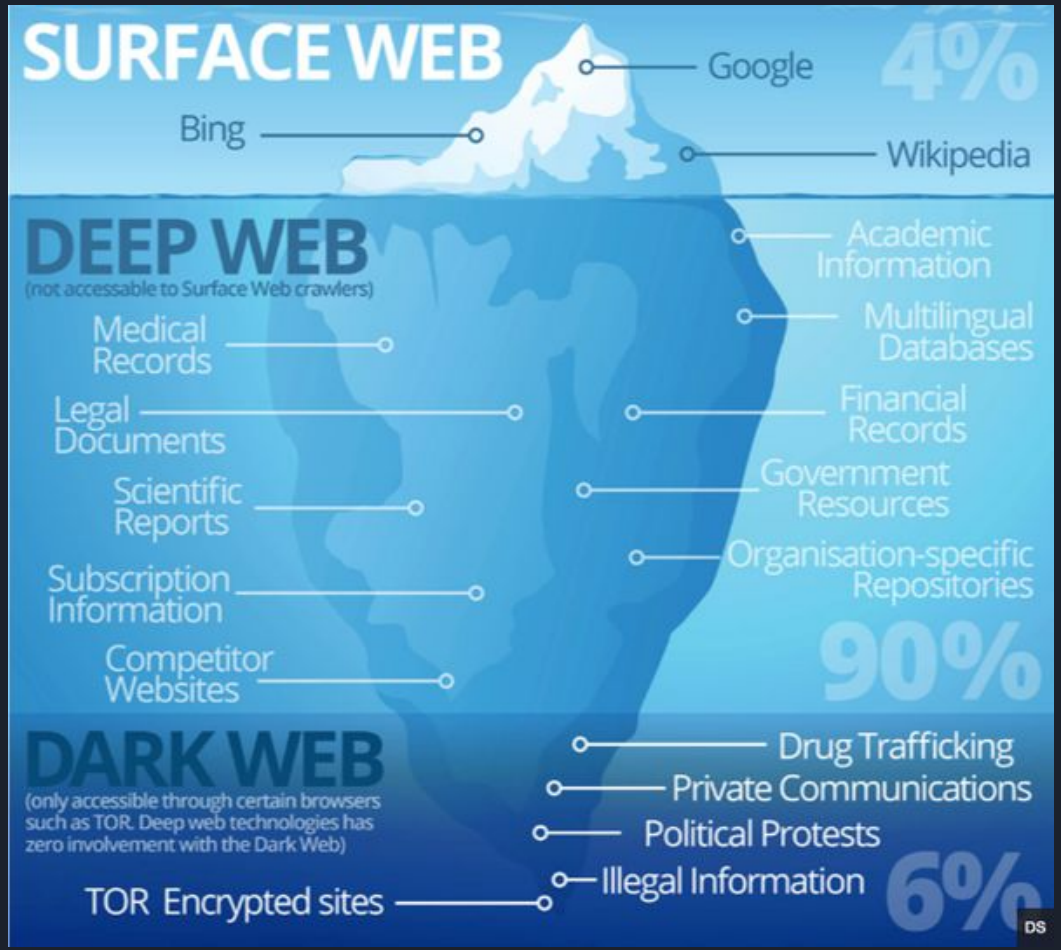
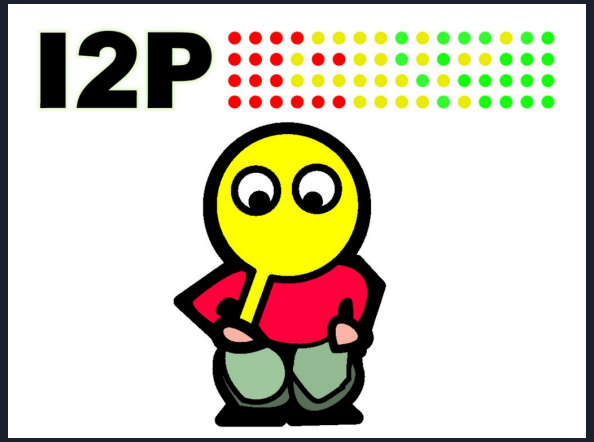
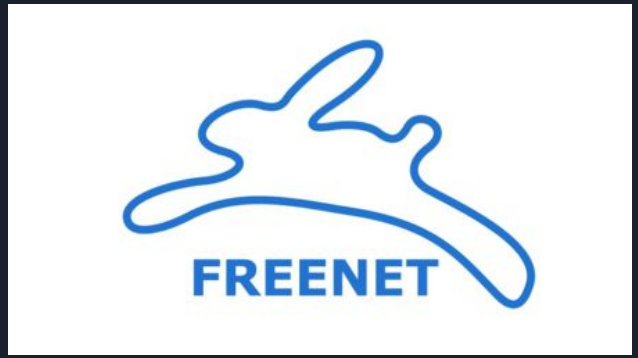
All about the Darknet


SURFACE WEB
Google
4%
Bing
Wikipedia
DEEP WEB
(not accessable to Surface Web crawlers)
Academic Information
Multilingual Databases
Medical Records
Financial Records
Legal Documents
Government Resources
Scientific Reports
Organisation-specific Repositories
Subscription Information
90%
Competitor Websites
DARK WEB
(only accessible through certain browsers such as TOR. Deep web technologies has zero involvement with the Dark Web)
Drug Trafficking
Private Communications
Political Protests
Illegal Information
TOR Encrypted sites
6%
DS


I2P

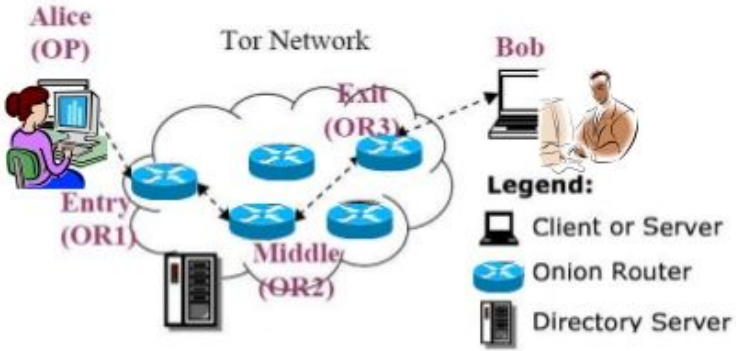

FREENET

Darknet

- a collection of different custom protocols built on top of standard protocols
- purposefully hidden

TOR

Components of TOR



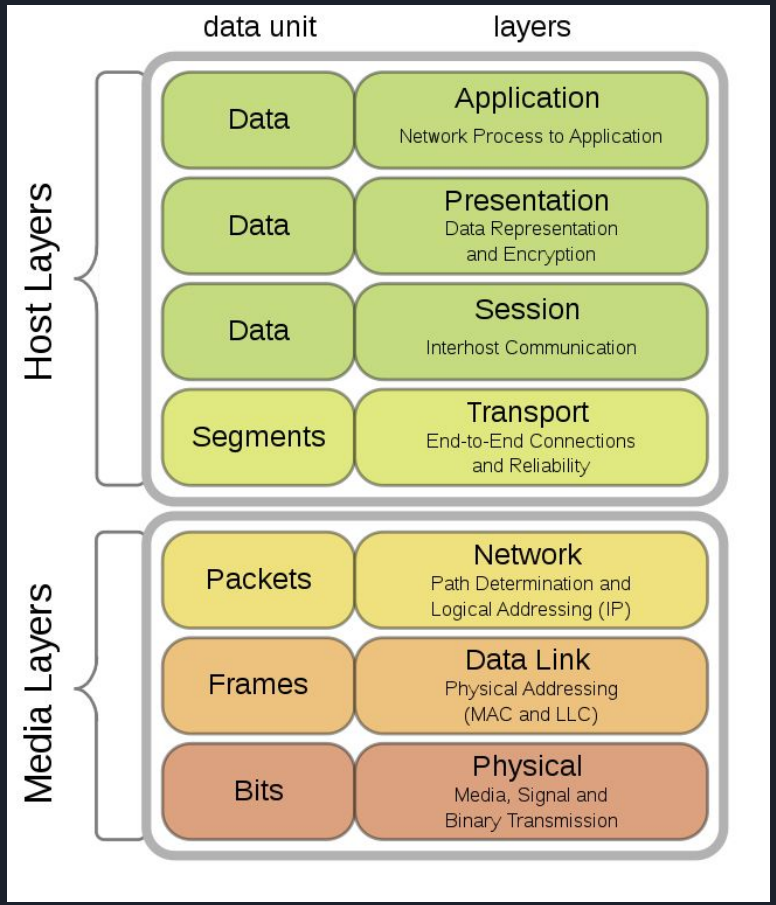
- **Client**: the user of the TOR network
- **Server**: the target TCP applications such as web servers
- **TOR (onion) router**: the special proxy relays the application data
- **Directory server**: servers holding TOR router information

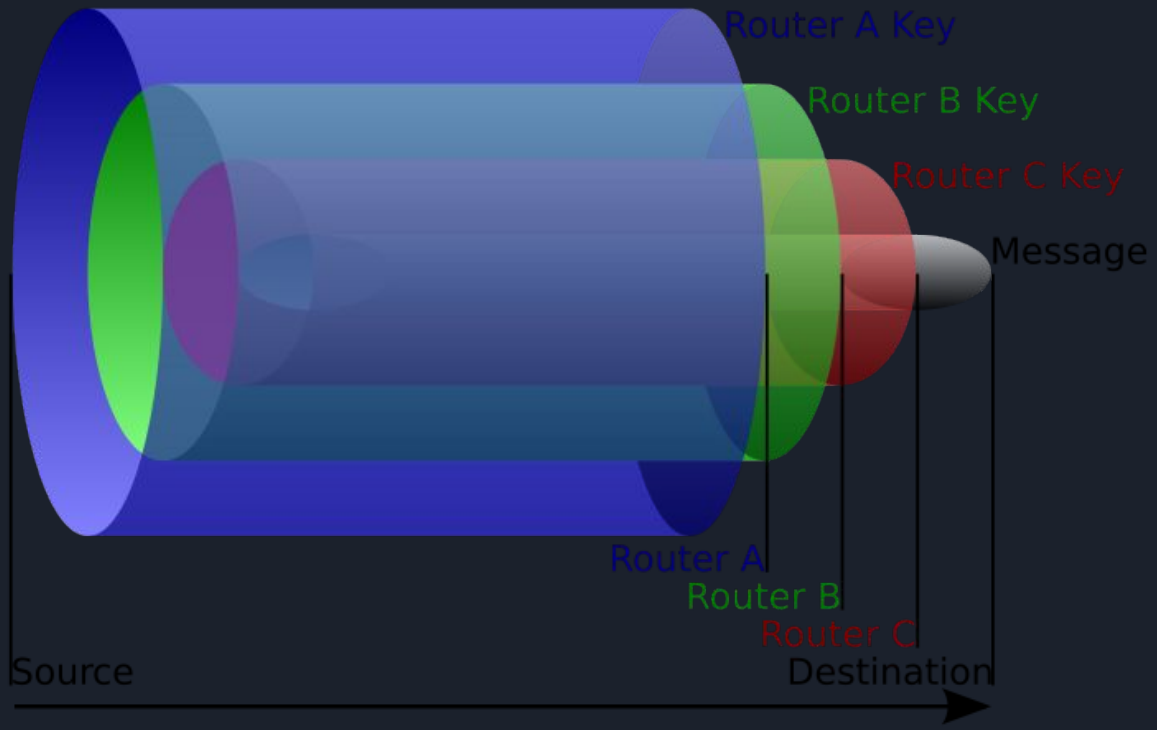
Types of Nodes

- Entry/Guard nodes
- Exit nodes
- Middle Relays
- Bridges

TOR

- You can route all TCP traffic through TOR
- TLS over TCP
- Recommended to use the TOR browser for connecting to .onion sites

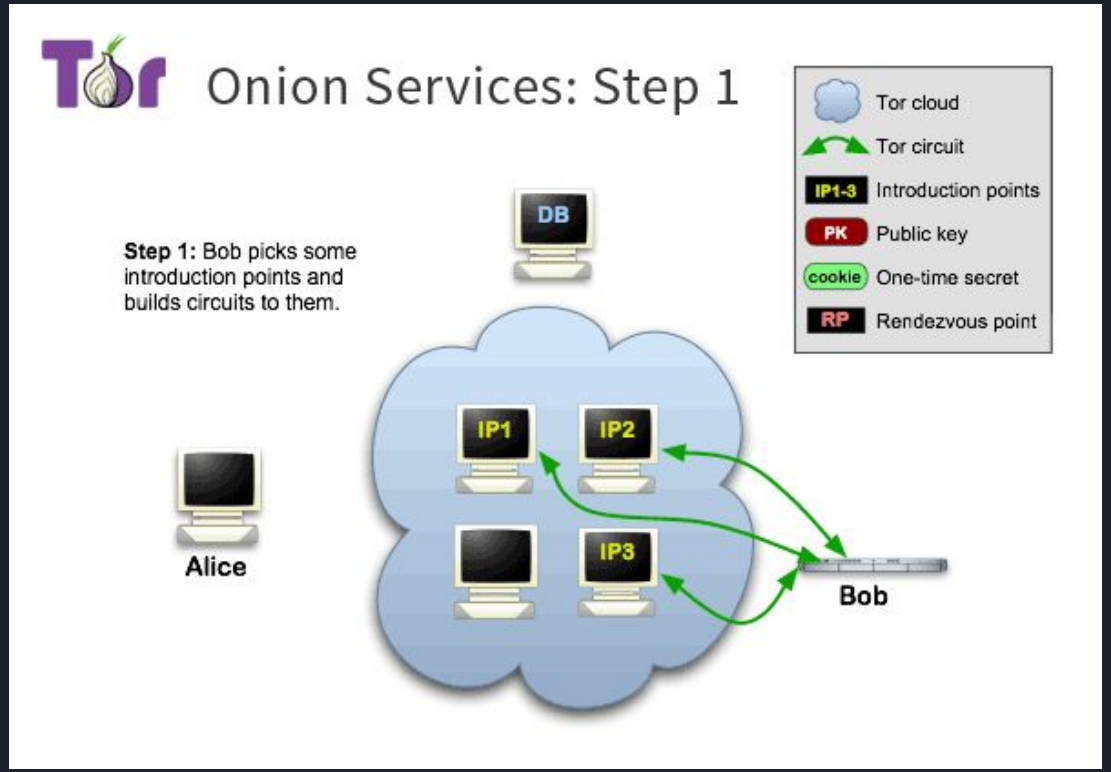

data unit
layers
Host Layers
Data
Application
Network Process to Application
Data
Presentation
Data Representation and Encryption
Data
Session
Interhost Communication
Segments
Transport
End-to-End Connections and Reliability
Media Layers
Packets
Network
Path Determination and Logical Addressing (IP)
Frames
Data Link
Physical Addressing (MAC and LLC)
Bits
Physical
Media, Signal and Binary Transmission


Router A Key
Router B Key
Router C Key
Message
Router A
Router B
Router C
Source
Destination

Hidden Services

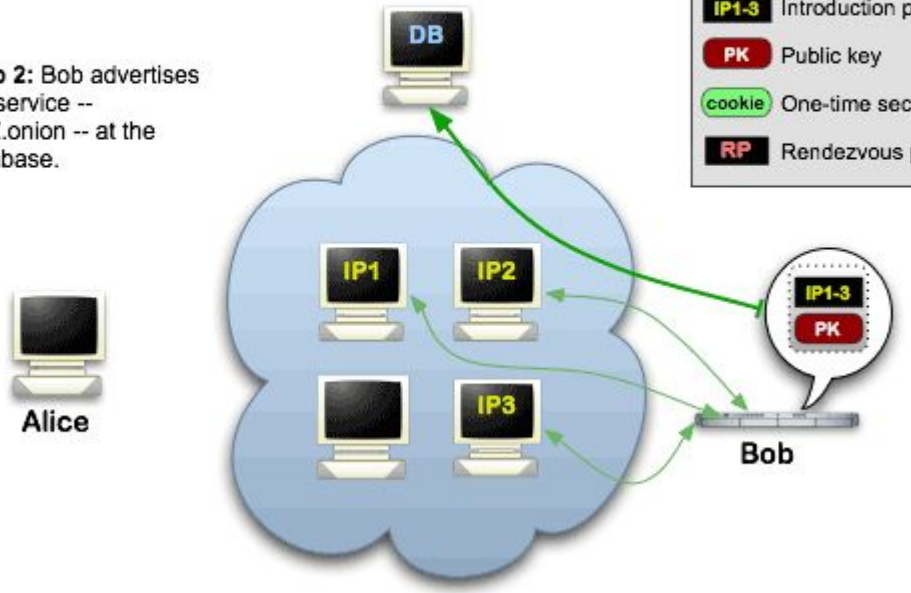
- Allows host to provide a service w/o exposing their IP address
- Can only connect via TOR
- Clients can connect via a chosen rendezvous point

Onion Services: Step 1



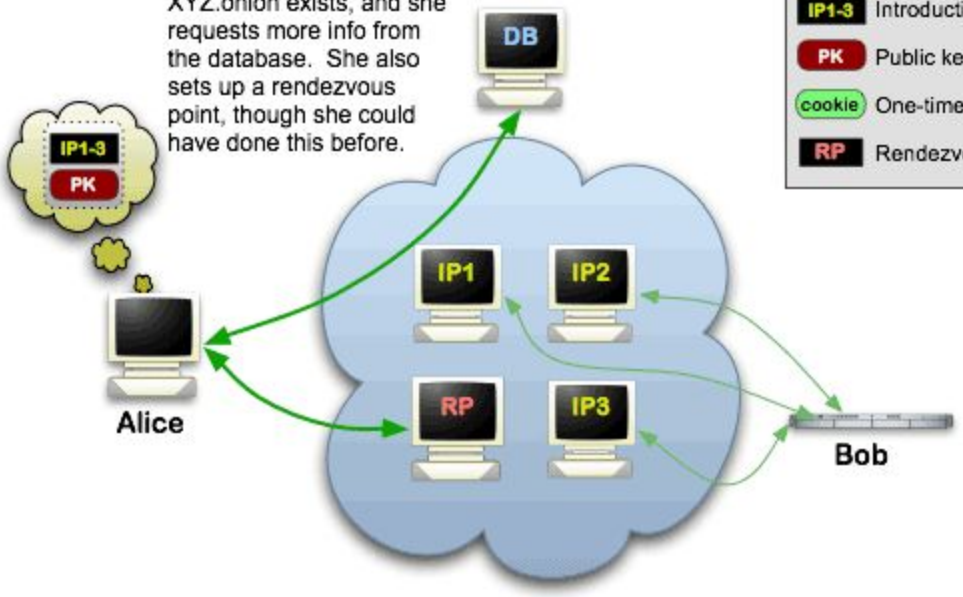
Onion Services: Step 2

Step 2: Bob advertises his service -- XYZ.onion -- at the database.



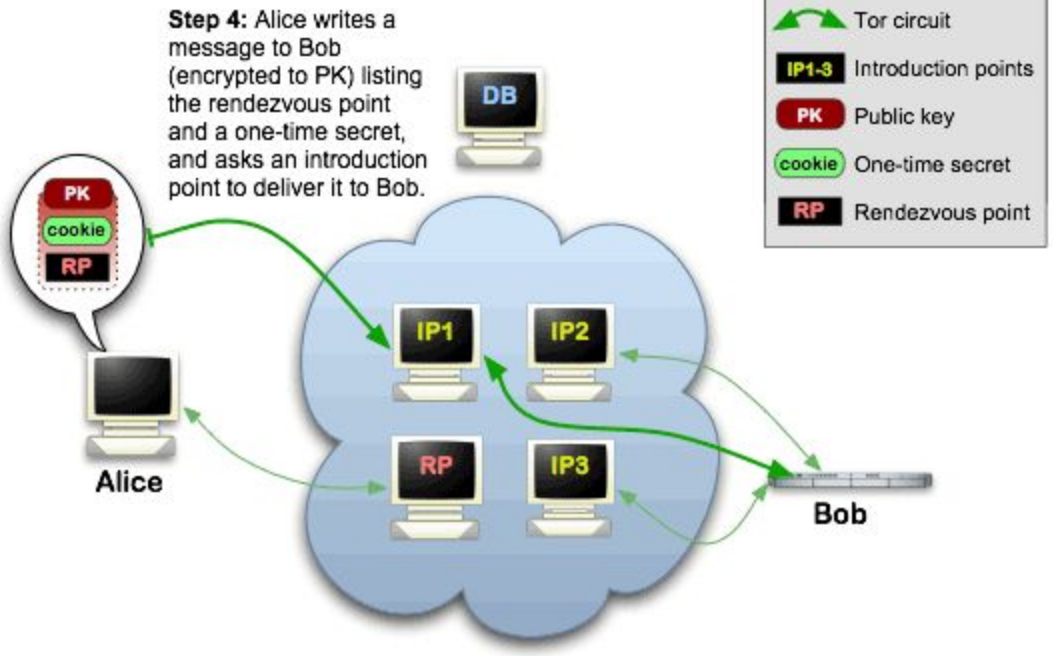
Onion Services: Step 3

Step 3: Alice hears that XYZ.onion exists, and she requests more info from the database. She also sets up a rendezvous point, though she could have done this before.



- Tor cloud
- Tor circuit
- IP1-3 Introduction points
- PK Public key
- cookie One-time secret
- RP Rendezvous point

Onion Services: Step 4



NOTE:

You can still easily get caught while using TOR if you’re being a brainlet.

Exhibit A: Harvard Bomb Hoax

- TLDR: A Harvard student got caught sending a fake bomb threat to the school to get out of finals
- Mistake 1: Using TOR on school wifi
- Could have used a bridge or walked to the nearest McDonalds w/ wifi

Exhibit B: Lulzsec

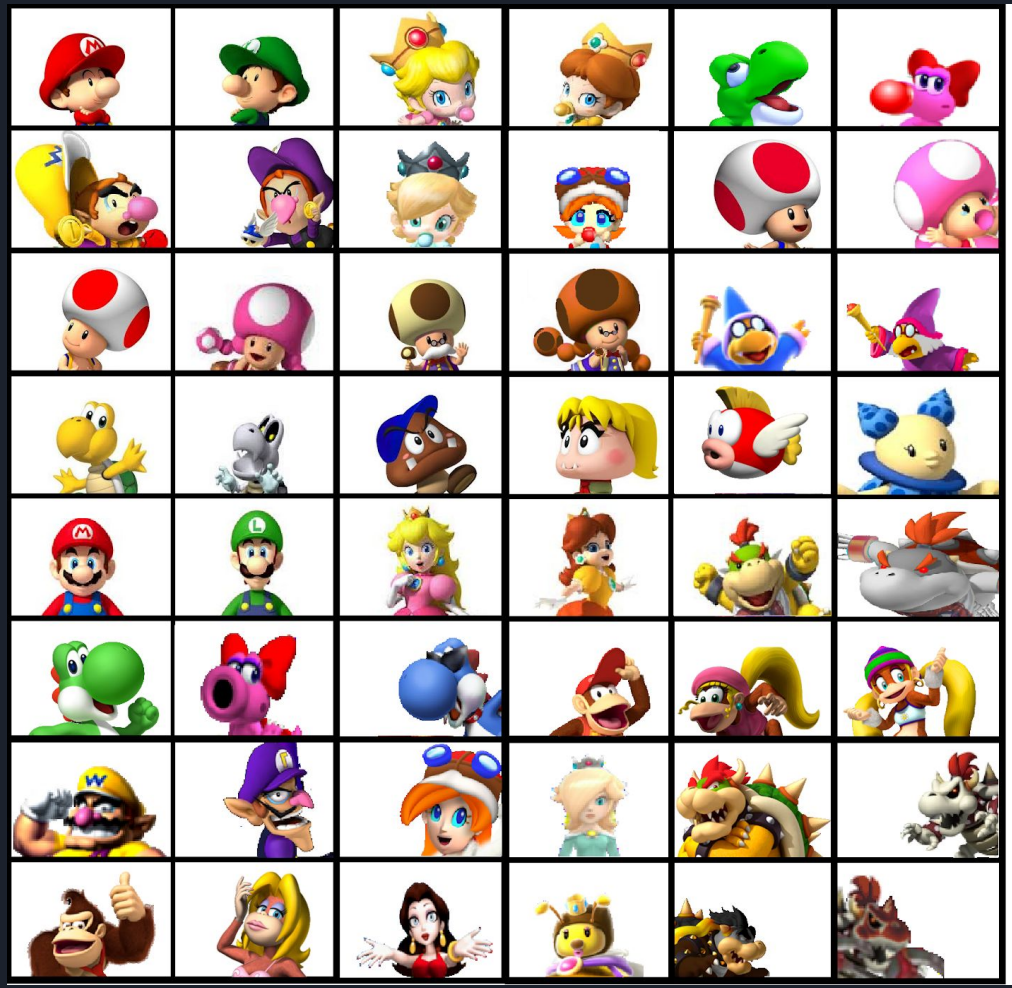
- TLDR: Hacker group that got busted by the FBI because one galaxy brain connected to IRC via clearnet

Main TOR weaknesses

- can get pawned by exit node if the onion service doesn’t encrypt their traffic
- pretty easy to tell if you’re using TOR
- can be vulnerable to correlation attacks

Roleplaying Time


VENEZUELA
COLOMBIA
PANAMA
COSTA RICA
NICARAGUA
EL SALVADOR
GUATEMALA
HONDURAS
BELIZE
JAMAICA
HAITI
CUBA
THE BAHAMAS
Gulf of Mexico
CARIBBEAN SEA
ATLANTIC OCEAN
PACIFIC OCEAN
ARCTIC OCEAN
Geographic Information and Flags of All North American Countries
TEXAS
ONTARIO
QUEBEC
ALASKA
Greenland
Baffin Bay
LABRADOR SEA
BEAUFORT SEA
RUSSIA



Baby Weight

Light Weight

Medium Weight

Heavy Weight

Step 1:

- Use Tails or Whonix
- Mario should make sure to encrypt his Tails Persistent Boot

Step 2

- Acquire some crypto
- Mario would use Monero if possible, but Toad is a normie and only accepts Bitcoin
- Mario should transfer his crypto to a second wallet for plausible deniability(this second wallet should be located on his Tails distro)

Step 3

- Always buy w/in the mushroom kingdom
- Speed = Safety!
- Mario should use his own name to avoid suspicion
- Mario should encrypt his address w/ Toad's PGP key