**Tor Browser**

**Cyber Intel**

# Executive Summary

The Tor Browser is a free and open-source web browser that provides users with anonymity, privacy protection, and the ability to bypass censorship. This report explores the scope, features, and limitations of Tor Browser. The report highlights that Tor Browser allows users to browse the internet anonymously by routing their traffic through a network of volunteer-operated relays. It encrypts data multiple times, making it challenging for anyone monitoring online activities to trace them back to the user. The browser also offers access to websites on the dark web or deep web, although caution should be exercised due to associated risks.

This report explores how to install Tor Browser, connection to Tor Network and viewing Tor Circuit. This report also includes advanced Tor Browser settings like connecting to built-in Bridges, connection to Tor Network using a proxy and viewing browser logs.

# Index

[**Executive Summary 2**](#_xp7yznorkjzb)

[**Index 2**](#_raps74n1txlm)

[**1. Introduction 2**](#_hrm9ydutbi2c)

[**2. Tool Details 2**](#_qg8ihxnbvis5)

[**3. Installation 3**](#_rdib537dfb4r)

[**4. Execution 3**](#_2z3me3opwt4e)

[**5. Scope and Limitations 3**](#_9f1twuiulcq7)

[**6. Conclusion 3**](#_8kvf4t1kjyqg)

[**7. References (if any) 4**](#_dsefb4qutzic)

# Introduction

The Tor Browser is a free and open-source web browser that allows users to browse the internet anonymously. It is based on the Mozilla Firefox web browser and focuses on privacy, security, and circumventing online censorship.

Tor stands for The Onion Router, which refers to the layered encryption used by the network. When using Tor Browser, your internet traffic is routed through a series of volunteer-operated servers called nodes or relays. Each relay only knows about the previous node and next node in the chain, ensuring that no single server can see both ends of your connection.

This routing process helps protect your identity as it becomes difficult for anyone monitoring your internet activity to trace it back to you. Additionally, Tor Browser also encrypts your data multiple times before sending it over the network, further enhancing security.

One key feature of Tor Browser is its ability to access websites on the dark web or deep web. These are parts of the internet not indexed by search engines and often associated with illegal activities. While not all content on these networks is illegal or harmful, caution should be exercised when accessing them due to their reputation.

# Tool Details

Tool available at – <https://www.torproject.org/>

Accessed –

* using Microsoft Edge
* on 24 September 2023
* no VPN required

Use case list –

1. Anonymous browsing: Tor Browser allows users to browse the internet anonymously, concealing their IP address and making it difficult for websites or entities to track their online activities.

2. Circumventing censorship: In countries where certain websites or content are blocked or censored, Tor Browser can be used to bypass these restrictions and access information freely.

3. Online privacy protection: With growing concerns about data collection by governments and corporations, using Tor Browser helps safeguard personal information from being tracked or monitored by third parties.

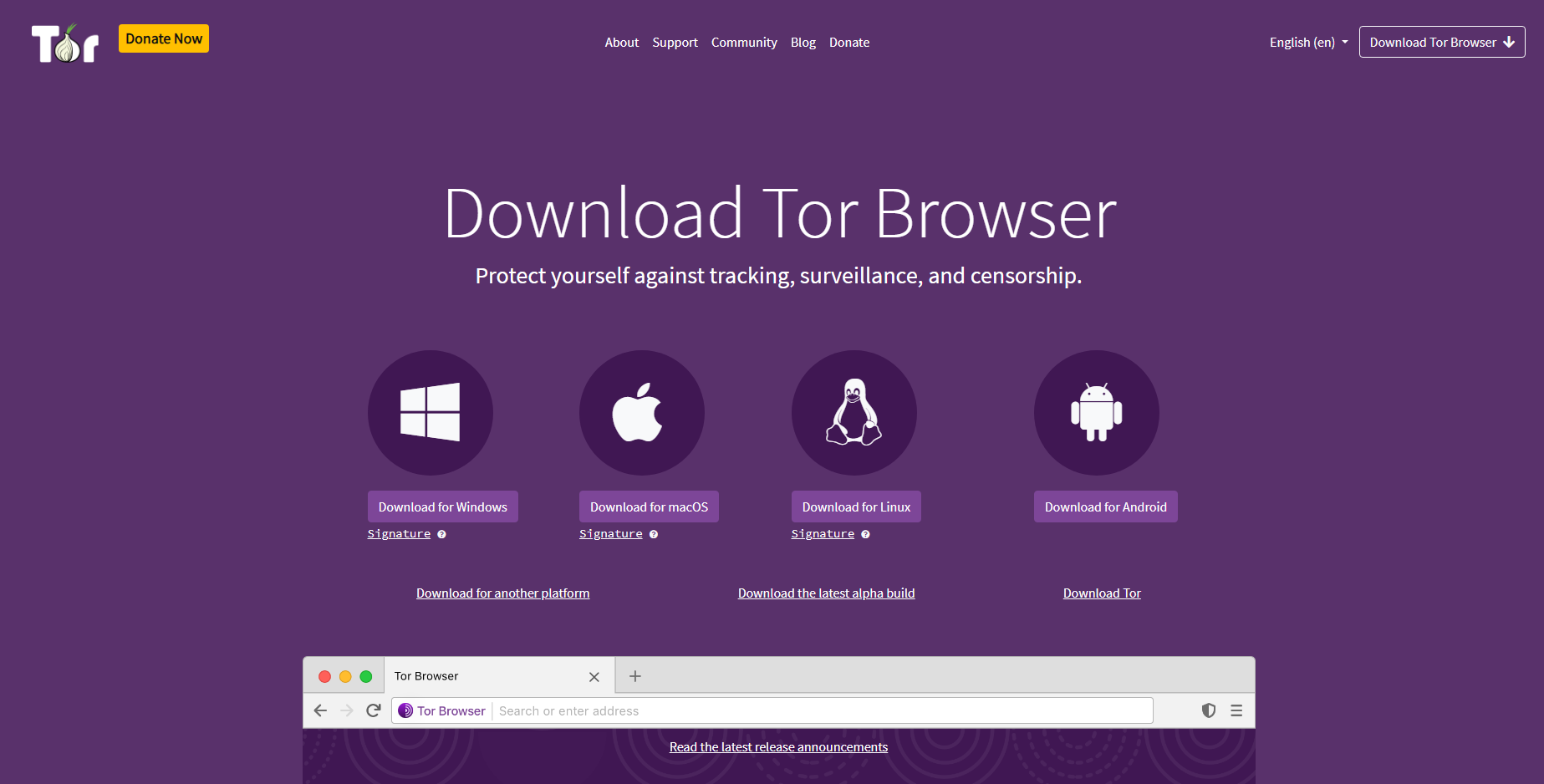
4. Accessing the dark web safely: While caution is advised when exploring the dark web due to its association with illegal activities, individuals may still choose to visit specific sites on these networks that provide valuable information without compromising their anonymity.

Other use cases include –

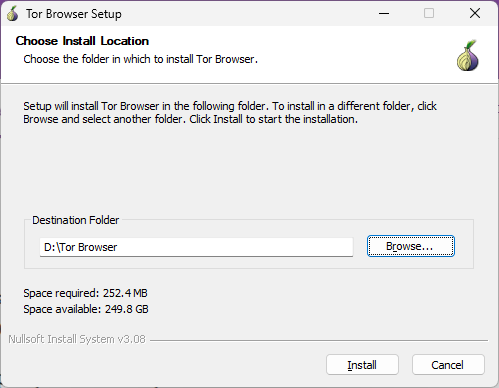
* Researching sensitive subjects
* Secure communication
* Protecting financial transactions
* Testing website accessibility globally
* Evading targeted advertising

# Installation

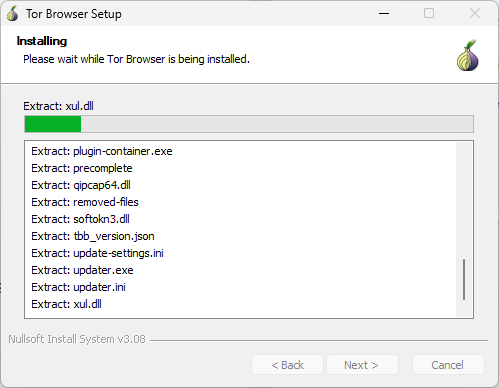
* Navigate to <https://www.torproject.org/download/> and download the executable pack for the operating system running on the device.

****

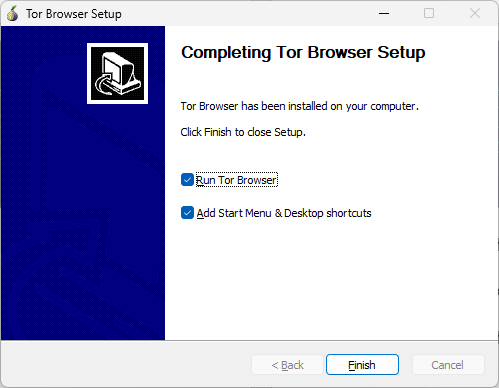
* After running the executable file, select the language and give the path to download Tor Browser.

****

* The installation starts

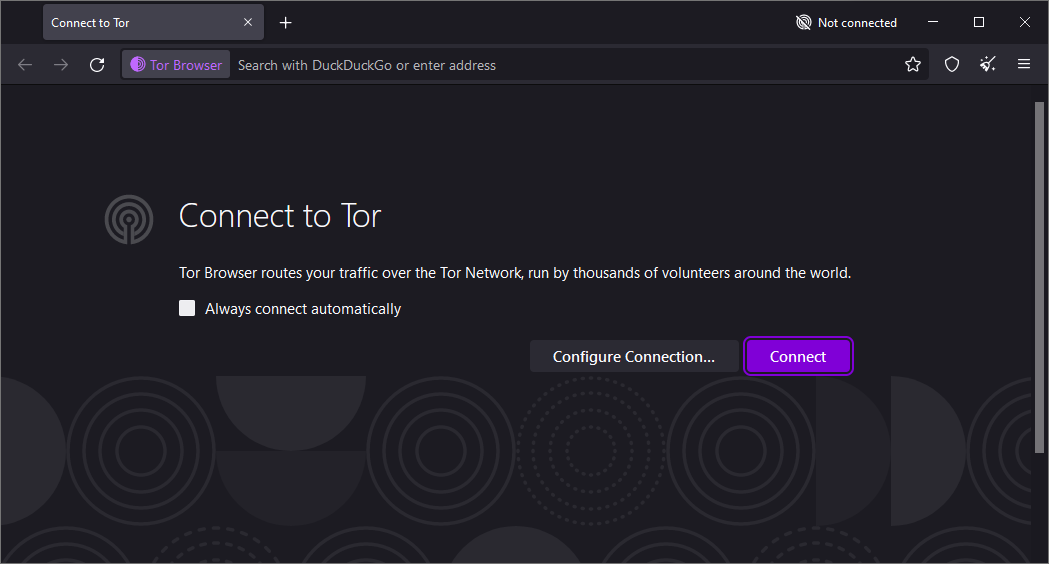
****

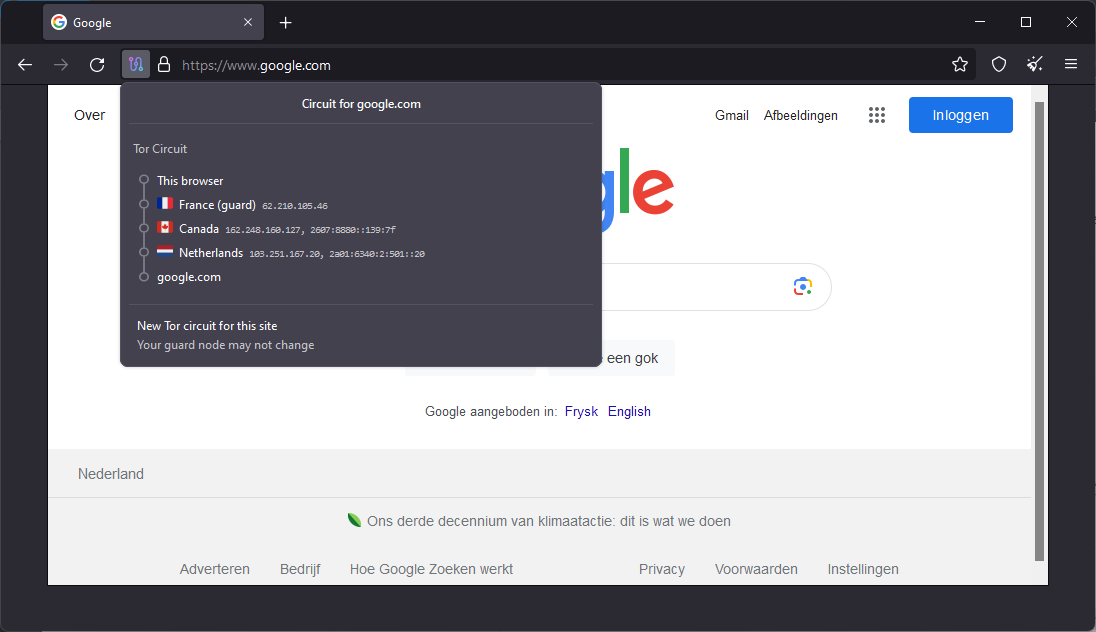
* After some time, the browser will be installed

****

# Execution

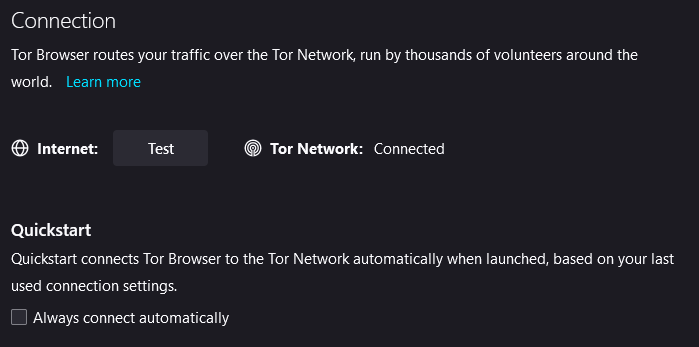
* After opening the Tor Browser, click on connect to start the Tor circuit –



* After connection is successful visit any site and click on the Tor circuit to view the locations/IPs from which data passes.

Exploring Tor settings in Tor Browser –

* Connection to Tor Network and Quickstart Auto-connect: The major differences between a normal browser and the Tor browser is its functionality to connect to Tor Network. The Tor browser allows to connect to Toe Network automatically on startup or on user input.

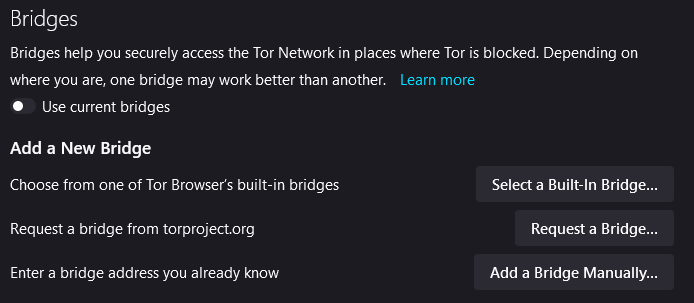


* Bridges in Tor Browser –

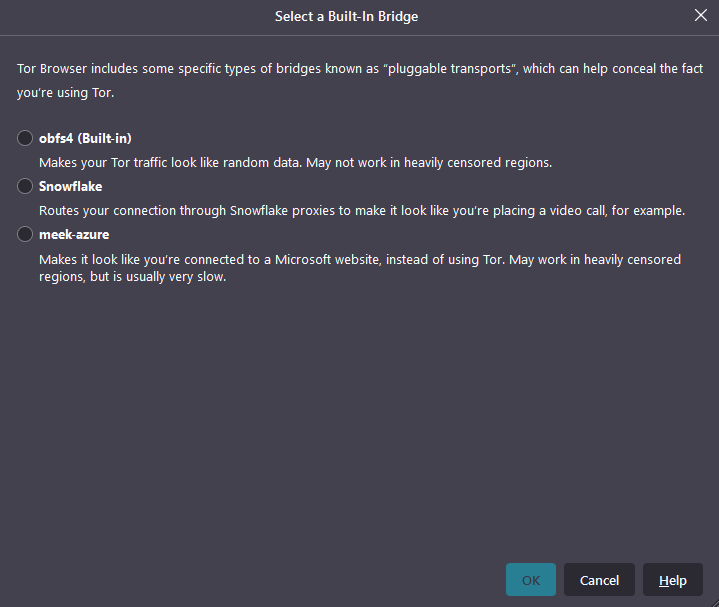
Bridges in Tor Browser are a feature that helps users overcome censorship and access the Tor network when standard entry points, known as "public relays," are blocked or restricted. In some countries or networks, authorities may actively block access to public relays, making it difficult to connect to the Tor network.

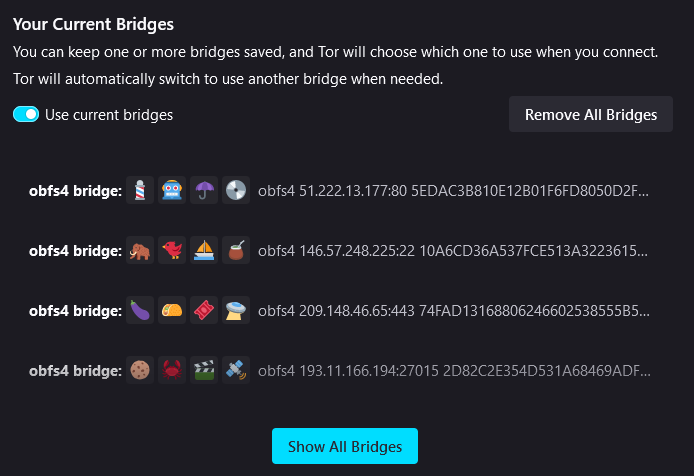
To address this issue, bridges act as alternative entry points that are not publicly listed. They provide an additional layer of obfuscation by disguising the fact that a user is connecting to the Tor network. By using bridges, users can bypass censorship measures and gain access to Tor even in restrictive environments.

Bridges work by allowing users to obtain unique bridge addresses from trusted sources outside of the censored network. These addresses are then entered into the Tor Browser's configuration settings, which instructs the browser to use these specific entry points instead of public relays.

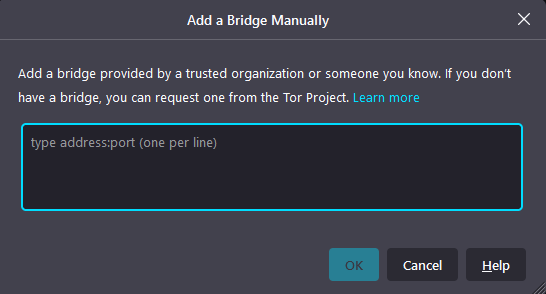


Selecting Tor Browser built-in Bridge –



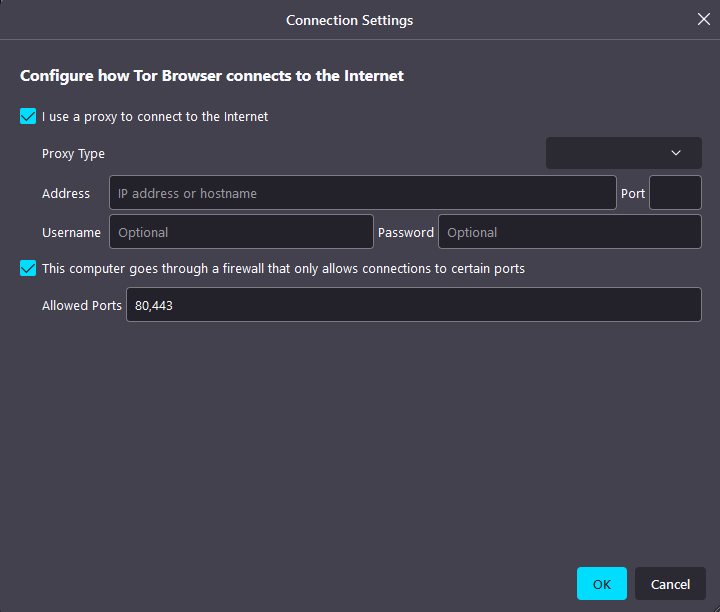


Connecting to a Bridge manually using address –

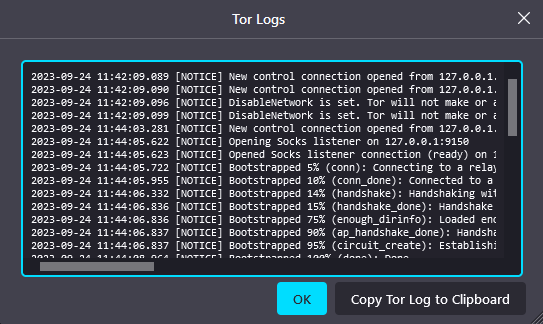


* Advanced Settings

Connecting Tor Network using proxy address –



Viewing Tor Logs –



# Scope and Limitations

Tor Browser offers users the ability to browse the internet anonymously, concealing their IP address and making it difficult for websites or entities to track their online activities. By routing internet traffic through a series of encrypted relays, Tor Browser helps protect user privacy and prevents third parties from monitoring or intercepting data. Tor Browser can be used to circumvent censorship imposed by governments or organizations, allowing users to access blocked websites and content freely. Tor Browser enables private and secure communication channels that are resistant to surveillance using built-in encryption and secure services. Tor Browser helps prevent advertisers, data brokers, and other entities from tracking user behaviour across different websites

Due to the multi-layered encryption process utilized by the network, browsing speed may be slower compared to regular browsers as data has to pass through multiple nodes before reaching its destination. Some websites may block or restrict access from connections originating from known Tor exit nodes due to security concerns or attempts at preventing abuse on their platforms. While rare, there have been instances where malicious actors have set up rogue exit nodes in an attempt to monitor or manipulate traffic passing through them. This highlights the importance of only accessing trusted HTTPS-enabled sites when using Tor Browser.

# Conclusion

Tor Browser serves as a valuable tool for individuals seeking anonymity, privacy protection, and access to uncensored content on the internet. By routing internet traffic through a network of volunteer-operated relays, it enables users to browse the web anonymously and circumvent censorship imposed by governments or organizations. Tor Browser provides users with an effective means of maintaining their online privacy, accessing blocked websites or content freely, engaging in secure communication channels, and protecting against tracking and profiling.

# References

* <https://www.torproject.org/>