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

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

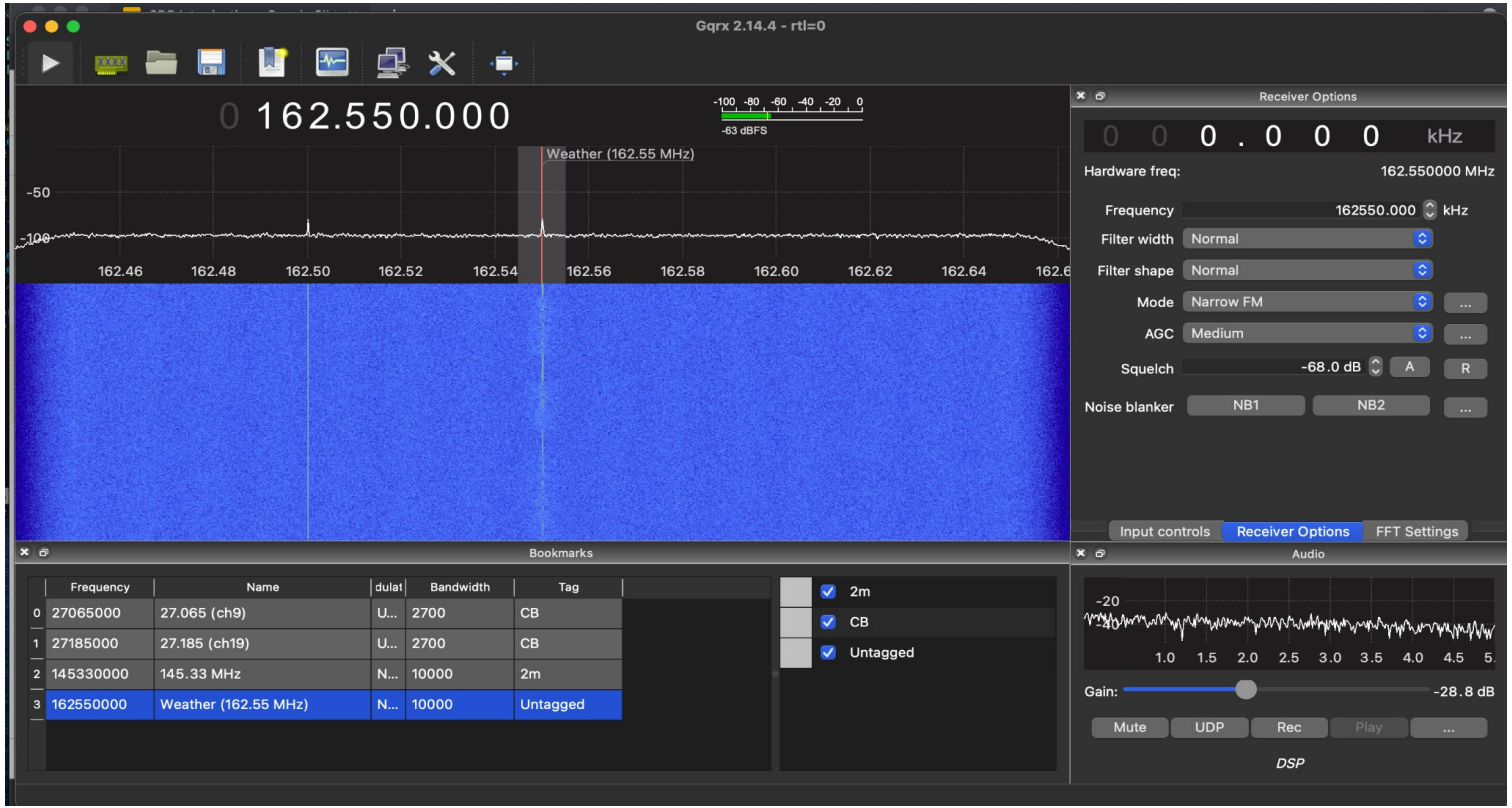
- Software abstraction layer for hardware
- Provides common API to access different hardware devices

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

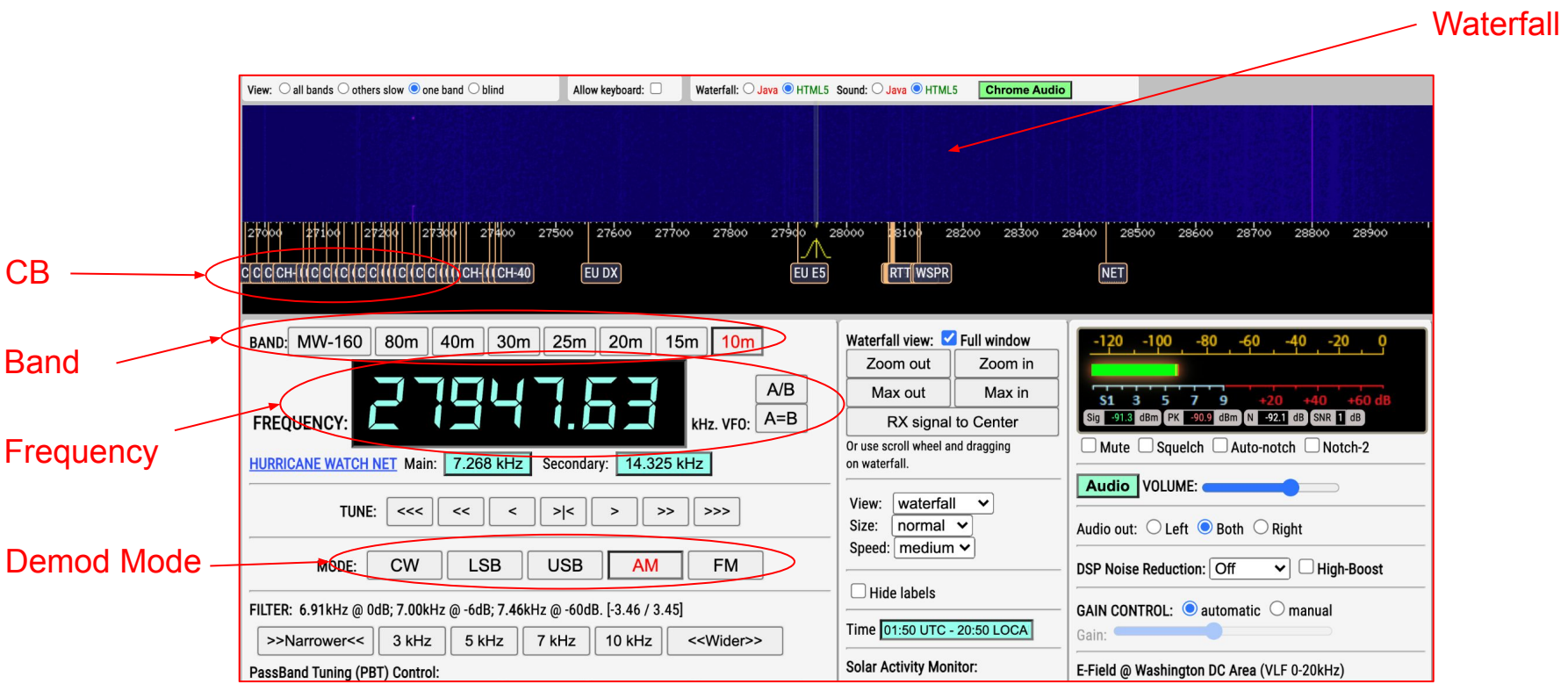
- The supplied “rabbit ears” are sufficient for most signals.
- You may have to adjust the length or orientation.
- Specialized antennas may be necessary for specific signals.

But I’m *REALLY* Cheap!

https://www.websdr.org

Example Online Radio

Example Online Radio - Explained



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/