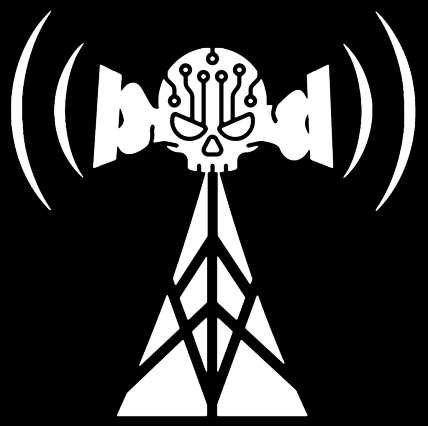
Uncovering Cellphone Risks:

Interception and Other Mobile Attacks



CELLULAR
ASSAULT
VILLAGE

Henry N. Caga (@hncaga)

whoami

Henry N. Caga

Infosec Engineer (2017)

CEH, ECSA, LPT (Master), eCPTXv2

Independent Security Researcher /
Bug Bounty Hunter

Acknowledged / Rewarded by:

Google (HoF Rank: 472)
Twitter
Cloudflare
etc..

eBay / PayPal
Yahoo!
UnionBankPH

15 years in a Law Enforcement Agency

INTERPOL IT Crime Investigation working party (2007)

First appearance (2004)

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
- ...other attacks

Disclaimer

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!

CELLULAR ASSAULT VILLAGE

What is IMSI?

CELLULAR ASSAULT VILLAGE

From Wikipedia, the free encyclopedia

The **international mobile subscriber identity** (**IMSI**) /ˈɪmziː/ is a number that uniquely identifies every user of a cellular network.[1] It is stored as a 64-bit field and is sent by the mobile device to the network. It is also used for acquiring other details of the mobile in the home location register (HLR) or as locally copied in the visitor location register. To prevent eavesdroppers from identifying and tracking the subscriber on the radio interface, the IMSI is sent as rarely as possible and a randomly-generated TMSI is sent instead.

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.

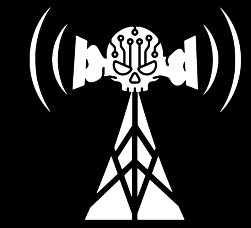
- They can mimic legitimate cell towers to trick nearby cell phones into connecting to them.

- 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)

CELLULAR ASSAULT VILLAGE

```
File  Edit  View  Search  Terminal  Help
 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:E0[redacted],Arfcn:47,Lac:2B[redacted],Bsic:10
Operator:"Globe Telecom",MCC:515,MNC:02,Rxlev:27,Cellid:5[redacted],Arfcn:27,Lac:4F[redacted],Bsic:21
Operator:"SMART Gold",MCC:515,MNC:03,Rxlev:22,Cellid:C[redacted],Arfcn:48,Lac:2B[redacted],Bsic:3F
Operator:"Globe Telecom",MCC:515,MNC:02,Rxlev:24,Cellid:C[redacted],Arfcn:844,Lac:4F[redacted],Bsic:15
Operator:"Globe Telecom",MCC:515,MNC:02,Rxlev:30,Cellid:56[redacted],Arfcn:27,Lac:4[redacted],Bsic:21
Operator:"Globe Telecom",MCC:515,MNC:02,Rxlev:23,Cellid:B7[redacted],Arfcn:839,Lac:4F[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
```

"AT+CNETSCAN" OUTPUT

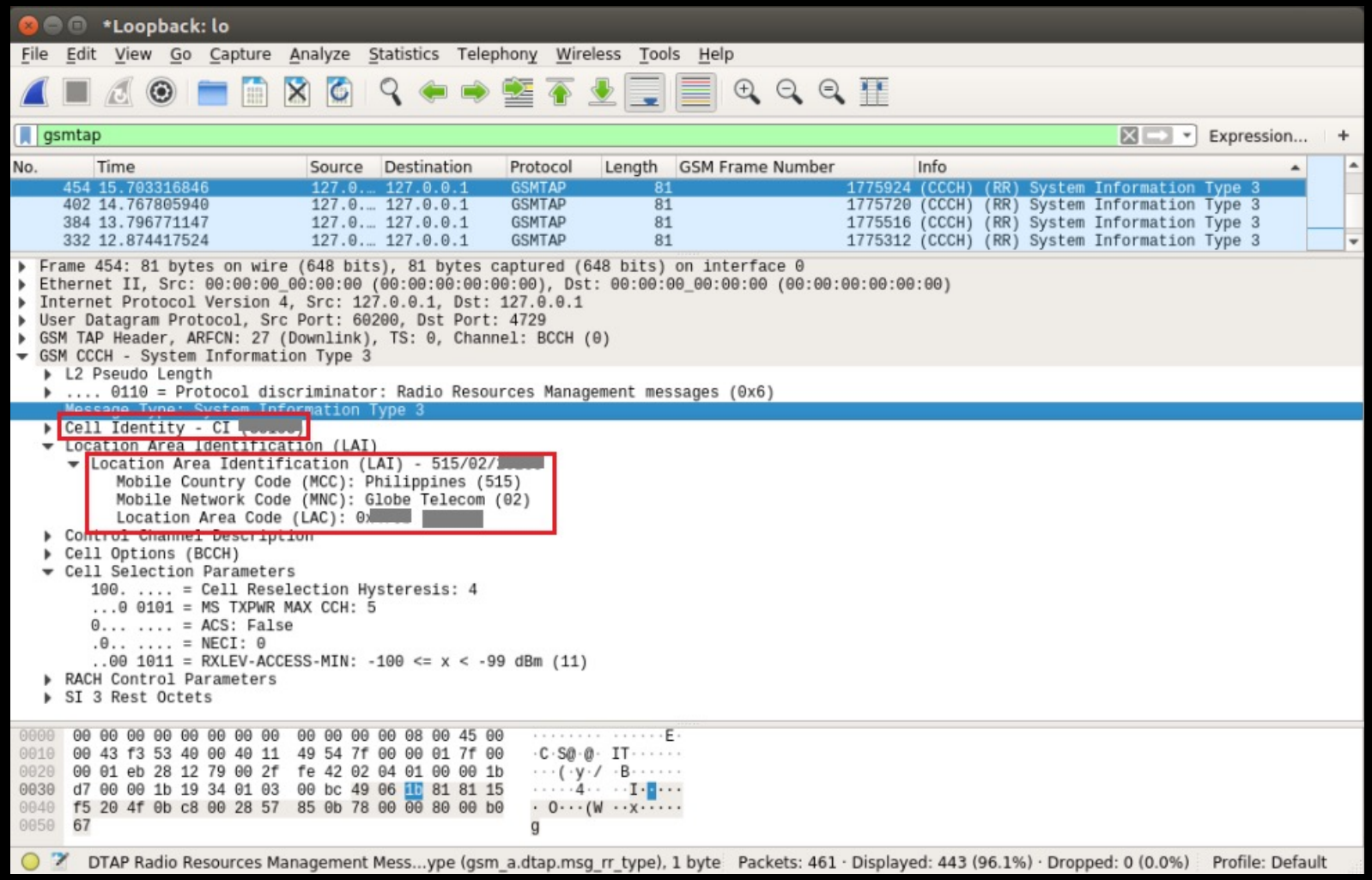
Simulate the process of a cell phone searching for an accessible cell tower and identifying the strongest signal.

Wireshark

CELLULAR ASSAULT VILLAGE

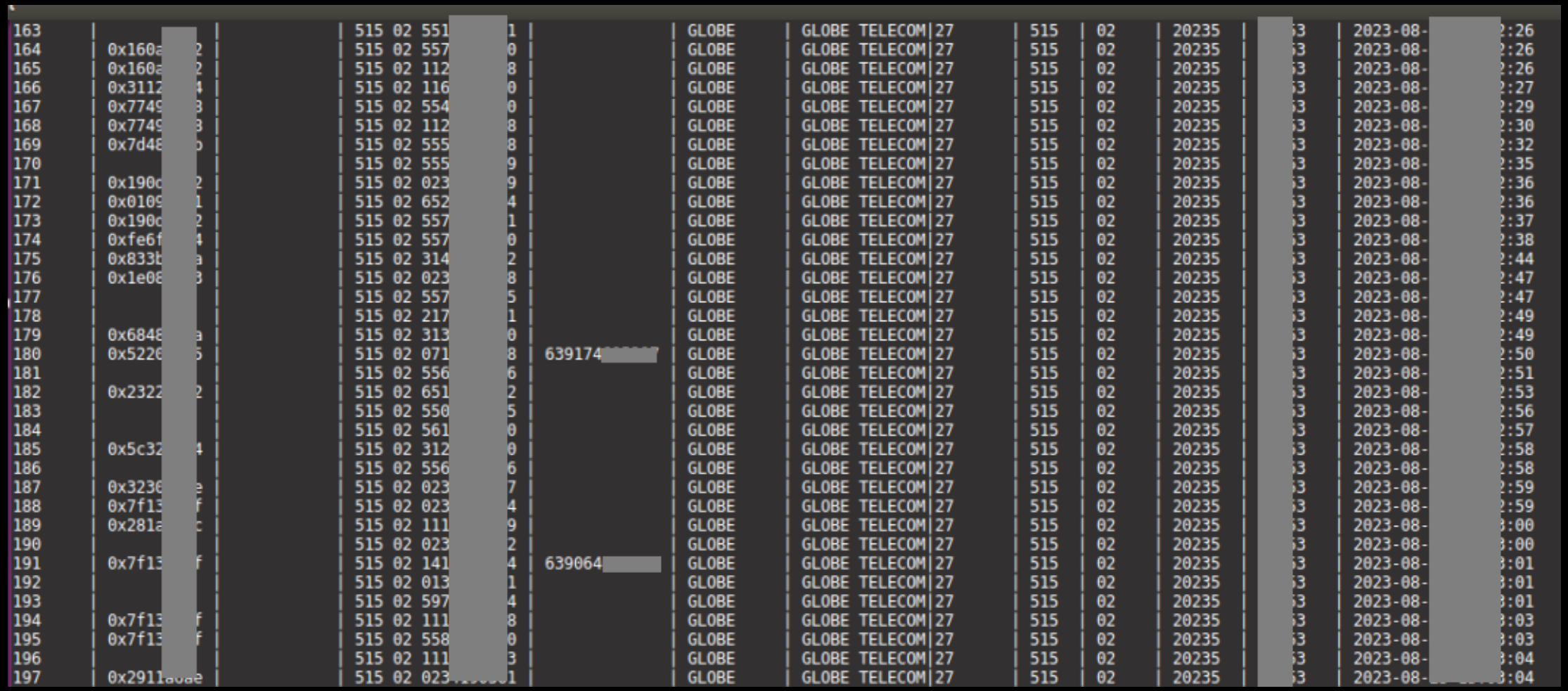
Un-encrypted packets can be viewed in Wireshark

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



Tower Sniffing

Automating tasks using Python in conjunction with Tshark.



163			515 02 551	1		GLOBE	GLOBE TELECOM|27	515	02	20235		2023-08- :26
164	0x160a 2		515 02 557	0		GLOBE	GLOBE TELECOM|27	515	02	20235		2023-08- :26
165	0x160a 2		515 02 112	8		GLOBE	GLOBE TELECOM|27	515	02	20235		2023-08- :26
166	0x3112 4		515 02 116	0		GLOBE	GLOBE TELECOM|27	515	02	20235		2023-08- :27
167	0x7749 3		515 02 554	0		GLOBE	GLOBE TELECOM|27	515	02	20235		2023-08- :29
168	0x7749 3		515 02 112	8		GLOBE	GLOBE TELECOM|27	515	02	20235		2023-08- :30
169	0x7d48 5		515 02 555	8		GLOBE	GLOBE TELECOM|27	515	02	20235		2023-08- :32
170			515 02 555	9		GLOBE	GLOBE TELECOM|27	515	02	20235		2023-08- :35
171	0x190c 2		515 02 023	9		GLOBE	GLOBE TELECOM|27	515	02	20235		2023-08- :36
172	0x0109 1		515 02 652	4		GLOBE	GLOBE TELECOM|27	515	02	20235		2023-08- :36
173	0x190c 2		515 02 557	1		GLOBE	GLOBE TELECOM|27	515	02	20235		2023-08- :37
174	0xfe6f 4		515 02 557	0		GLOBE	GLOBE TELECOM|27	515	02	20235		2023-08- :38
175	0x833b a		515 02 314	2		GLOBE	GLOBE TELECOM|27	515	02	20235		2023-08- :44
176	0x1e08 3		515 02 023	8		GLOBE	GLOBE TELECOM|27	515	02	20235		2023-08- :47
177			515 02 557	5		GLOBE	GLOBE TELECOM|27	515	02	20235		2023-08- :47
178			515 02 217	1		GLOBE	GLOBE TELECOM|27	515	02	20235		2023-08- :49
179	0x6848 a		515 02 313	0		GLOBE	GLOBE TELECOM|27	515	02	20235		2023-08- :49
180	0x5226 5		515 02 071	8	639174	GLOBE	GLOBE TELECOM|27	515	02	20235		2023-08- :50
181			515 02 556	6		GLOBE	GLOBE TELECOM|27	515	02	20235		2023-08- :51
182	0x2322 2		515 02 651	2		GLOBE	GLOBE TELECOM|27	515	02	20235		2023-08- :53
183			515 02 550	5		GLOBE	GLOBE TELECOM|27	515	02	20235		2023-08- :56
184			515 02 561	0		GLOBE	GLOBE TELECOM|27	515	02	20235		2023-08- :57
185	0x5c32 4		515 02 312	0		GLOBE	GLOBE TELECOM|27	515	02	20235		2023-08- :58
186			515 02 556	6		GLOBE	GLOBE TELECOM|27	515	02	20235		2023-08- :58
187	0x3230 e		515 02 023	7		GLOBE	GLOBE TELECOM|27	515	02	20235		2023-08- :59
188	0x7f13 f		515 02 023	4		GLOBE	GLOBE TELECOM|27	515	02	20235		2023-08- :59
189	0x281a c		515 02 111	9		GLOBE	GLOBE TELECOM|27	515	02	20235		2023-08- :00
190			515 02 023	2		GLOBE	GLOBE TELECOM|27	515	02	20235		2023-08- :00
191	0x7f13 f		515 02 141	4	639064	GLOBE	GLOBE TELECOM|27	515	02	20235		2023-08- :01
192			515 02 013	1		GLOBE	GLOBE TELECOM|27	515	02	20235		2023-08- :01
193			515 02 597	4		GLOBE	GLOBE TELECOM|27	515	02	20235		2023-08- :01
194	0x7f13 f		515 02 111	8		GLOBE	GLOBE TELECOM|27	515	02	20235		2023-08- :03
195	0x7f13 f		515 02 558	0		GLOBE	GLOBE TELECOM|27	515	02	20235		2023-08- :03
196			515 02 111	3		GLOBE	GLOBE TELECOM|27	515	02	20235		2023-08- :04
197	0x2911a0a2		515 02 023	1		GLOBE	GLOBE TELECOM|27	515	02	20235		2023-08- :04

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 and Tshark

```
GNU nano 2.5.3                                File: monitor.py

        execute_cmd("touch " + tmpCMFile)
    if os.path.isfile(tmpIAFile):
        execute_cmd("rm " + tmpIAFile)
        execute_cmd("touch " + tmpIAFile)

    # SI 5
    cmd = 'stdbuf -oL tshark -i lo -Y "gsm_a.dtap.msg_rr_type == 0x1d" -V 2>/dev/null | stdbuf -oL grep -E "GSM Frame Number: | Sub-Slot: | = ARFCN: | Epoch Time: " > ' + tmpSI5File + ' &'
    execute_cmd(cmd)

    # PAGING RESPONSE
    cmd = 'stdbuf -oL tshark -i lo -Y "gsm_a.dtap.msg_rr_type == 0x27" -V 2>/dev/null | stdbuf -oL grep -E "GSM Frame Number: | TMSI/P-TMSI: | Sub-Slot: | = ARFCN: | Epoch Time: " > ' + tmpPagingFile + ' &'
    execute_cmd(cmd)

    # CM SERVICE REQUEST
    cmd = 'stdbuf -oL tshark -i lo -Y "gsm_a.dtap.msg_mm_type == 0x24" -V 2>/dev/null | stdbuf -oL grep -E "GSM Frame Number: | TMSI/P-TMSI: | Sub-Slot: | = ARFCN: | Epoch Time: " > ' + tmpCMFile + ' &'
    execute_cmd(cmd)

    # IMMEDIATE ASSIGNMENT
    cmd = 'stdbuf -oL tshark -i lo -Y "gsm_a.dtap.msg_rr_type == 0x3f" -V 2>/dev/null | stdbuf -oL grep -E "GSM Frame Number: | Sub-Slot: | = ARFCN: | Epoch Time: " > ' + tmpIAFile + ' &'
    execute_cmd(cmd)
```

Encrypted but crackable packets and bursts are captured

Terminal

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
```

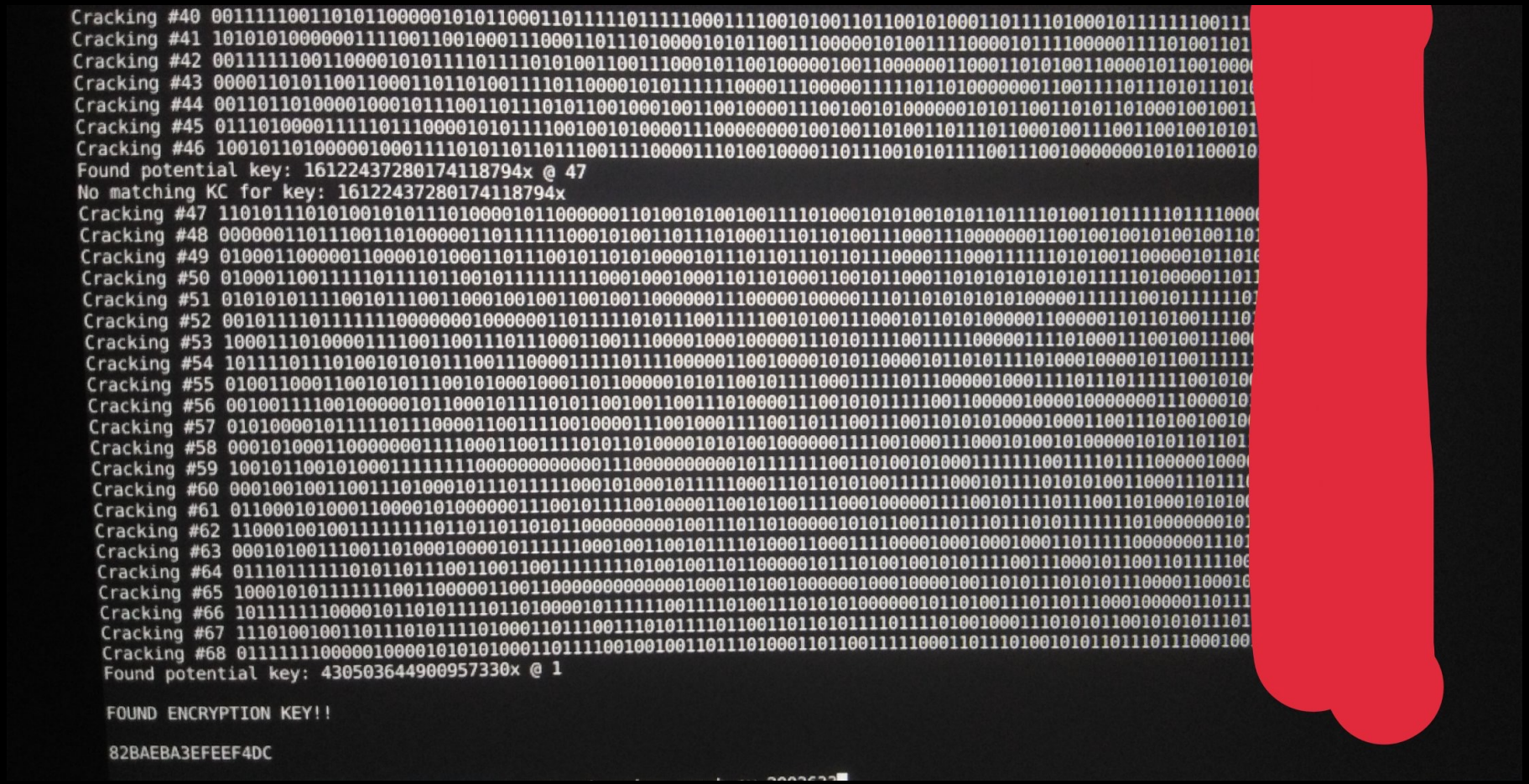
DEMO

Cracking key, reading SMS and listening calls from cell towers

NO!

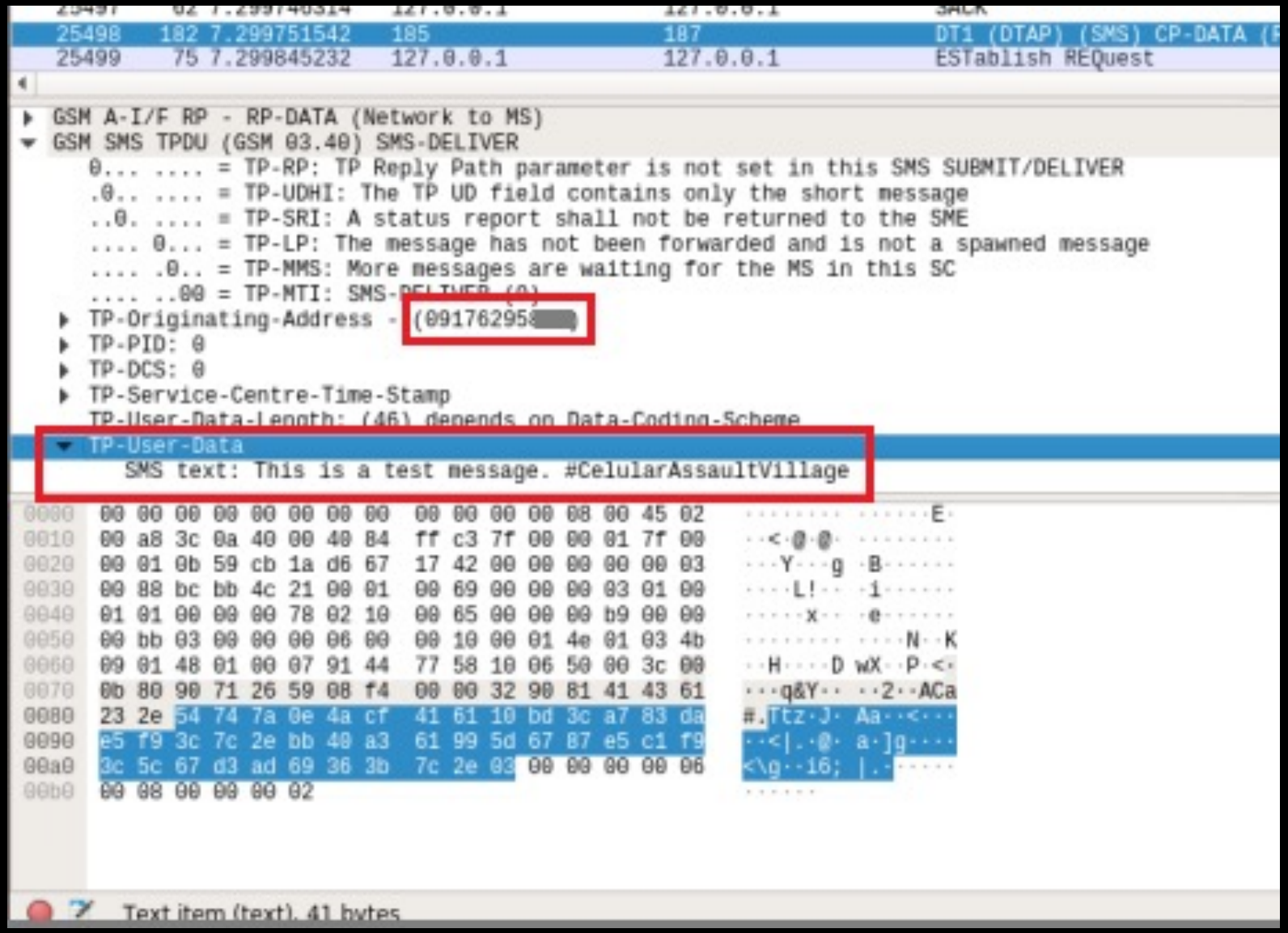
Retrieving Encryption Key

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



Reading SMS

SMS in plaintext after using the Kc.



Fake Cell Towers (Active Interceptors)

CELLULAR ASSAULT VILLAGE

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

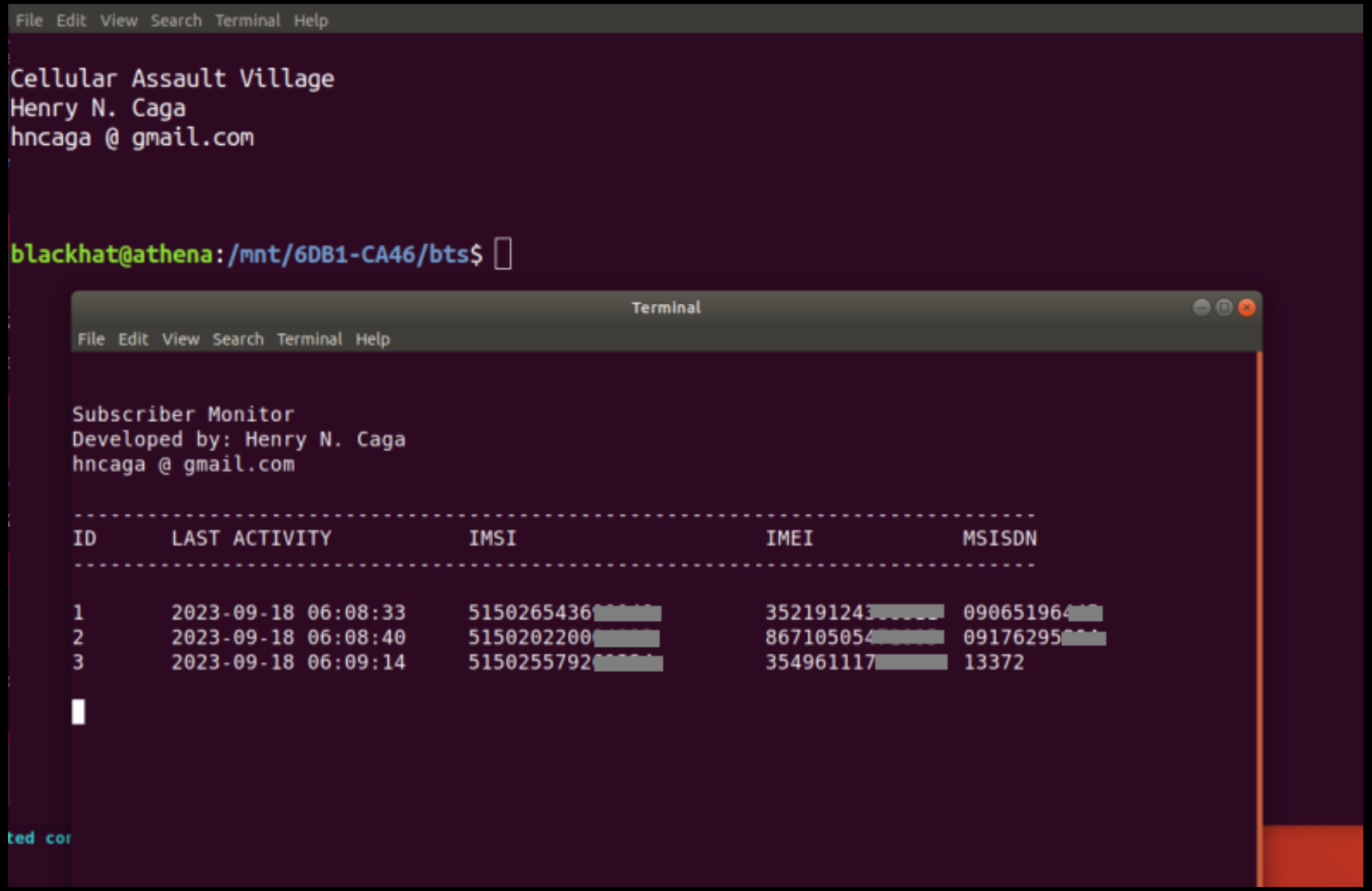
Running a fake cell tower and waiting for mobile devices

Fake Cell Tower

CELLULAR ASSAULT VILLAGE

Data Captured:

- IMSI
- IMEI
- MSISDN



Why are mobile phones attracted to Fake Towers?

CELLULAR ASSAULT VILLAGE

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

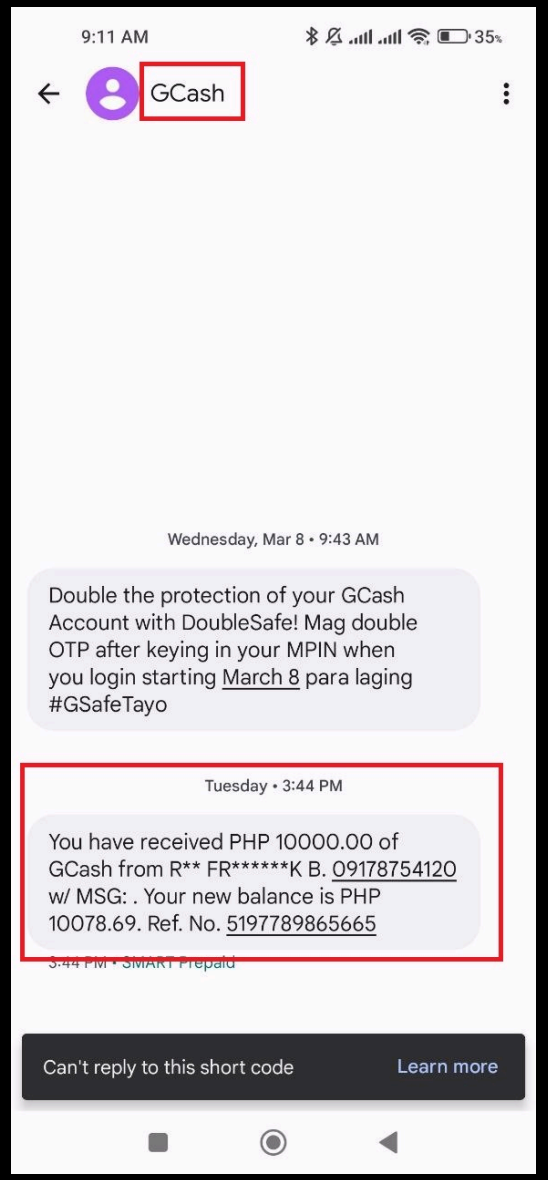
Mobile Number / Name Spoofing

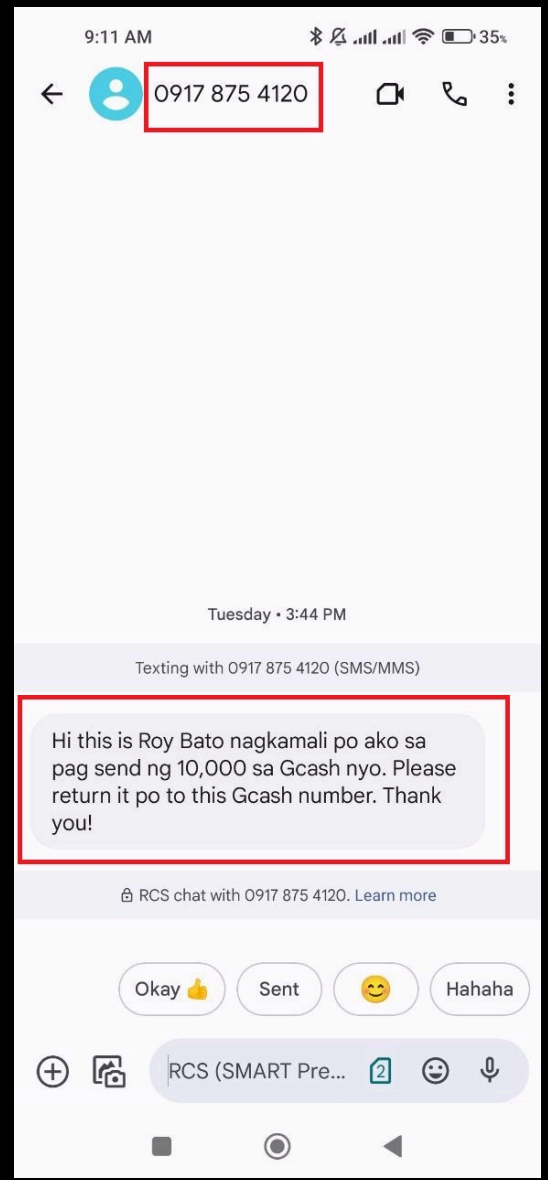
Scammers Using Spoofing

CELLULAR ASSAULT VILLAGE

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.

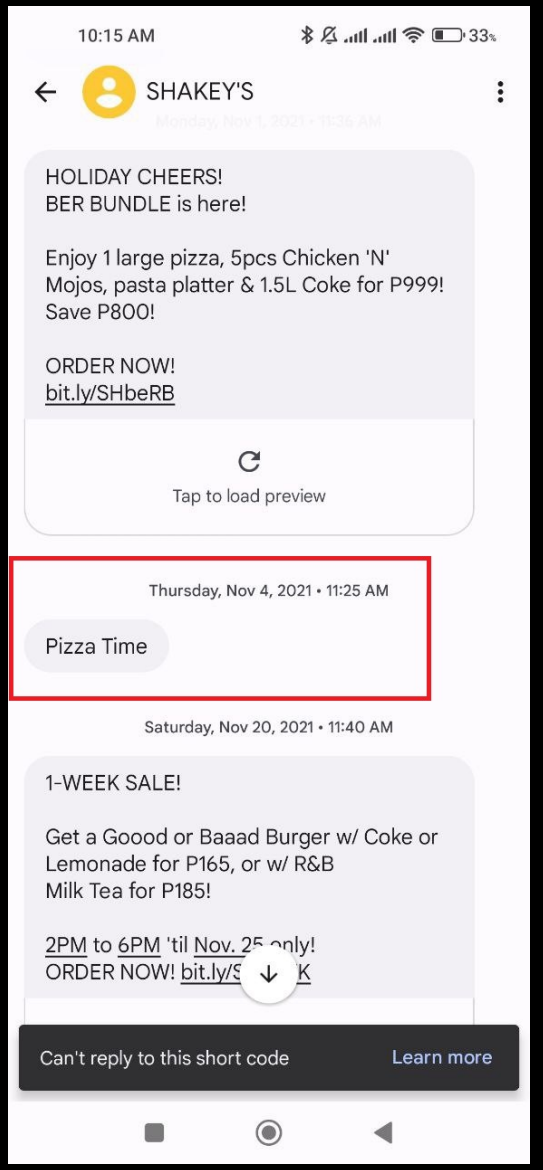




Real Messages / Fake Messages

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.



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

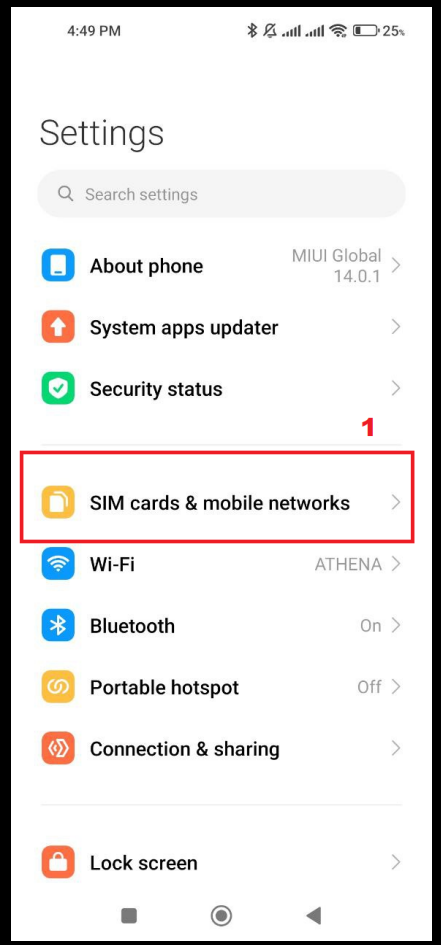
SMS Interception / Calls Hi-Jacking

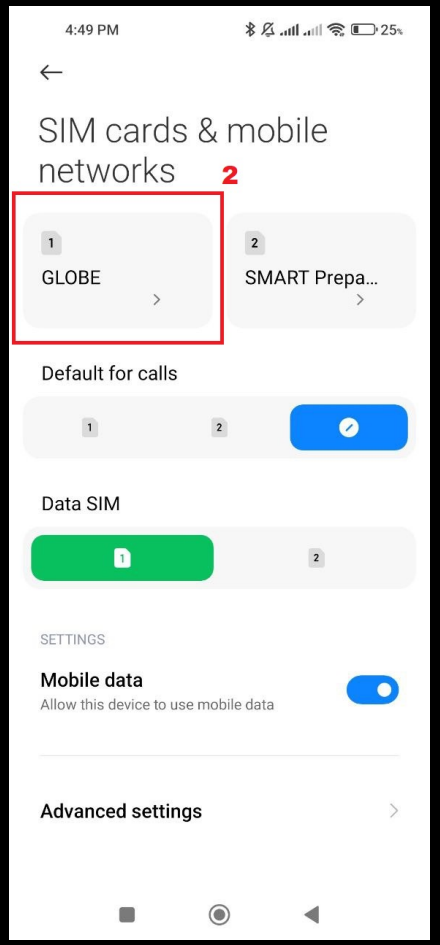
(Volunteers are Welcome)

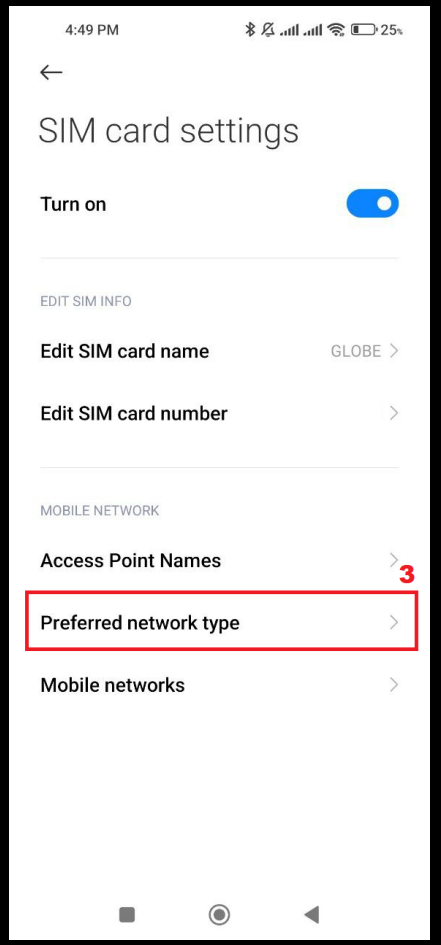
Volunteers?

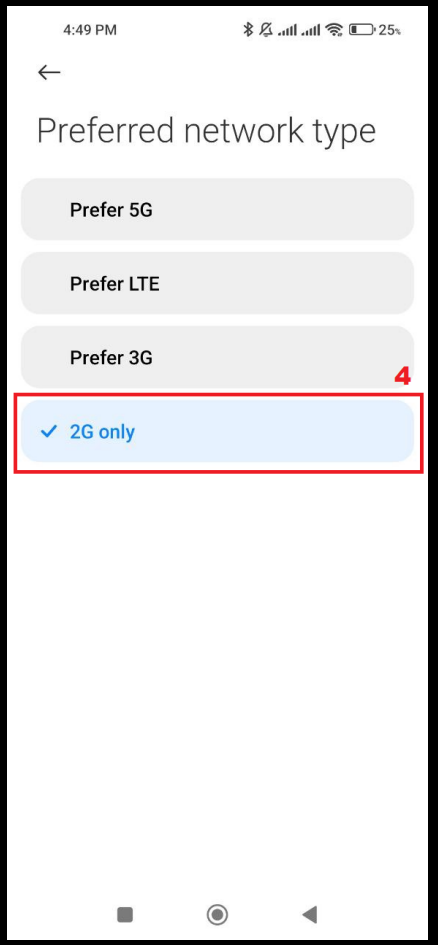
CELLULAR ASSAULT VILLAGE

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









Other Mobile Attacks

Man in the Middle (MITM)

- Allow the victims to access to the internet
- Allow sending of links
- Sniff traffic
- Scan for open ports
- Scan for vulnerabilities to access files or data

Other Mobile Attacks

Distribution of Malware

- Sending of binary files (Applets)
- Running the applets every time the phone restarts
- Monitoring of target even if connected to legitimate network

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

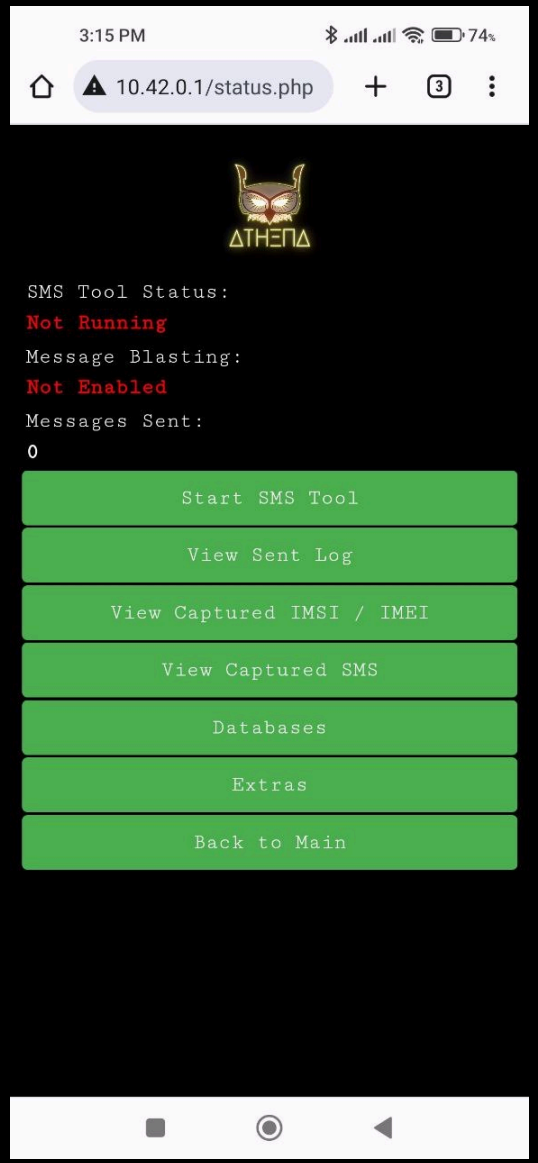
- IMSI Catcher for Higher Generations (Another equipment for 3G, 4G/LTE, 5G)

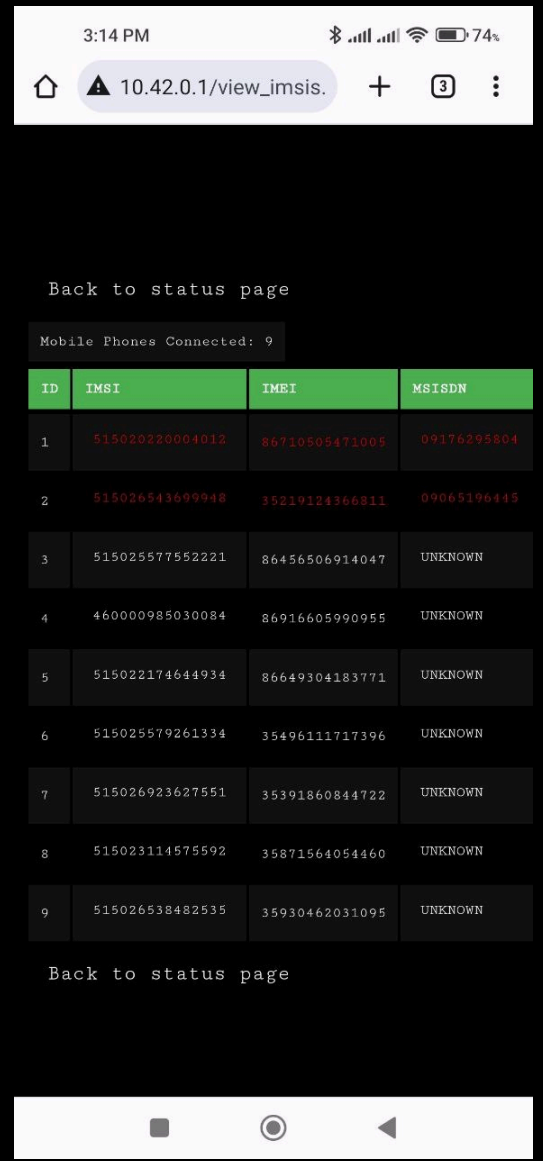
- Send deceptive signals to mobile devices, making them believe that higher-generation networks (3G, 4G/LTE, 5G) are not available in the area. This encourages the mobile devices to "fall back" to a lower-generation network, such as 2G, which may be less secure.

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

On-going Project (Athena)

CELLULAR ASSAULT VILLAGE





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 essential 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