The Tor Project

Our mission is to be the global resource for technology, advocacy, research and education in the ongoing pursuit of freedom of speech, privacy rights online, and censorship circumvention.
• Online Anonymity
  – Open Source
  – Open Network

• Community of researchers, developers, users and relay operators.

• U.S. 501(c)(3) non-profit organization
Estimated 2,000,000 to 8,000,000 daily Tor users
Threat model: what can the attacker do?

Alice

Anonymity network

Bob

watch Alice!

Control part of the network!

watch (or be!) Bob!
Anonymity isn't encryption: Encryption just protects contents.
Metadata

Data about data

“Metadata was traditionally in the card catalogs of libraries”
– Wikipedia

“We kill people based on metadata”
Anonymity serves different interests for different user groups.

“It's privacy!”
Anonymity serves different interests for different user groups.

“Anonymity”

Private citizens

“"It's privacy!""

Businesses

“It's network security!”
Anonymity serves different interests for different user groups.

“Anonymity”

Governments

“It's traffic-analysis resistance!”

Anonymity

Private citizens

“It's privacy!”

Businesses

“It's network security!”
Anonymity serves different interests for different user groups.

- **Human rights activists**: “It's reachability!”
- **Governments**: “It's traffic-analysis resistance!”
- **Private citizens**: “It's privacy!”
- **Businesses**: “It's network security!”

Diagram content:
- Anonymity
- Human rights activists
- Governments
- Private citizens
- Businesses
The simplest designs use a single relay to hide connections.

(example: some commercial proxy providers)
But a central relay is a single point of failure.
... or a single point of bypass.

Timing analysis bridges all connections through relay \( \Rightarrow \) An attractive fat target
So, add multiple relays so that no single one can betray Alice.
Alice makes a session key with R1
...And then tunnels to R2...and to R3
Explore. Privately.

You’re ready for the world’s most private browsing experience.
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 will 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 single point of failure or centralized entity you need to trust in order to
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: measuring diversity over time)

• #2: Diversity of users and reasons to use it. 50000 users in Iran means almost all of them are normal citizens.
Transparency for Tor is key

- Open source / free software
- Public design documents and specifications
- Publicly identified developers
- Not a contradiction: privacy is about choice!
But what about bad people?

- Remember the millions of daily users.
- Still a two-edged sword?
- Good people need Tor much more than bad guys need it.
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

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

This site has been blocked according to the government filtering policy.
If you feel this page has been blocked in error, kindly fill out the form here and we will investigate.

Thank You.

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

If you feel this is an error then please send a message to help@isp.org.
Directly connecting users from the Islamic Republic of Iran

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

- Flashproxy (Stanford), websocket
- FTEProxy (Portland St), http via regex
- Stegotorus (SRI/CMU), http
- Skypemorph (Waterloo), Skype video
- uProxy (Google), webrtc
- ScrambleSuit (Karlstad), obfs-based
- Telex (Michigan/Waterloo), traffic divert
MESS WITH ONE OF US.
MESS WITH ALL OF US.

Supporting totalitarian regimes is our business.
Sleep safe Assad, Blue Coat is here.
Auskwärtiges Amt
Werderscher Markt 1
I CAN HAZ FREEDOM?
“Still the King of high secure, low latency Internet Anonymity”

Contenders for the throne:
• None
Snowflake Options

This page enables you to use your web browser as a proxy to help other Internet users in censored places. When you click yes, your browser will act as a censorship circumvention proxy as long as you are viewing a page with the snowflake badge.

For more information on this system click here.

Do you want your browser to act as a proxy?

Yes  No

Snowflake Proxy is ACTIVE

Thank you for contributing to internet freedom!
Arms races

- Censorship arms race is bad
- Surveillance arms race is worse
  - And centralization of the Internet makes it worse still
Step 5: Bob connects to the Alice's rendezvous point and provides her one-time secret.
Welcome to Riseup Black

This is the home of the Riseup "Black" services, our new enhanced security VPN and (soon) En application.

**Important:** To avoid possible issues, you will need to create a new account (this means a new username) for these services. But don’t fear, you will be later able to use your current username if you want.

Log in to change your account settings or create support tickets for Riseup Black services.

Create a new user account for Riseup Black. For greater security, we strongly recommend you create your account via the Bitmask application instead. Remember: to avoid possible issues, you cannot use your current riseup.net username at this stage. But don’t fear, you will be able to do it later.
Onion service properties

• Self authenticated
• End-to-end encrypted
• Built-in NAT punching
• Limit surface area
• No need to “exit” from Tor
1 Million People use Facebook over Tor

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.

This is why in the last two years we built the Facebook onion site and onion-mobile site, helped standardise the "onion" domain name, and implemented Tor connectivity for our Android mobile app by enabling connections through Orbot.
SecureDrop

Today, 30+ organizations use SecureDrop

https://securedrop.org/directory
Salut !

Salut Korben !

cà fonctionne, c'est cool. A qui ai je l'honneur ?

Oui, c'est cool. Je suis un lecteur de ton site, Paul.

enchanté !

j'ai commenté qu'une fois un article sur Mario64 porté sur plateforme x86
OnionShare

Stuff2Share.zip
SHA1 checksum: 594574079686e954e1689f0a06a80774d1913213
File size: 527.5 KiB

Give this URL to the person you're sending the file to:
http://6iyarl3yttnsodcp.onion/rghhlpzcsfm4wcdqoxvjtllu24

Copied URL to clipboard
Tor isn't foolproof

- Opsec mistakes
- Browser metadata fingerprints
- Browser exploits
- Traffic analysis
How can you help?

- Run a relay (or a bridge)
- Teach your friends about Tor, and privacy in general
- Help find -- and fix -- bugs
- Work on open research problems (petsymposium.org)
- donate.torproject.org
Relay operator meetup, today

15:00 today in room H.3244
ooni.torproject.org
World Map

Measurements
- More than 100,000
- More than 10,000
- Less than 10,000

Discoveries
- Confirmed censorship cases
- Vendors identified