

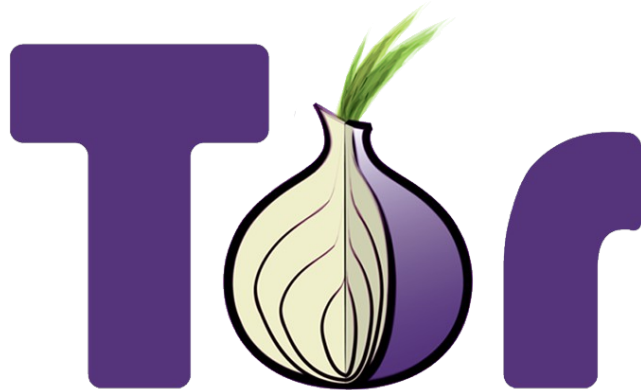
20 Years of Onion Routing For a Better Internet

Nathan Freitas

nathan@freitas.net @n8fr8

<https://torproject.org>

<https://guardianproject.info>



20 Years of Onion Routing

"Internet Communication Resistant to Traffic Analysis," 1997 Navy Research Lab Review, Washington, DC, April 1997, pp. 109-111.

Determining who is talking to whom (called traffic analysis) is an important source of intelligence information. As military grade communication devices increasingly depend on the public communications infrastructure, it is important to use that infrastructure in ways that are resistant to traffic analysis. It may also be useful to communicate anonymously, for example when gathering intelligence from public databases.

We describe bidirectional and real-time Anonymous Connections that are strongly resistant to eavesdropping and traffic analysis attacks by both insiders and outsiders. If necessary, communication is made anonymous by removing identifying information from the data stream. These anonymous connections have been prototyped in a system that protects the privacy of communication over the Internet and, in particular, the World Wide Web.

Anonymous connections can protect both identity and location in many switched communication systems, such as wired, cellular, or satellite phone networks.

<http://www.onion-router.net/Publications.html#new-slides>

Intelligence Information

Traffic Analysis

Identity

Location

ANONYMITY

but also...

CONFIDENTIALITY

AUTHENTICATION

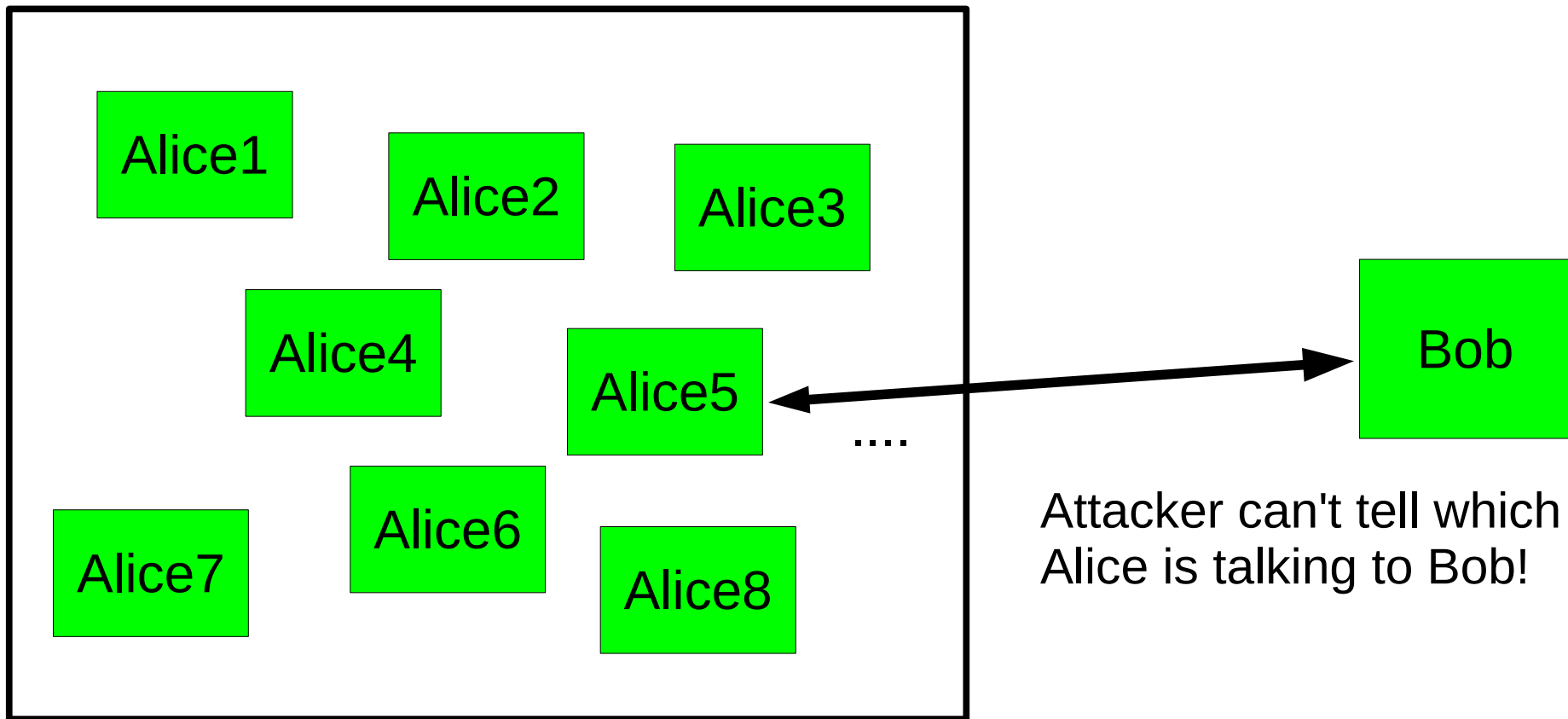
You can't tell who did what

“Who wrote this blog post?”

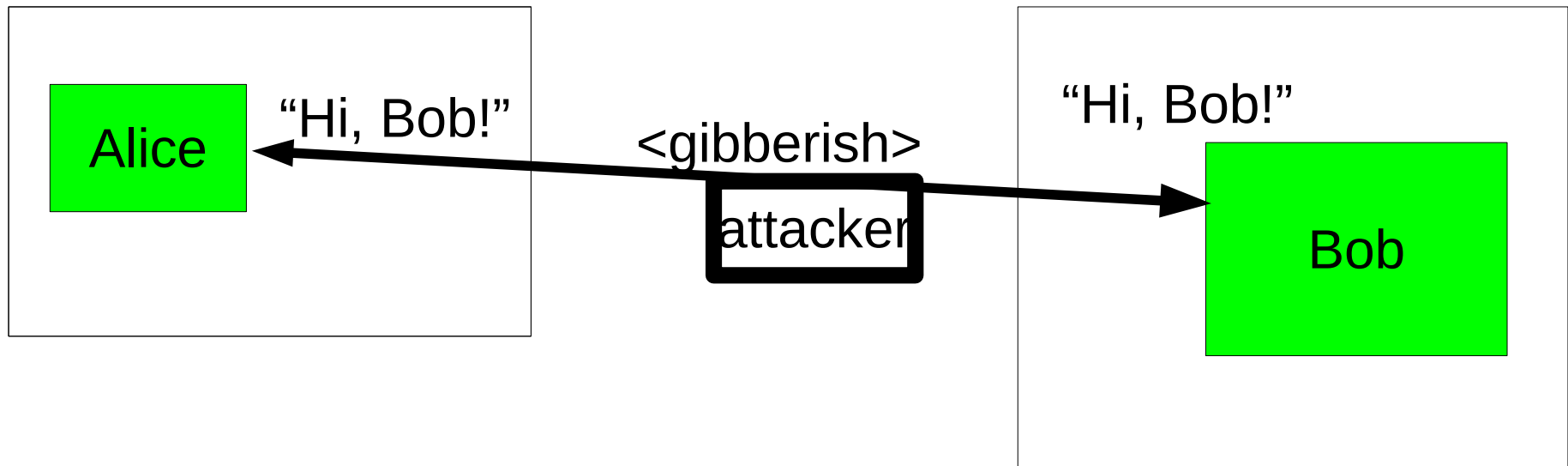
“Who's been viewing my site?”

“Who's been chatting with who?”

Indistinguishable within a set

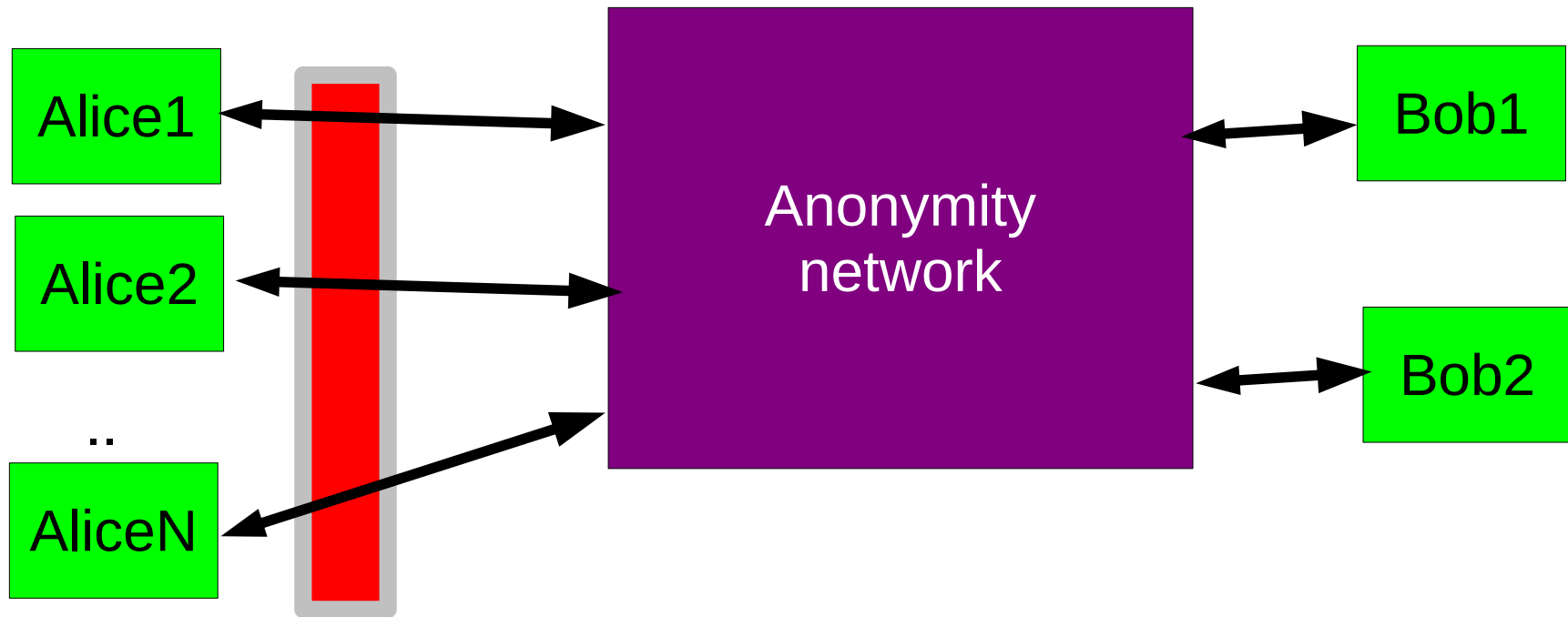


**Encryption just protects content.
Anonymity protects metadata.**



Anonymity isn't steganography:

**Attacker can tell that Alice is talking;
just not to whom.**



Anonymity is not wishful thinking...

“You can't prove it was me!”

“Promise you won't look!”

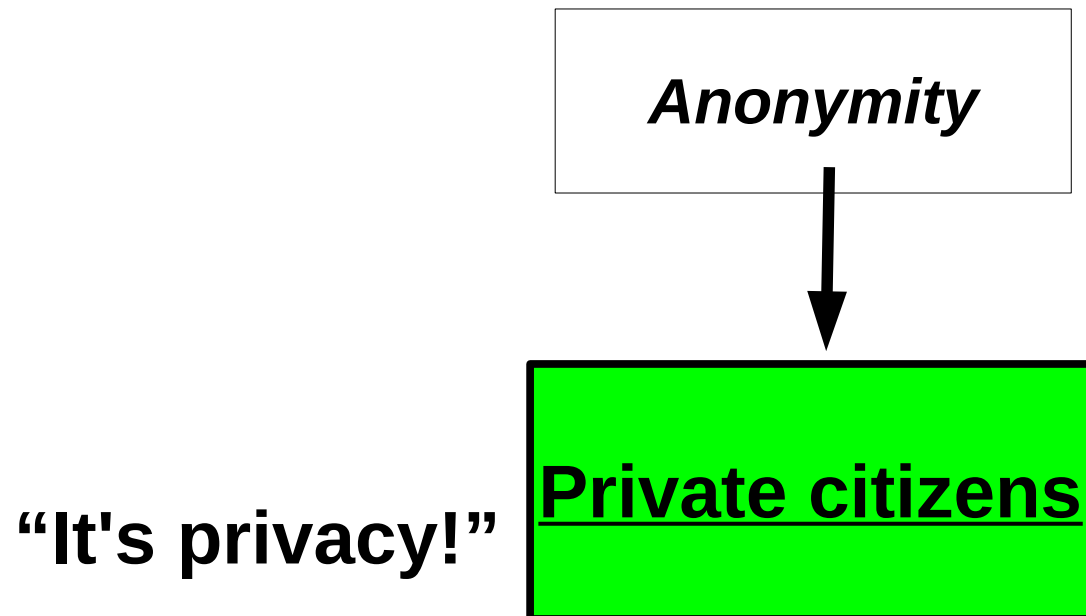
“Promise you won't remember!”

“Promise you won't tell!”

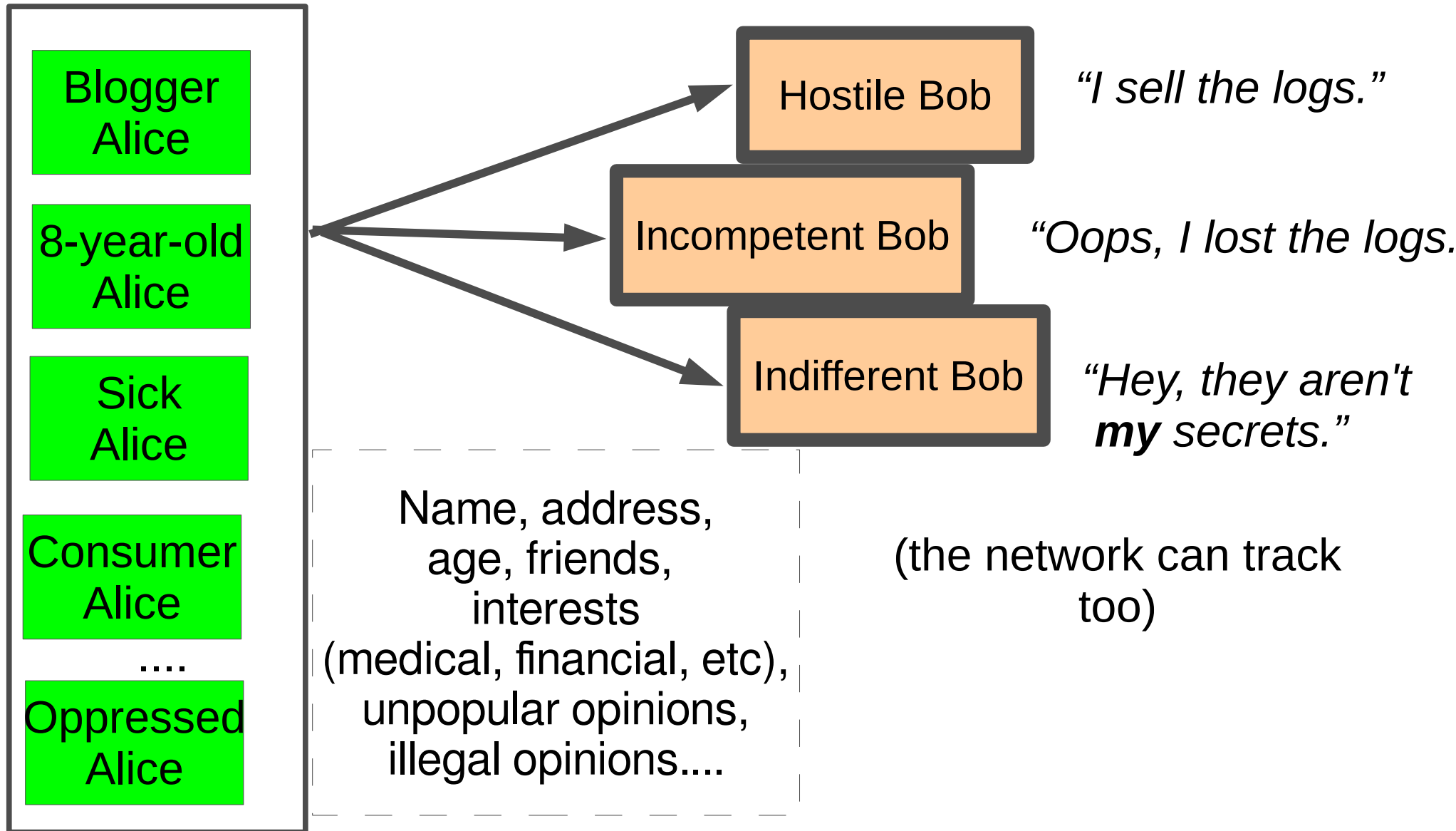
“I didn't write my name on it!”

“Isn't the Internet already anonymous?”

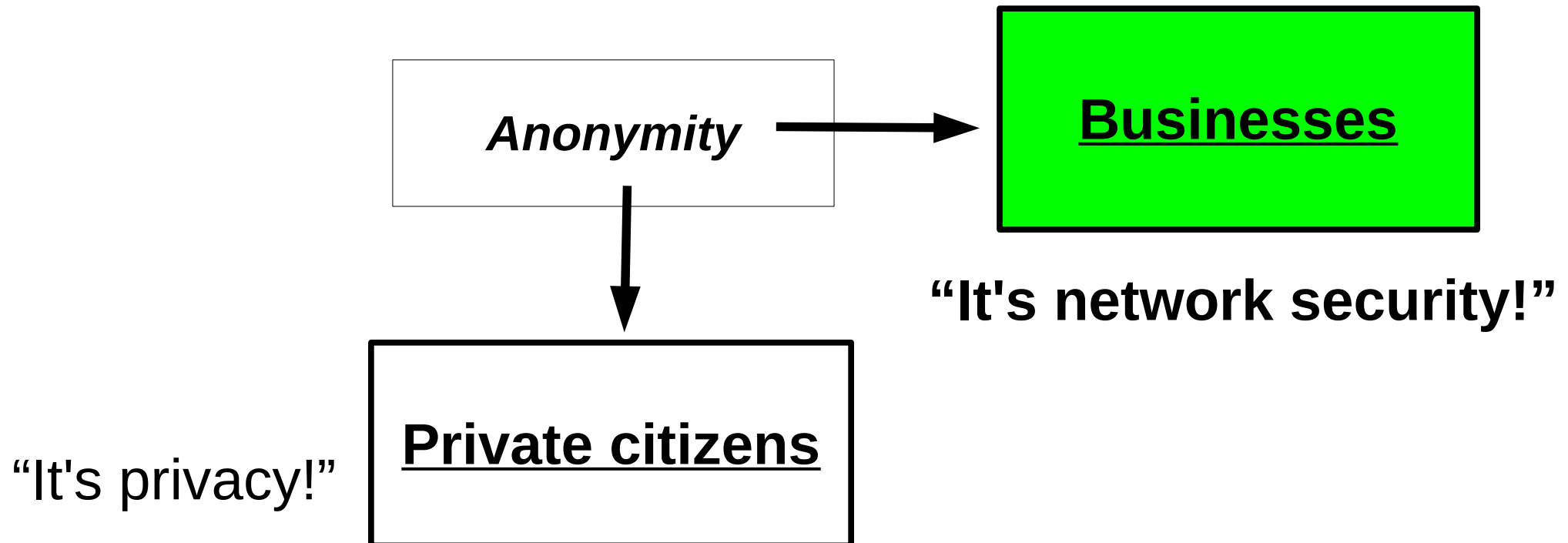
Anonymity serves different interests for different user groups.



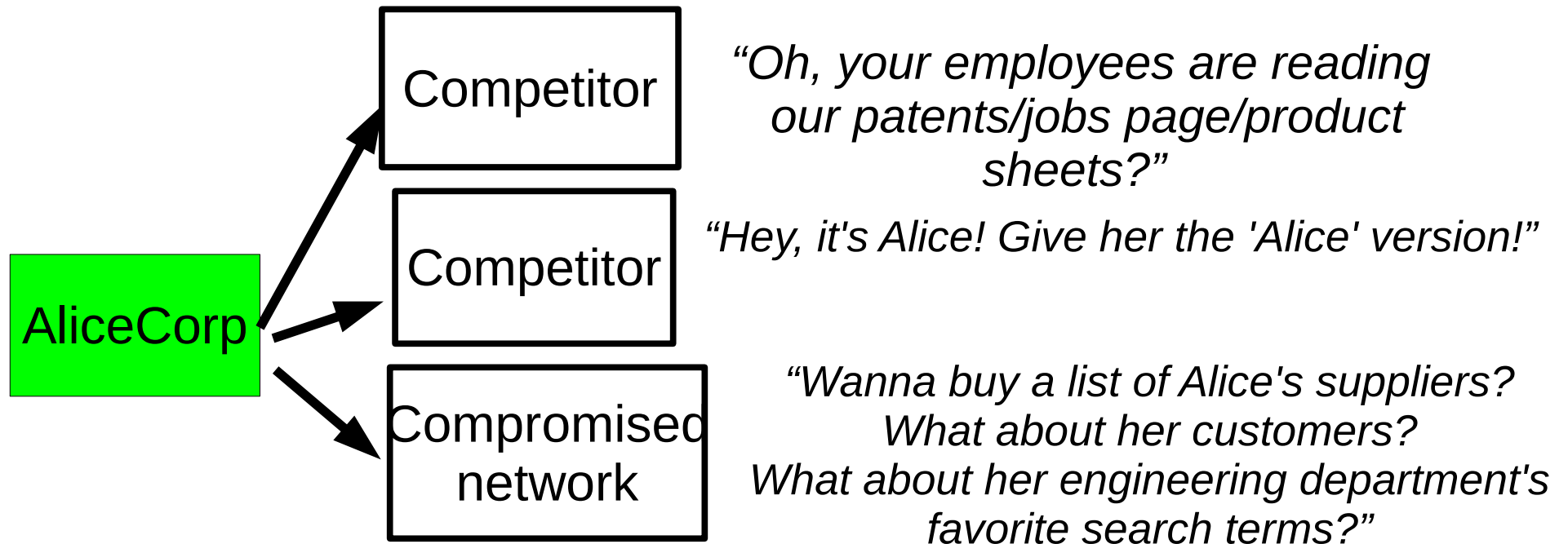
Regular citizens don't want to be watched and tracked.



Anonymity serves different interests for different user groups.

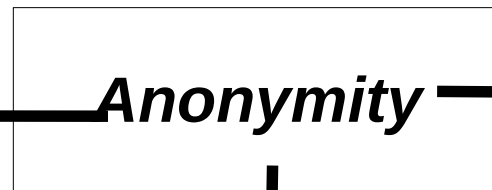
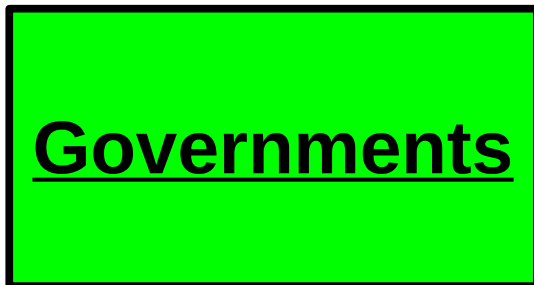


Businesses need to keep trade secrets.



Anonymity serves different interests for different user groups.

“It's traffic-analysis resistance!”

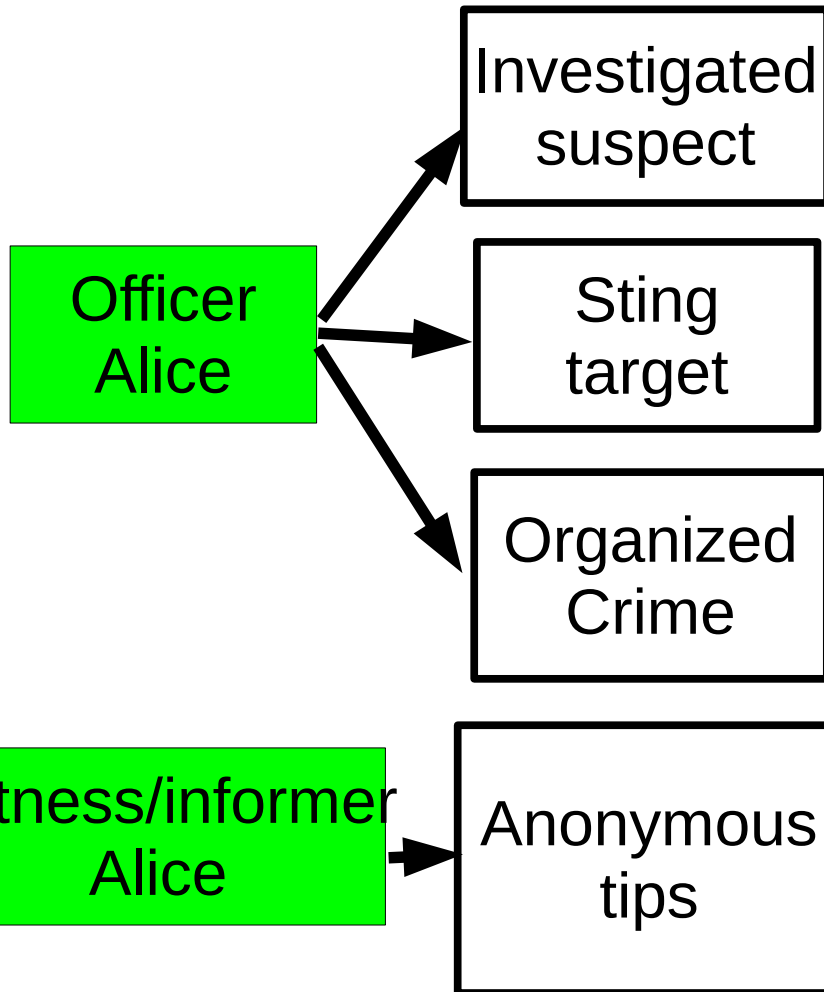


“It's network security!”

“It's privacy!”



Law enforcement needs anonymity to get the job done.



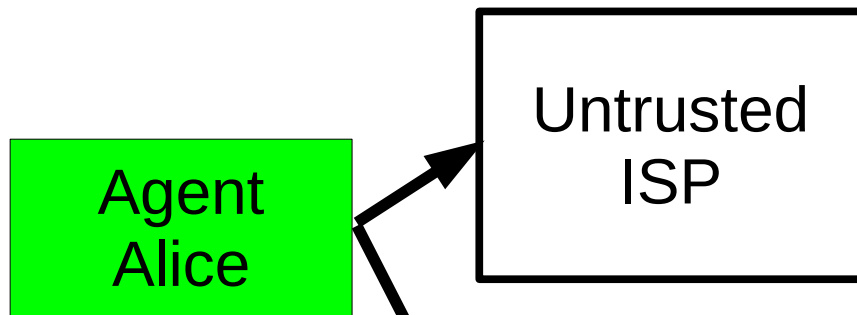
“Why is alice.localpolice.gov reading my website?”

“Why no, alice.localpolice.gov! I would never sell counterfeits on ebay!”

“Is my family safe if I go after these guys?”

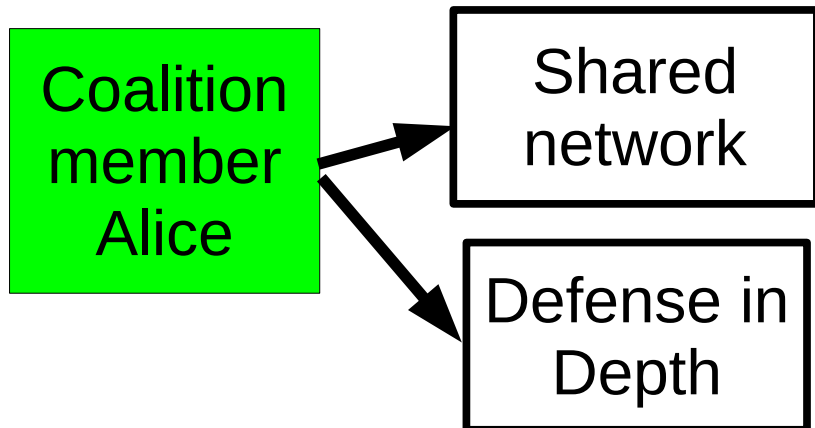
“Are they really going to ensure my anonymity?”

Governments need anonymity for their security



“What will you bid for a list of IP addresses that get email from .mil?”

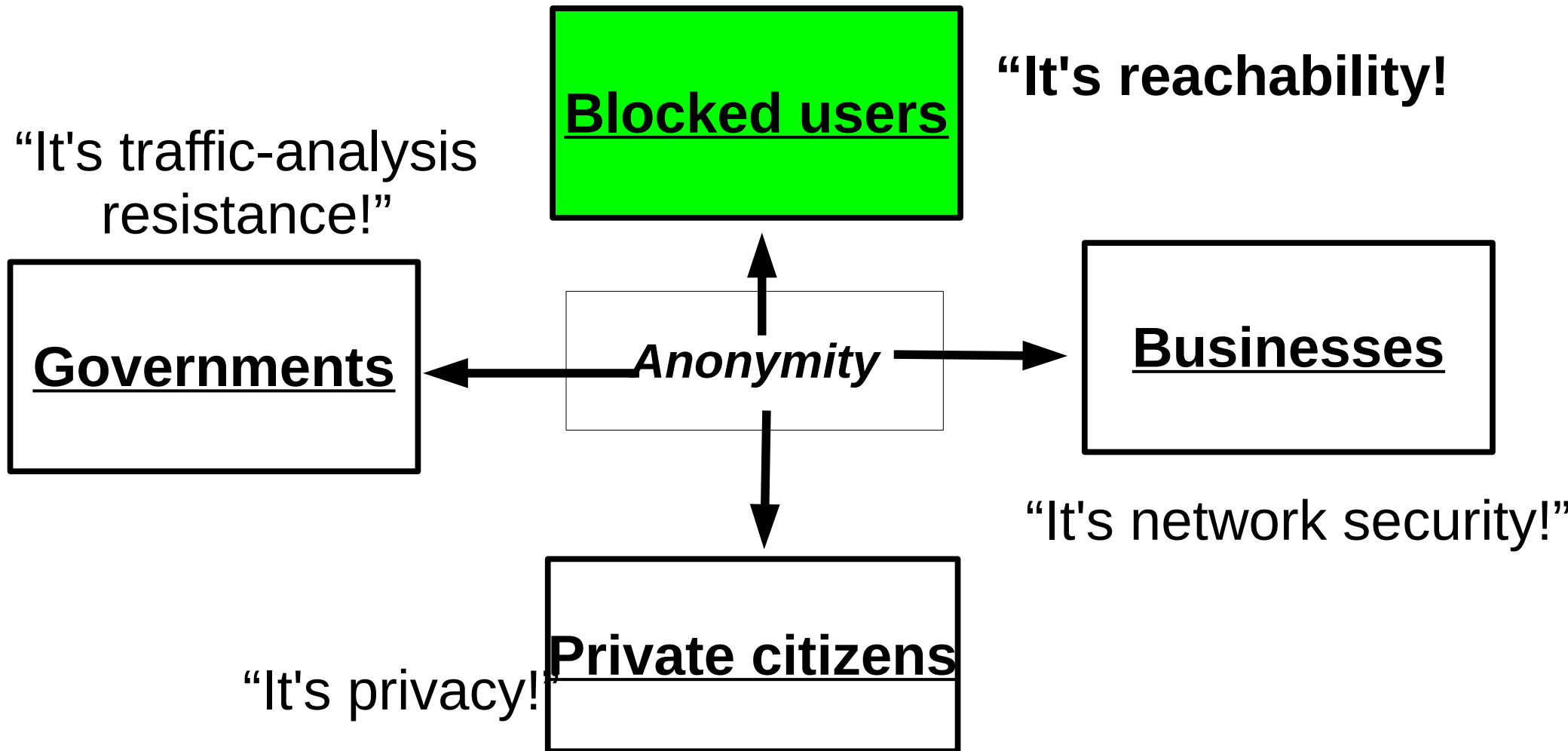
“What does the CIA Google for?”



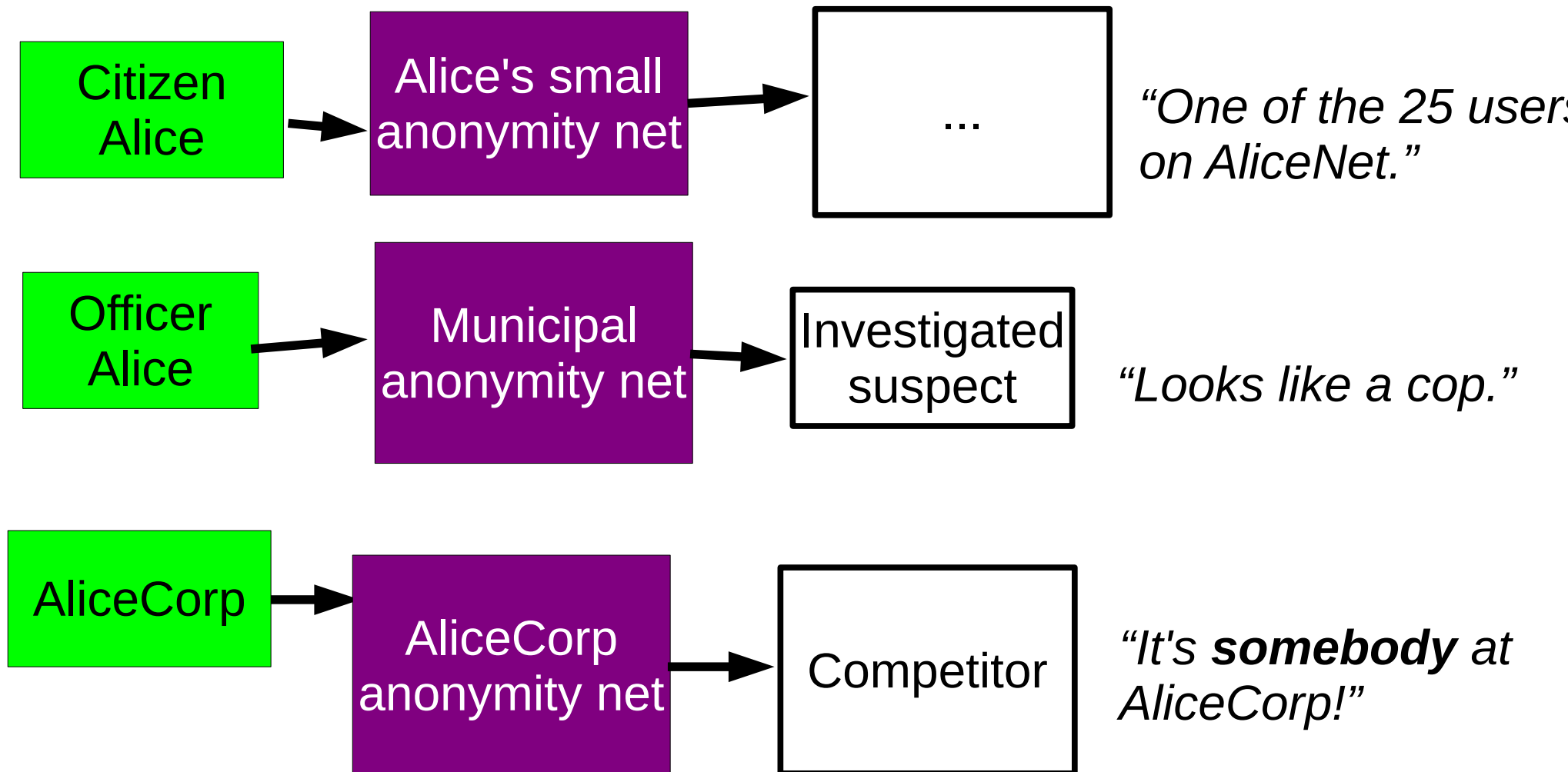
“Do I really want to reveal my internal network topology?”

“What about insiders?”

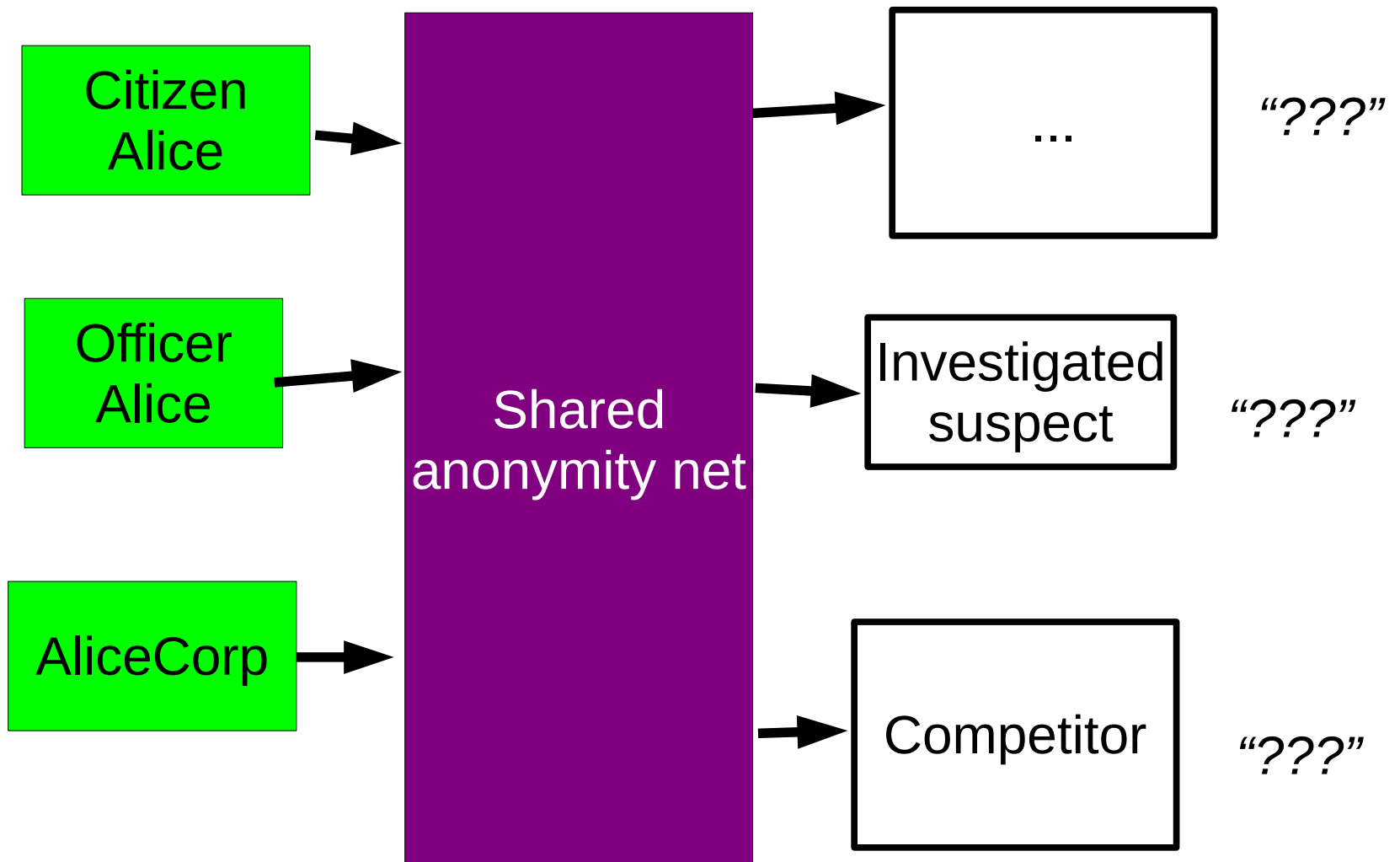
Anonymity serves different interests for different user groups.



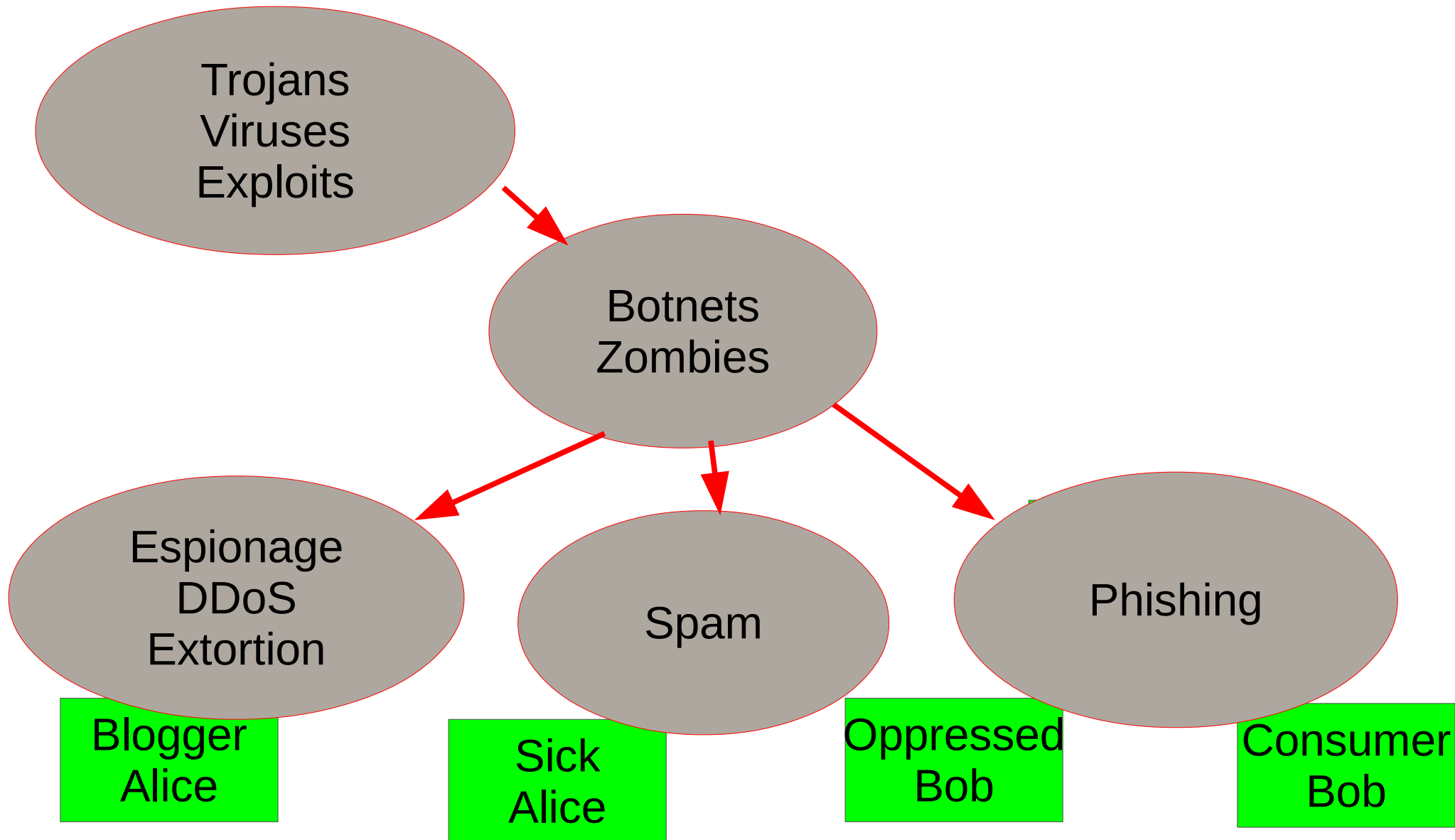
One is the loneliest number...



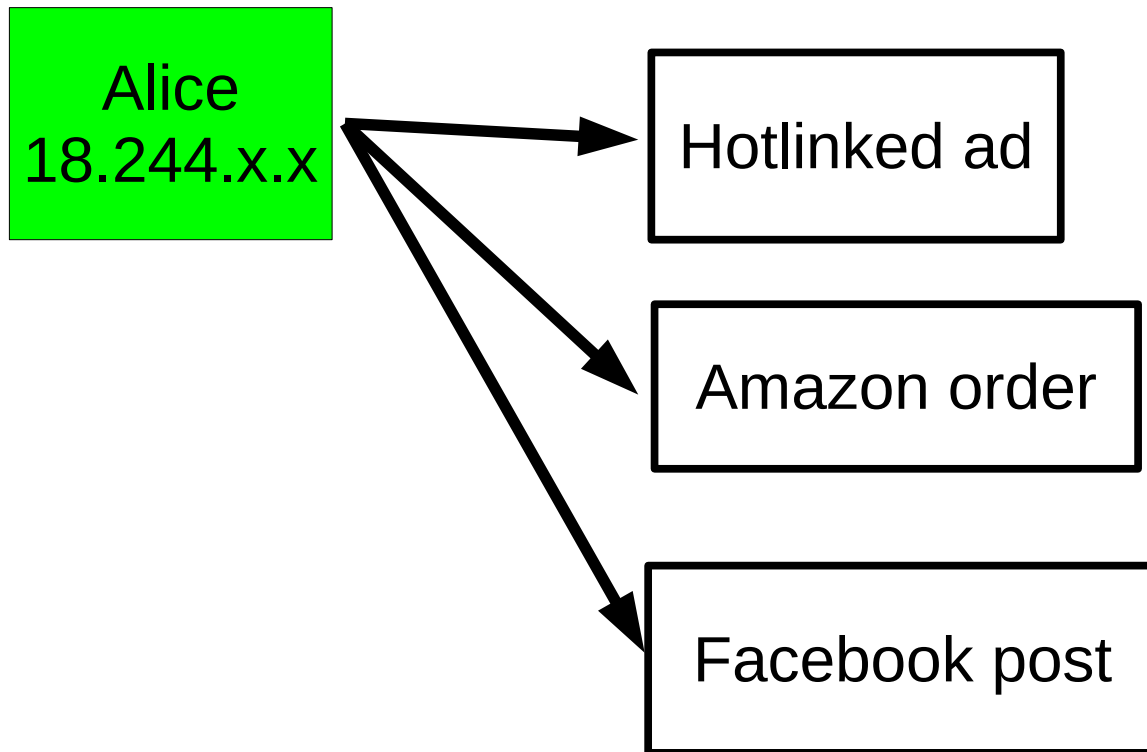
“Anonymity loves company!”



Currently, bad actors on the Internet are doing fine



IP addresses can be enough to bootstrap knowledge of identity.



Tor is not the first or only design for anonymity.

Low-latency

Single-hop
proxies

V1 Onion
Routing (~96)

Java Anon Proxy
(~00-)

Crowds
(~96)

ZKS
“Freedom”
(~99-01)

Tor
(01-)

High-latency

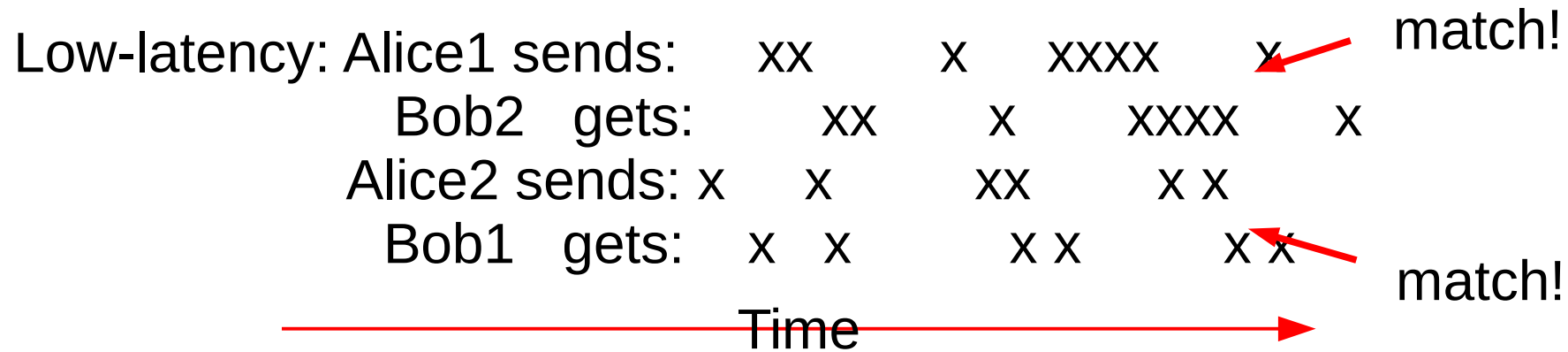
Chaum's Mixes
(1981)

anon.penet.fi (~91)

Remailer networks:
cypherpunk (~93),
mixmaster (~95),
mixminion (~02)

...and more!

Low-latency systems are vulnerable to end-to-end correlation attacks.



High-latency:

Alice1 sends:	xx	x	xxxx	
Alice2 sends:	x	x	xx	x x
Bob1 gets:		xx	xxxx
Bob2 gets:		x	xxxxxx

The diagram illustrates a high-latency end-to-end correlation attack. It shows four rows of data: Alice1 sends, Alice2 sends, Bob1 gets, and Bob2 gets. The data is represented by 'x' characters. Alice1 sends 'xx', 'x', and 'xxxx'. Alice2 sends 'x', 'x', and 'xx'. Bob1 gets 'xx' and 'xxxx'. Bob2 gets 'x' and 'xxxxxx'. The packets are not correlated (no match!) because the latency is high. A red arrow at the bottom points from left to right, labeled 'Time'.

These attacks work in practice. The obvious defenses are expensive (like high-latency), useless, or both.

Still, we focus on low-latency,
because it's more useful.

Billions of people use the web, messaging, media streaming and other applications everyday.

The Tor Project, Inc.

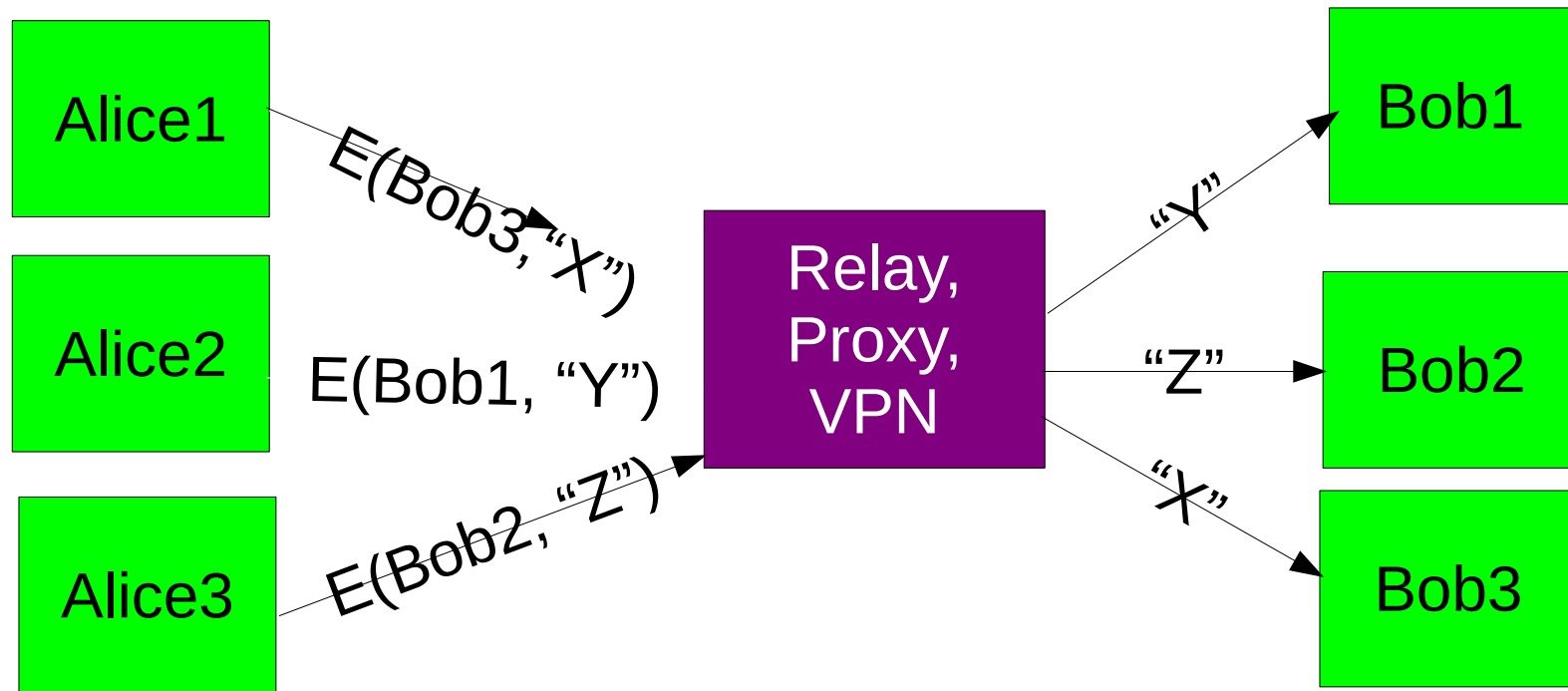


- 501(c)(3) non-profit organization dedicated to the research and development of tools for online anonymity and privacy
- online anonymity software and network
- open source project
- active research environment

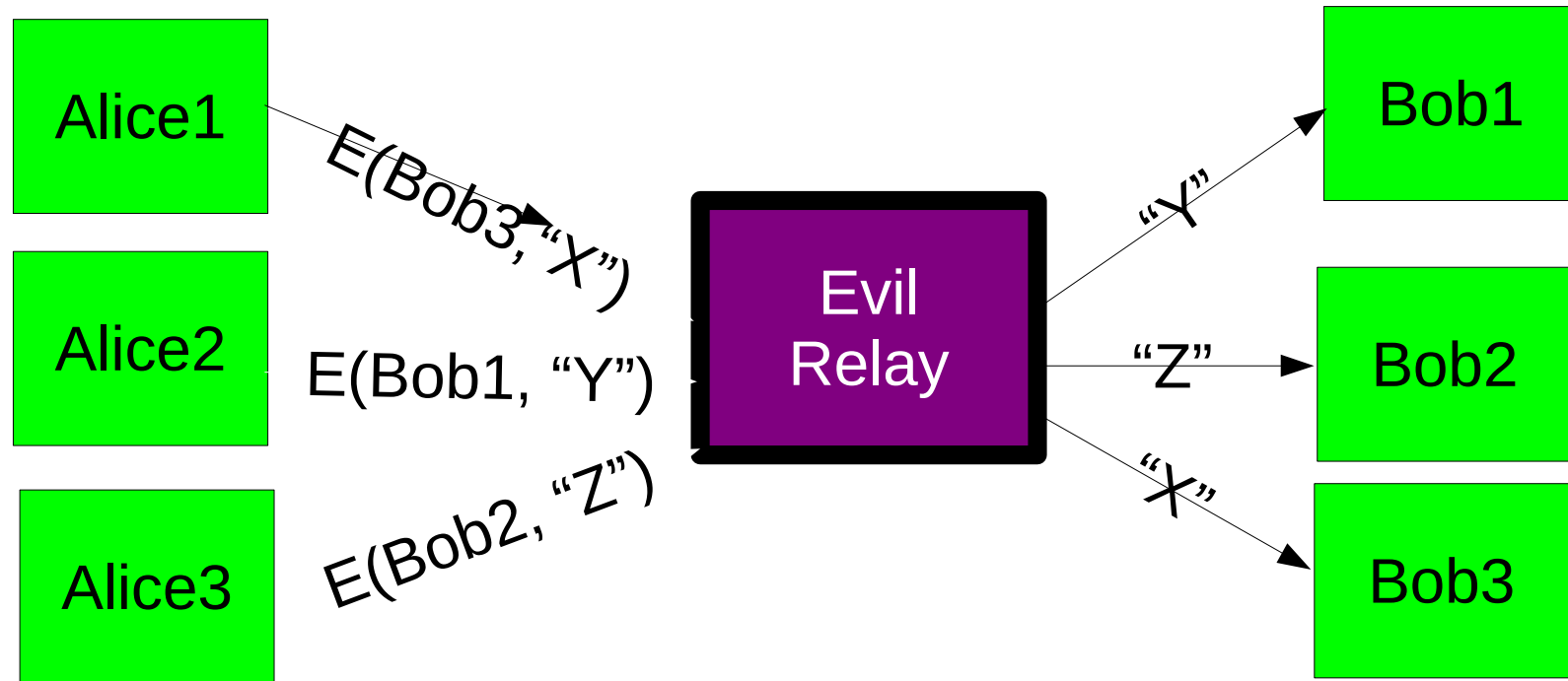
Estimated ~1,000,000
daily Tor users



The simplest designs use a single relay to hide connections.

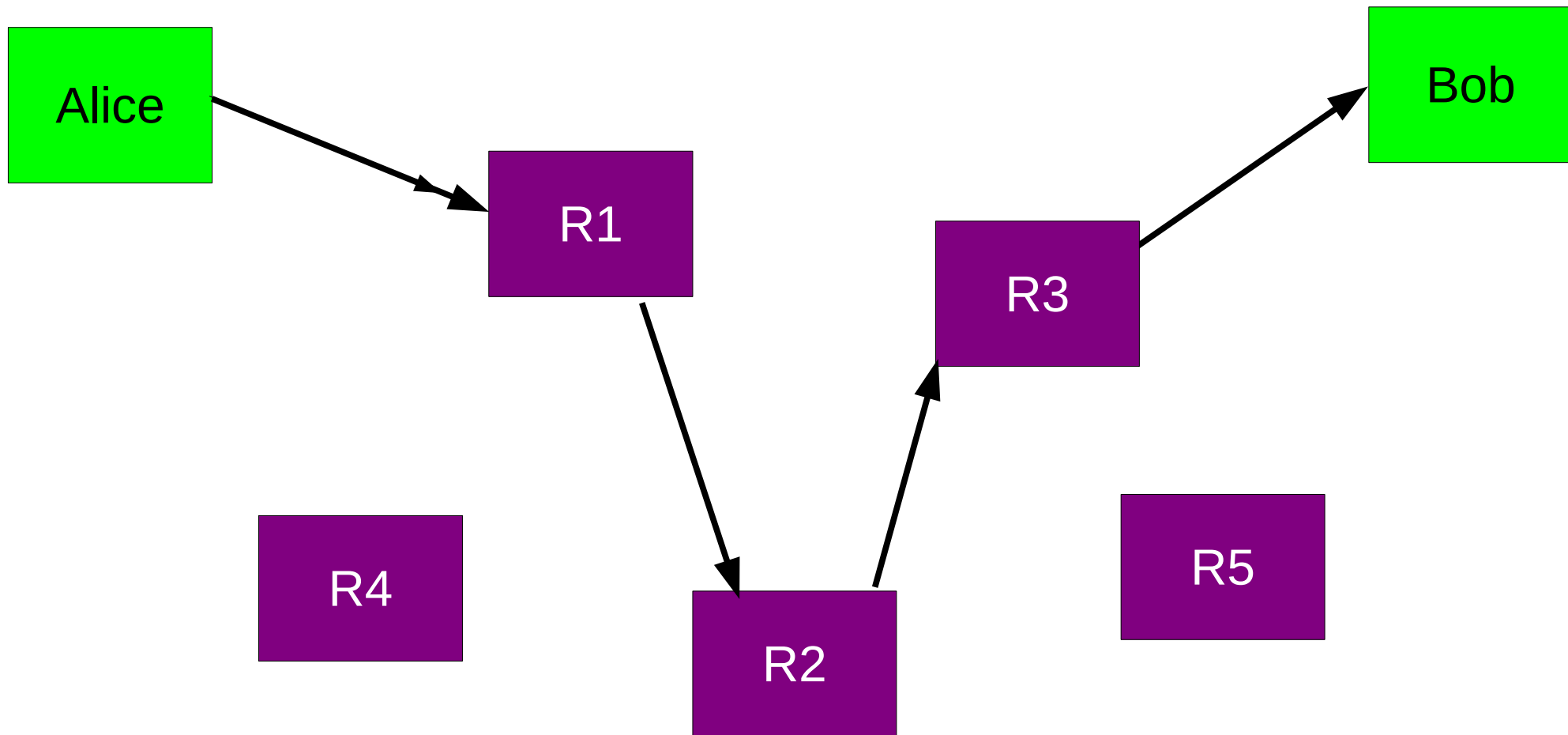


But a single relay is a single point of failure.

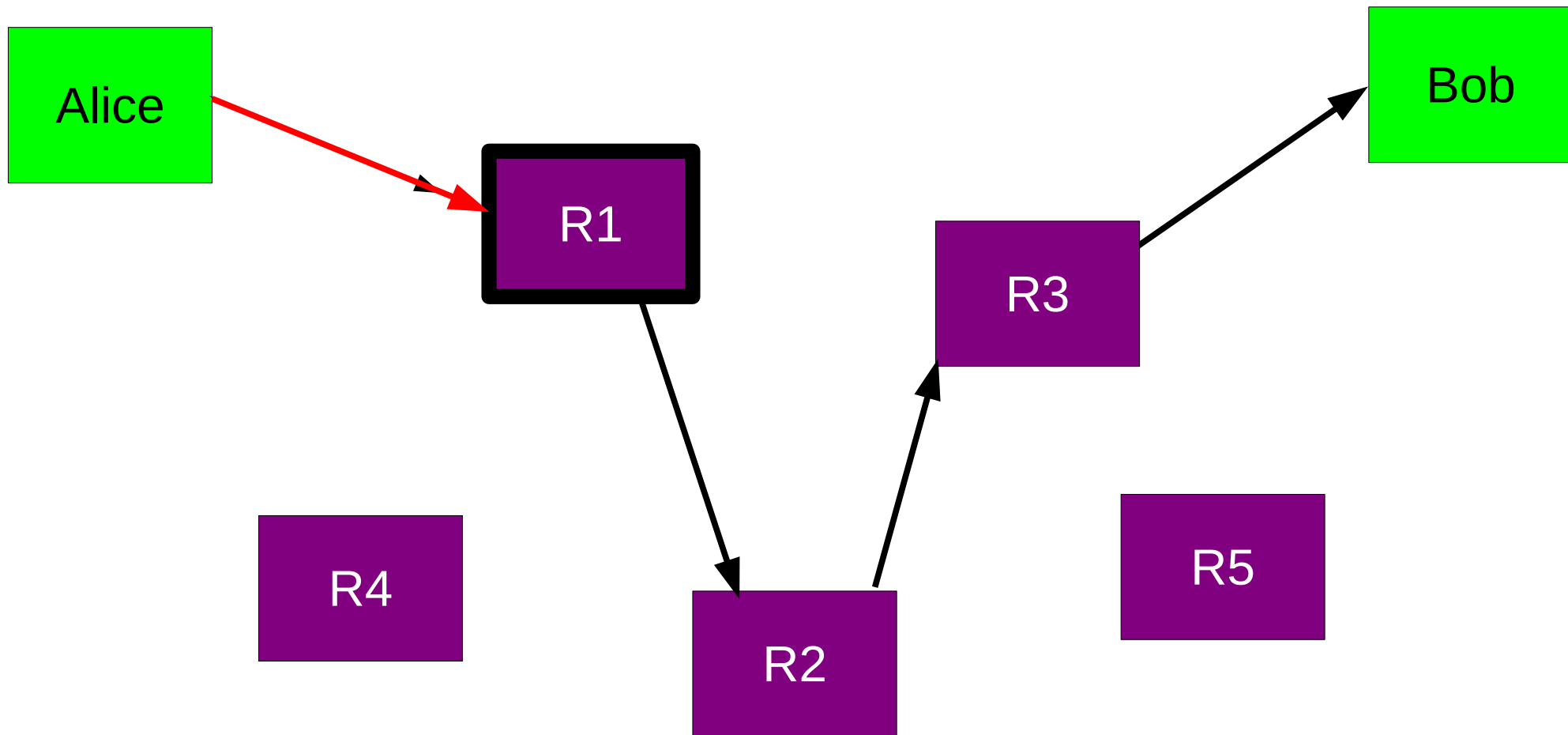


Eavesdropping the relay works too.

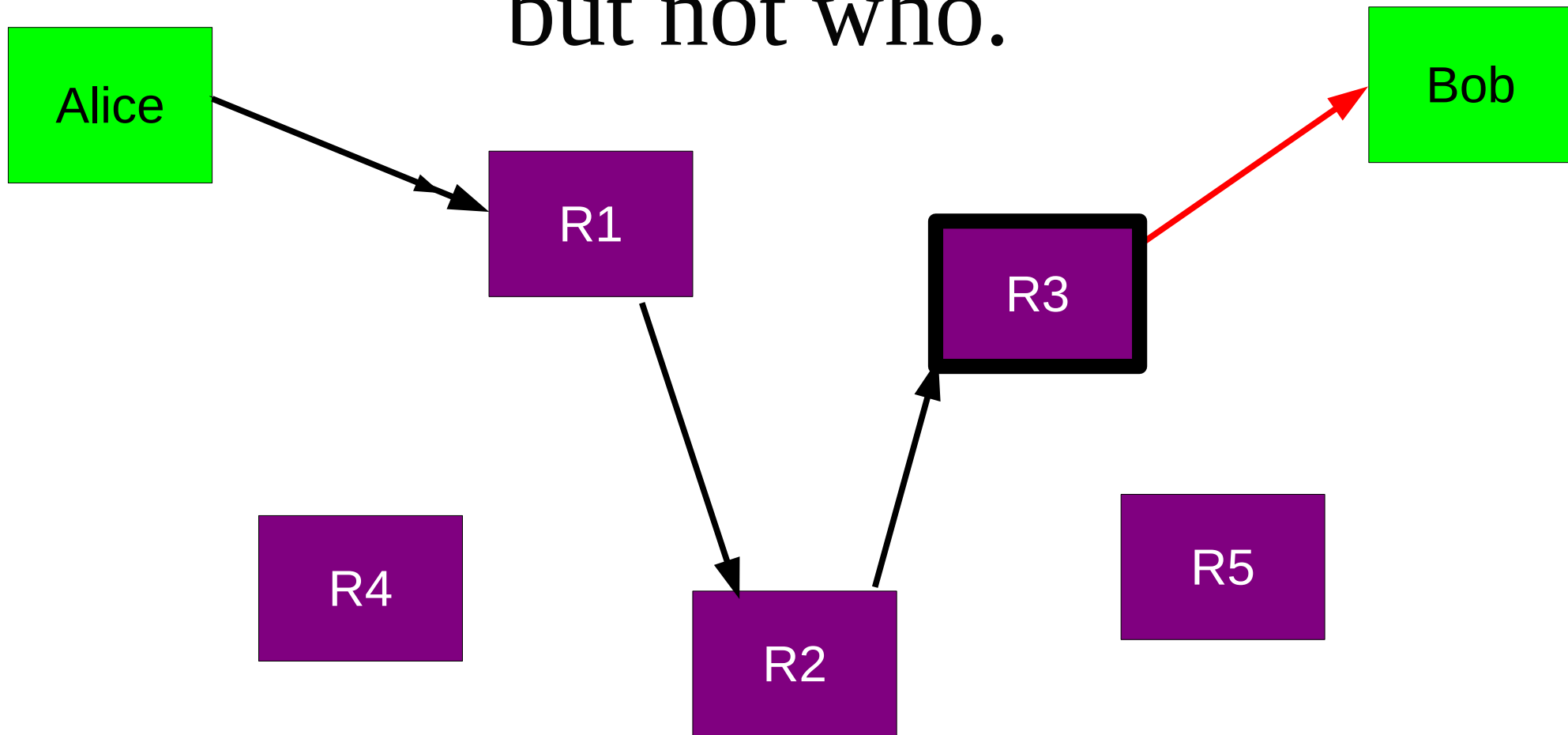
So, add multiple relays so that no single one can betray Alice.



A corrupt first hop can tell that Alice is talking, but not to whom.



A corrupt final hop can tell that somebody is talking to Bob, but not who.



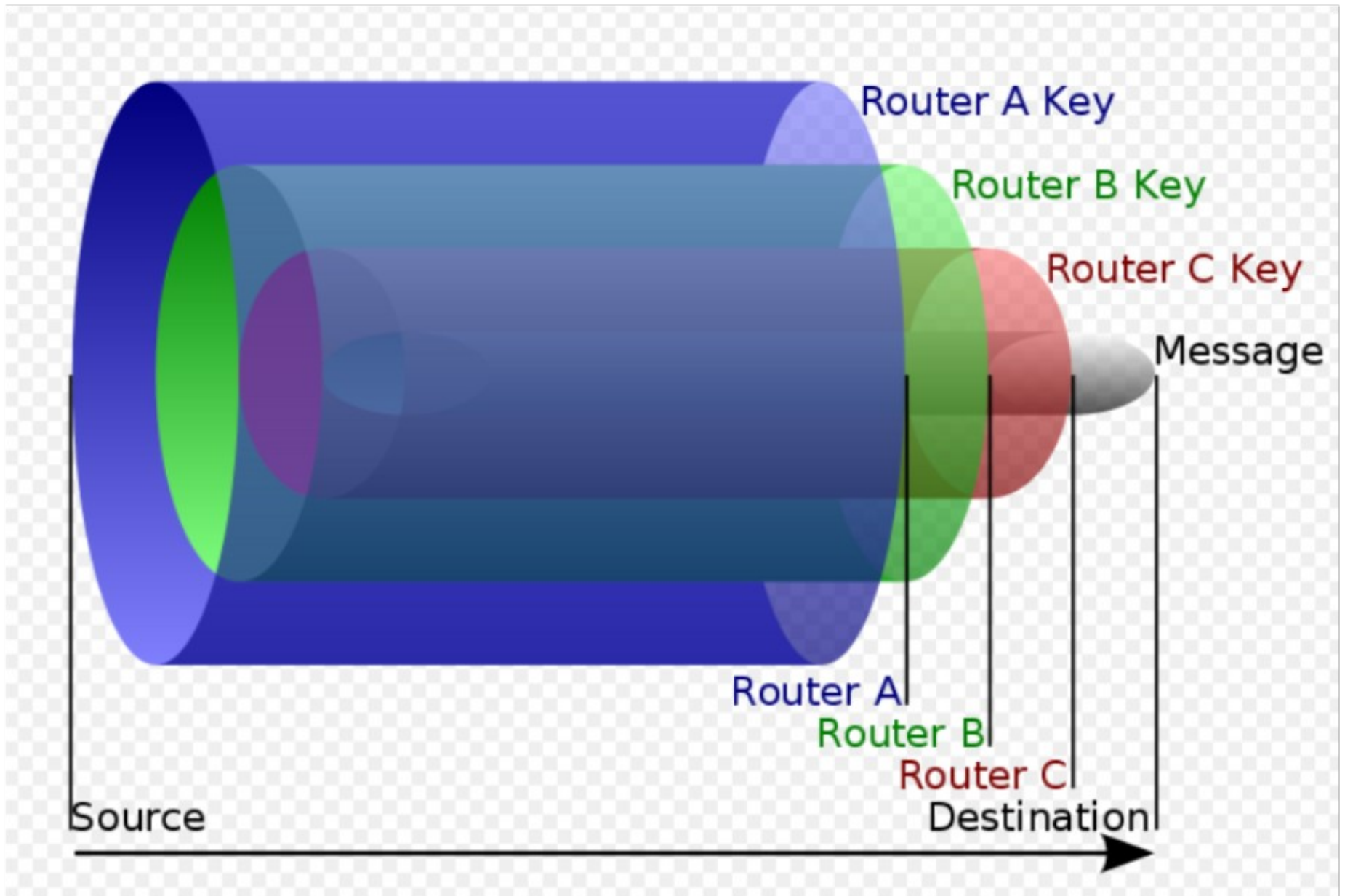
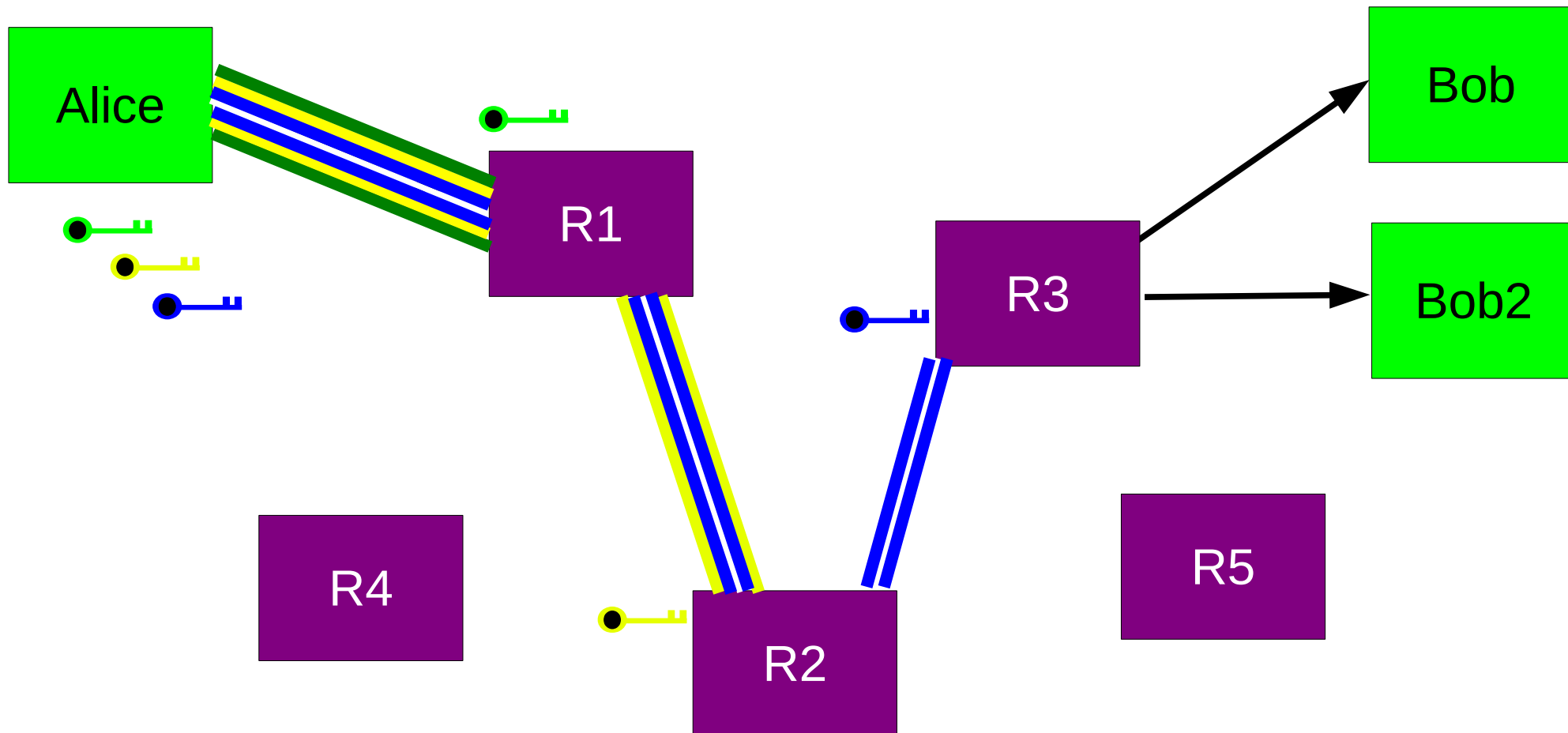
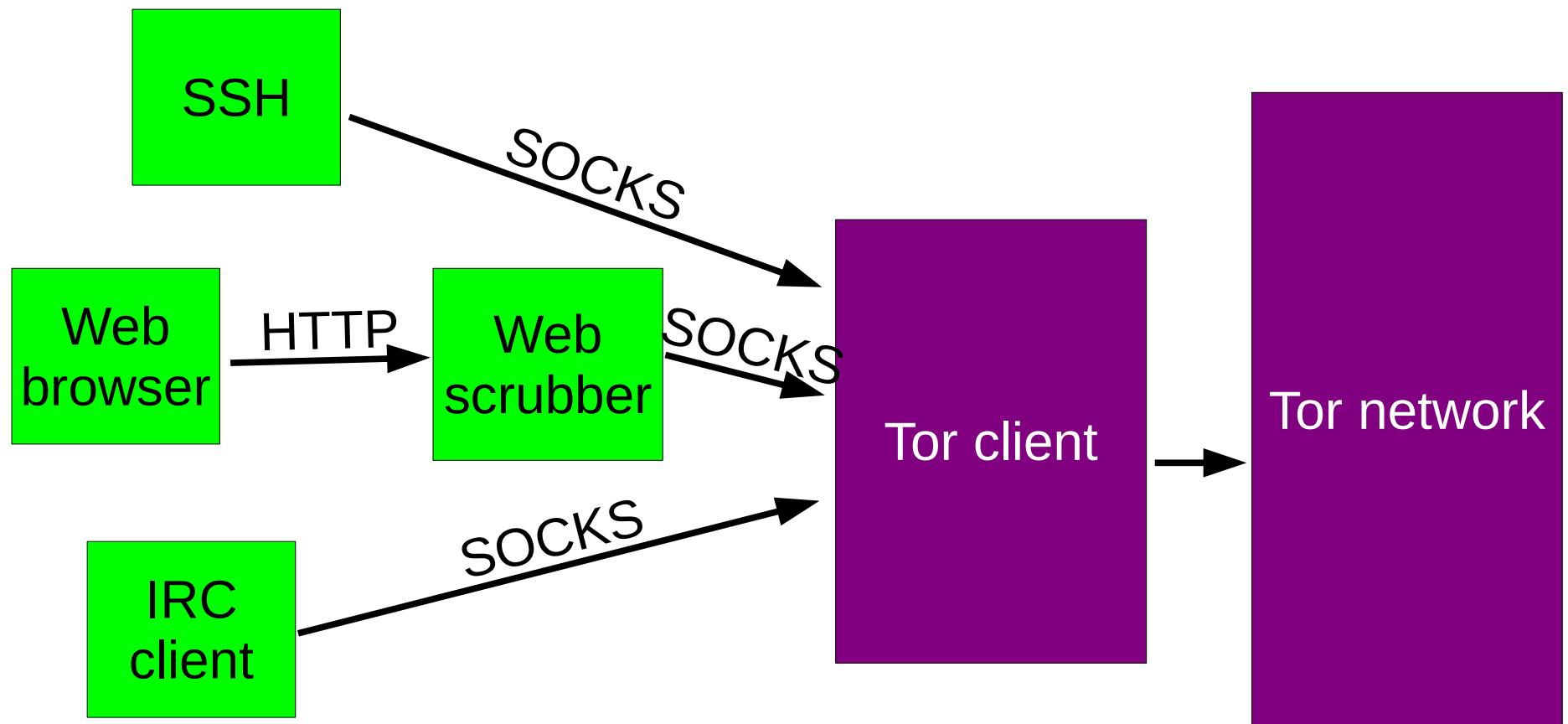


Photo courtesy Wikimedia Commons

**Alice makes a session key with R1
...And then tunnels to R2...and to R3**

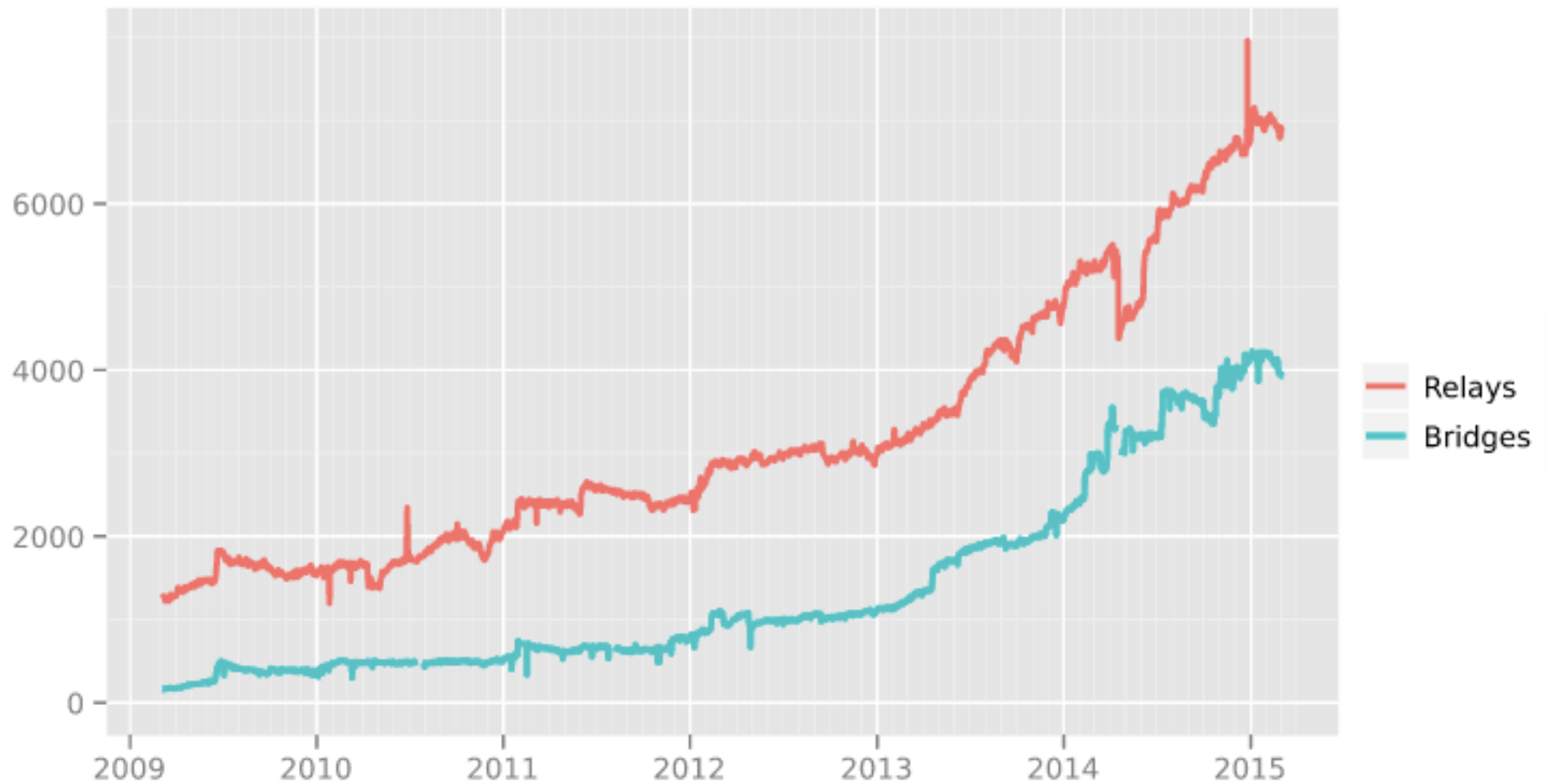


Tor anonymizes TCP streams only:
it needs other applications to clean
high-level protocols.



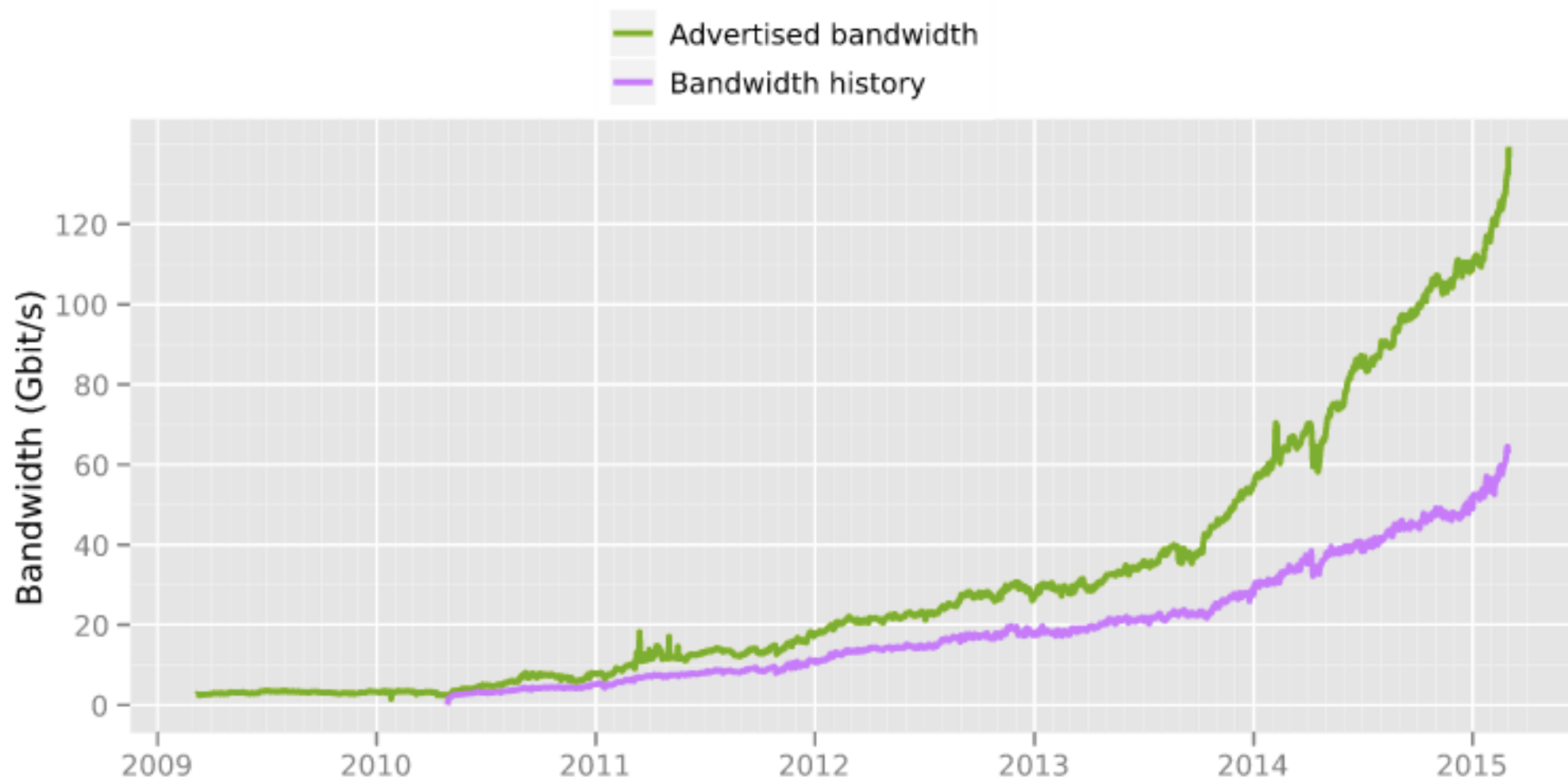
Tor is currently the largest strong anonymity network ever deployed.

Number of relays



The Tor Project - <https://metrics.torproject.org/>

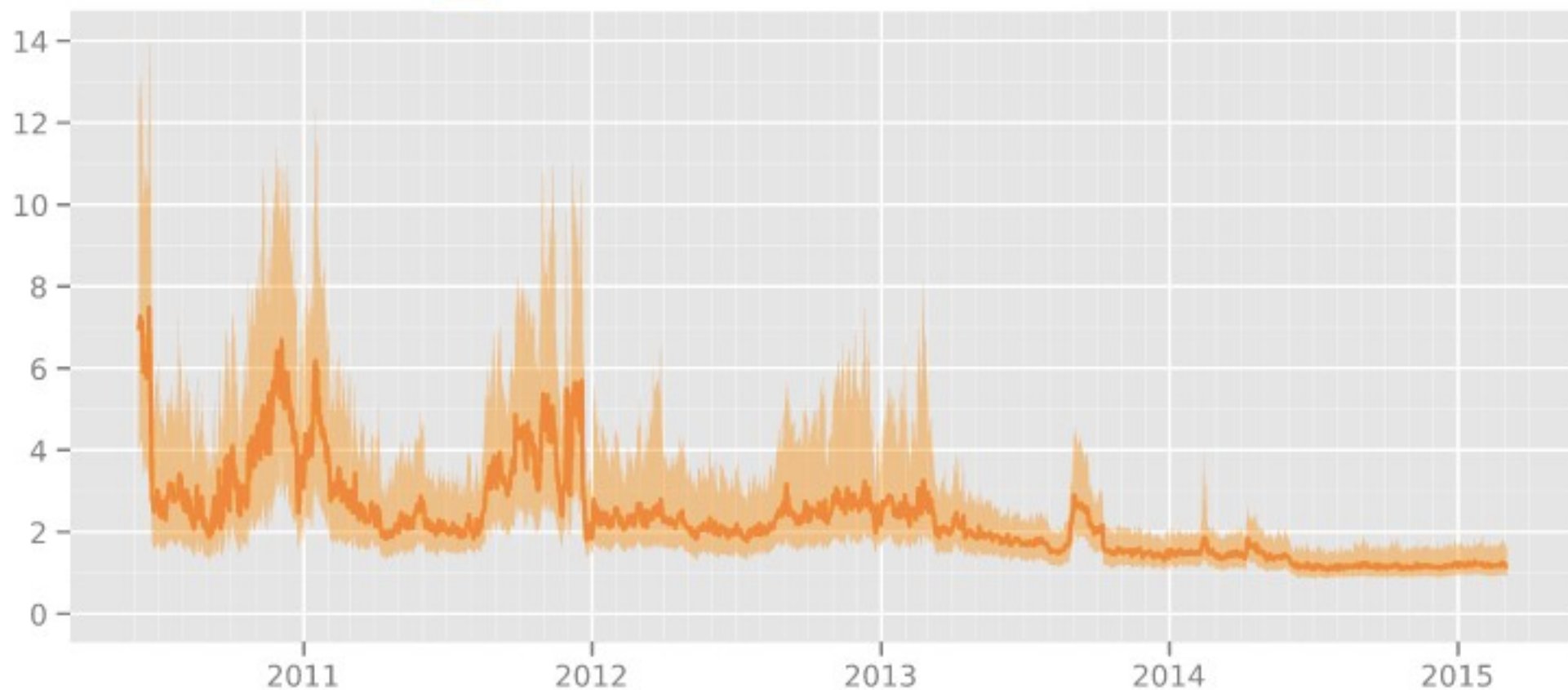
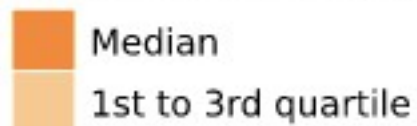
Total relay bandwidth



The Tor Project - <https://metrics.torproject.org/>

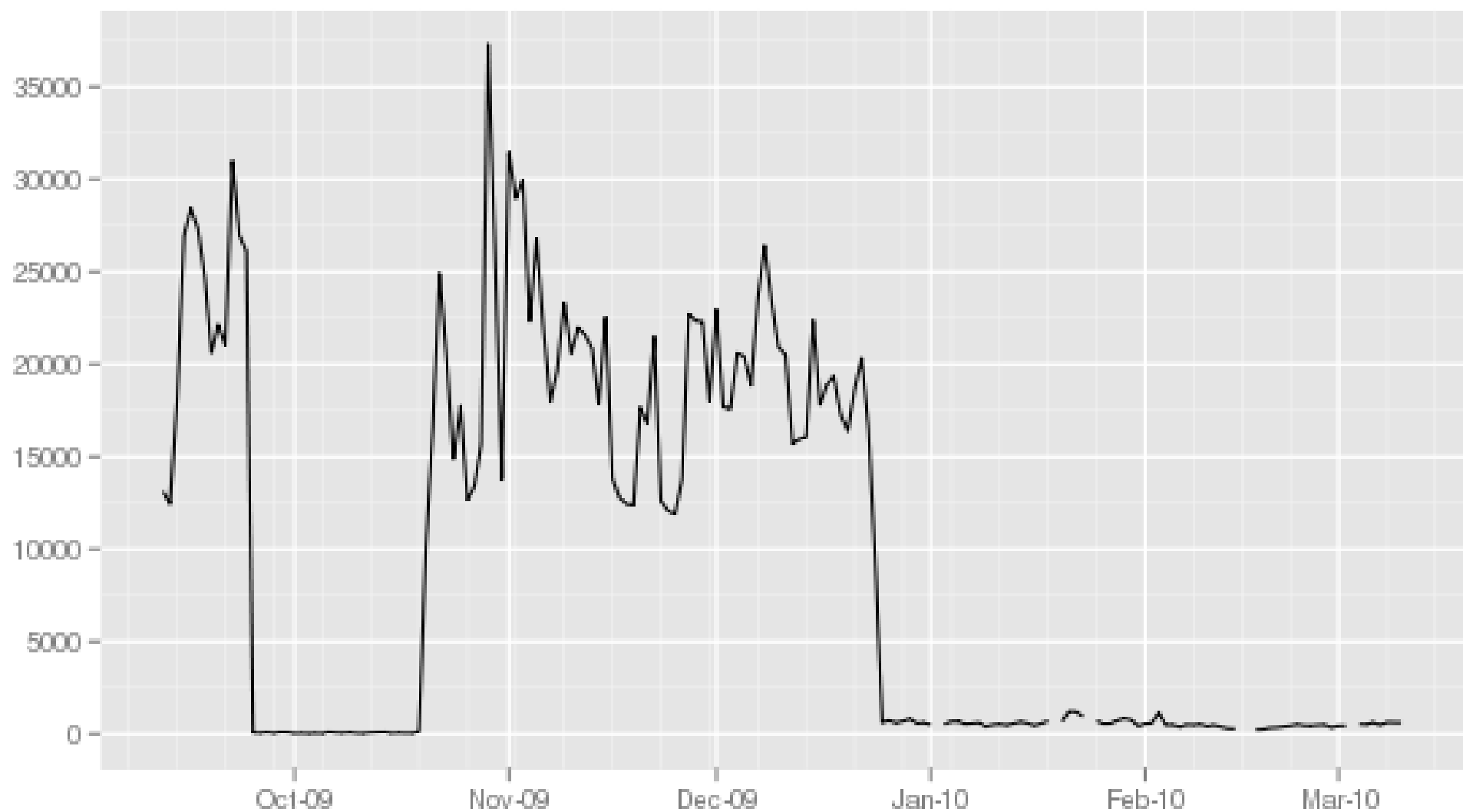
Time in seconds to complete 50 KiB request

Measured times on all sources per day

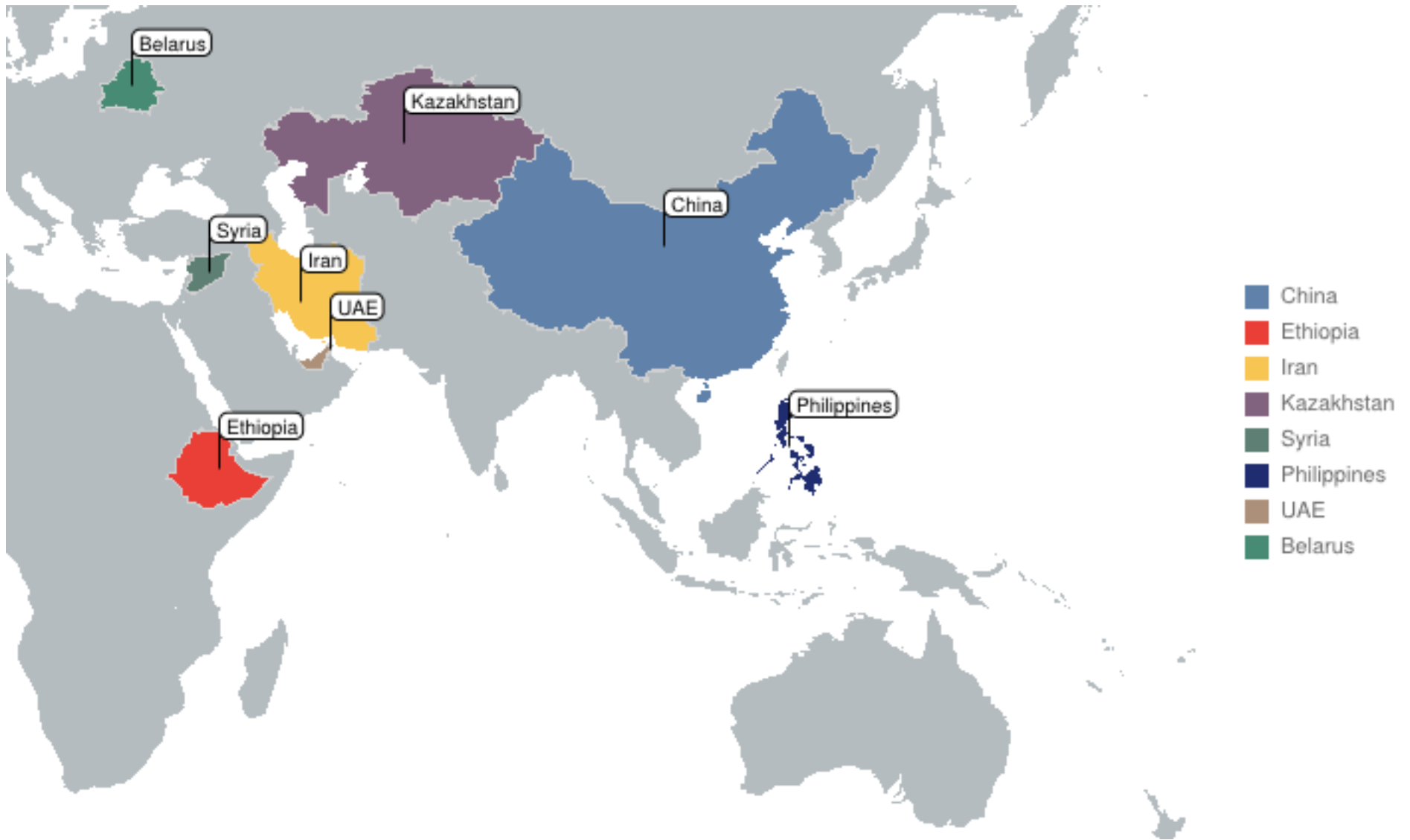


The Tor Project - <https://metrics.torproject.org/>

Recurring, directly connecting Chinese Tor users (past 180 days)

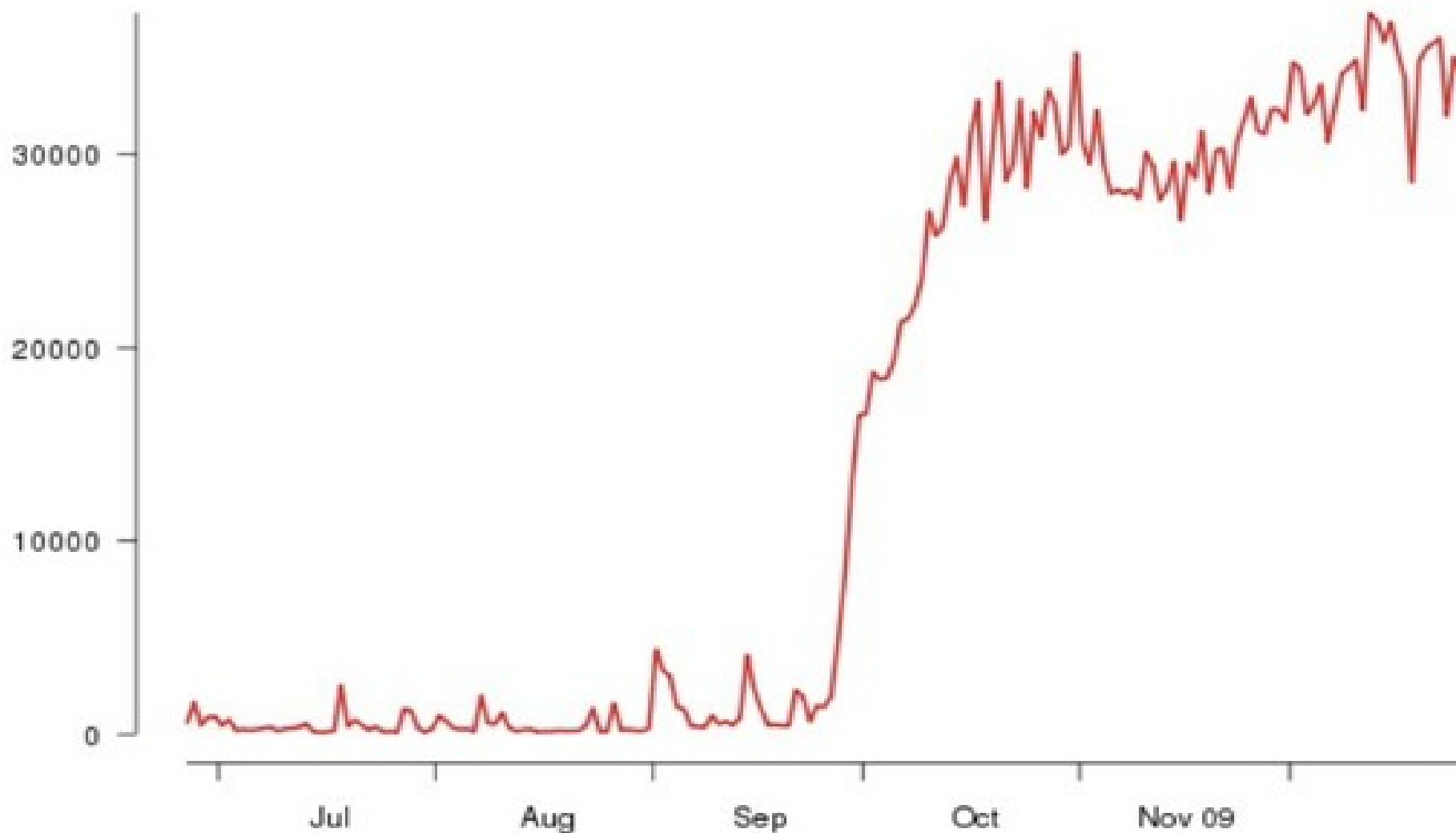


Tor protocol is targeted and filtered

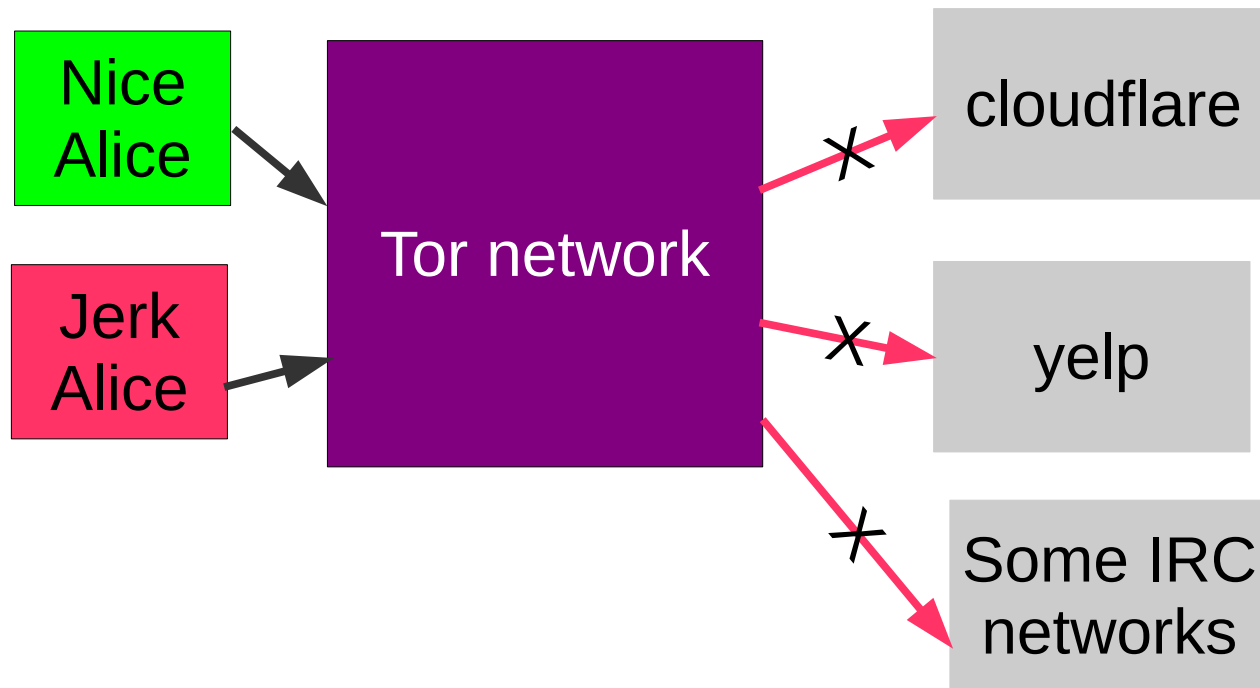


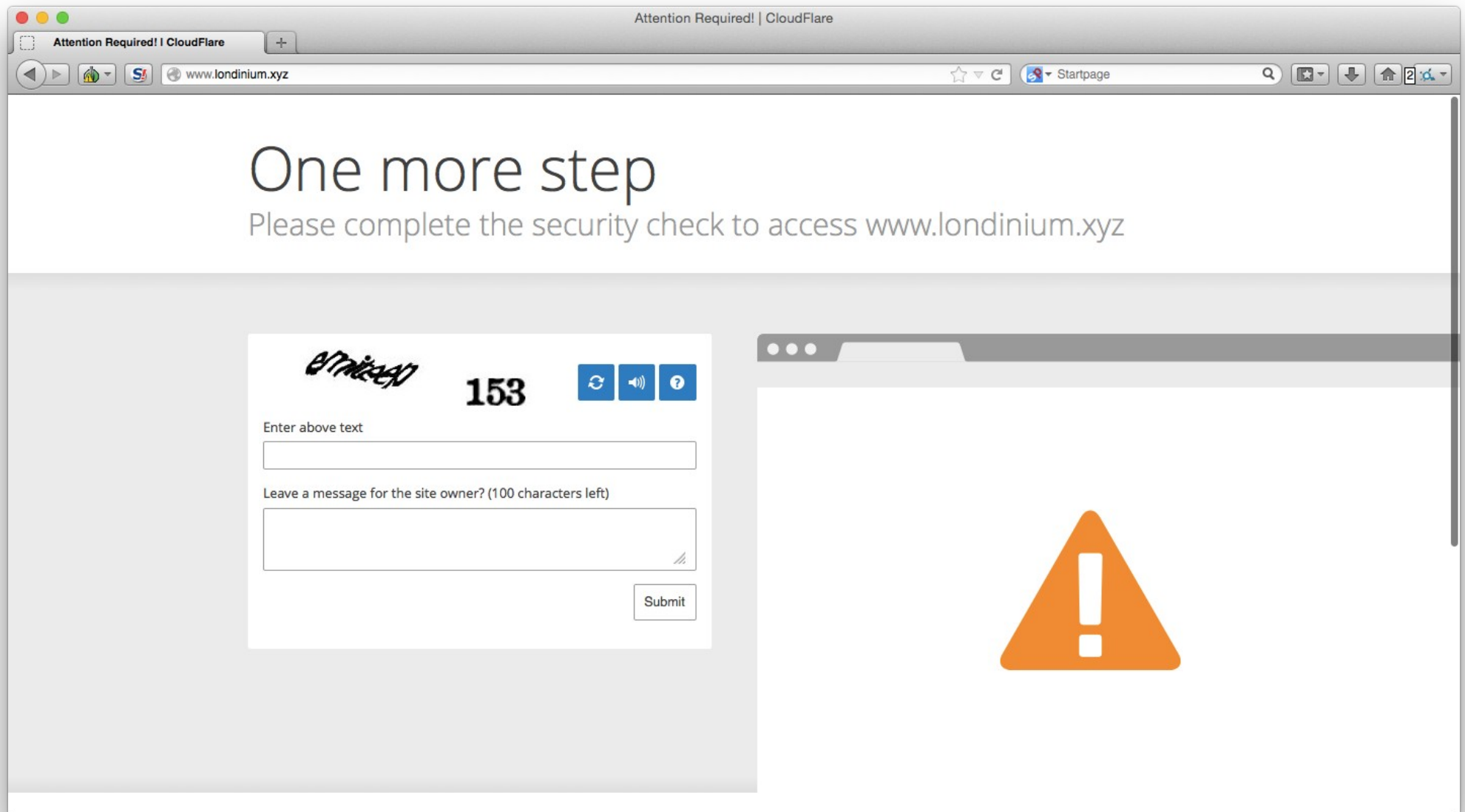
Tor Bridges Help!

Chinese Tor users via bridges



Problem: Abusive users get the whole network blocked.





The Great Cloudflare Captcha Kerfuffle of 2016....

- Tor doesn't magically encrypt the Internet
- Operating Systems and Applications leak your info
- Browser Plugins, Cookies, Extensions, PDF, SVG, and apps all conspire against you



Tor Official & Community Apps



Tor Browser

Tor Browser contains everything you need to safely browse the Internet.



Orbot

Tor for Google Android devices.



Tails

Live CD/USB operating system preconfigured to use Tor safely.



Arm

Terminal (command line) application for monitoring and configuring Tor.



Atlas

Site providing an overview of the Tor network.



Pluggable Transports

Pluggable transports help you circumvent censorship.



Stem

Library for writing scripts and applications that interact with Tor.



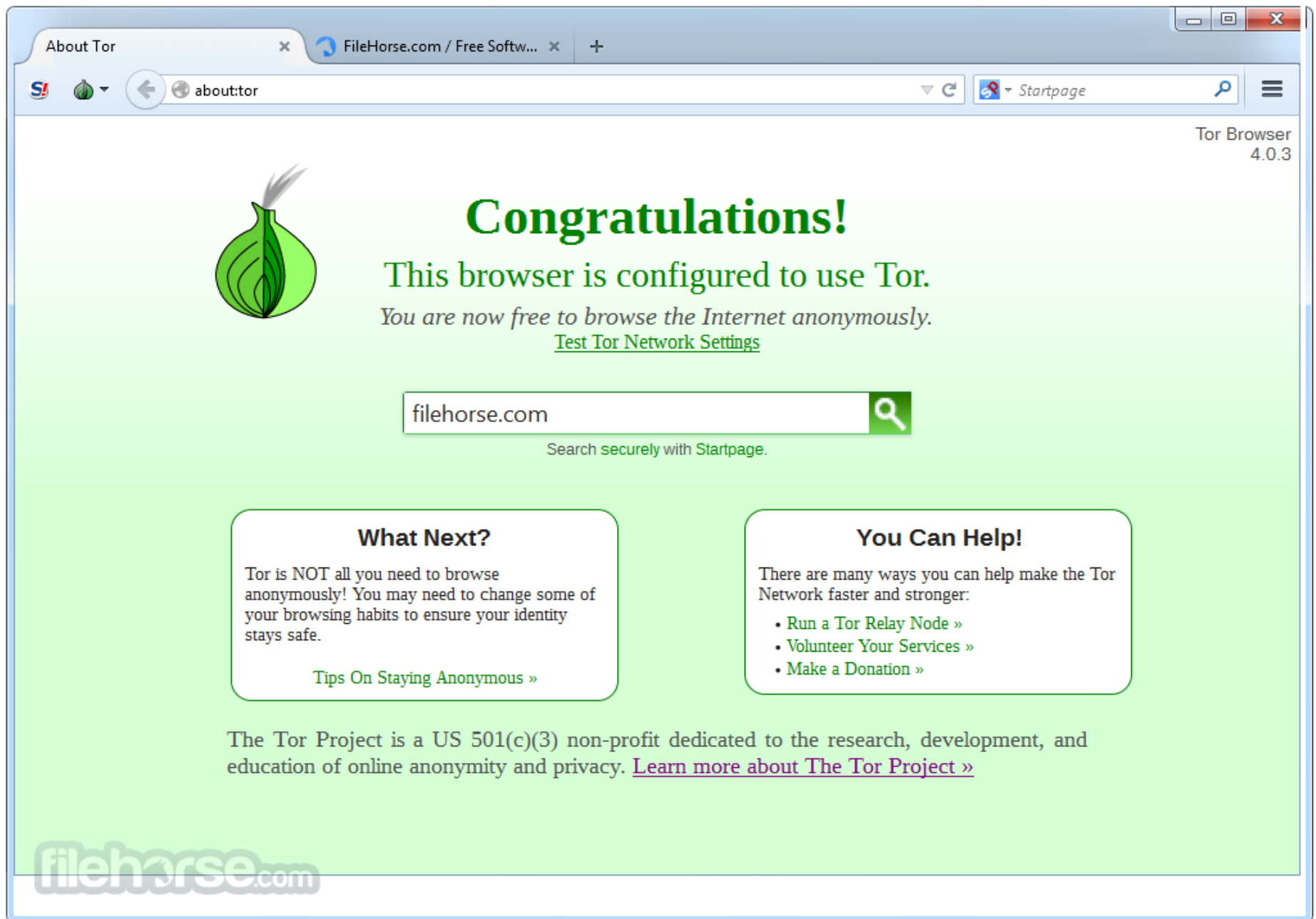
OONI

Global observatory monitoring for network censorship.







Open Observatory of Network Interference
ooni

<https://www.torproject.org/projects/projects>

Tor Browser




TAILS












Applications Places System    USA   Fri Aug 16, 10:40 AM 


Computer
amnesia's Home
Trash
Tails documentation
Report a Bug

Are you using Tor? - Iceweasel

File Edit View History Bookmarks Tools Help

Are you using Tor? 

     <https://check.torproject.org>    Startpage H   



Congratulations. Your browser is configured to use Tor.

Please refer to the [Tor website](https://www.torproject.org/) for further information about using Tor safely. You are now free to browse the Internet anonymously.

Tor Bandwidth Usage

Recv: 66.54 KB (0.00 KB/s)
Sent: 19.13 KB (0.00 KB/s)

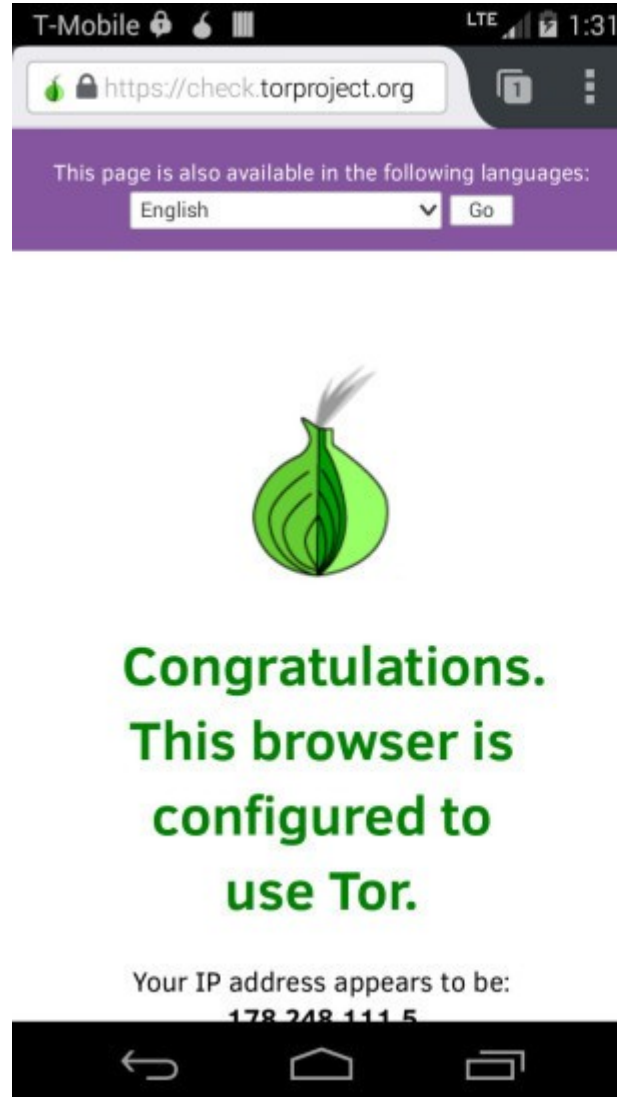
10.00 KB/s
7.50 KB/s
5.00 KB/s
2.50 KB/s

Show Settings Reset

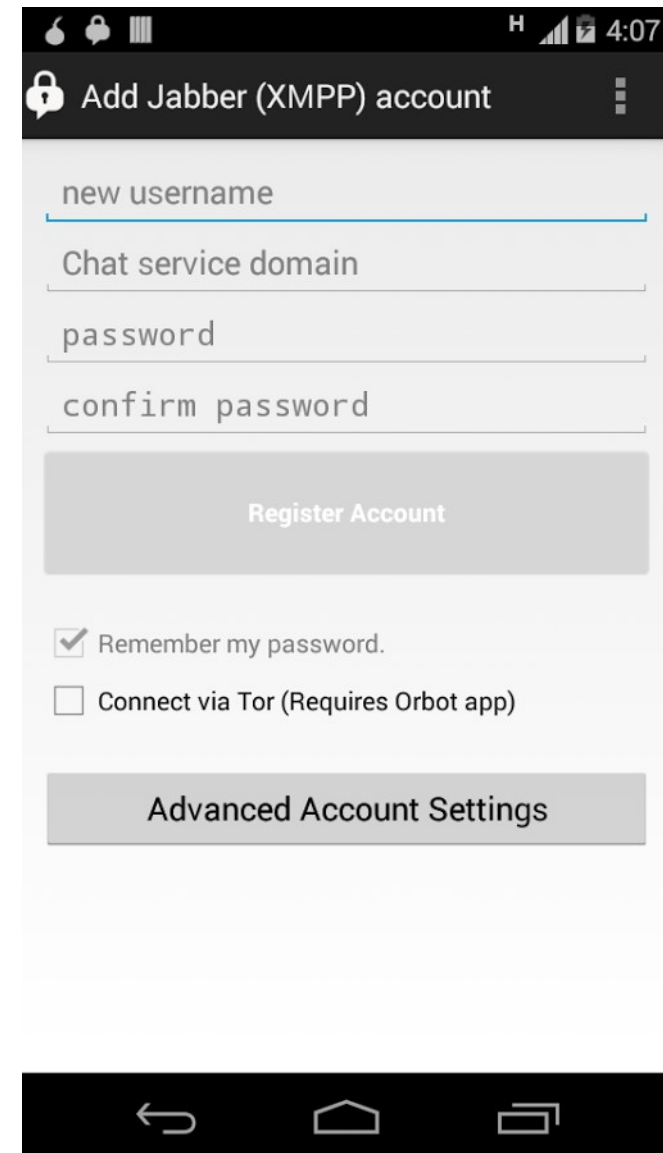
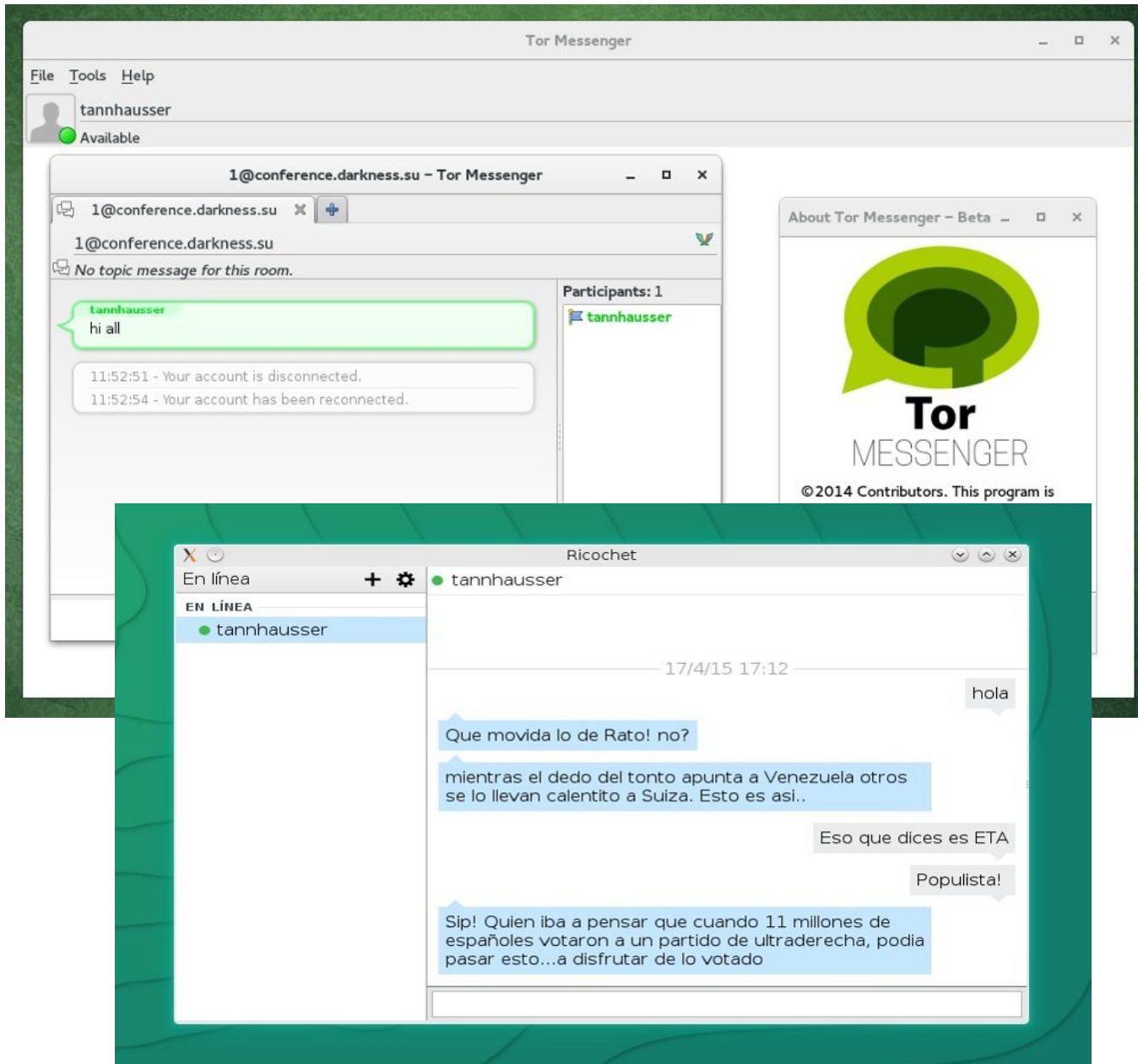
Since: Aug 16 11:30:14

Are you using Tor? - Ic... Tor Bandwidth Usage

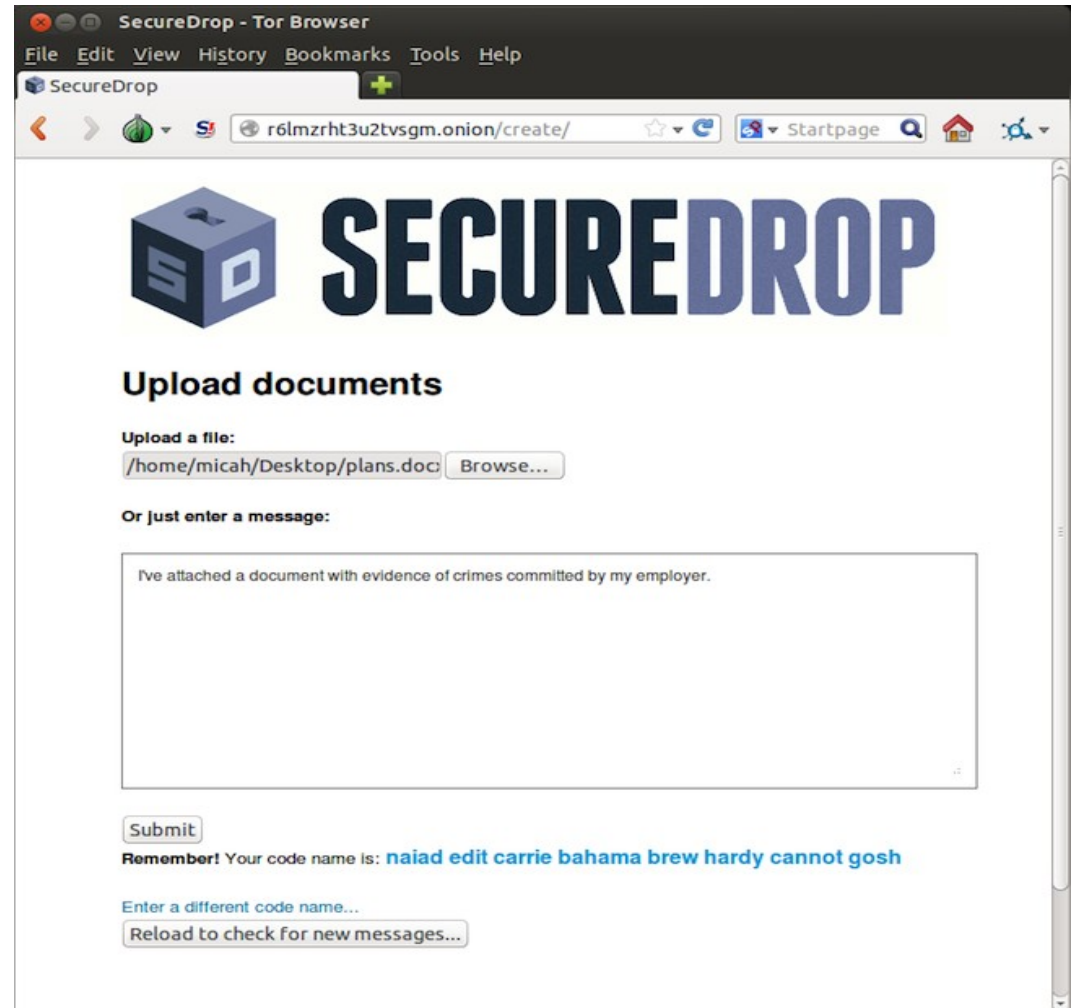
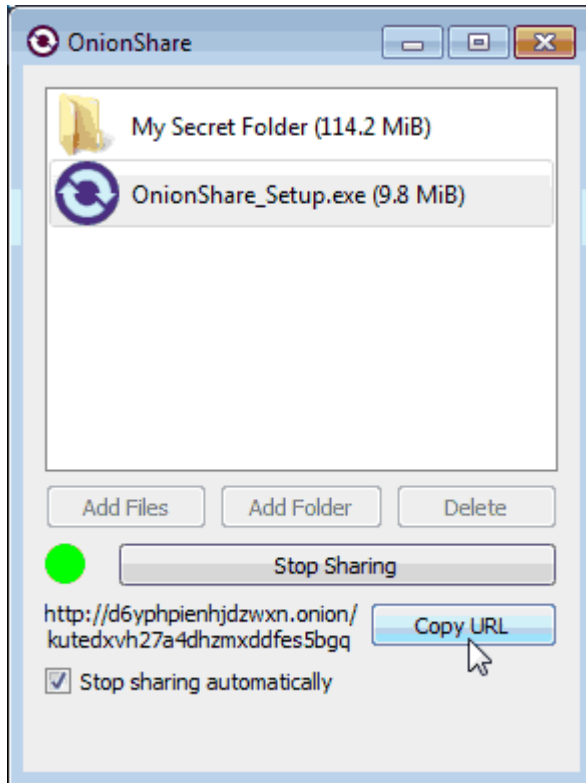
Orbot + Orfox (Android)



Messaging over Tor

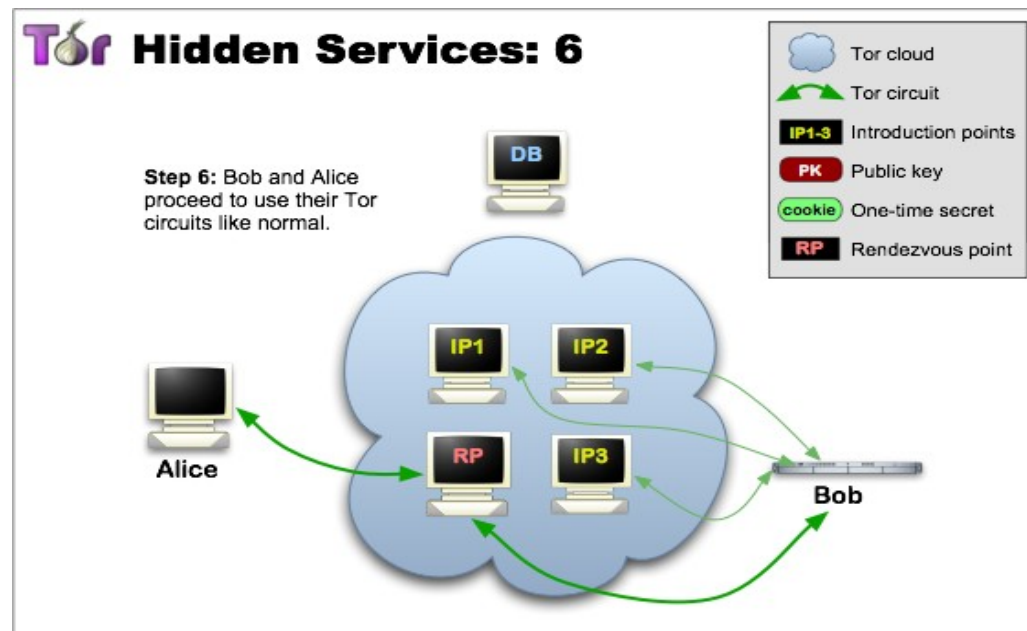


File Sharing over Tor



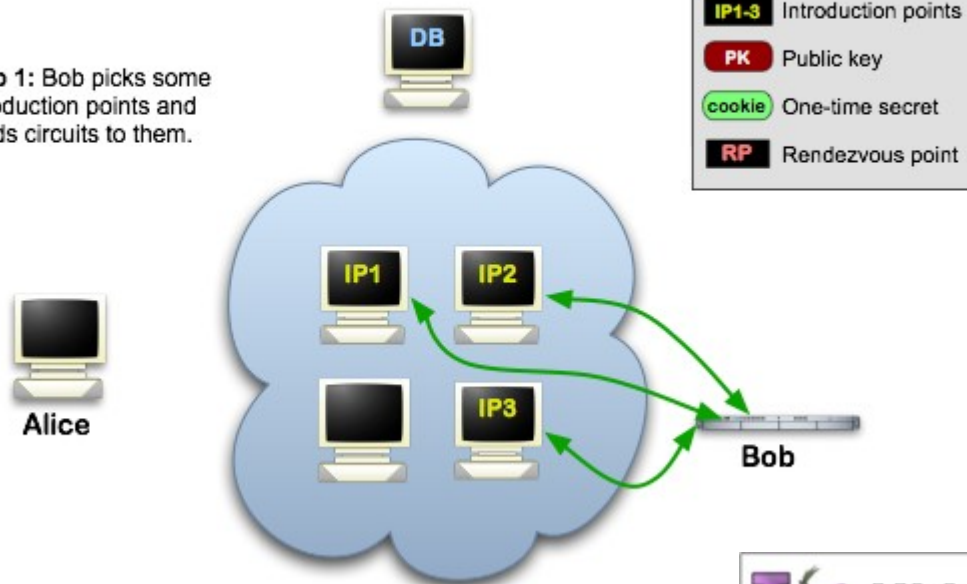
Hidden Services aka “Onion Sites”

- Developed by US NRL and Finnish Defense
- Hides location and routing information of both the server and client
- DHT Directory design



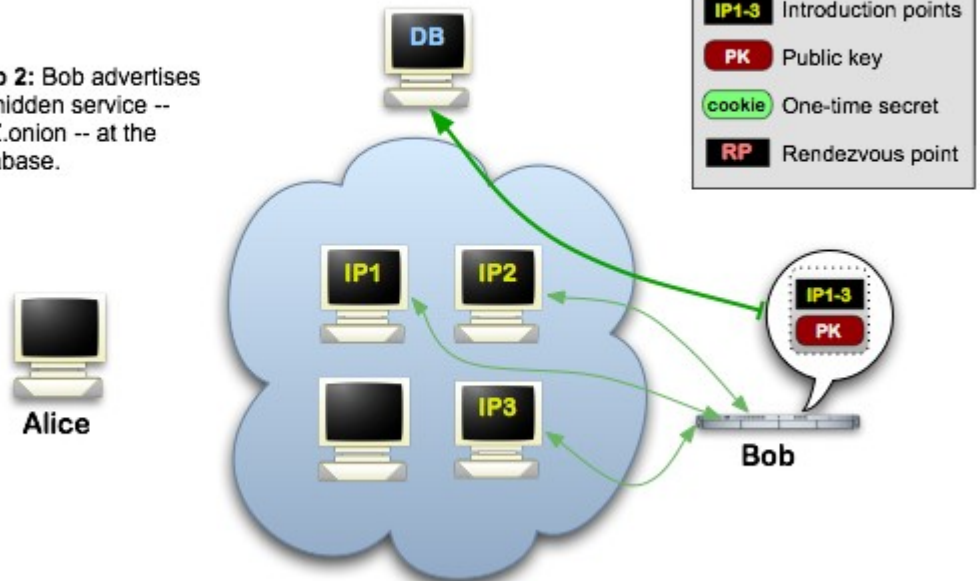
Tor Hidden Services: 1

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



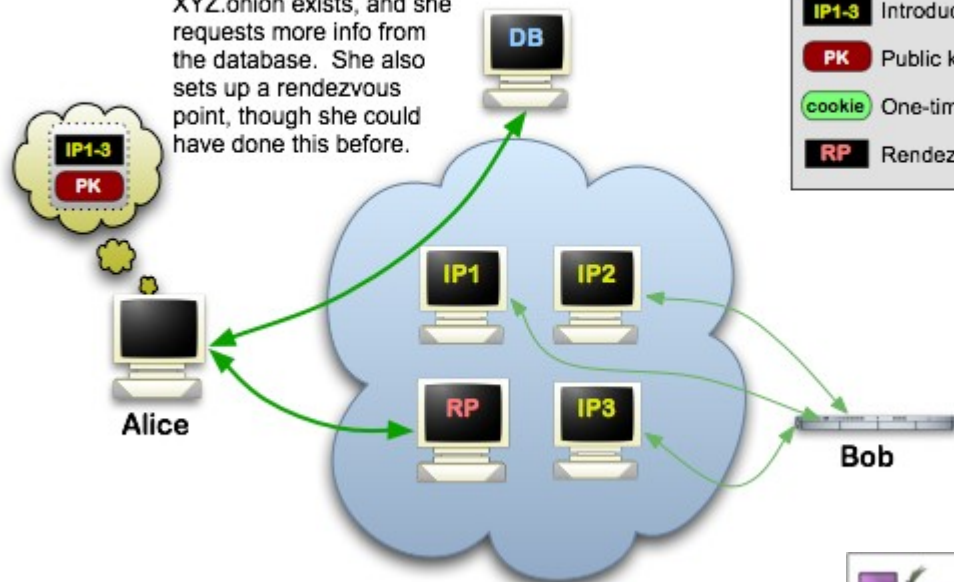
Tor Hidden Services: 2

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



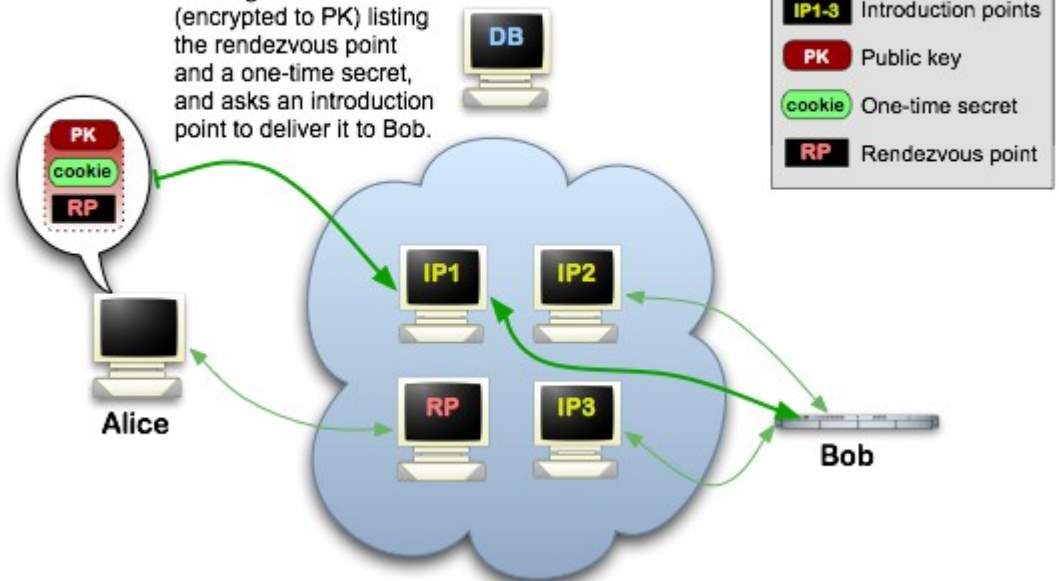
Tor Hidden Services: 3

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.



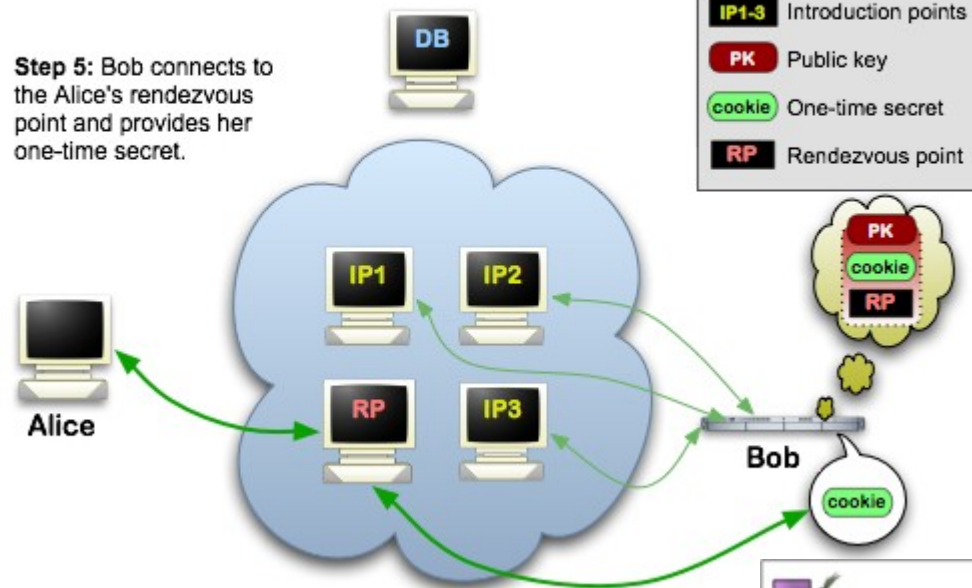
Tor Hidden Services: 4

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.



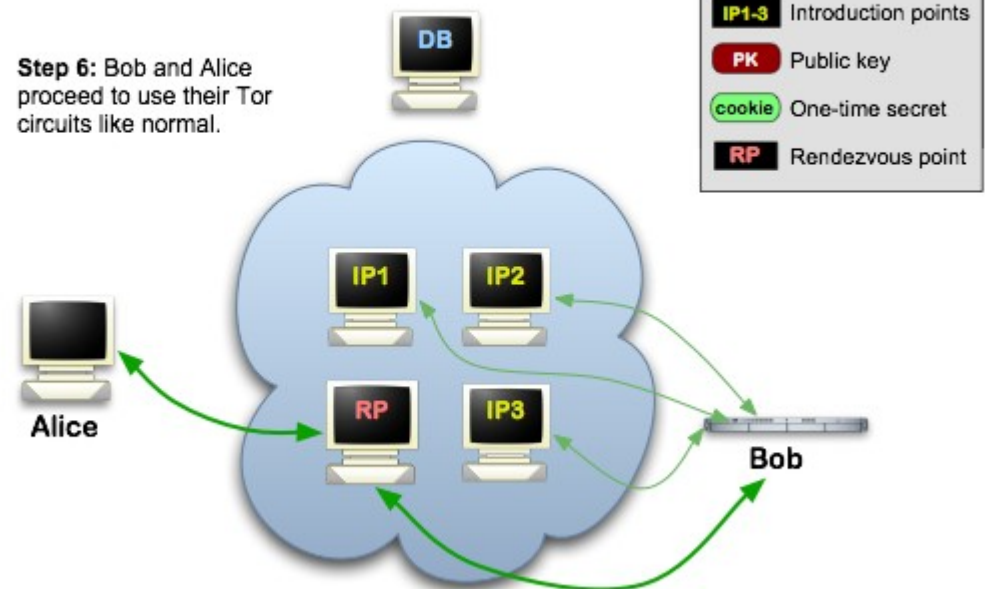
Tor Hidden Services: 5

Step 5: Bob connects to the Alice's rendezvous point and provides her one-time secret.



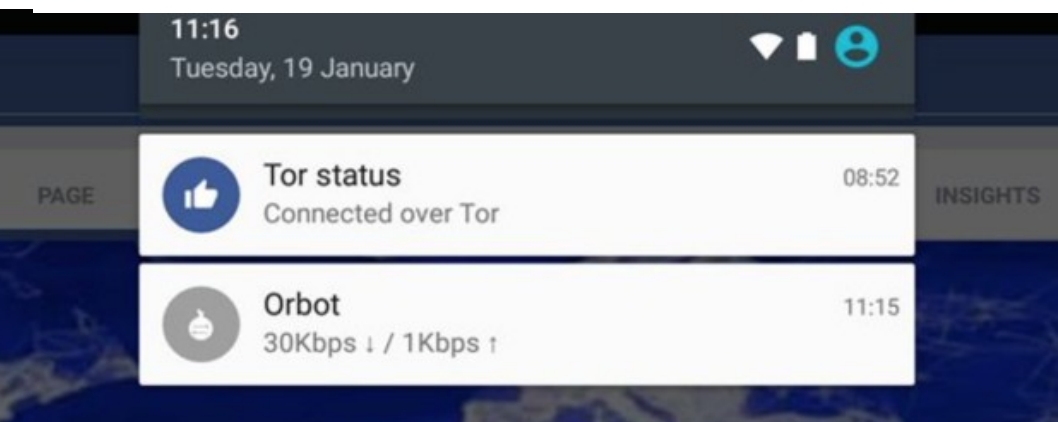
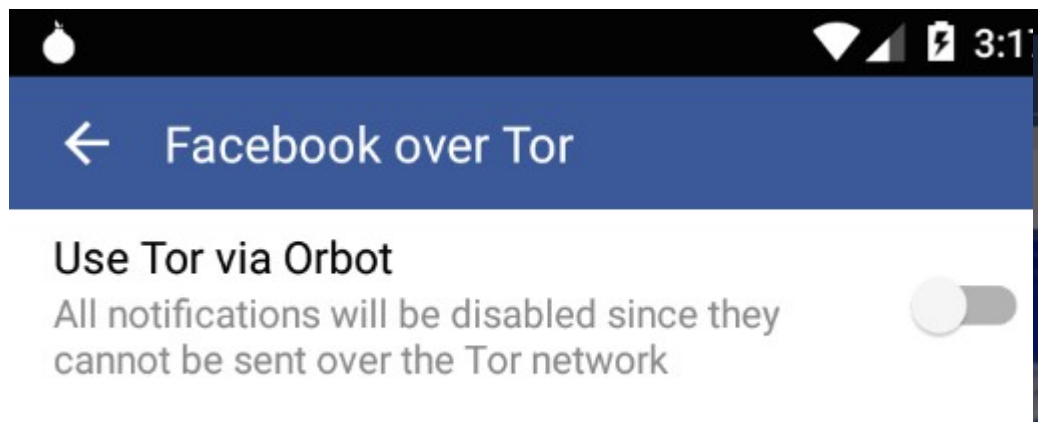
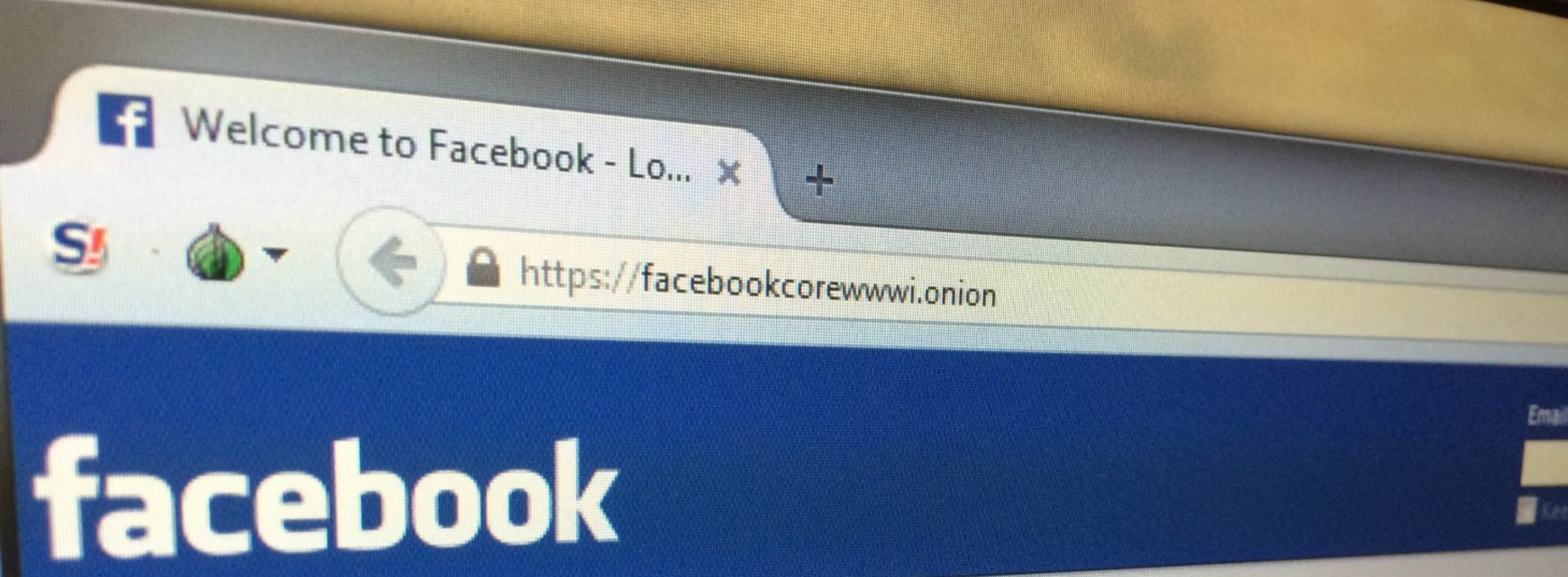
Tor Hidden Services: 6

Step 6: Bob and Alice proceed to use their Tor circuits like normal.



**On the way to anonymity,
Tor has significantly improved
confidentiality and authentication
options for production internet services.**

Enter Facebook...



Facebook chose Tor because it was the best option to make their users more secure.

Tor makes the Internet more secure through confidential and authenticated communication channels for any app or site.

Anonymity is for everyone.