Measuring I2P Censorship at a Global Scale



Nguyen Phong Hoang, Sadie Doreen, Michalis Polychronakis

Stony Brook University

OPEN TECHNOLOGY FUND

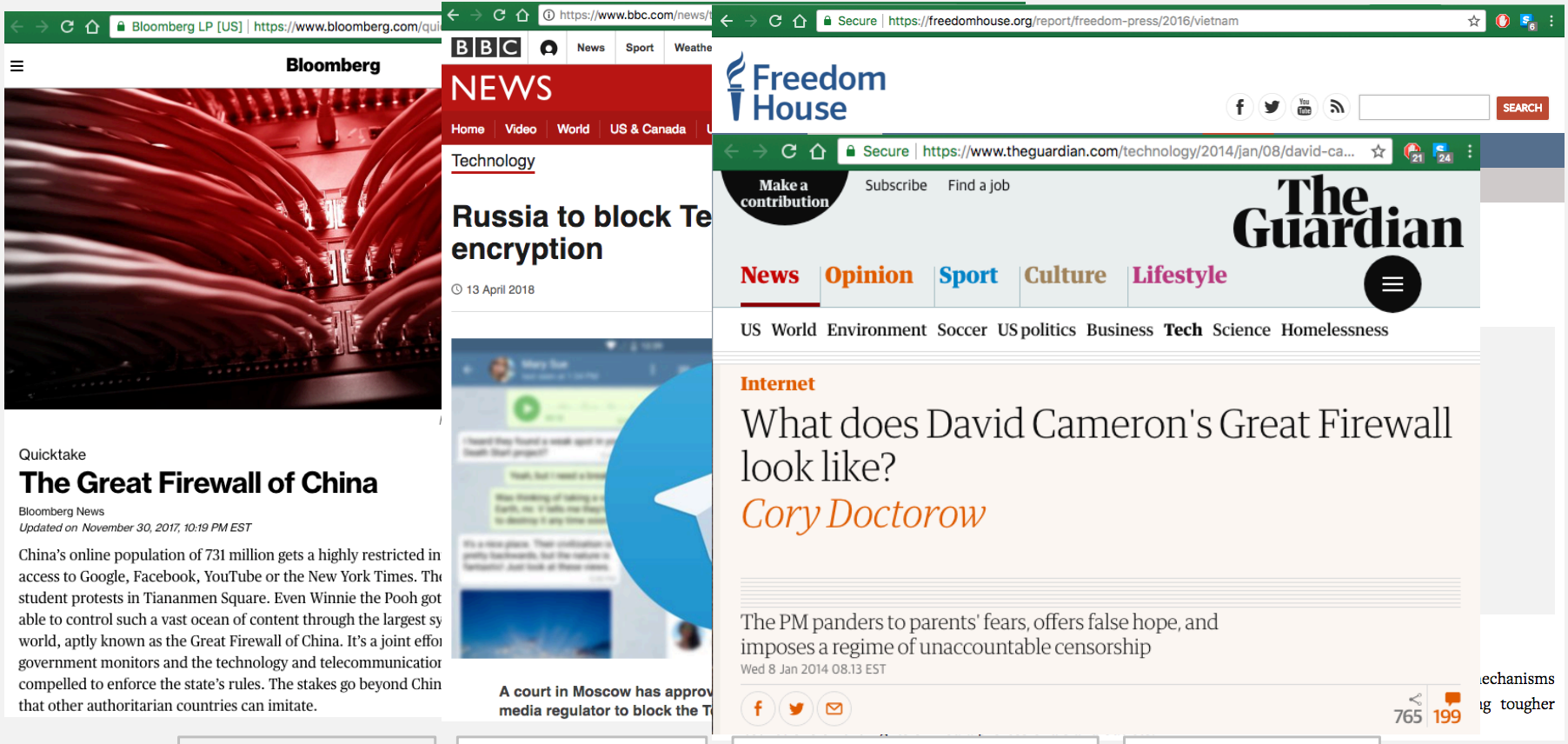
I2P

FOCI '19

Outline

- I2P – The Invisible Internet Project
- Measurement method
- Experimental results
- Conclusion

Online surveillance and Internet censorship



Circumvention tools



NordVPN

Hotspot Shield

OPENVPN

BLOCKED

I2P

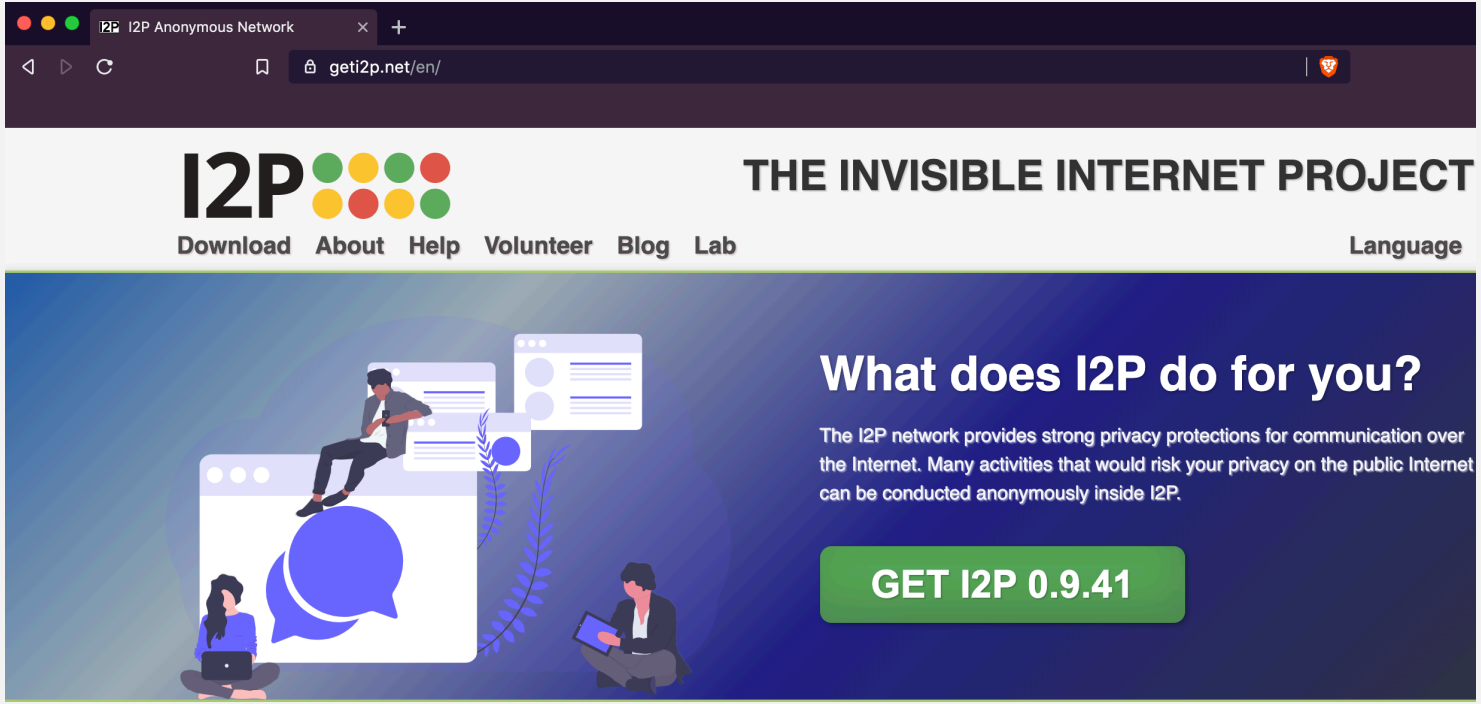
Motivation

Many prior studies have measured censorship on other circumvention tools

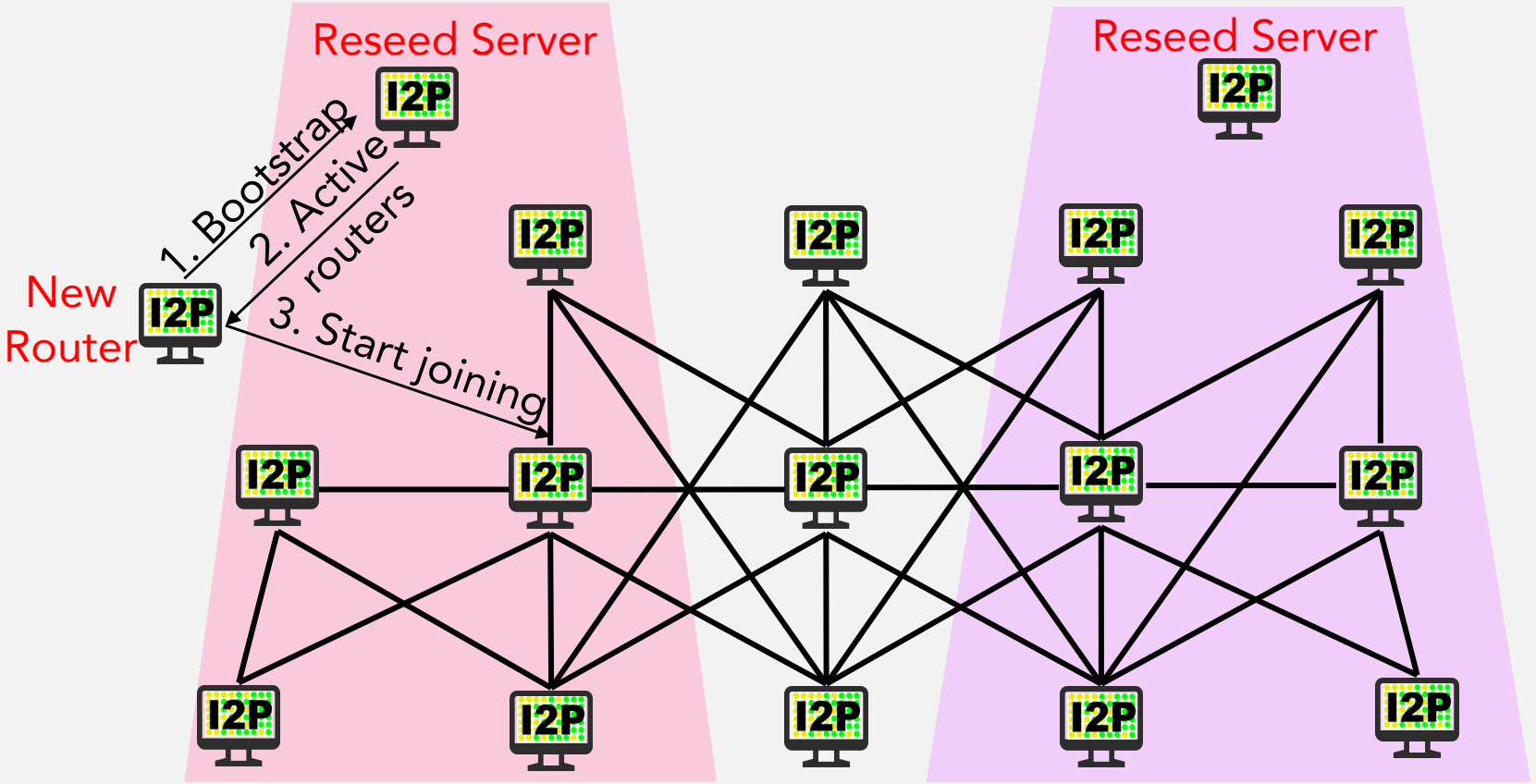
None has investigated the blocking status of I2P at a large scale

I2P typical installation

https://geti2p.net OR http://i2p-projekt.de/



I2P Bootstrapping



Methodology

What to test?

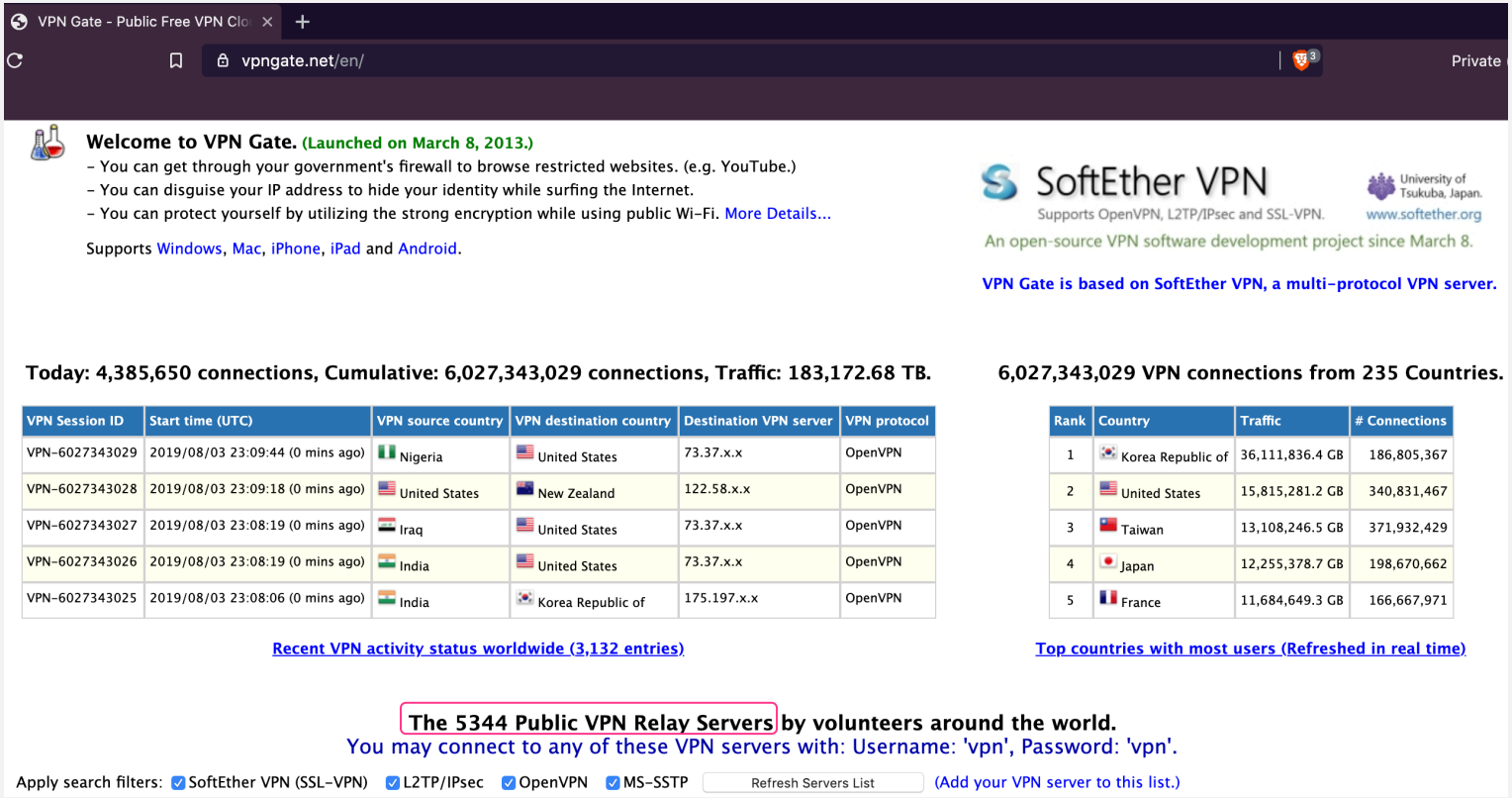
- The official site (https://geti2p.net)
- The mirror site (http://i2p-projekt.de)
- Reseed servers
- Active I2P routers

Methodology

What to test?	DNS	SNI	TCP	Block page
Official site	◉	◉	◉	◉
Mirror site	◉		◉	◉
Reseed servers	◉		◉	
Active I2P routers			◉	

Methodology

How to test?



VPN Session ID	Start time (UTC)	VPN source country	VPN destination country	Destination VPN server	VPN protocol
VPN-6027343029	2019/08/03 23:09:44 (0 mins ago)	Nigeria	United States	73.37.x.x	OpenVPN
VPN-6027343028	2019/08/03 23:09:18 (0 mins ago)	United States	New Zealand	122.58.x.x	OpenVPN
VPN-6027343027	2019/08/03 23:08:19 (0 mins ago)	Iraq	United States	73.37.x.x	OpenVPN
VPN-6027343026	2019/08/03 23:08:19 (0 mins ago)	India	United States	73.37.x.x	OpenVPN
VPN-6027343025	2019/08/03 23:08:06 (0 mins ago)	India	Korea Republic of	175.197.x.x	OpenVPN

Rank	Country	Traffic	# Connections
1	Korea Republic of	36,111,836.4 GB	186,805,367
2	United States	15,815,281.2 GB	340,831,467
3	Taiwan	13,108,246.5 GB	371,932,429
4	Japan	12,255,378.7 GB	198,670,662
5	France	11,684,649.3 GB	166,667,971

DNS-based blocking

China is dominant in terms of DNS-based blocking, poisoning the official domain and 3 reseed servers.

64.33.88.0	**66.220.152.0**	67.228.235.0
203.161.230.0	**66.220.149.0**	67.228.126.0
31.13.72.0	**31.13.84.0**	174.37.175.0
4.36.66.0	75.126.33.0	**31.13.97.0**
74.86.151.0	**69.171.247.0**	**31.13.73.0**
74.86.12.0	**69.171.237.0**	208.101.60.0
69.63.184.0	**69.171.234.0**	199.59.148.0
69.171.229.0	**69.171.233.0**	199.59.149.0

Leakage of DNS Injection

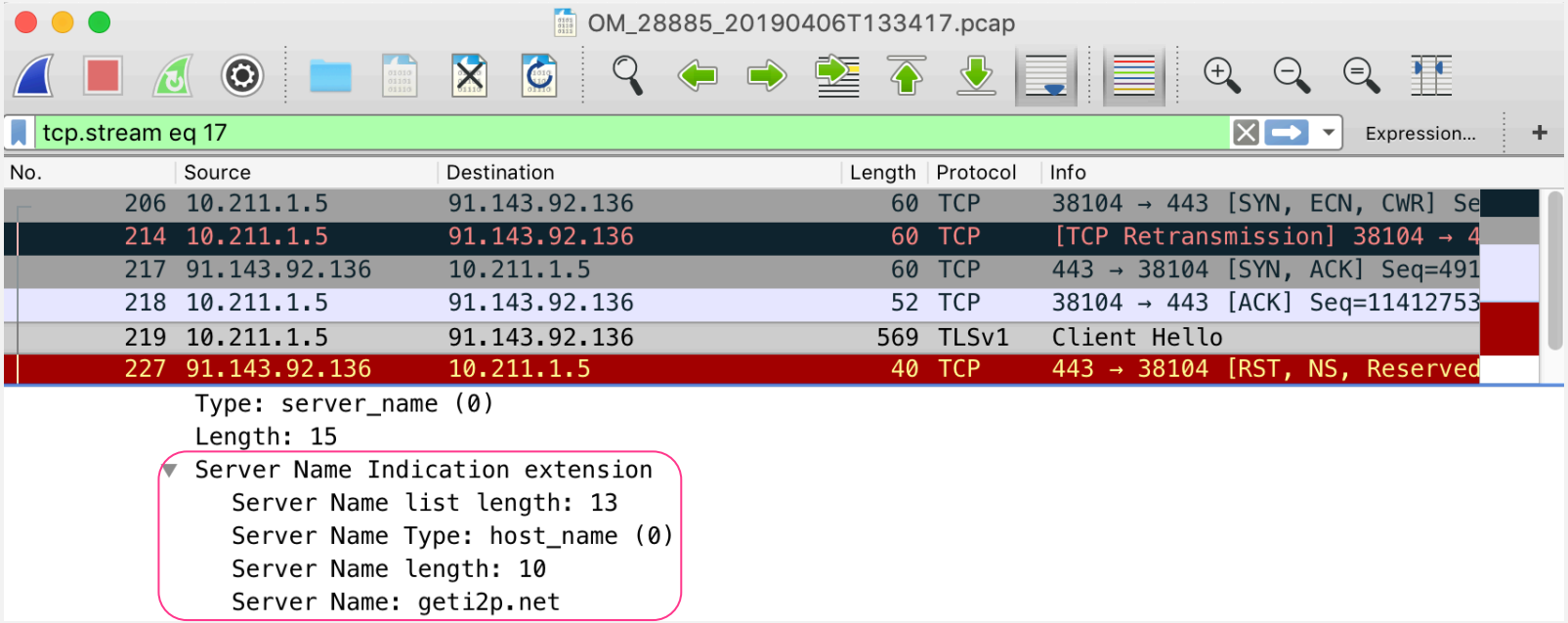
Similar poisoned DNS responses were also detected at two network locations in South Korea:

- AS38676 flexnetworks
- AS9848 Sejong Telecom

Only responses from open resolvers were poisoned, those from local recursive resolvers were not

SNI-based blocking

SNI-based blocking was detected in Oman and Qatar when visiting the official homepage (https://geti2p.net)



SNI-based blocking

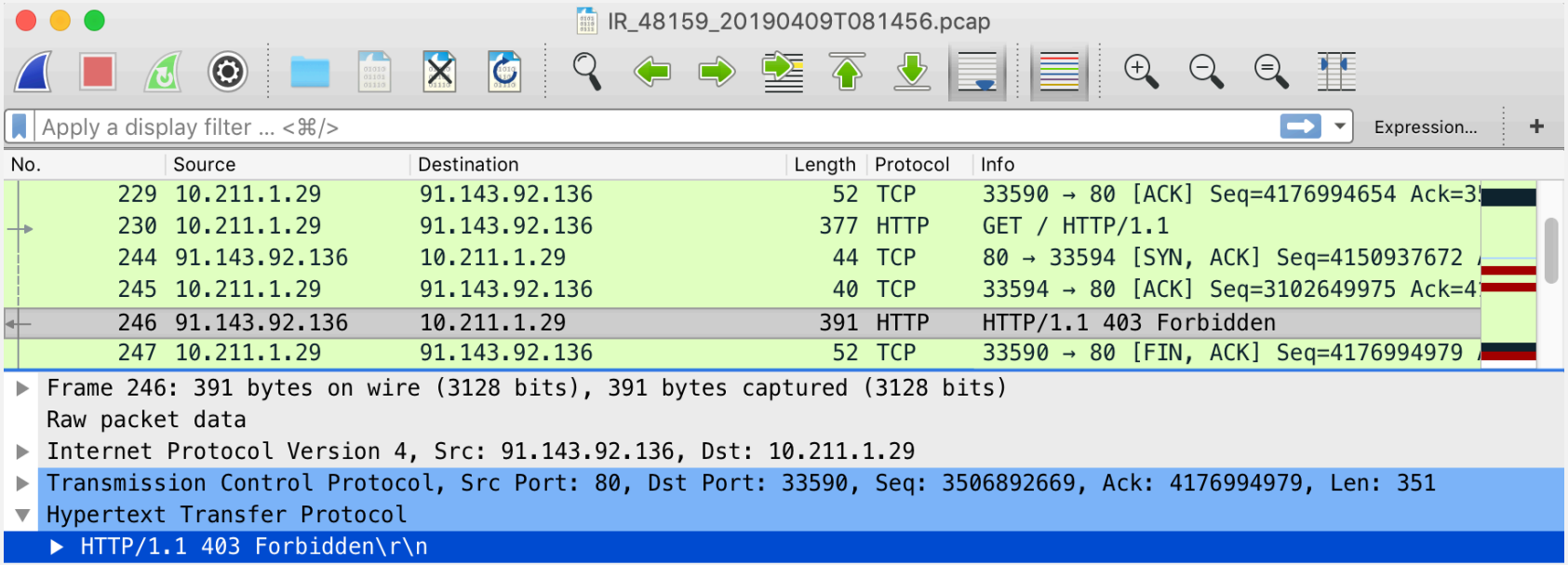
China, however, doesn't block the official homepage (https://geti2p.net) using SNI-based blocking

OONI recently reported that China employs both DNS-based and SNI-based blocking to censor Wikipedia

→ The Great Firewall applies different blocking techniques on different domains and services

TCP Packet Injection

TCP packet injection was detected in Iran, Oman, Qatar, and Kuwait when visiting the mirror site (http://i2p-projekt.de)



Block page

Oman's block page delivered through TCP injection when visiting the mirror site (http://i2p-projekt.de)



Block page

Qatar's block page delivered through TCP injection when visiting the mirror site (http://i2p-projekt.de)



Block page

AS47589 Kuwait Telecom Company's block page delivered through TCP injection when visiting the mirror site (http://i2p-projekt.de)

No block page was detected at other 5 networks: AS3225, AS42961, AS9155, AS6412, and AS196921



Summary of censored countries

Country	Domain-name-based blocking		TCP packet injection	Block page
	DNS	SNI		
China	geti2p.net reseed.i2p-projekt.de netdb.i2p2.no i2p.mooo.com	N/A	N/A	N/A
Iran	N/A	N/A	i2p-projekt.de	N/A
Oman	N/A	geti2p.net	geti2p.net i2p-projekt.de	i2p-projekt.de
Qatar	N/A	geti2p.net	geti2p.net i2p-projekt.de	i2p-projekt.de
Kuwait	N/A	N/A	i2p-projekt.de	i2p-projekt.de

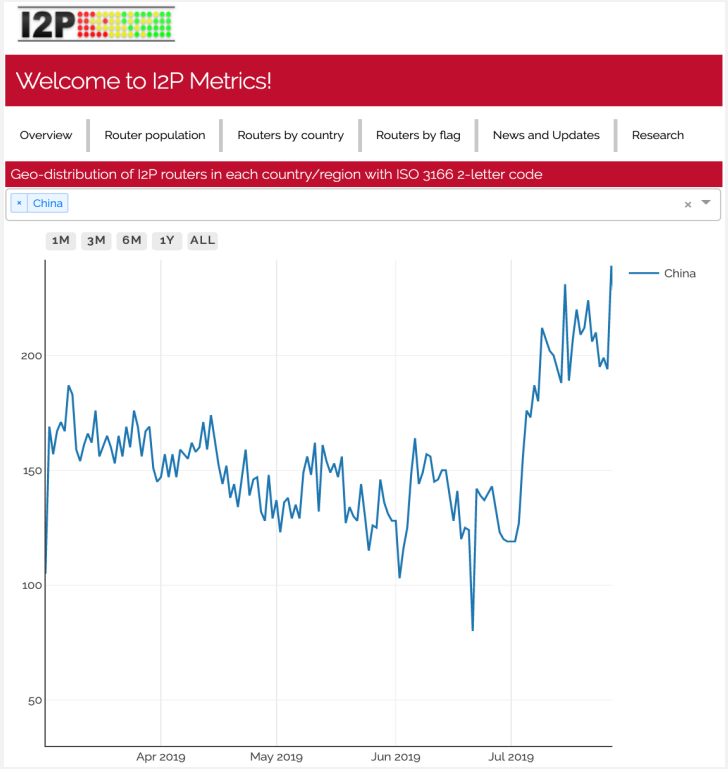
Discussion

Encrypted domain name resolution can remedy DNS-based blocking in China

Encrypted Server Name Indication may change the way censors block sites

Is IP-based blocking an effective next option?

Hoang et al. IMC' 18



Conclusion

Within a period of one month, we conducted a total of 54K measurements from 1.7K networks in 164 countries

Using different techniques to detect DNS poisoning, SNI-based blocking, network packet injection, and block pages, we discovered I2P blocking attempts in China, Iran, Oman, Qatar, and Kuwait

I2P

Important Notice

Measuring I2P Censorship at a Global Scale

Q&A