Censorship Circumvention with Tor

Alexander Færøy

September 5, 2019

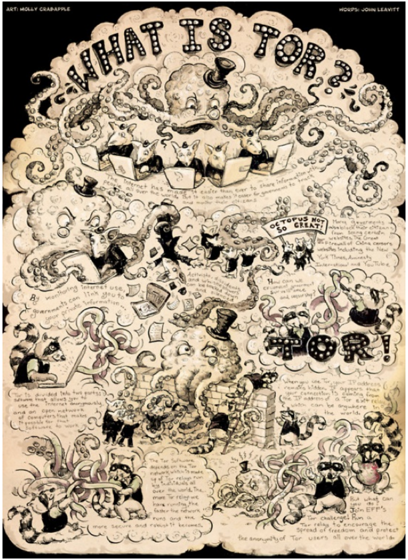
Driving IT Aarhus

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 web browsers, consulting, and firmware development.
- Co-organizing the annual Danish hacker festival BornHack on Funen.

What is Tor?

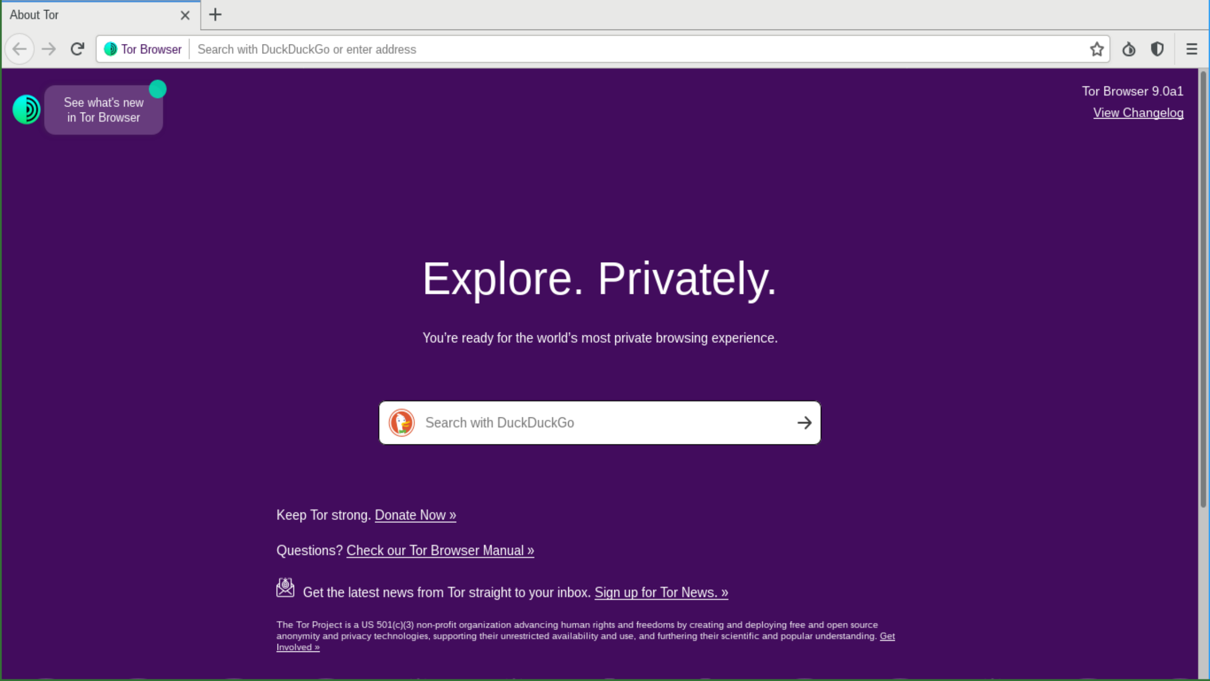
- Online anonymity, and censorship circumvention.
  - Free software.
  - Open network.
- Community of researchers, developers, users, and relay operators.
- U.S. 501(c)(3) non-profit organization.


ART: MOLLY CRABAPPLE
WORDS: JOHN LEAVITT
WHAT IS TOR?
The Internet has made it easier than ever to share information with people all over the world. But it also makes it easier for governments to track and monitor their citizens
OCTOPUS NOT SO GREAT!
Many governments also block their citizens from seeing certain websites. The Great Firewall of China censors websites including the New York Times, Amnesty International and YouTube
By monitoring internet use, governments can link you to your private information...
Activists, dissidents and whistleblowers can be tracked down and silenced
How can we circumvent government surveillance and censorship?
TOR!
Tor is divided into two parts: software that allows you to use the Internet anonymously, and an open network of computers that makes it possible for that software to work
When you use Tor, your IP address remains hidden. It appears that your connection is coming from the IP address of a Tor exit relay which can be anywhere in the world.
The Tor Software depends on the Tor network, which is made up of Tor relays run by individuals all over the world. The more Tor relays we have running, the faster the network runs and the more secure and robust it becomes.
But what can you do? Join EFF's Tor challenge! Run a Tor relay to encourage the spread of freedom and protect the anonymity of Tor users all over the world.

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.



Explore. Privately.

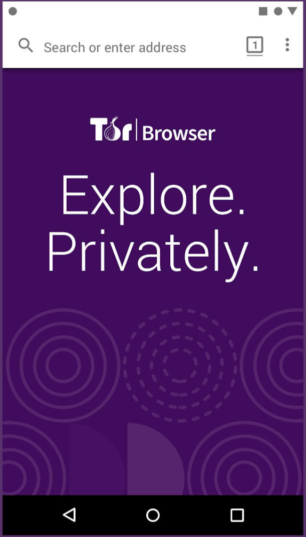
You're ready for the world's most private browsing experience.

Keep Tor strong. Donate Now »

Questions? Check our Tor Browser Manual »

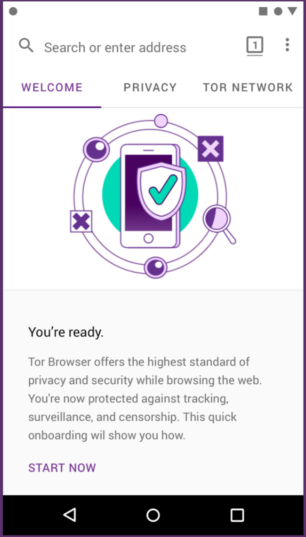
Get the latest news from Tor straight to your inbox. Sign up for Tor News. »

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 Browser

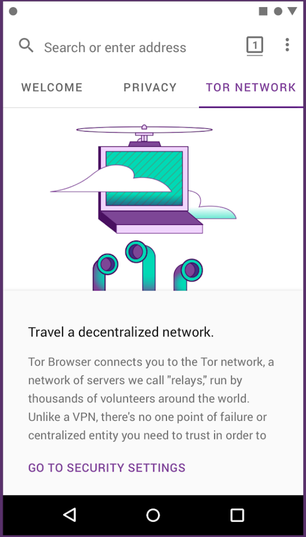
Explore.
Privately.



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 wil show you how.

START NOW

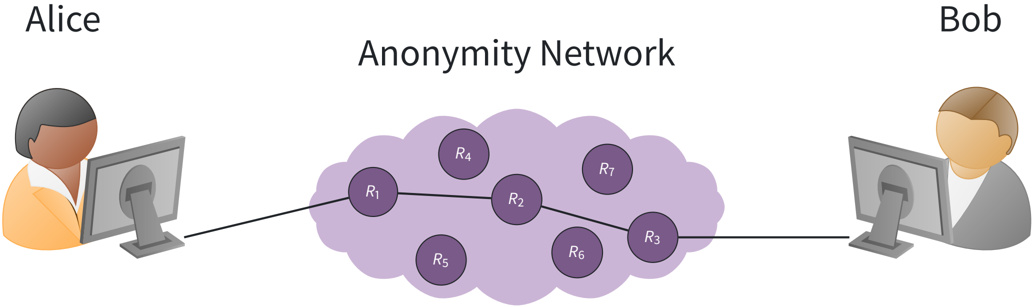


Travel a decentralized network.

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

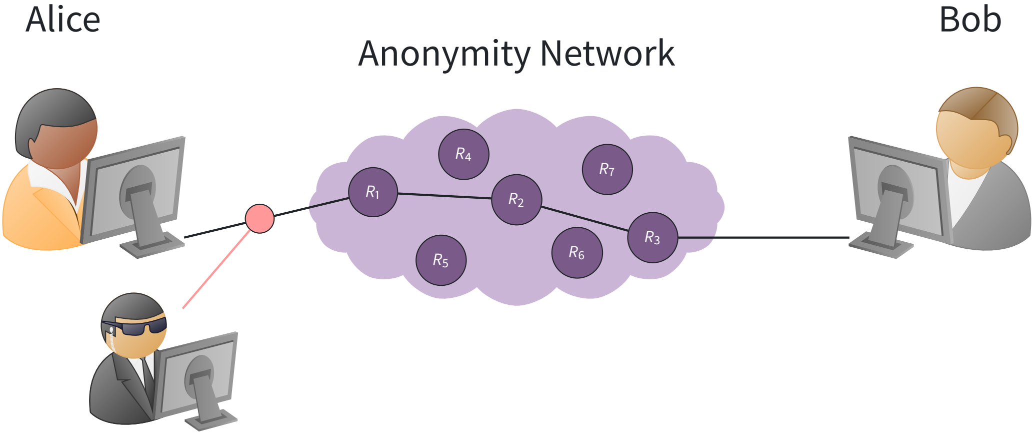
GO TO SECURITY SETTINGS

Threat Model



What can the attacker do?

Threat Model

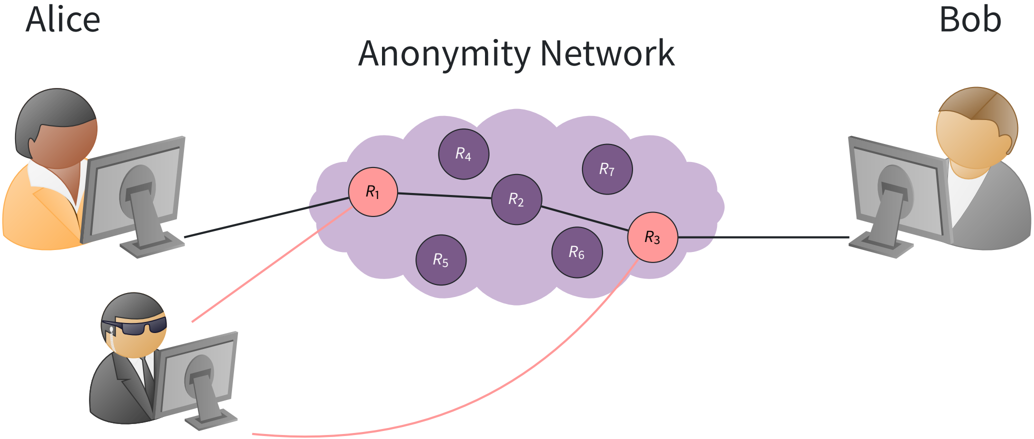


Alice

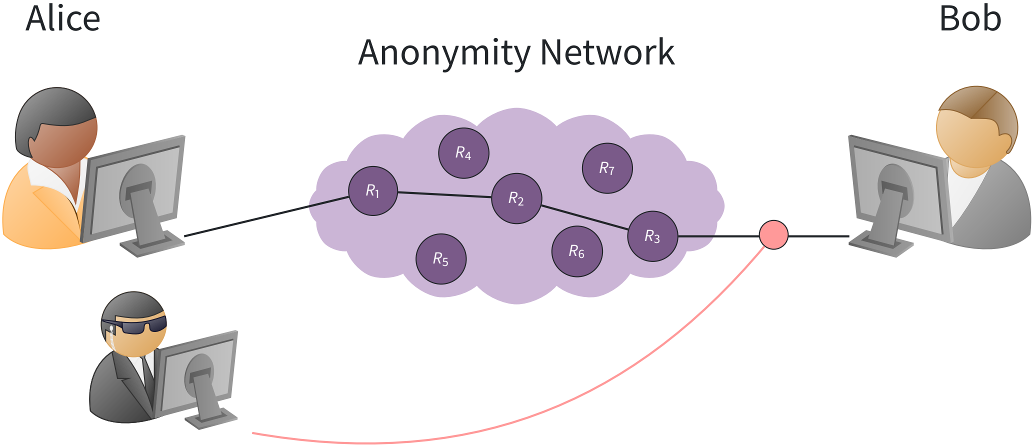
Anonymity Network

Bob

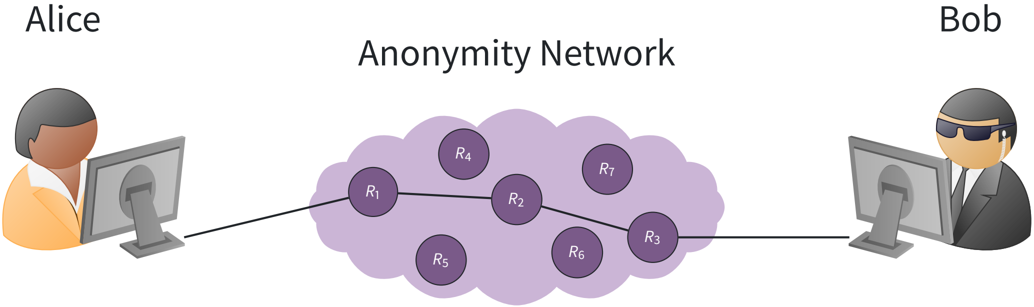
Threat Model



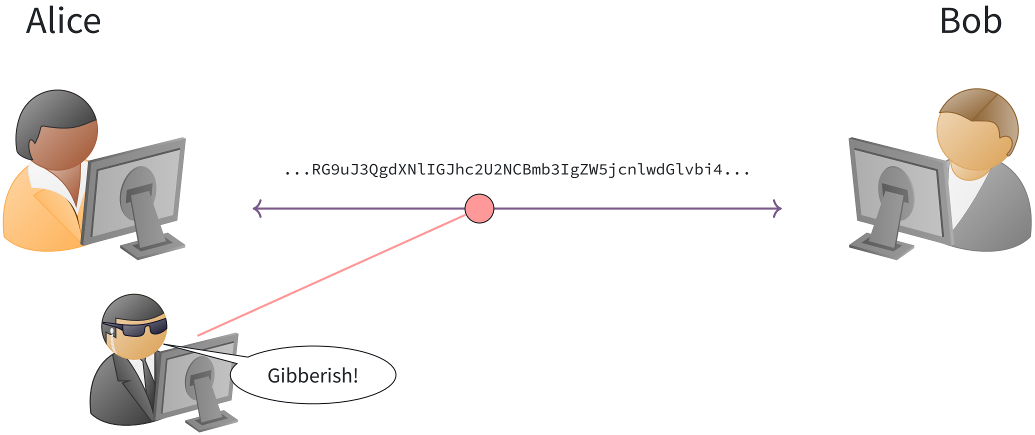
Threat Model



Threat Model



Anonymity isn’t Encryption



Alice

Bob

...RG9uJ3QgdXNlIGJhc2U2NCBmb3IgZW5jcnlwdGlvbi4...

Gibberish!

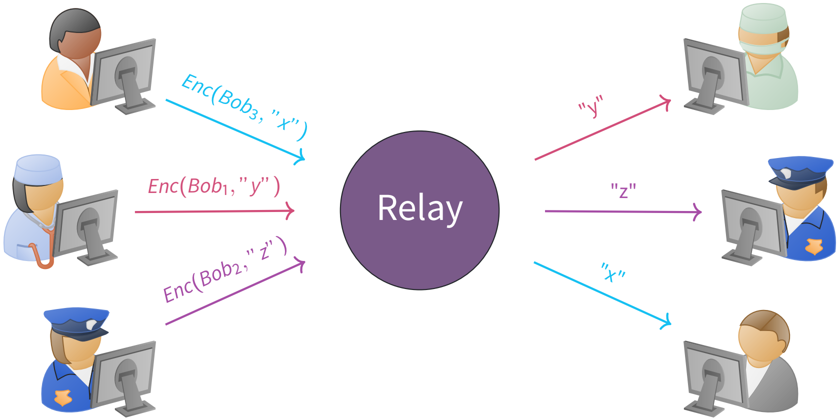
Encryption just protects contents.

Metadata

"We Kill People Based on Metadata."

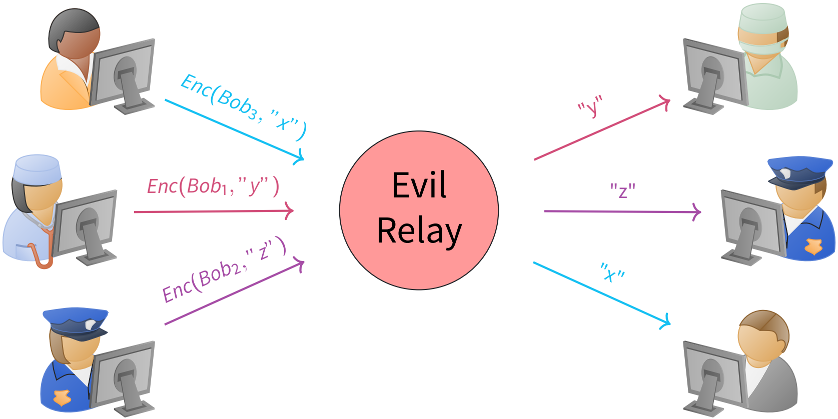
—Michael Hayden, former director of the NSA.

A Simple Design

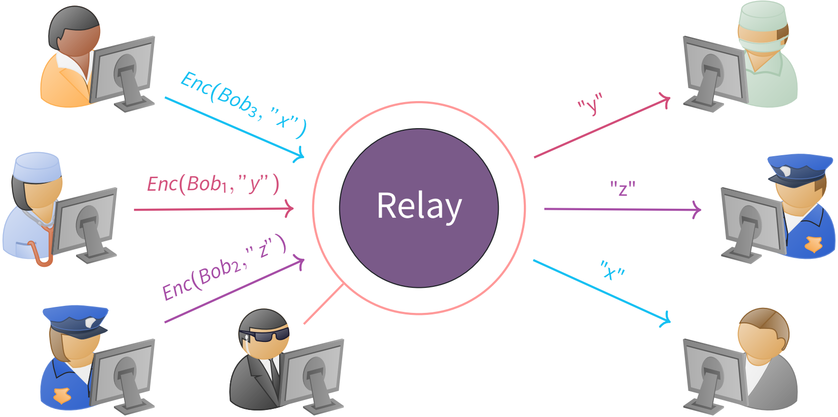


Equivalent to some commercial proxy providers.

A Simple Design

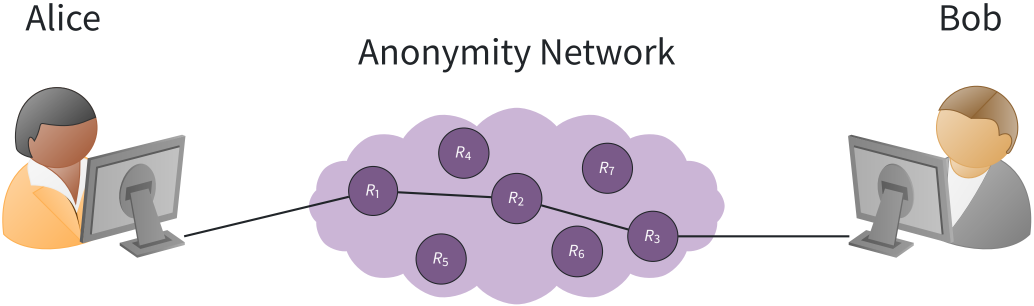


A Simple Design



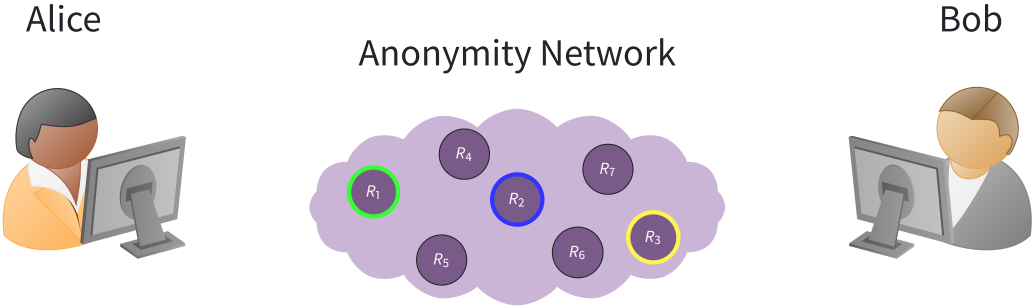
Timing analysis bridges all connections going through the relay.

The Tor Design



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

The Tor Design



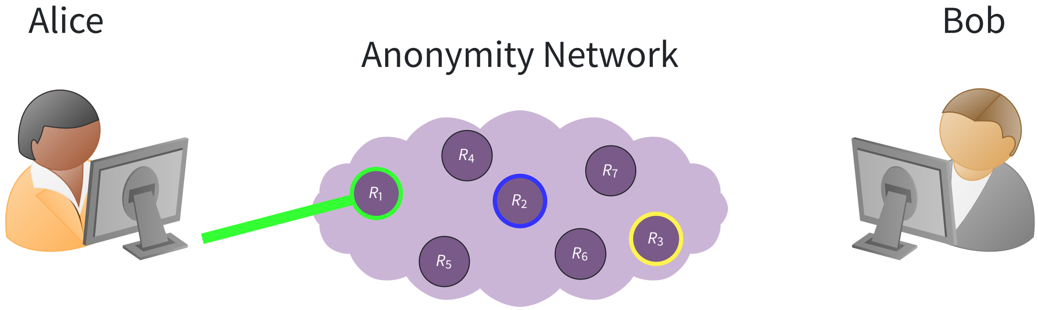
Alice

Anonymity Network

Bob

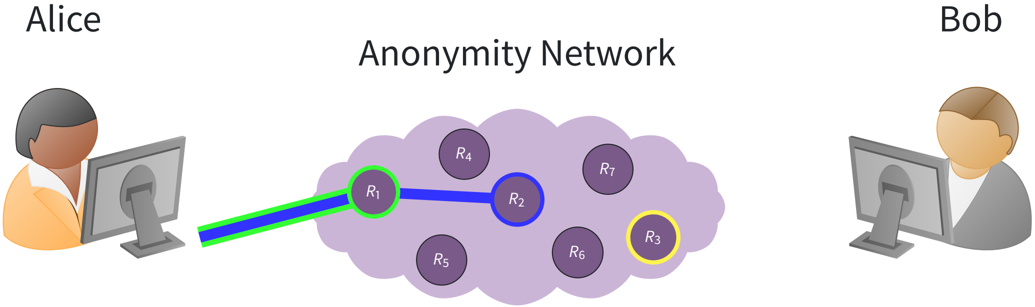
Alice picks a path through the network: R_1, R_2, and R_3 before finally reaching Bob.

The Tor Design



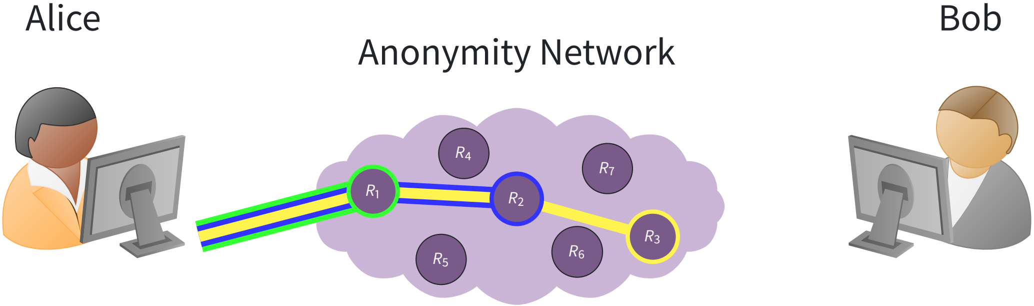
Alice makes a session key with R_1.

The Tor Design



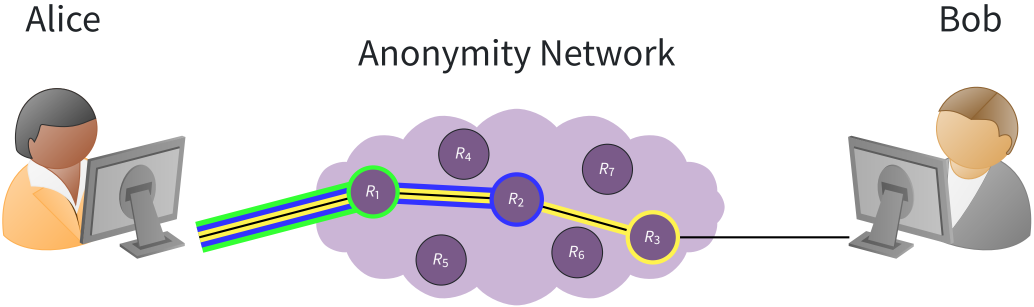
Alice asks R_1 to extend to R_2.

The Tor Design



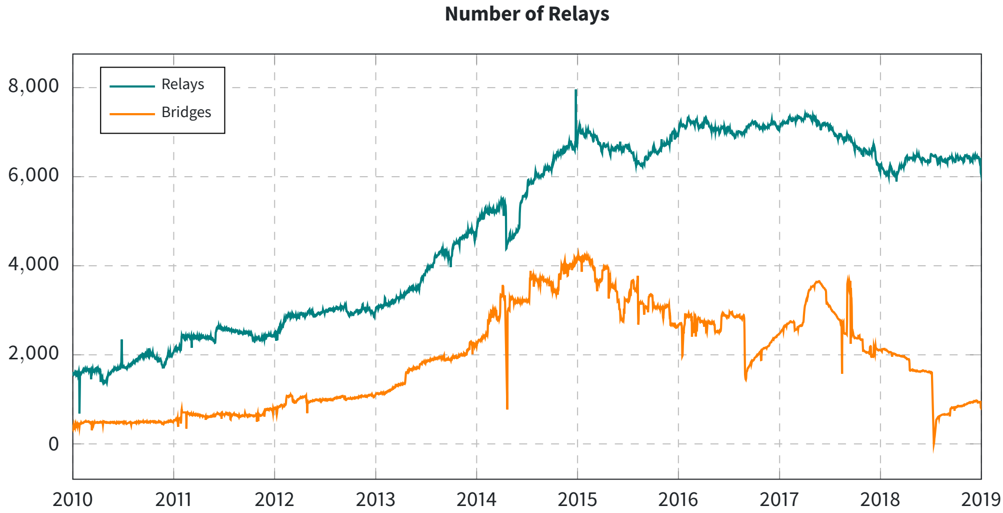
Alice asks R_2 to extend to R_3.

The Tor Design



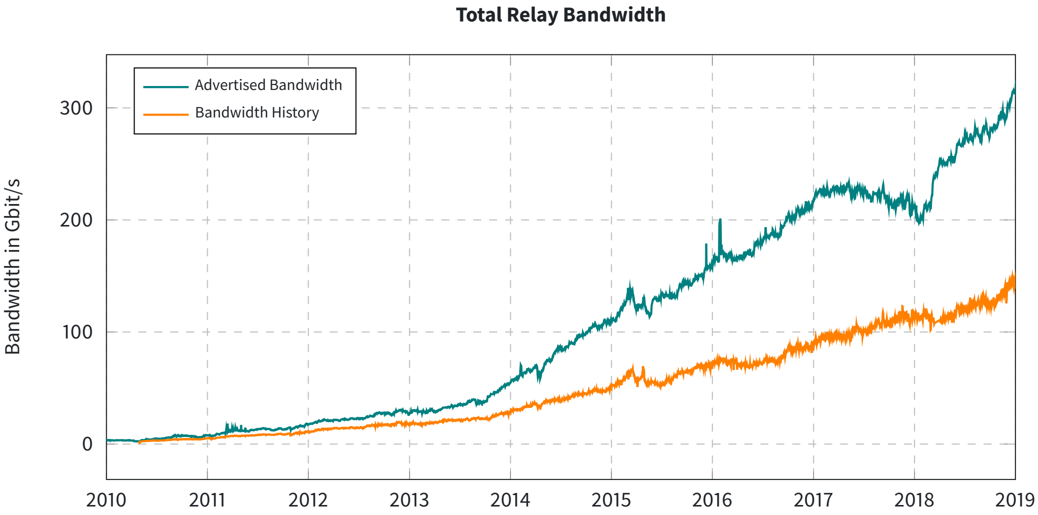
Alice finally asks R_3 to connect to Bob.

The Tor Network



Source: metrics.torproject.org

The Tor Network



Source: metrics.torproject.org

The Tor Network

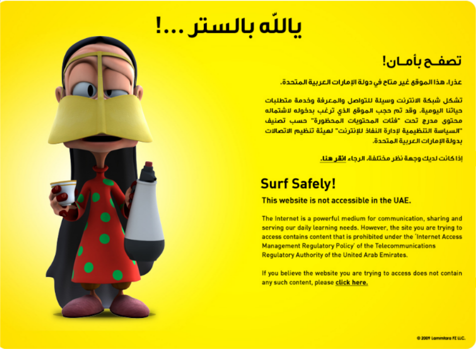
Tor’s **safety** comes from **diversity**:

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.
   Research problem: How do we measure diversity over time?
2. Diversity of users and reasons to use it. 50000 users in Iran means almost all of them are normal citizens.

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.



تصفـح بأمـان!

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

تشكل شبكة الانترنت وسيلة للتواصل والمعرفة وخدمة متطلبات حياتنا اليومية. وقد تم حجب الموقع الذي ترغب بدخوله لاشتماله محتوى مدرج تحت "فئات المحتويات المحظورة" حسب تصنيف "السياسة التنظيمية لإدارة النفاذ للإنترنت" لهيئة تنظيم الاتصالات بدولة الإمارات العربية المتحدة.

إذا كانت لديك وجهة نظر مختلفة، الرجاء انقر هنا.

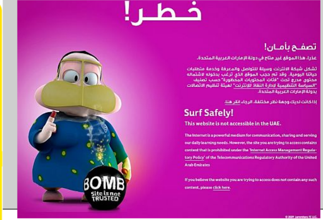
Surf Safely!

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.

© 2009 Lammtara FZ LLC.



تصفـح بأمـان!

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

تشكل شبكة الانترنت وسيلة للتواصل والمعرفة وخدمة متطلبات حياتنا اليومية. وقد تم حجب الموقع الذي ترغب بدخوله لاشتماله محتوى مدرج تحت "فئات المحتويات المحظورة" حسب تصنيف "السياسة التنظيمية لإدارة النفاذ للإنترنت" لهيئة تنظيم الاتصالات بدولة الإمارات العربية المتحدة.

إذا كانت لديك وجهة نظر مختلفة، الرجاء انقر هنا.

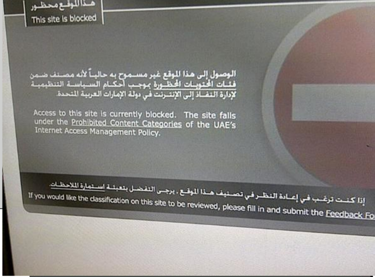
Surf Safely!

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.

© 2009 Lammtara FZ LLC.



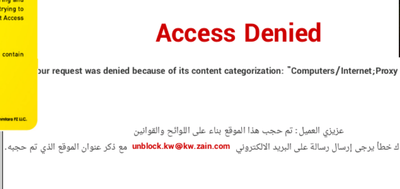
هـذا الموقـع محظـور
This site is blocked

الوصول إلى هذا الموقع غير مسموح به حالياً لأنه مصنف ضمن فئات المحتويات المحظورة بموجب أحكام السياسة التنظيمية لإدارة النفاذ 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 Fo



Access Denied

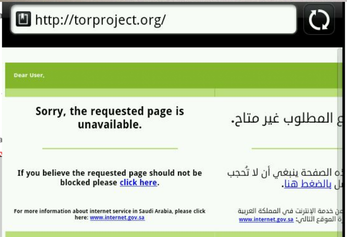
our request was denied because of its content categorization: "Computers/Internet;Proxy Avoida

عزيزي العميل : تم حجب هذا الموقع بناء على اللوائح والقوانين

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

Dear Customer: This site has

categorizing this site, please



http://torproject.org/

Dear User,

Sorry, the requested page is unavailable.

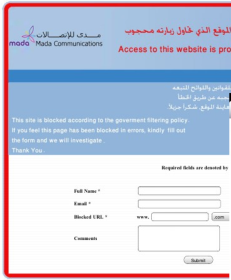
المطلوب غير متاح.

If you believe the requested page should not be blocked please click here.

ه الصفحة ينبغي أن لا تُحجب
ل بالضغط هنا.

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

ن خدمة الإنترنت في المملكة العربية
ة الموقع التالي: www.internet.gov.sa



مـــدى للإتصـــالات
mada Mada Communications

ان الموقع الذي تحاول زيارته محجوب

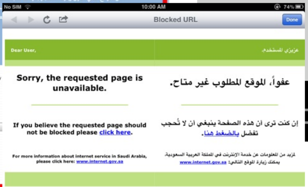
Access to this website is prohibited

ان الموقع الذي تحاول زيارته محجوب وذلك طبقاً للقوانين واللوائح المتبعه
حجبه عن طريق الخطأ
عاينة للوقع. شكراً جزيلاً.

This site is blocked according to the goverment filtering policy.
If you feel this page has been blocked in errors, kindly fill out the form and we will investigate .
Thank You .

Required fields are denoted by

Full Name *
Email *
Blocked URL * www. .com
Comments
Submit



No SIM 10:00 AM 74%

Blocked URL Done

Dear User, عزيزي المستخدم،

Sorry, the requested page is unavailable.

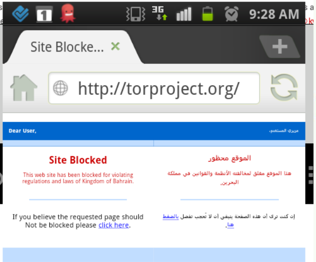
عفواً، الموقع المطلوب غير متاح.

If you believe the requested page should not be blocked please click here.

إن كنت ترى أن هذه الصفحة ينبغي أن لا تُحجب تفضل بالضغط هنا.

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

لمزيد من المعلومات عن خدمة الإنترنت في المملكة العربية السعودية، يمكنك زيارة الموقع التالي: www.internet.gov.sa



9:28 AM

Site Blocke... ✕

http://torproject.org/

Dear User, عزيزي المستخدم،

Site Blocked

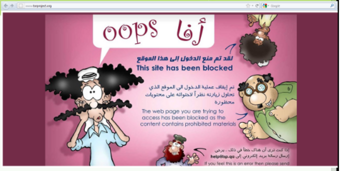
This web site has been blocked for violating regulations and laws of Kingdom of Bahrain.

الموقع محظور

هذا الموقع مغلق لمخالفته الأنظمة والقوانين في مملكة البحرين.

If you believe the requested page should Not be blocked please click here.

إن كنت ترى أن هذه الصفحة ينبغي أن لا تُحجب تفضل بالضغط هنا.



www.torproject.org

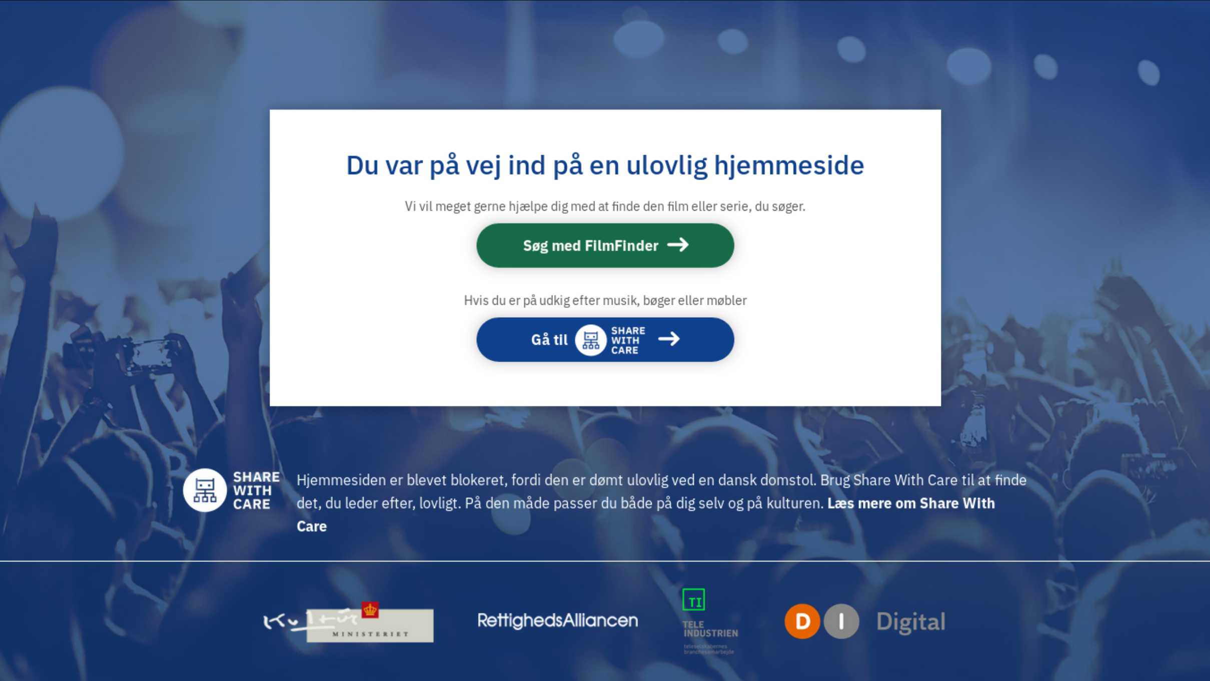
لقد تم منع الدخول إلى هذا الموقع
This site has been blocked

تم إيقاف عملية الدخول الى الموقع الذي تحاول زيارته نظراً لاحتوائه على محتويات محظورة

The web page you are trying to access has been blocked as the content contains prohibited materials

إذا كنت ترى أن هناك خطأ في ذلك .. يرجى إرسال رسالة بريد إلكتروني إلى help@isp.qa

If you feel this is an error then please send



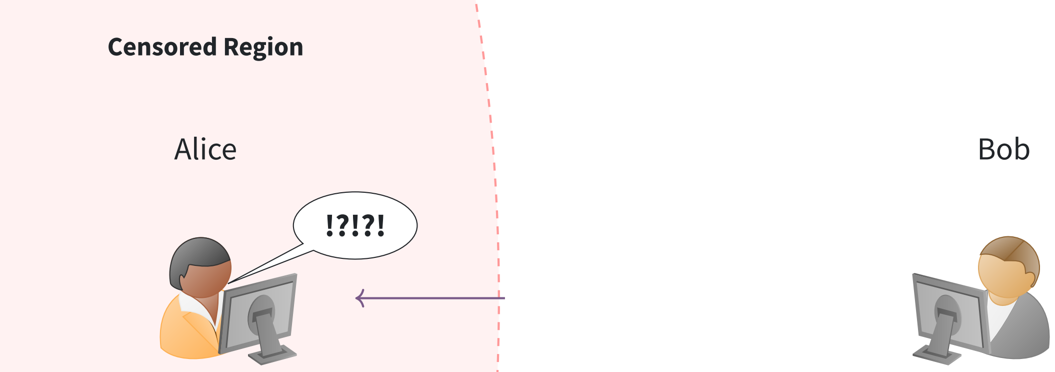
Du var på vej ind på en ulovlig hjemmeside

Vi vil meget gerne hjælpe dig med at finde den film eller serie, du søger.

Hvis du er på udkig efter musik, bøger eller møbler

Hjemmesiden er blevet blokeret, fordi den er dømt ulovlig ved en dansk domstol. Brug Share With Care til at finde det, du leder efter, lovligt. På den måde passer du både på dig selv og på kulturen. **Læs mere om Share With Care**

Introduction to Censorship



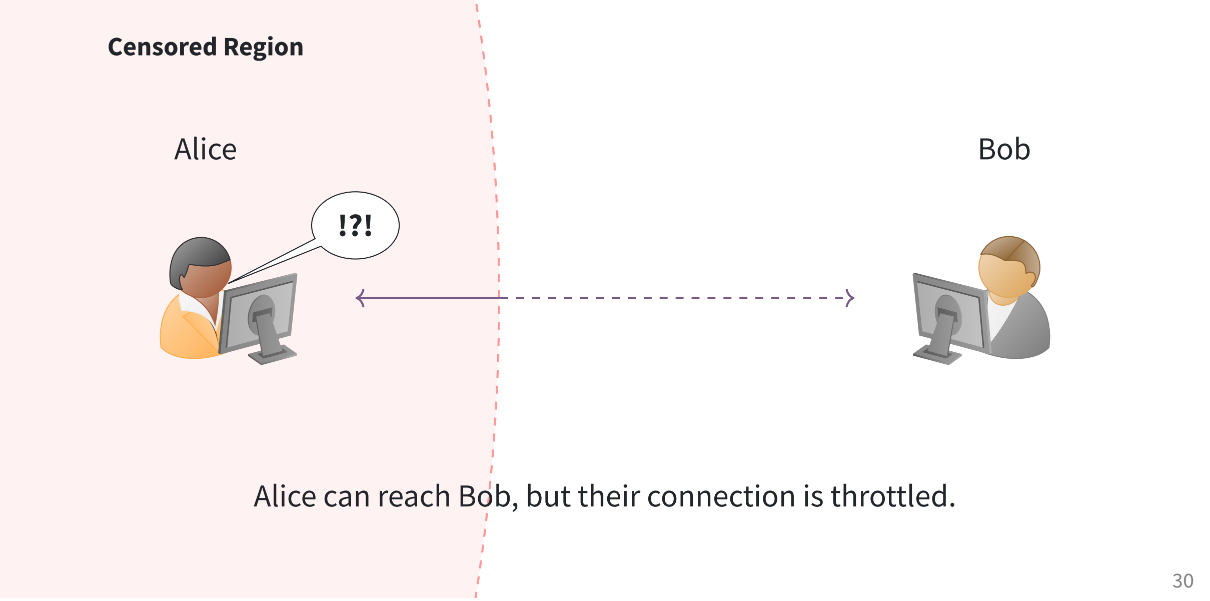
Censored Region

Alice

Bob

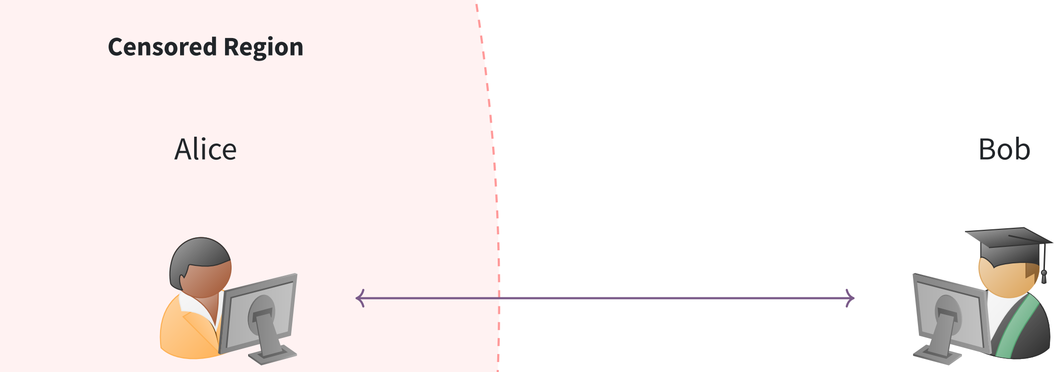
Alice is unable to reach Bob.

Introduction to Censorship



Alice can reach Bob, but their connection is throttled.

Introduction to Censorship



Censored Region

Alice

Bob

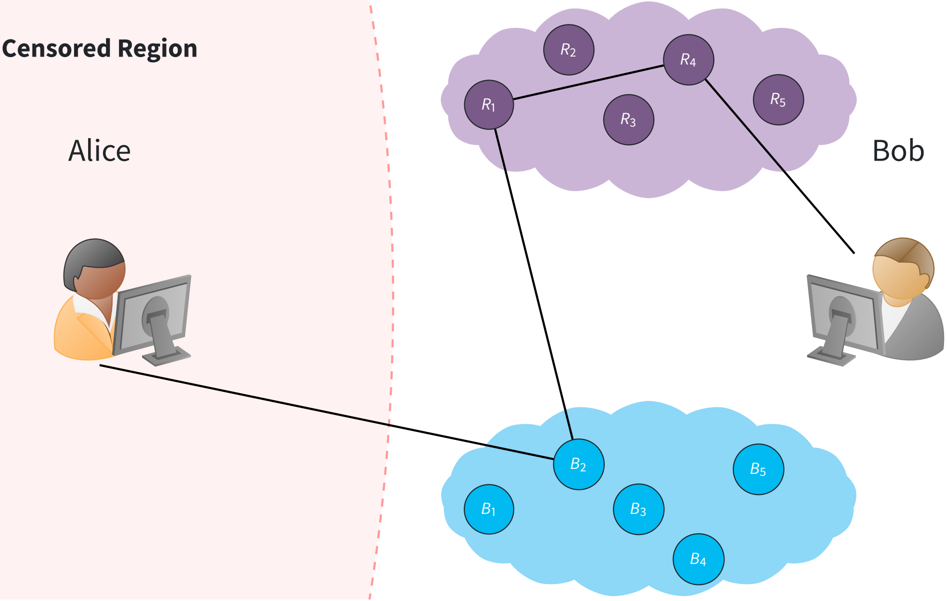
Alice can reach Bob because the censor thinks Bob is fine.

Anti-censorship Strategies

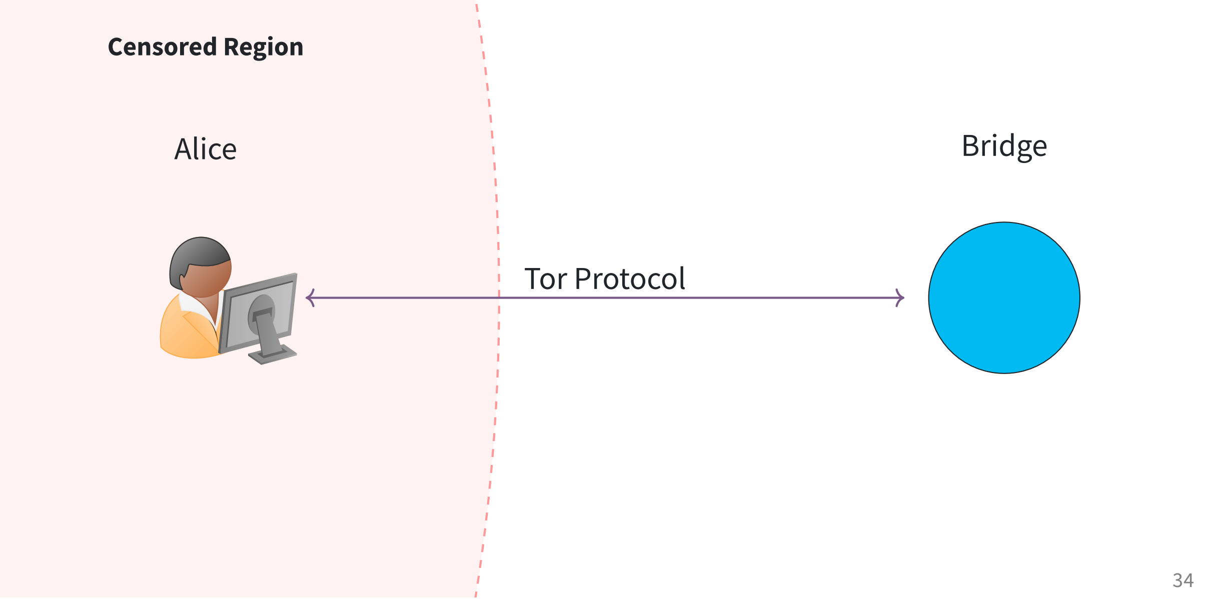
1. Censors will apply censorship to **all** relays in the network and effectively block access to the Tor network.
2. Censors will apply censorship to **known** bridges.

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



Bridges



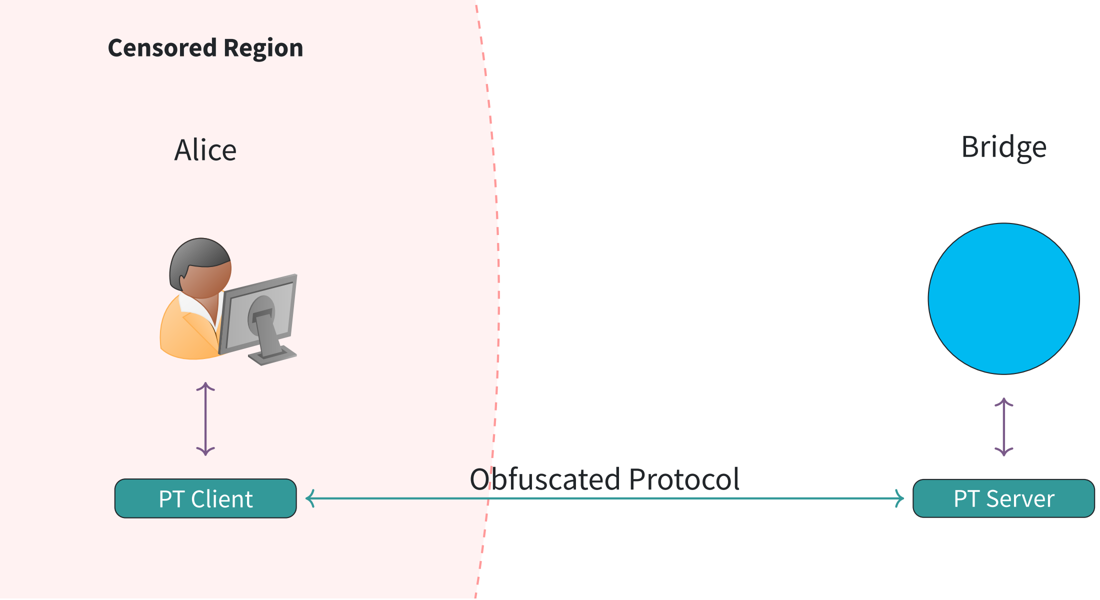
Censored Region

Alice

Tor Protocol

Bridge

Bridges and Pluggable Transports



Censored Region

Alice

Bridge

PT Client

Obfuscated Protocol

PT Server

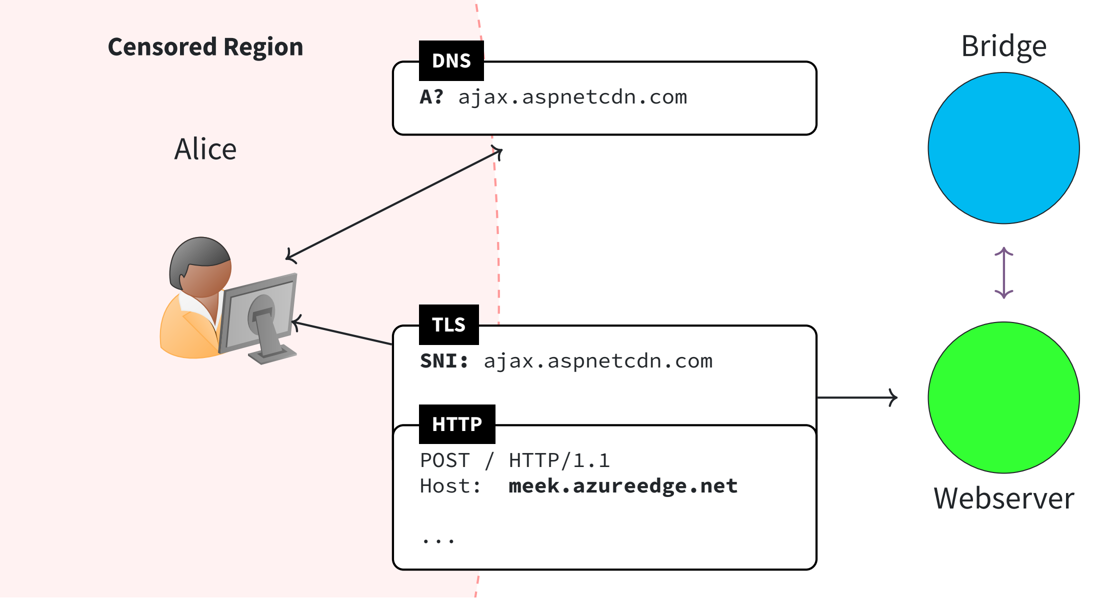
Pluggable Transports

- 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)

- Does full x25519 handshakes, but uses Elligator2 to map elliptic curve points.
- Allows you to tune timers for traffic.
- Makes active probing hard unless the adversary knows the parameters of the given bridge.

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** :-(

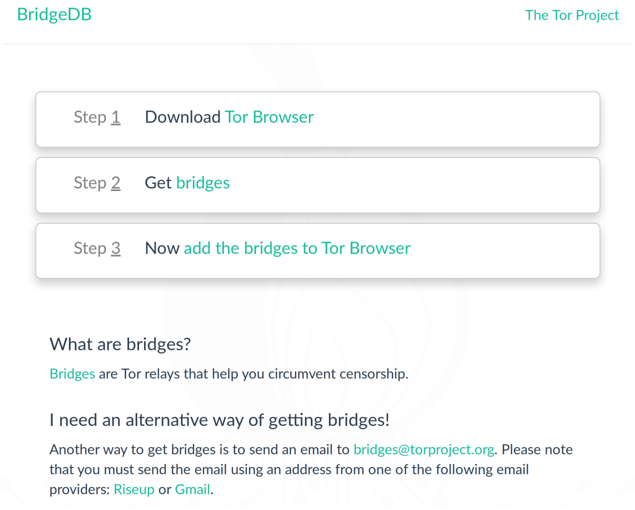
Unpopular with the cloud providers:

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?
- Using message queue services provided by the different cloud vendors?
- 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?

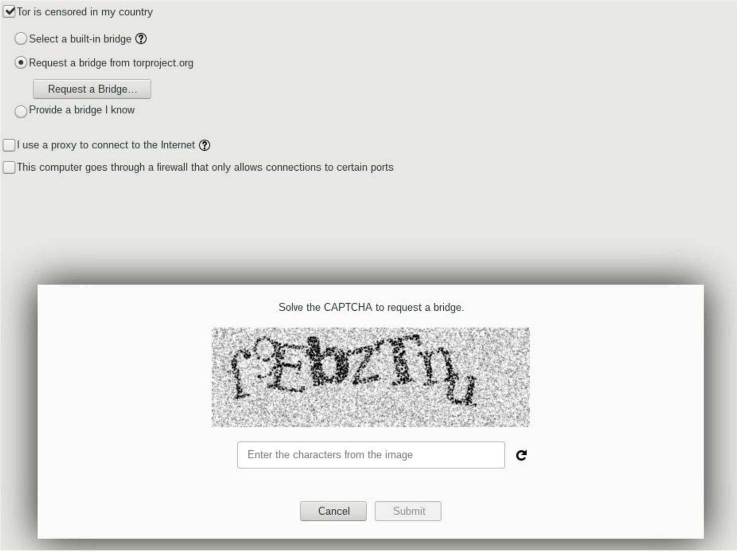
Bridges are Tor relays that help you circumvent censorship.

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

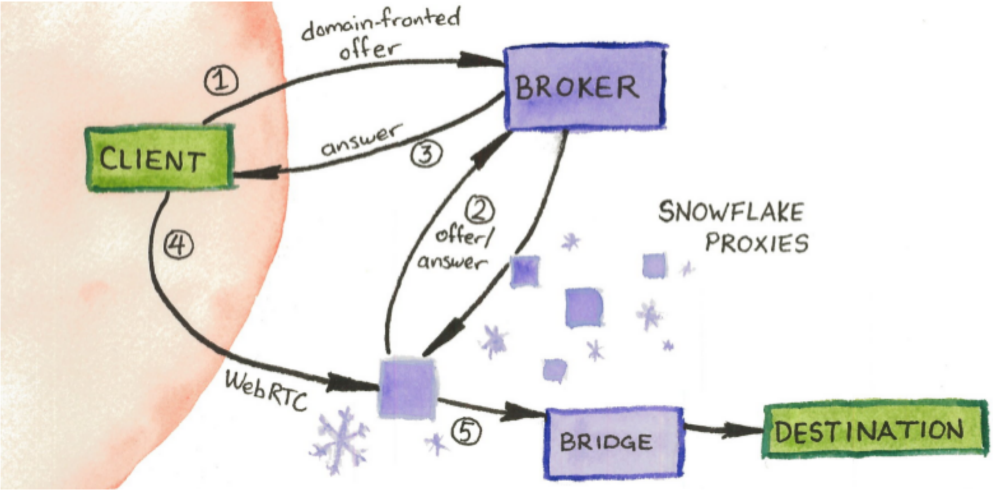
○ Provide a bridge I know

□ I use a proxy to connect to the Internet ?

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

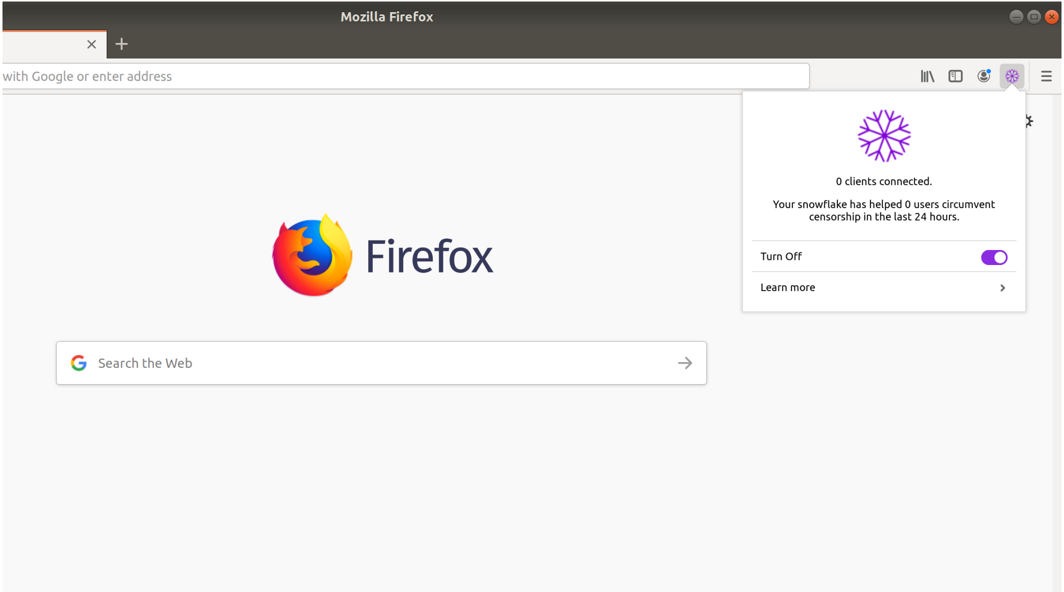
Solve the CAPTCHA to request a bridge.

Snowflake



Source: snowflake.torproject.org

Snowflake



0 clients connected.

Your snowflake has helped 0 users circumvent censorship in the last 24 hours.

Turn Off

Learn more

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?