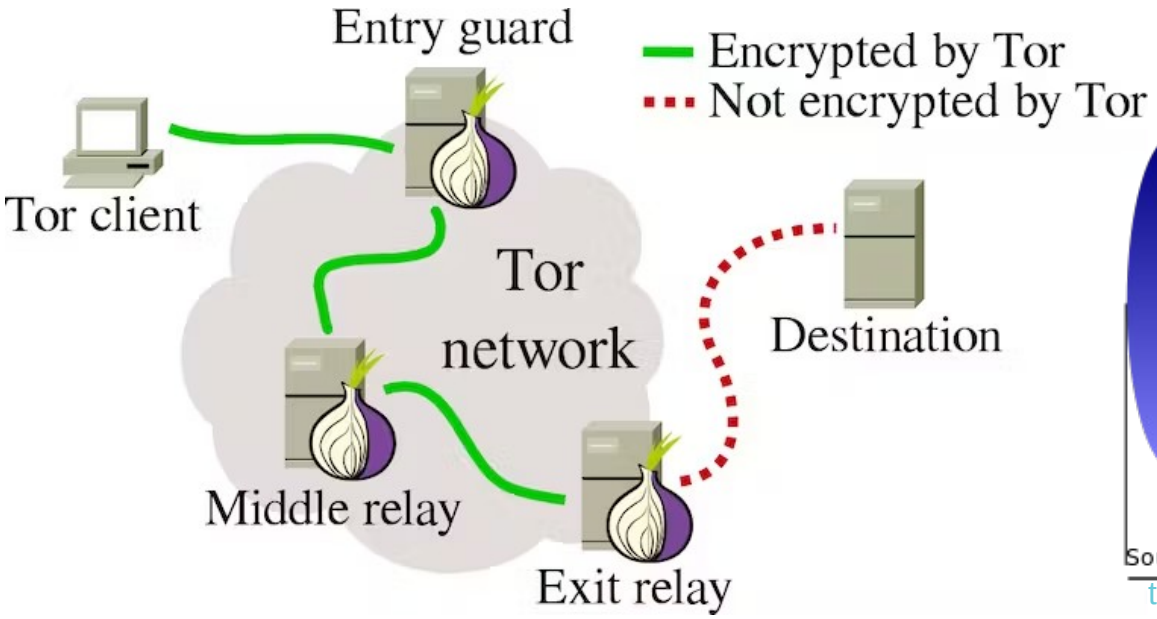
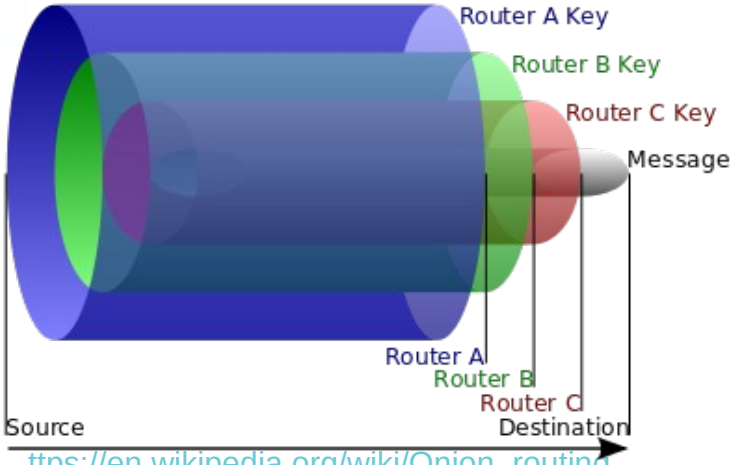
CSE 468 Fall 2023 Tor lecture

jedimaestro@asu.edu

- Some slides I stole
- Some more slides I stole
- Both are from https://community.torproject.org/training/resources/
- See also
  - https://community.torproject.org/onion-services/setup/

Tor in a nutshell





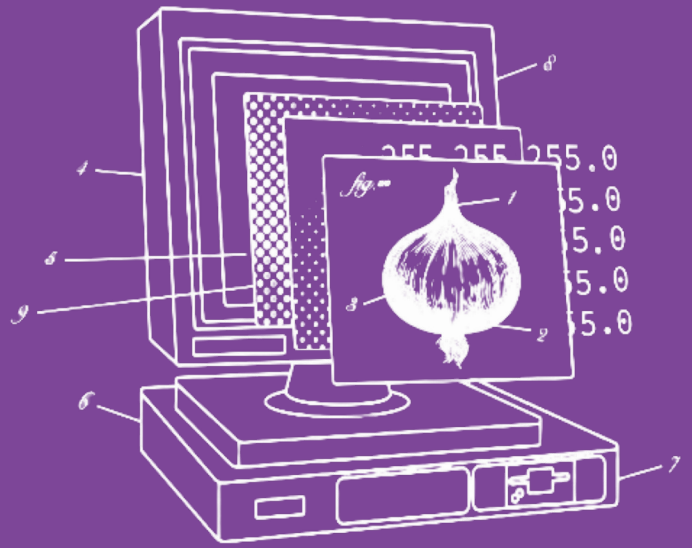
ttps://en.wikipedia.org/wiki/Onion_routing

https://theconversation.com/tor-upgrades-to-make-anonymous-publishing-safer-73641

Why are we learning about Tor?

- Brings together many concepts from the course
  - Encryption, anti-censorship and NIDS evasion, privacy, anonymity, *etc.*
- A basic network security tool that many people use for many different things

Introduction to Onion Services



torproject.org

Before we begin…

- Do you use Tor?
  - If not, why?
  - If yes, do you have questions or concerns?
- What do you know about Onion Services?

Table of contents

1. Introduction to Tor
2. Applications that run on the Tor network
3. Introduction to Onion Services (.onion)
4. When digital evidence leads to prosecution
5. “Deep” or “Dark” Web?
6. Hands-on activities (OnionShare)
7. Tor secure access package and onion support
8. Latest developments

Introduction to Tor

Connecting through **HTTP**

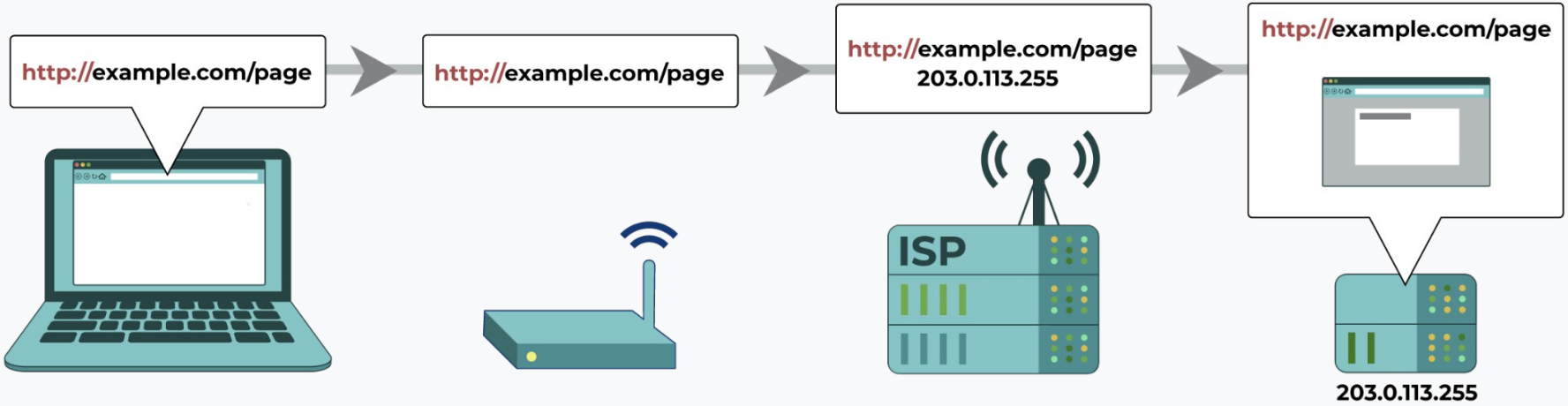


Image source: eff.org

Connecting through **HTTPS**

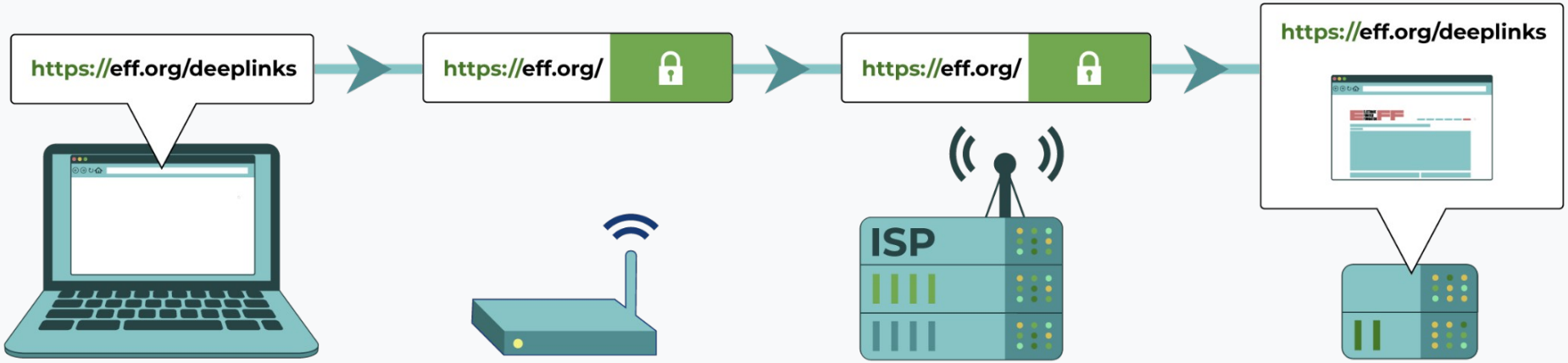


Image source: eff.org

Connecting through VPN

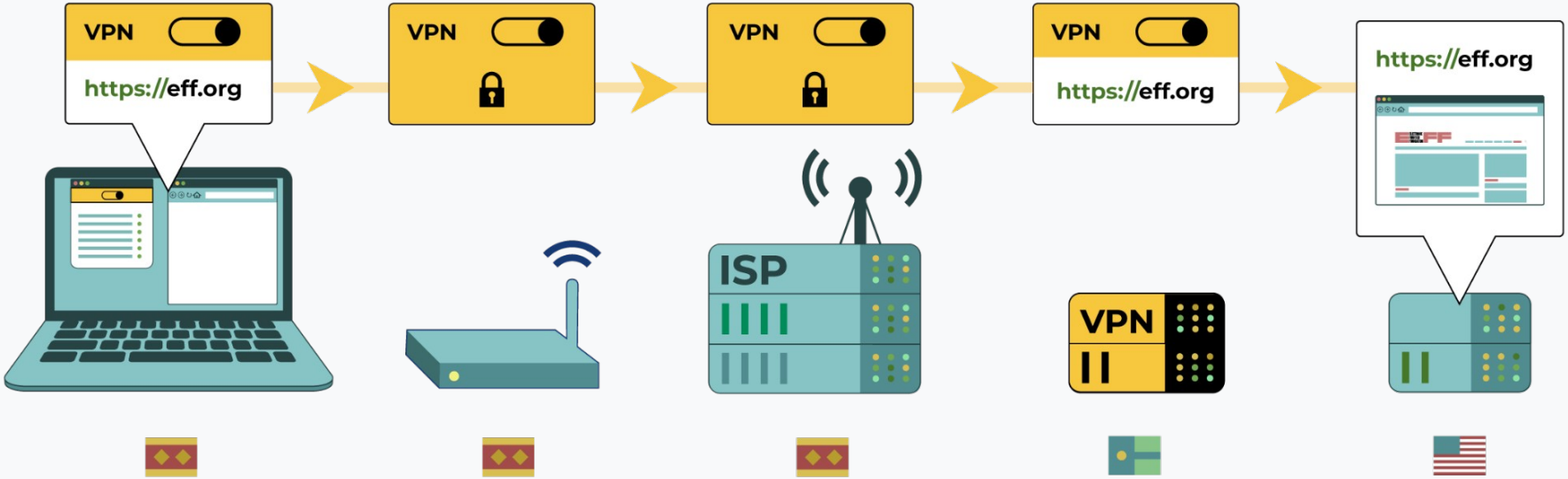


Image source: eff.org

Connecting through Tor

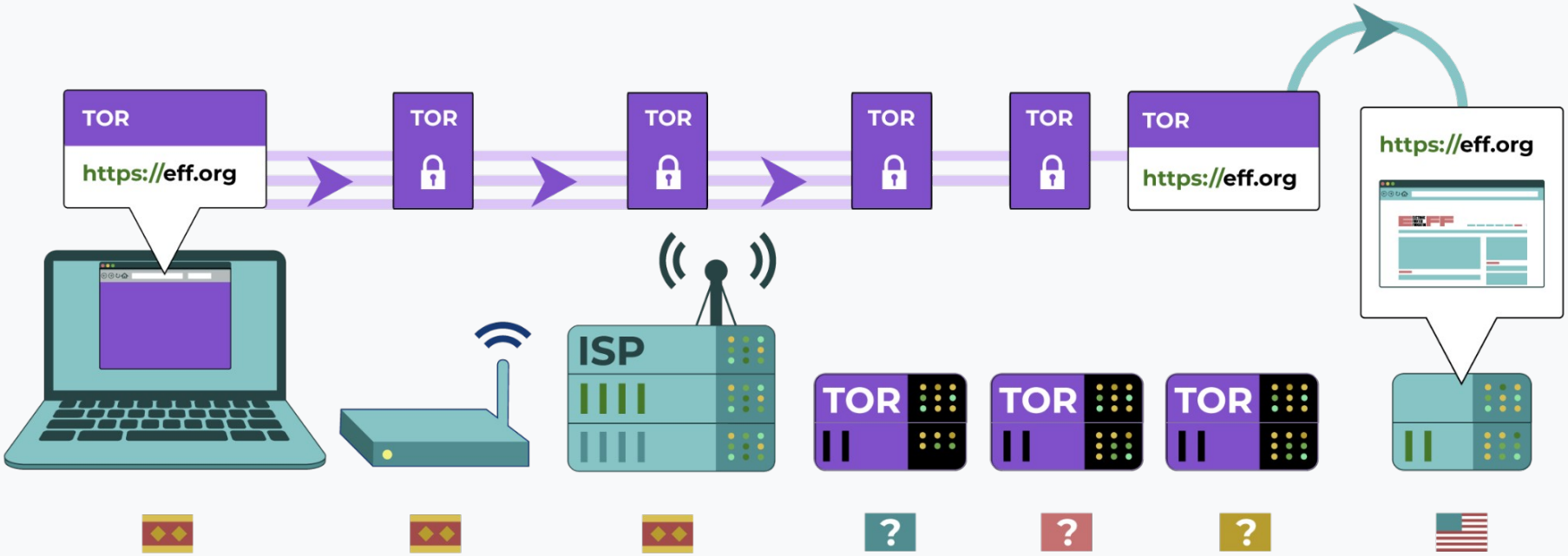


Image source: eff.org

Who can see your activity through **HTTPS** and **what** can they see?

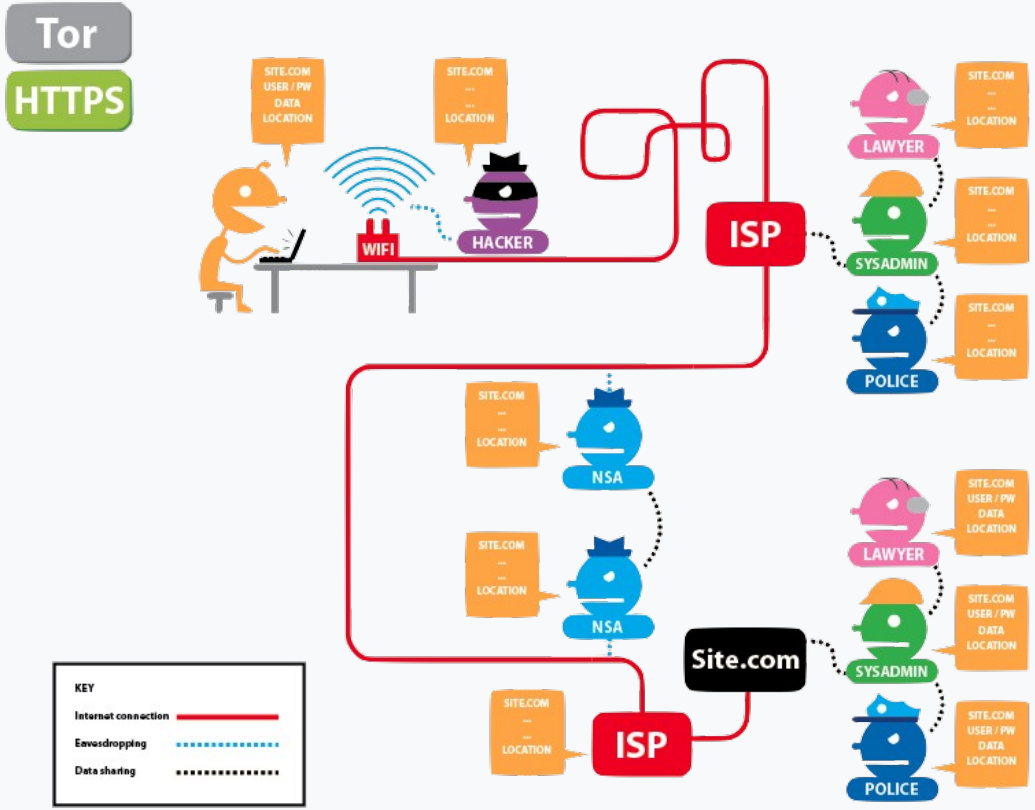


Image source: eff.org

Who can see your activity through **Tor** and **HTTPS** and **what** can they see?

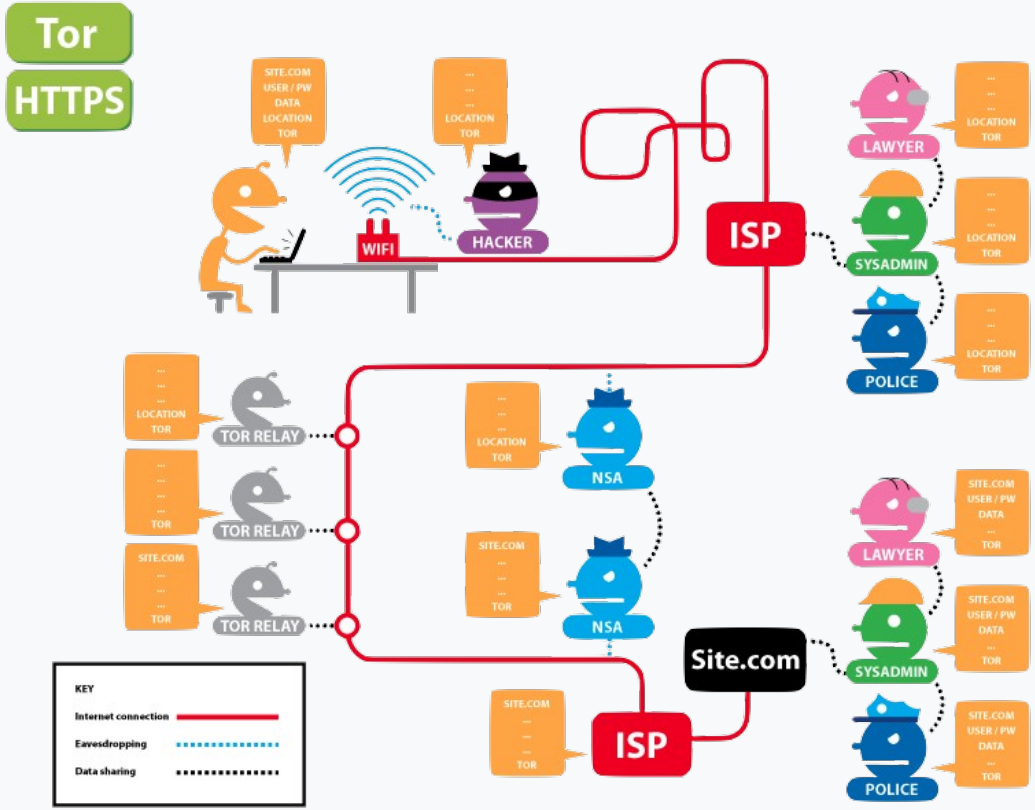
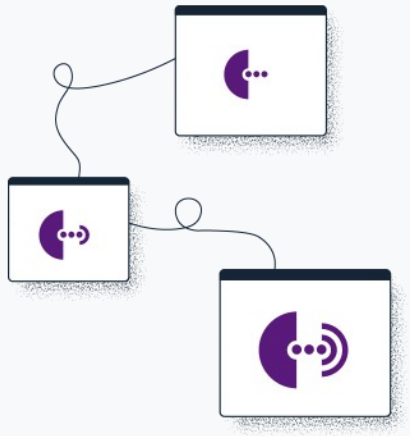


Image source: eff.org

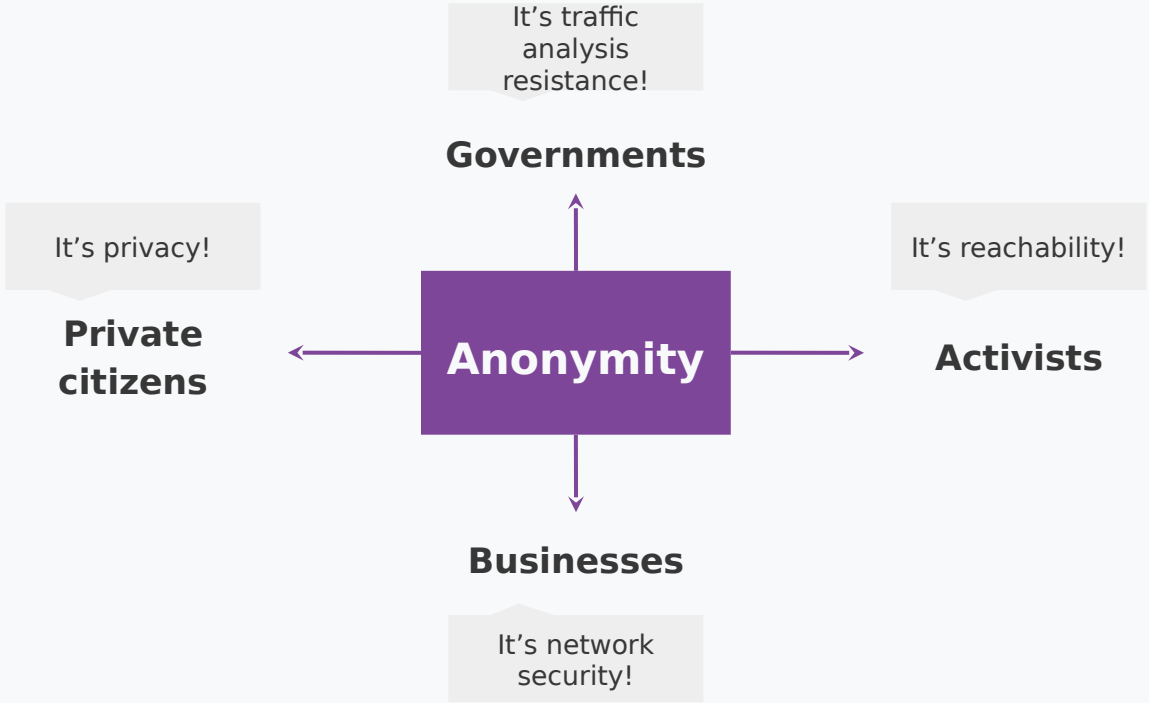
Different ways of defining Tor

- Tor ⇒ free software created at NRL starting 2001/2.
- Tor ⇒ an open network of ~9,500 nodes – anyone can join!
- Tor ⇒ a browser that connects you to the Tor network.
- Tor ⇒ a US non-profit formed in 2006.
- Tor ⇒ a community of volunteers, researchers, developers, trainers, advocates from all over the world.



Fighting the Internet’s original sins

- It’s Tor (not capitalized).
- The goal is to have a way to use the internet with as much privacy as possible:
  a. by routing traffic through multiple nodes; and
  b. by encrypting traffic multiple times – hence the term “onion routing”.
- Tor provides **anonymity**, which mitigates against both surveillance and censorship.


It’s traffic analysis resistance!
Governments
It’s privacy!
It’s reachability!
Private citizens
Anonymity
Activists
Businesses
It’s network security!

We kill people based on metadata

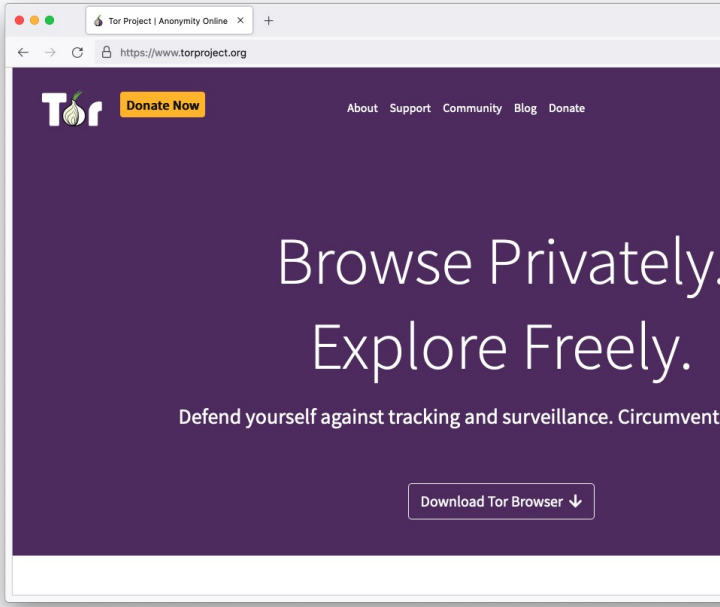
Director of the NSA and CIA
General Michael Hayden

Two sides of the same coin

- Censorship and surveillance go hand-in-hand.
- In order to **block** access to an online service, censors need to **spot** when users want to access said service.
- Anonymity grants protection from surveillance and censorship.

What is Tor Browser?

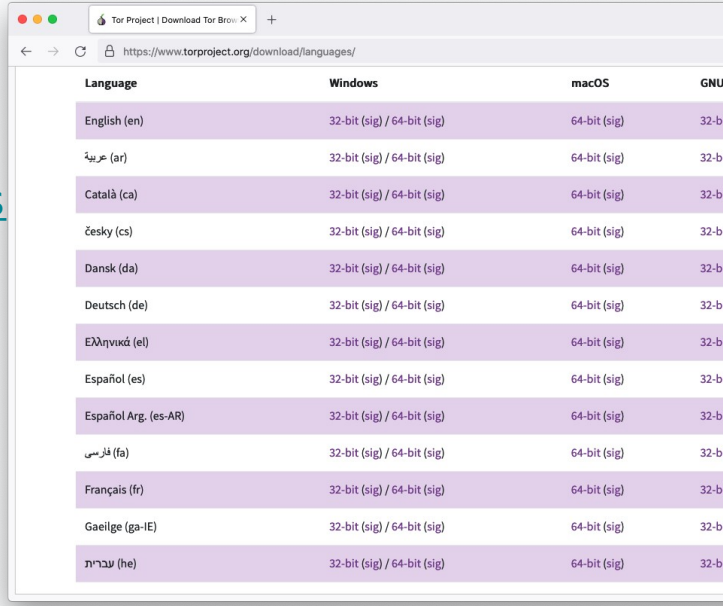
- Just like any other browser (Chrome, Firefox, Safari, Yandex) except it does not expose traffic.
- Traffic is encrypted and bounces through three random volunteer-run nodes called **relays**.
- When using Tor Browser, we don’t know who you are or what you’re visiting.



Multilingual Browser

- Tor Browser is available in **many languages**: https://www.torproject.org/download/languages/

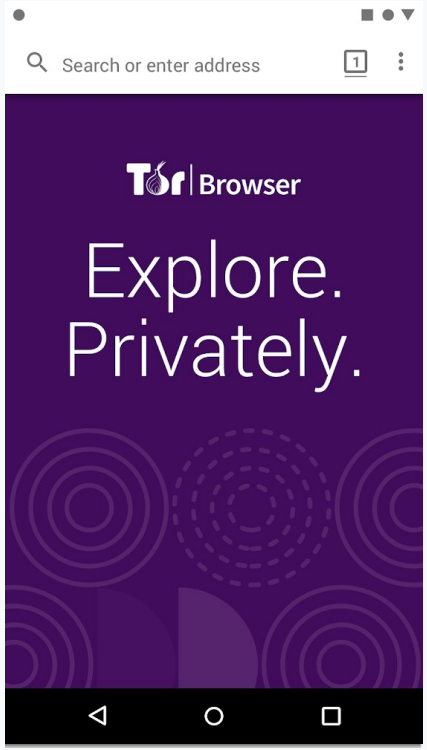
- Tor Browser manual is a user-friendly guide for novice users and is also multilingual: https://tb-manual.torproject.org/



Tor Browser on Android

Developed by the Tor Project

https://www.torproject.org/download/



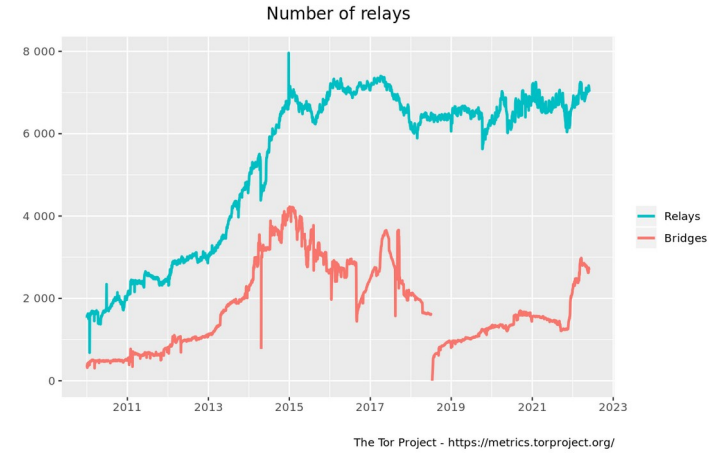
Onion Browser on iOS

Developed by the Guardian Project

https://onionbrowser.com/

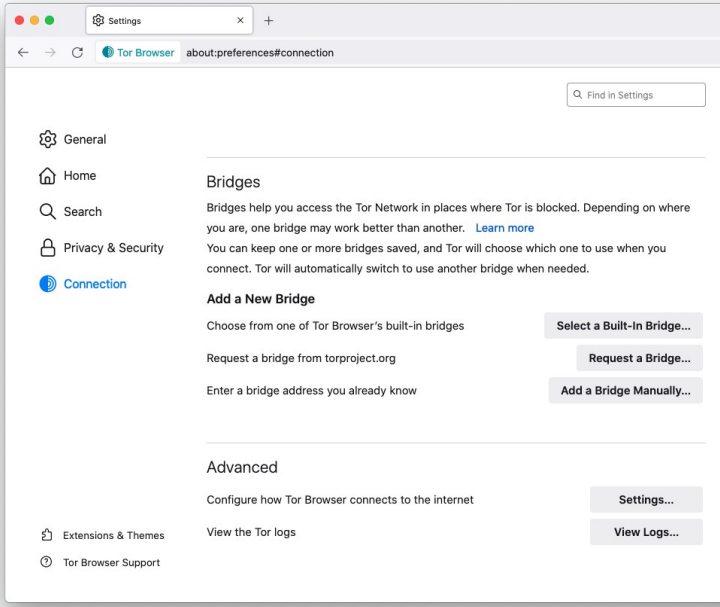
A growing network of relays

- Tor relays and bridges are run by volunteers from around the world, including individuals, NGOs, and companies.
- They form the backbone of the Tor network.
- Today we count: 7000+ relays and 2660+ bridges.



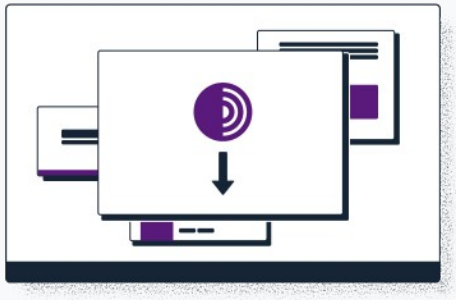
Bypassing censorship of the Tor network

- Direct access to Tor may be blocked by some Internet Service Providers and governments.
- Tor Browser includes circumvention tools for getting around these blocks called bridges.
- Bridges are relays that are private and harder to block: https://bridges.torproject.org/



Bypassing censorship of torproject.org

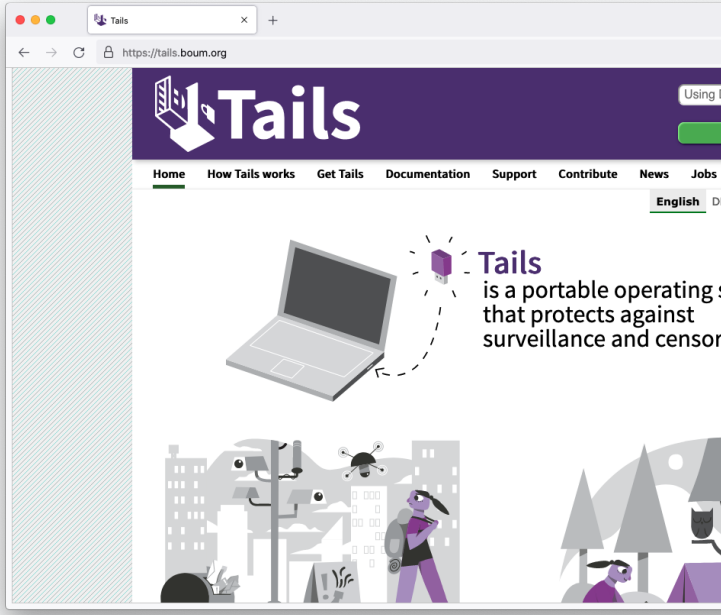
- Tor Project website could be blocked on your network.
- Multiple circumvention methods:
  - Mirror websites: https://tor.eff.org/ and https://tor.calyxinstitute.org/
  - Requesting Tor Browser bundle via email: gettor@torproject.org
  - Requesting Tor Browser bundle via Telegram: https://t.me/gettor_bot



Applications that run on the Tor network

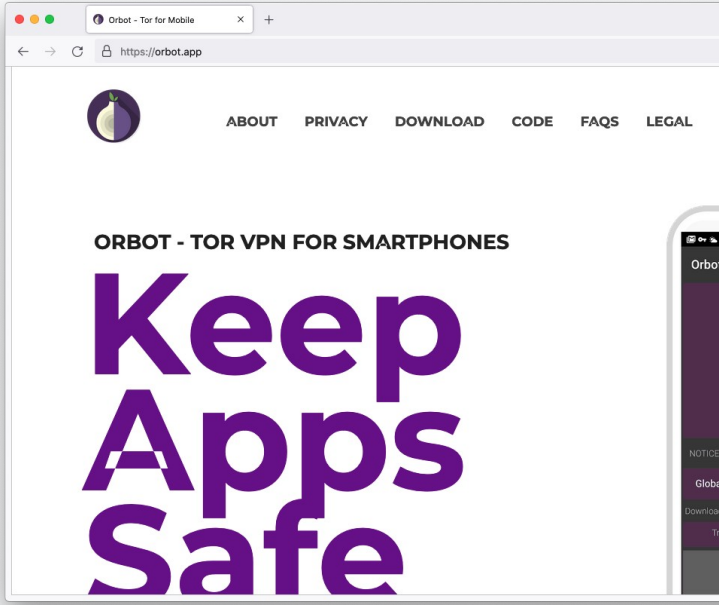
Operating system

- Tails is an operating system (like Windows and macOS) that can be run straight from a USB.
- Tails ⇒ The Amnesic Incognito Live System.
- Tails isolates the connection of all applications through Tor and comes with a set of secure applications.
- An independent project: https://tails.boum.org/



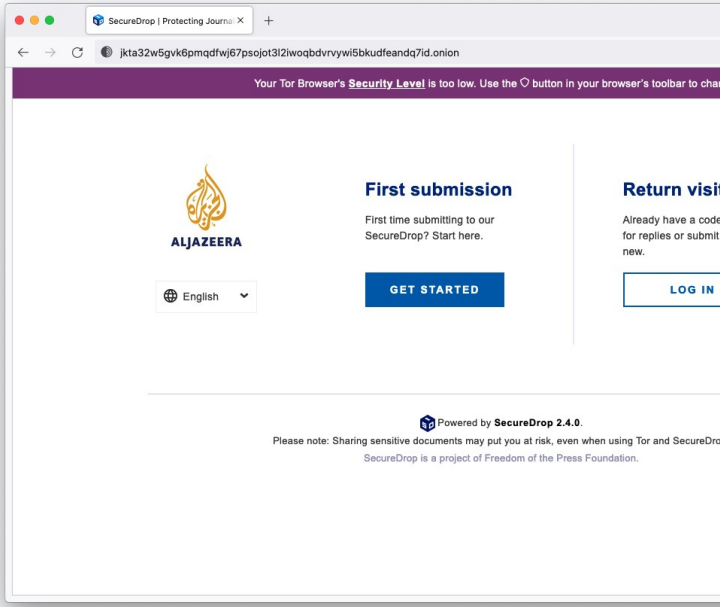
System-wide VPN

- Orbot routes mobile apps' traffic through Tor, you can select specifically which apps to run through Tor.
- Orbot is available on iOS and Android.
- Developed and maintained by the Guardian Project: https://orbot.app/



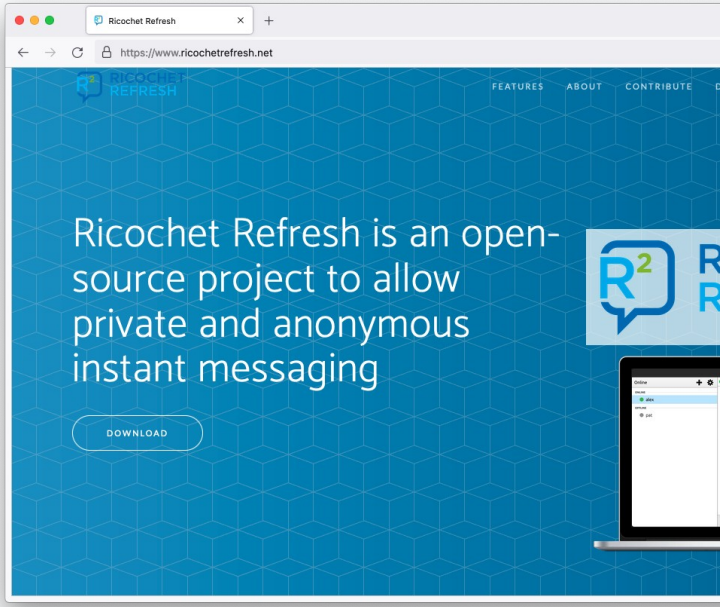
Secure whistleblowing

- SecureDrop and GlobaLeaks are tools for whistleblowers to communicate securely with journalists.
- Newsrooms around the world have set up their own whistleblowing platforms to receive leaks securely.



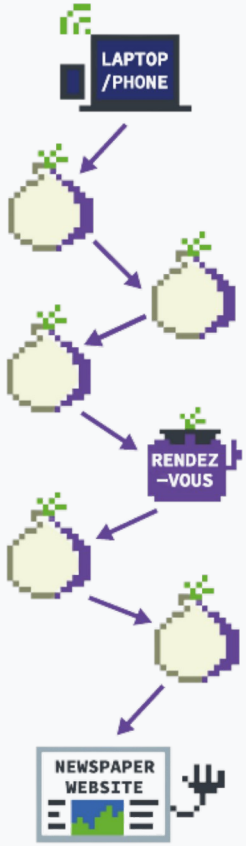
Anonymous peer-to-peer messaging

- Ricochet Refresh is an instant messenger that routes all messages through Tor.
- Nobody knows who you're talking to, or what you're talking about.
- Supported by Blueprint for Free Speech: https://www.blueprintforfreespeech.net/

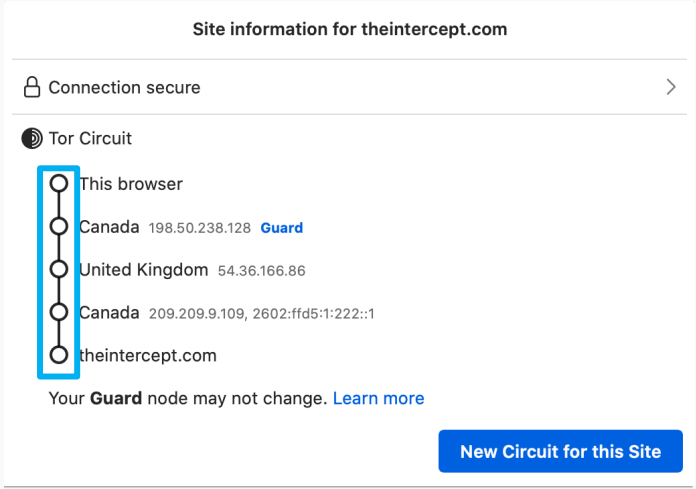


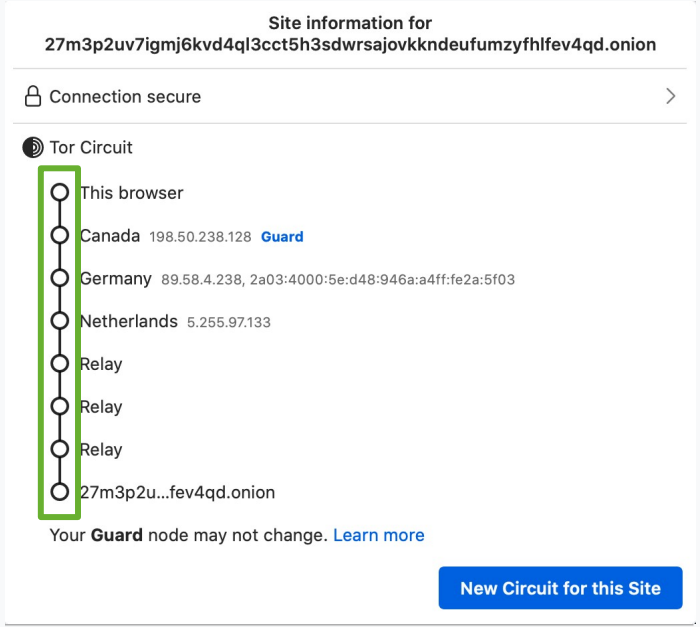
Introduction to Onion Services (.onion)

- Onion Services are online services that are only available through the Tor network.
- An Onion Service connects to a rendez-vous node/relay inside the Tor network; and the user wanting to connect to it does the same.
- As a user, you never leave the Tor network when visiting an Onion Service.
- Onion Services provide end-to-end encryption: both visitor and website use Tor (without HTTPS).



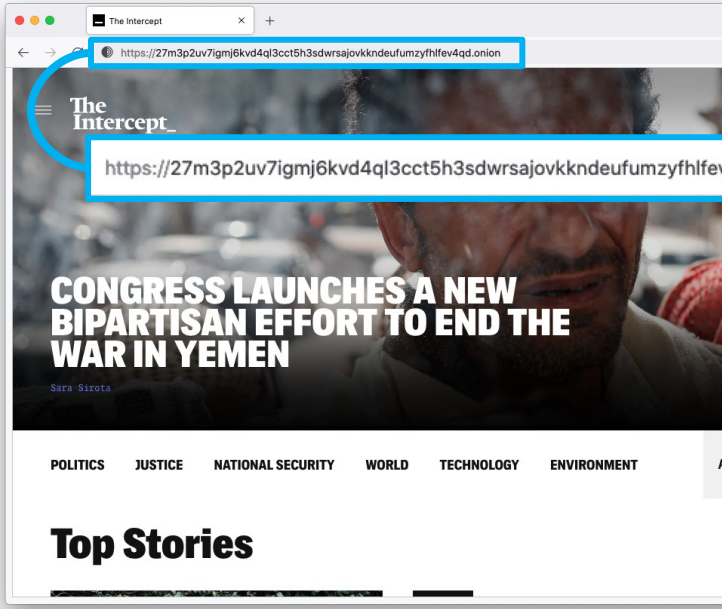
Visiting the Intercept's site on Tor Browser vs. visiting the Intercept's onion service





.onion addresses

- Just like any other website, you need to know the address of an onion service in order to reach it.
- The .onion address is automatically generated, so there is no need to purchase a domain.
- An onion address is a string of 56 random letters and numbers followed by ".onion".



Censorship resistance

- Both location and IP address of an Onion Service are hidden, making it difficult to censor or identify who runs the service. Used to be called “hidden services”.
- Tor exit nodes can block websites (rare), Onion Services never exit the Tor network.
- It’s the **most censorship-resistant technology** available out there as long as the Tor network is reachable.

Metadata obfuscation and elimination

- When you use the Tor network to browse the web you are not sending any information by default of who you are or where you are connecting from.
- The Onion Services use the Tor network to eliminate information about where they are situated.
- Using them **eliminates all metadata** that may be associated with the service otherwise.

Maximum harm reduction

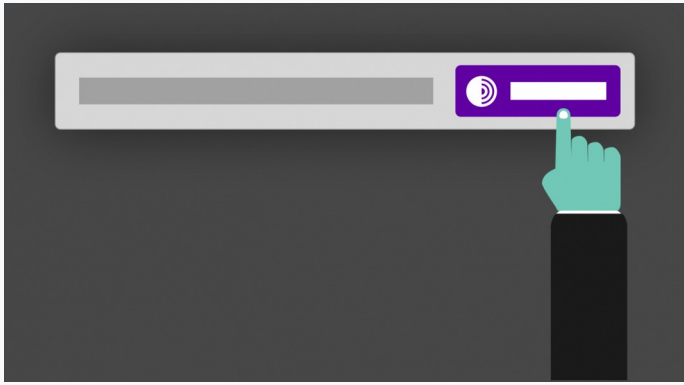
- Leaving the Tor network still puts users at risk of censorship and other security and privacy risks, Onion Services almost **diminish these risks**.
- Even if websites are under DDOS, Onion Services could still give access to content of the site (in the case that the onion service itself is not under DDOS!).

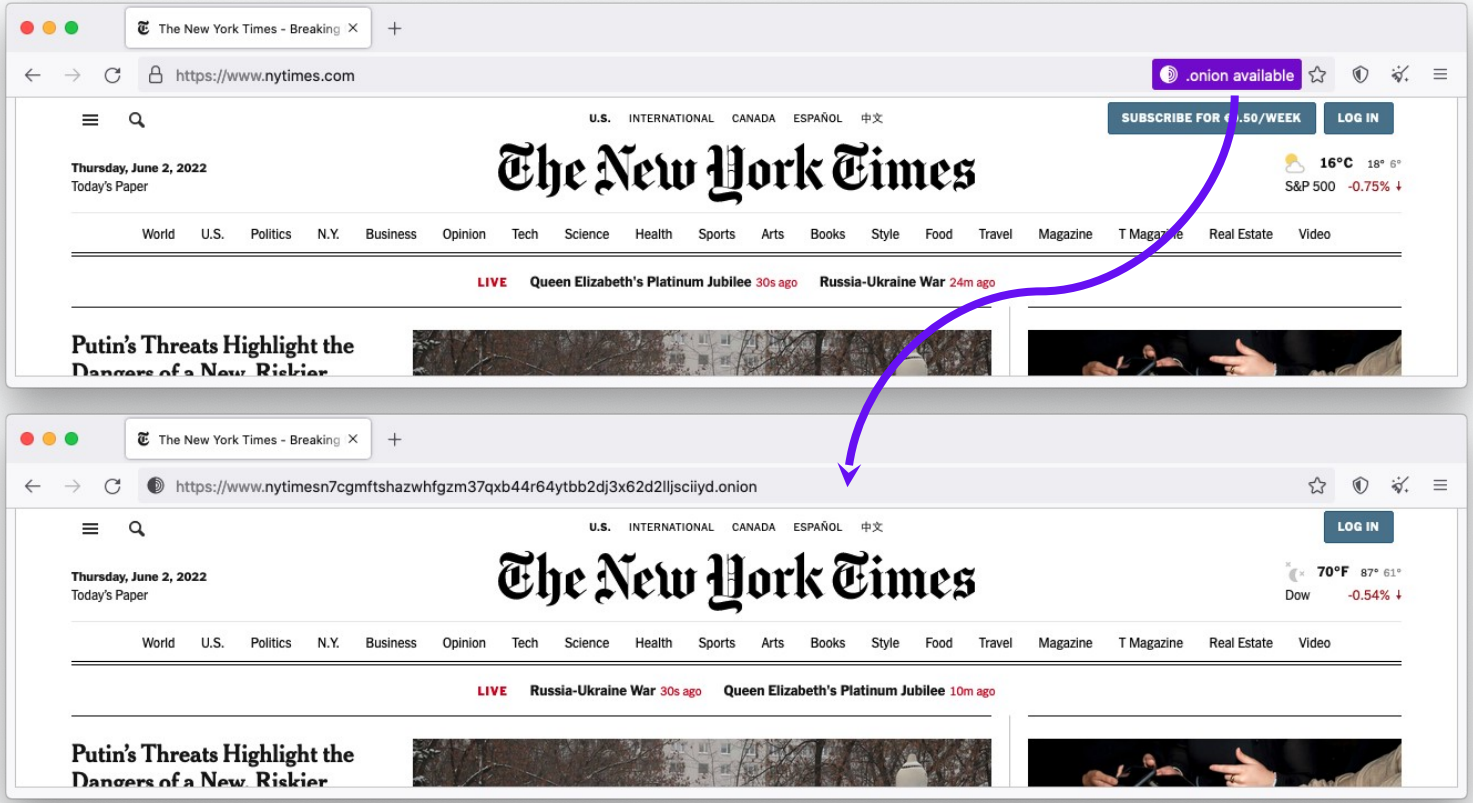
Decentralizing the web

- To deploy an Onion Service, you don't need a static or dedicated IP address nor need to purchase a domain and submit it for approval.
- For smaller websites like blogs, there’s no need for expensive hardware.
- Deployment is easy: you don't need to forward ports or configure your modem.

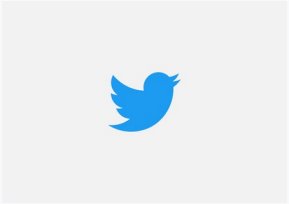
Onion-Location

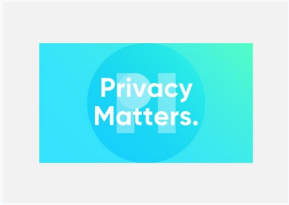
- **Onion-Location** is an HTTP header that websites can use to advertise their onion counterpart.
- If the website that you're visiting has an onion service, a purple suggestion pill will prompt at the URL bar saying ".onion available".
- When you click it, the website will be reloaded and redirected to its onion counterpart.




The New York Times - Breaking
https://www.nytimes.com
.onion available
U.S. INTERNATIONAL CANADA ESPAÑOL 中文
SUBSCRIBE FOR
LOG IN
Thursday, June 2, 2022
Today's Paper
The New York Times
16°C 18° 6°
S&P 500 -0.75%
World U.S. Politics N.Y. Business Opinion Tech Science Health Sports Arts Books Style Food Travel Magazine T Magazine Real Estate Video
LIVE Queen Elizabeth's Platinum Jubilee 30s ago Russia-Ukraine War 24m ago
Putin's Threats Highlight the
The New York Times - Breaking
https://www.nytimesn7cgmftshazwhfgzm37qxb44r64ytbb2dj3x62d2lljsciiyd.onion
U.S. INTERNATIONAL CANADA ESPAÑOL 中文
LOG IN
Thursday, June 2, 2022
Today's Paper
The New York Times
70°F 87° 61°
Dow -0.54%
World U.S. Politics N.Y. Business Opinion Tech Science Health Sports Arts Books Style Food Travel Magazine T Magazine Real Estate Video
LIVE Russia-Ukraine War 30s ago Queen Elizabeth's Platinum Jubilee 10m ago
Putin's Threats Highlight the

Popular Onion Services





Benefits of Onion Services

1. Censorship resistance as long as the user has access to Tor.
2. End-to-end encryption between user and website.
3. Contributing to the decentralization of the web.
4. Tor network sustainability.
5. Protection of sources, whistleblowers, and journalists.
6. Opportunity to educate users about privacy by design.
7. Metadata obfuscation and elimination.

Comparison

	Regular Website	Website Over Tor	Onion Service
Censorship Resistance:	**Poor** Website can easily be censored	**Good** Censorship still possible via exit nodes	**Very good** Accessible as long as Tor is reachable, address not censorable
Privacy Safeguards:	**Very poor** Minimal safeguards: HTTPS, no tracking, hosting jurisdiction, etc.	**Good** Data correlation is not an eliminated risk	**Very good** End-to-end encryption for user and service, anonymity for both
Metadata Elimination:	**Poor** Data about online activity recorded by websites and entities passing traffic	**Good** Data about online activity can be recorded by website if user logs in and identifies themselves	**Very good** Metadata logging eliminated on both ends, but website can record data if user logs in

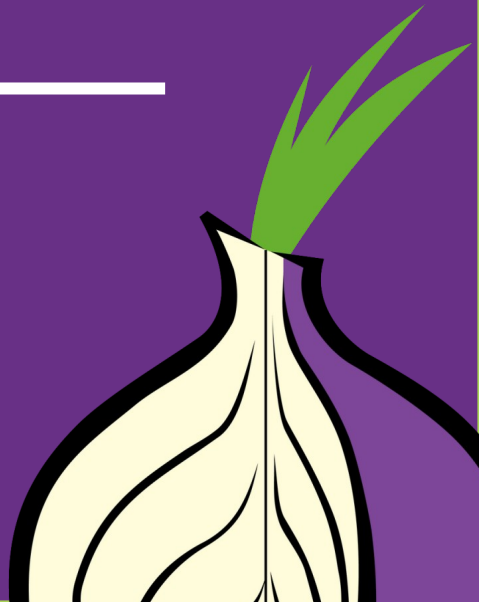
Why Onion Services matter

- Many cases documented where digital evidence has led to prosecution of dissidents, activists, people seeking abortion, etc.
- Ensuring people access your site via your Onion Service increases their digital and physical safety.

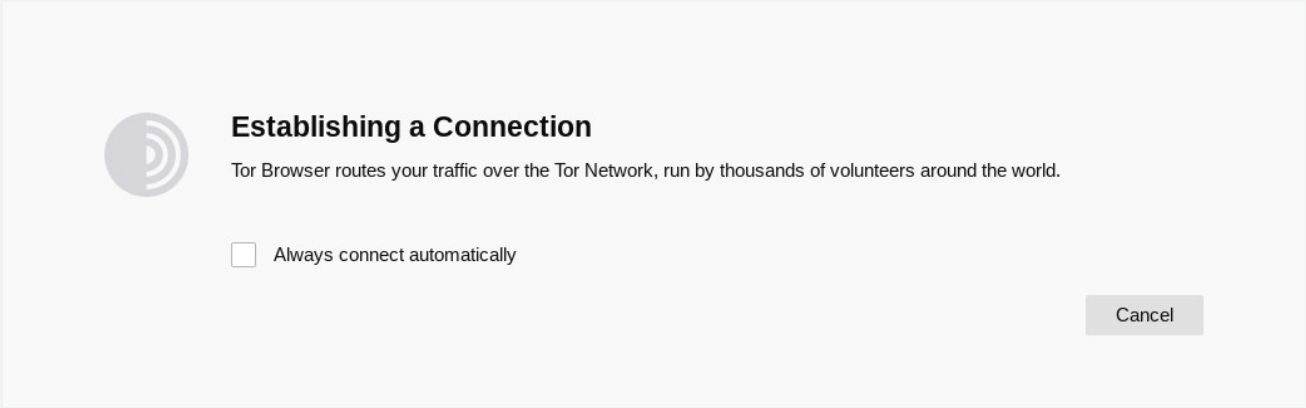
---snip---

- The above slides continue, see original if you’re interested, now plagiarizing some slides about evading censorship...

What do you do when Tor is blocked?



I downloaded Tor Browser, but it won’t connect



If this screen takes a long time and does not connect, you may need a bridge or pluggable transport

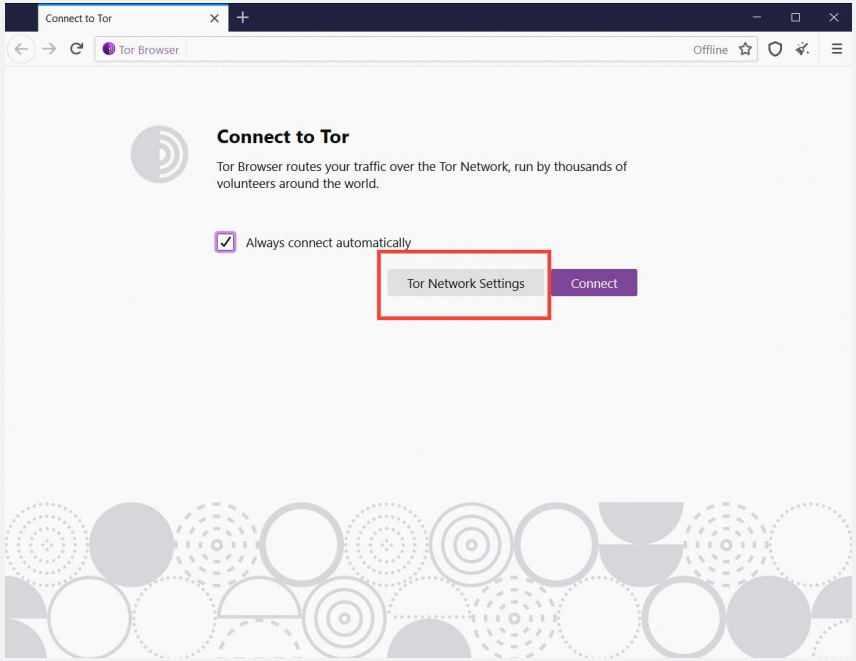
When torproject.org is blocked

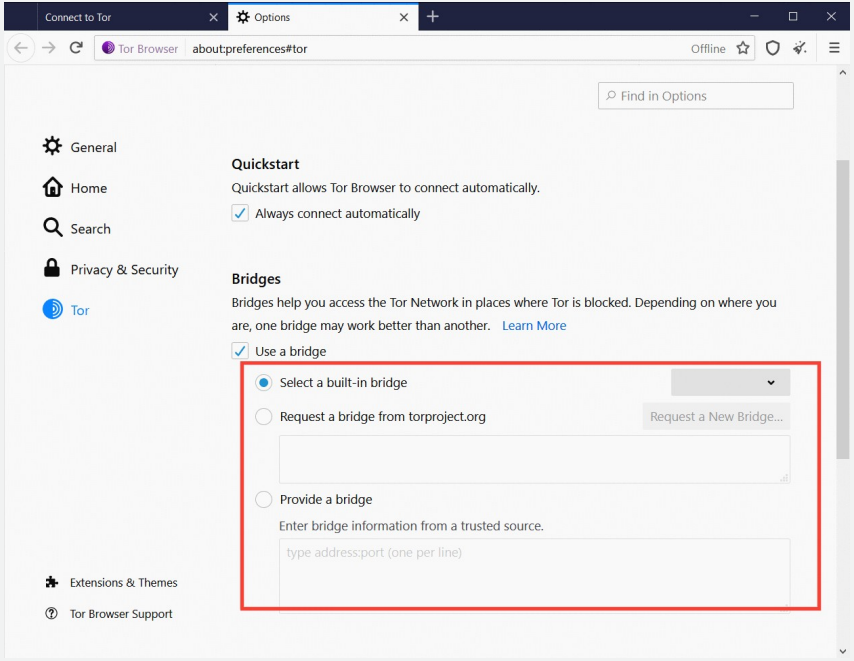
- **Mirrors**
  - https://tor.eff.org/
  - http://tor.calyxinstitute.org/ (if https is blocked)
- **GetTor email**: gettor@torproject.org
  - Contact from a Gmail or Riseup account
- **Flash drive with Tor** on it from someone you trust
- Get the EXE, DMG, tar.xz, don’t copy the installed folder
- Downloading Tor Browser from a non-official source is dangerous!

Bridges and pluggable transports

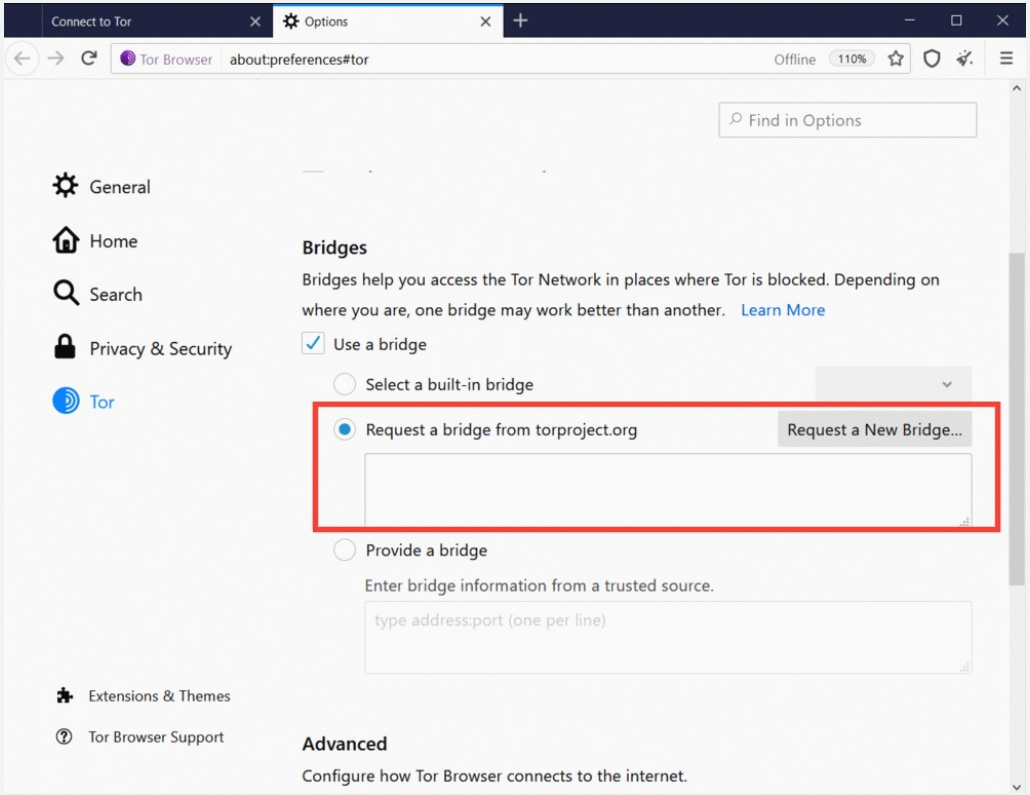
- Bridges are relays that are not listed publicly
- Get bridges directly from Tor Browser (moat)
- Or from the website https://bridges.torproject.org or send an email to bridges@torproject.org from a Gmail, or Riseup.net account
- Or get a bridge address from a trusted person
- Pluggable transports can be used like bridges to disguise Tor traffic (also called “built-in bridges”)

Bridges and pluggable transports

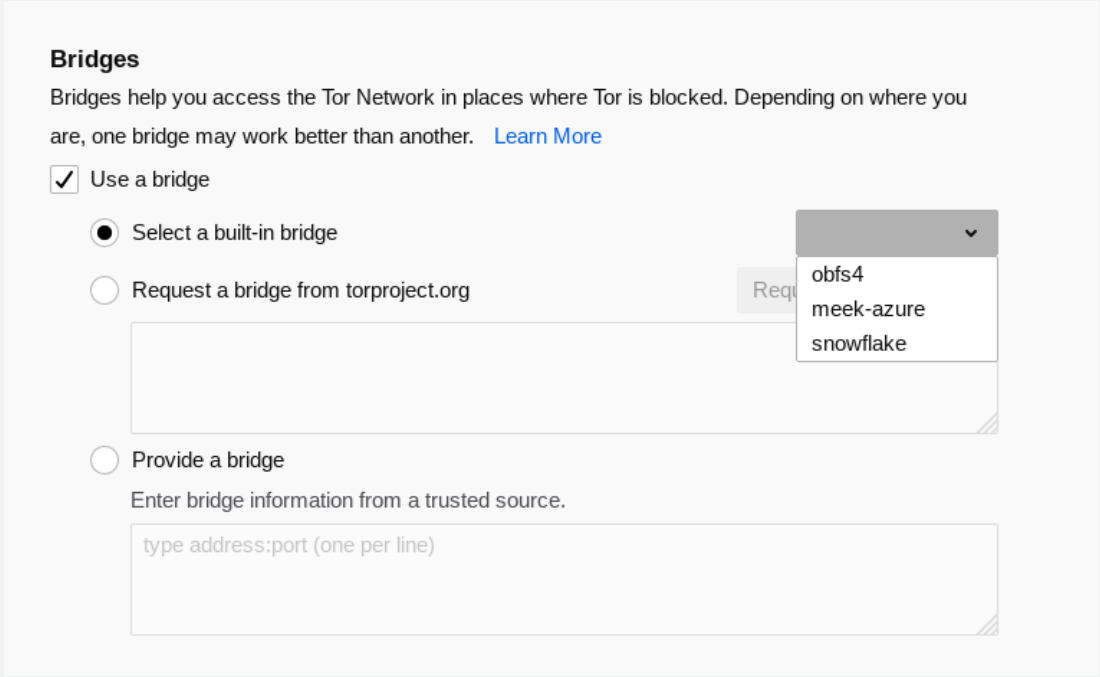




Request a bridge



Or select a built-in bridge



Pluggable transports

- **obfs4**: makes Tor traffic look random; works in many situations including China (if not, try meek).
- **meek-azure**: makes it look like Microsoft traffic; works in China.
- **snowflake**: proxies traffic through temporary proxies using WebRTC (under development). https://snowflake.torproject.org

obfs4 = ScrambleSuit, basically

- https://arxiv.org/pdf/1305.3199.pdf

ScrambleSuit: A Polymorph Network Protocol to Circumvent Censorship

Philipp Winter
Karlstad University

Tobias Pulls
Karlstad University

Juergen Fuss
Upper Austria University of Applied Sciences

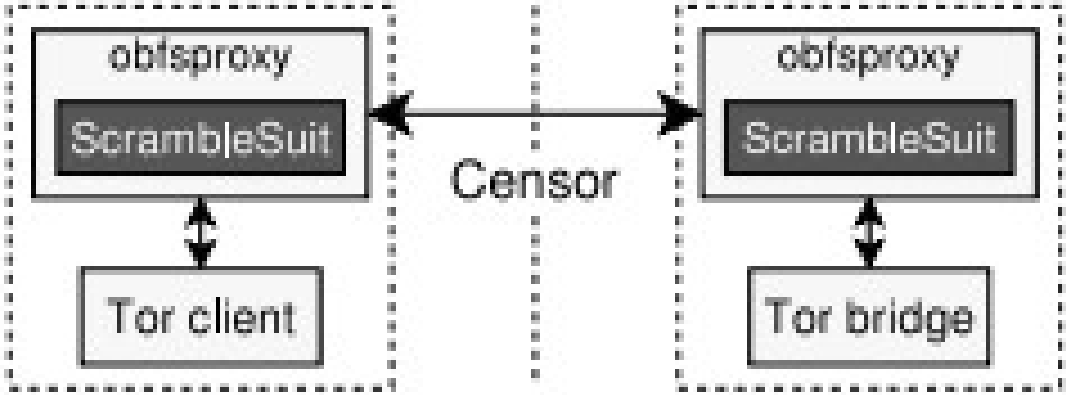


Figure 2: ScrambleSuit is a module for obfsproxy which provides a SOCKS interface for local applications. The traffic between two obfsproxy instances is disguised by ScrambleSuit.

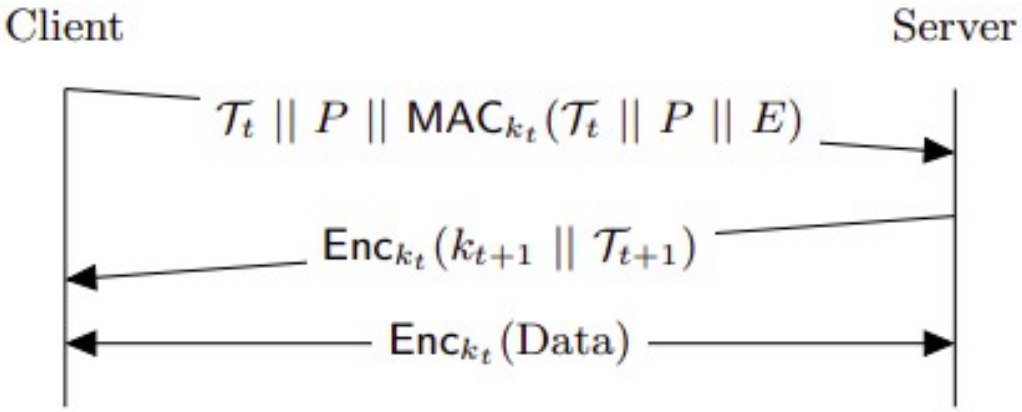
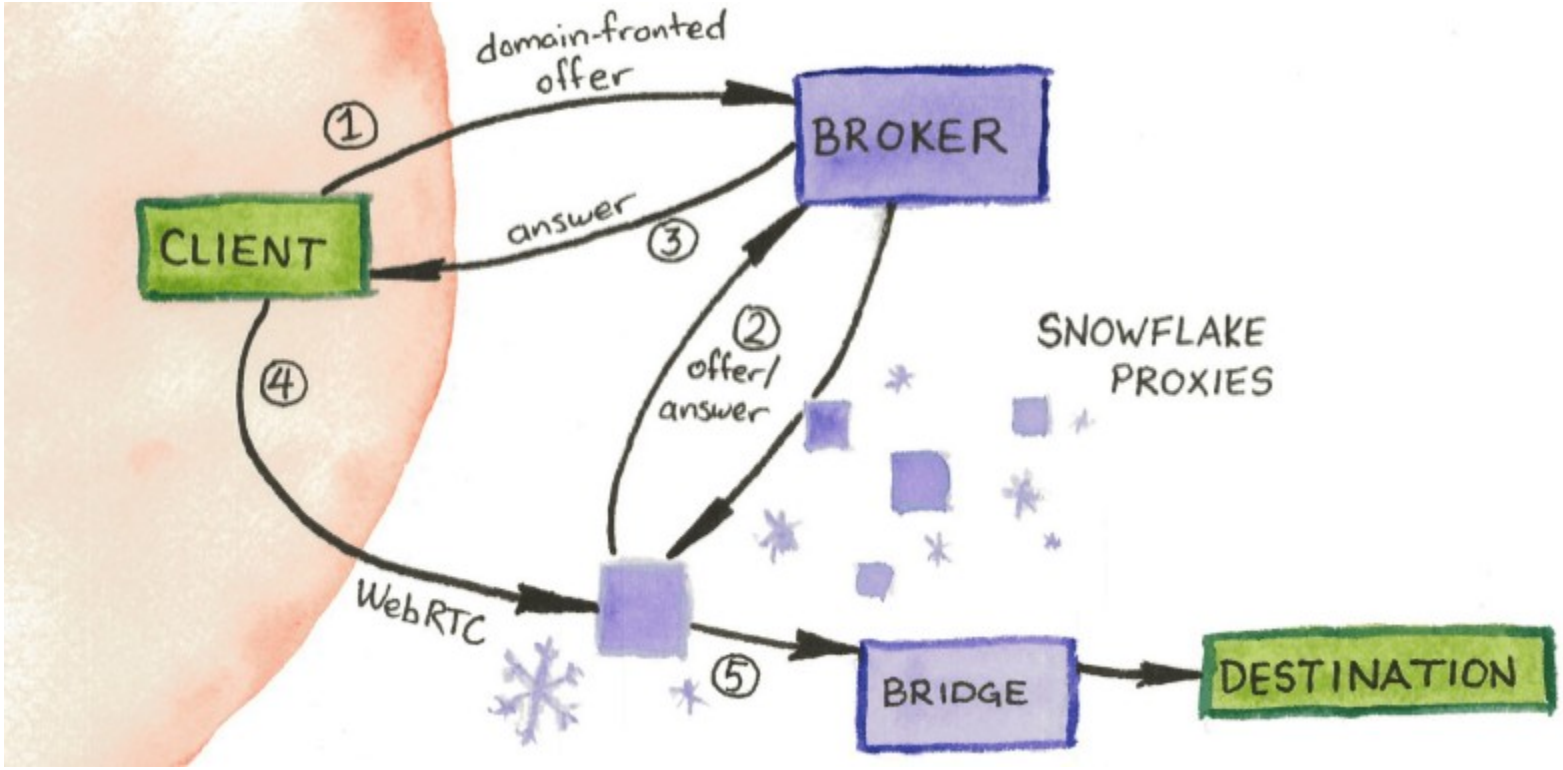


Figure 4: The client redeems a valid session ticket $\mathcal{T}_t$ containing the master key k_t. The server responds by issuing a new ticket $\mathcal{T}_{t+1}$ for future use. Both parties then exchange application data.

meek

- “Domain fronting”
- Use a Content Distribution Network the censor won’t block
  - Costs money
  - Censors have a business relationship with CDNs

https://snowflake.torproject.org/



Payload By encrypting all ScrambleSuit traffic, we eliminate all payload fingerprints such as Tor's TLS cipher list [12].

Packet length distribution Among other things, we seek to get rid of Tor's characteristic 586-byte packets [16, 36]. We do so by morphing Tor's packet length distribution to a randomly chosen distribution.

Inter arrival times Similar to the packet length obfuscation, we camouflage the inter arrival times by employing small and random sleep intervals before writing data on the wire.

OONI

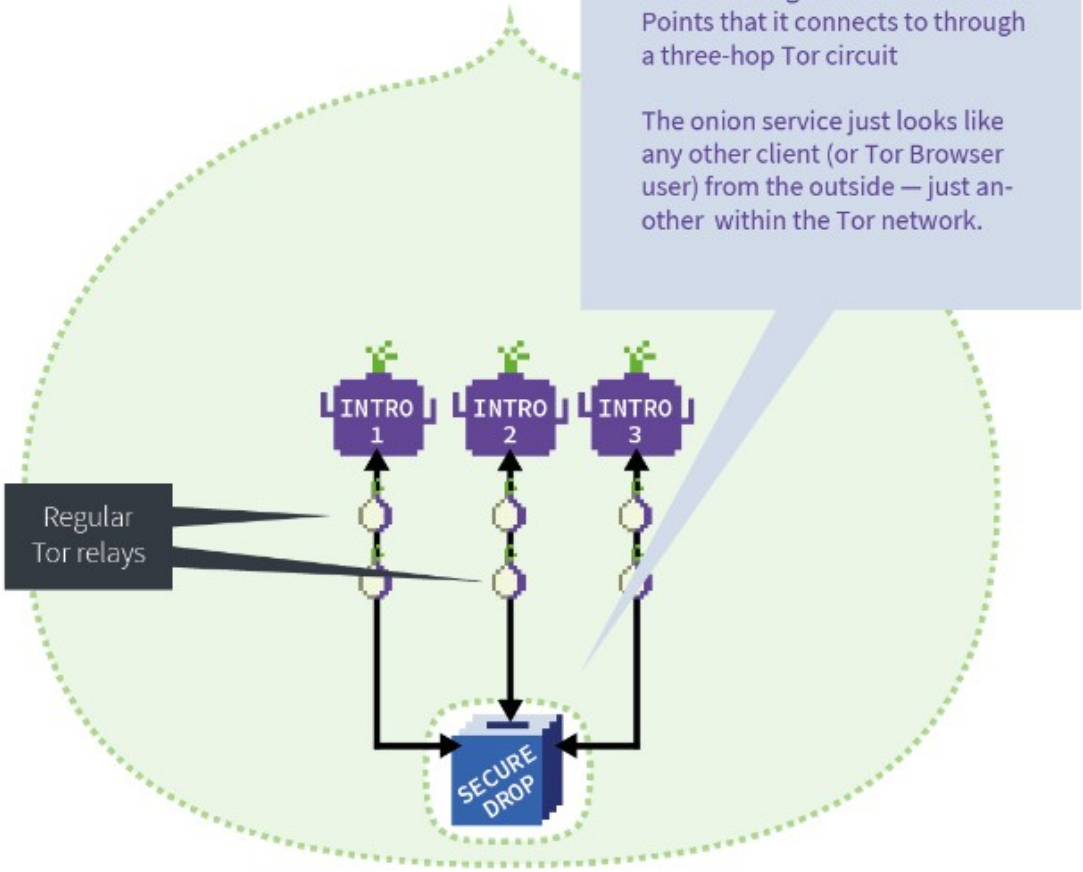
- Open Observatory of Network Interference: https://ooni.torproject.org
- Country-level reports of specific censorship tools in use on certain websites
- View their reports: https://explorer.ooni.org/
- Or use your own OONI Probe to test websites: available in App Store and Google Play.

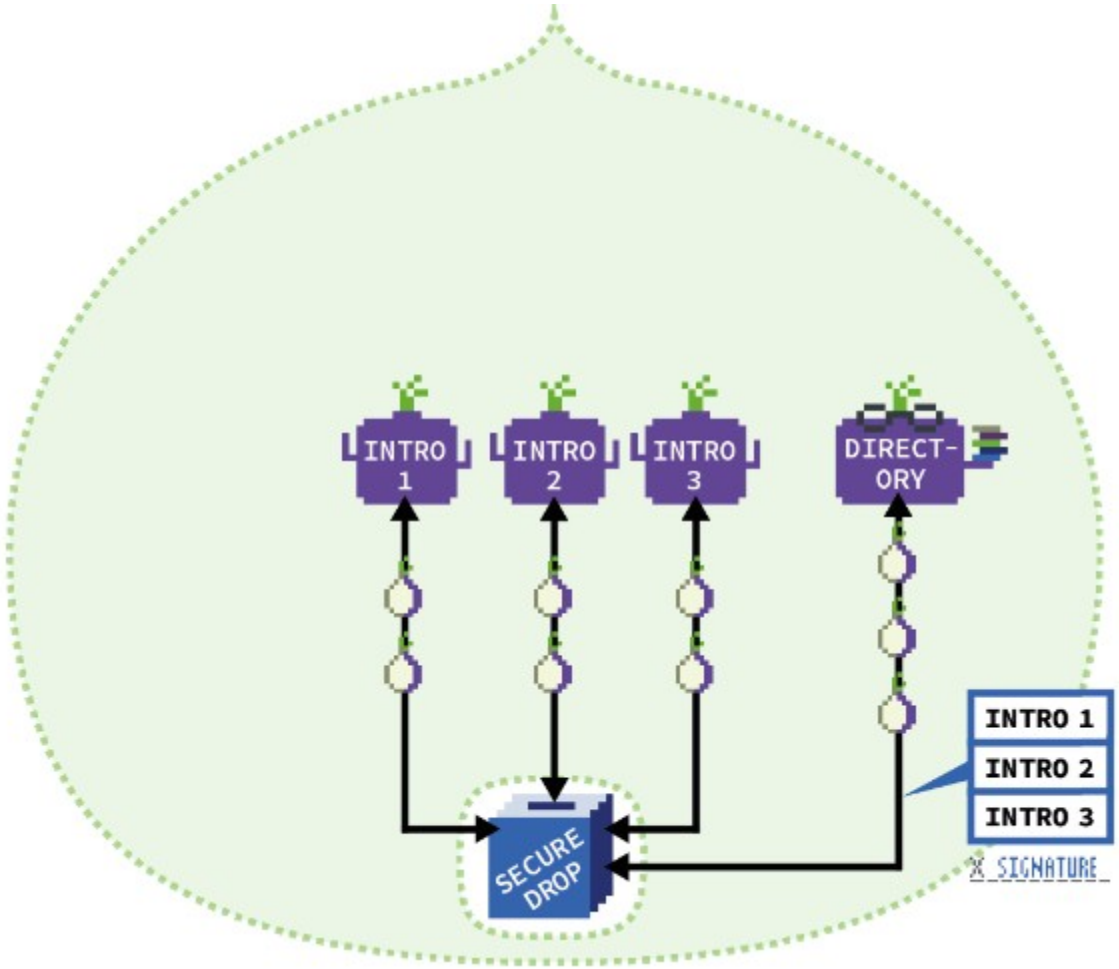
Now some images plagiarized from…

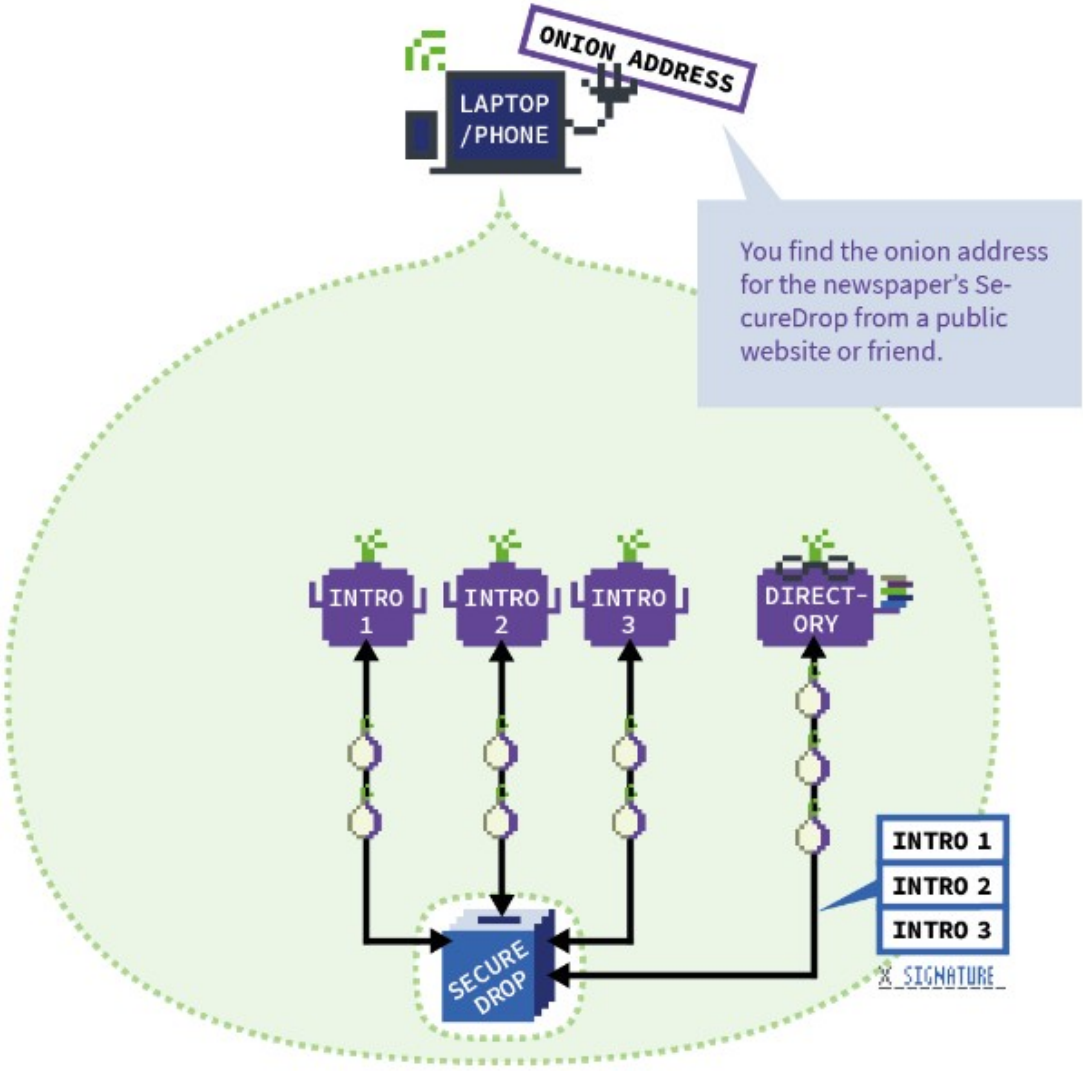
https://community.torproject.org/onion-services/overview/

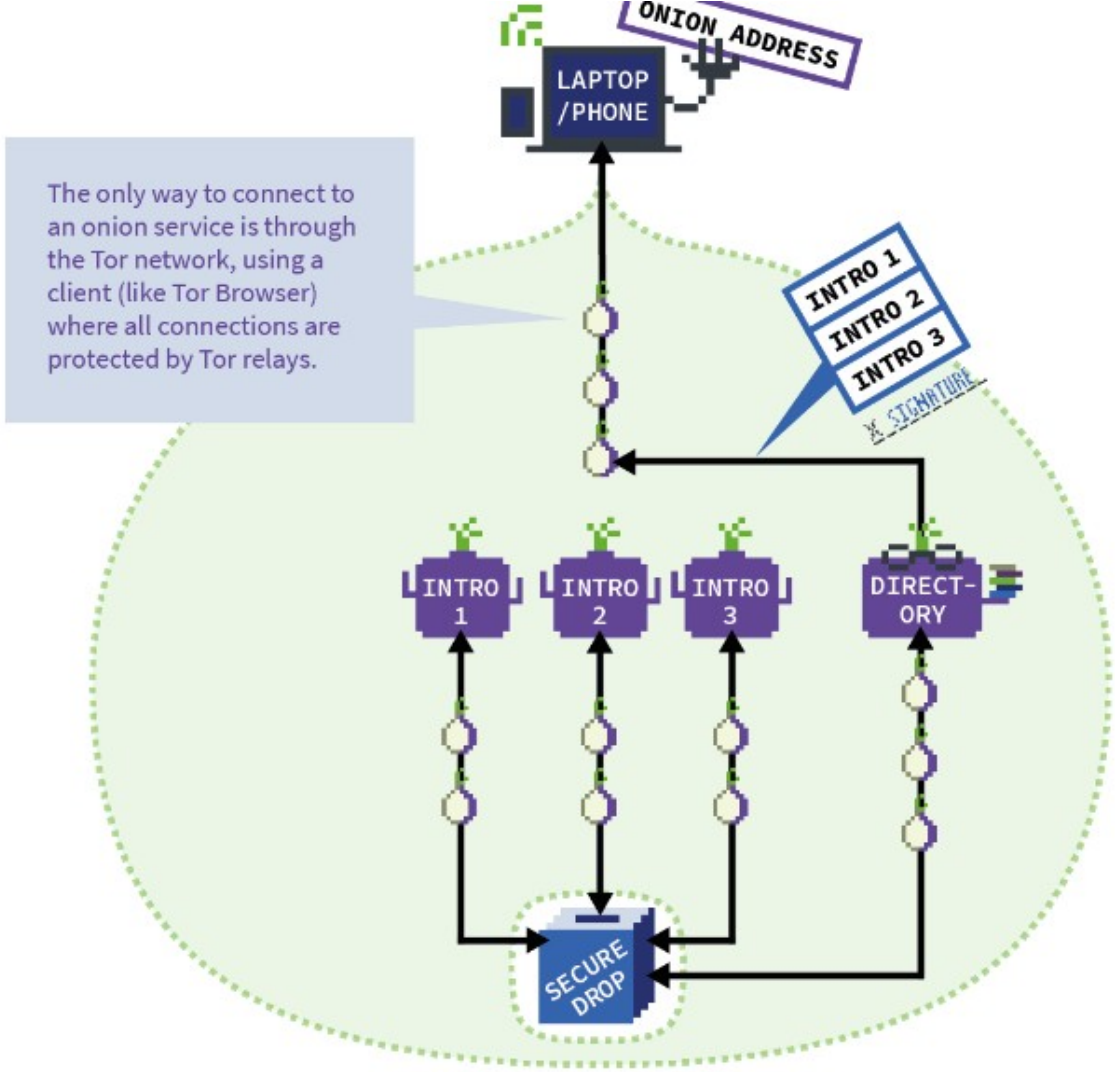
The onion service (SecureDrop) hides and protects itself behind the Tor network by only allowing access through three Introduction Points that it connects to through a three-hop Tor circuit

The onion service just looks like any other client (or Tor Browser user) from the outside — just another within the Tor network.

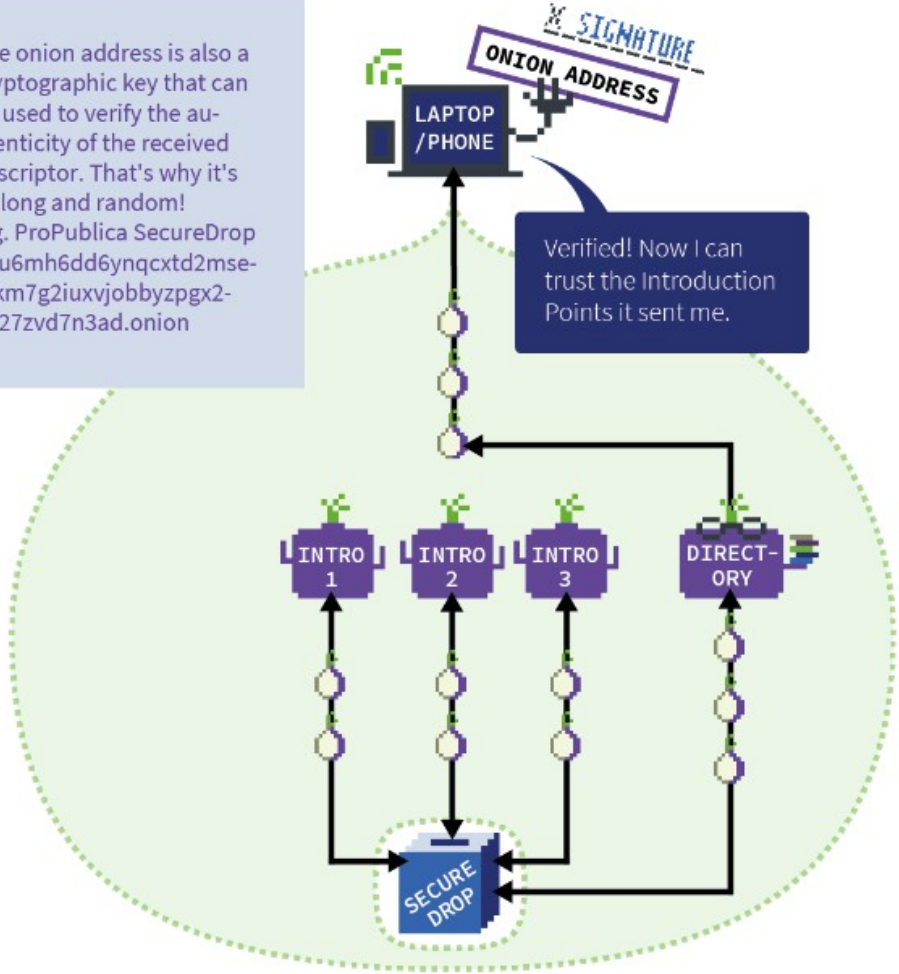


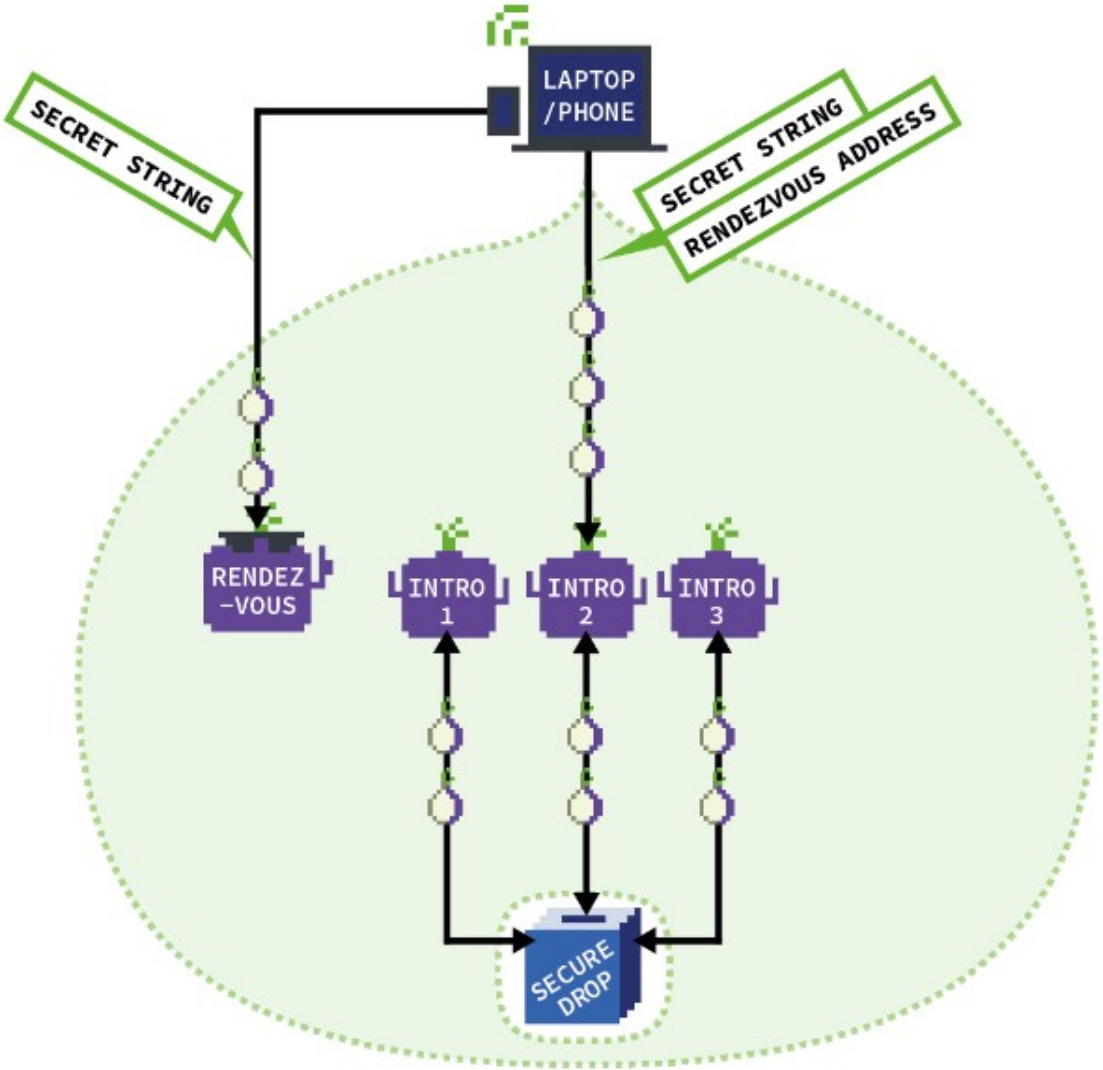

INTRO 1
INTRO 2
INTRO 3
DIRECT-ORY
SECURE DROP
INTRO 1
INTRO 2
INTRO 3
X SIGNATURE

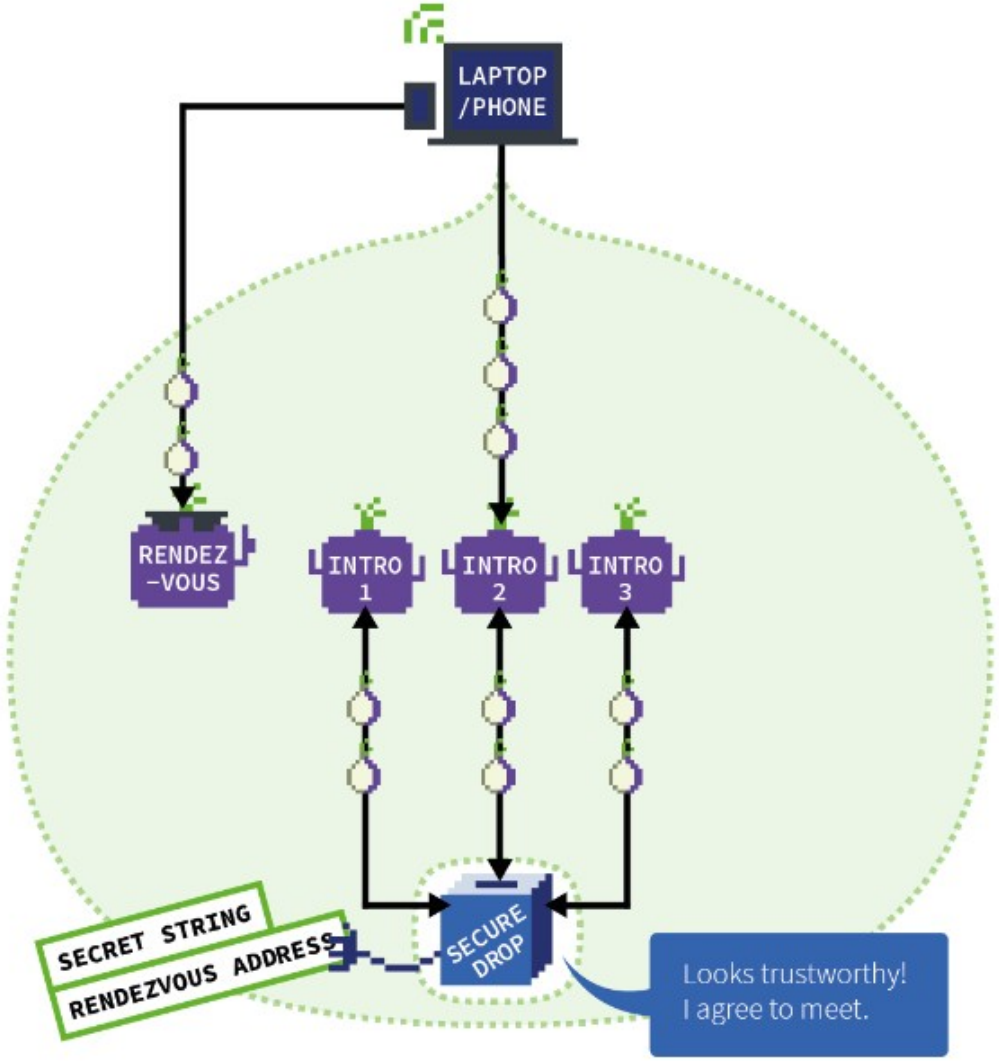

ONION ADDRESS
LAPTOP /PHONE
You find the onion address for the newspaper's SecureDrop from a public website or friend.
INTRO 1
INTRO 2
INTRO 3
DIRECT-ORY
INTRO 1
INTRO 2
INTRO 3
SIGNATURE
SECURE DROP

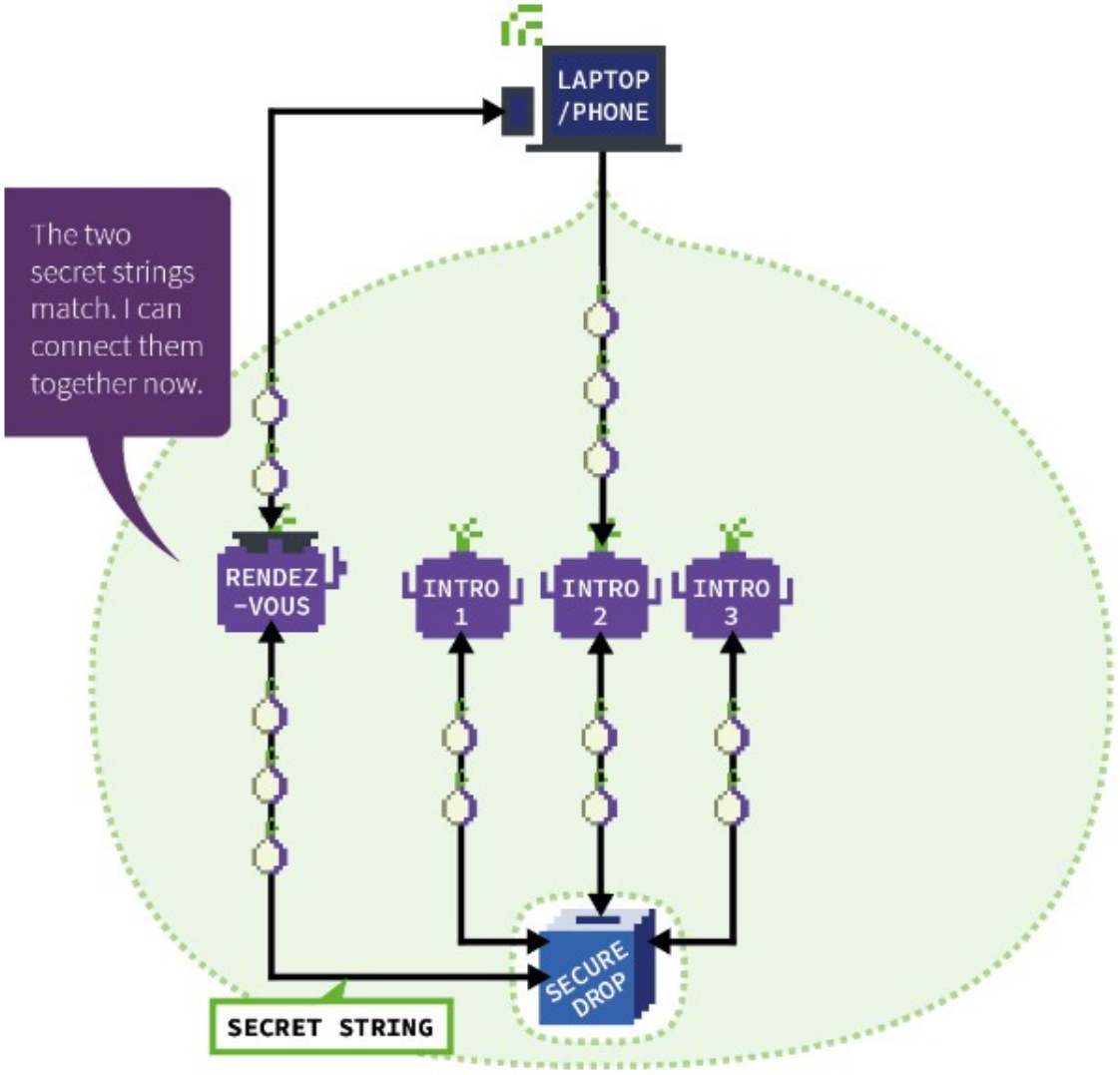

ONION ADDRESS
LAPTOP /PHONE
The only way to connect to an onion service is through the Tor network, using a client (like Tor Browser) where all connections are protected by Tor relays.
INTRO 1
INTRO 2
INTRO 3
SIGNATURE
INTRO 1
INTRO 2
INTRO 3
DIRECT-ORY
SECURE DROP

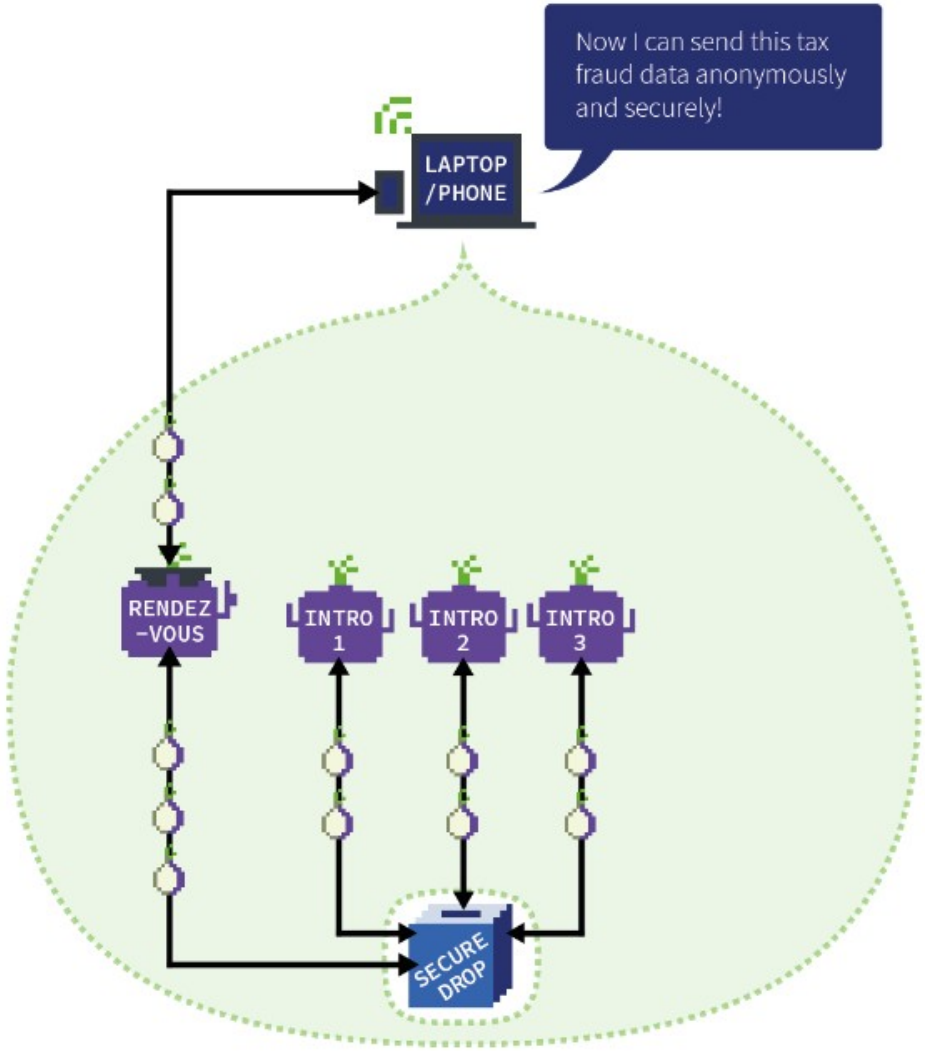
The onion address is also a cryptographic key that can be used to verify the authenticity of the received descriptor. That's why it's so long and random!
E.g. ProPublica SecureDrop
lvtu6mh6dd6ynqcxtd2mse-qfkm7g2iuxvjobbyzpgx2-jt427zvd7n3ad.onion




LAPTOP
/PHONE
SECRET STRING
SECRET STRING
RENDEZVOUS ADDRESS
RENDEZ
-VOUS
INTRO
1
INTRO
2
INTRO
3
SECURE
DROP


LAPTOP
/PHONE
RENDEZ
-VOUS
INTRO
1
INTRO
2
INTRO
3
SECRET STRING
RENDEZVOUS ADDRESS
SECURE
DROP
Looks trustworthy!
I agree to meet.


LAPTOP
/PHONE
The two secret strings match. I can connect them together now.
RENDEZ
-VOUS
INTRO
1
INTRO
2
INTRO
3
SECURE
DROP
SECRET STRING


Now I can send this tax fraud data anonymously and securely!
LAPTOP /PHONE
RENDEZ -VOUS
INTRO 1
INTRO 2
INTRO 3
SECURE DROP