

# Boring filter: The anatomy of a network sandbox for Android.

FOSDEM 2026

Murtaza Aliakbar

**AOSP: 5yrs at Lab126 (2010)**

**Distributed DBs: 3yrs at AWS**

Dad to a boy: 1yrs -

**Rethink: 5yrs -**

Dad to twins: 1yrs -

Android.

App sandbox

Linux + BSD

netd & dnspoxyd

TUN

App sandbox.



seccomp

Middleware

DAC

Capabilities

MAC

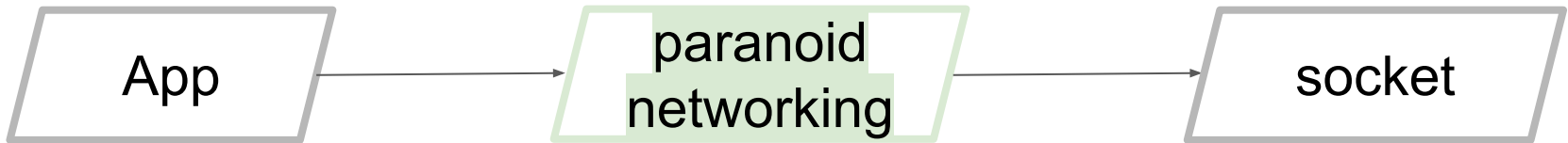
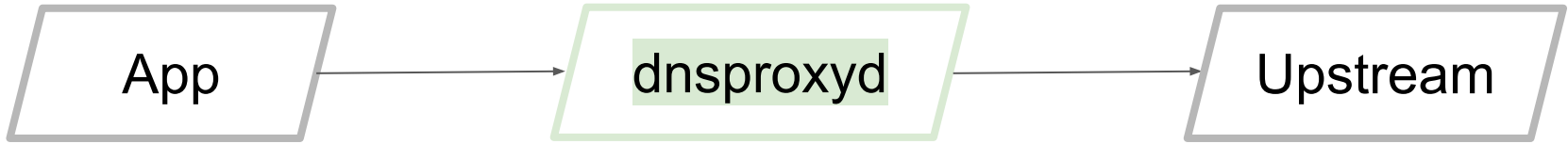
Linux + BSD.

```
\n\n// The FreeBSD complex function implementations\n// appear to be better\n// than the other BSDs', but they're\n// incomplete. We take the FreeBSD\n// implementations when they exist, but fill\n// out the rest from NetBSD...
```

\

```
// BSD-based systems like Android/macOS have  
getprogname(). Others need us to provide one.
```

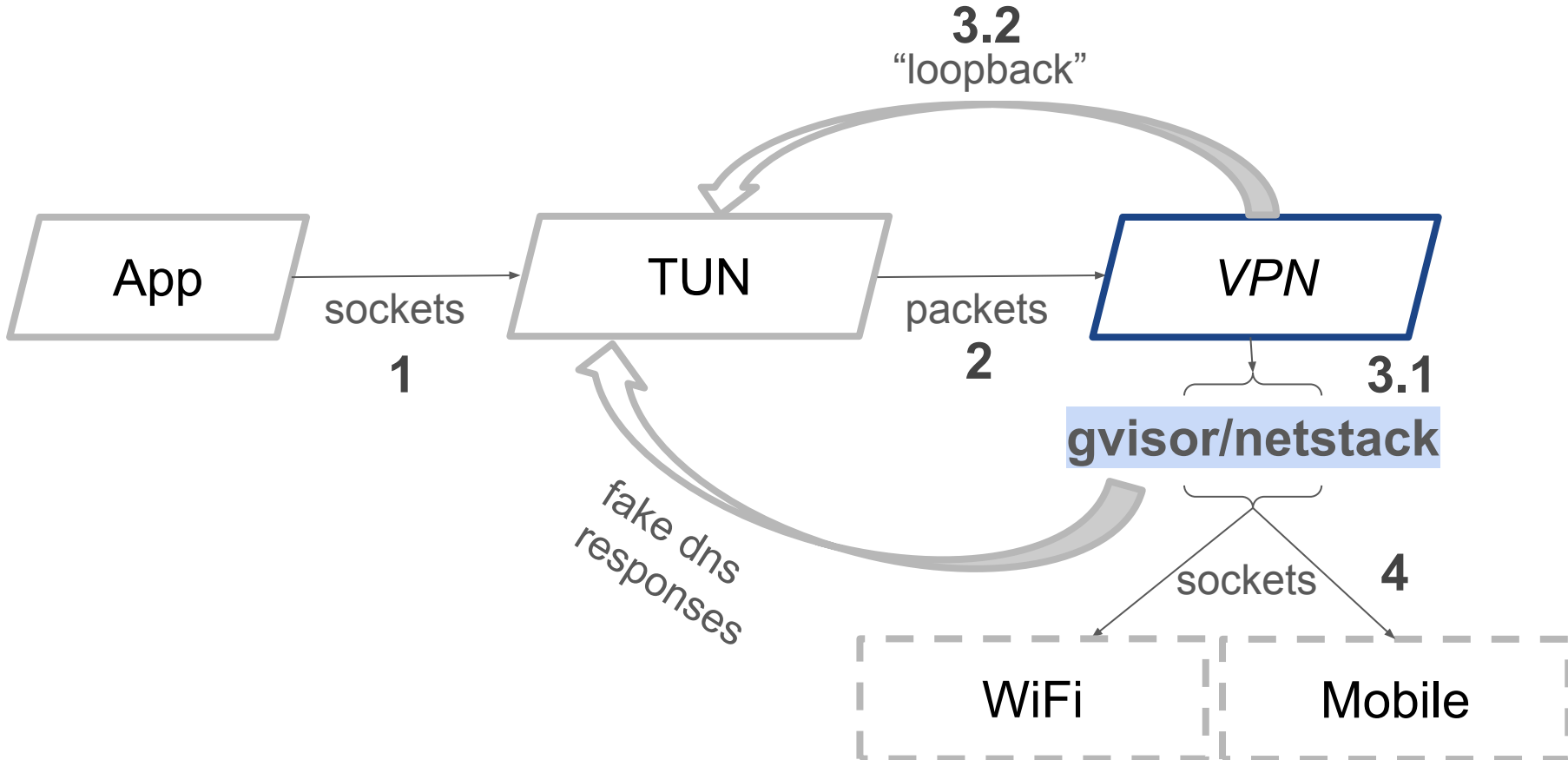
netd & dnspoxyd.

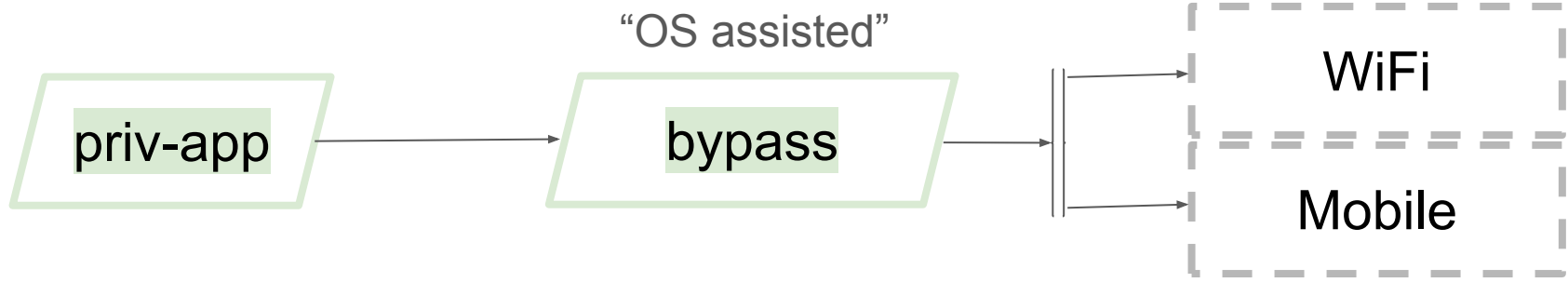
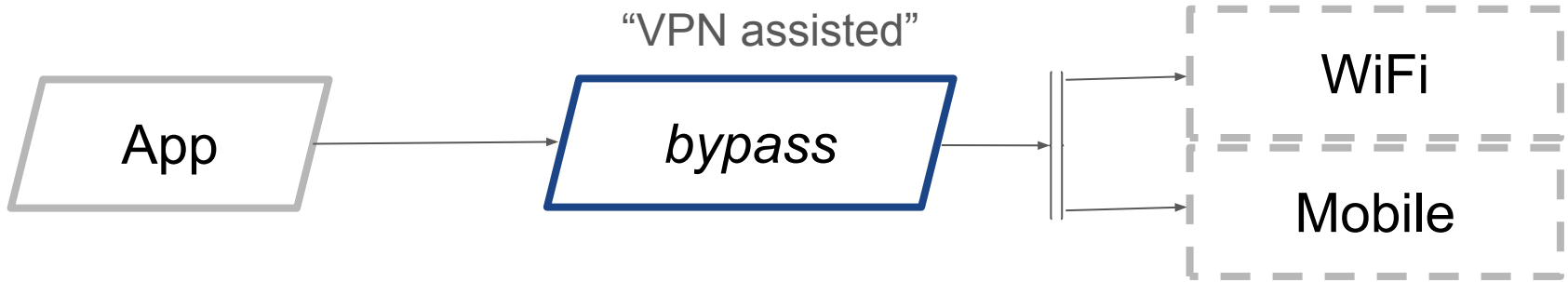


TUN.

\

... Having VPN support built into the OS with a well defined API for apps to implement it with leak blocking support ... is a far better approach which can be done correctly instead of the mess on laptops/desktops ... [Android's] high level design approach is a far better one. It needs a major overhaul to heavily use network namespaces instead of the current messy approach built on a legacy design.







# Rethink.

RETHINK ❤️

**DNS**  
Fast

**Firewall**  
2 universal rule(s)  
4 IP & Port rule(s)  
21 domain rule(s)

**Proxy**  
1 Idle  
WireGuard

**Logs**  
96K connections  
150K queries  
since 24 January

**Apps**

	BLOCKED 343	ISOLATED 48
72 / 469	BYPASSED 5	EXCLUDED 1

IPv4, IPv6  
PROTOS

|| STOP ▾

PROTECTED WITH WIREGUARD

Home Stats Rethink+ Configure About

۲

You can use RethinkDNS and avoid compatibility issues with captive portals. This is one of the options we recommend for GrapheneOS users.

RethinkDNS is implemented as a VPN service but it has support for local filtering combined with optionally using a WireGuard VPN or multiple chained WireGuard VPNs ...



DNS

Firewall

WireGuard

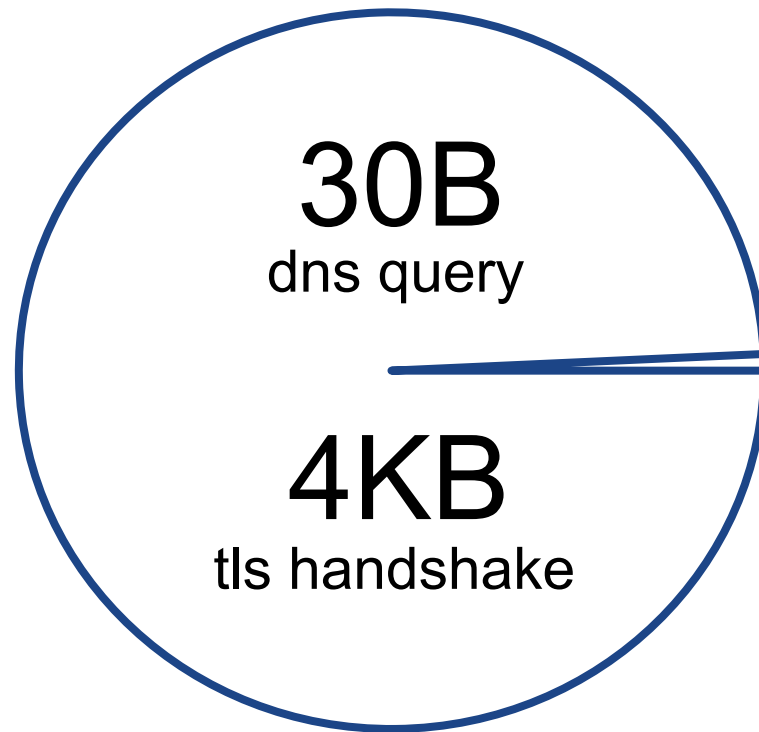
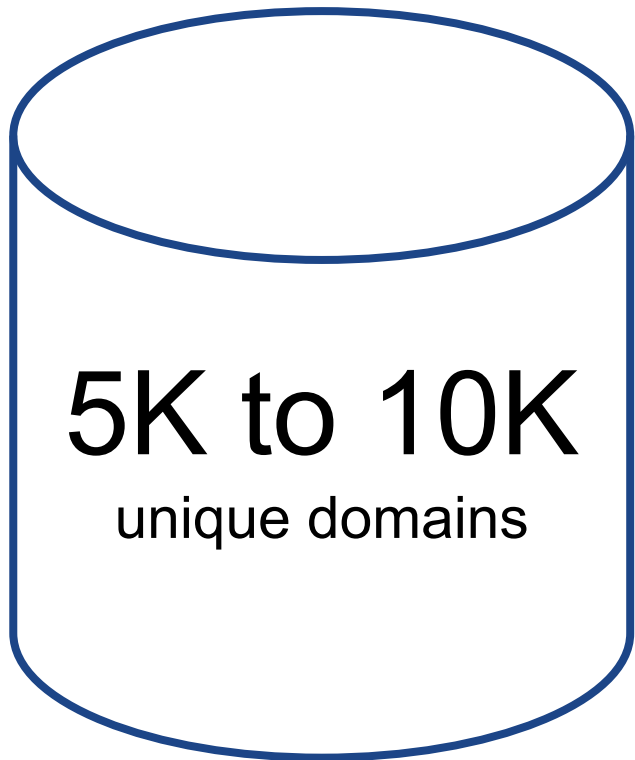
Anti-censorship



# DNS.

Protocol	Fast	Private	Secure	Anonymous
DoH (DNS-over-HTTPS)		●	●	
DoT (DNS-over-TLS)		●	●	
DC (DNSEncrypt)		●	●	●
DNS 53 (DNS Proxy)	●			
ODoH (Oblivious DNS-over-HTTPS)		●	●	●
RDNS (Rethink DNS)	●	●	●	●

● FAST ● PRIVATE ● SECURE ● ANONYMOUS



۲

O(1) LFU Cache

Coalesced requests

Pooled connections

TLS Session Resumption

۲

“bootstrap”

- dns resolver for dns resolver

“per-app”

- split tunneling; caching

۲

# DNS over TCP

- relatively complex

# HTTPS / SVCB

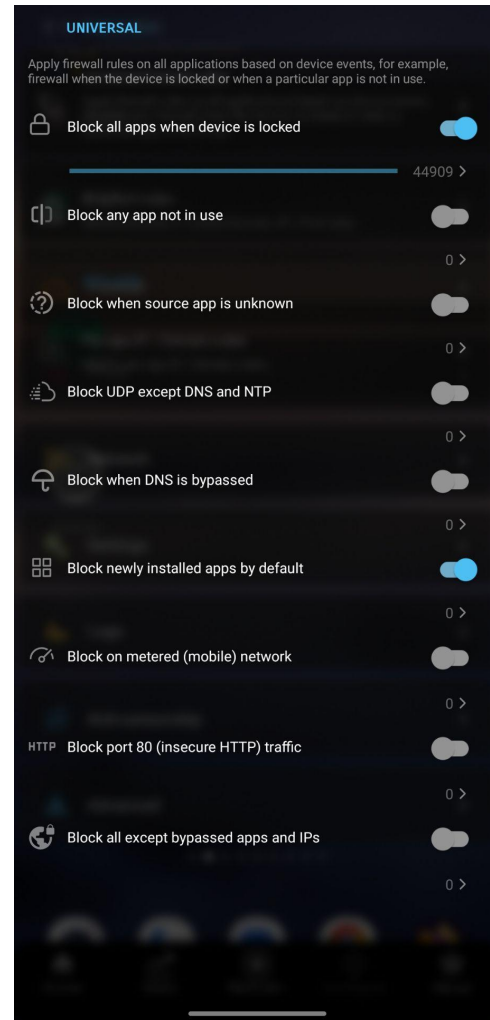
- ech; ip hints ...

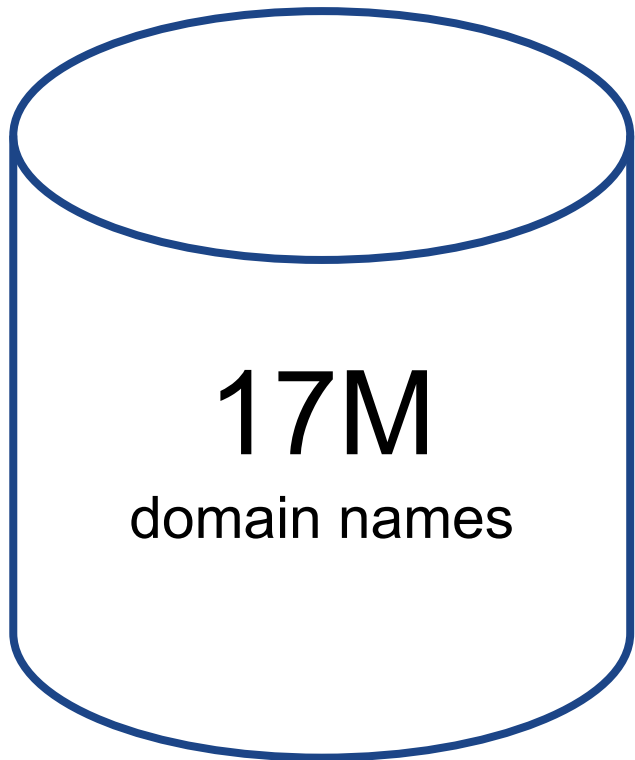
۲

```
example.com SVCB IN 0 example.net
example.net CNAME IN example.org
example.org SVCB IN 0 example.us
example.us SVCB IN 1 cloaked.uk (ipv4hint=2.2.2.2,
ipv6hint=2:2::2)
cloaked.uk SVCB IN 0 example.de
example.de CNAME IN cloaked.fr
cloaked.fr SVCB IN 1 . (ipv4hint=..., ipv6hint=...)
cloaked.fr SVCB IN 2 cloaked.es (ipv4hint=..., ...)
cloaked.es CNAME IN cloaked.it
cloaked.it A IN 4.4.4.4
cloaked.it AAAA IN 4:4::4
```



# Firewall.





**512MB**  
available memory



۲

## Succinct tries

- for domain names; mmap'd

## Critbit tries

- for ip addresses; in-memory

۲

“Isolate”

- block all ips by default

“Stall data”

- on ~~network~~ connectivity loss

۲

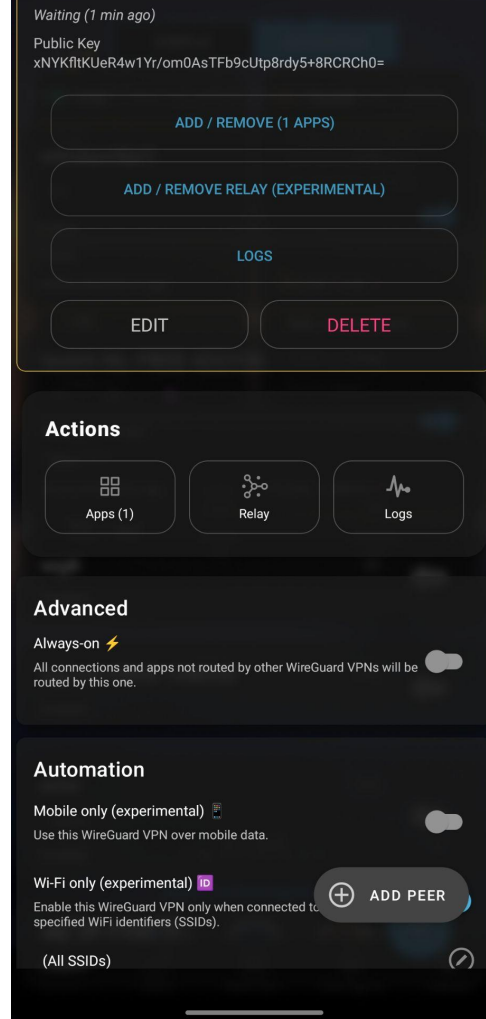
“Endpoint-Independent Mapping”

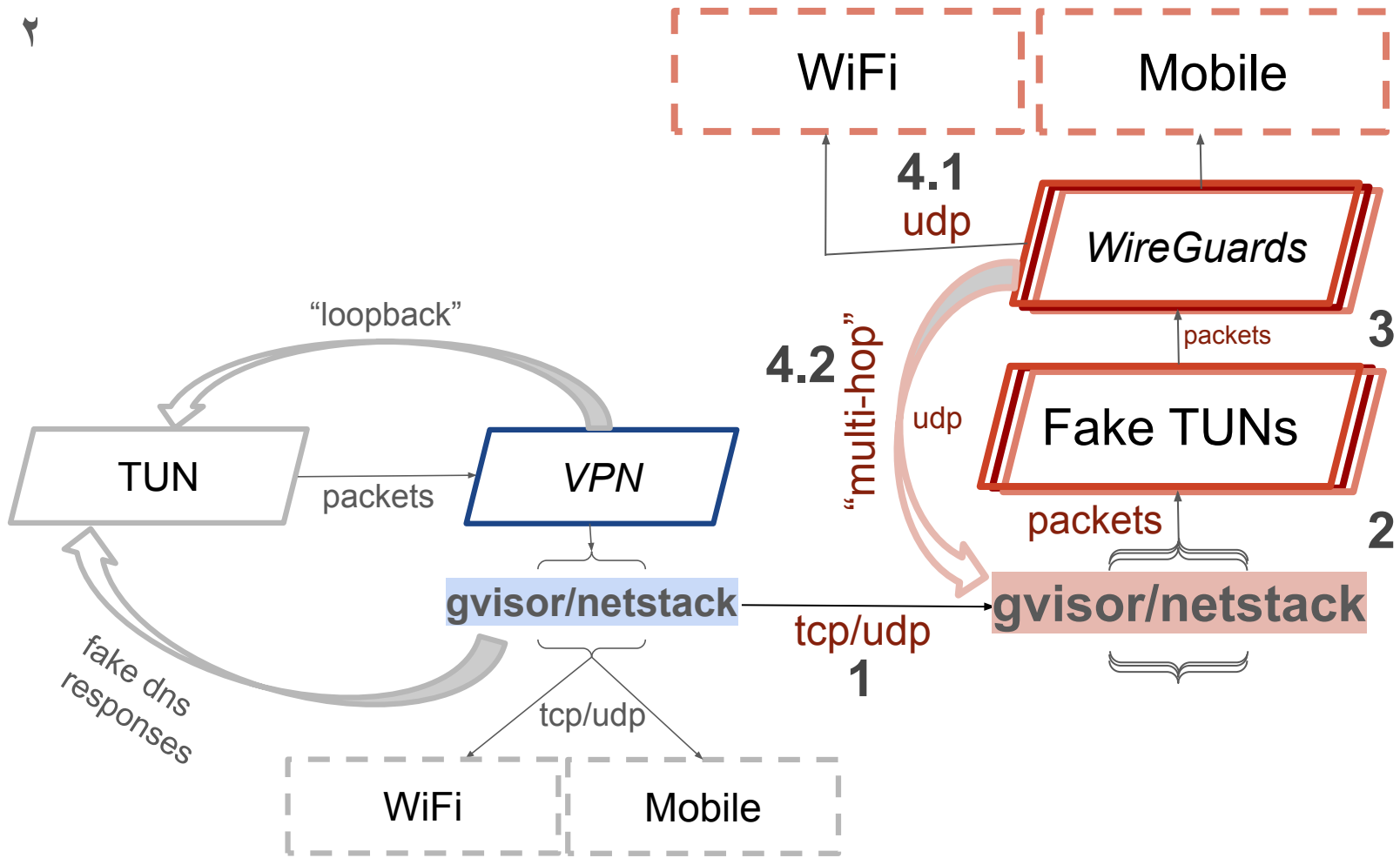
- rfc4787, rfc5382

“Block when DNS bypassed”

- apps may do their own DoH

# WireGuard.





۲

# RTC / HFT clocks

- not monotonic in Go

# “Roaming sockets”

- road warrior setup



**Anti-censorship.**

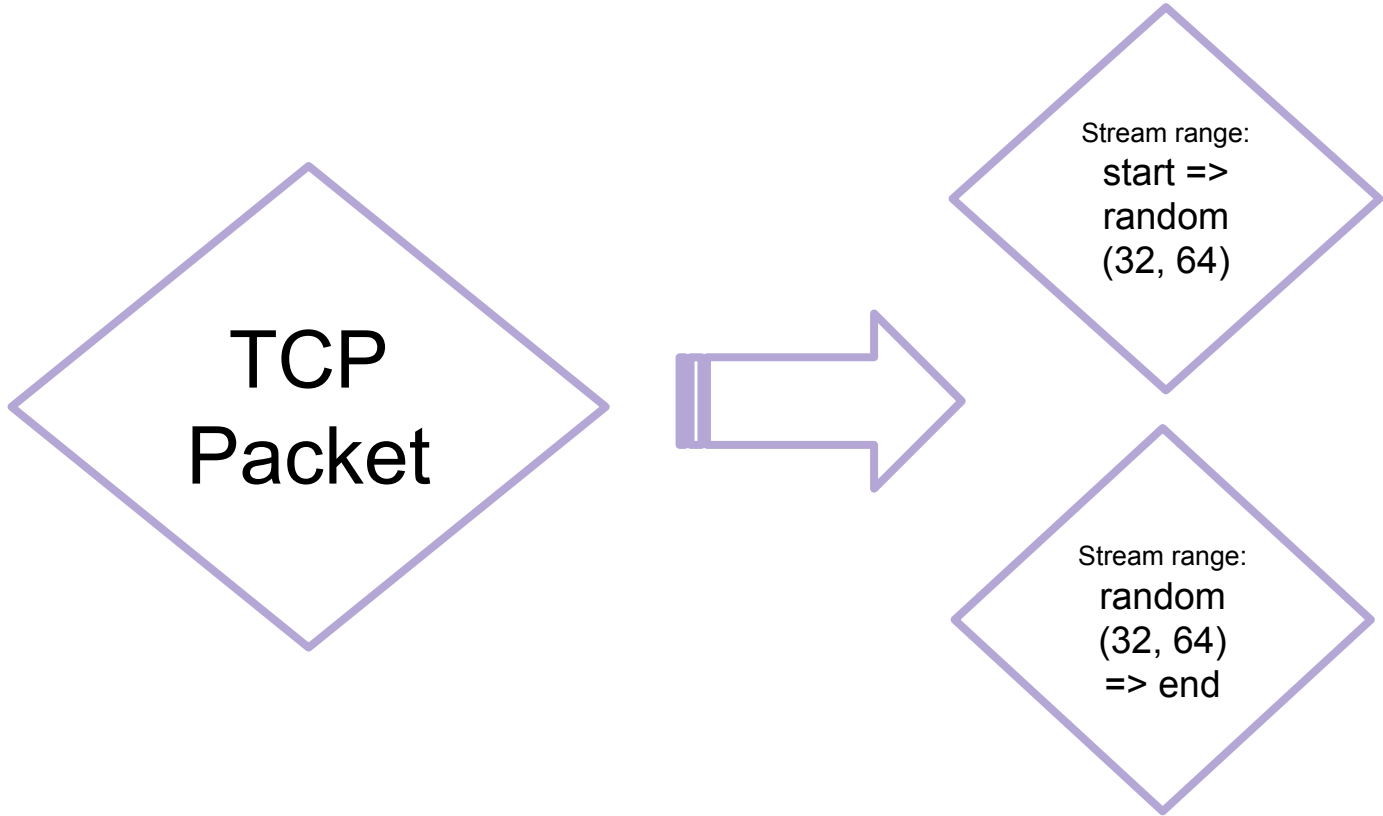
۲

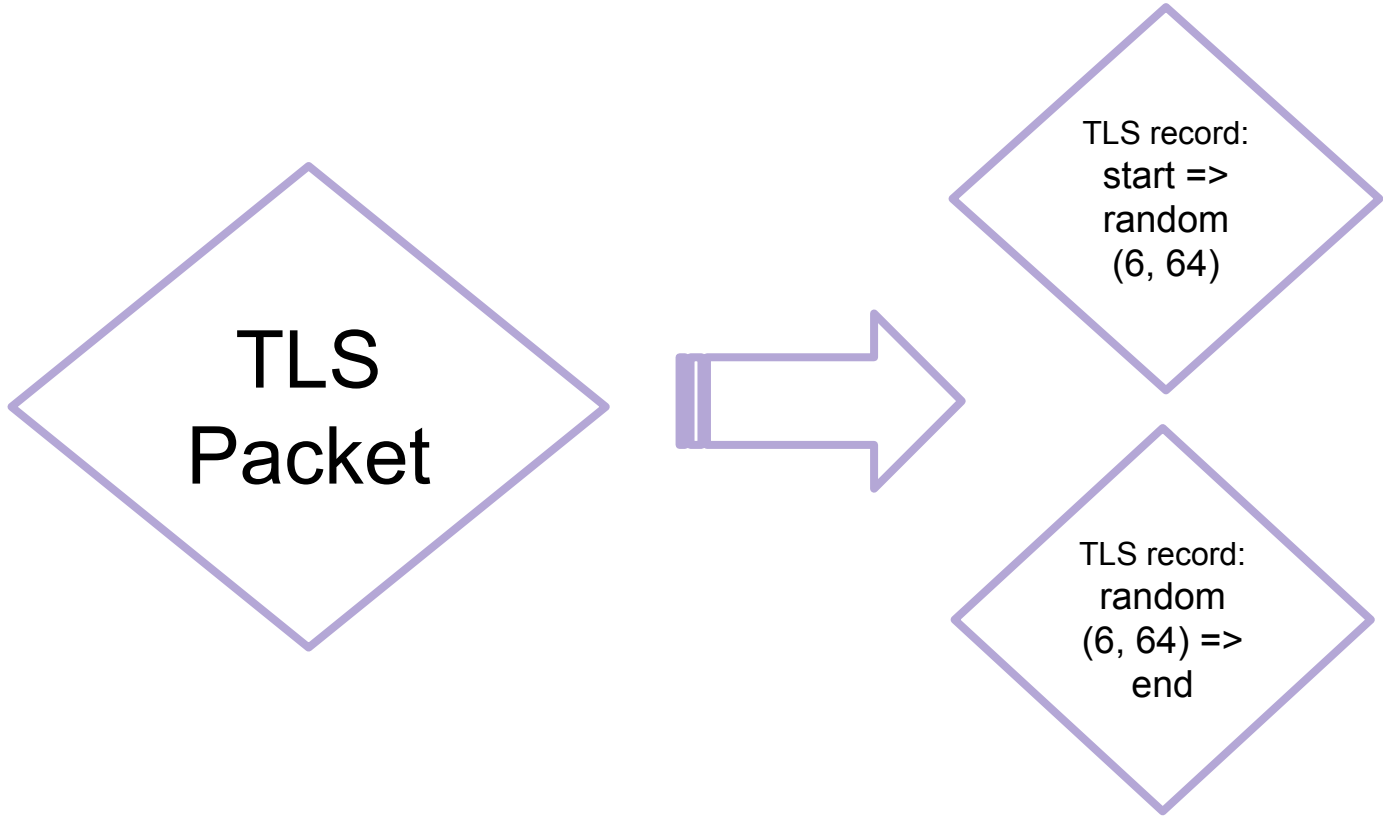
Fragmentation

Desync

Domain Fronting

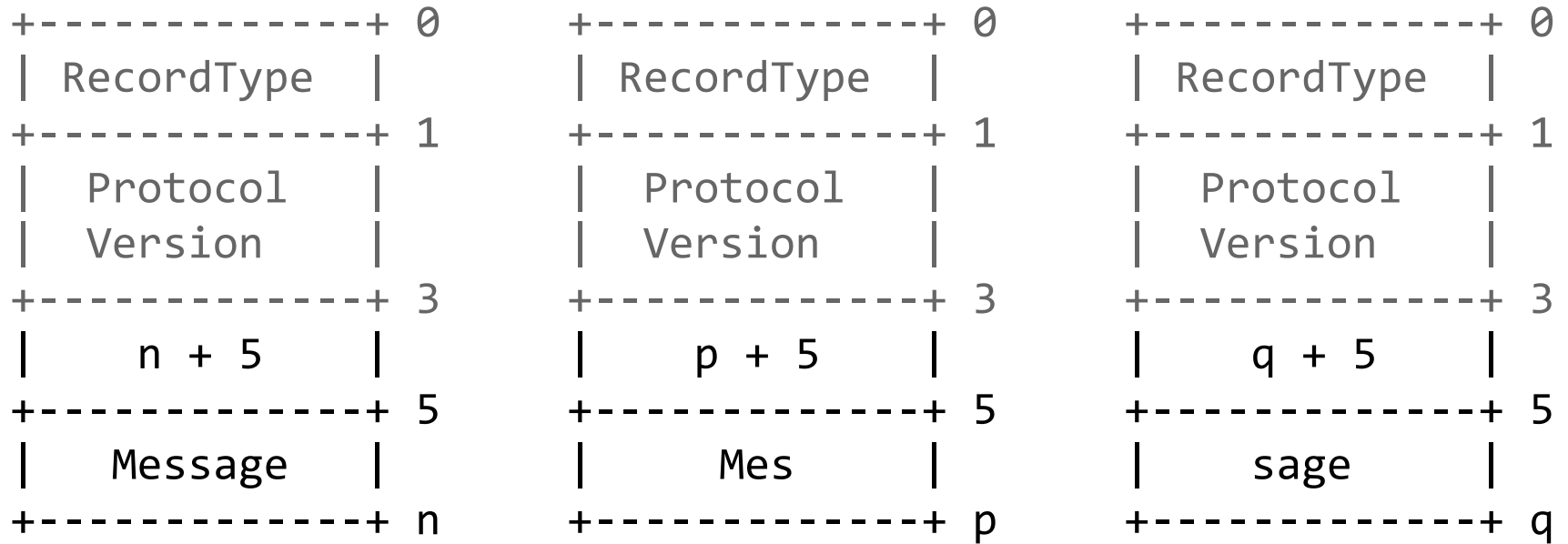
IP Fronting

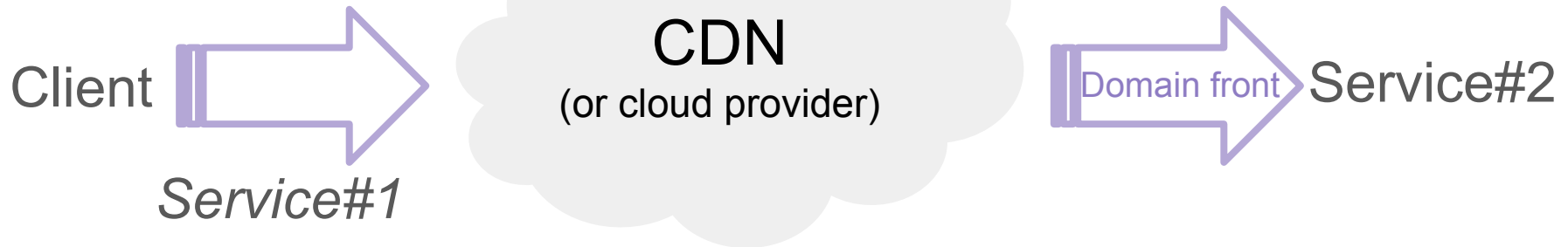
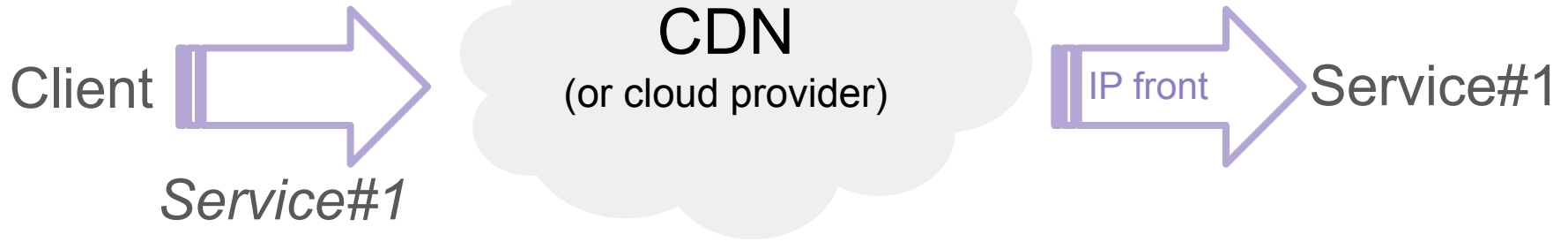






## TLS record fragmentation:







Go.

۳

argc, argv, auxv...?

cgo is not Go!

Memory safety.

SQLite.

۳

auxv.

₃

```
panic: runtime error: index out of range [1]  
with length 1
```

```
Fatal signal 6 (SIGABRT), code -6 (SI_TKILL) in  
tid 24352, pid 20760 (celzero.bravedns)  
#00 pc 0000000000451f08  
/data/app/com.celzero.bravedns-.../base.apk  
(offset 0x3120000) (runtime.raise.abi0+40)
```

۳

cgo.

۳

Go code & C code have to agree on ... address space, signal handlers, TLS slots ... Go's calling convention or growable stacks ... so a call down to C code must record all the details of the goroutine stack, switch to the C stack, and run C code which has no knowledge of how it was invoked, or the larger Go runtime in charge of the program.

... it is C's world, you're just living in it.



**MTE.**

۳

```
//go:nosplit
func findnull(s *byte) int {
    ...
    // pageSize is the unit we scan at a time
    looking for NULL.
    const pageSize = 4096
    ...
}
```



SQLite.



Network DNS

Search apps, IPs, domains

Zoho Mail	HTTPS	🇺🇸
<b>136.143.189.177</b> appctics.zoho.com	13:58:16	35 sec
2.8 KB ▲ / 8.5 KB ▼		
OBrain + 47 other app(s)	HTTPS	🇺🇸
<b>64.ff9b1.ffe:3436.4f2d</b> httpdns-push.heytapmobile.com	13:58:14	0 sec
0 B ▲ / 0 B ▼		
OBrain + 47 other app(s)	HTTPS	🇨🇦
<b>54.236.190.94</b> httpdns-push.heytapmobile.com	13:58:13	0 sec
0 B ▲ / 0 B ▼		
Zoho Mail	HTTPS	🇮🇳
<b>103.103.196.81</b> mproxy.zoho.in	13:58:11	Active
Zoho Mail	HTTPS	🇮🇳
<b>103.103.196.81</b> mproxy.zoho.in	13:58:11	Active
Zoho Mail	HTTPS	🇮🇳
<b>103.103.196.81</b> mproxy.zoho.in	13:58:11	Active
OBrain + 47 other app(s)	HTTPS	🇺🇸
<b>52.20.60.62</b> httpdns-push.heytapmobile.com	13:58:10	0 sec
0 B ▲ / 0 B ▼		
OBrain + 47 other app(s)	HTTPS	🇺🇸

1 hr 24 hr 7 day

Zoho Mail: Search domain names

🇺🇸	accounts.zoho.in	468
🇺🇸	appctics.zoho.com	347
🇺🇸	mproxy.zoho.in	243
🇺🇸	mproxy.zoho.com	193
🇺🇸	contacts.zoho.in	10

Network DNS

Search apps, IPs, domains

🇺🇸	vortex.data.microsoft.com	14:01:37	4ms
	Link to Windows		
	ZZ (0.0.0.0)		
🇺🇸	IPv6	DNS S3	
🇺🇸	vortex.data.microsoft.com	14:01:37	3ms
	Link to Windows		
	ZZ (-)		
🇺🇸	IPv4	DNS S3	
🇺🇸	vortex.data.microsoft.com	14:00:01	27ms
	Link to Windows		
	ZZ (0.0.0.0)		
🇺🇸	IPv6	DNS S3	
🇺🇸	vortex.data.microsoft.com	14:00:01	21ms
	Link to Windows		
	ZZ (-)		
🇺🇸	IPv4	DNS S3	🟢
🇺🇸	cloudconf-app-in.heytapmobile.com	13:59:14	22ms
	Phone Manager		
	ZZ (0.0.0.0)		
🇺🇸	IPv6	DNS S3	🟢
🇺🇸	cloudconf-app-in.heytapmobile.com	13:59:14	19ms
	Phone Manager		
	ZZ (-)		
🇺🇸	IPv4	DNS S3	🟢
🇺🇸	cloudconf-app-in.heytapmobile.com	13:58:44	33ms
	Phone Manager		
	ZZ (0.0.0.0)		
🇺🇸	IPv6	DNS S3	🟢
🇺🇸	cloudconf-app-in.heytapmobile.com	13:58:44	23ms
	Phone Manager		
	ZZ (-)		

۳

Batching writes

Write-heavy in-memory table

Analytical queries

Backup & restore



**FOSS.**

⚡

... I've been happily using RethinkDNS in recent days, integrating it with Orbot's SOCKS proxying. This gives me a VPN-based Firewall, more secure DNS-over-HTTPS/TLS options, & traffic over Tor in one smooth setup.

⚡

Obscure networks

Widely-deployed but fragmented

OS ecosystem

Observability & security layer

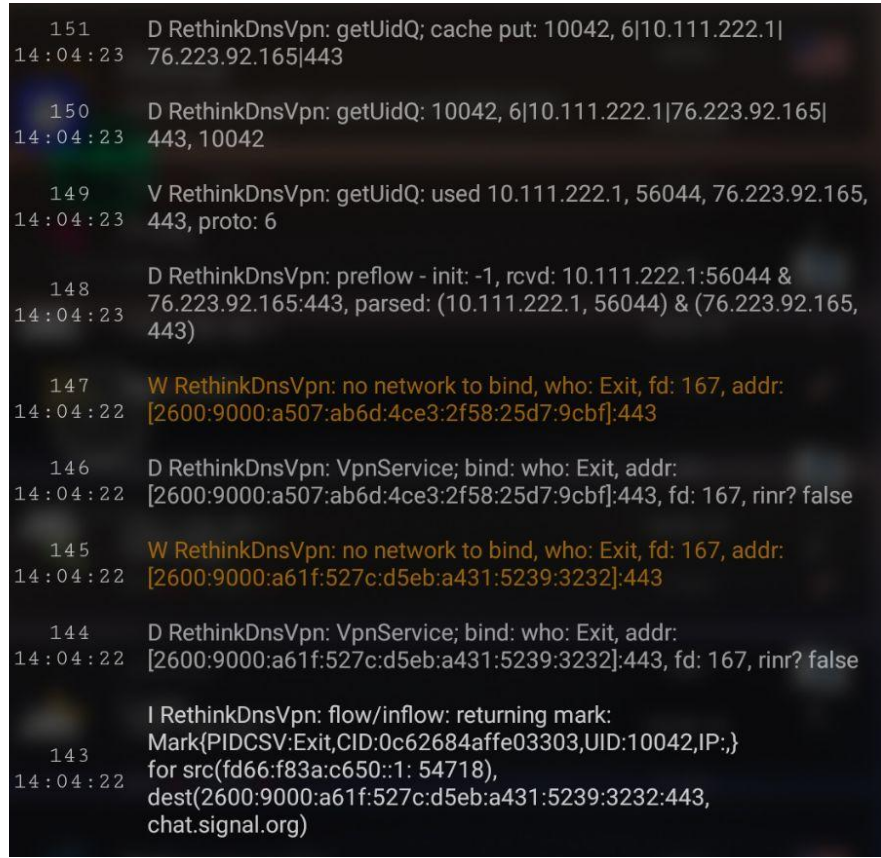
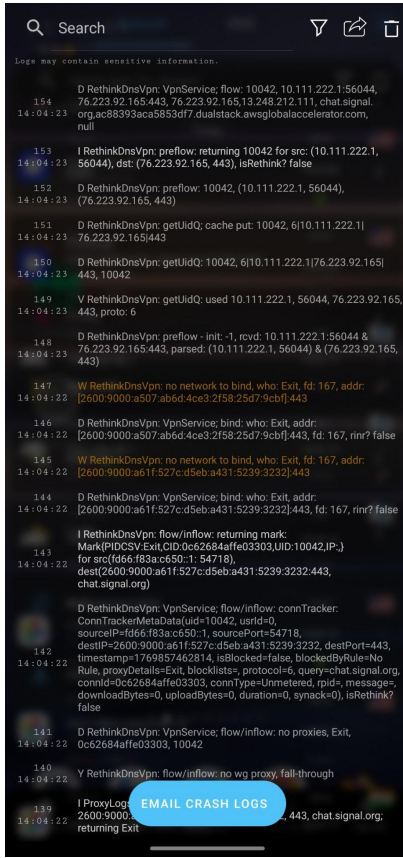
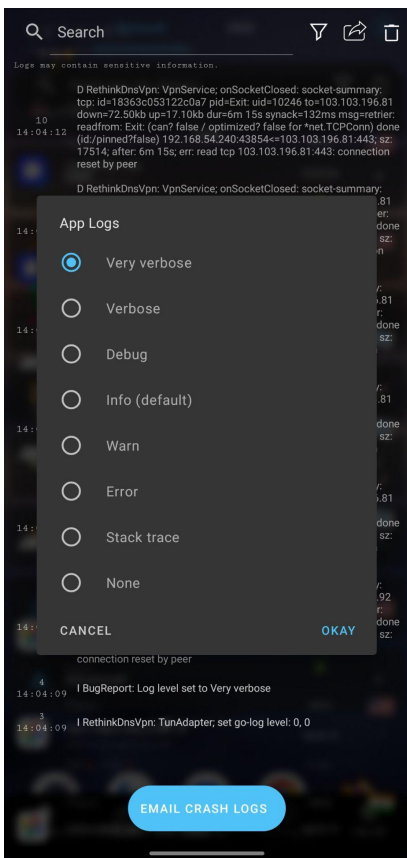
⚡

Real-time logs & stats.

Bug capture & reports.

Telegram & subreddit.

Translations.

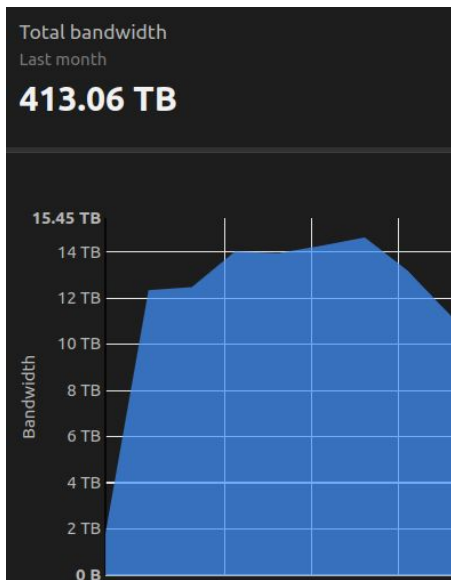




3M  
500TB

900K  
Play Store

150K  
F-Droid



### VPNs

1. ProtonVPN - Secure and Free VPN 611\_343
2. Rethink: DNS + Firewall + VPN 150\_915
3. Mullvad VPN: privacy is a universal right 150\_693
4. Tailscale 127\_490
5. Calyx VPN 107\_032
6. WG Tunnel 102\_494
7. RiseupVPN 91\_547
8. Windscribe 73\_392

o

# Funding.

•

... Sponsor the development of the Rethink DNS + Firewall open source project, on which 2 engineers work full-time. As of March 2025, our costs are \$1500 per month.

•

Mozilla Builders

FLOSS United

FLOSS/fund

Cloudflare

# Mozilla Builders.

•

July to Oct '20

21 among 1200 teams

Mentorship

\$12K



**FOSS United.**

◦

'23 & '24

India-focused

Active support

\$12K

FLOSS/fund.

•

'25

India-based

No strings attached

\$25K



Cloudflare.

•

'20 - '26

Infrastructure credits

Enterprise support

O(\$\$\$)

03 [research.google/pubs/the-android-platform-security-model](https://research.google/pubs/the-android-platform-security-model)  
05 [hernan.de/blog/tailoring-cve-2019-2215-to-achieve-root](https://hernan.de/blog/tailoring-cve-2019-2215-to-achieve-root)  
14 [github.com/celzero/rethink-app/issues/224](https://github.com/celzero/rethink-app/issues/224)  
16 [news.ycombinator.com/item?id=45562664](https://news.ycombinator.com/item?id=45562664)  
21 [github.com/serverless-dns/lfu-cache/blob/2812043995e/strat/o1.js#L23](https://github.com/serverless-dns/lfu-cache/blob/2812043995e/strat/o1.js#L23)  
28 [datatracker.ietf.org/doc/html/rfc4787](https://datatracker.ietf.org/doc/html/rfc4787)  
28 [datatracker.ietf.org/doc/html/rfc5382](https://datatracker.ietf.org/doc/html/rfc5382)  
40 [github.com/golang/go/issues/25035](https://github.com/golang/go/issues/25035)  
42 [dave.cheney.net/2016/01/18/cgo-is-not-go](https://dave.cheney.net/2016/01/18/cgo-is-not-go)  
44 [github.com/golang/go/blob/acd65ebb13a/src/runtime/string.go#L508](https://github.com/golang/go/blob/acd65ebb13a/src/runtime/string.go#L508)  
48 [x.com/rethinkdns/status/1706356861350580261](https://x.com/rethinkdns/status/1706356861350580261)  
51 [gitlab.com/fdroid/wiki/-/wikis/Featured-Apps](https://gitlab.com/fdroid/wiki/-/wikis/Featured-Apps)  
53 [svc.rethinkdns.com/r/sponsor](https://svc.rethinkdns.com/r/sponsor)  
58  
[medium.com/mozilla-builders/mozilla-builders-fix-the-internet-showcase-24-awesome-pitches-much-much-more-fcd9c9ebb042](https://medium.com/mozilla-builders/mozilla-builders-fix-the-internet-showcase-24-awesome-pitches-much-much-more-fcd9c9ebb042)  
60 [fossunited.org/blog/organization/announcing-follow-on-grant-to-rethink-dns](https://fossunited.org/blog/organization/announcing-follow-on-grant-to-rethink-dns)  
62 [floss.fund/blog/second-tranche-2025-anniversary](https://floss.fund/blog/second-tranche-2025-anniversary)

**Merci. Bedankt.**

FOSDEM 2026

Murtaza Aliakbar