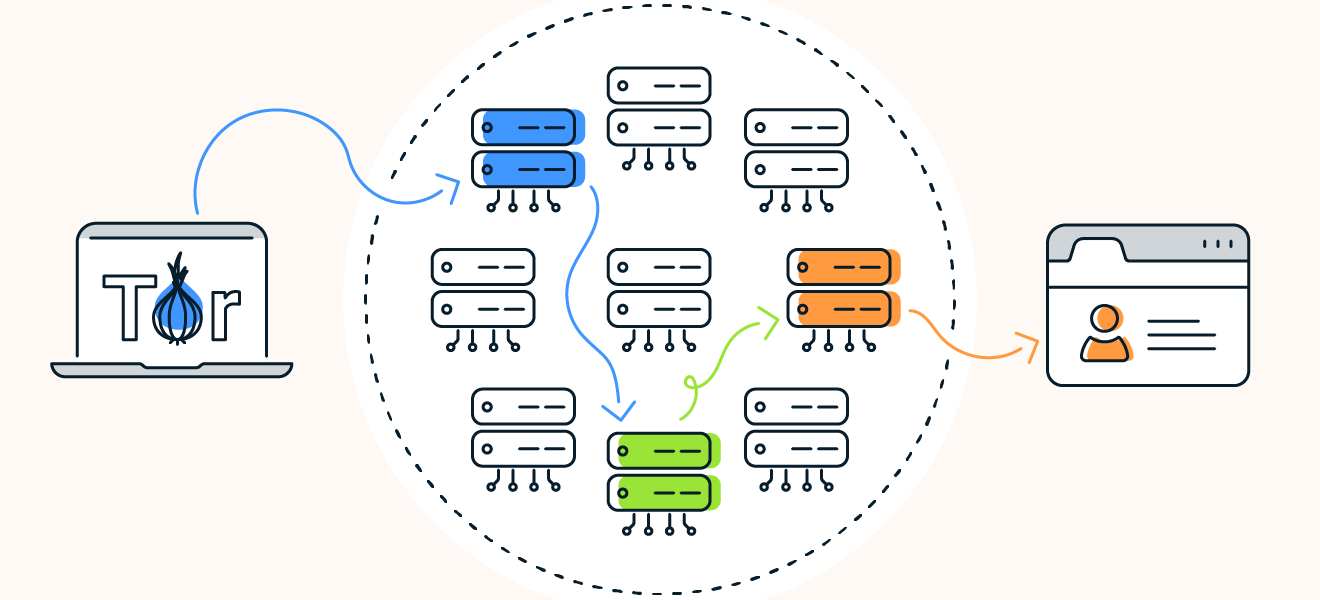
TOR Browser

1)Analysing Tor Traffic with Wireshark:

Traffic is encrypted:Tor is a decentralized network.It contains many nodes comparable to the layers of an onion.

**Entry/Guard node:** First, Tor Browser randomly connects to a publicly known entry node. The entry node introduces your data into the Tor circuit by decrypting the first layer of encryption to uncover the address of the middle node, where it forwards your data.



**Middle node:** This node receives the request from the entry node. It knows the IP address of the entry node where the request came from, but it doesn’t know the encrypted IP of the original requester. The middle node decrypts the next packet, revealing the next node in the circuit, but the content and final destination of the request remain encrypted.

**Exit node:** The exit node receives the request and decrypts the last packet, revealing the final destination. Once the last layer of encryption is peeled off, the decrypted data leaves the Tor network.

Tor encrypts your traffic multiple times, making it very difficult for anyone to intercept or read it.

Slower than other browsers: **Data travels more slowly as a result of this** routing procedure, slowing down browsing.

2)Torrc file:

Torrc File is modified to :

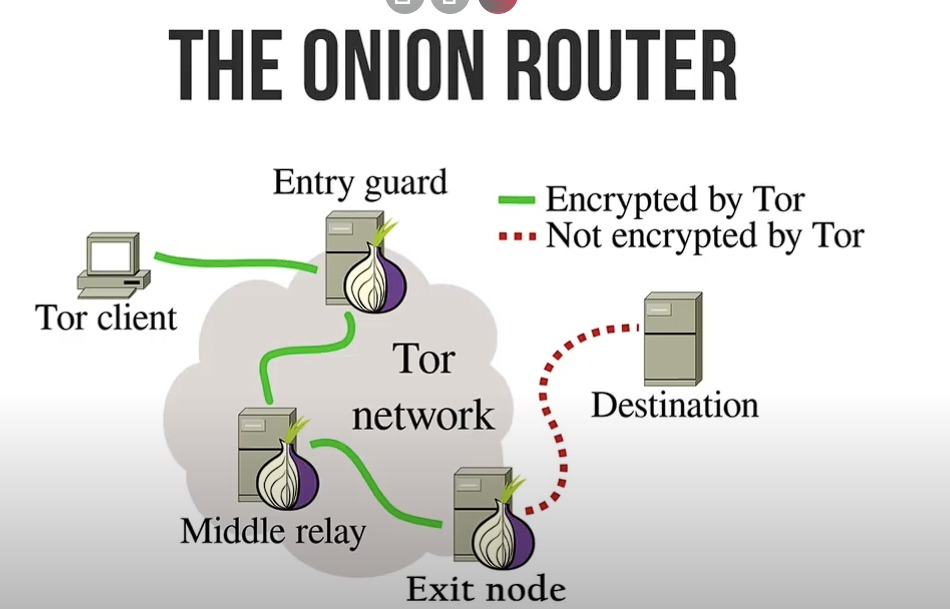
🡪Change geographic locations

🡪Change IP address and location of entry ,exit relays.

I have now changed to Germany IP address.

3)Tor Security Features:

🡪 **Encrypted Traffic:** Tor encrypts your data multiple times, making it extremely challenging for anyone to intercept or read your communications.



🡪 **Bypasses Censorship:** Tor enables you to bypass censorship and access blocked websites and content by circumventing firewalls and restrictions.

🡪 **Hidden IP Address:** Tor conceals your IP address by routing your traffic through a network of volunteer servers, making it difficult to trace your online activity.

**🡪Protection Against Surveillance:** Tor enhances your privacy by making it hard for anyone to monitor or track your online activities.

🡪 **Free and Open-Source:** Tor is available for free and is open-source software, allowing anyone to inspect the code and ensure its security.

🡪 **User-Friendly:** Tor is relatively simple to use, even for those with little technical expertise

Tor with HTTPS:

Tor is anonymity software that hides IP address from the website you are visiting by sending your traffic through three hops, also called Tor relays. HTTPS encrypts your web traffic between your browser and the website you are visiting. These two technologies are separate but complimentary.