Introduction to Tor & Onion Services

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. Tor ecosystem of tools
3. Introduction to Onion Services
4. “Deep/Dark” Web?
5. Hands-on activities
6. Latest developments

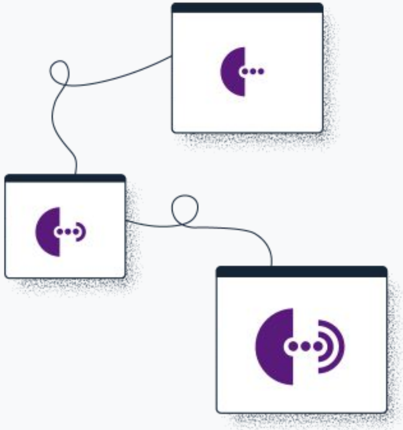
Introduction to Tor

What is Tor?

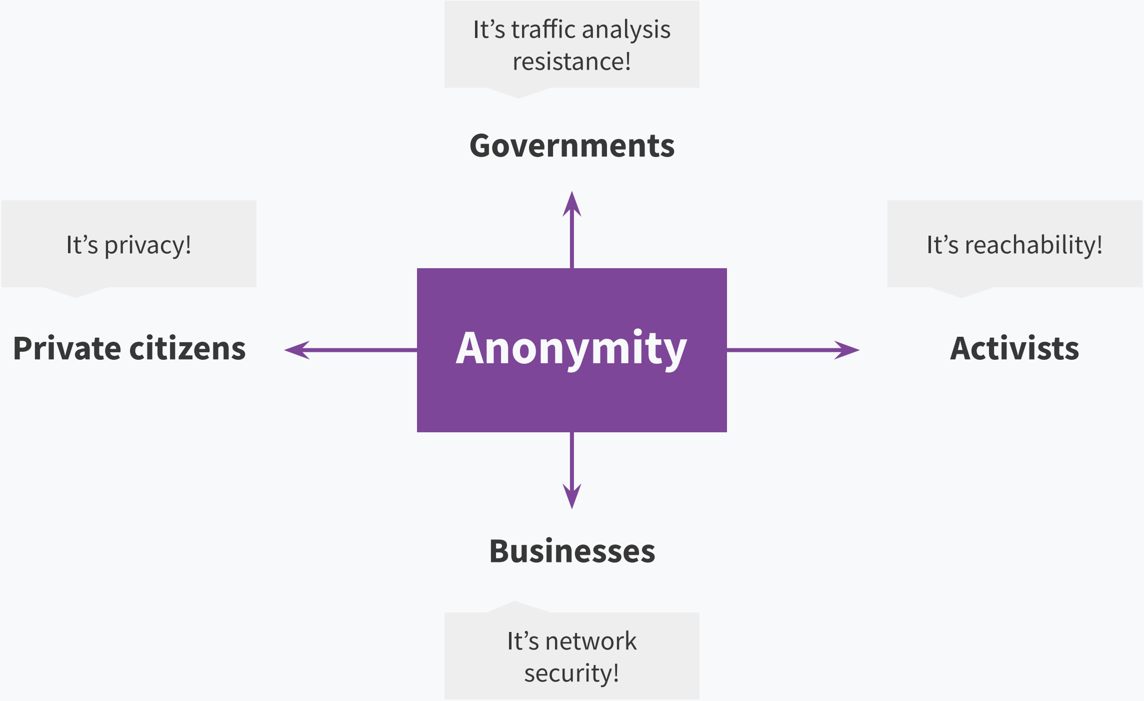
- It’s Tor (not capitalized).
- The goal is to have a way to use the internet with as much privacy as possible:
    a. by routing traffic through multiple servers; and
    b. by encrypting it each step of the way.
- Hence the term “onion routing”.
- Tor provides anonymity, mitigating against surveillance and censorship.

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.



“We kill people based on metadata”



It's traffic analysis resistance!

Governments

It's privacy!

Private citizens

Anonymity

It's reachability!

Activists

Businesses

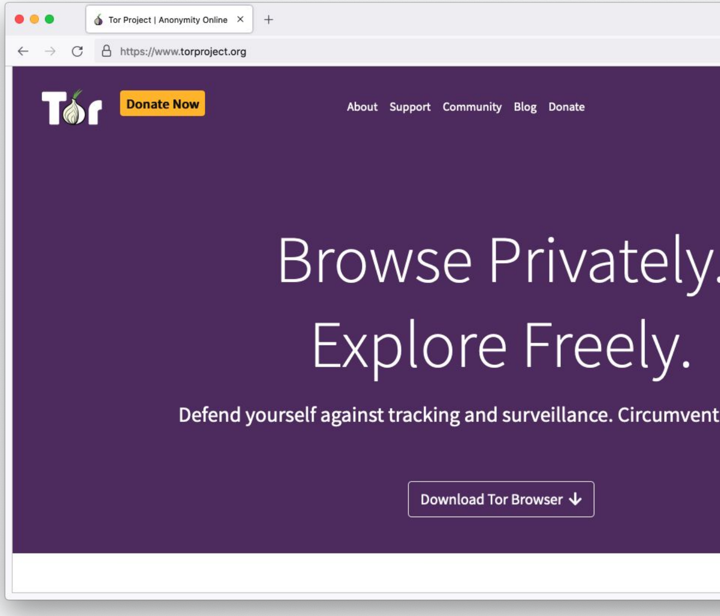
It's network security!

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.



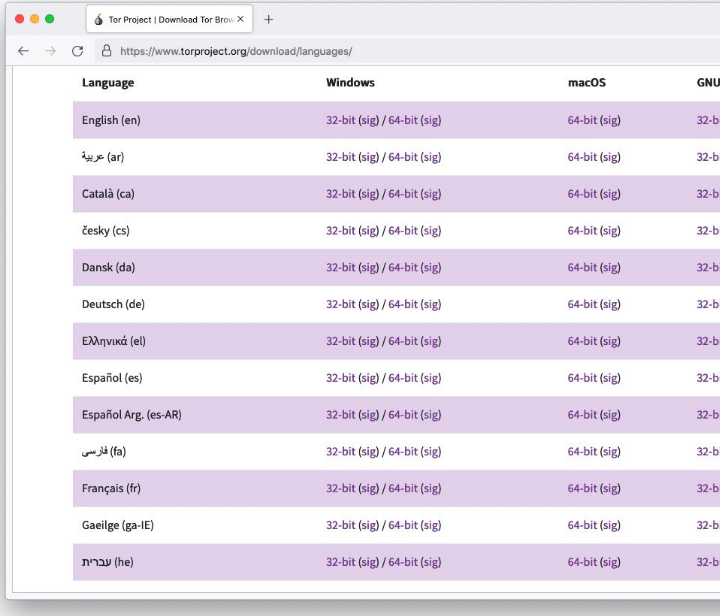
Browse Privately.

Explore Freely.

Defend yourself against tracking and surveillance. Circumvent

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/

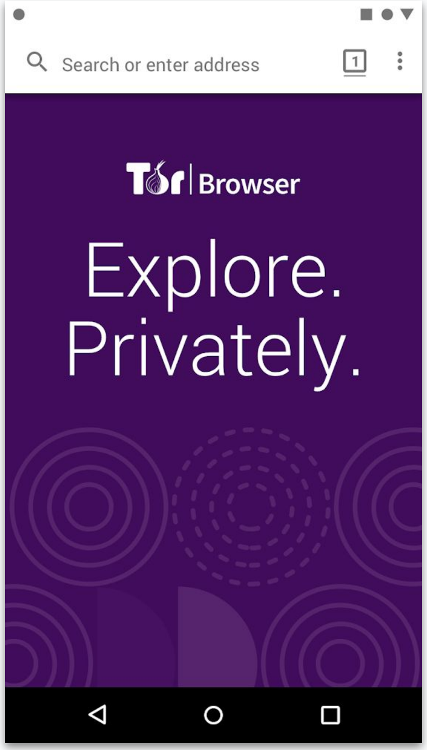

Tor Project | Download Tor Brow
https://www.torproject.org/download/languages/

Language	Windows	macOS	GNU
English (en)	32-bit (sig) / 64-bit (sig)	64-bit (sig)	32-b
عربية (ar)	32-bit (sig) / 64-bit (sig)	64-bit (sig)	32-b
Català (ca)	32-bit (sig) / 64-bit (sig)	64-bit (sig)	32-b
česky (cs)	32-bit (sig) / 64-bit (sig)	64-bit (sig)	32-b
Dansk (da)	32-bit (sig) / 64-bit (sig)	64-bit (sig)	32-b
Deutsch (de)	32-bit (sig) / 64-bit (sig)	64-bit (sig)	32-b
Ελληνικά (el)	32-bit (sig) / 64-bit (sig)	64-bit (sig)	32-b
Español (es)	32-bit (sig) / 64-bit (sig)	64-bit (sig)	32-b
Español Arg. (es-AR)	32-bit (sig) / 64-bit (sig)	64-bit (sig)	32-b
فارسی (fa)	32-bit (sig) / 64-bit (sig)	64-bit (sig)	32-b
Français (fr)	32-bit (sig) / 64-bit (sig)	64-bit (sig)	32-b
Gaeilge (ga-IE)	32-bit (sig) / 64-bit (sig)	64-bit (sig)	32-b
עברית (he)	32-bit (sig) / 64-bit (sig)	64-bit (sig)	32-b

Tor Browser on Android

Developed by the Tor Project

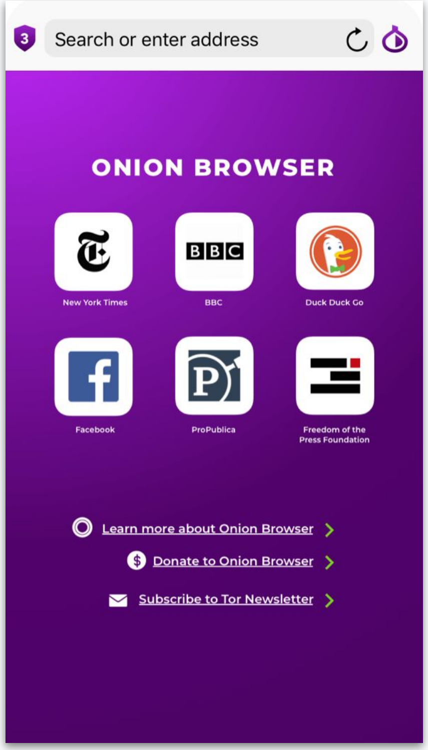
https://www.torproject.org/download/



Onion Browser on iOS

Developed by the Guardian Project

https://onionbrowser.com/



Connecting through **HTTP**

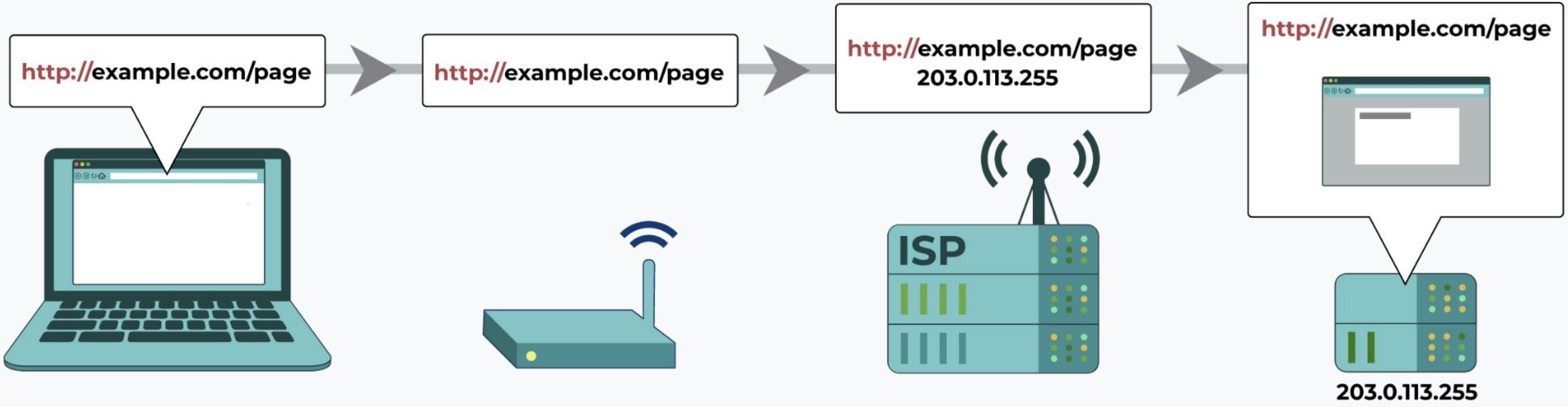


Image source: eff.org

Connecting through HTTPS

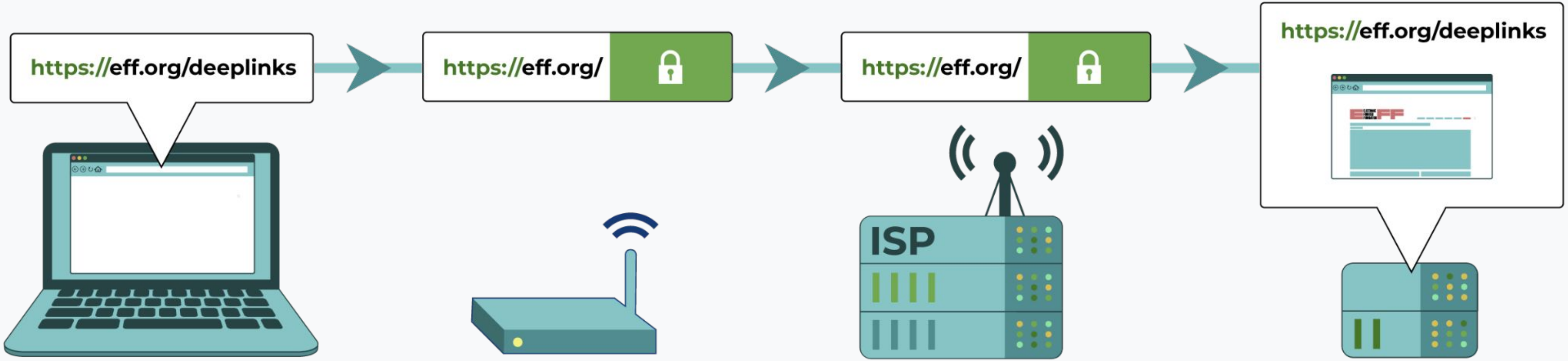


Image source: eff.org

Connecting through VPN

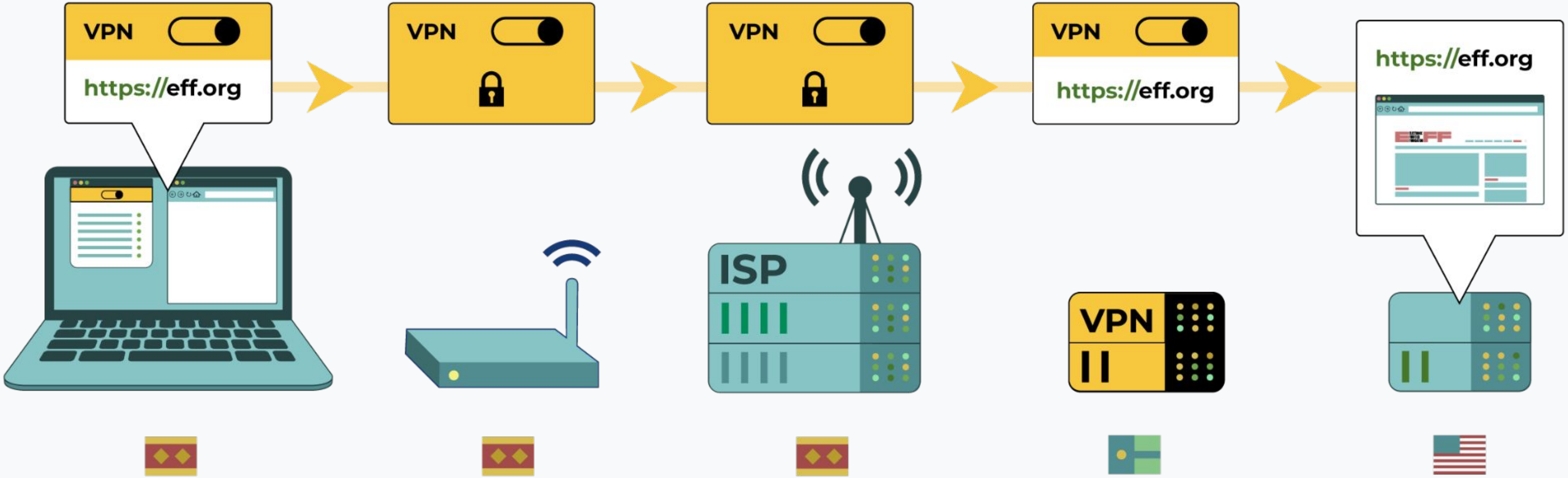


Image source: eff.org

Connecting through Tor

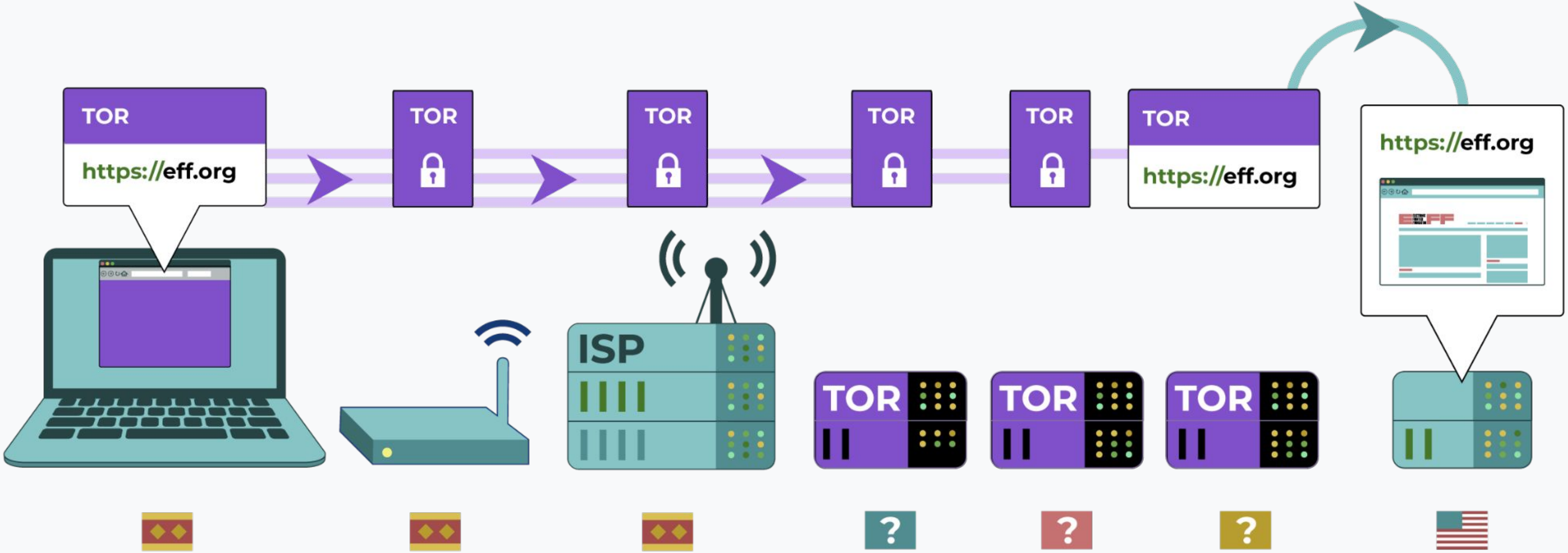
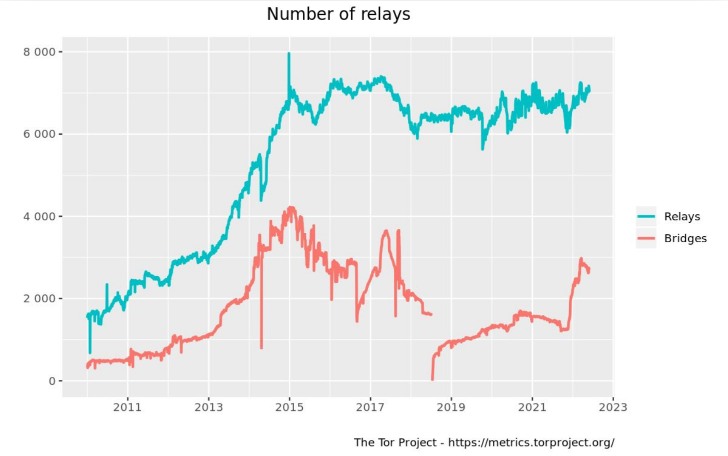


Image source: eff.org

A growing network of relays

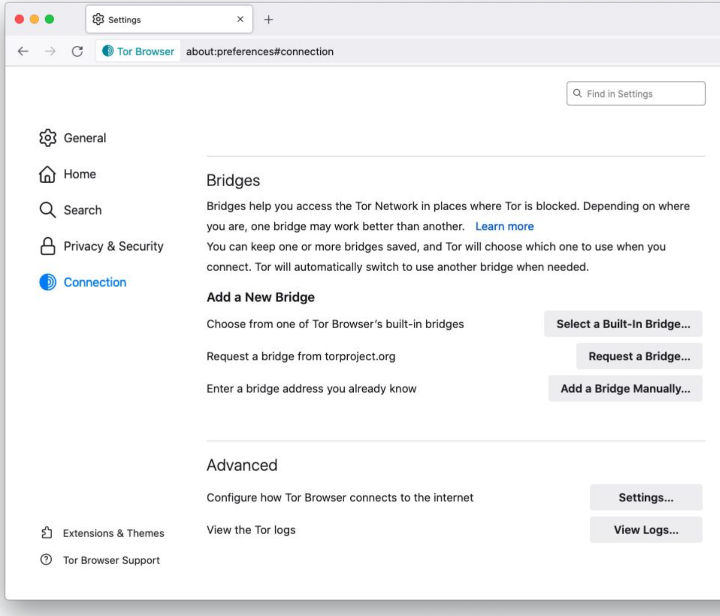
- Tor relays and bridges are run by volunteers from around the world, including individuals, NGOs, and companies.
- They form the backbone of the Tor network.
- Today we count: 7000+ relays and 2660+ bridges.



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

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/



Bridges

Bridges help you access the Tor Network in places where Tor is blocked. Depending on where you are, one bridge may work better than another. Learn more

You can keep one or more bridges saved, and Tor will choose which one to use when you connect. Tor will automatically switch to use another bridge when needed.

Add a New Bridge

Choose from one of Tor Browser's built-in bridges — Select a Built-In Bridge...

Request a bridge from torproject.org — Request a Bridge...

Enter a bridge address you already know — Add a Bridge Manually...

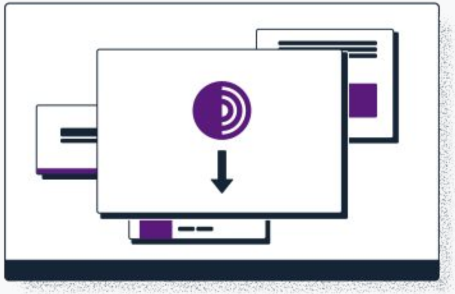
Advanced

Configure how Tor Browser connects to the internet — Settings...

View the Tor logs — View Logs...

Bypassing censorship of torproject.org

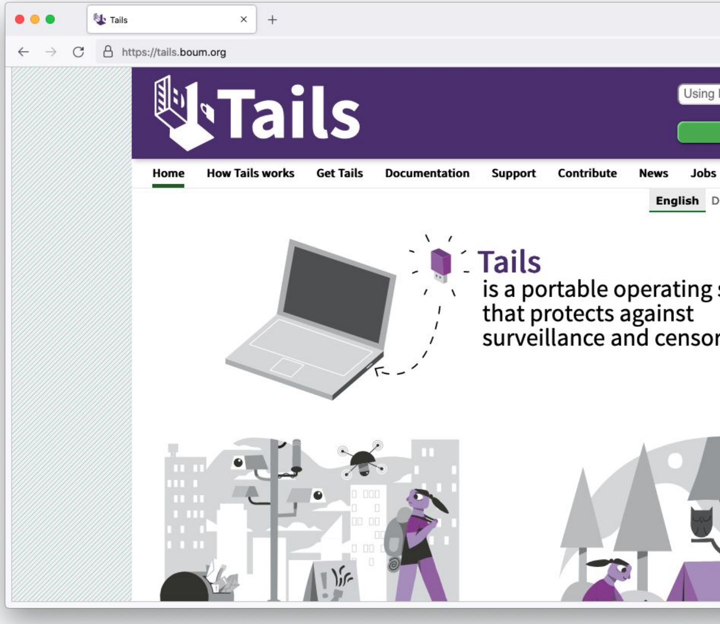
- Tor Project website could be blocked on your network.
- Multiple circumvention methods:
  - Mirror websites to download Tor Browser;
  - Emailing GetTor to receive browser bundle via email - gettor@torproject.org.



Applications that run on the Tor network

Operating system

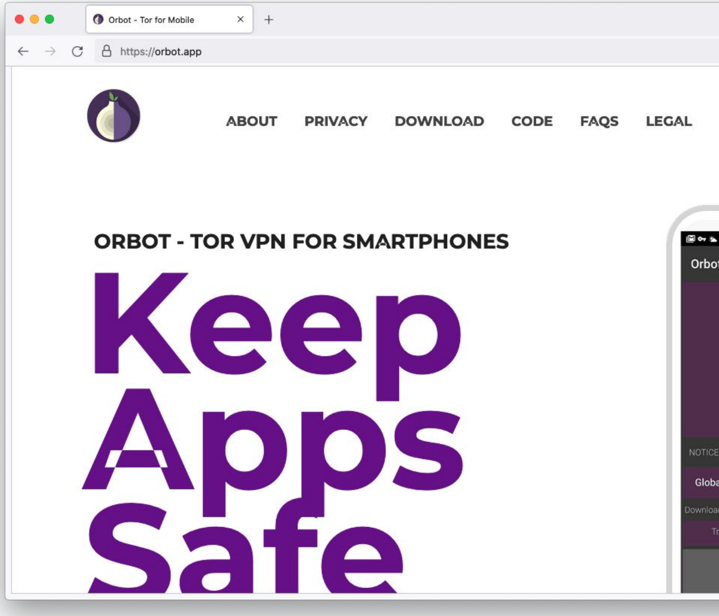
- Tails is an operating system (like Windows and macOS) that can be run straight from a USB.
- Tails ⇒ The Amnesic Incognito Live System.
- Tails isolates all of your connection of all applications through Tor and comes with a set of secure applications.
- An independent project: https://tails.boum.org/



Tails
is a portable operating
that protects against
surveillance and censor

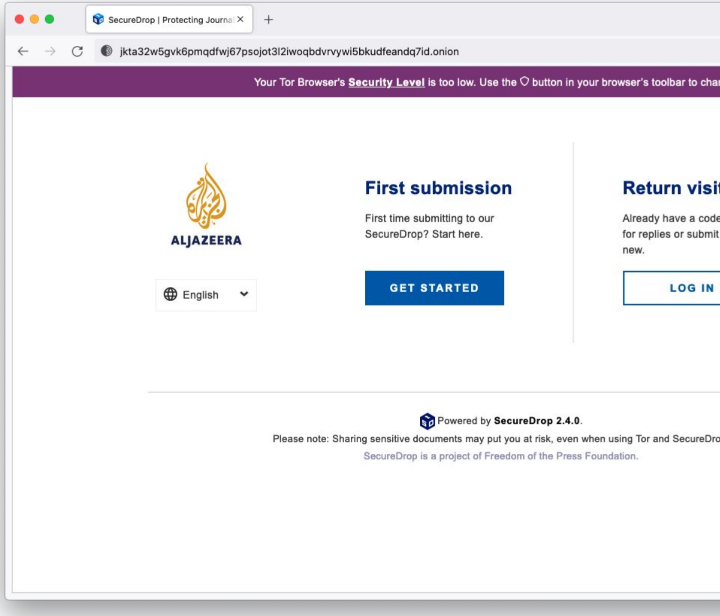
System-wide VPN

- 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.



SecureDrop | Protecting Journa
jkta32w5gvk6pmqdfwj67psojot3l2iwoqbdvrvywi5bkudfeandq7id.onion
ALJAZEERA
English
GET STARTED
LOG IN

Your Tor Browser's **Security Level** is too low. Use the ♡ button in your browser's toolbar to char

First submission

First time submitting to our SecureDrop? Start here.

Return visi

Already have a code for replies or submit new.

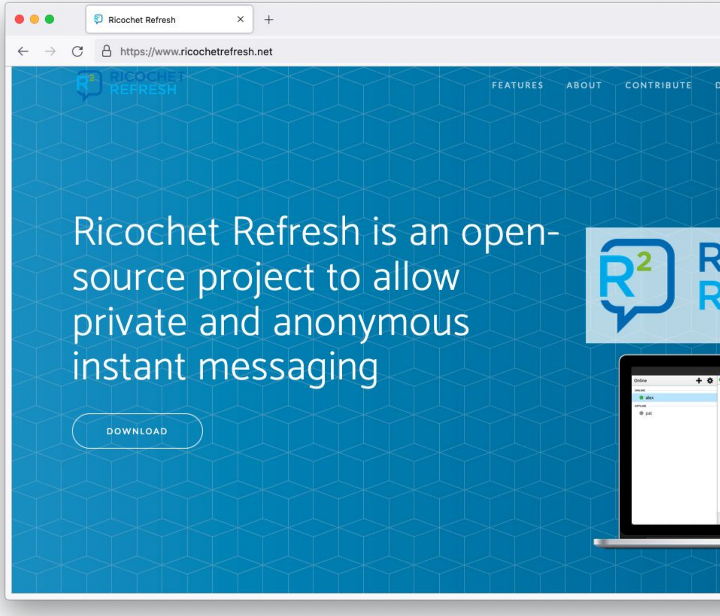
Powered by **SecureDrop 2.4.0**.

Please note: Sharing sensitive documents may put you at risk, even when using Tor and SecureDro

SecureDrop is a project of Freedom of the Press Foundation.

Anonymous peer-to-peer messaging

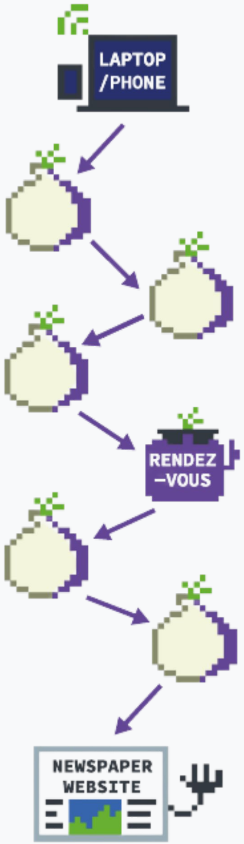
- Ricochet Refresh is an instant messenger that routes all messages through Tor.
- Nobody knows who you're talking to, or what you're talking about.
- Supported by Blueprint for Free Speech: https://www.blueprintforfreespeech.net/



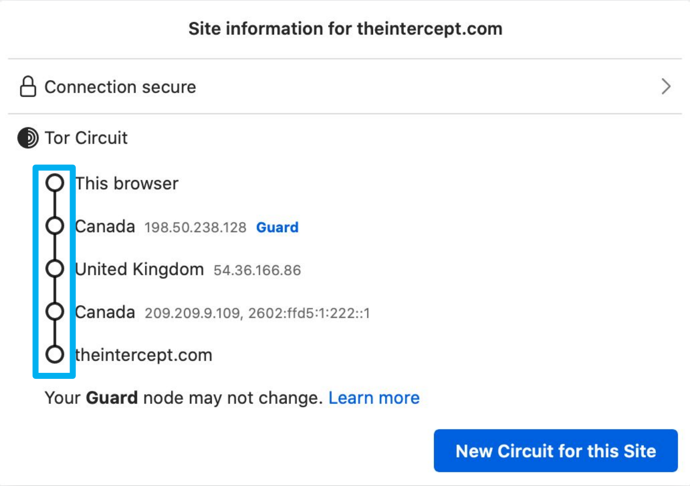
Ricochet Refresh is an open-source project to allow private and anonymous instant messaging

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



Site information for theintercept.com

Connection secure

Tor Circuit

This browser

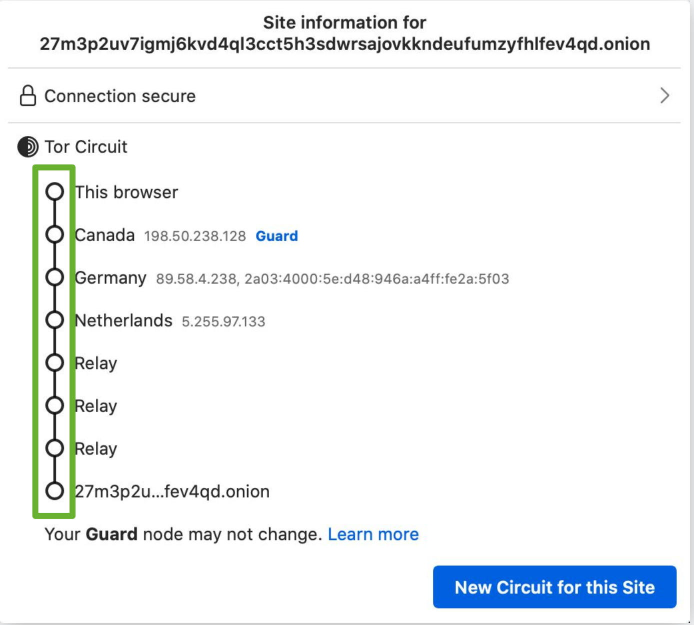
Canada 198.50.238.128 Guard

United Kingdom 54.36.166.86

Canada 209.209.9.109, 2602:ffd5:1:222::1

theintercept.com

Your **Guard** node may not change. Learn more



Site information for
27m3p2uv7igmj6kvd4ql3cct5h3sdwrsajovkkndeufumzyfhlfev4qd.onion

Connection secure

Tor Circuit

This browser

Canada 198.50.238.128 Guard

Germany 89.58.4.238, 2a03:4000:5e:d48:946a:a4ff:fe2a:5f03

Netherlands 5.255.97.133

Relay

Relay

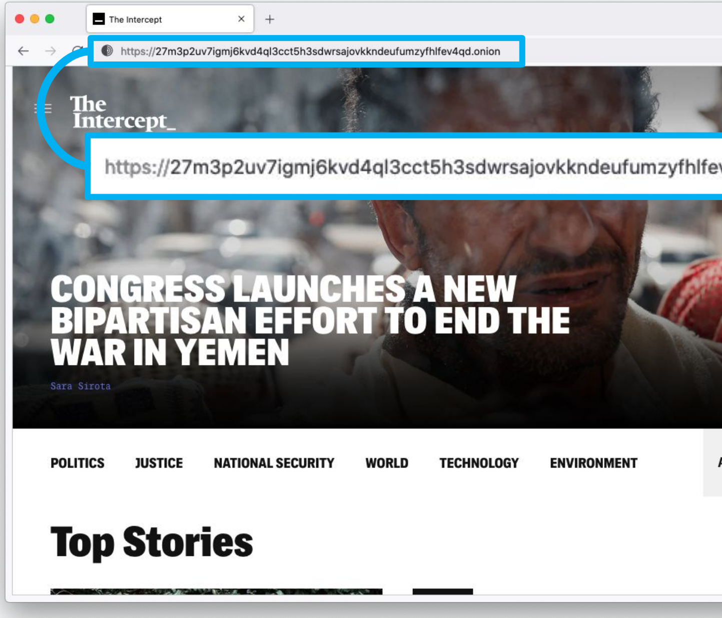
Relay

27m3p2u...fev4qd.onion

Your **Guard** node may not change. Learn more

.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".



The Intercept

https://27m3p2uv7igmj6kvd4ql3cct5h3sdwrsajovkkndeufumzyfhlfev4qd.onion

https://27m3p2uv7igmj6kvd4ql3cct5h3sdwrsajovkkndeufumzyfhlfe

CONGRESS LAUNCHES A NEW BIPARTISAN EFFORT TO END THE WAR IN YEMEN

Sara Sirota

Censorship resistance

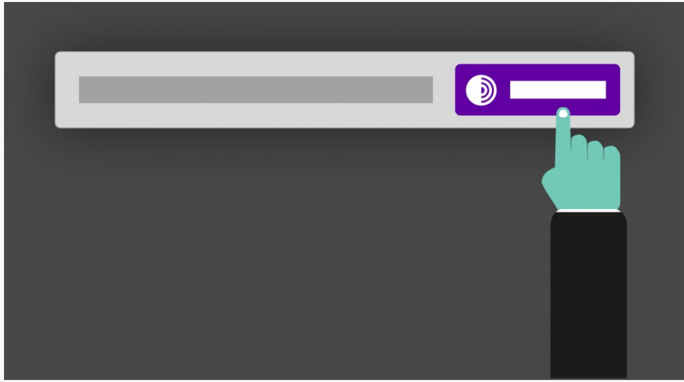
- Both location and IP address of an Onion Service are hidden, making it difficult to censor or identify who runs the service.
- This is why they used to be called “hidden services”.
- It’s the most censorship-resistant technology available out there.

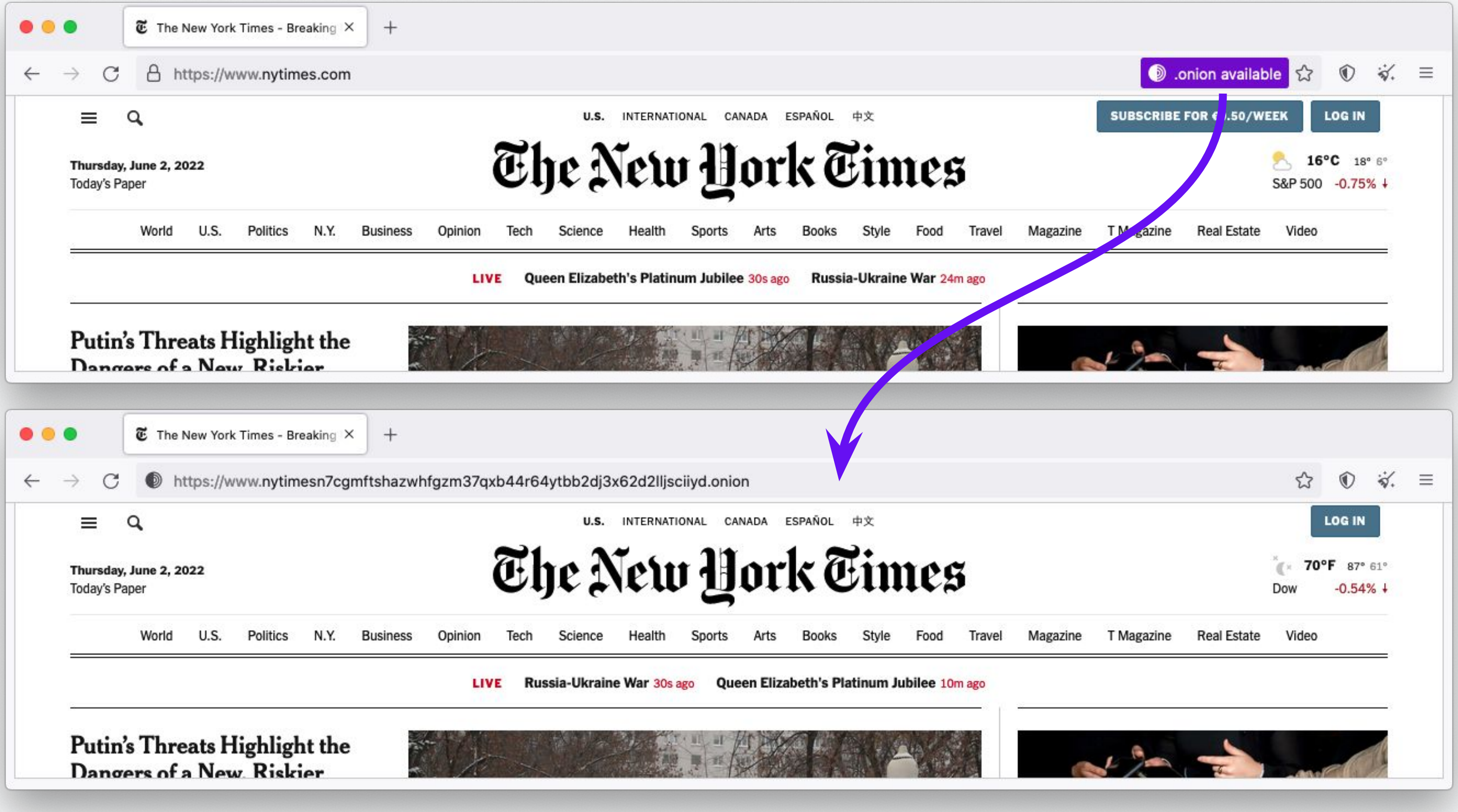
Decentralizing the web

- 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 €.50/WEEK
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 Dangers of a New, Riskier
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 Dangers of a New, Riskier

Popular Onion Services

The Intercept_

BBC

PROPUBLICA

The New York Times

RISEUP

facebook

brave

FREEDOM OF THE PRESS FOUNDATION

Privacy Matters.

FRONT LINE DEFENDERS

debian

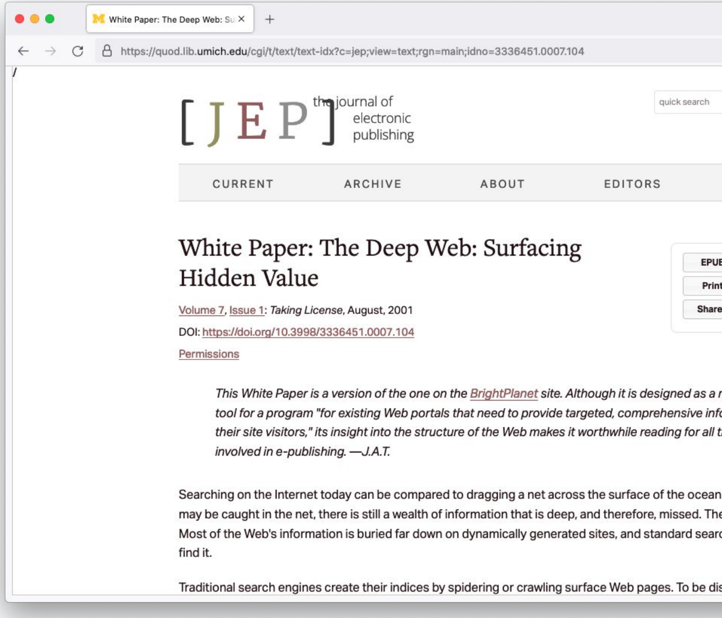
The many benefits of Onion Services

1. Enables freedom of press and censorship circumvention
2. Level up service privacy
3. Decentralization of the web
4. Network sustainability
5. Protection of sources, whistleblowers, and journalists
6. Opportunity to educate users about privacy by design
7. Metadata obfuscation and/or elimination

“Deep” / “Dark” Web?

What’s actually the “deep” web?

- Refers to content on the World Wide Web that is not indexed by search engines, often hidden behind passwords, etc.
- American computer scientist Michael K. Bergman is linked to coining the expression, “the deep web”.


White Paper: The Deep Web: Su
https://quod.lib.umich.edu/cgi/t/text/text-idx?c=jep;view=text;rgn=main;idno=3336451.0007.104
[JEP] the journal of electronic publishing
quick search
CURRENT
ARCHIVE
ABOUT
EDITORS
EPUB
Print
Share

White Paper: The Deep Web: Surfacing Hidden Value

Volume 7, Issue 1: *Taking License*, August, 2001

DOI: https://doi.org/10.3998/3336451.0007.104

Permissions

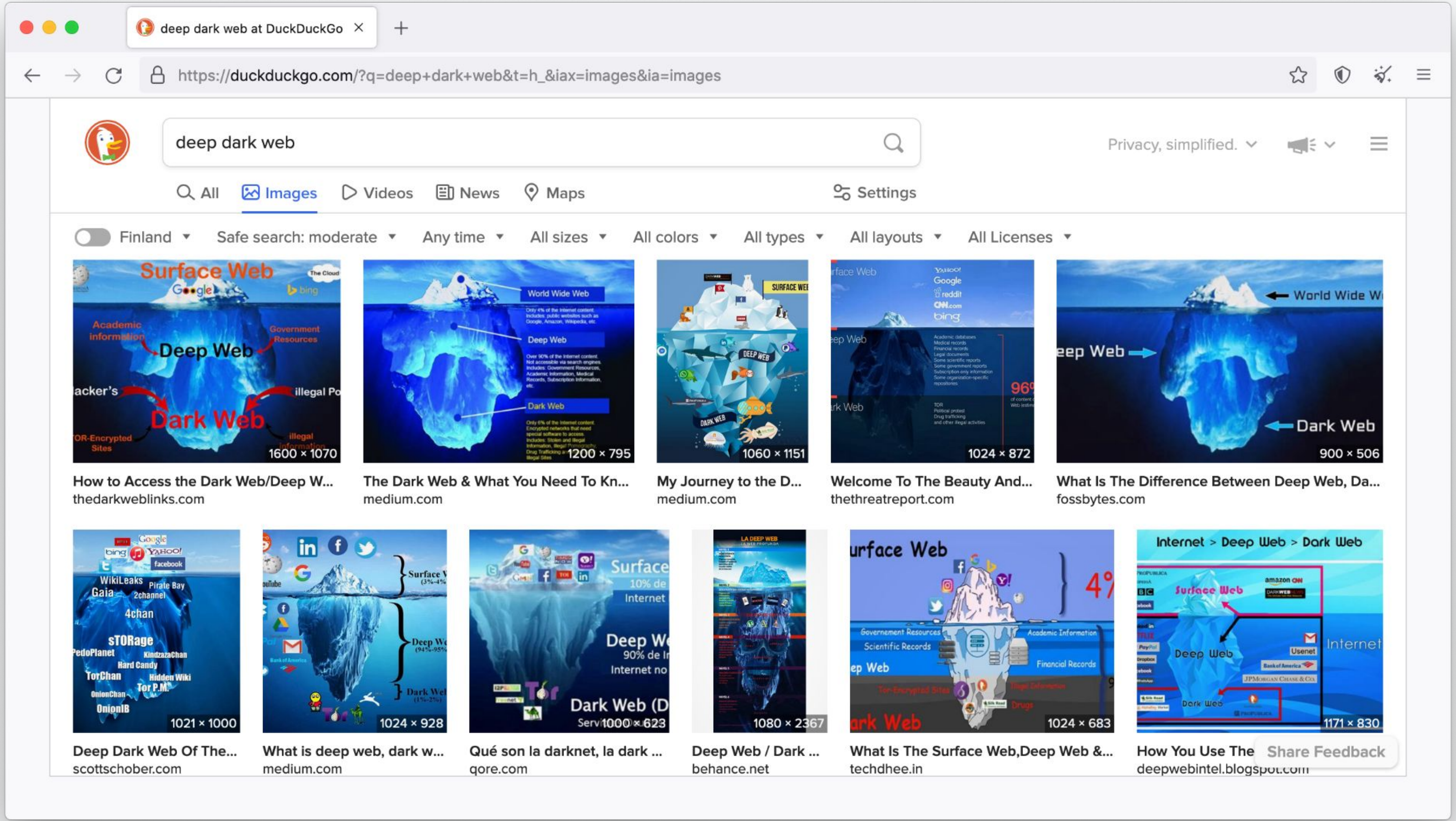
> *This White Paper is a version of the one on the BrightPlanet site. Although it is designed as a r tool for a program "for existing Web portals that need to provide targeted, comprehensive info their site visitors," its insight into the structure of the Web makes it worthwhile reading for all t involved in e-publishing. —J.A.T.*

Searching on the Internet today can be compared to dragging a net across the surface of the ocean may be caught in the net, there is still a wealth of information that is deep, and therefore, missed. The Most of the Web's information is buried far down on dynamically generated sites, and standard searc find it.

Traditional search engines create their indices by spidering or crawling surface Web pages. To be dis

Important to note about the “dark web”

- The “dark web” is an illusion.
- The term used often to speak negatively about encryption, in the context of encouraging encryption backdoors.



deep dark web at DuckDuckGo

https://duckduckgo.com/?q=deep+dark+web&t=h_&iax=images&ia=images

deep dark web

Privacy, simplified.

All | Images | Videos | News | Maps | Settings

Finland ▾ | Safe search: moderate ▾ | Any time ▾ | All sizes ▾ | All colors ▾ | All types ▾ | All layouts ▾ | All Licenses ▾

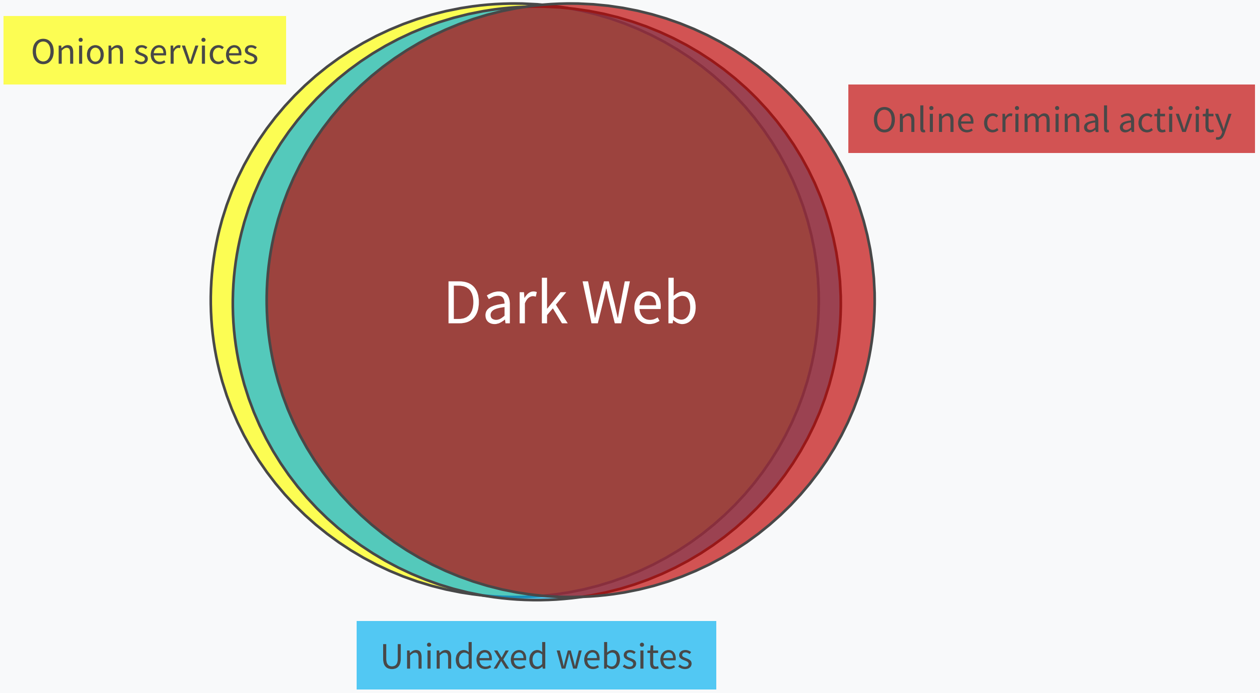
Size	Title	Source
1600 × 1070	How to Access the Dark Web/Deep W...	thedarkweblinks.com
1200 × 795	The Dark Web & What You Need To Kn...	medium.com
1060 × 1151	My Journey to the D...	medium.com
1024 × 872	Welcome To The Beauty And...	ththreatreport.com
900 × 506	What Is The Difference Between Deep Web, Da...	fossbytes.com
1021 × 1000	Deep Dark Web Of The...	scottschober.com
1024 × 928	What is deep web, dark w...	medium.com
1000 × 623	Qué son la darknet, la dark ...	qore.com
1080 × 2367	Deep Web / Dark ...	behance.net
1024 × 683	What Is The Surface Web,Deep Web &...	techdhee.in
1171 × 830	How You Use The	deepwebintel.blogspot.com

Share Feedback

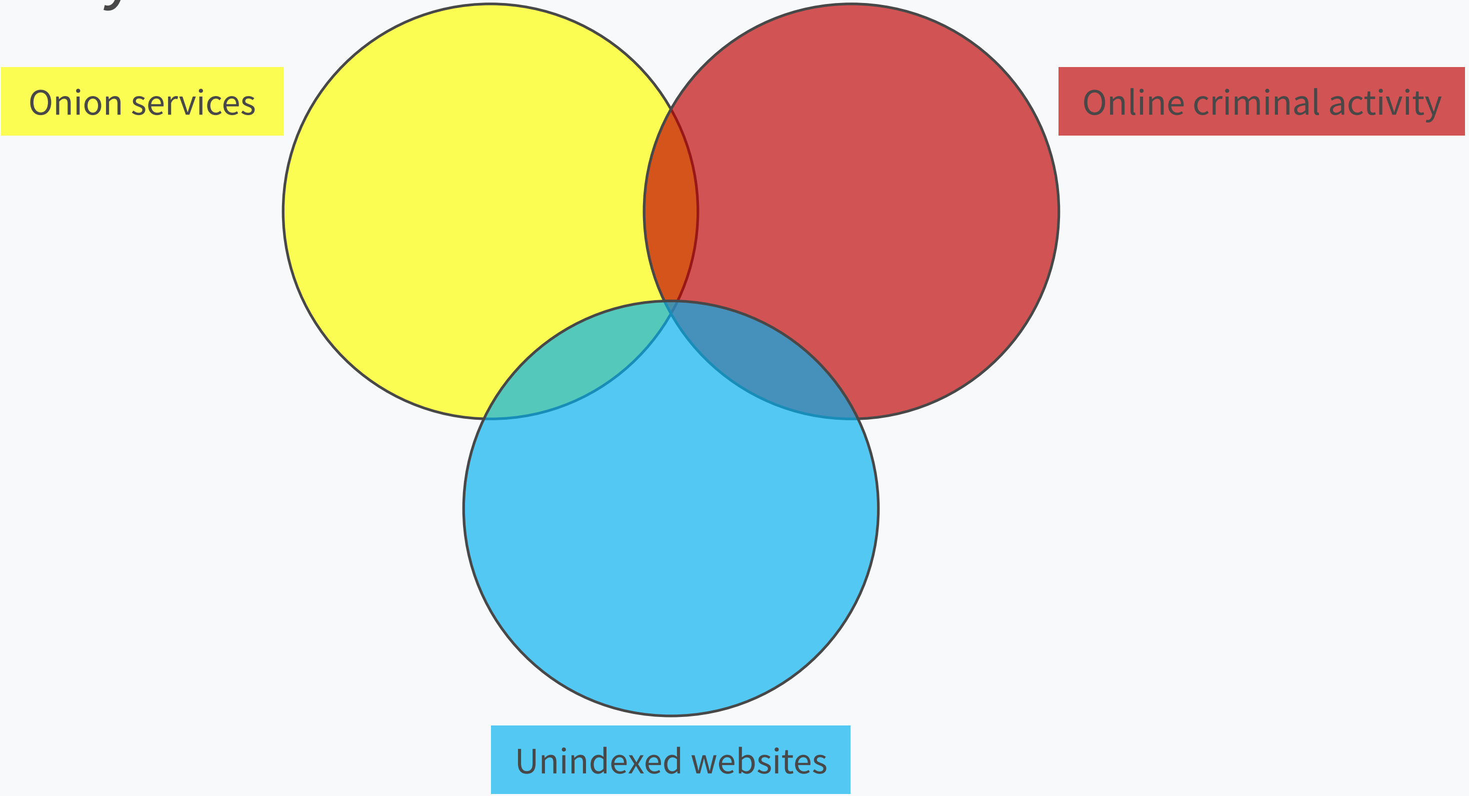
Iceberg analogies

- The web is usually represented as an elongated iceberg with ~90% of its body deep below water.
- This iceberg's orientation is unstable and won't be found in nature floating like this, it would only float on its side...
- More importantly, it's a false analogy of the web that doesn't serve any purpose other than spread misconceptions.

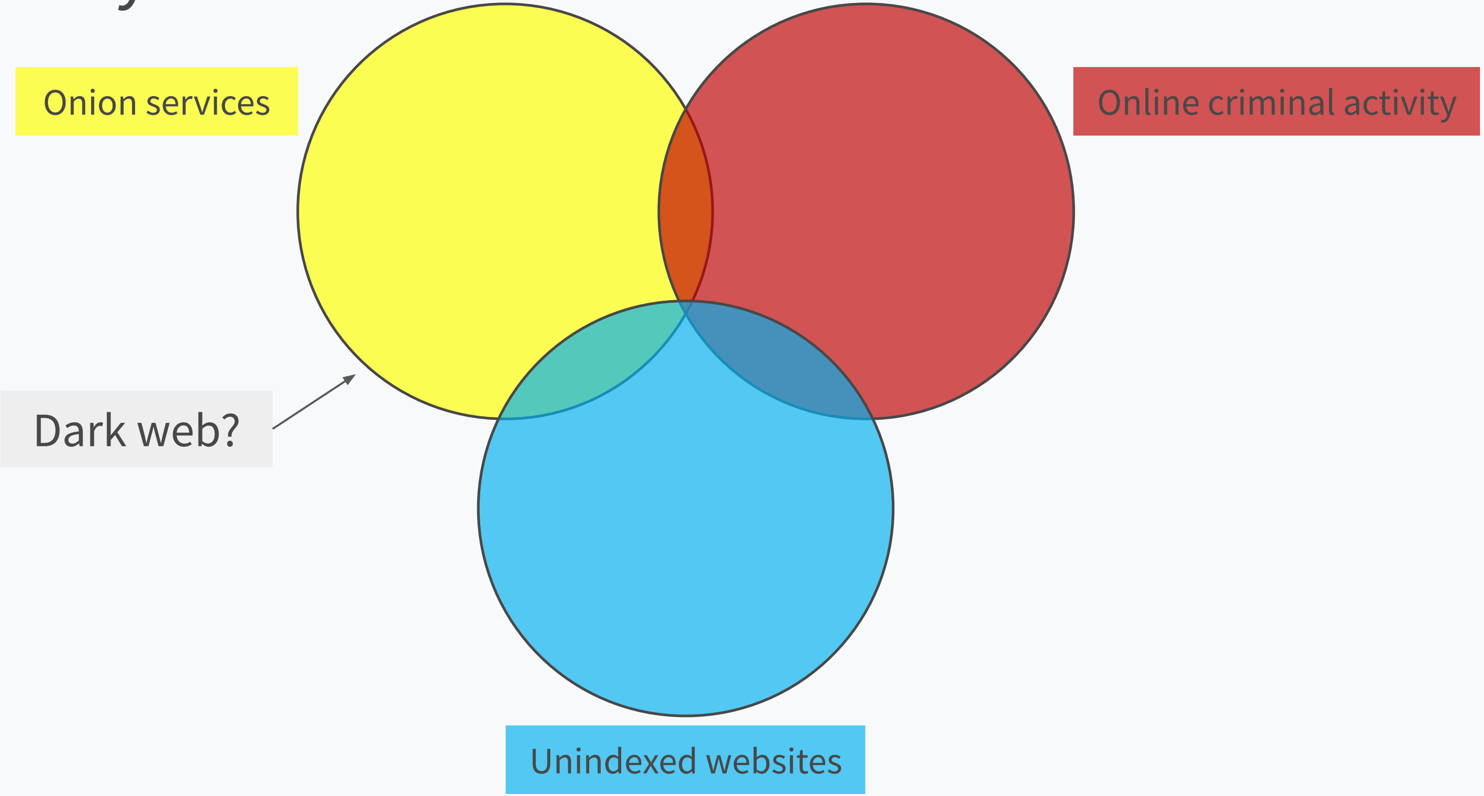
How the “Dark Web” is usually represented



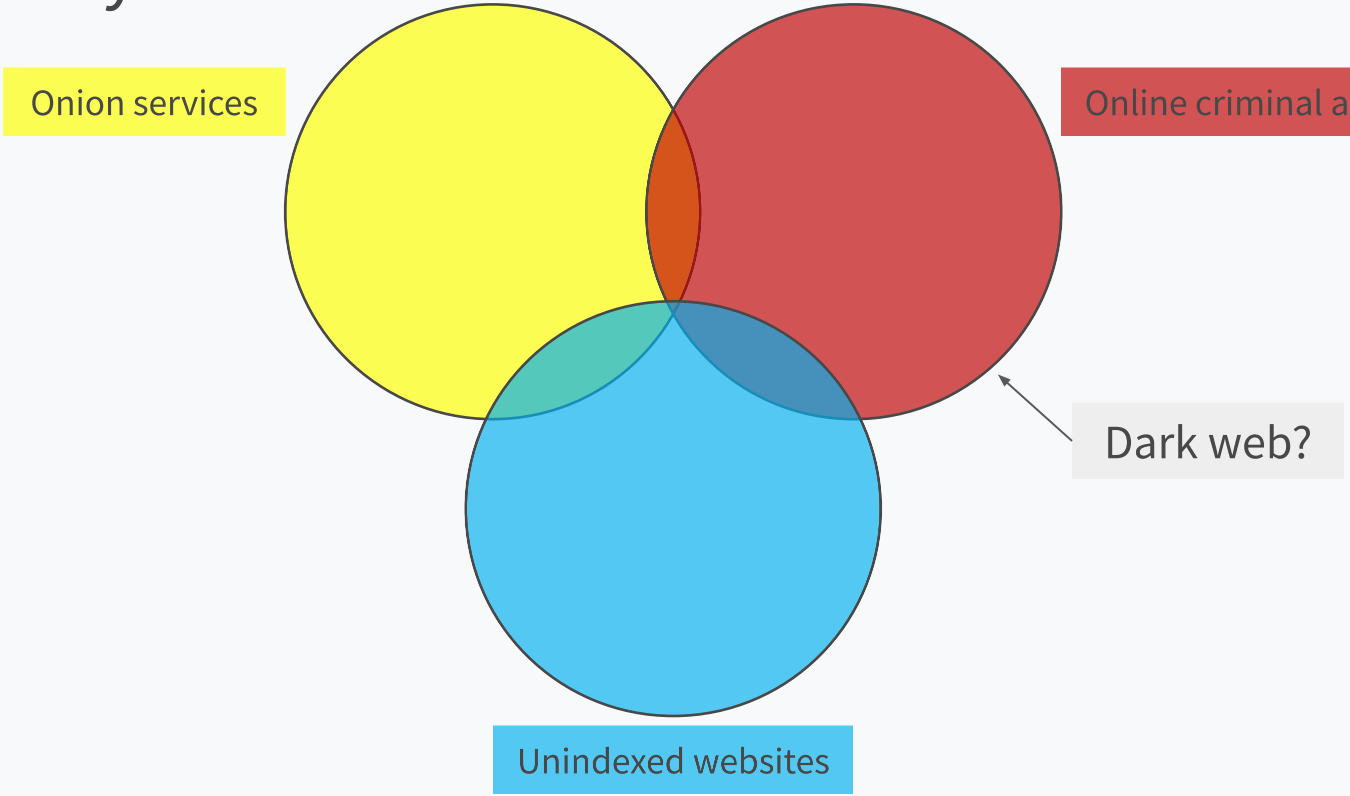
The reality


Onion services
Online criminal activity
Unindexed websites

The reality


Onion services
Online criminal activity
Dark web?
Unindexed websites

The reality



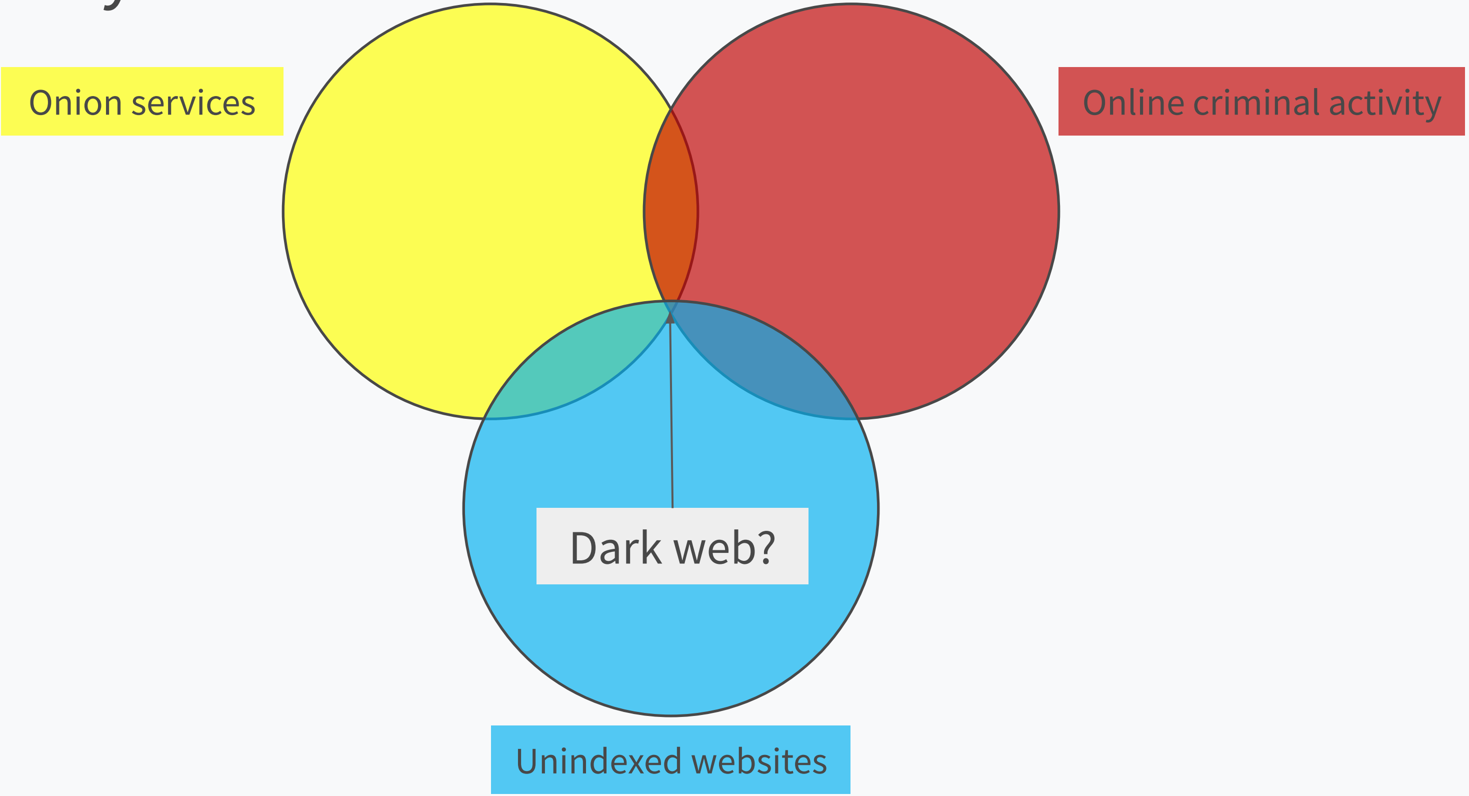
Onion services

Online criminal activity

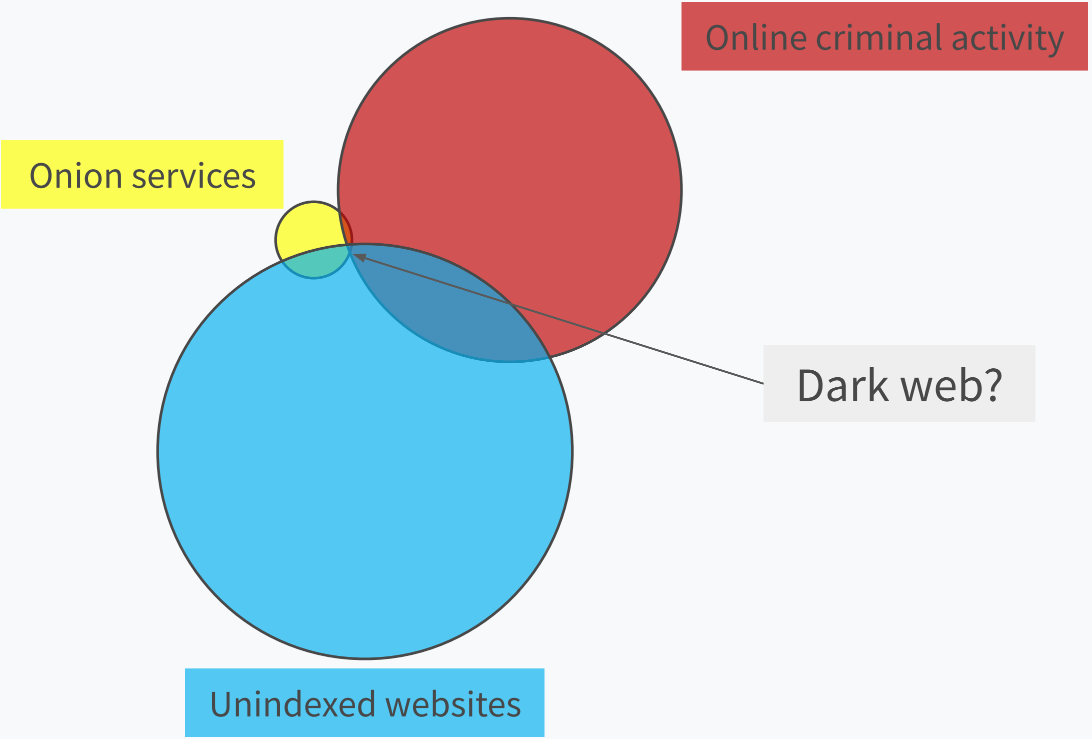
Dark web?

Unindexed websites

The reality

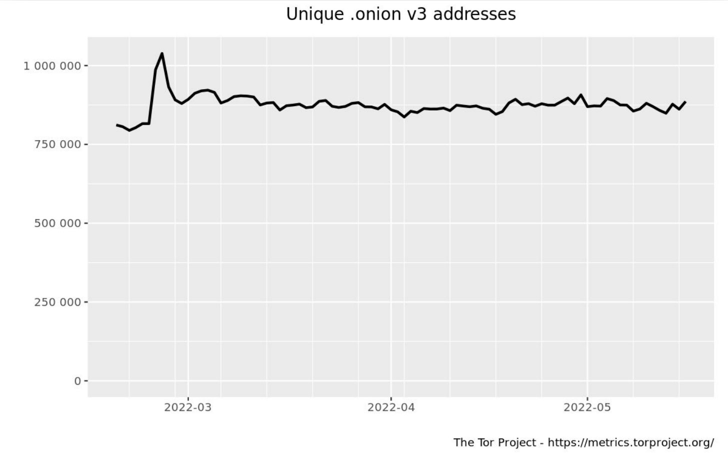

Onion services
Online criminal activity
Dark web?
Unindexed websites

It’s important to look at scale



Metrics on Onion Services

- Approximately ~886k Onion Services (v3).
- Relay bandwidth: ~750 Gbit/s.
- Onion Services traffic: ~9 Gbit/s.
- Onion services represent ~1.2% of Tor’s traffic.
- Tor metrics portal: https://metrics.torproject.org/



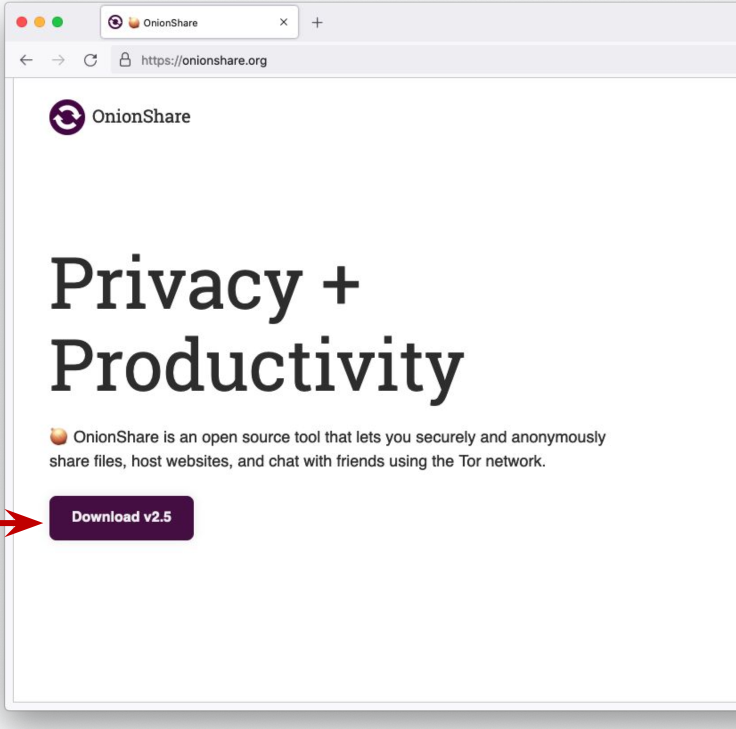
Activity 1: deploying an Onion Service

OnionShare

- OnionShare is an open source tool that allows secure and anonymous file sharing, website hosting, and chatting.
- All communication happens on the Tor network.
- Link: https://onionshare.org/

Step 1: Download OnionShare

- Available on: Windows, macOS, Linux.
- Link: https://onionshare.org/

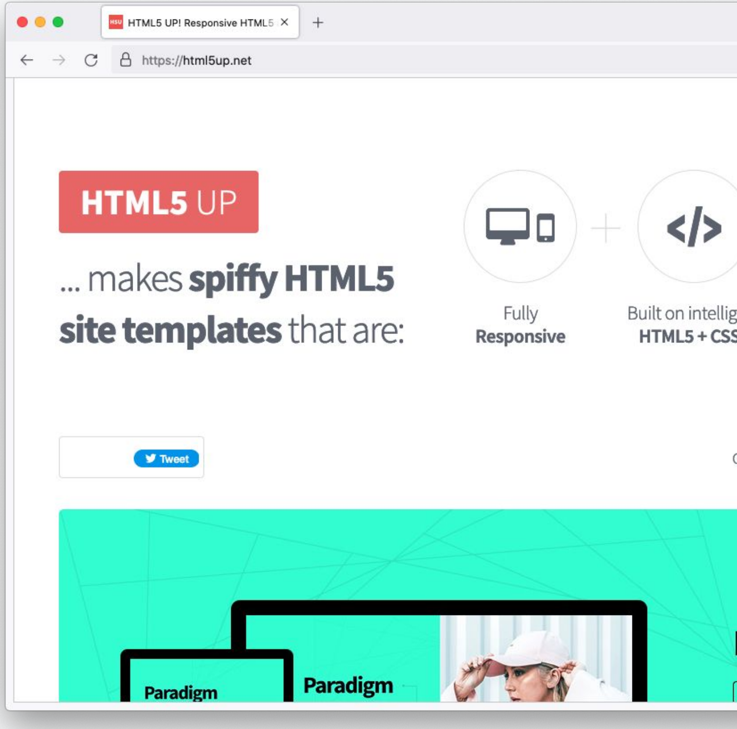


Privacy + Productivity

OnionShare is an open source tool that lets you securely and anonymously share files, host websites, and chat with friends using the Tor network.

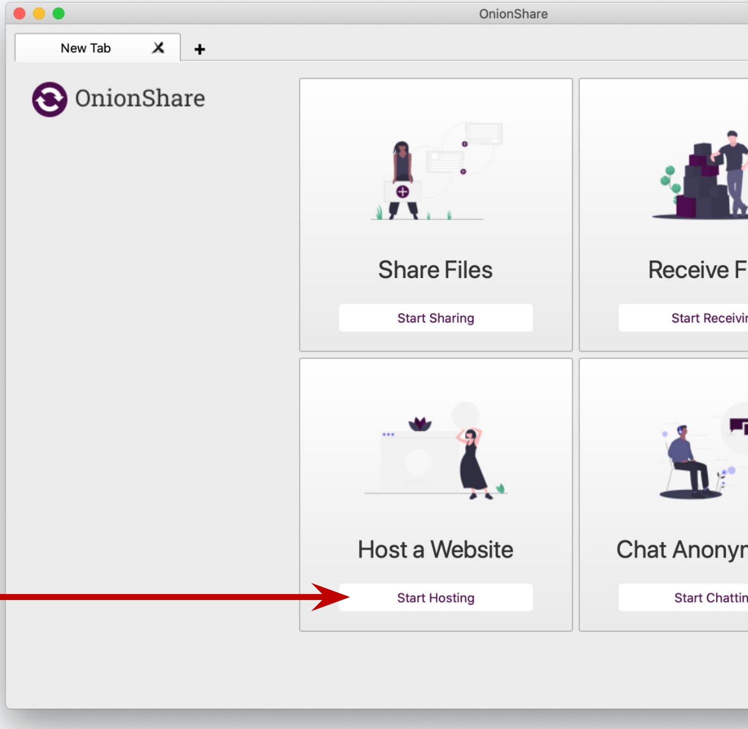
Step 2: Download a website template

- Choose any website template you can download and edit quickly.
- Suggested: any template from https://html5up.net/



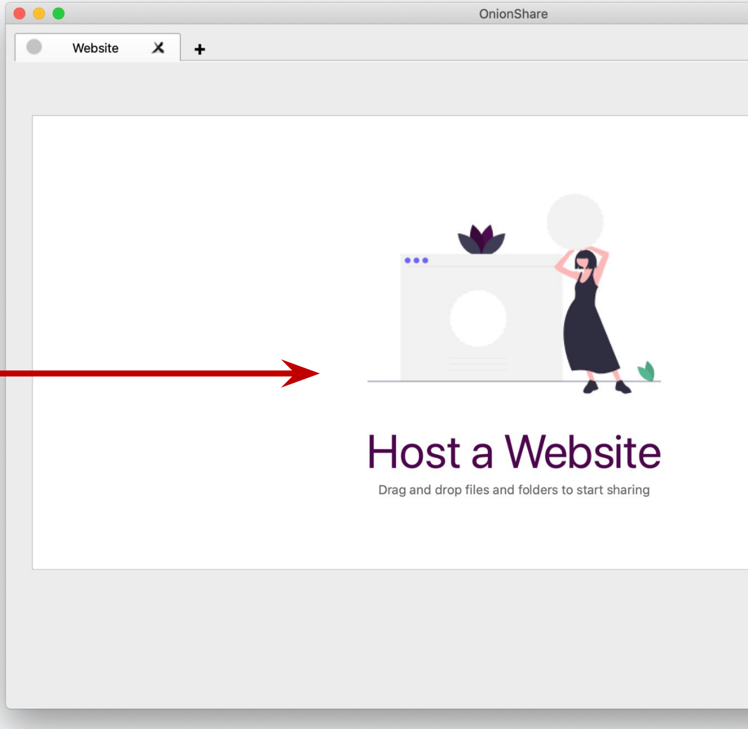
Step 3: Select “Host a Website”

- In the “Host a Website” section, click “Start Hosting”



Step 4: Upload website template

- Drag and drop the website template folder into the section.

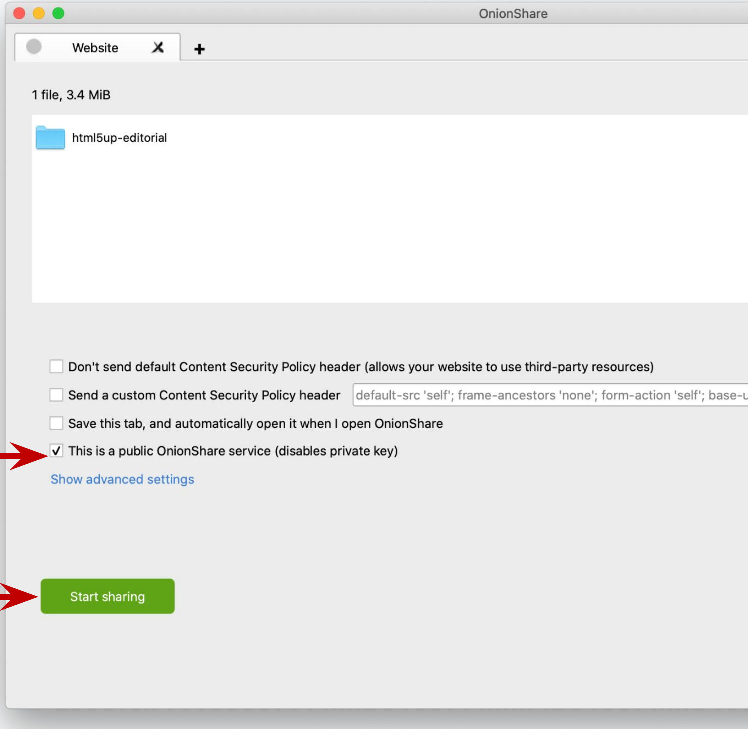


Host a Website

Drag and drop files and folders to start sharing

Step 5: Launch your Onion Service

- Select “This is a public OnionShare service”
- Click on “Start sharing”



1 file, 3.4 MiB

html5up-editorial

□ Don't send default Content Security Policy header (allows your website to use third-party resources)

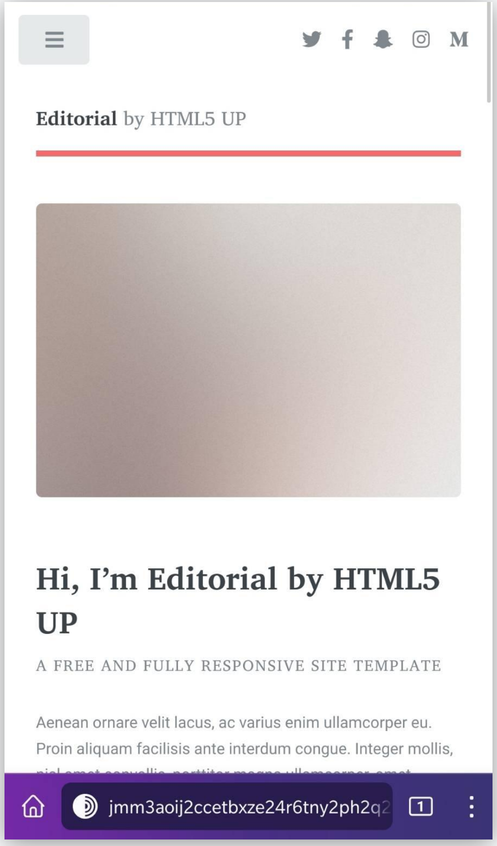
□ Send a custom Content Security Policy header default-src 'self'; frame-ancestors 'none'; form-action 'self'; base-u

□ Save this tab, and automatically open it when I open OnionShare

☑ This is a public OnionShare service (disables private key)

Step 6: Share your .onion address!

- Your Onion Service is now live.
- Tip: you must keep your OnionShare window on your device open as long as you want people to be able to visit your site.



Editorial by HTML5 UP

Hi, I’m Editorial by HTML5 UP

A FREE AND FULLY RESPONSIVE SITE TEMPLATE

Aenean ornare velit lacus, ac varius enim ullamcorper eu. Proin aliquam facilisis ante interdum congue. Integer mollis,

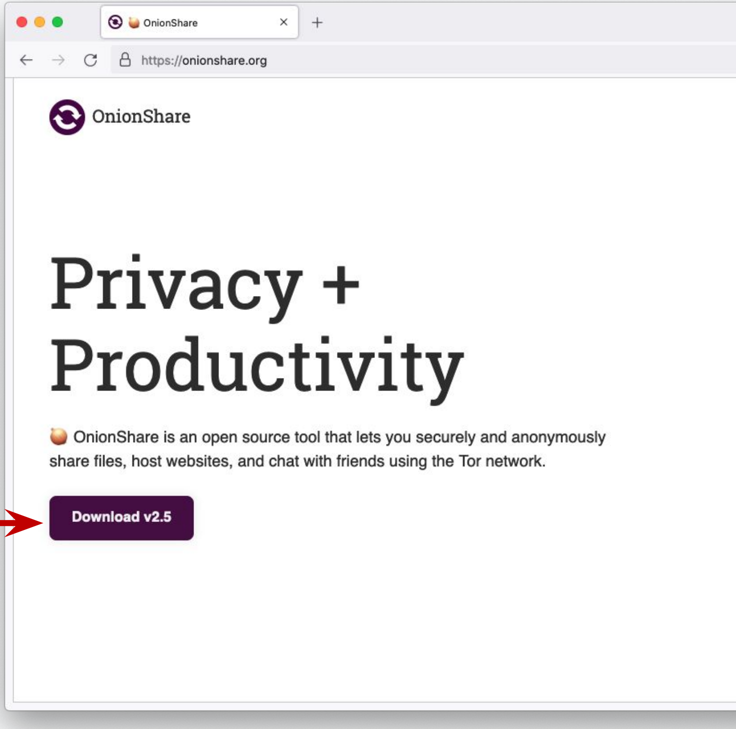
Activity 2: sharing files securely

OnionShare

- OnionShare is an open source tool that allows secure and anonymous file sharing, website hosting, and chatting.
- All communication happens on the Tor network.
- Link: https://onionshare.org/

Step 1: Download OnionShare

- Available on: Windows, macOS, Linux.
- Link: https://onionshare.org/

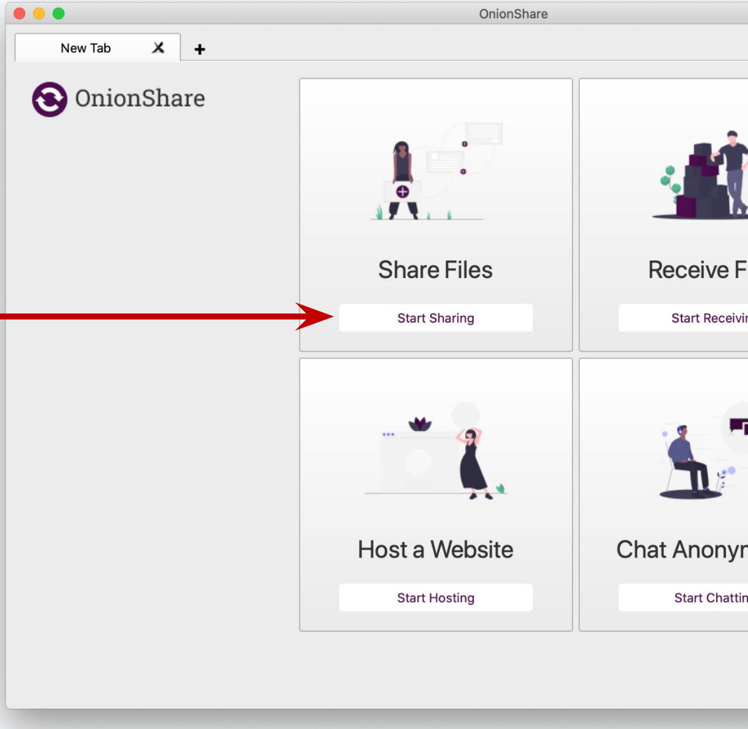


Privacy + Productivity

OnionShare is an open source tool that lets you securely and anonymously share files, host websites, and chat with friends using the Tor network.

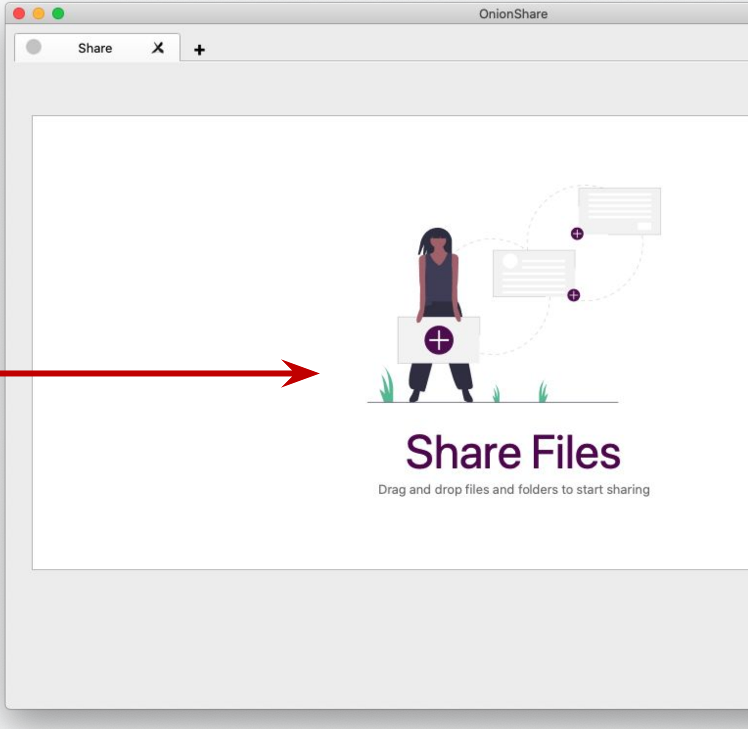
Step 2: Select “Share Files”

- In the “Share Files” section, click “Start Sharing”



Step 3: Upload your file

- Drag and drop the file into the folder into the section.

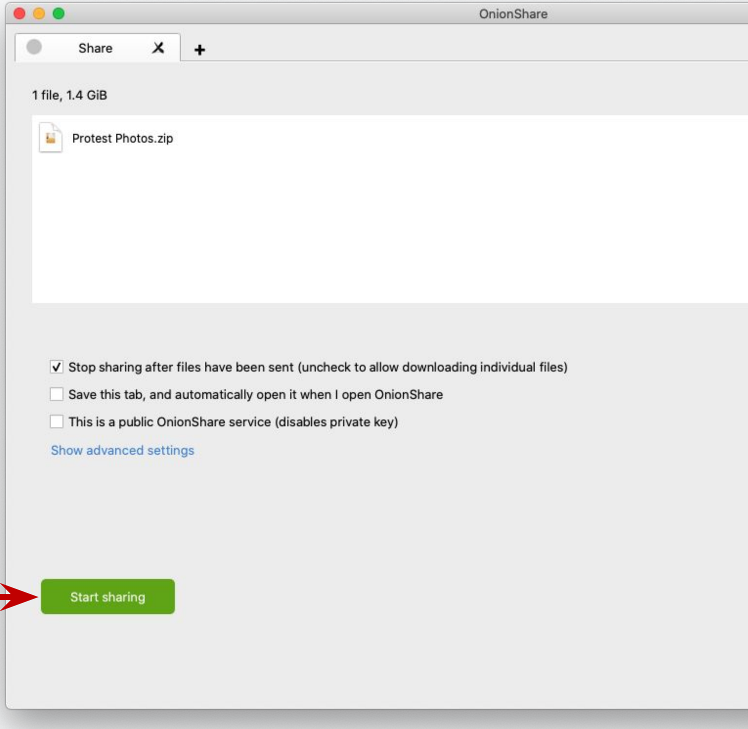


Share Files

Drag and drop files and folders to start sharing

Step 4: Share your file

- Click on “Start Sharing”



1 file, 1.4 GiB

Protest Photos.zip

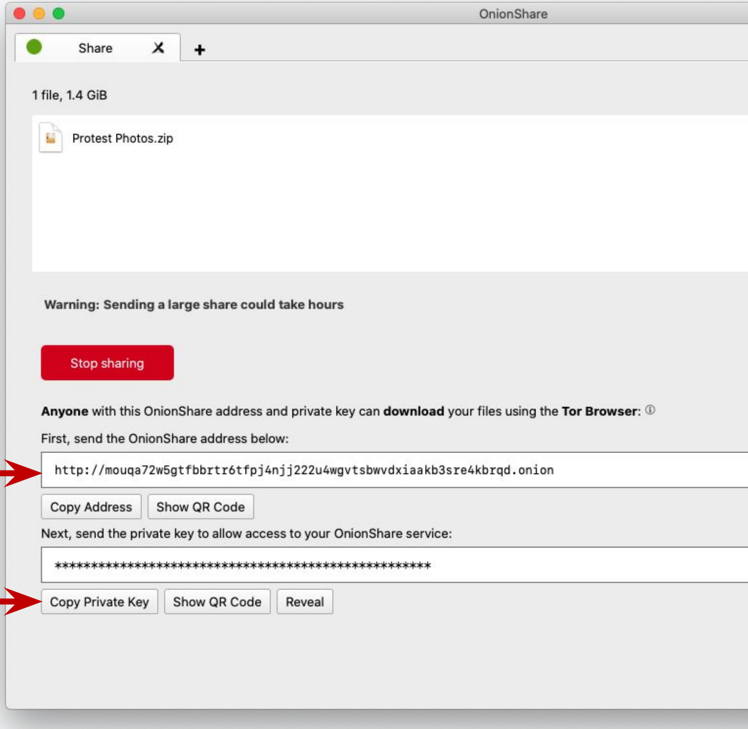
☑ Stop sharing after files have been sent (uncheck to allow downloading individual files)

□ Save this tab, and automatically open it when I open OnionShare

□ This is a public OnionShare service (disables private key)

Step 5: Copy and share the address and key

- Copy the address and share it with the intended recipient (e.g. via email).
- Copy the private key and share it to the same recipient, preferably through a different channel (e.g. via instant messaging).



1 file, 1.4 GiB

Protest Photos.zip

Warning: Sending a large share could take hours

Anyone with this OnionShare address and private key can **download** your files using the **Tor Browser**:

First, send the OnionShare address below:

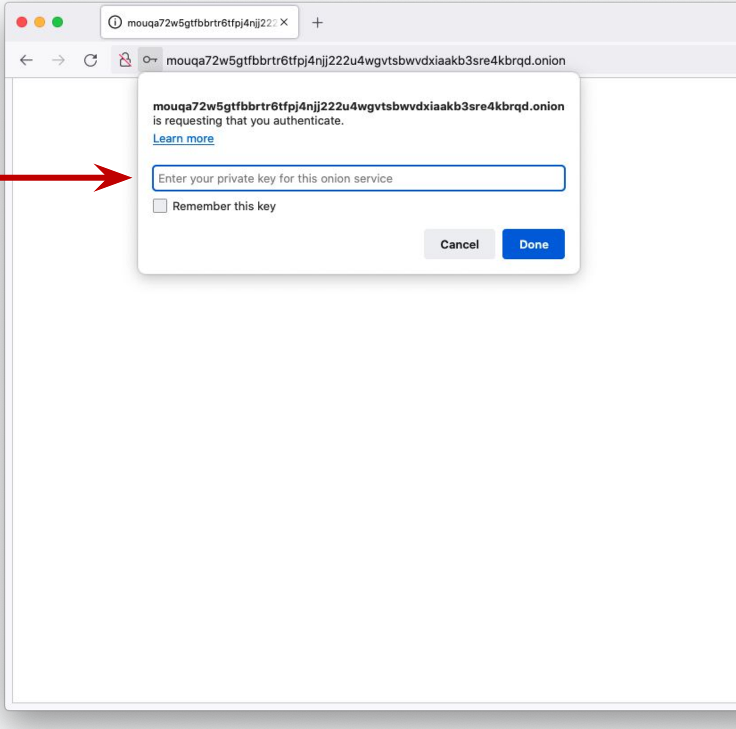
```
http://mouqa72w5gtfbbrtr6tfpj4njj222u4wgvtsbwvdxiaakb3sre4kbrqd.onion
```

Next, send the private key to allow access to your OnionShare service:

```
****************************************************
```

Step 6: Download through Tor Browser

- The recipient can download the file through Tor Browser by entering the address and key in the URL bar.
- Tip: you must keep your OnionShare window on your device open as long as you want people to download your file.



mouqa72w5gtfbbrtr6tfpj4njj222u4wgvtsbwvdxiaakb3sre4kbrqd.onion
is requesting that you authenticate.
Learn more

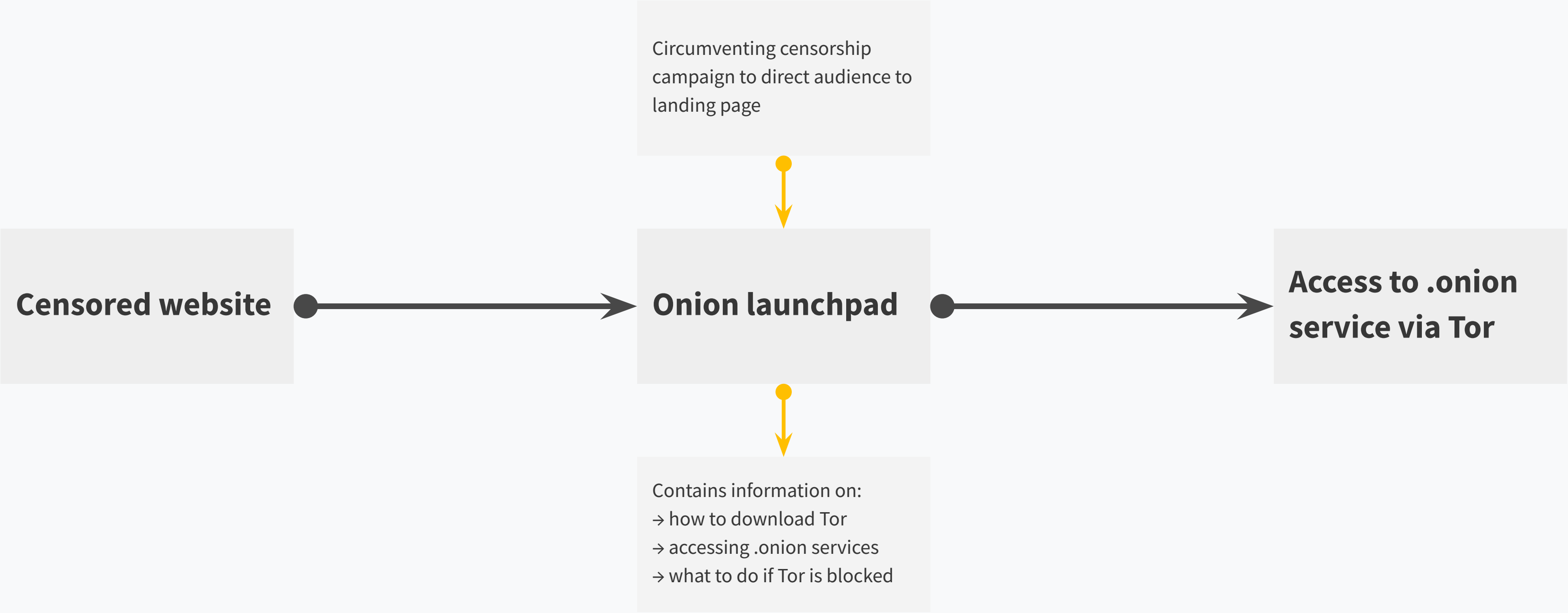
Enter your private key for this onion service

□ Remember this key

mouqa72w5gtfbbrtr6tfpj4njj22
mouqa72w5gtfbbrtr6tfpj4njj222u4wgvtsbwvdxiaakb3sre4kbrqd.onion
Cancel
Done

How the Tor Project can support you with Onion Servicing

Onion Service landing page



Circumventing censorship campaign to direct audience to landing page

Censored website

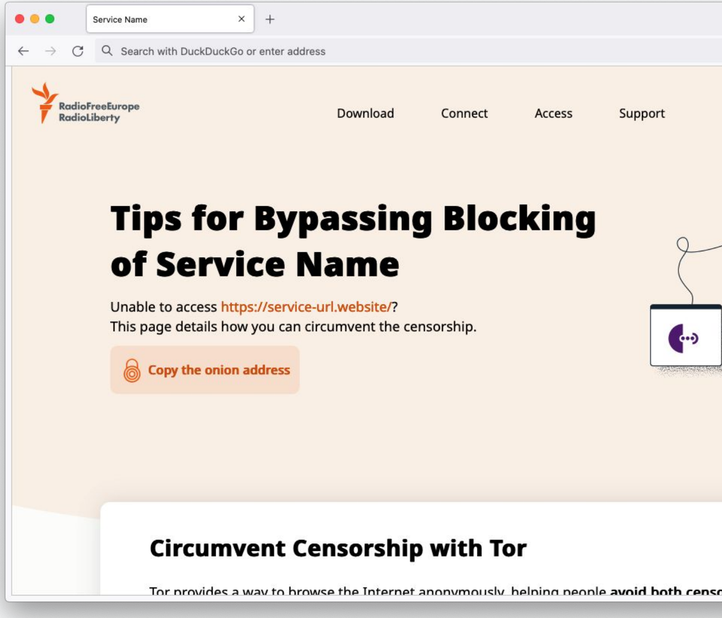
Onion launchpad

Access to .onion service via Tor

Contains information on:
→ how to download Tor
→ accessing .onion services
→ what to do if Tor is blocked

Onion Service landing page

- Landing page explains how to download and connect to Tor, and how to access the Onion Services.
- Content available in over 60 languages!
- Open source project that you can customize: https://gitlab.torproject.org/tpo/onion-services/sponsor123-landing-page



Service Name
Search with DuckDuckGo or enter address
RadioFreeEurope RadioLiberty
Download
Connect
Access
Support

Tips for Bypassing Blocking of Service Name

Unable to access https://service-url.website/?
This page details how you can circumvent the censorship.

Circumvent Censorship with Tor

Tor provides a way to browse the Internet anonymously, helping people **avoid both censo**

Useful links

- Tor Project Forum: https://forum.torproject.net/c/support/onion-services
- Tor Browser Manual: https://tb-manual.torproject.org
- Support portal: https://support.torproject.org/
- Community team: https://community.torproject.org/onion-services/

Onionize your workflow

that lets you securely anonymously share files, host websites, and chat with friends using the Tor network.

onionshare.org

securedrop.org

```
https://community.torproject.org/onion-services/advanced/opsec/
```

Grow your onion

anywhere, nor does you

From the network's point of view, the onion service is any other Tor client. That means onion service operators don't need to worry about having their server IP address linked, flagged, or blocklisted as part of the Tor network.

For more information about onion services, read Tor Project's Community portal:

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

IDENTIFY THE ONION

.onion TLD
The address of an onion service is automatically generated, so the operators do not need to purchase a domain name; the .onion URL also helps Tor ensure that it is connecting to the right location and that the connection is not being tampered with.

Onion icon
The tiny onion icon can help you to identify Onion services. Look for it in Tor Browser.

Onion address
An onion address is a string of 56 (and in V2 format, 16) mostly random letters and numbers, followed by ".onion". All traffic between Tor users and onion services is end-to-end encrypted, so you do not need to worry about connecting over HTTPS.

GROW YOUR ONION

How to set up an onion service for your website on Debian based Operating System.

! Note: The symbol # refers to running the code as root.

Get a working Tor

To configure Tor package repository enable the Torproject package repository by following these instructions:

1. Install apt-transport-https

To enable all package managers using the libapt-pkg library to access metadata and packages available in sources accessible over https (Hypertext Transfer Protocol Secure).

```
# apt install apt-transport-https
```

Add the following entries to /etc/apt/ ... or a new file in /etc/apt/

```
...roject.org
```

Configure your Tor onion service

The next step is opening the config file of Tor (torrc) and doing the appropriate configurations to setup an onion service. Depending on your operating system and setup, your Tor configuration file can be at a different location or look different.

You will need to put the following two lines in your torrc file:

```
HiddenServiceDir /var/lib/tor/onion_service/
HiddenServicePort 80 127.0.0.1:80
```

Now save your torrc and restart Tor.

```
$ sudo systemctl tor restart
```

If Tor starts up again, great. Otherwise, something is wrong. First look at your logfiles for hints.

Edit website configuration file

If you're running multiple onion sites on the same web server, remember to edit your web server virtual host file and add the onion address for each website.

...service works

... go to your ... file named

WHY USE ONIONS?

Decentralization
There's no central authority that approves or rejects onion services. The address of an onion service is automatically generated. Operators don't use the regular DNS infrastructure and do not need to purchase or register a domain name.

Metadata obfuscation or 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.

Network sustainability
Onion services don't use the same circuit path as regular Tor connections. The traffic generated by them doesn't leave the Tor network, and therefore, these onion circuits free up Exit relay bandwidth for others. Beyond that, when a service is available over onion ... diversity to the Tor network. It uses a ... the network, avoiding exit

Freedom of press and censorship circumvention
Regular Tor connections already provide censorship circumvention, but only onion services can anonymize both parts of communication - users and provider -, creating a metadata free communication between the user of the service and the service itself.

Censorship technologies are being deployed by different actors, like governments and Internet providers, worldwide to block access to free press and privacy tools.

To protect freedom of speech and freedom of opinion in censored spaces, major media organizations have made their websites available over onion services in the last few years.

That's the case of NY Times, ProPublica, Deutsche Welle, BBC, The Markup and other newsrooms.

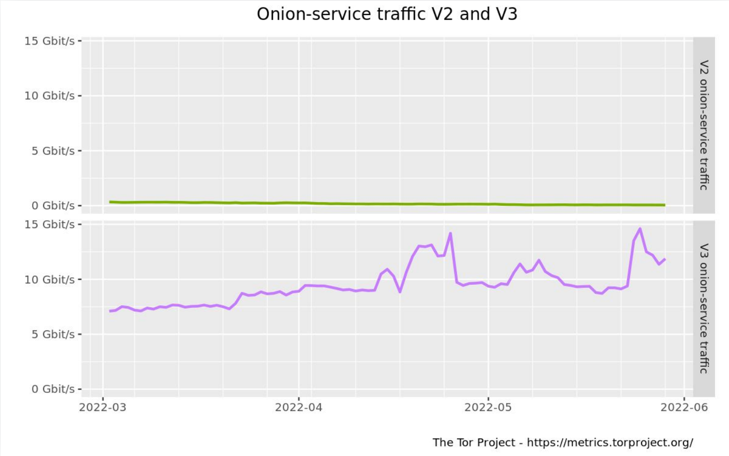
Protect sources, whistleblowers, and journalists
Many journalists and media organizations use tools based on onion services to protect their sources. They share and accept documents from anonymous sources using tools like SecureDrop, GlobaLeaks, or OnionShare.

...ate users about privacy by design
... an excellent example of privacy by ... is secure and ... available

Latest developments

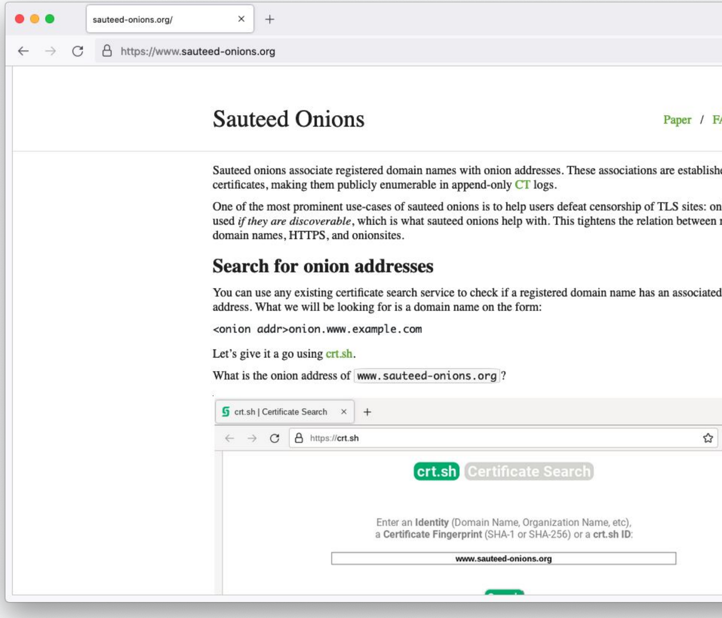
Version 3 of Onion Services

- Version 3 of Onion Services launched in 2018.
- Most Onion Service operators have migrated.
- More on version 2 deprecation: https://blog.torproject.org/v2-deprecation-timeline/



Sauteed Onions

- Sauteed onions improve transparency and discoverability of Onion Services.
- Sauteed onions associate registered domain names with onion addresses, via TLS certificates.
- “Sauteed” because when onions are cooked they become transparent!



Sauteed Onions

Sauteed onions associate registered domain names with onion addresses. These associations are establish certificates, making them publicly enumerable in append-only CT logs.

One of the most prominent use-cases of sauteed onions is to help users defeat censorship of TLS sites: on used *if they are discoverable*, which is what sauteed onions help with. This tightens the relation between domain names, HTTPS, and onionsites.

Search for onion addresses

You can use any existing certificate search service to check if a registered domain name has an associated address. What we will be looking for is a domain name on the form:

```
<onion addr>onion.www.example.com
```

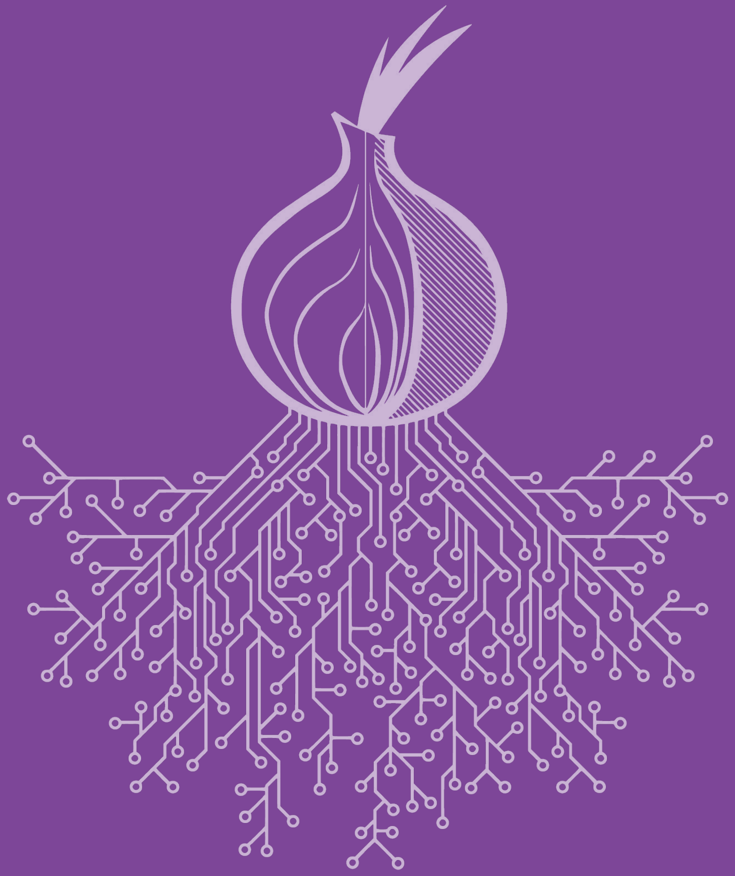
Let’s give it a go using crt.sh.

What is the onion address of `www.sauteed-onions.org`?

Enter an **Identity** (Domain Name, Organization Name, etc), a **Certificate Fingerprint** (SHA-1 or SHA-256) or a **crt.sh ID**:

www.sauteed-onions.org

Thank you!



torprojectorg