

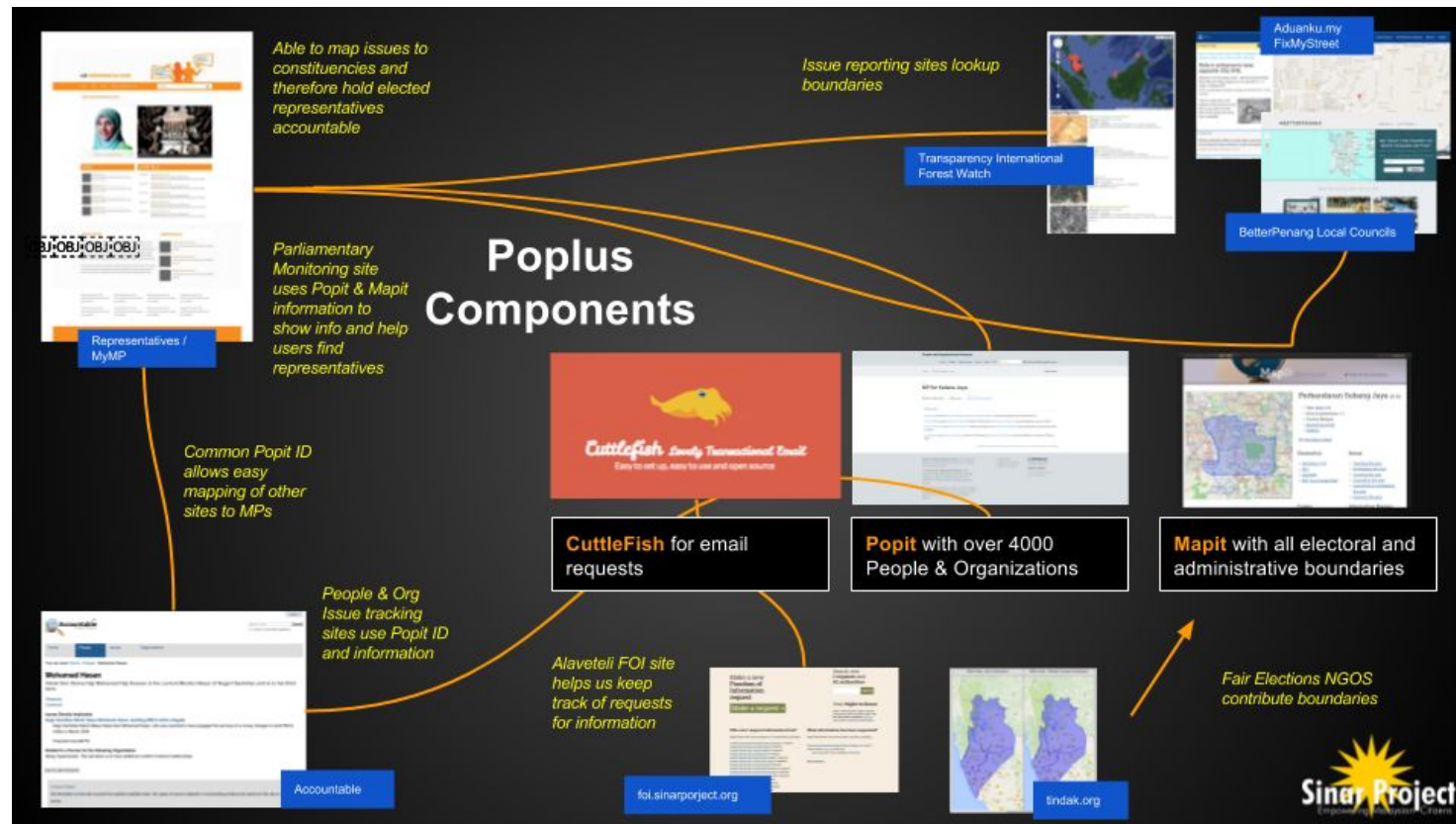


## **Collecting Evidence of Internet Censorship**

### **in Southeast Asia and Beyond**

RightsCon, 30<sup>th</sup> March 2017

Ng Swee Meng (Sinar Project) & Maria Xynou (OONI)



Sinar Project is an initiative using open technology and applications to systematically make important information public and more accessible to the Malaysian people.

Our project relies on web services, thus censorship can affect our project. Thus we start investigating censorship situation in Malaysia more deeply. Thus we use ooni for this work

Free software project (under the Tor Project) aimed at empowering decentralized efforts in increasing transparency of **Internet censorship** around the world.



Since 2012, OONI has collected millions of network measurements *across more than 100 countries* around the world, shedding light on various instances of network interference.



<https://ooni.torproject.org>

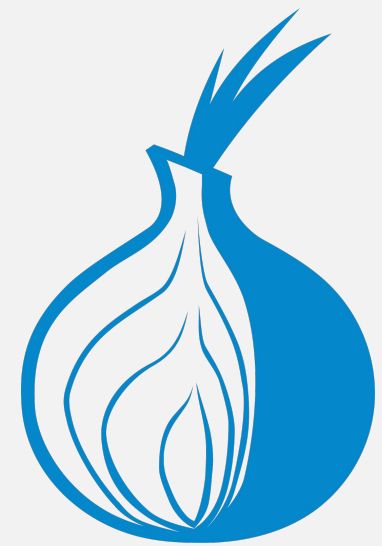
# OOONI: Open Observatory of Network Interference



Blocking of **websites**



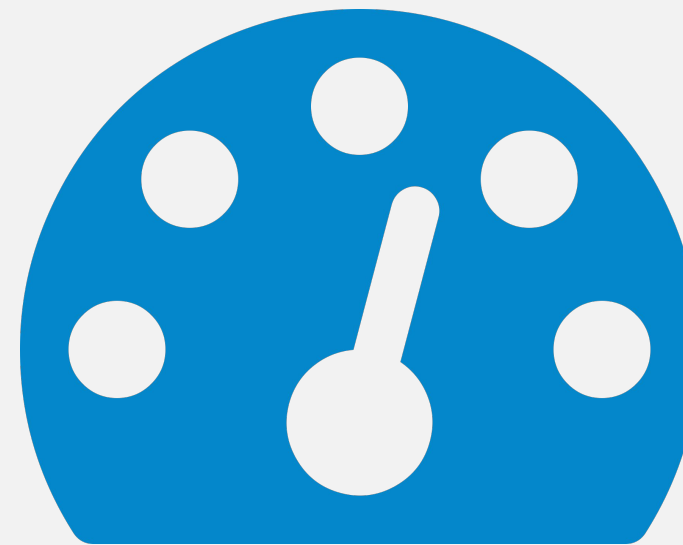
Blocking of **instant messaging apps**



Blocking of **censorship circumvention tools**



Detection of **middle boxes**



Measurement of network **speed & performance**

# OOONI Software Tests

# Examining Internet censorship in Southeast Asia

# Malaysia



**39 websites** found to be blocked through the DNS injection of block pages.

News outlets, blogs, and medium.com blocked for covering the 1MDB scandal.

<https://ooni.torproject.org/post/malaysia-report/>

# Network Landscape



**21 Million internet user** as of 2016

**68% internet penetration**

**Five ISP** each provide mobile and/or fiber to home

<https://ooni.torproject.org/post/malaysia-report/>

# Legal background



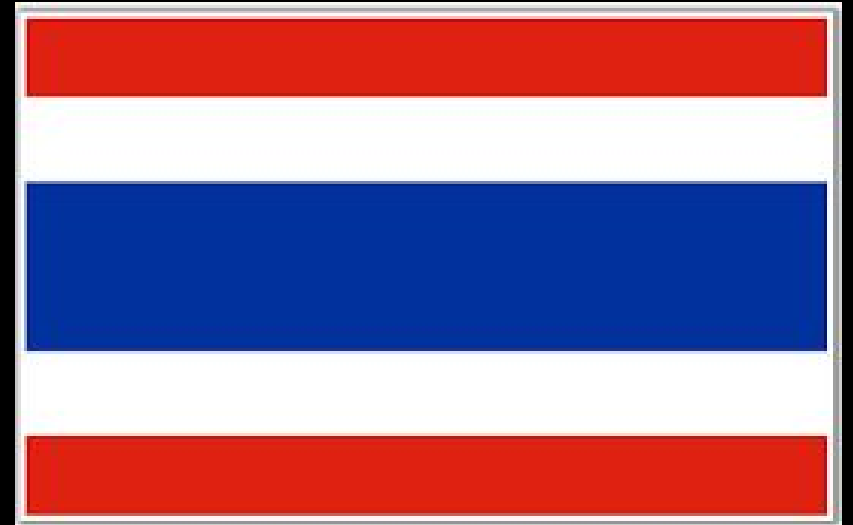
Law on site blocking is via  
Communication Multimedia Act

There's other law, mostly involve jail  
time but not internet shutdown, thus out  
of scope of ooni

<https://ooni.torproject.org/post/malaysia-report/>



# Thailand

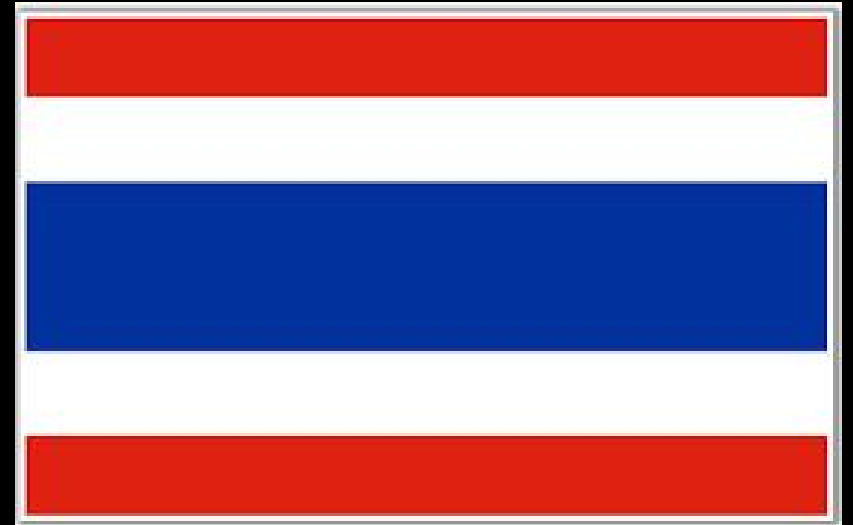


Blocked sites include:

- News outlets (nypost.com, dailymail.co.uk)
- 
- Wikileaks.org
- 
- Circumvention tool sites (e.g. hotspotshield.com)

<https://ooni.torproject.org/post/thailand-internet-censorship/>

# Network landscape



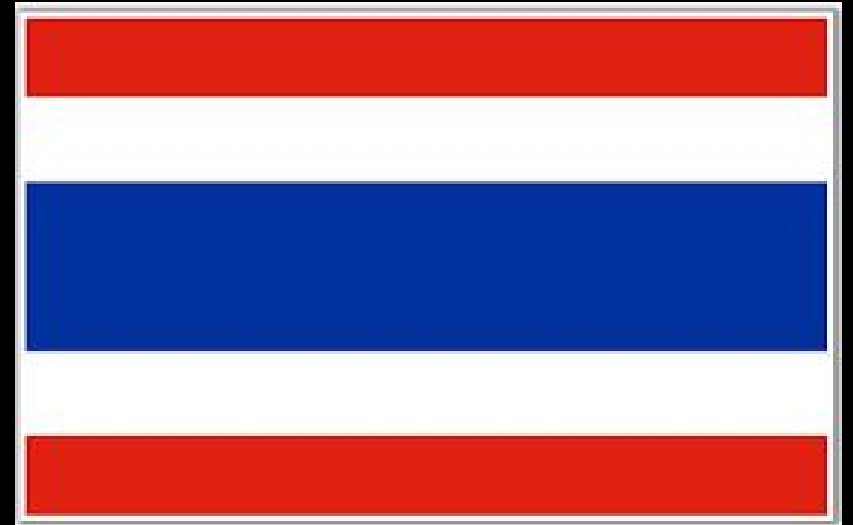
7 major ISP 6 providing mobile internet

59.8% internet penetration rate in 2016

Because of relationship between ISP and official, ISP will cooperate with censorship

<https://ooni.torproject.org/post/thailand-internet-censorship/>

# Legal Background



Law that create censorship:

Lèse-majesté law

Computer Related Crime Act

ISA

<https://ooni.torproject.org/post/thailand-internet-censorship/>

# Myanmar



The sites of the U.S embassy in Myanmar and of the Organization of American States (OAS) presented strong signs of TCP/IP and HTTP blocking.

Blue Coat software was detected by ooniprobe in 2012. No signs of this software appeared to currently be present in the 6 networks where tests were recently run.

# Network landscape



19% internet penetration on 2016

Only Myanmar Posts and Telecom (MPT) and Bagan Cybertech (currently Yatanarpon Telecom) are available to user

Both are controlled by government

# Legal background



Telecommunication Law 2013 allows the government to censor information/setup surveillance

There is also other law, like Computer Science Development, for permit to import computing equipment, defamation law etc.

This involve jailtime

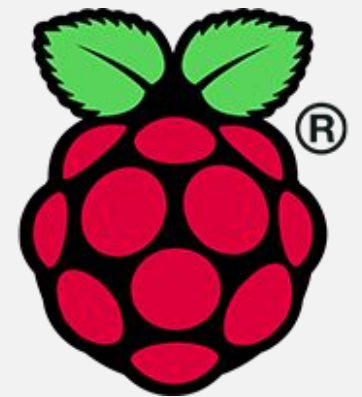
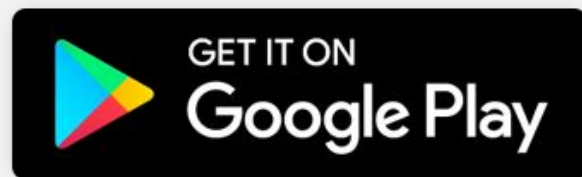
# How to collect evidence of Internet censorship in your country

Linux or  
macOS

Android

iOS

RaspberryPi




Running ooniprobe





# ooniprobe Dashboard

ooniprobe 2.2.0.rc1 | **running**  | Location: IS (AS47172)

Test Tor



Test the Web



Test Instant Messaging Apps



Test for Middle Boxes

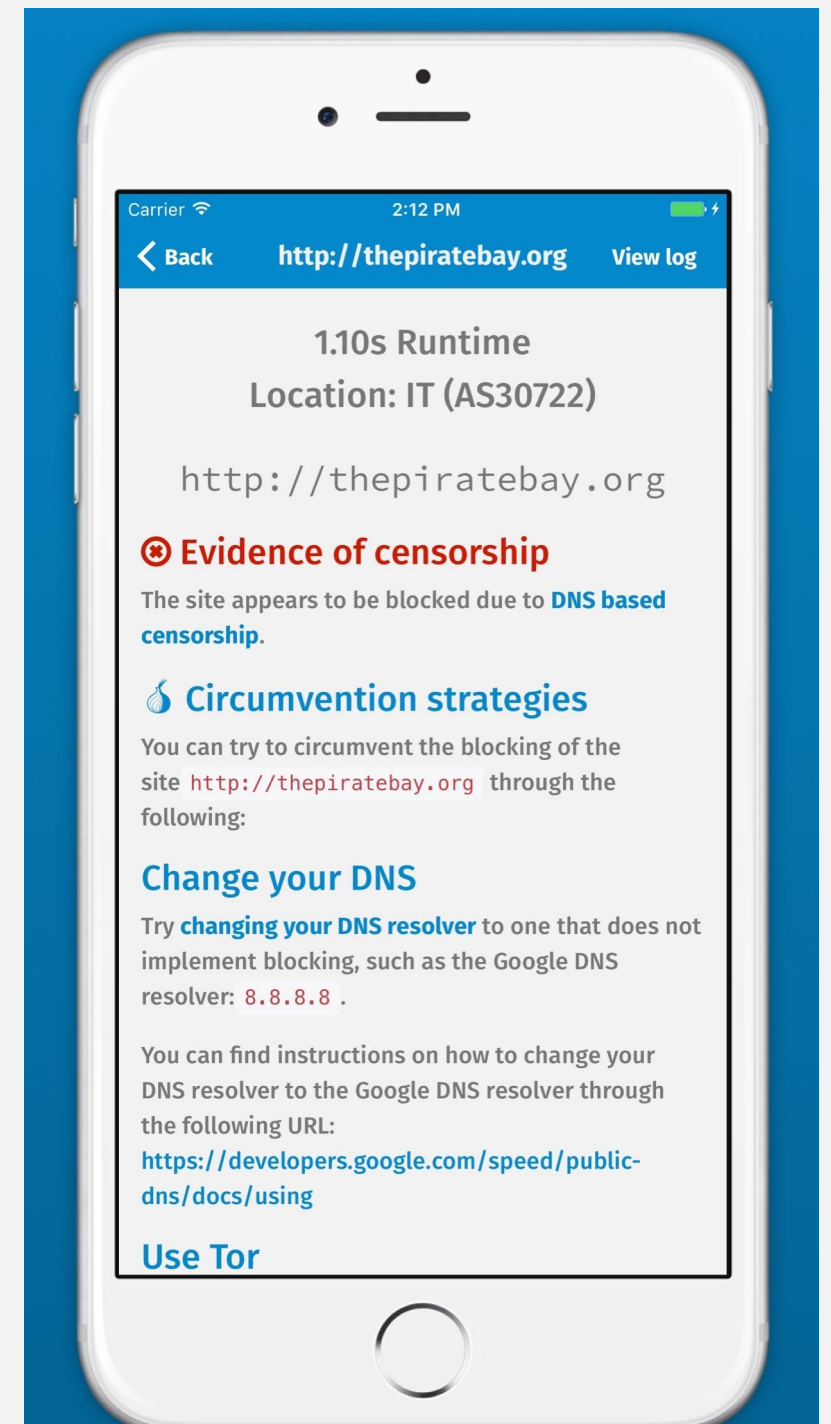
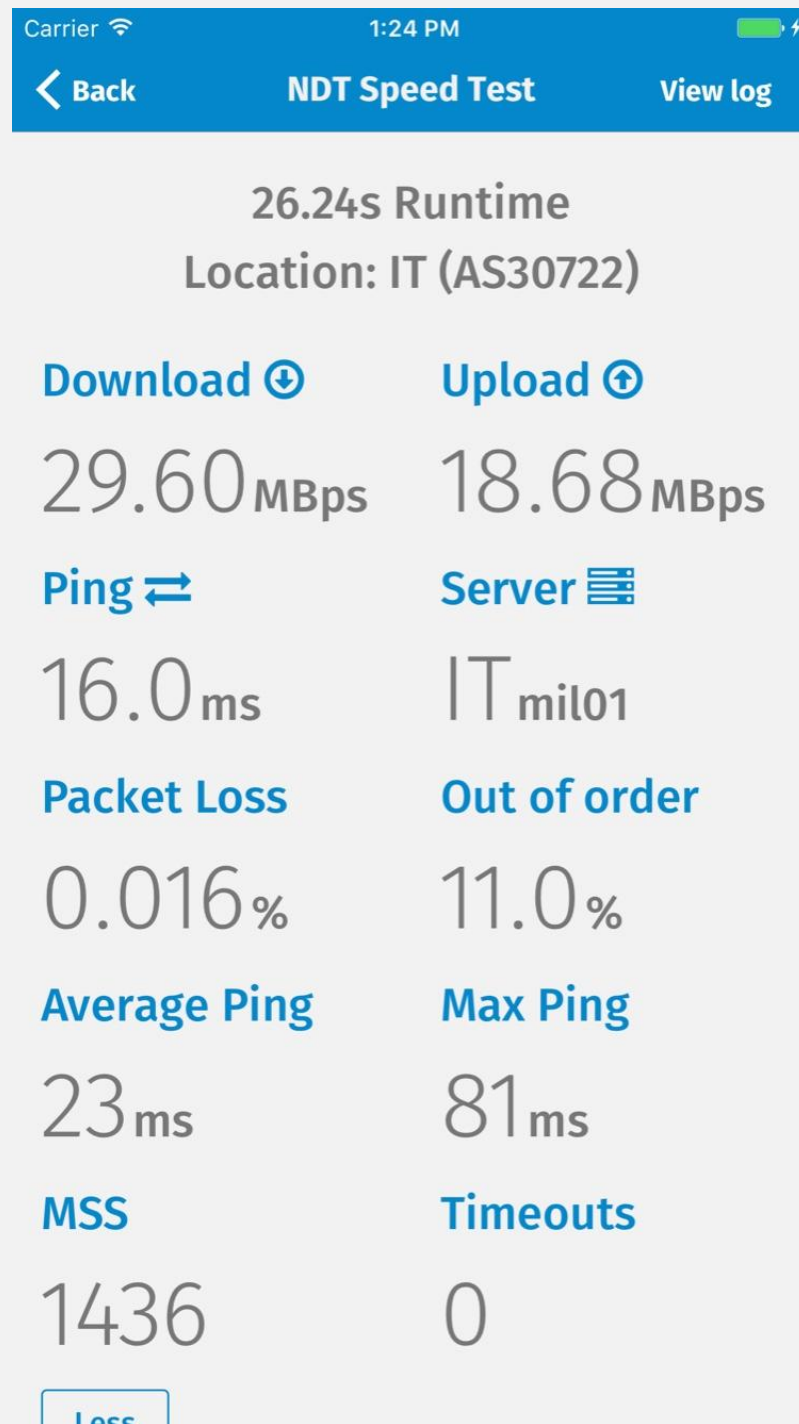
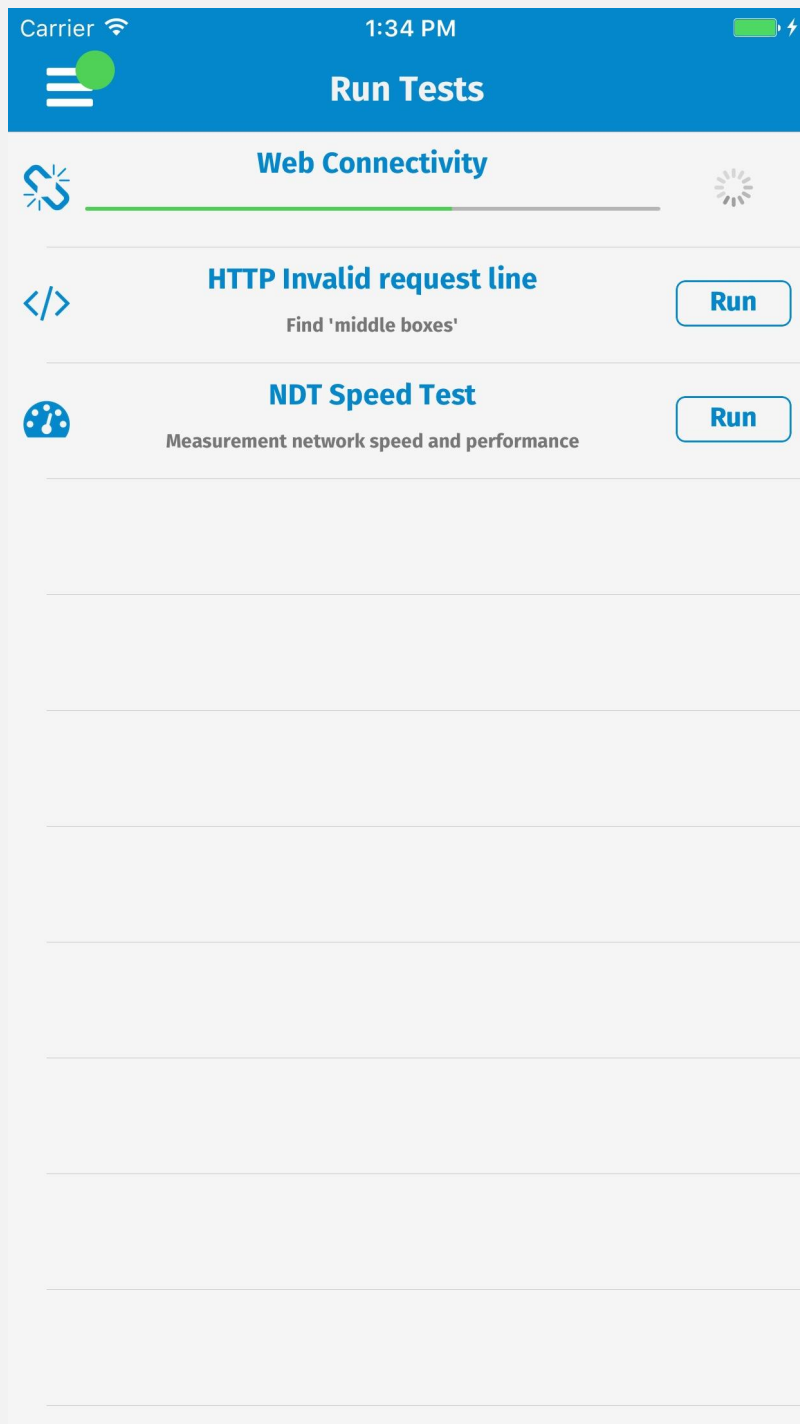


Your recent test results will appear here once the tests have finished running! As you run more tests, you can view past results in the "Measurements" page.

# ooniprobe Web User Interface (macOS & Linux)



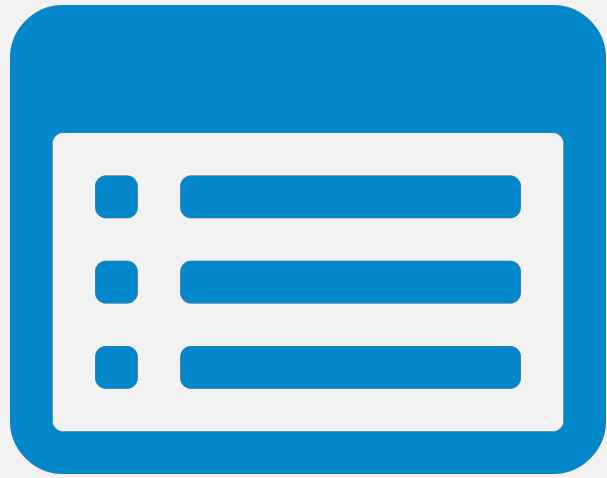
Raspberry Pi



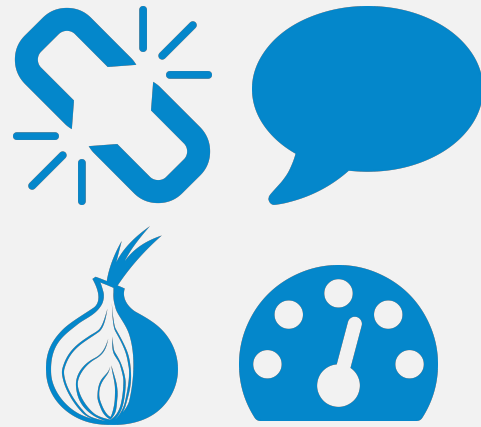
ooniprobe mobile app

- 
- Anyone monitoring your internet activity (e.g. ISP) will know that you are running ooniprobe.
- 
- Types of URLs tested include provocative or objectionable sites (e.g. pornography).
- 
- OONI's “HTTP invalid request line” test could be viewed as a form of “hacking”.
- 
- The use of ooniprobe might potentially be viewed as illegal or anti-government activity.
- 
- *<https://ooni.torproject.org/about/risks/>*

Risks: ooniprobe is a tool for investigations!



Contribute to test lists



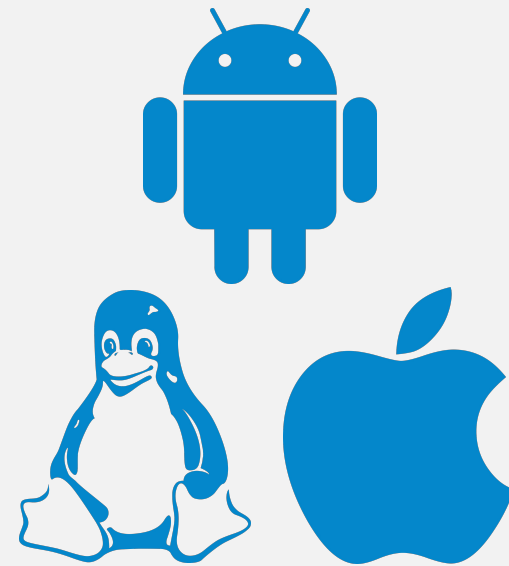
Types of test to run



Privacy settings



How you upload data



Platform for running ooniprobe

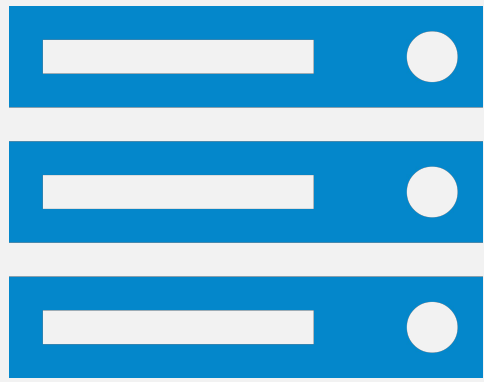
Choices you can make

- 
- **Global list:** Internationally relevant websites
- 
- **Country-specific lists:** Websites that are relevant to a specific country
- 
- How to contribute to test lists:
- <https://ooni.torproject.org/get-involved/contribute-test-lists/>
- 
- Citizen Lab github repo:
- <https://github.com/citizenlab/test-lists>

Test lists:

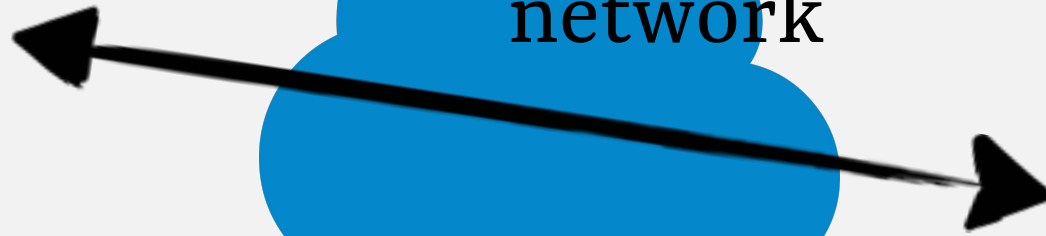
Determining which sites to test for censorship

Control



Probe

Uncensored network

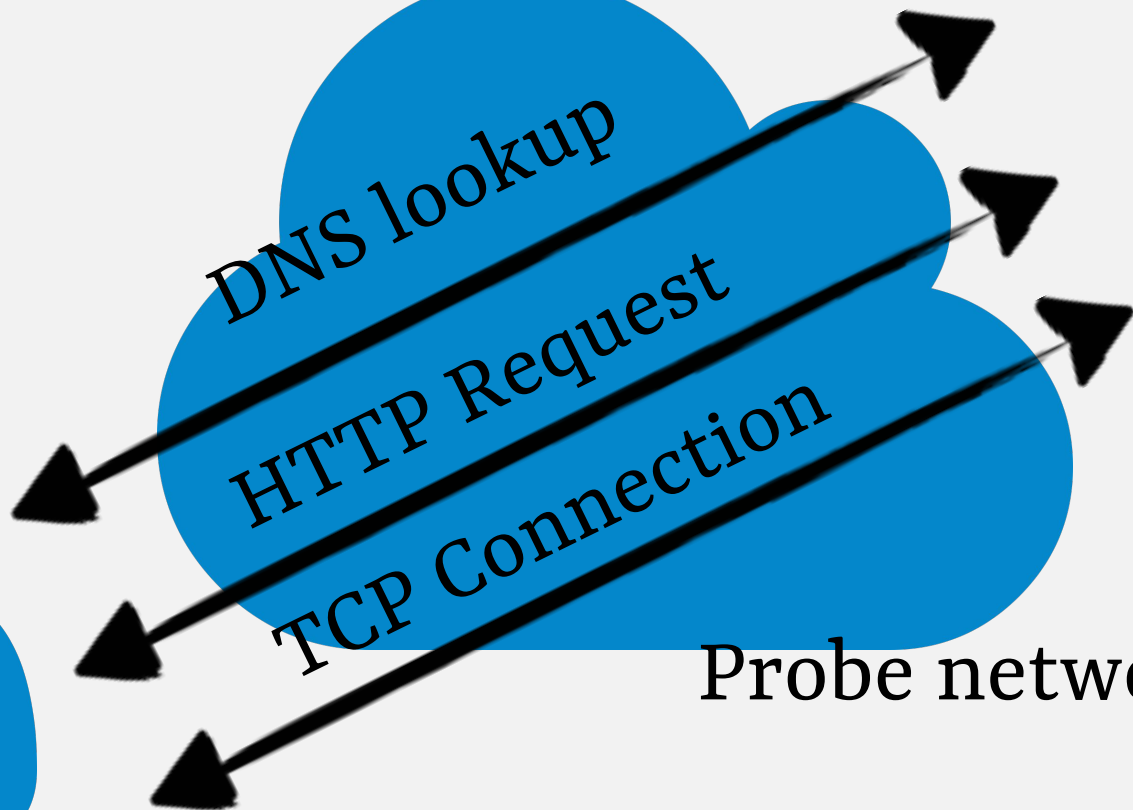


Website

DNS lookup

HTTP Request

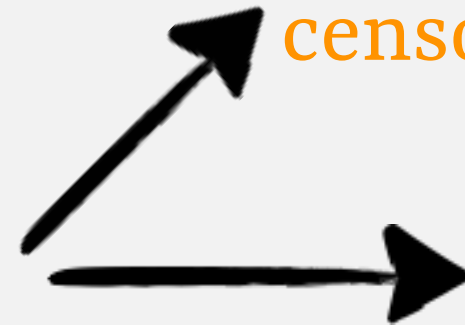
TCP Connection



Probe network

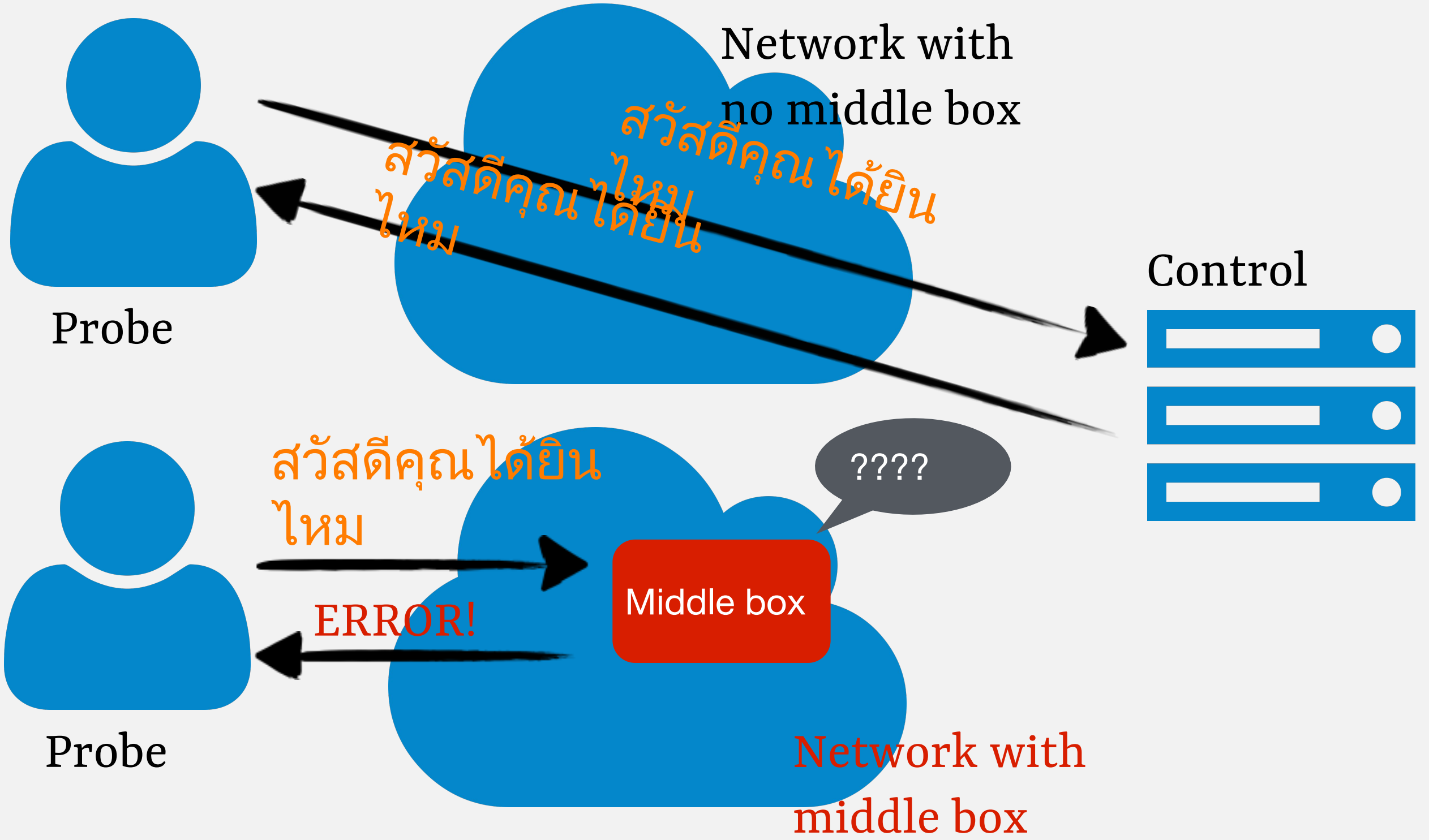
If **Control** != **Experiment**

Possible censorship



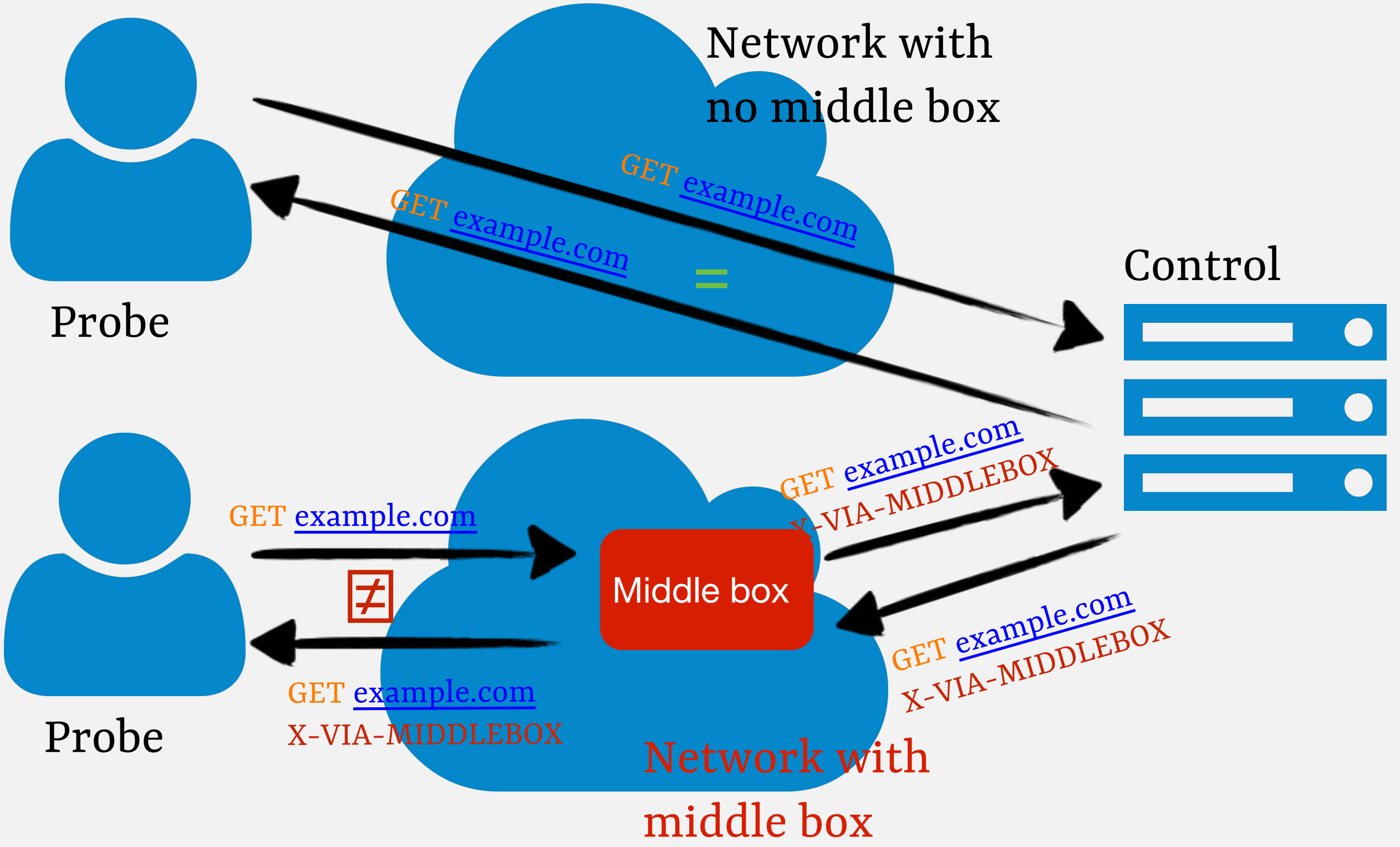
OK

# Web Connectivity



# HTTP Invalid Request Line





# HTTP Header Field Manipulation

- 
- Country code (e.g. BR for Brazil)
- 
- Autonomous System Number (ASN)
- 
- Date & time of measurements
- 
- Network measurement data (depending on the type of test)
- 
- *Note:* IP addresses & other potentially identifying information might unintentionally be collected.
- 
- **OOONI Data Policy:** <https://ooni.torproject.org/about/data-policy/>

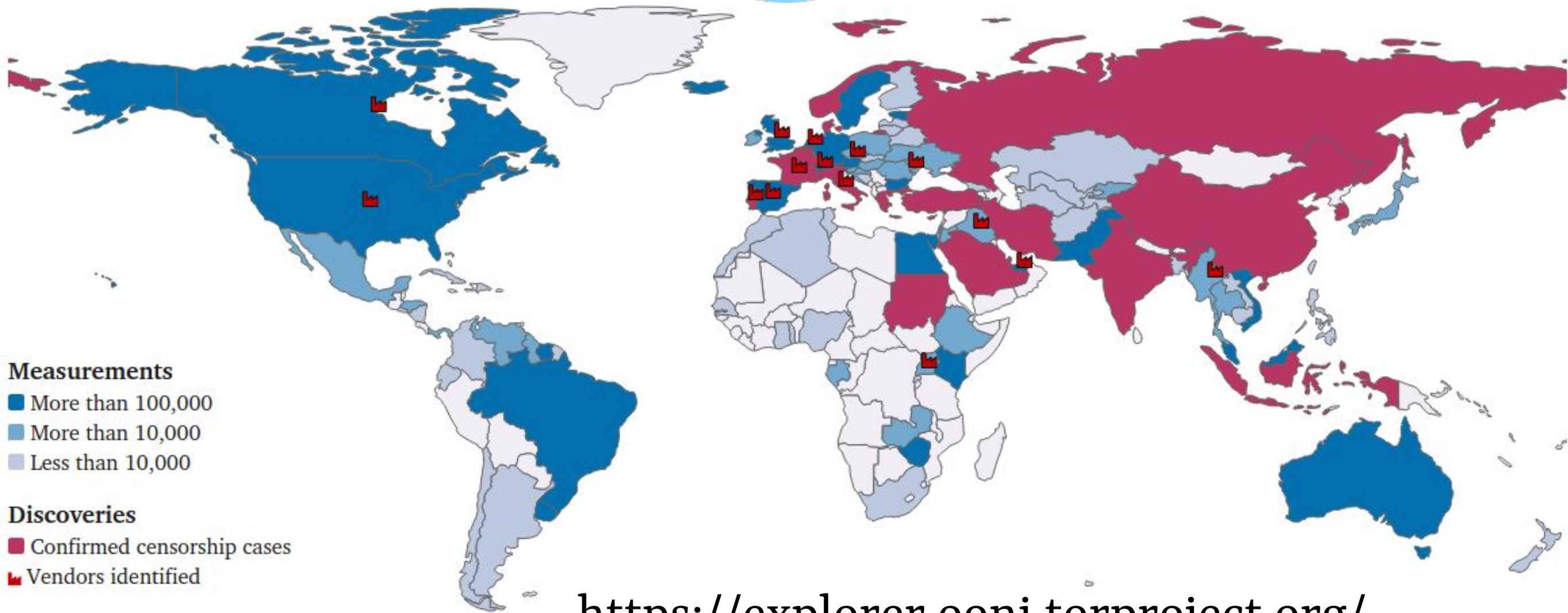
# Data ooniprobe collects

- 
- Tor hidden services (recommended!)
- 
- HTTPS collectors
- 
- Cloud-fronting

Uploading data to OONI servers

- 
- **Evidence** of censorship events
- 
- **Transparency** of global internet controls
- 
- Allows researchers to conduct **independent studies** & to explore other research questions
- 
- Allows the public to **verify** OONI's findings

# Open Data



# OOONI Explorer

# Welcome to the OONI measurements page

---

Download and search for **raw** OONI measurements

[View files](#)

[API documentation](#)

[Statistics](#)

<https://measurements.ooni.torproject.org/>

# Measurement API

- “Normal” and “anomalous” measurements.
- “Anomalous” measurements *MIGHT* contain evidence of censorship, but not necessarily (i.e. false positives).
- We only confirm a case of censorship when we have detected a **block page**.

Interpreting the data

- OONI Partnership Program
- Monthly community meetings on <https://slack.openobservatory.org>
- Run ooniprobe
- Contribute to test lists
- Analyze the data
- Tell stories
- Host an OONI workshop, spread the word! :)

Get involved!



- **OOONI:** <https://ooni.torproject.org/>
- **Sinar Project:** <http://sinarproject.org/>
- **OOONI Explorer:** <https://explorer.ooni.torproject.org/>
- **Measurement API:** <https://measurements.ooni.torproject.org/>
- **Software:** <https://github.com/TheTorProject/ooni-probe>
- **Email:** [contact@openobservatory.org](mailto:contact@openobservatory.org)
- **Twitter:** @OpenObservatory, @sinarproject
- **IRC:** #ooni ([irc.oftc.net](https://irc.oftc.net)) - <https://slack.openobservatory.org/>

## Resources & contacts