Software-Defined Radio 101

Capturing Your First RF CTF Flag

Bryan Kobe, @kobeski1906, github.com/bkobe
https://github.com/bkobe/Presentations/

Outline

Background

Introduction to SDR: What is it?

Hardware

Software

Tactics, Techniques, and Procedures

Background - A bit about myself

EE degree in analog/digital electronic design, microcontrollers/microprocessors, and wireless/optical electronics.

Hobbies in ham radio: Radio, repeaters, tower (antenna) systems, and associated test equipment (2011)

Started in SDR back in DC24 (2016) with an RTL-SDR and a HackRF One

Continue work in SDR, namely radio mesh networks now.

Member of the WhatTheFreq! and Hard Hat Brigade (@hardhatbrigade) - come check us out there too!

What is SDR?

“Radio communication system where components that conventionally have been implemented in analog hardware (mixers, filters, amplifiers, modulators/demodulators, detectors, etc.) are instead implemented by means of software on a computer or embedded system.” (Wikipedia)

Concept on the “quickest” way to get the analog signal from antenna sampled digitally and into a computing system for analysis, and possible re-transmission
(Computers >> DSPs >> FPGAs)

Basics of Analog to Digital Conversion, just much faster (ksps to Msps), and some front-end hardware to connect the antenna to ADC.

SDR with HackRF Training Series (with Mike Ossmann from Great Scott Gadgets)
https://youtube.com/playlist?list=PLu0BPYzTjiHru1KmPThmbY-8rRm3EWvUQ

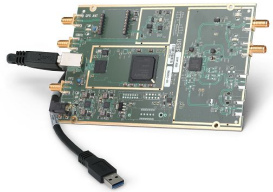
Hardware: A History

Air Force SpeakEasy Program (1990-1995)

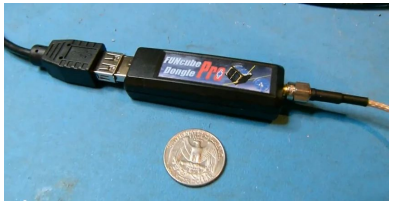
Army Joint Tactical Radio System (JTRS) (2000)

Dawn of RTL-SDR by Eric Fry and Group on DVB-T USB TV Tuner cards (2010)

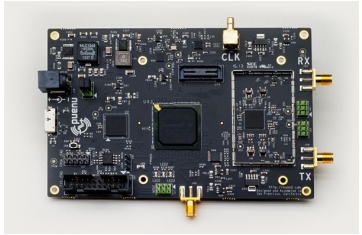
Ettus Research (2010)



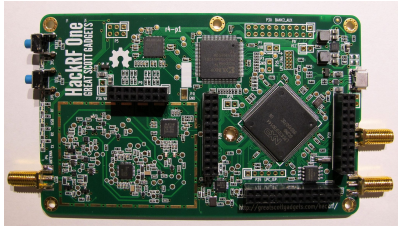
AMSAT-UK Funcube-1 USB sound card dongle (2013)



Nuand BladeRF (2013)



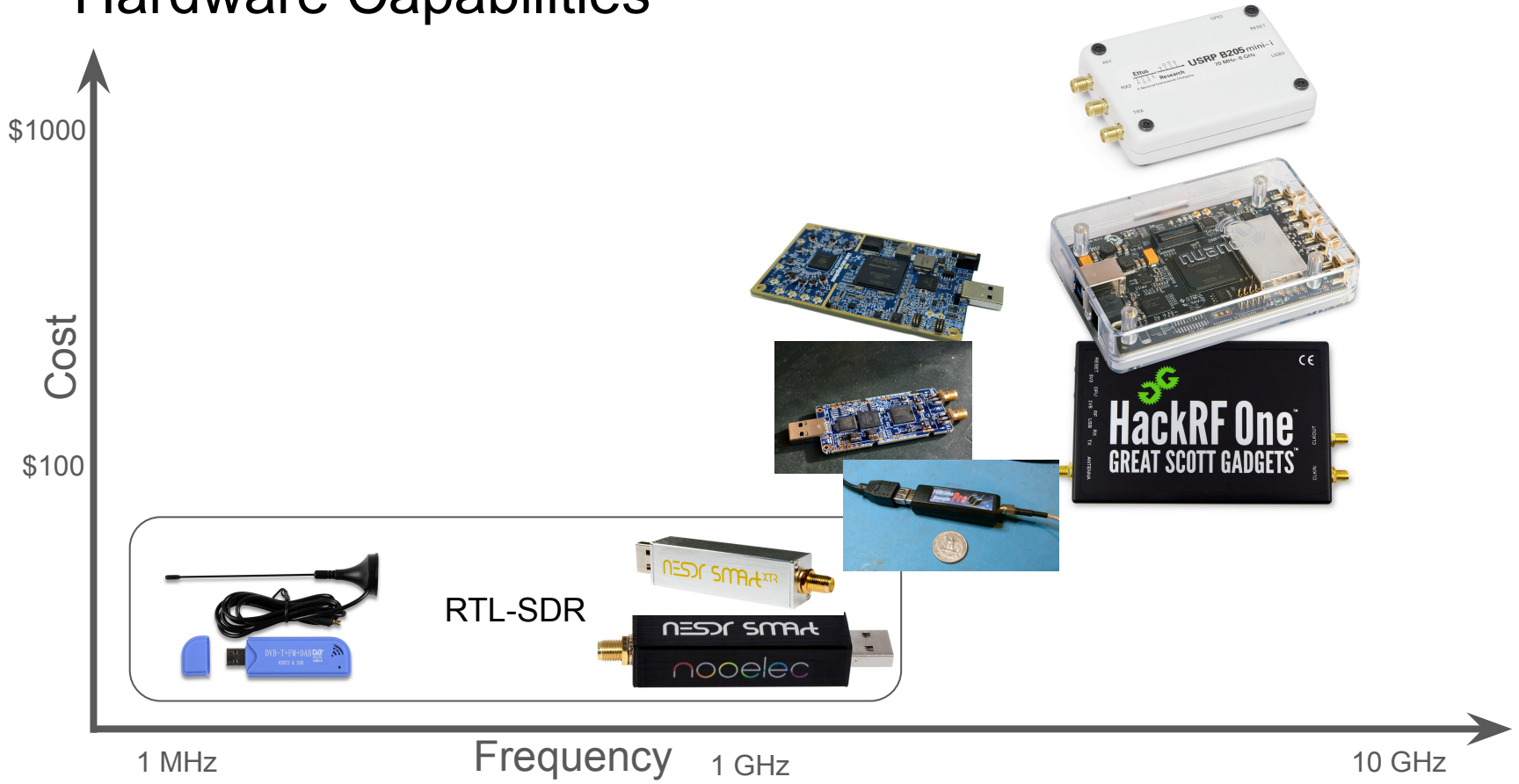
Jawbreaker and HackRF One (2014)



LimeSDR (2013-2014)

2015+

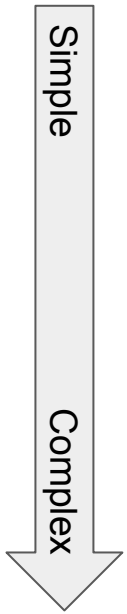
Hardware Capabilities



Hardware Capabilities

SDR	Price	Frequency Range	Max. Sample Rate	Transmit?
RTL-SDR	<$40	<1 MHz to ~1.8 GHz	<2-3 Msps	No - RX only
AMSAT FCD Pro+	<$200	100kHz to 1.9GHz	192 ksps	No - RX only
LimeSDR/Mini	$100-$400	100 kHz to 3.8 GHz	<61.44 Msps	Yes
GSG HackRF One	~$300	1 MHz to 6 GHz*	<20 Msps	Yes
Nuand BladeRF 2.0 (micro xA4)	~$500	47 MHz to 6 GHz	<61.44 Msps	Yes
USRP b200 Series	>$1000	70 MHz to 6 GHz	<56 Msps	Yes

Software



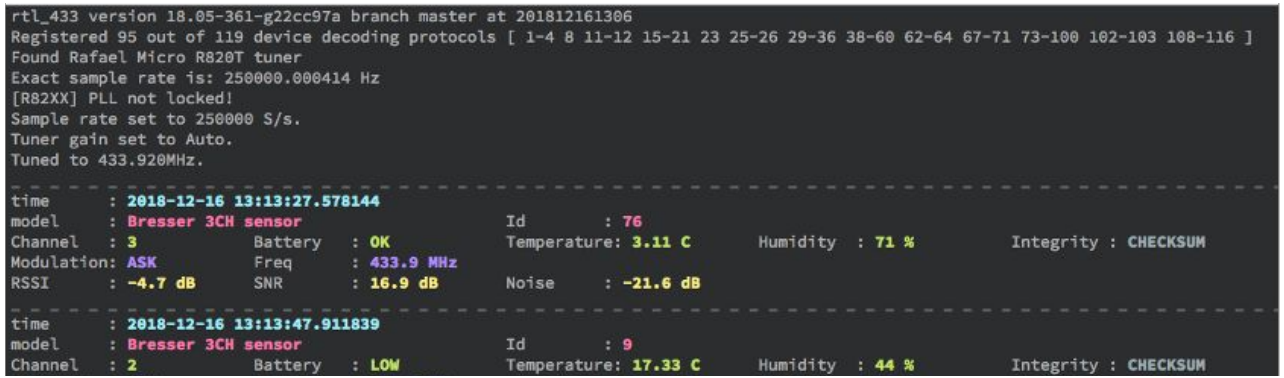
- rtl-* (rtl-power, rtl-fm**, rtl_433**) - Basic CLI tools, but also some gems
- **GQRX** (gqrx-sdr), SDR++, SDR# (SDR sharp)
- **FLDigi** - Decoding/demodulation of many ham digital modes
- **Inspectrum** - time-based analysis of signals
- Universal Radio Hacker (**URH**)
- SDR Angel
- **GNU Radio** Companion

rtl_433

https://github.com/merbanan/rtl_433

Command line tool that uses the rtl-sdr hardware to decode and print data out to a terminal session window

Can decode a wide variety of sub-GHz devices (like weather stations, wireless doorbell, and other things in several bands)



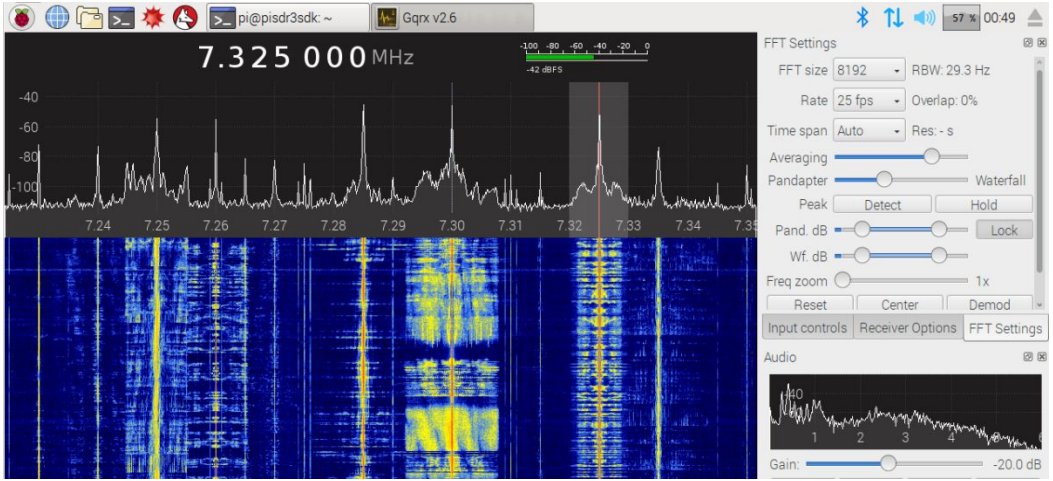
TPMS-https://r-c-y.net/posts/tpms/ >> “rtl_433 -M level -f 315000000”)

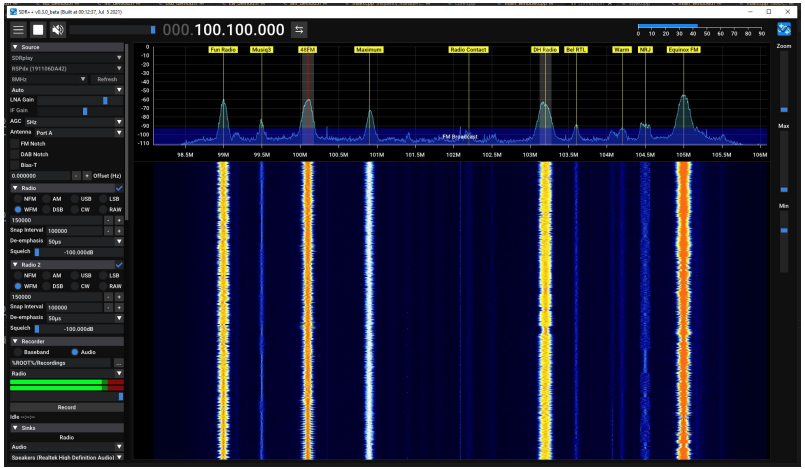
SDR++, SDR#, and gqrx-sdr

Frequency spectrum and waterfall-based GUI to view what the SDR is receiving

Good starting point to tune around and listen for the signals (CTF flags)

Has some settings (like gain, FFT window setting, and window type, but can also be left to default settings)

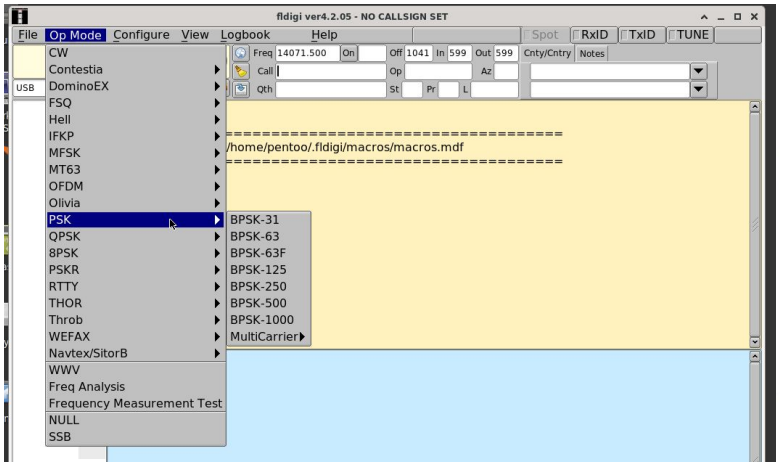


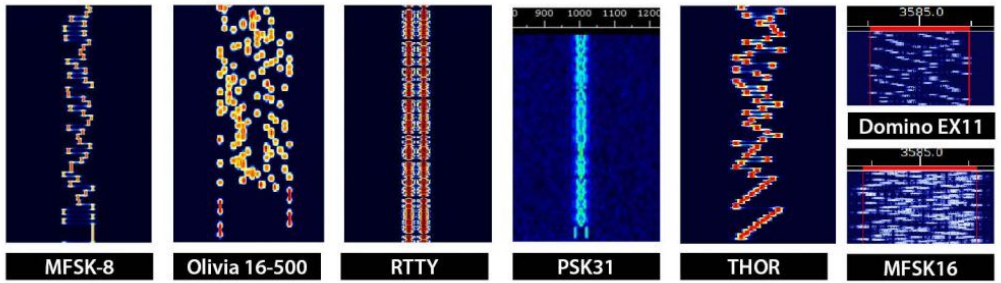


Fast Light DIGItal (fldigi)

A soundcard/audio-based modem software to keyboard to keyboard digital messages in the ham radio community

Used for some of the virtual challenges, and some in-the-room ones. Can use simple audio coupling to mic in and demodulate





https://sarc.org.au/fl-digi/

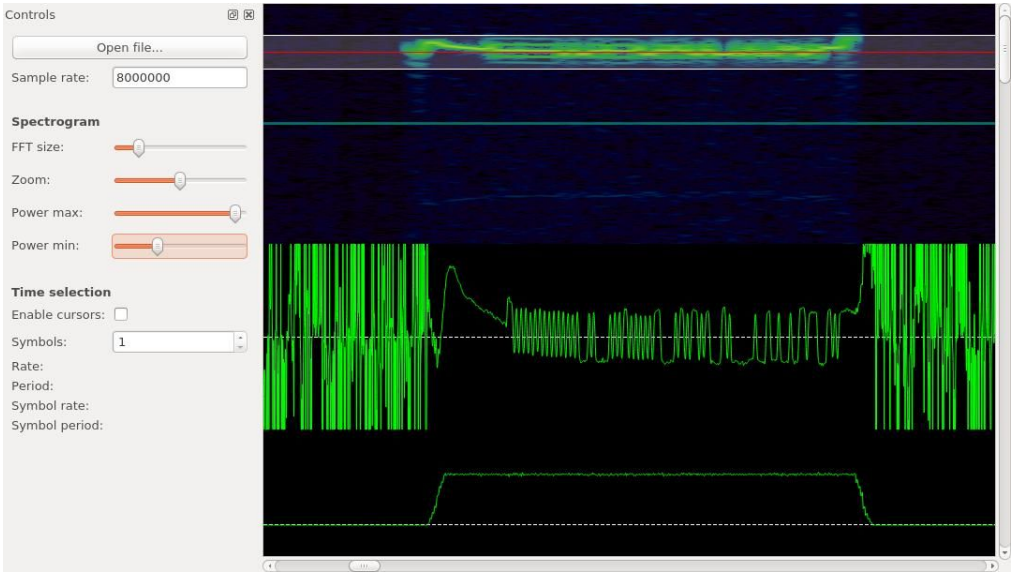
inspectrum

Good for time-domain analysis of signals (like binary shift keying or on-off keying)

Capture can be pre-recorded and loaded. Nice for decoding at your leisure vs real-time on the waterfall.

Takes raw IQ files (like from gqrx) with Several types, and allows for viewing relationship (amplitude, phase, freq, etc.)

*.sigmf-meta, *.sigmf-data - SigMF recordings
*.cf32, *.fc32, *.cfile - Complex 32-bit floating point samples (GNU Radio, osmocom_fft)
*.cf64, *.fc64 - Complex 64-bit floating point samples
*.cs32, *.sc32, *.c32 - Complex 32-bit signed integer samples (SDRAngel)
*.cs16, *.sc16, *.c16 - Complex 16-bit signed integer samples (BladeRF)
*.cs8, *.sc8, *.c8 - Complex 8-bit signed integer samples (HackRF)
*.cu8, *.uc8 - Complex 8-bit unsigned integer samples (RTL-SDR)
*.f32 - Real 32-bit floating point samples
*.f64 - Real 64-bit floating point samples (MATLAB)
*.s16 - Real 16-bit signed integer samples
*.s8 - Real 8-bit signed integer samples
*.u8 - Real 8-bit unsigned integer samples



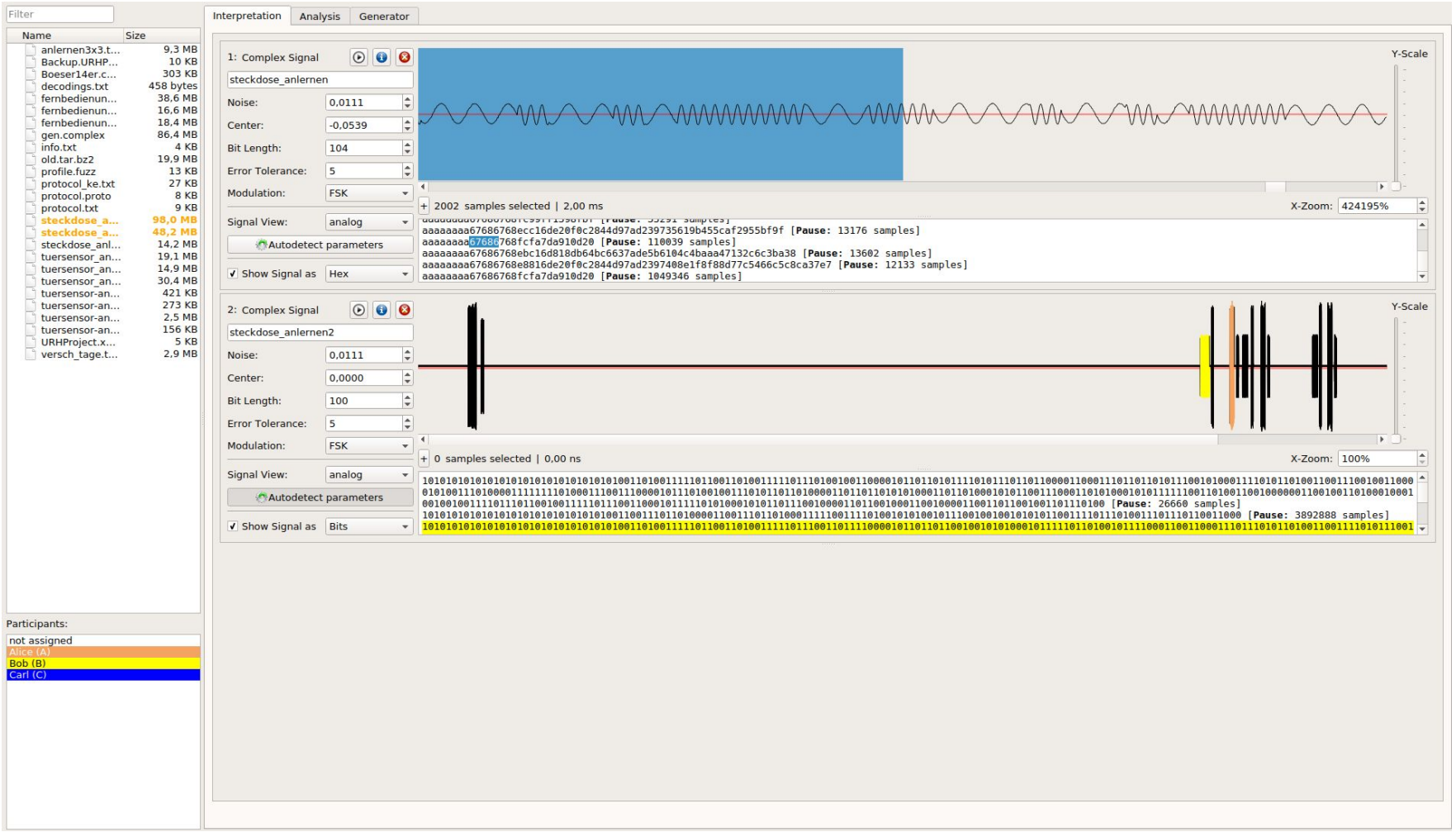
Universal Radio Hacker (URH)

Most/all SDRs noted in the hardware section are supported for input capture and (if SDR has transmit) sending transmissions.

Does allow for scanning the spectrum, but main functionality is analysis of captured signals. Has tools for replay, editing, and dissecting modulated packets to ones and zeros.

Closest to a “wireshark-like” interface where information can be visualized, manipulated, and sent back. RX >> demod >> analysis >> mod >> TX

https://github.com/jopohl/urh

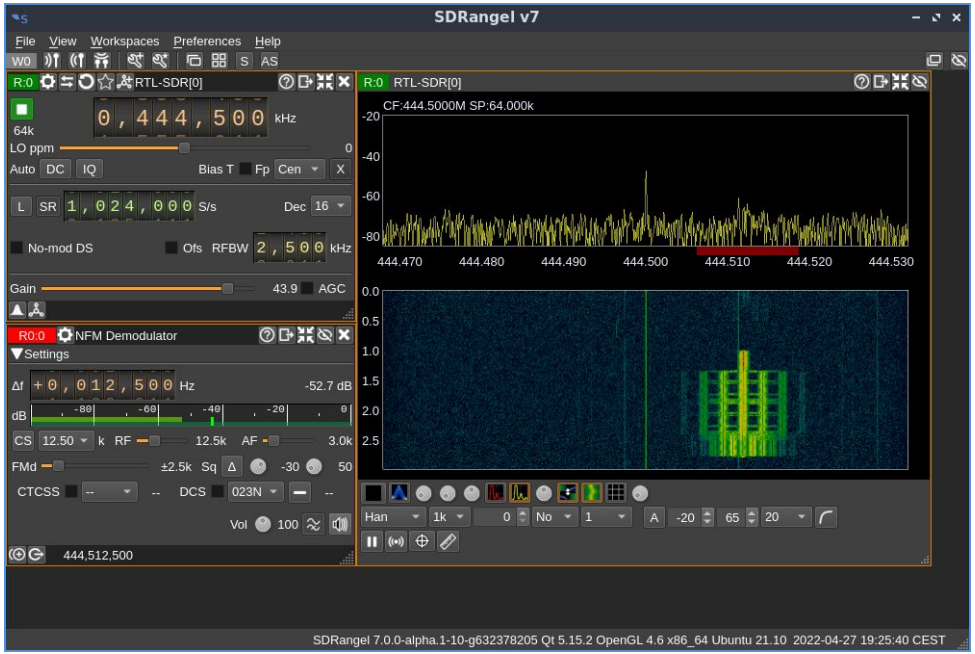

Filter
Name
Size
anlernen3x3.t... 9,3 MB
Backup.URHP... 10 KB
Boeser14er.c... 303 KB
decodings.txt 458 bytes
fernbedienun... 38,6 MB
fernbedienun... 16,6 MB
fernbedienun... 18,4 MB
gen.complex 86,4 MB
info.txt 4 KB
old.tar.bz2 19,9 MB
profile.fuzz 13 KB
protocol_ke.txt 27 KB
protocol.proto 8 KB
protocol.txt 9 KB
steckdose_a... 98,0 MB
steckdose_a... 48,2 MB
steckdose_anl... 14,2 MB
tuersensor_an... 19,1 MB
tuersensor_an... 14,9 MB
tuersensor_an... 30,4 MB
tuersensor-an... 421 KB
tuersensor-an... 273 KB
tuersensor-an... 2,5 MB
tuersensor-an... 156 KB
URHProject.x... 5 KB
versch_tage.t... 2,9 MB
Participants:
not assigned
Alice (A)
Bob (B)
Carl (C)
Interpretation
Analysis
Generator
1: Complex Signal
steckdose_anlernen
Noise: 0,0111
Center: -0,0539
Bit Length: 104
Error Tolerance: 5
Modulation: FSK
Signal View: analog
Autodetect parameters
Show Signal as Hex
Y-Scale
2002 samples selected | 2,00 ms
X-Zoom: 424195%
aaaaaaaa67686768ecc16de20f0c2844d97ad239735619b455caf2955bf9f [Pause: 13176 samples]
aaaaaaaa67686768fcfa7da910d20 [Pause: 110039 samples]
aaaaaaaa67686768ebc16d818db64bc6637ade5b6104c4baaa47132c6c3ba38 [Pause: 13602 samples]
aaaaaaaa67686768e8816de20f0c2844d97ad2397408e1f8f88d77c5466c5c8ca37e7 [Pause: 12133 samples]
aaaaaaaa67686768fcfa7da910d20 [Pause: 1049346 samples]
2: Complex Signal
steckdose_anlernen2
Noise: 0,0111
Center: 0,0000
Bit Length: 100
Error Tolerance: 5
Modulation: FSK
Signal View: analog
Autodetect parameters
Show Signal as Bits
Y-Scale
0 samples selected | 0,00 ns
X-Zoom: 100%
[Pause: 26660 samples]
[Pause: 3892888 samples]

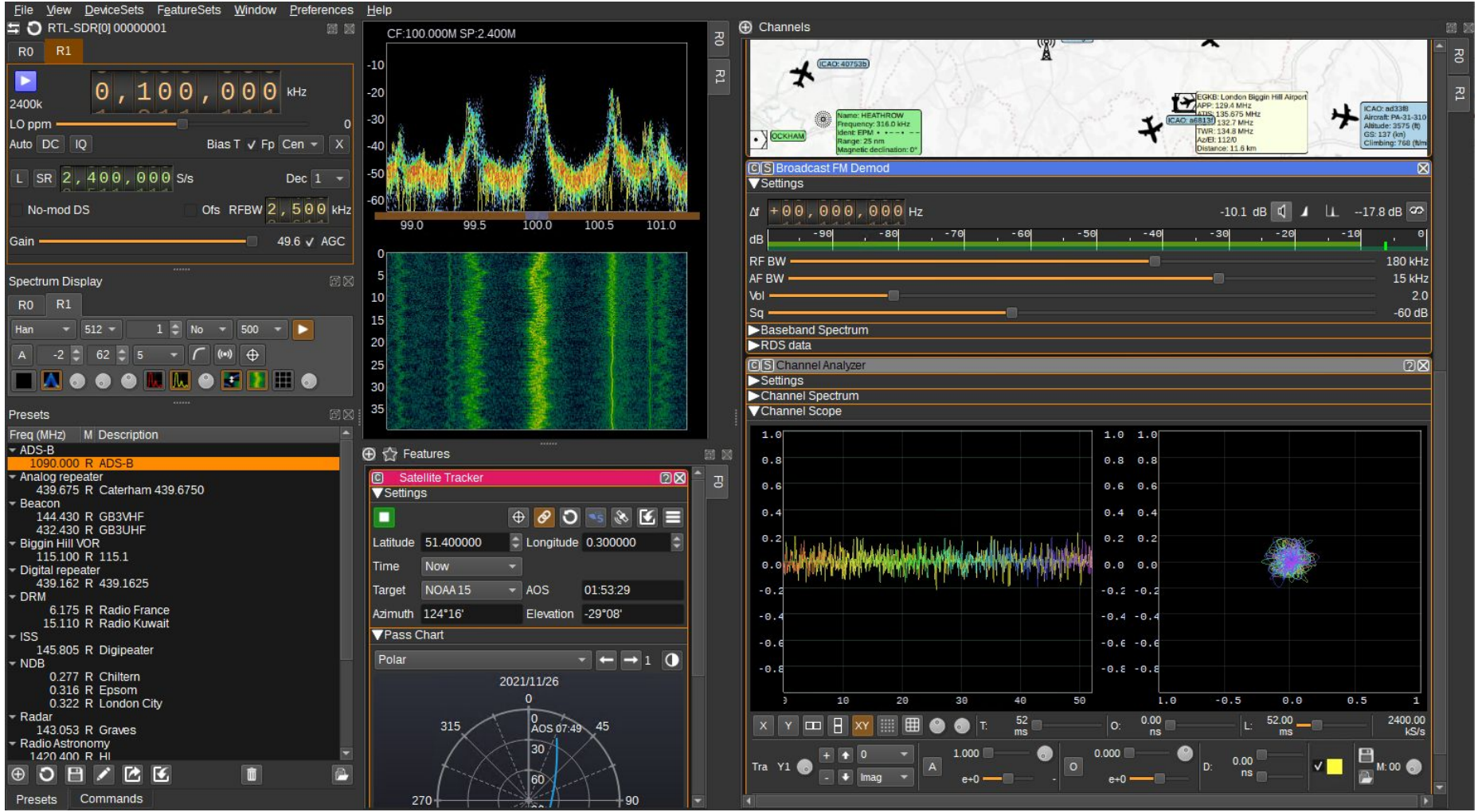
SDR Angel

Getting into a “sandbox” type of environment where you have a workspace with customizable functions and features. Needs to be constructed for an application.

Has a LOT of features that can mod/demod, decode and visualize, but also a lot of RTFM

Overall, a powerful program that has capability to tackle most of the use-cases here.



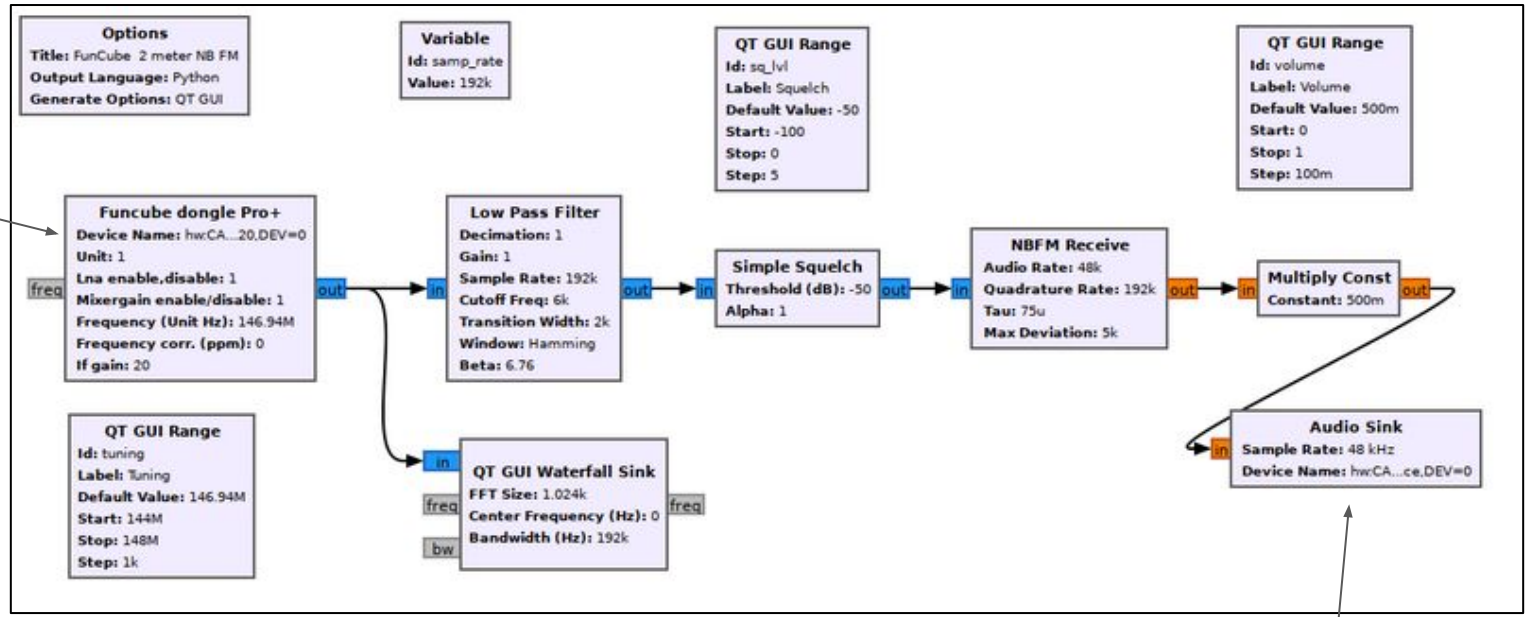

File View DeviceSets FeatureSets Window Preferences Help
RTL-SDR[0] 00000001
R0 R1
2400k
0,100,000 kHz
LO ppm 0
Auto DC IQ Bias T Fp Cen X
L SR 2,400,000 S/s Dec 1
No-mod DS Ofs RFBW 2,500 kHz
Gain 49.6 AGC
Spectrum Display
R0 R1
Han 512 1 No 500
A -2 62 5
Presets
Freq (MHz) M Description
ADS-B
1090.000 R ADS-B
Analog repeater
439.675 R Caterham 439.6750
Beacon
144.430 R GB3VHF
432.430 R GB3UHF
Biggin Hill VOR
115.100 R 115.1
Digital repeater
439.162 R 439.1625
DRM
6.175 R Radio France
15.110 R Radio Kuwait
ISS
145.805 R Digipeater
NDB
0.277 R Chiltern
0.316 R Epsom
0.322 R London City
Radar
143.053 R Graves
Radio Astronomy
1420.400 R HI
Presets Commands
CF:100.000M SP:2.400M
-10 -20 -30 -40 -50 -60
99.0 99.5 100.0 100.5 101.0
0 5 10 15 20 25 30 35
R0 R1
Features
F0
Satellite Tracker
Settings
Latitude 51.400000 Longitude 0.300000
Time Now
Target NOAA 15 AOS 01:53:29
Azimuth 124°16' Elevation -29°08'
Pass Chart
Polar 1
2021/11/26
0 45 90 270 315
AOS 07:49
30 60
Channels
R0 R1
ICAO:407535
EGKB: London Biggin Hill Airport
APP: 129.4 MHz
AIR: 135.675 MHz
TWR: 132.7 MHz
TWR: 134.8 MHz
Name: HEATHROW
Frequency: 316.0 kHz
Ident: EPM
Range: 25 nm
Magnetic declination: 0°
AzEl: 112/0
Distance: 11.6 km
OCKHAM
ICAO: ad33f8
Aircraft: PA-31-310
Altitude: 3575 (ft)
GS: 137 (kn)
Climbing: 768 (ft/m
Broadcast FM Demod
Settings
Δf +00,000,000 Hz
-10.1 dB --17.8 dB
dB -90 -80 -70 -60 -50 -40 -30 -20 -10 0
RF BW 180 kHz
AF BW 15 kHz
Vol 2.0
Sq -60 dB
Baseband Spectrum
RDS data
Channel Analyzer
Settings
Channel Spectrum
Channel Scope
1.0 0.8 0.6 0.4 0.2 0.0 -0.2 -0.4 -0.6 -0.8
10 20 30 40 50
1.0 -0.5 0.0 0.5 1
X Y XY T: 52 ms O: 0.00 ns L: 52.00 ms 2400.00 kS/s
Tra Y1 0 Imag A 1.000 e+0 0.000 e+0 O D: 0.00 ns M: 00

GNU Radio Companion

Most complex (for this talk), but also the most configurable in terms of building custom SDR software to read from and/or send to the radio hardware

Uses concept of flowgraphs (with python under the hood) to process information flow from a receiver source block (the SDR) to any number of blocks. Demodulators, resamplers, filters, graphic “instrumentation”, and also plenty of GUI objects for making your own dashboards for custom functions.

You “wire” inputs to outputs, with each I/O color coded on its data type (complex numbers, real floats, bitstreams, etc)


Options
Title: FunCube 2 meter NB FM
Output Language: Python
Generate Options: QT GUI
Variable
Id: samp_rate
Value: 192k
QT GUI Range
Id: sq_lvl
Label: Squelch
Default Value: -50
Start: -100
Stop: 0
Step: 5
QT GUI Range
Id: volume
Label: Volume
Default Value: 500m
Start: 0
Stop: 1
Step: 100m
Input
Funcube dongle Pro+
Device Name: hw:CA...20,DEV=0
Unit: 1
Lna enable,disable: 1
Mixergain enable/disable: 1
Frequency (Unit Hz): 146.94M
Frequency corr. (ppm): 0
If gain: 20
freq
out
Low Pass Filter
Decimation: 1
Gain: 1
Sample Rate: 192k
Cutoff Freq: 6k
Transition Width: 2k
Window: Hamming
Beta: 6.76
Simple Squelch
Threshold (dB): -50
Alpha: 1
NBFM Receive
Audio Rate: 48k
Quadrature Rate: 192k
Tau: 75u
Max Deviation: 5k
Multiply Const
Constant: 500m
QT GUI Range
Id: tuning
Label: Tuning
Default Value: 146.94M
Start: 144M
Stop: 148M
Step: 1k
QT GUI Waterfall Sink
FFT Size: 1.024k
Center Frequency (Hz): 0
Bandwidth (Hz): 192k
freq
bw
Audio Sink
Sample Rate: 48 kHz
Device Name: hw:CA...ce,DEV=0
Output

Packaging all this into a distro?

- Kali Linux (Debian-based): Can run USB bootable in a live environment, and typically has most of the drivers and software needed for SDR.
- Pentoo Linux (Gentoo-based): Another good option to just boot into a live environment. Has all the software needed to start capturing flags.
- DragonOS (Ubuntu-based): A live image that has all the SDR software and dependencies. Can run in multiple environments (live USB, dual boot install, or virtual machine). https://cemaxecuter.com/
- Windows? Hit or miss. Need to manually load the [Zadig] drivers for SDR, then installers for the above programs. Not all the above will be available.

Tactics, Techniques, and Procedures - Knowing Where to Look

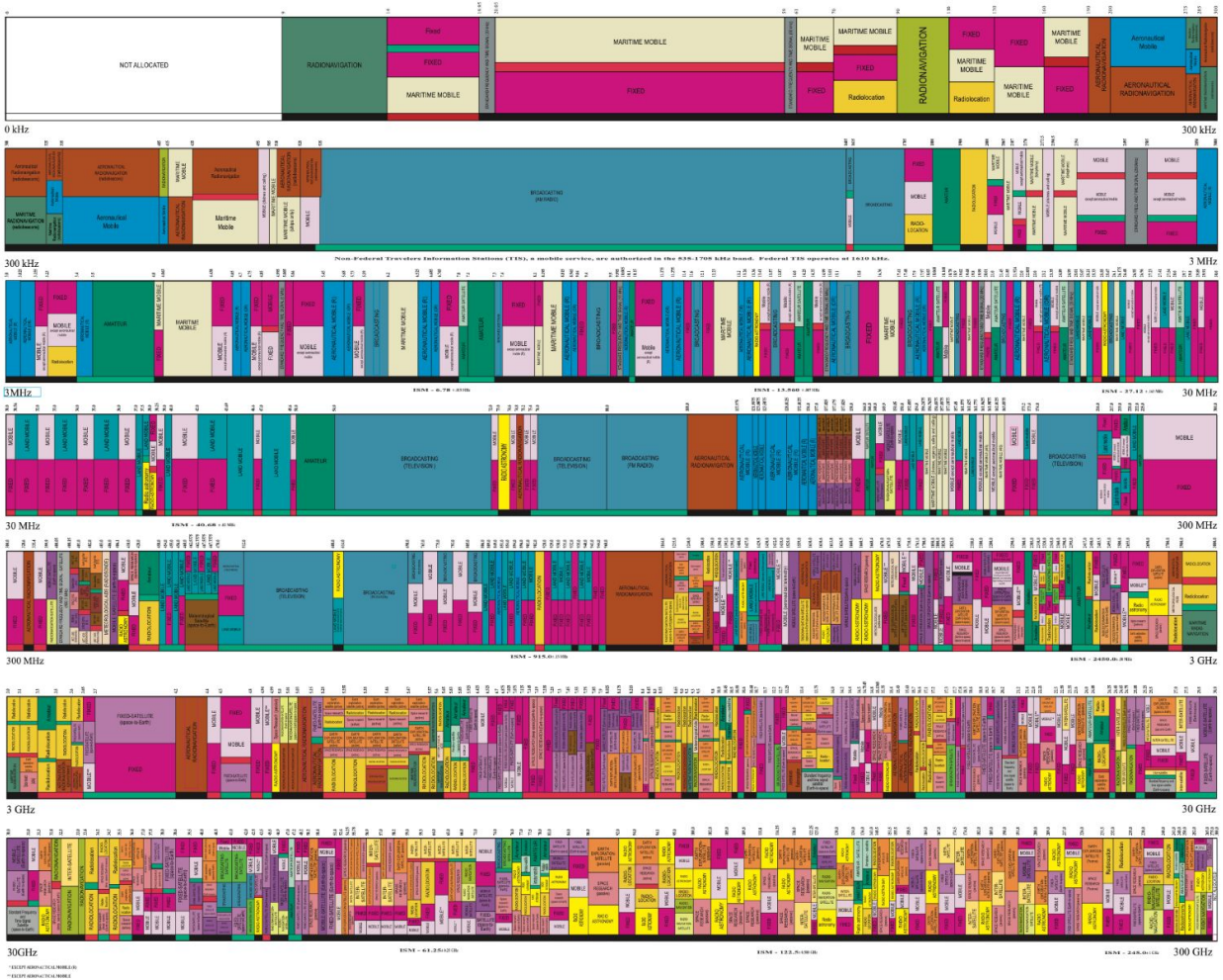
Having the entire 0 to 6 (or so) GHz is an awful lot of space. Even to break up into “chunks” and listen (at the sample rate of your SDR)... There has to be a better way.

Consider all bands you work with and use day to day.
Cellular (quad-band, LTE), GPS, WiFi, Bluetooth…

What if there was a way to target areas to look?

UNITED STATES FREQUENCY ALLOCATIONS

THE RADIO SPECTRUM



RADIO SERVICES COLOR LEGEND

- AERONAUTICAL MOBILE
- AERONAUTICAL MOBILE SATELLITE
- AERONAUTICAL RADIONAVIGATION
- AMATEUR
- AMATEUR SATELLITE
- BROADCASTING
- BROADCASTING SATELLITE
- EARTH EXPLORATION SATELLITE
- FIXED
- FIXED SATELLITE
- INTER-SATELLITE
- LAND MOBILE
- LAND MOBILE SATELLITE
- MARITIME MOBILE
- MARITIME MOBILE SATELLITE
- MARITIME RADIONAVIGATION
- METEOROLOGICAL
- METEOROLOGICAL SATELLITE
- MOBILE
- MOBILE SATELLITE
- RADIO ASTRONOMY
- RADIODETERMINATION SATELLITE
- RADIOLOCATION
- RADIOLOCATION SATELLITE
- RADIONAVIGATION
- RADIONAVIGATION SATELLITE
- SPACE OPERATION
- SPACE RESEARCH
- STANDARD FREQUENCY AND TIME SIGNAL
- STANDARD FREQUENCY AND TIME SIGNAL SATELLITE

ACTIVITY CODE

- FEDERAL EXCLUSIVE
- FEDERAL/NON-FEDERAL SHARED
- NON-FEDERAL EXCLUSIVE

ALLOCATION USAGE DESIGNATION

SERVICE	EXAMPLE	DESCRIPTION
Primary	FIXED	Capital Letters
Secondary	Mobile	1st Capital with lower case letters

This chart is a graphic single-point-in-time portrayal of the Table of Frequency Allocations used by the FCC and NTIA. As such, it may not completely reflect all aspects, i.e. footnotes and recent changes made to the Table of Frequency Allocations. Therefore, for complete information, users should consult the Table to determine the current status of U.S. allocations.

U.S. DEPARTMENT OF COMMERCE
National Telecommunications and Information Administration
Office of Spectrum Management

JANUARY 2016

https://upload.wikimedia.org/wikipedia/commons/c/c7/United_States_Frequency_Allocations_Chart_2016_-_The_Radio_Spectrum.pdf

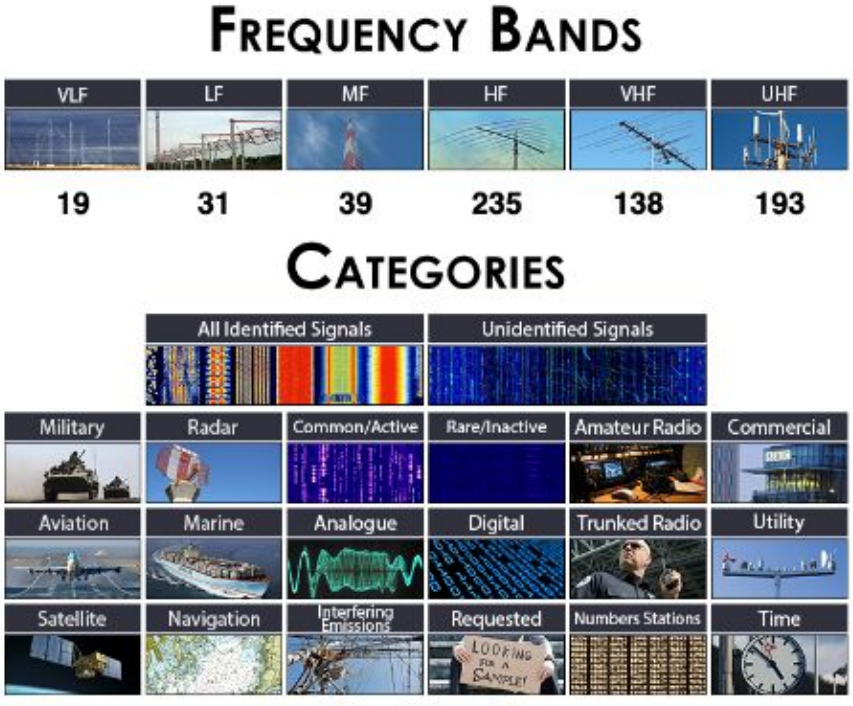
Tactics, Techniques, and Procedures

Look in the Industrial, Scientific, and Medical (ISM) and Amateur Radio bands
    420 to 450 MHz might have some interesting signals.
    900 to 930 MHz can be another good area.

Look for the waterfall “spray paint” before the start of the signal, followed by something like morse code (OOK), amplitude shift keying, or frequency shift keying (< 30 sec transmission).

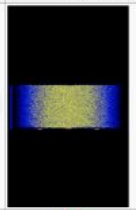
For unknown signal audio, use the signal identification wiki to listen to some different common modulation formats.
https://www.sigidwiki.com/wiki/Signal_Identification_Guide

SigID Wiki (https://www.sigidwiki.com/wiki/Signal_Identification_Guide)



Color Legend

Inactive (No longer in use)	Active (Currently in active use)	Status Unknown or Intermittent

Signal Name	Description	Frequency	Mode	Modulation	Bandwidth	Location	Sample Audio	Waterfall image
8PSK	8PSK is an amateur digital UTF8-text and data mode designed by John Phelps KL4YFD in 2014. It's goal is to provide medium speed data using generic FM and SSB radios.	3 MHz — 3,000 MHz	USB,FM	8PSK	125 Hz — 1.2 kHz	Worldwide	0:00 / 0:00	
ALE-400	ALE-400 is an amateur version of the 2G ALE standard. It is adapted to the demands of amateur radio emergency traffic handling.	1.806 MHz — 144.163 MHz	USB	MFSK	400 Hz	Worldwide	0:00 / 0:00	
AMSAT-P3D	AMSAT-P3D (Known as Phase 3D, OSCAR-40, and AO-40) is a amateur radio satellite built by AMSAT. As of 2004, the satellite's systems have failed.	145.805 MHz — 24,048.285 MHz	USB	PSK	1.6 kHz	Worldwide	0:00 / 0:00	

Where to go from here?

Sit down at a table, get the SDR plugged in and listen!

[If on the defcon secure wifi] the virtual challenges are a great way to segway into the in-room activities. GNU Radio flowgraphs are available to stream the SDR info right to your PC for decoding (hint: fldigi or qsstv might be useful for it)

Get to know people, and ask questions! We all had to start somewhere…