

Tor Baião com Cebola

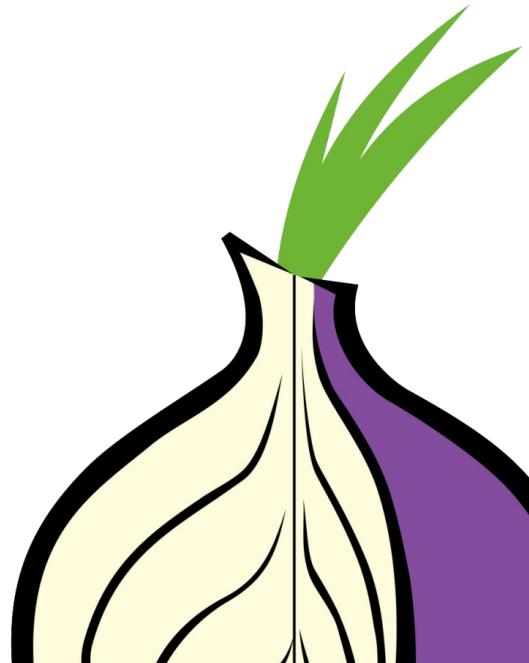
CriptoBaião - Fortaleza, Brasil - 30 de Março de 2019

Vinícius Zavam
egypcio@torproject.org
13AC CF3E D4E3 B36F 626F D3AE 415C 6534 13B4 3475



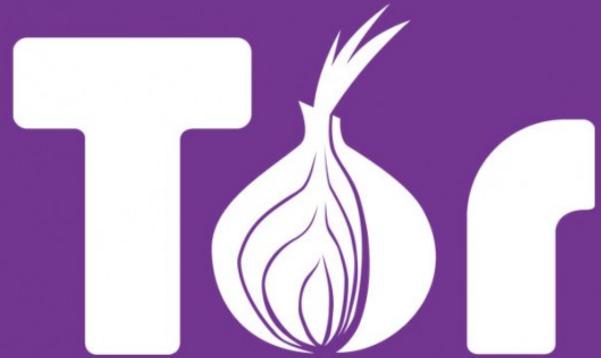
agenda

- conceitos básicos sobre **Tor**
 - definições (resumo)
 - visão simplificada da rede
 - alternativas à gosto
- perguntas frequentes
 - quem usa?
 - por que usar?
 - mas ...
- esforços relacionados
- ferramentas extras
- informações adicionais sobre a rede
 - ingresso dos nós na rede
 - obtenção do navegador com uma ajudinha extra
 - pontes (nós de entrada)
 - obfuscadores de tráfego
- serviços acebolados
- gráficos e números interessantes (estatísticas)
- colaboração, suporte e pesquisa



conceitos básicos sobre Tor

- definições (resumo)
 - organização sem fins lucrativos;
 - fundada nos EUA em 2006 (Cambridge, Seattle);
 - 501(c)(3); pesquisa e educação;
 - protocolos de comunicação;
 - software livre (gratuito); código aberto; ipv6;
 - primeira versão data de 2002; licença BSD;
 - rede de servidores, operados por voluntários;
 - pessoas físicas; cidadãos comuns;
 - empresas; instituições de ensino; fundações;
 - navegador web;
 - baseado no Mozilla Firefox.



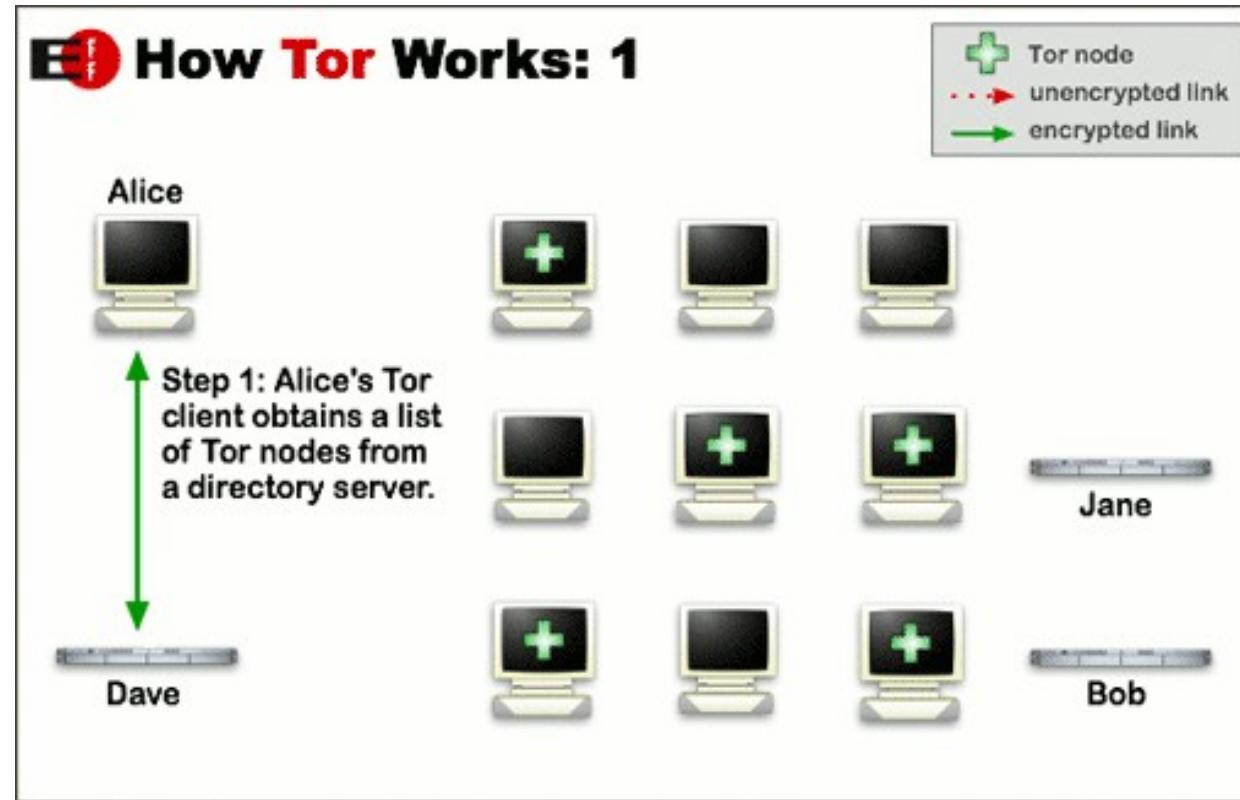
Isabela Bagueros, diretora executiva do projeto Tor



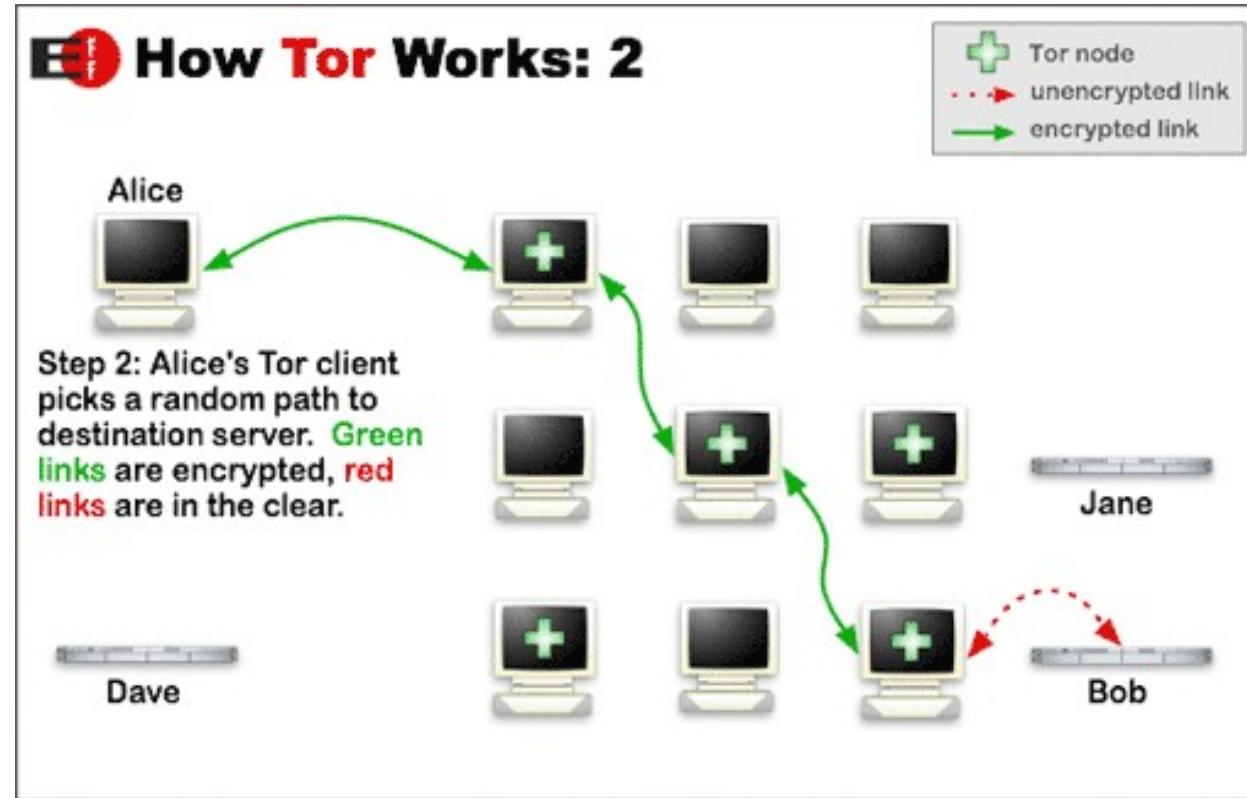


Roger Dingledine, criador e principal desenvolvedor do projeto Tor – junto com *Nick M.* e *Paul S.*

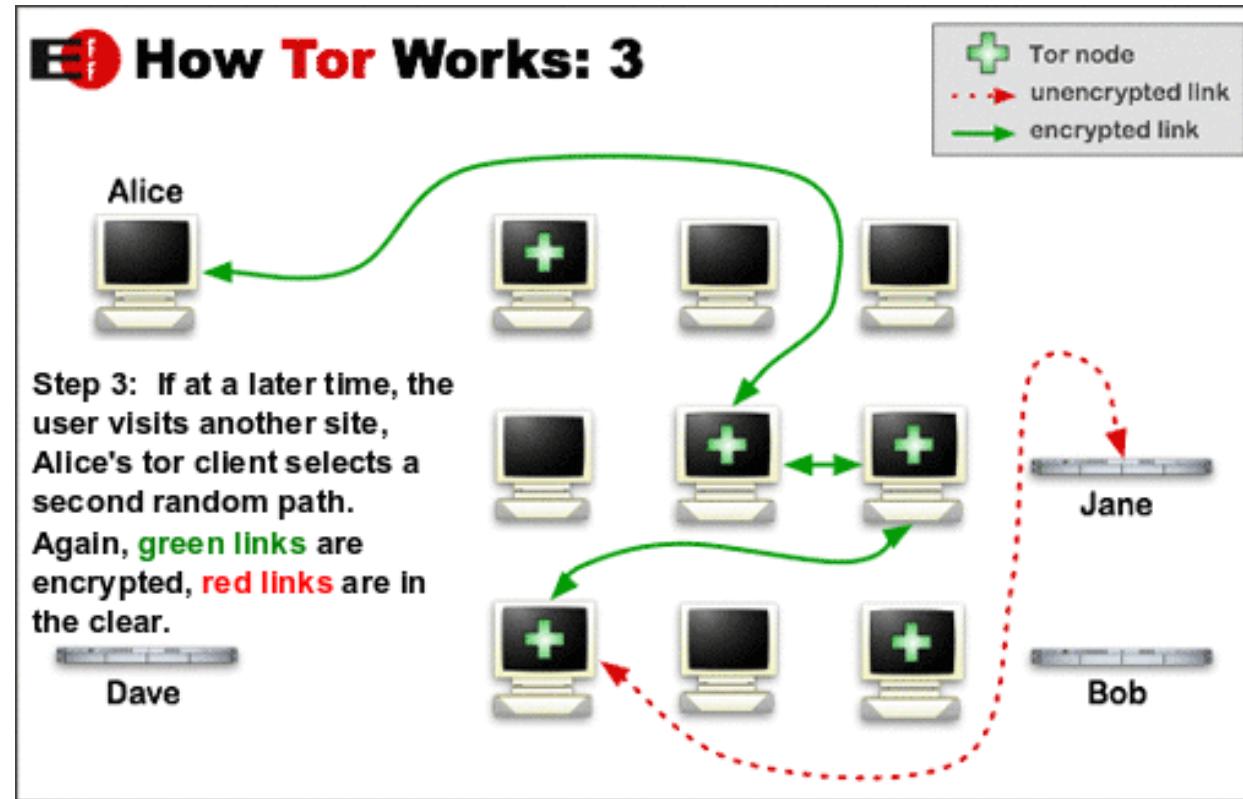
- visão geral



- visão geral



- visão geral





Roger, descobrindo que ‘aquela’ foto foi usada para apresentá-lo como criador do Tor

- alternativas à gosto
 - modo privado;
 - extensões;
 - *proxy*;
 - outros navegadores;
 - rede virtual privada (vpn);
 - i2p; freenet.

perguntas frequentes

- quem usa?
 - eu (pessoas comuns);
 - famílias inteiras;
 - jornalistas; {ciber}ativistas;
 - denunciantes (delatores);
 - militares (exército, marinha, aeronáutica, ...);
 - investigadores, empresários/executivos;
 - cientistas, pesquisadores, estudantes, professores;
 - hotéis/pousadas/albergues/livrarias;
 - público especializado.



Aphex Twin

@AphexTwin

Follow



<http://syro2eznzea2xbpi.onion>

8:00 AM - 18 Aug 2014

3,290 Retweets 2,764 Likes



232

3.3K

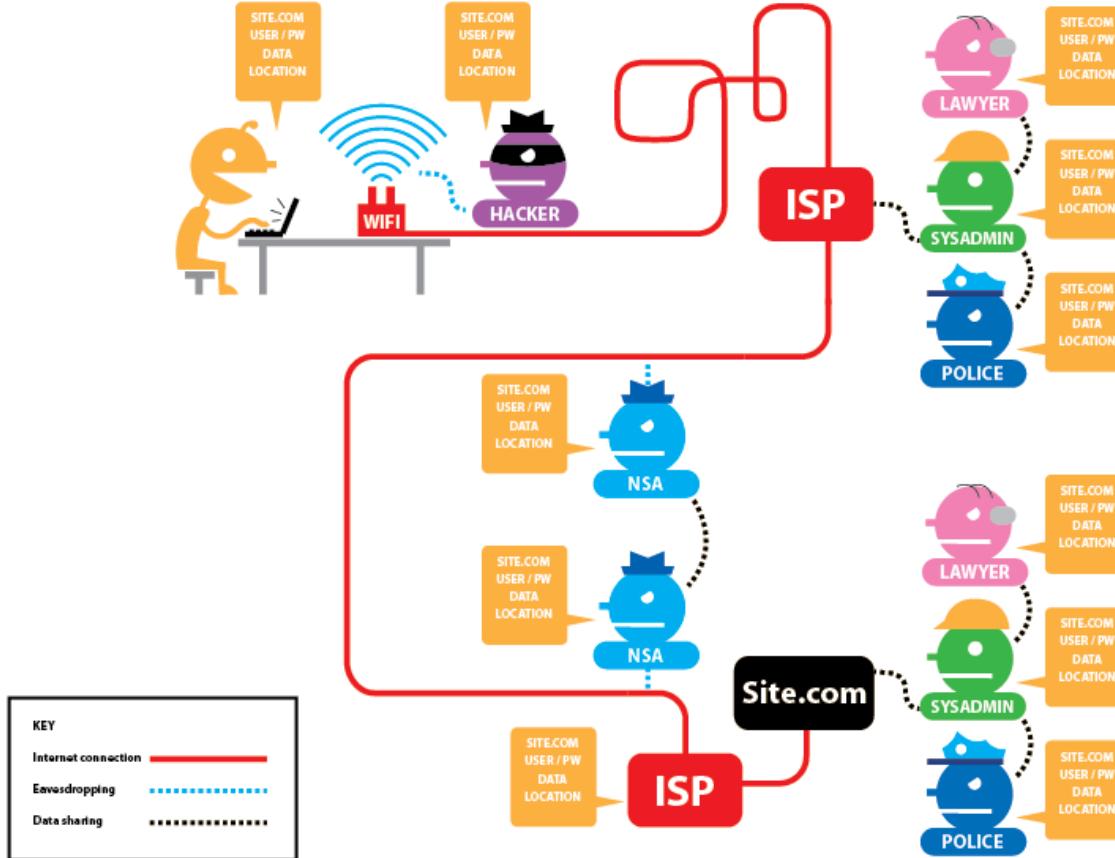
2.8K

<https://twitter.com/AphexTwin/status/501383043643621376>

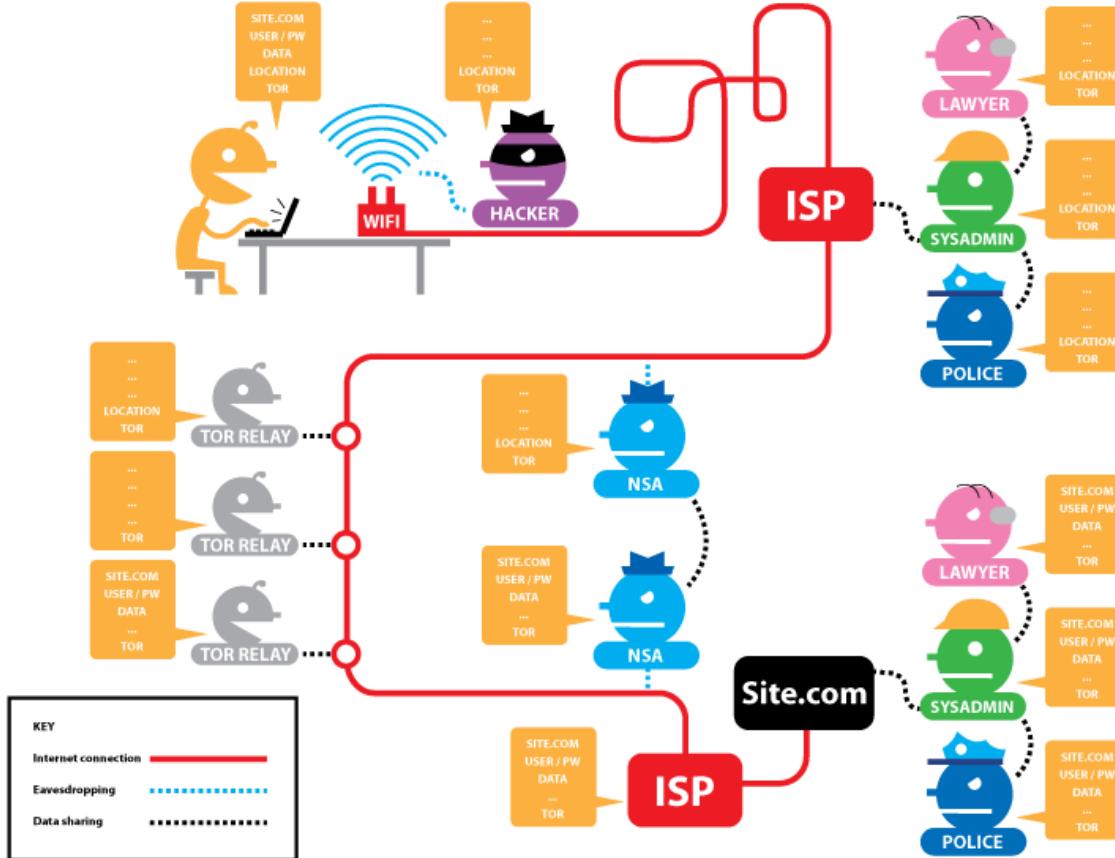
- por que usar?
 - venda de cliques;
 - análise de perfis sociais;
 - geo localização (proteção de integridade física);
 - imprensa livre (liberdade de expressão);
 - denúncias (delações).

- por que usar?
 - pesquisa acadêmica;
 - trocas de contexto (sessões no navegador);
 - censura;
 - boicote;
 - investigações;
 - troca de informações sigilosas;
 - *pentest*.

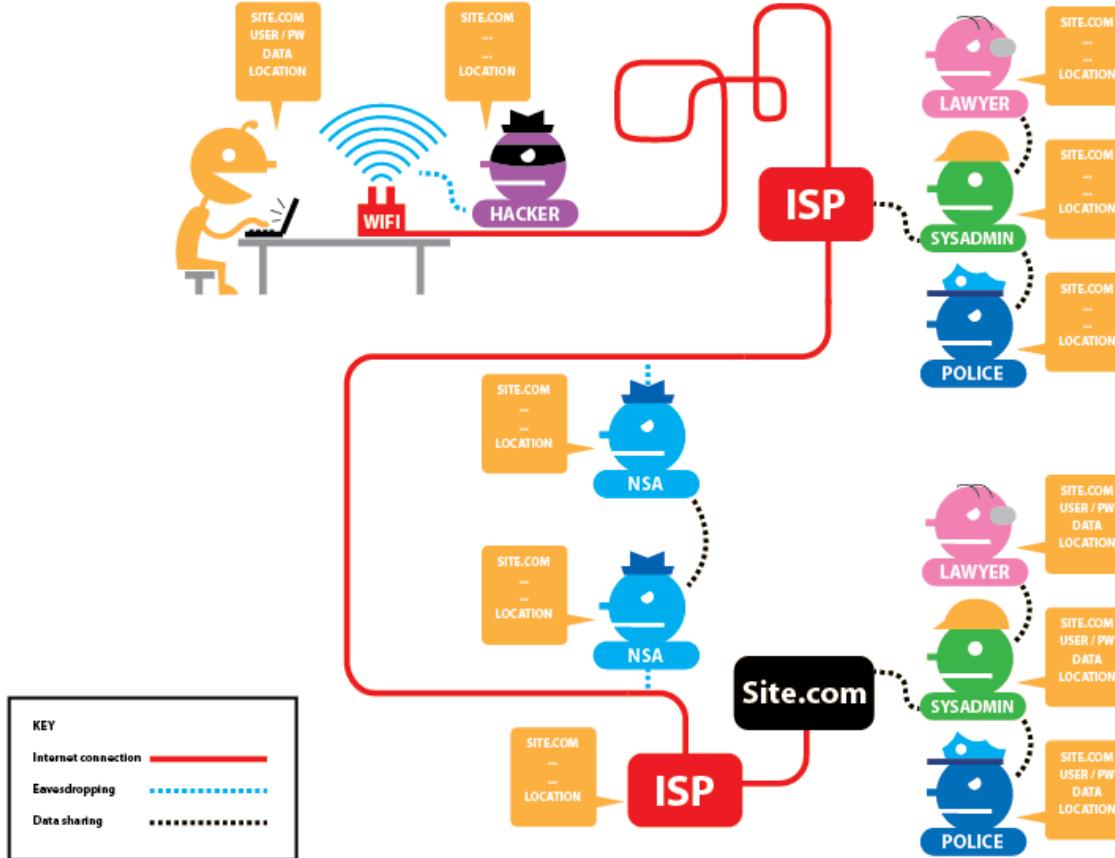
sem Tor, sem HTTPS



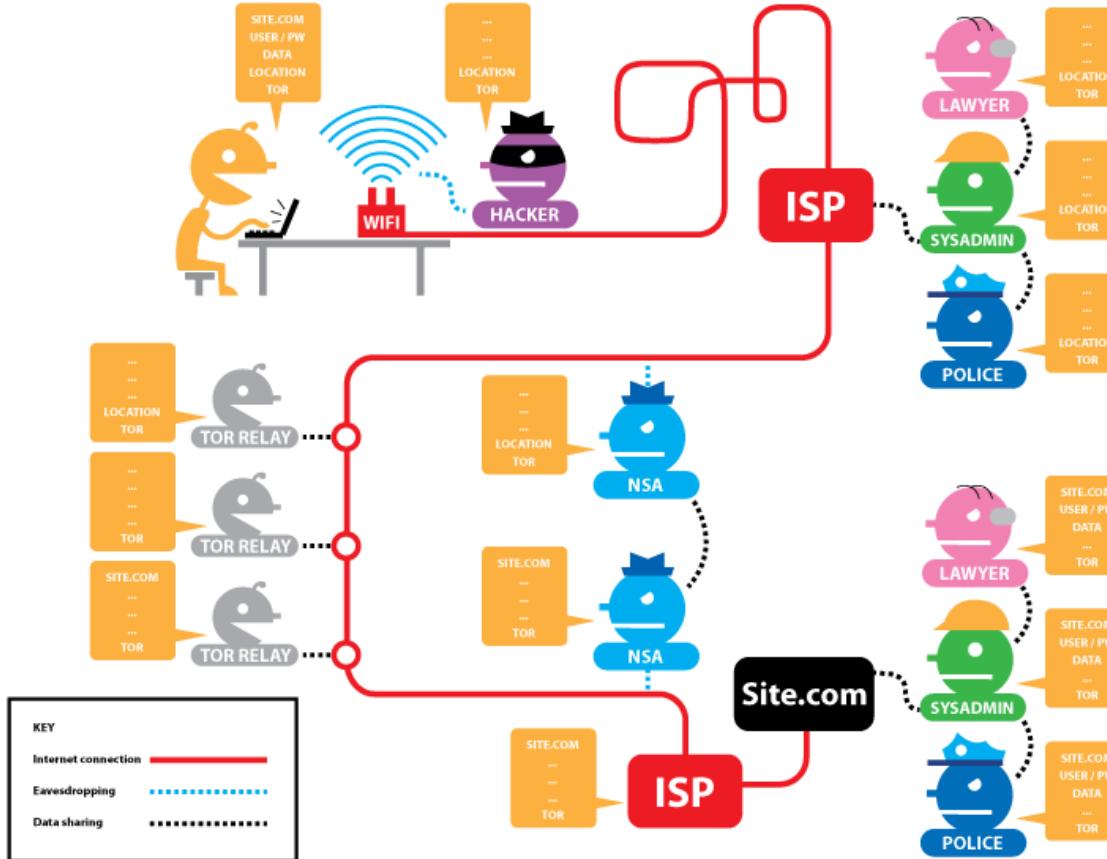
com Tor, sem HTTPS



sem Tor, com HTTPS



com Tor, com HTTPS



- mas ...
 - criminosos? *hackers?* *trolls?*
 - ataques distribuídos de negação de serviço?
 - minha rede de IRC favorita?
 - colabora com envio de *SPAM*?
 - pode ser distribuido livremente?
 - **tor?** **Tor?** TOR? Thor? t0r? T0r?
 - financiado por militares?
 - vírus? *backdoor*?
 - aplicações compatíveis?
 - problemas por colaborar?

- *mas ...*
 - necessito de um hardware específico?
 - não poderia ser mais rápida? (quero assistir *Netflix*)
 - bloqueio de certos conteúdos ou sítios web?
 - mais saltos = mais privacidade! como não pensaram nisso?!
 - publicar lista de nós?
 - compartilhamento de arquivos na rede?
 - **tor? Tor? TOR? Thor? t0r? T0r?**
 - gostei! como colaborar? <3

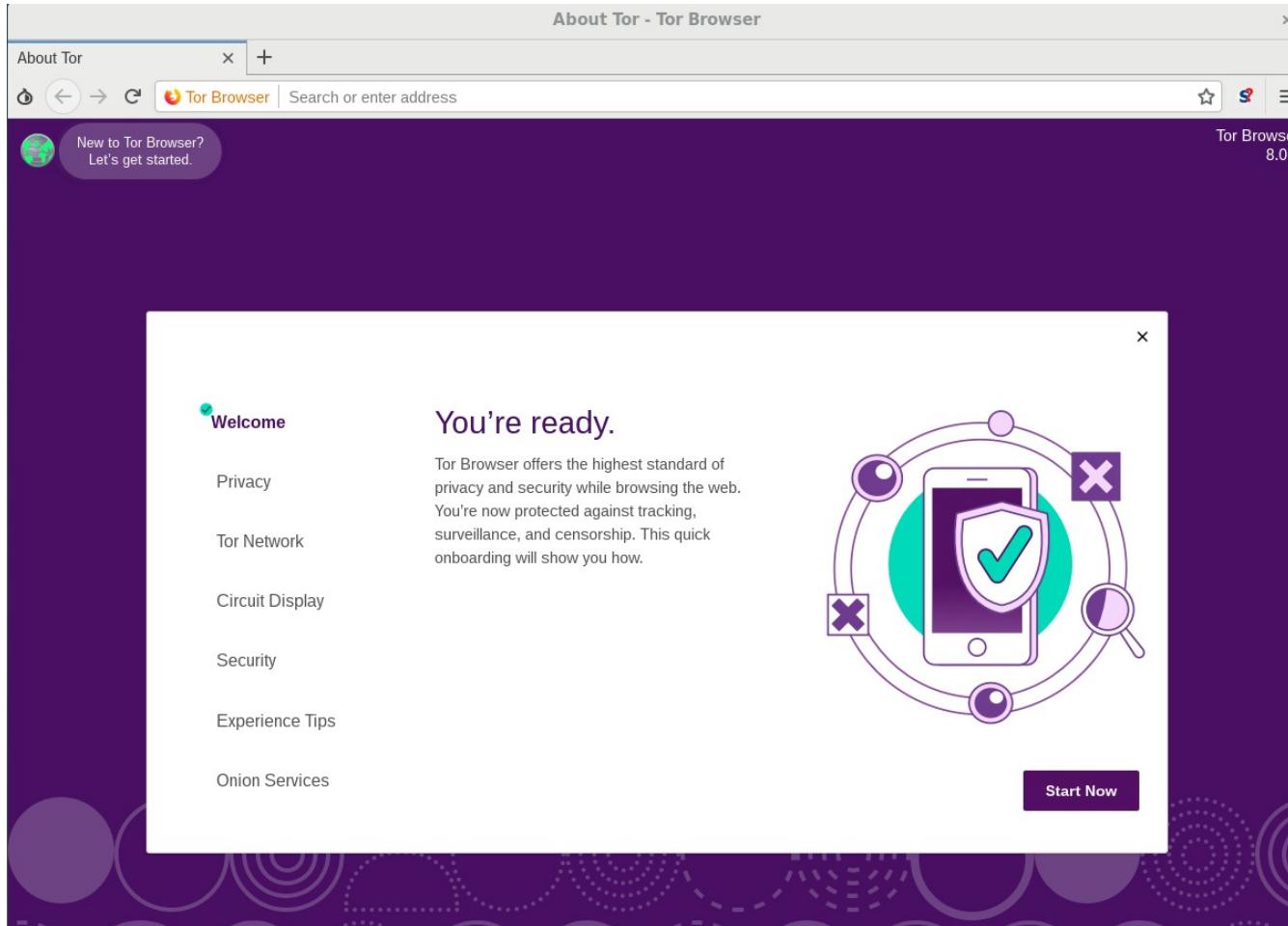
- mas como abordar e conversar sobre anonimato?
 - CIDADÃO; privacidade.
 - EMPRESAS; segurança.
 - GOVERNOS; resistência à análise de tráfego.
 - ATIVISTAS; drible à censura.

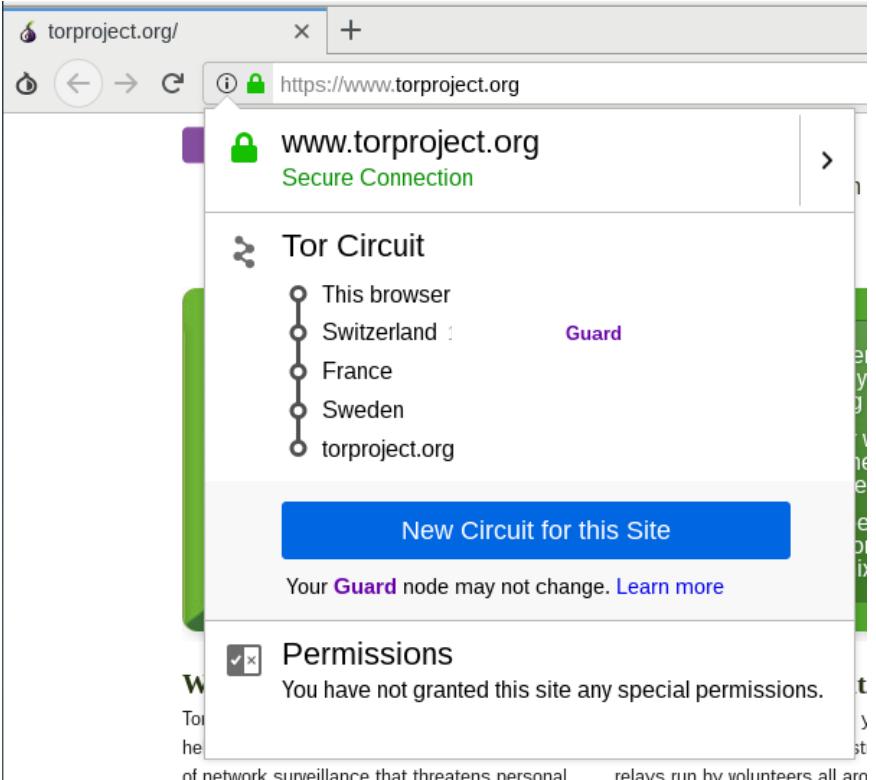
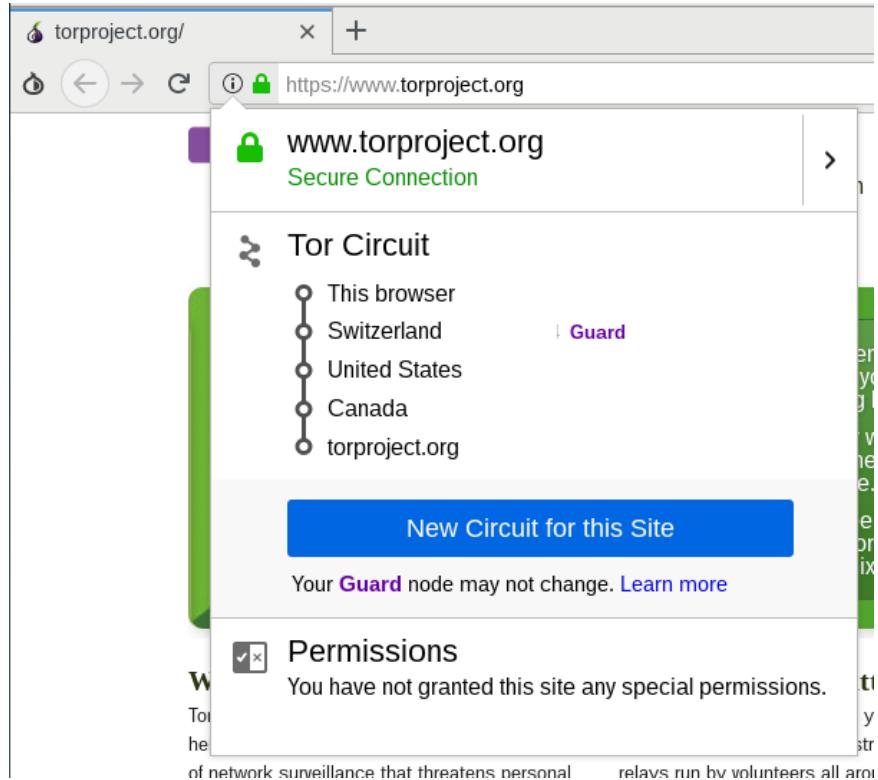
esforços relacionados



BROWSER
БРАВОЗЕР







108 CENSORED 40

- evita repasse do seu
endereço IP



previne análise de
tráfego local



mitiga revelar sua
geolocalização



previne compartilhar sua
impressão digital



previne trocas de contextos
entre abas



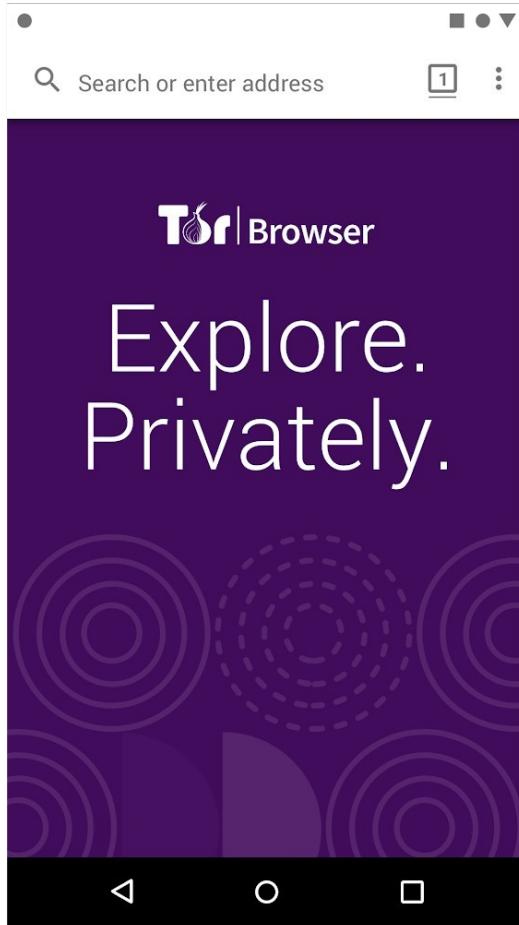
isola *cookies* e *scripts*



escritas mínimas em disco



não salva histórico
de navegação



Search or enter address [1] ⋮

WELCOME PRIVACY TOR NETWORK



You're ready.

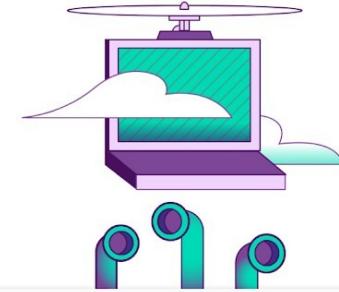
Tor Browser offers the highest standard of privacy and security while browsing the web. You're now protected against tracking, surveillance, and censorship. This quick onboarding will show you how.

[START NOW](#)

◀ ○ □

Search or enter address [1] ⋮

WELCOME PRIVACY TOR NETWORK

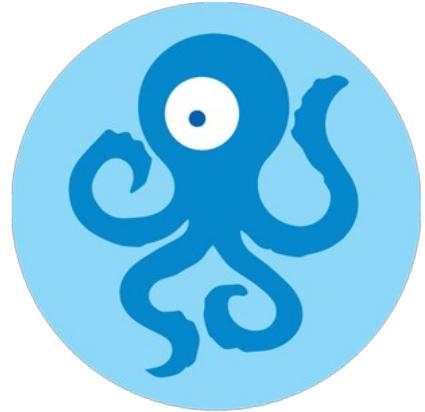


Travel a decentralized network.

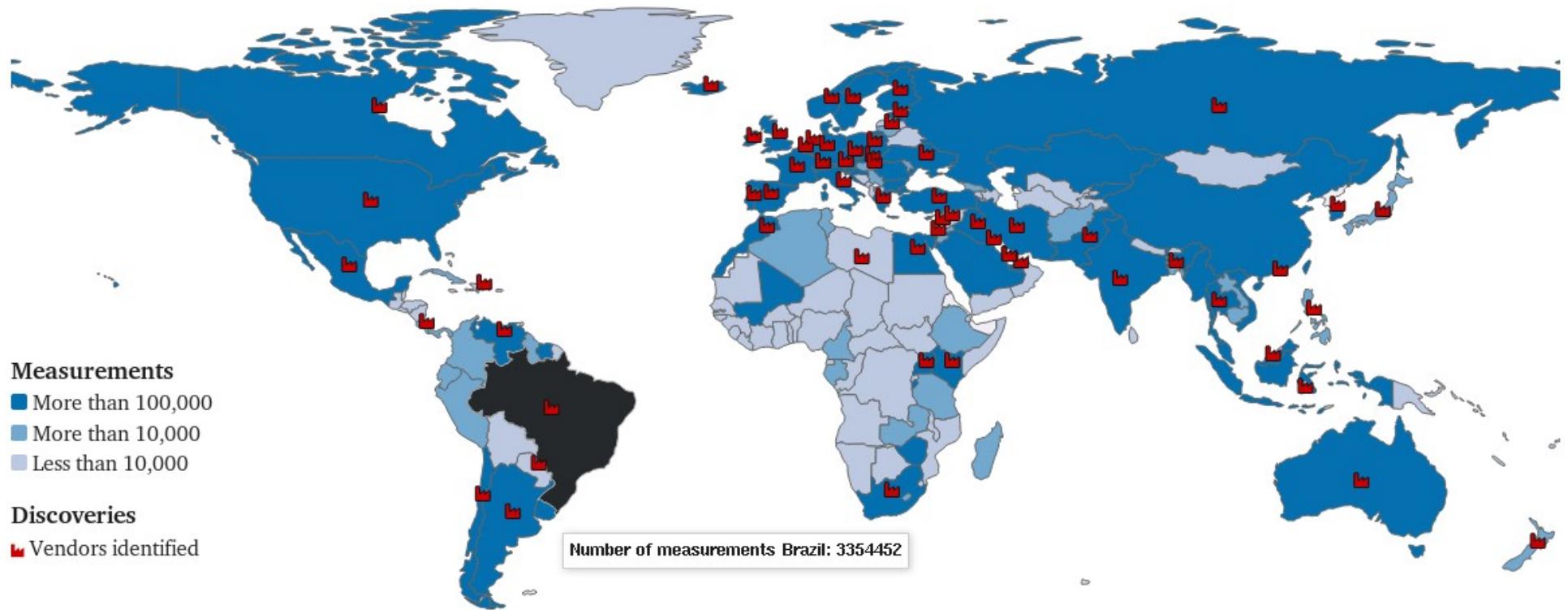
Tor Browser connects you to the Tor network, a network of servers we call "relays," run by thousands of volunteers around the world. Unlike a VPN, there's no one point of failure or centralized entity you need to trust in order to

[GO TO SECURITY SETTINGS](#)

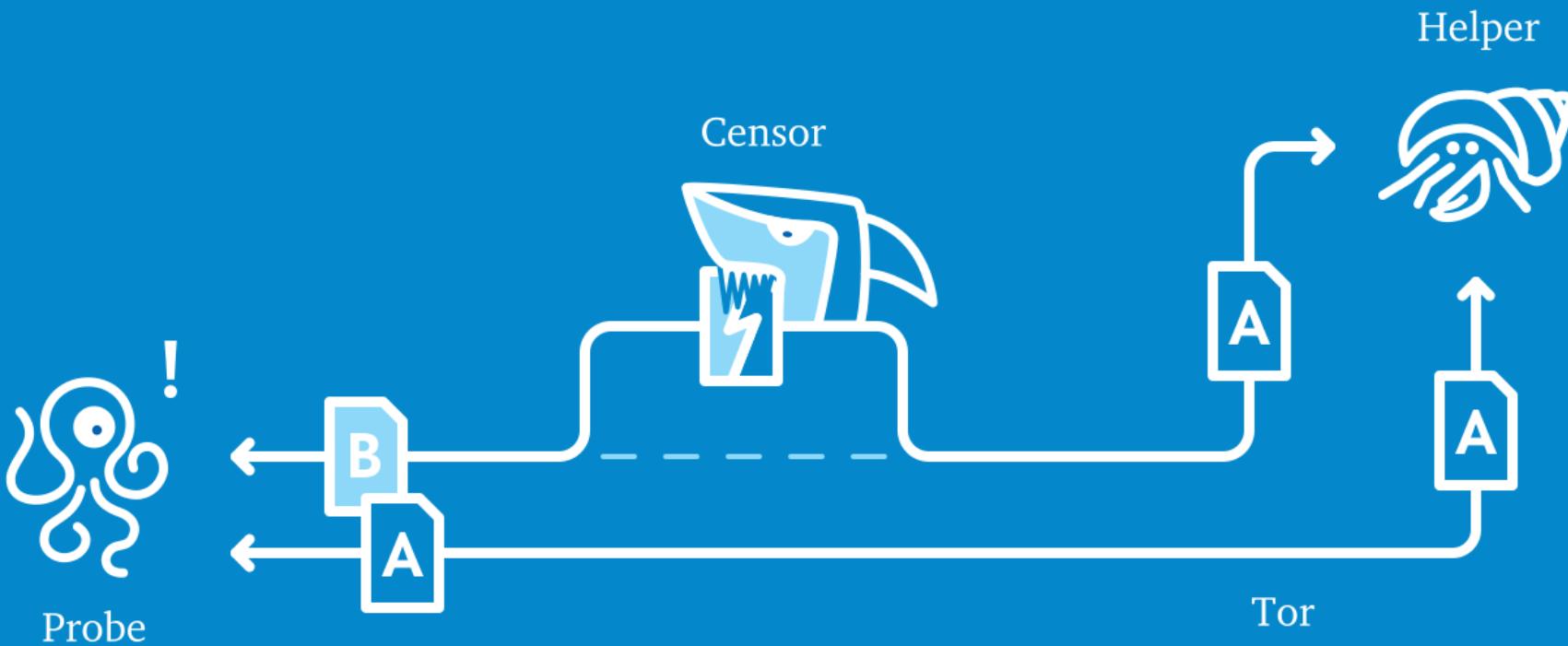
◀ ○ □

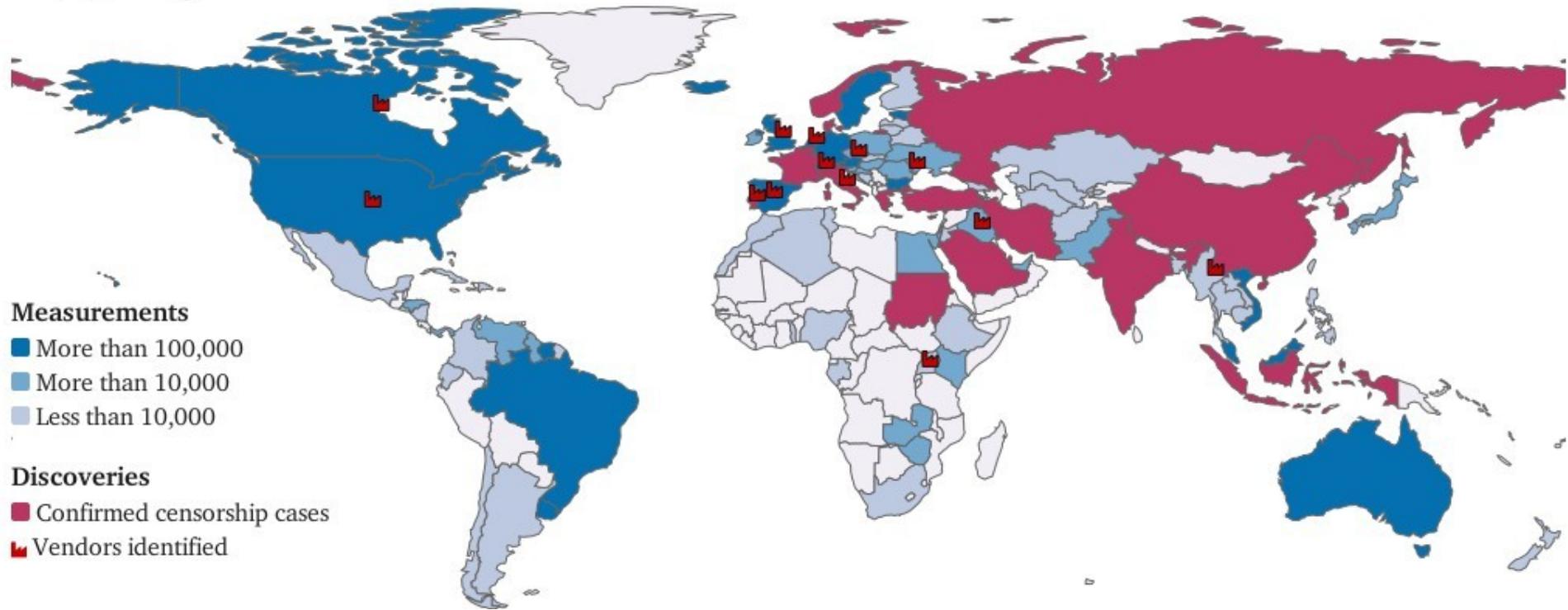


Open Observatory of Network Interference
ooni



<https://explorer.onion.torproject.org>





<https://explorer.ooni.torproject.org>



Edward Snowden 

@Snowden

Follow

v

DHS fought to stop libraries from using privacy technology, but [@LibraryFreedom](#) beat them. Librarians are badass.

Dan Gillmor  @dangillmor

Just donated to the excellent Library Freedom Project. Here's [why.libraryfreedomproject.org/libraries-tor-...](https://libraryfreedomproject.org/libraries-tor-...) Should have done this sooner.

11:24 AM - 11 Oct 2015

<https://libraryfreedomproject.org>

<https://twitter.com/snowden/status/653275043087151105>



Edward Snowden esperando um açaí misto lá na Gorete



– infelizmente, Edward nunca foi na Gorete –



Alison Macrina e Nima Fatemi, durante primeira fase do projeto de implementação de nós de saída em bibliotecas públicas

TorBSD Diversity Project - TDP



Categoria do Relatório: [RELAYS](#)

Data: **20190320**

Fonte: onionoo.torproject.org/details

Contagem Geral, por Sistema Operacional

Sist. Operacional	Contagem (unidades)
=====	=====
TOTAL (6540)	6540
Linux	6044 (92.4%)
FreeBSD	316 (4.8%)
OpenBSD	77 (1.2%)
Windows	70 (1.1%)
Darwin	16 (0.2%)
SunOS	5 (0.1%)
NetBSD	5 (0.1%)
ElectroBSD	4 (0.1%)
DragonFly	2 (0.0%)
GNU/kFreeBSD	1 (0.0%)



Categoria do Relatório: [RELAYS](#)

Data: **20190320**

Fonte: onionoo.torproject.org/details

Largura de Banda, por Sistema Operacional

Sist. Operacional	Banda (bytes)
TOTAL (6540)	46582231070
Linux (6044)	42672726257 (91.6%)
FreeBSD (316)	3314165434 (7.1%)
OpenBSD (77)	312187268 (0.7%)
Windows (70)	132065771 (0.3%)
ElectroBSD (4)	47542563 (0.1%)
Darwin (16)	38342647 (0.1%)
SunOS (5)	32633133 (0.1%)
NetBSD (5)	23141477 (0.0%)
DragonFly (2)	7295922 (0.0%)
GNU/kFreeBSD (1)	2130598 (0.0%)

Categoria do Relatório: [BRIDGES](#)

Data: **20190320**

Fonte: onionoo.torproject.org/details

Largura de Banda, por Sistema Operacional

Sist. Operacional	Banda (bytes)
TOTAL (939)	762049891
Linux (890)	748170422 (98.2%)
FreeBSD (24)	7195249 (0.9%)
OpenBSD (11)	3422706 (0.4%)
Windows (9)	2321365 (0.3%)
Darwin (3)	810515 (0.1%)
NetBSD (1)	76800 (0.0%)
DragonFly (1)	52834 (0.0%)

▼ Router Name	▼ Bandwidth (KB/s)	▲ Uptime	▼ Hostname	▼ ORPort	▼ DirPort
coruja	110	9 d		█ O ▲	9001
cebolinha	92	137 d		█ □ O ▲	443 80
DNCRJ	77	46 d		█ O ▲	9001
Ixoliva	48	11 h		█ □ ▲	9001
francisco	31	10 d		█ O ▲	9001
satoshitor	25	91 d		⚡ □ O ▲	443 80
Relay01	17	81 d		⚡ □ O ▲	443
ididteditheconfigsr	12	23 h		█ □ ▲	9001
Unnamed	8	11 h		█ □ █	4433
Baldur	1	13 d		O ▲	9001
unknow	1	19 h		△	9001
Amor	0	16 h		█ □ █	9030
astuterelay	0	5 h		█ □ ▲	9001
cristina	0	2 d		█ □ ▲	443 80
Izkill	0	24 h		█ □ ▲	9001
marihess	0	21 h		█ □ ▲	9001
OrbotRelay	0	2 h		△	9001
SanToRelay	0	4 d		█ □ ▲	9001
shad0wguyirc	0	19 h		█ □ O ▲	443
topcat	0	17 d		O ▲	9001
Unnamed	0	5 h		△	443
Unnamed	0	91 d		O ▲	9001
warpzone	0	21 h		O ▲	8181

▼ ▼ Router Name	▼ Bandwidth (kB/s)	▲ Uptime	▼ Hostname	▼ ORPort	▼ DirPort	
SPFCFutebol	2976	177 d 6 h		⚡ 🌐 ○ 🔍	9001	9030
tauro	1955	104 d 9 h		⚡ 🌐 🔍 🔍	443	80
gregory	1269	259 d 8 h		⚡ 🌐 ○ 🔍	593	21462
bearmeettea	1246	3 d 10 h		⚡ 🌐 ○ 🔍	22407	19747
xtermnginx	1245	41 d 4 h		⚡ 🌐 ○ 🔍	1468	3334
overlay	1207	275 d 5 h		⚡ 🌐 ○ 🔍	8307	635
trueconf	1201	275 d 12 h		⚡ 🌐 ○ 🔍	26378	22316
uhwfa	1199	117 d 23 h		⚡ 🌐 🔍	10672	4466
Unnamed	1195	10 d 8 h		⚡ 🌐 🔍	26155	11718
utzer2	1195	75 d 23 h		⚡ 🌐 ○ 🔍	443	9030
Unnamed	1194	31 d 10 h		⚡ 🌐 ○ 🔍	16313	862
Unnamed	1186	1 d 3 h		⚡ 🌐 ○ 🔍	31140	14388
echykd	1157	33 d 13 h		⚡ 🌐 ○ 🔍	7325	16350
ecramrelay1	1115	9 d 18 h		⚡ 🌐 ○ 🔍	9001	None
galpao	1025	4 d 8 h		⚡ 🌐 🔍	9001	None
brasilhostil	854	4 d 15 h		⚡ 🌐 🔍	9000	9001
torbsd2	815	11 d 20 h		⚡ 🌐 🔍	3389	None
Unnamed	613	9 d 22 h		⚡ 🌐 ○ 🔍	23138	32276
brasilhostil2	597	4 d 15 h		⚡ 🌐 ○ 🔍	9100	9101
Relay01	560	96 d 19 h		⚡ 🌐 ○ 🔍	443	9030
▼ ▼ Router Name	▼ Bandwidth (kB/s)	▲ Uptime	▼ Hostname	▼ ORPort	▼ DirPort	
torbsd4	553	11 d 20 h		⚡ 🌐 🔍	9000	None
torbsd3	518	11 d 20 h		⚡ 🌐 🔍	7331	None
ecramrelay2	417	9 d 3 h		🌐 ○ 🔍	9001	None
Unnamed	389	6 d 17 h		⚡ 🌐 ○ 🔍	9001	9030
torbsd5	386	11 d 19 h		⚡ 🌐 🔍	21	None
arbitrium	335	7 d 20 h		🌐 ○ 🔍	9001	9030
RjPi1	248	3 d 17 h		⚡ 🌐 🔍	4430	8000
BR101	233	8 d 17 h		⚡ 🌐 ○ 🔍	9001	9030
Unnamed	231	0 d 8 h		🌐 ○ 🔍	9001	None
nohcego	204	0 d 16 h		⚡ 🌐 🔍	2223	None
torbsd	157	11 d 19 h		🌐 🔍	1194	None
torbsd6	151	11 d 20 h		🌐 🔍	22	None
ImOHelping	141	2 d 14 h		🌐 ○ 🔍	9001	9030
lxoliva	131	0 d 3 h		🌐 ○ 🔍	9001	9030
mmacedo	116	1 d 10 h		🌐 ○ 🔍	9001	None
observable	107	210 d 9 h		🌐 ○ 🔍	28042	16256
Unnamed	81	0 d 18 h		🌐 ○ 🔍	9001	None
UbuntuCore196	68	0 d 5 h		🌐 ○ 🔍	37313	None
UbuntuCore196	66	2 d 1 h		🌐 ○ 🔍	46293	None
UbuntuCore197	54	0 d 8 h		🌐 ○ 🔍	35927	None
▼ ▼ Router Name	▼ Bandwidth (kB/s)	▲ Uptime	▼ Hostname	▼ ORPort	▼ DirPort	
UbuntuCore196	52	0 d 4 h		🌐 ○ 🔍	44301	None

Advertised										
Nickname [†]	Bandwidth	Uptime	Country	IPv4	IPv6	Flags	Add. Flags	ORPort	DirPort	Type
● taur0 (1)	2.36 MiB/s	2d 22h	BR		-	⚡ ⚡ ⚡ ⚡ ⚡ ⚡ ⚡ ⚡ ⚡ ⚡		443	80	Relay
● citsp64 (1)	1.92 MiB/s	96d 23h	BR		-	⚡ HS ⚡ ⚡ ⚡ ⚡ ⚡ ⚡ ⚡ ⚡	⚠	443	0	Relay
● Netburst (1)	1.64 MiB/s	7d 20h	BR		-	⚡ HS ⚡ ⚡ ⚡ ⚡ ⚡ ⚡ ⚡ ⚡	v6	443	69	Relay
● Relay01 (1)	1.51 MiB/s	52d 22h	BR		-	⚡ HS ⚡ ⚡ ⚡ ⚡ ⚡ ⚡ ⚡ ⚡	v6	443	9030	Relay
● SPFCFutebol (1)	1.42 MiB/s	1y 24d 23h	BR		-	⚡ HS ⚡ ⚡ ⚡ ⚡ ⚡ ⚡ ⚡ ⚡	⚠	9001	9030	Relay
● cnsp1 (1)	1.42 MiB/s	1d 18h	BR		-	⚡ ⚡ ⚡ ⚡ ⚡ ⚡ ⚡ ⚡ ⚡ ⚡	⚠	443	0	Relay
● anarres (2)	1.41 MiB/s	10d 6h	BR		-	⚡ HS ⚡ ⚡ ⚡ ⚡ ⚡ ⚡ ⚡ ⚡		9000	9001	Relay
● anarres (2)	1.41 MiB/s	10d 6h	BR		-	⚡ HS ⚡ ⚡ ⚡ ⚡ ⚡ ⚡ ⚡ ⚡		9100	9101	Relay
● vovis (1)	1.39 MiB/s	2d 17h	BR		-	⚡ ⚡ ⚡ ⚡ ⚡ ⚡ ⚡ ⚡ ⚡ ⚡		9001	9030	Relay
● BrasilHostil (7)	1.35 MiB/s	1d 23h	BR		-	⚡ ⚡ ⚡ ⚡ ⚡ ⚡ ⚡ ⚡ ⚡ ⚡		9300	0	Relay
● alqnetwork (1)	1.29 MiB/s	3d 15h	BR		-	⚡ ⚡ ⚡ ⚡ ⚡ ⚡ ⚡ ⚡ ⚡ ⚡		443	80	Relay
● 1964NuncaMais (6)	1.29 MiB/s	11d 6h	BR		-	⚡ HS ⚡ ⚡ ⚡ ⚡ ⚡ ⚡ ⚡ ⚡	⚠	443	9000	Relay
● utzer2 (15)	1.27 MiB/s	243d 2h	BR		-	⚡ HS ⚡ ⚡ ⚡ ⚡ ⚡ ⚡ ⚡ ⚡	⚠	443	9030	Relay
● ImOHpi (1)	1.27 MiB/s	2d 18h	BR		-	⚡ ⚡ ⚡ ⚡ ⚡ ⚡ ⚡ ⚡ ⚡ ⚡		9003	9030	Relay
● cebolitos (1)	1.24 MiB/s	7d 18h	BR		-	⚡ HS ⚡ ⚡ ⚡ ⚡ ⚡ ⚡ ⚡ ⚡		9001	0	Relay
● snap269 (1)	1.23 MiB/s	7d 2h	BR		-	⚡ ⚡ ⚡ ⚡ ⚡ ⚡ ⚡ ⚡ ⚡ ⚡		44797	0	Relay
● Bolsonaro2018 (1)	1.19 MiB/s	5d 3h	BR		-	⚡ HS ⚡ ⚡ ⚡ ⚡ ⚡ ⚡ ⚡ ⚡		12345	23456	Relay
● ecramprelay1 (1)	1.18 MiB/s	4d 10h	BR		-	⚡ HS ⚡ ⚡ ⚡ ⚡ ⚡ ⚡ ⚡ ⚡	⚠	9001	0	Relay
● snap269 (1)	1.09 MiB/s	1d 10h	BR		-	⚡ ⚡ ⚡ ⚡ ⚡ ⚡ ⚡ ⚡ ⚡ ⚡		46593	0	Relay
● desnaturaludo (1)	987.72 KiB/s	17d 19h	BR		-	⚡ ⚡ ⚡ ⚡ ⚡ ⚡ ⚡ ⚡ ⚡ ⚡		20044	20045	Relay
● sucuri (1)	802 KiB/s	2d 6h	BR		-	⚡ ⚡ ⚡ ⚡ ⚡ ⚡ ⚡ ⚡ ⚡ ⚡		9001	9030	Relay
● snap269 (1)	772 KiB/s	4h 34m	BR		-	⚡ ⚡ ⚡ ⚡ ⚡ ⚡ ⚡ ⚡ ⚡ ⚡		41213	0	Relay
● Bael (2)	657.77 KiB/s	205d 2h	BR		-	⚡ ⚡ ⚡ ⚡ ⚡ ⚡ ⚡ ⚡ ⚡ ⚡	⚠	9001	9030	Relay
● Coderi (2)	640.8 KiB/s	124d 6h	BR		-	⚡ ⚡ ⚡ ⚡ ⚡ ⚡ ⚡ ⚡ ⚡ ⚡	⚠	9001	9030	Relay
● Tapioca (1)	594.63 KiB/s	23d 22h	BR		-	⚡ HS ⚡ ⚡ ⚡ ⚡ ⚡ ⚡ ⚡ ⚡		443	9030	Relay
Total	35.97 MiB/s									

Showing 1 to 25 of 47 entries





PRIVACY & ANONYMITY OS

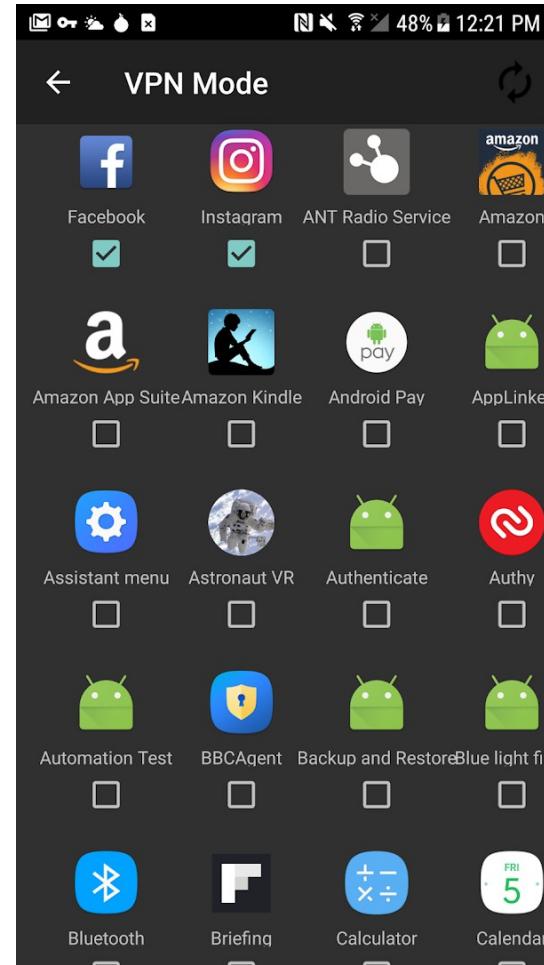
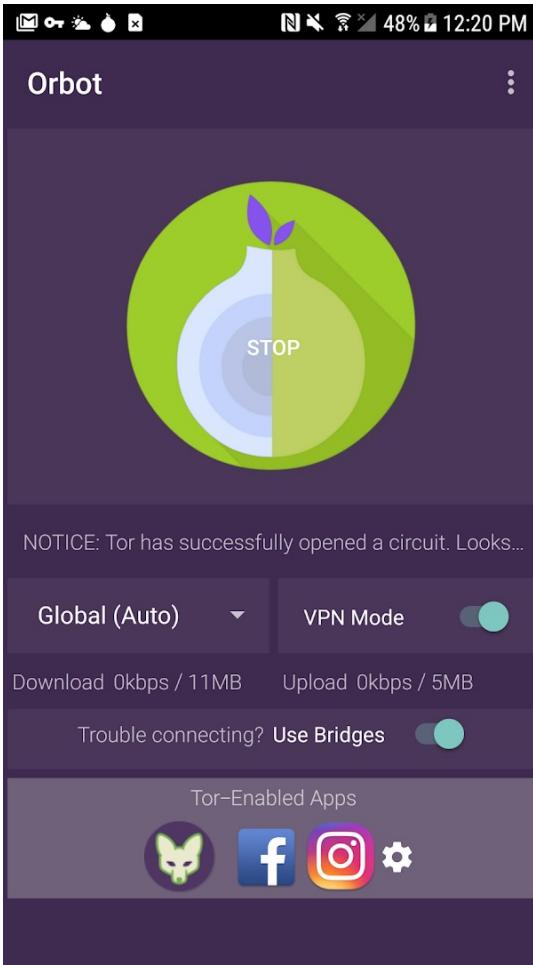


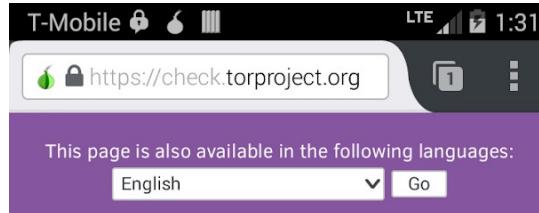
QUBES OS



GUARDIAN PROJECT

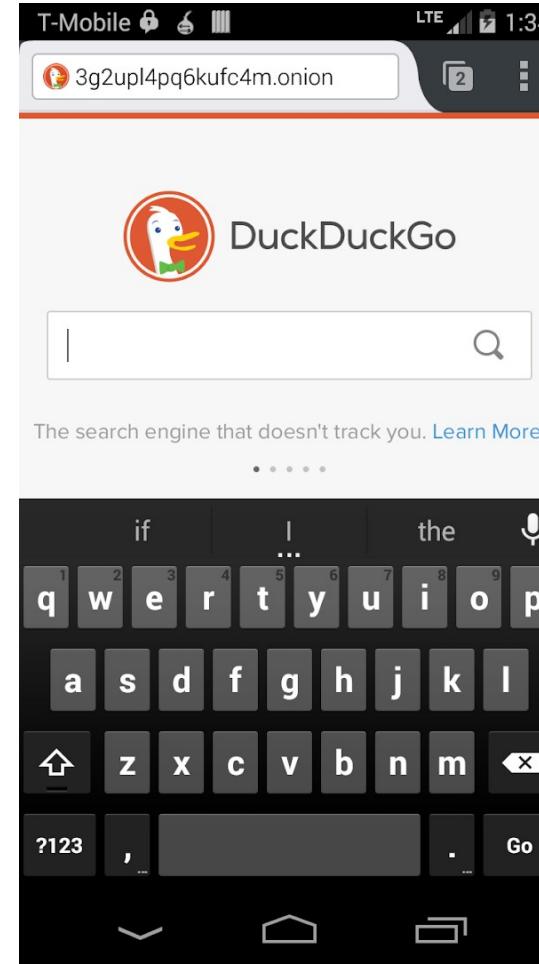
<https://guardianproject.info>

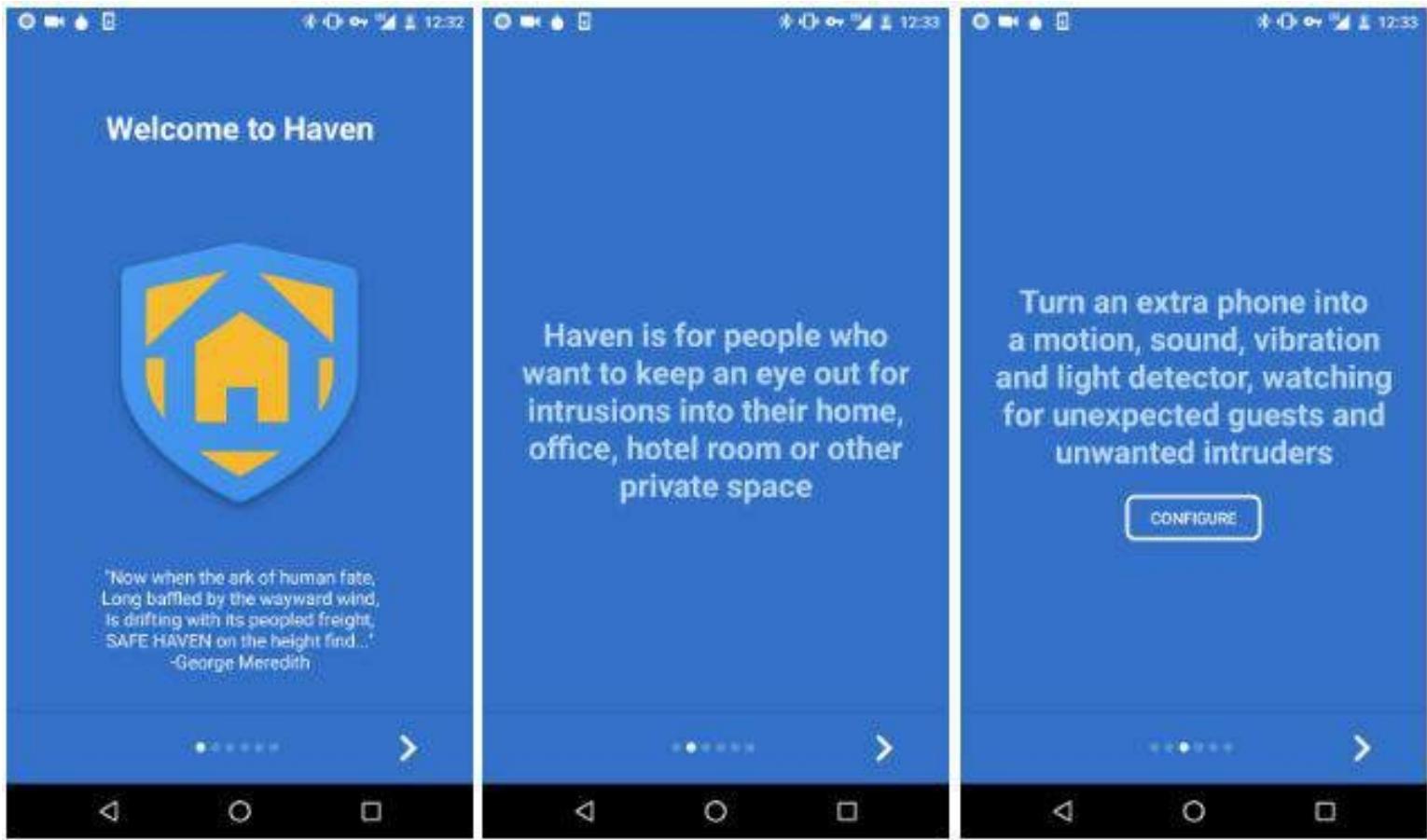




**Congratulations.
This browser is
configured to
use Tor.**

Your IP address appears to be:







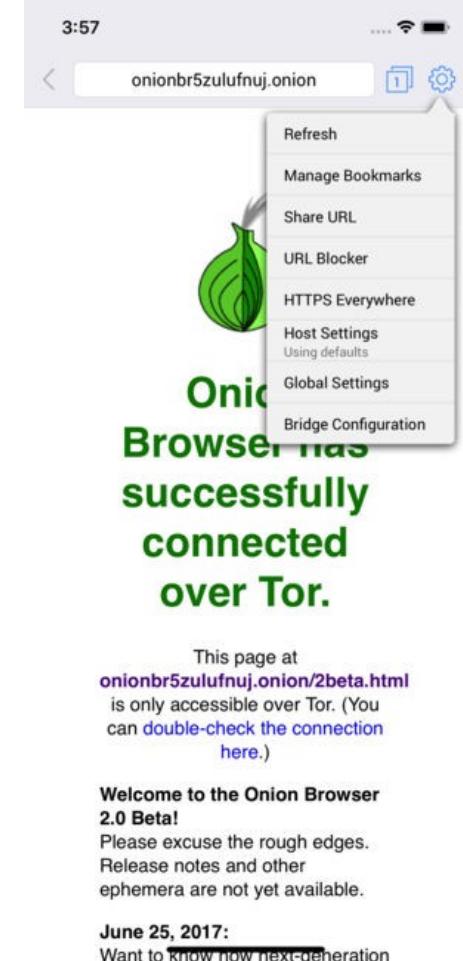
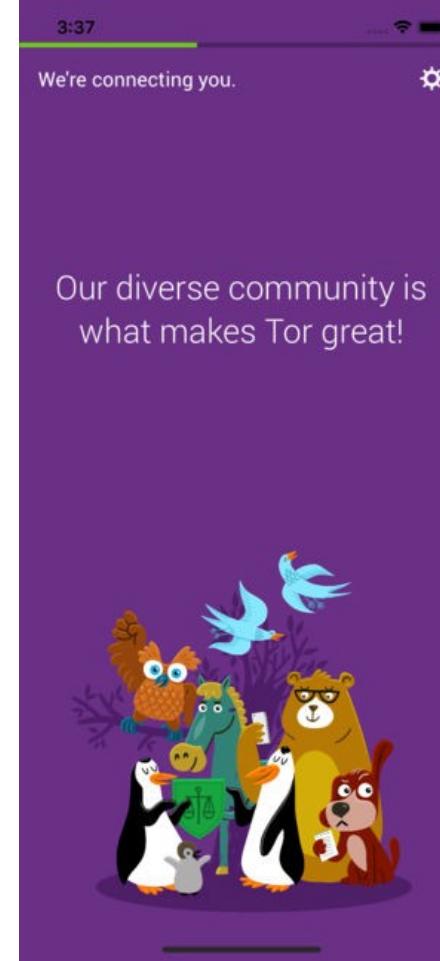
Onion Browser

17+

Secure, anonymous web with Tor
Mike Tigas

★★★★★ 3.7, 328 Ratings

Free · Offers In-App Purchases



Ricochet I.M.

Mensagens instantâneas anônimas para privacidade real; uma abordagem diferente que não confia em ninguém para proteger sua privacidade.

- *elimina metadados. ninguém sabe quem você é, nem com quem fala ou o que você diz;*
- *presa anônimo. compartilhe o que você quer, sem compartilhar sua identidade e localização;*
- *ausenta escutas. não há servidores para monitorar, censurar ou comprometer;*
- *seguro por padrão. a segurança não é segura até que seja automática e fácil de usar.*



The image shows two windows from the Ricochet application. The left window, titled "Ricochet", displays a list of connections: "En ligne" (online) with "Lecteur 1" connected, and a "REQUÊTES" section with "John Brooks". The right window, titled "Lecteur 1", shows a conversation between "Lecteur 1" and "John Brooks". The messages are:

- Lecteur 1: Salut !
- John Brooks: Salut Korben !
- Lecteur 1: ça fonctionne, c'est cool. A qui ai je l'honneur ?
- John Brooks: Oui, c'est cool. Je suis un lecteur de ton site, Paul.
- Lecteur 1: enchanté !
- John Brooks: j'ai commenté qu'une fois un article sur Mario64 porté sur plateforme x86



Briar é um aplicativo de mensagens projetado para quaisquer pessoas que precisem se comunicar com outras pessoas ou entidades de uma forma segura, fácil e robusta.

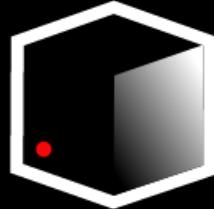
Ao contrário de aplicativos semelhantes, ele não depende de servidores dedicados à entrega das mensagens.

Caso sua conexão com a Internet não esteja funcionando, o aplicativo pode sincronizar via Bluetooth ou Wi-Fi, mantendo as informações fluindo. O tráfego pela Internet também pode ser feito através da rede Tor.



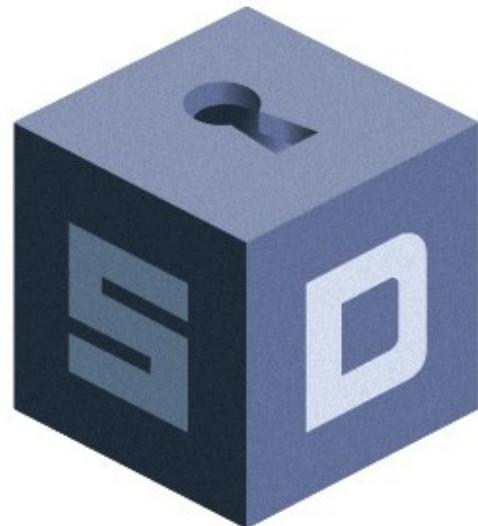
TorBirdy

THE NEW YORKER
SECUREDROP



<https://projects.newyorker.com/securedrop/>

Antes conhecido como *StrongBox*, o *SecureDrop* mantido pelo *New Yorker* é um serviço oferecido pelo jornal para que você possa compartilhar dicas, informações e arquivos dignos de se tornarem notícia, cuja importância ou sensibilidade exige um grau maior de anonimato e segurança do que é oferecido por meios convencionais.



<https://securedrop.org/overview>

SECUREDROP

originalmente desenvolvido por Aaron Swartz e James Dolan, sob o nome de DeadDrop



The International Consortium
of Investigative Journalists



Nova Zelândia

The New York Times

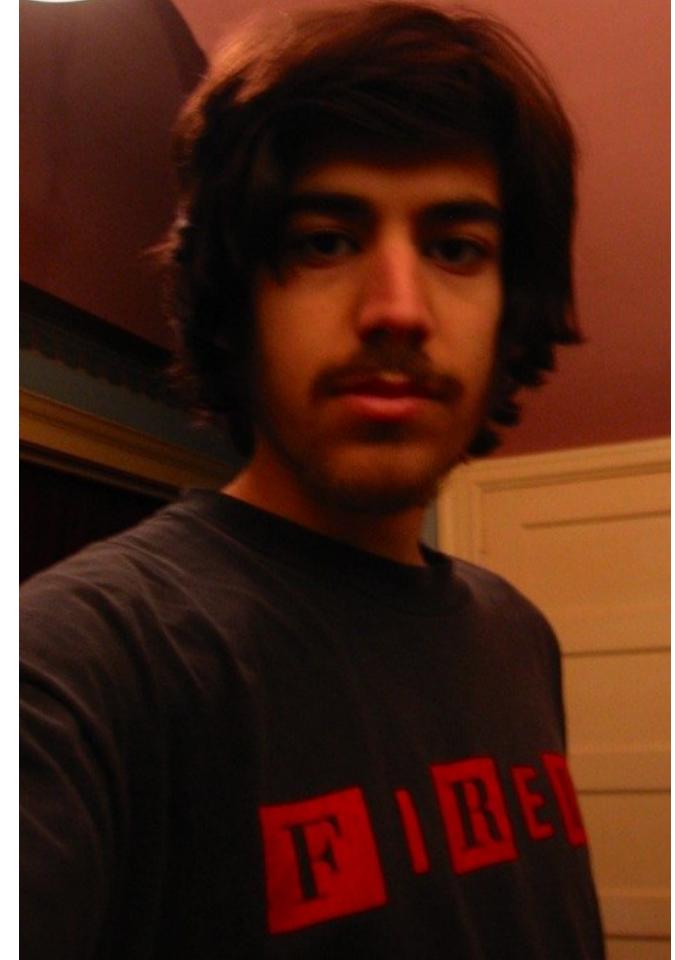




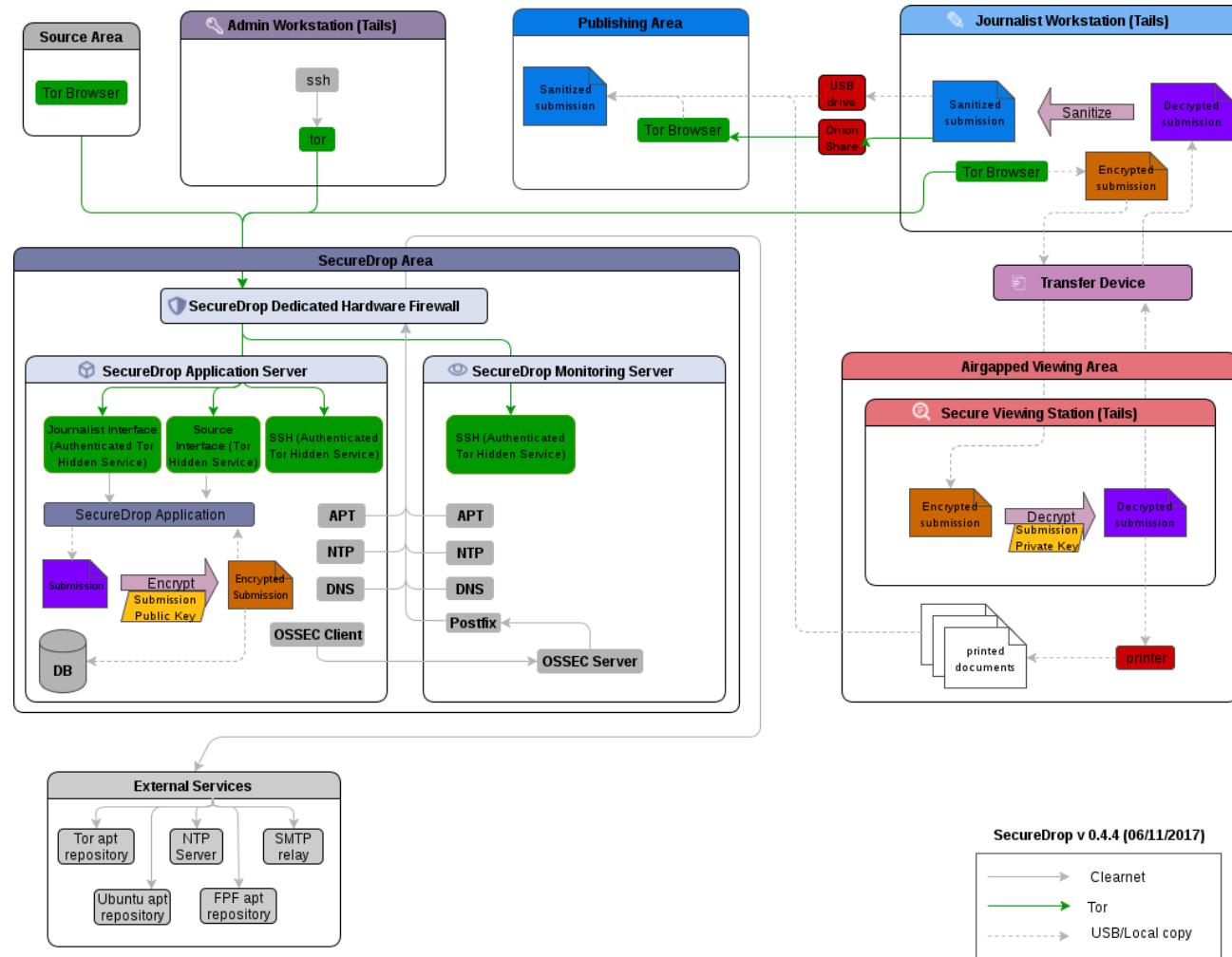
<https://securedrop.org/directory>



The
Intercept_



James Dolan e Aaron Swartz





torproject.org

"GloboLeaks (...) won't have any central point of failure"

Forbes

"Their project aims to make a suite of software (...) to (...) maintain a whistle-blowing platform"



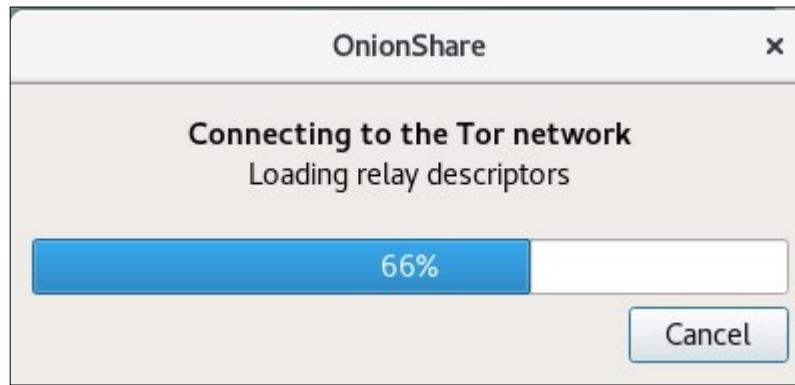
"Tor2web is a positive step for those who want to publish anonymously without sacrificing the exposure"

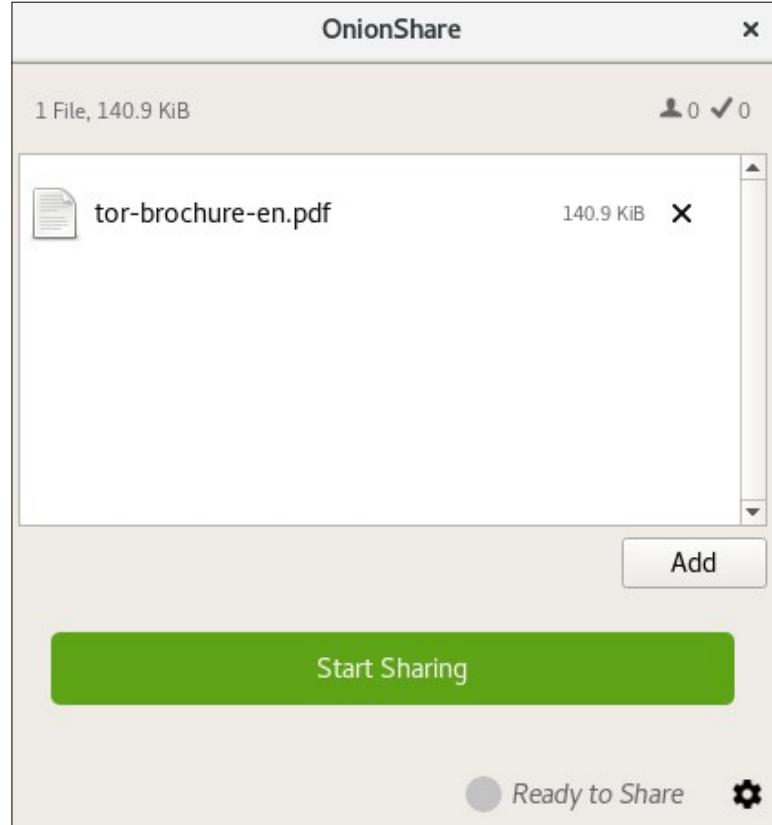


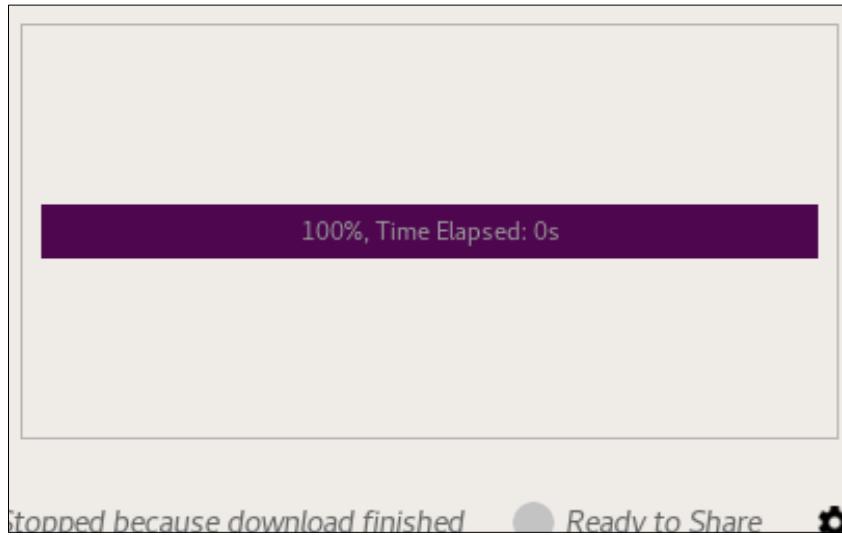
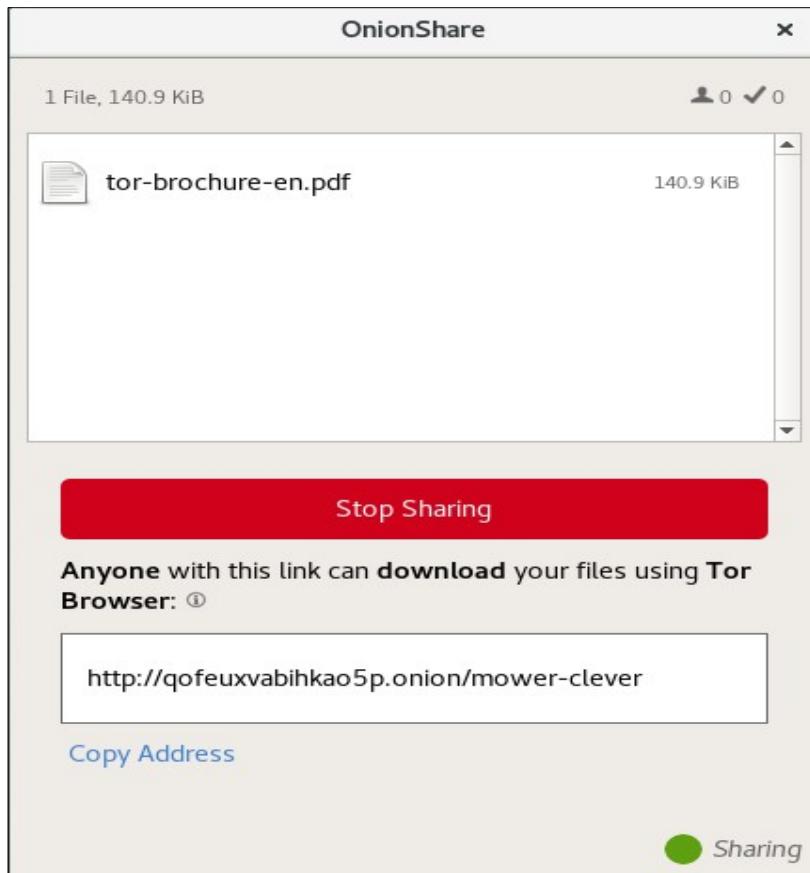
OnionShare



<https://onionshare.org>



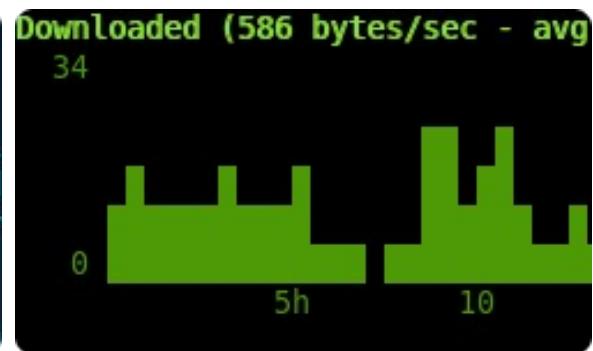


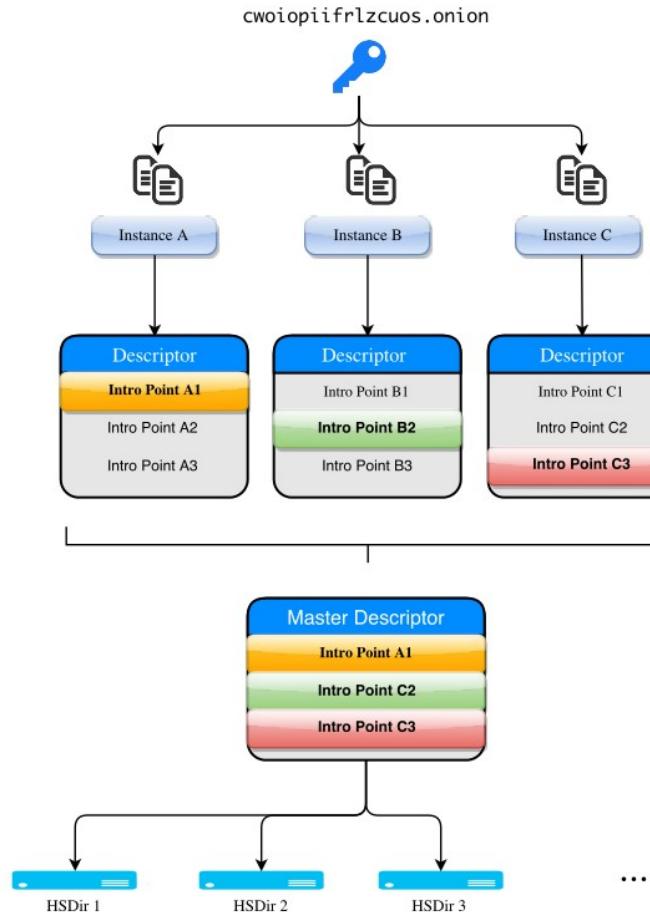


nyx

```
18:49:57 [INFO] router_pick_pub  
18:49:57 [INFO] resolve_my_addr  
    public IP addresses.  
18:49:57 [INFO] resolve_my_addr  
18:49:57 [INFO] resolve_my_addr  
18:49:57 [BW] READ: 586, WRITTE  
18:49:56 [BW] READ: 0, WRITTEN:  
18:49:55 [BW] READ: 0, WRITTEN:  
18:49:54 [BW] READ: 1172, WRITT
```

```
3 User tor  
4 DataDirectory /etc/tor  
5 SocksPort 0  
6 SocksListenAddress 127.0.0.1  
7 PidFile /var/run/tor/tor.pid  
8 Log notice file /var/log/tor  
9 RunAsDaemon 1  
10 ControlPort 9051  
11 HashedControlPassword 16:22B
```





- ferramentas extras
 - DNS
 - unbound;
 - BIND
 - doh-proxy (facebook);
 - dnscrypt-proxy;
 - GPG/PGP
 - keybase;
 - enigmail; k-9;
 - containers, e virtualização
 - docker; jails (FreeBSD);
 - KVM, Xen, VirtualBox, QEMU, bhyve (FreeBSD), vmm (OpenBSD).
 - BIOS e sistemas operacionais “*libres*”
 - coreboot;
 - libreboot;
 - trisquel;
 - pureos (purism);
 - librecmc;

- ferramentas extras
 - análise ou remoção de metadados
 - metagoofil;
 - mat;
 - detectores de intrusão
 - suricata;
 - snort;
 - zeek (bro);
 - gerenciadores de senhas
 - keepassx;
 - bitwarden
 - autenticação de múltiplos fatores
 - OTP
 - andotp;
 - linotp;
 - privacyidea;
 - yubikey;

- ferramentas extras

- miscelânia

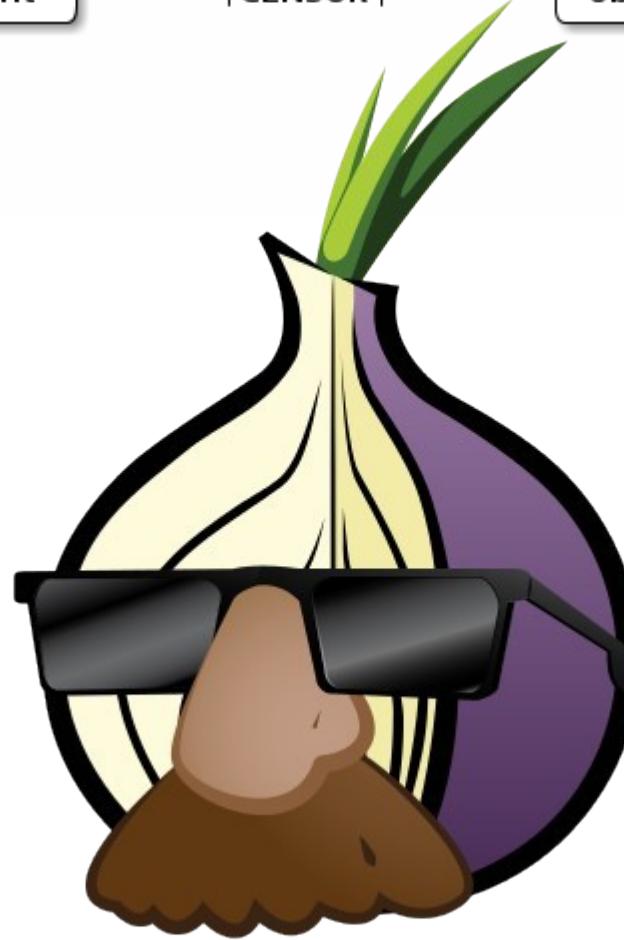
- nextcloud; owncloud; send (mozilla); up1 (riseup);
 - luks; veracrypt; geli (freebsd); bioctl (openbsd);
 - nautilus wipe, shred; dd; bcwipe;
 - ossec; clamav;
 - pf; ipfw, netfilter (iptables); npf; ufw;
 - wireshark (tshark); tcpdump;
 - socat; netcat (nc); redsocks; torsocks; proxychains;
 - privoxy; polipo; squid; haproxy;
 - ntpd; openntpd; ntpdate; htpdate;

informações adicionais sobre a rede

- ingresso de nós na rede
 - primeira fase (3 dias), medição passiva de banda;
 - segunda fase (5 dias), medição ativa de banda;
 - terceira fase (60 dias), indicação de consenso;
 - quarta fase (demais dias), promoção estável.
- obtenha o navegador com uma ajudinha extra
 - Get Tor
 - <https://gettor.torproject.org>;
 - https://twitter.com/get_tor (*atenção para o uso do sublinhado*)

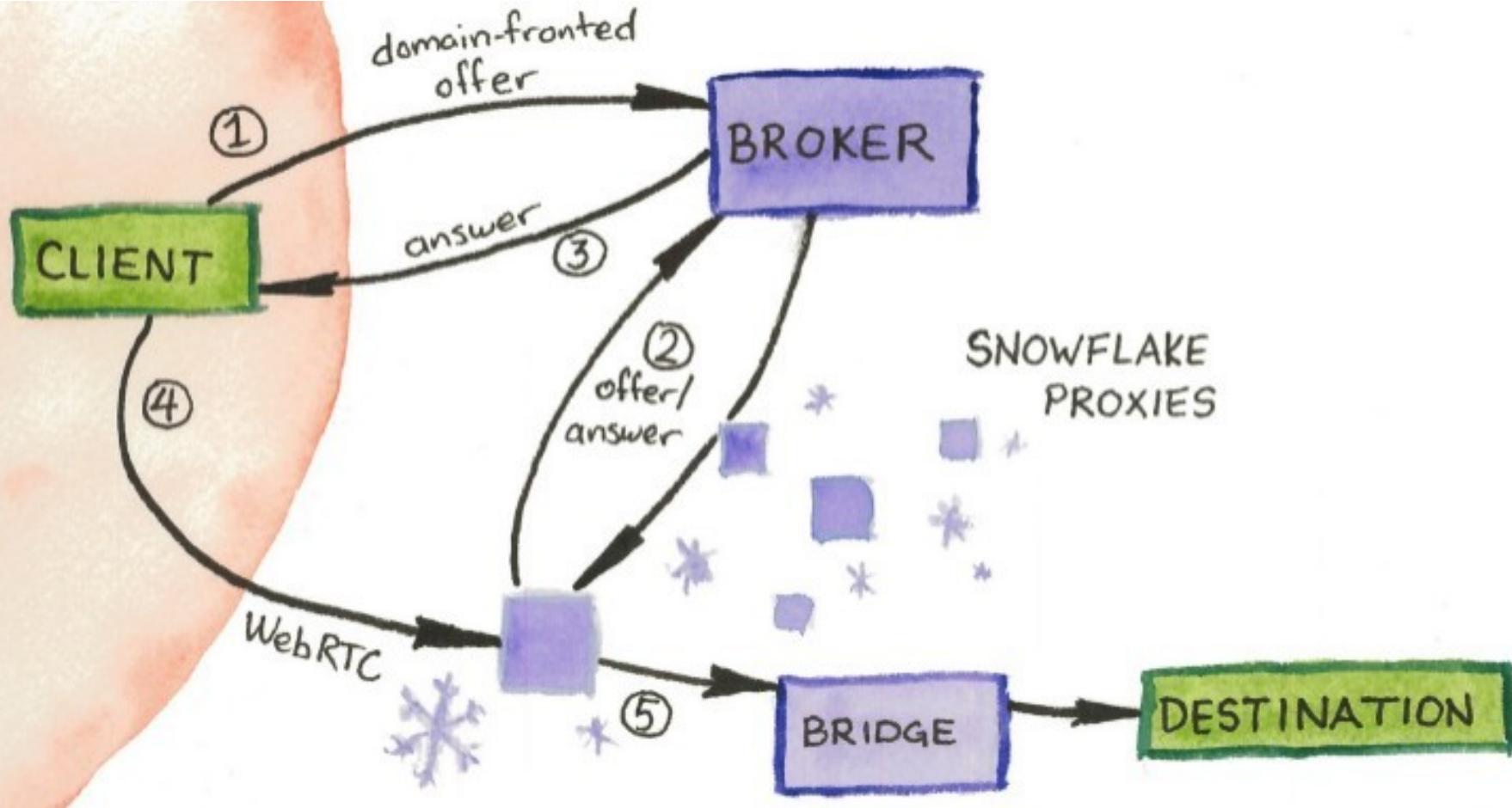
- pontes (nós de entrada camaradas)
 - semelhante a um nó guarda;
 - lista com endereços não é publicada;
 - <https://bridges.torproject.org>;
 - bridges@torproject.org – Gmail, Riseup, Yahoo!;
 - compartilhada (disponível quando solicitada manualmente);
 - privada (disponível apenas para vc, ou contatos próximos);
 - embutidas no navegador;
 - auxilio dos obfuscadores de tráfego.

obfuscadores de tráfego



- obfuscadores de tráfego
 - **fte**, imita tráfego HTTP comum;
 - **obfs**
 - **obfs3**, gera tráfego randomizado;
 - **obfs4**, aprimoração do anterior que funciona na China;
 - **meek**
 - meek-amazon;
 - meek-azure (funciona na China).

- flashproxy (Stanford) | Web Socket
- stegotorus (SRI/CMU) | HTTP
- SkypeMorph (Waterloo) | Skype Videocall
- uProxy (Google) | WebRTC
- ScrambleSuit (Karlstad) | obfs-based
- Telex (Michigan/Waterloo) | Traffic Divert



serviços acebolados

- ***.onion**
 - */torspec/address-spec.txt*;
 - */torspec/rend-spec-v2.txt*;
 - */torspec/rend-spec-v3.txt*.
- encriptação fim-a-fim;
- auto-autenticados (dispensa autoridade certificadora);
- drible sob tradução de endereços de rede (NAT punching);
- não necessita sair para a Internet;
 - menor contato com mundo exterior;
- modo privado/restrito (stealth mode);
- HTTP*, SSH/SFTP, SMTP/IMAP, ...

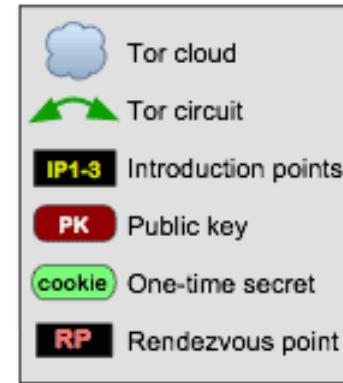
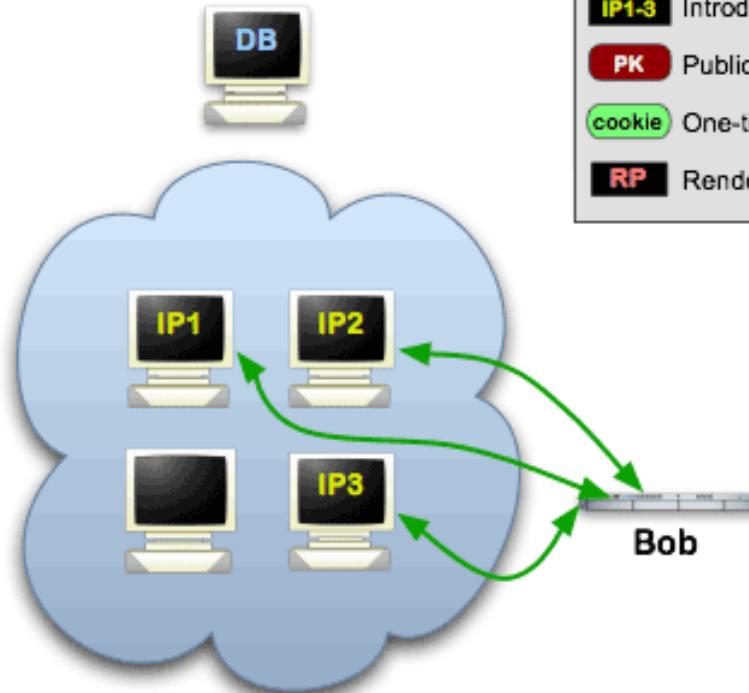


Onion Services: Step 1

Step 1: Bob picks some introduction points and builds circuits to them.



Alice



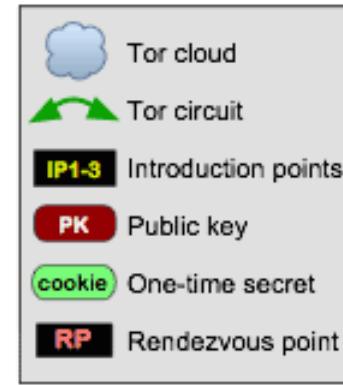
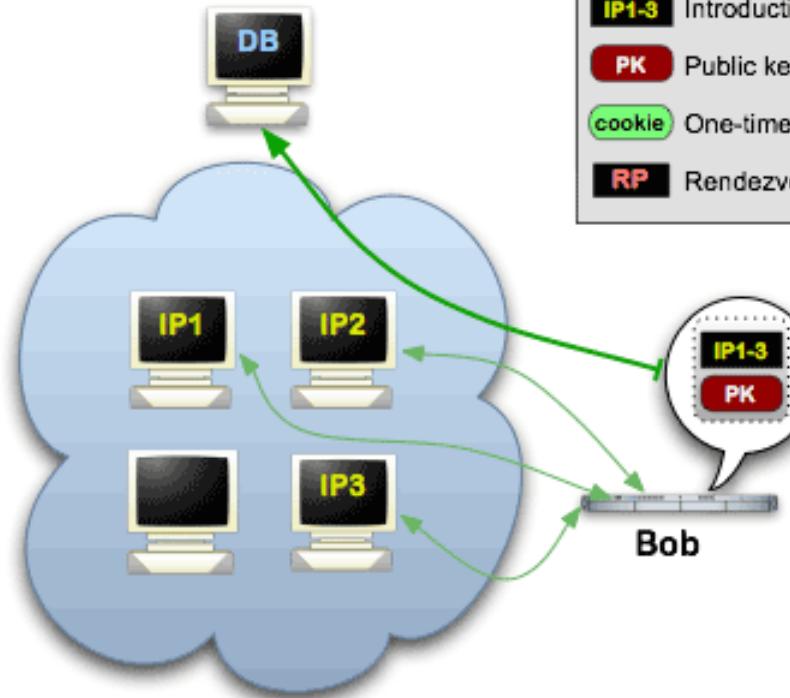


Onion Services: Step 2

Step 2: Bob advertises his service -- XYZ.onion -- at the database.



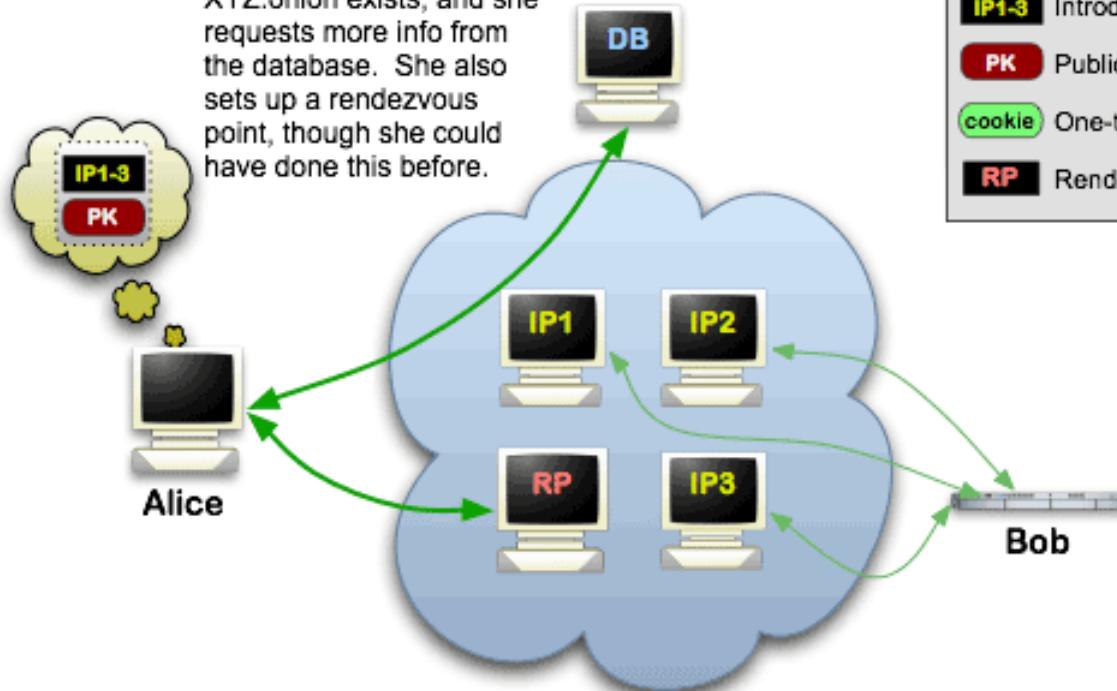
Alice





Onion Services: Step 3

Step 3: Alice hears that XYZ.onion exists, and she requests more info from the database. She also sets up a rendezvous point, though she could have done this before.

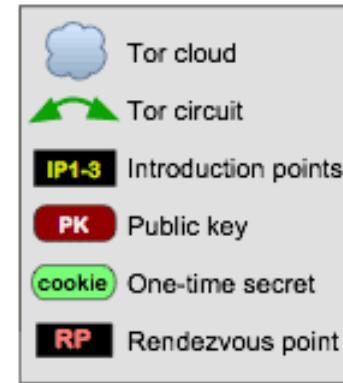
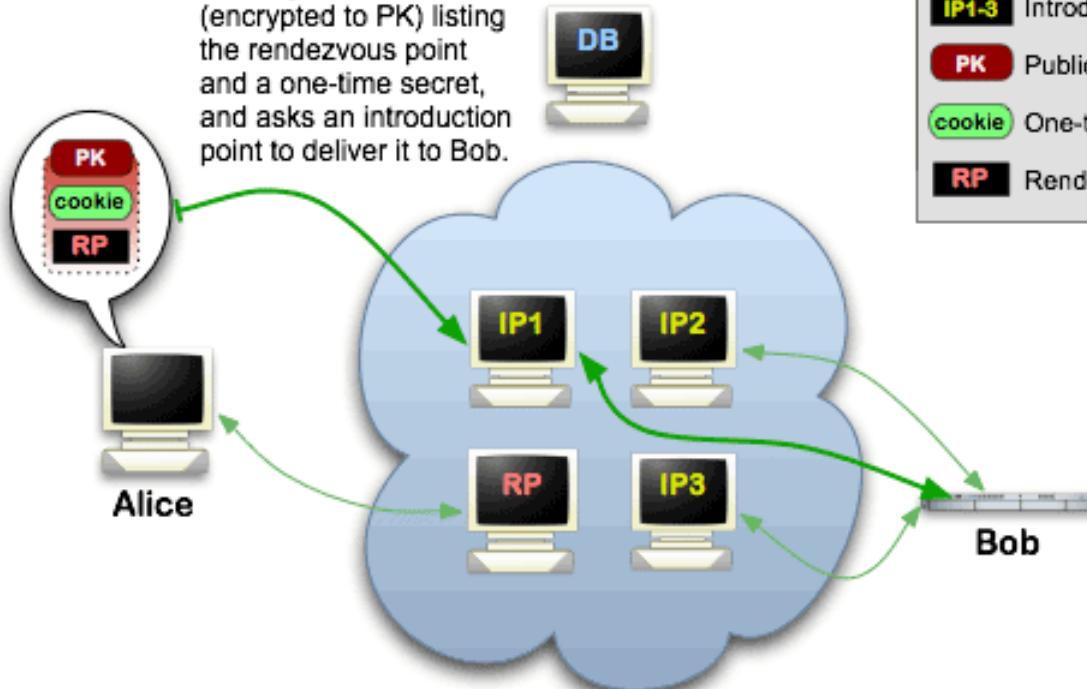


	Tor cloud
	Tor circuit
	IP1-3 Introduction points
	PK Public key
	cookie One-time secret
	RP Rendezvous point



Onion Services: Step 4

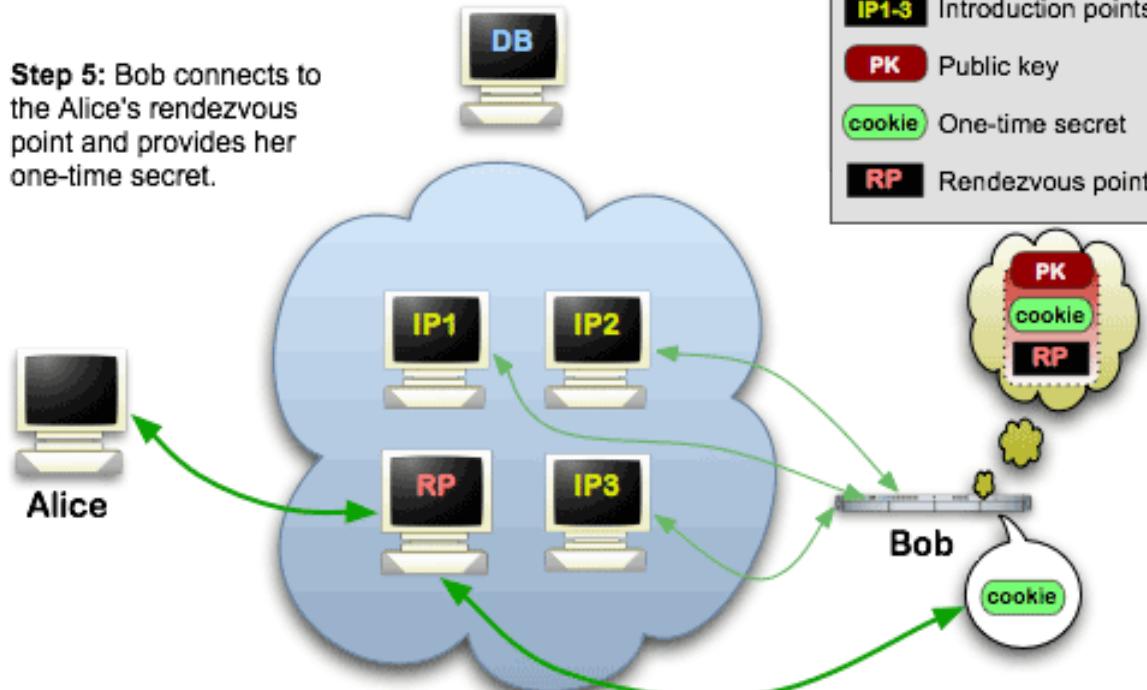
Step 4: Alice writes a message to Bob (encrypted to PK) listing the rendezvous point and a one-time secret, and asks an introduction point to deliver it to Bob.





Onion Services: Step 5

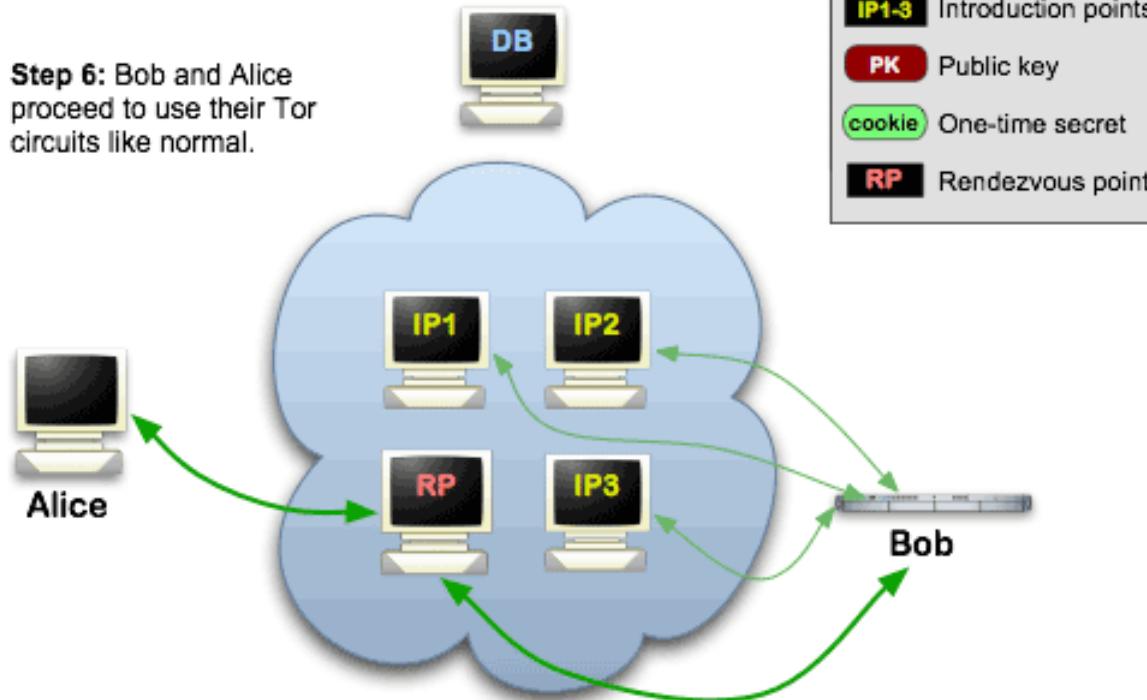
Step 5: Bob connects to the Alice's rendezvous point and provides her one-time secret.





Onion Services: Step 6

Step 6: Bob and Alice proceed to use their Tor circuits like normal.



gráficos e números interessantes



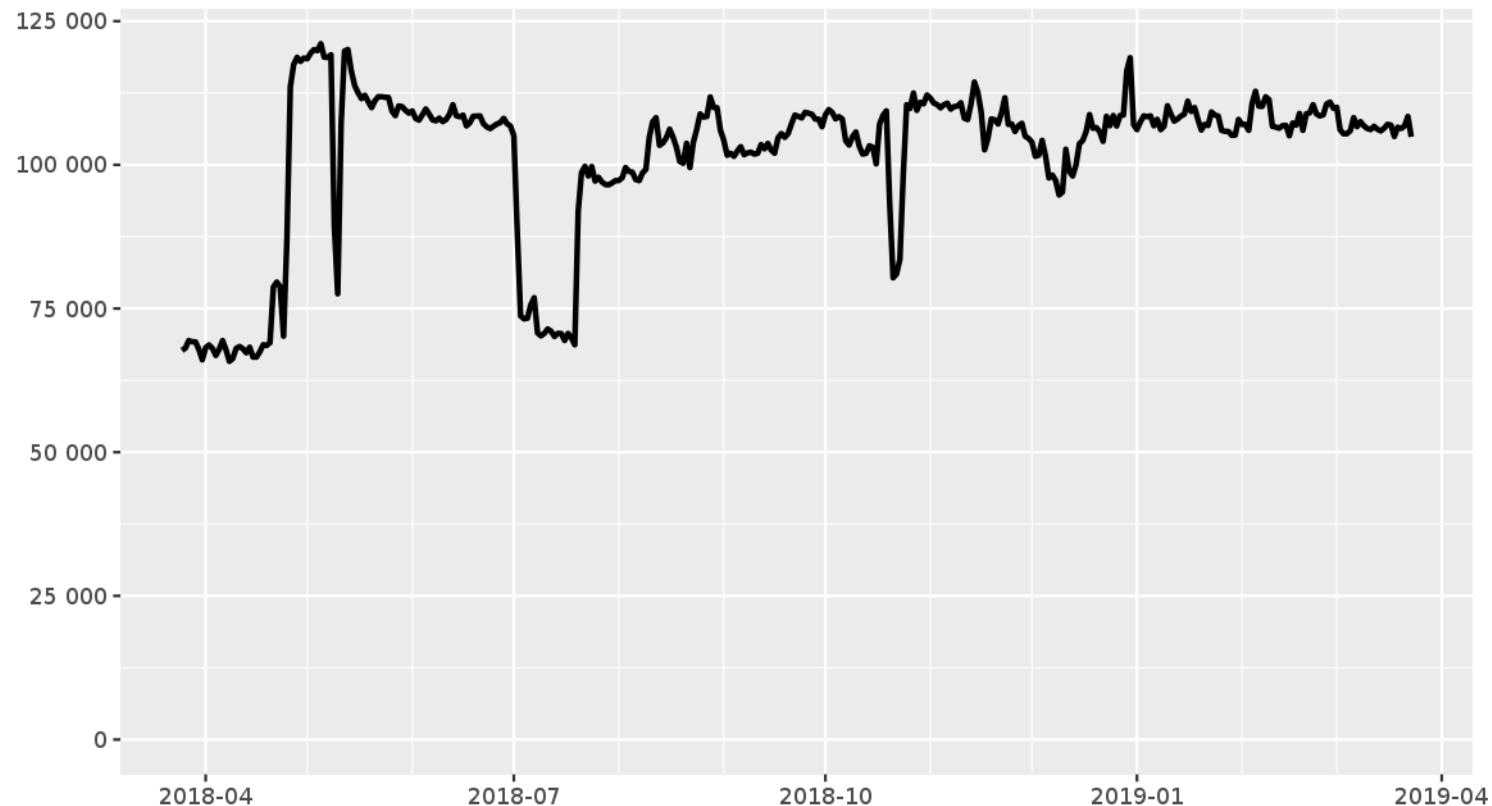
1 Million People use Facebook over Tor

 FACEBOOK OVER TOR · FRIDAY, APRIL 22, 2016 

People who choose to communicate over Tor do so for a variety of reasons related to privacy, security and safety. As we've written previously it's important to us to provide methods for people to use our services securely – particularly if they lack reliable methods to do so.

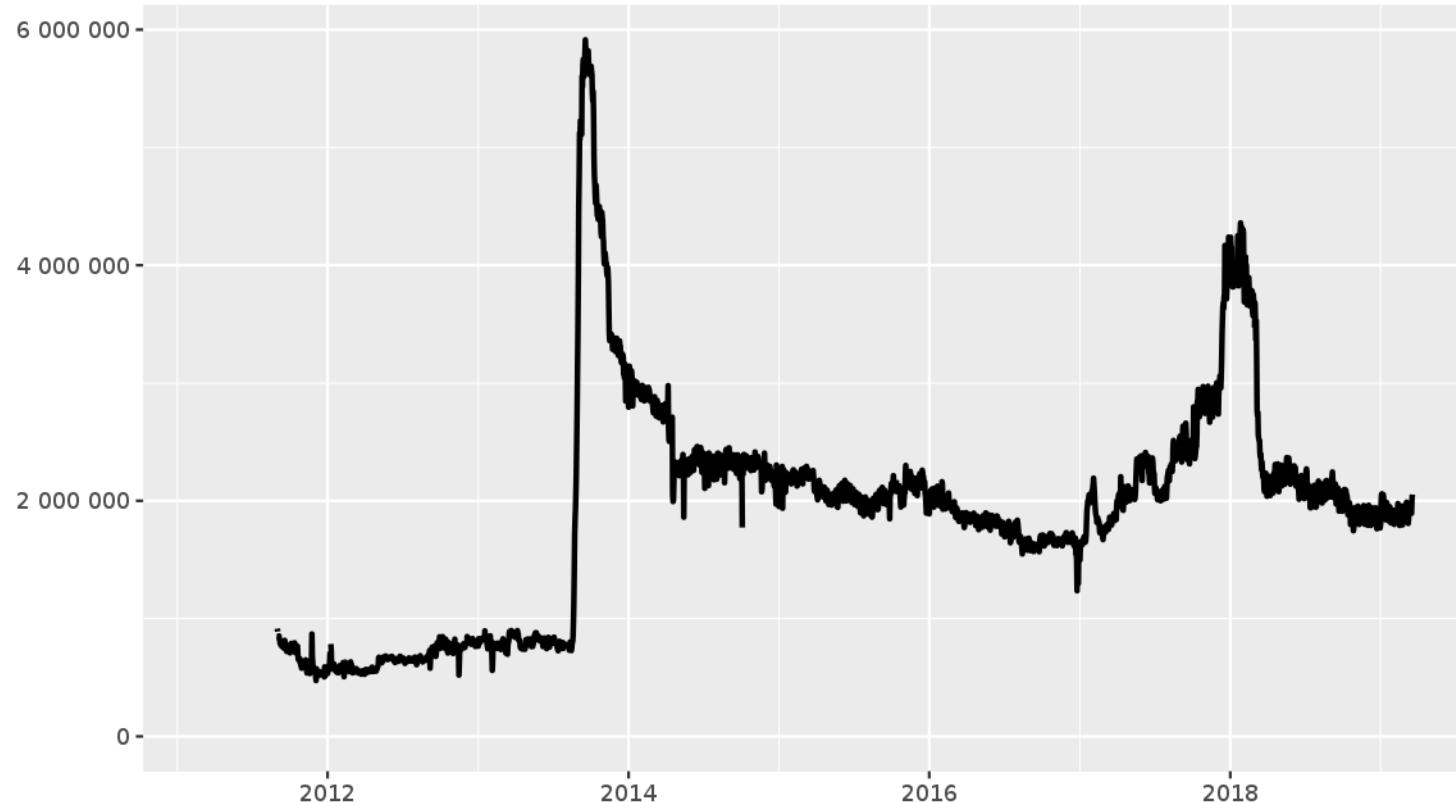
<https://www.facebook.com/notes/facebook-over-tor/1-million-people-use-facebook-over-tor/865624066877648>

Unique .onion addresses



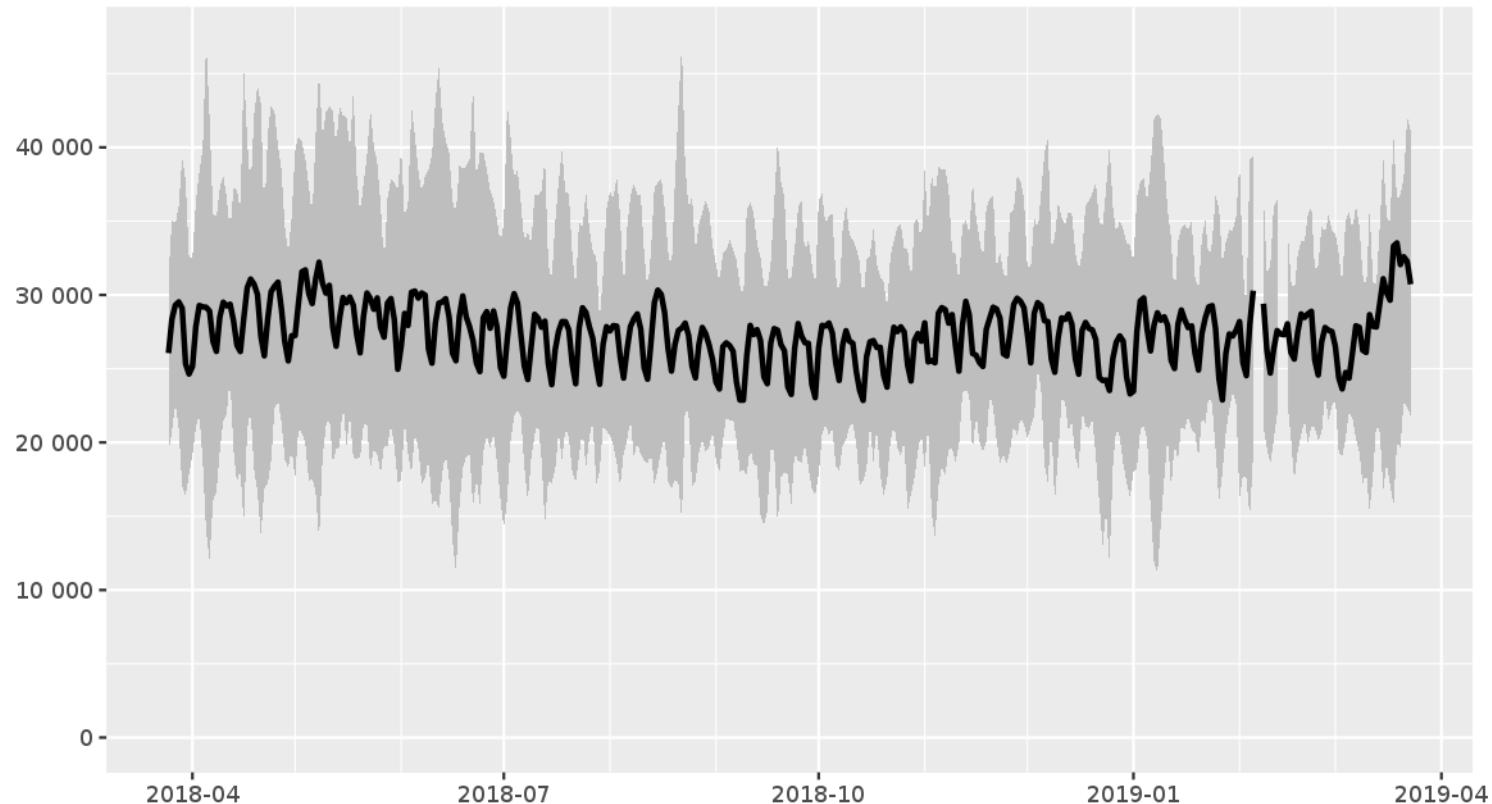
The Tor Project - <https://metrics.torproject.org/>

Directly connecting users



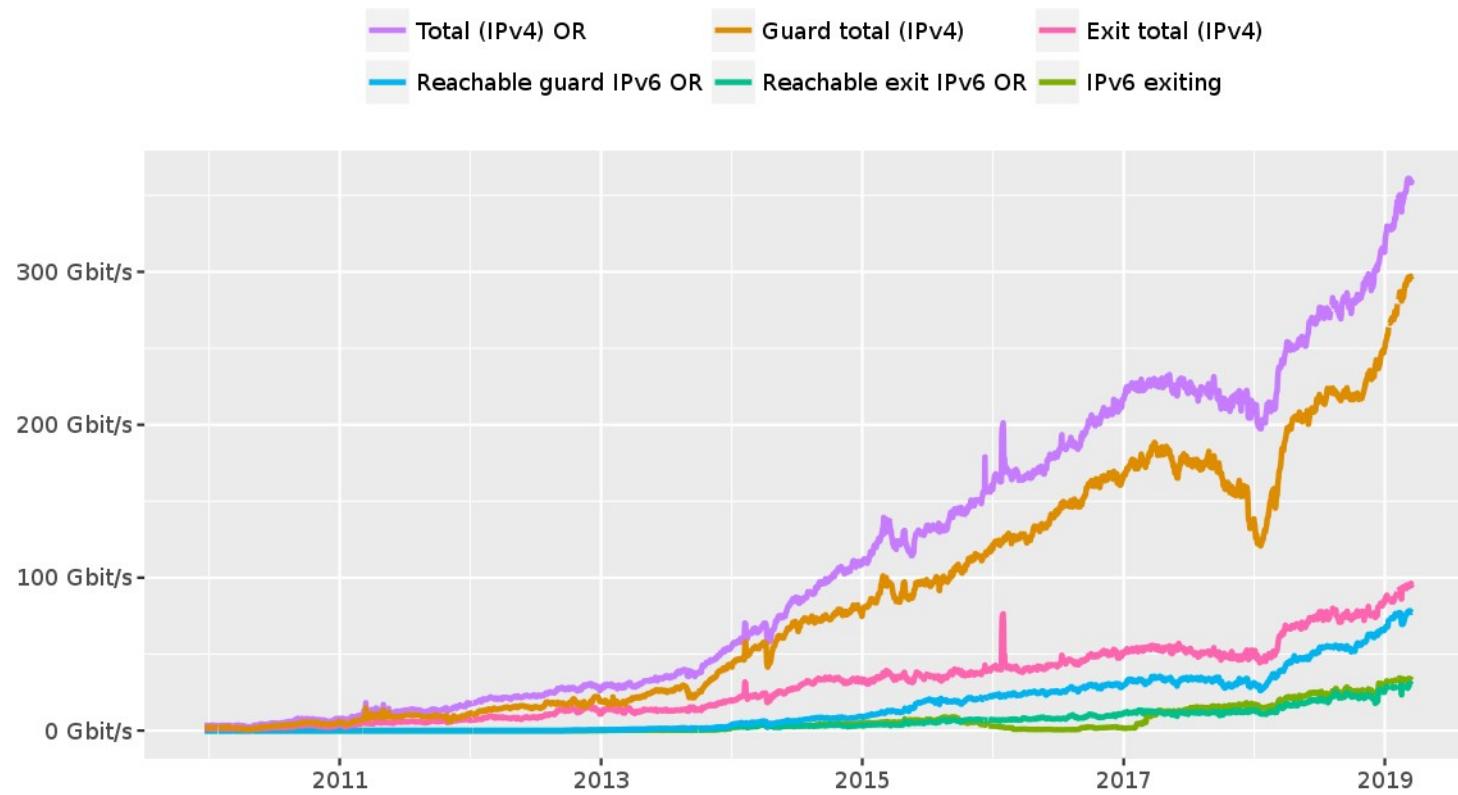
The Tor Project - <https://metrics.torproject.org/>

Directly connecting users from Brazil



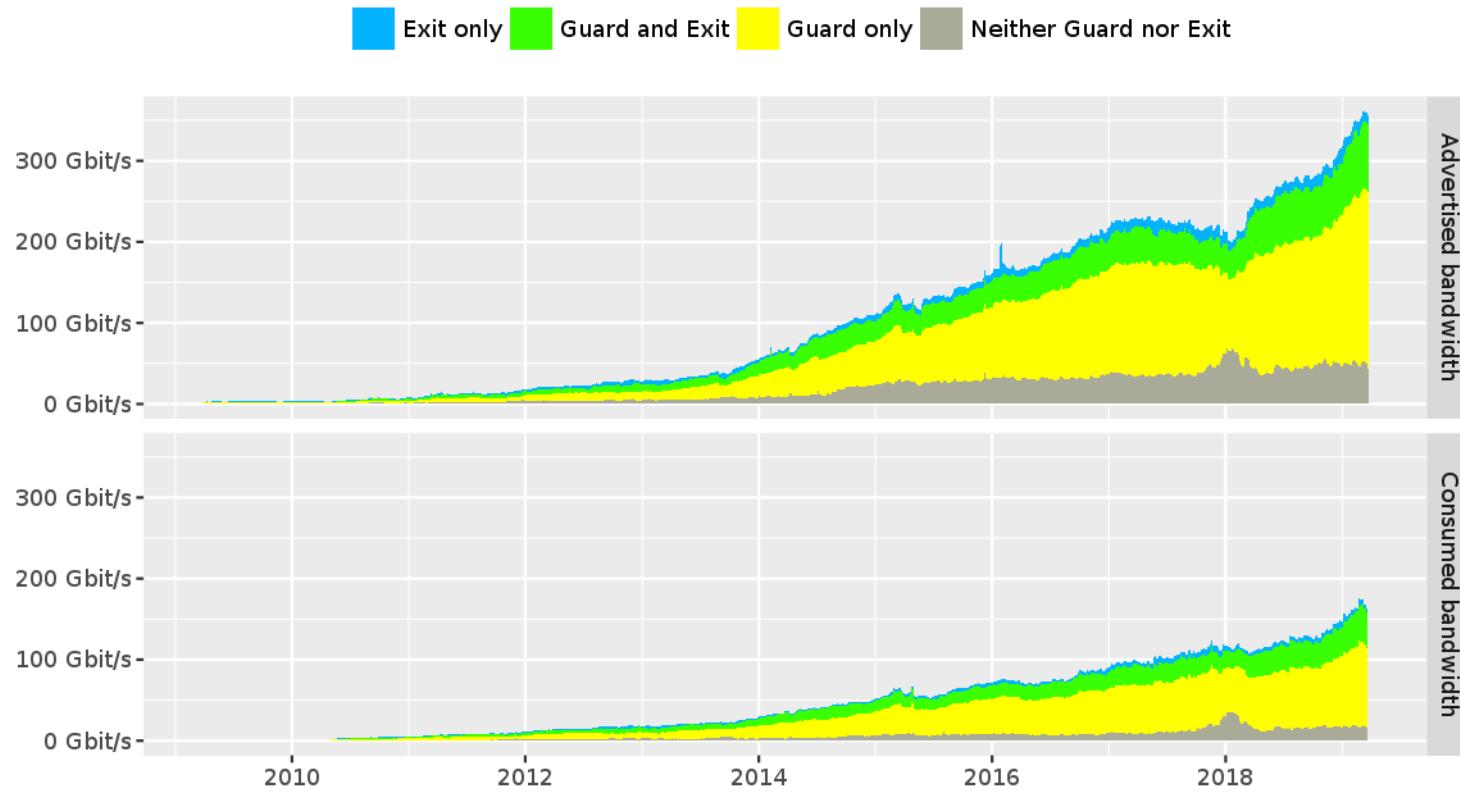
The Tor Project - <https://metrics.torproject.org/>

Advertised bandwidth by IP version



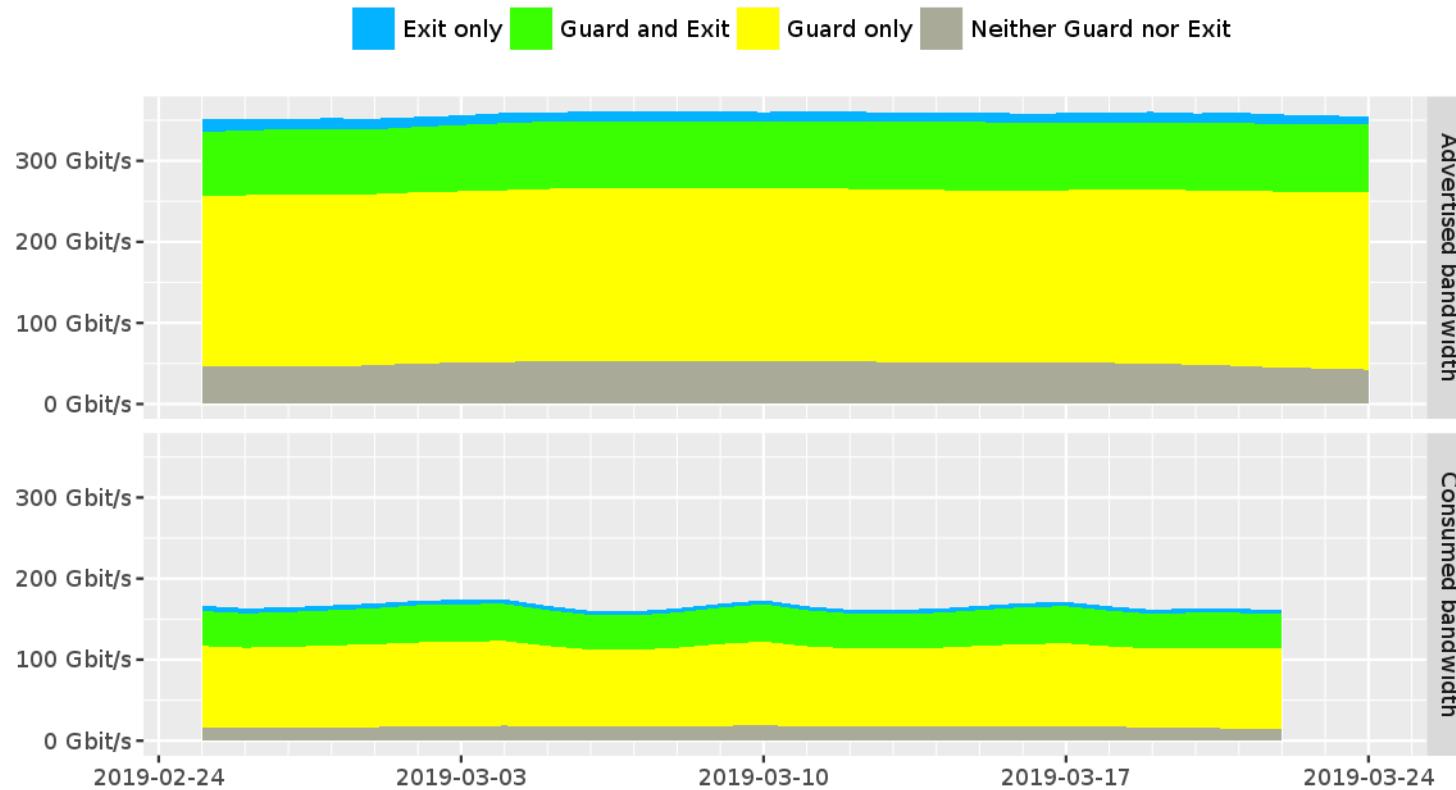
The Tor Project - <https://metrics.torproject.org/>

Advertised and consumed bandwidth by relay flags



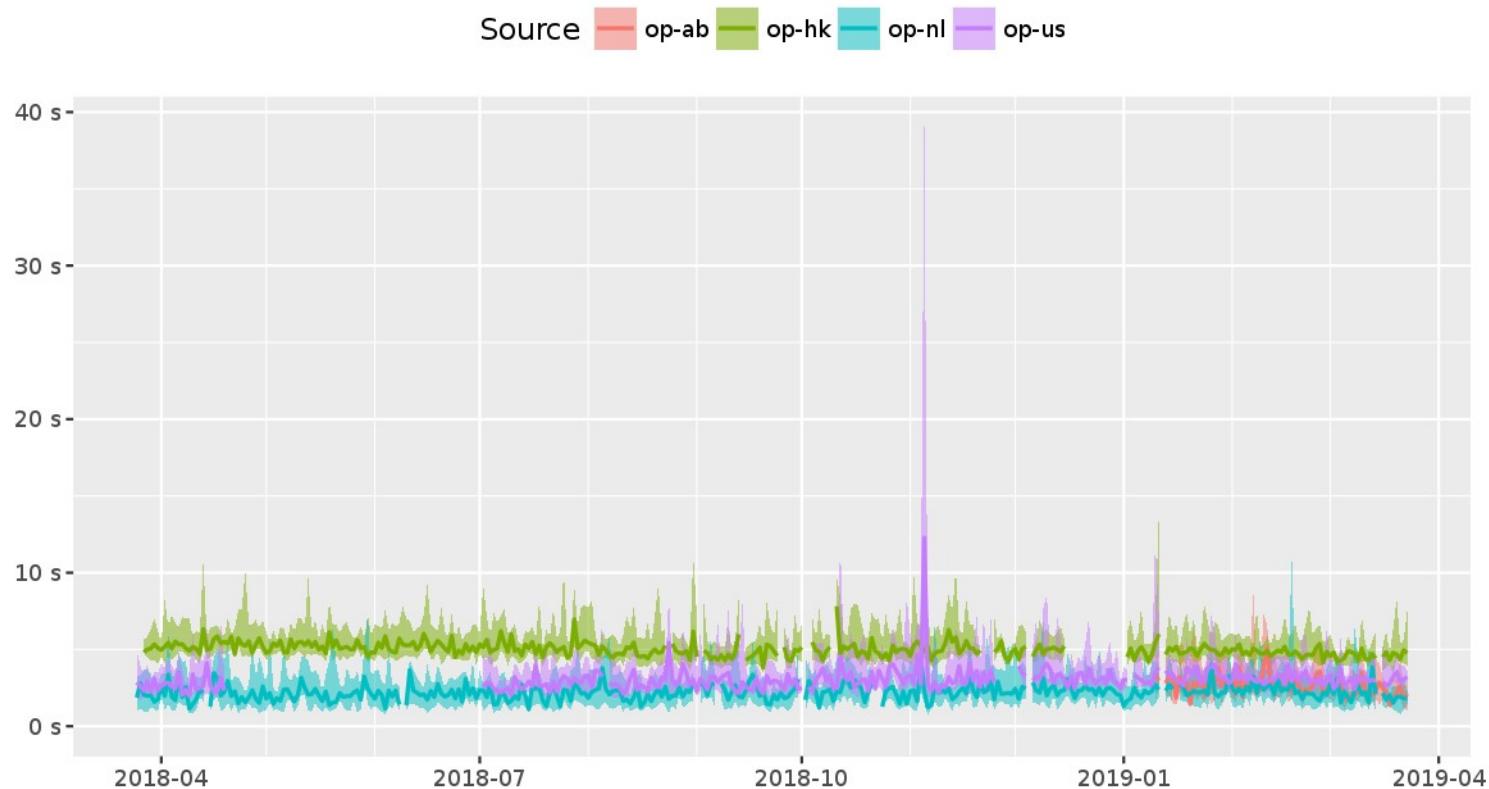
The Tor Project - <https://metrics.torproject.org/>

Advertised and consumed bandwidth by relay flags

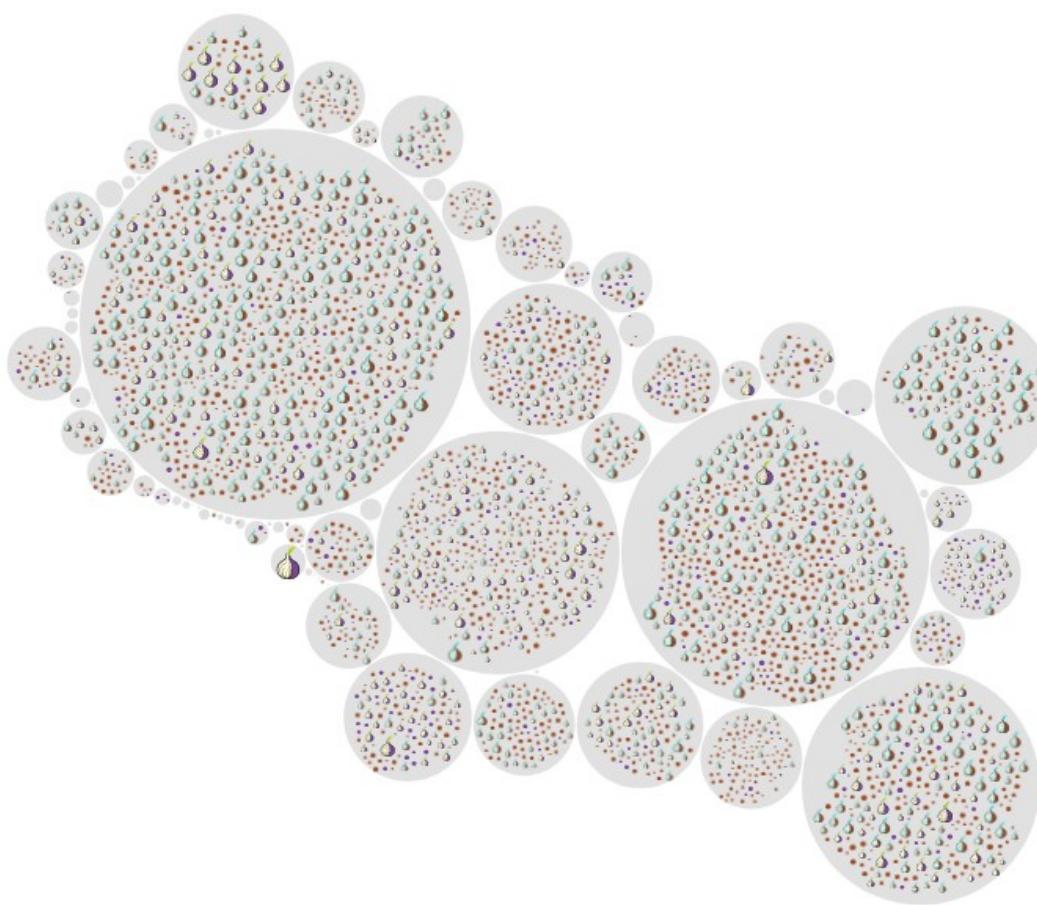


The Tor Project - <https://metrics.torproject.org/>

Time to complete 1 MiB request to public server

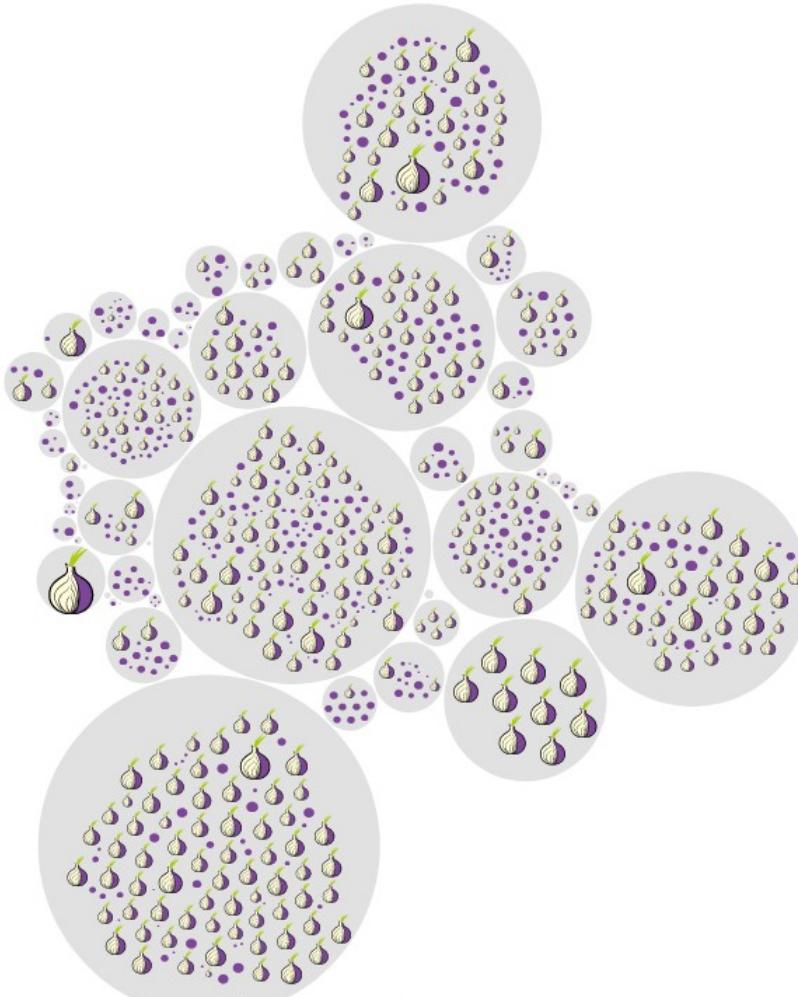


The Tor Project - <https://metrics.torproject.org/>



85 countries with 6608 relays (3215 visible)

2019-03-20 19:00:00



55 countries with 893 exits (750 visible)
2019-03-20 19:00:00



colaboração, suporte e pesquisa

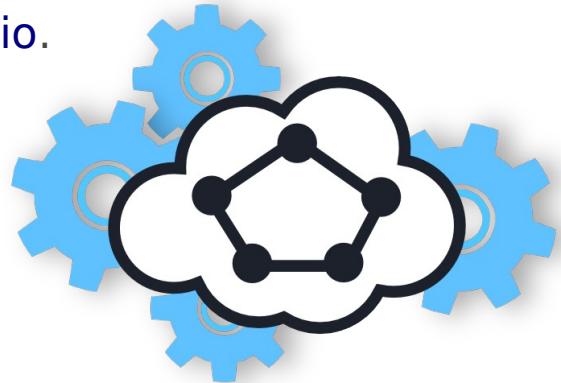
- sítio web oficial (em português)
 - <https://www.torproject.org/pt-BR;>
- canais de comunicação
 - <https://blog.torproject.org;>
 - [https://twitter.com/torproject;](https://twitter.com/torproject)
- métricas, status e históricos
 - [https://metrics.torproject.org;](https://metrics.torproject.org/)
 - [https://metrics.torproject.org/exonerator.html;](https://metrics.torproject.org/exonerator.html)
 - [https://torstatus.rueckgr.at;](https://torstatus.rueckgr.at)
 - [https://torstatus.blutmagie.de;](https://torstatus.blutmagie.de)
 - [https://onionite.now.sh;](https://onionite.now.sh)
 - [https://github.com/kargig/tormap;](https://github.com/kargig/tormap)

- IRC (OFTC.net)
 - #tor, #tor-dev, #tor-relays, #tor-onions, **#tor-south**
 - #ooni, #ooni-dev
- listas de discussão
 - <https://lists.torproject.org>;
 - <https://www.nycbug.org/index?action=lists>.
- documentação (wiki)
 - <https://trac.torproject.org/projects/tor>;
 - <https://trac.torproject.org/projects/tor/wiki/org/teams/CommunityTeam/Projects/GlobalSouth>;
 - <https://wiki.torbsd.org>;
 - <https://trac.torproject.org/projects/tor/wiki/TorRelayGuide-ptbr>.

- entidades colaboradoras

- derechosdigitales.org;
- torservers.net
 - icetor.is;
 - digitale-gesellschaft.ch;
 - enn.lu;
 - awp.is;
- noisebridge.net;
- emeraldonion.org;
- nos-oignons.net;
- dfri.se.

- códigos fonte
 - <https://gitweb.torproject.org>;
 - <https://github.com/ooni>;
- pesquisa
 - <https://research.torproject.org>;
- simulação e testes
 - <https://trac.torproject.org/projects/tor/wiki/doc/TorChutneyGuide>;
 - <https://shadow.github.io>.





Tor Baião com Cebola

CriptoBaião - Fortaleza, Brasil - 30 de Março de 2019

Vinícius Zavam
egypcio@torproject.org
13AC CF3E D4E3 B36F 626F D3AE 415C 6534 13B4 3475

