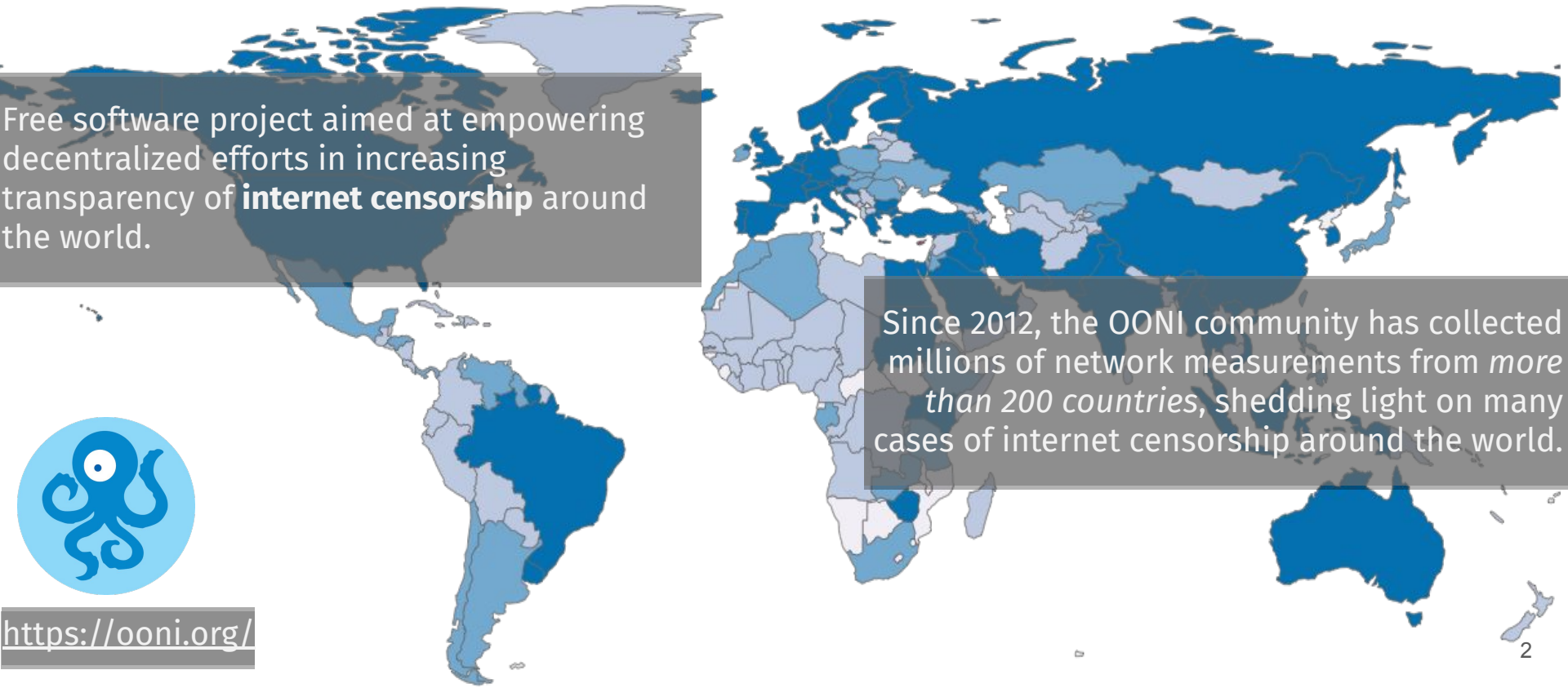
DNS Privacy Workshop 2021 @ NDSS

Measuring DoT/DoH Blocking with OONI: a Preliminary Study

Simone Basso (OONI)

21st February 2021

OONI: Open Observatory of Network Interference

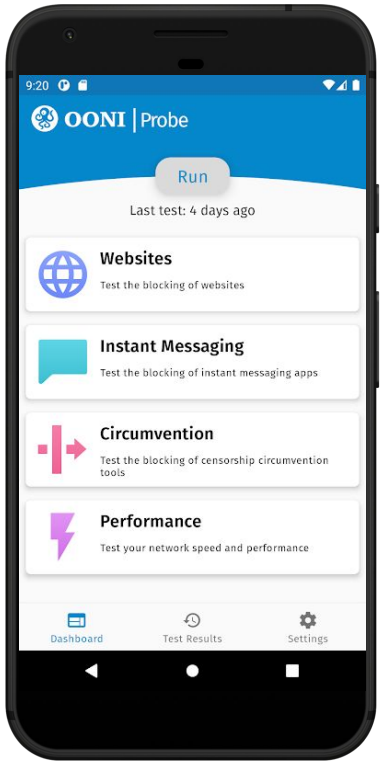


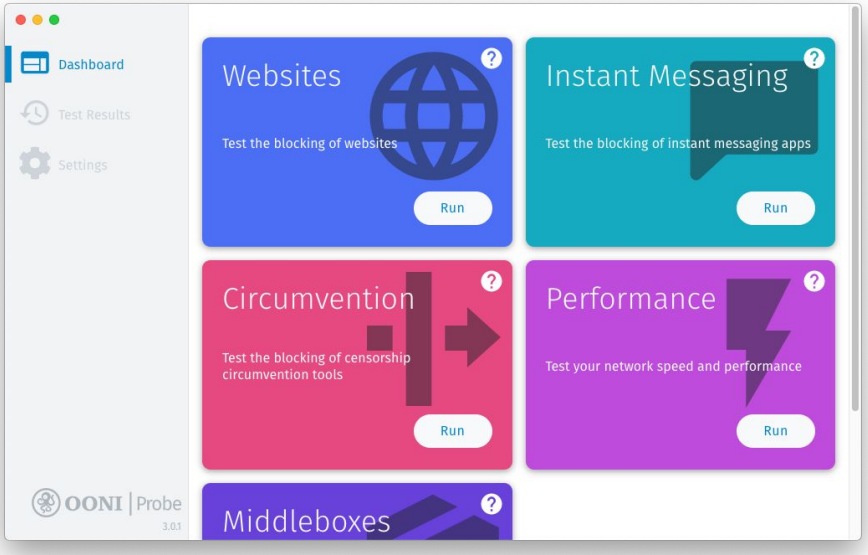
Free software project aimed at empowering decentralized efforts in increasing transparency of **internet censorship** around the world.

Since 2012, the OONI community has collected millions of network measurements from *more than 200 countries*, shedding light on many cases of internet censorship around the world.

https://ooni.org/

OONI Probe (https://ooni.org/install)

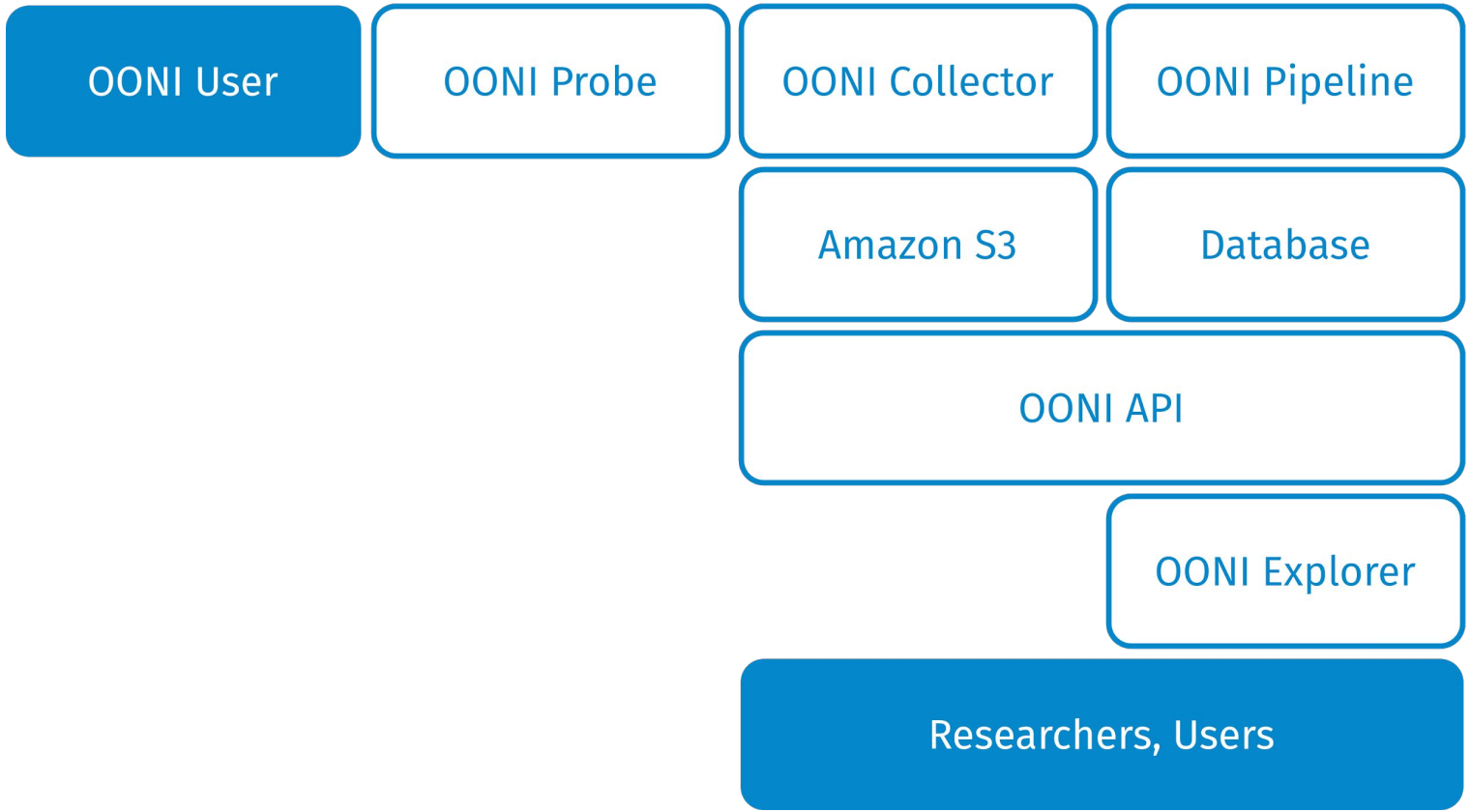




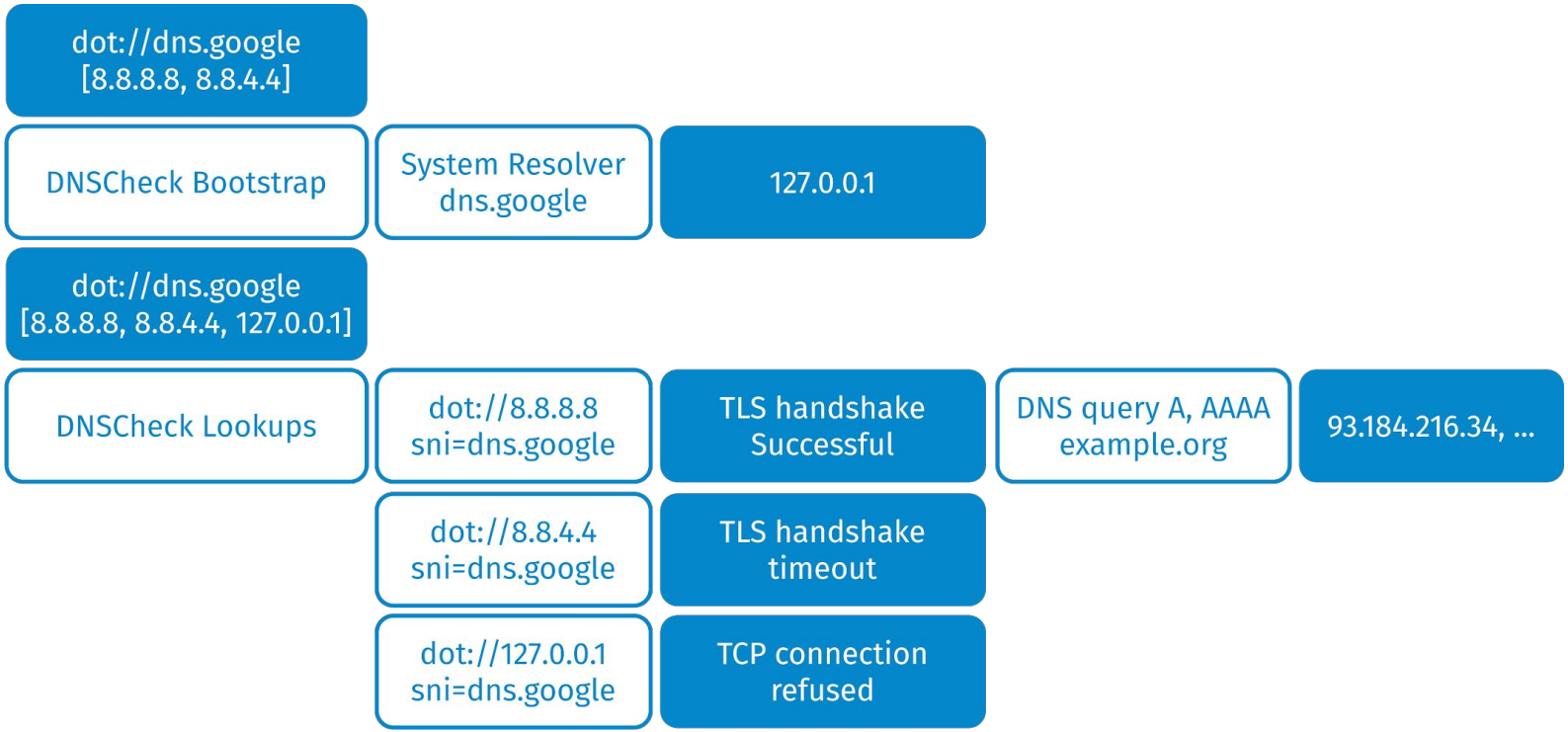
Motivations for Measuring DoT/DoH Blocking

Image source: https://en.wikipedia.org/wiki/Peace_of_M%C3%BCnster

Value Chain of a OONI Measurement



The DNSCheck Experiment



Measurements campaign

- From 15th December 2020 to 10th January 2021
- 123 DoT/DoH services (=> 461 TCP/QUIC endpoints)
- The paper and this presentation focus on DoH over TCP only
- We used an experimental CLI client (miniooni)

Country	ASN	Type
Kazakhstan	AS48716	VPS
Iran	AS197207	Mobile
China	AS45090	VPS

Main Findings

	Kazakhstan	Iran	China
Successful DoT lookups	8157 (95%)	1156 (50%)	4332 (93%)
Successful DoH lookups	16466 (82%)	4824 (92%)	9414 (89%)

- Most endpoints fail or succeed consistently
- 1.1.1.1:853 and 1.0.0.1:853 were blocked and unblocked frequently in KZ
- Same for 1.1.1.1:853 in IR
- dot://dot-jp.blahdns.com was unblocked in CN around 1st January 2021
- dns.adguard.com resolved to 10.10.34.36 in IR

Classification of Failed Endpoints by Resolver

Resolver	Kazakhstan		Iran		China	
	DoT	DoH	DoT	DoH	DoT	DoH
Cloudflare (AS13335)	408 (91%)	3109 (88%)	158 (14%)	52 (13%)	230 (74%)	532 (47%)
Others	38 (9%)	413 (12%)	976 (86%)	337 (87%)	81 (26%)	590 (53%)

Distribution of Lookups Failures (DoT)

Failure	Kazakhstan	Iran	China
Timeout after* the TLS handshake	323 (72%)	79 (7%)	2 (~0%)
TLS handshake timeout	88 (20%)	906 (80%)	63 (20%)
Connect timeout	1 (~0%)	72 (6%)	233 (75%)
RST during TLS handshake	1 (~0%)	74 (7%)	0 (0%)
Other	33 (8%)	3 (~0%)	13 (~5%)

*The client thinks the TLS handshake is over because it sends the final messages, and some application data, but it will later need to retransmit them and eventually times out.

Distribution of Lookups Failures (DoH)

Failure	Kazakhstan	Iran	China
Timeout after the TLS handshake	2701 (77%)	160 (41%)	3 (~0%)
TLS handshake timeout	331 (9%)	1 (~0%)	61 (5%)
Connect timeout	397 (11%)	72 (19%)	813 (72%)
RST during TLS handshake	1 (~0%)	77 (20%)	152 (14%)
Other	92 (3%)	79 (20%)	93 (9%)

SNI-based blocking in Kazakhstan (DoH)

Address	SNI	Result	Frequency
2606:4700::6810:f8f9	cloudflare-dns.com	Timeout after the TLS handshake	85 (99%)
2606:4700::6810:f8f9	cloudflare-dns.com	Connect timeout	1 (1%)
2606:4700::6810:f8f9	mozilla.cloudflare-dns.com	Success	88 (100%)

Endpoint-based Blocking in Iran (DoT)

Address	SNI	Result	Frequency
8.8.4.4	8888.google	TLS handshake timeout	40 (100%)
8.8.4.4	null	TLS handshake timeout	40 (100%)
8.8.8.8	8888.google	Success (TLSv1.3)	40 (100%)

TCP-based Blocking in China (DoT)

Address	SNI	Result	Frequency
1.1.1.1	1dot1dot1dot1.cloud...	Connect timeout	77 (100%)
1.1.1.1	one.one.one.one	Connect timeout	77 (100%)
1.1.1.1	null	Connect timeout	76 (100%)

Future Work

- Make DNSCheck available to all OONI Probe users
- Continue studying QUIC blocking
- Experiment with cloudflare/go to use Encrypted Client Hello
- “Parrot” the fingerprint of popular TLS implementations

Thank you!

contact@openobservatory.org

https://slack.ooni.org/

@OpenObservatory

https://github.com/ooni