Scratching your Brain into Dark Web

By: Arpit Maheshwari

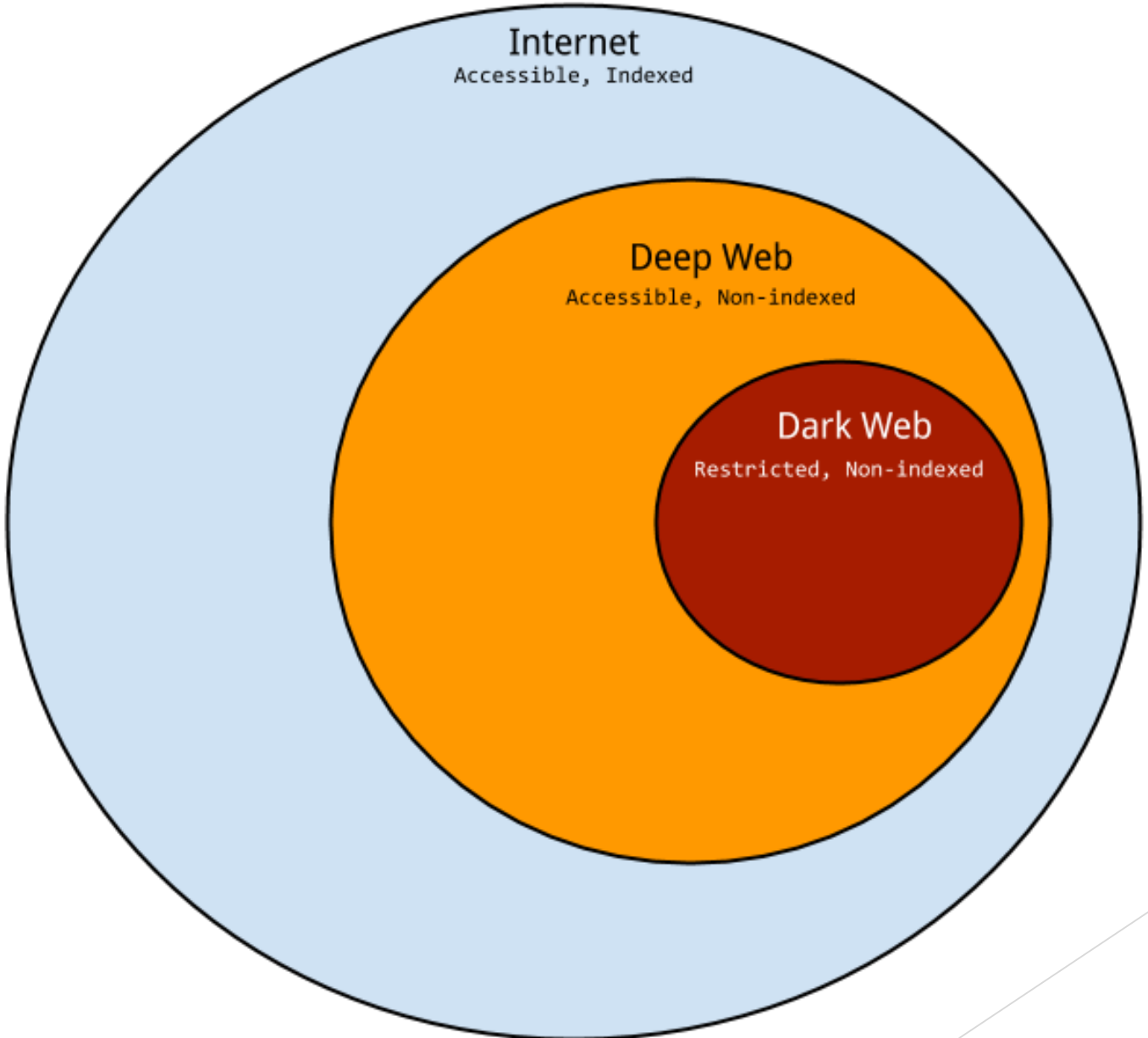
Who am I ?

- Arpit Maheshwari (C|EH, E|CSA, C|HFI, Cyber Law Certified)
- News Bytes Speaker
- Learner | Researcher in Cyber Security Field
- Entrepreneur
- Interested In : Wi-Fi Hacking & Travelling to New Places

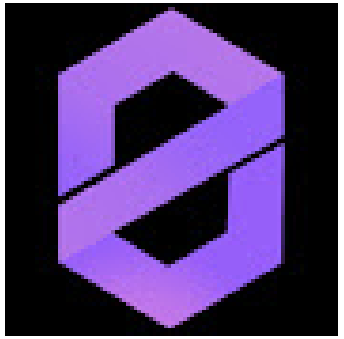
Web

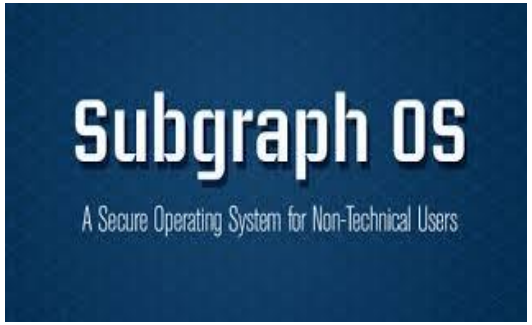

DARK WEB
BREAKING NOW
ISIS USING THE "DARK WEB" AS A WEAPON
CNN
DOW -36.94
SITUATION ROOM
VS
DEEP WEB

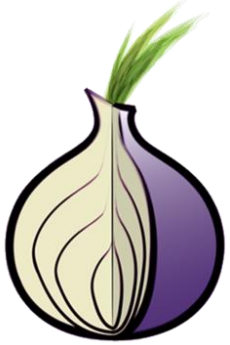
Deep Web Vs Dark Web

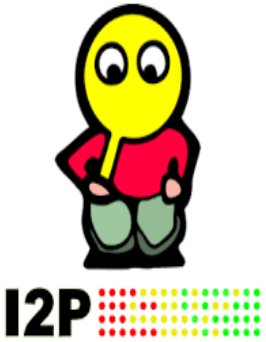


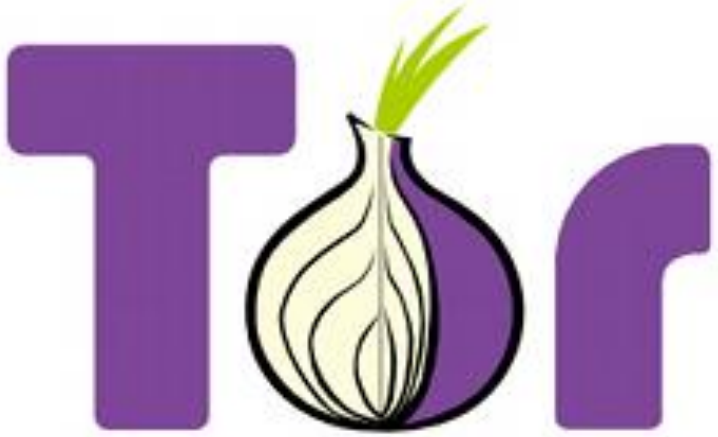
Dark Web Examples











TorProject.org

Tor Fluzzy Icon Set
by jord99

For aethetics only -
Not affiliated with Tor

Offline

Online

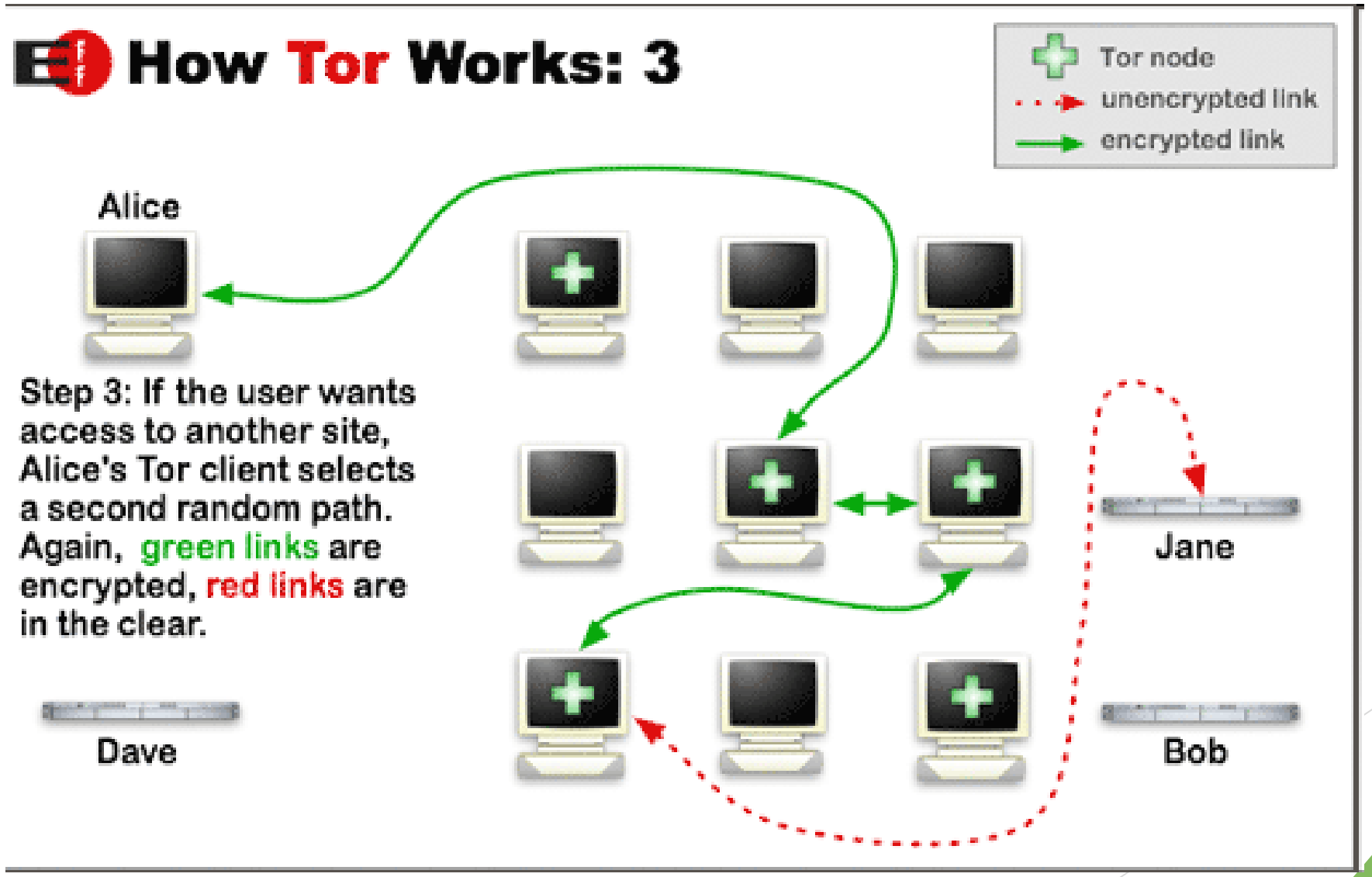
Starting

Stopping

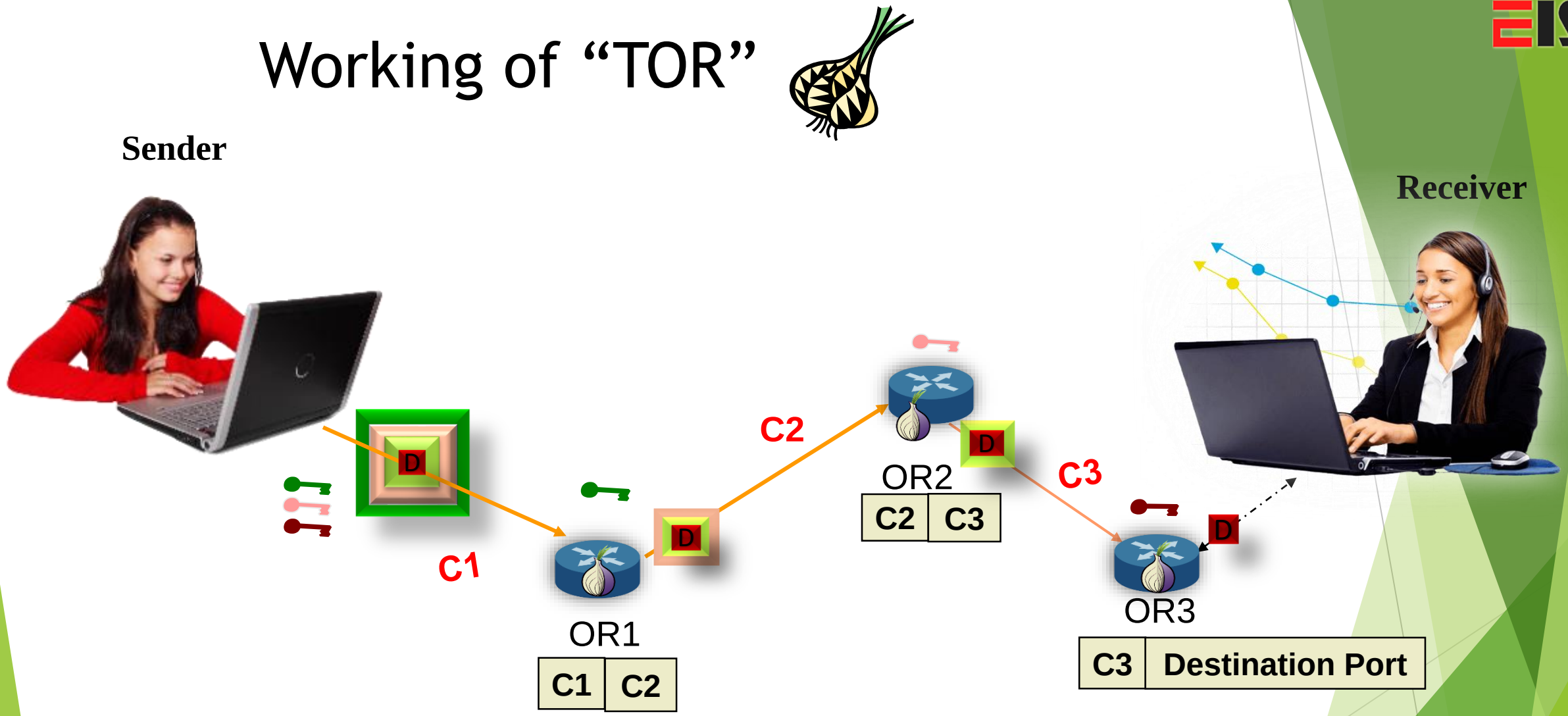
About Famous “TOR”

- TOR Tunneled Onion Routing
- By US navy in mid 1990
- Website no. 200,000 to 400,000 estimated rest NOBODY knows
- Location of the administrators is virtually untraceable
- Speed is Highly Compromised
- Is it Secure or Not ? Again debatable !

About Famous “TOR”

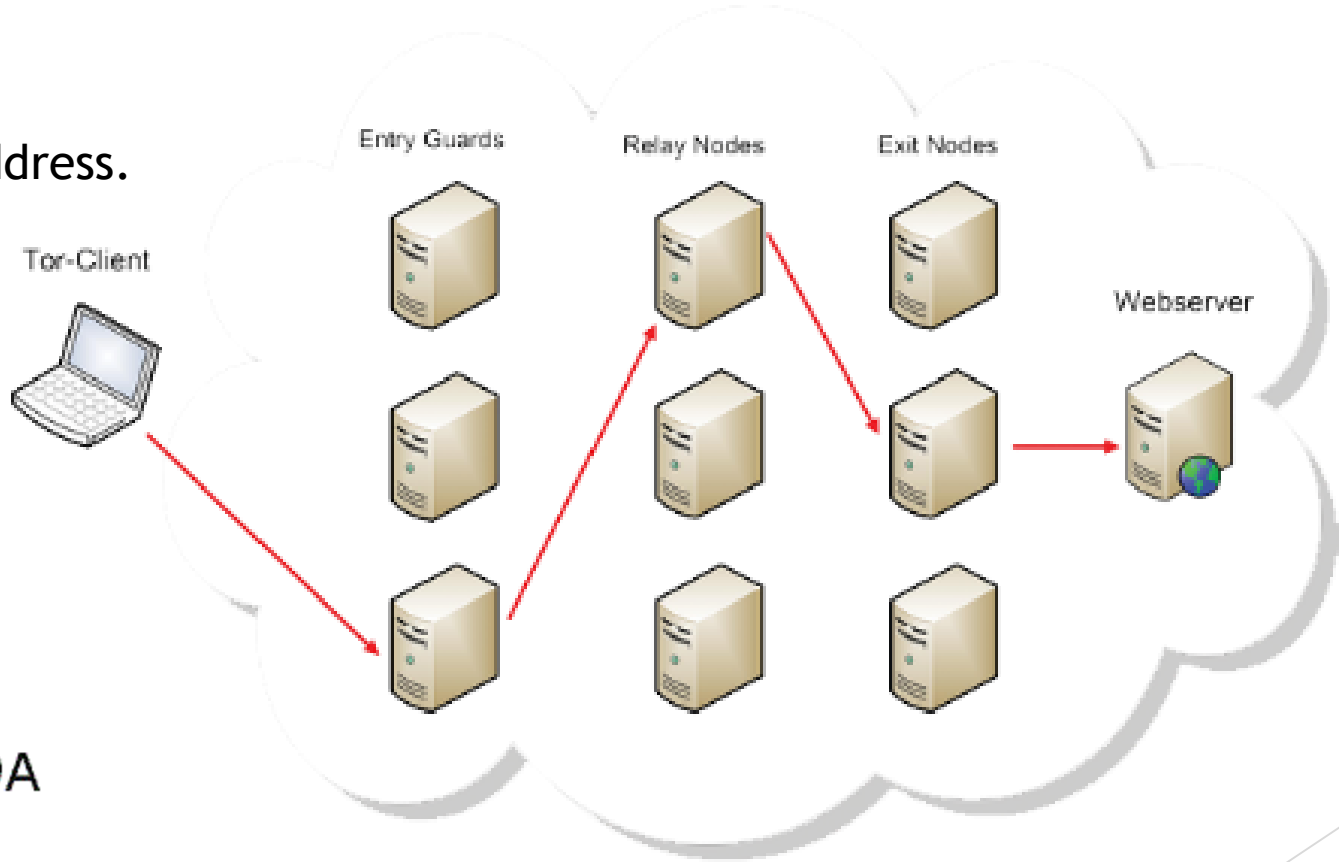


Working of “TOR”



Insiders for TOR

TOR works with MAC Address.



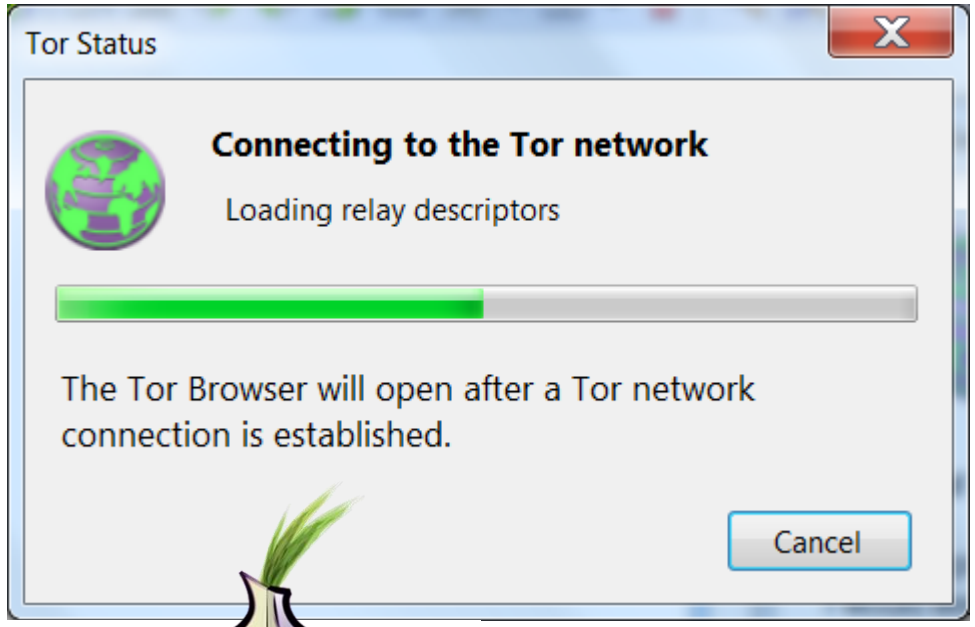
MAC address

D4-BE-D9-8D-46-9A

Note: TOR encrypts your connection not your data

Moving to ONION Url

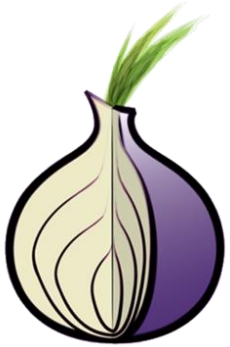
Step 1: Install Tor

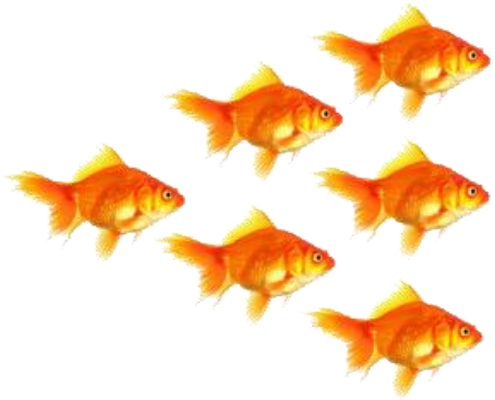


Tor must always be on your system for the hidden service to be accessible

Moving to ONION Url

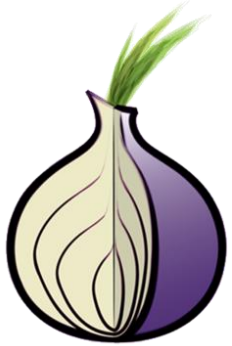
Step 2: Install & Configure A Web Server

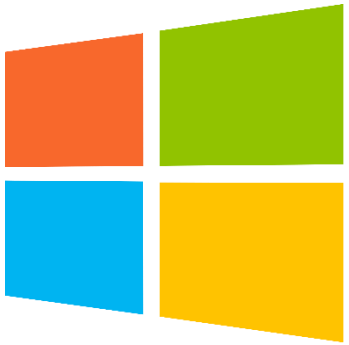


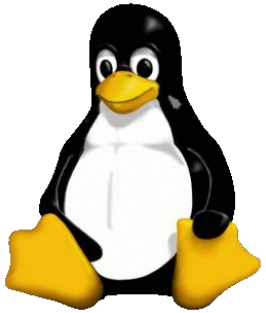


Moving to ONION Url

Step 2: Install & Configure A Web Server

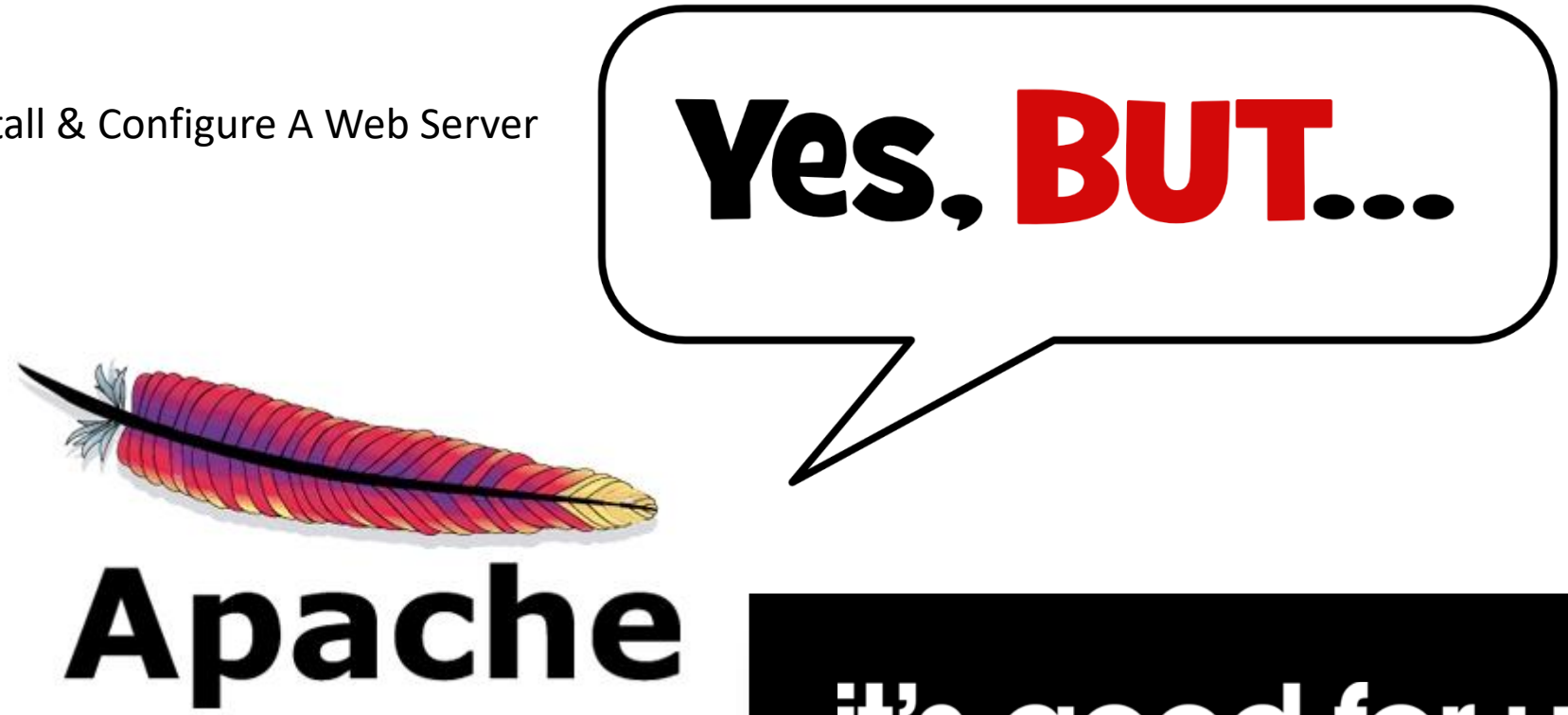




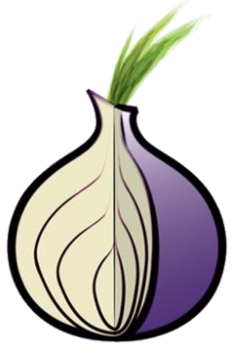


Moving to ONION Url

Step 2: Install & Configure A Web Server



Moving to ONION Url

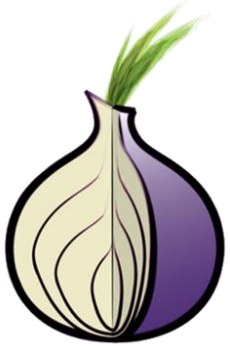


Step 2: Install & Configure A Web Server

- Web server Configuration is very important.
- Ensure it isn’t leaking any information that could be used to identify you, i.e. IP address.
- You can use any other webserver but remember to configure properly.

Moving to ONION Url

Step 3: Configure The Hidden Service

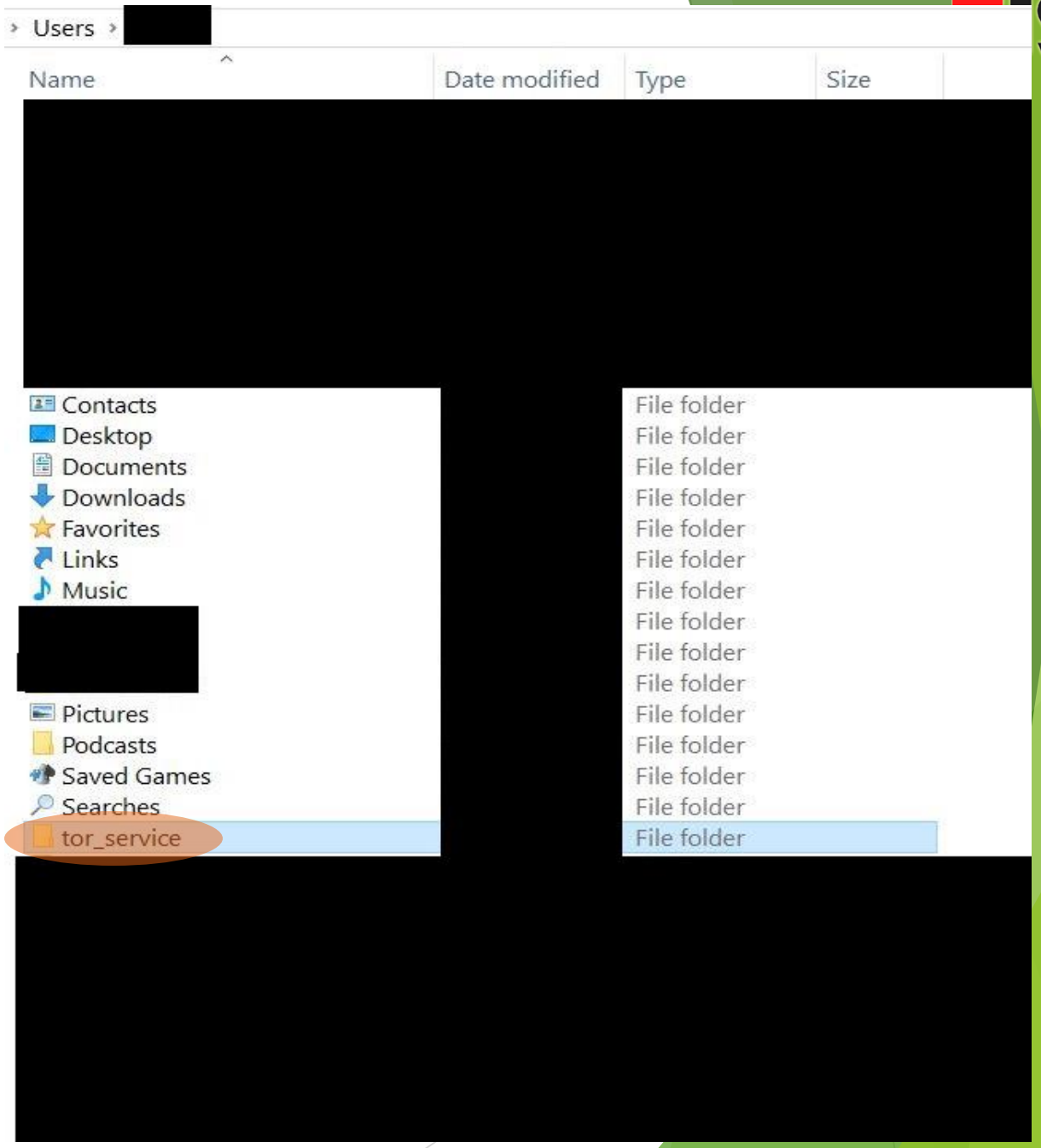
- Tell  about it.
- By adding this information to the torrc file.
  - Shut Down TOR
  - *Tor Browser\Data\Tor*
  - # Hidden Service
    HiddenServiceDir
    C:\Users**Name**\tor_service
    HiddenServicePort 80 127.0.0.1:80

```
# This file was generated by Tor; if you edit it, comments will not be preserved
# The old torrc file was renamed to torrc.orig.1 or similar, and Tor will ignore it

DataDirectory D:\Program Files\Tor Browser\Browser\TorBrowser\Data\Tor
GeoIPFile D:\Program Files\Tor Browser\Browser\TorBrowser\Data\Tor\geoip
GeoIPv6File D:\Program Files\Tor Browser\Browser\TorBrowser\Data\Tor\geoip6
HiddenServiceStatistics 0

# Hidden Service
HiddenServiceDir C:\Users\[redacted]\tor_service
HiddenServicePort 80 127.0.0.1:81
```

Moving to ONION Url

Step 3: Configure The Hidden Service

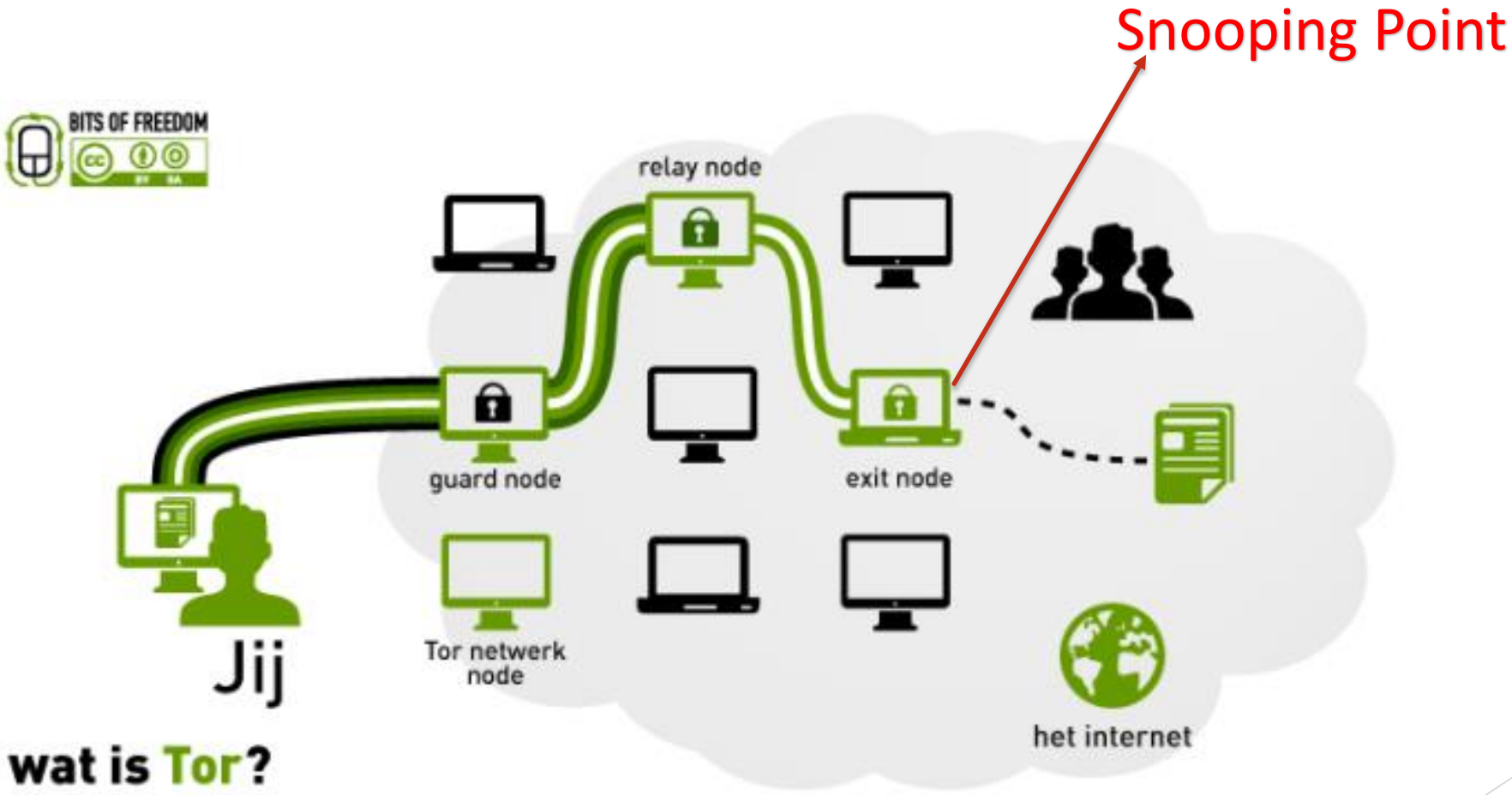
- Create Folder in C:\Users\Name\tor_service



Tools for Onion Name Generator

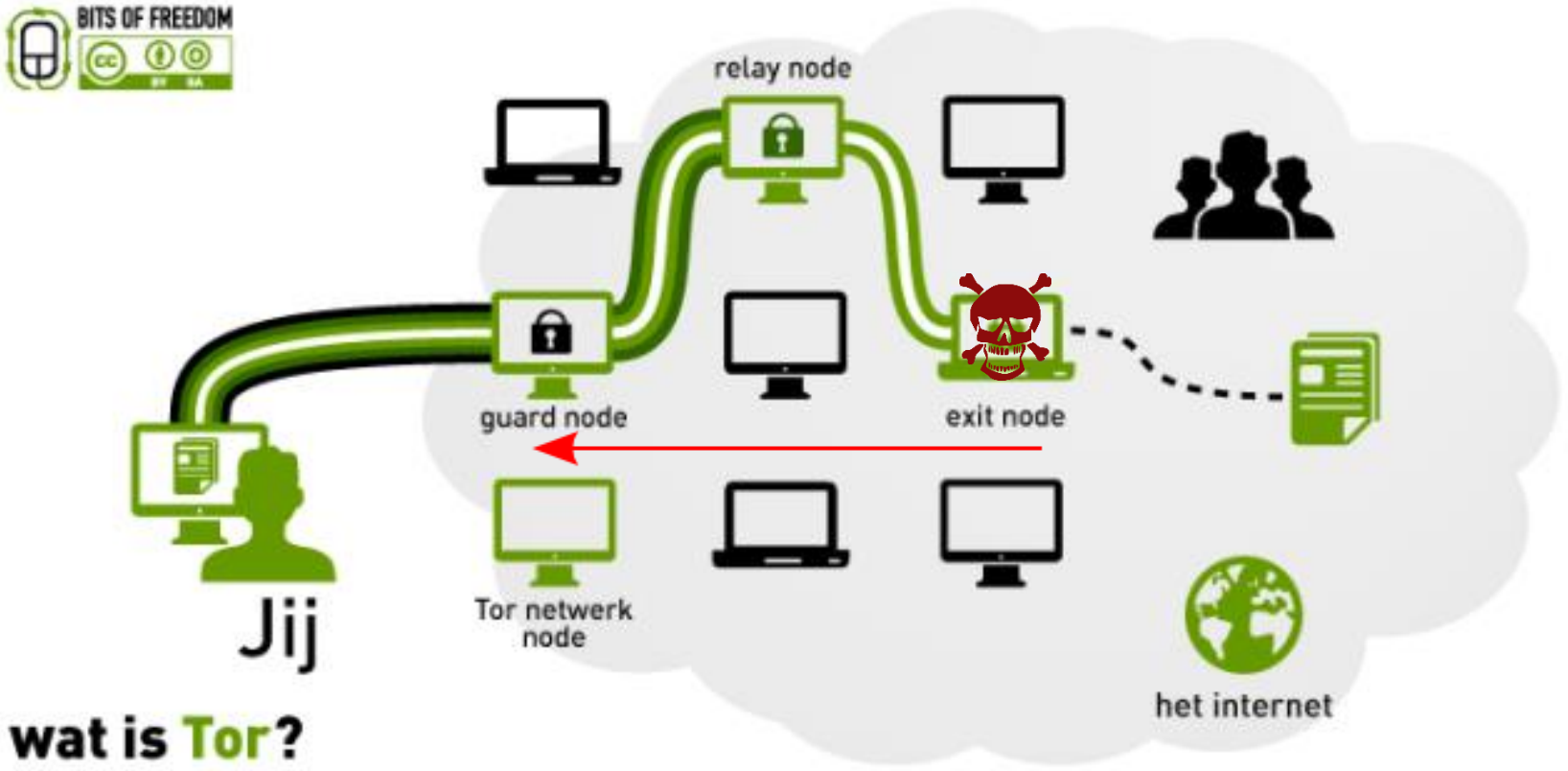
- **Shallot (onion hash)** is an older program, there are newer alternatives available now:
- **Scallion** - uses GPU hashing, needs .NET Mono: http://github.com/lachesis/scallion
- **Eschalot** - uses wordlist search, needs Unix or Linux: http://blacksunhq56imku.onion

Big Loophole with TOR



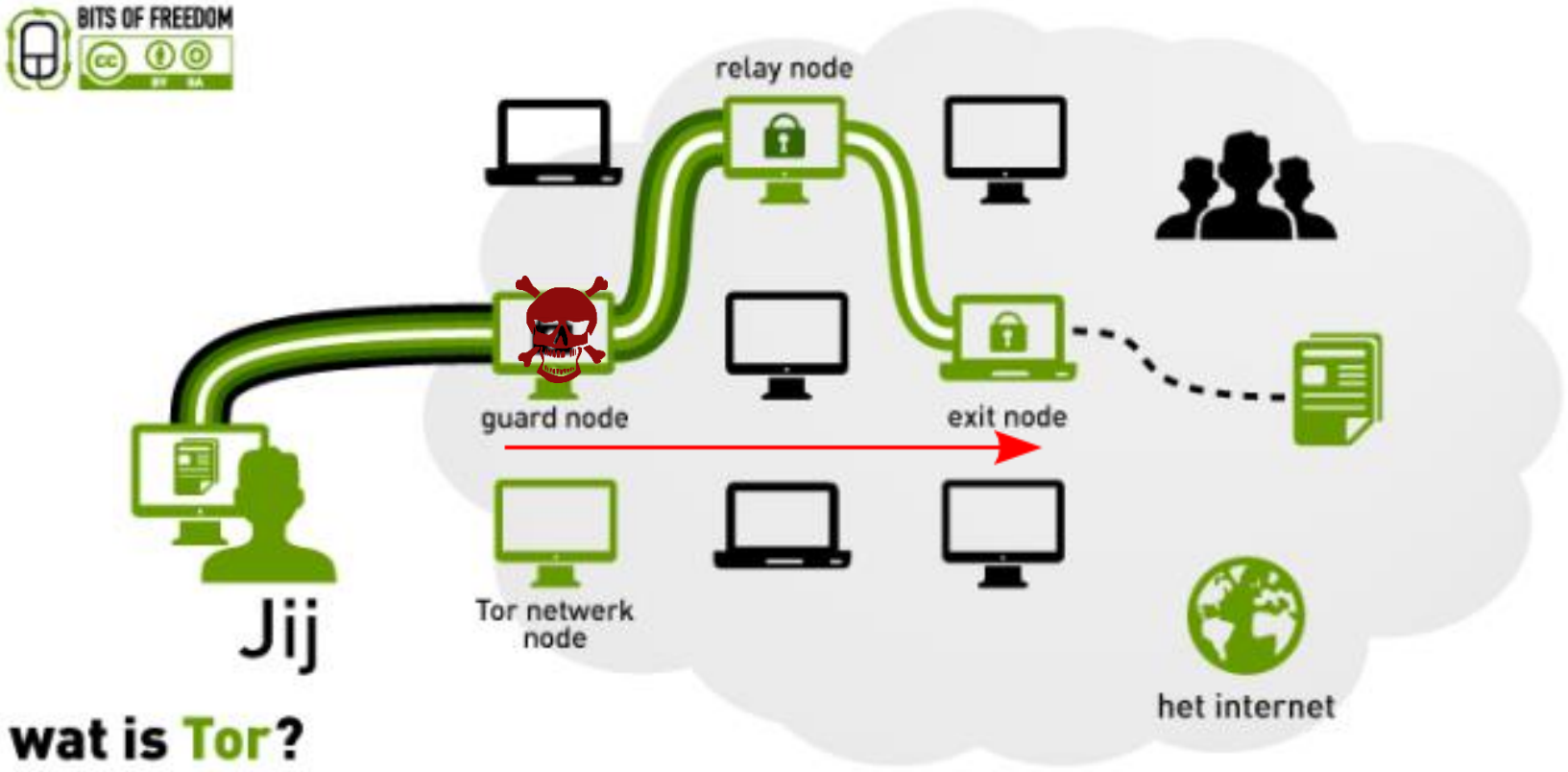
Big Loophole with TOR

- Exit Node of Tor is compromised, it is traceable



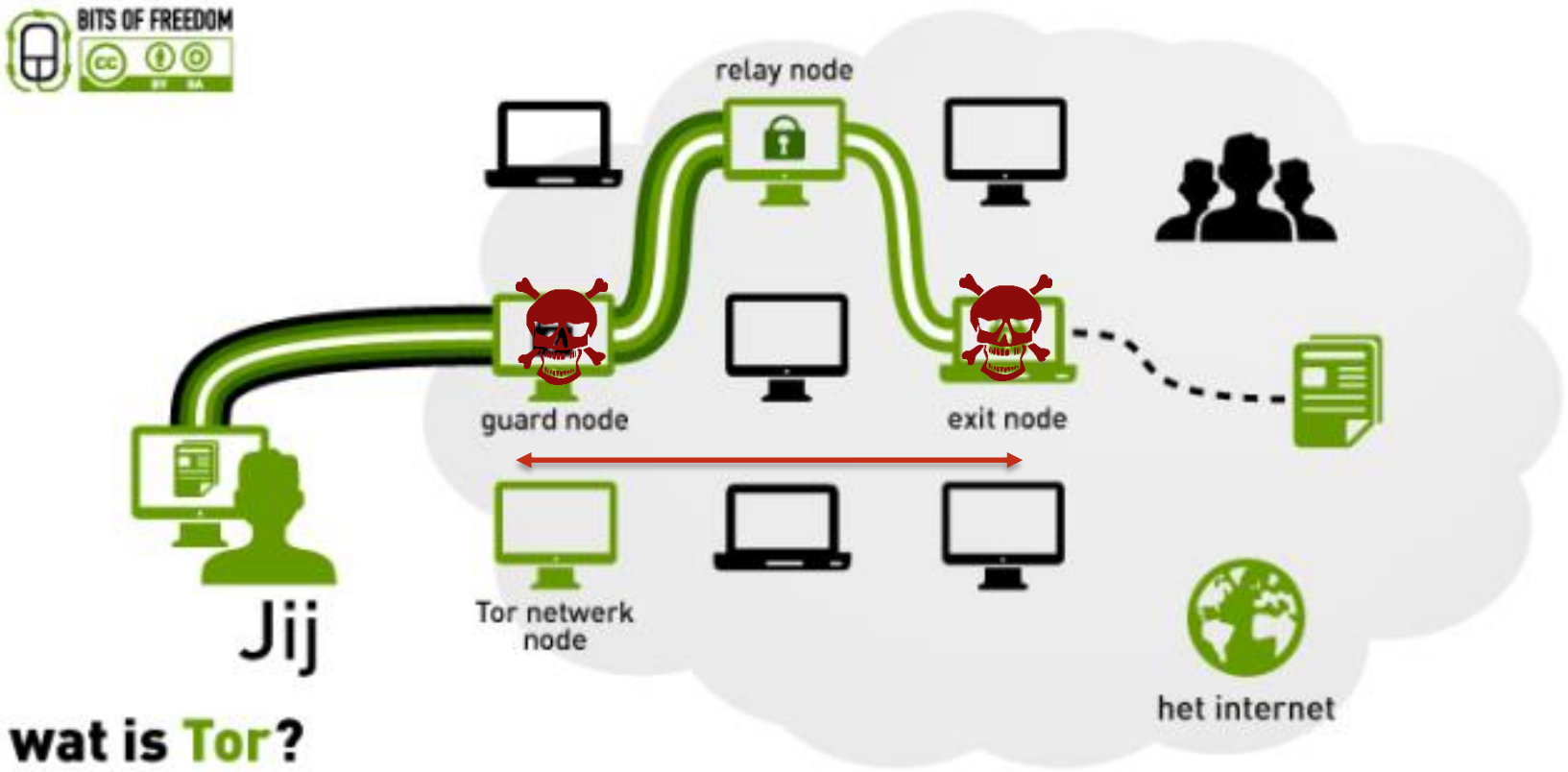
Big Loophole with TOR

- Entry Node of Tor is compromised, it is traceable



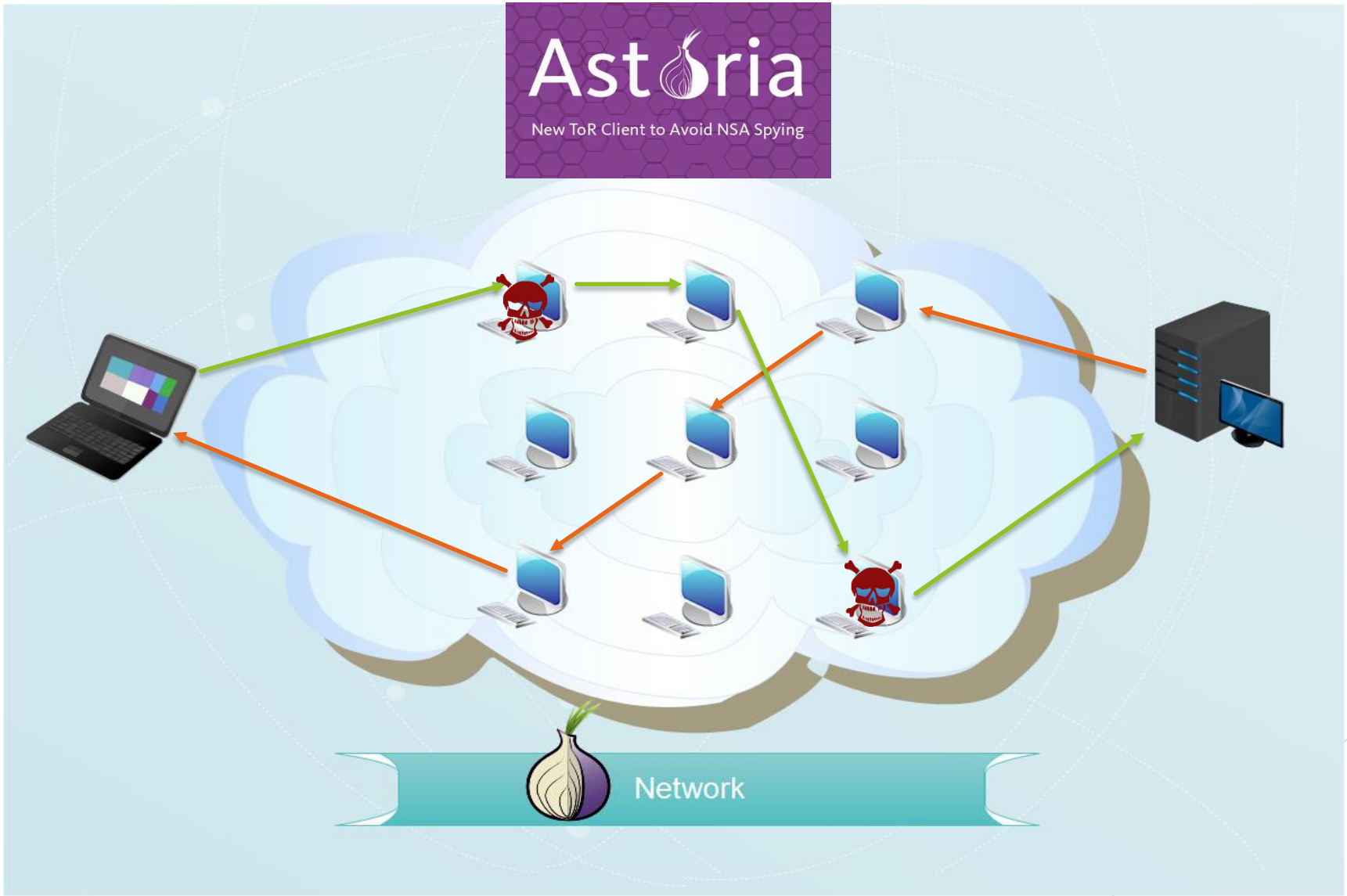
Big Loophole with TOR

- Entry Node & Exit Node of Tor is compromised, it is traceable



Overcoming Loophole with TOR (Back Tracing)

Working



Overcoming Loophole with TOR (Speed)

High Speed Onion Routing at Network Layer

- Only Symmetric Keys are used
- Hidden services select a rendezvous point and set up a session using the Sphinx protocol
- Then publish an AHDR to a directory that has the encrypted information about how to get from the rendezvous point to the service.

Note: Next Node Address intermediate node have to find and maintain Encryption Keys n Info.

But in Hornet this load is reduced

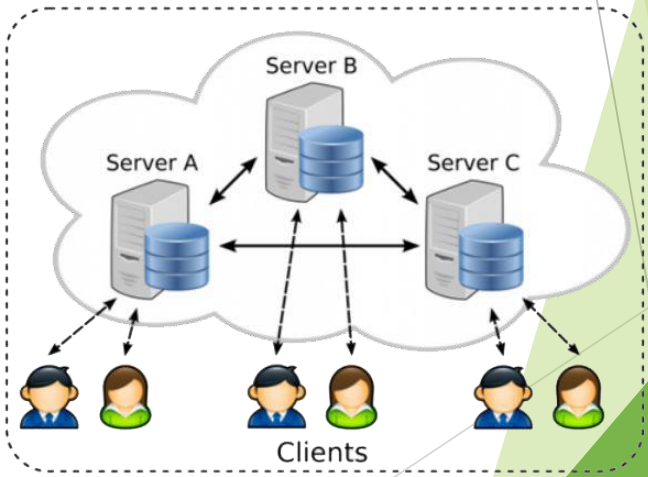
☹ But Still this is a paper with a tone of hypes

Overcoming Tor Several Attacks

Working

- Shuffle Data Packets at each server
- Random Shuffling of data packets will leave no trace for sender or receiver.

- Msg: 1 2 3 sent to server A then
- Server B will send 3 1 2
- Server C will send 3 2 1



Thank You...!!!