2019

Dave Connett

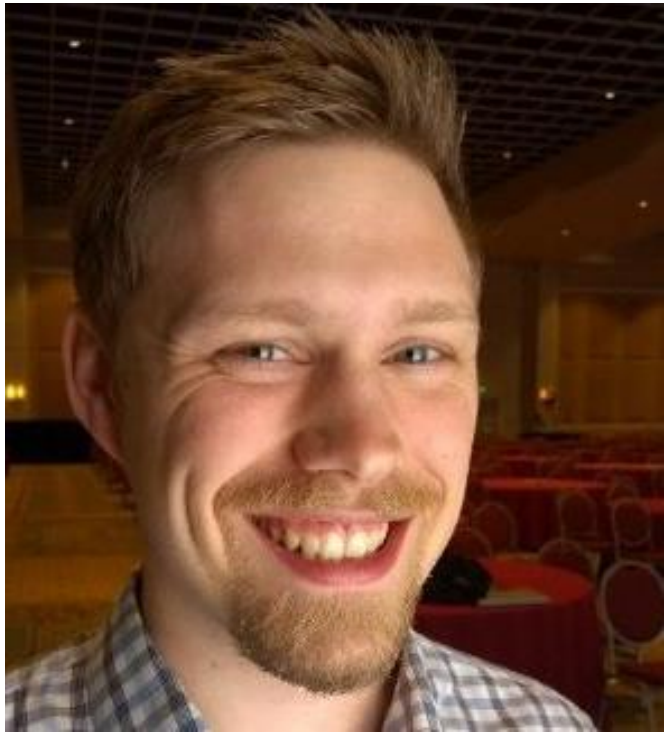
WIRELESS

RADIO BIBLE

Background

Dave Connett aka DJ Aeonik

- Data Analytics / Reverse Engineering / Ham Radio
- Automotive / Retail / Consultant / Research



What is a Radio? - Mathematical Theory of Communication

- 1948 article by Claude E. Shannon ("the father of information theory")
- Communication System:
  - Information Source
  - Transmitter
  - Channel
  - Receiver
  - Destination

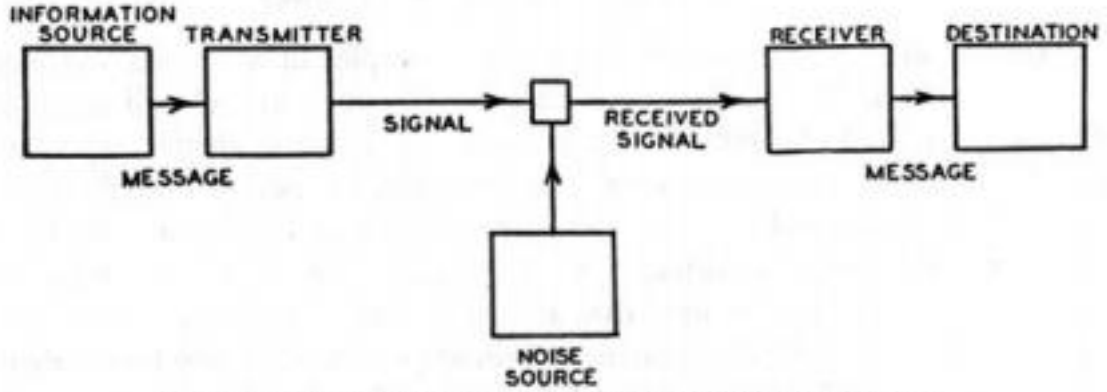
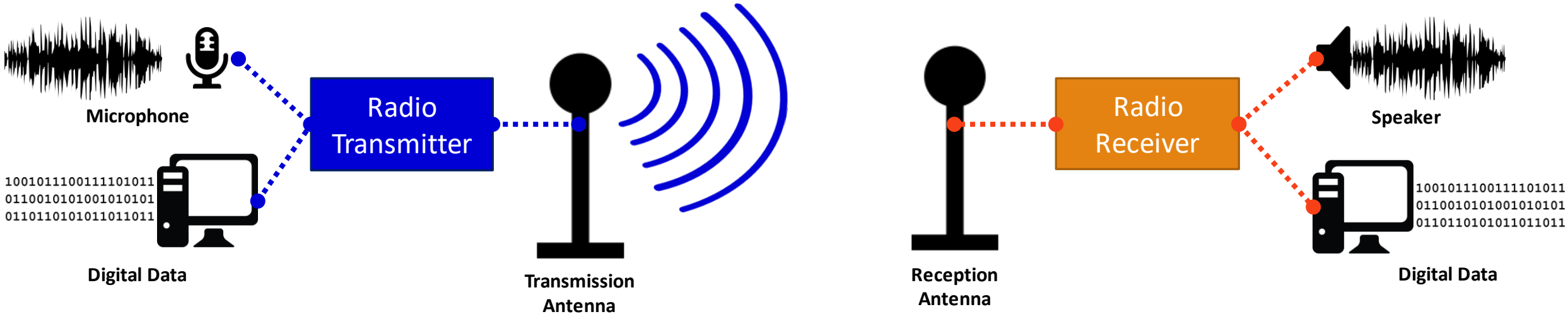


Fig. 1—Schematic diagram of a general communication system.

From "A Mathematical Theory of Communication

What is a Radio? – Components

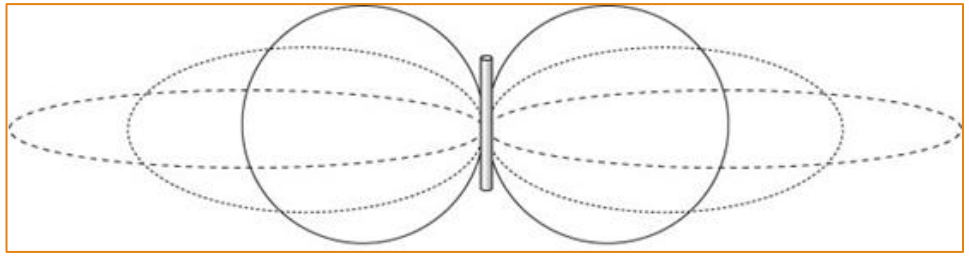
- Antenna
- Receiver
- Transmitter
- Transceiver (combination of Receiver and Transmitter)



What is a Radio? – Components

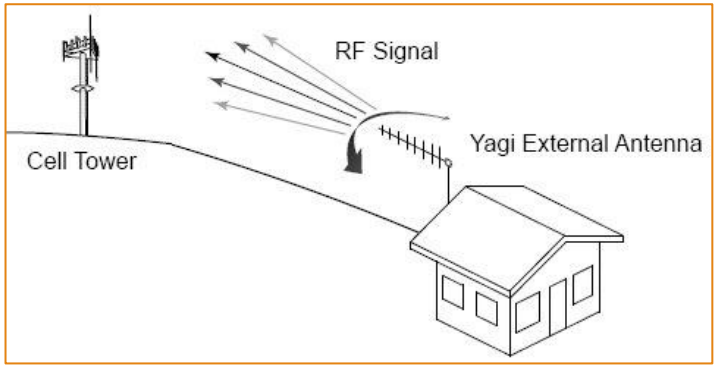
Antennas

- A wire which radiates a radio frequency.
- Directional
- Omnidirectional
  - Bidirectional (Dipole)



Dipole (Omnidirectional)

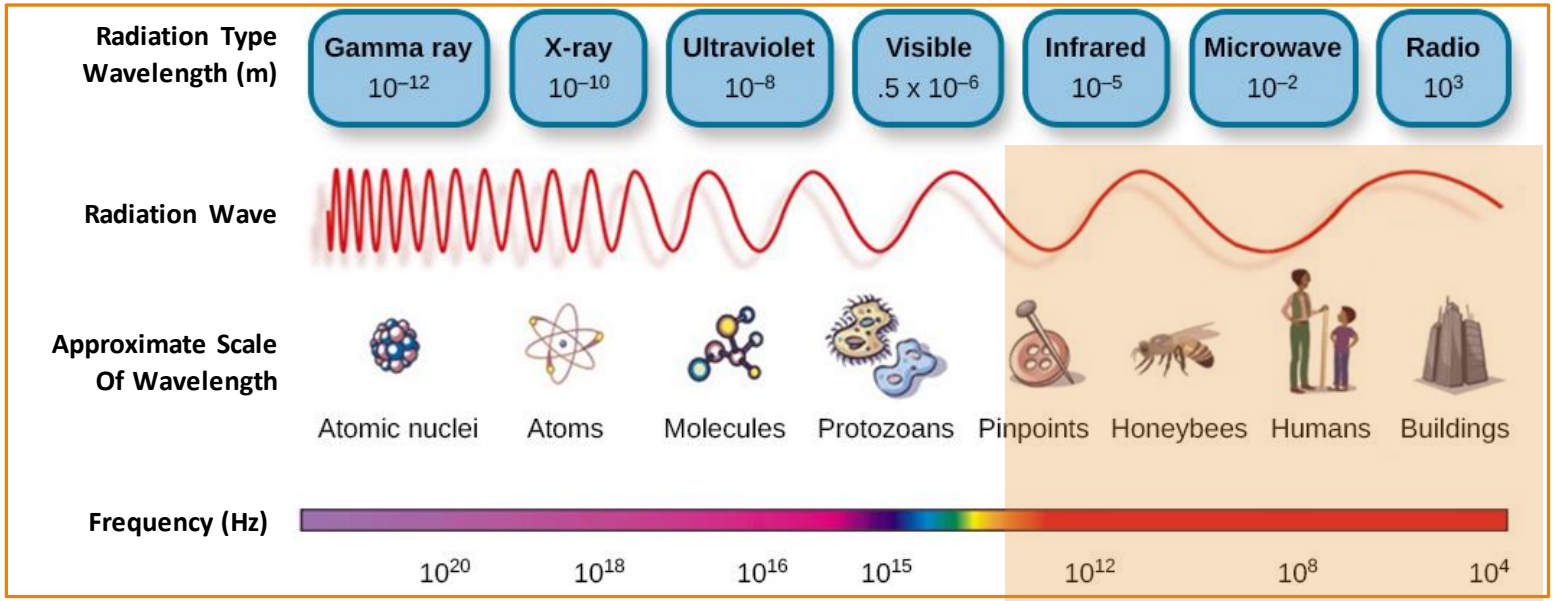
Cell Tower



Yagi

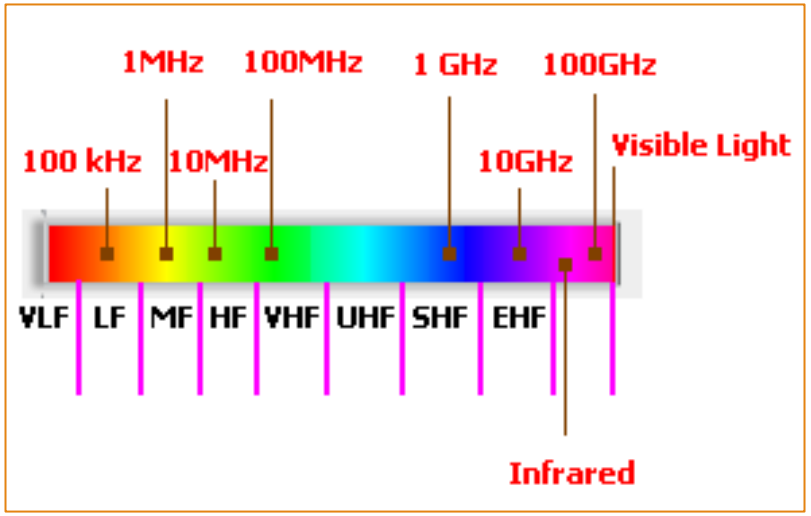
What is RF? – Electromagnetic Radiation

Radio Waves - A form of electromagnetic radiation with an identified radio frequency which range from 3 kHz to 300 GHz.



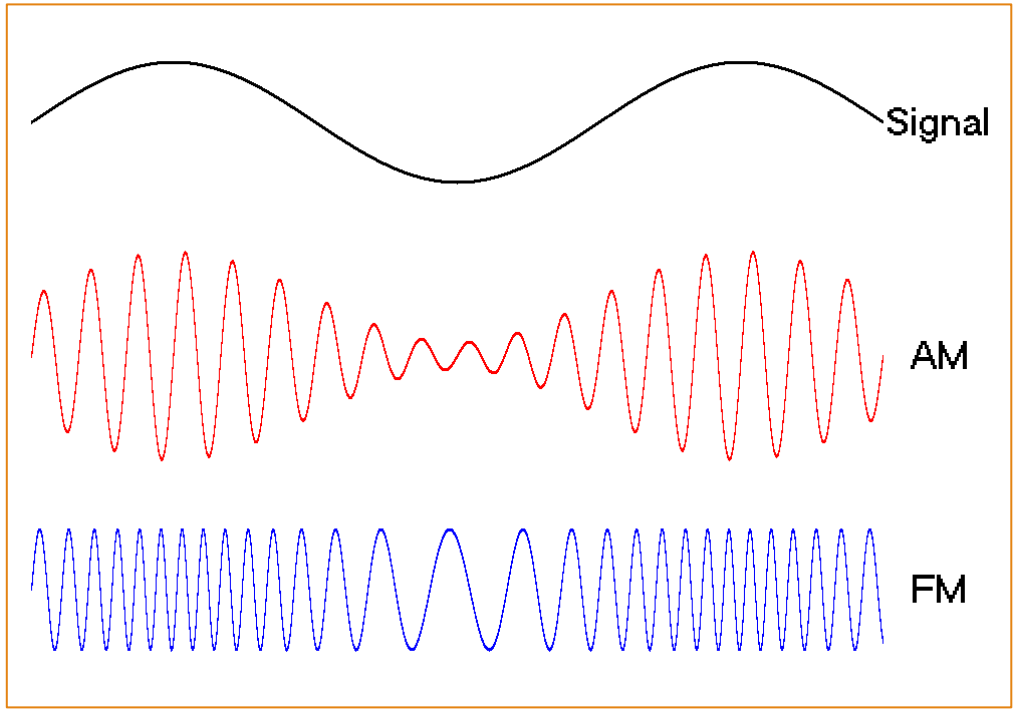
What is RF? – Radio Frequency

A frequency or band of frequencies in the range 10^2 to 10^{11} or 10^{12} Hz, which are suitable for use in telecommunications.



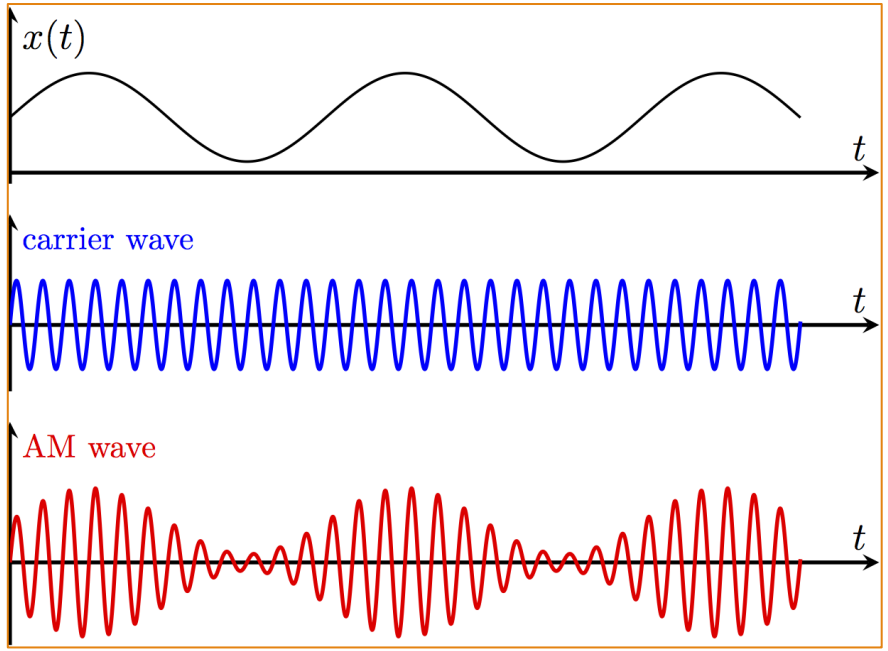
What is RF? – Radio Frequency Signal

A wireless electromagnetic signal used as a form of telecommunication.



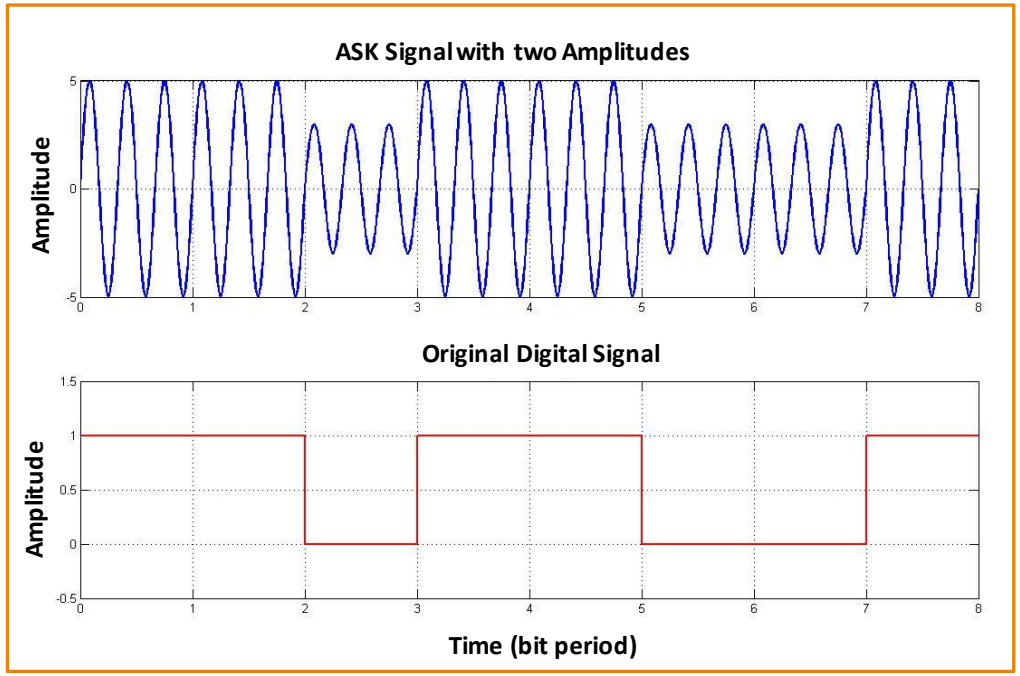
Amplitude Modulation (AM)

A modulation technique used in electronic communication, most commonly for transmitting information via a radio carrier wave.



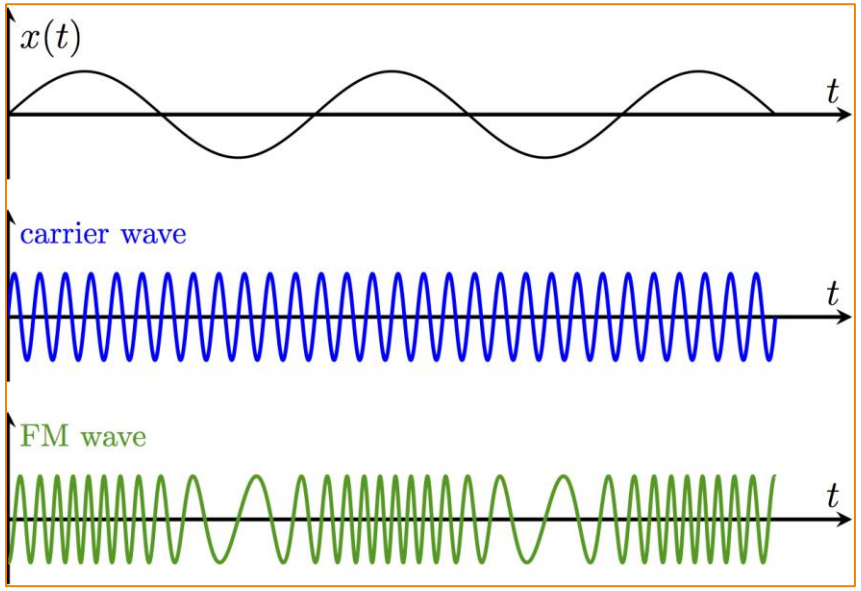
Amplitude Shift-Keying (ASK)

A form of amplitude modulation that represents digital data as variations in the amplitude of a carrier wave.



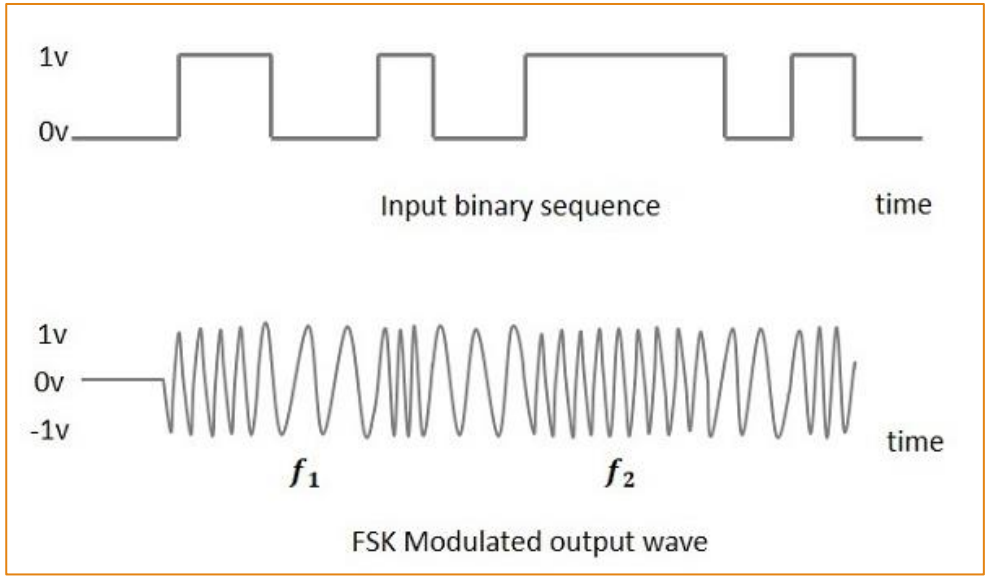
Frequency Modulation (FM)

The modulation of a radio or other wave by variation of its frequency, especially to carry an audio signal.



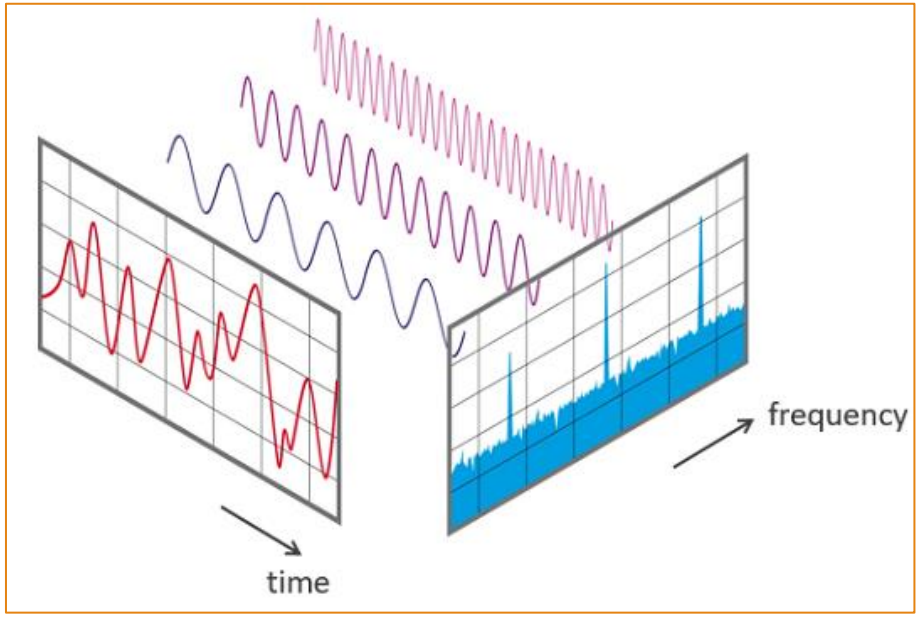
Frequency Shift-Keying (FSK)

A frequency modulation scheme in which digital information is transmitted through discrete frequency changes of a carrier signal.



Fast Fourier Transform (FFT)

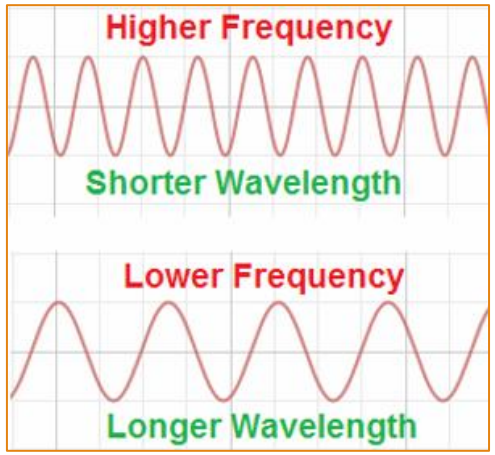
An algorithm that samples a signal over a period of time (or space) and divides it into its frequency components



RF Characteristics

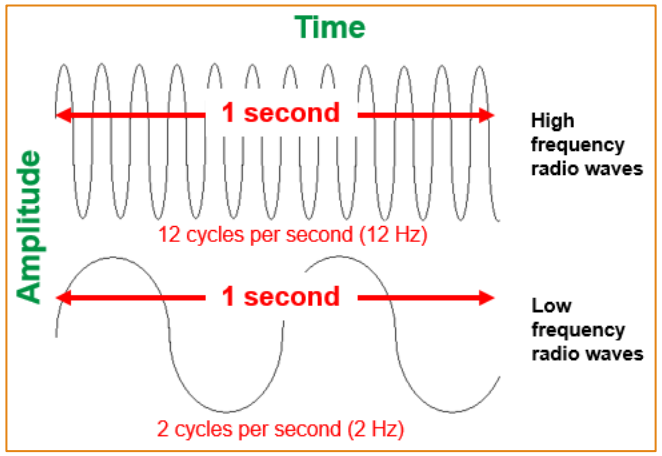
Wavelength

- Distance between two successive points of a wave pattern
- The lower your frequency the longer the wave is



Frequency

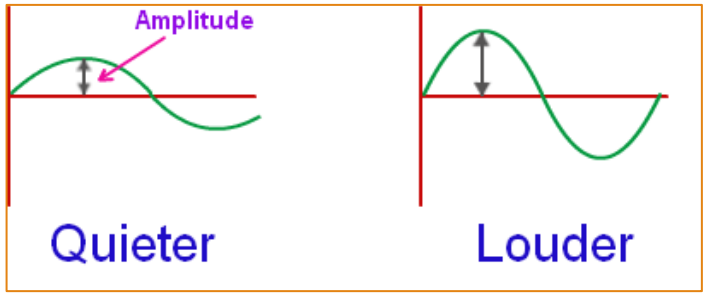
- Number of cycles within a specified time interval. Measured in hertz (Hz).
- 1 hertz = 1 cycle per second
- 1 KHz = 1,000 Hz
- 1 MHz = 1,000,000 Hz
- 1 GHz = 1,000,000,000 Hz



RF Characteristics

Amplitude

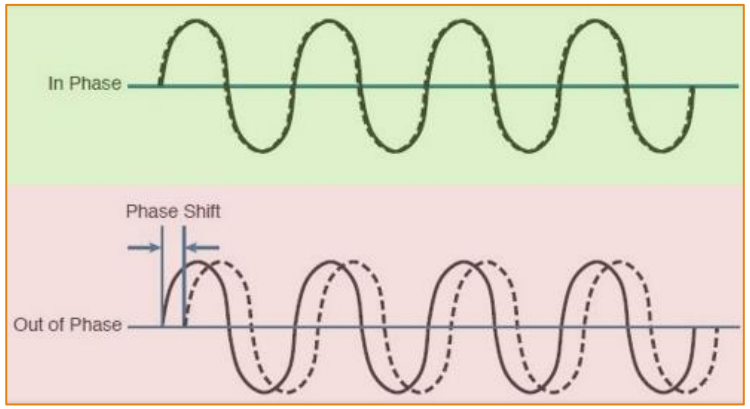
- Strength or power of the wave
- Transmit power depending on application
  - Wi-Fi/Bluetooth Power: ~0.001W to 0.1W
  - GPS Power: ~2000W from satellite
  - Cell Tower Power: ~10W to 500W



Phase

- Relationship between two or more signals which share the same frequency
- Measured in distance, time or degree

In Phase = Two waves which peaks align
Out of Phase = Two waves which peaks do not align



RF Characteristics

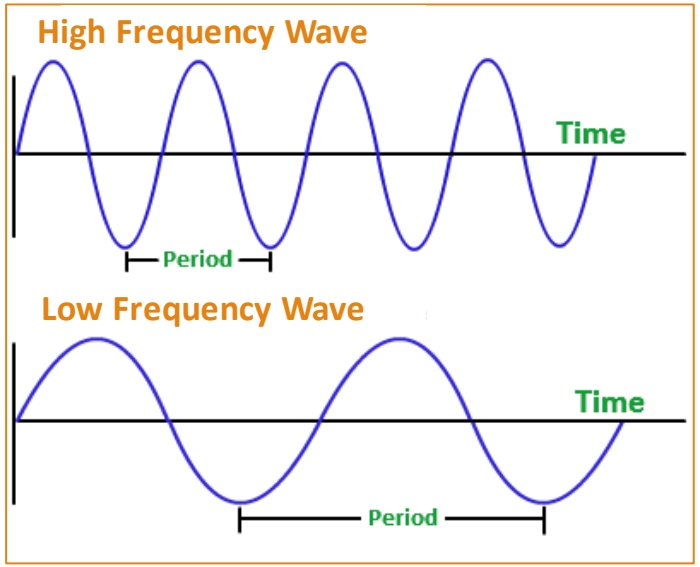
Wavelength & Frequency Relationship

- There is an inverse relationship between wavelength and frequency.
- Three components of relationship:
  1. Frequency (f)
  2. Wavelength (λ)
  3. Speed of light (c)

$$\lambda = c / f$$

$$f = c / \lambda$$

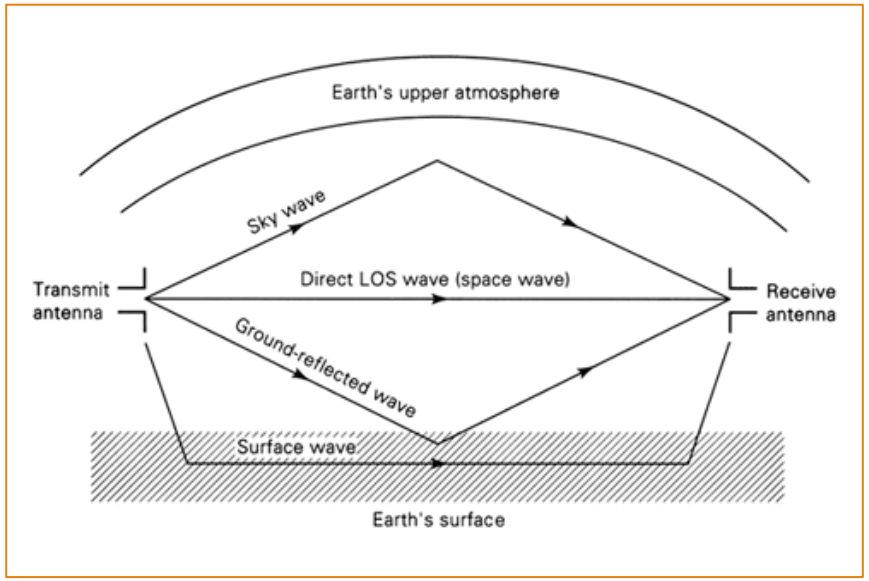
The longer the wavelength, the lower the frequency and vice versa.



RF Behaviors

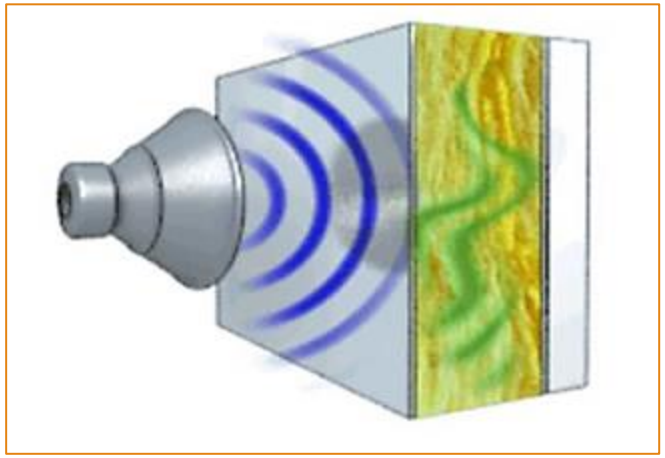
Wave Propagation

- As the wave moves away from the antenna, it will broaden or spread



Absorption

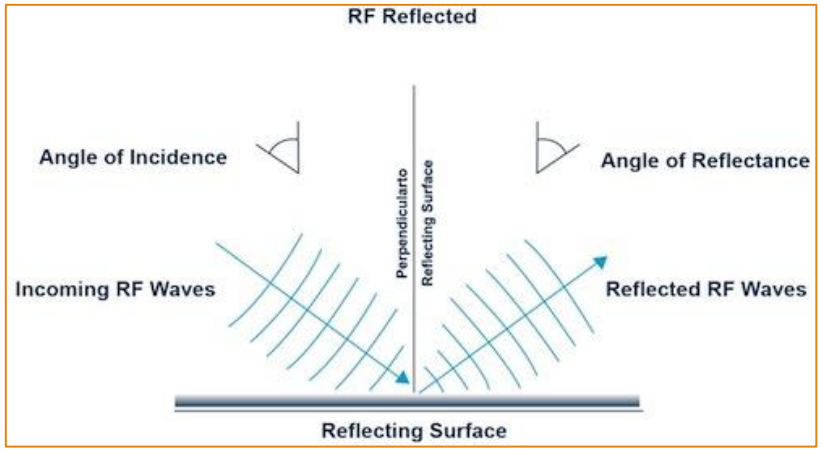
- Most material will absorb some amount or all of the RF signal
- Denser materials will absorb more RF
- Directly affects the amplitude of the wave



RF Behaviors

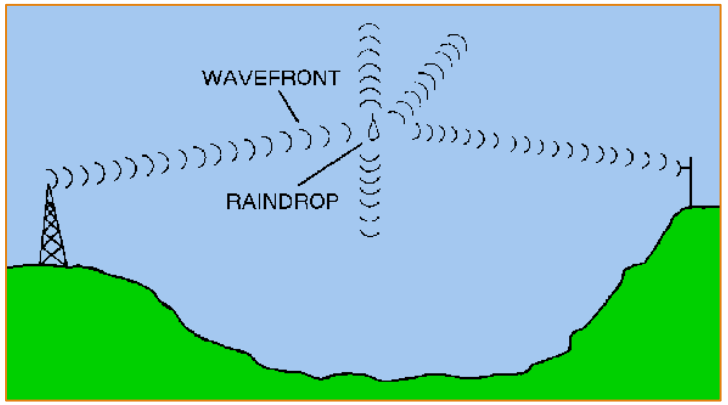
Reflection

- When a wave bounces off an object instead of traveling through it.
- Can cause multipath signal
- Microwave reflection occurs between 1GHz and 300 GHz



Scattering

- Multiple reflections
- Occurs when the wavelength is larger than pieces of the medium the signal is hitting
- Can occur when a wave encounters an uneven surface (raindrops)



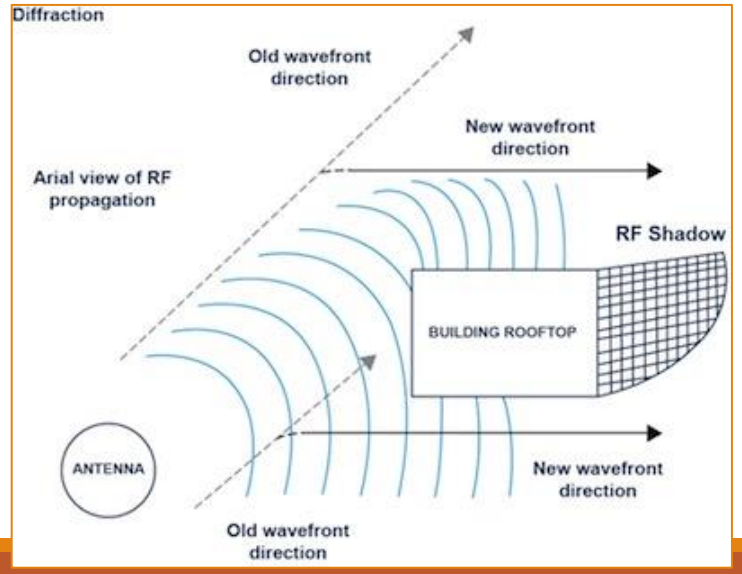
RF Behaviors

Defraction

- Defraction
- The bending of an RF signal as it passes through a medium with a different density
- Commonly occurs due to atmospheric conditions:
  - Water vapor
  - Change in air temperature
  - Change in air pressure

Diffraction

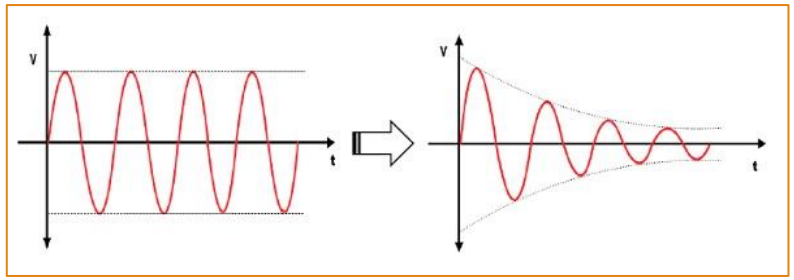
- The bending and spreading of an RF signal when it encounters an obstruction
- Typically caused by a partial blockage of the RF signal



RF Behaviors

Loss (attenuation)

- Decrease of amplitude or signal strength
- Water is a major source of absorption

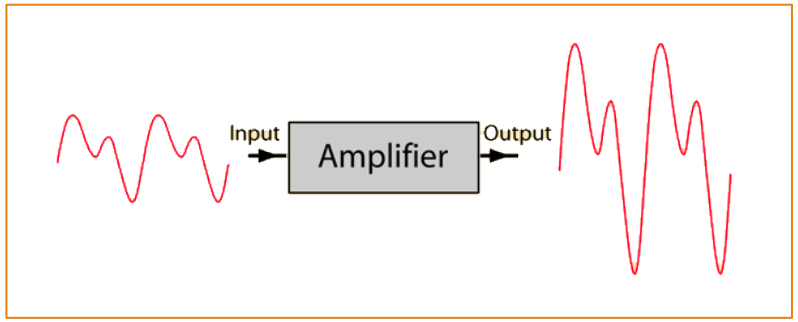


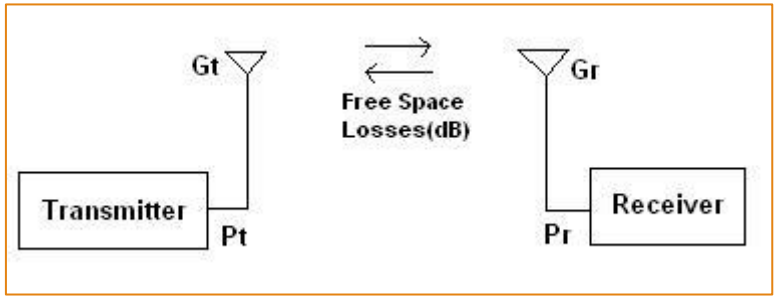
Free space path loss (FSPL)

- Attenuation of a signal as it travels
- Loss of signal strength caused by the natural broadening of the waves

Gain (amplification)

- Increase of amplitude or signal strength
- Two types of gain:
  - Active Gain – increase caused by adding power
  - Passive Gain – increase caused by focusing the RF signal, typically by an antenna

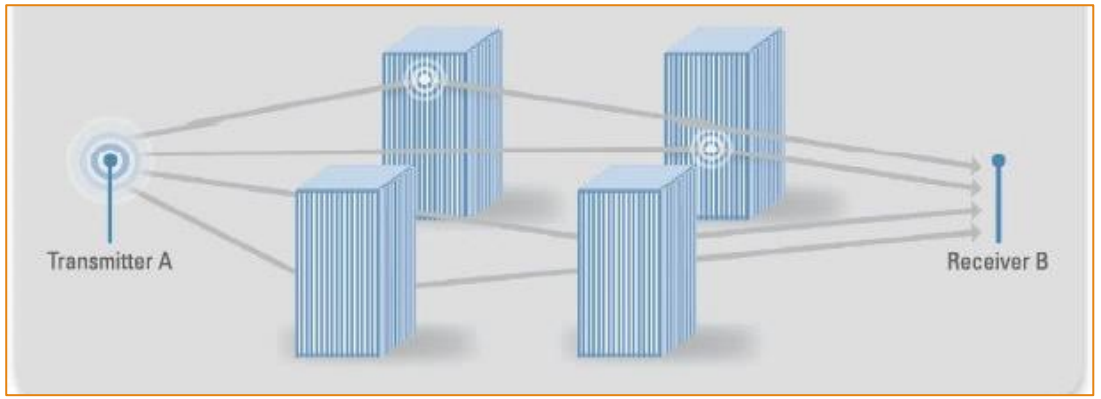




RF Behaviors

Multipath

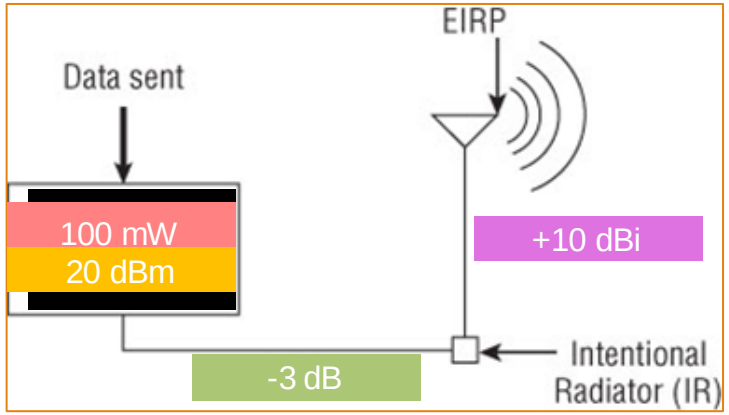
- Two or more paths of a signal arrive at a receiving antenna at the same time or within nanoseconds of each other.
- Delay Spread – Time differential between multipath signals
- Four Possible Results:
  - Upfade – increased signal strength
  - Downfade – decreases signal strength
  - Nulling – signal cancellation
  - Data corruption (most common)



RF Measurements

Units of Power

- Measures transmission amplitude and received amplitude
- Absolute power / relative power measurements
- Units of Power:
  - WATT (W), Milliwatt (**mW**)
- Decibels relatives to milliwatt (**dBm**) – **How loud is it?**



Units of Comparison

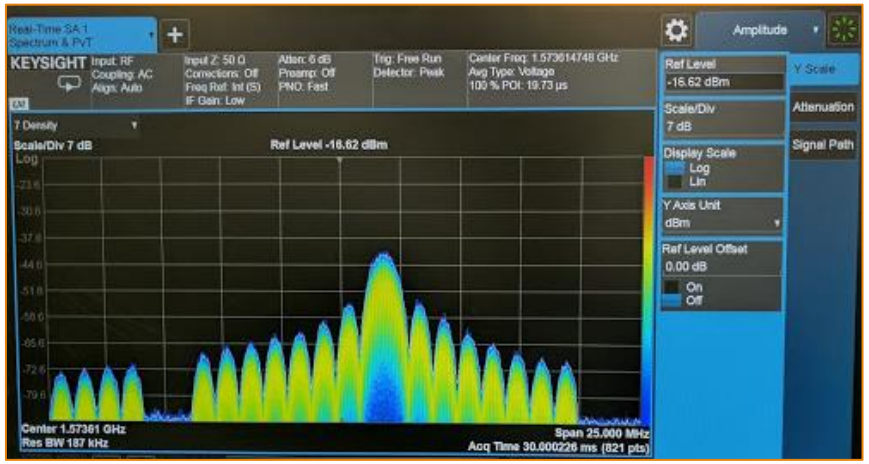
- Measures difference between signals
- Units of Comparison:
  - Decibel (**dB**)
    - 1 bel = ratio of 10 to 1 between the power of two values
  - Decibels relative to isotropic radiator (**dBi**)
    - Gain of the antenna
  - Decibel-milliwatts (**dBm**)
    - Translating the wattage to the decibe

Rule of 10s and 3s

- Provides an approximate value (fairly accurate)
- Four basic rules:
  - 3 dB gain, **double the power**
  - 3 dB loss, **halve the power**
  - 10 dB gain, **power times 10**
  - 10 dB loss, **power divided by 10**

Spectrum Analyzer

Measures the magnitude of an input signal versus frequency within the full frequency range of the instrument.



L1 Band (1575.42 MHz) GPS Spoof

What is SDR? (Software Defined Radio)

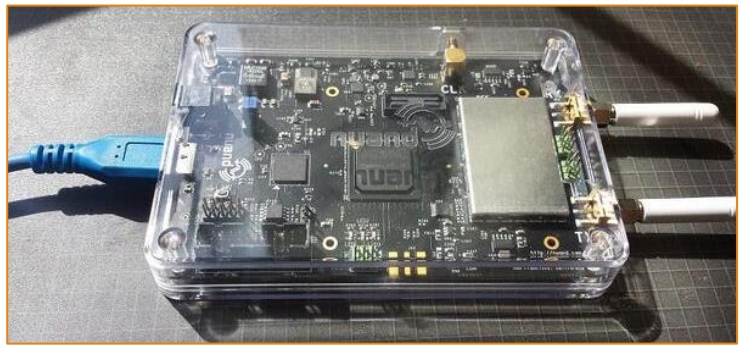
A radio system where components that have been traditionally implemented in hardware are instead implemented in software.

Defined by IEEE P1900.1

- "Radio in which some or all of the physical layer functions are software defined"

HackRF One

Ettus USRP



BladeRF

RTL-SDR

$20 devices for listening

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

Tuner	Frequency range
Elonics E4000	52 – 2200 MHz with a gap from 1100 MHz to 1250 MHz (varies)
Rafael Micro R820T/2	24 – 1766 MHz (Can be improved to ~13 - 1864 MHz with experimental drivers)
Fitipower FC0013	22 – 1100 MHz
Fitipower FC0012	22 – 948.6 MHz
FCI FC2580	146 – 308 MHz and 438 – 924 MHz (gap in between)

Table Source: Osmocom

HackRF One

$300 device for transmit or receive
https://greatscottgadgets.com/hackrf/

Specifications:

- 1 MHz to 6 GHz operating frequency
- half-duplex transceiver
- up to 20 million samples per second
- 8-bit quadrature samples (8-bit I and 8-bit Q)
- compatible with GNU Radio, SDR#, and more
- software-configurable RX and TX gain and baseband filter
- software-controlled antenna port power (50 mA at 3.3 V)
- SMA female antenna connector
- SMA female clock input and output for synchronization
- convenient buttons for programming
- internal pin headers for expansion
- Hi-Speed USB 2.0
- USB-powered
- open source hardware

bladeRF

$420+ device for transmit and receive

https://www.nuand.com

Specifications:

- Fully bus-powered USB 3.0 SuperSpeed Software Defined Radio
- Portable, handheld form factor: 5" by 3.5"
- Extensible gold plated RF SMA connectors
- 300MHz - 3.8GHz RF frequency range
- Independent RX/TX 12-bit 40MSPS quadrature sampling
- Capable of achieving full-duplex 28MHz channels
- 16-bit DAC factory calibrated 38.4MHz +/-1ppm VCTCXO
- On-board 200MHz ARM9 with 512KB embedded SRAM (JTAG port available)
- On-board 40KLE or 115KLE Altera Cyclone 4 E FPGA (JTAG port available)
- 2x2 MIMO configurable with SMB cable, expandable up to 4x4
- Modular expansion board design for adding GPIO, Ethernet, and 1PPS sync signal and expanding frequency range, and power limits
- DC power jack for running headless
- Highly efficient, low noise power architecture
- Stable Linux, Windows, Mac and GNURadio software support
- Hardware capable of operating as a spectrum analyzer, vector signal analyzer, and vector signal generator

YARD Stick One

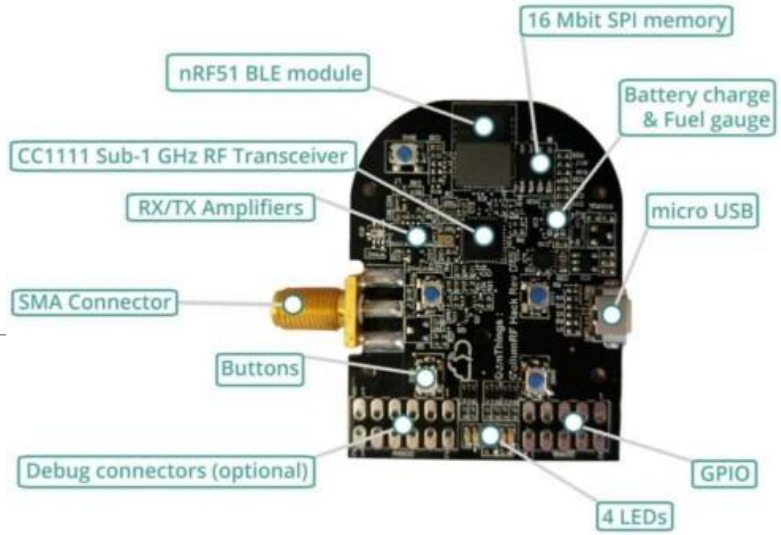
$120 device for transmit or receive

https://greatscottgadgets.com/yardstickone/

Specifications:

- half-duplex transmit and receive
- official operating frequencies: 300-348 MHz, 391-464 MHz, and 782-928 MHz
- unofficial operating frequencies: 281-361 MHz, 378-481 MHz, and 749-962 MHz
- modulations: ASK, OOK, GFSK, 2-FSK, 4-FSK, MSK
- data rates up to 500 kbps
- Full-Speed USB 2.0

pandwaRF



$170 device for transmit and receive

https://pandwarf.com/

Specifications:

- Bluetooth Smart Module ISP130301, based on nRF51
- CC1111 Low-Power SoC with Sub-1 GHz RF Transceiver
- Multi frequencies (from 300 MHz to 928 MHz)
- Multi modulation (ASK/OOK/MSK/2-FSK/GFSK)
- Transmit and receive in half duplex mode
- Support data rates up to 500 kBaud
- Open hardware
- Full speed USB: 12 Mbps (Linux or Android)
- Bluetooth Smart 4.0 (Android)
- USB charging & battery powered
- 4 buttons to assign codes
- 4 Status LEDs
- 16 Mbit Flash Memory to save custom RF protocols
- Rechargeable battery powered for stand-alone operation
- Battery fuel gauge
- RX amplifier for improved sensitivity: +13dB from 300MHz-1GHz
- TX amplifier for higher output power: +20dB @ 433MHz & +17dB @ 900MHz
- SMA connector for external antenna
- Antenna port power control for external LNA
- 22-pin expansion and programming header
- Included: Battery and injection molded plastic enclosure

Wi-Fi Pineapple

$100 device for hacking Wi-Fi

https://www.wifipineapple.com/

WiFi Pineapple NANO

The ultimate WiFi pentest companion, in your pocket.

- 6th generation WiFi Pineapple software featuring PineAP, web interface and modules
- Dual discrete 2.4 GHz b/g/n Atheros radios
- Up to 400 mW per radio with included antennas
- Integrated Power over USB Ethernet Plug
- Memory expansion via Micro SD (up to 200 GB)
- Optional mobile EDC Tactical case and battery
- USB 2.0 Host accessory expansion port

WiFi Pineapple TETRA

The amplified, dual-band (2.4/5 GHz) powerhouse.

- 6th generation WiFi Pineapple software featuring PineAP, web interface and modules
- Dual discrete 2.4/5 GHz a/b/g/n Atheros 2:2 MIMO radios
- 4 onboard Skybridge amplifiers
- Up to 800 mW per radio with included antennas
- Integrated Power over USB Ethernet Port
- Integrated Power over USB Serial Port
- Onboard NAND Flash (2 GB)
- USB 2.0 Host and RJ45 Ethernet Ports

Proxmark3

$300 device for RFID/HID hacking

hackerwarehouse.com/product/proxmark3-rdv2-kit/

Specifications:

- Read just about any RFID tag
- Pretend to be a reader or a tag
- Sniff communications between a reader and tag
- Operate in standalone mode without a PC (USB battery required)
- Improved LF and HF antennas
  - LF antenna: 35.23 V @ 125.00 kHz
  - LF antenna: 27.64 V @ 134.00 kHz
  - LF optimal: 35.39 V @ 127.66 kHz
  - HF antenna: 24.08 V @ 13.56 MHz
- Enhanced antenna wires
- 512KB of dual bank flash memory (AT91SAM7S512)
- Improved shell
- Power indicator LED

Ettus Research USRP

$4,000+ device for transmit and receive

ettus.com/product/category/USRP-X-Series

Specifications:

- Two wide-bandwidth RF daughterboard slots
  - Up to 160MHz bandwidth each (wideband versions of CBX, WBX, SBX)
  - Daughterboard selection covers DC to 6 GHz
- Large customizable Xilinx Kintex-7 FPGA for high performance DSP
- Multiple high-speed interfaces
  - Dual 10 Gigabit Ethernet - 2x RX at 200 MSps per channel
  - Dual 10 Gigabit Ethernet - 4x RX at 80 MSps per channel
  - PCIe Express (Desktop) - 200 MS/s Full Duplex
  - ExpressCard (Laptop) - 50 MS/s Full Duplex
  - Dual 1 Gigabit Ethernet - 25 MS/s Full Duplex
- UHD architecture provides compatibility with
  - GNU Radio
  - C++/Python API
  - Amarisoft LTE 100
  - OpenBTS
  - Other third-party software and frameworks
- Flexible clocking architecture
  - Configurable sample clock
  - Optional GPS-disciplined OCXO
  - Coherent operation with OctoClock and OctoClock-G
- Compact and rugged half-wide 1U form factor for convenient desktop or rack mount usage
- Digital I/O accessible on the front panel for custom control and interfacing from the FPGA

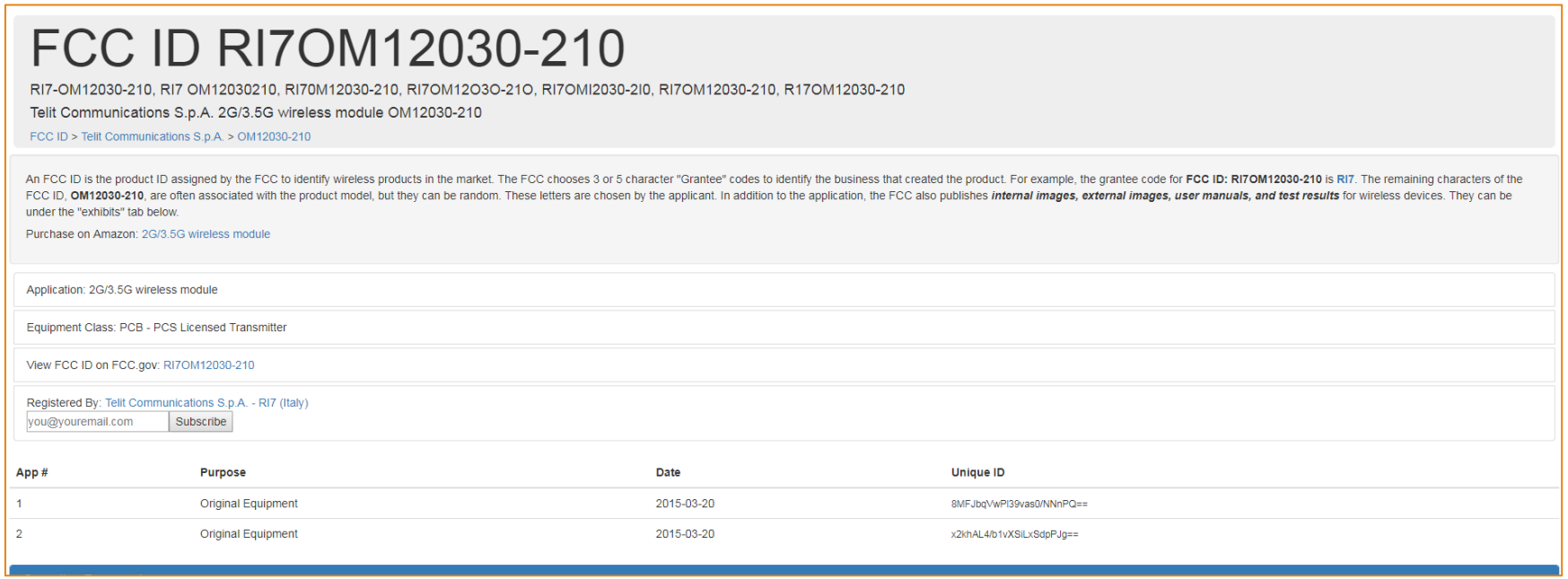
FCCID Look-up – Physical Inspection

What to look for? – FCC ID / IMEI #

FCCID Look-up – Research

Type FCC ID # into Google:

FCC ID RI7OM12030-210



FCC ID RI7OM12030-210

RI7-OM12030-210, RI7 OM12030210, RI70M12030-210, RI7OM12O3O-21O, RI7OMI2030-2I0, RI7OM12030-210, R17OM12030-210

Telit Communications S.p.A. 2G/3.5G wireless module OM12030-210

FCC ID > Telit Communications S.p.A. > OM12030-210

An FCC ID is the product ID assigned by the FCC to identify wireless products in the market. The FCC chooses 3 or 5 character "Grantee" codes to identify the business that created the product. For example, the grantee code for **FCC ID: RI7OM12030-210** is RI7. The remaining characters of the FCC ID, **OM12030-210**, are often associated with the product model, but they can be random. These letters are chosen by the applicant. In addition to the application, the FCC also publishes ***internal images, external images, user manuals, and test results*** for wireless devices. They can be under the "exhibits" tab below.

Purchase on Amazon: 2G/3.5G wireless module

Application: 2G/3.5G wireless module

Equipment Class: PCB - PCS Licensed Transmitter

View FCC ID on FCC.gov: RI7OM12030-210

Registered By: Telit Communications S.p.A. - RI7 (Italy)

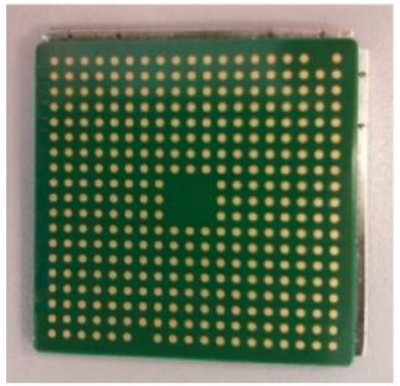
you@youremail.com Subscribe

App #	Purpose	Date	Unique ID
1	Original Equipment	2015-03-20	8MFJbqVwPI39vas0/NNnPQ==
2	Original Equipment	2015-03-20	x2khAL4/b1vXSiLxSdpPJg==

FCCID Look-up – Research

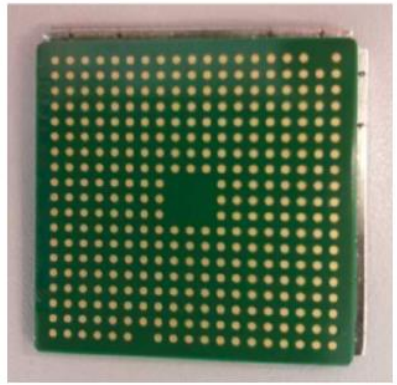
OM12030/210

External pictures



OM12030/210

Internal pictures



Operating Frequencies

Frequency Range	Power Output	Tolerance
824.2-848.8 MHz	344.3 mW	1ppm
826.4-846.6 MHz	199.9 mW	1ppm
826.4-846.6 MHz	124.2 mW	1ppm
1.7124-1.7526 GHz	89.5 mW	1ppm
1.7124-1.7526 GHz	98.2 mW	1ppm
1.8502-1.9098 GHz	535.8 mW	1ppm
1.8502-1.9098 GHz	209.9 mW	1ppm
1.8524-1.9076 GHz	184.9 mW	1ppm
1.8524-1.9076 GHz	114.8 mW	1ppm

June 25th, 2019

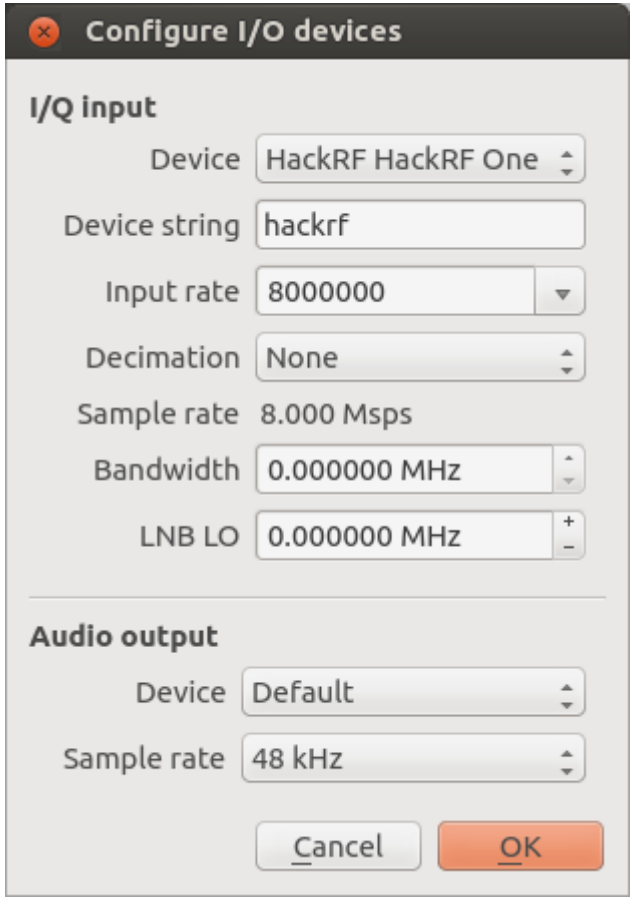
Dave Connett

GQRX QUICK AND SIMPLE GUIDE

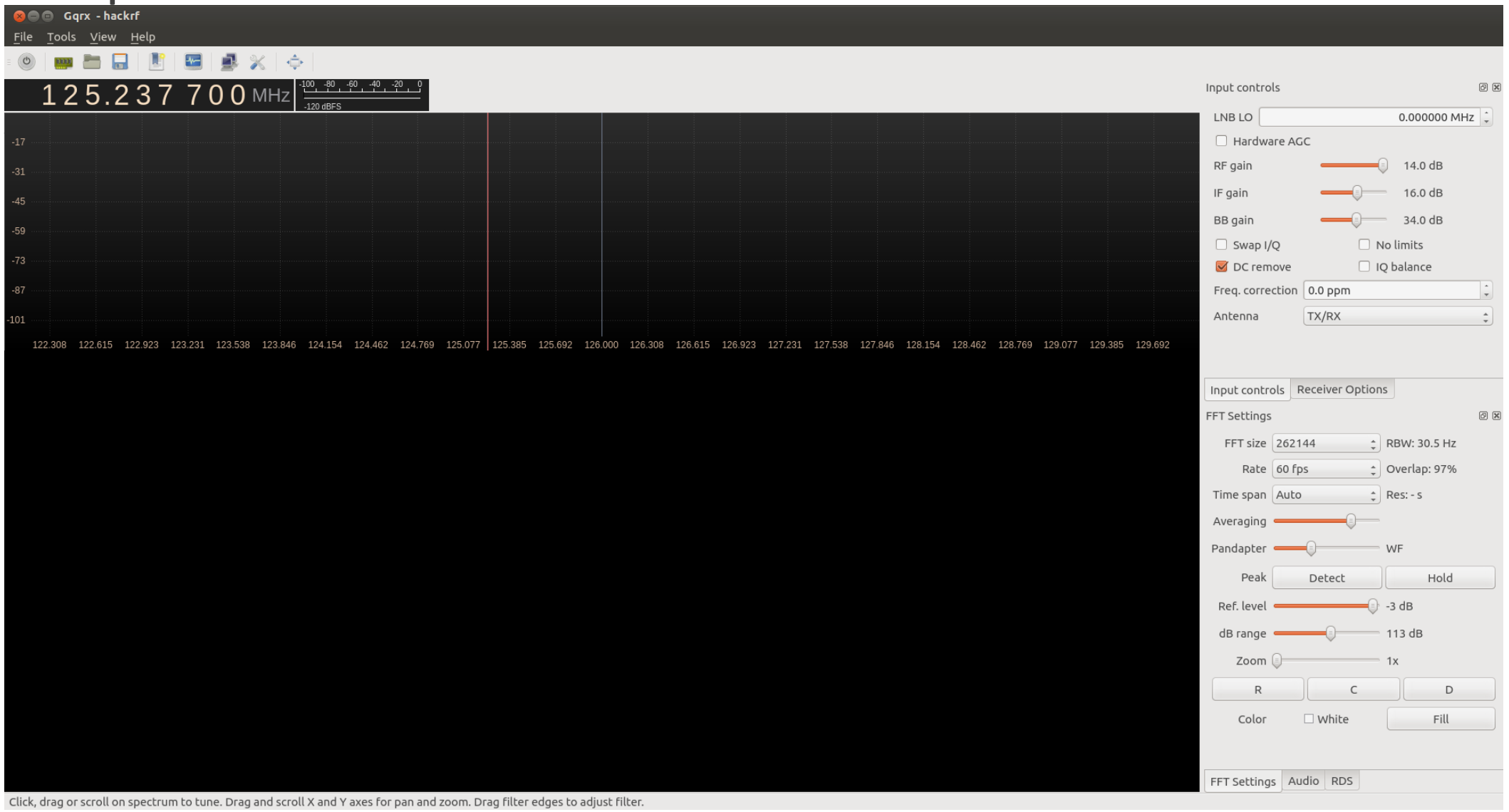
Step 1 - Configuration

Two important settings:

1. Device: HackRF One
2. Input Rate: 8000000 (8 Mega samples / second)



Step 2 – Main Screen

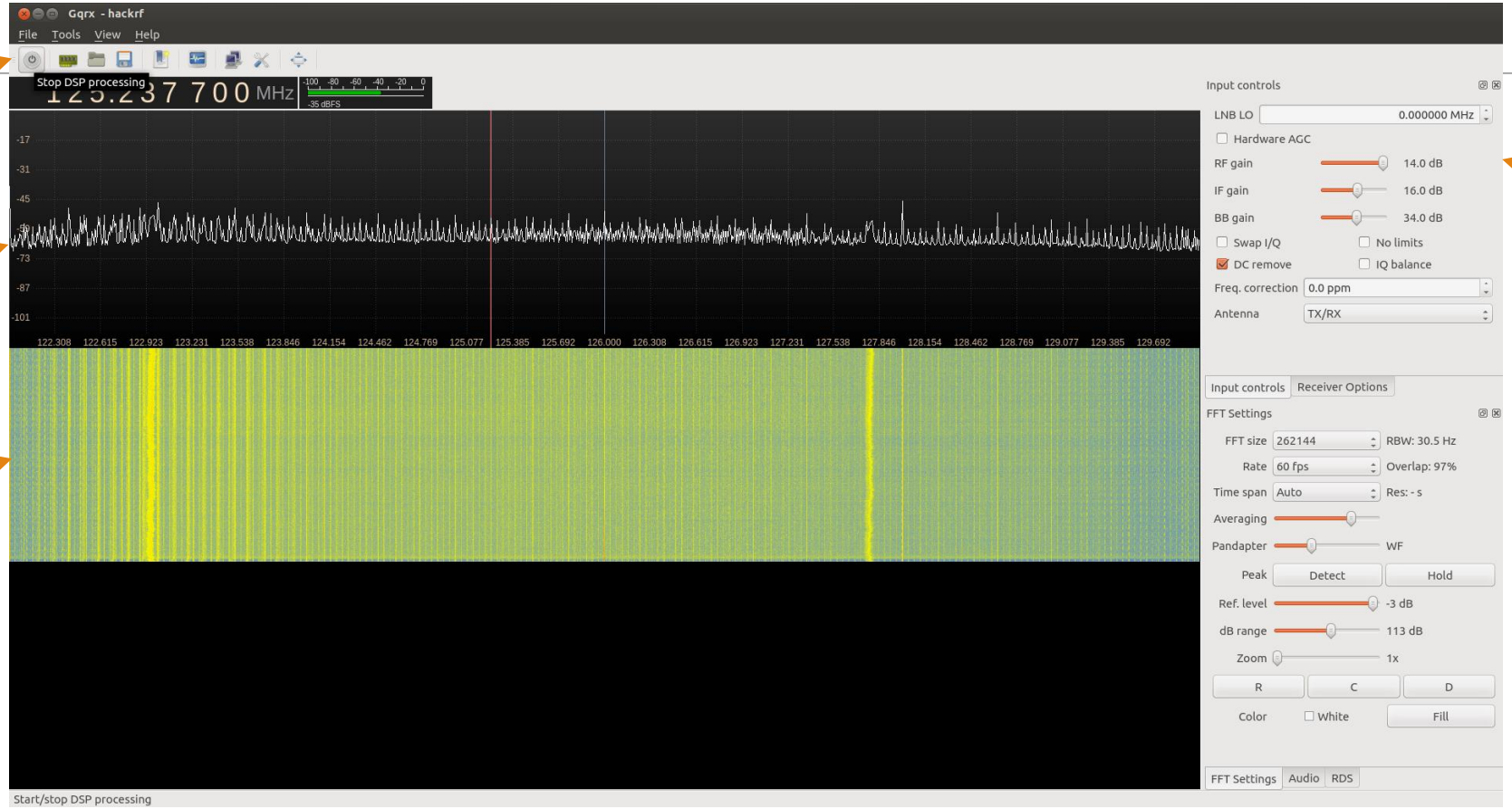


Step 3 – Activate Receiver

Start Button

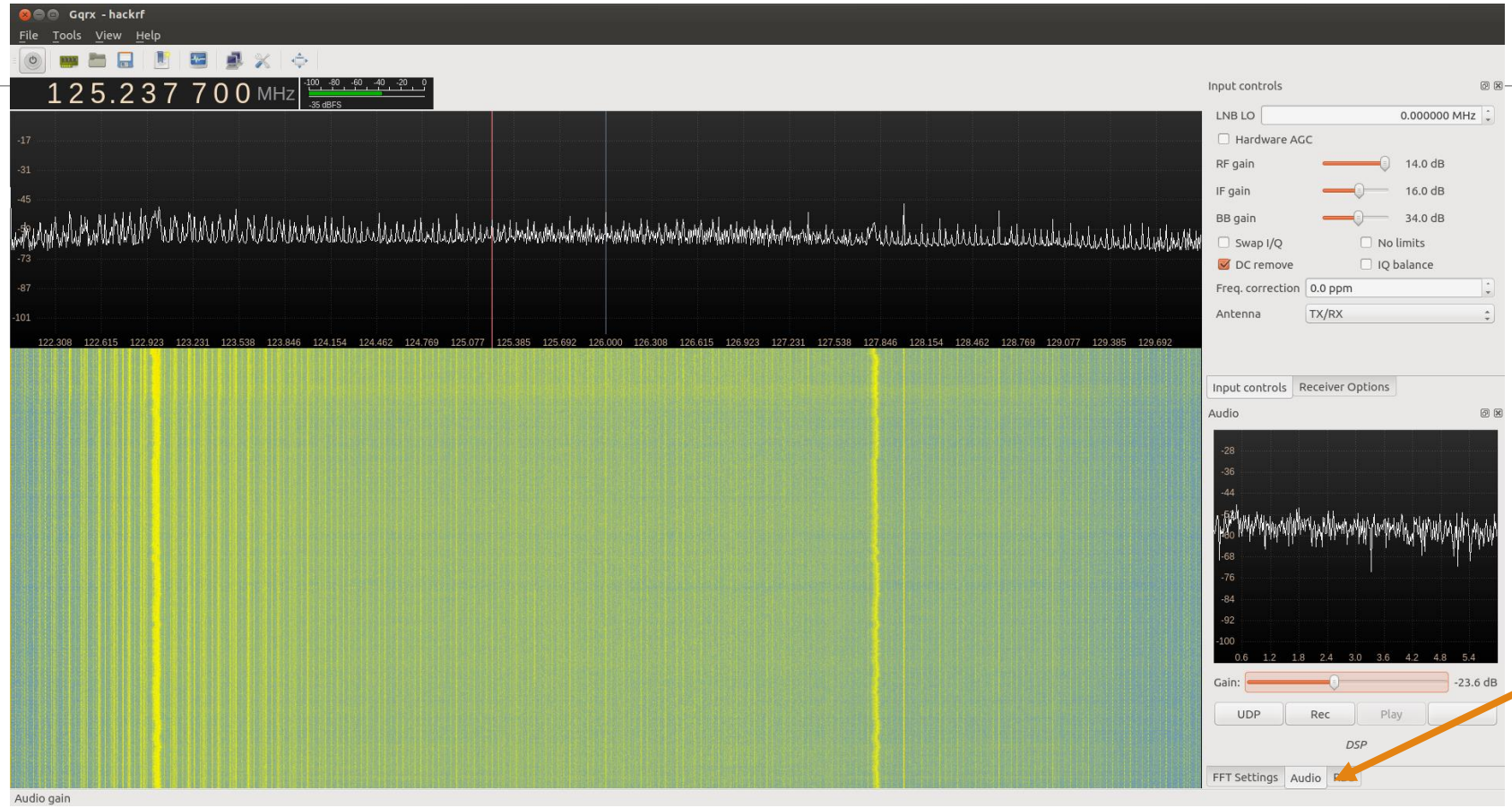
Frequency View

Waterfall View (Spectrogram)



Control Panel

Step 4 – Gain



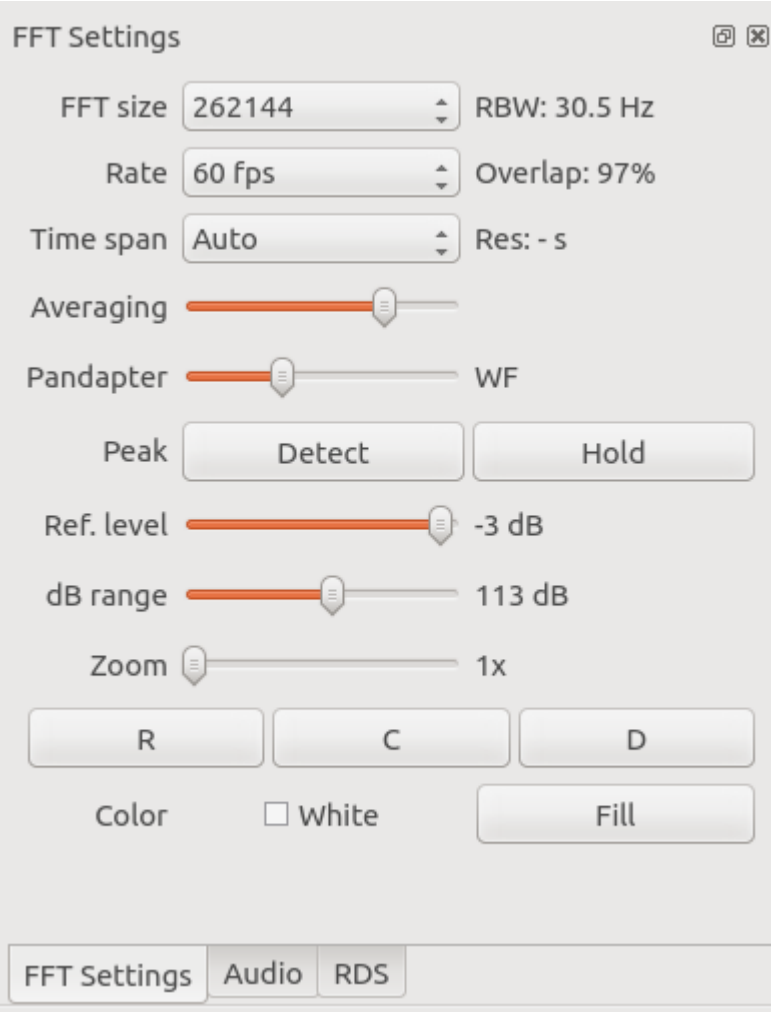
Audio Panel

- Control Volume (Gain)
- Record Audio
- Playback Audio

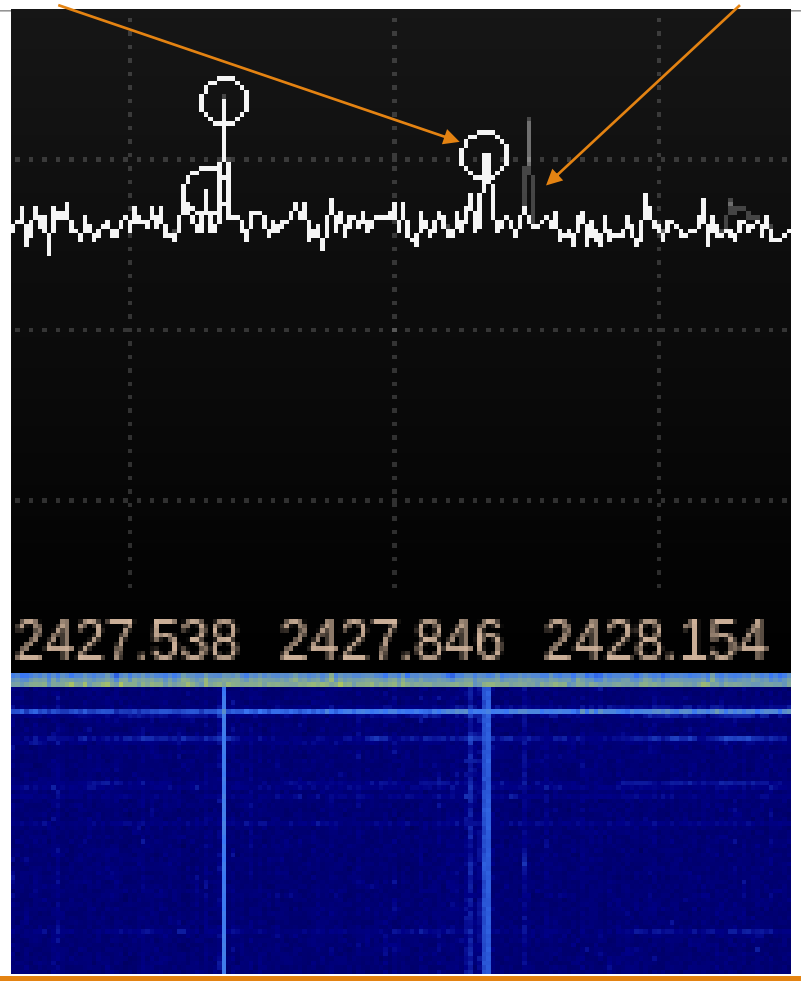
Step 5 – FFT Settings

Four common settings:

1. FFT Size – Sets resolution of waterfall and frequency view.
   Higher = Better
   Higher = More CPU
2. Peak Detect – Highlights and measures peak signals
3. Peak Hold – Keep outline of highest waves
4. Zoom – …



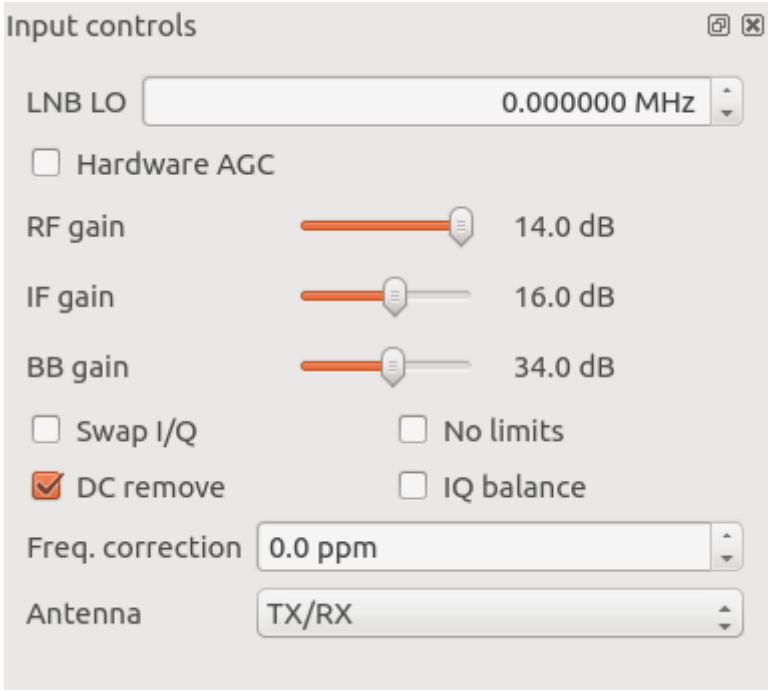
Step 6 – Peak Detect and Peak Hold



Step 7 – Input Settings (aka the HackRF)

Three common settings:

1. RF Gain – On or Off (14 dB is somewhat misleading)
   On = Better signals, but more noise
2. IF Gain and BB Gain
   Generally leave them around 16 dB or 24 dB
   Higher = louder signals, but much more noise
3. DC Remove - Remove annoying spike in the middle screen



Step 8 – Example Signal

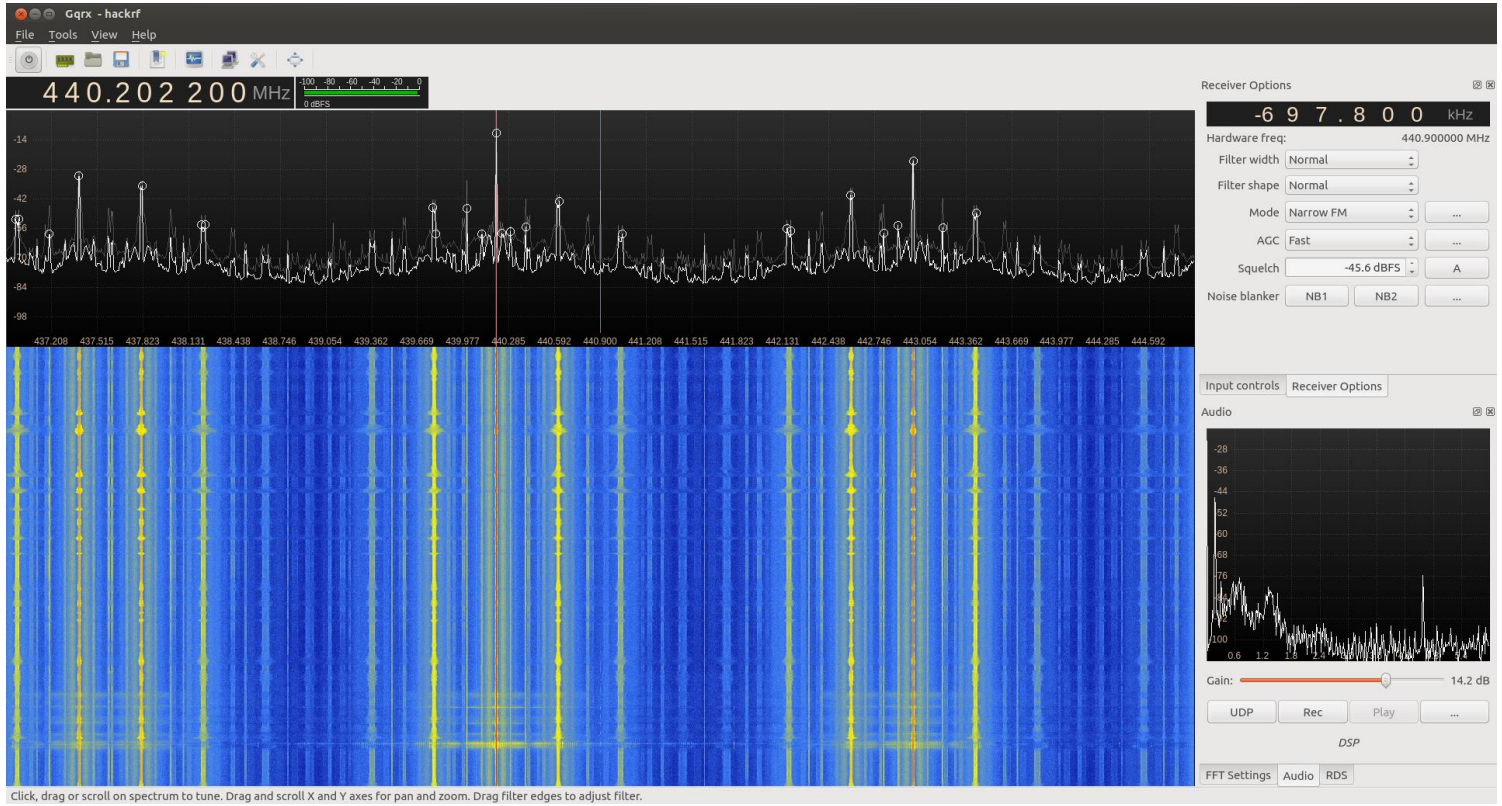
Signal = solid spike

This example is a walkie talkie

Notice: the signal is so loud it has “harmonics”, signals repeated nearby

Note: if a signal is louder than 5 dB it can damage the HackRF

(not -5 dB)



Keep away from powerful RF sources
Towers, powerful radios, directional antennas, etc…
Turn RF gain down to compensate for loud signals

Step 9 – Demodulate Signal

Click on a signal to highlight it and play it over sound

Receiver options control the demodulation

Important Settings:

1. FM, AMFilter Width – Set the size of the signal
   Look this up, or guess
2. Mode , Raw IQ etc…
   Play with these settings to find the right sounding option
   Raw IQ is usually best to use when importing to other programs
3. Squelch – Don't play static noise, only signals
   Select an area with no signal and click the "A" to automatically set

Step 8 – Example Signal

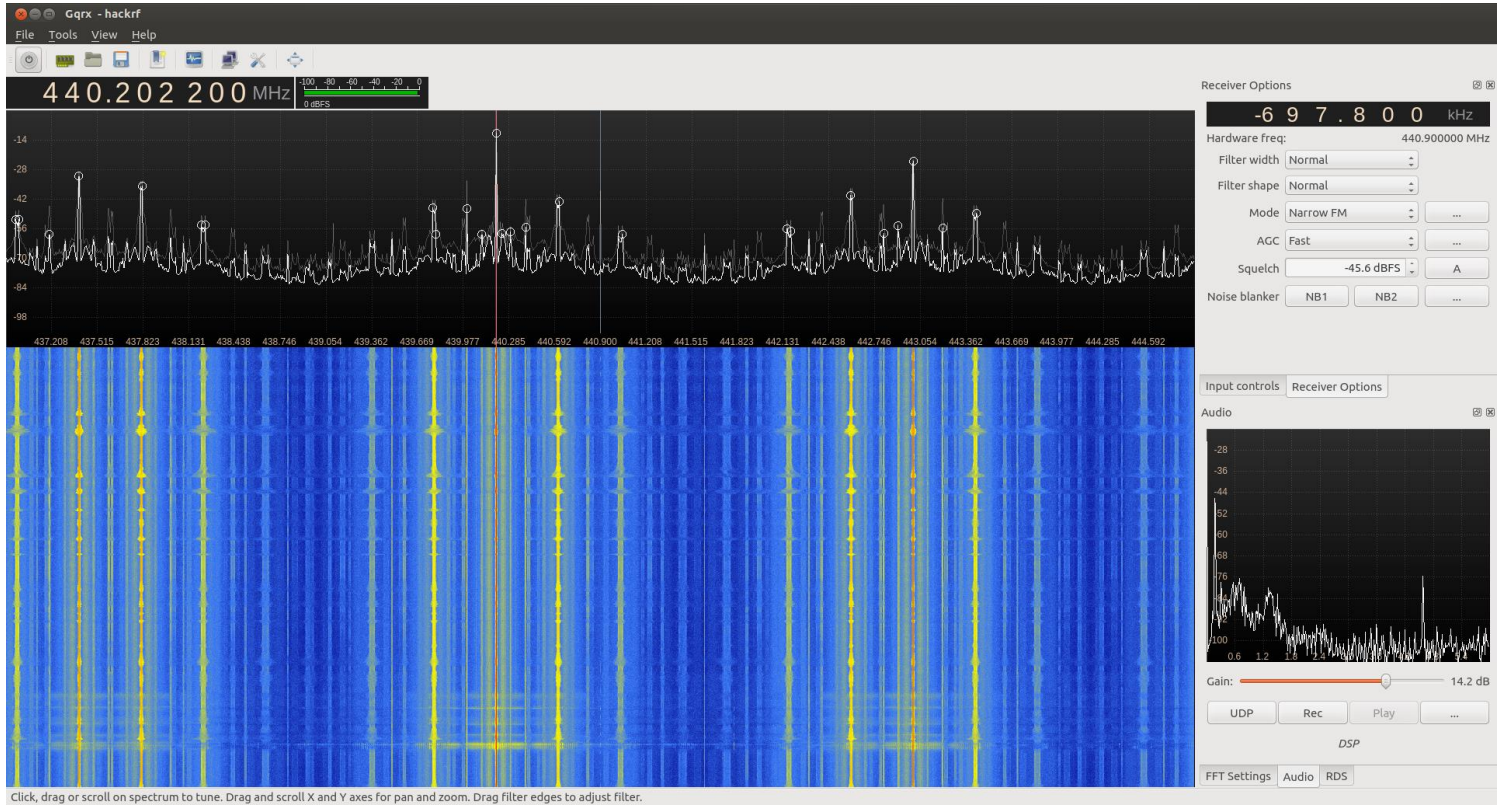
Signal = solid spike

This example is a walkie talkie

Notice: the signal is so loud it has “harmonics”, signals repeated nearby

Note: if a signal is louder than 5 dB it can damage the HackRF

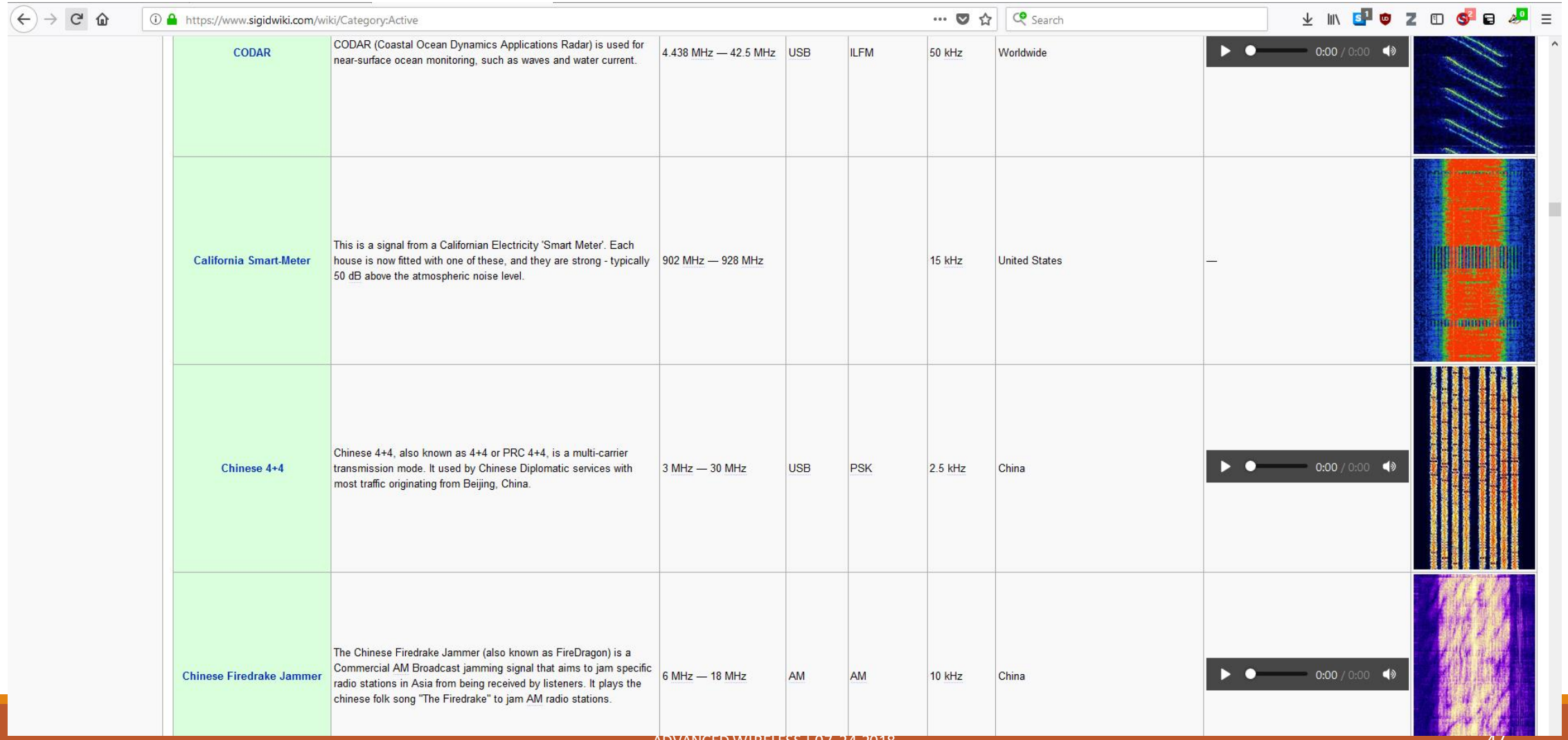
(not -5 dB)



Keep away from powerful RF sources
Towers, powerful radios, directional antennas, etc…
Turn RF gain down to compensate for loud signals

Step 9 – Other Signals

www.sigidwiki.com is a great source for active signals



CODAR	CODAR (Coastal Ocean Dynamics Applications Radar) is used for near-surface ocean monitoring, such as waves and water current.	4.438 MHz — 42.5 MHz	USB	ILFM	50 kHz	Worldwide	0:00 / 0:00
California Smart-Meter	This is a signal from a Californian Electricity 'Smart Meter'. Each house is now fitted with one of these, and they are strong - typically 50 dB above the atmospheric noise level.	902 MHz — 928 MHz			15 kHz	United States	—
Chinese 4+4	Chinese 4+4, also known as 4+4 or PRC 4+4, is a multi-carrier transmission mode. It used by Chinese Diplomatic services with most traffic originating from Beijing, China.	3 MHz — 30 MHz	USB	PSK	2.5 kHz	China	0:00 / 0:00
Chinese Firedrake Jammer	The Chinese Firedrake Jammer (also known as FireDragon) is a Commercial AM Broadcast jamming signal that aims to jam specific radio stations in Asia from being received by listeners. It plays the chinese folk song "The Firedrake" to jam AM radio stations.	6 MHz — 18 MHz	AM	AM	10 kHz	China	0:00 / 0:00

Step 10 – Other Resources

sigidwiki.com - Resource for signal identification

radioreference.com - Database of radio stations, repeaters, and communication frequencies

websdr.org - Tune into SDRs around the world, or broadcast yours to the world

w1hkj.com/FldigiHelp-3.21/Modes - Ham Radio Digital Signals

arrl.org/getting-licensed - Get licensed to broadcast around the world

rtl-sdr.com - Keep up to date with SDR news and experiments

cgran.org - Huge collection of advanced GNURadio blocks

June 25th, 2019

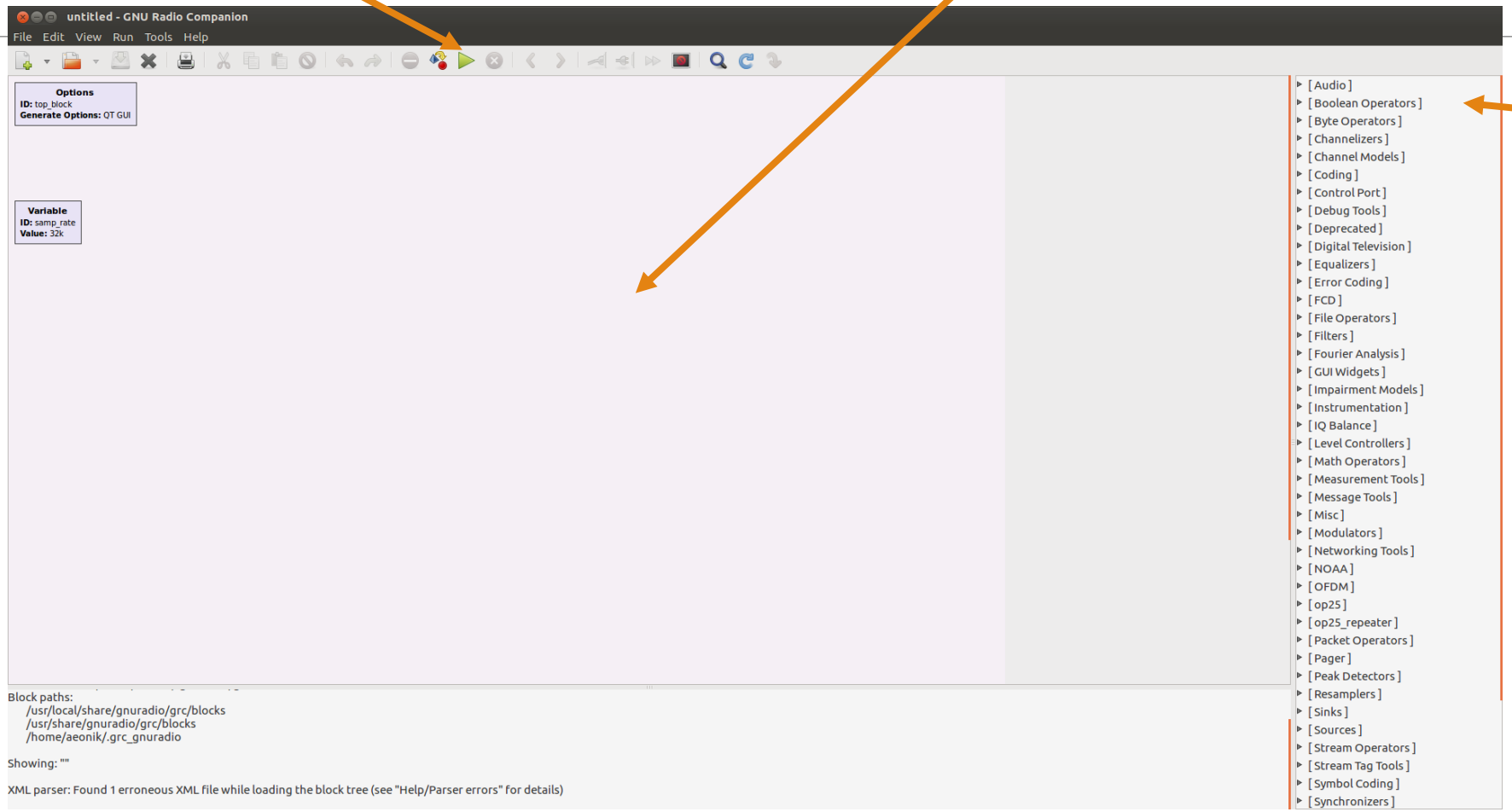
Dave Connett

GNU RADIO GUIDE

GNU Radio Starting Page

Play Flow Chart

Flow Chart Canvas



Function Blocks

Console Output

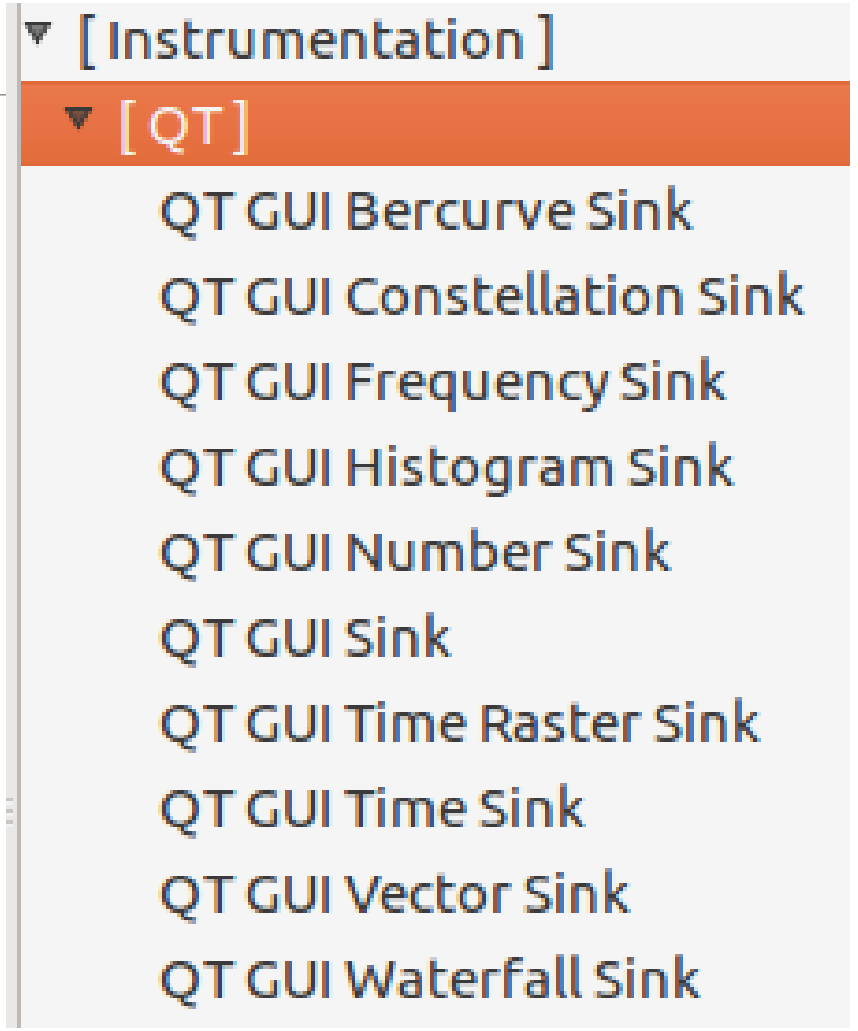
Function Blocks

Must Have Blocks:

- Source
- Sink

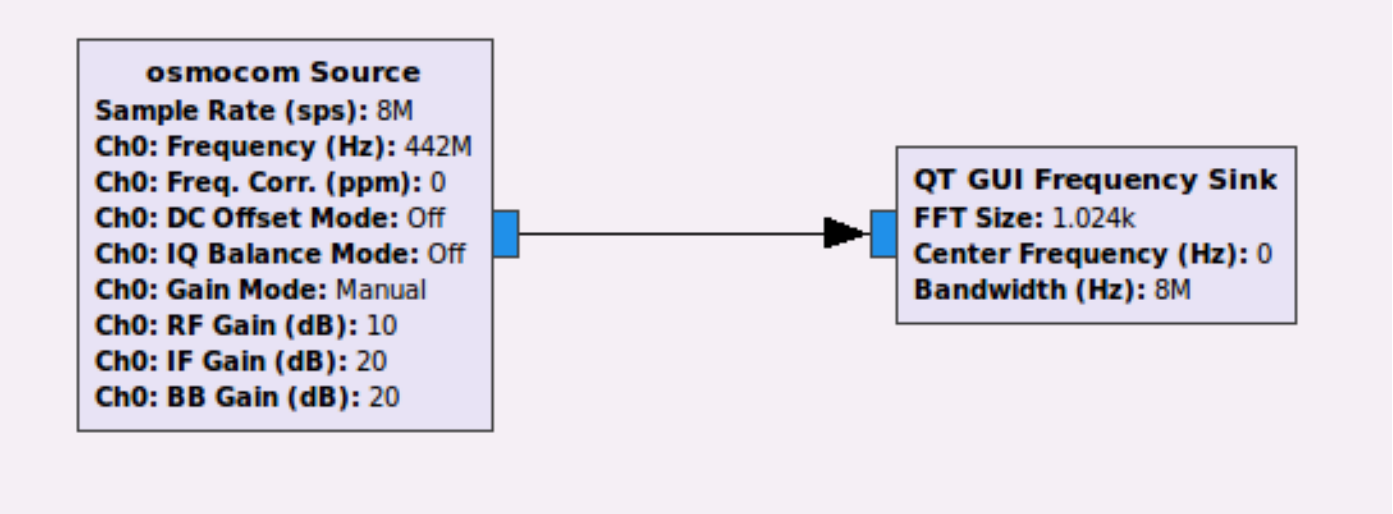
Most Common Blocks:

- Filters
- Instrumentation (aka measurements)
- Modems (Modulators and Demodulators)
- Variables and Controls



Very Simple Flow Chart

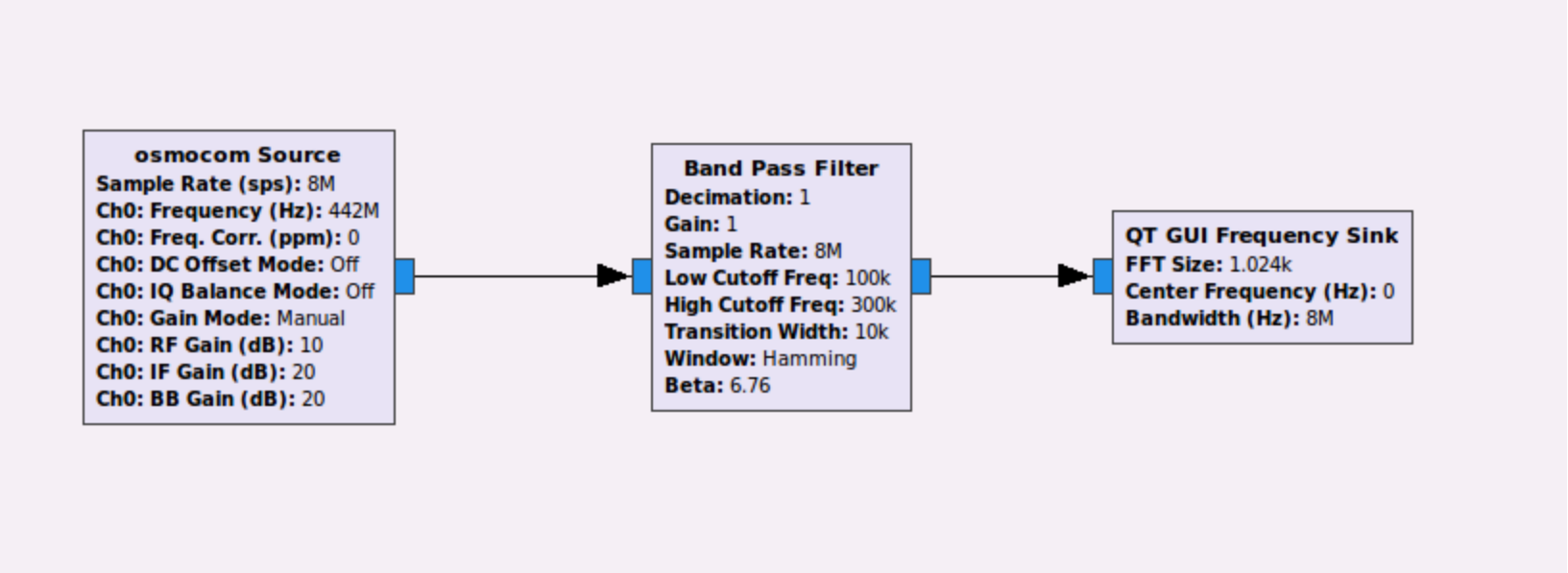
Osmocom Source (HackRF) to Frequency Sink
A very basic copy of GQRX Visuals



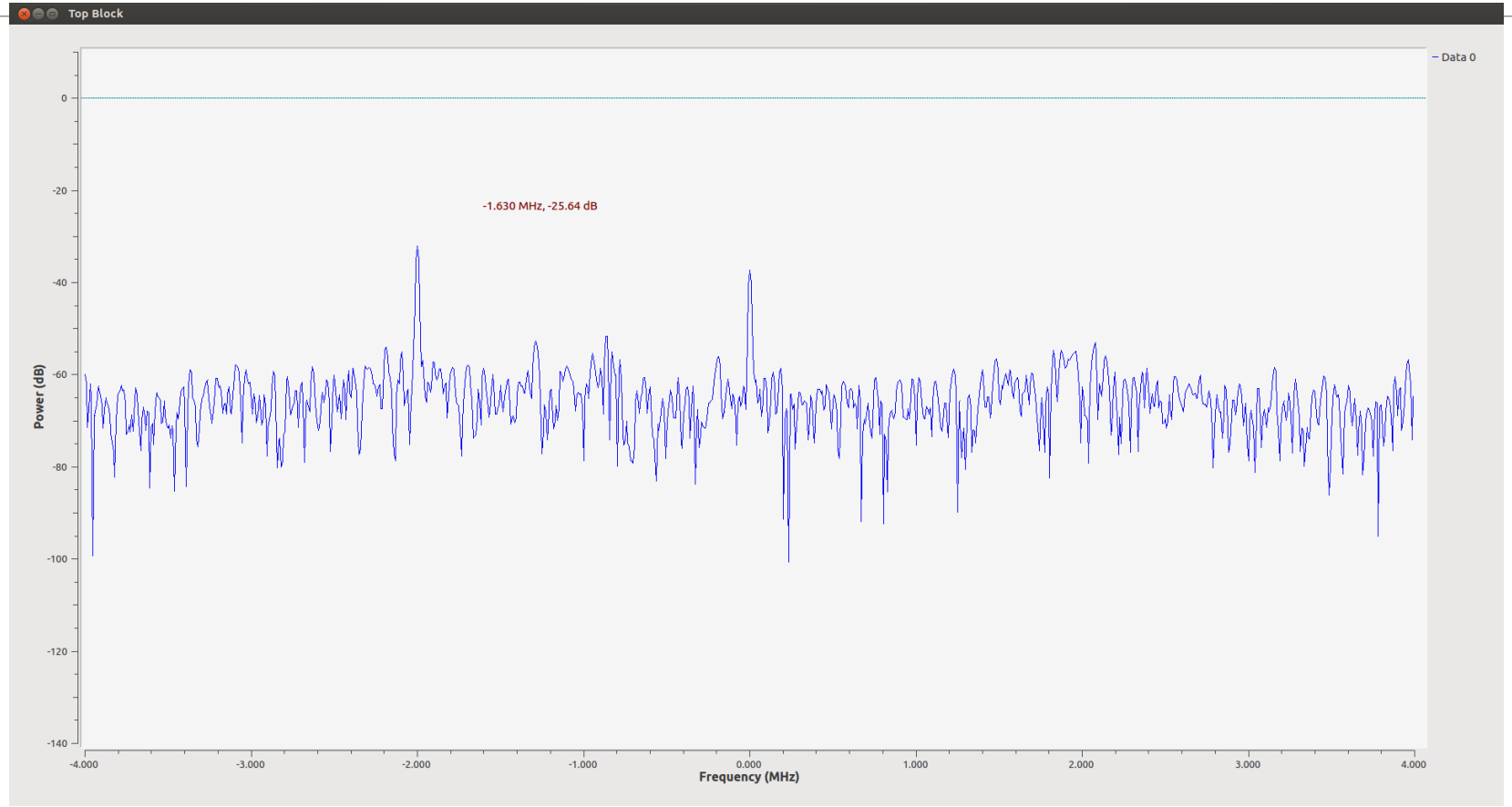
Simple Filter Added

The Band Pass Filter is used to narrow in on a signal

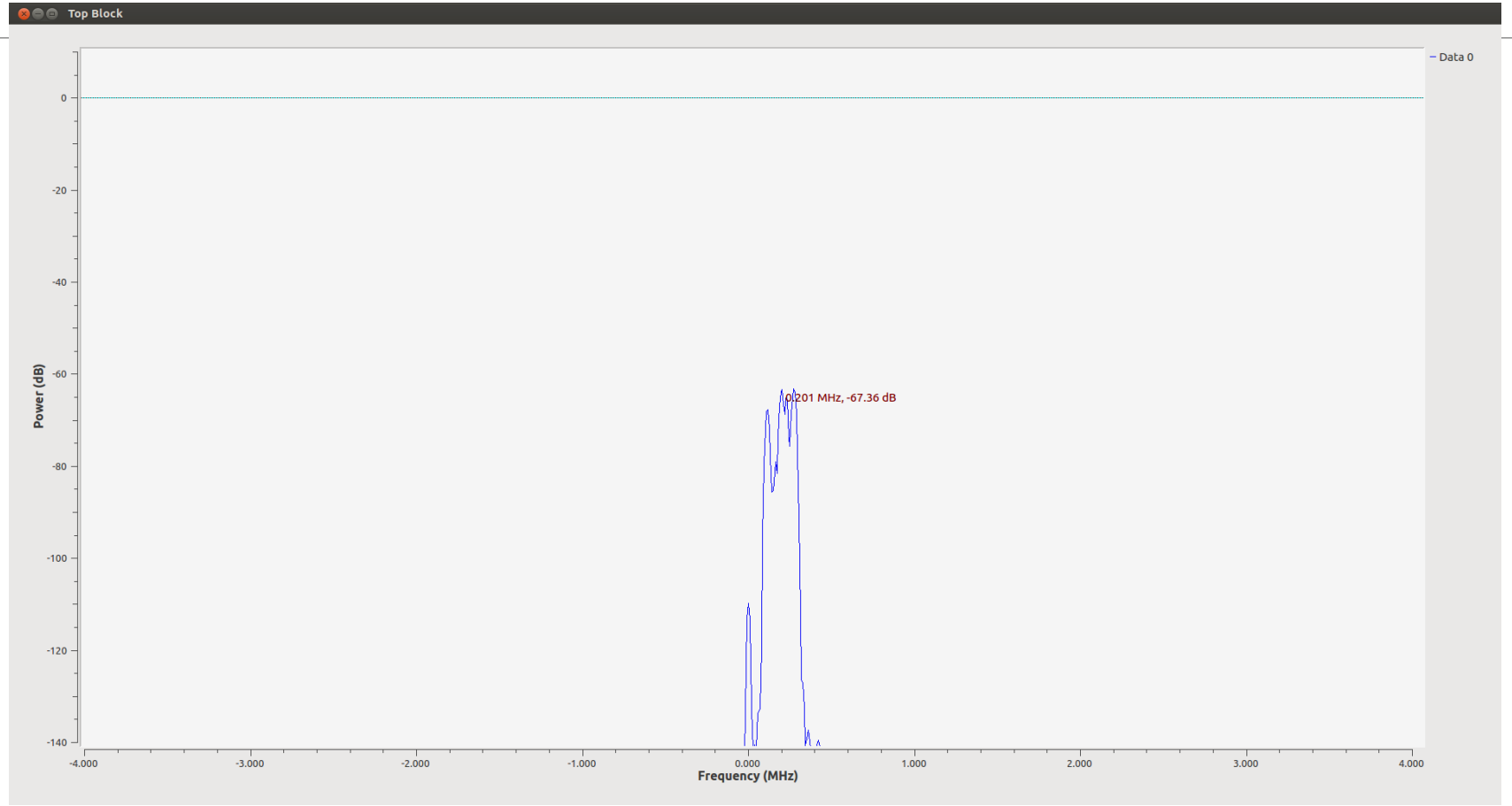
Combination of a low pass and a high pass filter



Frequency Sink Without Filter

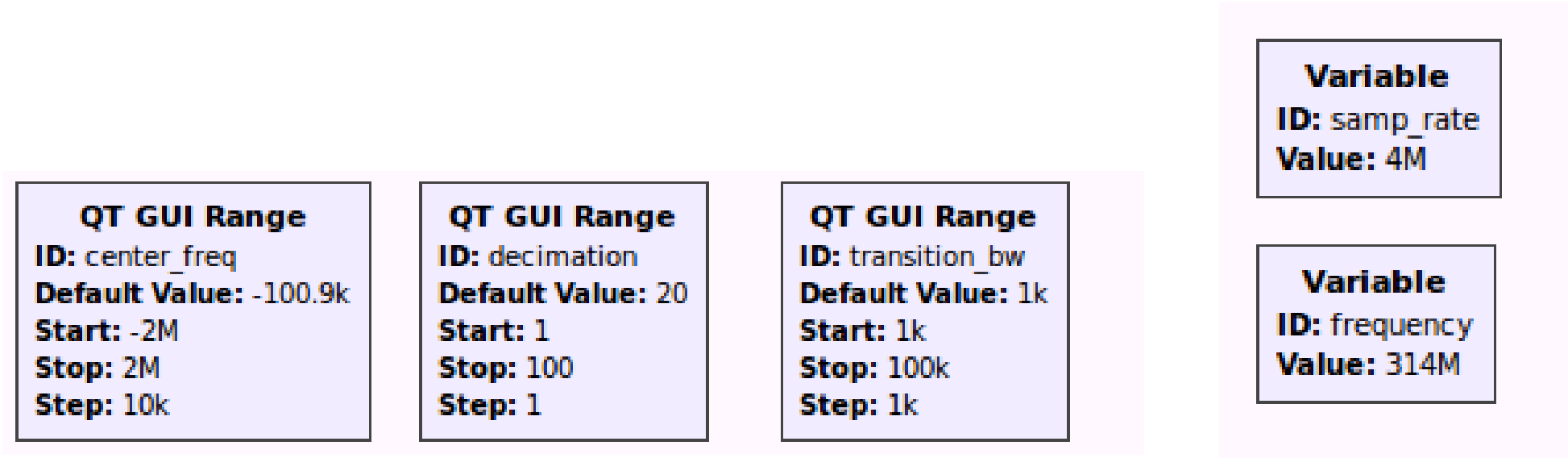


Frequency Sink With Bandpass Filter

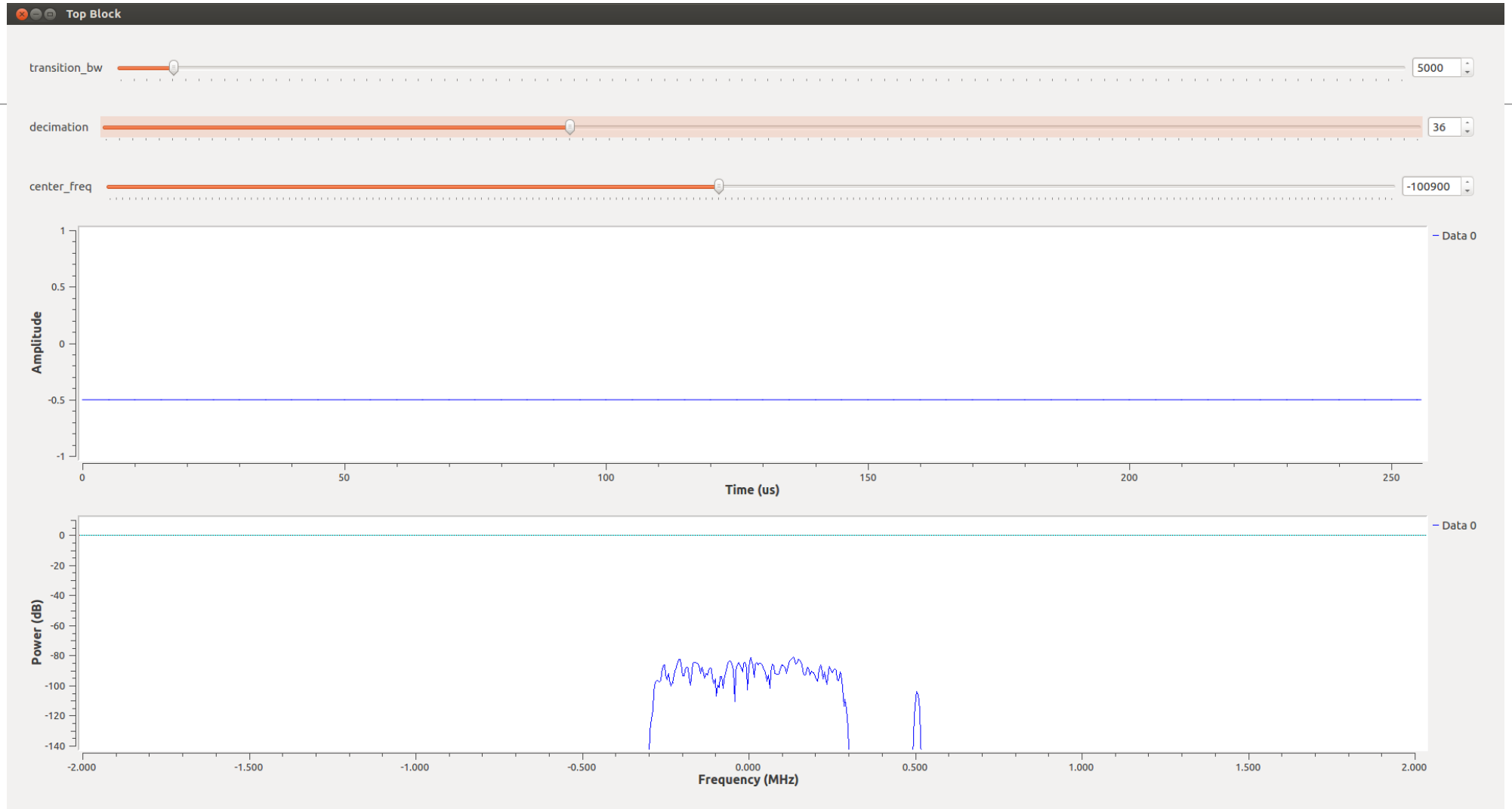


Variables and Controls

- Variables allow us set important settings in one place
- Controls like the ‘Range’ slider bar allows us to change variables live



Example of Range Controls



Block Settings

- Each block can have complicated settings
- Double click to change these settings
- Block will have a red title if there is an error
- To find the right settings: follow our Radio Bible, search the Internet, and learn the theory for each block