HackRF One and Portapack H2 User Manual	Document ID	Version	Pages
	HackRF-01	1.0	9

Ver.	Author	Description	Date
1.0	Admin		2024.6.17

Content

1 Introduction

HackRF One is the current hardware platform for the HackRF project. It is a Radio peripheral capable of transmission or reception of radio signals from 2402-2480MHz. Designed to enable test and development of modern and next generation radio technologies, HackRF One is an open source hardware platform that can be used as a USB peripheral or programmed for stand-alone operation.

The PortaPack is add-on for the HackRF radio (HackRF + PortaPack + Accessory Amazon bundle) which allows you to go portable with the HackRF and a battery pack. It features a small touchscreen LCD and an iPod like control wheel that is used to control custom HackRF firmware which includes an audio receiver, several built in digital decoders and transmitters too. With the PortaPack no PC is required to receive or transmit with the HackRF. The PortaPack is a very handy partner to the HackRF. It allows you to experiment with, record, listen, decode and transmit RF signals out in the field, without the need for any computer. You do need to be responsible and careful with the device though, as there is the huge potential of getting in trouble with it if you start transmitting illegal things.

Note: Please do use the device in accordance with your local laws and regulations.

1.1 Main Features

The hardware version of HackRF One is **R10**, which is the latest revision has made lots of hardware improvements. The R10 is based on R8, reverting most of the changes made in R9 and making the device much more compatible with the mayhem portapack firmware. For example, the **MAX2837** is much more suitable for portapack than MAX2839. And the portapack H2 is R4, which is the most stable portapack in the current market.

The specific hardware improvements are given in the following fingure. It includes the RF protection, CLK IN/OUT protection and MicroUSB protection. The Added RF protection against excessive RF at the antenna port (Tx and Rx), providing protection for both the transmit amplifier and the receive LNA.

1.2 HackRF One Specification

- ✧ half-duplex transceiver
- ✧ operating freq: 2402-2480MHz
- ✧ supported sample rates: 2 Msps to 20 Msps (quadrature)
- ✧ resolution: 8 bits
- ✧ interface: High Speed USB (with USB Micro-B connector)

- ✧ power supply: USB bus power
- ✧ software-controlled antenna port power (max 50 mA at 3.3 V)
- ✧ SMA female antenna connector (50 ohms)
- ✧ SMA female clock input and output for synchronization
- ✧ convenient buttons for programming
- ✧ pin headers for expansion
- ✧ portable
- ✧ open source

1.2.1 Interfaces

(1) RESET

The RESET button resets the microcontroller. This is a reboot that should result in a USB re-enumeration.

(2) DFU

The DFU button invokes a USB DFU bootloader located in the microcontroller's ROM. This bootloader makes it possible to unbrick a HackRF One with damaged firmware because the ROM cannot be overwritten.

To invoke DFU mode: Press and hold the DFU button. While holding the DFU button, reset the HackRF One either by pressing and releasing the RESET button or by powering on the HackRF One. Release the DFU button.

The DFU button only invokes the bootloader during reset. This means that it can be used for other functions by custom firmware.

(3) External Clock Interface (CLKIN and CLKOUT)

HackRF One produces a 10 MHz clock signal on CLKOUT. The signal is a 10 MHz square wave from 0 V to 3 V intended for a high impedance load.

The CLKIN port on HackRF One is a high impedance input that expects a 0 V to 3 V square wave at 10 MHz. Do not exceed 3.3 V or drop below 0 V on this input. Do not connect a clock signal at a frequency other than 10 MHz (unless you modify the firmware to support this). You may directly connect the CLKOUT port of one HackRF One to the CLKIN port of another HackRF One.

HackRF One uses CLKIN instead of the internal crystal when a clock signal is detected on CLKIN. The switch to or from CLKIN only happens when a transmit or receive operation begins.

To verify that a signal has been detected on CLKIN, use hackrf_debug --si5351c -n 0 -r. The expected output with a clock detected is [0] -> 0x01. The expected output with no clock detected is [0] -> 0x51.

(4) LEDs

Button/Light	Function
Reset Button	Used to reboot the HackRF One, equivalent to unplugging the device and plugging it back in ("HackRF One One," n.d.).
3v3 LED 1V8 LED RF LED	All three of these LEDs are used to indicate power and should be lit when the HackRF One is plugged in. The various colors are used to distinguish between the multiple LEDs on the side of the HackRF One ("FAQ," n.d.).
USB LED	Indicates that the HackRF One is communicating over USB ("FAQ," n.d.).
DFU Button	Used to install or update the firmware if it is not working properly or has never been installed ("HackRF One," n.d.).
RX LED	An orange light that indicates that the device is receiving information ("FAQ," n.d.).
TX LED	A red light that indicates that the device is transmitting information ("FAQ," n.d.).

1.2.2 Transmit Power:

The maximum TX power is between 0 and 10 dBm.

Overall, the output power is enough to perform over-the-air experiments at close range or to drive an external amplifier. If you connect an external amplifier, you should also use an external bandpass filter for your operating frequency.

1.2.3 Receive Power:

The maximum RX power of HackRF One is -5 dBm. Exceeding -5 dBm can result in permanent damage!

In theory, HackRF One can safely accept up to 10 dBm with the front-end RX amplifier disabled. However, a simple software or user error could enable the amplifier, resulting in permanent damage. It is better to use an external attenuator than to risk damage.

1.3 Portapack H2 Specification

The PortaPack is add-on for the HackRF radio (HackRF + PortaPack + Accessory Amazon bundle) which allows you to go portable with the HackRF and a battery pack. It features a small touchscreen LCD and an iPod like control wheel that is used to control custom HackRF firmware which includes an audio receiver, several built in digital decoders and transmitters too. With the PortaPack no PC is required to receive or transmit with the HackRF.

The PortaPack is a very handy partner to the HackRF. It allows you to experiment with, record, listen, decode and transmit RF signals out in the field, without the need for any computer. You do need to be responsible and careful with

the device though, as there is the huge potential of getting in trouble with it if you start transmitting illegal things.

Items	Description
HackRF One Firmware	Flashed the latest github Mayhem **2.0.1** firmware, ready to use. **We are a trusted device vendor recommended by the github portapack-mayhem Project**.
Hardware Version	HackRF One: R10 Portapack H2: R4
New CPLD Code of Portapack H2	From Jan 20th 2024 updated new CPLD code so the reset button doesn't freeze the device.
Portapack Screen	3.2 inch Touch Screen
Speaker	Sound pressure level: 89 ±3 dB
Lithium Battery	Built-in 2500 mAh Lithium Battery
Lithium Button Battery	Built-in CR1220 battery with RTC clock function (record current time when saving baseband file)
TCXO Clock	Built-in TCXO high-precision clock (0.5ppm), the frequency is as accurate as the walkie-talkie. It automatically switches the external TCXO
TF Card Slot	With TF card slot (store data, playback data, frequency management)
Github Links	https://greatscottgadgets.com/hackrf/ https://github.com/portapack-mayhem/mayhem-firmware

2 HackRF with Portapack tutorial

This chapter gives the tutorial for the HackRF One and Portapack H2.

2.1 Power-on and Power-off

One click the knob button to boot the device and double click the knob button to turn off the device.

2.2 BLE Receiver Function

Main menu-->Receive-->BLE Rx, enter into the BLE receive function.

This is the main view which provides the user with incoming packet entries captured by the BLE Scanning.

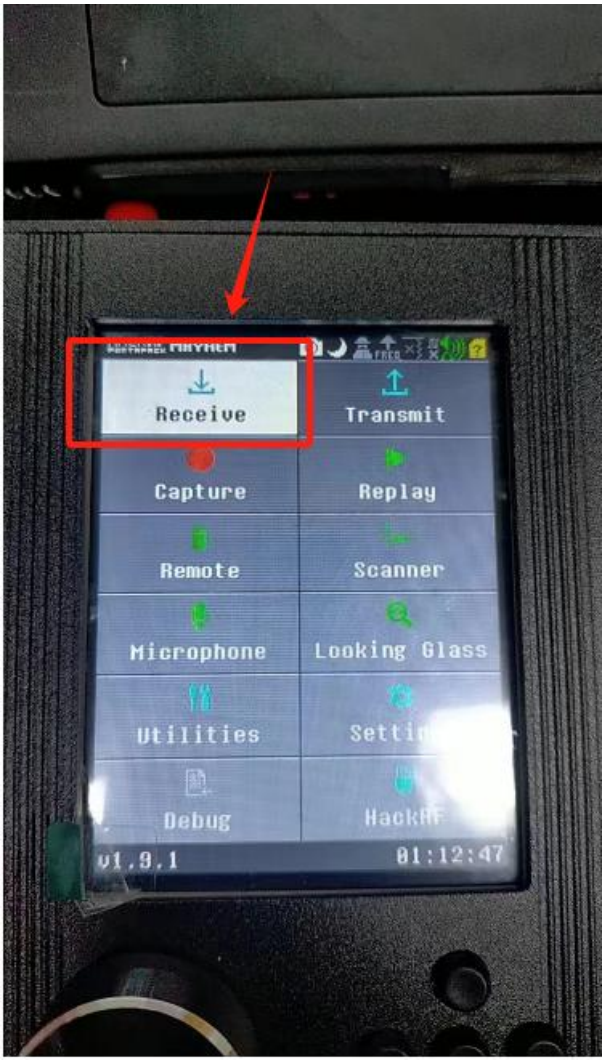
- ✧ The BLE app upon entry will scan for BLE advertisement packets, and report them on the screen. The Channel knob can be used to select which advertisement channel to listen on. There is an Auto feature which will switch channels upon receiving a new packet. (Randomized from 37-39).
- ✧ Once found the user can then select an individual MAC Address entry to pull up a more detailed view of the captured data packet.
- ✧ The Sort Knob will sort the list of MAC indices by either Ascending MAC Address, dB, or by most recently updated entry.
- ✧ The Filter button allows the user to filter based on the hex data of each packet. It also allows for filtering based on the ASCII name of the device (if found). More on that below.
- ✧ The Name toggle allows the user to toggle off and on name display, if there is a name associated with the device. Not all devices have a name string. This name string is being parse from the Shortened and Complete Local Name packet type. See BLE Spec for information on packet types.
- ✧ The Clear button allows the user to clear entries as they fill up the screen.
- ✧ The Export CSV file allows the user to export the current list of packet entries into a csv style file. Upon resaving the file, the file will update the existing entries with new data, as well as append new entries to the existing file.
- ✧ The Tx button allows the user to switch to the BLE Tx app. See BLETX for more information.

2.3 BLE Receiver Operation Instruction

This chapter gives the detail operation instruction for the BLE Receiver.

Step 1, Boot the device via one click the knob button of the device.

Step 2, enter into the top menu, find and click the menu Receive;



Step 3, click the BLE Rx , enter into the BLE icon, then you will enter into the BLE receive function.

Step 4, receive the BLE signal.

Step 5, Turn off the device via double click the knob button.

2.4 BLE Transmitters Function

Main menu-->Transmit-->BLE Tx, enter into the BLE transmit function.

The BLETX application is intended for importing a BLE Advertisement file, parsed by the application and transmit it OTA.

The BLETX application has two modes, both which can be used after importing a file.

- ✧ Single transmit mode. (This mode transmits a single BLE packet OTA given the file parameters.)
- ✧ Loop Mode (This mode continuously transmits by the total number of repeats given by the file.)

A file must be present, unless moving from the BLE RX app, in order to transmit a packet. Use the Open file button to select which file to transmit. Information on file format is found below. Once loaded, the screen will update the UI with the current packet to send. If there are multiple packets in the file, the screen will update this information based on which packet is being transmitted.

The Speed setting allows the user to adjust how fast the transmit occurs.

Current Speed table is as follows:

✧ Speed 1: 16ms per packet.

✧ Speed 2: 32ms per packet.

✧ Speed 3: 48ms per packet.

✧ Speed 4: 100ms per packet.

✧ Speed 5: 200ms per packet.

Note: Values are approximate based on a 16ms timer period.

The Channel setting allows you to select which channel to transmit on.

The Advertisement PDU Type setting allows you to select between various types of advertisement types.

The Random toggle allows you to randomize the MAC Address that you send out with each packet.

The Save Packet saves to file the current packet list in TX format to the name you specify.

The Switch to RX button will send you to the BLE RX App. See BLE RX App for more information.

The progress bar will update, (in Loop Mode), to show how many of the current packets are left to be transmitted. This is also seen by the Packets Left indicator on screen.

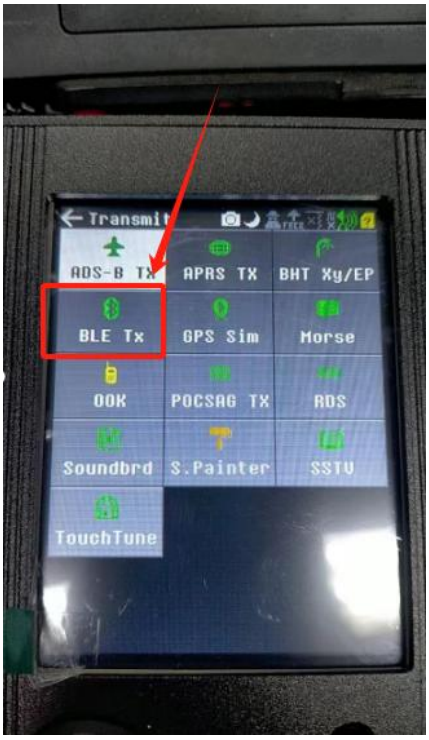
2.5 BLE Transmitter Operation Instruction

This chapter gives the detail operation instruction for the BLE Transmitter.

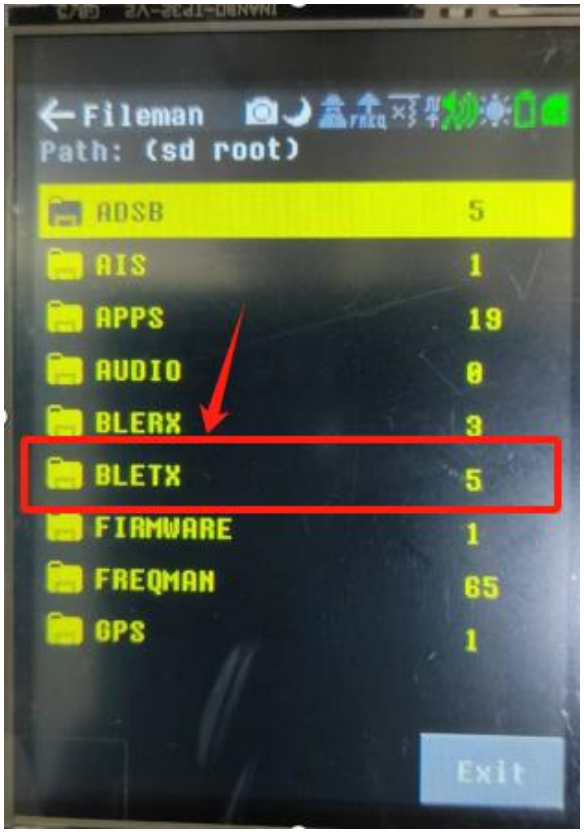
Step 1, Boot the device via one click the knob button of the device.

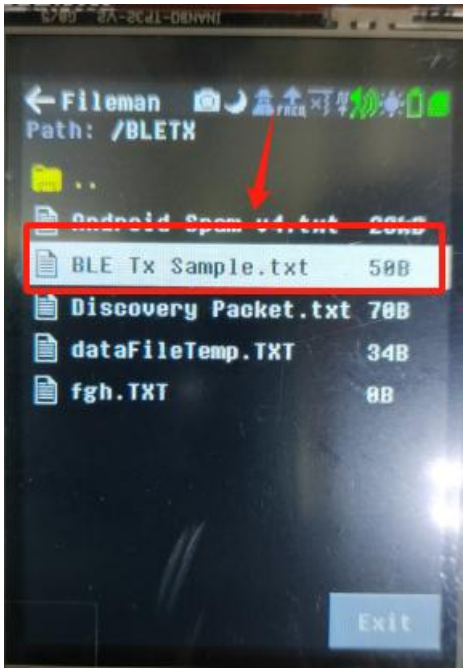
Step 2, enter into the top menu, find and click the menu Transmit;

Step 3, click the BLE Tx , enter into the BLE icon, then you will enter into the BLE transmit function.



Step 4, transmit the BLE signal. Click the <Open file>, and enter into BLERX file, find <BLE TX Sample.txt>.





Find the Loop parameter box, and one click the center button of these five buttons to enable it.

Step 5, click the transmit icon to send the BLE signals (one click the center button of these five buttons when your cursor move to the following icon). Then the device will transmit the BLE signal. You need to one click the center button of these five buttons to stop the transmitting.

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Any Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

-Reorient or relocate the receiving antenna.

-Increase the separation between the equipment and receiver.

-Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

-Consult the dealer or an experienced radio/TV technician for help.

FCC Radiation Exposure statement

The device has been evaluatec to meel general RF exposure requirement. The device can be used in porlable exposure condition without restriction.