# Deep and Dark Web

## Text

Are you in need of a kidney, a heart, a brain, or any other organ in the human body? Do you want to get rid of a terrible person while also making a profit? Are you a fan of child abuse? Well, then I have the perfect solution! I present you: The Deep and Dark Web.

Surely, most people have already heard of at least one of those terms but very few have accessed either of them and this is because of the nature of these networks.

In order to understand what the Deep and Dark Web are, we need to take a look at the Internet as a whole. Think of the it as a giant floating iceberg. The visible upper part is what we call ‘the surface web’ – the websites we use on a regular basis. They account for 5% of internet traffic. The Deep Web accounts for 90% of internet traffic and the rest 5% comprise of Dark Web webpages.

Deep Web is the invisible part of the Internet. Every day, people use thousands if not millions of websites. However, what they see on their screens is only a small fraction of reality. In order to display the information, websites run numerous processes and contain many webpages which are hidden from view.

For example, an online retail shop uses a database to retrieve specific information, but the average user cannot access the product database. An online banking website displays information about bank accounts but requires identification to access and manipulate any of the bank accounts. Sending emails requires the user to enter a form but numerous processes occur offscreen.

All these pages, queries, databases and processes cannot be accessed by searching for them in ordinary search engines such as Google or Bing. This is achieved by using several different techniques:

1. Contextual Web: pages display content based on context: role and IP of a user
2. Dynamic content: web pages which are displayed in response to a query
3. Limited Access Content: webpages that prevent robots and bots from reading their content and making copies of it. This is achieved by using the Robots Exclusion Standard or CAPTCHAS
4. Non-HTML/Text content: storing data as part of an image or a video prevents the search engines from “understanding” the meaning
5. Private web: webpages that require accounts
6. Scripted content: webpages which are accessed through links, created by JavaScript
7. Unlinked content: webpages, the links for which do not exist in other websites
8. Using a robots.txt file, which advises robots not to crawl the webpage. The robots exclusion standard, also known as the robots exclusion protocol or simply robots.txt, is a standard used by websites to communicate with web crawlers and other web robots. The standard specifies how to inform the web robot about which areas of the website should not be processed or scanned. Robots are often used by search engines to categorize websites.

All the above-mentioned examples of websites are legal. However, the Deep Web does not consist only of harmless websites. Criminals have taken advantage of the techniques preventing indexing and have created webpages through which human and drug trafficking are done. The part of the Deep Web that involves illegal webpages and activities is called ‘The Dark Web’.

How Tor works:

* Isolates websites so that third parties can’t gather information
* Hides the IP address
* Hides device information
* Encripts traffic three times by passing it through reliable volunteer-run servers
* Allows visiting websites that are banned or hidden

The browser achieves this by packing your traffic by prossessing it through three servers called nodes. Think of your data as if it’s a letter that your sending on the mail. If you give it to the Post like that, anyone can read what you’ve written. But if you put that letter in an envelope, then that envelope in a second envelope, and then in a third one, etc., no matter where you letter turns up, every mailman will only be able to open one envelope at a time, and in the end, only the receiver will be able to read the letter.

However, large websites such as Google or Facebook and Security agencies are able to break the encryption and see your original IP address. Oppressive governments outright block traffic coming from Tor browsers.

That’s where a VPN comes in handy. It doesn’t simply hide your IP address like Tor does. It outright changes it. If one uses only a VPN, his IP address is safe but the history of visited websites isn’t. If one uses only Tor, the websites he visited are hidden but the IP address can be compromised. If both are used simultaneously, even if either the website data or IP address are discovered, the other information would be safe.

There are two ways to use this technique:

* Tor over VPN: First, the VPN changes the IP address, then Tor encrypts the data. It’s the easier way but governments can see you are using Tor and therefore start tracking you or even block you.
* VPN over Tor: First, Tor hides the data. Then, the VPN changes the IP address. That way, governments don’t know you’re using Tor but websites don’t either. This makes .onion websites inaccessible.

So, if all these pages are hidden and inaccessible via a search engine or a hyperlink, how do people use them? The answer is: special instruments. It turns out that there are several search engines, designed particularly to index Deep Web pages. Some of the most famous are:

* DeepPeep
* Intute (no longer maintained)
* Deep Web technologies
* Scirus (retired)
* Ahmia.fl
* Google designed the Sitemap Protocol and OAI-PMH mechanism to crawl deep webpages

There are two general ways to access a website without knowing its address: searching for it in any search engine or clicking a link in an already visited website. However,

Silk Road was an online black market and the first modern darknet market, best known as a platform for selling illegal drugs.[7] As part of the dark web,[8] it was operated as a Tor hidden service, such that online users were able to browse it anonymously and securely without potential traffic monitoring. The website was launched in February 2011. In November 2020, the United States government seized more than $1 billion worth of bitcoin connected to Silk Road.