First steps

Identify your device

There are many different versions of the PortaPack. It is important that you identify the correct version as this can affect how you install the firmware and device initial start-up. It is recommended you read the description of versions here. The H2 and H2+ versions are a slightly improved version, but the people making these copies never published the circuit diagrams or Code, hence breaking the license terms.

The main difference are the controls and the screen size, along with the codec and processor chip. The H2 / H2+ has extra circuitry to manage the battery charging and powering on/off. In this document, there is a brief description about the details. Check a more technical comparison here.

Up to date information

There is a Discord server "HackRF PortaPack Mayhem". This has all the current talk and information.

Power on/off

The original H1 powers instantly when you plug a power supply into the USB port. To turn it off, just unplug it. Similar to the issues with some USB cables while upgrading the firmware, the quality of your cable might affect the performance.

To power on/off the H2, you need to hold the middle button (knob or pushbutton) for few seconds. See more details here.

For most H2+ models, click the knob to power on, double-click the knob to power off.

Extra functionality (H2 and H2+)

Charging

This version can charge the internal lipo battery via the USB. There is a led indicator that turns off when the charging is done, but it might flicker. On some models (H2+) there are 4 leds below the knob that represent the state of the battery charge: 25%, 50%, 75%, 100%. When charging, one will flash dependent on the current charge state of the battery. See more details here.

Battery life

An internal battery between 1000 and 2500 mAh should last for several hours of use, depending on use of apps. The standby consumption is very low, around 52 µA, so you do not need to worry about having to remove/disconnect the battery in normal circumstances.

About firmwares

If you bought a standalone HackRF, it probably came with the GSG firmware flashed onto it. This enables usage over USB from a computer.

When buying pre-assembled HackRF + PortaPack bundles, they typically come with some version of the Mayhem firmware. One important thing to understand is that the firmware is always flashed onto the HackRF board; the PortaPack has no flash nor CPU. It is basically an interface module that enables standalone usage without a computer. It provides an LCD screen, buttons, an audio codec IC, an SD card slot, a coin cell battery to preserve settings and time between uses, and in some versions, a high-precision clock signal and a battery.

Although the Mayhem firmware allows you to directly use many functions in the field, standalone without a computer, it also provides a “HackRF mode,” which enables the user to start a version of the original GSG firmware and use your HackRF via USB, controlled by a computer. However, if you separate the two boards, you won’t be able to use the menu GUI and enable “HackRF mode.” So, if you want to use your HackRF board alone (detached), you’ll need to flash it with the GSG firmware.

In case you bought a PortaPack separately or want to upgrade your firmware, check out our Update Firmware page! Update firmware

Redirections on this manual/project

We are using Grabify to get statistics from our links. This may include affiliate links or involve multiple redirections.

Some ad-blocks and privacy lists can report/block these links. Please consider adding our links to your whitelist and sending a request to companies blocking this service, as it does not make sense—any service could be used to monitor clicks.

Usage cautions

⚠ The LNA of HackRF is sensitive and can get damaged! ⚠

Prevention

SMA port

- DO NOT swap the antenna while power is on.
- If you use an antenna that has an exposed metal part, DO NOT touch the antenna with you hands/body (Static electricity can damage the LNA).

Monitoring range

- You shouldn't receive near high power transmitters, even if it's not in the range that you are monitoring.

Diagnostic

- Try to listen to local radio. Try it with AMP both ON and OFF.
- Try to capture and replay a non-rolling-code. Try it with AMP both on and off.

Check more details about tx and rx issues.

Repair

How to replace the broken component

Intended use and Legality

> ⚠Warning

> This is not intended to be legal advice and should not be construed as authoritative, accurate or complete for your or any jurisdiction. You should seek the advice of a local legal professional to clarify the legality of your usage of HackRF One, Portapack and Mayhem for your jurisdiction.

Background

HackRF One

The HackRF One was originally conceived of and created by Security Researcher and Hardware Hacker Michael Ossmann. Previously Ossmann had created other devices primarily for security research in the area of RF. These devices include the YARD Stick One, a general purpose Software Designed Transceiver capable of transmitting and receiving signals below 1GHz, and the UberTooth One a device made specifically for Bluetooth Penetration Testing and Security Research.

The HackRF One can be seen as a logical progression from these devices, extending both functionality and frequency coverage.

Portapack

The Portapack was originally designed and created by Security Researcher and Hardware Hacker Jared Boone as a way to provide portable operating capabilities for the HackRF One.

Open Source Hardware and Software

All of the original source code, documentation and design files for HackRF One are copyright Michael Ossmann and licensed under the GNU GPL 2.0.

All of the original source code, documentation and design files for Portapack H1 are copyright Jared Boone and licensed under the GNU GPL 2.0.

The implications of the above are that anyone can take any of these source files and add, modify, extend and release their work, providing they make available on request, any additions, modifications and extensions they have made and license this under the GPL 2.0.

There is no restriction on using any of this for commercial gain. That being said, there is also no implication or warranty of fitness made by either the original authors or any subsequent contributors or vendors. Do your research and Caveat Emptor.

Intended Use

The HackRF One was originally designed as a tool for RF analysis and research, particularly in the domain of Information Security.

The Portapack was originally designed to facilitate the portable use of HackRF One for RF analysis and research, particularly in the domain of Information Security.

However, the HackRF One is fundamentally a general purpose Software Defined Radio. As such, it can be put to any use that a radio with similar characteristics can be. The Portapack is fundamentally a control surface for the HackRF One, and as such can be used for any general control of the SDR.

Unauthorised Access

Since much of the software and use-cases for the HackRF One and Portapack centres around Information Security Research, there is plenty of opportunity for getting into legal hot-water. The area of Security Research is as yet a legal grey-area, with many of the laws governing it being quite antiquated, and often not relevant to the technology of today. As such, it is advised that you only ever transmit where explicitly permitted, and when doing Security Research, that you only access or act upon devices you own or are explicitly permitted to access or act upon.

Transmitting

In general, it should be assumed that transmitting radio signals is not legal. Transmitting radio signals with intent, or lack of duty-of-care to cause interference, disruption or min-information even more so.

That being said, there are transmissions that are not illegal. Transmissions in the ISM bands are license-free in most jurisdictions, once certain power levels are adhered to. This is bearing the section on causing interference, above, in mind.

Amateur Radio Operators, depending on jurisdiction, license category, adherence to terms-of-license, local laws etc. have access to far more spectrum, and far higher power levels. Again, without causing interference through intent or lack of care.

Receiving

In general, in most jurisdictions, receiving radio signals is not illegal. Your specific case should be verified with a local legal professional.

Features

Your HackRF (the board under the PortaPack) has the ability to send or receive radio waves in a broad frequency range. Some of its specs are:

- Transceiver: Half-duplex
- Operating frequency: 1 MHz to 6 GHz
- Supported sample rates: 2 to 20 Msps (quadrature)
- Resolution: 8 bits
- Max TX power (you can also check an empirical measurement):
  - 10 to 2150 MHz: 5 to 15 dBm, increasing as frequency decreases
  - 2150 to 2750 MHz: 13 to 15 dBm
  - 2750 to 4000 MHz: 0 to 5 dBm, increasing as frequency decreases
  - 4000 to 6000 MHz: -10 to 0 dBm, increasing as frequency decreases
- Max RX power: -5 dBm. Exceeding -5 dBm can result in permanent damage! Can safely accept up to 10 dBm with the front-end RX amplifier disabled
- CLKOUT/CLKIN: 10 MHz square wave (0V to 3V for a high impedance load)

From that list that might be confusing for the first user, we could extract few interesting points:

- Half-duplex: Means that it can send OR receive, but not send AND receive in a particular instant.
- Operating frequency: goes from 1 MHz to 6 GHz, that means that the device is able to send and receive signals from almost all the common sources you can imagine. You can see the range with more details here.

PortaPack Versions (which one to buy)

Introduction

PortaPack is an add-on for the HackRF Software Defined Radio (SDR) platform that adds a touchscreen display, buttons, and additional functionality to transform it into a portable SDR device. There are many versions of PortaPack available on the market, created by different manufacturers, often with varying features such as larger screens, added charging capabilities, or different main chips due to price and availability.

This guide provides an overview of various PortaPack versions, their compatibility with Mayhem, and key differences between models. Please ensure you verify hardware compatibility with the vendor before purchasing, as manufacturers frequently change components without notice.

Table of Contents

Portapack Versions Comparison

There are many different versions of PortaPack, mainly due to Chinese companies putting their own take of the design such as adding a larger screen, adding charging or changing the main chip due to price and availability.

Most manufactures changes components frequently without notifying anyone, thus you should always ask the vendor the compatibility of their hardware before you buy, even if a specific vendor/store/seller already has a lot of positive reviews.

Asking which one to buy in the community is welcomed, however it could be not helping since things changing fast and no one can guarantee you that something will be 100% working.

The current list is:

Version	Compatible	Screen Size	Onboard Mic	Battery IC	GPIO Port	AK4951 Codec	WM8731 SSOP Codec	WM8731L QFN Codec	CPLD	INS 8002E Audio Amp	LTK 8002D Audio Amp	CS 8122S Audio Amp
H1 R1	👍	2.4"	✗	✗	✗		✓		QFP64			
H1 R2	👍	2.4"	✗	✗	✗	✓			QFP64			
H2M (Mayhem edition)	👍	3.2"	✓	✗	✗			✓	QFP100			
H2 (H2 R1)	👍	3.2"	✗	✗	✗	✓			QFP64			
H2 (maxgeek)	❓	3.2"	✗	✗	✗				QFP64			
H2 (old OpenSource SDRLab version)	👍	3.2"	✗	✗	✗	✓			QFP64			✓
H2+ R2	👍	3.2"	✗	✗	✗		✓		QFP64			
H2+ R3	👍	3.2"	✗	✗	✗		✓		QFP100	✓		
H2+ R4	👍	3.2"	✗	✗	✗			✓	QFP100		✓	
H2+ R5	👍	3.2"	✗	✗	✗							
H3	💩	2.4"	❓	✗	✗	✓			QFP64			
H3 mini/ H2 Plus	💩	3.2"	❓	✗	✗	✓			QFP100			
H4	👍	3.2"	✓	✓	✓			✓	QFP100			
H4M (Mayhem edition)	❤️👍	3.2"	✓	✓	✓			✓	QFP100			

> ⓘ Note
>
> - **Any** versions of H3 are **incompatible** (we will never do support of this hardware), do not buy them as they're scam.
> - "H2+" and "H2 Plus" are different devices, even if their names sounds similar.

Legend

- 👍 Compatible
- ❓ Compatibility unknown
- ✓ Included
- 🚫 Not compatible
- ❤️ Recommended

HackRF

If you want to support the original creators of the HackRF, we would highly recommend purchasing a GSG HackRF though one of their resellers listed here.
https://greatscottgadgets.com/hackrf/one/

FAQ

Q: Which one should I buy?
A: Please refer to the comparison table above.

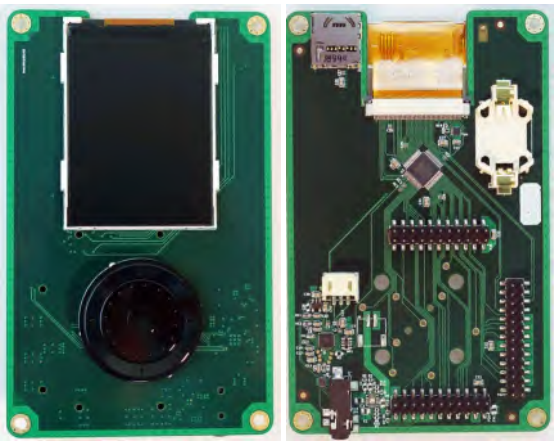
Q: Should I buy a pre-assembled unit or buy parts separately and assemble it myself?
A: It depends on your skills. If it's your first time assembling a device, there might be challenges. However, if you want an original/genuine HackRF, buying the parts separately is your only choice.

Q: How do I know if the device from a specific vendor/store/seller works or is compatible?
A: Check the hints at the top of this page and always verify compatibility with the vendor.

Detailed PortaPack Version Descriptions

Below are a more detailed look at the different variations of PortaPacks

H1(R1/R2)



Differences:

- The H1R1 has a WM8731 audio chip
- The H1R2 has a AK4951 audio chip
- Some versions have a touch screen while a lot of the clones do not

H2

Differences:

- Bigger touch screen
- Different control/button layout
- Built in battery

H2M (Mayhem Edition)

> Tip
> *Click the images to see them on their full glory*

Differences:

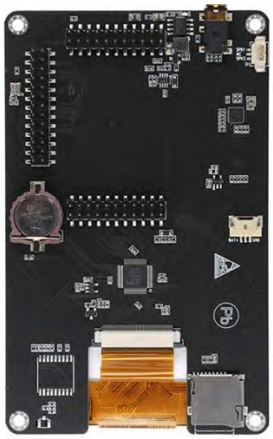
- Custom PCB built specifically for Mayhem with all the top contributors names silkscreened on the back of it and the Mayhem logo on the front.
- This usually comes with a new crystal clear case so you can see all the beautiful silkscreen art.
- Comes with a built in microphone.
- Has new CPLD code so the reboot button doesn't freeze the device unlike some of the other H2's on the market.

H2 (old OpenSourceSDRLab version)


Differences:

- AK4951 with 3W CS8122S Amplifier chip (INS8002e clone) -- speaker shuts off automatically when headphones plugged in
- NOTE: Do not enable AK4951 Speaker Output icon on title bar on this model or the AK4951 IC may overheat (CS8122S and AK4951 speaker outputs seem to be tied together on PCB)

H2+ R1



Differences:

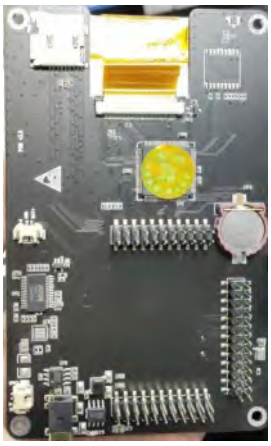
- Similar to H2 in early versions except claim for better TXCO spec(questionable) and board marked as H2+.
- Battery state indicator with 4 leds under Encoder Knob for 25%,50%,75%,100%,flashing while charging, steady when that level full.

H2+ R2

Differences:

- Similar to H2+R1 except using the WM8731 Codec and has an added audio power amp INS8002E. The front face of the board is marked as H2+ as in H2+R1 above.

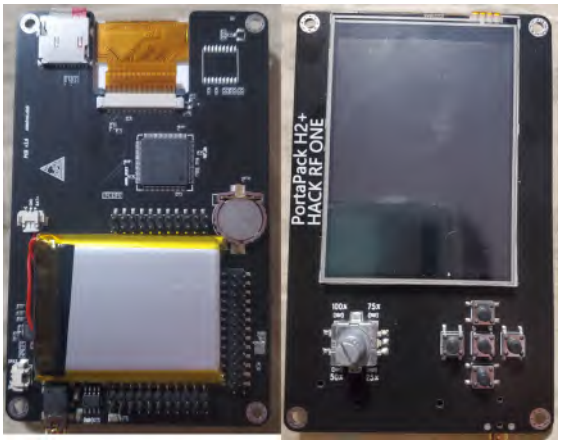
H2+ R3



Differences

- Similar to H2+R2 except
- This versions the standard CPLD 5M40ZE64CN5 was replaced with EPM240T100C5N (due to cost and supply issues by supplier "OpenSourceSDR Lab") which has caused some issues (they issued their work around fixes in a version 1.4.3) and resolved in version 1.5.x due to a lot of hard work.

H2+ R4



Differences

- Similar to the H2+R3 except it now uses the AG256SL100 IC as well as the 28 pin QFN WM8731L instead of the 38 pin QFN AK4951. Marked as "PCB v3.6 mmdvm.club".
- 3W LTK8002D SOP8 Class D amplifier for the speaker (INS8002e clone).
- Power IC IP5306 SOP8.
- Inserting headphone plug doesn't disable the speaker.

H2+ R5

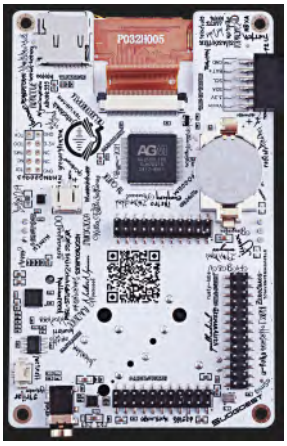
Bascially H2 with internal microphone and a independent power switch (but only pad/hole exist in some of the boards.)
Community reported it works (including the internal microphone), but other infomation are unknown.

H3

Uses custom close source firmware. **Not compatible with Mayhem. Do not buy or support as it's a scam**

This also exists as H2 Plus. Uses custom close source firmware (Ref.). **Not compatible with Mayhem(Ref.).

(NEW) **H4M (Mayhem Edition)**



> Tip
> *Click the images to see them on their full glory*

Differences:

- 🔌 GPIO port! The H4M adds a GPIO port so users can make their own add-ons for the H4M, just like the flipper.
- 🔋 Advanced battery management IC (battery %, voltage, current/draw, etc...)
- 🕹️ Single power on/off switch.
- 🚫 When powered off, the battery will no longer phantom drain.
- 📱 flat design, going back to the iPod style click wheel. (so no more broken buttons and encoders!)
- ⚡ Improved charge speeds.
- 🎙️ Built in mic (and mic switch between internal and external).
- 🖥️ Matte screen.
- 💎 This usually comes with a new crystal clear case so you can see all the beautiful silkscreen art.
- 🛠️ Custom PCB built specifically for Mayhem with all the top contributors names silkscreened on the back of it and the Mayhem logo on the front.

Where to buy?

Directly from the manufacturer OpenSourcesSDRLab
Worldwide - OpenSourcesSDRLab

- H4M & HackRF With Type C (R10C)
- H4M (with case, speaker and battery)

Worldwide - AliExpress

- H4M & HackRF With Type C (R10C)
- H4M (with case, speaker and battery)

US and EU - AliExpress

- H4M & HackRF With Type C (R10C)
- H4M (with case, speaker and battery)

Clifford's-version

The user Clifford Heath designed a version that added RF fronted protections, to prevent the easy-to-break LNA.

Testing

Some users (1) and GSG claim this modification weakens the signals to become even not acceptable.
Other users report that this version is more sensitive.

Results

Inconclusive for the moment

Conclusions

Inconclusive for the moment

Firmware update procedure

Common workflow

1. Update your SD card content
2. Connect USB cable
3. Use one of the following methods:
    - Enter HackRF mode, flash with hackrf_spiflash
    - Stay in Mayhem mode, use hackrf.app website (this automatically update external sdcard apps corresponding to the firmware version)
    - Copy firmware all in one tar package into SD card, and offline update with Flash Utility app in portapack (this automatically update external sdcard apps corresponding to the firmware version)

Detailed video guide

If you prefer watching a video guide, check this.

Detailed Firmware Update procedures

Using firmware file from github release page and the Flash Utility

- Get the latest firmware from the GitHub release (latest by date) page
- Copy it to your SDCARD, put it back in your PortaPack
- Flash it via the Flash Utility in "Utilities" menu on your PortaPack

> Note
>
> - If you don't see the Flash Utility app, try using other methods to update to latest version
> - The Flash Utility can also be used to program new firmware from a bin file stored on a MicroSD card

Using firmware file from github release page and the classic hackrf_spiflash tool

> Note
>
> ⚠ Using that method, you NEED to update the SDCARD content accordingly to the release you choose, else the external apps will not work !

Windows

1. Connect the device via USB.
2. Switch to HackRF mode via the on-screen option. (In the PortaPack)
3. Double click `flash_portapack_mayhem.bat` and follow the instructions.
4. Reboot the device.

Linux

1. Connect the device via USB
2. Switch to HackRF mode via the on-screen option. (In the PortaPack)
3. Upload the firmware with `hackrf_spiflash -w new_firmware_file.bin` (eg. portapack-h1_h2-mayhem.bin for mayhem firmware or hackrf_one_usb.bin for stock HackRF firmware)
4. Reboot the device

> Note
>
> - To Ubuntu and Mint user: Ubuntu based distro never maintains their repo for HackRF host (cli client) package. You'll face a lot of weird problems if your HackRF is R9. To resolve these, please compile the HackRF package yourself, or use another distro.

MacOS

1. If necessary, install the HackRF tools: `brew install hackrf`
2. Connect the device via USB
3. Switch to HackRF mode via the on-screen option (in the PortaPack)
4. Upload the firmware with `hackrf_spiflash -w new_firmware_file.bin`
5. Reboot the device

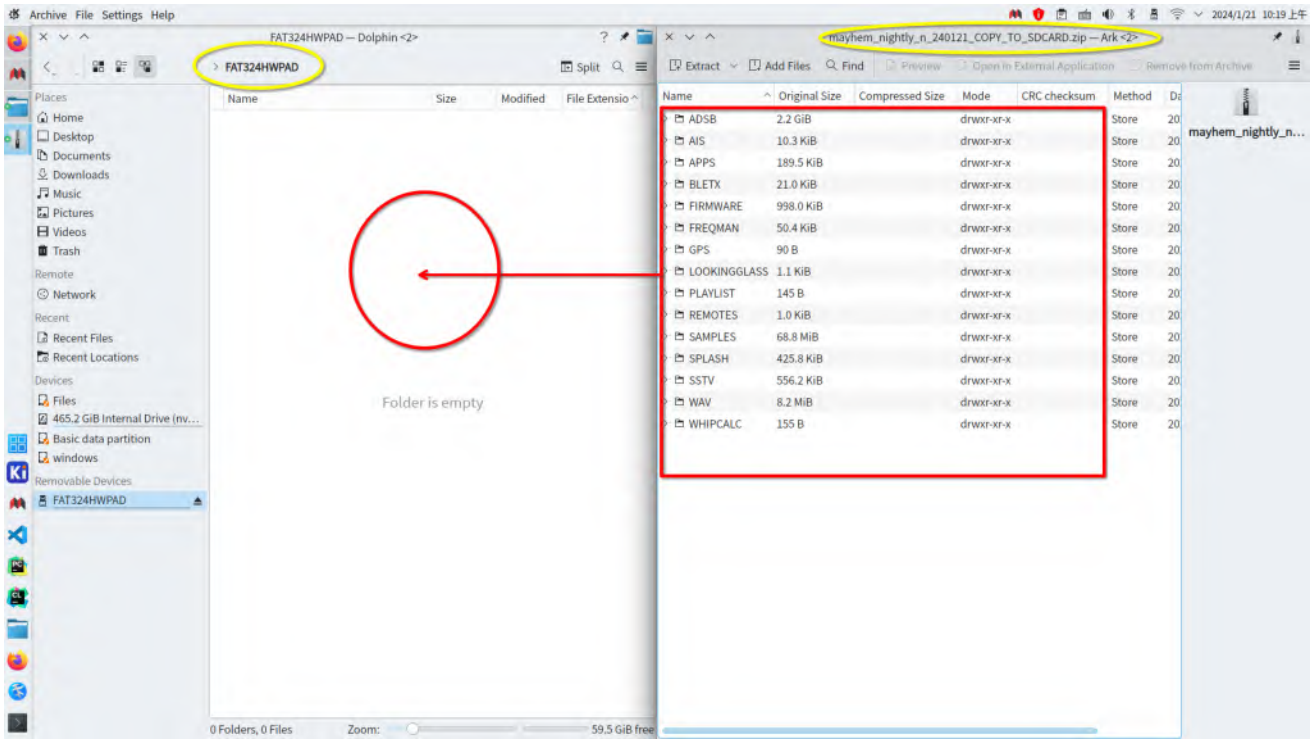
Update SDCARD files

You need to provide a MicroSD with enough space (16GB is recommended, over 32GB will be omitted due the limits of the FAT32). This is necessary for certain functionality, like the world map, GPS simulator, external apps, and others.

Get the latest files from the GitHub release (latest by date) page. You need to uncompress (using 7-zip) the files from `mayhem_vX.Y.Z_COPY_TO_SDCARD.7z` to a FAT32 formatted MicroSD card.

> Note
>
> How to put into SD card?
> Extract the root directory of the 7z archive into the root directory of your SD card.

- Don't put the 7z archive file directly into your SD card.
- Don't extract into any sub-folder of SD card.
- Don't use unbranded SD card.



Troubleshooting

- Please check this guide
- External apps (.ppma files in the APPS folder) will only function if their version matches the firmware version
- Please check the FAQ
- If your fimware version is lower or equal to v2.0.0 or nightly n_240114, you can only update firmware in HackRF mode with classic procedure
- Updating using the hackrf.app website is only working for stable version bigger or equal to v2.0.1, nightly version newer than n_240114
- When downgrading, please make sure SD card content versions match.
- Mayhem firmware contains HackRF firmware. You DO NOT need to flash HackRF firmware.
- In theory, it is impossible to brick the device, since you can always try the DFU recovery procedure. However, the updating might become fiddly in certain conditions. So you probably need basic computer usage knowledge (running/installing software, read documents, knowing USB ports, adjust system settings, reading English, etc.) if you don't, you probably should ask your friends or someone who knows these things to do it for you.

Updating the Xilinx CPLD on hackrf board

You can update the CPLD manually:

First get the original HackRF project into your computer:

```
git clone https://github.com/greatscottgadgets/hackrf
```

Then, connect your portapack into your machine, put it into HackRF mode and use the following command in order to update the CPLD:

```
hackrf_cpldjtag -x hackrf/firmware/cpld/sgpio_if/default.xsvf
```

LED1/2/3 blinking means CPLD program success. LED3/RED steady means error. Wait for the message 'Write finished' and power OFF / Disconnect your portapack from your machine.

Description of the hardware

External

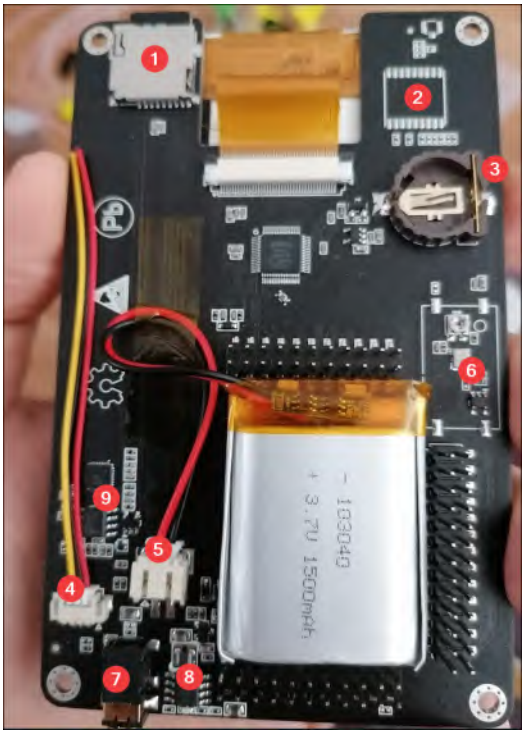
1. Antenna (the connector is a *female SMA*, so the antenna needs to be *male SMA*, and not *RPSMA*)
2. Encoder thumb wheel (on the H1 has a different layout, but the same functionality). Pushing the wheel down once to turn ON, or twice quickly to turn OFF.
3. Directional pushbuttons and Enter/Select in the center
4. CLK IN
5. CLK OUT
6. Micro usb port and next to it, charging led indicator (in the H2, this might flicker while charging but will *mostly* turn off when the battery is full)
7. Headset/Microphone (standard smartphone 4 segment 3.5mm connector)
8. Receive and transmit leds (indicates the current operation, since the HackRF is half-duplex, only one of this will be lit at every moment)
9. Other status leds (1.8V: rail status, RF: internal power supply, USB: connection to host is active)

   Note: In normal operation, 3.3V, 1.8V, RF lights will be ON.

10. DFU mode button (check the firmware update procedure for details)
11. 3.3V rail status led
12. Reset button

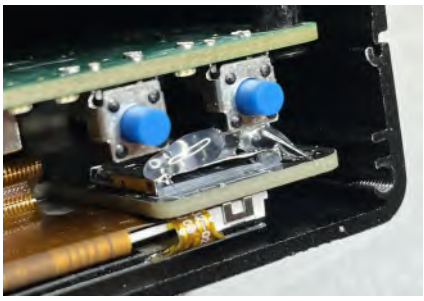
Check care of PortaPack/HackRF for general guidelines of how to take care of your device.

PortaPack internals



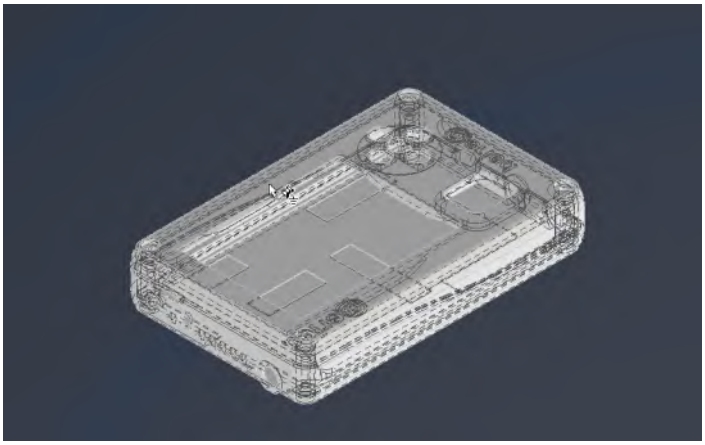
1. MicroSD card slot (insert the card with the contacts looking to the same direction as the screen)
2. GPS module option (has not been implemented)
3. Memory backup coin cell (compatible with CR1225 or CR1220 in the H2, and with the CR2032 or CR2025 in the H1)
4. Speaker connector (yellow and red go to the speaker coil, black is ground and can be left disconnected)
5. Battery connector

6. TCXO clock (it might be populated with SMD components like in the upper image, unpopulated or populated with a shielded module)
7. Headset/Microphone jack (In case of the H2 the internal speaker switches automatically when the headset is plugged)
8. USB charging circuitry (only the units with battery; this is a standard power bank chipset)
9. Audio amp circuitry

> Tip
> Adding a small bead of hot-glue on the top of the SD card slot, as shown here, will prevent the SD card from falling down inside the case when it's being inserted.
> 

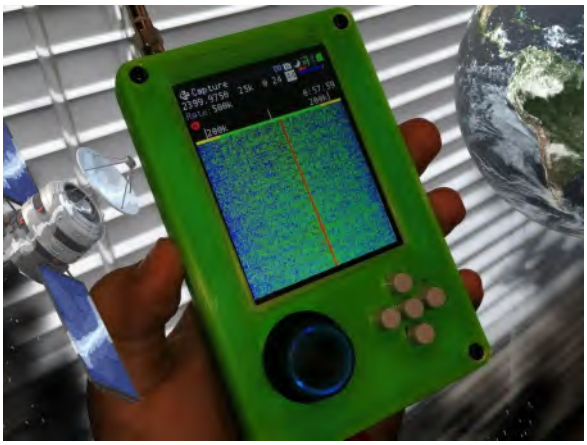
3d printed enclosure

The first enclosure was made around march 2020, combined with the first versions of this firmware. For technical information about this check here.



H2

Many PortaPacks on AliExpress come with a metal or plastic enclosure. Enclosure dimensions, simplicity of assembly/disassembly, connector labeling (if any), and speaker hole positions (if any) varies by supplier. Some users feel that a metal enclosure is safer for devices that contain LiPo batteries.
You can 3D-print the following enclosure for your Portapack:



Encoder knob:

And the following magnetic cover (consider that most of the commercial cases that clone the design of the enclosure include plastic screws, hence this wont work):

If you do not own a 3d printer, you have other options:

- Weerg for a high quality print
- 3DHubs for a low cost alternative
- Tindie another alternative, with a lot of customization options
- Injection moulded version of the case

If you need a different design, or material, check more options directly in Aliexpress.
For a comparison between the results of the different fabrication techniques, check: https://youtu.be/lB-vc-Y13PM

Assembly

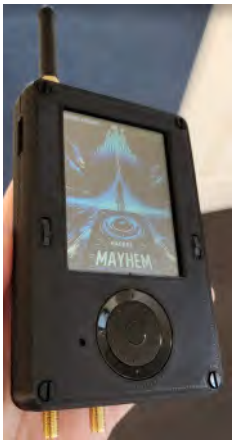
Check the `assembly.pdf` from the case files for instructions.

Speaker

You can easily place a small speaker inside. There is no holes in the case but it seems that the sound quality actually improves with the case:
https://www.youtube.com/watch?v=XkaGV9muvbg
Check more details about the speaker (details and wiring) here.

H4M

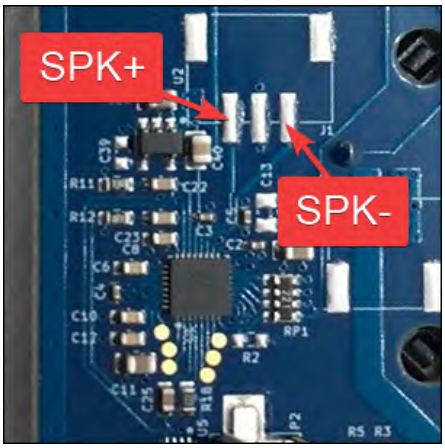
This version includes a new knob, switches and other refined features, while keeping the compact size:



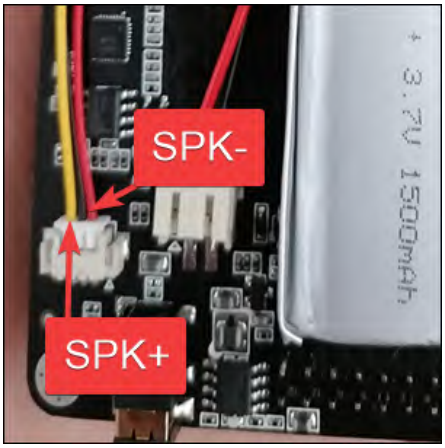
Internal speaker

Pinout

Both versions have a similar layout for the pins you need to use. In the H1, the connector might not be populated and look like this:



On the H2, normally the connector and cable (use the red and yellow wires, isolate the black one) is included as seen here:



For both versions, you need a small speaker. Typically a laptop speaker will work, for example: https://a.aliexpress.com/_mLuZk4U

Connect `SPK+` and `SPK-` to the speaker and use double sided tape to fix it to the PCB.

Speaker test: https://www.youtube.com/watch?v=XkaGV9muvbg

Additional details

A speaker has two wires, `SPK+` and `SPK-`. While there is no sound, the speaker floats on a magnetic field in the middle of its range. When `SPK+` is high the speaker moves forward. When `SPK-` is high the speaker moves backwards. The distance forward and backwards depends entirely on the voltage level.

On the PortaPack, the speaker connector has 3 pins.

`SPK+` is the pin nearest to the edge of the board `GND` is the connector in the middle, skip it `SPK-` is towards the centre of the board

H1 specific setup

On the H1 with an AK4951 codec, when you add the new speaker you may find that there is no audio. In this case, use the speaker icon on the title bar to enable the speaker output (grey with "X" indicates muted; green with no "X" indicates it's unmuted).

Warning: Do not set the speaker icon to "unmuted" if the speaker already works when "muted", as on one model of the OpenSourceSDRLab PortaPack H2 which has two audio chips with their outputs tied together (overheating will result if they're both enabled).

SMD buttons and caps

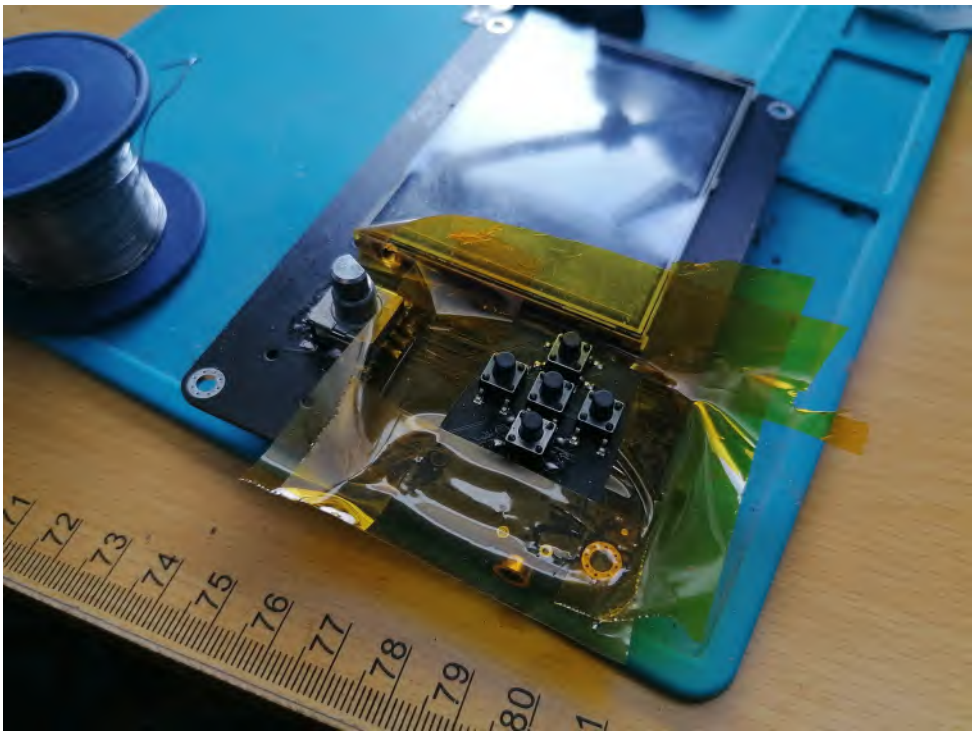
Push-buttons

Current PortaPack models have five push buttons on the front (UP, DOWN, LEFT, RIGHT, and SELECT) and two on the top (DFU and RESET). In most cases, a long press of a directional button will repeat automatically after a short delay (firmware may define additional behavior for a long press of any button).

If the push buttons "stick", check to make sure that the buttons are centered in the holes in the case, and are not rubbing against the inside of the holes.

If the push-buttons are intermittently unresponsive, first make sure that the Portapack firmware is upgraded to version 1.7.1. or later, which improves handling of glitchy switch contacts. The type of push-buttons used on the Portapack is SMD tactile switches of 6 mm per side and 7 mm of height. You can buy replacements here: https://a.aliexpress.com/_dZqx4vv

The easiest way to remove them is to clip the legs off, clean the pads carefully with solder wick and solder the new buttons.



You can also find replacement caps for the tactile switches: https://www.aliexpress.com/item/1005001700437278.html
Alternative caps for the switches: https://www.ebay.com/itm/284831256446

Encoder knob

> Note
> This section is mostly talking about H2

Encoder for H2/H2+ uses a 30-step EC11 encoder with push button and shaft length of 12.5mm.

A short press of the push button turns on the PortaPack; a long press or two short presses turns off the PortaPack. If no click is felt when the knob is pressed, there may be insufficient clearance between the knob and the case, in which case some padding may be added inside the knob shaft.

A malfunctioning rotary encoder may sometimes work better if the knob is pressed slightly to the left when rotating. Make sure that the Portapack is running firmware version 1.7.1. or later, which improves handling of glitchy switch contacts. Encoder dial sensitivity can also be modified in Settings.

Plastic knob

Depending on the shaft of your encoder, you can use diverse knobs:

Encoder Replacement on PortaPack H2

Disassemble the device

1. Unscrew the screws and SMA connector rings.
2. Pull apart the case and carefully separate the PortaPack from the HackRF by gently pulling upwards to disconnect the pins.
3. Disconnect the speaker and battery.

Removing the Encoder

The encoder is mounted in a way that makes it difficult to desolder due to pin placement. If you are having trouble with this, try the following technique:

1. Use a pair of tin snips to cut the encoder's leads and remove the encoder.
2. Apply flux to the solder pads.
3. Carefully heat each pad with a soldering iron, one by one, to remove the clipped leads. This approach reduces strain on the pads and lowers the risk of tearing up the traces.

> ⚠ Warning
> The upper-most pin is close to the screen, take care not to scorch it with your soldering iron.

Installing the Replacement Encoder

The replacement rotary encoder will likely have long leads designed for through-hole mounting. However, the PortaPack uses surface mounting for this component, so the leads will need to be trimmed down. Here's how to do it:

> ⓘ Note
> Correct lead length is important to avoid clearance issues when reassembling the case.

1. **Trim the Leads:** Shorten the encoder leads so that they are approximately flush with the body of the encoder. This will ensure that the encoder sits stably and doesn't increase the height of the assembly.
2. After trimming, solder the encoder on the PCB, taking care to align it correctly before soldering.
3. After soldering each pin, do a visual inspection to ensure there is good electrical contact.

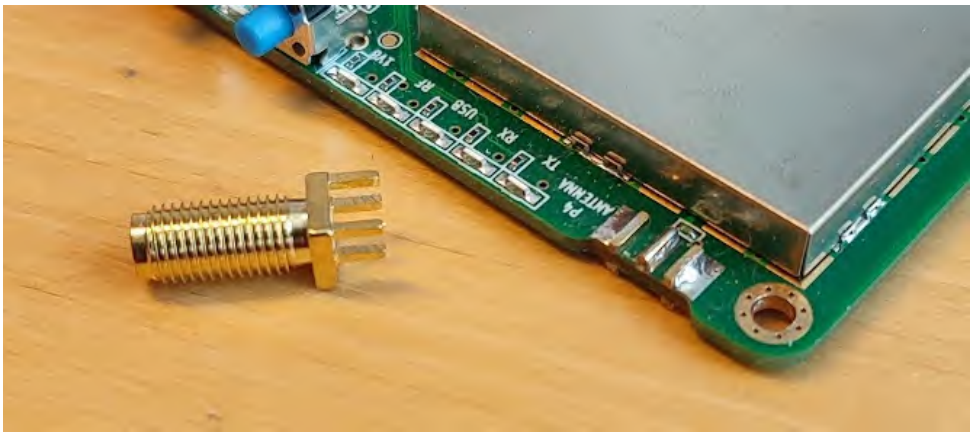
Reassembly

Once the new encoder is in place, follow the disassembly steps in reverse to reassemble your PortaPack.

SMA Antenna connector

> ⓘ Note
> It is a good idea to protect the antenna connectors with a silicone cover

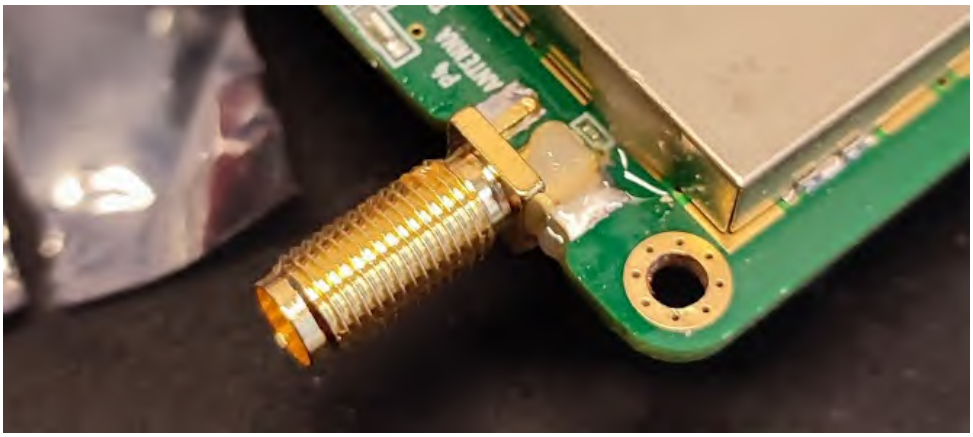
The antenna connectors on the HackRF board are the `18.5 mm` variant available here.
Notice that you *could* fit the `SMA-KE 18.5mm` variant, but it will be not the perfect fit for the type of pcb mount used in originally.



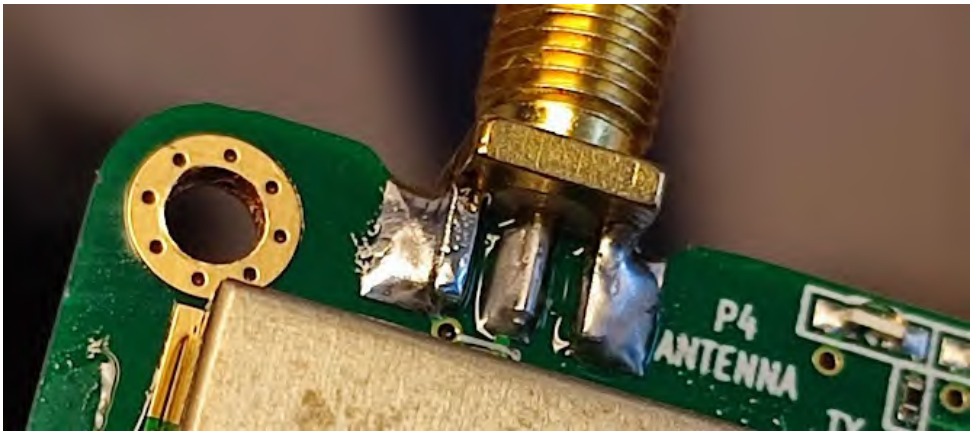
Replacing a broken connector

1. Desolder the original, use enough flux (i.e. this "self cleaning" variant) and fresh solder. If there is parts of the SMA connector still there, it might be more difficult to remove because the thermal mass.

2. Clean the pads
3. Place the new one. It will be very tight. Align it correctly



4. Solder and clean the residual flux

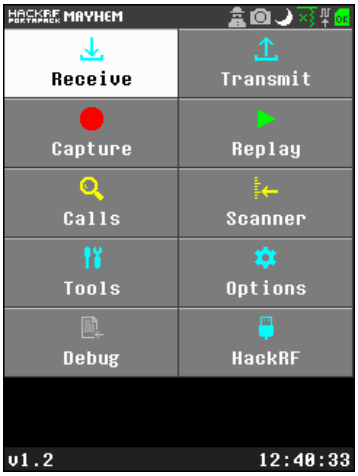


User interface

Boot splash screen

From version 1.4.2, you can set a custom boot splash screen.

Main screen



The Main Screen of Portapack Mayhem comprises two main regions:

- Title Bar
- Main Menu

Splash screen

Introduction

Are you bored of the standard power on screen?
Do you want your own image at power up to personalize your device?
You can!

Save a **240x304 24-bit BMP file** named `splash.bmp` in the root of the SD card, and it will be used as a starting up splash screen !

Beginning in firmware version 1.7.4, the splash screen BMP files stored on the SD card can be viewed in the File Manager application and set to be the current splash screen with a single click.

You can share and get ready to use images in the `#splash-screens` channel over our Discord group.

There is also https://ppsplash.creativo.hu/ where you can choose and download splash screens from a curated selection

You can of course use https://hackrf.app/ to upload them directly to SPLASH directory (firmware version >= 2.0.1 is needed)

⚠ If your firmware is recent enough, it may support activation/deactivation of the splash screen via a checkbox in Settings/User Interface/Splash Screen. Don't forget to check it if the splash screen isn't displayed at startup ! ⚠

Example

Tools / How-to

Use your favorite picture editor to adjust size, or use "convert" from ImageMagick, which is a powerful image manipulation tool. It is open source and available for all common operating systems.

To just scale the picture down, use:

```
$ convert source.jpg -resize 240x304 destination.bmp
```

If you see and don't want a frame left and right, you can adjust the convert with:

```
$ convert source.jpg -resize 240x304 -gravity center -extent 240x304 destination.bmp
```

To choose the filling color when resizing/extending the image, add '-background color' after 'source.jpg':

```
$ convert source.jpg -background "#000000" -resize 240x304 -gravity center -extent 240x304 destination.bmp
```

or

```
$ convert source.jpg -background black -resize 240x304 -gravity center -extent 240x304 destination.bmp
```

The list of predefined colors can be obtained with `convert -list color`

To check if the splash got the required parameter, check:

```
$ identify destination.bmp
destination.bmp BMP3 240x300 240x304+0+0 8-bit sRGB 216054B 0.000u 0:00.000
```

If it is saying '8-bit', you're good. It's the number of bits by color components. For sRGB, 8+8+8 = 24-bit

Limitations

- image have to be a 24 bits bitmap
- width have to be exactly 240 pixels wide
- height have to be in the [1 , 304] range. Any additional lines will be cut

Title bar

The PortaPack Mayhem title bar consists of a number of icons, some of which trigger actions and some of which are used to indicate the status of certain subsystems. In some older versions, the title bar also contained either the application name or firmware name and version in the form **MAYHEM vX.Y.Z** where the versioning is consistent with the standard semantic versioning (major.minor.release) format. This was moved to the footer in latest versions.

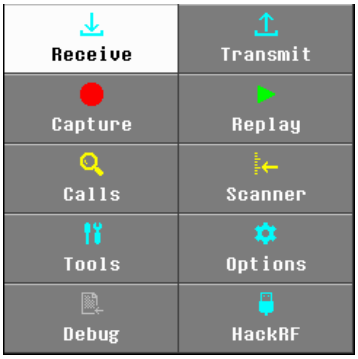
Actionable icons can be accessed by touch, or by using the directional buttons (H2) or the directional ring (H1) to move the highlight that indicates which icon is selected. If the highlight is on the main menu, using the *up* button will move it to the title bar.

Infrequently used icons may be hidden using Settings -> User Interface, if desired.

The sections of the title bar, along with their functionality, are (from left to right):

Image	Function	Actionable
Back	Back arrow to previous screen/Return to menu	Yes
Name	Application name, when click -> same with Back	Yes
	Take screenshot	Yes
	Activate sleep mode	Yes
	Toggle stealth mode. Green if selected	Yes
/	Toggle Up conversion or Down conversion. Green if activated.	Yes
/	Toggle DC power on antenna port. Yellow if selected	Yes
	Indicate status of external clock. Green if selected	Yes
/	Enable/mute audio (speaker & headphone)	Yes
/	Enable speaker output on PortaPack with AK4951 codec. Green if activated. Warning: Do not enable if speaker already works when disabled, as on OpenSourceSDRLab PortaPack H2.	Yes
	Brightness adjust	Yes
	Indicate presence of SD card. Green if SD card was found	No

Main menu



The Main Menu page of Mayhem comprises a number of buttons to access the various functionality groups of the firmware, a Title bar giving functions and at the bottom of page, the version number and if enabled in options the time.

Button	Functional Group
Receive	Receiver Applications
Transmit	Transmit Applications
Capture	Permit Recording or 'Capture' of RF to facilitate analysis or Replay Attack
Replay	Transmit a previously recorded RF Capture file
Calls	Detect any signals within a specified bandwidth, similar to 'Close Call function on scanners
Scanner	Step through a list of pre-defined frequencies, stopping if squelch is broken (signal detected)
Tools	Covers Frequency manager lists in SD card,File manager,Signal Generator,WAV File Viewer,Wipe SD Card,Antenna Length Calculator

Button	Functional Group
Options	Audio tone setting,Radio Settings,UI Interface settings e.g.Clock,Set Date/Time,Touch screen Calibrate
Debug	Covers Memory use,SD Card info,Peripherals use,Temperature,Button and Encoder Test
HackRF	Switch to HackRF mode for use from a USB Host device (eg. computer)

Main Controls

Frequency

When a Frequency field is selected, the frequency can be updated in several ways: Turning the encoder dial will adjust the frequency by the Step size. A short press of the select button will bring up a screen where the frequency can be entered directly. A long press of the Select button allows enters a mode where individual digits may be adjusted using the dial (press Select again to exit this tuning mode).

Step size

The step size when changing frequency can be changed as a secondary function when the frequency is selected. The range of settings are: 10M,1M,500k,250(N2),100k(FM2),50k(FM1),25k(EU NFM),12k5(EU NFM),10k(US AM),9k(EU AM),8.33k(AIR),6k3 (EU DIG),5k(SA AM),3k,1k,100Hz, 50Hz and 10Hz.

Bandwidth

It is often the case that the PortaPack user does not know the filter bandwidth to use or what they have selected. The system uses: Finite Impulse Response (FIR) Filters and the settings are held in the dsp_fir_tap_hpp file, and are selected from the use interface. They can be selected for different modulation modes.

- **NFM:** It should be noted for the NFM, there are 3 emission types 16KF3E (16k),11KF3E (11k)and 8K5F3E (8k5) .The 16k option should be selected when the channel spacing is 25kHz. For 12.5kHz then normally 8.5kHz should be used, but some over modulated system may benefit with using the 11kHz bandwidth filter.
- **WFM:** This is emission types 200KF8E emission type. The Wide Band filter is limited to 96kHz stereo signal and then combined to a 48Khz mono signal.
- **AM:** The AM emission types supported are:
- *9K00A3E for AM double sideband 9kHz.*
- *6K00A3E for AM double sideband 6kHz.*
- *2K80J3E for AM Lower Side Band LSB -3 - 0kHz.*
- *2K80J3E for AM Lower Side Band USB 0 - 3kHz.*
- *150HA1A / 150HJ2A for AM Continuous Wave. The filter is 200 Hz wide and centred around 700Hz.*
- **TPMS:** This is a non standard specialized shaped filter that is 200kHz wide.

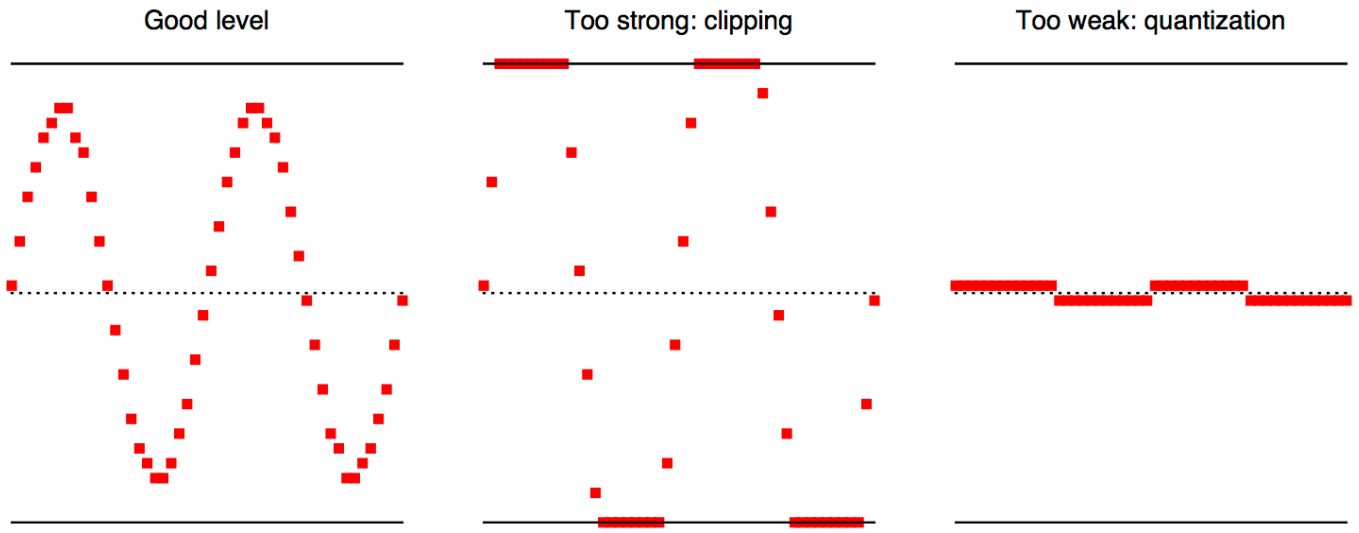
Gain Controls

The Gain Controls are critical to the best use of the PortaPack / HackRf. HackRF provides three different analogue gain controls on RX and two on TX. The three RX gain controls are RF “amp”, 0dB or +14 dB),”IF“ 0 to 40 dB in 8 dB steps), and baseband Vga (0 to 62 dB in 2 dB steps). The two TX gain controls are at the RF (0 or 14 dB) and IF (0 to 47 dB in 1 dB steps) stages.

HackRF has two RF amplifiers close to the antenna port, one for TX and one for RX. These amplifiers have two settings: on or off. In the off state, the amps are completely bypassed. They nominally provide 14 dB of gain when on, but the actual amount of gain varies by frequency. In general, expect less gain at higher frequencies. For fine control of gain, use the IF and/or baseband gain options.

It should be noted in the PortaPack, **the RF settings are called either “Amp” or not labelled**, and may be shown next to the IF / Baseband setting as a “0” or “1” for RX or in the case of Audio App it appears when you select either IF/ Baseband gain as "Amp" on the line below. For the TX then its shown as “0” or “14" this adds 14dB of gain to the output signal.

A good default setting for RX is to start with is RF (Amp=0) i.e. RF amp is off, IF=16, Baseband=16. Increase or decrease the IF and baseband gain controls roughly equally to find the best settings for your situation. Turn on the RF amp if you need help picking up weak signals. If your gain settings are too low, your signal may be buried in the noise. If one or more of your gain settings is too high, you may see distortion (look for unexpected frequencies that pop up when you increase the gain) or the noise floor may be amplified more than your signal.



To get the optimal level use the radio saturation monitor in the radio section of the DFU Overlay.

SD Card content and modification

The SD Card provides a memory resource that can be tailored to the specific user. Technical details of the card are given here. The SD Card Standard image is supplied as part of the standard firmware download. Instructions for its use are supplied elsewhere. The following folders on the SD Card contains various app-specific information (some of these folders are included in the SD Card image file, and some may be created afterwards either by firmware or by the user):

- **ADSB:** The ADBS Folder has databases of Airlines, IACO and is where the world map is located. See separate page on how to generate the map.

- **AIS:** Holds the AIS database.
- **APPS:** Holds "external" apps. Several apps have been moved from firmware flash ROM to external files (with .ppma extension) stored on the SD card, to make room in the Mayhem ROM for new apps and features.
- **APRS:** Holds log files from the APRS-RX app.
- **AUDIO:** Holds audio recordings (WAV) from the Audio app.
- **BLERX:** Holds log files from the BLE-RX app.
- **BLETX:** Holds files for the BLE-TX app.
- **CAPTURES:** Holds IQ capture files (C16/C8 and their metadata TXT files) from the Capture app.
- **DEBUG:** Holds various debugging log files.
- **FIRMWARE:** bin files can be placed here and used to update the PortaPack firmware without a computer.
- **FREQMAN:** Holds FreqMan DB files which are lists of frequencies that can be loaded by various apps. They can be viewed and edited using the FreqMan app.
    - **Fixed frequencies in Apps:** It should be noted that in some Apps that the frequency ranges are fixed in the App and are not selectable in from FREQMAN lists. Example of this are "AIS" and TPMS. (In some cases the .ini settings file may be modified manually to change the frequency and other settings that aren't configurable when running the app itself.)
- **GPS:** This file holds information on how to generate GPS-Simulation files.
- **LOGS:** Holds log files for various apps like ADSB, POCSAG, ERT, etc.
- **LOOKINGGLASS:** This folder holds a text file that is used in the LOOKINGGLASS App and is a list of the frequency scan ranges and a description. It should be noted that this APP can have only have ranges that are a minimum of 240MHz in size.In addition the range must start form 10MHz. the nominal Minimum operational frequency of HackRF. Therefore you need to consider this in planning the frequency range listed. For example you could not have a range for VHF amature band , You can only have a range from 10-250 MHz. These are very wide ranges in keeping with the Ap concept of Wide Scan of the spectrum.
- **PLAYLIST:** Holds playlist files (PPL) for the Replay app.
- **REMOTES:** Holds remote files (REM) used by the Remote and TouchTune apps.
- **SAMPLES:** Holds an example of some settings for the use in OOK TX App
- **SCREENSHOTS:** Holds screenshots (SCR) taken on the device.
- **SETTINGS:** Holds settings for applications. If you're having a problem with an app, try deleting its settings file to restore defaults (the .ini file will be rewritten any time an app is exited). An optional "blacklist" file may also be stored in this directory (lists any unwanted apps).
- **SPECTRUM:** Holds BMP images for the Spectrum Painter app.
- **SPLASH:** Holds custom splash screen BMP files. (Note however that the currently-active splash image file must be in the root directory and named "splash.bmp").
- **SSTV:** Holds some Standard Images for the use in the SSTV app.
- **WAV:** Holds sound files that are used in the SoundBoard app.
- **WHIPCALC:** Holds information on the Whip lengths that are used in the App calculation. Additional Whips can be added with their specific details.

SD card contents can be viewed/edited using the File Manager application, or via USB from a computer using the "SD over USB" app, or the physical SD card can be removed from PortaPack and plugged into a computer. Use caution when reinstalling the SD card into the PortaPack as it may fall into the device and require case disassembly to fetch it.

NOTE: The File Manager app currently has a memory limitation; an "out of memory" fault may occur with a large number of files in a single folder (more than about 80, depending on firmware version).

Text Entry

The text entry view allows you to modify text. Use the buttons on the screen to update the text field at the cursor. For the most part this is self-explanatory, but there are a few features that are worth pointing out.

- **Cursor** - with the text field selected, use the encoder or the left/right buttons to set the cursor position.
- **Insert/Overwrite** - with the text field selected, pressing the select button will toggle between insert and overwrite modes. Overwrite mode will invert the cursor to indicate it is active.
- **Delete-to-Cursor** - Long-press select in the text field to delete all the text up the cursor position.
- **Raw byte entry** - with the raw number field selected, use the encoder to select a byte value. Pressing select will enter that byte value into the text field. This can be used to insert a byte or a .
- **Mode button** - pressing the mode button (lower right) will toggle the keyboard between Alpha and Numeric/Symbol modes.
- **<DEL** - Delete the specific char which is before (at the left of) the cursor.

Backing out of the control will not save changes. Changes are saved when the OK button is pressed.

Powering the PortaPack

The Portapack H1 or H2 are powered via the USB 2.0 connector on the HackRF One. In the case of the H2, it can have an internal LiPo battery that can be charged via the USB 2.0 socket.

The maximum size of battery that can be installed in a typical metal cases is 2500mAh, but 2100mAh would be a better fit.
Based on testing the Portapack/HackRF consumes between 250mA (1.25W) when just menu screen is on and 550mA peak (2.75W) when audio is at full volume and receiving signals.

In the cases of charging from the USB, then the peak of 1.5 A is seen with the portapack in use though does drop as the charging takes place. The charge rate of the battery is a peak of about 1000mA dropping back to 600mA-700mA and takes between 3-4 hours to charge depending on battery size and the quality of the cable,longer cables will charger slower.

When on an internal battery (say 2500mAh) the Portapack H2, has between 4-5 hours of life depending on use and battery state.

Battery charger modifications

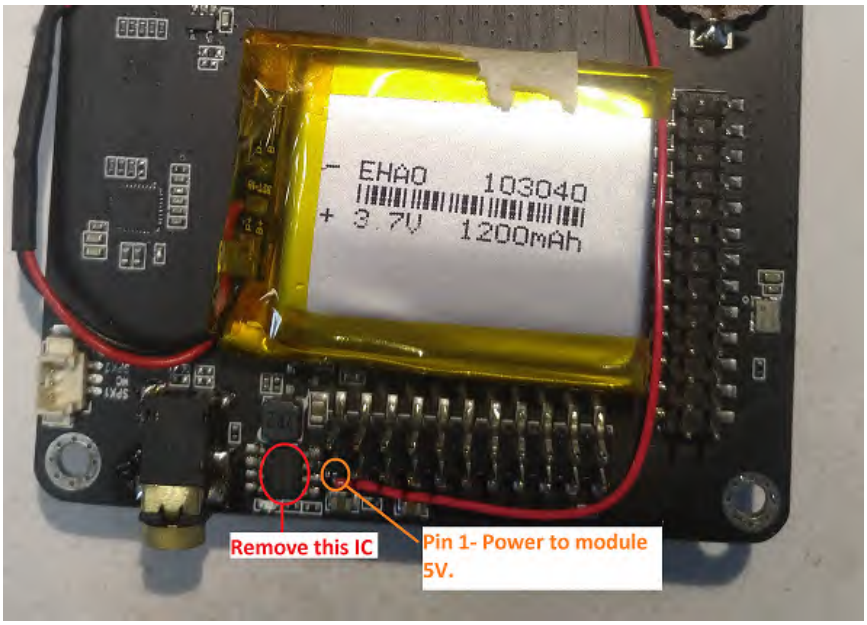
When connected to the computer or a powerbank, with a visible signal on the portapack or PC screen, some have interfering and harmonic signals that can be generated by the battery charger of the portapack itself. Before doing any modifications you have to ensure yourself that the problem is really coming from the charging. Some users have the problem only when the battery is not full, so do not have it at all.

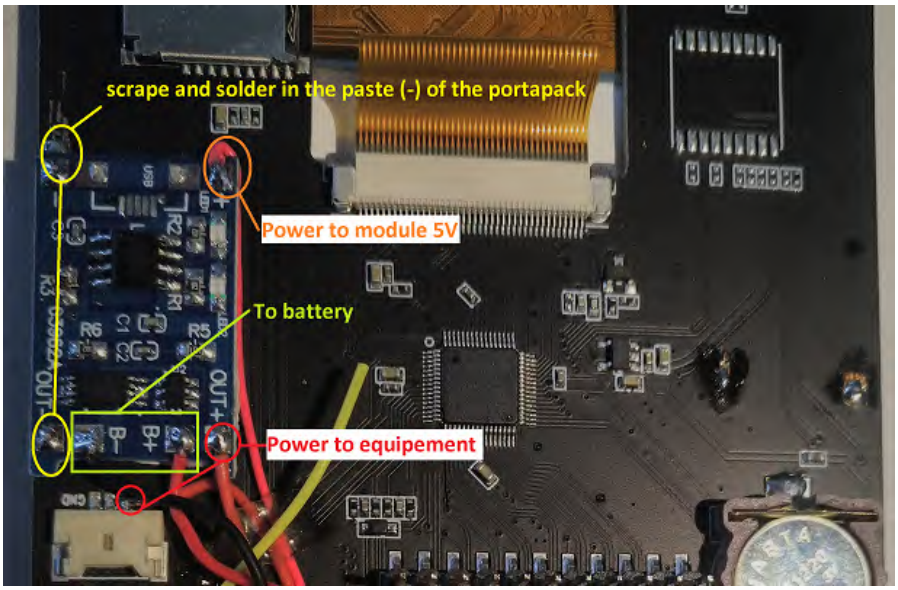
If you identified the problem correctly, you can try to solve it by discarding the charging IC module in favor of an IC module like tp4056, with battery overcharge protection (4.2V), battery discharge protection(2.9V) and with battery charge current control (for that you have to change a resistance in the module).

With this battery charging module, even using a powerbank, the interference due to the old noisy charging IC is gone.

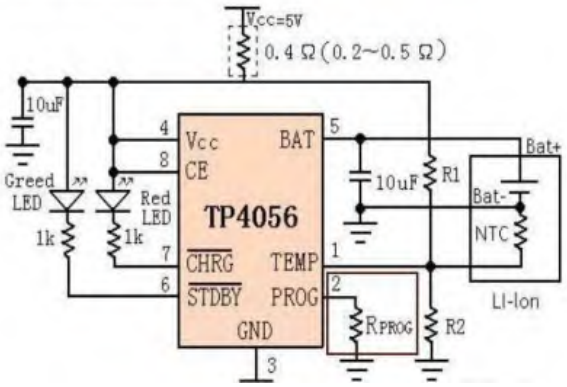
See the following pictures for more informations, and take a look at the related issue


TP4056 Lithium Battery Charging Processor
DW01A Lithium Battery
Protection Circuit
input: 4.5 - 8.0V
max. 1.2A
charging:
4.2V, max 1A
output:
Vbatt, max. 3A
Charging Indicator
Charging End Indicator
8205A Dual Power MOSFET
Battery Disconnect Switch


EHAO
103040
3.7V
1200mAh
Remove this IC
Pin 1- Power to module
5V.



RPROG (k)	IBAT (mA)
10	130
5	250
4	300
3	400
2	580
1.66	690
1.5	780
1.33	900
1.2	1000



SolveBoard

Problem	Solution
Does not boot / white screen / black screen	Check Won't boot and Config Menu.
Only turn on once after flashing	Flashing with DFU only make the firmware go to RAM. You need to flash to the SPI flash once again(with regular flash methods)
Crash / Guru Meditation.	Try Full reset. If still does not work, try Updating the Xilinx CPLD on hackrf board. If nothing works, report an issue on GitHub.
Freeze when launch specific app (but no crash or Guru Meditation)	It's mostly from power part. Try: -Full charge -Change battery -Plug into a reliable power source -Change battery -Change at least 5 cables -Remove addon board if plugged in
No splash screen / No time & date / Touchscreen does not work / Status bar icon disappeared / Backlight timeout abnormal / Encoder dial abnormal	Check settings.
It says xxx missing / can't find xxx / xxx read error / xxx is outdated / xxx empty or you can't see xxx.	Make sure sdcard contents matches your firmware version.
Apps are missing or greyed out after upgrading.	Make sure sdcard contents matches your firmware version, particularly the external APPS folder, and make sure you correctly put the sdcard contents.
`hackrf_info` says `Hardware does not appear to have been manufactured by Great Scott Gadgets`	It's because you have a Hackrf clone instead of original from GSG. If you believe it's a mistake, contact the seller or GSG official support.
Unexpected spike on my waterfall / IQ / spectrum.	It's either a DC offset or noise from power. For reducing the noise, try using the internal battery. For DC offset, there's nothing you can do, however it's normal on SDR.

Problem	Solution
My computer can't see my HackRF	Try at least 5 different cables. If you are on Windows, try to install drivers in release package. Also try your luck with Zadig. If not working, try on a Linux machine (exclude Ubuntu)
My sound board app can't see the files i putted in, but my fileman app can	folow Soundboard to make correct file
Screen went black when transmit / replay	Check Stealth Mode
Fail / freeze when recording / Can't see files even if I correctly put sdcard content	Make sure your sdcard is FAT32 format, and make sure it's a branded one with acceptable quality
My GPS-Simulation Doesn't work. / My bluetooth doesn't work.	Most modern devices use cellular to verify GPS. Make sure your devicce is vuln to gps-sim. Go to Settings - Radio, and make sure the "Reference Source" says "External". If not, then check the last checkbox and see if it's getting better.
Charging is very slow	Check the following things: - Try at least 5 cables. - Use a good adapter, for example a 5V1A **branded** adapter - Don't use computer or laptop or similar thing to charge.
How to turn on/off	One of these may turn on and another may turn off: - Single press the knob - Double press the knob - Long press the knob - Plug in USB cable - Unplug USB cable
Replay app show empty list	You didn't press correct button. Check wiki
Issues related to sdcard	- use BRANDED sdcard from reliable seller. - Use FAT32 format - correctly put sdcard content which matches your firmware versions
DFU suffix CRC doesn't match / Cannot open DFU device	If you are on Windows, try to install drivers in release package. Also try your luck with Zadig. If not working, try on a Linux machine (exclude Ubuntu)
Screen backlight never turned off automatically even I correctly set the timeout count	Auto set threshold, follow this: https://github.com/portapack-mayhem/mayhem-firmware/wiki/Settings#touchscreen-threshold
Issue that related to dial/knob/encoder	Go to setting, try all the dial sensitivity and rate multiplier
Something else	Check more *Troubleshooting* topics on the sidebar

Won't boot

My device wont start up

White screen

If you device won't boot and leaves you on white screen, then you will need to power off the device and then holding the **UP** button while you power it on. This could take up to 10 seconds.

If this does not work, then try the same thing but this time holding the **DOWN** button (Remembering to wait up to 10 seconds).

What this is doing is loading a different LCD driver to get your devices screen to work.

Once that is done you should be able to reboot normally without any issues.

Black screen

If you device won't boot and leaves you on a black screen, then you will need to power off the device and then hold down the **LEFT** button while you power it on. This could take up to 10 seconds.

Description

- UP key = LCD driver 1
- DOWN key = LCD driver 2
- OK/SELECT key = Reset/Automatic detection
- LEFT key = LCD driver 2 QFP100 chip
- RIGHT key = LCD driver 1 QFP100 chip

If you are having trouble understanding these procedures, here is a step-by-step instruction:

1. power off your device
2. press and holding one of the buttons listed above. （**DO NOT RELEASE IT YET**）
3. power on
4. Wait for at least 10 seconds.
5. if : you see the screen displaying any valid content*, release the button you have chosen.
   else if : you still not seeing any valid content* displayed, choose another button and start again from step 1.
6. power off, wait 5s, power on again **without** holding any buttons listed above, check if it boot successfully.
   if : you see the screen display any valid content* : we are done.
   else if : it boots successfully last round, but fail again this time : check the coin battery.

p.s. ^valid content : either a splash screen or any of the interface

> ⓘNote
> H2+ usually require you to hold the **UP key** on the first boot to configure them.

*This is valid from nightly version **n_220412** and stable release version: **v1.5.1***

H2+ (and H1) not powering up, just black LCD (after flashing new Mayhem FW, and it is ignoring previous above key buttons init description):

If your device was working correctly before updating the firmware, and now you see a black screen after it's been flashed and it is ignoring the keyboard of the above instructions and looks like it's bricked (or also if the Mayhem menus appear but running any app causes an M0 guru fault indicating that the ROM may be partially flashed),

then you have several options to try below depending the situation. Make sure the PortaPack is charged using a separate 5V USB power adapter (not connected to the PC). After charging, connect the USB cable from your PC to the device and follow the steps below:

(1) If your device is still detecting correctly the USB plug to your USB PC

(showing in the front of the HackRF board a green LED when plug in USB cable), then you are lucky; it means that your device is in “hackrf mode”, with good USB communication, **then just follow the below process (I)**

(2) If you have an H1 device (without integrated battery) that does not detect any USB communication

(usually no need to disassemble), try to set up it to DFU mode (by holding in the DFU button while turning on power or attaching the USB cable). In DFU mode, the device will show up as an "NXP LPC" USB device. While in DFU mode, execute the following command:

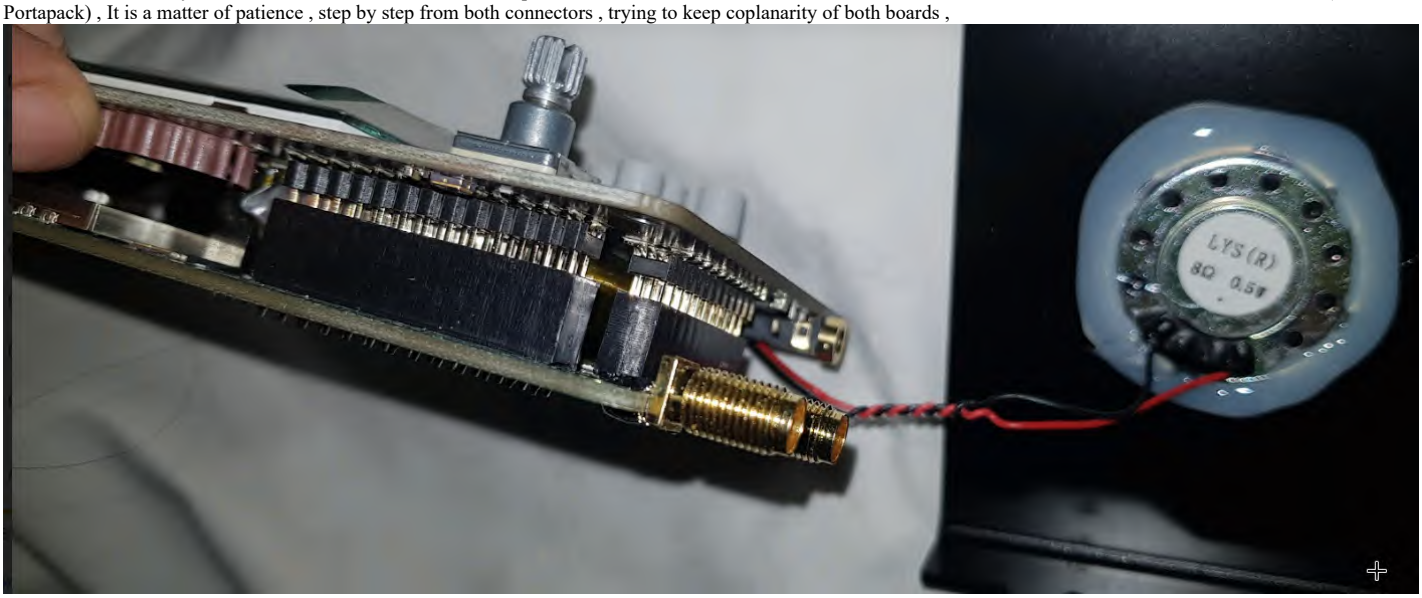
```
dfu-util --device 1fc9:000c --alt 0 --download hackrf_one_usb.dfu
```

(Alternatively, run the `dfu_hackrf_one.bat` file, which performs the command above.)

You will see from that point that the green USB LED from the Hackrf becomes active when the USB cable is connected, and the linux command lsusb should show a "Great Scott Gadgets HackRF One" device. If hackrf mode has been entered successfully, **then just follow the below process (I)**. If not, see more DFU information: Update firmware troubleshooting.

(3) If you have an H2+ (with integrated battery) device that does not detect any USB communication,

first try the steps under (2) above. If that does not work, then disassembling the HackRF from the PortaPack will be necessary to get the device into DFU mode. In that case, Dissassemble carefully both boards from the metal case box. Separate with maximum care to not bend / force so much the PCB's and the LCD Panel , both boards (Hackrf - Portapack) , It is a matter of patience , step by step from both connectors , trying to keep coplanarity of both boards ,



(A) Once disassembled, pick up your hackrf board, and connect it to USB. If it's not bricked, you will have a green LED when plugging USB (indicating HackRF mode is enabled). if it is bricked you will need to enter DFU mode (by holding in the DFU button while turning on power or attaching the USB cable). In DFU mode, the device will show up as an "NXP LPC" USB device. Execute the following command to get the device into HackRF mode:

```
dfu-util --device 1fc9:000c --alt 0 --download hackrf_one_usb.dfu
```

(Alternatively, run the `dfu_hackrf_one.bat` file, which performs the command above.)

You will see from that point that the green USB LED from the Hackrf becomes active when the USB cable is connected, and the linux command lsusb should show a "Great Scott Gadgets HackRF One" device. If hackrf mode has been entered successfully, **then just follow the below process (I)**. If not, see more DFU information: Update firmware troubleshooting.

Special Step process (I) to recover it (usually only needs to be done just once)

Assuming that you are here, with already in correct Hackrf mode (with green LED when connecting USB cable to the USB). If you have already done the steps below in the past, you can skip to just flashing the firmware to the latest version using HackRF mode; see Update firmware.

In case that you have H2+ Portapack with big CPLD QFP100: flash it with special fw jumbo77 1.43 first

In case that you have H1/H2+ Portapack with standard small CPLD QFP64: flash it with official Mayhem fw 1.43 first

If you came from case (3) above, assemble both boards again.

Then , (a) Confirm correct boot up of fw version 1.43 (special jumbo 1.4.3 for big CPLD QFP100, or official 1.4.3 for std CPLD QFP64)

(b) From that 1.43 fw ,with correct boot, put the device in “hackRF mode” and flash it again, but now with latest Mayhem firmware.

(c) At first power up, keep pressing the appropriate button for your unit for more than 2 secs, until getting correct LCD display, and it should work all correctly !

Explanation

Firmware starting at version 1.5.4 and onward contain the Pull Request 662 that uses the persistent memory to test and store the hardware and LCD config settings . That memory uses the same back up voltage than the Real Time Clock calendar, both needs a healthy cell battery button voltage. Sometimes, in a re flashing process , although we got good battery cell button voltage, the unit seems to be badly initializing those persistent bytes and we got strange black screen. Doing those above steps probably reset the persistent memory. That's just a guess.

Additional notes :

I used to have many frequent “black LCD boot brick” when exchanging binaries compiled with different gcc-arm… version , from 9.4 to 10.3 or 12 . But thanks to @u–foka‘s PR fix pmem -> make backup_ram_t data members volatile #1135, all those problems are gone , and now I do not have any persistent memory boot problems , so I do not need to go back to any old version 1.4.3 anymore.

H4 users

If you got any addon plugged in, try to remove it, and power off, wait a bit, and power on your device. If the addon board / module has problems, it can extremely slow down the boot, and the working. (usually happens when the I2C line goes wrong, and each operation have to wait for the timeout)

Config Menu

The config menu is like a mini BIOS that runs before the firmware is loaded. It currently controls two settings.

- **The config menu does not use the LCD screen.** Do not expect any output there. The config menu does only use the reset and DFU button for input and the TX, RX and USB LEDs for output.

Entering the Config Menu

You can enter the config menu by pressing reset twice.

- In case of a crash while the firmware is loading the config menu will activate automatically on next boot.
- Some versions of the PortaPack do not have a working reset button. If the device resets when the usb cable is unplugged this can be used to enter the config menu when it's performed twice quickly enough.

When done correctly the TX, RX and USB LEDs will blink fast (8 times per second). At this point press the DFU button once to show the currently active options.

Available Settings and how to read the blink patterns

- LCD driver (TX LED)
  - Option 1: Automatic detection (TX LED off)
  - Option 2: LCD driver 1 (TX LED on)
  - Option 3: LCD driver 2 (TX LED blinking fast)
  - Option 4: LCD driver 2 QFP100 chip (TX LED blinking slow)
  - Option 5: LCD driver 1 QFP100 chip (TX LED inverse blink slow)

  `The LCD driver can also be set at power on with the up/down/etc buttons. See [Won't boot](Won't-boot)`
- Disable external TCXO (RX LED)
  - Option 1: external TCXO enabled/autodetect (RX LED off)
  - Option 2: external TCXO disabled (RX LED on)

  `The "Disable external TCXO" option can also be set in Settings > Radio`

Switching between modes

Press the DFU button to switch to the next option. 10 presses will return you to the original active option.

- **Don't press the DFU button too fast. Hold it down for at least 200ms or it might be ignored.**
- Once a new option is active it is immediately saved. The device can be restarted and the new selected option will be active.

Unwanted Config Menu activation

In some cases a PortaPack may start up intermittently in Config Menu mode, such as when the power button is pressed twice rapidly, or if a little electrical noise occurs when a USB cable is attached. If this occurs frequently (dark screen and blinking LEDs), the Config Menu code can be disabled using the Settings -> Config Mode app (which sets a flag in persistent memory to disable the Config Menu completely).

Firmware upgrade

One of the main sources of problems while updating the firmware is the quality of the USB cable. Try with several ones just to be sure before trying any other solution.

Black or white screen?

If you get a black or white screen after updating, please check the wiki here: Won't boot

An application is not starting anymore?

Maybe an update in the application settings broke the settings file for the app. Just go in the SETTINGS folder at the root of the SD card and delete the related settings file. As an example lets take the audio app: if we follow the previously mentioned method, then we just go and delete the rx_audio.ini file in SETTINGS directory. This will force a new settings file to be generated with all new needed parameters at the next attempt to launch the app.

If an app is missing entirely, or greyed out, make sure that apps are placed in the APPS folder of the SD card and that their version matches that of the firmware. Many apps have been moved from flash ROM to the SD card to make room for new apps.

Update failed on Ubuntu/Mint/Ubuntu based distro?

For Ubuntu and Mint user: Ubuntu based distro never maintains their repo for hackrf package. You'll face a lot of weird problems if your hackrf is R9.
To resolve these, please compile hackrf package yourself, or use other distro.

DFU

This is a special mode to update the firmware in case of problems. To enable this, you should reset your device holding the RESET and DFU buttons at the same time, while doing this, release RESET, and then release DFU. The leds should be ON and the screen wont show anything.

> Sometimes it's tricky to entering DFU mode, here are some ways to entering it if you have no luck with the method above:
> W1. Press and holding DFU button, then plug the USB cable, then release the DFU button.
> W2. Press and holding DFU button, then single press the knob, then release the DFU button, then plug the USB cable.
> W3. Plug in USB. Press and hold DFU button and unplug USB. Release DFU button and plug USB back in.

Windows

If you are in Windows, from the release package double click `dfu_hackrf_one.bat` and follow the instructions. Do not disconnect or reset your PortaPack after that procedure, continue in the step 3 of the normal procedure.

MacOS

DFU Utils CLI tools for MacOS available through MacPorts or Homebrew

1. If necessary, install the DFU tools: `brew install dfu-util`
2. Connect the device via USB
3. Switch to DFU mode as per the section above: *DFU*
4. Upload the firmware with `dfu-util --device 1fc9:000c --download hackrf_one_usb.dfu --reset`
5. Reboot the device

Linux

DFU Utils CLI tools for Linux available in standard repositories

1. If necessary, install the DFU tools (example for Debian/Ubuntu variants): `sudo apt install dfu-util`
2. Connect the device via USB
3. Switch to DFU mode as per the section above: *DFU*
4. Upload the firmware with `dfu-util --device 1fc9:000c --download hackrf_one_usb.dfu --reset`
5. Reboot the device

Alternative environment

You may be able to try in a virtual environment, completely isolated from your current OS:

1. Download http://eu2-dist.gnuradio.org/ and burn the ISO and boot from it, select the LIVE Image
2. Once in the environment, Open a Command Prompt and type: `sudo apt-get install dfu-util`
3. Connect your device to your computer
4. Press RESET and DFU buttons at the same time, and while doing this, release RESET, and then release DFU
5. Open a terminal and type `dfu-util --device 1fc9:000c --download hackrf_one_usb.dfu --reset`
6. After that, without disconnecting it, you can upload the firmware with `hackrf_spiflash -w new_firmware_file.bin`

Notes

If you have an existing HackRF One and you've acquired a Portapack separately (from third party suppliers), do the following:

1. Make sure you flash the HackRF One first before attempting anything with the HackRF One + Portapack combo. The code to run Portpack comes from the HackRF One firmware as flashed.
2. If you don't flash the HackRF One and just plugged in the Portapack and powered up the setup, the screen on the Portapack will flash and nothing else will be seen. This does not mean that the Portapack is faulty.
3. After flashing the HackRF One, you can plug in the Portapack and when the setup is powered up. you will see the screen show the UI for the version of the firmware that was flashed into the HackRF One.

Video

The following video explains all possible outcomes while trying to update the firmware and possible mitigations: https://www.youtube.com/watch?v=_zx4ZvurgOs
There is another very good video about the general overview, also including the update procedure: https://www.youtube.com/watch?v=kjFB58Y1TAo

Still stuck?

If you still experience problems after reading this and checking the video, submit an issue.
Also, there is a lot more details on the HackRF wiki.

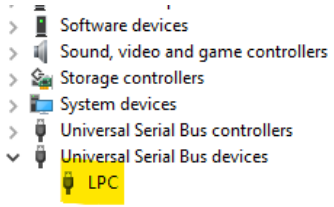
Diagnose firmware update in Windows

If you cant get firmware to update/install on your device do these steps.
Try boot into DFU mode by:

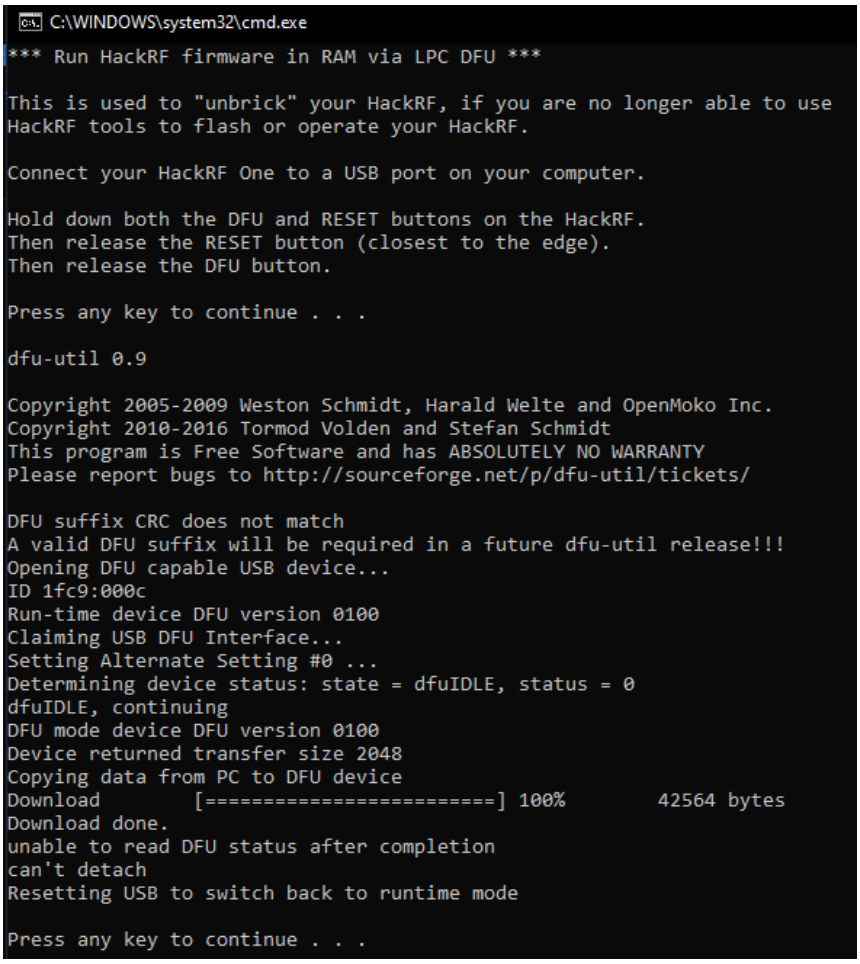
1. Plug device into computer
2. Press and HOLD the DFU button, While still holding the DFU button, press and release the reset button (WHILE STILL HOLDING THE DFU BUTTON).

   Note : in some particular H2 (ex H2R4 with battery), reset button does not make a proper reset , it just freeze the screen , and do not allow you to enter in DFU . In that case, unplug it from the computer, switch off the unit with two short pushes to the big encoder knob button (power off). And then keep pressing DFU button , a short push button to the encoder knob button (power on) leads you into a proper DFU Mode. And now you can plug it through USB cable to the computer, and continue with process.

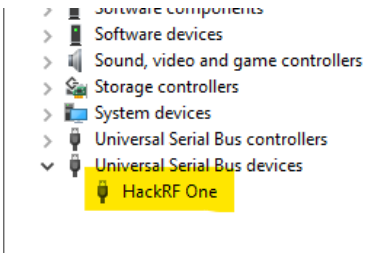
3. Check Windows device manager and see if you have LPC showing up



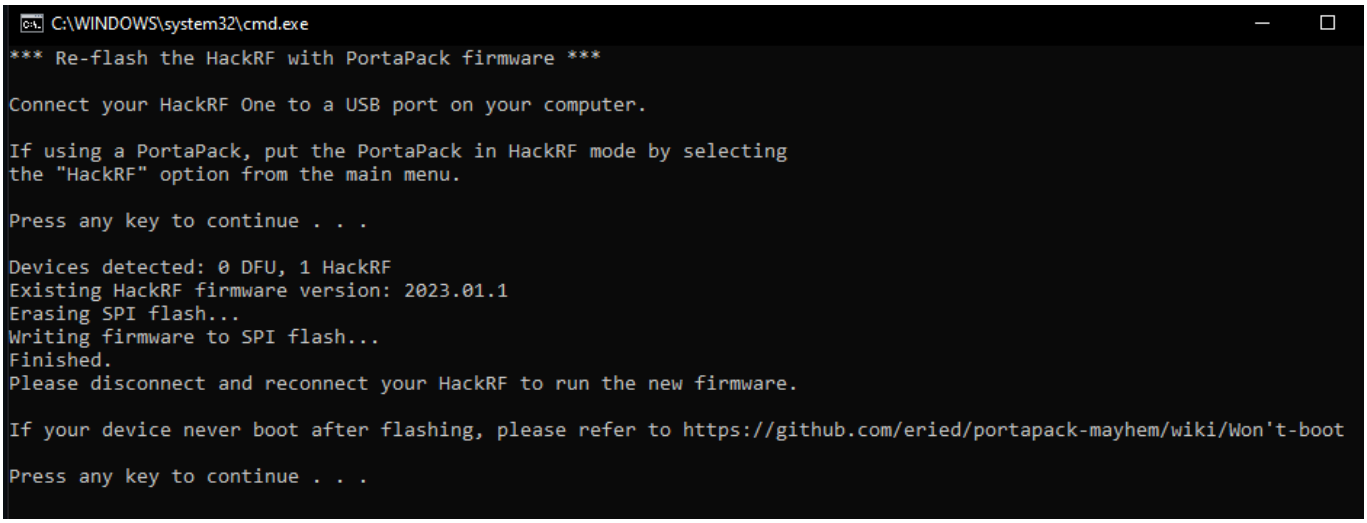
4. If it shows up then make sure you download the latest version of **mayhem_vx.x.x_FIRMWARE.zip** from GitHub here https://github.com/portapack-mayhem/mayhem-firmware/releases/latest. You can then run "dfu_hackrf_one.bat". Now double check the file name as they look quite similar.
5. Once it opens, press enter on your keyboard and you should see the following:



6. Once that is done, you need to check device manager and see if you can now see a new device showing up



7. If this device is showing up, then you can now run "flash_portapack_mayhem.bat" and press enter. You should now see the following:



8. Once that is done, you should be able to press the reset button and your device will boot up. If not, then please refer to the wiki here: [Won't boot] (https://github.com/portapack-mayhem/mayhem-firmware/wiki/Won't-boot

Unknown device

If you see **Unknown device** then you will need to install your device drivers.

1. Download Zadig for USB driver installation

Go to the Zadig website and download the latest version of Zadig. Zadig is a tool that allows you to install the necessary drivers for USB devices like the HackRF.

2. Connect your HackRF device

Plug in your HackRF device into a USB port on your computer.

3. Run Zadig

Open Zadig as an administrator (right-click and choose "Run as administrator"). In Zadig, go to Options > List All Devices.

4. Select the HackRF device

From the dropdown list, select HackRF One or HackRF. If you can't find it, look for USB devices and match the HackRF device by its USB ID (usually it’s something like 1d50:6089).

5. Install WinUSB driver

Once you have selected the HackRF device, set the driver to WinUSB (this is usually the default driver). Click Install Driver or Replace Driver if there is already a driver installed. Wait for the installation to complete.

6. Verify Installation

After the driver installation, you can confirm that the HackRF device is working by using tools like SDR# (SDRSharp) or GNU Radio. Download SDR# from AirSpy to test your HackRF and ensure it's detected properly.

7. Install HackRF Tools (Optional)

If you want to use the HackRF command-line utilities, you can download the official HackRF tools from the Great Scott Gadgets GitHub. Extract the tools and add the folder to your system's PATH to use the commands like hackrf_info, hackrf_transfer, etc. After following these steps, your HackRF device should be ready to use on Windows 11.

Receive Quality Issues

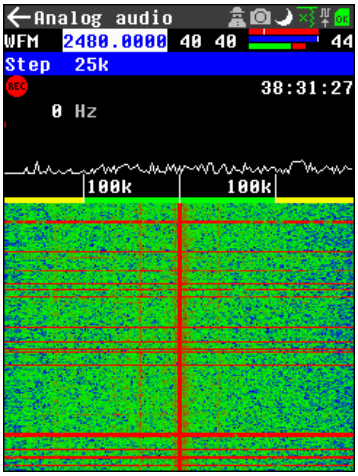
Not able to receive any signal/Noisy waterfall

Antennas

Are you using the correct antenna? Is it plugged in correctly? this sounds silly, but It could be as simple as that

Gain settings

The gain settings are always arranged the same, VGA gain on the right and LNA on the left (both with value "40" in the image below).



Description of the gain settings

The VGA or **V**ariable **G**ain **A**mplifier can be set to any number between 0-62. It amplifies pretty much everything and is basically a fine-tuning adjustment, I find it works best between 8-16.

The LNA, or **L**ow **N**oise **A**mplifier, can only be set to six settings: 0, 8, 16, 24, 32, 40. the LNA will try it's best to increase the signal-to-noise ratio. 24 or 32 work pretty well most of the time.

TX amp

The TX amplifier *can* be used to help increase receive quality, but it is delicate and discouraged most of the time.

Nearby Transmitters

Nearby, High-Powered transmitters, such as FM stations and trunking stations, can overload your HackRF and create a lot of noise (think of it like clipping in audio). You could consider getting a band block/pass filter to block out common overloading sources like FM stations, rtl-sdr.com sells a nice 88-108 block filter for FM.

Local Noise Sources

There are many devices that can cause wideband noise: Screens, USB hubs, poorly designed cables, power supplies, faulty wiring, etc.. You can go around unplugging things or flipping breakers to figure out what might be the source of noise. Simply walking outside might help as well.

Power Banks

Many power banks can be a local noise source, try different power banks if you can.

H2 Internal Battery Charger

A few people have reported that the internal battery charger on some H2 models can cause noise when plugged in. There isn't really a fix for this unless you want to go about putting another charger. Please report as an issue if you find this issue, with detailed photos of the PCB of your H2. Check the following video to see how a normal functioning H2 does not produce extra noise related to the battery charger.

Broken RF Chain

It may be entirely possible that something in the RF front end is broken, commonly the TX amp. The best way to go about troubleshooting this is to open up an issue on the HackRF Github explaining the issue, they'll try their best to guide you through it, and if you have a genuine GSG HackRF you might be able to get it replaced.

Intermittent Signal Loss/Noise

Loose Cable Connections

As stated before, check you cable connections and antenna. Wiggle things around and see if any dramatic change is reflected in the waterfall.

Nearby Transmitters

Nearby transmitter can also cause intermittent signal loss, the culprit is almost always pager traffic as those signals can be very strong and transmit intermittently. A nearby trunking repeater could also be to blame.

H2 Internal Battery Charger

The H2 Internal Battery Charger can also intermittently cause noise when plugged in. Check this.

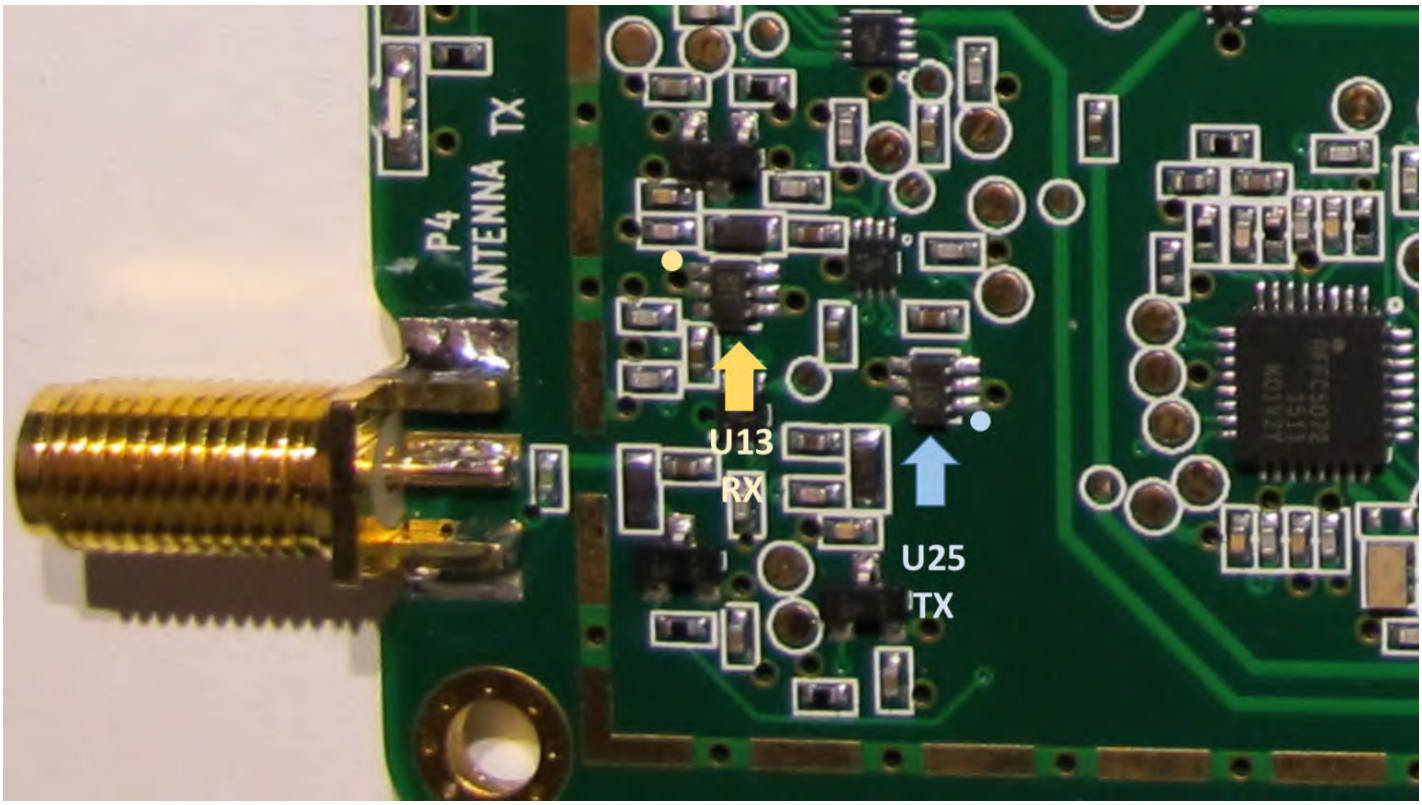
Local Noise Sources

There are many devices that can cause intermittent wideband noise: Screens, USB hubs, poorly designed cables, power supplies, faulty wiring, etc.. You can go around unplugging things or flipping breakers to figure out what might be the source of noise. Simply walking outside might help as well.

No TX/RX

The MGA-81563 can be damaged easily, but you can buy (relatively cheap: https://s.click.aliexpress.com/e/_Dl4U7YI) and replace them yourself. For more information about this procedure, please check https://www.onesdr.com/2020/04/09/how-to-fix-a-broken-hackrf/

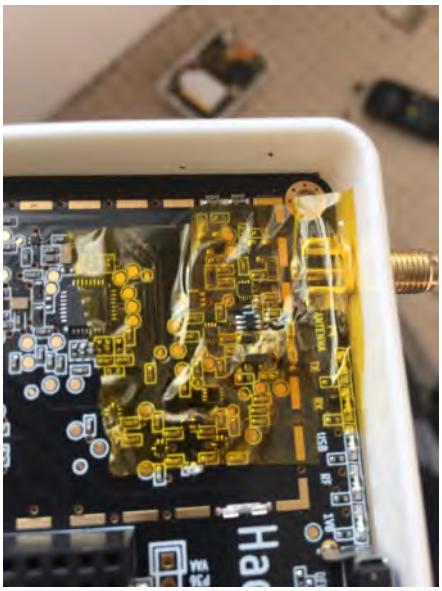
The previous link has a very good reference picture:



RX problems

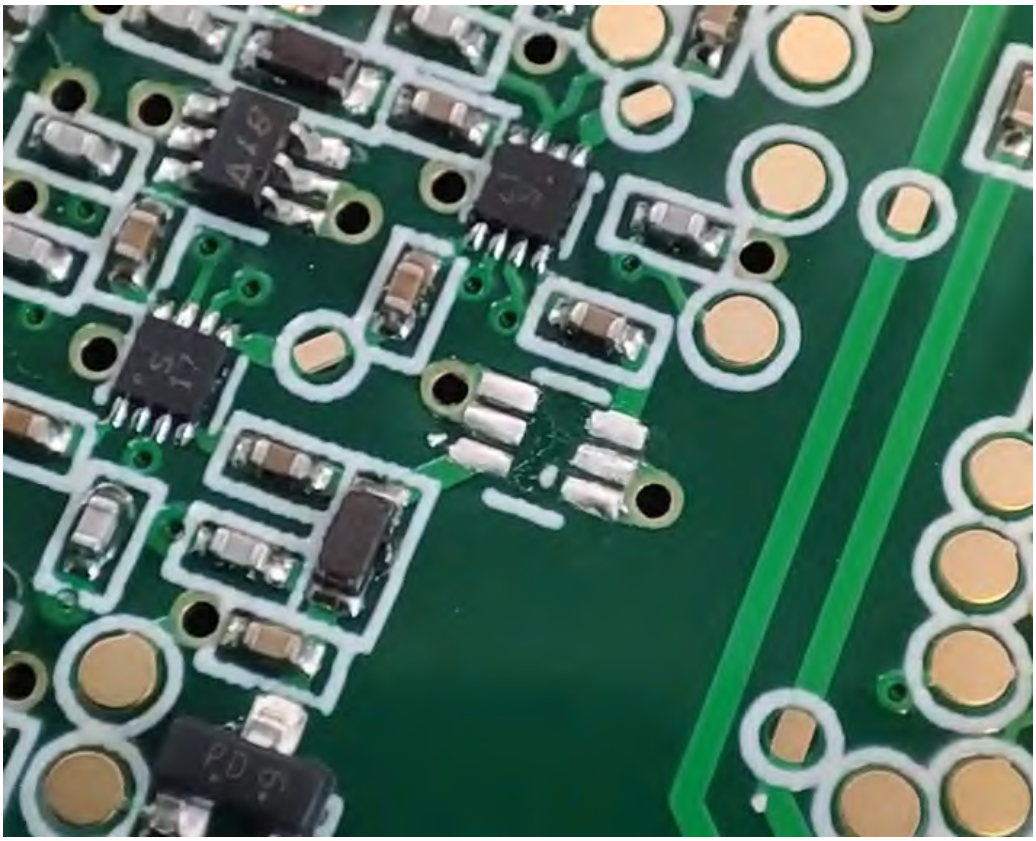
If you find on a strong signal such as an broadcast FM station that you select Amp as "0" and you get a signal and then select Amp "1" and you do not then this is a good sign that the RF Preamplifier u13 (MGA-81563) is damaged. This can happen if you use a stronger transmitter near to your HackRF.

It is possible to replace the damaged IC with simple tools (soldering iron, solder wick). First solder flood the damaged component to remove it, preferably protecting the surrounding. Clean the pads and replace the component:

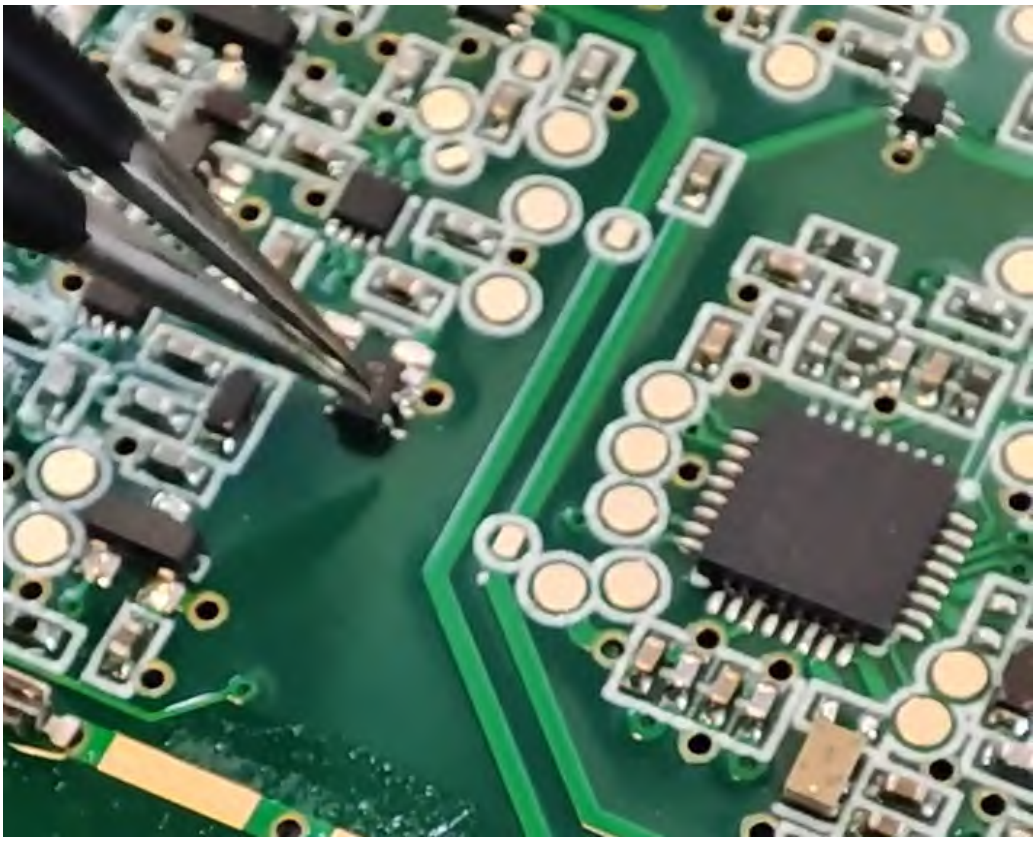


TX problems

The same component is used for TX, which also can be damaged. Below is an example of the replacement procedure. First remove and clean the pads. This can be done with hot air or normal soldering iron:



For the orientation, you could use the text of the chip itself. It should be "up", pointing to the antenna jack of the HackRF:



TX Carrier Only

If your portapack is only transmitting a carrier wave, then this could be an indication of an outdated CPLD image. See Updating the Xilinx CPLD on hackrf board for how to update the CPLD.

H2+ speaker modifications

Amplifier volume gain

The H2+ Version R2, R3 and R4 uses an WM8731 Codec and supports a speaker using a dedicated Audio Amplifier INS8002e. This is a 3-watt amplifier and should give a high volume.

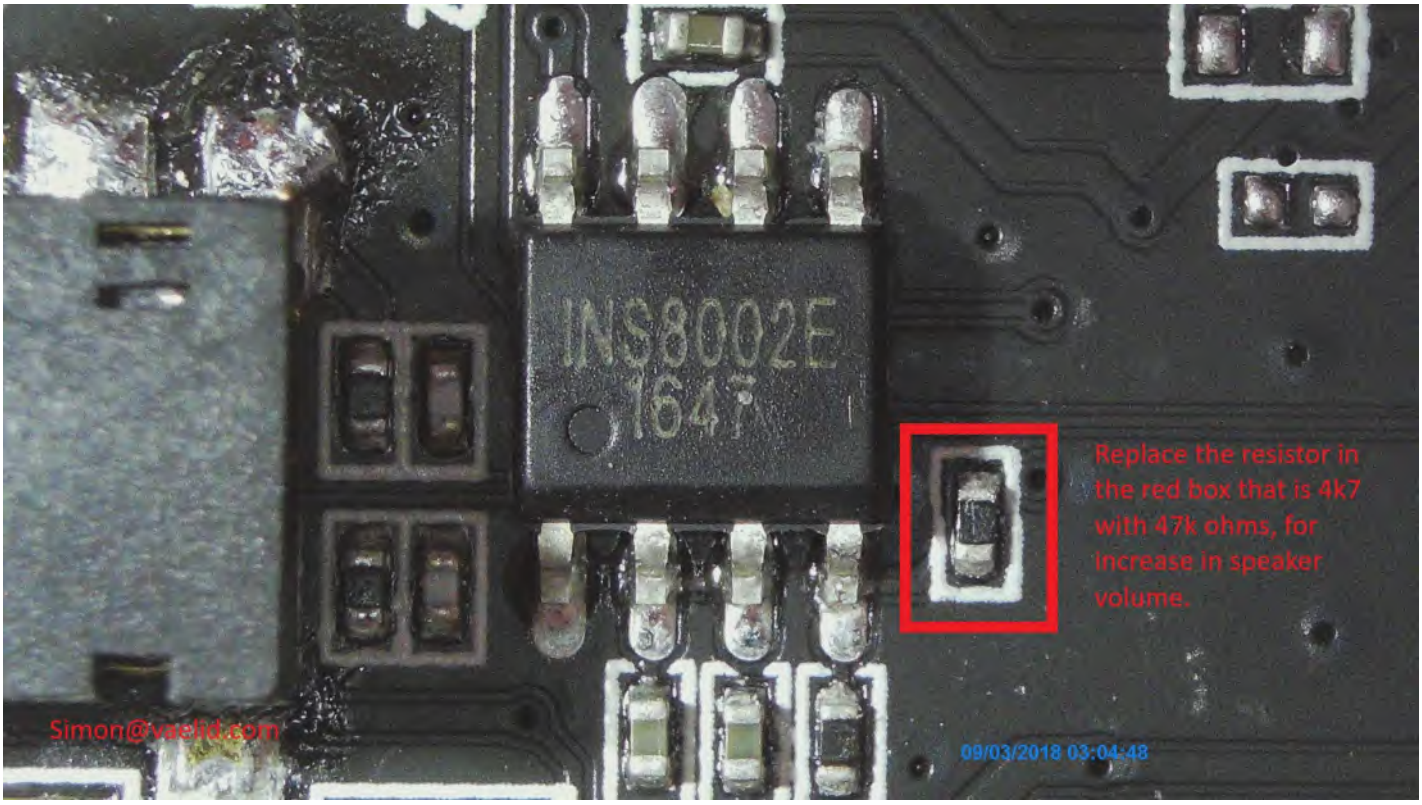
The issue is that when the volume is at 50 (Default) it gives a good safe volume level in the headphones, but the speaker audio is unable to be heard unless you turn up the volume to 80+ on the volume setting and even then, the audio is low.

Having traced the circuit on the PCB, and studied the chip specifications for the WM8731 and INS8002e, there is an error in the selected component, for the INS8002 gain setting of what is a Power Op-Amp.

The power audio amp input is taken from “Right Channel” headphone connection on the speaker side of the of the headphone socket switch and is connected to the audio amp via a capacitor and 4k7 resistor. The feedback resistor from the output to the input is also 4k7 resistor. This sets the gain for the audio amp at 1. This is totally inadequate.

In tests the feedback resistor can be changed to 47K. This gives a gain of 10 and provided a reasonable safe audio speaker level when the speaker is selected at the default value.

The replacement of the resistor is not easy, and then you need the skills and tools to remove and replace it. The current resistor is SMD 0402 being just 1.0mm long and 0.5mm wide, The indicated resistor should be remove with soldering iron solder pads cleaned and fluxed, and the new resistor added. A larger SMD could be used if soldered to one pad and small wire connected from the other pad to the other end of the SMD.



Silencing internal speaker when using audio jack

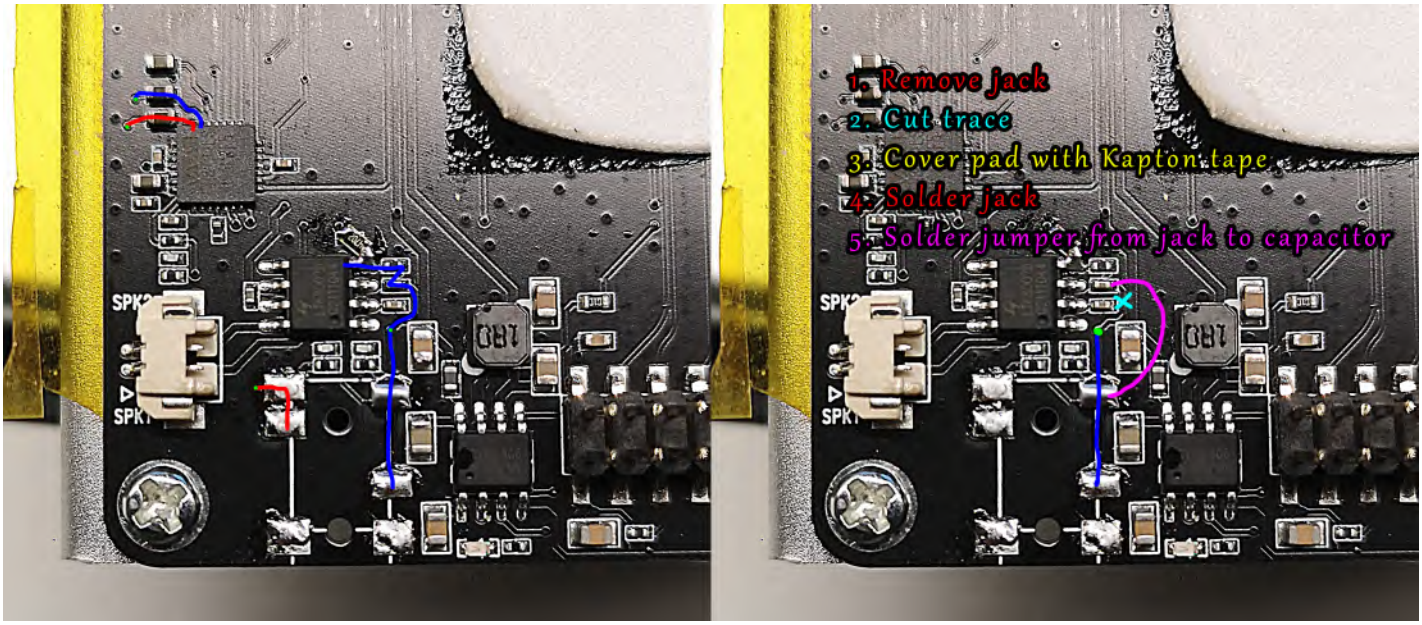
In the H2+ R4 version the headphone jack switch is disabled. When a pair of headphones are plugged in the internal speaker is not disconnected.

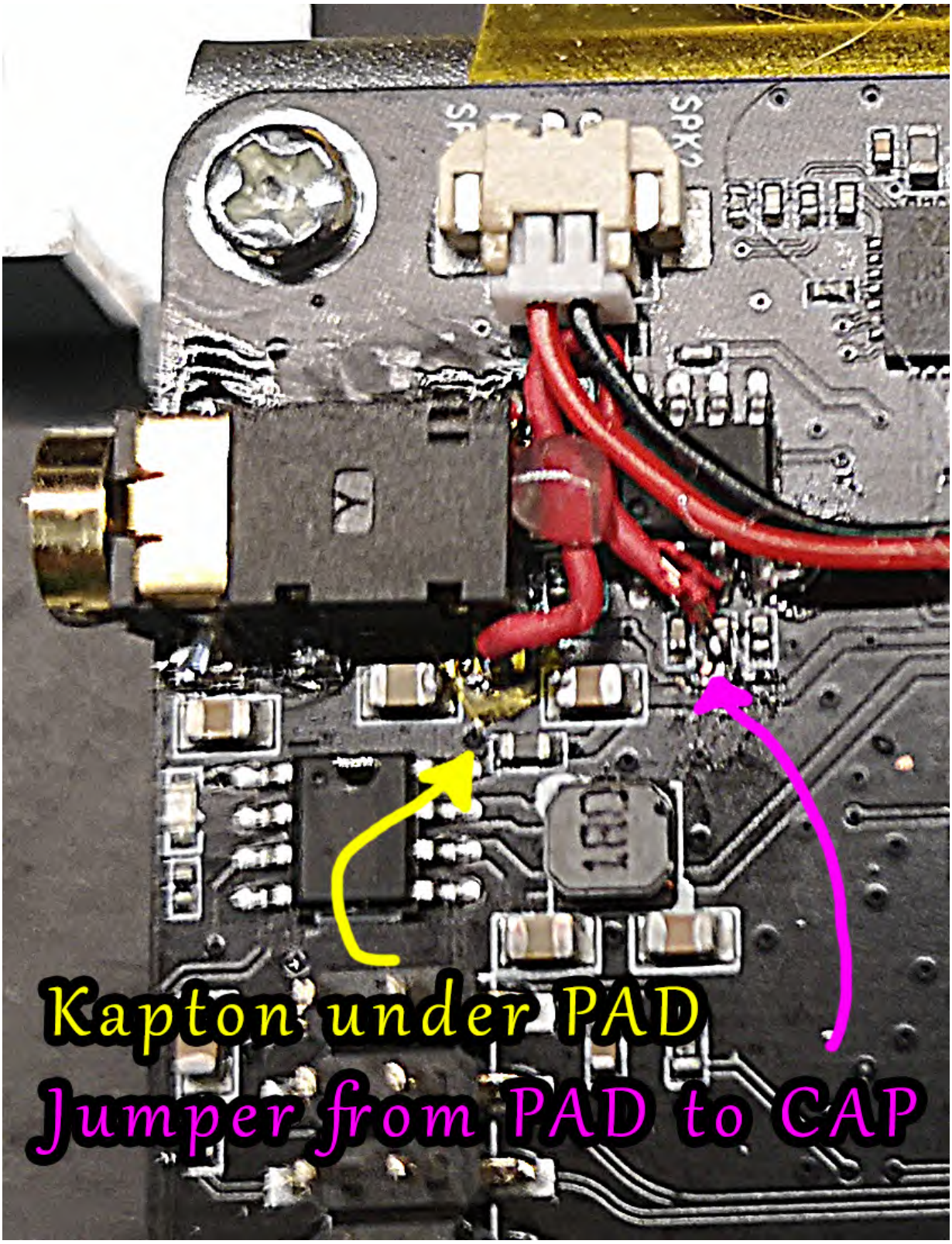
A simple but delicate modification can enable the headphone switch functionality by placing some Kapton tape over the PCB PAD and soldering a small wire from the headphone jack connector to the capacitor into the speaker amplifier.

After the modification when a pair of headphones is plugged in the internal speaker is silenced.

In the first image red traces are for the left channel and blue for the right channel.

1. Remove the headphone jack and clean the pads.
2. Cut the blue trace between the PCB VIA (green dot) and capacitor to the amplifier. Be careful of the other traces.
3. Place a small piece of Kapton tape over the the PAD (top right in the photos).
4. Solder the headphone jack back in place.
5. Solder a short wire from the headphone jack pin to the capacitor (glue the wire to the PCB to avoid it damaging the pin or capacitor).



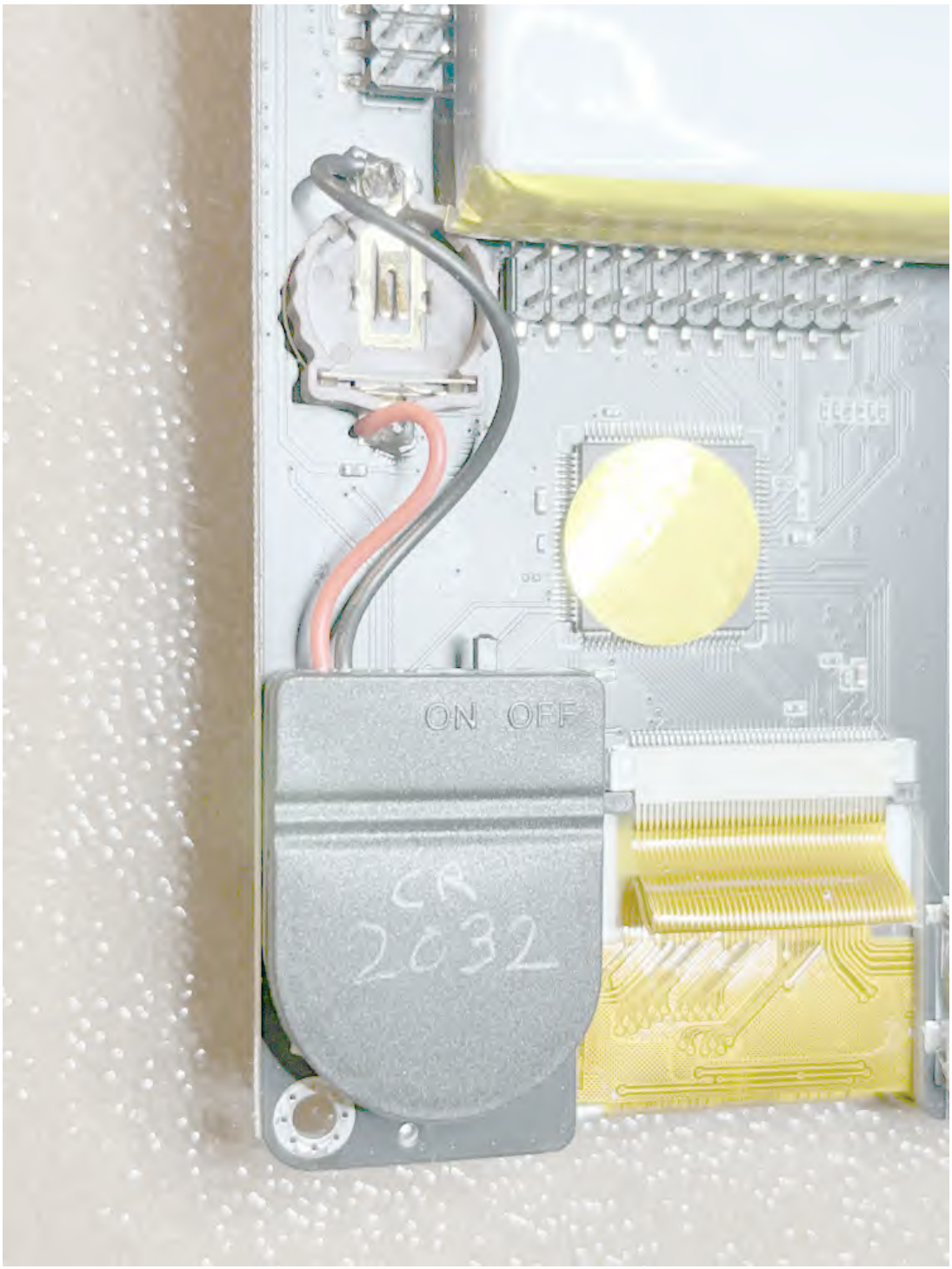


Dead Coin Cell Battery

The coin cell battery is used to preserve settings stored in persistent memory (P.Mem), as well as to power the RTC clock. The smaller coin cell battery used on the PortaPack H2 does not last long and replacing the coin cell can be a chore, depending on the case style.

To partially work around a dead or missing coin cell battery, persistent memory settings can be configured to save settings to the SD card (see Settings -> P.Memory Mgmt). This allows all settings to be preserved, but does not resolve the issue with not keeping time.

Those with an H2 model and soldering skills might want to consider adding a larger CR2032 battery holder such as the one below (attached with double-stick foam tape), to lengthen the time that the coin battery lasts by about 6X:



Factory Defaults

Why a reset to factory defaults

Sometimes with an update some settings management is changed and render the actual settings set in various place not working correctly or clearly killing some apps.
To resolve this you can try to reset these settings. For that, you'll have to clear the persistent settings and clean some directories on your SDCARD.

Guide

The best way to achieve the reset is to take out the SDCARD and do the cleanings on it on computer.
Boot the unit without the SDCARD (you may need to press your boot key), get into the 'Settings' / 'P.Memory Mgmt' menu and clean the persistent memory using the button.
Shutdown.
While you're at it update the SDCARD content to latest if not done.
Put back the SDCARD.
Boot (may need boot key).
You can now use your device like if it was installed first.

SDCARD

'SETTINGS' directory

Delete all the files under 'SETTINGS' to reset "App Load and Save" settings as well as the configuration of the "P.Mem" menu. (note: this does not reset the persistent memory itself).

'hardware' directory

NOTE FIRST: this reset the saved boot config key. In case you think it's not booting because of a bad saved detection, delete the file under that directory.

PERSISTENT MEMORY

Get into 'Settings' , 'P.Memory Mgmt' and click on the '! reset p.mem, load defaults !'. This resets all configuration settings that are stored in persistent memory. Note that persistent memory settings are sometimes reset automatically following a firmware upgrade or downgrade, specifically if there is a firmware change that affects the persistent memory data format, or if the coin cell battery is discharged. For a complete list of settings stored in persistent memory, the "Debug Dump" app can be used to create a file listing all persistent memory settings.

In case the p.mem contents somehow block the startup (the screen stays black and the RX led blinks rapidly that typically happen after flashing a different build) the p.mem can be ignored during startup by holding down the left and right buttons while starting up the device.

DFU overlay

While Mayhem firmware is running, a short press of the DFU button will cause an overlay to be displayed with information about the two CPUs and memory. A second press of the DFU button will display Receiver settings. A third press will hide the overlay.

Full reset

Steps

1. Backup your importance files in your sdcard to a computer or somewhere safe.
2. Download the latest Nightly release from GitHub.
3. Take out your sdcard, take out your coin battery (button battery) and put them in somewhere safe and make sure they don't touch each other.
4. Following one of these ways to enter DFU mode (You may need to try one or more for success):
    - holding the RESET and DFU buttons at the same time, while doing this, release RESET, and then release DFU. The LEDs should be ON, and the screen won't show anything.
    - Press and holding DFU button, then plug the USB cable, then release the DFU button.
    - Press and holding DFU button, then single press the knob, then release the DFU button, then plug the USB cable.
    - Plug in USB. Press and hold DFU button and unplug USB. Release DFU button and plug USB back in.
5. Flash the hackrf firmware with DFU tool:
    - windows: From the release package you downloaded in step 2, double click `dfu_hackrf_one.bat` and follow the instructions. Do not disconnect or reset your PortaPack after that procedure.
    - Linux/ macOS:
        1. Use your package manager to install `dfu-util`package, the command could be `sudo apt install dfu-util` or `brew install dfu-util` or `pacman -Sy dfu-util` or others depnding on your distro.
        2. Unarchive the release package you downloaded in step 2, open a terminal, `cd` into the dir you unarchived, input `dfu-util --device 1fc9:000c --download hackrf_one_usb.dfu --reset` and check if it succeed.
        3. Do not disconnect or reset your PortaPack after that procedure.
6. Note that at this point, you had never unplugged or reboot your PortaPack. Now flash latest Mayhem firmware (which is different thing from the one we did above):
    - windows: From the release package you downloaded in step 2, double click `flash_portapack_mayhem.bat` and follow the instructions.
    - Linux/ macOS:
        1. Use your package manager to install `hackrf`package, the command could be `sudo apt install hackrf` or `brew install hackrf` or `pacman -Sy hackrf` or others depending on your distro.
        2. Unarchive the latest firmware package you downloaded.
        3. `cd`to the dir which you unarchived the firmware package.
        4. Excute `hackrf_spiflash -w ./firmware/portapack-h1_h2-mayhem.bin`
7. Download the latest Nightly SDCARD contents from GitHub.
8. Unarchive the latest Nightly SDCARD contents you downloaded.
9. Format your sdcard to FAT32 format.
10. Put everything you unarchived in step 8 into your sdcard, but don't insert your sdcard yet.
11. Try Won't Boot steps if needed.
12. If everything goes well, you can power off, wait at least 1 minute, insert your sdcard, and then put the coin batter back into portapack.
13. Power on, go into `Settings` -> `P .Memory Mgmt` -> `Reset P.Mem to defaults` -> `YES`, Then Power off, wait at least 1 minute.
14. Try Won't Boot steps again if needed (because without both sdcard and coin battery, the boot config won't be saved).
15. Boot the device, finished.

Notes

- If your device cannot be recognized no matter whatever you do:
    - Try on a Linux machine.
    - Try at least 5 different cables.
- If you are a Ubuntu or Ubuntu based user:
    - Ubuntu doesn't update their `hackrf`packages in their stable repo (till 2024.Jan.02, they're still keeping 2021 version), so you might have a bunch of issues. Just don't use Ubuntu or Ubuntu based distro, or if you have to, compile the hackrf host software (not firmware) yourself.
- You can try to update the Xilinx cpld on Hackrf, following this: https://github.com/portapack-mayhem/mayhem-firmware/wiki/Updating-the-Xilinx-CPLD-on-hackrf-board
- Submit a GitHub issue if the problem you are trying to resolve still exist.

Applications

Categories

There are separate categories for the applications

- Receive
- Transmit
- Capture
- Replay

- Search
- Scanner
- Microphone
- Looking Glass
- Tools
- Options
- Debug
- HackRF

Colors

For each application there is a color associated with the application

- Green - mostly fully implemented.
- Yellow - Working with some features missing.
- Orange - Beta/in development, most likely not working.
- Red - Destructive Utility. (i.e. Wipe SD Card)

External Apps

External Apps (.ppma files) are placed in the APPS folder on the SD Card, and their versions must match the currently-running firmware. Mayhem developers may move some lesser-used and incomplete apps from internal to external to make room in the firmware flash ROM for new applications.

Receivers

The following is based on extracts from HackRF Documentation that can be found here.

What is the minimum signal power level that can be detected by HackRF?

This isn't a question that can be easily answered for a general purpose SDR platform such as HackRF. Any answer would be very specific to a particular application, and is determined by many factors including:

- **Modulation:** The Modulation Depth and type used (M)
- **Frequency:** That is used (F).
- **Software:** that is designed (S).
- **Configuration:** of the App (C).
- **Bit error rate:** The % error experienced (E).

Changing any of those variables (M, F, S, C, or E) would change the answer to the question. Even a seemingly minor software update might result in a significantly different answer. To learn the exact answer for a specific application, you would have to measure it yourself. The Receivers Apps have a variable sensitivity to radio signals, and it should be considered that The HackRF has a much weaker performance compared to an optimised radio system designed to operate at set frequencies. In addition, it will be open to interference and spurious signals as it does not have any RF filtering. This would need to be provided by the addition of External filters. There are many relatively cheap ones available to purchase with good performance.

These specifications can be used to roughly determine the suitability of HackRF for a given application. Testing is required to finely measure performance in an application. Performance can typically be enhanced significantly by selecting an appropriate antenna, external amplifier, and/or external filter for the application.

What is the Receive Power of HackRF?

The maximum RX power of HackRF One is -5 dBm. Exceeding -5 dBm can result in permanent damage! This is often seen, see notes on Preamplifier IC replacement.

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.

AFSK

This App Does not work.While it is marked as beta the Receiver has a constant stream of random characters regardless of the frequency or Modem Setting. In the code it referes to the Settings used for LCR. This app need detailled study to determine why the relative simple App that has components in many other Apps does not work.

AIS Boats

AIS

Automatic Identification System (AIS) is a tracking system used by water-going vessels. It is described in ITU Recommendation M.1371..

The PortaPack AIS receiver decodes information coming from vessels and base stations, on one of two selectable VHF frequencies, 161.975 MHz (channel 87B) or 162.025 MHz (channel 88B). Others frequencies can be added to the SD Card Under AIS.

The Key Items on the App that can be selected with the cursor and changed with the encoder knob are:

- **Title bar:** The usual Items may be changed and displayed.
- **Ch:** The selection of the channel number, eitehr 87B or 88B.
- **Gain:** Setting are shown in order of Amp 0=0db or 1=14dB, LNA(IF) (0-40) and VGA (Baseband Gain) (0-62).

The App page shows two columns of received data, the Maritime Mobile Service Identity and the vessel name or call sign, if it was received. By selecting the received data line this opens a detailed view, giving the most recent details received from the vessel. It should be noted that dependant on the activity of the vessel that the information will be sent every few minutes to every few seconds if traveling at speed.

Analog TV

The analog TV receiver app currently supports wideband amplitude-modulated PAL only. This signal used to be widely adopted for television broadcasts. The picture is assumed to be 625-line x 768-width interlaced but app reduces the image size to 52-line x 128-width to reduce processing overhead and to fit on the PortaPack screen. The resulting 52x128 image is then stretched to 104-line x 128-width for improved proportions, and multiple frames are displayed on top of one another in lieu of de-interlacing (i.e. the first image may be just the odd lines, the second may be the even lines, and repeat).

The app does not yet support sync signals detection, so frames may be misaligned both horizontally and vertically and will tend to drift over time. The picture can temporarily be aligned left/right by moving focus down to the screen area and turning the encoder dial to adjust the offset.

The app only shows black and white images (color images are received but are displayed in black and white).

It is important to manually adjust the amplification settings for improved picture contrast, since this is an amplitude-modulated signal and an automatic gain control is not yet implemented in software.

This app does not yet support NTSC, or SSTV.

References:

https://www.youtube.com/watch?v=VxBReLPbfZc
https://blog.csdn.net/shukebeta008/article/details/104741355

APRS

Automatic Packet Reporting System

- Display streams of informations using APRS protocol
- The information displayed is the received streams and a list of the "Source" "Location" "Hits" and "Time".
- The coloured bars display the received signal strength (Red), baseband signal strength (Blue).

Pre-configured "Regions" (geographic area)

- North America (NA)
- Europe/Uk (EUR)
- Australia (AUS)
- New Zealand (NZ)
- ISS (International Space Station)
- MAN (Manual) if the frequency is manually changed

Controls

Frequency input, if not using Pre-Configured setting.

- Use rotary encoder over frequency field to move it by steps of 100 Hz
- Press middle button over frequency field to manually enter a frequency using keypad

Radio settings

From left to right:

- AMP , "0" or "1"
- LNA
- VGA

Volume

- audio volume level is placed after the colored signal strength bars. When focus is over it, use rotary encoder

Audio

The Audio App is the main way that signals can be heard and seen in detail. Three types of decoders are provided for audio modulated signals and a spectrum view of the signals. The user interface has the ability to view and change:

- **SPEC:** Display a Spectrum of the received signal and allow viewing of 10MHz of RF Spectrum, centered on a configurable frequency, with 5MHz above the frequency and 5MHz below.
- **AM:** Demodulate and Record RF Signals modulated using the Amplitude Modulation scheme. It can demodulate Double-Sideband AM (ITU Designation: A3E) and both Lower-Sideband and Upper-Sideband Single-Sideband AM (ITU Classification: R2E, H3E, J3E) signals.
- **NFM:** The Narrow Band Frequency Modulation decoding ITU Classification: FM3
- **WFM:** The Wide FM Receiver is a Sub-Application of the Audio Receiver Application. Its purpose is to Demodulate and Record RF Signals modulated using the Frequency Modulation scheme. It can demodulate mono and stereo Wide FM signals of 200KHz bandwidth. Such signals are commonly used for VHF FM Broadcast services.

The Key Items on the App that can be seen or selected with the cursor and changed with the encoder knob are:

- **Title bar:** The usual Items may be changed and displayed.
- **Mode:** On the line below title bar is the demodulation mode AM, NFM, WFM, SPEC. When either of these are selected it will bring up a secondary set of relevant items on the line below. These are discussed in secondary items below.
- **Frequency:** The Centre frequency of the demodulation band.

    Note 1 : From Frequency field, you can move down to the below Step field , to adjust your best suitable Freq-step, according to your needs.

    Note 2 : If you have load/save App Settings from SD card enabled, it will continue to use what it was last set at. And you can always edit the file in the SD card, /SETTINGS/rx_audio .ini and edit the step size there, according to your needs in that App.

Note 3 : Additionally , to be more user friendly , from version 1.7.4+ holding in the Select button on the Frequency field for a second until a digit turns blue, then you can use Left/Right select which digit you'd like to adjust, and then you can use the Encoder Dial to adjust any digit up/down by 1 to tune more precisely. (Press Select again to exit this tuning mode.

- **Gain:** Settings are shown in order of LNA(IF) (0-40) and VGA (Baseband Gain) (0-62). When either of these are selected in the secondary line the AMP setting is shown and can be as either set to 0=0db or 1=14dB.
- **Signal Display:** The three coloured displays are top to bottom RSSI(Red/Blue) with an average marker in the line. Next is the Baseband signal and last the Audio level.
- **Volume:** The Last item on this line is the audio volume control (O-99) that is used with either headphone or speaker if fitted.
- **Secondary Information:** This line provides associated information for the following items these are:
    - **AM:** Bandwidth settings of DSB 9k, DSB 6k, USB+3k, LSB-3k, CW. The Spectrum view is +/-20k.
    - **NFM:** Bandwidth Settings of 16k,11k,8k5. Note there is no setting for the more common 6k5 used in European Spectrum plans. Next item is SQ: which is shown in the format of 40/99 allow the noise squelch point to be set Between 0-99. Typically, around 40-50 is a good threshold.
    - **Gain:** The RF Amp settings. The Spectrum view is +/-20k.
    - **WFM:** There are three option filters in that Secondary settings :
    - (1) 200k ,the original filter for commercial FM stations with soft transition,
    - (2) 180k with sharp transition, for also commercial FM broadcast station, specially useful to improve demodulated S/N in around 6 to 8 dB‘s in weak signals .
    - (3) 40k with also sharp transition, for supporting NOAA APT weather satellite reception in 137 MHz . (that filter is too narrow for WFM with 75khz delta deviation and can produce audio distortion in the demodulated sound). The Spectrum view is +/-100k with a marker That may be changed (though seem the incorrect value).
    - Just below REC Icon we have a marker Frequency field input (0 Hz) , that we can adjust from 0..48kHz range with the knob rotary encoder, with 200 Hz step jumps. It will move a short vertical red line pointer cursor across the Multiplex FM demodulated baseband FFT spectrum graphic. It could be useful to see and confirm the exact frequency of those spectrum peaks, like the below picture , showing 19Khz pilot carrier tone from a usual Stereo FM Broadcasting.


```
* **SPEC.** The spectrum Secondary Items allows the view of the RF spectrum with different setting for maximum bandwidth shown:

        20M with markers at +/- 5M
        10M with markers at +/- 3M
        5M with markers at +/- 2M
        2M with markers at +/- 500k
        1M with markers at +/- 300k
        500k with markers at +/-200k
```

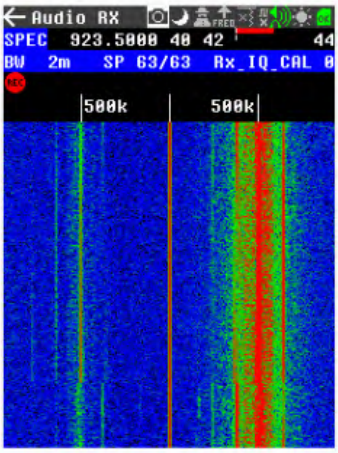
The next item is the setting of the bin sizes used for the waterfall (0-63) with “0” being the minimum information being the fastest display and “63” the maximum information collected the slowest display. Adjust to give a balance of speed and information seen.

And next right to that field ,while you are still in SPEC mode, you will see the Rx_IQ_CAL field. It actually can improve (8 to 10 dB's from worse CAL point to the best one) the receiver Image Reject Ratio (IRR) only in the Receiver Applications that are using Zero IF-frequency tuning ,like this SPECTRUM mode. This calibrated value will be stored in the SD card , /settings/rx_audio.ini .

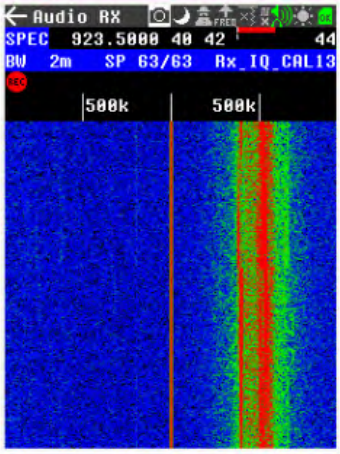
To calibrate it , you will need to try to find some clean isolated continuous air carrier signal (please make sure that it is a real air signal, not internal harmonic residual interference clock beats) , and try to tune it , (for example, to the right of the positive frequencies). Select properly the SPEC BW to try to isolate that air carrier signal (in below example , I selected BW = 2 Mhz). Then, to make slightly more visible the bare Image mirror frequency -that appears in the other symetric left part screen.-, you will need to start set up CAL to 0 (min). Then , you will need to adjust AMP , LNA and GAIN to receive strong enough signal to the right part (but at the same time , not so strong to not produce intermodulations , otherwise re-adjust again decreasing AMP, LNA, GAIN) , and not so weak , till just getting the carrier +freq. clean (desired carrier signal) , and its bare visible Image mirror Signal (in the other symetrical -xx mirror freq . (unwanted Image signal to be minimized) . Then, when you got similar situation as left below picture, you can start adjusting Rx IQ phase CAL till minimizing the received Image "mirror" signal (as in the middle below picture).

That below example is calibrating H2+ old r6 version (max2837) that has 31 steps ,(Note , using Hackrf r9 (max2839 ,you will have 64 steps)

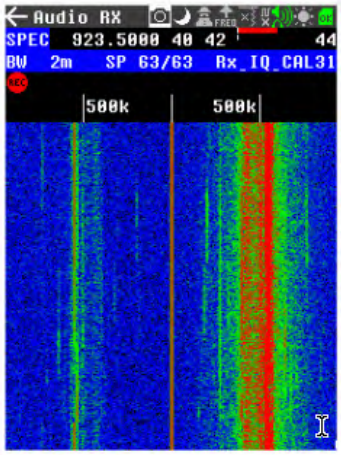
Rx_IQ_CAL = 0/31 (Min value)



Rx_IQ_CAL = 13 (best calibration)



Rx_IQ_CAL = 31/31 (Max value)



- **CTCSS:** This Continuous Tone Coded Squelch System is a display at the end of the secondary information line. It is used by many systems and standardised by EIA/TIA, with a description here. In the NFM mode in Audio app, the tone field is increased from 11 to 14 characters. Now , the CTCSS tone frequency and CTCSS code numbers are displayed at once (if a matching freq was found in the tone_key table). See the Annex to this document below. It should be noted that most of the time the display is jumping around and only clearly displays the received tone when there is a gap in the voice and the Signal is of good quality.
- **Record:** The record button if selected will show the record file name, % of the SD Card used, and at the end of the line is the total recording time available left on the SD card and this decrements when recording. The file name of the recorded 16-bit mono WAV file includes the date, time, and radio tuning frequency. The WAV file sampling rate depends on the receiver mode; 48KHz for WFM, 24KHz for NFM, or 12KHz for AM.

CTCSS Tone List

```
None      0.0
0 XZ      67.000
1 WZ      69.400
2 XA      71.900
3 WA      74.400
4 XB      77.000
5 WB      79.700
6 YZ      82.500
7 YA      85.400
8 YB      88.500
9 ZZ      91.500
10 ZA      94.800
11 1ZB      97.400
12 21Z      100.000
13 1A      103.500
14 1B      107.200
15 2Z      110.900
16 2Z      114.800
17 2B      118.800
18 3Z      123.000
19 3A      127.300
20 3B      131.800
21 4Z      136.500
22 4A      141.300
23 4B      146.200
24 5Z      151.400
25 5A      156.700
40 --      159.800
26 5B      162.200
41 --      165.500
27 6Z      167.900
42 --      171.300
28 6A      173.800
43 --      177.300
29 6B      179.900
44 --      183.500
30 7Z      186.200
45 --      189.900
31 7A      192.800
46 --      196.600
47 --      199.500
32 M1      203.500
48 8Z      206.500
33 M2      210.700
34 M3      218.100
35 M4      225.700
49 9Z      229.100
36 --      233.600
37 --      241.800
38 --      250.300
50 0Z      254.100
Axient 28kHz      28000.0
Senn. 32.768k      32768.0
Senn. 32.000k      32000.0
Sony 32.382k      32382.0
Shure 19kHz      19000.0
```

BLE RX

As of 10/31/23, the previous BLE implementation has been updated, and improved to correct some of the issues in the previous BTLE app.
This BLE app has several features which I will highlight in a brief overview.

Main Menu:

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

1. The BLE app upon entry will scan for **only** 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 randomly from Channel 37-39 every 100ms.
2. Once found the user can then select an individual MAC Address entry to pull up a more detailed view of most recently captured data packet from this MAC Address.
3. The **Sort Knob** will sort the list of MAC indices by either Ascending MAC Address, device name, number of hits, dB, or by most recently updated entry.
4. 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.
5. 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.
6. The **Log** toggle allows BLE app to write all filtered packet data into SD card under `/BLERX/Logs`. Each log entry contains timestamp, packet type, length of the packet, MAC address, and packet data.
7. The **Clear** button allows the user to clear entries as they fill up the screen.
8. 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.
9. The **Tx** button allows the user to switch to the BLE Tx app. See BLETX for more information.

Packet Detail Menu:

This menu is a more single detailed view on a specific entry selected by the Main Menu. More specific packet information is laid out here such as:

1. The **MAC Address**
2. The **PDU Type** which displays the last received PDU packet type as noted here:

Type	Name	Description
`00`	`ADV_IND`	Scannable advertising indication for all devices
`01`	`ADV_DIRECT_IND`	Directed advertising to a specific device indicating that only that device can connect
`02`	`ADV_NONCONN_IND`	Advertising indication but not accepting connections or scans
`03`	`SCAN_REQ`	Sent by a device to receive more info from scannable advertisers
`04`	`SCAN_RSP`	Response to 03 containing more info
`05`	`CONNECT_REQ`	Sent to an advertiser to initiate a connection
`06`	`ADV_SCAN_IND`	Scannable advertising indication but not accepting connections
`07`	`ADV_EXT_IND`	BT 5.0, points to additional data on secondary channels
`09`	`AUX_ADV_IND`	BT 5.0, scannable advertising indication for all devices on secondary channels
`0A`	`AUX_SCAN_REQ`	BT 5.0, sent by a device to receive more info from scannable advertisers on secondary channels
`0B`	`AUX_SCAN_RSP`	BT 5.0, response to 0A containing more info
`0C`	`AUX_CONNECT_REQ`	BT 5.0, sent to an advertiser to initiate a connection
`0D`	`AUX_CHAIN_IND`	BT 5.0, chains advertising packets together when they get too big
`0E`	`AUX_CONNECT_RSP`	BT 5.0, response to 0C
`10-26`	Link Layer	Link layer setup and operation
`26-FF`	Data	General data and proprietary

3. The last packets received for each data type, their length, and their contents.
4. The **Send** button immediately moves the user to the BLE TX app and allows the user to transmit the selected packet data.
5. The **Save** button allows the user to save packets in the format used by the BLE TX app.
6. The **Done** button brings the user back to the Main Menu.

Video:

Below short example on using the BLE Rx App.
https://vimeo.com/886881206?share=copy

References:

BLE Tx App: Bluetooth Low Energy Transmitter
BLE Packet Types: https://www.bluetooth.com/wp-content/uploads/Files/Specification/Assigned_Numbers.pdf?id=3
Reference Code Used in Porting Protocol: https://github.com/JiaoXianjun/BTLE

ERT Meter

Encoder receiver transmitter (ERT) is a packet radio protocol developed by Itron for automatic meter reading of water, gas and electricity. The system uses OOK short range radio which is transmitted in the unlicensed 902-928 MHz ISM band, so that meters can be read from a passing vehicle. This is mainly used in USA. The data is not encrypted, and does not have functions to enable full control. The system is not as advanced as a smart meter and lacks the control or security in the data transferred. Supported message protocols are IDM, SCM, and SCM+.

The Key Items on the App that can be selected with the cursor and changed with the encoder knob are:

- **Title bar:** The usual Items may be changed and displayed.
- **Frequency:** The default frequency of 911.6 MHz can be modified in newer firmware (the ISM band is commonly ~902 MHz to 928 MHz).
- **Gain:** Setting are shown in order of AMP 0=0db or 1=14dB, LNA(IF) (0-40) and VGA (Baseband Gain) (0-62).

Fields displays in the App are as follows:

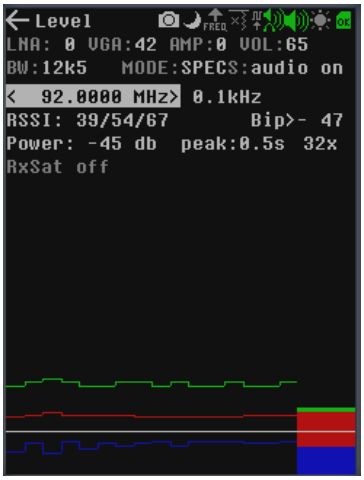
- **ID:** this is the meter ID (in decimal format; should match number/barcode printed on meter).
- **Ty (or Tp):** This is the type of meter as indicated in the message. (Likely meter type codes include Electric: 4, 5, 7, 8, 12; Gas: 0, 1, 2, 9, 12; Water: 3, 11, 13)
- **Consumpt:** The Meter reading value.
- **Tamp:** Tamper flags. For SCM type meters the tamper flags are shown as single-digit physical/encoder tamper flags respectively. For SCM+ or IDM type meters the tamper flags are shown as a 4-digit hexadecimal value.
- **Ct (or Cnt):** The count of the number of readings with the same meter ID (or ++ if the value exceeds the field width on the screen).

The PortaPack ERT receiver monitors approximately 2.5 MHz centered around 911.6 MHz. It does not implement channel filters, so sensitivity is reduced in exchange for monitoring more simultaneous "channels".

If a FAT-formatted micro SD card is present when this mode is entered, the receiver will log received packets to a file named "ERT.TXT". The log file contains one line per packet received. Each line consists of a timestamp in sortable "YYYYMMDDHHMMSS" format, the Manchester-decoded data bits, a "/", and a per-bit Manchester coding error indicator ("1" if the data bit is in error), and the meter ID. Received data that looks like it might be a packet (based on the sync bits) but has an invalid checksum will not be listed on the screen although it will be listed in the log file for debug purposes; adjusting the gain values may help in this case.

Level

Level App



Introduction

The level app is as simple as possible and allow you to monitor available level meters in a single view. CTCSS tone showed if NFM is selected.

Buttons

- [LNA] , [VGA] , [AMP] , [VOL] => gains, amplification on/off and volume
- [BW] , [Mode] , [STEP] => bandwidth, demodulation and step
- [FREQ] , [AUDIO] => Frequency adjustement, audio on/off (audio button also controls beep mode in SPEC)
- [PEAK] => enable peak hold and timer, or disable it
- [xXX] => set the number of columns in the live history

Informations on screen

- RSSI: min, average, max values, beep squelch value in db (adjustable)
- POWER: current db power level
- RxSat: Receiver Saturation in percent. Ideal value around 80%. Color gradient between (0,blue),(80,green),(100,red) [CTCSS tone if NFM is selected]

Right level meter

- RSSI min => blue fill
- RSSI avg => horizontal white bar
- RSSI max => red fill, peak hold in green if enable

Graphs

- RSSI min, average, max => blue, white and red lines clipped between [31, 170] and scaled along the height of the RSSIGraph widget
- POWER => green line, clipped between [-100 , +20] and scaled along the height of the RSSIGraph widget

NRF

NRF is a proprietary low-power and low-cost transceiver in the 2.4Ghz range produced by Nordic Semiconductor. It mainly used for remotes, keyboards and mice and in general low power comunication. It is often seen as nFR24L01 and similar cheap transceivers popular with the hobby electronics crowd. It is also popular in radio control of mini-drone.

With this app, you can use portapack to decode the data sent from NRF24L01, and also see some data messages in 2.4GHz. I currently supports only 250KPS mode.

References:

https://www.youtube.com/watch?v=8ZnWxhCkDkk

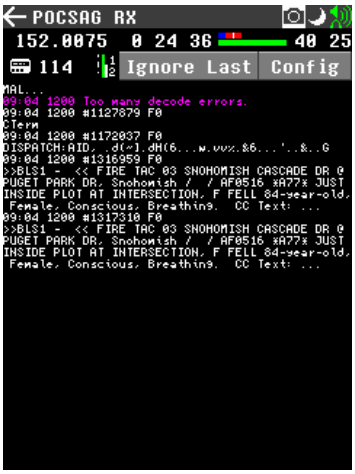
https://blog.csdn.net/shukebeta008/article/details/105478579

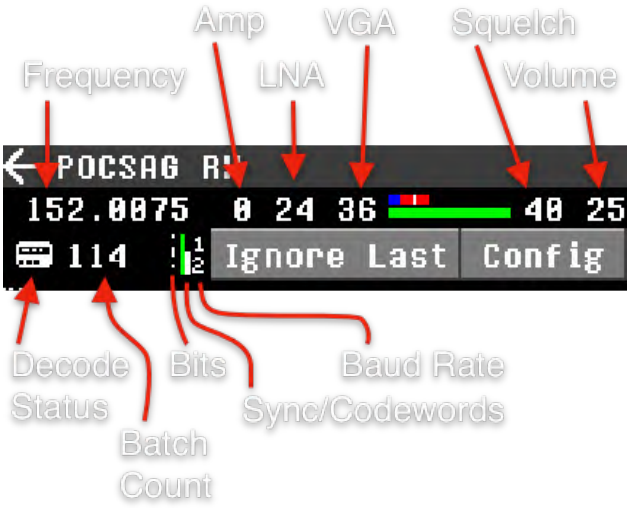
POCSAG

Receives pager messages using the POCSAG protocol.

This protocol operates in the VHF/UHF bands using FSK modulation. More technical details can be found by following the links in the References section.

UI Overview





Settings

- **Frequency**: Sets the frequency to receive pager messages on. Can be adjusted with the encoder thumb wheel, on-screen numpad, or loaded from frequencies saved on an SD card. 439.9875 MHz is the most popular worldwide frequency used by Amateur radio for POCSAG. Amateur radio POCSAG uses 1200bps.
- **RF amplifier** (0 or 1): Enables/disables the internal RF amplifier.
- **LNA gain** (0, 8, 16, 24, 32, 40): Sets the LNA gain. Further information: Description of the gain settings
- **VGA gain** (0 to 62): Sets the VGA gain. Further information: Description of the gain settings
- **RSSI/Audio**: Top bar indicates signal strength. Bottom bar indicates the audio level. The audio bar can be useful for tuning settings without headphones/speaker to hear the tone.
- **Squelch** (0-99): Sets the signal to noise threshold. 0 disables squelch. Higher values allow more noise. Should be set so that strong signals are clearly received without any dropped audio.
- **Volume**: Output volume for the received audio. Can be used to monitor received signal quality.

Information

- **Decoder Status**: Indicates the status of the decoder state machine. White: Idle, Cyan: Clear, Yellow: Waiting for message start, Green: Waiting for rest of message.
- **Batch Count**: Number of message batches that have been received. A batch has 16 codewords.
- **Bits**: Displays the bits that are being decoded into codewords.
- **Sync**: Green when the frame decoder has received a "sync" frame. Messages are not decoded unless a sync frame is found.
- **Codewords**: Shows the number of codewords in the current batch. When the bar fills, the batch is complete and is processed.
- **Baud Rate**: The detected rate of the current message. 05: 512bps, 12: 1200bps, 24: 2400bps.

Buttons

- **Ignore Last**: Enables "Ignore" mode for the last received address.
- **Config**: Enters the settings page to configure options.

Config

- **Enable Log**: Logs messages to the SD Card at "LOGS/POCSAG.TXT"
- **Log Raw Data**: Logs the batch codewords as hexadecimal. Useful for debugging decoder bugs.
- **Use Small Font**: Uses the 5x8 font in the UI to show more messages on the screen.
- **Hide Bad Data**: Don't show (or log) codewords that fails checksum validation.
- **Hide Addr Only**: Don't show (or log) codewords that don't contain a message.
- **Enable Ignored Address**: Don't show (or log) codewords sent to the specified address.
- **Beta**: Enable the new POCSAG baseband processor. The app *must* be restarted for this to take effect.
- **Save**: Save any settings changes.

NOTE: App Settings must be enabled for settings to be saved.

Message Display

Typical message:

```
12:34 1200 #432123 F2
This is a test message
```

Description (from top-left):

- `12:34` - **Time**: The time that the message was received (time from PortaPack).
- `1200` - **Data rate**: The data rate used to receive the message.
- `#432123` - **Address**: The address of the intended pager recipient.
- `F2` - **Function**: (0 to 3) Indicates the type or source of message sent (can be used to provide a category of sorts).
- `This is a test message` - **Message**: The message data displayed as ASCII.

References

The following resources provide more technical information about the POCSAG protocol:

- POCSAG - Signal Identification Wiki - Provides frequencies commonly used in different countries and regions
- POCSAG - WikiPedia

Radiosonde

Radio Types + Values Implemented

https://radiosondy.info/
https://sondehub.org/

MeteoModem M10

- Latitude
- Longitude
- Altitude
- Battery Voltage
- Serial Number

MeteoModem M20

- Latitude
- Longitude
- Altitude

MeteoModem M2K2

- Latitude
- Longitude
- Altitude
- Battery Voltage

Vaisala RS41-SG

- Signature
- Serial
- Battery Voltage
- Frame Number

- Altitude
- Latitude
- Longitude

Checkboxes

Beep

Enabling "Beep" will cause an RSSI-level dependent beep to occur whenever a packet is received. (Audio frequency of the beep will correspond to signal strength)

Log

Enabling "Log" will cause any received packets to be logged in the file /LOGS/SONDE.TXT.

CRC

Enables CRC checking.

Map Buttons

See QR

Press the "See QR" button to generate a Geo URI QR code in the form "geo:latitude,longitude". Scanning the displayed QR code on a cellphone should result in the phone opening its map application to the specified latitude/longitude coordinates.

See on map

Pressing the "See on map" button opens the world map view to the specified coordinates (the world_map.bin file must be found in the /ADSB folder on the SD card)

Recon

Recon App

Important note

Repeater and all associated repeat modes are under development. The documentations related to it are for devs/nightly testers. You will not yet find it in stable.

Introduction

The Recon app is full rework of the Scanner app, offering different possibilities and customisations.

Both are using all the frequencies in their hand and pause on a frequency when matching criteria (like modulation, amplitude,...)

The Recon is using a different approach than the Scanner app it is originated from: it does not use a thread for frequency shifting and else rely on the statistics update event message to do the work.

This allow perfect matching between 'shifting to a new frequency' and 'waiting for the first statistic update of that frequency'. The Recon app will stop into any frequency carrying a signal strong enough. You can adjust the signal power threshold with the SQUELCH

In AM/NFM/WFM mode

The statistics only update once each 100ms, the minimum lock waiting time is also 100 ms, and the quickest frequency scanned rate is 10/s.

In SPEC mode

The statistics are updated differently in regard of the bandwidth used.

The average locking times / scan rates are in the following the table (they may change when there are baseband or record process modifications)

- average of 10/s from 12.5k to 1500k
- average of 5/s from 1750k to 3000k
- average of 3/s from 3000k to 5000k

Limitations

The portapack hardware is limited, and so is the list of elements that you can load.

A maximum number of 115 elements is allowed. One more element is allowed to detect that the file was truncated.

If a file was loaded and truncated, the displayed list name and current entry description are in yellow instead of other colors.

TODO first

If you are launching the Recon app for the first time, chances are high that you do not have the wanted options selected by default.

We highly encourage you to go and check what's under the "CONFIG" button and get yourself used to the 'Main' and 'More' pages under it.

Common defaults options to set

Go into "CONFIG":

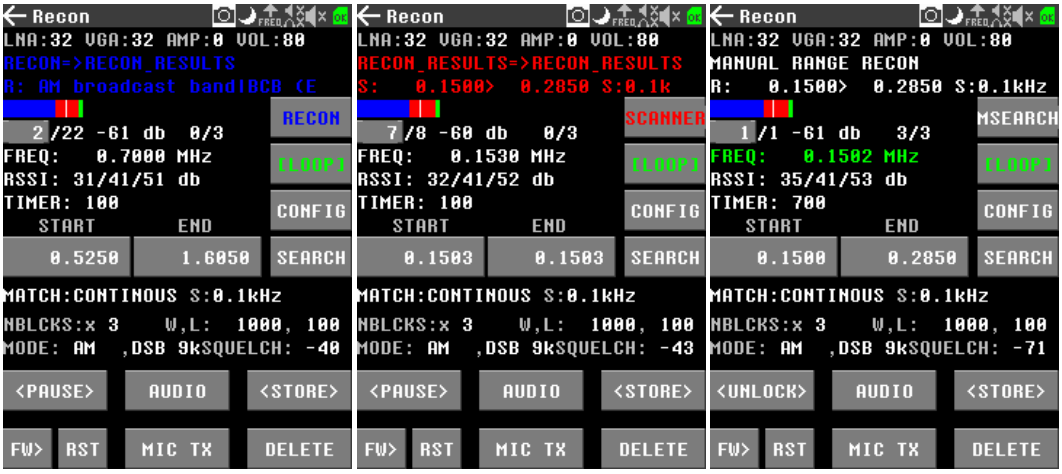
Main:

- Check input file and output file name
- Check options under it. A lots are complaining that the search is not starting by itself, but they do not have 'autostart recon' checked.

More:

- Check that 'input: load freqs' and 'input: load ranges' are checked

Main Screens



Buttons and information description, from top to bottom, and left to right. [NAME] is used to mark a button / gui element that the user can change, else it's a description of an onscreen information.

- [LNA] , [VGA] , [AMP] , [VOL] => gains, amplification on/off , volume
- Current input file name => will be in yellow if file contain too much lines or red if an error description is shown, or follow mode colors
- Current entry description => input name, will be in yellow if file contain too much lines or red if an error description is shown, or follow mode colors
- [RssiGraph], [MODE] => radio levels indication, jump to level app on click. Mode is one of [RECON/SCAN/MANUAL] and show actual mode, and switch to next mode on click

- [XXX] / XXX , XX db, XX/XX value => index of the current frequency in the loaded list (move with encoder, or set a value by clicking), number of frequencies in the list, actual DB value, number of locks / number of needed locks for a match, button to the settings page. Will be in red if file contain too much lines or if an error description is shown
- FREQ: XXXX , [LOOP] => Current frequency , [LOOP] button to control continuous mode or not (green is on, white is off)
- RSSI: XXX/XXX/XXX => Current min/med/max RSSI values in db
- TIMER, CTCSS, [CONFIG] => elapsed timer for current frequency lock (0 if no lock) , detected tone if NFM is selected, and CONFIG button to set things like input/output files
- [START], [END], [SEARCH] => set the manual start and end of a range and launch a search on it. These values will be updated by the search if auto update m-ranges is checked. If highlighted, you can use the rotary encoder to adjust start or end
- [MatchMode] , [STEP] => Matching mode, manual range steps
- [NBLocks] , [W] , [L] => NBLocks is the numbers of locks we need to have a match. [W] (wait after match) is the time we will stay on the frequency if it's reaching nb_locks during lock_wait (continuously or sparsely). If wait is a negative number, then it represent the time we are staying on a matched frequency waiting for new activity, and a new lock during the wait restart the counters (you keep staying on it until a full wait without a lock is reached). [L] (lock duration) is the maximum time we stay on a freq waiting for all locks in SPARSE match mode, and the time we are waiting for the first lock in CONTINUOUS match mode.
- [MODULATION] , [BW] , [SQUELCH] => actual modulation and bandwidth ,squelch is the level of DB needed to start to lock on a signal
- [PAUSE] , [AUDIO] , [STORE] => pause or resume the search. If highlighted, you can use the rotary encoder to manually step in the frequencies/ranges, jump to Audio App, store actual frequency in output file. Audio button is becoming red in auto record modes to indicate that a record in ongoing
- [FW], [RST], [MIC TX] , [REMOVE/DELETE] => forward/reverse , reset search (it's restarting from the beginning of input file), jump to Mic app, Remove a frequency from active/loaded list in RECON mode or Delete from both active/loaded list and output file in SCAN mode

CONFIG

Main RECON settings page

- input file => File from which we will load frequencies or ranges to search (default FREQMAN/RECON.TXT)
- output file => File into which we will save frequency using STORE button or autosave mode (default FREQMAN/RECON_RESULTS.TXT)
- output file name => The name of the current output file. Can be edited when clicking on it so you can set a new filename
- autosave freqs => During the search, matching frequencies will be saved without clicking on STORE. No duplicates will be made
- auto start search => Search will start when entering the app, or when going in and out of CONFIG
- continuous => If checked then the search will loop when reaching boundaries of the loaded input file or the manual range search
- clear output at start => If checked then the output file is blanked at app start. If you're using that feature and want to keep one of your search results, do not forgot to go into filemanager to rename the file before starting the Recon app one more time

More CONFIG settings page

One of the first two options have to be checked else nothing will be loaded at all and only manual range search will be available

- load freq => allow load of frequencies
- load repeater => allow load of frequencies
- load range => allow load of ranges
- load hamradio => allow load of ham radios
- auto update m-ranges => if checked then the manual range start and stop values are updated using the actual searched range values. If it's actually searching a frequency, manual ranges are untouched
- record locked period=> activate auto record during locked wait (green) state. In audio modes, a wav file with actual time of capture as filename is created in AUDIO directory. In SPEC mode, a raw c16 with actual time of capture as filename is created in CAPTURES directory.
- repeater,[keep or delete] => activate repeat function, keep or delete repeated files. nb => number of repetitions

- amp => enable/disable amp when TX repeat is on. gain => gain to use when TX repeat is on

!! WARNING: YELLOW COLORED OPTION ARE FOR TX CONFIG !!

!! WARNING: USING REPEATER ACTIVATE RECON TX ABILITIES !!

!! WARNING: BE CAUTIOUS WITH 'auto record locked period' OPTION. DON'T FORGET CLEANING UP FROM TIMES TO TIMES, TOO MUCH FILES WILL CRASH THINGS !!

Recon/Search/Manual

When using the Recon app, 3 modes are accessibles.

You can switch from RECON to SEARCH using the GUI button, and to Manual search using the Manual-S button (just under the RECON/SEARCH button).

RECON mode

Mode button is in blue, and the label is 'RECON'.

In that mode it takes what you choose in "CONFIG/select input file" and use it as the list to search. The matched frequencies (if autosave is checked or 'add' is used) are put in what you choose in "CONFIG/select output file".

REMOVE is removing current entry from active/loaded list. No files are touched.

STORE is adding current entry to output file.

In that mode you have an input search/recon list, and an output file. You can temporary 'disable' some entries by a hit on REMOVE. Clicking on RST is reloading the fully populated list.

SCAN mode

Mode button is in red, and the label is 'SCAN'.

In that mode it takes what you choose in "CONFIG/select output file" and use it as the list to search.

The matched frequencies (if autosave is checked or 'add' is used) are put in what you choose in "CONFIG/select output file".

DELETE is removing current entry from active/loaded list and from output file.

STORE is adding current entry to output file.

In that mode you have the same file used as an input list and an output file.

MANUAL-S

In that mode RECON or SEARCH mode are invalidated. Values in GUI are used as a single range entry.

The matched frequencies (if autosave is checked or 'add' is used) are put in what you choose in "CONFIG/select output file".

STORE and REMOVE are working on the output file but changes are not reflected in the used list since it's a loaded range.

In that mode you have a single range as an input list, and an output file.

Wait/lock Coloring conditions:

Lock coloration (only in SPARSE matching mode):

- if lock duration is lower or equal to (min_lock_duration x nb_locks) => value is in yellow to indicate that there is not enough time to match nb_locks. Coloration are not used in CONTINUOUS as lock timer is disarmed at first lock count.

Wait coloration:

- if wait is between [-500,500] ms and not 0, it's red because the audio will have hard time start and stop that quick during consecutive matches
- if wait it > 500 it's the time we are staying on a matching freq before skipping, wait value is in white
- if wait < -500 it's the time we are waiting for new activity before skipping. Any new activity (db>squelch) is resetting the timer to 'abs(wait)', wait value is in green
- if wait == 0 it's recon mode. No wait after match. No audio start/stop. Matching freqs are auto saved according to the options in CONFIG, wait value is in blue

Color meaning for main freq

- white => pause / reading signal
- yellow => got a lock, trying to achieve a match (when we have nb_locks counted during lock_wait, continuously or sparsely)
- green => during a search : locked , during a pause: current freq is matching squelch level and nb_locks have been reached

Wait modes

- wait is the timer started after a matched frequency
- wait > 0 : after a lock stay on freq for 'wait' msecs before skipping to next
- wait == 0 => immediately leave freq after a lock. Use in conjonction of autosave option to make a quick map of matching frequencies
- wait < 0 : after a lock stay on freq for 'wait' msecs before skipping to next, each new lock (db>squelch) reset the counter to 'wait'

Lock counts

Lock count is reset to 0 after using one of the following buttons:

- PAUSE
- FW,RW
- CONFIG
- SQUELCH

Matching modes

Continuous

- measurement is done in lock_wait msecs
- at each loop if the mean db is > squelch, it's a lock
- in that mode you need consecutive nb_locks to match a frequency
- it's quicker because we do not wait lock_wait to get nb_locks, it's matching as soon as the counter is reached. It can also miss signals since it's rigorous and skip if there is a gap between matches

Sparse

- measurement is done in lock_wait msecs
- at each loop if the mean db is > squelch, it's a lock
- we need nb_locks before lock_wait expires, but we can have some that are not matching, the lock_count is kept until nb_locks or the timer is set
- it may take longer: any first match is going to trigger a delay of lock_wait, which wait until it reach 0 or nb_locks is reached. It's less sensible to bad reception
- the lock duration timer can be yellow colored to indicate that you're not leaving enough time for a SPARSE match of nb_locks to happen

Frequencies to scan

The application parses `FREQMAN\RECON.TXT` by default. If you set something else in the CONFIG menu under input, then the specified file will be used You can use the Frequency manager app (Tools -> **Freq manager**) to add more entries to that list

Alternatively, you are able to manually input a search range "on the fly" by keying in START and END frequencies. It will uses the selected step on screen

If highlighted you can also use the rotary encoder on start / end buttons to adjust the frequency

Modulation Mode

You can select between **AM** , **NFM** and **WFM** modulation modes

On each modulation you can select bandwidth according to modulation value

Step can also be changed, and is only used in range search (manual or not)

If a custom modulation/bandwidth/step is set on the actual freqman entry (from freqman file), it's used as new defaults for next entries

Persistant settings

In the idea to be more user friendly the Recon app is keeping some settings in memory and on the sd card. All the settings that you can set in CONFIG menus will be saved and restored upon poweroff/on or app restart

Squelch is saved between runs / updates

Freqman file format

See Freqman Manager page

HamRadio type

HamRadio type is special case.

It represents a Ham Radio relay: relay RX freq for frequency_a (r=) , relay TX freq for frequency_b (t=)

In Recon, when current type is HamRadio:

- Both RX and TX frequencies are scanned for activity as two single frequencies
- When clicking 'MIC' while on one of the HamRadio entry frequencies, Mic TX frequency is set to relay RX frequency, and Mic RX frequency is set to relay TX frequency

Repeater type

Repeater type is special case. It's an entry that allows the portapack to act as a half duplex Repeater.

The frequency_a (l=) is the Repeater listening frequency, and frequency_b (t=) is the Repeater TX frequency

!! WARNING: These functions are activating TX in Recon. You have to know what you do !!

If you want to use the Repeater functionality:

- in CONFIG, 'record locked period' and 'repeat' have to be checked
- while you're at it, set the number of reps and the delay before each TX
- the modulation type have to be SPEC and use the target relay signal bandwidth

In Recon, when current type is Repeater and repeater mode is DISABLED:

- only listening freq is used to check on activity (l=)
- entry will be scanned as single frequency

In Recon, when current type is Repeater and repeater mode is ENABLED:

- listening freq is used to check on activity (l=)
- entry will be scanned as single frequency
- on squelch level match raw record is started
- on timeout or inactivity timeout the raw record is stopped
- tx delay is played if any
- raw record is replayed using the Repeater TX (t=) frequency

Raw Record, when used in conjunction of Repeater, is using the same file to store the record: /CAPTURES/RECON_REPEAT.C16

Advanced Repeater configuration

The Repeater, in addition of Recon, can be used as a half duplex multiplexed relay.

Here is a graph showing how Alice and Bob could talk using a Repeater list in Recon

Repeater half duplex dual direction example

```
flowchart LR
subgraph Repeater half duplex dual direction
        AliceTX(Alice TX)
        AliceRX(Alice RX)
        BobTX(Bob TX)
        BobRX(Bob RX)
        R1TX(Repeater 1 TX)
        R1RX(Repeater 1 RX)
```

```
        R2TX(Repeater 2 TX)
        R2RX(Repeater 2 RX)
        AliceTX-->R1RX--->R1TX--->BobRX
        BobTX-->R2RX--->R2TX--->AliceRX
        subgraph Alice
                AliceTX
                AliceRX
        end
        subgraph Bob
                BobRX
                BobTX
        end
        subgraph Recon Repeater's list
                subgraph "Repeater 1"
                        R1RX
                        R1TX
                end
                subgraph "Repeater 2"
                        R2RX
                        R2TX
                end
        end
end
```

Loading

In our example:

- a single portapack is used
- in a freqman file, we are using two Repeater entries: R1 and R2
- R1 is to repeat Alice TX to Bob RX
- R2 is to repeat Bob TX to Alice RX
- Recon is set in autostart, continuous scan
- Wait timeout is set to -1500 (which in our case mean stop recording after 1500ms of inactivity)
- Lock timeout is set to 100
- Match Mode is set to continuous
- NB match is set to 3
- auto record locked, repeater are checked
- nb repeat is set to 1 and the delay to 0

What is going to happen:

- Alice is going to use any tone/start delay to open Repeater 1
- Recon is matching a squelch level on Repeater 1 and is going to start record
- Alice have stopped talking. 1500 ms later, the record is stopped
- Recon transmit the record to Bob, using Repeater 1 TX frequency
- Bob hear Alice. He wants to answer, and send to Repeater 2
- Recon is matching a squelch level on Repeater 2 and is going to start record
- Bob have stopped talking. 1500 ms later, the record is stopped
- Recon transmit the record to Alice, using Repeater 2 TX frequency

What are the possibilities:

- as long as Alice and Bob are not talking simultaneously, they can use the Repeater as much times each as they want
- you can add more Repeaters in the list. Keep in mind that it's 100ms more scan time for each entry

Workflow and tips

Classic workflow

- Select an input an output file, adjust the settings in CONFIG while you're at it
- Start the RECON, match frequencies, add them to your output file using autosave or STORE button
- Switch to SCAN mode to refine your results

Repeater workflow:

- Select a prepared input file / use the classic workflow to set the frequencies you want in the scanner list
- In CONFIG/MORE, be sure that repeaters options are set (enable/disable, nb rep, tx amp, tx gain, load repeater entries)
- For a repeater mode, Recon entries have to use SPEC mode. Set the bandwidth accordingly, it's used as record/replay bandwidth
- Select the lowest lock time value (l) : 100
- Select a negative wait locked value, it means on freq as long as there no more than 'wait locked' msec of inactivity. -1500 proved to be good for conversations, for signals you may reduce the wait locked. It's also the minimum recorded time by the way.
- Set a squelch level that allow to only catch what you want. As an example, here I have a background noise of -40 db, when I hit the remote the level is going up to +5 db. To filter sparse signals from my remote, I set squelch of -10db, and adjust it down to catch more, up to catch less
- If you're not in 'autostart' you'll have to press 'RESUME' at start and after a record. Don't forget to set it in 'CONFIG' if needed
- Having 'LOOP' enabled is a good idea whatever your list is (it will allow you to avoid pressing RESUME each time too)
- Set number of matching packet from 1 to 3 as you want to quickly start recording and not wait for precisely long signal
- Set match type to continuous match
- Let it run
- Hit the remote / Make a MicTX com / whatever you're allowed to record and repeat
- auto record should start (RAW button should go red)
- at the end of record, progress bar of replay is shown / played / hidden

Tips:

- When a file is loaded and checkbox 'autostart searching' have been checked, the search is starting as soon as the apps open up, using last launch settings
- If 'autostart searching' is not used, then at the app start the last input list is loaded and the search is set in pause on the first frequency of the list
- To start a search using the input file, use the PAUSE/CONTINUE/RESTART or RST button

- To start a search using the manual entry fields on the main screen, fill START/END and use the SEARCH button
- The rotary encoder can be used on the PAUSE/CONTINUE/RESTART and START/END buttons to adjust the frequencies values
- On a frequency match, if the focus is given to the PAUSE/CONTINUE/RESTART button, press the button or use the rotary encoder to allow you to continue the search. It allows you to go to next freq, and trough both direction, changing the search direction on the fly. Pressing the button while in frequency match (locked mode continue the search using actual direction
- Recon app is doing it's best when using ranges
- Use a low squelch value and step down little by little to start to catch stronger frequencies first. If you're using a too low squelch value then the search will stop on a lot of unwanted but matching criteria frequencies
- Input and output file should not be the same files. While it's not advised it's working but you loose the ability to delete while in recon mode
- Both STORE and autosave will save frequency with current searched frequency or range description, or "ADD FQ" if no description

Troubleshooting

Most of the time if the Recon app is not working as you expected it's coming from a SDCARD problem. You need a SDCARD for the Recon app to save settings between runs and between settings menu / main gui

If not you will not be able to load a file from FREQMAN directory / save settings

if no frequencies are loading, check that by default the 'input: load X' fields in 'Recon app -> CONFIG -> More' are all checked. And yes, you HAVE to click save in ordre to save the settings

If by some magic you somewhat trashed the configuration and the app isn't starting anymore, try to delete the SETTINGS/recon.ini and SETTINGS/recon.cfg and SETTINGS/recon.ini files using the tools/file manager app

If you're not having your frequencies searched in both direction, maybe you miswrote 'a=' for a single frequency entry

Using the same input and output file is not going to pause a problem until you forgot to uncheck 'clear output at start'. Yeah, you've just clear what you wanted to scan

Scan speed vs Chosen modulation mode

Detection of power level to match against the given squelch value is made at each firmware statistic updates. This determine how long we are staying on a frequency to have a corresponding squelch value.

In all AM/NFM/WFM modes, it's an average of 100ms per statistic update.

In SPEC mode it's somewhat consistent around 100ms from 12.5k up to 1500k included, from which the statistics updates are taking longer, from 300ms to a bit under 5000ms the wider the bandwidth

Power consumption

A continuous search of 63H41M43S was run by user @vag3d, using the default antenna. Settings were a range from 10MHz to 6GHz, WFM, 5kHz steps, 1s wait

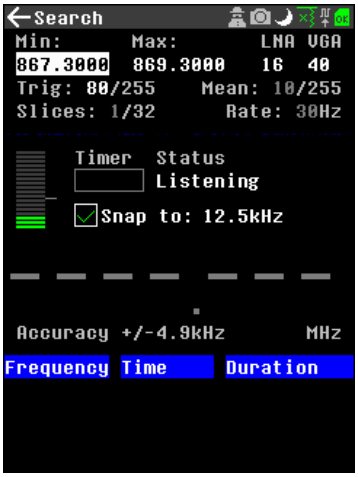
Results: 8002 matching frequencies in the output list, and a consumption as following: 63:41:43 4.8659V 0.4191A 120.448Wh 24.796Ah

The search results were having this form: f=14670000,d=R 10.0000>6000.0000 S 0.0050

Search

Initially from: https://github.com/furrtek/portapack-havoc/wiki/Close-Call

The Search app is similar in functionality found on many Uniden scanners. It allows to define a frequency range to scan (min/max), and a power threshold. If a signal appears above the RF signal threshold for a sufficient amount of time, the signal's frequency is "locked", shown in green on the main display and logged in a table at the bottom of the screen. Unfortunately, it does not allow you to listen to the call or jump to the say the audio App screen with the selected call frequency. You need to manually note the frequency and then place it in another App to listen to the frequency. The Speed of scanning is based the frequency range set. The frequency range if larger than 2.5 MHz will be split in to slices that are scanned. The scan time significantly increase when you have multiple slices.



The Key Items on the App that can be selected with the cursor and changed with the encoder knob are:

- **Title bar:** The usual Items may be changed and displayed.
- **Min:** The minimum frequency. The minimum and maximum frequency are held in persistent memory and are available o return to the App.
- **Max:** The maximum frequency. Regardless of setting of the frequency settings the scan of the frequency spectrum is a minimum of 2.5MHz or multiple slices up to a maximum of 32 (80MHz).
- **LNA:** The LNA(IF) (0-40).
- **VGA:** VGA (Baseband Gain) (0-62). Note there is no RF AMP gain setting and is set at 0dB.
- **Trig:** Alter the Threshold setting (0-255) for the recording of the signal.
- Snap to: Enable to set to record the frequency to the nearest 12.5kHz.

The display information Items are:

- **Mean:** This is the mean signal level received, the Trigger level need to be set above this level.
- **Slices:** The number of “Slices” of the frequency scan range that is to be covered. The maximum is 32 i.e., 80MHz.
- **Rate:** the scanning rate.
- **Timer:** A bar showing the timer counting down.
- **Status:** Showing what the App is currently doing” Listening”, “Locked”, “Out of range”. The “Out of range” indication is shown when a frequency is found that meets the threshold conditions but is outside the frequency range selected and will be shown as light grey in the “Dashed lines” display.
- **Dashed lines:** These are where the detected frequency is displayed and shows initially grey and when reached the timer threshold then turns green.

- **Frequency Time Duration Log:** This is where a detected and locked frequency is logged and display. The logged items can be selected with cursor/ encoder Knob. This then displays the frequency pad where the frequency can be Loaded, saved to a file for example called “Calls” in the SD card. On return it then goes to the “Min:” frequency at the top of the App.

Items that could be improved in the App are:

- The ability to link from the log selection in the log to the Audio Listening App and be able to listen to the audio of the call.
- Select the actual frequency range not in 2.5MHz slices.

TPMS Cars

Tire Pressure Monitoring System (TPMS) operate in the ISM Licence free bands. In USA and most of the world they use 315MHz, in Europe the frequency is 433.92MHz. The TPMS App work well with many common standards used in the automotive industry particularly from Schrader TPMS sensors., and this seems a common standard used in the automotive industry.

The TPMS App display is configured to display the decoded data received from the tire pressure sensors. The interval of the data being sent by each tire varies from every few seconds to minutes depending on the car and sensors, often triggered by wheel movement or rapid pressure changes. Most Schrader sensors can also be triggered to transmit data using a TPMS test tool (which transmits a signal on 125 kHz).

The Key Items on the App that can be selected with the cursor and changed with the encoder knob are: Title bar: The usual Items may be changed and displayed.

- **Frequency:** Either 315MHz or 433.92MHz
- **kPa/PSI :** By highlighting this item the units of pressure displayed can be changed between kPA and PSI.
- **C/F :** By highlighting this item the units of temperature displayed can be changed between Celsius and Fahrenheit.
- **Gain:** Setting are shown in order of Amp 0=0db or 1=14dB, LNA(IF) (0-40) and VGA (Baseband Gain) (0-62).

Data fields are:

- **Tp:** This is the type of the tire sensor decoded the following are coded in the App. Some types of TPMS sensors are not supported.
  - 0 = None
  - 1= FLM_64
  - 2= FLM_72
  - 3= FLM_80
  - 4= Schrader
  - 5= GMC_96
- **ID:** The ID of the tire sensor being 8 hexadecimal characters. Note that sometimes the label printed on the actual temperature sensor is in decimal format.
- **Pres:** This is the pressure in either kilo Pascals (kPa) or Pounds Per Square Inch (PSI).
- **Temp:** The temperature of the tire in either degrees Celsius (C) or Fahrenheit (F). Note Spurious data has been seen and may be due to receive errors, unsupported protocols, or failed sensors. Pressure and temperature ranges may vary depending on sensor model, so best to compare to dash readings, if available.
- **Cnt:** This is the count of messages received from each sensor.
- **Flags:** Information on the type of sensor is only for Schrader and have decode for: fsk_19k, ook_8k192, ook_8k4.

If a FAT-formatted micro SD card is present when this mode is entered, the receiver will log received packets to a file named "TPMS.TXT". The log file contains one line per packet received. Each line consists of a timestamp in sortable "YYYYMMDDHHMMSS" format, receiver frequency, modulation, deviation, symbol rate, and data. The data field consists of Manchester-decoded data bits, a "/", and a per-bit Manchester coding error indicator ("1" if the data bit is in error).

Weather/SubGhzD

> Note
> The wiki is yet to be completed. **Please feel free to add content and collaborate**.

The Weather and SubGhzD apps are supposed to decode AM modulated common signals, like weather stations or rf remotes.

You can check the currently supported protocols here: baseband/fprotos

> Important
> This program is sensitive to signal strength, so if you set values too high or too low, it will not be able to decode.

Ideal values are around: AMP 0, LNA 32, VGA 20. If still nothing, play with these values, try to reduce or increment.

Common frequencies:

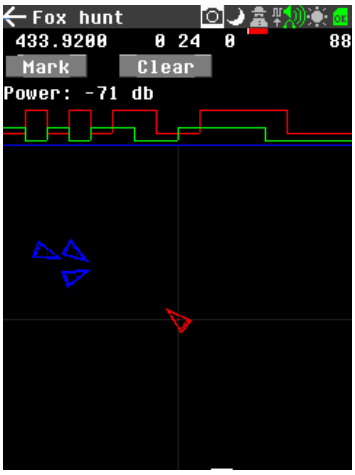
- 433.92 MHz (EU)
- 315 MHz (US, Japan)
- 868 MHz (EU + others)

Fox-Hunt

The Fox Hunt app is designed to help you with the Fox Hunt game, where you need to find transmitters. But it is not only helps you with that game, but you can find other signal sources with it easier.

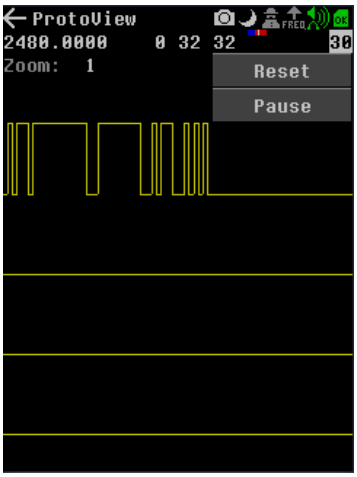
You'll need to set the app to the required frequency. You can set AMP, LNA, VGA, and speaker volume. Speaker will play the AM signal it receives, for the game it is mostly a morse code. There is a signal strength widget, what is a great indicator when used with **directional antenna**!

The app **supports external GPS and orientation module**, so you can see your current orientation and position in the map. You can add markers, so you it can help you find the source. It helps a lot if you zoom in the map a lot!



ProtoView

ProtoView



The ProtoView application is pretty simple:

- tune in a frequency you want to monitor
- adjust AMP/LNA/VGA and Volume (volume may not do anything)
- use the pause button to stop refreshing the view
- use the reset button to reset the view
- use the zoom to zoom in and out the displayed signal

When in pause mode, a 'shift' field appears. Go over the shift value, use the rotary encoder, and shift trough the signal.

Transmitters

The following are Extracts from HackRF Documentation that can be found here.. This applies to all Transmissions using the HackRF/ PortaPack.

What is the Transmit Power of HackRF?

HackRF One’s absolute maximum TX power varies by operating frequency:

- 1 MHz to 10 MHz: 5 dBm to 15 dBm, generally increasing as frequency increases.
- 10 MHz to 2150 MHz: 5 dBm to 15 dBm, generally decreasing as frequency increases.
- 2150 MHz to 2750 MHz: 13 dBm to 15 dBm.
- 2750 MHz to 4000 MHz: 0 dBm to 5 dBm, decreasing as frequency increases.
- 4000 MHz to 6000 MHz: -10 dBm to 0 dBm, generally decreasing as frequency increases. Through most of the frequency range up to 4 GHz, the maximum TX power is between 0 and 10 dBm. The frequency range with best performance is 2150 MHz to 2750 MHz.

What gain controls are provided by HackRF?

HackRF provides two TX gain controls are LNA (I) (0 to 47 dB in 1 dB steps) and RF AMP (0 or 14 dB)

Use of HackRF

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.Note there are no Filters in the HackRF to limit spurious transmissions and this must be provided by external circuitry.

WARNING

Before you transmit, know your laws. HackRF One has not been tested for compliance with regulations governing transmission of radio signals. You are responsible for using your HackRF One legally.

ADS-B(S)

WARNING

- This application is intended solely for **experimental** purposes. It should not be used for **any other reason**.
- It is your responsibility to adhere to all local, state, national, and international laws while conducting **experiments** with this application. Any illegal activities are strictly prohibited.
- This application is not designed for use by individuals under the age of 18. By conducting an **experiment** with this application, you confirm that you are of legal age in your jurisdiction.
- All **experiments** conducted using this application are done at your own risk. We are not liable for any damages or losses that may occur as a result of your use.
- We do not and had never provide(d) any form of assistance or support for your **experiments**. You are solely responsible for any outcomes or consequences that may arise.
- By using this application, you agree to indemnify and hold harmless the developers and all associated parties from any and all claims, damages, losses, liabilities, costs, and expenses (including legal fees) arising out of your use of this application or your violation of these terms.
- This application is provided "as is" without warranty of any kind, either express or implied, including, but not limited to, the warranties of any case.
- We reserve the right to modify these terms and conditions at any time without prior notice. Your continued use of this application following any changes signifies your acceptance of our updated terms.

This is a potentially dangerous App. The HackRF could be used to generate valid ADS-B messages and if these are radiated then it could effect both how aircraft and navigation systems see each other. Therefore, it should only be used in a closed RF environment or when there is no direct transmission.

The Key Items on the App that can be selected with the cursor and changed with the encoder knob are:

- **Title bar:** The usual Items may be changed and displayed.
- **Tab pages:** The Tab pages for the settings that are can be selected are **Position, Callsign, Speed, Squawk**. This data is not held in persistent memory except for the frequency.

Position Tab

ICAO24: This code is selected with rotary encoder to enter the 6 digit numeric number. This is sometimes called the Mode S code and is a 24-bit unique number that is assigned to each vehicle or object that can transmit ADS-B messages. It is usually transmitted by aircraft but some airport ground vehicles and multi-lateration towers also have ICAO24 codes assigned to them. Transmit position: this is a tick box to enable the transmission of Alt. Lat. Lon

- **Alt:** Sets height in feet.
- **Lat:** Setting of Latitude is in Degrees Minutes and Second and set with encoder knob. The numeric value is given to the right hand side
- **Lon:** Setting of Longitude is in Degrees Minutes and Second and set with encoder knob. The numeric value is given to the righthand side.
- **Set from Map:** the Lat and long can be set form the map view and using the touch screen if desired. Note to save the value is a “OK” button but this is hidden behind the Digital values of the Lat and Lon. But if you touch this, are it will appear.

Callsign Tab

- **Transmit callsign:** This is a tick box to turn on the transmission of the Callsign. The callsign is entered in the text pad and is 8 characters long.

Speed Tab

- **Transmit speed:** This is a tick box to turn on the transmission of the speed.
- **Speed:** The value is selected and the rotary encoder is used to select the value 0-999kn, unit: knots.
- **Bearing:** The value is selected and the rotary encoder is used to select the value 0-359 Degrees. (to be more friendly user, the input bearing angle direction is also displayed in the top right Compas circle UI)
- **Vertical Rate:** The value is selected and the rotary encoder is used to select the value -4096 to +4096 ft/min in steps of 64 (following the encoding standard). It indicates the vertical rate speed of the plane (+) climbing , (-) descending. In real plane ,that Vr source data information can come from GNSS or Barometric altitude equipment. In mayhem fw , we are simulating a fix source from GNSS. Example about climb vert. rate (+) : The Cessna 172 is a four-seat aircraft. At maximum weight it has a VY of 75 kn (139 km/h) indicated airspeed[4] providing a rate of climb of 721 ft/min (3.66 m/s)). Example about descend vert. rate (-): The profile varies from airport to airport, but generally, around five miles from the runway, the airplane is at landing speed, with slats/flaps in the landing position, vertical descent speed less than 1,000 feet per minute and the engines powered up properly.

Squawk Tab

- **Transmit squawk:** This is a tick box to turn on the transmission of the Squawk code.
- **Squawk:** A discrete transponder code (often called a squawk code), can be selected with rotary encoder and has specific meanings. The system identifies an aircraft through a four-digit octal number. (each digit number from 0-7), which provides up to 4.096 possilbe codes. The squawk code range is from 0-7777.
  Squawk codes are usually random, but there are a handful of specialized squawk codes that are reserved for unique or specialized situations or aircraft.
  https://en.wikipedia.org/wiki/List_of_transponder_codes

Some public pilot user interface equipment examples (from Wikipedia),

Common to all Tabs

- **Frequency:** At the lower part of the App is the Frequency setting. This is stored in persistent memory
- **Step size:** This is next to the frequency and allows the selection of the standard step sizes.
- **Gain:** The gain setting are below the frequency and marked (0-47) LNA(IF) and AMP 0=0db or 1=14dB.
- **Start:** This button starts the transmission and if pressed again can stop the transmission.

APRS

[Automatic Packet Reporting System] The APRS TX App sends messages on the selected frequency. The App allows the configuration of the APRS Stream. The App is marked as Beta, but it does send decodable messages in AFSK in the right AX.25 format.

The App has settings for:

- "Source:" Address is typically the transmitting Callsign. The field is selected by moving the cursor to the right side of the Label using the arrow buttons, and selecting each alphanumeric character needed then stepping the cursor on to the next position until all 6 fields are completed. Then step on to "SSID:" and select the numeric number 0-15. The most common SSID value for the PortaPack is 0.
- Destination Address "Dest.:" is typically the receiving Callsign. The field is selected by moving the cursor to the right side of the Label using the arrow buttons, and selecting each alphanumeric character needed then stepping the cursor on to the next position until all 6 fields are completed. Then step on to "SSID:" and select the numeric number 0-15. When testing, 0 is the best choice.
- The message content can be added in the "Info field:" by selecting the "Set" Button. A maximum of 30 characters can be added, but not the typical maximum of 67 or 256.

At the bottom of the App Screen, you will find:

- Select the Primary Frequency by cursor for TX from the on-screen keypad. In general, Region 1 (Europe and Africa) is 144.800, Region 2 (Americas) is 144.390, and Eastern Asia is 144.640. Other areas vary.
- Select the Frequency Step size by cursor, then use rotary selection e.g 12k5
- Select the Deviation by cursor, then use rotary selection e.g. 5kHz
- The Gain IF setting is a range of 0-47, and Amp is either 0dB or 14dB (on or off). Note that the color of the gain setting changes color based on the TX total output power setting. It is a combined total of IF and AMP: 0-17 Green, 18-38 Yellow, 39-47 Orange, and 48-61 Red.

The transmission is triggered by the "Start" Button and stops after the end of the message sequence.

A great way to test transmission is by running another local SDR receiver set to your PortaPack frequency and observing the results on the spectrum display. I used an RTL-SDR device with the software SDR++ piped into the software QTMM AFSK1200 Decoder, both of which are free software.

Some example message formats are as follows. Many more are in the APRS Protocol Reference Manual.

• Position Lat/Long: nnnn.nnA/nnnn.nnB/ > Example: New York City, USA could be: 4071.27N/7400.59W/Hello from NYC

• Altitude can be expressed in the message by adding /A=1234 > Example: Example: New York City, USA at 105 ft above sea level could be: 4071.27N/7400.59W/Hello from NYC /A=105

• Local Date and Time (MDHM): @nnnnnnnn/ where the first two numbers are the Month, the next two numbers are the Day, the next two numbers are the Hours, and the last two numbers are the Minutes (in 24-hour format). > Example: April the 18th at 16:54 in the afternoon could be: @04181654/Happy World Ham Day

• Zulu/UTC Date and Time (MDHM): /nnnnnnnnz/ where the first two numbers are the Month, the next two numbers are the Day, the next two numbers are the Hour, and the last two numbers are the Minutes (in 24-hour format). > Example: April the 18th at 16:54 in the afternoon UTC could be: /04181654z/Happy World Ham Day

• Putting it all together: New York City, USA on April 18th at 16:54 local time at 105 feet above sea level and a message could be: > @04181654/4071.27N/7400.59W/Happy World Ham Day /A=105

BHT Xy/EP

This is an App (in French) allows some control over street lights. The system is manufacture by BH-Technologies for many French municipalities. It provides a system to turn on/off streetlights via a radio signal in the 31~32MHz, only works in France. Some information on BHT system is available on their publicly available commercial brochures here.

Xy/EP is a Remote streetlight management protocol only seen in some European cities.

BLE TX

Main Menu:

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.

1. Single transmit mode. (This mode transmits a single BLE packet OTA given the file parameters.)
2. 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.

1. 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.
2. The **Channel** setting allows you to select which channel to transmit on.
3. The **Advertisement PDU Type** setting allows you to select between various types of advertisement types.
4. The **Random** toggle allows you to randomize the MAC Address that you send out with each packet.
5. The **Save Packet** saves to file the current packet list in TX format to the name you specify.
6. 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.

Example of file:

Below is an example of how the text file show be formatted in order for it to be correctly parsed by the application. To get this transmission to show up on a BLE Scanner app set the toggle to ADV_NONCONNECT

010203040506 190953445220426c7565746f6f7468204c6f7720456e65726779 1000

010203040506 (MAC Address you want to be transmitted. Must be exactly 12 characters)

190953445220426c7565746f6f7468204c6f7720456e65726779 (Packet Data you want to be transmitted. Must be less than 62 characters, 31 byte max advertisement length per BLE spec.) In this case we are transmitting a packet with data: **SDR Bluetooth Low Energy**

1000 (Number of times you want the packet to be repeated.)

Its important to note all parameters must be delimited by a single space.

Note: Each line must follow this format for each packet.

010203040506 190953445220426c7565746f6f7468204c6f7720456e65726779 500 010203040507 190953445220426c7565746f6f7468204c6f7720456e65726779 500

References:

BLE Rx App: https://github.com/portapack-mayhem/mayhem-firmware/wiki/Bluetooth-Low-Energy-Receiver

Advertisement PDU Types: https://novelbits.io/bluetooth-low-energy-advertisements-part-1/

Burger Pager

Burger Pager app.

Is used to page / trigger restaurant pagers. The devices work at the 467.750 Mhz. range.

More info on it look at tiger tony's site : https://hackaday.com/2019/06/04/your-table-is-ready-courtesy-of-hackrf/

GPS Sim

WARNING

- This application is intended solely for **experimental** purposes. It should not be used for **any other reason**.
- It is your responsibility to adhere to all local, state, national, and international laws while conducting **experiments** with this application. Any illegal activities are strictly prohibited.
- This application is not designed for use by individuals under the age of 18. By conducting an **experiment** with this application, you confirm that you are of legal age in your jurisdiction.
- All **experiments** conducted using this application are done at your own risk. We are not liable for any damages or losses that may occur as a result of your use.
- We do not and had never provide(d) any form of assistance or support for your **experiments**. You are solely responsible for any outcomes or consequences that may arise.
- By using this application, you agree to indemnify and hold harmless the developers and all associated parties from any and all claims, damages, losses, liabilities, costs, and expenses (including legal fees) arising out of your use of this application or your violation of these terms.
- This application is provided "as is" without warranty of any kind, either express or implied, including, but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement.
- We reserve the right to modify these terms and conditions at any time without prior notice. Your continued use of this application following any changes signifies your acceptance of our updated terms.

This app allows you to broadcast GPS baseband signal data streams.

Generator

You can use gps-sdr-sim to generate data for this app.

`gps-sdr-sim -e RINEX_NAVIGATION_FILE -l LAT,LONG,HEIGHT -b 8 -o SOMENAME.C8`

That will create `SOMENAME.C8`, but note that you also need to specify its sample rate and frequency in another file, as explained below.

RINEX navigation file for GPS ephemerides

Download the latest file for this parameter directly from Nasa: https://cddis.nasa.gov/archive/gnss/data/daily/

Sample rate and frequency specification

Create `SOMENAME.TXT` with:

```
sample_rate=SAMPLE_RATE
center_frequency=1575420000
```

Known working values for the `SAMPLE_RATE`:

- 2600000
- 2500000
- 1250000

This file should use the same filename as the .C8 file but with .TXT extension. It contains the sample rate and center frequency for the .C8 file. Copy the files to your PortaPack MicroSD and open the .C8 file in the GPS Sim app.

Example 1

Create a rather small polygon with a path in KML format (i.e. a path you might want to simulate to walk). You can use Google Earth or another solution like https://www.doogal.co.uk/polylines.php. Load that file in the free SatGen NMEA simulator. In the generator, change the frequency to 10 Hz and export the NMEA.

`gps-sdr-sim.exe -e brdc1180.20n -g NMEA.txt -b 8 -o TESTGPS.C8`

You also need to create `TESTGPS.TXT` as specified above.

Example 2

For a fixed position, use `gps-sdr-sim -e brdc1500.20n -s 1250000 -b 8 -o gpssim.C8 -l 30.286502,120.032669,100 -d 100`

Test with a `gpssim.txt` as follows:

```
sample_rate=1250000
center_frequency=1575420000
```

Example 3

> **NOTE:** The website nmeagen may add timestamps to the output. That might be problematic for the simulation

We can create a realistic movement using a NMEA GGA stream generator like https://nmeagen.org/. In this website create several multi point lines with the positions you want. Download the NMEA file clicking "Generate NMEA file".

```
gps-sdr-sim.exe -e brdc3540.14n -g OUTPUT.nmea -b 8 -d DURATION -o MYGPSWALK.C8
```

You also need to create `MYGPSWALK.TXT` as specified above.

Compatibility

Depending on several factors, results may vary. A modern device will use several sources and methods to validate the current position, so spoofing positions may not be possible in all situations. To improve your chances to receive simulated GPS data, try:

- Turn off Wifi/BT/Cellular and positioning-enhancements (best airplane mode)
- Go inside, where the device loses GPS signal
- Reboot the device after doing the previous two steps

If the device runs Android, follow your attempts with GPS Test.

Some known results

> ⓘ Note
> This table contains only few examples, since newer phones use many ways to ensure the position is accurate, becomes harder to spoof GPS

Type	Make	Model	Locks on spoofed GPS?	GPS acts "jammed"?	Comments
Tablet	Samsung	Note 7	No	Yes	
Phone	Samsung	S8	**Yes**	No	WIFI must be off
Phone	Huawei	P30 lite	No	Yes	
Phone	Huawei	Mate 10 Pro	No	NO	6 or 7 satelites: No fix
Smartwatch	Huawei	Amazfit Bip	**Yes**	No	
Phone	Apple	iPhone 6	**Yes**	No	Works with WIFI on
Phone	ZTE	Axon 7	**Yes**	No	Works with WIFI on
Phone	Xiaomi	Mi5	**Yes**	No	Works with WIFI on
Phone	Samsung	S20+ 4G	**Yes**	No	WIFI must be off
Smartwatch	Samsung	Gear S3 WiFi	**Yes**	No	Location over GPS only
Phone	OnePlus	7 Pro	No	No	Doesn't seem to do anything
Phone	Samsung	S21 Ultra	**Yes**	No	
Tablet	Apple	S21 Ultra	No	No	Doesn't seem to do anything
Laptop	Apple	MacBookPro M1	No	No	Doesn't seem to do anything

Jammer

WARNING

- This application is intended solely for **experimental** purposes. It should not be used for **any other reason**.
- It is your responsibility to adhere to all local, state, national, and international laws while conducting **experiments** with this application. Any illegal activities are strictly prohibited.
- This application is not designed for use by individuals under the age of 18. By conducting an **experiment** with this application, you confirm that you are of legal age in your jurisdiction.
- All **experiments** conducted using this application are done at your own risk. We are not liable for any damages or losses that may occur as a result of your use.
- We do not and had never provide(d) any form of assistance or support for your **experiments**. You are solely responsible for any outcomes or consequences that may arise.
- By using this application, you agree to indemnify and hold harmless the developers and all associated parties from any and all claims, damages, losses, liabilities, costs, and expenses (including legal fees) arising out of your use of this application or your violation of these terms.
- This application is provided "as is" without warranty of any kind, either express or implied, including, but not limited to, the warranties of any case.
- We reserve the right to modify these terms and conditions at any time without prior notice. Your continued use of this application following any changes signifies your acceptance of our updated terms.

About

The App can transmit various forms of noise to cause a denial of service in radio devices. This includes cell phones, cordless phones, Wi-Fi, remote controls, and other devices. A number of people have tested the jamming capability and found it to work though very dependent on the configuration the interference source, and the power of the signal. The jamming range of the system due to the low transmit power will be in the range of a few meters. Good antennas and power amplifiers can increase the strength of the jamming signal.

The App has three tabs for Range 1, Range 2, Range 3. These can be separately enabled and work in a sequential way moving from range 1,2,3. This will limit the scan time in each range and of the interfering signal that is generated. The total for the interference range is a maximum limit of 24Mhz. The movement of the jamming signal across the band is carried out in 1MHz chunks (Hops) and the hop time is set to move to the next band segment in sequential order.

The output power of the Jammer is set at the maximum level posible, typicall 5-10dBm.

Settings

The items described below are applicable to each of the 3 Range Tabs. Key Items on each of the Range App tabs, that can be selected with the cursor and changed with the encoder knob are:

- **Title bar:** The usual items may be changed and displayed.
- **Enable range:** This tick box enables this range.
- **Load Range:** This brings up the frequency ranges stored in FREQMAN directory in the SD card. Each category can be selected and then the individual ranges selected. It is good to select ranges with in the Jammer category and that you make sure they are less than 24MHz for the start to end range.
- **Start:** This sets the start range. It can be manually completed or loaded as part of the load range.
- **Centre:** This sets the center of the range. It can be manually completed or loaded as part of the load range.
- **Stop:** This sets the stop range. It can be manually completed or loaded as part of the load range
- **Range:** This sets the range (Max 24MHz).It can be manually completed or loaded as part of the load range
- **Type:** This is the type of jamming signal of: Random CW, SW sweep, FM tone, Random FSK.
- **Speed:** This is the speed that the jamming signal is moved across the hop segment selected.
- **Hop:** This is the hopping interval between the 1MHz segment that the jamming signal is transmitting. There are 6 values from 10ms to 10s. The information next to Type: (see above) e.g. 1/ 4 indicates that is the jamming signal is in the first 1MHz Hop; there are 4 Hops. If the frequency is a fraction of a Hop then it will generate the jamming signal in that Hop for the same time as other Hops
- **TX:** The Time the Jammer App is Transmitting

- **Sle3p:** The sleep time between Transmission.
- **Jitter:** This setting alters the deviation from true periodicity of the signal and is used to increase the spectral density of the jamming signal. It can be set between 1 and 60.
- **Start:** This enables the start of the jamming signal an after the TX time, it will pause for the Sleep time, and then restart. If the button is pressed it will stop the transmission.

USE

The jamming effect is very dependent on the configuration of the above settings. It is recommended that you start with a small frequency range; if possible. But lets take Wi-Fi in the 2.4GHz range channels 1, 6, or 11. As an example, we can generate more than 24Mhz wide of the start frequency of 2.400GHz start to 2.424GHz. We can set:

- Type: Rand CW,
- Speed: 10Hz,
- Hop 10ms,
- TX: 10Secs,
- Sle3p: 2Secs
- Jitter: 20/60.

This signal, unless it is very close to the device, will not jam the target signals even though the average power across the band is +7dBm. If the target is in a narrower frequency range, then it has a greater affect, in terms of jamming due to the increase of Spectral density of the jamming signal.

LGE Tool

This Tool was ported from https://github.com/furrtek/portapack-havoc. Furrtek stated in 17 Apr 2020,that the tool was used to mess around with a particular French brand of laser tag equipment. This tool's name and this last sentence contains enough search terms :). The brand isn't clearly specified because it's a trade mark.

Morse

The Morse App sends Morse coded message either in CW or FM. There are some pre-configured foxhunt messages , but these are not useful as in most countries a callsign must be part of the message, or sent at regular intervals.

The Key Items on the App that can be selected with the cursor and changed with the encoder knob are:

- **Title bar:** The usual Items may be changed and displayed.
- **Foxhunt:** This tick box enables the pre-set messages strings (11 of them) that are selected on the same line such as “3 (MOS)”.
- **Speed:** Select the speed of transmission in Words Per Minute. (10-45). Note the label should be “wpm” not “wps”, this is a bug.
- **Tone:** This sets the tone for the FM transmission (0-9999).
- **Modulation:** This is set to CW or FM.
- **Loop:** this set the looping of the message and has a value of “Off” or 6 time settings from 5 Second to 5 Minutes.
- **Set message:** When selected, this brings up the a text keypad and enables the construction of a message.
- **Frequency:** At the lower part of the App is the Frequency setting. This is stored in persistent memory.
- **Step size:** This is next to the frequency and allows the selection of the standard step sizes.
- **Deviation:** This is located next to the Step size and allows the setting of deviation from 1 kHz to 150kHz.
- **Gain:** The gain setting are below the frequency and marked (0-47) LNA(IF) and AMP 0=0db or 1=14dB.
- **Transmission Progress bar:** This bar indicated the progress of the transmission. Above it is shown the transmission time based on the message length.
- **Start:** This button starts the transmission and if pressed again can stop the transmission.

Important note

Due to the way it is designed, the first 2 characters are somewhat not sent. If you encounter the problem, try prefixing your message with two characters, like 'E' and space. Example: "E MyMessageStartsHere" (see issue !303 if you think you can help)

OOK

WARNING

- This application is intended solely for **experimental** purposes. It should not be used for **any other reason**.
- It is your responsibility to adhere to all local, state, national, and international laws while conducting **experiments** with this application. Any illegal activities are strictly prohibited.
- This application is not designed for use by individuals under the age of 18. By conducting an **experiment** with this application, you confirm that you are of legal age in your jurisdiction.
- All **experiments** conducted using this application are done at your own risk. We are not liable for any damages or losses that may occur as a result of your use.
- We do not and had never provide(d) any form of assistance or support for your **experiments**. You are solely responsible for any outcomes or consequences that may arise.
- By using this application, you agree to indemnify and hold harmless the developers and all associated parties from any and all claims, damages, losses, liabilities, costs, and expenses (including legal fees) arising out of your use of this application or your violation of these terms.
- This application is provided "as is" without warranty of any kind, either express or implied, including, but not limited to, the warranties of any case.
- We reserve the right to modify these terms and conditions at any time without prior notice. Your continued use of this application following any changes signifies your acceptance of our updated terms.

On–off keying (OOK) denotes the simplest form of amplitude-shift keying (ASK) modulation that represents digital data as the presence or absence of a carrier wave. OOK system often have a coding sequence. OOK is often used in remote garage and gate keys, often operating at 315 MHz or 433.92 MHz. Most modern systems though use a rolling code system to prevent Replay attacks.

The App has a number of Pre-configured Device types such as 2260,2262,16 Bit, 1527, 526E, T12E, 5026, UM3750, BA5104,145026, HT6***, TC9148.

There are 2 Tabs. Key Items on each of the App tabs, that can be selected with the cursor and changed with the encoder knob are:

Common to all TABs

- **Title bar:** The usual items may be changed and displayed.
- **Frequency:** At the lower part of the App is the Frequency setting. This is stored in persistent memory
- **Step size:** This is next to the frequency and allows the selection of the standard step sizes.
- **Gain:** The gain setting are below the frequency and marked (0-47) LNA(IF) and AMP 0=0db or 1=14dB.
- **Start:** This button starts the transmission and if pressed again can stop the transmission.

Config Tab

- **Type:** This is the selection of a pre-Configured Encoder/ decoder chip Type.
- **Clk:** Selects the frequency of the OOK switching rate. This is interlinked to the frame rate for example 1kHz clock is 36000 10^6 s frame rate. Range of clock is 1-500KHz.

- **Frame:** This can be selected but as stated above sets the clock and frame rate. The settings go from 30 10^6s to 36000 10^6s.
- **Symbols:** This is the pattern of the symbol message sent. The 0/1 can be change to alter the OOK pattern. Note the pattern is made up as shown in the letters line of A for Address, D for DATA, S for Sync .
- **Waveform:** This shows the diagrammatic view of the waveform sent.
- **Progress Bar:** When the transmission is started it shows the progress of the transmission while sending. Not many of the transmission are very short and looks like they are not sent.

Scan Tab

This is not implemented.

POCSAG

POCSAG is a pager protocol used commercially and by Amateur Radio. Amateur Radio DAPNET alphanumeric POCSAG is transmitted on UHF Narrow FM 439.9875 MHz at 1200 baud. See the DAPNET wiki for more info: hampager.de/dokuwiki/doku.php

RDS

"RDS" stands for "Radio Data System" and it allows FM broadcasters to send far more than just an analogue audio signal out over the air waves. Using a 57 kHz "subcarrier," stations can transmit digital RDS data for reception by RDS-equipped FM tuners. This technology opens up a whole new range of features help to the listener with RDS reception capability. Typical information can you expect depends on what the broadcaster transmits and what your device can pick up. There are two categories, Static and Dynamic.

A full description of the system is here.

RDS "Static" services include:

Program Service Name (PS): This is a displays a name instead of frequency. Program Type Code (PTY): This identifies a particular type of broadcast (Rock, Jazz, Sports, Talk, News, Classical, etc.) So far, 24 categories have been defined and assigned in the RDS system. Program Identification Codes (PI): Is a four-digit hexadecimal code. It is allocated on a country basis and usually made up of a Country Identifier followed by 3 ID unique characters. This is one of the rarely-seen "hidden" RDS features . Alternate Frequency (AF): If PI is one of RDS' "back office" functions, AF is what you'll see in action all the time. Alternate Frequency Switching (AF) automatically returns your FM tuner to the strongest signal carrying that program. Traffic Program (TP): This symbol alerts you to the fact that the station you're listening too regularly broadcasts special traffic information. Think of TP as the "indicator " for Traffic Announcement (TA).

RDS "Dynamic" services:

Traffic Announcement (TA): This is the active side of TP capability. This guarantees up-to-the-minute information sent to the driver. Radio Text (RT): This feature allows a broadcaster to send up to a 64-character message that could scroll across your radio's display, things like sports scores, song titles, artist or album names, even advertisements. Clock Time (CT): An RDS-equipped station broadcasts a time and date synch signal once a minute. Emergency Alert System (EAS): PTY code # 31 If your RDS tuner senses an emergency code, it will flash an ALERT message.

The Function in RDS App

The RDS App has 4 Tabs: Name: Text: Time: Audio:. In the Current App V 1.4.3 only Name: and Text: are implemented. Key Items on each of the App tabs, that can be selected with the cursor and changed with the encoder knob are:

Common to all TAB

- **Title bar:** The usual items may be changed and displayed.
- **Program Type:** There are 31 pre-set Program types.
- **Program ID:** The Program ID is 4-character Hex from 0000 to FFFF.
- **TP:** This tick box select the sending of a Traffic Program Symbol.

At the Bottom of the App Page are settings related to the RF configuration these being:

- **Frequency:** At the lower part of the App is the Frequency setting. This is stored in persistent memory.
- **Step size:** This is next to the frequency, it allows the selection of the standard step sizes.
- **Gain:** The gain setting are below the frequency and marked (0-47) LNA(IF) and AMP 0=0db or 1=14dB.
- **Start:** This button starts the transmission, and if pressed again, can stop the transmission.

Name Tab

- **Transmit PSN:** The program service name can be sent if the tick Box is selected.
- **PSN:** This is the Program Service Name. This is added by selecting the Set Button. This brings up the text Keypad so the name can be entered. (maximum limit of 8 characters)
- **Stereo:** A tick box to select this function. (Not known if this works).
- **Music:** A tick box to select this function. (Not known if this works).
- **Traffic Announcement:** A tick box to select this function. (Not known if this works).

Text Tab

- **Transmit Radiotext:** This tick box enables the sending of Radio text.
- **Set:** The Set button brings up the Text Keypad and allows text to be entered up to 28 characters.

Time Tab

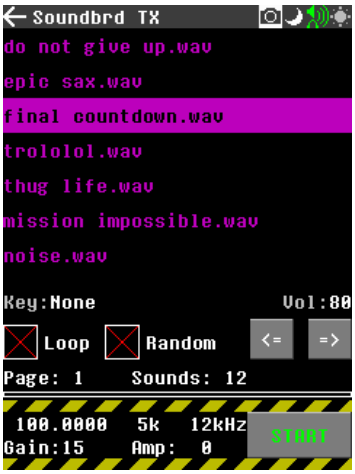
- **Transmit Date & Time:** This is a tick box to enable, but the page states that it is "Not yet Implemented".

Audio Tab

- **Transmit Audio:** This is a tick box to enable, but the page states that it is "Not yet Implemented".

Soundboard

The soundboard app will play and transmit whatever sound file in the WAV directory of the SD card is selected when the START button is hit, or it will play a random file if the "Random" box is checked. Sound is transmitted as FM with the bandwidth set in the black and yellow TX box.



'Key' allows the transmitted carrier to be encoded with a CTCSS subaudiable tone, or a pilot tone for compatibility with various cordless mic systems listed below. Note that audio output to the speaker is disabled if tone key is enabled.

- Axient 28kHz
- Sennheiser 32.768kHz
- Sennheiser 32.000kHz
- Sony 32.382kHz
- Shure 19kHz

Sounds should be 8-bit unsigned or 16-bit signed mono .wav files between 24000 and 48000 Hz. This can be done in Audacity by first making sure the track is Mono by going to Tracks>Mix>Mix Stereo Down to Mono and then choose "Other Uncompressed Files" in the export dialog and set Header to "WAV (Microsoft)" and Encoding to "Unsigned 8-bit PCM".

The bandwidth setting should be the sample rate in which the wav file was recorded. The provides sample wav files are sampled at 48000 Hz (48kHz). If you record your own wav source and it is sampled at a different rate, this setting should be changed to match the source sample rate.

The frequency step setting is used in tuning through the possible frequencies of a given band. In the AM band, stations have a maximum bandwidth of 10kHz, with 5kHz above and below the frequency.

Spectrum Painter

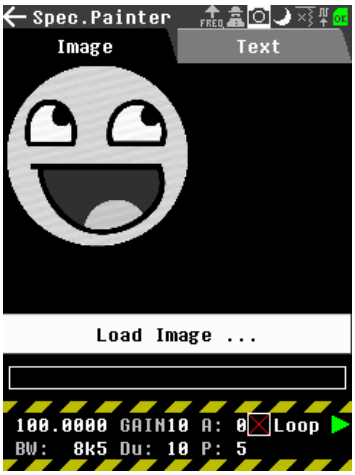
The Spectrum Painter app allows to "paint" an image or text in a way that it appears on the waterfall view.

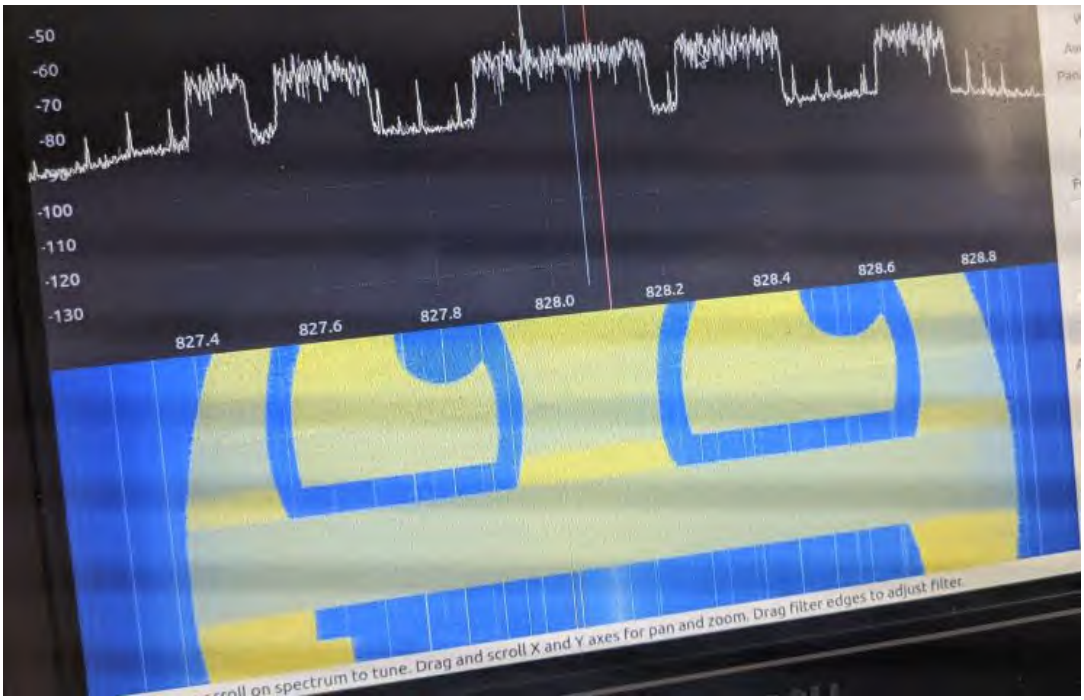
Options

- Center frequency
- VGA (Gain)
- Amplifier
- Loop
- Bandwidth
  - Note that the default bandwidth of 8k5 Hz is too low in most cases (eg. when viewing multiple MHz).
- Duration of transmission
- Pause between transmissions when loop is active

Images

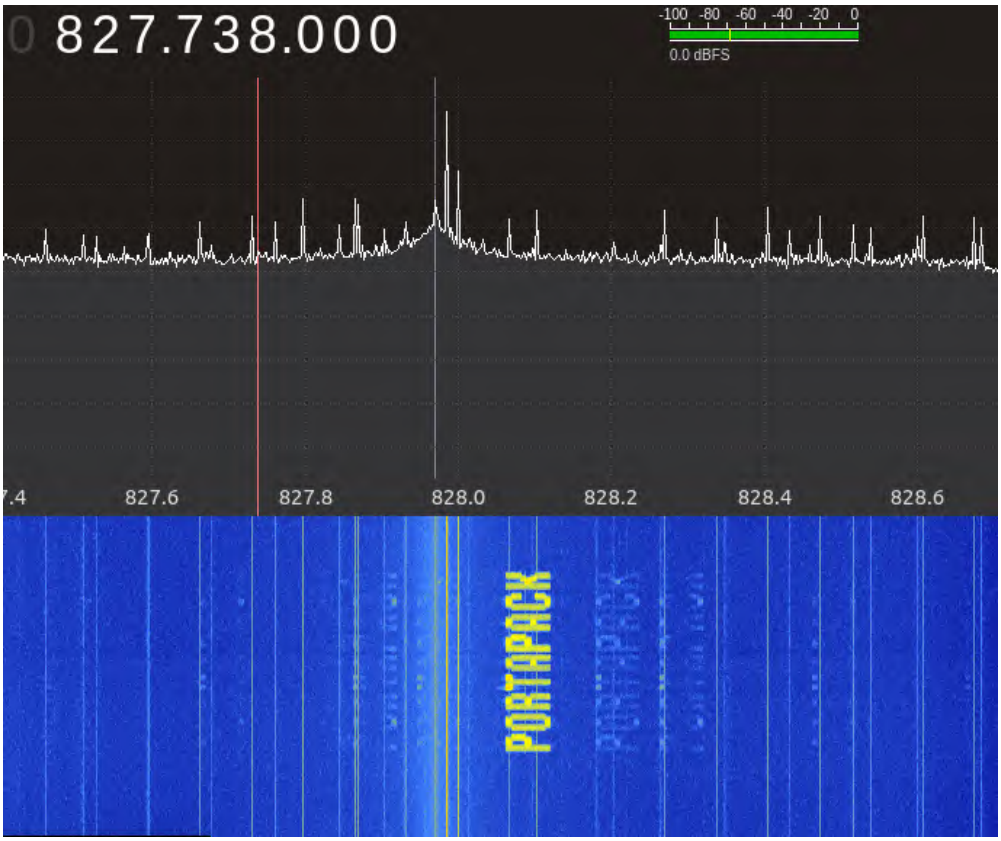
- Place 24 bit .BMP files on the sd card in the folder SPECTRUM
  - 16 and 32 bit .BMP should work as well, but are not testet.
- The resolution should be quite high for a good result. A width of 2048 pixels is not a problem.
  - Use a power of 2 for the width for optimal result. (eg. 512 / 1024 / 2048 / ...)





Text

- Messages up to 300 characters are supported



SSTV

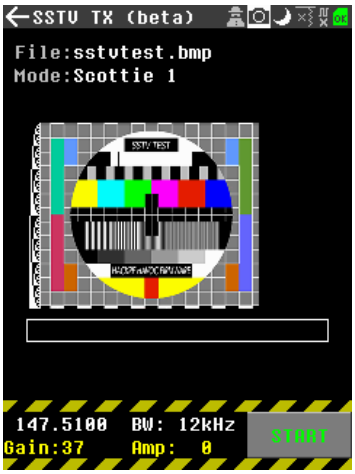
The SSTV app allows you to send .bmp images that you have loaded onto the SD card. The current supported modes include Scottie 1, Scottie 2, Scottie DX, Martian 1, Martian 2, and SC2-180 modes. Currently, FM is the only modulation supported.

Sending

To send an image, select the bitmap image, the mode, and the frequency you'd like to transmit on ,using the jog wheel (knob). For amateur radio, 12kHz seems to produce a good image.

Image requirements

Only 24bit BMP files with a size of 320x256 pixels are supported



TEDI/LCR

LCR Langage de Commande Routier in english means Road Command Language and is a frame generator & transmitter that is used for dynamic road equipment and their computer systems.It is used in the regulation and monitoring of traffic and its environment: PMV , video cameras , tunnel management, emergency telephone and radio network (RAU and BAU), video switching matrices, weather stations, retention basins, electrical distribution, etc. It is basically a Bell202 transmitter with special string formatting.

TouchTunes

About

TouchTunes is a popular Jukebox company that can be found in various bars, pubs, and restaurants all over North America.

TouchTunes Jukebox's (Gen2 and above) use a wireless remote that transmits NEC encoded messages using ASK/OOK at 433.92MHz. These remotes are used for basic Jukebox functions such as On/Off, Skip Song, Volume, Etc. The wireless messages are addressed using PINs 000-255 to prevent mutable units from interfering with each other.

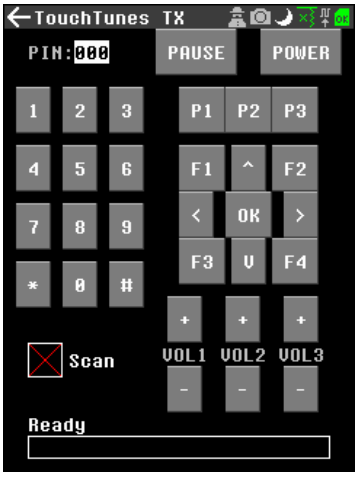
Most of the time the remote's PIN is left as default 000

This application emulates TouchTunes wireless remotes (Gen2 and newer) and has the ability to brute force addresses.

Original research can be found HERE and on NotPike's blog.

How To Use

- **Start the application:** Go to Transmit→TouchTune.



- **Transmit a command:** Simply press the button on the touch screen or highlight/select the button with the physical controls.
- **Change the PIN:** Highlight the 3 digits in the top left hand corner and use the jog wheel to change the value. (Default is 000)
- **Brute force a command:** Select the "Scan" option (green check mark) then transmit. This option will transmit the command 256 times starting with PIN 000 to 255. (PIN will change to 255 after all commands are transmitted)
- **EW Mode (Experimental):** EW (Electronic Warfare) Mode will prevent others from sending commands to your target jukebox while still allowing you to have control. When the "EW Mode" is selected (green check mark), a continuous CW at 433.92MHz will be transmitted in an attempt to jam the jukebox's receiver. You can still transmit commands while "EW Mode" is active. The jamming signal will automatically turn off / turn on when you transmit commands.

TouchTunes Message Structure

Below is all the technical data regarding the wireless message structure.

Basic Info

- **Frequency:** 433.92MHz
- **Modulation:** ASK/OOK
- **Protocol:** NEC
- **Symbol Rate:** 1766
- **Symbol Period:** 566us

NEC Format

- **Short(0):** 10 (OOK: ON OFF)
- **Long (1):** 1000 (OOK: ON OFF OFF OFF)

Message Structure

- **Structure:** {PREAMBLE} {SYNC} {PIN} {COMMAND} {TAIL}
- **Preamble (Literal Symbols):** 0xFFFF00
- **Sync (Decoded NEC):** 0x5D
- **PIN 000-255 (Decoded NEC):** 0x00-0xFF (LSB)
- **Tail (Literal Symbols):** 0x8

Commands (Pre NEC Encode)

Note: Commands are doubled with the 2nd half being reversed. For example, Pause 0x32 will translate to 0x3223 before being encoded to the literal symbols 0xA88A8AA2A880.

- 0x32: Pause
- 0x78: On/Off
- 0x70: P1
- 0x60: P2 Edit Queue
- 0x20: F1 Restart
- 0xF2: Up
- 0xA0: F2 Key
- 0x84: Left
- 0x44: OK
- 0xC4: Right
- 0x30: F3 Mic A Mute
- 0x80: Down
- 0xB0: F4 Mic B Mute
- 0xF0: 1
- 0x08: 2
- 0x88: 3
- 0x48: 4
- 0xC8: 5
- 0x28: 6
- 0xA8: 7
- 0x68: 8
- 0xE8: 9

- 0x18: * Music_Karaoke
- 0x98: 0
- 0x58: # Lock_Queue
- 0xD0: Zone 1 Vol+
- 0x90: Zone 2 Vol+
- 0xC0: Zone 3 Vol+
- 0x50: Zone 1 Vol-
- 0x10: Zone 2 Vol-
- 0x40: Zone 3 Vol-

Example

- **Command:** Pin 000 - On/Off
- **Literal Symbols (HEX):** ffff00 a2888a2 aaaa 8888aa2aa2220 (PREAMBLE SYNC PIN COMMAND TAIL)
- **Literal Symbols (BIN):** 11111111111111110000 10 1000 10 1000 1000 1000 10 1000 10 10 10 10 10 10 10 10 1000 1000 1000 1000 10 10 10 1000 10 10 10 10 1000 1000 1000 100000

BLESpam

With this app you can spam various BLE packets. You can choose from the above list:

- **Android**: this creates a FastPair attack that pop ups around 10 devices with a 15 min cooldown on all nearby (and supported) Android phones.
- **iOS**: same as above, but for iOS, and the limits are depends on the version of the iOS.
- **iOS crash**: can pop up nearby device dialogs, and after around a minute the UNPATCHED iOS devices will crash. Power cycle will recover it.
- **Windows**: same as the Android version, but for Windows. Limits are unknown, based on patch levels. Needs a supported and enabled HW.
- **Samsung**: same as the Android but for Samsung specific "EasySetup" protocol.
- **NameSpam**: just shows a lot of pre defined names in the BT device list.
- **NameRandom**: shows a lot of BT devices on the list, with names crafted from random characters.
- **All-safe**: shuffles the attack types except iOs crash.
- **All**: shuffles all the attack types. NOTE : A lot of this attack don't work today (patched)

There is a check box: **Rnd devices**. For some attacks it is better to turn it off, and for some it is better to keep it on. Check it against your target device. It randomizes the MAC of the emulated BLE device if turned on.

There is a console that shows some of the sent packets (rate limited), so you can learn what is happening.

> Important
>
> As as with other TX applications, it is important that, use them carefully. Avoid interfering with anything or causing harm to others. Be responsible and follow all regulations and laws.

Capture

Capture App is designed to capture I/Q data to a file on the SD card. Captured data is stored as pairs of 16-bit signed values in a .C16 file (complex 16 bit), or optionally 8-bit signed values in a .C8 file (complex 8 bit). C16 values are stored in little-endian format. The Metadata (“Center frequency” and Bandwidth) is stored in a .TXT file with the same name.In GRC, the "file source" and "ishort to complex" blocks can be used to process the data.

The Sampling rate used may not be supported by some MicroSD cards, it is best to use high speed class SD cards. The HackRF PortaPack Capture/Replay functionality is based on Havoc firmware version.

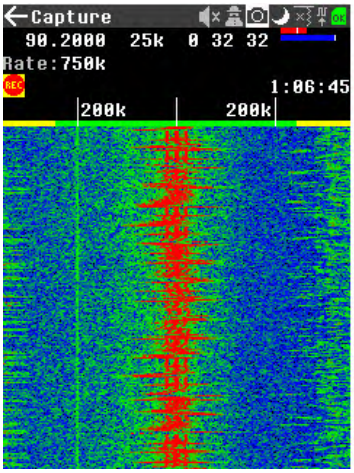
The Key Items on the App that can be selected with the cursor and changed with the encoder knob are:

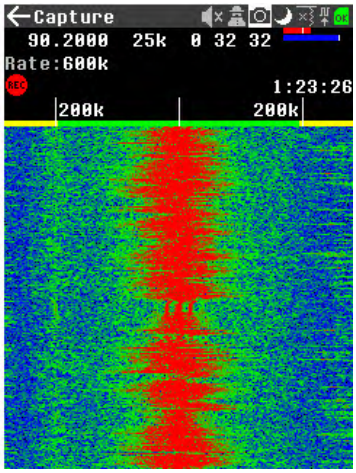
- **Title bar:** The usual Items may be changed and displayed.
- **Frequency:** The setting of the frequency using the keypad can be completed and is stored in persistant memory so can be returned to when the App is used again. But if you have load/save App Settings enabled from SD card, it will continue to use what it was last set at. And you can always edit the file in the SD card, /SETTINGS/rx_capture.ini and edit those related default parameters, according to your needs in that App.
    - Note : Additionally , to be more user friendly , from version 1.7.4+ holding in the Select button on the Frequency field for a second until a digit turns blue, then you can use Left/Right select which digit you'd like to adjust, and then you can use the Encoder Dial to adjust any digit up/down by 1 to tune more precisely. (Press Select again to exit this tuning mode.
- **Step Size:** The selected step size of frequency adjustment carried out by the Rotary encoder.
- **Gain:** Amp (0dB or 14dB), LNA(IF) (0-40),VGA(Baseband)(0-62)
- **Rate:** The sample rate, which by its nature set the set bandwidth of capture. This is shown in the markers around the centre line of the waterfall display. The sample rate is variable from 12k5 to 2750K (*) in many steps. You need to ensure that the sample rate is more than twice the bandwidth of the signal you want to capture see (Nyquist Principle / also called Shannon’s Law)
- **Format:** The user can select two file formats, of the recorded IQ data 16 / 8 bits : C16 (complex 16) or C8 (complex 8), and its related file extension ".C16" or "C8". (By default we are preselecting C16).
- **Trim:** If checked, the capture will attempt to be automatically trimmed to only contain the signal part. This is not reversable. Consider using the IQ Trim utility instead if you're not sure you can capture the signal again.

Note (*) : Currently , **for correct reliable Replay application ,you should ONLY use Capture App selecting any Bandwidth capture <= 1Mhz (but 500Khz is the recommended for majority micro SD cards compatibility because it requires a quite common average write speed in our system >2MB/sec,C16)**. From 600khz till 1Mhz (and 1.25 MHz) , you will need more fast and good quality micro SD card (with min average write speed in our system >3MB/sec (for BW=750khz,C16) , and >4MB/sec (for BW=1Mhz ,C16), (>5MB/sec for BW=1.25Mhz ,C16) and with as small as possible write random latency. (In the GUI , those correct bandwidth capture options appear with the Normal usual "REC" icon Background color, as user recommended BW capture options). If you face too much % dropped samples when recording , you can retry it reducing C16 to C8 , that also reduces the needed average write speed :2 (example 1Mhz rec will need average sd interface speed of 4MB/sec in C16 or 2MB/sec in C8).

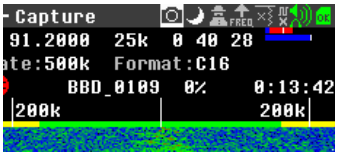
Recently, thanks to x4 Oversampling and /4 Decimation introduction , we have also added 1.25Mhz BW REC , but it is in the limit of our hardware System and it starts to have some M4 sample drops. (It is still experimental).

Above 1.25Mhz till 5.5Mhz bandwith options (with YELLOW REC button background Icon), in current fw version , the recorded files have periodical sample drops , and therefore it can not record all full original samples content and therefore it is NOT useful for the Replay App , just useful to check the spectrum image, example using the linux tool "inspectrum" or "Audacity") . Anyway when replaying those captured files , the replay time will be shorter than real . but normally you should still get a correct modulation, but in case of voice contents, it would sound , unnatural , "like with accelerated playing speed" , because in fact,due to Hackrf One System (HW+SW) limitations, those recorded files (under those high speed BW with YELLOW icon) have decimated its content - when recorded there were skipped some real time samples.



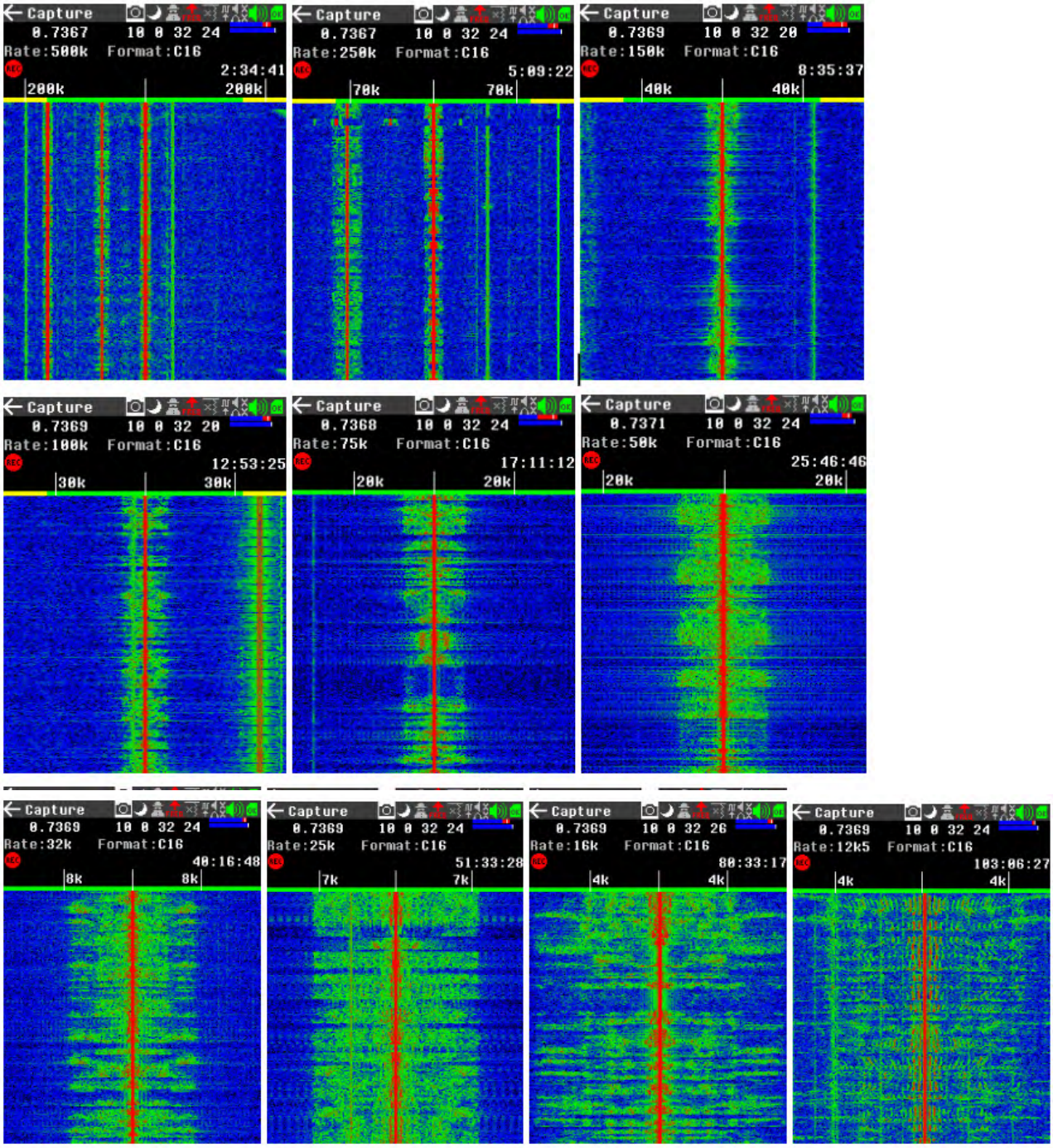


- **Record Button:** The red button shows as Rec or Stop. If record is selected then it will record the I/Q file. To the side of the Record Button is additional information that is shown for the recording file, % of Dropped Samples, total Recording Time Remaining. (As we mentioned above, for correct Replay operatons, please make sure to select a proper Capture bandwith option , with normal black background "REC" icon , not the yellow one.)



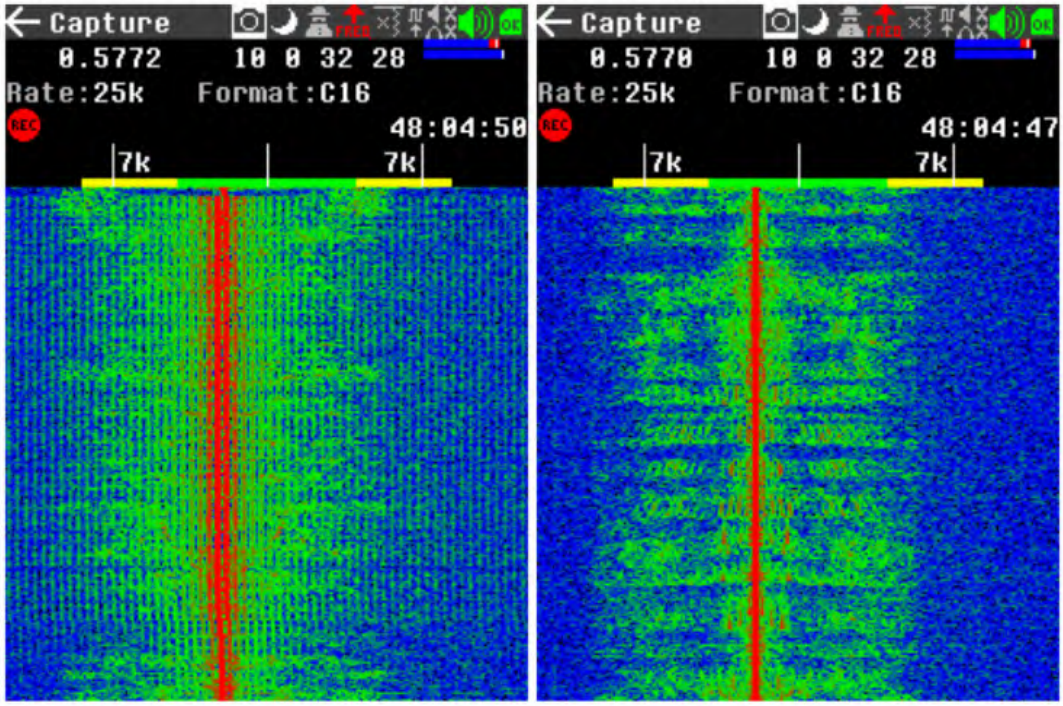

```
* File Name (as above example , BBD_0109.C16, based on the selected format C16)
* % of Dropped Samples (recording error rate, due to SD card write latency, above sample 0%)
* Total Recording Time Remaining (based on available SD card capacity , above example 0h: 13min: 42 secs)
```

From nightly 23-08-19 onwards, we revised and extended a good functionality of all low bit rate bandwith REC options If you adjust correctly the GAIN and LNA and center freq. it is possible to capture good bit streams in C16 / C8 format , Pls. find attached some screenshot examples , capturing the same tuned AM MF band broadcasting with a BW aprox of 16Khz , using an upconverter ,



Depending on the tuned frequency, (mainly visible in 25k, 32k, 50k and 75k) we may got a random strange left picture effect -on the screen, it seems not affecting to the recorded files.C16 or .C8 - with “vertical stripes” , this can be easily corrected, just readjusting the center frequency some Hz up or down , till trying to have full convergence of these vertical red carriers to the central unique one , with +-10Hz steps.

Left : Worse shift L.O. respect vertical stripe effect in the LCD screen
Right : Best tuned image , adj. steps +- 10 Hz till getting vert lines convergence.



Please check the video below for HackRF PortaPack Capture/Replay functionality.

> ⓘNote
> If you have an external GPS module attached, and after starting the Capture app you receive a valid GPS signal the CAPTURE will contain GPS meta data too. The filename will get _GEO appended. If you share this recording, it could contain sensitive info. You can remove it by editing the TXT, and removing the GPS data.

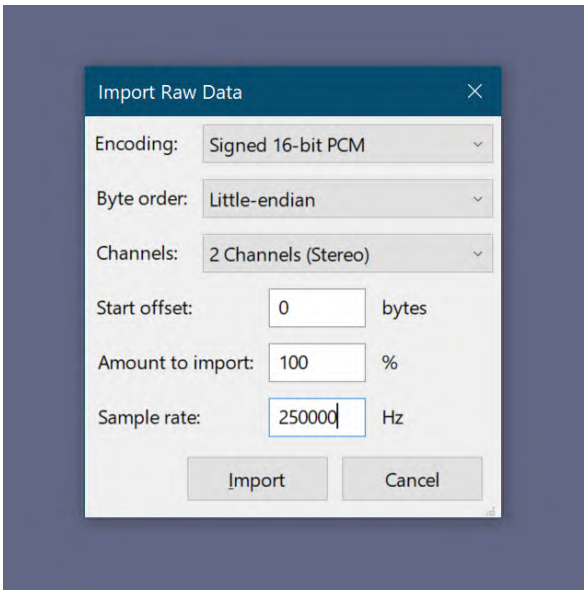
C16 Format

The Capture app records into C16 files, and the Replay app read those files. *(Support for C8 format has since been added to firmware, but this chapter assumes that files were captured in C16 format; most instructions below apply to C8 files as well by just replacing the 16 with 8.)*

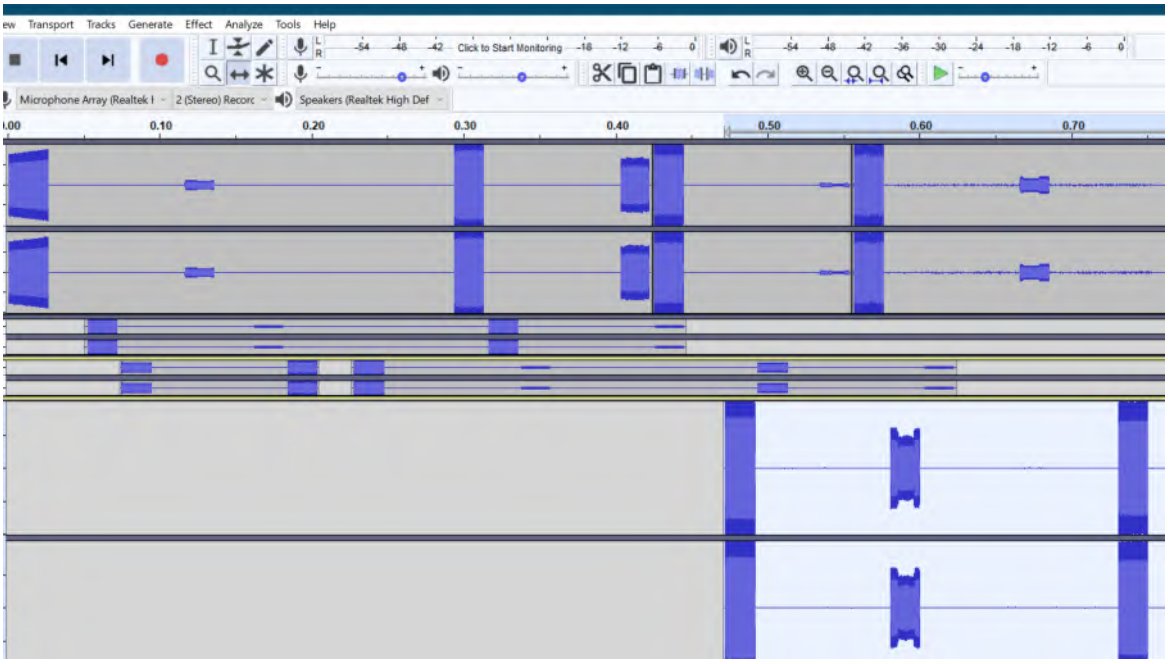
As described in an issue in PortaPack's repo, this format consist of a tuple of 16 bits signed integers. The first number is I and second Q, forming a complex number. As a result, you get a tridimensional representation of the capture: the real and the imaginary parts in the file (I and Q) versus the time (defined by the sample rate, in this case in an adjacent TXT file with the same filename as the C16).

Capture Manipulation (Audacity)

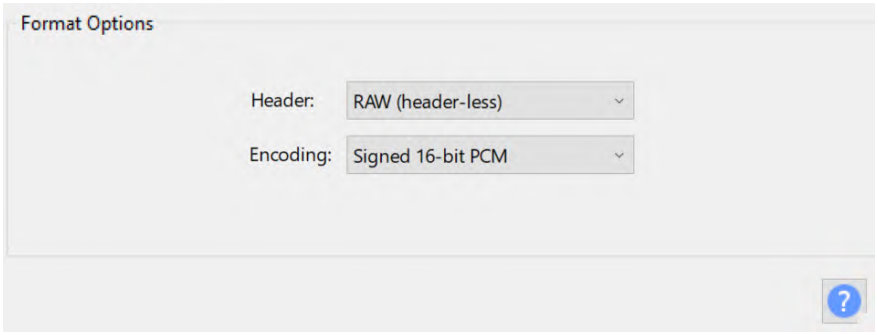
You can open the C16 file in Audacity importing it as *Raw data*. Consider the sample rate you used when you did the capture.



It is possible to manipulate the data as if it was audio. When importing the file as signed 16 bit PCM with two channels, the upper channel contains the I and the second Q, as explained above. You can apply filters, add silences, trim, mix and merge.



To export the data as a C16 file, select Export, Export Audio ... and then select RAW as a 16 bit signed PCM. After saving, change the extension and you will be able to use the file in the Replay app.



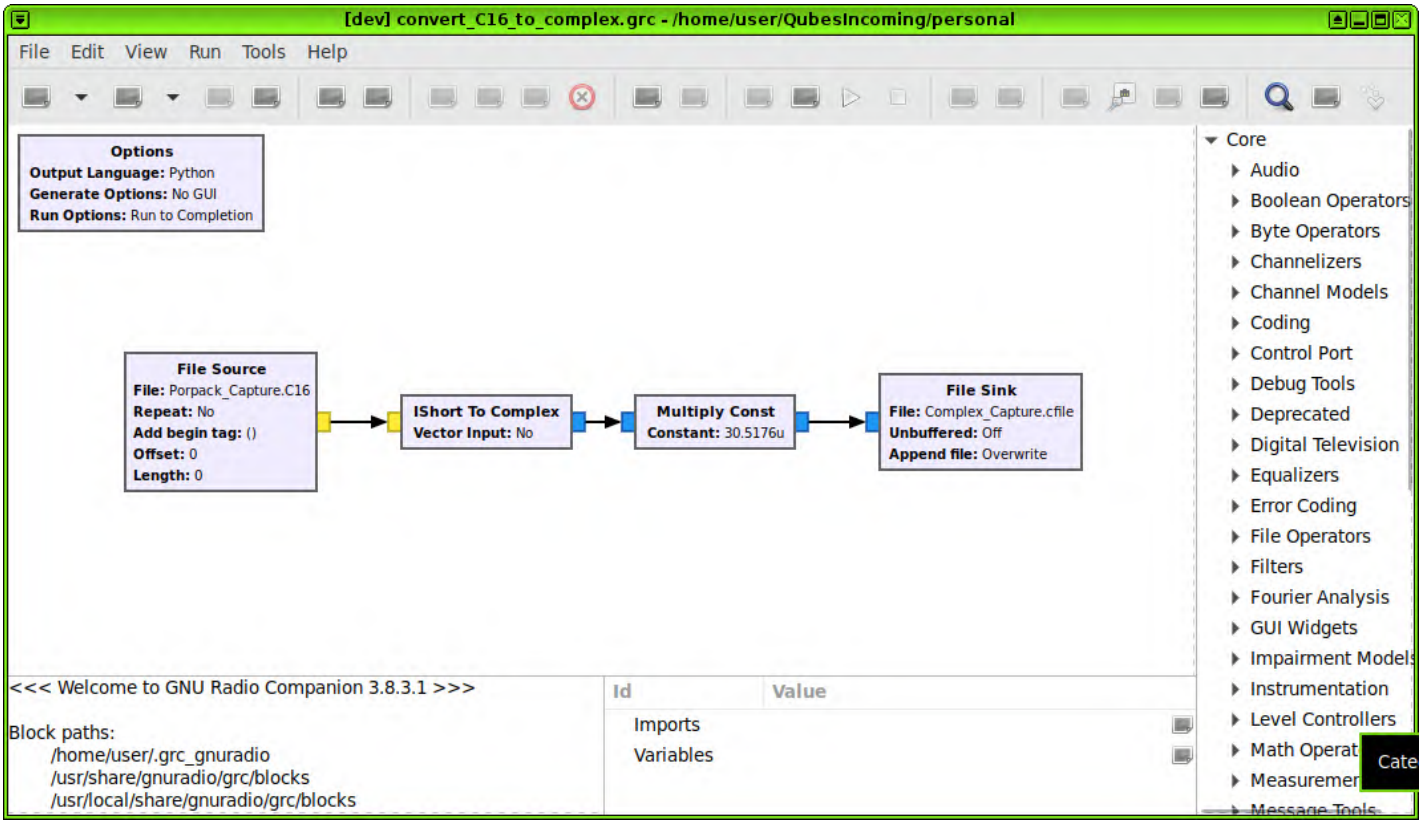
For using the new C16 file in the Replay app, you will also need to include a TXT file with the following metadata (frequency and sample rate):

```
sample_rate=<RATE IN HZ>
center_frequency=<FREQ IN HZ>
```

As a final remark, if you created a new file, be sure that the Project Rate matches your capture:

Capture Manipulation (GNU Radio)

You can use GNU Radio Companion (GRC) to convert the C16 short into a complex IQ file.



As seen in the image above you'll need to bring in the original C16 file using the GRC block `File Source` setting the output type to short, pipe it to `IShort To Complex`, then `Multiply Consent` using the magic number 1.0 / 32768.0 for the constant, and finally export it with `File Sink`.

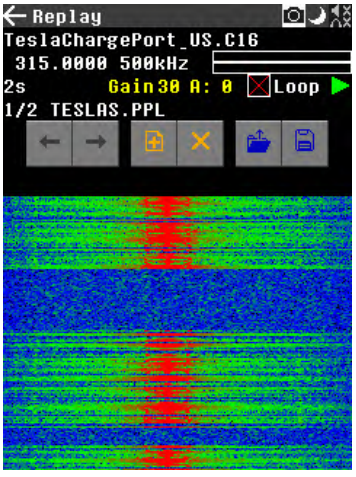
The reason that the value 32768.0 is used to normalize the C16 capture is because int16 has a range of -32768 to +32767. 2^15 is 32768.0, so dividing int16 value by 2^15 gives a number that is normalized between -1 and +1.

This GRC script can be found at [firmware/tools/convert_C16_to_complex.grc]

Replay

This app allows captured signals to be replayed.

The UI



Top controls

- The top line is the name of the currently selected capture file to play (*.C8 or *.C16) .
- The second line has the Frequency (which can be modified) and the capture's sample rate.
- At the end of the second line, there are two progress bars. The top indicates the progress in playlist, and the bottom indicates the transmit progress of the current item.
- The third line indicates the length in seconds of the current item. You can set the TX gain (0-47), TX amp (0|14), loop mode, and toggle playback.
- The fourth line indicates in the left part , the current item number / from total items in that list , (example 1/2) , and in the right , the current playlist file name (could be new if we want to save later , or existing one if we are pre-loading it).

Buttons

- Left/Right buttons allow you to change the currently selected track.
- "+ File" button will open the file picker to select a new C8/C16 (capture) file to add at the *END* of the playlist.
- X button will delete the currently selected item from the playlist.
- Open button will open the file picker to select a new PPL (playlist) file. This will overwrite the current playlist.
- Save button will save the modification to the current playlist.

Tips and Quirks

- When "Loop" is checked, it will continue to play the entire playlist until stopped.
- Playback always restarts from the beginning of the playlist.
- Once a capture has been added to the playlist, you can modify the playback center frequency. This is done on a per-track basis and is *NOT* saved as part of the playlist.
- If a capture file is missing its metadata (partner) file, then the TX frequency and 500K sample rate are assumed.
- A new, unique file name is created when a new capture file is added to an empty playlist. This playlist is not saved unless you press save.
- You can also browse to a Capture (C8/C16) or Playlist (PPL) file in the FileMan and select it to open it in Replay.
- NB: Delay (see below) hangs the UI thread and will appear to freeze the device. You have to restart to interrupt the delay.

Replay Single File

When the app starts, you have an empty playlist and the "+ File" button is focused. If you just want to play back a single item, press the "+ File" button and select a C8/C16 file with the file picker. The play button will be automatically focused once you've made a selection. This allows for fast, 2-click, playback.

Playlist

A sample TESLA.PPL file is included in the SD card.

The file with PPL extension is just text file, you could edit it with any of the text editor.

Playlist files are comma delimited and have the following structure:

```
ABSOLUTE_PATH_TO_C16_FILE,DELAY
#COMMENTS
```

For example, a valid playlist file could contain:

```
# Playlist file example
# capture path, pre-delay milliseconds (optional)
/SAMPLES/TeslaChargePort_US.C16
/SAMPLES/TeslaChargePort_EU_AU.C16,100
```

It will do:

1. Play SAMPLES/TeslaChargePort_US.C16 referring the freq and rate config of its partner file
2. pause 100 ms
3. Play SAMPLES/TeslaChargePort_EU_AU.C16 referring the freq and rate config of its partner file
4. over.

When "Loop" is checked, the playlist will be repeated until you manually stop it by press the "stop" button. Once stopped, playback will start over from the beginning of the list.

Remote

The remote app allows you to create a custom remote UI and bind buttons to captures.

Main UI

- **Remote Title** - The top line is the title of the remote. Select it to edit it.
- **Remote Buttons** - Up to 12 customizable buttons per remote. Select a button to transmit the capture file. Press again to stop. Long-press select to edit or delete the button.
- **Waterfall** - A small waterfall is shown while transmitting below the button grid.
- **Gain** - Control the transmitter Gain and Amp. The color indicates the overall transmitter power.

- **Loop** - Continuously transmit until stopped.
- **Filename** - Shows remote file name. Select it to rename the remote file.
- **Add Button** - Add a new button to the grid. New buttons will open in edit mode when you press them.
- **New Remote** - Start editing a new, empty remote.
- **Open Remote** - Open an existing remote file (REM) from the SD card.

Button Edit UI

- **Name** - The button's text.
- **Path** - Select to pick a capture file.
- **Freq** - The center frequency to send on. Will default to the capture file's metadata if found.
- **Rate** - The sample rate of the capture file. Uses the capture file's metadata or defaults to 500K. Cannot be set in the UI.
- **Icon** - The icon to show on the button.
- **FG Color** - The button's foreground color.
- **BG Color** - The button's background color.
- **Preview** - Shows what the button will look like.
- **Trash** - Deletes this button and returns to the main screen.
- **Done** - Save this button and returns to the main screen.

Tips

- Remotes are automatically saved on exit.
- Use the IQ Trim tool to trim silence from captures so they start instantly.

REM Files

Remote files can be edited in a text editor. Empty lines and lines starting with **#** are ignored. The first non-ignored line is the remote "Title". The remaining lines (up to 12) are read as remote buttons. They have the following format.

```
capture path,button text,icon index,fg color index,bg color index,center frequency,samplerate
```

The position of buttons on the screen can be changed by reordering lines in the REM file.

Scanner

The scanner should be able to scan about 20 frequencies per second, as it requires about 50ms to stabilize after re-tuning.

The scanner will stop on any frequency carrying a signal strong enough. You can adjust the signal threshold with SQUELCH.

For better scanning precision, once a frequency with a powerful enough signal is found, the scanner will analyze it for some extra milliseconds, in order to confirm that the signal is still present (and not a spurious peak).

Big Numbers Frequency

The big numbers display will show the frequency currently being scanned, using the following color code criteria:

- GREY: Scanning
- YELLOW: Analyzing possible signal
- GREEN: Found a strong enough signal

Scan vs Search Modes

The scanner can either *Scan* frequencies from a frequency list in memory, or *Search* all frequencies sequentially between a starting and ending frequency range. The `SRCH`/`SCAN` button toggles between those two operating modes of the scanner app (button indicates the mode that will be switched to when pressed).

Frequency List

The application loads a list of frequencies (f=) and/or a search range from `FREQMAN\SCANNER.TXT` by default, or you can use the `LOAD` button to load from a different file. You can use the Frequency manager app (Tools -> **Freq manager**) to create or edit frequency list files.

If the application finds a frequency *range* (a=,b=,s=) in the frequency file, it is loaded into the SEARCH START and END and STEP fields (the Scanner app only supports one search range per file). Alternatively, you are able to manually input a search range "on the fly" by keying in SEARCH START and END frequencies and the STEP selector.

If app settings are enabled, the last used frequency list will be used on startup.

Manually Selecting Entries or Frequencies

Whenever the `<PAUSE>`/`<RESUME>` button is highlighted, the rotary encoder may be used to scroll through the frequencies in the Scan list, or through the Search range (regardless whether *Pause* is active).

The current item field "X / Y" can also be focused and the rotary encoder may be used to scroll through as well.

Radio Settings

- **Gain:** Setting are shown in order of **AMP** 0=0db or 1=14dB, **LNA**(IF) (0-40) and **VGA** (Baseband Gain) (0-62). (These settings are preserved per App if "App Settings" is enabled in Setup)
- **VOL:** Audio volume.
- **SQ:** Squelch level. When *Pause* is not active, the squelch level determines the minimum signal level that will cause the scanner to pause on a strong signal while scanning or searching (until the **Wsa** Wait timer expires). When paused for any reason, the squelch level also determines whether audio output is enabled or *squelched*.
- **MODE:** Modulation mode; **AM** (DSB 9k, DSB 6k, USB+3k, LSB-3k, CW), **NFM** or **WFM**.
- **BW:** Select signal bandwidth (available values depend on modulation **MODE** setting).
- **STEP:** Selects frequency step increment when performing a sequential **SEARCH**.

Buttons

The purpose of each of the buttons on the screen is as follows:

- `LOAD`: Loads scan frequency lists and/or search ranges from a file (in **Freq Manager** format).
- `MCLR`: Clear list of scan frequencies in the temporary scanning memory (frequencies may subsequently be added to the scan list using `ADD FQ` or `LOAD`).

- SRCH/SCAN: Switches between Search mode (using the search frequency range) and Scan mode (going through the list of saved frequencies), as described above.
- <PAUSE>/<RESUME: Manually Pause / Resume the scanning. The **Rotary Encoder** is enabled to manually scroll through frequencies when this button is highlighted. In SCAN mode, turning the dial will go through the list of saved frequencies. In SEARCH mode, turning the dial will go through the search range. When paused or not, the *Squelch* setting may need to be lowered to hear weak signals.
- FORWARD/REVERSE: Change scanning direction (button shows direction that will be switched to if pressed).
- MIC TX: Jump into the MIC TX/RX app (2-WAY Radio)
- AUDIO: Jump into the RX->AUDIO app (for further analysis)
- DEL FQ: Delete the current frequency on display from the (temporary) scanning memory
- ADD FQ: Add the current frequency into the SCANNER.TXT file

Delay Settings

There are two user-adjustable wait settings while scanning:

- **Wsa:** Wait time while Signal Active, in seconds. When this wait time expires, scanner will skip to the next frequency automatically, even if there is a strong signal present. A value of 0 disables this timer, resulting in the scanner remaining on a strong signal forever, or until changed by the **Rotary Encoder**. A non-zero value of **Wsa** is also known as "Browse" mode.
- **Wsl:** Wait time after Signal Loss, in seconds. When a strong signal drops below the squelch threshold, scanner will remain on this frequency for the specified number of seconds before skipping to the next frequencies.

Other Fields

When scanning, the current frequency index is shown on the screen, along with the count of number of frequencies in the scan list. If a description is found in a loaded frequency file, the description will also be displayed on the screen above the Big Numbers Frequency (otherwise the loaded file name will appear, or "SEARCHING..." in Search mode).

Freqman File Format

See Freqman Manager page

Example: Using Scanner as a Broadcast FM Radio Tuner

Follow the instructions below to use Scanner as a Broadcast FM Radio Tuner:

1. Press LOAD, use dial to select FM_STANDARD_BAND.TXT frequency file, and click Select. (This will load the Search frequency range, frequency step, mode [WFM], and default bandwidth.)
2. Optionally adjust the Volume (VOL), Squelch (SQ), LNA/VGA/AMP RF gain, and Wsa delay settings.
3. Press <PAUSE> to stop the automatic searching.
4. Press arrow keys to move focus to the <PAUSE>/<RESUME> button. When the <PAUSE>/<RESUME> button is highlighted, the manual dial can be used to tune to an FM radio station.
5. Press ADD FQ to add the current frequency to the selected frequency file. Repeat tuning & adding to store additional frequencies.
6. In future listening sessions, just load the same file (step 1) and Scanner will loop through the saved frequencies, spending "Wsa" delay time on each saved station. To stay on a saved station indefinitely, press <PAUSE>. To manually change stations, move focus to the <PAUSE>/<RESUME> button and use the tuning dial. Additional stations may be added in the future by pressing SRCH, then ADD FQ as desired (step 5). Consider renaming the frequency file to SCANNER.TXT if you wish it to be loaded automatically whenever the app is started.

Also see: Recon app

Advanced users may want to try the Recon app, which is a more fully-featured Scanner application.

Microphone Transceiver

Checking Portapack-Havoc repository , we can see , that this excellent app was initially developped by Furrtek in 2017.

- "**Microphone FM transmit with CTCSS**", providing support to Narrow Band FM Transmitter + CTCSS & Receiver in Half Duplex operation, like a walkie-talkie (two-way directional voice communication but one at a time).

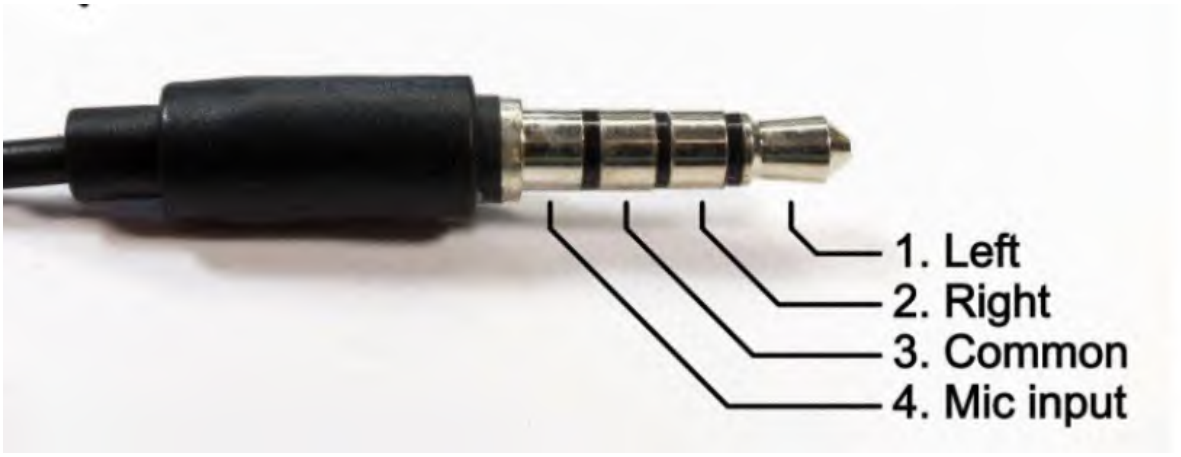
Later on , thanks to many other great sw developers , gradually it has been added many more nice functionalities (VOX control, Roger Beep,...) ,and improving it day by day ... And from Sept -2020, it was also added the support of multi analogue mic Modulation types in half duplex TX / RX, highly appreciated specially by all ham amateur radio community. Those mod types are widely used in LF, HF , VHF, 2m band , maritime communications ,airport airband communications, UHF PMR446,... And since them we are currently supporting those following ones (valid from , Nightly Release - 2022-10-17 onwards) :

- Narrow and normal band FM (NBFM/FM),
- Wide band FM (WBFM),
- Double side band AM with carrier,(DSB-C,AM),
- Upper Side Band (USB),
- Low Side Band (LSB)
- Double Side Band with suppressed carrier (DSB-SC).

Key Controls

- **VU-meter:** Just launching that Mic App, the left side peak audio VU-meter is active, and you can plug your head mic set and confirm its sensitivity and correct operation. The sensitivity of the microphone is shown on the lefthand side of the LCD screen, and should be configured so the range is green for most of the audio and never hits red to limit over deviation of the signal. Note, this feature is not working once we activate below "Rx audio listen" ; but in any case, when pressing PTT, in TX mode, it always works.

- 



- **MIC. GAIN:** Cursor selection and use rotary encoder is used to select a fixed gain of x0.5, x1.0, x1.5, x2.0. The setting needs to be selected based, on the Microphone used which is connected via the Headset/ Microphone socket (standard smartphone 4 segment 3.5mm connector).

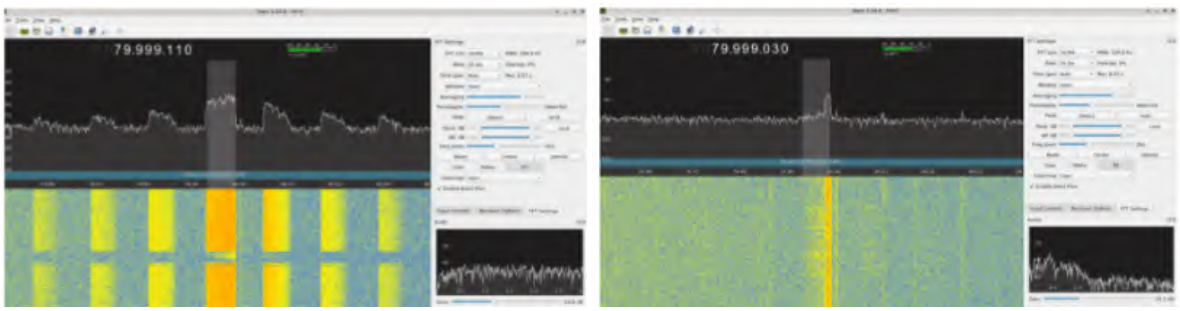
That mic gain adjustment is in fact a post scaling by above factors (x0.5, x1.0, x1.5, x2.0) , of each captured mic voice data . Then ,that adjustment should be only used,to make mic gain fine tuning of the non distorted voice . But if the captured data is already distorted , due to too much mic sensitivity , or to close mic-mouth distance, or too loud voice , the ADC saturation , should be addressed by other means (ALC or Boost adjustment (*1) , or increasing mic-mounth cms distance , or reducing the voice loudness.)

If you want to know the audio codec IC of your Portapack board, you do not need to dissassembly the boards, just go to the "debug" -> peripherals menu , and you will see which peripheral device, you can explore, looking its register map values. In the audio block icon , you will see the audio codec IC name , mounted on your Portapack board : AK4951 or WM8731. (see annexed photo of both two devices)

- 

Automatic mic Level Control "ALC" (AK4951 sound codec IC) or "Boost" pre-amplifier mic control adjustment (WM8731 audio codec IC) : (*1)

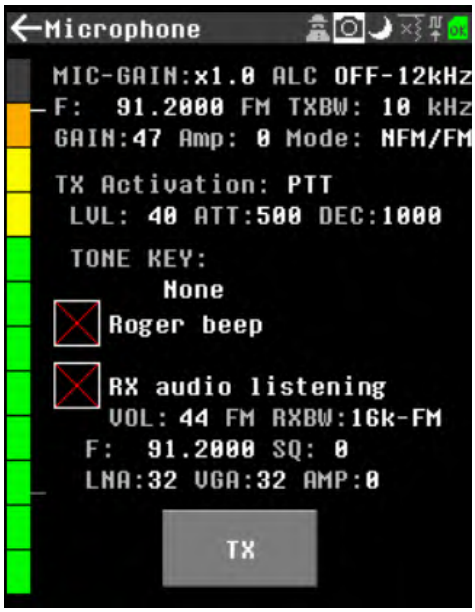
To minimize that mic ADC saturation (and consequently, audio distortion , and spectrum harmonics radiation), we introduced ALC(AK4951) and Boost(WM8731) control options.

- 

With proper adjustment , we can solve that mic ADC saturation, and adapt correctly to our mic gain sensitivity , and the distance mic-mouth from the speaker , and the user voice loudness ... That proper settings , can be done, selecting the best ALC or Boost option (checking that the mic voice sound Vumeter (left mic volume peak bar indication) is below 80-90%, in the green area, see annexed pictures) (example LSB with low modulation index)

1. - **ALC Automatic mic volume Level Control** (available in Portapack boards that uses AK4951 audio codec platform) : With those "ALC" GUI options, user can adjust from +12 dB's to -12 dB's mic gain. For instance , if we want ,to talk , like handsfree mode , and pick up all the voices and sounds inside our room (from 50 cms till several meters distance from the mic, we can select +12 dB's) , If we want to talk around 15 to 20 cms , we can select +0dB's or -3dB's depending on the loudness of our voice … If we want to avoid saturation when shouting , or talking touching the mic with the lips , you can reduce it til -9, -12 dB's If you leave the default OFF settings , you will have exactly same Mic settings as in previous Mayhem FW versions <=1.4.3 , without activating any digital ALC block of in the AK4951. When we saiy , "OFF - 12Khz" it just means that the audio base band output from the IC 4951 has this initial max bandwith, but obviously ,later , when it is post-processed and used for modulation , it is also reduced it. We tried to use and combine several nice

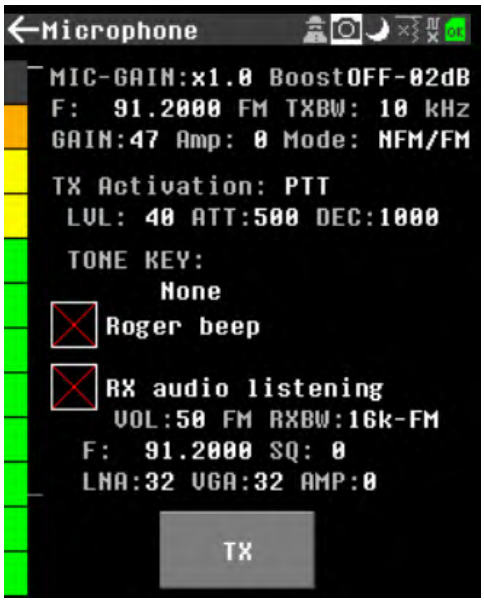
programmable digital features, like , ALC , Wind Nose Filter, LPF , and boosting peaking Equalizer, and also Pre-amp mic level. Ex. +12dB-6Khz , means activated ALC with maximum gain of 12dB's and with digital Low Pass Filter of 6kHz .



USER GUI LABEL : ALC - Bandith :	PRE-AMP MIC	DIG-ALC VOL& REF (max gain at ALC recovery operation)	DIG -WIND NOISE FILTER (Auto detected dynamic HPF)	DIG EQUALIZER (f0, BW) *3dBs peaking	DIG 1st Order LPF (fcut)
OFF-12kHz (Default options)	+21dB's (current)	OFF	OFF	OFF	OFF
+12dB-6kHz	+21dB's (current)	+12dB's	ON	OFF	6 khz
+09dB-6kHz	+21dB's (current)	+09dB's	ON	OFF	6 khz
+06dB-6kHz	+21dB's (current)	+06dB's	ON	OFF	6 khz
+03dB-2kHz	+21dB's (current)	+03dB's	ON	EQ1 ~2 kHz (f0:1.150Hz, fb:1.700Hz)	3,5khz
+03dB-4kHz	+21dB's (current)	+03dB's	ON	EQ2 ~2700 Hz (f0:1.475Hz, fb:2.450Hz)	4khz
+03dB-6kHz	+21dB's (current)	+03dB's	ON	OFF	6 khz
+00dB-6KHz	+21dB's (current)	+00dB's	ON	OFF	6 khz
-03dB-6KHz	+21dB's (current)	-03dB's	ON	OFF	6 khz
-06dB-6KHz	+21dB's (current)	-06dB's	ON	OFF	6 khz
-09dB-6KHz	+18dB's	-09dB's	ON	OFF	6 khz
-12dB-6KHz	+15dB's	-12dB's	ON	OFF	6 khz

2. ◦ **Boost mic** (in Portapack boards that uses WM8731 audio codec platform) :

With those "Boost· GUI options, user can adjust from +12 dB's to -08 dB's mic gain. We have added five user "**Boost**" options , activating on/off , the mic-boost pre-amplifier (+20 dB's) and playing with internal captured data, to allow smaller steps. In order to avoid mic distortion, We only recommend to use the pre-amplifier boost on , when we are using low sensitivity mics or when we are keeping some distance (example >15 cms) to the mic :



WM8731 GUI FM relative Gain Mode	Mic-boost (on/off) +20dB/0dB	Internal effective audio capture gain	Relative mic gain dB's Respect current fw ref (+20dB's)
+12 dBs	+20 dB's (**Mic boost ON**)	+12 dBs	+20+12=32 dB's 32-20 (fw 1.5.x) = +12 **(+12dB ref fw 1.5x)** (No sat. > 15 cms)
+06 dBs	+20 dB's (**Mic boost ON**)	+6 dBs	+20+6=26 dB's 26-20 (fw 1.5.x) = +06 **(+06dB ref fw 1.5x)** (No sat. > 15 cms)
+04 dB's	+0 dB's (Mic boost OFF)	+24 dBs	-0+24= +24 dB's 24-20 (fw 1.5.x) = +04 (+04 vs dB ref fw 1.5x) (No sat. > 2-3 cms)
-02 dB's (Default option)	+0 dB's (Mic boost OFF)	+18 dBs	-0+18 = +18 dB's 18-20 (fw 1.5.x) =-02 (-02 dB's vs ref fw 1.5x) (No sat. > 2-3 cms)
-08 dB's	+0 dB's (Mic boost OFF)	+12 dBs	+0+12 = +12 dB's 12-20 = -08 (-08 dB's vs ref fw 1.5x)

We also added several new features : a new check box (next to Roger beep) to the user to be able to select Separated (default)) / Common freq. RX tuning control respect TX freq., another one "Hear Mic" (see attached new updated GUI pictures), and small new TX feature, new GUI about IQ TX phase calibration adjustment . (It is in the bottom right part of the screen) : "TX-IQ-CAL", and a TXBW selection in SSB mode :

- **F:** This field set the TX Frequency for the transmitter. Use encoder dial to adjust by Step value (uses a default step value, or step value saved in SETTINGS\tx_mic.ini file if "Load App Settings" is enabled). A long press of the Select button allows adjusting frequency digits individually.
- **F_RX:** This field set the RX Frequency for the receiver.
- **TXBW:** This field sets the FM BandWidth of the transmission under normal conditions from 0-150 kHz. (In fact,in FM mode it is the +/- FM deviation in Khz that we will apply to the modulator.). Recently , also in SSB mode (USB or LSB) , we allow to the user to set up audio baseband BW to be transmitted (2KHz, 3kHz). (sse annexed example spectrum)

- **GAIN:** Is set for TX LNA(IF) and (0-47)
- **AMP:** RF TX amplifier , 0dB or 14dB.
- **MOD:** to set the selected analogue TX & RX modulation type : NFM-FM // WFM // AM // USB // LSB // DSB
    - Narrow band FM (NFM-FM) TX ,and supporting NFM-FM RX : BW: 8K5 (8K50F3E) , 11Khz (11K0F3E) ,and FM RX BW :16Khz (16K0F3E)
    - Wide band FM (WBFM) TX , and supporting WFM RX of the following BW: 200kHz (Emissions Designator 200KF3E), 180khz and 40khz (see more details below)
    - Amplitude Modulation (AM) TX fixed to the standard AM-6K00A3E, but supporting AM RX with two selectable receiver bandwidth filters, BW : 9 and 6kHz (covering both side lateral bands, AM DSB with carrier AM-9K00A3E / AM-6K00A3E)
    - Upper Side Band (USB) TX , supporting USB RX with BW : 3kHZ (SSB-3K00J3E)
    - Lower Side Band (LSB) TX, supporting LSB RX with BW : 3kHZ (SSB-3K00J3E)
    - Double Side Band with suppressed carrier (DSB), supporting DSB RX with BW : 6 kHZ (covering both side lateral bands)
- **TX Activation:** Field can be selected for one of three settings. Off, PTT, AUTO. In the PTT setting, the PortaPack will transmit when the TX button and the bottom of the App screen is pressed on the touch screen. The AUTO is also known as a VOX control (automatic PTT transmission activated by voice). In AUTO the Receiver section below ("Rx audio listening") is not available , but the triggering is set by the following 3 settings.
    - **LVL:** The level that triggers the transmission is set by the audio level going over the threshold value set (0-255). This can be seen as a grey dash marked next to the vu-meter and shows its current setting compared to the microphone level.
    - **ATT:** This is the attack time of the microphone audio level must be above the set threshold to start transmitting (0 to 999mS). Higher attack helps avoid false triggers but might cut off the first words you say.
    - **DEC:** This is the decay time of the microphone audio signal falls below the threshold level be for the transmission is stopped (0 to 9999mS). Lower decay avoids silence at the end of the message but might cut you off in the middle of a sentence. Adjust levels depending on your speaking habits.
- **TONE KEY (CTCSS) :** Continuous Tone-Coded Squelch System or CTCSS is one type of in-band signaling that is used to reduce the annoyance of listening to other users on a shared two-way radio communication channel, sometimes referred to as tone squelch.
- Note1 the level of the Tone % compared to the Microphone setting is set in Options >Audio.
- Note2, that feature is only available in both FM modes (NFM-FM / WFM).
- **Check box Roger beep:** This tick is activating an ending sequence of six consecutive digital synthesized audio tones , to indicate that the operator has concluded speaking.
- Note: that feature is not available in SSB modes (USB , LSB)
- **Check box Hear Mic:** This feature will allow to the user to check his Mic through the combined headphone and mic headset , without the need to use an additional receiver.It works for both Portapack audio codec platforms : AK4951 / WM8731 . You can adjust the Mic sound volume with the same below receiver VOL .
- Notes: to avoid user confusions, that audio sound feature is disabled when user selects to hear the receiver demodulated sound . In both audio codec platforms, when clicking that “Hear Mic” , we are changing the default pre-setting ALC or BOOST option to the best that has maximum audio codec volum sound …
- **Check box F = F_RX:** (Added from [Nightly Release - 2023-04-05] It allows to the user to select Separated / Common tuning frequency from Receiver(RX) to the Transmitter(TX). Once is marked , we have a common same frequency (F = F_TX) and therefore, to not confuse to the user , we hide the bottom independent F_RX field . (as you could see in the two above GUI pictures)
- **Check box RX audio listening:** The Tick box to select this item is difficult to select with cursor having to go down and up though item, and with some luck you may enable the box. It is better to select from the touch screen. If this is enabled then it will turn on the Audio Receiver and with the following setting will allow you to listen to a receive channel when not transmitting. The TX-RX timing gap is not known. The frequency can be set separately or Common to that of the transmitter section above. The following setting can be applied to the receiver.
- Note : this feature is not available when we are in AUTO VOX control .
- **VOL :** Audio receiver volume control.
- **RX BW:** This GUI option , allows several analogue demodulation options :

  in NFM-FM mode to set up the receiver Bandwidth setting. It can be set to either

    - 8k5kHz- NFM (delta FM deviation +/- 1,25 khz, FM index modulation:0,4)
    - 11Khz - NFM (delta FM deviation +/- 2,50 khz, FM index modulation:0,75)
    - 16kHz - FM (delta FM deviation +/- 5,0 khz, FM index modulation:1,6)

  In WFM mode

    - 200Khz FM bandwidth , for commercial FM stations with soft band pass transition. And recently also added the bandwiths BW: 180khz and 40khz (that last one, mainly for NOAA analog FM APT - 137 Mhz reception), both with sharp stop band transition.

  In AM

    - DSB1 -9Khz, DSB2-6Khz bandwidth.

In USB , upper +3khz single side band.

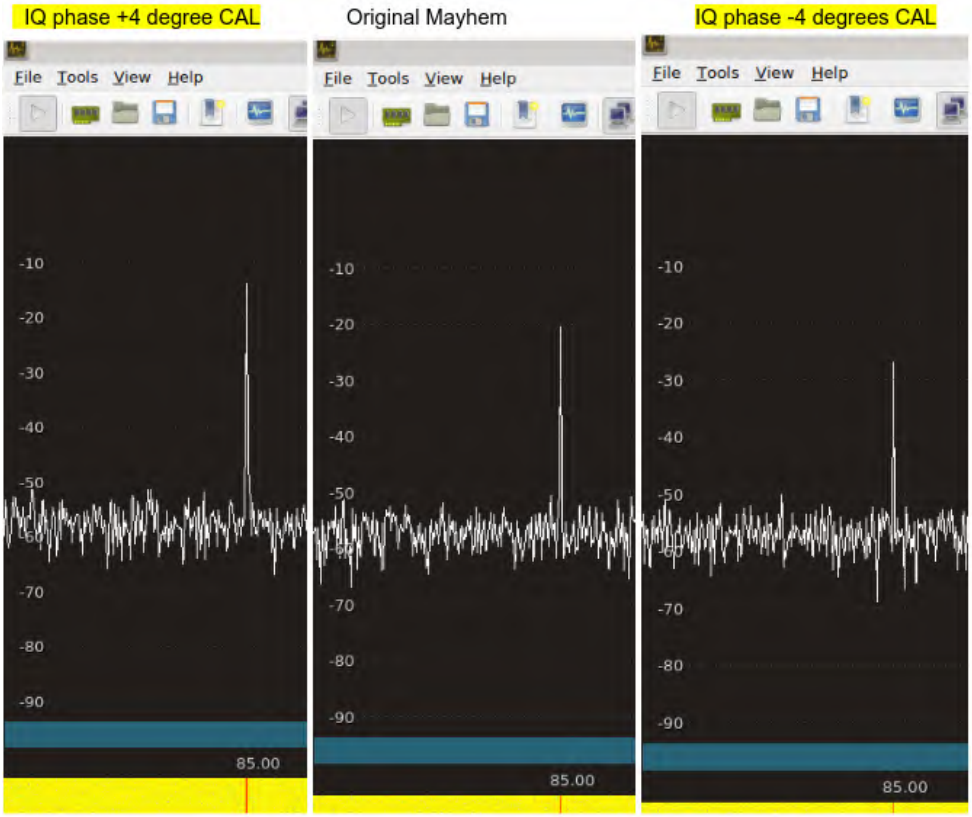
In LSB , lower -3khz single side band.

In DSB-SC , we can select to demodulate any of both SSB bands (LSB, USB). In DSB-SC mod type , both side bands has exactly the same modulated content, but sometimes we may have more particular interference signals in one side than the other.

- **F:** The RX frequency can be set in the usual way with text pad when selected
- **SQ:** This can be set between 0 and 99 typically 50 is threshold.
- **GAIN:** The RX gain setting of LNA(IF) (0-40)
- **VGA:** RX (Baseband)(0-62)
- **AMP:** RX LNA pre-amplifer 0=0dB or 1=14dB.
- **TX-IQ-CAL:** TX I/Q channel phase calibration, to adjust the imbalance IQ modulator phase error. The adjustment range is (+4º ...-4º). Specially usefull to optimize the SSB (USB-LSB) or DSB-SC , Suppressed carrier . In Hackrf versions r1 to r8 , we are using max2837 , that has a calibration register settings of 5 bits , in Hackrf r9 , we are using max2839, that has 6 bits to cover the same range (+4º,..., -4º phase adj).

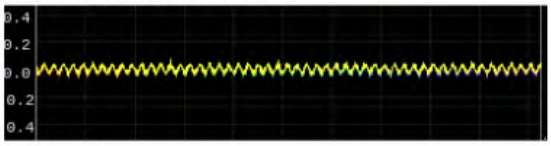
At the moment we do not have any automatic IQ imbalance phase error calibration process. You will need some other SDR receiver , and check the suppressed carrier level when you push PTT _TX in SSB (USB or LSB) without any modulation, and then go to the right modify the "TX-IQ-CAL" value , and press again PTT_TX till getting the lower attenuated "suppressed carrier.

As example , see the attenuation of the residual SSB carrier effect, when adjusting that IQ Phase calibration value in an H1R1 with max2837,

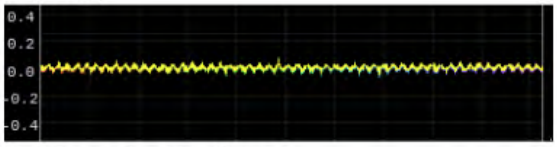


Checking in that above sample ,temporal demodulated residual oscilloscope simulation by SDRangel :

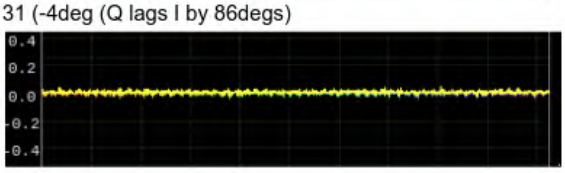
00 (+4deg (Q lags I by 94degs)



15 (+0deg)



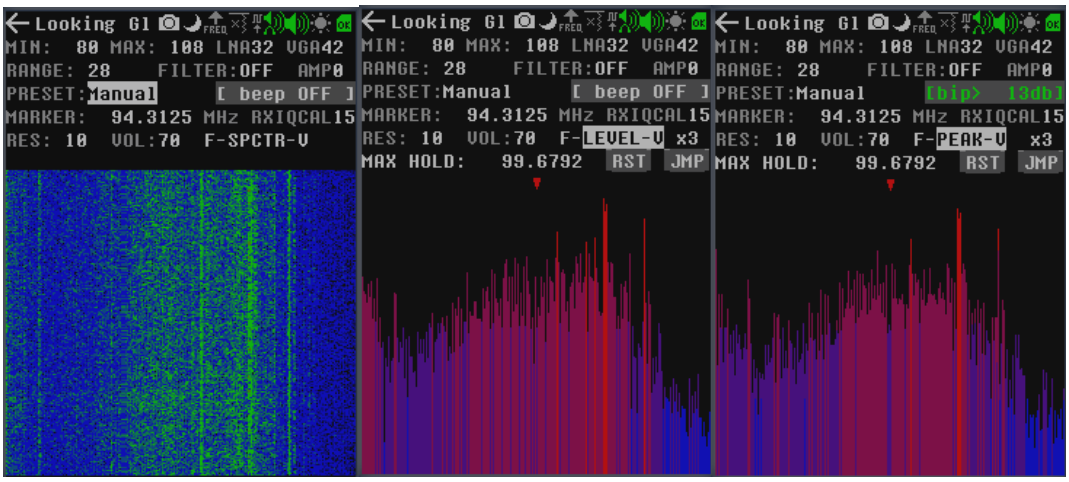
31 (-4deg (Q lags I by 86degs)



Note this Mic application while performing a transmit function may well over deviate and generate unwanted harmonics.

Looking Glass

Looking Glass



This App Provides a view of the spectrum over a very wide range of frequencies. The waterfall display is updated with each full scan.

It should be noted that for wide scan frequency ranges the scanning time is very long and the display can look like it has frozen.

The key is to keep the band scanned as small as possible. While the HackRF is in RF terms a poor receiver in terms of sensitivity, the Portapack/ HackRF can be a very useful tool to scan for local radio signals when using the appropriate antenna.

The Looking glass is an excellent tool to visualise the spectrum and if set to a narrow scanning range can see the on/off patterns of the radio transmission.

The frequency ranges are held in the SD card >LOOKINGGLASS>PRESETS.TXT. It should be noted that the size of the frequencies should be keep small to limit the memory use.

Key Controls

- MIN / MAX: Place the cursor on the “MIN” or “MAX” fields and use the rotary encode to select the frequencies for the MIN and MAX frequencies in increments of 'steps'. The Label “RANGE” shows the scan range set.
- Range value: place the cursor over the range value and click to lock/unlock the range when changing MIN/MAX.
- Gain: Gain Setting: Cursor can be used to select and adjust the LNS(IF) (0-40), VGA(0-62) and RF AMP “0” (off) and 1 (14dB).
- FILTER: Move the cursor to the FILTER field and select either OFF, MED, HIGH. These setting adjust the display to show differing views (that do change depending on the Speed of scan and Gain settings. Use the One that give the best contrast of the detected signals.
- PRESET: Move the cursor to the “PRESET:” field to select one of the pre-set frequency ranges set in the SD Card.
- BEEP: enable/disable on click, when enable select beep squelch value in db
- MARKER: If you place cursor over the field and turn the rotary encoder a red marker arrow will appear on top of the cascade so you can see approximate idea of the frequency for each pixel. The interval of the marker that is changed by the encoder knob, is shown and is based on the scan range. If you press the encoder know or Button then it will take you to the Audio App for more detailed view of the signal with setting of 1mHz Steps and a 10mHz view. Unfortunately, on return to the LOOKINGGLASS App the display goes to default settings.
- RXIQCAL: It actually can improve (8 to 10 dB's from worse Calibration point to the best one) the receiver Image Reject Ratio (IRR). This CAL feature only is available in the Receiver Applications that are using Zero IF-frequency tuning ,like this Looking Glass and Audio SPECTRUM mode. This calibrated value will be stored in the SD card , /settings/rx_glass.ini. (A good default value is to use the central value 15/32 in max2837 (non r9 HackRF version devices) , 31/64 in max2839 (r9 HackRF versions). (To see more extended calibration details , pls check Audio App SPECTRUM wiki part)
- RES: The field can be changed by the rotary encoder to select the resolution (FFT Trigger point) (2-128). The default setting is 32. This allows the display to show better the Signals received and should be adjusted in conjunction with “Gain:” and “FILTER:”.
- VOL: This field controls the volume of the beeps when beeps are enabled
- S-/F-: Slow but more accurate scan / Fast but less accurate scan.
- SPECTR/LIVE-V/PEAK-V: This field can be changed by the rotary encoder to select spectrum scrolling view (default),the live frequency power level view, or the peak frequency level view.

Additional LIVE-V / PEAK-V controls

When switching on one of these mode, one more filter button 'x0 to x9' and one more line of widget are added: 'MAX HOLD: VALUE "

- x0 to x9: integration multiplier field, only shown if LIVE-V is selected. From x0, the quickest integration but with noises and spikes, to x9, the slowest integration, but more clean and less spikes.
- RST: reset the most powerful detected frequency and clear the screen
- JMP: Jump to audio app on MAX HOLD detected frequency

Utilities

- Freq manager
- File manager
- Signal gen
- Wav viewer
- Antenna Length
- Wipe SD card
- Flash Utility
- SD over USB

Antenna length

This application calculates the optimal antenna length for any specific frequency you may input, displaying the result in both **Metric** and **Imperial** units.

You can also change the wave type from a preset list of divisors including full, half, quarter waves (and other divisors) which is handy for choosing an appropriate antenna (if not the best one -a.k.a full wave one-).

NEWBIE NOTE: The need for selecting the right ("tuned" or "matched") antenna for each frequency is of paramount importance, otherwise the RX or TX will be less than optimal, and under some circumstances (such as grossly mismatched antenna under high power TX) you could even end up damaging your equipment (this is true for all radio TX equipment).

Adding your own antennas

This Antenna calculator app goes a step further, by calculating and displaying in simple terms how much you should extend any pre-defined telescopic antenna you may own, which is of great help while doing some field work and having to resource to whatever Antennas you included on your kit.

For this to work, you will need a microSD card inserted on your Portapack. A simple text file with the antennas you use needs to be present under /WHIPCALC/ANTENNAS.TXT

ANTENNAS.TXT example

```
#antenna label,elements length in mm, separated by a commas
ANT700,95,134,175,206,230,245
ANT500,185,315,450,586,724,862
TELESCOPIC,118,183,253,326,399,476
Cheap 11cm,118,183,253,326,399,476
```

The txt file syntax is self-explanatory with the included comment on top of it.

Telescopic

- ANT500
- ANT700
- Generic Telescopic H2 (12 cm)
- Generic Telescopic H1

Fixed

- Magnetic fixed
- GPS: 1575.42 MHz
- Baofeng

References

Episode 44: telescopic antenna of the HackRF (The RF Noob) https://www.youtube.com/watch?v=MzbAEBghcPM

File manager

Used to manage files on the SD Card.

Controls

- Use the encoder or up and down buttons to move between items.
- Use the select (center) key enter a folder or to select an item to take an action on.
- Use the right button to select a folder to take an action on (e.g. rename a folder).
- Use the left button or select the ".." folder to go up a directory.
- click on "-->" to get to next page, you will generally find it at the bottom of the list
- click on "<--" to get to previous page, you will generally find it at the top the list

A small, blinking arrow on the right indicates that there are more items if you scroll down.

Pagination

When there are too much elements, the sorting is disabled (not enough memory to do it) but the pagination is turning on, allowing to view a lot more elements.

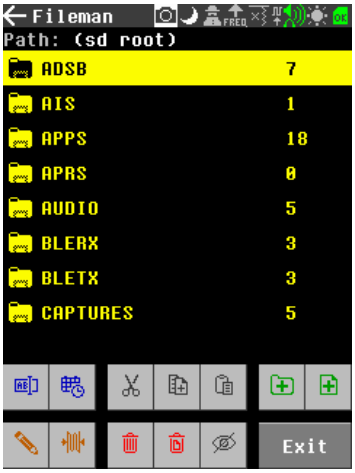
On pagination buttons lines and in place of the size, there will be a page number indicating to which page you will be going.

File type handlers

Selecting certain types of files launch a viewer for the content. Use the right button to enter the toolbar for these file types. Exiting the viewer when launched this way will return back to Fileman.

- BMP files will open in the Splash viewer. If the file is of the correct size and type, it can be set as the splash screen.
- TXT files will open in Notepad
- PPL and C8 and C16 files will open in Replay in the correct mode.
- PNG file will open the Screenshot viewer (this can only view screenshots generated on the device). When viewing a screenshot, press any key to return back to Fileman.

Buttons



When an item has been selected, the following commands are available in the toolbar.

- Rename - rename the file or folder.
- Timestamp Rename - rename the file or folder with the date appended.
- Cut - add the selected file or folder to the clipboard to be moved (by using Paste).
- Copy - add the selected item to the clipboard to be copied.
- Paste - move/copy the content of the clipboard into the current folder.
- New Folder - create a new folder in the current folder.
- New File - create an empty file in the current folder.
- Notepad - open the file in the text editor.
- Trim - open a capture file in the IQ Trim app.
- Delete - delete the file or folder.
- Clean - erase all the files in the folder.
- Show Hidden - shows hidden files.
- Exit - exit the file manager.

Partner files

- Capture files (.C8 or .C16) will have a "partner" .TXT file containing metadata. Renaming or deleting one of the pair will prompt the same action to be applied to the other.

Known folders include

- / (root) folder - holds current splash screen file (splash.bmp), and the folders below.
- ADSB - holds map and airline data for the ADSB RX app.
- AIS - holds data for the AIS app.
- APPS - holds external apps such as PacMan and Calculator (app version on SD card must exactly match firmware version or it cannot be executed).
- APRS - holds captures from the APRS app.
- AUDIO - holds captures from the Audio app.
- CAPTURES - holds captures from the Capture app.
- DEBUG - holds debug dump files created from the Debug Dump app.
- FIRMWARE - recommended directory to store alternate Mayhem firmware images.
- FREQMAN - holds frequency list files for the Freqman, Scanner, Recon, and Looking Glass apps.
- GPS - holds data for the GPS Sim app.
- LOGS - holds logs from various apps like ADSB-RX, ERT, TPMS, Pocsag and Radiosnde.
- LOOKING GLASS - holds preset frequency ranges for Looking Glass app.
- PLAYLIST - holds play list files for the Playlist app.
- SCREENSHOTS - holds screenshots.
- SETTINGS - holds saved App Settings (.ini files), PMEM_FILEFLAG and pmem_settings (only if persistent memory is being saved on the SD card), DATE_FILEFLAG (for incrementing pseudo-date only when coin cell battery is dead), and blacklist (list of apps to be disabled [1.8.0 firmware])
- SPLASH - holds example splash screen files. To select a new splash screen, open a BMP file with FileMan and press the Right button to copy it to the root directory as your new splash.bmp file ("Show Splash" also needs to be enabled on the Settings->User Interface page).

Known Issues

- items are listed unsorted after a fixed number of element (hardware limitation, no enough memory to sort all the files).
- Copy & Paste does not work on folders. (Note that Cut & Paste *is* now supported on folders.)
- Folders must be empty in order to be deleted (use the Clean button to empty a folder first).
- Cut/Copy/Paste does not work with "partner" files.

Tip: Use the SD-over-USB utility for more advanced file and folder editing via an attached computer.

Freq manager

Freqman file format

freqman file support:

- empty lines
- comment lines
- max entry description size: 30 characters
- max number of entries by file: 150

⚠ anything which is not matching one of the described fields is ignored

⚠ In case you hit the maximum number of entries in a list, file is truncated.

Description of the fields

'f=freq' for one Single frequency entry
'a=start_frequency,b=end_frequency' for a Range entry
'r=ham_relay_rx_freq,t=ham_relay_tx_freq' for a HamRadio entry
'l=repeater_listening_freq,t=repeater_tx_freq' for a Repeater entry
m=modulation
bw=bandwidth
s=step
d=description
All fields except [f=|, [a=,b=|, [r=,t=| and [l=,t=| are mandatory.
If nothing specified actual value is used, even if actual value is 'not set'
Any application using the original load_freqman_file will only load frequencies, and will try to populate a range in the list instead of manually stepping in. For developers: I've made a new load_freqman_file_ex func which do return an old list format depending on the parameters
The Recon app is using the old as the new format, taking informations in account when they exist.

Freqman file example

```
f=468000000
f=468000000,d=Single Freq
f=468000000,m=AM,d=Single Freq AM
f=468000000,m=NFM,d=Single Freq NFM
f=468000000,m=WFM,d=Single Freq WFM
f=468000000,m=AM,bw=DSB 9k,d=Single Freq AM DSB
f=468000000,m=AM,bw=USB,d=Single Freq AM USB
f=468000000,m=AM,bw=LSB,d=Single Freq AM LSB
a=87000000,b=110000000
a=87000000,b=110000000,m=AM,s=100kHz,d=AM radio search
a=87000000,b=110000000,m=AM,bw=DSB 9k,s=250kHz,d=AM radio search LSB
a=87000000,b=110000000,m=WFM,bw=200k,s=50kHz,d=WFM radio search s=50kHz
r=430150000,t=430550000
r=430150000,t=430550000,d=HAM radio
r=430150000,t=430550000,m=AM,bw=DSB 9k,d=HAM radio
l=430150000,t=430150000,m=SPEC,bw=150k,d=100k repeat
l=430150000,t=430150000,m=SPEC,bw=1000k,d=1000k repeat
l=430150000,t=431150000,m=SPEC,bw=1000k,d=1000k repeat txoffset 1MHz
```

Possible values for modulation/bandwidth

- AM (DSB 9k , DSB 6k , USB+3k , LSB-3k , CW)
- NFM (8k5 , 11k , 16k)
- WFM (200k , 180k , 40k)
- SPEC (12k5 , 16k , 25k , 32k, 50k , 75k, 100k , 150k , 250k , 500k , 600k , 750k , 1000k , 1250k, 1500k , 1750k , 2000k , 2250k, 2500k , 3000k, 3500k, 4000k, 4500k, 5000k, 5500k)

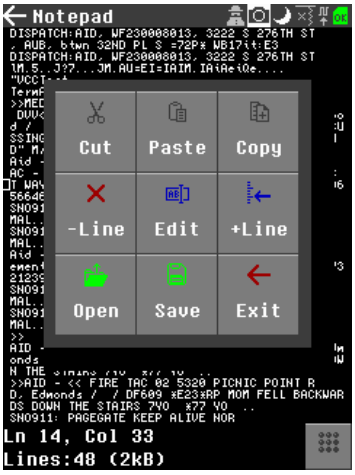
Possible values for Steps

- 5kHz , 6.25kHz , 8.33kHz , 9kHz , 10kHz , 12.kHz , 15kHz , 25kHz , 50kHz , 100kHz , 250kHz , 500kHz , 1MHz

Notepad

Views text files and supports very basic editing.

The interface



The menu button on the bottom right opens and closes the main menu. On start, this button will immediately show the file picker.
The file can be navigated with the direction buttons. Additionally, the encoder can be used to scroll. The encoder direction is set by the last direction button that was pressed. If you want scroll horizontally, first press the left or right button. When scrolling vertically, the encoder moves 16 lines per step in order to make scrolling through large files

easier.

The center (select) button will show the main menu. To close the menu again, click the menu button on the bottom right.

Opening a file

There are two ways to open a file. If you first open Notepad, select the menu button and the file picker will be displayed. You can also open a file from within Fileman by selecting a file and clicking the Notepad icon in the toolbar.

Editing a file.

The following edit modes have been implemented.

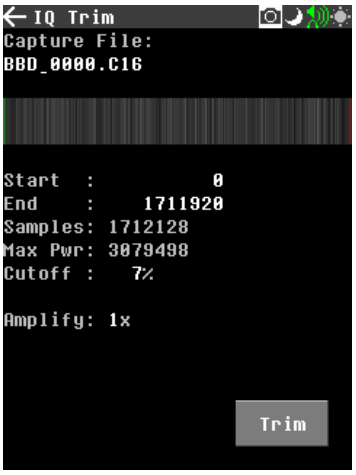
- Delete line (- Line) - deletes the line the cursor is on.
- Add line (+ Line) - adds a new line above the line the cursor is on. If the cursor is at the very end of the file, adds the newline below the cursor.
- Edit - opens the text entry view to edit the current line. If the line is very long, this may crash due to memory constraints. Using "back" will cancel the edit. Selecting "Ok" will commit the edit to the file.

Known limitations

- Exiting Notepad with the "back" button (top left) will *not* prompt you to save. Your changes are not lost. Any in-progress edits are saved in the temp file "filename.ext~". You can recover this file using "Rename" in Fileman.
- Edits on larger files are slow. It currently requires multiple passes over the file contents because all operations are performed directly on the file contents (vs. in-memory) in order to work within the memory constraints of the device.
- The first edit is additionally slow because it copies the source file on first write. This is to allow changes to be made that can be discarded.
- There's currently no UI indication that the program is performing IO. As long as you don't see a fault, it should be working. Just be patient.
- Cut/Copy/Paste is not implemented yet.
- The cursor doesn't automatically get updated after edits. Navigation will snap the cursor back to the text.

IQ Trim

IQ Trim allows you to trim "radio silence" from the beginning and end of a C16 or C8 capture file.



UI Components

- **Capture path** - select to pick the capture file to open.
- **IQ Display** - shows the IQ file power in 240 buckets. Green/Red lines indicate the Start/End positions.
- **Start** - Starting sample of the trim region. Can be modified.
- **End** - Ending sample of the trim region. Can be modified.
- **Samples** - Number of samples in the capture file.
- **Max Pwr** - Power (complex magnitude) of the "strongest" sample in the capture file.
- **Cutoff** - Signal to Noise cutoff as a percentage of the Max Pwr. Can be modified.
- **Amplify** - The signal (and noise) in the trimmed file can also be amplified, which might help if the captured signal was weak.

Trimming Capture Files

1. Open a capture file. You should hopefully see a trimmable region in the IQ Display control.
    - If you don't see a block in the IQ Display, the capture signal was too weak for the tool.
2. Manually set Start/End or use the Cutoff % to automatically trim.
3. Press "Trim" - the file will be edited. It does not make a backup so be careful with your favorite sample files. Maybe use FileMan to make a backup first.

Splitting Capture Files

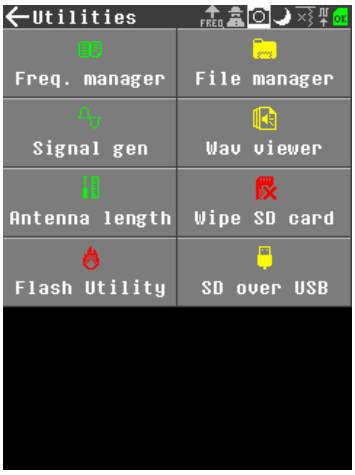
Capture files can be split into multiple files using FileMan and Trim. Use FileMan to make copies of the original capture file, then trim each copy using manually specified Start/End positions. (After splitting, the resulting files can be trimmed too, if desired.)

SD over USB

This application allows you to access the content of the sd card over the USB interface.

SD over USB

Just start the app and click "Run"



While the USB Mass Storage Mode is active, a little USB icon will be displayed.

Now just use the Portapack as if it was an sd card reader.

Note that "SD over USB" is very slow, around 400-500 kb/s, so in some cases it may be faster to remove the SD card and plug it into your computer. It may take up to 2 hours to copy the 2GB world_map.bin file to the SD card using "SD over USB", for example.

Signal gen

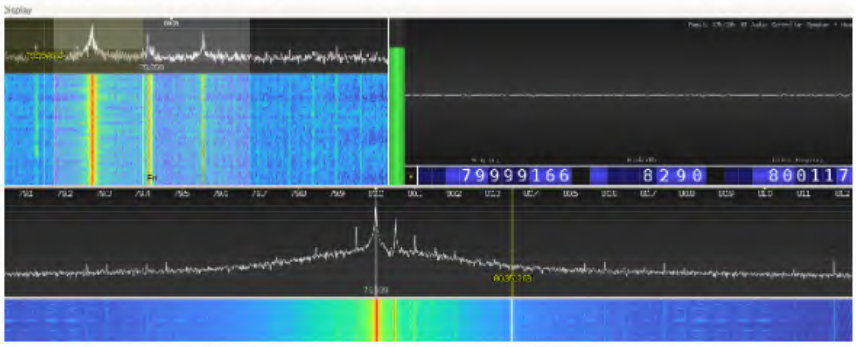
The signal generator found under Utilities can be used to generate a carrier which can be FM modulated with the following waveforms as defined by the Shape function.

- CW : unmodulated carrier
- Sine signal
- triangle signal
- sawtooth up signal
- sawtooth down signal
- square signal
- noise signal

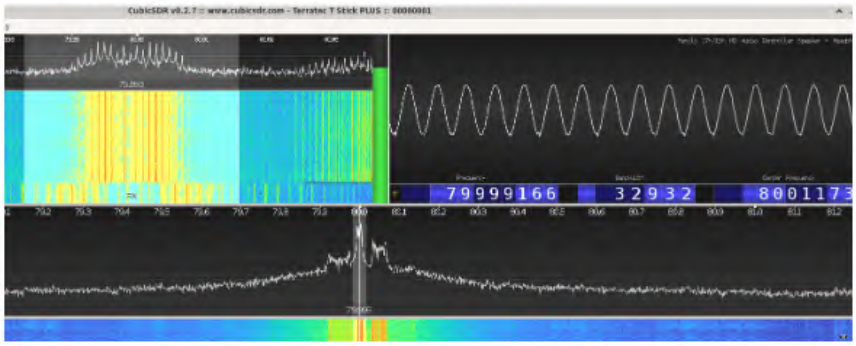
* Sine / Triangle / Sawtooth up / Sawtooth down / Square

We can select the periodic signal to modulate the carrier , in FM .(and we can adjust below the delta FM deviation)

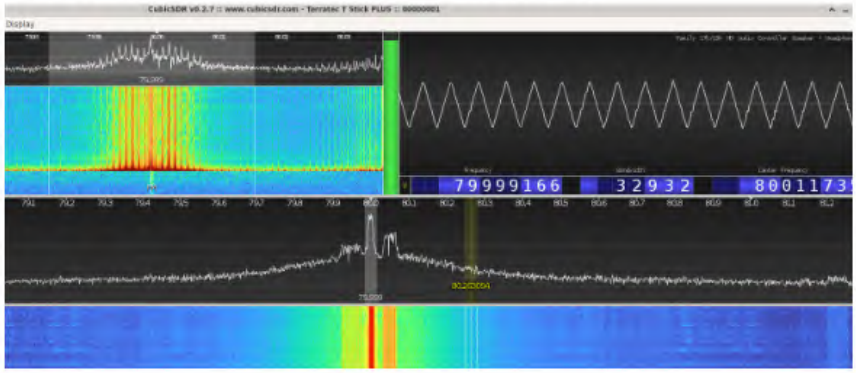
CW (just carrier no modulation)



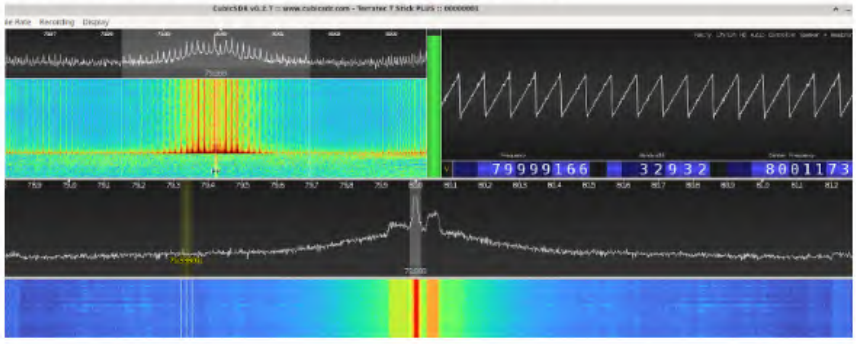
SINE (we can select throught the GUI the tone frequency)



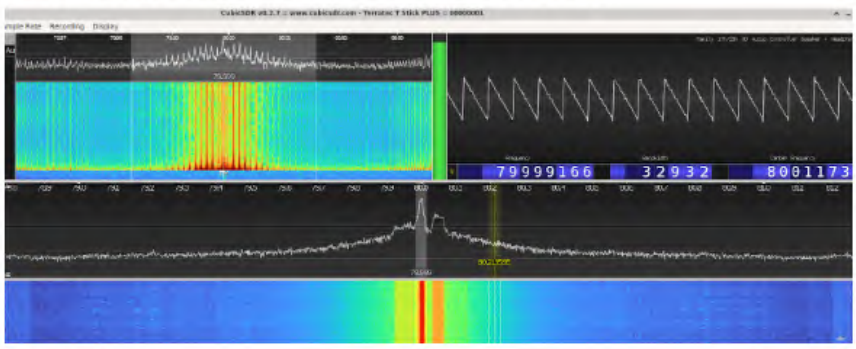
TRIANGLE , (we can select throught the GUI the tone frequency)



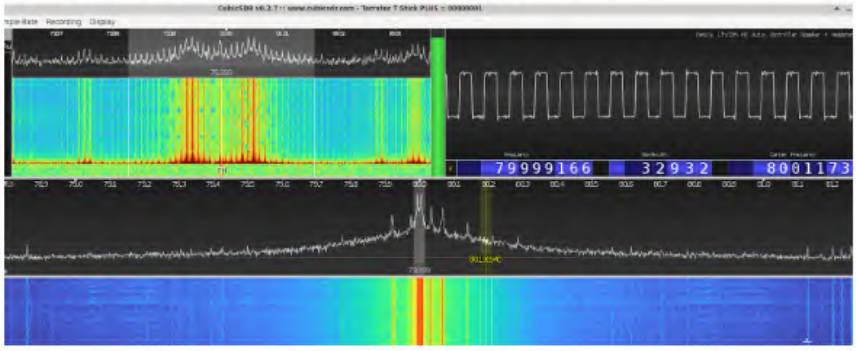
SAW UP. (we can select throught the GUI the tone frequency)



SAW DOWN , (we can select throught the GUI the tone frequency)



SQUARE , (we can select throught the GUI the tone frequency)



Tone defines the frequency of modulation.

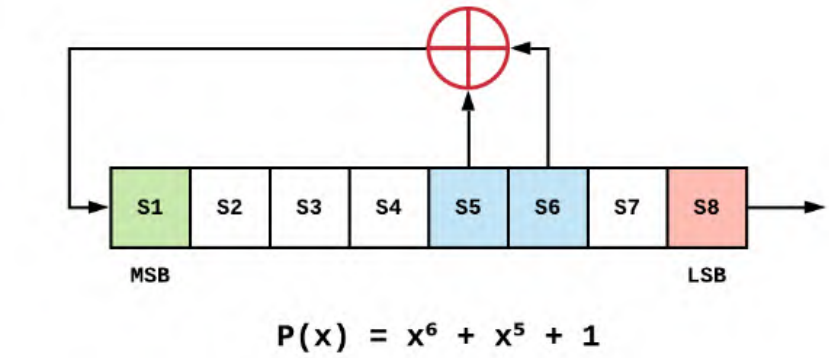
Update when unchecked requires the user to drop carrier, then re-start carrier in order for a change of modulation Shape or Tone frequency to take effect. When checked, values will update on the fly.

Stop after 1s limits carrier duration to 1 second

* White Noise generator options:

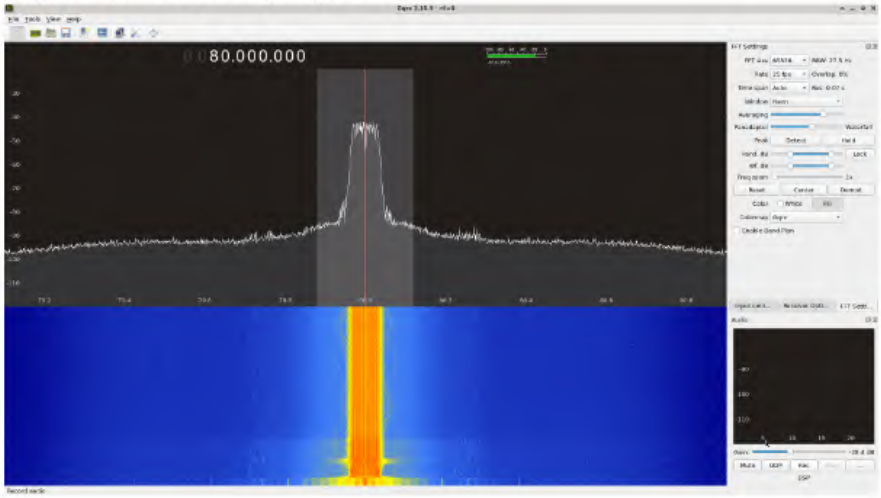
We are generating simulated White Noise ,using pseudo random noise generator, 8 bits linear-feedback shift register (LFSR) algorithm, variant Fibonacci. (Following this wiki link)

Example of the implementation of a 8 bite Noise option

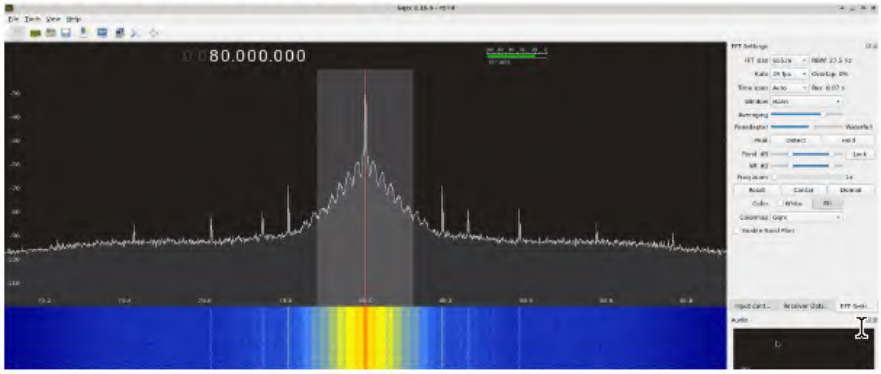


We have introduced only one user option, about Noise generator , using the best LFSR that we tested : 16 bit polynomial feedback LFSR , that has longer random sequence period and produces more continuous spectrum.Using noise generator, we can hear in any FM receiver the random noise (and we can also see the random demodulated signal, as it is attached below) and the peak radiated spectrum power is now just -10 dB's compared to the triangle or saw signal , that is fine (acceptable) . (not -40 or -50 dB's as it was before, really too small) .

TX gain 43 , reference triangle signal

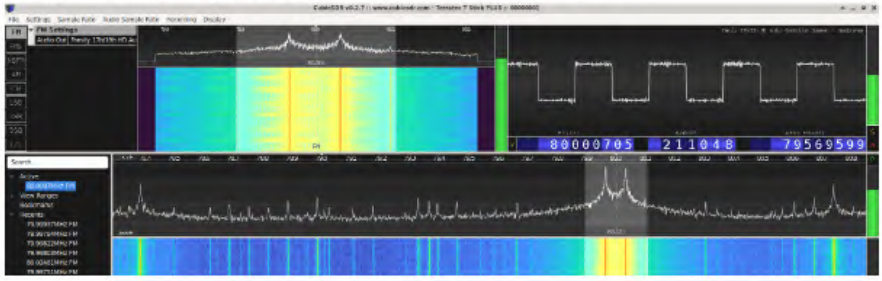


This PR Noise signal , radiated power spectrum

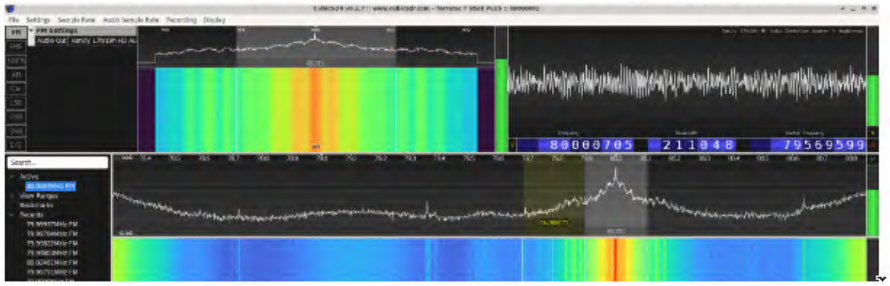


See on top right corner the pseudo random noise demodulated sinal

example, reference square signal , demodulated top right corner



Noise signal , this PR using 16 bit , we can see the demodulated baseband random noise.



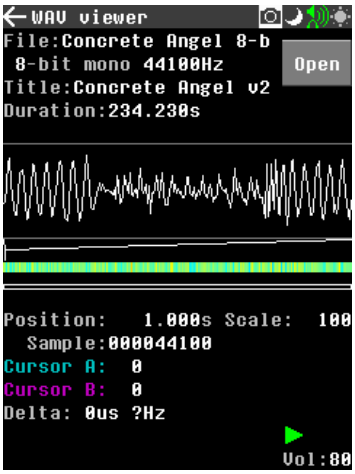
Update when unchecked requires the user to drop carrier, then re-start carrier in order for a change of modulation Shape or Tone frequency to take effect. When checked, values will update on the fly.

Stop after 1s limits carrier duration to 1 second

Wav Viewer

Wav Viewer

The Wav Viewer app can be used to view and play back 8-bit unsigned or 16-bit signed mono WAV files. Sample WAV files may be found in the WAV folder of the SD card, and WAV files captured using the Audio app will be placed in the AUDIO folder of the SD card. Using a PC, WAV files can be created from an existing MP3 file using Audacity or ffmpeg, e.g. `ffmpeg -i lovely_music.mp3 -ar 48000 -ac 1 -acodec pcm_u8 lovely_music.wav`



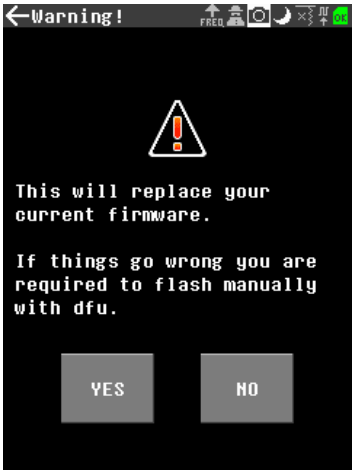
Flash Utility

This application allows you to install a new firmware on your PortaPack. The Flash utility is the update method of choice for users that may not want to run an application on their PC, have compatibility issues with their OS, or may want to switch between firmware versions when in the field.

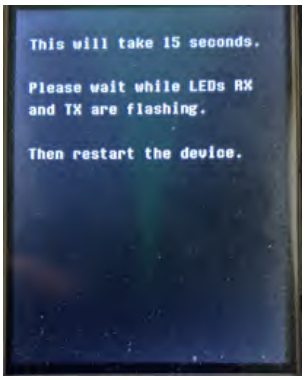
The Flash Utility

- **Step 1:** Compile or download the image. For example the latest nightly build from https://github.com/portapack-mayhem/mayhem-firmware/releases. If you download and unzip the latest mayhem_v#.#.#_COPY_TO_SDCARD.zip contents to your SD card, the latest firmware image will be found in the FIRMWARE folder (this method also updates the external app files in the APPS folder as well as data files needed for other apps).
- **Step 2:** If you download only the file mayhem_v#.#.#_FIRMWARE.zip, extract the portapack-h1_h2-mayhem.bin file and place it in the FIRMWARE folder of your SD card. (The SD card may be physically plugged into your computer, or left installed in the PortaPack using the "SD over USB" app and connected with a USB cable.) See note below regarding external apps.
- **Step 3:** Start the Flash Utility and select the new .bin file.

NOTE: If original firmware running on your portapack is version 1.9.2 or later, it has a Flash Utility that supports ppfw.tar files that contain the firmware image plus all external apps. In this case, you only need to download the one file mayhem_v#.#.#.ppfw.tar and place it in the FIRMWARE folder of your SD card. When you select this file in the newer Flash Utility, the Flash Utility will automatically extract all the external apps to the APPS folder and flash the firmware .bin file.



- Step 4: Select Yes



- Step 5: Watch the LEDs blink and wait the 15 seconds. If your original firmware was version 1.9.0 or later, the portapack will automatically reset itself after the new firmware is installed. Otherwise:
- Step 6: Double press the knob to turn off the portapack.
- Step 7: Press the knob to turn on the portapack. You should now have the new firmware installed.

External apps

The version of any External Apps must match the version of the currently running firmware. If only the main firmware is updated, old external apps in the APPS folder of the SD card will not run. See note in Step 1 above.

If things go wrong

Sometimes something goes wrong and you are in a state where the portapack refuses to turn on again. You should know that no matter what you do, you can always recover from such situation. The portapack has a dfu that can never be deleted / overridden and should be used in this situation: Update-firmware-troubleshooting

Wipe SD card

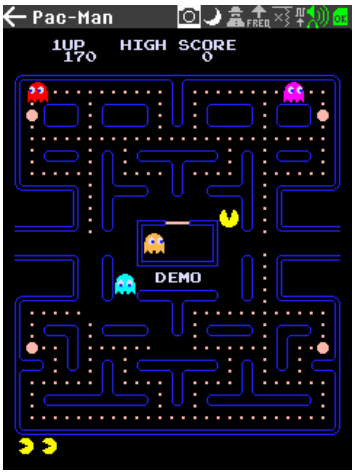
Fast fill 512 random block into your sdcard to destroy all data that it has. Do not use this tool unless you are sure you currently need to destroy all the data and you wanted it not recoverable [1].

Warning: This tool is not for formatting or cleaning sdcard. As long as you wiped your SD Card with this tool, you would need to format it again with a computer or other similar devices (But not your hackrf or portapack) before you can use it again (save things into it).

p.s. [1] ^ This is not a guarantee.

Pac-Man

It's a game. You might have heard of it. When the pac-man eat the big dots, the ghosts become sad face, and you can eat them. Hit Select button to start. Long press back button or long press the title to exit it.



Cheat:
We have cheat mode, find out yourself!

WardriveMap

If you have any Captures that has geotag, this app will show those in a map. While using the app and you have attached an external GPS, it'll move the map while you move. You can also move manually if you change the Lat / Lon, but then GPS won't affect the map's position.

Over the map marker, there is the file name of the capture.

> ⓘNote
> Maximum 30 captures can be viewed at once. You can move the map, or zoom in further to see other captures.

Random password

This app use AFSK demodulated data as random seeds for each char, use LCG + one more random layer as PRNG algorithms to generate passwords.

In theory if the quality of seeds (which is from mostly radio noise) is good enough, then the password randomization would be good enough. But usually they are not, or we don’t know, or they do but not stable. So even if this is more secure than many other PRNG generators, in the best case it even can be considered as TRNG generators, don’t use this at high security scenes, for example money-related things.

All the “send” button/checkbox in this app means send via serial async messages, check serial page in this wiki for more details.

Flood mode is from streaming generated code, this will always streaming into serial, alternatively you can check the savin checkbox to save generated codes and seeds. Keep in mind that with seeds, you can generated same code with proper PRNG, so they are same level of security, don't leak them.

Each shuffle algo and what it can bring you

There are two dimensions of password safety:

- Entropy: When you generate mass of password, it should split evenly in the possible space, that controls password quality. In this app, the only entropy provider is the demodulated AFSK data. the LCG/ sha-512/ shuffle algo won't bring more entropy.
- Randomness: It controls how many total possibilities can be generated. In this app, the only randomness provider is the "each digits using different seed in the buffer" algorithm, which spread the total possible combination into the max value of possibility: (CHARNUMBER)^{DIGITS}.

Algo / Source	Bring Entropy ?	Bring Randomization ?	Bring difficult to reverse calculation ?	Made it harder to Brute-Force ?	Time Complexity and Space Complexity
Use time as seeds to pick a random frequency with LCG to fetch AFSK data	⛔	✅	⛔	⛔	O(1) - O(1)
The original demodulated AFSK data as seeds	✅	⛔	⛔	⛔	O(1) - O(1)
Each digits using different seed in the buffer	✅	⛔	⛔	✅	O(n^DITIGS_NUMBER) - O(n^DITIGS_NUMBER)
The LCG PRNG algo inside of cpp STL	⛔	✅	⛔	⛔	O(n) - O(1)
Shuffle with two groups of seeds	⛔	✅	⛔	✅	O(n) - O(n)
The SHA-512 hash algo	⛔	✅	✅	⛔	O(n) - O(1)
Result	✅ x 2	✅ * 4	✅ * 1	✅ * 2	

Settings

This section provides a set of utilities that can be used to configure some aspects of the PortaPack and are described below. Settings are saved in persistent memory.

Audio

This setting allows adjustment of the following audio parameters:

- Tone Key (CTCSS) mixer setting when transmitting, as a percent of the audio level.
- Audio Beep on speaker/headphone in certain apps when receiving a data packet.

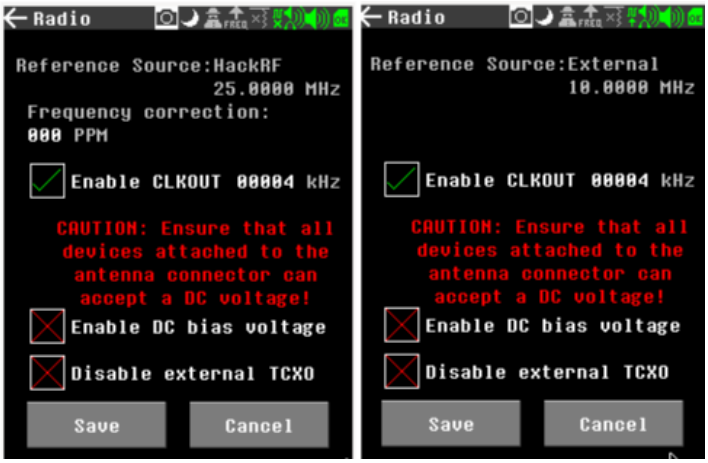
Radio

In the radio section there are three options,

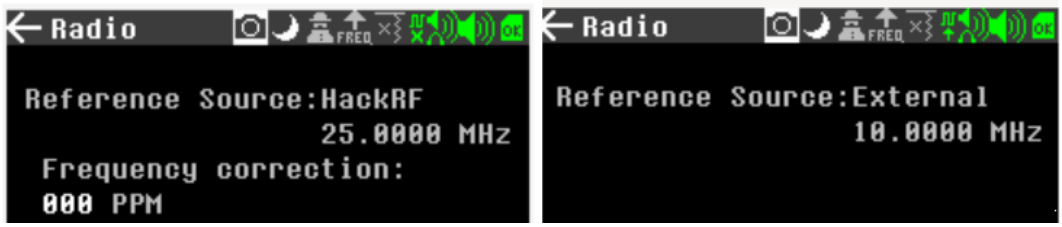
1. Enable/disable the Clock Output. (it can be activated / deactivated by top title bar (CLKout icon) : green icon means activated, or thought that radio menu (check-box)

   Note 1 : In r9 Hackrf platform , due to our complex fw Architecture and usage of Si5351A , we have fixed the synthetized CLK out freq to 10Mhz.

   Note 2 : In all previous r1 to r8 Hackrf platforms , as we are using Si5351C, we do not have that limitation , and user can change the CLKOUT frequency between 4 kHz to 60000 kHz; press OK when the frequency is highlighted to select which digit position to modify and then use the encoder to scroll through the digit values. (it works with both clock references, the internal Hackrf (25Mhz) and the external -when available- from Portapack (TCXO 10Mhz). Once enabled the CLK_out , the new introduced frequency will be updated to the CLK_out port, as soon as you press below SAVE button.

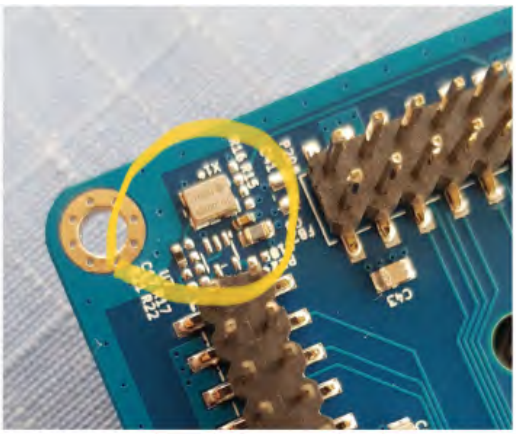


Note 3 : Zooming previous picture , when the unit detects that external CLOCK_in -usually 10Mhz reference- (from Portapack or from external source) , it is indicated in the top title CLK_in icon with some top arrow below the icon (right picture) . In case of no detection , it is indicated with some "X" below the icon (left picture),and in that case, the system takes the internal 25Mhz Hackrf clock reference.



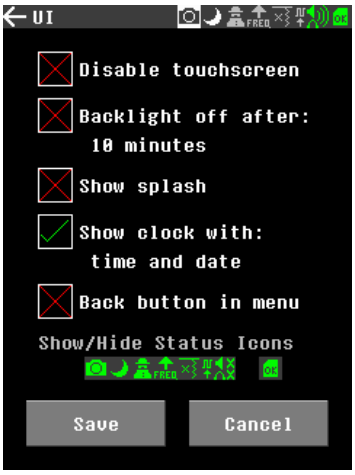
Warning note : be awared that some of current market Portapack boards may have an integrated low ppm TCXO 10Mhz clock generator mounted, and when it is built in, it is connected in parallel to the external Hackrf CLK_in port connector. So in that special case , that internal PP clock signal is present always in the SMA CLK_in connector (this s a strange case, because in those devices, CLK_in is behaving as real embedded ref. output of internal TCXO 10Mhz clock) , and you should better not connect any other external signal generator there (unless you dissassembly the Portapack from Hackrf) , because otherwise, you will connect two clock signal generators in parallel -the embedded one to the external one -, and you may damage that Portapack TCXO clock IC circuit.

Here below , you can see two different examples of the embedded TCXO 10Mhz ref. clock, in a PP H1 brd (left side) , PP H2 brd (right side) boards :



2. Enable/disable the Antenna Bias voltage. (it can be activated / deactivated by top title bar (DC bias icon) : green icon means activated, or thought that radio menu (check-box) . If enabled, ensure that all devices attached to the antenna connector can accept a DC bias voltage.
3. Enable/disable the External TCXO Clock input. (it can be activated / deactivated by that radio menu (check-box). Sometimes, in low battery charge voltage, or other low output TCXO voltage amplitude (much lower than the expected 3.3V pk-pk from ground) , we may have some boot problems with that external TCXO signal and in that case, we may want to deactivate it.

User Interface



The UI interface setting for the following can be Enabled (tick) or Disabled (x) or selected value for the backlight timeout:

- Touchscreen can be enabled or disabled.
- Backlight off after 5,15,30 seconds, 1,3,5,10 minutes, or never (default).
- Show the Splash screen at power-up.
- Show the clock - Selects whether to display date and time on the home screen (update by moving the cursor to the select item and use the rotary knob to adjust the value).
- Back button in menu - Enables a "Back" button on all menu screens.
- Show/Hide Status Icons - Select which status bar icons are visible or hidden.

Date/Time

Set the date and time which will appear on the home screen (if enabled), in log entries, and file time stamps. A coin cell is required to keep the time updated when the PortaPack is off. If the coin cell battery is dead/missing but there is an SD card, the date will be advanced by 1 day every time the Portapack is rebooted, so that log entries/files will be in chronologically ascending order.

If Daylight Savings Time (DST) is enabled, the time is advanced by one hour during the indicated date range specified as the Nth Day-of-Week in Nth Month (note that the time displayed on this screen is assumed to already be corrected for DST so the time entered should be the same as appears on other clocks). To learn the Daylight Savings Time date range for your area, see Wikipedia Daylight Savings Time By Country. The precise *hour* of the time change is as shown on the screen and is not configurable.

Note that it takes about a second to save the time when the Save button is pressed. Daylight Savings Time is supported in firmware version 2.0.0 or higher.

Calibration

This provides an app for the calibration of the touch screen and alignment by following on screen instruction.

You have to keep pressed for at least a second on each target for the app to guess the touch area correctly and show next target on release.

Touchscreen Threshold

The touchscreen's resistance detection layer can be eventually wore out (it's inside the soft layer so use screen protector won't slow it down) by using it, or it's originally bad quality, so you maybe need to tune the threshold if you can't touch an area, or some region are kept pressing even if you are not pressing it (which causes the back light keeps on forever because the device think you are keep touching the screen)

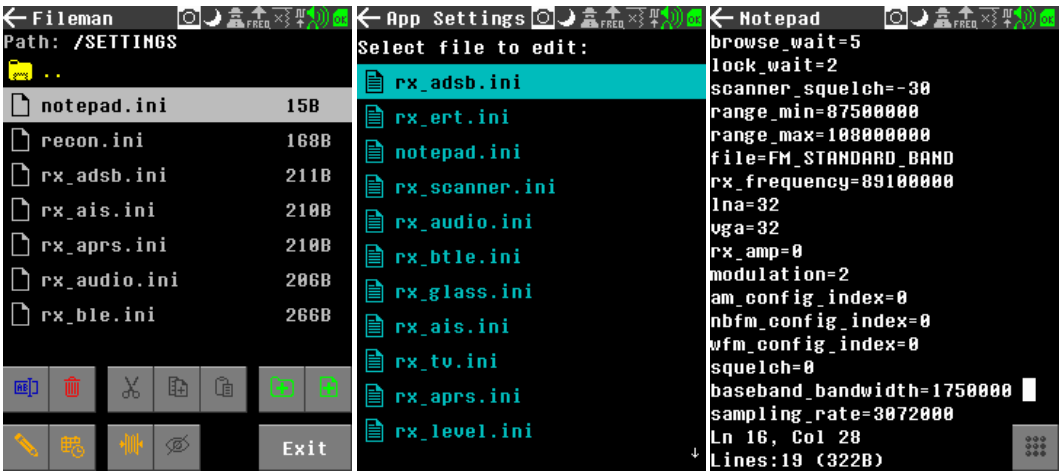
In the best case the threshold should be 1, but considering the most case that the layer already kind of damaged, we default it to 32.

If you are having issues listed above, just press Auto detect, and follow the guide, and it will automatically tune to a value that good for your device.

When auto detecting, don't touch the screen, until count down finished. otherwise it will give you a bad value. But don't worry if you mistakenly touched, just need to start over and nothing bad would happen.

App Settings

Settings for each app are saved in corresponding .ini files in the /SETTINGS folder to maintain persistence, if a formatted SD card is installed. An updated .ini file is saved whenever the app is closed. To reset an app to default settings, the corresponding .ini file may be safely deleted and a new file will be created automatically when the app is subsequently executed. Alternatively, individual lines in the file may be deleted to reset only a subset of application settings. For debug purposes, note that some additional configuration settings may be found in the .ini file that are not configurable in the app itself.

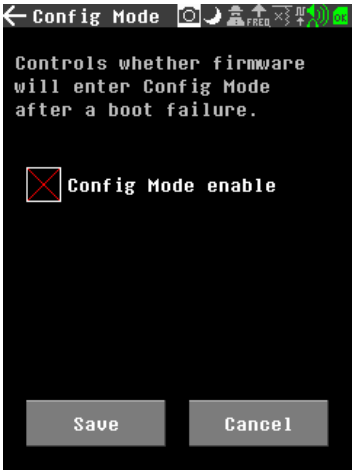


blacklist

To disable specific apps completely, a text file named "blacklist" can be created manually in the SETTINGS folder using the Notepad application. Unwanted applications should be listed in this file using their case-sensitive application name (text that appears under the app's screen icon), and they will be disabled (hidden) effective on the next boot. List one application per line. (Requires 1.8.0+ firmware and an SD card)

Config Mode

In some cases a PortaPack may start up intermittently in Config Menu mode, such as when the power button is pressed twice rapidly, or if a little electrical noise occurs when a USB cable is attached. If this occurs frequently (dark screen and blinking LEDs), the Config Menu code can be disabled using the Settings -> Config Mode app (which sets a flag in persistent memory to disable Config Menu activation).



Converter

Set up convert or down convert mode.

Widgets:

- show / hide icon, hiding will also disable any up / down conversion
- enable / disable converter
- (+) or (-) set the offset sign
- set the offset

When using an upconverter it's common to use an offset to access the correct frequency. As an example, if you want to use a HamItUp which is designed to listen from 60KHz to 30MHz, you'll need to tune your portapack to 125 MHz (or any other frequency used in the upconverter local oscillator) + the frequency you need.

Doing the calculation and tuning while adding the frequencies can be a bit tedious. Don't worry: just got into your portapack's settings, Radio menu, and set the shifting you need. You can set up conversion (+) or down conversion (-) in the Settings/Converter menu.

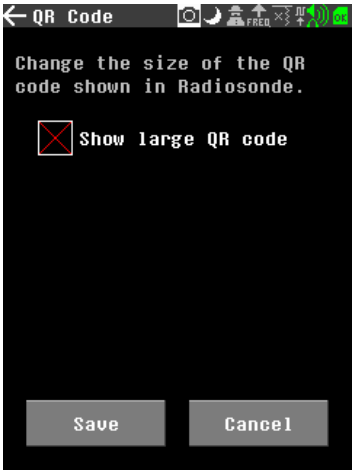
When the option is on, the displayed frequency is the one you want to tune in, and the real tuned frequency is displayed frequency plus or minus offset. When the option is off, the displayed frequency is the one you want to tune in, and the real tuned frequency is the displayed frequency.

You can turn it on and off using the checkbox while in Radio menu, or using the top bar icon 'Freq', with an arrow telling you if it's up or down conversion.

Note: This has the same effect as using the top bar 'Freq' icon. While in the radio menu, the synchronisation of the top bar 'Freq' status and the checkbox is not implemented when toggling the top bar 'up' icon. The status is saved, and the last to talk is setting the status.

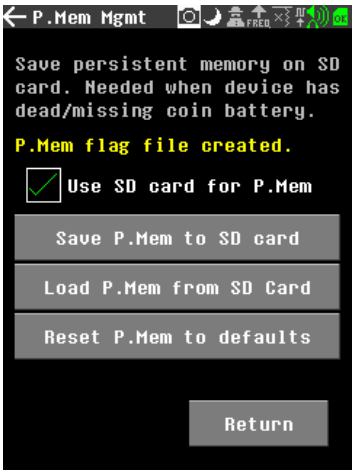
QR code

Set the size of the displayed QR code in the RadioSonde app. (As of the n_240322 build, the regular QR code is displayed larger and this settings screen is no longer available)



P.Memory Mgmt

Set persistent memory options.

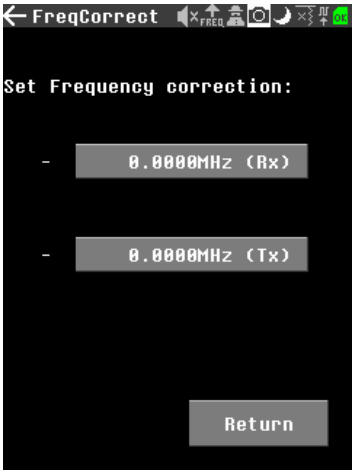


There are 256 bytes of persistent memory where settings are saved when there is a working coin battery. Note that a dead/missing coin battery will not prevent startup or display any messages, but settings will be lost after a power cycle. To prevent this, settings may be stored in a file on the SD card versus in the persistent memory, if enabled. Widgets:

- use sdcard for pmem: if checked the firmware will try to load last saved settings at startup. The checkbox is configuring a flag file under SETTINGS for it to work without coin battery.
- save p.mem to sdcard : save actual persistent memory onto the sdcard
- load p.mem from sdcard : manually load persistent memory from sdcard
- !reset p.mem, load defaults! : reset the persistent memory to defaults

FreqCorrect

Set TX and or RX Frequency correction in Hz.



A value between [-4,+4] MHz of correction is accepted, else it's truncated due to the variable used in persistent memory.

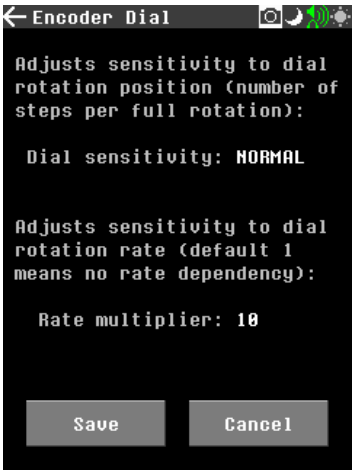
Use the '+' or '-' filed to change to correction mode (addition or subtraction).

Use the MHz RX and MHz TX field to set the correction in each mode.

Settings are automatically saved in persistent memory.

Encoder Dial

Allows the sensitivity of the encoder dial position between Low, Normal, and High (this adjusts the number of steps for a full rotation). The rotation rate multiplier adjusts the number of steps that occur when the dial is rotated faster, for faster scrolling through frequencies, file lists, volume setting, etc.



SD Card

Enables higher speed access to the SD card (only works on higher-speed SD card models).

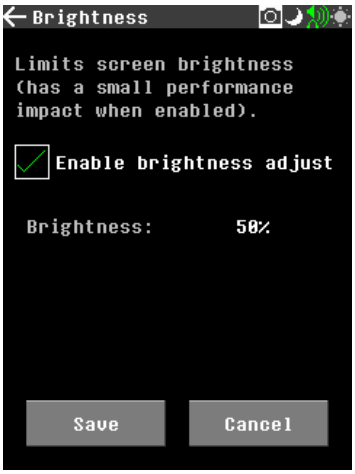
Use the Test button to try it before saving this setting in persistent memory. Files may not be read or written properly if this is enabled on a slower SD card.

Brightness

It's not really changing the voltage of LED backlight, but use a "cover layout" like those brightness adjustments android app do (actually it's changing all the rendering color but I was just make it sounds more clear). So don't expect image quality but it indeed saves some eyesight in night. Brightness may also be adjusted by clicking the brightness icon on the status bar.

what if you enabled dark brightness and now in sunlight and can't see the screen?

The brightness icon is the most top-right button on screen, thus you can: boot, press many times right and up arrow button, then press center button, so you can adjust the brightness even if you can't see the screen.



Menu Color

The Menu Color app can be used to change the background color scheme of the app menu buttons from the default grey to suit your preference.

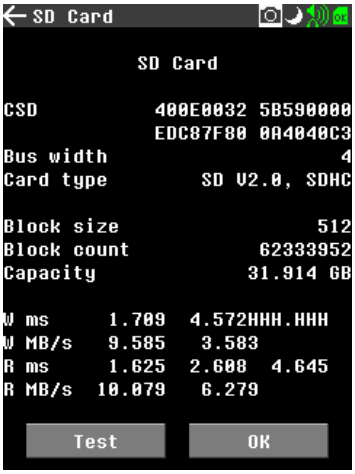
Debug

Memory Usage

Gives the information on the memory used by M0 core.

SD Card

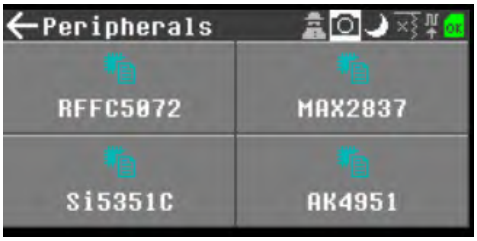
Gives information on the SD card and allows it to be tested.

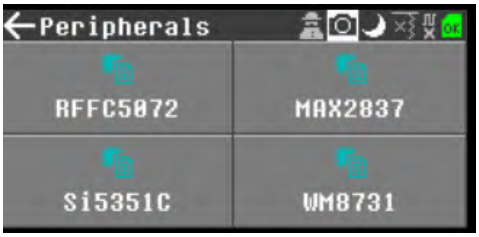


Peripherals

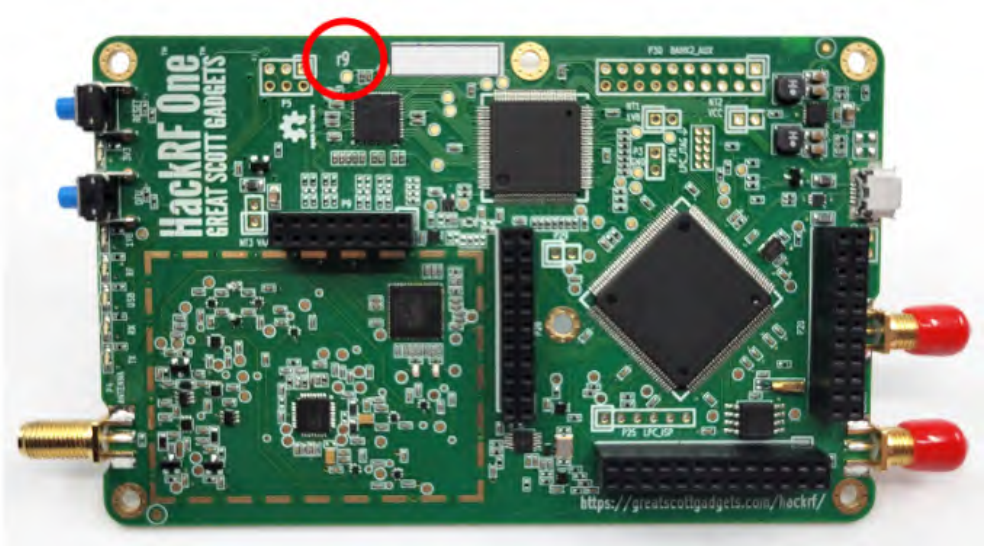
Gives information on the peripherals:

- RFFC5072
- MAX2837
- SI5351C
- WM8731 or Ak4951 (depending on the IC audio codec detected in your PP brd)





Note : Recently (Manufacturing year: 2023) GSG introduced the new r9 Hackrf board version (already compatible with Hackrf and Portapack-Mayhem fw's).



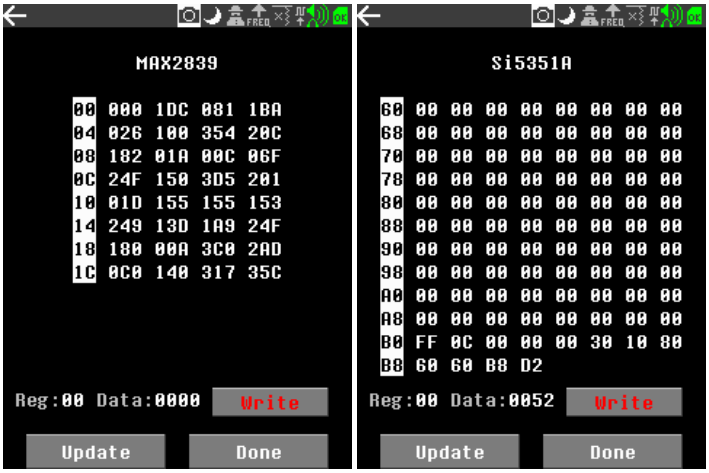
That new Hackrf board revision r9 has two 2 IC's changes:

- MAX2837 was replaced by MAX2839.
- Si5351C was replaced by Si5351A with additional clock distribution. A series diode was added to the antenna port power supply.

Starting with HackRF One r6, hardware revisions are detected by firmware and reported by hackrf_info.

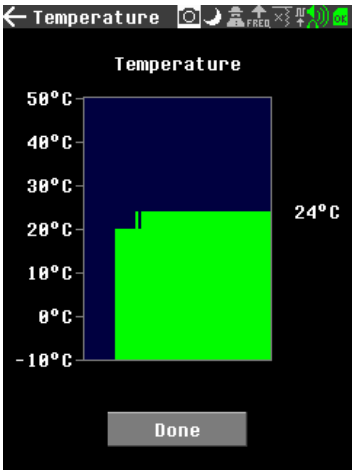
Thanks to GSG developers and our Mayhem git admin , we merged their commit about all those r9 hw support in our Portapack Mayhem Debug menu tool. And now you can also easily detect that r9 version without disassembling the boards :

Individual registers of each peripheral IC can be read or written with this application. If the peripheral has more registers than fits on the screen, the encoder dial can be turned when the Update button is highlighted to view the additional registers. Care should be taken when writing, as it may be possible to cause hardware damage by writing to some memory locations.



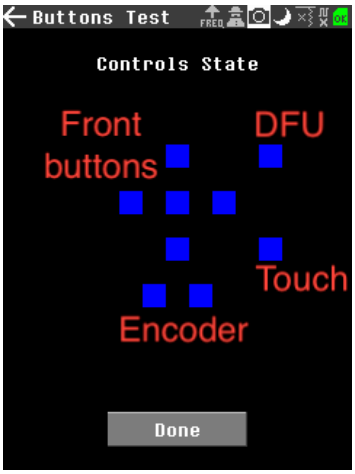
Temperature

Data is provided by the MAX 2837 (or MAX 2839) on chip digital temperature sensor. The accuracy is quoted as 4.33°C per value.



Buttons Test

This shows when either the buttons are pressed, the encode knob is turned or the screen is touched. It can also show if the encoder when turned is cleanly stepping the states as it is turned. Encoder sensitivity is now adjustable in Settings, and the encoder can be desoldered and replaced with a better-quality version if it has issues. The test screen also has an option for testing the "long press" feature which is applicable to the directional keys and the DFU switch only.



Touch Test

Allows testing the Touch Screen calibration (and your artistic skill) by drawing on the screen using a stylus.

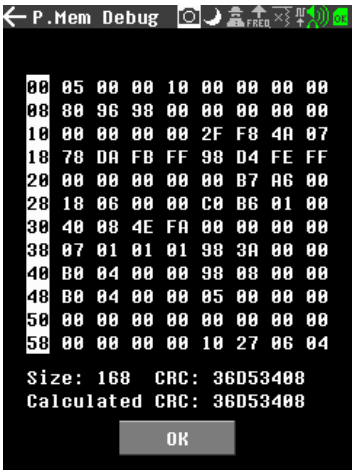
The following controls are available:

- Select key returns to Debug menu.
- Left key changes the pen to a random color (hold in the button to rotate through them faster); this can also be done while drawing.
- Down key clears the screen to a random color (like shaking your Etch-a-Sketch).
- Turning the Encoder dial changes the pen size.

To save your masterpiece, note that the screen-shot icon is still active but hidden (it will become visible if that precise spot of the Touch Screen is pressed). Try the Settings -> Touch app for improving calibration of your touchscreen.

Pers. Memory

Displays the contents of the persistent memory area. (256 bytes)



It is split into three pages, pages can be changes with the encoder and the current offset from the start of p.mem area is displayed in the left column.

At the bottom it displays also the current size of the data_t struct (this is what we persist into p.mem) and the currently stored checksum (it is calculated from the first 252 bytes of the p.mem area when changes are made to the settings and then written to the last 4 bytes of p.mem)

The version of the stored config isn't displayed separately but it can be seen as the first 4 bytes of the p.mem area.

Debug Dump

Writes a file containing debug information to the DEBUG folder.

Memory Dump

Allows a region of memory to be saved to a file in the DEBUG folder in hexadecimal ASCII format, and allows direct read/write access to specified memory locations for debug purposes. Memory addresses should be a multiple of 4 to avoid causing a fault. Care should be taken when writing, as it may be possible to cause hardware damage by writing to some memory addresses.

M0 Stack Dump

Writes a file containing M0 stack contents to the DEBUG folder.

Font Viewer

Displays the 5x8 and 8x16 font character sets.

Audio Test

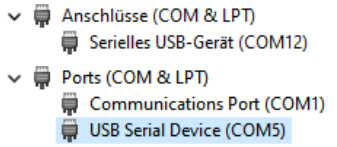
Generates a sine wave beep of the specified frequency and duration (0 means an infinite duration) to test the audio output and speaker/headphones frequency response.

HackRF Mode

This allows the PortaPack controls to be bypased and enable the control via USB directly to the HackRF. The menu option offers a button to switch to HackRF mode. When this mode is seleced a blue Screen showing GNU Block Diagram is shown. To come out of this mode, the reset button needs to be pressed.

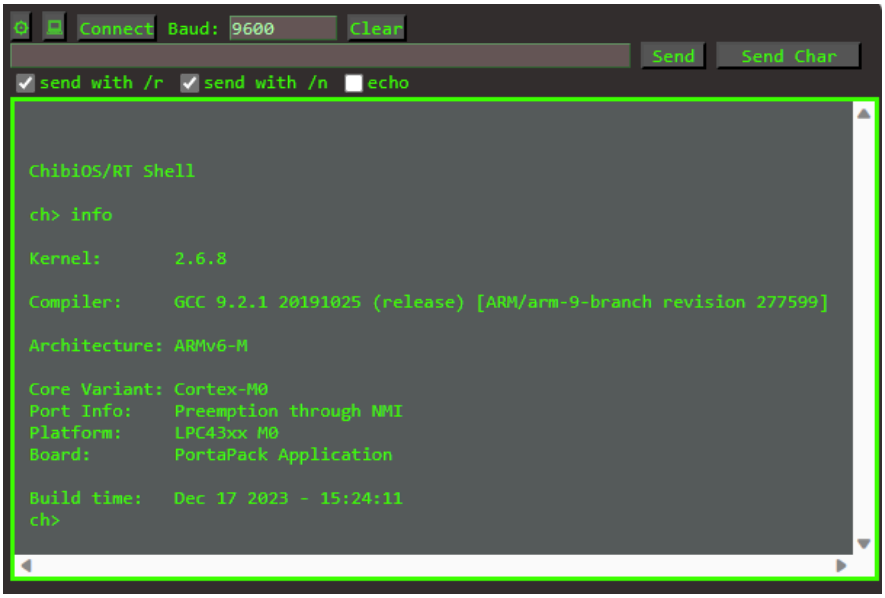
USB Serial Console

The PortaPack Mayhem firmware exposes a serial console via USB when connected to a computer.



Any serial terminal client can be used to connect like PuTTY, minicom, screen, HTerm. There are even web based ones (Chrome&Edge, no Firefox): https://www.serialterminal.com/ or **https://hackrf.app/**

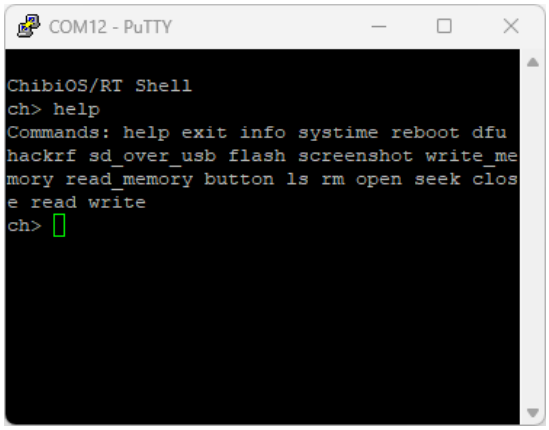
The terminal exposes the ChibiOS/RT Shell:



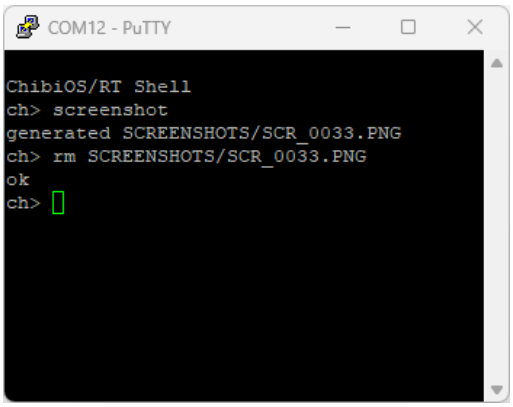
You SHOULD NOT enter HackRF mode (AKA the mode with blue screen) when using the serial console, whether with PWA app (hackrf.app) or other serial tools. That saying, you need to keep your portapack on but in normal mode (instead of entering hackrf mode) to use it.

Available Commands

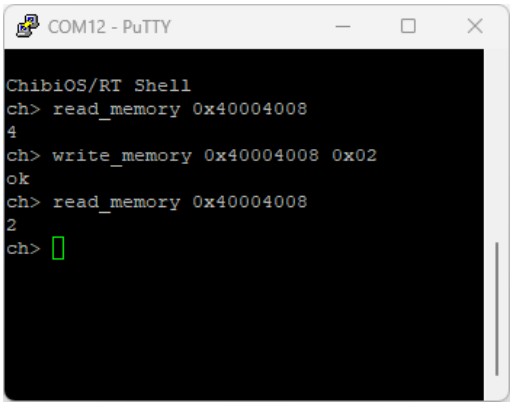
- `help`: lists all available commands.



- `info`: shows the ChibiOS/RT system details.
- `systime`: shows the uptime in ms.
- `reboot`: reboots the PortaPack. This will also work on devices where the reset button is not working.
- `dfu`: reboots the PortaPack into DFU firmware upgrade mode.
- `hackrf`: Starts the original HackHF firmware to use the PortaPack as HackHF.
- `sd_over_usb`: Starts the SD Over USB mode.
- `flash`: This is the Flash Utility.
- `screenshot`: Takes a screenshot.



- `cmd_screenframe`: Replies with the screen's content. Format is 1 line / screen line, and for each pixel HEX (2 char) in the R,G,B order. So one line will be 720 + newline.
- `cmd_screenframeshort`: Replies with the screen's content. Format is 1 line / screen line, and for each pixel you'll get 1 character. Format is '00RRGGBB' + 32. So for black you'll get 32 (' '). For white 95 ('_').
- `gotgps`: You can send apps your current position. Format `gotgps lat lon <alt> <speed> <satinuse>`. Lat, lon is mandantory with '.' as a decimal separator.
- `gotorientation`: You can send apps your current orientation. Format `gotorientation angle`. Send only integer, where 0 mean North, 90 East, 400 mean 'not set'.
- `applist`: Shows the apps that can be started with `appstart` command. You'll get 3 parameters per line: app short name (you'll need to use this with appstart), app's full name, and app category.
- `appstart`: You can start apps from the list given by the `applist` command. 1 paremeter needed, the app's short name. It'll stop any running apps.
- `write_memory`: Writes arbitrary memory locations.



- `read_memory`: Reads arbitrary memory locations.
- `button`: Simulates a button press
  - button 1: Right
  - button 2: Left
  - button 3: Down
  - button 4: Up
  - button 5: Select/Enter
  - button 6: DFU
  - button 7: Rotary Left
  - button 8: Rotary Right
- `touch`: Emulates touch event (press + release). Need to pass the x y coordinates of the event, and 0 < x < screen_width, 0 < y < screen_height must be met.
- `keyboard`: Emulates keypress event for the supported widgets. One parameter must be a string that has the HEX (2 char) representation of the desired key. You can send multiple characters at once. Backspace is 08. "Hello world" sent in one command: `keyboard 48656C6C6F20776F726C64`.
- `ls`: Lists files and directories.
- `mkdir`: Creates a directory.
- `unlink`: Deletes a file.
- `fopen`: Opens a file for reading and modification.

> Note
> The current position will be set to the end of the file. Use `fseek 0` to move to the start of the file.

- `fseek`: Sets the current position inside the currently opened file.
- `fclose`: Closes the currently opened file.
- `ftruncate`: Removes all content in the file behind the current position.
- `ftell`: Shows the current position is the file.
- `fread`: Reads n bytes from the currently opened file.

> Tip
> there is a faster binary read option: `frb`

- `fwrite`: Writes bytes from the currently opened file.

```
ChibiOS/RT Shell
ch> open /APPS/pacman.ppma
ch> seek 0
ch> read 64
000008107D34081001000000722596F7
5061632D4D616E00000000000000000000
00000000C007E00FF01FF807F8017800
F801F807F01FE00FC007000000000000
ch> seek 0
ch> write 000008107D34081001000000722596F7
ch> write 000008107D34081001000000722596F7
ch> write 000008107D34081001000000722596F7
ch> write 000008107D34081001000000722596F7
ch> seek 0
ch> read 64
000008107D34081001000000722596F7
000008107D34081001000000722596F7
000008107D34081001000000722596F7
000008107D34081001000000722596F7
```

> Tip
> there is a faster binary write option: `fwb`

- `pmemreset`: Sets all values in PMEM to default. Pass the "yes" as a parameter, that indicates you know what are you doing.
- `settingsreset`: Deletes all INI files from settings folder, resetting app settings. Pass the "yes" as a parameter, that indicates you know what are you doing.
- `sysinfo`: show system hardware informations.

```
ch>sysinfo
M0 heap: 32400
M0 stack: 407
M0 cpu%: 0
M4 heap: 0
M4 stack: 0
M0 cpu%: 0
M4 miss: 0
uptime: 15
ch>
```

- `radioinfo`: show radio settings.

```
ch>radioinfo
receiver_model.target_frequency: 1090000000
receiver_model.baseband_bandwidth: 1750000
receiver_model.sampling_rate: 3072000
receiver_model.modulation: 1
receiver_model.am_configuration: 0
receiver_model.nbfm_configuration: 0
receiver_model.wfm_configuration: 0
transmitter_model.target_frequency: 1090000000
transmitter_model.baseband_bandwidth: 1750000
transmitter_model.sampling_rate: 3072000
ch>
```

- `sendpocsag`: Opens the Pocsag TX app, and sends a message defined in the command.

```
addr and msglen is mandatory, other parameters has a default value.
After you send this message, there will be a prompt `send <mgslen> bytes`. then you need to send JUST that amount of bytes that will be the message.
The Pocsag TX app will start, set the desired options, and send the message.
```

- `setfreq`: Set the radio frequency.

Parameter: target frequency in HZ.
Only works in the following RX apps: Audio, Capture, ERT, Pocsag, APRS, Level, Looking Glass, Sonde, SubGHZd, Weather.
Not supported in other apps that are using frequency range, or automatically set / hopping frequencies.