UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA

FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

CARRERA DE TELECOMUNICACIONES

TRABAJO DE INTEGRACIÓN CURRICULAR

Propuesta Tecnológica, previa a la obtención del Título de:

INGENIERO EN TELECOMUNICACIONES

“Desarrollo de un módulo didáctico para demostrar la vulnerabilidad en la capa de enlace de datos del modelo OSI utilizando tecnología SDR”

AUTOR

ANÍBAL ANDRÉS GUTIÉRREZ ALVARADO

DOCENTE TUTOR

ING. DANIEL ARMANDO JARAMILLO CHAMBA, MGTR.

LA LIBERTAD – ECUADOR

2024

AGRADECIMIENTO

A Dios por respaldarme y fortalecerme en los momentos más difíciles de la carrera, siempre reconociendo que sin su ayuda nada de esto hubiese sido posible.

A mis padres quienes han sido pilar fundamental para mi formación humana centrada en valores y mi formación profesional basada en el estudio como una herramienta útil de vida.

A mi esposa e hijo por ser el motor que alimentó mi motivación, para seguir sin desistir pese a las adversidades y a las circunstancias que nos entrega esta vida.

A todas aquellas personas que de una u otra manera aportaron de manera significativa en mi formación como profesional.

Por último, pero no menos importante, a los docentes de la carrera de telecomunicaciones quienes con su experiencia y conocimiento lograron que desarrolle una pasión por la carrera, y en especial agradezco a mi tutor el ingeniero Daniel Jaramillo ya que su asesoramiento fue el indicado para poder desarrollar este trabajo.

Aníbal Gutiérrez Alvarado.

DEDICATORIA

Quiero dedicar el esfuerzo y sacrificio de este trabajo a Dios, a mis padres el señor Segundo Gutiérrez Flores y la señora Fanny Alvarado Ríos quienes me han apoyado de principio a fin sin escatimar nada, dándome la mejor herencia que para mí ha sido mi formación como profesional, a mi esposa y a mi hijo Mathias Gutiérrez por compartir este hermoso capítulo de mi vida, y a quien en vida fue el ingeniero José Francisco Hsieh Ching (+) quien me convenció de que la inteligencia puede ser reemplazada con disciplina, esfuerzo y dedicación para con ello poder lograr cualquier meta establecida.

Aníbal Andrés Gutiérrez Alvarado

APROBACIÓN DEL DOCENTE TUTOR

En mi calidad de docente tutor del trabajo de integración curricular denominado: **"Desarrollo de un módulo didáctico para demostrar la vulnerabilidad en la capa de enlace de datos del modelo OSI utilizando tecnología SDR"**, elaborado por el estudiante **Aníbal Andrés Gutiérrez Alvarado**, de la carrera de Telecomunicaciones de la Universidad Estatal Península de Santa Elena, me permito declarar que luego de haber orientado, estudiado y revisado, lo apruebo en todas sus partes y autorizo al estudiante iniciar los trámites legales correspondientes.

La Libertad, 5 julio de 2024.

Ing. Daniel Armando Jaramillo Chamba, Mgt.

TUTOR

APROBACIÓN DEL DOCENTE TUTOR ESPECIALISTA

En mi calidad de docente tutor especialista del trabajo de integración curricular denominado: **"Desarrollo de un módulo didáctico para demostrar la vulnerabilidad en la capa de enlace de datos del modelo OSI utilizando tecnología SDR"**, elaborado por el estudiante **Aníbal Andrés Gutiérrez Alvarado**, de la carrera de Telecomunicaciones de la Universidad Estatal Península de Santa Elena, me permito declarar que luego de haber orientado, estudiado y revisado, lo apruebo en todas sus partes y autorizo al estudiante iniciar los trámites legales correspondientes.

La Libertad, 24 de julio de 2024.

Ing. Fernando Chamba Macas, Mgt.

TUTOR ESPECIALISTA

TRIBUNAL DE SUSTENTACIÓN

Ing. Ronald Rovira Jurado, Ph.D.
DIRECTOR DE LA CARRERA

Ing. Fernando Chamba Macas, Mgt.
DOCENTE ESPECIALISTA

Ing. Daniel Jaramillo Chamba, Mgt.
DOCENTE TUTOR GUÍA

Ing. Corina Gonzabay De la A, Mgt.
SECRETARIA

Ing. Luis Amaya Pariño, Mgt.
DOCENTE GUÍA UIC II

RESUMEN

El presente documento de investigación damnifica el desarrollo de un módulo didáctico que demuestra la vulnerabilidad en la capa de enlace de datos del modelo OSI, utilizando tecnología de Radio Definida por Software (SDR). El objetivo general es que los investigadores apliquen ataques a sistemas inalámbricos cliente/servidor utilizando escenarios definidos por radio SDR para exponer las vulnerabilidades de la capa de enlace de datos bajo los estándares del modelo OSI. Para alcanzar esto, se establecen varios objetivos específicos. Primero, se realizará un análisis exploratorio de las distintas aplicaciones del dispositivo HackRF One, para comprender sus posibles usos. Además, se configurará una conexión punto a punto entre un nodo cliente y un nodo servidor usando módulos de Arduino, con el propósito de revelar las vulnerabilidades existentes. También se recolectarán datos de la transmisión inalámbrica a través del programa URH para aplicar ataques como Eavesdropping, Replay y Man in the Middle. Finalmente, se implementará un módulo didáctico que interconecte todos los dispositivos, culminando en la elaboración de un manual práctico orientado a demostrar ataques en la transmisión inalámbrica. Este proyecto busca ofrecer una herramienta educativa y práctica que permita a los estudiantes entender y mitigar riesgos asociados a la seguridad en redes inalámbricas.

PALABRAS CLAVE: Ataques, Capa de Enlace de Datos, Vulnerabilidades, Módulo Didáctico.

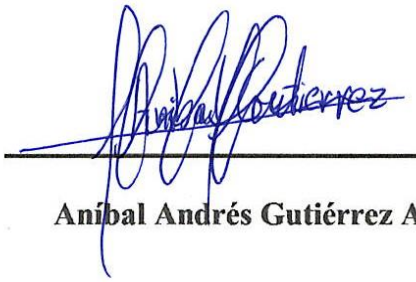
ABSTRAC

This research document outlines the development of a didactic module that demonstrates network layer vulnerabilities in the OSI model using Software Defined Radio (SDR) technology. The general objective is for researchers to apply attacks to client/server wireless systems using SDR-defined radio scenarios to expose network layer vulnerabilities under the OSI model standards. To achieve this, several specific objectives are established. First, an exploratory analysis of the various applications of the HackRF One device will be conducted to understand its potential uses. Additionally, a point-to-point connection between a client node and a server node will be configured using Arduino modules to reveal existing vulnerabilities. Wireless transmission data will also be collected using the URH program to apply attacks such as Eavesdropping, Replay, and Man in the Middle. Finally, a didactic module interconnecting all devices will be implemented, culminating in the development of a practical manual aimed at demonstrating attacks on wireless transmission. This project seeks to provide an educational and practical tool that allows students to understand and mitigate risks associated with wireless network security.

KEYWORDS: Attacks, Data Link Layer, Vulnerabilities, Didactic Module.

DECLARACIÓN

El contenido del presente Trabajo de Integración Curricular es de mi responsabilidad; el patrimonio intelectual del mismo pertenece a la Universidad Estatal Península de Santa Elena.



Aníbal Andrés Gutiérrez Alvarado

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

ÍNDICE DE ABREVIATURA

ABREVIATURA	SIGNIFICADO
CPLDs	Complex Programmable Logic Device (Dispositivo Lógico Programable Complejo).
CPU	Central Processing Unit (Unidad Central de Procesamiento).
DC	Direct Current (Corriente Continua)
DDOS	Distributed Denial of Service (Denegación de Servicio Distribuido).
DOS	Denial of Service (Denegación de Servicio).
ESET	Essential Security against Evolving Threats (Seguridad Esencial contra Amenazas en Evolución).
FACSISTEL	Facultad de Sistemas y Telecomunicaciones.
FM	Frequency Modulation (Frecuencia Modulada).
FPGAs	Field Programmable Gate Array (Matriz de Puertas Lógicas Programable en Campo).
GFSK	Gaussian Frequency Shift Keying (Modulación por Desplazamiento de Frecuencia Gaussiana).
GNU	GNU's Not Unix (GNU No es Unix).
HDMI	High-Definition Multimedia Interface (Interfaz Multimedia de Alta Definición).
HF	High Frequency (Alta Frecuencia).

I/O	Input/Output (Entrada/Salida).
IBM	International Business Machines (Máquina de Negocios Internacionales).
IDE	Integrated Development Environment (Entorno de Desarrollo Integrado).
IOT	Internet Of Things (Internet de las Cosas).
IP	Internet Protocol (Protocolo de Internet).
ISO	International Organization for Standardization (Organización Internacional de Normalización).
KTH	Kungliga Tekniska Högskolan (Instituto Real de Tecnología).
LED	Light Emitting Diode (Diodo Emisor de Luz).
MITM	Man in the middle (Hombre en el medio).
N.A.	Normalmente Abierto.
N.C.	Normalmente Cerrado.
OSI	Open System Interconnection (Interconexión de Sistemas Abiertos).
PCB	Printed Circuit Board (Placa de Circuito Impreso)
RF	Radio Frequency (Radio Frecuencia).
SBC	Single Board Computer (Computadoras de Placa Única).
SDR	Software Defined Radio (Radio Definida por Software).
SNA	Systems Network Architecture (Arquitectura de Red de Sistemas).

STEM	Science, Technology, Engineering and Mathematics (Ciencia, Tecnología, Ingeniería y Matemáticas).
TCP/IP	Transmission Control Protocol/Internet Protocol (Protocolo de control de transmisión/Protocolo de Internet).
TTL	Transistor – Transistor Logic (Lógica Transistor – Transistor)
UART	Universal Asynchronous Receiver/Transmitter (Receptor/Transmisor Asíncrono Universal).
UHF	Ultra High Frequency (Frecuencia Ultra Alta).
UPSE	Universidad Estatal Península de Santa Elena.
URH	Universal Radio Hacker (Hacker de Radio Universal).
USB	Universal Serial Bus (Bus Universal en Serie).
VCC	Voltaje de Corriente Continua.
VHF	Very High Frequency (Frecuencia Muy Alta).

ÍNDICE DE ANEXOS

INTRODUCCIÓN

En la era digital actual, la seguridad de las redes se ha convertido en un campo de estudio esencial, particularmente en el contexto de las comunicaciones inalámbricas, donde las vulnerabilidades pueden ser explotadas por actores maliciosos para comprometer la integridad y privacidad de la información transmitida. El modelo OSI, que sirve como marco de referencia para entender la estructura de las redes, identifica la capa de enlace de datos como una de las más críticas en términos de seguridad. Este trabajo de integración curricular se enfoca en la exploración y demostración de las vulnerabilidades presentes en esta capa a través del uso de tecnología de Radio Definida por Software (SDR) [1].

Mediante la implementación de un módulo didáctico, se busca no solo identificar y analizar estos riesgos, sino también ofrecer una herramienta educativa que permita a estudiantes y profesionales desarrollar habilidades prácticas para la detección y mitigación de ataques en entornos inalámbricos. Este enfoque práctico tiene el potencial de fortalecer la comprensión de la seguridad en redes y de promover una cultura de prevención y respuesta efectiva frente a amenazas cibernéticas.

Además, el creciente uso de dispositivos inalámbricos en numerosos sectores, desde comunicaciones personales hasta infraestructuras críticas, subraya la importancia de diseñar y validar sistemas que sean seguros y resistentes a intrusiones. La vulnerabilidad en la capa de enlace de datos puede ser particularmente perjudicial, ya que permite a los atacantes manipular, interceptar o redirigir el flujo de datos. Para abordar estas amenazas, el presente estudio se centra en el uso de la tecnología SDR, una herramienta versátil que facilita el análisis y la implementación de pruebas de seguridad en frecuencias y protocolos utilizados en la comunicación inalámbrica.

El objetivo de este trabajo es triple: primero, se pretende profundizar en el conocimiento y las aplicaciones del HackRF One, un dispositivo SDR que permite la recepción y transmisión de señales de radio. Segundo, se busca establecer un ambiente controlado para simular ataques, utilizando configuraciones punto a punto entre nodos cliente y servidor. Finalmente, el proyecto culmina en la creación de un módulo didáctico que integra todos estos elementos en un manual práctico, proporcionando a los estudiantes un recurso integral para la comprensión y aplicación de estrategias de seguridad en la capa de enlace de datos. Con este enfoque, se espera no solo elevar el nivel de conocimiento técnico, sino también fomentar un enfoque proactivo hacia la seguridad cibernética en futuros profesionales del área [2].

Este escrito no sólo contribuye al campo académico y profesional mediante la demostración de vulnerabilidades específicas y la presentación de técnicas de mitigación, sino que también enriquece la experiencia educativa al proporcionar un enfoque práctico y tangible sobre los riesgos de seguridad en la capa de enlace de datos. Al finalizar la investigación, se espera que los estudiantes y profesionales equipados con este conocimiento y habilidades sean capaces de aplicar métodos de seguridad más efectivos y desarrollar soluciones innovadoras frente a las amenazas emergentes en entornos de enlaces inalámbricos. El módulo didáctico diseñado no solo servirá como una herramienta pedagógica, sino también como un catalizador para futuras investigaciones y desarrollos en el ámbito de la ciberseguridad, promoviendo un enfoque más robusto y consciente frente a los desafíos que presenta la era digital.

CAPÍTULO I

GENERALIDADES

1.1. ANTECEDENTES

El modelo OSI se desarrolló en 1984 por la ISO, siendo un estándar que se propuso como objetivo lograr la interconexión de sistemas sin importa que estas sean de distintas procedencias. Este modelo consta de 7 capas o también llamados niveles, cada una de estas capas o niveles tienen definidas sus funciones para lograr la intercomunicación entre protocolos. El modelo OSI define la funcionalidad de los protocolos para obtener un modelo estándar, entre las capas del modelo OSI se tiene la capa de enlace de datos [1].

La capa de enlace de datos del modelo OSI tiene como función principal establecer una transmisión de información y datos de manera segura, esta transmisión se puede dar a través de una red móvil, informática o inalámbrica. Dentro de las tecnologías de transmisión de información y datos se encuentran las comunicaciones inalámbricas. La capa de enlace de datos es una de las más vulnerables dentro del modelo OSI [2].

La vulnerabilidad se puede presentar por la debilidad propia del sistema permitiendo ser atacado, así queda expuesto a recibir daño dentro de la capa de enlace de datos por alguna amenaza, el caso más frecuente de vulnerabilidad en la capa de enlace de datos es la amenaza de robo de identidad, consiste en engañar al usuario haciéndole creer que está conectado directamente con el servidor entregando así sus datos y contraseñas, al momento de materializarse la amenaza en la capa de enlace de datos esta entra en riesgo [3].

El riesgo se expresa como la probabilidad de que un sistema sufra un percance en la seguridad [3], dando paso a los ataques informáticos dentro de ellos se puede hacer referencia a

los ataques más conocidos en la transmisión de datos guiados y no guiados de la capa de enlace de datos del modelo OSI.

El primer ataque es “EAVESDROPPING” que traducido al español significa escuchar secretamente tiene como principales acciones el “sniffing” escuchar y el “capturing” grabar o capturar una conversación, los datos no serán adulterados permaneciendo intactos, pero al contrario en la privacidad esta será comprometida [4].

El segundo ataque es “REPLAY ATTACK” que traducido al español significa ataque de repetición en donde el atacante tiene conexión entre el emisor y receptor, este reenvía información validada que fue interceptada con anterioridad [5].

El tercer ataque es “MAN IN THE MIDDLE (MITM)” que traducido al español significa hombre en el medio en donde el intermediario o atacante tiene conexión entre el emisor y receptor, pudiendo capturar información, modificarla y enviarla haciendo creer que existe una conexión directa entre ellos [6].

En estos ataques el emisor no es consciente de haber enviado la información al atacante y tendrá la impresión de haber enviado la información al receptor destinado.

La tecnología SDR se considera como el futuro de las comunicaciones inalámbricas debido a que soporta los estándares modernos con los que se desarrollan las nuevas tecnologías [7], el HackRF One es un dispositivo SDR que recibe y transmite frecuencias desde 100MHz a 6GHz convirtiéndose en un transceptor [8], es muy difícil conseguirlo en Ecuador, este dispositivo funciona en el software de uso libre URH. URH es compatible con Windows, Linux y macOS, este software sirve para la investigación de protocolos inalámbricos y tiene soporte para la mayoría de los dispositivos SDR [9].

URH tiene un instalador ligero para Windows, una vez que se haya instalado en la computadora, el programa nos presenta una interfaz en la que se debe configurar los parámetros del dispositivo SDR, en este caso el dispositivo es el HackRF One, con la configuración se busca que el programa reconozca al dispositivo SDR para luego utilizar las funciones que ofrece URH como lo son el analizador de espectro, grabar datos, guardar los datos grabados y reproducir datos guardados todo esto a la frecuencia que se desee trabajar, estas funciones permiten que el dispositivo se comporte como un transceptor para así poder realizar un ataque "MITM" y un ataque "Replay" mediante la técnica del "Eavesdropping" a un sistema inalámbrico de encendido de diodos leds, el cual está desarrollado con la tecnología Arduino en conjunto de un kit de módulos de RF apc220 compatibles con Arduino.

Con todos estos elementos se pretende diseñar un módulo didáctico para mostrar la vulnerabilidad de transmisión de información y datos de forma inalámbrica que existe en la capa de enlace de datos del modelo OSI para que sea implementado en el laboratorio de Telecomunicaciones de la facultad de Sistemas y Telecomunicaciones perteneciente a la Universidad Estatal Península de Santa Elena.

En el año 2020 en la Universidad Complutense de Madrid, España. Se realiza un trabajo a cargo de Elizabeth Rivera sobre la explotación de las vulnerabilidades de IOT utilizando tecnología SDR con bloques de programación lógica en GNURadio, dentro los objetivos específicos está el interceptar una señal a una determinada frecuencia para posteriormente realizar un ataque "replay". Diseña un servidor, un cliente con módulos de Arduino y módulos de RF a 434MHz, para poder receptar la señal se utiliza el dispositivo SDR llamado RTL-SDR que se programa como un receptor FM en GNURadio, una vez que se recepte la señal del cliente al servidor esta es grabada para volver a ser retransmitida, pero reemplazando el cliente con el

dispositivo HackRF One programado como un transmisor mediante bloques de programación en GNURadio, con ello se cumple el objetivo del trabajo. Dentro de los resultados del análisis de vulnerabilidad en RF se realizó tres tipos de ataques el sniffing que fue efectivo debido a que los dispositivos empleados no presentaron algún tipo de seguridad y este ataque se representa como la base para los demás ataques, el ataque de ingeniería inversa con resultado favorable porque se logra "clonar" él cliente usando el dispositivo SDR HackRF One y también "clonar" la señal transmitida, por último, se tiene el ataque replay que al lograr retransmitir la señal capturada se sobreentiende que el ataque fue efectivo ante la vulnerabilidad que existe entre la comunicación inalámbrica del cliente y el servidor [10].

En el año 2021 en el KTH Real Instituto de Tecnología de Estocolmo, Suecia (KTH Royal Institute of Technology Stockholm, Sweden). Se publica el trabajo de Axel Lindeberg que lleva como título Hacking Into Someone´s Home using Radio Waves – Ethical Hacking of Securitas´ Alarm System (Hackear dentro de la casa de alguien utilizando ondas de radio – Hacking Ético de un Sistema de Alarmas Seguritas), el objetivo del trabajo es evaluar el sistema de alarmas de la marca seguritas para determinar si este es seguro o no y para ello se realiza un análisis completo de la vulnerabilidad en la comunicación de radiofrecuencia del sistema de alarmas. Dentro de los ataques que se realizan se encuentra el ataque replay empleando un dispositivo SDR y el software URH. En el análisis de los resultados se presenta una vulnerabilidad de nivel crítico en el protocolo de radiofrecuencia lo que permite al atacante desarmar el sistema de alarmas eludiendo la seguridad de este [11].

1.2. DESCRIPCIÓN DEL PROYECTO

Se plantea la propuesta tecnología para mostrar la vulnerabilidad en la capa de enlace de datos del modelo OSI con la "IMPLEMENTACIÓN DE UN MÓDULO DIDÁCTICO PARA LA

APLICACIÓN DE ATAQUES DE TIPO EAVESDROPPING, MAN IN THE MIDDLE Y ATAQUE REPLAY A LA TRANSMISIÓN DE DATOS POR RADIOFRECUENCIA ENTRE CLIENTE/SERVIDOR, UBICADO EN EL LABORATORIO DE TELECOMUNICACIONES DE LA UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA" y está constituido por lo siguiente componentes:

1) 1 dispositivo SDR HackRF One.
2) 2 módulos de Arduino Mini Pro Atmega328P de 5V.
3) 1 kit Módulo Apc220 De RF.
4) 8 resistencias, diodos led y pulsadores.
5) 1 computadora de escritorio.

Este proyecto tiene como enfoque el desarrollo de un módulo didáctico que se constituye por un NODO CLIENTE (transmisor), NODO SERVIDOR (receptor) y un ATACANTE (dispositivo SDR HackRF One y una computadora de escritorio con el software URH instalado).

El NODO CLIENTE se compone por un microcontrolador Arduino Mini Pro Atmega328P de 5V, un módulo apc220 de RF, el código fuente de programación con función de transmisor y 8 pulsadores que mediante programación se encargarán de enviar los datos de on-off al receptor.

El NODO SERVIDOR se compone por un microcontrolador Arduino Mini Pro Atmega328P de 5V, un módulo apc220 de RF, el código fuente de programación con función de receptor y 8 diodos leds con su respectiva resistencia que mediante programación se encargarán de encender o apagar algún led según en el dato recibido.

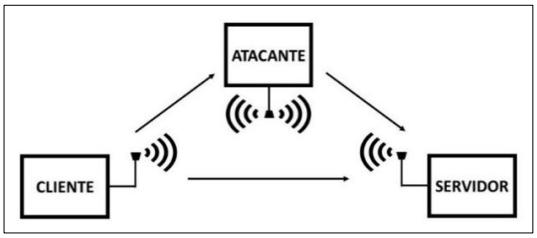
Este sistema se encuentra comunicado entre el NODO CLIENTE y el nodo SERVIDOR de manera inalámbrica por radiofrecuencia, que controlará el encendido o apagado de diodos leds. El ATACANTE mediante el software URH podrá interceptar, observar, grabar, modificar,

transmitir y retransmitir datos enviados del nodo CLIENTE al nodo SERVIDOR como se muestra en la Figura 1.

Con la unión de todos estos elementos se estima tener un módulo didáctico para demostrar la vulnerabilidad que existe en la capa de enlace de datos de la transmisión por radiofrecuencia ante amenazas, bajo la aplicación de ataques informáticos como Eavesdropping, Man in the middle y Replay. Este módulo queda implementado en el laboratorio de telecomunicaciones de la Universidad Estatal Península de Santa Elena.

Figura 1

Diagrama esquemático del sistema



Nota: Representación esquemática del ataque al sistema, fuente Autor

1.3. OBJETIVOS DEL PROYECTO

1.3.1. OBJETIVO GENERAL:

Aplicar ataques dentro de sistemas inalámbricos orientados a clientes/servidores utilizando escenarios definidos por radio SDR para demostrar vulnerabilidades en la capa de enlace de datos del modelo OSI.

1.3.2. OBJETIVOS ESPECÍFICOS:

- Analizar los diferentes tipos de aplicaciones del dispositivo HackRF One mediante una investigación exploratoria para conocer el uso que se le puede dar.

- Realizar una conexión punto a punto entre el NODO CLIENTE y el NODO SERVIDOR mediante la programación de los módulos de Arduino para mostrar la vulnerabilidad que poseen.
- Obtener datos de la transmisión inalámbrica mediante el uso del programa URH para la aplicación de los ataques Eavesdropping, Replay y Man in the middle.
- Implementar un módulo didáctico mediante la interconexión de todos los dispositivos para la elaboración del manual de una práctica orientada a los ataques en la transmisión inalámbrica.

1.4. RESULTADOS ESPERADOS

Identificar las vulnerabilidades que existe en la capa de enlace de datos del modelo OSI por medio de la aplicación de ataques.

Entender el funcionamiento de los dispositivos SDR en las comunicaciones inalámbricas.

Desarrollar dos códigos de programación uno con función de transmisor y el otro con función de receptor para los módulos de Arduino en conexión a los módulos apc220 de RF.

Diseñar un circuito impreso y un modelado 3D, de la conexión de los componentes que conforman tanto al nodo CLIENTE como al nodo SERVIDOR.

Realizar diseños en 3D de las carcasas que contienen la circuitería del nodo CLIENTE y la circuitería del nodo SERVIDOR.

Demostrar la vulnerabilidad del sistema cliente/servidor ante la aplicación de los ataques de tipo Eavesdropping, Replay y Man in the middle.

Reforzar la enseñanza sobre las vulnerabilidades en la seguridad de redes inalámbricas mediante la práctica en un módulo didáctico implementado en el laboratorio de Telecomunicaciones.

1.5. JUSTIFICACIÓN

La tecnología avanza de manera exponencial abriendo camino a nuevos dispositivos con tecnologías del futuro como es el caso del dispositivo SDR HackRF One, este soporta los nuevos estándares comerciales de las redes móviles como por ejemplo el 5G, a la tecnología de este dispositivo SDR se la considera como el futuro de las comunicaciones inalámbricas. Con el dispositivo HackRF One se contribuye en el aprendizaje de las comunicaciones y seguridad de redes inalámbricas orientado a los estudiantes de la carrera de telecomunicaciones, debido a que con este dispositivo se puede detectar las vulnerabilidades que existen en dispositivos de RF por medio de realización de ataques a la transmisión de datos, así los estudiantes podrán adquirir nuevos conocimientos mediante la práctica.

Esta propuesta tecnológica beneficia de manera directa a los estudiantes de grado de la carrera de telecomunicaciones incentivando el desarrollo de prototipos para aprendizaje en base a la investigación, aportando en el conocimiento de materias de especialidad como lo son las comunicaciones inalámbricas, redes de datos, seguridad de redes inalámbrica, etc. Y de forma indirecta se beneficia la facultad de Sistemas y Telecomunicaciones de la Universidad Estatal Península de Santa Elena, ya que esta propuesta tecnológica al ser implementada en el laboratorio de Telecomunicaciones este se equipa con tecnología moderna.

Con esta investigación se pretende conocer las vulnerabilidades que se tiene en la capa de enlace de datos del modelo OSI de los dispositivos que utilizan RF como medio de comunicación, como es el caso de los dispositivos IOT, de esta manera surge la idea del diseño de un módulo didáctico que se base en el hacking ético para estudiar y evaluar las posibles soluciones de protección o mitigación ante los ataques que se presentan en estos dispositivos.

1.6. METODOLOGÍA

Para el desarrollo de este proyecto se consideró utilizar los siguientes tipos de metodologías:

1.6.1 INVESTIGACIÓN EXPLORATORIA

Este tipo de investigación se realiza mediante la revisión de repositorios académicos, fuentes bibliográficas, artículos científicos que estén basados en temas relacionados como: Vulnerabilidades de las capas del modelo OSI, Ataques en la transmisión de la capa de enlace de datos del modelo OSI, Vulnerabilidades de los dispositivos IOT, Ataque Man in the middle con tecnología SDR, Mitigación de ataques replay con dispositivos SDR, etc.

1.6.2 INVESTIGACIÓN APLICADA

Este tipo de investigación se lo realiza con la técnica de prueba y error en la interconexión de los dispositivos, con el fin de comprobar que exista una buena comunicación entre ellos y en caso de que no exista corregir los problemas de conexión. El hecho de no tener problemas en la conexión y que sea efectiva entre los dispositivos significa que no hay riesgo de fallos al momento de realizar los ataques al módulo didáctico luego de ser implementado.

Las fases de la aplicación de los métodos de investigación se detallan de la siguiente manera:

FASE 1: Investigación y estudio, sobre el modelo OSI, capas del modelo OSI, capa de enlace de datos del modelo OSI y sus ataques, comunicaciones inalámbricas, recepción y transmisión de datos, dispositivos SDR, dispositivo HackRF One, módulos de Arduino y apc220 RF, software de Arduino IDE, RF Magic y URH, herramientas de modelados 3D.

En esta etapa se recopila toda la información teórica para poder cumplir el primer objetivo específico propuesto. Se revisa los conceptos sobre el modelo OSI y sus características, capas del

modelo OSI, capa de enlace de datos del modelo OSI, vulnerabilidades y tipos de ataques dentro de la capa de enlace de datos del modelo OSI.

Se estudia la tecnología SDR, el dispositivo HackRF One y sus diferentes tipos de aplicaciones, los módulos de Arduino pro mini con el microcontrolador ATMEGA 328P, los módulos APC220 de RF junto al software RF Magic para su configuración.

Se analiza el tipo de software que se va a utilizar según sus características como por ejemplo software de programación, de configuración, de ataques y de diseño y modelado 3D.

FASE 2: Diseño, armado y modelado 3D del circuito, programación, diseño de las carcasas para los nodos, conexión y verificación de los dispositivos para la aplicación de los ataques al sistema previa a la obtención de datos.

En esta fase se cumple el objetivo específico número 2 que es el desarrollo de los nodos del sistema cliente / servidor para establecer la comunicación entre ambos nodos previa a la aplicación de ataques.

En el software de simulación se realiza el diseño esquemático y el modelado 3D de los circuitos que llevan el nodo CLIENTE y el nodo SERVIDOR para construir el diseño PCB de cada nodo. Posteriormente se arma el nodo CLIENTE y el nodo SERVIDOR utilizando las PCB, los módulos de Arduino mini pro, el kit de los módulos de RF apc220, los pulsadores, diodos leds y la alimentación para cada uno.

Se realiza la programación de los nodos mediante el software Arduino IDE para los que uno de los módulos de Arduino pro mini trabaje como un transmisor y el otro como un receptor. En el software de modelado 3D se realiza el diseño de las carcasas para los respectivos nodos.

Después, de tener el armado de los nodos con su respectivo código de programación se procede a la verificación de la conexión entre los mismos, considerando que si la conexión es estable el resultado que se obtiene al momento de la instalación del módulo didáctico es favorable.

FASE 3: Toma de datos con el dispositivo HackRF One, aplicación de ataques con el software URH.

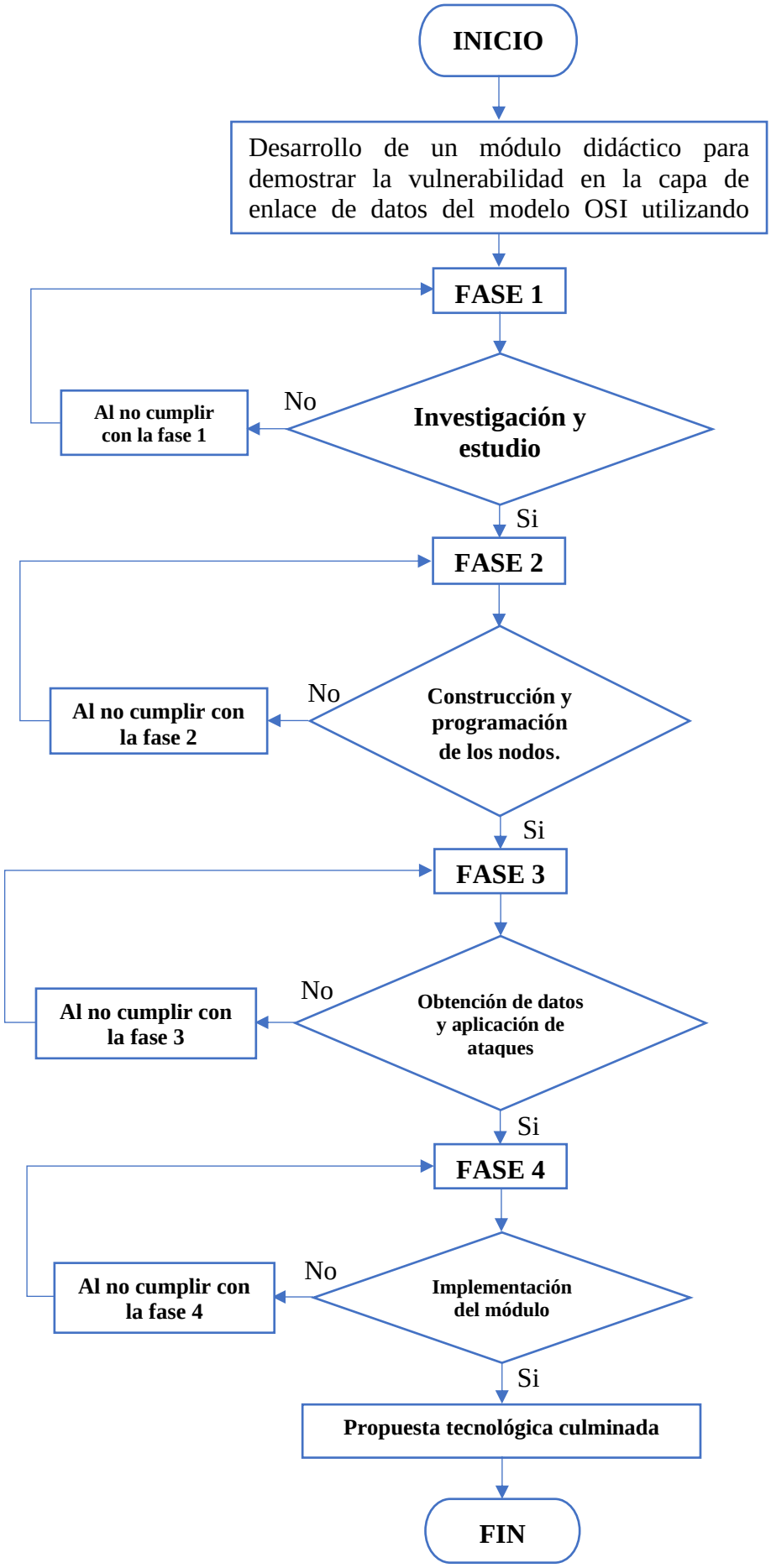
En esta fase se cumple el objetivo específico número 3 que es la toma de datos para la aplicación de los ataques a la comunicación de los nodos. Se utiliza el dispositivo HackRF One como herramienta para la captura de datos en la comunicación de los nodos a través del software URH, para posteriormente aplicar los ataques utilizando los datos capturados.

FASE 4: Diseño, modelado, posicionamiento e implementación del módulo didáctico dentro del laboratorio de telecomunicaciones.

En esta fase se cumple el objetivo específico número 4 que es la implementación del módulo para realizar un manual de la práctica orientada a los ataques en RF. Se utiliza un software de arquitectura o de modelado 3D para diseñar, modelar y posicionar el módulo didáctico dentro del laboratorio de telecomunicaciones. Teniendo el producto final se elabora un manual de la práctica.

Realizadas las 4 fases del proyecto se cumple el objetivo general de la propuesta tecnológica.

A continuación, se detalla el diagrama de flujo de la propuesta tecnológica:


INICIO
Desarrollo de un módulo didáctico para demostrar la vulnerabilidad en la capa de enlace de datos del modelo OSI utilizando
FASE 1
Investigación y estudio
No
Al no cumplir con la fase 1
Si
FASE 2
Construcción y programación de los nodos.
No
Al no cumplir con la fase 2
Si
FASE 3
Obtención de datos y aplicación de ataques
No
Al no cumplir con la fase 3
Si
FASE 4
Implementación del módulo
No
Al no cumplir con la fase 4
Si
Propuesta tecnológica culminada
FIN

CAPITULO II

DESARROLLO DE LA PROPUESTA

2.1 MARCO CONTEXTUAL

En el año 2020 la llegada de la pandemia COVID-19 al ecuador obligó a millones de personas a adoptar la virtualidad como modalidad de trabajo, educación, entretenimiento, comercio, etc. Los ciberataques no se hicieron esperar por parte de los cibercriminales quienes, aprovecharon la situación para realizar actividades maliciosas como el robo de identidad, el robo de datos personales, ataques a conexiones remotas convirtiéndose en una amenaza latente para muchas empresas a nivel nacional [12].

Según los datos de ESET en 2020 los ataques phishing aumentaron un 200% en el Ecuador esto representó el 5,1% a nivel de América Latina ocupando el séptimo lugar de países con más ciberataques [13]. El índice de la ciberseguridad en el Ecuador es tan bajo que apenas y bordea los 25 puntos de 100 [14], en 2022 Ecuador se encontró en el quinto lugar de países con más ciberataques con un 9% a nivel Latinoamericano siendo Perú el primero con el 18% [15].El ataque phishing tiene como base el ataque eavesdropping y se deriva de un ataque MIMT el cual permite leer, capturar y modificar información de manera inalámbrica o cableada.

La Universidad Estatal Península de Santa Elena (UPSE) se creó el 22 de julio del 1998 mediante Ley No 110 expedida por el entonces Congreso Nacional en la presidencia del Arq. Sixto Duran Ballen [16], en la actualidad la UPSE cuenta con 7 facultades y 18 carreras, dentro de ellas se encuentra la Facultad de Sistemas y Telecomunicaciones (FACSISTEL) la cual oferta la carrera de Telecomunicaciones, esta carrera cuenta con el Laboratorio de Telecomunicaciones en donde se va a desarrollar la propuesta tecnológica.

En la malla curricular de la carrera de Telecomunicaciones se tiene la asignatura de Seguridad de redes inalámbricas, la propuesta tecnológica contribuye de manera significativa para esta asignatura porque la propuesta está dirigida a demostrar la vulnerabilidad de la capa de enlace de datos del modelo OSI ante ataques en dispositivos orientados a cliente/servidor de forma inalámbrica mediante un módulo didáctico implementado en el laboratorio de Telecomunicaciones. Con esta clase de propuesta tecnológica se incentiva a los estudiantes al desarrollo de prototipos para brindar seguridad a las redes inalámbrica de manera que se pueda disminuir el porcentaje de ciberataques y aumentar el porcentaje de la ciberseguridad en el Ecuador.

2.2 MARCO CONCEPTUAL

En este apartado se va a definir los conceptos de modelo en capas, vulnerabilidades en los sistemas de comunicaciones, hardware programable, software de programación, módulos de RF, software de simulación de circuitos electrónicos, software de modelado 3D, dispositivos SDR, software para dispositivos SDR y los ataques a la comunicación por RF.

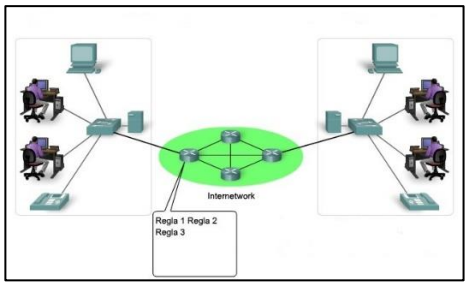
2.2.1 MODELO EN CAPAS DE RED

El modelo en capas de red facilita al diseño de los protocolos, debido a que los protocolos que se tienen por cada capa trabajan con determinadas funciones, ayuda a la interconexión de productos de diferentes marcas para que puedan en la misma red sin problemas, no permita que las capas se vean afectadas en caso de que en una determinada capa exista algún cambio en su tecnología, también entrega un lenguaje común para describir tanto a las funciones como a las capacidades que se tiene en la red [17].

En otras palabras, con el modelo en capas se puede diseñar redes multiservicios, redes complejas y redes utilizando dispositivos de diferentes fabricantes como se referencia en la Figura 2.

Figura 2

Representación de un diseño de una red multiservicio



Nota. La figura representa el diseño de una red multiservicio utilizando productos de distintos fabricantes, tomada de [18]

Los modelos de red en capas se pueden dividir en dos [17]:

- **Modelos de Protocolos.** – Este modelo se ajusta con exactitud a la estructura de una suite de protocolos que se tenga, brindando la funcionalidad que se necesita para que exista la interconexión entre la red de datos y la red humana.
- **Modelos de Referencia.** – Este modelo se adapta con todos los tipos de protocolos y servicios existentes de red describiendo que función se debe cumplir por cada capa específica, pero sin exigir una forma específica para lograrlo.

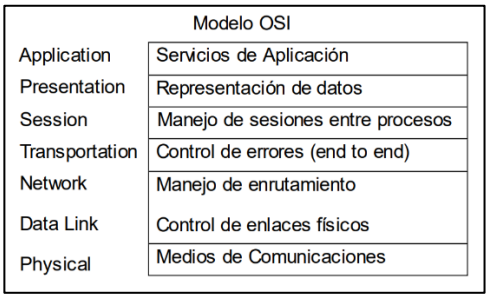
2.2.1.1 MODELO OSI

El modelo OSI es un modelo de referencia que pertenece a ISO y representa un esquema lógico en el que se visualiza la agrupación de funciones que intervienen en el procesamiento y transmisión de datos. Este modelo consiste en 7 capas con su respectiva función que se detallan a continuación, la capa de aplicación ofrece servicios de aplicación, la capa de presentación se

encarga de la representación de datos, la capa de sesión maneja las sesiones entre procesos, la capa de transporte realiza el control de errores, la capa de red maneja el enrutamiento, la capa de enlace de datos controla los enlaces físicos y por último la capa física que representa a los medios de comunicación [19], como se muestra en la Figura 3.

Figura 3

Modelo OSI



Nota. La figura representa las capas del modelo OSI y sus funciones, tomada de [19]

2.2.1.1.1. VULNERABILIDADES DEL MODELO OSI

El objetivo de las vulnerabilidades genéricas del Modelo OSI es dar a conocer las falencias y las técnicas habituales utilizadas para llevar a cabo ataques contra la seguridad de la serie de protocolos TCP/IP, los cuales afectan la disponibilidad, confidencialidad e integridad de la información. Los ataques pueden verse motivados por distintos propósitos entre ellos la interrupción de un sistema, el fraude, la penetración de algún sistema, la extorsión, la venganza, la sustracción de informacion confidencial o el acceso no permitido a un sistema. Los ataques pueden provenir de usuarios que sean autentificados o de atacantes externos [20].

Estas vulnerabilidades pueden ser clasificadas en dos criterios diferentes. El criterio 1 se basa en el número de paquetes necesarios para llevar a cabo el ataque, este se divide en dos tipos de vulnerabilidades la atómica que solo se necesita un paquete para llevar a cabo el ataque y la

compuesta que requiere de varios paquetes para que sea explotada. El criterio 2 se basa en la información necesaria para realizar el ataque, este se divide en dos tipos de vulnerabilidades la de contexto que solo requiere la información de la cabecera del protocolo y de contenido que necesita tanto la información de la cabecera del protocolo como el campo de datos o tambien conocido como payload las vulnerabilidades [21], pueden ser divididas como en la Figura 4.

Figura 4

División de vulnerabilidades

Context	*Ping of death* *Land attack* *WinNuke*	*Port scan* *SYN Flood* *TCP hijacking*
Content	*DNS attack* *Proxied RPC* *IIS attack*	*SMTP attacks* *String matches* *Sniffing*
	Atomic	**Composite**

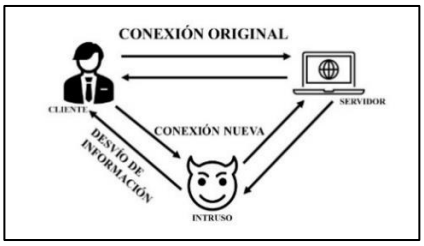
Nota. La figura representa la división de vulnerabilidades según su criterio, tomada de [21].

2.2.1.1.1.1. VULNERABILIDAD EN LA CAPA DE ENLACE DE DATOS DEL MODELO OSI

La vulnerabilidad en la capa de enlace de datos del modelo OSI es un punto crítico en la seguridad de las redes de comunicación. Esta capa, la segunda en el modelo, se encarga de estructurar los datos en tramas, y su vulnerabilidad puede tener consecuencias devastadoras. Los ataques a esta capa pueden capturar tramas legítimas y retransmitirlas para engañar al receptor (ver Figura 5), interrumpir el flujo de datos, causar un comportamiento no deseado o incluso exponer datos sensibles. El envio de tramas de datos por RF son particularmente susceptibles a ataques, ya que un atacante puede manipular las tramas para redirigir el tráfico de manera maliciosa [22].

Figura 5

Ataque en la capa de enlace de datos del Modelo OSI

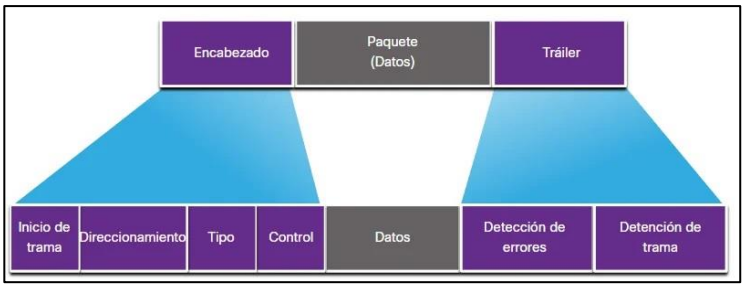


Nota. La figura representa el desvío de información ante una vulnerabilidad en la capa de enlace de datos del modelo OSI, fuente Autor

Las tramas de datos en la capa de enlace de datos del modelo OSI, son unidades de información estructuradas para el intercambio de datos entre dispositivos inalámbricos. Estas tramas incluyen campos como el preámbulo para la sincronización, el delimitador de inicio, las direcciones de origen y destino, el tipo de datos, la carga útil y una secuencia de verificación para asegurar la integridad de los datos [23], como se muestra en el Figura 6.

Figura 6

Trama de enlace de datos



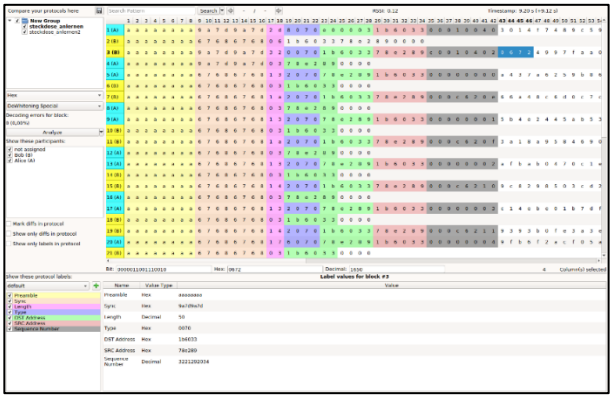
Nota. La figura representa la trama y sus campos, fuente https://calculadoraip.org/ccna1/capa-de-enlace-de-datos/

En comunicaciones RF, las tramas son vulnerables a intercepción de datos (eavesdropping), donde un atacante puede capturar las tramas transmitidas como se muestra en la

Figura 7, exponiendo información sensible; ataques de repetición (replay attacks), en los que se retransmiten tramas legítimas para repetir acciones no autorizadas; y ataques de intermediario (MITM), donde un atacante intercepta, modifica y retransmite tramas sin ser detectado.

Figura 7

Captura de una trama



Nota. La figura muestra la captura de tramas de datos por RF, fuente https://github.com/jopohl/urh

Para mitigar estas amenazas, es crucial implementar encriptación de datos para ataques de tipo eavesdropping, nonces y timestamps para ataques de tipo replay y autenticación mutua para ataques de tipo MITM.

2.2.1.2 MODELO SNA (IBM)

El Sistema de Red de Sistemas (SNA) desarrollado por IBM es un modelo en capas de red que ha sido ampliamente utilizado en el mundo de la informática durante décadas. El modelo SNA se compone de múltiples capas, cada una con funciones específicas las cuales se muestran en la Figura 8, que trabajan juntas para facilitar la comunicación en las redes de IBM. En su núcleo, el SNA se centra en proporcionar una estructura sólida y jerárquica para la comunicación de datos, lo que facilita la interoperabilidad y la gestión de sistemas dentro de un entorno de red [24].

Figura 8

Modelo SNA (IBM)

Modelo SNA (IBM)	
CAPA	FUNCIÓN
7	Realiza el servicio de Transacciones
6	Se encarga de la presentación
5	Controla el flujo de datos
4	Controla la transmisión
3	Controla el camino
2	Controla el encale de datos
1	Nivel Físico

Nota. La figura representa las capas del modelo SNA (IBM) con su respectiva función, fuente Autor.

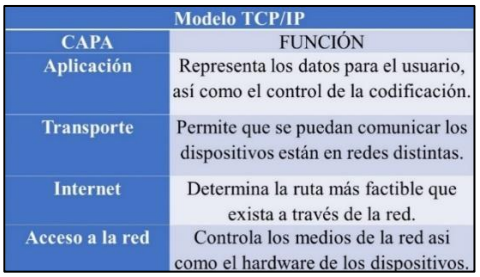
El modelo SNA ha sido valioso en entornos empresariales, ya que permite la conexión de múltiples sistemas y dispositivos, lo que resulta en una colaboración eficiente y una gestión centralizada. A medida que la tecnología de redes ha evolucionado, el SNA ha sido adaptado y extendido para satisfacer las necesidades cambiantes de las organizaciones. Aunque en la actualidad se han desarrollado otros modelos en capas de red, el SNA sigue siendo un ejemplo destacado de cómo una estructura jerárquica puede mejorar la comunicación y la gestión en un entorno de red complejo.

2.2.1.3 MODELO TCP/IP

El Modelo TCP/IP, también conocido como el Protocolo de Control de Transmisión/Protocolo de Internet, es un modelo en capas ampliamente utilizado en el mundo de las comunicaciones de redes. Este modelo consta de cuatro capas: la capa de enlace de datos, la capa de red, la capa de transporte y la capa de aplicación. Cada capa tiene funciones específicas y trabaja en conjunto para permitir la comunicación eficiente en redes IP [25], como se muestra en la Figura 9.

Figura 9

Modelo TCP/IP



Modelo TCP/IP	
CAPA	FUNCIÓN
Aplicación	Representa los datos para el usuario, así como el control de la codificación.
Transporte	Permite que se puedan comunicar los dispositivos están en redes distintas.
Internet	Determina la ruta más factible que exista a través de la red.
Acceso a la red	Controla los medios de la red asi como el hardware de los dispositivos.

Nota. La figura representa las capas del modelo TCP/IP con sus funciones específicas, fuente Autor

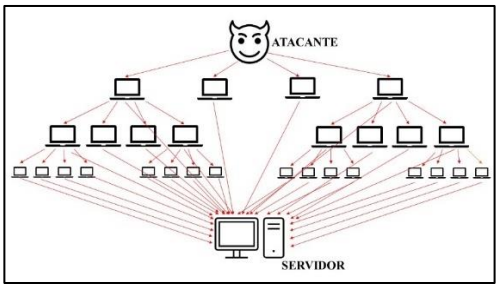
Con el pasar del tiempo el Modelo TCP/IP se ha convertido en el estándar dominante en la comunicación de redes, especialmente en Internet. Su diseño modular y su flexibilidad han permitido su adaptación a una amplia variedad de aplicaciones y entornos de red. A medida que la tecnología de redes ha evolucionado, el Modelo TCP/IP ha seguido siendo relevante y ha proporcionado un marco sólido para la comunicación global. Su éxito radica en gran parte en su capacidad para admitir diferentes protocolos y tecnologías subyacentes, lo que lo convierte en un modelo escalable y versátil que sigue siendo fundamental en la infraestructura de Internet.

2.2.2. VULNERABILIDAD EN LOS SISTEMAS DE COMUNICACIONES

La vulnerabilidad en los sistemas de comunicaciones es un tema crítico en la era digital actual. A medida que las organizaciones y las personas dependen cada vez más de las comunicaciones electrónicas, los sistemas se vuelven objetivos valiosos para los ciber atacantes. Estos sistemas pueden sufrir una variedad de amenazas, que van desde ataques de denegación de servicio distribuido (DDoS) que interrumpen la conectividad como se aprecia en la Figura 8, hasta ataques de interceptación de datos que comprometen la confidencialidad de la información transmitida [26], como se muestra en la Figura 10.

Figura 10

Ataque DDoS



Nota. La figura representa un servido recibiendo un ataque DDoS, fuente Autor.

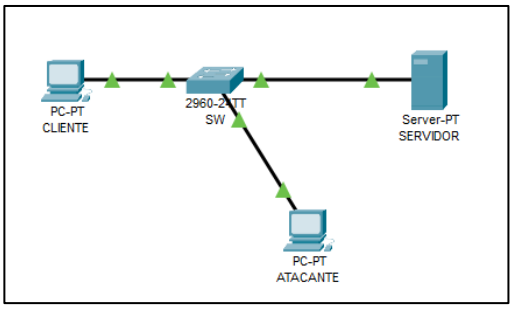
Para abordar la vulnerabilidad en los sistemas de comunicaciones, es esencial implementar medidas de seguridad efectivas, lo cual incluye el uso de cifrado sólido para proteger los datos en tránsito, la autenticación de usuarios y dispositivos, la segmentación de redes para limitar el alcance de posibles ataques y la capacitación de los usuarios para que estén alerta ante posibles amenazas. Además, la colaboración entre organizaciones, gobiernos y entidades internacionales es crucial para combatir amenazas a gran escala y garantizar la integridad de las comunicaciones en un mundo cada vez más interconectado.

2.2.2.1. VULNERABILIDADES DE LAS COMUNICACIONES ALÁMBRICAS

Las comunicaciones alámbricas, a pesar de su uso extendido y la aparente seguridad que ofrecen, también presentan vulnerabilidades significativas en los sistemas de comunicaciones. Los cables que conectan dispositivos y redes pueden ser propensos a ataques físicos, como el acceso no autorizado a través de la manipulación de cables o la inserción de dispositivos de escucha en la infraestructura de red, tales riesgos pueden exponer la información confidencial y comprometer la integridad de las comunicaciones [27], como se muestra en la Figura 11.

Figura 11

Comunicación alámbrica vulnerada



Nota. La figura representa la conexión de un atacante por medio físico a una red, fuente Autor.

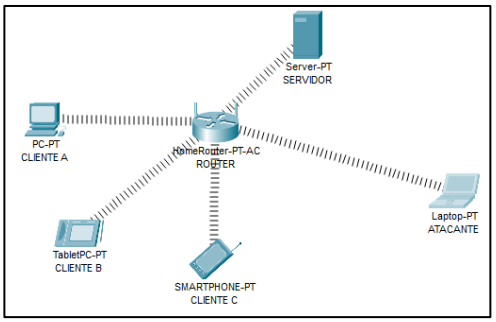
Para mitigar las vulnerabilidades en las comunicaciones alámbricas, es fundamental implementar prácticas de seguridad física, como el acceso restringido a áreas sensibles y la monitorización de la infraestructura de cableado. También es importante utilizar tecnologías de cifrado para proteger los datos en tránsito a través de los cables. La seguridad de la red alámbrica debe ser una parte integral de la estrategia de seguridad de una organización, ya que, aunque menos visible que las amenazas cibernéticas, las vulnerabilidades en las comunicaciones alámbricas pueden tener un impacto significativo en la seguridad y la confidencialidad de los datos.

2.2.2.2. VULNERABILIDADES DE LAS COMUNICACIONES INALÁMBRICAS

Las comunicaciones inalámbricas, si bien ofrecen una mayor flexibilidad y movilidad, también presentan una serie de desafíos y vulnerabilidades en los sistemas de comunicaciones. Estos sistemas, como Wi-Fi, Bluetooth y 4G/5G, son particularmente susceptibles a amenazas como la interceptación de señales, ataques de suplantación de identidad y ataques de denegación de servicio. La falta de cables en las comunicaciones inalámbricas hace que sea más fácil para los atacantes acceder y perturbar las redes, lo que puede poner en peligro la confidencialidad y la integridad de los datos transmitidos [27], como se muestra en la Figura 12.

Figura 12

Comunicación inalámbrica vulnerada



Nota. La figura representa la conexión de un atacante por medio inalámbrico a una red, fuente Autor.

Para abordar estas vulnerabilidades en las comunicaciones inalámbricas, es esencial implementar medidas de seguridad robustas, como la autenticación sólida de dispositivos, el cifrado de datos y la gestión adecuada de claves de seguridad. Además, la concienciación y la educación de los usuarios sobre las mejores prácticas de seguridad en redes inalámbricas son fundamentales. La evolución constante de las tecnologías inalámbricas exige que las organizaciones y los usuarios estén al tanto de las últimas amenazas y soluciones de seguridad para garantizar que las comunicaciones inalámbricas sigan siendo seguras y fiables en un mundo cada vez más interconectado.

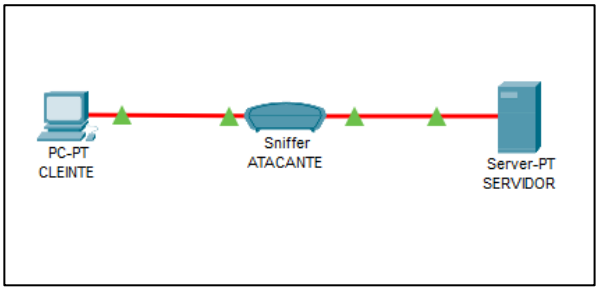
2.2.2.3. VULNERABILIDADES DE LAS COMUNICACIONES ÓPTICAS

Las comunicaciones ópticas, que se basan en la transmisión de datos a través de señales de luz a través de fibras ópticas, representan una forma avanzada de comunicación que ha revolucionado la velocidad y la capacidad de las redes de telecomunicaciones. Sin embargo, también conllevan su propia serie de vulnerabilidades en los sistemas de comunicaciones (ver Figura 13). Los cables de fibra óptica, aunque altamente seguros en comparación con otros medios

de transmisión, aún pueden ser vulnerables a daños físicos, como cortes o roturas, que pueden interrumpir la conectividad y exponer puntos débiles en la infraestructura [28].

Figura 13

Comunicación por fibra óptica vulnerada



Nota. La figura representa la conexión de un atacante por medio óptico a una red, fuente Autor.

Para abordar las vulnerabilidades en las comunicaciones ópticas, es esencial implementar medidas de seguridad física, como la protección de las fibras ópticas y la redundancia en la infraestructura. Además, el cifrado de datos en las comunicaciones ópticas es fundamental para proteger la información transmitida. La seguridad en las comunicaciones ópticas es especialmente relevante en entornos críticos, como las redes de telecomunicaciones de alta velocidad y las redes de transporte de datos, donde la integridad y la confidencialidad de la información son de vital importancia.

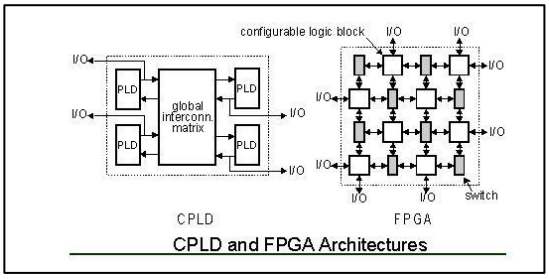
2.2.3. HARDWARE PROGRAMABLE

El hardware programable se refiere a dispositivos electrónicos cuya funcionalidad puede configurarse y reconfigurarse mediante software. Este enfoque proporciona una flexibilidad significativa en comparación con el hardware tradicional, que tiene una funcionalidad fija. Los dispositivos de hardware programable, como las FPGAs (Field-Programmable Gate Arrays) y CPLDs (Complex Programmable Logic Devices) (ver Figura 14), permiten a los ingenieros y

desarrolladores diseñar y personalizar circuitos electrónicos de acuerdo con las necesidades específicas de sus aplicaciones [29].

Figura 14

Arquitectura de FPGA y CPLD



Nota. La figura representa la configuración interna de FPGA y CPLD, fuente https://www.ic-cracker.com/fpga-cpld-difference/

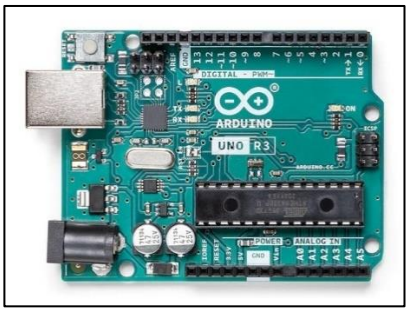
El hardware programable ofrece ventajas notables en términos de velocidad de desarrollo, capacidad de prototipado y adaptación a requisitos cambiantes, ya que los diseñadores pueden utilizar herramientas de diseño de hardware específicas para configurar la funcionalidad de estos dispositivos de manera eficiente. Además, las FPGAs y CPLDs son especialmente útiles en aplicaciones que requieren un alto rendimiento y baja latencia, como procesamiento de señales, criptografía y aceleración de algoritmos.

2.2.3.1.ARDUINO

El Arduino es un ejemplo destacado de hardware programable (ver Figura 15) que ha ganado popularidad en el ámbito de la electrónica y la programación. Se trata de una plataforma de código abierto que combina hardware y software para crear dispositivos electrónicos personalizados. Los usuarios pueden programar microcontroladores Arduino para realizar una amplia gama de tareas, desde controlar luces y sensores en proyectos de bricolaje hasta desarrollar sistemas de automatización más complejos [30].

Figura 15

Placa UNO R3 de Arduino



Nota. La figura representa la placa UNO R3, fuente https://store.arduino.cc/products/arduino-uno-rev3

El enfoque accesible y de código abierto de Arduino lo hace particularmente atractivo para principiantes y entusiastas de la electrónica. La plataforma proporciona una amplia variedad de placas y módulos que se pueden programar utilizando el entorno de desarrollo integrado de Arduino. Los proyectos que utilizan Arduino a menudo involucran sensores, actuadores y componentes electrónicos, lo que permite a los usuarios aprender sobre electrónica y programación de manera práctica.

2.2.3.2.RASPBERRY PI

El Raspberry Pi (ver Figura 16) es una plataforma de hardware programable de bajo costo que ha ganado una gran popularidad en la comunidad de entusiastas de la electrónica y la informática. Se trata de una serie de computadoras de placa única (SBC) que ofrecen un conjunto de componentes esenciales para la informática, como CPU, memoria, puertos USB y HDMI, en un factor de forma compacto. Lo que hace que el Raspberry Pi sea especialmente atractivo es su capacidad de programación y personalización [31].

Figura 16

Placa Pi 5 de Raspberry

Nota. La figura representa la placa Pi 5, fuente https://www.raspberrypi.com/products/

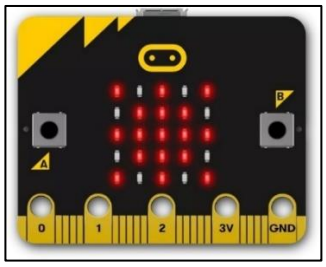
Con el paso del tiempo la plataforma de hardware Raspberry Pi ha demostrado ser una herramienta valiosa en la educación y la formación en ciencias de la computación y la electrónica. Su accesibilidad y bajo costo permiten a estudiantes y aficionados adentrarse en el mundo de la programación y la electrónica sin necesidad de una inversión significativa. Además, su comunidad activa y el soporte de código abierto fomentan la colaboración y la innovación en proyectos diversos

2.2.3.3.MICRO: BIT

La placa micro: bit (ver Figura 17) es otro ejemplo destacado de hardware programable que se ha convertido en una herramienta invaluable en la enseñanza y el aprendizaje de la programación y la electrónica. Este pequeño dispositivo, del tamaño de una tarjeta de crédito, está diseñado para ser accesible y fácil de usar, especialmente para estudiantes y principiantes en electrónica y programación. El micro: bit incorpora sensores, luces LED y conexiones inalámbricas, lo que permite a los usuarios crear una amplia variedad de proyectos interactivos [32].

Figura 17

Placa de micro: bit



Nota. La figura representa un icono de un sol, fuente https://microbit.org/projects/make-it-code-it/here-comes-the-sun/

Esta es una herramienta efectiva para fomentar el interés en STEM y la programación en los estudiantes jóvenes, su versatilidad y asequibilidad lo convierten en una plataforma ideal para proyectos educativos que van desde juegos y simulaciones hasta la creación de dispositivos interactivos. Al igual que el Raspberry Pi y Arduino, el micro: bit ha demostrado ser una plataforma valiosa para la enseñanza y la experimentación en el campo de la tecnología, y sigue siendo una herramienta prometedora para inspirar a la próxima generación de innovadores y programadores.

2.2.4. SOFTWARE DE PROGRAMACIÓN

El software de programación es una herramienta esencial para los desarrolladores y programadores en la creación y modificación de aplicaciones informáticas, tales herramientas proporcionan un entorno de desarrollo que permite a los programadores escribir, depurar y probar el código necesario para construir software funcional. Los lenguajes de programación, como Java, Python, C++ y otros, se utilizan junto con el software de programación para traducir el código escrito por el programador en instrucciones comprensibles para la computadora [33].

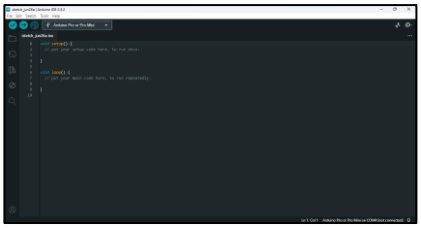
El software de programación varía en función de la plataforma y el lenguaje de programación elegidos. Existen opciones de código abierto, como Visual Studio Code, y herramientas comerciales como Microsoft Visual Studio. Además, los entornos de desarrollo integrado (IDE) son populares entre los programadores, ya que ofrecen una solución completa que incluye un editor de código, un depurador y herramientas de compilación.

2.2.4.1.ARDUINO IDE

El Arduino IDE (Entorno de Desarrollo Integrado) es una herramienta de programación ampliamente utilizada en la comunidad de Arduino y la electrónica de bricolaje. Este software se ha diseñado específicamente para programar placas Arduino, que son dispositivos de hardware programable, este proporciona una interfaz de usuario sencilla y un entorno de desarrollo intuitivo que permite a los usuarios escribir y cargar código en las placas Arduino de manera eficiente [34].

Figura 18

Software Arduino IDE



Nota. La figura representa la interfaz del software Arduino IDE, fuente Autor.

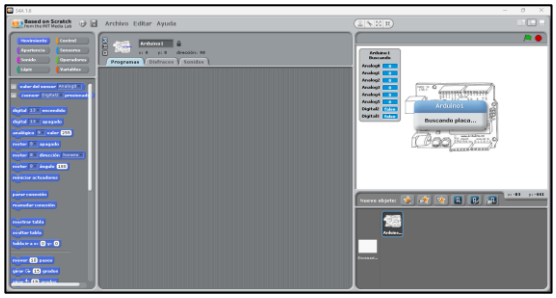
A través de este los programadores pueden acceder a una amplia variedad de bibliotecas y recursos de código abierto que facilitan el desarrollo de proyectos personalizados. Además, la comunidad de Arduino es activa y colaborativa, lo que promueve el intercambio de conocimientos y la creación de proyectos innovadores. Motivo por el cual el Arduino IDE sigue siendo una opción atractiva para quienes desean experimentar con hardware programable y desarrollar proyectos electrónicos personalizados de manera efectiva.

2.2.4.2.S4A

S4A es un entorno de programación visual diseñado para introducir a principiantes en el mundo de la programación de una manera accesible. A diferencia de los lenguajes de programación tradicionales, esta utiliza bloques de programación que se ensamblan como piezas de un rompecabezas en lugar de requerir la escritura de código. Tal enfoque permite a los usuarios crear proyectos interactivos, lo que lo convierte en una herramienta valiosa para la educación en ciencias de la computación y la creatividad [35].

Figura 19

Software S4A



Nota. La figura representa la interfaz del software S4A, fuente Autor.

Los proyectos creados en S4A pueden variar desde simulaciones educativas y aplicaciones de juegos simples. Además, la plataforma cuenta con una comunidad en línea activa que comparte proyectos y recursos, lo que promueve el aprendizaje colaborativo y la inspiración entre los usuarios. Motivo por el cual S4A sigue siendo una forma efectiva y atractiva de introducir a personas de todas las edades en el mundo de la programación y la informática.

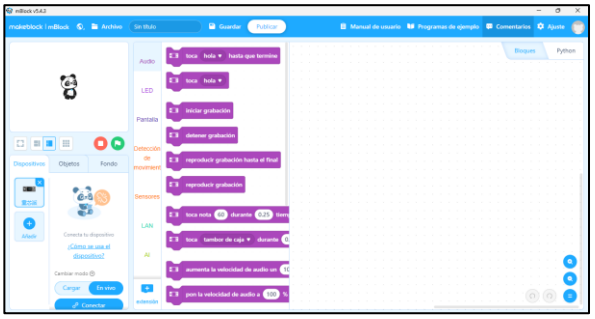
2.2.4.3.MBLOCK

mBlock, también conocido como mBlock 5, es un entorno de programación basado en bloques que se utiliza principalmente en la enseñanza de programación y robótica. Está diseñado para hacer que la programación sea accesible y atractiva para principiantes, especialmente para

niños y jóvenes que deseen aprender a codificar y controlar robots y otros dispositivos electrónicos [36].

Figura 20

Software mBlock



Nota. La figura representa la interfaz del software mBlock, fuente Autor.

Este utiliza una interfaz de programación de arrastrar y soltar, donde los usuarios ensamblan bloques gráficos para crear secuencias de comandos que controlan el comportamiento de los robots y otros proyectos electrónicos, lo cual elimina la necesidad de escribir código desde cero, lo que facilita la curva de aprendizaje y permite a los usuarios centrarse en la lógica de programación y la creatividad.

2.2.5. MÓDULOS DE RF

Los módulos de RF (Radiofrecuencia) son componentes esenciales en las comunicaciones inalámbricas, que permiten la transmisión y recepción de señales de radio en una variedad de aplicaciones. Estos módulos están diseñados para operar en diferentes frecuencias de radio, como 434 MHz, 868 MHz o 2.4 GHz, y se utilizan en sistemas de control remoto, comunicaciones IoT (Internet de las cosas), sistemas de alarma, telecomunicaciones y más [37].

La versatilidad de los módulos de RF los convierte en componentes fundamentales en el diseño de sistemas inalámbricos, tales módulos se utilizan en una variedad de aplicaciones donde

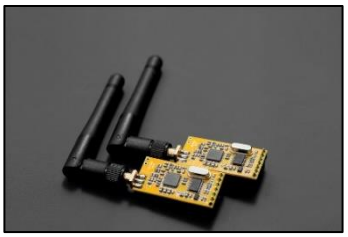
la comunicación inalámbrica es esencial, como la transmisión de datos entre sensores y actuadores, la comunicación entre dispositivos remotos y la conectividad en redes de sensores. Los módulos de RF ofrecen una amplia gama de opciones en términos de alcance, velocidad de transmisión y características, lo que permite a los diseñadores adaptar sus aplicaciones a las necesidades específicas de su proyecto

2.2.5.1.APC220 RF

El APC220 RF (ver Figura 21) es un módulo de radiofrecuencia (RF) que se ha ganado reconocimiento por su uso en aplicaciones de comunicación inalámbrica a corta distancia. Este módulo de RF opera en la banda de frecuencia de 434 MHz, lo que le permite transmitir datos de manera confiable a través de distancias relativamente cortas, generalmente de unos pocos cientos de metros. El APC220 RF se utiliza en una variedad de aplicaciones, como control remoto de dispositivos, telemetría, monitoreo de sensores y sistemas de adquisición de datos inalámbricos [37].

Figura 21

Módulos APC220



Nota. La figura representa los módulos APC220 de RF, fuente https://www.dfrobot.com/product-57.html

Una de las ventajas del APC220 RF es su facilidad de uso y configuración, ya que dicho modulo se comunica mediante una interfaz UART, lo que significa que puede conectarse

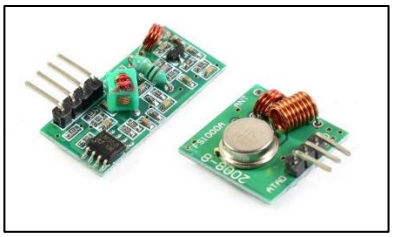
directamente a microcontroladores como Arduino o Raspberry Pi, lo que a su vez también facilita la integración en proyectos de electrónica. Además, el APC220 RF se suministra con su propio software de configuración, lo que permite a los usuarios personalizar la frecuencia de transmisión, la velocidad de datos y otros parámetros de comunicación según sus necesidades específicas.

2.2.5.2.FS1000A - XY-MK-5V

El módulo transmisor FS1000A y el módulo receptor XY-MK-5V de RF a 433 MHz (ver Figura 22) son dispositivos populares en el mundo de la radiofrecuencia, conocidos por su versatilidad y uso generalizado en aplicaciones de comunicación inalámbrica, permitiéndole operar en la banda de frecuencia de 433 MHz, que es ampliamente aceptada y regulada en muchas regiones del mundo, hecho el cual los convierte en una opción atractiva para proyectos que requieren una comunicación inalámbrica confiable a distancias moderadas, como sistemas de control remoto, sistemas de alarma, sistemas de monitoreo y transmisión de datos a corta distancia [38].

Figura 22

Módulos FS1000A - XY-MK-5V



Nota. La figura representa el módulo transmisor (FS1000A) y receptor (XY-MK-5V), fuente https://naylampmechatronics.com/blog/32_comunicacion-inalambrica-con-modulos-de-rf-de-433mhz.html

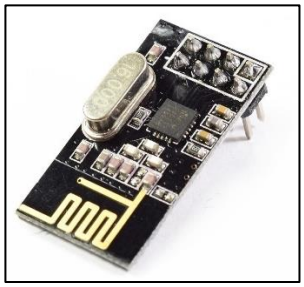
Este módulo es sumamente popular entre los entusiastas de la electrónica y la robótica debidos a su facilidad de uso y la disponibilidad de bibliotecas y recursos de código abierto que simplifican la implementación en proyectos. Así como también su diseño simple y su capacidad para transmitir y recibir datos a través de antenas de bajo costo lo hacen adecuado para aplicaciones de bricolaje y prototipado.

2.2.5.3.NRF24L01

El módulo NRF24L01 (ver Figura 23) es un componente de radiofrecuencia (RF) ampliamente utilizado en aplicaciones de comunicación inalámbrica, conocido por su versatilidad y su capacidad de comunicación a corta y media distancia. Este módulo opera en la banda de frecuencia de 2.4 GHz y utiliza la modulación GFSK (Modulación por Desplazamiento de Frecuencia con Saltos de Fase Gaussiana) para transmitir datos de manera eficiente y confiable [37].

Figura 23

Módulo NRF24L01



Nota. La figura representa el módulo NRF24L01, fuente https://naylampmechatronics.com/inalambrico/38-modulo-rf-nrf24l01.html

Lo que hace que el NRF24L01 sea especialmente atractivo es su capacidad para configurar redes inalámbricas de nodo a nodo, lo que permite la comunicación bidireccional entre varios

dispositivos. Este módulo se ha vuelto popular en aplicaciones de Internet de las cosas (IoT) y en proyectos de robótica donde se requiere una comunicación inalámbrica confiable y eficiente.

2.2.6. SOFTWARE DE SIMULACION DE CIRCUITOS ELECTRÓNICOS

El software de simulación de circuitos electrónicos es una herramienta esencial en el campo de la electrónica y la ingeniería, la utilización de este tipo de software permite a los ingenieros y diseñadores crear modelos virtuales de circuitos eléctricos y electrónicos, lo que les permite evaluar y probar el funcionamiento de sus diseños antes de implementarlos en la vida real [39].

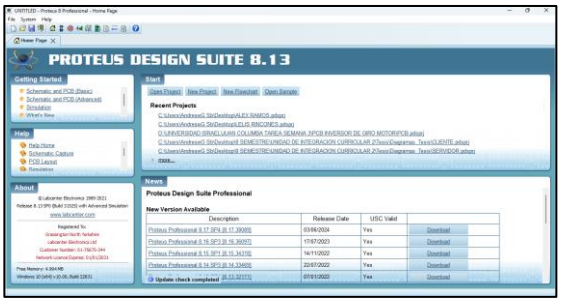
Este tipo de software se utiliza en una amplia gama de aplicaciones, desde la investigación y desarrollo de productos electrónicos hasta la educación en ciencias de la computación y electrónica. Los ingenieros pueden utilizar estos programas para optimizar el rendimiento de sus diseños, identificar posibles problemas y reducir el tiempo y los costos asociados con la creación de prototipos físicos.

2.2.6.1.PROTEUS

Proteus es un software de simulación de circuitos electrónicos ampliamente utilizado en la industria y la educación, tal herramienta proporciona a los ingenieros y diseñadores una plataforma integral para crear y simular circuitos eléctricos y electrónicos con una precisión impresionante. Proteus incluye una extensa biblioteca de componentes electrónicos, desde componentes básicos como resistencias y transistores hasta microcontroladores y sensores, lo que permite a los usuarios diseñar circuitos complejos con facilidad [39].

Figura 24

Proteus



Nota. La figura representa la interfaz de Proteus v8.13, fuente Autor.

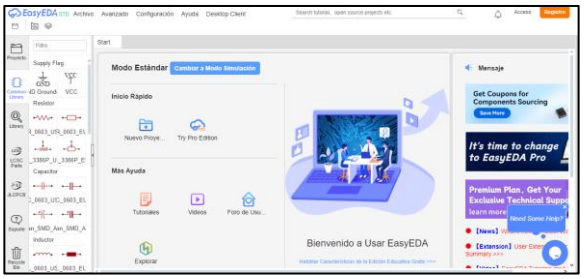
Una de las características más destacadas de Proteus es su capacidad de simular tanto el comportamiento eléctrico como el comportamiento del software en microcontroladores integrados, lo cual les permite a los diseñadores de sistemas emular el funcionamiento completo de un dispositivo electrónico, lo que es especialmente útil en el desarrollo de sistemas embebidos.

2.2.6.2.EASYEDA

EasyEDA es un software de simulación de circuitos electrónicos basado en la nube que se ha ganado una sólida reputación en la comunidad de diseño de electrónica. Este entorno de diseño proporciona una plataforma en línea que permite a los ingenieros y diseñadores crear, simular y compartir circuitos electrónicos de manera colaborativa, ya que cuenta con una interfaz de usuario intuitiva que simplifica el proceso de diseño [40].

Figura 25

Easy EDA



Nota. La figura representa la interfaz de Easy EDA online, fuente https://easyeda.com/editor

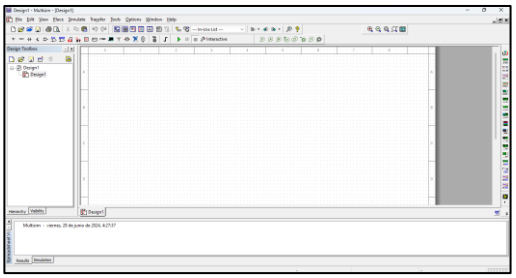
Este software incluye características de colaboración en tiempo real que facilitan el trabajo en equipo en proyectos de diseño de electrónica, ya que a través de este los usuarios pueden compartir sus proyectos, colaborar en tiempo real y comentar sobre diseños, lo que mejora la eficiencia y la comunicación en el desarrollo de circuitos electrónicos. Motivo por el cual la misma se ha convertido en una herramienta valiosa para la comunidad de diseño de electrónica y ha contribuido a la simplificación y democratización del proceso de diseño de circuitos electrónicos.

2.2.6.3.MULTISIM

Multisim es un software de simulación de circuitos electrónicos desarrollado por National Instruments, conocido por su capacidad avanzada de simulación y análisis. Esta herramienta es ampliamente utilizada en la industria y la educación para el diseño y la evaluación de circuitos electrónicos, este le permite a los ingenieros y diseñadores crear esquemáticos electrónicos y realizar simulaciones de circuitos de manera precisa y eficiente [40].

Figura 26

Multisim



Nota. La figura representa la interfaz de Multisim, fuente Autor.

Una de las características destacadas de Multisim es su capacidad para realizar simulaciones tanto de dominio de tiempo como de dominio de frecuencia, lo que permite a los usuarios analizar el comportamiento de los circuitos en una variedad de condiciones y escenarios, esta herramienta también ofrece características avanzadas de análisis de señales, como análisis de Fourier y análisis de ruido, que son esenciales en aplicaciones de diseño electrónico de alta precisión.

2.2.7. SOFTWARE DE MODELADO 3D

El software de modelado 3D es una herramienta fundamental en campos como el diseño industrial, la arquitectura, la animación y la impresión 3D. Estas aplicaciones permiten a los diseñadores y artistas crear representaciones tridimensionales de objetos y entornos de manera digital. Los programas de modelado 3D proporcionan una variedad de herramientas y características que permiten a los usuarios esculpir, modelar y texturizar objetos en un espacio tridimensional [41].

Este tipo de software varía en complejidad, desde herramientas de modelado básicas dirigidas a principiantes hasta aplicaciones de modelado y animación de alta gama utilizadas por profesionales. Algunos ejemplos populares de software de modelado 3D incluyen:

2.2.7.1. SKETCHUP

SketchUp es un software de modelado 3D ampliamente utilizado en campos como la arquitectura, el diseño de interiores, la ingeniería y la construcción, tal programa se destaca por su interfaz de usuario intuitiva y su capacidad para crear modelos 3D con facilidad, lo que lo hace especialmente popular entre los diseñadores y arquitectos, así como también el hecho de que le permite a los usuarios diseñar edificios (ver Figura 27), objetos, paisajes y más mediante herramientas de modelado 3D simples de usar, como extrusión y dibujo a mano alzada [42].

Figura 27

SketchUp

Nota. La figura representa un modelado de edificios en 3D, fuente https://www.sketchup.com/es

Lo que diferencia a SketchUp del resto de software de modelado 3d es su accesibilidad y versatilidad, ya que, mediante esta, sus usuarios pueden crear modelos desde cero o importar y editar modelos existentes en una variedad de formatos, lo que facilita la colaboración y la interoperabilidad en proyectos de diseño. Además, SketchUp se utiliza en la etapa inicial de diseño para la visualización de conceptos y en la etapa final para la generación de documentos y planos detallados.

2.2.7.2. AUTODESK INVENTOR

Inventor es un software de modelado 3D y diseño asistido por ordenador (CAD) desarrollado por Autodesk, este programa es una de las herramientas más ampliamente utilizadas en el mundo del diseño, la ingeniería y la arquitectura (ver Figura 28). Mediante este software se ofrece una amplia gama de capacidades de modelado 3D que permiten a los usuarios crear modelos tridimensionales de objetos y estructuras con un alto nivel de detalle y precisión [41].

Figura 28

Autodesk Inventor

Nota. La figura representa un modelo comercial de enfriador en 3D, fuente https://www.autodesk.com/es/products/inventor/overview

La interoperabilidad de Inventor con otros programas de diseño y la disponibilidad de numerosos complementos y aplicaciones de terceros amplían su funcionalidad, lo que lo convierte en una herramienta esencial en el mundo del diseño y la ingeniería para diseñadores de interiores, arquitectos, ingenieros civiles y mecánicos. Contribuyendo en gran manera a la eficiencia y precisión en el desarrollo de proyectos complejos.

2.2.7.3. ADOBE ILLUSTRATOR

Adobe Illustrator es un software de diseño gráfico vectorial ampliamente utilizado en la creación de ilustraciones y gráficos en 2D, pero no es un software de modelado 3D. A diferencia de herramientas de modelado 3D como AutoCAD, Blender o SketchUp, Illustrator se centra en la

creación de imágenes y gráficos en dos dimensiones (ver Figura 29). Los usuarios de Illustrator aprovechan sus capacidades de dibujo vectorial para crear ilustraciones, logotipos, diseño de carteles y gráficos vectoriales que son escalables sin pérdida de calidad [43].

Figura 29

Adobe Illustrator

Nota. La figura representa una ilustración en 3D, fuente https://www.adobe.com/ec/products/illustrator.html

Lo que distingue a Illustrator es su amplia gama de herramientas y capacidades de dibujo vectorial, que permiten a los diseñadores crear obras de arte altamente detallada y versátil, este software incluye una variedad de pinceles, formas, efectos y filtros que permiten la creación de diseños personalizados. Illustrator se utiliza en diversas industrias, desde la publicidad y el diseño de marca hasta la creación de ilustraciones para libros y medios digitales

2.2.8. DISPOSITIVOS SDR

Los dispositivos SDR (Software Defined Radio) son una tecnología revolucionaria en el campo de las comunicaciones y la radio, dichos dispositivos permiten a los usuarios capturar, procesar y transmitir señales de radio utilizando software y hardware flexibles. A diferencia de los receptores de radio tradicionales, que dependen de circuitos y componentes fijos, los SDR utilizan hardware configurable y software para adaptarse a diferentes frecuencias y modulaciones [44].

La flexibilidad y la capacidad de adaptación de los dispositivos SDR han transformado la forma en que se abordan los desafíos en comunicaciones y radiofrecuencia. Los investigadores y profesionales pueden utilizar SDR para explorar y analizar el espectro de radio, desarrollar sistemas de comunicación personalizados y realizar pruebas de protocolos de comunicación.

2.2.8.1. HACKRF ONE

El HackRF One (ver Figura 30) es un dispositivo SDR (Software Defined Radio) ampliamente utilizado que se destaca por su versatilidad y capacidad de adaptación, este dispositivo permite a los usuarios capturar, transmitir y manipular señales de radio de manera flexible a través de software, lo que lo convierte en una herramienta valiosa para una amplia gama de aplicaciones ya que posee un rango de frecuencias, desde 1 MHz hasta 6 GHz [44].

Figura 30

HackRF One

Nota. La figura representa al dispositivo SDR HackRF One, fuente https://greatscottgadgets.com/hackrf/one/

Este dispositivo de SDR es ampliamente utilizado por entusiastas de la radio afición, investigadores en telecomunicaciones y profesionales de seguridad informática, ya que proporciona una plataforma flexible y poderosa para experimentar con señales de radio y desarrollar soluciones personalizadas en el campo de las comunicaciones inalámbricas.

2.2.8.2. RTL-SDR

El RTL-SDR (ver Figura 31) es un dispositivo económico y versátil que ha ganado una gran popularidad en la comunidad de radioaficionados, entusiastas de la radio y profesionales que trabajan en el campo de las comunicaciones. Este dispositivo utiliza un sintonizador de televisión digital (RTL2832U) y un chip de radio definida por software (SDR) para capturar señales de radio y procesarlas mediante software [45].

Figura 31

RTL-SDR

Nota. La figura representa el dispositivo RTL-SDR, fuente https://www.rtl-sdr.com

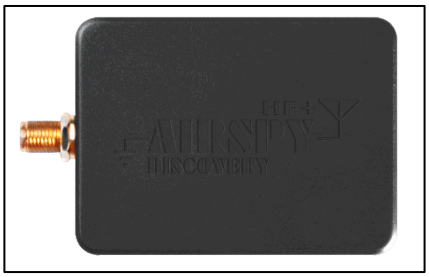
En la actualidad el RTL-SDR se ha convertido en una herramienta de aprendizaje poderosa y accesible para aquellos que desean explorar el mundo de la radio y la radiofrecuencia, y ha encontrado aplicaciones en la seguridad de la radio y en la monitorización del espectro electromagnético, lo que lo convierte en un dispositivo SDR muy valorado en diversas comunidades.

2.2.8.3. AIRSPY SDR

El Airspy SDR (ver Figura 32) es un dispositivo de alta calidad que ha ganado reconocimiento por su rendimiento y versatilidad en el mundo de la radio definida por software. Diseñado por Airspy, este dispositivo ofrece un amplio rango de frecuencias de operación, lo que permite la captura y procesamiento de señales en una variedad de bandas de radio, desde HF (alta frecuencia) hasta VHF y UHF [45].

Figura 32

AIRSPY SDR



Nota. La figura representa al dispositivo AIRSPY SDR, fuente https://airspy.com

Este dispositivo se destaca por su capacidad de sintonización y su capacidad de recepción de señales débiles, lo que lo hace especialmente valioso en aplicaciones de monitoreo de radio y recepción de señales de radio de banda ancha. Los usuarios pueden utilizar software de SDR, como SDR# o GNU Radio, para explorar y decodificar una variedad de señales, incluyendo transmisiones de radio, señales de radioaficionados, sistemas de comunicación de radio bidireccional y más.

2.2.9. SOFTWARE PARA DISPOSITIVOS SDR

El software para dispositivos SDR (Software Defined Radio) es una parte esencial de la experiencia de SDR, ya que permite a los usuarios interactuar con los dispositivos SDR y procesar las señales de radio de manera efectiva, este software se utiliza para controlar, sintonizar y decodificar señales de radio en un entorno de software, lo que hace que los dispositivos SDR sean altamente versátiles y personalizables [46].

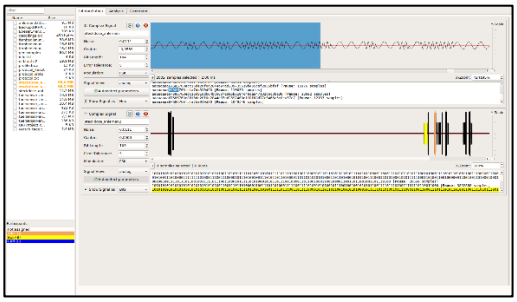
Existen numerosos programas de software SDR disponibles, y la elección del software depende en gran medida de las necesidades y preferencias del usuario. Algunos ejemplos populares incluyen:

2.2.9.1. URH

Universal Radio Hacker (URH) es un software de código abierto para dispositivos SDR (Software Defined Radio) que se ha ganado una creciente popularidad en la comunidad de radioaficionados, investigadores y entusiastas de la radio definida por software. URH ofrece una plataforma versátil para la recepción (ver Figura 33), decodificación y análisis de señales de radio [46].

Figura 33

Universal Radio Hacker



Nota. La figura representa la extracción de datos de una señal de RF, fuente https://github.com/jopohl/urh

Este software también incluye herramientas avanzadas para la demodulación y el análisis de señales, lo que facilita la comprensión y el estudio de señales de radio. Su naturaleza de código abierto y su comunidad activa de usuarios y desarrolladores contribuyen a su evolución constante y su versatilidad en el ámbito de la radio definida por software, denominándose de esta manera como una herramienta poderosa para aquellos que buscan explorar y experimentar con el mundo de las señales de radio y las comunicaciones inalámbricas.

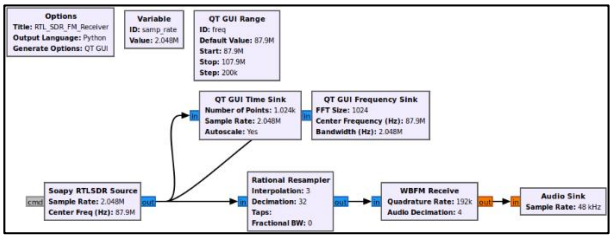
2.2.9.2. GNU RADIO

GNU Radio es un software de código abierto ampliamente utilizado en el ámbito de la radio definida por software (SDR), este programa ofrece una plataforma de desarrollo y procesamiento

de señales de radio altamente flexible y versátil (ver Figura 34), así como también permite a los usuarios crear flujos de trabajo personalizados para el procesamiento y análisis de señales de radio mediante un enfoque de "arrastre y soltar" de bloques funcionales que representan operaciones específicas [47].

Figura 34

GNU Radio



Nota. La figura representa un receptor FM para RTL-SDR, fuente https://wiki.gnuradio.org/index.php

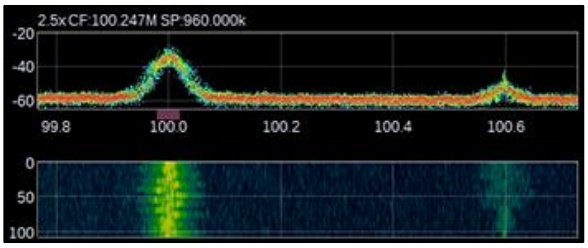
Mediante este software los usuarios pueden diseñar flujos de trabajo para recibir, decodificar, modular y analizar señales de radio en una amplia variedad de bandas de frecuencia, lo que lo hace valioso para aplicaciones que van desde la radio afición y la seguridad inalámbrica hasta la investigación y desarrollo de comunicaciones inalámbricas.

2.2.9.3. SDRANGEL

SDRangel es un software de código abierto diseñado para funcionar con dispositivos SDR (Software Defined Radio) y proporciona una amplia gama de funcionalidades para la recepción, demodulación y análisis de señales de radio (ver Figura 35), este programa se destaca por su interfaz de usuario amigable y su versatilidad en la manipulación de señales de radio [47].

Figura 35

SDRangel



Nota. La figura representa el análisis de una señal en SDRangel, fuente https://www.sdrangel.org

Lo que hace que SDRangel sea valioso es su amplia variedad de funciones, que incluyen una amplia gama de modos de demodulación, capacidades de decodificación de señales digitales, capacidades de grabación y reproducción de señales, y un conjunto de herramientas para el análisis del espectro. Los usuarios pueden aprovechar estas funciones para explorar y decodificar señales en el espectro de radio, lo que lo convierte en una herramienta poderosa en aplicaciones que van desde la radio afición y la investigación en telecomunicaciones

2.2.10. ATAQUES A LA COMUNICACIÓN POR RF

Los ataques a la comunicación por radiofrecuencia (RF) representan una preocupación importante en el ámbito de la seguridad y la privacidad en las comunicaciones inalámbricas, tales ataques pueden tomar diversas formas y tienen como objetivo interceptar, interrumpir o manipular las señales de RF utilizadas en dispositivos y sistemas de comunicación inalámbrica [5].

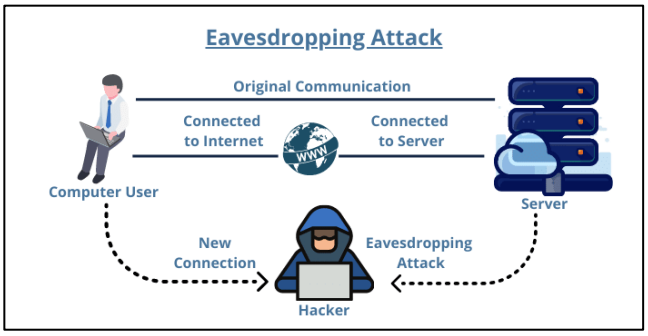
Los atacantes pueden utilizar técnicas de interceptación para escuchar y capturar comunicaciones privadas, lo que plantea serias amenazas para la confidencialidad de la información transmitida. Además, los ataques de denegación de servicio (DoS) pueden sobrecargar redes inalámbricas, causando la interrupción de servicios críticos y la degradación del rendimiento de las comunicaciones.

2.2.10.1. EAVESDROPPING

El Eavesdropping, o escucha clandestina, es una forma de ataque a la comunicación por radiofrecuencia (RF) que implica la interceptación no autorizada de señales de radio transmitidas entre dispositivos o sistemas (ver Figura 36). En este tipo de ataque, un intruso captura y monitoriza las señales RF con el objetivo de escuchar o registrar las comunicaciones de las partes legítimas [5].

Figura 36

Eavesdropping Attack



Nota. La figura representa un ataque Eavesdropping, fuente https://networksimulationtools.com/eavesdropping-attack-network-projects/

Esta forma de ataque plantea una seria amenaza a la privacidad y la confidencialidad de la información transmitida, ya que permite a un atacante obtener acceso a datos sensibles o conversaciones privadas, dicha técnica es particularmente preocupante en aplicaciones críticas, como comunicaciones militares, redes inalámbricas empresariales y sistemas de control industrial, donde la seguridad de la información es fundamental.

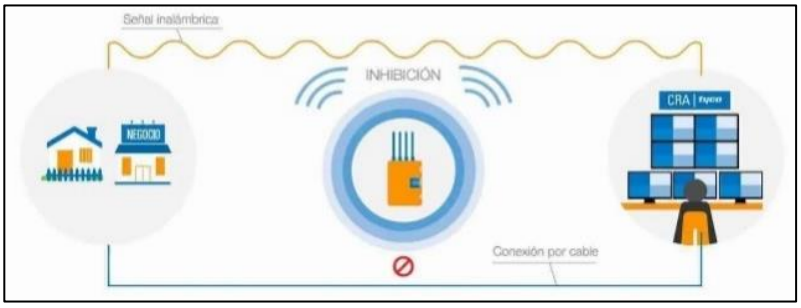
2.2.10.2. INHIBICIÓN DE SEÑAL

La inhibición de señal es un tipo de ataque a la comunicación por radiofrecuencia (RF) que implica la interferencia deliberada en las señales de RF transmitidas entre dispositivos o sistemas

(ver Figura 37). En este tipo de ataque, un intruso utiliza un dispositivo de inhibición de señal para emitir señales de interferencia en las mismas frecuencias que se utilizan para las comunicaciones legítimas, lo cual provoca la pérdida de conectividad y la interrupción de las comunicaciones inalámbricas [48].

Figura 37

Inhibición de señal



Nota. La figura representa la inhibición de una señal de RF, fuente https://www.altaico.es/anti-inhibidores-de-frecuencias/

Para mitigar la amenaza de la inhibición de señal, se utilizan medidas de seguridad y técnicas de detección. Una de las estrategias más comunes es la implementación de sistemas de respaldo y redundancia, que permiten a las comunicaciones cambiar a frecuencias alternativas o rutas en caso de interferencia. Además, se emplean sistemas de detección de interferencias para identificar y localizar fuentes de inhibición de señal.

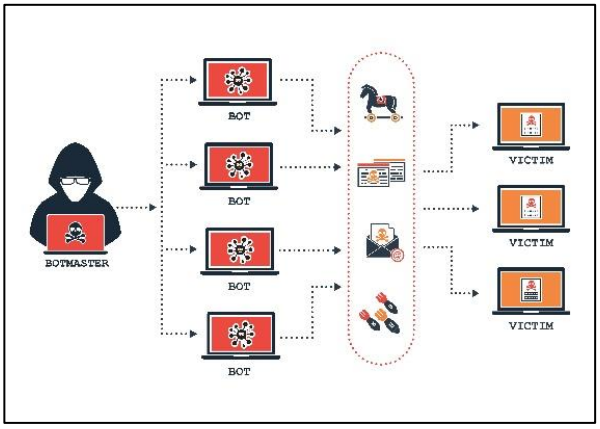
2.2.10.3. DOS

El ataque de denegación de servicio (DoS, por sus siglas en inglés) es una forma de ataque a la comunicación por radiofrecuencia (RF) que tiene como objetivo saturar una red inalámbrica o un dispositivo SDR (Software Defined Radio) con una cantidad excesiva de tráfico, lo que resulta en la interrupción de las comunicaciones legítimas (ver Figura 38). En un ataque DoS, un intruso

genera deliberadamente una gran cantidad de señales de RF para sobrecargar los canales de comunicación o los recursos de hardware, lo que provoca la pérdida de conectividad y la degradación del rendimiento de la red inalámbrica [48].

Figura 38

Ataque DoS



Nota. La figura representa un ataque DoS, fuente https://www.incibe.es/ciudadania/blog/que-son-los-ataques-dos-y-ddos

La mitigación de los ataques DoS en las comunicaciones por RF implica la implementación de medidas de seguridad y la monitorización activa de la red. Los sistemas de detección de intrusiones y la gestión de tráfico pueden ayudar a identificar y mitigar los ataques DoS en tiempo real, al tiempo que se utilizan técnicas de autenticación y cifrado de datos para proteger la integridad y la confidencialidad de las comunicaciones. La redundancia en las comunicaciones y la capacidad de cambiar a frecuencias alternativas o rutas de transmisión también son estrategias útiles para garantizar la continuidad de las comunicaciones en caso de un ataque DoS.

CAPITULO III

COMPONENTES DE LA PROPUESTA

3.1 COMPONENTES FÍSICOS DE LOS NODOS CLIENTE/SERVIDOR

3.1.1 BAQUELITA

La baquelita (ver Figura 39) es muy importante dentro del proyecto, debido a que un lado de la baquelita es un sustrato aislante y el otro lado es una placa recubierta de cobre, en la parte de cobre se imprimirá el diseño de las pistas previamente elaboradas en el software Proteus a partir de un diagrama esquemático, convirtiéndose asi en una PCB. Se van a utilizar dos PCB una para el transmisor (CLIENTE) y otra para el receptor (SERVIDOR), a su vez en las PCB se montan todos los elementos electrónicos correspondientes a la circuitería. En la Tabla 1 se puede observar algunas propiedades y características de la baquelita.

Figura 39

Baquelita

Nota. La figura representa una baquelita virgen, fuente Autor.

Tabla 1

Datos Técnicos de la Baquelita

Datos Técnicos	
Propiedades	**Características**

Resistencia dieléctrica alta.	• Aísla componentes electrónicos. • Evita cortocircuitos.
Estabilidad térmica.	• Soporta altas temperaturas. • Al soldar componentes electrónicos no se deforma.
Rigidez.	• Permite la perforación. • Sostiene el montaje de los componentes.
Aislamiento eléctrico.	• Evita interferencias. • Evita fuga de corriente entre componentes.

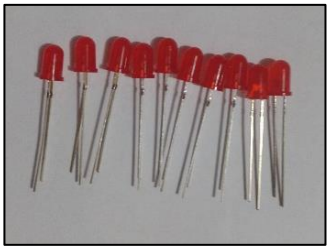
Nota. Esta tabla representa algunos datos técnicos de la baquelita, fuente Autor

3.1.2 DIODO LED

El diodo LED (ver Figura 40) sirve como un indicador visual, debido a que emite luz cuando esta polarizado directamente (el terminal ánodo en positivo y el terminal cátodo en negativo) y se le aplica una corriente eléctrica. En el proyecto se requiere de 8 diodos LED de color rojo que van montados en la PCB del nodo SERVIDOR. Los diodos LED tienen una variedad de colores y por cada color dependiendo del fabricante se tiene sus especificaciones. En la Tabla 2 puede observar las especificaciones técnicas del diodo LED color rojo.

Figura 40

Diodos LED



Nota. La figura representa diez diodos LED, fuente Autor.

Tabla 2

Especificaciones técnicas del diodo LED rojo

Datos Técnicos	
Color	Rojo
Longitud de Onda	630 nm
Corriente	20 mA
Voltaje	2 a 2.4 V
Voltaje típico	2V

Nota. Esta tabla representa los datos técnicos del diodo LED rojo, fuente Autor

3.1.3 RESISTENCIA

La resistencia (ver la Figura 41) sirven para limitar la corriente que pasa a través de un diodo LED y asi no dañarlo, existe una variedad de valores óhmicos para las resistencias lo cual implica calcular el valor ideal de la resistencia para el diodo LED, esto se lo hace utilizando la siguiente formula:

$$R = \frac{V_{alimentación} - V_{LED}}{I_{LED}}$$

Donde:

- R será la resistencia del diodo LED.
- $V_{alimentación}$ el voltaje de alimentación del circuito.
- V_{LED} el voltaje del diodo LED.
- I_{LED} la corriente del diodo LED.

El voltaje de alimentación es de 5V, el diodo LED de color rojo cuenta con una caída de tensión de 2V aproximadamente y se quiere trabaje con una corriente de 10mA, utilizando la formula se tiene:

$$R = \frac{5V - 2V}{10x10^{-3}A}$$

$$R = \frac{3V}{\frac{10}{1000}A}$$

$$R = \frac{3000\,V}{10\,A}$$

$$R = 300\,\Omega$$

Una resistencia con valor de 300 ohmios no es considerada comercial y peor en países que no se dedican a fabricarlas, entonces se toma una resistencia que si sea comercial como es el caso de una resistencia con un valor de 330 ohmios. Se necesitan 8 resistencias que van montadas en la PCB del nodo SERVIDOR para evitar que los diodos LED sean dañados. En la Tabla 3 puede observar las especificaciones técnicas de la resistencia.

Figura 41

Resistencia

Nota. La figura representa una resistencia de 330 ohms, fuente Autor.

Tabla 3

Especificaciones técnicas de las Resistencias

Datos Técnicos	
Resistencia	330 ohmios
Tolerancia	5%
Código de Color	Naranja-Naranja-Café-Dorado
Tipo	Película de carbón
Voltaje Max. Operación	350V
Polarización	Ninguna
Temperatura operación	-55C° - +155C°
Empaquetado	Recubrimiento conformado, axial
Dimensiones	Diámetro del cuerpo: 2.3mm Longitud del cuerpo: 6mm Diámetro del terminal: 28mm Longitud del terminal: 0.55mm

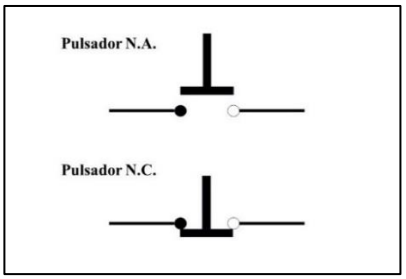
Nota. Esta tabla representa los datos técnicos de una resistencia de 330 ohmios, fuente Autor

3.1.4 PULSADOR

El pulsador sirve para activar o desactivar temporalmente el paso de la corriente a través una conexión electrónica, existen distintos tipos de pulsadores, pero los principales son N.A. (normalmente abierto) y N.C. (normalmente cerrado) (ver Figura 42). En la Tabla 4 puede observar sus características.

Figura 42

Pulsadores



Nota. La figura representa los tipos de pulsadores, fuente Autor.

Tabla 4

Características de los pulsadores N.A. y N.C.

Características	**Pulsador N.A.**	**Pulsador N.C.**
Estado inicial	Circuito abierto	Circuito cerrado
Estado al ser pulsado	Circuito cerrado	Circuito abierto
Función principal	Activado al ser presionado	Desactivado al ser presionado
Uso común	Interruptor de encendido	Interruptor de apagado
Aplicaciones típicas	• Encendido o apagado de un diodo LED. • Inicio o apagado de un proceso	• Paro de emergencia • Detención de un proceso

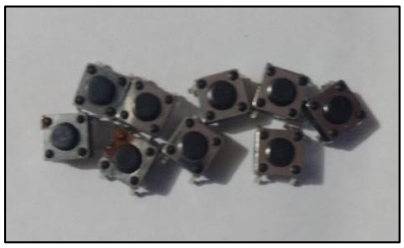
Nota. En la tabla se representan las diferencias entre los pulsadores N.A. y N.C. en base a sus características, fuente Autor.

El tipo de pulsador ideal el proyecto por sus características (ver Tabla 4) es el pulsador N.A. Existen una gran variedad de modelos de este tipo de pulsador, el modelo a utilizar en el

proyecto es el B3f-4055 (ver Figura 43). En la Tabla 5 puede observar las especificaciones técnicas del pulsador B3f-4055.

Figura 43

Pulsadores B3f-4055



Nota. La figura representa 9 pulsadores Bef-4055 N.A., fuente Autor.

Tabla 5

Especificaciones técnicas del pulsador B3f-4055

Datos Técnicos	
Configuración de contactos	SPST-NO (Normalmente Abierto)
Capacidad de carga de contactos DC a carga resistiva	50mA / 24V CC
Fuerza de conmutación	2.55N
Dimensiones del cuerpo	1.2 x 1.2 cm
Modo de actuación	OFF – (ON)
Temperatura de trabajo	-25°C – 70°C
Resistencia máx. de contactor	100mΩ
Resistencia de aislamiento mín.	0.1GΩ
Durabilidad mecánica	1000000 ciclos

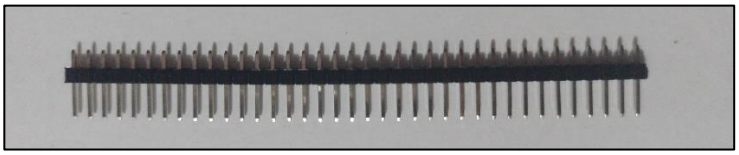
Nota. Esta tabla representa los datos técnicos del pulsador B3f-4055, fuente Autor.

3.1.5 ESPADINES

Los espadines son tiras que permite conectar elementos electrónicos entre sí, sujetar microcontroladores y pueden ser soldados sobre PCBs, existen de dos tipos hembra y macho. Los espadines para utilizar son los de tipo macho (ver Figura 44) ya que van solados en las PCBs y sirven para sujetar el microcontrolador de Arduino modelo pro mini. En la Tabla 6 puede observar las especificaciones técnicas de los espadines.

Figura 44

Espadines



Nota. La figura representa una tira de 40 pines de espadines, fuente Autor.

Tabla 6

Especificaciones técnicas de los Espadines

Datos Técnicos	
Tipo	Macho
Número de pines	40 pines
Espacio entre pines	2.54 mm
Altura del plástico	2.5 mm
Longitud de la punta	3 mm
Corriente máx.	3ª

Temperatura de funcionamiento	-55°C - +105°C

Nota. Esta tabla representa los datos técnicos de los espadines, fuente Autor.

3.1.6 TARJETA MICROCONTROLADOR DE ARDUINO

La tarjeta microcontrolador de Arduino tiene una amplia funcionalidad, una de sus funciones es la comunicación inalámbrica, ya que al ser complementada con módulos de RF permite transmitir y recibir datos de forma inalámbrica. Existe una gran variedad de modelos y sus diversas versiones, los modelos más populares en el mercado son Arduino Uno, Arduino Nano y Arduino Pro mini. En la Tabla 7 puede observar una comparación entre los modelos Uno, Nano y Pro mini.

Tabla 7

Comparación entre el Arduino Uno, Nano y Pro mini

Diferencias			
	Arduino Uno	**Arduino Nano**	**Arduino Pro Mini**
Aspecto			
Tamaño	68.6 x 53.4 mm	18 x 45 mm	18 x 33 mm
Microcontrolador	ATmega328P	ATmega328	ATmega328
Pines	14	22	14
Voltaje de operación	5V	5V	3.3V o 5V
Memoria Flash	32 KB	32 KB	32 KB
Memoria SRAM	2 KB	2 KB	2 KB
Velocidad de reloj	16 MHz	16 MHz	8 MHz – 16 MHz

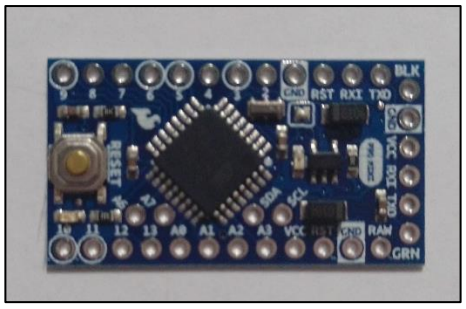
Puerto USB	Sí	Sí	No
Precio	27.60 $	24.90 $	10.95 $
Integración	Buena	Buena	Útil para espacios reducidos

Nota. Esta tabla representa las diferencias entre los modelos más populares de Arduino, fuente Autor.

La tarjeta microcontroladora para utilizar es la del Arduino Pro mini (ver Figura 45), por su tamaño es ideal para reducir espacio en la construcción de los nodos, cuenta con el microcontrolador ATmega328 que tiene un bajo consumo de energía, es fácil de conseguir en el mercado por su precio que es relativamente económico en comparación de otras opciones, cuenta con 14 pines digitales I/O y trabaja con un voltaje de operación de 5V a 16 MHz. Una desventaja es que no cuenta con un puerto USB por lo que se debe utilizar un convertidor USB a TTL. En la Tabla 8 puede observar las especificaciones técnicas del Arduino Pro mini.

Figura 45

Arduino Pro mini



Nota. La figura representa la tarjeta microcontroladora ATmega328 Pro mini de Arduino, fuente Autor.

Tabla 8

Especificaciones técnicas del Arduino Pro mini

Datos Técnicos	
Microcontrolador	ATmega328
Velocidad de reloj	16 MHz con resonador externo (0.5% de tolerancia)
Espesor PCB	0,8 mm
Conexión USB	No
Regulador	5V
Salida máx. de corriente	150mA
Protección contra sobre corriente	Sí
Peso	< 2 gramos
VCC	5V – 12V
LED de estado y alimentación	Sí
Pines analógicos	8
Pines digitales I/O	14
Tamaño	18 x 33 mm

Nota. Esta tabla representa los datos técnicos del Arduino Pro mini, fuente Autor.

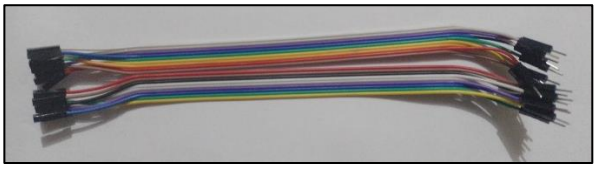
3.1.7 CABLE DUPONT

El cable Dupont sirve para realizar conexiones entre dispositivos y existen tres tipos macho – macho, hembra – hembra y macho – hembra (ver Figura 46), dentro del proyecto se utiliza el cable Dupont tipo hembra – hembra, se encarga de realizar la conexión entre el Arduino Pro mini

y el convertidor USB a TTL para transferir el código de programación. En la Tabla 9 puede observar las especificaciones técnicas del cable Dupont.

Figura 46

Cable Dupont



Nota. La figura representa el cable Dupont de tipo hembra – macho, fuente Autor.

Tabla 9

Especificaciones técnicas del cable Dupont

Datos Técnicos	
Terminal	Hembra – Hembra
Color	Paquete Arcoíris
Longitud	20 cm
Cantidad de cables	40
Ancho de los cables juntos	5.5 cm
Voltaje máx.	300V

Nota. Esta tabla representa los datos técnicos del Cable Dupont, fuente Autor.

3.1.8 CONVERTIDOR USB A TTL

El convertidor USB a TTL establece la comunicación serial entre una computadora a través de su puerto USB y un dispositivo electrónico que utilice niveles lógicos TTL para transferir datos. Existe una variedad de chips para este tipo de convertidores entre los más comunes se tiene el

convertidor CH340G, CP2102 y FT232RL. En la Tabla 10 puede observar una comparación entre los modelos CH340G, CP2102 y FT232R.

Tabla 10

Comparación entre los chips CH340G, CP2102 y FT232RL

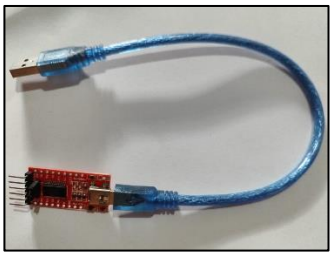
	Diferencias		
	CH340G	**CP2102**	**FT232RL**
Característica			
Fabricante	WCH (Nanjing Qinheng)	Silicon Labs	FTDI
Velocidad de Datos	Hasta 2 Mbps	Hasta 2 Mbps	Hasta 3 Mbps
Compatibilidad	Limitada	Amplia	Amplia
Soporte	Normal	Normal	Robusto
Consumo energético	Bajo	Bajo	Bajo
Precio	3.50 $	6.00 $	4.50 $

Nota. Esta tabla representa las diferencias entre los modelos más comunes de convertidores, fuente Autor.

El convertidor USB a TTL para utilizar es el FT232RL (ver Figura 47) ya que tiene una velocidad de datos más alta, su compatibilidad es amplia, el soporte es robusto y tiene un precio moderado, lo que permite que cargue la programación al Arduino Pro mini de manera más eficiente. En la Tabla 11 puede observar las especificaciones técnicas del convertidor USB a TTL FT232RL.

Figura 47

Convertidor USB a TTL



Nota. La figura representa el convertidor USB a TTL FT232RL, fuente Autor.

Tabla 11

Especificaciones técnicas del Convertidor con chip FT232RL

Datos Técnicos	
Modelo	FTDI232RL
Voltaje de operación	3.3V – 5V
Fusible de protección (contra sobrecarga)	500Ma
Velocidad versión USB	1.1/3.0 Mbps
Indicador de comunicación	RXD/TXD
Distribución de pines	Pin 1: DTR Pin 2: RXD Pin 3: TXD Pin 4: VCC Pin 5: CTS Pin 6: GND

Ancho de banda	48 MHz
Temperatura de operación	-40°C – 85°C

Nota. Esta tabla representa los datos técnicos del Convertidor con chip FT232RL, fuente Autor.

3.1.9 MÓDULOS COMUNICACIÓN INALÁMBRICOS POR RF

Los módulos de comunicación inalámbrica por RF sirven para transmitir datos entre dos tarjetas de Arduino sin necesidad de cables mediante una comunicación punto a punto. Existen varios módulos de RF compatibles con Arduino entre los más utilizados están APC220, FS1000A – XY-MK-5V y NRF24L01. En la Tabla 12 puede observar una comparación entre los módulos APC220, FS1000A – XY-MK-5V y NRF24L01.

Tabla 12

Comparación entre los chips APC220, FS1000A - XY-MK-5V y NRF24L01

	Diferencias		
	APC220	**FS1000A - XY-MK-5V**	**NRF24L01**
Característica			
Frecuencia	418 – 455 MHz	433 MHz	2.4 GHz
Alcance típico	1000 m	200 m	100 m
Velocidad de datos	19.2 Kbps	4 – 10 Kbps	2 Mbps
Protocolo	ISO14443	Sin protocolo estándar	SPI
Consumo de energía	Moderado	Bajo	Variable
Costo	30 $	5$	15$

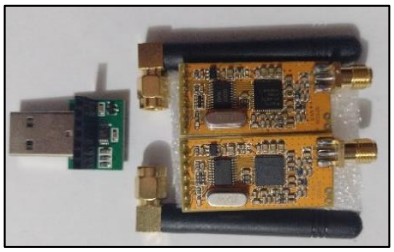
Uso común	Comunicaciones de largo alcance	Comunicaciones de corto alcance	Redes de sensores inalámbricos

Nota. Esta tabla representa las diferencias entre los módulos más comunes de RF, fuente Autor.

Los módulos de RF para utilizar son los APC220 (ver Figura 48), debido a que la frecuencia en la que trabaja cada módulo es configurable en un rango de 418 – 455 MHz dependiendo lo que se necesite, en el caso de este proyecto los módulos están configurados a una frecuencia de 434MHz. Tienen una capacidad de alcance hasta 1 km por lo que su velocidad de datos no es tan rápida, pero cumple con lo propuesto, tiene una configuración de 7 pines (ver Tabla 13) y utiliza un protocolo de comunicación propio el ISO14443, tiene un consumo de energía moderado y se los utilizan para comunicaciones de largo alcance. Su precio es un poco elevado en comparación a los otros, pero por sus características los hacen ideales para este proyecto. En la Tabla 14 puede observar las especificaciones técnicas de los módulos APC220.

Figura 48

Módulos APC220



Nota. La figura representa los módulos APC220 de RF, fuente Autor.

Tabla 13

Configuración de pines del módulo APC220

Configuración de pines del módulo APC220

Pin No.	Nombre del Pin	Descripción
1	**GND**	Conexión a tierra de la fuente de alimentación
2	**VCC**	Fuente de alimentación DC 3.5V – 5.5V
3	**EN**	Alimentación habilitada, ≥1.6V o vacía, ≤ 0.5V en suspensión
4	**RXD**	Entrada UART, TTL
5	**TXD**	Salida UART, TTL
6	**MUX**	El pin se expande para otras funciones
7	**SET**	Configuración de parámetros, configuración en línea compatible

Nota. Esta tabla representa la descripción de los pines de los módulos APC220, fuente Autor.

Tabla 14

Especificaciones técnicas de los módulos APC220

Datos Técnicos	
Frecuencia de trabajo	418 MHz a 455MHz (configurable)
Modulación	GFSK
Intervalo de frecuencia	200 KHz
Potencia transmitida	20mW (10 niveles)
Sensibilidad recibida	-113dBm@9600 bps
Velocidad en el aire	2400 – 19200 bps
Velocidad UART	1200 – 57600 bps
Paridad de la serie COM	8E1/8N1/8O1

Buffer COM	256 bytes
Humedad	10% ~ 90%
Temperatura	-30°C – 85°C
Tensión de alimentación	3.5V – 5.5V (ondulación ±50mV)
Corriente transmitida	≤ 42mA@20mW
Corriente recibida	≤ 28mA
Corriente en apagado	≤ 5μA
Distancia	1000 m (espacio abierto)
Dimensiones	37.5 mm x 18.3 mm x7.0 mm

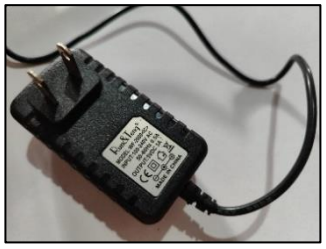
Nota. Esta tabla representa los datos técnicos de los módulos APC220, fuente Autor.

3.1.10 FUENTE DE ALIMENTACIÓN

La fuente de alimentación o cargador proporciona la energía necesaria para que los dispositivos electrónicos funcionen de manera correcta. La fuente de alimentación para este proyecto es de 5V a 3A (ver Figura 49) ya que tanto el Arduino Pro mini como el módulo APC220 tienen como voltaje de operación 5V, por otro lado, los 3A aseguran que los dispositivos electrónicos tengan un buen consumo de energía. En la Tabla 15 se puede observar las especificaciones técnicas de la fuente de alimentación.

Figura 49

Fuente de alimentación



Nota. La figura representa la fuente de alimentación Run&Teng de 5V a 3A, fuente Autor.

Tabla 15

Especificaciones técnicas de la fuente de alimentación

Datos técnicos	
Marca	Run&Teng
Modelo	WF-2000<IC>
Voltaje de entrada	100V – 240V
Frecuencia de trabajo	50 Hz – 60 Hz 0.5A
Voltaje de salida	5V
Corriente de salida	3A
Longitud del cable	80 cm (aprox.)

Nota. Esta tabla representa los datos técnicos del cargador Run&Teng, fuente Autor.

3.2 DISPOSITIVO PARA GENERAR LOS ATAQUES

3.2.1 EQUIPO SDR

El equipo SDR sirve para recibir, procesar y transmitir señales de RF mediante software. La señal recibida por el equipo SDR a través de un software puede ser grabada, guarda y procesada, permite la aplicación de técnicas de modulación o demodulación para volver a ser transmitida. Existen un sin número de equipos SDR, entre los más utilizados están el HACKRF ONE, el RTL2832U y el AIRSPY SDR. En la Tabla 16 puede observar una comparación entre los equipos HACKRF ONE, el RTL2832U y el AIRSPY SDR.

Tabla 16

Comparación entre los equipos HACKRF ONE, el RTL2832U y el AIRSPY SDR

Diferencias			
Características	**HACKRF ONE** 	**RTL2832U** 	**AIRSPY HF+ DISCOVERY SDR** 
Rango de frecuencia	1MHz – 6GHz	24 MHz – 1.7 GHz	0.5 kHz – 31 MHz 60 MHz – 260 MHz
Ancho de banda	Max. 20 MHz	Max. 3.2 MHz	660 kHz HF 1.2 MHz VHF
Muestra de cuadratura	8 – bits I 8 – bits Q	8 – bits I 8 – bits Q	12 – bits
Modos de recepción	AM, FM, SSB, CW, Digital, ADS-B, entre otros.	AM, FM, SSB, CW, Digital, ADS-B, entre otros.	AM, FM, SSB, CW, Digital, ADS-B, entre otros.
Software con licencias de código abierto	Si	Si	Limitadas
Hardware con licencias de código abierto	Si	No	No

Interfaz	USB 2.0 Hi – Speed	USB 2.0	USB 2.0
Potencia de transmisión	Max. 5mW, con amplificador externo 50mW	No puede transmitir solo receptar.	No puede transmitir solo receptar.
Software soportado	URH, GNU Radio, SDRangel, entre otros.	URH, GNU Radio, SDRangel, entre otros.	URH, GNU Radio, SDRangel, entre otros.
Precio	340 $	35$	184$

Nota. Esta tabla representa las diferencias entre los equipos SDR más comunes de RF, fuente Autor.

El equipo para utilizar en el proyecto es el HackRF One (ver Figura 50), debido a que se trata de un periférico de SDR que tiene la capacidad de operar con señales de RF permitiendo recibirlas y transmitirlas, en el rango de frecuencia desde 1 MHz hasta los 6 GHz con un ancho de bando máximo de 20 MHz. Puede transmitir datos por RF con una potencia máxima de 5 mW y si se implementa un amplificar externo, la potencia máxima alcanza los 50 mW.

Tiene licencias de código abierto tanto para hardware como software, es compatible con una variedad de modos de recepción con una muestra de fase(I) y cuadratura(Q) de 8 – bits. Cuenta con una interfaz USB de alta rapidez de transmisión de datos y es compatible con una variedad de aplicación para software definido por radio. Su precio es un poco elevado en comparación a los otros equipos, pero por sus características lo hacen ideal para este proyecto. En la Tabla 17 puede observar las especificaciones técnicas del HackRF One.

Figura 50

HackRF One

Nota. La figura representa el equipo HackRF One, fuente Autor.

Tabla 17

Especificaciones técnicas del equipo SDR HackRF One

Datos técnicos	
Rango de frecuencia	1 MHz – 6 GHz
Muestreo	Tasa de muestreo: 20 Msps Resolución de muestra: 8 bits
Modo de operación	- Transmisión - Recepción
Conexión	Interfaz USB 2.0 de alta velocidad
Ancho de banda	Max. 20 MHz
Potencia de salida	Max. 15 dBm
Entradas y salidas	Conector de antena: SMA Puerto de reloj externo: SMA GPIO: 8 pines

Voltaje de alimentación	5V – USB
Consumo de energía	500 mA
Dimensiones	60mm x 95mm x 12mm
Peso	200 g
Compatibilidad de software	URH, GNURadio, entre otros.
Temperatura de operación	0°C - 85°C
Plataforma	Hardware y software de código abierto

Nota. Esta tabla representa los datos técnicos del equipo SDR HackRF One, fuente Autor.

La placa electrónica del HackRF One (ver Figura 51), cuenta los siguientes componentes: El MAX2839 que es un transceptor RF MIMO de banda ancha inalámbrico a (2.3 – 2.7) GHz (ver Figura 52), para mayor informacion revise el Anexo 1. El MAX5864 que es un frontal analógico ADC/DAC de ultra bajo consumo con alto rendimiento dinámico a 22 Msps (ver Figura 53), para mayor informacion revise el Anexo 2. El Si5351 que es un generador de clock programable (ver Figura 54), para mayor informacion revise el Anexo 3. El LPC4320 que es un microcontrolador de 32 bits de alto rendimiento baso en núcleos Arm® Cortex®-M4/M0 (ver Figura 55), para mayor informacion revise el Anexo 4. El RFFC5072 que es un sintonizador de banda ancha de 85 – 4200 MHz / VCO con mezclador de RF integrado de 6 GHz (ver Figura 56), para mayor informacion revise el Anexo 5. El W25Q80BV que es una memoria flash serial de 8M-BIT con SPI doble y cuádruple (ver Figura 57), para mayor informacion revise el Anexo 6. En la Figura 58 se presenta el diagrama de bloques del HackRF One con todos los componentes mencionados.

Figura 51

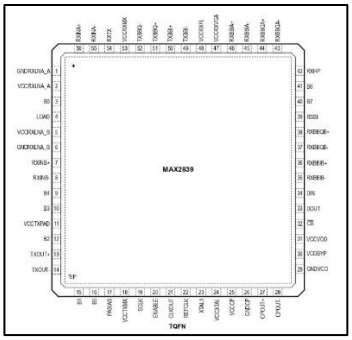
Placa del HackRF One

Nota. La figura representa la placa electrónica del HackRF One, fuente

https://hackrf.readthedocs.io/en/latest/hackrf_one.html

Figura 52

MAX2839

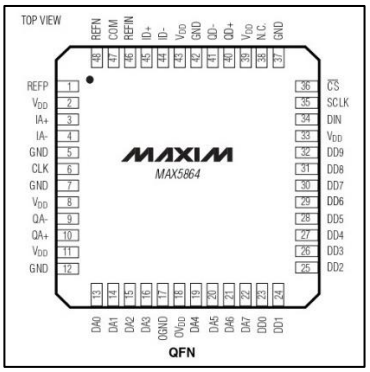


Nota. La figura representa la configuración de pines del MAX2839, fuente

https://www.analog.com/en/products/max2839.html

Figura 53

MAX5864

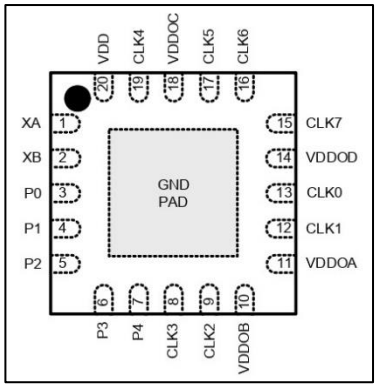


Nota. La figura representa la configuración de pines del MAX5864, fuente

https://www.analog.com/en/products/max5864.html

Figura 54

Si5351

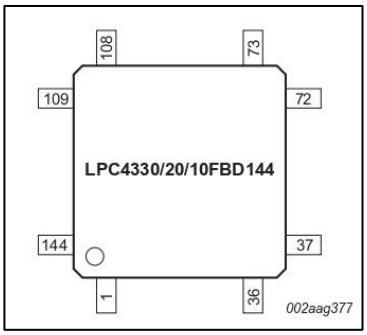


Nota. La figura representa la configuración de pines del Si5351¸ fuente

https://www.mouser.com/new/skyworks-solutions/skyworks-si5351-clock-generators/

Figura 55

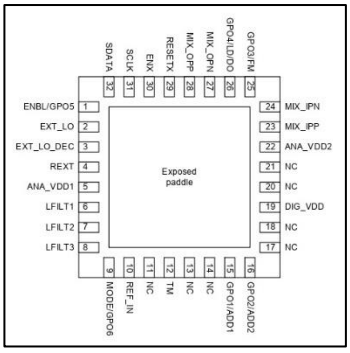
LPC4320



Nota. La figura representa la configuración de pines del LPC4320, fuente https://www.nxp.com/part/LPC4320FBD144

Figura 56

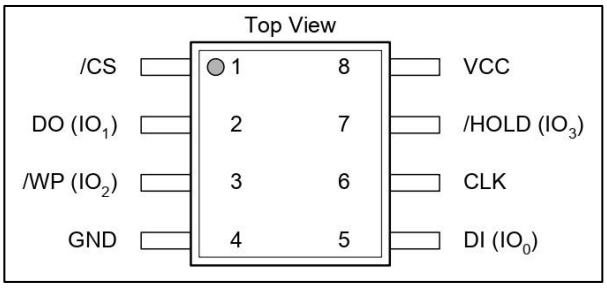
RFFC5072



Nota. La figura representa la configuración de pines del RFFC5072, fuente https://www.qorvo.com/products/p/RFFC5072

Figura 57

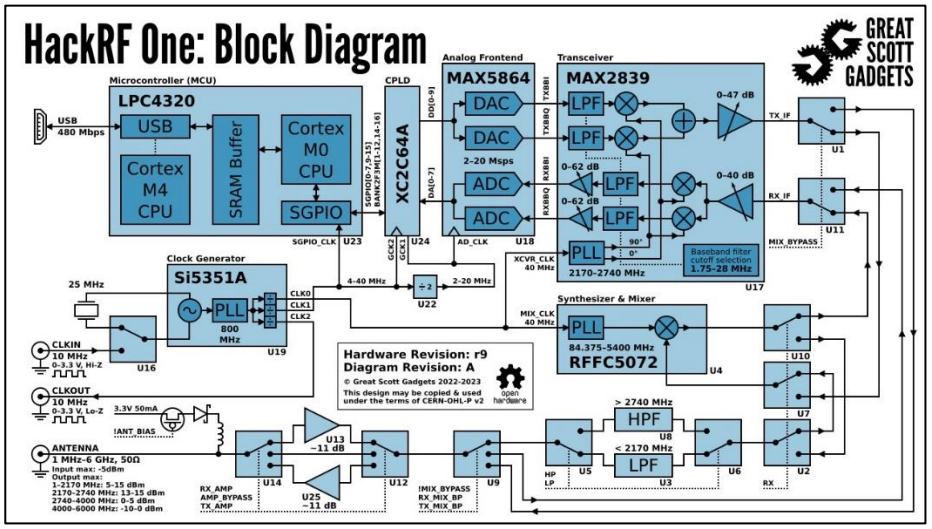
W25Q80BV



Nota. La figura representa la configuración de pines del W25Q80BV, fuente https://www.winbond.com/hq/support/documentation/levelOne.jsp?__locale=en&DocNo=DA00-W25Q80BV

Figura 58

HackRF One: Diagrama de bloques



Nota. La figura representa el diagrama en bloques del funcionamiento del HackRF One, fuente https://hackrf.readthedocs.io/en/latest/hardware_components.html

El dispositivo HackRF One consta de 4 indicadores LED, los cuales se describe el funcionamiento en la Tabla 18. De igual manera consta de dos botones, los cuales se describe el

funcionamiento en la Tabla 19. Tambien posee dos interfaces externas de reloj, las cuales se describe el funcionamiento en la Tabla 20.

Tabla 18

Indicadores LED del HackRF One

Indicadores Led	
Indicador LED	**Funcionamiento**
3V3	Fuente de alimentación principal activada.
1V8	Fuentes de alimentación adicionales activadas.
RF	Firmware en ejecución.
USB	Dispositivo conectado a PC.
RX – TX	Recepción y transmisión en ejecución.

Nota. Esta tabla representa el funcionamiento de los indicadores LED en el HackRF One, fuente Autor.

Tabla 19

Botones del HackRF One

Botones	
Botón	**Funcionamiento**
RESET	Resetea el microcontrolador.
DFU	Desbloque el modo de operación DFU

Nota. Esta tabla representa el funcionamiento de los botones en el HackRF One, fuente Autor

Tabla 20

Interfaces externas de reloj del HackRF One

Interfaces externas de reloj	
Interfaz	**Funcionamiento**
CLKOUT	Entrega una señal de onda cuadrada de 3.3V a frecuencia de 10 MHz para una carga de impedancia alta.
CLKIN	Es una entrada con una alta impedancia que recibe una señal onda cuadrada precisamente a 3.3V, no mayor ni menor a una frecuencia de 10MHz.

Nota. Esta tabla representa el funcionamiento de las interfaces externas de reloj en el HackRF One, fuente Autor.

Analizando la característica del dispositivo HackRF One, en base a sus componentes en la Tabla 21 se mencionan algunos de sus usos. Dentro del proyecto, la aplicación del dispositivo HackRF One es la captura de datos, el procesamiento de los datos capturados y la transmisión de los datos procesados, a una señal de RF de 434 MHz.

Tabla 21

Usos del dispositivo HackRF One

Usos		
Componente	**Funcionamiento**	**Aplicación**
MAX2839	Capturar y transmitir señales de radio en un rango de frecuencias entre 1 MHz – 6 GHz.	• Recepción y transmisión de radioaficionado. • Transmisor AM – FM.

MAX5864	Digitalizar y convertir señales analógicas de alta frecuencia.	• Monitoreo del espectro radioeléctrico.
SI5351	Proporcionar y recibir señales de reloj.	• Generador de señal de onda cuadrada.
LPC4320	Gestionar la configuración, controlar y procesar datos en tiempo real.	• Procesamiento digital de señales por RF. • Control de hardware en aplicaciones SDR.
RFFC5072	Sintonizar una extensa gama de frecuencias.	• Sintonizador de radio AM – FM
W25Q80BV	Almacenar datos capturados y configuraciones de usuario.	• Duplicados de llaves por RF.

Nota. Esta tabla menciona algunas aplicaciones para el dispositivo HackRF One, fuente Autor.

3.3 COMPONENTES LÓGICOS

3.3.1 SOFTWARE DE PROGRAMACIÓN PARA EL MICROCONTROLADOR DE LAS TARJETAS DE ARDUINO PRO MINI

El software de programación sirve para escribir, editar y gestionar códigos de programación destinados a microcontroladores, estos códigos pueden ser representados mediante escritura o bloques. La finalidad de esta herramienta es la creación de códigos de programación para el desarrollo de aplicaciones personalizadas que permitan controlar hardware específico. Existe una variedad de softwares para el microcontrolador de las tarjetas de Arduino Pro mini,

entre los más utilizados están Arduino IDE, S4A y mBlock. En la Tabla 22 puede observar una comparación entre los softwares Arduino IDE, S4A y mBlock.

Tabla 22

Comparación entre los softwares Arduino IDE, S4A y mBlock

Diferencias			
Características	**Arduino IDE**	**S4A**	**mBlock**
Lenguaje de programación	C/C++	Scratch	Scratch
Requisitos para programación	Conocimientos básicos en C/C++	Sin experiencia	Sin experiencia
Flexibilidad y control	Control total sobre el hardware de Arduino	Control mínimo sobre el hardware de Arduino	Control mínimo sobre el hardware de Arduino
Compatibilidad	Específico para Arduino	Específico para Arduino	Arduino entre otros
Precio	Gratis	Gratis	Gratis

Nota. Esta tabla representa las diferencias entre los softwares más comunes para los microcontroladores de las tarjetas de Arduino Pro mini, fuente Autor.

El software de programación para el microcontrolador de las tarjetas de Arduino Pro mini que se va a utilizar es el Arduino IDE, debido a que, es un software gratis y oficial de Arduino, utiliza un lenguaje de programación C/C++ permitiendo el control total sobre el hardware que se quiera implementar en las tarjetas de Arduino Pro mini. En la Tabla 23 se puede observar las especificaciones del software Arduino IDE y en la Tabla 24 los requisitos mínimos para la instalación del software Arduino IDE.

Tabla 23

Especificaciones del software Arduino IDE

Especificaciones	
Lenguaje de programación	C, C++
Sistemas operativos soportados	Windows macOS Linux
GUI	Editor de código Consola serial
Compilador	GNU AVR
Carga de programas	Mediante cable USB
Librerías	Incluye librerías predeterminadas y permite descargar adicionales
Compatibilidad	Compatible con todas las tarjetas de Arduino
Licencia	Código abierto bajo licencia GNU.

Nota. Esta tabla representa las especificaciones del software de Arduino IDE, fuente Autor.

Tabla 24

Requisitos mínimos del software Arduino IDE

Requisitos mínimos			
Características	**Windows**	**macOS**	**Linux**
Procesador	Procesador a 1 GHz	Procesador Intel	Procesador a 1 GHz
RAM	2 GB	2GB	2 GB
Espacio en disco	250 MB	250 MB	250 MB

			Ubuntu 14.04
Versión mínima	Windows 7	macOS 10.10	Debian 8.0
			Fedora 22

Nota. Esta tabla representa los requisitos mínimos del software Arduino IDE, fuente Autor.

3.3.2 SOFTWARE DE DISEÑO ESQUEMÁTICO/PCB PARA LOS NODOS CLIENTE/SERVIDOR

EL software de diseño esquemático/PCB sirve para diseñar y simular diagramas de circuitos electrónicos (esquemáticos), permite crear diseños para PCB a partir de un diagrama esquemático. Este software facilita el desarrollo de prototipos electrónicos en proyectos, en donde se necesite un dispositivo electrónico que no se encuentre en el mercado. Existe una variedad de softwares de diseño esquemático/PCB, entre los más utilizados están Proteus, Multisim y EasyEDA. En la Tabla 25 puede observar una comparación entre los softwares Proteus, Multisim y EasyEDA.

Tabla 25

Comparación entre los softwares Proteus, Multisim y EasyEDA

Diferencias			
Características	**Proteus**	**Multisim**	**EasyEDA**
Diseño esquemático	Editor completo con muchos símbolos de componentes.	Editor completo con muchos símbolos de componentes.	Editor limitado con algunos símbolos de componentes.

Simulación de circuitos	SPICE avanzada para circuitos analógicos y digitales. Microcontroladores y microprocesadores.	SPICE avanzada para circuitos analógicos y digitales. FPGA y microcontroladores.	SPICE básica para circuitos analógicos y digitales.
Diseño de PCB	Diseños multicapa con reglas de diseño avanzadas.	No soporta.	Diseños multicapa básico.
Biblioteca de componentes	Amplia con opción de importa o crear componentes.	Amplia con opción de importa o crear componentes.	Solo los componentes por defecto.
Simulación de microcontroladores	Soporta varios microcontroladores incluido Arduino.	Soporta algunos microcontroladores.	Solo soporta los principales microcontroladores
Generación de gerber	Completa con opciones avanzadas.	Limitada a través de Ultiboard.	Completa con opciones avanzadas.
Interfaz de usuario	Intuitiva.	Intuitiva.	Intuitiva.
Precio	Licencia comercial alta.	Licencia comercial alta.	Gratuito.

Nota. Esta tabla representa las diferencias entre los softwares más comunes para el diseño esquemático/PCB, fuente Autor.

El software de diseño esquemático/PCB para la circuitería de los nodos CLIENTE/SERVIDOR que se va utilizar es Proteus , debido a que, es un software intuitivo con un editor de diseño completo, permite la simulación SPICE de diferentes componentes en

multicapa con reglas de diseño avanzadas, se puede importar o crear componentes que no estén en la librería que viene por defecto, soporta varios microcontroladores incluyendo la tarjeta microcontroladora Pro mini de Arduino y genera el archivo gerber para la PCB. Este software es de pago con una licencia comercial alta, pero en base a sus características lo vuelve ideal para este proyecto. En la Tabla 26 se puede observar las especificaciones del software Proteus y en la Tabla 27 los requisitos mínimos para la instalación del software Proteus.

Tabla 26

Especificaciones del software Proteus

	Especificaciones
Diseño esquemático	Editor completo con biblioteca de componentes personalizables.
Simulacion de circuitos	SPICE avanzada.
Diseño de PCB	Max. 16 capas con ruteo automático/manual.
Biblioteca de componentes	Amplia con opción de importación y creación de componentes.
Generación de gerber	Completa con opciones avanzadas.
Interfaz de usuario	Intuitiva personalizable con herramientas de visualización en 3D.
Soporte técnico	Documentación y tutoriales.
Licencia	Comercial.

Nota. Esta tabla representa las especificaciones del software de Proteus, fuente Autor.

Tabla 27

Requisitos mínimos del software Proteus

Componente	**Requisitos mínimos**
Sistema operativo	Windows 7, 8, 10 (32-bit y 64-bit)

Procesador	Intel Pentium 4
RAM	4 GB (recomendable)
Espacio en disco	1 GB

Nota. Esta tabla representa los requisitos mínimos del software Proteus, fuente Autor.

3.3.3 SOFTWARE SDR PARA GENERACIÓN DE ATAQUES A LOS NODOS CLIENTE/SERVIDOR

El software SDR sirve para realizar diversos tipos de ataques, como eavesdropping, man in the middle y ataques replay, con el objetivo de identificar las vulnerabilidades en un sistema de comunicación por radio. Un escenario para analizar estas vulnerabilidades puede ser en la capa de enlace de datos del modelo OSI de algún dispositivo de RF. Existen una variedad de software SDR, entre los más utilizados están URH, GNU Radio y SDRangel. En la Tabla 28 puede observar una comparación entre los equipos URH, GNU Radio y SDRangel.

Tabla 28

Comparación entre los softwares URH, GNU Radio y SDRangel

Diferencias			
Características	**URH**	**GNU Radio**	**SDRangel**
Propósito	Análisis y decodificación de señales RF.	Plataforma de desarrollo SDR flexible.	Plataforma SDR multifuncional.
Simulación y análisis	Captura, análisis y procesamiento de señales.	Diseño y simulacion de sistemas completos de comunicación.	Captura y análisis de señales en tiempo real.

Soporte de protocolos	Amplio.	Muy amplio.	Amplio.
Capacidades de ataque	Eavesdropping, man in the middle, ataques replay, etc.	Interferencia, sniffing, inyección de paquetes, ataques replay, etc.	Interferencia, sniffing, inyección de paquetes, ataques replay, etc.
Plataforma	Windows, macOS y Linux.	Windows, macOS y Linux.	Windows, macOS y Linux.
Hardware compatible	Múltiples equipos SDR incluyendo HackRF One.	Múltiples equipos SDR incluyendo HackRF One.	Múltiples equipos SDR incluyendo HackRF One.
Licencia	Código abierto.	Código abierto.	Código abierto.
Precio	Gratis.	Gratis.	Gratis.

Nota. Esta tabla representa las diferencias entre los softwares SDR más comunes para la generación de ataques, fuente Autor.

El software SDR para la generación de ataques que se va a utilizar es URH, debido a que, es un software de código abierto gratis, trabaja con diversas plataformas, se enfoca en la decodificación de señales RF, permite la captura, el análisis y el procesamiento de señales. Este software es compatible con múltiples equipos SDR incluyendo al HackRF One, permitiendo realizar ataques como eavesdropping, man in the middle, ataques replay. En la Tabla 29 se puede observar las especificaciones del software URH y en la Tabla 30 los requisitos mínimos para la instalación del software URH.

Tabla 29

Especificaciones del software URH

	Especificaciones
Captura de señales RF	Permite la captura de señales RF a través de equipos SDR compatibles.
Grabación de señales RF	Graba y almacena señales RF previamente capturadas.
Transmisión de señales RF	Posibilita la transmisión de señales RF a través de equipos SDR compatibles.
Modulación	Permite la modulación de señales como AM, FM, PSK, QPSK, entre otros.
Demodulación	Soporta la demodulación de señales de varios tipos de modulación.
Análisis de señales RF	Permite realizar un análisis detallado de las señales capturadas.
Interfaz Grafica	Intuitiva.
Plataforma	Windows, macOS y Linux.
Soporte técnico	Documentación y comunidad en GitHub.
Licencia	Gratuita de código abierto.

Nota. Esta tabla representa las especificaciones del software de URH, fuente Autor.

Tabla 30

Requisitos mínimos del software URH

Componente	Requisitos mínimos
Sistema operativo	Windows 7, 8, 10 (32-bit y 64-bit)
Procesador	Intel Core I3

RAM	4 GB (recomendable)
Espacio en disco	1 GB
Otros	Python 3.6 o superior instalado

Nota. Esta tabla representa los requisitos mínimos del software URH, fuente Autor.

3.3.4 SOFTWARE DE MODELADO 3D PARA EL ENCAPSULADO DE LA CIRCUITERÍA DE LOS NODOS CLIENTE/SERVIDOR

El software de modelado 3D sirve para crear, modificar y visualizar modelos tridimensionales. Este software facilita el diseño y prototipado de encapsulados para circuitería electrónica, asi como el modelado 3D de edificaciones. Existen una variedad de software de modelado 3D, entre los más utilizados están SketchUp, Autodesk Inventor y Adobe Illustrator. En la Tabla 31 puede observar una comparación entre los equipos SketchUp, Autodesk Inventor y Adobe Illustrator.

Tabla 31

Comparación entre los softwares SketchUp, Autodesk Inventor y Adobe Illustrator

Diferencias			
Características	**SketchUp**	**Autodesk Inventor**	**Adobe Illustrator**
Modelado 3D	Si.	Si.	Limitado a ciertos gráficos.
Precisión de modelado	Alta.	Muy alta.	Moderada.
Compatibilidad de formatos	DWG, DXF, 3DS, DAE, KMZ, STL, OBJ, XSI, WRL, entre otros.	DWG, DXF, IAM, IPT, STEP, IGES, STL, SAT, entre otros.	AI, EPS, PDF, SVG, DWG, DXF, PSD, TIFF, PNG, JPG.

Renderizado	Básico.	Avanzado.	Básico para gráficos 2D.
Herramienta de diseño	Herramientas de dibujo.	Diseño paramétrico.	Herramientas de dibujo vectorial.
Interfaz de usuario	Intuitiva.	Compleja.	Intuitiva.
Extensiones	Biblioteca de extensiones propia.	Compatibilidad con extensiones externas.	Extensiones desde Adobe Creative Cloud.
Tipo de Licencia	Gratuita / Suscripción.	Suscripción.	Suscripción.

Nota. Esta tabla representa las diferencias entre los softwares de modelado 3D más comunes, fuente Autor.

El software de modelado 3D para el encapsulado de la circuitería de los nodos CLIENTE/SERVIDOR que se va a utilizar es el SketchUp, debido a que, permite el modelado 3D de alta precisión, la interfaz de usuario es intuitiva con una biblioteca de extensiones propia, su herramienta para diseñar es de tipo dibujo con un renderizado básico y al ser compatible con el formato stl permite imprimir los modelos 3D. En la Tabla 32 se puede observar las especificaciones del software SketchUp y en la Tabla 33 los requisitos mínimos para la instalación del software SketchUp.

Tabla 32

Especificaciones del software SketchUp

	Especificaciones
Facilidad de Uso	Interfaz intuitiva con herramientas de arrastre.
Herramientas de diseño	Herramientas de dibujo 2D y 3D, modelado de sólidos y superficies.

Precisión de modelado	Alta precisión.
Renderizado	V-Ray entre otros motores de renderizados externos.
Compatibilidad de formatos	Soporta múltiples formatos incluyendo stl.
Extensiones y plugins	Amplia biblioteca de extensiones y plugins.
Escalabilidad	Adecuado para proyectos de diferentes escalas.
Edición paramétrica	Soporta plugins de funcionalidades paramétricas externos.
Soporte	Soporte técnico en línea.
Licencia	Gratuita / Suscripción.

Nota. Esta tabla representa las especificaciones del software SketchUp, fuente Autor.

Tabla 33

Requisitos mínimos del software SketchUp

Componente	Requisitos mínimos
Sistema operativo	Windows 7, 8, 10 (32-bit y 64-bit)
Procesador	Intel Core I3
RAM	8 GB (recomendable)
Espacio en disco	1 GB
Tarjeta gráfica	Tarjeta de video 3D con 512 MB
Otros	OpenGL 3.0

Nota. Esta tabla representa los requisitos mínimos del software SketchUp, fuente Autor.

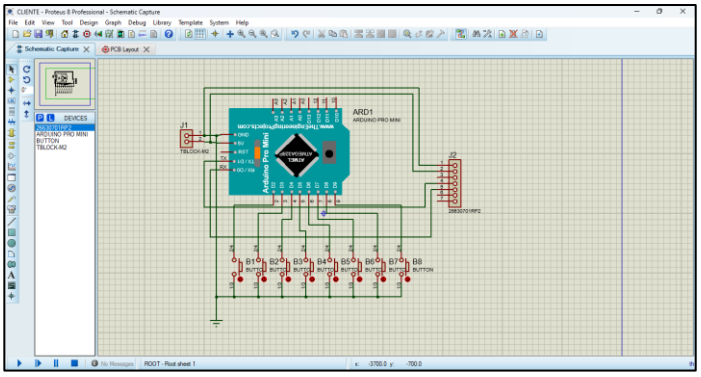
3.4 DISEÑO ESQUEMÁTICO/PCB EN PROTEUS

3.4.1 DISEÑO ESQUEMÁTICO DE LA CIRCUITERÍA DEL NODO CLIENTE

El diseño esquemático de la circuitería del nodo CLIENTE esta realizado en el software Proteus (ver Figura 59), se conforma de diferentes componentes electrónicos que interconectados entre si hacen la función de un circuito de transmisión RF, para una mejor visualización del diseño revise el Anexo 7. En la Tabla 34 se puede detallan los componentes utilizados.

Figura 59

Diseño esquemático del nodo CLIENTE



Nota. La figura representa el diseño esquemático para el nodo CLIENTE en el software Proteus, fuente Autor.

Tabla 34

Componentes del diseño esquemático del nodo CLIENTE

Componentes utilizados		
Cantidad	**Componente**	**Función**
1	Arduino Pro mini	Microcontrolador.
1	TBLOCK-M2	Entrada para la fuente de alimentación.
1	26630701RP2	Entrada para el módulo Apc220.

8	Push Button	Envio de pulsos RF a los diodos LED.

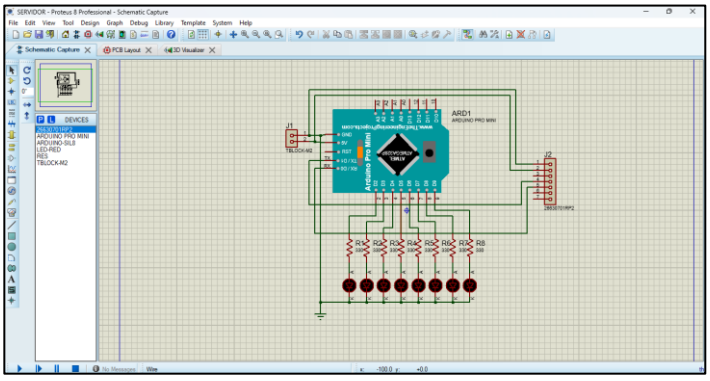
Nota. Esta table muestra los componentes del diseño esquemático del nodo SERVIDOR en Proteus, fuente Autor.

3.4.2 DISEÑO ESQUEMÁTICO DE LA CIRCUITERÍA DEL NODO SERVIDOR

El diseño esquemático de la circuitería del nodo SERVIDOR esta realizado en el software Proteus (ver Figura 60), se conforma de diferentes componentes electrónicos que interconectados entre si hacen la función de un circuito de recepción RF, para una mejor visualización del diseño revise el Anexo 8. En la Tabla 35 se puede detallan los componentes utilizados.

Figura 60

Diseño esquemático del nodo SERVIDOR



Nota. La figura representa el diseño esquemático para el nodo SERVIDOR en el software Proteus, fuente Autor.

Tabla 35

Componentes del diseño esquemático del nodo SERVIDOR

Componentes utilizados		
Cantidad	**Componente**	**Función**
1	Arduino Pro mini	Microcontrolador.

1	TBLOCK-M2	Entrada para la fuente de alimentación.
1	26630701RP2	Entrada para el módulo Apc220.
8	RES	Resistencia de protección para los diodos LED.
8	LED – RED	Recepción de pulso RF de los pulsadores.

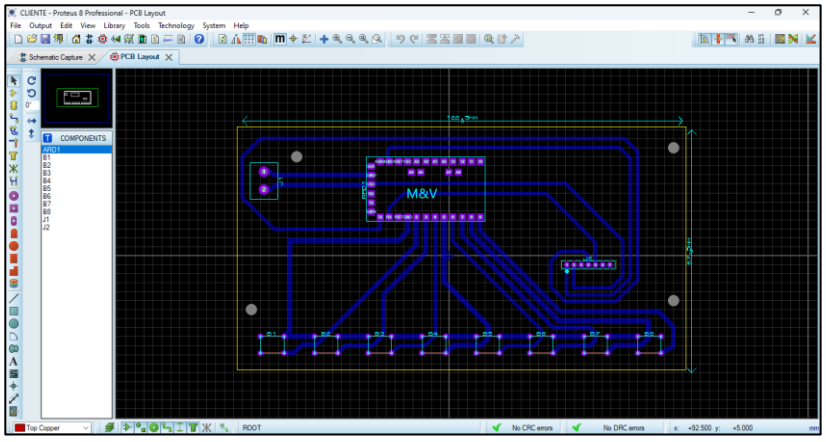
Nota. Esta table muestra los componentes del diseño esquemático del nodo SERVIDOR en Proteus, fuente Autor.

3.4.3 DISEÑO PCB PARA LA CIRCUITERÍA DEL NODO CLIENTE

El diseño PCB para la circuitería del nodo CLIENTE está realizado en Proteus (ver Figura 61), se realiza partiendo del diseño esquemático y lleva los mismos componentes (ver la Tabla 34), para una mejor visualización del diseño PCB del nodo CLIENTE revise el Anexo 9. En el apartado PCB Layout de Proteus se crea la Board Edge de 122.5 mm x 67.5 mm, dentro de la Board Edge creada se van ubicando los componentes, para crear las pistas se utiliza la herramienta Track Mode con la que se va conectando componente por componente de acuerdo al diseño esquemático. Para una mejor visualización revise el Anexo 9.

Figura 61

Diseño PCB del nodo CLIENTE



Nota. La figura representa del diseño PCB del nodo CLIENTE en Proteus, fuente Autor.

Adicional, Proteus cuenta con la herramienta 3D Visualizer, que permite visualizar el producto final de la circuitería del nodo CLIENTE mediante un modelo 3D (ver Figura 62), este modelado 3D se lo puede exportar en un archivo de formato iges para luego poder modelar el encapsulado.

Figura 62

Modelado 3D de la circuitería del nodo CLIENTE

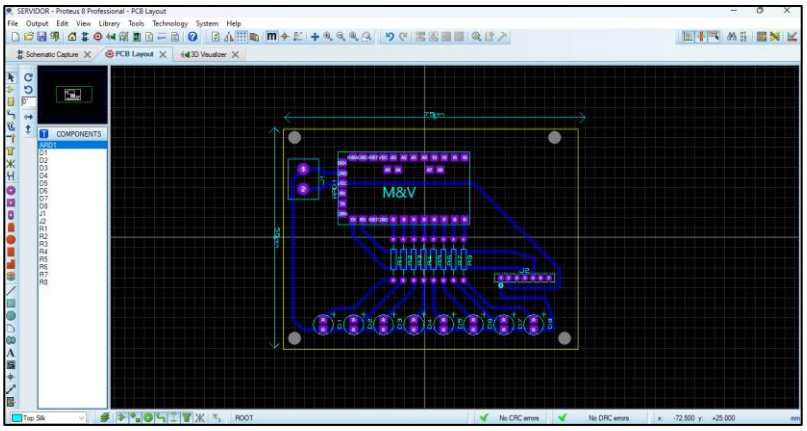
Nota. La figura representa el modelado 3D de la circuitería del nodo CLIENTE en Proteus, fuente Autor.

3.4.4 DISEÑO PCB PARA LA CIRCUITERÍA DEL NODO SERVIDOR

El diseño PCB para la circuitería del nodo SERVIDOR está realizado en Proteus (ver Figura 63), se realiza partiendo del diseño esquemático y lleva los mismos componentes (ver la Tabla 35), para una mejor visualización del diseño PCB del nodo SERVIDOR revise el Anexo 10. En el apartado PCB Layout de Proteus se crea la Board Edge de 75 mm x 55 mm, dentro de la Board Edge creada se van ubicando los componentes, para crear las pistas se utiliza la herramienta Track Mode con la que se va conectando componente por componente de acuerdo al diseño esquemático. Para una mejor visualización revise el Anexo 10.

Figura 63

Diseño PCB del nodo SERVIDOR

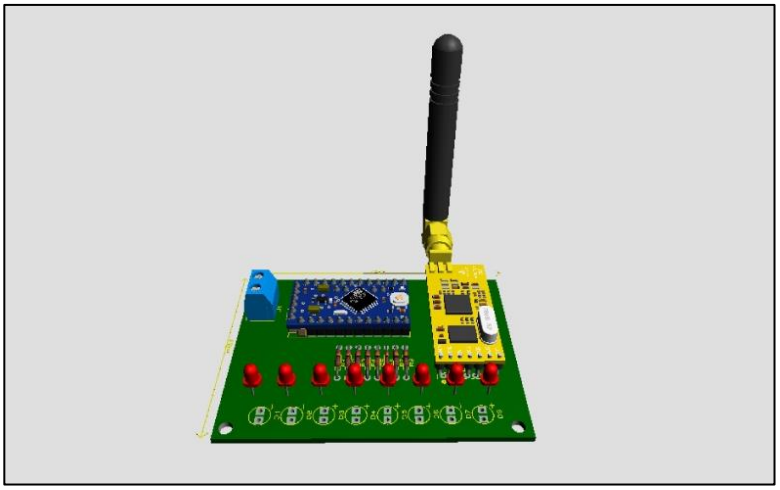


Nota. La figura representa del diseño PCB del nodo SERVIDOR en Proteus, fuente Autor.

Adicional, Proteus cuenta con la herramienta 3D Visualizer, que permite visualizar el producto final de la circuitería del nodo SERVIDOR mediante un modelo 3D (ver Figura 64), este modelado 3D se lo puede exportar en un archivo de formato iges para luego poder modelar el encapsulado.

Figura 64

Modelado 3D de la circuitería del nodo SERVIDOR



Nota. La figura representa el modelado 3D de la circuitería del nodo CLIENTE en Proteus, fuente Autor.

3.5 CÓDIGOS DE PROGRAMACIÓN EN ARDUINO

3.5.1 CÓDIGO DE PROGRAMACIÓN DEL NODO CLIENTE (TRANSMISOR)

El código de programación del nodo CLIENTE está realizado en Arduino IDE, controla el encendido y apagado de ocho diodos LED, mediante la lectura de ocho pulsadores conectados a los pines digitales del 2 al 9 configurados como entrada. Cada pulsador usa una resistencia pull-up interna, que al momento de ser presionado cambia el estado del diodo LED correspondiente entre encendido/apagado (inicialmente se encuentran apagados) en el nodo SERVIDOR y envía un mensaje por el puerto serial indicando el cambio. En la programación se espera a que se suelte el pulsador antes de leer nuevamente su estado para evitar múltiples cambios con una sola pulsación, y se le añade un retardo de 50 milisegundos para evitar rebotes en los pulsadores. Para la visualización del código de programación para el nodo cliente revise el Anexo 11.

3.5.2 CÓDIGO PARA EL NODO SERVIDOR (RECEPTOR)

El código de programación del nodo SERVIDOR está realizado en Arduino IDE, controla el encendido y apagado de ocho diodos LED, mediante la recepción de cadenas de texto a través del puerto serial que son emitidas por el nodo CLIENTE. Los ocho diodos LED están conectados a los pines digitales del 2 al 9 configurados como salida, cada diodo LED lleva una resistencia externa. La programación hace que se lea continuamente las cadenas recibidas, dependiendo del contenido de la cadena recibida se enciende o apaga el diodo LED correspondiente al pin especificado y este proceso se repite para cada uno de los diodos LED. Para la visualización del código de programación para el nodo cliente revise el Anexo 12.

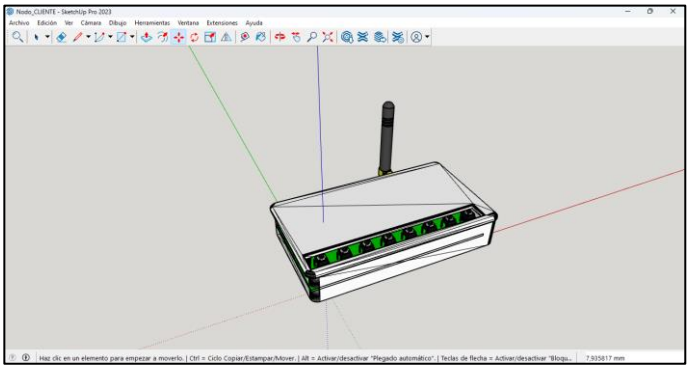
3.6 MODELADO 3D EN SKETCHUP

3.6.1 MODELADO DEL ENCAPSULADO DEL NODO CLIENTE

El modelado del encapsulado para la circuitería del nodo CLIENTE está realizado en SketchUp (ver Figura 65), y parte desde el archivo de formato iges proporcionado por el programa Proteus (ver Figura 62). El archivo de formato iges facilita tener una idea más clara de las dimensiones y detalles para el encapsulado, agilizando el trabajo de forma eficiente. Para una mejor visualización del modelado revise el Anexo 13.

Figura 65

Modelado del encapsulado para el nodo CLIENTE



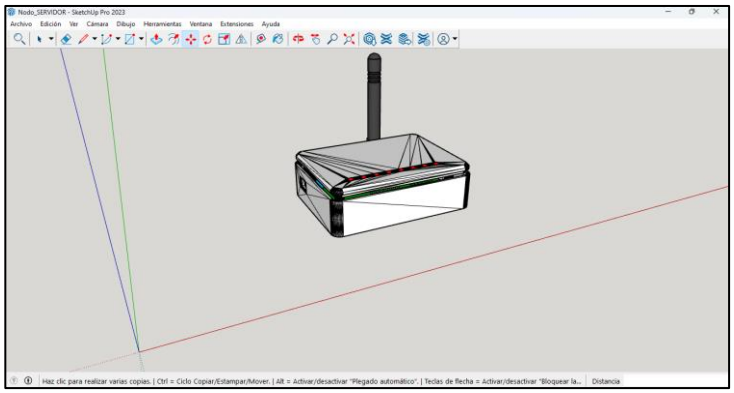
Nota. La figura representa el modelado 3D del encapsulado del nodo CLIENTE en SketchUp, fuente Autor.

3.6.2 MODELADO DEL ENCAPSULADO DEL NODO SERVIDOR

El modelado del encapsulado para la circuitería del nodo SERVIDOR está realizado en SketchUp (ver Figura 66), y parte desde el archivo de formato iges proporcionado por el programa Proteus (ver Figura 64). El archivo de formato iges facilita tener una idea más clara de las dimensiones y detalles para el encapsulado, agilizando el trabajo de forma eficiente. Para una mejor visualización del modelado revise el Anexo 14.

Figura 66

Modelado del encapsulado para el nodo SERVIDOR



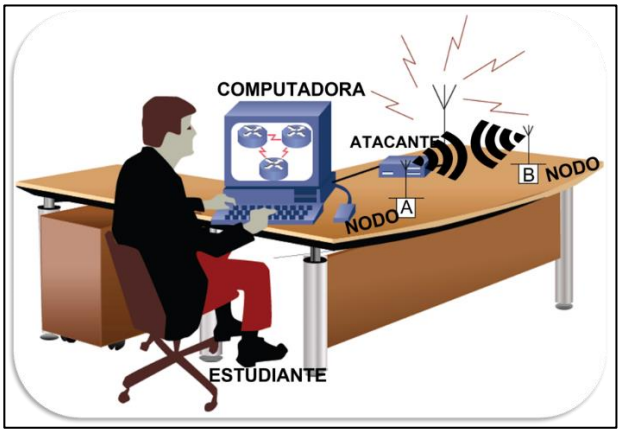
Nota. La figura representa el modelado 3D del encapsulado del nodo SERVIDOR en SketchUp, fuente Autor.

3.6.3 MODELADO DE LA PROPUESTA DENTRO DEL LABORATORIO DE TELECOMUNICACIONES

La propuesta del módulo educativo está dirigida para el laboratorio de Telecomunicaciones de la UPSE (ver Figura 67), El modelado 3D de la propuesta está realizado en SketchUp. Para una mejor visualización del modelado de la propuesta revise el Anexo 15.

Figura 67

Propuesta tecnológica



Nota. La figura hace referencia de la propuesta dentro del laboratorio de telecomunicaciones, fuente Autor.

3.7 PRODUCTO FINAL

3.7.1 NODO CLIENTE

El producto final del nodo CLIENTE (ver Figura 68) consiste de dos partes la circuitería y la impresión 3D del encapsulado para la circuitería. La circuitería cuenta de la unificación de los componentes físicos con la PCB, por otro lado, el encapsulado es la impresión 3D del modelado hecho en SketchUp. Para ver la evidencia de la construcción del nodo CLIENTE revise el Anexo 16.

Figura 68

Nodo CLIENTE

Nota. La figura representa el nodo CLIENTE como producto final, fuente Autor.

3.7.2 NODO SERVIDOR

El producto final del nodo SERVIDOR (ver Figura 69) consiste de dos partes la circuitería y la impresión 3D del encapsulado para la circuitería. La circuitería cuenta de la unificación de los componentes físicos con la PCB, por otro lado, el encapsulado es la impresión 3D del modelado

hecho en SketchUp. Para ver la evidencia de la construcción del nodo SERVIDOR revise el Anexo 17.

Figura 69

Nodo SERVIDOR

Nota. La figura representa el nodo SERVIDOR como producto final, fuente Autor.

3.8 FACTIBILIDAD DE LA PROPUESTA TECNOLÓGICA

3.8.1 FACTIBILIDAD EDUCATIVA

La factibilidad educativa de la propuesta tecnológica dentro del laboratorio de telecomunicaciones de la Universidad Estatal Península de Santa Elena es altamente factible. Beneficia directamente a las asignaturas de Comunicaciones Inalámbricas y Seguridad en Redes Inalámbricas. En la asignatura de Comunicaciones Inalámbricas, permite la emulación de escenarios de conectividad por RF, facilitando la comprensión práctica de la transmisión, modulación y análisis espectral de señales RF. En la signatura de Seguridad de Redes Inalámbricas, proporciona una plataforma para explorar y comprender las vulnerabilidades de las redes inalámbricas, permitiendo a los estudiantes practicar la identificación y mitigación de riesgos adicionales como el sniffing, jamming y spoofing en un entorno controlado.

La integración de un dispositivo SDR en el plan de estudios ofrece un enfoque didáctico, práctico y activo al aprendizaje, aumentando la comprensión teórica y técnica de los estudiantes. La disponibilidad de equipos y software de código abierto, junto con la capacitación adecuada del docente, garantizará el éxito del proyecto. Los estudiantes desarrollarán habilidades técnicas valiosas en el uso de dispositivos SDR, análisis de señales y seguridad de redes, preparándolos de mejor manera para el mercado laboral en telecomunicaciones como lo es la ciberseguridad. Además, el proyecto es escalable, permitiendo futuras expansiones e integraciones de nuevos módulos didácticos.

3.8.2 COSTO DE EQUIPOS

A continuación, en la Tabla 36 se detalla el costo de los equipos utilizados dentro de la propuesta.

Tabla 36

Costo de Equipos

Dispositivos	Cant.	Valor Unidad	Valor Total
HackRF One	1	347$	347$
CPU	1	300$	300$
Monitor	1	90$	90$
Mouse	1	10$	10$
Teclado	1	10$	10$
Cable HDMI	1	5$	5$
	TOTAL		762$

Nota. En esta tabla se detallan el costo de los equipos utilizados en la propuesta, fuente Autor.

3.8.3 COSTO DE MATERIALES

A continuación, en la Tabla 37 se detalla el costo de los materiales utilizados dentro de la propuesta.

Tabla 37

Costo de Materiales

Materiales	Cant.	Valor Unidad	Valor Total
Arduino pro mini ATmega328	2	11$	22$
Tira de espadines	1	0.75$	0.75$
Conector de bloque 2 entradas	2	0.20$	0.40$
Módulo FT232PL / USB TTL	1	6$	6$
Cable USB a mini-USB	1	1$	1$
Kit de módulos RF APC220	1	30$	30$
Resistencias 330 ohm	8	0.10$	0.80$
Diodo LED rojo	8	0.10$	0.80$
Pulsadores	8	0.20$	1.60$
Baquelita 15x20	2	1.50$	3$
Fuente de alimentación 5V/2A	2	5$	10$
Cable dupont x 40 / 20cm	1	2$	2$
Rollo de estaño	1	5$	5$
Pasta para Soldar	1	3$	3$
Cautín	1	4$	4$
TOTAL			90.35$

Nota. En esta tabla se detallan el costo de los materiales utilizados en la propuesta, fuente Autor.

3.8.4 COSTO VARIO

A continuación, en la Tabla 38 se detalla el costo vario utilizado dentro de la propuesta.

Tabla 38

Costo Vario

Concepto	Cant.	Valor Unidad	Valor Total
Impresión PCB circuitería	2	10$	20$
Impresión 3D Modelados	2	10$	20$
Envio HackRF One – USA	1	20$	20$
Envio Kit módulos APC220 – China	1	20$	20$
Transportación	-	-	20$
TOTAL			100$

Nota. En esta tabla se detallan el costo vario utilizado en la propuesta, fuente Autor.

3.8.5 COSTO TOTAL

A continuación, en la Tabla 39 se detalla el costo total utilizado dentro de la propuesta.

Tabla 39

Costo total

COSTO TOTAL	
Costo de equipos	762$
Costo de materiales	90.35$
Costo vario	100$
TOTAL	952.35$

Nota. En esta tabla se detallan el costo total de la propuesta, fuente Autor.

CAPITULO VI

RESULTADOS

4.1 PRUEBAS

4.1.1 PRUEBA 1 – ATAQUE EAVESDROPPING

La primera prueba consiste en generar un ataque de tipo eavesdropping a la capa de enlace de datos del nodo CLIENTE, este ataque se basa en la intercepción y captura de datos, haciendo referencia a la escucha en lo secreto. La aplicación de este ataque se hace al nodo CLIENTE, debido a que este nodo envia una cadena de caracteres (trama de datos) al nodo SERVIDOR por RF.

Para la preparación de este ataque, se conecta el dispositivo HackRF One a la computadora por medio de su cable USB, en el programa URH se utiliza la herramienta “Record Signal” que se encuentra en el apartado File, al abrirse la ventana de “Record Signal” se puede configura el dispositivo SDR.

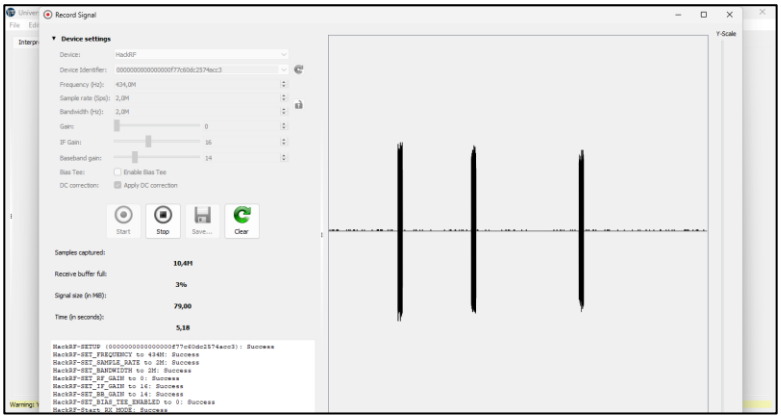
Para configurar el dispositivo SDR en el atributo “Device” se selecciona HackRF y para que el programa detecte el dispositivo se da clic en la flecha verde, luego en el atributo “Frecuency (Hz)” colocamos la frecuencia a la que trabaja el nodo CLIENTE que es de 434 MHz, realizando todo eso el escenario está preparado para el ataque, solo resta pulsar “Start” para empezar la captura.

Al pulsar “Start” el dispositivo HackRF One a través del programa URH empieza a capturar los datos que existan en la frecuencia 434 MHz (ver Figura 70), en el nodo CLIENTE se realiza la secuencia de pulsaciones, que en este caso es pulsador 1 (luz2on), pulsador 2 (luz3on) y pulsador 3(luz4on), esta secuencia es enviada por RF al nodo SERVIDOR como una cadena de caracteres

(tramas de datos). El nodo SERVIDOR al recibir esta secuencia enciende en primer lugar el LED 1, luego el LED 2 y por último el LED 3.

Figura 70

Captura de datos - Prueba 1

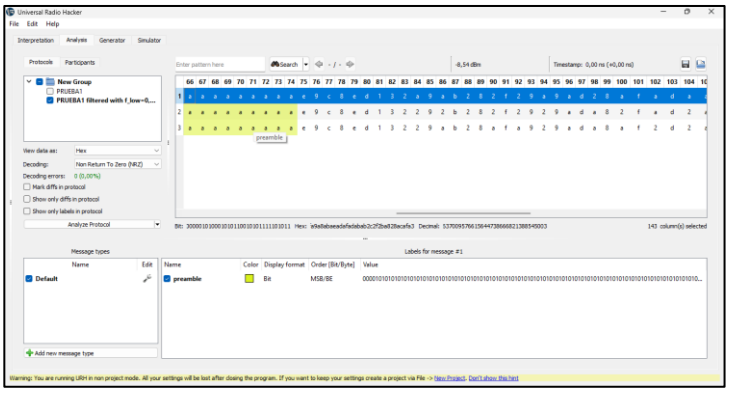


Nota. La figura representa la captura de datos para la prueba 1, fuente Autor.

Luego de ser capturada esta cadena es guardada en un archivo formato complex16s con el nombre PRUEBA1, una vez guardado el archivo y al cerrar la ventana de “Record Signal”, se abre la ventana de “Interpretation” en donde se procesa la señal análoga capturada para obtener una señal digital demodulada. Una vez procesada la señal en la ventana “Analysis” se muestra la trama de datos capturada (ver Figura 71). Revise el Anexo 18 para visualizar todo el proceso.

Figura 71

Captura de la trama - Prueba 1



Nota. En la figura se observa la trama de datos captura en la prueba 1, fuente Autor.

4.1.2 PRUEBA 2 – ATAQUE REPLAY

La segunda prueba consiste en generar un ataque de tipo replay a la capa de enlace de datos del nodo CLIENTE, este ataque se basa en la captura y retransmisión de datos sin modificarlos. La aplicación de este ataque se hace al nodo CLIENTE, debido a que este nodo envia una cadena de caracteres (trama de datos) al nodo SERVIDOR por RF.

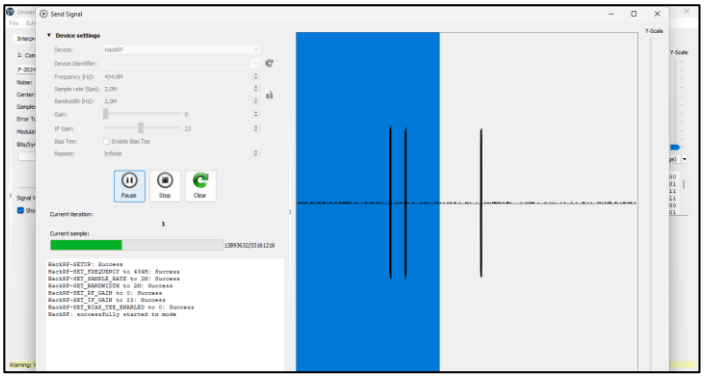
Para la preparación de la prueba, la configuración del equipo y la captura de la trama de datos se realiza el mismo proceso que en la prueba 1, pero con las siguientes modificaciones, en el nodo CLIENTE la secuencia de pulsaciones es pulsador 1 (luz2on), pulsador 3 (luz4on) y pulsador 5(luz6on), la capturada esta cadena es guardada con el nombre PRUEBA2.

Para retransmitir la trama de datos sin modificaciones, se dirige a la ventana “Interpretation” al lado de la palabra “Complex Signal” se encuentra el botón “Replay Signal”, al dar clic al botón se abre la ventana “Send Signal”, allí se verifica que este seleccionado e identificado el dispositivo HackRF. Luego se da clic en el botón “Start” y la señal con la trama de datos capturada empieza a ser retransmitida (ver Figura 72), en el nodo SERVIDOR sin tocar los

pulsadores del nodo CLIENTE se muestra el encendido de los diodos LED en la secuencia LED1, LED3 y LED5. Revise el Anexo 19 para visualizar todo el proceso.

Figura 72

Retransmisión de la trama capturada - Prueba 2



Nota. La figura muestra la retransmisión de la trama sin modificaciones de la prueba 2, fuente Autor.

4.1.3 PRUEBA 3 – ATAQUE MITM

La tercera prueba consiste en generar un ataque de tipo MITM (modificación de datos) a la capa de enlace de datos del nodo CLIENTE, este ataque se basa en la captura y retransmisión de datos, pero modificándolos. La aplicación de este ataque se hace al nodo CLIENTE, debido a que este nodo envia una cadena de caracteres (trama de datos) al nodo SERVIDOR por RF.

Para la preparación de la prueba, la configuración del equipo y la captura de la trama de datos se realiza el mismo proceso que en la prueba 1, pero con las siguientes modificaciones, en el nodo CLIENTE la secuencia de pulsaciones es pulsador 3 (luz4on), pulsador 5 (luz6on) y pulsador 7(luz8on), la capturada esta cadena es guardada con el nombre PRUEBA3.

La modificación de la señal capturada se la realiza en la ventana “Interpretation”, la señal que se muestra como PRUEBA 3 tiene la secuencia de pulsador 3 (luz4on), pulsador 5 (luz6on) y

pulsador 7(luz8on), entonces el programa permite cortar la señal de los pulsos y pegarlos de tal manera que la secuencia inicial sea modificada, en este caso la señal modificada tiene la secuencia de pulsador 7 (luz8on), pulsador 3 (luz4on) y pulsador 5(luz6on) (ver Figura 73).

Figura 73

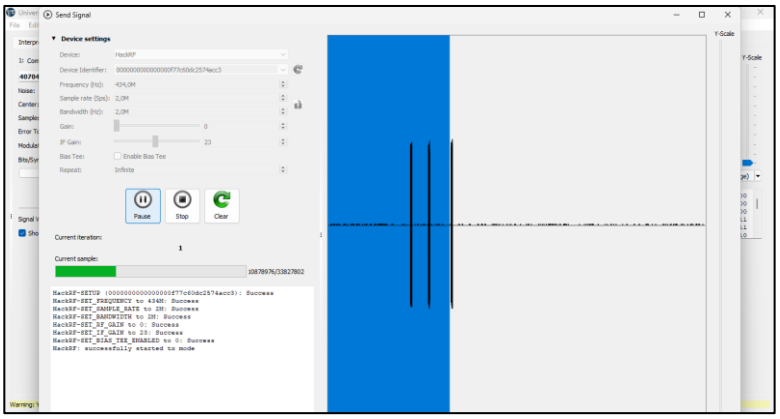
Señal modificada - Prueba 3

Nota. En la figura se muestra la trama de la secuencia modificada para la prueba 3, fuente Autor.

Para retransmitir la trama de datos modificada, se dirige a la ventana “Interpretation” al lado de la palabra “Complex Signal” se encuentra el botón “Replay Signal”, al dar clic al botón se abre la ventana “Send Signal”, allí se verifica que este seleccionado e identificado el dispositivo HackRF. Luego se da clic en el botón “Start” y la señal con la trama de datos modifica empieza a ser transmitida (ver Figura 74), en el nodo SERVIDOR sin tocar los pulsadores del nodo CLIENTE se muestra el encendido de los diodos LED en la secuencia LED7, LED3 y LED5. Revise el Anexo 20 para visualizar todo el proceso.

Figura 74

Transmisión de la señal modificada - Prueba 3



Nota. En la figura se nuestra la transmisión de la trama modificada en la prueba 3, fuente Autor.

4.2 ANÁLISIS DE RESULTADOS

La aplicación de los ataques Eavesdropping, Replay y Man in the Middle (MITM) permitieron demostrar las vulnerabilidades presentes en la capa de enlace de datos del modelo OSI de los nodos CLIENTE/SERVIDOR. Los resultados de las pruebas hechas muestran que es posible interceptar, capturar y modificar datos en la comunicación entre nodos cliente y servidor, lo que incita a la importancia de implementar medidas de seguridad para proteger las transmisiones inalámbricas. Para mitigar los ataques de tipo eavesdropping se puede implementar la encriptación de los datos de la trama, para mitigar los ataques de tipo ataques replay se puede colocar un timestamps a la trama de datos y para mitigar los ataques de tipo MITM se puede solicitar una autenticación mutua entre ambos nodos.

El uso del dispositivo HackRF One y el programa URH permitió un entendimiento profundo del funcionamiento de los dispositivos SDR en comunicaciones inalámbricas. Se logró configurar y utilizar el dispositivo HackRF One para realizar los tres tipos de ataques, demostrando

su capacidad para analizar, capturar y manipular señales de radiofrecuencia, lo cual es esencial para la evaluación de la seguridad en redes inalámbricas.

Se desarrolló exitosamente dos códigos de programación, uno para la función de transmisor y otro para la función de receptor, utilizando la tarjeta microcontroladora Pro mini de Arduino y el módulo APC220 de RF. La programación y configuración de estos módulos permitió establecer una conexión punto a punto efectiva entre los nodos CLIENTE/SERVIDOR, lo que facilitó la demostración de las vulnerabilidades. Además, se diseñó y modeló en 3D tanto el circuito impreso como los encapsulados que contienen la circuitería de los nodos, logrando una integración eficiente de los componentes.

El módulo didáctico fue implementado con éxito, interconectando todos los dispositivos necesarios para realizar las prácticas orientadas a los ataques en la transmisión inalámbrica. Este módulo, junto con el manual de la práctica para el estudiante (ver Anexo 21), proporciona una herramienta educativa que refuerza la enseñanza sobre las vulnerabilidades en la seguridad de redes inalámbricas en un entorno controlado dentro del laboratorio de Telecomunicaciones.

CONCLUSIONES

- El dispositivo HackRF One es altamente versátil con amplias aplicaciones en telecomunicaciones. Además de la recepción y transmisión de señales RF, es útil en el análisis de seguridad de sistemas inalámbricos, la educación en nuevas tecnologías, el monitoreo del espectro radioeléctrico, las comunicaciones de radioaficionados, el procesamiento de datos RF, y el desarrollo de prototipos de radio para redes de próxima generación.

- La conexión punto a punto entre los nodos CLIENTE/SERVIDOR se realizó con éxito, es el proceso más importante porque genera la comunicación inalámbrica a la que se le aplican los ataques para identificar los puntos débiles en la transmisión de datos.
- La captura de datos en la transmisión inalámbrica con el programa URH fue exitosa, permitiendo realizar ataques de eavesdropping, replay y man in the middle. Esto confirmó la capacidad de URH para capturar y analizar transmisiones inalámbricas, destacando la facilidad con la que pueden ser interceptadas y manipuladas.
- La interconexión de todos los dispositivos creó un entorno práctico controlado para demostrar ataques en la transmisión inalámbrica. Este módulo didáctico servirá como herramienta educativa, permitiendo a los estudiantes comprender profundamente las vulnerabilidades en las comunicaciones inalámbricas y las técnicas para explotarlas.
- El sistema de comunicación RF demostró ser vulnerable a ataques de eavesdropping, replay y MITM. La captura y retransmisión de señales RF sin autenticación o cifrado facilita la explotación de estas vulnerabilidades, comprometiendo la seguridad de la capa de enlace de datos del modelo OSI al permitir que las señales sean obtenidas y reutilizadas sin ser detectadas.

RECOMENDACIONES

- Explorar minuciosamente las capacidades del dispositivo HackRF One en artículos científicos e investigaciones que cuenten con su respectiva sustentación teórica, para el desarrollo de nuevas aplicaciones en las telecomunicaciones del futuro.
- Mejorar la programación de los nodos, para no solo transmitir una cadena de caracteres sino también textos largos o imágenes y poder aprovechar al máximo las funcionalidades del software URH.

- Considerar la inclusión de otros tipos de ataques y técnicas de mitigación en el módulo didáctico para ofrecer una experiencia educativa más completa.
- Implementar algún tipo de seguridad a la cadena de caracteres, como la encriptación de datos, un timestamps a la trama o la autenticación mutua de los nodos CLIENTE/SERVIDOR, para visualizar el comportamiento del ataque y saber si pudo o no ser mitigado.
- Mejorar el módulo educativo implementando una tarjeta NodeMCU ESP8266 o una tarjeta NodeMCU ESP32 como cliente y la nube como servidor, para analizar ataques en la capa de red del modelo OSI.

BIBLIOGRAFÍA

[1] G. R. Malpica Vidal, «Propuesta de implementación de una red de datos inalámbrica administrada con servidor Centos en la I. E. Simón Antonio Bolívar Palacios,» 2023. [En línea]. Available: https://hdl.handle.net/20.500.13032/31776. [Último acceso: 17 Noviembre 2023].

[2] D. R. David Patiño y E. A. Sánchez Galindo, «Las amenazas de seguridad a las que se enfrenta IoT y las soluciones en desarrollo,» 2021. [En línea]. Available: http://hdl.handle.net/11349/29310. [Último acceso: 18 Noviembre 2023].

[3] AMBIT TEAM, «Diferencias entre amenaza, vulnerabilidad y riesgo,» 2022. [En línea]. Available: https://www.ambit-bst.com/blog/diferencias-entre-amenaza-vulnerabilidad-y-riesgo. [Último acceso: 23 Noviembre 2023].

[4] J. S. Rondon Sanabria y A. F. Bravo Montoya, «Esquema de Seguridad de Datos Entre los Nodos y el Gateway en una Red LoRaWan,» 2019. [En línea]. Available: http://hdl.handle.net/11349/25252. [Último acceso: 23 Noviembre 2023].

[5] Gesteira, «Pruebas de intrusión en automóviles mediante ataques de radio frecuencia. Análisis de vulnerabilidades,» 2022. [En línea]. Available: http://hdl.handle.net/11531/66178. [Último acceso: 11 Noviembre 2023].

[6] G. Sánchez Bautista y L. Ramírez Chávez, «Amenazas de seguridad a considerar en el desarrollo de software,» 2022. [En línea]. Available: https://doi.org/10.29057/xikua.v10i19.8118. [Último acceso: 23 Noviembre 2023].

[7] G. G. Jaramillo Pizarro, «Desarrollo de un algoritmo de Modulación en Espacio, Tiempo y Frecuencia Ortogonal (OTFS) en un Software Definido por Radio (SDR).,» 2023. [En línea]. Available: http://dspace.ups.edu.ec/handle/123456789/26444. [Último acceso: 23 Noviembre 2023].

[8] C. Noboa Terán, «Análisis y Evaluación de la Plataforma de Radio Definido por Software de Bajo Costo: Adalm- Pluto SDR Active Learning Module,» 2020. [En línea]. Available: http://www.dspace.espol.edu.ec/handle/123456789/56362. [Último acceso: 23 Noviembre 2023].

[9] V. Montejo del Pino, «Ciberataque en dispositivo IOT de reducidas prestaciones,» 2021. [En línea]. Available: https://oa.upm.es/67591/. [Último acceso: 23 Noviembre 2023].

[10] E. Rivera Arellano, «Explotar vulnerabilidades de IOT con GNUradio y SDR,» 2023. [En línea]. Available: https://hdl.handle.net/20.500.14352/9076. [Último acceso: 23 Noviembre 2023].

[11] A. Lindeberg, «Hacking Into Someone's Home using Radio Waves: Ethical Hacking of Securitas' Alarm System,» 2021. [En línea]. Available: https://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-302999. [Último acceso: 23 Noviembre 2023].

[12] M. Onofa, «Ataques cibernéticos amenazan seguridad en Ecuador,» Diálogo Americas, 2022. [En línea]. Available: https://dialogo-americas.com/es/articles/ataques-ciberneticos-amenazan-seguridad-en-ecuador/#.Y5-r0XbMLre. [Último acceso: 28 Noviembre 2023].

[13] L. Abril, «Ecuador está entre los países con más ciberataques en América Latina,» El Comercio, 2021. [En línea]. Available: https://www.elcomercio.com/tendencias/tecnologia/ecuador-ciberataques-america-latina-hacker.html. [Último acceso: 28 Noviembre 2023].

[14] T. Menéndez, «Ecuador registra un bajo índice de ciberseguridad,» Primicias, 2021. [En línea]. Available: https://www.primicias.ec/noticias/sociedad/ecuador-registra-bajo-indice-ciberseguridad/. [Último acceso: 28 Noviembre 2023].

[15] L. Abril, «El 9% de las empresas de Ecuador sufrió algún incidente de ciberseguridad,» El Comercio, 2022. [En línea]. [Último acceso: 28 Noviembre 2023].

[16] P. Mero, «RESEÑA HISTORICA DE LA UPSE,» electro10, 2014. [En línea]. [Último acceso: 28 Noviembre 2023].

[17] Cisco Networking Academy, «Beneficios del uso de un modelo en capas,» CCNA: Introduction to Networks, [En línea]. Available: https://www.netacad.com/es/courses/networking/ccna-introduction-networks. [Último acceso: 29 Noviembre 2023].

[18] C. Henao Pinto, «Diseño de una red LAN para la empresa Bits Americas S.A.S.,» 2019. [En línea]. Available: http://hdl.handle.net/20.500.12495/6211. [Último acceso: 28 Noviembre 2023].

[19] R. Echeverría Portillo y M. Celis Ortega, «TCP/IP e Interconexión de Redes. Introducción a la Arquitectura Internet OSI. Un Modelo de Referencia,» *Polibits,* vol. 20, p. 25, 1998.

[20] N. Ramírez Galvis, J. Rivera Cardona y C. Mejía Londoño, «Vulnerabilidad, tipos de ataques y formas de mitigarlos en las capas del modelo OSI en las redes de datos de las organizaciones,» 2012. [En línea]. Available: https://hdl.handle.net/11059/2734. [Último acceso: 29 Noviembre 2023].

[21] R. Siles Peláes, de *Análisis de seguridad de la familia de protocolos TCP/IP y sus servicios asociados,* Primera ed., 2002, pp. 25-26.

[22] Á. &. Chalan, «Políticas de ciberseguridad para los dispositivos de capa-dos en el centro de datos del hospital de Latacunga,» 2022. [En línea]. Available: https://repositorio.pucesa.edu.ec/handle/123456789/3516. [Último acceso: 11 Noviembre 2023].

[23] C. Obando I, «Seguridad a nivel de enlace de datos en el modelo de interconexión de sistemas abiertos (OSI),» *iname,* vol. 2, nº 2, pp. 71-78, Junio 2022.

[24] Echegaray, «Capa de aplicación,» 2021. [En línea]. Available: https://hdl.handle.net/20.500.12394/9062. [Último acceso: 11 Noviembre 2023].

[25] Eraso, «Modelos TCP/IP y OSI,» 2019. [En línea]. Available: https://repositorio.konradlorenz.edu.co/handle/001/1397. [Último acceso: 11 Noviembre 2023].

[26] R. &. Espinosa, «Análisis de brechas de seguridad en redes LPWAN: SIGFOX y LORAWAN en base a la norma ISO 27001:2013,» 2023. [En línea]. Available: http://repositorio.uisrael.edu.ec/handle/47000/3564. [Último acceso: 11 Noviembre 2023].

[27] Olarte, «Seguridad informática y la vulnerabilidad del sistema de información inalámbrico en la municipalidad provincial de la convención, periodo 2020,» 2023. [En línea]. Available: http://repositorio.ulp.edu.pe/handle/ULP/49. [Último acceso: 11 Noviembre 2023].

[28] Arias, «Análisis de un enlace de comunicaciones ópticas inalámbricas en espacio libre para medir tasa de error de bits, calidad y potencia de la señal desde la universitaria Agustiniana hasta el colegio Agustiniano Tagaste,» 2021. [En línea]. Available: http://repositorio.uniagustiniana.edu.co/handle/123456789/1702. [Último acceso: 11 Noviembre 2023].

[29] Burbano, «Controlador lógico programable bajo software y hardware libre,» 2022. [En línea]. Available: http://repositorio.utn.edu.ec/handle/123456789/12632. [Último acceso: 11 Noviembre 2023].

[30] C. &. Estrada, «Implementación de un sistema automatizado para riego basado en la tecnología arduino para controlar balance de humedad de suelo en el recinto Siete Ríos,» 2021. [En línea]. Available: http://repositorio.utc.edu.ec/handle/27000/7302. [Último acceso: 11 Noviembre 2023].

[31] Heredia, «Implementación de un prototipo NAS con Raspberry Pi con software libre.,» 2022. [En línea]. Available: http://bibdigital.epn.edu.ec/handle/15000/22844. [Último acceso: 11 Noviembre 2023].

[32] Guzman, «Diseño y modelado de una arquitectura hardware de un clasificador basado en máquinas de soporte vectorial,» 2022. [En línea]. Available: http://repositorio.utm.mx:8080/jspui/handle/123456789/455. [Último acceso: 11 Noviembre 2023].

[33] N. &. Frutos, «Sistema para el control de procesos en el desarrollo de software y en la planificación de las actividades del Departamento de T.I. de la Cooperativa de Ahorro y Crédito San Francisco Ltda.,» 2021. [En línea]. Available: https://repositorio.uta.edu.ec/jspui/handle/123456789/33844. [Último acceso: 11 Noviembre 2023].

[34] D. &. L. Amestica, «An Experimental Comparison of Arduino IDE Compatible Platforms for Digital Control and Data Acquisition Applications,» 2019. [En línea]. Available: https://doi.org/10.1109/CHILECON47746.2019.8986865. [Último acceso: 11 Noviembre 2023].

[35] A. &. B. Molina, «La resolución de problemas basada en el método de Pólya usando el pensamiento computacional y Scratch con estudiantes de Educación Secundaria,» 2020. [En línea]. Available: https://hdl.handle.net/11162/198459. [Último acceso: 11 Noviembre 2023].

[36] Pumar, «Programación y creatividad unidas en Mblock,» 2021. [En línea]. Available: https://dialnet.unirioja.es/servlet/articulo?codigo=8213439. [Último acceso: 11 Noviembre 2023].

[37] F. &. M. Szychowski, «Módulos transceptores de radiofrecuencia para pruebas de comunicación en ambiente selvático,» 2021. [En línea]. Available: https://hdl.handle.net/20.500.12219/3184. [Último acceso: 11 Noviembre 2023].

[38] P. &. Velosa, «Implementación de un sistema de geoposicionamiento con transmisión de coordenadas por radiofrecuencia,» 2021. [En línea]. Available: https://doi.org/10.47961/2145194X.227. [Último acceso: 11 Noviembre 2023].

[39] P. &. Ruiz, «Caracterización de Software de Simulación de Circuitos Electrónicos Como Alternativas de uso en Educación Superior,» 2021. [En línea]. Available: https://repositorio.udes.edu.co/handle/001/7884. [Último acceso: 11 Noviembre 2023].

[40] O. &. Pérez, «Desarrollo de repositorio Web de software de simulación de circuitos electrónicos para uso en la Educación Superior,» 2020. [En línea]. Available: https://dialnet.unirioja.es/servlet/articulo?codigo=7787733. [Último acceso: 11 Noviembre 2023].

[41] Navarrete, «Comparación de los sistemas de modelado 3d y diseño para estructuras orientadas a la construcción en el cantón Babahoyo.,» 2022. [En línea]. Available: http://dspace.utb.edu.ec/handle/49000/12708. [Último acceso: 11 Noviembre 2023].

[42] M. &. Tonguino, «Diseño de un laboratorio virtual de ensayos destructivos y metalografía mediante el software sketchup y shapespark para prácticas en las asignaturas de ciencias de materiales,» 2021. [En línea]. Available: http://repositorio.uisek.edu.ec/handle/123456789/4244. [Último acceso: 17 Noviembre 2023].

[43] Gutierrez, «Proyecto de diseño y modelado de un personaje en 3D,» 2023. [En línea]. Available: https://riunet.upv.es/handle/10251/195263. [Último acceso: 11 Noviembre 2023].

[44] Suárez, «Radioespectrómetro solar basado en Software Defined Radio (SDR),» 2022. [En línea]. Available: http://hdl.handle.net/10017/53351. [Último acceso: 11 Noviembre 2023].

[45] B. &. Rodríguez, «Implementación de un módulo educativo para el análisis de la vulnerabilidad de dispositivos IoT, empleando SDR y GNU radio.Implementación de un módulo educativo para el análisis de la vulnerabilidad de dispositivos IoT, empleando SDR y GNU radio.,» 2023. [En línea]. Available: https://repositorio.upse.edu.ec/handle/46000/10317. [Último acceso: 11 Noviembre 2023].

[46] Rivera, «Implementación de Software Defined Radio en sistemas de comunicaciones actuales,» 2021. [En línea]. Available: https://hdl.handle.net/11441/109235. [Último acceso: 11 Noviembre 2023].

[47] Álvarez, «Diseño de un sistema SDR (Radio Definida por Software) mediante FPGA para la recepción de dispositivos RFID,» 2021. [En línea]. Available: https://uvadoc.uva.es/handle/10324/50027. [Último acceso: 11 Noviembre 2023].

[48] Vizcaino, «Optimización de una red Lan después de un ataque Ddos detectado con técnicas de inteligencia artificial,» 2022. [En línea]. Available: http://dspace.ups.edu.ec/handle/123456789/22264. [Último acceso: 11 Noviembre 2023].

ANEXOS

Anexo 1 – MAX2839 DATASHEET

EVALUATION KIT AVAILABLE

MAX2839

2.3GHz to 2.7GHz MIMO Wireless Broadband RF Transceiver

General Description

The MAX2839 direct conversion, zero-IF, RF transceiver is designed specifically for 2GHz 802.16e MIMO mobile WiMAX® systems. The device incorporates one transmitter and two receivers, with > 40dB isolation between each receiver. The MAX2839 completely integrates all circuitry required to implement the RF transceiver function, providing RF to baseband receive path, and baseband to RF transmit path, VCO, frequency synthesizer, crystal oscillator, and baseband/control interface. The device includes a fast-settling sigma-delta RF synthesizer with smaller than 40Hz frequency steps and a crystal oscillator that allows the use of a low-cost crystal in place of a TCXO. The transceiver IC also integrates circuits for on-chip DC-offset cancellation, I/Q error, and carrier leakage detection circuits. An internal transmit to receive loopback mode allows for receiver I/Q imbalance calibration. The local oscillator I/Q quadrature phase error can be digitally corrected in approximately 0.125° steps. Only an RF bandpass filter (BPF), crystal, RF switch, PA, and a small number of passive components are needed to form a complete wireless broadband RF radio solution.

The MAX2839 completely eliminates the need for an external SAW filter by implementing on-chip programmable monolithic filters for both the receiver and transmitter, for all 2GHz and 802.16e profiles and WIBRO. The baseband filters along with the Rx and Tx signal paths are optimized to meet the stringent noise figure and linearity specifications. The device supports up to 2048 FFT OFDM and implements programmable channel filters for 3.5MHz to 20MHz RF channel bandwidths. The transceiver requires only 2µs Tx-Rx switching time. The IC is available in a small 56-pin TQFN package measuring 8mm x 8mm x 0.8mm.

Applications

- 802.16e Mobile WiMAX Systems
- Korean WIBRO Systems
- Proprietary Wireless Broadband Systems
- 802.11g or n WLAN with MRC or MIMO Down Link

WiMAX is a registered certification mark and registered service mark of the WiMAX Forum.

Benefits and Features

- 2.3GHz to 2.7GHz Wideband Operation
- Dual Receivers for MIMO, Single Transmitter
- Complete RF Transceiver, PA Driver, and Crystal Oscillator
  - 2.3dB Rx Noise Figure on Each Receiver
  - -35dB Rx EVM for 64QAM Signal
  - 0dBm Linear OFDM Transmit Power (64QAM)
  - -70dBr Tx Spectral Emission Mask
  - -35dBc LO Leakage
  - Automatic Rx DC Offset Correction
  - Monolithic Low-Noise VCO with -39dBc Integrated Phase Noise
  - Programmable Rx I/Q Lowpass Channel Filters
  - Programmable Tx I/Q Lowpass Anti-Aliasing Filters
  - Sigma-Delta Fractional-N PLL with < 40Hz Step
  - 62dB Tx Gain Control Range with 1dB Step Size, Digitally Controlled
  - 95dB Rx Gain Control Range with 1dB Step Size, Digitally Controlled
  - 60dB Analog RSSI Instantaneous Dynamic Range
  - 4-Wire SPI Digital Interface
  - I/Q Analog Baseband Interface
  - Digital Tx/Rx Mode Control
  - Digitally Tuned Crystal Oscillator
  - On-Chip Digital Temperature Sensor Readout
- +2.7V to +3.6V Transceiver Supply
- Low-Power Shutdown Current
- Small, 56-Pin TQFN Package (8mm x 8mm x 0.8mm)

Ordering Information

PART	TEMP RANGE	PIN-PACKAGE
MAX2839ETN+TD	-40°C to +85°C	56 TQFN-EP*

+Denotes a lead(Pb)-free/RoHS-compliant package.
T = Tape and reel.
**EP = Exposed pad.*
D = Dry pack.

Pin Configuration and Block Diagram/Typical Operating Circuit appear at end of data sheet.

maxim integrated™

19-3218; Rev 2; 7/15

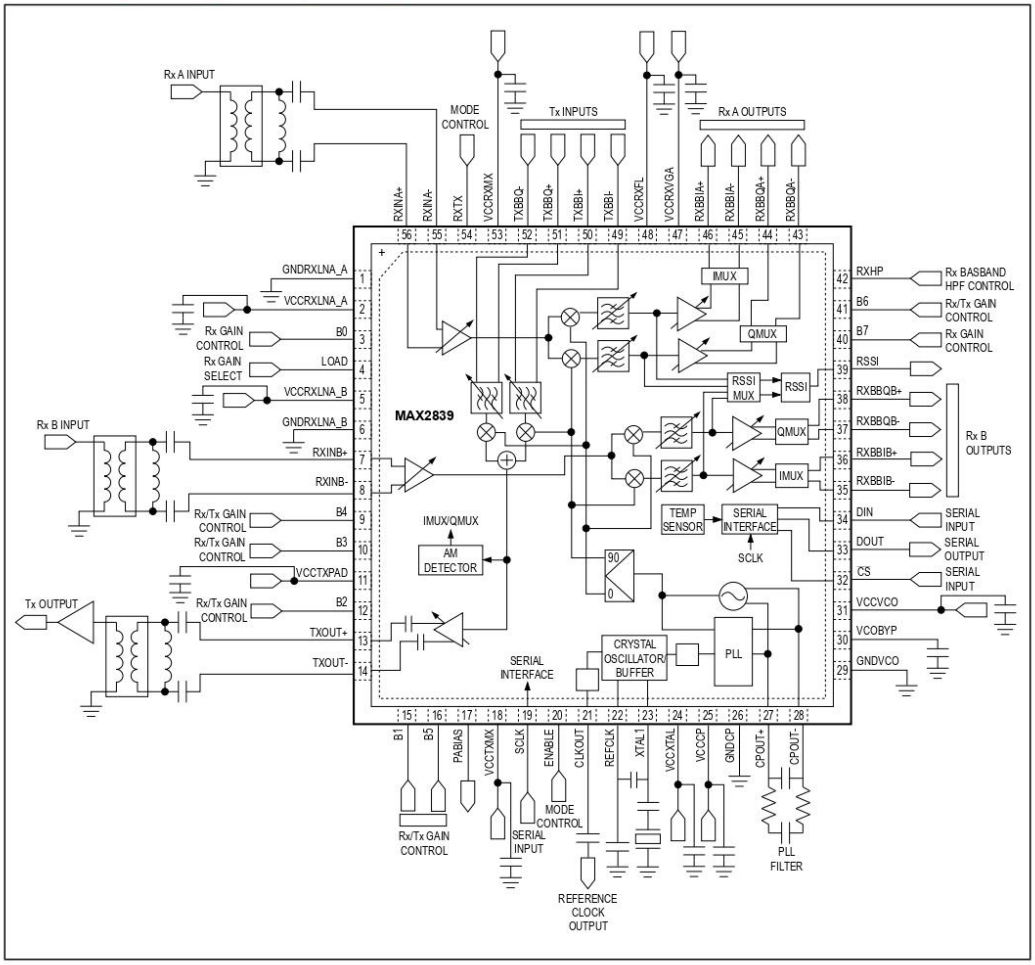
Pin Description

PIN	NAME	FUNCTION
1	GNDRXLNA_A	Receiver A LNA Ground
2	VCCRXLNA_A	Receiver A LNA Supply Voltage. Bypass with a 22pF capacitor as close as possible to the pin.
3	B0	Receiver Gain-Control Logic Input Bit 0
4	LOAD	Receiver Gain Select. Positive edge trigger latches digital gain inputs B0–B7 to receive A. Negative edge trigger latches digital gain inputs B0–B7 to receive B.
5	VCCRXLNA_B	Receiver B LNA Supply Voltage. Bypass with a 22pF capacitor as close as possible to the pin.
6	GNDRXLNA_B	Receiver B LNA Ground
7	RXINB+	Receiver B LNA Differential Input. Input is internally DC-coupled.
8	RXINB-	
9	B4	Receiver and Transmitter Gain-Control Logic Input Bit 4
10	B3	Receiver and Transmitter Gain-Control Logic Input Bit 3
11	VCCTXPAD	Supply Voltage for Transmitter PA Driver. Bypass with a 22pF capacitor as close as possible to the pin.
12	B2	Receiver and Transmitter Gain-Control Logic Input Bit 2
13	TXOUT+	Power Amplifier Driver Differential Output. The pins have internal AC blocking capacitors.
14	TXOUT-	
15	B1	Receiver and Transmitter Gain-Control Logic Input Bit 1
16	B5	Receiver and Transmitter Gain-Control Logic Input Bit 5
17	PABIAS	Transmit External PA Bias DAC Output
18	VCCTXMX	Transmitter Upconverter Supply Voltage. Bypass with a 22pF capacitor as close as possible to the pin.
19	SCLK	Serial-Clock Logic Input of 4-Wire Serial Interface
20	ENABLE	Transceiver Enable
21	CLKOUT	Reference Clock Buffer Output
22	REFCLK	Crystal or Reference Clock Input. AC-couple a crystal or a reference clock to this analog input.
23	XTAL1	XTAL Input. Connect the other terminal of the XTAL to this pin.
24	VCCXTAL	Crystal Oscillator Supply Voltage. Bypass with a 100nF capacitor as close as possible to the pin.
25	VCCCP	PLL Charge-Pump Supply Voltage. Bypass with a 100nF capacitor as close as possible to the pin.
26	GNDCP	Charge-Pump Circuit Ground
27	CPOUT+	Differential Charge-Pump Output. Connect the frequency synthesizer's loop filter between these pins (see the *Typical Operating Circuit*).
28	CPOUT-	
29	GNDVCO	VCO Ground
30	VCOBYP	On-Chip VCO Regulator Output Bypass. Bypass with a 1µF capacitor to GND. Do not connect other circuitry to this pin.
31	VCCVCO	VCO Supply Voltage. Bypass with a 22nF capacitor as close as possible to the pin.
32	$\overline{CS}$	Chip-Select Logic Input of 4-Wire Serial Interface
33	DOUT	Data Logic Output of 4-Wire Serial Interface
34	DIN	Data Logic Input of 4-Wire Serial Interface
35	RXBBIB-	Receiver B Baseband I-Channel Differential Outputs
36	RXBBIB+	

Pin Description (continued)

PIN	NAME	FUNCTION
37	RXBBQB-	Receiver B Baseband Q-Channel Differential Outputs
38	RXBBQB+	
39	RSSI	Receiver Signal Strength Output
40	B7	Receiver Gain-Control Logic Input Bit 7
41	B6	Receiver and Transmitter Gain-Control Logic Input Bit 6
42	RXHP	Receiver Baseband AC-Coupling Highpass Corner Frequency Control Logic Input. For typical WiMAX application, connect pin to ground.
43	RXBBQA-	Receiver Baseband Q-Channel Differential Outputs
44	RXBBQA+	
45	RXBBIA-	Receiver A Baseband I-Channel Differential Outputs
46	RXBBIA+	
47	VCCRXVGA	Receiver VGA Supply Voltage. Bypass with a 100nF capacitor as close as possible to the pin.
48	VCCRXFL	Receiver Baseband Filter Supply Voltage. Bypass with a 100nF capacitor as close as possible to the pin.
49	TXBBI-	Transmitter Baseband I-Channel Differential Inputs
50	TXBBI+	
51	TXBBQ+	Transmitter Baseband Q-Channel Differential Inputs
52	TXBBQ-	
53	VCCRXMX	Receiver Downconverters Supply Voltage. Bypass with a 22pF capacitor as close as possible to the pin.
54	RXTX	Receive/Transmit Mode Enable
55	RXINA-	Receiver A LNA Differential Input. Input is internally DC-coupled.
56	RXINA+	
—	EP	Exposed Paddle. Internally connected to GND. Connect to a large ground plane for optimum RF performance and enhanced thermal dissipation. Not intended as an electrical connection point.

Block Diagram/Typical Operating Circuit



Documentación completa: https://www.analog.com/en/products/max2839.html

Anexo 2 – MAX5864 DATASHEET

19-2915; Rev 1; 10/03

EVALUATION KIT AVAILABLE

MAXIM

Ultra-Low-Power, High-Dynamic-Performance, 22Msps Analog Front End

MAX5864

General Description

The MAX5864 ultra-low-power, highly integrated analog front end is ideal for portable communication equipment such as handsets, PDAs, WLAN, and 3G wireless terminals. The MAX5864 integrates dual 8-bit receive ADCs and dual 10-bit transmit DACs while providing the highest dynamic performance at ultra-low power. The ADCs' analog I-Q input amplifiers are fully differential and accept $1V_{P-P}$ full-scale signals. Typical I-Q channel phase matching is ±0.1° and amplitude matching is ±0.03dB. The ADCs feature 48.5dB SINAD and 69dBc spurious-free dynamic range (SFDR) at f_{IN} = 5.5MHz and f_{CLK} = 22Msps. The DACs' analog I-Q outputs are fully differential with ±400mV full-scale output, and 1.4V common-mode level. Typical I-Q channel phase match is ±0.15° and amplitude match is ±0.05dB. The DACs also feature dual 10-bit resolution with 71.7dBc SFDR, and 57dB SNR at f_{OUT} = 2.2MHz and f_{CLK} = 22MHz.

The ADCs and DACs operate simultaneously or independently for frequency-division duplex (FDD) and time-division duplex (TDD) modes. A 3-wire serial interface controls power-down and transceiver modes of operation. The typical operating power is 42mW at f_{CLK} = 22Msps with the ADCs and DACs operating simultaneously in transceiver mode. The MAX5864 features an internal 1.024V voltage reference that is stable over the entire operating power-supply range and temperature range. The MAX5864 operates on a +2.7V to +3.3V analog power supply and a +1.8V to +3.3V digital I/O power supply for logic compatibility. The quiescent current is 5.6mA in idle mode and 1µA in shutdown mode. The MAX5864 is specified for the extended (-40°C to +85°C) temperature range and is available in a 48-pin thin QFN package.

Applications

Narrowband/Wideband CDMA Handsets and PDAs

Fixed/Mobile Broadband Wireless Modems

3G Wireless Terminals

Ordering Information

PART	TEMP RANGE	PIN-PACKAGE
MAX5864ETM	-40°C to +85°C	48 Thin QFN-EP* (7mm x 7mm)
MAX5864E/D	-40°C to +85°C	Dice**

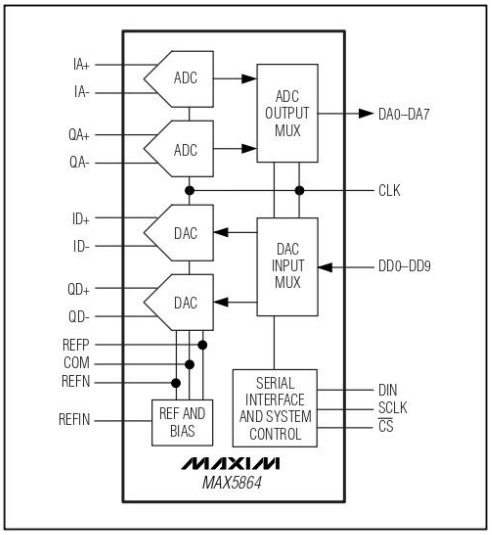
*EP = Exposed paddle.
**Contact factory for dice specifications.

Pin Configuration appears at end of data sheet.

Features

- **Integrated Dual 8-Bit ADCs and Dual 10-Bit DACs**
- **Ultra-Low Power**
  - **42mW at f_{CLK} = 22MHz (Transceiver Mode)**
  - **34mW at f_{CLK} = 15.36MHz (Transceiver Mode)**
  - **Low-Current Idle and Shutdown Modes**
- **Excellent Dynamic Performance**
  - **48.5dB SINAD at f_{IN} = 5.5MHz (ADC)**
  - **71.7dB SFDR at f_{OUT} = 2.2MHz (DAC)**
- **Excellent Gain/Phase Match**
  - **±0.1° Phase, ±0.03dB Gain at f_{IN} = 5.5MHz (ADC)**
- **Internal/External Reference Option**
- **+1.8V to +3.3V Digital Output Level (TTL/CMOS Compatible)**
- **Multiplexed Parallel Digital Input/Output for ADCs/DACs**
- **Miniature 48-Pin Thin QFN Package (7mm × 7mm)**
- **Evaluation Kit Available (Order MAX5865EVKIT)**

Functional Diagram



For pricing, delivery, and ordering information, please contact Maxim/Dallas Direct! at 1-888-629-4642, or visit Maxim's website at www.maxim-ic.com.

Ultra-Low-Power, High Dynamic-Performance, 22Msps Analog Front End

Pin Description

PIN	NAME	FUNCTION
1	REFP	Upper Reference Voltage. Bypass with a 0.33µF capacitor to GND as close to REFP as possible.
2, 8, 43	V_{DD}	Analog Supply Voltage. Bypass V_{DD} to GND with a combination of a 2.2µF capacitor in parallel with a 0.1µF capacitor.
3	IA+	Channel IA Positive Analog Input. For single-ended operation, connect signal source to IA+.
4	IA-	Channel IA Negative Analog Input. For single-ended operation, connect IA- to COM.
5, 7, 12, 37, 42	GND	Analog Ground. Connect all pins to GND ground plane.
6	CLK	Conversion Clock Input. Clock signal for both ADCs and DACs.
9	QA-	Channel QA Negative Analog Input. For single-ended operation, connect QA- to COM.
10	QA+	Channel QA Positive Analog Input. For single-ended operation, connect signal source to QA+.
11, 33, 39	V_{DD}	Analog Supply Voltage. Connect to V_{DD} power plane as close to the device as possible.
13–16, 19–22	DA0–DA7	ADC Tri-State Digital Output Bits. DA7 is the most significant bit (MSB), and DA0 is the least significant bit (LSB).
17	OGND	Output Driver Ground
18	OV_{DD}	Output Driver Power Supply. Supply range from +1.8V to V_{DD} to accommodate most logic levels. Bypass OV_{DD} to OGND with a combination of a 2.2µF capacitor in parallel with a 0.1µF capacitor.
23–32	DD0–DD9	DAC Digital Input Bits. DD9 is the MSB, and DD0 is the LSB.
34	DIN	3-Wire Serial Interface Data Input. Data is latched on the rising edge of the SCLK.
35	SCLK	3-Wire Serial Interface Clock Input
36	$\overline{CS}$	3-Wire Serial Interface Chip Select Input. Apply logic low enables the serial interface.
38	N.C.	No Connection
40, 41	QD+, QD-	DAC Channel-QD Differential Voltage Output
44, 45	ID-, ID+	DAC Channel-ID Differential Voltage Output
46	REFIN	Reference Input. Connect to V_{DD} for internal reference.
47	COM	Common-Mode Voltage I/O. Bypass COM to GND with a 0.33µF capacitor.
48	REFN	Negative Reference I/O. Conversion range is $\pm(V_{REFP} - V_{REFN})$. Bypass REFN to GND with a 0.33µF capacitor.
—	EP	Exposed Paddle. Exposed paddle is internally connected to GND. Connect EP to the GND plane.

Ultra-Low-Power, High Dynamic-Performance, 22Msps Analog Front End

Detailed Description

The MAX5864 integrates dual 8-bit receive ADCs and dual 10-bit transmit DACs while providing ultra-low power and highest dynamic performance at a conversion rate of 22Msps. The ADCs' analog input amplifiers are fully differential and accept $1V_{P-P}$ full-scale signals. The DACs' analog outputs are fully differential with ±400mV full-scale output range at 1.4V common mode.

The MAX5864 includes a 3-wire serial interface to control operating modes and power management. The serial interface is SPI™ and MICROWIRE™ compatible. The MAX5864 serial interface selects shutdown, idle, standby, transmit, receive, and transceiver modes.

The MAX5864 can operate in FDD or TDD applications by configuring the device for transmit, receive, or transceiver modes through a 3-wire serial interface. In TDD mode, the digital bus for receive ADC and transmit DAC can be shared to reduce the digital I/O to a single 10-bit parallel multiplexed bus. In FDD mode, the MAX5864 digital I/O can be configured for an 18-bit, parallel multiplexed bus to match the dual 8-bit ADC and dual 10-bit DAC.

The MAX5864 features an internal precision 1.024V bandgap reference is stable over the entire power-supply and temperature ranges.

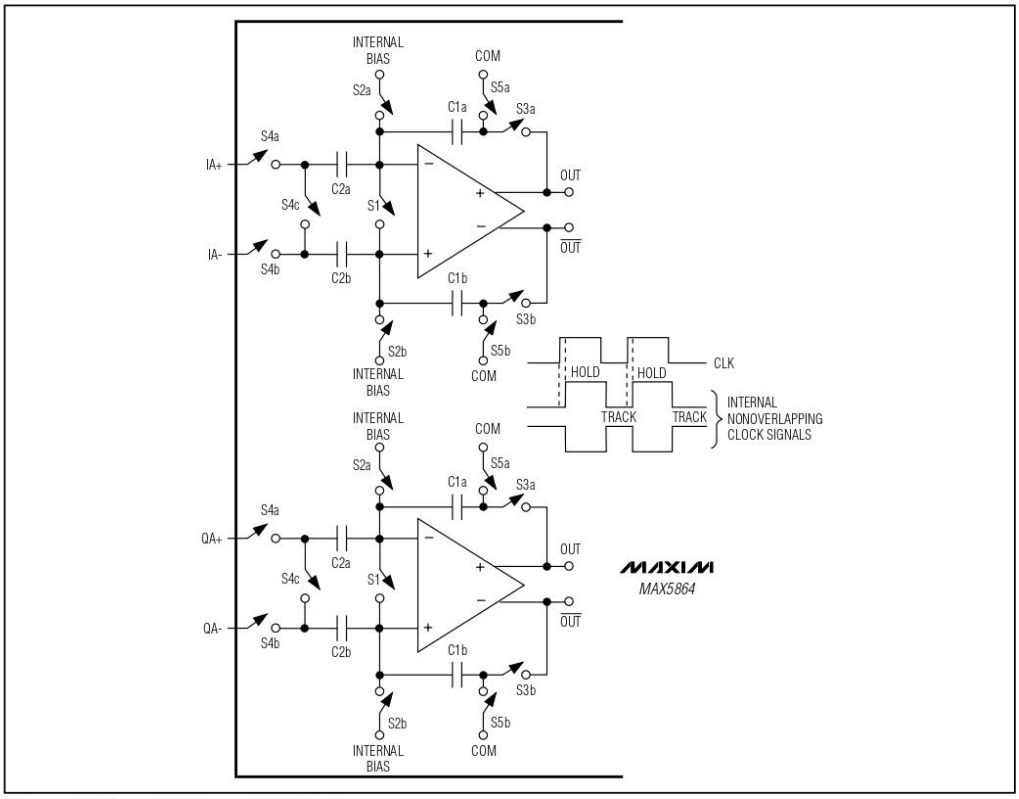


Figure 1. MAX5864 ADC Internal T/H Circuits

SPI is a trademark of Motorola, Inc. MICROWIRE is a trademark of National Semiconductor Corp.

Documentación completa: https://www.analog.com/en/products/max5864.html

Anexo 3 – SI5350 A DATASHEET

SKYWORKS®

Si5350A-B

FACTORY-PROGRAMMABLE ANY-FREQUENCY CMOS CLOCK GENERATOR

Features

- https://www.skyworksinc.com/Products/Timing/CMOS-Clock-Generators
- Generates up to 8 non-integer-related frequencies from 2.5 kHz to 200 MHz
- Exact frequency synthesis at each output (0 ppm error)
- Glitchless frequency changes
- Low output period jitter: < 70 ps pp, typ
- Configurable Spread Spectrum selectable at each output
- User-configurable control pins:
  - Output Enable (OEB_0/1/2)
  - Power Down (PDN)
  - Frequency Select (FS_0/1)
  - Spread Spectrum Enable (SSEN)
- Supports static phase offset
- Rise/fall time control
- Operates from a low-cost, fixed frequency crystal: 25 or 27 MHz
- Separate voltage supply pins provide level translation:
  - Core VDD: 1.8 V, 2.5 V or 3.3 V
  - Output VDDO: 1.8 V, 2.5 V or 3.3 V
- Excellent PSRR eliminates external power supply filtering
- Very low power consumption (25 mA core, typ)
- Available in 3 packages types:
  - 10-MSOP: 3 outputs
  - 16-QFN (3x3 mm): 4 output
  - 20-QFN (4x4 mm): 8 output
- PCIE Gen 1 compatible
- Supports HCSL jitter compatible swing

Applications

- HDTV, DVD/Blu-ray, set-top box
- Audio/video equipment, gaming
- Printers, scanners, projectors
- Handheld instrumentation
- Residential gateways
- Networking/communication
- Servers, storage
- XO replacement

Description

The Si5350A is a highly-flexible, user-definable custom clock generator that is ideally suited for replacing crystals and crystal oscillators in cost-sensitive applications. Based on a PLL + high resolution fractional divider MultiSynth™ architecture, the Si5350A can generate any frequency up to 200 MHz on each of its outputs with 0 ppm error. Spread spectrum is selectable (on/off) on any of the outputs. Custom Si5350A configurations can be created using ClockBuilder Pro.

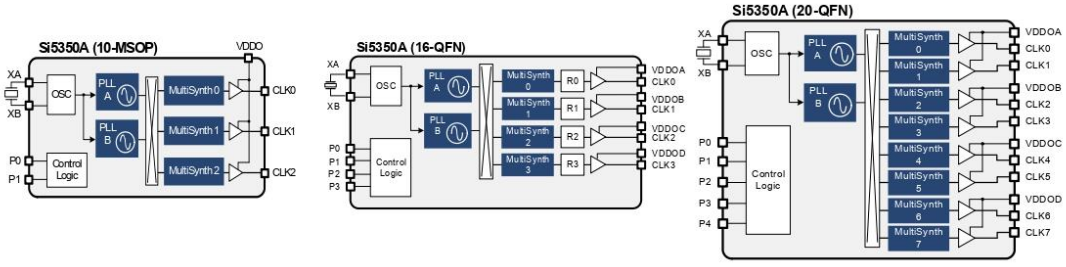
10-MSOP

16-QFN

20-QFN

Ordering Information:
See page 22

Functional Block Diagrams



5. Functional Description

The Si5350A's synthesis architecture consists of two high-frequency PLLs in addition to one high-resolution fractional MultiSynth™ divider per output. Block diagrams of the 3-, 4-, and 8-output versions are shown in Figure 4. This unique architecture allows the Si5350A to simultaneously generate up to eight independent, non-integer-related frequencies. In addition, some MultiSynth™ dividers are configurable with two different frequencies (F1_x, F2_x). This allows a pin-controlled, glitchless frequency change at the corresponding output (CLK0 to CLK2).

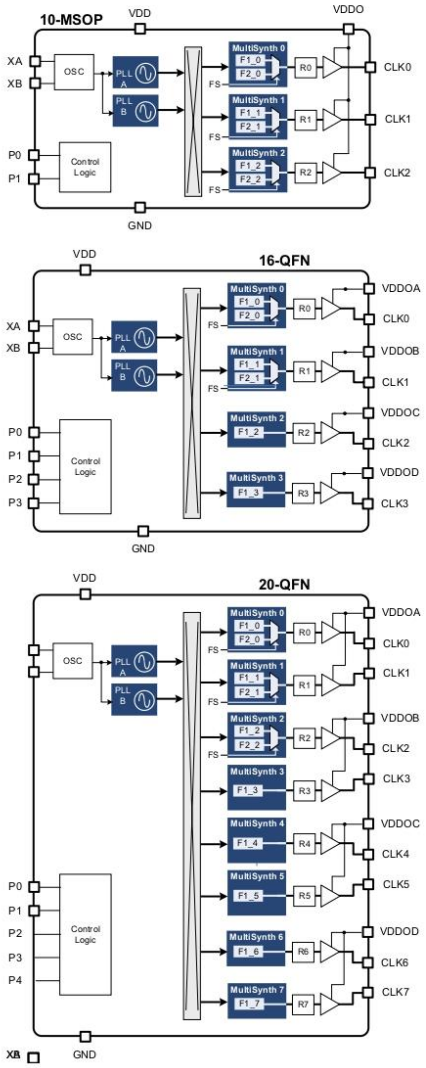


Figure 4. Block Diagrams of 3-Output, 4-Output, and 8-Output Si5350A Devices

7. Pin Descriptions

7.1. 20-Pin QFN

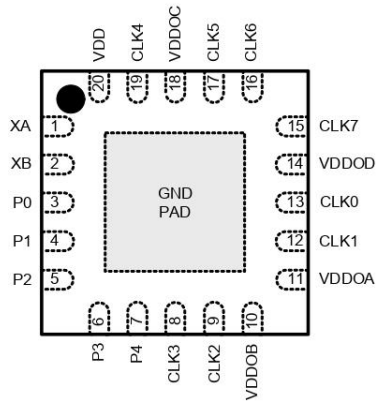


Figure 11. Si5350A 20-Pin QFN Top View

Pin Name	Pin Number	Pin Type*	Function
XA	1	I	Input pin for external XTAL.
XB	2	I	Input pin for external XTAL.
CLK0	13	O	Output Clock 0.
CLK1	12	O	Output Clock 1.
CLK2	9	O	Output Clock 2.
CLK3	8	O	Output Clock 3.
CLK4	19	O	Output Clock 4.
CLK5	17	O	Output Clock 5.
CLK6	16	O	Output Clock 6.
CLK7	15	O	Output Clock 7.
P0	3	I	User configurable input pin 0. See Section 6.3.
P1	4	I	User configurable input pin 1. See Section 6.3.
P2	5	I	User configurable input pin 2. See Section 6.3.
P3	6	I	User configurable input pin 3. See Section 6.3.
P4	7	I	User configurable input pin 4. See Section 6.3.
VDD	20	P	Core voltage supply pin. See Section 6.4.2.
VDDOA	11	P	Output voltage supply pin for CLK0 and CLK1. See Section 6.4.2.
VDDOB	10	P	Output voltage supply pin for CLK2 and CLK3. See Section 6.4.2.
VDDOC	18	P	Output voltage supply pin for CLK4 and CLK5. See Section 6.4.2.
VDDOD	14	P	Output voltage supply pin for CLK6 and CLK7. See Section 6.4.2.
GND	Center Pad	P	Ground.
***Note:** I = Input, O = Output, P = Power			

Documentación completa: https://www.mouser.com/new/skyworks-solutions/skyworks-si5351-clock-generators/

Anexo 4 – LPC4320 DATASHEET

LPC4350/30/20/10

32-bit ARM Cortex-M4/M0 flashless MCU; up to 264 kB SRAM; Ethernet; two HS USBs; advanced configurable peripherals

Rev. 4.6 — 14 March 2016 **Product data sheet**

1. General description

The LPC4350/30/20/10 are ARM Cortex-M4 based microcontrollers for embedded applications which include an ARM Cortex-M0 coprocessor, up to 264 kB of SRAM, advanced configurable peripherals such as the State Configurable Timer/PWM (SCTimer/PWM) and the Serial General-Purpose I/O (SGPIO) interface, two high-speed USB controllers, Ethernet, LCD, an external memory controller, and multiple digital and analog peripherals. The LPC4350/30/20/10 operate at CPU frequencies of up to 204 MHz.

The ARM Cortex-M4 is a 32-bit core that offers system enhancements such as low power consumption, enhanced debug features, and a high level of support block integration. The ARM Cortex-M4 CPU incorporates a 3-stage pipeline, uses a Harvard architecture with separate local instruction and data buses as well as a third bus for peripherals, and includes an internal prefetch unit that supports speculative branching. The ARM Cortex-M4 supports single-cycle digital signal processing and SIMD instructions. A hardware floating-point processor is integrated in the core.

The ARM Cortex-M0 coprocessor is an energy-efficient and easy-to-use 32-bit core which is code- and tool-compatible with the Cortex-M4 core. The Cortex-M0 coprocessor offers up to 204 MHz performance with a simple instruction set and reduced code size. In LPC43x0, the Cortex-M0 coprocessor hardware multiply is implemented as a 32-cycle iterative multiplier.

See Section 17 “References” for additional documentation.

2. Features and benefits

- Cortex-M4 Processor core
  - ARM Cortex-M4 processor, running at frequencies of up to 204 MHz.
  - Built-in Memory Protection Unit (MPU) supporting eight regions.
  - Built-in Nested Vectored Interrupt Controller (NVIC).
  - Hardware floating-point unit.
  - Non-maskable Interrupt (NMI) input.
  - JTAG and Serial Wire Debug (SWD), serial trace, eight breakpoints, and four watch points.
  - Enhanced Trace Module (ETM) and Enhanced Trace Buffer (ETB) support.
  - System tick timer.

- Cortex-M0 Processor core
  - ARM Cortex-M0 co-processor capable of off-loading the main ARM Cortex-M4 application processor.
  - Running at frequencies of up to 204 MHz.
  - JTAG and built-in NVIC.
- On-chip memory
  - Up to 264 kB SRAM for code and data use.
  - Multiple SRAM blocks with separate bus access. Two SRAM blocks can be powered down individually.
  - 64 kB ROM containing boot code and on-chip software drivers.
  - 64 bit + 256 bit general-purpose One-Time Programmable (OTP) memory.
- Clock generation unit
  - Crystal oscillator with an operating range of 1 MHz to 25 MHz.
  - 12 MHz Internal RC (IRC) oscillator trimmed to 1.5 % accuracy over temperature and voltage.
  - Ultra-low power Real-Time Clock (RTC) crystal oscillator.
  - Three PLLs allow CPU operation up to the maximum CPU rate without the need for a high-frequency crystal. The second PLL is dedicated to the High-speed USB, the third PLL can be used as audio PLL.
  - Clock output.
- Configurable digital peripherals
  - Serial GPIO (SGPIO) interface.
  - State Configurable Timer (SCTimer/PWM) subsystem on AHB.
  - Global Input Multiplexer Array (GIMA) allows to cross-connect multiple inputs and outputs to event driven peripherals like the timers, SCTimer/PWM, and ADC0/1.
- Serial interfaces
  - Quad SPI Flash Interface (SPIFI) with 1-, 2-, or 4-bit data at rates of up to 52 MB per second.
  - 10/100T Ethernet MAC with RMII and MII interfaces and DMA support for high throughput at low CPU load. Support for IEEE 1588 time stamping/advanced time stamping (IEEE 1588-2008 v2).
  - One High-speed USB 2.0 Host/Device/OTG interface with DMA support and on-chip high-speed PHY (USB0).
  - One High-speed USB 2.0 Host/Device interface with DMA support, on-chip full-speed PHY and ULPI interface to external high-speed PHY (USB1).
  - USB interface electrical test software included in ROM USB stack.
  - Four 550 UARTs with DMA support: one UART with full modem interface; one UART with IrDA interface; three USARTs support UART synchronous mode and a smart card interface conforming to ISO7816 specification.
  - Up to two C_CAN 2.0B controllers with one channel each. Use of C_CAN controller excludes operation of all other peripherals connected to the same bus bridge. See Figure 1 and Ref. 2.
  - Two SSP controllers with FIFO and multi-protocol support. Both SSPs with DMA support.
  - One SPI controller.

- One Fast-mode Plus I^2C-bus interface with monitor mode and with open-drain I/O pins conforming to the full I^2C-bus specification. Supports data rates of up to 1 Mbit/s.
- One standard I^2C-bus interface with monitor mode and with standard I/O pins.
- Two I^2S interfaces, each with DMA support and with one input and one output.

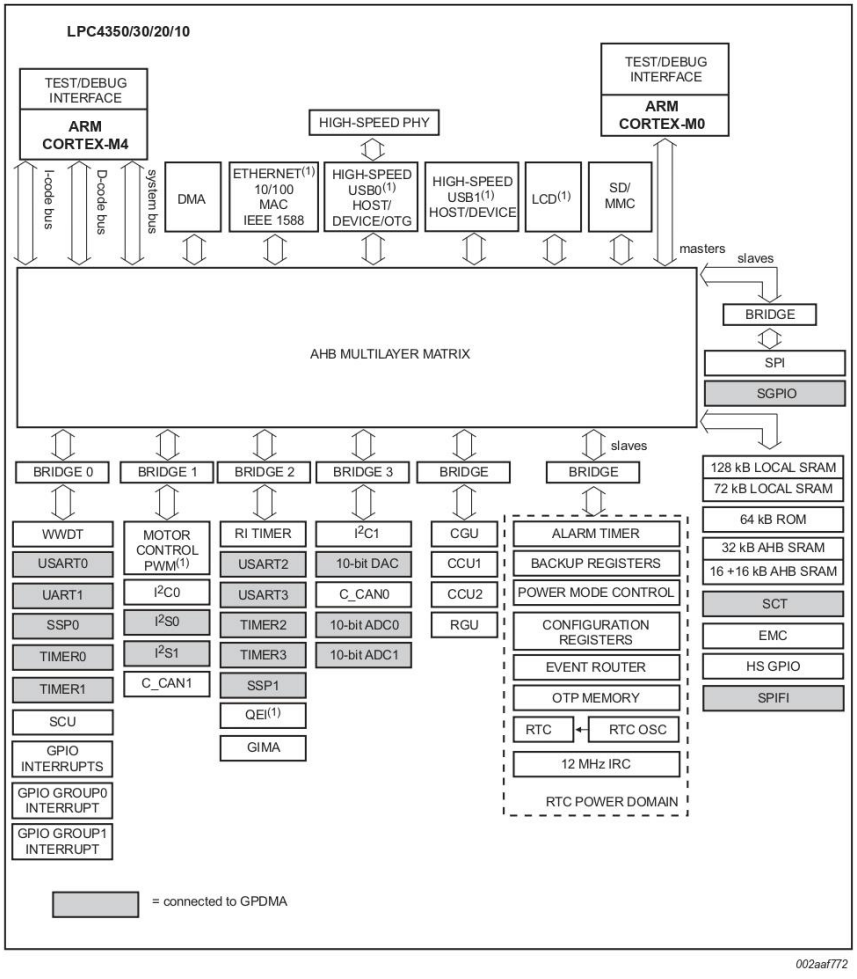
- Digital peripherals
  - External Memory Controller (EMC) supporting external SRAM, ROM, NOR flash, and SDRAM devices.
  - LCD controller with DMA support and a programmable display resolution of up to 1024 H × 768 V. Supports monochrome and color STN panels and TFT color panels; supports 1/2/4/8 bpp Color Look-Up Table (CLUT) and 16/24-bit direct pixel mapping.
  - Secure Digital Input Output (SD/MMC) card interface.
  - Eight-channel General-Purpose DMA controller can access all memories on the AHB and all DMA-capable AHB slaves.
  - Up to 164 General-Purpose Input/Output (GPIO) pins with configurable pull-up/pull-down resistors.
  - GPIO registers are located on the AHB for fast access. GPIO ports have DMA support.
  - Up to eight GPIO pins can be selected from all GPIO pins as edge and level sensitive interrupt sources.
  - Two GPIO group interrupt modules enable an interrupt based on a programmable pattern of input states of a group of GPIO pins.
  - Four general-purpose timer/counters with capture and match capabilities.
  - One motor control Pulse Width Modulator (PWM) for three-phase motor control.
  - One Quadrature Encoder Interface (QEI).
  - Repetitive Interrupt timer (RI timer).
  - Windowed watchdog timer (WWDT).
  - Ultra-low power Real-Time Clock (RTC) on separate power domain with 256 bytes of battery powered backup registers.
  - Alarm timer; can be battery powered.
- Analog peripherals
  - One 10-bit DAC with DMA support and a data conversion rate of 400 kSamples/s.
  - Two 10-bit ADCs with DMA support and a data conversion rate of 400 kSamples/s. Up to eight input channels per ADC.
- Unique ID for each device.
- Power
  - Single 3.3 V (2.2 V to 3.6 V) power supply with on-chip internal voltage regulator for the core supply and the RTC power domain.
  - RTC power domain can be powered separately by a 3 V battery supply.
  - Four reduced power modes: Sleep, Deep-sleep, Power-down, and Deep power-down.
  - Processor wake-up from Sleep mode via wake-up interrupts from various peripherals.
  - Wake-up from Deep-sleep, Power-down, and Deep power-down modes via external interrupts and interrupts generated by battery powered blocks in the RTC power domain.

- Brownout detect with four separate thresholds for interrupt and forced reset.
- Power-On Reset (POR).
- Available as LBGA256, TFBGA180, and TFBGA100 packages and as LQFP144 package.

3. Applications

- Motor control
- Power management
- White goods
- RFID readers
- Embedded audio applications
- Industrial automation
- e-metering

5. Block diagram



(1) Not available on all parts (see Table 2).

Fig 1. LPC4350/30/20/10 Block diagram

Documentación completa: https://www.nxp.com/part/LPC4320FBD144

Anexo 5 – RFFC5072 DATASHEET

rfmd

RFFC5071/5072

WIDEBAND SYNTHESIZER/VCO WITH INTEGRATED 6GHz MIXER

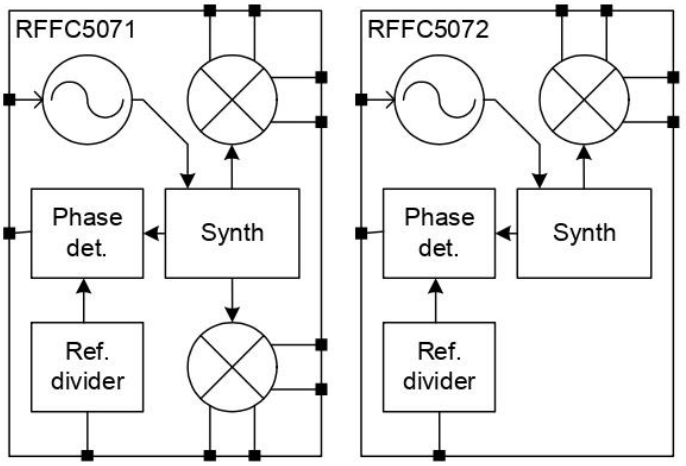
Package: QFN, 32-Pin, 5mm x 5mm

Features

- 85MHz to 4200MHz LO Frequency Range
- Fractional-N Synthesizer with Very Low Spurious Levels
- Typical Step Size 1.5Hz
- Fully Integrated Low Phase Noise VCO and LO Buffers
- Integrated Phase Noise
  - 0.18° rms at 1GHz
  - 0.50° rms at 3GHz
- High Linearity RF Mixer(s)
- 30MHz to 6000MHz Mixer Frequency Range
- Input IP3 +23dBm
- Mixer Bias Adjustable for Low Power Operation
- Full Duplex Mode (RFFC5071)
- 2.7V to 3.3V Power Supply
- Low Current Consumption
- 3- or 4-Wire Serial Interface

Applications

- Wideband Radios
- Distributed Antenna Systems
- Diversity Receivers
- Software Defined Radios
- Frequency Band Shifters
- Point-to-Point Radios
- WiMax/LTE Infrastructure
- Satellite Communications
- Wideband Jammers



Functional Block Diagram

Product Description

The RFFC5071 and RFFC5072 are re-configurable frequency conversion devices with integrated fractional-N phased locked loop (PLL) synthesizer, voltage controlled oscillator (VCO) and either one or two high linearity mixers. The fractional-N synthesizer takes advantage of an advanced sigma-delta modulator that delivers ultra-fine step sizes and low spurious products. The PLL/VCO engine combined with an external loop filter allows the user to generate local oscillator (LO) signals from 85MHz to 4200MHz. The LO signal is buffered and routed to the integrated RF mixers which are used to up/down-convert frequencies ranging from 30MHz to 6000MHz. The mixer bias current is programmable and can be reduced for applications requiring lower power consumption. Both devices can be configured to work as signal sources by bypassing the integrated mixers. Device programming is achieved via a simple 3-wire serial interface. In addition, a unique programming mode allows up to four devices to be controlled from a common serial bus. This eliminates the need for separate chip-select control lines between each device and the host controller. Up to six general purpose outputs are provided, which can be used to access internal signals (the LOCK signal, for example) or to control front end components. Both devices operate with a 2.7V to 3.3V power supply.

Optimum Technology Matching® Applied

☐ GaAs HBT	☐ SiGe BiCMOS	☐ GaAs pHEMT	☐ GaN HEMT
☐ GaAs MESFET	☐ Si BiCMOS	☑ Si CMOS	☐ BiFET HBT
☐ InGaP HBT	☐ SiGe HBT	☐ Si BJT	☐ LDMOS

7628 Thorndike Road, Greensboro, NC 27409-9421 · For sales or technical support, contact RFMD at (+1) 336-678-5570 or customerservice@rfmd.com.

Pin Names and Descriptions

Pin	Name	Description
1	ENBL/GPO5	Device Enable pin (see note 1 and 2).
2	EXT_LO	External local oscillator input (See note 4).
3	EXT_LO_DEC	Decoupling pin for external local oscillator (See note 4).
4	REXT	External bandgap bias resistor (See note 3).
5	ANA_VDD1	Analog supply. Use good RF decoupling.
6	LFILT1	Phase detector output. Low-frequency noise-sensitive node.
7	LFILT2	Loop filter op-amp output. Low-frequency noise-sensitive node.
8	LFILT3	VCO control input. Low-frequency noise-sensitive node.
9	MODE/GPO6	Mode select pin (See note 1 and 2).
10	REF_IN	Reference input. Use AC coupling capacitor.
11	NC	
12	TM	Connect to ground.
13	MIX1_IPN	Differential input 1 (see note 4). On RFFC5072 this pin is NC.
14	MIX1_IPP	Differential input 1 (see note 4). On RFFC5072 this pin is NC.
15	GPO1/ADD1	General purpose output / MultiSlice address bit.
16	GPO2/ADD2	General purpose output / MultiSlice address bit.
17	MIX1_OPN	Differential output 1 (see note 5). On RFFC5072 this pin is NC.
18	MIX1_OPP	Differential output 1 (see note 5). On RFFC5072 this pin is NC.
19	DIG_VDD	Digital supply. Should be decoupled as close to the pin as possible.
20	NC	
21	NC	
22	ANA_VDD2	Analog supply. Use good RF decoupling.
23	MIX2_IPP	Differential input 2 (see note 4).
24	MIX2_IPN	Differential input 2 (see note 4).
25	GPO3/FM	General purpose output / frequency control input.
26	GPO4/LD/DO	General purpose output / Lock detect output / serial data out.
27	MIX2_OPN	Differential output 2. (see note 5).
28	MIX2_OPP	Differential output 2. (see note 5).
29	RESETX	Chip reset (active low). Connect to DIG_VDD if asynchronous reset is not required.
30	ENX	Serial interface select (active low) (See note 1).
31	SCLK	Serial interface clock (see note 1).
32	SDATA	Serial interface data (see note 1).
Exposed paddle		Ground reference, should be connected to PCB ground through a low impedance path.

Note 1: An RC low-pass filter could be used on this line to reduce digital noise.

Note 2: If the device is under software control this input can be configured as a general purpose output (GPO).

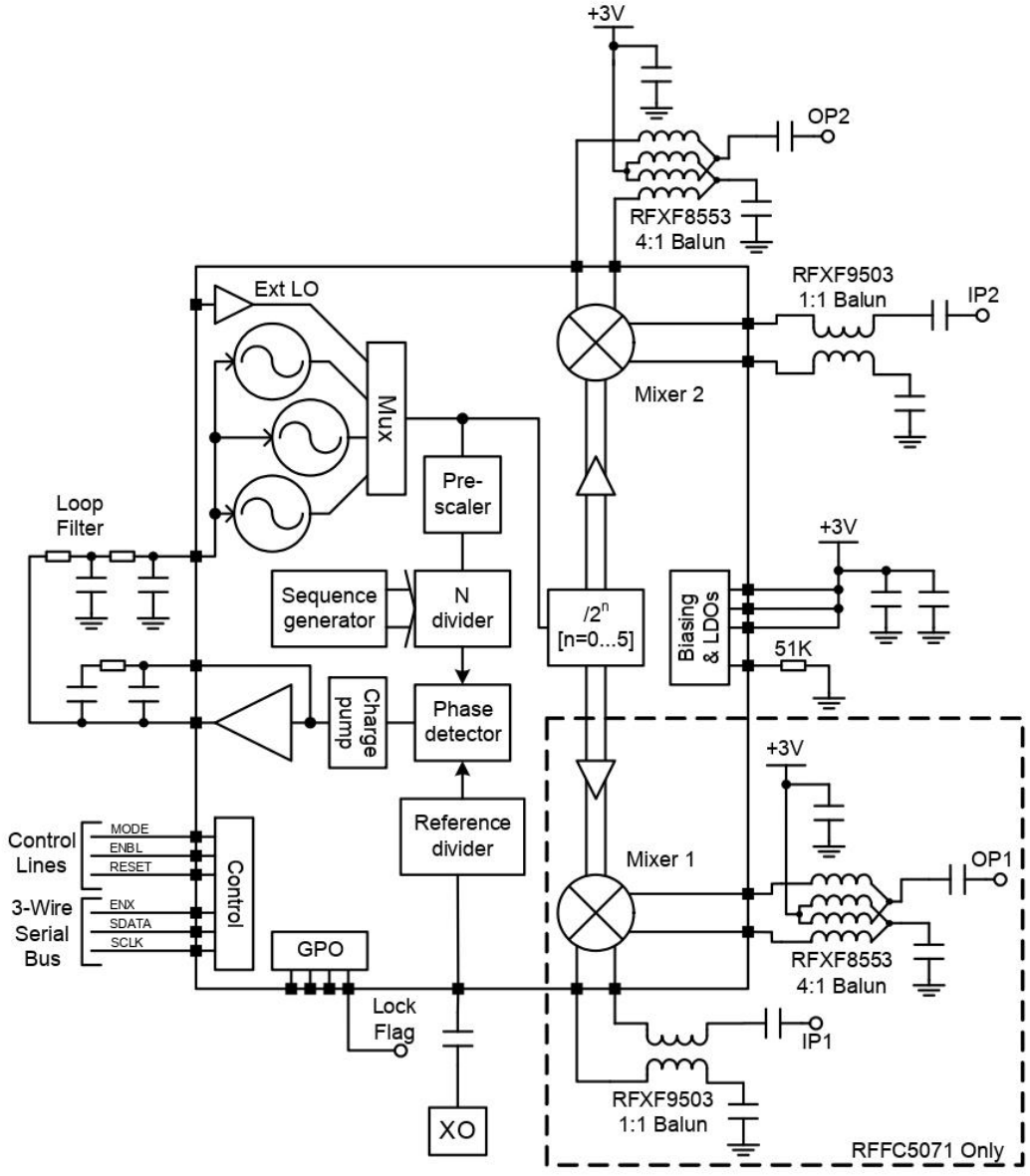
Note 3: Connect a 51KΩ resistor from this pin to ground. This pin is sensitive to low frequency noise injection.

Note 4: DC voltage should not be applied to this pin. Use either an AC coupling capacitor as part of lumped element matching network or a transformer (see application schematic).

Note 5: This pin must be connected to ANA_VDD2 using an RF choke or transformer (see application schematic).

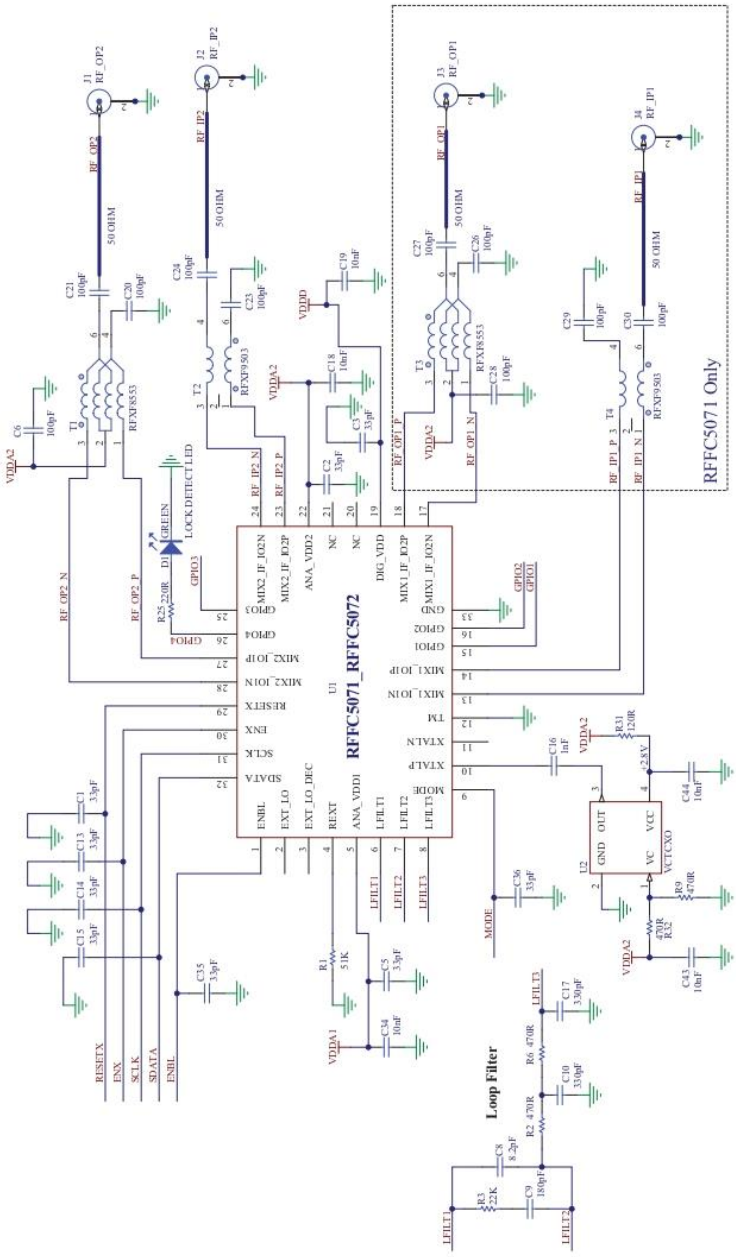
7628 Thorndike Road, Greensboro, NC 27409-9421 · For sales or technical support, contact RFMD at (+1) 336-678-5570 or customerservice@rfmd.com.

Detailed Functional Block Diagram

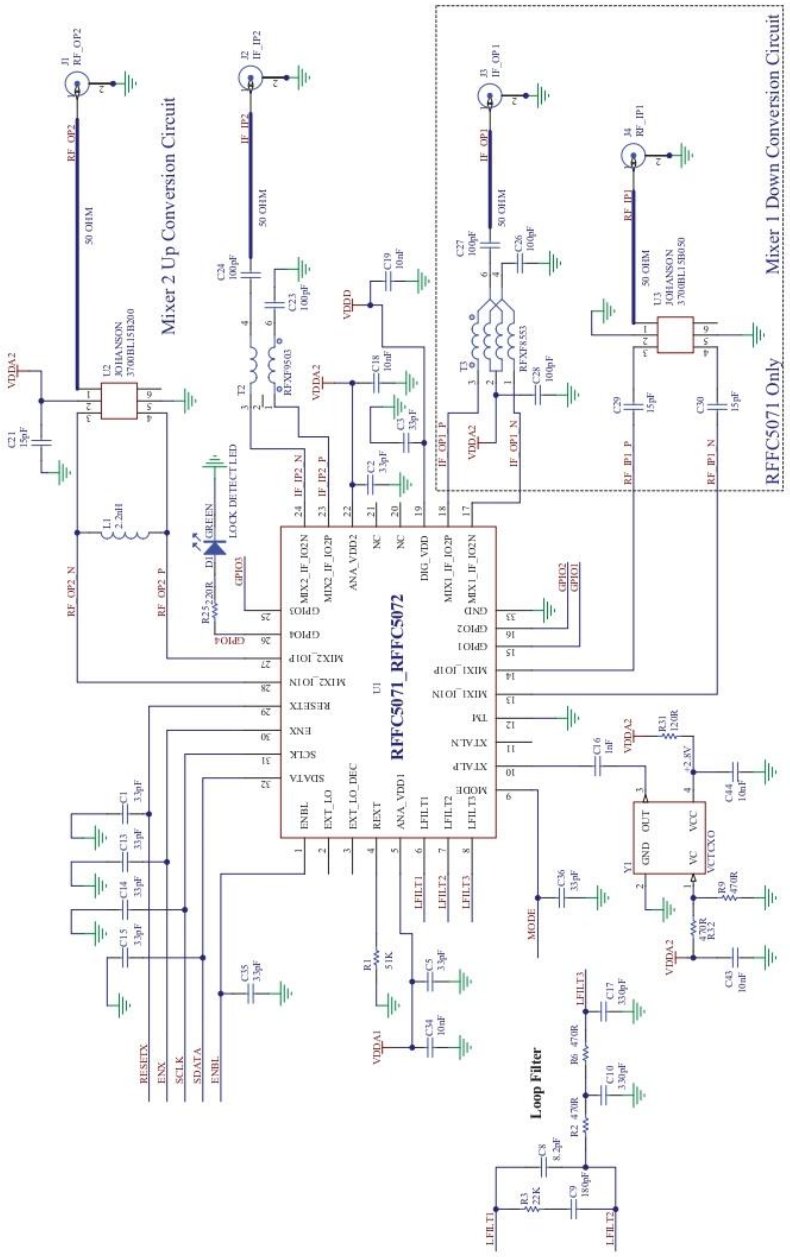


Note: Wideband transmission line transformer baluns shown above for operation to ~2.5GHz. Substitute baluns for higher frequency applications as required.

Wideband Application Schematic (<2.5GHz)



Narrowband 3.7GHz Application Schematic



7628 Thorndike Road, Greensboro, NC 27409-9421 · For sales or technical support, contact RFMD at (+1) 336-678-5570 or customerservice@rfmd.com.

Documentación completa: https://www.qorvo.com/products/p/RFFC5072

Anexo 6 – W25Q80BV DATASHEET

winbond

1. GENERAL DESCRIPTION

The W25Q80BV (8M-bit) Serial Flash memory provides a storage solution for systems with limited space, pins and power. The 25Q series offers flexibility and performance well beyond ordinary Serial Flash devices. They are ideal for code shadowing to RAM, executing code directly from Dual/Quad SPI (XIP) and storing voice, text and data. The device operates on a single 2.5V to 3.6V power supply with current consumption as low as 4mA active and 1µA for power-down.

The W25Q80BV array is organized into 4,096 programmable pages of 256-bytes each. Up to 256 bytes can be programmed at a time. Pages can be erased in groups of 16 (4KB sector erase), groups of 128 (32KB block erase), groups of 256 (64KB block erase) or the entire chip (chip erase). The W25Q80BV has 256 erasable sectors and 16 erasable blocks respectively. The small 4KB sectors allow for greater flexibility in applications that require data and parameter storage. (See figure 2.)

The W25Q80BV supports the standard Serial Peripheral Interface (SPI), and a high performance Dual/Quad output as well as Dual/Quad I/O SPI: Serial Clock, Chip Select, Serial Data I/O0 (DI), I/O1 (DO), I/O2 (/WP), and I/O3 (/HOLD). SPI clock frequencies of up to 104MHz are supported allowing equivalent clock rates of 208MHz (104MHz x 2) for Dual I/O and 416MHz (104MHz x 4) for Quad I/O when using the Fast Read Dual/Quad I/O instructions. These transfer rates can outperform standard Asynchronous 8 and 16-bit Parallel Flash memories. The Continuous Read Mode allows for efficient memory access with as few as 8-clocks of instruction-overhead to read a 24-bit address, allowing true XIP (execute in place) operation.

A Hold pin, Write Protect pin and programmable write protection, with top, bottom or complement array control, provide further control flexibility. Additionally, the device supports JEDEC standard manufacturer and device identification with a 64-bit Unique Serial Number.

2. FEATURES

- **Family of SpiFlash Memories**
  - W25Q80BV: 8M-bit/1M-byte (1,048,576)
  - 256-byte per programmable page
  - Standard SPI: CLK, /CS, DI, DO, /WP, /Hold
  - Dual SPI: CLK, /CS, IO_0, IO_1, /WP, /Hold
  - Quad SPI: CLK, /CS, IO_0, IO_1, IO_2, IO_3
- **Highest Performance Serial Flash**
  - 104MHz Dual/Quad SPI clocks
  - 208/416MHz equivalent Dual/Quad SPI
  - 50MB/S continuous data transfer rate
  - Up to 8X that of ordinary Serial Flash
  - More than 100,000 erase/program cycles(1)
  - More than 20-year data retention
- **Efficient "Continuous Read Mode"**
  - Low Instruction overhead
  - Continuous Read with 8/16/32/64-Byte Wrap
  - As few as 8 clocks to address memory
  - Allows true XIP (execute in place) operation
  - Outperforms X16 Parallel Flash
- **Low Power, Wide Temperature Range**
  - Single 2.5 to 3.6V supply
  - 4mA active current, <1µA Power-down current
  - -40°C to +85°C operating range
- **Flexible Architecture with 4KB sectors**
  - Uniform Sector/Block Erase (4/32/64K-bytes)
  - Program one to 256 bytes
  - Erase/Program Suspend & Resume
- **Advanced Security Features**
  - Software and Hardware Write-Protect
  - Top/Bottom, 4KB complement array protection
  - Lock-Down and OTP array protection
  - 64-Bit Unique Serial Number for each device
  - Discoverable Parameters (SFDP) Register
  - 3X256-Byte Security Registers with OTP locks
  - Volatile & Non-volatile Status Register Bits
- **Space Efficient Packaging(1)**
  - 8-pin SOIC 150/208-mil
  - 8-pad USON 2x3-mm
  - 8-pad WSON 6x5-mm
  - 8-pin PDIP 300-mil
  - Contact Winbond for KGD and other options

Note 1. Some package types are special orders, please contact Winbond for ordering information.

3. PACKAGE TYPES AND PIN CONFIGURATIONS

W25Q80BV is offered in an 8-pin SOIC 150-mil or 208-mil (package code SN & SS), an 8-pin , an 8-pad WSON 6x5-mm (package code ZP), an 8-pad USON 2x3-mm (package code UX),and an 8-pin PDIP 300-mil (package code DA) as shown in Figure 1a-d respectively. Package diagrams and dimensions are illustrated at the end of this datasheet.

3.1 Pin Configuration SOIC 150 / 208-mil

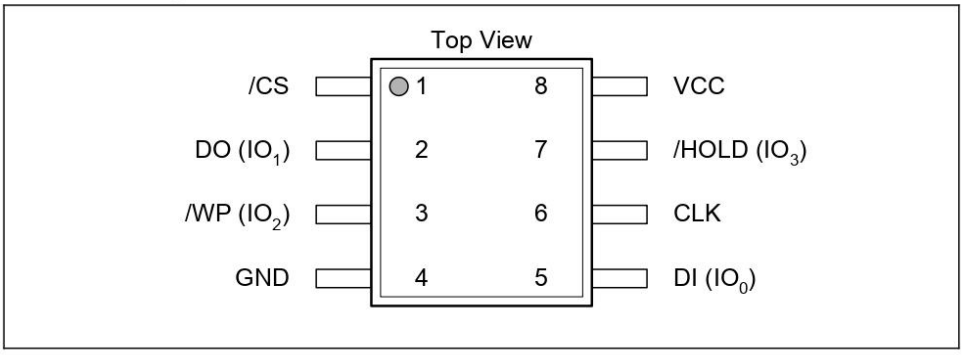


Figure 1a. W25Q80BV Pin Assignments, 8-pin SOIC 150 / 208-mil (Package Code SN, SS, SV, ST)

3.2 Pad Configuration WSON 6x5-mm / USON 2x3-mm

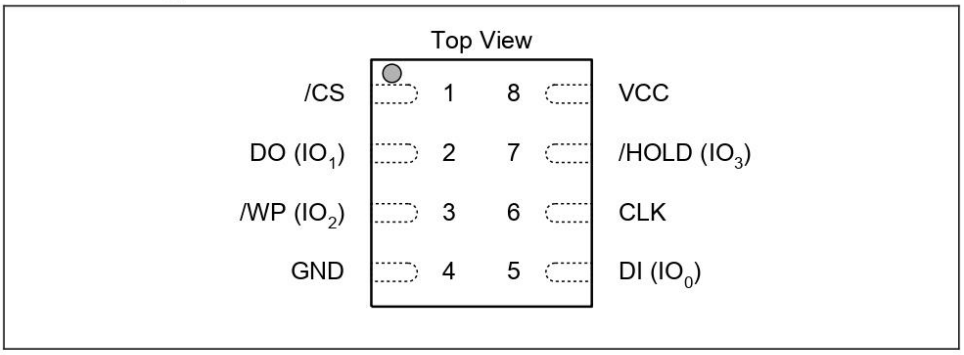


Figure 1b. W25Q80BV Pad Assignments, 8-pad WSON 6x5-mm, USON 2x3-mm (Package Code ZP, UX)

3.3 Pin Configuration PDIP 300-mil

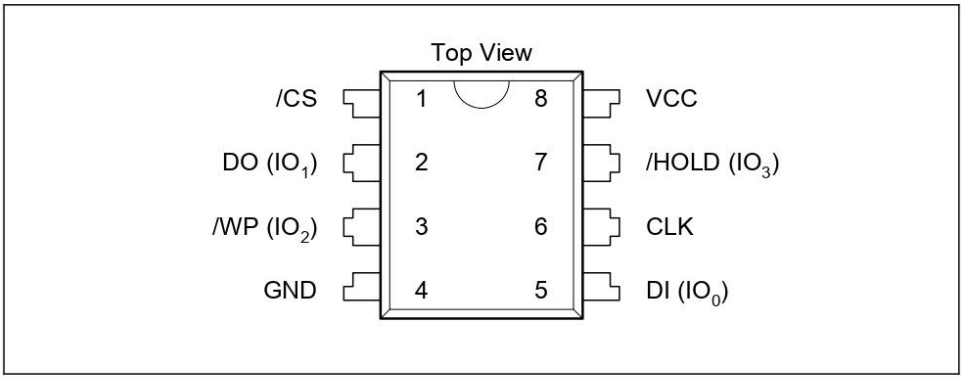


Figure 1c. W25Q80BV Pin Assignments, 8-pin PDIP (Package Code DA)

3.4 Pin Description SOIC, WSON, USON & PDIP 300-mil

PIN NO.	PIN NAME	I/O	FUNCTION
1	/CS	I	Chip Select Input
2	DO (IO1)	I/O	Data Output (Data Input Output 1)*1
3	/WP (IO2)	I/O	Write Protect Input (Data Input Output 2)*2
4	GND		Ground
5	DI (IO0)	I/O	Data Input (Data Input Output 0)*1
6	CLK	I	Serial Clock Input
7	/HOLD (IO3)	I/O	Hold Input (Data Input Output 3)*2
8	VCC		Power Supply

*1 IO0 and IO1 are used for Standard and Dual SPI instructions

*2 IO0 – IO3 are used for Quad SPI instructions

3.5 pin descriptions

3.6 Chip Select (/CS)

The SPI Chip Select (/CS) pin enables and disables device operation. When /CS is high the device is deselected and the Serial Data Output (DO, or IO0, IO1, IO2, IO3) pins are at high impedance. When deselected, the devices power consumption will be at standby levels unless an internal erase, program or write status register cycle is in progress. When /CS is brought low the device will be selected, power consumption will increase to active levels and instructions can be written to and data read from the device. After power-up, /CS must transition from high to low before a new instruction will be accepted. The /CS input must track the VCC supply level at power-up (see “Write Protection” and figure 38). If needed a pull-up resister on /CS can be used to accomplish this.

3.7 Serial Data Input, Output and IOs (DI, DO and IO0, IO1, IO2, IO3)

The W25Q80BV supports standard SPI, Dual SPI and Quad SPI operation. Standard SPI instructions use the unidirectional DI (input) pin to serially write instructions, addresses or data to the device on the rising edge of the Serial Clock (CLK) input pin. Standard SPI also uses the unidirectional DO (output) to read data or status from the device on the falling edge of CLK.

Dual and Quad SPI instructions use the bidirectional IO pins to serially write instructions, addresses or data to the device on the rising edge of CLK and read data or status from the device on the falling edge of CLK. Quad SPI instructions require the non-volatile Quad Enable bit (QE) in Status Register-2 to be set. When QE=1, the /WP pin becomes IO2 and /HOLD pin becomes IO3.

3.8 Write Protect (/WP)

The Write Protect (/WP) pin can be used to prevent the Status Register from being written. Used in conjunction with the Status Register’s Block Protect (CMP, SEC, TB, BP2, BP1 and BP0) bits and Status Register Protect (SRP) bits, a portion as small as a 4KB sector or the entire memory array can be hardware protected. The /WP pin is active low. When the QE bit of Status Register-2 is set for Quad I/O, the /WP pin function is not available since this pin is used for IO2. See figure 1a-c for the pin configuration of Quad I/O operation.

3.9 HOLD (/HOLD)

The /HOLD pin allows the device to be paused while it is actively selected. When /HOLD is brought low, while /CS is low, the DO pin will be at high impedance and signals on the DI and CLK pins will be ignored (don’t care). When /HOLD is brought high, device operation can resume. The /HOLD function can be useful when multiple devices are sharing the same SPI signals. The /HOLD pin is active low. When the QE bit of Status Register-2 is set for Quad I/O, the /HOLD pin function is not available since this pin is used for IO3. See figure 1a-c for the pin configuration of Quad I/O operation.

3.10 Serial Clock (CLK)

The SPI Serial Clock Input (CLK) pin provides the timing for serial input and output operations. ("See SPI Operations")

winbond

4. BLOCK DIAGRAM

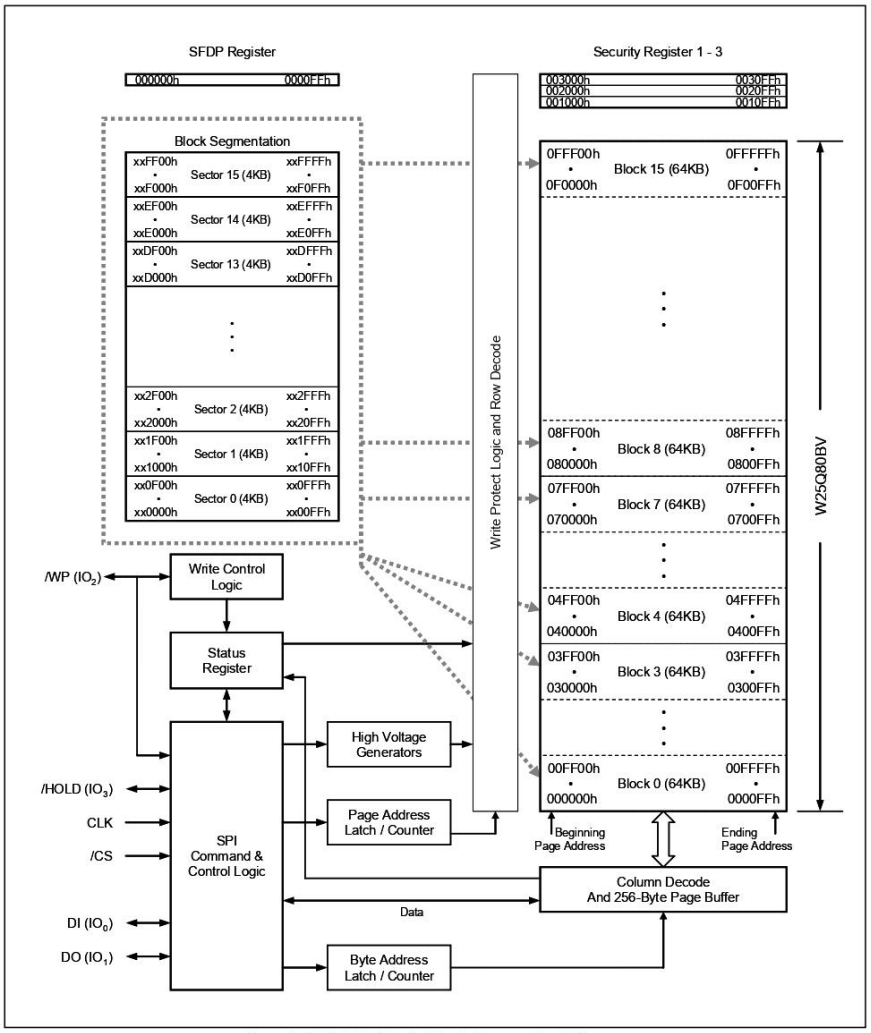
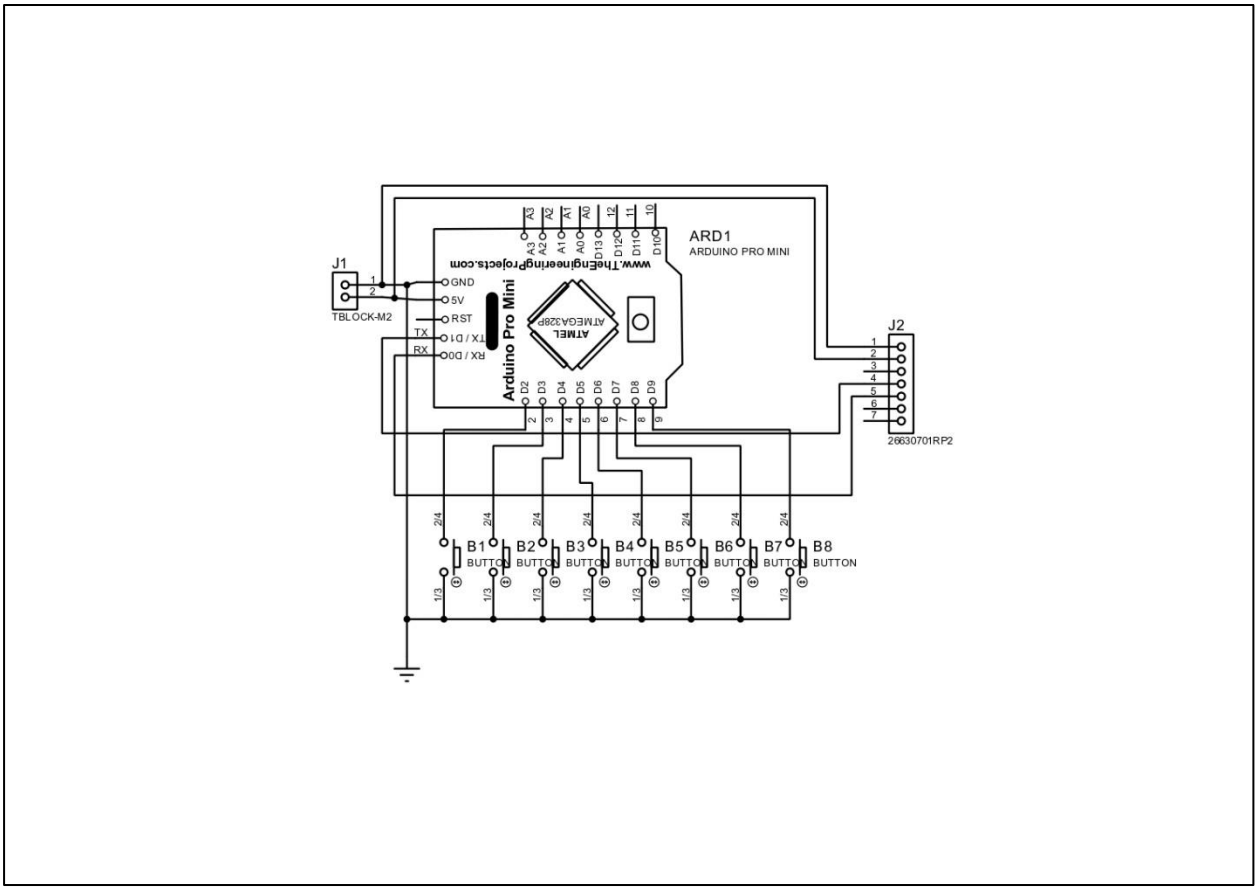


Figure 2. W25Q80BV Serial Flash Memory Block Diagram

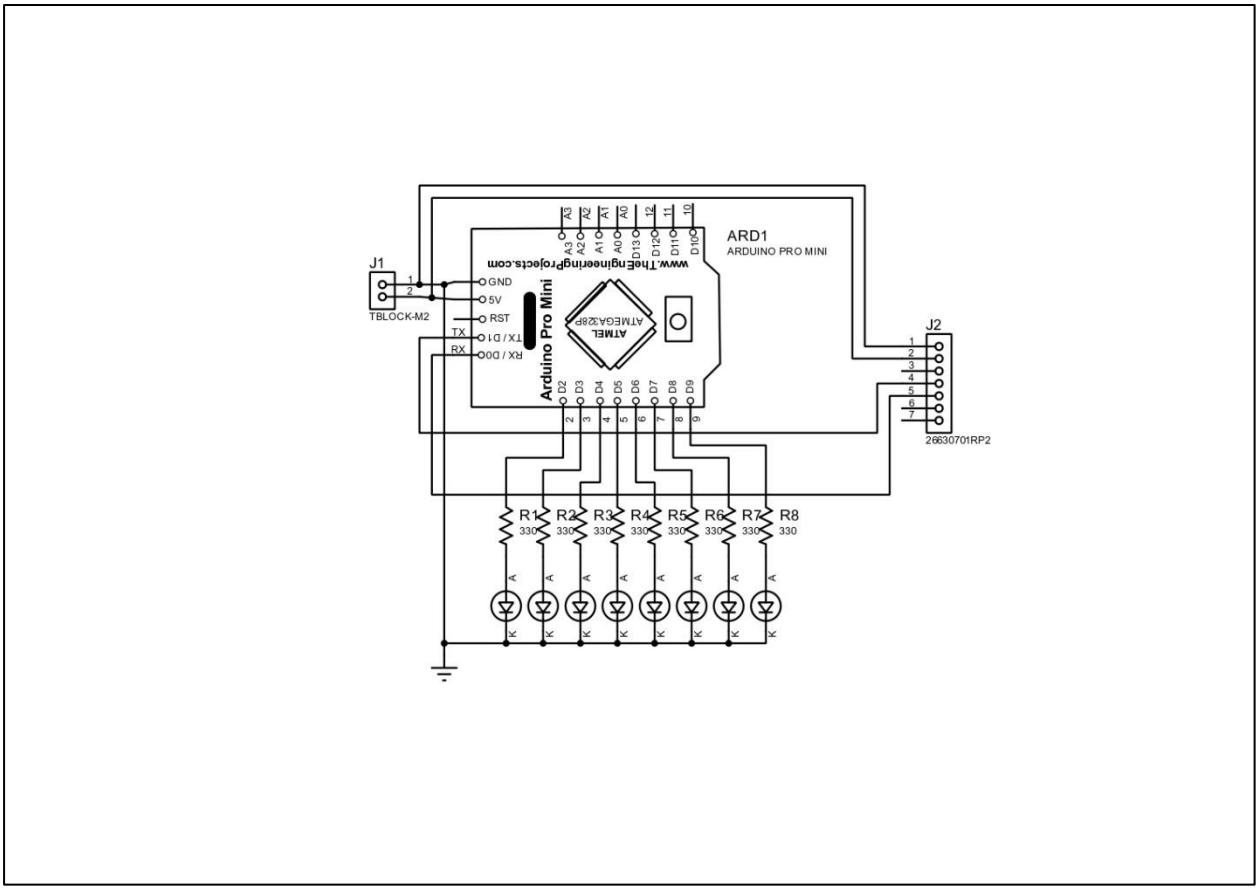
Documentación completa:

https://www.winbond.com/hq/support/documentation/levelOne.jsp?__locale=en&DocNo=DA00-W25Q80BV

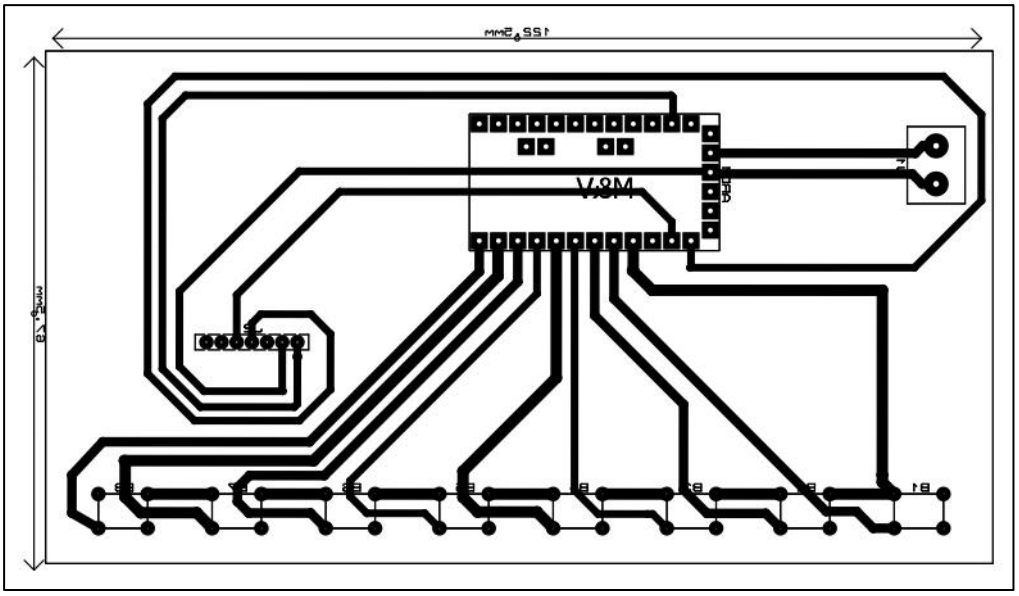
Anexo 7 – Diseño esquemático del nodo CLIENTE



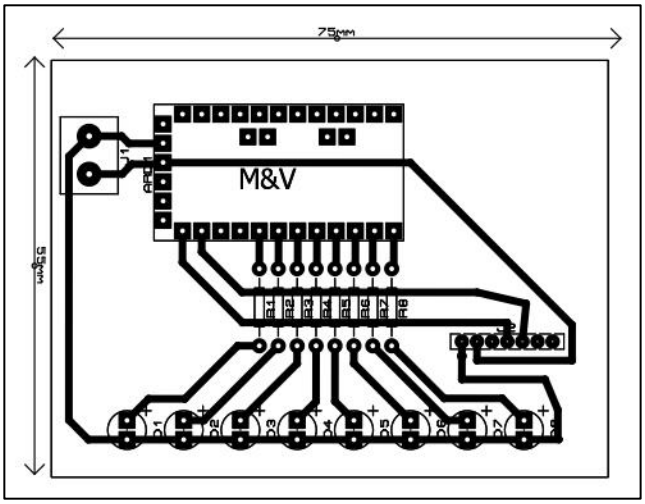
Anexo 8 – Diseño esquemático del nodo SERVIDOR



Anexo 9 – Diseño PCB del nodo CLIENTE



Anexo 10 – Diseño PCB del nodo SERVIDOR



Anexo 11 – Código de programación para el nodo CLIENTE (transmisor)

```
//declaración de variables
int  pul2 = 0;
int  pul3 = 0;
int  pul4 = 0;
int  pul5 = 0;
int  pul6 = 0;
int  pul7 = 0;
int  pul8 = 0;
int  pul9 = 0;
int estado2 = 0;
int estado3 = 0;
int estado4 = 0;
int estado5 = 0;
int estado6 = 0;
int estado7 = 0;
int estado8 = 0;
int estado9 = 0;

void setup()
{
Serial.begin(9600);//Velocidad del puerto serial
pinMode(2, INPUT_PULLUP);
pinMode(3, INPUT_PULLUP);
pinMode(4, INPUT_PULLUP);
pinMode(5, INPUT_PULLUP);
pinMode(6, INPUT_PULLUP);
pinMode(7, INPUT_PULLUP);
pinMode(8, INPUT_PULLUP);
pinMode(9, INPUT_PULLUP);
}

void loop() {
//Lectura de botones
pul2 = digitalRead(2);
pul3 = digitalRead(3);
pul4 = digitalRead(4);
pul5 = digitalRead(5);
pul6 = digitalRead(6);
pul7 = digitalRead(7);
pul8 = digitalRead(8);
pul9 = digitalRead(9);

//Enciende o apaga la luz
if (pul2 == LOW) {//Si el pulsador 2 está precionado se cumple esta condición
pul2 = digitalRead(2);//Leemos el estado del botón nuevamente
if(estado2 ==0){//Si la variable estado2 es igual a 0 se cumple esta condición
Serial.print("luz2on");// Enviamos esta cadena de caracteres x el puerto serial para encender la luz
estado2 =1;//Asignamos el valor 1 a la variable "estado2"
} else{
 Serial.print("luz2off");//Enviamos esta cadena para apagar la luz
 estado2 =0;
  }
while(pul2 == LOW){
pul2 = digitalRead(2);//Se cumple esta condición mientras esté precionado el botón
    }
  }
//-----------------------------------------------------------------------------
//Enciende o apaga la luz
if (pul3 == LOW) {//Si el pulsador 3 está precionado se cumple esta condición
pul3 = digitalRead(3);//Leemos el estado del botón nuevamente
if(estado3 ==0){//Si la variable estado3 es igual a 0 se cumple esta condición
```

```
  Serial.print("luz3on");// Enviamos esta cadena de caracteres x el puerto serial para encender la luz
  estado3 =1;//Asignamos el valor 1 a la variable "estado3"
  } else{
   Serial.print("luz3off");//Enviamos esta cadena para apagar la luz
   estado3 =0;
    }
  while(pul3 == LOW){
  pul3 = digitalRead(3);//Se cumple esta condición mientras esté precionado el botón
      }
    }
  //-------------------------------------------------------------------------------
  //Enciende o apaga la luz
  if (pul4 == LOW) {//Si el pulsador 4 está precionado se cumple esta condición
  pul4 = digitalRead(4);//Leemos el estado del botón nuevamente
  if(estado4 ==0){//Si la variable estado4 es igual a 0 se cumple esta condición
  Serial.print("luz4on");// Enviamos esta cadena de caracteres x el puerto serial para encender la luz
  estado4 =1;//Asignamos el valor 1 a la variable "estado4"
  } else{
   Serial.print("luz4off");//Enviamos esta cadena para apagar la luz
   estado4 =0;
    }
  while(pul4 == LOW){
  pul4 = digitalRead(4);//Se cumple esta condición mientras esté precionado el botón
      }
    }
  //-------------------------------------------------------------------------------
  //Enciende o apaga la luz
  if (pul5 == LOW) {//Si el pulsador 5 está precionado se cumple esta condición
  pul5 = digitalRead(5);//Leemos el estado del botón nuevamente
  if(estado5 ==0){//Si la variable estado5 es igual a 0 se cumple esta condición
  Serial.print("luz5on");// Enviamos esta cadena de caracteres x el puerto serial para encender la luz
  estado5 =1;//Asignamos el valor 1 a la variable "estado5"
  } else{
   Serial.print("luz5off");//Enviamos esta cadena para apagar la luz
   estado5 =0;
    }
  while(pul5 == LOW){
  pul5 = digitalRead(5);//Se cumple esta condición mientras esté precionado el botón
      }
    }
  //-------------------------------------------------------------------------------
  //Enciende o apaga la luz
  if (pul6 == LOW) {//Si el pulsador 6 está precionado se cumple esta condición
  pul6 = digitalRead(6);//Leemos el estado del botón nuevamente
  if(estado6 ==0){//Si la variable estado6 es igual a 0 se cumple esta condición
  Serial.print("luz6on");// Enviamos esta cadena de caracteres x el puerto serial para encender la luz
  estado6 =1;//Asignamos el valor 1 a la variable "estado6"
  } else{
   Serial.print("luz6off");//Enviamos esta cadena para apagar la luz
   estado6 =0;
    }
  while(pul6 == LOW){
  pul6 = digitalRead(6);//Se cumple esta condición mientras esté precionado el botón
      }
    }
  //-------------------------------------------------------------------------------
  //Enciende o apaga la luz
  if (pul7 == LOW) {//Si el pulsador 7 está precionado se cumple esta condición
  pul7 = digitalRead(7);//Leemos el estado del botón nuevamente
  if(estado7 ==0){//Si la variable estado7 es igual a 0 se cumple esta condición
  Serial.print("luz7on");// Enviamos esta cadena de caracteres x el puerto serial para encender la luz
  estado7 =1;//Asignamos el valor 1 a la variable "estado7"
  } else{
   Serial.print("luz7off");//Enviamos esta cadena para apagar la luz
   estado7 =0;
    }
  while(pul7 == LOW){
  pul7 = digitalRead(7);//Se cumple esta condición mientras esté precionado el botón
      }
    }
  //-------------------------------------------------------------------------------
  //Enciende o apaga la luz
  if (pul8 == LOW) {//Si el pulsador 8 está precionado se cumple esta condición
  pul8 = digitalRead(8);//Leemos el estado del botón nuevamente
  if(estado8 ==0){//Si la variable estado8 es igual a 0 se cumple esta condición
  Serial.print("luz8on");// Enviamos esta cadena de caracteres x el puerto serial para encender la luz
  estado8 =1;//Asignamos el valor 1 a la variable "estado8"
  } else{
   Serial.print("luz8off");//Enviamos esta cadena para apagar la luz
   estado8 =0;
    }
  while(pul8 == LOW){
  pul8 = digitalRead(8);//Se cumple esta condición mientras esté precionado el botón
      }
    }
  //-------------------------------------------------------------------------------
  //Enciende o apaga la luz
  if (pul9 == LOW) {//Si el pulsador 9 está precionado se cumple esta condición
  pul9 = digitalRead(9);//Leemos el estado del botón nuevamente
  if(estado9 ==0){//Si la variable estado9 es igual a 0 se cumple esta condición
  Serial.print("luz9on");// Enviamos esta cadena de caracteres x el puerto serial para encender la luz
  estado9 =1;//Asignamos el valor 1 a la variable "estado9"
  } else{
```

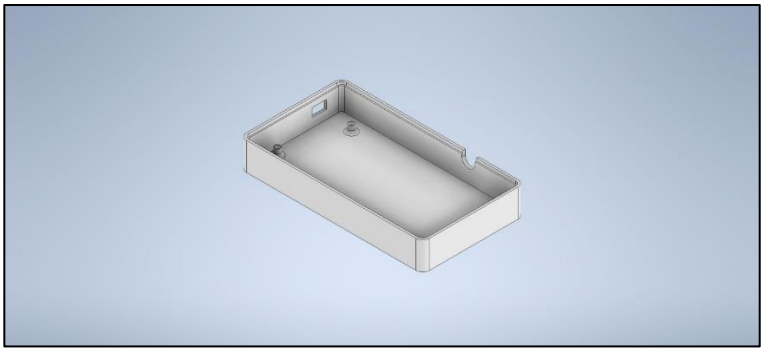
```
155     Serial.print("luz9off");//Enviamos esta cadena para apagar la luz
156     estado9 =0;
157      }
158    while(pul9 == LOW){
159    pul9 = digitalRead(9);//Se cumple esta condición mientras esté precionado el botón
160        }
161      }
162    //--------------------------------------------------------------------------------
163      delay(50);
164   }
```

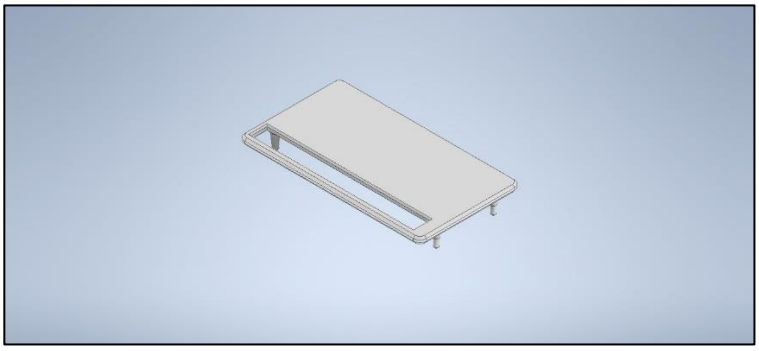
Anexo 12 – Código de programación para el nodo SERVIDOR (receptor)

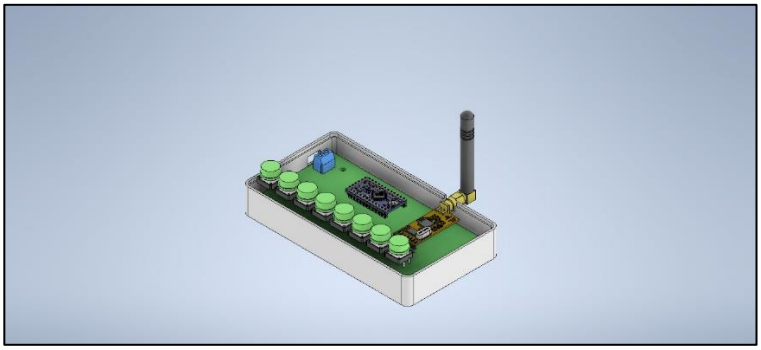
```
String cadena;
int luz2 = 2;
int luz3 = 3;
int luz4 = 4;
int luz5 = 5;
int luz6 = 6;
int luz7 = 7;
int luz8 = 8;
int luz9 = 9;
void setup () {
    Serial.begin(9600);// setea la velocidad del puerto serial
    pinMode(luz2, OUTPUT);
    pinMode(luz3, OUTPUT);
    pinMode(luz4, OUTPUT);
    pinMode(luz5, OUTPUT);
    pinMode(luz6, OUTPUT);
    pinMode(luz7, OUTPUT);
    pinMode(luz8, OUTPUT);
    pinMode(luz9, OUTPUT);
    digitalWrite(2, LOW);
    digitalWrite(3, LOW);
    digitalWrite(4, LOW);
    digitalWrite(5, LOW);
    digitalWrite(6, LOW);
    digitalWrite(7, LOW);
    digitalWrite(8, LOW);
    digitalWrite(9, LOW);
    delay(10);
  }
void loop () {
  //lee las cadenas que ingresan al puerto serie
  if (Serial.available())  {
    cadena = String("");
    while (Serial.available()) {
      cadena = cadena + char(Serial.read());
      delay(1);
        }
        }
//---------------------------------------------------------------------
 if (cadena == "luz2on") {//compara el valor de la cadena obetinada
digitalWrite (luz2,HIGH);//Al recibir la cadena luz2on, enciende el LED del pin2
    }
 if (cadena == "luz2off") {//compara el valor de la cadena obetinada
digitalWrite (luz2,LOW);//Al recibir la cadena luz2off, apaga el LED del pin2
    }
//---------------------------------------------------------------------
 if (cadena == "luz3on") {//compara el valor de la cadena obetinada
digitalWrite (luz3,HIGH);//Al recibir la cadena luz2on, enciende el LED del pin3
    }
 if (cadena == "luz3off") {//compara el valor de la cadena obetinada
digitalWrite (luz3,LOW);//Al recibir la cadena luz2off, apaga el LED del pin3
    }
//---------------------------------------------------------------------
 if (cadena == "luz4on") {//compara el valor de la cadena obetinada
digitalWrite (luz4,HIGH);//Al recibir la cadena luz2on, enciende el LED del pin4
    }
 if (cadena == "luz4off") {//compara el valor de la cadena obetinada
digitalWrite (luz4,LOW);//Al recibir la cadena luz2off, apaga el LED del pin4
    }
//---------------------------------------------------------------------
 if (cadena == "luz5on") {//compara el valor de la cadena obetinada
digitalWrite (luz5,HIGH);//Al recibir la cadena luz2on, enciende el LED del pin5
    }
 if (cadena == "luz5off") {//compara el valor de la cadena obetinada
digitalWrite (luz5,LOW);//Al recibir la cadena luz2off, apaga el LED del pin5
    }
//---------------------------------------------------------------------
 if (cadena == "luz6on") {//compara el valor de la cadena obetinada
digitalWrite (luz6,HIGH);//Al recibir la cadena luz2on, enciende el LED del pin6
    }
 if (cadena == "luz6off") {//compara el valor de la cadena obetinada
digitalWrite (luz6,LOW);//Al recibir la cadena luz2off, apaga el LED del pin6
    }
//---------------------------------------------------------------------
 if (cadena == "luz7on") {//compara el valor de la cadena obetinada
digitalWrite (luz7,HIGH);//Al recibir la cadena luz2on, enciende el LED del pin7
    }
 if (cadena == "luz7off") {//compara el valor de la cadena obetinada
digitalWrite (luz7,LOW);//Al recibir la cadena luz2off, apaga el LED del pin7
    }
//---------------------------------------------------------------------
 if (cadena == "luz8on") {//compara el valor de la cadena obetinada
digitalWrite (luz8,HIGH);//Al recibir la cadena luz2on, enciende el LED del pin8
    }
```

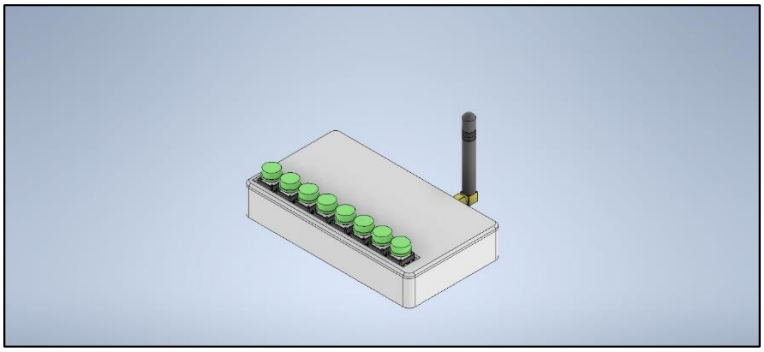
```
 if (cadena == "luz8off") {//compara el valor de la cadena obetinada
digitalWrite (luz8,LOW);//Al recibir la cadena luz2off, apaga el LED del pin8
    }
//-----------------------------------------------------------------
 if (cadena == "luz9on") {//compara el valor de la cadena obetinada
digitalWrite (luz9,HIGH);//Al recibir la cadena luz2on, enciende el LED del pin9
    }
 if (cadena == "luz9off") {//compara el valor de la cadena obetinada
digitalWrite (luz9,LOW);//Al recibir la cadena luz2off, apaga el LED del pin9
    }
}
```

Anexo 13 – Modelado del encapsulado del nodo CLIENTE

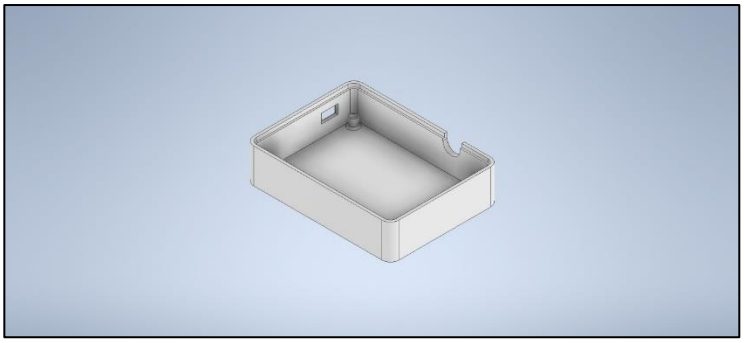


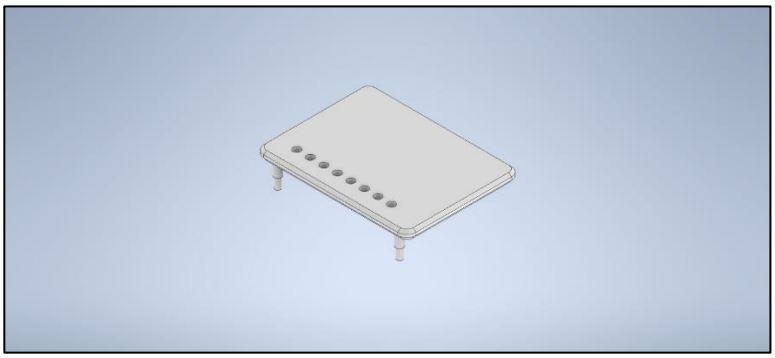


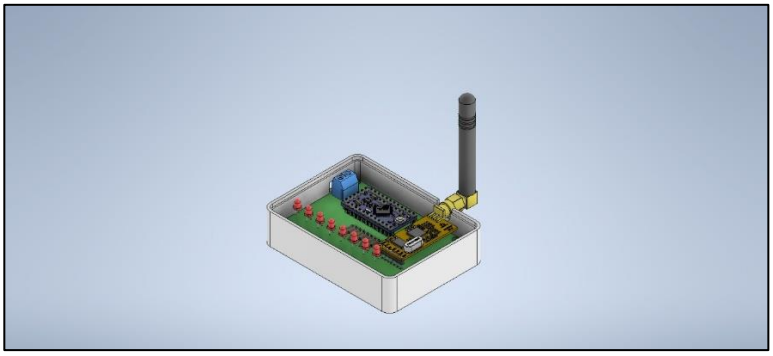


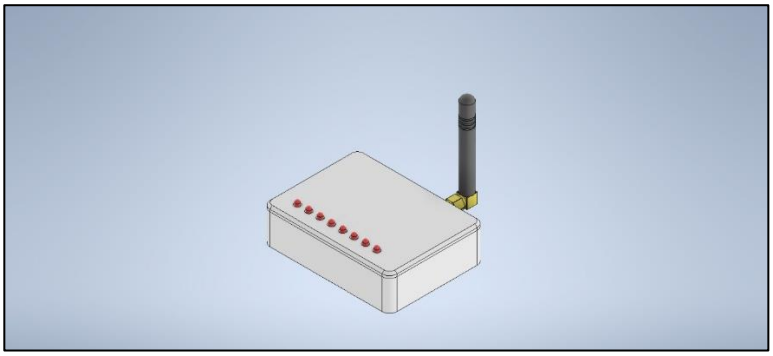


Anexo 14 – Modelado del encapsulado del nodo SERVIDOR

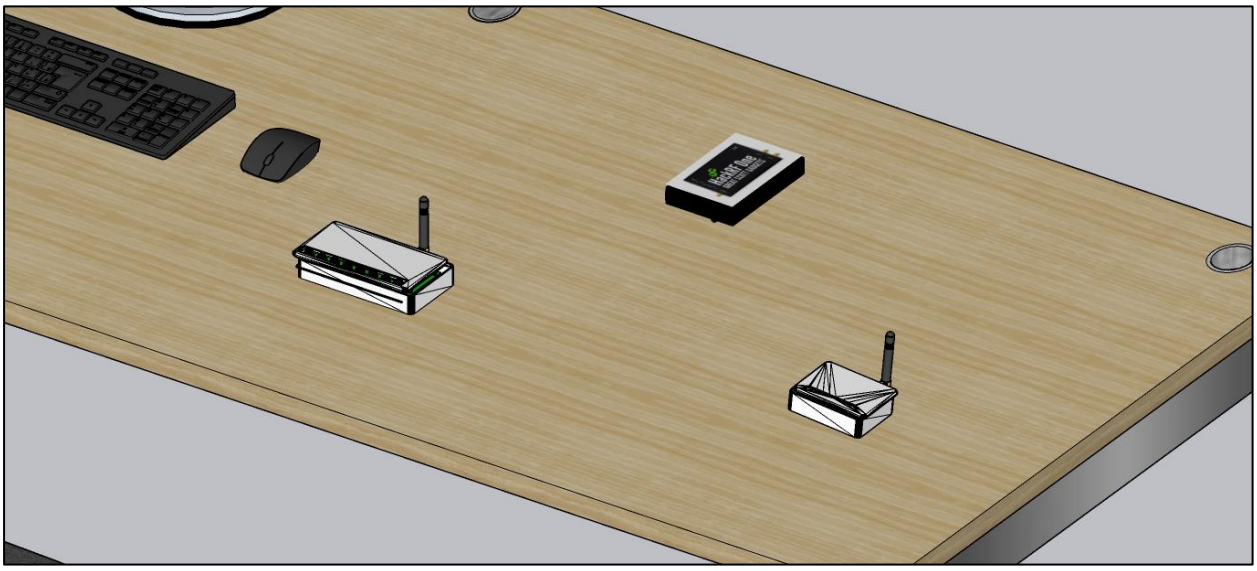




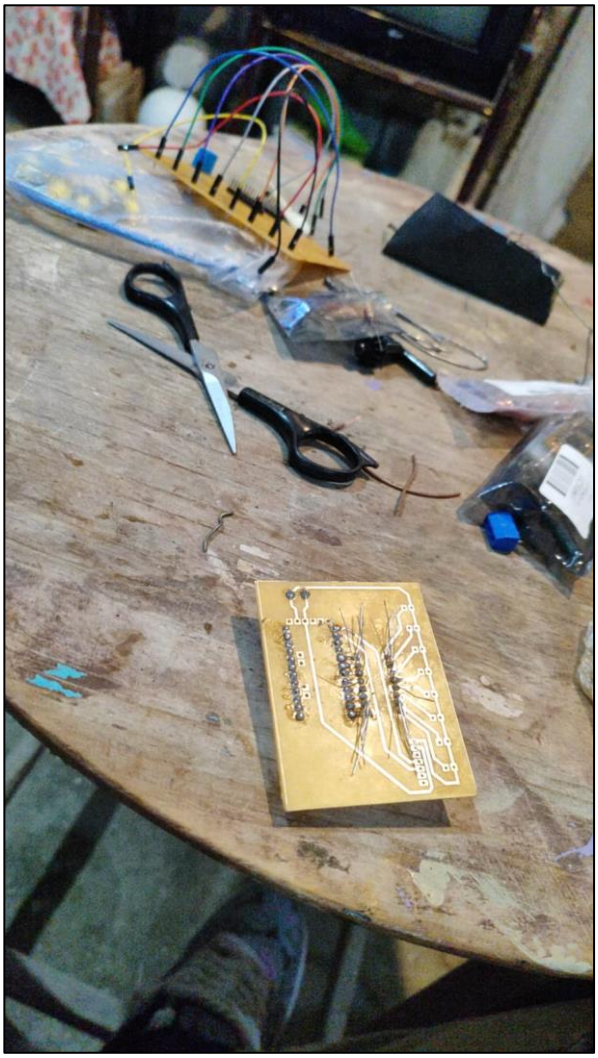


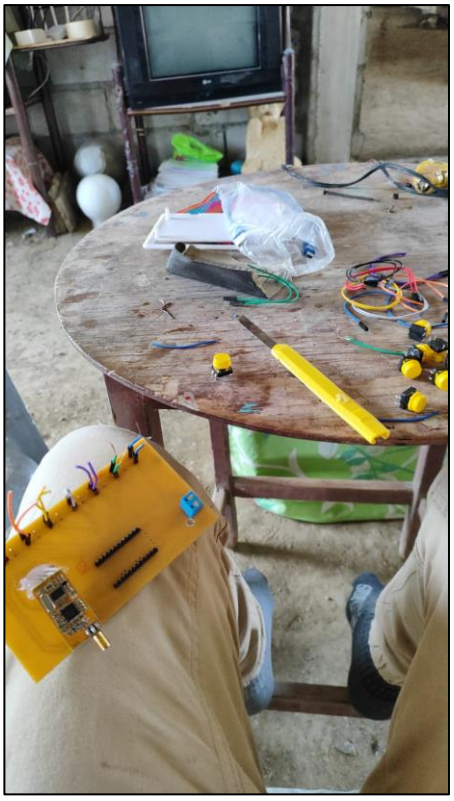


Anexo 15 – Modelado de la propuesta dentro del laboratorio de telecomunicaciones

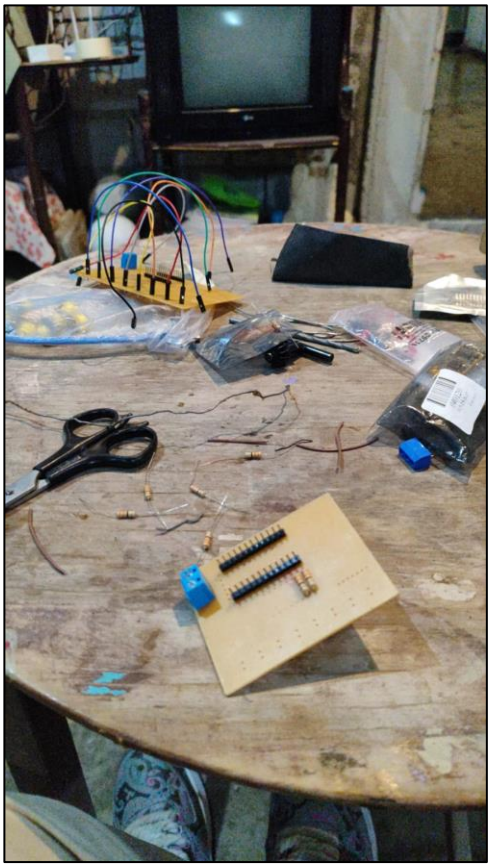


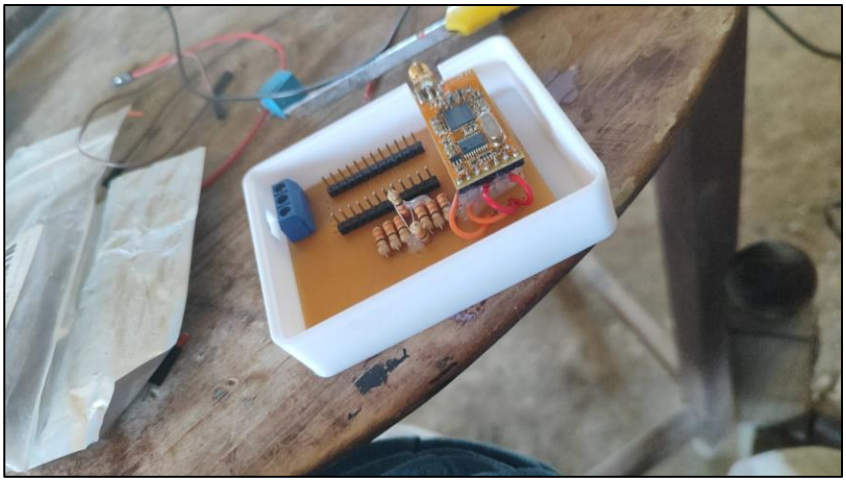
Anexo 16 – Construcción del nodo CLIENTE

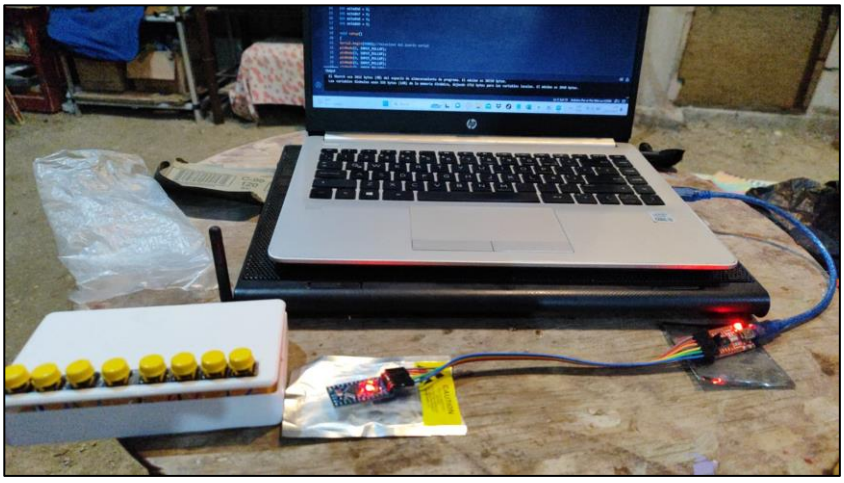




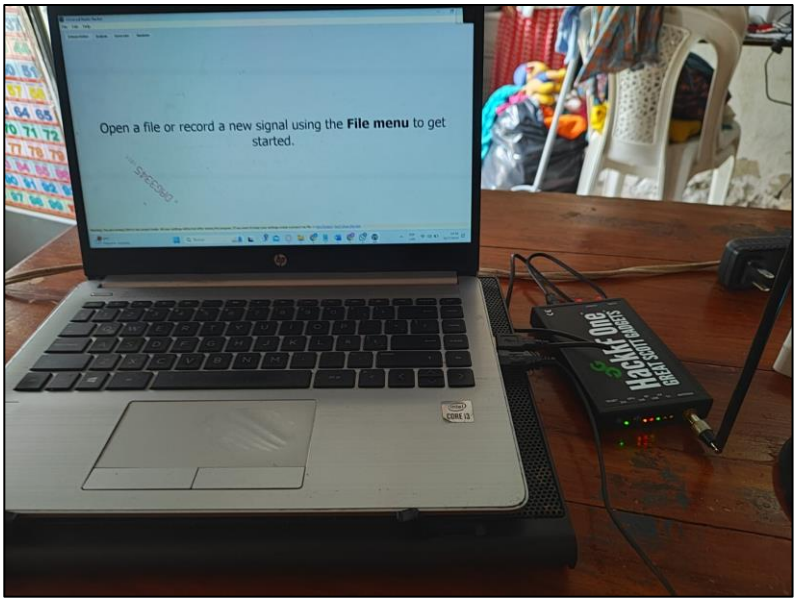
Anexo 17 – Construcción del nodo SERVIDOR

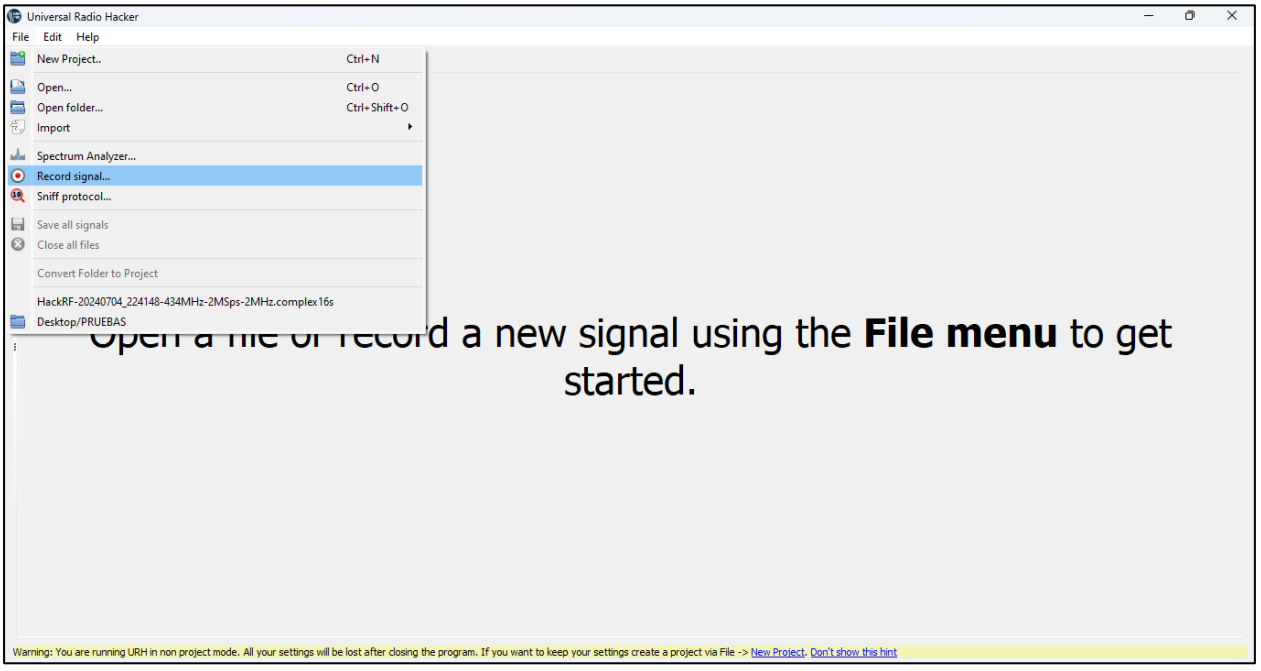


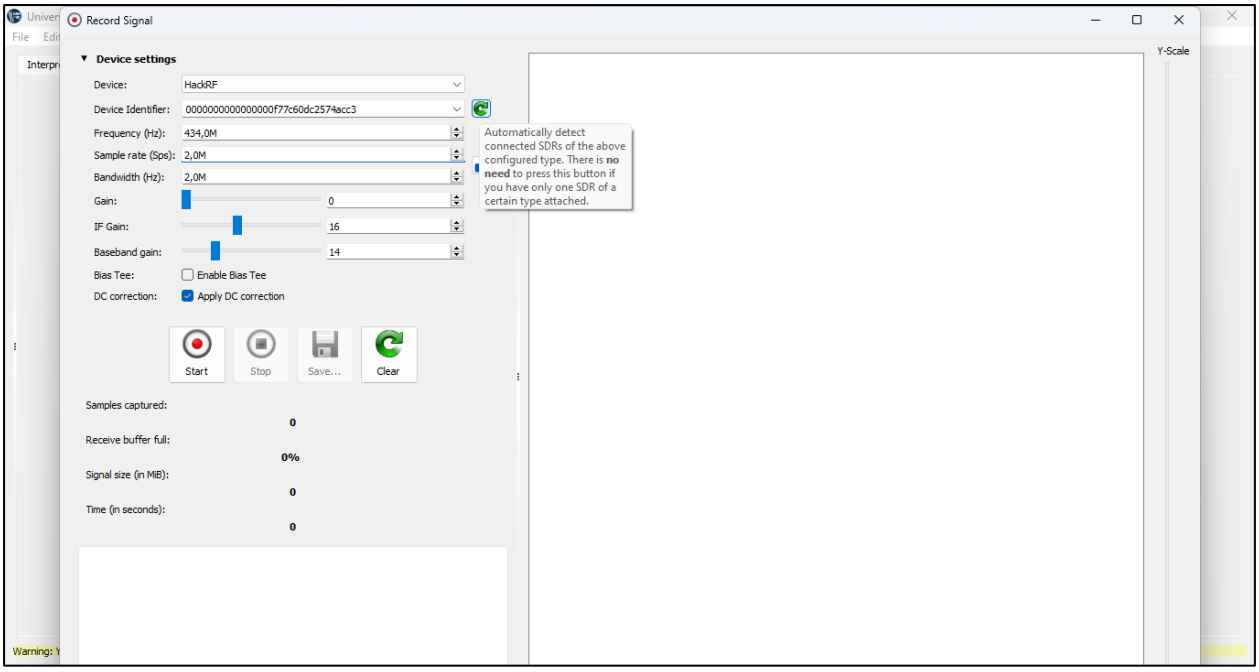


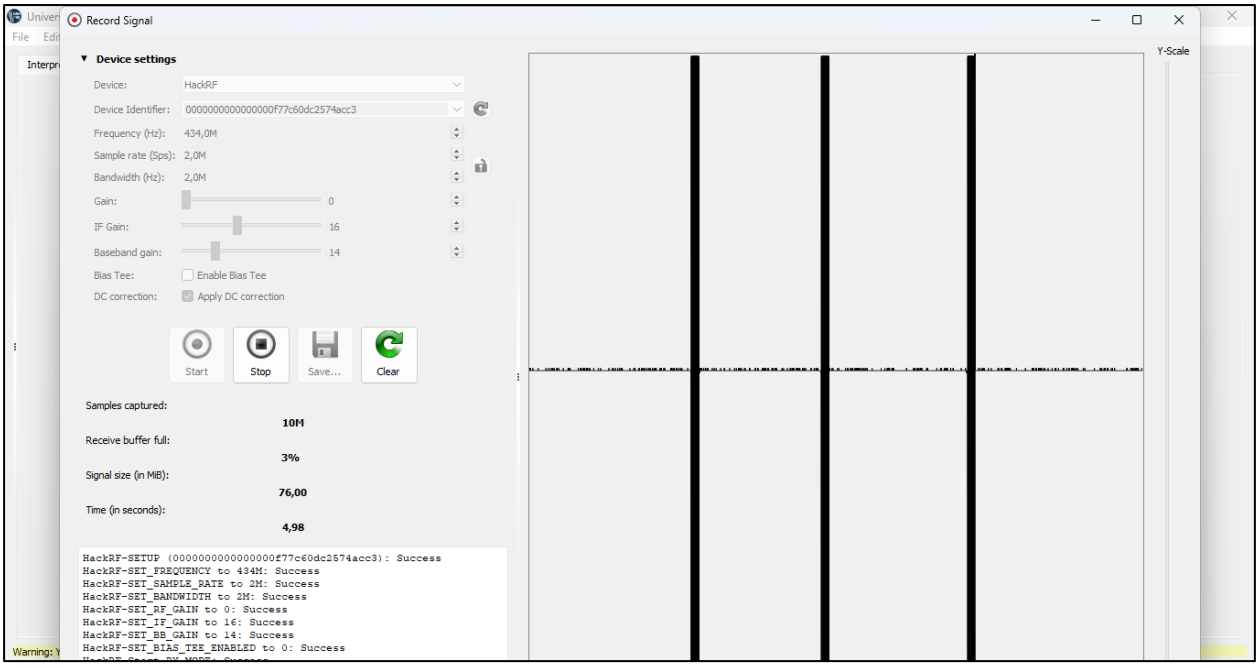


Anexo 18 – Ataque eavesdropping

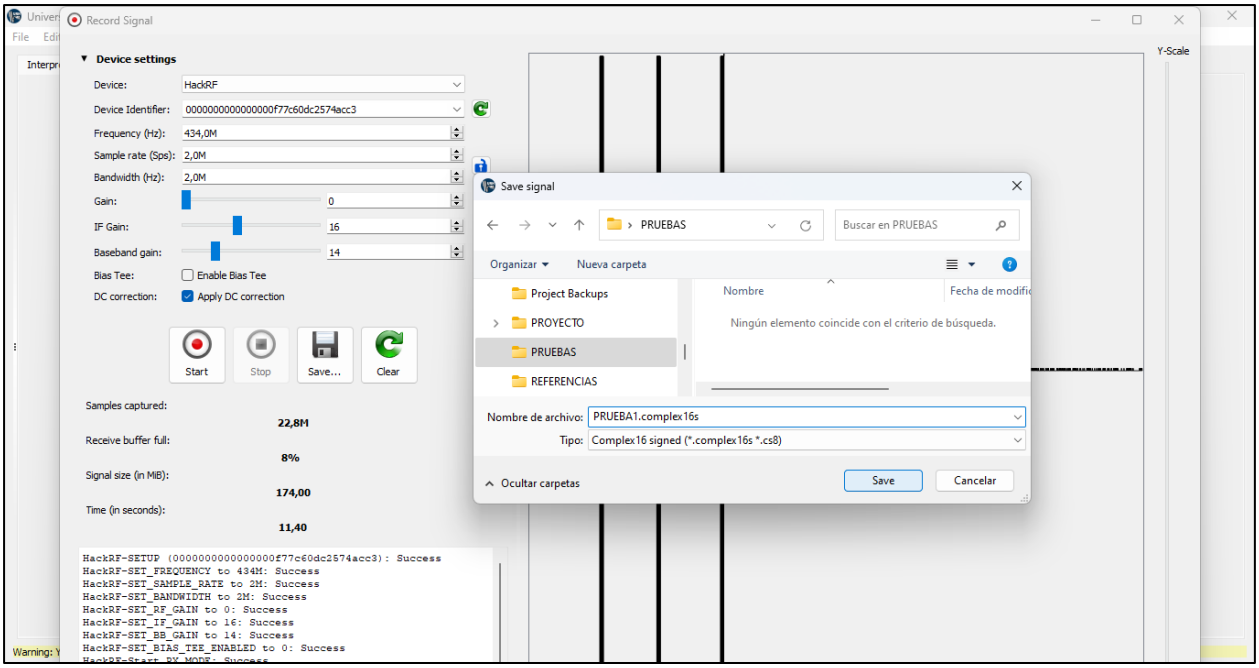


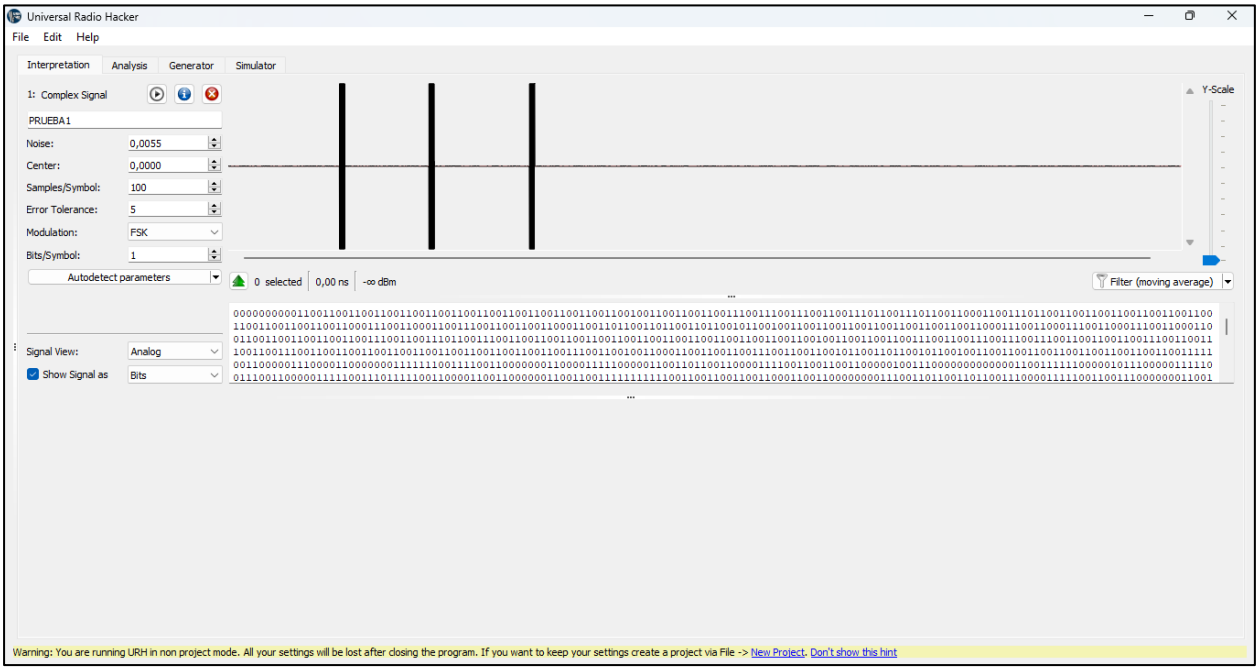


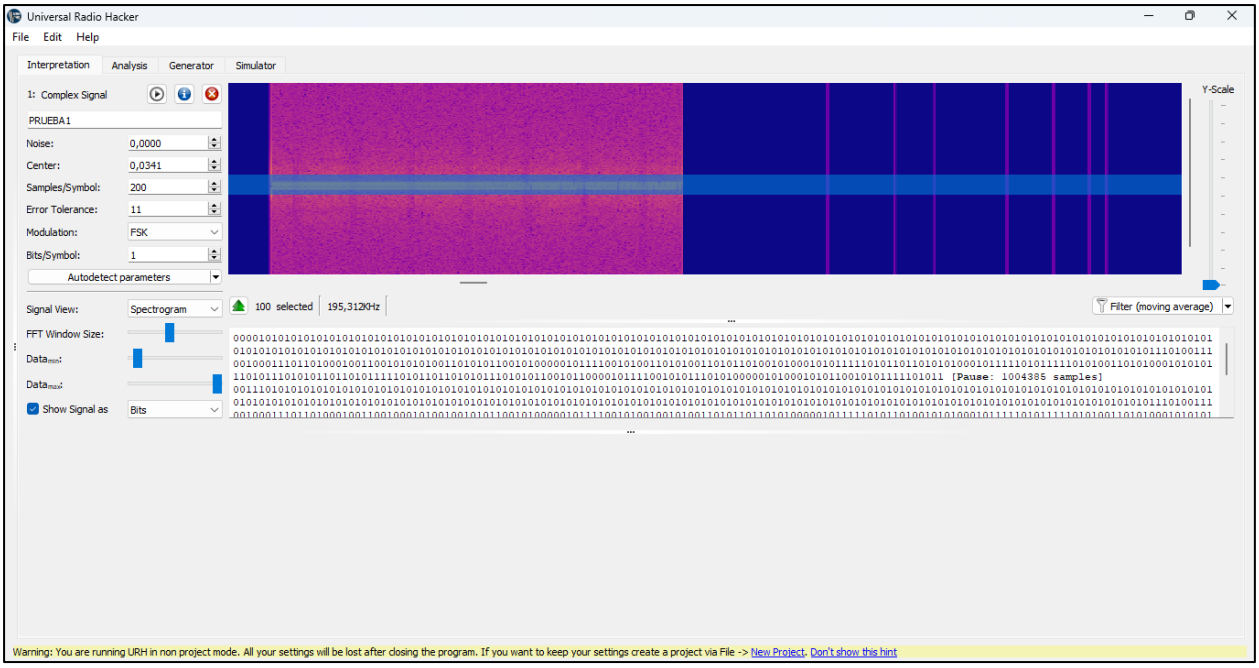

Record Signal
Device settings
Device:
HackRF
Device Identifier:
0000000000000000f77c60dc2574acc3
Frequency (Hz):
434,0M
Sample rate (Sps):
2,0M
Bandwidth (Hz):
2,0M
Gain:
IF Gain:
16
Baseband gain:
14
Bias Tee:
Enable Bias Tee
DC correction:
Apply DC correction
Automatically detect connected SDRs of the above configured type. There is no need to press this button if you have only one SDR of a certain type attached.
Start
Stop
Save...
Clear
Samples captured:
0
Receive buffer full:
0%
Signal size (in MiB):
0
Time (in seconds):
0
Y-Scale

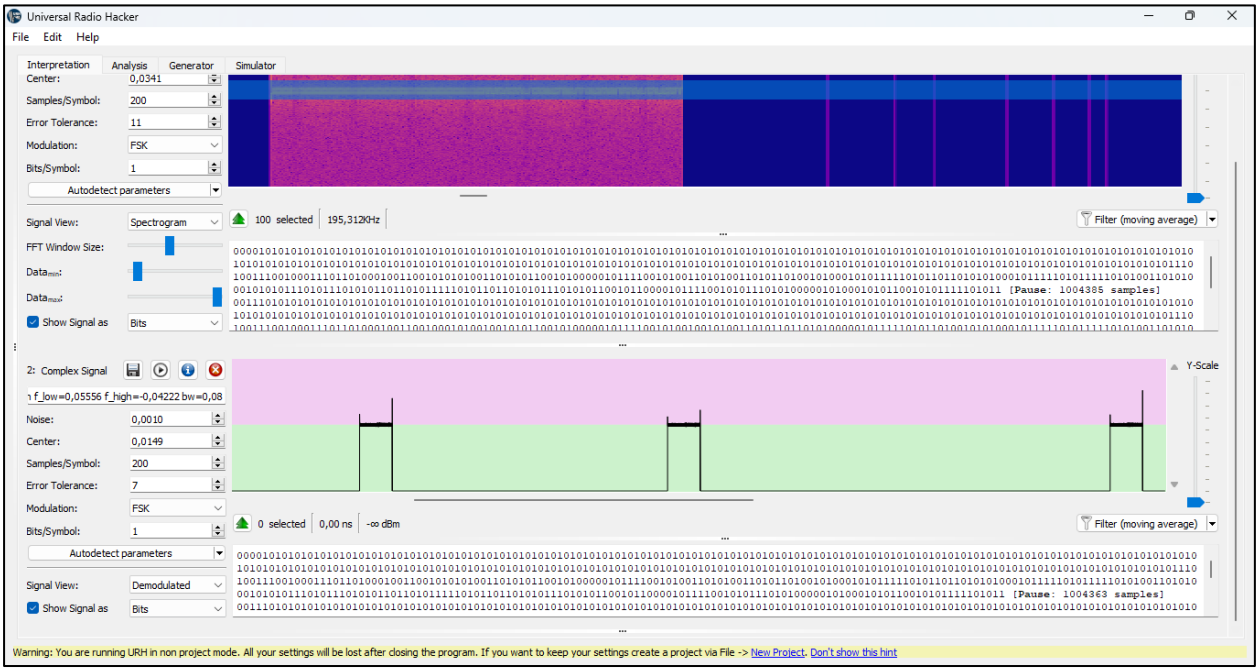

Record Signal
Device settings
Device: HackRF
Device Identifier: 0000000000000000f77c60dc2574acc3
Frequency (Hz): 434,0M
Sample rate (Sps): 2,0M
Bandwidth (Hz): 2,0M
Gain: 0
IF Gain: 16
Baseband gain: 14
Bias Tee: Enable Bias Tee
DC correction: Apply DC correction
Start
Stop
Save...
Clear
Samples captured:
10M
Receive buffer full:
3%
Signal size (in MiB):
76,00
Time (in seconds):
4,98
HackRF-SETUP (0000000000000000f77c60dc2574acc3): Success
HackRF-SET_FREQUENCY to 434M: Success
HackRF-SET_SAMPLE_RATE to 2M: Success
HackRF-SET_BANDWIDTH to 2M: Success
HackRF-SET_RF_GAIN to 0: Success
HackRF-SET_IF_GAIN to 16: Success
HackRF-SET_BB_GAIN to 14: Success
HackRF-SET_BIAS_TEE_ENABLED to 0: Success
Y-Scale

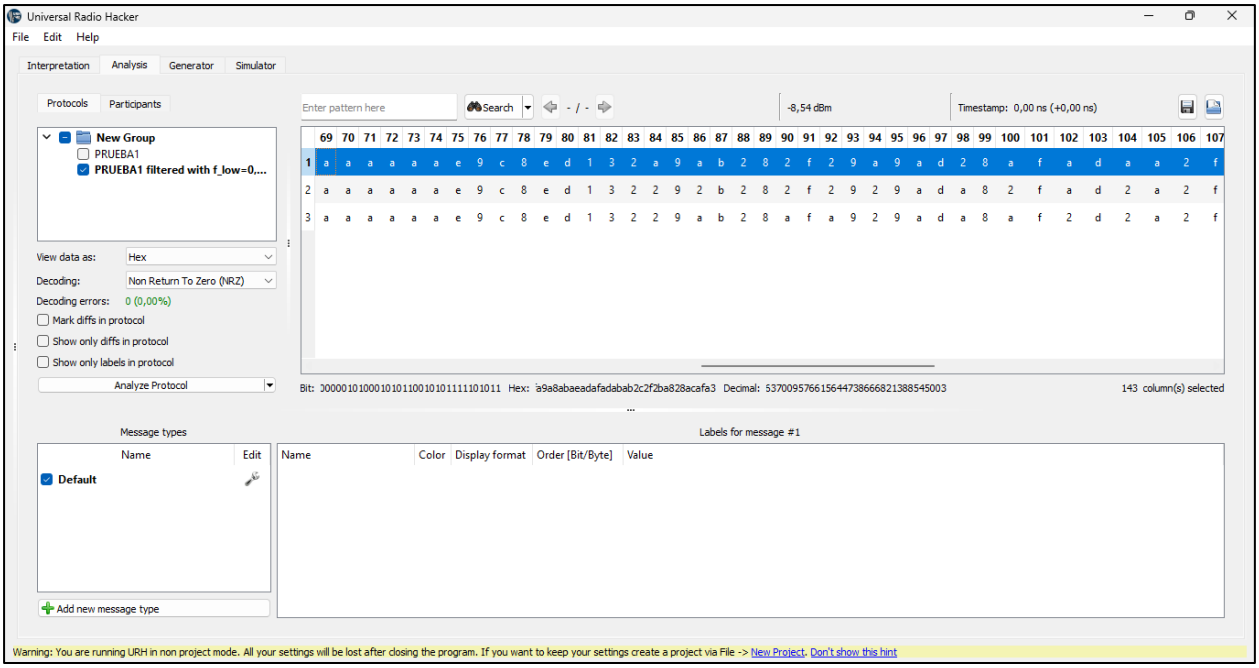

HackRF One


Record Signal
Device settings
Device: HackRF
Device Identifier: 0000000000000000f77c60dc2574acc3
Frequency (Hz): 434,0M
Sample rate (Sps): 2,0M
Bandwidth (Hz): 2,0M
Gain: 0
IF Gain: 16
Baseband gain: 14
Bias Tee: Enable Bias Tee
DC correction: Apply DC correction
Start
Stop
Save...
Clear
Samples captured: 22,8M
Receive buffer full: 8%
Signal size (in MiB): 174,00
Time (in seconds): 11,40
HackRF-SETUP (0000000000000000f77c60dc2574acc3): Success
HackRF-SET_FREQUENCY to 434M: Success
HackRF-SET_SAMPLE_RATE to 2M: Success
HackRF-SET_BANDWIDTH to 2M: Success
HackRF-SET_RF_GAIN to 0: Success
HackRF-SET_IF_GAIN to 16: Success
HackRF-SET_BB_GAIN to 14: Success
HackRF-SET_BIAS_TEE_ENABLED to 0: Success
Y-Scale
Save signal
PRUEBAS
Buscar en PRUEBAS
Organizar
Nueva carpeta
Project Backups
PROYECTO
PRUEBAS
REFERENCIAS
Nombre
Fecha de modific
Ningún elemento coincide con el criterio de búsqueda.
Nombre de archivo: PRUEBA1.complex16s
Tipo: Complex16 signed (*.complex16s *.cs8)
Ocultar carpetas
Save
Cancelar

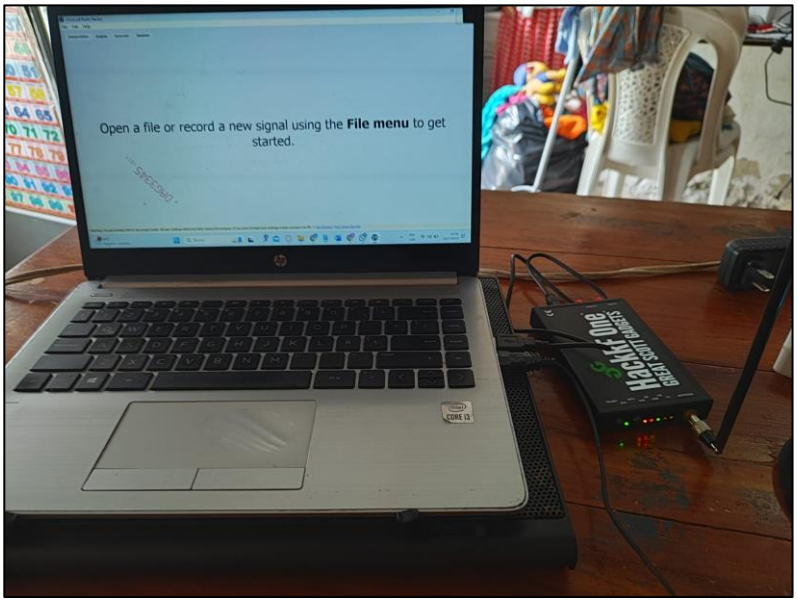

Universal Radio Hacker
File Edit Help
Interpretation
Analysis
Generator
Simulator
1: Complex Signal
PRUEBA1
Noise: 0,0055
Center: 0,0000
Samples/Symbol: 100
Error Tolerance: 5
Modulation: FSK
Bits/Symbol: 1
Autodetect parameters
Signal View: Analog
Show Signal as Bits
Y-Scale
0 selected
0,00 ns
-∞ dBm
Filter (moving average)
Warning: You are running URH in non project mode. All your settings will be lost after closing the program. If you want to keep your settings create a project via File -> New Project. Don't show this hint


Universal Radio Hacker
File Edit Help
Interpretation Analysis Generator Simulator
1: Complex Signal
PRUEBA1
Noise: 0,0000
Center: 0,0341
Samples/Symbol: 200
Error Tolerance: 11
Modulation: FSK
Bits/Symbol: 1
Autodetect parameters
Signal View: Spectrogram
FFT Window Size:
Data min:
Data max:
Show Signal as Bits
100 selected
195,312KHz
Y-Scale
Filter (moving average)
[Pause: 1004385 samples]
Warning: You are running URH in non project mode. All your settings will be lost after closing the program. If you want to keep your settings create a project via File -> New Project. Don't show this hint

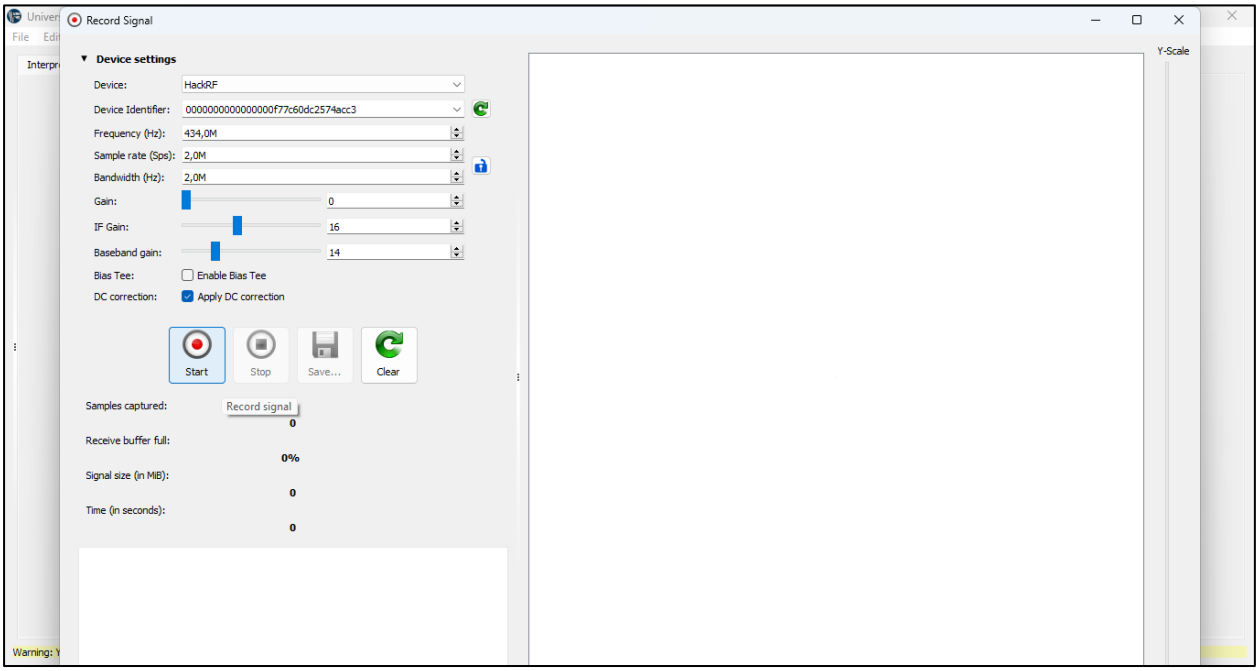

Universal Radio Hacker
File Edit Help
Interpretation Analysis Generator Simulator
Center: 0,0341
Samples/Symbol: 200
Error Tolerance: 11
Modulation: FSK
Bits/Symbol: 1
Autodetect parameters
Signal View: Spectrogram
FFT Window Size:
Data min:
Data max:
Show Signal as Bits
100 selected
195,312KHz
Filter (moving average)
[Pause: 1004385 samples]
2: Complex Signal
f_low=0,05556 f_high=-0,04222 bw=0,08
Noise: 0,0010
Center: 0,0149
Samples/Symbol: 200
Error Tolerance: 7
Modulation: FSK
Bits/Symbol: 1
Autodetect parameters
Signal View: Demodulated
Show Signal as Bits
0 selected
0,00 ns
-∞ dBm
Y-Scale
Filter (moving average)
[Pause: 1004363 samples]
Warning: You are running URH in non project mode. All your settings will be lost after closing the program. If you want to keep your settings create a project via File -> New Project. Don't show this hint

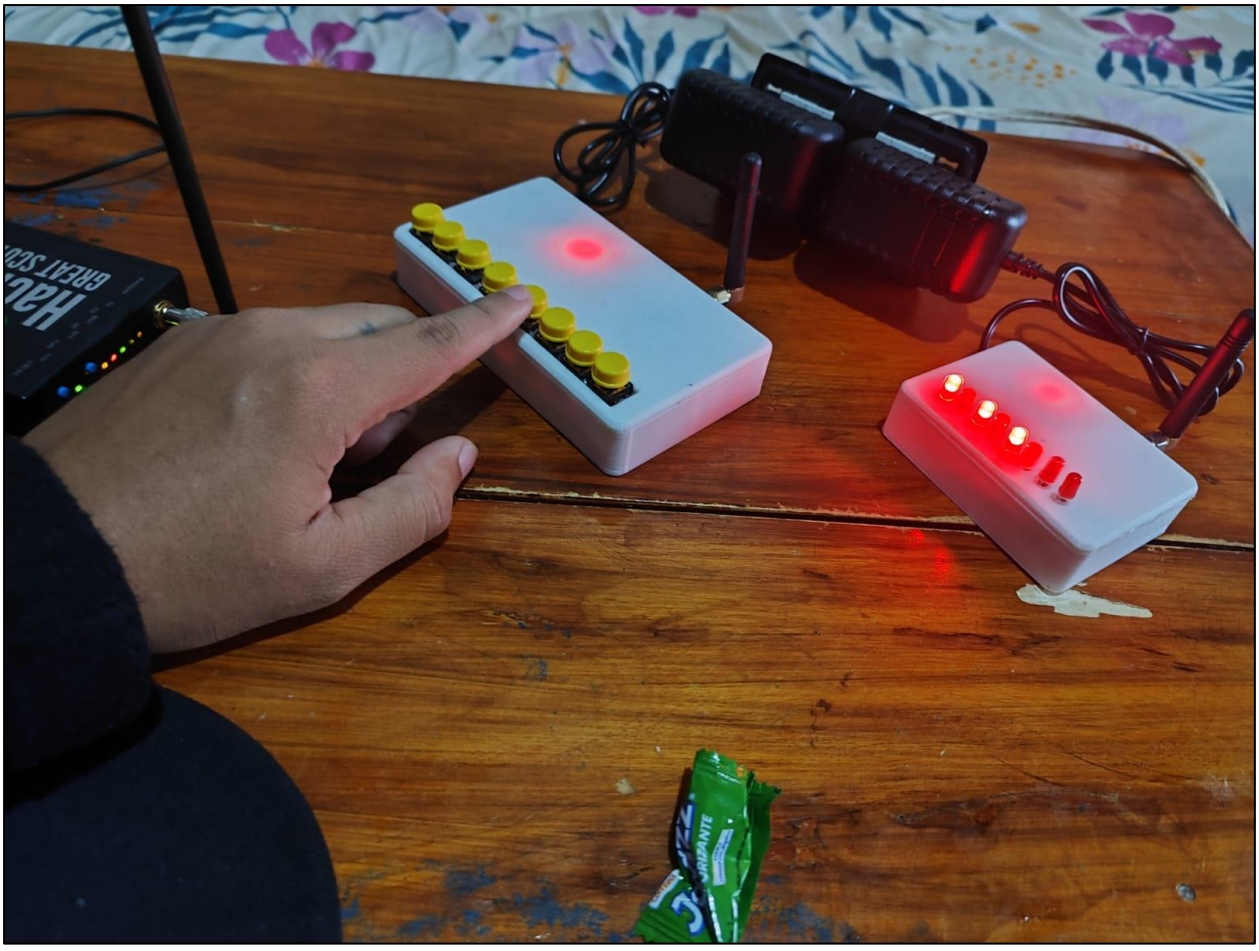


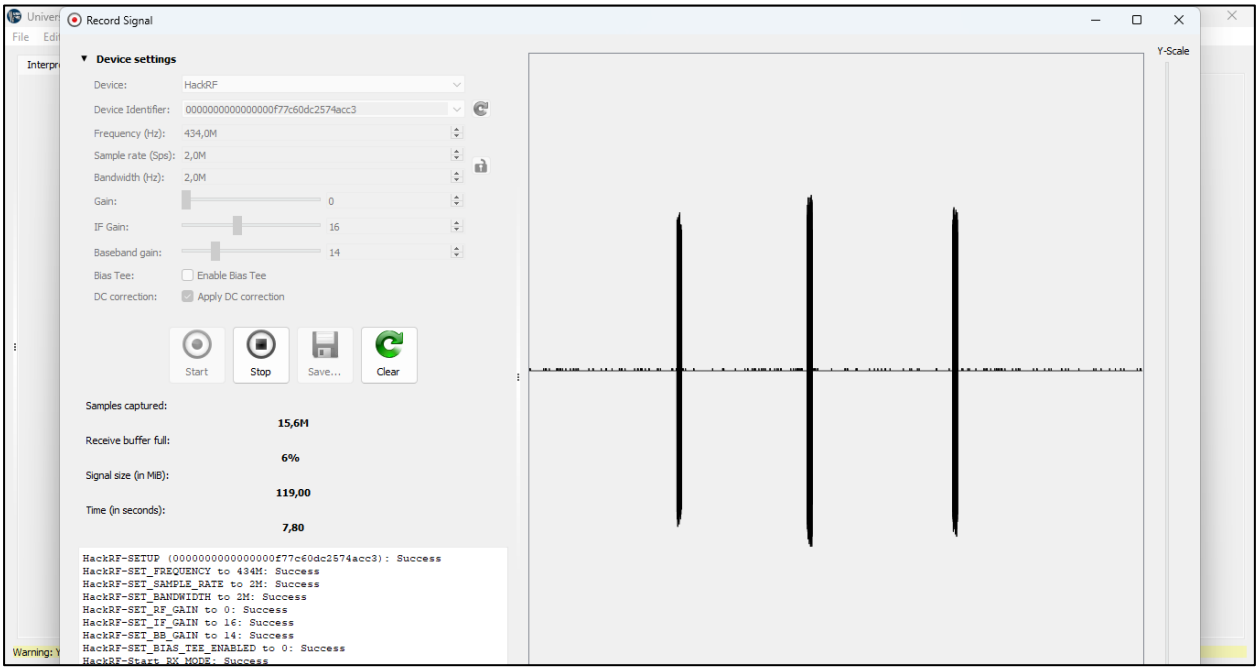
Anexo 19 – Ataque replay

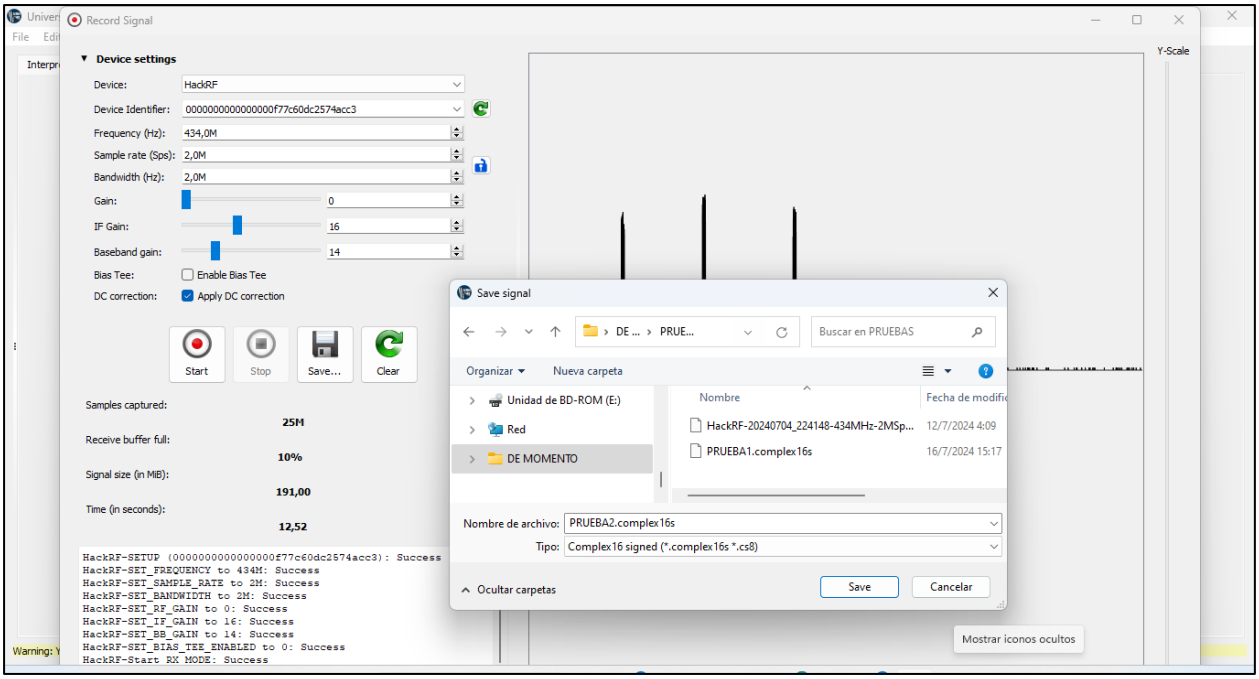


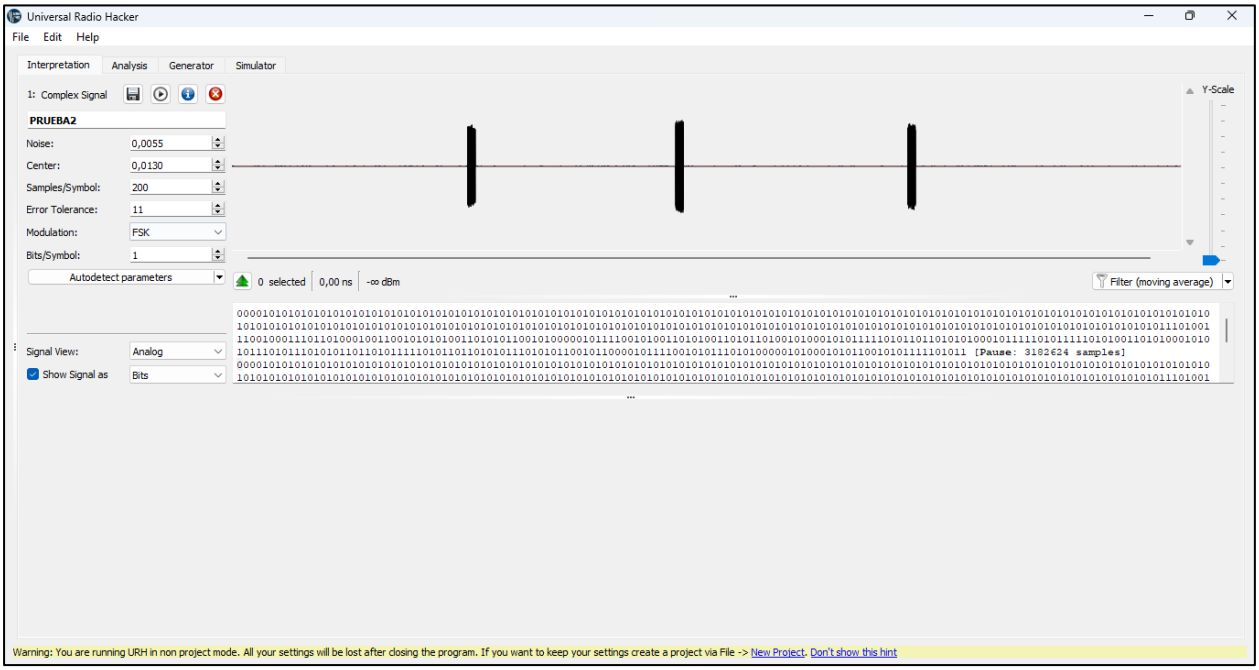

Universal Radio Hacker
File Edit Help
New Project.. Ctrl+N
Open... Ctrl+O
Open folder... Ctrl+Shift+O
Import
Spectrum Analyzer...
Record signal...
Sniff protocol...
Save all signals
Close all files
Convert Folder to Project
Open a file or record a new signal using the **File menu** to get started.
Warning: You are running URH in non project mode. All your settings will be lost after closing the program. If you want to keep your settings create a project via File -> New Project. Don't show this hint

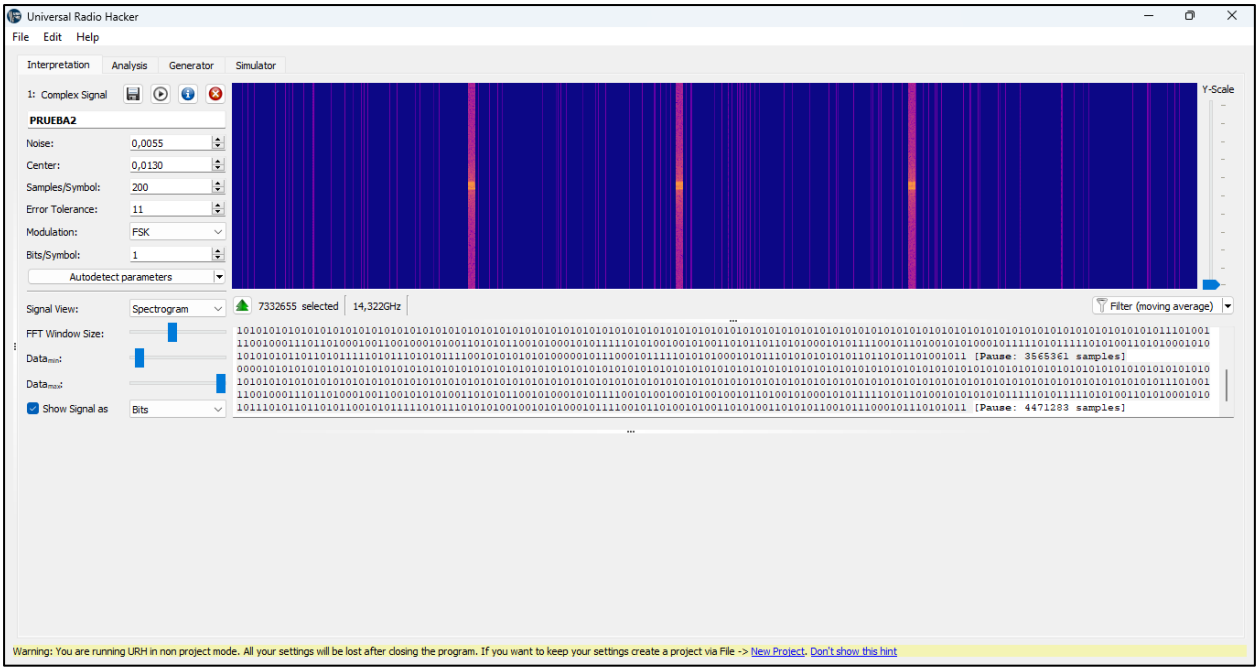

Record Signal
Device settings
Device: HackRF
Device Identifier: 0000000000000000f77c60dc2574acc3
Frequency (Hz): 434,0M
Sample rate (Sps): 2,0M
Bandwidth (Hz): 2,0M
Gain: 0
IF Gain: 16
Baseband gain: 14
Bias Tee: Enable Bias Tee
DC correction: Apply DC correction
Start
Stop
Save...
Clear
Samples captured: 0
Record signal
Receive buffer full: 0%
Signal size (in MiB): 0
Time (in seconds): 0
Y-Scale

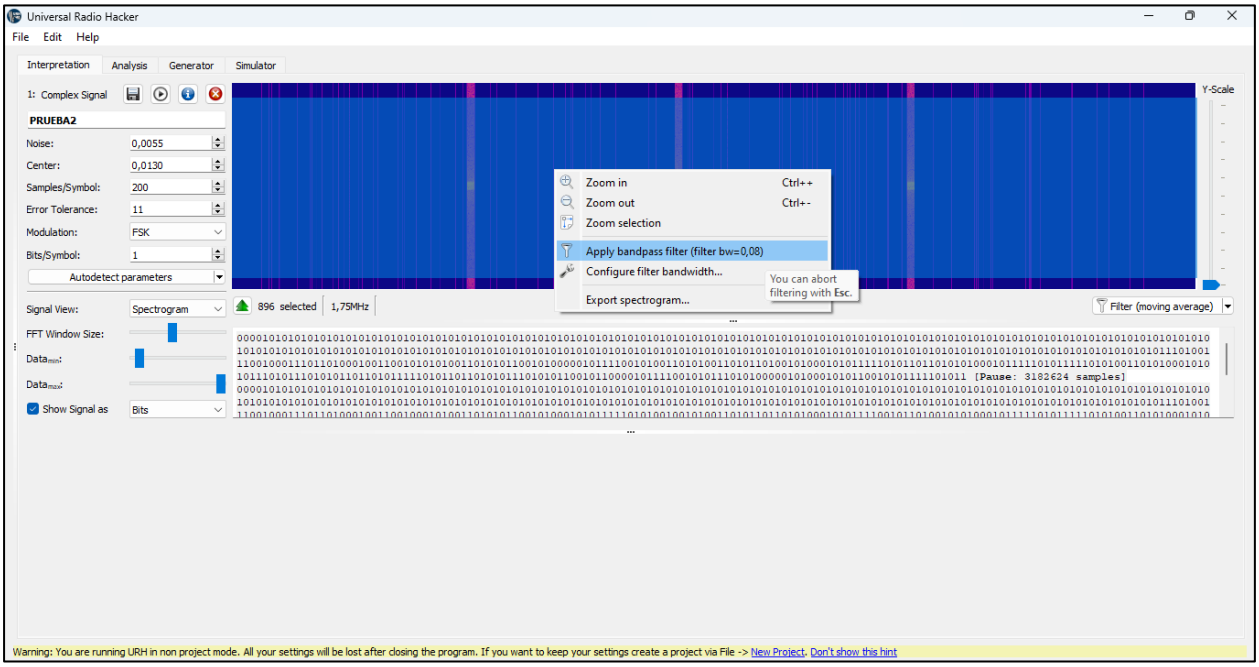


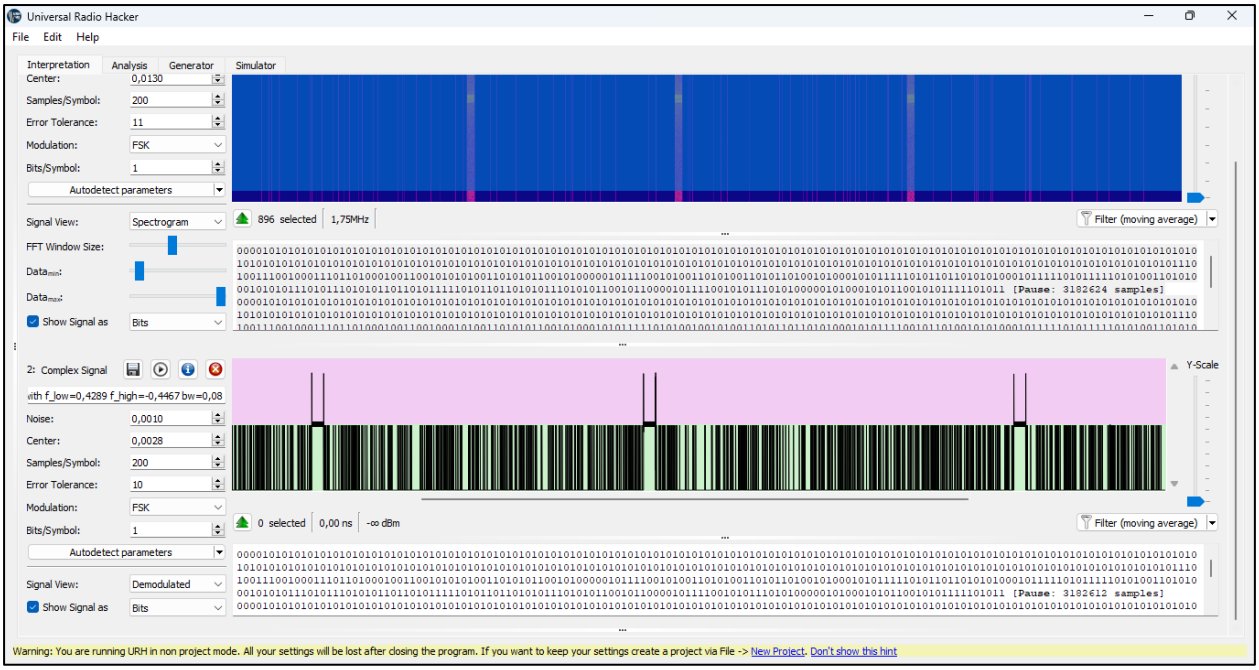

Record Signal
Device settings
Device: HackRF
Device Identifier: 0000000000000000f77c60dc2574acc3
Frequency (Hz): 434,0M
Sample rate (Sps): 2,0M
Bandwidth (Hz): 2,0M
Gain: 0
IF Gain: 16
Baseband gain: 14
Bias Tee: Enable Bias Tee
DC correction: Apply DC correction
Start
Stop
Save...
Clear
Samples captured:
15,6M
Receive buffer full:
6%
Signal size (in MiB):
119,00
Time (in seconds):
7,80
HackRF-SETUP (0000000000000000f77c60dc2574acc3): Success
HackRF-SET_FREQUENCY to 434M: Success
HackRF-SET_SAMPLE_RATE to 2M: Success
HackRF-SET_BANDWIDTH to 2M: Success
HackRF-SET_RF_GAIN to 0: Success
HackRF-SET_IF_GAIN to 16: Success
HackRF-SET_BB_GAIN to 14: Success
HackRF-SET_BIAS_TEE_ENABLED to 0: Success
HackRF-Start RX MODE: Success
Y-Scale

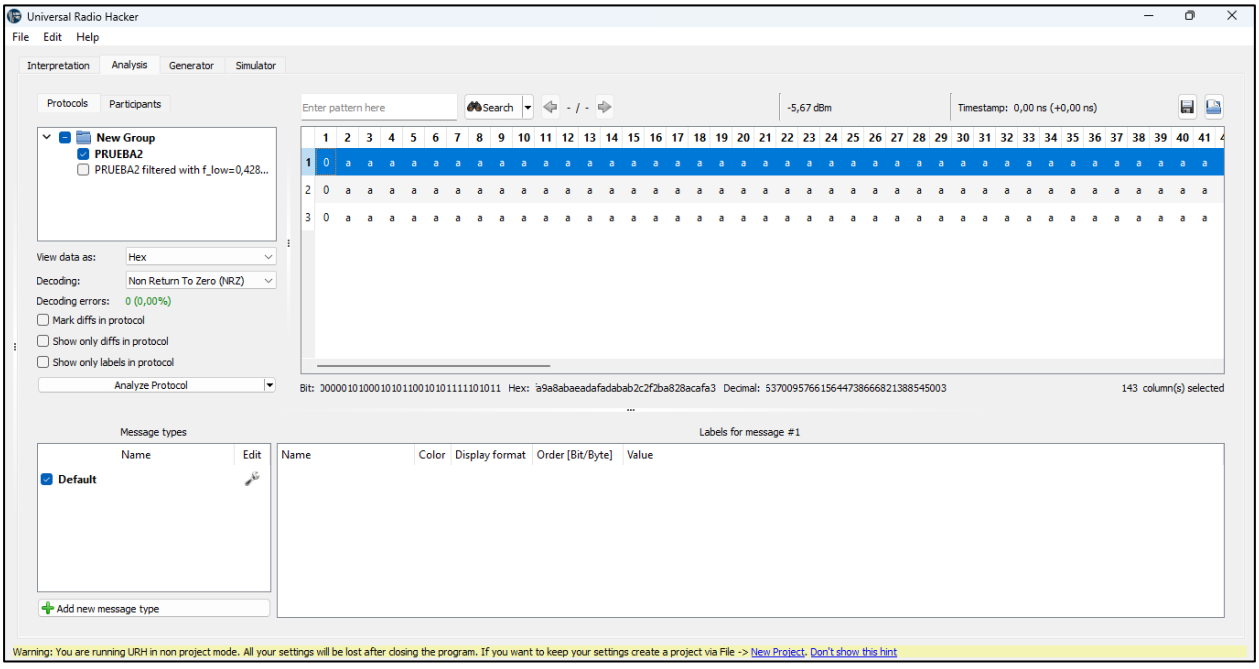

Record Signal
Device settings
Device: HackRF
Device Identifier: 0000000000000000f77c60dc2574acc3
Frequency (Hz): 434,0M
Sample rate (Sps): 2,0M
Bandwidth (Hz): 2,0M
Gain: 0
IF Gain: 16
Baseband gain: 14
Bias Tee: Enable Bias Tee
DC correction: Apply DC correction
Start
Stop
Save...
Clear
Samples captured: 25M
Receive buffer full: 10%
Signal size (in MiB): 191,00
Time (in seconds): 12,52
HackRF-SETUP (0000000000000000f77c60dc2574acc3): Success
HackRF-SET_FREQUENCY to 434M: Success
HackRF-SET_SAMPLE_RATE to 2M: Success
HackRF-SET_BANDWIDTH to 2M: Success
HackRF-SET_RF_GAIN to 0: Success
HackRF-SET_IF_GAIN to 16: Success
HackRF-SET_BB_GAIN to 14: Success
HackRF-SET_BIAS_TEE_ENABLED to 0: Success
HackRF-Start RX MODE: Success
Y-Scale
Save signal
Buscar en PRUEBAS
Organizar
Nueva carpeta
Unidad de BD-ROM (E:)
Red
DE MOMENTO
Nombre
HackRF-20240704_224148-434MHz-2MSp... 12/7/2024 4:09
PRUEBA1.complex16s 16/7/2024 15:17
Nombre de archivo: PRUEBA2.complex16s
Tipo: Complex16 signed (*.complex16s *.cs8)
Ocultar carpetas
Save
Cancelar
Mostrar iconos ocultos


Universal Radio Hacker
File Edit Help
Interpretation Analysis Generator Simulator
1: Complex Signal
PRUEBA2
Noise: 0,0055
Center: 0,0130
Samples/Symbol: 200
Error Tolerance: 11
Modulation: FSK
Bits/Symbol: 1
Autodetect parameters
Signal View: Analog
Show Signal as Bits
0 selected 0,00 ns -∞ dBm
Filter (moving average)
Y-Scale
[Pause: 3182624 samples]
Warning: You are running URH in non project mode. All your settings will be lost after closing the program. If you want to keep your settings create a project via File -> New Project. Don't show this hint

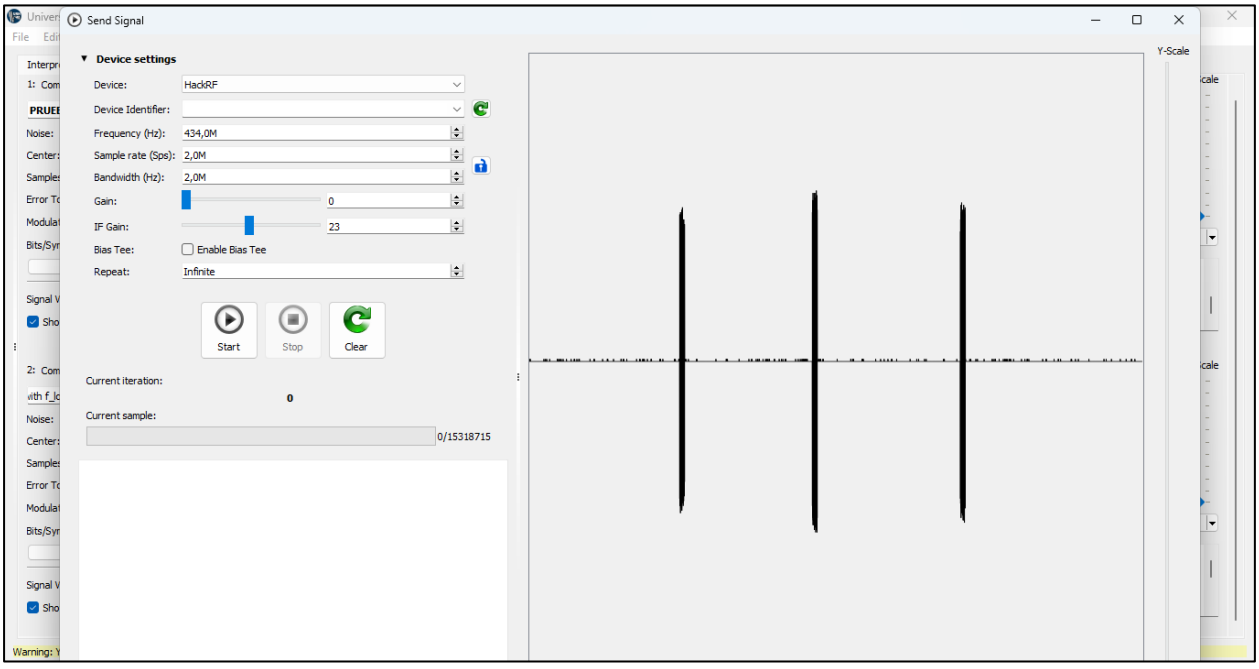

Universal Radio Hacker
File Edit Help
Interpretation Analysis Generator Simulator
1: Complex Signal
PRUEBA2
Noise: 0,0055
Center: 0,0130
Samples/Symbol: 200
Error Tolerance: 11
Modulation: FSK
Bits/Symbol: 1
Autodetect parameters
Signal View: Spectrogram
FFT Window Size:
Data min:
Data max:
Show Signal as Bits
7332655 selected
14,322GHz
Y-Scale
Filter (moving average)
[Pause: 3565361 samples]
[Pause: 4471283 samples]
Warning: You are running URH in non project mode. All your settings will be lost after closing the program. If you want to keep your settings create a project via File -> New Project. Don't show this hint

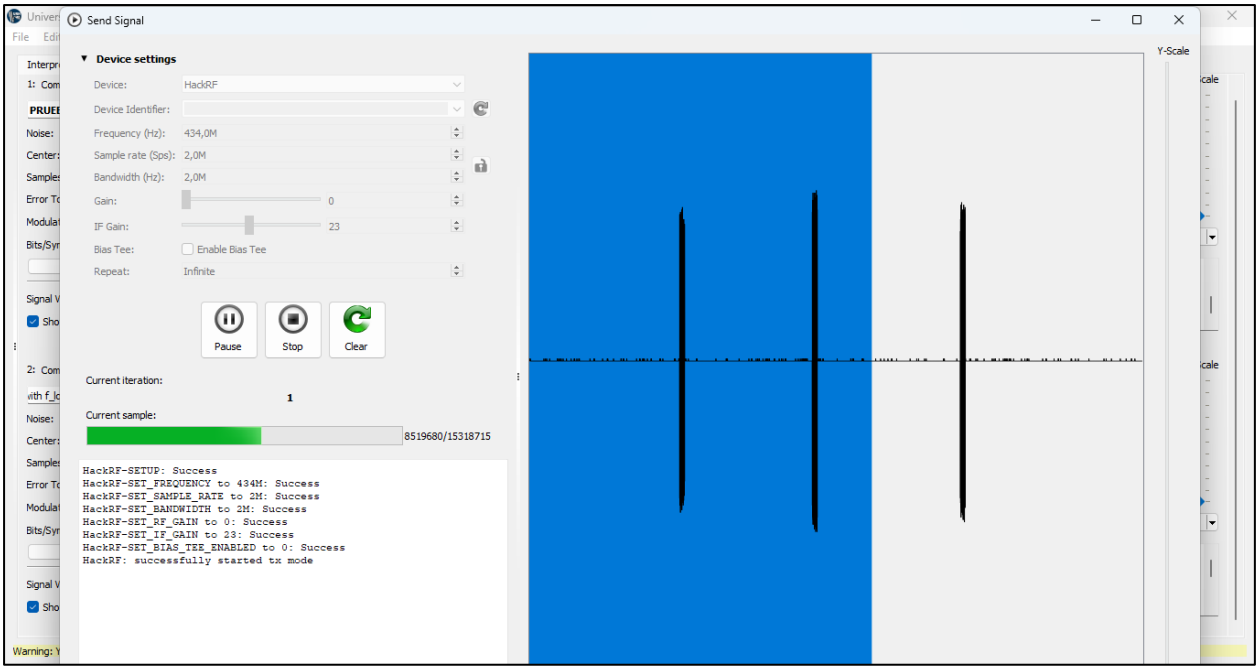

Universal Radio Hacker
File Edit Help
Interpretation Analysis Generator Simulator
1: Complex Signal
PRUEBA2
Noise: 0,0055
Center: 0,0130
Samples/Symbol: 200
Error Tolerance: 11
Modulation: FSK
Bits/Symbol: 1
Autodetect parameters
Signal View: Spectrogram
FFT Window Size:
Data min:
Data max:
Show Signal as Bits
896 selected
1,75MHz
Y-Scale
Zoom in Ctrl++
Zoom out Ctrl+-
Zoom selection
Apply bandpass filter (filter bw=0,08)
Configure filter bandwidth...
Export spectrogram...
You can abort filtering with Esc.
Filter (moving average)
[Pause: 3182624 samples]
Warning: You are running URH in non project mode. All your settings will be lost after closing the program. If you want to keep your settings create a project via File -> New Project. Don't show this hint

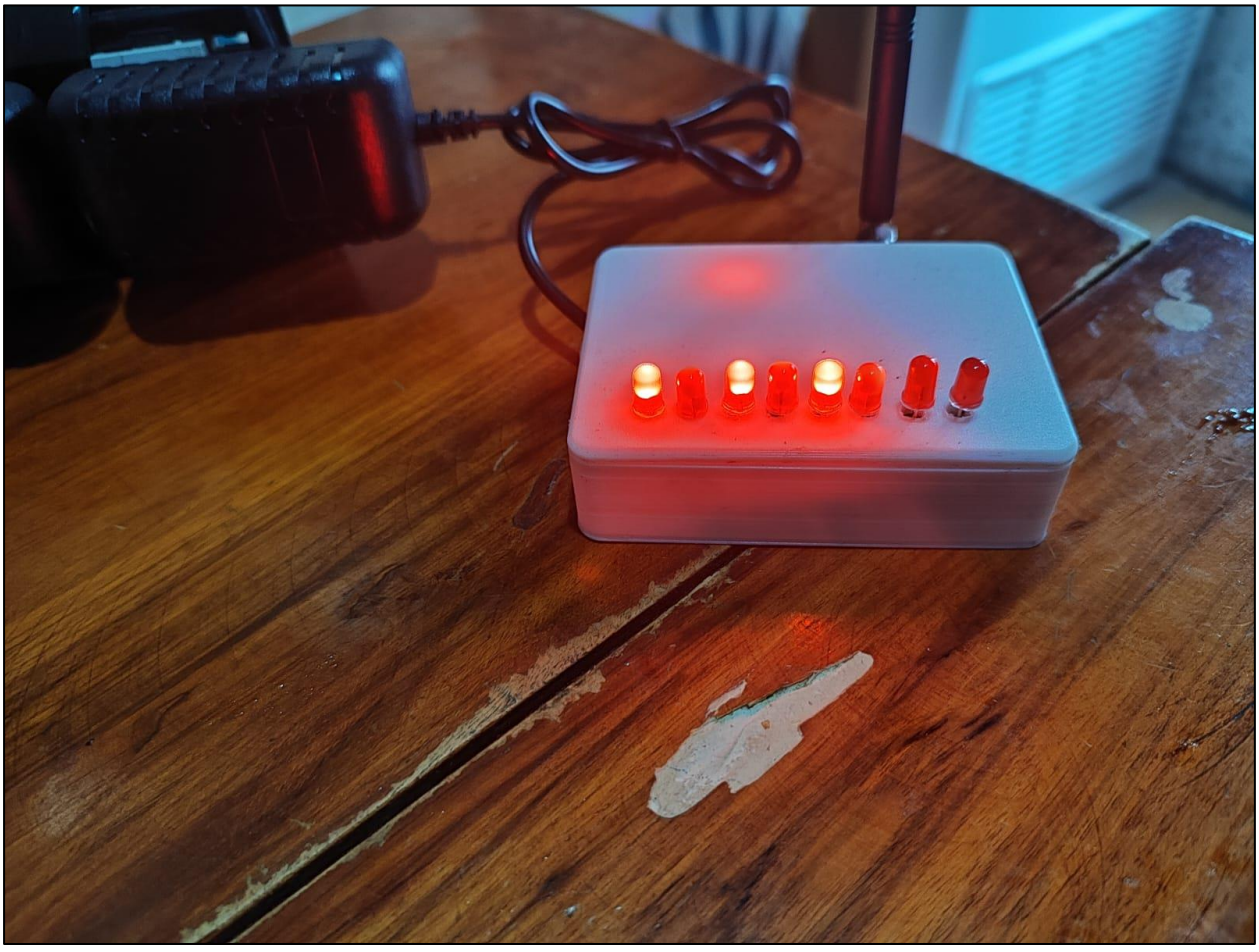

Universal Radio Hacker
File Edit Help
Interpretation Analysis Generator Simulator
Center: 0,0130
Samples/Symbol: 200
Error Tolerance: 11
Modulation: FSK
Bits/Symbol: 1
Autodetect parameters
Signal View: Spectrogram
FFT Window Size:
Data min:
Data max:
Show Signal as Bits
896 selected 1,75MHz
Filter (moving average)
[Pause: 3182624 samples]
2: Complex Signal
with f_low=0,4289 f_high=-0,4467 bw=0,08
Noise: 0,0010
Center: 0,0028
Samples/Symbol: 200
Error Tolerance: 10
Modulation: FSK
Bits/Symbol: 1
Autodetect parameters
Signal View: Demodulated
Show Signal as Bits
Y-Scale
0 selected 0,00 ns -∞ dBm
Filter (moving average)
[Pause: 3182612 samples]
Warning: You are running URH in non project mode. All your settings will be lost after closing the program. If you want to keep your settings create a project via File -> New Project. Don't show this hint


Universal Radio Hacker
File Edit Help
Interpretation Analysis Generator Simulator
Protocols Participants
Enter pattern here
Search
-5,67 dBm
Timestamp: 0,00 ns (+0,00 ns)
New Group
PRUEBA2
PRUEBA2 filtered with f_low=0,428...
View data as: Hex
Decoding: Non Return To Zero (NRZ)
Decoding errors: 0 (0,00%)
Mark diffs in protocol
Show only diffs in protocol
Show only labels in protocol
Analyze Protocol
Bit: 0000010100010101100101011111010 11 Hex: a9a8abaeadafadabab2c2f2ba828acafa3 Decimal: 537009576615644738666821388545003
143 column(s) selected
Message types
Name Edit
Default
Add new message type
Labels for message #1
Name Color Display format Order [Bit/Byte] Value
Warning: You are running URH in non project mode. All your settings will be lost after closing the program. If you want to keep your settings create a project via File -> New Project. Don't show this hint

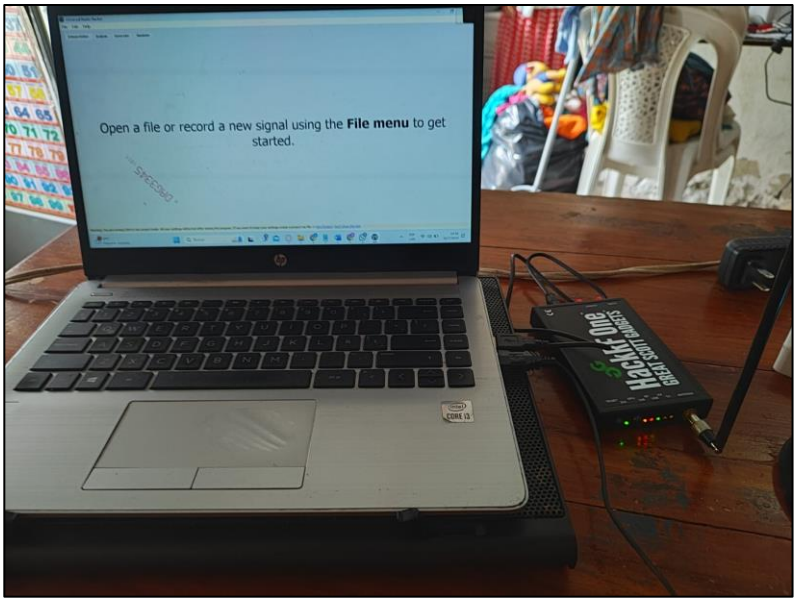

Universal Radio Hacker
File Edit Help
Interpretation Analysis Generator Simulator
1: Complex Signal
PRUEBA2
Replay signal
Noise: 0,0055
Center: 0,0130
Samples/Symbol: 200
Error Tolerance: 11
Modulation: FSK
Bits/Symbol: 1
Autodetect parameters
Signal View: Analog
Show Signal as Bits
Y-Scale
0 selected 0,00 ns -∞ dBm
Filter (moving average)
2: Complex Signal
with f_low=0,4289 f_high=-0,4467 bw=0,08
Noise: 0,0010
Center: 0,0028
Samples/Symbol: 200
Error Tolerance: 10
Modulation: FSK
Bits/Symbol: 1
Autodetect parameters
Signal View: Demodulated
Show Signal as Bits
Warning: You are running URH in non project mode. All your settings will be lost after closing the program. If you want to keep your settings create a project via File -> New Project. Don't show this hint

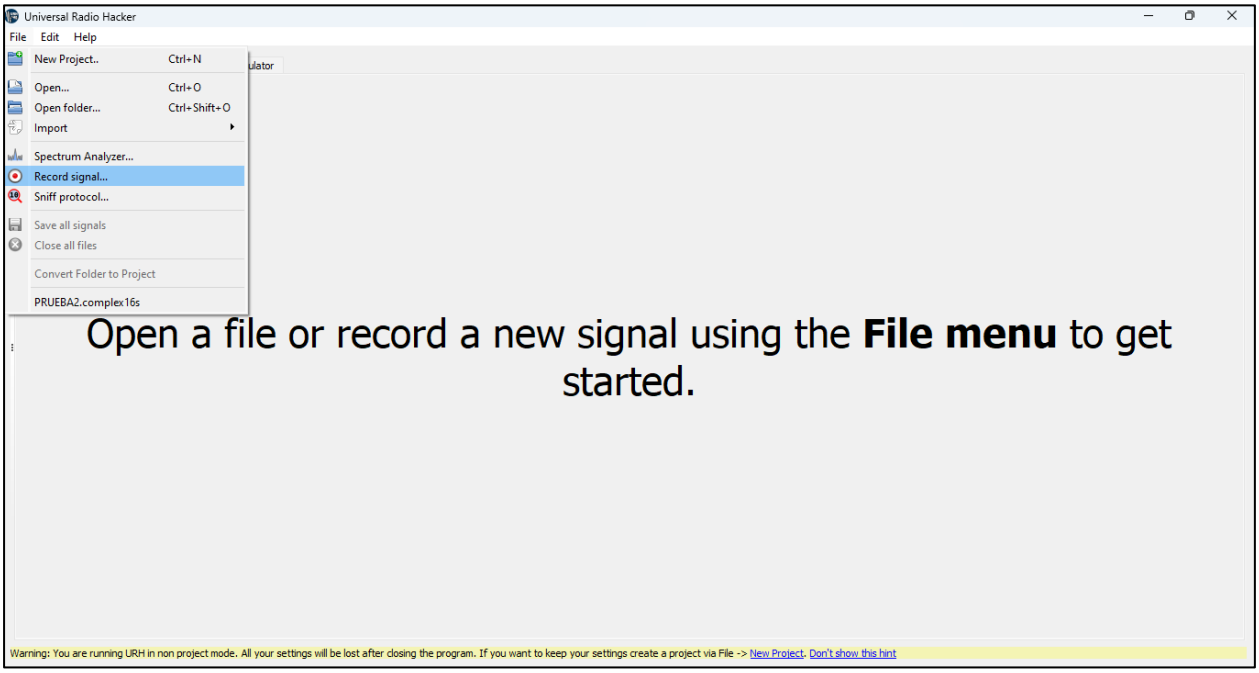

Send Signal
Device settings
Device: HackRF
Device Identifier:
Frequency (Hz): 434,0M
Sample rate (Sps): 2,0M
Bandwidth (Hz): 2,0M
Gain: 0
IF Gain: 23
Bias Tee: Enable Bias Tee
Repeat: Infinite
Start
Stop
Clear
Current iteration:
0
Current sample:
0/15318715
Y-Scale

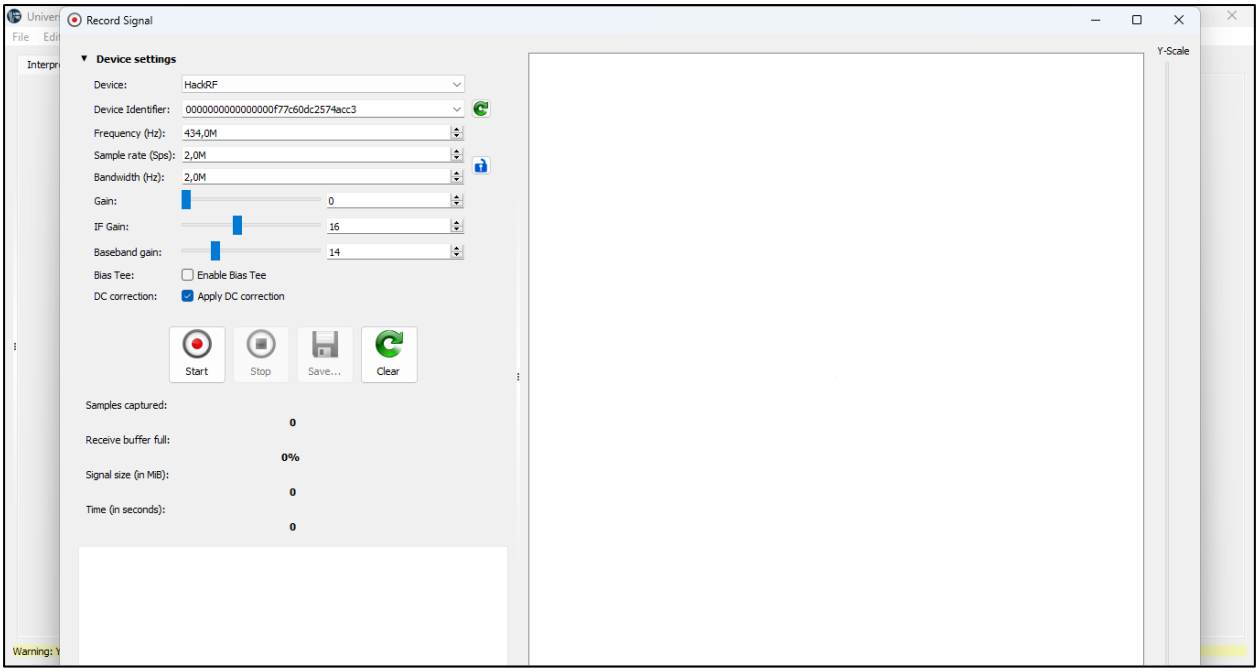

Send Signal
Device settings
Device: HackRF
Device Identifier:
Frequency (Hz): 434,0M
Sample rate (Sps): 2,0M
Bandwidth (Hz): 2,0M
Gain: 0
IF Gain: 23
Bias Tee: Enable Bias Tee
Repeat: Infinite
Pause
Stop
Clear
Current iteration:
1
Current sample:
8519680/15318715
HackRF-SETUP: Success
HackRF-SET_FREQUENCY to 434M: Success
HackRF-SET_SAMPLE_RATE to 2M: Success
HackRF-SET_BANDWIDTH to 2M: Success
HackRF-SET_RF_GAIN to 0: Success
HackRF-SET_IF_GAIN to 23: Success
HackRF-SET_BIAS_TEE_ENABLED to 0: Success
HackRF: successfully started tx mode
Y-Scale

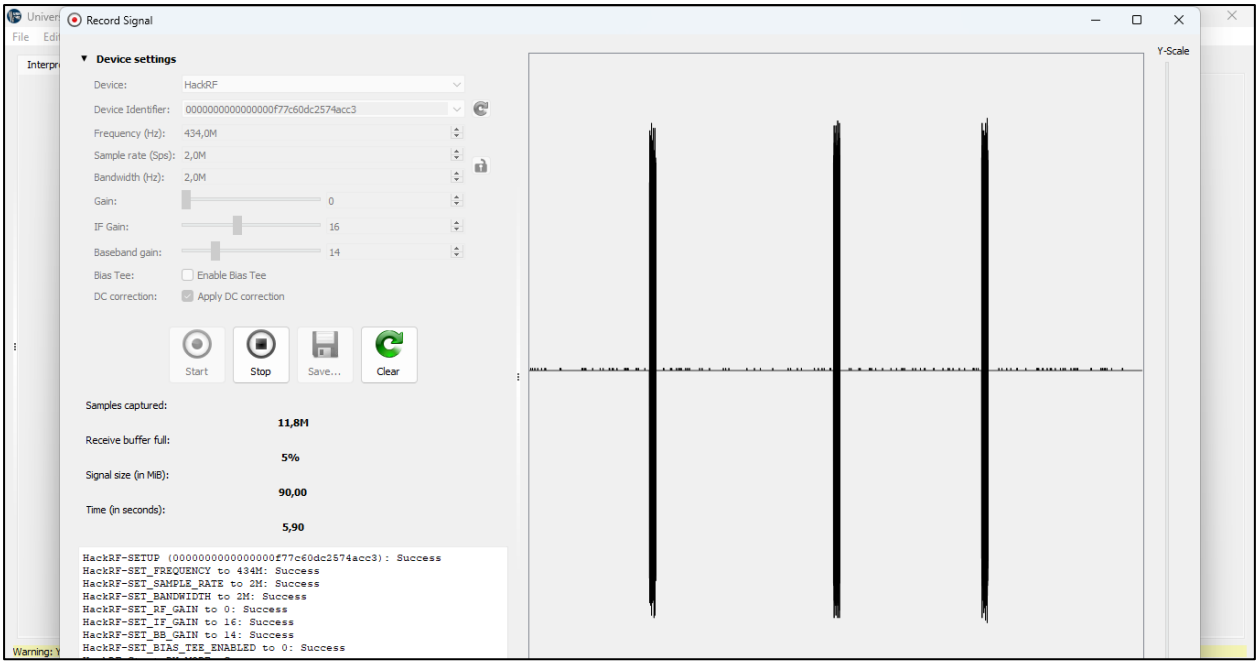


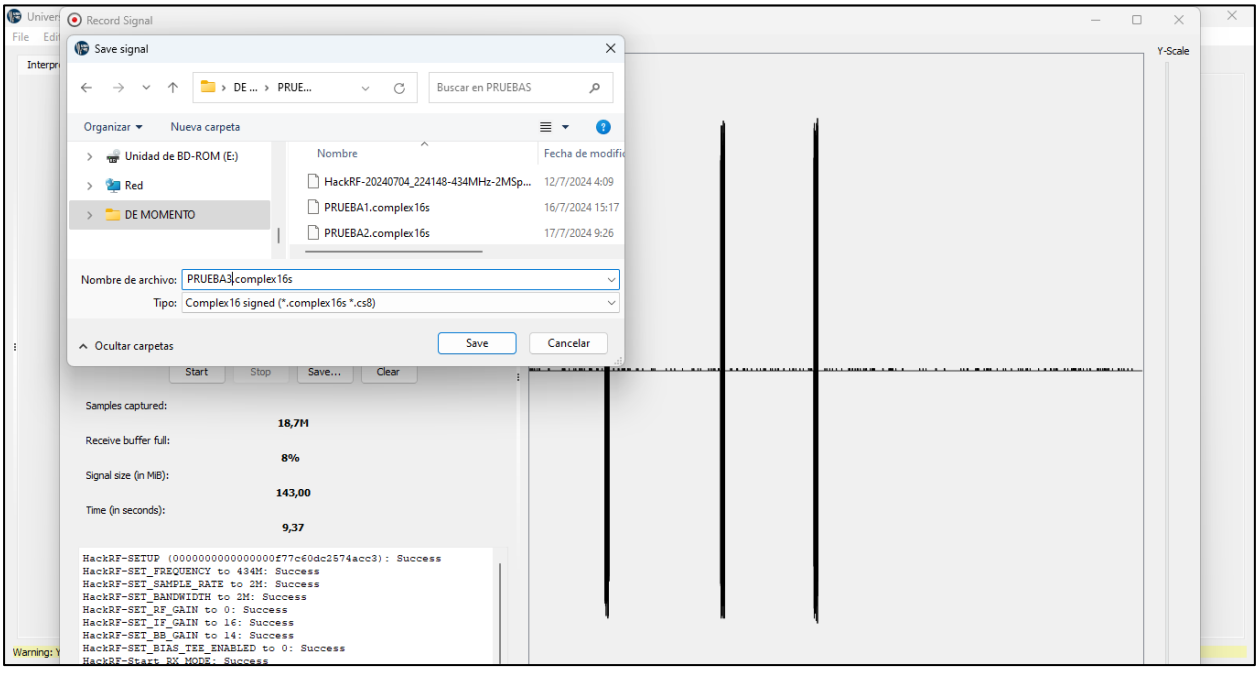
Anexo 20 – Ataque MITM

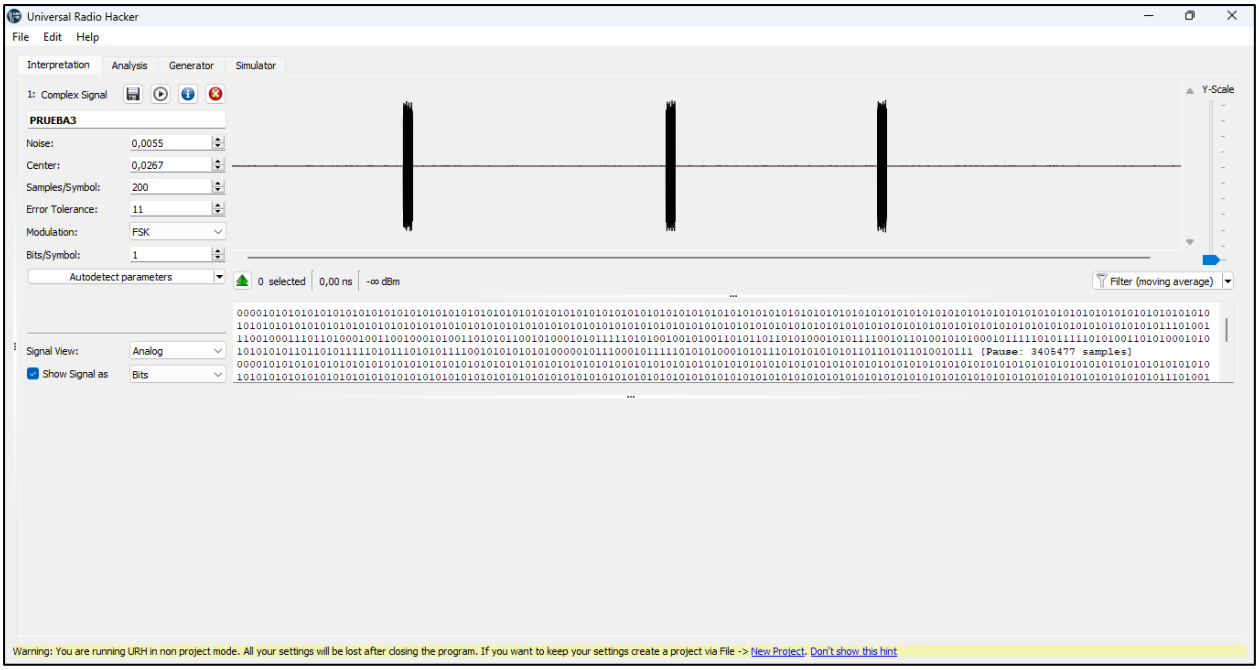


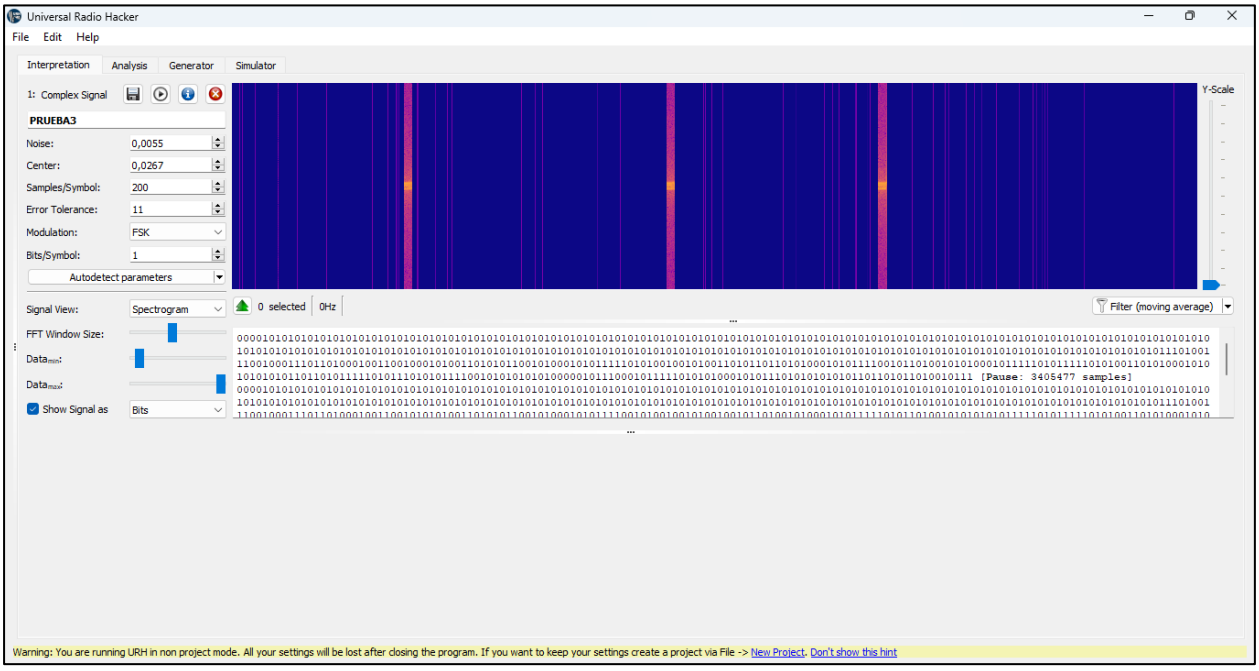


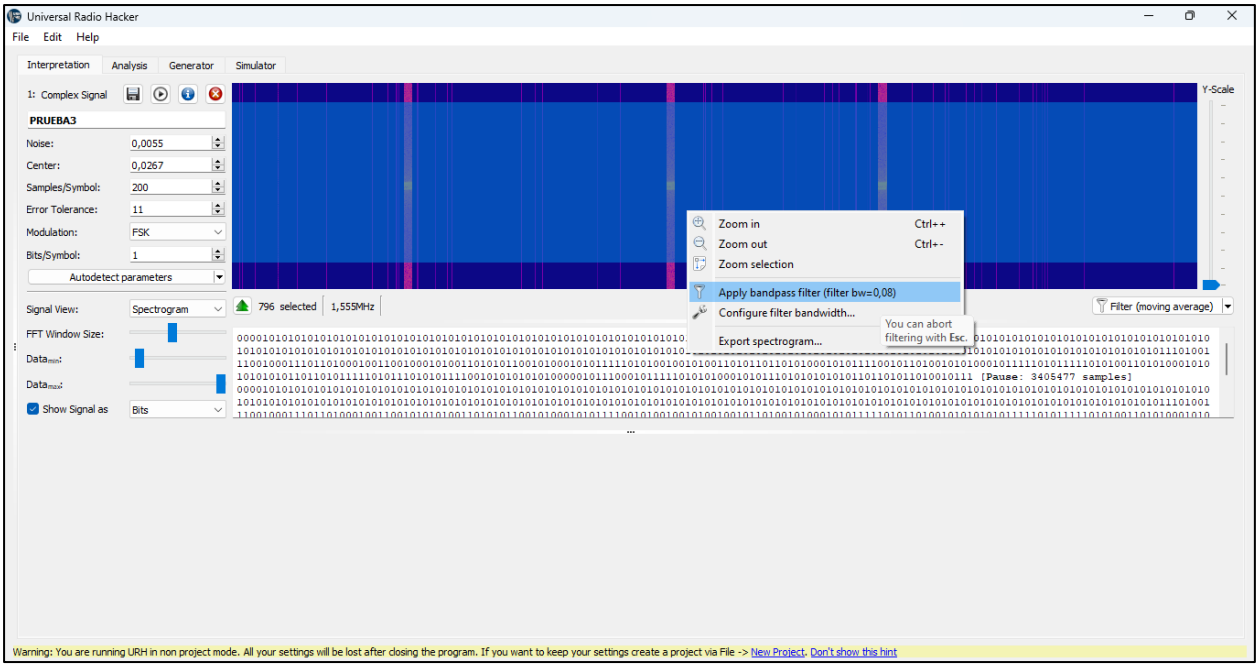

Record Signal
Device settings
Device:
HackRF
Device Identifier:
0000000000000000f77c60dc2574acc3
Frequency (Hz):
434,0M
Sample rate (Sps):
2,0M
Bandwidth (Hz):
2,0M
Gain:
IF Gain:
Baseband gain:
Bias Tee:
Enable Bias Tee
DC correction:
Apply DC correction
Start
Stop
Save...
Clear
Samples captured:
Receive buffer full:
Signal size (in MiB):
Time (in seconds):
Y-Scale


Record Signal
Device settings
Device: HackRF
Device Identifier: 0000000000000000f77c60dc2574acc3
Frequency (Hz): 434,0M
Sample rate (Sps): 2,0M
Bandwidth (Hz): 2,0M
Gain: 0
IF Gain: 16
Baseband gain: 14
Bias Tee: Enable Bias Tee
DC correction: Apply DC correction
Start
Stop
Save...
Clear
Samples captured:
11,8M
Receive buffer full:
5%
Signal size (in MiB):
90,00
Time (in seconds):
5,90
HackRF-SETUP (0000000000000000f77c60dc2574acc3): Success
HackRF-SET_FREQUENCY to 434M: Success
HackRF-SET_SAMPLE_RATE to 2M: Success
HackRF-SET_BANDWIDTH to 2M: Success
HackRF-SET_RF_GAIN to 0: Success
HackRF-SET_IF_GAIN to 16: Success
HackRF-SET_BB_GAIN to 14: Success
HackRF-SET_BIAS_TEE_ENABLED to 0: Success
Y-Scale

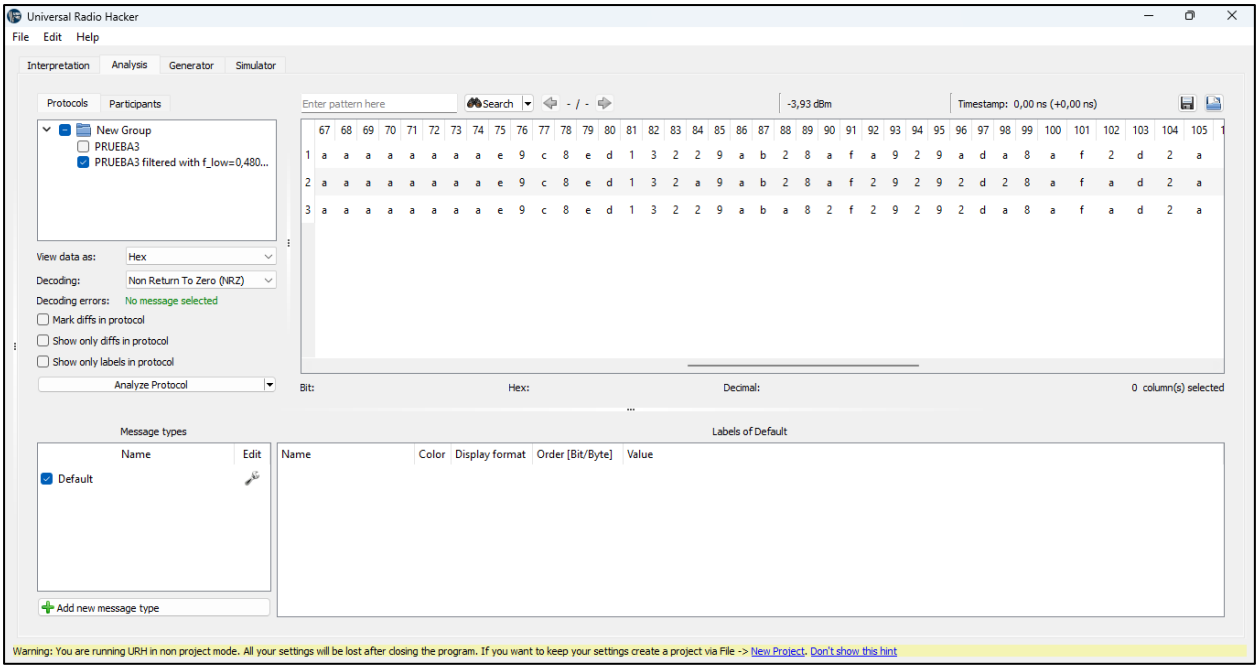

Record Signal
Save signal
DE ... › PRUE...
Buscar en PRUEBAS
Organizar
Nueva carpeta
Unidad de BD-ROM (E:)
Red
DE MOMENTO
Nombre
Fecha de modifi
HackRF-20240704_224148-434MHz-2MSp... 12/7/2024 4:09
PRUEBA1.complex16s 16/7/2024 15:17
PRUEBA2.complex16s 17/7/2024 9:26
Nombre de archivo: PRUEBA3.complex16s
Tipo: Complex16 signed (*.complex16s *.cs8)
Ocultar carpetas
Save
Cancelar
Start
Stop
Save...
Clear
Samples captured:
18,7M
Receive buffer full:
8%
Signal size (in MiB):
143,00
Time (in seconds):
9,37
HackRF-SETUP (0000000000000000f77c60dc2574acc3): Success
HackRF-SET_FREQUENCY to 434M: Success
HackRF-SET_SAMPLE_RATE to 2M: Success
HackRF-SET_BANDWIDTH to 2M: Success
HackRF-SET_RF_GAIN to 0: Success
HackRF-SET_IF_GAIN to 16: Success
HackRF-SET_BB_GAIN to 14: Success
HackRF-SET_BIAS_TEE_ENABLED to 0: Success
HackRF-Start RX MODE: Success
Y-Scale

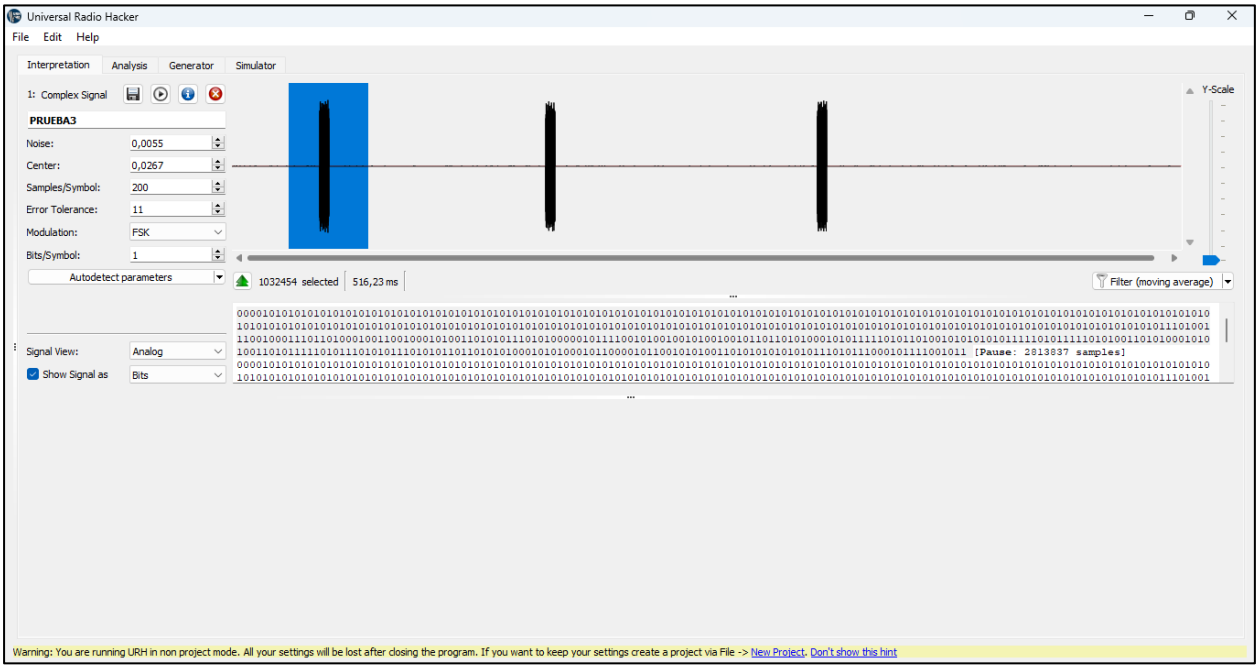

Universal Radio Hacker
File Edit Help
Interpretation Analysis Generator Simulator
1: Complex Signal
PRUEBA3
Noise: 0,0055
Center: 0,0267
Samples/Symbol: 200
Error Tolerance: 11
Modulation: FSK
Bits/Symbol: 1
Autodetect parameters
Y-Scale
0 selected 0,00 ns -∞ dBm
Filter (moving average)
Signal View: Analog
Show Signal as Bits
[Pause: 3405477 samples]
Warning: You are running URH in non project mode. All your settings will be lost after closing the program. If you want to keep your settings create a project via File -> New Project. Don't show this hint

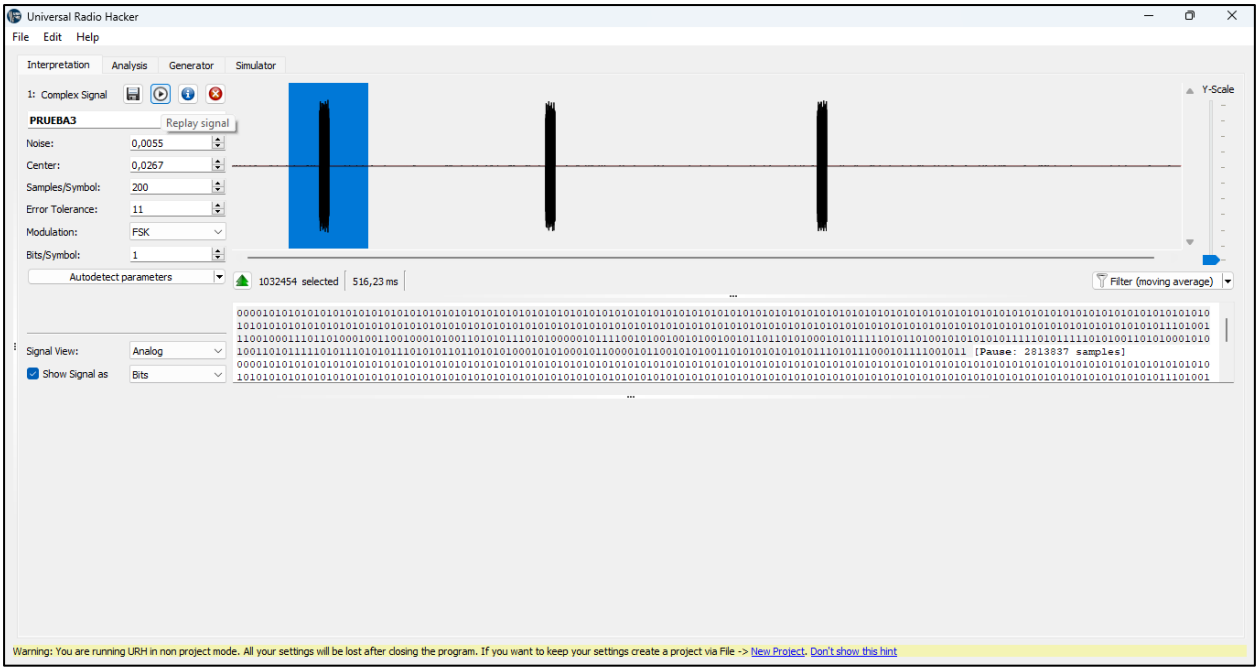

Universal Radio Hacker
File Edit Help
Interpretation Analysis Generator Simulator
1: Complex Signal
PRUEBA3
Noise: 0,0055
Center: 0,0267
Samples/Symbol: 200
Error Tolerance: 11
Modulation: FSK
Bits/Symbol: 1
Autodetect parameters
Y-Scale
Signal View: Spectrogram
FFT Window Size:
Data min:
Data max:
0 selected 0Hz
Filter (moving average)
Show Signal as Bits
[Pause: 3405477 samples]
Warning: You are running URH in non project mode. All your settings will be lost after closing the program. If you want to keep your settings create a project via File -> New Project. Don't show this hint

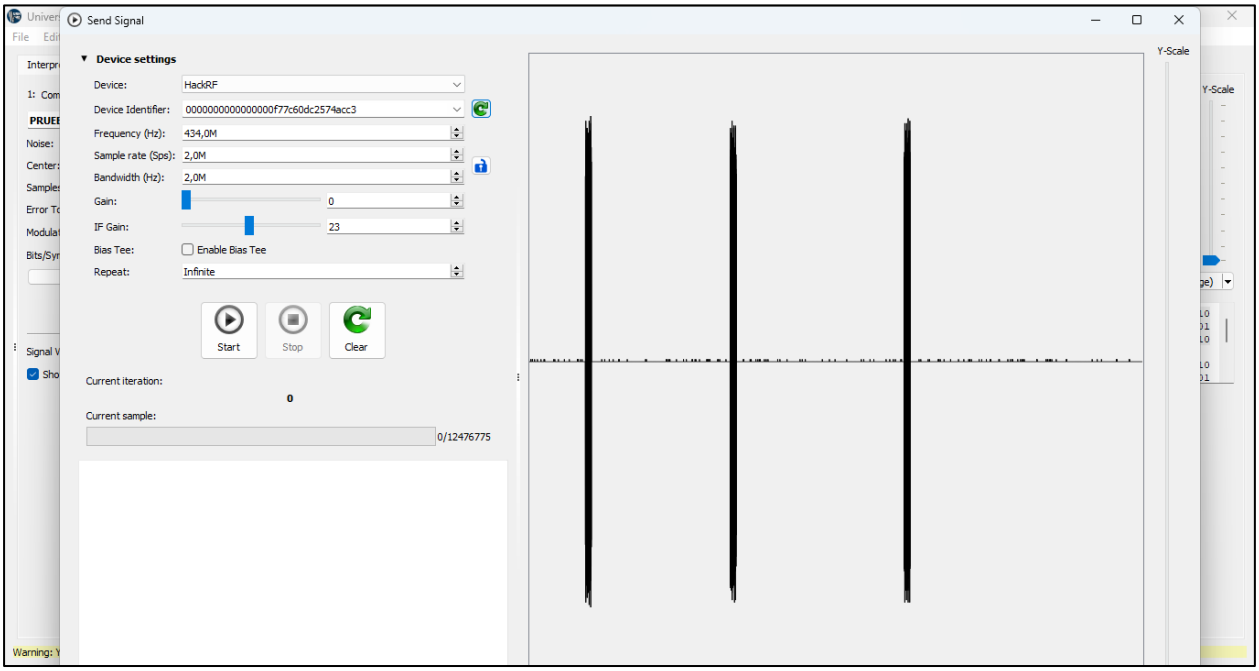

Universal Radio Hacker
File Edit Help
Interpretation Analysis Generator Simulator
1: Complex Signal
PRUEBA3
Noise: 0,0055
Center: 0,0267
Samples/Symbol: 200
Error Tolerance: 11
Modulation: FSK
Bits/Symbol: 1
Autodetect parameters
Signal View: Spectrogram
FFT Window Size:
Data min:
Data max:
Show Signal as Bits
796 selected 1,555MHz
Y-Scale
Zoom in Ctrl++
Zoom out Ctrl+-
Zoom selection
Apply bandpass filter (filter bw=0,08)
Configure filter bandwidth...
Export spectrogram...
You can abort filtering with Esc.
Filter (moving average)
[Pause: 3405477 samples]
Warning: You are running URH in non project mode. All your settings will be lost after closing the program. If you want to keep your settings create a project via File -> New Project. Don't show this hint

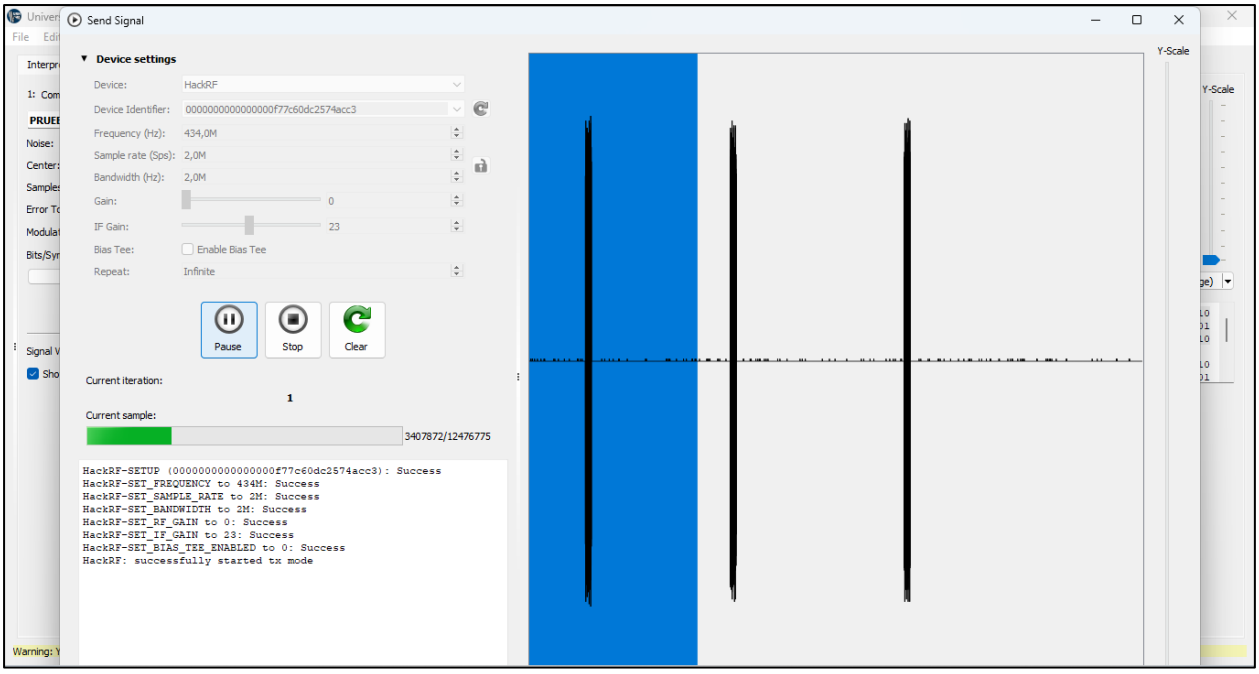

Universal Radio Hacker
File Edit Help
Interpretation Analysis Generator Simulator
Center: 0,0267
Samples/Symbol: 200
Error Tolerance: 11
Modulation: FSK
Bits/Symbol: 1
Autodetect parameters
Signal View: Spectrogram
FFT Window Size:
Data min:
Data max:
Show Signal as Bits
984 selected 1,922MHz
Filter (moving average)
[Pause: 3405477 samples]
2: Complex Signal
with f_low=0,4808 f_high=-0,4808 bw=0,08
Noise: 0,0010
Center: 0,0039
Samples/Symbol: 200
Error Tolerance: 9
Modulation: FSK
Bits/Symbol: 1
Autodetect parameters
Signal View: Demodulated
Show Signal as Bits
Y-Scale
0 selected 0,00 ns -∞ dBm
Filter (moving average)
[Pause: 3405085 samples]
Warning: You are running URH in non project mode. All your settings will be lost after closing the program. If you want to keep your settings create a project via File -> New Project. Don't show this hint

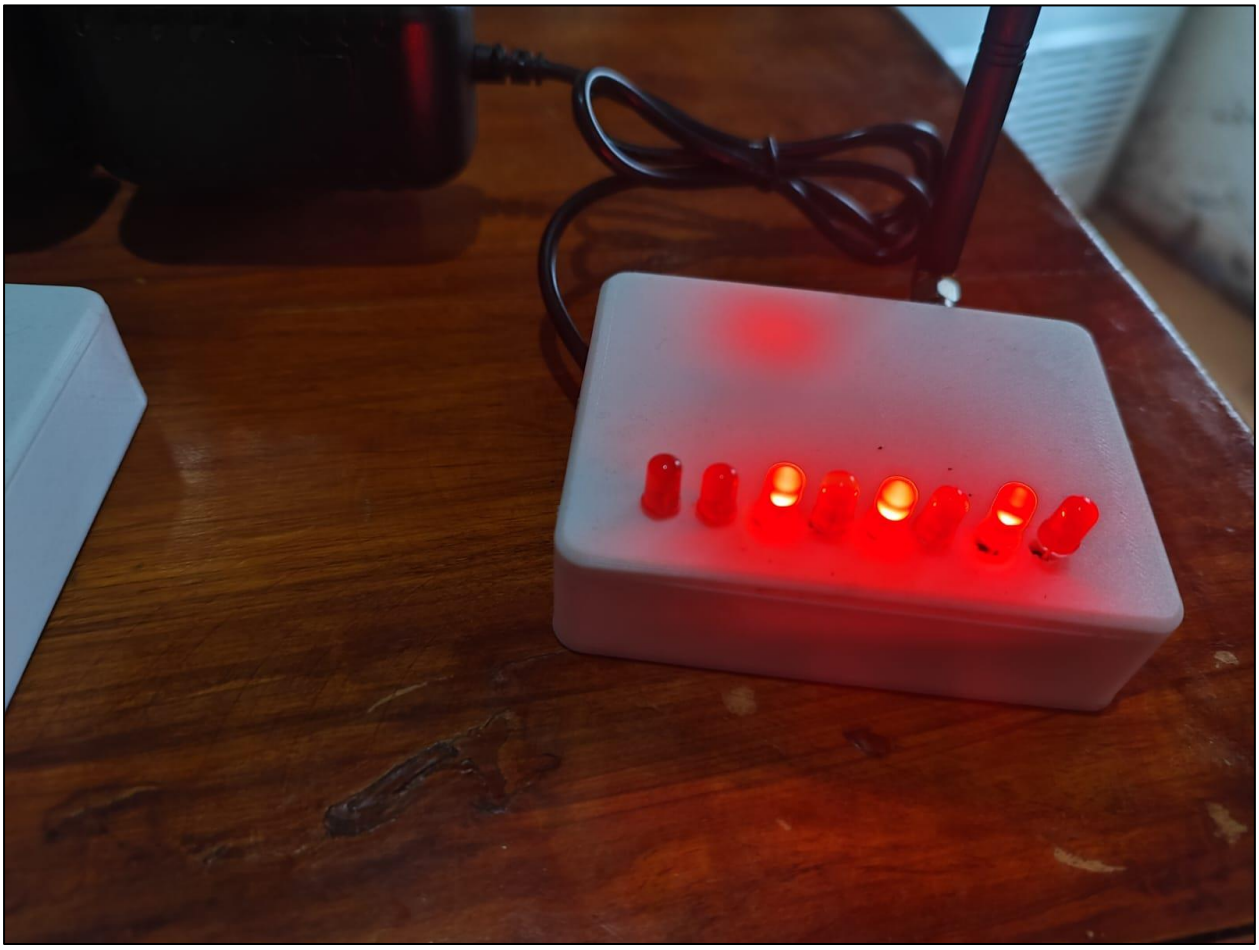

Universal Radio Hacker
File Edit Help
Interpretation Analysis Generator Simulator
Protocols Participants
New Group
PRUEBA3
PRUEBA3 filtered with f_low=0,480...
Enter pattern here
Search
-3,93 dBm
Timestamp: 0,00 ns (+0,00 ns)
View data as: Hex
Decoding: Non Return To Zero (NRZ)
Decoding errors: No message selected
Mark diffs in protocol
Show only diffs in protocol
Show only labels in protocol
Analyze Protocol
Bit:
Hex:
Decimal:
0 column(s) selected
Message types
Name
Edit
Default
Add new message type
Labels of Default
Name
Color
Display format
Order [Bit/Byte]
Value
Warning: You are running URH in non project mode. All your settings will be lost after closing the program. If you want to keep your settings create a project via File -> New Project. Don't show this hint


Universal Radio Hacker
File Edit Help
Interpretation Analysis Generator Simulator
1: Complex Signal
PRUEBA3
Noise: 0,0055
Center: 0,0267
Samples/Symbol: 200
Error Tolerance: 11
Modulation: FSK
Bits/Symbol: 1
Autodetect parameters
Signal View: Analog
Show Signal as Bits
Y-Scale
1032454 selected
516,23 ms
Filter (moving average)
[Pause: 2813837 samples]
Warning: You are running URH in non project mode. All your settings will be lost after closing the program. If you want to keep your settings create a project via File -> New Project. Don't show this hint


Universal Radio Hacker
File Edit Help
Interpretation Analysis Generator Simulator
1: Complex Signal
PRUEBA3
Replay signal
Noise: 0,0055
Center: 0,0267
Samples/Symbol: 200
Error Tolerance: 11
Modulation: FSK
Bits/Symbol: 1
Autodetect parameters
Y-Scale
1032454 selected
516,23 ms
Filter (moving average)
Signal View: Analog
Show Signal as Bits
[Pause: 2813837 samples]
Warning: You are running URH in non project mode. All your settings will be lost after closing the program. If you want to keep your settings create a project via File -> New Project. Don't show this hint


Send Signal
Device settings
Device: HackRF
Device Identifier: 0000000000000000f77c60dc2574acc3
Frequency (Hz): 434,0M
Sample rate (Sps): 2,0M
Bandwidth (Hz): 2,0M
Gain: 0
IF Gain: 23
Bias Tee: Enable Bias Tee
Repeat: Infinite
Start
Stop
Clear
Current iteration:
0
Current sample:
0/12476775
Y-Scale


Send Signal
Device settings
Device:
HackRF
Device Identifier:
0000000000000000f77c60dc2574acc3
Frequency (Hz):
434,0M
Sample rate (Sps):
2,0M
Bandwidth (Hz):
2,0M
Gain:
IF Gain:
Bias Tee:
Enable Bias Tee
Repeat:
Infinite
Pause
Stop
Clear
Current iteration:
1
Current sample:
3407872/12476775
HackRF-SETUP (0000000000000000f77c60dc2574acc3): Success
HackRF-SET_FREQUENCY to 434M: Success
HackRF-SET_SAMPLE_RATE to 2M: Success
HackRF-SET_BANDWIDTH to 2M: Success
HackRF-SET_RF_GAIN to 0: Success
HackRF-SET_IF_GAIN to 23: Success
HackRF-SET_BIAS_TEE_ENABLED to 0: Success
HackRF: successfully started tx mode
Y-Scale



Anexo 21 – Manual de práctica para estudiantes

Facultad de Sistemas y Telecomunicaciones
Telecomunicaciones

INFORMACIÓN GENERAL					
Carrera:	Telecomunicaciones				
Asignatura:	Comunicaciones Inalámbricas – Seguridad de Redes Inalámbricas				
Estudiantes:	Anibal Andres Gutierrez Alvarado				
Período Lectivo:	2024-1	**Modalidad:**	Presencial	**Curso:**	8vo

INFORMACIÓN DE LA PRÁCTICA	
Práctica N°:	1
Tema de la Práctica:	VULNERABILIDADES EN LA CAPA DE ENLACE DE DATOS DEL MODELO OSI
Laboratorio / taller donde se desarrolló la práctica:	LABORATORIO DE TELECOMUNICACIONES

INFORME

OBJETIVOS:

Comprender las principales vulnerabilidades en la capa de enlace de datos, especialmente aquellas relacionadas con eavesdropping, replay attacks y man-in-the-middle (MITM).

Realizar ataques de eavesdropping, replay y MITM en un entorno controlado utilizando el módulo didáctico para demostrar cómo estos ataques pueden comprometer la seguridad de la comunicación entre el nodo CLIENTE y el nodo SERVIDOR.

Investigar técnicas de seguridad para mitigar las vulnerabilidades identificadas, como encriptación, autenticación y el uso de timestamps.

Documentar el proceso, los resultados y las conclusiones de los experimentos, presentando los hallazgos de manera clara.

MATERIALES:

MÓDULO:	**INSUMOS / MATERIALES:**
Módulo didáctico.	Nodo CLIENTE Nodo SERVIDOR HackRF One Computadora Software URH (Universal Radio Hacker)

FUNDAMENTO TEÓRICO

La capa de enlace de datos del modelo OSI es responsable de la transferencia de datos entre dos nodos adyacentes en una red. Esta capa incluye protocolos y mecanismos que garantizan una comunicación fiable y eficiente, gestionando la detección y corrección de errores, así como el control de flujo y acceso al medio. Sin embargo, las comunicaciones en esta capa son vulnerables a diversos tipos de ataques, especialmente en entornos inalámbricos.

Vulnerabilidades en la Capa de Enlace de Datos

La intercepción de datos, o eavesdropping, ocurre cuando un atacante escucha las transmisiones entre dos nodos. En un entorno RF, la señal se propaga por el aire, lo que facilita su captura por cualquier dispositivo dentro del alcance.

En un ataque de repetición, el atacante captura tramas de datos válidas y las retransmite para replicar acciones autorizadas. Esto puede llevar a la repetición de comandos o la reutilización de autenticaciones.

En un ataque MITM, el atacante intercepta y potencialmente modifica las comunicaciones entre dos nodos. El atacante se sitúa entre el nodo CLIENTE y el nodo SERVIDOR, alterando o leyendo los datos transmitidos sin que las partes legítimas lo detecten.

Realización de Ataques

Eavesdropping: Captura de las transmisiones RF entre los nodos para demostrar la capacidad de interceptar datos sin autorización.

Replay Attack: Repetición de tramas capturadas para mostrar cómo las acciones pueden ser replicadas y el sistema comprometido.

MITM: Interposición de un nodo atacante entre el CLIENTE y el SERVIDOR para interceptar y modificar las comunicaciones.

Técnicas de Seguridad

Los datos transmitidos se cifran utilizando algoritmos como AES para prevenir su lectura por parte de interceptores no autorizados.

Los timestamps se usan para asegurar que cada trama sea única y evitar ataques de repetición.

La autenticación mutua permite que el nodo SERVIDOR no pueda ser engañado, debido que para recibir información primero deben autenticar al nodo CLIENTE.

Configuración del Entorno

Configuración de los dispositivos nodo CLIENTE y nodo SERVIDOR en el laboratorio de telecomunicaciones para simular una red punto a punto en un entorno controlado.

Uso del equipo SDR (Software Defined Radio), software SDR y sus herramientas de captura de paquetes para monitorear y analizar la comunicación por RF (Radiofrecuencia).

ESCENARIO DE PRUEBA

La Universidad Estatal Península de Santa Elena (UPSE) está conformada por 7 facultades, la Facultad de Ciencias Administrativas, la Facultad de Ciencias Sociales y de la Salud, la Facultad de Ciencias de la Educación e Idiomas, la Facultad de Sistemas y Telecomunicaciones, la Facultad de Ciencias de la Ingeniería, la Facultad de Ciencias del Mar y la Facultad de Ciencias Agrarias, adicional tiene un departamento redes en donde se encuentran todos los equipos servidores que administran la red de la UPSE, cada facultad cuenta con una secretaría física en donde se guardar documentos importantes de cada carrera.

Las 7 secretarias y el departamento de redes cuentan con un sistema de apertura por RF, es decir que cada uno de estos lugares tiene una llave por RF que facilita la apertura en comparación al sistema fisco tradicional de llaves.

Para emular este escenario se trabaja con el módulo didáctico asignado para esta práctica. El nodo CLIENTE consta de 8 pulsadores, cada pulsador emula la llave RF de cada lugar mencionado,

es decir, si lo vemos de izquierda a derecha la asignación de los pulsadores se aprecia en la siguiente tabla.

Llave de la secretaría - Facultad de Ciencias Administrativas	Pulsador 1
Llave de la secretaría - Facultad de Ciencias Sociales y de la Salud	Pulsador 2
Llave de la secretaría - Facultad de Ciencias de la Educación e Idiomas	Pulsador 3
Llave de la secretaría - Facultad de Sistemas y Telecomunicaciones	Pulsador 4
Llave de la secretaría - Facultad de Ciencias de la Ingeniería	Pulsador 5
Llave de la secretaría - Facultad de Ciencias del Mar	Pulsador 6
Llave de la secretaría - Facultad de Ciencias Agrarias	Pulsador 7
Llave - Departamento de Redes	Pulsador 8

El nodo SERVIDOR consta de 8 diodos LED, cada diodo LED emula la apertura de cada puerta de los lugares mencionados, es decir, si lo vemos de izquierda a derecha la asignación de los diodos LED se aprecia en la siguiente tabla.

Puerta de la secretaría - Facultad de Ciencias Administrativas	LED 1
Puerta de la secretaría - Facultad de Ciencias Sociales y de la Salud	LED 2
Puerta de la secretaría - Facultad de Ciencias de la Educación e Idiomas	LED 3
Puerta de la secretaría - Facultad de Sistemas y Telecomunicaciones	LED 4
Puerta de la secretaría - Facultad de Ciencias de la Ingeniería	LED 5
Puerta de la secretaría - Facultad de Ciencias del Mar	LED 6
Puerta de la secretaría - Facultad de Ciencias Agrarias	LED 7
Puerta - Departamento de Redes	LED 8

El dispositivo HackRF One es utilizado como atacante y el software URH es utilizado para el proceso de los ataques.

La meta de la práctica obtener las 8 llaves RF y por lo menos abrir 3 de estos lugares en mención para evaluar la vulnerabilidad del sistema de apertura.

Al final debe de proponer un tipo de seguridad para mitigar las vulnerabilidades en el sistema de apertura de los departamentos.

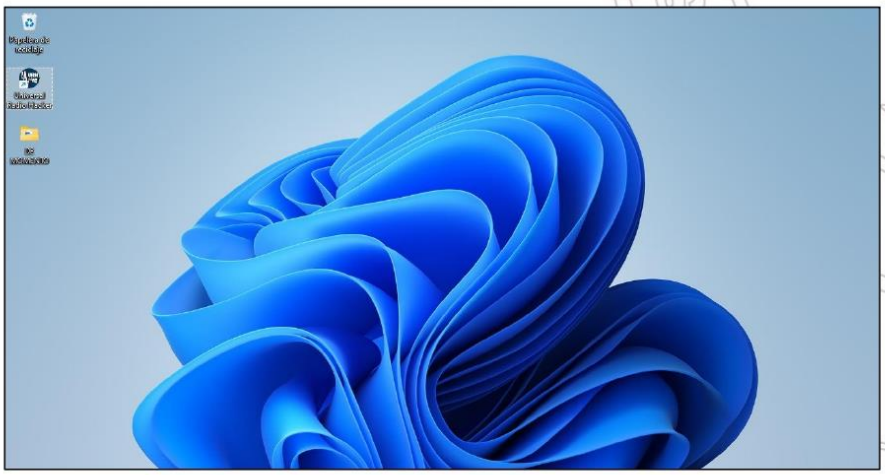
Nota: Es importante desconectar los nodos de la corriente luego de cada prueba para evitar volcados de memorias.

CÁLCULOS / SIMULACIÓN / PROCEDIMIENTO

Se conecta el dispositivo HackRF One a la computadora.

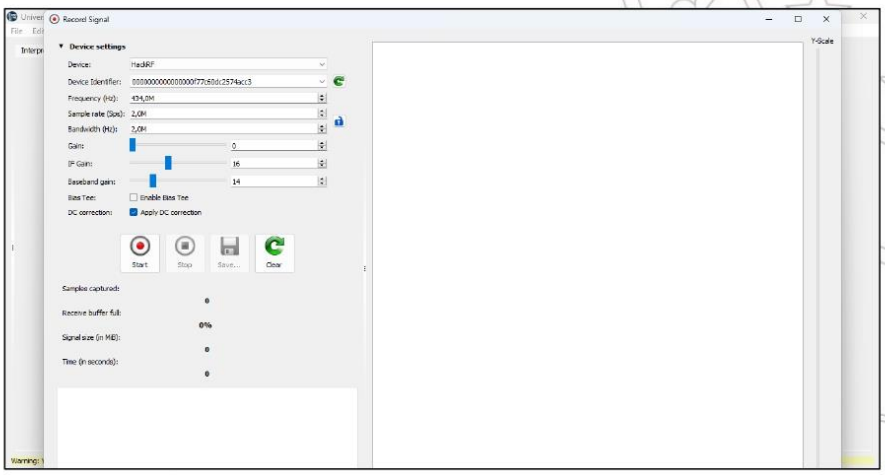
Se conectan los nodos CLIENTE/SERVIDOR a la corriente.

Abrimos el programa Universal Radio Hacker (URH)



En la pestaña File seleccionamos Record Signal.

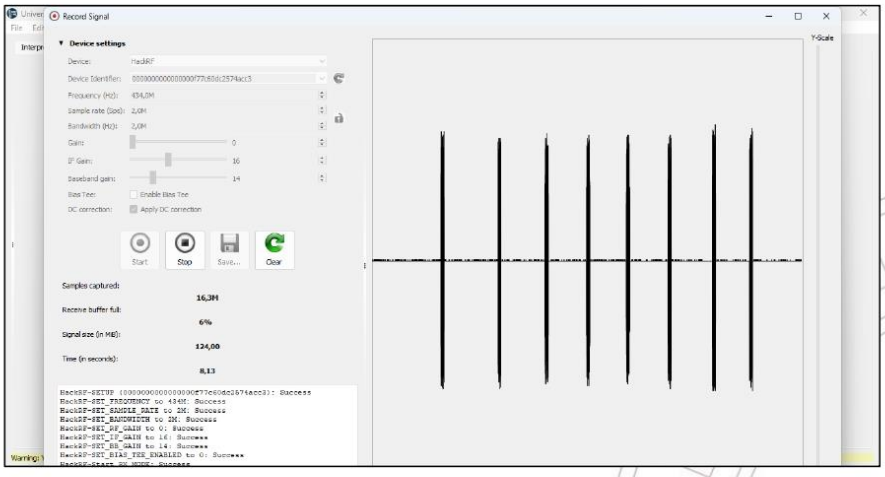
Se abre la ventana Record Signal aquí se procede a configurar el equipo SDR, en Device ubicamos HackRF, luego damos clic en la flecha verde que está en Device Identifier para que el programa pueda identificar nuestro dispositivo SDR, en Frequency (Hz) se configura la frecuencia que en este caso es de 434 MHz, debido a que, los nodos CLIENTE/SERVIDOR trabajan a esa frecuencia. Al presionar Start empieza la captura de datos en la frecuencia de 434 MHz.



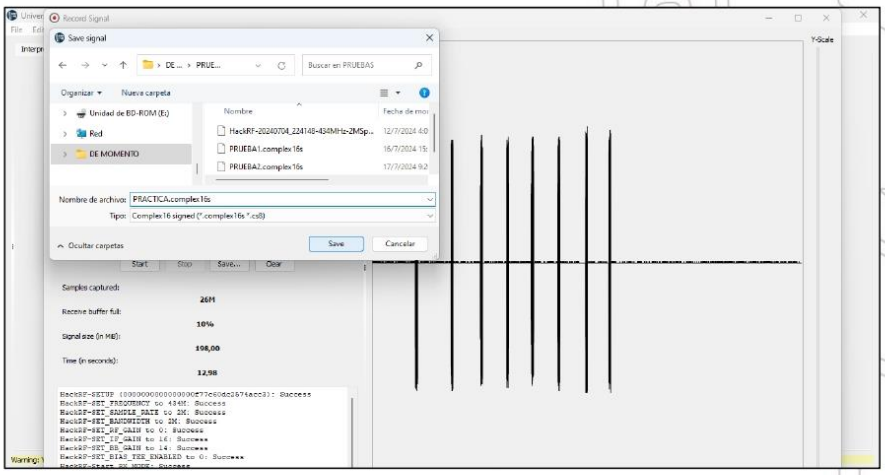
Una vez que empiece la captura de datos, se procede a presionar los pulsadores de izquierda a derecha tomando en cuenta la siguiente tabla.

Llave de la secretaría - Facultad de Ciencias Administrativas	Pulsador 1
Llave de la secretaría - Facultad de Ciencias Sociales y de la Salud	Pulsador 2
Llave de la secretaría - Facultad de Ciencias de la Educación e Idiomas	Pulsador 3
Llave de la secretaría - Facultad de Sistemas y Telecomunicaciones	Pulsador 4
Llave de la secretaría - Facultad de Ciencias de la Ingeniería	Pulsador 5
Llave de la secretaría - Facultad de Ciencias del Mar	Pulsador 6
Llave de la secretaría - Facultad de Ciencias Agrarias	Pulsador 7
Llave - Departamento de Redes	Pulsador 8

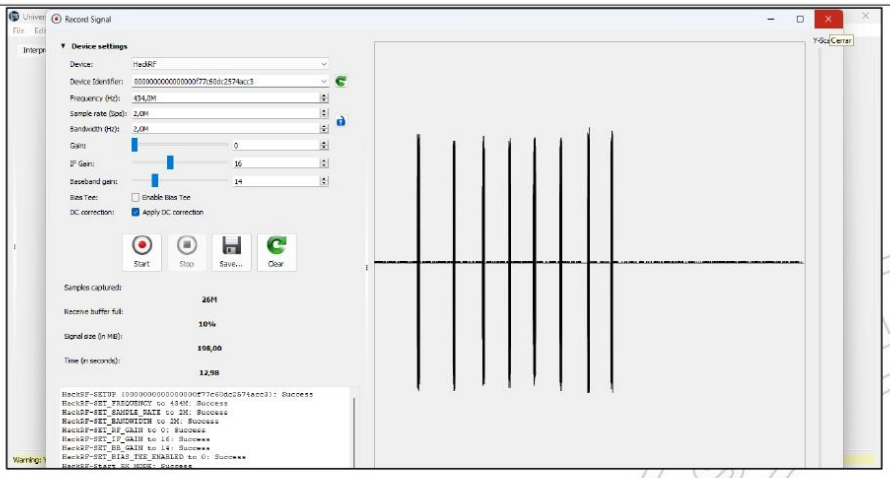
Al terminar de presionar los pulsadores, damos en Stop para detener la captura.



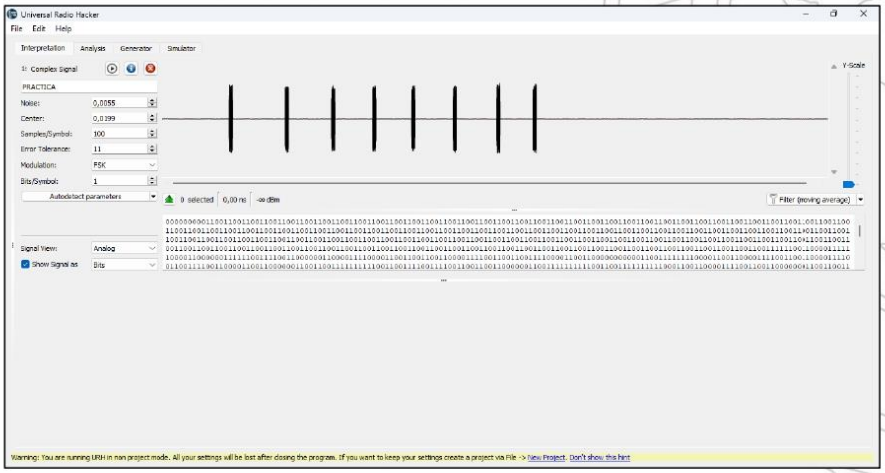
Cuando se detiene la captura tenemos la opción Save que permite guardar los datos capturados, en este caso lo guardamos con el nombre PRACTICA en alguna carpeta previamente creada.



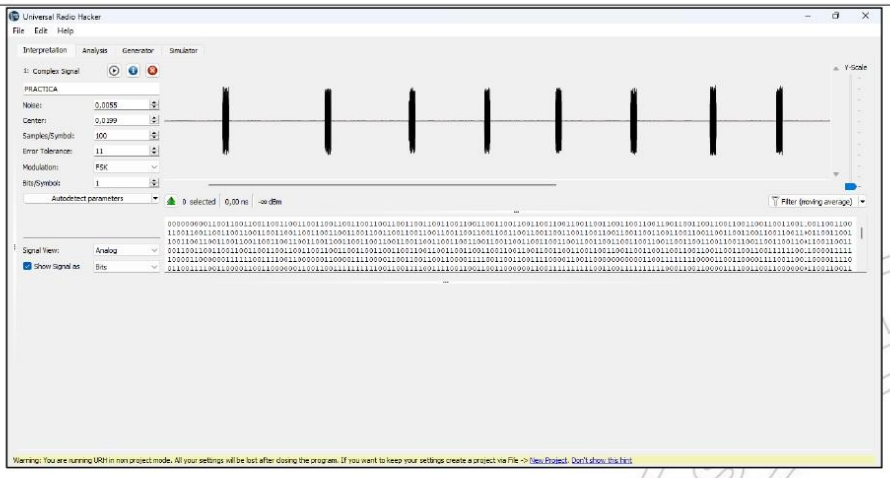
Una vez que se guarde el archivo podemos cerrar la ventana Record Signal.



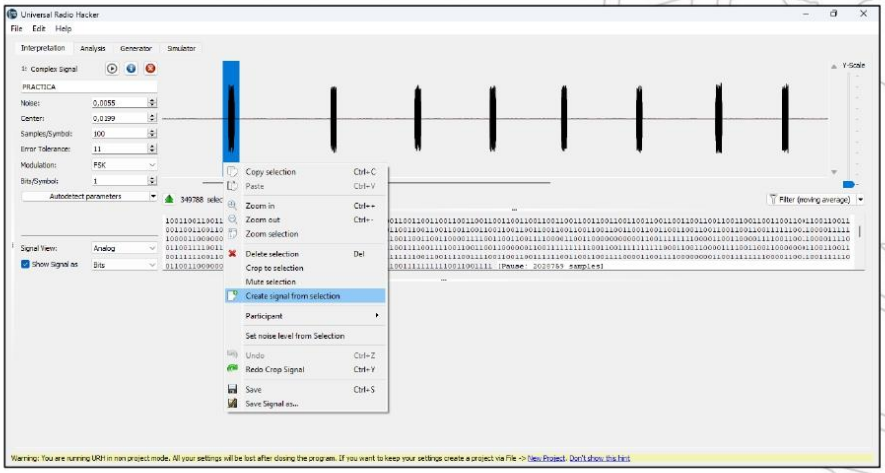
Al cerrar la ventana Record Signal inmediatamente nos aparece la pantalla de Interpretation en donde vamos a trabaja con la señal capturada.



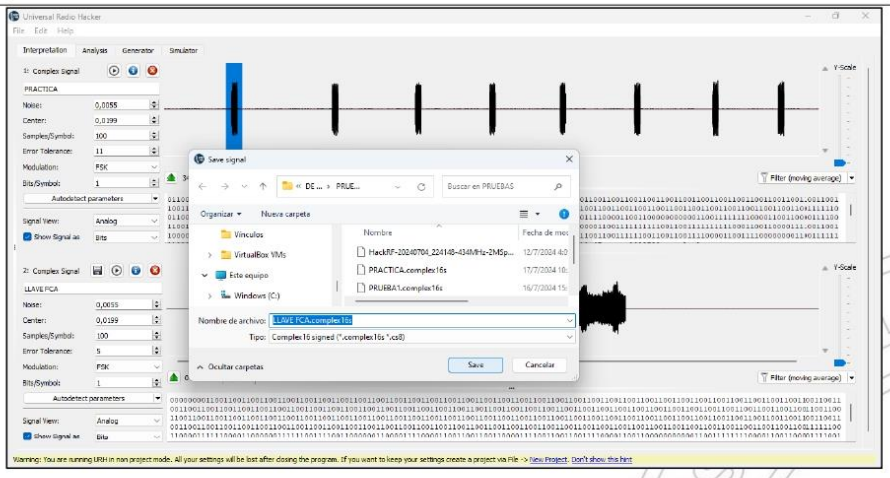
Con el mouse podemos hacer un poco de zoom para ajustar la señal y poder visualizarla de mejor manera.



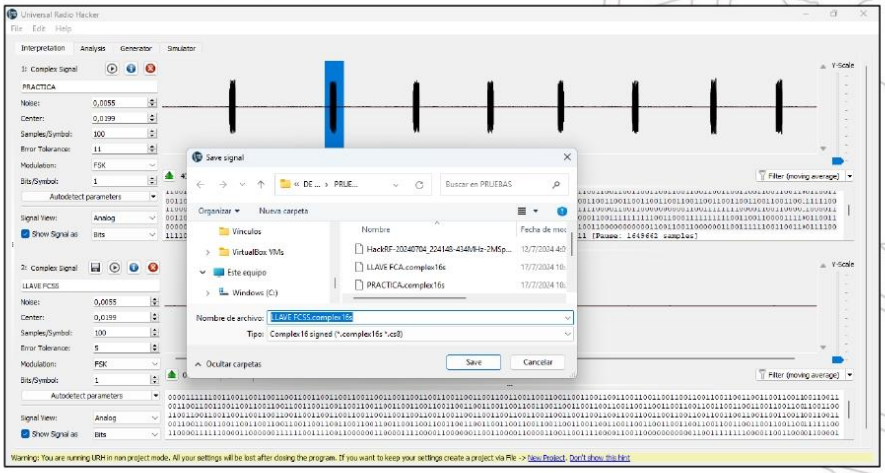
Podemos observar que tenemos las ocho cadenas de caracteres capturadas ahora vamos a seleccionar la primera y damos Create signal from selection para crear la primera llave.



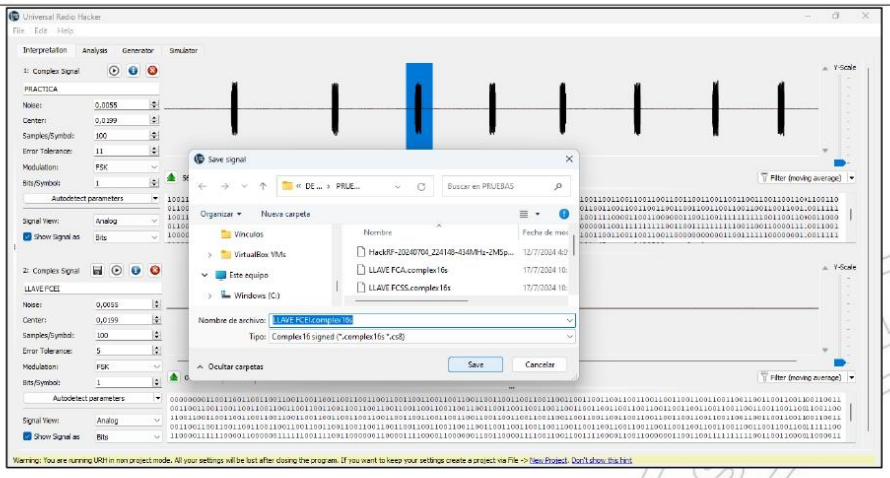
Nos aparecerá la señal creada en la parte de abajo procedemos a cambiarle el nombre tomando en cuenta la tabla de la asignación de los pulsadores para la emulación de cada facultad. En este caso la primera es la llave de la secretaría - Facultad de Ciencias Administrativas y la renombramos como LLAVE FCA, y pulsamos el icono del disquete para luego dar a Save.



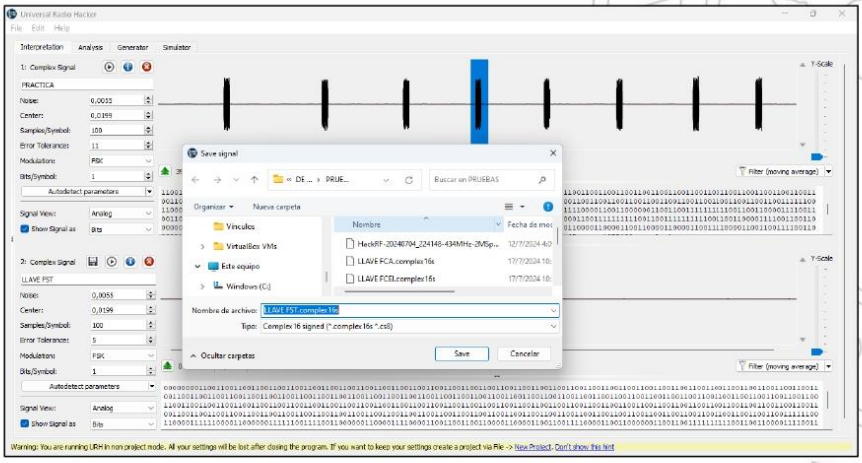
La segunda es la llave de la secretaría - Facultad de Ciencias Sociales y de la Salud, la renombramos como LLAVE FCSS, y pulsamos el icono del disquete para luego dar a Save.



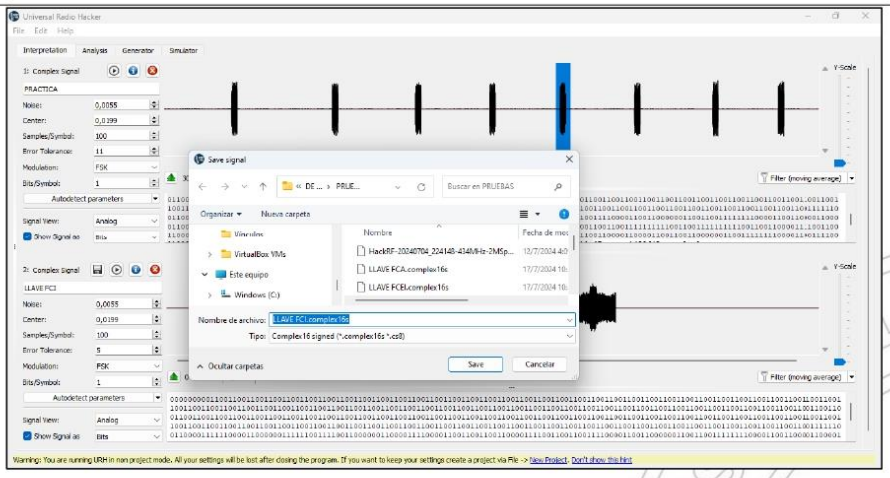
La tercera es la llave de la secretaría - Facultad de Ciencias de la Educación e Idiomas, la renombramos como LLAVE FCEI, y pulsamos el icono del disquete para luego dar a Save.



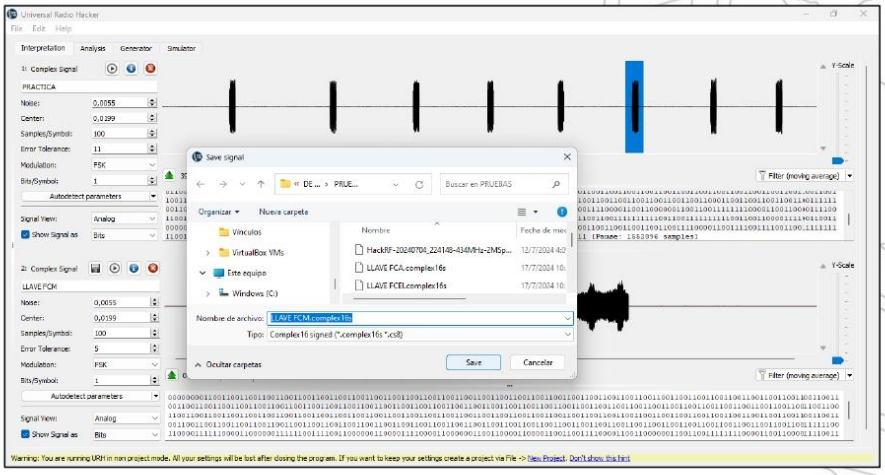
La cuarta es la llave de la secretaría - Facultad de Sistemas y Telecomunicaciones, la renombramos como LLAVE FST, y pulsamos el icono del disquete para luego dar a Save.



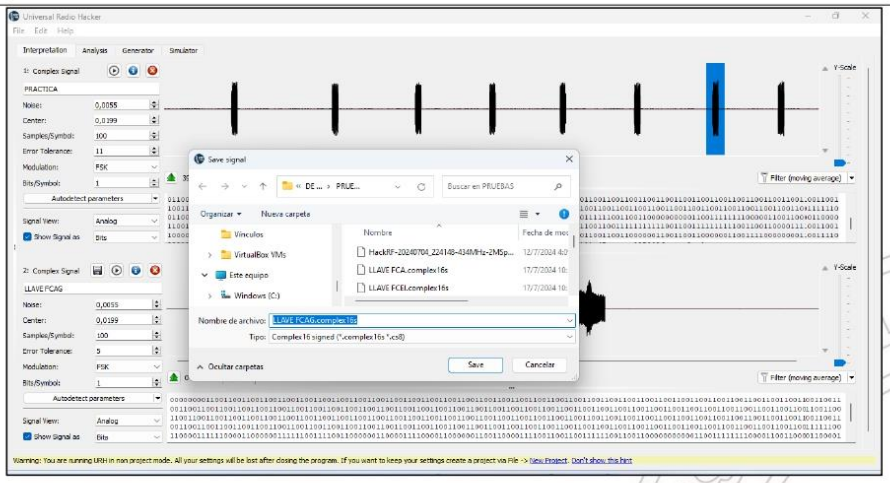
La quinta es la llave de la secretaría - Facultad de Ciencias de la Ingeniería, la renombramos como LLAVE FCI, y pulsamos el icono del disquete para luego dar a Save.



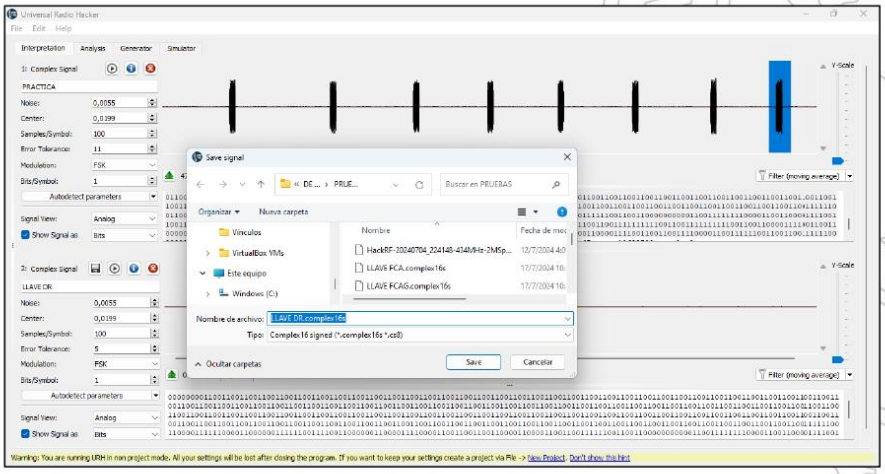
La sexta es la llave de la secretaría - Facultad de Ciencias del Mar, la renombramos como LLAVE FCM, y pulsamos el icono del disquete para luego dar a Save.



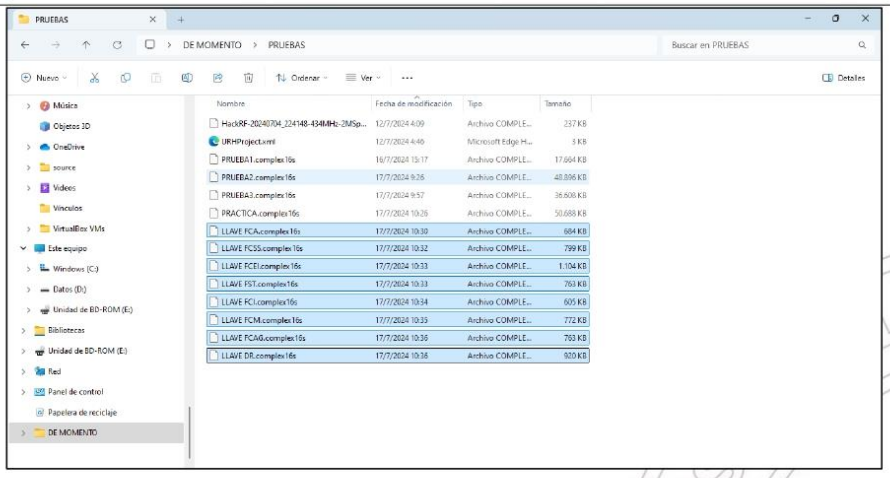
La séptima es la llave de la secretaría - Facultad de Ciencias Agrarias, la renombramos como LLAVE FCAG, y pulsamos el icono del disquete para luego dar a Save.



La octava es la llave - Departamento de Redes, la renombramos como LLAVE DR, y pulsamos el icono del disquete para luego dar a Save.



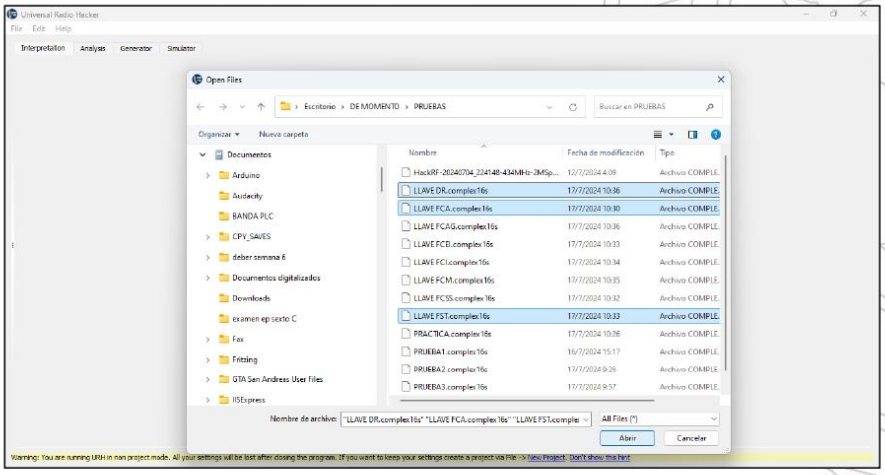
Una vez terminado este proceso, podemos visualizar que se ha cumplido con la primera meta que es la obtención de las 8 llaves RF.



Cerramos todas las ventanas y volvemos a abrir el programa URH.

En la pestaña File seleccionamos Open

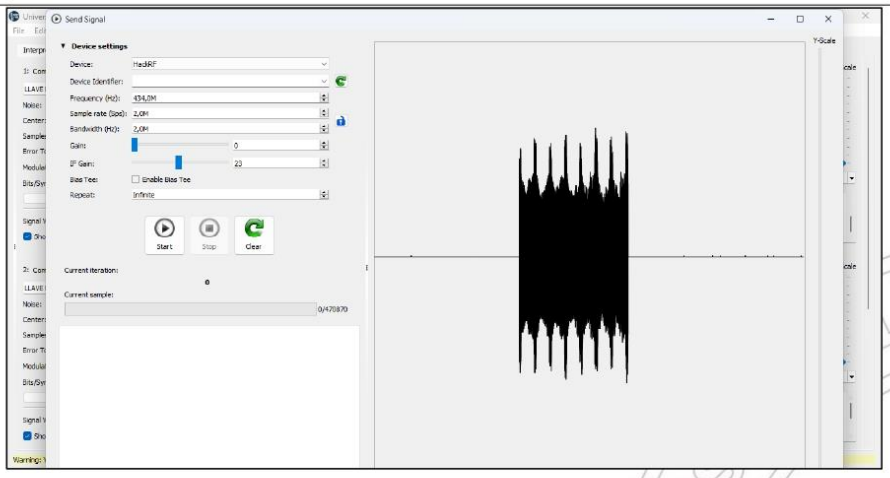
Se abre la carpeta en donde hemos guardado las llaves, en este caso la meta abrir al menos 3 lugares, se va a abrir las llaves FCA, FST y DR. Seleccionamos las tres y le damos en Abrir.



El programa procede a cargar las tres llaves con su respectivo nombre para la identificación.

La primera llave a reproducir es la LLAVE DR, damos clic en el icono de Replay Signal

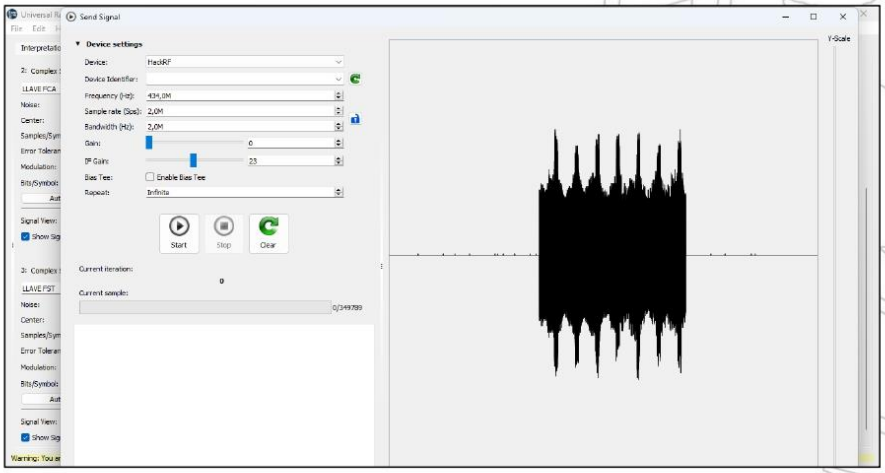
Se abre la ventana Send Signal, en la parte repeat cambiamos Infinite por 1 para que solo se reproduzca una vez, luego damos clic en Start para que empiece la reproducción de la LLAVE DR.



Observamos en el nodo SERVIDOR que sin manipular el nodo CLIENTE hemos abierto el Departamento de Redes.

La segunda llave a reproducir es la LLAVE FCA, damos clic en el icono de Replay Signal

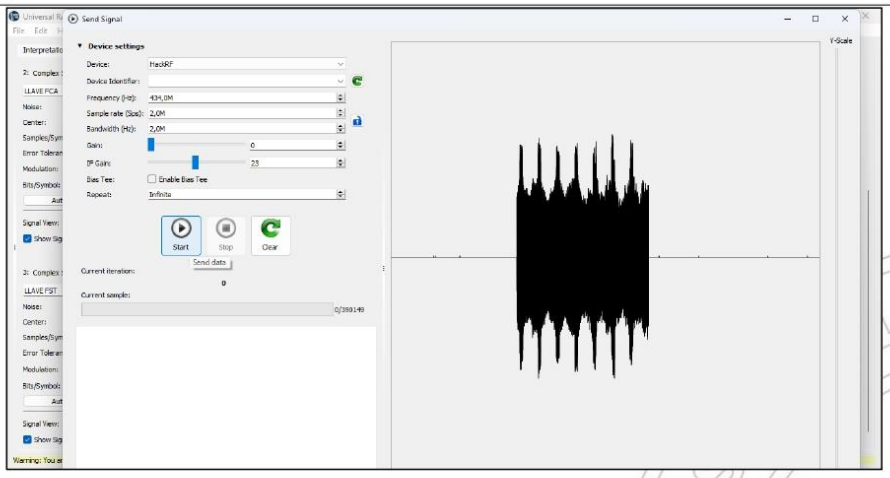
Se abre la ventana Send Signal, en la parte repeat cambiamos Infinite por 1 para que solo se reproduzca una vez, luego damos clic en Start para que empiece la reproducción de la LLAVE FCA.



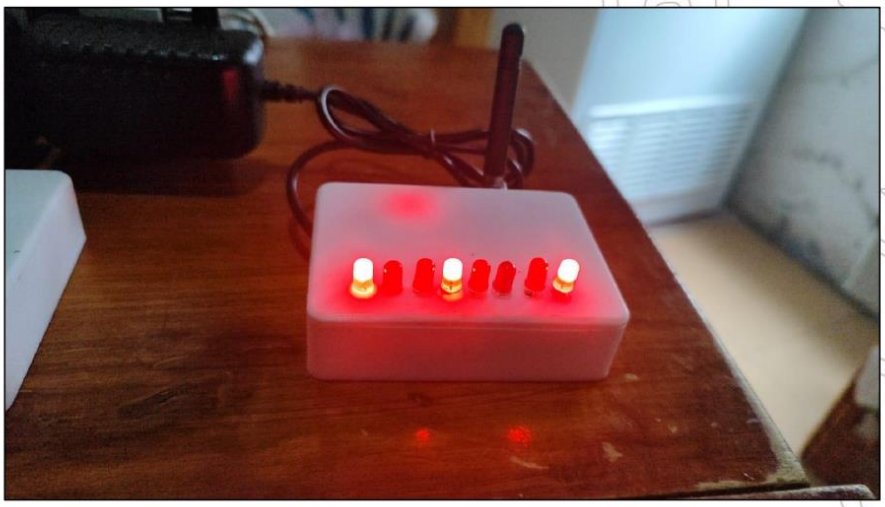
Observamos en el nodo SERVIDOR que sin manipular el nodo CLIENTE hemos abierto la secretaría de la Facultad de Ciencias Administrativas.

La tercera llave a reproducir es la LLAVE FST, damos clic en el icono de Replay Signal

Se abre la ventana Send Signal, en la parte repeat cambiamos Infinite por 1 para que solo se reproduzca una vez, luego damos clic en Start para que empiece la reproducción de la LLAVE FST.



Observamos en el nodo SERVIDOR que sin manipular el nodo CLIENTE hemos abierto la secretaría de la Facultad de Sistemas y Telecomunicaciones. Con esto cumplimos la segunda meta que es de abrir al menos 3 lugares.



Por último, se deben desconectar los nodos CLIENTE/SERVIDOR de la corriente.

PREGUNTAS

¿Qué tipo de seguridad podría implementar para evitar el ataque de tipo eavesdropping? ¿Y por qué?

Utilizar algoritmos de cifrado robustos (como AES) para encriptar las señales RF, asegurando que solo los dispositivos autorizados con la clave adecuada puedan interpretar y utilizar las señales.

¿Qué tipo de seguridad podría implementar para evitar el ataque de tipo replay? ¿Y por qué?

Incluir nonces (números aleatorios utilizados una sola vez) o marcas de tiempo en las transmisiones RF para prevenir ataques de repetición. Cada señal de apertura debería ser única y tener una validez limitada en el tiempo.

RESULTADOS:

Utilizando el dispositivo HackRF One y el software URH, se capturaron las señales RF emitidas por las llaves de los pulsadores correspondientes a las 8 ubicaciones.

Se identificaron y registraron correctamente las señales de las 8 llaves RF correspondientes a las secretarías de las 7 facultades y el departamento de redes.

Las señales RF fueron interceptadas con éxito mientras se transmitían entre el nodo CLIENTE y el nodo SERVIDOR.

Las señales capturadas fueron retransmitidas, logrando abrir la secretaria de la Facultad de Sistemas y Telecomunicaciones, la secretaria de la Facultad de Ciencias Administrativas y el departamento de redes.

PRÁCTICA COMPLEMENTARIA

El trabajador de un parque está encargado de encender las lámparas al anochecer de manera manual a través de una llave por RF, hay cuatro lámparas ubicadas en los puntos cardinales del parque al norte está la luz 1, al este la luz 2, al sur la luz 3 y al oeste la luz 4. Siempre hace el encendido de las lámparas en la secuencia norte, este, sur y oeste. Utilizando el módulo didáctico para esta práctica, realice la modificación de la secuencia de tal manera que sea sur, este, oeste y norte, tome en cuenta la siguiente tabla.

Lampara Norte	Pulsador 1	LED 1
Lampara Este	Pulsador 2	LED 2
Lampara Sur	Pulsador 3	LED 3
Lampara Oeste	Pulsador 4	LED 4

Nota: Tome en consideración la visualización de los nodos de izquierda a derecha para identificar el pulsador y led designado.

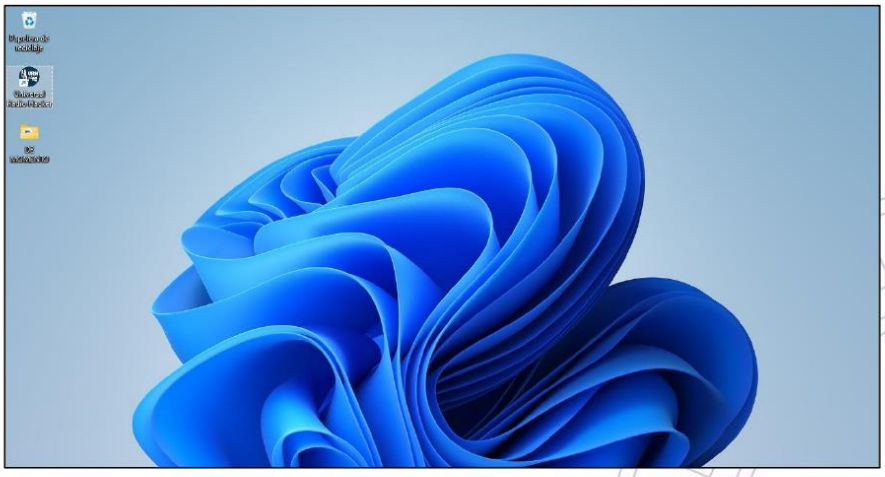
Nota: Es importante desconectar los nodos de la corriente luego de cada prueba para evitar volcados de memorias.

Desarrollo

Se conecta el dispositivo HackRF One a la computadora.

Se conectan los nodos CLIENTE/SERVIDOR a la corriente.

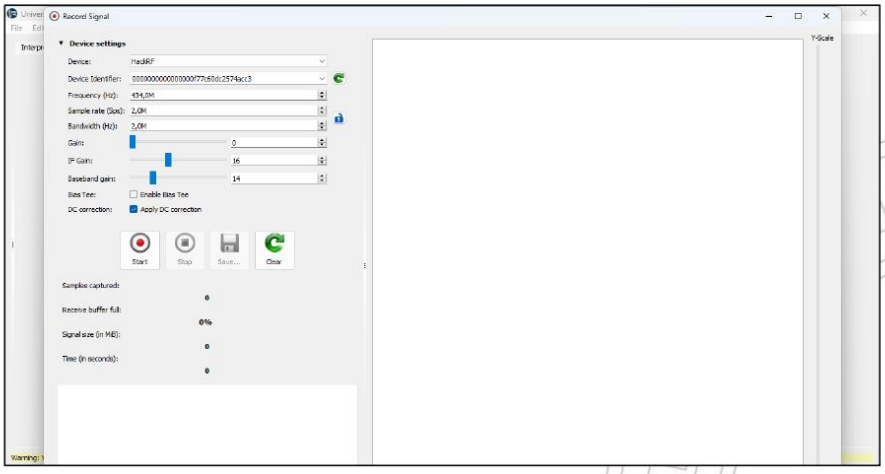
Abrimos el programa Universal Radio Hacker (URH)



En la pestaña File seleccionamos Record Signal.

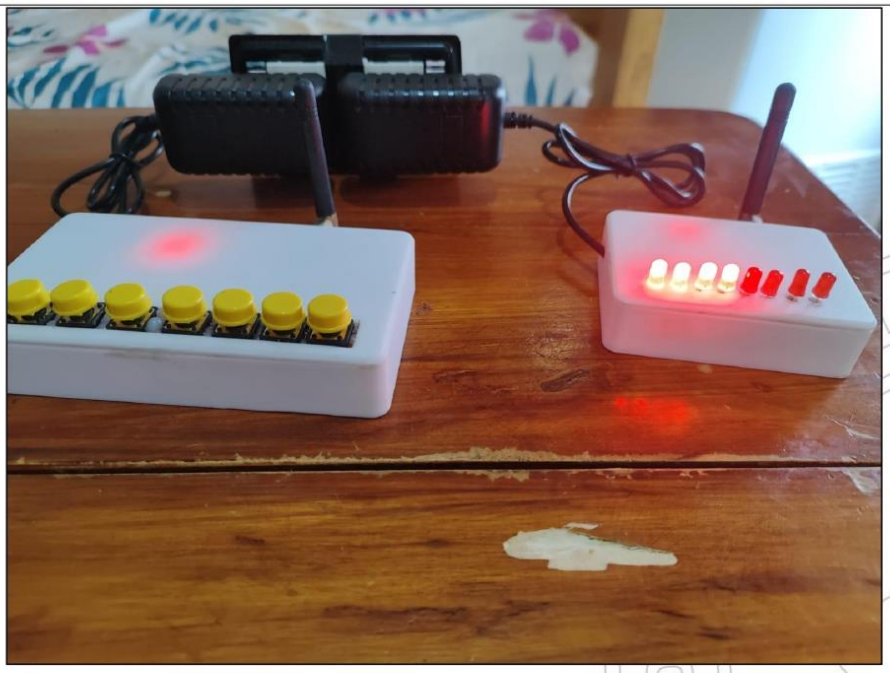
Se abre la ventana Record Signal aquí se procede a configurar el equipo SDR, en Device ubicamos HackRF, luego damos clic en la flecha verde que está en Device Identifier para que el programa pueda identificar nuestro dispositivo SDR, en Frequency (Hz) se configura la frecuencia

que en este caso es de 434 MHz, debido a que, los nodos CLIENTE/SERVIDOR trabajan a esa frecuencia. Al presionar Start empieza la captura de datos en la frecuencia de 434 MHz.

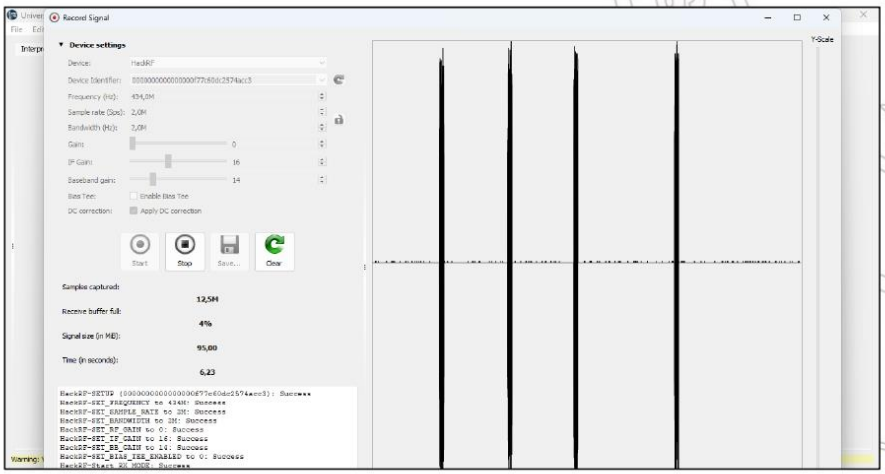


Una vez que empiece la captura de datos, se procede a presionar los pulsadores con la secuencia norte, este, sur y oeste, de izquierda a derecha tomando en cuenta la siguiente tabla.

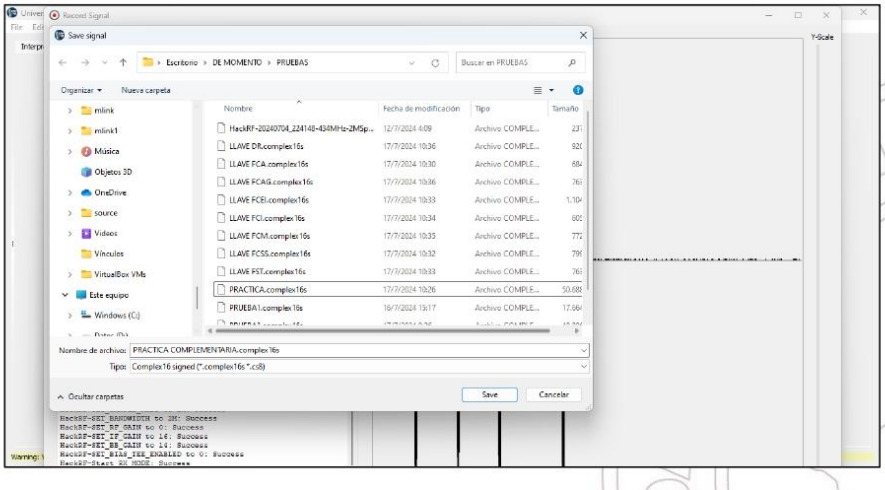
Lampara Norte	Pulsador 1	LED 1
Lampara Este	Pulsador 2	LED 2
Lampara Sur	Pulsador 3	LED 3
Lampara Oeste	Pulsador 4	LED 4



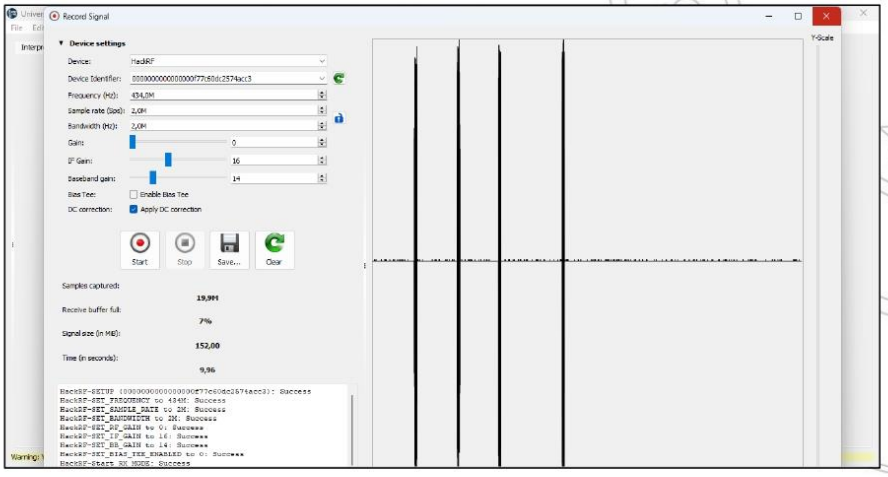
Al terminar de presionar los pulsadores, damos en Stop para detener la captura.



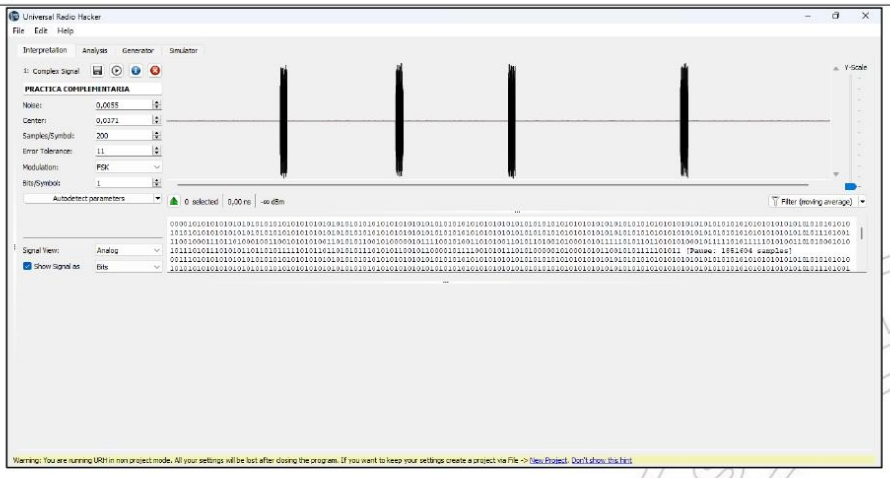
Cuando se detiene la captura tenemos la opción Save que permite guardar los datos capturados, en este caso lo guardamos con el nombre PRACTICA COMPLEMENTARIA en alguna carpeta previamente creada.



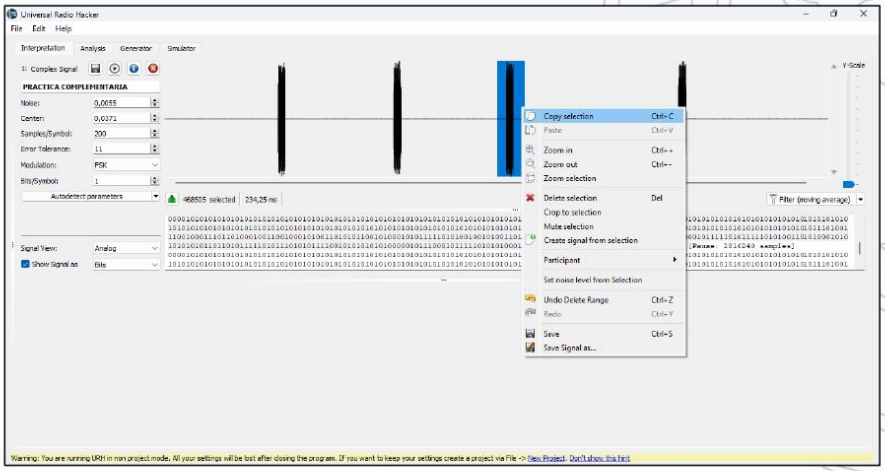
Una vez que se guarde el archivo podemos cerrar la ventana Record Signal.



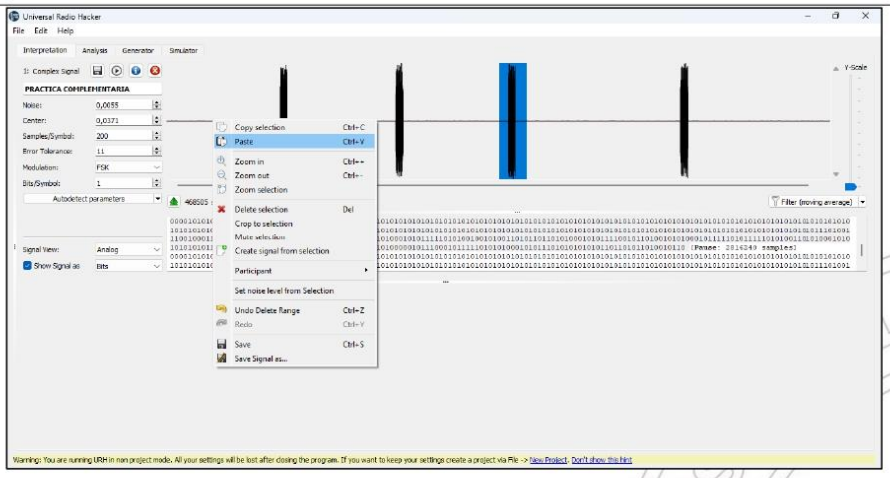
Con el mouse podemos hacer un poco de zoom para ajustar la señal y poder visualizarla de mejor manera.



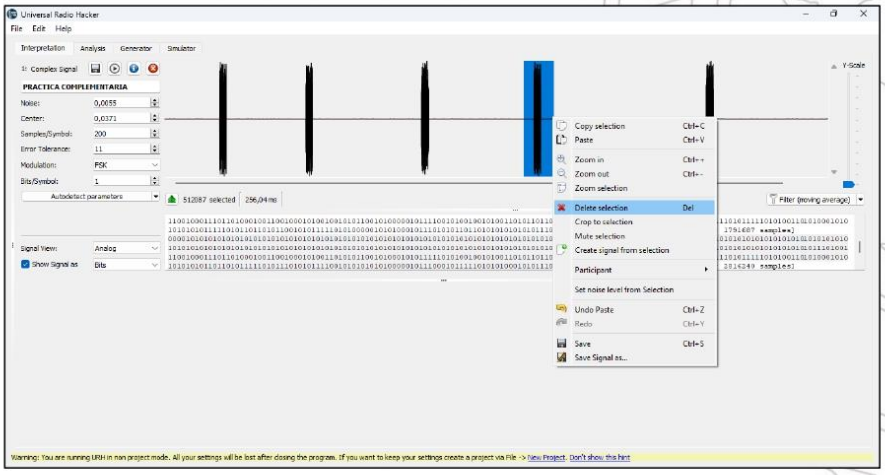
Aquí comenzamos a realizar las modificaciones de acuerdo a la nueva secuencia, copiamos la señal de la lampara Sur.



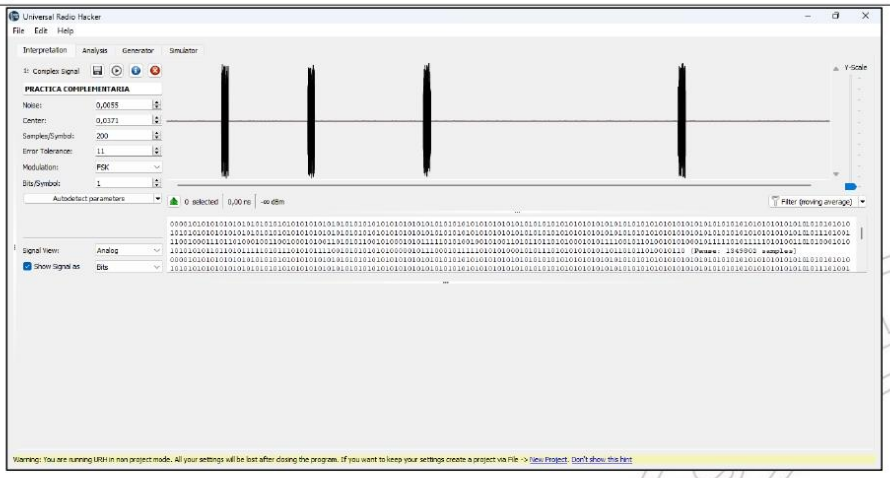
Pegamos la copia de la señal al inicio de la secuencia.



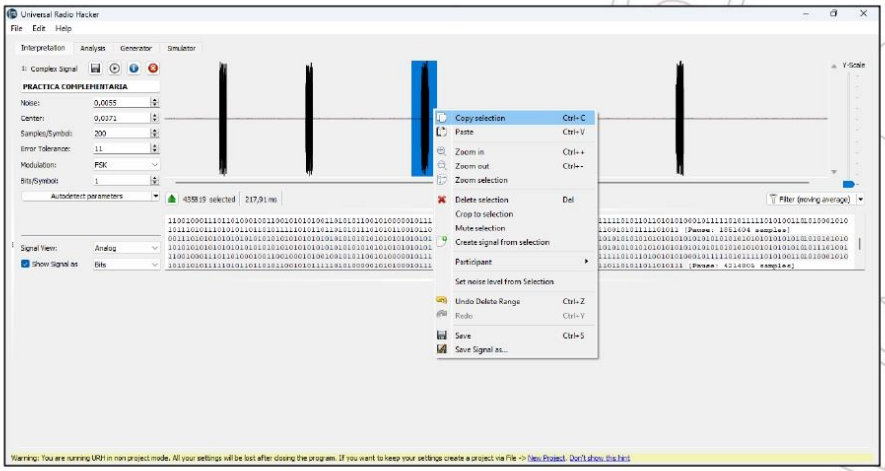
Una vez que se tiene pegada la copia de la señal sur al inicio, se procede a eliminar la señal original sur.



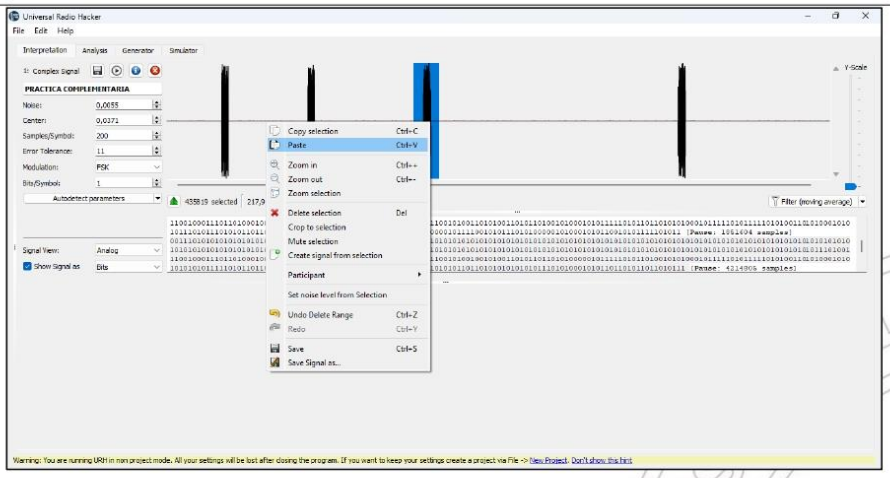
Así obtenemos la secuencia sur, norte, este y oeste.



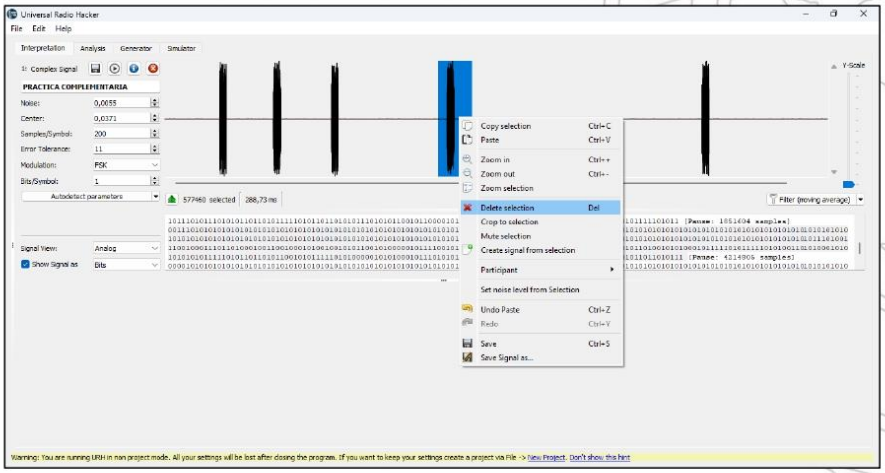
Copiamos la señal de la lampara Este.



Pegamos la copia de la señal este después de la señal sur.

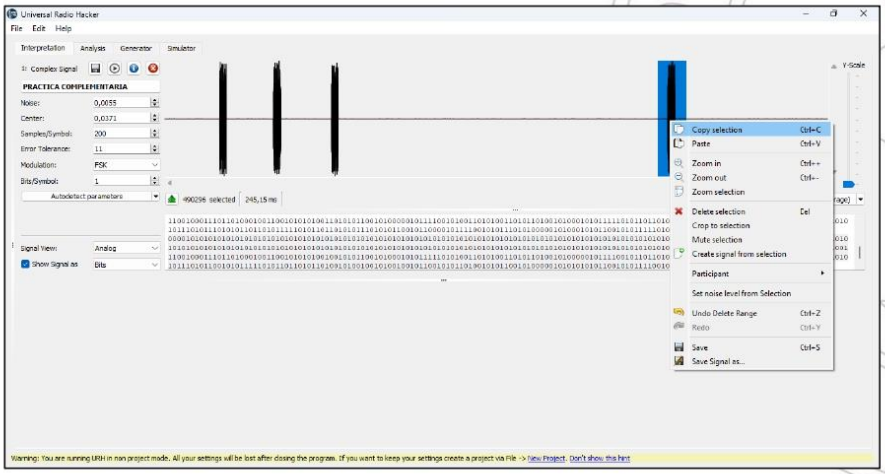


Una vez que se tiene pegada la copia de la señal este después de la señal sur, se procede a eliminar la señal original este.

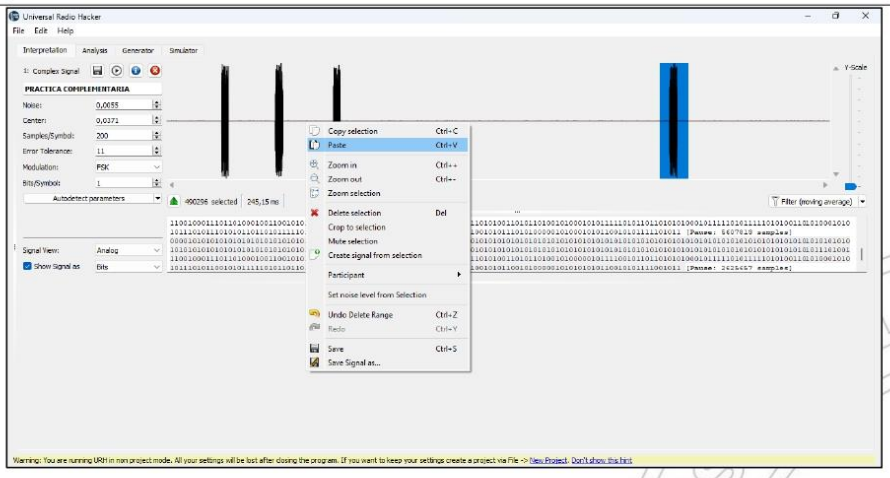


Así obtenemos la secuencia sur, este, norte y oeste.

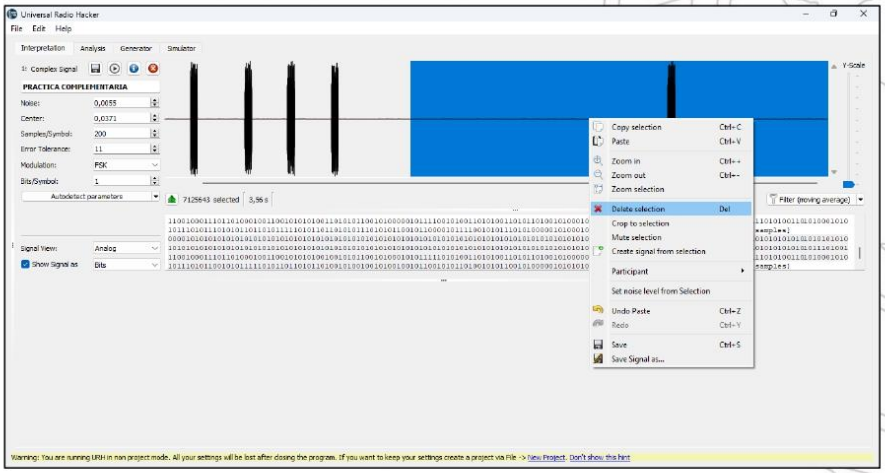
Copiamos la señal de la lampara Oeste.



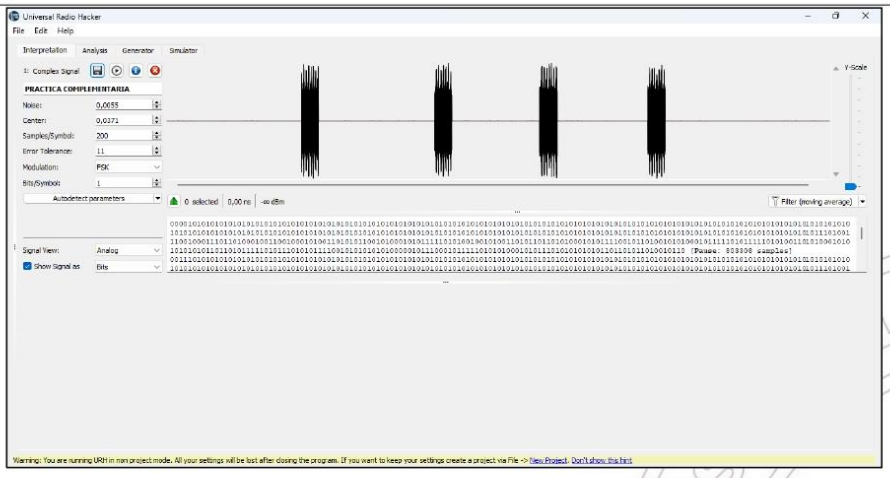
Pegamos la copia de la señal oeste después de la señal este.



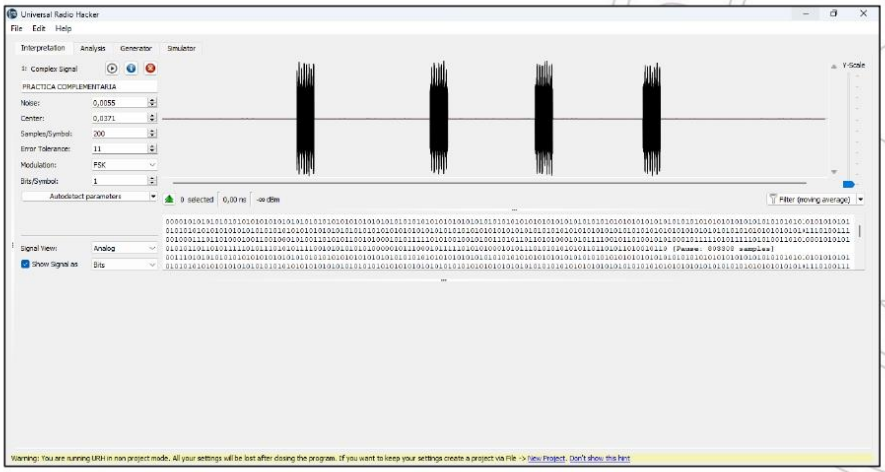
Una vez que se tiene pegada la copia de la señal oeste después de la señal este, se procede a eliminar la señal original oeste.



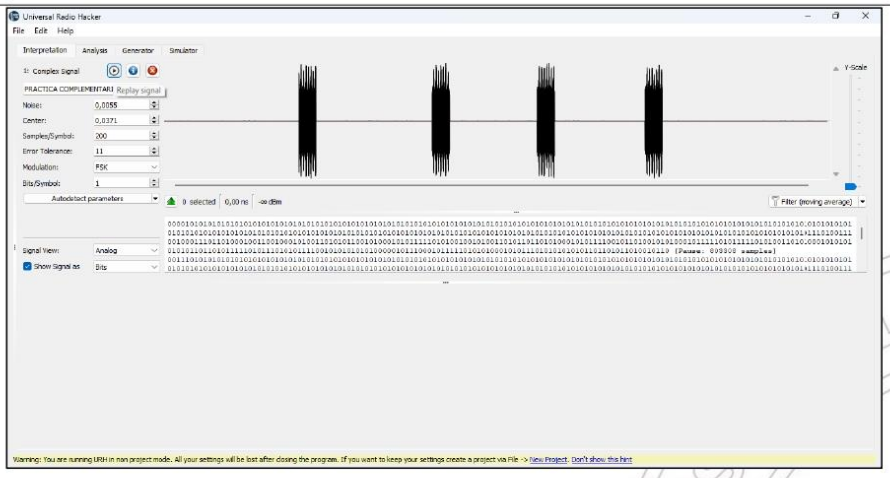
Así obtenemos la secuencia sur, este, oeste y norte cumpliendo con la meta. Le damos clic en el icono del disquete para guardar la señal modificada.



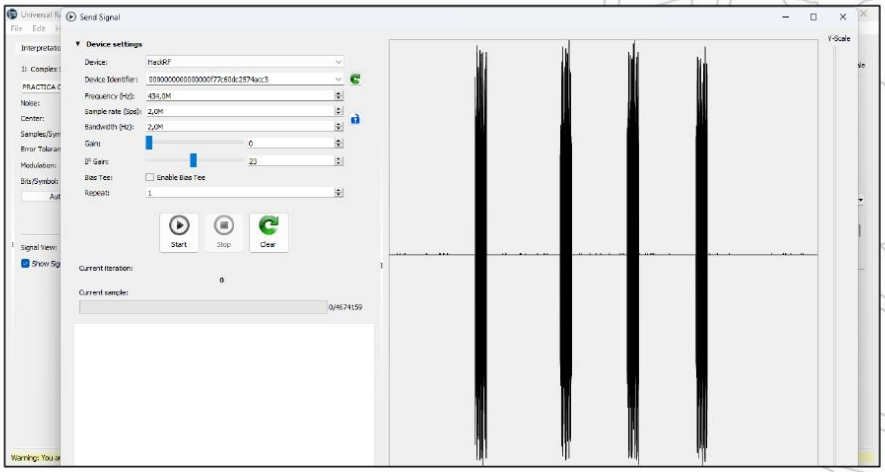
Podemos observar la secuencia solicitada sur, este, oeste y norte.



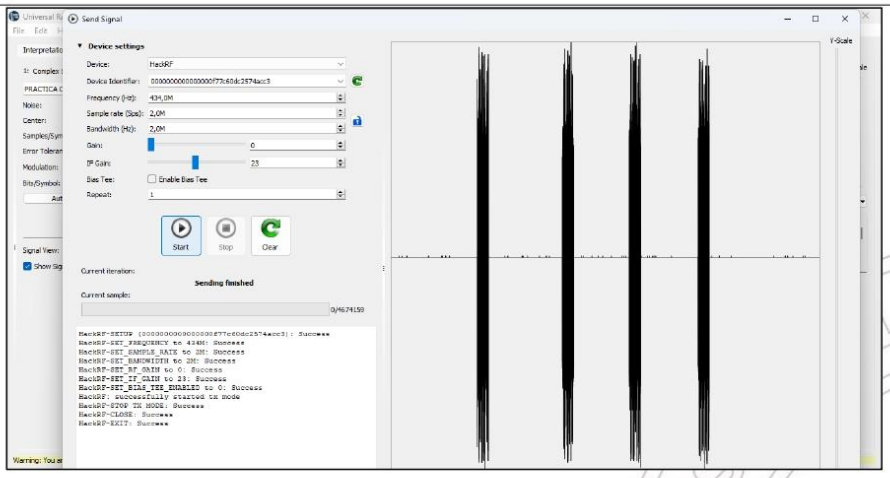
Damos clic en el incono de Replay Signal.



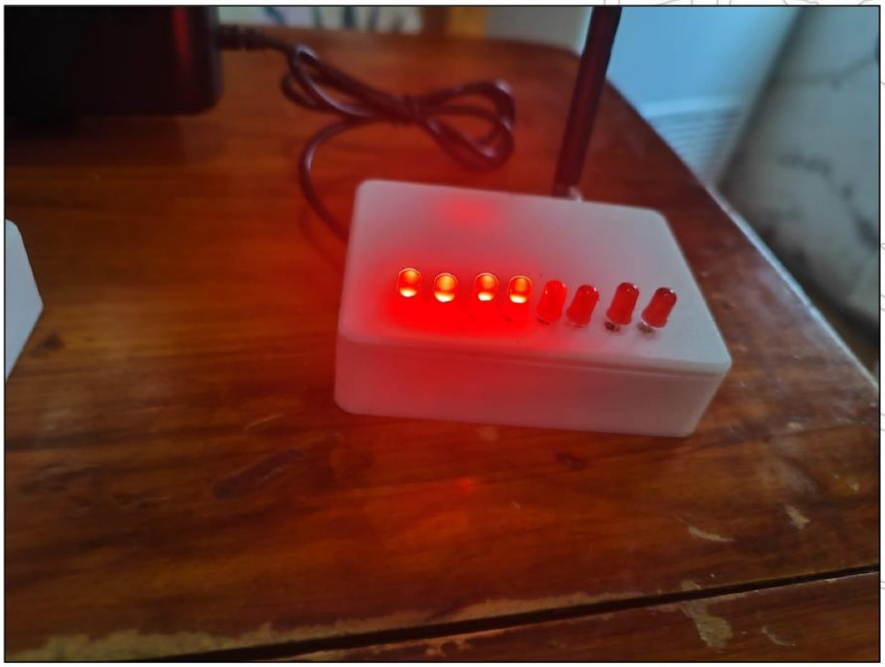
Se abre la ventana Send Signal para transmitir la señal modificada, en la parte de abajo en Repeat se coloca 1, para que solo se repita una vez.



Al dar clic en Start, se transmite la señal.



Se puede observar en el nodo SERVIDOR como se encienden los diodos LED con la secuencia modificada.



Por último, se deben desconectar los nodos CLIENTE/SERVIDOR de la corriente.

Resultado

Se logró aplicar exitosamente un ataque de intermediario (MITM) utilizando el módulo didáctico, lo que permitió interceptar y modificar la secuencia de encendido de las lámparas en el parque. Originalmente, la secuencia de encendido era norte, este, sur y oeste. Después de realizar el ataque, se modificó la secuencia a sur, este, oeste y norte. Esto se confirmó visualizando la activación de los LEDs correspondientes en el nodo SERVIDOR del módulo didáctico, en el orden modificado: LED 3 (sur), LED 2 (este), LED 4 (oeste), y LED 1 (norte).

PREGUNTAS

¿Qué tipo de seguridad podría implementar para evitar el ataque de tipo MITM? ¿Y por qué?

Para mitigar esta vulnerabilidad, se recomienda implementar un sistema de autenticación y encriptación para las señales RF. Esto puede incluir el uso de cifrado AES para asegurar que las señales transmitidas no puedan ser interceptadas y alteradas por terceros no autorizados. Además, implementar un mecanismo de autenticación mutua entre el transmisor (llave RF) y el receptor

(controlador de lámparas) garantizaría que solo los dispositivos autorizados puedan enviar y recibir comandos, asegurando la integridad de la secuencia de encendido.

CONCLUSIONES:

El sistema de apertura basado en llaves RF demostró ser vulnerable a ataques de intercepción (eavesdropping) y repetición (replay attacks), permitiendo el acceso no autorizado a áreas protegidas.

La captura y retransmisión de señales RF sin autenticación adicional o cifrado eficaz facilita la explotación de estas vulnerabilidades.

La capacidad de obtener y reutilizar las señales RF sin ser detectado compromete seriamente la seguridad de las áreas críticas dentro de la universidad.

La apertura exitosa de puertas utilizando señales capturadas indica que cualquier persona con el equipo adecuado puede acceder a áreas restringidas, lo que representa un riesgo significativo para la seguridad.

El sistema de encendido de lámparas por RF es vulnerable a ataques de intermediario (MITM), lo que permite a un atacante interceptar, alterar y retransmitir las señales de control, modificando la secuencia de encendido sin el conocimiento del operador legítimo. Esto pone de manifiesto la falta de medidas de seguridad robustas en la transmisión de señales RF, que pueden ser fácilmente manipuladas.

La práctica permite a los estudiantes comprender las amenazas en las comunicaciones RF y aprender a implementar contramedidas efectivas. Esta experiencia práctica fortalece el conocimiento teórico y desarrolla habilidades críticas para la seguridad en redes inalámbricas.

RECOMENDACIONES:

Utilizar algoritmos de cifrado robustos (como AES) para encriptar las señales RF, asegurando que solo los dispositivos autorizados con la clave adecuada puedan interpretar y utilizar las señales.

Implementar un sistema de autenticación bidireccional donde tanto el nodo CLIENTE como el nodo SERVIDOR se autentiquen mutuamente antes de realizar cualquier acción de apertura. Esto podría involucrar el uso de certificados digitales o tokens de autenticación.

Incluir nonces (números aleatorios utilizados una sola vez) o marcas de tiempo en las transmisiones RF para prevenir ataques de repetición. Cada señal de apertura debería ser única y tener una validez limitada en el tiempo.

Implementar sistemas de monitoreo que detecten actividades sospechosas, como intentos de repetición de señales o patrones inusuales de acceso. Los intentos de acceso no autorizados deben ser registrados y reportados para tomar acciones inmediatas.

Establecer un programa de actualización regular de las llaves RF y los protocolos de comunicación para asegurar que cualquier vulnerabilidad descubierta se aborde rápidamente y se mejore continuamente la seguridad del sistema.

REFERENCIAS:

N. Ramírez Galvis, J. Rivera Cardona y C. Mejía Londoño, «Vulnerabilidad, tipos de ataques y formas de mitigarlos en las capas del modelo OSI en las redes de datos de las organizaciones,» 2012. [En línea]. Available: https://hdl.handle.net/11059/2734. [Último acceso: 29 Noviembre 2023].

Á. &. Chalan, «Políticas de ciberseguridad para los dispositivos de capa-dos en el centro de datos del hospital de Latacunga,» 2022. [En línea]. Available: https://repositorio.pucesa.edu.ec/handle/123456789/3516. [Último acceso: 11 Noviembre 2023].

C. Obando I, «Seguridad a nivel de enlace de datos en el modelo de interconexión de sistemas abiertos (OSI),» iname, vol. 2, nº 2, pp. 71-78, Junio 2022.

Gesteira, «Pruebas de intrusión en automóviles mediante ataques de radio frecuencia. Análisis de vulnerabilidades,» 2022. [En línea]. Available: http://hdl.handle.net/11531/66178. [Último acceso: 11 Noviembre 2023].

A. Lindeberg, «Hacking Into Someone's Home using Radio Waves: Ethical Hacking of Securitas' Alarm System,» 2021. [En línea]. Available: https://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-302999. [Último acceso: 23 Noviembre 2023].