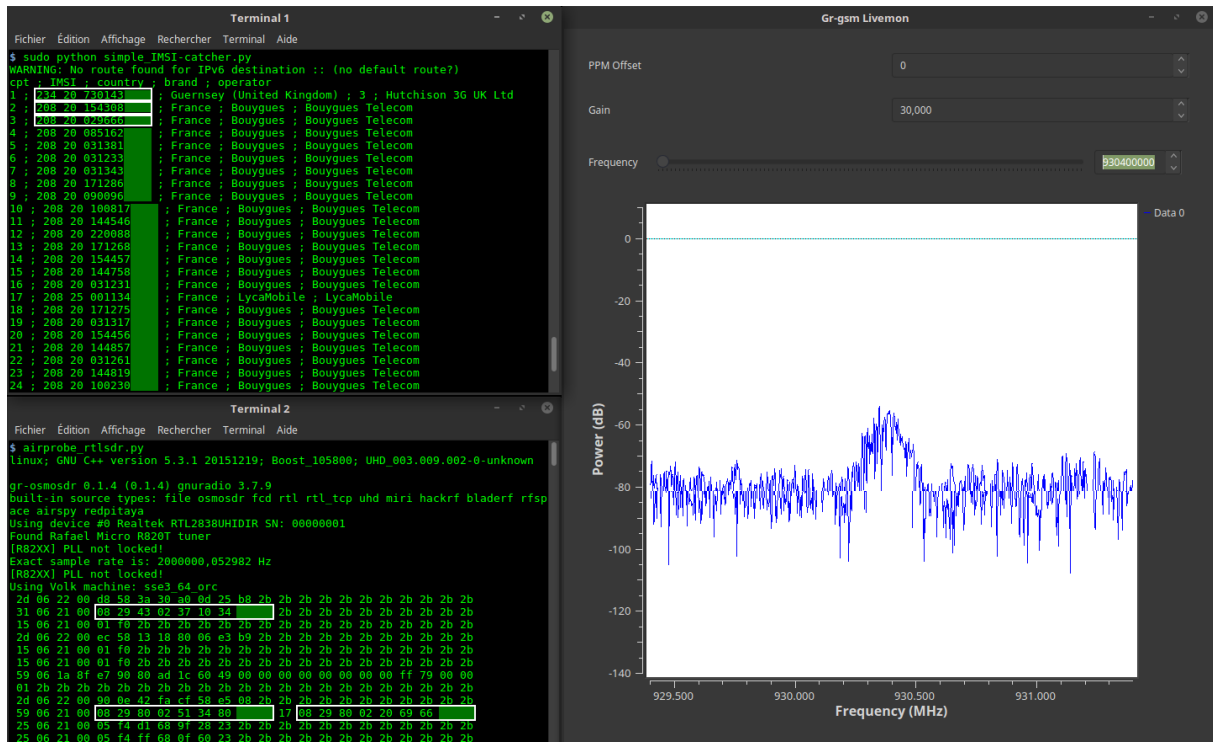


IMSI-catcher

This program shows you IMSI numbers, country, brand and operator of cellphones around you.

/! This program was made to understand how GSM network work. Not for bad hacking !



What you need

1 PC with Gnu/Linux. Tested with :

- debian 10
- Ubuntu 20.04/LinuxMint 20+
- Kali 2020+

1 SDR receiver. Tested with :

- USB DVB-T key (RTL2832U) with antenna (less than 15\$)
- OsmocomBB phone
- HackRF
- BladeRF

Setup

```
1 git clone https://github.com/Oros42/IMSI-catcher.git
2 cd IMSI-catcher
```

or

```
1 wget https://github.com/Oros42/IMSI-catcher/archive/master.zip && unzip
  -q master.zip
2 cd IMSI-catcher-master
```

```
1 sudo apt install python3-numpy python3-scipy python3-scapy
```

Warning : don't use python 3.9 (ctypes bug)!

You have the choice with 2 types of gr-gsm's install : in your OS or with docker.

Install gr-gsm in your OS (recommended)

```
1 sudo apt-get install -y \
2     cmake \
3     autoconf \
4     libtool \
5     pkg-config \
6     build-essential \
7     python-docutils \
8     libcppunit-dev \
9     swig \
10    doxygen \
11    liblog4cpp5-dev \
12    gnuradio-dev \
13    gr-osmosdr \
14    libosmocore-dev \
15    liborc-0.4-dev \
16    swig
```

```
1 gnuradio-config-info -v
```

if >= 3.8

```
1 git clone -b maint-3.8 https://github.com/velichkov/gr-gsm.git
```

else (3.7)

```
1 git clone https://git.osmocom.org/gr-gsm
```

```
1 cd gr-gsm
2 mkdir build
3 cd build
```

```
4 cmake ..
5 make -j 4
6 sudo make install
7 sudo ldconfig
8 echo 'export PYTHONPATH=/usr/local/lib/python3/dist-packages/:
    $PYTHONPATH' >> ~/.bashrc
```

Install gr-gsm with Docker

```
1 sudo xhost +local:docker
2 docker pull atomicpowerman/imsi-catcher
3 docker run -ti --net=host -e DISPLAY=$DISPLAY --privileged -v /dev/bus/
    usb:/dev/bus/usb atomicpowerman/imsi-catcher bash
```

Run all `grgsm_*` in this docker.

Usage

We use `grgsm_livemon` to decode GSM signals and `simple_IMSI-catcher.py` to find IMSIs.

```
1 python3 simple_IMSI-catcher.py -h
```

```
1 Usage: simple_IMSI-catcher.py: [options]
2
3 Options:
4  -h, --help                show this help message and exit
5  -a, --alltmsi             Show TMSI who haven't got IMSI (default :
    false)
6  -i IFACE, --iface=IFACE  Interface (default : lo)
7
8  -m IMSI, --imsi=IMSI     IMSI to track (default : None, Example:
9                          123456789101112 or "123 45 6789101112")
10 -p PORT, --port=PORT     Port (default : 4729)
11 -s, --sniff              sniff on interface instead of listening on port
12                          (require root/suid access)
13 -w SQLITE, --sqlite=SQLITE
14                          Save observed IMSI values to specified SQLite
15                          file
15 -t TXT, --txt=TXT        Save observed IMSI values to specified TXT file
16 -z, --mysql              Save observed IMSI values to specified MYSQL DB
17                          (copy
17                          .env.dist to .env and edit it)
```

Open 2 terminals.

In terminal 1

```
1 sudo python3 simple_IMSI-catcher.py -s
```

In terminal 2

```
1 grgsm_livemon
```

Now, change the frequency until it display, in terminal, something like that :

```
1 15 06 21 00 01 f0 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
2 25 06 21 00 05 f4 f8 68 03 26 23 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
3 49 06 1b 95 cc 02 f8 02 01 9c c8 03 1e 57 a5 01 79 00 00 1c 13 2b 2b
```

Wireshark

You can watch GSM packets with wireshark.

```
1 sudo apt install wireshark
2 sudo wireshark -k -Y '!icmp && gsmtap' -i lo
```

Find frequencies

```
1 grgsm_scanner
```

```
1 ARFCN: 974, Freq: 925.0M, CID: 2, LAC: 1337, MCC: 208, MNC:
  20, Pwr: -41
2 ARFCN: 976, Freq: 925.4M, CID: 4242, LAC: 1007, MCC: 208, MNC:
  20, Pwr: -45
```

Now, you can set the frequency for `grgsm_livemon`:

```
1 grgsm_livemon -f 925.4M
```

Or, for hackrf, fetch the kalibrate-hackrf tool like this:

```
1 sudo apt-get install automake autoconf libhackrf-dev
2 git clone https://github.com/scateu/kalibrate-hackrf
3 cd kalibrate-hackrf/
4 ./bootstrap
5 ./configure
6 make
7 sudo make install
```

Run

```
1 kal -s GSM900
```

```
1 kal: Scanning for GSM-900 base stations.
2 GSM-900:
3     chan:    14 (937.8MHz + 10.449kHz)    power: 3327428.82
4     chan:    15 (938.0MHz + 4.662kHz)    power: 3190712.41
5 ...
```

Log data in mysql

Use `db-example.sql` to create your DB.

```
1 cp .env.dist .env
2 nano .env
3 # set your config
4 sudo apt install python-decouple python3-mysqldb
```

```
1 sudo python3 simple_IMSI-catcher.py -s --mysql
```

scan-and-livemon (no longer used)

Scan frequencies and listen the 1st found :

In terminal 1

```
1 python3 scan-and-livemon
```

In terminal 2

```
1 python3 simple_IMSI-catcher.py
```

Links

Setup of Gr-Gsm : <https://osmocom.org/projects/gr-gsm/wiki/Installation> and <https://github.com/velichkov/gr-gsm>

Frequency : <http://www.worldtimezone.com/gsm.html> and https://fr.wikipedia.org/wiki/Global_System_for_Mobile

Mobile Network Code : https://en.wikipedia.org/wiki/Mobile_Network_Code

Scapy : <http://secdev.org/projects/scapy/doc/usage.html>

IMSI : <https://fr.wikipedia.org/wiki/IMSI>

Realtek RTL2832U : <https://osmocom.org/projects/sdr/wiki/rtl-sdr> and <http://doc.ubuntu-fr.org/rtl2832u>
and <http://doc.ubuntu-fr.org/rtl-sdr>

Donate

To support my work, a tipee would be nice ;-)

<https://liberapay.com/Oros/>