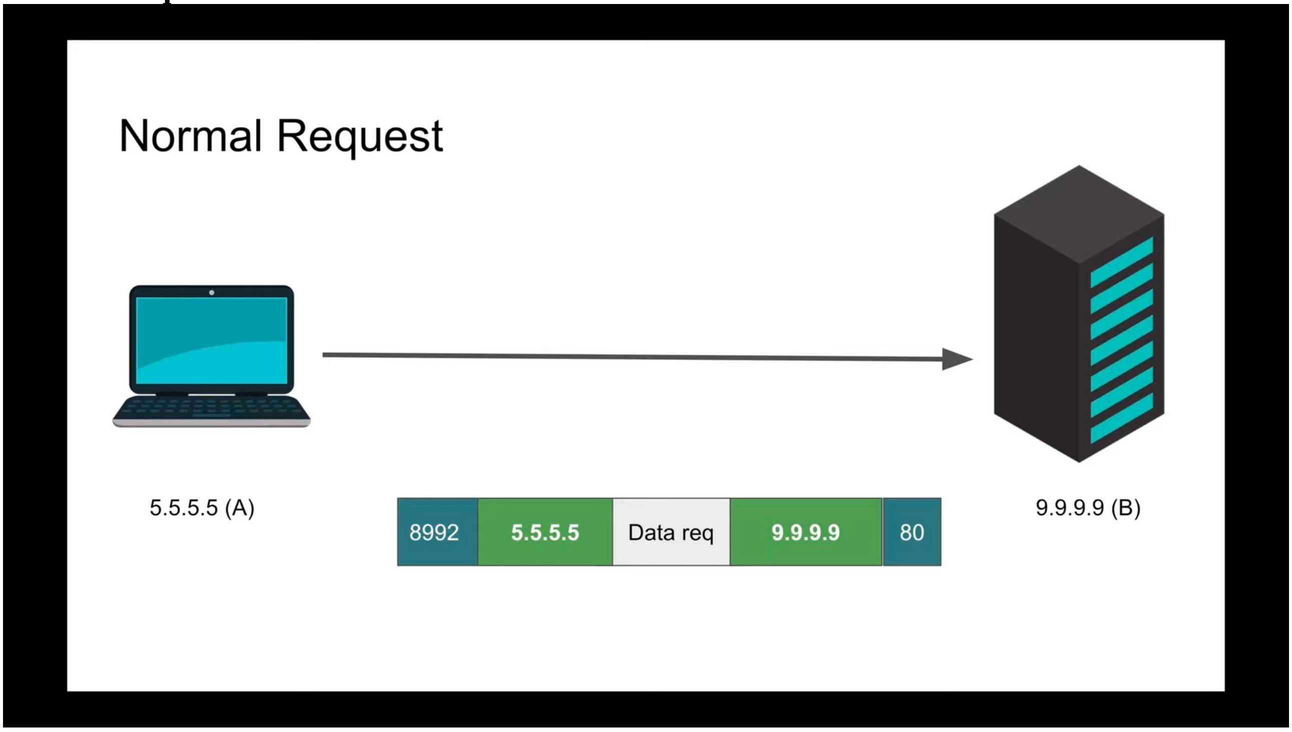
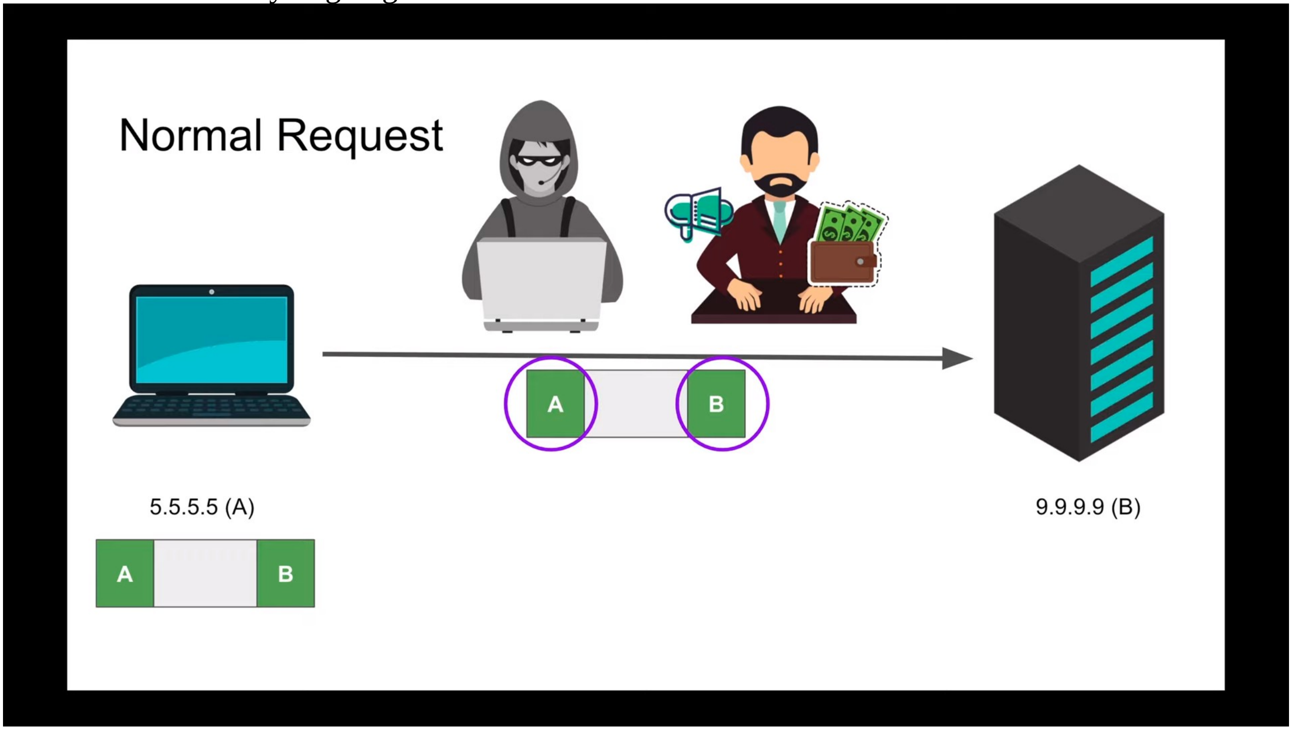
# Onion Router working

In order to understand the Onion Routing which is most secure Routing we must have to understand the Simple Request from client to server or Normal Request from client to Server.

**Normal Request :**



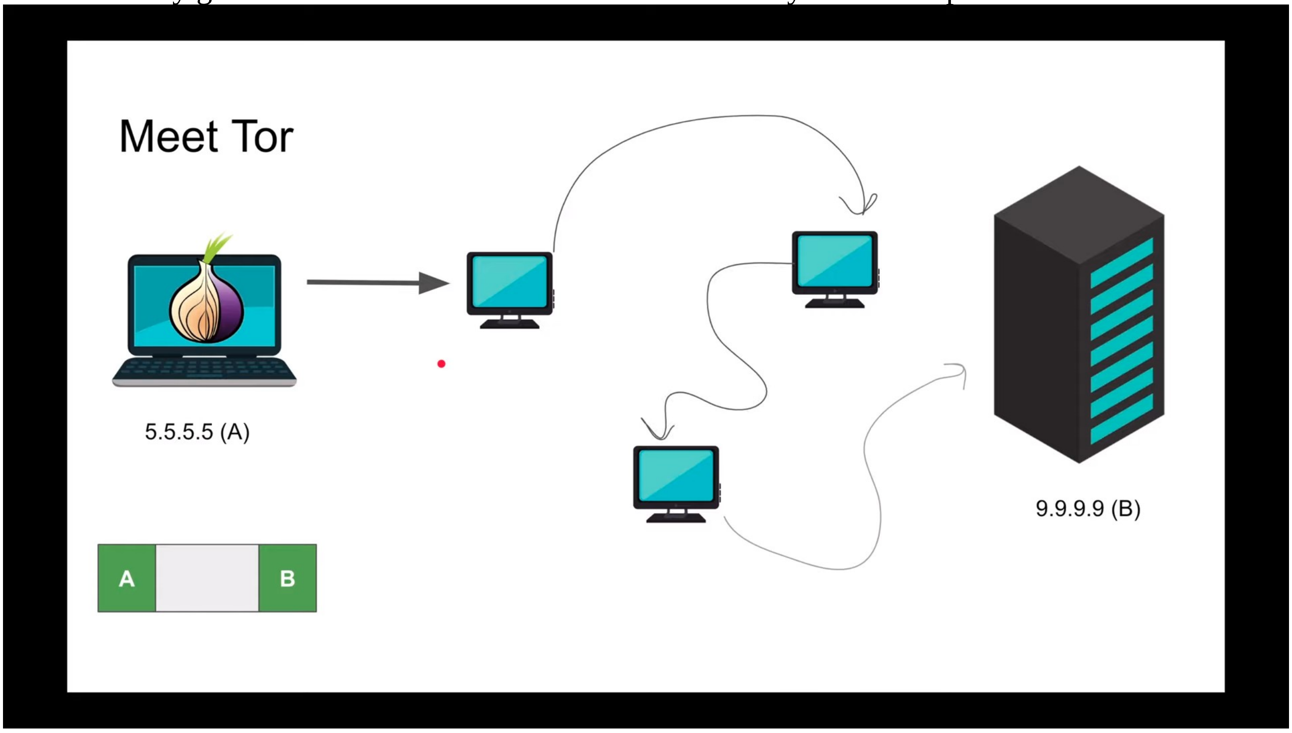
As show in the figure A is let suppose is client and B is Server . Our Job is to transfer the information from A to B with security like No one can see this. But what actually happened when you send the request from A to B . There are some hacker are sitting there between the server and client then they will use your source information from where you are coming catch that information as well as where are you going.



But if you are using HTTPS and send TCP request then no one can hack this until you handshakes with the server then become end to end encrypted. Now lets come to The ***Tor Routing working.***

# *Tor Routing Working*

The Tor routing working differently. When client is ready to send the request from client to server then client say give me three or other Tor Node which actually it self computer or like IP Address.

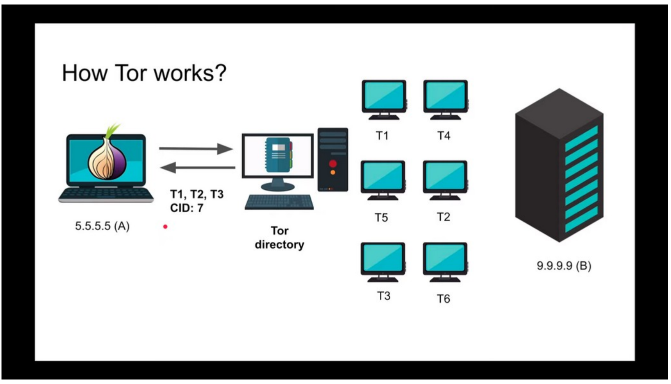


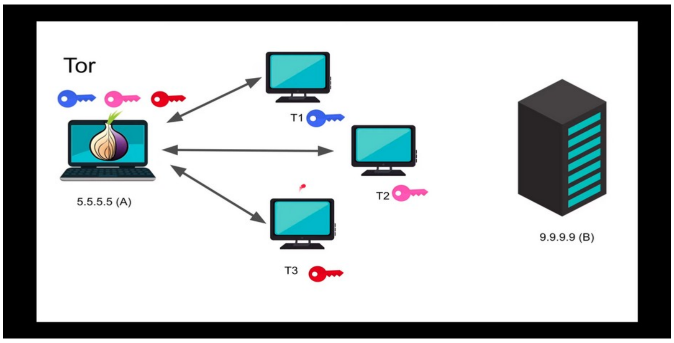
As you can see in the diagram. When client can’t send the request directly before reach the request on the server it passed many TOR Node which it self computer like Ip address.

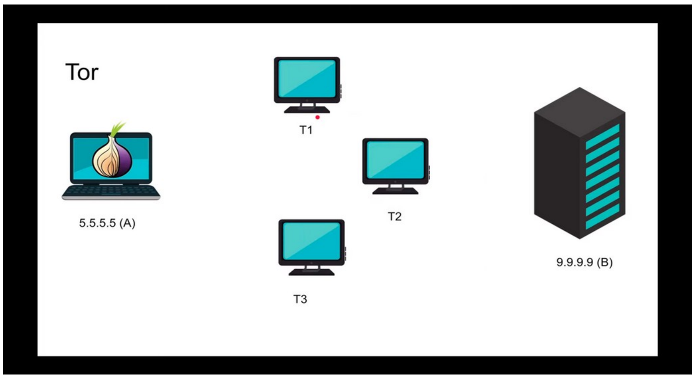
**Working:**

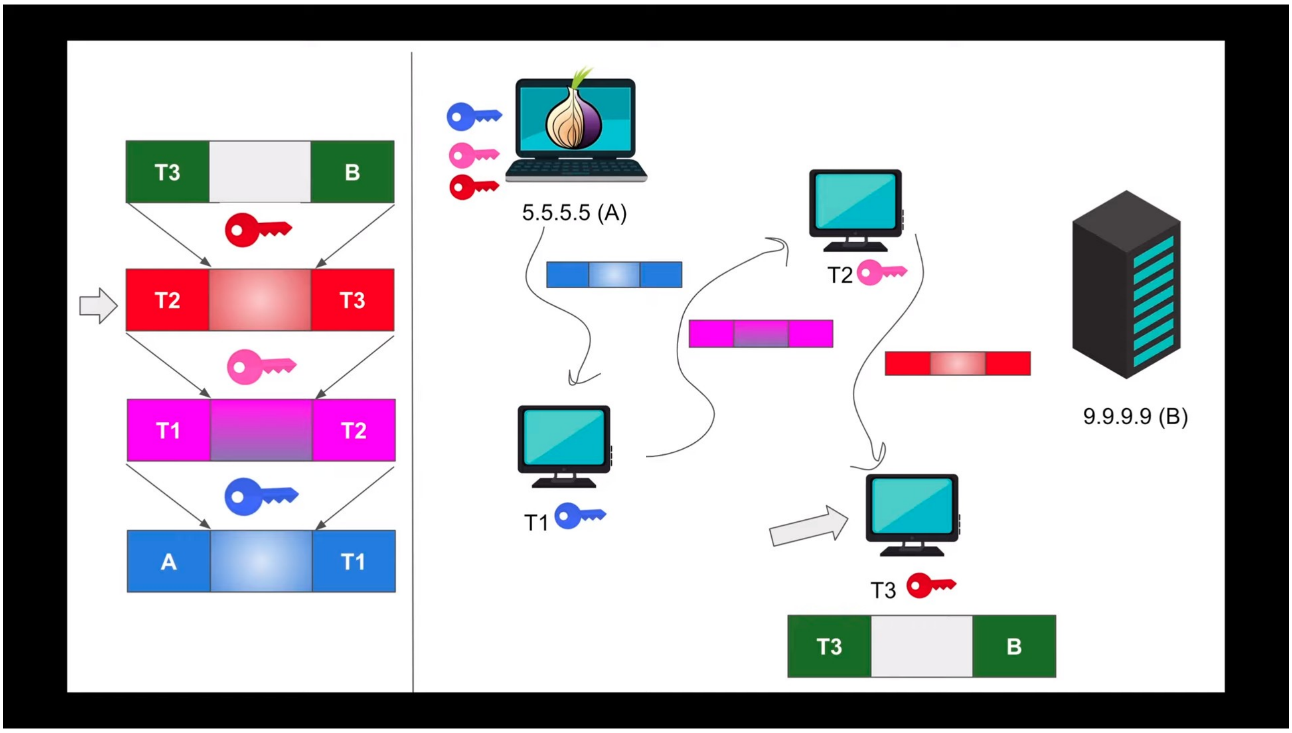
1. When client is ready to request to Server .its give the Three Tor node from the Tor Directory. Client A know the T1 and T1 know the Client A.

2 : When Tor Directory return the three Tor Node. And Every node as own Ecrypted key T1 has own Encrypted key and T2 has own Encrypted key and T3 has own Encrypted key.









Then Client A send Request to T3 because T3 has the last node after this node we need to move the our real destination. When T3 get the request from client A then T3 become source and B is destination and T3 send the Request  to T2  then T2 become source and B become Destination and then send the request to T1 then T1 become source and T2 become destination and send the request to client the  A become source and T1 become destination Now the our final product is ready (source)A Data T1 (Dest).Then Request send to T1 first and Then move to T2 and Then move to T3 and move to Server. In this way no one can know where the request is coming.

**Request back:**

When the request from the server then first come to T3 and Then T2 and then T1 and Then Client. Every Tor node have own encrypted key.