Low Cost Stingrays (IMSI-Catchers)

Pedro Candel aka “s4ur0n” (@NN2ed_s4ur0n)

Whoami


```
class PedroC:
    def __init__(self):
     self.name =         'Pedro Candel'
     self.email =        's4ur0n@s4ur0n.com'
     self.web =       'https://www.s4ur0n.com'
     self.nick =      '@NN2ed_s4ur0n'
     self.company =   'CS³ Group'
     self.role =         'Security Researcher'
     self.work =     [ 'Reversing', 'Malware', 'Offensive Security', '…' ]
     self.groups =       [ 'mlw.re', 'OWASP', 'NetXploit', '...' ]
```

mlw.re

OWASP
Open Web Application Security Project

Low Cost Stingrays (IMSI-Catchers)

1. Introducción
2. Stingrays (Productos comerciales)
3. Low Cost IMSI-Catcher
4. Problemas encontrados
5. Jammers
6. CS³ IIC (Interactive IMSI Catcher)

1. Introducción

Conceptos básicos 101

Introducción

- An **International Mobile Subscriber Identity-catcher**, or IMSI-catcher, is a telephone eavesdropping device used for intercepting mobile phone traffic and tracking location data of mobile phone users.

- Essentially a **"fake"** mobile tower acting between the target mobile phone and the service provider's real towers, it is considered a man-in-the-middle (MITM) attack.

- The **3G wireless** standard **mitigates some risk** due to mutual authentication required from both the handset and the network.

- However, sophisticated attacks may be able to **downgrade 3G and LTE to non-LTE** network services which ***do not require mutual authentication***.

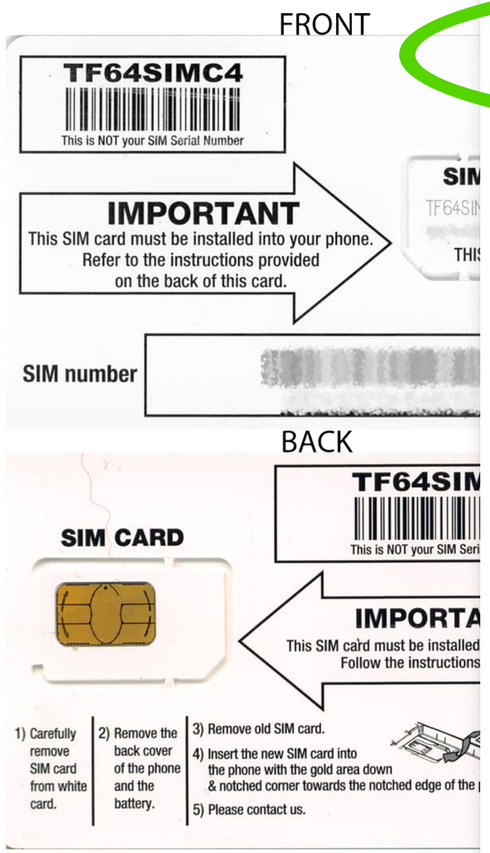
- **Source**: https://en.wikipedia.org/wiki/IMSI-catcher

Introducción

- **Tipos**:
  - **Pasivo** (Sólo
  - **Activo** (Emisi

Introducción

- **SIM 101**



File Name	File ID	Size
EF LP	6F05	1-n bytes nth language code
EF IMSI	6F07	9 bytes
EF KC	6F20	9 bytes
EF HPPLMN	6F31	1 byte
EF SST	6F38	X bytes X >= 2
EF BCCH	6F74	16 bytes
EF ACC	6F78	2 bytes
EF FPLMN	6F7B	12 bytes
EF LOCI	6F7E	11 bytes
EF AD	6FAD	3 + X bytes
EF Phase	6FAE	1 byte

ER FILE (MF)

	Size
	10 bytes

Introducción

- **IMSI 101 (International Mobile Subscriber Identity)**

  - Es un **número de 15 dígitos** que reconoce el operador que está usando su teléfono.

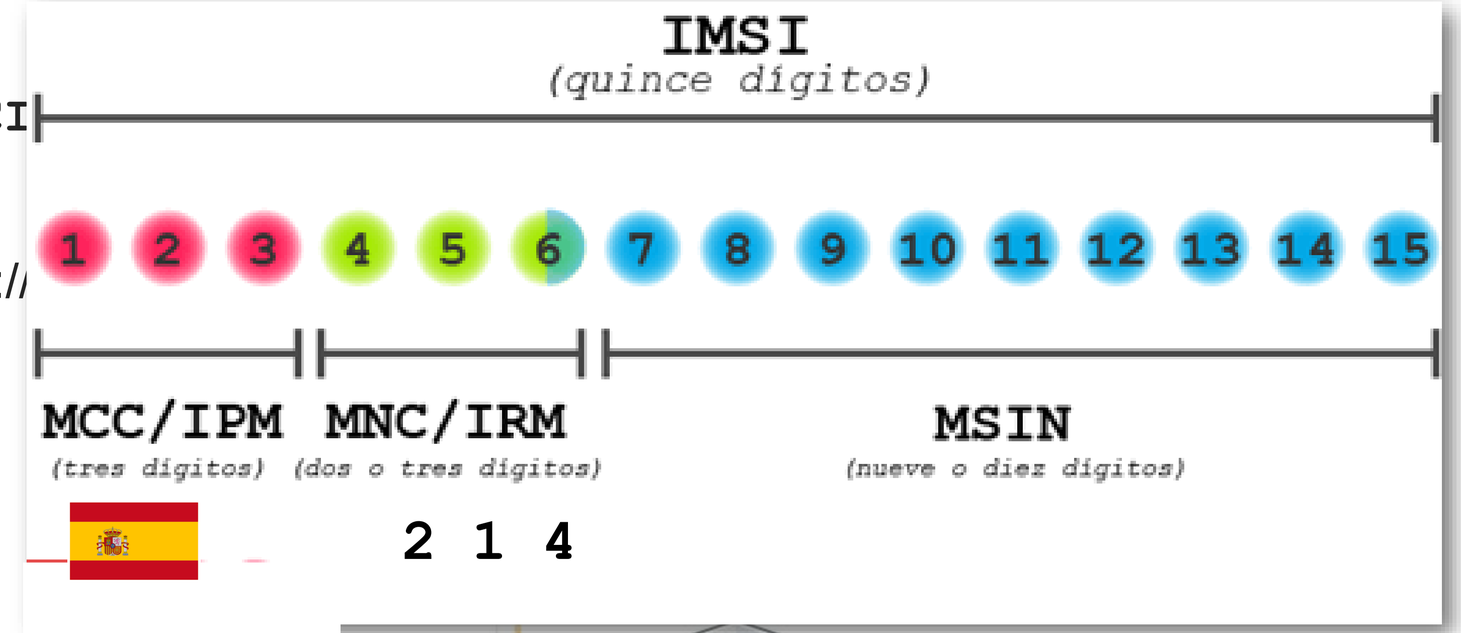
  - Cada IMSI es un **código único**.

  - El dispositivo lo **almacena** y lo **envía** de **forma segura** a su red ***para identificarlo***.

  - Los números IMSI están **asociados a redes móviles**, tanto GPRS/EDGE en 2G, UMTS/HSPA en 3G y en LTE (4G).

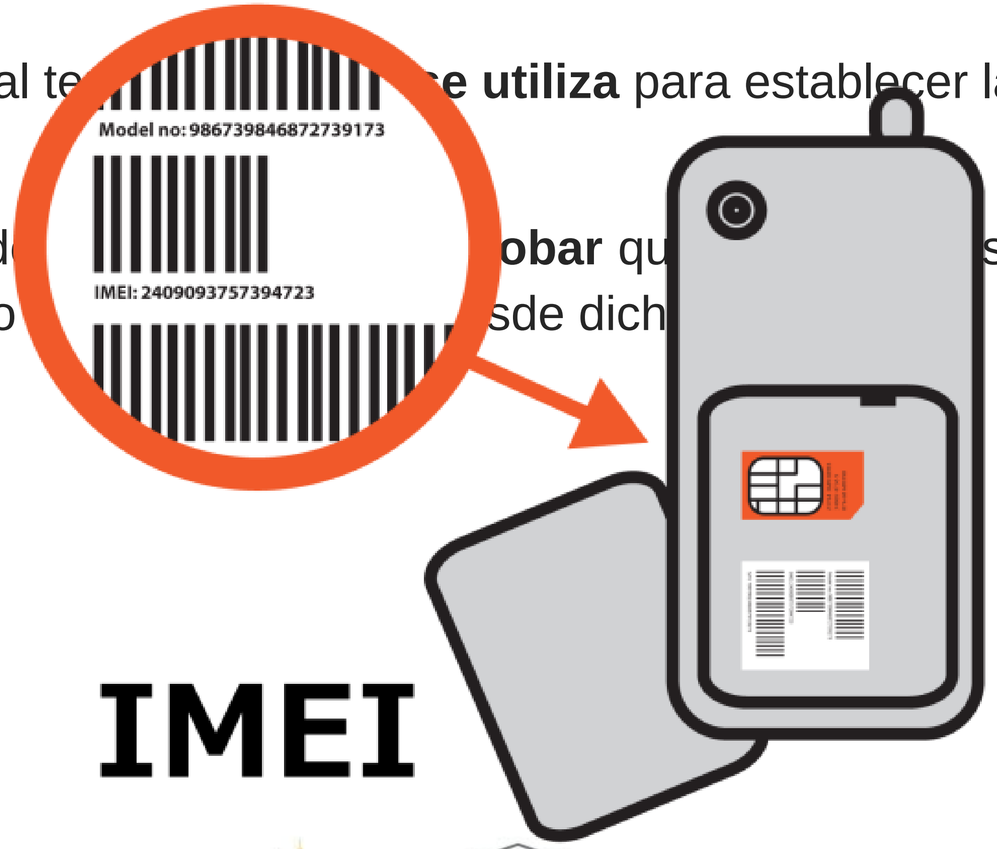
Introducción

- El IMSI se encuentra compuesto por **3 partes**:
  - **MCC** (Mobile Country Code) con 3 dígitos.
  - **MNC** (Mobile Network Code) con 3 dígitos EMEA y 2 dígitos NAR.
  - **MSIN** (Mobile Subscriber Identification Number) con 9 ó 10 dígitos.
- **AT+CI**
- https://



Introducción

- **IMEI 101 (International Mobile Station Equipment Identity)**
  - **Identifica** al te… **se utiliza** para establecer la comunicación.
  - Los operad… **obar** qu… s válido y no ha sido denunciado … sde dich…
  - **AT+CGSN**
  - ***#06#**



- **Conexión 101**

  - La **conexión inicial** le da al dispositivo móvil un **código temporal de identidad de abonado móvil** (**TMSI**).

  - Se utiliza para las identificaciones de suscriptores **cada vez que accede a la red móvil**.

  - El número temporal **se genera** mientras el teléfono se está inicializando ya que el número IMSI original **no se puede transmitir**.

  - El teléfono solo genera un número temporal de TMSI y **la red lo usa para identificarlo**.

Introducción

- Las bases de datos de suscriptores permanentes incluyen **HLR** (**Home Location Register**) y **VLR** (**Visitor Location Register**).

- El código IMSI obtiene la **información detallada** sobre el dispositivo móvil en la base de datos **HLR** y **VLR**.

- Para que ***no pueda ser obtenido***, el IMSI… sólo se usa cuando el TMSI (Temporary Mobile Subscriber Identity) **no se encuentra disponible**, p.e. en la conexión inicial.

- El VLR es responsable de la **localización actual** de un suscriptor y **asigna** un TMSI.

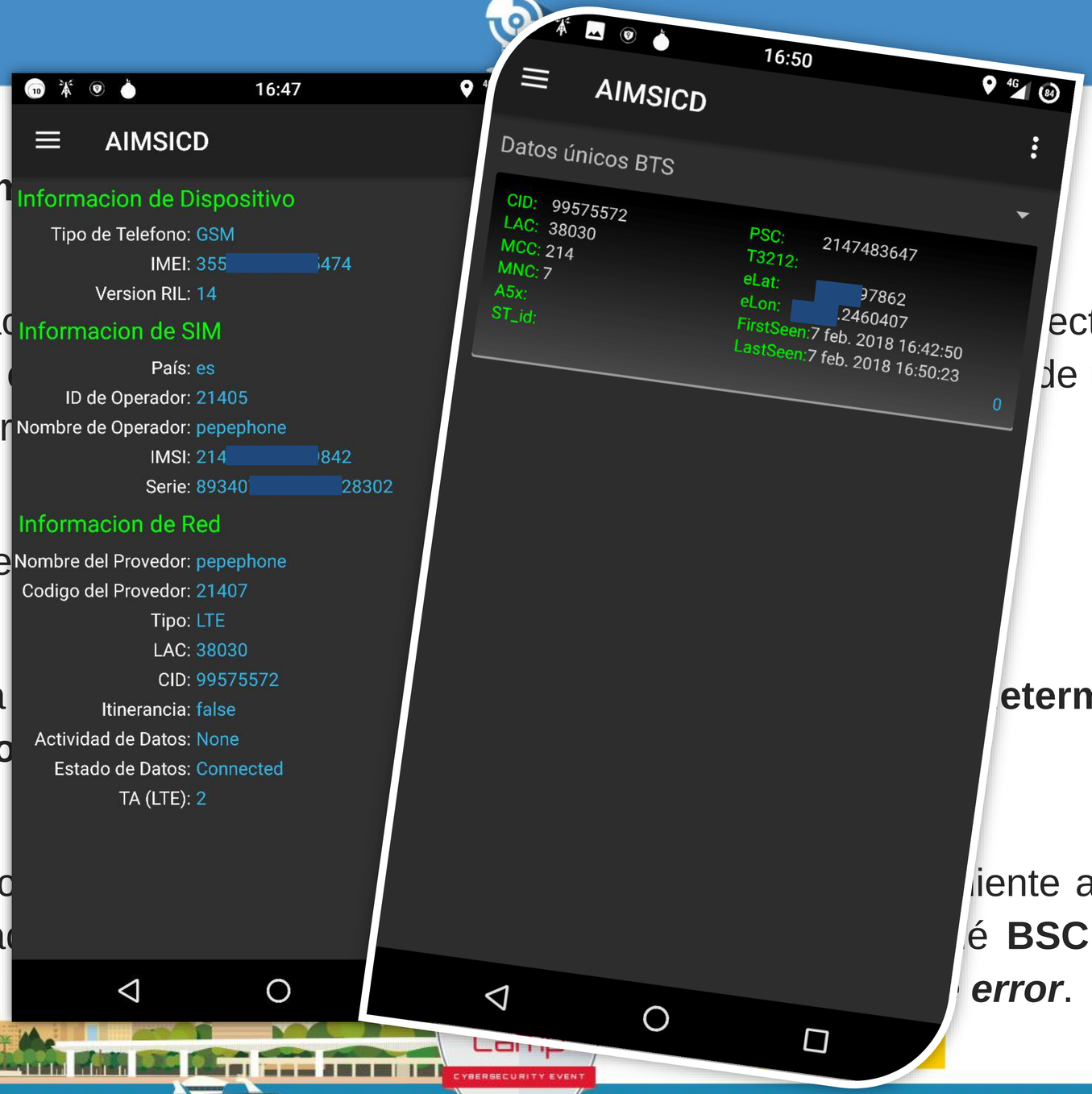
Introducción

- El terminal **almacena el TMSI en la SIM** y en el VLR

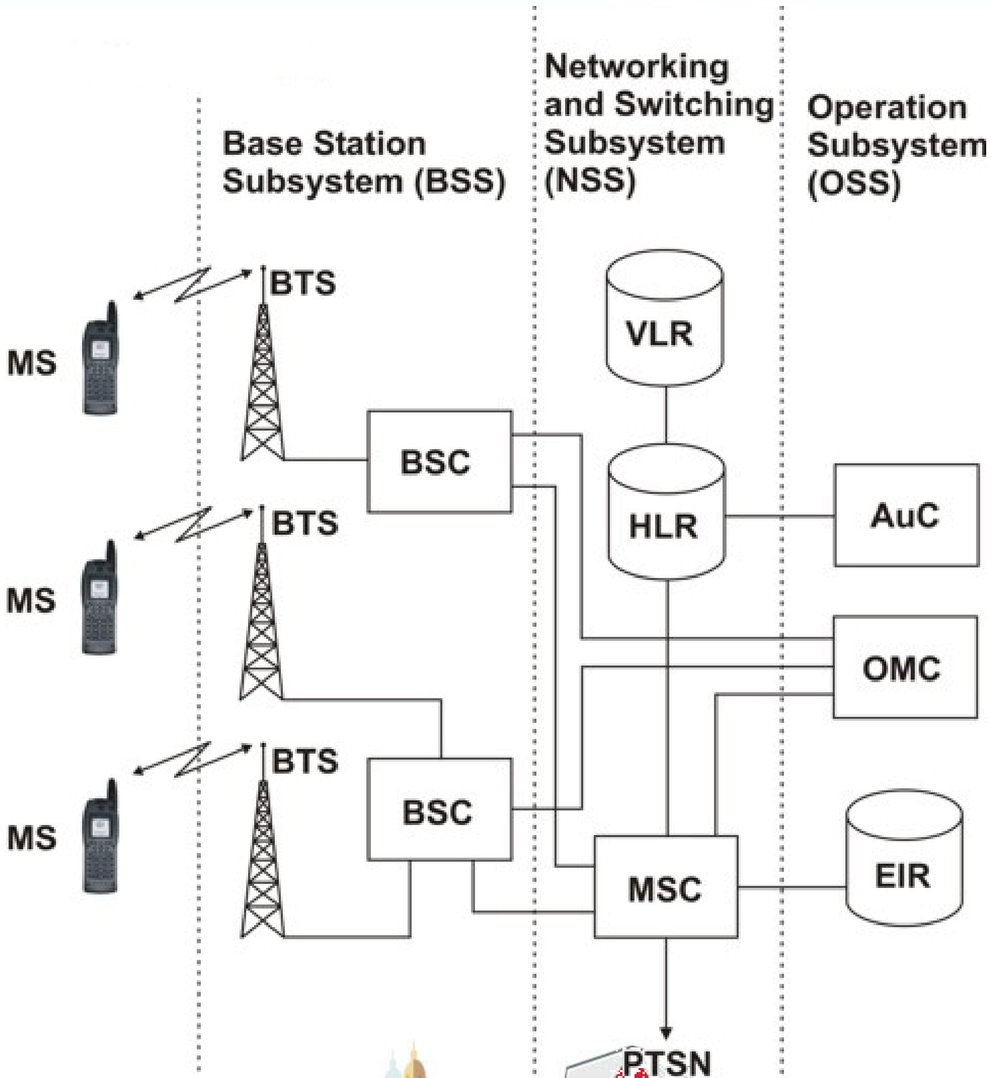
- Consulta al **HLR de origen** los permisos del usuario (por ejemplo, si puede hacer llamadas o no).

Introducción

- **HLR (Hon**
  - Almac ectado o no y las de usar, tipo de ter
  - Es de
  - Cada **eterminado y únic**
  - Al rec iente al número llama é **BSC** hay que pedir ***error***.



Introducción



2. Stingrays

Productos Comerciales

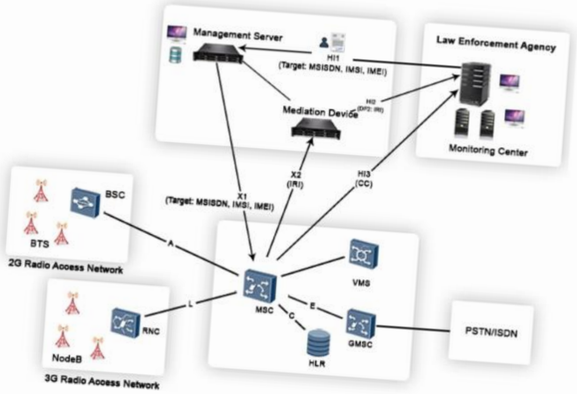
https://www.shoghicom.com/cellular-network-lawful-interception.php

SHOGHI

ABOUT US PRODUCTS SERVICES CAREER SUPPORT

Description

Shoghi Lawful Interception Solution for cellular networks has been designed to intercept the traffic of GSM and CDMA cellular users from Telecom Service Provider's switch. Shoghi provides a comprehensive solution that delivers state-of-the-art surveillance capabilities for interception of Voice Calls, SMS, sent/received e-mails, browsed Webpages, Facebook, Twitter, Skype (voice call log) and VoIP sessions along with CDR from GSM and CDMA cellular networks. System is also equipped with CDR analysis application to perform the automatic linking and associations of the targets. SCL-LICN is equipped with HTTPS interception module to handle the IP traffic from HTTPS/SSL secured site like Facebook, Twitter, Gmail, Yahoo Mail etc.



SCL-LICN is capable of monitoring Voice and SMS along with CDR from traditional GSM and CDMA networks and IP data from next generation packet-switched networks, 2G/3G mobile networks (e.g. GPRS, EDGE, UMTS). System provides interception of e-mail, browsed webpages, and VoIP sessions etc from IP data. The SCL-LICN solution usually acts as a bridge or mediator between the service provider's network and the LEA's monitoring centers.

The SCL-LICN supports both ETSI and CALEA interface and can be integrated with switches of popular manufacturers like Alcatel Lucent, Juniper, Ericsson, Cisco etc. Shoghi provides turnkey solution which covers Probe, Mediation device and Processing Server at the service provider's side and target provisioning system at LEA side.

Shoghi's Probes, mediation device and provisioning systems can be suitably customized to integrate with service provider's switch to implement the interception as per specific national legal requirements.

Shoghi Cellular M
scenarios. Cellular
handset and the B

Cellular monitorin

nission critical
etween mobile

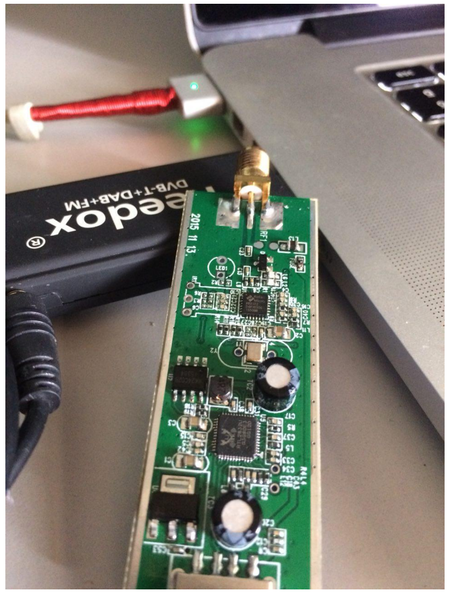
while moving.

- Wideban
- Passive C
- Semi Act

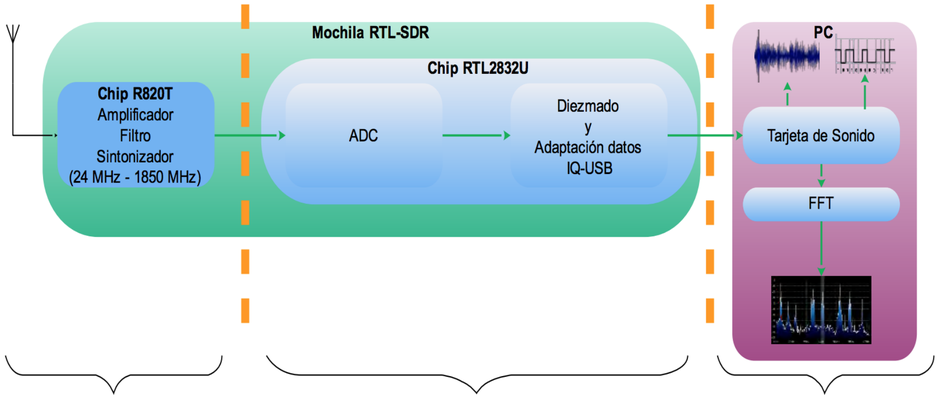
3. Low Cost IMSI-Catcher

SDR (Software Defined Radio)

Dongle USB DVB-T (RTL2832U)



- Rango de frecuencias: **24-1766 MHz**
- Ancho de banda: **2.4 MHz**
- Coste: **~12 €**
- Modificaciones:
  - Hardware: UpConverters/DownConverters para LF/MH/HF.
  - Software: Drivers modificados para ajustar la Frecuencia Intermedia.



Low Cost IMSI-Catcher (SDR)

https://github.com/Oros42/IMSI-catcher

IMSI-catcher

What you need

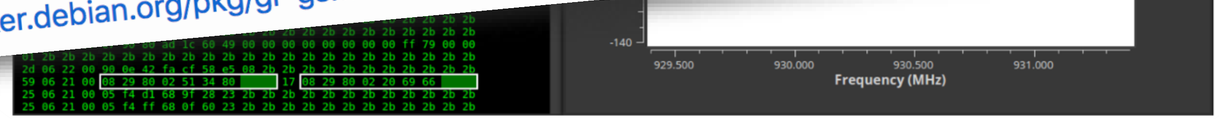
1 PC
1 USB DVB-T key (RTL2832U) with antenna (less than 15$) or a OsmocomBB phone or HackRF

Setup

```
sudo apt install python-numpy python-scipy python-scapy

sudo add-apt-repository -y ppa:ptrkrysik/gr-gsm
sudo apt update
sudo apt install gr-gsm
```

If gr-gsm failled to setup. Try this setup : https://github.com/ptrkrysik/gr-gsm/wiki/Installation
Debian : https://tracker.debian.org/pkg/gr-gsm



- **Instalación**

- `$ sudo apt-get update`
- `$ sudo apt-get upgrade`
- `$ sudo apt-get -y install wim net-tools git python-pip gnutls-dev cmake libboost-all-dev libcppunit-dev swig doxygen liblog4cpp5-dev python-numpy python-scipy python-scapy automake autoconf libhackrf-dev wireshark sqlite3`
- `$ pip install PyBOMBS`
- `$ pybombs auto-config`
- `$ pybombs recipes add-defaultspybombs prefix init /usr/local -a default -R gnuradio-default`
- `$ pybombs install` **`gr-gsm`**

- **SoapySDR**

- `$ cd /usr/local`
- `$ git clone https://github.com/pothosware/SoapySDR.git`
- `$ cd SoapySDR`
- `$ mkdir build`
- `$ cd build`
- `$ cmake ..`
- `$ make -j4`
- `$ sudo make install`
- `$ sudo ldconfig -v`

- **GNU Radio GSM**

- `$ cd /usr/local`
- `$ git clone https://github.com/ptrkrysik/gr-gsm.git`
- `$ cd gr-gsm`
- `$ mkdir build`
- `$ cd build`
- `$ cmake ..`
- `$ make`
- `$ sudo make install`
- `$ sudo ldconfig -v`

Low Cost IMSI-Catcher (SDR)

- **Kalibrate**

- `$ cd /usr/src`
- `$ git clone https://github.com/steve-m/kalibrate-rtl`
- `$ cd kalibrate-rtl/`
- `$ ./bootstrap`
- `$ ./configure`
- `$ make`
- `$ sudo make install`

- **GNU Radio OsmoSDR**

```
$ cd /usr/src
$ git clone git://git.osmocom.org/gr-osmosdr
$ cd gr-osmosdr
$ mkdir build
$ cd build
$ cmake ../
$ make
$ sudo make install
$ sudo ldconfig -v
```

Low Cost IMSI-Catcher (SDR)

- **IMSI Catcher (Oros42)**

- `$ cd /usr/src`
- `$ git clone` **`https://github.com/Oros42/IMSI-catcher`**
- `$ cd IMSI-catcher`

Low Cost IMSI-Catcher (SDR)

- **Funcionamiento**:

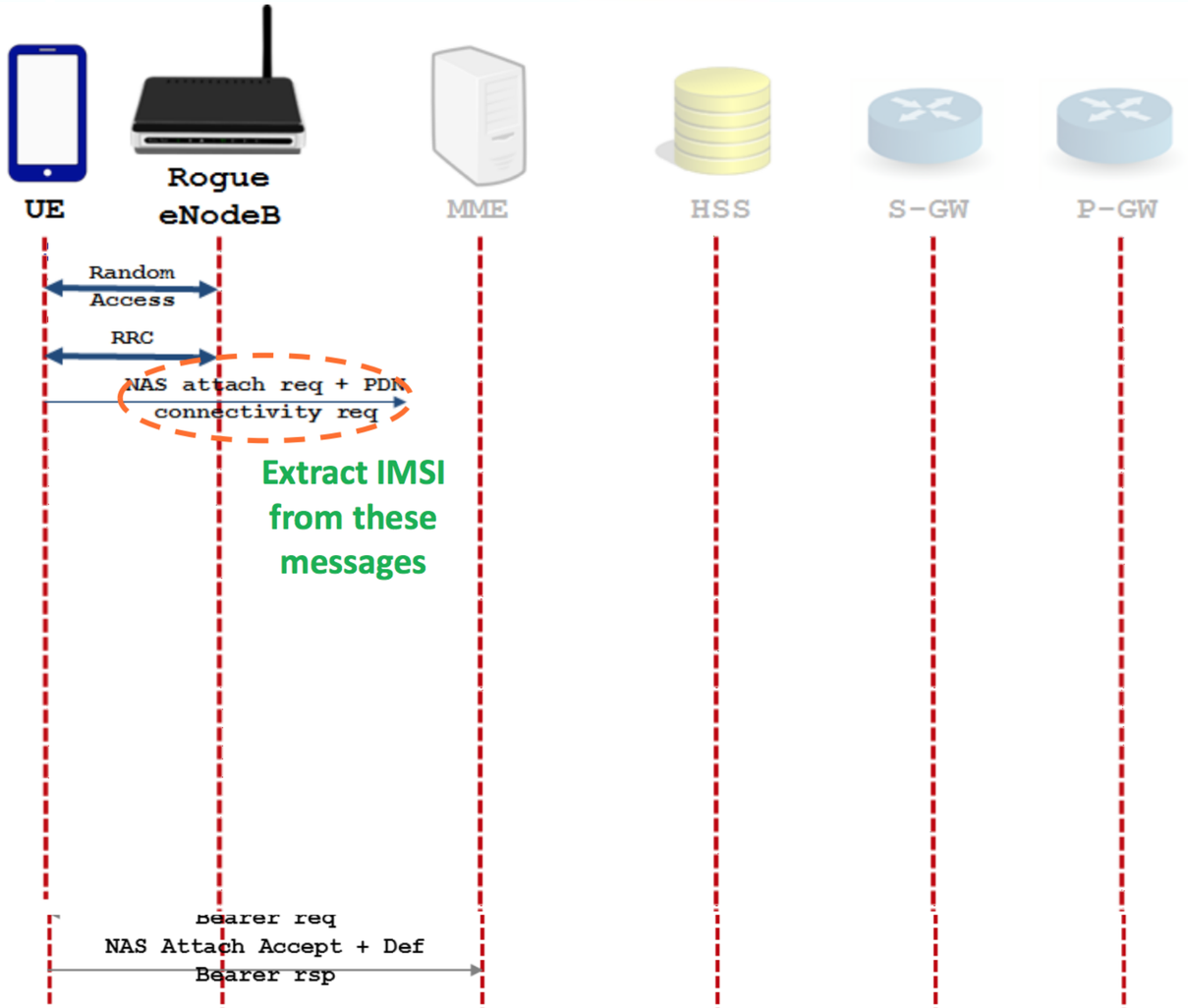
- `$ cd /usr/src`
- **`$ python sim`**
- **`$ grgsm_live`** **`rt=10000`**
- **`$ wireshark`** **`-i lo`**

LOW-COST LTE IMSI CATCHER (STINGRAY)

- Despite common assumptions, in LTE the IMSI is always transmitted in the clear at least once
  - If the network has never seen that UE, it must use the IMSI to claim its identity
  - A UE will trust *any* eNodeB that claims it has never seen that device (pre-authentication messages)
  - IMSI can also be transmitted in the clear in error recovery situations (very rare)
- Implementation
  - USRP B210
  - LTE base station – OpenLTE (modified LTE_fdd_eNodeB)
    - Added feature to record IMSI from Attach Request messages
  - Send attach reject after IMSI collection
  - Tested with my phone and 2 LTE USB dongles
    - Experiments in controlled environment
- **Stingrays also possible in LTE without need to downgrade connection to GSM**
  - Low-cost IMSI catcher (under $2000)

- Source: [2016] http://rogerpiquerasjover.net/LTE_open_source_HackerHalted.pdf

¿Y en 3G/4G qué hacemos?



- Source: [2016] http://rogerpiquerasjover.net/LTE_open_source_HackerHalted.pdf

¿Y en 3G/4G qué hacemos?

```
77 [MESSAGE] 6 -> 8 0 0103:9902850 NAS_UPLINK_DATA_IND ue_id 0x00000002 len 17
78 [MESSAGE] 8 -> 9 0 0103:9903210 EMMAS_DATA_IND ue id 0x00000002 len 17 tai:  plmn 242.[redacted] tac[redacted]
79 [EVENT] 9 0103:990822T3470 stopped UE 0x00000002
80 [MESSAGE] 9 -> 9 0 0103:990956EMMREG_COMMON_PROC_CNF ue id 0x00000002
81 [EVENT] 9 0103:991075EMM state DEREGISTERED UE 0x00000002
82 [MESSAGE] 8 -> 13 0 0103:9911920 S6A_AUTH_INFO_REQ IMSI 242[redacted] visited_plmn 242.[redacted] re_sync 0
83 [MESSAGE] 13 -> 8 0 0103:9921110 S6A_AUTH_INFO_ANS imsi 242[redacted] DIAMETER_AUTHENTICATION_DATA_UNAVAILABL
84 [EVENT] 7 0103:9921680 S6A_AUTH_INFO_ANS S6A Failure imsi 242[redacted]
85 [MESSAGE] 8 -> 9 0 0103:9921820 EMMCN_AUTHENTICATION_PARAM_FAIL
```

Figure 4: IMSI Capture

28	56.711592	127.0.0.1	127.0.1.10	S1AP/NAS-EPS	186 id-uplinkNASTransport, Attach request, PDN connectivity request
35	81.793250	127.0.0.1	127.0.1.10	S1AP/NAS-EPS	194 id-initialUEMessage, Attach request, PDN connectivity request
46	106.793796	127.0.0.1	127.0.1.10	S1AP/NAS-EPS	194 id-initialUEMessage, Attach request, PDN connectivity request
47	106.795616	127.0.1.10	127.0.0.1	S1AP/NAS-EPS	110 SACK id-downlinkNASTransport, Identity request
48	106.812750	127.0.0.1	127.0.1.10	S1AP/NAS-EPS	138 SACK id-uplinkNASTransport, Identity response
55	106.816179	127.0.1.10	127.0.0.1	S1AP/NAS-EPS	110 SACK id-downlinkNASTransport, Attach reject

```
NAS-PDU: 074403
Non-Access-Stratum (NAS)PDU
    0000 .... = Security header type: Plain NAS message, not security protected (0)
    .... 0111 = Protocol discriminator: EPS mobility management messages (0x07)
    NAS EPS Mobility Management Message Type: Attach reject (0x44)
EMM cause
    Cause: Illegal UE (3)
```

Figure 5: ATTACH_REJECT Message

- Source: [2017] https://arxiv.org/abs/1702.04434

2.7 Vulnerabilities in LTE

Previous research has discovered that even with mutual authentication and strong encryption algorithms, a big portion of the signaling messages is sent as plaintext. These are broadcast messages sent to all surrounding base stations (including IMSI Catchers) and can easily be sniffed by a malicious person [LJL+16]. The NAS signaling messages listed below may be processed by the EPS Mobility Management (EMM) entity before the network has established a secure NAS signaling connection [3GP11c]:

- IDENTITY REQUEST (if requested identification parameter is IMSI)
- AUTHENTICATION REQUEST
- AUTHENTICATION REJECT
- ATTACH REJECT (if the EMM cause is not #25)
- DETACH ACCEPT (for non switch off)
- TRACKING AREA UPDATE REJECT (if the EMM cause is not #25)
- SERVICE REJECT (if the EMM cause is not #25)

- Source: [2018] https://brage.bibsys.no/xmlui/handle/11250/2462189

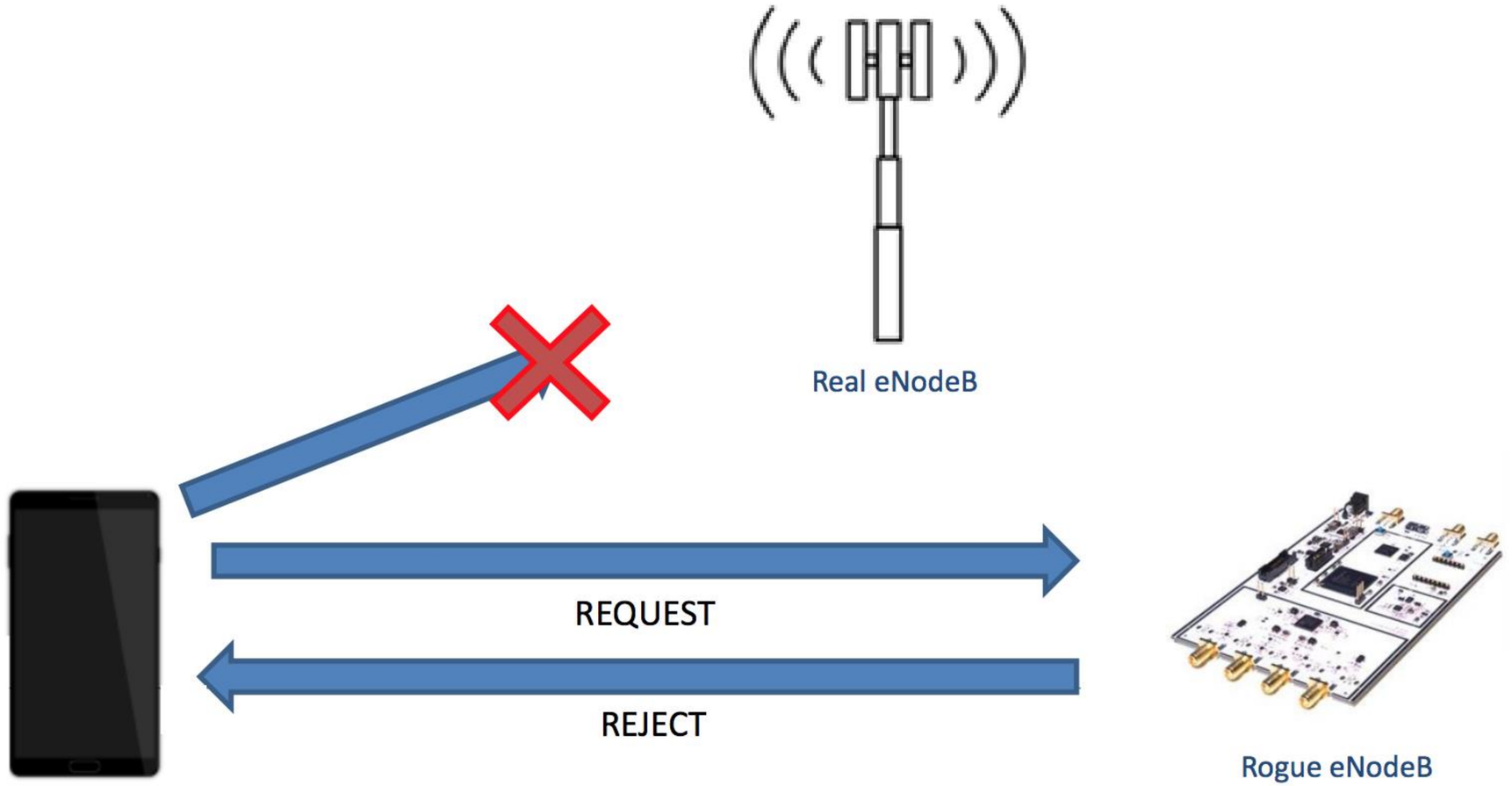
4. Problemas encontrados

Aspectos técnicos del GNU/Linux y el SDR

Problemas técnicos

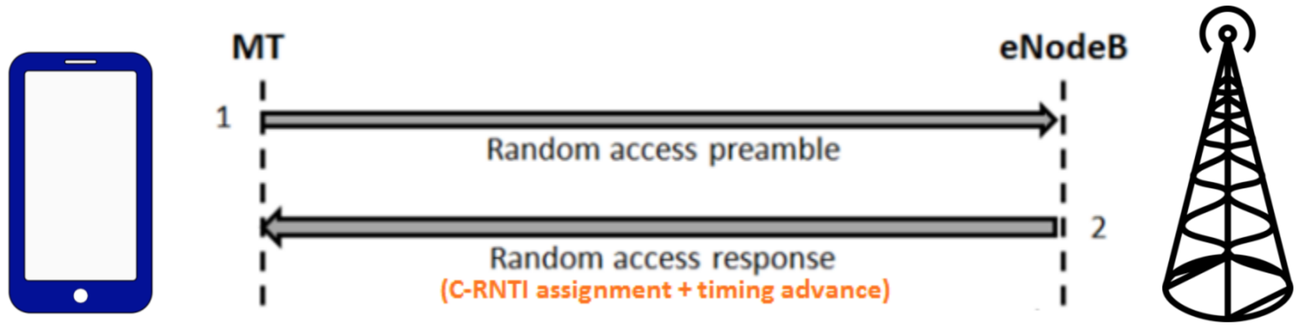
- `cmake ../ -DINSTALL_UDEV_RULES=ON \`
  `-DDETACH_KERNEL_DRIVER=ON`
- Modo **headless** sin interface gráfica.
- Frecuencia(s) y calibración de los dispositivos.
- Etc, etc, etc...

Problemas técnicos



LOCATION LEAKS AND DEVICE TRACKING

- RNTI
  - PHY layer id sent in the clear in EVERY SINGLE packet, both UL and DL
  - Identifies uniquely every UE within a cell
    - Changes infrequently
    - Based on several captures in the NYC and Honolulu areas
  - No distinguishable behavior per operator or per base station manufacturer
  - Assigned by the network in the MAC RAR response to the RACH preamble



- Source: [2016] http://rogerpiquerasjover.net/LTE_open_source_HackerHalted.pdf

5. Jammers

Inhibidores de señal

Jammers

https://eee.yasar.edu.tr/wp-content/uploads/2015/06/cem_anil_kivanc_jammer_poster_yasar.pdf

VCO (ZX95-2500W+)

The frequency range: 800-2700 MHz
RF Output : 1-4 dBm

	Frequency Band (MHz)	Center Frequency (MHz)	Tuning Voltage (Volts)	Bandwidth (MHz)	Voltage Peak to Peak(V_{pp})
GSM-900	935-960	947.5	0.7	25	0.25
GPS	565-1585	1575	7.7	20	0.22
GSM-1800	805-1820	1812.5	10.8	15	0.2

Jammers

	HackRF	bladeRF		USRP		
		x40	x115	B100 Starter	B200	B210
Radio Spectrum	30 MHz – 6 GHz	300 MHz – 3.8 GHz		50 MHz – 2.2 GHz [1]	50MHz – 6 GHz	
Bandwidth	20 MHz	28 MHz		16 MHz [2]	61.44 MHz [3]	
Duplex	Half	Full		Full	Full	2x2 MIMO
Sample Size (ADC/DAC)	8 bit	12 bit		12 bit / 14 bit	12 bit	
Sample Rate (ADC/DAC)	20 Msps	40 Msps		64 Msps / 128 Msps	61.44 Msps	
Interface (Speed)	USB 2 HS (480 megabit)	USB 3 (5 gigabit)		USB 2 HS (480 megabit)	USB 3 (5 gigabit)	
FPGA Logic Elements	[4]	40k	115k	25k	75k	150k
Microcontroller	LPC43XX	Cypress FX3		Cypress FX2	Cypress FX3	
Open Source	Everything	HDL + Code Schematics		HDL + Code Schematics	Host Code [5]	
Availability	January 2014	Now		Now	Now	
Cost	$300 [6]	$420	$650	$675	$675	$1100

SDR “selectivo”

- Proyecto **Modmobmap** (recupera información de las celdas 2G/3G/4G) con un dispositivo móvil auxiliar y ofrece la información por API o en ficheros JSON.

- https://github.com/Synacktiv/Modmobmap

- Selección del **operador** (automático o manual)

- Selección del **canal** (automático o manual)

```
# sudo python modmobmap.py -m servicemode
=> Requesting a list of MCC/MNC. Please wait, it may take a while...
[+] New cell detected [CellID/PCI-DL_freq  (83-6400)]
 Network type=4G
 PLMN=151515-1515
 Band=20
 Downlink EARFCN=6400
Found 5 operator(s)
{u'20810': u'F SFR', u'20820': u'F-Bouygues Telecom', u'20815': u'Free', u'20801': u'Orange F', u'20811'
: u'SFR Home 3G'}
[+] Unregistered from current PLMN
[+] New cell detected [CellID/PCI-DL_freq  (f0e02-10787)]
 Network type=3G
 PLMN=208-1
 Band=1
 Downlink UARFCN=10787
 Uplink UARFCN=9837
=> Changing MCC/MNC for: 20810
[+] New cell detected [CellID/PCI-DL_freq  (298-6400)]
 Network type=4G
 PLMN=208-10
 Band=20
 Downlink EARFCN=6400
[+] New cell detected [CellID/PCI-DL_freq  (298-6300)]
 Network type=4G
 PLMN=208-10
 Band=20
 Downlink EARFCN=6300
[+] New cell detected [CellID/PCI-DL_freq  (298-6200)]
 Network type=4G
 MN=208-10
```

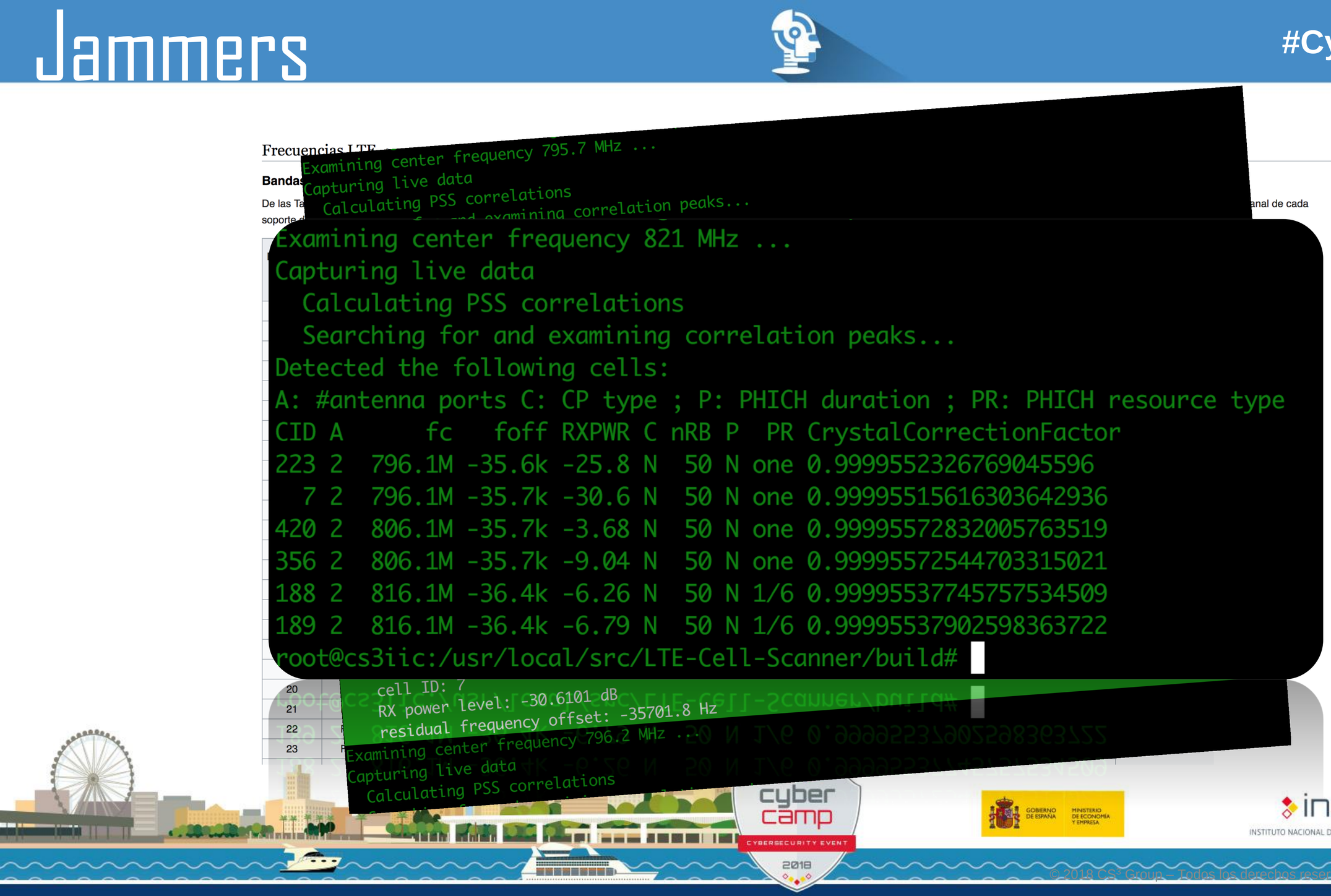
Frecuencias 2G / 3G / 4G

- https://www.frequencycheck.com/search?s=spain
- https://www.mincotur.gob.es/telecomunicaciones/espectro/Paginas/cnaf.aspx
- https://www.cellmapper.net/
- Etc...

Frecuencias 2G

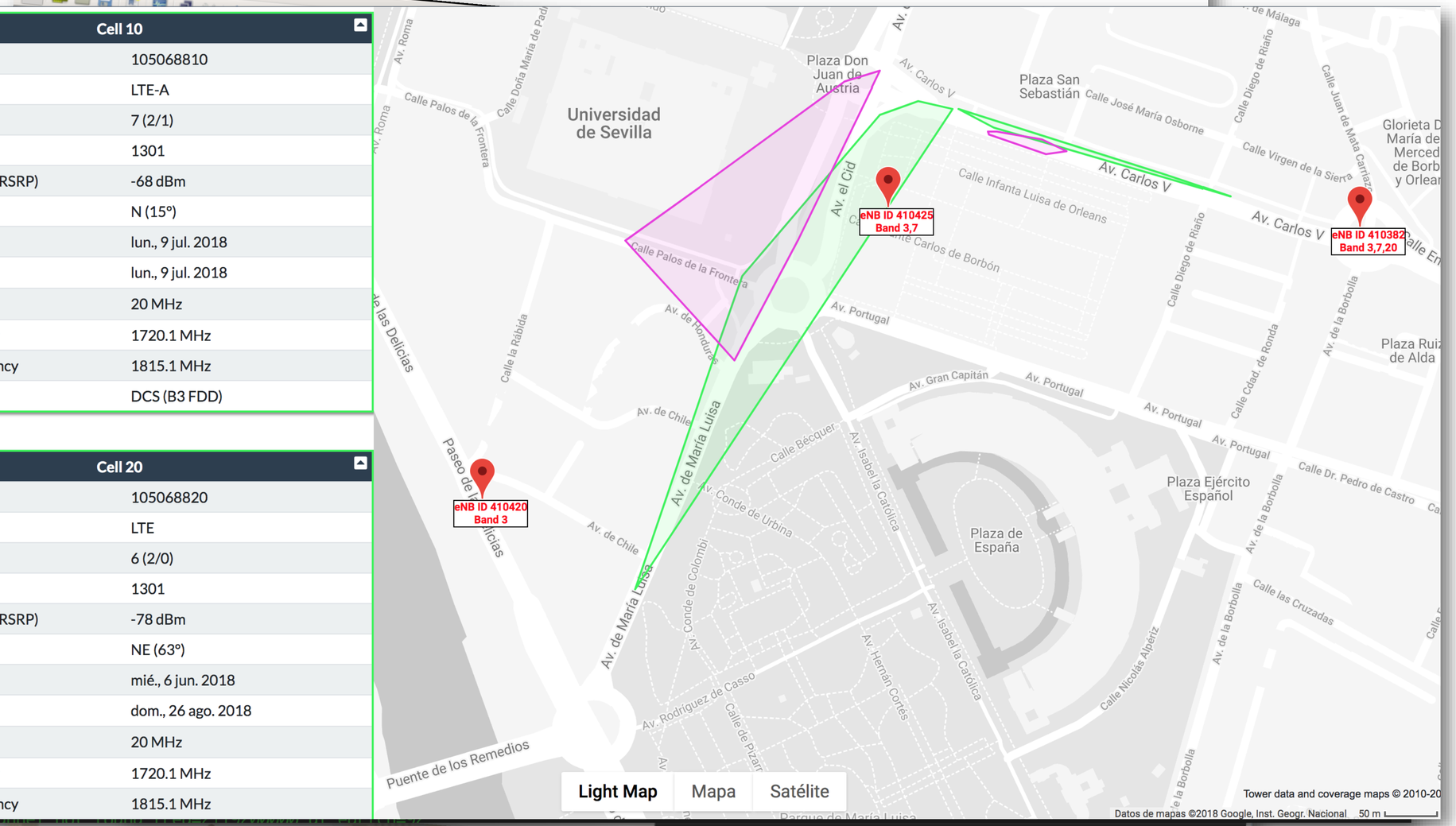
```
root@cs3iic:/usr/local/src/LTE-Cell-Scanner/build# grgsm_scanner

ARFCN:  976, Freq:  925.4M, CID:   220, LAC: 18105, MCC: 214, MNC:   3, Pwr: -33
ARFCN:  979, Freq:  926.0M, CID:     0, LAC: 18100, MCC: 214, MNC:   3, Pwr: -39
ARFCN:  980, Freq:  926.2M, CID:   216, LAC: 18100, MCC: 214, MNC:   3, Pwr: -37
ARFCN:  981, Freq:  926.4M, CID:   170, LAC: 18100, MCC: 214, MNC:   3, Pwr: -34
ARFCN:  982, Freq:  926.6M, CID:     0, LAC: 18105, MCC: 214, MNC:   3, Pwr: -33
^C^C^Croot@cs3iic:/usr/local/src/LTE-Cell-Scanner/build#
```



Cell 10	
Cell Identifier	105068810
System Subtype	LTE-A
PCI	7 (2/1)
EARFCN	1301
Maximum Signal (RSRP)	-68 dBm
Direction	N (15°)
First Seen	lun., 9 jul. 2018
Last Seen	lun., 9 jul. 2018
Bandwidth*	20 MHz
Uplink Frequency	1720.1 MHz
Downlink Frequency	1815.1 MHz
Frequency Band	DCS (B3 FDD)

Cell 20	
Cell Identifier	105068820
System Subtype	LTE
PCI	6 (2/0)
EARFCN	1301
Maximum Signal (RSRP)	-78 dBm
Direction	NE (63°)
First Seen	mié., 6 jun. 2018
Last Seen	dom., 26 ago. 2018
Bandwidth*	20 MHz
Uplink Frequency	1720.1 MHz
Downlink Frequency	1815.1 MHz



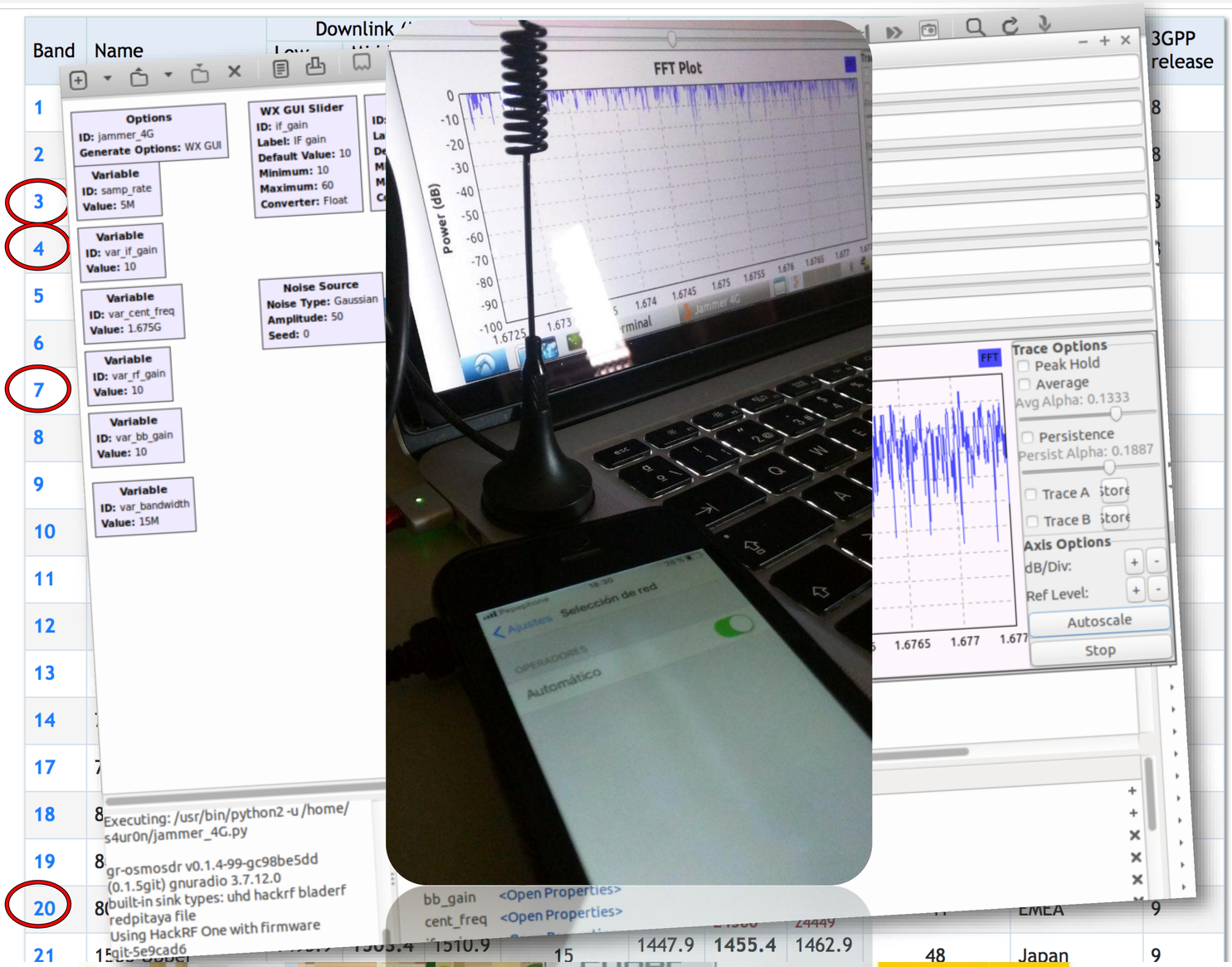
Jammers

niviuk.free.fr/lte_band.php

SDR

-
-
-
-

Hz).



6. CS³ IIC

Interactive IMSI Catcher

CS³ IIC (Interactive IMSI Catcher)

Características:

- OpenSource
-
-
-
- D
- R
- Lo
- Ea
- Etc

GRACIAS