3 WAYS TO ACCESS THE DARK WEB (TOR NETWORK) FOR SECURITY REASERCH

By Mohammed Choglay

Contents

Ethical and Legal Notice

The report aims to show the most secure way to access the dark web for security research. Utilising Tor or accessing the dark web is not illegal in itself. However, it is unlawful to carry out any illicit acts anonymously. To irritate, you will be held responsible for the actions that you carry.

Also, if you consider using the dark web, you need to use it ethically and have a valid reason if you don't stick to Chrome.

This document is intended to provide guidance on securely accessing the dark web for research purposes only. It is important to note that we do not condone, endorse, or support any illegal activities, including but not limited to hacking, cybercrime, illegal drug trafficking, illegal arms trade, or any other unlawful actions on the dark web. Any such activities are strictly prohibited and are subject to prosecution under the law.

What is the tor browser?

The Tor browser is a browser that focuses on anonymity by hiding your IP and browsing activity. This is achieved by ensuring the network traffic is redirected through multiple routers. These are defined as nodes.

In a more general sense, this is like a regular web browser that can view standard websites like Chrome and Firefox (e.g. .co.uk, .com, etc.) but can view the dark web, which is an onion link. The top-level domain for this is: **.onion**

Example domain	Example Type
https://www.bbc.co.uk	Clear Net Domain Example
https://www.bbcweb3hytmzhn5d532owbu6oqadra5z3ar726vq5kgwwn6aucdccrad.onion	Dark Web Domain Example
https://hfhjsfjhdjsjfgvgdhxjfbdfhdjfy8488374dhsafuhffduhdufshg.onion	Dark Web Domain Example

Installing Tor

To install Tor:

1. Utilise a web browser to navigate to the. You will be presented with four different operating systems.
2. Download the operating system you require for our cause Windows will be used.
3. Ensure that you verify the signature of the download to ensure the application has not been tampered with or compromised.

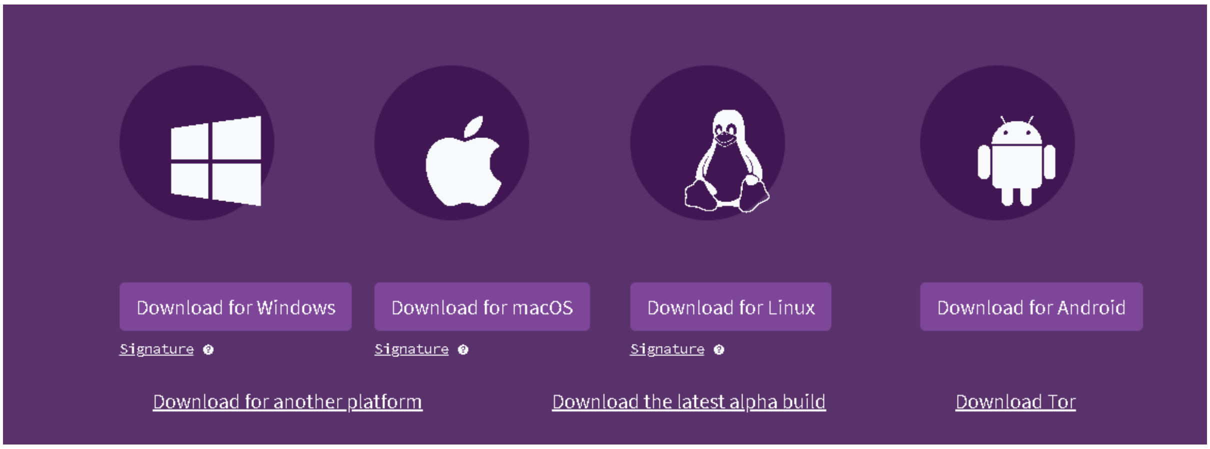
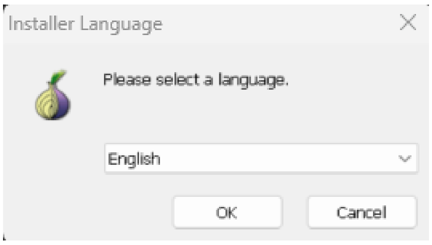


Figure 1 – OS the Tor project support

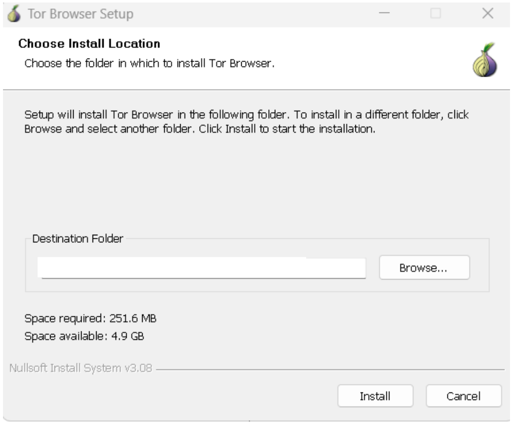
The main installation procedure is simple. Please start by selecting your chosen language and then the destination path of where you want to install it. The final step is paramount as you need to ensure you don't want to run the Tor browser yet, so ensure it is untoggled.



Installer Language

Please select a language.

English



Tor Browser Setup

Choose Install Location

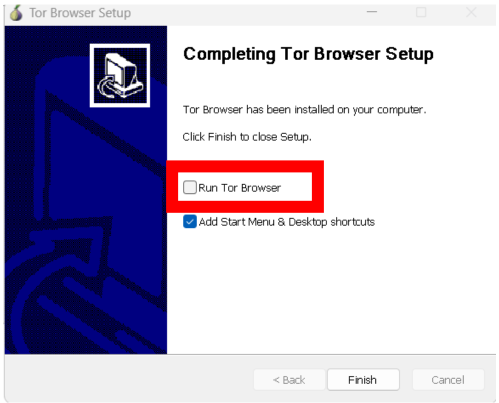
Choose the folder in which to install Tor Browser.

Setup will install Tor Browser in the following folder. To install in a different folder, click Browse and select another folder. Click Install to start the installation.

Destination Folder

Space required: 251.6 MB
Space available: 4.9 GB

Nullsoft Install System v3.08



Tor Browser Setup

Completing Tor Browser Setup

Tor Browser has been installed on your computer.

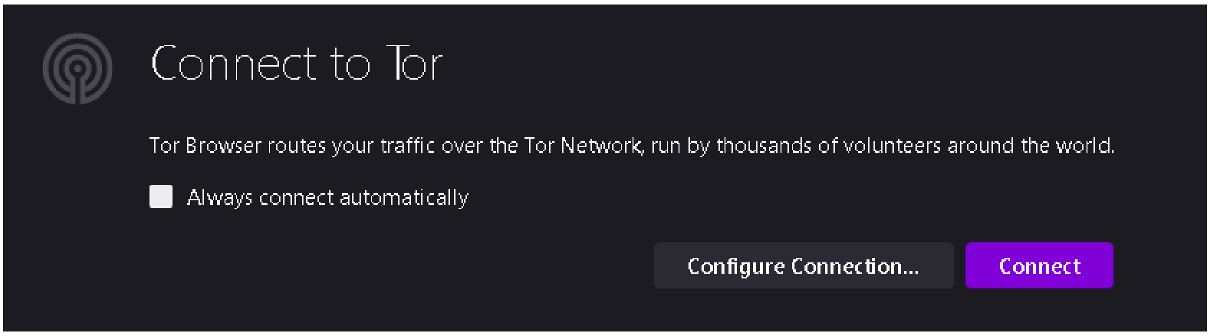
Click Finish to close Setup.

□ Run Tor Browser

☑ Add Start Menu & Desktop shortcuts

The default way (Level 1)

Now that Tor is installed, you can just run the Tor browser and start your connection by clicking the purple connect button on launch to access onion links (dark web pages). However, there are more secure ways to go about it.



Connect to Tor

Tor Browser routes your traffic over the Tor Network, run by thousands of volunteers around the world.

□ Always connect automatically

Figure 2 - button for tor connection

Using the diagram below, you see that you're exposing yourself as you connect to the first onion router, as your IP (internet protocol) is not masked with a VPN. This means you don't have complete anonymity, as your ISP will know you are using Tor even though you have two more onion routers/nodes in place.

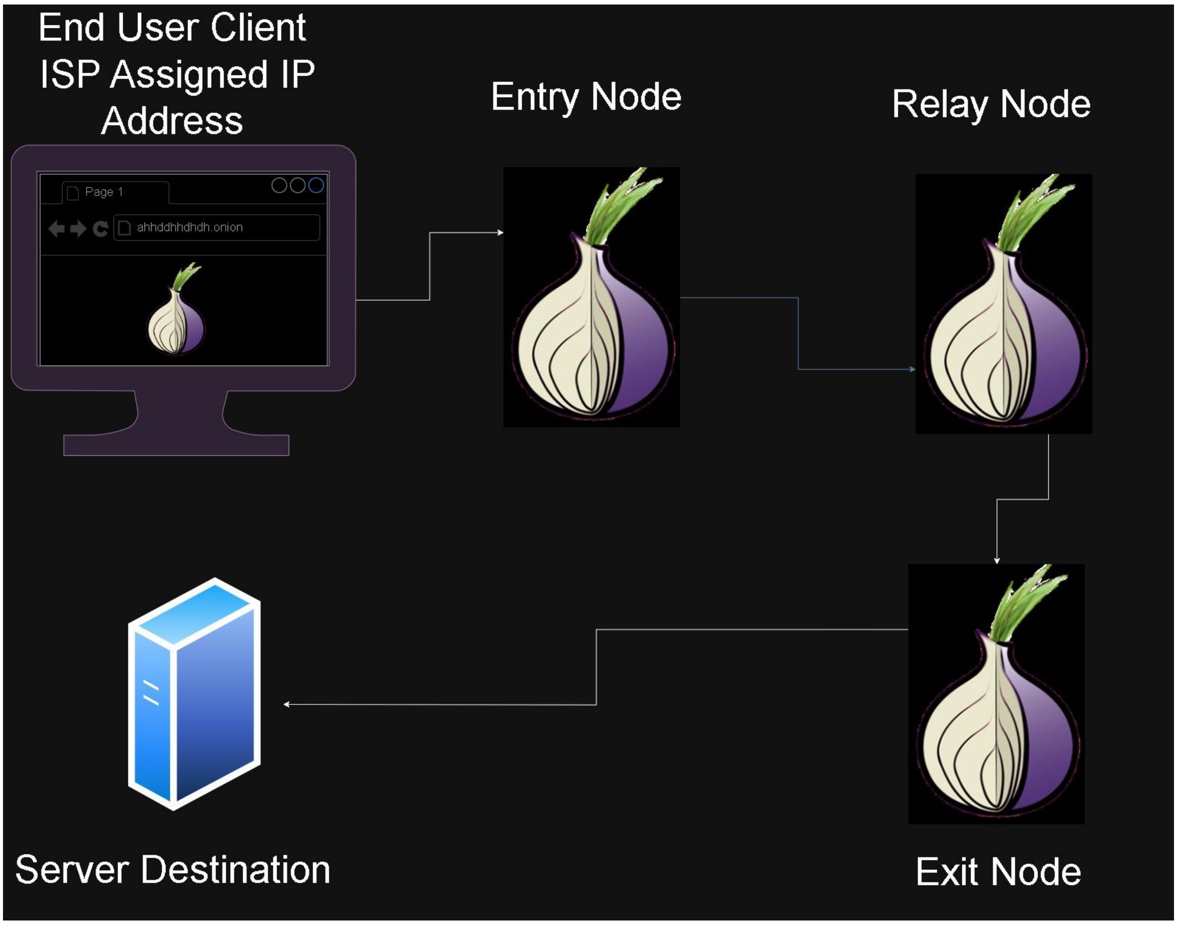


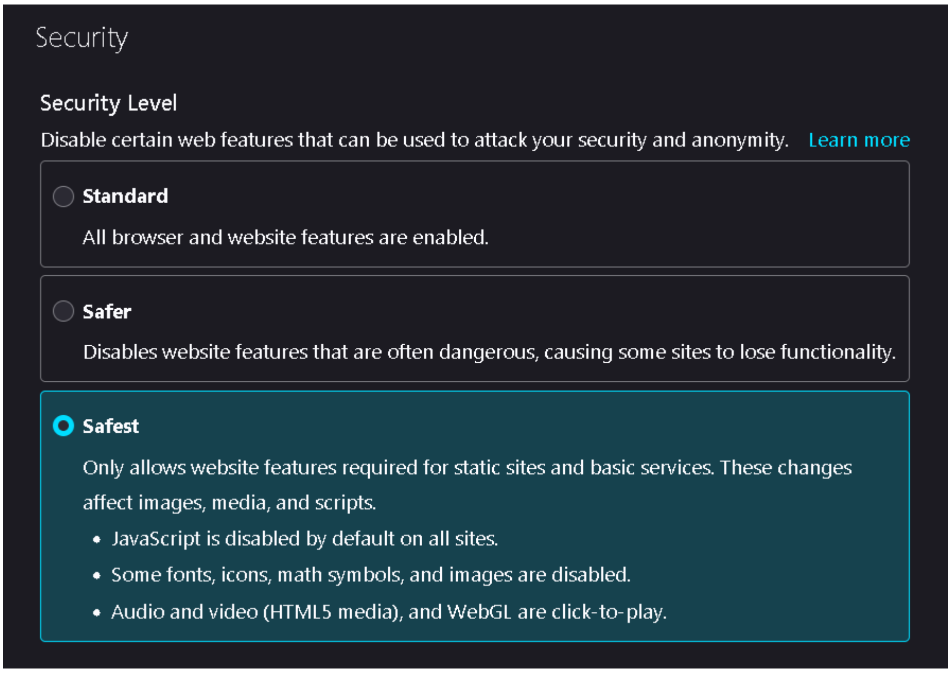
Figure 3 - Diagram of tor connection without VPN

When it comes to good OpSec (operational security), don't be lazy because this can lead to your being hacked or traced on the dark web. So, always take the safest option if feasible.

VPN and security setting configuration (Level 2)

The second securest way is to utilise a VPN to mask your IP address before opening and connecting to Tor. Once that's done, you want to select 'configure connection' on launch. Then select the 'privacy and security' option on the left-hand side, and then under 'security', select 'safest'. Once done, you can initiate the tor connection by pressing the purple 'connect' button shown in Figure 2 above.

In Figure 4 the settings are set to safest because this will ensure that every visit is static. This will turn off certain features on the website as certain threat actors may use malicious tactics on the dark web that can have harmful effects.



Security

Security Level

Disable certain web features that can be used to attack your security and anonymity. Learn more

○ **Standard**

All browser and website features are enabled.

○ **Safer**

Disables website features that are often dangerous, causing some sites to lose functionality.

● **Safest**

Only allows website features required for static sites and basic services. These changes affect images, media, and scripts.

- JavaScript is disabled by default on all sites.
- Some fonts, icons, math symbols, and images are disabled.
- Audio and video (HTML5 media), and WebGL are click-to-play.

Figure 4 - safest security setting

Now that a VPN is being utilised, you have an extra layer of protection which does not compromise you. This provides you with correct anonymity; even your ISP does not know you are using the Tor network.

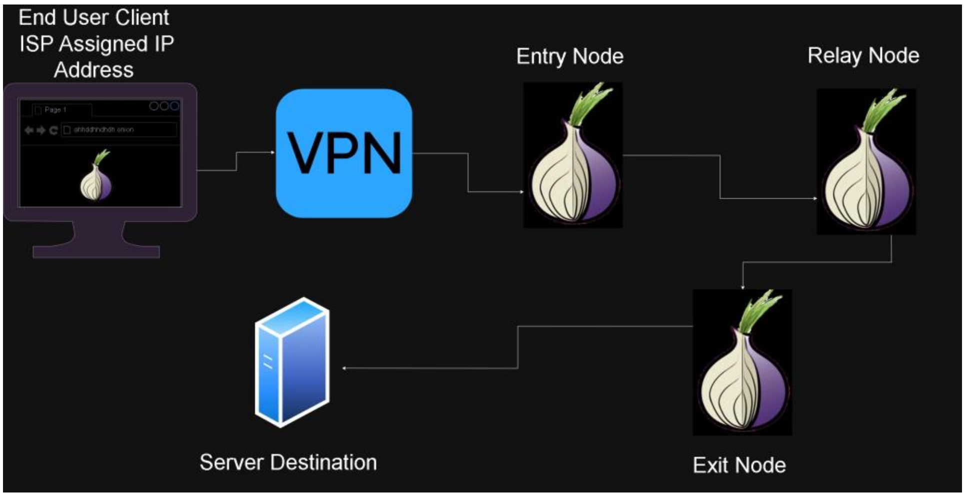


Figure 5 - Diagram of tor connection with VPN

Tails (Level 3)

The securest way of using Tor is a unique OS (operating system) known as "Tails". This OS works by running from memory once booted from the USB. Once booted in from the USB, the whole system runs from memory, so nothing is permanently stored as RAM is volatile, and tails is made to be "amnesic".

The installation process of tails:

1. To install tails, head over to their website.
2. Verify your download to ensure it's trusted. Use tails file upload check or use OpenPGP signatures.
3. Download "balenaEtcher" for Windows (used to burn images to disks and USB). If you use a different OS, you may need to find an alternative, as the application might not be compatible.
4. Open "balenaEtcher", select an image file, select the target USB and press "flash".
5. Once flashed, bosh, you are done. Just plug the USB into the computer and boot from the USB.
6. Remember to connect to a VPN before connecting to TOR. So, you use the browser to download a VPN.