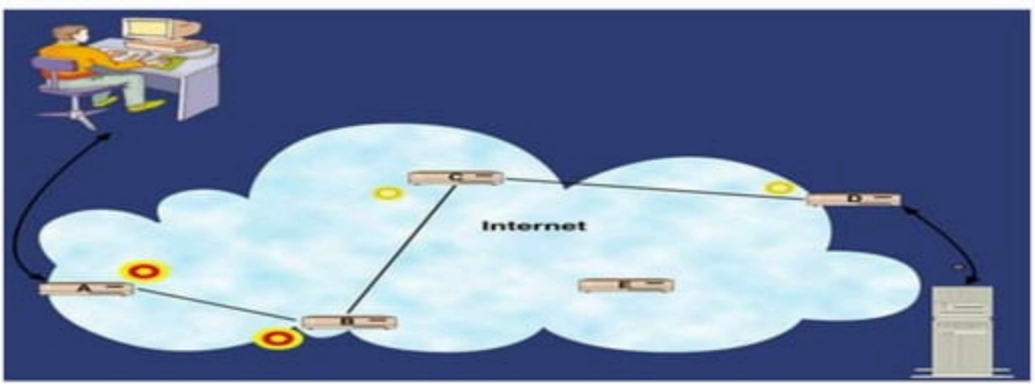
Who needs Anonymity

- Government Organization ?
- Private Organization?
- Hackers
- And yes !!!Criminals? But they already have it
- What About YOU

TOR

- Onion routing is an anonymous communication technique over a computer network. Messages are constantly encrypted and then sent through several network nodes called onion routers which creates a circuit of nodes



Anonymous Connection and Onion Routing

Who is Talking to Whom ?

In a Public Network

>Packet headers identify recipients

>Packet routes can be tracked

Traffic Analysis Reveals Identities

>Who is searching a public database?

>Which companies are collaborating?

>What are you talking to via-Email?

>What do you shop online?

Tor Objectives

Design an infrastructure that

>Makes traffic analysis hard

>Separates identification from routing

Our goals is anonymous connections, not anonymous communication.

An infrastructure, Onion Routing, has been implemented.

Steps for Onion Routing

> Define the route

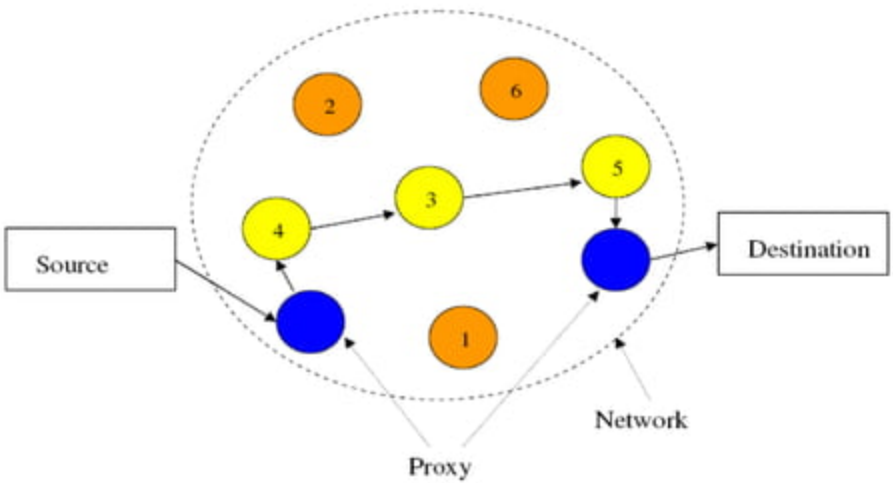
>Construct the anonymous connection

>Move and encrypt the data through the connection

>Destroy the anonymous connection

Example

- Let onion routers 4, 3, and 5 be randomly selected by the onion proxy



TOOLS

- TOR BROWSER
- TOR GATEWAY
- TOR WORK STATION
- JANUSVM

References

- https://www.torproject.org/about/overview.html.en
- http://www.onion-router.net/
- http://ntrg.cs.tcd.ie/undergrad/4ba2.05/group10/index
- http://en.wikipedia.org/wiki/Onion_routing