
SECURITY (COMP0141): TOR



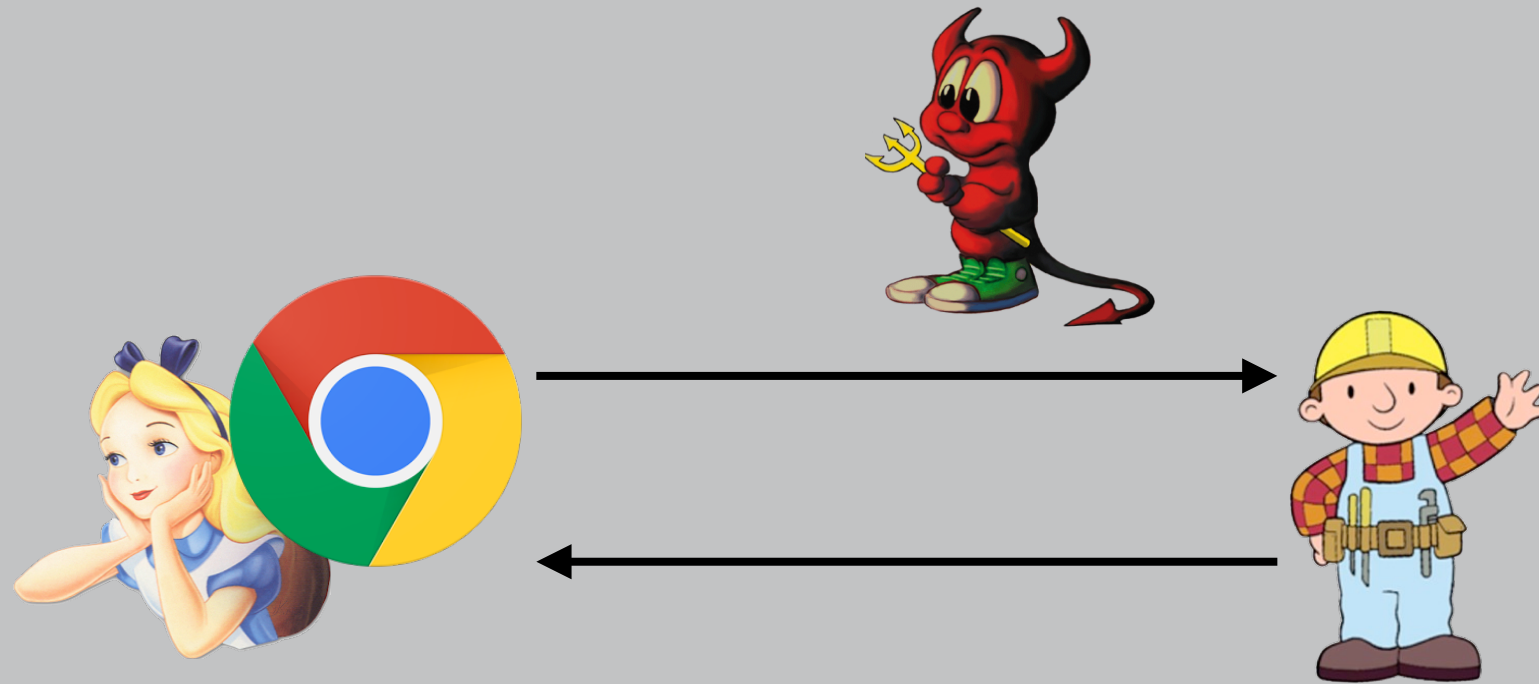
CONFIDENTIALITY, REVISITED

- **Tor**
- browser fingerprinting
- forward secrecy
- revocation

integrity

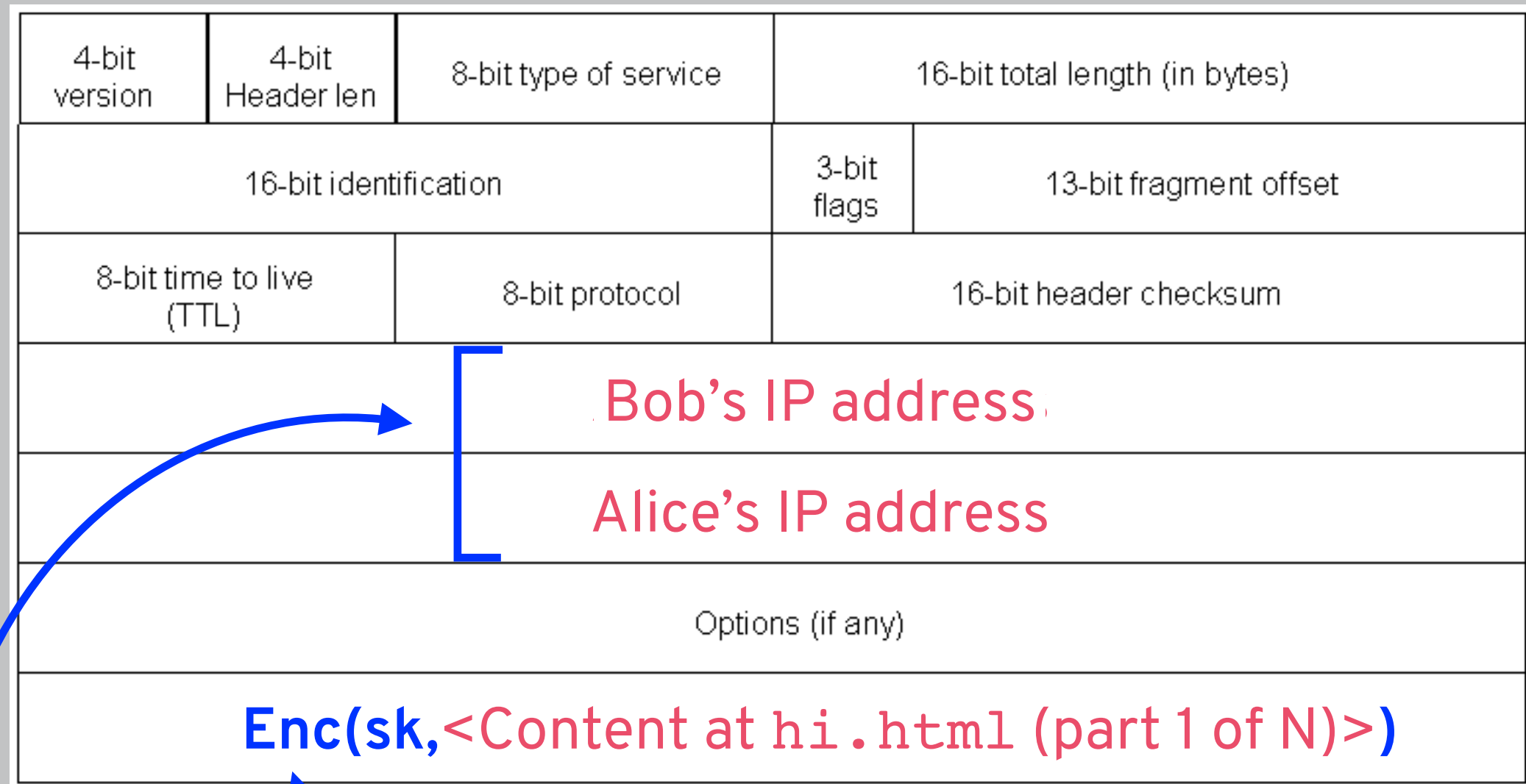
availability

THREAT MODEL




Is there an eavesdropper spying on your web traffic?

ENCRYPTED WEB TRAFFIC



The diagram shows an IP header structure with the following fields:

4-bit version	4-bit Header len	8-bit type of service	16-bit total length (in bytes)	
16-bit identification			3-bit flags	13-bit fragment offset
8-bit time to live (TTL)		8-bit protocol	16-bit header checksum	
				
Options (if any)				
Enc(sk, <Content at hi.html (part 1 of N)>)				

HTTPS can hide content...

...but this still reveals a lot of information!

TOR



h
e

o
u
t
e
r

the onion
(multiple layers
of encryption)

so exit node sees
message, but where
did it come from?

keys for PKE

peeling off
a layer



$m = \text{"Hi!"}$

$\text{Enc}(\text{key}, m)$

$\text{Enc}(\text{key}, m)$

m

$\text{Dec}(\text{key}, \text{Enc}(\text{key}, m))$

$\text{Dec}(\text{key}, \text{Enc}(\text{key}, m))$



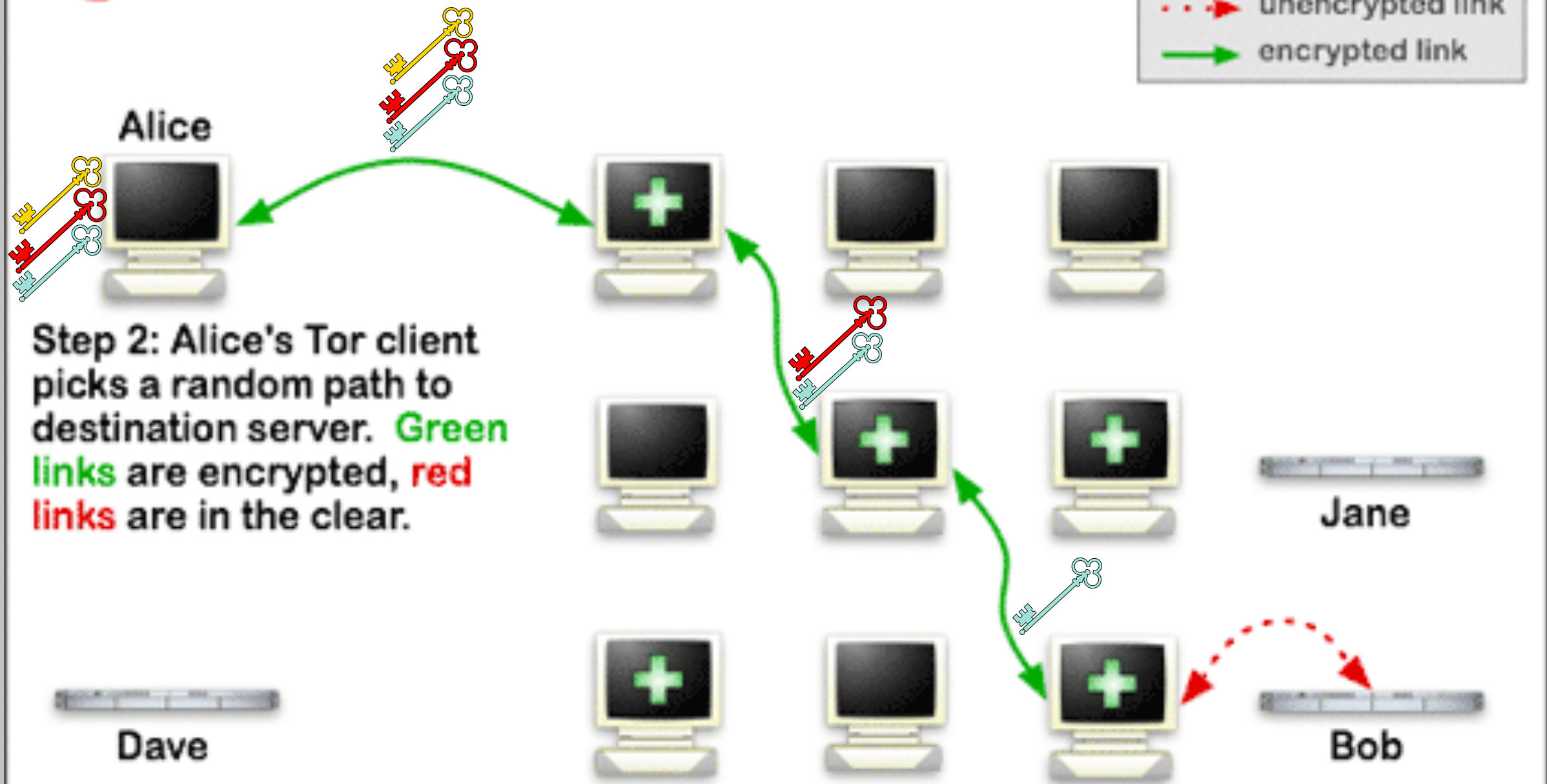
HOW TOR WORKS

How Tor Works: 1



HOW TOR WORKS

How Tor Works: 2



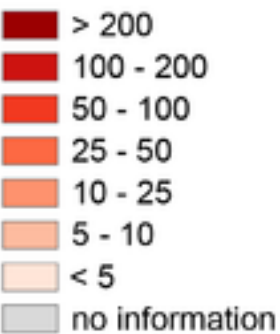
QUESTIONS ABOUT TOR

q: what if I want to ban Tor users from my site?

a: block exit nodes. (Wikipedia, etc. do this.)

The anonymous Internet

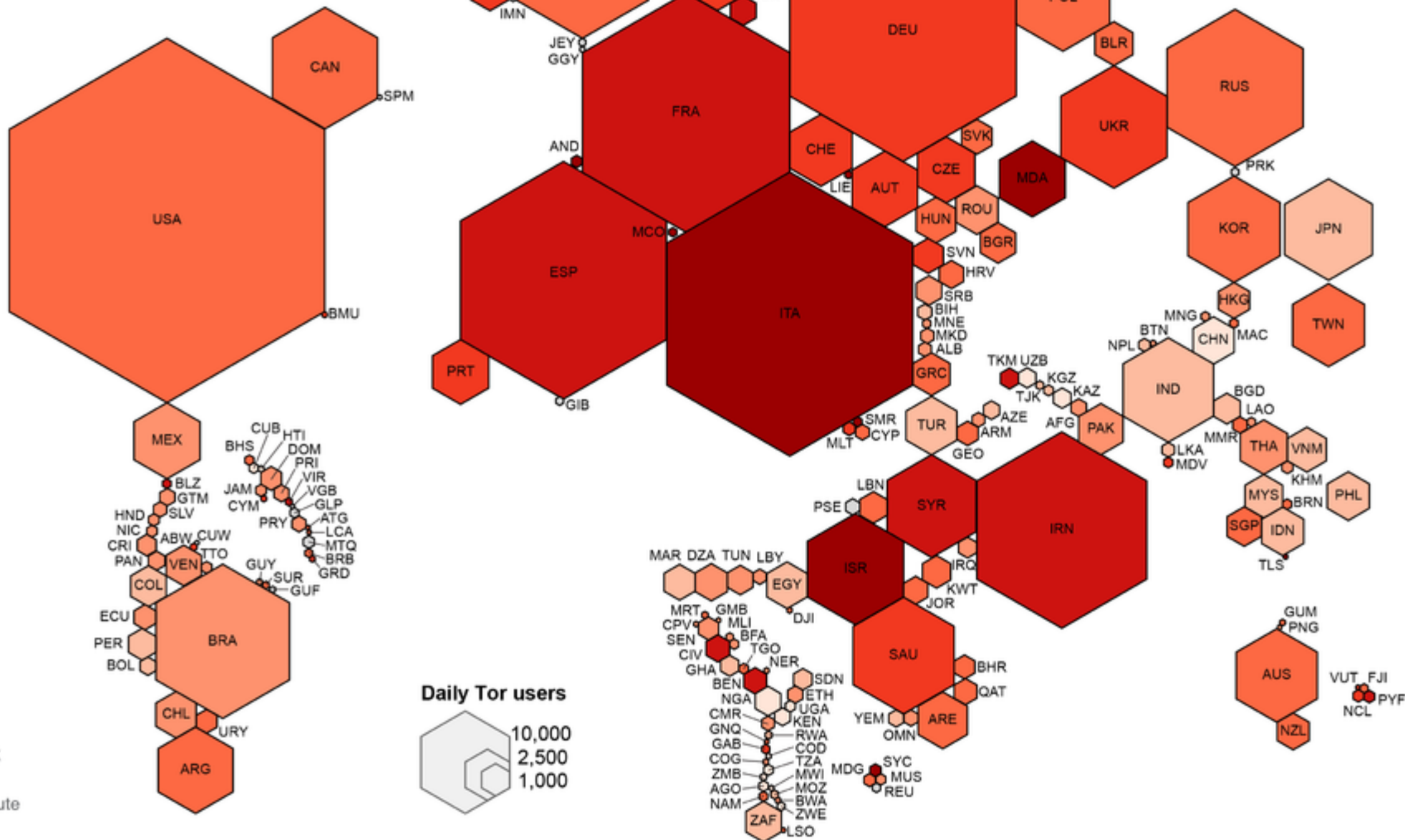
**Daily Tor users
per 100,000
Internet users**



Average number of Tor users per day calculated between August 2012 and July 2013

data sources:
Tor Metrics Portal
metrics.torproject.org
World Bank
data.worldbank.org

by Mark Graham
(@geoplace) and
Stefano De Sabbata
(@maps4thought)
Internet Geographies at
the Oxford Internet Institute
2014 • geography.oii.ox.ac.uk



QUESTIONS ABOUT TOR

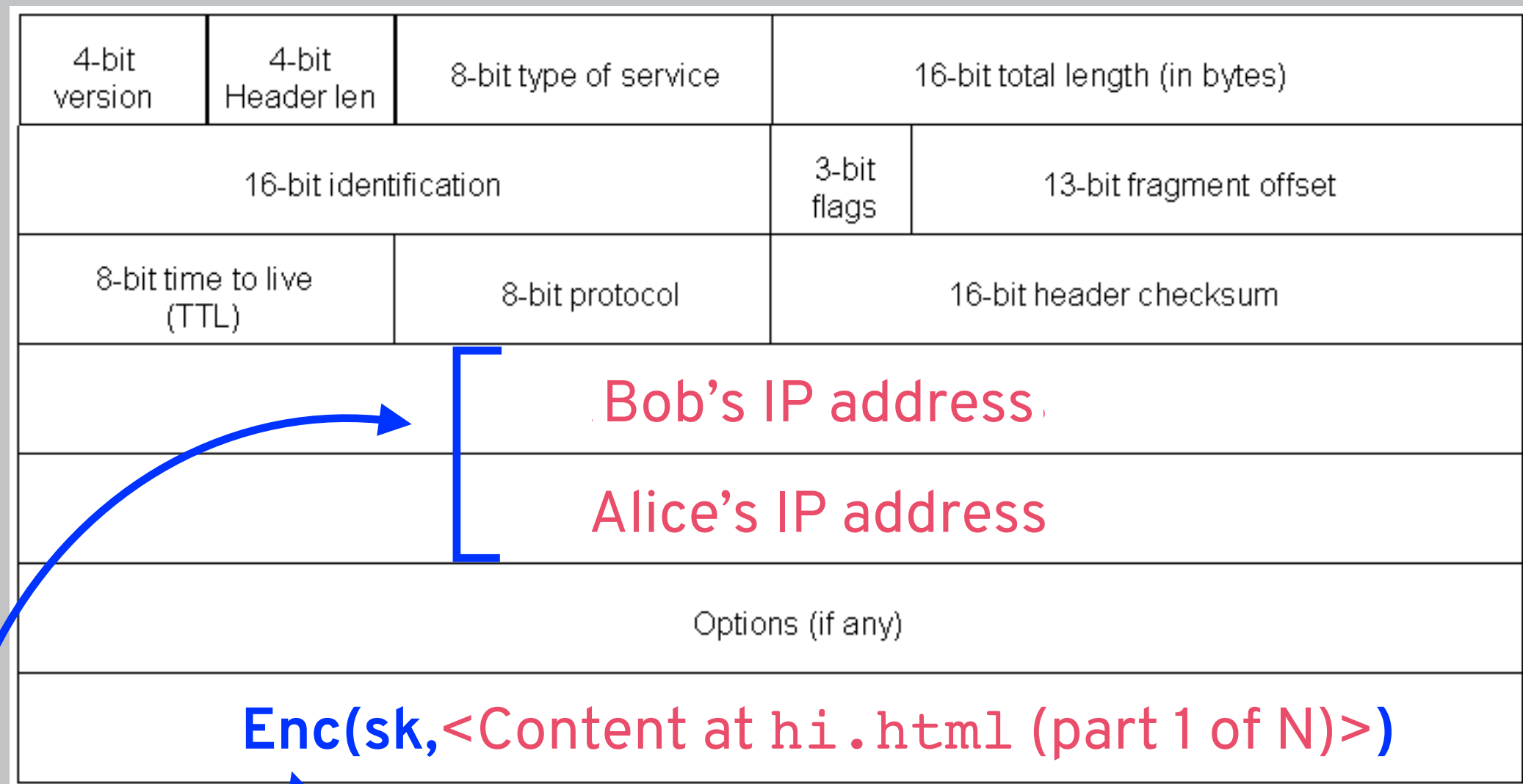
q: what if I want to ban Tor users from my site?

a: block exit nodes. (Wikipedia, etc. do this.)

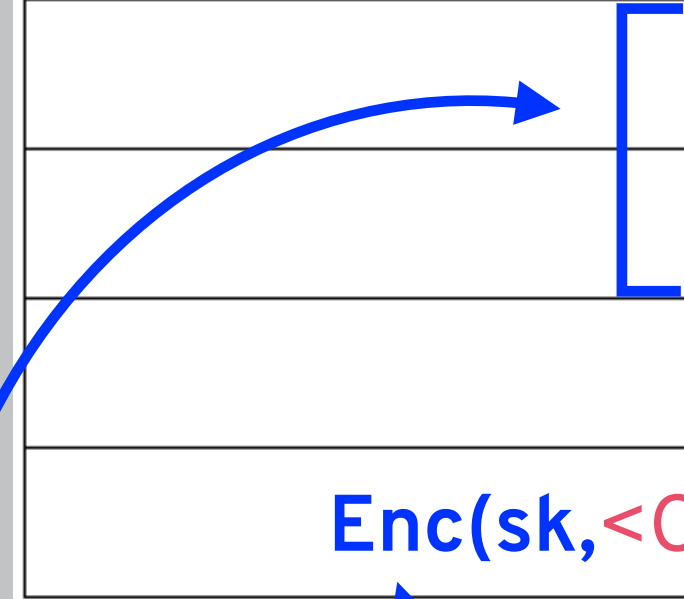
q: does Tor also hide the content of my web traffic?

a: no! just routing; for content need to use HTTPS.

ENCRYPTED WEB TRAFFIC



The diagram shows an IP packet structure with the following fields:

4-bit version	4-bit Header len	8-bit type of service	16-bit total length (in bytes)	
16-bit identification			3-bit flags	13-bit fragment offset
8-bit time to live (TTL)		8-bit protocol	16-bit header checksum	
			Bob's IP address	
			Alice's IP address	
Options (if any)				
Enc(sk, <Content at hi.html (part 1 of N)>)				

HTTPS can hide content...

...and Tor can hide this.

QUESTIONS ABOUT TOR

q: what if I want to ban Tor users from my site?

a: block exit nodes. (Wikipedia, etc. do this.)

q: does Tor also hide the content of my web traffic?

a: no! just routing; for content need to use HTTPS.

q: does Tor just let me visit normal websites anonymously?

a: no. **Hidden services** exist only within Tor network.

TOR HIDDEN SERVICES

How Tor Works: 2

activist 😐

Alice



Step 2: Alice's Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.



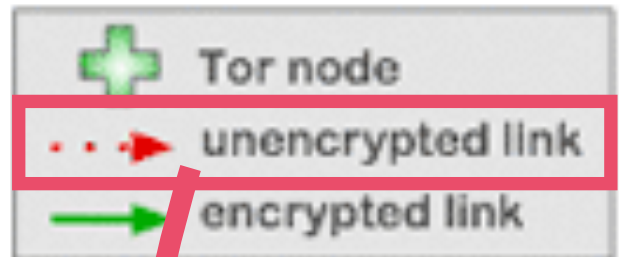
Dave



Jane



Bob

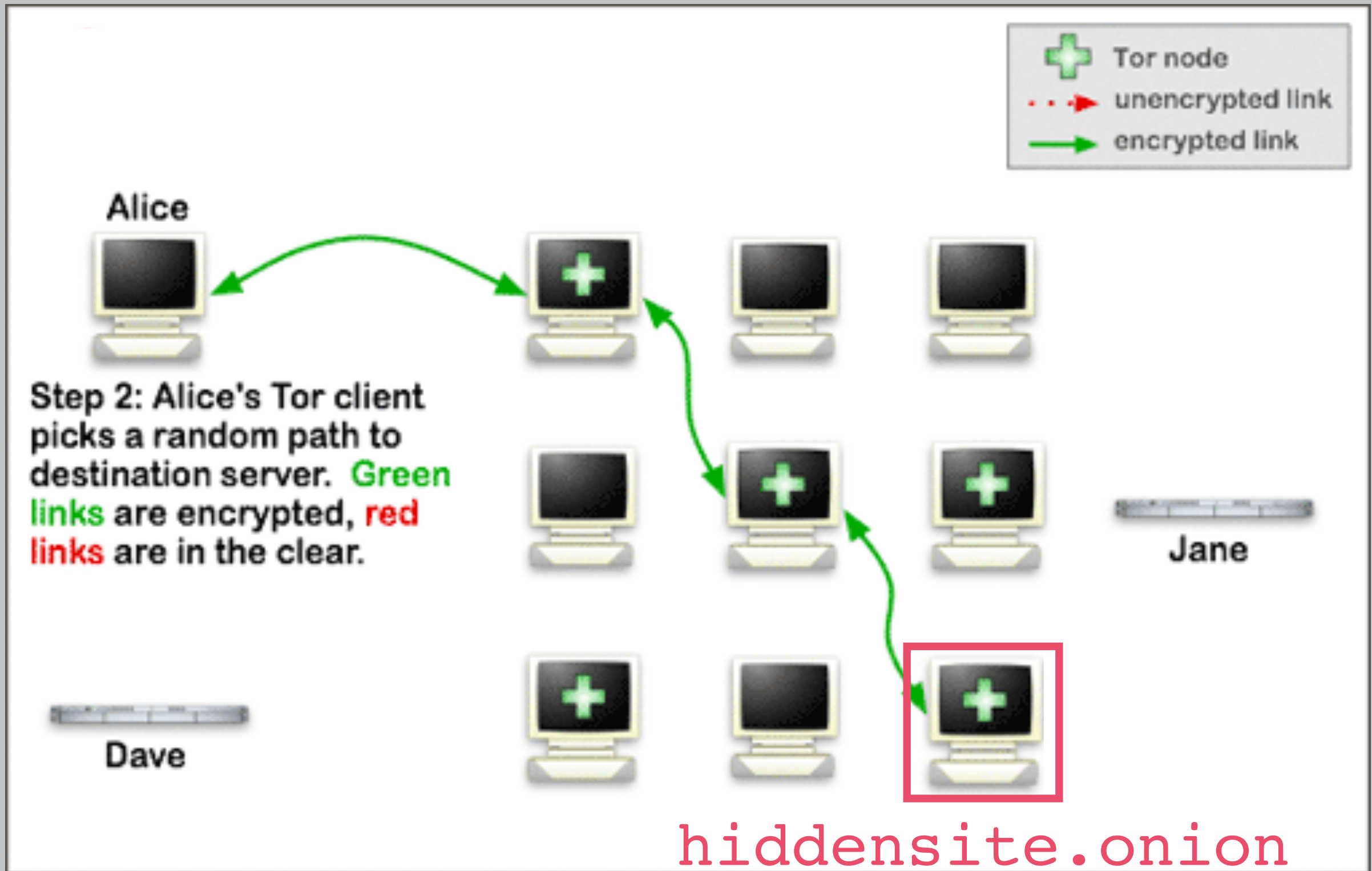


still needs to host site somewhere!

~~news outlet~~

activist news outlet

TOR HIDDEN SERVICES



CONFIDENTIALITY, REVISITED

- Tor
- **browser fingerprinting**
- forward secrecy
- revocation

integrity

availability