

Introduction to The Tor Ecosystem

Privacy, Anonymity, and Anti-censorship

Alexander Færøy

October 30, 2019

Swiss Web Security Day



About Me

- Core Developer at The Tor Project since early 2017.
- Free Software developer since 2006.
- Worked with distributed systems in the Erlang programming language, WebKit-based mobile browsers, embedded development, and software development consulting.
- Co-organizing the annual Danish hacker festival **BornHack**.



What is Tor?

- Online anonymity, and censorship circumvention.
 - Free software.
 - Open network.
- Community of researchers, developers, users, and relay operators.
- U.S. 501(c)(3) non-profit organization.

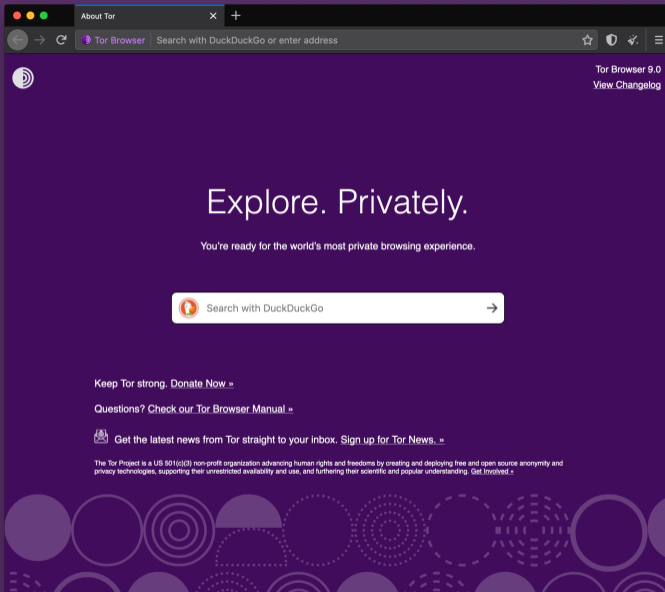


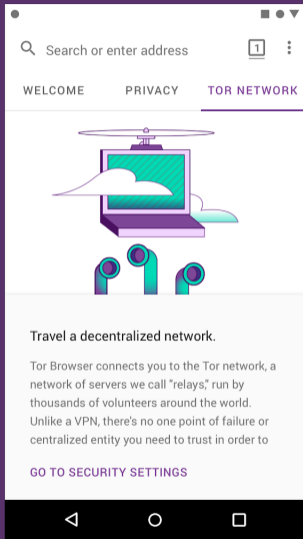
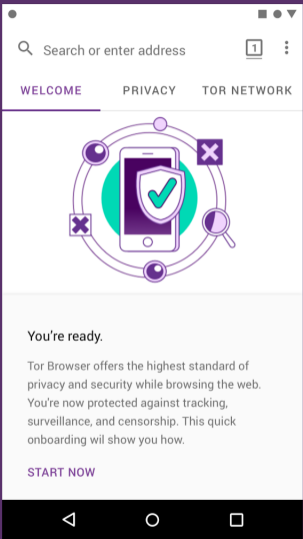
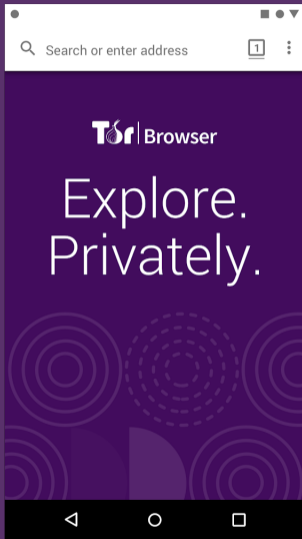
History

1990s	Onion routing for privacy online.
Early 2000s	Working with the U.S. Naval Research Laboratory.
2004	Sponsorship by the Electronic Frontier Foundation.
2006	The Tor Project, Inc. became a non-profit.
2007	Expansion to anti-censorship.
2008	Tor Browser development.
2010	The Arab spring.
2013	The summer of Snowden.
2018	Dedicated anti-censorship team created

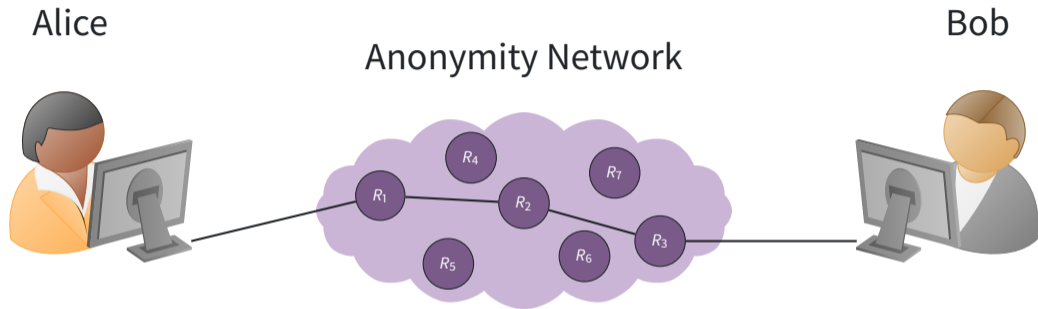
Somewhere between 2,000,000 and 8,000,000 daily users.





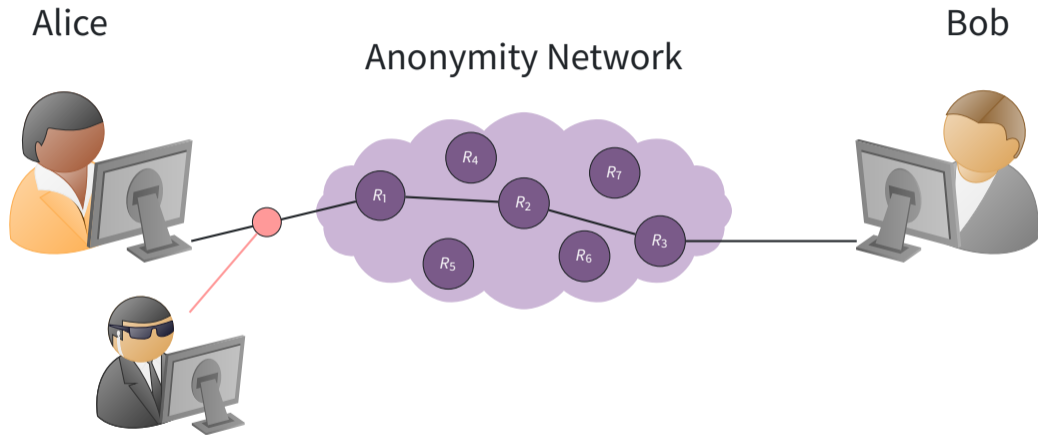


Threat Model

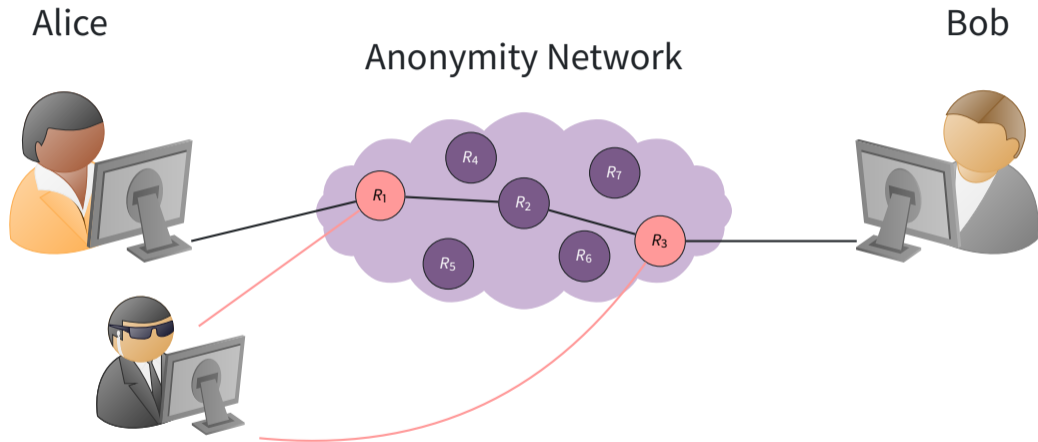


What can the attacker do?

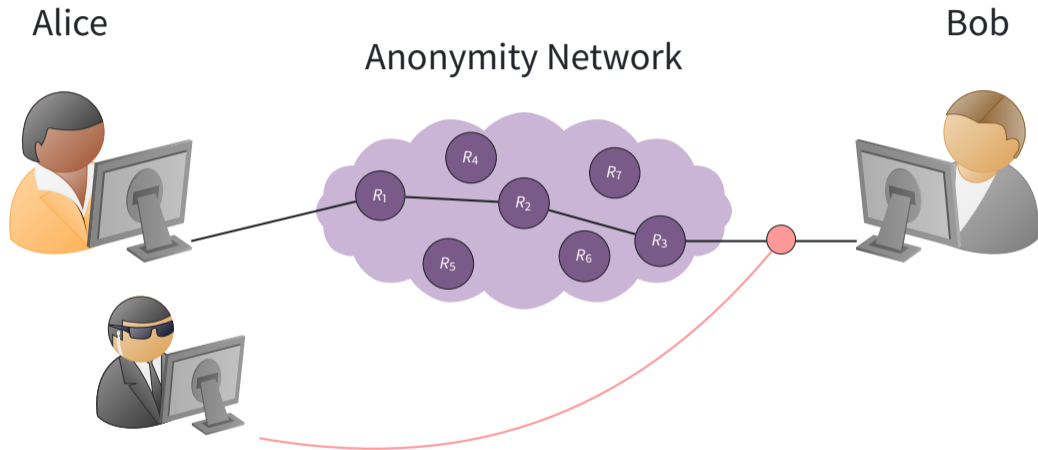
Threat Model



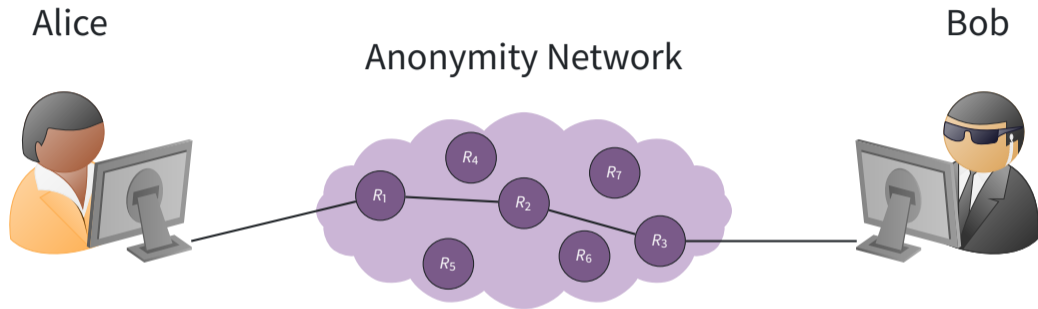
Threat Model



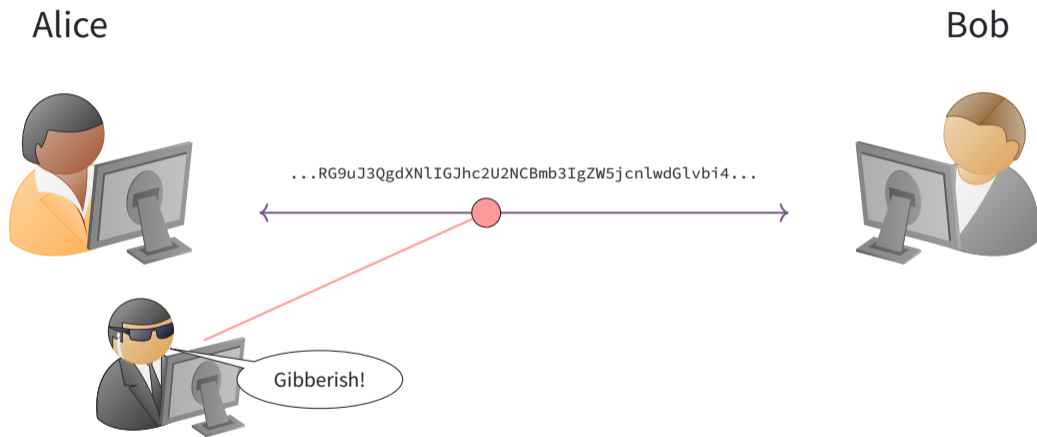
Threat Model



Threat Model



Anonymity isn't Encryption



Encryption just protects contents.

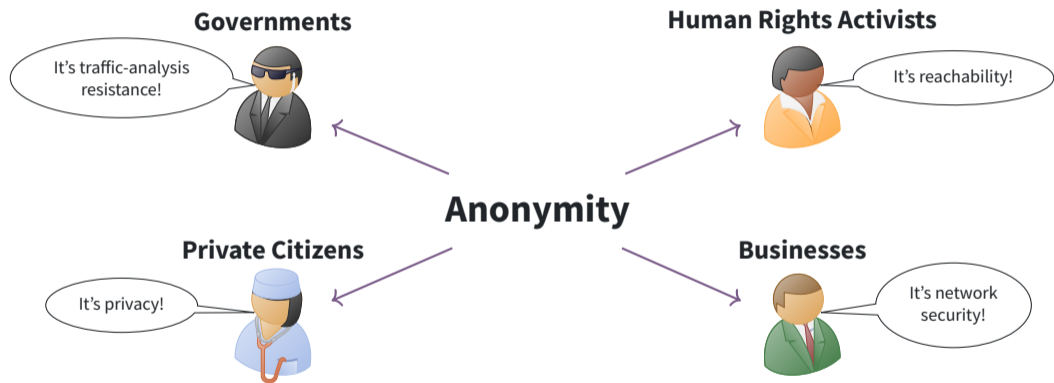
Metadata



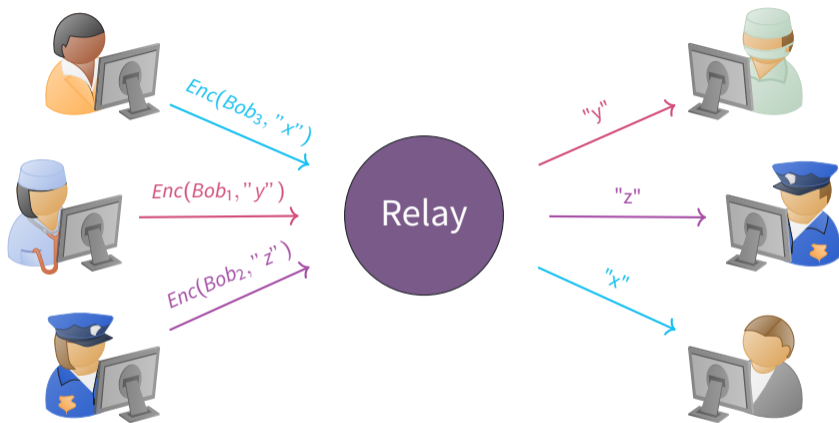
"We Kill People Based on Metadata."

—Michael Hayden, former director of the NSA.

Different Purposes of Anonymity

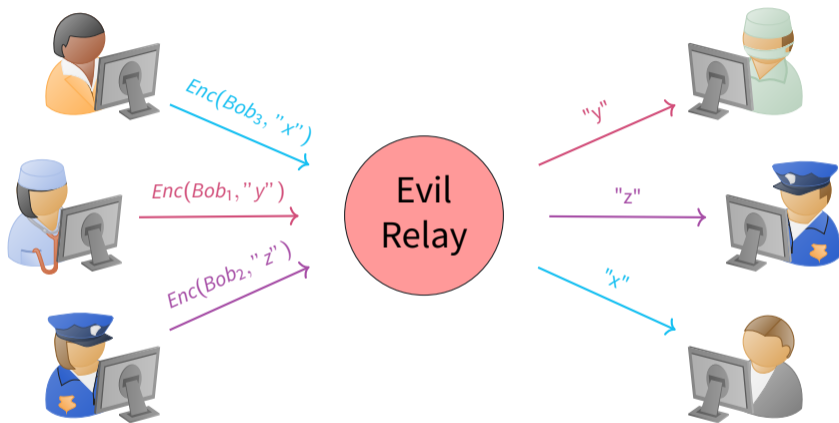


A Simple Design

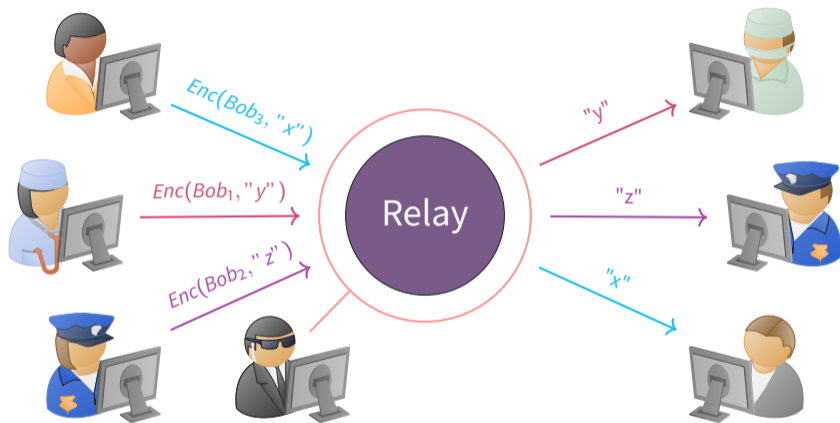


Equivalent to some commercial proxy providers.

A Simple Design

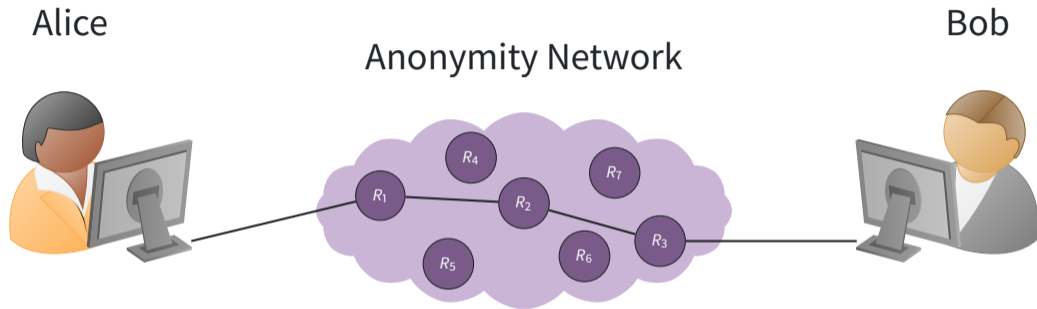


A Simple Design



Timing analysis bridges all connections going through the relay.

The Tor Design



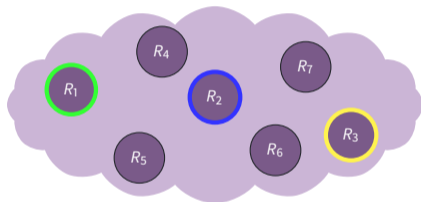
Add multiple relays so that no single relay can betray Alice.

The Tor Design

Alice



Anonymity Network

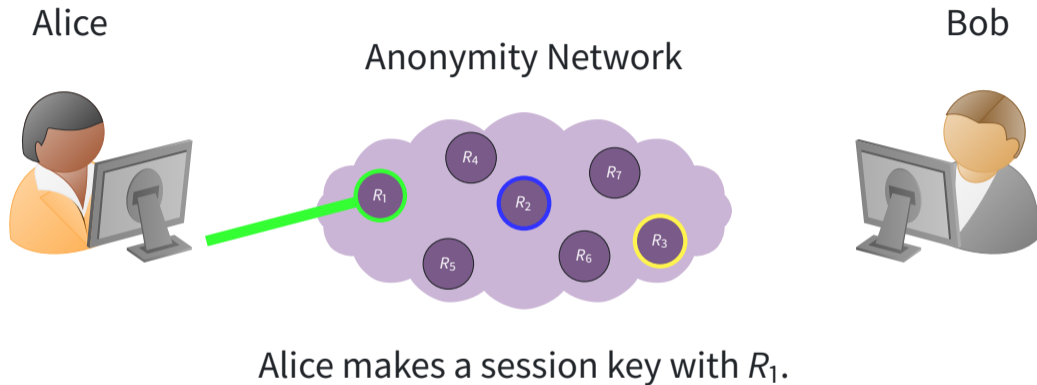


Bob



Alice picks a path through the network: R_1 , R_2 , and R_3 before finally reaching Bob.

The Tor Design

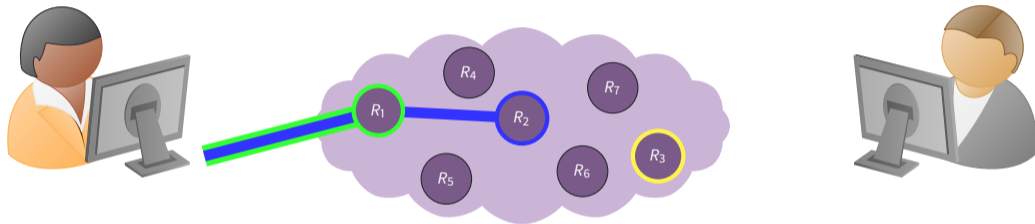


The Tor Design

Alice

Anonymity Network

Bob



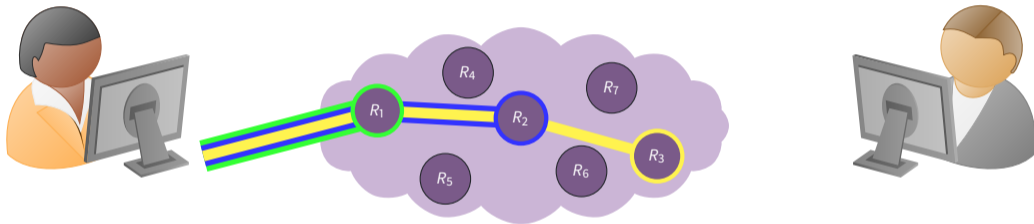
Alice asks R_1 to extend to R_2 .

The Tor Design

Alice

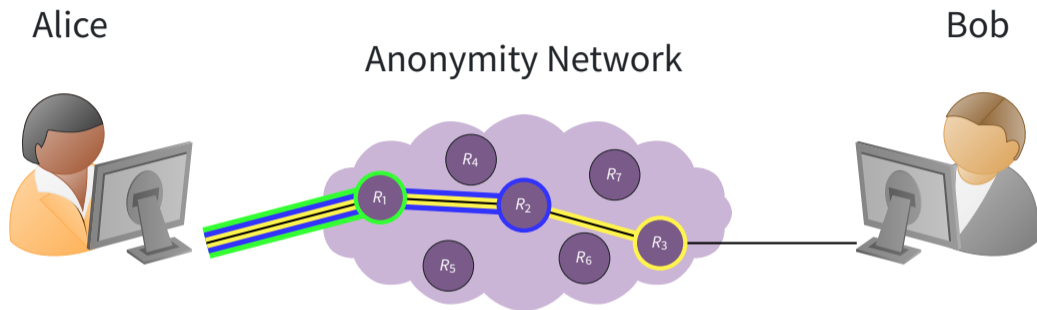
Anonymity Network

Bob



Alice asks R_2 to extend to R_3 .

The Tor Design



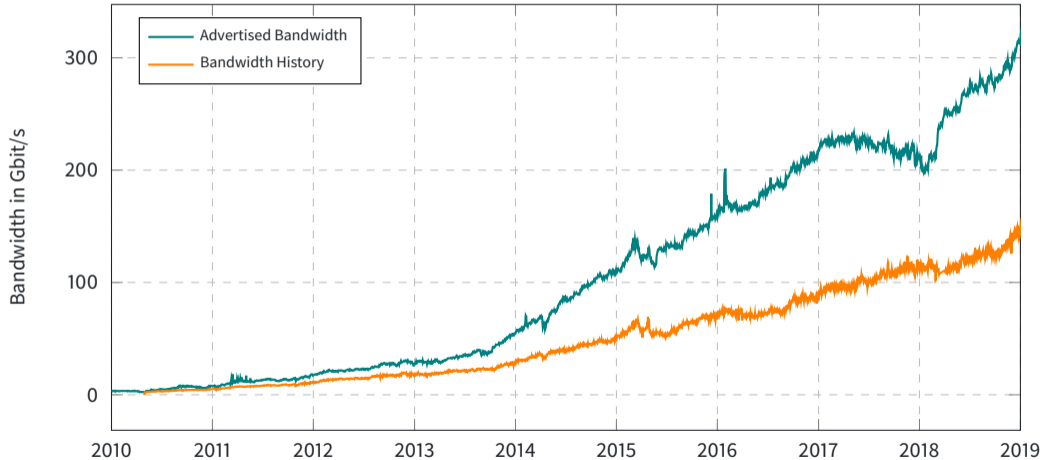
Alice finally asks R_3 to connect to Bob.

The Tor Network

- An open network – everybody can join!
- Between 6000 and 7000 relay nodes.
- Kindly hosted by various individuals, companies, and non-profit organisations.
- 9 Directory Authority nodes and 1 Bridge Authority node.

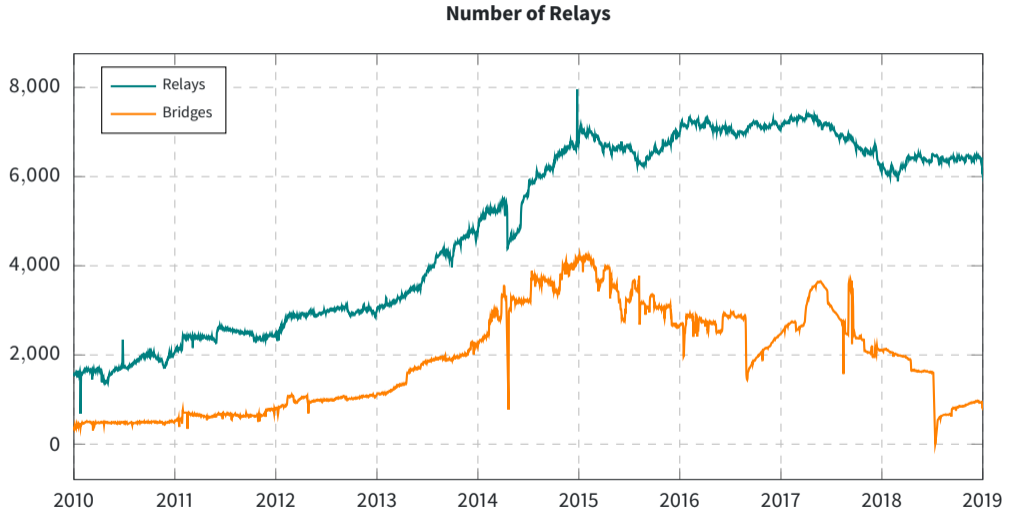
The Tor Network

Total Relay Bandwidth



Source: metrics.torproject.org

The Tor Network



Source: metrics.torproject.org

The Tor Network

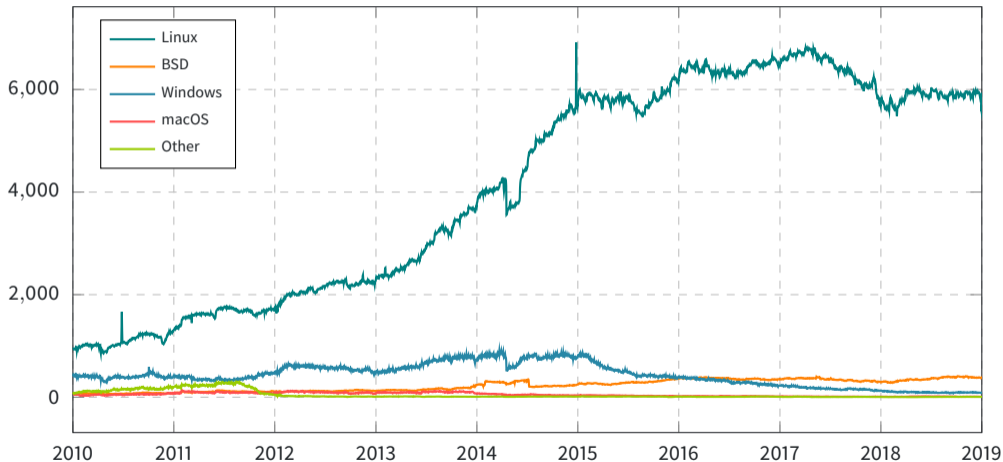
Tor's **safety** comes from **diversity**:

1. Diversity of relays. The more relays we have and the more diverse they are, the fewer attackers are in a position to do traffic confirmation.
2. Diversity of users and reasons to use it. 50,000 users in Iran means almost all of them are normal citizens.

Research problem: How do we measure diversity over time?

The Tor Network

Number of Relays per Platform



Source: metrics.torproject.org

I'm a doctor in a very political town. I have patients who work on legislation that can mean billions of dollars to major telecom, social media, and search concerns.

When I have to do research on diseases and treatment or look into aspects of my patients' histories, I am well aware that my search histories might be correlated to patient visits and leak information about their health, families, and personal lives. **I use Tor to do much of my research when I think there is a risk of correlating it to patient visits.**

—Anonymous Tor User.

The Tor Browser

A modified version of Firefox Extended Support Release (ESR).

- Includes Tor, Pluggable Transports, and support extensions.
- Includes EFF's HTTPS Everywhere extension to protect against malicious Exit node operators.
- Includes No Script to protect against various attacks from JavaScript code.

Tor Project | Anonymity Online

https://www.torproject.org

Site Information for www.torproject.org

Connection

Secure Connection

Tor Circuit

This browser

Lithuania 195.189.96.148 Guard

Germany 131.188.40.188

Austria 109.70.100.7

torproject.org

New Circuit for this Site

Your Guard node may not change. Learn more

Permissions

You have not granted this site any special permissions.


rt Community Blog Donate English (En)

Download Tor Browser

Privately.
e Freely.

and surveillance. Circumvent censorship.

Download Tor Browser



BLOCK TRACKERS

Tor Browser isolates each website you visit so third-party trackers and ads can't follow you. Any cookies

The Tor Browser

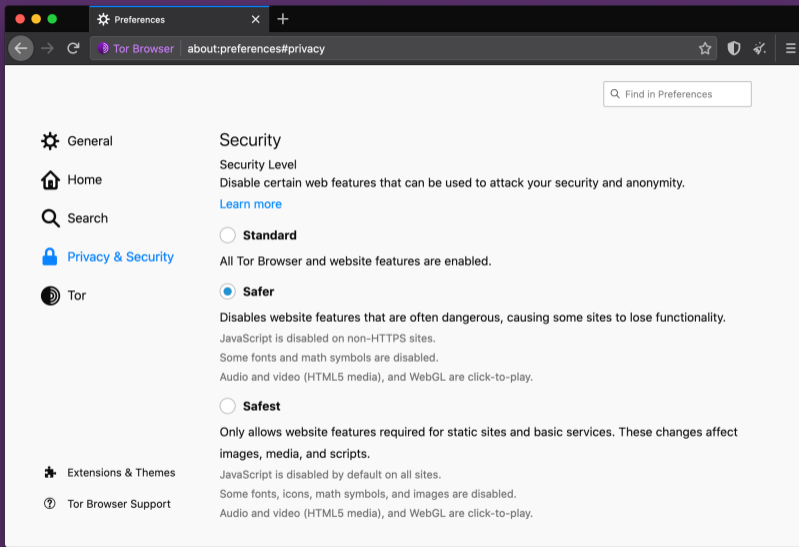
The philosophy behind the design choices in Tor Browser:

- Preserve existing user model.
- Favor changes that are least likely to break sites.
- Plugins must be restricted.
- Minimize Global Privacy Options.
- No filters.
- Stay current.

The Tor Browser

The security requirements are primarily concerned with ensuring the safe use of Tor.

- Proxy Obedience.
- State Separation.
- Disk Avoidance.
- Application Data Isolation.



The Tor Browser

Focus on strong privacy protection:

- Cross-Origin Identifier Unlinkability.
- Cross-Origin Fingerprinting Unlinkability.
- Long-Term Unlinkability.

Mozilla/5.0 (Windows NT 6.1; rv:60.0) Gecko/20100101 Firefox/60.0

The Tor Browser

Attribute	Value
User agent ⓘ	Mozilla/5.0 (X11; Fedora; Linux x86_64; rv:67.0) Gecko/20100101 Firefox/67.0
Accept ⓘ	text/html,application/xhtml+xml,application/xml;q=0.9;/*;q=0.8
Content encoding ⓘ	gzip, deflate, br
Content language ⓘ	en-US,en;q=0.5
List of plugins ⓘ	
Platform ⓘ	Linux x86_64
Cookies enabled ⓘ	yes
Do Not Track ⓘ	yes
Timezone ⓘ	-120
Screen resolution ⓘ	1920x1080x24
Use of local storage ⓘ	yes
Use of session storage ⓘ	yes
Canvas ⓘ	Cwm fjordbank glyphs vext quiz, 😊 Cwm fjordbank glyphs vext quiz, 😊
WebGL Vendor ⓘ	Intel Open Source Technology Center
WebGL Renderer ⓘ	Mesa DRI Intel(R) UHD Graphics 620 (Kabylake GT2)

Firefox 60

Attribute	Value
User agent ⓘ	Mozilla/5.0 (Windows NT 6.1; rv:60.0) Gecko/20100101 Firefox/60.0
Accept ⓘ	text/html,application/xhtml+xml,application/xml;q=0.9;/*;q=0.8
Content encoding ⓘ	gzip, deflate
Content language ⓘ	en-US,en;q=0.5
List of plugins ⓘ	
Platform ⓘ	Linux x86_64
Cookies enabled ⓘ	yes
Do Not Track ⓘ	NC
Timezone ⓘ	0
Screen resolution ⓘ	1000x900x24
Use of local storage ⓘ	yes
Use of session storage ⓘ	yes
Canvas ⓘ	
WebGL Vendor ⓘ	Not supported
WebGL Renderer ⓘ	Not supported

Tor Browser

I live in Iran and I have been using Tor for censorship circumvention. During political unrest while the government tightens grip on other censorship circumvention alternatives, **Tor with obfuscation plugins remains the only solution.**

Tor changed my personal life in many ways. **It made it possible to access information on Youtube, Twitter, Blogger and countless other sites.** I am grateful of Tor project, people working on it as well as people running Tor nodes.

—Anonymous Tor User.

يالله بالستر...!

تصفح بأمان!

عزيزي، هذا الموقع غير متاح في دولة الإمارات العربية المتحدة.

تتشكل شبكة الإنترنت وسيلة للتواصل والمعرفة وخدمة متطلبات حياتنا اليومية. وقد تم حجب الموقع الذي ترغب بدخوله لاشتماله محتوى مرع لحد "فئات المحتويات المحظورة" حسب تصنيف "السياسة التنظيمية لإدارة النظم للإنترنت" لهيئة تنظيم الاتصالات بدولة الإمارات العربية المتحدة.

إذا كنت لديك وجهة نظر مختلفة، الرجاء إخبار هنا.

Surf Safely!

This website is not accessible in the UAE.

The Internet is a powerful medium for communication, sharing and serving our daily learning needs. However, the site you are trying to access contains content that is prohibited under the 'Internet Access Management Regulatory Policy' of the Telecommunications Regulatory Authority of the United Arab Emirates.

If you believe the website you are trying to access does not contain any such content, please [click here](#).



خطراً!

تصفح بأمان!

عزيزي، هذا الموقع غير متاح في دولة الإمارات العربية المتحدة.
تشكل شبكة الإنترنت وسيلة للتواصل والمعرفة وخدمة متطلبات حياتنا اليومية. وقد تم حجب الموقع الذي ترغب بدخوله لاشتماله محتوى مرع لحد "فئات المحتويات المحظورة" حسب تصنيف "السياسة التنظيمية لإدارة النظم للإنترنت" لهيئة تنظيم الاتصالات بدولة الإمارات العربية المتحدة.

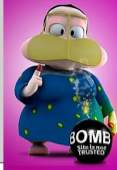
إذا كنت لديك وجهة نظر مختلفة، الرجاء إخبار هنا.

Surf Safely!

This website is not accessible in the UAE.

The Internet is a powerful medium for communication, sharing and serving our daily learning needs. However, the site you are trying to access contains content that is prohibited under the 'Internet Access Management Regulatory Policy' of the Telecommunications Regulatory Authority of the United Arab Emirates.

If you believe the website you are trying to access does not contain any such content, please [click here](#).



Access Denied

Your request was denied because of its content categorization: "Computers/Internet/Proxy Avoidance"

عزيزي العميل : تم حجب هذا الموقع بناء على القوائم والقوانين

بأن هناك خطأ يرجى إرسال رسالة على البريد الإلكتروني unblock.kw@kw.zain.com مع ذكر عنوان الموقع الذي تم حجب.

Dear Customer: This site has been blocked for categorizing this site, please



Site Blocked...
http://torproject.org/

Dear User,

الموقع محظور
هذا الموقع محظور لانتهاكه الأنظمة والقوانين في مملكة البحرين.

Site Blocked
This web site has been blocked for violating regulations and laws of Kingdom of Bahrain.

إذا كنت ترى أن هذه الصفحة ينبغي أن لا تحجب فعلياً [انقر هنا](#).

If you believe the requested page should Not be blocked please [click here](#).

الموقع محظور
هذا الموقع محظور لانتهاكه الأنظمة والقوانين في مملكة البحرين.

إذا كنت ترى أن هذه الصفحة ينبغي أن لا تحجب فعلياً [انقر هنا](#).

If you believe the requested page should Not be blocked please [click here](#).

هذا الموقع محظور
This site is blocked

الوصول إلى هذا الموقع غير مسموح به حالياً لأنه مصنف ضمن فئات المحتويات المحظورة بموجب أحكام السياسة التنظيمية لإدارة النظم إلى الإنترنت في دولة الإمارات العربية المتحدة.

Access to this site is currently blocked. The site falls under the Prohibited Content Categories of the UAE's Internet Access Management Policy.

إذا كنت ترغب في إعادة النظر في تصنيف هذا الموقع، يرجى التفضل بتعبئة استمارة الملاحظات.

If you would like the classification on this site to be reviewed, please fill in and submit the Feedback Form.

<http://torproject.org/>

Dear User,

Sorry, the requested page is unavailable.

If you believe the requested page should not be blocked please [click here](#).

For more information about internet service in Saudi Arabia, please click here: www.internet.gov.sa

خدمة الإنترنت في المملكة العربية السعودية
الموقع الإلكتروني: www.internet.gov.sa

إذا كنت ترى أن هذه الصفحة ينبغي أن لا تحجب فعلياً [انقر هنا](#).

If you believe the requested page should not be blocked please [click here](#).

For more information about internet service in Saudi Arabia, please click here: www.internet.gov.sa

خدمة الإنترنت في المملكة العربية السعودية
الموقع الإلكتروني: www.internet.gov.sa

إذا كنت ترى أن هذه الصفحة ينبغي أن لا تحجب فعلياً [انقر هنا](#).

If you believe the requested page should not be blocked please [click here](#).

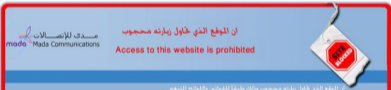
الموقع محظور
هذا الموقع محظور لانتهاكه الأنظمة والقوانين في مملكة البحرين.

إذا كنت ترى أن هذه الصفحة ينبغي أن لا تحجب فعلياً [انقر هنا](#).

If you believe the requested page should Not be blocked please [click here](#).

الموقع محظور
هذا الموقع محظور لانتهاكه الأنظمة والقوانين في مملكة البحرين.

إذا كنت ترى أن هذه الصفحة ينبغي أن لا تحجب فعلياً [انقر هنا](#).



الموقع الذي تحاول زيارته محظور
Access to this website is prohibited

Dear Customer: This site has been blocked for categorizing this site, please

Site Blocked...
http://torproject.org/

Dear User,

الموقع محظور
هذا الموقع محظور لانتهاكه الأنظمة والقوانين في مملكة البحرين.

Site Blocked
This web site has been blocked for violating regulations and laws of Kingdom of Bahrain.

إذا كنت ترى أن هذه الصفحة ينبغي أن لا تحجب فعلياً [انقر هنا](#).

If you believe the requested page should Not be blocked please [click here](#).

الموقع محظور
هذا الموقع محظور لانتهاكه الأنظمة والقوانين في مملكة البحرين.

إذا كنت ترى أن هذه الصفحة ينبغي أن لا تحجب فعلياً [انقر هنا](#).

Introduction to Censorship

Censored Region

Alice



Bob



Alice is unable to reach Bob.

Introduction to Censorship

Censored Region

Alice



Bob



Alice can reach Bob, but their connection is throttled.

Introduction to Censorship

Censored Region

Alice



Bob



Alice can reach Bob because the censor thinks Bob is fine.

Anti-censorship Strategies

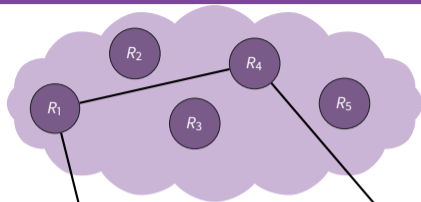
1. Censors will apply censorship to **all** relays in the network and effectively block access to the Tor network.
2. Censors will apply censorship to **known** bridges.

Solution: We make it difficult to find and block bridges and we make it difficult to learn if a given connection is between a Tor user and an entry-point into the Tor network.

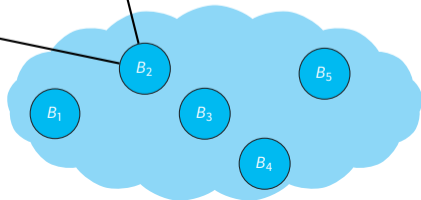
Bridges

Censored Region

Alice



Bob



Bridges

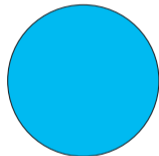
Censored Region

Alice



Tor Protocol

Bridge



Bridges and Pluggable Transports

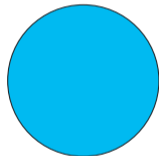
Censored Region

Alice



PT Client

Bridge



PT Server

Obfuscated Protocol



Pluggable Transports

- Allows people to easily build, experiment, and deploy their own obfuscation technology without having to modify the Tor source code itself.
- The specification for Pluggable Transports is open and allows other vendors to implement support for PTs in their own products.
- Allows people to experiment with different transports for Tor that might not be doing any anti-censorship related obfuscation.

Obfourscator (obfs4)

- Makes it hard for passive DPI to verify the presence of the obfs4 protocol unless the adversary knows the bridge parameters.
- Makes active probing hard unless the adversary knows the bridge parameters.
- Uses Tor's ntor handshake (x25519), but uses Elligator2 to encode the elliptic-curve points to be indistinguishable from uniform random strings. The link layer encryption uses NaCl secret boxes (XSalsa20 and Poly1305).

SNI Domain Fronting using Meek

Censored Region

Alice



DNS

A? ajax.aspnetcdn.com

TLS

SNI: ajax.aspnetcdn.com

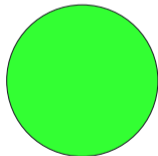
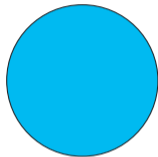
HTTP

POST / HTTP/1.1

Host: **meek.azureedge.net**

...

Bridge



Webserver

SNI Domain Fronting using Meek

Very **efficient**, but **expensive** :-)

Unpopular with the cloud providers:

Google Never been a supported feature of Google.

Amazon Already handled as a breach of AWS ToS.

Domain Fronting in the Future?

- Use Encrypted SNI?
- Use message queue services hosted by the different cloud providers?
- Generally continue to use centralized services to give people in censored areas access.

Bridge Distribution

BridgeDB

The Tor Project

Step 1 Download [Tor Browser](#)

Step 2 Get [bridges](#)

Step 3 Now [add the bridges to Tor Browser](#)

What are bridges?

[Bridges](#) are Tor relays that help you circumvent censorship.

I need an alternative way of getting bridges!

Another way to get bridges is to send an email to bridges@torproject.org. Please note that you must send the email using an address from one of the following email providers: [Riseup](#) or [Gmail](#).

Source: bridges.torproject.org

Bridge Distribution using Moat

☒ Tor is censored in my country

☐ Select a built-in bridge ?

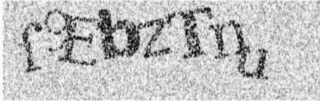
☒ Request a bridge from torproject.org

☐ Provide a bridge I know

☐ I use a proxy to connect to the Internet ?

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

Solve the CAPTCHA to request a bridge.



Enter the characters from the image

Snowflake

Censored Region

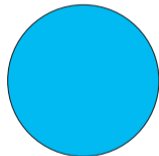
Alice



Snowflake PT Client

Snowflake Broker

Bridge



Snowflake PT Server



Snowflake

Censored Region

Alice

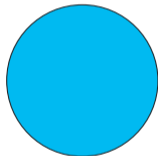


Snowflake PT Client

Snowflake Broker

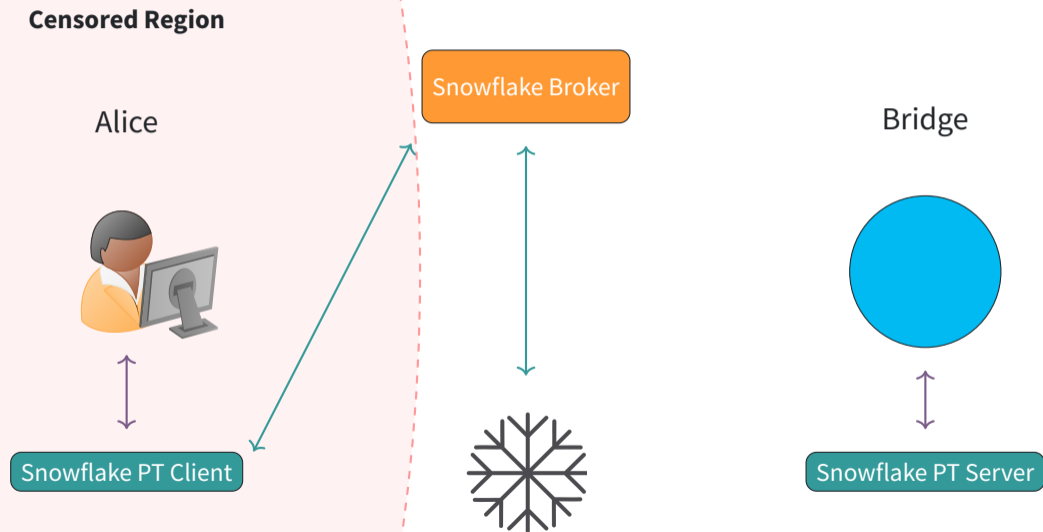


Bridge



Snowflake PT Server

Snowflake



Snowflake

Censored Region

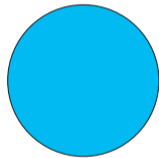
Alice



Snowflake PT Client

Snowflake Broker

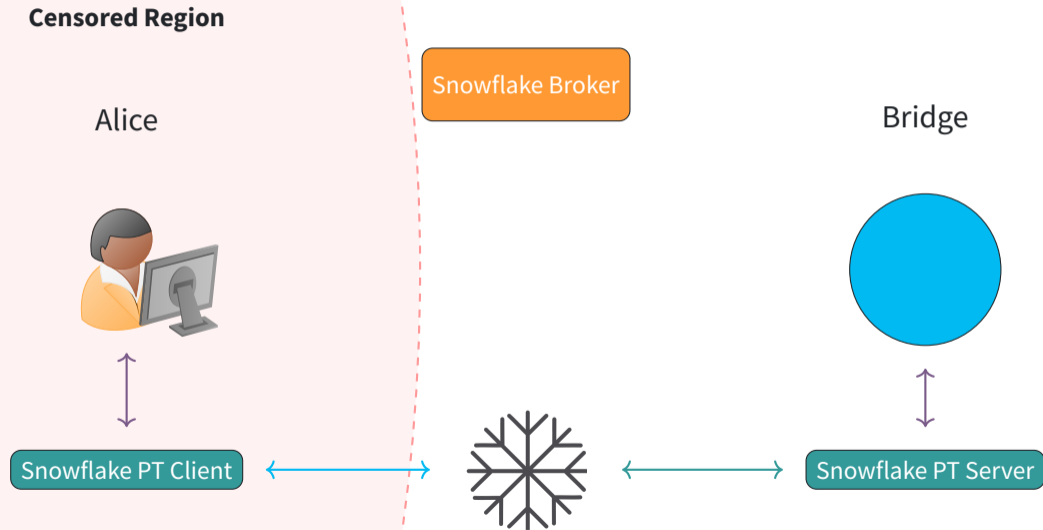
Bridge



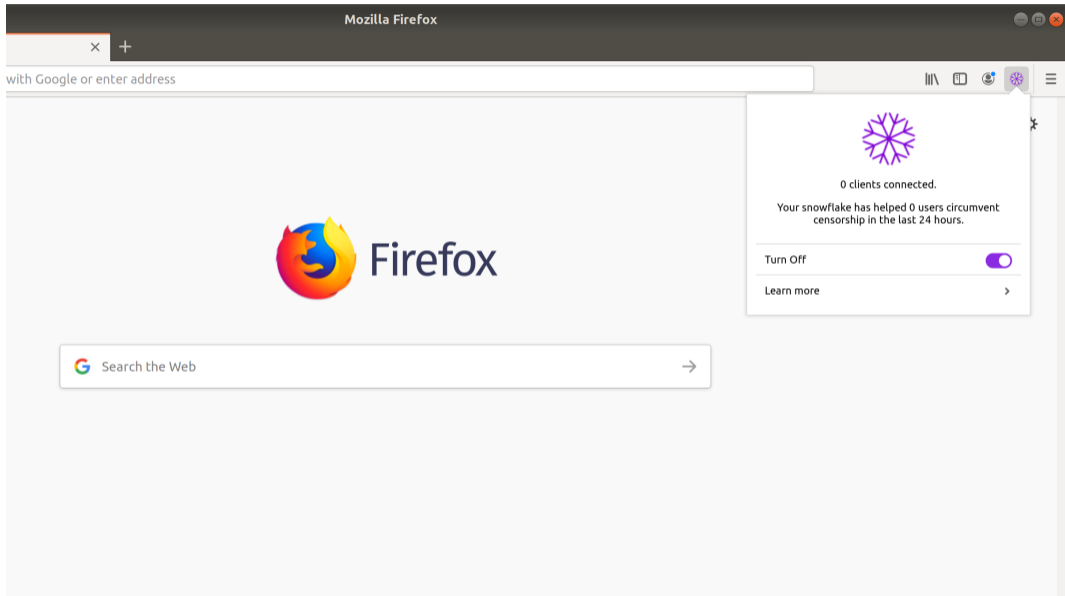
Snowflake PT Server



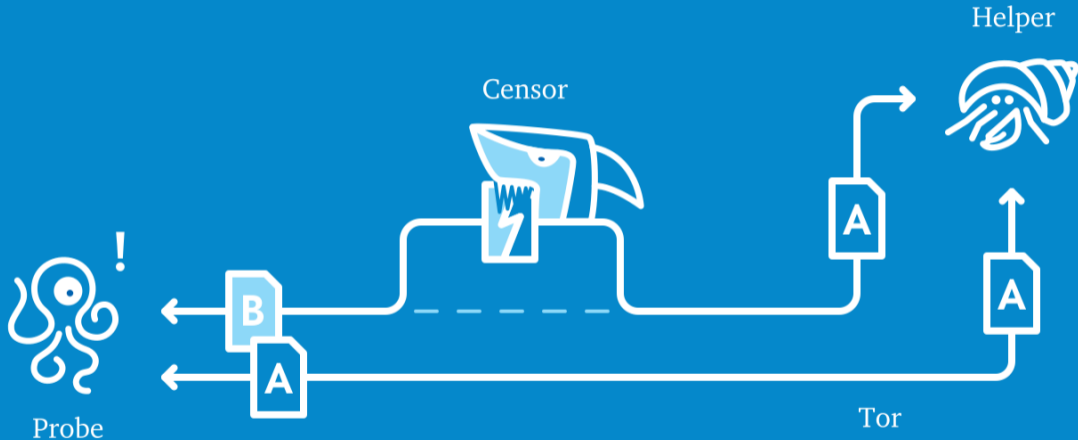
Snowflake

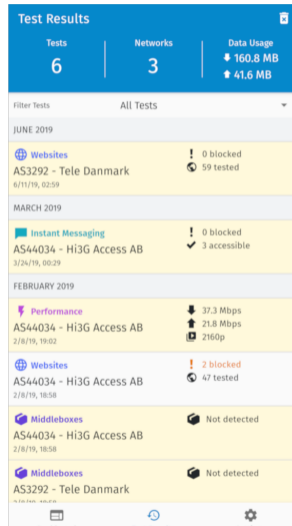
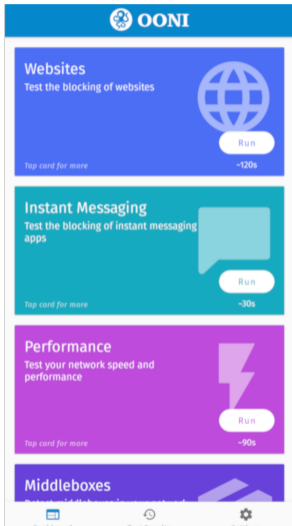


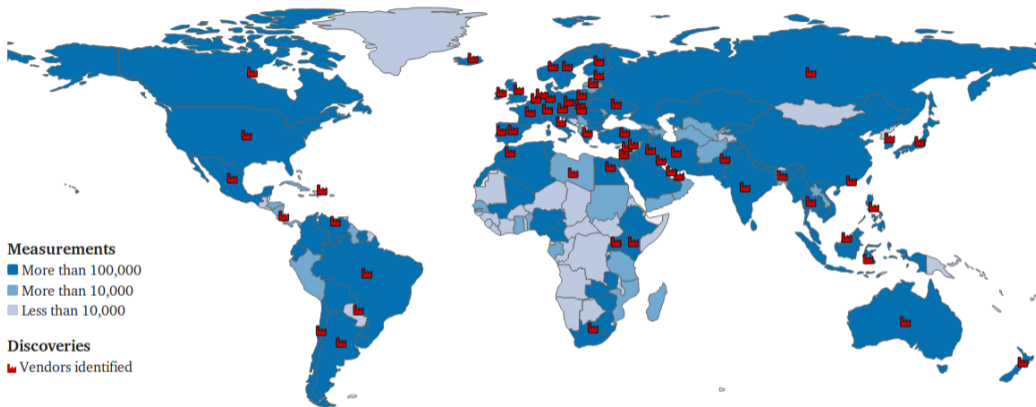
Snowflake



Open Observatory of Network Interference







Check it out at explorer.ooni.io

Tor is not foolproof

- Operational security mistakes.
- Browser metadata fingerprinting.
- Browser exploits.
- Traffic analysis.

How can you help?

- Run a Tor relay or a bridge!
- Teach others about Tor and privacy in general.
- Find, and maybe fix, bugs in Tor.
- Test Tor on your platform of choice.
- Work on some of the many open research projects.
- Donate at donate.torproject.org



Questions?



This work is licensed under a
Creative Commons
Attribution-ShareAlike 4.0 International License

