ONIONIZE YOUR WORKFLOW

SHARE FILES SECURELY AND PUBLISH CONTENT USING ONIONSHARE

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

onionshare.org

SHARE AND ACCEPT DOCUMENTS SECURELY WITH SECUREDROP

SecureDrop is an open source whistleblower submission system that media organizations and NGOs can install to securely accept documents from anonymous sources.

securedrop.org

HAVE METADATA FREE COMMUNICATIONS WITH RICCOCHET

Ricochet Refresh is a peer-to-peer messenger app that uses Tor to connect clients. When you start Ricochet Refresh it creates a Tor onion service on your computer.

ricochetrefresh.net

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

Grow your onion

THE FUTURE IS CYBERFEMINIST

Fernanda runs a women's collective focused on reproductive rights in Brazil, where abortion is criminalized. Fernanda and her colleagues built a website with information about abortion access, birth control, and other resources for people seeking reproductive information. If this website were linked back to them, they might be arrested or worse.

So Fernanda and her colleagues created the website using Tor onion services, which not only **protects them from being discovered as the operators of the server**, but helps **protect visitors to their website** by requiring that they use Tor Browser.

HOW DO ONION SERVICES WORK?

A potential adopter has probably already heard about the Tor Project, the network and even Tor relays, and that's great! But onion services aren't like a Tor relay in the network.

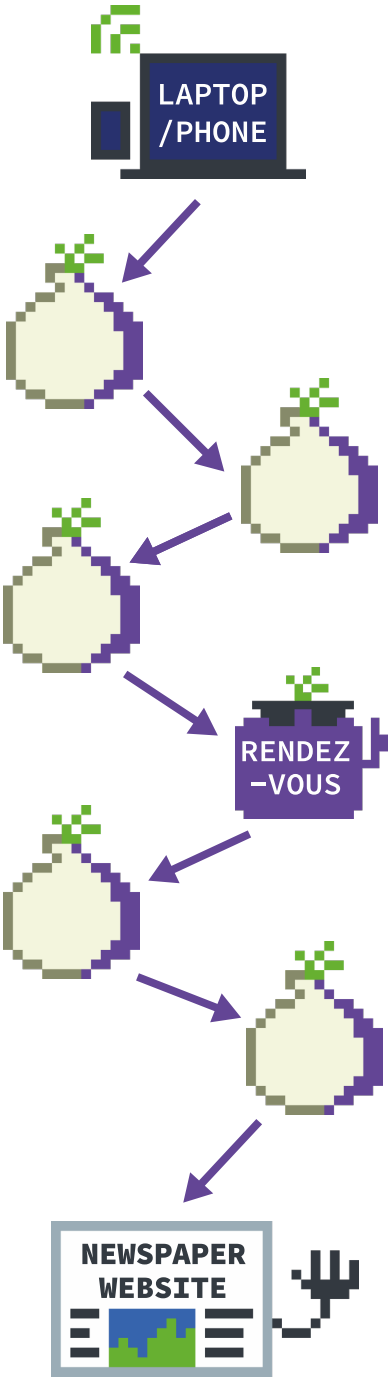
A Tor Onion Service connects to rendezvous nodes in the tor network; a client connection to the onion service does the same. This means that connections from the client to the server never leave the Tor network.

In contrast to running a Tor relay, running a Tor Onion Service does not result in your IP address being publicly listed anywhere, nor does your service relay other Tor traffic.

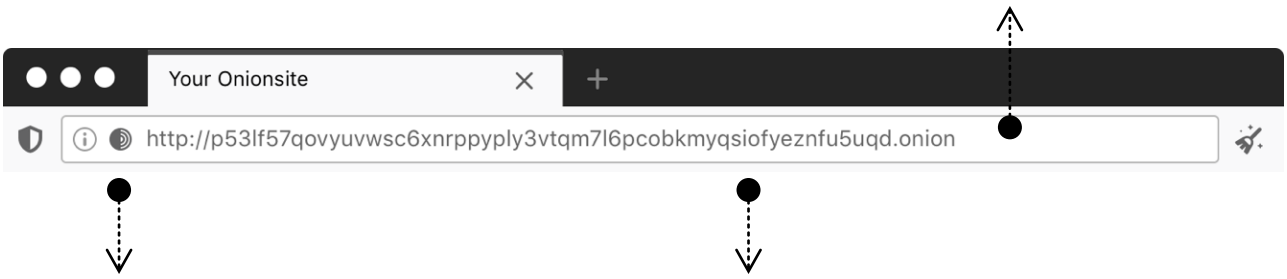
From the network's point of view, the onion service looks like any other Tor client. That means onion service operators don't need to worry about having their server IP address linked, flagged, or blocklisted as part of the Tor network.

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

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



IDENTIFY THE ONION



Onion icon

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

.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 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
```

2. Add the following entries to /etc/apt/sources.list or a new file in /etc/apt/sources.list.d/

```
deb https://deb.torproject.org/torproject.org buster main
deb-src https://deb.torproject.org/torproject.org buster main
```

3. Then add the gpg key used to sign the packages by running the following commands at your command prompt

```
# wget -qO- https://deb.torproject.org/torproject.org/A3C4F0F979CAA22CDBA8F512EE8CBC9E886DDD89.asc | gpg --import
# gpg --export A3C4F0F979CAA22CDBA8F512EE8CBC9E886DDD89 | apt-key add -
```

4. Install tor and tor debian keyring

We provide a Debian package to help you keep our signing key current. It is recommended you use it. Install it with the following commands:

```
# apt update
# apt install tor deb.torproject.org-keyring
```

Get a web server working

Nginx is available in the main repository of multiple Linux and *BSD distributions.
To install nginx package:

```
$ sudo apt install nginx
```

By default, the web server will be running on localhost:80 at the end of the installation.

Once your web server is set up, make sure it works: open your browser and go to http://localhost/. Then try putting a file in the main html directory, and make sure it shows up when you access the site.

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 restart tor
```

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.

Test that your onion service works

Now to get your onion service address, go to your HiddenServiceDir directory, and find a file named hostname. The hostname file in your onion service configuration directory contains the hostname for your new onion v3 service. The other files are your onion service keys, so it is imperative that these are kept private.

If your keys leak, other people can impersonate your onion service, deeming it compromised, useless, and dangerous to visit.

Now you can connect to your onion service using Tor Browser!

More Resources

As a next step, you might want to enable Onion-Location and advertise your onion site to all Tor Browser users, when they visit your website:

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

If it's your friend first time using onion services, share with them the Tor Browser User Manual:

`https://tb-manual.torproject.org/onion-services/`

It's also possible to make a very private onion service, protected by a private key and user authorization. Learn more:

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

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 services, it adds diversity to the Tor network. It uses a different set of circuits on the network, avoiding exit relays altogether.

Level up your service privacy
Beyond websites and onion sites, it's possible to do many things with onion services, for example, email.

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.

Educate users about privacy by design
Onion services are an excellent example of privacy by design technology, where one is secure and anonymous by default. Making your service available over onion services is an opportunity to educate the general public about Tor and how a more secure way to access the internet looks like: easy as browsing a web page.

Remember, an onion a day keeps the surveillance away!