CSCI 466: Networks

Halloween Special – TOR, Dark Net, Anonymity

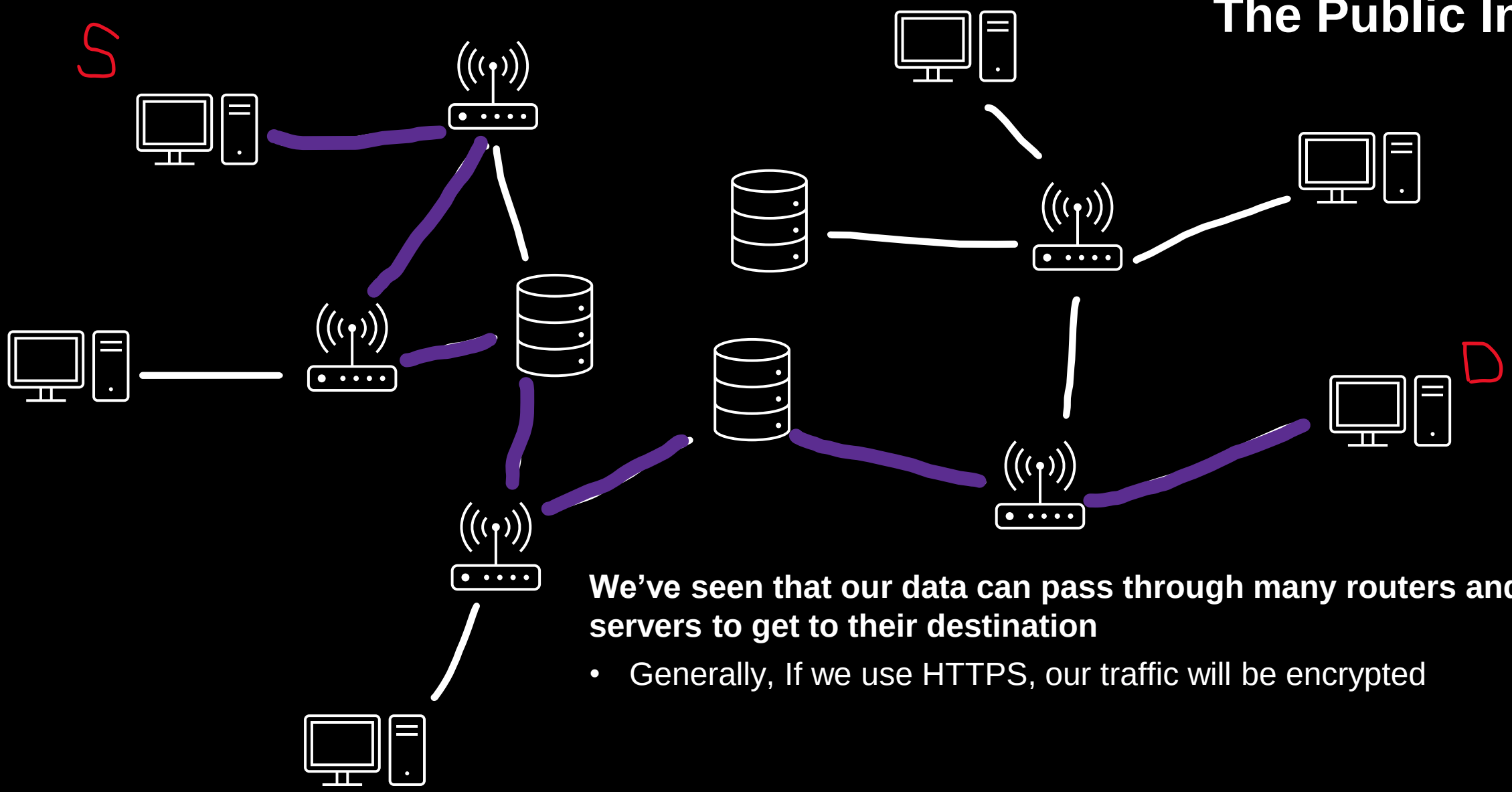
Trigger warning: We will briefly be mentioning sexual abuse and exploitation via the internet

*All images are stolen from the internet

Announcements

- **PA3 due Nov 11th @ 11:59 PM**
- **I might be on a watch list**

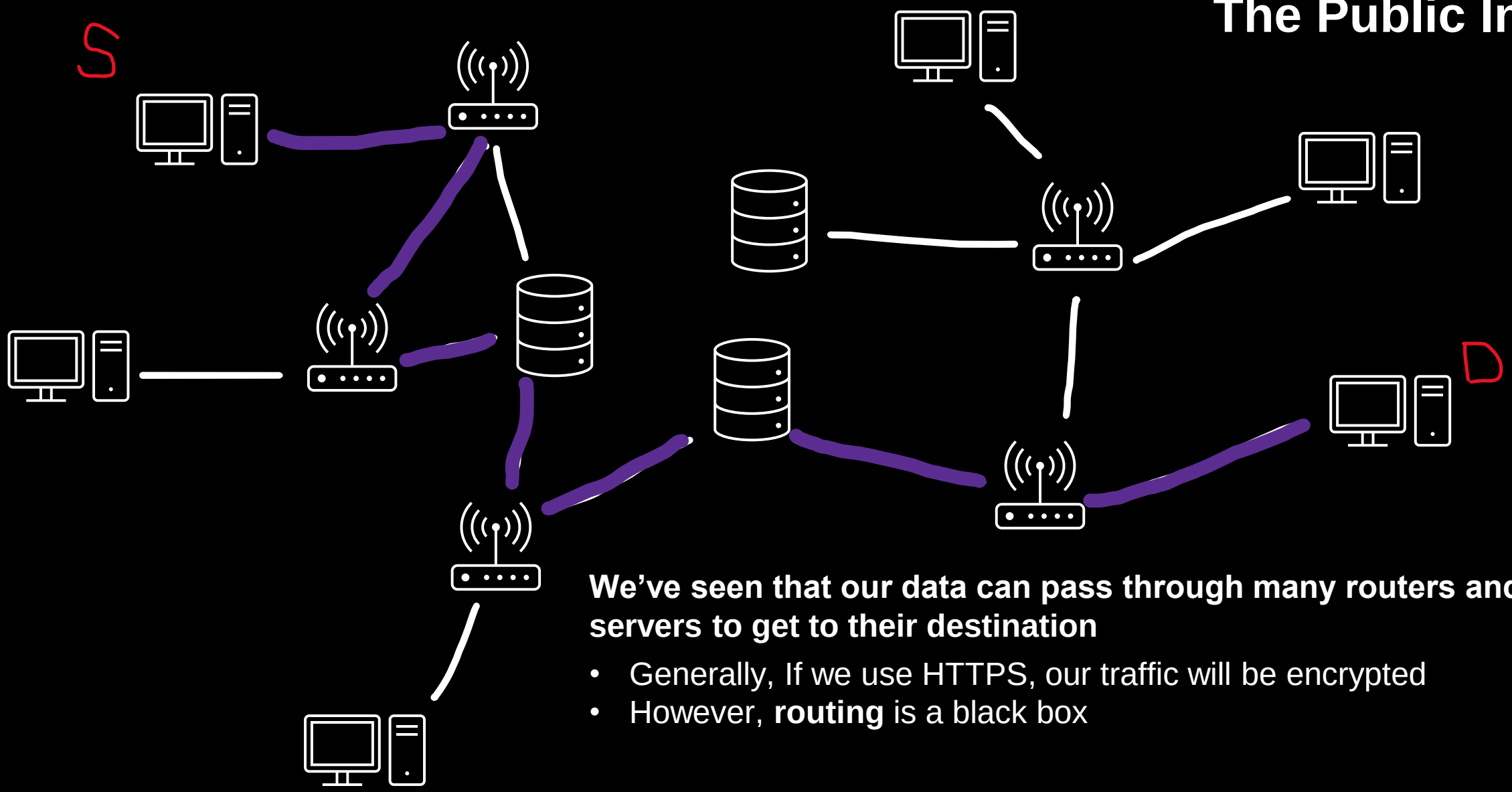
The Public Internet



We've seen that our data can pass through many routers and servers to get to their destination

- Generally, If we use HTTPS, our traffic will be encrypted

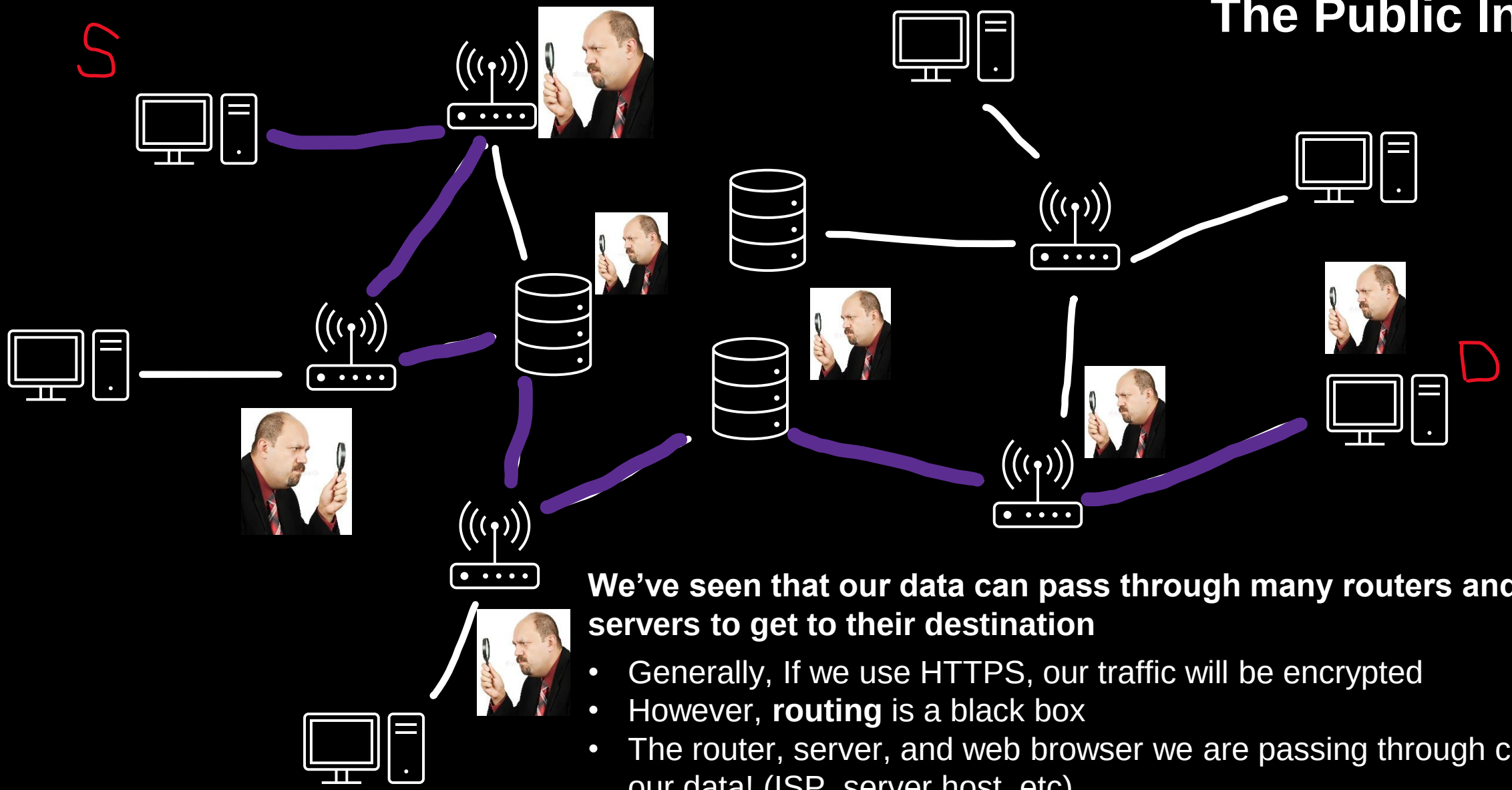
The Public Internet



We've seen that our data can pass through many routers and servers to get to their destination

- Generally, If we use HTTPS, our traffic will be encrypted
- However, **routing** is a black box

The Public Internet



We've seen that our data can pass through many routers and servers to get to their destination

- Generally, If we use HTTPS, our traffic will be encrypted
- However, **routing** is a black box
- The router, server, and web browser we are passing through can track our data! (ISP, server host, etc)
  → IP address, Cookies, physical location

The Public Internet

servers destination

- Generally, If we use HTTPS, our traffic will be encrypted
- However, **routing** is a black box
- The router, server, and web browser we are passing through can track our data! (ISP, server host, etc)
  → IP address, Cookies, physical location

TOR (The Onion Router)

- Developed by US Naval Research Laboratory to protect American Intelligence Communications online. Released publicly in 2004

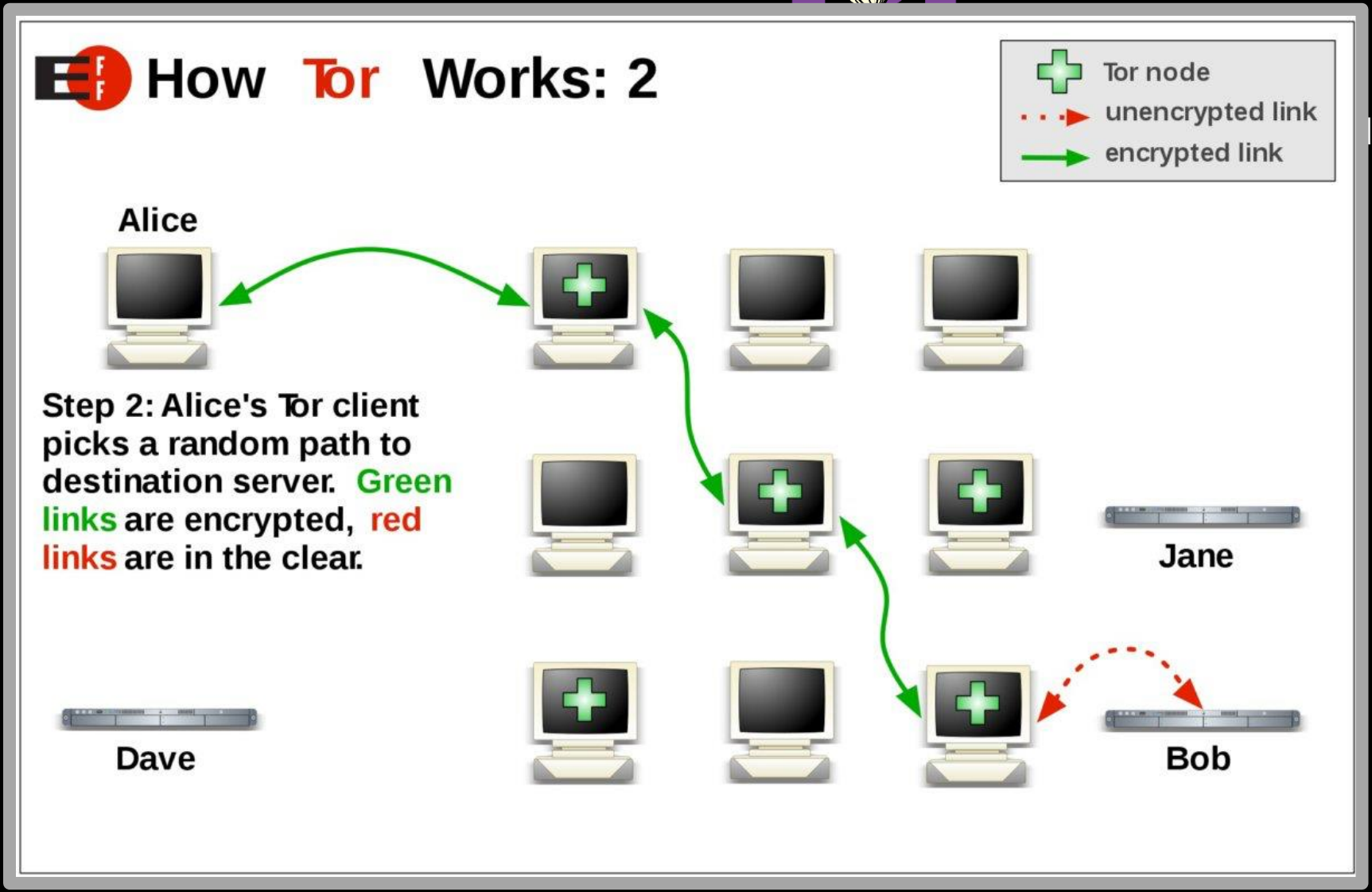
TOR (The Onion Router)

- Developed by US Naval Research Laboratory to protect American Intelligence Communications online. Released publicly in 2004

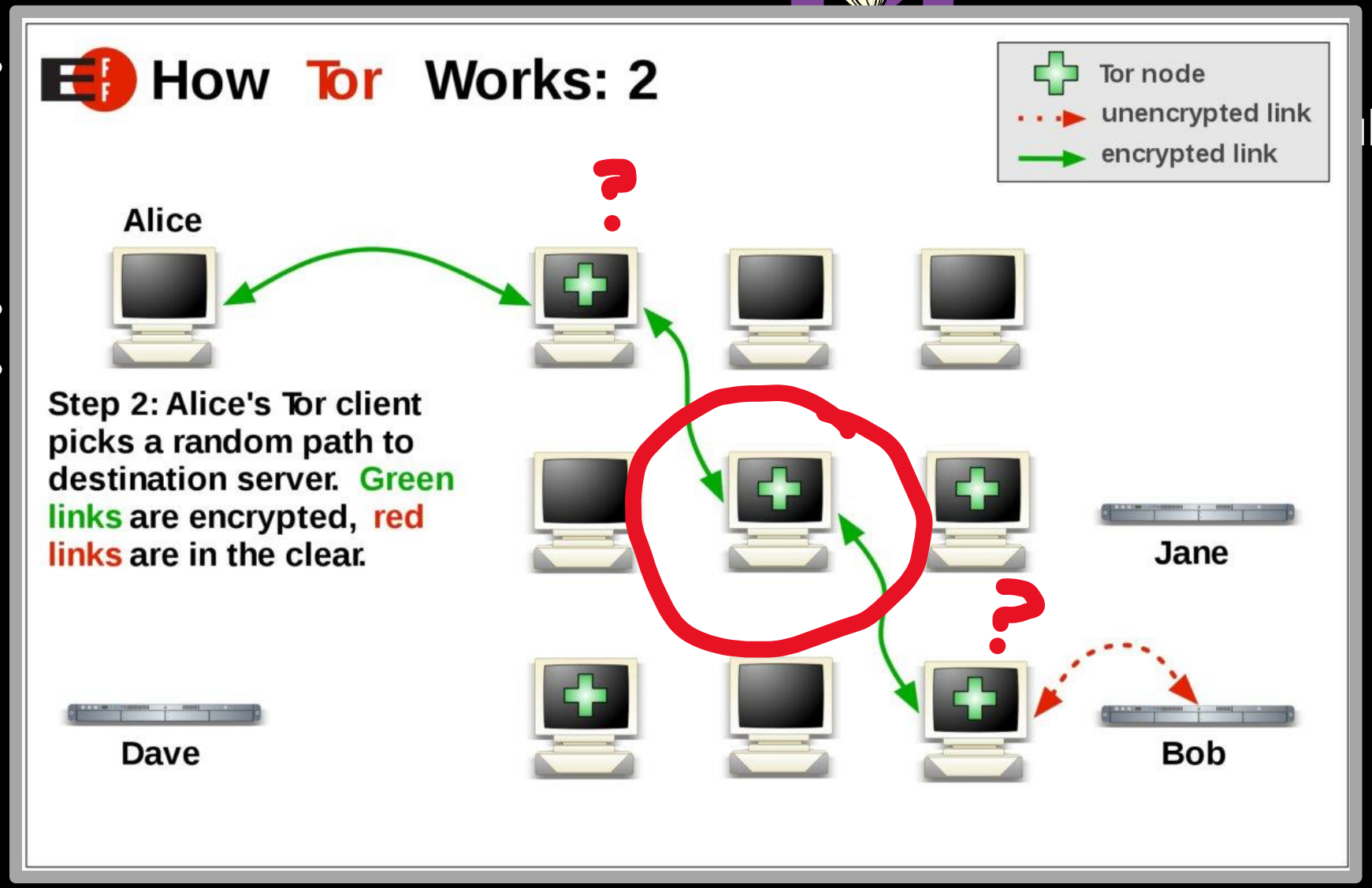
- Built on P2P architecture,
- → Messages are passed through a network of Tor nodes.

TOR (The Onion Router)

- blicly



TOR (The Onion Router)

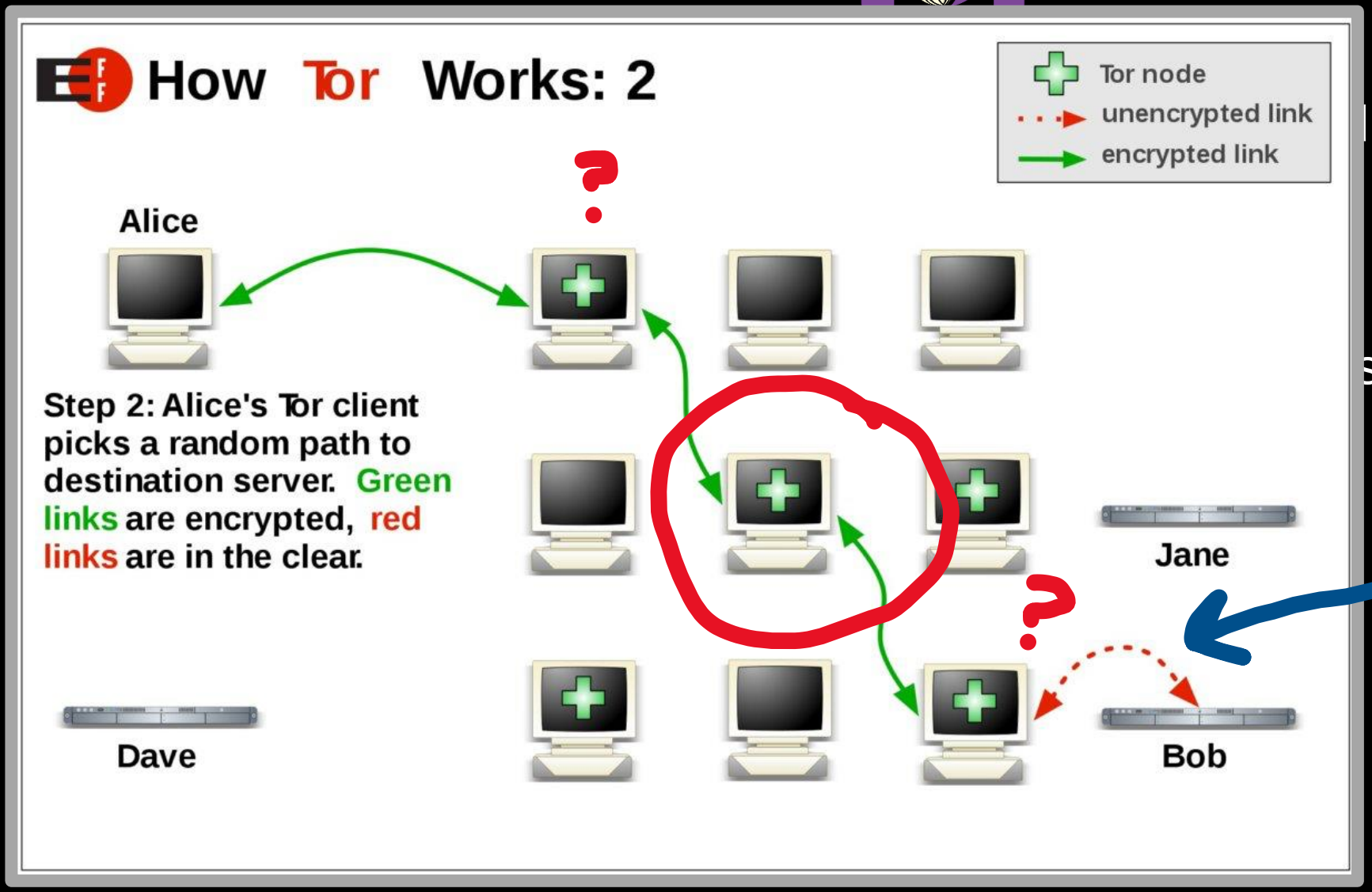


- blicly

From this Node's perspective it only can see the previous node and the next node

It has no idea who the original sender was

TOR (The Onion Router)



publicly

s.

Not totally safe. Messages leaving an “exit node” will be in cleartext

Random path each time!

TOR (The Onion Router)

- Developed by US Naval Research Laboratory to protect American Intelligence Communications online. Released publicly in 2004

- Built on P2P architecture,
- → Messages are passed through a network of Tor nodes.
- → Encrypted throughout the entire process. Cant tell who sent what

- Browser can be found online as a modified version of Firefox (Slow)
- → You can visit `.onion` links

TOR (The Onion Router)

Onion Links websites that are not accessible by normal web browser
→ **.onion instead of .com, .net, etc**

TOR (The Onion Router)

Onion Links websites that are not accessible by normal web browser
→ **.onion instead of .com, .net, etc**

We next need to understand how search engines store, or **index** webpages

Web browsers will utilize a **web crawler** that automatically scans the internet and pulls the static content

This content is put into a database (the same database we use when we search for stuff)

A special algorithm is used to rank indexed content based on relevancy

TOR (The Onion Router)

- Developed by US Naval Research Laboratory to protect American Intelligence Communications online. Released publicly in 2004

- Built on P2P architecture,
- → Messages are passed through a network of Tor nodes.
- → Encrypted throughout the entire process. Cant tell who sent what

- Browser can be found online as a modified version of Firefox (Slow)
- → You can visit `.onion` links

TOR (The Onion Router)

- Developed by US Naval Research Laboratory to protect American Intelligence Communications online. Released publicly in 2004

- Built on P2P architecture,
- → Messages are passed through a network of Tor nodes.
- → Encrypted throughout the entire process. Cant tell who sent what

- Browser can be found online as a modified version of Firefox (Slow)
- → You can visit `.onion` links

- "Good" uses for TOR browser:

TOR (The Onion Router)

- Developed by US Naval Research Laboratory to protect American Intelligence Communications online. Released publicly in 2004

- Built on P2P architecture,
- → Messages are passed through a network of Tor nodes.
- → Encrypted throughout the entire process. Cant tell who sent what

- Browser can be found online as a modified version of Firefox (Slow)
- → You can visit `.onion` links

- "Good" uses for TOR browser:
- → Online privacy, Governments that censor and heavily monitor the internet

TOR (The Onion Router)

- Developed by US Naval Research Laboratory to protect American Intelligence Communications online. Released publicly in 2004

- Built on P2P architecture,
- → Messages are passed through a network of Tor nodes.
- → Encrypted throughout the entire process. Cant tell who sent what

- Browser can be found online as a modified version of Firefox (Slow)
- → You can visit `.onion` links

- "Good" uses for TOR browser:
- → Online privacy, Governments that censor and heavily monitor the internet

- "Bad" uses for TOR browser:
- →

TOR (The Onion Router)

- Developed by US Naval Research Laboratory to protect American Intelligence Communications online. Released publicly in 2004

- Built on P2P architecture,
- → Messages are passed through a network of Tor nodes.
- → Encrypted throughout the entire process. Cant tell who sent what

- Browser can be found online as a modified version of Firefox (Slow)
- → You can visit `.onion` links

- "Good" uses for TOR browser:
- → Online privacy, Governments that censor and heavily monitor the internet

- "Bad" uses for TOR browser:
- → Criminal Activity that is difficult to track

Practically impossible to conduct mass surveillance

The Depth of the Internet

Onion Links websites that are not accessible by normal web browser
→ **.onion instead of .com, .net, etc**

What sort of things will not be indexed by our web browser?

The Depth of the Internet

Onion Links websites that are not accessible by normal web browser
→ **.onion instead of .com, .net, etc**

What sort of things will not be indexed by our web browser?

→ Dynamic content, content that requires authentication, passwords, etc

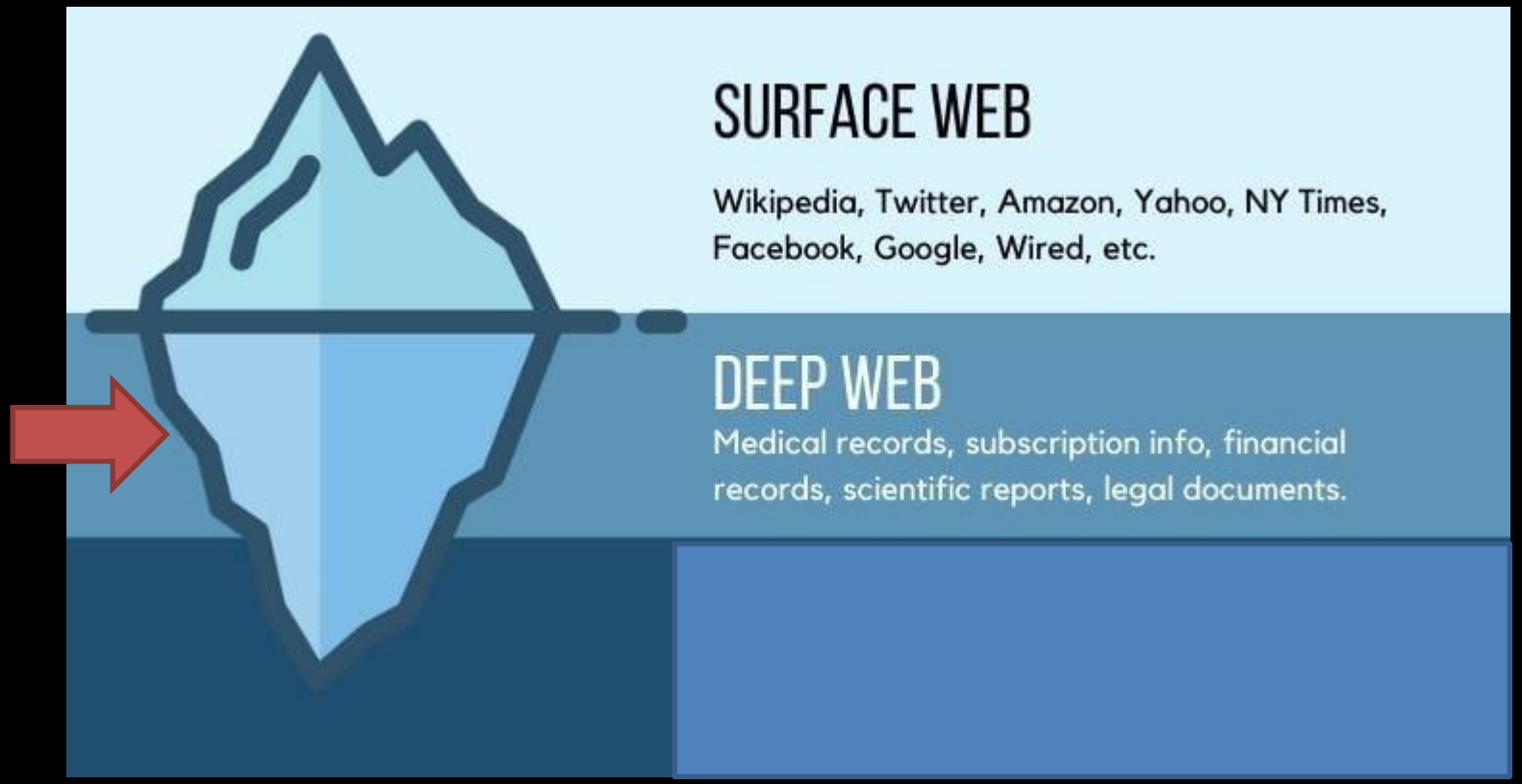
The Depth of the Internet

Onion Links websites that are not accessible by normal web browser
→ **.onion instead of .com, .net, etc**

The **deep web** is the area of the internet that is not accessible by normal browsers (90%)

- This includes information such as emails, financial information, records, private social media content, personal data

Pretty benign stuff, but remember that this data requires authentication to access



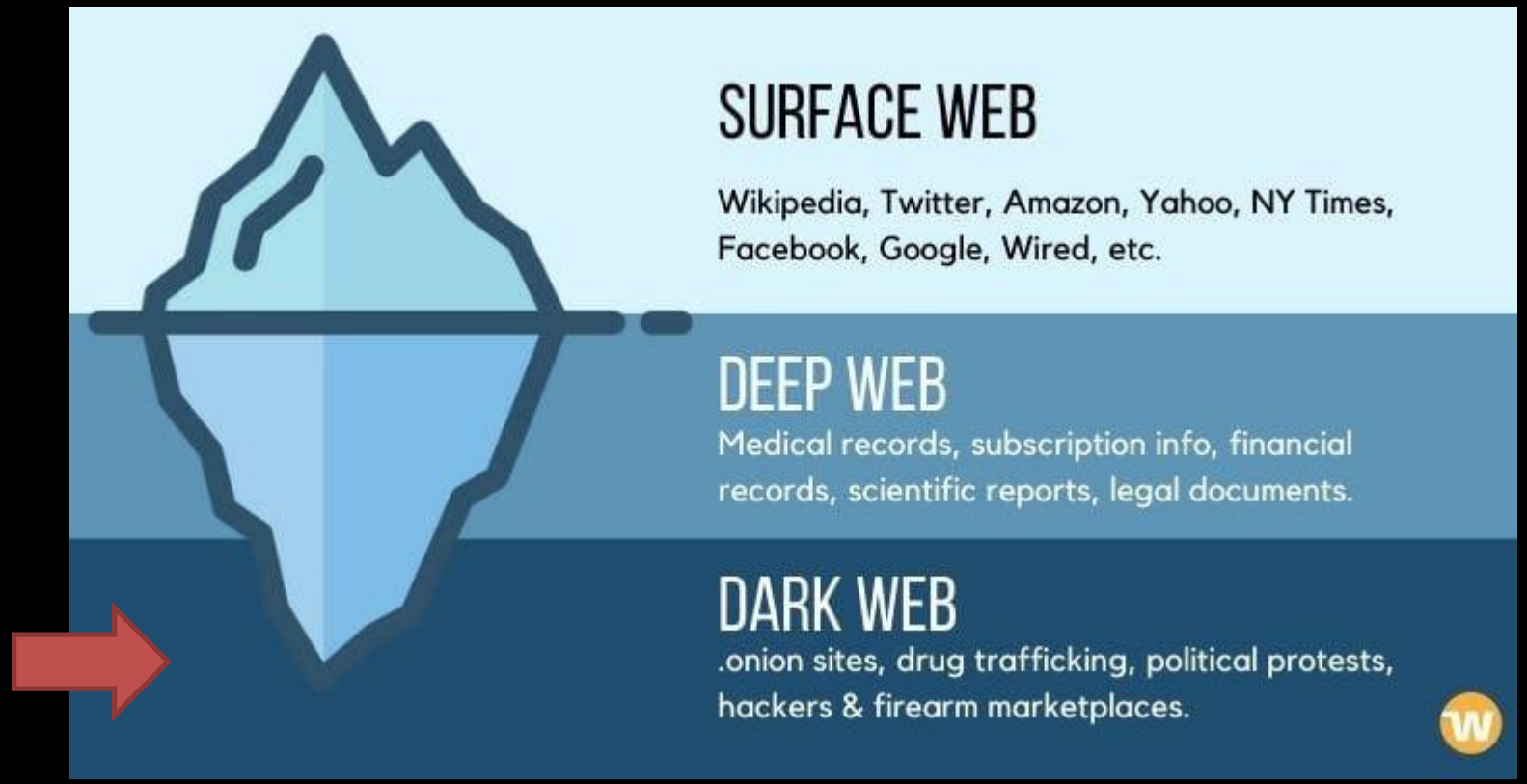
The Depth of the Internet

Onion Links websites that are not accessible by normal web browser
→ .onion instead of .com, .net, etc

The **deep web** is the area of the internet that is not accessible by normal browsers (90%)

The **dark web** is the area of the internet the is hidden and requires a Tor browser

- Hosts web services for both legal/illegal activities



The Dark Net

The “Good”

- **Anonymous political discussion**
- **Selling of legal goods**
- **Whistleblowers**

*subjective (this also does not reflect my personal opinion)

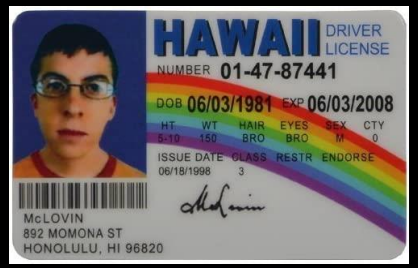
The Dark Net

The "Good"

- **Anonymous political discussion**
- **Selling of legal goods**
- **Whistleblowers**

The Really Bad

- **Selling of *(illegal)* firearms**
- **Selling of Fake Identification**
- **Selling of stolen passwords/credential**
- **Crypto shenanigans + Malware**



*subjective (this also does not reflect my personal opinion)

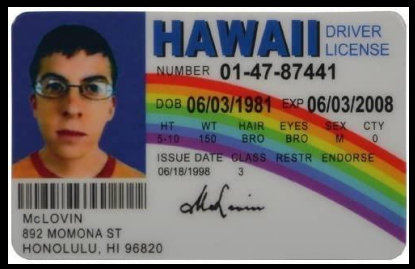
The Dark Net

The "Good"

- Anonymous political discussion
- Selling of legal goods
- Whistleblowers

The Really Bad

- Selling of *(illegal)* firearms
- Selling of Fake Identification
- Selling of stolen passwords/credential
- Crypto shenanigans + Malware



Purchased with bitcoins

The Really Ugly *(unfortunately the most common uses)*

- Selling of drugs
- Human Trafficking + Illegal Pornography
- Hitman Services

*subjective (this also does not reflect my personal opinion)

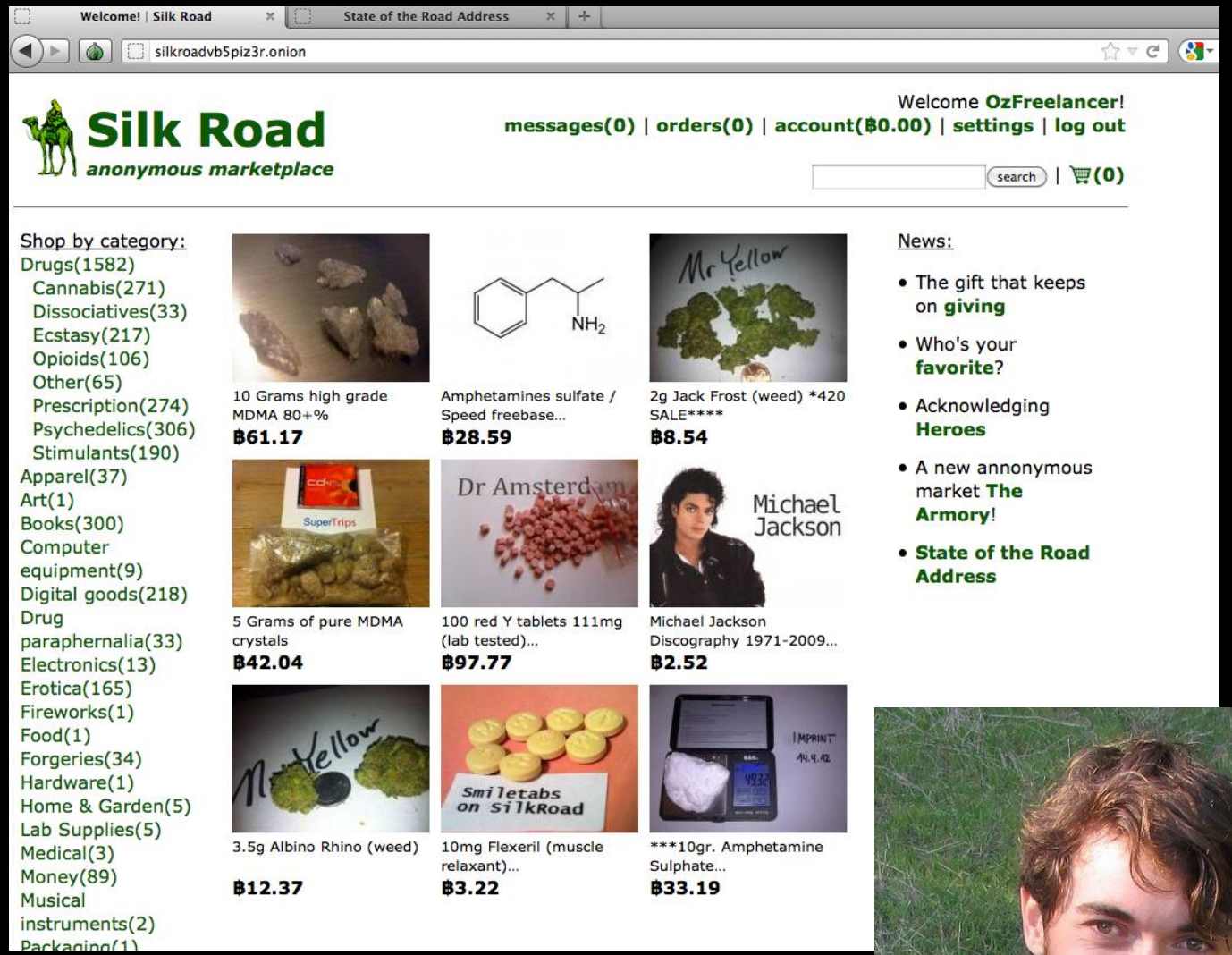
The Silk Road

Famous dark net marketplace for selling drugs, fake identities, and some legal goods

Accumulated $15 million in sales

Started by Ross Ubricht in 2011
→ Advocate for free market, Libertarian politics
→ Wanted a place “where you could buy anything anonymously with no trail whatsoever”

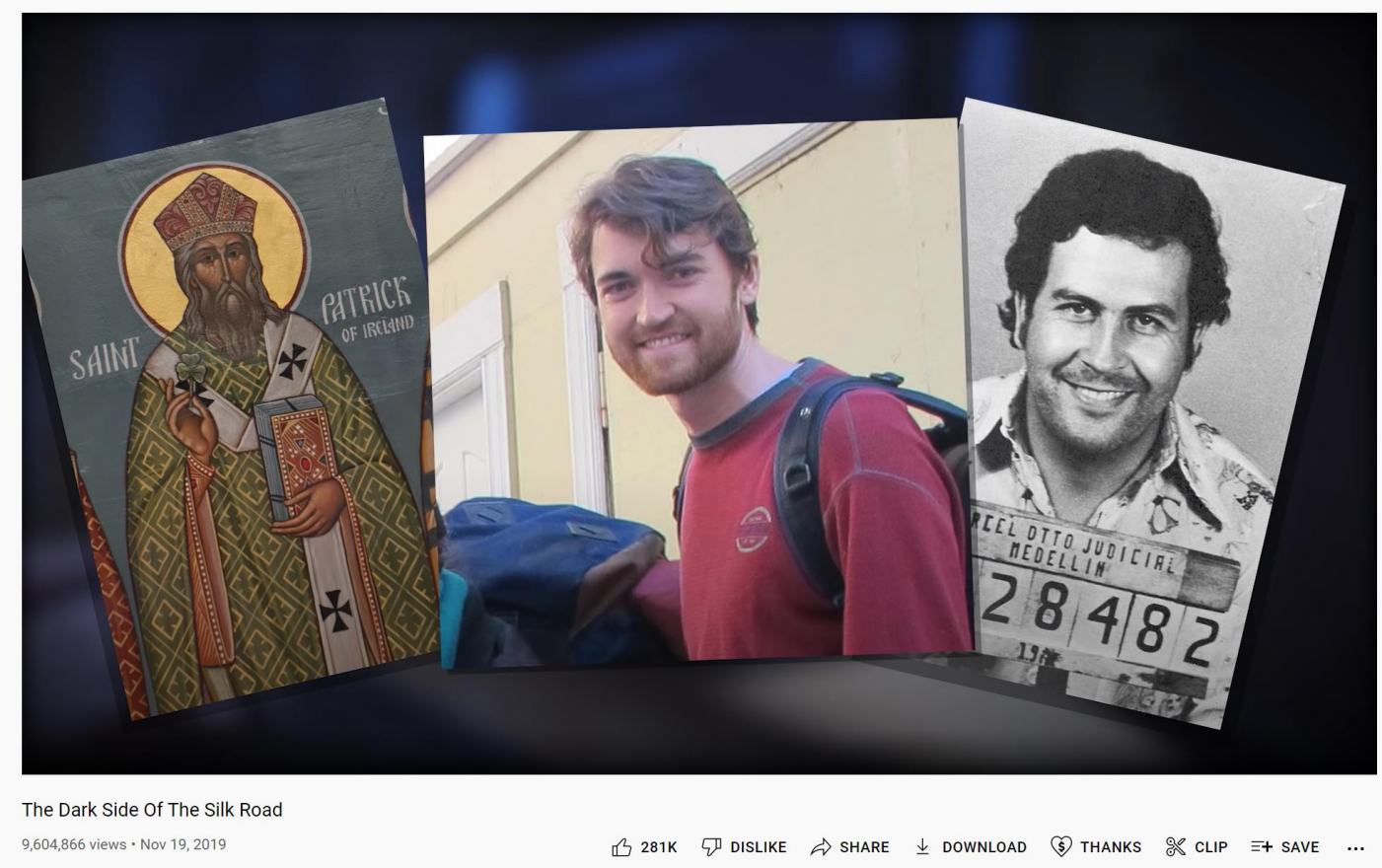
Arrested in 2013 after DEA+FBI tracked him to a San Francisco library
→ How? He posted on stack overflow with his real name (lmao)



Ross Urbricht
Aka “Dread Pirate Roberts”

Serving double life sentence in jail (rip bozo) … also allegedly hired several hitman

More…



https://www.youtube.com/watch?v=GpMP6Nh3FvU&ab_channel=BarelySociable

Legality and Policing the Darknet

Is it illegal to browse the dark net?

Legality and Policing the Darknet

Is it illegal to browse the dark net?

Legality and Policing the Darknet

Is it illegal to browse the dark net?

Downloading TOR is not illegal, and accessing the dark web is not illegal

BUT, when you start engaging in illegal activities, then you have broken the law

Legality and Policing the Darknet

Is it illegal to browse the dark net?

Downloading TOR is not illegal, and accessing the dark web is not illegal

BUT, when you start engaging in illegal activities, then you have broken the law

Because the dark web is being used more as a criminal platform, law enforcement presence has also increased

How to find and arrest criminals?

- Going undercover
- Seizure of illegal websites + data
- (Legal*) malware installation

Conclusion

There are parts on the internet we cannot normally access

Unfortunately, these parts host some very evil content

You should be aware that these places exist, but I recommend not visiting them

Anonymity and privacy on the internet can be a sensitive subject, but there are tools (**TOR**) that can be used to boost your privacy

We will talk more about security and privacy on the internet in the coming weeks