The bridge to possible

Peeling an onion

a short travel into the Darknet

Frederic Detienne

cisco Live!

BRKSEC-2172

Cisco Webex App

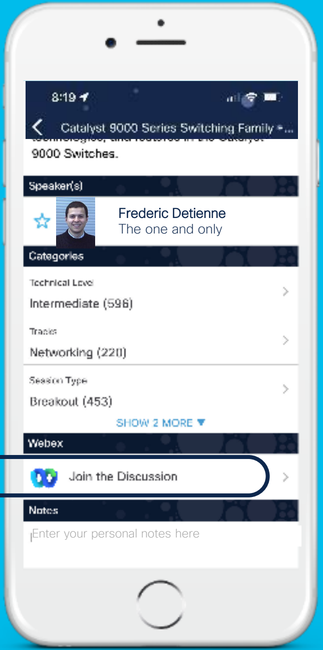
Questions?

Use Cisco Webex App to chat
with the speaker after the session

How

1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated until February 24, 2023.



8:19

Catalyst 9000 Series Switching Family +...

9000 Switches.

Speaker(s)

Frederic Detienne
The one and only

Categories

Technical Level
Intermediate (596)

Tracks
Networking (220)

Session Type
Breakout (453)

SHOW 2 MORE ▼

Webex

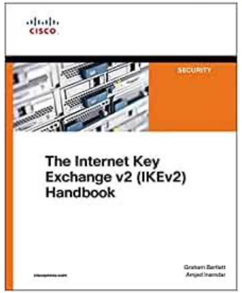
Join the Discussion

Notes

Enter your personal notes here

Who’s Frederic ?

- Belgian
  - lives in Aywaille (NOT Hawaii)
- Joined Cisco on January 1, 1997
  - fd@cisco.com
- Distinguished Engineer (TAC)
  - Web Content, AAA, Firewalls, VPNs, IPTV
  - Bit of everything (stuff nobody else wanted)
  - Invented DMVPN, FlexVPN
  - Focus on Serviceability
  - Invented RADKit



SECURITY

The Internet Key Exchange v2 (IKEv2) Handbook

Graham Bartlett
Amjad Inamdar

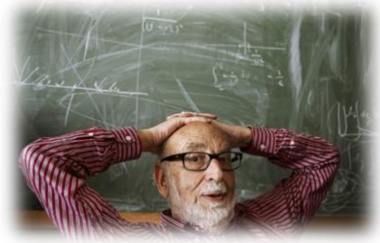
ciscopress.com

Cisco Remote Automation Development Kit (RADKit)

CISCO RADKIT.
FROM NETOPS TO DEVOPS.

RADKit is a network-wide orchestrator. Experience a radical new way of addressing your equipment, boost your Cisco Services, and expand your capabilities.

All tech. No fluff.



Session Objectives

- Shed light on the Dark Web
  - A little
- Technical TOR understanding
  - A lot
- Buy drugs, weapons, shop for body parts…
  - Not at all

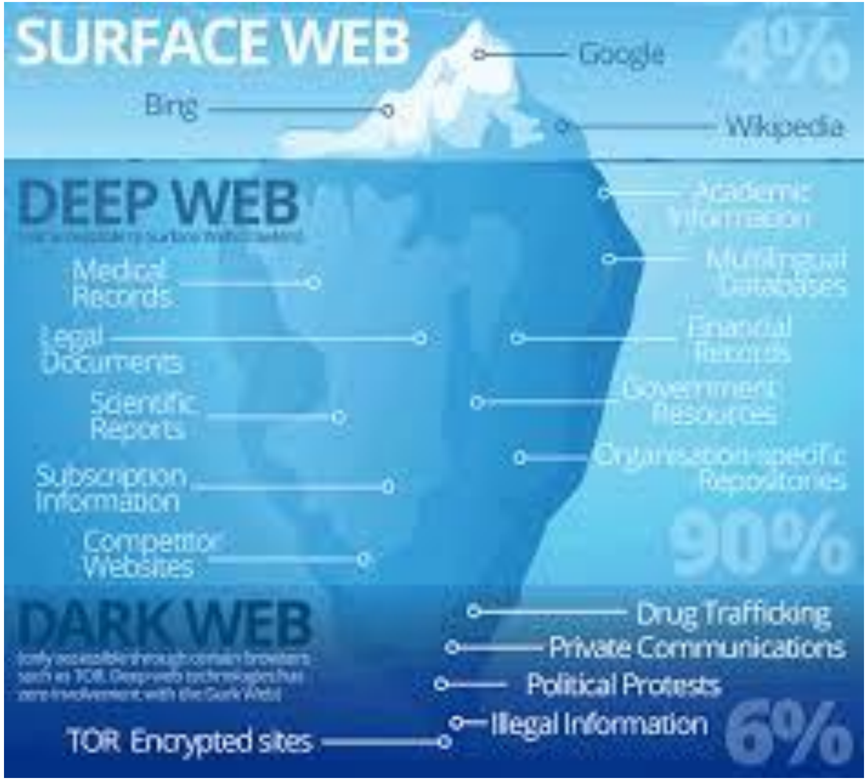
Agenda

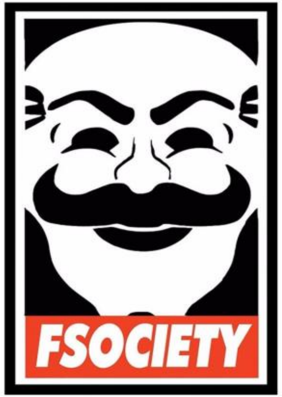
- Introduction
- About Tor
  - Onion Routing
  - Obfuscation
- Integration of Tor in other Apps
- Conclusion

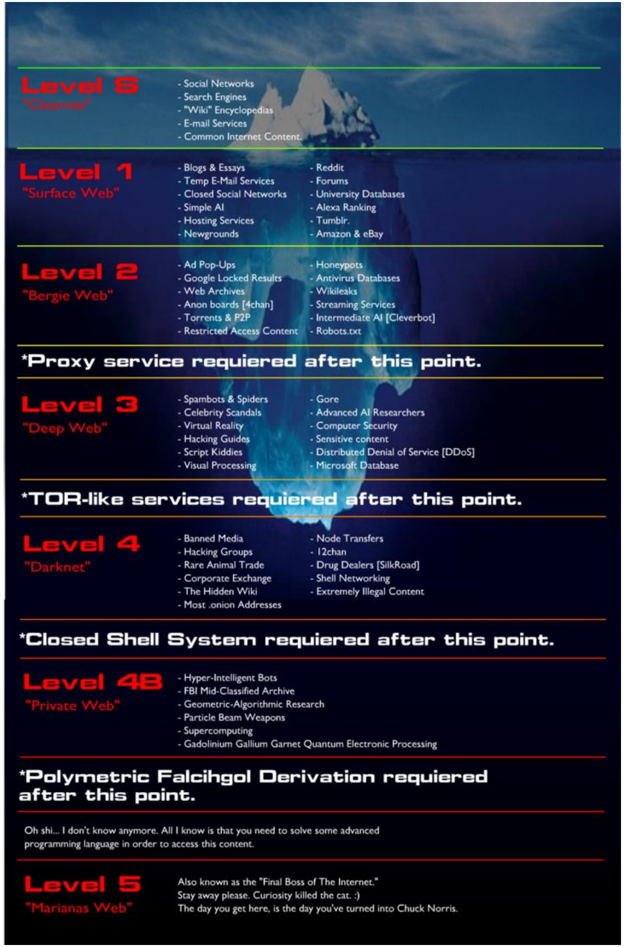
History of the Darknet

- 1991: Internet becomes publicly available
- 2000s: Release of Freenet:
  - Thesis project of the university of Edingburgh student Ian Clarke
  - Goal: create a new distributed information storage and retrieval system to autonomously communicate and share files
  - Freenet lays the ground for the Tor Project (different sources)
- 2002: Launch of TOR:
  - Researchers at the U.S. Naval Research Laboratory release an early version of Tor ("The Onion Router")
  - The U.S. government's Naval Research Laboratory developed Tor for members of the U.S. intelligence community to use the Internet without risk of identification
- 2004: Open Source Release of Tor by the US government:
  - Continued maintenance through a non profit project named the Tor Project

The Deep Web / The Dark Web







Level S "Clearnet"

- Social Networks
- Search Engines
- "Wiki" Encyclopedias
- E-mail Services
- Common Internet Content.

Level 1 "Surface Web"

- Blogs & Essays
- Temp E-Mail Services
- Closed Social Networks
- Simple AI
- Hosting Services
- Newgrounds
- Reddit
- Forums
- University Databases
- Alexa Ranking
- Tumblr.
- Amazon & eBay

Level 2 "Bergie Web"

- Ad Pop-Ups
- Google Locked Results
- Web Archives
- Anon boards [4chan]
- Torrents & P2P
- Restricted Access Content
- Honeypots
- Antivirus Databases
- Wikileaks
- Streaming Services
- Intermediate AI [Cleverbot]
- Robots.txt

***Proxy service requiered after this point.**

Level 3 "Deep Web"

- Spambots & Spiders
- Celebrity Scandals
- Virtual Reality
- Hacking Guides
- Script Kiddies
- Visual Processing
- Gore
- Advanced AI Researchers
- Computer Security
- Sensitive content
- Distributed Denial of Service [DDoS]
- Microsoft Database

***TOR-like services requiered after this point.**

Level 4 "Darknet"

- Banned Media
- Hacking Groups
- Rare Animal Trade
- Corporate Exchange
- The Hidden Wiki
- Most .onion Addresses
- Node Transfers
- I2chan
- Drug Dealers [SilkRoad]
- Shell Networking
- Extremely Illegal Content

***Closed Shell System requiered after this point.**

Level 4B "Private Web"

- Hyper-Intelligent Bots
- FBI Mid-Classified Archive
- Geometric-Algorithmic Research
- Particle Beam Weapons
- Supercomputing
- Gadolinium Gallium Garnet Quantum Electronic Processing

***Polymetric Falcihgol Derivation requiered after this point.**

Oh shi... I don't know anymore. All I know is that you need to solve some advanced programming language in order to access this content.

Level 5 "Marianas Web"

Also known as the "Final Boss of The Internet."
Stay away please. Curiosity killed the cat. :)
The day you get here, is the day you've turned into Chuck Norris.

Surface Web vs. Deep Web vs. Darknet

In Summary

Surface Web:

- Public websites and content available on search engines (indexed)
- Accessible by anyone

Deeb Weeb:

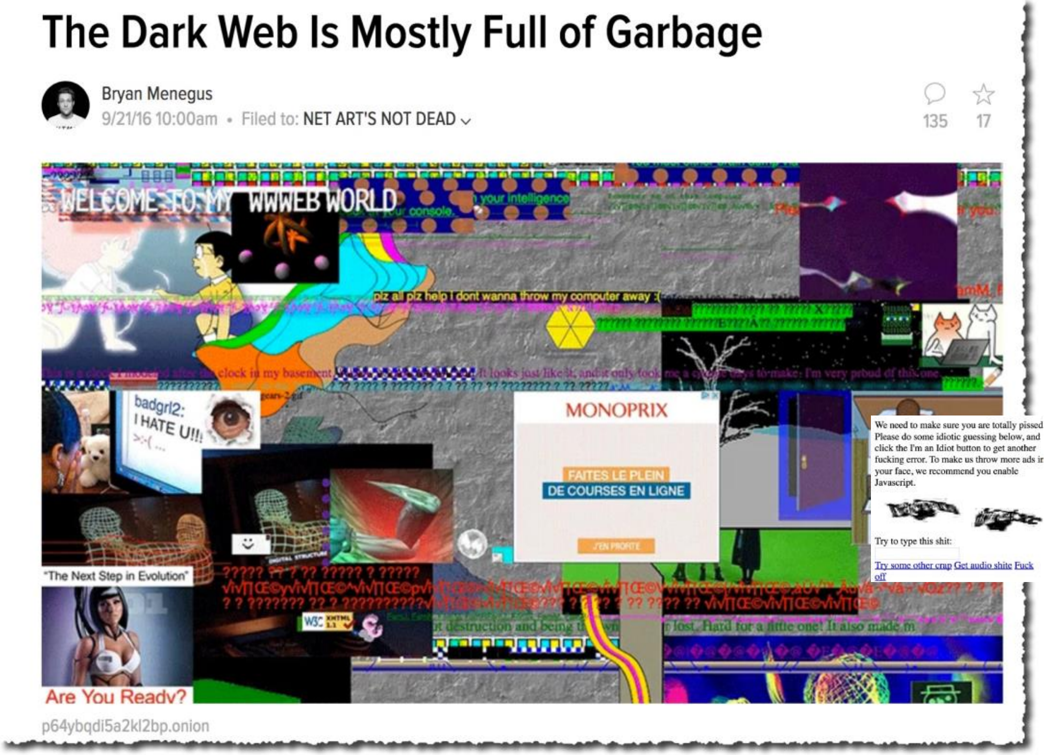
- Content not available on search engines (not indexed), e.g. bank data, cloud data
- Private databases, which require access authorization, e.g. intranet site, online forums/marketplaces

Dark Web / Darknet:

- Encrypted portion of the internet not indexed by search engines
- Requires specific configurations or authorization to access; allows users to remain anonymous

The (partial) Reality

https://gizmodo.com/the-deep-web-is-mostly-full-of-garbage-1786857267



The Dark Web Is Mostly Full of Garbage

Bryan Menegus
9/21/16 10:00am • Filed to: NET ART'S NOT DEAD

135 17

This is a clock I modeled after the clock in my basement. It looks just like it, and it only took me a couple days to make. I'm very proud of this one

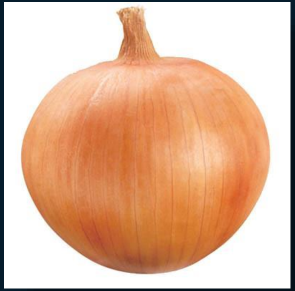
We need to make sure you are totally pissed Please do some idiotic guessing below, and click the I'm an Idiot button to get another fucking error. To make us throw more ads ir your face, we recommend you enable Javascript.

Try to type this shit:

Try some other crap Get audio shite Fuck off

p64ybqdi5a2kl2bp.onion

About Tor



The Onion router

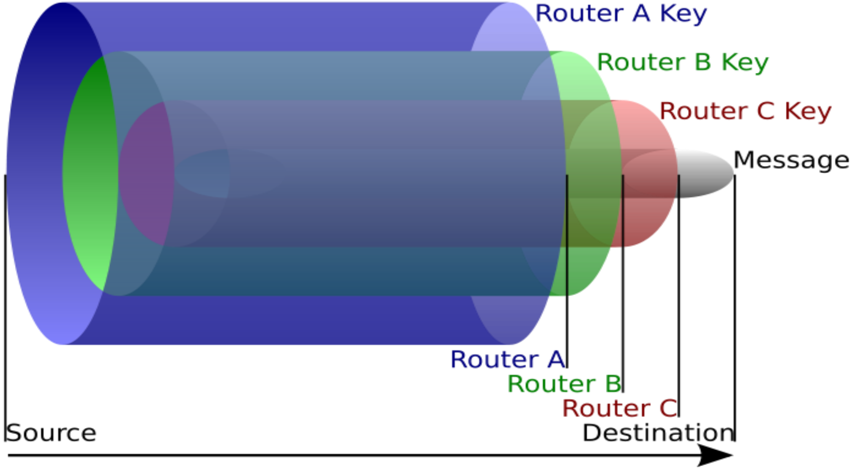
Open source SW / public design specs

Data is constantly encrypted at multiple layers

Sent through multiple routers. Each router decrypts the outer layer and finds routing instructions

Sends the data to the next router

Result is a completely encrypted path using random routers

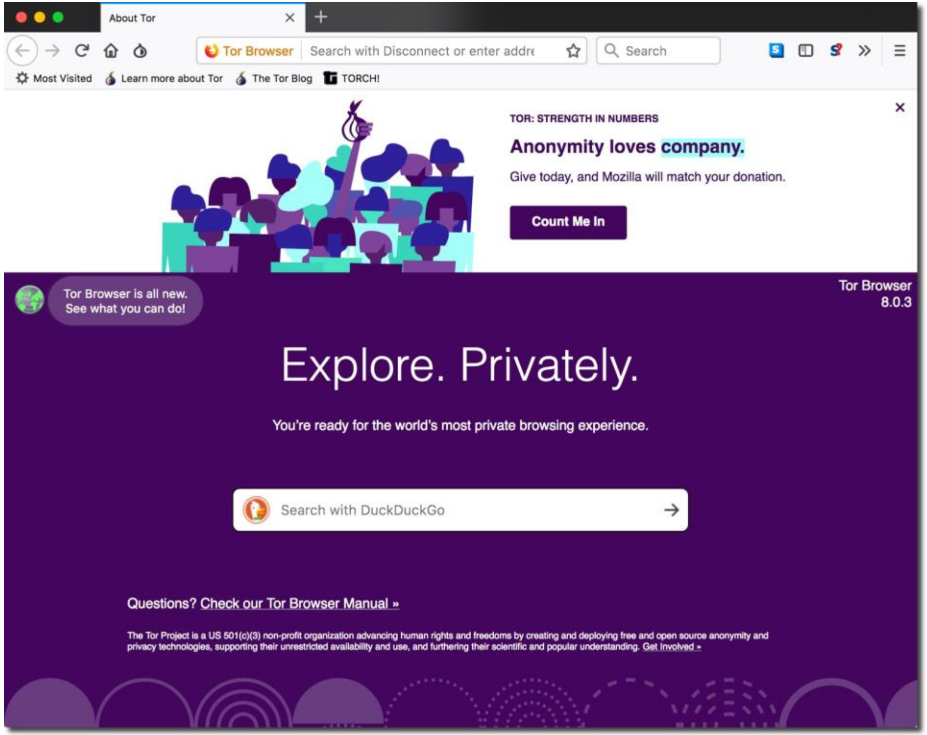


How is the Tor Network built?

- The Tor network consists of relays
- Relays are just nodes where the Tor software is installed
- They build encrypted connections to other relays, forming an overlay network
- Everyone can run a Tor relay and contribute to the network…

The Tor Browser – Connecting to the Tor Network

- Goal: Provide anonymity and access to censored and/or hidden resources
- Special browser based on mozilla firefox to establish a circuit through the Tor network
- Can connect directly or through proxies
- Often used in combination with VPNs



TOR: STRENGTH IN NUMBERS

Anonymity loves company.

Give today, and Mozilla will match your donation.

Count Me In

Tor Browser is all new. See what you can do!

Tor Browser 8.0.3

Explore. Privately.

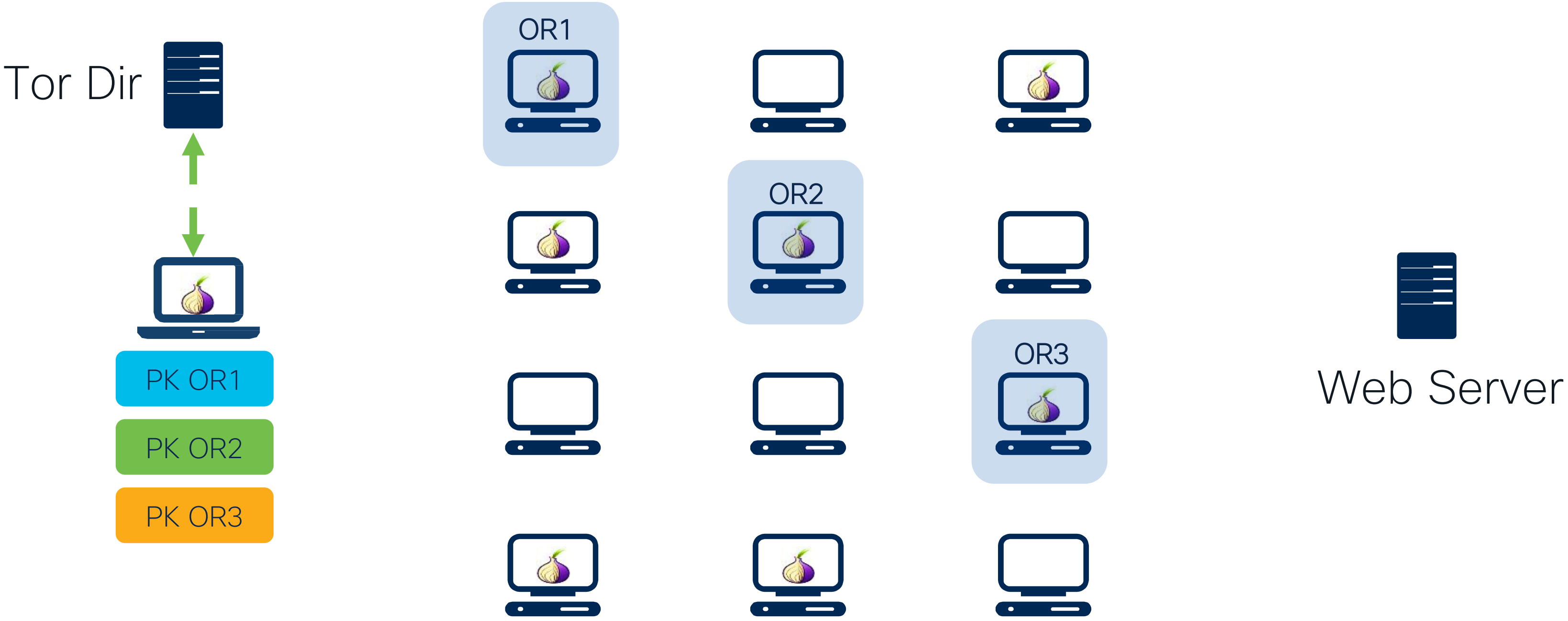
You're ready for the world's most private browsing experience.

Search with DuckDuckGo

Questions? Check our Tor Browser Manual »

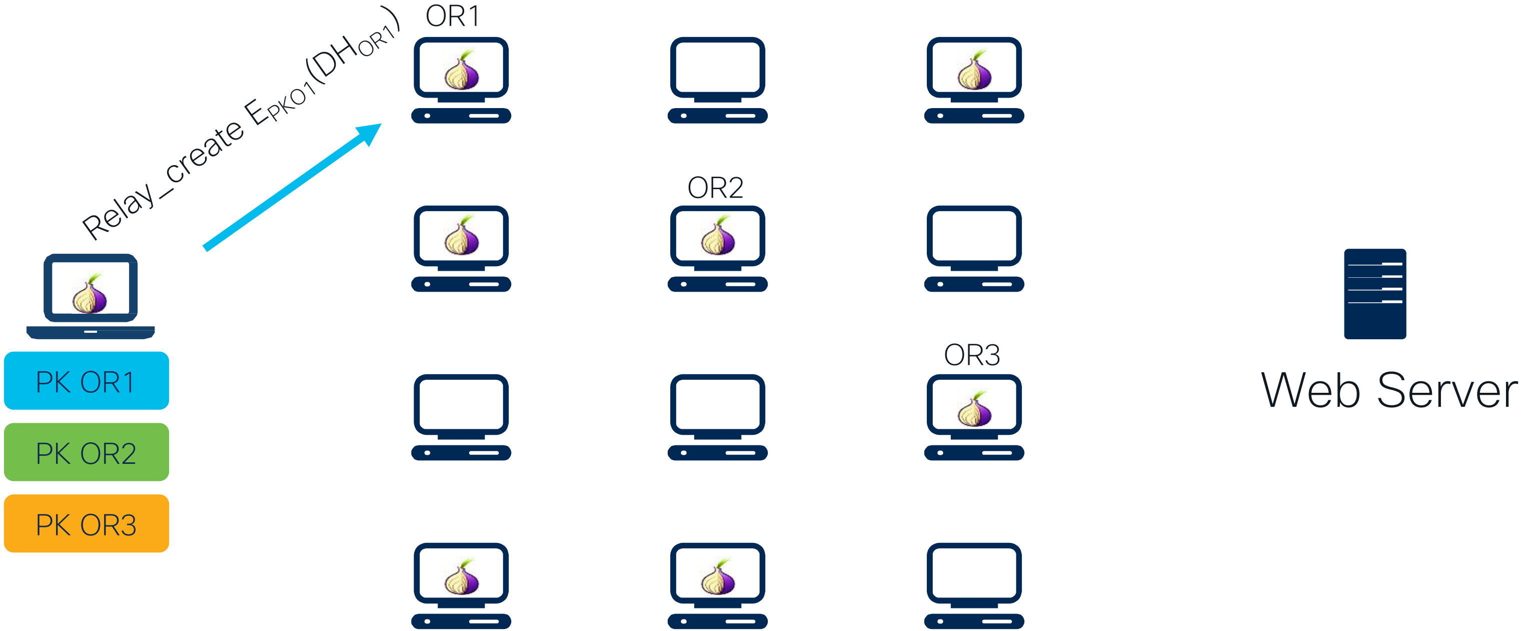
The Tor Project is a US 501(c)(3) non-profit organization advancing human rights and freedoms by creating and deploying free and open source anonymity and privacy technologies, supporting their unrestricted availability and use, and furthering their scientific and popular understanding. Get Involved »

Tor Relay



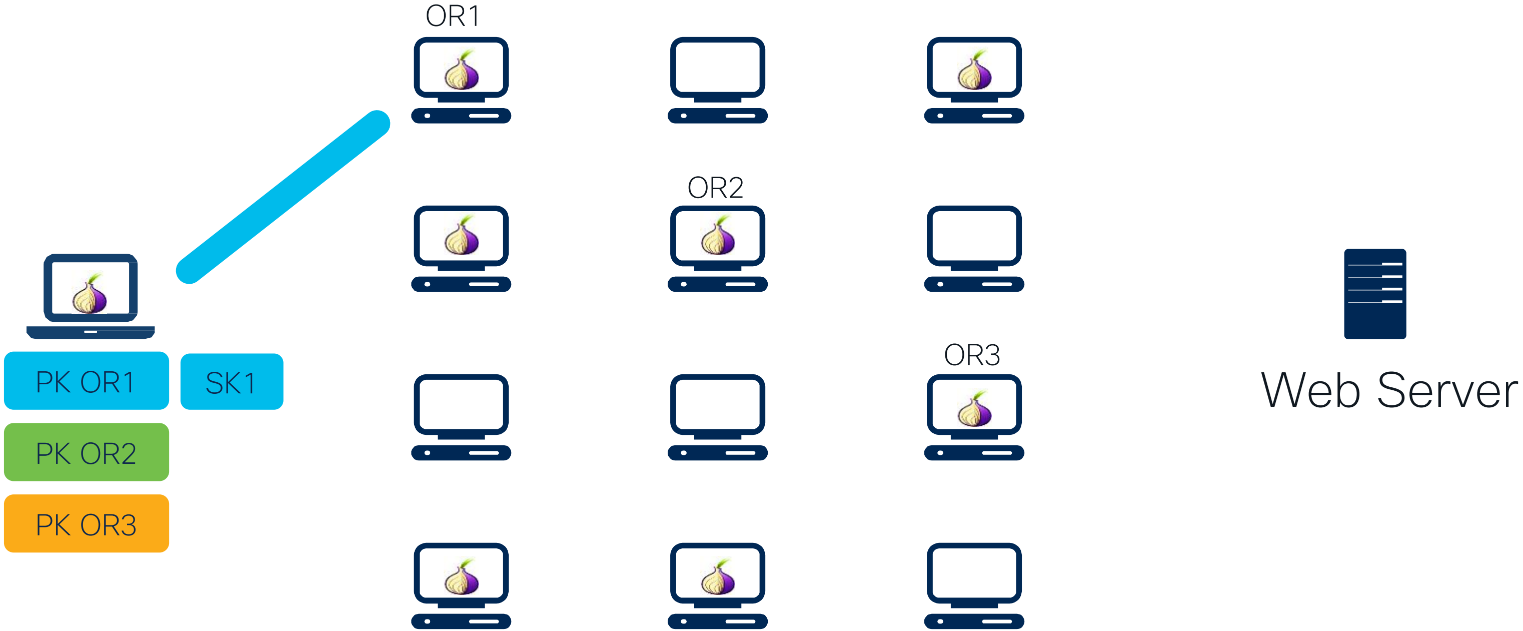
Tor Client selects 3 random Routers out of all Tor Relays and get their public keys

Tor Relay



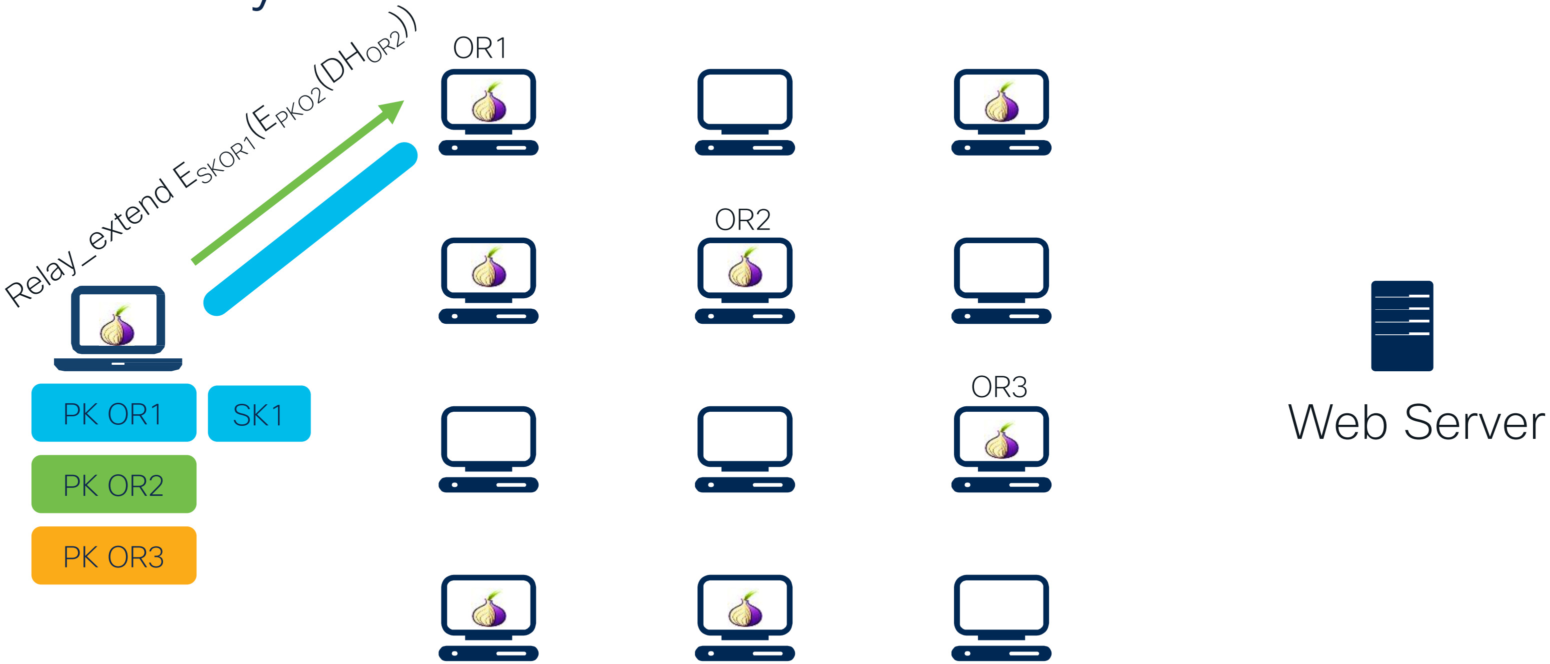
Tor Client sends DH Handshake to OR1, encrypted with public key of OR1, called “relay_create”

Tor Relay



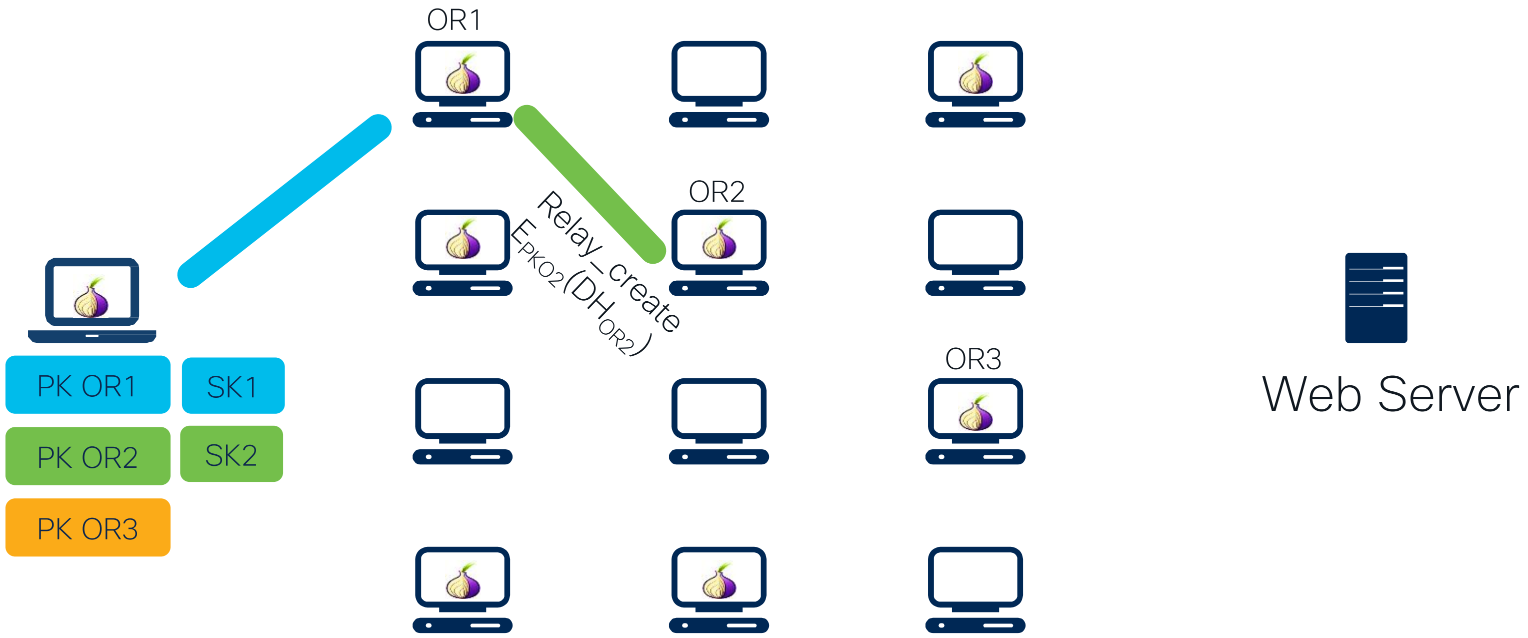
OR1 completes handshake, symmetric key is created

Tor Relay



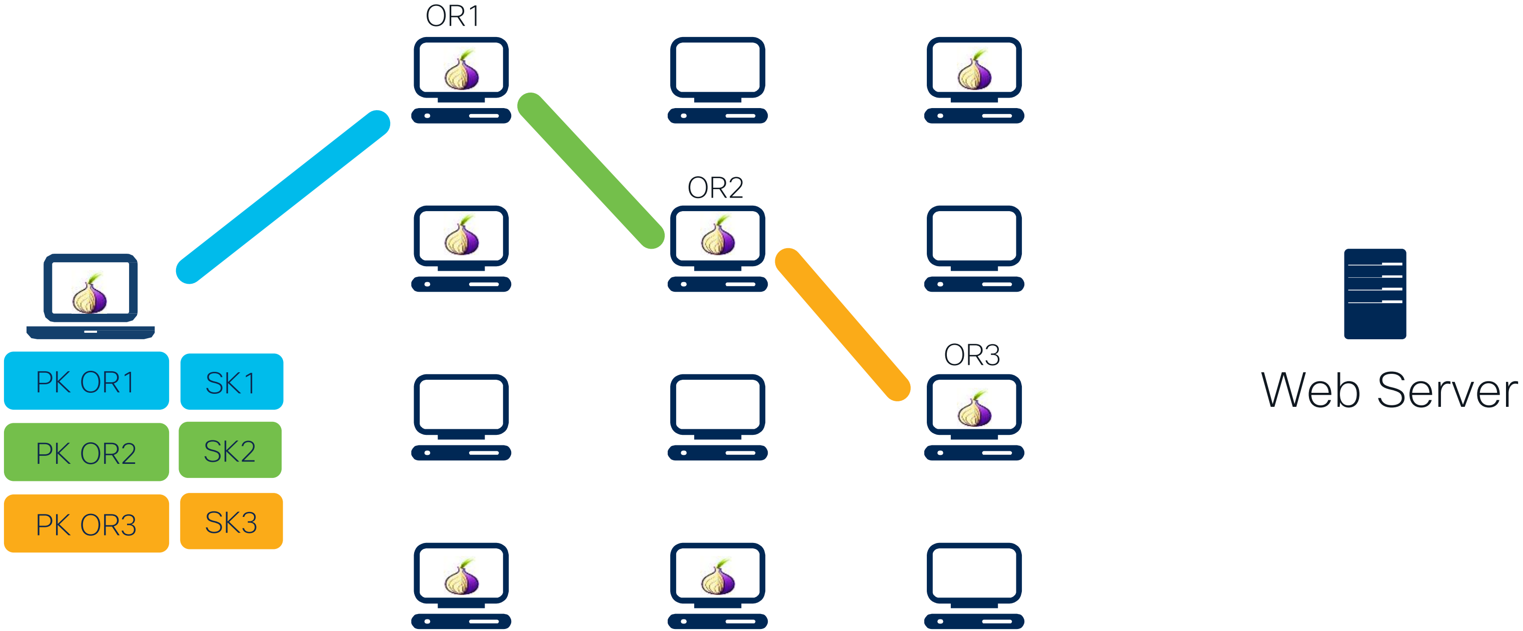
Tor Client sends “relay_extend” to OR1, requesting to extend the circuit to OR2. Keyshare for OR2 is protected by the public key of OR2

Tor Relay



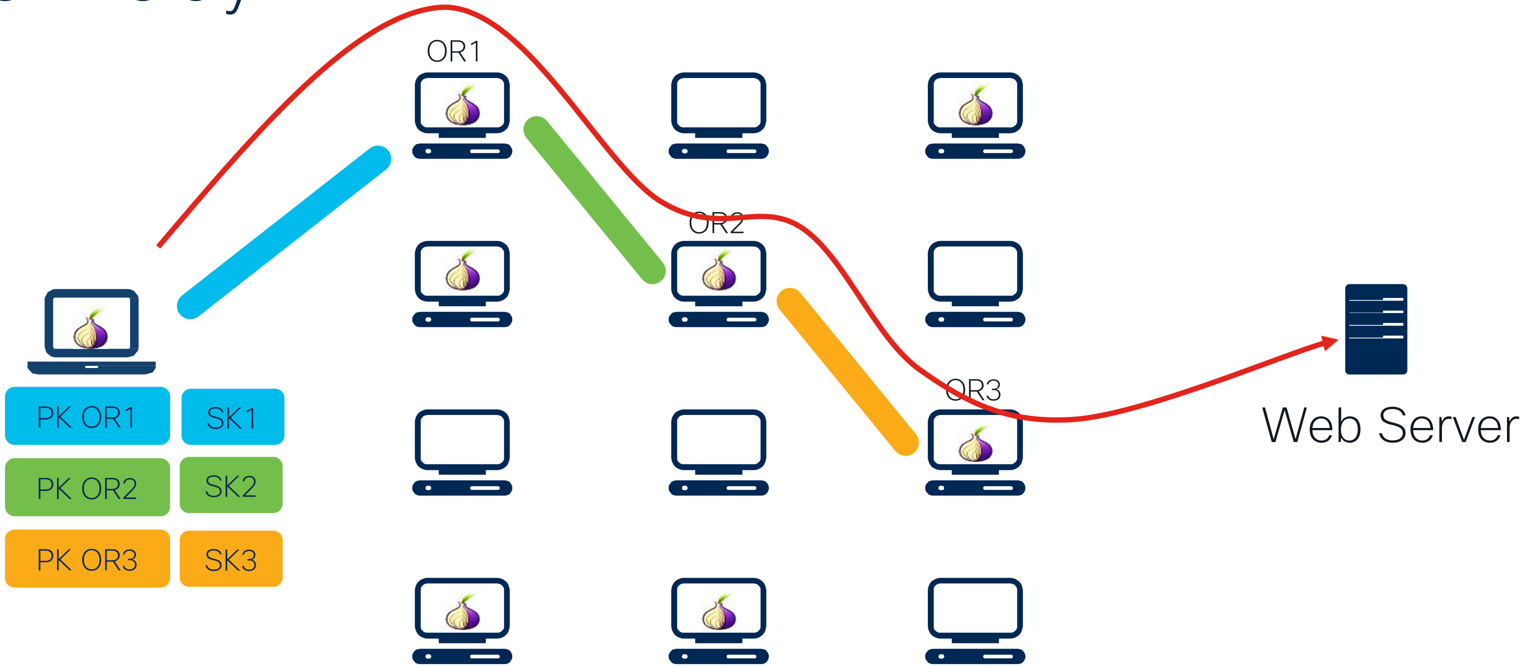
OR1 send “relay_create” to OR2, OR2 responds and circuit with symmetric key is created to OR2

Tor Relay



"relay_extend" to OR3, create a circuit

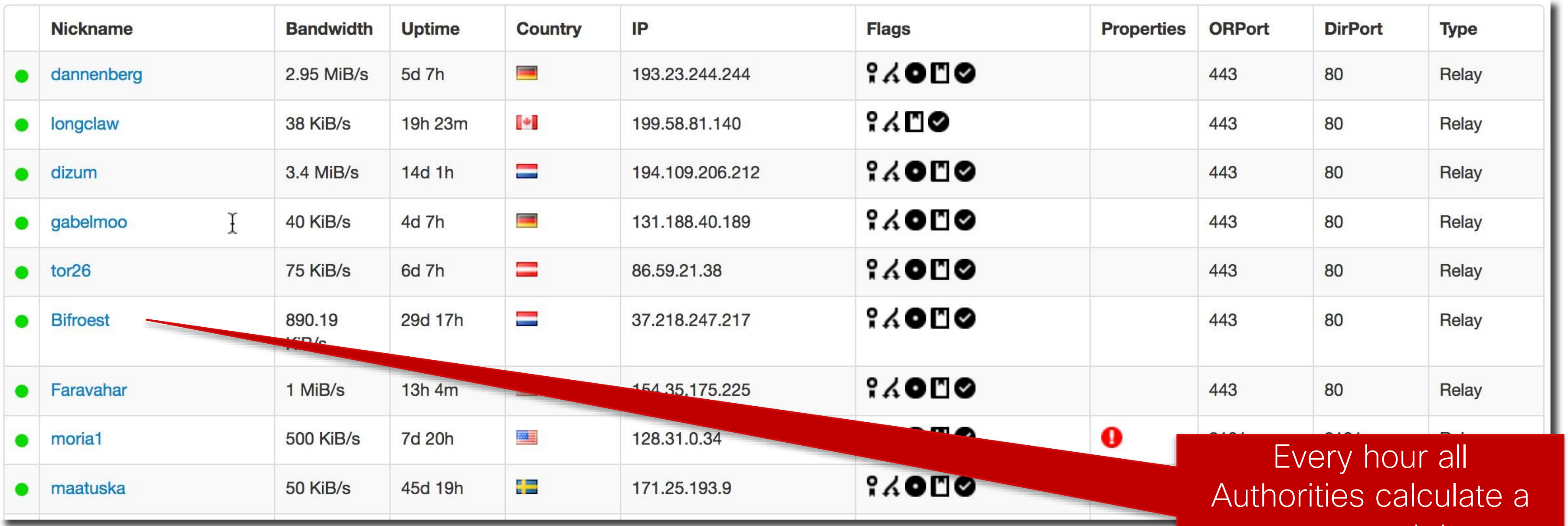
Tor Relay



Web Request follow the circuits

Tor Directory Authorities

https://atlas.torproject.org/#search/flag:authority

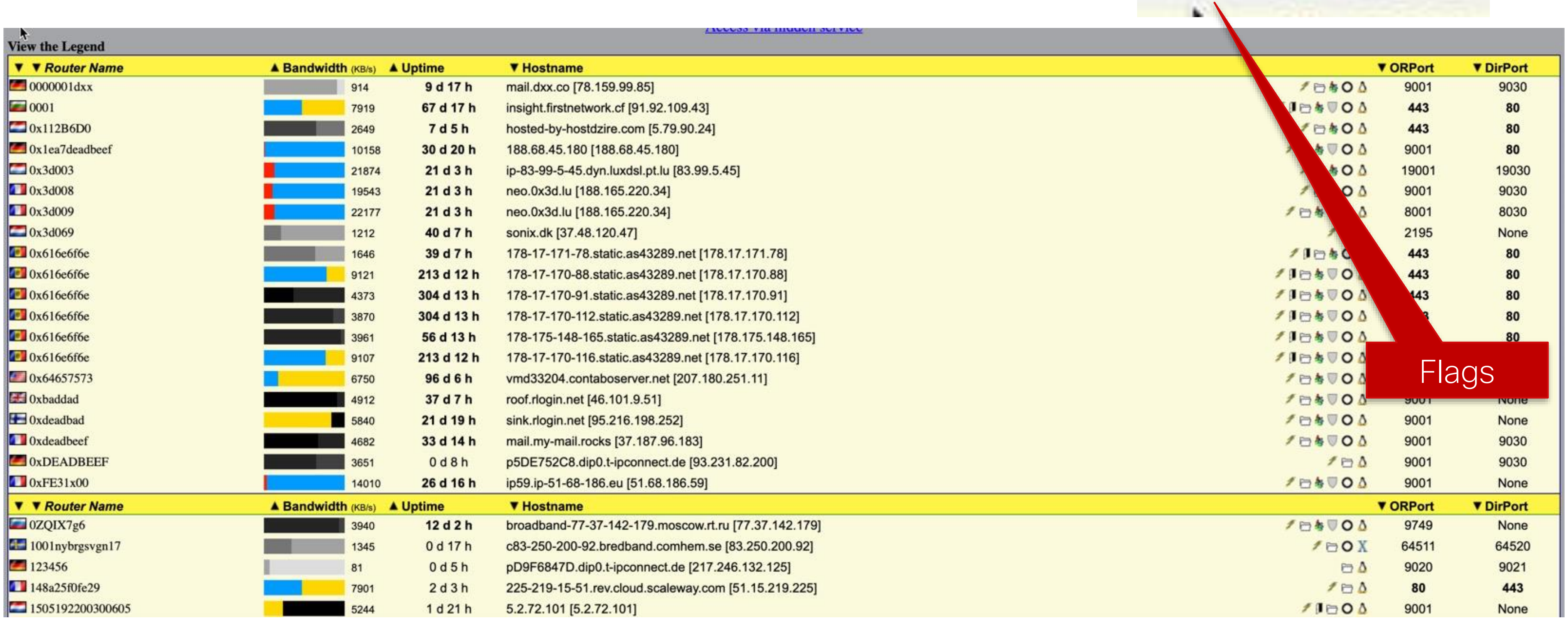


	Nickname	Bandwidth	Uptime	Country	IP	Flags	Properties	ORPort	DirPort	Type
●	dannenberg	2.95 MiB/s	5d 7h	🇩🇪	193.23.244.244	🔑 ⑂ ● □ ✓		443	80	Relay
●	longclaw	38 KiB/s	19h 23m	🇨🇦	199.58.81.140	🔑 ⑂ □ ✓		443	80	Relay
●	dizum	3.4 MiB/s	14d 1h	🇳🇱	194.109.206.212	🔑 ⑂ ● □ ✓		443	80	Relay
●	gabelmoo	40 KiB/s	4d 7h	🇩🇪	131.188.40.189	🔑 ⑂ ● □ ✓		443	80	Relay
●	tor26	75 KiB/s	6d 7h	🇦🇹	86.59.21.38	🔑 ⑂ ● □ ✓		443	80	Relay
●	Bifroest	890.19 KiB/s	29d 17h	🇳🇱	37.218.247.217	🔑 ⑂ ● □ ✓		443	80	Relay
●	Faravahar	1 MiB/s	13h 4m	[illegible]	154.35.175.225	🔑 ⑂ ● □ ✓		443	80	Relay
●	moria1	500 KiB/s	7d 20h	🇺🇸	128.31.0.34	● □ ✓	❗	[illegible]	[illegible]	[illegible]
●	maatuska	50 KiB/s	45d 19h	🇸🇪	171.25.193.9	🔑 ⑂ ● □ ✓				

Every hour all Authorities calculate a common status document called the "consensus"

List of all Tor Relays

https://torstatus.rueckgr.at/

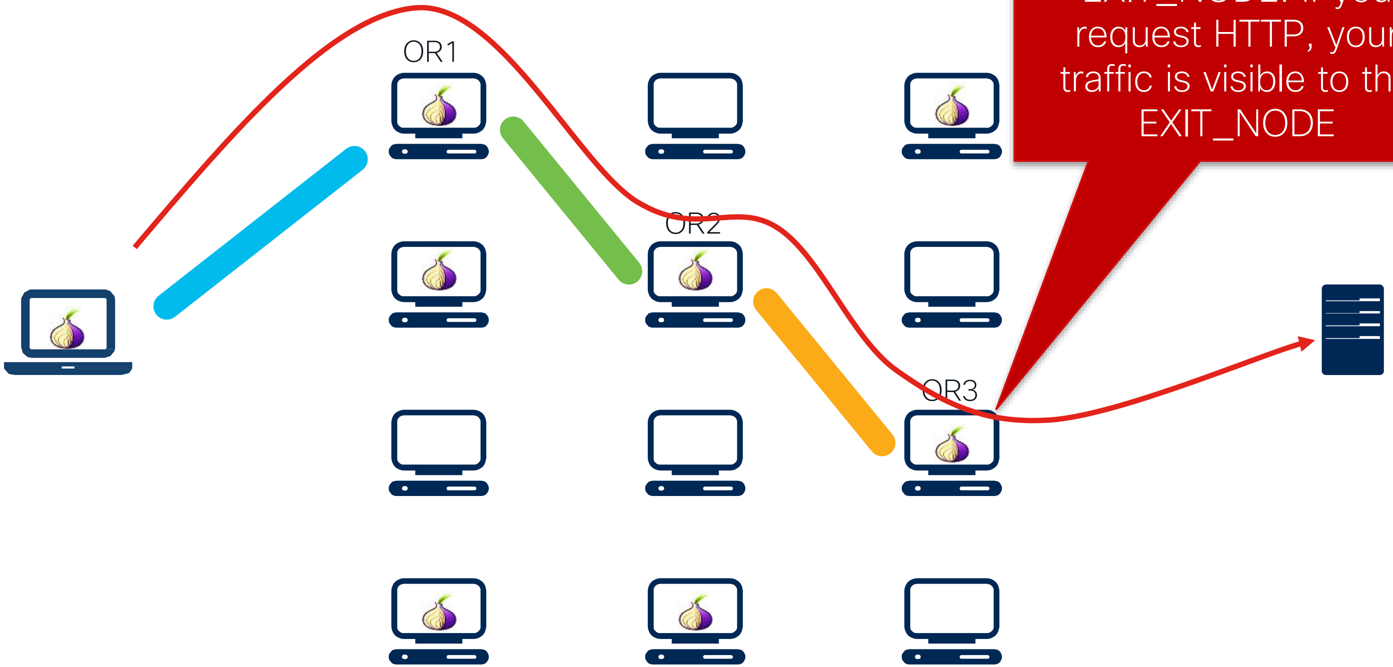

Access via hidden service

View the Legend

Router Name	Bandwidth (KB/s)	Uptime	Hostname	ORPort	DirPort
0000001dxx	914	9 d 17 h	mail.dxx.co [78.159.99.85]	9001	9030
0001	7919	67 d 17 h	insight.firstnetwork.cf [91.92.109.43]	443	80
0x112B6D0	2649	7 d 5 h	hosted-by-hostdzire.com [5.79.90.24]	443	80
0x1ea7deadbeef	10158	30 d 20 h	188.68.45.180 [188.68.45.180]	9001	80
0x3d003	21874	21 d 3 h	ip-83-99-5-45.dyn.luxdsl.pt.lu [83.99.5.45]	19001	19030
0x3d008	19543	21 d 3 h	neo.0x3d.lu [188.165.220.34]	9001	9030
0x3d009	22177	21 d 3 h	neo.0x3d.lu [188.165.220.34]	8001	8030
0x3d069	1212	40 d 7 h	sonix.dk [37.48.120.47]	2195	None
0x616e6f6e	1646	39 d 7 h	178-17-171-78.static.as43289.net [178.17.171.78]	443	80
0x616e6f6e	9121	213 d 12 h	178-17-170-88.static.as43289.net [178.17.170.88]	443	80
0x616e6f6e	4373	304 d 13 h	178-17-170-91.static.as43289.net [178.17.170.91]	443	80
0x616e6f6e	3870	304 d 13 h	178-17-170-112.static.as43289.net [178.17.170.112]	[illegible]	80
0x616e6f6e	3961	56 d 13 h	178-175-148-165.static.as43289.net [178.175.148.165]	[illegible]	80
0x616e6f6e	9107	213 d 12 h	178-17-170-116.static.as43289.net [178.17.170.116]	[illegible]	[illegible]
0x64657573	6750	96 d 6 h	vmd33204.contaboserver.net [207.180.251.11]	[illegible]	[illegible]
0xbaddad	4912	37 d 7 h	roof.rlogin.net [46.101.9.51]	9001	None
0xdeadbad	5840	21 d 19 h	sink.rlogin.net [95.216.198.252]	9001	None
0xdeadbeef	4682	33 d 14 h	mail.my-mail.rocks [37.187.96.183]	9001	9030
0xDEADBEEF	3651	0 d 8 h	p5DE752C8.dip0.t-ipconnect.de [93.231.82.200]	9001	9030
0xFE31x00	14010	26 d 16 h	ip59.ip-51-68-186.eu [51.68.186.59]	9001	None
Router Name	**Bandwidth (KB/s)**	**Uptime**	**Hostname**	**ORPort**	**DirPort**
0ZQIX7g6	3940	12 d 2 h	broadband-77-37-142-179.moscow.rt.ru [77.37.142.179]	9749	None
1001nybrgsvgn17	1345	0 d 17 h	c83-250-200-92.bredband.comhem.se [83.250.200.92]	64511	64520
123456	81	0 d 5 h	pD9F6847D.dip0.t-ipconnect.de [217.246.132.125]	9020	9021
148a25f0fe29	7901	2 d 3 h	225-219-15-51.rev.cloud.scaleway.com [51.15.219.225]	80	443
1505192200300605	5244	1 d 21 h	5.2.72.101 [5.2.72.101]	9001	None

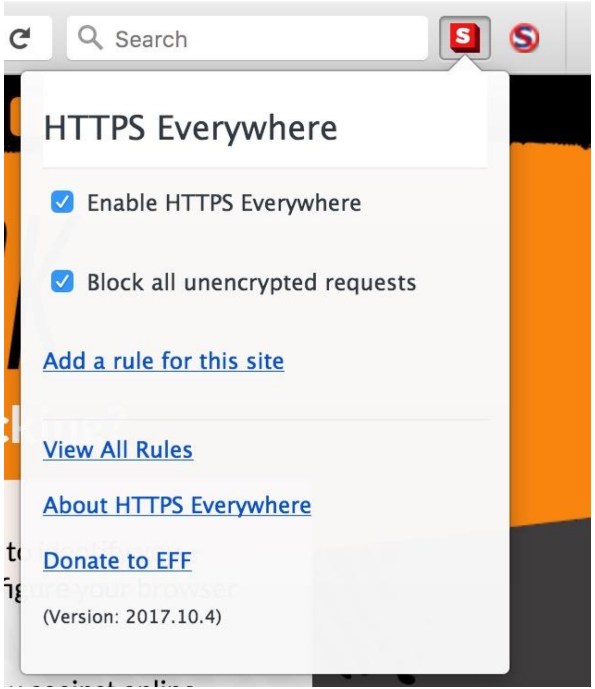
Flags

Tor Relay



EXIT_NODE: if you request HTTP, your traffic is visible to the EXIT_NODE

Tor Browser – Don't leak information!



Search

HTTPS Everywhere

☑ Enable HTTPS Everywhere

☑ Block all unencrypted requests

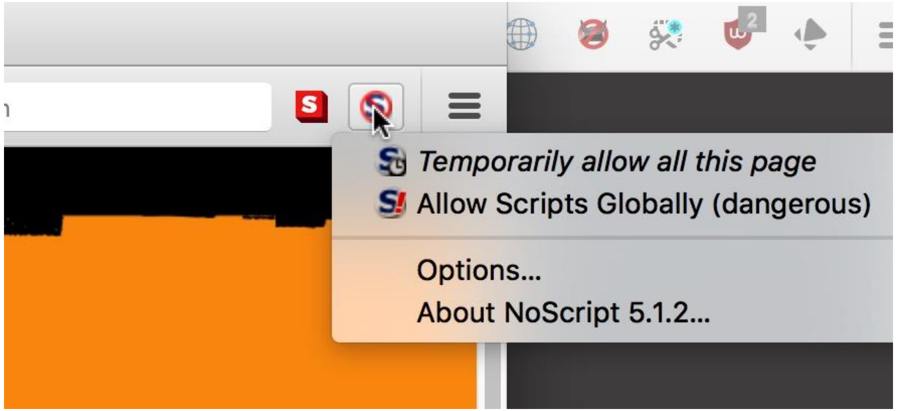
Add a rule for this site

View All Rules

About HTTPS Everywhere

Donate to EFF

(Version: 2017.10.4)



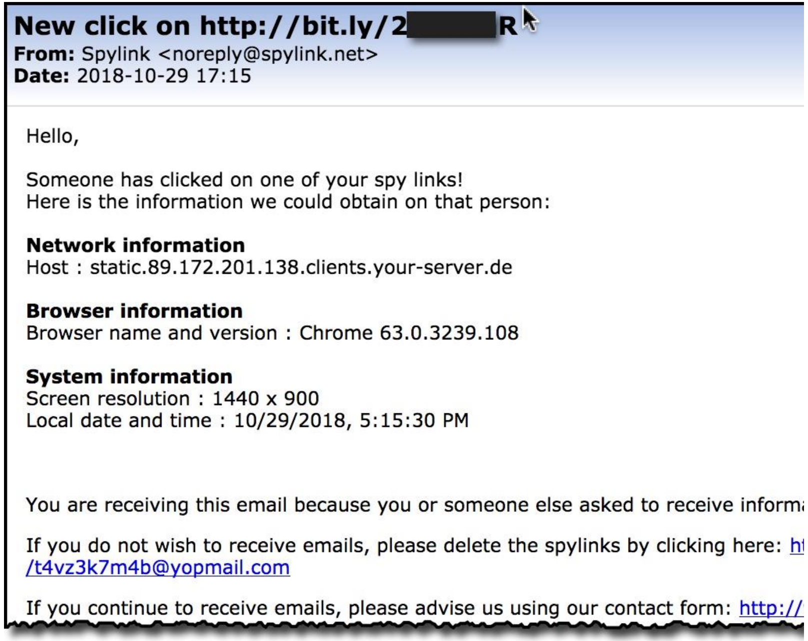
Temporarily allow all this page

Allow Scripts Globally (dangerous)

Options...

About NoScript 5.1.2...

Do your own spylink ☺



New click on http://bit.ly/2[redacted]R
From: Spylink <noreply@spylink.net>
Date: 2018-10-29 17:15

Hello,

Someone has clicked on one of your spy links!
Here is the information we could obtain on that person:

Network information
Host : static.89.172.201.138.clients.your-server.de

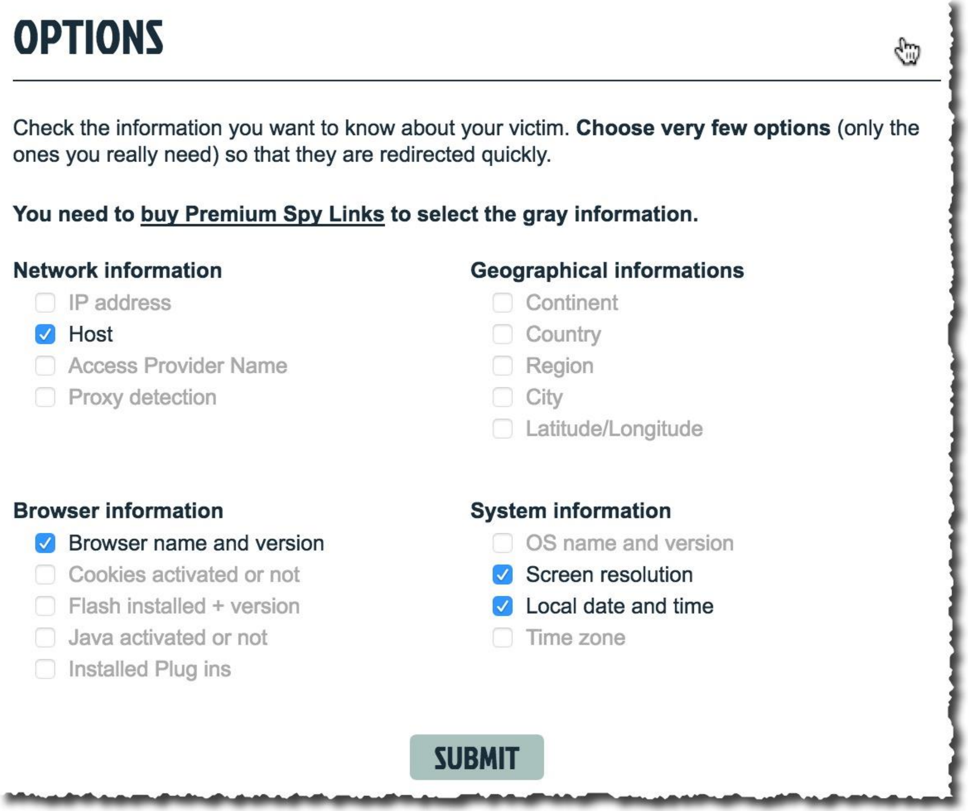
Browser information
Browser name and version : Chrome 63.0.3239.108

System information
Screen resolution : 1440 x 900
Local date and time : 10/29/2018, 5:15:30 PM

You are receiving this email because you or someone else asked to receive informa

If you do not wish to receive emails, please delete the spylinks by clicking here: ht
/t4vz3k7m4b@yopmail.com

If you continue to receive emails, please advise us using our contact form: http://



OPTIONS

Check the information you want to know about your victim. **Choose very few options** (only the ones you really need) so that they are redirected quickly.

You need to buy Premium Spy Links to select the gray information.

Network information
□ IP address
☑ Host
□ Access Provider Name
□ Proxy detection

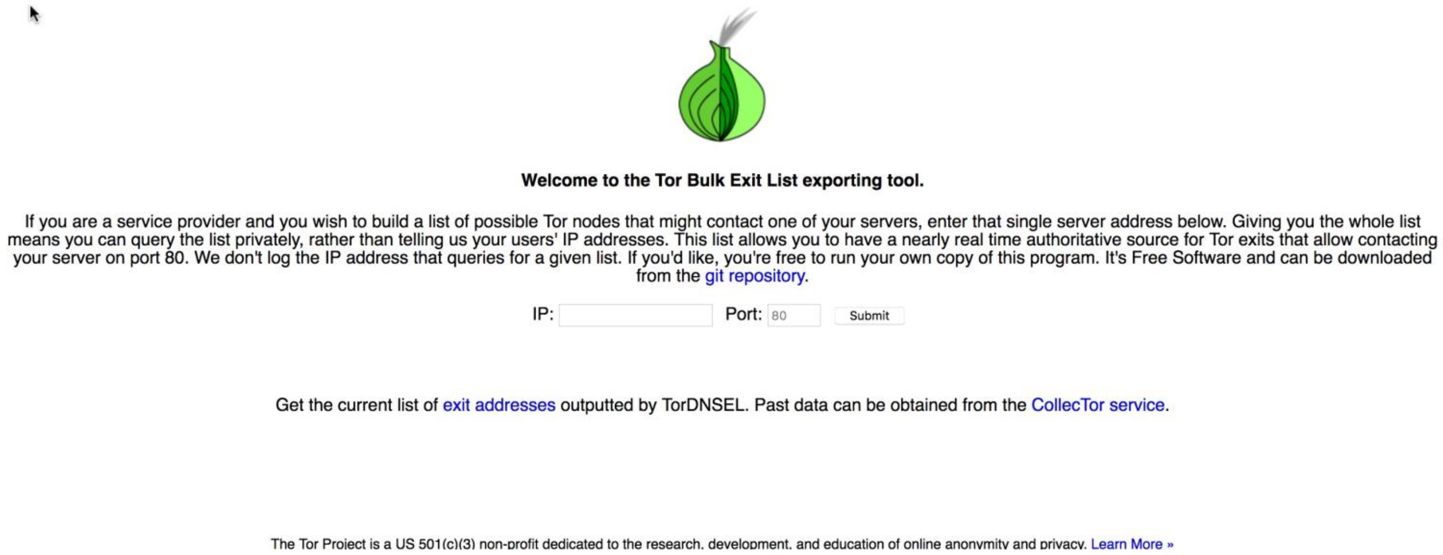
Geographical informations
□ Continent
□ Country
□ Region
□ City
□ Latitude/Longitude

Browser information
☑ Browser name and version
□ Cookies activated or not
□ Flash installed + version
□ Java activated or not
□ Installed Plug ins

System information
□ OS name and version
☑ Screen resolution
☑ Local date and time
□ Time zone

Tor Exit Relay List

https://check.torproject.org/cgi-bin/TorBulkExitList.py



Welcome to the Tor Bulk Exit List exporting tool.

If you are a service provider and you wish to build a list of possible Tor nodes that might contact one of your servers, enter that single server address below. Giving you the whole list means you can query the list privately, rather than telling us your users' IP addresses. This list allows you to have a nearly real time authoritative source for Tor exits that allow contacting your server on port 80. We don't log the IP address that queries for a given list. If you'd like, you're free to run your own copy of this program. It's Free Software and can be downloaded from the git repository.

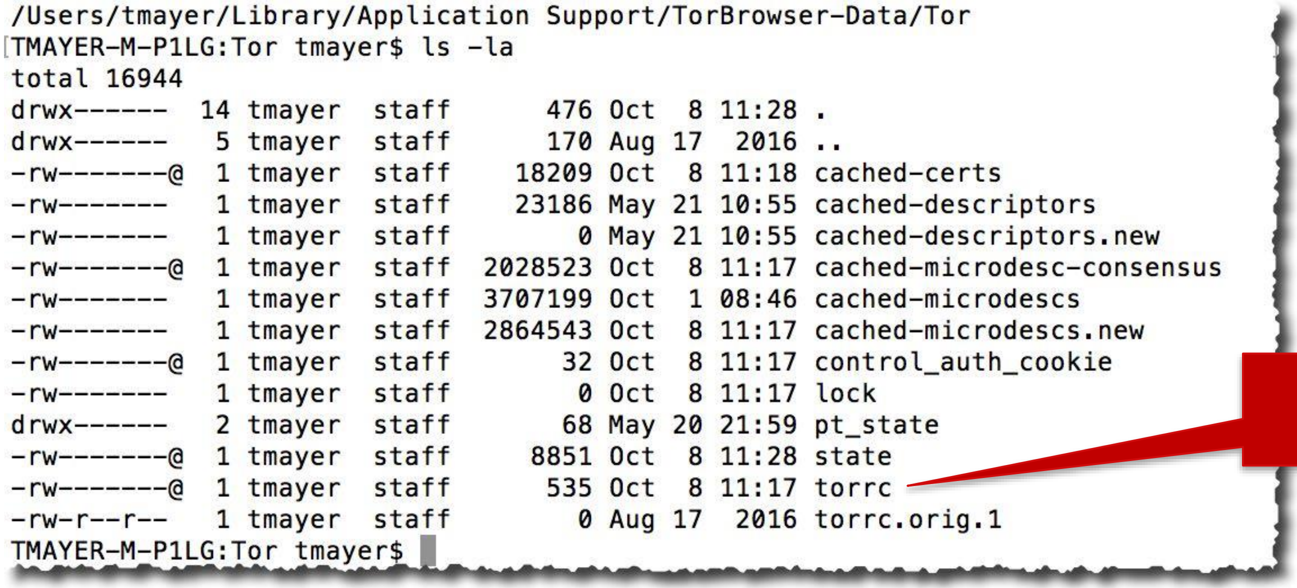
IP: Port: 80 Submit

Get the current list of exit addresses outputted by TorDNSEL. Past data can be obtained from the CollecTor service.

The Tor Project is a US 501(c)(3) non-profit dedicated to the research, development, and education of online anonymity and privacy. Learn More »

Setting up a TOR Relay or Bridge

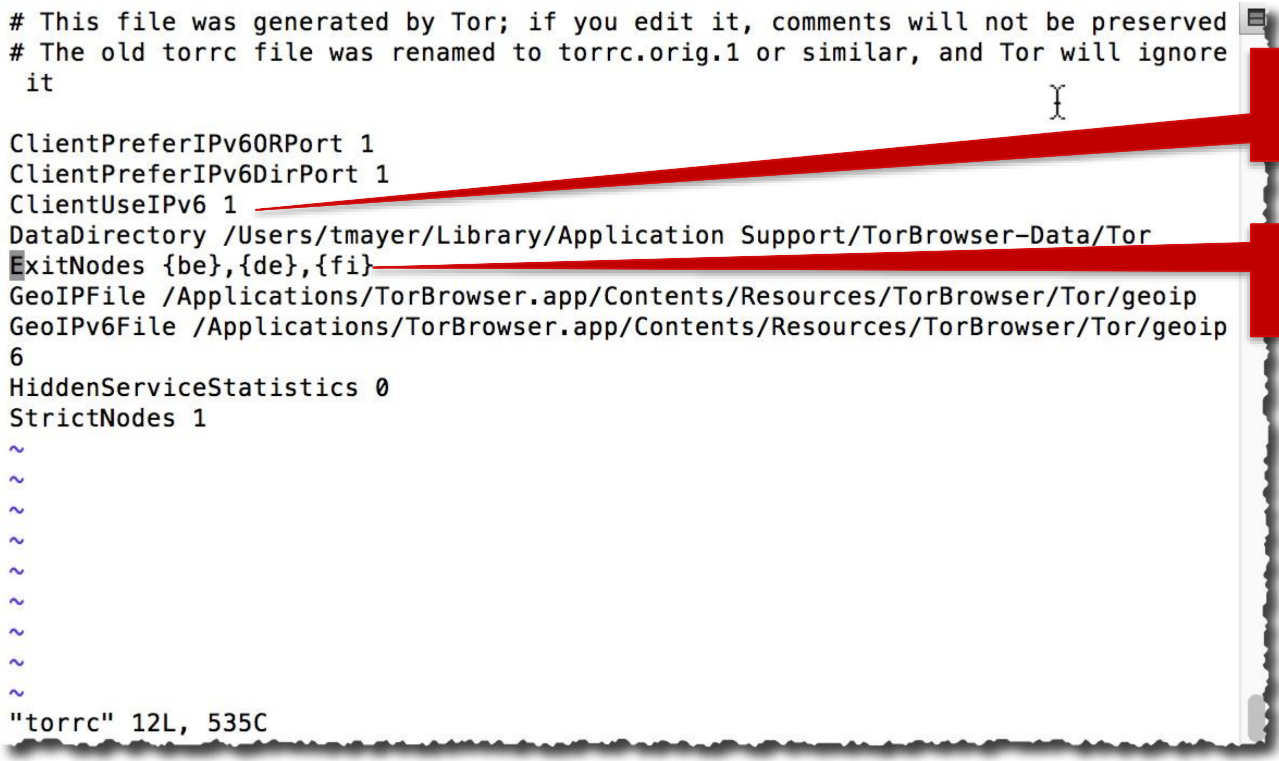
Customizing Tor



```
/Users/tmayer/Library/Application Support/TorBrowser-Data/Tor
[TMAYER-M-P1LG:Tor tmayer$ ls -la
total 16944
drwx------   14 tmayer  staff      476 Oct  8 11:28 .
drwx------    5 tmayer  staff      170 Aug 17  2016 ..
-rw-------@   1 tmayer  staff    18209 Oct  8 11:18 cached-certs
-rw-------    1 tmayer  staff    23186 May 21 10:55 cached-descriptors
-rw-------    1 tmayer  staff        0 May 21 10:55 cached-descriptors.new
-rw-------@   1 tmayer  staff  2028523 Oct  8 11:17 cached-microdesc-consensus
-rw-------    1 tmayer  staff  3707199 Oct  1 08:46 cached-microdescs
-rw-------    1 tmayer  staff  2864543 Oct  8 11:17 cached-microdescs.new
-rw-------@   1 tmayer  staff       32 Oct  8 11:17 control_auth_cookie
-rw-------    1 tmayer  staff        0 Oct  8 11:17 lock
drwx------    2 tmayer  staff       68 May 20 21:59 pt_state
-rw-------@   1 tmayer  staff     8851 Oct  8 11:28 state
-rw-------@   1 tmayer  staff      535 Oct  8 11:17 torrc
-rw-r--r--    1 tmayer  staff        0 Aug 17  2016 torrc.orig.1
TMAYER-M-P1LG:Tor tmayer$
```

“torrc” = config file

Customizing Tor (2)

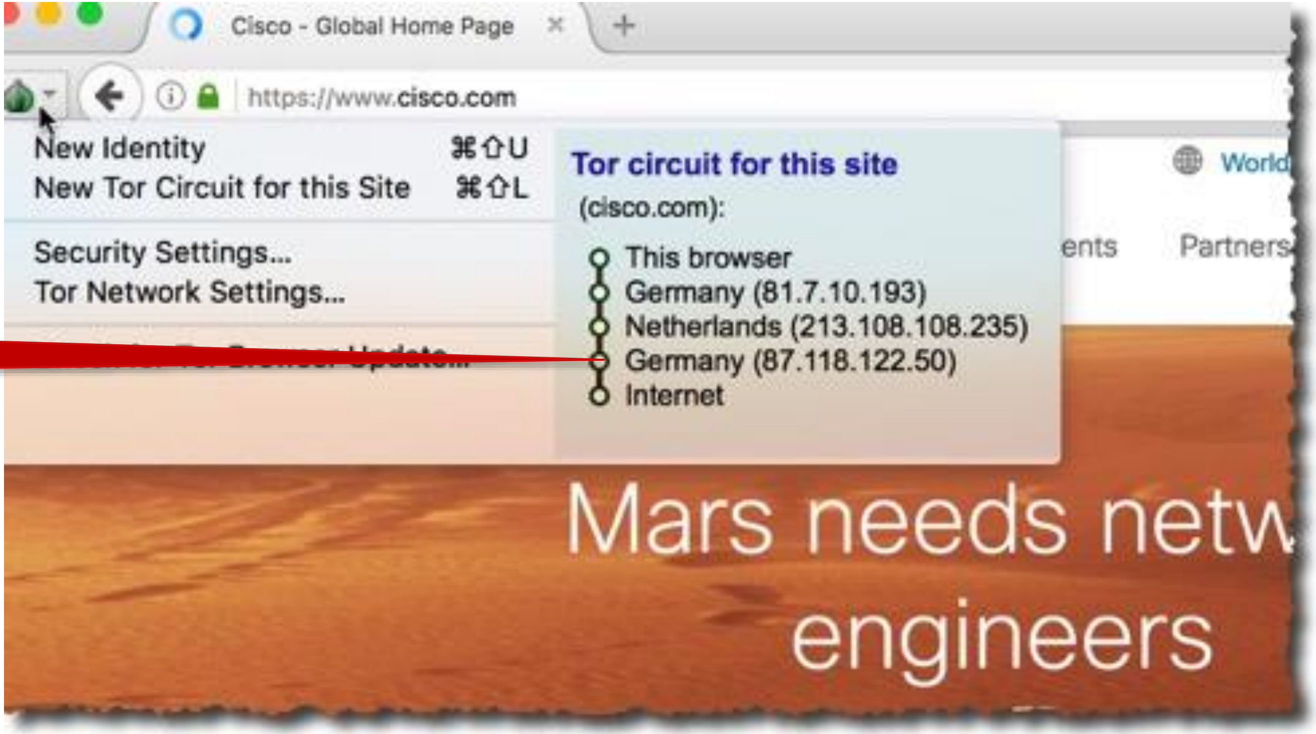


```
# This file was generated by Tor; if you edit it, comments will not be preserved
# The old torrc file was renamed to torrc.orig.1 or similar, and Tor will ignore
 it

ClientPreferIPv6ORPort 1
ClientPreferIPv6DirPort 1
ClientUseIPv6 1
DataDirectory /Users/tmayer/Library/Application Support/TorBrowser-Data/Tor
ExitNodes {be},{de},{fi}
GeoIPFile /Applications/TorBrowser.app/Contents/Resources/TorBrowser/Tor/geoip
GeoIPv6File /Applications/TorBrowser.app/Contents/Resources/TorBrowser/Tor/geoip
6
HiddenServiceStatistics 0
StrictNodes 1
~
~
~
~
~
~
~
~
~
"torrc" 12L, 535C
```

Also use IPv6 relays

Define Geolocation of your ExitNodes

Customizing Tor (3)



Tor circuit for this site
(cisco.com):

- This browser
- Germany (81.7.10.193)
- Netherlands (213.108.108.235)
- Germany (87.118.122.50)
- Internet

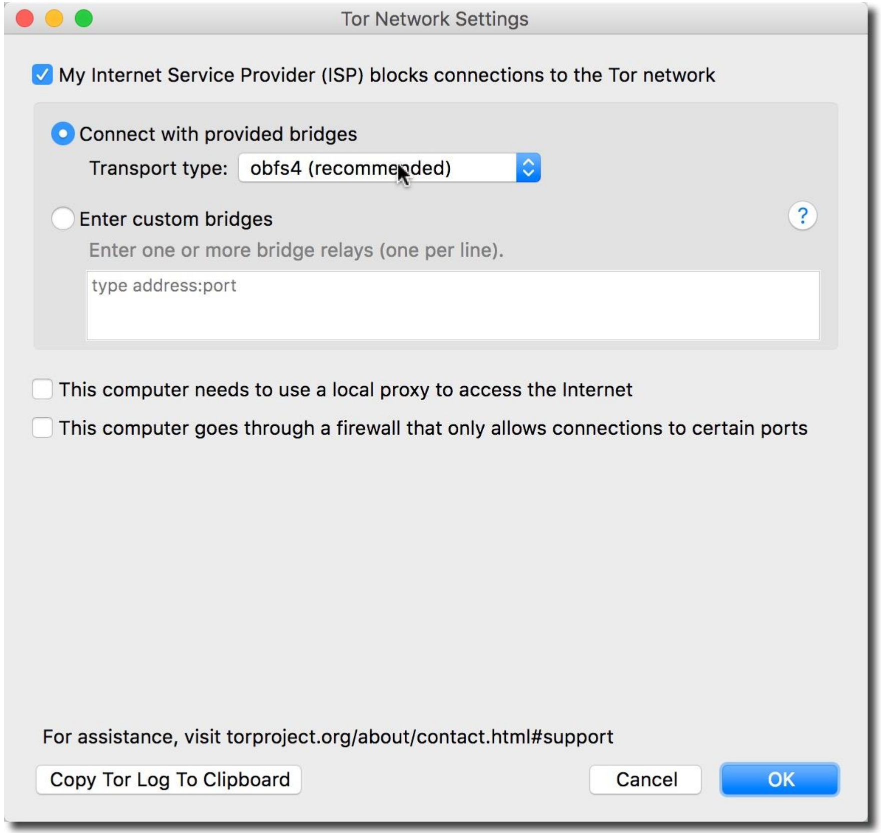
ExitNode from Germany

Bridges

Bridges are relays that are not announced in the directory servers

You can request bridges but will not get the full list

3 bridges are provided



☑ My Internet Service Provider (ISP) blocks connections to the Tor network

● Connect with provided bridges

Transport type: obfs4 (recommended)

○ Enter custom bridges

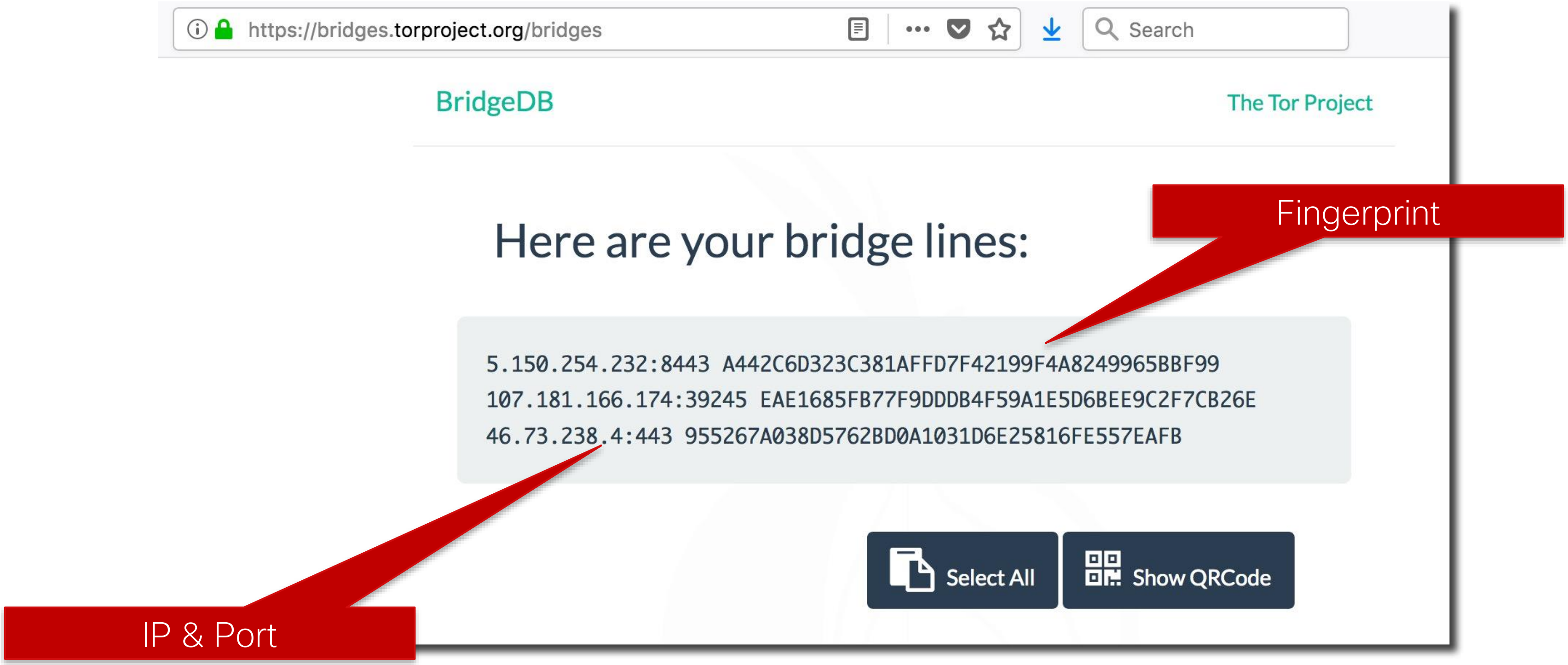
Enter one or more bridge relays (one per line).

□ This computer needs to use a local proxy to access the Internet

□ This computer goes through a firewall that only allows connections to certain ports

For assistance, visit torproject.org/about/contact.html#support

Custom Bridges



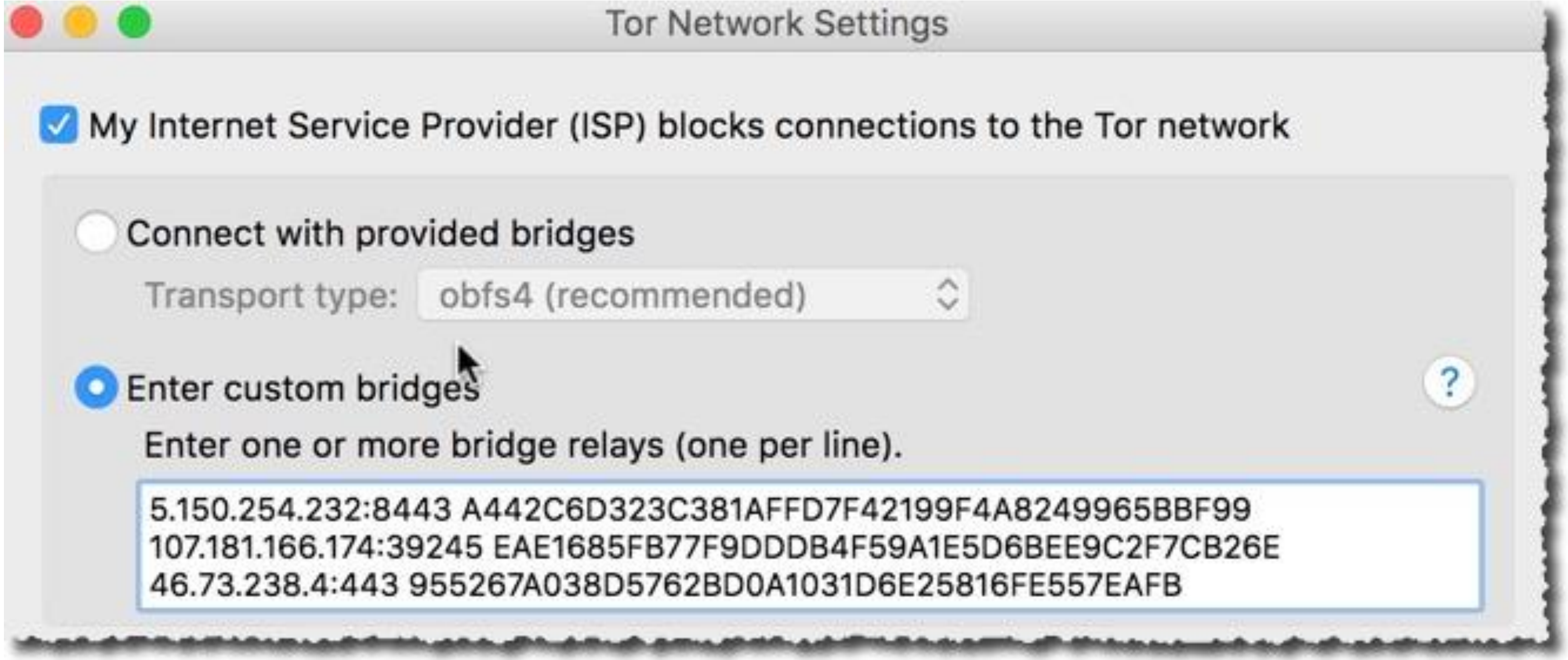
Here are your bridge lines:

```
5.150.254.232:8443 A442C6D323C381AFFD7F42199F4A8249965BBF99
107.181.166.174:39245 EAE1685FB77F9DDDB4F59A1E5D6BEE9C2F7CB26E
46.73.238.4:443 955267A038D5762BD0A1031D6E25816FE557EAFB
```

Fingerprint

IP & Port

Custom Bridges



Tor Network Settings

☑ My Internet Service Provider (ISP) blocks connections to the Tor network

○ Connect with provided bridges

Transport type: obfs4 (recommended)

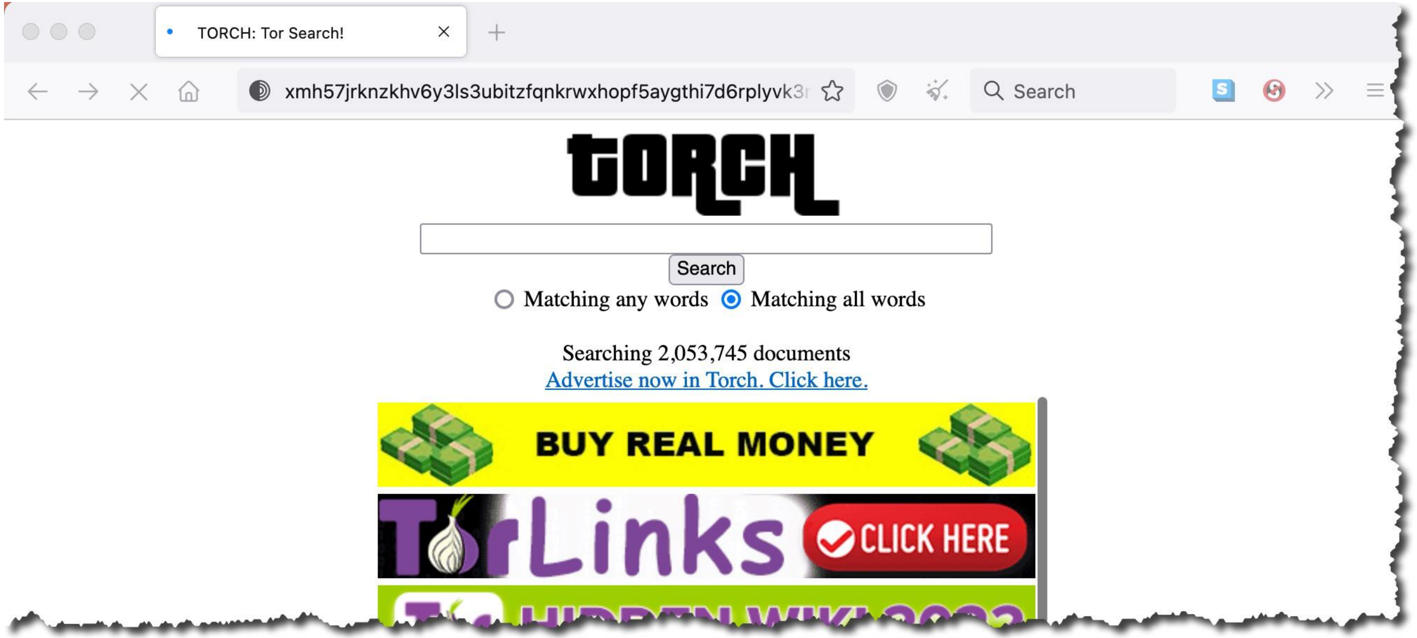
● Enter custom bridges

Enter one or more bridge relays (one per line).

```
5.150.254.232:8443 A442C6D323C381AFFD7F42199F4A8249965BBF99
107.181.166.174:39245 EAE1685FB77F9DDDB4F59A1E5D6BEE9C2F7CB26E
46.73.238.4:443 955267A038D5762BD0A1031D6E25816FE557EAFB
```

Hidden Websites – ”.onion” links

http://xmh57jrknzkhv6y3ls3ubitzfqnkrwxhopf5aygthi7d6rplyvk3noyd.onion



○ Matching any words ● Matching all words

Searching 2,053,745 documents

Advertise now in Torch. Click here.

Let’s go shopping! NOT

Darknet: Use Cases

Criminal Activities

- Financial crime
- Sexual abuse
- Illegal goods and services, e.g. drugs, guns
- Cyber crime: hacking services, malware as a service
- Human trafficking
- Extremism

Legitimate Activities

- Intelligence community
- Whistleblowing and journalism to protect the the sources' identity
- Ordinary citizens evading restrictions by their government
- Privacy-cautious individuals who value anonymity

Activities on the Darknet

Torbox – torbox36ijlcevujx7mjb4oiusvwgvmue7jfn2cvutwa6kl6to3uyqad.onion

Mail2Tor – mail2torjgmxgexntbrmhvgluavhj7ouul5yar6ylbvjkxwqf6ixkwyd.onion

- Shops and Markets
- File Sharing
- Messaging Services:
  - Mail Services, e.g., ProtonMail, TorBox/Mail2Tor (darknet exclusive)
- Forums:
  - Some hacking forums are available on the darknet and surface web, e.g., XSS , others can only be accessed from the darknet, e.g., Dread
  - Focus of cyber crime: Social engineering, malware selling, requests for hacking, hacking tutorials, etc.

Darknet Price Index 2022

Service	Price
Cloned American Express with PIN	$25
Credit card details, account balance up to $5 000	$120
Stolen online banking logins (min $100 in account)	$35
Hacked facebook account	$45
Hacked Gmail account	$65
Netflix Account - 1 year subscription	$25
Netherlands Passport	$3 800
Email database dumps (10 million US email addresses)	$120
Malware (depending on quality, etc.)	$500-5 000
DDoS attack (unprotected website 10-50k requests per second, 1 week	$450

All right! I got it!
Show me now...

My Secret Identity

TheMaskedCucumber@mail2tor.com

(do not forget your hoodie and mask)

Running your own relay

The Ultimate Ubuntu TOR Installation Guide

```
curl -sS https://deb.torproject.org/torproject.org/A3C4F0F979CAA22CDBA8F512EE8CBC9E886DDD89.asc |
sudo gpg --dearmor -o /etc/apt/trusted.gpg.d/torproject.gpg
```

```
sudo add-apt-repository deb http://deb.torproject.org/torproject.org/ `(lsb_release -c -s)` main
```

lsb_release gets the proper OS release name (the fancy Ubuntu release name like Jammy, Kinetic, ...)

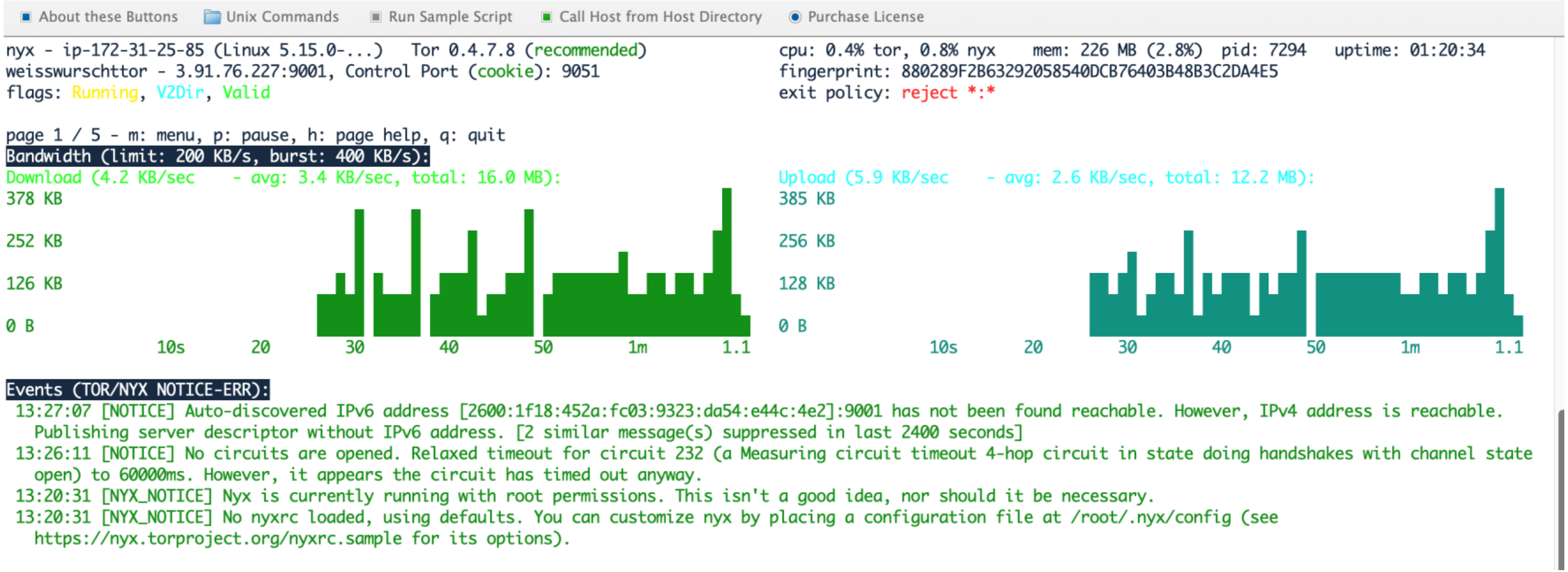
```
sudo apt update
sudo apt upgrade
sudo apt install tor
sudo apt install nyx
```

Steps for becoming a relay

- service tor stop
- vi /etc/tor/torrc
  - ORPort 9001
  - ORPort [insert your IPv6 Address]:9001
  - Address [own IP or Domain]
  - Nickname [some name]
  - ControlPort 9051
  - CookieAuthentication 1
  - RelayBandwidthRate 100 KB # Throttle traffic to 100KB/s (800Kbps)
  - RelayBandwidthBurst 200 KB # But allow bursts up to 200KB/s (1600Kbps)
  - ContactInfo toby < TheMaskedCucumber AT mail2tor DOT com>
  - ExitPolicy reject *:*

Do not participate as an Exit Gateway

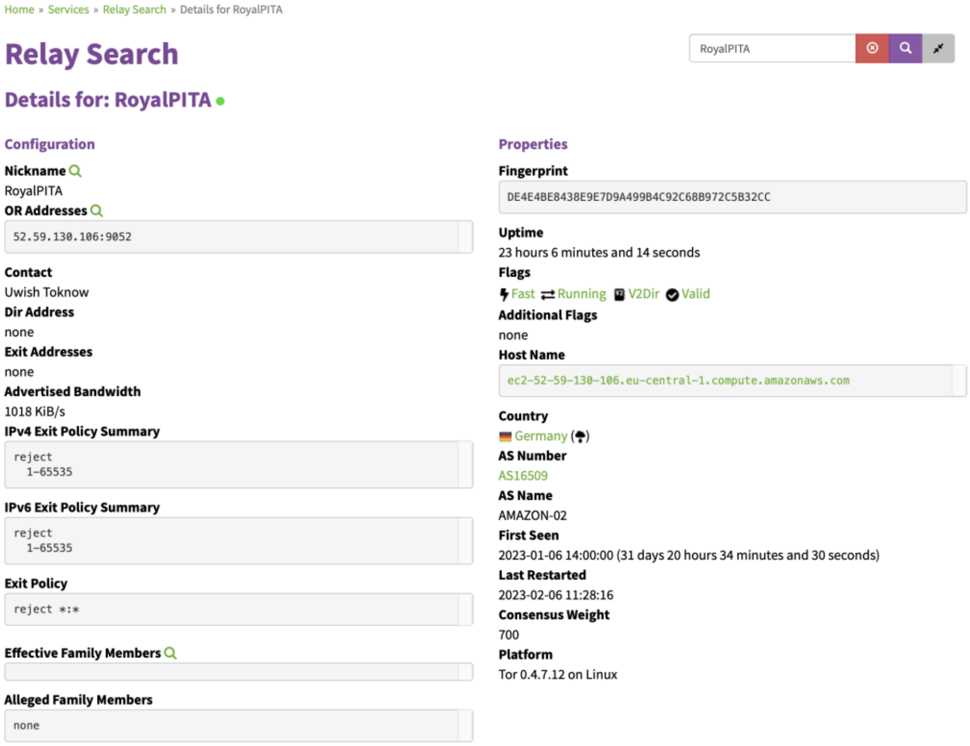
After installation



```
nyx - ip-172-31-25-85 (Linux 5.15.0-...)   Tor 0.4.7.8 (recommended)            cpu: 0.4% tor, 0.8% nyx    mem: 226 MB (2.8%)  pid: 7294   uptime: 01:20:34
weisswurschttor - 3.91.76.227:9001, Control Port (cookie): 9051                  fingerprint: 880289F2B63292058540DCB76403B48B3C2DA4E5
flags: Running, V2Dir, Valid                                                     exit policy: reject *:*

page 1 / 5 - m: menu, p: pause, h: page help, q: quit
Bandwidth (limit: 200 KB/s, burst: 400 KB/s):
Download (4.2 KB/sec    - avg: 3.4 KB/sec, total: 16.0 MB):                   Upload (5.9 KB/sec    - avg: 2.6 KB/sec, total: 12.2 MB):
378 KB                                                                        385 KB

252 KB                                                                        256 KB

126 KB                                                                        128 KB

0 B                                                                           0 B
                10s       20        30        40        50        1m        1.1               10s       20        30        40        50        1m        1.1

Events (TOR/NYX NOTICE-ERR):
 13:27:07 [NOTICE] Auto-discovered IPv6 address [2600:1f18:452a:fc03:9323:da54:e44c:4e2]:9001 has not been found reachable. However, IPv4 address is reachable.
   Publishing server descriptor without IPv6 address. [2 similar message(s) suppressed in last 2400 seconds]
 13:26:11 [NOTICE] No circuits are opened. Relaxed timeout for circuit 232 (a Measuring circuit timeout 4-hop circuit in state doing handshakes with channel state
   open) to 60000ms. However, it appears the circuit has timed out anyway.
 13:20:31 [NYX_NOTICE] Nyx is currently running with root permissions. This isn't a good idea, nor should it be necessary.
 13:20:31 [NYX_NOTICE] No nyxrc loaded, using defaults. You can customize nyx by placing a configuration file at /root/.nyx/config (see
   https://nyx.torproject.org/nyxrc.sample for its options).
```

My relay

https://metrics.torproject.org



Home » Services » Relay Search » Details for RoyalPITA

Relay Search

RoyalPITA

Details for: RoyalPITA ●

Configuration

Nickname

RoyalPITA

OR Addresses

```
52.59.130.106:9052
```

Contact

Uwish Toknow

Dir Address

none

Exit Addresses

none

Advertised Bandwidth

1018 KiB/s

IPv4 Exit Policy Summary

```
reject
  1-65535
```

IPv6 Exit Policy Summary

```
reject
  1-65535
```

Exit Policy

```
reject *:*
```

Effective Family Members

Alleged Family Members

```
none
```

Properties

Fingerprint

```
DE4E4BE8438E9E7D9A499B4C92C68B972C5B32CC
```

Uptime

23 hours 6 minutes and 14 seconds

Flags

Fast ⇄ Running V2Dir ✓ Valid

Additional Flags

none

Host Name

```
ec2-52-59-130-106.eu-central-1.compute.amazonaws.com
```

Country

Germany (♦)

AS Number

AS16509

AS Name

AMAZON-02

First Seen

2023-01-06 14:00:00 (31 days 20 hours 34 minutes and 30 seconds)

Last Restarted

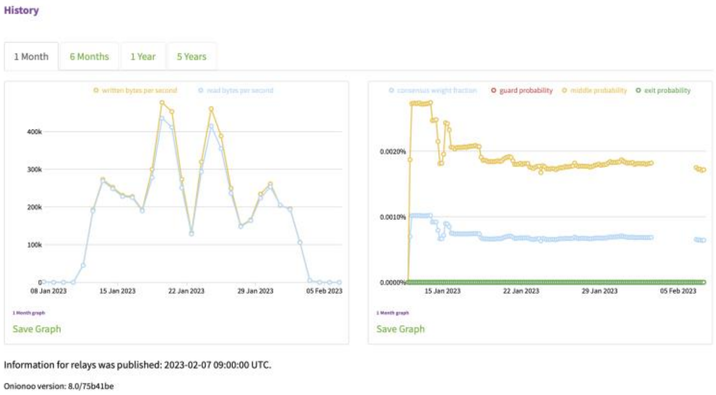
2023-02-06 11:28:16

Consensus Weight

700

Platform

Tor 0.4.7.12 on Linux



History

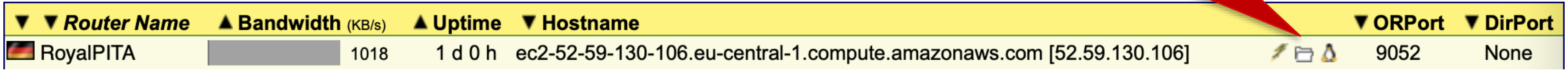
Information for relays was published: 2023-02-07 09:00:00 UTC.

Onionoo version: 8.0/75b41be

Torstatus

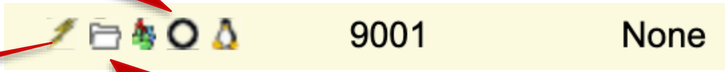
https://torstatus.rueckgr.at/

Nearly no flags assigned



▼	▼ Router Name	▲ Bandwidth (KB/s)	▲ Uptime	▼ Hostname		▼ ORPort	▼ DirPort
	RoyalPITA	1018	1 d 0 h	ec2-52-59-130-106.eu-central-1.compute.amazonaws.com [52.59.130.106]		9052	None

Got the ”stable” flag



	9001	None

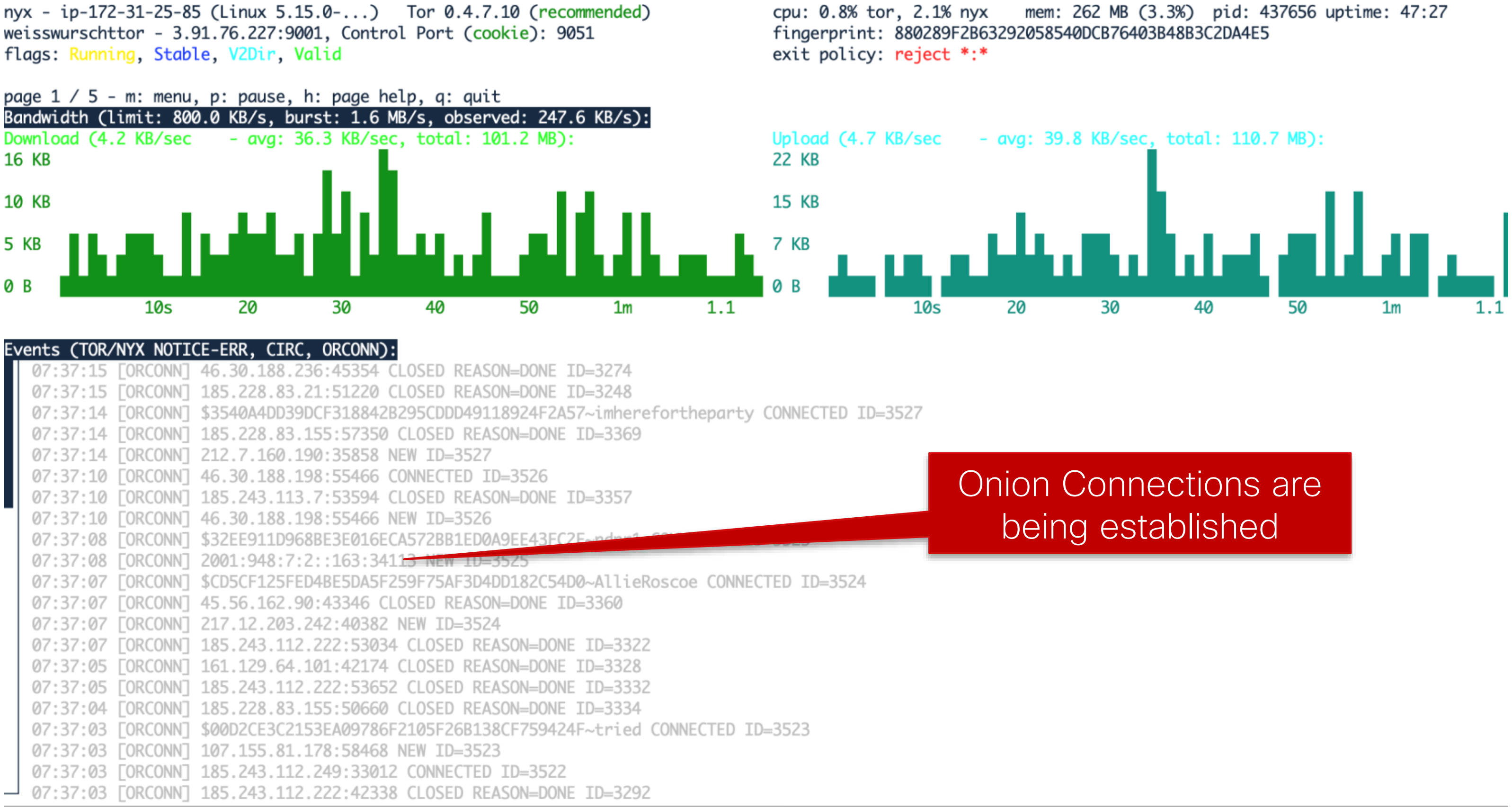
Got the ”fast” flag

Got the ”HS Dir Server” flag

Phases of becoming a relay

- Days 0-3: the unmeasured phase.
- Days 3-8: network authorities start the remote measurement phase (the ramp-up guard phase).
- Days 8-68: guard phase (where load counter intuitively drops and then rises higher).

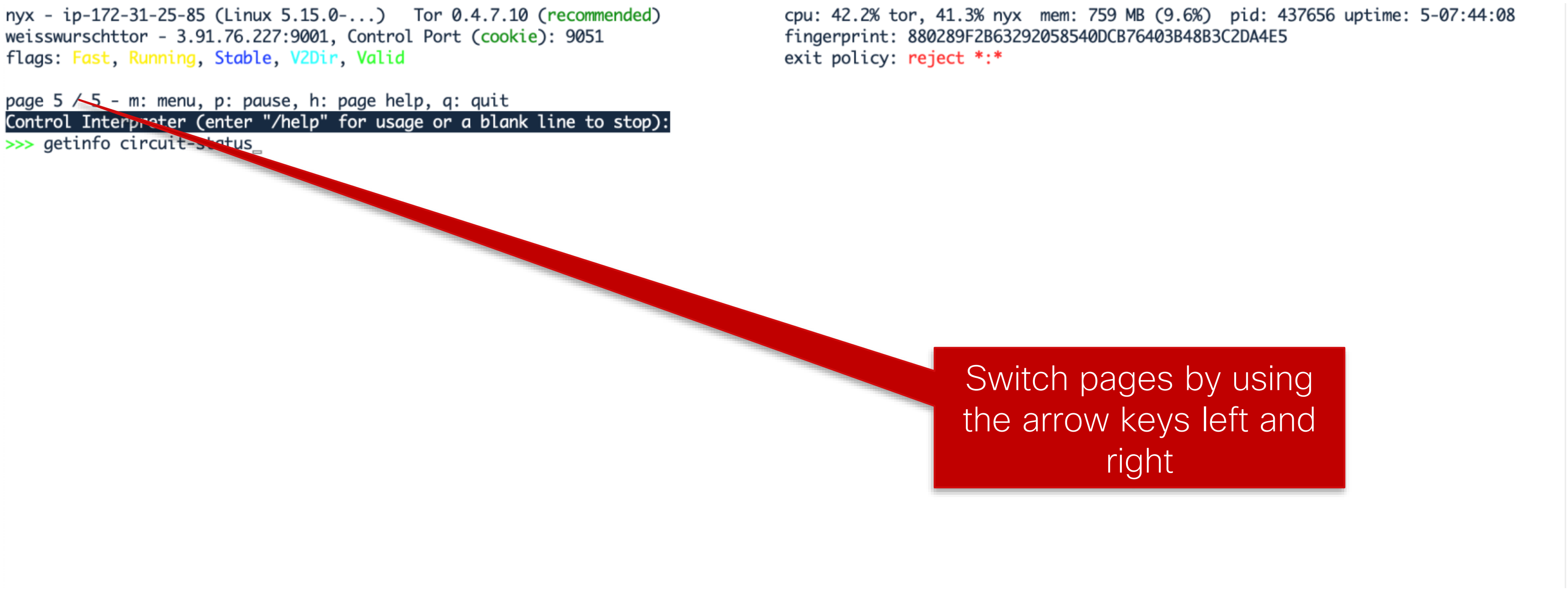
Torstatus



```
nyx - ip-172-31-25-85 (Linux 5.15.0-...)   Tor 0.4.7.10 (recommended)      cpu: 0.8% tor, 2.1% nyx    mem: 262 MB (3.3%)  pid: 437656 uptime: 47:27
weisswurschttor - 3.91.76.227:9001, Control Port (cookie): 9051          fingerprint: 880289F2B63292058540DCB76403B48B3C2DA4E5
flags: Running, Stable, V2Dir, Valid                                      exit policy: reject *:*

page 1 / 5 - m: menu, p: pause, h: page help, q: quit
Bandwidth (limit: 800.0 KB/s, burst: 1.6 MB/s, observed: 247.6 KB/s):
Download (4.2 KB/sec     - avg: 36.3 KB/sec, total: 101.2 MB):            Upload (4.7 KB/sec     - avg: 39.8 KB/sec, total: 110.7 MB):
16 KB                                                                     22 KB

10 KB                                                                     15 KB

5 KB                                                                      7 KB

0 B                                                                       0 B
          10s      20       30       40       50       1m       1.1               10s      20       30       40       50       1m       1.1

Events (TOR/NYX NOTICE-ERR, CIRC, ORCONN):
  07:37:15 [ORCONN] 46.30.188.236:45354 CLOSED REASON=DONE ID=3274
  07:37:15 [ORCONN] 185.228.83.21:51220 CLOSED REASON=DONE ID=3248
  07:37:14 [ORCONN] $3540A4DD39DCF318842B295CDDD49118924F2A57~imherefortheparty CONNECTED ID=3527
  07:37:14 [ORCONN] 185.228.83.155:57350 CLOSED REASON=DONE ID=3369
  07:37:14 [ORCONN] 212.7.160.190:35858 NEW ID=3527
  07:37:10 [ORCONN] 46.30.188.198:55466 CONNECTED ID=3526
  07:37:10 [ORCONN] 185.243.113.7:53594 CLOSED REASON=DONE ID=3357
  07:37:10 [ORCONN] 46.30.188.198:55466 NEW ID=3526
  07:37:08 [ORCONN] $32EE911D968BE3E016ECA572BB1ED0A9EE43FC2F~ndnr1
  07:37:08 [ORCONN] 2001:948:7:2::163:34113 NEW ID=3525
  07:37:07 [ORCONN] $CD5CF125FED4BE5DA5F259F75AF3D4DD182C54D0~AllieRoscoe CONNECTED ID=3524
  07:37:07 [ORCONN] 45.56.162.90:43346 CLOSED REASON=DONE ID=3360
  07:37:07 [ORCONN] 217.12.203.242:40382 NEW ID=3524
  07:37:07 [ORCONN] 185.243.112.222:53034 CLOSED REASON=DONE ID=3322
  07:37:05 [ORCONN] 161.129.64.101:42174 CLOSED REASON=DONE ID=3328
  07:37:05 [ORCONN] 185.243.112.222:53652 CLOSED REASON=DONE ID=3332
  07:37:04 [ORCONN] 185.228.83.155:50660 CLOSED REASON=DONE ID=3334
  07:37:03 [ORCONN] $00D2CE3C2153EA09786F2105F26B138CF759424F~tried CONNECTED ID=3523
  07:37:03 [ORCONN] 107.155.81.178:58468 NEW ID=3523
  07:37:03 [ORCONN] 185.243.112.249:33012 CONNECTED ID=3522
  07:37:03 [ORCONN] 185.243.112.222:42338 CLOSED REASON=DONE ID=3292
```

Onion Connections are being established

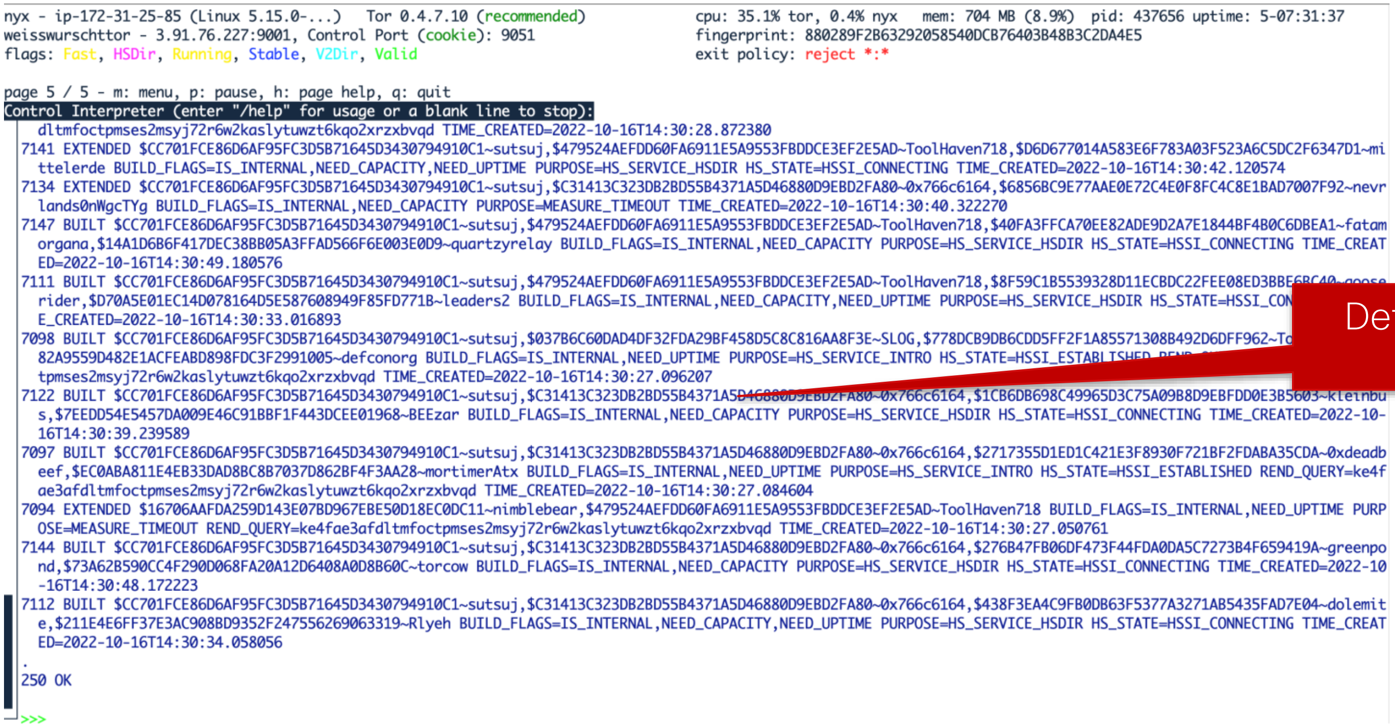
Connect to the Control Port Console



```
nyx - ip-172-31-25-85 (Linux 5.15.0-...)   Tor 0.4.7.10 (recommended)          cpu: 42.2% tor, 41.3% nyx  mem: 759 MB (9.6%)  pid: 437656 uptime: 5-07:44:08
weisswurschttor - 3.91.76.227:9001, Control Port (cookie): 9051                fingerprint: 880289F2B63292058540DCB76403B48B3C2DA4E5
flags: Fast, Running, Stable, V2Dir, Valid                                     exit policy: reject *:*

page 5 / 5 - m: menu, p: pause, h: page help, q: quit
Control Interpreter (enter "/help" for usage or a blank line to stop):
>>> getinfo circuit-status_
```

Switch pages by using the arrow keys left and right

Detailed Circuit view via Tor Control Port



```
nyx - ip-172-31-25-85 (Linux 5.15.0-...)   Tor 0.4.7.10 (recommended)            cpu: 35.1% tor, 0.4% nyx   mem: 704 MB (8.9%)  pid: 437656 uptime: 5-07:31:37
weisswurschttor - 3.91.76.227:9001, Control Port (cookie): 9051                  fingerprint: 880289F2B63292058540DCB76403B48B3C2DA4E5
flags: Fast, HSDir, Running, Stable, V2Dir, Valid                                exit policy: reject *:*

page 5 / 5 - m: menu, p: pause, h: page help, q: quit
Control Interpreter (enter "/help" for usage or a blank line to stop):
   dltmfoctpmses2msyj72r6w2kaslytuwzt6kqo2xrzxbvqd TIME_CREATED=2022-10-16T14:30:28.872380
 7141 EXTENDED $CC701FCE86D6AF95FC3D5B71645D3430794910C1~sutsuj,$479524AEFDD60FA6911E5A9553FBDDCE3EF2E5AD~ToolHaven718,$D6D677014A583E6F783A03F523A6C5DC2F6347D1~mi
   ttelerde BUILD_FLAGS=IS_INTERNAL,NEED_CAPACITY,NEED_UPTIME PURPOSE=HS_SERVICE_HSDIR HS_STATE=HSSI_CONNECTING TIME_CREATED=2022-10-16T14:30:42.120574
 7134 EXTENDED $CC701FCE86D6AF95FC3D5B71645D3430794910C1~sutsuj,$C31413C323DB2BD55B4371A5D46880D9EBD2FA80~0x766c6164,$6856BC9E77AAE0E72C4E0F8FC4C8E1BAD7007F92~nevr
   lands0nWgcTYg BUILD_FLAGS=IS_INTERNAL,NEED_CAPACITY PURPOSE=MEASURE_TIMEOUT TIME_CREATED=2022-10-16T14:30:40.322270
 7147 BUILT $CC701FCE86D6AF95FC3D5B71645D3430794910C1~sutsuj,$479524AEFDD60FA6911E5A9553FBDDCE3EF2E5AD~ToolHaven718,$40FA3FFCA70EE82ADE9D2A7E1844BF4B0C6DBEA1~fatam
   organa,$14A1D6B6F417DEC38BB05A3FFAD566F6E003E0D9~quartzyrelay BUILD_FLAGS=IS_INTERNAL,NEED_CAPACITY PURPOSE=HS_SERVICE_HSDIR HS_STATE=HSSI_CONNECTING TIME_CREAT
   ED=2022-10-16T14:30:49.180576
 7111 BUILT $CC701FCE86D6AF95FC3D5B71645D3430794910C1~sutsuj,$479524AEFDD60FA6911E5A9553FBDDCE3EF2E5AD~ToolHaven718,$8F59C1B5539328D11ECBDC22FEE08ED3BBE6BC40~goose
   rider,$D70A5E01EC14D078164D5E587608949F85FD771B~leaders2 BUILD_FLAGS=IS_INTERNAL,NEED_CAPACITY,NEED_UPTIME PURPOSE=HS_SERVICE_HSDIR HS_STATE=HSSI_CON
   E_CREATED=2022-10-16T14:30:33.016893
 7098 BUILT $CC701FCE86D6AF95FC3D5B71645D3430794910C1~sutsuj,$037B6C60DAD4DF32FDA29BF458D5C8C816AA8F3E~SLOG,$778DCB9DB6CDD5FF2F1A85571308B492D6DFF962~To
   82A9559D482E1ACFEABD898FDC3F2991005~defconorg BUILD_FLAGS=IS_INTERNAL,NEED_UPTIME PURPOSE=HS_SERVICE_INTRO HS_STATE=HSSI_ESTABLISHED
   tpmses2msyj72r6w2kaslytuwzt6kqo2xrzxbvqd TIME_CREATED=2022-10-16T14:30:27.096207
 7122 BUILT $CC701FCE86D6AF95FC3D5B71645D3430794910C1~sutsuj,$C31413C323DB2BD55B4371A5D46880D9EBD2FA80~0x766c6164,$1CB6DB698C49965D3C75A09B8D9EBFDD0E3B5603~kleinbu
   s,$7EEDD54E5457DA009E46C91BBF1F443DCEE01968~BEEzar BUILD_FLAGS=IS_INTERNAL,NEED_CAPACITY PURPOSE=HS_SERVICE_HSDIR HS_STATE=HSSI_CONNECTING TIME_CREATED=2022-10-
   16T14:30:39.239589
 7097 BUILT $CC701FCE86D6AF95FC3D5B71645D3430794910C1~sutsuj,$C31413C323DB2BD55B4371A5D46880D9EBD2FA80~0x766c6164,$2717355D1ED1C421E3F8930F721BF2FDABA35CDA~0xdeadb
   eef,$EC0ABA811E4EB33DAD8BC8B7037D862BF4F3AA28~mortimerAtx BUILD_FLAGS=IS_INTERNAL,NEED_UPTIME PURPOSE=HS_SERVICE_INTRO HS_STATE=HSSI_ESTABLISHED REND_QUERY=ke4f
   ae3afdltmfoctpmses2msyj72r6w2kaslytuwzt6kqo2xrzxbvqd TIME_CREATED=2022-10-16T14:30:27.084604
 7094 EXTENDED $16706AAFDA259D143E07BD967EBE50D18EC0DC11~nimblebear,$479524AEFDD60FA6911E5A9553FBDDCE3EF2E5AD~ToolHaven718 BUILD_FLAGS=IS_INTERNAL,NEED_UPTIME PURP
   OSE=MEASURE_TIMEOUT REND_QUERY=ke4fae3afdltmfoctpmses2msyj72r6w2kaslytuwzt6kqo2xrzxbvqd TIME_CREATED=2022-10-16T14:30:27.050761
 7144 BUILT $CC701FCE86D6AF95FC3D5B71645D3430794910C1~sutsuj,$C31413C323DB2BD55B4371A5D46880D9EBD2FA80~0x766c6164,$276B47FB06DF473F44FDA0DA5C7273B4F659419A~greenpo
   nd,$73A62B590CC4F290D068FA20A12D6408A0D8B60C~torcow BUILD_FLAGS=IS_INTERNAL,NEED_CAPACITY PURPOSE=HS_SERVICE_HSDIR HS_STATE=HSSI_CONNECTING TIME_CREATED=2022-10
   -16T14:30:48.172223
 7112 BUILT $CC701FCE86D6AF95FC3D5B71645D3430794910C1~sutsuj,$C31413C323DB2BD55B4371A5D46880D9EBD2FA80~0x766c6164,$438F3EA4C9FB0DB63F5377A3271AB5435FAD7E04~dolemit
   e,$211E4E6FF37E3AC908BD9352F247556269063319~Rlyeh BUILD_FLAGS=IS_INTERNAL,NEED_CAPACITY,NEED_UPTIME PURPOSE=HS_SERVICE_HSDIR HS_STATE=HSSI_CONNECTING TIME_CREAT
   ED=2022-10-16T14:30:34.058056
 .
 250 OK

>>>
```

Detailed view on the circuits

Some Control fun ;)

https://iphelix.medium.com/hacking-the-tor-control-protocol-fb844db6a606

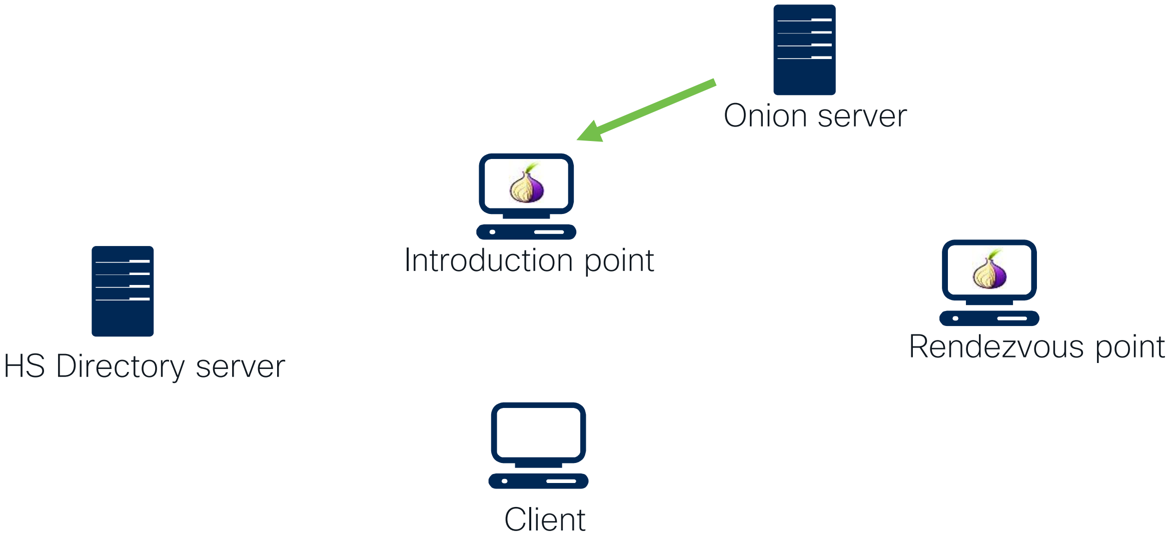
mapaddress www.cnn.com=www.bbc.co.uk

Redirect all traffic for CNN to BBC ;)

(Need to be an exit node for this)

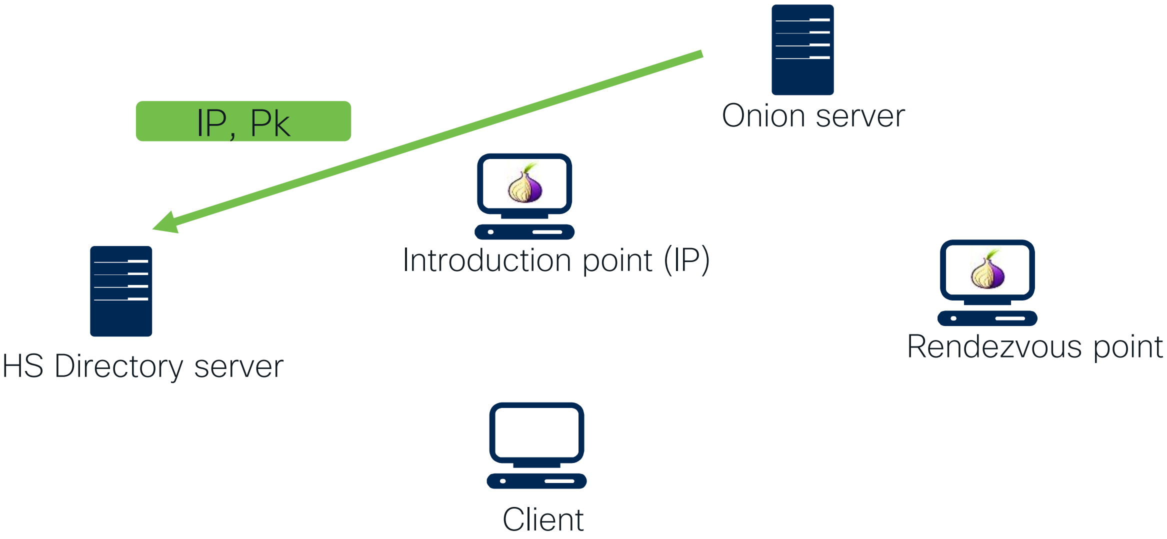
Onionrouting & Hidden Services

Onionrouting



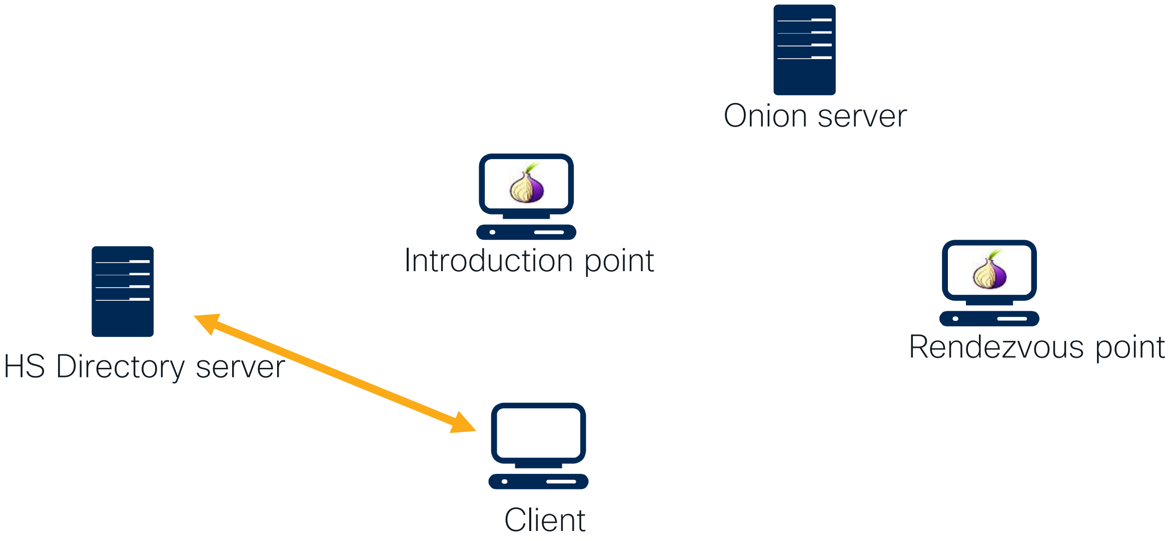
Setup hidden service (create public and private key) and create a circuit to chosen Introduction point(s)

Onionrouting (2)



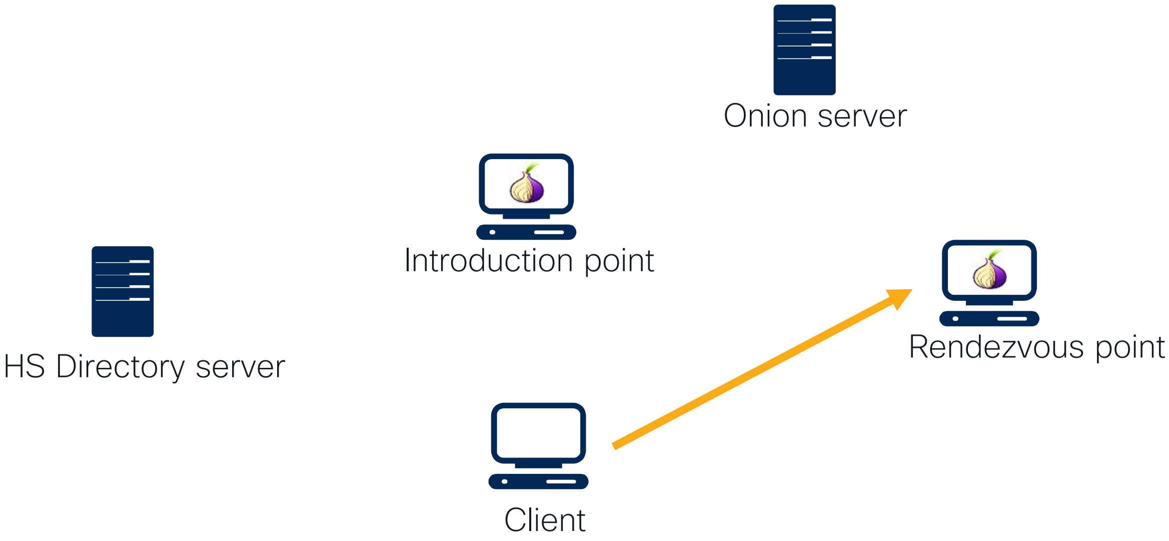
Publish hidden service in six of the directory servers. The servers are calculated based on a function including the consensus status document and the “.onion” address. Repeat once a day (different HSDirs…)

Onionrouting (3)



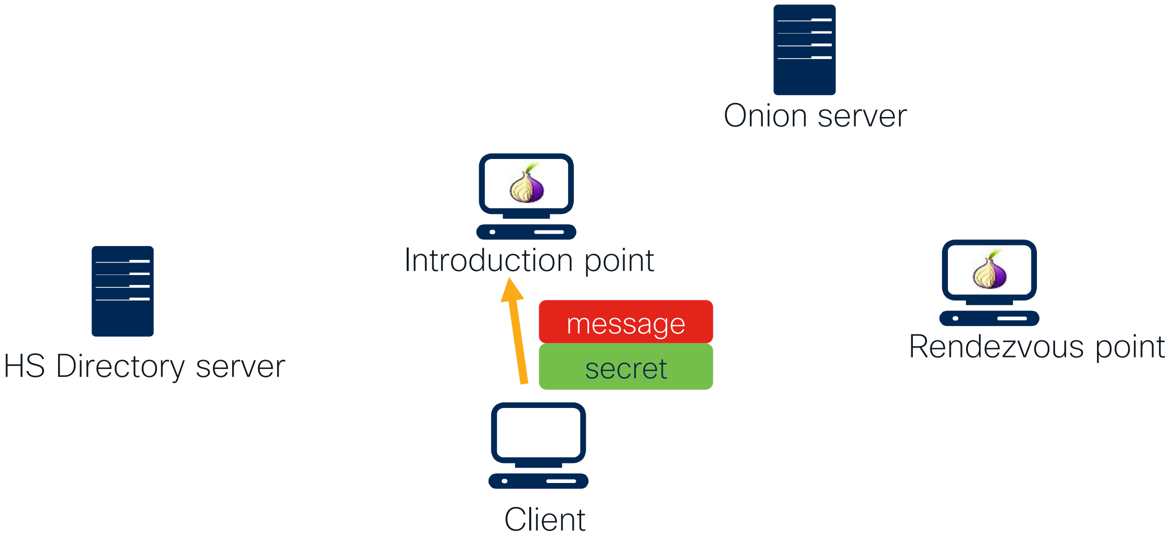
Client asks one of the directory server for the hidden service.
Client gets the public key and the Introduction Points for that service.

Onionrouting (4)



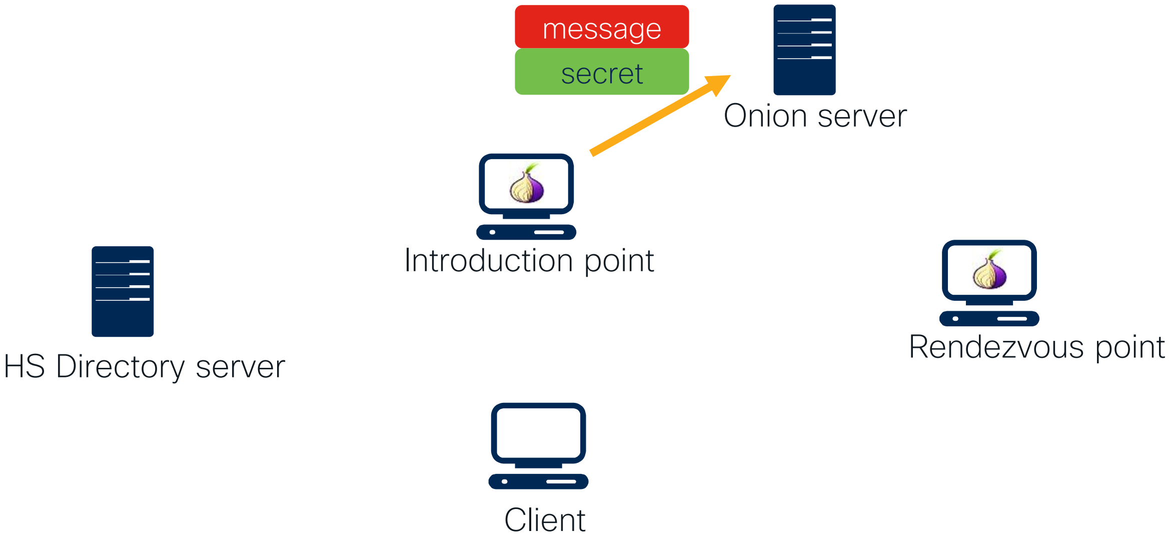
Client selects a random relay node as a rendezvous point

Onionrouting (5)



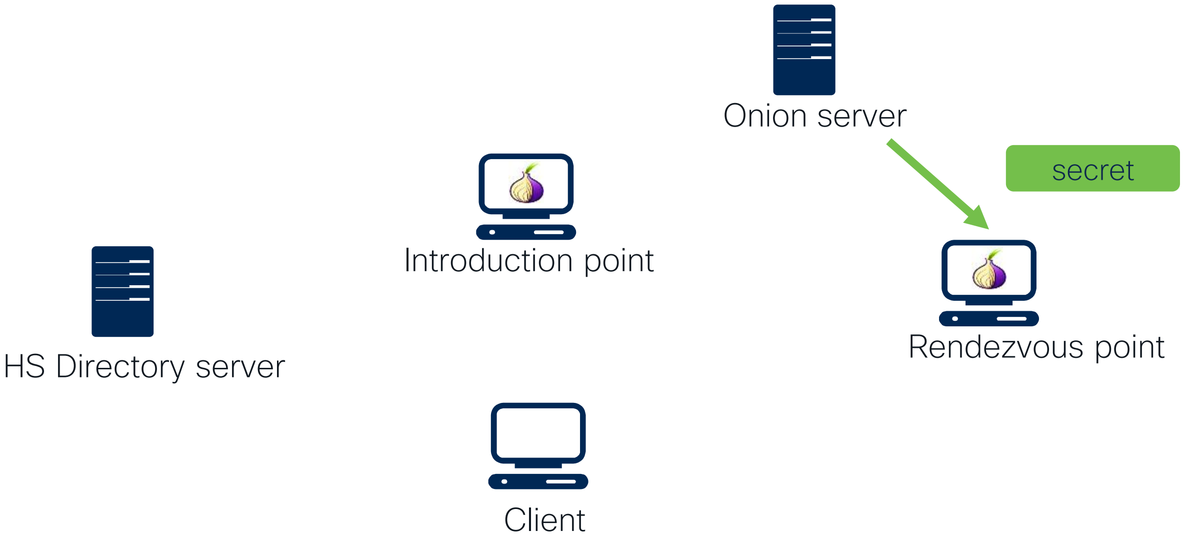
Client contacts the introduction point, requesting to forward the information about the rendezvous point to the hidden server. Message includes a one-time secret

Onionrouting (6)



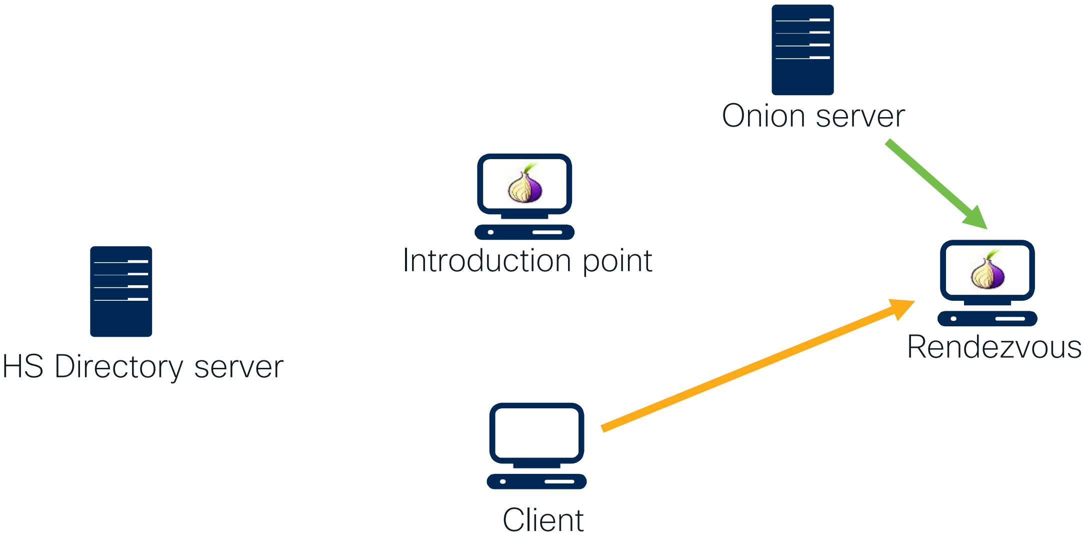
IP contacts the hidden server, telling him about the RP

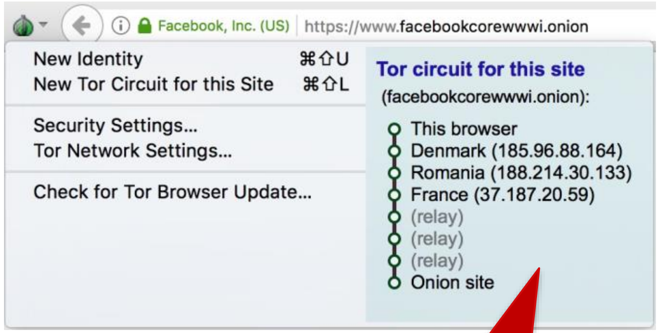
Onionrouting (7)



Server builds a circuit to the RP, providing the one-time secret from the client

Onionrouting (8)





https://www.facebookcorewwwi.onion

Tor circuit for this site

(facebookcorewwwi.onion):

- This browser
- Denmark (185.96.88.164)
- Romania (188.214.30.133)
- France (37.187.20.59)
- (relay)
- (relay)
- (relay)
- Onion site

3 relays from client, 3 relays from server

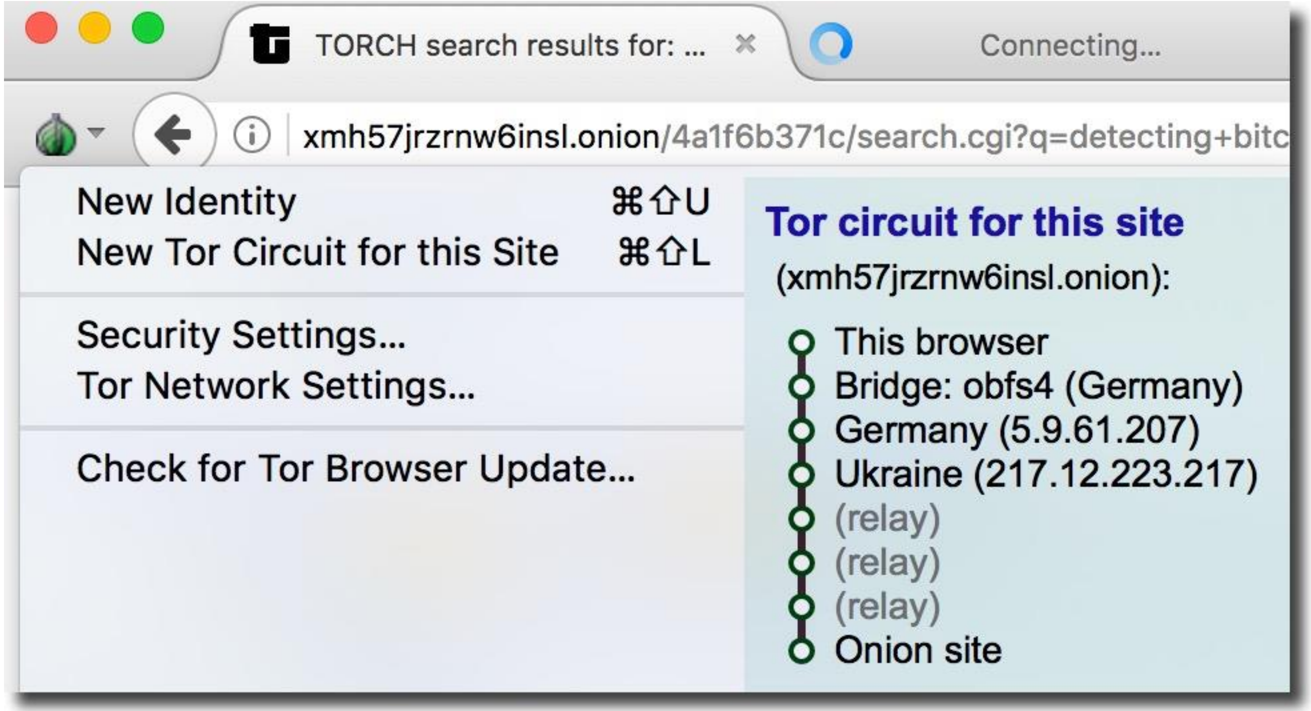
Client communicates to the hidden server via the rendezvous point

DEMO: Onionshare

Obfuscation

Pluggable Transport

https://www.pluggabletransports.info/



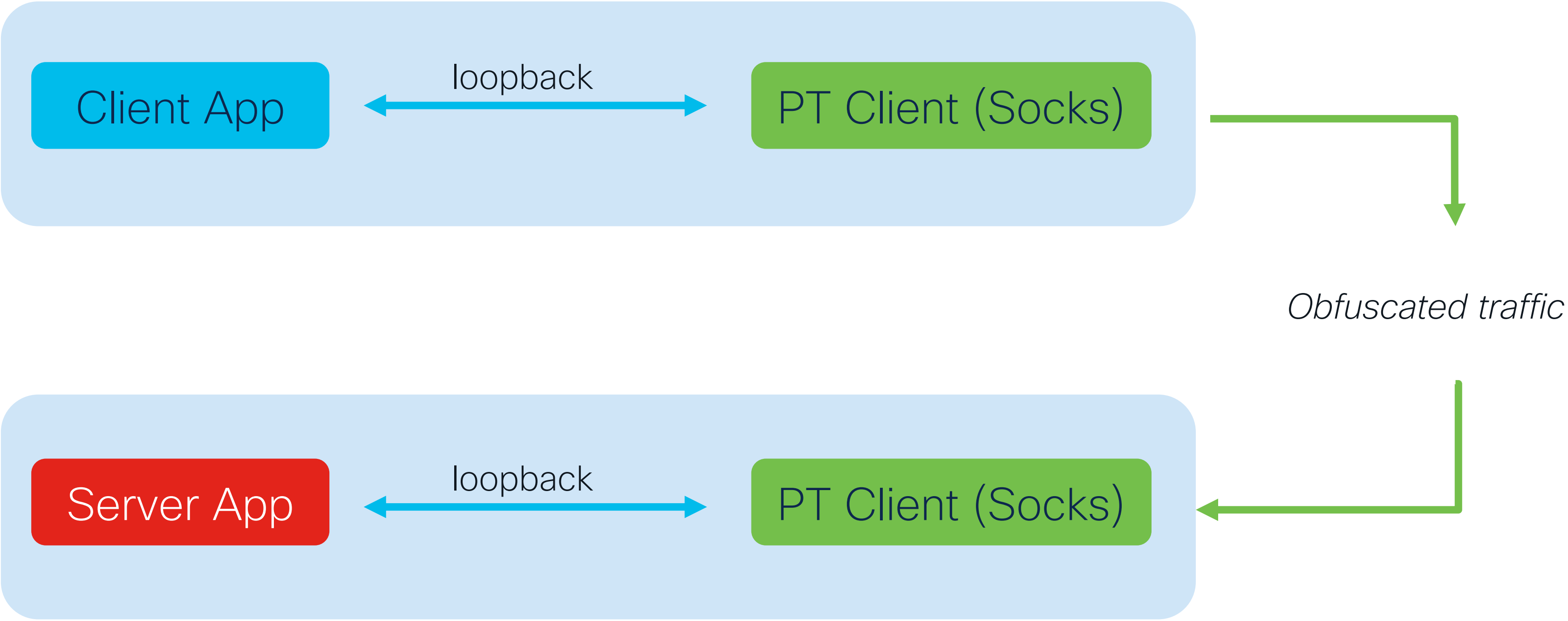
TORCH search results for: ...
Connecting...
xmh57jrzrnw6insl.onion/4a1f6b371c/search.cgi?q=detecting+bitc
New Identity ⌘⇧U
New Tor Circuit for this Site ⌘⇧L
Security Settings...
Tor Network Settings...
Check for Tor Browser Update...

Tor circuit for this site

(xmh57jrzrnw6insl.onion):

- This browser
- Bridge: obfs4 (Germany)
- Germany (5.9.61.207)
- Ukraine (217.12.223.217)
- (relay)
- (relay)
- (relay)
- Onion site

Tor Pluggable Transport (PT)



Tor Pluggable Transport (PT)

https://www.torproject.org/docs/pluggable-transports.html.en

- Obfs2
  - Use a additional encryption layer to obfuscate. Key is exchanged in cleartext.
- Obfs3
  - Negotiation of a DH Key for obfuscation. Not resistant for active probing.
- Obfs4
  - Authenticate with a pre-shared key, distributed out-of-band. Resistant against active probing. Obfuscate with DHE.
- Meek
  - Obfuscate in http and TLS, leveraging domain fronting

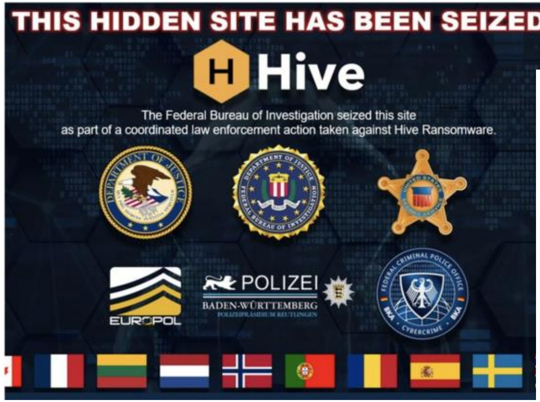
DEMO: SSH over Tor

Let's get caught!
Eventually…

Law Enforcement Efforts

DARK WEB | Ireland helps FBI take down illegal ransomware server used by cyber criminals

The operation dismantled servers of the HIVE ransomware infrastructure on Thursday, 26 January.



THIS HIDDEN SITE HAS BEEN SEIZED

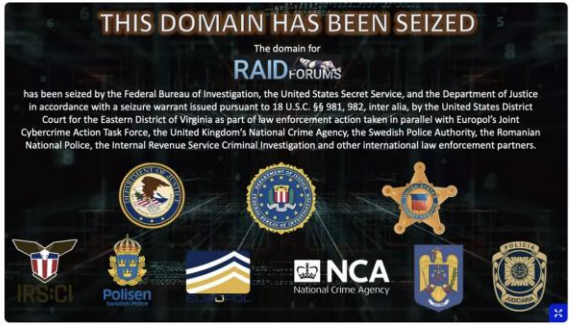
Hive

The Federal Bureau of Investigation seized this site as part of a coordinated law enforcement action taken against Hive Ransomware.

NEWS

One of the world's biggest hacker forums taken down

The illegal marketplace 'RaidForums' has been shut down and its infrastructure seized as a result of Operation TOURNIQUET, a complex law enforcement effort coordinated by Europol to support independent investigations of the United States, United Kingdom, Sweden, Portugal, and Romania. The forum's administrator and two of his accomplices have also been arrested.



THIS DOMAIN HAS BEEN SEIZED

The domain for

RAID FORUMS

has been seized by the Federal Bureau of Investigation, the United States Secret Service, and the Department of Justice in accordance with a seizure warrant issued pursuant to 18 U.S.C. §§ 981, 982, inter alia, by the United States District Court for the Eastern District of Virginia as part of law enforcement action taken in parallel with Europol's Joint Cybercrime Action Task Force, the United Kingdom's National Crime Agency, the Swedish Police Authority, the Romanian National Police, the Internal Revenue Service Criminal Investigation and other international law enforcement partners.

OMG!OMG! IS ONE OF THE DARKNET MARKETS FIGHTING FOR PRIMACY AFTER THE TAKEDOWN OF HYDRA.

Dina Temple-Raston and Kendra Hanna
September 6, 2022

Q & A: What comes after Hydra, the darknet marketplace that changed everything?

Darknet Monitoring

- Monitoring of the darknet for information leaks, e.g. passwords, intellectual property, databases and other potential threats

- Continuous monitoring and alerts based on specific criteria:
  - Corporate email addresses
  - Company name and industry

- Cisco also monitors TOR relays

- General trend: Professionalization/industrialization of cyber crime economy

How SILK ROAD owner was revealed

- Ross Ulbricht, the mastermind behind Silk Road

- On October 11, 2011, an account named “altoid” posted on bitcointalk.org a thread titled “a venture backed bitcoin startup company”, looking for partners for a bitcoin startup. Altoid referred people to contact him at rossulbricht@gmail.com. He also discussed the “Silk Road” marketplace in the thread. Shortly after, Silk Road was advertised on the forum “shroomery.org” by a user also named “altcoin”.

- Ross’s Youtube channel and Google Plus page included links to Mises Institute, an Austrian blog that published content related to the economic theory. On the Silk Road forum, DRP also backlinked to Mises Institute and shared the site’s content there. Through one of these posts, he mentioned that his time zone is the (PT), i.e. the Pacific Time zone.

- Ross posted on Stakoverflow this question “How can I connect to a Tor hidden service using curl in PHP?”. Initially, Ross posted the question using an account aliased with his real name, yet less than a minute later, the account’s alias was changed to “frosty”.

- Ross bought 9 fake identification documents that included his real picture, yet different names. The US border customs intercepted the package which had been shipped from Canada to Ross’s apartment in San Francisco.

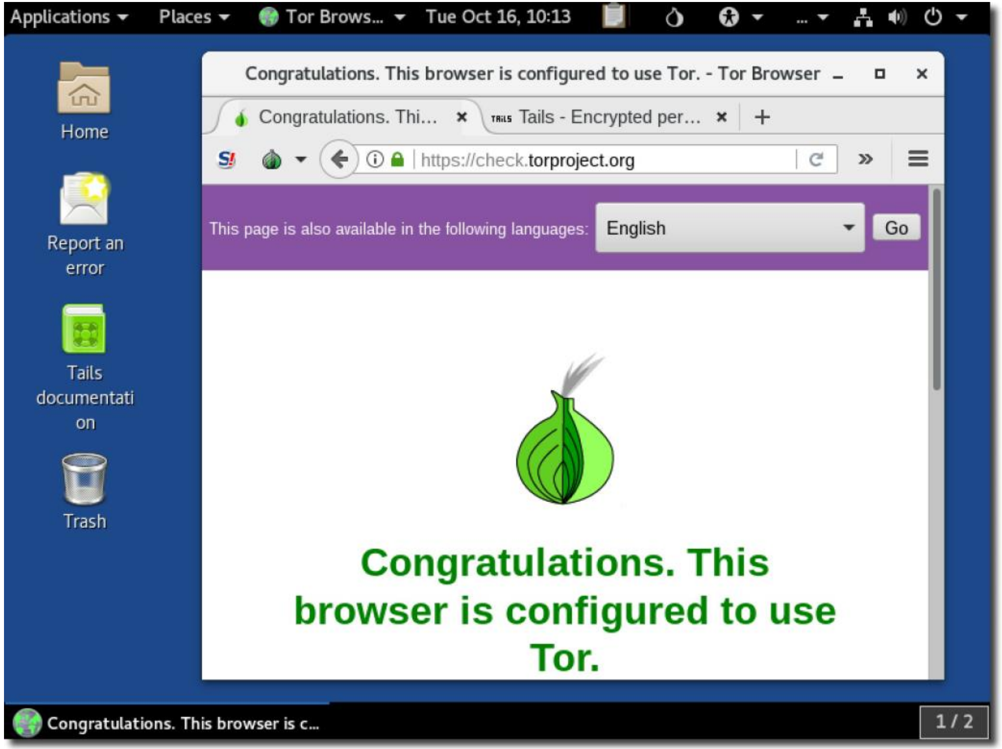
Meet Saskia

- This is **Saskia Laura Schröer**
  - She would like to hear from you about cyber attacks and how her research can help. Your needs for protective or reactive detection, your industry specificities…
- Security Consulting Engineer at the Cisco EMEA Security Centre of Excellence
- Background in Networking, Security and Artificial Intelligence
- **PhD Candidate at the University of Liechtenstein – Focus: Offensive use of AI in Cyber Attacks**
- Feel free to reach out on [LinkedIn]() or via sschroer@cisco.com
- She’s probably in the room… reach out!

Wrapping up

Tails

- https://tails.boum.org
- Secure OS based on modified Linux
- Only communicates outside via Tor
  - Has Thunderbird, Pidgin IM, etc. already preconfigured
- Can be run from USB Stick


Applications
Places
Tor Brows...
Tue Oct 16, 10:13
Home
Report an error
Tails documentation
Trash
Congratulations. This browser is configured to use Tor. - Tor Browser
Congratulations. Thi...
Tails - Encrypted per...
https://check.torproject.org
This page is also available in the following languages:
English
Go
Congratulations. This browser is c...
1 / 2

Congratulations. This browser is configured to use Tor.

Summary of Tor usage guidelines

Basic security:

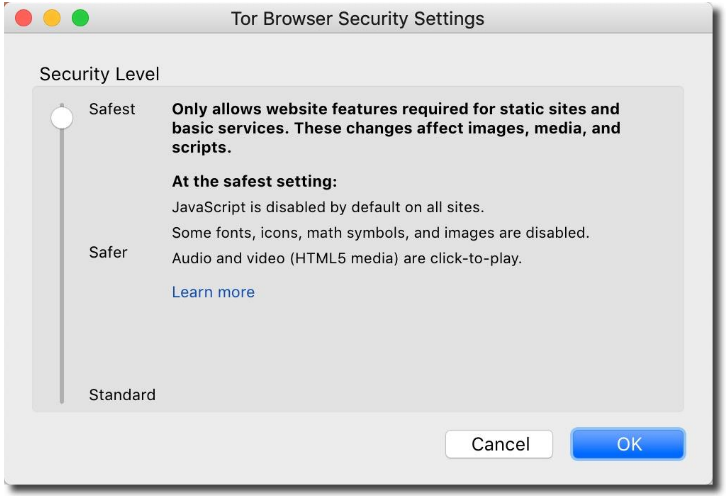
- Disable automatic launch of scripts by using setting of “safest”
- Avoid darknet sites that do not offer HTTPS
- Do not reuse same logins on darknet and clearnet! (Silk Road..)
- Communicate using PGP (email, IM, etc…)

Intermediate security = Basic security plus

- Use Tor over VPN
- Learn to use bridges with Tor
- Use a safe OS like “Tails”

High Security = Intermediate security plus

- Dedicated, trusted hardware (no virtual image)
- Use Qubes https://www.qubes-os.org/


Tor Browser Security Settings

Security Level

Only allows website features required for static sites and basic services. These changes affect images, media, and scripts.

At the safest setting:

JavaScript is disabled by default on all sites.

Some fonts, icons, math symbols, and images are disabled.

Audio and video (HTML5 media) are click-to-play.

Learn more

Continue your security journey

Feb 9 | 10:00

IBOSEC-2006

Empty Threats - Building Your Own Cyber Threat Picture

Feb 9 | 10:30

BRKSEC-2101

Malware Execution As A Service: a Deep Dive into CSMA Advanced File Analysis

Feb 10 | 09:00

BRKSEC-3129

Public Key Cryptography - from RSA and EC to post-quantum

FINISH

Feb 10 | 09:00

LTRSEC-2006

Breach Defense Technologies

Complete your Session Survey

- Please complete your session survey after each session. Your feedback is important.
- Complete a minimum of 4 session surveys and the Overall Conference survey (open from Thursday) to receive your Cisco Live t-shirt.

- All surveys can be taken in the Cisco Events Mobile App or by logging in to the Session Catalog and clicking the "Attendee Dashboard” at https://www.ciscolive.com/emea/learn/sessions/session-catalog.html

Continue Your Education

- Visit the Cisco Showcase for related demos.
- Book your one-on-one Meet the Engineer meeting.
- Attend any of the related sessions at the DevNet, Capture the Flag, and Walk-in Labs zones.
- Visit the On-Demand Library for more sessions at ciscolive.com/on-demand.

The bridge to possible

Thank you

cisco Live!

cisco Live!