

USENIX SECURITY 2026

Revelio: A Global Study of VoIP Blocking

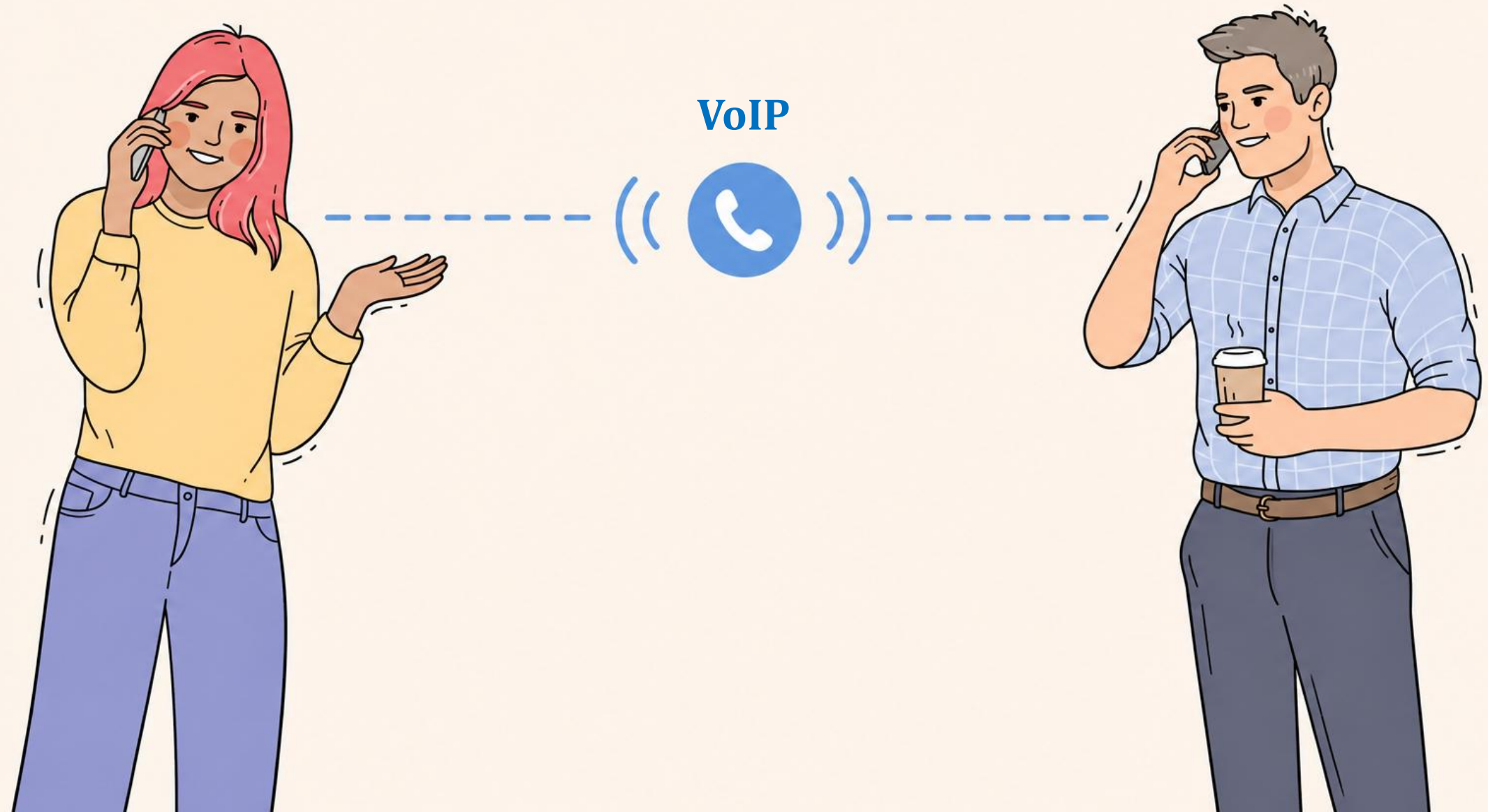
The first remote, global measurement of VoIP call censorship

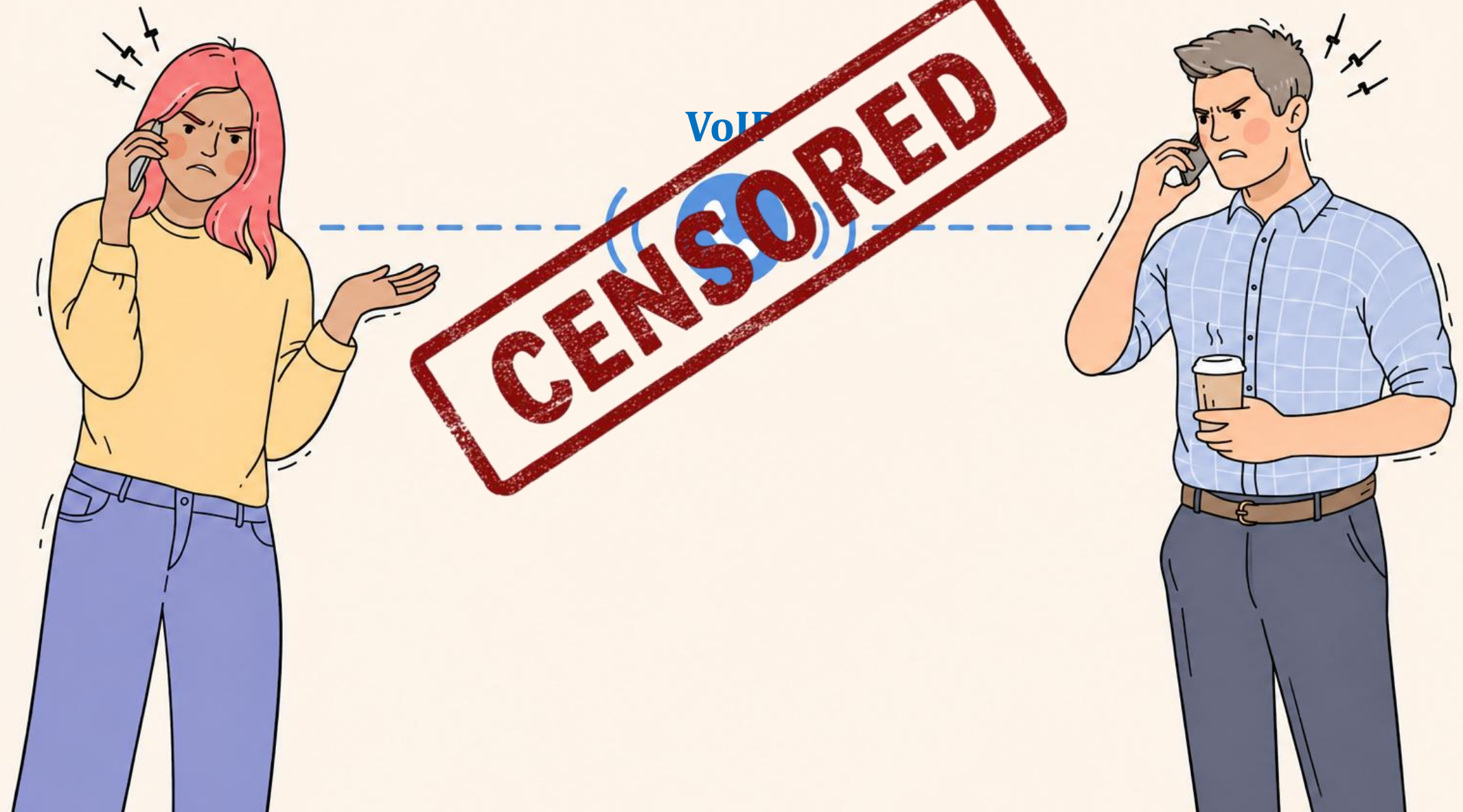
Arjun Gupta
IIT Bombay

Roya Ensafi
University of Michigan

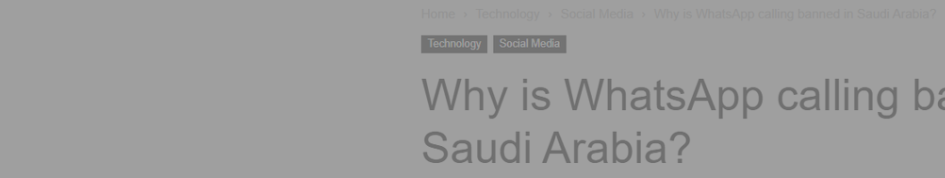
Piyush Kumar
IIT Delhi

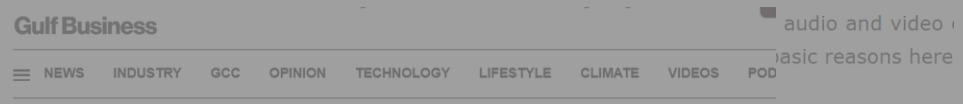
Devashish Gosain
IIT Bombay

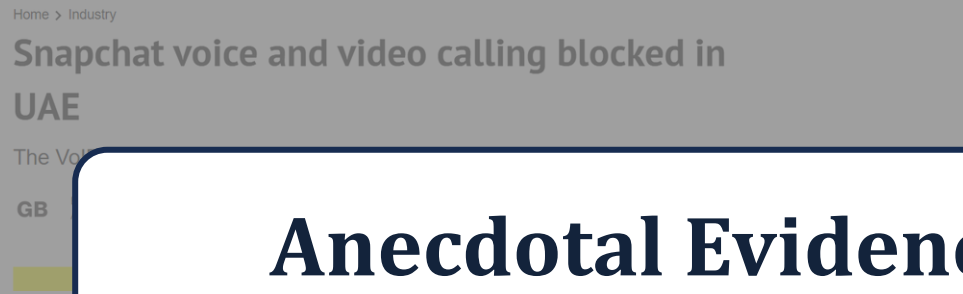

VoIP

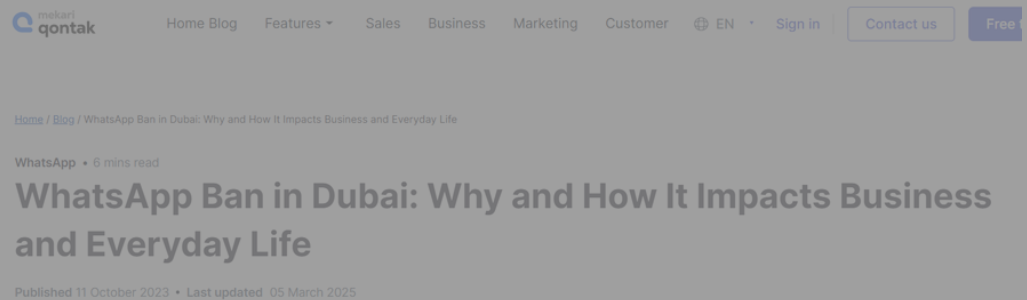

VoIP
CENSORED

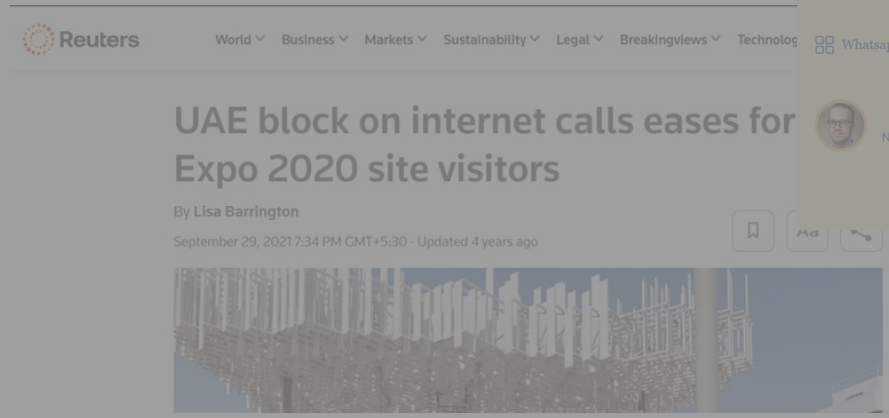
Anecdotal Evidences For Call Blocking



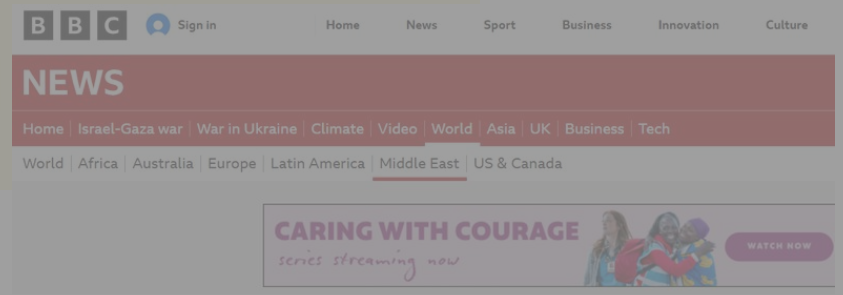












Home › Technology › Social Media › Why is WhatsApp calling banned in Saudi Arabia?

Technology Social Media

Why is WhatsApp calling banned in Saudi Arabia?

audio and video
basic reasons here

Gulf Business

NEWS INDUSTRY GCC OPINION TECHNOLOGY LIFESTYLE CLIMATE VIDEOS POD

Home › Industry

Snapchat voice and video calling blocked in UAE

The VoIP service is the latest to be blocked in the country

GB BY ROBERT ANDERSON
APRIL 10, 2016

FOLLOW US

mekari qontak Home Blog Features Sales Business Marketing Customer EN Sign in Contact us Free

Home / Blog / WhatsApp Ban in Dubai: Why and How It Impacts Business and Everyday Life

WhatsApp • 6 mins read

WhatsApp Ban in Dubai: Why and How It Impacts Business and Everyday Life

Published 11 October 2023 • Last updated 05 March 2025

Written by: Pamela

MenaVPN VPN servers Download Pricing Blog Support

Why is WhatsApp banned in Egypt

Whatsapp Call September 28th, 2023

Written By Nigel Thompson

Last Updated March 13th, 2024

Reuters World Business Markets Sustainability Legal Breakingviews Technolog

UAE block on internet calls eases for Expo 2020 site visitors

By Lisa Barrington

September 29, 2021 7:34 PM GMT+5:30 · Updated 4 years ago



BBC Sign in Home News Sport Business Innovation Culture

NEWS

Home | Israel-Gaza war | War in Ukraine | Climate | Video | World | Asia | UK | Business | Tech

World | Africa | Australia | Europe | Latin America | Middle East | US & Canada

CARING WITH COURAGE
series streaming now
WATCH NOW

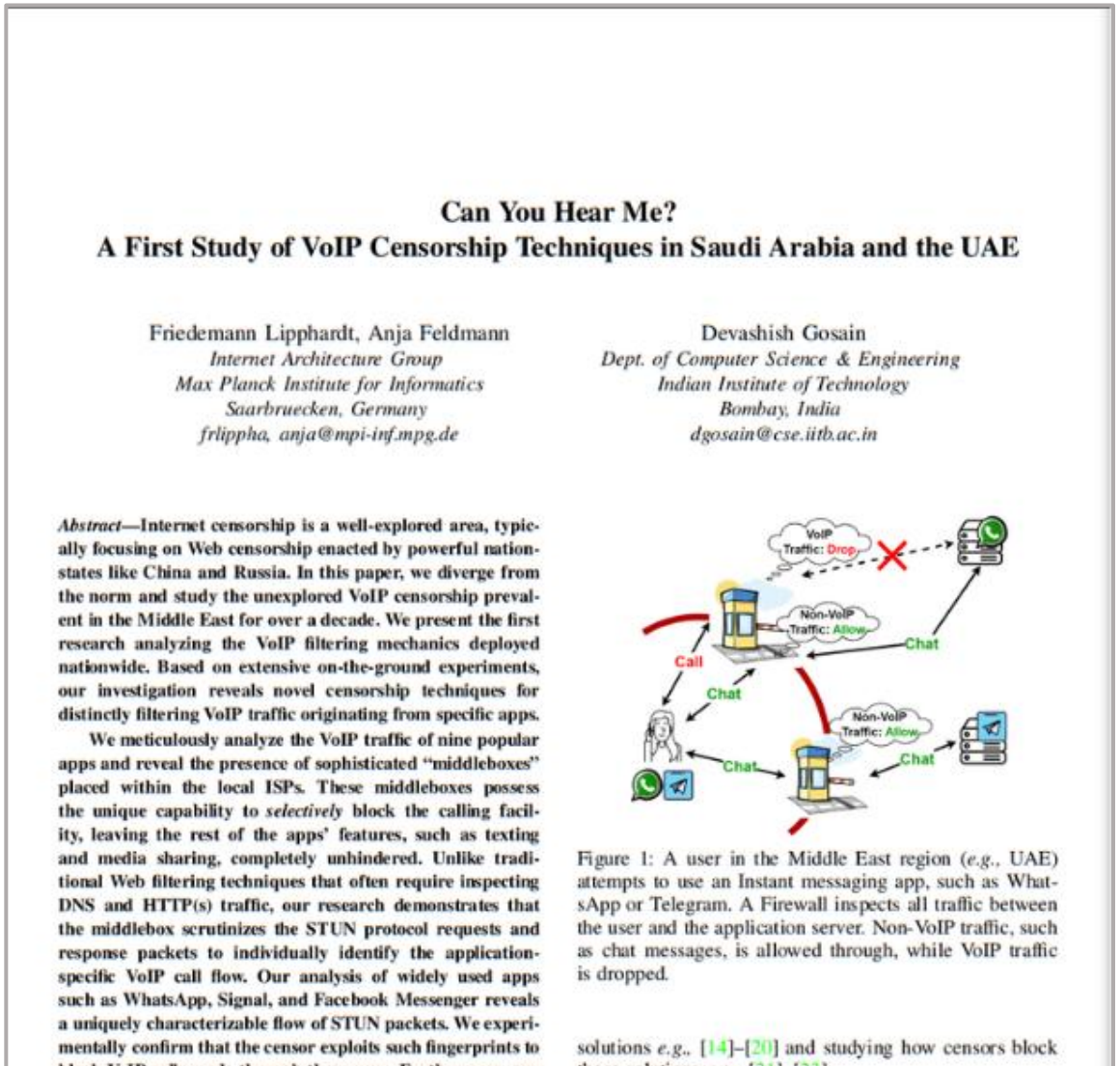
Saudi Arabia blocks Viber messaging service

6 June 2013

Why Studying VoIP Censorship Is Tough?

(Mechanics of VoIP censorship is completely unknown)

Liphardt et. al. (Euro S&P 2025)



Can You Hear Me?
A First Study of VoIP Censorship Techniques in Saudi Arabia and the UAE

Friedemann Lipphardt, Anja Feldmann
Internet Architecture Group
Max Planck Institute for Informatics
Saarbruecken, Germany
frlippha, anja@mpi-inf.mpg.de

Devashish Gosain
Dept. of Computer Science & Engineering
Indian Institute of Technology
Bombay, India
dgosain@cse.iitb.ac.in

***Abstract*—Internet censorship is a well-explored area, typically focusing on Web censorship enacted by powerful nation-states like China and Russia. In this paper, we diverge from the norm and study the unexplored VoIP censorship prevalent in the Middle East for over a decade. We present the first research analyzing the VoIP filtering mechanics deployed nationwide. Based on extensive on-the-ground experiments, our investigation reveals novel censorship techniques for distinctly filtering VoIP traffic originating from specific apps.**

We meticulously analyze the VoIP traffic of nine popular apps and reveal the presence of sophisticated "middleboxes" placed within the local ISPs. These middleboxes possess the unique capability to *selectively* block the calling facility, leaving the rest of the apps' features, such as texting and media sharing, completely unhindered. Unlike traditional Web filtering techniques that often require inspecting DNS and HTTP(s) traffic, our research demonstrates that the middlebox scrutinizes the STUN protocol requests and response packets to individually identify the application-specific VoIP call flow. Our analysis of widely used apps such as WhatsApp, Signal, and Facebook Messenger reveals a uniquely characterizable flow of STUN packets. We experimentally confirm that the censor exploits such fingerprints to

Figure 1: A user in the Middle East region (*e.g.,* UAE) attempts to use an Instant messaging app, such as WhatsApp or Telegram. A Firewall inspects all traffic between the user and the application server. Non-VoIP traffic, such as chat messages, is allowed through, while VoIP traffic is dropped.

solutions *e.g.,* [14]–[20] and studying how censors block



Confirmed VoIP filtering pattern in two Middle Eastern countries

1. Saudi Arabia (SA)
2. United Arab Emirates (UAE)

For VoIP apps like WhatsApp & Signal

Research Gap Identified



Measuring VoIP censorship involved physical travel

- Using VPNs, VPS they were unable to trigger VoIP filtering remotely



Methodology is not scalable and cost ineffective

- Measurements need to run for one country at a time for limited apps during on ground tests

THE MEASUREMENT GAP

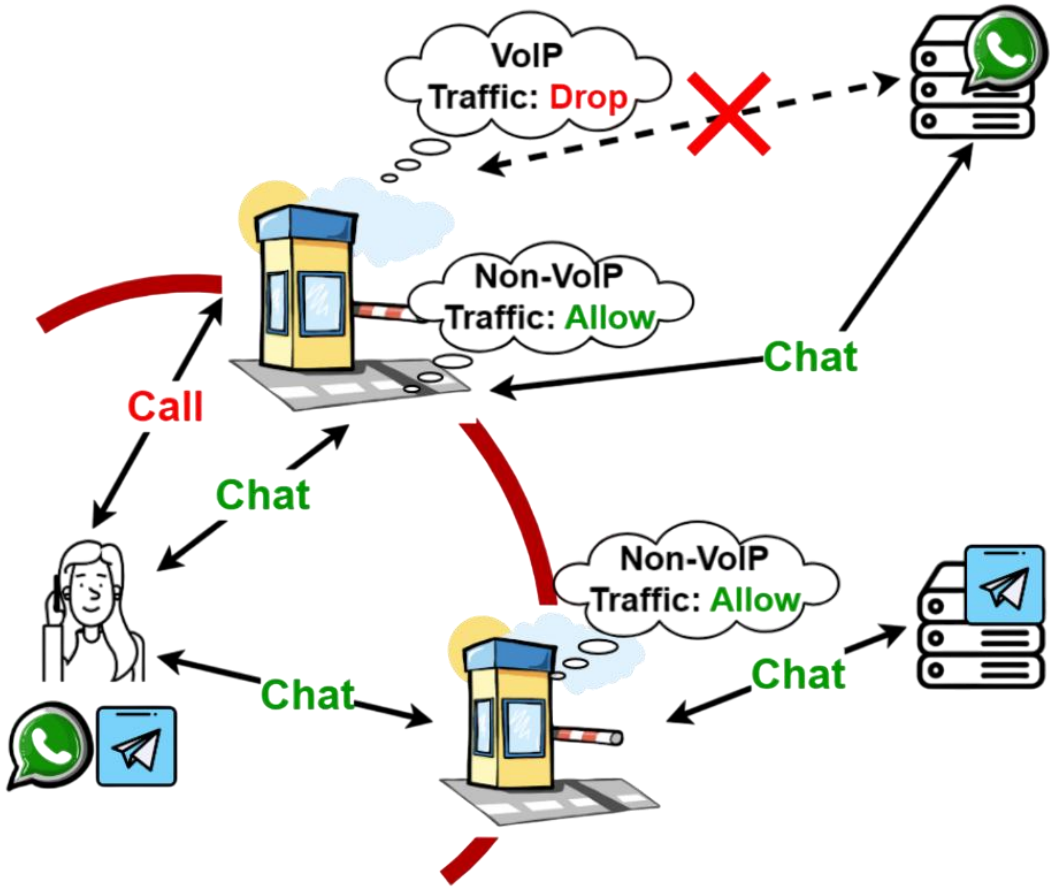
2

countries covered by prior work

Revelio: 71 countries

fully remote, no in person visits

Key Observation

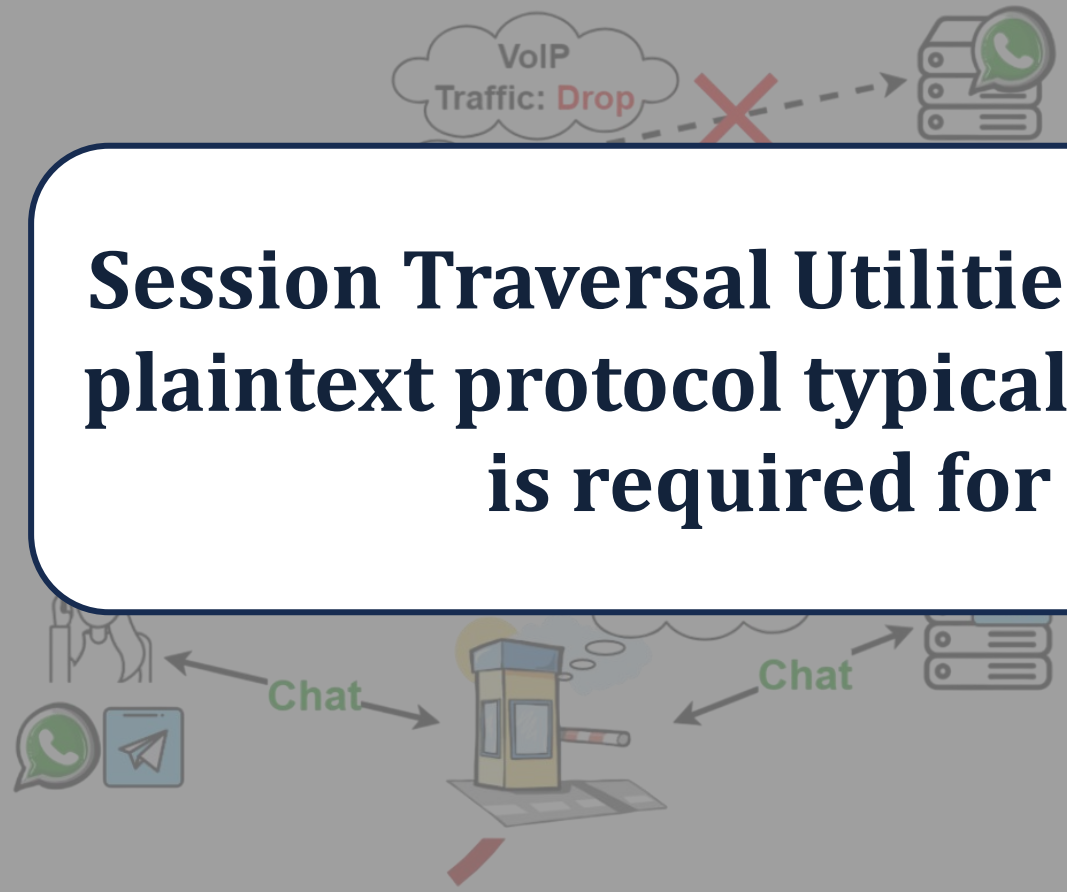


Specific blocking of VoIP calls but not the chats
Lipphardt et. al. (Euro S&P 2025)

IMPORTANT QUESTION -

How can censor block specific VoIP call traffic even for end-to-end encrypted IM app?

Key Observation

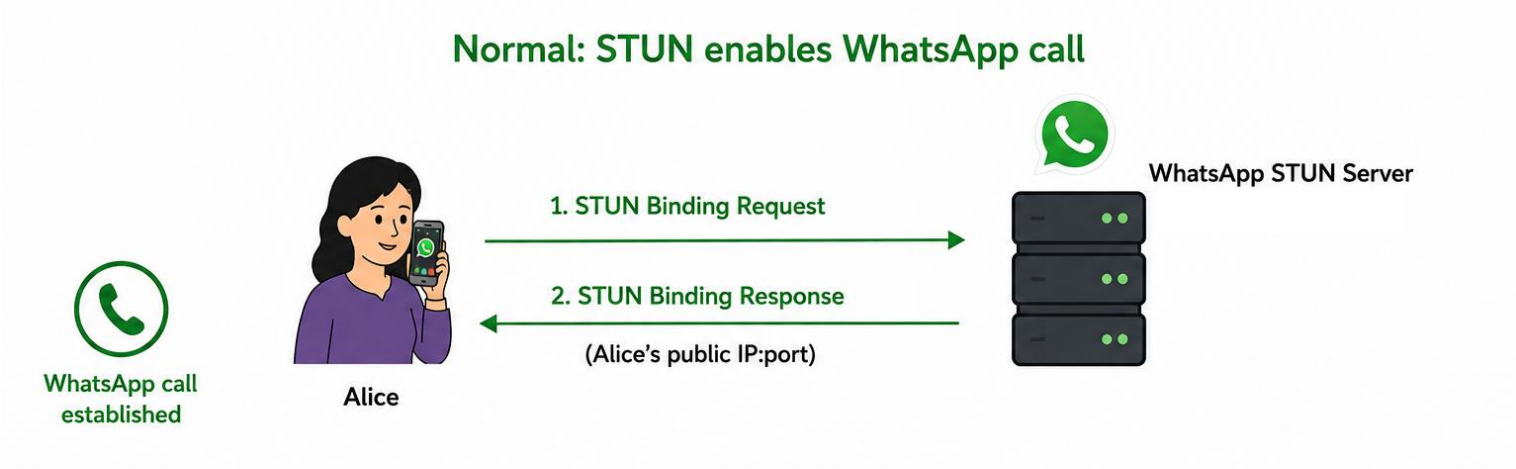


Session Traversal Utilities for NAT (STUN) is a plaintext protocol typically sent over UDP and is required for a VoIP call

Specific blocking of VoIP calls but not the chats
Lipphardt et. al. (Euro S&P 2025)

Key Observation

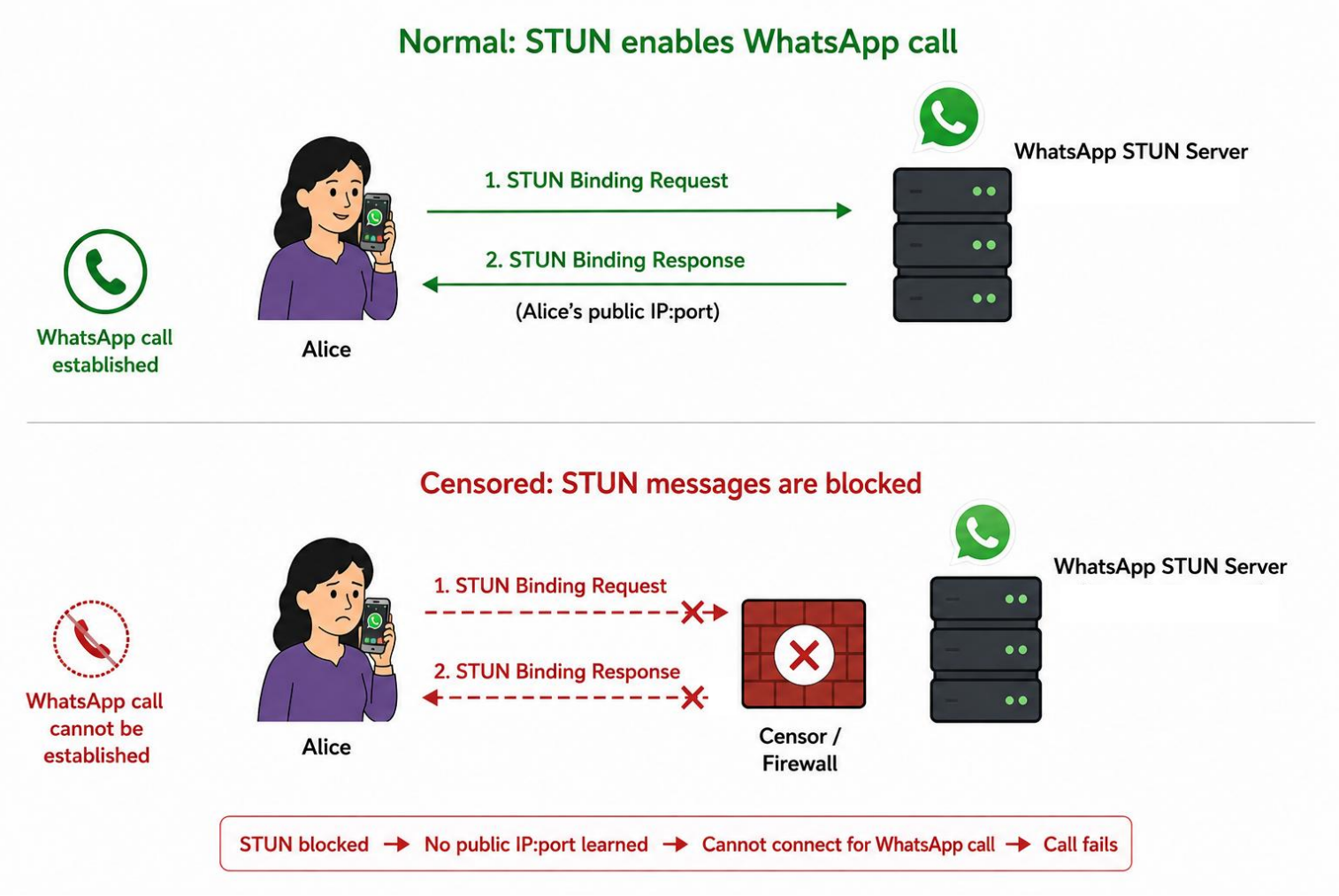
Normal flow for VoIP call establishment which requires STUN protocol for NAT traversal



Key Observation

Normal flow for VoIP call establishment which requires STUN protocol for NAT traversal

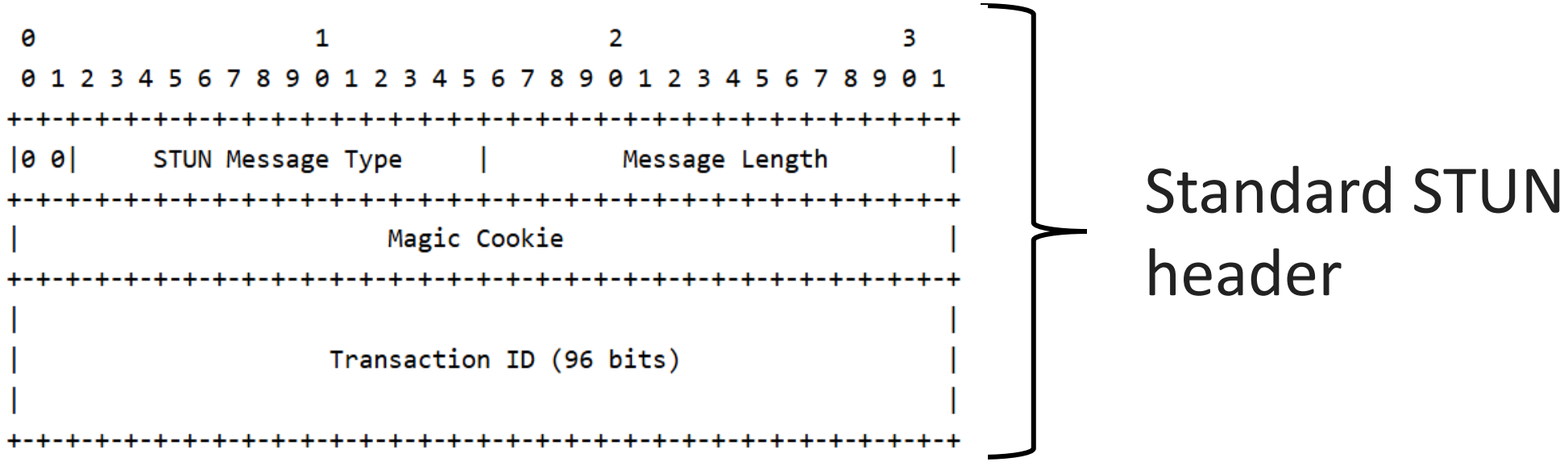
Lipphardt et. al. (Euro S&P 2025) reported that STUN protocol was specifically targeted for disrupting VoIP calls



How Did Censor Identify The STUN Packets To Block

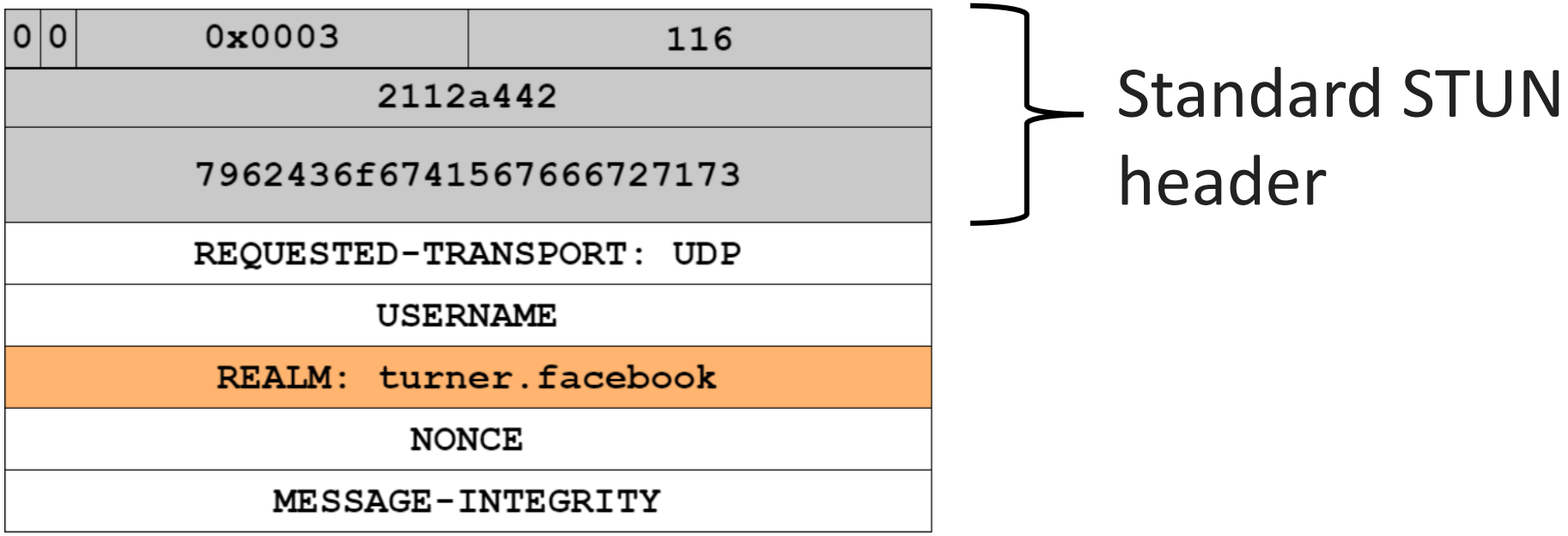
(App-Specific STUN Fingerprints)

STUN Fingerprints



Standard STUN header

STUN Fingerprints



Facebook Messenger STUN packet

Contains a plaintext string field “turner.facebook” which is easily detectable by censor

STUN Fingerprints

0	0	0x0003	116
2112a442			
7962436f6741567666727173			
REQUESTED-TRANSPORT: UDP			
USERNAME			
REALM: turner.facebook			
NONCE			
MESSAGE-INTEGRITY			

Facebook Messenger STUN packet

Contains a plaintext string field “turner.facebook” which is easily detectable by censor

0	0	0x0003	352
2112a442			
cd857b14f17d6c2b6d7c4b50			
Unknown attribute 0x4000			
RESERVATION-TOKEN			
RESERVATION-TOKEN			
RESERVATION-TOKEN			
Unknown attribute 0x4024			
XOR-RELAYED-ADDRESS			
MESSAGE-INTEGRITY			

WhatsApp STUN packet

Has unique attribute types which are not used by any other app, thus making it a distinct feature

STUN Fingerprints

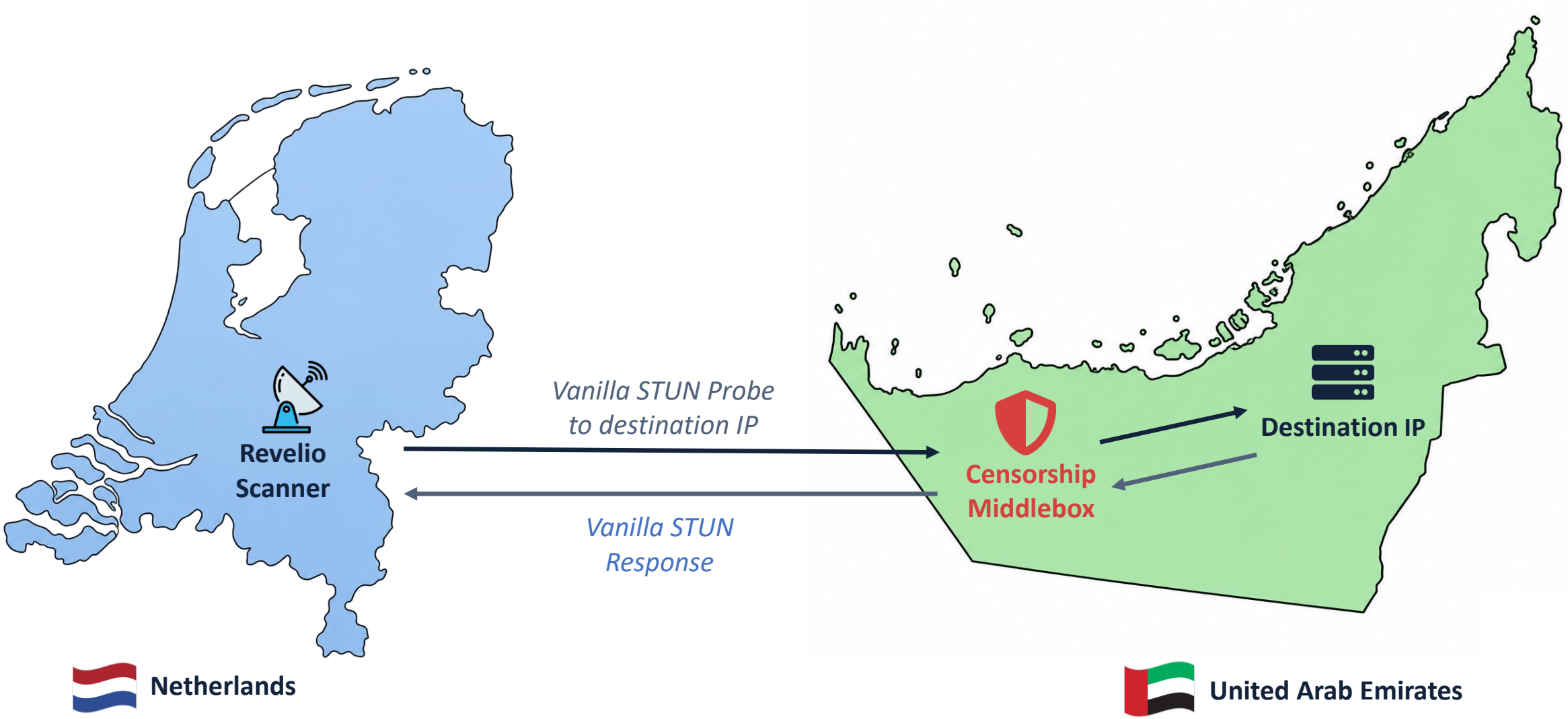
App	Packet Type	Fingerprinting Features
WhatsApp	Allocate Request Allocate Success Response	Unknown attributes: 0x4000, 0x4024, 0x4025, 0x4002
Telegram	Allocate Request Allocate Error Response Create Permission Request Channel Bind Request Refresh Request	Realm: telegram.org Destination port: 1400 Lifetime: 60 secs
Signal	Allocate Request Allocate Error Response Create Permission Request	Realm: turn.cloudflare.com signal.org Username regex: ^g.{64}$ Lifetime: 600 secs
Messenger Instagram	Allocate Request Allocate Error Response Allocate Success Response Create Permission Request Binding Request Binding Success Response	Unknown attributes: 0x4000, 0x4002, 0xcb01, 0xdaba Realm: turner.facebook Lifetime: 900 secs Destination port: 40003
Viber	Allocate Request Allocate Success Response	Realm: viber.com Lifetime: 600 secs Destination port: 443
Slack	Allocate Request Allocate Error Response Create Permission Request	Realm: *.app.chime.aws Lifetime: 600 secs
Webex	Binding Request	Software attribute: Cisco-Spark
Dialpad	Allocate Request Allocate Error Response Create Permission Request Refresh Request	Realm: ubervoip.net Username: fstelephony Software: Coturn-4.5.2 'dan Eider'
Jitsi Meet	Allocate Request Binding Success Response Create Permission Request	Realm: coturn.jitsi.net Destination port: 443 Username: 1766056259 (10)) Software: ice4j.org
Wire	Allocate Request Allocate Error Response Binding Success Response Create Permission Request	Realm: dummy.io Software: Coturn-wireapp/4.6.2j Username pattern: d=*.v=1.k=0.t=s.*
Teams	Allocate Request	Malformed/non-compliant STUN packets

We observed multiple STUN fingerprints in these popular VoIP apps

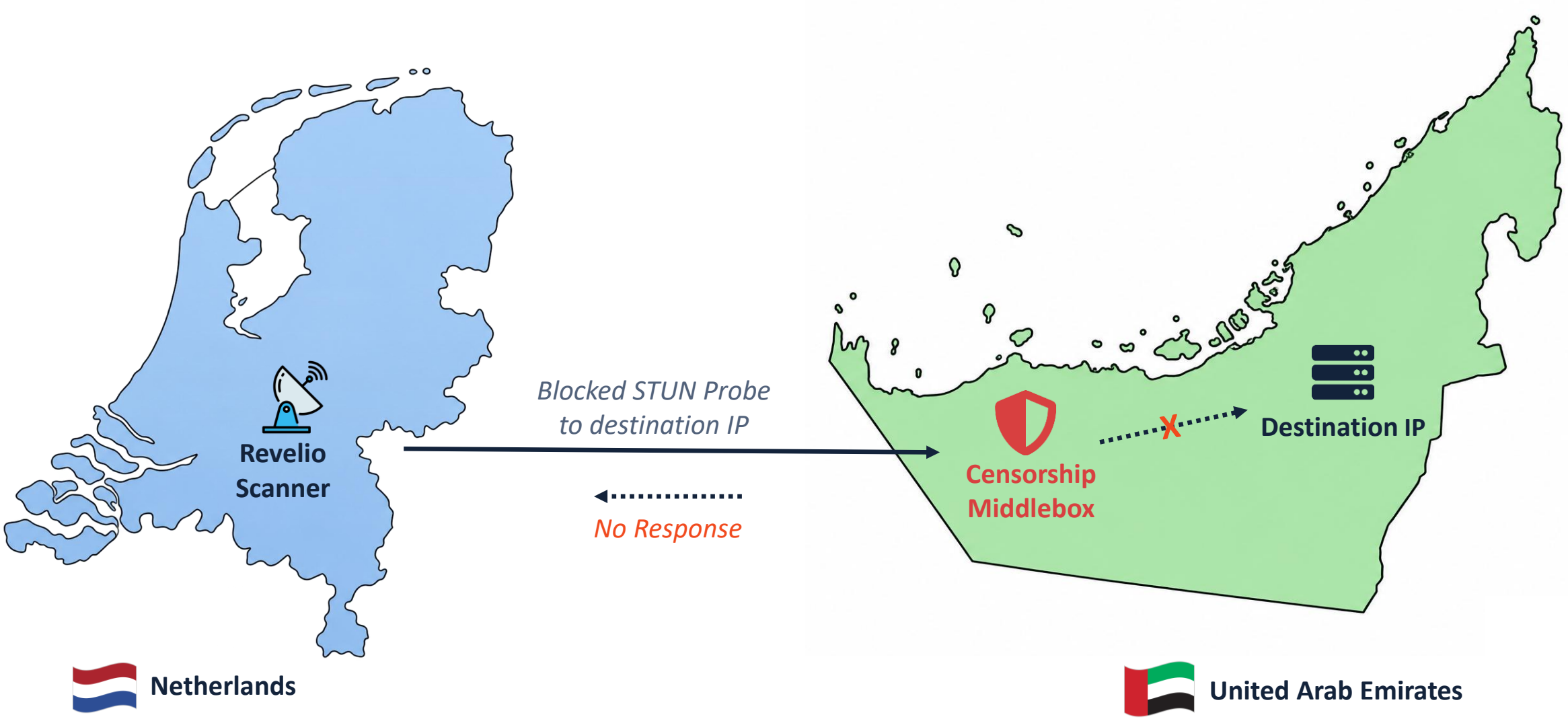
Let’s Deep Dive Into Revelio

(High Level Core Idea)

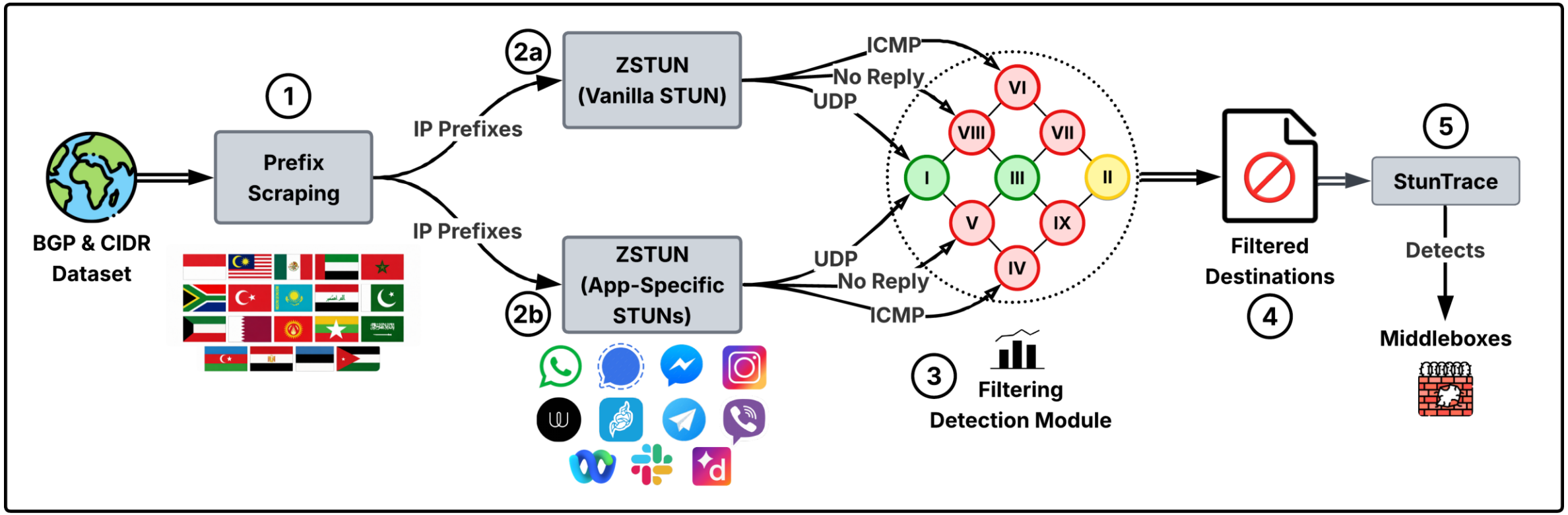
Detecting Censorship By Comparing Replies



Detecting Censorship By Comparing Replies



Overview Of Revelio



Collecting IP Prefixes Of Target Countries

HURRICANE ELECTRIC INTERNET SERVICES

Search

Networks: United Arab Emirates

Quick Links | Country Info

BGP Toolkit Home
BGP Prefix Report
BGP Peer Report
Super Traceroute
Super Looking Glass
Cert Search
Exchange Report
Bogon Routes
World Report
Multi Origin Routes
DNS Report
Top Host Report
RPKI & ASPA Report
Internet Statistics
Looking Glass
Network Tools App
IPv6 Certification
IPv6 Progress
Contribute Data
Credits
Contact Us

Networks: United Arab Emirates

ASN	Name	Adjacencies v4	Routes v4	Adjacencies v6	Routes v6
AS8529	Zain Omantel International FZ-LLC	1,710	2,170	1,629	1,222
AS8966	Etisalat - Emirates Telecommunications Corporation	1,340	3,274	582	284
AS15802	Emirates Integrated Telecommunications Company PJSC	1,179	356	321	270
AS59692	IQWeb FZ-LLC	292	485	8	1
AS60051	Earthlink Telecommunications Equipment Trading & Services DMCC	230	701	83	17
AS216071	SERVERS TECH FZCO	175	611	11	4
AS57187	Emirates Integrated Telecommunications Company PJSC	70	72	29	12
AS49813	Innova Co S.A.R.L.	70	7	0	0
AS41268	Sesameware FZ-LLC	68	7	20	3
AS200851	Bamboozle Web Services MEA FZ-LLC	65	9	50	10
AS51247	SkyCore Technologies L.L.C-FZ	61	13	61	3
AS200236	Saif Mohammed Alashram trading as Privacy Cloud Service & Datacenters Providers	59	1	60	4
AS215174	ProNow Tech CO. L.L.C	46	3	18	1
AS214362	MYGAMES MENA FZ LLC	44	1	0	0
AS5384	EMIRATES TELECOMMUNICATIONS GROUP COMPANY (ETISALAT GROUP) PJSC	35	2,817	2	815
AS60849	iLevant FZE	22	18	7	3
AS215730	H2NEXUS CLOUD SERVICES - FZCO	18	34	12	4
AS208800	G42 CLOUD TECHNOLOGY L.L.C.	16	23	4	1

+



Report for 8529

Name

OMANTEL-AS - Zain Omantel International FZ-LLC, AE

AS Adjacency Report

In the context of this report "Upstream" indicates that there is an adjacent AS that lines between the BGP table collection point (in this case at AS2.0) and the specified AS. Similarly, "Downstream" refers to an adjacent AS that lies beyond the specified AS. This upstream / downstream categorisation is strictly a description relative topology, and should not be confused with provider / customer / peer inter-AS relationships.

```
8529 OMANTEL-AS - Zain Omantel International FZ-LLC, AE

  Adjacency:    60  Upstream:    13  Downstream:    47
Upstream Adjacent AS list
  AS4637          ASN-TELSTRA-GLOBAL - Telstra Global, HK
  AS31452         ZAIN-BH-AS - ZAIN BAHRAIN B.S.C., BH
  AS39273         Kalaam-Telecom - Kalaam Telecom Bahrain B.S.C., BH
  AS137409        GSLNETWORKS-AS-AP - GSL Networks Pty LTD, AU
  AS3257          GTT-BACKBONE - GTT Communications Inc., US
  AS2497          IIJ - Internet Initiative Japan Inc., JP
  AS1299          TWELVE99 - Arelion Sweden AB, SE
  AS3320          DTAG - Deutsche Telekom AG, DE
```

Hurricane Electric Website (e.g., AS Information)

CIDR Report (e.g., Announced Prefixes)

Scraping websites to store IP prefixes for each target country (e.g., UAE)

Internet Wide Scans

Remote scanning at Internet scale requires

- Sending STUN packets to the complete IPv4 address space (millions of IPs) for a country
- Storing and analysing the response
- Repeating for multiple countries



Probing at Mass Scale For STUN



Zstun OUR TOOL

STUN-aware scanner

Scans a country's whole IPv4 space to find STUN endpoints, then sends three probe type to each.

Detecting One Case, Powered By Zstun

Zstun

OUR TOOL

STUN-aware scanner

Scans a country's whole IPv4 space to find STUN endpoints, then sends three probes to each: P1 vanilla · P2 app-specific · P3 obfuscated

PROBE TYPES

P1	Vanilla STUN
P2	App-specific STUN
P3	Obfuscated STUN

Detecting One Case, Powered By Zstun

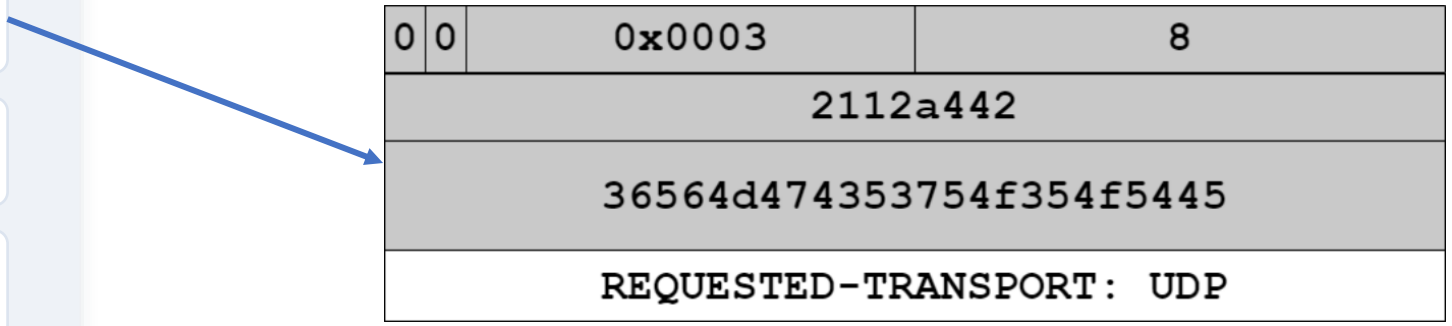
Zstun OUR TOOL

STUN-aware scanner

Scans a country's whole IPv4 space to find STUN endpoints, then sends three probes to each: P1 vanilla · P2 app-specific · P3 obfuscated

PROBE TYPES

P1	**Vanilla STUN**
P2	**App-specific STUN**
P3	**Obfuscated STUN**



Detecting One Case, Powered By Zstun

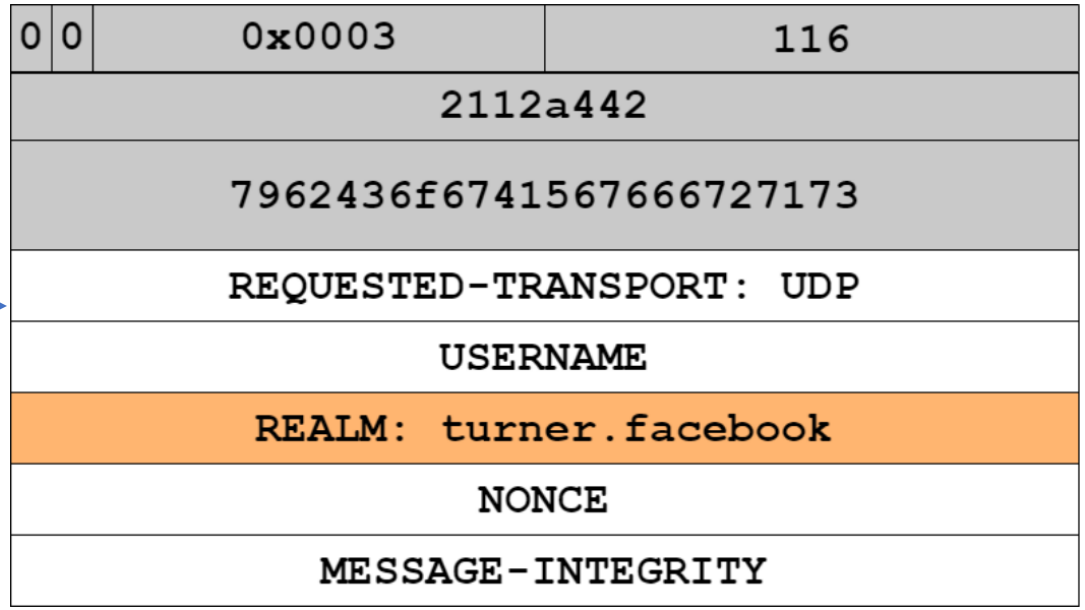
Zstun OUR TOOL

STUN-aware scanner

Scans a country's whole IPv4 space to find STUN endpoints, then sends three probes to each: P1 vanilla · P2 app-specific · P3 obfuscated

PROBE TYPES

P1	Vanilla STUN
P2	App-specific STUN
P3	Obfuscated STUN



Detecting One Case, Powered By Zstun

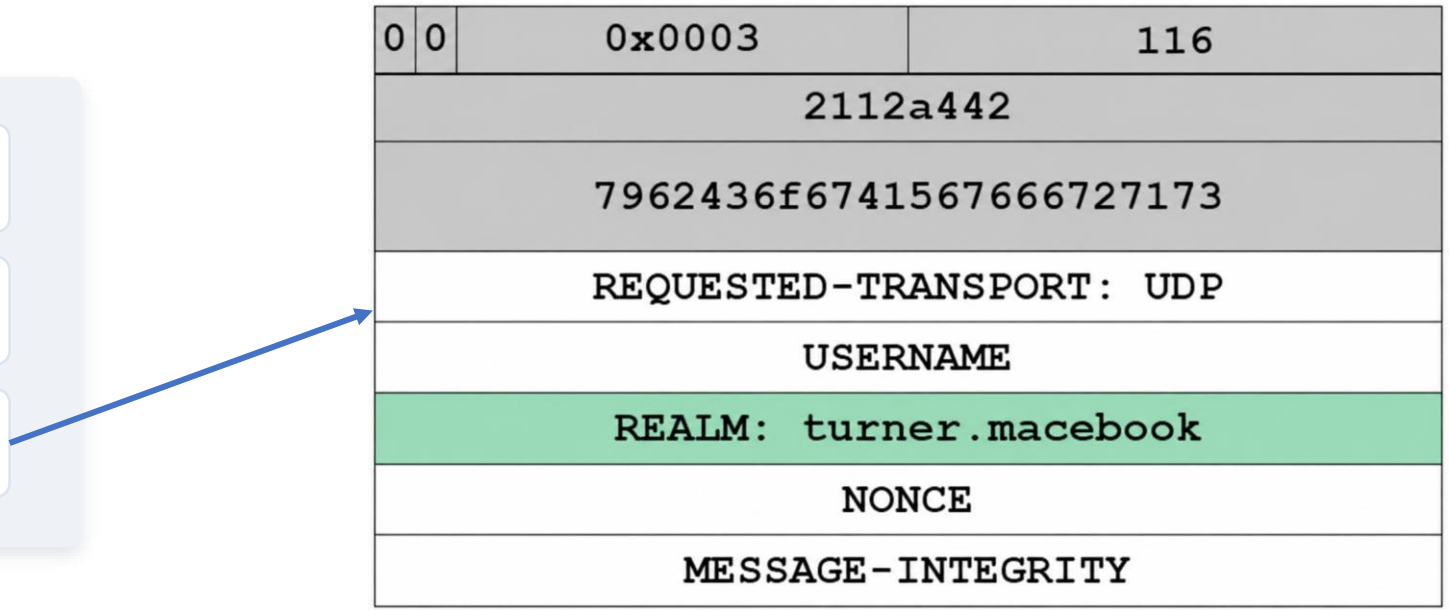
Zstun OUR TOOL

STUN-aware scanner

Scans a country's whole IPv4 space to find STUN endpoints, then sends three probes to each: P1 vanilla · P2 app-specific · P3 obfuscated

PROBE TYPES

P1	Vanilla STUN
P2	App-specific STUN
P3	Obfuscated STUN



Detecting One Case, Powered By Zstun

Zstun OUR TOOL

STUN-aware scanner

Scans a country's whole IPv4 space to find STUN endpoints, then sends three probes to each: P1 vanilla · P2 app-specific · P3 obfuscated

WORKED EXAMPLE

P1	Vanilla STUN	✓ STUN response (R1)
P2	App-specific STUN	✗ No response (R3)
P3	Obfuscated STUN	✓ STUN response (R1)

Only P2 is dropped, and P3 restores the reply, so Revelio marks this path filtered. The pattern of replies pins down the censorship behaviour to exactly one case (here it is Case V)

1 OF 9 CASES

I	IV	**V**
VI	II	VII
VIII	IX	III

Prefix Scraping 1 — Zstun Probing 2 — Forming Cases 3 — StunTrace 4 — Middleboxes 5

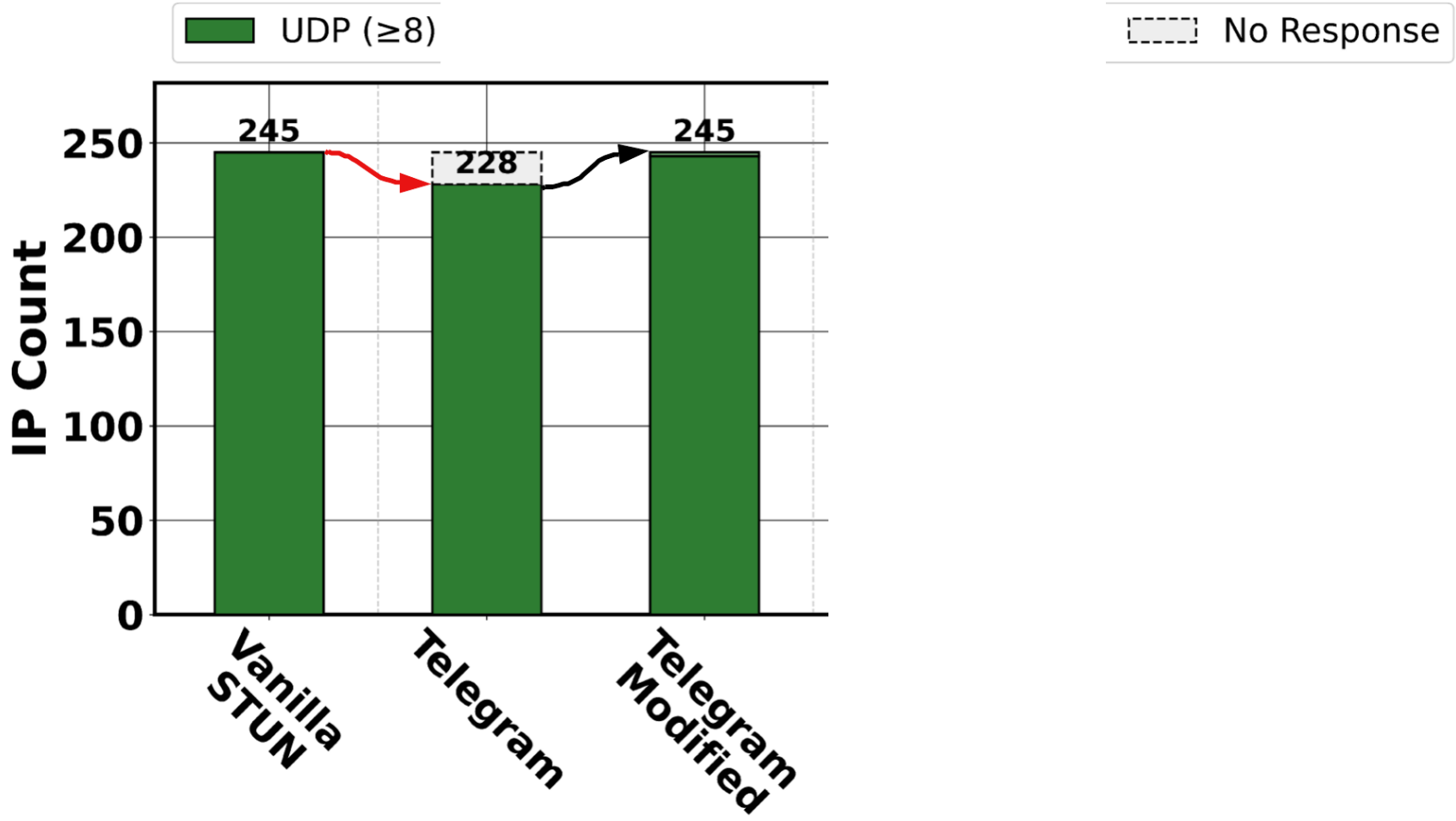
Results (Case-V)

P1 -> STUN and P2 -> No Response

Saudi Arabia

Results (Case-V)

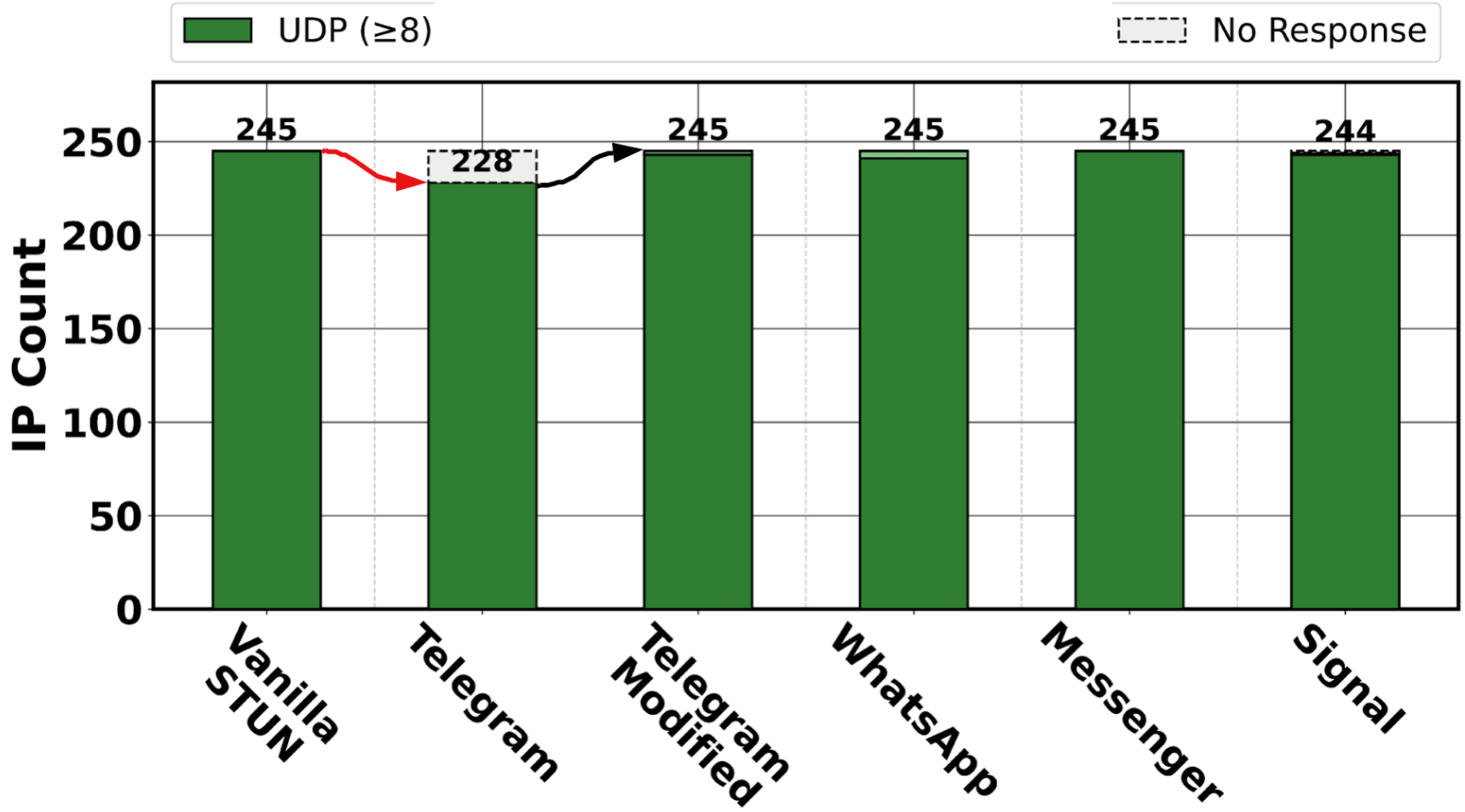
P1 -> STUN and P2 -> No Response



Saudi Arabia

Results (Case-V)

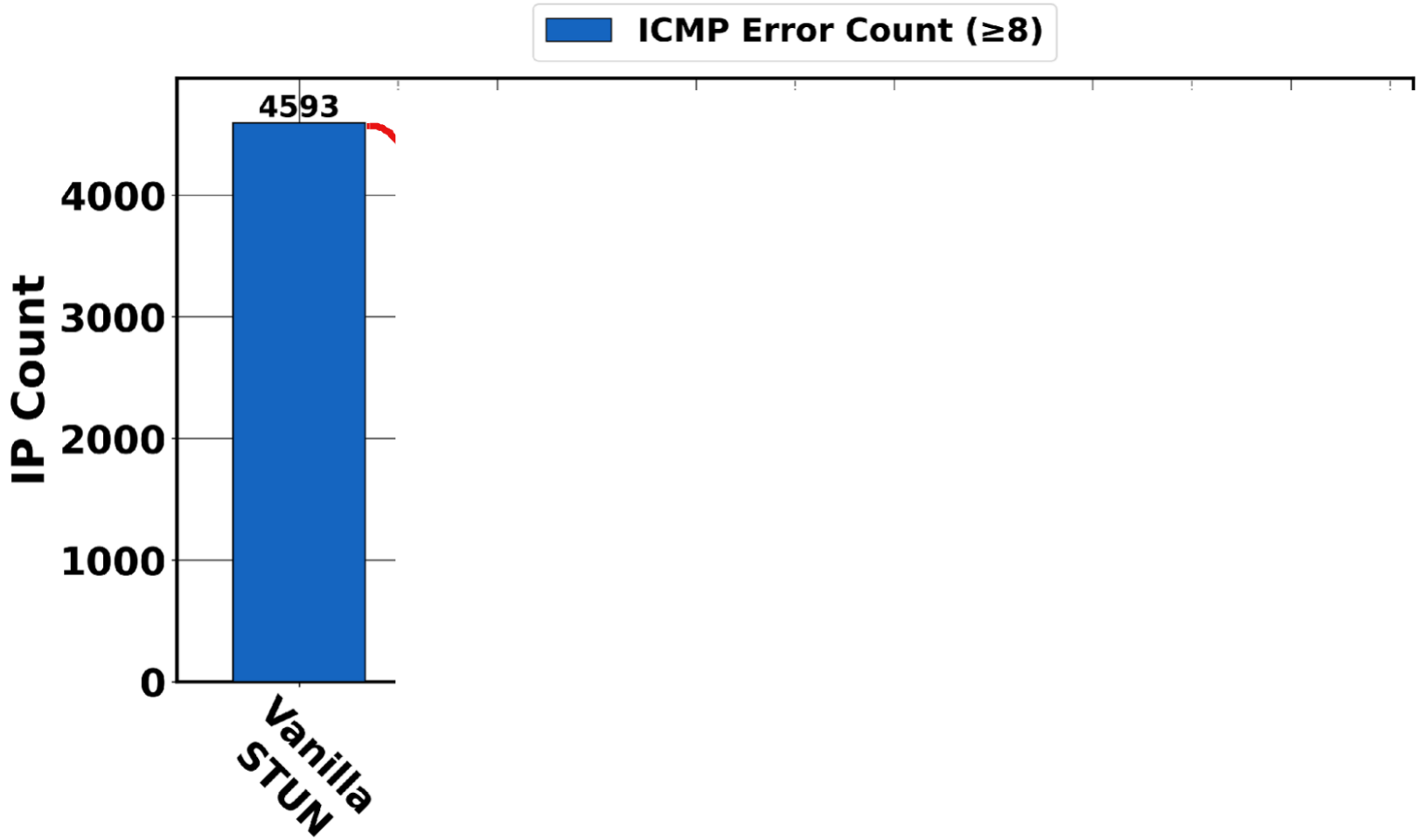
P1 -> STUN and P2 -> No Response



Saudi Arabia

Results (Case-VII)

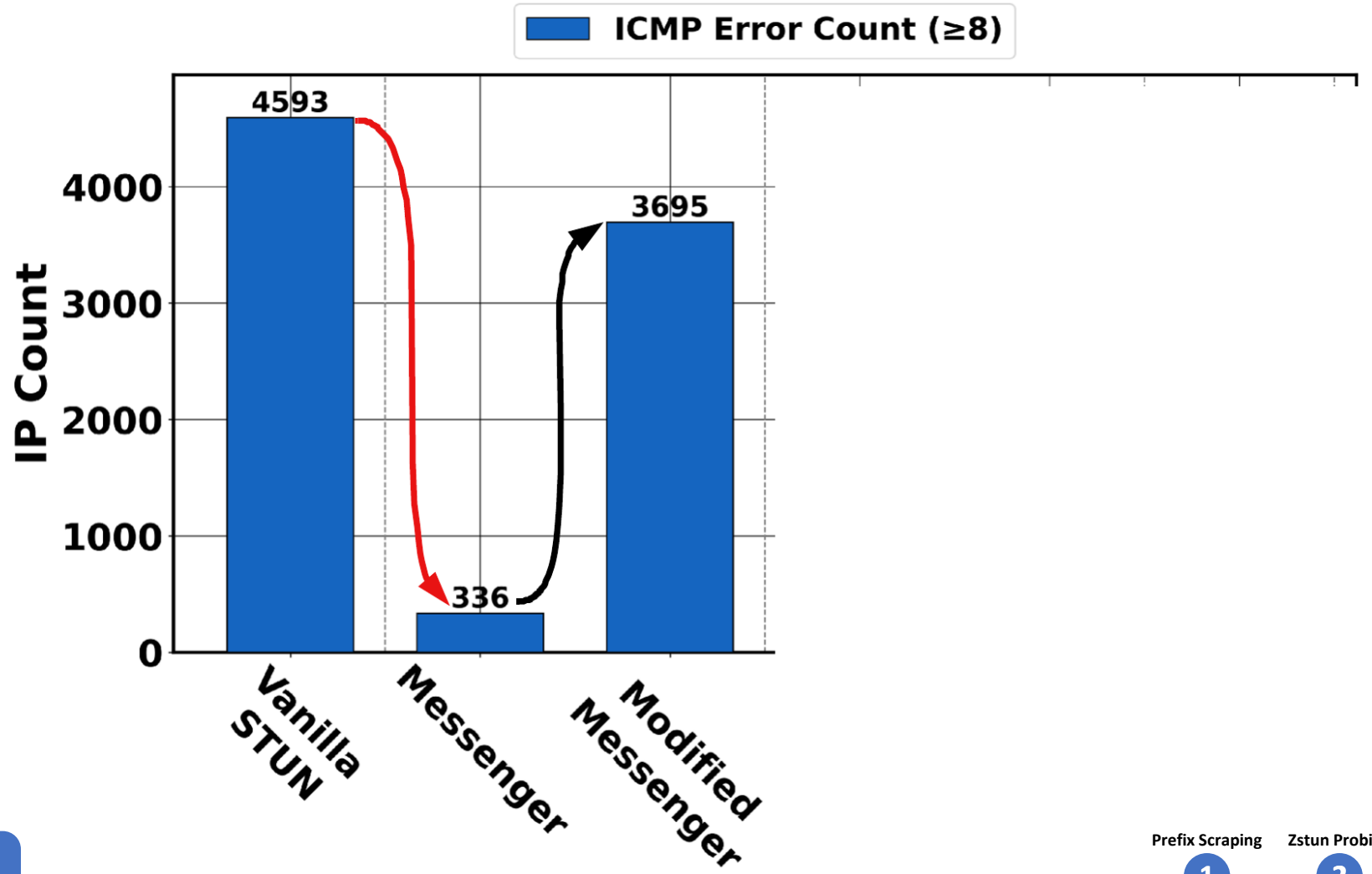
P1 -> ICMP and P2 -> No Response



Myanmar

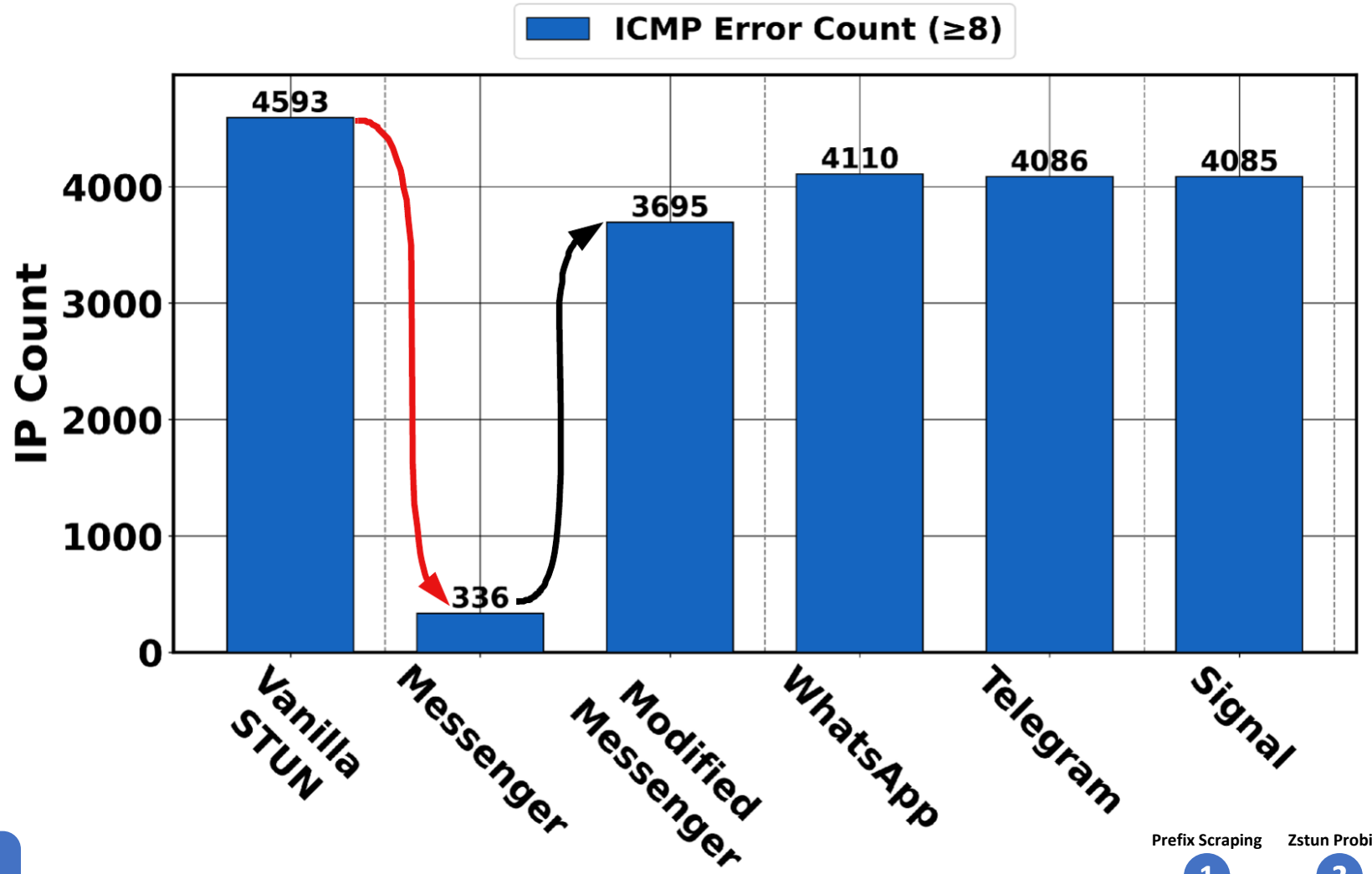
Results (Case-VII)

P1 -> ICMP and P2 -> No Response



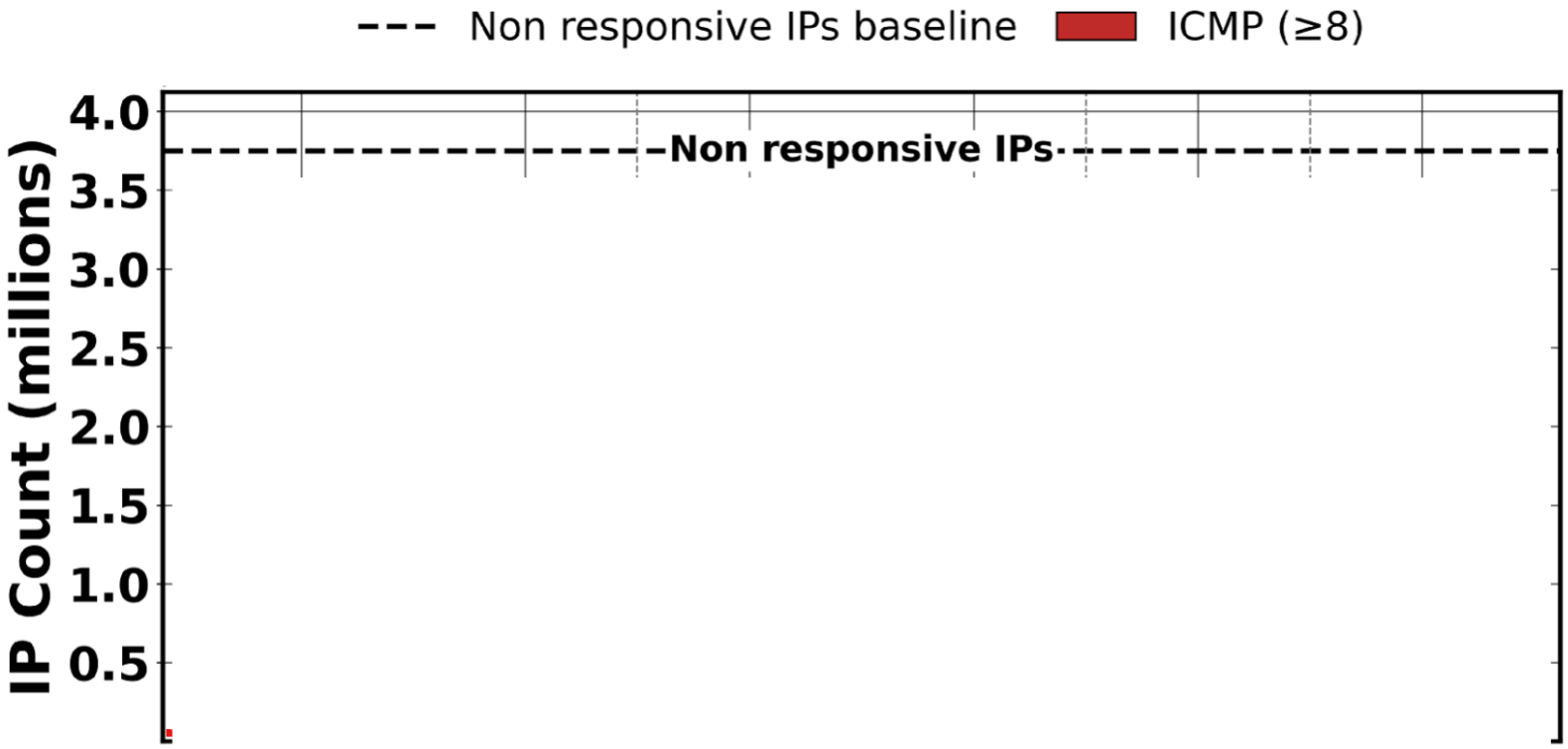
Results (Case-VII)

P1 -> ICMP and P2 -> No Response



Results (Case-IX)

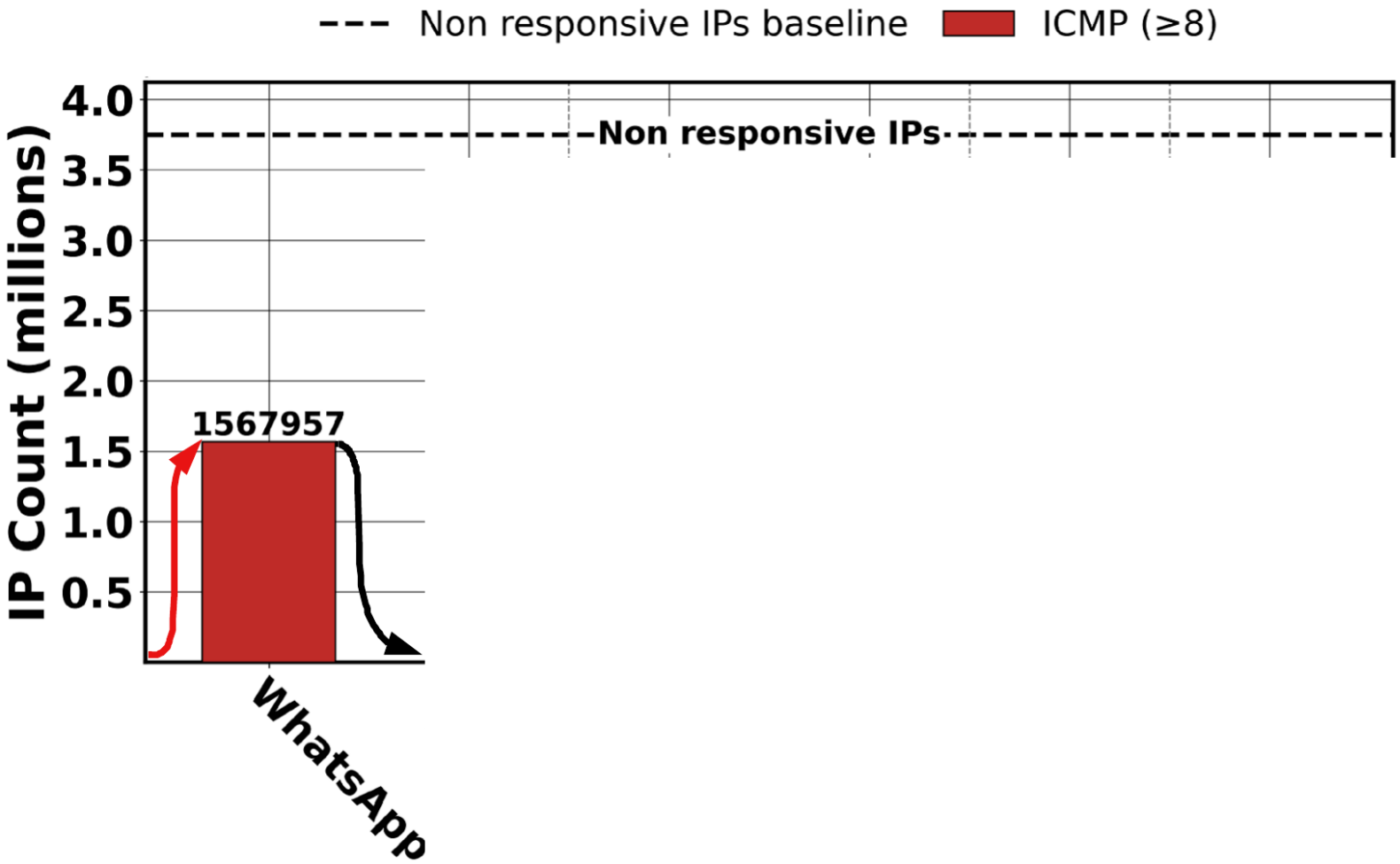
P1 -> No Response and P2 -> ICMP



United Arab Emirates

Results (Case-IX)

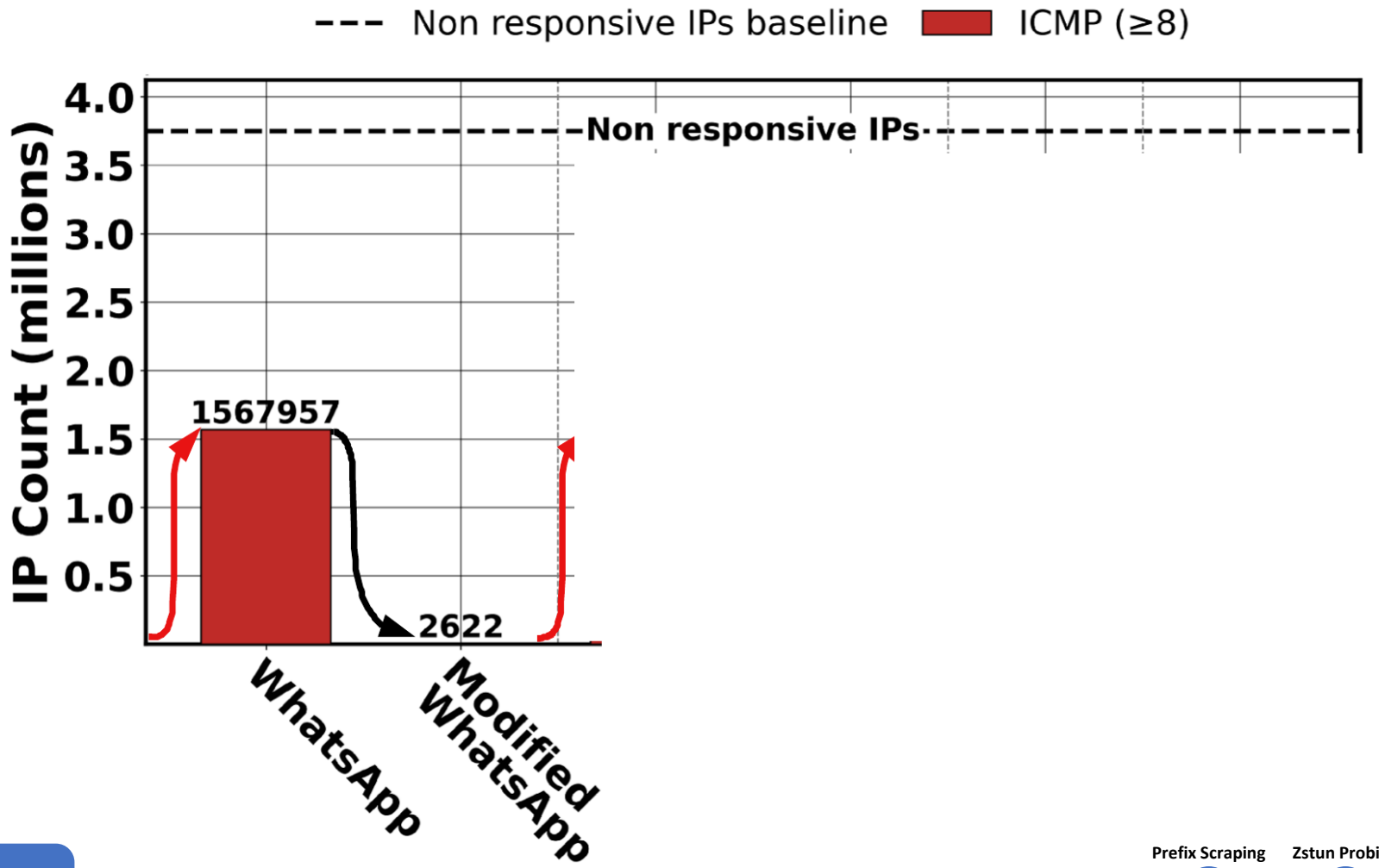
P1 -> No Response and P2 -> ICMP



United Arab Emirates

Results (Case-IX)

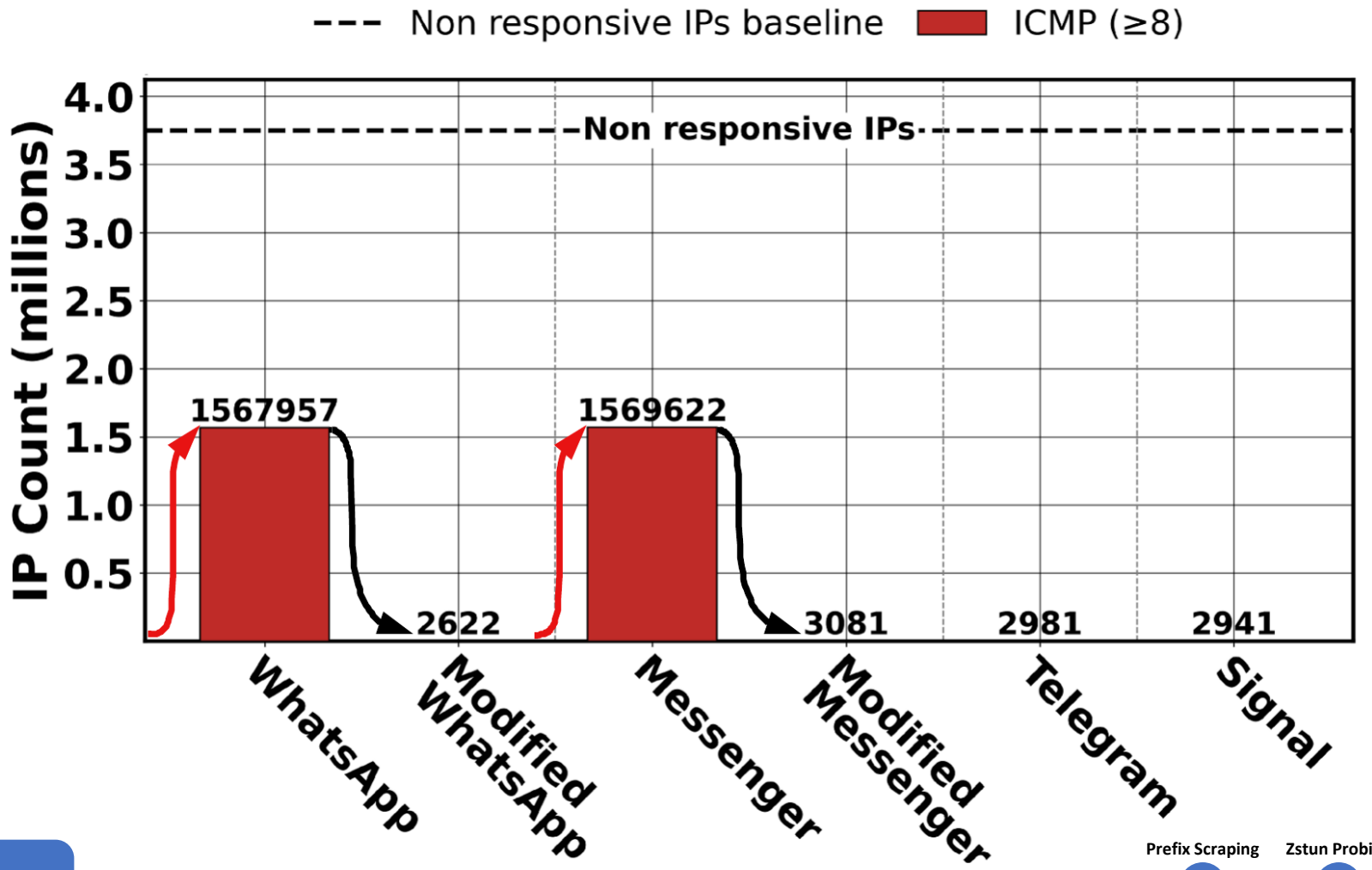
P1 -> No Response and P2 -> ICMP



United Arab Emirates

Results (Case-IX)

P1 -> No Response and P2 -> ICMP

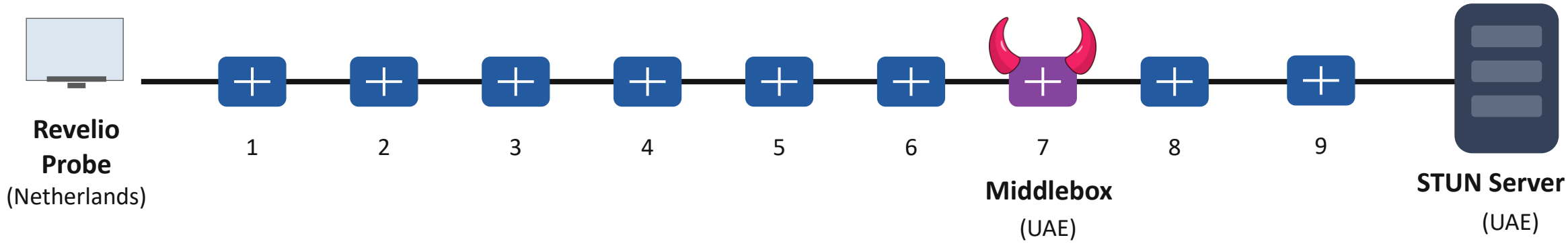


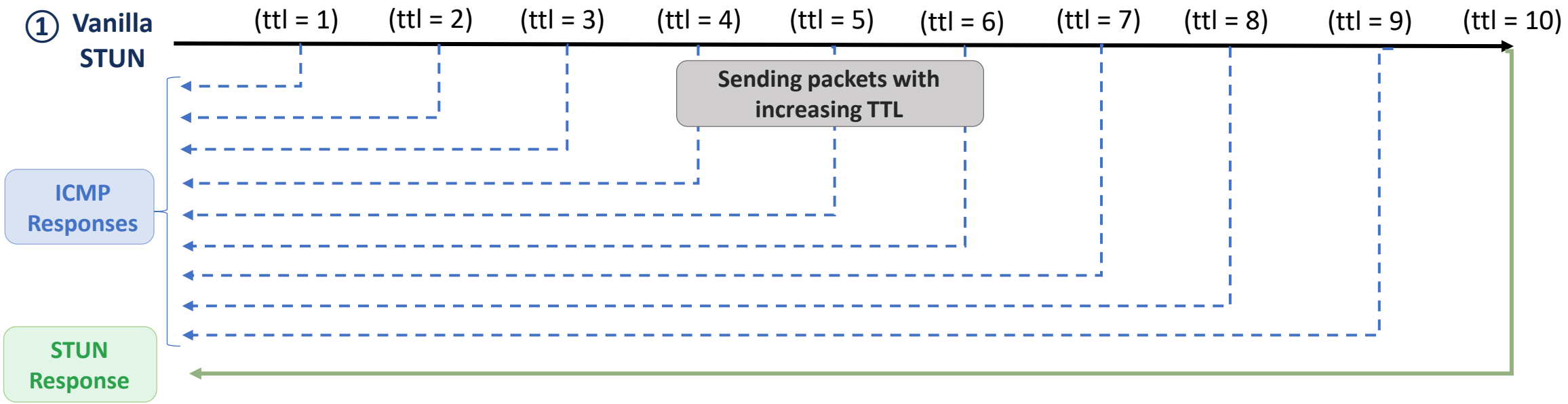
United Arab Emirates

Where Are These Censorship Causing Middlebox Placed?

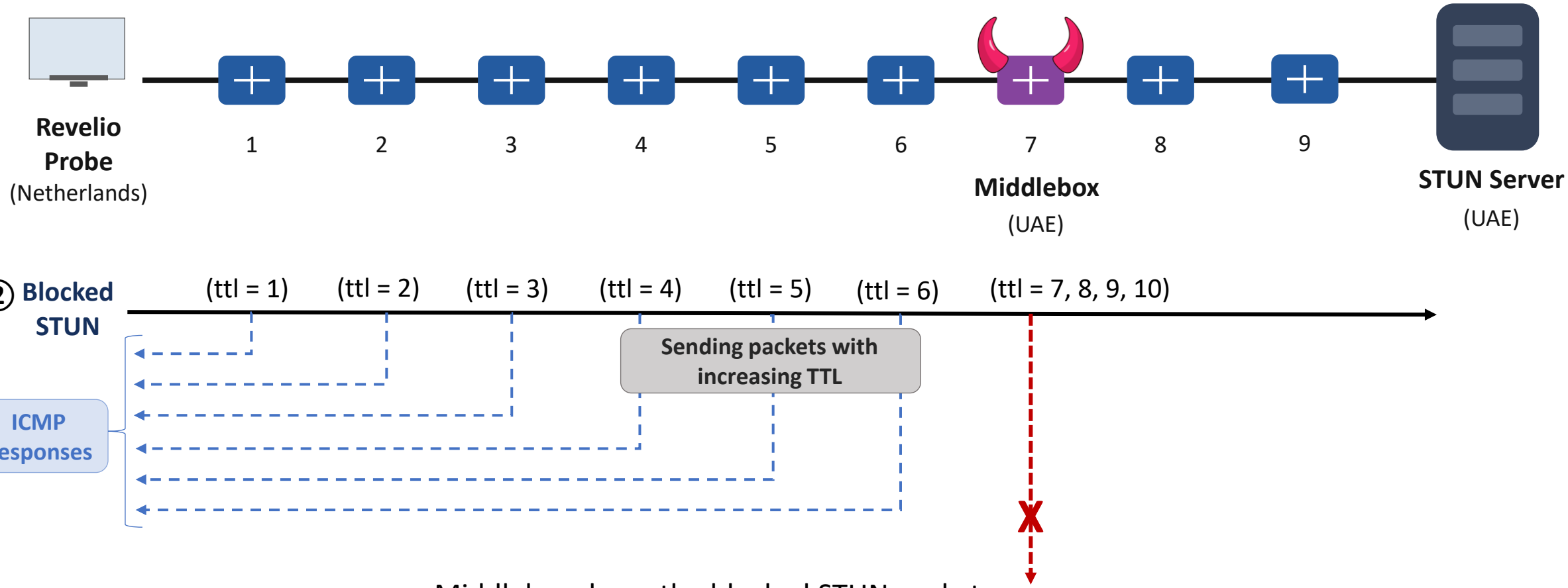
(Using STUN Trace to pinpoint middlebox hop)

STUN Trace (Vanilla STUN)





STUN Trace (Blocked STUN)

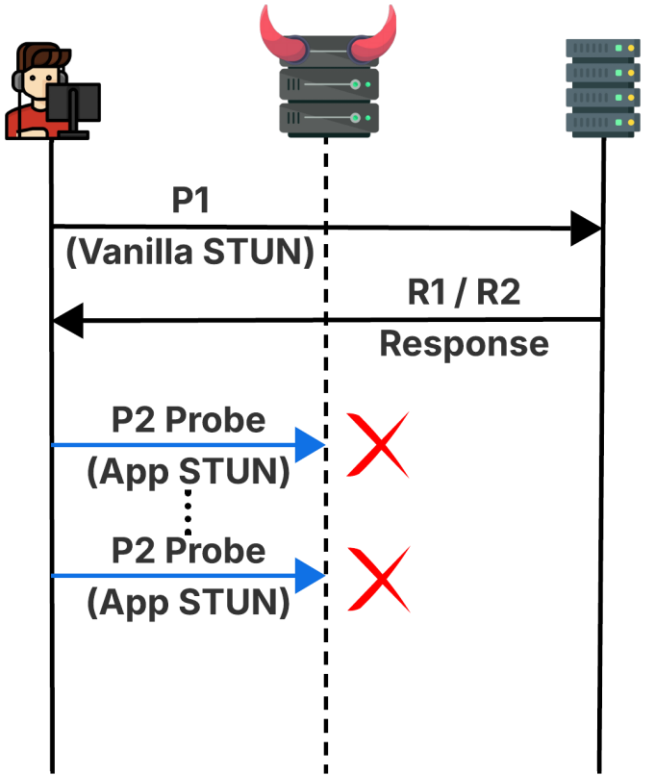


Middlebox drops the blocked STUN packets

Type Of Middleboxes

(Deduced using STUN Trace)

Type Of Middleboxes



(M1) Drop On First Encounter

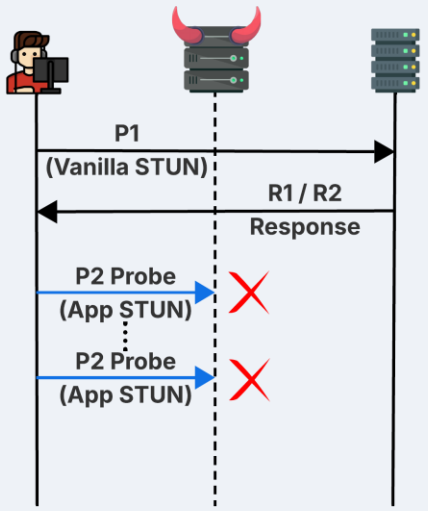
One out of Four types of middleboxes we found

- Vanilla STUN elicits some kind of response (UDP or ICMP) from the end destination
- Blocked App STUN cannot elicit same responses because the middlebox drops the packet on first encounter

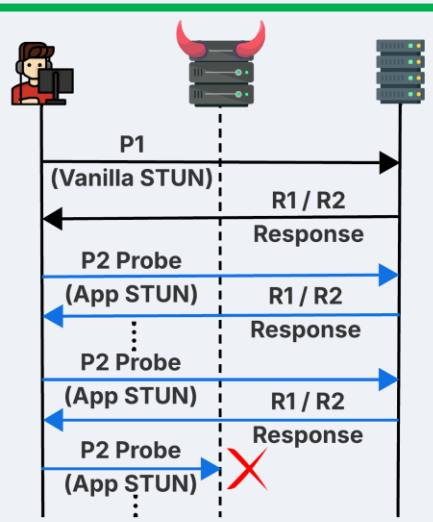
Type Of Middleboxes

The first catalog of STUN-blocking middleboxes

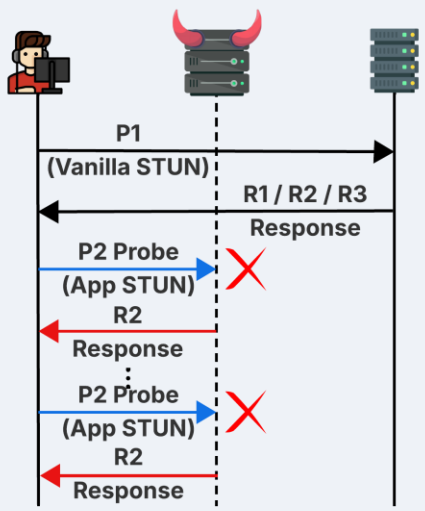
4 classes and 6 subtypes: drop on first contact, drop after a few packets, spoofed ICMP errors, and throttling (random, periodic, arithmetic).



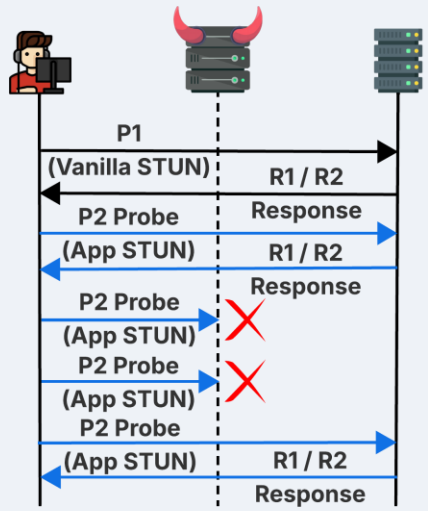
(M1) Drop On First Encounter



(M2) Drop After Multiple Encounters



(M3) Spoofed ICMP Error Messages



(M4) Throttled Responses

Result Summary

19

countries block VoIP calls

primarily via targeted interference with STUN traffic

71

Countries studied
known censors and uncensored-countries as control group

5

Apps actively blocked
WhatsApp · Telegram · Messenger · Signal · Instagram

4

Types of Middleboxes
Drop/throttle app-specific STUN packets; some reply with spoofed ICMP packets

VoIP Call Is Specifically Blocked?

Or

The VoIP App Is Blocked Entirely?

Checking For Web-Filtering

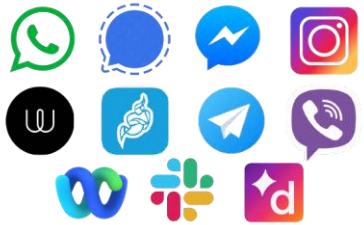
HYPERQUACK

Scalable Remote Measurement of Application-Layer Disruption

- Hyperquack measures keyword blocking at the application layer.
- It detects DPI interference with HTTP and HTTPS traffic by making use of publicly accessible web-servers with consistent behavior.

(**NDSS'20**) : R. Raman, A. Stoll, J. Dalek, R. Ramesh, W. Scott, R. Ensafi

Checking For Web-Filtering

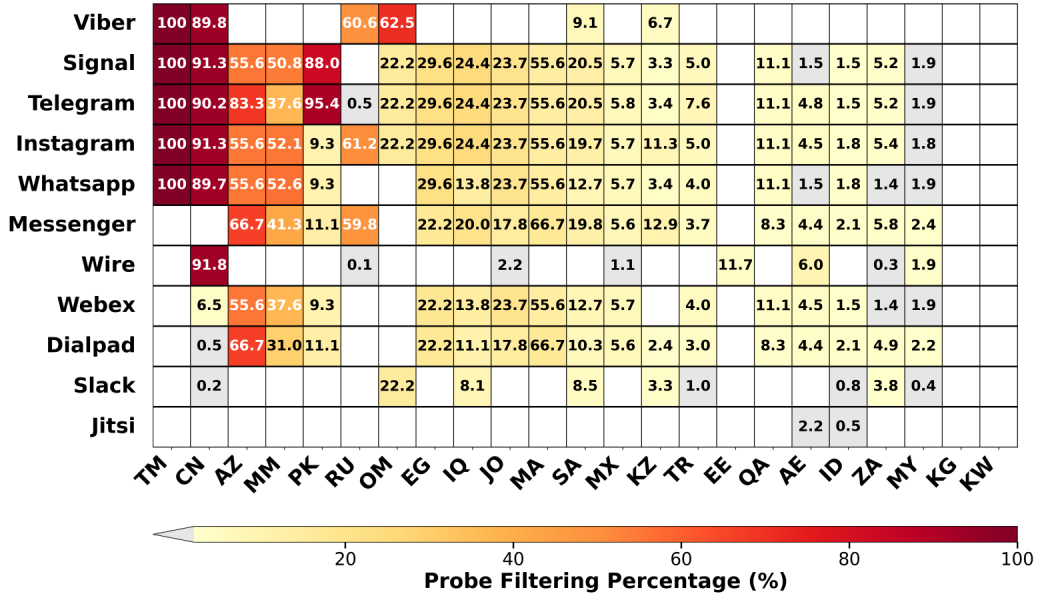


Collecting domain names and keywords associated with the VoIP App

for e.g., whatsapp.com, web.whatsapp.com

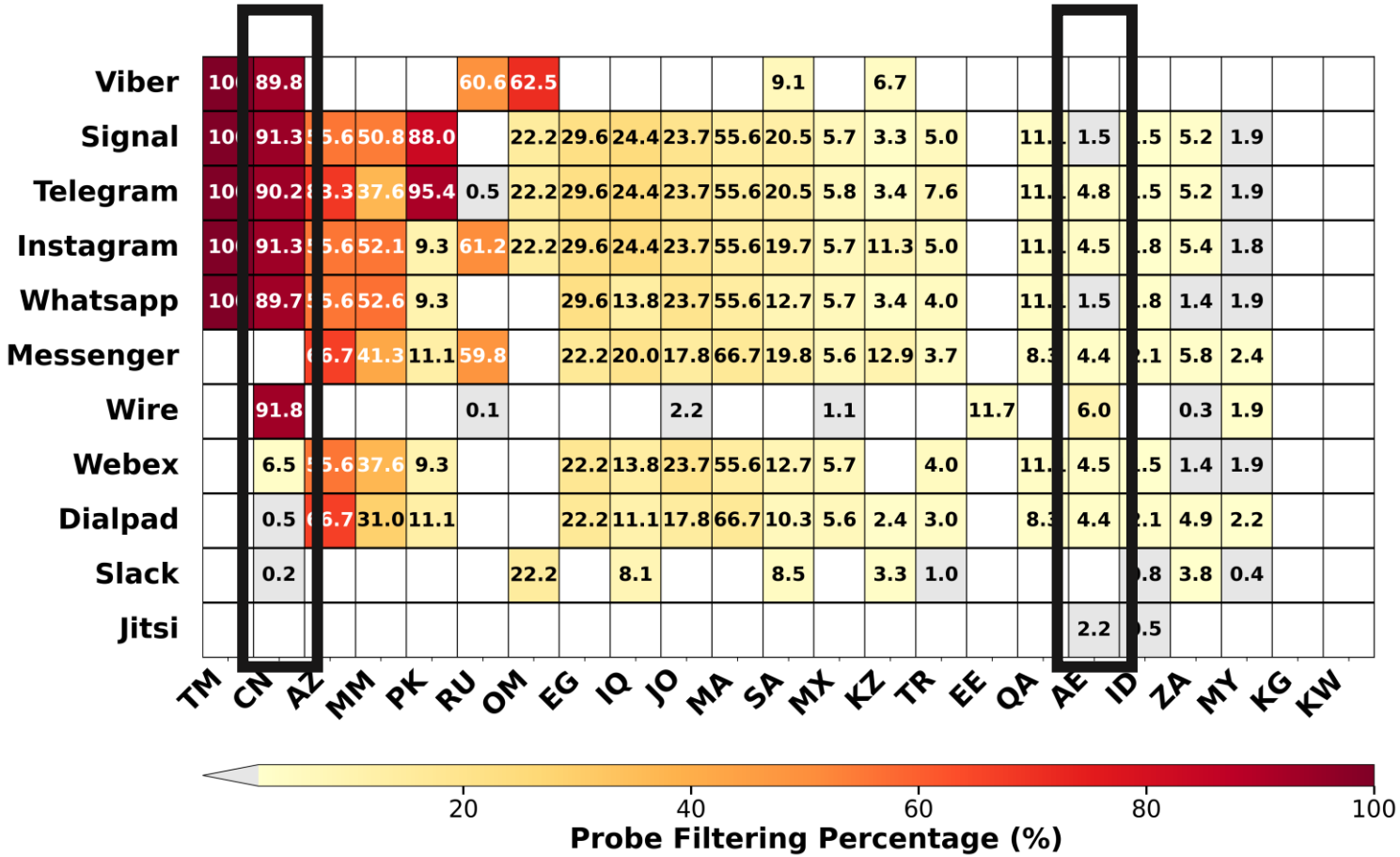


Hyperquack HTTP(S) Scans



Keyword Filtering Result

Hyperquack Results

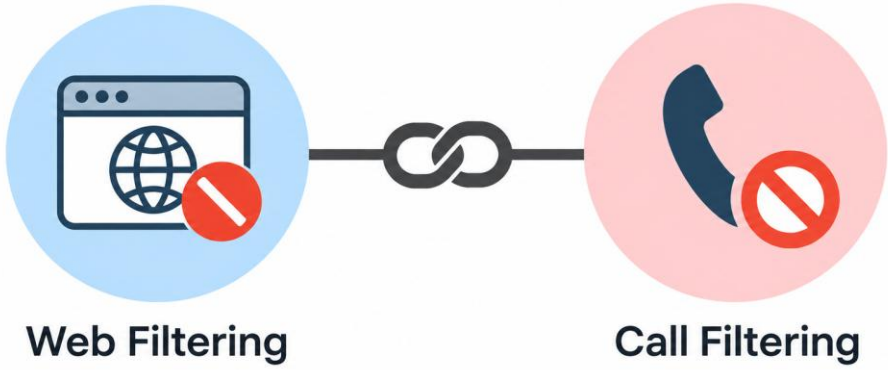


Relating Web and VoIP Blocking

Only STUN-Filtering
- E.g., Estonia and Kuwait

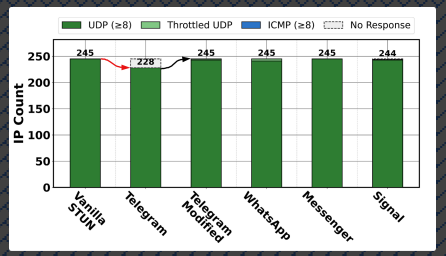
Both Web and STUN Filtering
- E.g., Pakistan and Myanmar

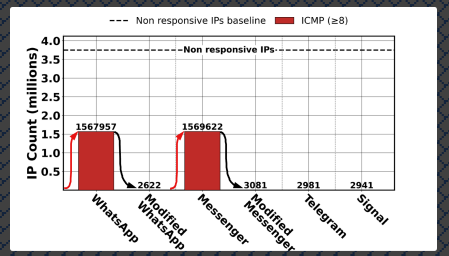
Only Web-Filtering
- E.g., China and Russia

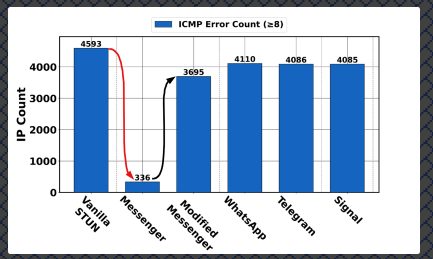


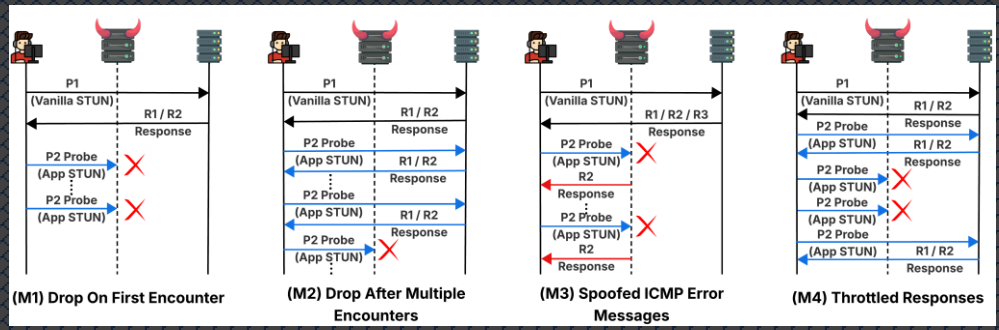
CONCLUSION

- Finding VoIP censorship while
  - Detecting remotely
  - At a global scale
  - For multiple VoIP apps
  - Identifying middleboxes









- Key takeaways
  - Blocking relies on a few simple app STUN fingerprints
  - Currently VoIP ecosystem does not provide protection against blocking
  - Need for designing resilient network protocols (including VoIP)

Revelio Artifact







Our code, analysis scripts and data are publicly available at this link →



https://doi.org/10.5281/zenodo.20362017

Revelio Research Team



Arjun Gupta
IIT Bombay
INDIA



Roya Ensafi
University of Michigan
UNITED STATES



Piyush Kumar
IIT Delhi
INDIA



Devashish Gosain
IIT Bombay
INDIA