Uncensor your voice with the Outline SDK

Anti-censorship in action. Case study of Meduza + Jigsaw

Splintercon - June 12, 2024

Vinicius Fortuna, Jigsaw (**fortuna@google.com**)

⌐ JIGSAW

Outline SDK

- Libraries - add network resilience to your app
  - Transports - shadowsocks, tls, websocket
  - Proxy protocols - shadowsocks, socks5, http
  - Proxyless strategies - encrypted DNS, packet manipulation, happy eyeballs, strategy finding
  - VPN - "tun2socks"
  - Mobileproxy - integrate into mobile apps
- Command-line Tools - experiment, measure, prototype
  - Fetch
  - Resolve
  - Local proxy

Content App Without MobileProxy
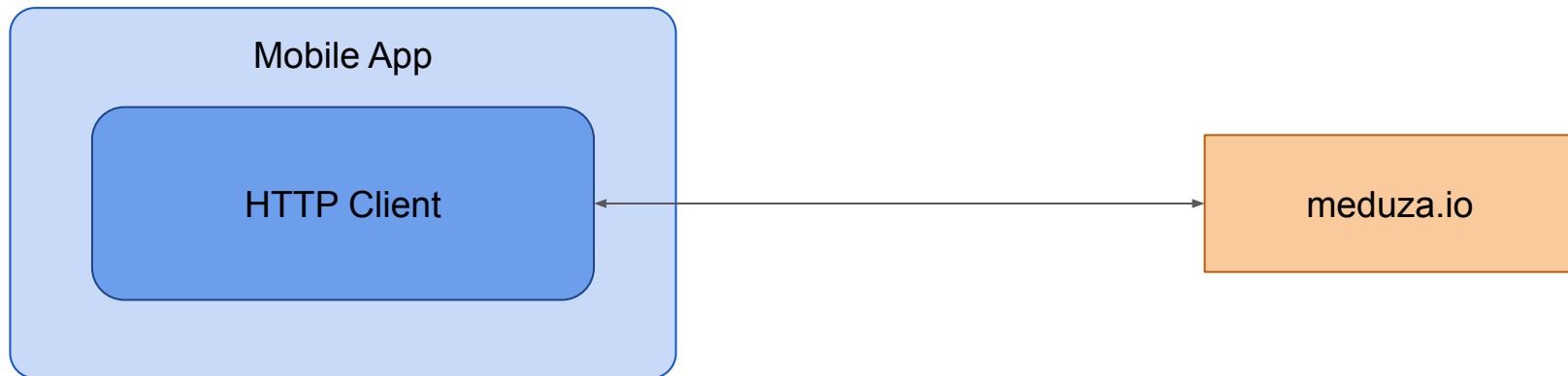
Content App With MobileProxy
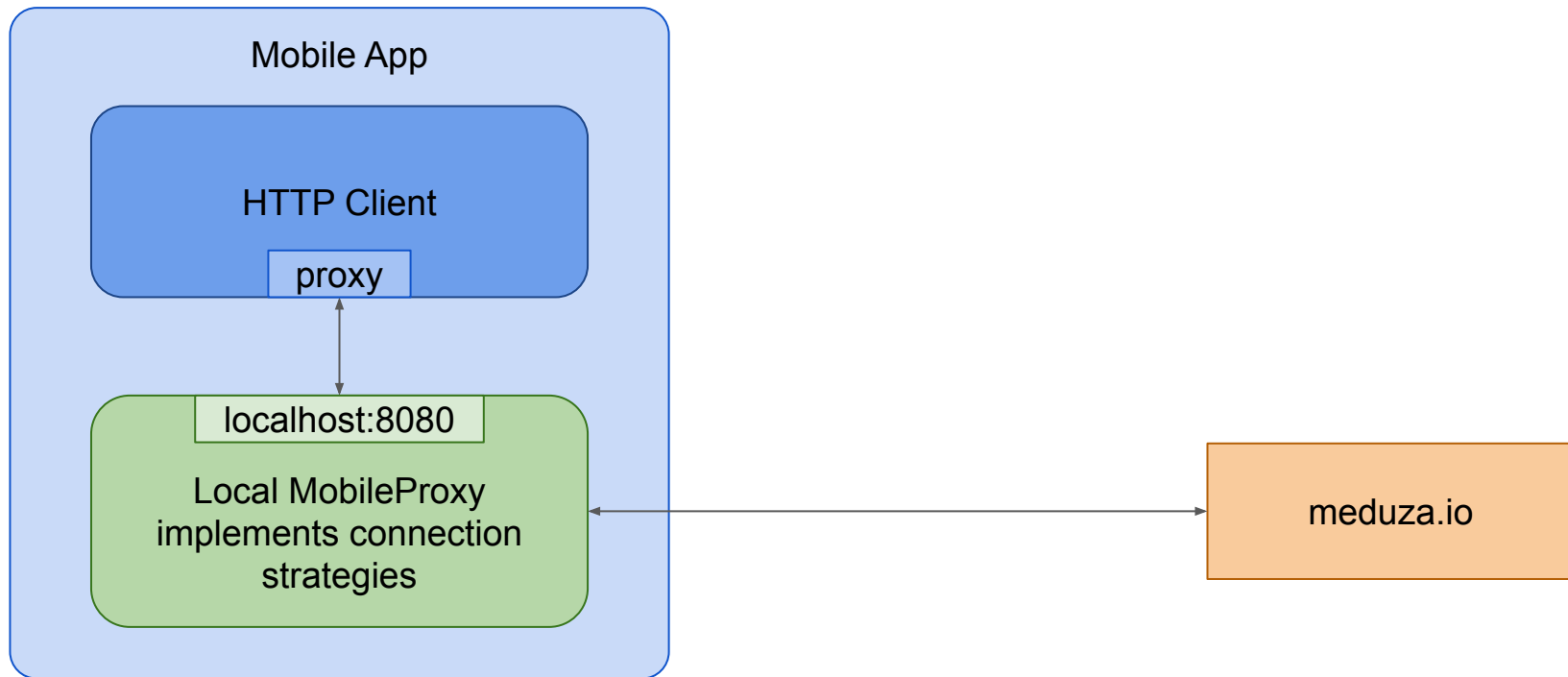
Smart Dialer

```
# Bee Line

!./go/bin/go run github.com/Jigsaw-Code/outline-sdk/x/examples/smart-proxy@073920c \
-v -config config.json -find_only=true -domain meduza.io \
-transport "socks5://package-${SOAX_PACKAGE}-sessionlength-3600-sessionid-BEELINE-country-ru-isp-bee%20line%20cable:${SOAX_KEY}@proxy.soax.com:5000"
```

```
Finding strategy
🧍 run DNS: {"https":{"name":"2620:fe::fe"}} (domain: meduza.io.)
🧍 run DNS: {"https":{"name":"9.9.9.9"}} (domain: meduza.io.)
💀 got DNS: {"https":{"name":"2620:fe::fe"}} (domain: meduza.io.), duration=291.366407ms, ips=[], status=request for A query failed: receive DNS message f
ailed: failed to get HTTP response: Post "https://[2620:fe::fe]:443/dns-query": dial DNS resolver failed: connection not allowed by ruleset ❌
🧍 run DNS: {"https":{"name":"149.112.112.112"}} (domain: meduza.io.)
🧍 run DNS: {"https":{"name":"2001:4860:4860::8888"}} (domain: meduza.io.)
🧍 run DNS: {"https":{"name":"8.8.8.8"}} (domain: meduza.io.)
💀 got DNS: {"https":{"name":"2001:4860:4860::8888"}} (domain: meduza.io.), duration=279.352402ms, ips=[], status=request for A query failed: receive DNS
message failed: failed to get HTTP response: Post "https://[2001:4860:4860::8888]:443/dns-query": dial DNS resolver failed: connection not allowed by rule
set ❌
🧍 run DNS: {"https":{"name":"2001:4860:4860::8844"}} (domain: meduza.io.)
💀 got DNS: {"https":{"name":"9.9.9.9"}} (domain: meduza.io.), duration=1.115947398s, ips=[104.18.1.79 104.18.0.79], status=ok ✅
🏆 selected DNS resolver {"https":{"name":"9.9.9.9"}} in 1.37s

🧍 run TLS: '' (domain: meduza.io.)
🧍 run TLS: 'split:1' (domain: meduza.io.)
🧍 run TLS: 'split:2' (domain: meduza.io.)
🧍 run TLS: 'tlsfrag:1' (domain: meduza.io.)
🧍 run TLS: 'tlsfrag:3' (domain: meduza.io.)
🧍 run TLS: 'tlsfrag:30' (domain: meduza.io.)
💀 got TLS: 'split:2' (domain: meduza.io.), duration=834.953239ms, status=ok ✅
🏆 selected TLS strategy 'split:2' in 1.34s

Found strategy in 2.70s
```

Smart Dialer

```
# MegaFon

!./go/bin/go run github.com/Jigsaw-Code/outline-sdk/x/examples/smart-proxy@073920c \
-v -config config.json -find_only=true -domain meduza.io \
-transport "socks5://package-${SOAX_PACKAGE}-sessionlength-3600-sessionid-MEGAFON-country-ru-isp-pjsc%20megafon:${SOAX_KEY}@proxy.soax.com:5000"
```

```
Finding strategy
🏃 run DNS: {"https":{"name":"2620:fe::fe"}} (domain: meduza.io.)
📡 got DNS: {"https":{"name":"2620:fe::fe"}} (domain: meduza.io.), duration=192.816703ms, ips=[], status=request for A query failed: receive DNS message failed: failed to get
HTTP response: Post "https://[2620:fe::fe]:443/dns-query": dial DNS resolver failed: connection not allowed by ruleset ❌
🏃 run DNS: {"https":{"name":"9.9.9.9"}} (domain: meduza.io.)
🏃 run DNS: {"https":{"name":"149.112.112.112"}} (domain: meduza.io.)
🏃 run DNS: {"https":{"name":"2001:4860:4860::8888"}} (domain: meduza.io.)
📡 got DNS: {"https":{"name":"2001:4860:4860::8888"}} (domain: meduza.io.), duration=203.561455ms, ips=[], status=request for A query failed: receive DNS message failed: faile
d to get HTTP response: Post "https://[2001:4860:4860::8888]:443/dns-query": dial DNS resolver failed: connection not allowed by ruleset ❌
🏃 run DNS: {"https":{"name":"8.8.8.8"}} (domain: meduza.io.)
🏃 run DNS: {"https":{"name":"2001:4860:4860::8844"}} (domain: meduza.io.)
📡 got DNS: {"https":{"name":"2001:4860:4860::8844"}} (domain: meduza.io.), duration=193.79844ms, ips=[], status=request for A query failed: receive DNS message failed: failed
to get HTTP response: Post "https://[2001:4860:4860::8844]:443/dns-query": dial DNS resolver failed: connection not allowed by ruleset ❌
🏃 run DNS: {"https":{"name":"8.8.4.4"}} (domain: meduza.io.)
📡 got DNS: {"https":{"name":"9.9.9.9"}} (domain: meduza.io.), duration=1.174786081s, ips=[104.18.0.79 104.18.1.79], status=ok ✅
🏆 selected DNS resolver {"https":{"name":"9.9.9.9"}} in 1.37s

🏃 run TLS: '' (domain: meduza.io.)
🏃 run TLS: 'split:1' (domain: meduza.io.)
🏃 run TLS: 'split:2' (domain: meduza.io.)
🏃 run TLS: 'tlsfrag:1' (domain: meduza.io.)
🏃 run TLS: 'tlsfrag:3' (domain: meduza.io.)
🏃 run TLS: 'tlsfrag:30' (domain: meduza.io.)
📡 got TLS: 'split:1' (domain: meduza.io.), duration=1.109760684s, handshake=EOF ❌
📡 got TLS: '' (domain: meduza.io.), duration=1.48908609s, handshake=tls: failed to verify certificate: x509: certificate is not valid for any names, but wanted to match meduz
a.io. ❌
📡 got TLS: 'split:2' (domain: meduza.io.), duration=987.648862ms, handshake=EOF ❌
🏃 run TLS: 'tlsfrag:200' (domain: meduza.io.)
📡 got TLS: 'tlsfrag:200' (domain: meduza.io.), duration=1.130057835s, status=ok ✅
🏆 selected TLS strategy 'tlsfrag:200' in 2.63s

Found strategy in 4.00s
```

← Different strategies on different ISPs

Proxyless Example - Iran

go run github.com/Jigsaw-Code/outline-sdk/x/examples/smart-proxy@latest -v -localAddr=localhost:1080 -domain www.youtube.com -config=<(curl -s 'https://raw.githubusercontent.com/Jigsaw-Code/outline-sdk/fortuna-newsmart/x/examples/smart-proxy/config.json')

```
🏃 run DNS: {"https":{"name":"2620:fe::fe"}} (domain: www.youtube.com.)
🏁 got DNS: {"https":{"name":"2620:fe::fe"}} (domain: www.youtube.com.), duration=900.716µs, ips=[], status=request for A
query failed: receive DNS message failed: failed to get HTTP response: Post "https://[2620:fe::fe]:443/dns-query": dial DNS
resolver failed: dial tcp [2620:fe::fe]:443: connect: network is unreachable ❌
🏃 run DNS: {"https":{"name":"9.9.9.9"}} (domain: www.youtube.com.)
🏃 run DNS: {"https":{"name":"149.112.112.112"}} (domain: www.youtube.com.)
🏁 got DNS: {"https":{"name":"9.9.9.9"}} (domain: www.youtube.com.), duration=284.756404ms, ips=[142.250.185.238
216.58.206.78 142.250.185.142 142.250.181.238 142.250.186.78 142.250.184.206 142.250.185.206 142.250.184.238 142.250.185.78
172.217.23.110 142.250.186.46 172.217.18.14 142.250.185.174 142.250.74.206 172.217.16.142 142.250.185.110], status=ok ✅
🏆 selected DNS resolver {"https":{"name":"9.9.9.9"}} in 0.29s

🏃 run TLS: '' (domain: www.youtube.com.)
🏁 got TLS: '' (domain: www.youtube.com.), duration=169.827438ms, handshake=read tcp
87.107.104.85:41316->142.250.185.238:443: read: connection reset by peer ❌
🏃 run TLS: 'split:1' (domain: www.youtube.com.)
🏁 got TLS: 'split:1' (domain: www.youtube.com.), duration=88.910714ms, handshake=read tcp
87.107.104.85:41318->142.250.185.238:443: read: connection reset by peer ❌
🏃 run TLS: 'split:2' (domain: www.youtube.com.)
🏁 got TLS: 'split:2' (domain: www.youtube.com.), duration=97.245811ms, handshake=read tcp
87.107.104.85:41320->142.250.185.238:443: read: connection reset by peer ❌
🏃 run TLS: 'tlsfrag:1' (domain: www.youtube.com.)
🏁 got TLS: 'tlsfrag:1' (domain: www.youtube.com.), duration=175.373294ms, status=ok ✅
🏆 selected TLS strategy 'tlsfrag:1' in 0.53s

Found strategy in 0.82s
```

Proxyless is being a success

that's so cool! it works on youtube and all https website in IRAN. keep up the good work!

★★★★★ April 15, 2024

I'm an Iranian writing this to thank the intra team for the lasted update. the client hello splitting is now perfectly working in Iran! ❤️ thank you so much for doing this update. we're in your favor, love you all ❤️ ❤️❤️

great news! I'm replying to you rn after unblocking reddit with intra!!

thank you so much guys, I don't know if you're a member of the intra team or not but I whole heartedly thank you for helping us Iranians.

love you from Iran ❤️❤️❤️

★★★★★ April 15, 2024

Best for youtube

literally the biggest update ever. thank you so much it's working for Iran

Thank you.
That's nice, but it only worked on YouTube, I couldn't open Facebook or Instagram with this method.
But YouTube's performance was great.

5:29 PM

JIGSAW

# How the Outline SDK is changing the game

- **Aligned incentives:** those bringing circumvention are the ones benefiting from it.
- **Easier problem:** provider controls both the server and the client, can make changes at the application layer (e.g. domain fronting, padding)
- **Reduced costs:** leverage proxyless strategies to proxy only when needed.
- **Technology sharing:** implement once, available to everyone who adopts the SDK. Reusable, composable, interoperable interfaces. Cross-platform.
- **Lower barrier to entry:** developers and researchers can implement new strategies and more easily get into the hands of users.
- **Diversity of providers:** the SDK creates opportunities for service providers specializing in circumvention infrastructure, creating a new market.

Who is using the Outline SDK?

- Circumvention tools
  - Outline Client and Server
  - Intra
  - Lantern
  - nthlink
- Apps
  - Balatarin
  - Meduza
  - Soon: RFE/RL and others
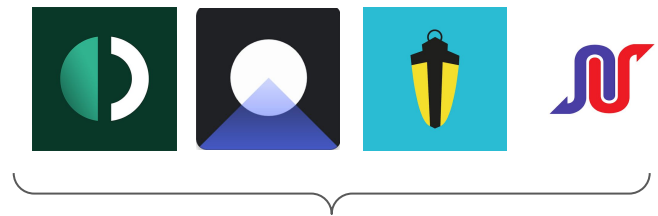
Outline SDK
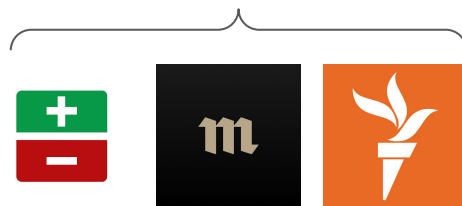
Call to Action

Use it

- Try the Outline SDK Tools
- Explore the SDK APIs
- Create your own tool, or modify one (e.g. create a probe or speed test)
- Integrate the SDK into your app with the mobileproxy
- Try to leverage it in the Blockathon later today!

Contribute

- Create a Dialer with a new protocol or strategy
- Provide feedback or start a discussion

Search the web for [Outline SDK]!