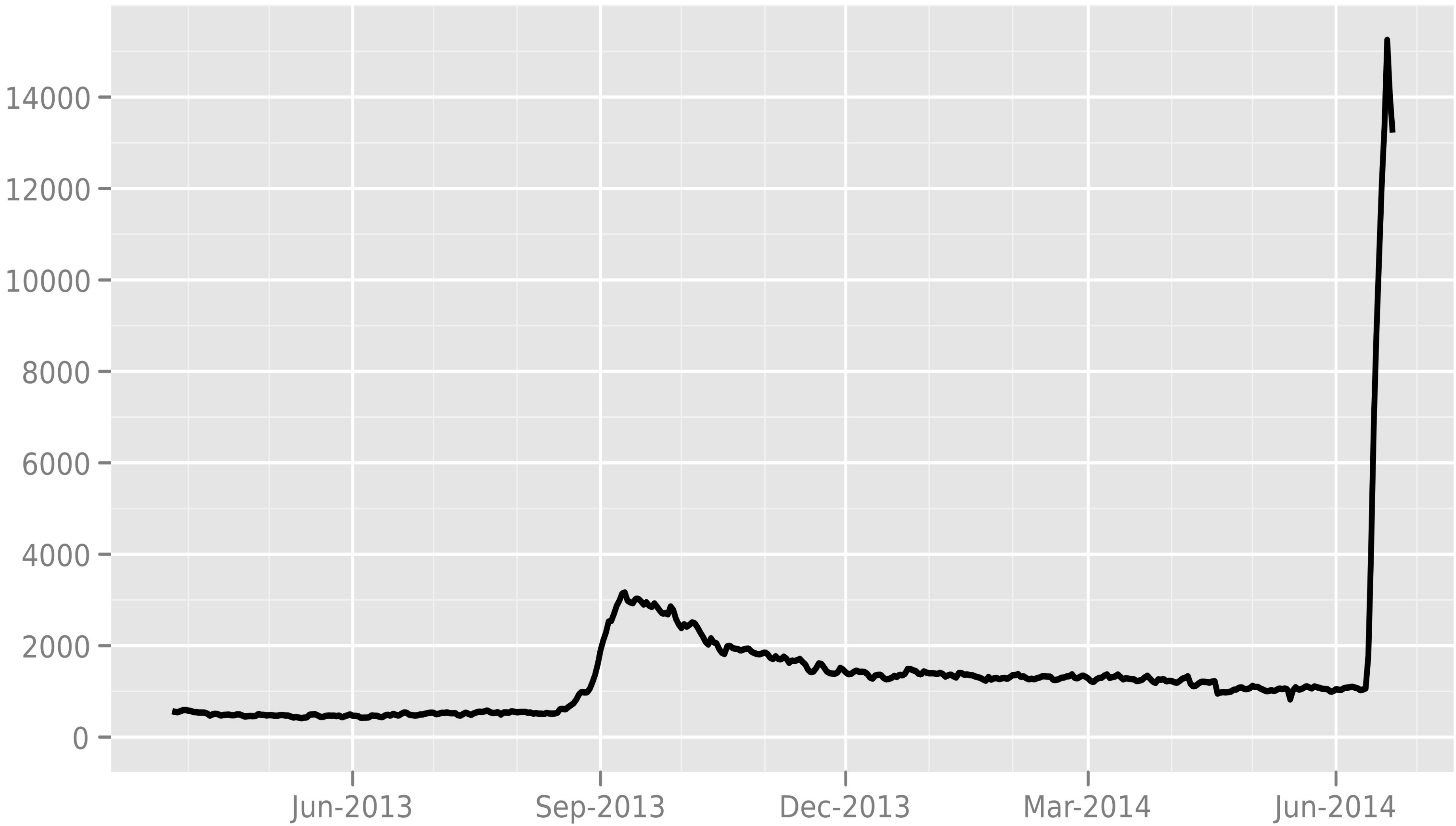
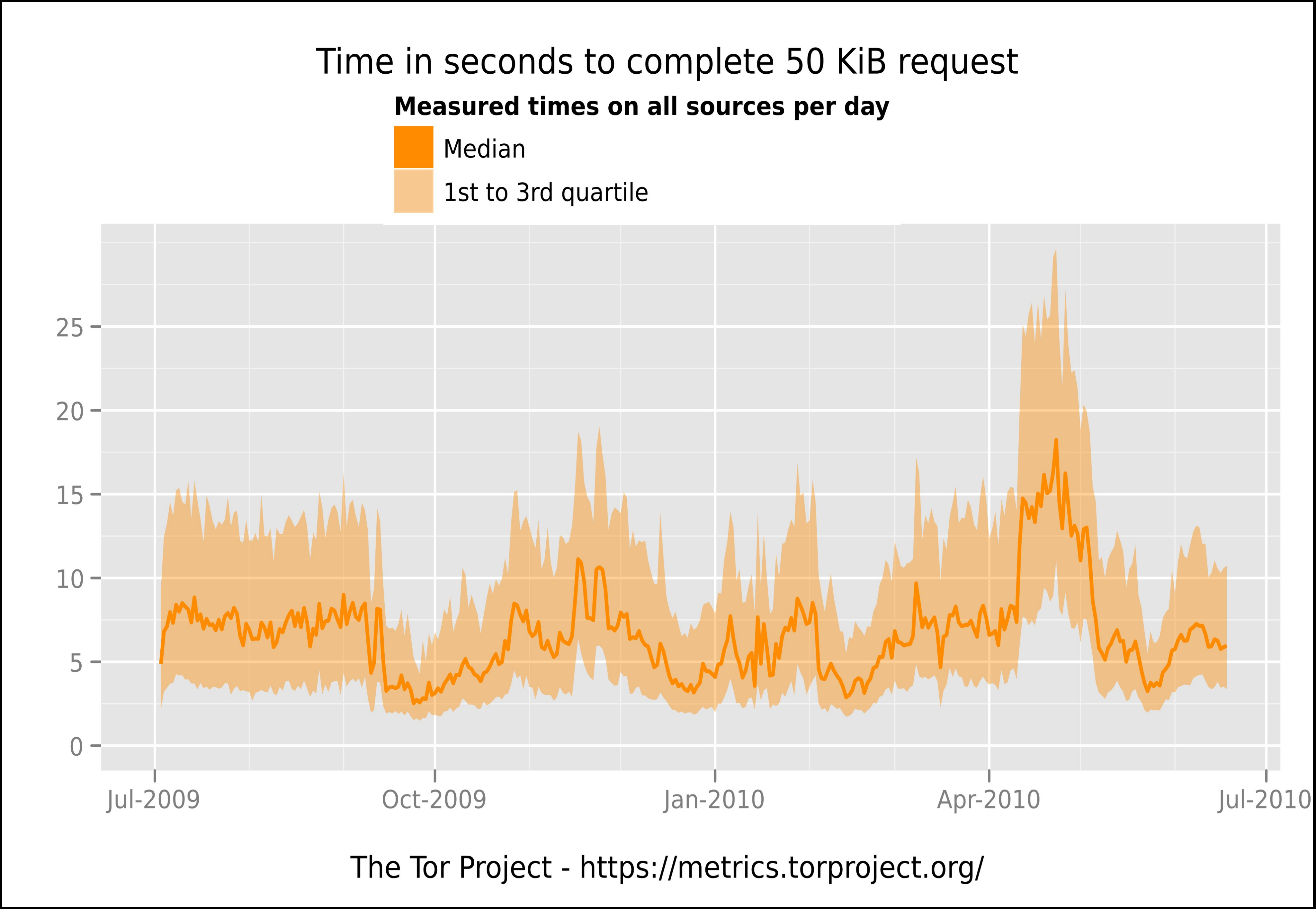
The Tor Project, Inc.

Our mission is to be the global resource for technology, advocacy, research and education in the ongoing pursuit of freedom of speech, privacy rights online, and censorship circumvention.

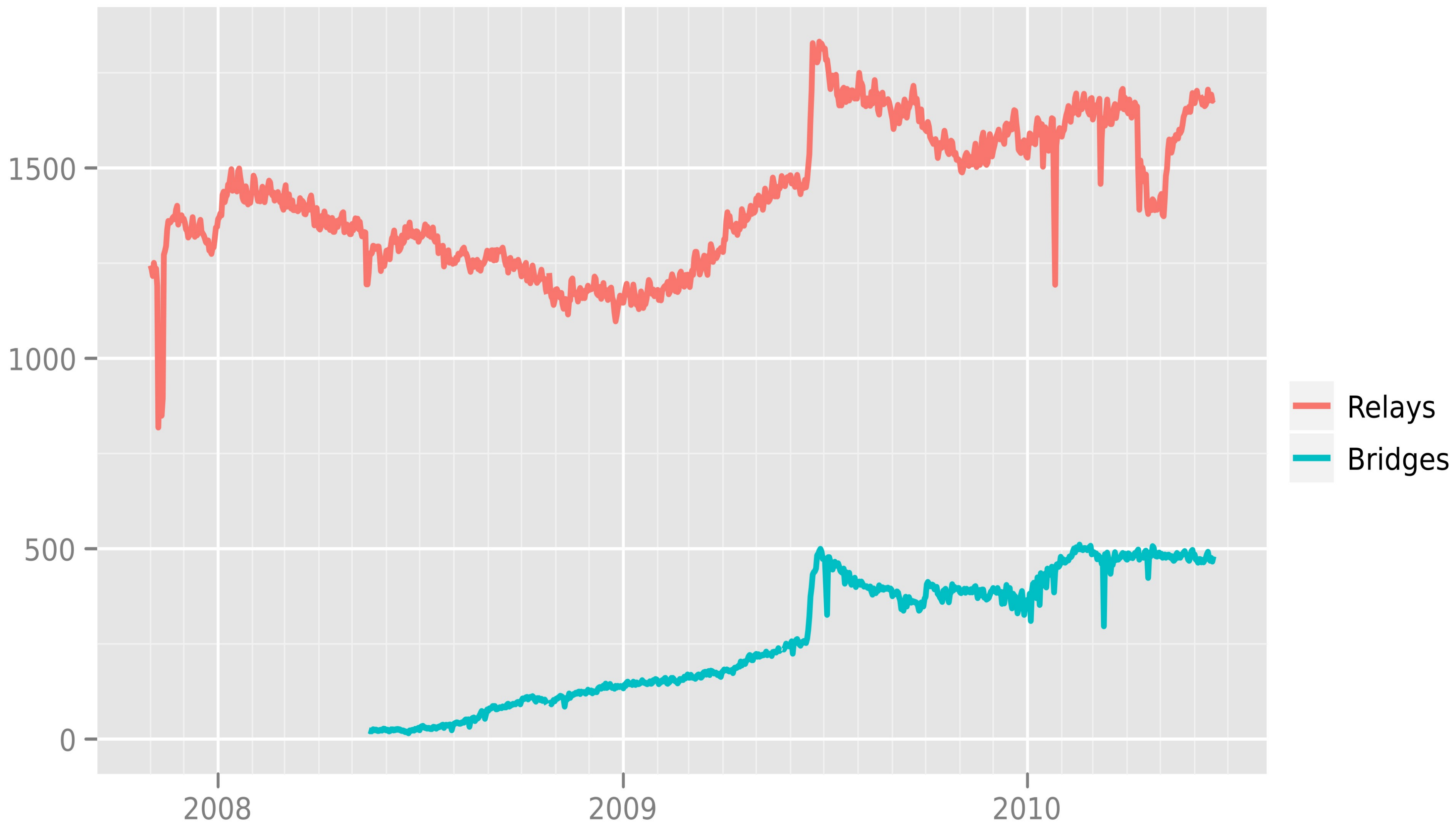
Directly connecting users from Iraq



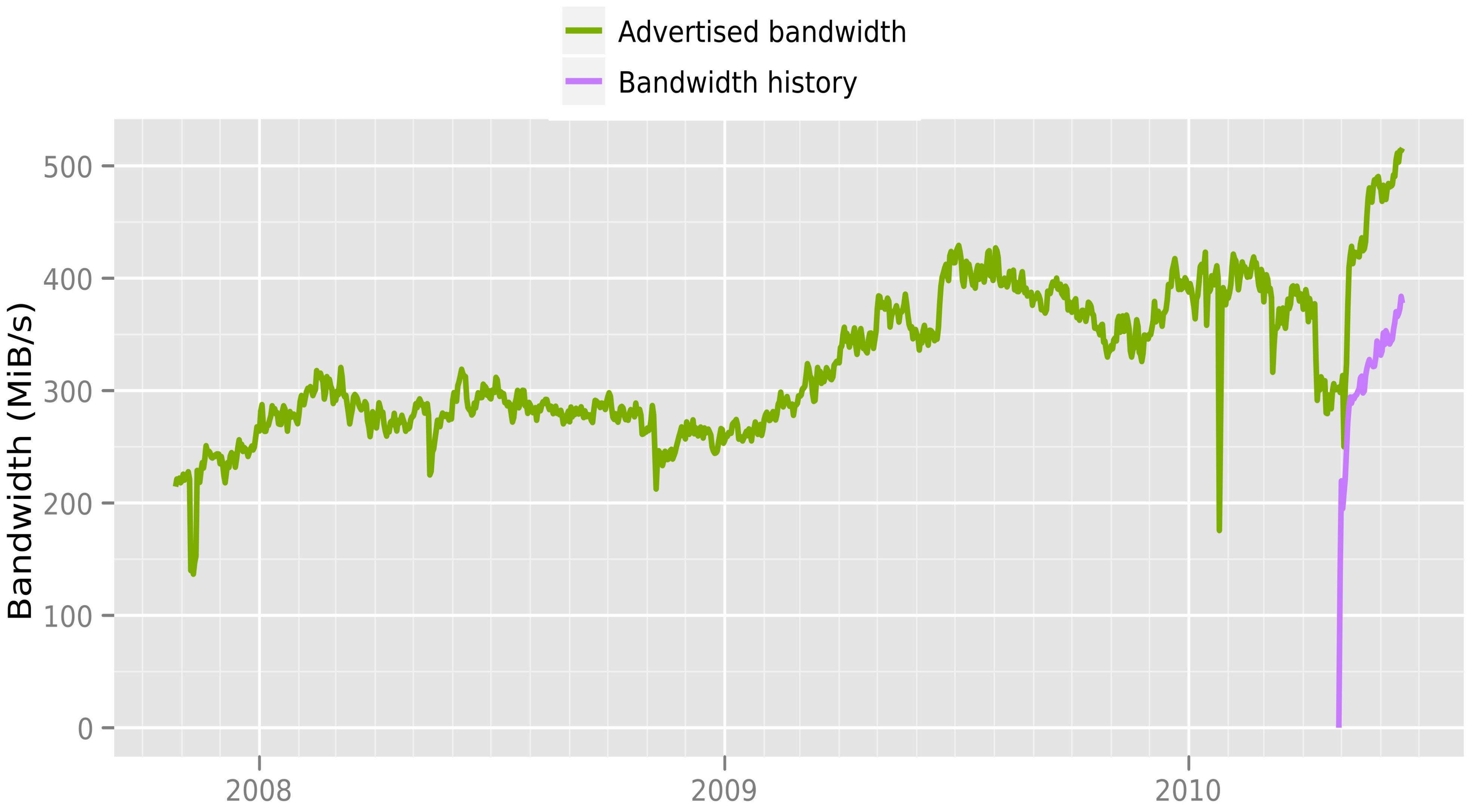
The Tor Project - https://metrics.torproject.org/


Time in seconds to complete 50 KiB request
Measured times on all sources per day
Median
1st to 3rd quartile
25
20
15
10
5
0
Jul-2009
Oct-2009
Jan-2010
Apr-2010
Jul-2010
The Tor Project - https://metrics.torproject.org/

Number of relays

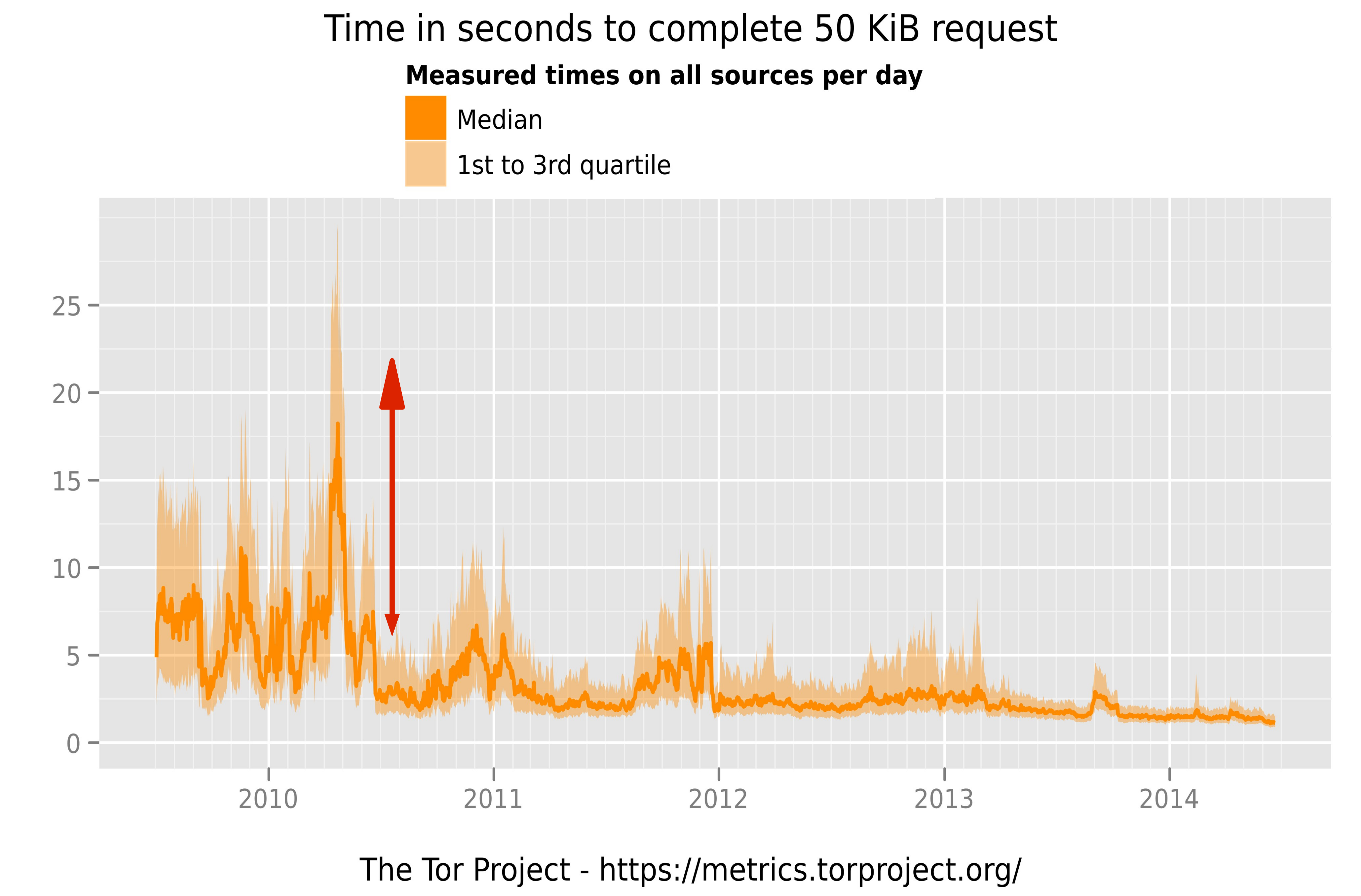


The Tor Project - https://metrics.torproject.org/



Total relay bandwidth

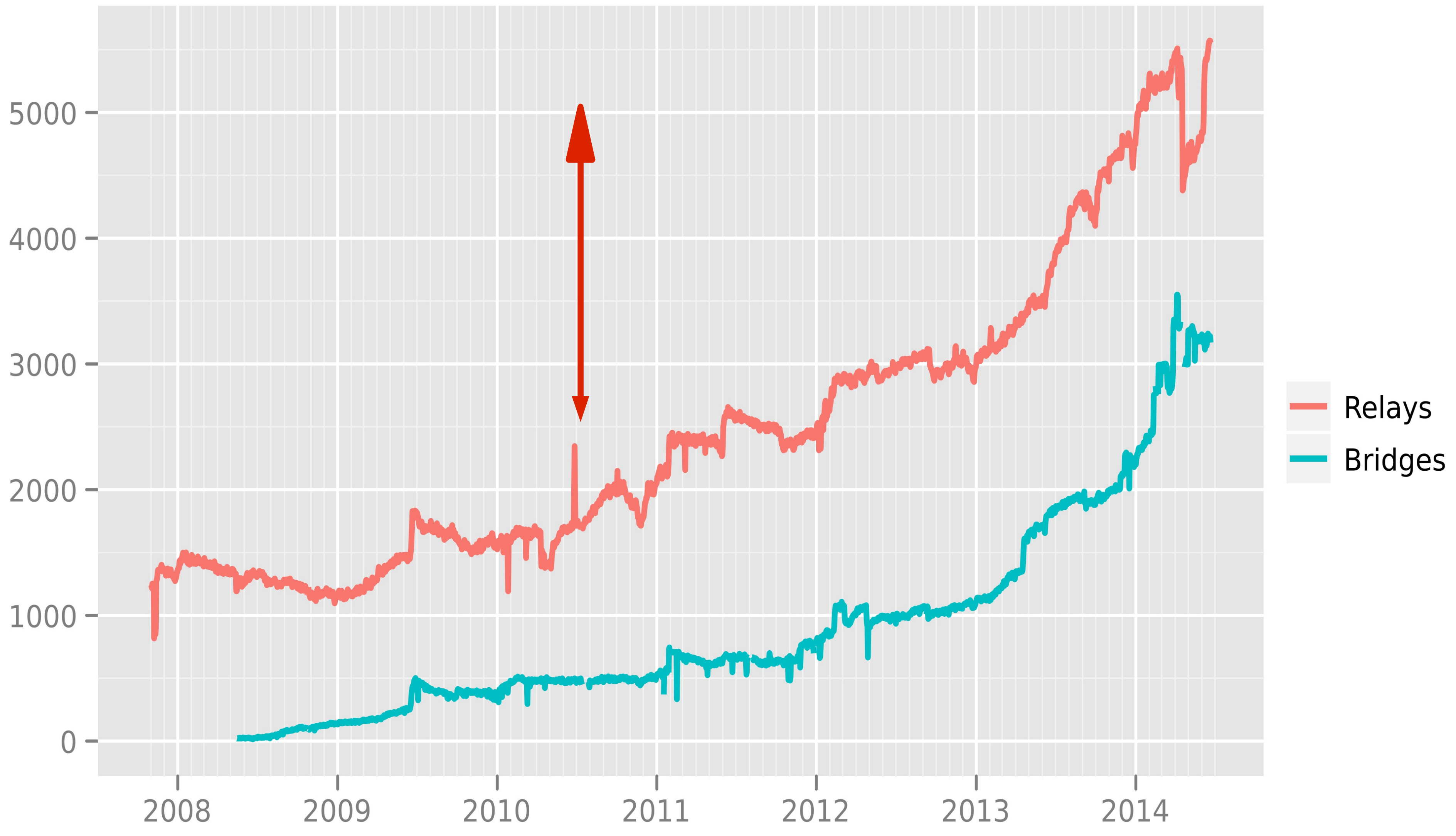
The Tor Project - https://metrics.torproject.org/



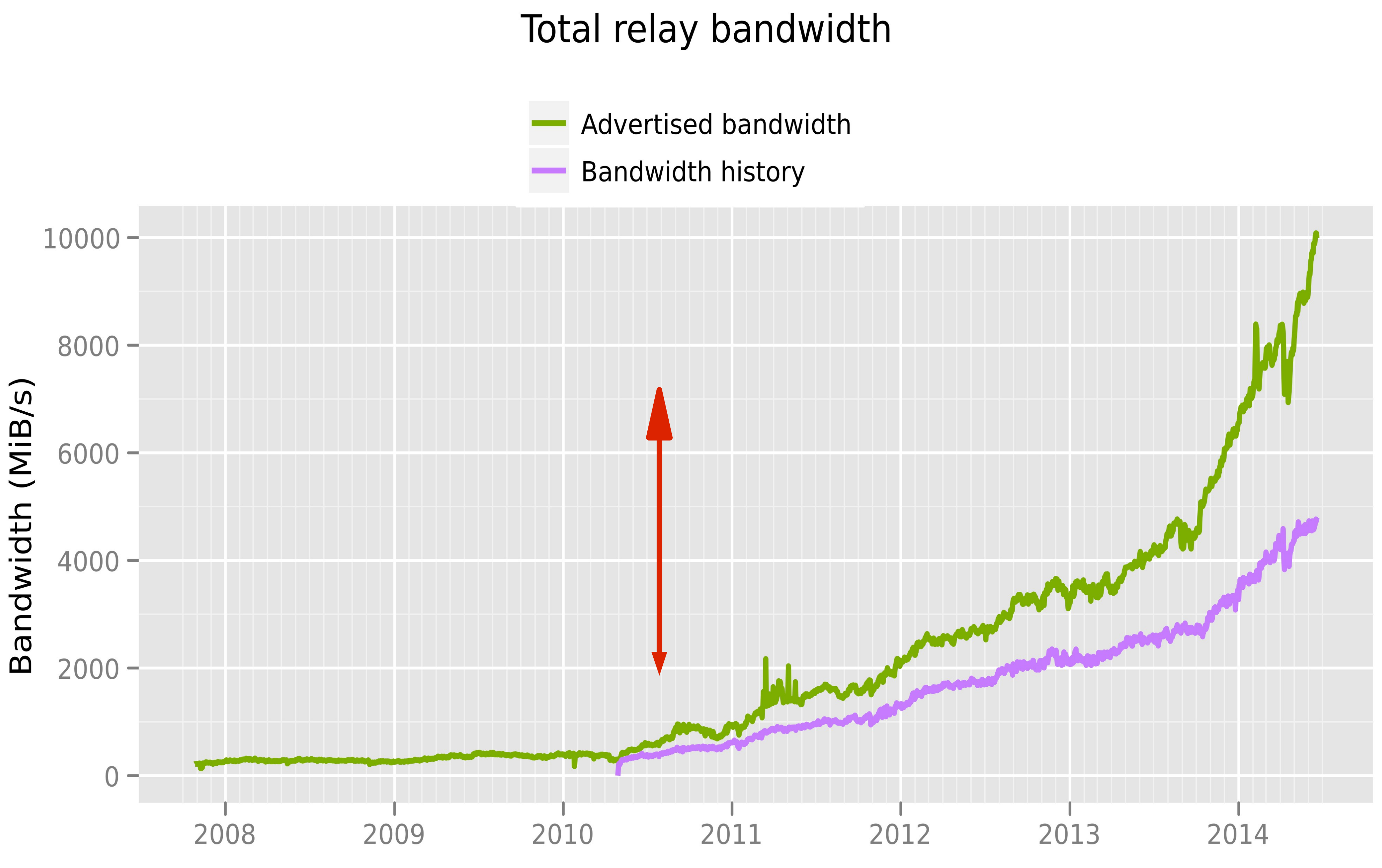
Time in seconds to complete 50 KiB request

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

Number of relays



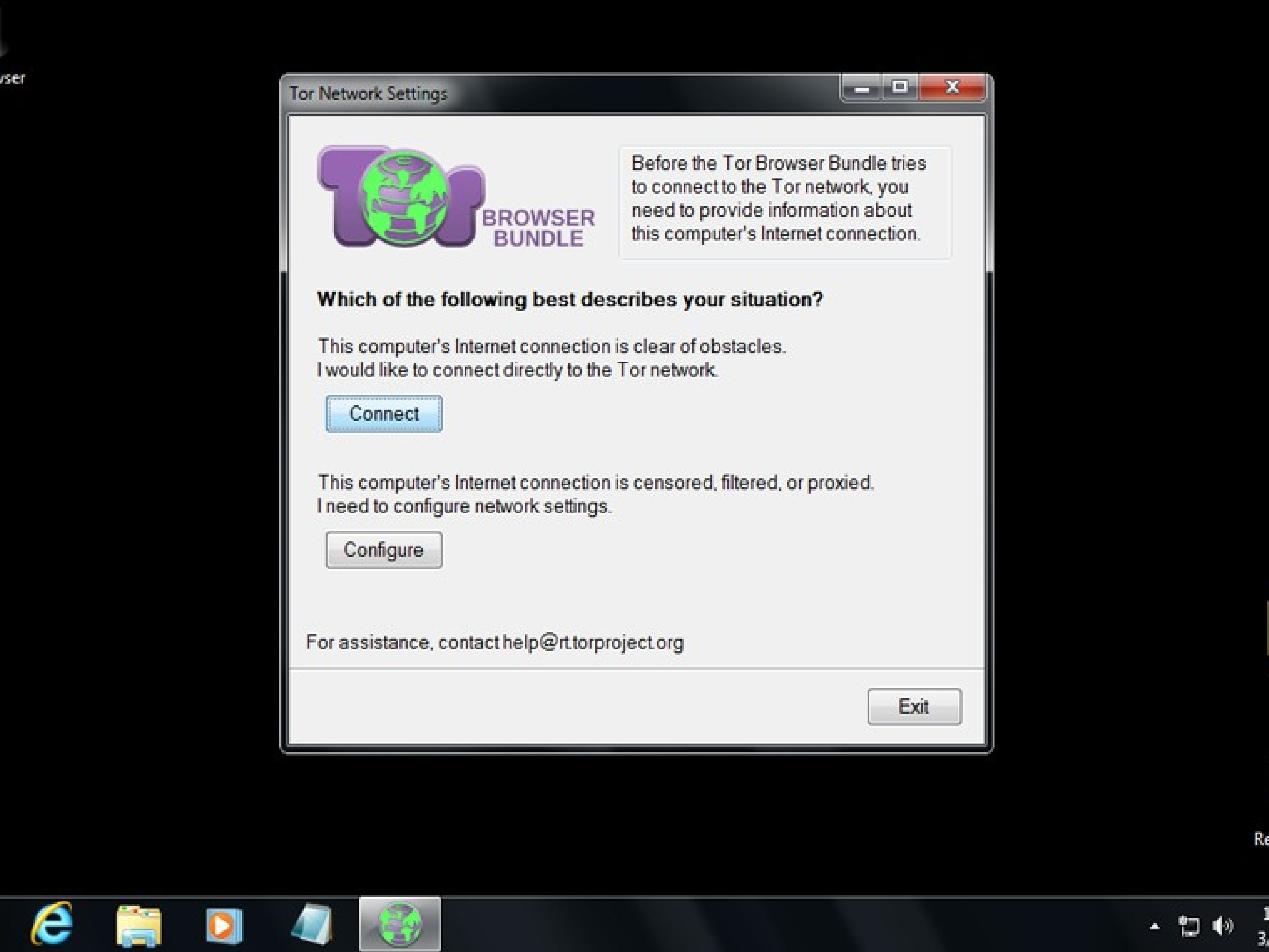
The Tor Project - https://metrics.torproject.org/



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

When we wrote the SAFER proposal

- Iran ran default-config Smartfilter
- China had blocked public Tor relays; vanilla bridges worked great there
- China did stateless regexp on TCP payload
- Tor was blending with SSL, because “who would block SSL”
- Before Tunisia, Egypt, Libya, Syria, ...



Tor Network Settings

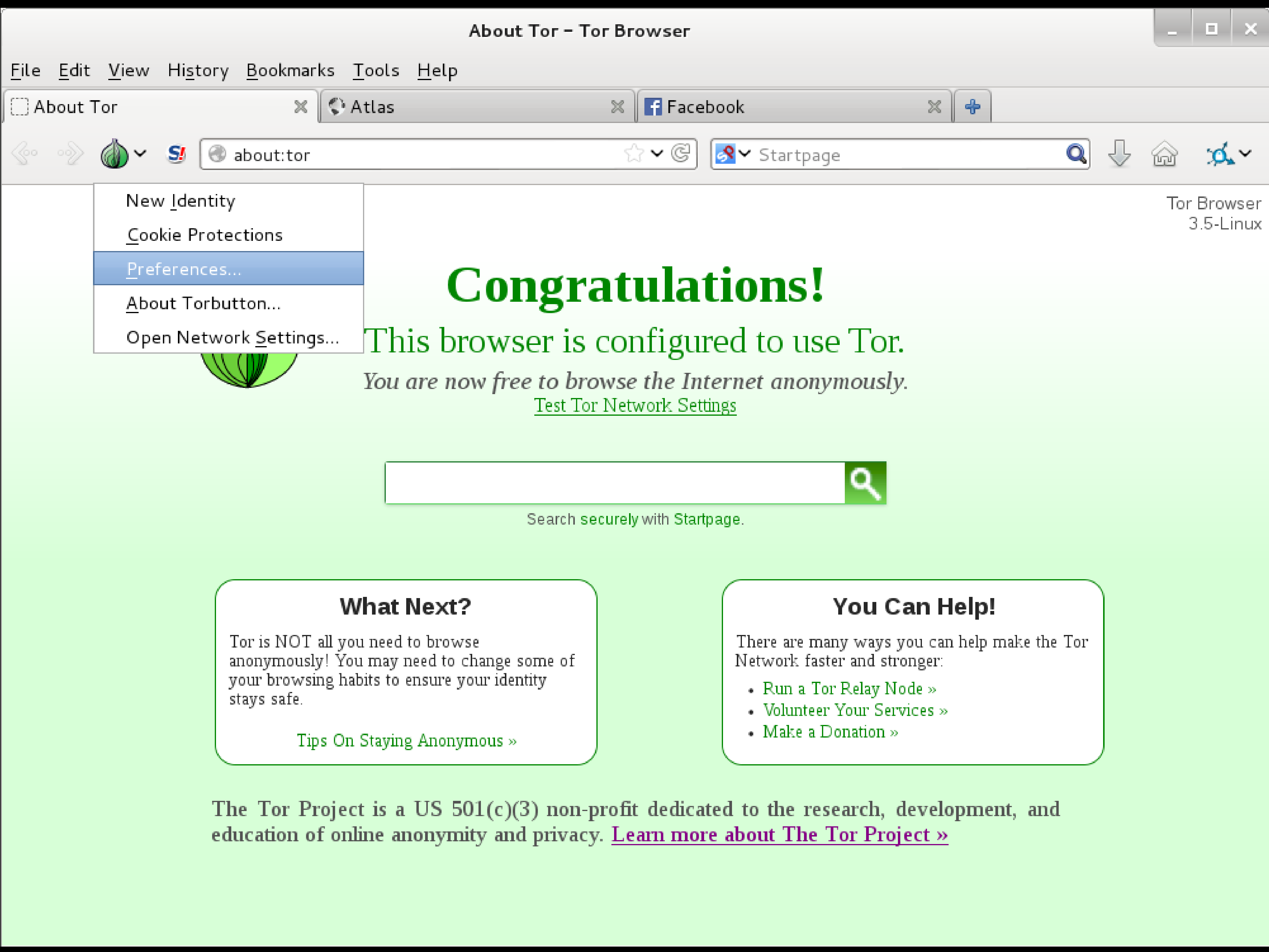
Before the Tor Browser Bundle tries to connect to the Tor network, you need to provide information about this computer's Internet connection.

Which of the following best describes your situation?

This computer's Internet connection is clear of obstacles.
I would like to connect directly to the Tor network.

This computer's Internet connection is censored, filtered, or proxied.
I need to configure network settings.

For assistance, contact help@rt.torproject.org



Congratulations!

This browser is configured to use Tor.

You are now free to browse the Internet anonymously.

Test Tor Network Settings

Search securely with Startpage.

What Next?

Tor is NOT all you need to browse anonymously! You may need to change some of your browsing habits to ensure your identity stays safe.

Tips On Staying Anonymous »

You Can Help!

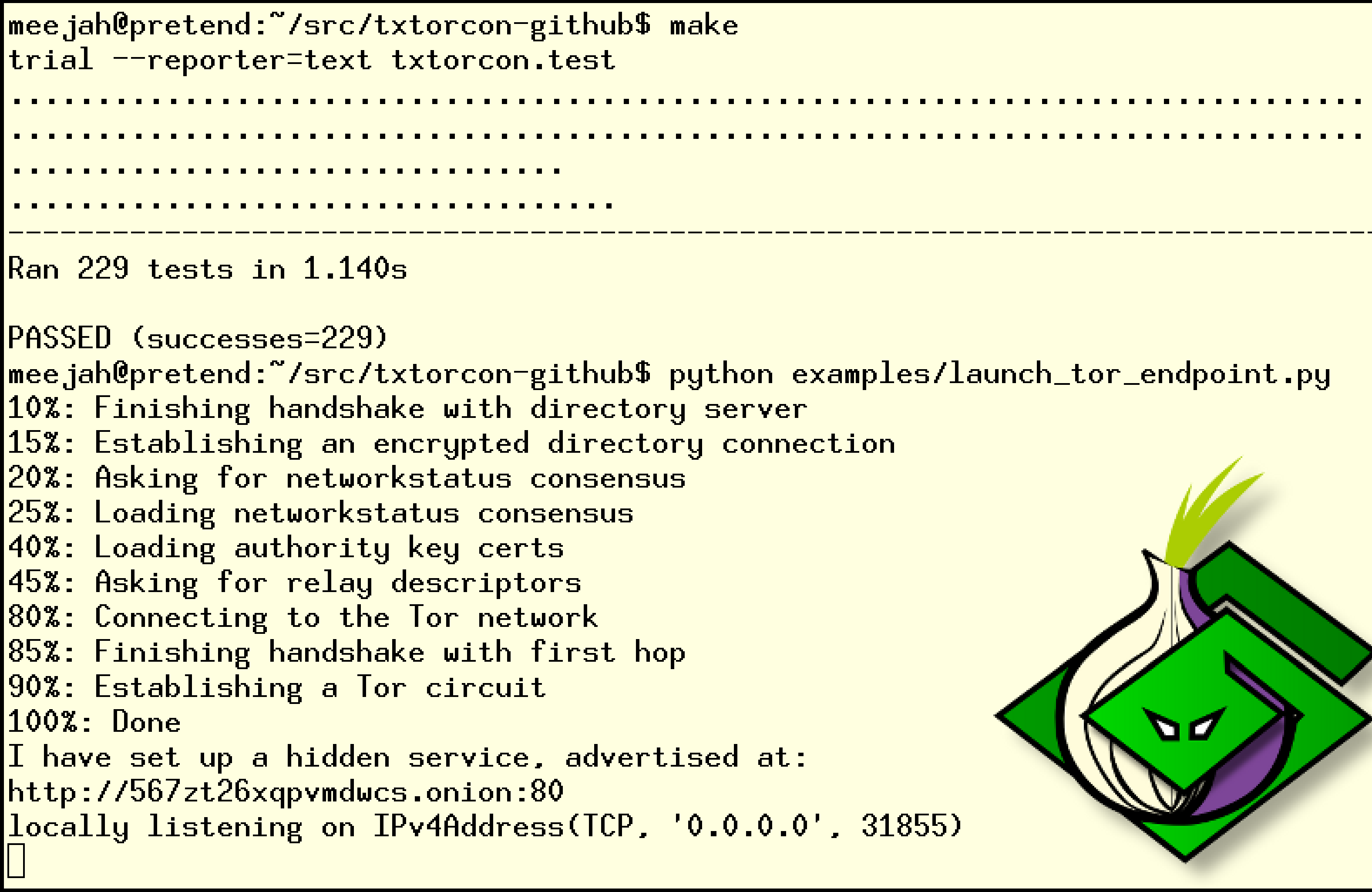
There are many ways you can help make the Tor Network faster and stronger:

- Run a Tor Relay Node »
- Volunteer Your Services »
- Make a Donation »

The Tor Project is a US 501(c)(3) non-profit dedicated to the research, development, and education of online anonymity and privacy. Learn more about The Tor Project »

Tor Controller Interface

- **stem**
- pytorctl
- jtorctl
- **txtorcon**

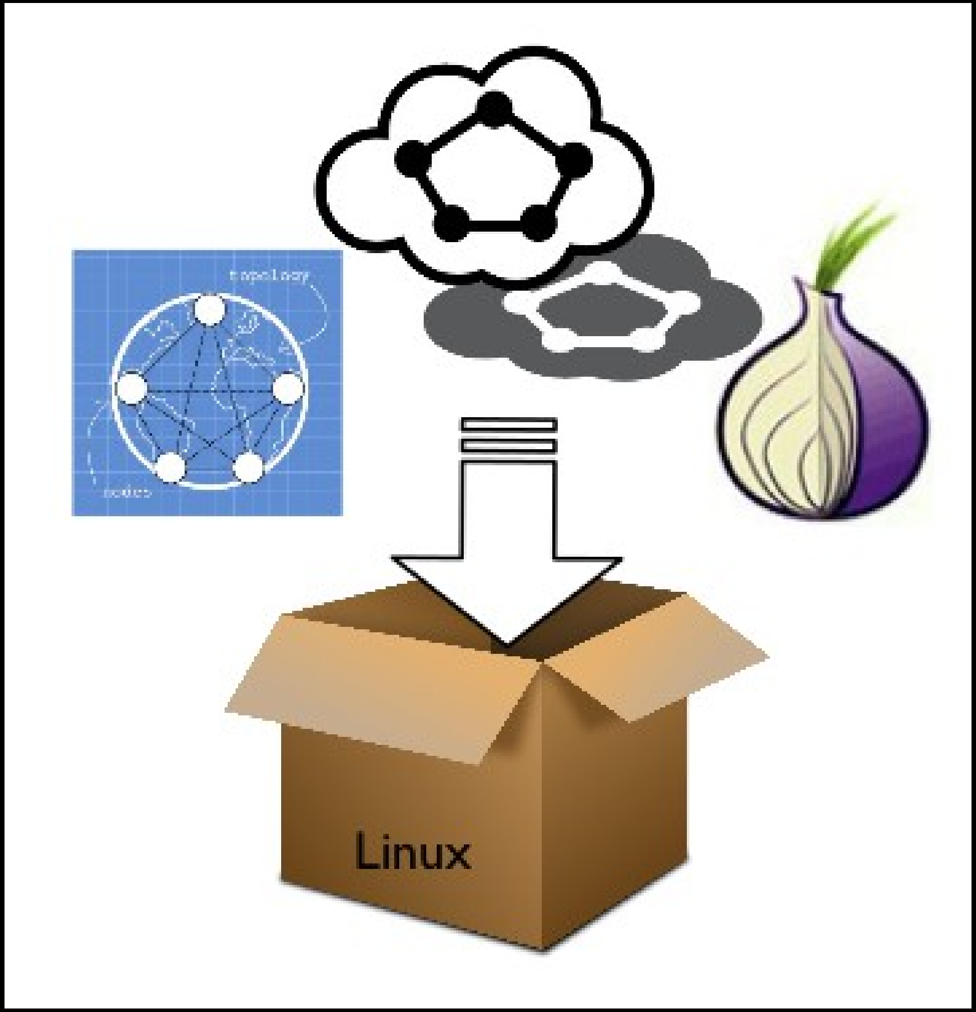


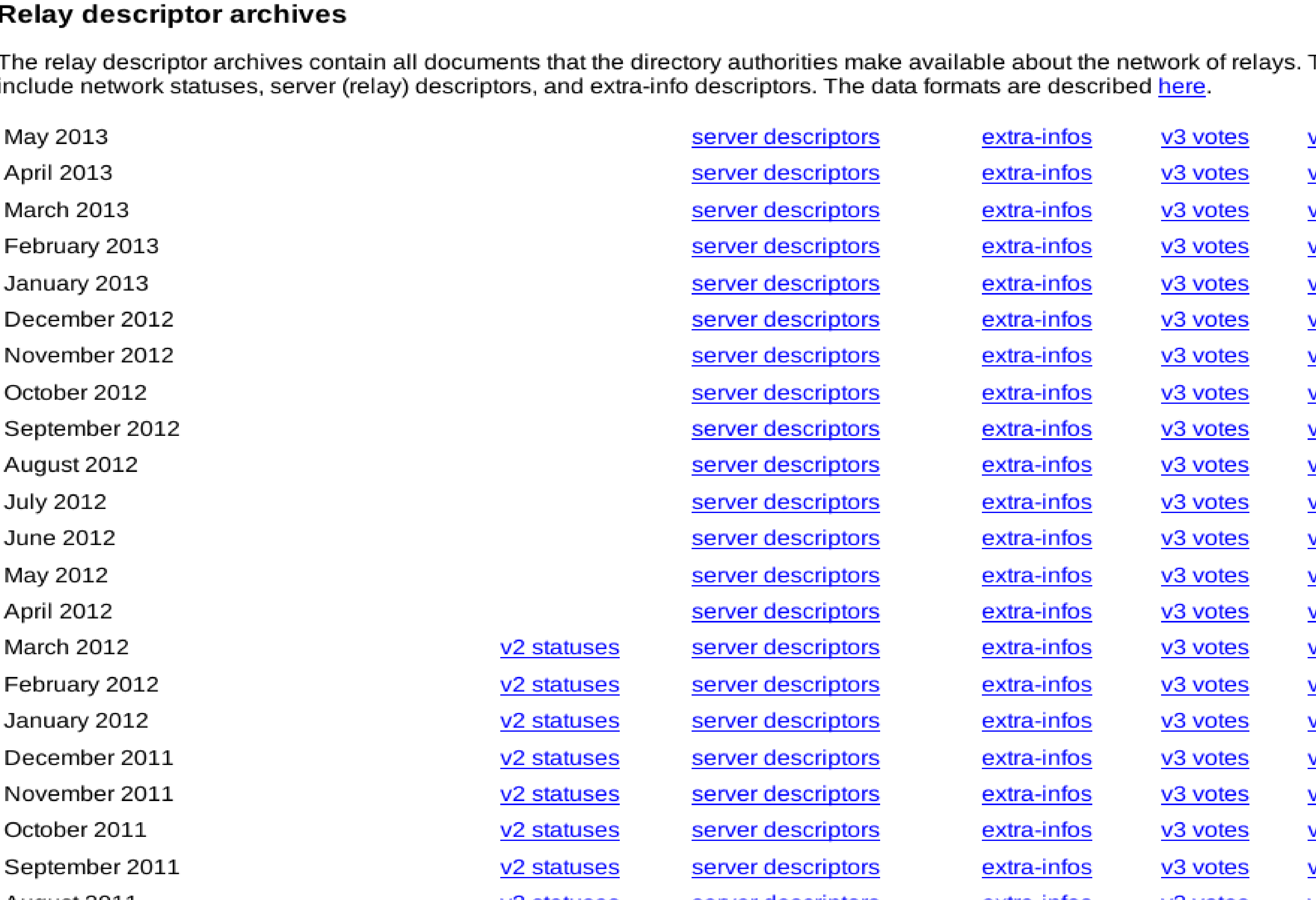
```
meejah@pretend:~/src/txtorcon-github$ make
trial --reporter=text txtorcon.test
..............................................................................
..............................................................................
................................
...................................
------------------------------------------------------------------------------
Ran 229 tests in 1.140s

PASSED (successes=229)
meejah@pretend:~/src/txtorcon-github$ python examples/launch_tor_endpoint.py
10%: Finishing handshake with directory server
15%: Establishing an encrypted directory connection
20%: Asking for networkstatus consensus
25%: Loading networkstatus consensus
40%: Loading authority key certs
45%: Asking for relay descriptors
80%: Connecting to the Tor network
85%: Finishing handshake with first hop
90%: Establishing a Tor circuit
100%: Done
I have set up a hidden service, advertised at:
http://567zt26xqpvmdwcs.onion:80
locally listening on IPv4Address(TCP, '0.0.0.0', 31855)
```

Tor network simulators

- **Shadow**
- ExperimenTor
- **Chutney**
- Puppetor



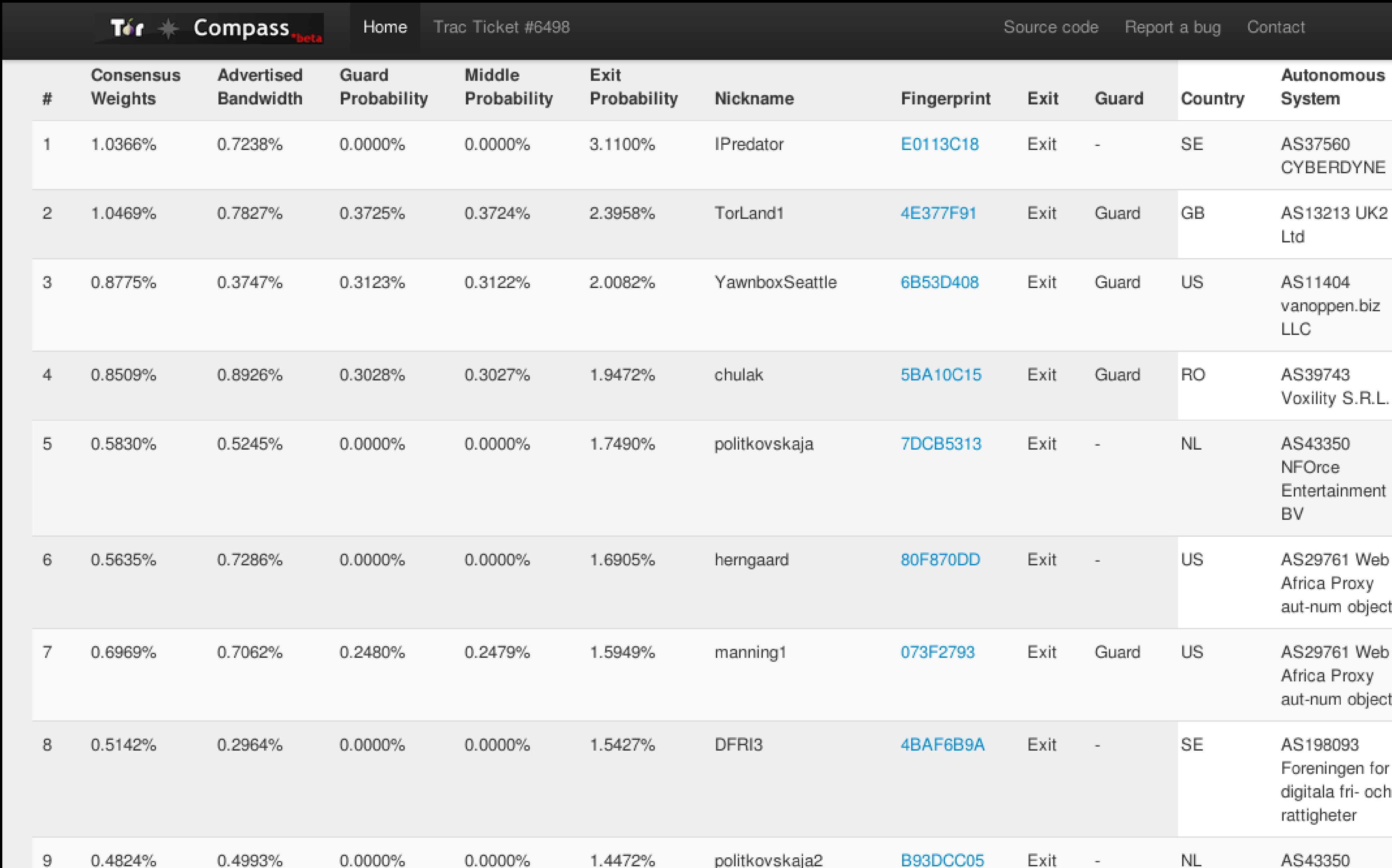


Relay descriptor archives

The relay descriptor archives contain all documents that the directory authorities make available about the network of relays. T include network statuses, server (relay) descriptors, and extra-info descriptors. The data formats are described here.

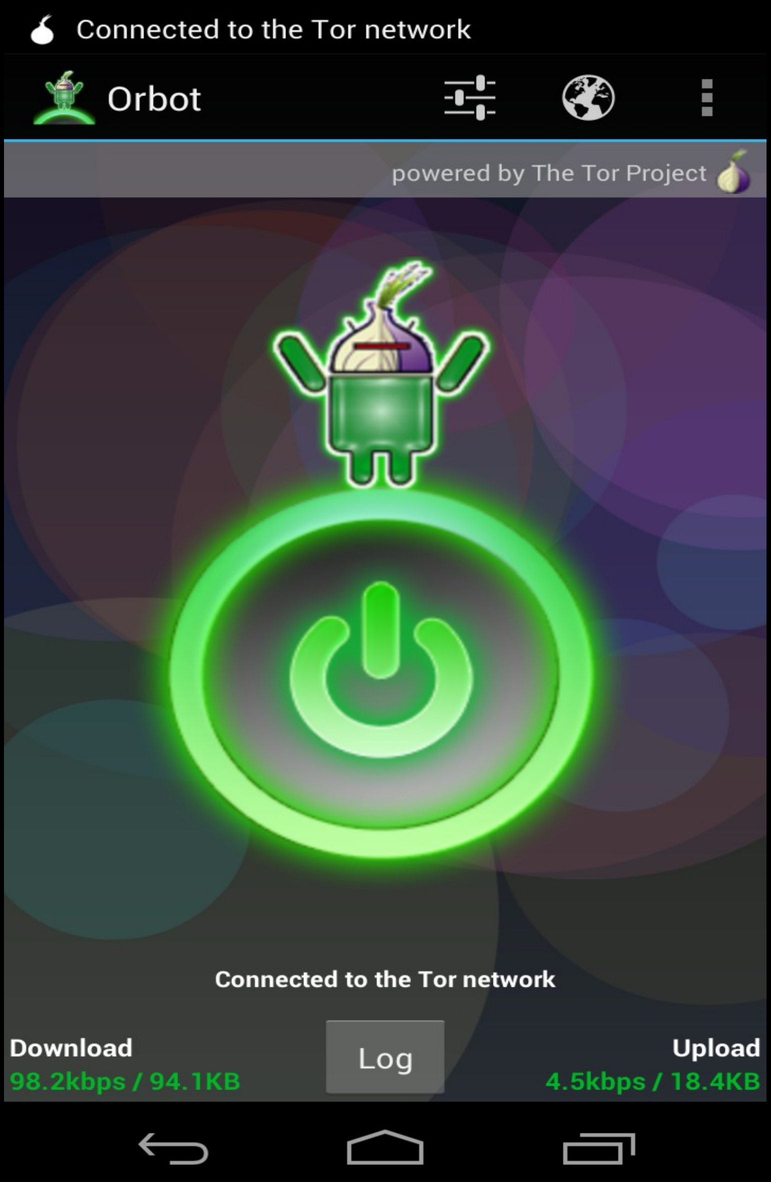
May 2013		server descriptors	extra-infos	v3 votes	v
April 2013		server descriptors	extra-infos	v3 votes	v
March 2013		server descriptors	extra-infos	v3 votes	v
February 2013		server descriptors	extra-infos	v3 votes	v
January 2013		server descriptors	extra-infos	v3 votes	v
December 2012		server descriptors	extra-infos	v3 votes	v
November 2012		server descriptors	extra-infos	v3 votes	v
October 2012		server descriptors	extra-infos	v3 votes	v
September 2012		server descriptors	extra-infos	v3 votes	v
August 2012		server descriptors	extra-infos	v3 votes	v
July 2012		server descriptors	extra-infos	v3 votes	v
June 2012		server descriptors	extra-infos	v3 votes	v
May 2012		server descriptors	extra-infos	v3 votes	v
April 2012		server descriptors	extra-infos	v3 votes	v
March 2012	v2 statuses	server descriptors	extra-infos	v3 votes	v
February 2012	v2 statuses	server descriptors	extra-infos	v3 votes	v
January 2012	v2 statuses	server descriptors	extra-infos	v3 votes	v
December 2011	v2 statuses	server descriptors	extra-infos	v3 votes	v
November 2011	v2 statuses	server descriptors	extra-infos	v3 votes	v
October 2011	v2 statuses	server descriptors	extra-infos	v3 votes	v
September 2011	v2 statuses	server descriptors	extra-infos	v3 votes	v
August 2011	v2 statuses	server descriptors	extra-infos	v3 votes	

compass.torproject.org



#	Consensus Weights	Advertised Bandwidth	Guard Probability	Middle Probability	Exit Probability	Nickname	Fingerprint	Exit	Guard	Country	Autonomous System
1	1.0366%	0.7238%	0.0000%	0.0000%	3.1100%	IPredator	E0113C18	Exit	-	SE	AS37560 CYBERDYNE
2	1.0469%	0.7827%	0.3725%	0.3724%	2.3958%	TorLand1	4E377F91	Exit	Guard	GB	AS13213 UK2 Ltd
3	0.8775%	0.3747%	0.3123%	0.3122%	2.0082%	YawnboxSeattle	6B53D408	Exit	Guard	US	AS11404 vanoppen.biz LLC
4	0.8509%	0.8926%	0.3028%	0.3027%	1.9472%	chulak	5BA10C15	Exit	Guard	RO	AS39743 Voxility S.R.L.
5	0.5830%	0.5245%	0.0000%	0.0000%	1.7490%	politkovskaja	7DCB5313	Exit	-	NL	AS43350 NFOrce Entertainment BV
6	0.5635%	0.7286%	0.0000%	0.0000%	1.6905%	herngaard	80F870DD	Exit	-	US	AS29761 Web Africa Proxy aut-num object
7	0.6969%	0.7062%	0.2480%	0.2479%	1.5949%	manning1	073F2793	Exit	Guard	US	AS29761 Web Africa Proxy aut-num object
8	0.5142%	0.2964%	0.0000%	0.0000%	1.5427%	DFRI3	4BAF6B9A	Exit	-	SE	AS198093 Foreningen for digitala fri- och rattigheter
9	0.4824%	0.4993%	0.0000%	0.0000%	1.4472%	politkovskaja2	B93DCC05	Exit	-	NL	AS43350

Orbot



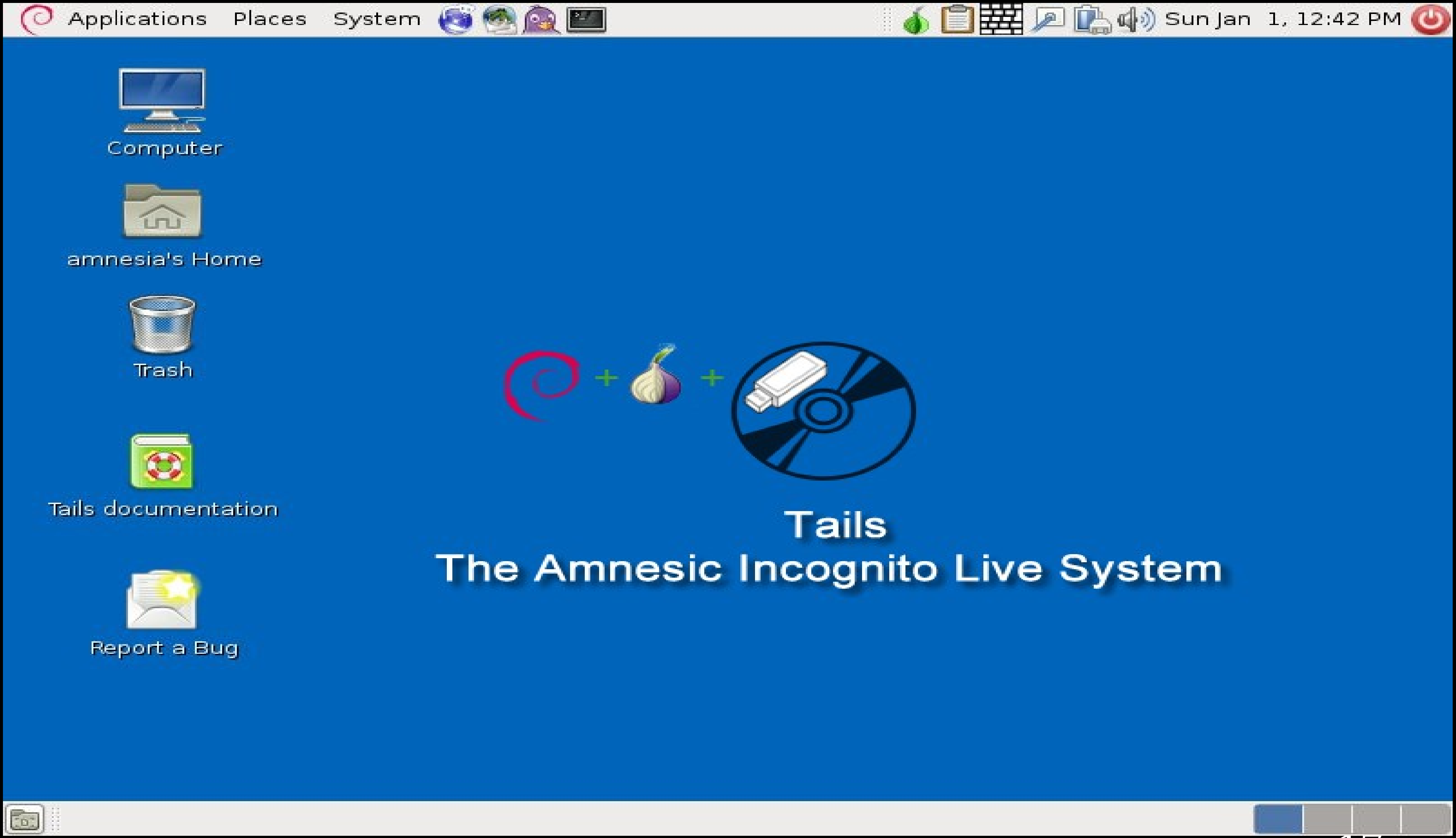
Connected to the Tor network

Connected to the Tor network

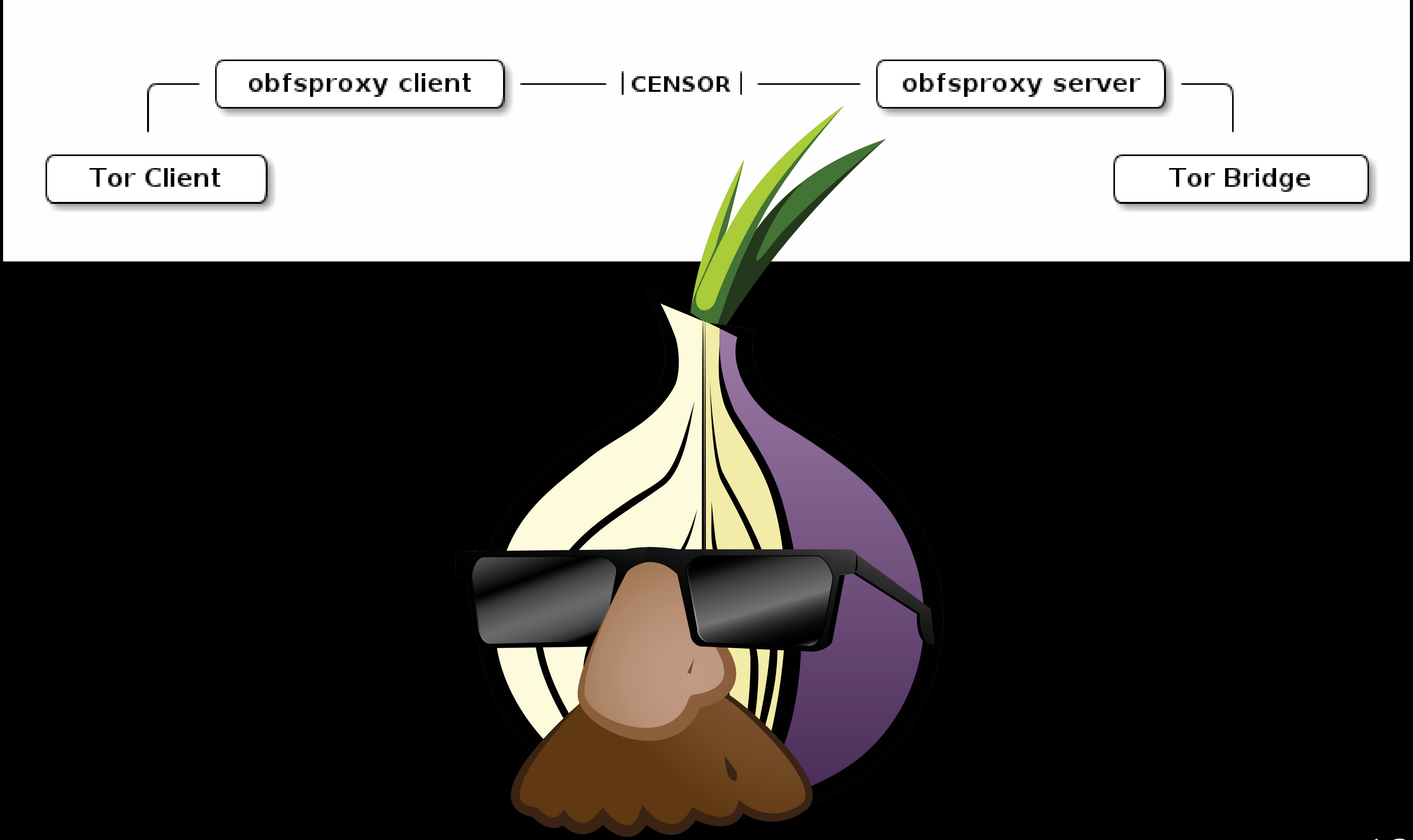
Download
98.2kbps / 94.1KB

Upload
4.5kbps / 18.4KB

Tails LiveCD



Pluggable transports



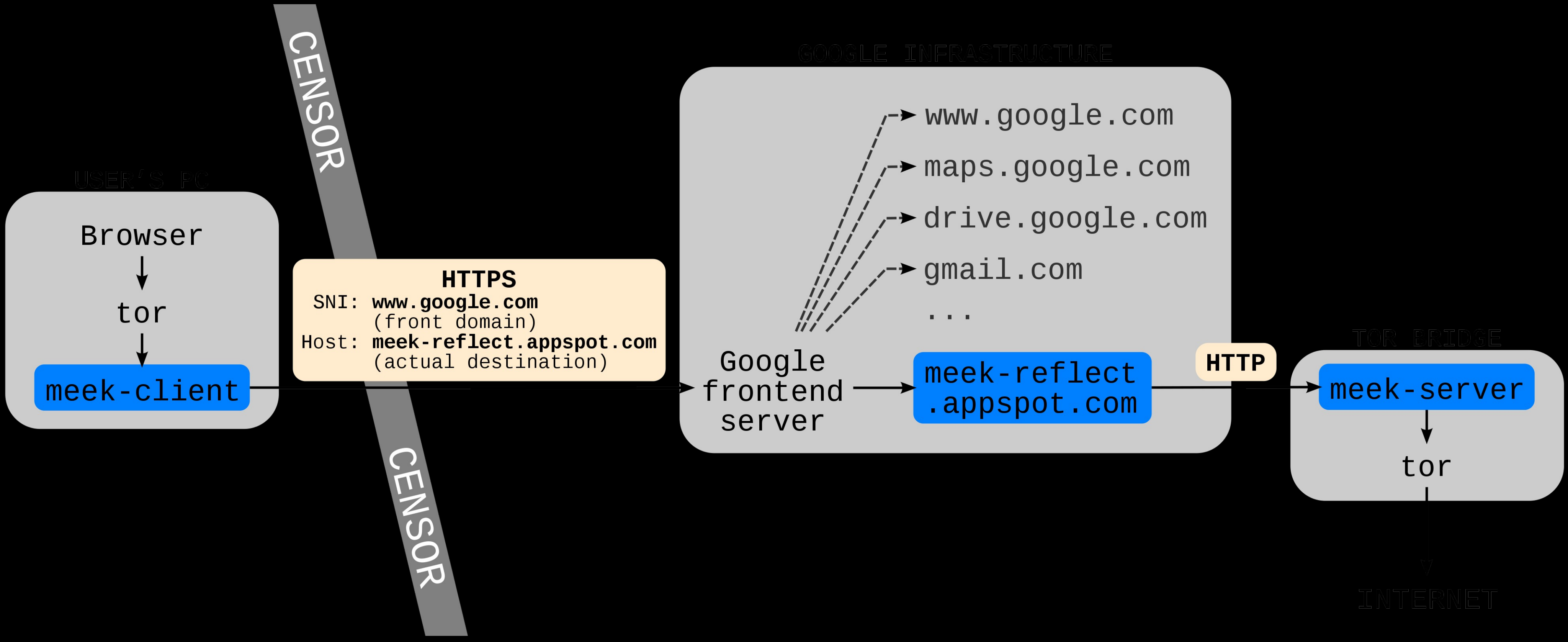
Tor Client

obfsproxy client

|CENSOR|

obfsproxy server

Tor Bridge



HTTPS

```
 SNI: www.google.com
      (front domain)
Host: meek-reflect.appspot.com
      (actual destination)
```

“Fronting”

- Google
- Amazon S3
- Cloudflare
- Akamai

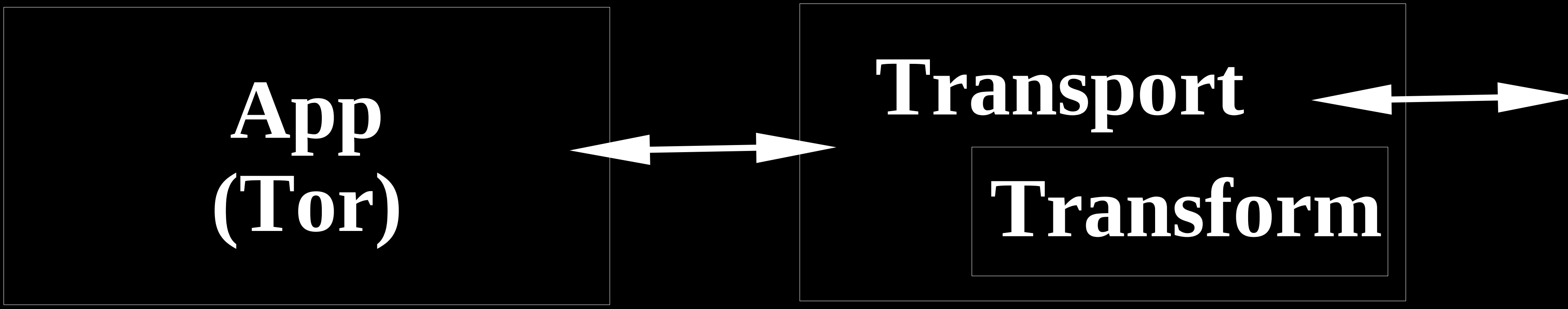
Obfs4

- Obfs3 used UniformDH, CTR-AES256, HMAC-SHA256
- Obfs4 uses Curve25519, Elligator2, HMAC-SHA256, XSalsa20/Poly1305, Siphash
- Go, C++, Python implementations (so all the Orbot users in Turkey can use it)

uProxy

- Google + UW collaboration
- Discovery: Google Plus contacts
  - But only one hop away (abuse)
- Transport: WebRTC (udp + sctp)

Composing and layering

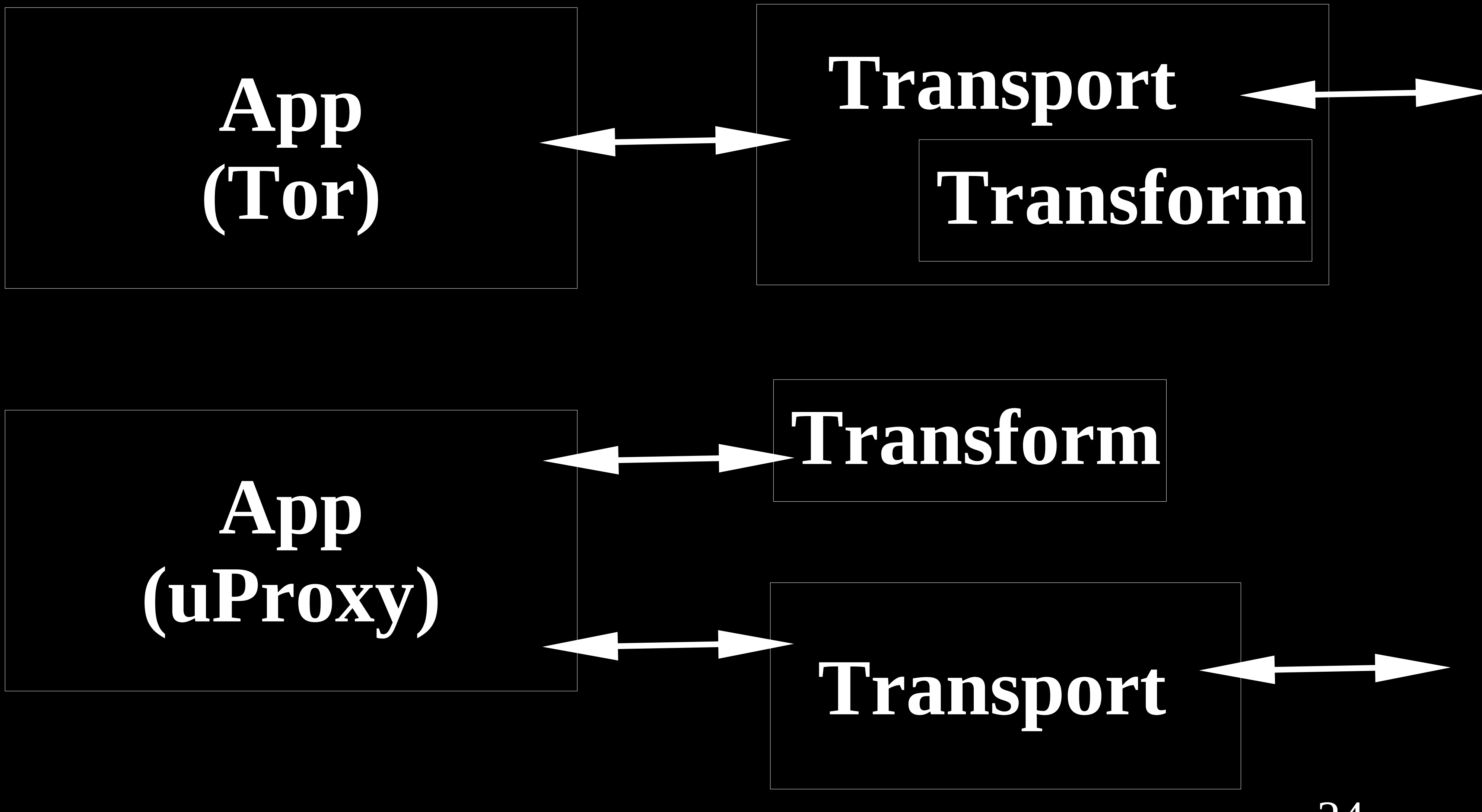


App
(Tor)

Transport

Transform

Composing and layering



App
(Tor)

Transport

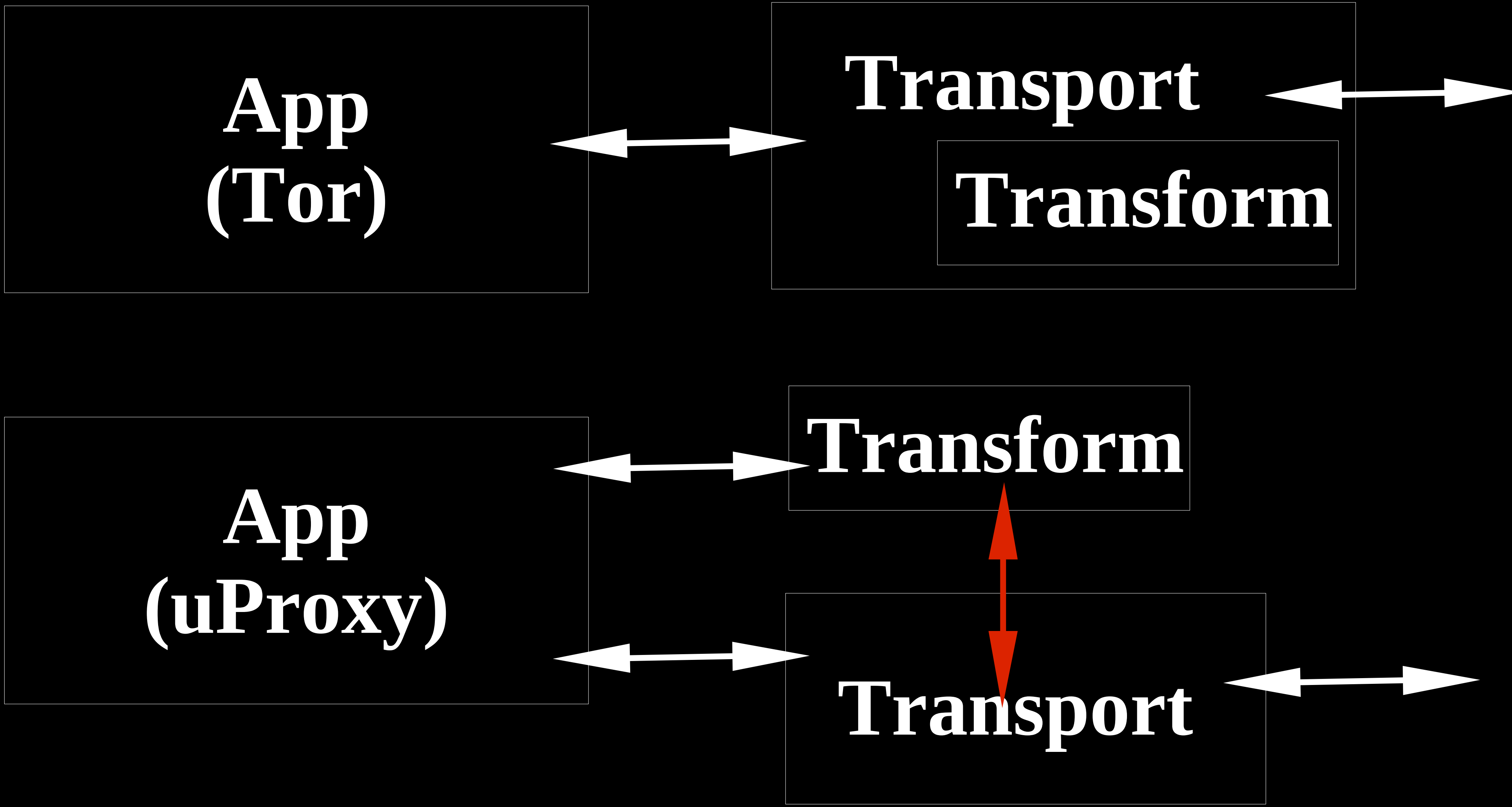
Transform

App
(uProxy)

Transform

Transport

Composing and layering



App
(Tor)

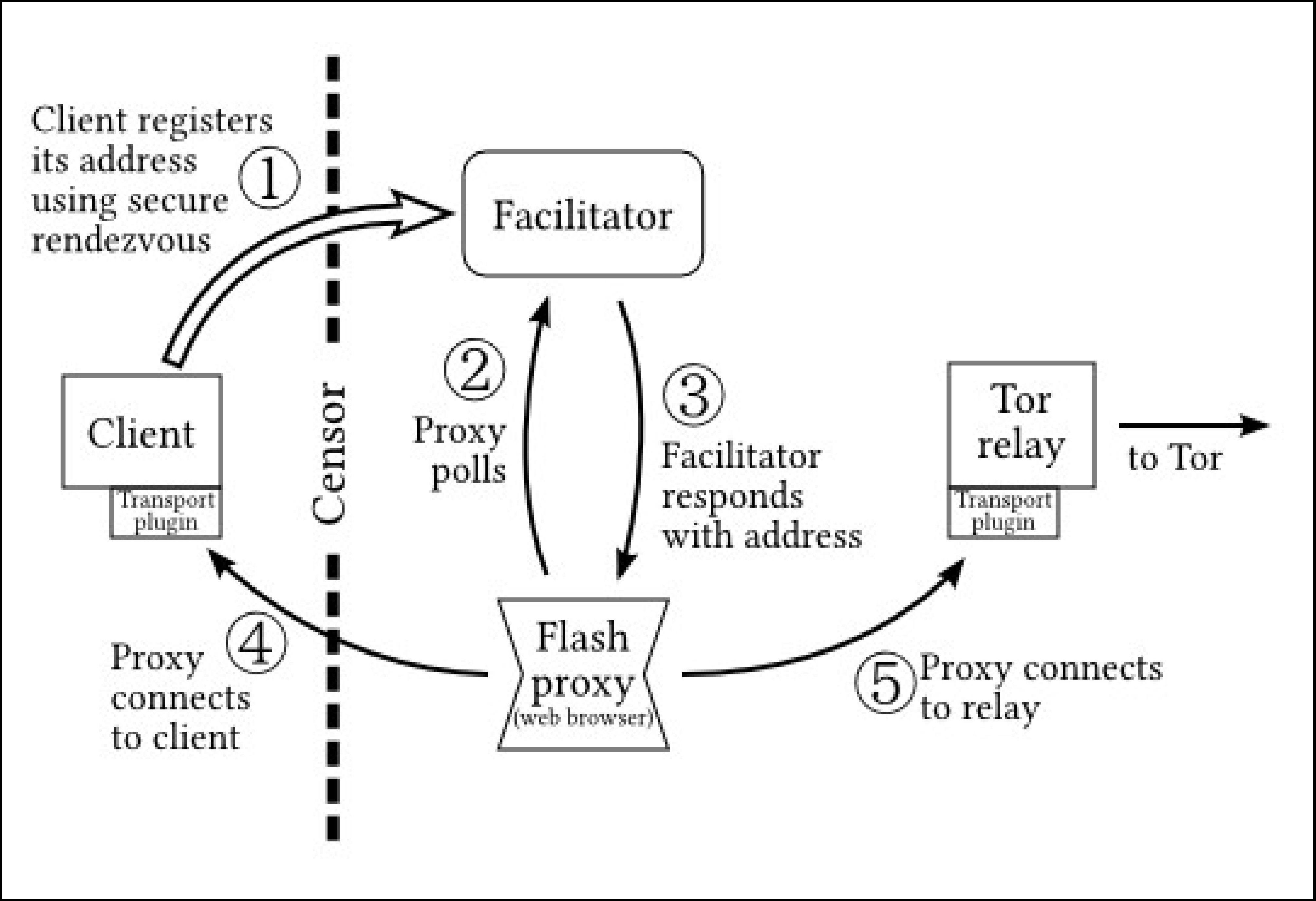
Transport

Transform

App
(uProxy)

Transform

Transport


Client registers its address using secure rendezvous
1
Facilitator
2
Proxy polls
3
Facilitator responds with address
Client
Transport plugin
Censor
Tor relay
Transport plugin
to Tor
4
Proxy connects to client
Flash proxy
(web browser)
5
Proxy connects to relay

Two paradigms

- “Look like nothing”
- “Look like something they expect”

- Active probing: what should your service look like if the client doesn't auth right?
- “Be not there” vs “Be innocent service”

Criteria for judging Pts (1)

How reviewed / reviewable is it?

- 1) Is the software published? Is it entirely free / open source? (~~Skype~~, ~~Windows~~)
- 2) Published design doc, w/ threat model? Spec? How much peer review?
- 3) What is its deployment history? Past publicity, number of users, etc.

Criteria for judging Pts (2)

Evaluation of design

- 4) How difficult/expensive will it be to block (by protocol, by endpoints, etc)
- 5) What anonymity impacts does it have?
- 6) What's the bandwidth overhead?
- 7) How does it fare against active probing?

Criteria for judging Pts (3)

Evaluation of implementation

- 8) Does it use Tor's PT API already?
- 9) Cross-platform, including mobile?
- 10) How easy is the build process? Includes dependencies, deployment scale
- 11) Is the code secure and maintainable?

Measurement Lab / Adversary Lab

- We need a set of benchmarks (“Iran 2011”) to test against – real attacks that we want to know how a given design fares against
- Background traffic issue
- Assessment needs to describe attributes, not conclusions. “China can't block this” vs “An adversary who does X would choose not to block this”

Measurement Framework

Need to extend the framework to include:

- Probing / active attacks
  - We need probe vectors! Skype connections, web connections, Tor connections, etc
- Pass traffic through transparent proxies

OONI:
Measuring interference in the wild

- Measuring censorship of destinations and protocols
- But just as importantly, preemptively tracking which protocols work where

Discovering blocking rules

- Imagine you have a trace that gets blocked, and a trace that doesn't get blocked
- And you can generate new traces and I'll classify them for you
- “Active learning” from ML literature

Techniques to slow down learning: take the feedback out of the loop

- China only samples traffic during periods of high load, so it misses some
- Censorship triggers a ten minute black hole
- DPI triggers active probing later
- Throttling makes classification fuzzy
- Is your vantage point representative?

Other outstanding issues: GetTor

- How to fetch Tor browser if torproject.org is blocked?
- Easy, but: how do you verify the signature?
- Easy, but: how do you download gnupg?
- Satori uses browser extension to check sigs, https github/S3/etc to fetch software

Three ways to destroy Tor

- 1) Legal / policy attacks
- 2) Make ISPs hate hosting exit relays
- 3) Make services hate Tor connections
  - Yelp, Wikipedia, Google, Skype, …
- #3 is getting worse due to centralization (Akamai, Cloudflare) and to outsourcing blacklists

Anonymity analysis

- The Internet is more centralized than we'd like
- Guard churn issue is huge
- Website fingerprinting not such a big deal due to false positives at scale?
- Application-level security still key

“Still the King of high secure,
low latency Internet Anonymity”

Contenders for the throne:

- None