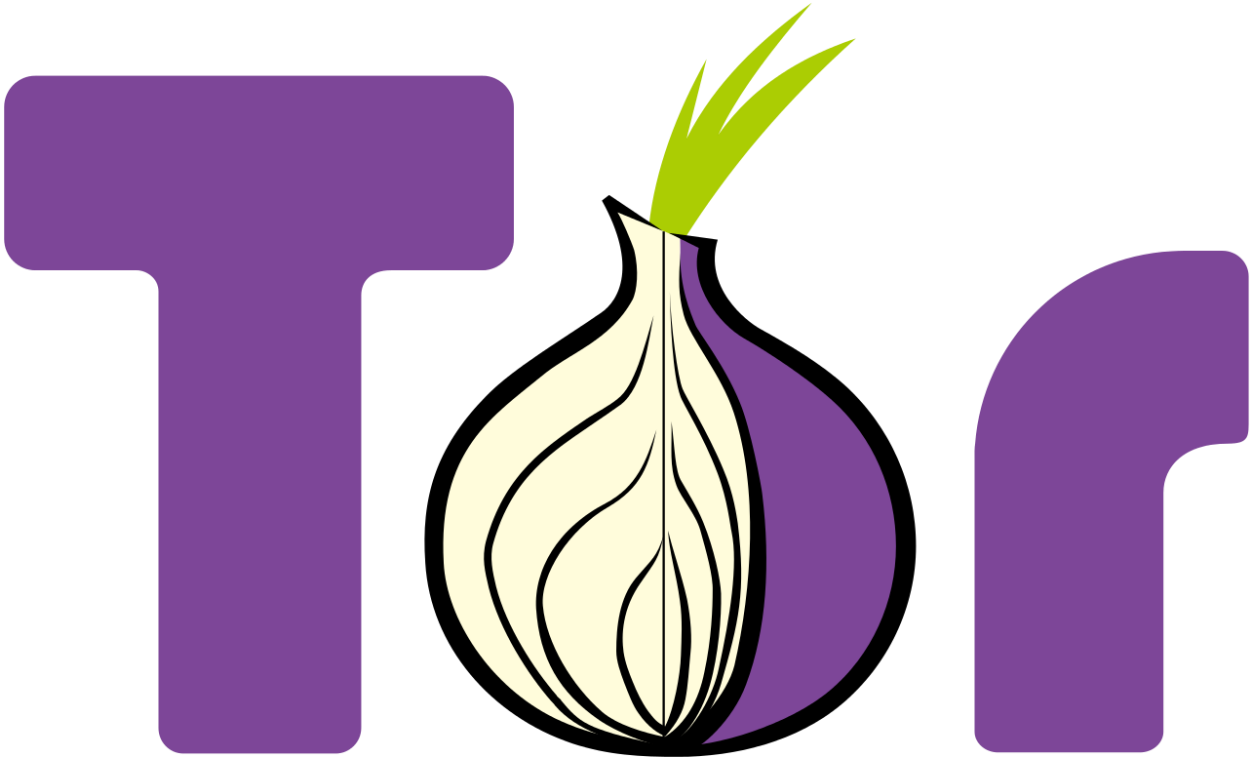
Layer of the Web Terminologies:

Tor:

TOR, Short for The Onion Routing. A network that provides anonymity and protects user privacy by routing traffic via a series of servers. Tor is a network of virtual tunnels that allows you to improve your privacy and security on the Internet. Tor routes traffic through a series of servers to hide the source of communications and protect user privacy and hide identity.

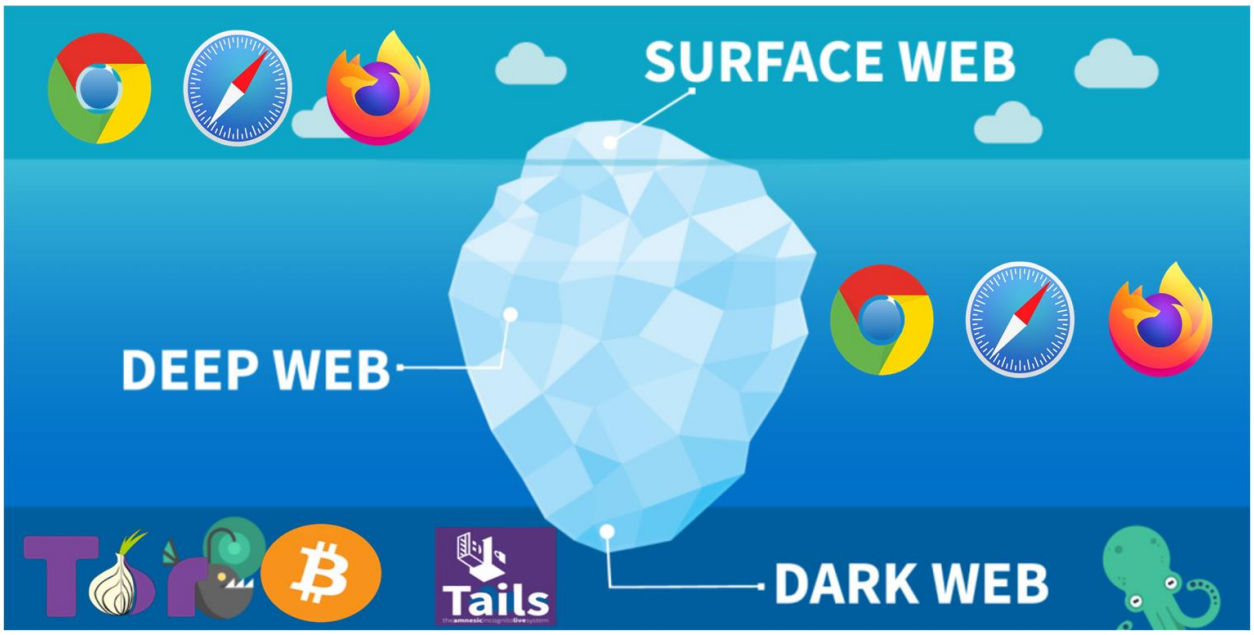


Tor Browser:

A web browser that implements the Tor network. Tor Browser prevents someone watching your connection from knowing what websites you visit. Tor Browser will block browser plugins such as Flash, RealPlayer, QuickTime, and others. browser is a web browser designed for anonymous web surfing and protection against traffic analysis. The Tor Browser hides your IP address and browsing activity by redirecting web traffic through a series of different routers known as nodes.

Onion:

A top-level domain (TLD) like .com and .org. A .onion domain consists of a hash of a public key and a .onion domain name. They are usually accessed only through a direct link. A top level Internet domain used by anonymous websites on the Dark Web. It is the website address that you can access only in the Tor anonymity browser.

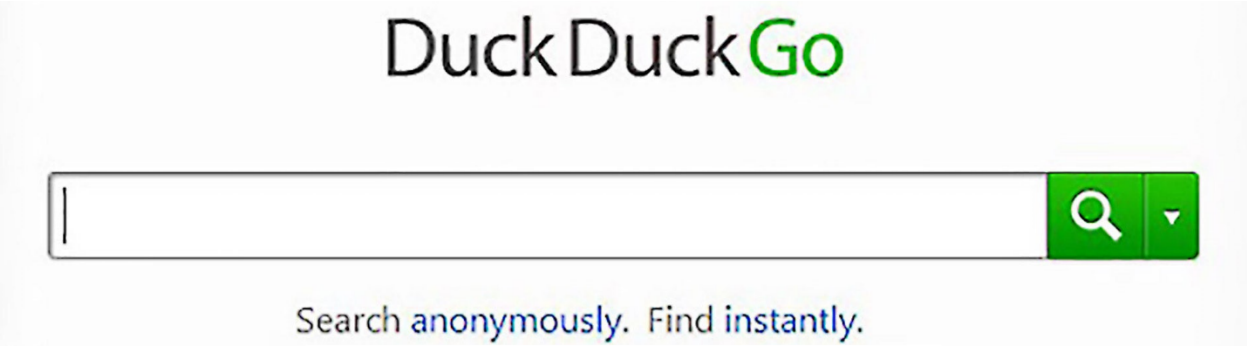


Tails OS:

Tails OS is used by journalists, activists, and others to keep their digital activity safe and anonymous. Tails is an operating system that's based on Debian Linux. You don't install it on your hard drive. It runs completely off of a USB thumb drive. Your work is temporarily stored in the RAM (Memory) of your computer. As soon as you shut your computer down, your RAM is empty, nothing is stored, and everything is forgotten. No traces are left on your computer. If you're using Tails to make a document, you'd better upload it to the internet because that's the only way it can be stored. Tails is a Linux variant. It comes with the Tor browser installed. Tails is intended primarily for booting from live USB flash drive. It probably provides the safest way to maintain anonymity and privacy when using the Tor Network.

HiddenWiki:

A website that contains direct links to hidden Tor-hosted sites. To get to Hidden Wiki, you have to Google search for the latest available URL, since the link changes often and you need a direct link. thehiddenwiki.org and duckduckgo.com

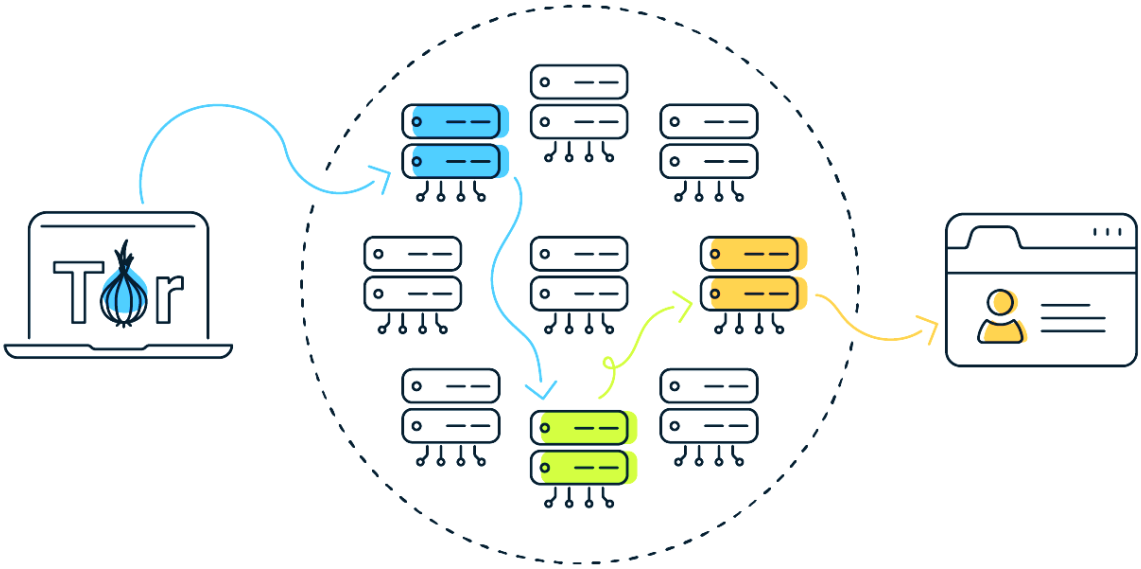


Bridge:

Also called bridge relays, bridges are Tor relays that are not listed in the main Tor relay directory, and are thus an alternate way of accessing the Tor network. They also make it harder for your ISP to know whether or not you are using Tor. Using bridges is not recommended unless you are in a country that censors Tor. If Tor is censored in your country, there is a way to bypass the censorship. Go to Configurations after the Tor Browser is launched. Check the box next to Tor is censored in my country, pick a bridge, and click Connect.

How Tor Works:

Tor passes data packets through a series of nodes. That path consists of three types of nodes: an entry node, a middle node, and an exit node. First, the traffic is encrypted and sent to the entry node. Next, layers of the data packet are stripped off each time it passes through one of the middle nodes. Finally, the exit node uses an unencrypted link to communicate with the target server outside Tor network. Each node can only access node before it & the one after it.



Examples of Surface Web include- Facebook, YouTube, ccn, bbc, yahoo, google, reddit, bing, Wikipedia, Regular Blogging Websites, and basically everything that we can see on any search engine's result page. Any browser with the proper credentials. ISP and other entities regularly track activity. Sites on the Surface web can be accessed using normal web browsers like Mozilla, Firefox, Google Chrome, Internet Explorer, Microsoft Edge and Safari.

Examples of Deep Web Include-Websites which can be accessed with a username and password such as email, cloud services, online banking, or paid subscription-based online media sites etc. Video-on-demand services like Netflix, Amazon Prime, or HBO. Educational or library websites. Any browser with the proper credentials. ISP and other entities regularly track activity. Sites on the deep web can be accessed using normal web browsers like Mozilla Firefox, Google Chrome, Internet Explorer, Microsoft Edge and Safari.

Examples of Dark Web include- Onion Sites, Hidden Marketplaces, Anonymous Journalism, Drug trafficking and other illegal activities, political protest, Drug trafficking, Child pornography, Illegal trading of human organs. Weapons and Hitmen. Tor Browser and other specialized browsers only. Many browsers make access less traceable but not truly anonymous.