

MANUAL DE INSTALACIÓN

1.Instalación drivers *RTL2832U* (I)

https://ranous.files.wordpress.com/2018/02/rtl-sdr4linux_quickstartv2-18.pdf

Para instalar el dongle rtl-sdr, primero hace falta instalar una serie de paquetes:

Primero ejecutamos una actualización de la base de datos de dependencias.

```
sudo apt-get update
```

En segundo lugar, instalamos todos los paquetes necesarios.

```
sudo apt-get install git cmake build-essential python-pip libusb-1.0-0-dev
```

Los 4 primeros paquetes son paquetes necesarios para la instalación y el quinto son los drivers para dispositivos usb.

2.Instalacion de *gr-gsm* y *gnuradio*

Primero instalamos pyBOMBS que es necesario para instalar todo o demás.

```
sudo pip install PyBOMBS
```

Después configuramos pyBOMBS para ajustar la instalación.

```
pybombs auto-config
pybombs recipes add-defaults
sudo pybombs prefix init /usr/local -a default_prx -R gnuradio-
default
sudo pybombs config default_prefix default_prx
```

Finalmente construimos e instalamos *gr-gsm*.

```
sudo pybombs install gr-gsm
```

Con este comando hacemos que pyBOMBS se encargue de toda la instalación. Son 3.5 GB y se instala en /usr/local/src. Para actualizar la cache de links del sistema operativo con esa nueva librería hay que poner:

```
sudo ldconfig
```

3.Instalación drivers *RTL2832U* (II)

```
sudo git clone git://git.osmocom.org/rtl-sdr.git
cd rtl-sdr/
sudo mkdir build
```

```
cd build
sudo cmake ../ -DINSTALL_UDEV_RULES=ON
sudo make
sudo make install
sudo ldconfig
sudo cp ../rtl-sdr.rules /etc/udev/rules.d/
```

A continuación, accedemos al directorio `/etc/modprobe.d` y creamos un nuevo fichero llamado `'blacklist-rtl.conf'`.

```
cd /etc/modprobe.d
sudo nano blacklist-rtl.conf
```

Continuando, añadimos al fichero la siguiente línea:

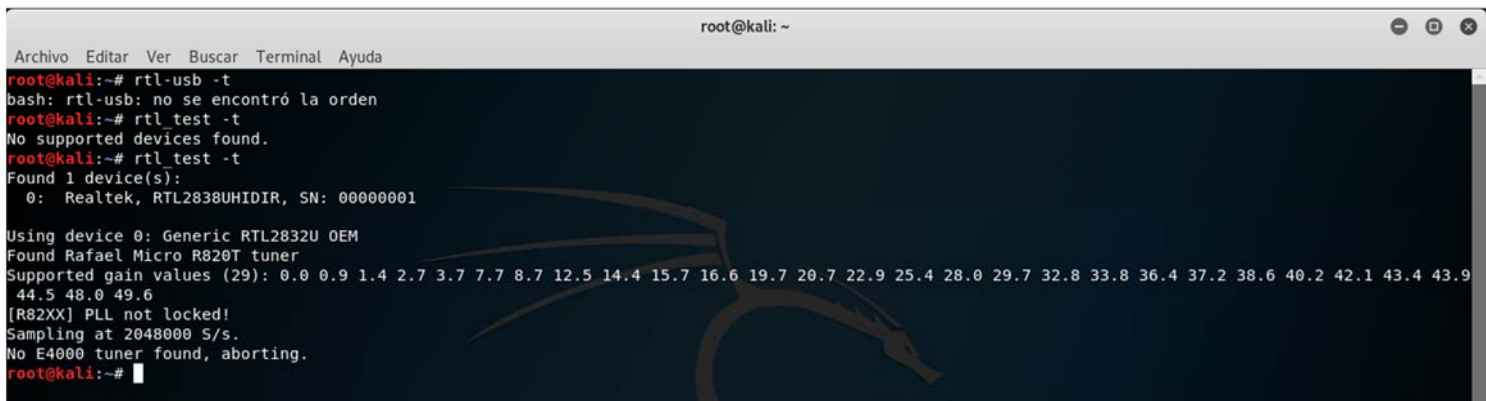
```
blacklist dvb_usb_rtl28xxu
```

Finalmente, guardamos el fichero y reiniciamos la máquina.

Para comprobar que el dongle funciona correctamente ejecutando el comando:

```
rtl_test -t
```

Deberíamos obtener:



```
root@kali: ~
Archivo Editar Ver Buscar Terminal Ayuda
root@kali:~# rtl_usb -t
bash: rtl_usb: no se encontró la orden
root@kali:~# rtl_test -t
No supported devices found.
root@kali:~# rtl_test -t
Found 1 device(s):
 0: Realtek, RTL2838UHDIDR, SN: 00000001

Using device 0: Generic RTL2832U OEM
Found Rafael Micro R820T tuner
Supported gain values (29): 0.0 0.9 1.4 2.7 3.7 7.7 8.7 12.5 14.4 15.7 16.6 19.7 20.7 22.9 25.4 28.0 29.7 32.8 33.8 36.4 37.2 38.6 40.2 42.1 43.4 43.9
44.5 48.0 49.6
[R82XX] PLL not locked!
Sampling at 2048000 S/s.
No E4000 tuner found, aborting.
root@kali:~#
```

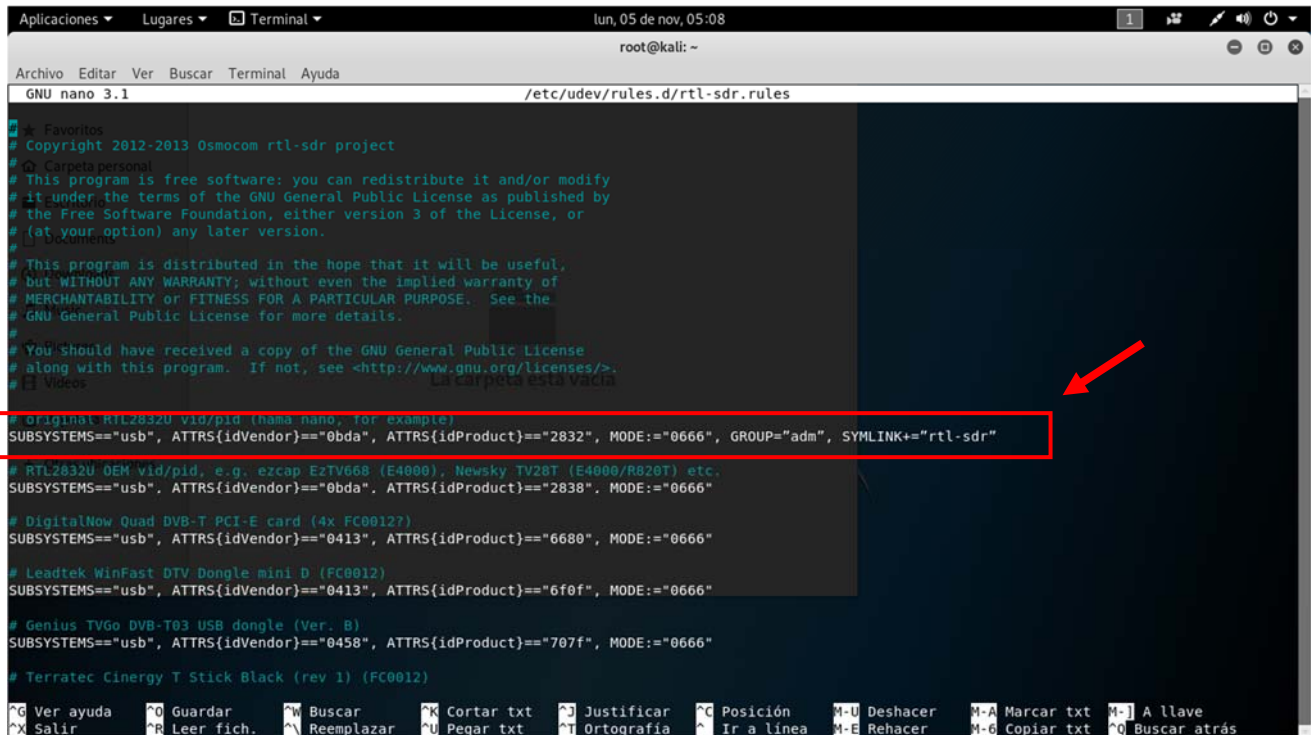
4.Modificar la siguiente regla de rtl-sdr

En el fichero `/etc/udev/rules.d/rtl-sdr.rules` debemos modificar la primera línea que no esté comentada.

Añadir al final de la línea:

, GROUP="adm", SYMLINK+="rtl-sdr"

Resultado:



```
GNU nano 3.1 /etc/udev/rules.d/rtl-sdr.rules
# Copyright 2012-2013 Osmocom rtl-sdr project
# This program is free software: you can redistribute it and/or modify
# it under the terms of the GNU General Public License as published by
# the Free Software Foundation, either version 3 of the License, or
# (at your option) any later version.
# This program is distributed in the hope that it will be useful,
# but WITHOUT ANY WARRANTY; without even the implied warranty of
# MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
# GNU General Public License for more details.
# You should have received a copy of the GNU General Public License
# along with this program. If not, see <http://www.gnu.org/licenses/>.
#
# Original RTL2832U vid/pid (nama nano, for example)
SUBSYSTEMS=="usb", ATTRS{idVendor}=="0bda", ATTRS{idProduct}=="2832", MODE=="0666", GROUP="adm", SYMLINK+="rtl-sdr"
# RTL2832U OEM vid/pid, e.g. ezcap EzTV668 (E4000), Newsky TV28T (E4000/R820T) etc.
SUBSYSTEMS=="usb", ATTRS{idVendor}=="0bda", ATTRS{idProduct}=="2838", MODE=="0666"
# DigitalNow Quad DVB-T PCI-E card (4x FC00127)
SUBSYSTEMS=="usb", ATTRS{idVendor}=="0413", ATTRS{idProduct}=="6680", MODE=="0666"
# Leadtek WinFast DTV Dongle mini D (FC0012)
SUBSYSTEMS=="usb", ATTRS{idVendor}=="0413", ATTRS{idProduct}=="6f0f", MODE=="0666"
# Genius TVGo DVB-T03 USB dongle (Ver. B)
SUBSYSTEMS=="usb", ATTRS{idVendor}=="0458", ATTRS{idProduct}=="707f", MODE=="0666"
# Terratec Cinergy T Stick Black (rev 1) (FC0012)
SUBSYSTEMS=="usb", ATTRS{idVendor}=="0413", ATTRS{idProduct}=="6f0f", MODE=="0666"
```

4.Instalación wireshark y tshark

```
sudo apt-get install wireshark tshark
```

CAPTURAS

1.Escanear frecuencias gsm

Ejecutar el comando:

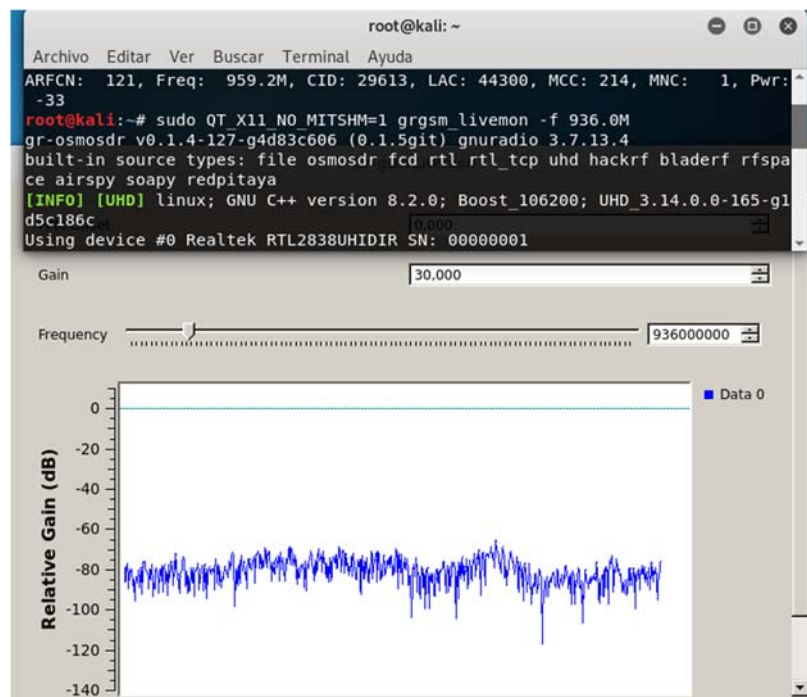
```
sudo grgsm_scanner
```

```
bash: grgsm_scanner: no se encontró el orden
root@kali:~# grgsm_scanner
ARFCN: 989, Freq: 928.0M, CID: 19, LAC: 16186, MCC: 214, MNC: 3, Pwr: -35
ARFCN: 992, Freq: 928.6M, CID: 74, LAC: 16186, MCC: 214, MNC: 3, Pwr: -35
ARFCN: 4, Freq: 935.8M, CID: 1522, LAC: 3109, MCC: 214, MNC: 7, Pwr: -37
ARFCN: 5, Freq: 936.0M, CID: 0, LAC: 3109, MCC: 214, MNC: 7, Pwr: -43
ARFCN: 21, Freq: 939.2M, CID: 2692, LAC: 3109, MCC: 214, MNC: 7, Pwr: -42
ARFCN: 100, Freq: 955.0M, CID: 15495, LAC: 44300, MCC: 214, MNC: 1, Pwr: -41
ARFCN: 102, Freq: 955.4M, CID: 15494, LAC: 44300, MCC: 214, MNC: 1, Pwr: -35
ARFCN: 106, Freq: 956.2M, CID: 29957, LAC: 44300, MCC: 214, MNC: 1, Pwr: -33
ARFCN: 109, Freq: 956.8M, CID: 30593, LAC: 44300, MCC: 214, MNC: 1, Pwr: -43
ARFCN: 112, Freq: 957.4M, CID: 0, LAC: 44300, MCC: 214, MNC: 1, Pwr: -33
ARFCN: 115, Freq: 958.0M, CID: 0, LAC: 44300, MCC: 214, MNC: 1, Pwr: -33
ARFCN: 116, Freq: 958.2M, CID: 33659, LAC: 44300, MCC: 214, MNC: 1, Pwr: -45
ARFCN: 121, Freq: 959.2M, CID: 29613, LAC: 44300, MCC: 214, MNC: 1, Pwr: -33
```

2.Mostrar gráfico y establecer frecuencia

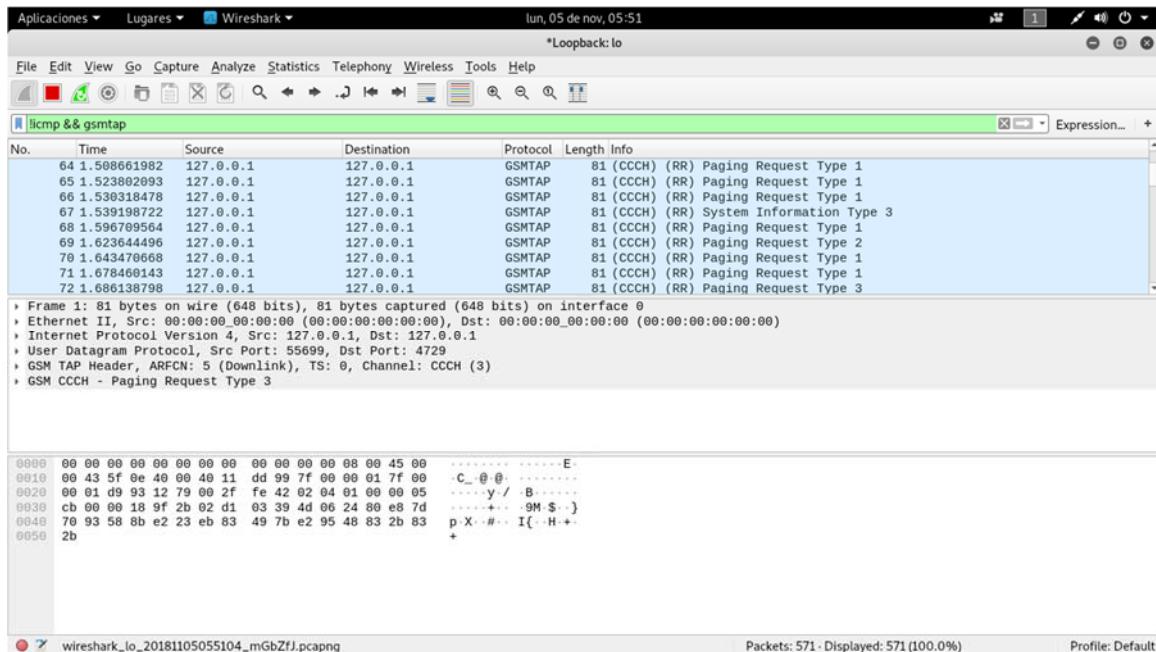
Ejecutar el comando:

```
sudo QT_X11_NO_MITSHM=1 grgsm_livemon -f frecuenciaAEscanear
```



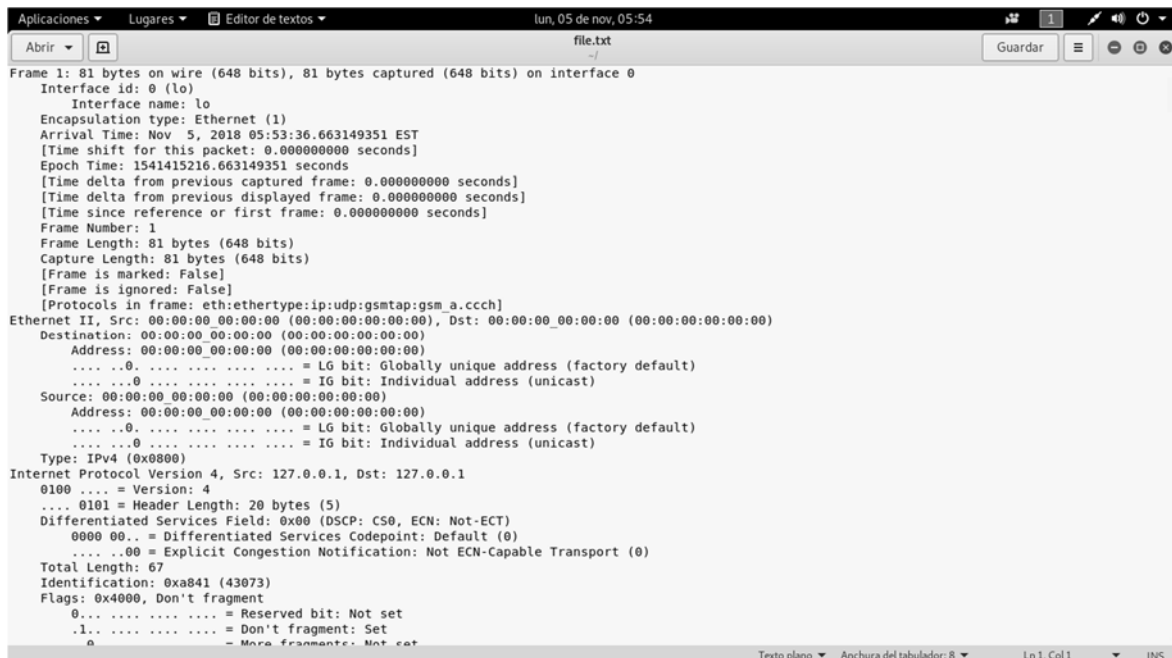
3. Visualizar tramas en Wireshark

```
sudo wireshark -k -Y '!icmp && gsmtap' -i lo
```



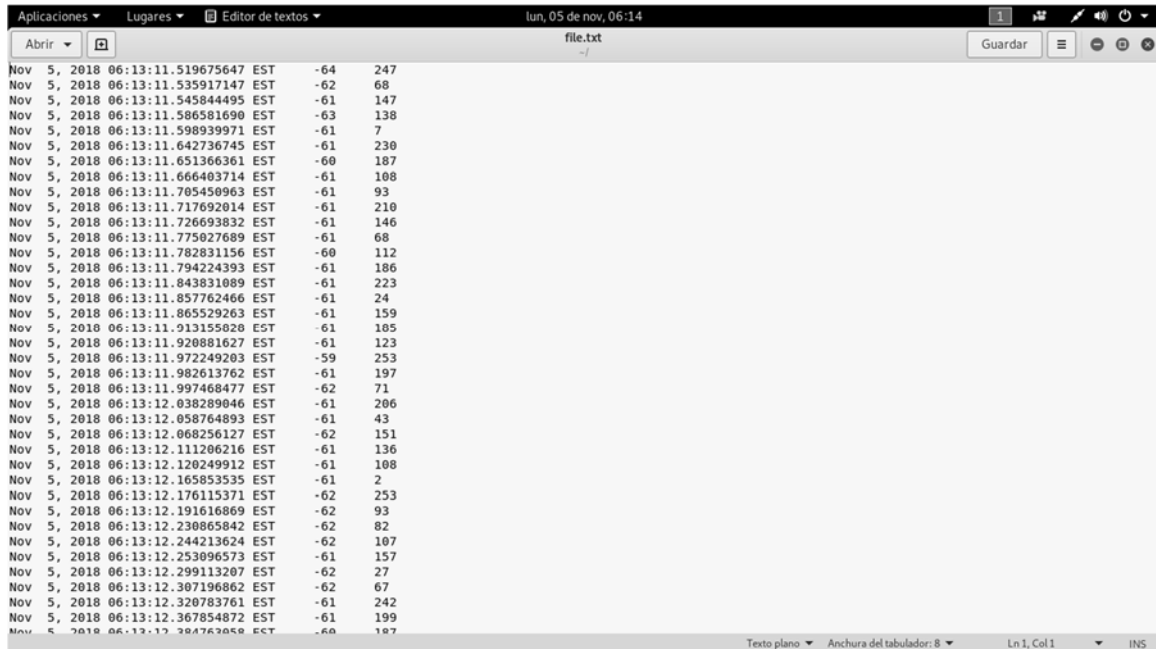
4. Exportar capturas a un fichero de texto

```
tshark -i lo -Y 'gsmtap && gsm_a.ccch' -c 1000 -V -T text > file.txt
```



5.Exportar los campos que nos interesan a un fichero de texto

```
tshark -i lo -Y 'gsmtap && gsm_a.ccch' -c 1000 -V -T fields -e  
frame.time -e gsmtap.signal_dbm -e gsmtap.antenna -e e212.imsi >  
file.txt
```



Nov 5, 2018 06:13:11.519675647	EST	-64	247
Nov 5, 2018 06:13:11.535917147	EST	-62	68
Nov 5, 2018 06:13:11.545844495	EST	-61	147
Nov 5, 2018 06:13:11.586581690	EST	-63	138
Nov 5, 2018 06:13:11.598939971	EST	-61	7
Nov 5, 2018 06:13:11.642736745	EST	-61	230
Nov 5, 2018 06:13:11.651366361	EST	-60	187
Nov 5, 2018 06:13:11.666403714	EST	-61	108
Nov 5, 2018 06:13:11.705450963	EST	-61	93
Nov 5, 2018 06:13:11.717692014	EST	-61	210
Nov 5, 2018 06:13:11.726693832	EST	-61	146
Nov 5, 2018 06:13:11.775027689	EST	-61	68
Nov 5, 2018 06:13:11.782831156	EST	-60	112
Nov 5, 2018 06:13:11.794224393	EST	-61	186
Nov 5, 2018 06:13:11.843831089	EST	-61	223
Nov 5, 2018 06:13:11.857762466	EST	-61	24
Nov 5, 2018 06:13:11.865529263	EST	-61	159
Nov 5, 2018 06:13:11.913155828	EST	-61	185
Nov 5, 2018 06:13:11.920881627	EST	-61	123
Nov 5, 2018 06:13:11.972249203	EST	-59	253
Nov 5, 2018 06:13:11.982613762	EST	-61	197
Nov 5, 2018 06:13:11.997468477	EST	-62	71
Nov 5, 2018 06:13:12.038289046	EST	-61	206
Nov 5, 2018 06:13:12.058764893	EST	-61	43
Nov 5, 2018 06:13:12.068256127	EST	-62	151
Nov 5, 2018 06:13:12.111206216	EST	-61	136
Nov 5, 2018 06:13:12.120249912	EST	-61	108
Nov 5, 2018 06:13:12.165853535	EST	-61	2
Nov 5, 2018 06:13:12.176115371	EST	-62	253
Nov 5, 2018 06:13:12.191616869	EST	-62	93
Nov 5, 2018 06:13:12.230865842	EST	-62	82
Nov 5, 2018 06:13:12.244213624	EST	-62	107
Nov 5, 2018 06:13:12.253096573	EST	-61	157
Nov 5, 2018 06:13:12.299113207	EST	-62	27
Nov 5, 2018 06:13:12.307196862	EST	-62	67
Nov 5, 2018 06:13:12.320783761	EST	-61	242
Nov 5, 2018 06:13:12.367854872	EST	-61	199
Nov 5, 2018 06:13:12.384763059	EST	-60	187

VERSIONES

Sistema operativo:

SMP Debian 4.18.10-2kali1 (2018-10-09)

PyBOMBS:

2.3.3

Gnuradio:

3.7.13.4

GNU C++:

8.2.0

Basado en el manual v2 de Miryam Subiza Erro