

A decorative graphic on the left side of the slide. It consists of a blue parallelogram and a light green parallelogram, both tilted at an angle. The blue shape is in the foreground, and the green shape is partially behind it. They are set against a dark blue background with faint, lighter blue diagonal stripes.

# All about the Darknet

# SURFACE WEB

Bing

Google

Wikipedia

4%

# DEEP WEB

(not accessible to Surface Web crawlers)

Medical  
Records

Legal  
Documents

Scientific  
Reports

Subscription  
Information

Competitor  
Websites

Academic  
Information

Multilingual  
Databases

Financial  
Records

Government  
Resources

Organisation-specific  
Repositories

90%

# DARK WEB

(only accessible through certain browsers  
such as TOR. Deep web technologies has  
zero involvement with the Dark Web)

TOR Encrypted sites

Drug Trafficking

Private Communications

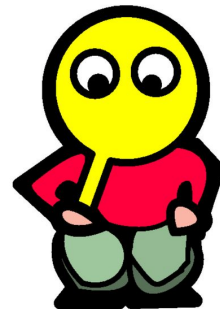
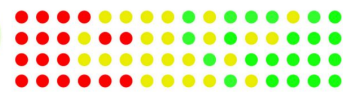
Political Protests

Illegal Information

6%



**I2P**



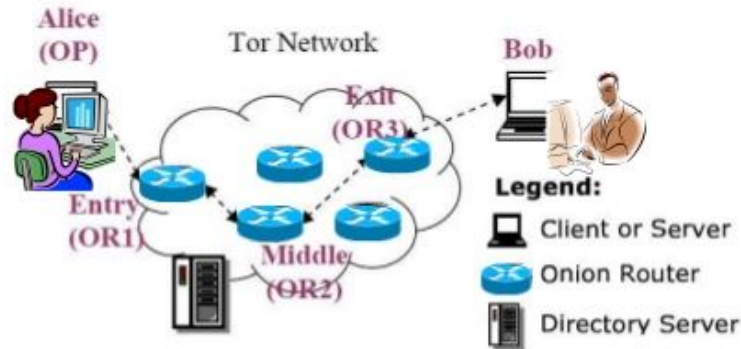


# Darknet

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

# TOR

## Components of TOR

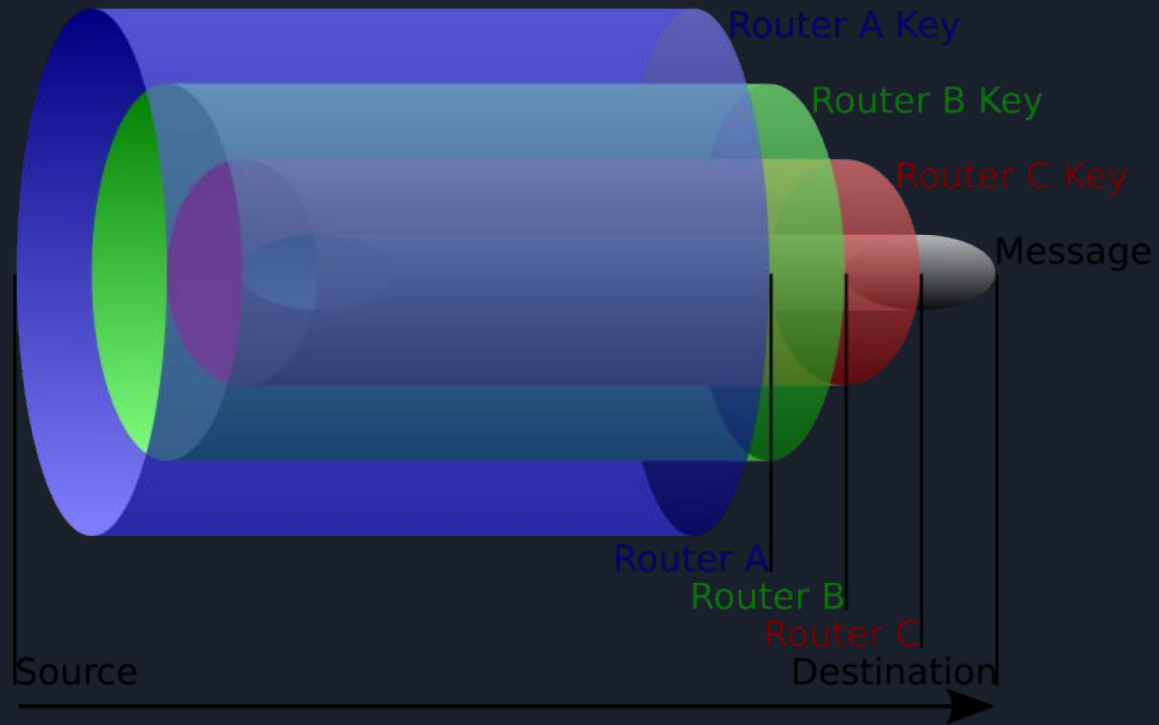


- **Client:** the user of the TOR network
- **Server:** the target TCP applications such as web servers
- **TOR (onion) router:** the special proxy relays the application data
- **Directory server:** servers holding TOR router information



# TOR

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





## 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

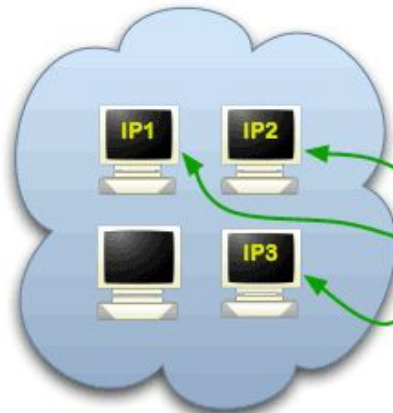
**Step 1:** Bob picks some introduction points and builds circuits to them.



Alice



DB



Bob

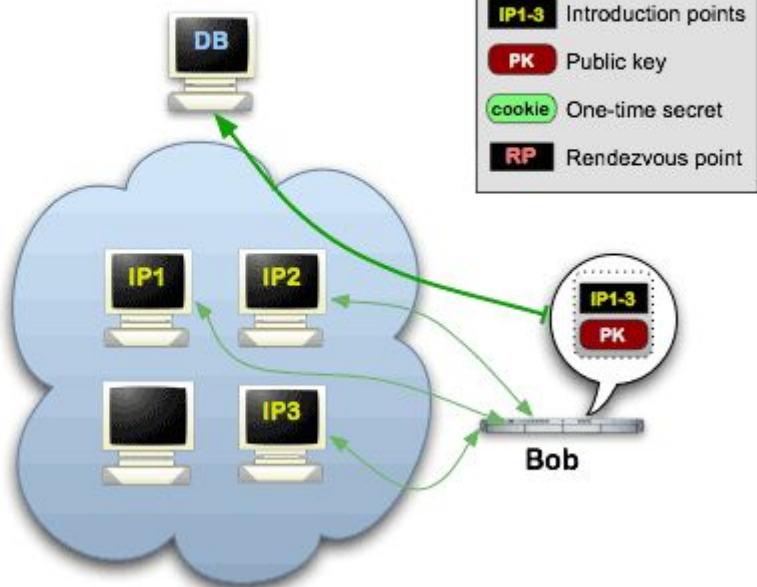


## Onion Services: Step 2

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



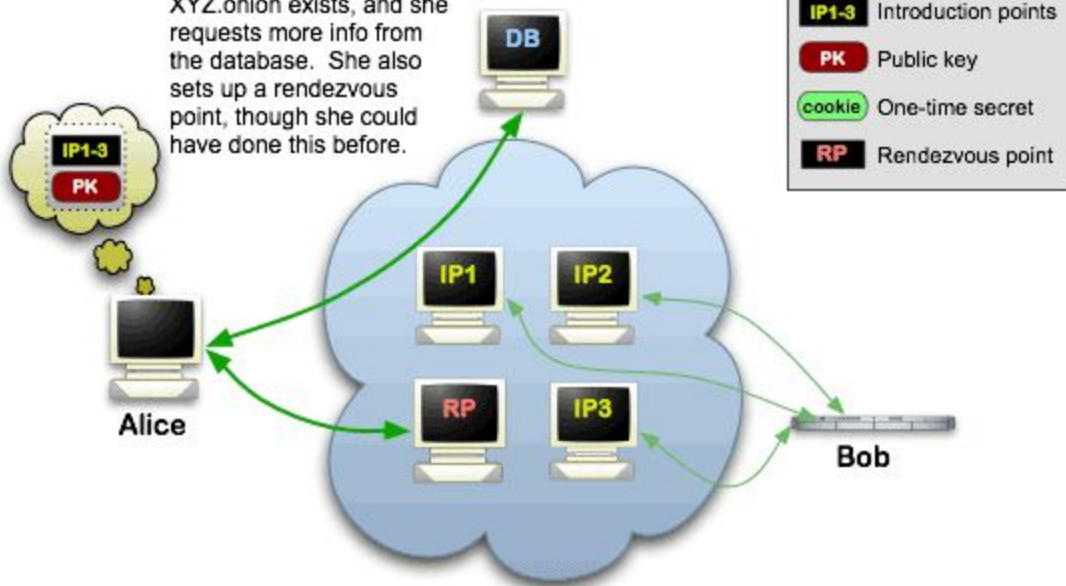
Alice





## Onion Services: Step 3

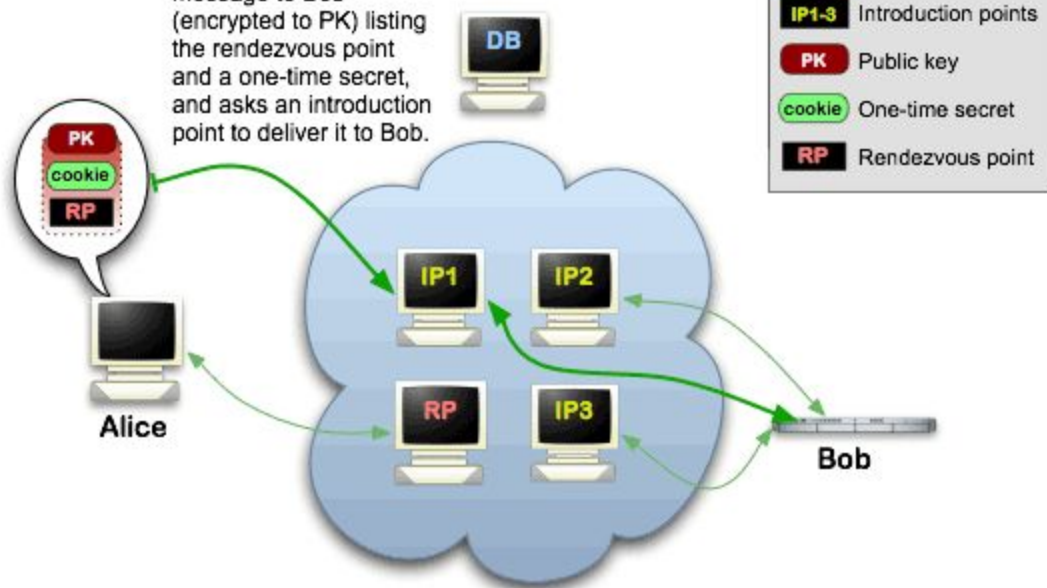
**Step 3:** Alice hears that XYZ.onion exists, and she requests more info from the database. She also sets up a rendezvous point, though she could have done this before.





## Onion Services: Step 4

**Step 4:** Alice writes a message to Bob (encrypted to PK) listing the rendezvous point and a one-time secret, and asks an introduction point to deliver it to Bob.





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

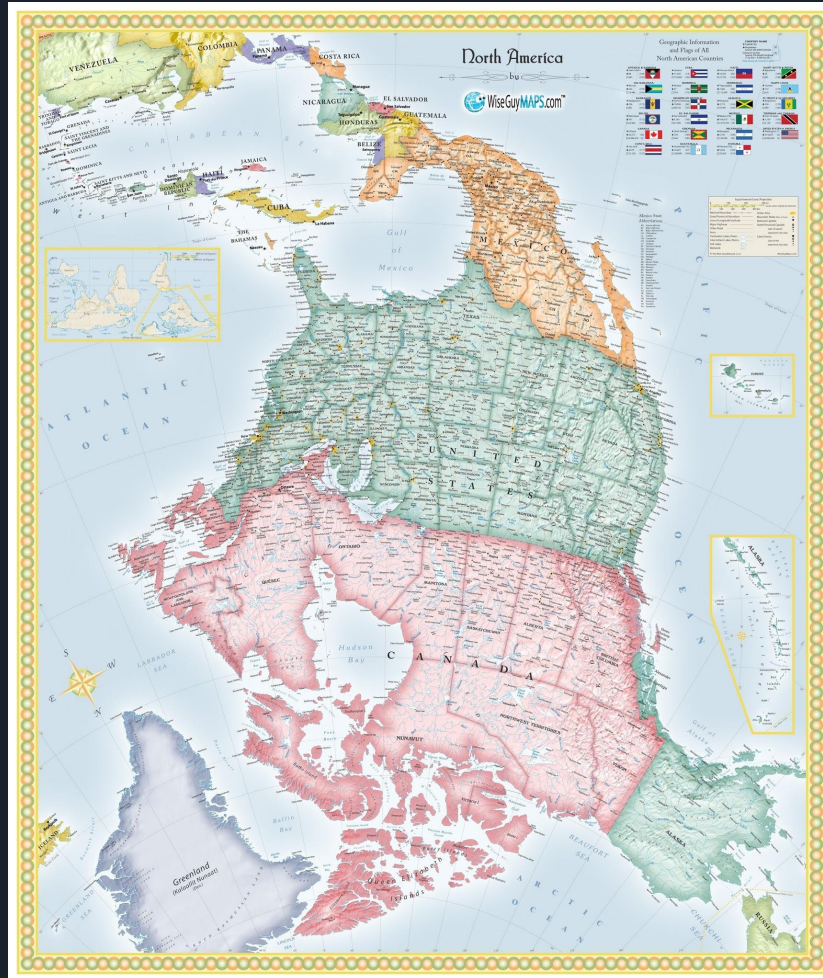
- can get pawned by exit node if the onion service doesn't encrypt their traffic
- pretty easy to tell if you're using TOR
- can be vulnerable to correlation attacks



# Roleplaying Time









## Step 1:

- Use Tails or Whonix
- Make sure you encrypt your Tails Live Boot



## Step 2

- Acquire some crypto
- Monero is recommended, but sometimes vendors only accept Bitcoin
- Make sure you transfer your bitcoin to another account for plausible deniability (this wallet should be on your Tails Live Boot)



## Step 3

- Always buy domestic
- Choose the fastest shipping option available
- Don't use a fake name, or deliver it to a PO box,
- Encrypt your address w/ the vendor's PGP key

<http://4mtu5pl6yp3fmvny.goomba/?ai=1675>