TOR

The secret world of the Darknet isn't entered via any gate, but throughout the TOR: TOR stands for "The Onion Router". The term "onion" identifies the layers that have to be penetrated from the information, unlike ordinary browsing, the pc doesn't connect directly to the server where the site is situated. Rather, a complete chain of servers take part with the link so as to produce the best possible anonymity.

The first Coating: Entry-Point

The entrance Stage (Server 1) to the TOR system receives the IP address from the PC. The TOR customer then connects your personal computer to some other server (server 2), the node. All information is encrypted on the way for this node.

The Second coating: TOR nodes

The node (Server 2) just knows the entrance node - although not your pc or your own IP address. The information sent through this node is encrypted and therefore can't be read by the node. Besides the entrance stage, the TOR node only knows the exit node (Server 3), i.e. the host that connects you to the page.

The third Twist: Exit Node

The exit Node (server 3) determines the true connection to the internet server where the requested goal page is situated. In the exit node, you are able to get the valid services which finish in .onion. Away from the TOR community, services together with the .onion expansion aren't available.

The Goal: Internet server

This is Wherever your trip ends - you have reached your destination. This is the point where the Deep webpage that you would like to get is saved. This internet server only knows the IP address of the exit node. The web server doesn't have to know the additional servers along with your PC. The information Packets between the notebook and the entrance point are all encrypted. The entry point gets the encrypted package, repacks it, adds the speech of this TOR node and its sender IP address. It then sends the package into the TOR node, which essentially does the exact same thing: it doesn't open the package, but flags its IP address as the sender also sends the entire thing on into the speech of the exit node. This manner, the IP address of the source device stays secure, because the site just knows the address of the exit node and every one of those individual cases only knows its closest neighbor. In this manner, the user remains anonymous. Of Course, you could even get "ordinary" clear webpages through the TOR browser. With normal web pages TOR acts like an ordinary browser. With profound webpages it seems somewhat different: Given the sophistication and higher number of links required, it is hardly surprising that obtaining a profound web page requires considerably longer than accessing a standard site.

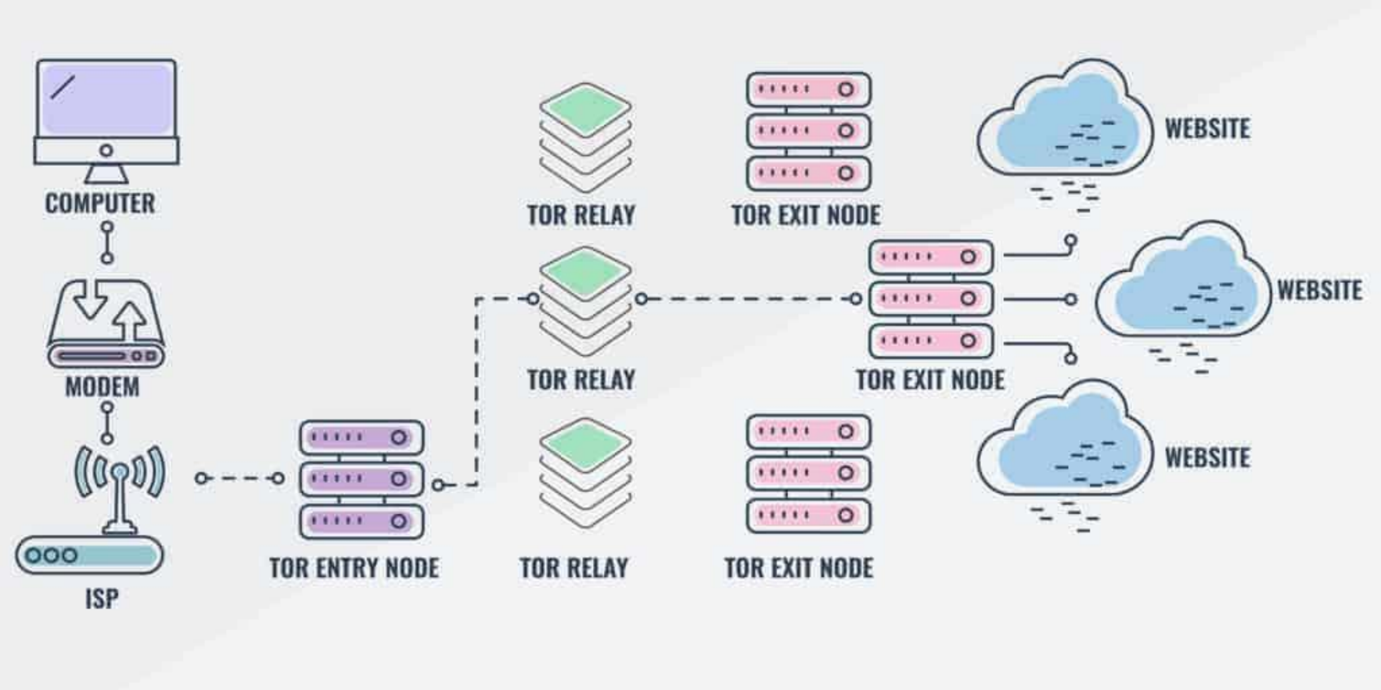

FIG: Simplified Tor Connection