# NAME: Vaibhav

ENROLLMENT NO.: A7605219068

Description of Class Case Study: Tor Browser

The Tor Browser is a web broswer that anonymizes your web traffic using the Tor network, making it easy to protect your identity online.

If you're investigating a competitor, researching an opposing litigant in a legal dispute, or just think it's creepy for your ISP or the government to know what websites you visit, then the Tor Browser might be the right solution for you.

## How to use the Tor Browser on mobile and cell phones

More and more people are browsing the web from their phones, and in poorer parts of the world that are mobile first, people are browsing the web only from their phones. As a result, the Tor Project has spent a couple years working to build a better Tor Browser for mobile phone users.

In September 2019, the Tor Project announced the [official release of Tor Browser for Android](https://blog.torproject.org/orfox-paved-way-tor-browser-android), replacing the Guardian Project's Orfox as the officially endorsed Tor Browser for Android. (The Guardian Project's similarly named Orbot, a Tor proxy for Android that lets you tunnel all your app traffic over Tor, not just web traffic, continues to be alive and well.)

Due to technical restrictions on Apple's proprietary iOS platform, the Tor Project has not yet released an official Tor Browser for iPhone and iPad users, but endorses [OnionBrowser](https://onionbrowser.com/" \t "_blank) for iOS users who want to browse the web anonymously. Major security improvements are in the pipeline for OnionBrowser, including fixing some information leakage issues and enabling per-website security parameters. The latest and greatest version of OnionBrowser should be out by early November 2019, the developers tell CSO.

## How Tor Browser works

Tor Browser routes all your web traffic through the Tor network, anonymizing it. As the images below illustrate, Tor consists of a three-layer proxy, like layers of an onion (hence Tor's onion logo). Tor Browser connects at random to one of the publicly listed entry nodes, bounces that traffic through a randomly selected middle relay, and finally spits out your traffic through the third and final exit node.

As a result, don't be surprised if Google or another service greets you in a foreign tongue. These services look at your IP address and guesstimate your country and language, but when using Tor, you will often appear to be in a physical location halfway around the world.

If you live in a regime that blocks Tor or need to access a web service that blocks Tor, you can also configure Tor Browser to use bridges. Unlike Tor's entry and exit nodes, bridge IP addresses are not publicly listed, making it difficult for web services, or governments, to blacklist those IP addresses.

The Tor network routes TCP traffic of all kinds but is optimized for web browsing. Tor does not support UDP, so don't try to torrent free software ISOs, as it won't work.

Tor Browser offers the best anonymous web browsing available today, but that anonymity is not perfect. We are currently witnessing an arms race between researchers seeking to strengthen Tor, or even develop a [next generation anonymity tool](https://arstechnica.com/information-technology/2016/08/building-a-new-tor-that-withstands-next-generation-state-surveillance/), and governments around the world studying how to break Tor's anonymity properties.