



HackRF

¿Qué es HackRF One y PortaPack H2?

- **HackRF One:**
 - Es una radio definida por software (SDR) de código abierto. Esto significa que es un dispositivo que puede transmitir y recibir señales de radio en un amplio rango de frecuencias.
 - Su versatilidad permite a los usuarios experimentar con diversas tecnologías inalámbricas, desde la radio FM hasta las comunicaciones móviles.
- **PortaPack H2:**
 - Es un complemento para el HackRF One que lo convierte en un dispositivo portátil e independiente.
 - Proporciona una pantalla, controles y una batería, lo que permite utilizar el HackRF One sin necesidad de un ordenador.
 - Convierte al HackRF One en una herramienta SDR portátil.

Usos lícitos:

- **Análisis de señales de radio:** Permite a los usuarios visualizar y analizar las señales de radio presentes en su entorno.

- **Desarrollo de sistemas inalámbricos:** Facilita la creación y prueba de nuevos protocolos y tecnologías inalámbricas.
- **Educación e investigación:** Es una herramienta valiosa para aprender sobre comunicaciones inalámbricas y realizar investigaciones en este campo.
- **Pruebas de seguridad:** Los profesionales de la seguridad pueden utilizarlo para evaluar la seguridad de sistemas inalámbricos.
- **Radioafición:** Permite a los radioaficionados experimentar con diversas formas de comunicación por radio.

Usos no lícitos:

- **Interferencia de señales:** Puede utilizarse para interferir intencionadamente en señales de radio, lo que puede ser ilegal y perjudicial.
- **Escucha de comunicaciones privadas:** Permite interceptar comunicaciones inalámbricas, lo que puede violar la privacidad de las personas.
- **Ataques de seguridad:** Puede utilizarse para realizar ataques contra sistemas inalámbricos, como la clonación de tarjetas de acceso o la manipulación de señales de GPS.
- **Inhibición de señales:** Se puede usar para bloquear señales, como alarmas de seguridad o sistemas de localización.

Versiones disponibles H1 y H2

Muchas veces navegando por la web encontramos dos variantes del portapack, la H1 y la H2, en esencia, son los mismo solamente que la última presenta algunas mejoras en lo que respecta a la pantalla y comandos.

PORTAPACK

Cuando hablamos de PORTAPACK nos referimos a una pequeña placa que se acopla a nuestro [HACKRF](#) y nos permite acceder a distintas funciones, algunas de estas se enumeran a continuación:

Transmision:

- ADS-B(S)
- [APRS](#)
- BHT Xy/EP

- [GPS Sim](#)
- Jammer
- Key Fob
- LGE Tool
- Morse
- Burger Pager
- POCSAG
- [SSTV](#)
- TEDI/LCR
- TouchTune
- [RDS](#)
- [OOK](#)
- [Soundboard](#)

Recepcion:

- [ADS-B](#)
- AIS Boats
- AFSK
- [BTLE](#)
- [NRF](#)
- [AudioSPECWFMNFMAM](#)
- [Analog TV](#)
- ERT Meter
- [POCSAG](#)
- [Radiosonde](#)
- [TPMS Cars](#)

Opciones del menú de PortaPack H2:

El menú del PortaPack H2 ofrece una amplia gama de funciones, algunas de las más comunes son:

- **Receive (Recibir):** Permite recibir y visualizar señales de radio en tiempo real.
- **Transmit (Transmitir):** Permite transmitir señales de radio en diversas frecuencias y modos.
- **Replay (Reproducir):** Permite grabar y reproducir señales de radio capturadas previamente.
- **Sniffer (Rastreador):** Permite rastrear y analizar señales de radio específicas, como redes Wi-Fi.
- **GPS:** Permite recibir y visualizar señales de GPS.
- **Settings (Ajustes):** Permite configurar diversos parámetros del dispositivo, como la frecuencia, el ancho de banda y la potencia de transmisión.

Firmware Mayhem

El firmware que controla todo, va instalado en la memoria interna del Hack RF. Lo podéis descargar de su página de [github](#).

ADS-B

ADS-B significa Automatic Dependent Surveillance - Broadcast y es un sistema de control del tráfico aéreo. Se utiliza para mostrar los movimientos de las aeronaves en el espacio aéreo. Este sistema estándar es relativamente joven y sólo existe desde 2005; en Estados Unidos será obligatorio para todos los participantes a partir de 2020. En Europa, el ADS-B es obligatorio a partir del 7 de diciembre de 2020 para las grandes aeronaves con un peso de despegue igual o superior a 5,7 toneladas o una velocidad superior a 250 KTAS (nudos de velocidad aérea real) en vuelo.

Mientras que el radar aerotransportado tradicional rastrea las aeronaves a través de la reflexión de las ondas de radar transmitidas, el ADS-B transmite activamente los datos de posición de las aeronaves, en este proceso los participantes determinan su posición de forma independiente utilizando los satélites de navegación y envían los datos de forma estandarizada a través de la frecuencia de **1090 MHz**. Las señales pueden oírse hasta 370 km de distancia, y en altitudes superiores incluso más.

AIS

El AIS (Sistema de identificación automática) es un sistema que transmite la posición de un barco para que otros barcos estén al tanto de la misma y así evitar colisiones. La Organización Marítima Internacional (OMI) exige el uso de AIS en buques de más de 300 toneladas brutas que realizan viajes internacionales. Muchos gobiernos nacionales han ordenado a los buques que caen fuera de la regulación de la OMI que usen AIS. Cada año, más de 400,000 dispositivos AIS diferentes transmiten la ubicación de embarcaciones junto con otras informaciones como identidad, rumbo y velocidad. Las estaciones terrestres y los satélites recogen esta información, de manera que los movimientos de un barco puedan ser rastreados incluso desde las zonas más remotas del océano.

Aunque el uso de AIS no es obligatorio a nivel global para los barcos de pesca, se estima que las embarcaciones con AIS representan más de la mitad del esfuerzo de pesca a más de 100 millas náuticas de la costa, y hasta el 80% de la pesca en alta mar. La cantidad de embarcaciones pesqueras con AIS aumenta entre un 10 y un 30 por ciento cada año, lo que hace que esta tecnología sea cada vez más informativa con el tiempo.

El AIS transmite en **161,975 y 162,025 Mhz**.

AFSK

La modulación por desplazamiento de frecuencia o FSK (del inglés Frequency Shift Keying) es una **técnica de modulación para la transmisión digital de información utilizando dos o más frecuencias diferentes para cada símbolo**.

A diferencia de la modulación de amplitud, que puede ser más susceptible a las interferencias, la FSK ofrece una alternativa sólida para la comunicación digital. Encuentra aplicaciones en varios campos, como **la radio, las telecomunicaciones y las redes informáticas**.

Cuando se usa una señal de audio modulada en FSK para modular a su vez una portadora de radio se denomina AFSK (audio FSK).

BTLE

BTLE, también conocido como **Bluetooth Low Energy**, Bluetooth LE o Bluetooth Smart, es un nuevo protocolo de comunicación que se ha agregado a la especificación Bluetooth (BT) 4.0. BTLE está destinado a proporcionar una alternativa de baja velocidad y bajo consumo de energía al Bluetooth Classic.

BTLE (Bluetooth 4.0) es una versión de menor consumo energético del estándar de comunicaciones inalámbricas Bluetooth, que funciona constantemente, anunciando la presencia de un dispositivo a los sensores locales y optimizando la duración de la batería del dispositivo en cuestión. En IoT, BLE permite una localización precisa y un seguimiento de las características sin reducir la duración de la batería.

Nos permite recibir las direcciones MAC de los dispositivos BLE que tengamos a nuestro alrededor. Su frecuencia de funcionamiento es sobre los **2,4 Ghz**

NRF

El adaptador NRF24L01 es un módulo de adaptador diseñado para utilizarse con el NRF24L01, que es un **transceptor inalámbrico de radiofrecuencia** (RF). Ambos componentes trabajan en conjunto para proporcionar una solución de comunicación inalámbrica en aplicaciones electrónicas.

El NRF24L01 **es un pequeño transceptor inalámbrico de muy bajo consumo y muy fácil de utilizar que funciona en el rango de los 2.4 GHz**. Puede enviar y recibir datos pero no puede hacerlo al mismo tiempo. Esto hace que se abarate su coste y su funcionamiento sea muy sencillo y robusto.

El módulo nRF24L01 es un componente que **permite la comunicación inalámbrica entre dos placas Arduino independientes**. Utiliza el transceptor de radio NRF24 y, en una placa de circuito impreso, se conecta a una antena para crear un transceptor de radio funcional.

En esta app podemos recibir los datos transmitidos por dispositivos que lleven el transmisor NRF24L01 en los **2,4 Ghz**.

Audio

En la aplicación audio podemos ver y escuchar señales si tenemos instalado un pequeño altavoz que viene por separado. Permite demodular AM, NFM y WFM. También dispone de banda lateral.

Tv analogica

Podemos demodular televisión analógica en formato PAL y solo en blanco y negro.

ERT Meter

El transmisor receptor codificador (ERT) es un protocolo de radio por paquetes desarrollado por Itron para la lectura automática de medidores. La tecnología se utiliza para transmitir

datos de medidores de servicios públicos a lo largo de un corto alcance, de modo que un vehículo utilitario pueda recopilar datos de los medidores sin que un trabajador inspeccione físicamente cada medidor.

Esta app permite recibir las señales de los contadores inteligentes, con frecuencias situadas entre los **900 y 920 Mhz**. Su creador indica que son usados mayoritariamente en USA.

POCSAG

POCSAG es un protocolo de transmisión de datos por radio que se utiliza **para transmitir mensajes unidireccionales a "buscapersonas"** . Los buscapersonas son pequeños receptores de radio que se activan cuando se les transmite un mensaje codificado correctamente a través de un canal de radio.

La radiobúsqueda comercial opera en las **bandas de 35-36, 43-44, 152-159 y 454-460 MHz (a veces denominadas "Banda Inferior") y en las bandas de 929 y 931 MHz (a veces denominadas "Banda Superior")**

En el mundo actual de tecnologías de comunicación avanzadas, es sorprendente que **el protocolo de búsqueda POCSAG/FLEX aún se utilice** . Sin embargo, existen varias buenas razones por las que sigue siendo valioso, especialmente para los servicios de emergencia.

Podemos recibir mensajes enviados a los buscapersonas, usados actualmente por los radioaficionados. La frecuencia usada en España es **144,8625 Mhz**.

Radiosondas

Una radiosonda es un dispositivo empleado en globos meteorológicos para medir varios parámetros atmosféricos y transmitirlos a un aparato receptor fijo. La frecuencia de radio de 403 MHz está reservada para uso con las radiosondas.

Son varias las ubicaciones en España desde donde se lanzan cada día un par de radiosondas montadas en globos que llegan hasta los 25.000 metros de altura. Con esta app podemos recibir varios tipos de radiosondas como las **MeteoModem M10, MeteoModem M2K2 y Vaisala RS41-SG**.

TPMS

TPMS significa **sistema de monitoreo de presión de neumáticos**. Como sugiere su nombre , un sistema de control de la presión de los neumáticos es más que una sola pieza. De hecho, TPMS incluye una válvula y un Sensor, y también es importante saber que no todos los sistemas TPMS son iguales.

El TPMS (por sus siglas en inglés) **supervisa continuamente la presión de inflado del neumático, y alerta al conductor si cae por debajo de cierto nivel.** Esta función de seguridad también disminuye el consumo de combustible y las emisiones de CO2 de su automóvil.

La frecuencia utilizada es **433.92 Mhz.**

Mandos Automóviles

Frecuencia de funcionamiento en el rango 433 MHz

Consideraciones importantes:

- El uso del HackRF One y el PortaPack H2 debe realizarse de acuerdo con las leyes y regulaciones locales.
- Es importante ser consciente de las posibles implicaciones éticas y legales del uso de estas herramientas.
- El usuario es el responsable del uso que le da a la herramienta.