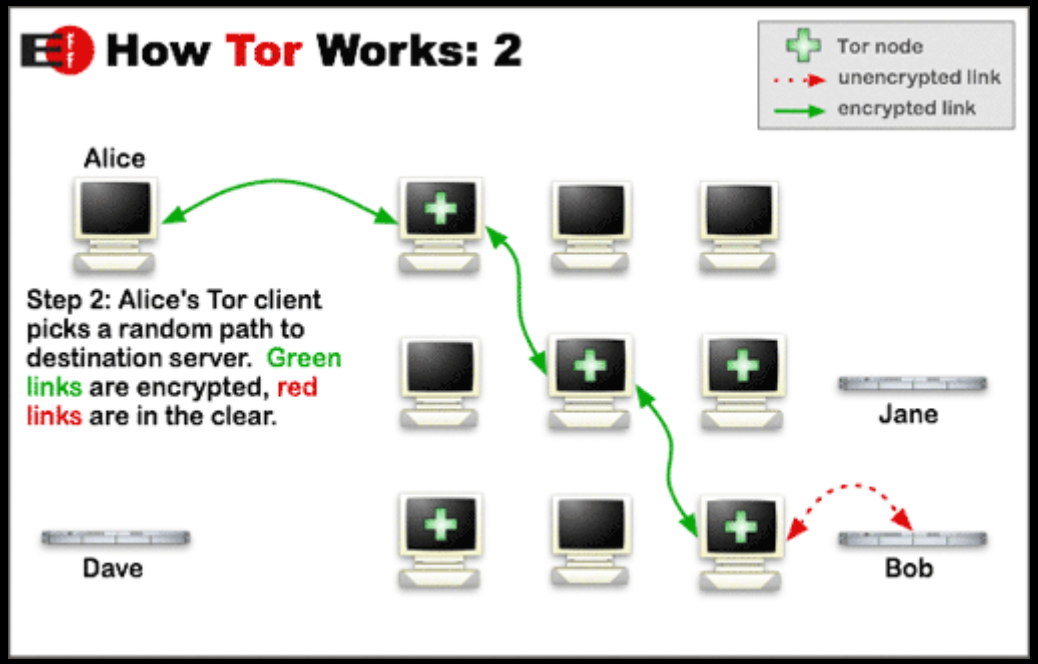
- „Clearnet“, „Surface Web“ – kennen wir
- „Deep Web“ – nicht von Suchmaschinen erfasst
- „Darknet“ – anonym, nur mit Zusatzsoftware ansprechbar

Warum kein VPN-Proxy?

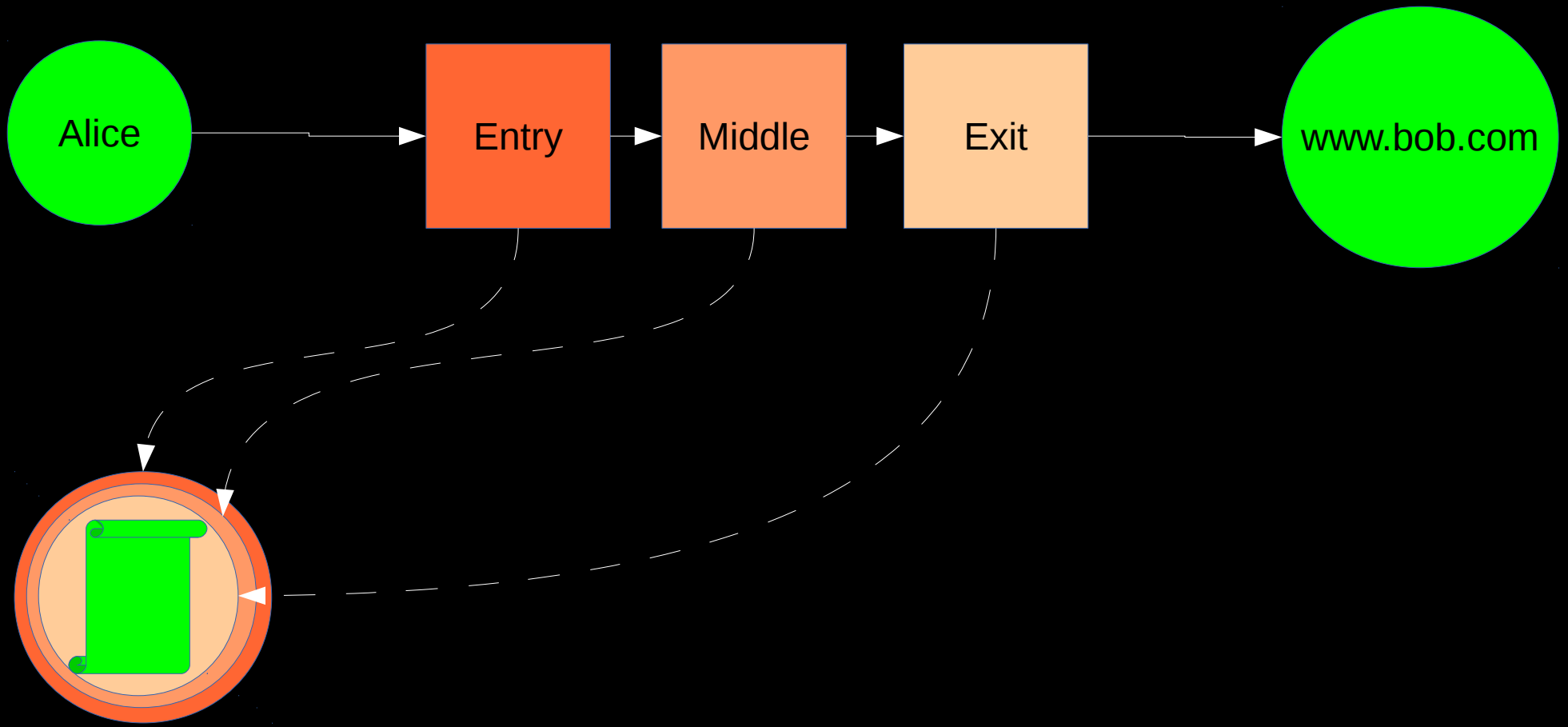


Anonymisierung mit Tor

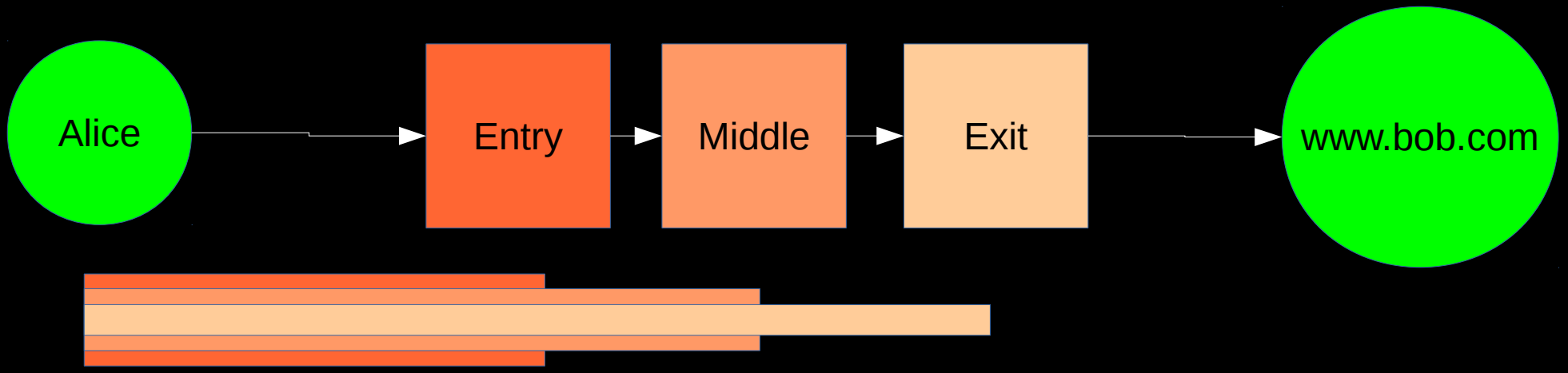
- https://www.torproject.org/
- Anonymisierung
- Anti-Zensur-Werkzeug



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 verschleiert 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

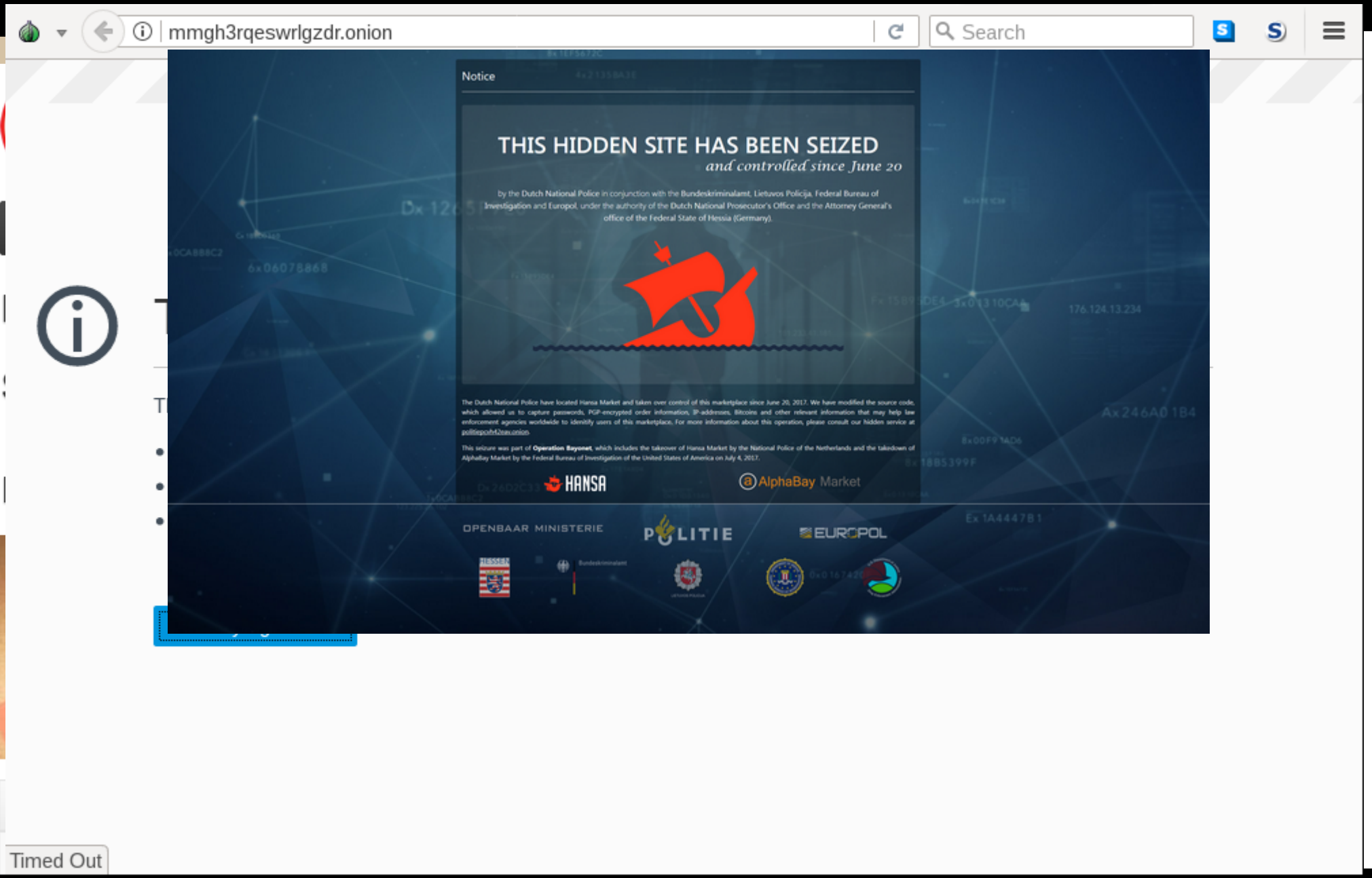
- Sex!
- Bombenbauanleitungen!
- Nazis!
- Drogen!
- Urheberrechtlich geschütztes Material!

Einstieg über ein hidden Wiki

Marketplace Commercial Services

http://6w6vcynl6dumn67c.onion/ – Tor Market Board – Anonymous Marketplace Forums
http://wvk32thojln4gpp4.onion/ – Project Evil
http://5mvm7cg6bgklfjtp.onion/ – Discounted electronics goods
http://lw4ipk5choakk5ze.onion/raw/evbLewgkDSVkifzv8zAo/ – Unfriendlysolution – Legit hitman service
http://nr6juudpp4as4gjg.onion/torgirls.html – Tor Girls
http://tuu66yxvrnn3of7l.onion/ – UK Guns and Ammo
http://nr6juudpp4as4gjg.onion/torguns.htm – Used Tor Guns
http://ucx7bkbi2dtia36r.onion/ – Amazon Business
http://nr6juudpp4as4gjg.onion/tor.html – Tor Technology
http://hbetshipq5yhhrsd.onion/ – Hidden BetCoin
http://cstoreav7i44h2lr.onion/ – CStore Carded Store
http://tfwdi3izigxllure.onion/ – Apples 4 Bitcoin
http://e2qizoerj4d6ldif.onion/ – Carded Store
http://jvrnuue4bvbftiby.onion/ – Data-Bay
http://bgkitnugq5ef2cpi.onion/ – Hackintosh
http://vlp4uw5ui22ljlg7.onion/ – EuroArms
http://b4vqxw2j36wf2bqa.onion/ – Advantage Products
http://ybp4oezfhk24hxmb.onion/ – Hitman Network
http://mts7hqqqeogujc5e.onion/ – Marianic Technology Services
http://mobil7rab6nuf7vx.onion/ – Mobile Store
http://54flq67kqr5wvjqf.onion/ – MSR Shop
http://yth5q7zdmqlycbcz.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://nr6juudpp4as4gjg.onion/betcoin.htm – Tor BetCoin
http://qizriixqwmeq4p5b.onion/ – Tor Web Developer
http://vfqnd6mieccqyiit.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://nr6juudpp4as4gjg.onion/tynermsr.htm – Tyner MSR Store

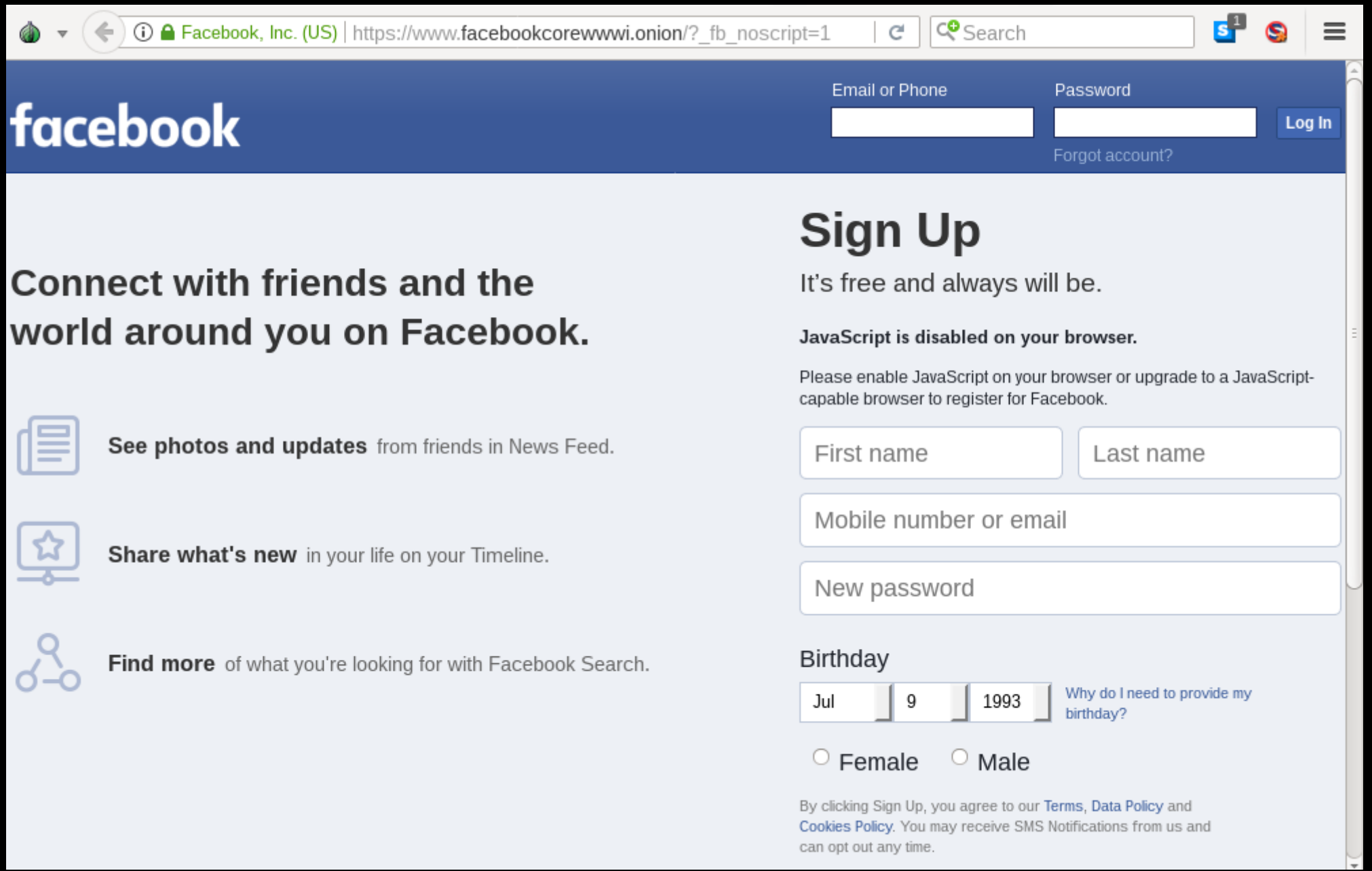
Ein Ausflug ins Darknet



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



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 rabiat gegen Tor-Aktivisten 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