Tor is a browser that allows access to the darkWeb.

It works quite simply.

There is a Tor network containing approximately seven thousand routers around the world.

The Tor browser's startup gold chooses three routers from the seven thousand and creates.

The user will send their message to Router 1

Router 1 will send the message to Router 2 and then Router 2 will send the message to Router 3.

Router 3 will then send the message to the desired site (in the example Netflix).

This method allows an anonymity because Netflix to communicate with you has to use an intermediary which makes that Netflix does not know your IP and thus does not know where you are and who you are.

Moreover, the communication between each router is encrypted which makes it very difficult to track you.

The tor logo is an onion precisely because the message has several layers of encryption. Like an onion that contains several layers above the edible part of the vegetable.

Anonymity disadvantage:

Some people take advantage of Tor's anonymity to sell illegal products.

Like drugs, selling weapons.

Unfortunately, Tor's anonymity also allows some people to create Nazi or racist blogs and forums without being condemned.

Tor with its anonymity allows a freedom that some can abuse and make this freedom harmful.

Debate

The debate is whether the anonymity that Tor allows is good or bad.