

# Software Defined Radio

Signal Hacking

# Thank you to our sponsors!



# Who Am I?

My name is **Darren Hale**.

I create software.

I'm easy to find online:

- LinkedIn: <https://linkedin.com/in/darrenhale>
- GitHub: <https://github.com/haled>
- Email: [darren.e.hale@gmail.com](mailto:darren.e.hale@gmail.com)

# What Is It?

“Software-defined radio (SDR) is a radio communication system where components that have been traditionally implemented in hardware (e.g. mixers, filters, amplifiers, modulators/demodulators, detectors, etc.) are instead implemented by means of software on a personal computer or embedded system.”

-- Wikipedia

# Tuning/VFO

- Most radios use a Variable Frequency Oscillator (VFO), or tuning knob, to adjust the signal being taken in by the radio.
- Usually implemented with capacitors and inductors to allow the user to adjust frequencies over a given range.
- Tuning range is limited by hardware components used.

# Signal Modulation/Demodulation

- Need to translate data into a radio frequency (modulation)
- Need to translate data out of a radio frequency (demodulation)
- Use a carrier wave to send data
  - Determined using the VFO
- Accomplished with hardware components
  - Different components for different modulation schemes
- Modulation and demodulation allow amplification to push the signal farther

# Signal Filtering

- Filtering ensures clean signals
  - Eliminate harmonics and isolate data
- Filter at the carrier and modulation frequencies
- Allows for amplification at the receiving end.
- For transmission, HAS to be done at exit point.

# Physical Radio (TS-850)





# But... What IS SDR?

Software Defined Radio is a combination of minimal radio hardware connected to a computer. The computer does the majority of the work!



# RTL-SDR

- Hardware dongle originally created as a cheap digital TV tuner.
- CHEAP!
  - \$30 - \$40 on Amazon
- Large tunable range (500 kHz - 1.75 GHz)



# My Original Kit



# Building Blocks

## GnuRadio

- C-based package to build “radios” with visual building blocks.
- Generates Python code/programs.

## SoapySDR

- Software abstraction layer for hardware
- Provides common API to access different hardware devices

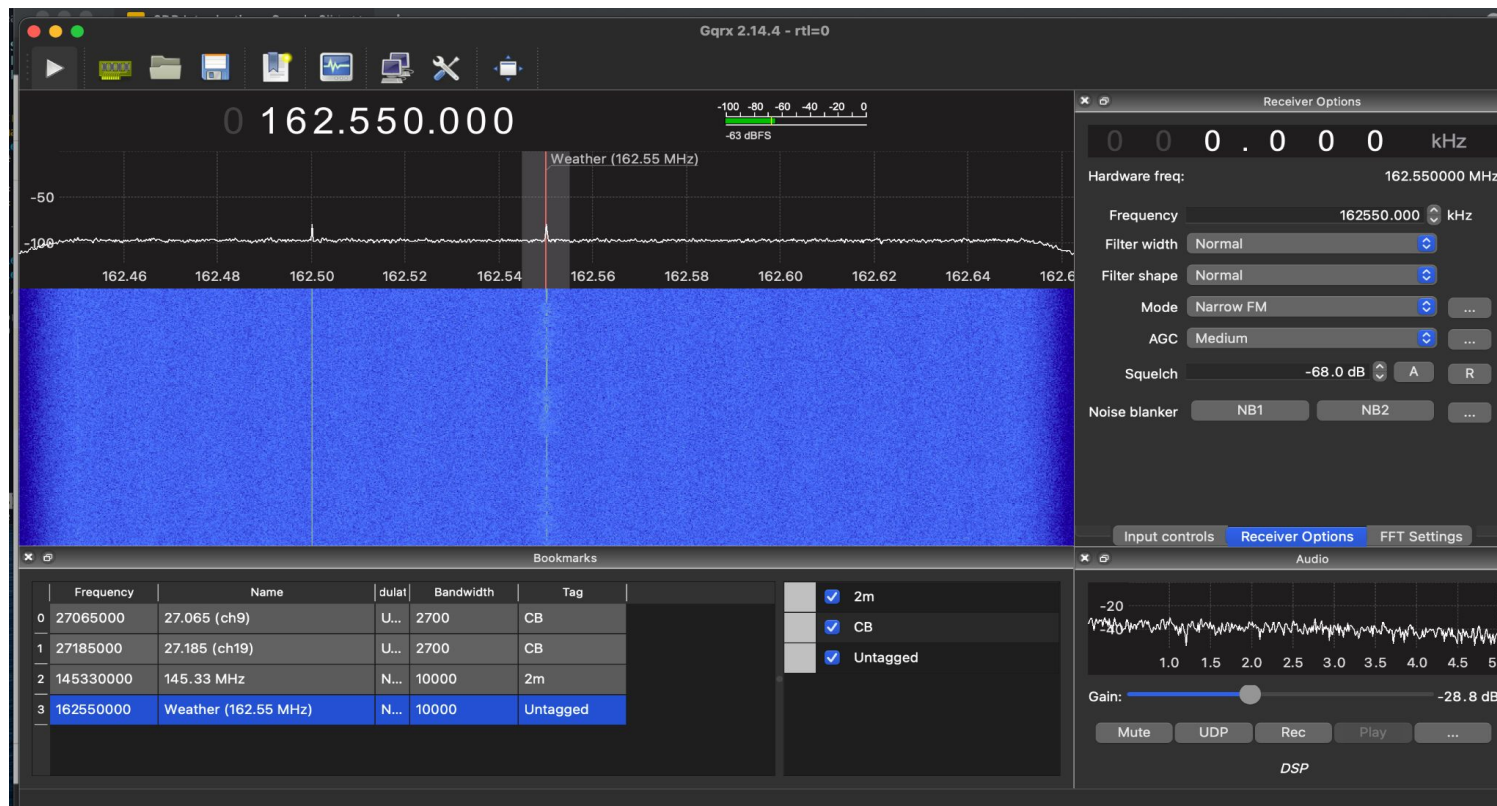
# Software

- GQRX
- CubicSDR
- SDR#
- SDRAngel
- Universal Radio Hacker (URH)
- DragonOS

# GQRX - Broadcast FM



# GQRX - NOAA Weather



# Signals to Play With

- CB
- Walkie Talkies
- NOAA Weather Radio
- NOAA Satellite Images
- Transmissions bounced off the ISS.
- ADS-B Aircraft Tracking
- Airport Tower Traffic
- Emergency Services
- Key FOBs
- Garage Door Openers
- etc.



# Note About Antennas

- The supplied “rabbit ears” are sufficient for most signals.
- You may have to adjust the length or orientation.
- Specialized antennas may be necessary for specific signals.

But I'm *REALLY* Cheap!

<https://www.websdr.org>

# Example Online Radio

View: ☐ all bands ☐ others slow ☒ one band ☐ blind Allow keyboard: ☐ Waterfall: ☐ Java ☒ HTML5 Sound: ☐ Java ☒ HTML5 Chrome Audio



BAND: MW-160 80m 40m 30m 25m 20m 15m **10m**

FREQUENCY: **27947.63** kHz. VFO: A/B A=B

[HURRICANE WATCH NET](#) Main: **7.268 kHz** Secondary: **14.325 kHz**

TUNE: <<< << < >< > >> >>>

MODE: CW LSB USB **AM** FM

FILTER: 6.91kHz @ 0dB; 7.00kHz @ -6dB; 7.46kHz @ -60dB. [-3.46 / 3.45]

>>Narrower<< 3 kHz 5 kHz 7 kHz 10 kHz <<Wider>>

PassBand Tuning (PBT) Control:

Waterfall view: ☒ Full window

Zoom out Zoom in

Max out Max in

RX signal to Center

Or use scroll wheel and dragging on waterfall.

View: waterfall Size: normal Speed: medium

☐ Hide labels

Time **01:50 UTC - 20:50 LOCA**

Solar Activity Monitor:



☐ Mute ☐ Squelch ☐ Auto-notch ☐ Notch-2

**Audio** VOLUME:

Audio out: ☐ Left ☒ Both ☐ Right

DSP Noise Reduction: Off ☐ High-Boost

GAIN CONTROL: ☒ automatic ☐ manual

Gain:

E-Field @ Washington DC Area (VLF 0-20kHz)

# Example Online Radio - Explained

Waterfall

CB

Band

Frequency

Demod Mode

The screenshot shows a web-based radio interface. At the top, there are view options: 'all bands', 'others slow', 'one band' (selected), and 'blind'. There are also checkboxes for 'Allow keyboard' and 'Waterfall' (set to 'HTML5'). Sound options include 'Java' and 'HTML5' (selected), with a 'Chrome Audio' button. The main display is a waterfall plot showing frequency from 27000 to 28900 kHz. A red circle highlights a cluster of signals around 27900 kHz, labeled 'CB'. Below the waterfall, a 'BAND' selector shows 'MW-160', '80m', '40m', '30m', '25m', '20m', '15m', and '10m' (selected), labeled 'Band'. The 'FREQUENCY' display shows '27947.63' kHz, labeled 'Frequency'. Below this, the 'HURRICANE WATCH NET' is shown with 'Main: 7.268 kHz' and 'Secondary: 14.325 kHz'. A 'TUNE' section has buttons for '<<<', '<<', '<', '>|<', '>', '>>', and '>>>'. The 'MODE' section has buttons for 'CW', 'LSB', 'USB', 'AM' (selected), and 'FM', labeled 'Demod Mode'. Below the mode buttons, the 'FILTER' section shows '6.91kHz @ 0dB; 7.00kHz @ -6dB; 7.46kHz @ -60dB. [-3.46 / 3.45]'. There are buttons for '>>Narrower<<', '3 kHz', '5 kHz', '7 kHz', '10 kHz', and '<<Wider>>'. At the bottom left, it says 'PassBand Tuning (PBT) Control:'. On the right side, there are controls for 'Waterfall view' (set to 'Full window'), 'Zoom out', 'Zoom in', 'Max out', 'Max in', and 'RX signal to Center'. Below these are instructions: 'Or use scroll wheel and dragging on waterfall.' There are also dropdowns for 'View' (set to 'waterfall'), 'Size' (set to 'normal'), and 'Speed' (set to 'medium'). A checkbox for 'Hide labels' is present. The 'Time' display shows '01:50 UTC - 20:50 LOCA'. At the bottom right, there is a 'Solar Activity Monitor' section. On the far right, there is a signal strength meter with a scale from -120 to 0 dB. Below it, there are checkboxes for 'Mute', 'Squelch', 'Auto-notch', and 'Notch-2'. The 'Audio' section has a 'VOLUME' slider. Below that, there are options for 'Audio out' (Left, Both, Right) and 'DSP Noise Reduction' (Off, High-Boost). The 'GAIN CONTROL' section has 'automatic' (selected) and 'manual' options, with a 'Gain' slider. At the bottom right, it says 'E-Field @ Washington DC Area (VLF 0-20kHz)'.

Let's Try It!

# Live ATC

Web site to listen in on air traffic frequencies. Besides being able to listen online, it provides the frequencies in use at selected airports.

<http://liveatc.net/>

# ADS-B

Automatic Dependent Surveillance - Broadcast (ADS-B) is a data broadcasting mechanism for aircraft that is a more reliable data exchange between aircraft than radar.

It's really cool!

<http://adsbexchange.com/>

# Let's Crash the Wi-Fi!

<http://na5b.com:8901/>



# Links

<https://www.amazon.com/RTL-SDR-Blog-RTL2832U-Software-Defined/dp/B0129EBDS2>

<https://gqrx.dk/>

<https://cubicsdr.com/>

<https://www.rtl-sdr.com/>

<http://websdr.org/>

<http://adsbexchange.com/>

<http://liveatc.net/>