Implementación de un modelo de medición de señales GSM mediante SDR

Edgar Alexander Sánchez Galindo
Juan Camilo Vargas Cepeda
Maykoll Chamorro Tovar

Universitaria Agustiniana
Facultad De Ingenierías
Programa De Ingeniería en Telecomunicaciones
Bogotá D.C
2018

Implementación de un modelo de medición de señales GSM mediante SDR

Edgar Alexander Sánchez Galindo
Juan Camilo Vargas Cepeda
Maykoll Chamorro Tovar

Director
Félix Roberto Gómez Devia

Trabajo de grado para optar al título de Ingeniero en Telecomunicaciones

Universitaria Agustiniana
Facultad De Ingenierías
Programa De Ingeniería en Telecomunicaciones
Bogotá D.C
2018

Resumen

El presente trabajo de investigación consiste en la implementación de un modelo de medición de señales Global System for Mobile Communications (GSM) mediante un Software Defined Radio (SDR), el cual brinda a los estudiantes de la Universitaria Agustiniana una alternativa práctica para el conocimiento y funcionamiento de las diferentes características que hacen parte de la señal GSM con la ayuda de SDR (HackRf One) y aplicaciones de software libre como GNU Radio y Wireshark. Para esto, se establecen las principales características de la señal GSM que se pueden medir con el SDR, determinando los requisitos de software, hardware y bloques de GNU Radio necesarios para su desarrollo. A fin de comprobar la efectividad del modelo de medición implementado, se exponen los resultados obtenidos, entre los cuales destacan elementos como las bandas de frecuencias asignadas para esta tecnología, el acceso a canal aleatorio (RACH), la asignación inmediata sobre el canal de control común (CCCH), Números de Canal de Radio Frecuencia absoluta (ARFCN), entre otros parámetros que proporcionan una base para el desarrollo de alternativas prácticas para el conocimiento y comprensión de las comunicaciones móviles.

Palabras Clave: Señal GSM, canales GSM, GNU Radio, SDR y Wireshark.

Abstract

The present research work consists of the implementation of a signal management model Global System for Mobile Communications (GSM) through a Software Defined Radio (SDR), which provides information to the students of the Universidad Agustiniana a practical alternative for the knowledge and functioning of the different.

features that are part of the GSM signal with the help of SDR (HackRf One) and free software applications such as GNU Radio and Wireshark. For this, the main characteristics of the GSM signal that can be measured with the SDR are established, determining the software, hardware and GNU Radio blocks requirements necessary for its development. In order to verify the effectiveness of the measurement model implemented, the results obtained are exposed, among which elements such as the frequency bands assigned for this technology, access to the random channel (RACH), the immediate assignment over the control channel stand out. common (CCCH), Absolute Radio Frequency Channel Numbers (ARFCN), among other parameters that provide a basis for the development of practical alternatives for knowledge and understanding of mobile communications. Keywords: GSM signal, GSM channels, GNU Radio, SDR and Wireshark.

Tabla de contenido

1. Introducción 11
2. Planteamiento del problema 12
3. Justificación 13
4. Objetivos 14
   4.1. Objetivo general 14
   4.2. Objetivos específicos 14
5. Marco referencial 15
   5.1. Marco teórico 15
   5.2. Marco conceptual 17
      5.2.1. Espectro electromagnético. 17
      5.2.2. Comunicaciones digitales. 17
      5.2.3. Comunicaciones móviles. 18
      5.2.4. Generaciones de las comunicaciones móviles. 18
      5.2.5. Tecnología GSM. 19
      5.2.6. Evolución de GSM. 20
      5.2.7. Estaciones base (BTS). 20
      5.2.8. Interfaz Um. 20
      5.2.9. Bandas de frecuencia GSM. 20
      5.2.10. ARFCN. 21
      5.2.11. Canales Físicos. 21
      5.2.12. Canales lógicos. 22
      5.2.13. Canales de tráfico (TCH). 22
      5.2.14. Canales de control (CCH). 23
      5.2.15. Acceso múltiple por división de frecuencia (FDMA). 24
      5.2.16. Acceso múltiple por división de tiempo (TDMA). 24
      5.2.17. Acceso múltiple por división de código (CDMA). 25
      5.2.18. Modulación GMSK. 25
      5.2.19. Radio definido por software (SDR). 26
      5.2.20. Protocolo GSMTAP. 26
      5.2.21. Importancia de la señal GSM. 26
      5.2.22. GSM en Colombia. 26
   5.3. Marco legal 27
6. Metodología 29

6.1. Enfoque metodológico 29
7. Administración del proyecto 30
7.1. Cronograma 30
7.2. Presupuesto 30
7.2.1. Presupuesto de recursos humanos. 30
7.2.2. Presupuesto de equipos. 31
7.2.3. Presupuesto de software. 31
7.2.4. Presupuesto de materiales y suministros. 31
7.2.5. Presupuesto de material bibliográfico. 31
7.2.6. Presupuesto general. 32
8. Desarrollo del proyecto 33
8.1. Principales características de la señal GSM que se son posibles de medir a través del SDR 33
8.1.1. Canales lógicos 33
8.1.2. Canales de tráfico. 33
8.1.3. Canales de radiodifusión (BCH – Broadcast Channels). 34
8.1.4. Canales de control dedicados (DCCH – Dedicated Control Channels). 34
8.1.5. Canales comunes de control (CCCH – Common Control Channels). 35
8.1.6. Parámetros de la telefonía celular. 35
8.1.7. Características generales GSM. 37
8.2. Requisitos de hardware y software necesarios para obtener los parámetros de la señal GSM 38
8.2.1. Software. 38
8.2.2. Ubuntu. 39
8.2.3. Kalibrate. 40
8.2.4. GQRX 41
8.2.5. GNU Radio. 42
8.2.6. GR-GSM. 43
8.2.7. Wireshark. 43
8.2.8. Hardware. 45
8.2.9. SDR - HackRF one (software definido por radio). 45
8.2.10. Antena ANT500. 46
8.3. Necesidades de configuración del SDR que responda a los requisitos de hardware y software que permita medir la señal GSM. 47

8.3.1. Librerías y paquetes. 48
8.3.2. Comandos utilizados. 48
8.3.3. Captura, decodificación y parámetros de la señal GSM. 50
8.4. medición y análisis de los parámetros de la señal GSM a través de SDR. 55
8.4.1. Inmediate assignment (Asignación inmediata) CCCH. 57
8.4.2. Paging request type 1 (Solicitud de paginación Tipo 1). 58
8.4.3. System information type 3 (Sistema de información tipo 3): 59
8.4.4. System information type 4 (Sistema de información tipo 4). 60
8.4.5. Tabla de parámetros. 61
Conclusiones 65
Recomendaciones 66
Referencias 67
Anexos 69

Lista de tablas

Tabla 1. Bandas de frecuencia GSM. 21
Tabla 2. Canales de tráfico TCH. 23
Tabla 3. Canales de control en GSM. 23
Tabla 4. Cronograma proyecto. 30
Tabla 5. Presupuesto de equipos. 30
Tabla 6. Presupuesto de Equipos. 31
Tabla 7. Presupuesto de software. 31
Tabla 8. Presupuesto de materiales y suministros. 31
Tabla 9. Presupuesto de material bibliográfico. 31
Tabla 10. Presupuesto Final. 32
Tabla 11. IMSI Colombia. 35
Tabla 12. ARFCN de las bandas de frecuencia. 36
Tabla 13. Características Generales GSM. 37
Tabla 14. Requisitos de hardware y software. 38
Tabla 15. Características computador. 45
Tabla 16. Características técnicas. 46
Tabla 17. Esquema para obtener parámetros. 47
Tabla 18. Comandos. 48
Tabla 19. Cuadro de Mediciones. 56
Tabla 20. Parametros Wireschark 61

Lista de figuras

Figura 1. División del espectro electromagnético. 17
Figura 2. Diagrama de bloques de un sistema de comunicaciones digitales. 18
Figura 3. Sistema de comunicaciones móviles por celdas. 18
Figura 4. Generaciones y servicios de las comunicaciones móviles. 19
Figura 5. Esquema general de una red GSM. 19
Figura 6. Evolución GSM. 20
Figura 7. Estaciones móviles 20
Figura 8. Esquema de acceso al medio GSM 22
Figura 9. Esquema canales lógicos. 22
Figura 10. FDMA. 24
Figura 11. TDMA. 25
Figura 12. CDMA. 25
Figura 13. Modulación GMSK 26
Figura 14. Diagrama de sistemas definidos por software. 26
Figura 15. Asignación de bandas de frecuencia GSM por operador en Colombia. 27
Figura 16. Canales GSM. 33
Figura 17. MCC y MNC Colombia. 36
Figura 18. Cell Id. 36
Figura 19. Timing advance. 37
Figura 20. Arquitectura implementada. 40
Figura 21. Escáner de frecuencias 41
Figura 22. Gqrx frecuencia exacta. 42
Figura 23. Programa GNURadio. 43
Figura 24. Gr-gsm para la decodificación de las tramas 43
Figura 25. Wireshark 44
Figura 26. Protocolo GSMTAP con Wireshark. 45
Figura 27. SDR-HackRF one. 46
Figura 28. Antena ANT500 46
Figura 29. Implementación HackRF One. 47
Figura 30. Escanear canales. 50
Figura 31. Canales encontrados. 50
Figura 32. Programa Gqrx. 50
Figura 33. Configure. 51

Figura 34. Configuración Gqrx. 51
Figura 35. Configuración frecuencia.. 52
Figura 36. Muestra de espectro.. 53
Figura 37. Comando GNURadio.. 53
Figura 38. Bloques GNURadio.. 54
Figura 39. Frecuencia Gr-gsm.. 54
Figura 40. Gr-gsm decodificación de las tramas.. 55
Figura 41. Wireshark parámetros y decodificación.. 55
Figura 42. Instalaciones Uniagustiniana.. 56
Figura 43. Trama de información. 56
Figura 44. Canal CCCH.. 58
Figura 45. Paging request. 59
Figura 46. System information type 3.. 60
Figura 47. System information type 4. 61
Figura 48. Mediciones realizadas en la semana de la Ingeniera Uniagustiniana.. 64

1. Introducción

El presente trabajo de investigación comprende el diseño y la implementación de un modelo de medición de señales GSM utilizando un Software Definido por Radio (SDR) con el fin de tomar tramas que se transportan sobre esa red y determinar las características básicas de esta. Esto con el fin de evidenciar a detalle los múltiples componentes que hacen parte de esta señal como los canales que utiliza, las frecuencias en la que opera y algunas de las interfaces más importantes.

Para esto, es necesario investigar cuales son los parámetros que se pueden obtener con el equipo SDR pertenecientes a la red GSM, junto con sus requerimientos a nivel de hardware y software para lograr el resultado. Mediante el desarrollo de este, se dará la facilidad de evidenciar características que permitan la comprensión de los términos asociados a las comunicaciones inalámbricas debido a la carencia de elementos o dispositivos que brindan esta posibilidad.

Para abordar la problemática, se utiliza el software de código libre GNU Radio debido a sus características y herramientas para realizar el tratado de la señal y obtener los datos necesarios para realizar la decodificación de los mismos, sumado al analizador de protocolos Wireshark que permitirá observar y analizar las tramas obtenidas y mostrar las características más importantes de la señal.

El modelo de medición consiste en realizar un censo o escaneo, para determinar cuáles son los canales que se encuentran a disposición al momento de utilizar el sistema con el fin de determinar con el analizador de espectro dónde se encuentra el tráfico más pesado de esta señal para posteriormente capturar las tramas y paquetes que contienen las características fundamentales de la señal GSM.

2. Planteamiento del problema

Actualmente la Universitaria Agustiniana en el plan de estudios de su programa Ingeniería en Telecomunicaciones cuenta con las asignaturas de comunicaciones móviles y sistemas inalámbricos, las cuales dedican una parte al conocimiento y funcionamiento de la señal GSM, en vista de que este ha sido un pilar fundamental para la evolución que han tenido las redes móviles en el último tiempo.

Este conocimiento se está impartiendo principalmente de forma teórica debido a la falta de prácticas con diferentes métodos que permitan a los estudiantes comprender, apropiar y profundizar los conocimientos adquiridos en este tema. En cierta parte también se debe a que la universidad no cuenta con equipos o dispositivos específicos en el conocimiento de la señal GSM. Por lo que es necesario examinar de qué manera es posible aprovechar ciertos dispositivos como el Radio Definido por Software (SDR), el cual cuenta con una variedad de funciones que pueden aplicarse para la identificación de criterios y características de la señal GSM. Lo que permitirá al estudiante adquirir competencias necesarias para desarrollar en la futura vida profesional.

Teniendo en cuenta lo anterior, surge la siguiente pregunta de investigación ¿Cómo se podría implementar un modelo de medición de los diferentes parámetros y características que hacen parte de una señal GSM mediante SDR?

3. Justificación

En la formación profesional del estudiante de ingeniería en Telecomunicaciones es importante desarrollar competencias en el campo de las redes móviles dado que son de suma importancia, según el estudio del primer trimestre de 2018 del MINTIC. En el primer trimestre de 2018, en Colombia se cuenta con 62’822.720 abonados a telefonía móvil y este periodo presenta un incremento de un poco más de 600.000 abonados con relación al último trimestre de 2017. Lo que indica que en la actualidad hay un incremento del 1% de abonados que hacen uso de esta tecnología.

Por tal razón el presente trabajo investigativo, busca que los estudiantes por medio de la implementación de un modelo de medición de señales GSM, mediante el desarrollo de prácticas de laboratorio con el uso del Radio Definido por Software (SDR), puedan comprender, afianzar y aplicar los conocimientos teóricos adquiridos en los cursos de comunicaciones móviles y sistemas inalámbricos. De igual forma, se busca que a través del estudio de la señal GSM los estudiantes puedan desarrollar habilidades y competencias necesarias para un buen desempeño profesional.

4. Objetivos

4.1. Objetivo general

Implementar un modelo de medición de parámetros de la señal GSM a través de prácticas de laboratorio mediante SDR.

4.2. Objetivos específicos

- Identificar las principales características de la señal GSM que se son posibles de medir a través del SDR.
- Establecer los requisitos de hardware y software necesarios para obtener los parámetros de la señal GSM.
- Determinar las necesidades de configuración del SDR que responda a los requisitos de hardware y software necesarios para medir la señal GSM.
- Realizar medición y análisis de los parámetros de la señal GSM a través de SDR.

5. Marco referencial

5.1. Marco teórico

A continuación, Se observan los planteamientos de diferentes autores referentes a GSM y SDR.

> Con respecto a SDR, Pino S., (Arguello H., 2013) hablan de la importancia de este dispositivo en la implementación de un modelo de comunicaciones y diseño de bancos de pruebas, mediante el procesamiento de señales y la separación de algoritmos. Con este estudio, es posible lograr el diseño de un banco de pruebas con el cual es posible dar solución a algunos problemas de sincronismo. El uso de plataformas de hardware y bancos de pruebas inalámbricos de comunicaciones toma el rol de validar las ganancias en el rendimiento consolidado en la teoría y en las simulaciones. En SDR, el desplazamiento de frecuencia convencional de la señal en el hardware de modulación, se reemplaza por un proceso de dos pasos que convierte la señal modulada digital de banda base en una señal analógica de banda de paso irradiada mediante la implementación de un sistema flexible utilizando de manera óptima dicha arquitectura, permite al usuario el acceso a un banco de pruebas SDR con el fin de que los investigadores al validar las teorías no tengan que diseñar completamente un banco de pruebas. Teniendo en cuenta los resultados obtenidos en mediciones inalámbricas de interiores, se evidencio que la operación del sistema se encuentre entre los 1 y 2 dB, ya que se encuentran por debajo de los 10dB muestra la efectividad de éste con respecto a la relación Señal a Ruido.

Por otra parte, en la investigación de Gaona E., Ávila M., Muskus G., (2014) se evidencian los resultados en una solución ofrecida para la calidad de voz en la rápida acción de desastres o emergencias, utilizando la conexión de diferentes tipos de terminales móviles comunes con los protocolos de la red GSM en la banda DSC-1800, y USRP, sumado con un sistema de voz IP.

En relación a GSM, (Bhatta A., Kumar A., 2015) mencionan como es el funcionamiento del protocolo de esta señal, el cual utiliza TDMA (Acceso múltiple por división de tiempo) y FDMA (Acceso múltiple por división de frecuencia) como técnicas de multiplexación con el fin de aprovechar al máximo las bandas de frecuencias asignadas a esta señal.

Así mismo (Gbadamosi S., Aibinu A., 2014) demuestran que es posible estimar la tasa de error de bit (BER) a través de un Radio Definido por Software (SDR) y la modulación de una portadora VHF la cual está modulada con codificación de cambio de frecuencia gaussiana GFSK.

> También, (Alcantú Y., 2015): explica las concepciones claves para realizar la decodificación de sincronismo de la interfaz de radio GSM, ya que los sistemas inalámbricos deben enfrentarse a múltiples percances en su transmisión. El objetivo de éste, es darle solución al proceso de sincronización de un analizador de protocolos de la capa física descritos en las normas GSM,

mediante la utilización del sistema SDR y la identificación de celdas de cobertura para los dispositivos móviles, realizando captura de datos en esta red con el fin de analizarlos de manera exhaustiva. Con esta investigación se posibilitó el primer diseño de un esquema que posibilita la decodificación del canal del sincronismo, mediante la demultiplexación en el estándar TDMA y la decodificación por análisis funcional, proyectando lograr la implementación de esta investigación en un sistema capaz de decodificar el canal del sincronismo para obtener el código de la estación base (BSIC) y el número de tramas (FN).

Además Machado J. (2015), menciona cómo es posible usar el SDR para dar soluciones de bajo costo que al combinarse con software gratuito para facilitar el examen del espectro, y de esta forma dar solución a problemas como detección de interferencias, asignación de distribuciones de frecuencias de manera eficiente, prueba de la operación de sistemas de repetidores y medición de sus parámetros eléctricos, identificación de intrusos del espectro y caracterización del ruido por bandas y regiones del mundo.

De igual forma Sastoque M., Puerto G.,Suarez G. (2017), Recalcan la importancia que está teniendo el concepto de Software Definido por Radio (SDR) gracias a aspectos como su adaptabilidad, interoperabilidad convergencia y la forma como se pueden implementar funcionalidades de acceso dinámico al espectro. Así mismo mencionan lo que el manejo del SDR permite, tales como su operación en diferentes estándares multibanda teniendo en cuenta que su procesamiento es digital en lugar de analógico.

Recientemente (Aggrawal K., Kamani M., Vachhani K., 2017). Muestran como con la ayuda de aplicaciones como GNU Radio, Wireshark y el dispositivo RTL-SDR; Se puede acceder a ciertos parámetros que hacen parte de la señal GSM como el protocolo de acceso a enlaces sobre el canal Dm (LAPDm), seguido de cómo se establece la capa RR, que incluye: acceso inicial sobre el canal de acceso aleatorio (RACH), activación del canal sobre la estación transceptora base (BTS), asignación inmediata sobre el canal de control común (CCCH) y establecimiento de conexión LAPDm.

5.2. Marco conceptual

5.2.1. Espectro electromagnético.

Se denomina espectro electromagnético a la distribución energética del conjunto de las ondas electromagnéticas. Así, el espectro electromagnético es una representación de todas las radiaciones de origen electromagnético que existen en la naturaleza, ordenadas según su frecuencia o su longitud de onda. Por convivencia se divide el espectro en varias regiones atendiendo a sus frecuencias (bandas de frecuencias), como se ilustra en la figura 1. (Huidobro, J. 2015).

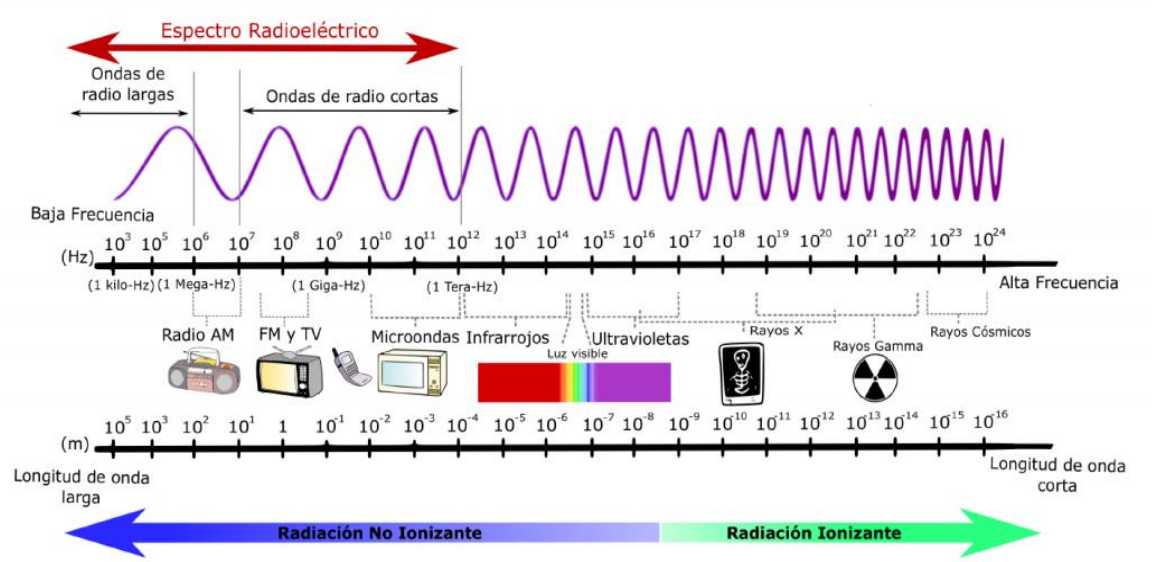


Figura 1. *División del espectro electromagnético. (Esopo 2016).*

5.2.2. Comunicaciones digitales.

Según Artes, A. et-al, (2012), las comunicaciones digitales, se refieren al proceso de conversión de un voltaje en unos y ceros que se distorsionan en el canal al momento de su transmisión, las cuales, por su carácter discreto, pueden ser reconstruidas en el destino, basados en el funcionamiento general de las comunicaciones digitales evidenciados en la figura 2.

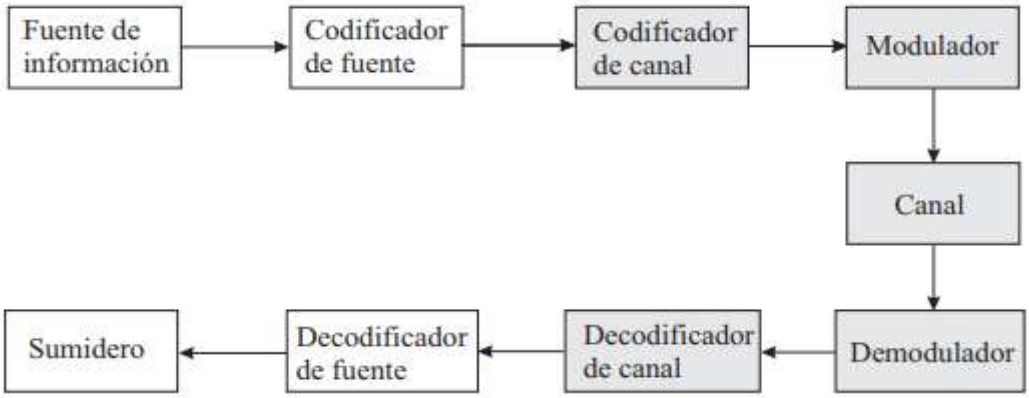


Figura 2. *Diagrama de bloques de un sistema de comunicaciones digitales. (Artes, A, et-al;2012).*

5.2.3. Comunicaciones móviles.

Como explica Rábanos, J. (2004), son servicios de radiocomunicaciones que se establecen entre diferentes tipos de estaciones, ya sean dos estaciones móviles o una fija y una móvil, y se clasifican según el entorno donde se desarrolle dicha comunicación. en la figura 3 se muestra el modelo actual de las comunicaciones móviles mediante celdas o células.

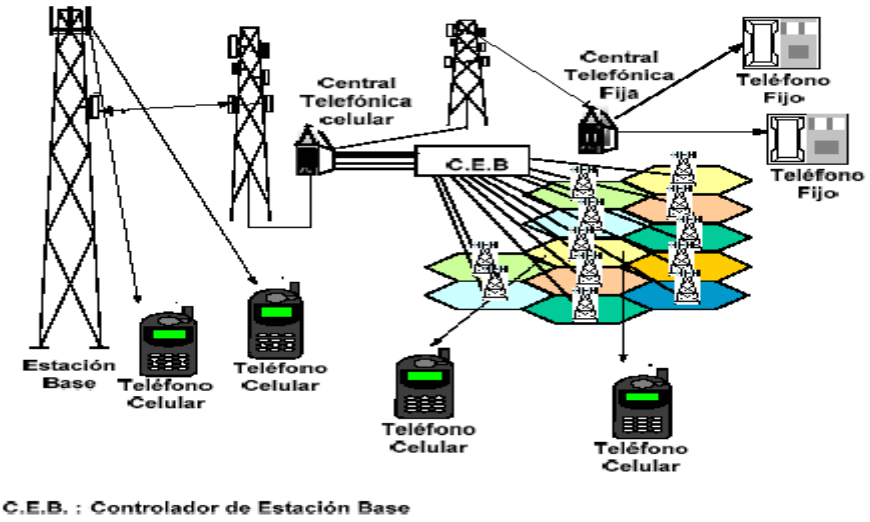


Figura 3. *Sistema de comunicaciones móviles por celdas. (Tispain , 2015).*

5.2.4. Generaciones de las comunicaciones móviles.

Huidobro, J. (2012), define las generaciones móviles, como los sistemas utilizados que evolucionan constantemente que se relacionan más que todo con las técnicas de acceso múltiple que permitan la eficiencia y calidad. cómo se evidencia en la figura 4, con la evolución de las generaciones.

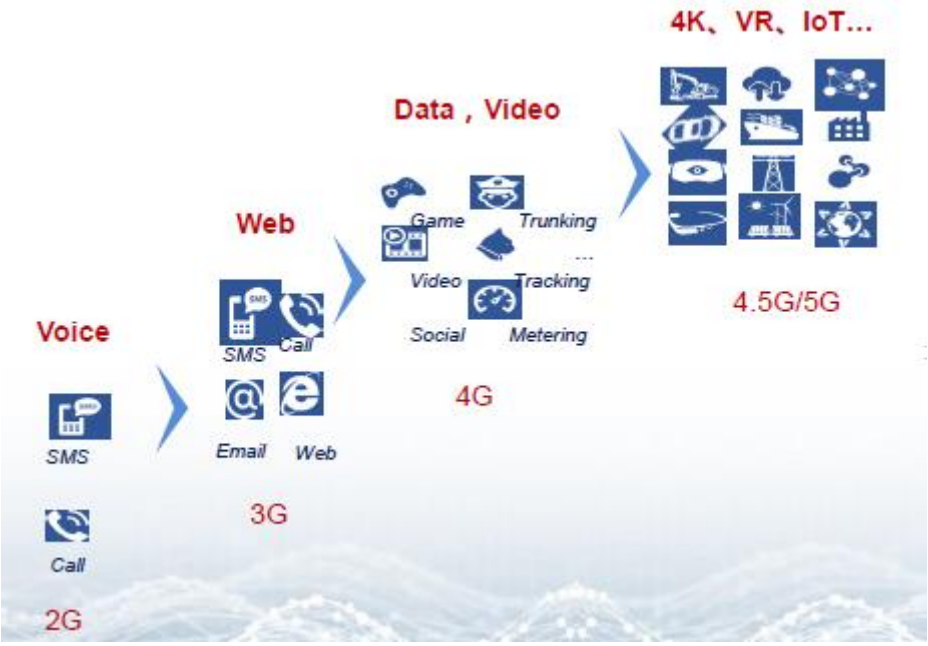


Figura 4. *Generaciones y servicios de las comunicaciones móviles. (Huawei, 2018).*

5.2.5. Tecnología GSM.

(Rouse, 2018) GSM utiliza una variación de acceso múltiple por división de tiempo (TDMA) y es la más utilizada de las tres tecnologías de telefonía inalámbrica digital: TDMA, GSM y acceso múltiple por división de código (CDMA). GSM digitaliza y comprime los datos, luego los envía por un canal con otros dos flujos de datos de usuario, cada uno en su propio intervalo de tiempo, es un sistema estándar, completamente definido, para la comunicación mediante teléfonos móviles que incorpora tecnología digital, considerado de segunda generación 2G, en la figura 5, muestra de manera resumida la arquitectura de la red GSM.

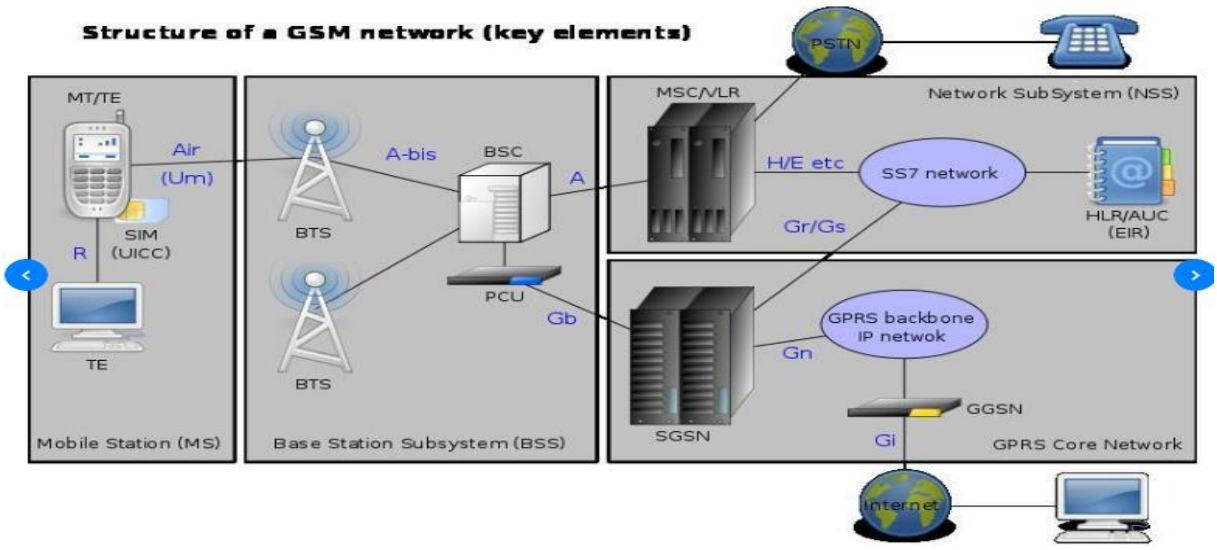


Figura 5*. Esquema general de una red GSM. (Masum, 2013).*

5.2.6. Evolución de GSM.

(Huidobro, 2015), indica que el estándar GSM en sus inicios, contaba con velocidades de 9,6 kbits/s, sin embargo, ha evolucionado considerablemente. Posterior a este, se desarrollaron diferentes tecnologías como el WAP el cual permite la combinación de internet y comunicaciones móviles, el GPRS que maneja una velocidad 115 kbits/s. Después vino EDGE con velocidades hasta de 300 kbit/s como se observa en la figura 6.

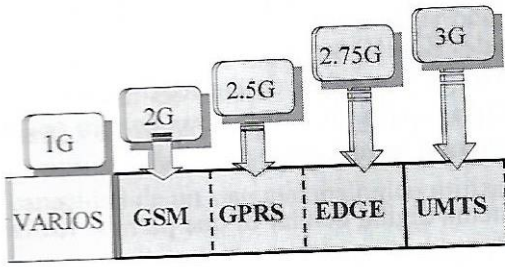


Figura 6. *Evolución GSM. (Huidobro, 2015).*

5.2.7. Estaciones base (BTS).

Las estaciones móviles se encargan de mantener el enlace radioeléctrico entre las estaciones móvil y la estación de control de servicio (BSC) durante la comunicación como muestra la figura 7. (Huidobro, 2015).

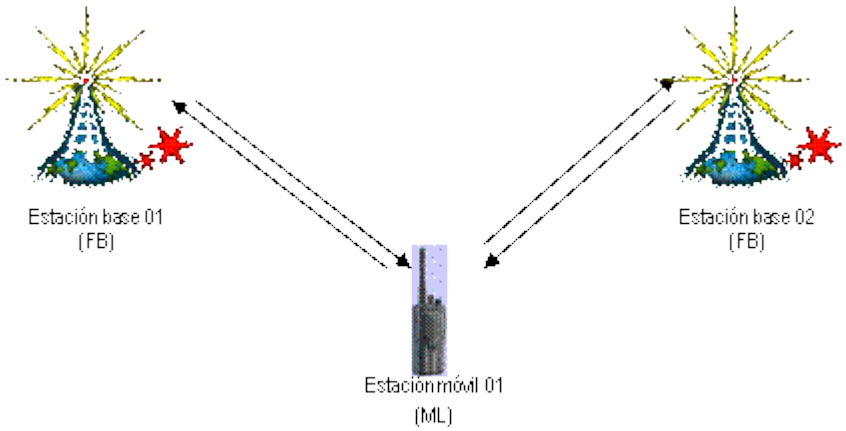


Figura 7. *Estaciones móviles. (portal.mtc, pág. 2000).*

5.2.8. Interfaz Um.

Es la interfaz radio, que se encuentra entre la estación móvil (BTS) y estación base del sistema (BSS). (Navarro, 2007).

5.2.9. Bandas de frecuencia GSM.

En el Proyecto de la universidad de Sevilla en España dicen que las redes GSM operan en cuatro bandas de frecuencias diferentes. La mayoría lo hace en la banda 900 MHz o en la de los

1800 MHz. Algunos países americanos usan a los 850 MHz y de los 1900 como lo vemos en la tabla 1. (Navarro, 2007).

Tabla 1.

Bandas de frecuencia GSM.

BAND	UPLINK (MHZ)	DOWNLINK (MHZ)	COMMENTS
380	380.2 - 389.8	390.2 - 399.8	
410	410.2 - 419.8	420.2 - 429.8	
450	450.4 - 457.6	460.4 - 467.6	
480	478.8 - 486.0	488.8 - 496.0	
710	698.0 - 716.0	728.0 - 746.0	
750	747.0 - 762.0	777.0 - 792.0	
810	806.0 - 821.0	851.0 - 866.0	
850	824.0 - 849.0	869.0 - 894.0	
900	890.0 - 915.0	935.0 - 960.0	P-GSM, i.e. Primary or standard GSM allocation
900	880.0 - 915.0	925.0 - 960.0	E-GSM, i.e. Extended GSM allocation
900	876.0 - 915	921.0 - 960.0	R-GSM, i.e. Railway GSM allocation
900	870.4 - 876.0	915.4 - 921.0	T-GSM
1800	1710.0 - 1785.0	1805.0 - 1880.0	
1900	1850.0 - 1910.0	1930.0 - 1990.0	

Nota: (Poole, 2014).

5.2.10. ARFCN.

(Navarro, 2007) El número absoluto de canal de radiofrecuencia es un numero exclusivo que se asigna a cada canal de radio en GSM. El ARFCN se puede utilizar para calcular la frecuencia exacta del canal de radio.

5.2.11. Canales Físicos.

(Navarro, 2007) En su proyecto argumenta GSM como un sistema multipartidario que utiliza, para acceder al medio, una combinación de TDMA (Time División Múltiple Access) y FDMA (Frecuency División Multiplex Access). El espacio entre portadora es de 200 KHz, permitiendo 124 canales radio en la banda de frecuencias de 850 MHz, con una duración de 4.615 ms. Como lo muestra la siguiente figura con cada ranura de tiempo (time-slot-TS-) de 0.577 ms.

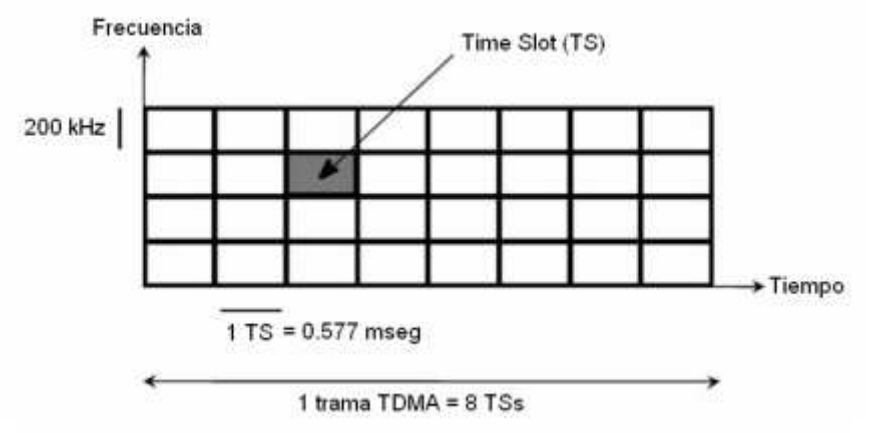


Figura 8. *Esquema de acceso al medio GSM. (Navarro, 2007).*

5.2.12. Canales lógicos.

(Tude, 2002) Dice en su revista Teleco.com la información del usuario (vos y datos) y los datos de control de señalización son trasmitidos en dos tipos básicos de canales lógicos que van a ocupar la estructura del cuadro (frame) TDMA: canal de tráfico (TCH) y canal de control (CCH) como lo vemos en la figura 9.

Estación Móvil			Aire	BTS		
Canales Lógicos TCH CCCH	<-->	Canales fisicos Canales de RF ranura de tiempo cuadro TDMA		canales fisicos canal de RF ranura de tiempo cuadro TDMA	<-->	Canales Lógicos TCH CCCH

Figura 9. *Esquema canales lógicos. (Tude, 2002).*

5.2.13. Canales de tráfico (TCH).

(Navarro, 2007) Un canal de tráfico puede trabajar en modo TCH/F (full-rate) o TCH/H (half-rate). En full-rate, la información de un usuario se transmite en una ranura de tiempo (time-slot), en cada trama. Para el modo half-rate, la información de un usuario se transmite en una ranura de tiempo, pero con trama de por medio. La siguiente tabla muestra el juego de canales de tráfico.

Tabla 2.

Canales de tráfico TCH.

Tipo de Canal	Denominación	Descripción
Canales de Tráfico (TCH)	TCH/FS	Voz (speech) a **13** Kbps
	TCH/F9.6	Datos a **9600** bps
	TCH/F4.8	Datos a **4800** bps
	TCH/F2.4	Datos a **2400** bps
	TCH/HS	Voz a **7** Kbps
	TCH/H4.8	Datos a **4800** bps
	TCH/H2.4	Datos a **2400** bps

Nota: (Navarro, 2007).

5.2.14. Canales de control (CCH).

(Navarro, 2007) Dice que en GSM, los canales de control están divididos en tres grupos como muestra en la siguiente tabla.

Tabla 3.

Canales de control en GSM.

Tipo de Canal	Denominación		Descripción
Canales de Control (CCH)	Canales de Broadcast	BCCH (Broadcast Control CHannel)	Canales de control utilizados para permitir el enganche a la red de las estaciones móviles y para el monitoreo de las potencias de celdas vecinas. Canales que radian (respectivamente): Información del sistema, una referencia de frecuencia y otra de tiempo.
		FCCH (Frequency Correction CHannel)	
		SCH (Synchronization CHannel)	
	Canales Comunes de Control	PCH (Pagging CHannel)	Canales usados para la reserva y establecimiento de un recurso radio y la asignación de canales de control.
		RACH (Random Access CHannel)	
		AGCH (Access Grant CHannel)	

	Canales de Control Dedicados	SDCCH (Stand-alone Control CHannel)	Canales de control bidireccionales utilizados para prestar los servicios de señalización y supervisión al usuario.
		SACCH (Slow-Associated Control CHannel)	
		FACCH (Fast-Associated Control CHannel)	

Nota: (Navarro, 2007).

5.2.15. Acceso múltiple por división de frecuencia (FDMA).

Acceso a las células dependiendo de la frecuencia, se para el espectro en distintos canales de voz, al dividir el ancho de banda en varios canales de uniformemente según las frecuencias de trasmisión. Los usuarios comparten el canal de comunicación y cada uno usa los diferentes subcanales particionados por la frecuencia como muestra la figura 10. (Huidobro, 2015).

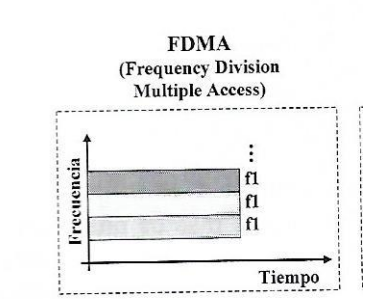


***Figura 10**. FDMA. (Huidobro, 2015).*

5.2.16. Acceso múltiple por división de tiempo (TDMA).

Define TDMA divide el canal de trasmisión en particiones de tiempo (times slots). Comprime las conversiones digitales y luego las envía utilizando la señal de radio por un periodo de tiempo. En este caso, distintos usuarios comparten el mismo canal de frecuencia, pero lo hacen en diferentes intervalos de tiempo como muestra la figura 11. (Huidobro, 2015).

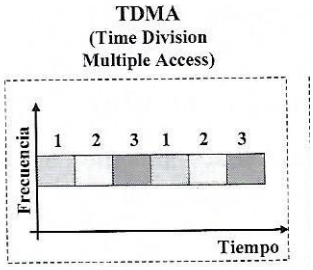


Figura 11. *TDMA. (Huidobro, 2015).*

5.2.17. Acceso múltiple por división de código (CDMA).

Esta Tecnología, luego de digitalizar la información la trasmite a través de todo el ancho de banda del que se dispone, a diferencia de TDMA y FDMA.

Las llamadas se sobreponen en el canal de transmisión, diferenciadas por un código de secuencia único. Esto permite que los usuarios compartan el canal y la frecuencia como muestra la figura 12. (Huidobro, 2015).

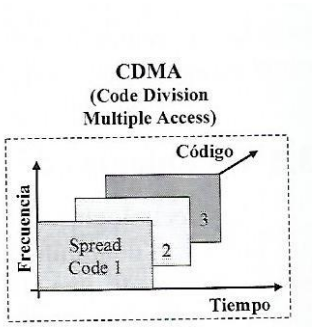
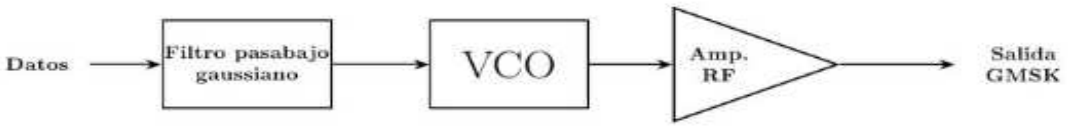


Figura 12. *CDMA. (Huidobro, 2015).*

5.2.18. Modulación GMSK.

Tutorial capa física CM dice, Es la abreviatura *Gaussian Minimum Shift Keying*. Esta modulación tiene memoria y por lo tanto la forma de onda en el instante, dependerá de los que se haya enviado anteriormente, su tecnología es de fácil fabricación y tiene una gran eficiencia, Se trata de un esquema de modulación digital por desplazamiento de frecuencia de fase continua. Los datos pasan por un filtro pasa bajo gaussiano antes de pasar al modulador, suavizando las transiciones de fase de la señal durante la trasmisión y reduciendo el ancho de banda necesario como lo muestra en la figura 13. (Almagro, 2008).



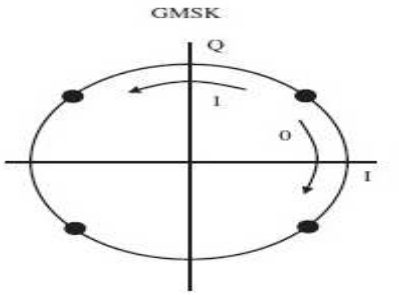


Figura 13. *Modulación GMSK. (Almagro, 2008).*

5.2.19. Radio definido por software (SDR).

Amador, J., Torres, N. (2013), definen como software definido por radio (SDR) a los dispositivos de radio multibanda con la capacidad de soportar protocolos e interfaces de aire mediante antenas de banda ancha, convertidores de análogo a digital y conversiones de radiofrecuencia, mediante la definición de sus características por software. En la figura 14, se muestra el diagrama de bloques que describe el funcionamiento de un SDR óptimo.

Figura 14*. Diagrama de sistemas definidos por software. (Torres N, 2013).*

5.2.20. Protocolo GSMTAP.

(HaraldWelte, 2010) define GSMTAP como un formato pseudo encabezado, usando para encapsular tramas desde una interfaz GSM u (area) en paquetes UDP/IP.

5.2.21. Importancia de la señal GSM.

Hoy en día GSM sigue siendo muy importante en el despliegue de redes móviles. GSM optimiza el espectro radioeléctrico, ofrece comunicaciones seguras, canales de frecuencia de mayor estabilidad en el servicio de voz, GSM dio inicio a los mensajes SMS y después multimedia, los principales números de emergencias trabajan bajo la señal GSM.

5.2.22. GSM en Colombia.

En Colombia la telefonía móvil celular se aprobó con la ley 37 de enero de 1993, la cual permite al Ministerio de Comunicaciones adjudicar la concesión del servicio de telefonía móvil

celular. Las comunicaciones móviles llegan a Colombia 15 años después que se inaugurara la primera red móvil en Japón, se crean los primeros operadores y se realizan subastas para adquisiciones de proveer el servicio sobre el recurso del espectro.

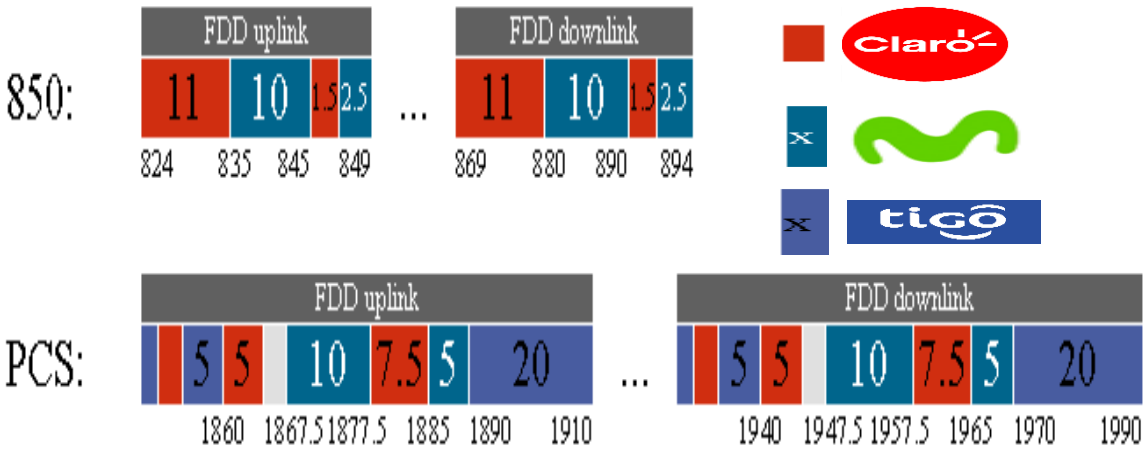


***Figura 15**. Asignación de bandas de frecuencia GSM por operador en Colombia. (spectrummonitoring.com, 2016).*

5.3. Marco legal

Para el caso del proyecto se trabajará la normativa basada en el uso de las comunicaciones móviles en Colombia y a nivel mundial; así como el uso de espectro radioeléctrico definido en la Constitución Nacional, leyes colombianas y normas internacionales.

Constitución Política de Colombia de 1991. "CAPÍTULO 2, DE LOS DERECHOS SOCIALES, ECONÓMICOS Y CULTURALES. Artículo 75. El espectro electromagnético es un bien público inajenable e imprescriptible sujeto a la gestión y control del Estado. Se garantiza la igualdad de oportunidades en el acceso a su uso en los términos que fije la ley. Para garantizar el pluralismo informativo y la competencia, el Estado intervendrá por mandato de la ley para evitar las prácticas monopolísticas en el uso del espectro electromagnético." (Constitución Política de Colombia, 1991).

Ley No. 1341 30 de Julio de 2009 dada por el ministerio de las Tecnologías información y las comunicaciones en Colombia donde dice "Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y las comunicaciones –TIC- se crea la agencia nacional de espectro y se dictan otras disposiciones." (MinTIC, 2009).

Resolución 754 de 2016 de la Agencia Nacional del Espectro: "Por la cual se reglamentan las condiciones que deben cumplir las estaciones radioeléctricas, con el objeto de controlar los niveles de exposición de las personas a los campos electromagnéticos y se dictan disposiciones relacionadas con el despliegue de antenas de radiocomunicaciones", en virtud de lo establecido

en los artículos 43 y 193 de la Ley 1753 de 2015 y se deroga la Resolución 387 de 2016" (ANE, 2016).

El Cuadro Nacional de Atribución de Frecuencias "En esta sección se encuentra un glosario de términos relevantes para la administración del espectro radioeléctrico, en la cual se adoptan las definiciones consignadas en el Reglamento de Radiocomunicaciones de la Unión Internacional de Telecomunicaciones (UIT). Dentro de estos términos se destacan los relacionados con los ejercicios de atribución, adjudicación y asignación, así como los 41 servicios radioeléctricos a los cuales se atribuyen las diferentes porciones de espectro. También se presentan las denominaciones de las estaciones y sistemas radioeléctricos, definiciones sobre la explotación y compartición de frecuencias" (ANE, 2016).

UIT-R M.1073-1, "SISTEMAS CELULARES DIGITALES DE TELECOMUNICACIONES MÓVILES TERRESTRES." Esta Recomendación establece recomendaciones sobre las características técnicas y de explotación de los sistemas celulares digitales de telecomunicaciones móviles terrestres para uso internacional y regional. Mediante la recopilación y comparación de las características de los mismos, así como la provisión de las referencias asociadas, la Recomendación suministra a las administraciones directrices para la evaluación de distintos sistemas celulares en sus aplicaciones proyectada (ITU-R, 1997).

UIT-R M.1036-5 . "Disposiciones de frecuencias para la implementación de la componente terrenal de las telecomunicaciones móviles internacionales (IMT) en las bandas identificadas en el Reglamento de Radiocomunicaciones (RR) para las IMT. Esta Recomendación proporciona directrices sobre la selección de disposiciones de frecuencias de transmisión y recepción aplicables a la componente terrenal de los sistemas IMT, así como sobre las propias disposiciones, con el objetivo de servir de ayuda a las administraciones en aspectos técnicos relativos al espectro que sean pertinentes para la implementación y utilización de la componente terrenal de IMT identificada en el RR. Las disposiciones de frecuencias se recomiendan desde el punto de vista de permitir la utilización más eficiente y eficaz del espectro para la provisión de servicios IMT, al tiempo que se minimiza el impacto sobre otros sistemas o servicios en dichas bandas, facilitando el crecimiento de los sistemas IMT." (ITU-R, 2015).

6. Metodología

6.1. Enfoque metodológico

En el presente trabajo, se utilizó el método de investigación cuantitativo, ya que, mediante números, datos y cifras tomadas con mediciones del sistema implementado, se da fundamento a este proyecto. Para comenzar, la investigación cuantitativa ofrece la posibilidad de generalizar los resultados más ampliamente, también otorga control sobre los fenómenos, así como un punto de vista de conteo y las magnitudes de éstos. Así mismo, brinda una gran posibilidad de réplica y un enfoque sobre puntos específicos de tales fenómenos, además que facilita la comparación entre estudios similares. (Hernández R., Fernández C., Baptista M. 2010).

Teniendo esto en cuenta, lo que plantea Gortari E. (1980) sobre el método científico en donde indica que "El método científico es una abstracción de las actividades que los investigadores realizan, concentrando su atención en el proceso de adquisición del conocimiento". Se toma como punto de partida para realizar la toma de mediciones con el fin de obtener parámetros presentes en las señales GSM como los canales, la potencia, la frecuencia en la que se encuentra, entre otros.

Para iniciar, se debe realizar un estudio en donde sea documentada toda la información con respecto a la tecnología a estudiar, es decir, aprender, analizar y conocer la teoría referente al sistema de señales móviles GSM y la tecnología a utilizar, que en este caso sería un SDR y la antena ATN500. Posteriormente se definen los requisitos de software, hardware y la configuración necesaria para realizar las mediciones.

Teniendo en cuenta las etapas del método científico que indica Hernández R. (2002). Se determina que mediante la observación de los sistemas disponibles en la Universitaria Agustiniana que permitan la comprensión y entendimiento del funcionamiento de las señales móviles, se evidencia que hay una carencia en sistemas de este tipo. Teniendo en cuenta los equipos a disposición, se pretende suplir esta necesidad mediante un SDR con el fin de realizar el análisis referente a las mediciones tomadas poder comprobar que el sistema sea útil y eficaz.

Por medio de los estudios realizados referentes al funcionamiento del sistema a utilizar y a la señal GSM se pueden generar la siguiente hipótesis referente al comportamiento que el modelo planteado puede tener:

El SDR por sus características técnicas es capaz de realizar las funciones requeridas, pero es indispensable configurarlo de manera adecuada de tal manera de evidenciar la información básica que posibilita el funcionamiento de esta red.

7. Administración del proyecto

7.1. Cronograma

A continuación, se presenta de manera detallada el desarrollo del proyecto.

Tabla 4.

Cronograma proyecto.

ACTIVIDADES	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Planteamiento del proyecto de investigación.																				
Estado del arte.																				
Recopilación de documentación (fabricantes, MinTic, operadores, etc).																				
Componentes del Software Definido por Radio (SDR).																				
Investigación de los parámetros de la señal GSM.																				
Recopilación de los requisitos sobre la señal GSM en Colombia.																				
Ejecutar los softwares necesarios para escanear la señal.																				
Implementación de SDR en la señal GSM.																				
Implementar Equipos para captar la señal GSM.																				
Plan de pruebas, lugares, espacio, tecnología y viabilidad.																				
Desarrollo de pruebas y revisión de parámetros dado por los programas.																				
Conclusiones																				
Documentación																				
Presentación																				

Nota: Fuente: (Autoría propia).

7.2. Presupuesto

A continuación, se muestra el presupuesto completo del proyecto.

7.2.1. Presupuesto de recursos humanos.

Tabla 5.

Presupuesto de equipos.

PERFIL	JUSTIFICACIÓN	CANTIDAD	VALOR
Investigador	Personas encargadas del desarrollo del proyecto	3	$1.047.274
Total			$3.141.822

Nota: Fuente: (Autoría propia).

7.2.2. Presupuesto de equipos.

Tabla 6.

Presupuesto de Equipos.

Equipo	Justificación	VALOR
Equipo de Computo	Equipo de cómputo para el desarrollo del proyecto.	$1.599.900
Equipo de SDR	Equipo de Escaneo de señal, Software definido por radio.	$1.077.225
TOTAL		$2.677.125

Nota: Fuente: (Autoría propia).

7.2.3. Presupuesto de software.

Tabla 7.

Presupuesto de software.

Software	Justificación	VALOR
Seguridad se sistemas operativos	Sistema de seguridad a sistema operativo.	$45.000
Office 365	Software para el desarrollo e información del proyecto.	$349.999
TOTAL		$394.999

Nota: Fuente: (Autoría propia).

7.2.4. Presupuesto de materiales y suministros.

Tabla 8.

Presupuesto de materiales y suministros.

Materiales*	Justificación	VALOR
Papelería	Impresiones y materiales de trabajo	$20.000
TOTAL		$20.000

Nota: Fuente: (Autoría propia).

7.2.5. Presupuesto de material bibliográfico.

Tabla 9.

Presupuesto de material bibliográfico.

Libro	ISBN	Justificación	VALOR
Telecomunicaciones Tecnologías, redes y servicio.	978-958-762-412-0	Libro de apoyo para el desarrollo del proyecto.	$79.999

TOTAL	$79.999

Nota: Fuente: (Autoría propia).

7.2.6. Presupuesto general.

Tabla 10.

Presupuesto Final.

ITEM	TOTAL
Recursos Humanos	$3.141.822
Equipos	$2.677.125
Software	$394.999
Materiales y suministros	$20.000
Material bibliográfico	$79.999
TOTAL	$6.308.945

Nota: Fuente: Autoría propia.

8. Desarrollo del proyecto

8.1. Principales características de la señal GSM que se son posibles de medir a través del SDR.

Para identificar las diferentes características que hacen parte de la señal GSM y que son posibles de medir a través del SDR fue necesario conocer los componentes que permiten el funcionamiento de esta señal y su arquitectura.

A continuación, se muestra la estructura de los canales lógicos pertenecientes a GSM.

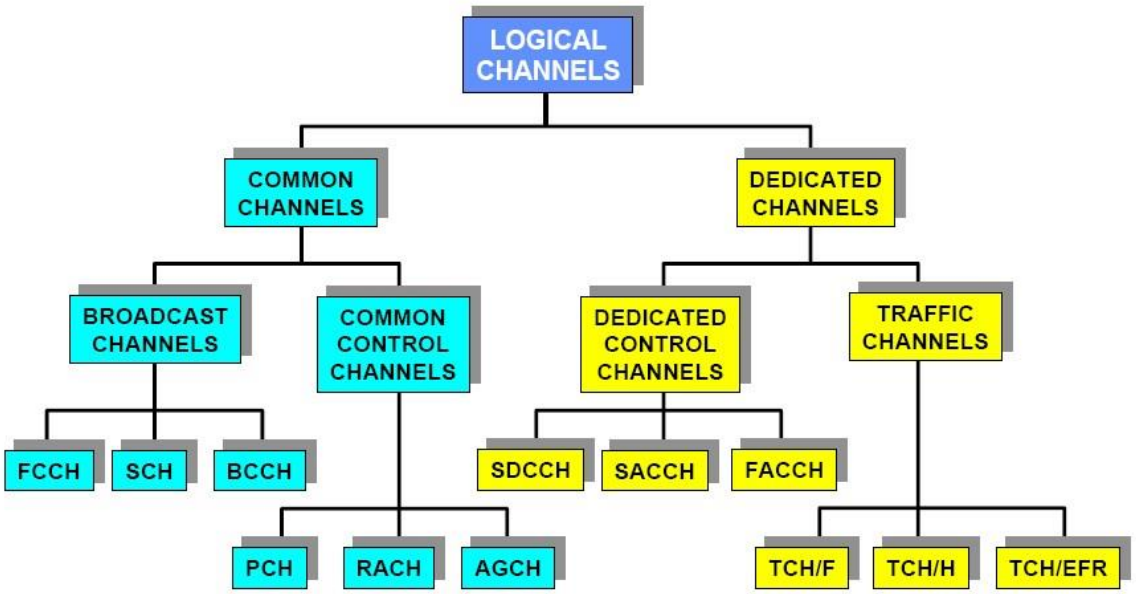


Figura 16. *Canales GSM. (Poole, 2014).*

8.1.1. Canales lógicos.

Un canal lógico no es más que una combinación ordenada de ráfagas dentro de una estructura de trama. En el sistema GSM existen dos tipos de canales lógicos:

- Canales de tráfico.
- Canales de control.

Dentro de los canales de control podemos distinguir:

- Canales de radiodifusión (BCH).
- Canales de control dedicados (DCCH).
- Canales comunes de control (CCCH).

8.1.2. Canales de tráfico.

Transmiten información generada por el usuario (voz digitalizada y/o datos).

Pueden clasificarse en:

- Traffic Channel/Full-rate Speech (TCH/FS), transmite información de voz

digitalizada a 13 Kb/seg.

- Traffic Channel/Half-rate Speech (TCH/HS), transmite información de voz digitalizada a 6,5 Kb/seg. Permite doblar aproximadamente el número de usuarios del sistema.
- Traffic Channel/Full-rate Data (TCH/F9.6, TCH/F4.8, TCH/F2.4), transmite información de datos a 9,6, 4,8 o 2,4 Kb/s.
- Traffic Channel/Half-rate Data (TCH/H4.8, TCH/H2.4), transmite información de datos a 4,8 o 2,4 Kb/s.

Todos estos canales lógicos utilizan una ráfaga normal para su transmisión.

8.1.3. Canales de radiodifusión (BCH – Broadcast Channels).

Proporcionan al móvil información suficiente para su sincronización con la red. Pueden distinguirse tres tipos de canales de radiodifusión:

- BCCH (Broadcast Control Channel). Se utiliza para informar al móvil de parámetros del sistema, necesarios para identificar la red y acceder a la misma. En particular transmite la identificación de la celda, área de localización, organización de los canales lógicos CCCH y parámetros de los grupos de búsqueda ("paging"). Se transmite dentro de una ráfaga normal y la información útil de cada bloque BCCH ocupa 23 octetos (184 bits).
- FCCH (Frequency Correction Channel). Informa al móvil de la frecuencia portadora de la estación base. Permite la sintonía de los receptores móviles. Se transmite dentro de una ráfaga de corrección de frecuencia.
- SCH (Synchronization Channel) Permite identificar la estación base sintonizada y sincronizarse con la estructura de trama. Informa al móvil de la secuencia de entrenamiento que utiliza la base y que es necesaria para la demodulación de la ráfaga. Se transmite dentro de una ráfaga de sincronización.

8.1.4. Canales de control dedicados (DCCH – Dedicated Control Channels).

Se utilizan para transmitir información de control entre la red y el móvil, o incluso entre los propios transceptores de radio. Pueden distinguirse tres tipos de canales de control dedicados:

- SACCH (Slow Associated Control Channel). transmite información de control dedicada al mantenimiento del enlace. Se utiliza siempre asociado a un canal de tráfico. En el enlace descendente transmite el valor de potencia a transmitir y el valor del Time Advance. En el enlace ascendente transmite medidas realizadas por el

móvil para los procesos de transferencia de llamada (Handover). Se transmite dentro de una ráfaga normal.

- FACCH (Fast Associated Control Channel). Reemplaza a un canal de tráfico y sirve para transmitir informaciones de control urgentes. Se transmite dentro de una ráfaga normal.
- SDCCH (Stand-alone Dedicated Control Channel). Se utiliza para intercambiar mensajes entre el móvil y la base, una vez el móvil ha accedido a una ráfaga y antes de establecer la comunicación. Se transmite dentro de una ráfaga normal.

8.1.5. Canales comunes de control (CCCH – Common Control Channels).

Permiten el establecimiento del enlace entre el móvil y la base. Puede distinguirse entre:

Originados en la base:

- PCH (Paging Channel). Avisa al móvil de las llamadas entrantes procedentes de la estación base. Se transmite dentro de una ráfaga normal.
- AGCH (Access Grant Channel). Concede o niega la llamada solicitada por el móvil. En caso de concesión de llamada también informa del valor del Time Advance. Se transmite dentro de una ráfaga normal.

Originados en el terminal:

- RACH (Random Access Channel). Se utiliza por el móvil para realizar una petición de llamada. Se transmite dentro de una ráfaga de acceso.

Todos los canales comunes de control se transmiten en una multitrama de 51 tramas.

8.1.6. Parámetros de la telefonía celular.

IMSI (international mobile subscriber identity o identidad internacional de abonado móvil) es el identificador de la línea o servicio, los operadores miran este número y de ahí pueden obtener el país o la red a la que pertenece, Los primeros tres números de la serie representan el código de país del teléfono, seguido por el código de la red. El último conjunto de dígitos del número IMSI representa al "número de suscriptor único" del dispositivo. como se muestra en la siguiente tabla.

Tabla 11.

IMSI Colombia.

IMSI: 7321014

MCC	732	Colombia
MNC	101	Claro

Nota:Fuente: (Autoría propia).

TMSI (Temporary Mobile Subscriber Identity o identidad temporal del suscriptor móvil) es la identidad que se envía más comúnmente entre el móvil y la red. El número es local para un área de ubicación, por lo que debe actualizarse cada vez que el móvil se traslada a una nueva área geográfica.

MCC (Mobile Country Code o código de país móvil) y **MNC** (Mobile Network Code o código de red móvil), son dos códigos numéricos usados para identificar el país y los operadores de telefonía móvil que utilizan y ciertas redes satelitales como lo muestra en a la figura.

Colombia				
732	001	Colombia Telecomunicaciones S.A. - Telecom	Operativa	N. D.
732	002	Edatel S.A.	Operativa	N. D.
732	101	Comcel S.A. Occel S.A. / Celcaribe	Operativa	GSM 850 / GSM 1900
732	102	Bellsouth Colombia S.A. (movistar)	Operativa	GSM 850 / GSM 1900 / CDMA2000 850
732	103	Colombia Móvil S.A.	Operativa	GSM 1900
732	123	Telefónica Móviles Colombia S.A. (movistar)	Operativa	GSM 850 / GSM 1900 / CDMA2000 850

Figura 17. *MCC y MNC Colombia. (Escobar, 2013).*

Cell ID (ID de celda) es un número generalmente único usado para identificar cada estación transceptora base (BTS) o sector de una BTS dentro de un código de área de ubicación si no está dentro de una red GSM, como lo muestra la siguiente figura.

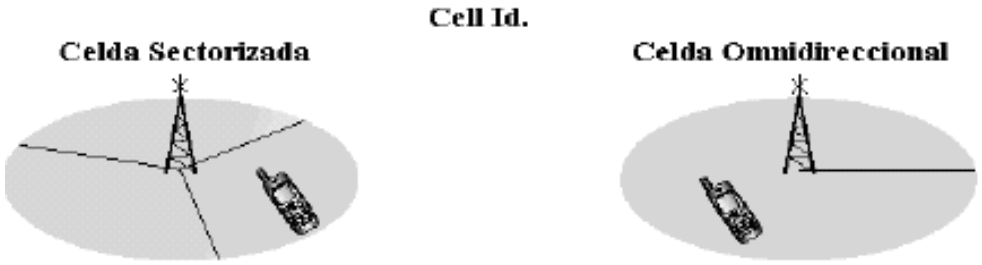


Figura 18. *Cell Id. (Hernandez, 2005).*

ARFCN (absolute radio-frequency channel number o número de canal de radiofrecuencia absoluto) es un código que especifica un par de portadoras de radio físicas usadas para transmisión y recepción en un sistema de radio móvil terrestre, uno para la señal de enlace ascendente y otro para la señal de enlace descendente como lo muestra la siguiente tabla.

Tabla 12.

ARFCN de las bandas de frecuencia.

GSM Band	ARFCN(N)	Uplink Frequency equation(F_{UL})	Downlink Frequency equation
GSM 450	259-293	450.6 + 0.2*(N-259)	$F_{UL}(N)$ + 10
GSM 480	306-340	479+0.2*(N-306)	$F_{UL}(N)$ + 10
GSM 750	438-511	747.2 + 0.2*(N-438)	$F_{UL}(N)$ + 30
GSM 850	128-251	824.2+0.2*(N-128)	$F_{UL}(N)$ + 45
P-GSM	1-124	890+0.2*N	$F_{UL}(N)$ + 45
E-GSM	975-1023	890+0.2*(N-1024)	$F_{UL}(N)$ + 45
GSM-R	955-1023	890+0.2*(N-1024)	$F_{UL}(N)$ + 45
DCS 1800	512-885	1710.2+0.2*(N-512)	$F_{UL}(N)$ + 95
PCS 1900	512-810	1850.2 + 0.2*(N-512)	$F_{UL}(N)$ + 80

Nota: (rfwireless, 2012)

LAC (location área code o código de área de ubicación) este código se utiliza como referencia única para la ubicación de un suscriptor móvil, es necesario para dirigirse al suscriptor en el caso de una llamada entrante.

Timing advance (avance temporal) es un parámetro que permite el BTS GSM para el control de los retrasos de la señal en su comunicación con el móvil. Es un sistema de sincronización entre la estación base (BS) y la estación móvil (MS) necesario en las redes celulares como método de acceso al medio y tienen una gran cobertura como lo muestra la siguiente imagen.

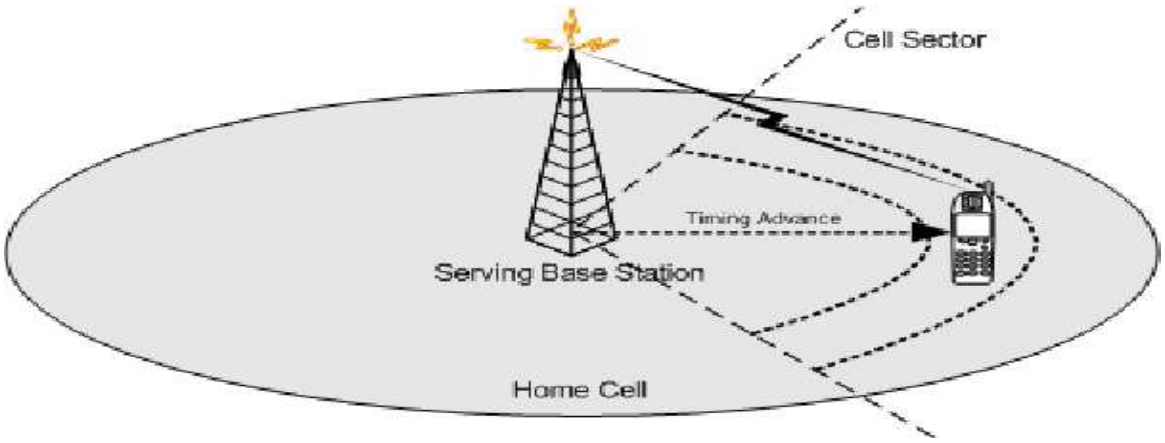


Figura 19. *Timing advance. (Resch, 2015).*

8.1.7. Características generales GSM.

En la siguiente tabla muestra los parámetros investigados más relevantes de la señal GSM.

Tabla 13.

Características Generales GSM.

Generalidad	Descripción
Generación, velocidad y Voz	2G – 14 Kbps – 64Kbps, buena calidad de Voz.
Métodos de acceso múltiple al medio	GSM – TDMA y CDMA
Modulación	GMSK- fase continua 8-PSK
Alcance	2 km
Banda de Frecuencias utilizadas.	850 MHz - 1900 MHz (GSM)
Ancho de Banda	200Khz
Voz	13 kbit/s (22,8 kbit/s bruta)
Datos	9,6 kbit/s, 4,8 kbit/s y 3,6 kbit/s

Nota: Fuente: (Autoría propia).

Con las especificaciones del SDR según el fabricante cumple con el requerimiento para captar la señal GSM.

8.2. Requisitos de hardware y software necesarios para obtener los parámetros de la señal GSM

(Bryon, 2013) En el desarrollo del presente proyecto se sacó la información del tutorial de la comunidad Scoyok y Slick97477 la cual titula "Captura GSM, decodificación con USRP y SDR en Linux Rolling Edition" En donde encontramos los requerimientos más indicados para censar las principales características nombradas en el anterior capitulo e implementarlos con los siguientes componentes:

Tabla 14.

Requisitos de hardware y software.

Software	Hardware
Ubuntu	Computador portátil
Kalibrate	SDR- HackRF One
GQRX.	Antena ANT500
GNU Radio	
GR-GSM.	
Wireshark	

Nota: Fuente: (Autoría propia).

8.2.1. Software.

Se entiende por software todos aquellos componentes que conforman un sistema informático que no son tangibles. El programa se puede definir como el conjunto de instrucciones que contiene un sistema, ya sea para poner en marcha el funcionamiento del mismo o desarrollar funciones orientadas al usuario.

El software que se utilizó para el diseño de este modelo fue:

8.2.2. Ubuntu.

Este Sistema operativo es el más indicado para el desarrollo del proyecto ya que cuenta con toda la estructura y programas elegidos para el fin del mismo.

Ubuntu es un sistema operativo de código abierto que se ejecuta desde el escritorio, a la nube, a todas las cosas conectadas a Internet. Este, está basado en estructura Debian, concentrándose en la simplicidad para su utilización, actualización periódica de versiones (cada 6 mese regularmente) y su poca complejidad a la hora de realizar la instalación.
Sus características principales son:

- Disponible en 4 arquitecturas: Intel x86, AMD64, SPARC (para esta última sólo existe la versión servidor).
- Los desarrolladores de Ubuntu se basan en gran medida en el trabajo de las comunidades de Debian y GNOME.
- Las versiones estables se liberan cada 6 meses y se mantienen actualizadas en materia de seguridad hasta 18 meses después de su lanzamiento.
- El entorno de escritorio oficial es Gnome y se sincronizan con sus liberaciones.
- Para centrarse en solucionar rápidamente los bugs, conflictos de paquetes, y demás problemas al lanzar nuevas versiones, se decidió eliminar ciertos paquetes del componente main, ya que no son populares o simplemente se escogieron de forma arbitraria por gusto o sus bases de apoyo al software libre.
- El navegador web oficial es Mozilla Firefox.
- Entre sus funciones de seguridad el sistema no permite activar, de forma predeterminada, procesos latentes al momento de instalarse. Por esta razón, no cuenta con un firewall predeterminado.
- Para labores/tareas administrativas en terminal incluye una herramienta llamada sudo (similar al Mac OS X), con la que se evita el uso del usuario root (administrador).
- Mejora la accesibilidad y la internacionalización, de modo que el software está disponible para tanta gente como sea posible. En la versión 5.04, el UTF-8 es la codificación de caracteres en forma predeterminada.
- No sólo se relaciona con Debian por el uso del mismo formato de paquetes deb, también tiene uniones muy fuertes con esa comunidad, contribuyendo con cualquier cambio directa e inmediatamente, y no solo anunciándolos. Esto sucede en los tiempos de lanzamiento.

Muchos de los desarrolladores de Ubuntu son también responsables de los paquetes importantes dentro de la distribución de Debian.

- Todos los lanzamientos de Ubuntu se proporcionan sin costo alguno. Los CDs de la distribución se envían de forma gratuita a cualquier persona que los solicite mediante el servicio ShipIt (la versión 6.10 no se llegó a distribuir de forma gratuita en CD, pero la versión 7.04 sí). También es posible descargar las imágenes ISO de los discos por transferencia directa o bajo la tecnología Bittorrent.

Como se observa en la figura, la arquitectura que se utilizó para el la implementación del modelo de medición de señales GSM es AMD64.

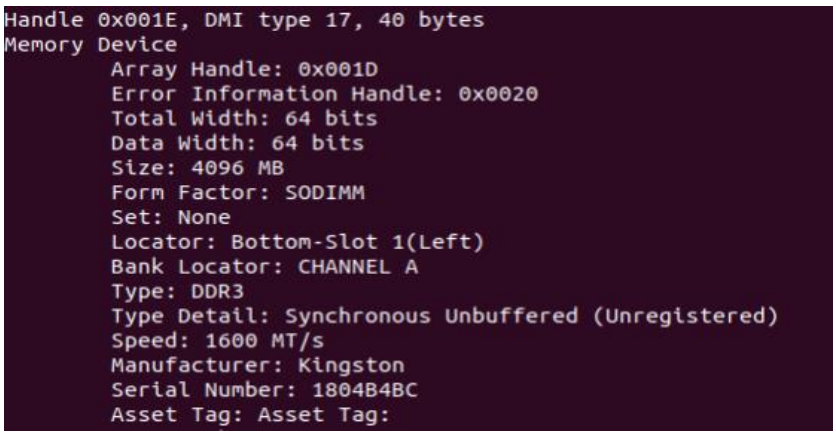


Figura 20. *Arquitectura implementada. Fuente: (Autoría propia).*

8.2.3. Kalibrate.

Es una aplicación basada en un hardware dongle (receptor de radio y televisión USB) de bajo presupuesto, el cual permite censar las frecuencias de GSM presentes en el momento, además de la intensidad. La utilización de este programa permite escanear las diferentes bandas de frecuencias GSM y evidenciar los distintos canales y ancho de banda con su potencia usados por las diferentes antenas BTS de los operadores de telefonía local, como muestra la siguiente figura encontramos diferentes canales en la banda de 850 Mhz.

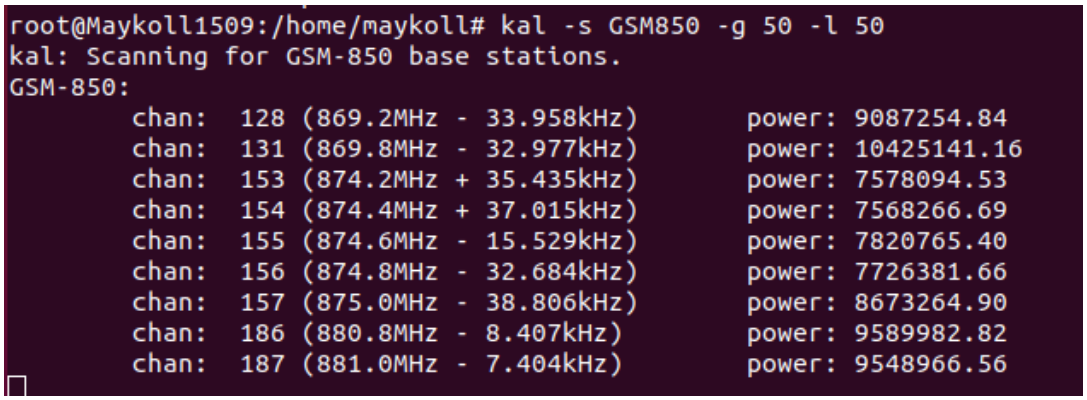


Figura 21. *Escáner de frecuencias. Fuente: (Autoría propia).*

8.2.4. GQRX.

Es un programa definido como radio receptor que funciona con la herramienta GNU Radio SDR framework y el conjunto de herramientas gráficas. Gqrx es una herramienta gratuita e incluye el código fuente licenciado bajo Gnu Gpl lo cual permite actualizar/modificar, su principal función es obtener una frecuencia exacta. Actualmente, correo sobre los sistemas operativos Linux y Mac y es utilizable con los siguientes dispositivos:

- Funcube Dongle Pro
- Pro+ RTL2832-U
- DVB-T dongles (rtlsdr via usb y tcp).
- OrmoSDR
- USRP
- HackRF
- Jawbreaker
- Nuan
- bladeRF

Entre algunas de sus funciones más importantes están:

- Descubrir dispositivos conectados a la computadora.
- Procesar datos I/Q desde los dispositivos soportados.
- Cambiar la frecuencia, ganar y aplicar varias correcciones (frecuencia, balance I/Q).
- Demoduladores AM, SSB, FM-N y FM-W (mono y estéreo).
- Modos especiales de FC para NOAA APT.
- Bandas variables y filtros de paso.
- AGC, supresor y blanqueo de ruido.
- Ploteo FFT y cascadas.
- Grabar y reproducir audio a/desde un archivo Wav.

- Analizador de espectro donde todas las señales procesadas son desactivadas.

A continuación, evidenciamos la obtención de frecuencia exacta figura 18.

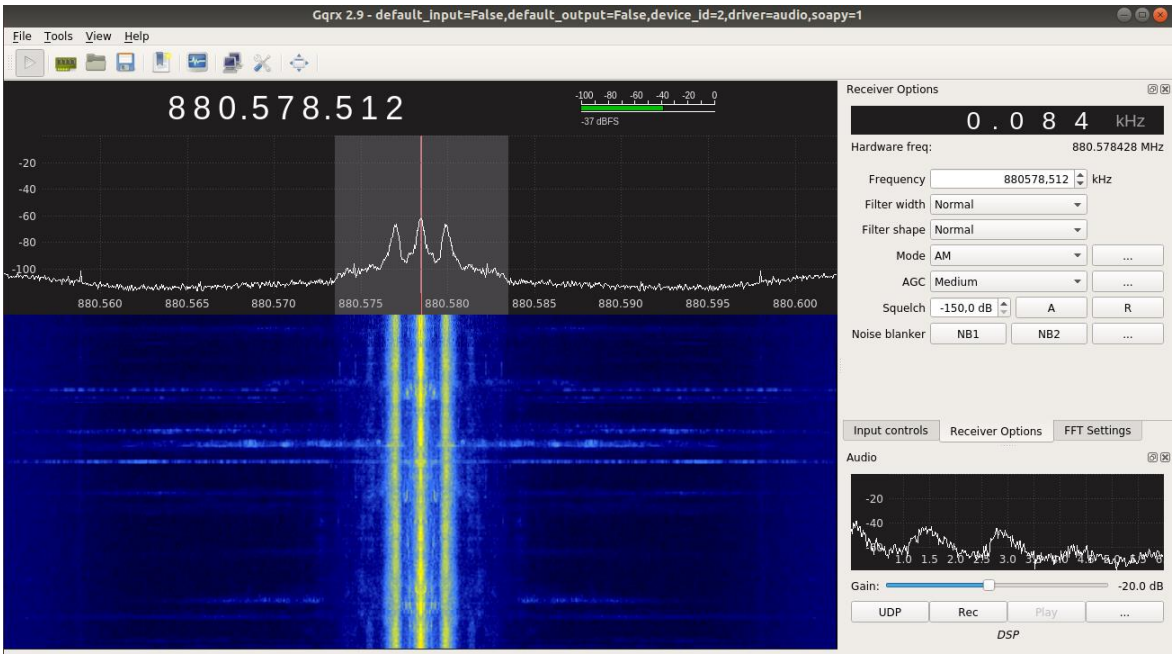


***Figura 22**. Gqrx frecuencia exacta. Fuente: (Autoría propia).*

8.2.5. GNU Radio.

GNU Radio es un programa libre compuesto por herramientas de desarrollo de software que proporciona bloques de procesamientos de señales. Puede ser utilizado con hardware de RF externo de bajo costo y alta disponibilidad para crear radios definidos por software, o sin hardware en un entorno de simulación. Este es muy utilizado en diversas áreas para apoyar tanto la investigación de comunicaciones inalámbricas como los sistemas de radio del mundo real.

GNU realiza el procesamiento de la señal que puede ser utilizado para escribir y/o crear aplicación para recibir o transmitir información mediante sus herramientas como ecualizadores, moduladores, decodificadores, filtros entre otros (estas herramientas son denominadas bloques). También puede utilizar hardware pare realizar transmisiones digitales, diseñando un modelo en el cual se puede realizar un análisis de los datos evidenciando el paso por cada uno de los bloques del sistema como lo muestra en la figura 19.

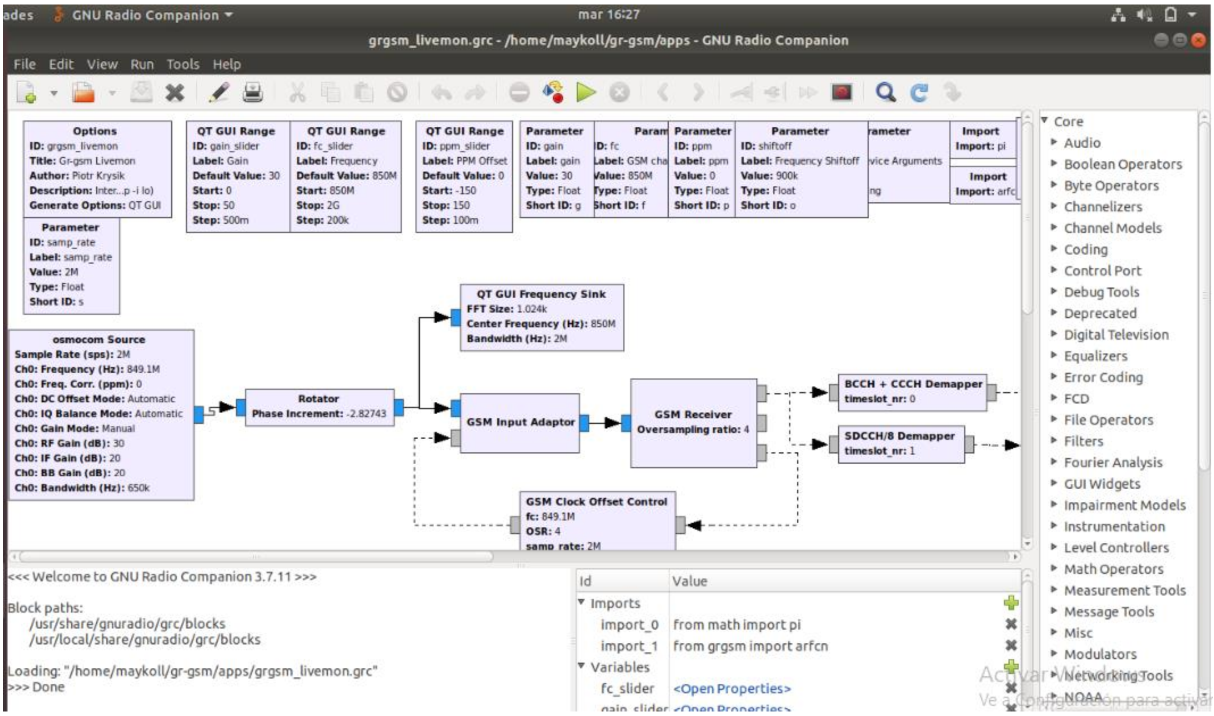


Figura 23. *Programa GNURadio. Fuente: (Autoría propia).*

8.2.6. GR-GSM.

Es un sistema de herramientas diseñados para implementar el protocolo de GSM, con el fin de recibir la información transmitida por los equipos/dispositivos que intervienen en la comunicación, adicional a esto tiene la capacidad de buscar las estaciones base y decodificar el tráfico de radio como lo muestra en la siguiente figura.

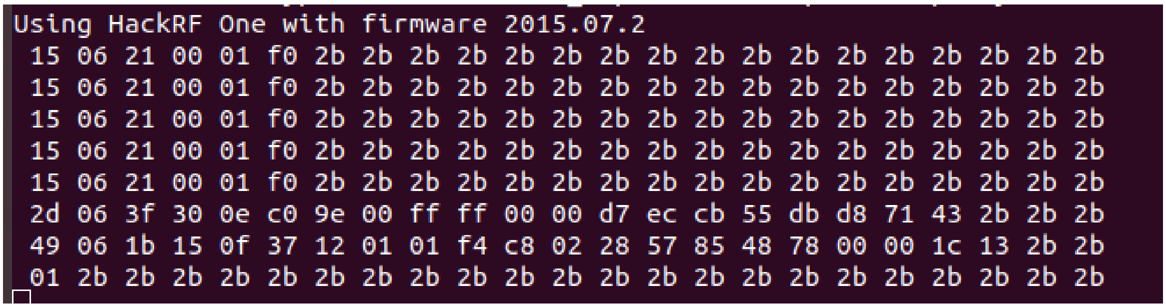


Figura 24. *Gr-gsm para la decodificación de las tramas. Fuente: (Autoría propia).*

8.2.7. Wireshark.

Wireshark es un analizador de paquetes de código abierto que se utiliza para examinar cada paquete que transita dentro de una de red y mostrar de la manera más detallada posible los datos del paquete. Este, se utiliza en varios ámbitos como lo pueden ser los administradores de red para solucionar problemas de red, los ingenieros de seguridad de redes lo utilizan para examinar problemas de seguridad, los ingenieros de control de calidad lo utilizan para verificar las aplicaciones de red, entre muchas otras.

Sus características principales son:

- Disponible en diversas plataformas como UNIX, LINUX, Windows y Mac OS.
- Captura los paquetes directamente desde una interfaz de red.
- Permite obtener detalladamente la información del protocolo(s) utilizado en el paquete capturado.
- Cuenta con la capacidad de importar/exportar los paquetes capturados desde/hacia otros programas.
- Filtra los paquetes que cumplan con un criterio definido previamente.
- Realiza la búsqueda de los paquetes que cumplan con un criterio definido previamente.
- Permite obtener estadísticas.
- Sus funciones gráficas son muy poderosas ya que identifica mediante el uso de colores los paquetes que cumplen con los filtros establecidos.

Como lo muestra en las siguientes figuras.

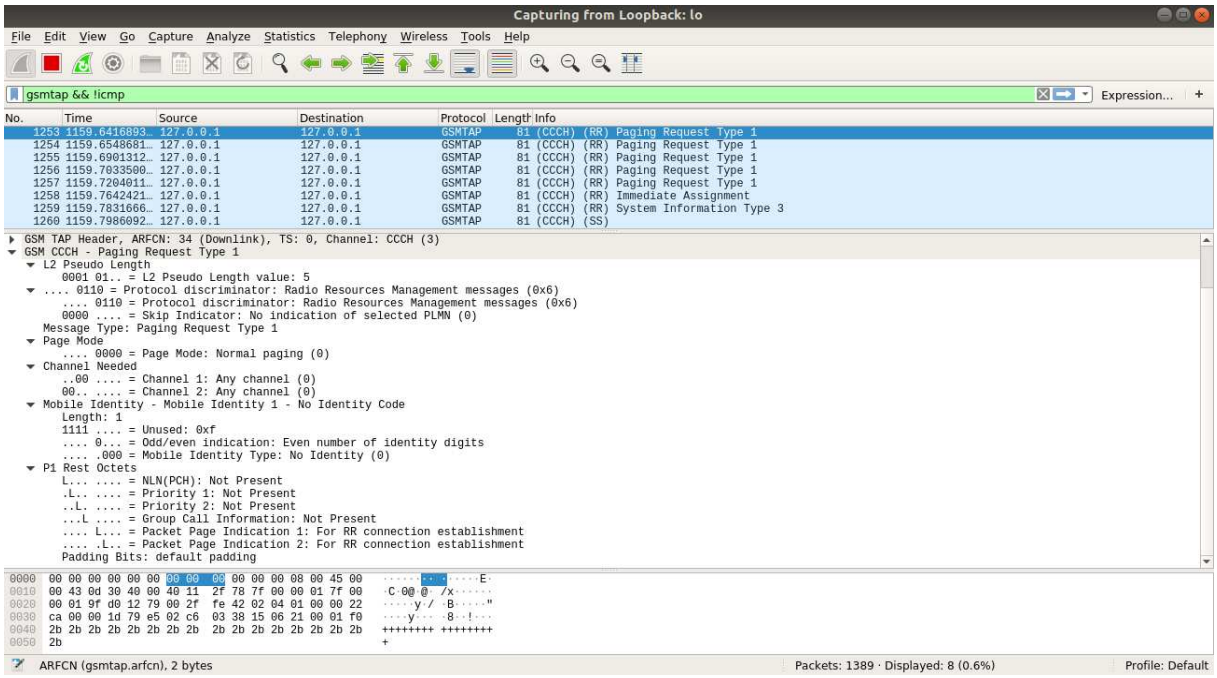


Figura 25. *Wireshark. Fuente: (Autoría propia).*

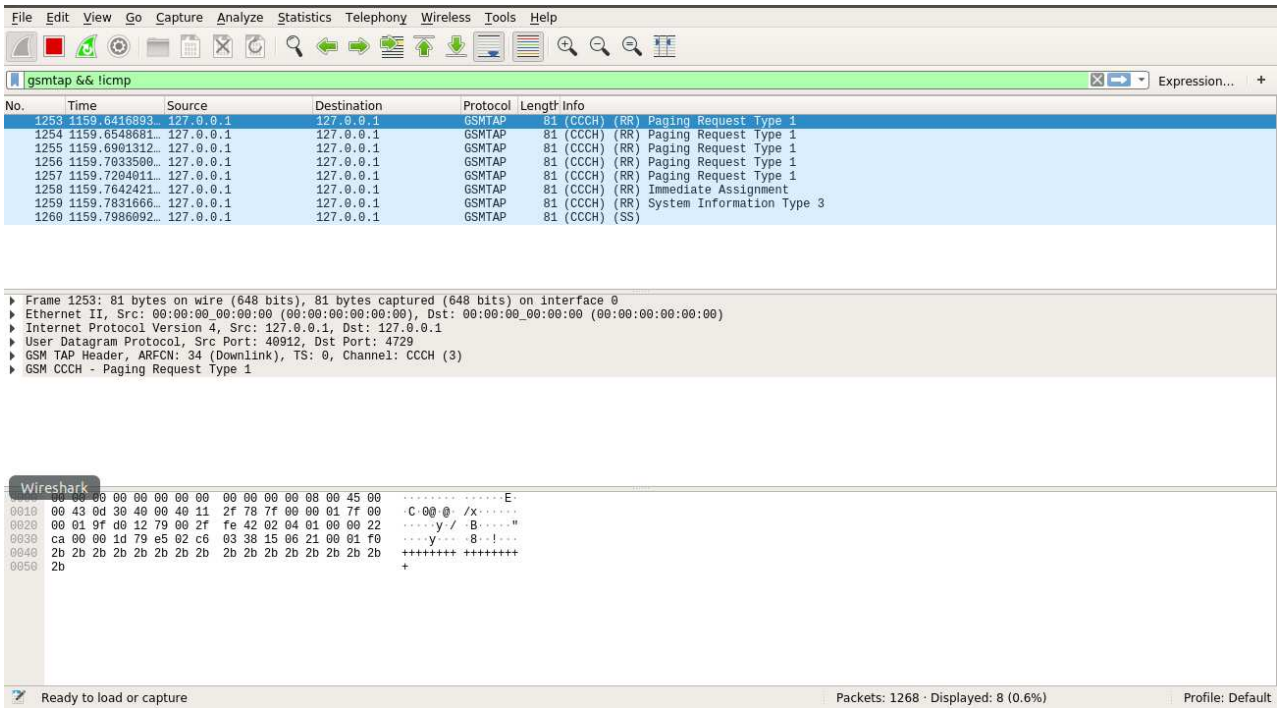


Figura 26. *Protocolo GSMTAP con Wireshark. Fuente (Autoría propia).*

8.2.8. Hardware.

Es la parte física y tangible con la que cuentan todos o la gran mayoría de los sistemas informáticos y de comunicaciones. En esto se incluyen todos los periféricos, dispositivos de entrada, de salida, cableado, componentes eléctricos, electromagnéticos o cualquier elemento físico que intervenga, es considerado Hardware.

El Hardware que se utilizó en la implementación de un modelo capaz de medir señales GSM, son los siguientes:

Computador portátil con las siguientes características.

Tabla 15.

Características computador.

Ítem	Característica
Procesador	AMD E2-7110 APU
Memoria RAM	4 GB
Tipo de sistema	Sistema operativo de 64 bits
Sistema operativo	Ubuntu 18.04

Nota: Fuente: (Autoría propia).

8.2.9. SDR - HackRF one (software definido por radio).

Es un periférico de radio definido por software con la capacidad de transmitir o recibir señales de radio entre 1 MHz a 6 GHz. Está diseñado para permitir pruebas y desarrollo de tecnologías de radio modernas y de próxima generación, ya que es una plataforma de hardware

de código abierto que se puede usar como un periférico USB o programado para un funcionamiento independiente.

Figura 27. *SDR-HackRF one. (greatscottgadgets, 2009).*

Características técnicas:

Tabla 16.

Características técnicas.

Ítem	Especificación
Frecuencia de operación	1MHz a 6MHz
Transceptor	Half Duplex
Muestra	cuadratura de 8 bits (I de 8 bits y Q de 8 bits)
RX y TX	Configurable
Alimentación de la antena	50 mA a 3,3 V
Antena	Conector SMA
Reloj	De salida SMA para sincronización
Expansión	Mediante cabezales internos
USB	2.0 de alta velocidad
Alimentación	Mediante USB
Hardware	Código abierto

Nota: Fuente (Autoría propia).

8.2.10. Antena ANT500.

ANT500 una antena telescópica diseñada para funcionar de 75 MHz a 1 GHz. Se puede ajustar su longitud desde 20 cm a 88 cm. Está fabricada en acero inoxidable y cuenta con un conector macho SMA, un eje giratorio, un codo ajustable y siendo una antena de uso general de 50 Ohmios.

Figura 28. *Antena ANT500. (greatscottgadgets, 2009).*

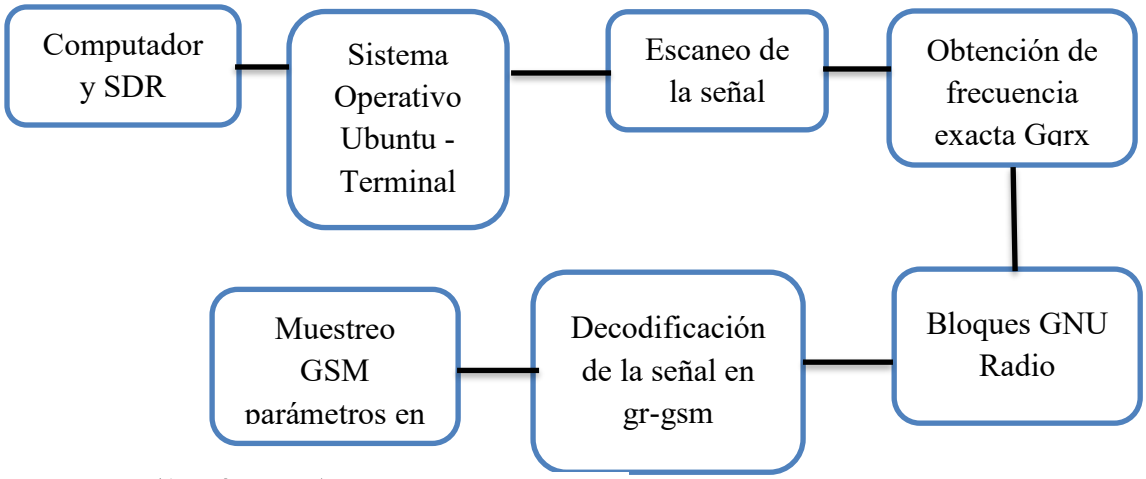
Con los diferentes software y hardware investigados implementaremos la práctica para entender más a profundidad las características de cada uno.

8.3. Necesidades de configuración del SDR que responda a los requisitos de hardware y software que permita medir la señal GSM.

Con los software y hardware identificados, los equipos configurados para captar la señal GSM y evidenciar sus características.

Tabla 17.

Esquema para obtener parámetros.



Nota: Fuente *(Autoría propia).*

La configuración se seguirá desarrollando con la tutorial para captura GSM nombrada anteriormente. (Bryon, 2013).

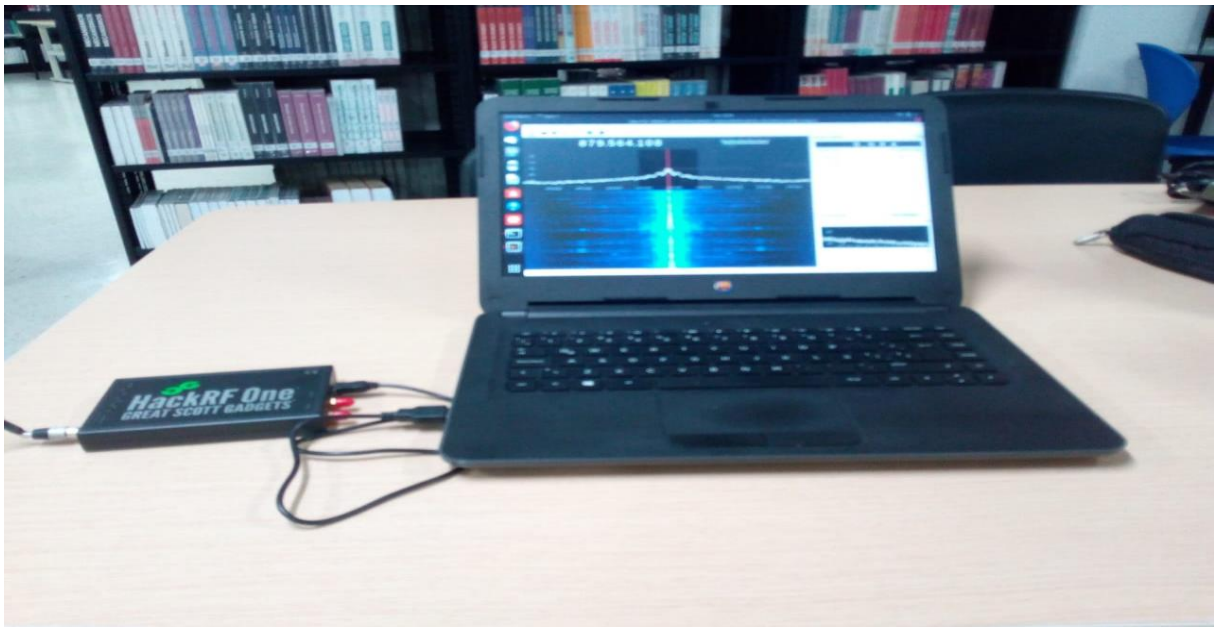


Figura 29. *Implementación HackRF One. Fuente: (Autoría propia).*

8.3.1. Librerías y paquetes.

Con los siguientes comandos, se descargan librerías y paquetes de vital importancia para el funcionamiento del análisis de la señal GSM.

apt-get install hackrf libhackrf-dev libhackrf.: este comando permite realizar la instalación de los paquetes y librerías que permiten que se reconozca el equipo HackRF One. Posterior a la correcta instalación de estos paquetes y librerias, se puede ejecutar el comando hackrf_info (con el equipo conectado) para verificar que haya sido exitosa la instalación

apt-get -y install git-core autoconf automake libtool g++ pgggython-dev swig libpcap0.8-dev: Este comando permite obtener los paquetes para el control sobre el diseño a realizar mediante herramientas de gestión de código distribuido, la cual se realiza de manera automática. Estos paquetes, cumplen con los estándares de GNU gestionando de manera automática los archivos generados mediante librerías genéricas. Adicional a esto también se obtiene el compilador en C++ y las herramientas de desarrollo para la construcción de módulos en Python o la incrustación de este en aplicaciones.

apt-get install gnuradio gnuradio-dev gr-osmosdr gr-osmosdr: Con este comando se instala el GNU Radio, junto con los paquetes del osmocom. Estos permiten que se reconozca el dispositivo para su posterior utilización.

apt-get install git cmake libboost-all-dev libcppunit-dev swig doxygen liblog4cpp5-dev python-scipy: este comando permite controlar el proceso de compilado de software utilizando archivos de configuración independientes al compilador. Genera adicional a esto también genera una unidad de bibliotecas, sistemas de documentación e interfaces en C/C++.

apt-get install build-essential libtool shtool autoconf automake git-core pkg-config make gcc: este comando descarga los paquetes esenciales para la compilación, junto con las librerias genéricas de GNU. Adicional a esto también se obtiene una herramienta portátil para GNU y los paquetes necesarios para entrelazar, administrar y compilar las bibliotecas.

apt-get install libpcsclite-dev: esta es una librería adicional, su función es el permiso de acceder a la tarjeta inteligente utilizando archivos de desarrollo (PC/SC).

8.3.2. Comandos utilizados.

Tabla 18.

Comandos.

• apt update
• apt upgrade -y

• apt-get install kali-linux-all
• apt-get install flashplugin-nonfree
• update-flashplugin-nonfree --install
• apt-get install hackrf libhackrf-dev libhackrf0
• apt-get -y install git-core autoconf automake libtool g++ python-dev swig libpcap0.8-dev
• apt-get install gnuradio gnuradio-dev gr-osmosdr gr-osmosdr
• apt-get install git cmake libboost-all-dev libcppunit-dev swig doxygen liblog4cpp5-dev python-scipy
• apt-get install build-essential libtool shtool autoconf automake git-core pkg-config make gcc
• apt-get install libpcsclite-dev (opcional)
• git clone
• cd gr-gsm
• git clone git://git.osmocom.org/libosmocore.git
• cd libosmocore
• autoreconf -i/configure
• make
• make install
• ldconfig -i
• cd ..mkdir build
• cd build
• cmake ..
• make
• make install
• ldconfig

Nota: Fuente: (Autoría propia).

Para la siguiente parte, se debe crear un archivo de texto que se llame config. conf. En él, se debe contener la siguiente información.

local_blocks_path=/usr/local/share/gnuradio/grc/blocks

Posterior a esto se tiene que ubicar manualmente el archivo. Haga clic en Inicio, haga clic en Otras ubicaciones, haga clic en Computadora, despues abra ETC, luego la carpeta de Gnuradio, luego guarde como en el editor de texto en esta ubicación.

- git clone https://github.com/scateu/kalibrate-hackrf.git
- cd kalibrate-hackrf

- ./bootstrap
- ./configure
- make
- make install
- ldconfig

8.3.3. Captura, decodificación y parámetros de la señal GSM.

A continuación, se muestra paso por paso el proceso a seguir para realizar el análisis de la señal GSM utilizando el SDR HackRF One.

Para empezar, con el comando kal -s GSM850 -g 50 -l 50, utilizamos el programa Kalibrate para escanear los canales disponibles de GSM en la banda de 850MHz para iniciar el análisis y decodificación de paquetes GSM.

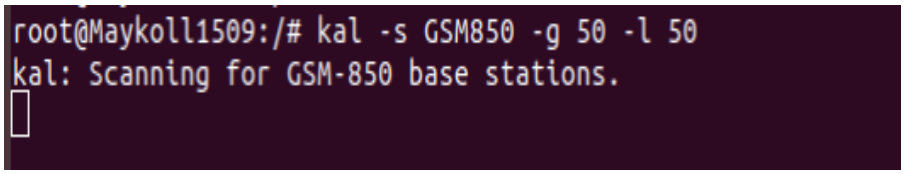


Figura 30. *Escanear canales. Fuente: (Autoría propia).*

Al ejecutar este comando se obtienen los canales con su respectiva frecuencia, como se muestra a continuación.

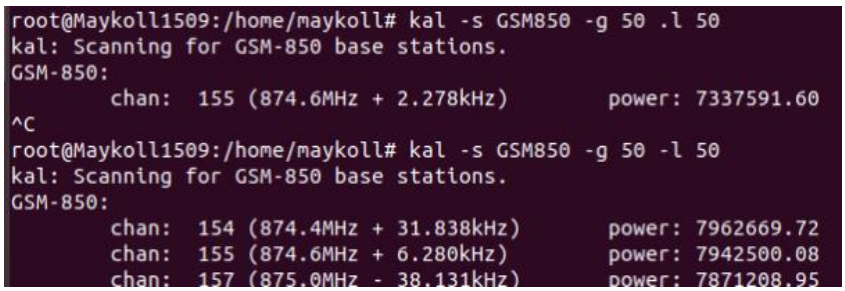


Figura 31. *Canales encontrados. Fuente: (Autoría propia).*

Posterior a obtener esta, procedemos a abrir el analizador de espectro GQRX para evidenciar el tráfico sobre alguna de las frecuencias obtenidas con anterioridad. Tener en cuenta que el comando se debe ejecutar como super usuario para obtener los resultados esperados.

Figura 32. *Programa Gqrx. Fuente: (Autoría propia).*

Al ejecutar el programa, se desplegará una pantalla una ventana como se muestra en la figura xx, en la cual, se debe tener en cuenta que el dispositivo debe estar en Default, tanto en I/Q input como en Audio Output.

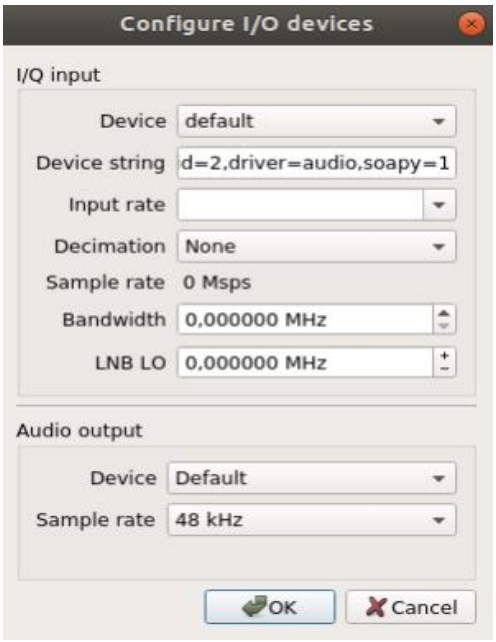


Figura 33. *Configure. Fuente: (Autoría propia).*

Adicional a esto en el recuadro de configuración de control remoto, se debe tener, en Listen on Port el puerto 7356 y en Allowed Hosts la dirección IP 127.0.0.1, esto con el fin de observar el tráfico sobre el canal de GSM.

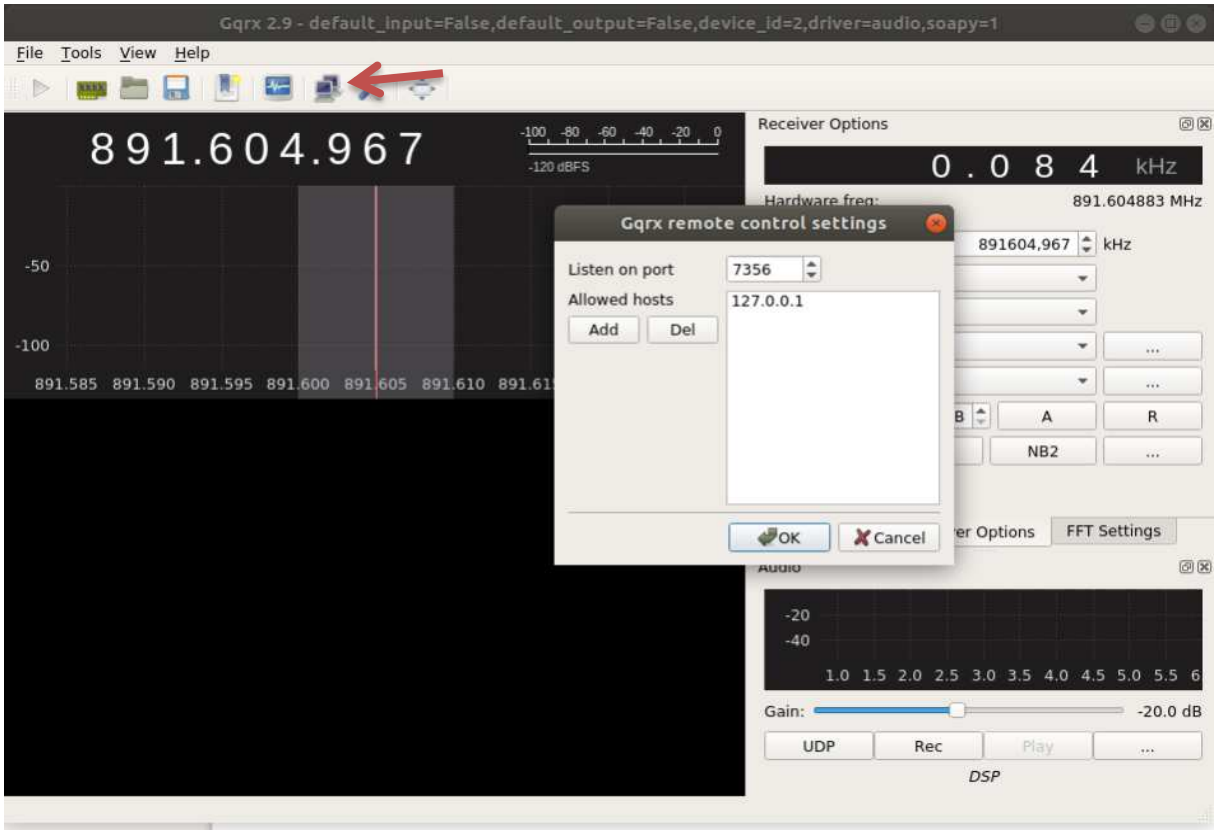


Figura 34. *Configuración Gqrx. Fuente: (Autoría propia).*

Después de esto, se debe ingresar la frecuencia en la parte superior del programa GQRX y ejecutar en con el botón de Play en la parte superior izquierda.

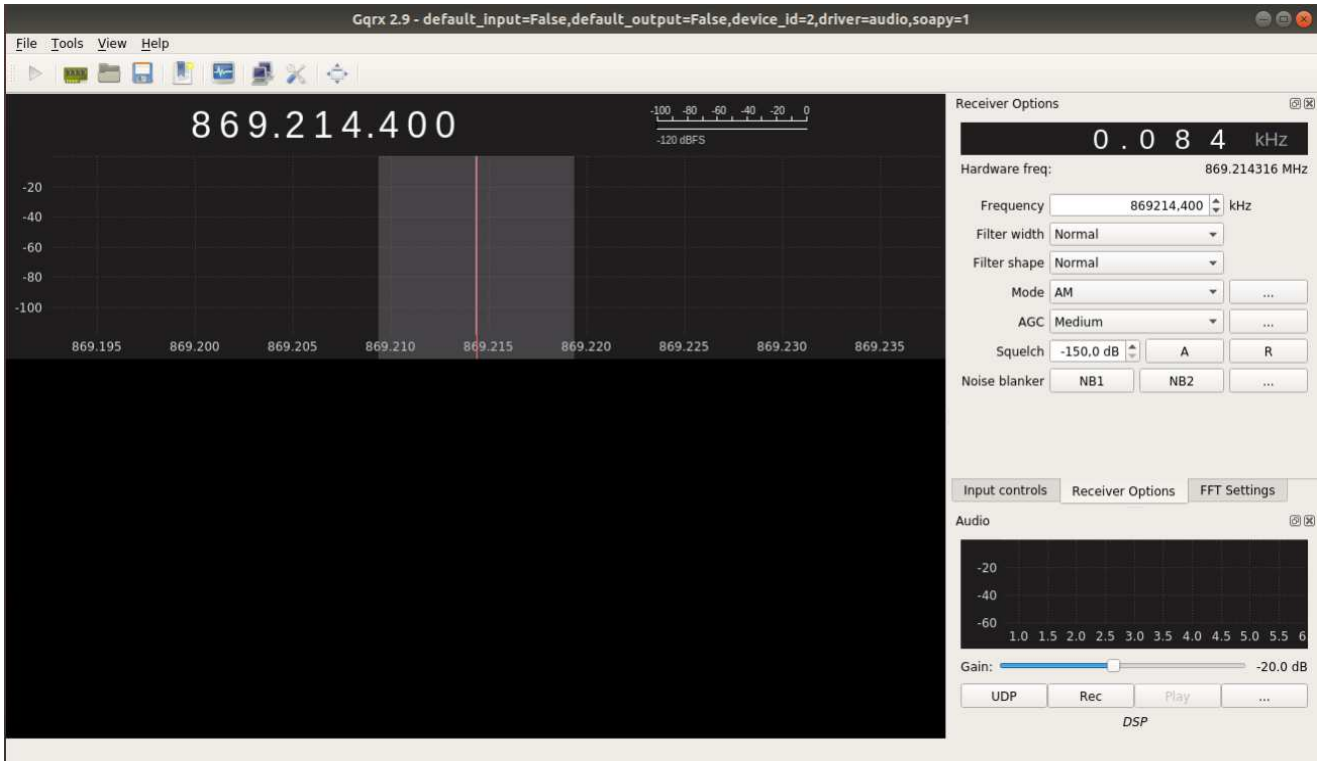


Figura 35. *Configuración frecuencia. Fuente: (Autoría propia).*

Al ejecutar el programa, debe mostrar el espectro, donde con color amarillo se puede diferenciar el tráfico más fuerte sobre esta frecuencia. Esto se realiza con el fin de evidenciar el mayor tráfico sobre el canal para proceder a realizar la decodificación mediante Gr-gsm y Wiresahrk.

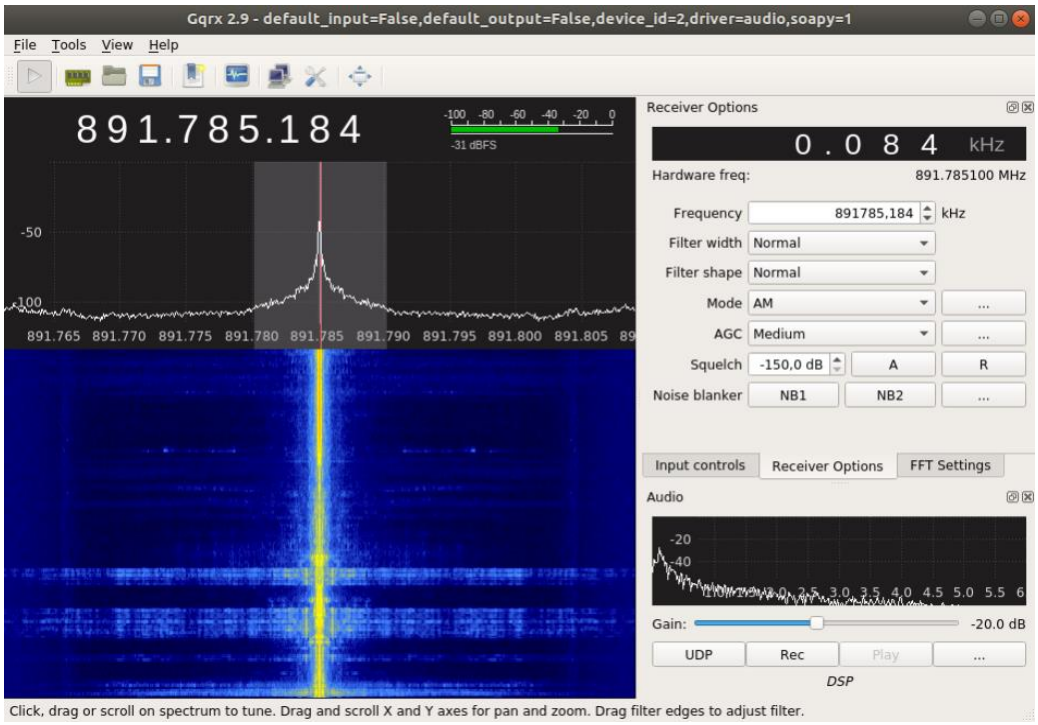


Figura 36. *Muestra de espectro. Fuente: (Autoría propia).*

Después de obtener esta información ya se puede cerrar este programa y abrir el archivo de GNU RADIO companion (con el comando gnuradio-companion grgsm_livemon.gr) con el cual se procederá con la decodificación del canal.

```
root@Maykol1509:/home/maykol/gr-gsm/apps# gnuradio-companion grgsm_livemon.grc
```

Figura 37*. Comando GNURadio. Fuente: (Autoría propia).*

Esta es la ventana que deberá abrir al ejecutar el comando mencionado. Se debe tener en cuenta la configuración mencionada anteriormente (la configuración de los bloques para el análisis de GSM en la banda de 850MHz).

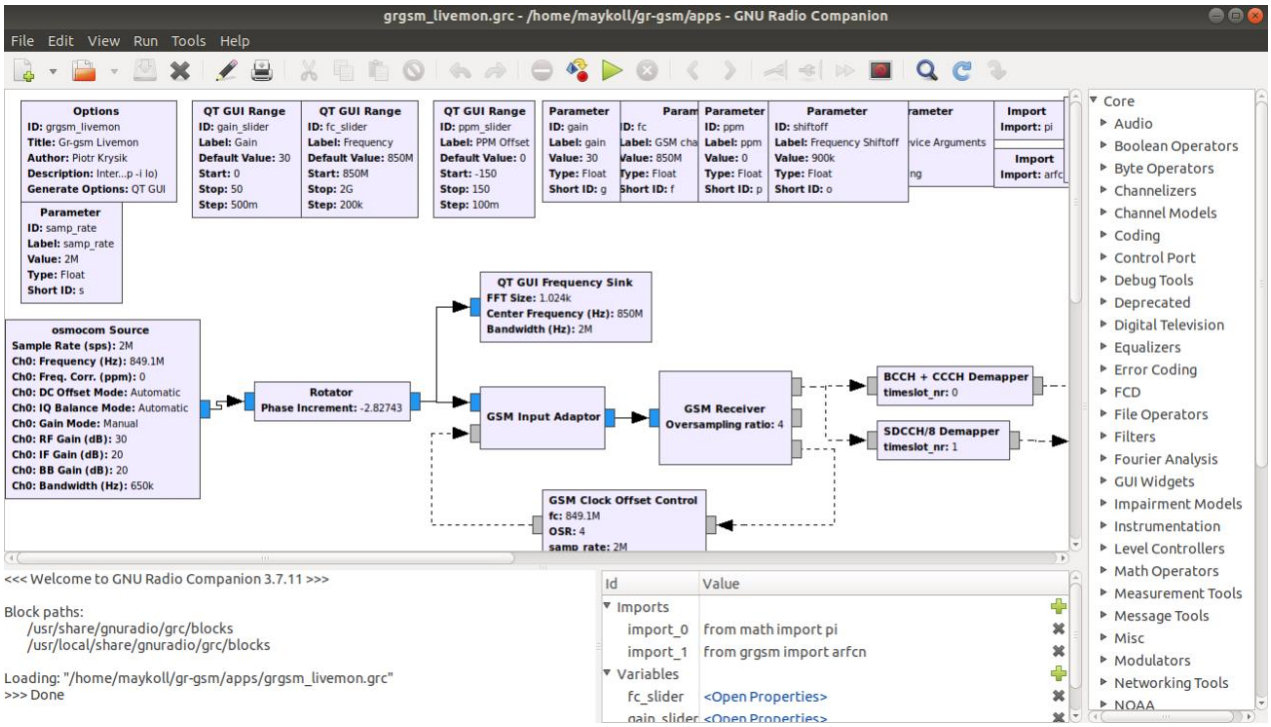


Figura 38. *Bloques GNURadio. Fuente: (Autoría propia).*

Al ejecutar el archivo desplegará una ventana en la cual se mostrará la forma de onda de

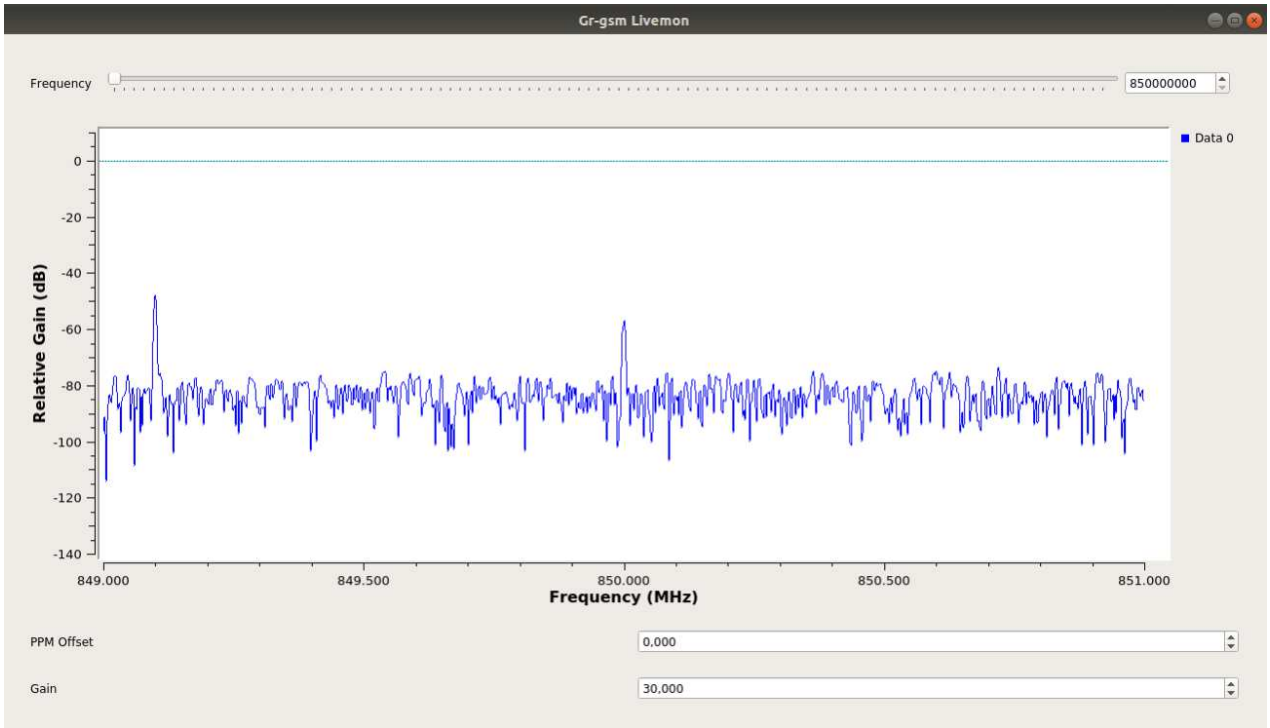


Figura 39*. Frecuencia Gr-gsm. Fuente: (Autoría propia).*

esta señal

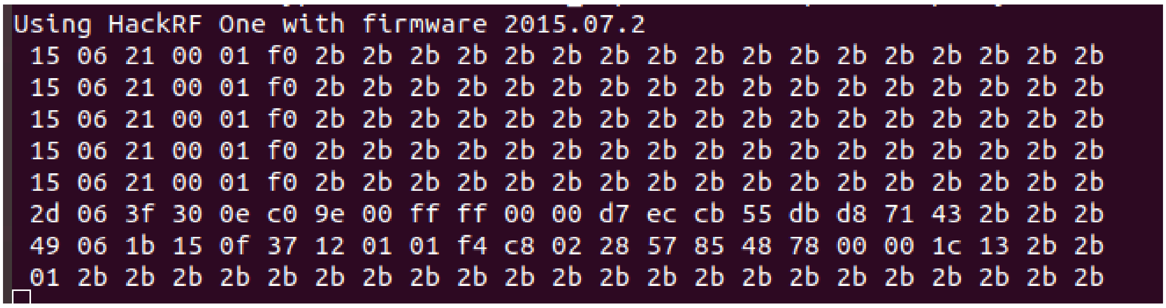


Figura 40. *Gr-gsm decodificación de las tramas. Fuente: (Autoría propia).*

En la parte superior derecha se debe ingresar la frecuencia exacta que se obtuvo con el programa GQRX y dar la tecla enter para que los paquetes de Gr-gsm empiecen a decodificar la información sobre el canal. Al hacer esto en la consola se deben mostrar los paquetes en Hexadecimal, que son lo que contienen las tramas y la información necesaria para que el programa Wireshark decodifique la información. Se debe abrir el Wireshark con el comando wireshark -k -Y 'gsmtap && !icmp' -i lo y de manera automática empezara a obtener las tramas y paquetes de la señal GSM que contiene información como el tipo de canal utilizado, se potencia frecuencia ubicación, entre otras.

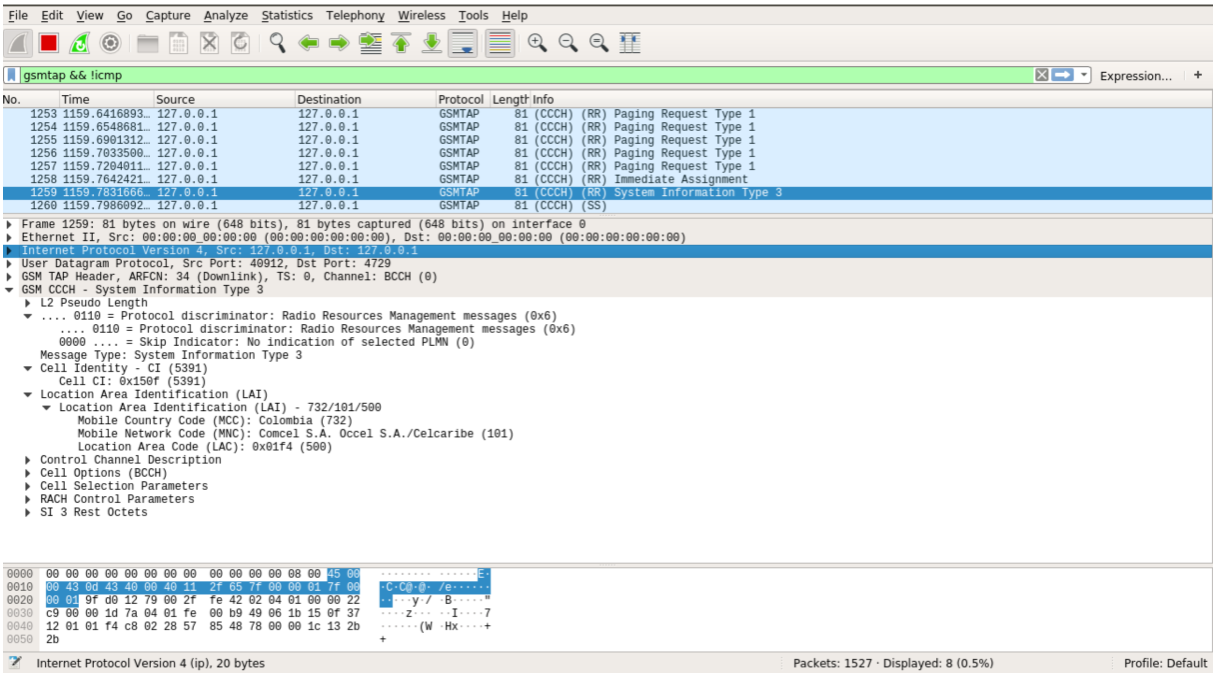


Figura 41. *Wireshark parámetros y decodificación. Fuente: (Autoría propia).*

8.4. medición y análisis de los parámetros de la señal GSM a través de SDR.

Para el desarrollo del proyecto se realizaron mediciones las cuales se generaron en las instalaciones de la Universitaria Uniagustiniana en la plazoleta central un lugar abierto y libre de obstáculos en un horario de 06:00 pm donde hay mucho ingreso de estudiantes al edificio, donde medimos las siguientes frecuencias que se muestran en la tabla.

Tabla 19.

Cuadro de Mediciones.

Canal	Frecuencia MHz	Operador
128	869.2	Claro
130	869.6	Claro
133	870.2	Claro
233	890.2	Claro
235	890.6	Claro

Nota: Fuente: (Autoría propia).

Coordenadas: 4°39'12.28"N, 74° 8'42.56"O

Imaginen tomada desde Google Earth Pro, figura 41.

Figura 42. *Instalaciones Uniagustiniana.* (Earth, 2016).

Teniendo en cuenta que para que Wireshark pueda contener la ráfaga o trama de información este genera un búfer provisional. La cual es enviada a una dirección IP o socket (127.0.0.1:4729) como lo muestra la siguiente figura:

Figura 43. *Trama de información. Fuente: (Autoría propia).*

Es esto lo que permite el acceso al protocolo GSMTAP el cual es utilizado para transportar las tramas de la interfaz aérea de GSM dentro de paquetes UDP/IP.

Esto lo que permite es ya iniciar con el proceso de obtención de datos de cada uno de los sistemas de información (SI).

Los contenidos de cada uno de los SI están distribuidos para que la información crucial se repita con más frecuencia.

Como es el caso del acceso sobre el canal de acceso aleatorio (RACH) en donde la MS comienza a acoplarse a una celda a través de una frecuencia BCCH (Broadcast Control Channel)).

Durante las pruebas se observaron los siguientes SI:

8.4.1. Inmediate assignment (Asignación inmediata) CCCH.

Cuando se activa este (SI) es porque el BSC envía un mensaje de Asignación inmediata a la estación móvil MS. Los parámetros que se visualizan en este (SI) podemos encontrar el Time Slot (ST), Channel Type (CCCH), El número de trama o RFN, Nivel de la señal Signal Level, referencia requerida (número aleatorio (RA) y canal), el avance de tiempo e información de salto de frecuencia. MS escucha continuamente todos los canales CCCH (canales de paginación (PCH) y canales de concesión de acceso (AGCH)) después de enviar un ’Solicitud de canal’ para verificar si se ha recibido la asignación.

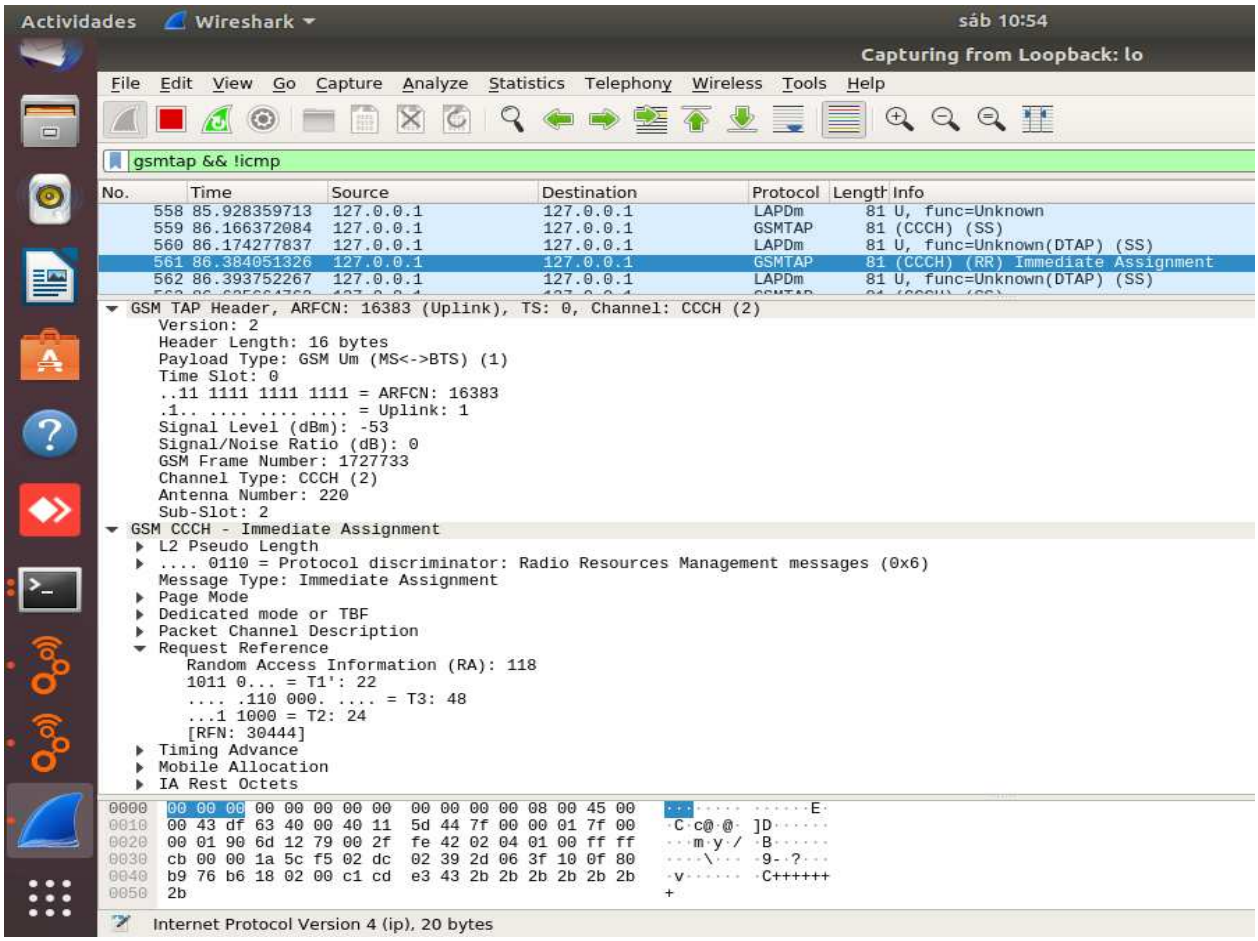


Figura 44. *Canal CCCH. (Autoría propia).*

8.4.2. Paging request type 1 (Solicitud de paginación Tipo 1).

En este SI podemos encontrar el canal de paginación (PCH) y el canal de concesión de acceso (AGCH) los cuales hacen parte de los canales de control común de enlace descendente (CCCH). Contienen una identidad MS que puede ser una identidad temporal llamada Identidad temporal de abonado móvil (TMSI) o una identidad permanente (IMSI).

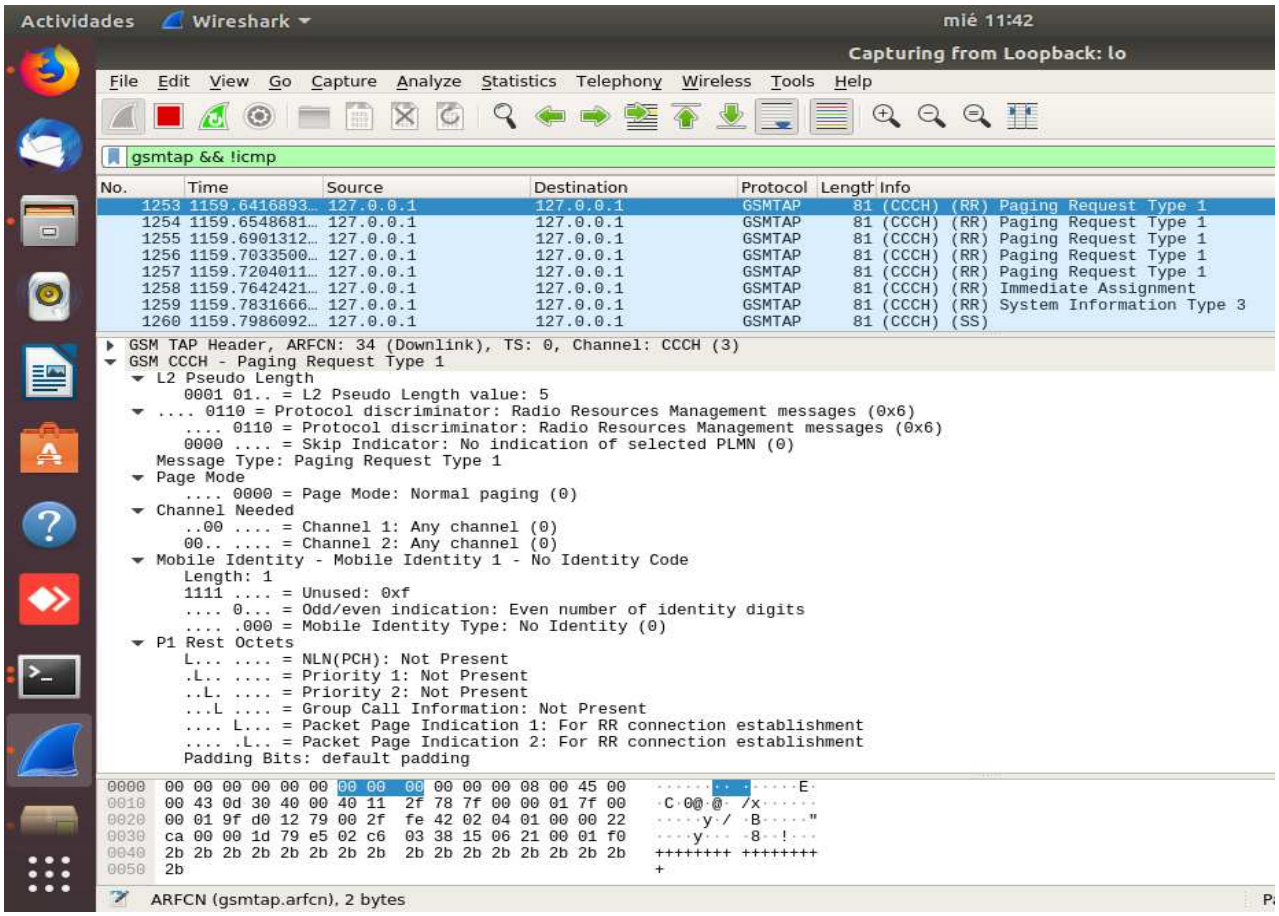


Figura 45. *Paging request type 1. Fuente: (Autoría propia).*

8.4.3. System information type 3 (Sistema de información tipo 3).

Proporciona una identificación del área de ubicación. La identidad global de célda (CGI), identidad de la celda (CI) y la identidad del área de ubicación (LAI). El LAI este valor es emitido a través del BCCH en diferentes (SI). El LAI comprende el Código de país móvil (MCC), el Código de red móvil (MNC) y el Código de área Local (LAC).

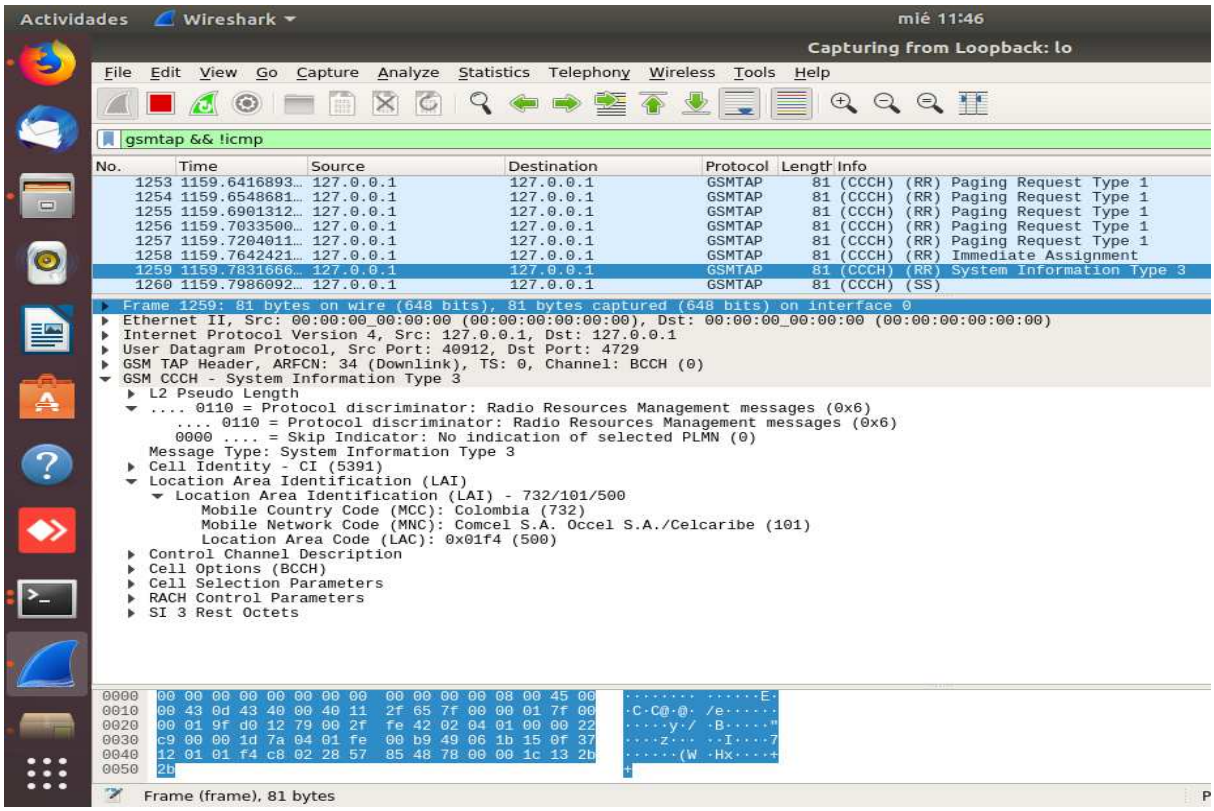


Figura 46. *System information type 3. Fuente: (Autoría propia).*

8.4.4. System information type 4 (Sistema de información tipo 4).

Así como el system infomation Type 3 es (SI) muestra parte de la identidad del área de ubicación (LAI), selección de celda parámetro y (RACH) Control Parámetro, información del sistema 4 proporciona la información sobre la descripción del canal y Asignación. La descripción del canal Se utiliza para proporcionar información de un canal asignado. Junto con su SACCH en el modo dedicado y el móvil. La asignación proporciona información en el caso cuando la frecuencia Se utiliza el salto. Lleva la lista de ARFCNs sobre qué celda Canal de emisión (CBCH) saltos de canal. Como lo muestra la figura.

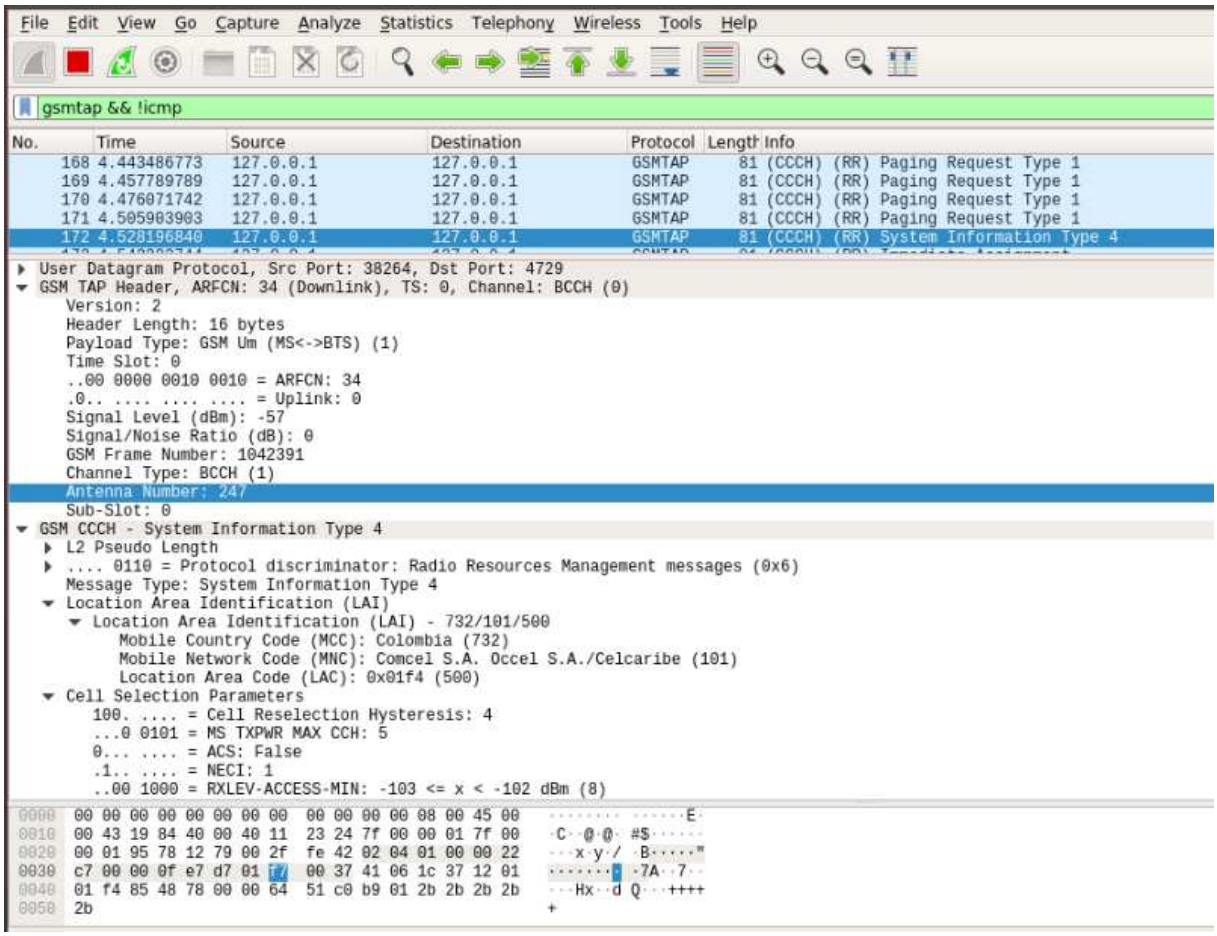


Figura 47*.System information type 4. Fuente: (Autoría propia).*

Teniendo cuenta estos resultados se pueden obtener no menos de alrededor de 14 parámetros los cuales hacen parte de la señal GSM y son poco comunes de ver en un analizador tradicional en la banda de frecuencia de 850 MHz en el operador Claro.

8.4.5. Tabla de parámetros.

La siguiente tabla muestra los parámetros encontrados.

Tabla 20.

Parametros Wireschark

SIGLA	NOMBRE	FUNCION	(SI) ASIGNADO
CCCH	Canales de control Común	Regular el acceso de los terminales al sistema	Paging Request Type 1
PCH	Canal de aviso de llamadas	Permitir a la BTS avisar al móvil que hay una llamada entrante hacia el terminal	Paging Request Type 1

AGCH	Canal de reconocimiento de acceso	Procesa la aceptación o no de la BTS la petición de acceso del móvil, y asigna canal dedicado	Paging Request Type 1
BCCH	Canal de control de broadcast	Comunica desde la estación base al móvil la información básica del sistema como Frecuencias, Combinación de canales, BTS vecina	System Information Type 3
CBCH	Canal de emisión	Trasmite mensajes de difusión celular	System Information Type 4
SACCH	Canal de control asociado lento	Transmite información rutinaria relativa a la llamada en curso, como mediciones, tiempo y calidad de canal	System Information Type 4
RACH	Canal de acceso aleatorio	Alberga las peticiones de acceso a red móvil a la BTS	System Information Type 4
ARFCN	Numero de canal de frecuencia absoluta	Número de canal asignado	System Information Type 4
MCC	Código de país del móvil	Muestra el código asignado al país	System Information Type 3
MNC	Código de operador del móvil	Muestra el código asignado al operador	System Information Type 3
LAC	Código de área local	Identificador de la red del operador dentro del país	System Information Type 3
RACH	Canal de acceso aleatorio	Alberga las peticiones de acceso a red móvil a la BTS	System Information Type 4

MCC	Código de país del móvil	Muestra el código asignado al país	System Information Type 3
MNC	Código de operador del móvil	Muestra el código asignado al operador	System Information Type 3
LAC	Código de área local	Identificador de la red del operador dentro del país	System Information Type 3
ST	Time Slot -	Intervalo de tiempo necesario	Inmediate Assignment
RFN	Numero de trama	Código de trama asignado	Inmediate Assignment

Nota: Fuente: (Autoría propia).

Figura 48. *Mediciones realizadas en la semana de la Ingeniera Uniagustiniana. Fuente: (Autoría propia).*

Conclusiones

Se ha logrado realizar la investigación de los parámetros que se pueden medir mediante el SDR con la correcta configuración de sus variables.

se establece y exponen los requisitos necesarios a nivel físico y lógico para la implementación del modelo desarrollado, teniendo en cuenta sus versiones y variables para lograr el correcto funcionamiento. Los softwares libres que se implementaron en la investigación permiten comprender de manera más clara la señal GSM, la forma que maneja y se visualiza el espectro, haciendo para el estudiante un aprendizaje más dinámico contribuyendo a su aprendizaje en los programas de comunicaciones móviles y sistemas inalámbricos.

las configuraciones necesarias se determinan de manera exitosa teniendo en cuenta las variables que pueden tomar. El SDR es una herramienta completa que permite realizar y otros tipos de montajes que permite realizar el estudio de esta y otras señales complejas siempre y cuando se realicen las correctas configuraciones y se cuenten con las herramientas tanto físicas como lógicas para lograrlo.

Con las pruebas realizadas con el modelo de medición implementado se lograron tomar datos y parámetros que permiten comprender mejor el funcionamiento de la señal GSM, como pueden ser los tipos de canales, protocolos que utiliza, tipos de acceso a la red, códigos que utiliza para la ubicación del abonado, entre otros.

Partiendo de la idea de contribuir con el proceso educativo, el modelo implementado logrará que los estudiantes de la carrera logren tener un punto de partida hacia el análisis y estudio de la señal GSM. Tomando como referencia el modelo de medición aquí descrito, se puede tomar como punto de partida para realizar un análisis más complejo y profundo, así como también descifrar la información que se transmite por este medio, con fines académicos y de aprendizaje.

Dado los resultados que se evidencian en el software Wireshark con parámetros encontrados, que se captaron en la señal GSM la cual se trabajó en la banda de frecuencia 850 MHz del operador claro, estos están ubicados en el system information type 3 que es donde esta la información de localización y parámetros como LAC para el caso de claro es 500, el MCC en Colombia con el 732 y otro parámetro importante es el MNC que indica las propiedades del operador para claro Colombia es el 732, además se encuentran los parámetros de canales lógico de control, las tramas y protocolos usado por la red GSM, con estos parámetros se entiende de una manera más clara las características y comportamientos de la señal mediante el uso de SDR.

Recomendaciones

Durante la investigación se observa la gran importancia que tienen las señales móviles GSM para las redes inalámbricas siendo esta la base de las comunicaciones móviles, se recomienda profundizar nuevos aspectos con la herramienta del SDR que se encuentra en el laboratorio ayuda al estudiante a ampliar sus conocimientos de una forma más didáctica.

En el proyecto de investigación se puede expandir a futuro revisando nuevas bandas de frecuencias en las señales y desarrollando más ideas sobre la red móvil GSM, como podrá ser una estación base.

Los softwares de radio libre son muy útiles para el conocimiento de las señales digitales se recomienda implementarlos más seguido en las diferentes materias relacionadas con la temática será de gran provecho.

El Software definido por radio es una herramienta muy útil que beneficiara a los estudiantes de ingeniería en telecomunicaciones de la Universitaria Uniagustiniana, se recomienda adecuar un laboratorio completo con practica de todo tipo de señales inalámbricas, con la implementación de los softwares libres.

Se recomienda a los profesores de redes móviles o inalámbricas implementar el modelo de mediciones de señales GSM mediante SDR para los estudiantes, esta investigación les ayudara a profundizar sus conocimientos y comprender de una manera más didáctica un tema de gran importancia para su futuro profesional como son las comunicaciones móviles y sus propiedades al igual de investigar sobre las siguientes tecnologías como los son UMTS y LTE.

Referencias

(ANE), A. N. (Julio de 2016). *Cuadro Nacional de atribuciones de bandas de frecuencia.* Obtenido de https://www.ane.gov.co/images/ArchivosDescargables/Planeacion/cnabf/cnabf.pdf.

A. Silva, G. M. (2003). *Performance analysis for data service in third generation mobile telecommunication networks.* Brasilia: Federal university od minas Gerais.

Alcantu, Y. (2015). *Ingeniería Electrónica, Automática y Comunicaciones. Vol. 36 No1.* La Habana: EAC ISSN 1815-5928.

Almagro, L. (2008). *cere.ugr.es*. Obtenido de Tutorial de la capa fisica en Comunicaciones Moviles: http://ceres.ugr.es/~alumnos/tutorialcfcm/dos.html

Amador, J. A. (2013). *Radio Definido por Software.* Revista Telematica Vol.12 No 2 ISSN 1929-3804.

apps., A. p. (2014). *Generaciones de tecnologias moviles*. Obtenido de https://www.androidestudio.com/2014/10/generaciones-de-las-tecnologias-moviles.html

Arguello, H. (2013). *Desing and implementation of a wireless software defined radio testbed.* rec. fac . nac. minas.

Artes, A. (2012). *Comunicaciones digitales.* Pearson Educacion/Prentice Hall.

Bryon, S. y. (2013). *Captura GSM, decodificacion con USRP y SDR.* Obtenido de https://docs.google.com/document/d/1E_LQZ0xTs697L-0QsANQ7sDzc09QhO_7q4ue_WXezI0/pub

Callado, C. F. (2010). *Metodologia de la investigacion.* Mexico: ISBN 978-607-15-0291-9.

colombia, S. d. (1990). *Ministerios de las comunicaciones*. Obtenido de ww.secretariasenado.gov.co/senado/basedoc/ley_0037_1993.html

Comunicaciones, C. n. (2017). *Caida de llamadas.* Bogota.

Earth, G. (17 de 1 de 2016). *Google Earth Pro*.

Eduardo Gaona, M. A. (2014). *Aproximacion de la calidad de voz y cobertura en una red GSM de emergencia, Vol. 24.* Cienc. Ing Neogranad.

Escobar, D. (08 de 07 de 2013). *OpenBTS y Asterisk*. Obtenido de http://hotfixed.net/wp-content/uploads/2013/07/msc1.jpg

greatscottgadgets. (2009). *greatscottgadgets.com.* Obtenido de https://greatscottgadgets.com/hackrf/

Harald. (2010). *Wiki.wireshark*. Obtenido de https://wiki.wireshark.org/GSMTAP.

HaraldWelte. (08 de 2010). *wiki.wireshark.org.* Obtenido de https://wiki.wireshark.org/GSMTAP

Hernandez, L. F. (2005). Plataforma para servicios de valor agregado basados en localización, en una red GSM, a partir de la medición de la intensidad de señal. *Revista de la Facultad de Ingeniería Universidad Central de Venezuela*.

Huawei. (2018). Servicios en auge como evolución de la red. *8vo congreso internacional del espectro* (pág. 3). Bogota: ANE.

Huidobro, J. M. (2015). *Telecomunicaciones Tecnolgias, redes y servicios.* Bogota: Ediciones de la U.

ITU-R. (1997).

ITU-R. (2015). *RECOMENDACIÓN UIT-R M.1036-5.*

Machado, J. (2015). Software Defined Radios: Basic principles and applications. *Faculta de ingenieria* , Vol. 24 No 38 Pag. 76 - 96.

Masum, S. (Mayo de 2013). *The structure of a GSM network, GSM System has three subgroups.* Obtenido de The structure of a GSM network [14] GSM System has three subgroups [15]

Miguel Angel, C. S. (2017). Opportunities to implement Software Defined Radio in network. *Faculta de ingenieria.*, 26.

Navarro, J. G. (Abril de 2007). *bibing.* Obtenido de http://bibing.us.es/proyectos/abreproy/11425/direccion/Memoria%252F

Ornetta, I. (s.f.). *La telefonia movil y su salud*. Obtenido de http://www.who.int/peh-emf/publications/en/esp_mobphonehealthbk.pdf

Poole, I. (2014). *Radio-Electronics.com*. Obtenido de GSM band allocations: https://www.radio-electronics.com/info/cellulartelecomms/gsm_technical/gsm-frequency-frequencies-bands-allocations.php

portal.mtc. (s.f.). *http://portal.mtc.gob.pe*. Obtenido de http://portal.mtc.gob.pe/comunicaciones/autorizaciones/servicios_privados/modalidades_servicios.html

privado, M. d. (s.f.). *Servicio Movil terreste*. Obtenido de http://portal.mtc.gob.pe/comunicaciones/autorizaciones/servicios_privados/modalidades_servicios.html.

Rabanos, J. (2004). Comunicaciones moviles. Universitaria Ramonarece.

Resch, B. (01 de 2015). *ResearchGate*. Obtenido de https://www.researchgate.net/figure/Positioning-Based-on-Cell-Identity-and-Timing-Advance_fig8_237748405

rfwireless. (2012). ARFCN calculator. *RF Wirelees World*, http://www.rfwireless-world.com/calculators/GSM-ARFCN-frequency-converter-calculator.html.

spectrummonitoring.com. (14 de Agosto de 2016). Obtenido de https://www.spectrummonitoring.com/frequencies/frequencies2.html#Colombia

Tispain . (05 de 2015). Obtenido de https://www.tispain.com/2015/05/como-se-conectan-los-telefonos-moviles.html

Tude, E. (2002). *http://www.teleco.com.br.* Obtenido de http://www.teleco.com.br/es/tutoriais/es_tutorialgsm/pagina_2.asp

Wikipedia. (2012). *Wikipedia*. Obtenido de https://es.wikipedia.org/wiki/Sistema_global_para_las_comunicaciones_m%C3%B3viles

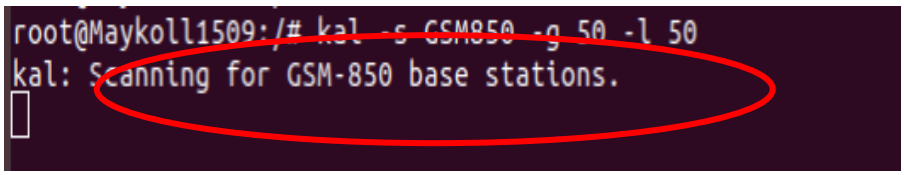
Anexos

Anexo 1. Instructivos para capturar la señal GSM.

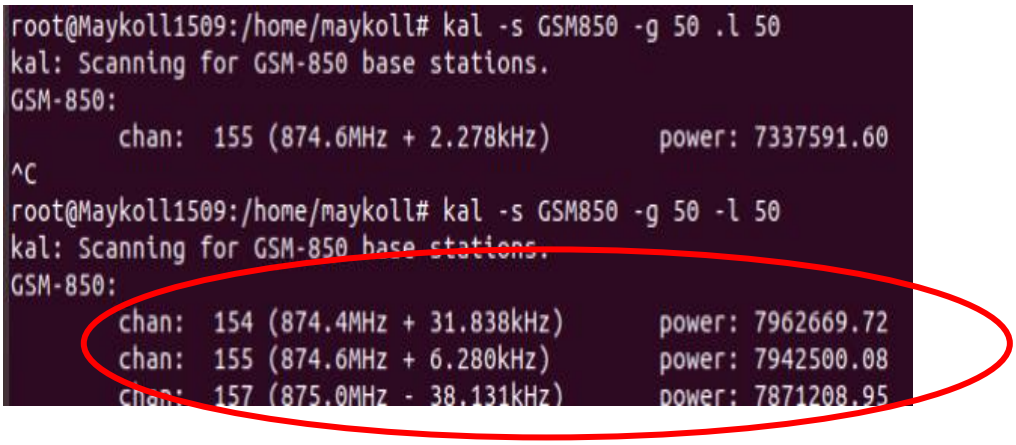
En el siguiente documento presentaremos de forma detalla el paso a paso para lograr capturar la señal GSM, decodificarla y lograr obtener los diferentes parámetros que no muestra el software final.

Después de haber descargado los paquetes, librerías y programas necesarios para realizar la decodificación de tramas de señales GSM, se procederá a explicar detalladamente el proceso a seguir para lograrlo.

Para empezar, en la consola del sistema operativo Ubuntu, se ingresa el comando *kal -s GSM850 -g 50 -l 50* (*sudo kal -s GSM850 -g 50 -l 50* para cuando no se está en super usuario (root)), para utilizar el programa Kalibrate para escanear los canales disponibles de GSM en la banda de 850MHz para iniciar el análisis y decodificación de paquetes GSM.



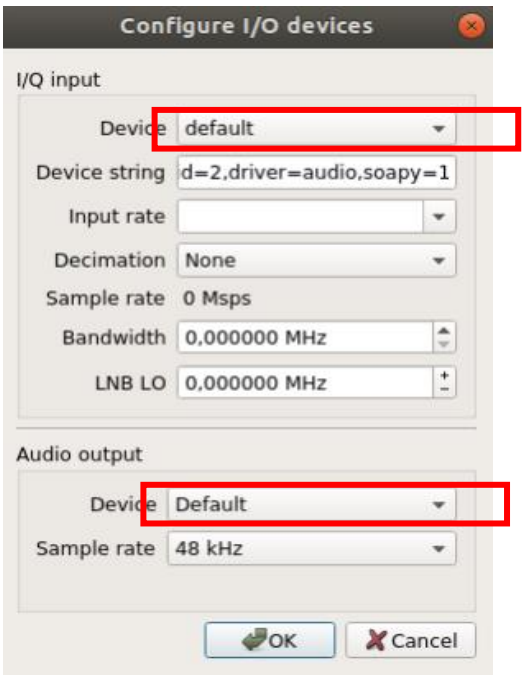
Al ejecutar este comando se obtienen los canales con su respectiva frecuencia y potencia, como se muestra a continuación.



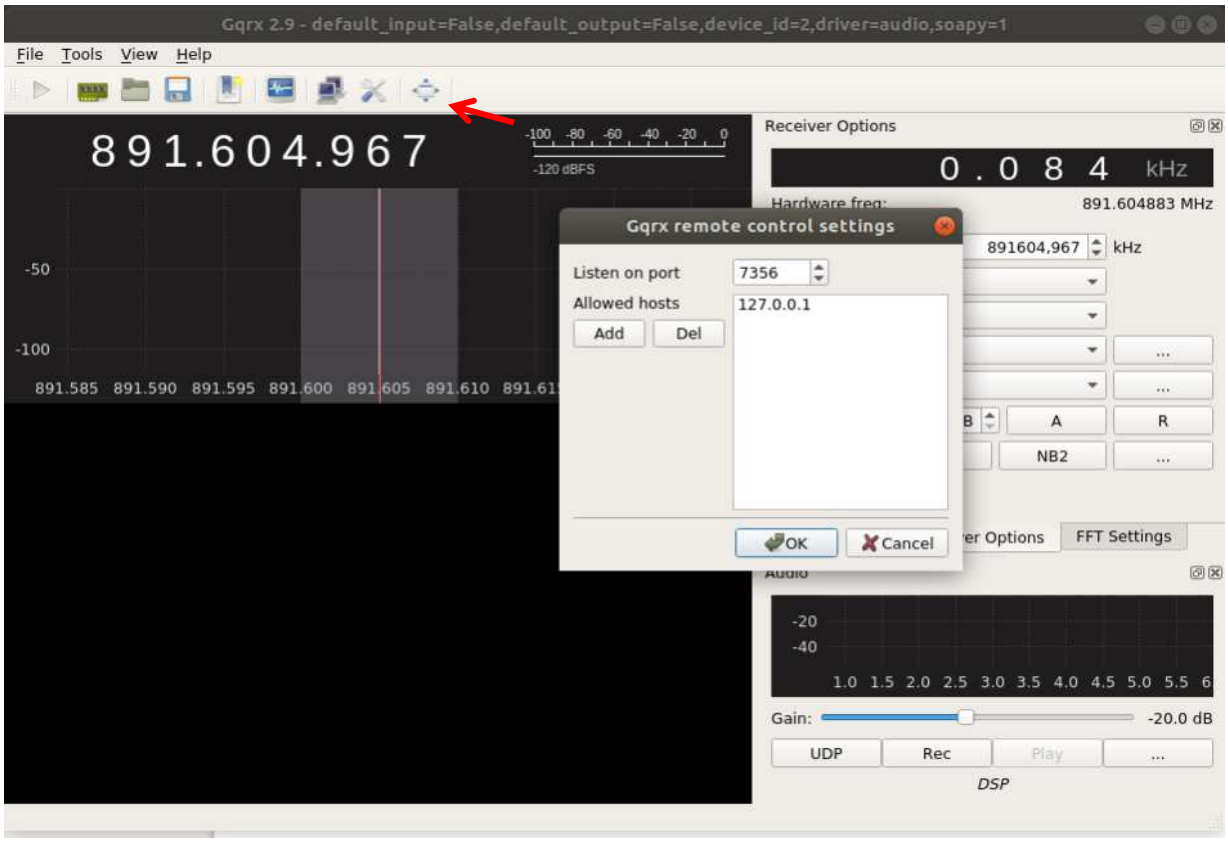
Posterior a obtener esto, se procede a abrir el analizador de espectro GQRX para evidenciar el tráfico sobre alguna de las frecuencias obtenidas con anterioridad. Tener en cuenta que el comando se debe ejecutar como super usuario para obtener los resultados esperados.

```
root@Maykoll1509:/home/maykoll# gqrx
```

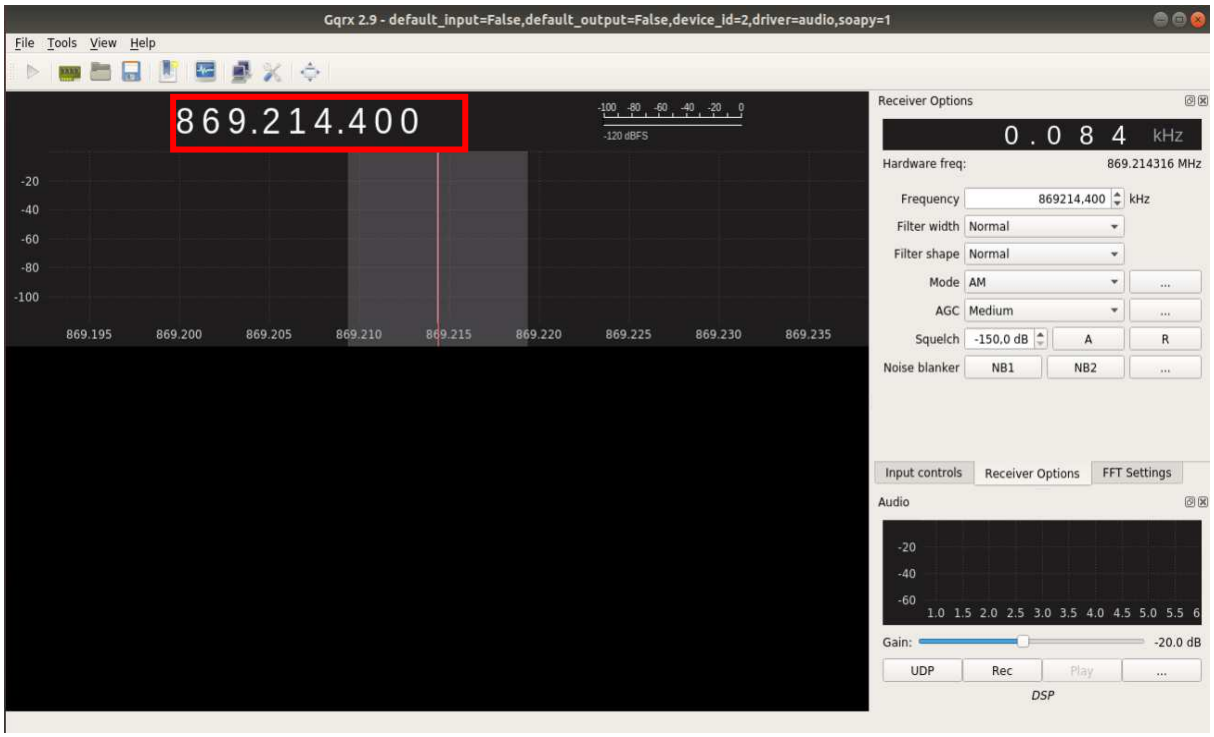
Al ejecutar el programa, se desplegará una pantalla una ventana como se muestra continuación, en la cual, se debe tener en cuenta que el dispositivo debe estar en Default, tanto en I/Q input como en Audio Output.



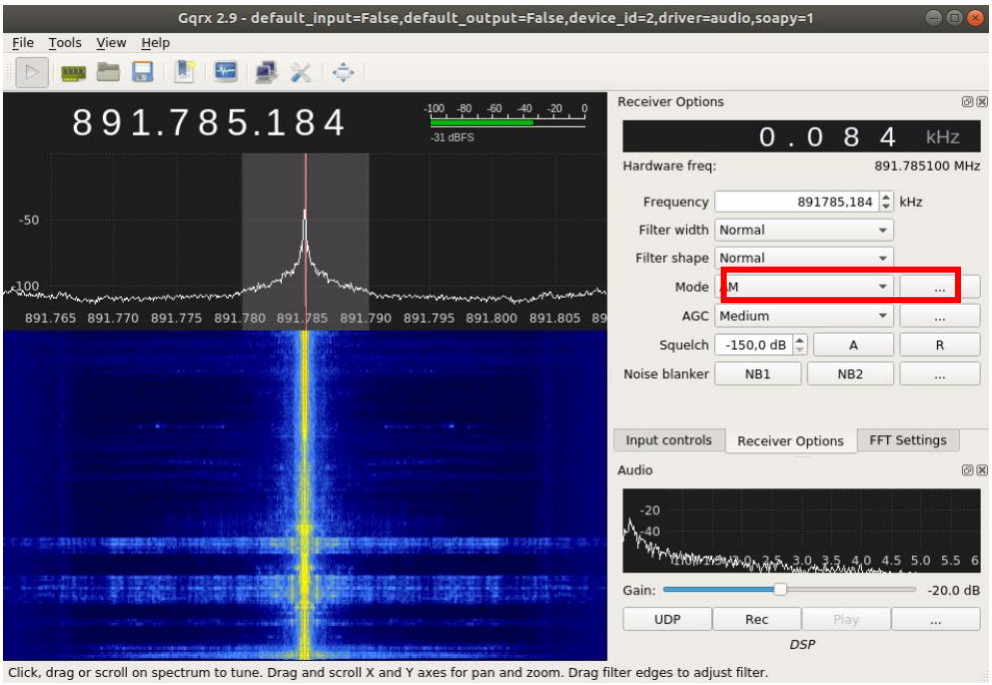
Al ingresar al programa, en el recuadro de configuración de control remoto, se debe tener, en Listen on Port el puerto 7356 y en Allowed Hosts la dirección IP 127.0.0.1, esto con el fin de observar el tráfico sobre el canal de GSM.



Después de esto, se debe ingresar la frecuencia en la parte superior del programa GQRX y ejecutar en con el botón de Play en la parte superior izquierda



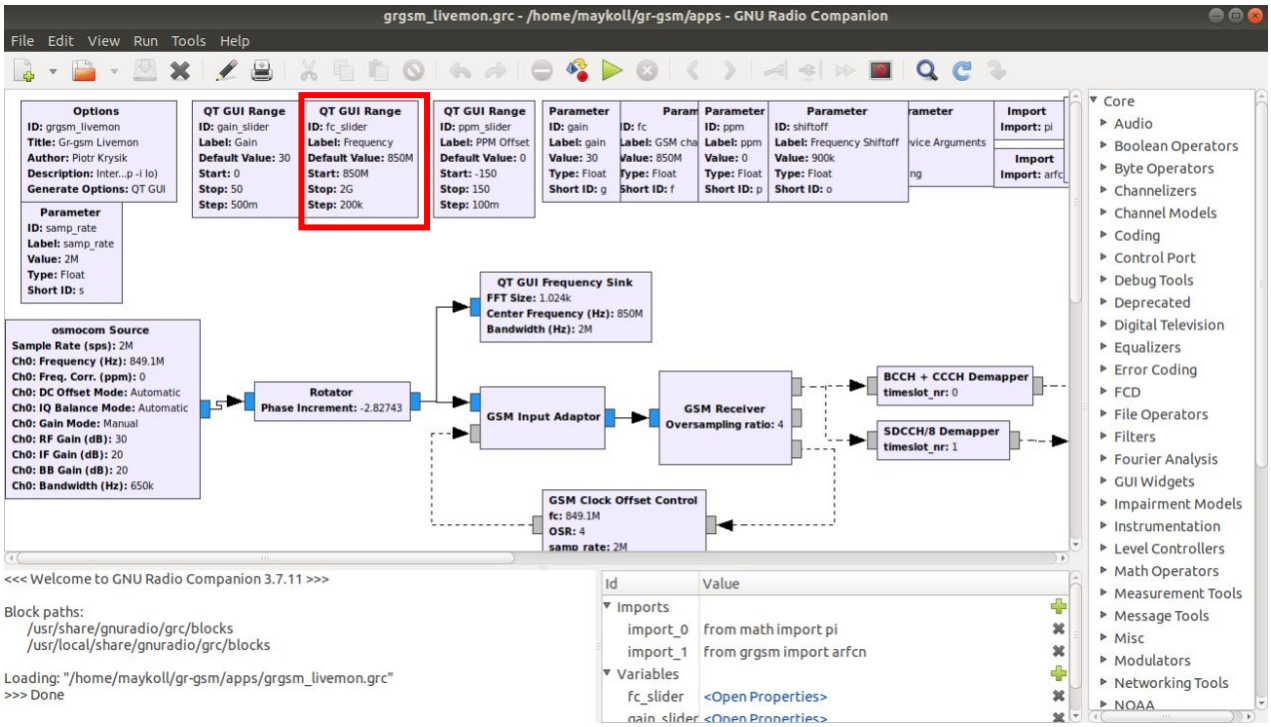
Al ejecutar el programa, debe mostrar el espectro, donde el color amarillo se puede diferenciar el tráfico más fuerte sobre esta frecuencia. Esto se realiza con el fin de evidenciar el mayor tráfico sobre el canal para proceder a realizar la decodificación mediante Gr-gsm y Wiresahrk. Tener en cuenta el recuadro "Mode" el cual debe estar en AM antes de proceder con la decodificación.



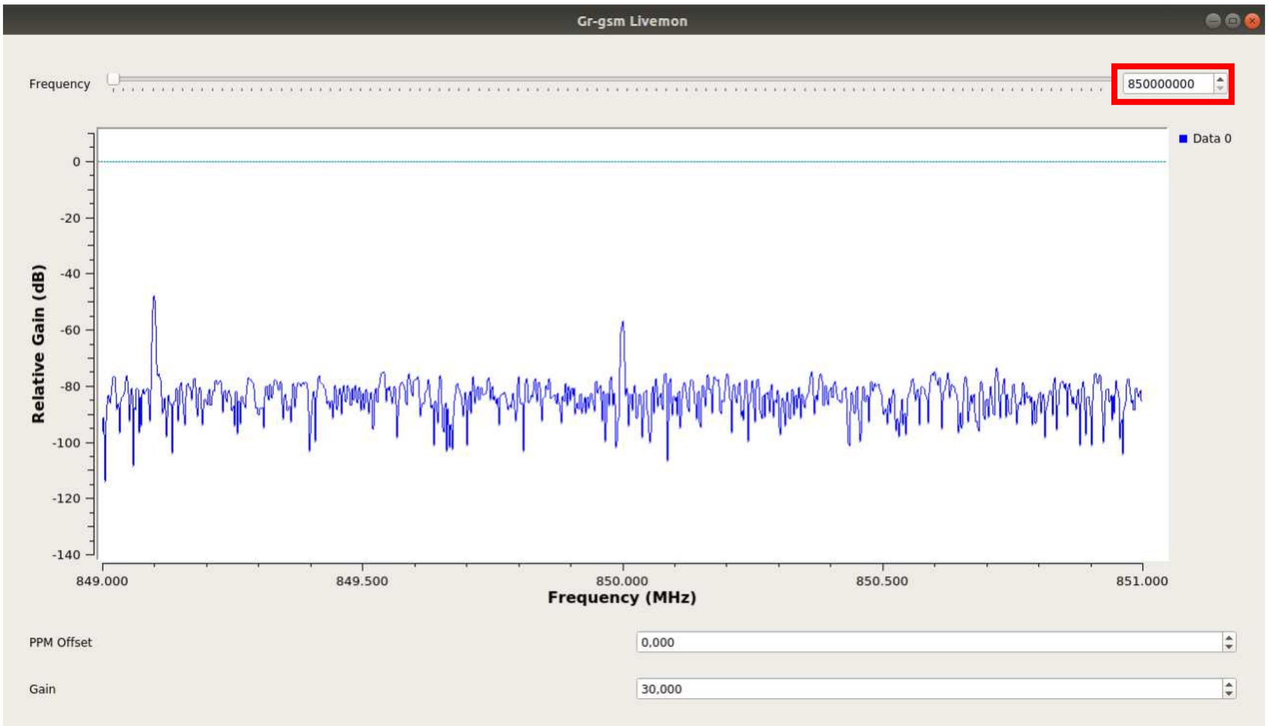
Después de obtener esta información ya se puede cerrar este programa y abrir el archivo de GNU RADIO companion (con el comando *gnuradio-companion grgsm_livemon.gr*) con el cual se procederá con la decodificación del canal.

```
root@Maykol1509:/home/maykol/gr-gsm/apps# gnuradio-companion grgsm_livemon.grc
```

Esta es la ventana que deberá abrir al ejecutar el comando mencionado. Antes de ejecutar el programa se debe tener en cuenta el recuadro señalado ya que, por defecto, viene con una frecuencia diferente a la que se utiliza en territorio colombiano. Es por esto que se debe verificar y cambiar la frecuencia de inicio a 850MHz (850e6).



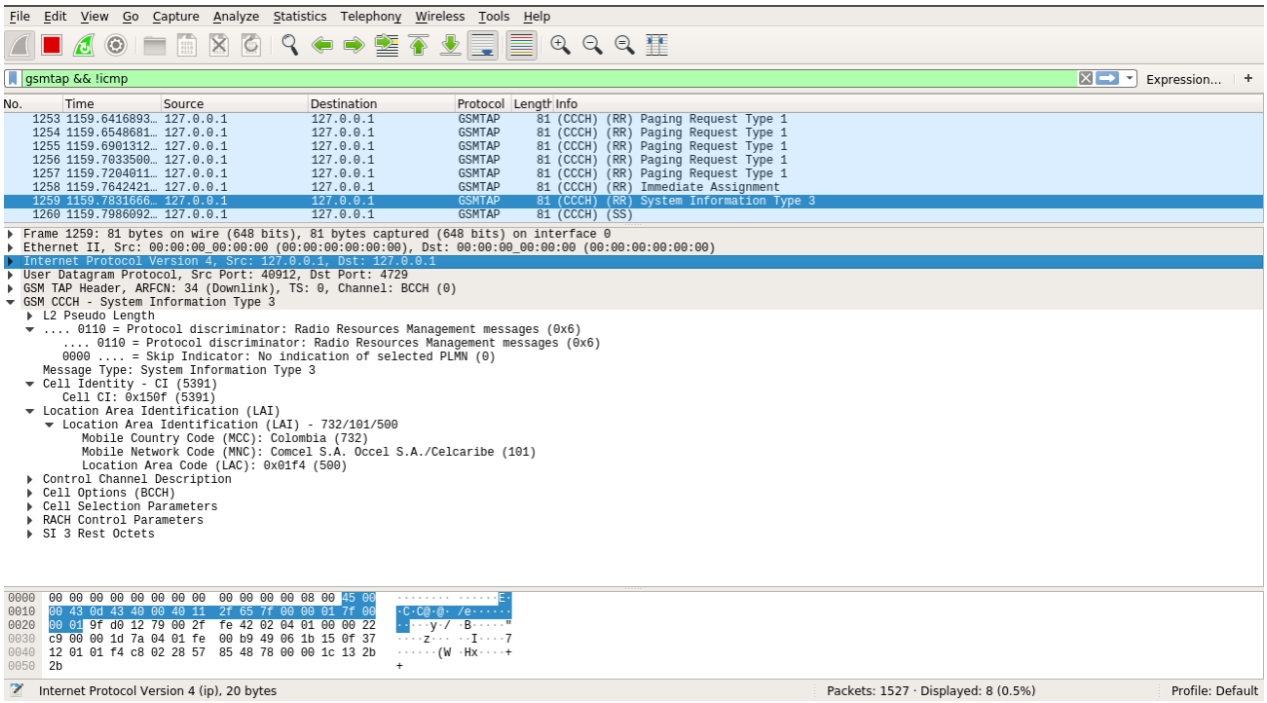
Después de esto, procedemos a ejecutar el programa, con lo cual se abrirá una ventana como se muestra a continuación. Es esta, en la parte superior derecha se debe ingresar la frecuencia exacta que se obtuvo con el GQRX (el mayor tráfico sobre el canal) para que el programa GR-GSM empiece a decodificar la señal.

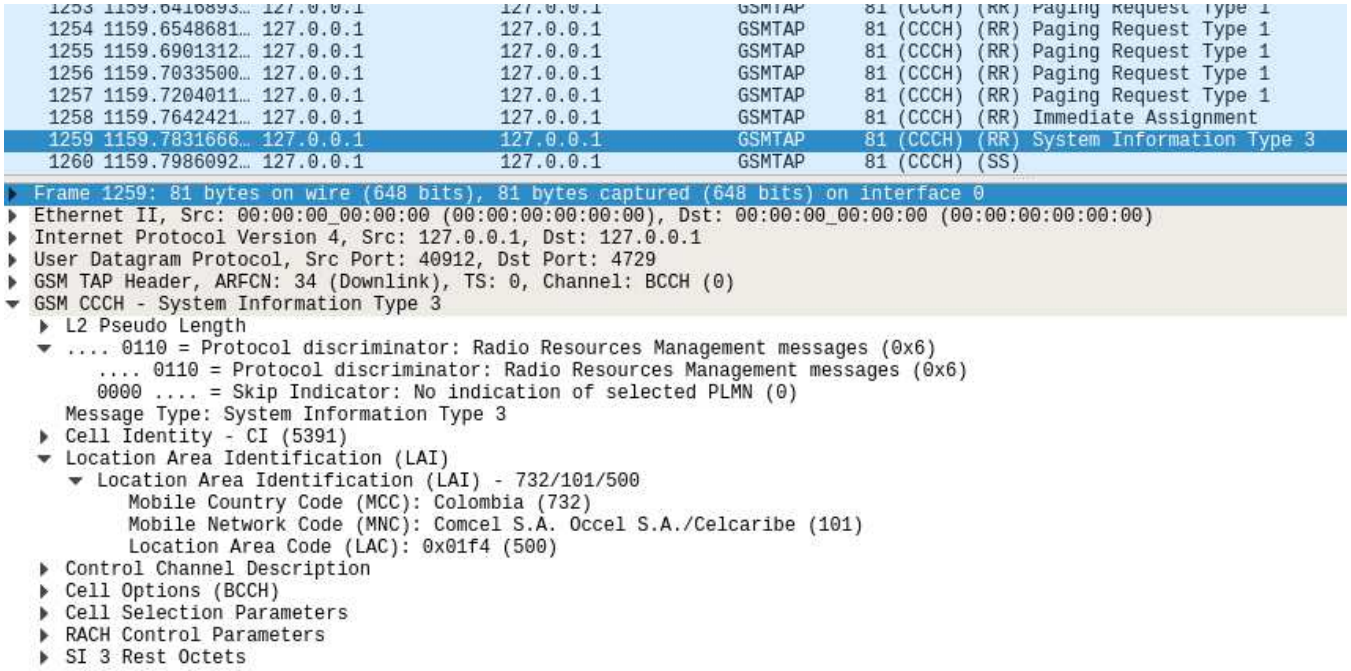


Una vez ingresada la frecuencia, se da en el botón enter para que inicie el proceso de decodificado de la señal. Una vez hecho esto el programa iniciara el proceso.

```
Using HackRF One with firmware 2015.07.2
 15 06 21 00 01 f0 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
 15 06 21 00 01 f0 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
 15 06 21 00 01 f0 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
 15 06 21 00 01 f0 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
 15 06 21 00 01 f0 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
 2d 06 3f 30 0e c0 9e 00 ff ff 00 00 d7 ec cb 55 db d8 71 43 2b 2b 2b
 49 06 1b 15 0f 37 12 01 01 f4 c8 02 28 57 85 48 78 00 00 1c 13 2b 2b
 01 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
```

Lo que se debe hacer es abrir otra consola, e ingresar el comando *wireshark -k -Y 'gsmtap && !icmp' -i lo* (preferiblemente como super usuario) para abrir el wireshark para analizar cada uno de los paquetes por separado y evidenciar la información que cada uno de estos contiene.

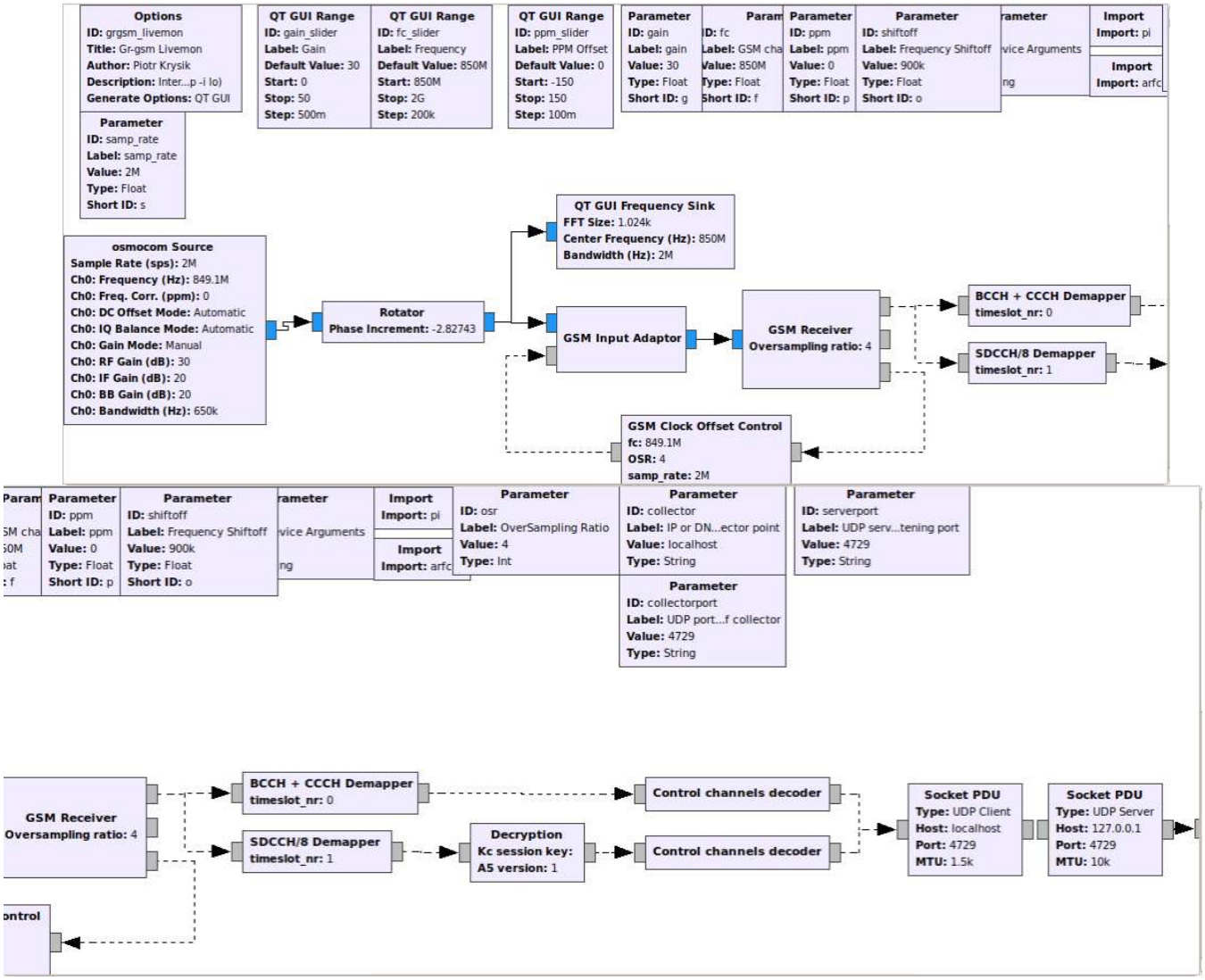


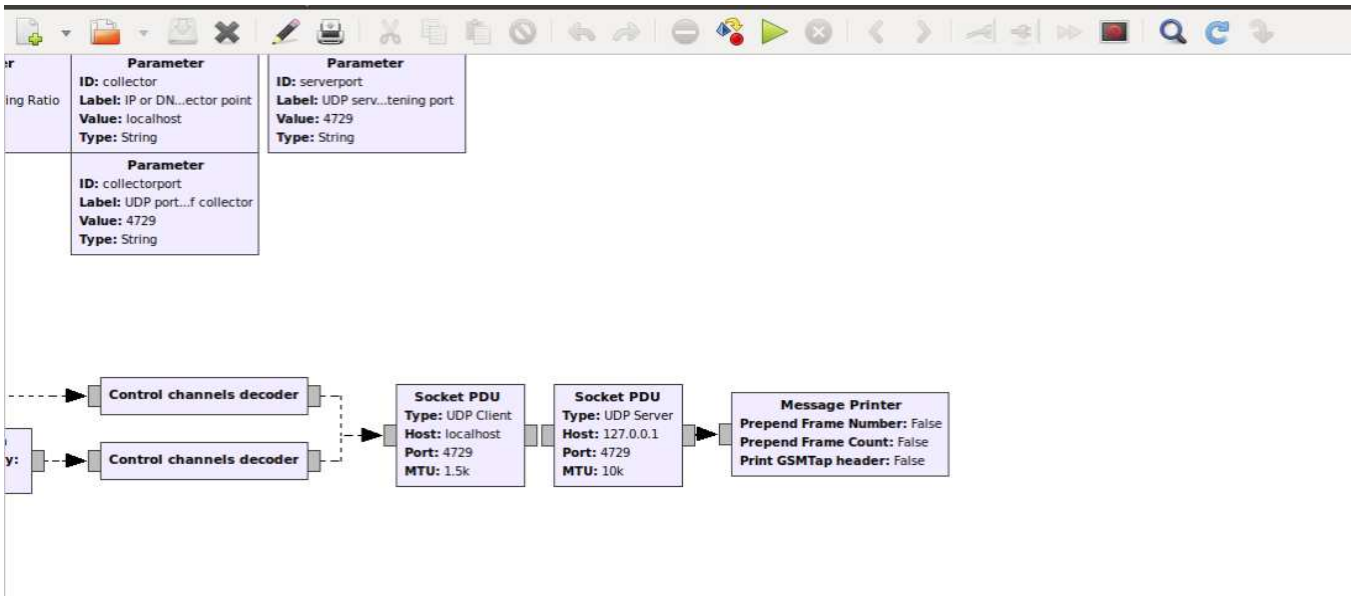


De esta manera encontraremos los parámetros de una señal GSM.

Anexo 2. Diagrama usado

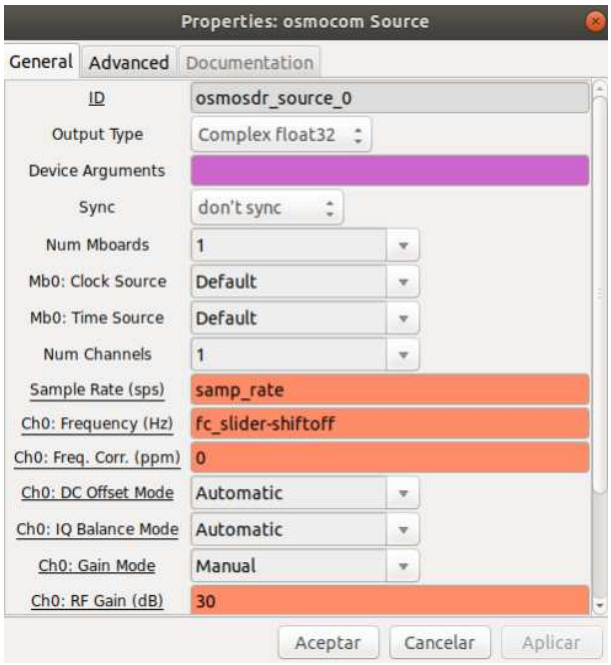
A continuación, encontraremos el diagrama de bloques de GNURadio-compaion grgsm_livemon.



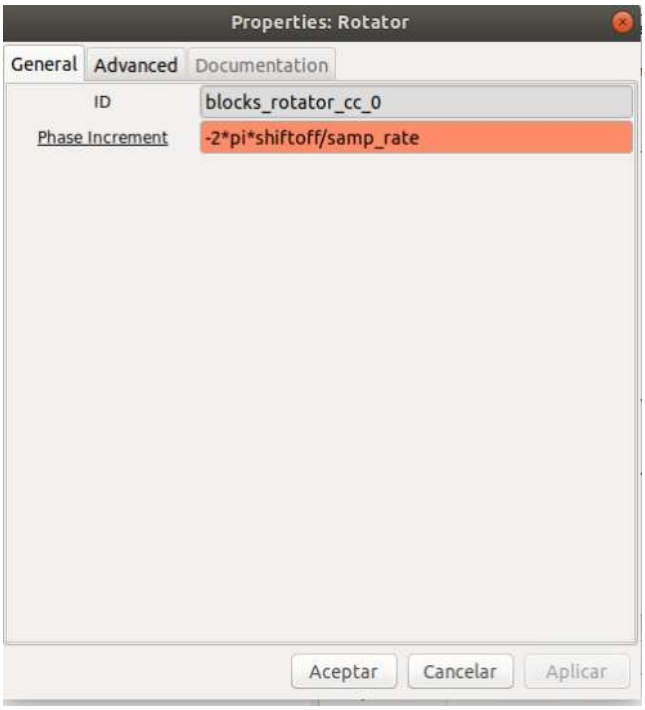


Configuración de los bloques en GNURadio

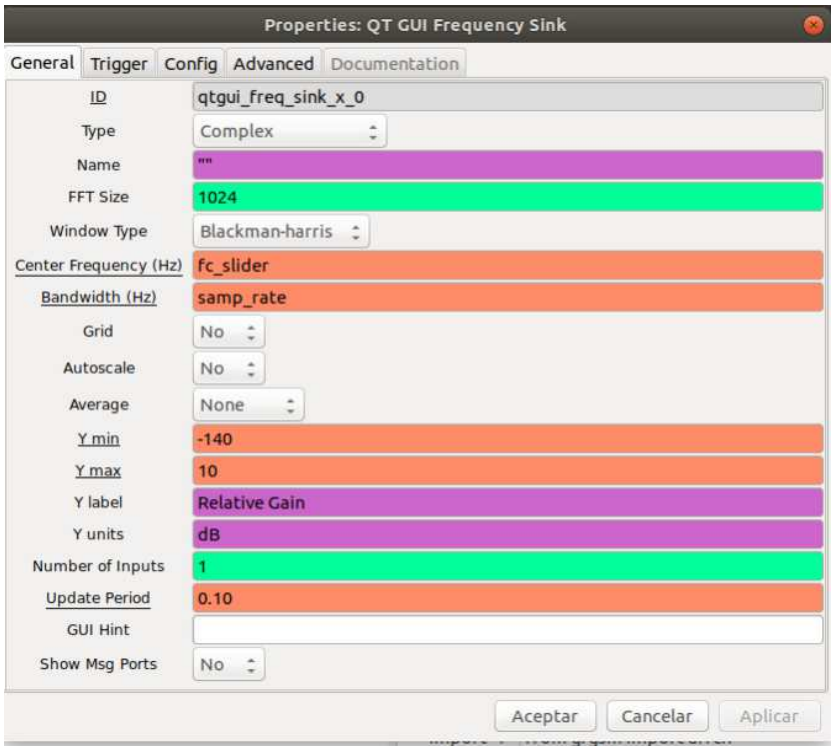
OSMOCOM SOURCE: El bloque *osmocom source* actúa como una interfaz entre la programación realizada y el hardware utilizado. Lo que hace es tomar las muestras de fase (I) y cuadratura (Q) digitalizadas por el HackRF One.



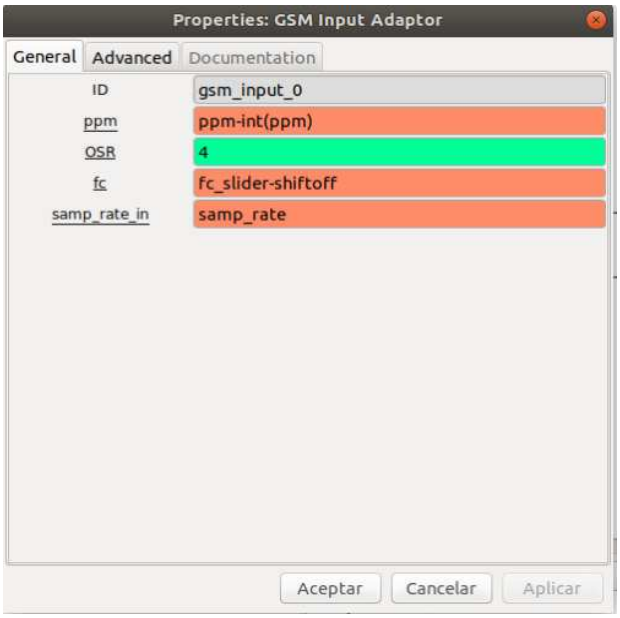
Rotator



QT GUI frecuency sink

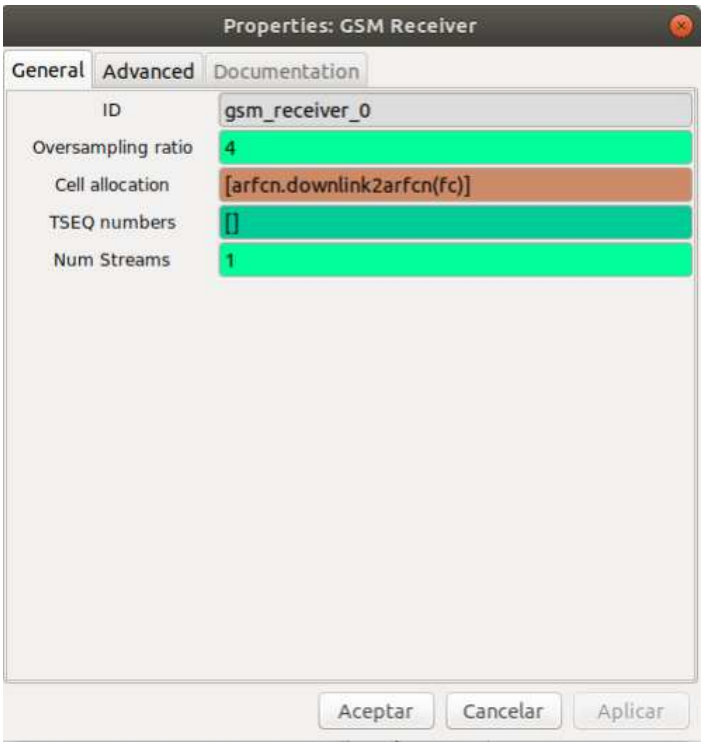


GSM input adaptor

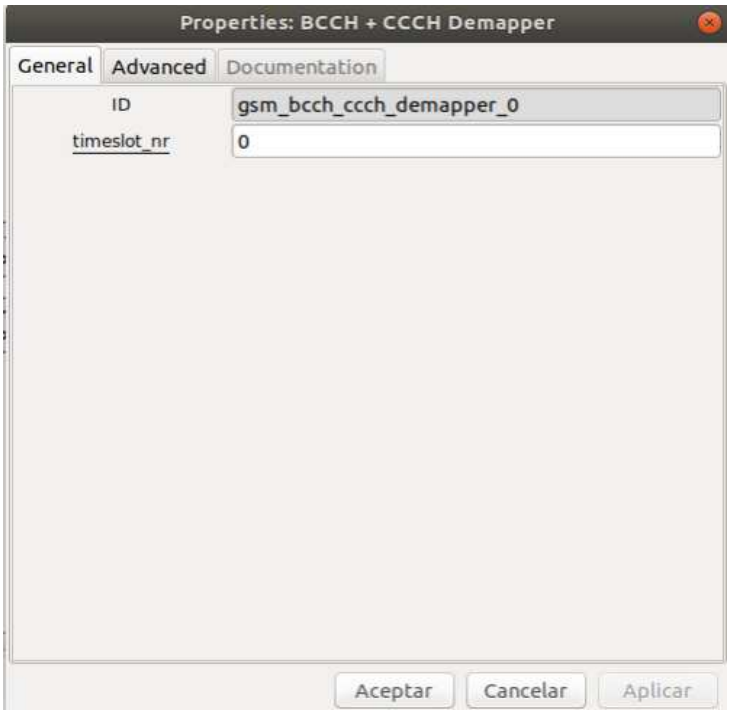


GSM clock offset control

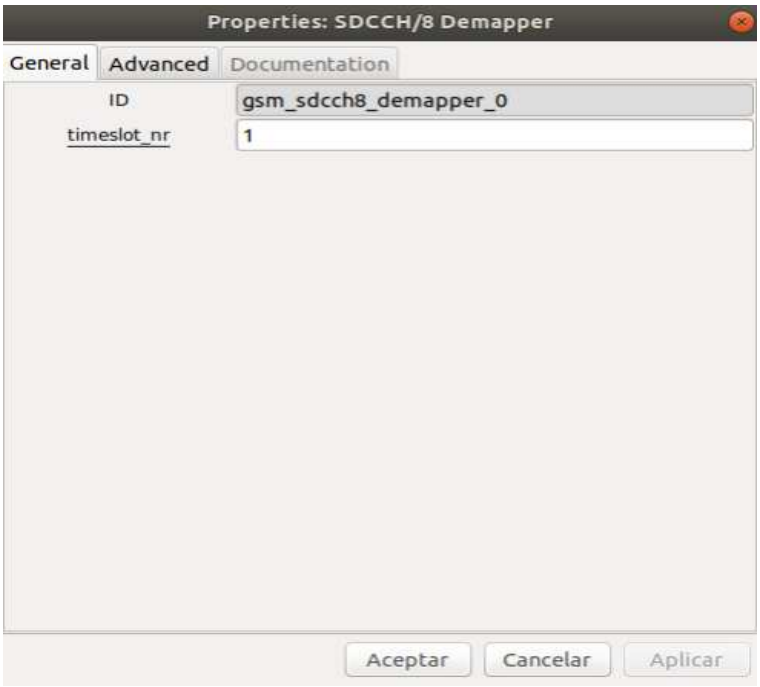
GSM Receiver



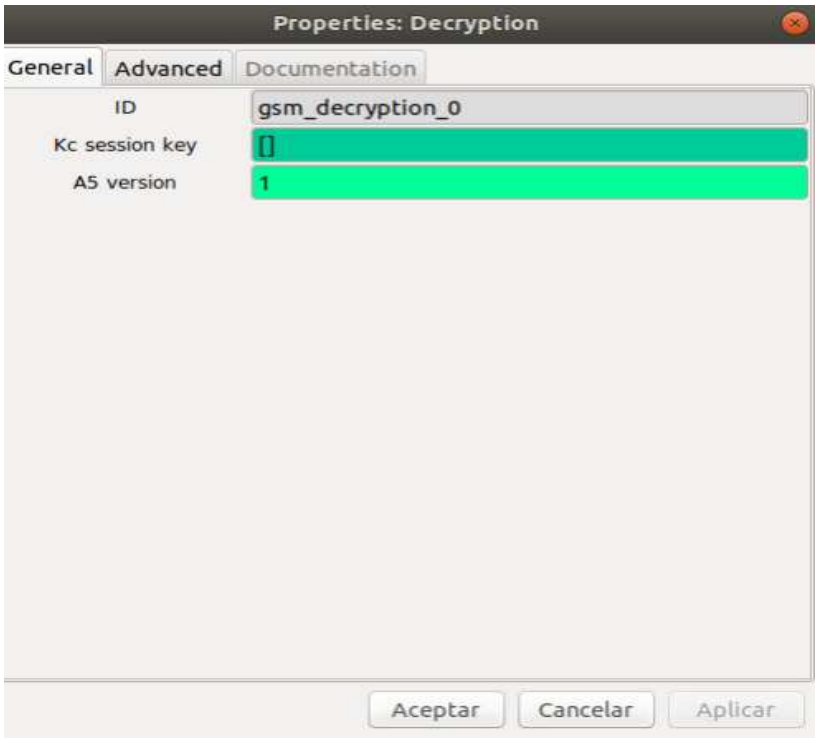
BCCH Y CCCH Demapper



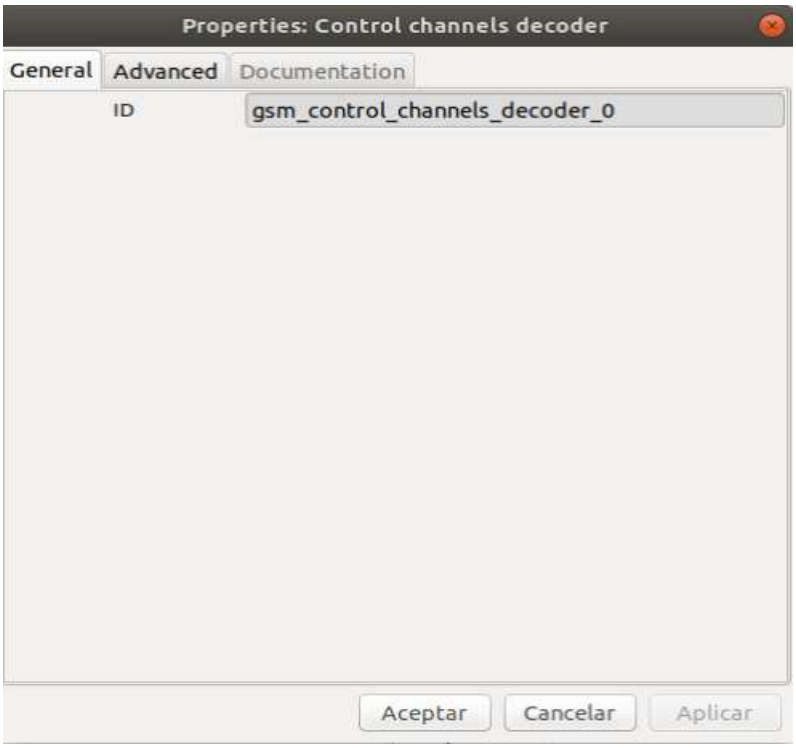
SDCCH/8 Demapper



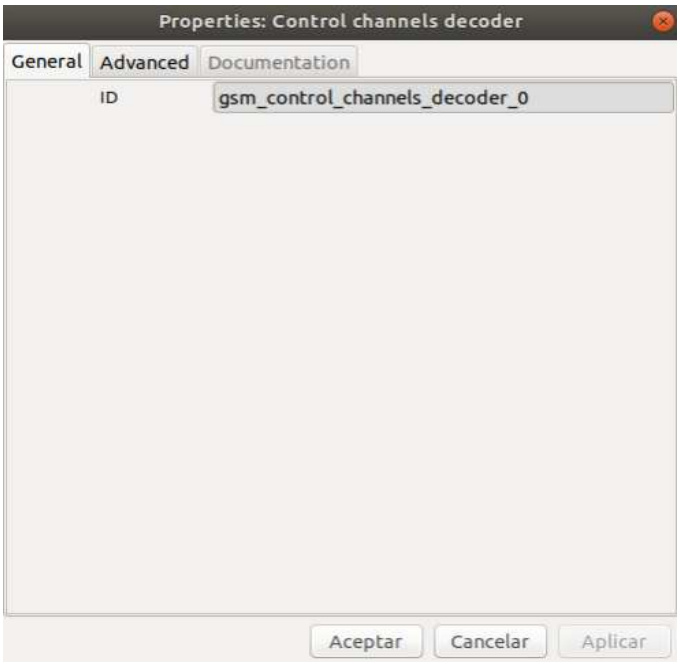
Decryption



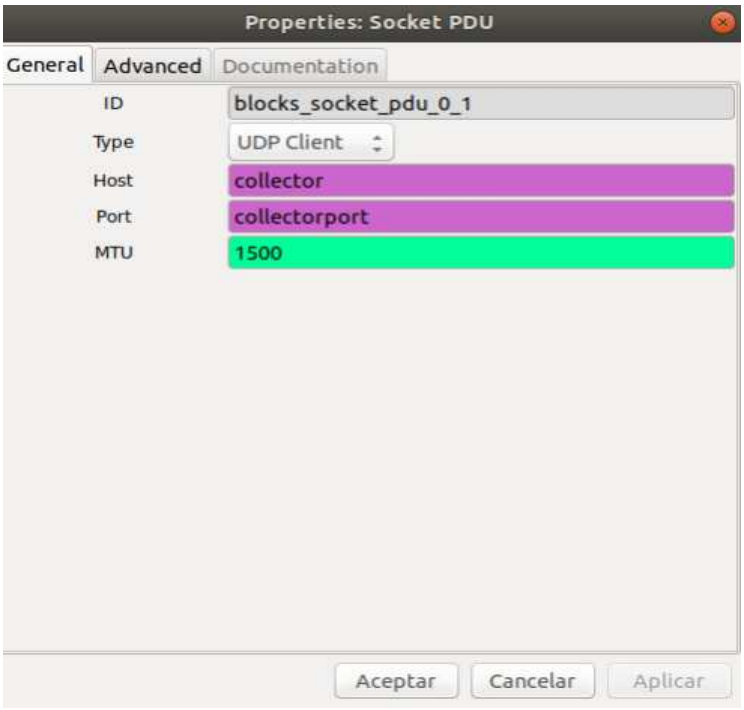
Control Channels Decoder



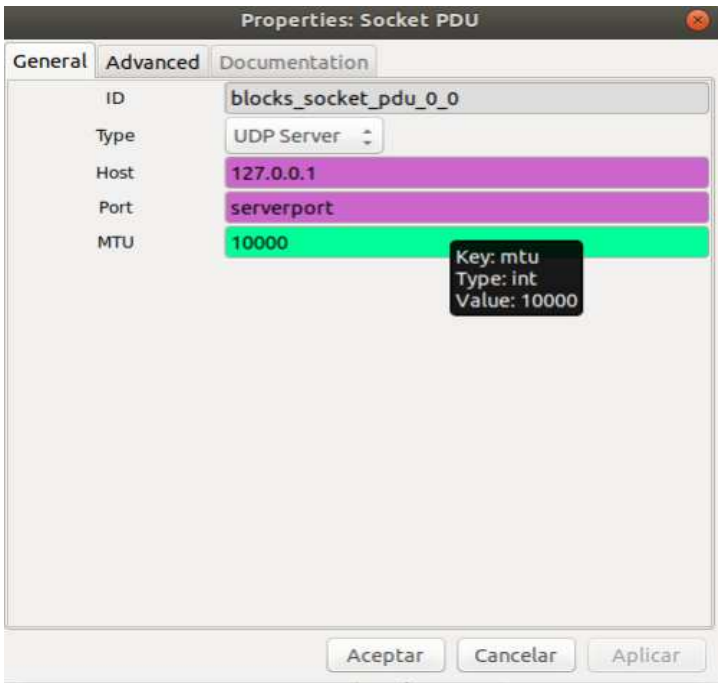
Control Channels Decoder



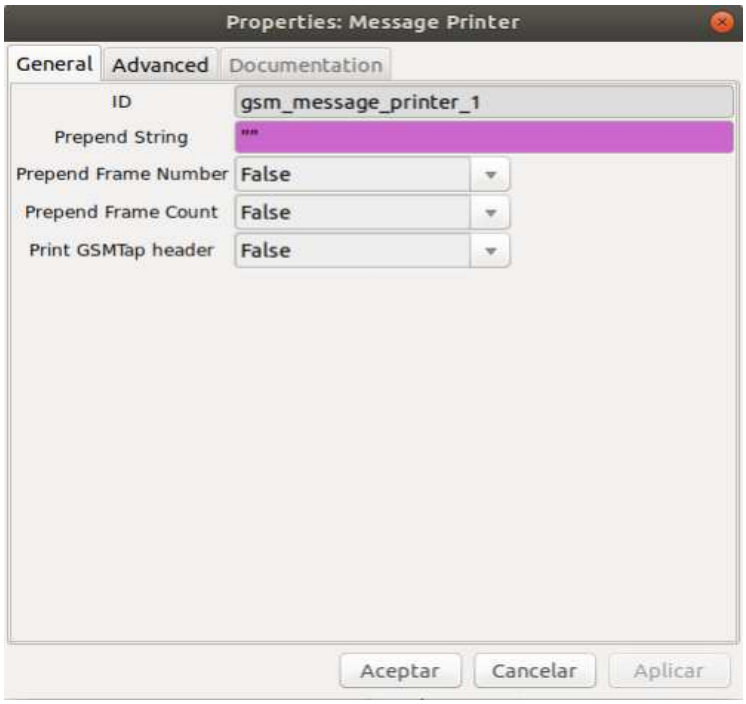
Socket PDU



Socket PDU

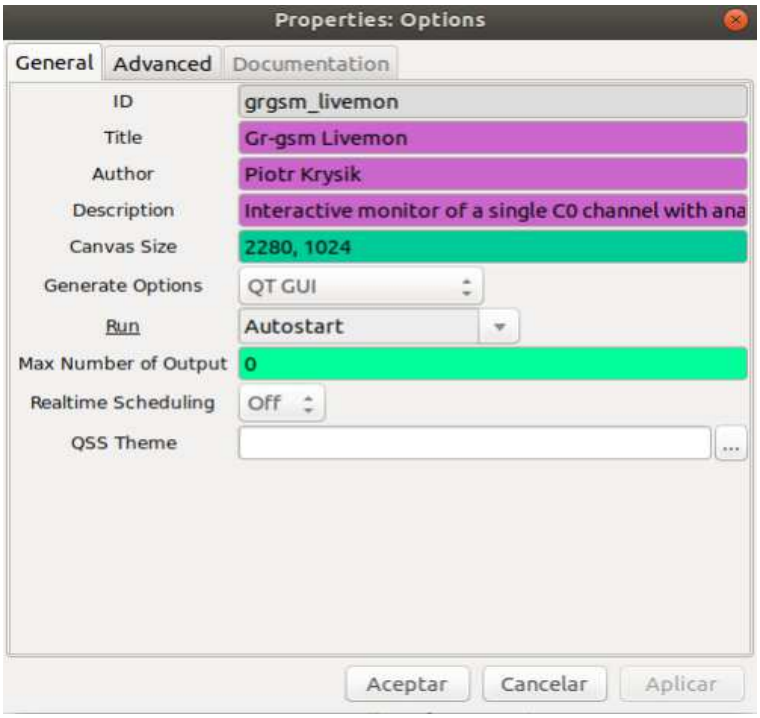


Message Printer



Variables

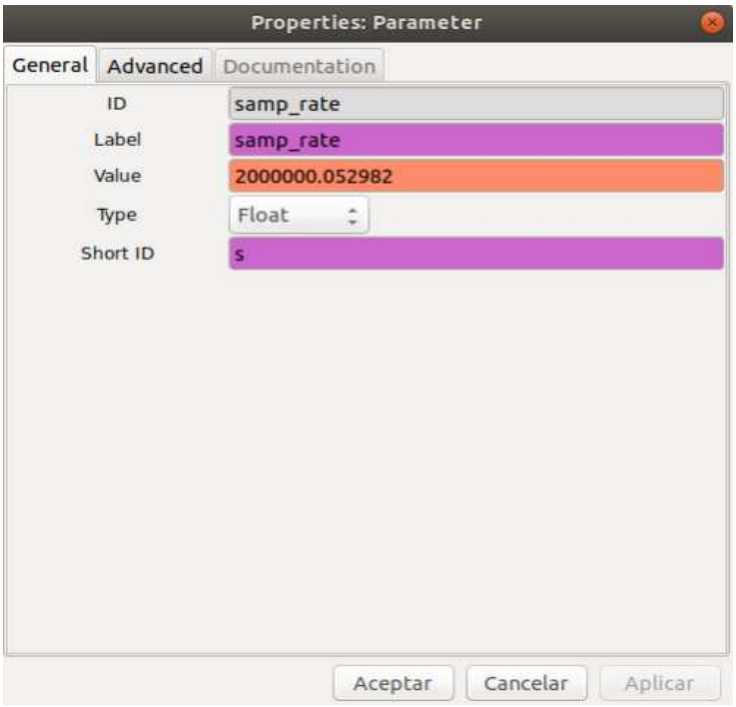
Options



Bloques Parameter: Este bloque representa un parámetro o variable en el gráfico de flujo. Este se puede utilizar para pasar los argumentos de la línea de comando a un bloque superior. El valor del parámetro no puede depender de ninguna variable.

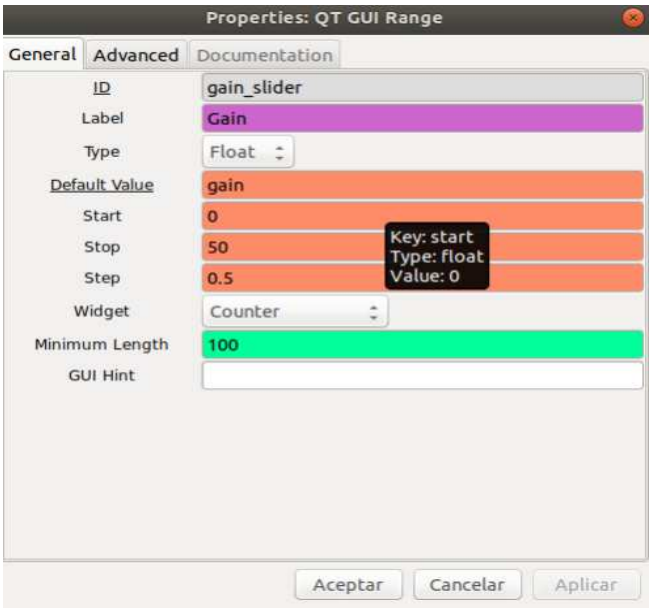
Parameter

ID: grgsm_livemon



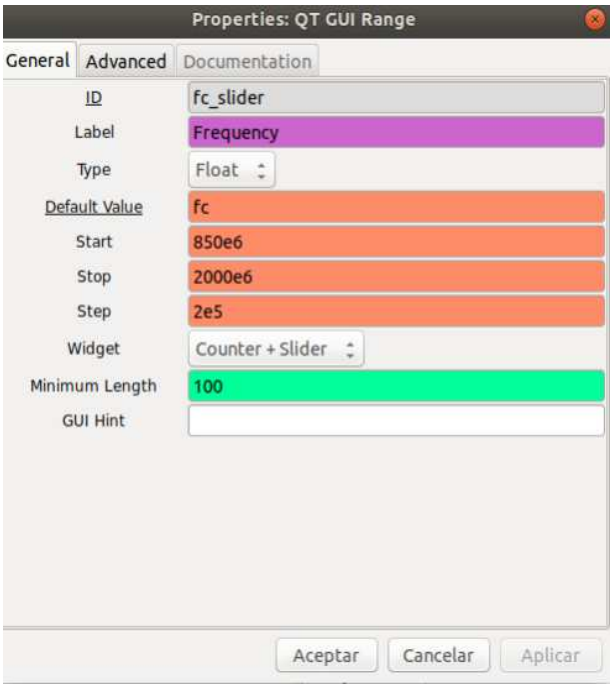
QT GUI range

ID: gain_slider



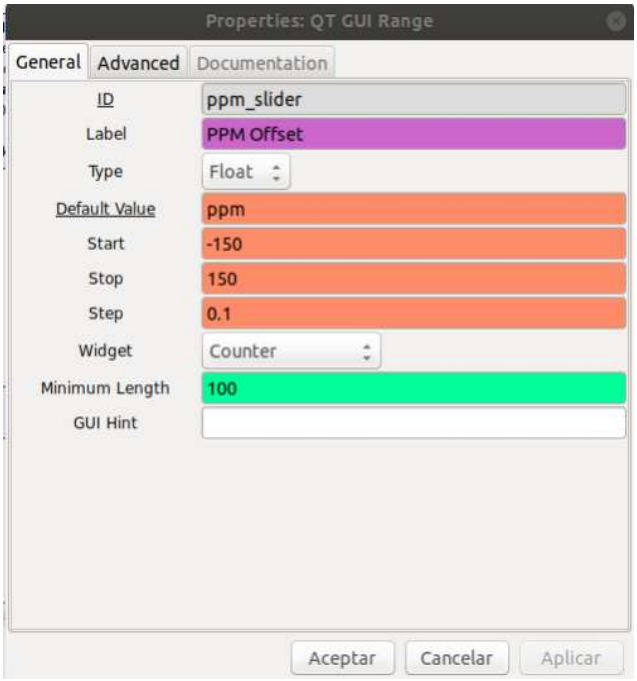
QT GUI Range

ID: fc_slider



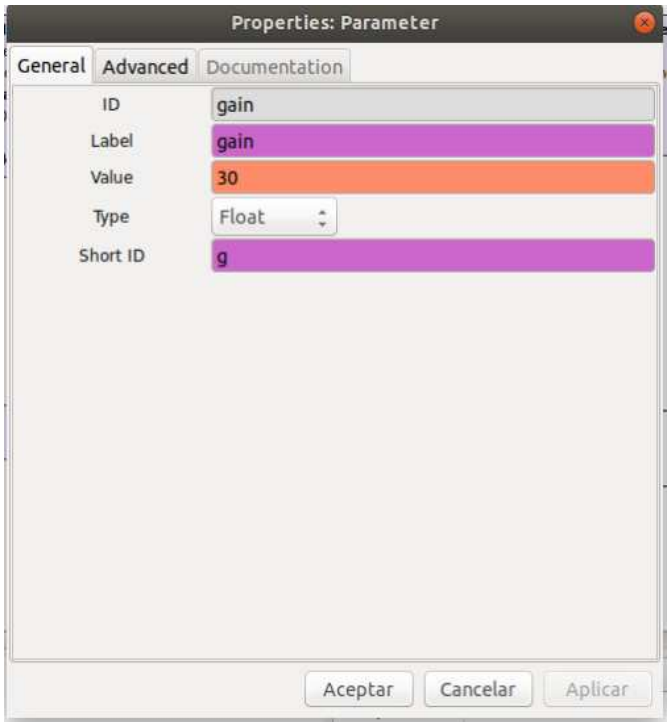
QT GUI Range

ID: ppm_slider



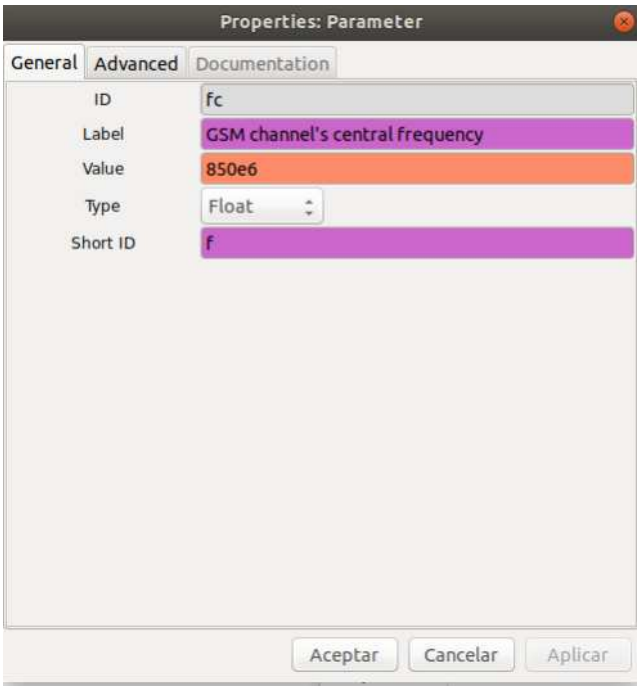
Parameter

ID: gain



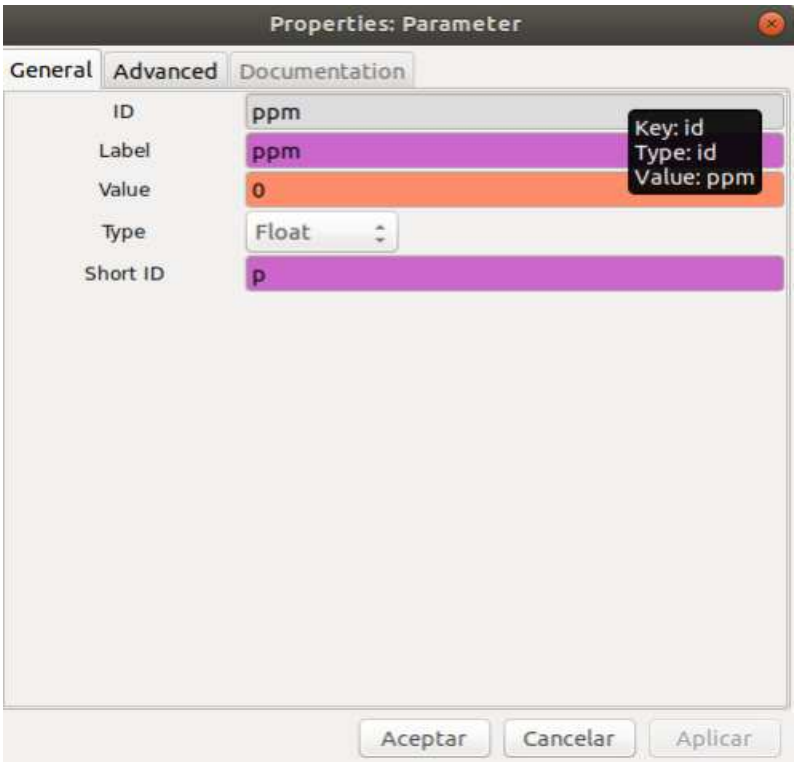
Parameter

ID: fc



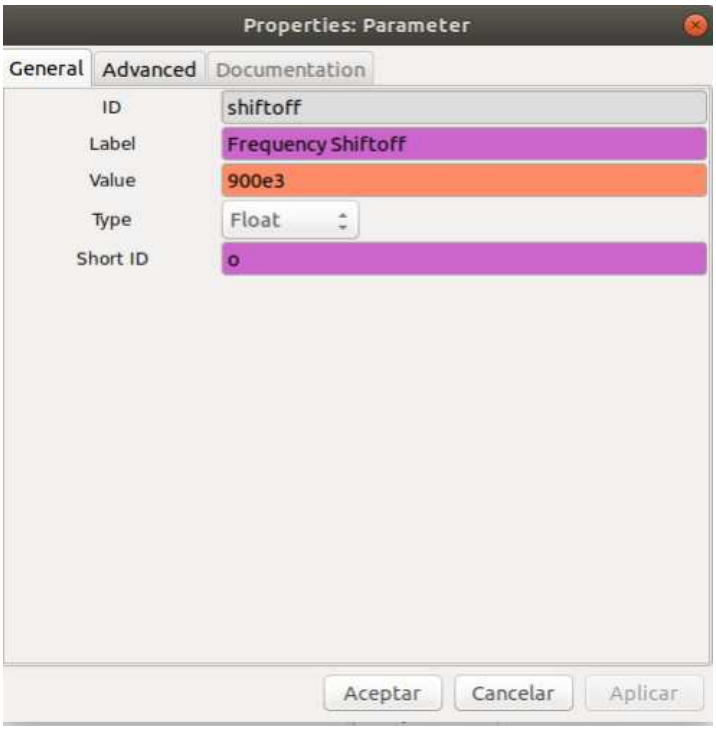
Parameter

ID: ppm



Parameter

ID: shiftoff



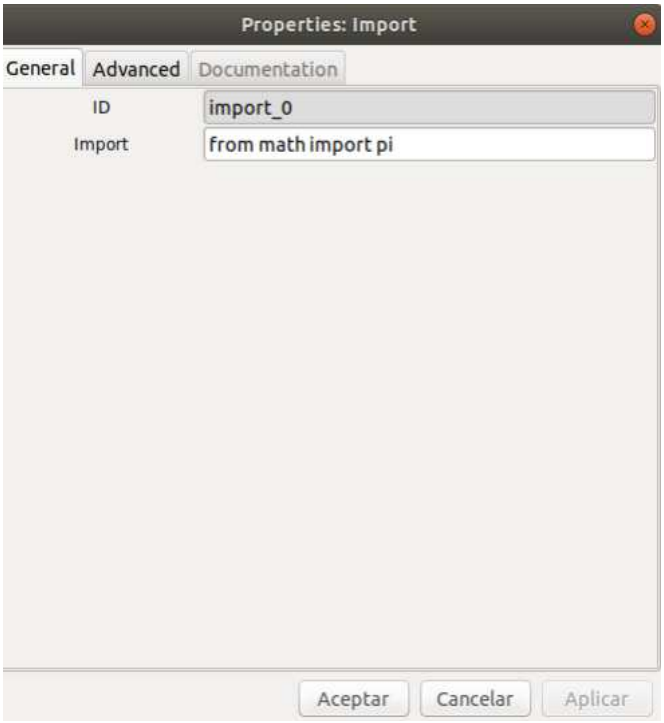
Parameter

ID: args

Bloques Import: Importar módulos adicionales de python en el espacio de nombres.

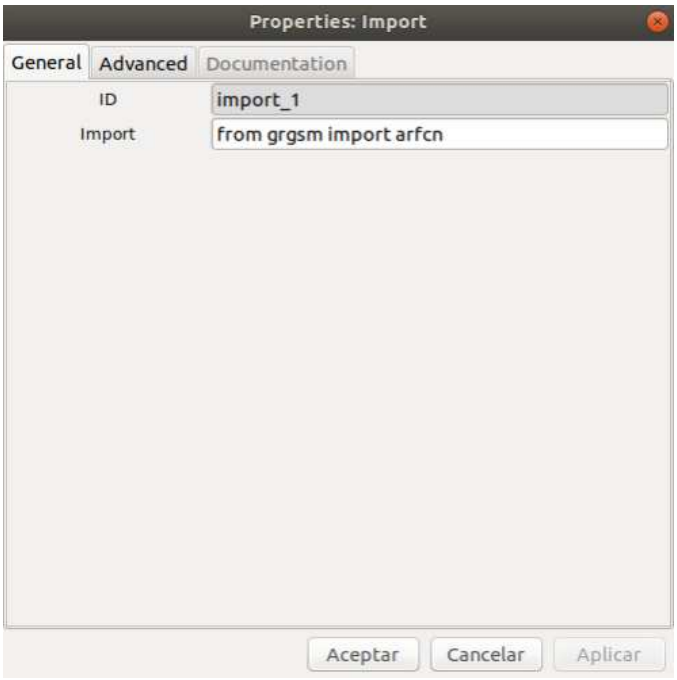
Import

ID: import



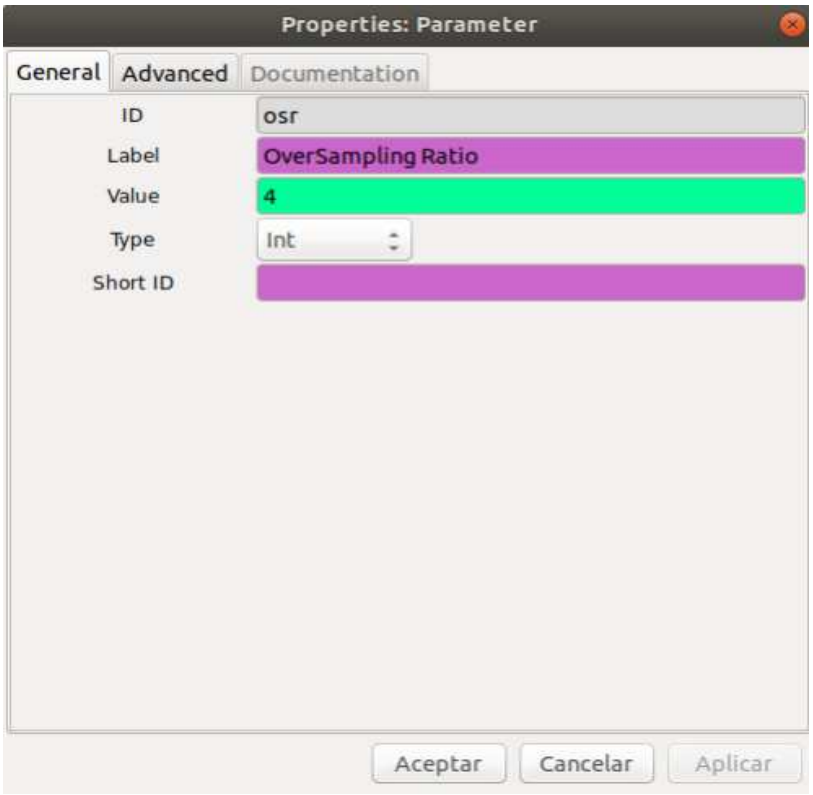
Import

ID: import_1



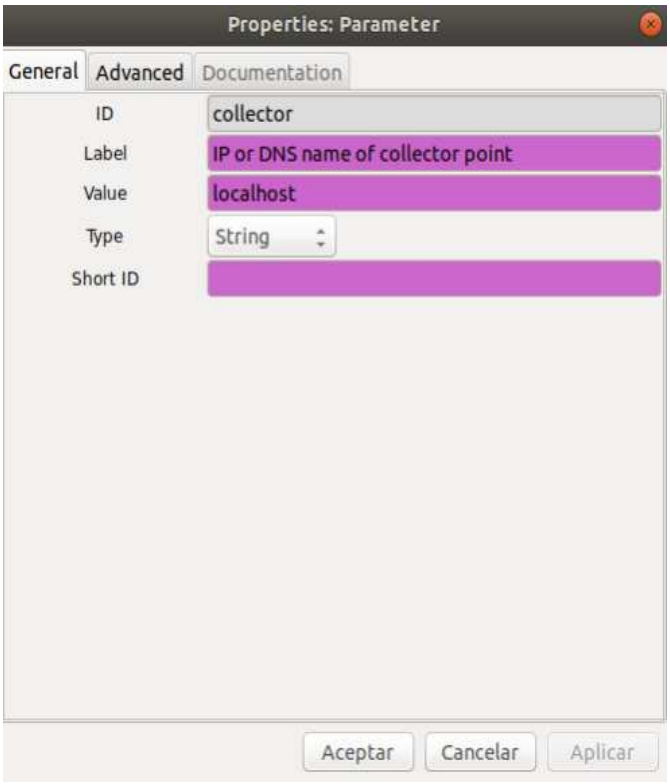
Parameter

ID: osr



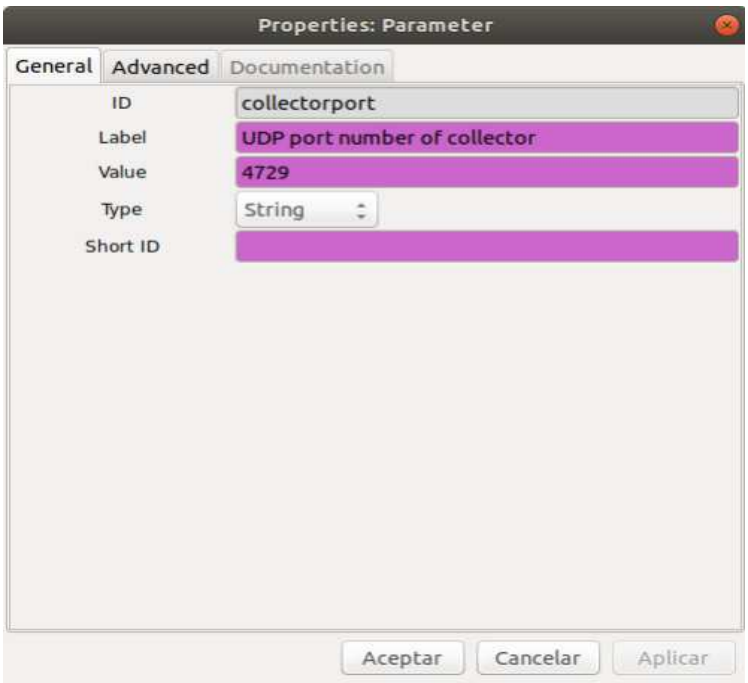
Parameter

ID: collector



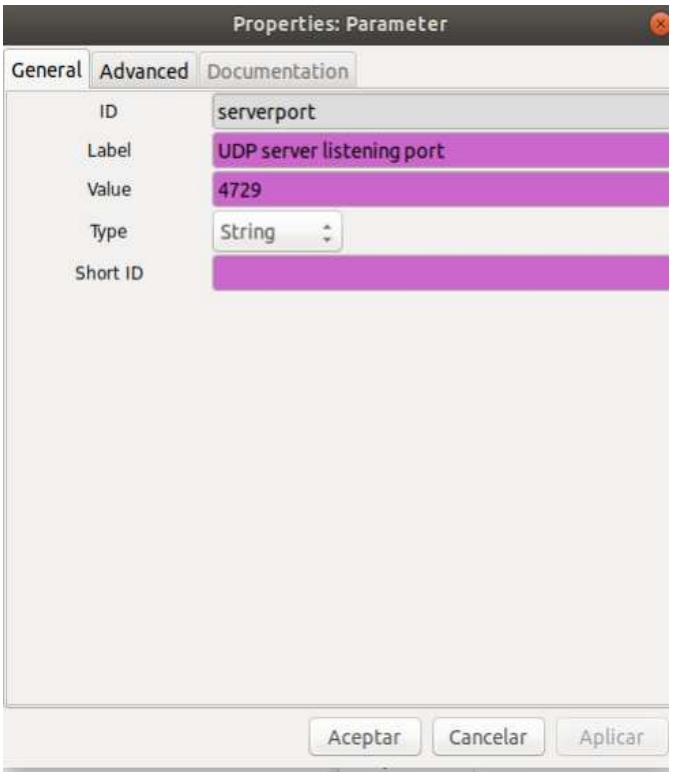
Parameter

ID: collectorport



Parameter

ID: serverport


Properties: Parameter
General
Advanced
Documentation
ID
serverport
Label
UDP server listening port
Value
4729
Type
String
Short ID
Aceptar
Cancelar
Aplicar