L.C.A.R.C.
Lake Conroe Amateur Radio Club
Est. 2019

Intro to SDR with RTL-SDRv3

AC5LC
EM20

Jim Gatwood – WA9JG

http://www.ac5lc.org

Who Am I

- Jim Gatwood
  - e-mail: jgatwood@ftsc.com
  - Twitter: @JimGat
- Director Managed Cybersecurity Services
  - Masters in Cybersecurity
- Blue Teamer
- Incident Responder
- Splunk Guru
- Forensicator
  - CHFI, CEH, …
- Ham Radio Operator WA9JG
  - 30+ years, ac5lc.org
- Hardware Hacker / Designer
- Technology Addict

Presentation Downloads

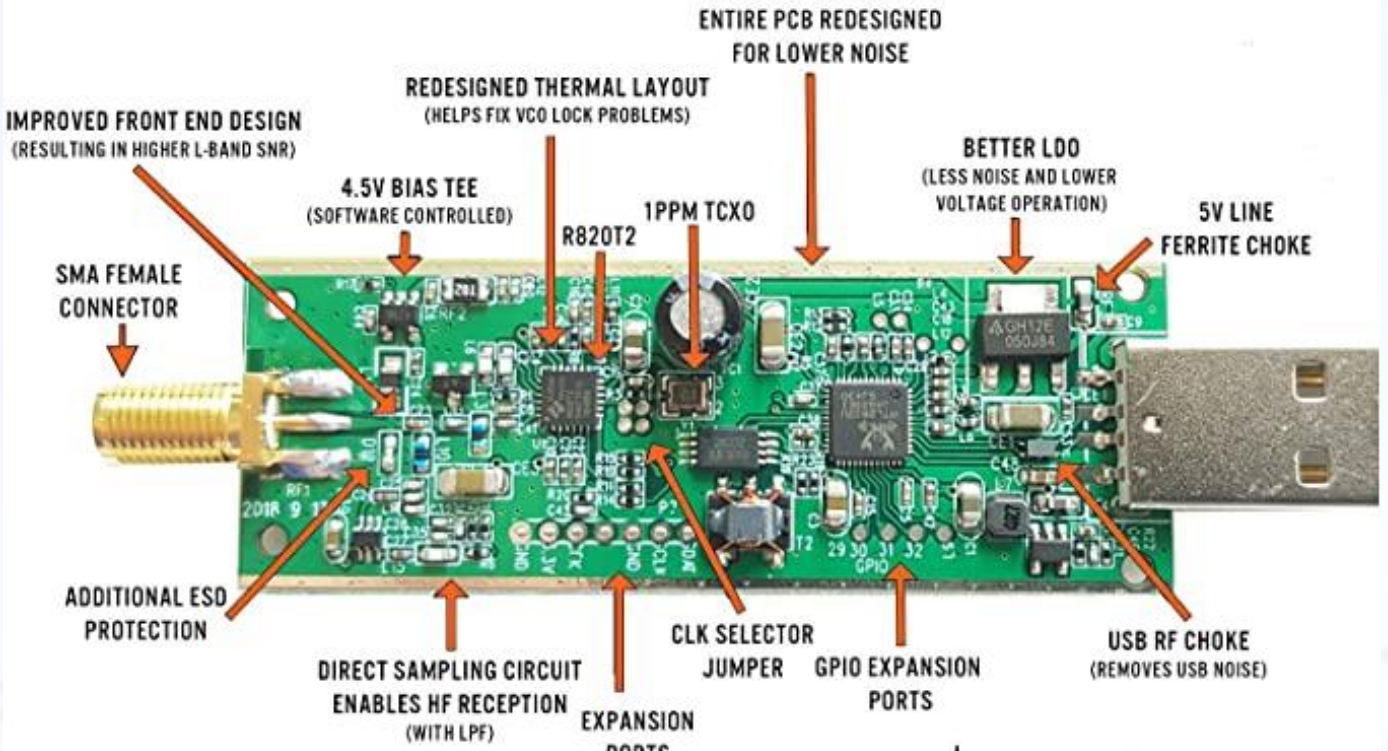
https://bit.ly/3AL4pQr

Suggested Hardware Used for this Presentation

https://www.ebay.com/itm/353279606578?mkcid=16&mkevt=1&mkrid=711-127632-2357-0&ssspo=F-ntAio_RQ6&sssrc=2047675&ssuid=&widget_ver=artemis&media=COPY

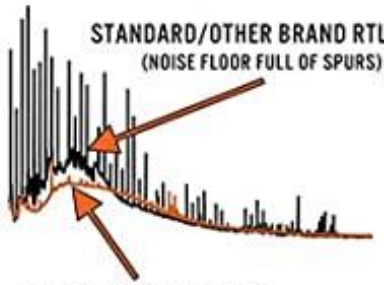
ebay Search = RTL-SDR Blog V3

CHOOSE A GENUINE RTL-SDR BLOG V3



TOUGH CONDUCTIVE
METAL ENCLOSURE
(REDUCES INTERFERENCE)

THERMAL PAD COOLING
(REMOVES HEAT FROM PCB AND
TRANSFERS IT TO THE METAL CASE
RESULTING IN NO HEAT RELATED
VCO LOCK PROBLEMS)



STANDARD/OTHER BRAND RTL-SDR
(NOISE FLOOR FULL OF SPURS)

RTL-SDR V3 NOISE FLOOR
(SIGNIFICANTLY REDUCED
SPURS/BIRDIES)

FULL 2-YEAR WARRANTY AGAINST MANUFACTURING FAULTS
EMAIL & FORUM SUPPORT
SUPPORTS THE BLOG FOR NEW CONTENT, TUTORIALS AND PRODUCTS!

GENUINE GUARANTEE:
BE WARY OF INFERIOR
RTL-SDR BLOG V3 COUNTERFEITS!

RTL SDR BLOG

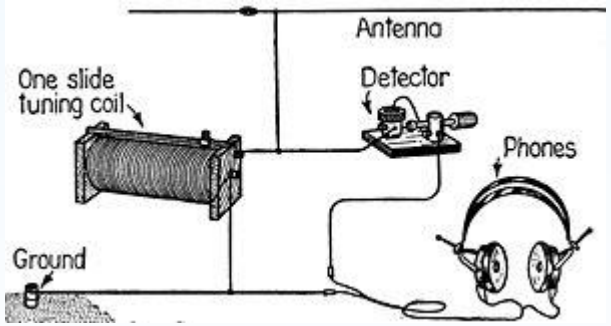
Antenna's Included

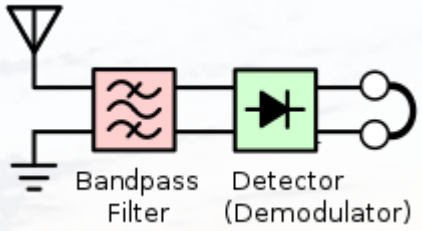
- Short Antennas for Higher Frequencies
- Longer Antennas for Lower Frequencies
- Antennas can capture a portion of the full radio wave. They do not have to equal the length of the radio wave.
  - Standard wavelength multiples for efficient resonant receiving.
    - 1/2, 1/4, and 5/8

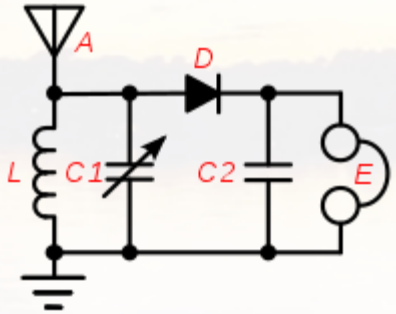
http://RTL-SDR.COM/DIPOLE

Over Simplified Version of a Radio Receiver

- Crystal Radio - https://en.wikipedia.org/wiki/Crystal_radio
  - Antenna
    - Straight piece of wire
      - Ideally resonant length - **468 / freq. in MHz = total length in feet** for a half wave dipole. **Ex. 468 / 0.750 MHz (AM 750) = ~ 624Ft**
        However, normal car AM radio band antennas are much shorter because of the use of different wave harmonics and additional electrical components.
  - Tuned Coil
    - Coiled wire – used as a tunable filter
  - Detector
    - Germanium Diode
    - Crystal “cat whisker” detector
    - Tempered Razor Blade “cat whisker” detector
  - Audio amplification device
    - Crystal Pezo Headphone (Super Sensitive to Small Voltages)







Old School Receivers

- Simple AM Transistor Radio
  - Multiple tuned static components to efficiently receive a specific frequency in every block stage.

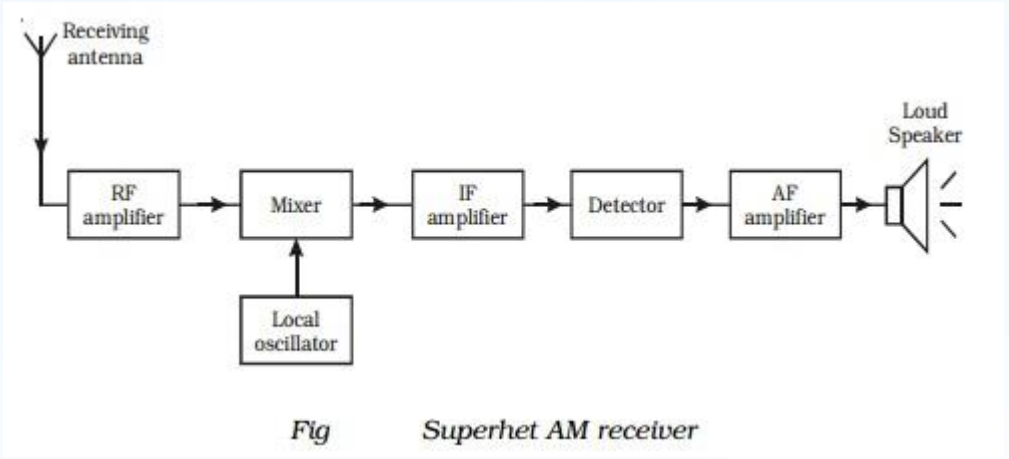
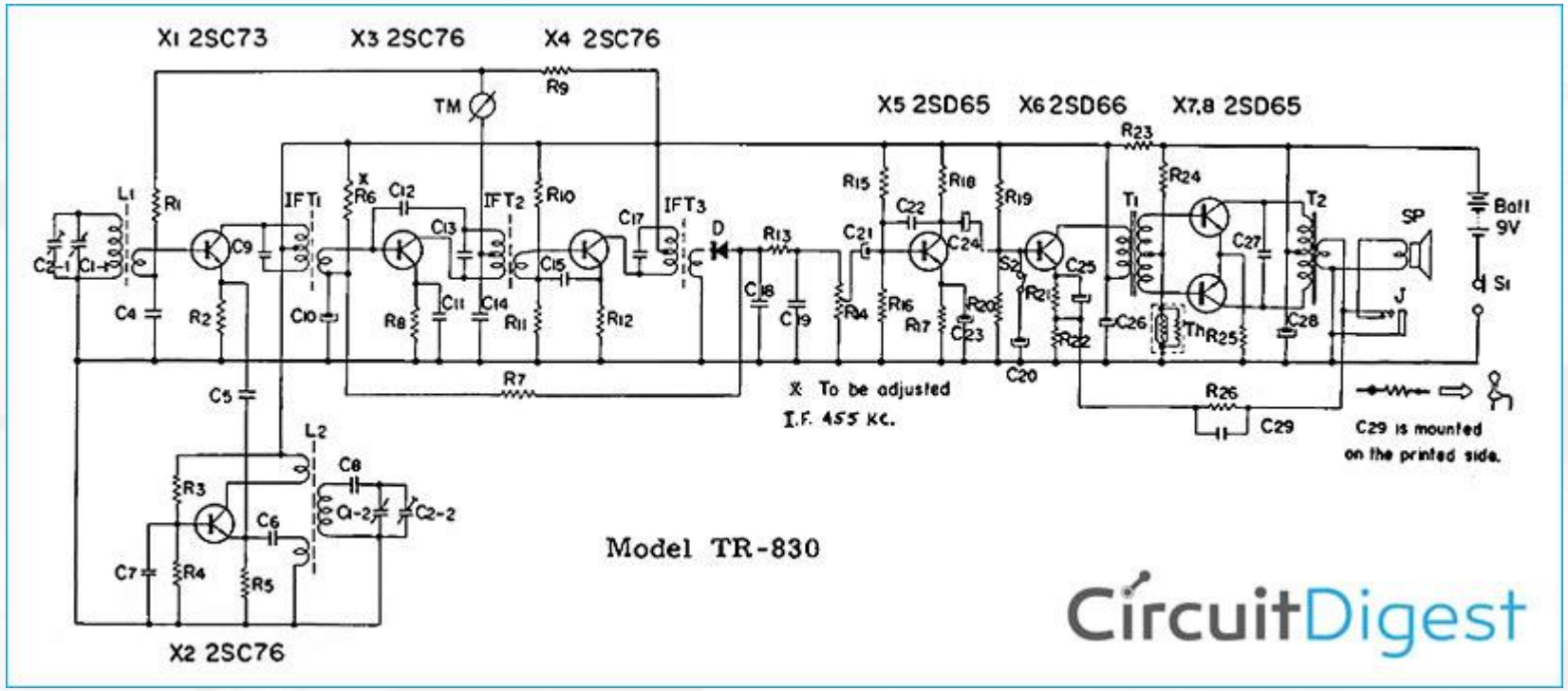


Fig Superhet AM receiver



How Software Defined Radio Works
(In grossly simplified format)

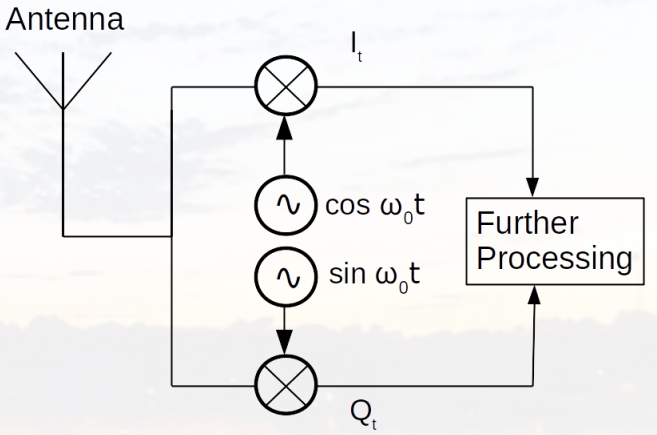
- Reception accomplished using two phase locked Analog to Digital converters (They sample voltage on the antenna wire over time)
  - One sample signal is referred to the **In-Phase (I)**
  - The other is referred to as the **Quadrature (Q)**

Quadrature-sampling is the process of digitizing a continuous (analog) bandpass signal and translating its spectrum to be centered at zero Hz.

Hardware

Software

- The two mathematically congruent samples recombine and are filtered in software to produce the desired signal based on frequency range.
  (Replaces the Mixer, IF and Filter stage of a standard receiver.)
- After the desired signal range is calculated it is passed to a Demodulation Stage to produce audio



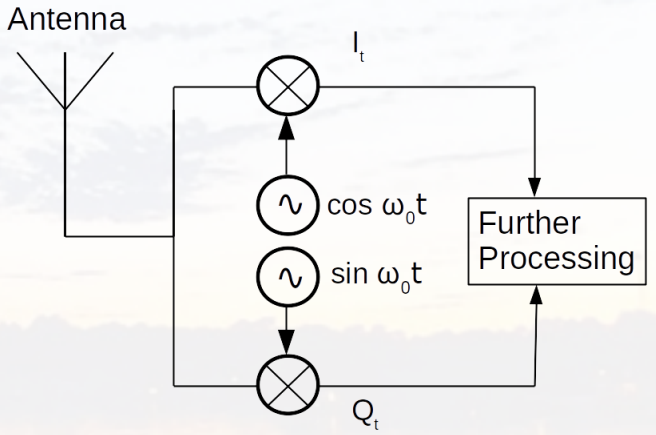
https://arachnoid.com/software_defined_radios/

Scientific Explanation of Quadrature Sampling - https://www.dsprelated.com/showarticle/192.php

DVB-T Dongle with Realtek RTL2832U = Cheep SDR
Max 3 MHz Bandwidth

Interesting Points of the SDR Process

- The I/Q signals are normally converted back to Analog signals that are sample rates similar to digital recorded audio.
  - 44.1KHz to 96KHz
  - Sound Like Static
  - Some ultra wide bandwidth devices directly translate digital IQ to the computer and software via high speed buss.
- Direct Sampling
  - A to D converters Directly Sample Antenna Signal > 2.4MHz on a RTL-SDR
- Standard IQ sampling (Quadrature)
  - Can Include a IQ up converter to establish higher frequency Ranges



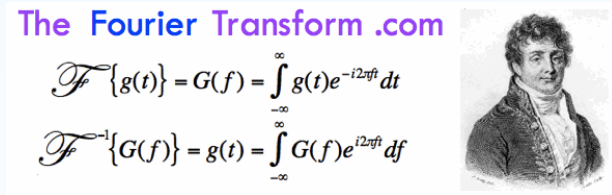
https://arachnoid.com/software_defined_radios/

DVB-T Dongle with Realtek RTL2832U = Cheep SDR Max 3 MHz Bandwidth

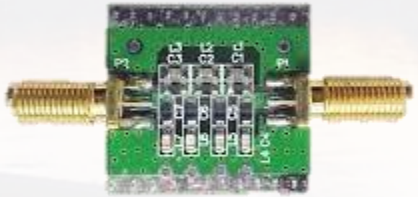
Why Software Defined Radio

- Larger Frequency Ranges with Fewer Analog Filter Components
  - Simplification of radio architectures and improved overall performance
  - The chance for new experimentation
- Dynamic Detector Stage
  - Can be modified by changing software code
    - Ability to alter functionality by downloading and running new software at will
  - New methods of detection and modulation/demodulation can be written using same hardware
  - The opportunity to recognize and avoid interference with other communications channels

Down Sides of SDR



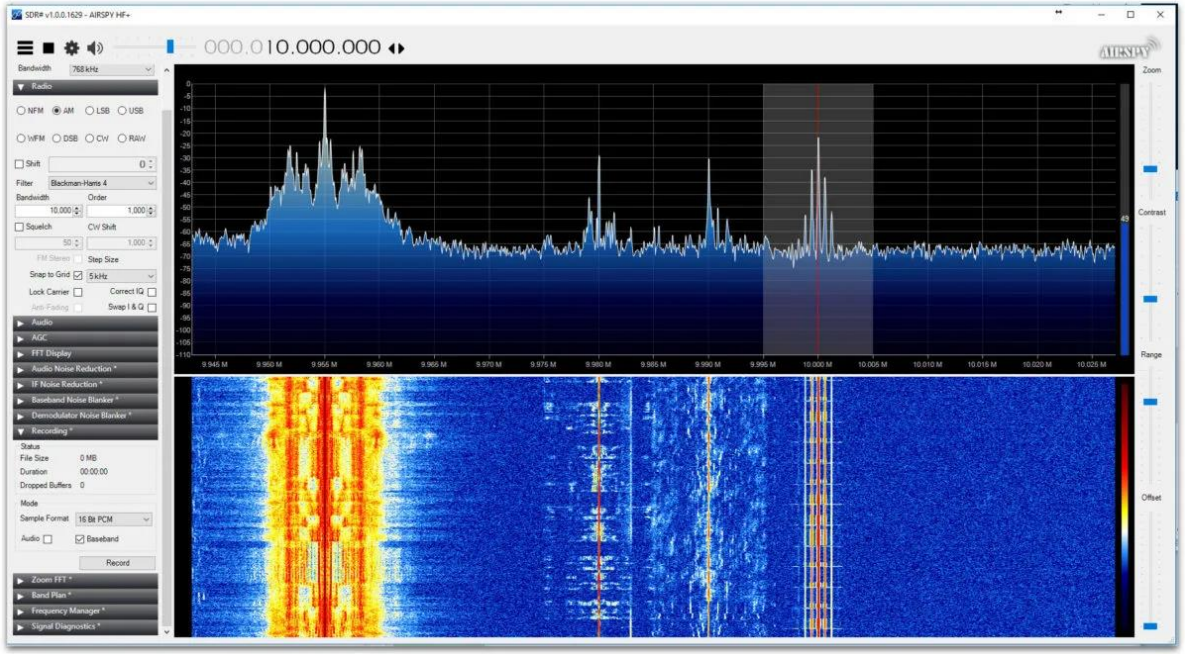
- Complex software required to operate the SDR
- Poor dynamic range in some SDR designs
  - Dynamic range is the ratio of the largest tolerable signal to the smallest usable signal.
    - Receiver dynamic range is a central issue for software-defined radio (SDR) designers today and a major obstacle to advancement in digital receiver designs. The challenge is to find an effective digital signal processing (DSP) implementation of receiver functions that achieves dynamic range sufficient for the frequency range of interest, whether it is HF, VHF or above.
    - Can be marginally mitigated in software by running them through mathematic concepts such as Fourier Transforms and other software filters.
    - Can be improved by adding hardware filters.



SDR Software

Fun Fact: The term "software radio" was coined by a team in Garland, TX in 1984 at what is now Raytheon

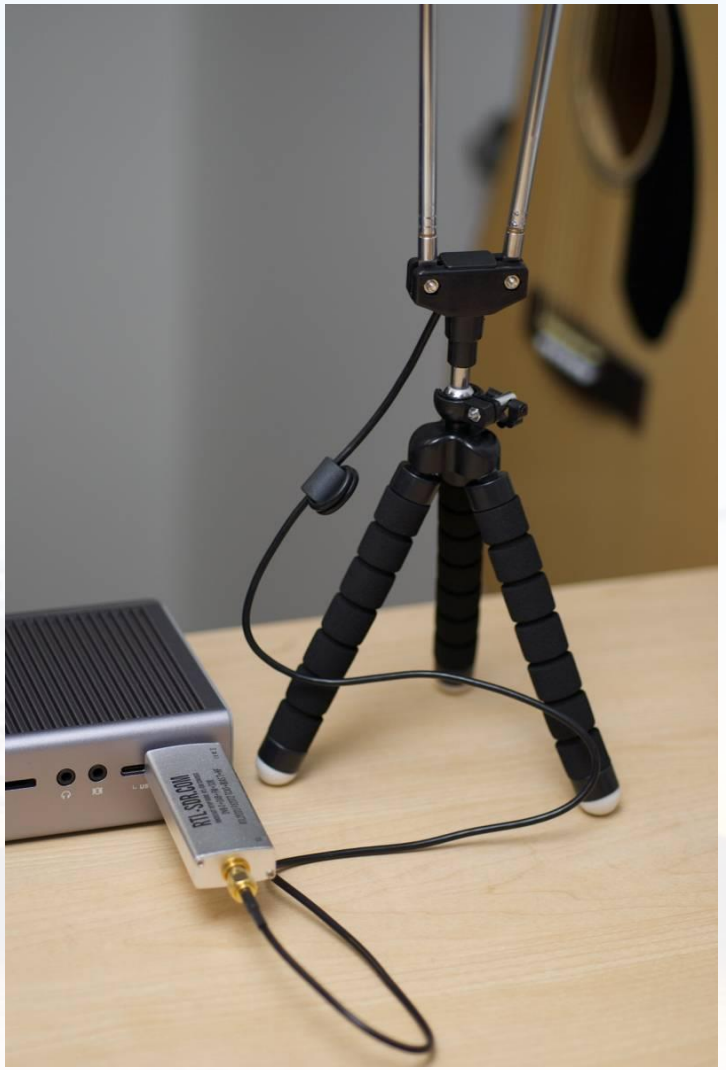
- Steps to get your SDR working
  - Install / Replace Drivers
    - Some operating systems identify the RTL2832U and auto install DVB-T drivers (Windows)
    - Some Linux distros include all kernel modules required to operate as an open SDR
  - Install SDR software
  - Understand configuration options
  - Start Listening
  - Windows- SDR#, HDSDR, GNU Radio
  - Linux- GQRX
  - Mac- CubicSDR, GQRX, GNU Radio



Connecting Antennas

- Connect the Antenna T to the SDR
- Connect the T to the Tripod or Suction Cup
- Screw the Long Antennas into the T
- Extend them about half their length

Long Wire Available on E-bay
https://www.ebay.com/itm/384773416124

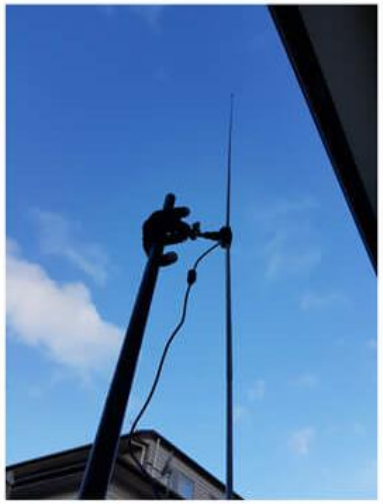


Antenna Orientations

Window Suction Cup Mount

V-Dipole Satellite Orientation

Flex Tripod Mount on Table



Flex-Tripod Mount to Pole

Flex Tripod Mount to Tree

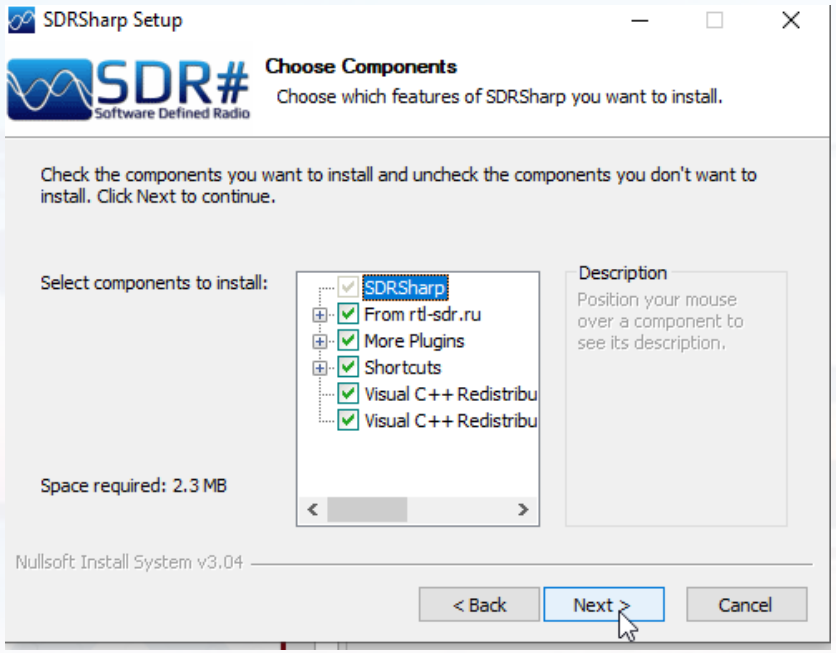
Flex Tripod Mount to Door

[Wide Band Antenna Options https://youtu.be/-vCu-npZSro](https://youtu.be/-vCu-npZSro)

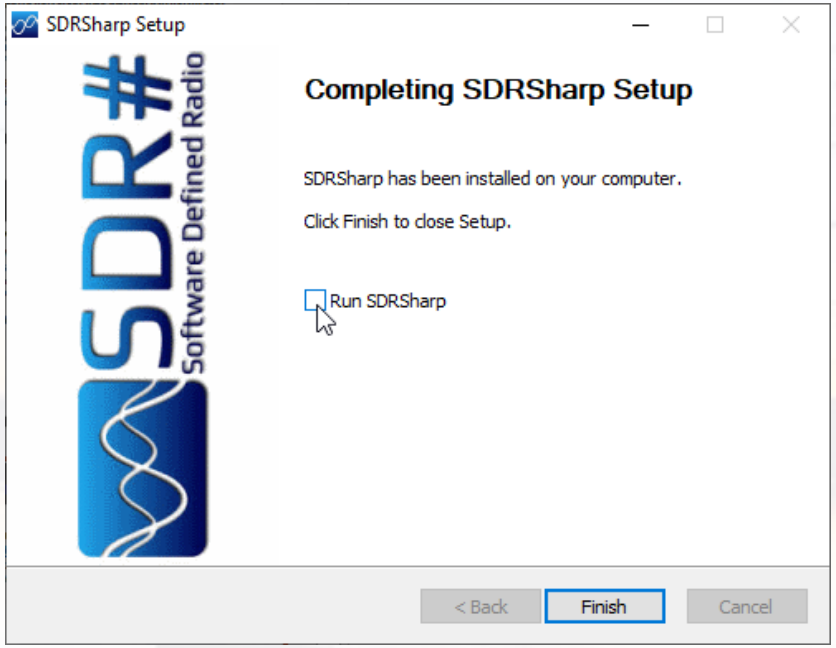
Windows Drivers / SRD Sharp (#)

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

- Get Full Install with Community Plugins
  - https://airspy.com/?ddownload=5544 (exactable installer simpler than Zip)
  - Run SDRSharp-installer.exe - Select defaults



- Let downloads complete
- Uncheck “Run SDR#” and Finish

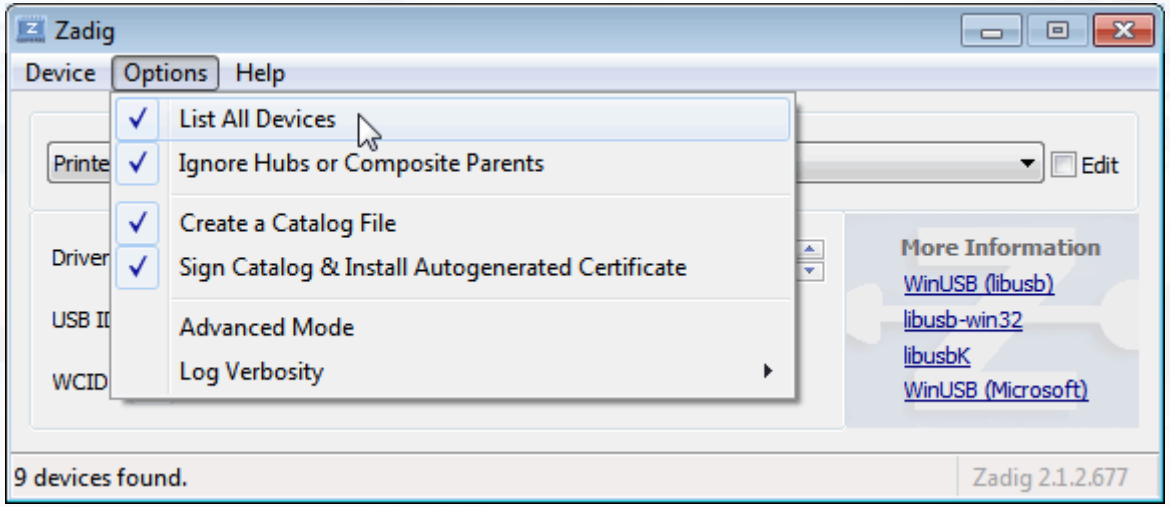


Windows Drivers / SRD Sharp (#)

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

- Plug In RTL-SDR
- Replace/Install USB Driver
  - Run Zadig from the SDR Sharp program group

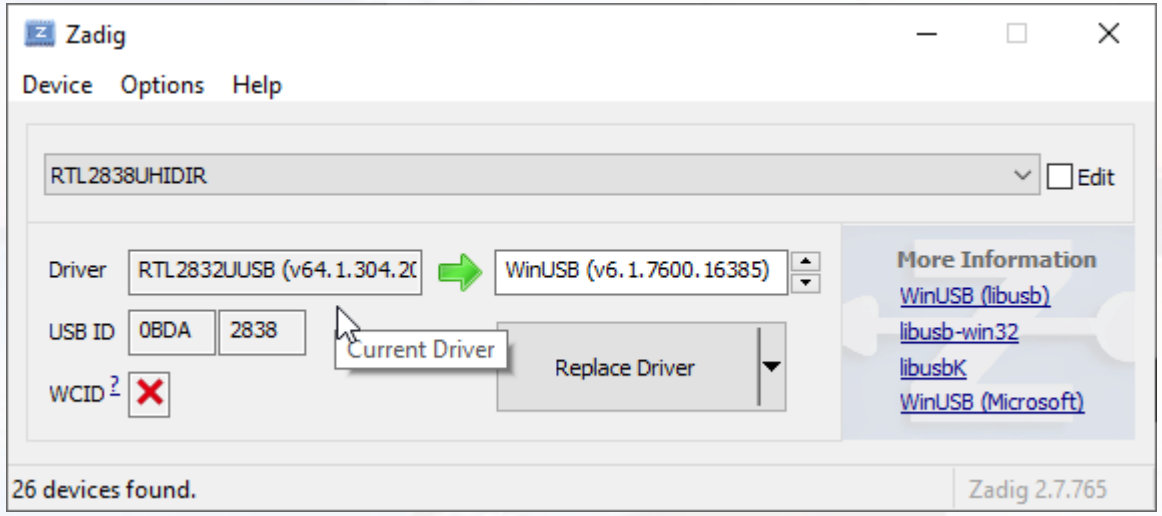
  - Go to "**Options->List All Devices**" and make sure this option is checked
  - In some cases you may need to also uncheck "**Ignore Hubs or Composite Parents**“ to see the RTL-SDR



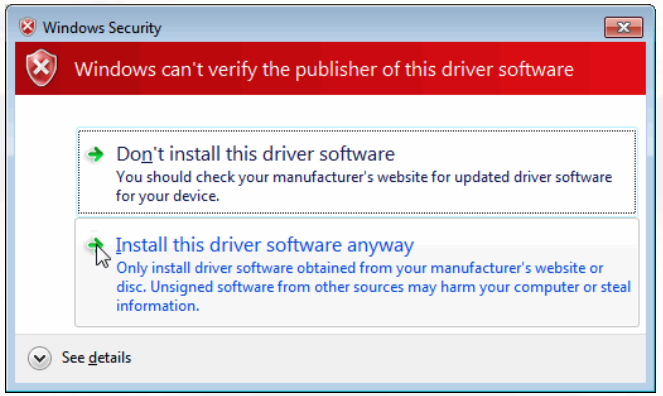
Windows Drivers / SRD Sharp (#)

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

- Replace/Install USB Driver
  - From the device drop down look for **RTL2832UHIDIR**, **RTL2832U**, or **Bulk-In, Interface (Interface 0)** ** Make Sure it is Zero and not 1 When selected you can also verify the USB ID is "0BDA 2838"*
  - In the right side driver window make sure **WinUSB** is selected
  - Be careful not to replace the driver of another USB device you will break it! To fix the error you will have use device manager to remove/update the driver of your original device.
  - Click **Replace Driver**



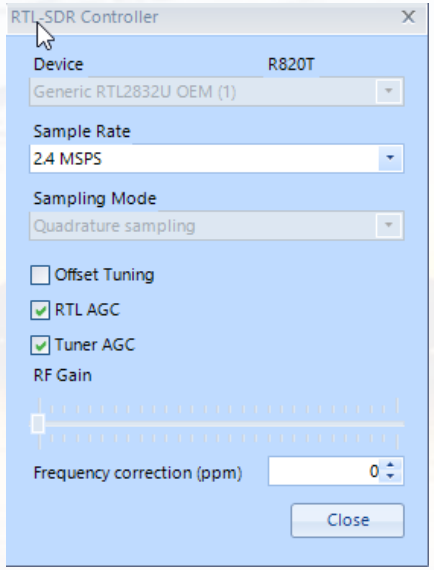
Note: On some PC's you might get a warning that the publisher cannot be verified, but just accept it by clicking on **"Install this driver software anyway"**. This will install the drivers necessary to run the dongle as a software defined radio.



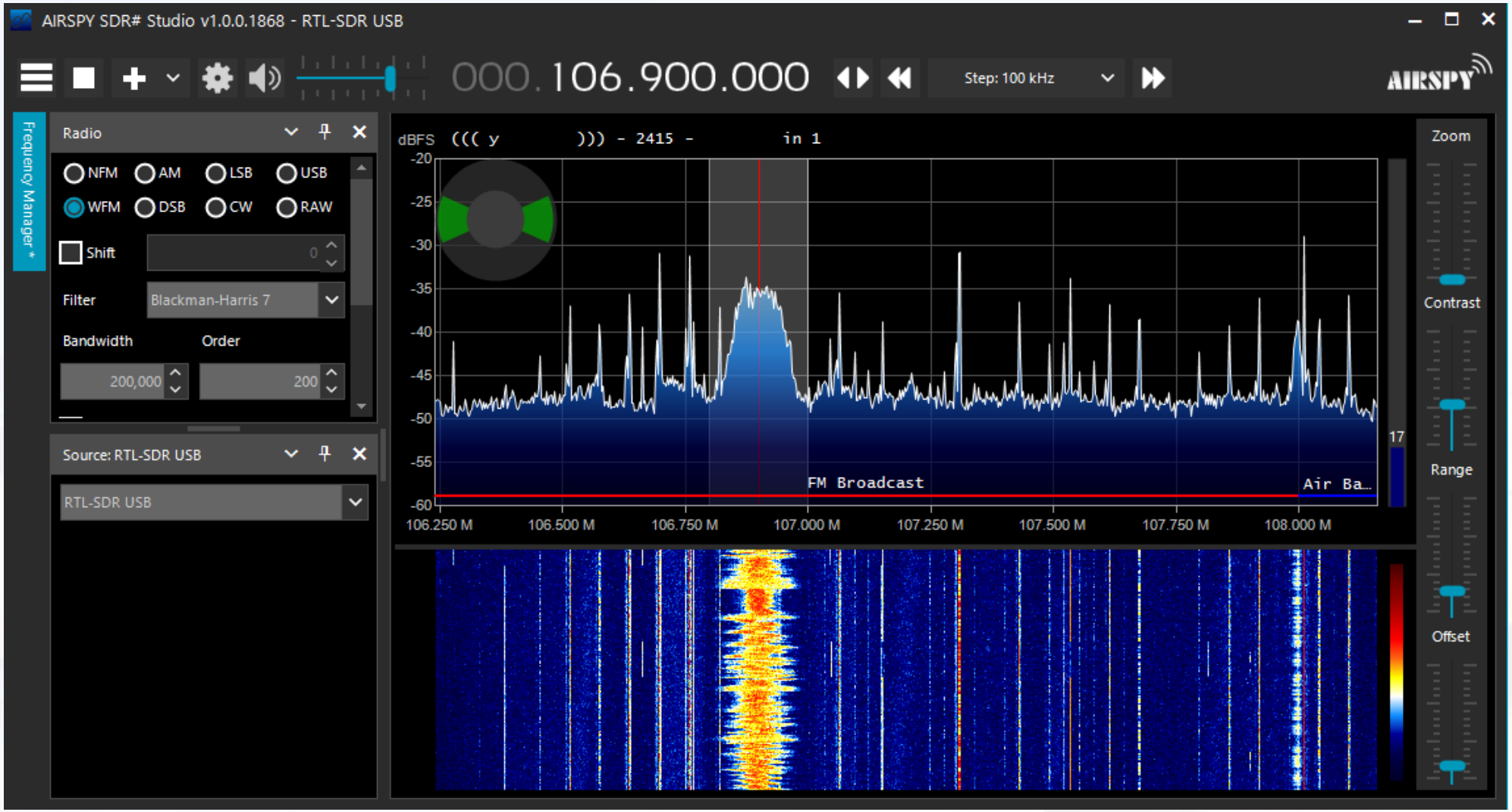
Windows Drivers / SRD Sharp (#)

- Run SDRSharp from the SDR Sharp Program Group 

  - Allow access to private networks if prompted by defender
  - On the top Menu Bar click the hamburger stack 
  - Click the source menu. There will now be a source window in the stack to the right.
  - In the dropdown directly under the Source window title (will probably say AIRSPY R2 / Mini) click the dropdown arrow.
  - Select RTL-SDR USB from the list
  - Press the Start Button to the Right of the hamburger stack 
    - You should hear static or music if tuned to a FM station with Antennas Attached
  - To increase the sensitivity click the Gear on the menu bar. 
    - In the RTL-SDR Controller Window Select **RTL AGC** and **Tuner AGC**



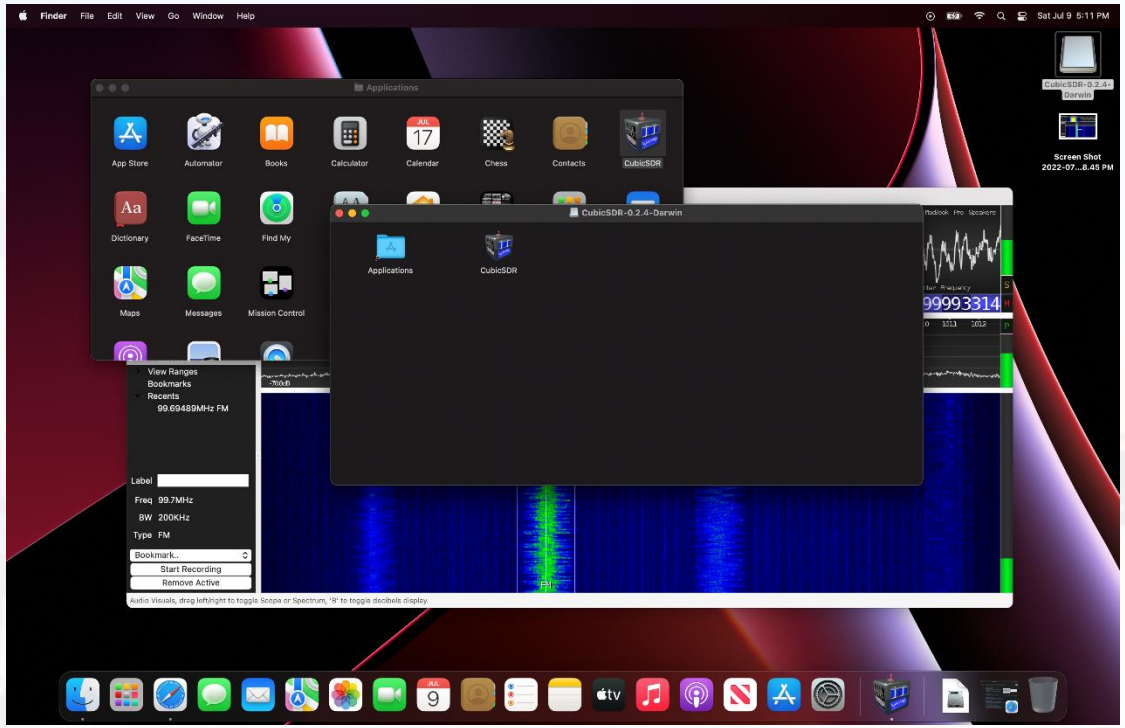
SDR#

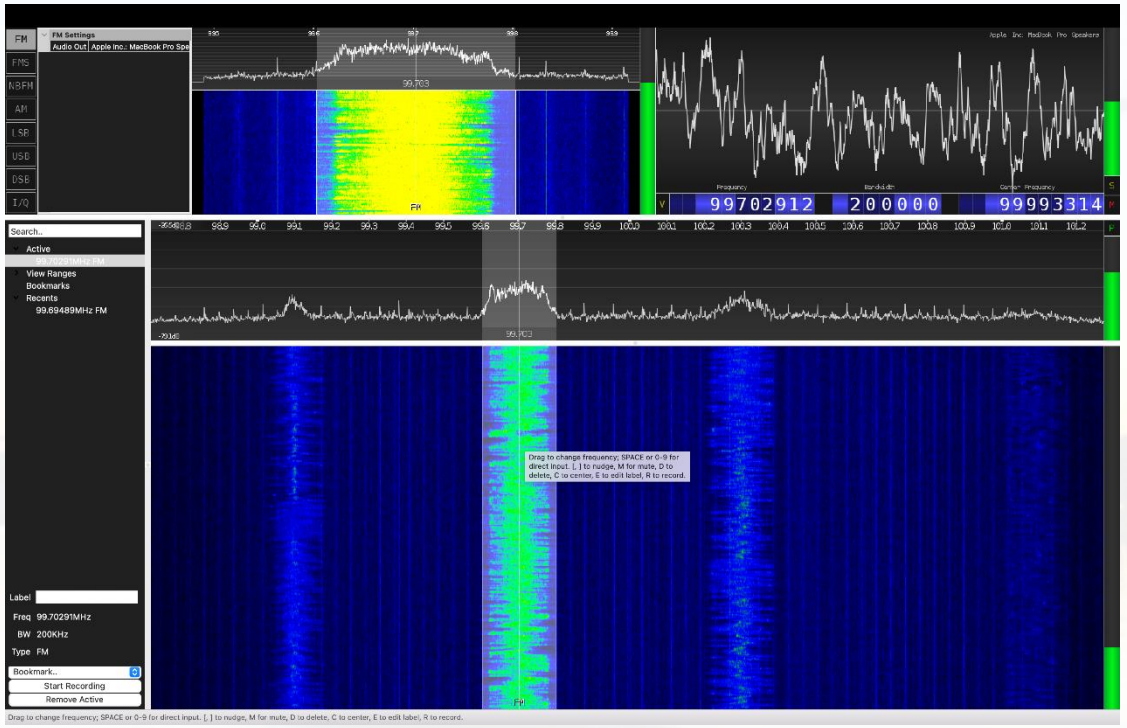

AIRSPY SDR# Studio v1.0.0.1868 - RTL-SDR USB
000.106.900.000
Step: 100 kHz
AIRSPY
Frequency Manager *
Radio
NFM
AM
LSB
USB
WFM
DSB
CW
RAW
Shift
0
Filter
Blackman-Harris 7
Bandwidth
Order
200,000
200
Source: RTL-SDR USB
RTL-SDR USB
dBFS (((y))) - 2415 - in 1
-20
-25
-30
-35
-40
-45
-50
-55
-60
FM Broadcast
Air Ba...
17
106.250 M
106.500 M
106.750 M
107.000 M
107.250 M
107.500 M
107.750 M
108.000 M
Zoom
Contrast
Range
Offset

MAC Software CubicSDR

https://cubicsdr.com/

- Download dmg file from https://github.com/cjcliffe/CubicSDR/releases/download/0.2.4/CubicSDR-0.2.4-Darwin.dmg
  - May require install of Rosetta if not installed
- Open Download – Move to Applications Folder
- Insert RTL-SDR – May require a USB C to A Adapter or Hub
- Open CubicSDR App – May ask if your sure you want to run a downloaded App
- Select RTL2832 – Tune and listen

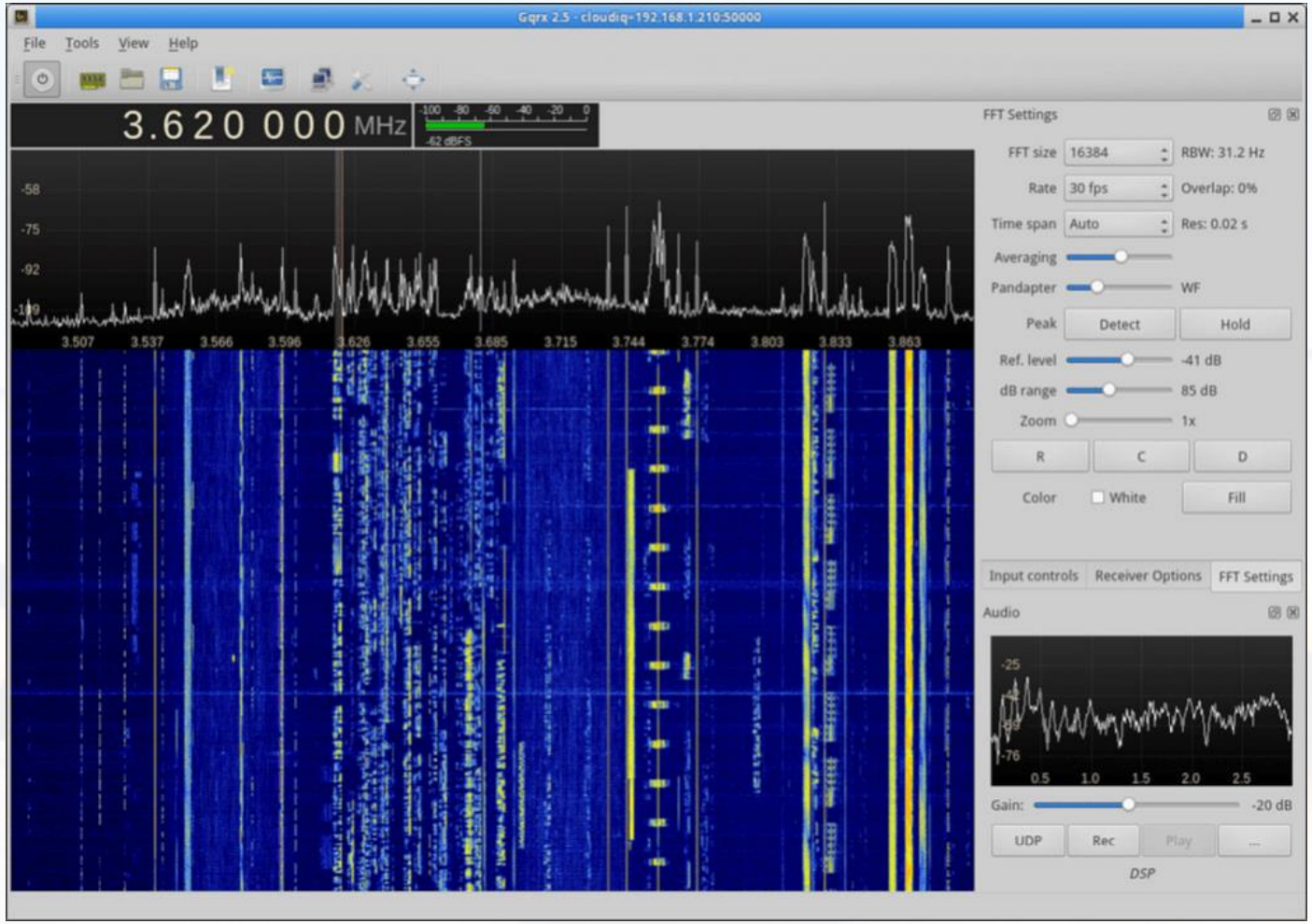




Linux / Raspberry Pi Software
GQRX – Powered by GNU Radio

- Debian: sudo apt-get install gqrx
- Redhat: sudo yum install gqrx
- Plug in RTL-SDR
- Launch from DM of choice
- Choose RTL-SDR from Dropdown
- Tune and Listen

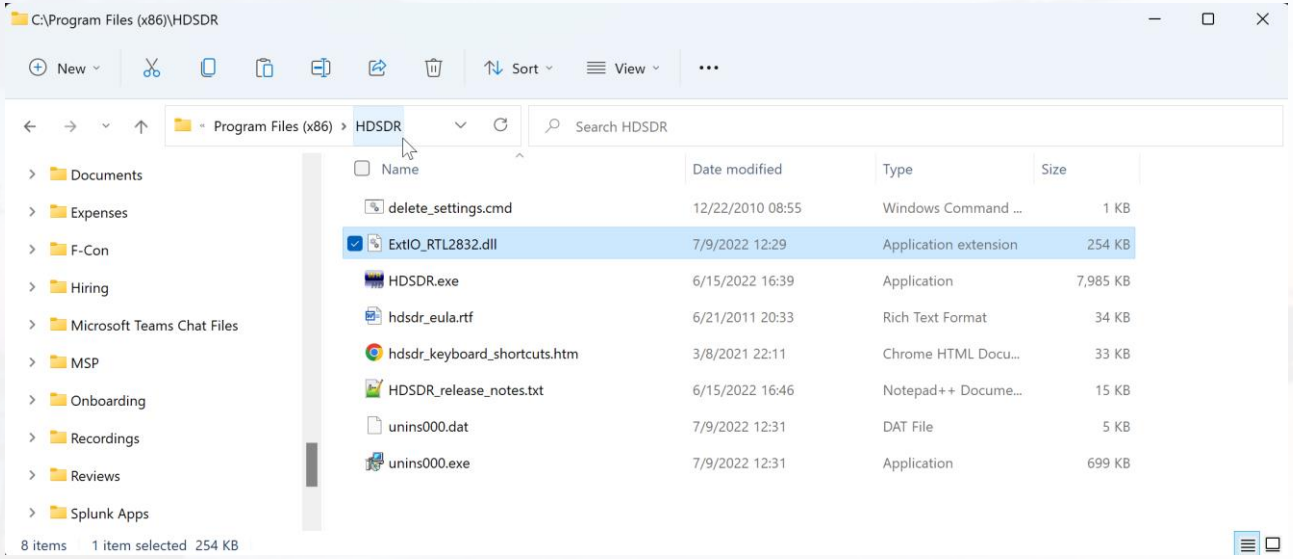
- Other Distros of Linux follow GNU Radio Install or Build Instructions https://wiki.gnuradio.org/index.php/InstallingGR

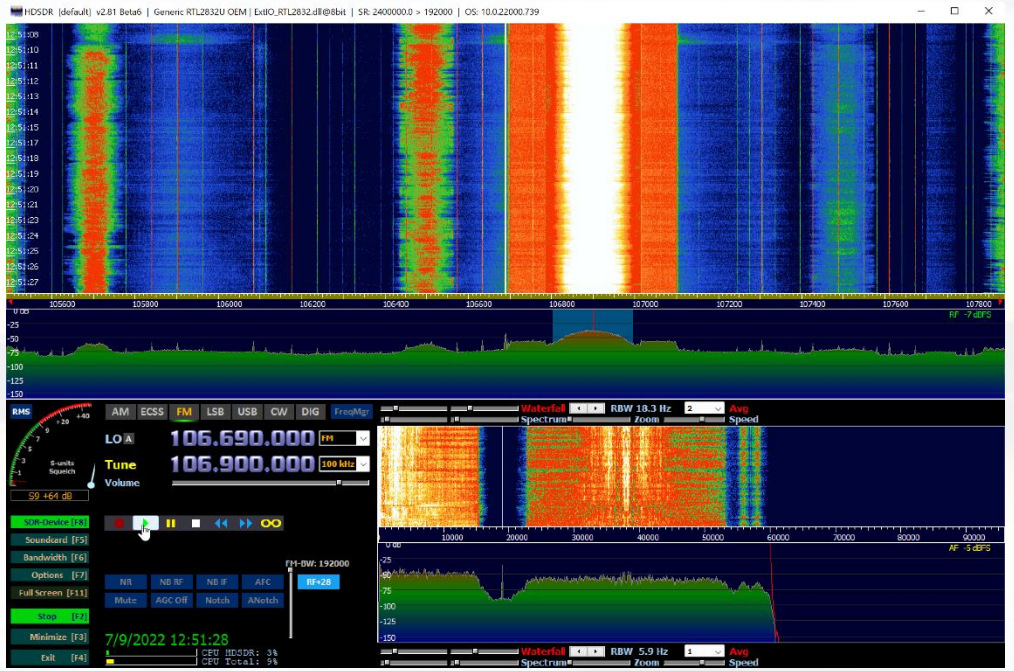


Alternate Software
HDSDR – Windows

http://www.hdsdr.de/

- Smooth Ham Radio Like Interface – Ideal for Ham Radio Pan Adapter
- Works well with WIN11 SDRSharp Still Has Glitches
- Minimal setup if Zadig WinUSB Drivers Installed - Supports V3 Bias T
  - Download Program - Install
  - Download ExtIO_RTL2832.dll - Place in program Directory



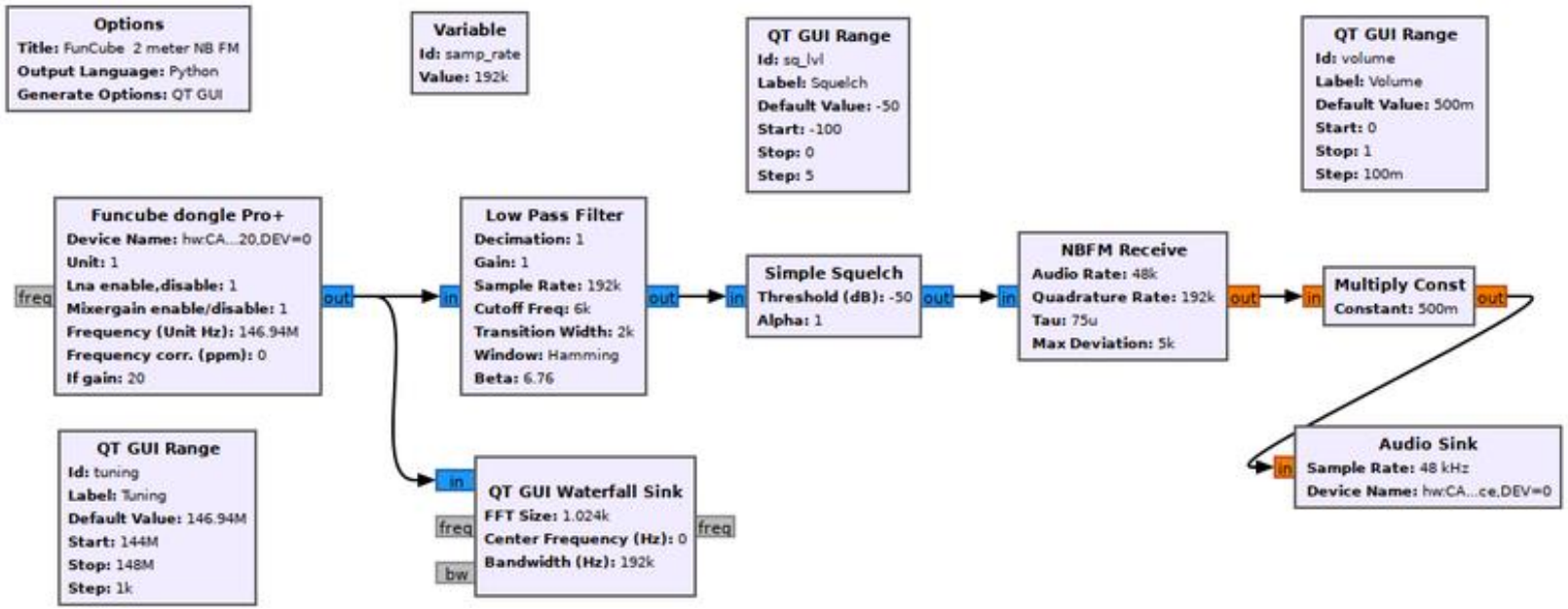


Alternate Software
GNU Radio – Linux, Windows, and MAC

https://wiki.gnuradio.org/

- Great for Experimentation – **Non Techies Beware**
- Receives and Transmits (on capable hardware)
- Requires a high Level of Configuration
- UI Uses Block Diagrams that Represent Python Functions

Linux	1.Install Ubuntu 20.04 (either as a VM or natively) 2.sudo add-apt-repository ppa:gnuradio/gnuradio-releases-3.9 3.sudo apt-get update 4.sudo apt-get install gnuradio python3-packaging	v3.9.5
Windows	1.Install the latest Radioconda installer 2.Launch "GNU Radio Companion" from the Start menu	v3.10.3
macOS	1.Install Homebrew 2.brew install gnuradio	v3.10.2



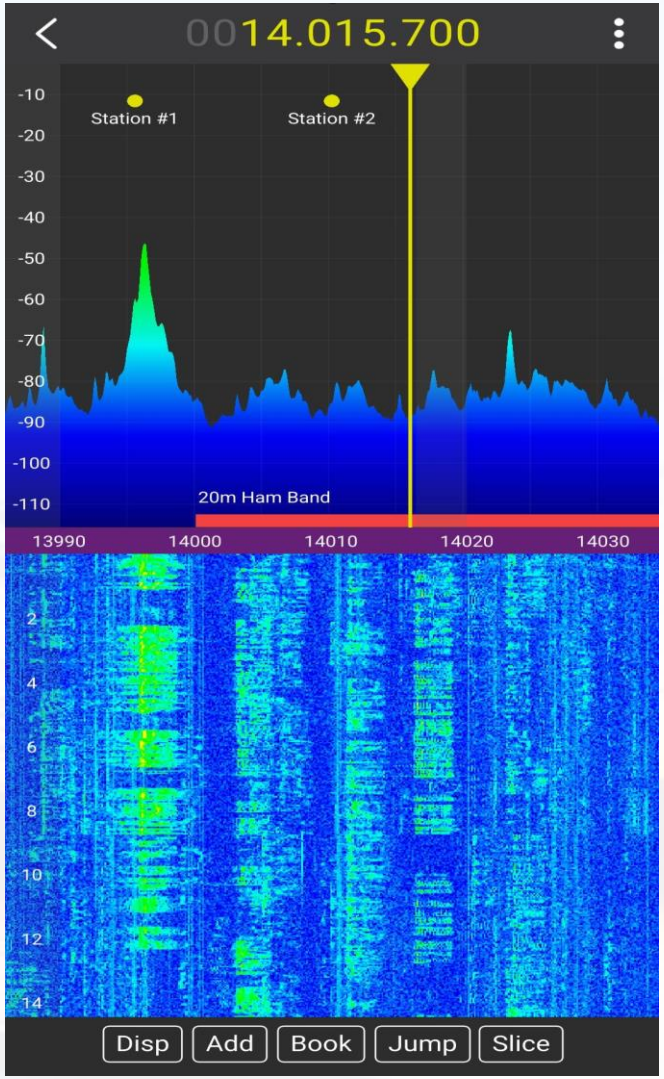
Alternate Software
MagicSDR – Android and Apple

https://magicsdr.com/

- Use an OTG cable to connect Directly to RTL-SDR or Network using an rtl_tcp server
- Supports AM, SSB, CW, NFM, WFM Demodulation

Download MagicSDR

Get it on Google Play Get it on App Store

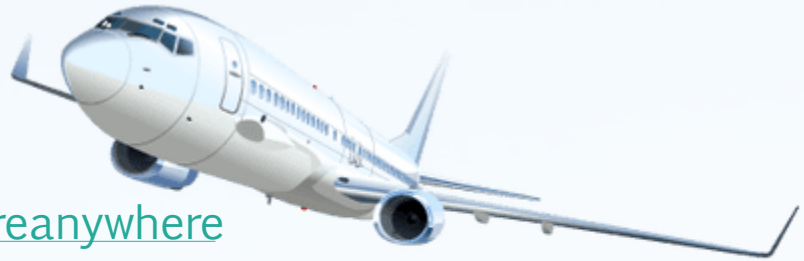


For Hackers

- 433MHz
  - RTL_433 – Temp and Humidity Sensors
    - Tech Minds Tutorial https://youtu.be/JdzVIjKA68o
    - https://github.com/winterrace/rtl_433_win/releases/
  - Wireless Door Bells
    - Ding Dong Ditch - https://youtu.be/BnwBdeQB7vQ
- Key Fob Decoding
  - Sammy Kamkar
    - DEF CON 23 - https://youtu.be/UNgvShN4USU
    - HACKADAY - https://youtu.be/tlwXmNnXeSY

Find the Frequency Range on any FCC approved device https://fccid.io

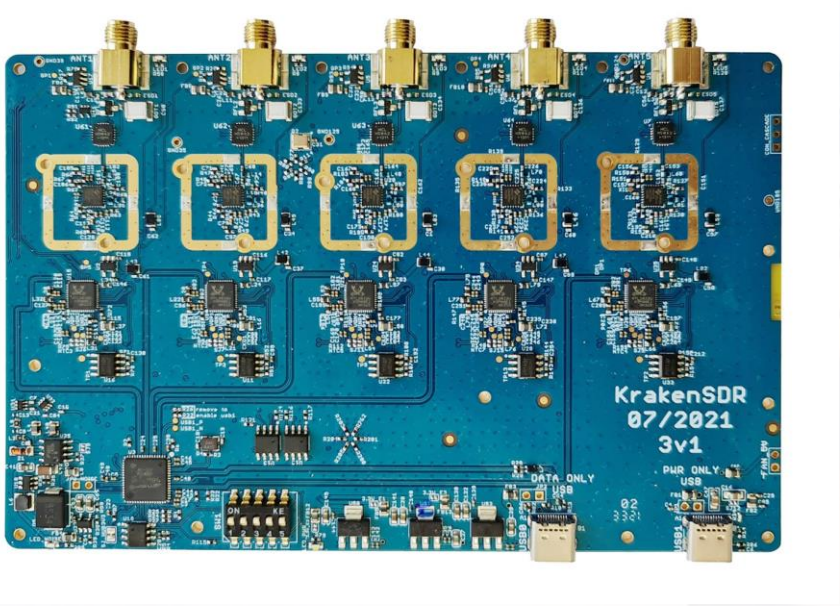
For Nosy Nellies

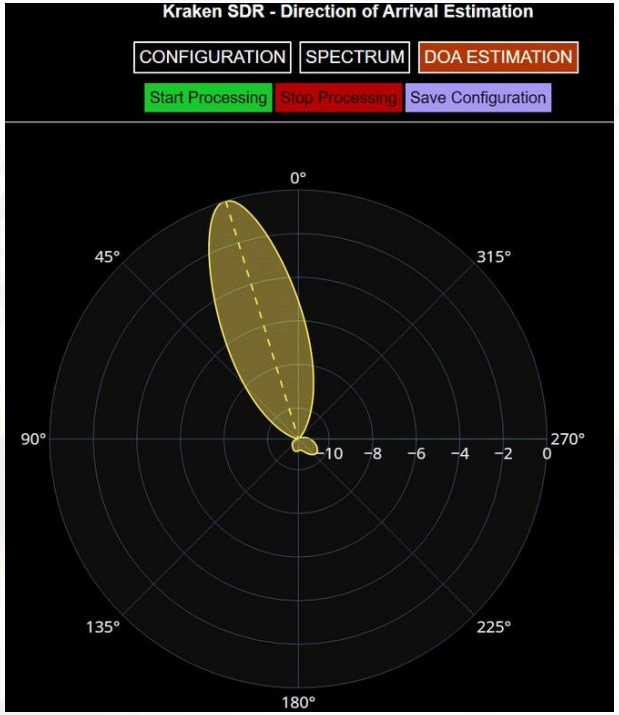


- ADS-B Flight Telemetry - 1090MHz
  - FlightAware
    - https://flightaware.com/ - https://go.flightaware.com/skyawareanywhere
  - Dump 1090
    - https://sonicgoose.com/using-dump1090-in-windows/
- Finding Local Signals to Listen to
  - https://www.radioreference.com/
- Police Fire and EMS * Many Law Enforcement are Now Using P25 Encryption*
  - uniTrunker
    - https://www.blackhillsinfosec.com/using-sdr-to-build-a-trunk-tracker-police-fire-and-ems-scanner/
    - http://www.unitrunker.com/download/
  - SDRTrunk
    - https://www.youtube.com/watch?v=UBrfqLc0E2U
    - https://github.com/DSheirer/sdrtrunk/releases

SDR Application in Radio Direction Finding and Radar

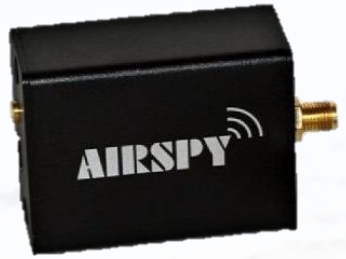
- Kraken SDR - https://www.crowdsupply.com/krakenrf/krakensdr
  - 5 SDR Receivers Same Clock Source
    - All In-Phase and Quadrature are time locked
    - Allows for the detection of which antenna/receiver see the signal first and which antenna/receiver see it last.
    - Allows software to make a two point calculation from a single signal





Alternate SDR Hardware

- Hack RF - https://bit.ly/3uBORe5
  - Half-duplex Transmit (low power) / Receive
  - RF coverage from 1 MHz to 6 GHz
  - 8-bit ADC
  - Wide Support (software and community)
- AirSpy R2 - https://airspy.com/airspy-r2/
  - Receive Only
  - RF coverage from 24 MHz to 1.7 GHz
  - Up to 20 MHz of instantaneous bandwidth
  - Flexible rate, 12-bit ADC and DAC
- ADALM-Pluto - https://bit.ly/3c2oW8R
  - Duplex Transmit/Receive
  - RF coverage from 325 MHz to 3.8 GHz
  - Up to 20 MHz of instantaneous bandwidth
  - Flexible rate, 12-bit ADC and DAC



More SDR Hardware

- Hack RF PortaPack H2 – eBay search
  - 3.2” Screen
  - 0.5ppm GPS Disciplined TXCO
  - Li-Po Battery
  - Flashable Firmware – Havoc MAYHEM
- Malachite SDR Receiver - https://bit.ly/3c1bQZo
  - 3.5 inch capacitive touch screen
  - Receive Only
  - RF coverage from 50 KHz to 2 GHz
  - 3000mAh Li-Po Battery
- Flex Radio - https://bit.ly/3nOCtnd
  - Multiple Models
  - 100W Transceive Half-Duplex
  - Ham HF Band Coverage 30 kHz-54 MHz
  - Up to 20 MHz of instantaneous bandwidth
  - Direct Sampling SDR 122.88 Msps – 16 bit

Links and Notes

- RTL-SDR V3 Specific Notes
  - https://www.rtl-sdr.com/rtl-sdr-blog-v-3-dongles-user-guide/
  - Direct Sampling HF Mode
    - This feature allows you to listen to HF signals between about 500 kHz to 28.8 MHz.
  - Bias Tee
    - https://www.youtube.com/watch?v=xK7c_dyD4NA
    - https://github.com/rtlsdrblog/rtl-sdr/releases/tag/v1.1

Thank You!

Questions?