

Do You See What I See?

Differential Treatment of Anonymous Users

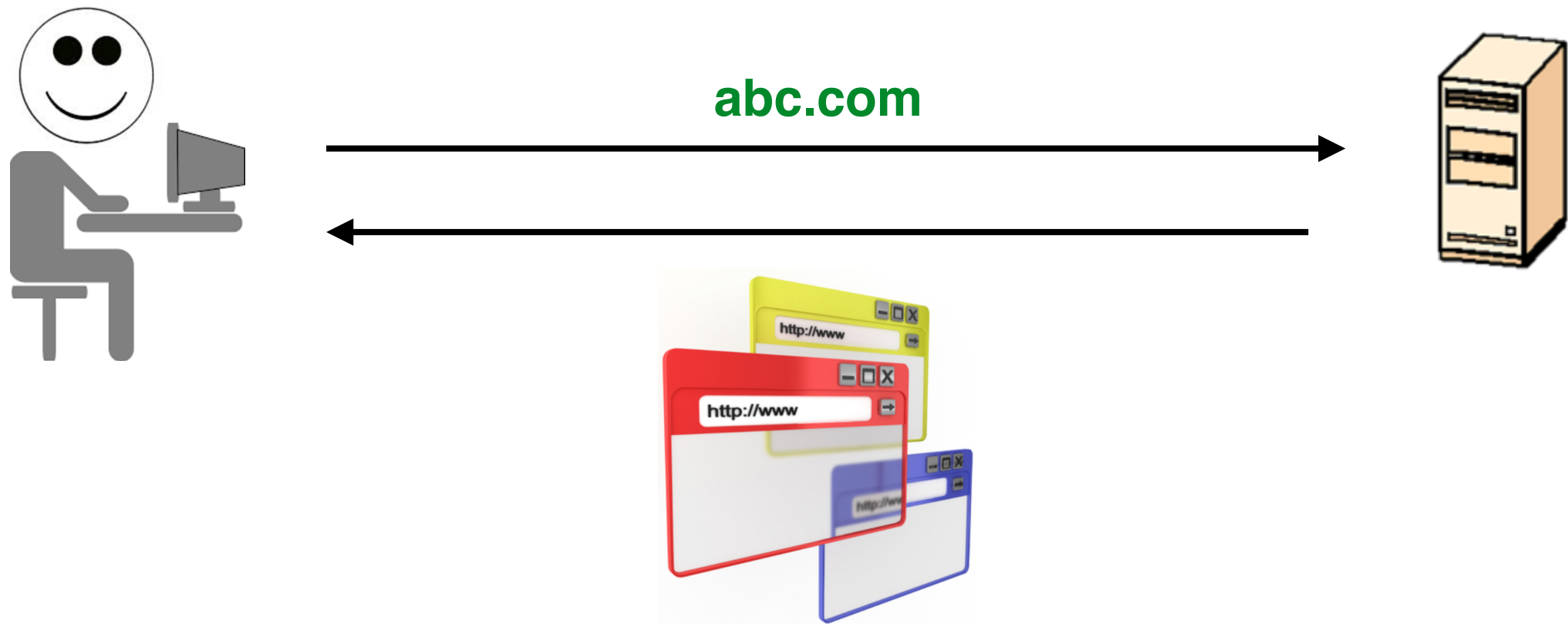
David Fifield (UC Berkeley)
Sadia Afroz (ICSI)

Sheharbano Khattak (University of Cambridge)
Mobin Javed (UC Berkeley)
Srikanth Sundaresan (ICSI)
Vern Paxson (UC Berkeley, ICSI)
Steven J. Murdoch (University College London)
Damon McCoy (NYU)

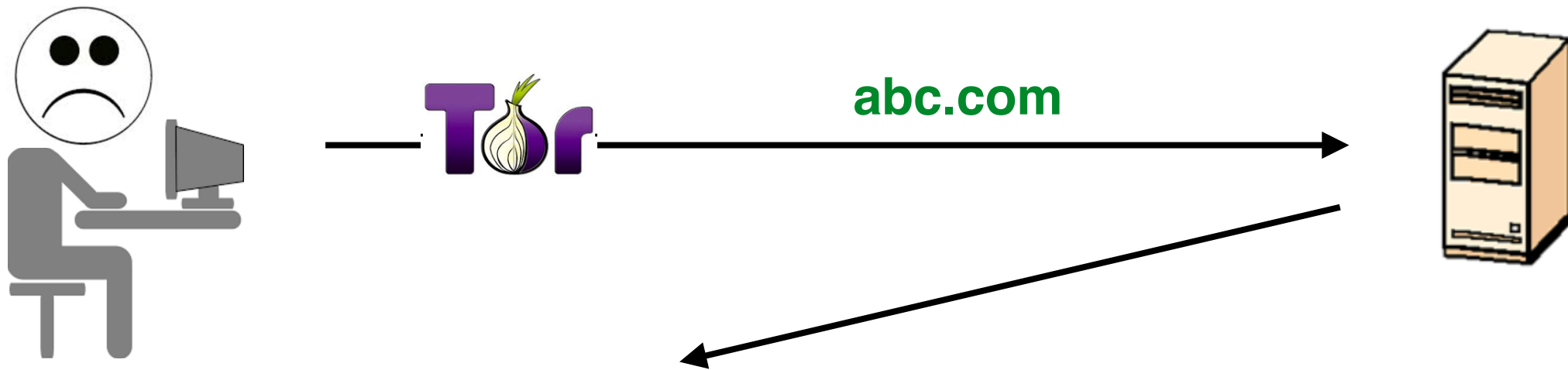


Modified from "Humanist Night" by Munguia

How **Regular** Users See the Web



How Tor Users See the Web



Access Denied

You don't have permission to access "http://www.foxnews.com/" on this server.

Reference #18.4d6e5668.1445538492.20b9c5ab

Error 403

Access denied. Your IP address [171.25.193.132] is blacklisted. If you feel this is in error please contact your hosting providers abuse department.

We're sorry, but we could not fulfill your request for / on this server.

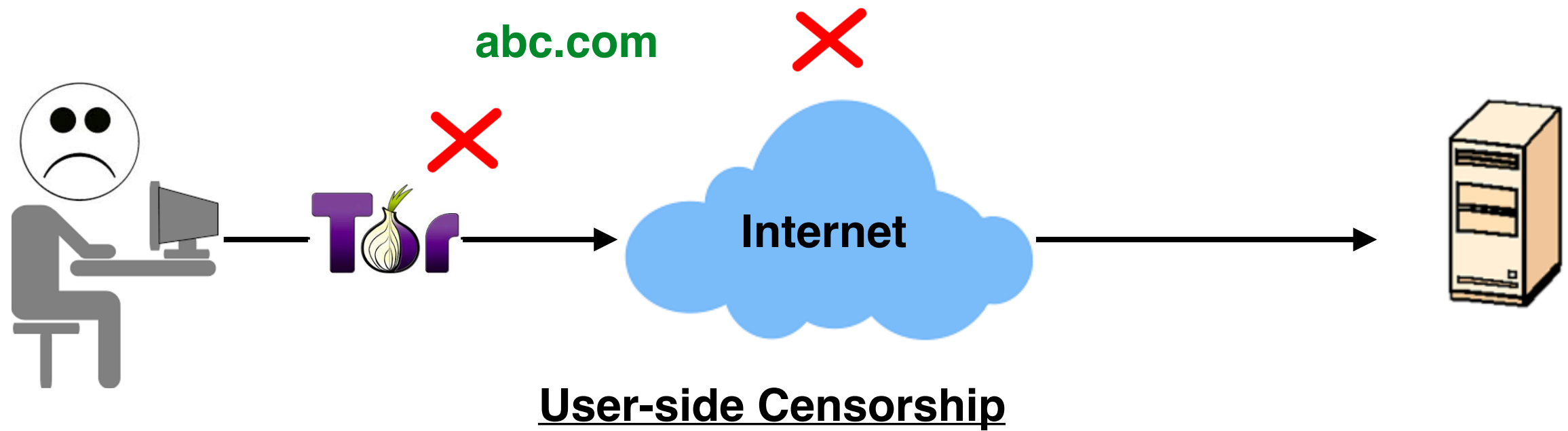
You do not have permission to access this server. Before trying again, run anti-virus and anti-spyware software and remove any viruses and spyware from your computer.

Your technical support key is: **591f-3905-2b02-1b1f**

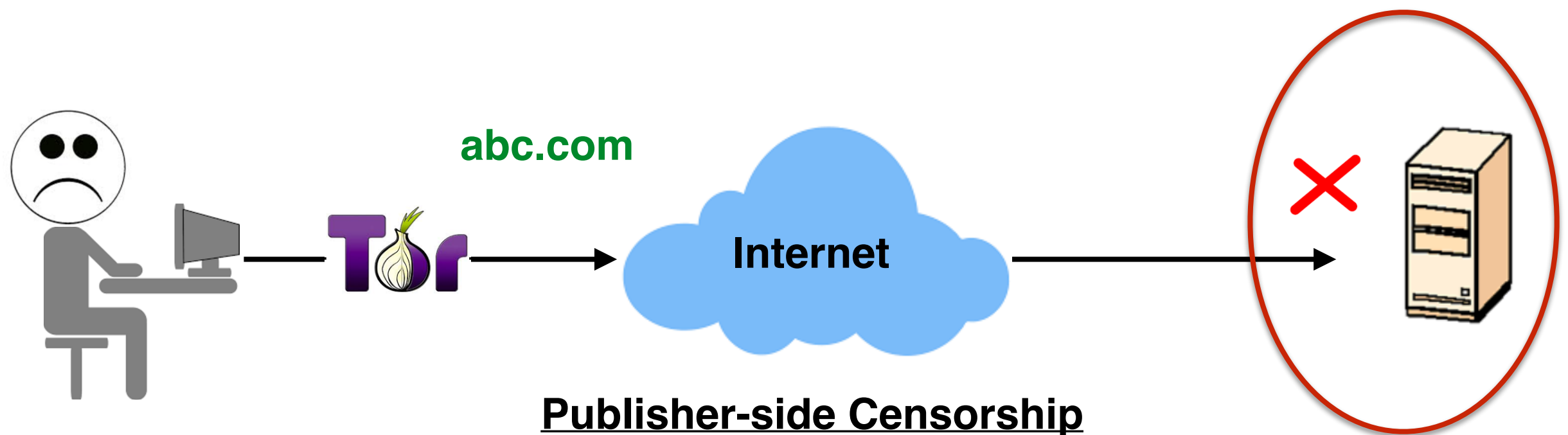
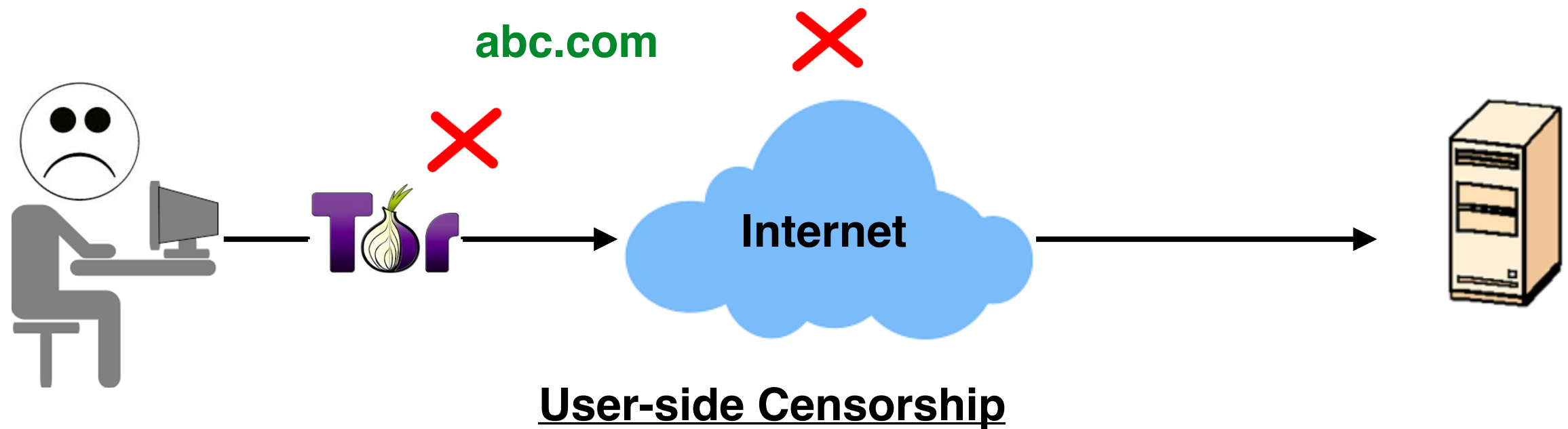
You can use this key to [fix this problem yourself](#).

If you are unable to fix the problem yourself, please contact [webmaster at monticello.org](mailto:webmaster@monticello.org) and be sure to provide the technical support key shown above.

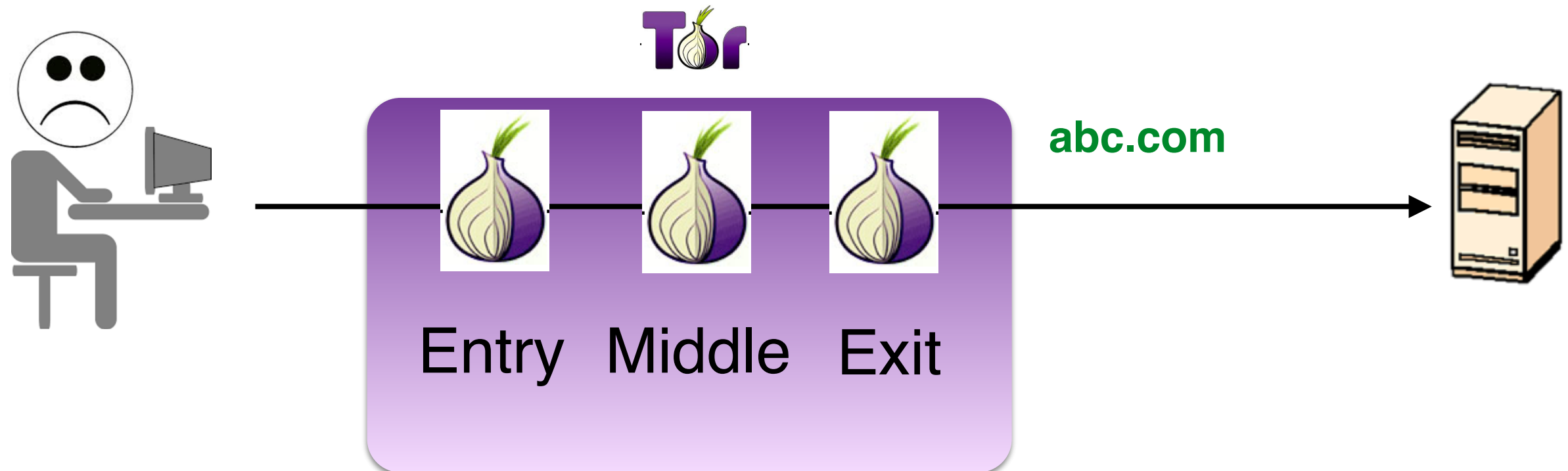
Difference w/ Traditional Censorship



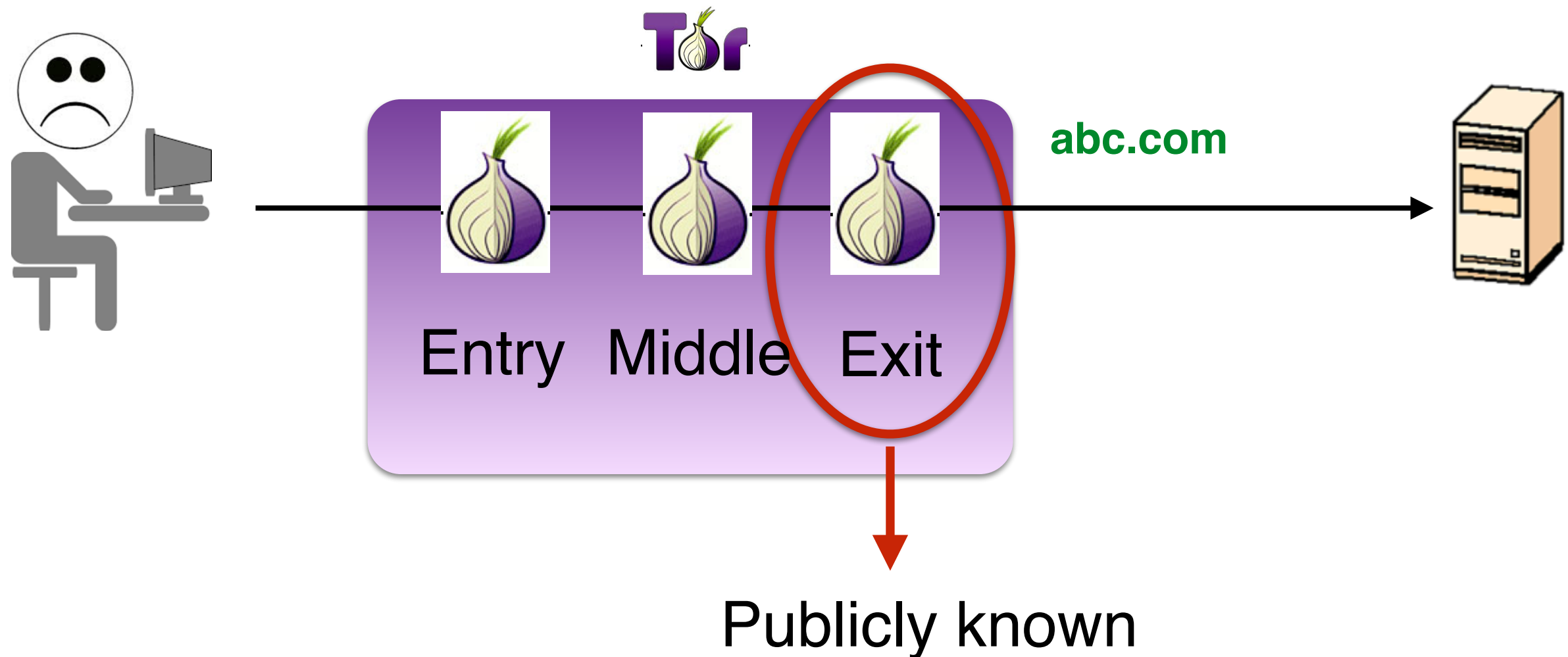
Difference w/ Traditional Censorship



How Do Websites Block Tor?



How Do Websites Block Tor?



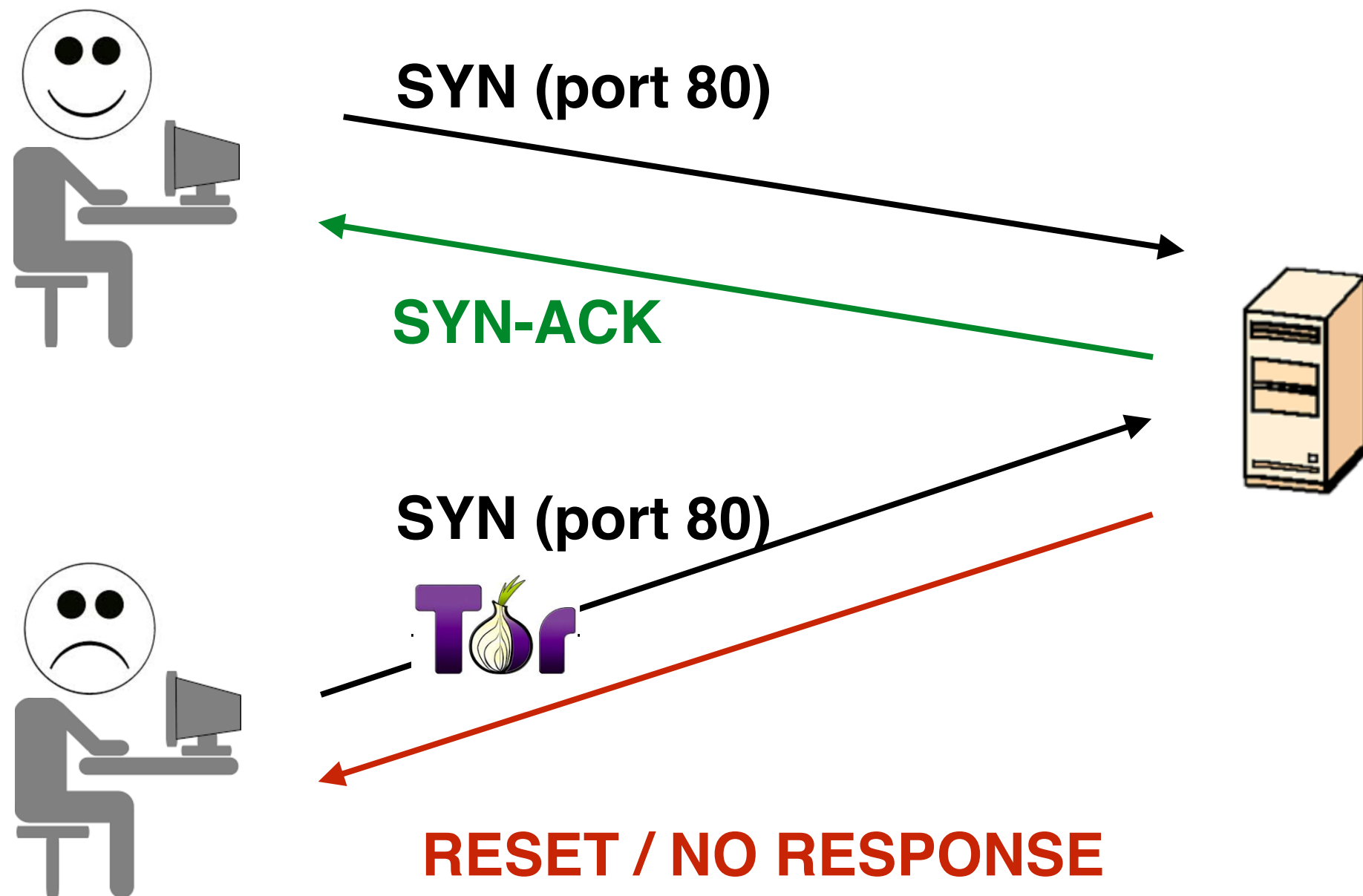
(<https://check.torproject.org/exit-addresses> for example.)

Measuring Tor Blocking by the Web

- Network layer blocking
- Application layer blocking
- Blocking over time (OONI)

Network-layer Discrimination

Does An IP Address Block Tor?



Measuring Tor Blocking at Scale



Scan IPv4

Control Node



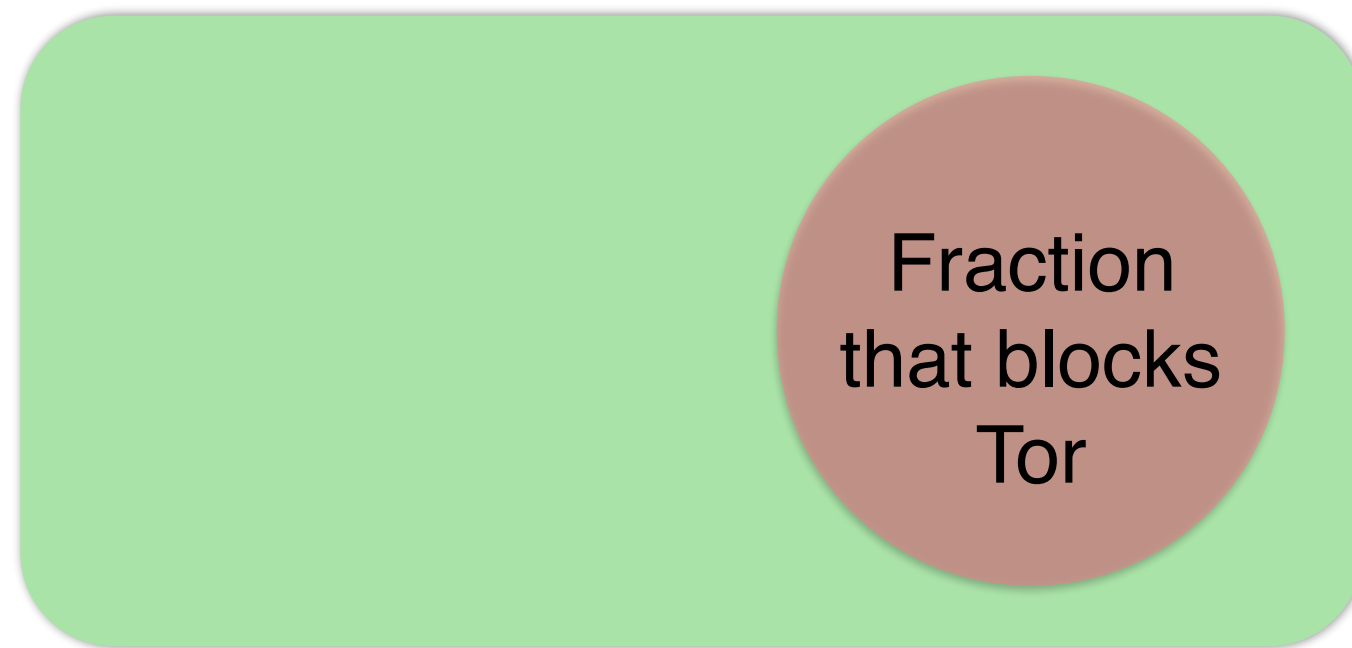
Scan IPv4

Tor Exit Node

- IPv4 ~ over 3 billion addrs
- 4 Tor Exit Nodes (USA, Romania, Netherlands)
- 3 Control Nodes (Michigan, Cambridge, Berkeley)

..But What is The Web?

- Web Footprint—a set of IP addresses that respond **successfully** to our **control scans** on port 80



Web Footprint

Challenges in Defining The Web

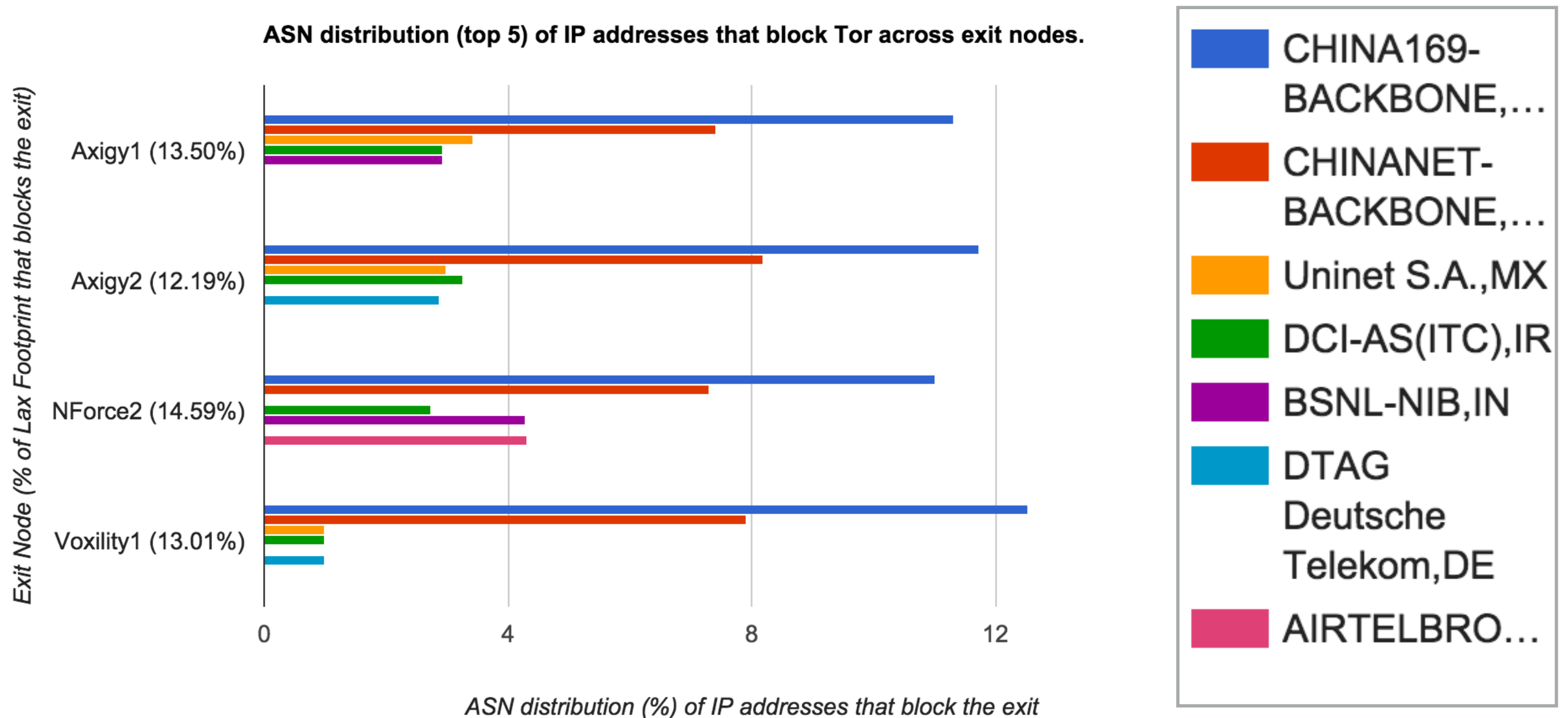
- What if a probe or response is lost?
 - ❖ Redundant probing
- Temporal and spatial churn in the Web Footprint:
 - ❖ Lax Web Footprint: IP addresses for which all control nodes see a response at least once (~96% of Web Footprint)
 - ❖ Strict Web Footprint: IP addresses for which all control nodes received a successful response on all days (~50% of Web Footprint)

Challenges in Defining The Web

- What if a probe or response is lost?
 - ❖ Redundant probing
- Temporal and spatial churn in the Web Footprint:
 - ❖ **Lax Web Footprint:** IP addresses for which all control nodes see a response at least once (~96% of Web Footprint)
 - ❖ **Strict Web Footprint:** IP addresses for which all control nodes receive a successful response on all days (~50% of Web Footprint)

At least 1.2% of the Web blocks Tor

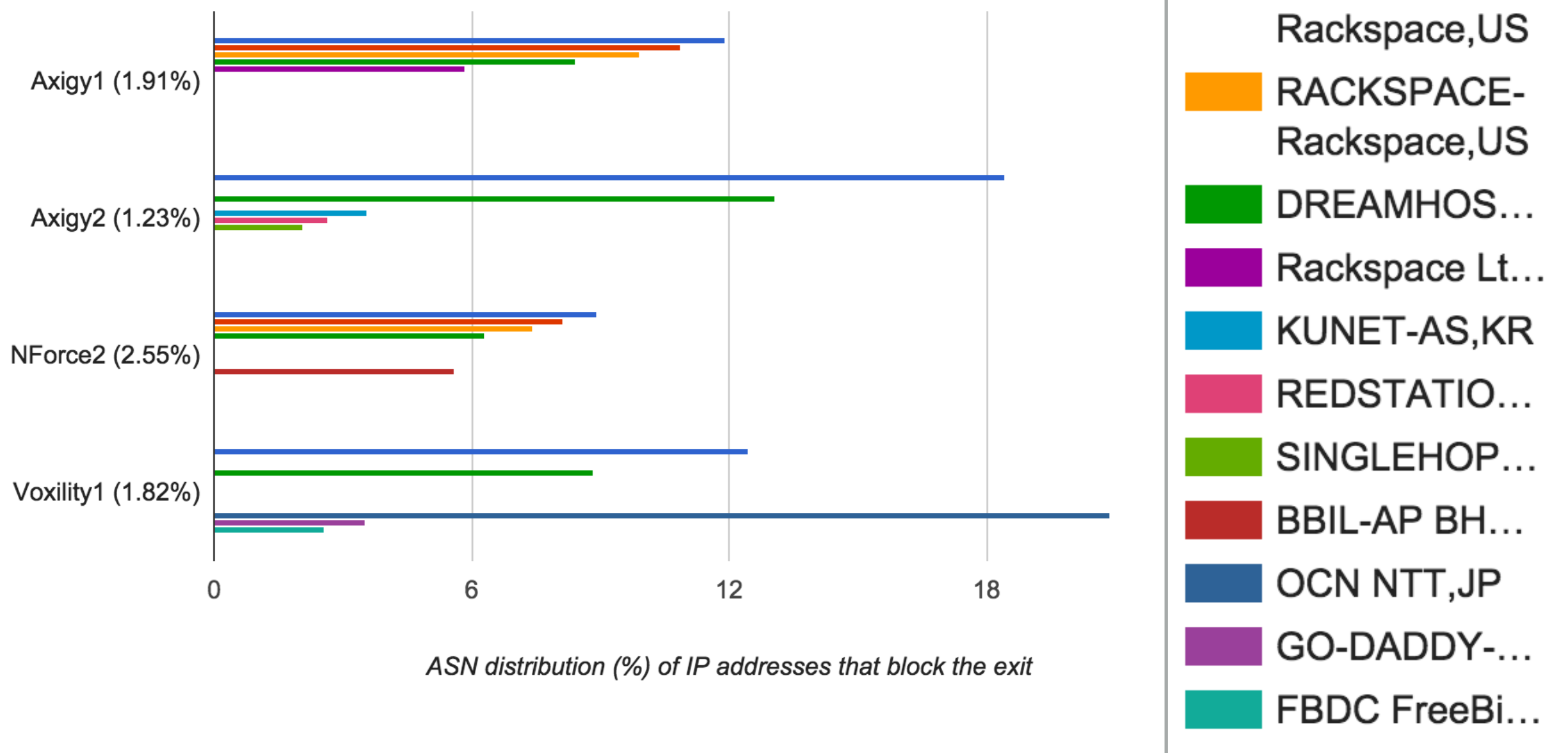
AS distribution of Top 5 Tor Blockers (Lax Footprint)



AS distribution of Top 5 Tor Blockers (Strict Footprint)





Exit Node (% of Strict Footprint that blocks the exit)

ASN distribution (top 5) of IP addresses that block Tor across exit nodes.



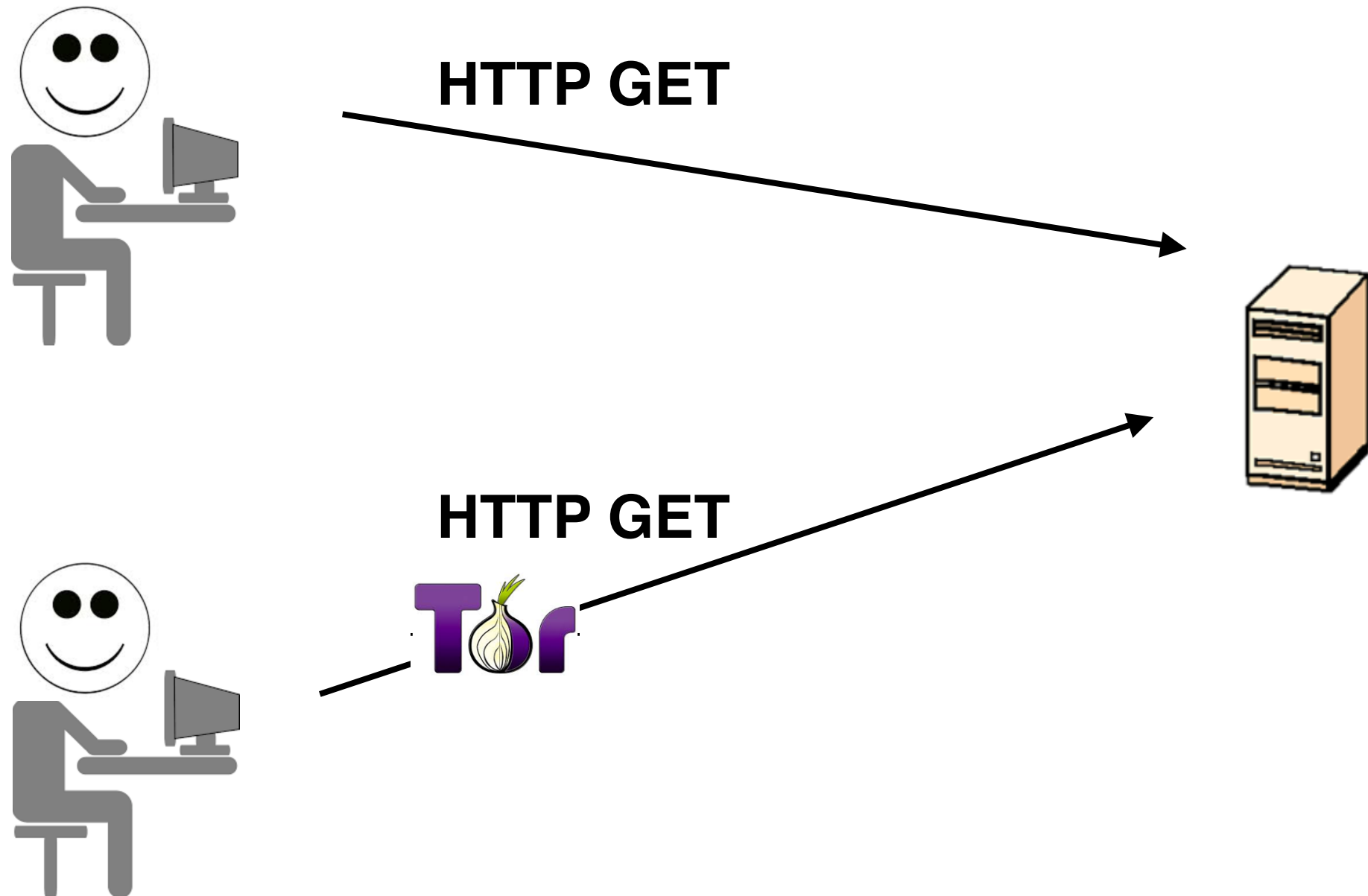
Geo Distribution of Top 5 ASes that do wholesale Tor blocking



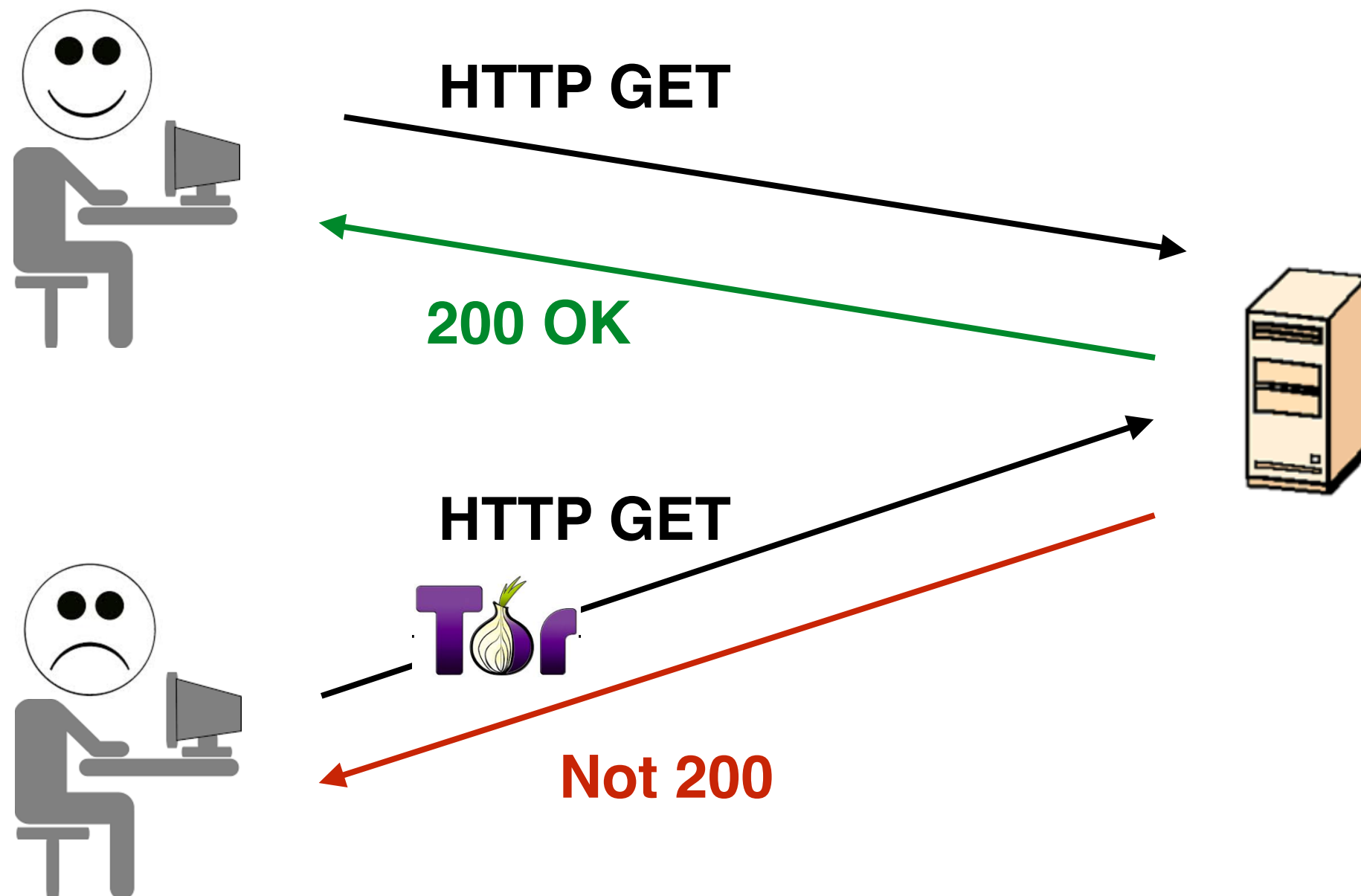
Axigy1 	Axigy2 	NForce2 	Voxility1 
MCCI-AS,IR RMH-14 - Rackspace,US RACKSPACE - Rackspace,US DREAMHOST-AS, LLC,US CNNIC-SGATHER-AP,CN	DREAMHOST-AS,US KUNET-AS,KR REDSTATION,GB LLC-SK-CONTINENT,RU tropicalweb-as,MZ	RMH-14-Rackspace,US RACKSPACE - Rackspace,US AIRCEL-IN Aircel Ltd.,IN DREAMHOST-AS, LLC,US Rackspace Ltd.,GB	OCN NTT Communications,JP DREAMHOST-AS, LLC,US KUNET-AS,KR BEKKOAME INTERNET INC.,JP tropicalweb-as,MZ

Application-layer Discrimination

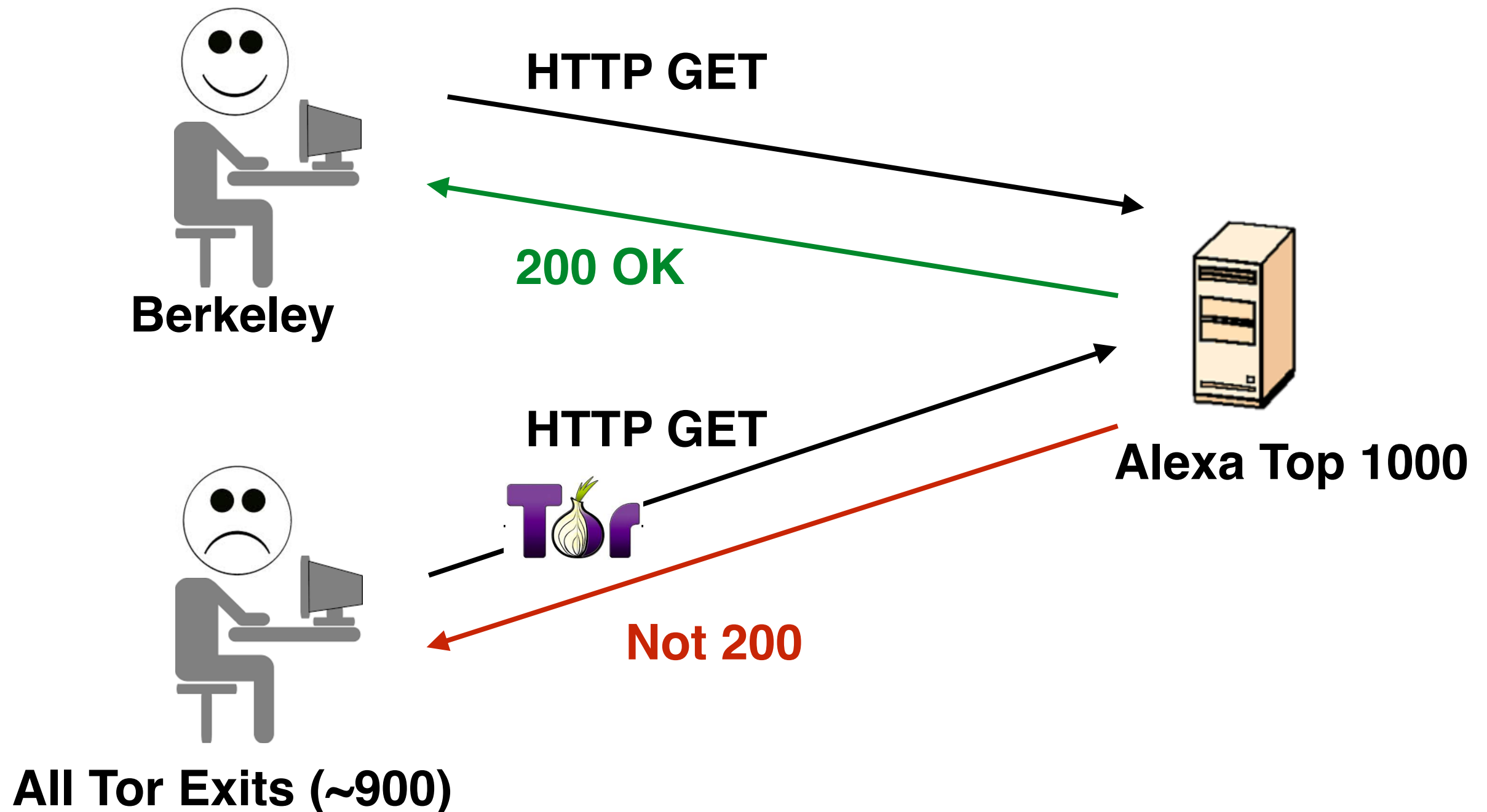
Does a Website Block Tor?



Does a Website Block Tor?



Does a Website Block Tor?



3.67% of Alexa Top 1k block Tor



Sorry, you're not allowed to access this page.

Your IP address is: 46.28.110.136

Please retry your request and [contact Yelp](#) if you continue experiencing issues.



This IP has been automatically blocked.
If you have questions, please email: blocks-b1451523930



Request denied

Sorry, we are unable to serve your request at this time due to unusual traffic from your network connection.

Please visit our [help page](#) and provide the information below for further assistance.

Reason codes:

3.67% of Alexa Top 1k block Tor

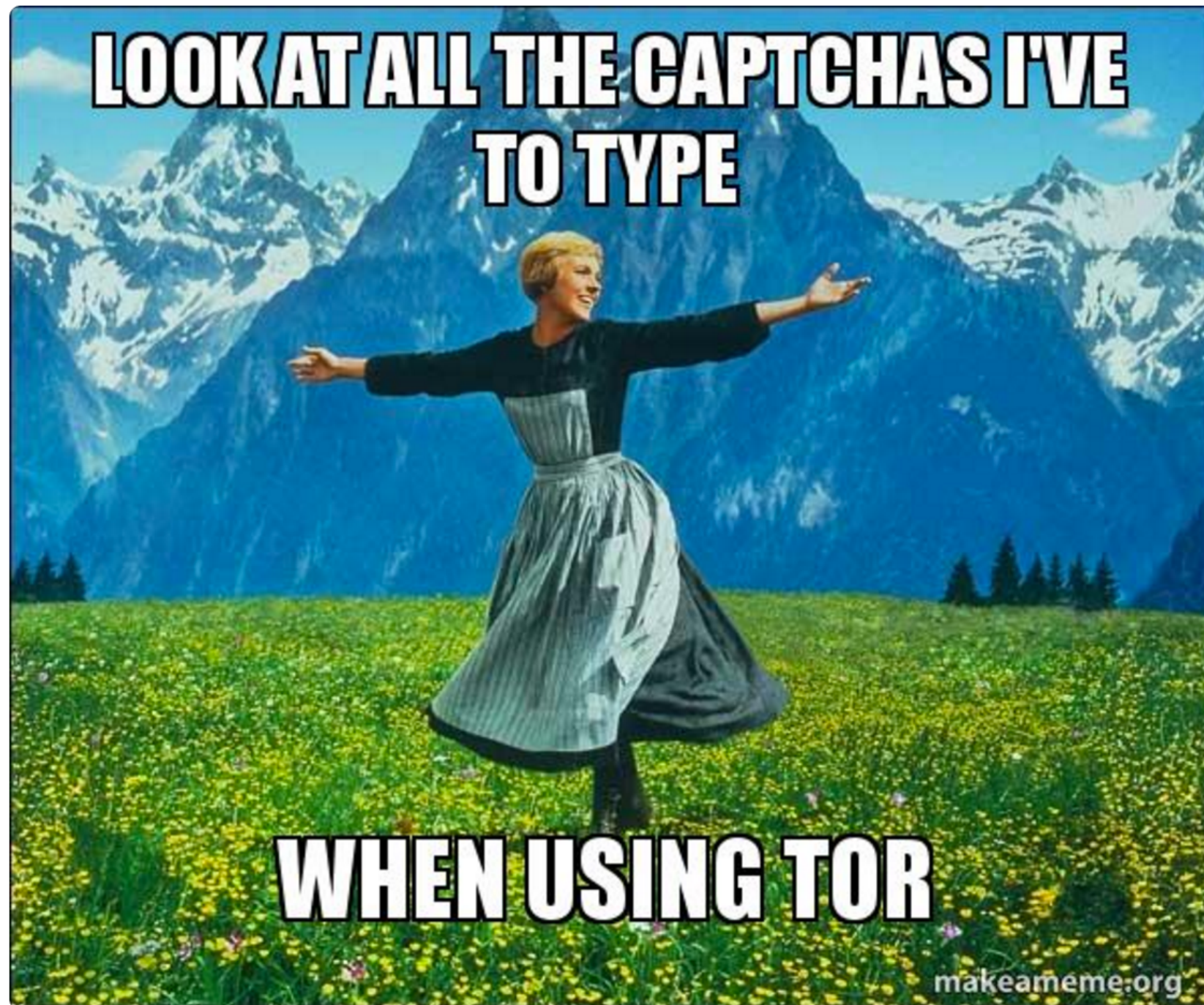


- “You don’t have permission to access this website”

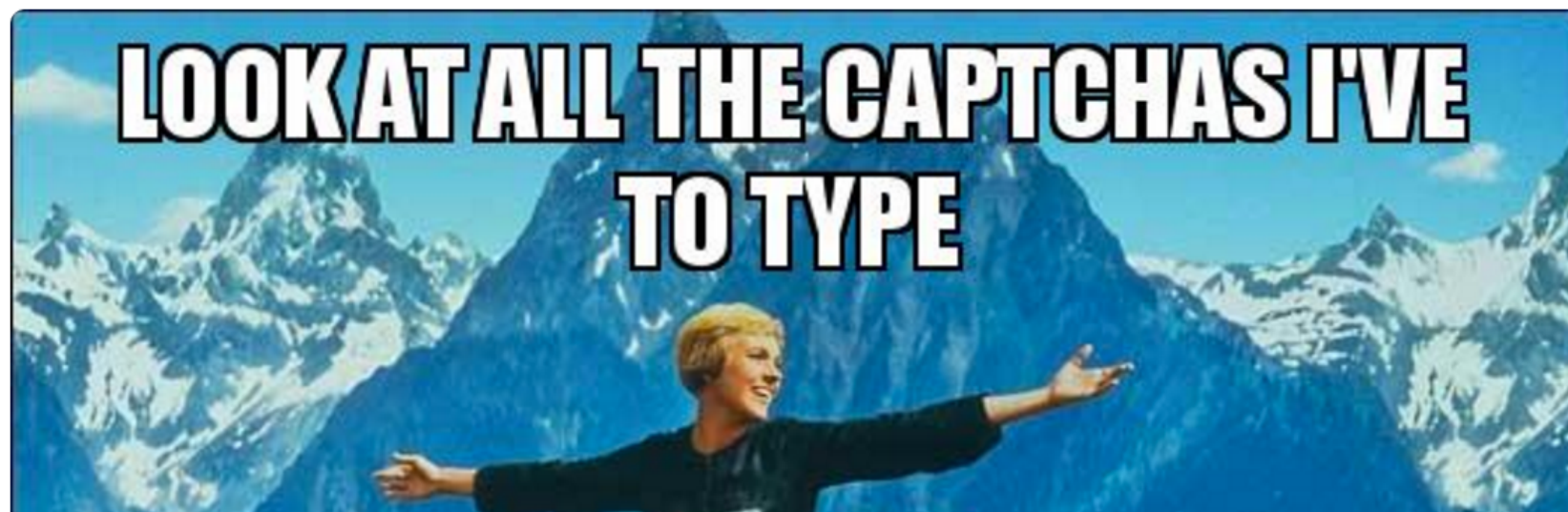


- Shows CAPTCHA

[#dontblocktor](#)



[#dontblocktor](#)

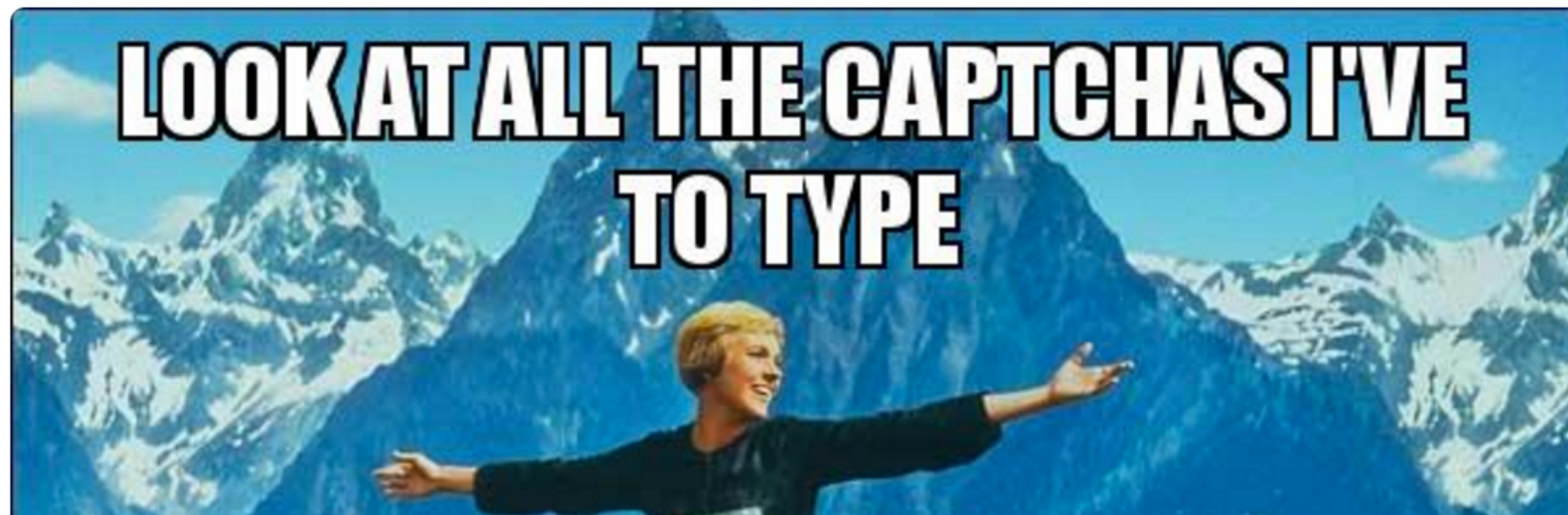


On February 9th, 2016 Anonymous said:
Tor is DEAD!
And Cloudflare KILLED it!
RIP Tor!

[reply](#)



[#dontblocktor](#)



On February 9th, 2016 Anonymous said:

Tor is DEAD!

And Cloudflare KILLED it!

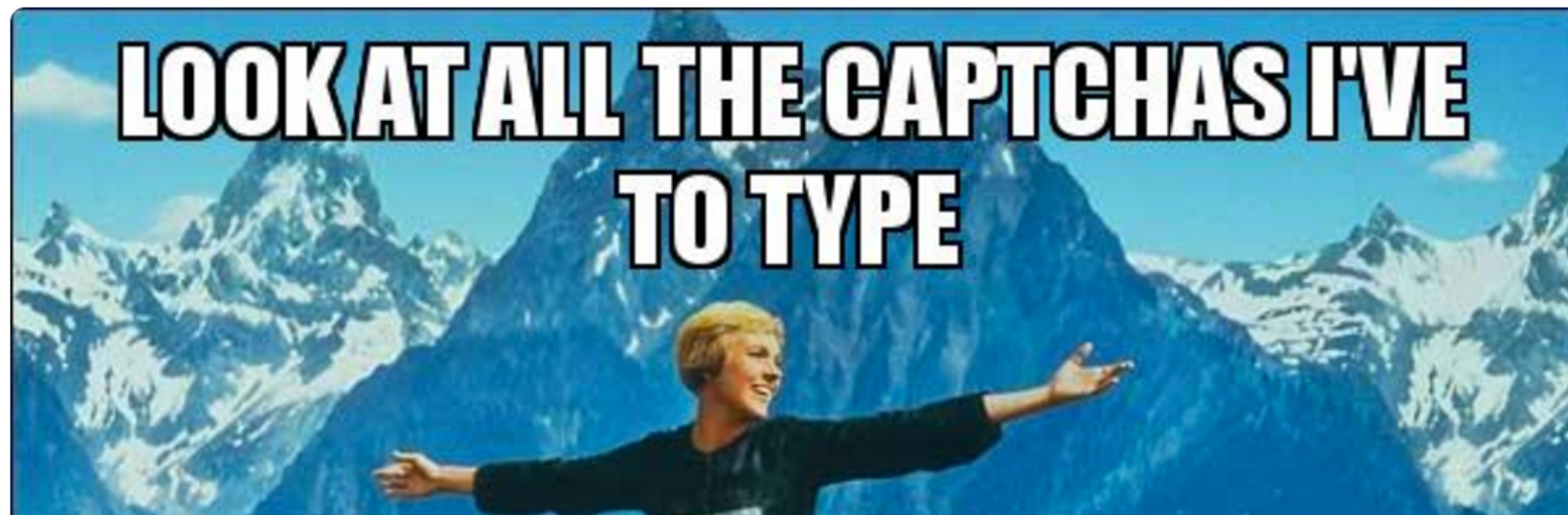
RIP Tor

On January 24th, 2016 Anonymous said:

Every time I use Tor I want to KILL everyone who works for Cloudflare.



[#dontblocktor](#)



On February 9th, 2016 Anonymous said:

Tor is DEAD!

And Cloudflare KILLED it!

RIP Tor

On January 24th, 2016 Anonymous said:

Every time I use Tor I want to KILL everyone who works for Cloudflare.



On February 9th, 2016 Anonymous said:

What is the point of Tor any more when it seems like the whole web is on Cloudflare!?

[#dontblocktor](#)

**LOOK AT ALL THE CAPTCHAS I'VE
TO TYPE**

**TRYING TO DECRYPT THE
CAPTCHAS**



WHEN USING TOR

makeameme.org

On February 9th, 2016
Tor is DEAD!

And Cloudflare Killed

RIP Tor

On Jan

Every

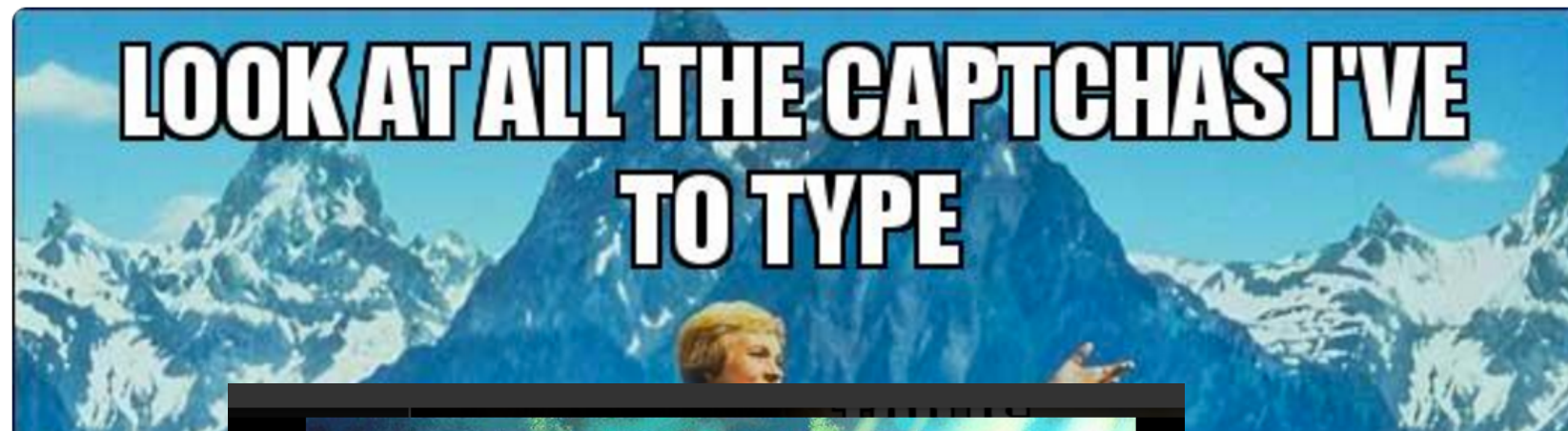
everyone who works for Cloudflare.

R

the whole web is on Clownfare!?

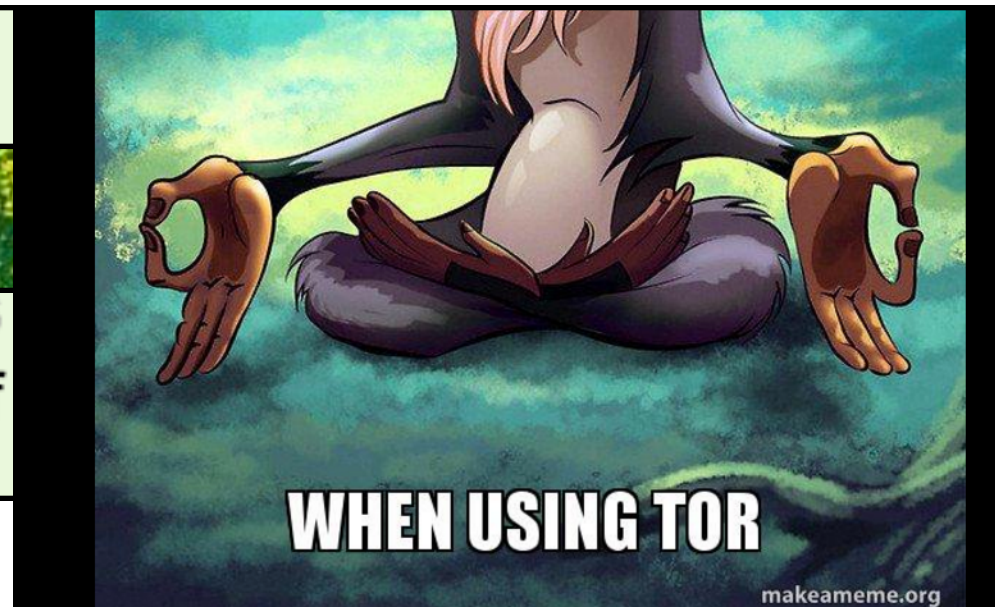
On February 9th, 2016
What is the point of

[#dontblocktor](#)



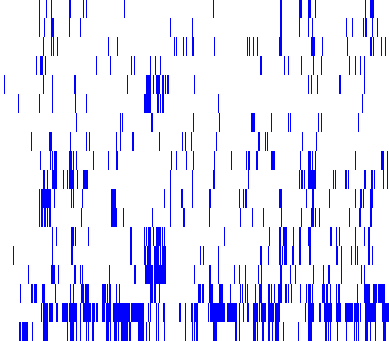
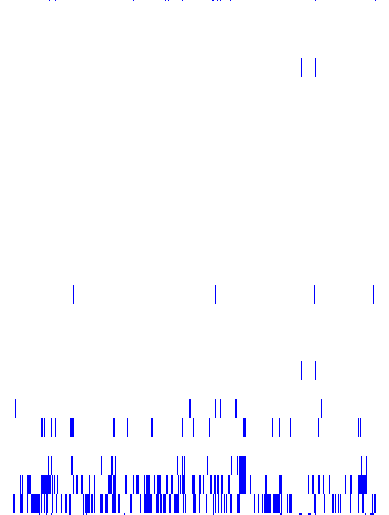
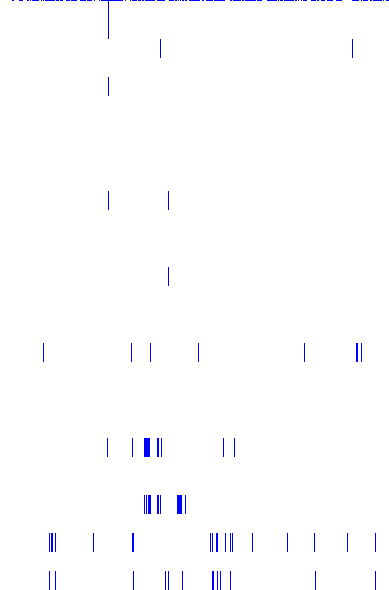
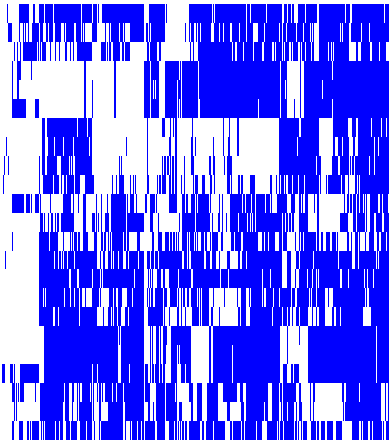
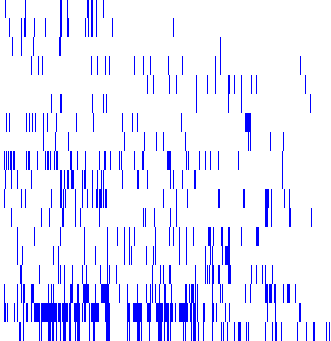
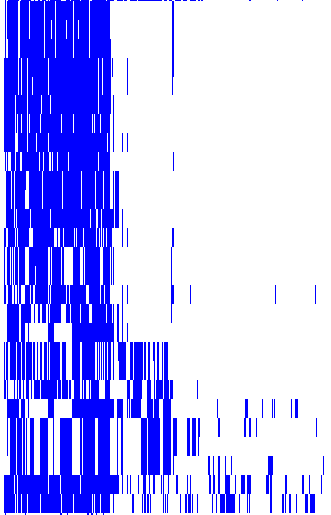
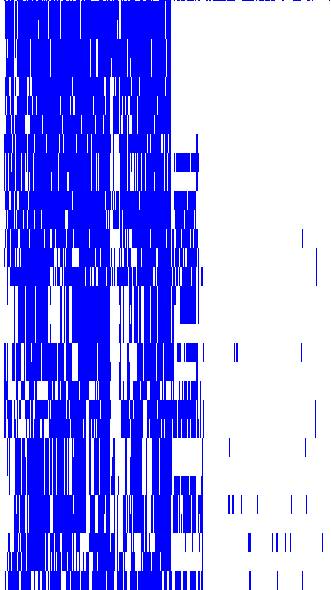
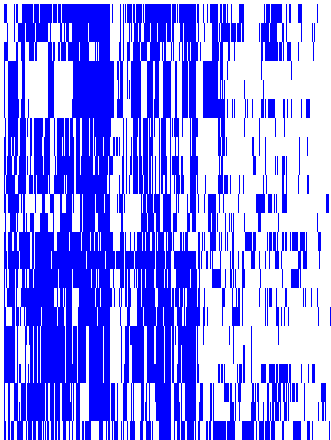
last night I had a dream that there were two new ways to solve cloudflare captchas: writing sentences w/ emoji & proving $P = NP$

On February 9th, 2016
What is the point of



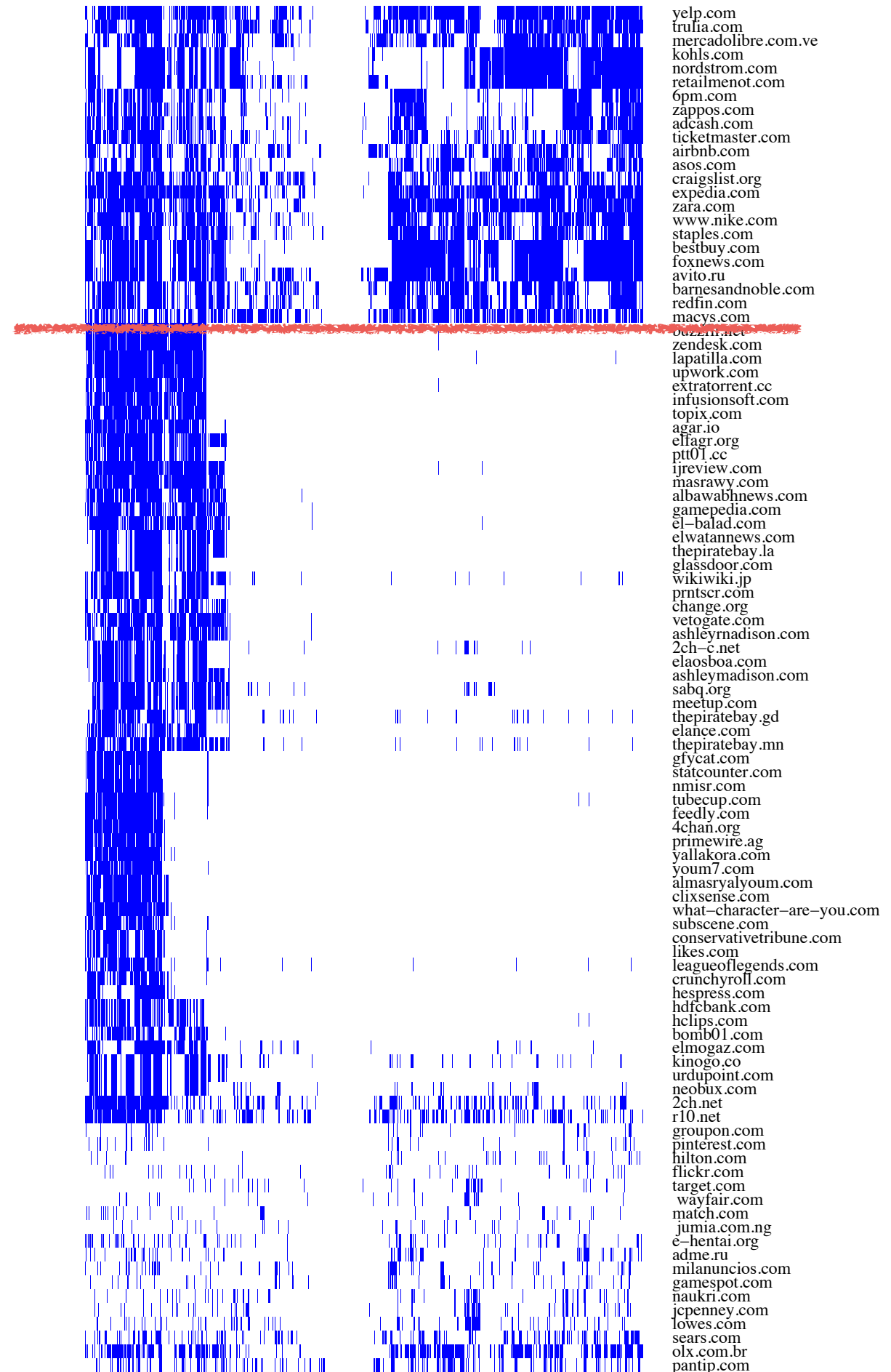
the whole web is on Clownfare!?

How many of the ~900 Tor exits
are blocked?



yelp.com
trulia.com
mercadolibre.com.ve
kohls.com
nordstrom.com
retailmenot.com
6pm.com
zappos.com
adcash.com
ticketmaster.com
airbnb.com
asos.com
craigslist.org
expedia.com
zara.com
www.nike.com
staples.com
bestbuy.com
foxnews.com
avito.ru
barnesandnoble.com
redfin.com
macys.com
buzzfil.net
zendesk.com
lapatilla.com
upwork.com
extratorrent.cc
infusionsoft.com
topix.com
agar.io
elfagr.org
ptt01.cc
ijreview.com
masrawy.com
albawabhnews.com
gamepedia.com
el-balad.com
elwatannews.com
thepiratebay.la
glassdoor.com
wikiwiki.jp
prntscr.com
change.org
vetogate.com
ashleymadison.com
2ch-c.net
elaosboa.com
ashleymadison.com
sabq.org
meetup.com
thepiratebay.gd
elance.com
thepiratebay.mn
gfycat.com
statcounter.com
nmisr.com
tubecup.com
feedly.com
4chan.org
primewire.ag
yallakora.com
youm7.com
almasryalyoum.com
clixsense.com
what-character-are-you.com
subscene.com
conservativetribune.com
likes.com
leagueoflegends.com
crunchyroll.com
hespress.com
hdfcbank.com
hclips.com
bomb01.com
elmogaz.com
kinogo.co
urdupoint.com
neobux.com
2ch.net
r10.net
groupon.com
pinterest.com
hilton.com
flickr.com
target.com
wayfair.com
match.com
jumia.com.ng
e-hentai.org
adme.ru
milanuncios.com
gamespot.com
naukri.com
jcpenny.com
lowes.com
sears.com
olx.com.br
pantip.com

~20 of Alexa top 1k websites
block > 50% of the exits



~20 of Alexa top 1k websites
block > 50% of the exits

~60 of Alexa top 1k websites
block < 25% of the exits



Why do exits get blocked?

- Two flavours:
 - ✦ Web services use **Tor specific blacklist**
 - ✦ **Block all** the Tor exits
 - ✦ Web services use **abuse-based blocking**
 - ✦ Block only exits with high abuse rate

Which exits are likely to have high abuse rate?

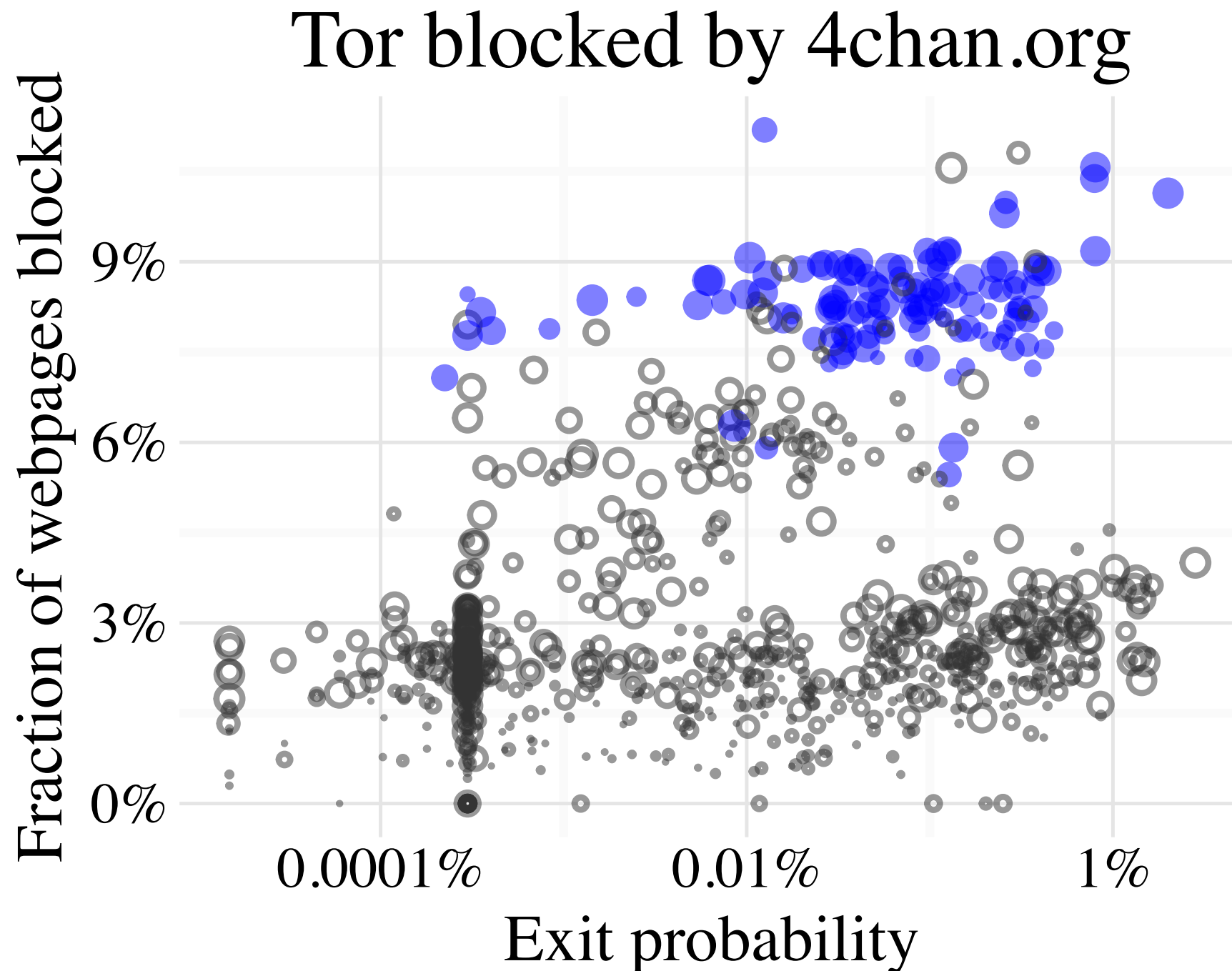
- Our hypothesis: high bandwidth and old age

Which exits are likely to have high abuse rate?

- Our hypothesis: high bandwidth and old age
- No statistically significant effect!
 - ❖ Except for few ...

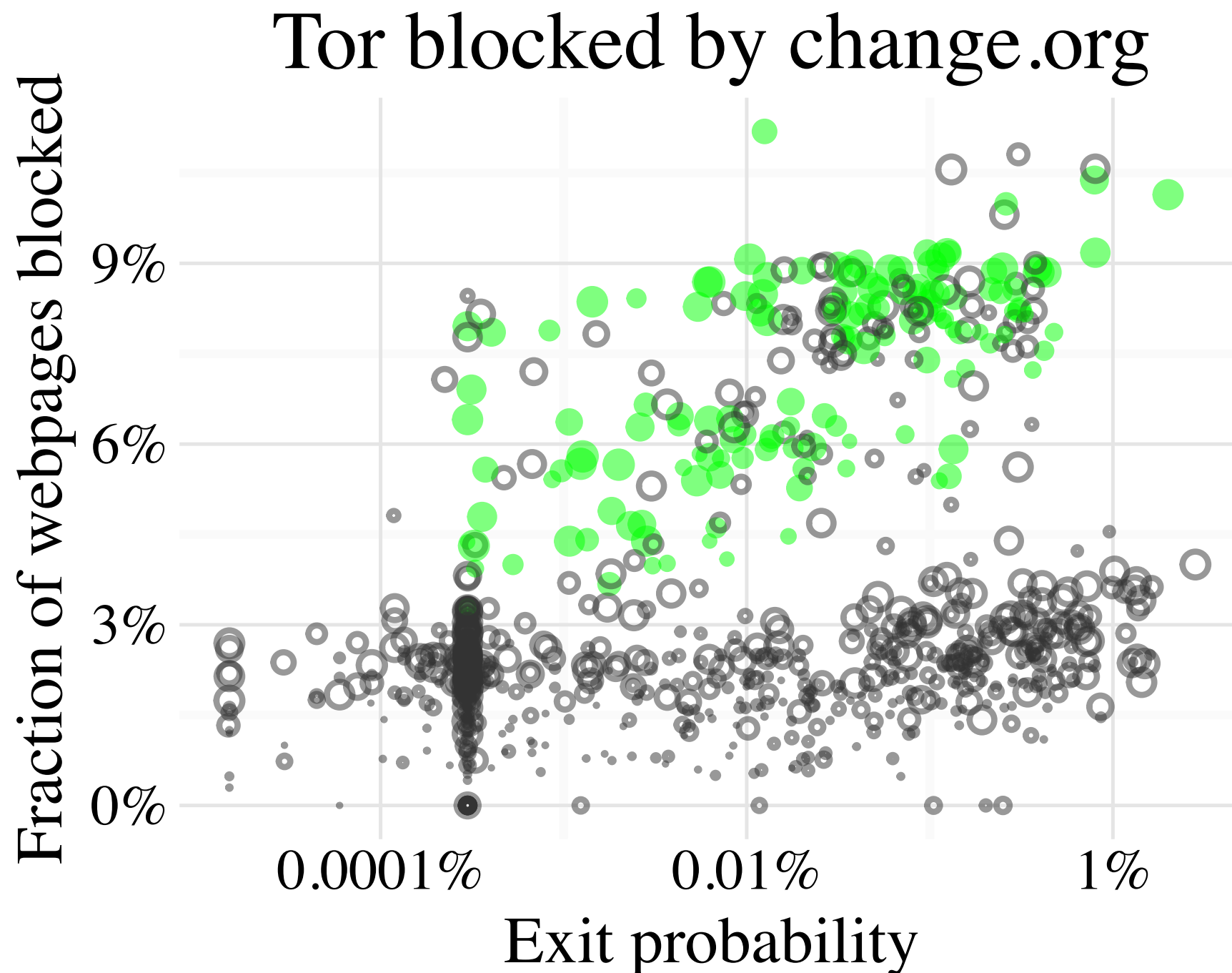
Which exits are blocked?

Old and high bandwidth



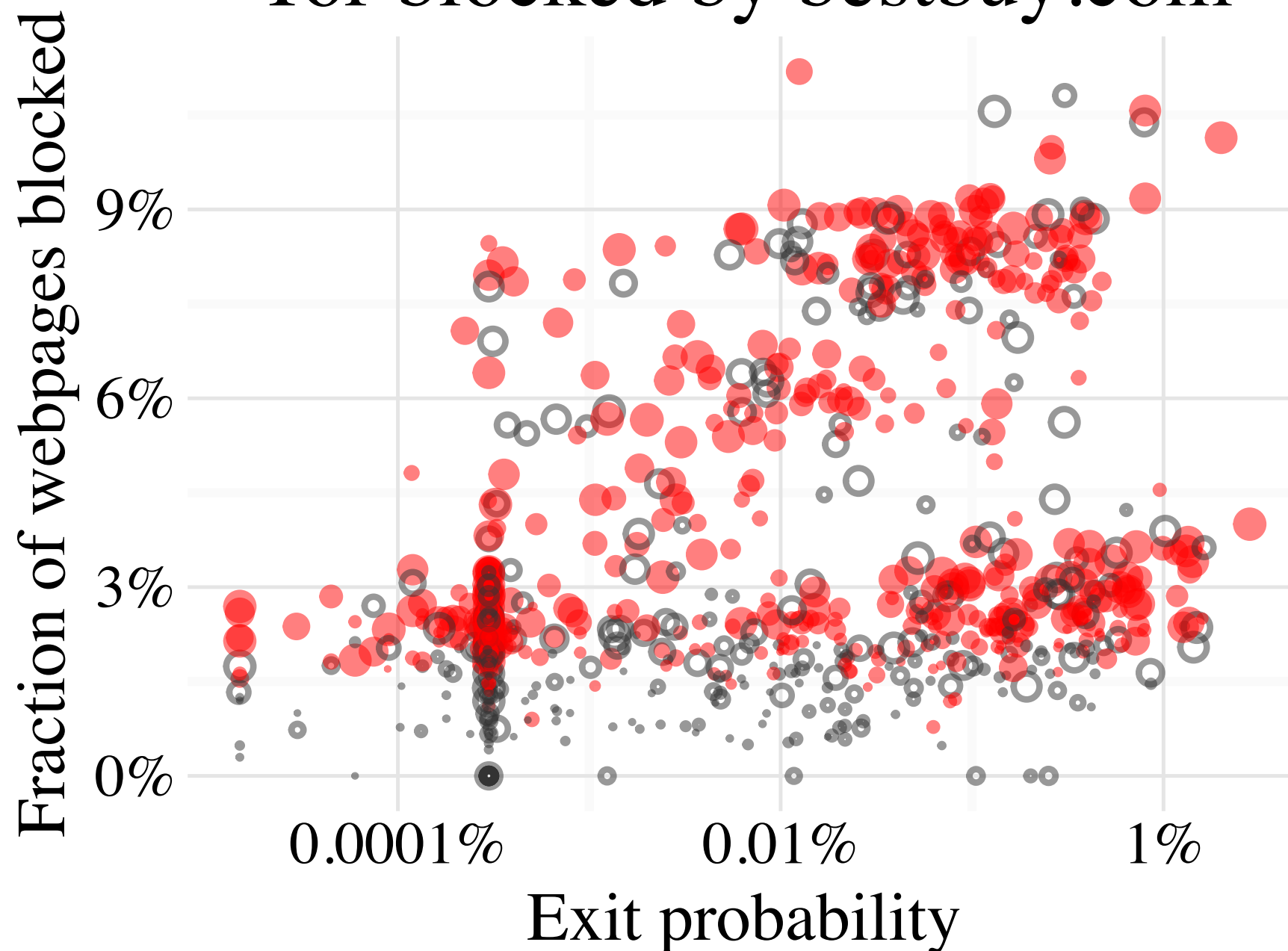
Which exits are blocked?

Old and high bandwidth



Akamai blocks most exits

Tor blocked by bestbuy.com



Homepage unblocked but blocked activity

- Google homepage was never blocked but searching was blocked from 23-40% of the ~900 exits.

Response to <https://www.google.com/#q=hello>

 Sorry...

We're sorry...

... but your computer or network may be sending automated queries. To protect our users, we can't process your request right now.

See [Google Help](#) for more information.

[Google Home](#)

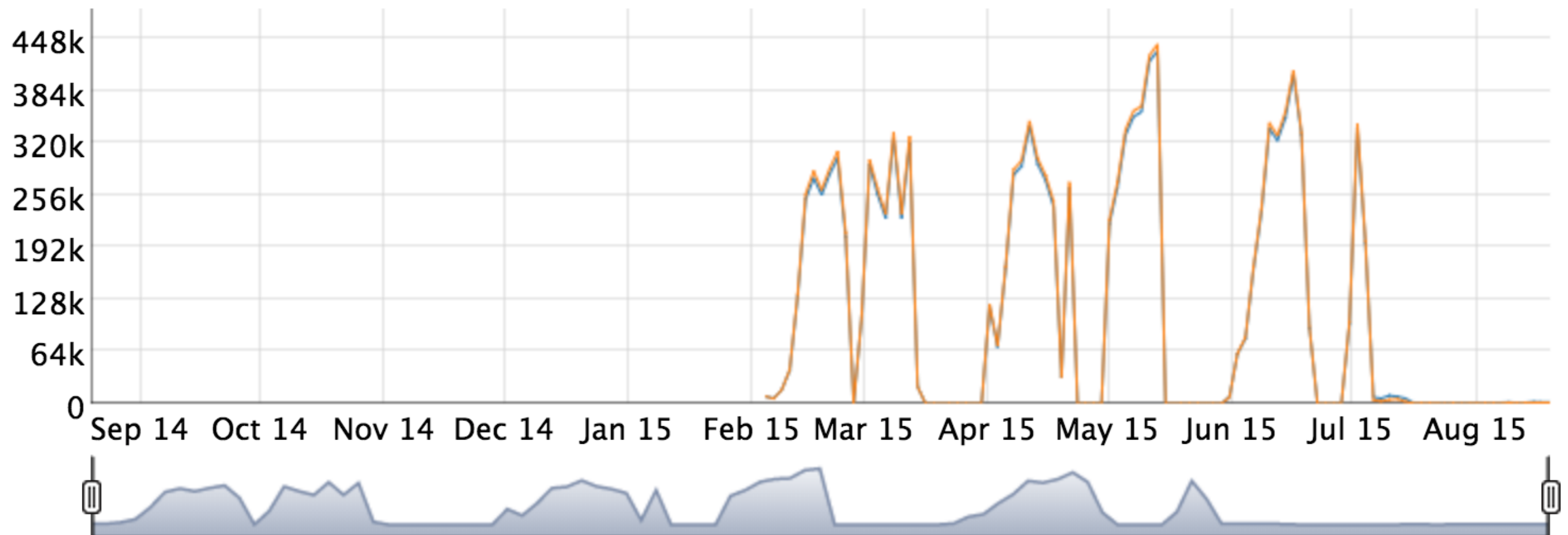
Exits that were never blocked

- 42 exits were never blocked

Exits that were never blocked

- 42 exits were never blocked

Uptime of one of the 42 exits

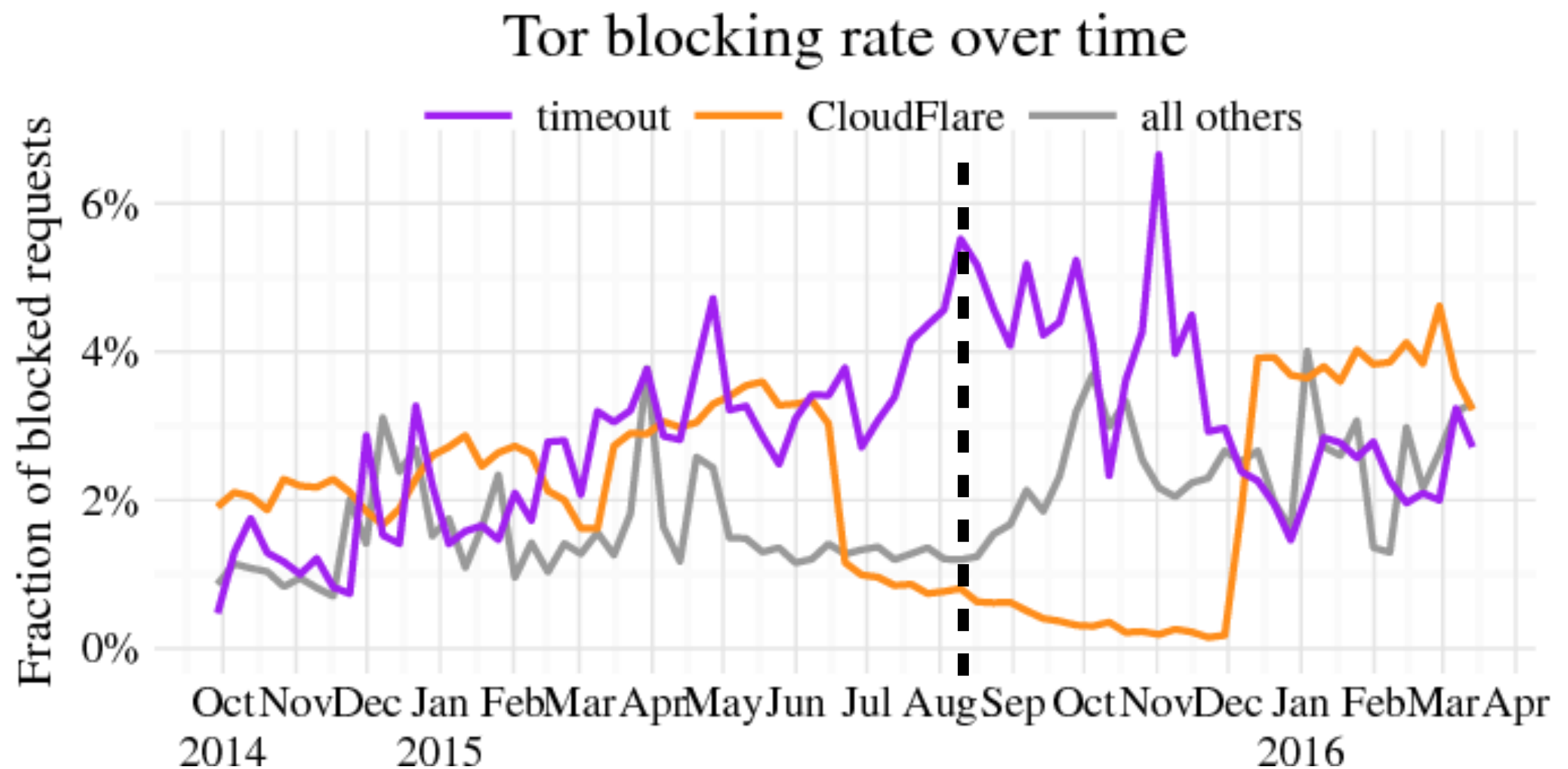


Historical Tor Blocking

- Open Observatory Network Interference (OONI)
 - ❖ Studies censorship in different countries
 - ❖ Visits website through Tor and without Tor
 - ❖ Over 2300 websites visited (Sep'14-Aug'15)

<http://explorer.ooni.io>

6.8% of 2300 websites blocked Tor

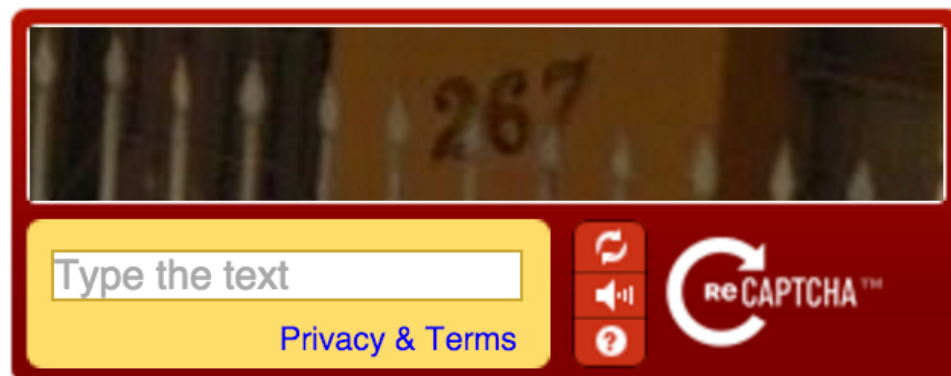


Sites that explicitly block Tor

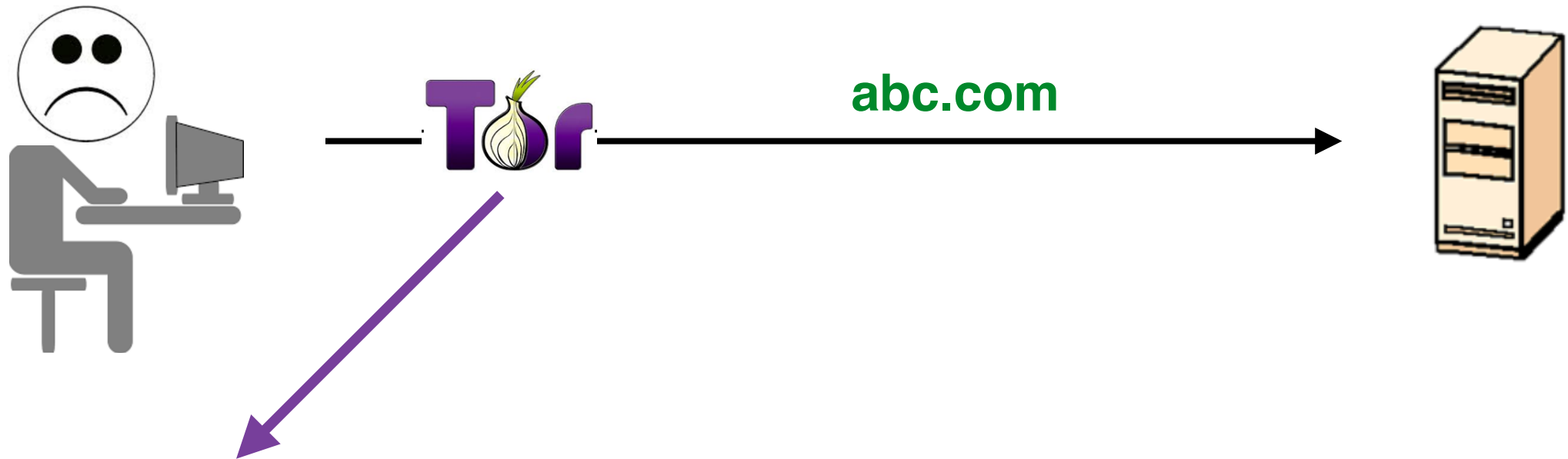
- Convio: Not Implemented Tor IP not allowed
- ezinearticles.com

It appears that you are using Tor anonymizing software

No Problem! We just need you to enter a Captcha so we can confirm that you are a person and not a bot.

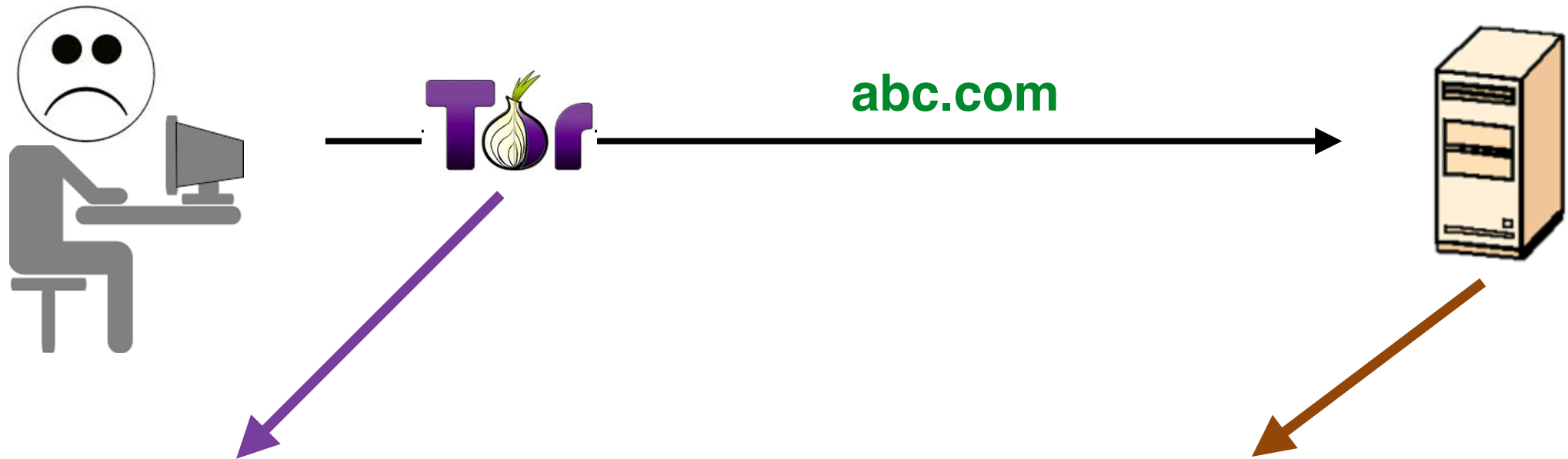


Solution?



- Contextual awareness
- Redesigning anonymity networks

Solution?

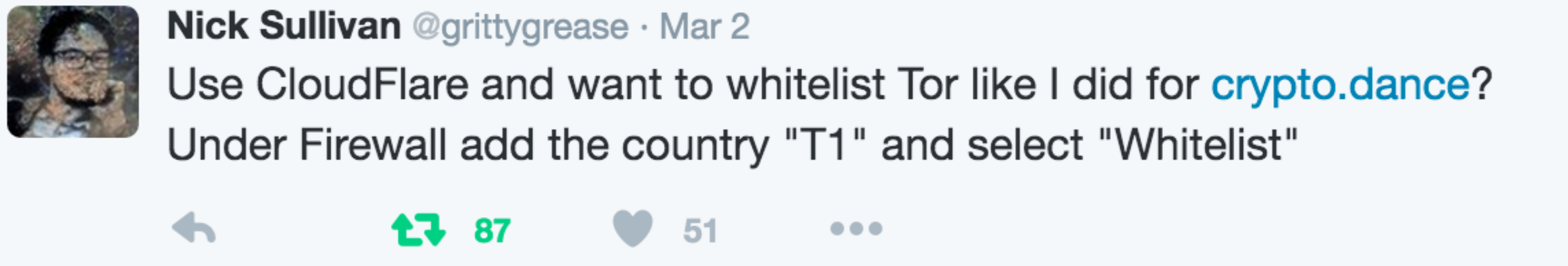


- Contextual awareness
- Redesigning anonymity networks

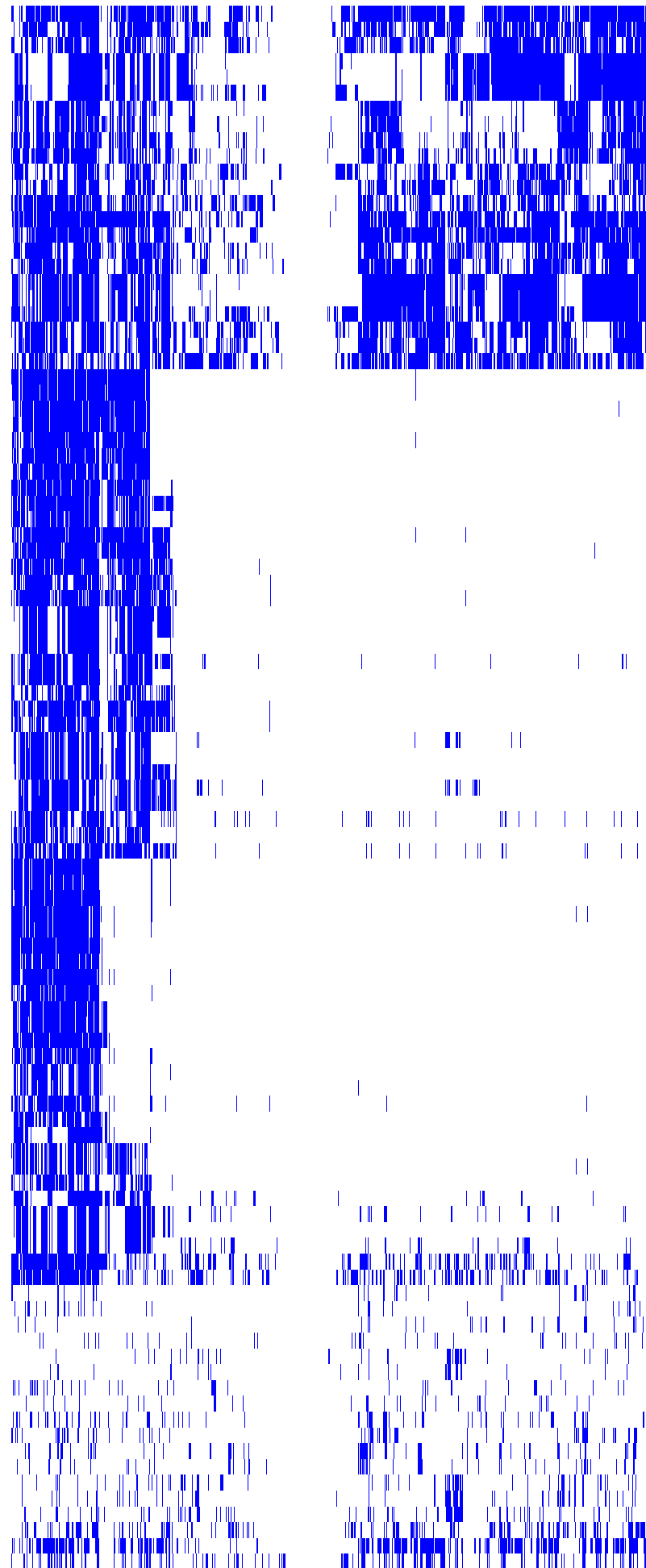
- Anonymous blacklisting
- Redesigning automated abuse-based blocking

New since this paper

- CloudFlare added Tor as a “country”

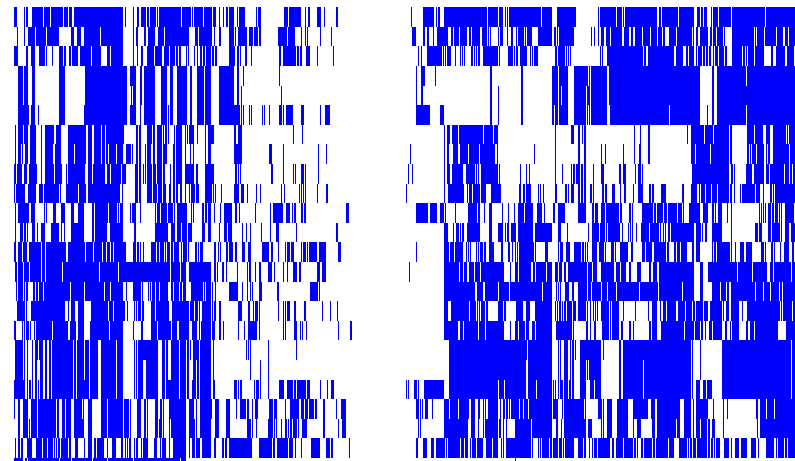


<---Tor exits (~900)---> Aug, 2015



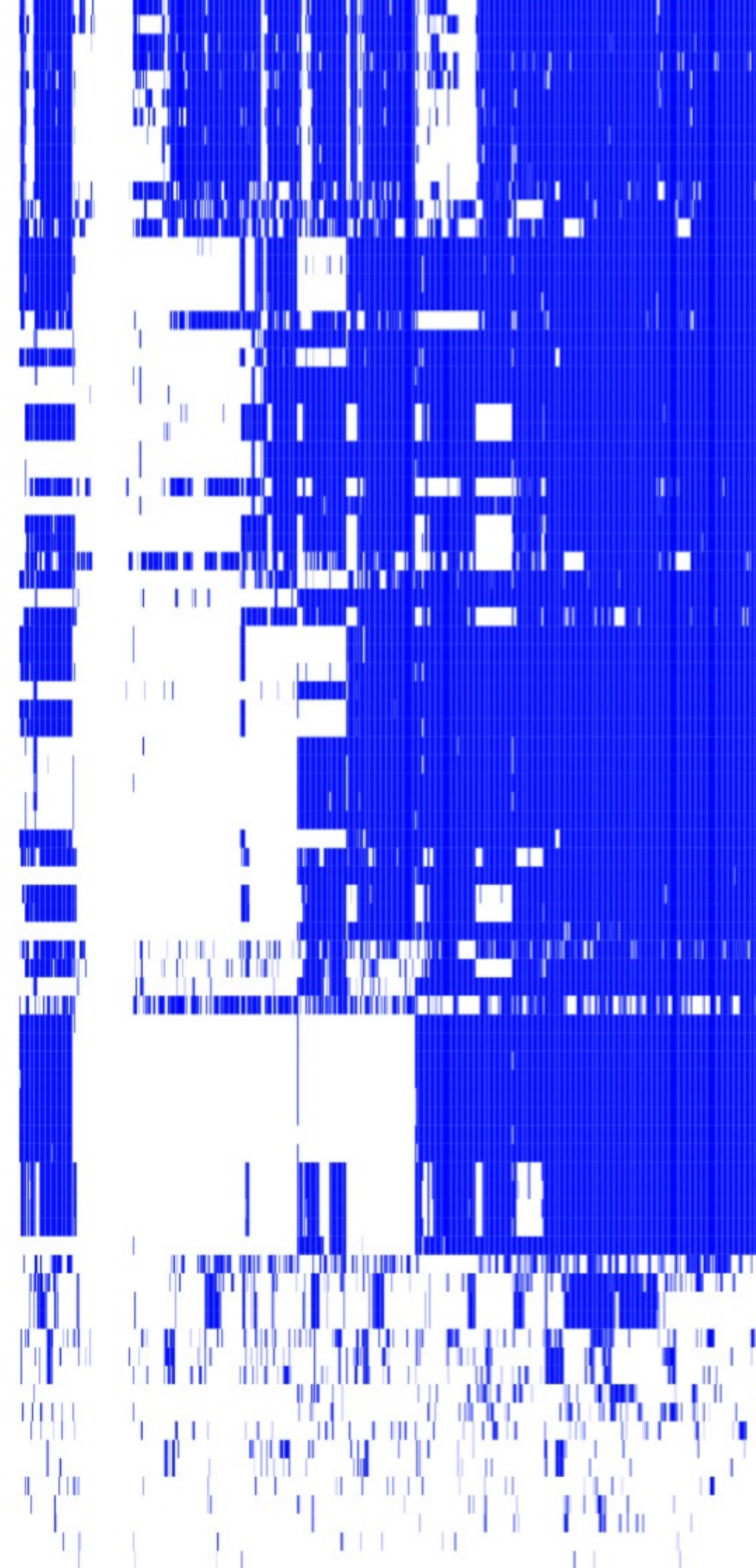
yelp.com
trulia.com
mercadolibre.com.ve
kohls.com
nordstrom.com
retailmenot.com
6pm.com
zappos.com
adcash.com
ticketmaster.com
airbnb.com
asos.com
craigslist.org
expedia.com
zara.com
www.nike.com
staples.com
bestbuy.com
foxnews.com
avito.ru
barnesandnoble.com
redfin.com
macys.com
buzzfil.net
zendesk.com
lapatilla.com
upwork.com
extratorrent.cc
infusionsoft.com
topix.com
agar.io
elfagr.org
ptt01.cc
ijreview.com
masrawy.com
albawabnews.com
gamepedia.com
el-balad.com
elwatannews.com
thepiratebay.la
glassdoor.com
wikiwiki.jp
prntscr.com
change.org
vetogate.com
ashleymadison.com
2ch-c.net
elaosboa.com
ashleymadison.com
sabq.org
meetup.com
thepiratebay.gd
elance.com
thepiratebay.mn
gfycat.com
statcounter.com
nmisr.com
tubecup.com
feedly.com
4chan.org
primewire.ag
yallakora.com
youm7.com
almasryalyoum.com
clixsense.com
what-character-are-you.com
subscene.com
conservativetribune.com
likes.com
leagueoflegends.com
crunchyrofl.com
hespress.com
hdfcbank.com
hclips.com
bomb01.com
elmogaz.com
kinogo.co
urdupoint.com
neobux.com
2ch.net
r10.net
groupon.com
pinterest.com
hilton.com
flickr.com
target.com
wayfair.com
match.com
jumia.com.ng
e-hentai.org
adme.ru
milanuncios.com
gamespot.com
naukri.com
jcpennney.com
lowes.com
sears.com
olx.com.br
pantip.com

<--Tor exits (~900)--> Aug, 2015



yelp.com
trulia.com
mercadolibre.com.ve
kohls.com
nordstrom.com
retailmenot.com
6pm.com
zappos.com
adcash.com
ticketmaster.com
airbnb.com
asos.com
craigslist.org
expedia.com
zara.com
www.nike.com
staples.com
bestbuy.com
foxnews.com
avito.ru
barnesandnoble.com
redfin.com
macys.com
buzzfil.net
zendesk.com
lapatilla.com
upwork.com
extratorrent.cc
infusionsoft.com
topix.com
agar.io
elfagr.org
ptt01.cc
ijreview.com
masrawy.com
albawabnews.com
gamepedia.com
el-balad.com
elwatannews.com
thepiratebay.la
glassdoor.com
wikiwiki.jp
prntscr.com
change.org
vetogate.com
ashleymadison.com
2ch-c.net
elaosboa.com
ashleymadison.com
sabq.org
meetup.com
thepiratebay.gd
elance.com
thepiratebay.mn
gfycat.com
statcounter.com
nmsr.com
tubecup.com
feedly.com
4chan.org
primewire.ag
yallakora.com
youm7.com
almasryalyoum.com
clixsense.com
what-character-are-you.com
subscene.com
conservativetribune.com
likes.com
leagueoflegends.com
crunchyroll.com
hespress.com
hdfcbank.com
hclips.com
bomb01.com
elmogaz.com
kinogo.co
urdupoint.com
neobux.com
2ch.net
r10.net
groupon.com
pinterest.com
hilton.com
flickr.com
target.com
wayfair.com
match.com
jumia.com.ng
e-hentai.org
adme.ru
milanuncios.com
gamespot.com
naukri.com
jcpennney.com
lowes.com
sears.com
olx.com.br
pantip.com

<--Tor exits (~900)--> (Feb, 2016)



avito.ru
ticketmaster.com
retailmenot.com
trulia.com
redfin.com
kohls.com
yelp.com
nordstrom.com
foxnews.com
zara.com
airbnb.com
lowes.com
macys.com
change.org
youm7.com
hdfcbank.com
urdupoint.com
expedia.com
elwatannews.com
primewire.ag
ashleymadison.com
wikiwiki.jp
el-balad.com
sabq.org
gamepedia.com
meetup.com
asos.com
agar.io
ijreview.com
masrawy.com
sears.com
leagueoflegends.com
kinogo.co
zendesk.com
tubecup.com
hclips.com
bomb01.com
2ch-c.net
nmsr.com
glassdoor.com
elmogaz.com
elance.com
ashleymadison.com
prntscr.com
topix.com
elaosboa.com
conservativetribune.com
upwork.com
lapatilla.com
buzzfil.net
infusionsoft.com
craigslist.org
2ch.net
neobux.com
barnesandnoble.com
statcounter.com
almasryalyoum.com
4chan.org
feedly.com
gfycat.com
clixsense.com
what-character-are-you.com
yallakora.com
likes.com
hespress.com
crunchyroll.com
subscene.com
extratorrent.cc
bestbuy.com
adcash.com
zappos.com
6pm.com
jcpennney.com
naukri.com
staples.com
ptt01.cc
e-hentai.org
gamespot.com
wayfair.com
target.com
match.com
pinterest.com
groupon.com
flickr.com
olx.com.br
www.nike.com
vetogate.com
jumia.com.ng
hilton.com
albawabnews.com
mercadolibre.com.ve
thepiratebay.mn
pantip.com
r10.net
thepiratebay.gd
thepiratebay.la
adme.ru
milanuncios.com
elfagr.org

Summary

- At least 1.2% of the Web block Tor (n/w)
- At least 3.67% of Alexa top 1k sites block Tor (app)
- Fine-grained discrimination?
- Who else is subject to this kind of discrimination?

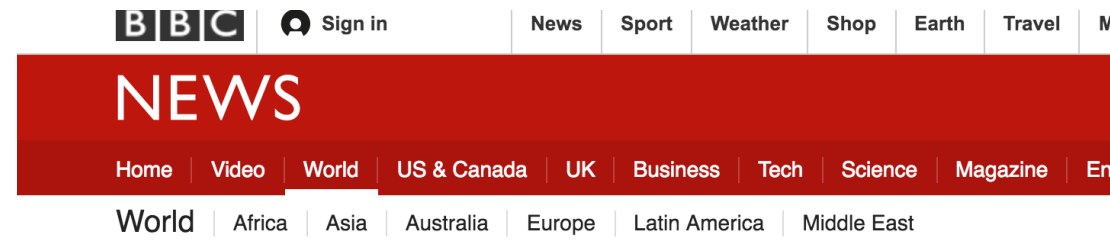
Tor users' experiences

- <https://pad.systemli.org/p/twitterdontblocktor>
- “Account has not been blocked. I use it with Tor Browser, Chrome, twitter app. note: my account is relatively old (2009) and has never been suspended.”
- “Account was blocked. Claims of detecting ‘abusive behavior’ but nothing of the sort happened, Account was created and used only through Tor. Only used to follow various people, almost no tweets sent. It was fine for months, then suddenly blocked one day. Still blocked. Twitter asks for a phone number. I refuse to provide one. I don't want to be forced into that network. Account still not recovered.”

What can Twitter do?

- Measure how many users you have on Tor.
<https://collector.torproject.org/#type-tordnse>
Match past exit IP addresses against your logs.
- Measure how often Tor users get extra challenges: lockouts or phone verifications, for example.
- Set up an onion service.
<https://lists.torproject.org/cgi-bin/mailman/listinfo/tor-onions>
<https://blog.torproject.org/blog/facebook-hidden-services-and-https-certs>

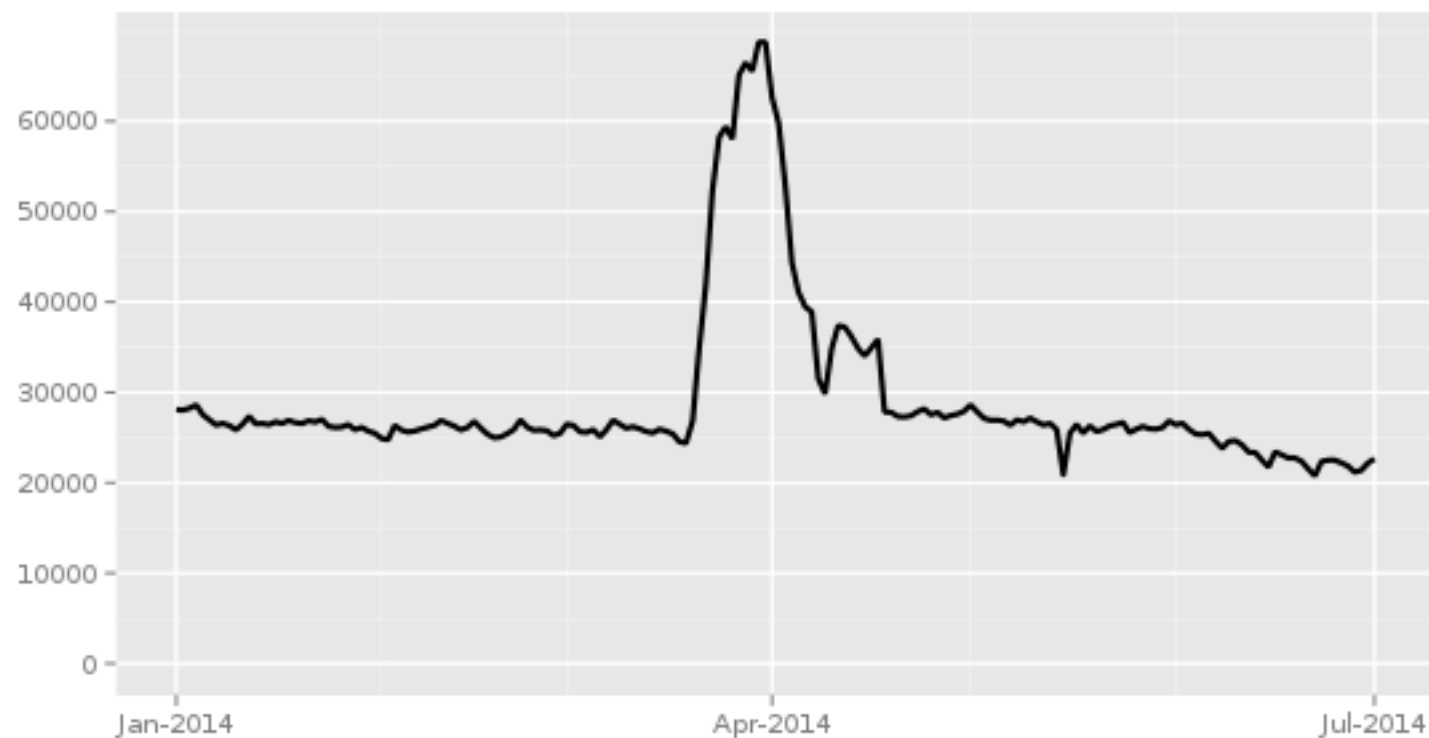
Some users turn to Tor when Twitter is blocked



Twitter website 'blocked' in Turkey

21 March 2014 | Europe

Directly connecting users from Turkey



Thanks
Q&A

fifield@eecs.berkeley.edu

sadia@icsi.berkeley.edu