Interpreting OONI data

OONI

- **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

- Transient network failures
- Unreliable servers
- DNS resolution
- Geographical distribution of content
- Software bugs

Why do false positives occur?

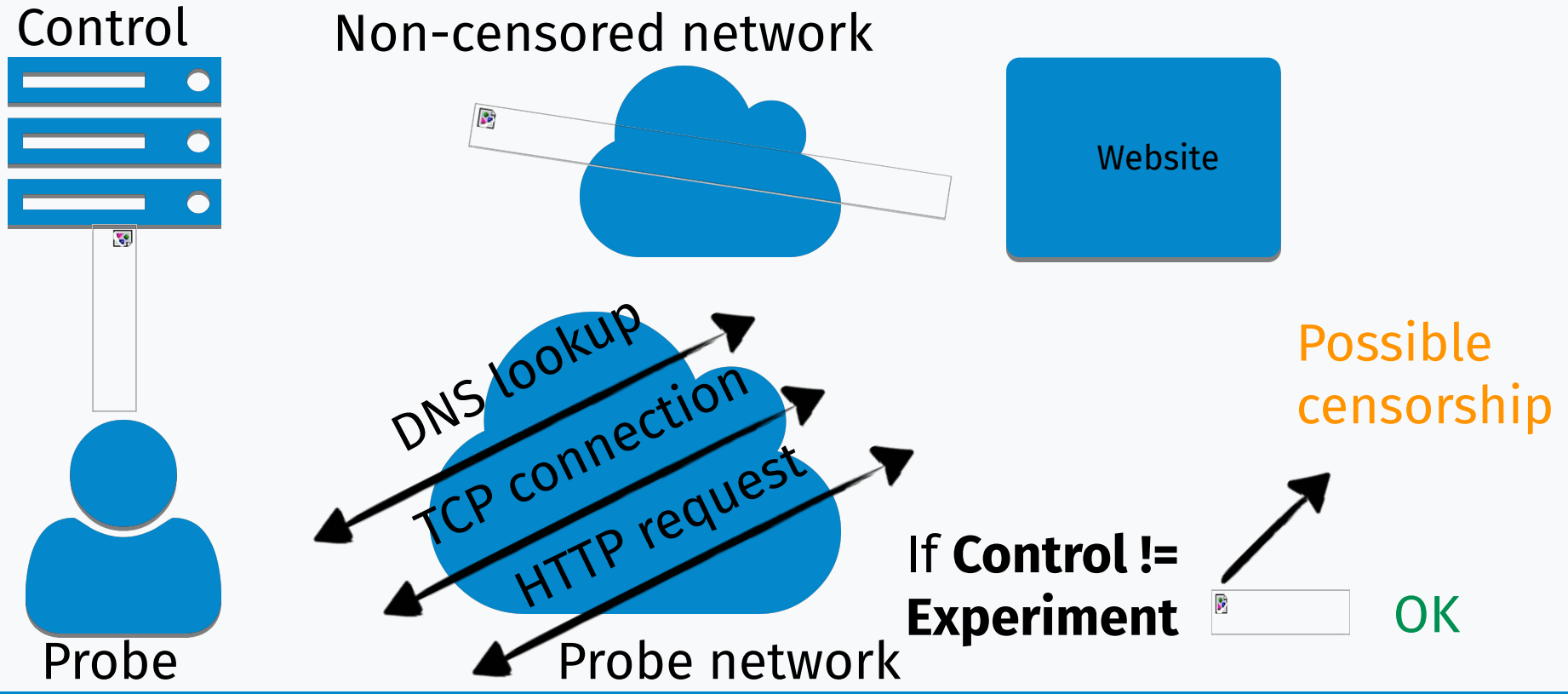
- Understanding **how OONI Probe tests work** (and inspecting relevant measurements)
- Checking whether the **type of anomaly** (DNS, TCP/IP, HTTP) is persistent
- Examining **OONI data in aggregate**
- Evaluating other possible reasons that might have triggered the “anomaly”

Identifying false positives

- **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/

Categories of OONI Probe tests



Web Connectivity test

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”)**

Web Connectivity test

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")**

Web Connectivity test

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:
  https://explorer.ooni.org/measurement/20210211T133445Z_webconnectivity_MM_133385_n1_0VXQa1P6EUPQ7GiP?input=http%3A%2F%2Fwww.facebook.com
- TCP/IP Blocking:
  https://explorer.ooni.org/measurement/20210209T115745Z_webconnectivity_MM_9988_n1_XGLPQSUvvkIaTrgi?input=http%3A%2F%2Fwww.facebook.com
- HTTP Failure:
  https://explorer.ooni.org/measurement/20210626T193802Z_webconnectivity_EG_24835_n1_GXUqHqrczEC0Ztbs?input=https%3A%2F%2Fwww.hrw.org%2F

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

WhatsApp test

Facebook Messenger is **likely blocked** if:

- **TCP connections** to Facebook's endpoints fail;
- **DNS lookups** do *not* resolve to IP addresses allocated to Facebook.

Facebook Messenger test

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.

Telegram test

This test tries to bootstrap a Psiphon tunnel & check if it works.

There are 3 possible outcomes:

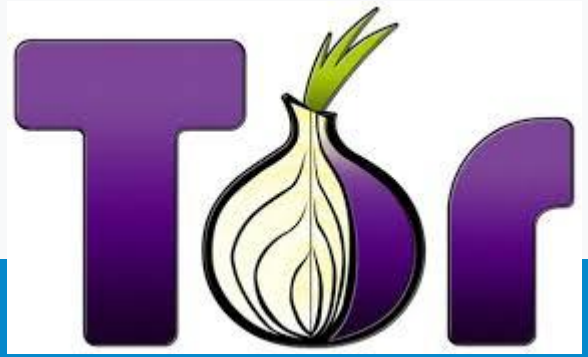
1. Psiphon bootstraps and it's able to fetch a webpage. ✔
2. Psiphon bootstraps, but it **can't fetch a webpage**. ❗
3. Psiphon **does not bootstrap**. ❗

Psiphon test

This test measures the reachability of:

- Tor directory authorities
- Tor bridges (obfs4)

If the above is successful, Tor probably works on your network.



Tor test

- High level test overview: https://ooni.org/nettest
- Detailed test specifications: https://github.com/ooni/spec

Learn more about tests

https://explorer.ooni.org/experimental/mat?probe_cc=BI&since=2020-05-15&until=2020-05-30&test_name=whatsapp&axis_x=measurement_start_day
https://explorer.ooni.org/experimental/mat?probe_cc=MM&since=2021-06-06&until=2021-07-07&test_name=whatsapp&axis_x=measurement_start_day
https://explorer.ooni.org/experimental/mat?probe_cc=MM&since=2021-06-06&until=2021-07-07&test_name=whatsapp&axis_x=measurement_start_day&axis_y=probe_asn
https://explorer.ooni.org/experimental/mat?probe_cc=IT&since=2021-06-06&until=2021-07-07&test_name=web_connectivity&axis_x=measurement_start_day&axis_y=category_code
https://explorer.ooni.org/experimental/mat?probe_cc=IR&since=2021-06-06&until=2021-07-07&test_name=web_connectivity&axis_x=measurement_start_day&axis_y=category_code
https://explorer.ooni.org/experimental/mat?since=2021-06-05&until=2021-07-06&test_name=web_connectivity&input=https%3A%2F%2Fwww.hrw.org%2F&axis_x=measurement_start_day&axis_y=probe_cc
https://explorer.ooni.org/experimental/mat?since=2021-06-06&until=2021-07-07&test_name=tor&axis_x=measurement_start_day&axis_y=probe_cc

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

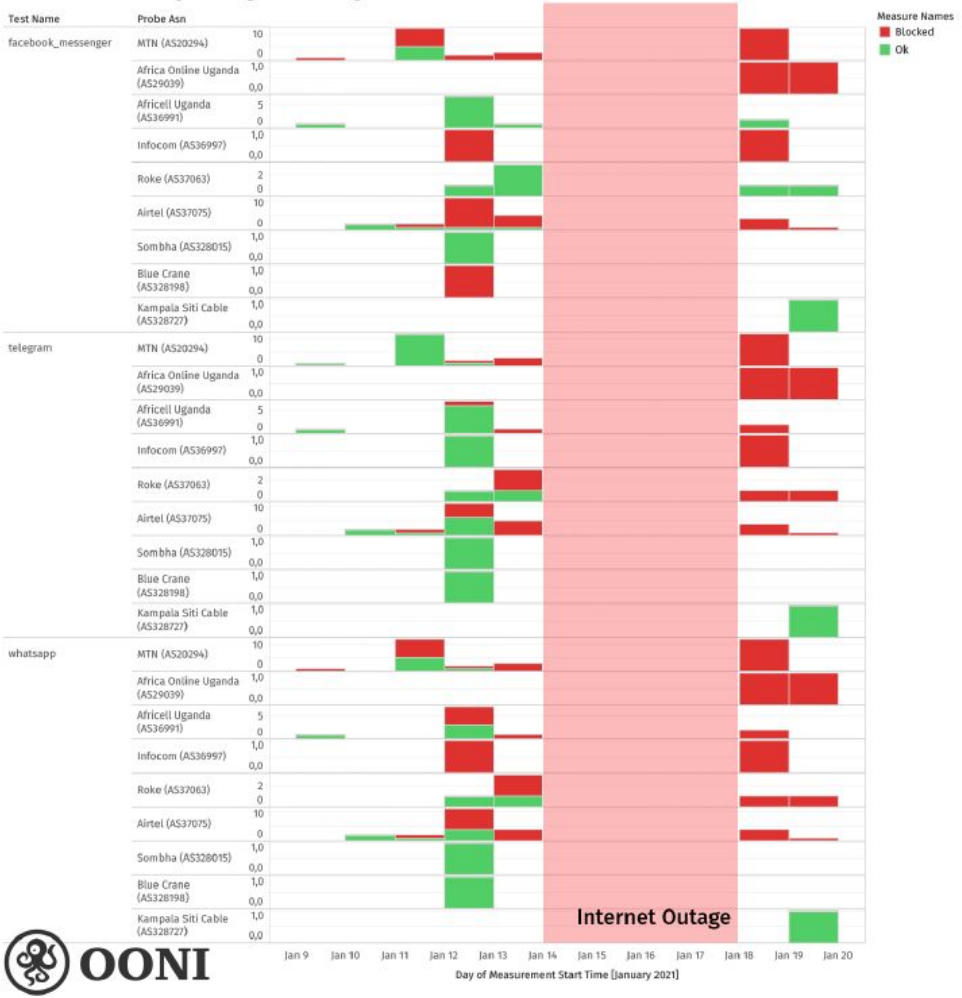
For older data

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.l.4.jsonl.gz

Accessing RAW data

Social media blocking amid Uganda's 2021 general election



OONI

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?