Introduction to The Tor Ecosystem

Privacy, Anonymity, and Anti-censorship

Alexander Færøy

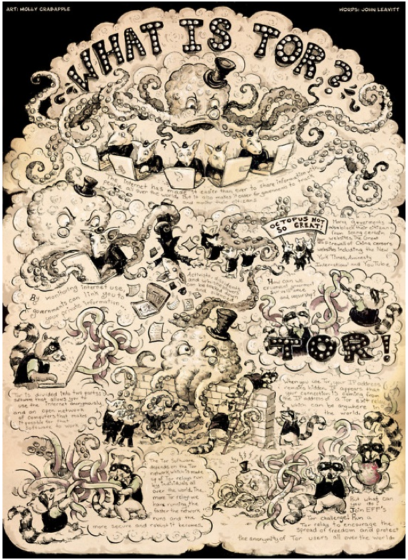
June 13, 2019

About Me

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

What is Tor?

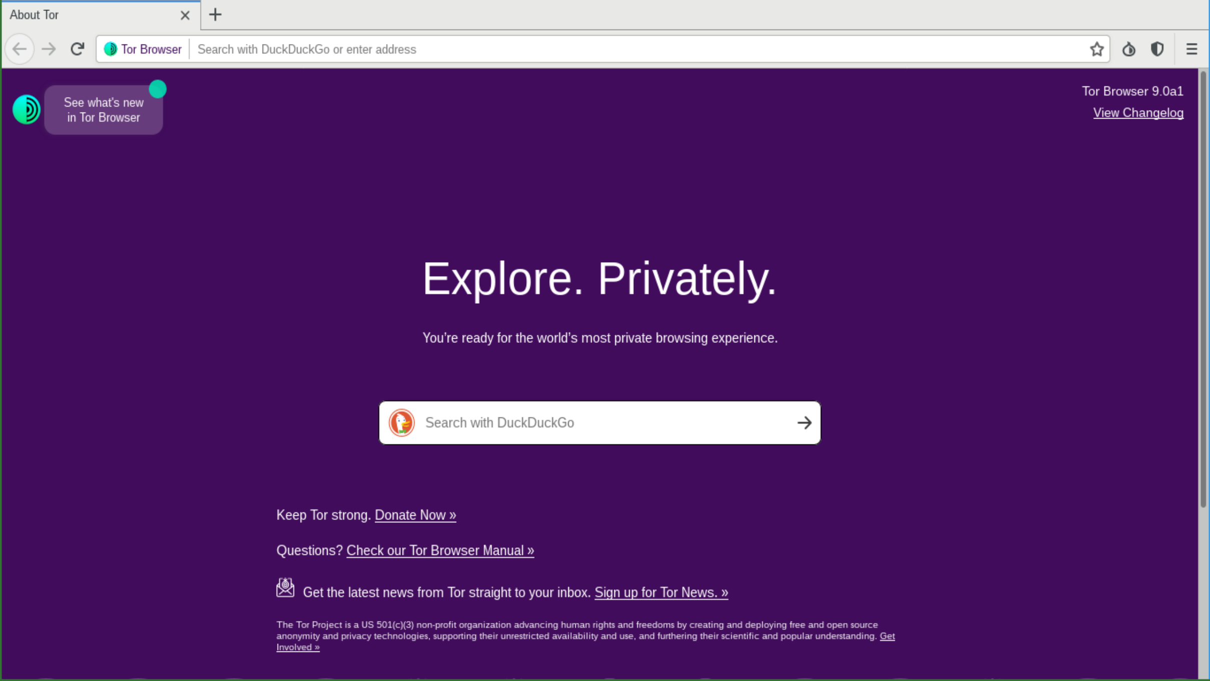
- Online anonymity and censorship circumvention.
  - Free software.
  - Open network.
- Community of researchers, developers, users, and relay operators.
- U.S. 501(c)(3) non-profit organization.


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 whistle-blowers 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.

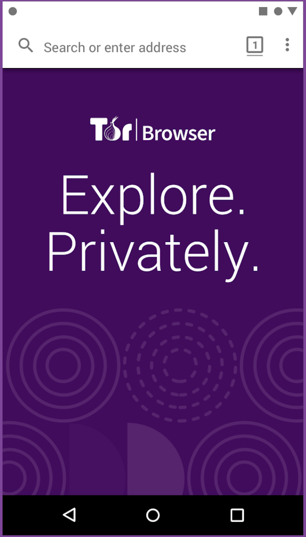
You're ready for the world's most private browsing experience.

Keep Tor strong. Donate Now »

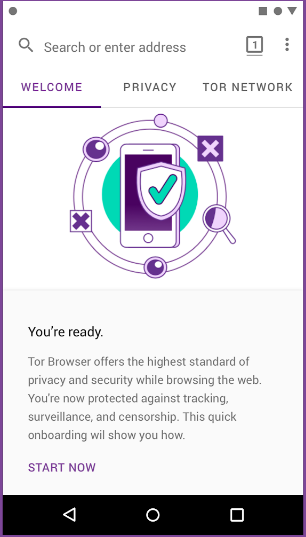
Questions? Check our Tor Browser Manual »

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 »

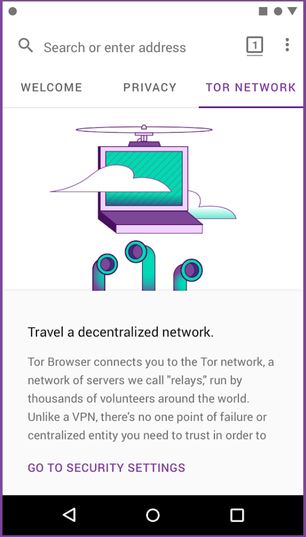


Explore. Privately.



You're ready.

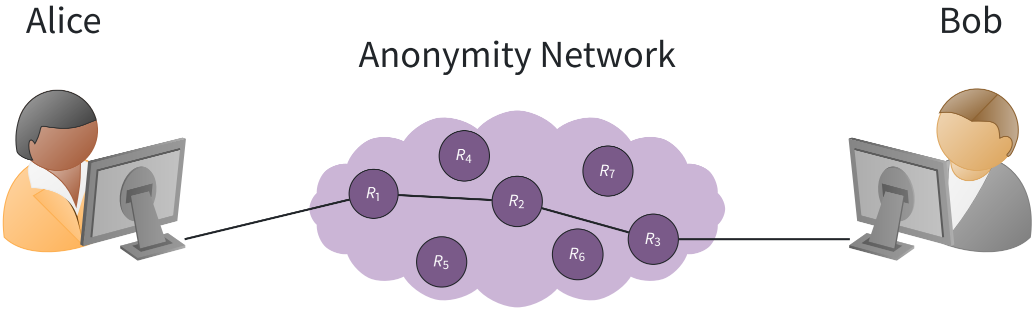
Tor Browser offers the highest standard of privacy and security while browsing the web. You're now protected against tracking, surveillance, and censorship. This quick onboarding wil show you how.



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

Threat Model



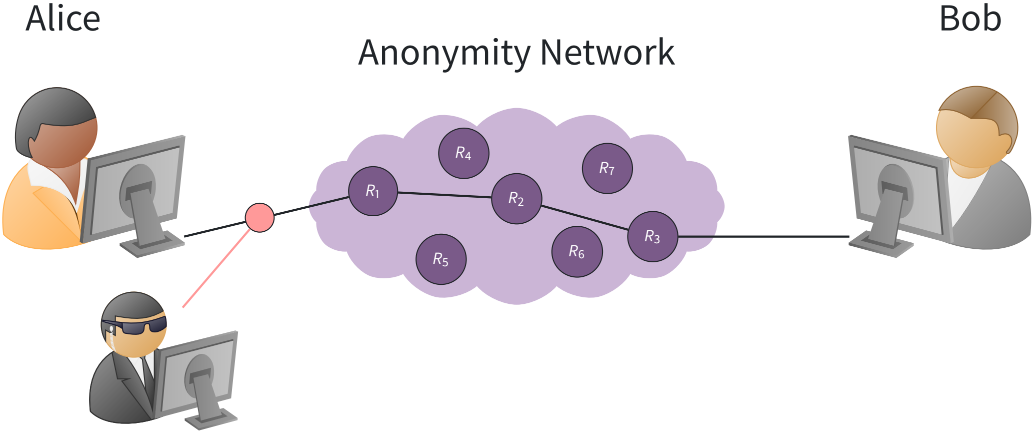
Alice

Anonymity Network

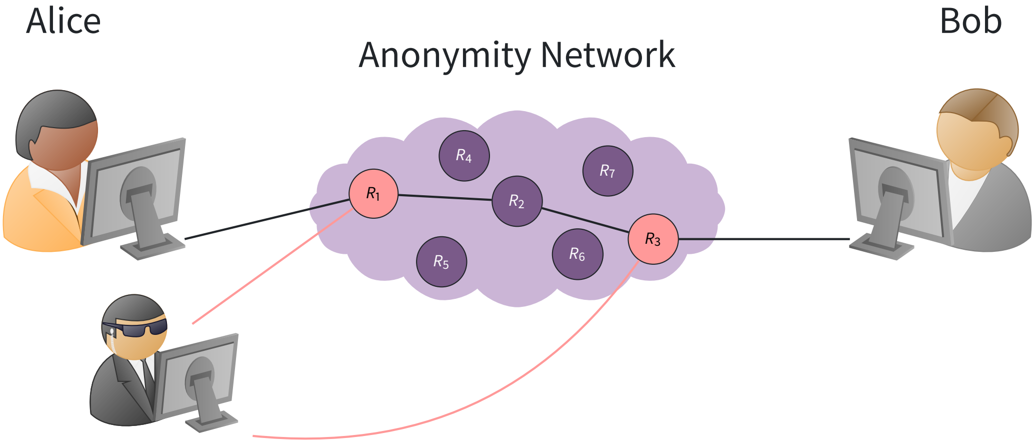
Bob

What can the attacker do?

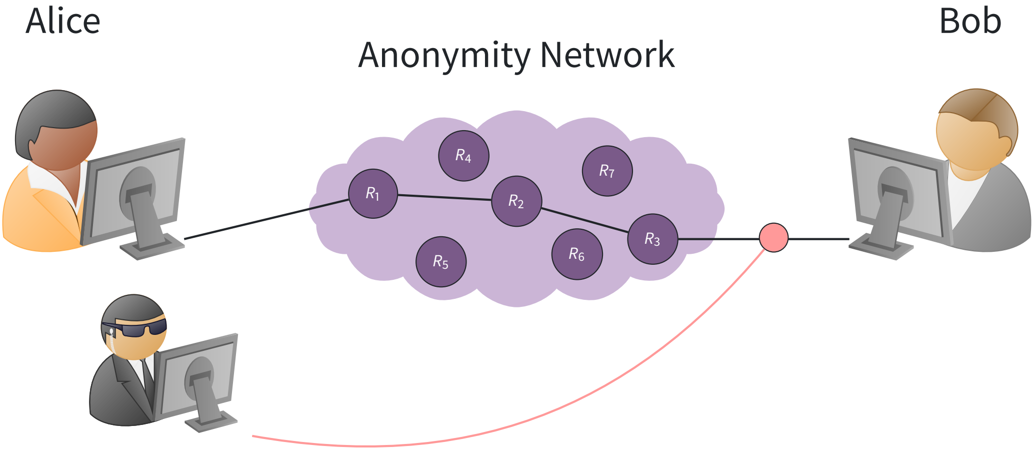
Threat Model



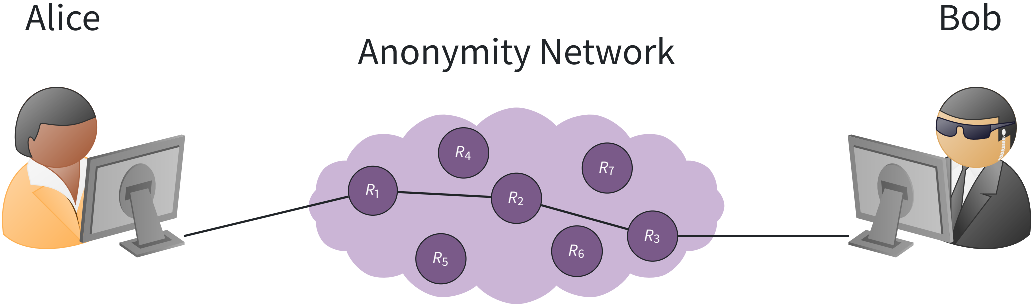
Threat Model



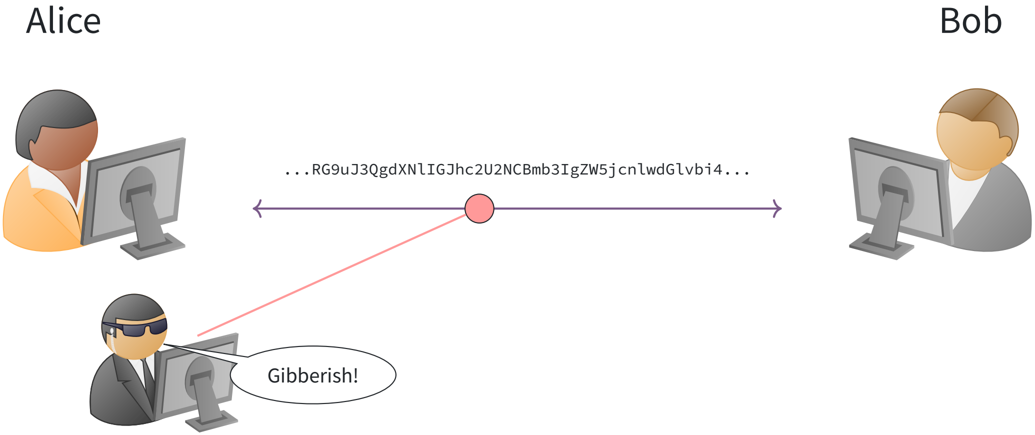
Threat Model



Threat Model



Anonymity isn’t Encryption



Encryption just protects contents.

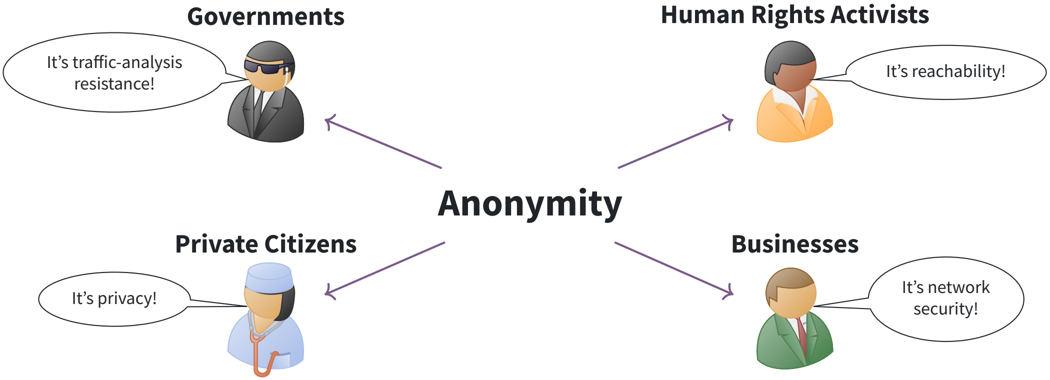
Metadata

The Data About Data

"We Kill People Based on Metadata."

—Michael Hayden, former director of the NSA.

Different Purposes of Anonymity



Governments

It's traffic-analysis resistance!

Human Rights Activists

It's reachability!

Anonymity

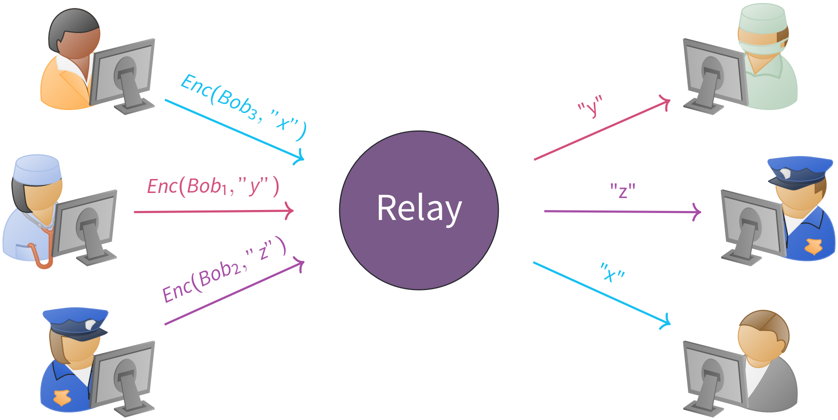
Private Citizens

It's privacy!

Businesses

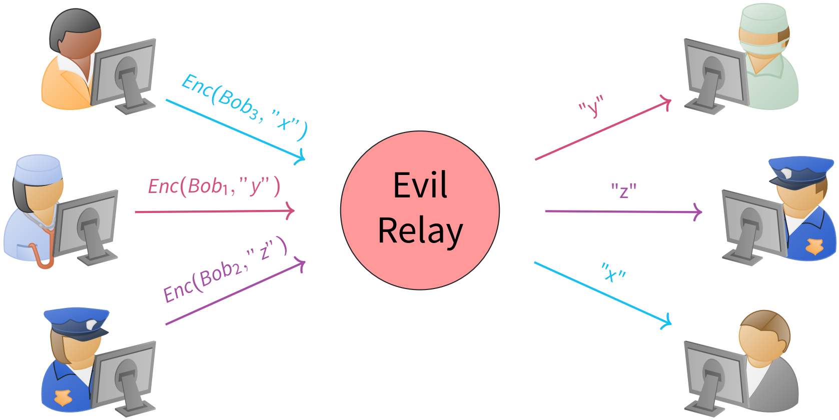
It's network security!

A Simple Design

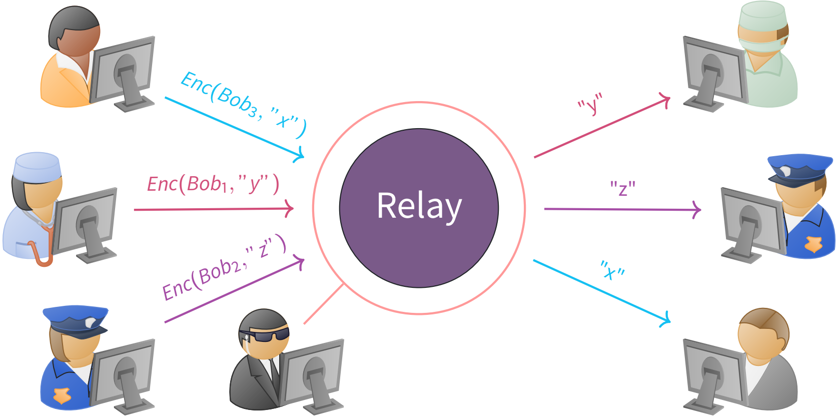


Equivalent to some commercial proxy providers.

A Simple Design

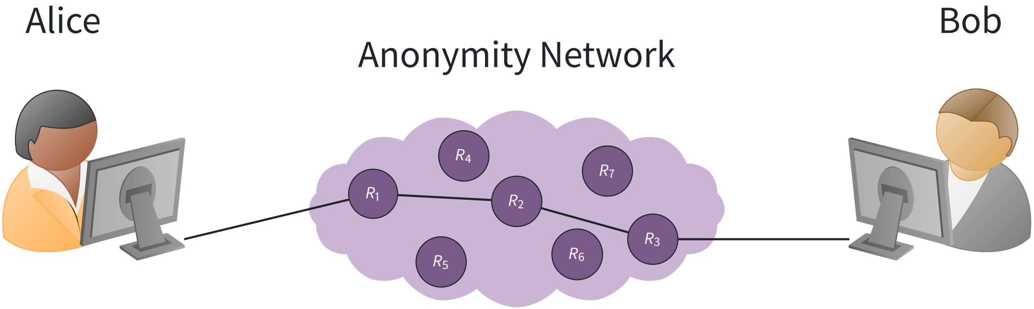


A Simple Design



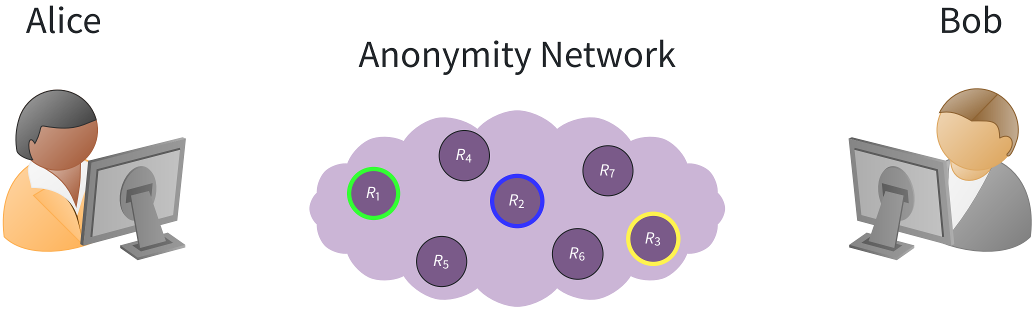
Timing analysis bridges all connections going through the relay.

The Tor Design



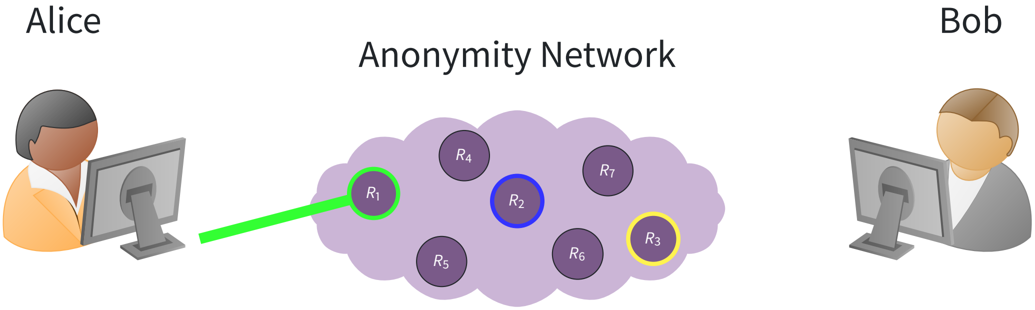
Add multiple relays so that no single relay can betray Alice.

The Tor Design



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

The Tor Design



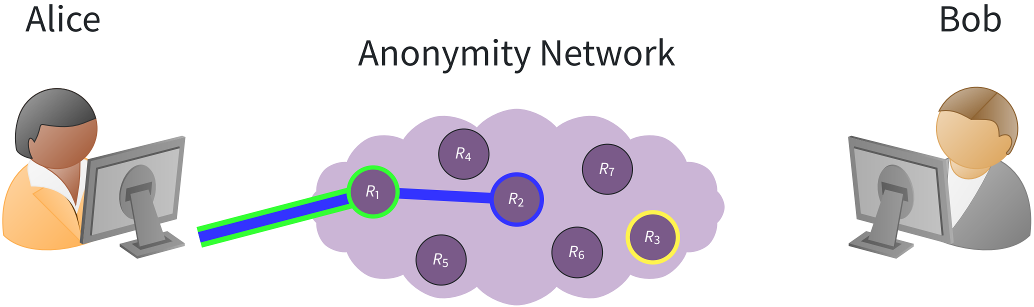
Alice

Anonymity Network

Bob

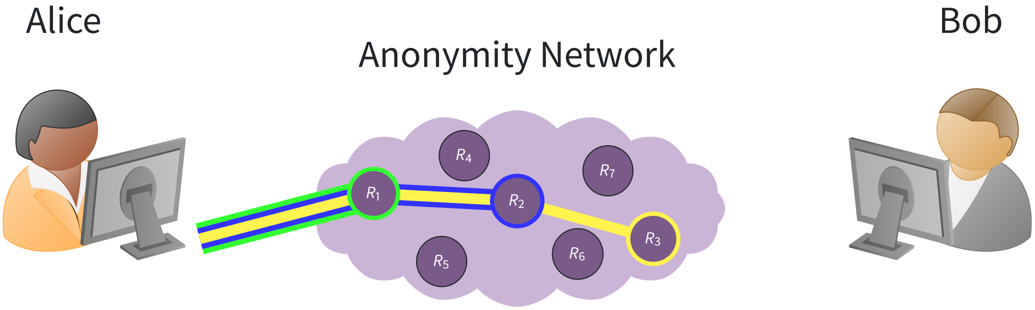
Alice makes a session key with R_1.

The Tor Design



Alice asks R_1 to extend to R_2.

The Tor Design



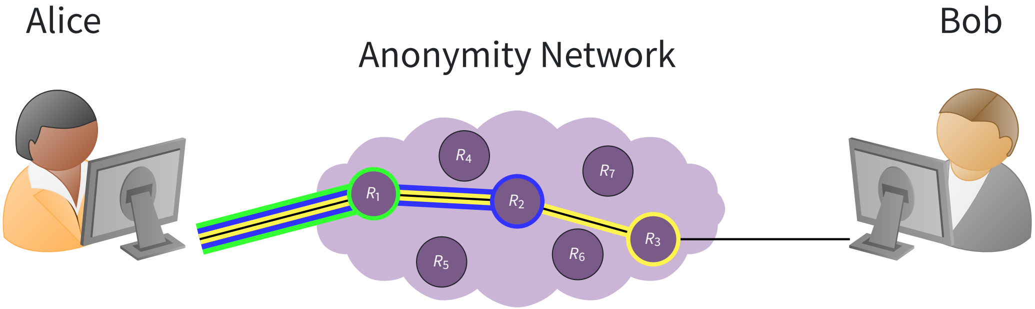
Alice

Anonymity Network

Bob

Alice asks R_2 to extend to R_3.

The Tor Design

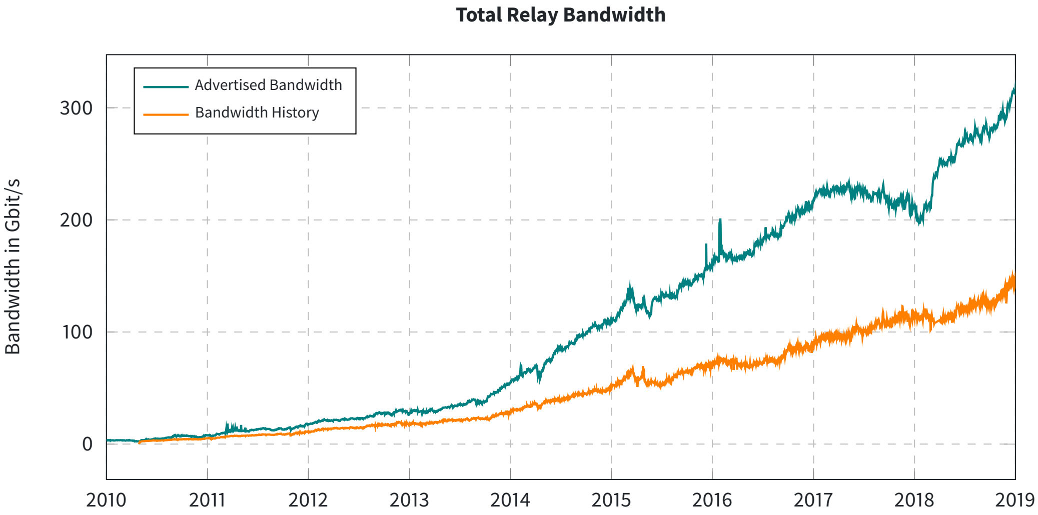


Alice finally asks R_3 to connect to Bob.

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.
- What is the IPv6 story?

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’m a political activist, part of a semi-criminalized minority. In my younger years I entered the public debate openly, and as a result got harassed by government agencies. I later tried to obfuscate my identity, but I found that my government has surprisingly broad powers to track down dissidents.

Only by using anonymizing means, among which Tor is key, can I get my message out without having police come to "check my papers" in the middle of the night. **Tor allows me freedom to publish my message to the world without being personally persecuted for it.**

Being a dissident is hard enough, privacy is already heavily curtailed, so anonymized communication is a godsend.

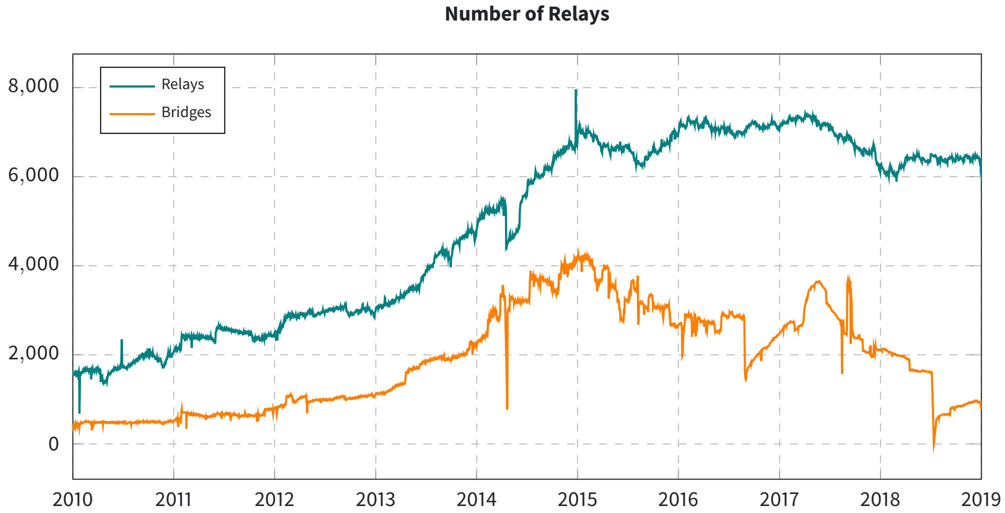
—Anonymous Tor User.

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.**

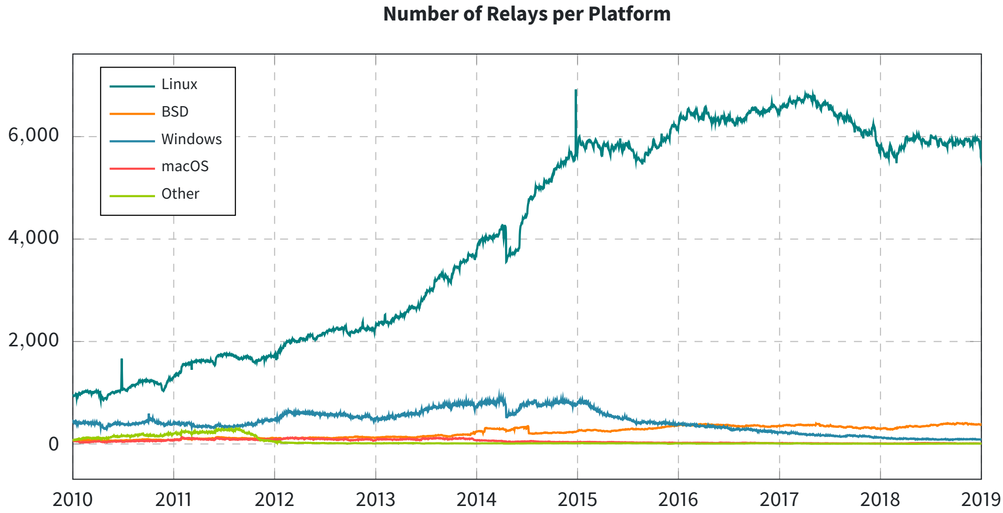
—Anonymous Tor User.

The Tor Network



Source: metrics.torproject.org

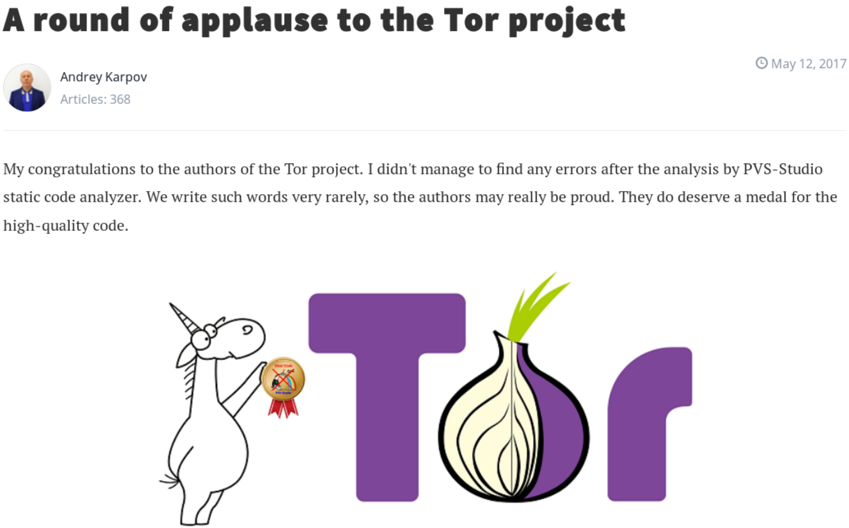
The Tor Network



Source: metrics.torproject.org

The Implementation of Tor

- The reference Tor implementation is written in the C programming language.
- Ongoing experiments with Mozilla's Rust programming language.
- Follow best practices: high coverage for tests, integration tests, coverity, static code analysis, and code review policies.
- Specification and discussion before implementation. Specifications can be found at gitweb.torproject.org/torspec.



A round of applause to the Tor project

Andrey Karpov

Articles: 368

May 12, 2017

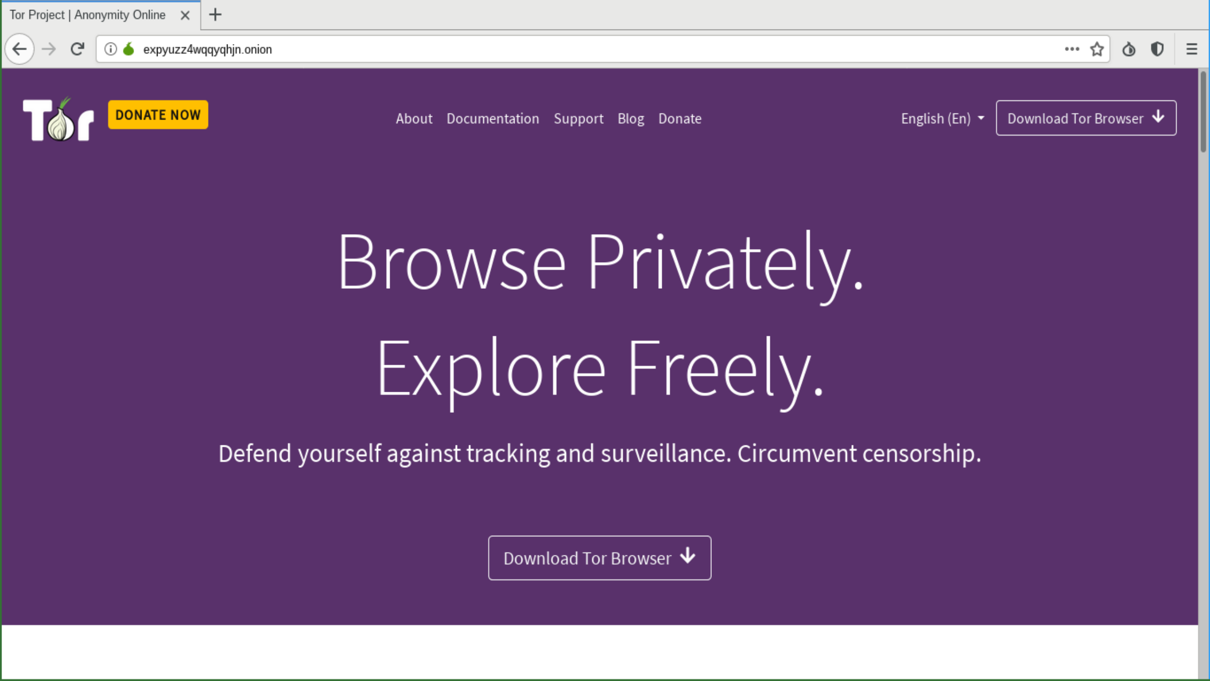
My congratulations to the authors of the Tor project. I didn't manage to find any errors after the analysis by PVS-Studio static code analyzer. We write such words very rarely, so the authors may really be proud. They do deserve a medal for the high-quality code.

Source: viva64.com

Onion Services

- Allows servers to be anonymous.
- The ".onion" Special-Use Domain Name (RFC 7686).
- Introduced in Tor version 0.0.6pre1 from April, 2004.
- Traffic stays within the Tor network: No need to exit the network.
- Onion addresses are either 16 characters long (for version 2) or 52 characters long (for version 3).

Research problem: How do we handle these long addresses?



Browse Privately.
Explore Freely.

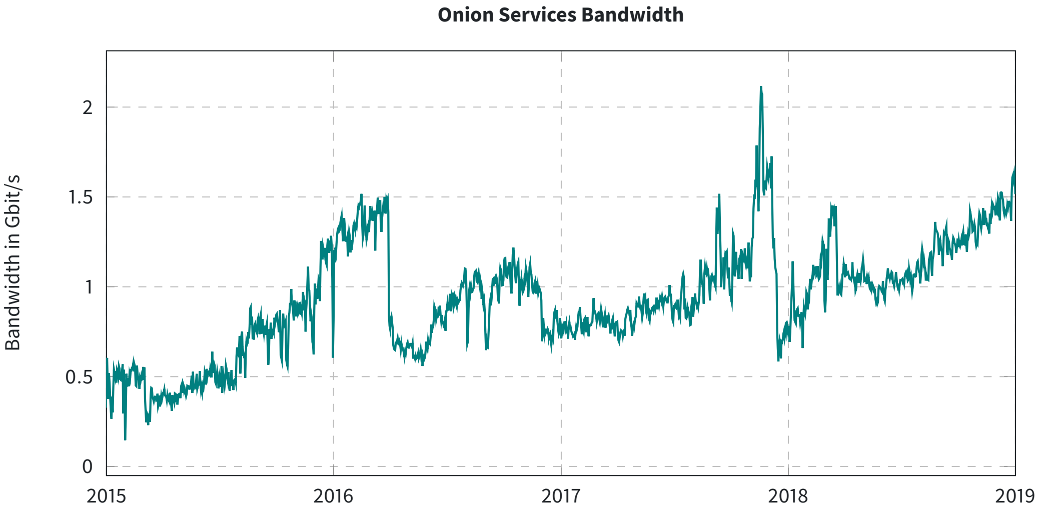
Defend yourself against tracking and surveillance. Circumvent censorship.

Onion Services

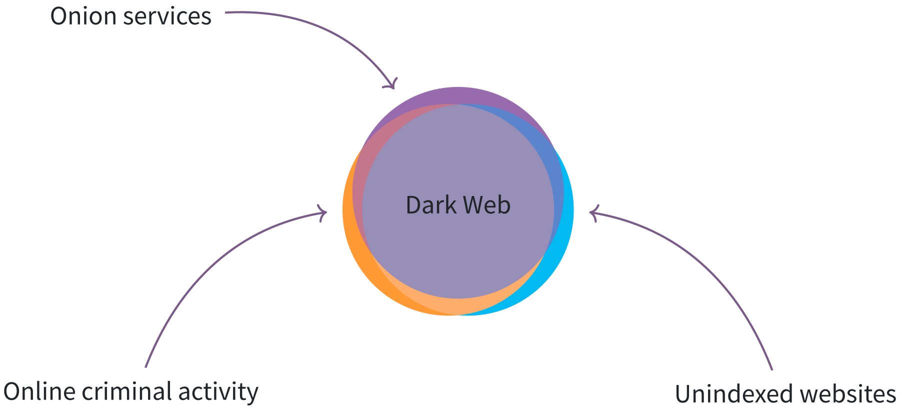
Properties includes:

- Self authenticated.
- End-to-end encrypted.
- Isolation and NAT punching.
- Minimized attack surface.
- Support for Unix domain sockets.

Onion Services



Source: metrics.torproject.org



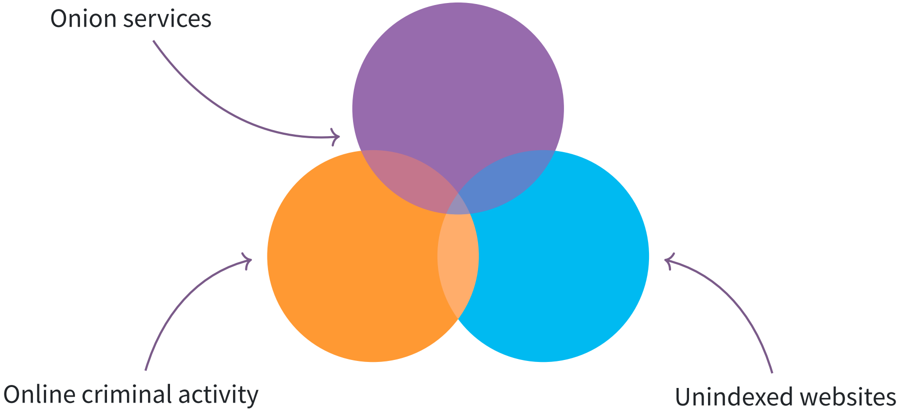
Onion services

Dark Web

Online criminal activity

Unindexed websites

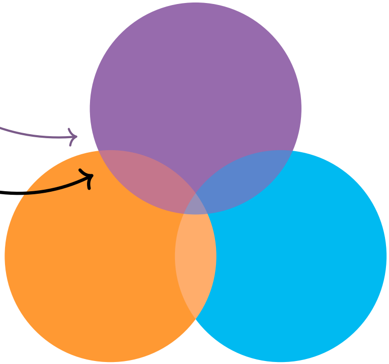
The "Dark Web" as popularly depicted.



Closer to reality.

Onion services

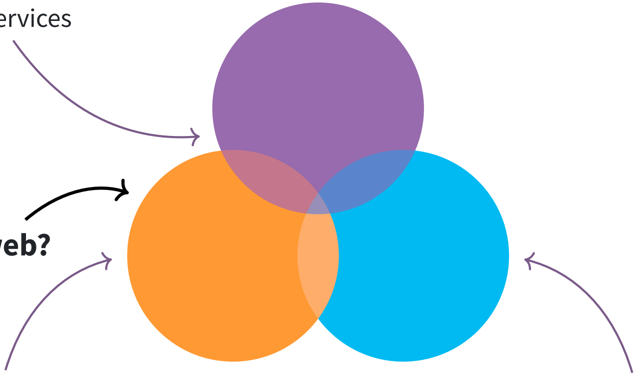
Dark web?



Online criminal activity

Unindexed websites

Closer to reality.



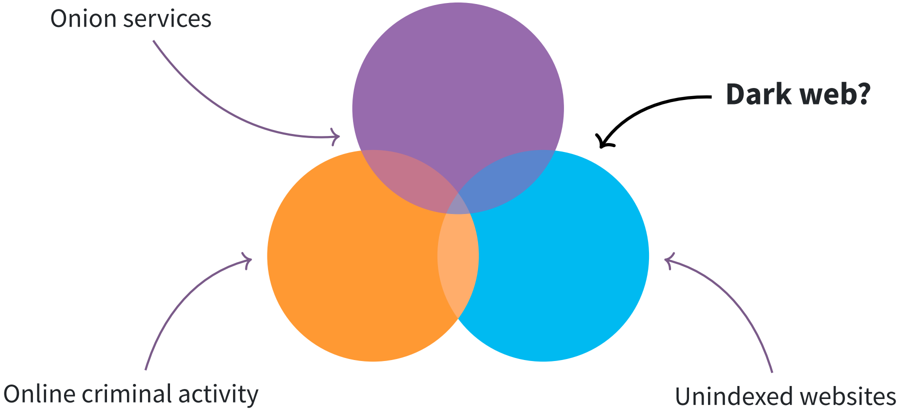
Onion services

Dark web?

Online criminal activity

Unindexed websites

Closer to reality.



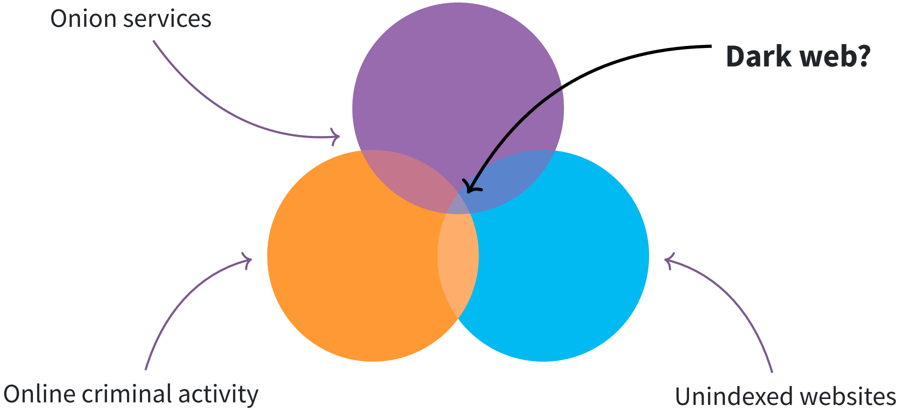
Onion services

Dark web?

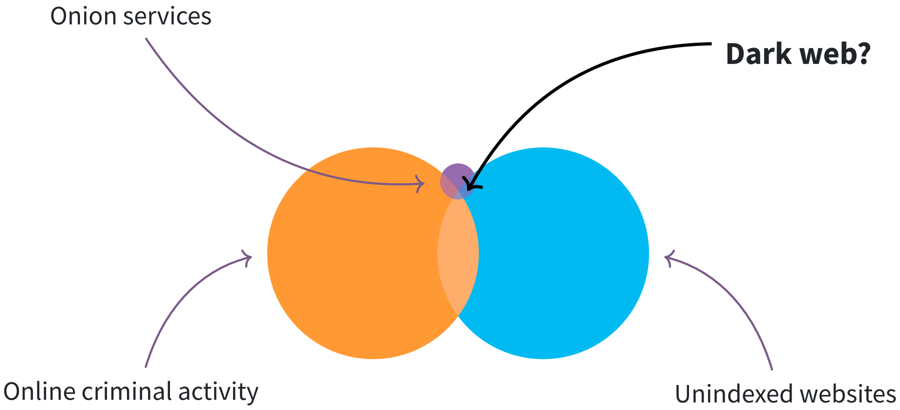
Online criminal activity

Unindexed websites

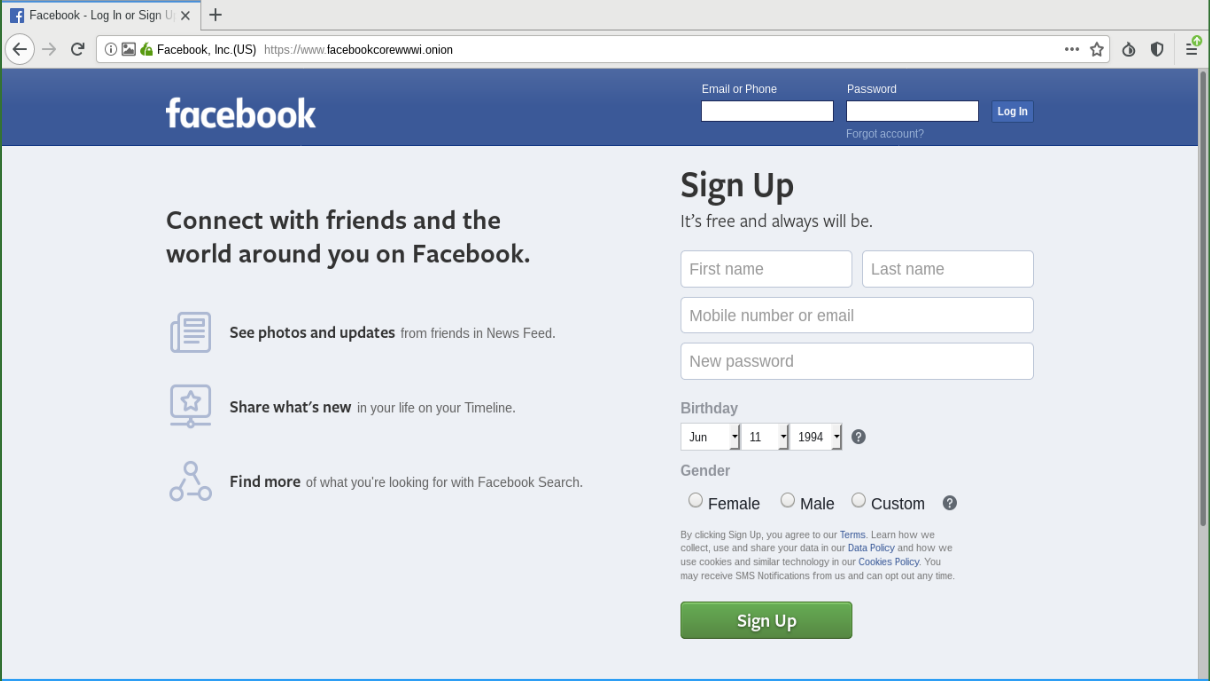
Closer to reality.



Closer to reality.



Scale also matters.



Facebook - Log In or Sign U
Facebook, Inc.(US) https://www.facebookcorewwwi.onion
facebook
Email or Phone
Password
Log In
Forgot account?

Connect with friends and the world around you on Facebook.

See photos and updates from friends in News Feed.

Share what's new in your life on your Timeline.

Find more of what you're looking for with Facebook Search.

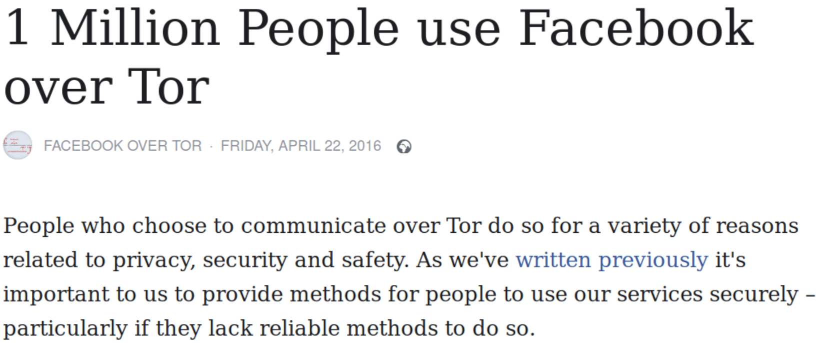
Sign Up

It's free and always will be.

Birthday: Jun 11 1994

Gender: ○ Female ○ Male ○ Custom

By clicking Sign Up, you agree to our Terms. Learn how we collect, use and share your data in our Data Policy and how we use cookies and similar technology in our Cookies Policy. You may receive SMS Notifications from us and can opt out any time.



1 Million People use Facebook over Tor

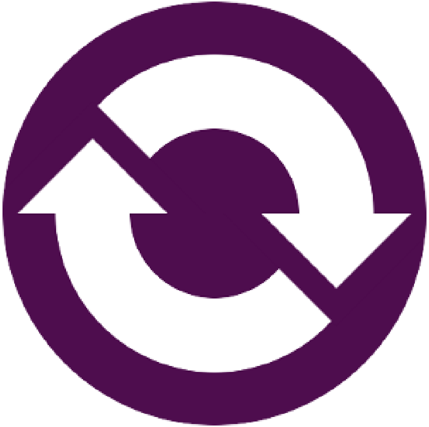
FACEBOOK OVER TOR · FRIDAY, APRIL 22, 2016

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.

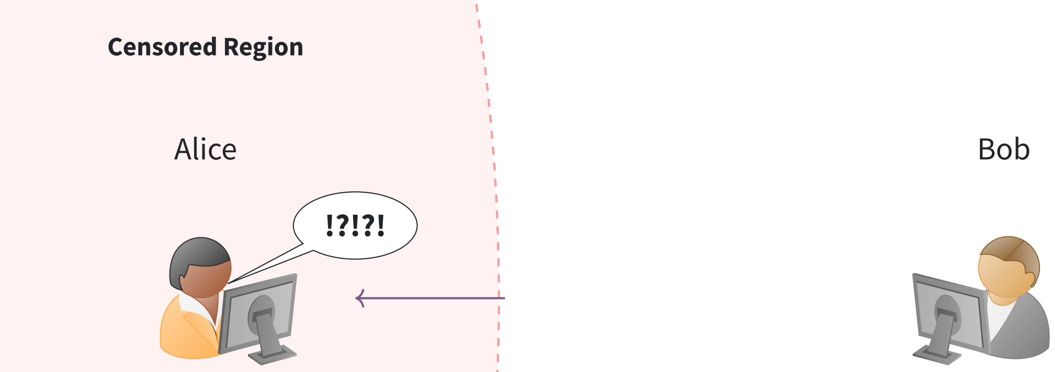
Source: facebook.com

SecureDrop

OnionShare

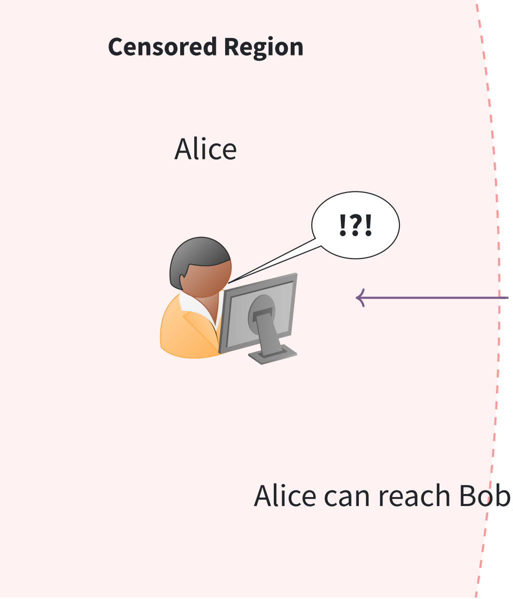


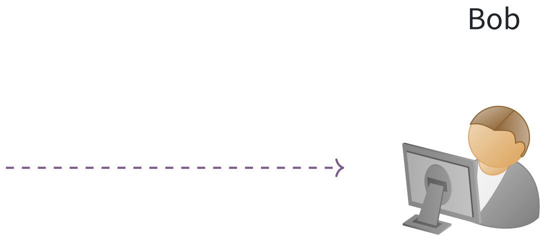
Introduction to Censorship



Alice is unable to reach Bob.

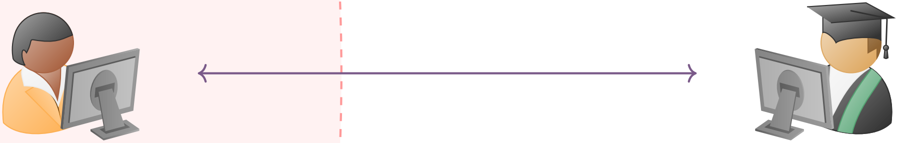
Introduction to Censorship





Alice can reach Bob, but their connection is throttled.

Introduction to Censorship

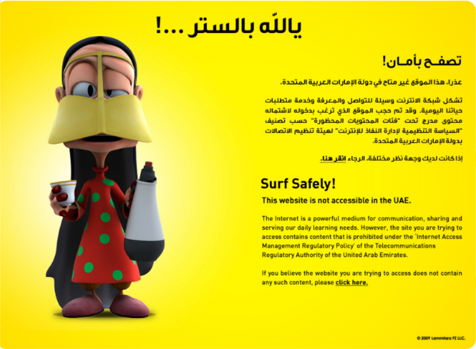


Censored Region

Alice

Bob

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



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.

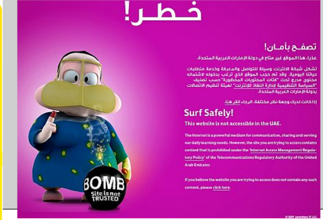
Surf Safely!

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.

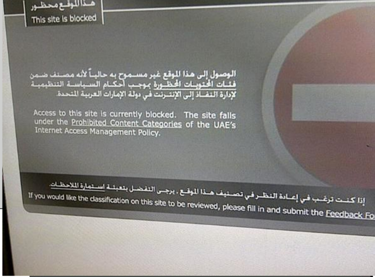
Surf Safely!

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.



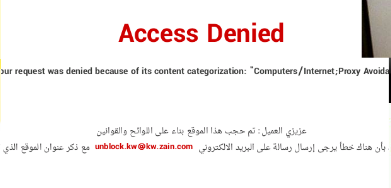
هـذا الموقـع محظـور
This site is blocked

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

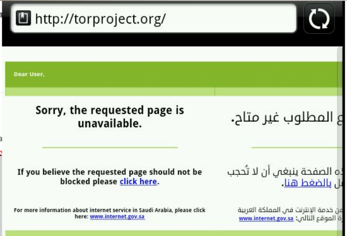
our request was denied because of its content categorization: "Computers/Internet;Proxy Avoida

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.

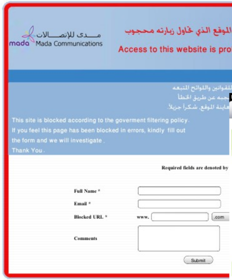
المطلوب غير متاح.

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



ان الموقع الذي تحاول زيارته محجوب

Access to this website is prohibited

ان الموقع الذي تحاول زيارته محجوب وذلك طبقاً للقوانين واللوائح المتبعه

جبه عن طريق الخطأ

عاينة الموقع. 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

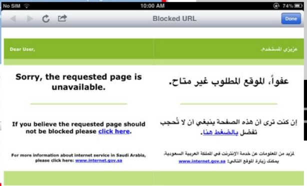
Full Name *

Email *

Blocked URL. * www. .com

Comments

Submit



Dear User,

عزيزي المستخدم،

Sorry, the requested page is unavailable.

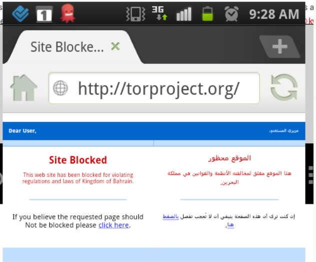
عفواً، الموقع المطلوب غير متاح.

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



http://torproject.org/

Dear User,

عزيزي المستخدم،

Site Blocked

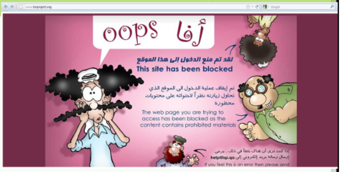
This web site has been blocked for violating regulations and laws of Kingdom of Bahrain.

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.



لقد تم منع الدخول إلى هذا الموقع

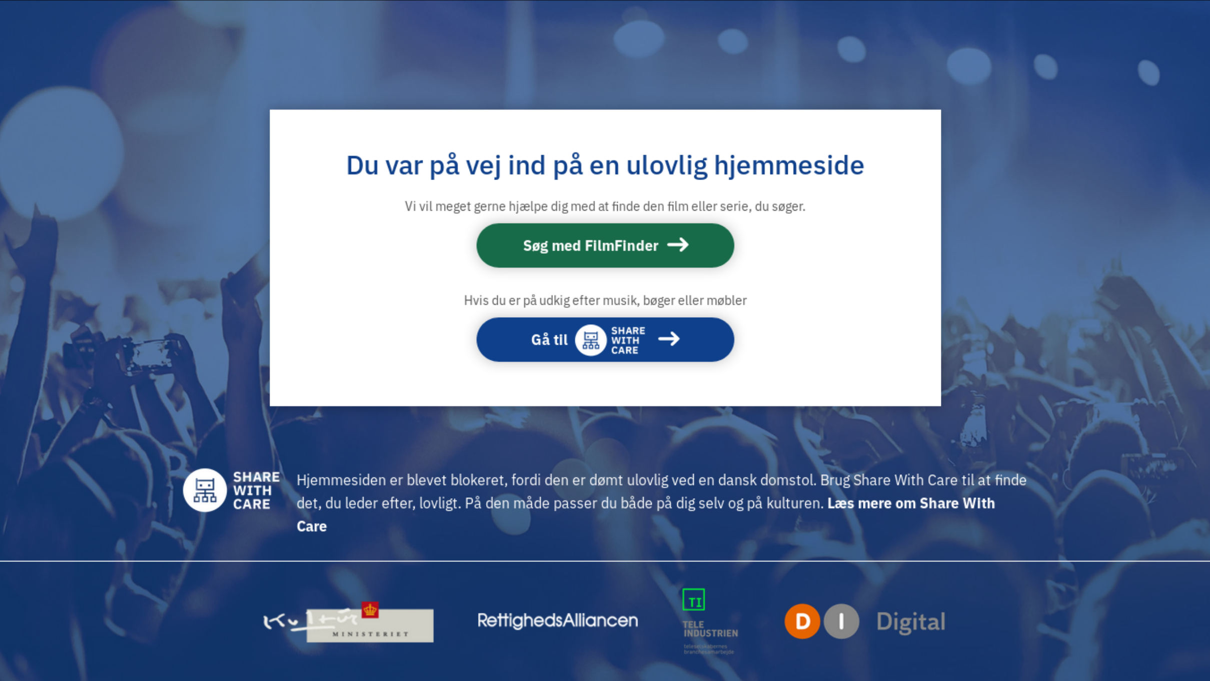
This site has been blocked

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



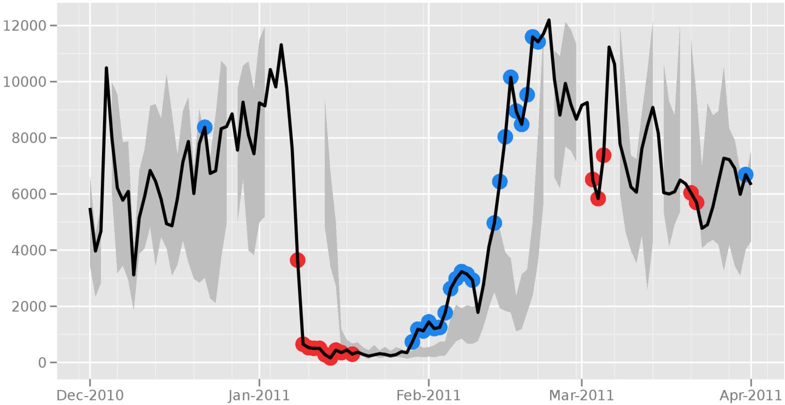
Du var på vej ind på en ulovlig hjemmeside

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**

Directly connecting users from the Islamic Republic of Iran

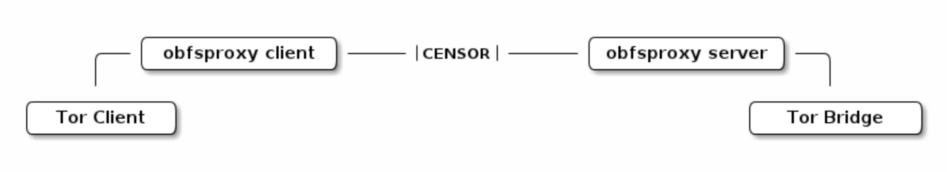


The Tor Project - https://metrics.torproject.org/

Anti-censorship Strategies

- Censors will apply censorship to nodes in the network.
- Same for known bridges.
- Solution: either make it hard to analyze the traffic or make it hard to block the bridges.

Pluggable Transports



obfsproxy client

| CENSOR |

obfsproxy server

Tor Client

Tor Bridge

Obfourscator (obfs4)

- Does full x25519 handshakes, but uses Elligator2 to map elliptic curve points.
- Allows you to tune timers for traffic.

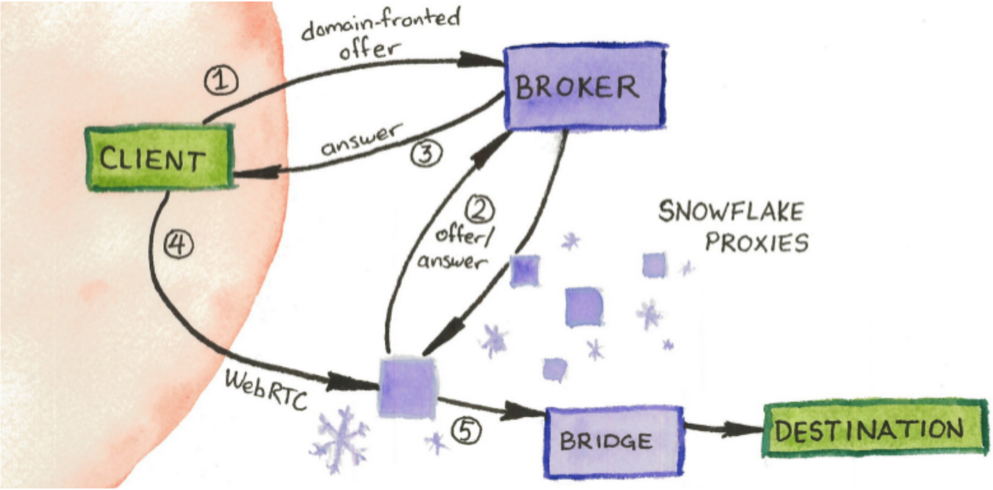
Meek

- Connect with TLS with SNI set to some large user of the cloud provider.
- Inside your TLS connection you do a normal HTTP request, but with the Host header set to the server you want to reach inside the cloud.
- Efficient, but expensive :-(

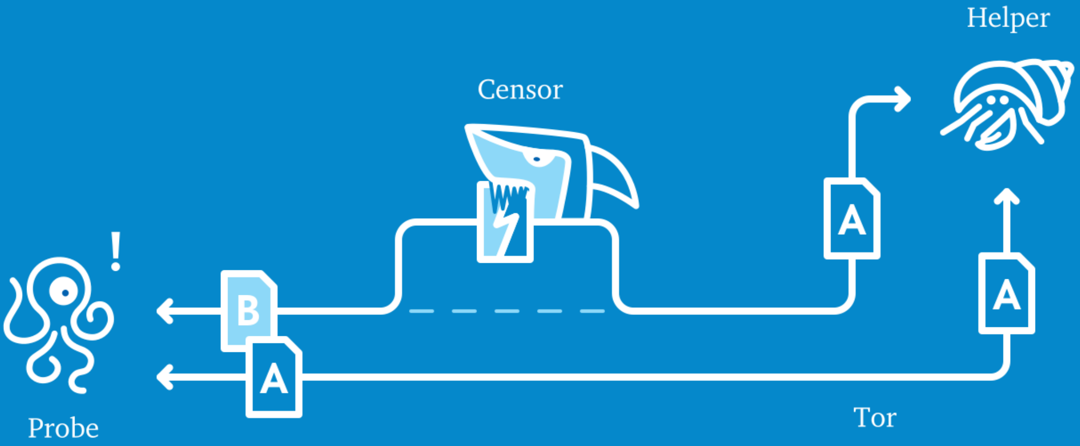
Domain Fronting

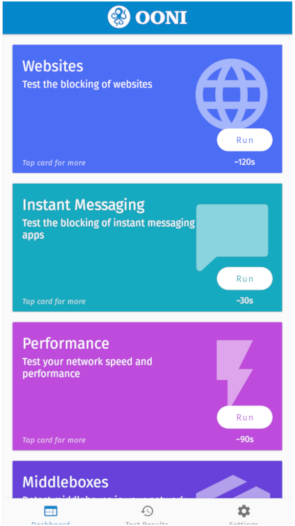
- Using ESNI?
- Using various cloud providers message queue services?
- Generally using large centralized services to give access to censored people.

Snowflake


domain-fronted offer
①
BROKER
CLIENT
answer
③
②
offer/ answer
SNOWFLAKE PROXIES
④
WebRTC
⑤
BRIDGE
DESTINATION

Open Observatory of Network Interference





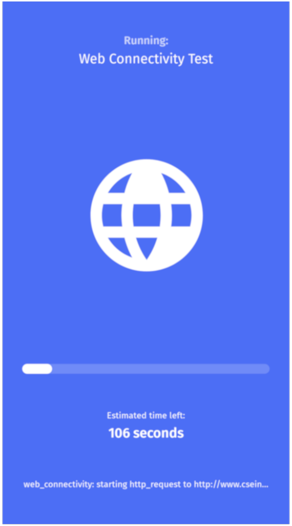
OONI

Websites
Test the blocking of websites
Run
Tap card for more
~120s

Instant Messaging
Test the blocking of instant messaging apps
Run
Tap card for more
~30s

Performance
Test your network speed and performance
Run
Tap card for more
~90s

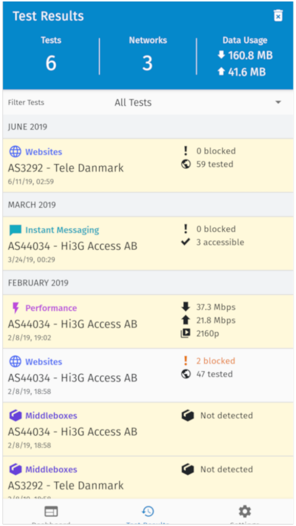
Middleboxes



Running:
Web Connectivity Test

Estimated time left:
106 seconds

web_connectivity: starting http_request to http://www.csein...



Test Results

Tests	Networks	Data Usage
6	3	⬇ 160.8 MB ⬆ 41.6 MB

Filter Tests All Tests

JUNE 2019

Websites
AS3292 - Tele Danmark
6/11/19, 02:59
! 0 blocked
59 tested

MARCH 2019

Instant Messaging
AS44034 - Hi3G Access AB
3/24/19, 00:29
! 0 blocked
✓ 3 accessible

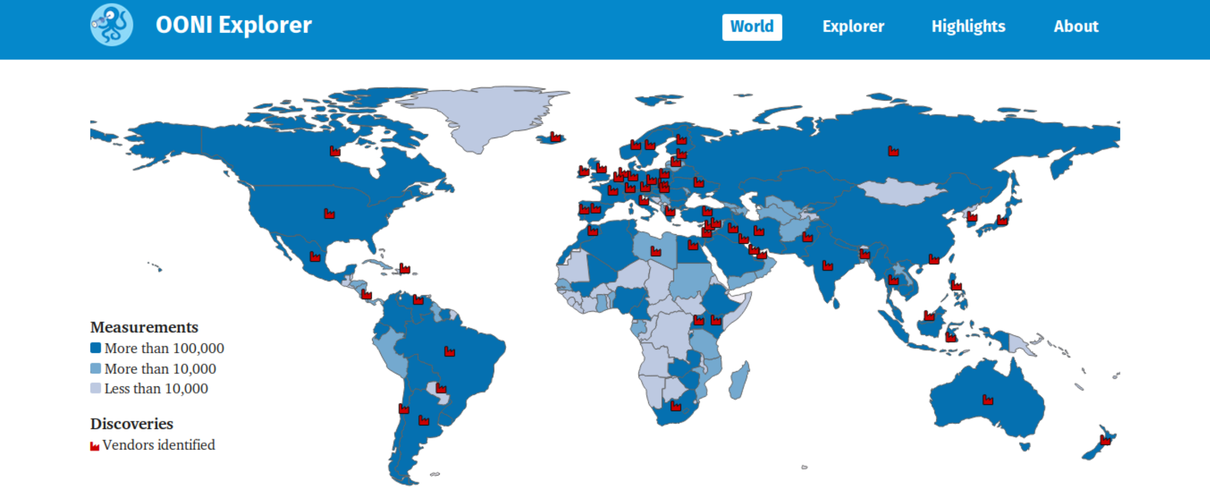
FEBRUARY 2019

Performance
AS44034 - Hi3G Access AB
2/8/19, 19:02
⬇ 37.3 Mbps
⬆ 21.8 Mbps
2160p

Websites
AS44034 - Hi3G Access AB
2/8/19, 18:58
! 2 blocked
47 tested

Middleboxes
AS44034 - Hi3G Access AB
2/8/19, 18:58
Not detected

Middleboxes
AS3292 - Tele Danmark
Not detected



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?