Introduction to Internet Censorship

"This website/URL has been blocked until further notice either pursuant to Court orders or on the Directions issued by the Department of Telecommunications"

OONI Partner Training 2021
Out of scope

- Censorship on social media platforms
- Internet outages/blackouts/shutdowns
- Takedown requests
- Online trolling
- Self-censorship
Internet censorship

● Censorship on the network level
● Blocking of websites and applications
Who implements internet censorship?
All Internet Service Licensees

Direction to block Internet Website.

Under the powers conferred by Section 69A of the Information Technology Act, 2000 and under the Information Technology (Procedures and Safeguards for Blocking of Access to Information) by Public Authorities Rules, 2009, it has been decided to immediately block the access to the following 32 URLs:

1. https://pastebin-it/  
5. https://pastew.org  
17. http://www.shelby.com/  
23. https://git.github.com  
32. https://cryptbin.com

2. All the Internet Service Licensees are accordingly directed to immediately block the access to above URLs.

3. The compliance be submitted immediately, failing which the Department may initiate action under Rule 12 of the Information Technology (Procedures and Safeguards for Blocking of Access to Information by Public Authorities) Rules, 2009. Kindly do not reproduce the names of URLs in the compliance letter. The contents of this letter may kindly be kept confidential.
Επιχειρήσατε πρόσβαση σε ιστότοπο μέσω του οποίου παρέχονται μη αδειοδοτημένες υπηρεσίες τυχαίων παιγνίων.

Σύμφωνα με τον νόμο, οι παροχοί υπηρεσιών διαδικτύου είναι υποχρεωμένοι να μην επιτρέψουν την πρόσβαση σε ιστότοπους μη αδειοδοτημένων παρόχων τυχαίων παιγνίων, οι οποίοι αναφέρονται στον οικείο κατάλογο (BlackList) που τηρεί η Ε.Ε.Ε.Π.

Εισηγητικά το η συμμετοχή σε τυχαία παιγνία, τα οποία διαρθρώνονται χωρίς άδεια από την Ελληνική Δημοκρατία, επιβάλλει αυστηρές διοικητικές και παικτικές κυρώσεις.
Access Restricted

Based on Regulation of the Minister of Communication and Information No. 19 of 2014
How is internet censorship implemented?

- IP blocking
- DNS tampering
- HTTP blocking (e.g. blockpages)
- SNI based filtering
Server
IP address

My IP Address
63.255.173.183
TCP/IP

Establishes a connection to an internet service
TCP/IP blocking

In IP and Protocol-Based blocking, the blocking device has a list of IP addresses to block called the "block list". Any attempt to connect to a server with an IP address on the block list will be interrupted.

With IP and Protocol-based blocking, a server that has both "bad" (bomb) and "good" (kitten) content will be unavailable, no matter what content is requested, when the IP address of that server is on the block list. Similarly, a server that is NOT on the block list will be accessible, without regard to the type of content on the server.

All content is blocked since this IP is on the list, including unintentional content.

No content from this server is blocked since this IP is not on the list. Even content we might want blocked.

- X = "Access denied to user. Content blocked"  
- ✔ = "User was able to view the content"
URL

Uniform Resource Locator

- **http://**
  - **www**
    - **google**
      - **.com**

**Protocol** (HyperText Transfer)

- **subdomain**
- **Top Level Domain** (TLD)
- **domain (name)**
Domain name

http://www.example.com/page.html
Domain Name System (DNS)

IP address
123.45.678.9

Domain
www.url.com
DNS tampering

Umbrella term used to describe various forms of DNS interference, including:

- DNS hijacking
- DNS spoofing

DNS tampering occurs when, upon performing a DNS Lookup for a website, a wrong IP address is returned, preventing you from visiting the requested website.
DNS hijacking

User

ooni.org
104.198.14.52
ooni.org
6.6.6.6

Honest DNS Server

Dishonest DNS Server
DNS spoofing

User → ooni.org → 6.6.6.6 → DNS Server

Censor DPI

104.198.14.52
Hypertext Transfer Protocol (HTTP)
Hypertext Transfer Protocol (HTTP)

How HTTP Works

Unencrypted transfer or exchange of data
HTTP blocking

- HTTP request intercepted (and redirected) by HTTP transparent proxy (e.g. serving a block page)
- Reset of the connection
Hypertext Transfer Protocol Secure (HTTPS)

Encrypted transfer or exchange of data
Transport Layer Security (TLS)

TLS is an encryption protocol designed to secure internet communications.
Server Name Indication (SNI)

SNI is an **extension for the TLS protocol**, designed to **specify the domain name** of the website during the TLS handshake.
SNI based filtering

- Reset connection
- Connection timeout

Investigating TLS blocking in India:
https://ooni.org/post/2020-tls-blocking-india/
Network measurement is the process of measuring certain attributes of a network.
Why measure networks?

- Check/confirm anecdotal reports
- Uncover information controls
- Transparency and oversight
- Collect evidence of information controls
How are networks measured?

- **Direct** measurement
  - Inside the country (requires volunteers/users)
  - Outside the country (remote scanning)

- **Indirect** measurement
  - Analysis of telemetry
Tools for measuring internet censorship
Types of questions answered through censorship measurement

- Which websites are blocked by my ISP?
- How does the blocking of websites differ across networks in my country?
- Are social media apps blocked by my ISP? If so, how do they block access?
- Do circumvention tools work in my network?
Questions?