Interpreting OONI data
• **Normal.** When everything is **OK** (e.g. tested website is accessible). ✔

• **Confirmed blocked.** We only *automatically confirm the blocking of a website* when we detect a block page. ❌

• **Anomalous.** **Signal that something is wrong** (we should check the measurement data more carefully). Anomalous measurements MIGHT contain evidence of censorship, but not necessarily (i.e. false positives).❗

**Interpreting OONI data**
Why do false positives occur?

- Transient network failures
- Unreliable servers
- DNS resolution
- Geographical distribution of content
- Software bugs
• Understanding **how OONI Probe tests work** (and inspecting relevant measurements)

• Checking whether the **type of anomaly** (DNS, TCP/IP, HTTP) is persistent

• Examining **OONI data in aggregate**

• Evaluating other possible reasons that might have triggered the “anomaly”

Identifying false positives
Categories of OONI Probe tests

- **Websites:**
  - Web connectivity test

- **Instant Messaging Apps:**
  - WhatsApp test
  - Facebook Messenger test
  - Telegram test
  - Signal test

- **Circumvention tools:**
  - Tor
  - Psiphon
  - RiseupVPN

- **Performance:**
  - NDT & DASH
  - Middlebox tests

https://ooni.org/nettest/
Web Connectivity test

Control

Non-censored network

Probe

DNS lookup
TCP connection
HTTP request

Probe network

Website

If Control != Experiment
Possible censorship
OK
1. **Resolver identification:** OONI Probe checks which is the IP address of your DNS resolver

2. **DNS lookup:** OONI Probe checks **which IP addresses** are mapped to the tested domains:
   
a. If the IP addresses from the control + user network **match** = Everything is OK
   
b. If the IP addresses from the control + user network **differ** = Sign of DNS tampering ("DNS anomaly")
3. **TCP connect:** OONI Probe tries to **connect** to the tested domains (based on the IP addresses identified during the DNS lookup):

   a. If the TCP connection is successful = **Everything is OK**
   b. If the TCP connection is **not** successful = **Sign of potential TCP/IP blocking (‘TCP/IP anomaly’)**
4. **HTTP request**: OONI Probe sends requests through the HTTP protocol to the server of the tested website.

   a. If the server responds with the content of the requested website = Everything is OK
   b. **Sign of potential HTTP blocking** (“HTTP anomaly”) if:
      - HTTP request fails; or
      - The **HTTP status codes** do not match; or
      - All of the following apply:
        1. The **body length** of the tested website differs (from the control + user networks);
        2. The **HTTP headers names** do not match;
        3. The **HTML title tags** do not match.

**Web Connectivity test**
Confirmed search query Saudi Arabia avaaz.com
https://explorer.ooni.org/measurement/20210624T190120Z_webconnectivity_SA_25019_n1_lwjTpFZm8RSoyDVu?input=http%3A%2F%2Favaaz.org%2F

DNS Tampering:

TCP/IP Blocking:

HTTP Failure:

Anomalous measurements
WhatsApp is **likely blocked** if:

- Checks for `web.whatsapp.com` fail; or
- Checks for the WhatsApp registration service fail; or
- Connections or DNS resolutions for the WhatsApp app endpoints fail
Facebook Messenger is likely blocked if:

- **TCP connections** to Facebook’s endpoints fail;
- **DNS lookups** do *not* resolve to IP addresses allocated to Facebook.
Telegram is **likely blocked** if:

- TCP connections to Telegram’s endpoints fail;
- HTTP requests (to Telegram endpoints + web.telegam.org) do *not* send back a consistent response.
This test tries to bootstrap a Psiphon tunnel & check if it works.

There are 3 possible outcomes:

1. Psiphon bootstraps and it’s able to fetch a webpage. ✔
2. Psiphon bootstraps, but it can’t fetch a webpage. ❗
3. Psiphon does not bootstrap. ❗
This test measures the reachability of:

- Tor directory authorities
- Tor bridges (obfs4)

If the above is successful, Tor probably works on your network.
• High level test overview: https://ooni.org/nettest
• Detailed test specifications: https://github.com/ooni/spec
Important to look at data in aggregate!
For data newer than 2020-10-20
s3://ooni-data-eu-fra/raw/{YYMMDD}/{HH}/{probe_cc}/{testname}/*.jsonl.gz

example:
s3://ooni-data-eu-fra/raw/20210630/11/IT/webconnectivity/2021063011_IT_webconnectivity.n0.1.jsonl.gz

For older data
s3://ooni-data-eu-fra/jsonl/{testname}/{probe_cc}/{YYMMDD}/{HH}/*.jsonl.gz

example:
s3://ooni-data-eu-fra/jsonl/webconnectivity/IT/20180105/00/20180105_IT_webconnectivity.1.4.jsonl.gz
# Social media blocking amid Uganda's 2021 general election

<table>
<thead>
<tr>
<th>Test Name</th>
<th>Probe Aim</th>
<th>Measure Names</th>
</tr>
</thead>
<tbody>
<tr>
<td>Facebook</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Messenger</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Telkom</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WhatsApp</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

![Graph showing social media blocking amid Uganda's 2021 general election](image-url)
Examine the testing of a website or app:

- On a **network level** (ASN)
- Over **time**
- Based on the **type of anomaly**

If the *same anomaly (e.g. DNS) is persistent in all measurements over time on the same network*, then it may provide a signal of potential censorship.

**Key takeaway**
Questions?