Taller de Telecomunicaciones Modalidad SDR

Proyecto Final
GSM Base Transceiver Station

Santiago Castro

23 de diciembre de 2016

1. Introducción

Este trabajo se trata de una brevísima introducción al estándar GSM (Global System for Mobile Communication) de redes celulares digitales. Se describirá a grandes rasgos de qué se trata esta tecnología y luego se pasará a realizar algunas demostraciones en las cuales se podrá ver cómo funciona GSM.

El acrónimo GSM se debe en realidad al Groupe Spéciale Mobile que tuvo la tarea de definir un nuevo estándar para las comunicaciones móviles que trabajara en las bandas de 900MHz y 1800MHz. En la actualidad también se utilizan las bandas 850MHz y 1900MHz como se verá más adelante. Este estándar utiliza radiobases terrenas para servir a los clientes, a cada estación se le asigna una porción de la banda para operar con el fin de evitar interferencias entre radiobases cercanas. Esto significa que pueden haber dos radiobases que utilicen la misma frecuencia pero deben estar lo suficientemente alejadas como para no interferir una con otra. La Figura 1 ilustra esta idea.

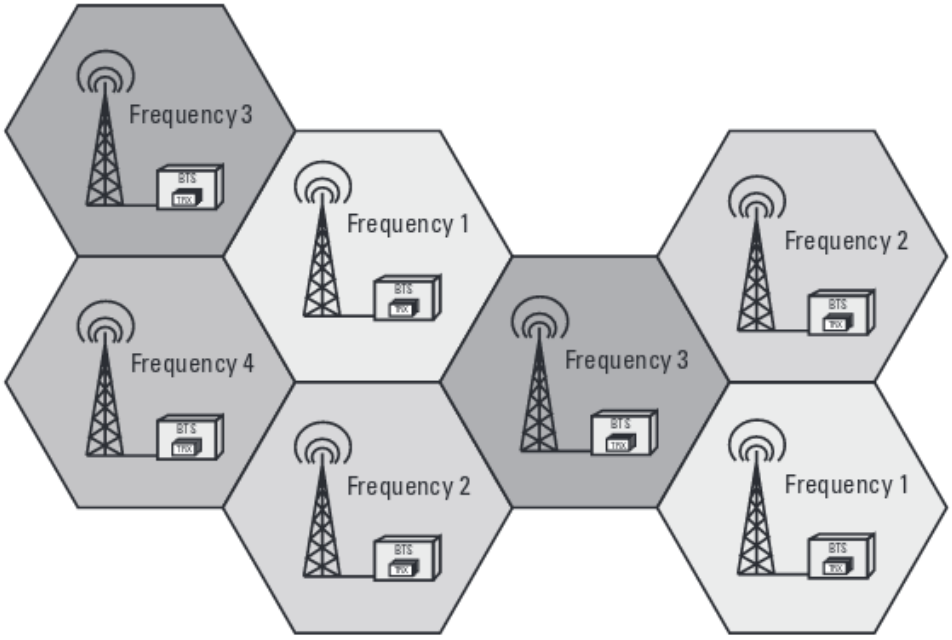


Figura 1: Radio de cobertura de las celdas.

La tecnología GSM utiliza una combinación de FDMA (Frecuency Division Multiple Access) y TDMA (Time Division Multiple Access), lo que resulta en un canal de dos dimensiones, temporal y frecuencial. Esto significa que el tiempo se divide en slots, y para transmitir cada equipo deberá hacerlo dentro de los slots asignados.

Para ver con más detalle el funcionamiento de GSM, se escaneará el espectro en busca de alguna señal y se analizarán tramas GSM. El hardware utilizado es un USRP B100 de Ettus Research. Los programas que se utilizaran son `grgsm_livemon` para capturar

señales GSM, `kalibrate-uhd` para detectar las señales GSM que se encuentren en el espectro, `wireshark` para capturar los paquetes recibidos. Wireshark es necesario pues `grgsm_livemon` entrega la señal cruda, es decir devuelve una tira de bytes imposible de interpretar a simple vista.

El LiveCD de GNU-Radio en su versión `ubuntu-14.04.5-desktop-amd64-gnuradio-3.7.10.1` ya viene con varias herramientas cargadas, y una de ellas es el `grgsm_livemon` por lo que no será necesario instalarla. Instalación de Wireshark:

`sudo apt-get install wireshark` Instalación de `kalibrate-uhd`:

`git clone http://github.com/ttsou/kalibrate-uhd.git ./bootstrap ./configure make` Esto creará una carpeta llamada `src` que adentro tiene el binario `kal`. Para realizar

un escaneo ejecutaremos `./kal -s GSM850 -g 40`, esto busca frecuencias que tengan señales GSM en la banda 850MHz. Las frecuencias obtenidas se muestran en la Figura 2, allí puede verse que el canal 250 (893.6MHz) es el que tiene mayor potencia, usaremos ese para las pruebas.

Al ejecutar `grgsm_livemon` y setear la frecuencia 893.6MHz se observa el espectro de la señal y por otra parte se vé como comienzan a decodificarse los bytes recibidos.

Esos bytes recibidos pueden interpretarse mediante Wireshark, para ello lo ejecutamos con privilegios y capturamos lo que ingresa por la interfaz 127.0.0.1. Lo que se obtiene son un montón de tramas que transportan información del sistema y datos entre el usuario y la celda. Las tramas System Information Type 1 contienen datos referentes a la descripción del canal de la celda y parámetros de control RACH. Las Type 2 contienen información acerca de las celdas vecinas, PLMN permitidos y parámetros RACH. Las Type 3 tienen información de la identidad y localización de la celda, descrición del canal de control y parámetros de selección de celda. Luego están los paquetes Paging Request, que es el tráfico entre la celda y algún cliente identificado por el número TMSI, un número aleatorio que asigna la radiobase cuando algún cliente establece un enlace.

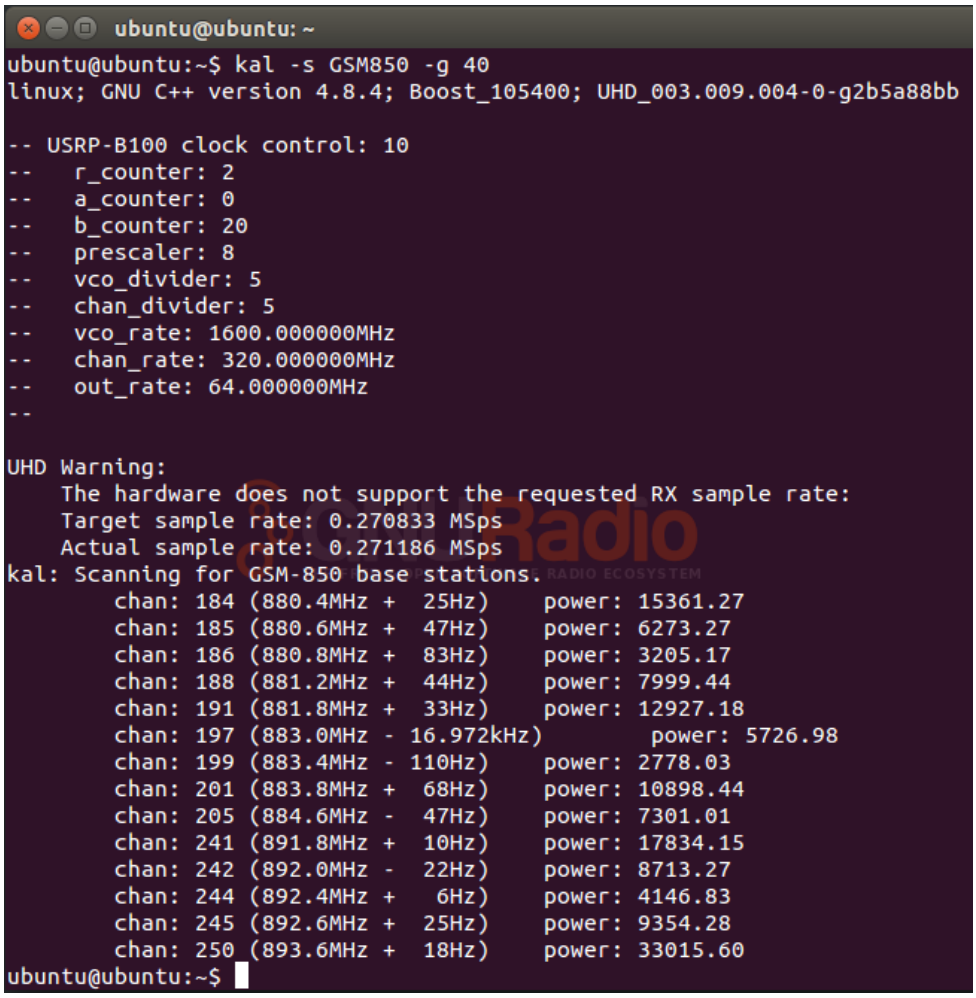


Figura 2: Bandas GSM encontradas.

Por ejemplo, en este caso puede verse que la señal corresponde a una celda de Movistar, de códigos `MCC=748`, `MNC=07`, `LAC=8311`, `CI=8837`. El sitio `http://cellidfinder.com/cells` permite saber donde se encuentra una celda a partir de estos códigos.

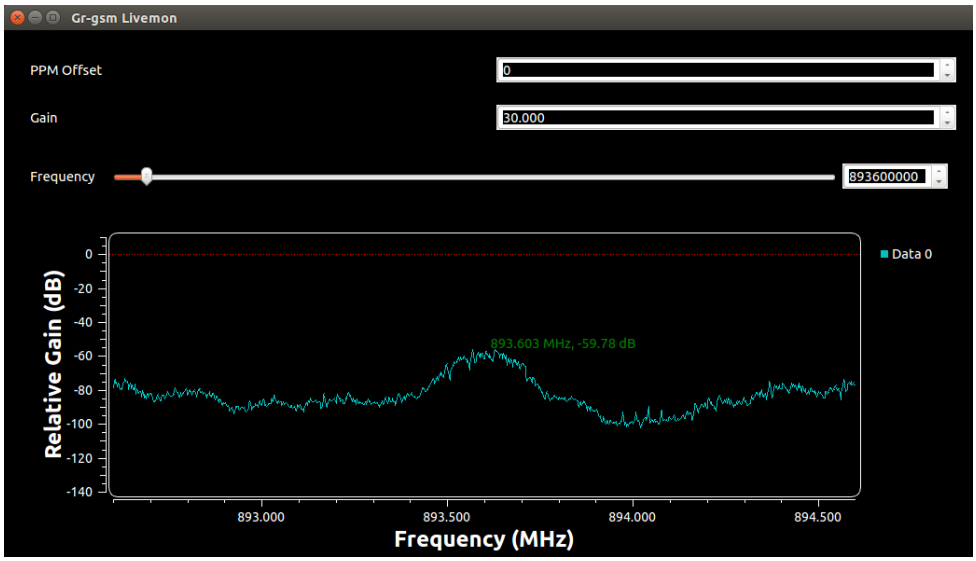


Figura 3: Espectro de la señal.

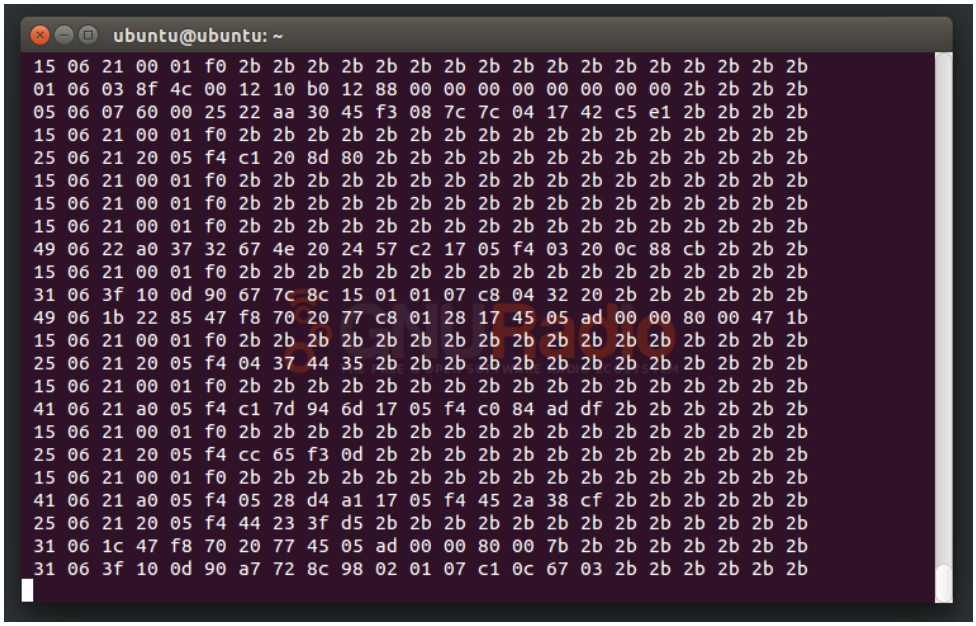
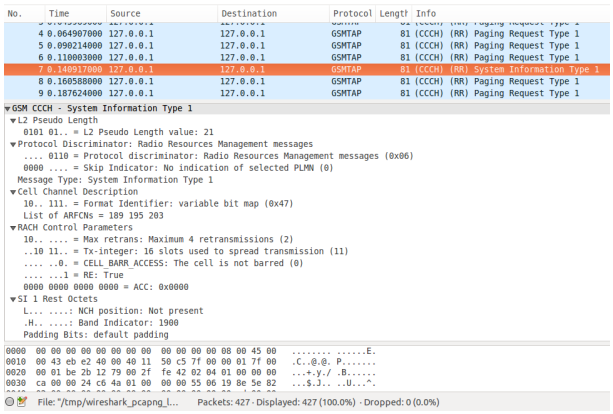


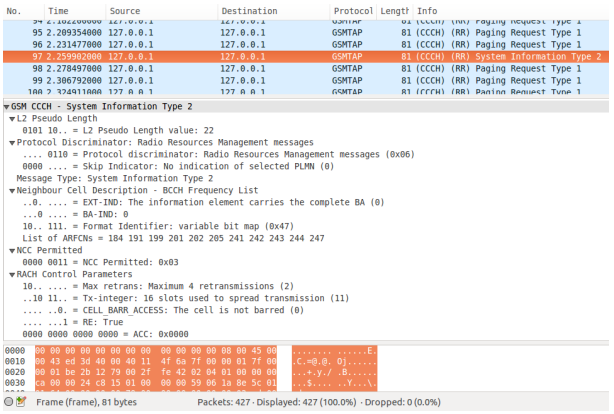
Figura 4: Captura de bytes.

2. Instalación del GSM Transceiver

Para la implementación de la celda GSM, se utilizó:
`Yate`, un motor de telefonía
`YateBTS`, una implementación de red celular GSM/GPRS basada en Yate

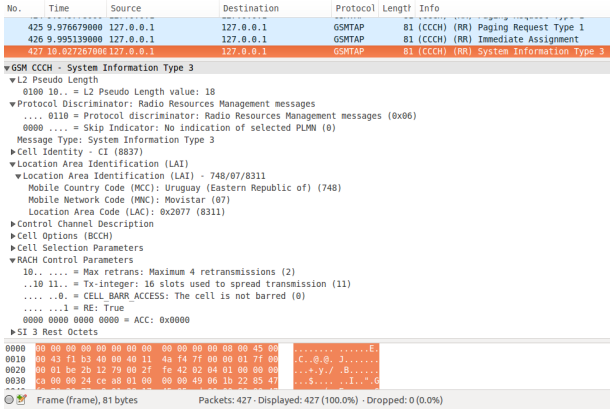


(a) System Information Type 1.

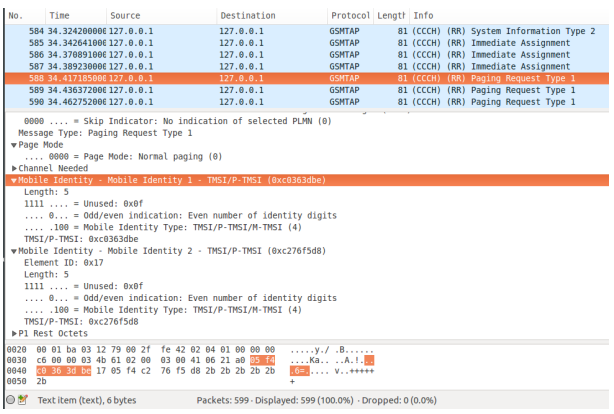


(b) System Information Type 2.

Figura 5: Tramas GSM.



(a) System Information Type 3.



(b) Paging Request Type 1.

Figura 6: Tramas GSM.

Para la interfaz web de YateBTS es necesario

`Apache HTTP Server`

`PHP 7.0`

`MySQL Server`

La instalación de Apache, PHP y MySQL se hará de forma sencilla omitiendo varios aspectos de seguridad ya que se utilizará solo a modo de probar el sistema.

Instalación de Apache:

`sudo apt-get update`

`sudo apt-get install apache2` Instalación de MySQL Server:

```
sudo apt-get install mysql-server
```

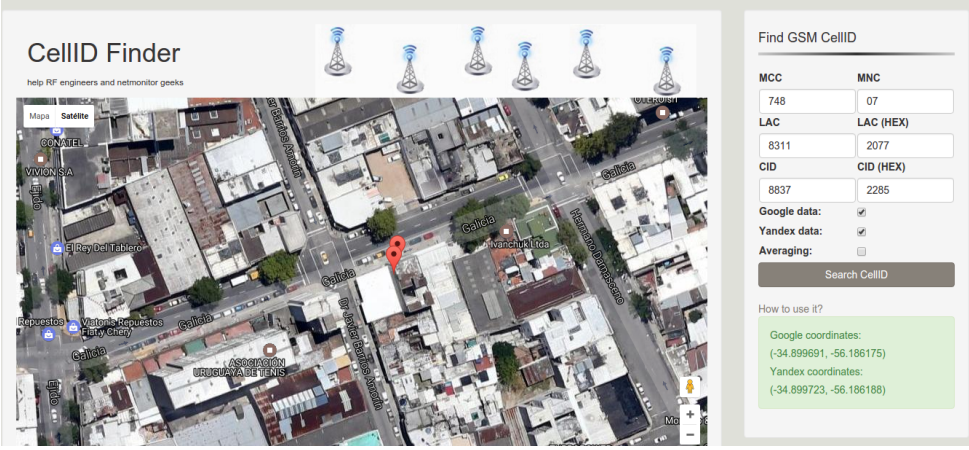


Figura 7: Ubicación de la celda.

Instalación de PHP:
Primero agregamos los repositorios para PHP7.0

```
sudo apt-add-repository ppa:andrej/php
sudo apt-get update
sudo apt-get install php libapache2-mod-php php-mcrypt php-mysql
```

Descargamos Yate y YateBTS de `https://launchpad.net/~sico/+archive/ubuntu/yate` y `http://yatebts.com/download.php`

Luego para compilar e instalar Yate:

```
cd yate
./autogen.sh
./configure --prefix=/usr/local
make -j4
sudo make install
sudo ldconfig
cd ..
```

Para YateBTS:

```
cd yatebts
./autogen.sh
./configure --prefix=/usr/local
make -j4
sudo make install
sudo ldconfig
```

Ahora creamos un link en la carpeta www del Apache a la web de YateBTS:
`cd /var/www/html/`
`sudo ln -s /usr/local/share/yate/nib_web nib` Otorgamos permisos a los archivos de configuración:
`sudo chmod -R a+w /usr/local/etc/yate` Ahora resta configurar los Virtual Hosts de Apache. Primero cambiamos los permisos para que el servidor pueda mostrar las páginas:
`sudo chmod -R 755 /var/www`

Luego creamos un nuevo archivo de Virtual Hosts:
sudo cp /etc/apache2/sites-available/000-default.conf /etc/apache2/sites-available/nib.conf
Lo editamos con nano y cambiamos el `DocumentRoot` para que levante nuestra web:

```
sudo nano /etc/apache2/sites-available/nib.conf
DocumentRoot = /var/www/nib
```

Guardamos, y habilitamos el sitio con `sudo a2ensite nib.conf`. Ahora reiniciamos el servidor con `sudo service apache2 restart` y ya se puede acceder a la web a través de `http://localhost/nib`.

En la interfaz web pueden setearse diversos parámetros, lo que interesa en este caso son la banda, la frecuencia y la potencia. El resto son parámetros de identificación de la red que pueden quedar como están. También está la posibilidad de ponerle un nombre a la red, pero no todos los teléfonos lo mostrarán. Luego en la pestaña Transceiver, se debe indicar qué imagen tiene que utilizar, en este caso por ser un USRP se elije UHD.

Ya estamos en condiciones de correr Yate con `sudo yate -s`. Si todo salió bien, se verá algo como lo que muestra la Figura 10.

Escaneando las redes disponibles con un teléfono aparece inmediatamente una red nueva llamada `00101`. Este nombre que no es el que se seteo, es la concatenación del MCC y el MNC. Sucede que por motivos de seguridad los teléfonos no muestran el nombre de red que uno establezca sino que recurren a algunos registros internos para los cuales los operadores tienen registrados sus códigos. De hecho haciendo pruebas con códigos de compañias de otros países (se utilizó el MMC=722 y MNC=341 correspondiente a la compañía Argentina Personal) se puede ver efectivamente cómo cambia el nombre automáticamente.

Al registrarse en la red el teléfono recibe un número via SMS con el que es posible enviar mensajes y realizar llamadas a otros móviles dentro de la red, con una calidad sorprendentemente buena.

Las Figuras 11(a), (b) y (c) son capturas de pantalla del teléfono que muestran todo esto.

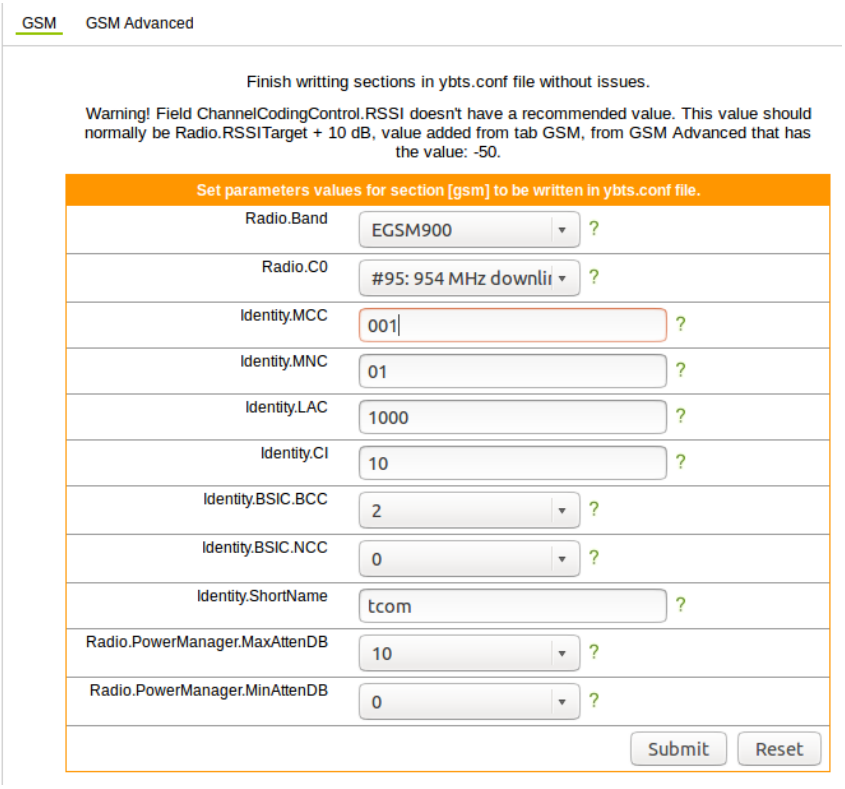


Figura 8: Interfaz web de YateBTS.

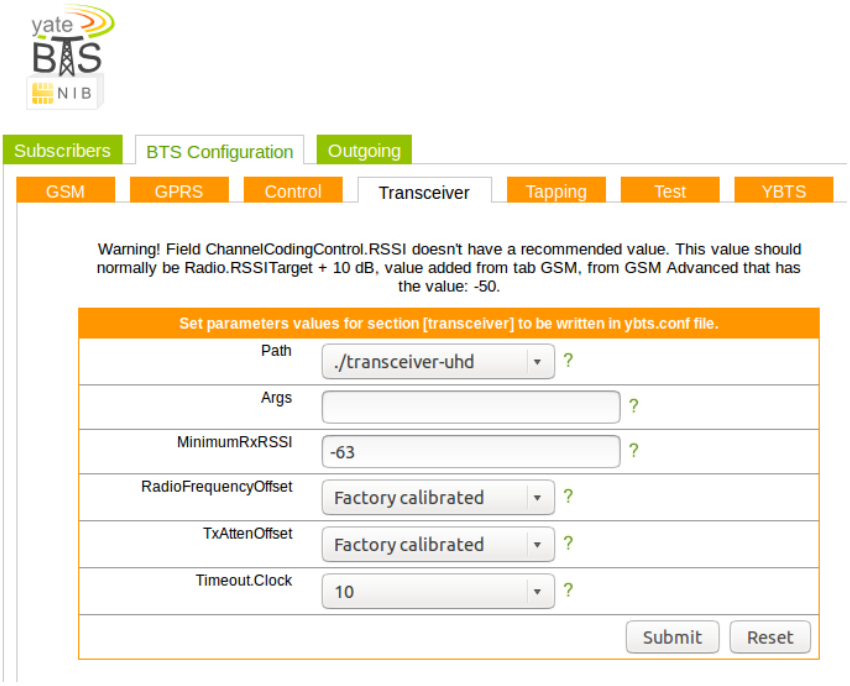
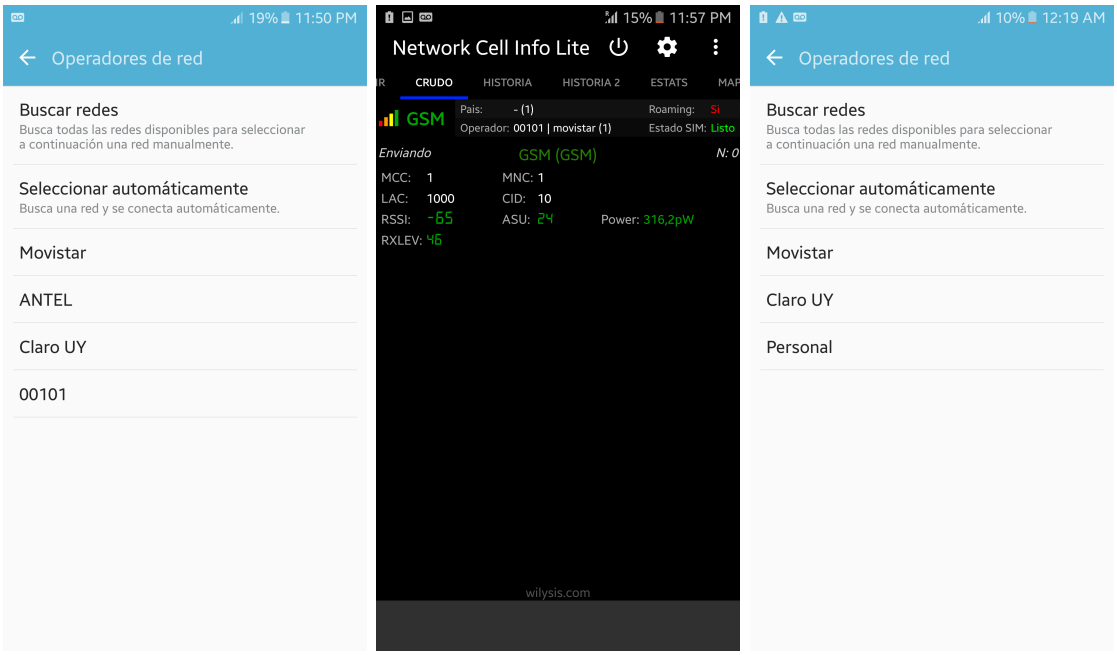


Figura 9

Figura 10



(a) (b) (c)

Figura 11: Capturas de pantalla del celular.