

Open Measurement of Internet Censorship

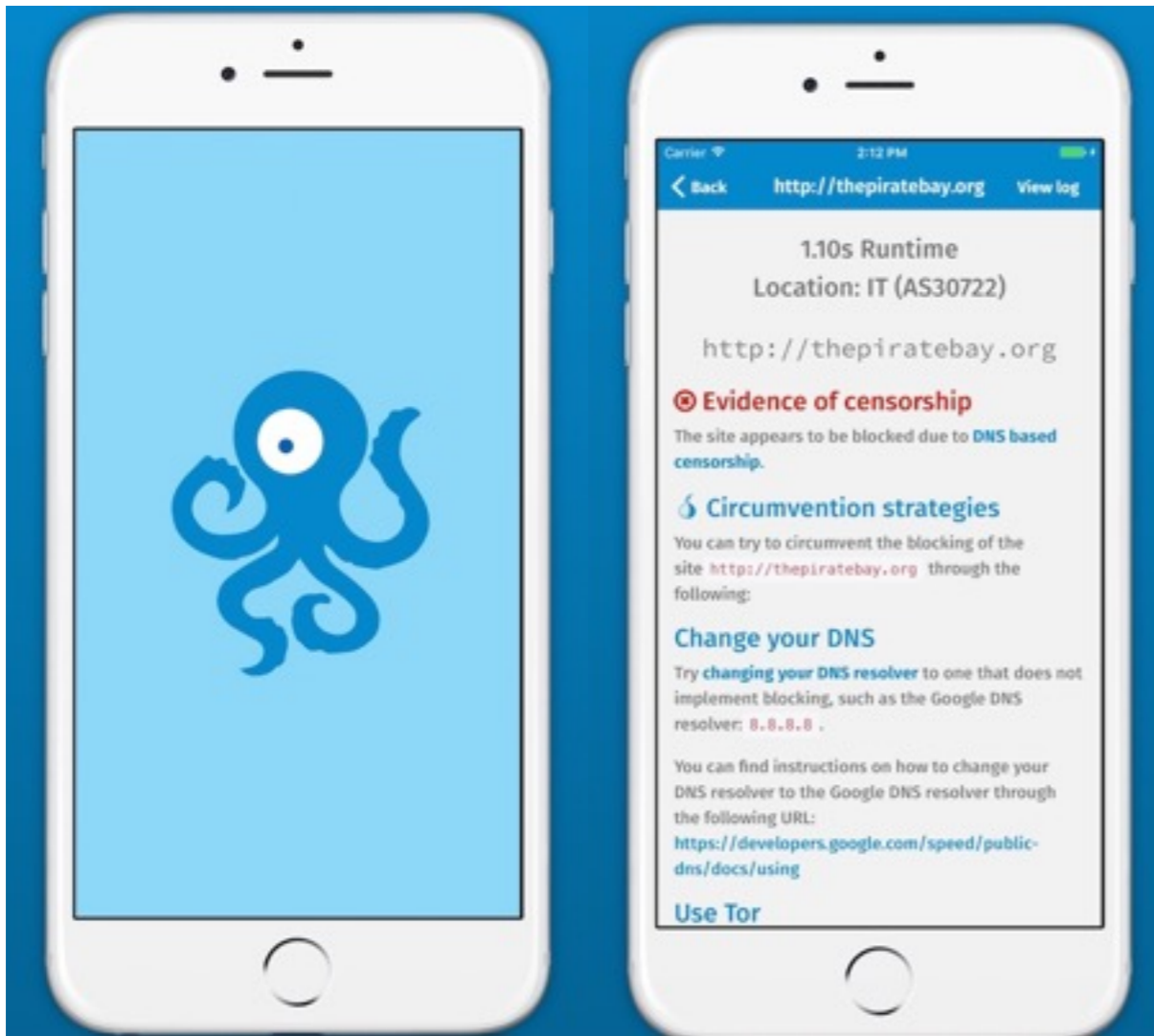
Will Scott
willscott@gmail.com

OONI



<https://ooni.io>

OONI



- Mobile App 2017
- Android, iOS
- HTTP connectivity
- Middle-box Detection
- NDT speed test

OONI



ooniprobe v2.1.0

running:

Country: GR (AS1241)

[home](#)

[decks](#)

[nettests](#)

[measurements](#)

[logs](#)

Web connectivity

blocking version: 0.1.0

Identifies the reason for blocking of a given URL by performing DNS resolution of the hostname, doing a TCP connect to the resolved IPs and then fetching the page and comparing all these results with those of a control.

[More Info](#)

[Run](#)

Whatsapp

blocking version: 0.5.0

This test checks to see if the servers used by whatsapp messenger are reachable

[More Info](#)

[Run](#)

Facebook Messenger

blocking version: 0.4.0

This test checks to see if the servers used by Facebook messenger are reachable

[More Info](#)

[Run](#)

HTTP Invalid Request Line

manipulation version: 0.2

Performs out of spec HTTP requests in the attempt to trigger a proxy error message.

[More Info](#)

[Run](#)

HTTP Header Field Manipulation

manipulation version: 0.1.5

Checks if the HTTP request the server sees is the same as the one that the client has created.

[More Info](#)

[Run](#)

Vanilla Tor

blocking version: 0.1.0

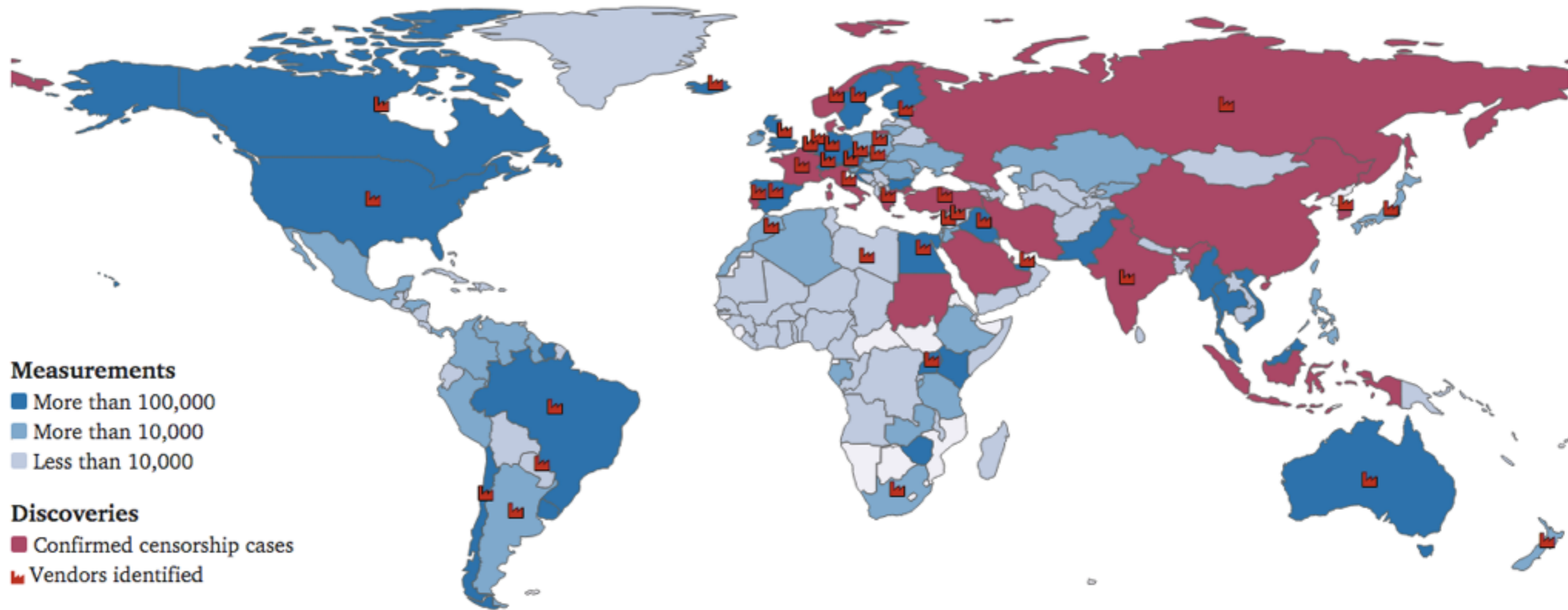
A test for checking if vanilla Tor connections work.

[More Info](#)

[Run](#)

OONI

World Map



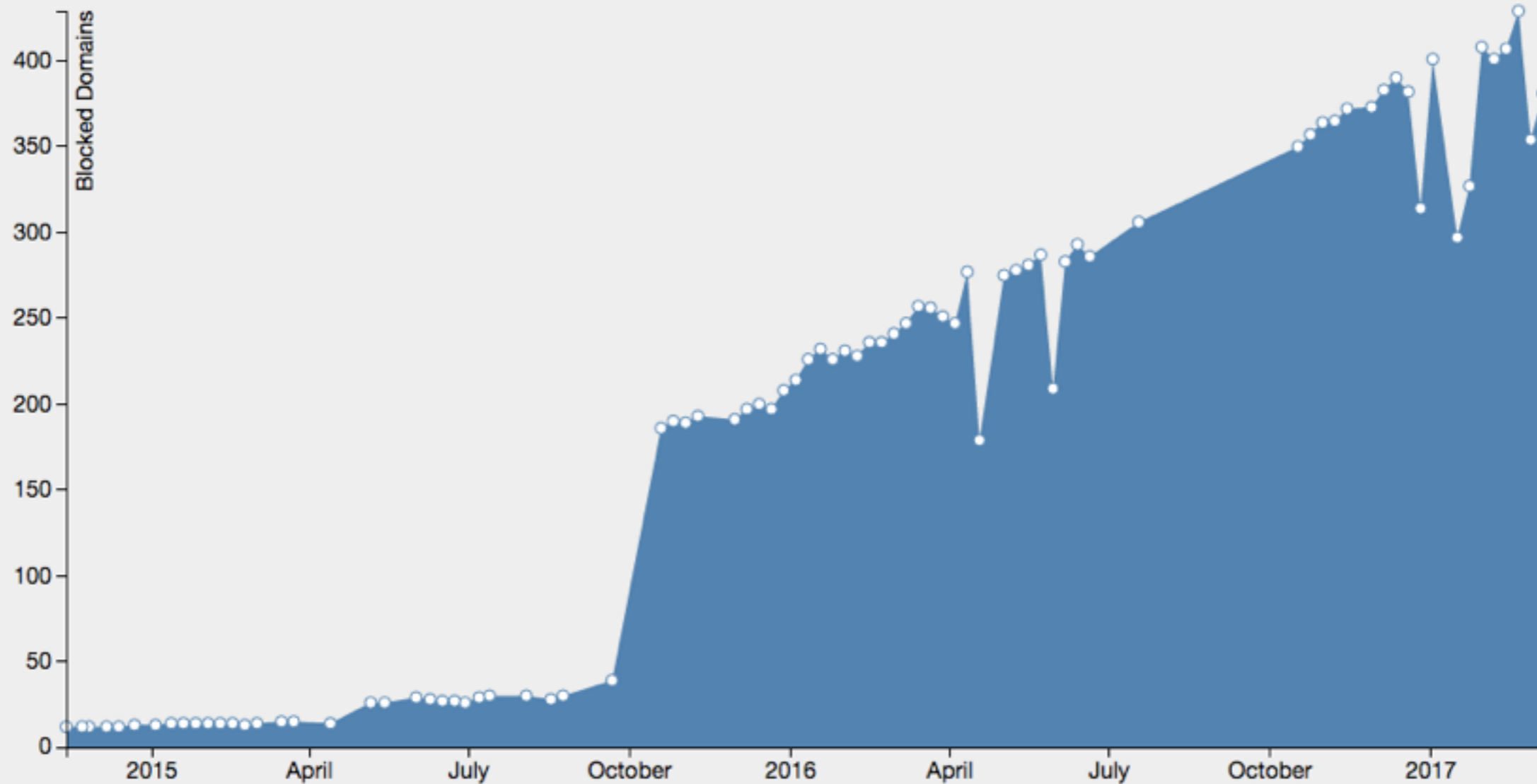
OONI

- URL List: <https://github.com/citizenlab/test-lists>
- C library: <https://github.com/measurement-kit>
- Reports for: Kenya, Malaysia, Ethiopia, Gambia, Belarus, Egypt, Zambia, Turkey, Uganda, Brazil

Satellite

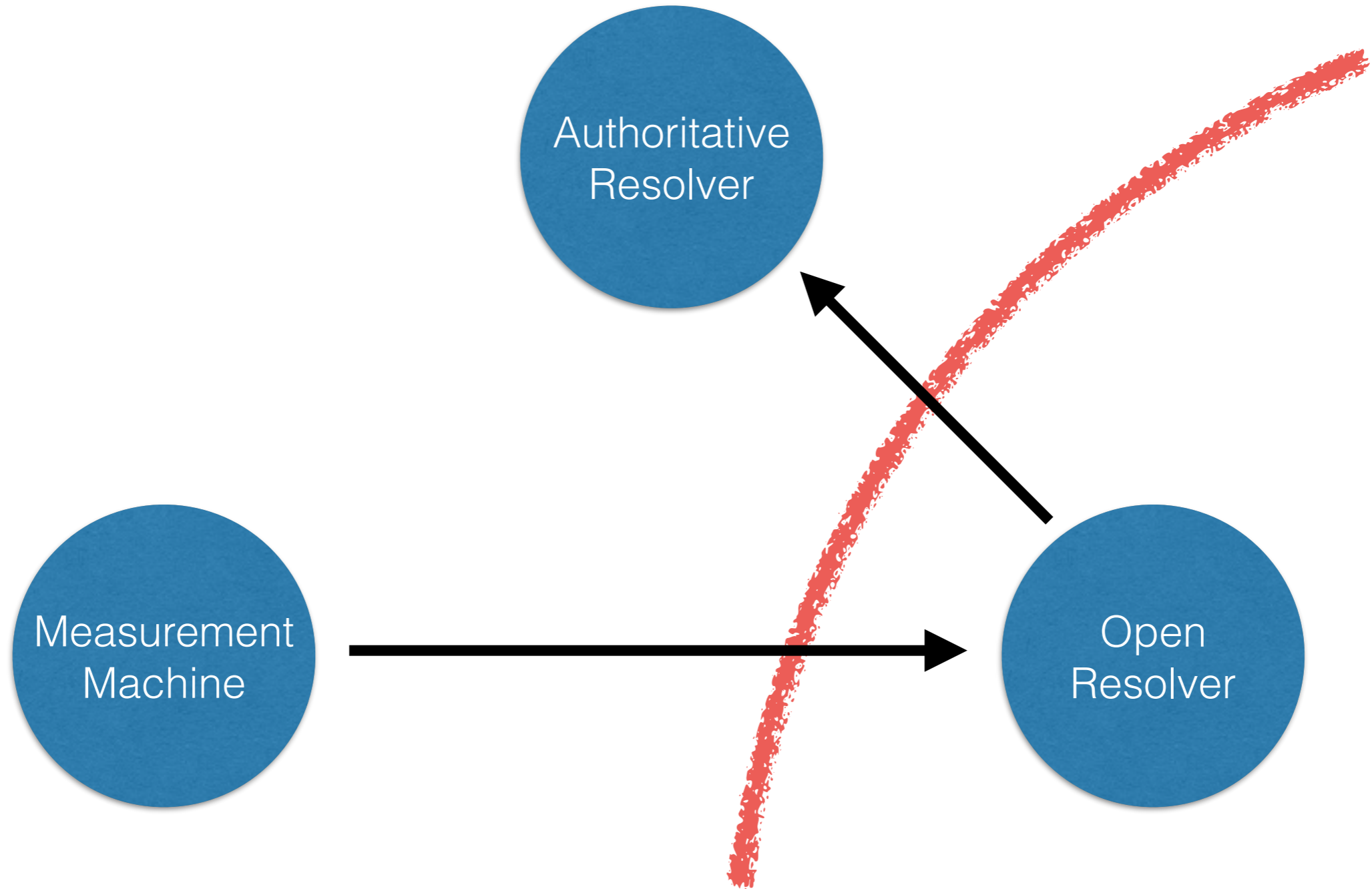


Satellite | Interference in Iran



<http://satellite.cs.washington.edu/>

Satellite



Satellite

- 7M distinct IPv4. 1.5M distinct /24
- Weekly Scan of Alexa top 10k domains
- 3 years of public data on <https://scans.io/>



Censys & Scans

The screenshot shows a web browser window with the URL <https://www.censys.io/data>. The page features a search bar at the top, followed by a section titled "Censys Data Collection" which describes the data gathering process from the University of Michigan. Below this is a call to action for users to help implement new protocols. The "Primary Datasets" section lists three categories: IPv4 Address Space, Alexa Top Million Domains, and X.509 Certificates. At the bottom, a section titled "Regularly Scheduled Scans" introduces a table with columns for Name, Port, Protocol, Subprotocol, Destination, and Last Scan.

Raw Data - Censys x Person 1

<https://www.censys.io/data>

censys About Search Reports SQL API Raw Data

Search Search

Censys Data Collection

Censys collects data about hosts and websites through horizontal scans of the public IPv4 address space and the [Alexa Top Million Domains](#). We validate, transform, and annotate this data with additional metadata (e.g., device model and geographic location) before we stream the records to a central database that maintains each host's state. We perform these scans from the University of Michigan using [ZMap](#), [ZGrab](#), and [ZTag](#). Detailed information about our data collection is available in our [research paper](#).

Looking for a protocol we don't scan or know how to identify a new type of device? Help us [implement it](#) and we'll add it to our roster.

Primary Datasets

We publish daily snapshots of what we know about each host, website, and certificate. These datasets contain structured, non-ephemeral JSON records that identify a host's configuration—similar to what is available in the search interface.

[IPv4 Address Space](#) [Alexa Top Million Domains](#) [X.509 Certificates](#)

Regularly Scheduled Scans

Below are the regularly scheduled scans that power Censys. For each scan, we publish the host discovery scans and parsed application handshakes. We typically scan each protocol at least once weekly.

Name	Port	Protocol	Subprotocol	Destination	Last Scan
------	------	----------	-------------	-------------	-----------

Censorship

- Four countries with significant DNS poisoning
 - Iran, Turkey, China, Indonesia
- 12 countries with explicit block pages
 - Russia, China, Iran, Saudi Arabia, Turkey, India, Indonesia, Greece, Sudan, Belgium, Cyprus, South Korea
- Many more with censorship:
 - Norway, France, Italy, Greece, Cyprus, Qatar, Portugal, Egypt, Thailand, Malaysia, Cuba, Ethiopia, Gambia

Censorship

- **Elections** are a common trigger for censorship.
- Censorship is often implemented by **ISPs**, not by the state, complicating attribution.
- Open measurements are **losing relevance** as censorship moves to social media and closed platforms.

Opportunities

- Format standardization
- Ground truth standardization
- Service Measurements

