Intro to SDR

A High Level Overview

From a Non-Ham about Radio Frequency
&
Observing The RF Environment Around You.

Who Am I

- Dustin / KE2EFX / BusySignal
- 20+ Years in IT and Information Security
  - BS in Electrical Engineering
- Former Professional Photographer
- Wicked Curious in all things Radio Frequency
  - 2022 / DEFCON 30
    World Wide WarDrive (WiFi collection)
  - Builder of WiFi and BTLE scanning and Monitoring equipment
  - Trunk Radio / Trunk Recorder Enthusiast
    (Public RF Comms for example Police Scanners)

SDR - Introduction Details

- General Definition:
  - Hardware Radio System where traditional components such as Mixers, Filters, Amplifiers, Modulators/Demodulators, detectors, ect are implemented via software on a Computer.

  - Offloading CPU/compute from the device to the computer CPU to reduce hardware costs.

SDR - Introduction Details

- Can provide greater flexibility and reconfiguration of frequency, modulation ect.
- Simple software controls from an application controlling the device.
- Core Components
  - Main PC / Computer with an SDR device with antenna connections

SDR - Flexible Scanner Functions

- Spectrum Analysis
  - An SDR can be used to visualize the Frequency Spectrum in real time - Waterfall - etc.
  - Showing signals in transmit

- Some of these examples are ones we already know and love
  - AM/FM
  - Airband : Aircraft and Airports
  - NOAA Weather Stations / Weather Updates / Emergency Broadcasts
  - Amateur Radio Signals / All of the Ham Operators

SDR - Flexible Functions

- Other Examples
  - Non-Encrypted Trunk Radio simulcasts
  - Suffolk County NY
    - https://www.radioreference.com/db/browse/ctid/1876

- Decode Over The Air packets
  - POCSAG
    - Pagers (decode with PDW, Multimon-NG)
    - I am not a lawyer - do not do this on systems you do not own
  - APRS
    - CubicSDR, GQRX

SDR - Hardware Solutions / Receive Only

- Inexpensive / Getting Started
  - RTL-SDR V3 / $30 ($40 for kit)
    - 24Mhz through 1766Mhz
    - USB, common support in apps
    - Receive only
    - 2.5Mhz Bandwidth (stable) / 8 bit resolution
  - Nooelec
    - 100khz - 1755Mhz ($45 for kit)
    - USB, common support in apps
    - Receive Only / 10Mhz bandwidth / 12 bit resolution

SDR - Hardware solutions / Receive Only

- Intermediate / Getting Started
  - AirSpy / $200
    - 24Mhz through 1800Mhz
    - USB, common support in apps
    - Receive Only / 10Mhz Spectrum Visibility
    - 12 bit resolution
  - SDRplay RSPdx-R2 / $235
    - 1Khz - 2Ghz
    - USB, supported in apps
    - Receive Only / 10Mhz Spectrum Visibility.
    - 14 bit resolution

SDR - Hardware solutions / Rx & Tx

- Example of equipment for Send/Receive
  - HackRF - $350
    - 30Mhz - 6000Mhz
    - 20Mhz Bandwidth / 8 bit

- Transmit - License required - Ham Operators included
  - More reasons for more people to get their licenses.

SDR - Software Solutions

- Windows
  - SDR++ - https://www.sdrpp.org/
- Linux
  - SDR++ : https://www.sdrpp.org/
  - Gqrx - https://www.gqrx.dk/
- Products can show full “water fall” of spectrum
- Tuning, Squelch, gain, recording all controls available

SDR - Software Solutions

- P25 / Trunking System Auto Scanning
  - Trunk Recorder - Linux
  - Listens to P25 trunking channels
    - Tunes radios to specific broadcast/freqs of broadcasts
  - Capable of recording and software scanner in browser ->

SDR - Flexible Scanner Functions

Suffolk County NY

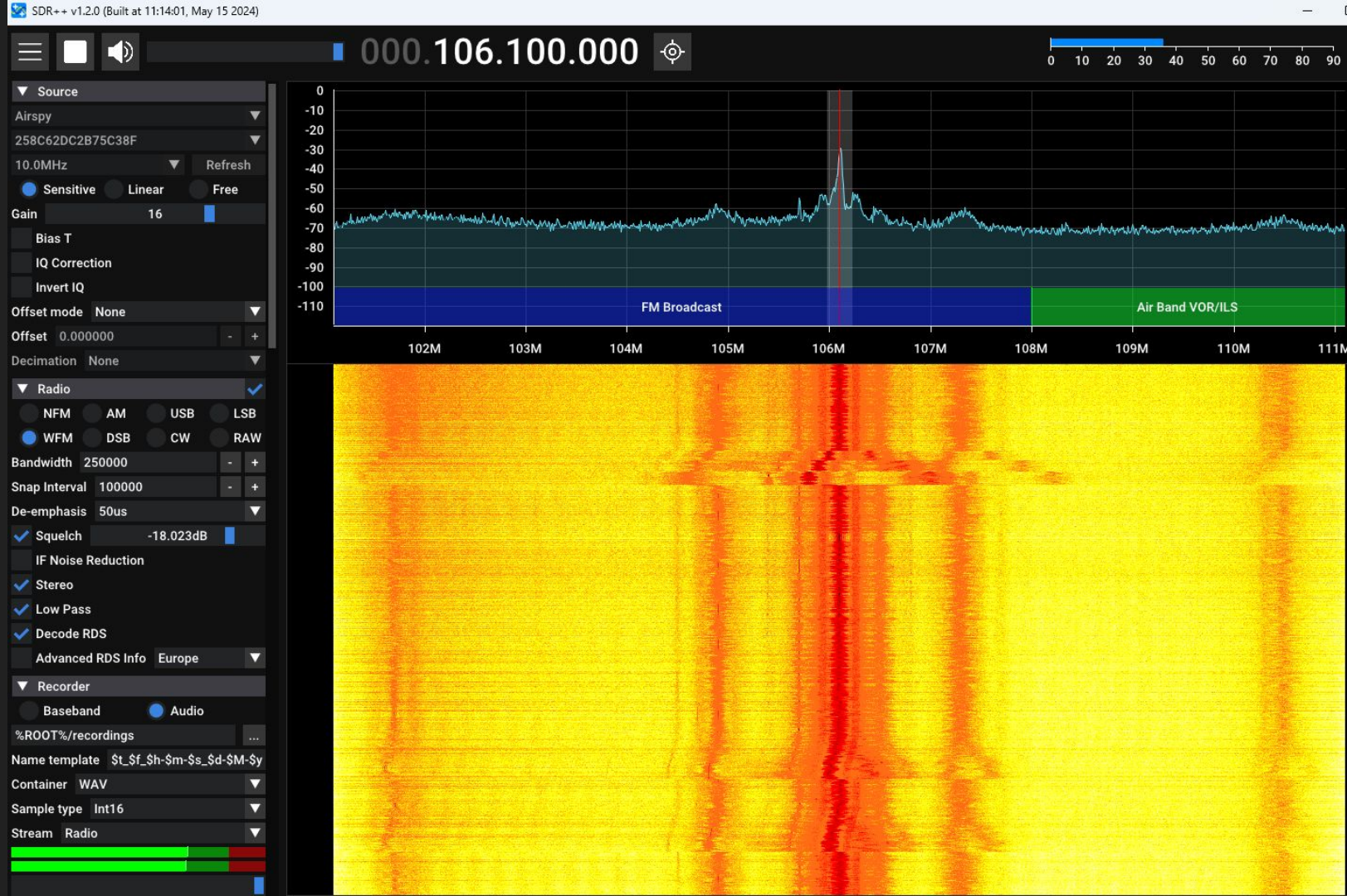
https://www.radioreference.com/db/browse/ctid/1876

Sites and Frequencies

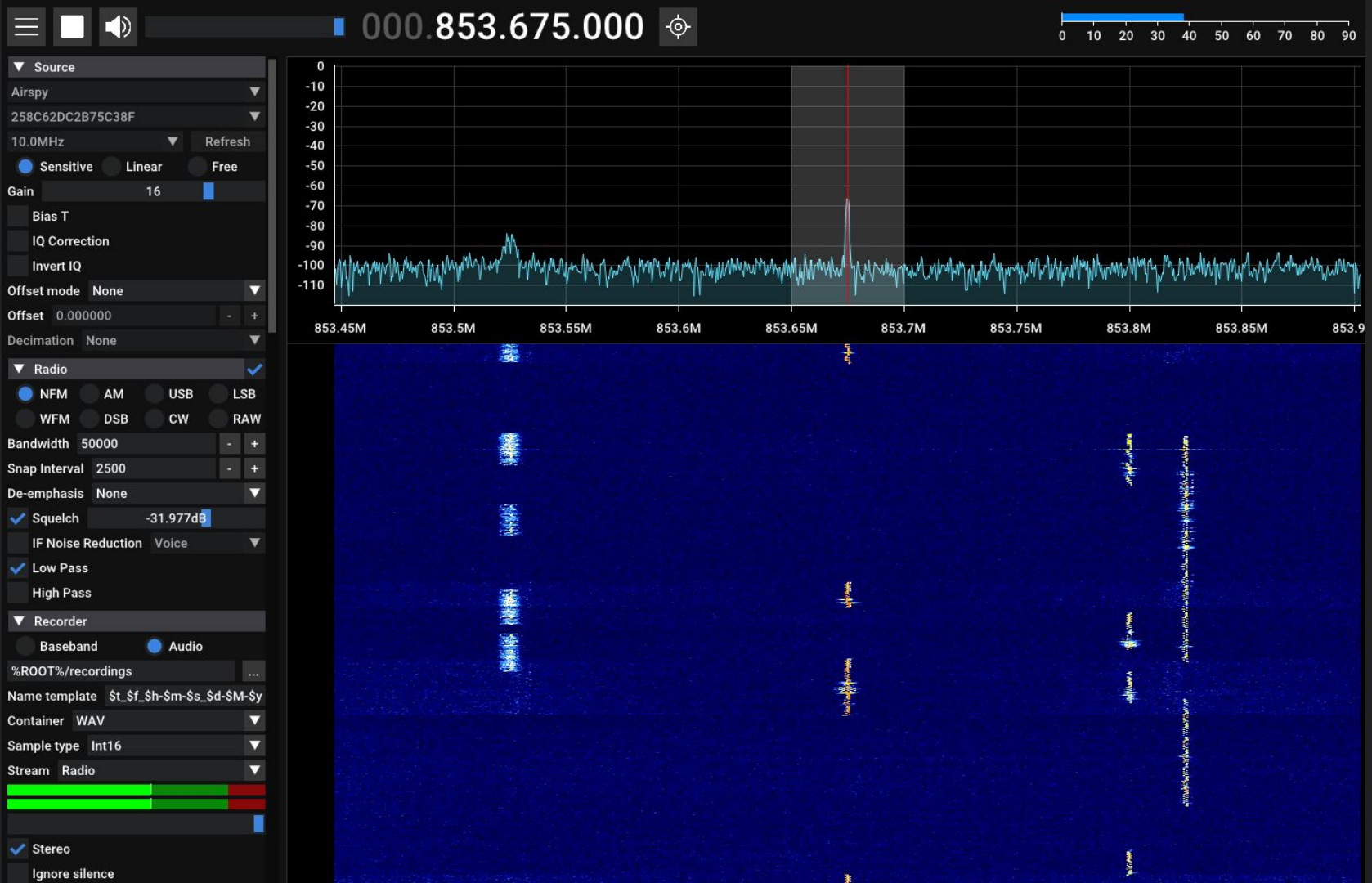
Red (c) are control channel capable frequencies

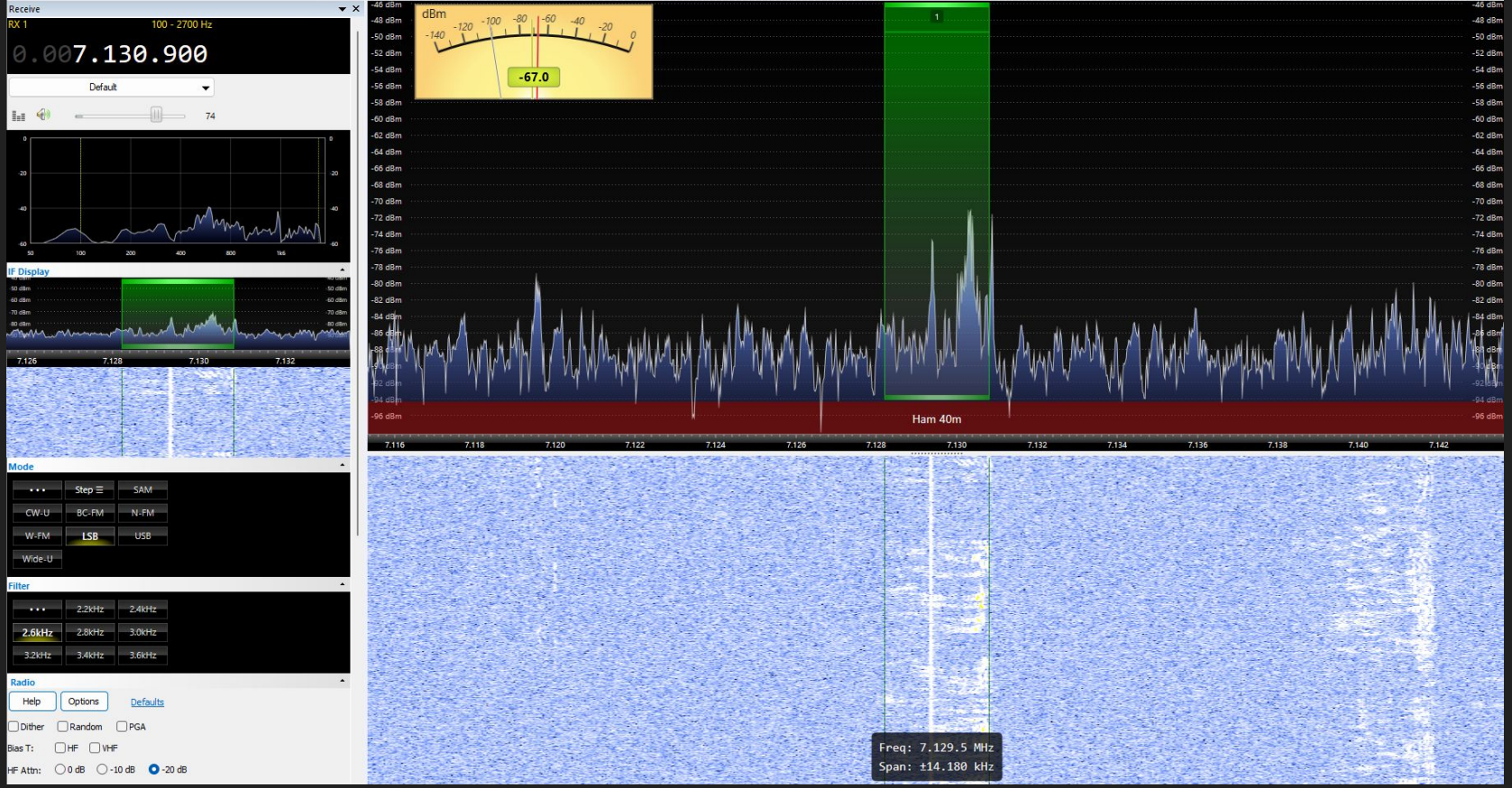
RFSS	Site	Name	Freqs							
1 (1)	003 (3)	700 West Simulcast	770.30625	770.50625	771.08125	771.58125	771.95625	772.28125c	772.91875c	773.65625c
			774.15625c							
1 (1)	004 (4)	800 Simulcast	851.0875	851.1625c	851.2375	852.425c	852.675c	852.7375c	852.850	852.925
			853.125	853.225	853.250	853.375	853.525			
1 (1)	005 (5)	Huntington	851.4625c	852.3125c	852.475c	852.950c				
1 (1)	006 (6)	1st Precinct (N. Lindenhurst)	851.475c	851.975c	852.225c	852.7125	853.300c	853.450		
1 (1)	007 (7)	Port Jefferson	851.125c	851.800	852.3625c	852.800c				
1 (1)	008 (8)	Montauk	851.3875c	851.600c	852.600c	853.300c				
1 (1)	009 (9)	700 East Simulcast	772.29375c	772.90625c	773.66875c	774.16875c				

SDR++


SDR++ v1.2.0 (Built at 11:14:01, May 15 2024)
000.106.100.000
0 10 20 30 40 50 60 70 80 90
Source
Airspy
258C62DC2B75C38F
10.0MHz
Refresh
Sensitive
Linear
Free
Gain 16
Bias T
IQ Correction
Invert IQ
Offset mode None
Offset 0.000000
Decimation None
Radio
NFM
AM
USB
LSB
WFM
DSB
CW
RAW
Bandwidth 250000
Snap Interval 100000
De-emphasis 50us
Squelch -18.023dB
IF Noise Reduction
Stereo
Low Pass
Decode RDS
Advanced RDS Info Europe
Recorder
Baseband
Audio
%ROOT%/recordings
Name template $t_$f_$h-$m-$s_$d-$M-$y
Container WAV
Sample type Int16
Stream Radio
0 -10 -20 -30 -40 -50 -60 -70 -80 -90 -100 -110
FM Broadcast
Air Band VOR/ILS
102M 103M 104M 105M 106M 107M 108M 109M 110M 111M

SDR++


000.853.675.000
0 10 20 30 40 50 60 70 80 90
Source
Airspy
258C62DC2B75C38F
10.0MHz
Refresh
Sensitive
Linear
Free
Gain 16
Bias T
IQ Correction
Invert IQ
Offset mode None
Offset 0.000000
Decimation None
Radio
NFM
AM
USB
LSB
WFM
DSB
CW
RAW
Bandwidth 50000
Snap Interval 2500
De-emphasis None
Squelch -31.977dB
IF Noise Reduction Voice
Low Pass
High Pass
Recorder
Baseband
Audio
%ROOT%/recordings
Name template $t_$f_$h-$m-$s_$d-$M-$y
Container WAV
Sample type Int16
Stream Radio
Stereo
Ignore silence
0 -10 -20 -30 -40 -50 -60 -70 -80 -90 -100 -110
853.45M 853.5M 853.55M 853.6M 853.65M 853.7M 853.75M 853.8M 853.85M 853.9



Software: SDR Console / Device: RX888mk2

Dual Antenna Device = HF / VHF (Discone Antenna +MLA-30 / Antenna with LNA)

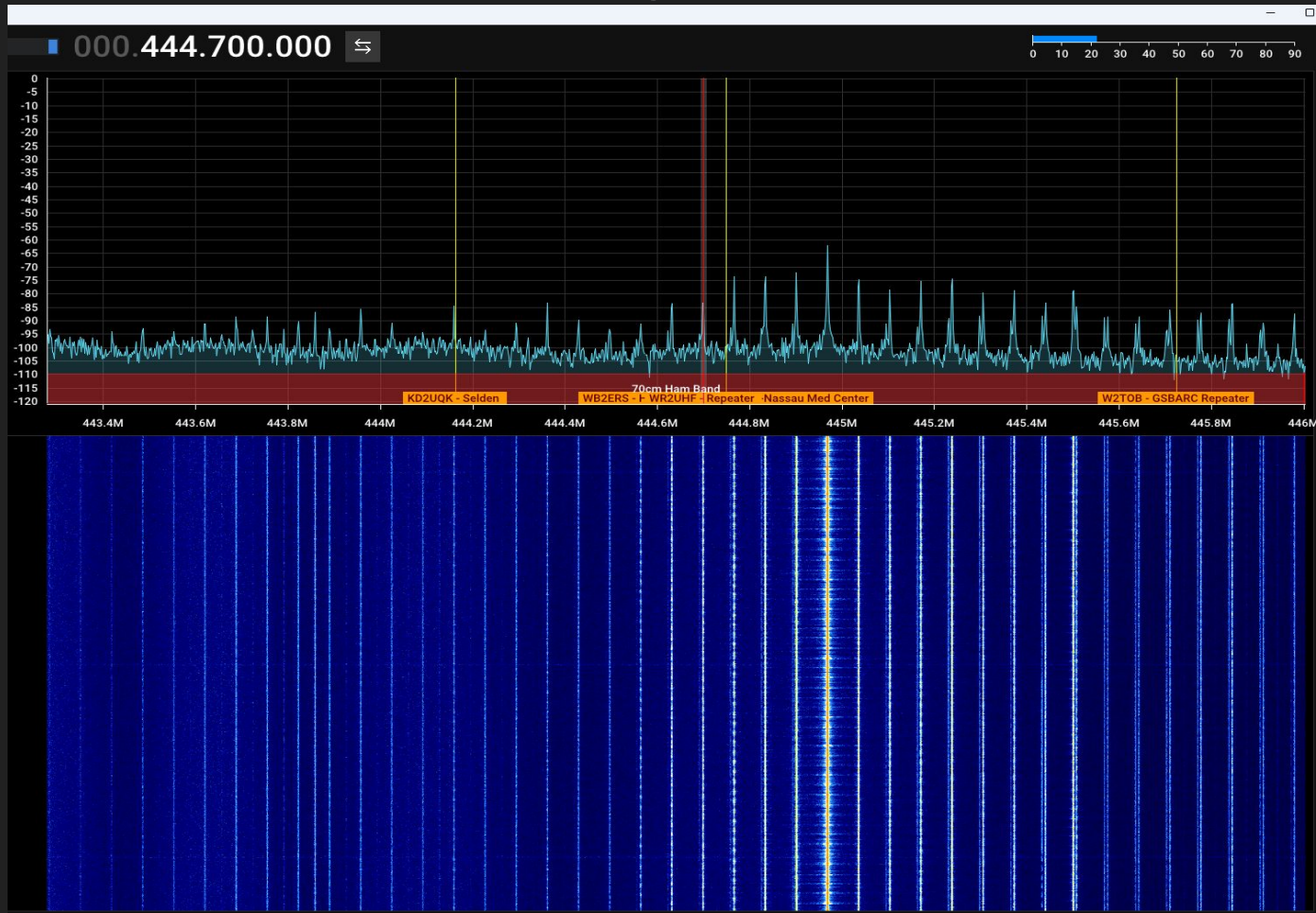
SDR - Waterfall / Troubleshooting

Noise

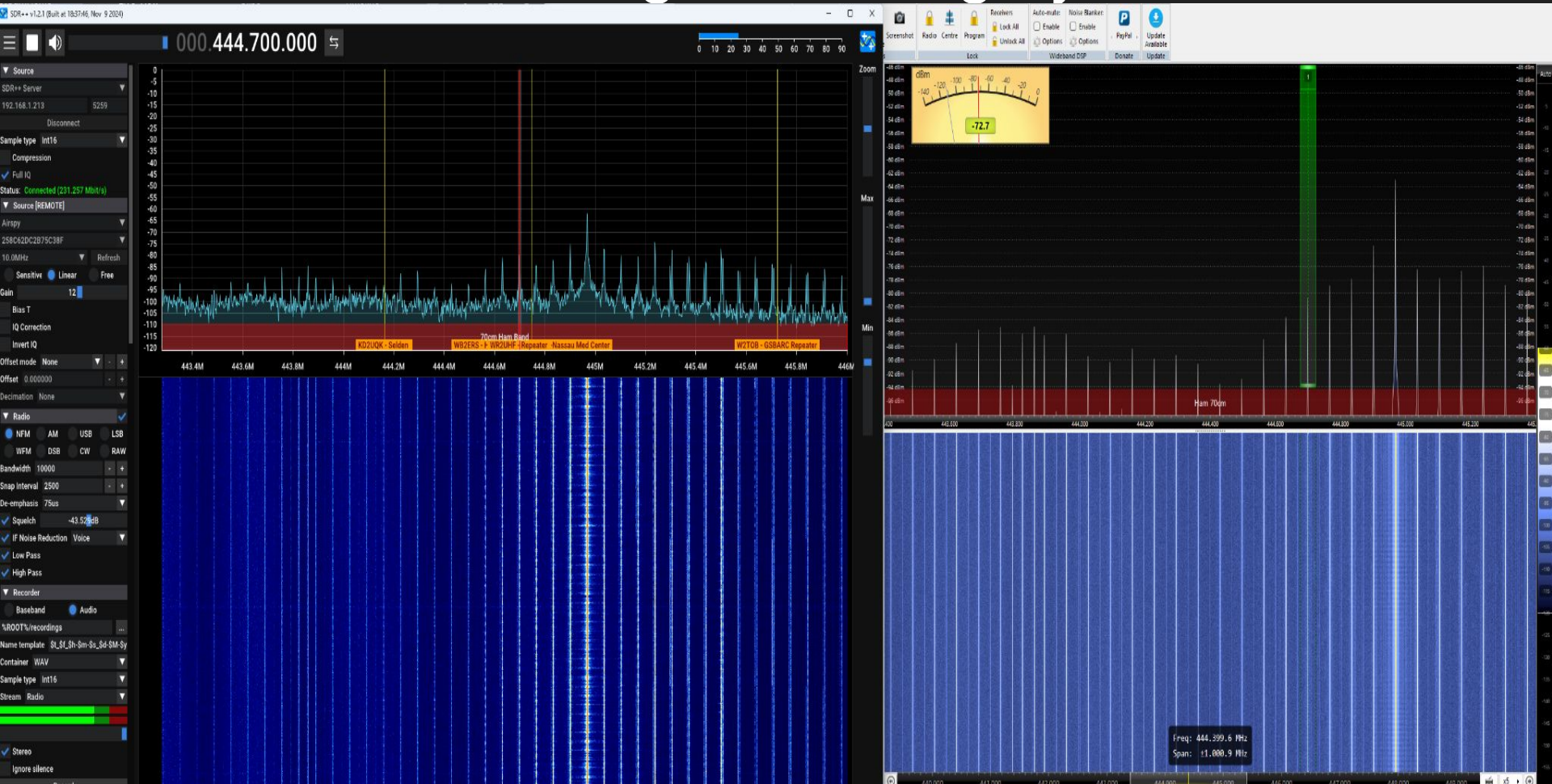
Harmonic

Is it coming from the system?

From the house?



SDR - Troubleshooting / Isolating Systems



SDR - Software Solutions

Linux - Kismet Wireless - www.kismetwireless.net

- Stand on the shoulders of giants
- Product Decodes RF/SDR components
  - Kismet extracts and presents items found
- Most open devices in the ISM band will show up.
- Examples:
  - ADSB (Plane Beacons), Water Meters, Weather/Temp Sensors, Vehicle Tire Pressure Sensors (TPMS), Other Sensors.

SDR - Software Solutions

Kismet - Shows the RTL-SDR directly in Data Source

Available Interface: rtl433-0 (rtl433)

Interface	rtl433-0
Capture Driver	rtl433
Hardware	rtlsdr
Type	rtl_433 USB SDR

Enable Source

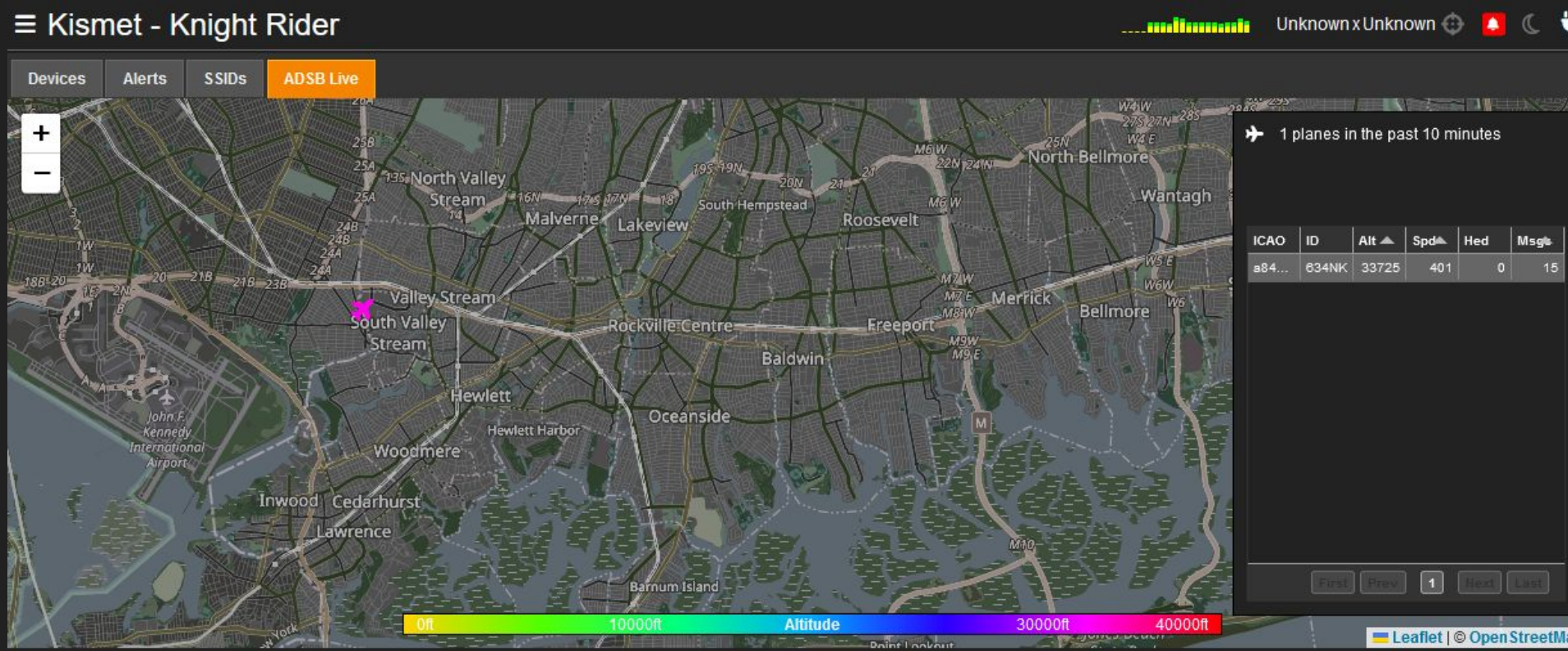
Available Interface: rtladsb-0 (rtladsb)

Interface	rtladsb-0
Capture Driver	rtladsb
Hardware	rtlsdr
Type	rtl_adsb USB SDR

Enable Source

SDR - Software Solutions

Kismet Wireless - Decoding ADSB - Plane Beacons



SDR - Software Solutions

Kismet Wireless - Decoding ADSB - Plane Beacons

≡ Kismet - Knight Rider

Unknown x Unknown

Devices | Alerts | SSIDs | ADSB Live

2 planes in the past 10 minutes

Flight:
Model: HAWKER BEE...WKER 900XP
Operator: BANK OF UTAH TRUSTEE
Altitude: 22050 ft
Speed: 423 MPH

ICAO	ID	Alt	Spd	Hed	Msgs
a2f3c5	29GP	22050	423	0	16
a84...	634NK	5450	399	0	30

First | Prev | 1 | Next | Last

0ft — 10000ft — Altitude — 30000ft — 40000ft

Leaflet | © OpenStreetMap

SDR - Software Solutions - Kismet Wireless

≡ Kismet - BusySignal HomeLab

Unknown
Unknown

Devices | Alerts | SSIDs | ADSB Live

12 planes in the past 10 minutes

ICAO	ID	Alt	Spd	Hed	Msg
a73...	565JB	2350	424	0	115
a7d...	605...	40000	401	216	51
ac6...	898...	16725	414	0	128
aae...	802...	17025	416	0	22
a3a...	334JB	27975	454	0	133
aa5...	766...	18325	373	0	17
aa9...	781...	625	418	0	177
ac2...	881...	2200	397	0	77
c6062	Unk...	36000	447	332	37
a65...	508JL	10525	308	0	47
407...	Unk...	11350	262	215	36
a67...	516...	38000	390	238	17

SDR - Software Solutions

Linux - Kismet Wireless - www.kismetwireless.net

Tire Pressure Sensor:

RF Sensor

Model	Toyota-d8e95f3d
Device ID	d8e95f3d
SNR	11
RSSI	-8
Noise	-19
Thermometer	
Temperature	33.80° F

M:
H:
D:

Tire pressure

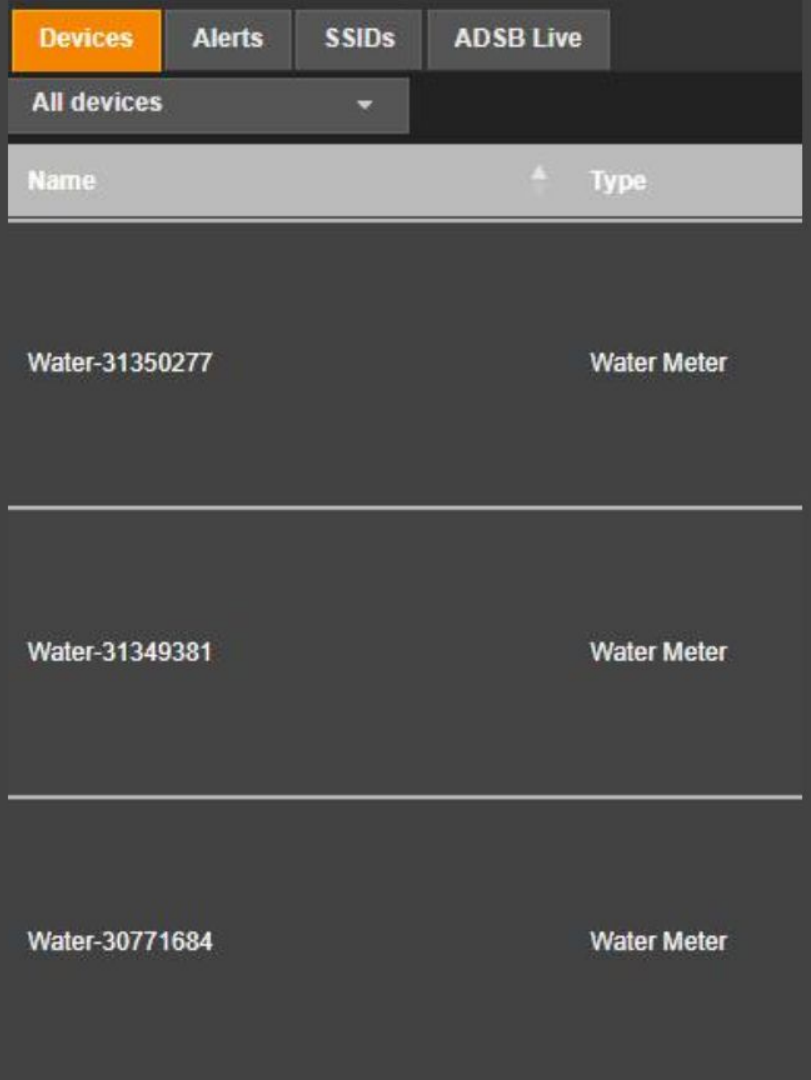
SDR - Software Solutions

Linux - Kismet Wireless - www.kismetwireless.net

Security Sensors:

SDR - Software Solutions

Water Meters:



Kismet:

Temp & Humidity Sensors:

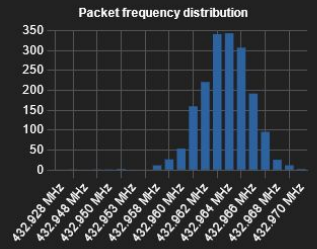
DEVICE: ACURITE-TOWER-13415

Device Info

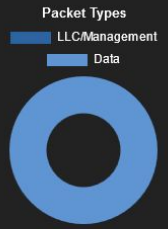
Name	Acurite-Tower-13415
Notes	*Empty*
MAC Address	36:67:0B:05:8F:22
Manufacturer	RF Sensor
Type	Sensor
First Seen	Fri Jan 03 2025 18:35:04 GMT-0500 (Eastern Standard Time)
Last Seen	Fri Jan 03 2025 21:27:32 GMT-0500 (Eastern Standard Time)

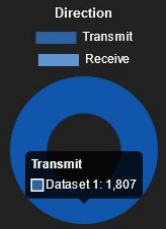
Frequencies

Channel	A
Main Frequency	432.959 MHz



Packets





Total Packets	1807
Rx Packets	0
Tx Packets	1807
LLC/Management	0
Error/Invalid	0
Data	1807
Encrypted	0
Filtered	0
Data Transferred	0 B

DEVICE: ACURITE-TOWER-13415

Device Info

RF Sensor

Model	Acurite-Tower-13415
SNR	13
Noise	-13
Sub-Channel	A
Battery	1

Thermometer

Temperature 29.12° F

M:
H:
D:

Moisture

Moisture (%) 59%

M:
H:
D:

Kismet Wireless

WiFi Devices

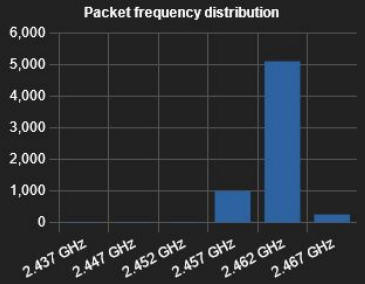
DEVICE: WAXXXXXXXXFI

Device Info

Name	WaXXXXXXXXFi
Notes	*Empty*
MAC Address	6E:22:32:XX:XX:XX
Manufacturer	Ubiquiti Inc
Type	Wi-Fi AP
First Seen	Fri Jan 03 2025 18:34:44 GMT-0500 (Eastern Standard Time)
Last Seen	Fri Jan 03 2025 21:34:40 GMT-0500 (Eastern Standard Time)

Frequencies

Channel	11
Main Frequency	2.467 GHz



Signal

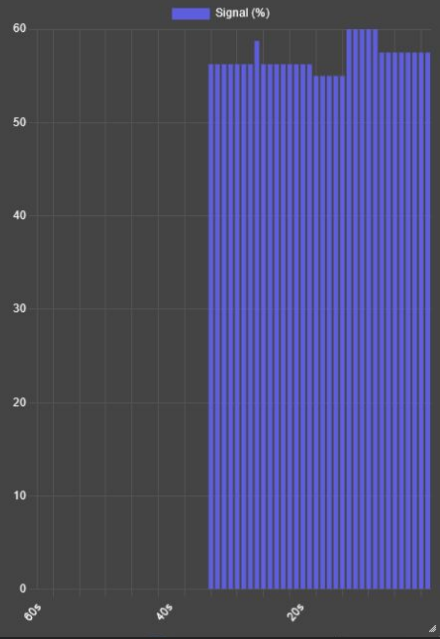
Monitor Signal	**Monitor**
Latest Signal	-53 dbm
Min. Signal	-86 dbm
Max. Signal	-43 dbm

Packets

SIGNAL 6E:22:32:XX:XX:XX WARDRIVEWIFI

Signal

Last Signal:	-54 dBm
Min Signal:	-86 dBm
Max Signal:	-43 dBm



Advertised SSIDs

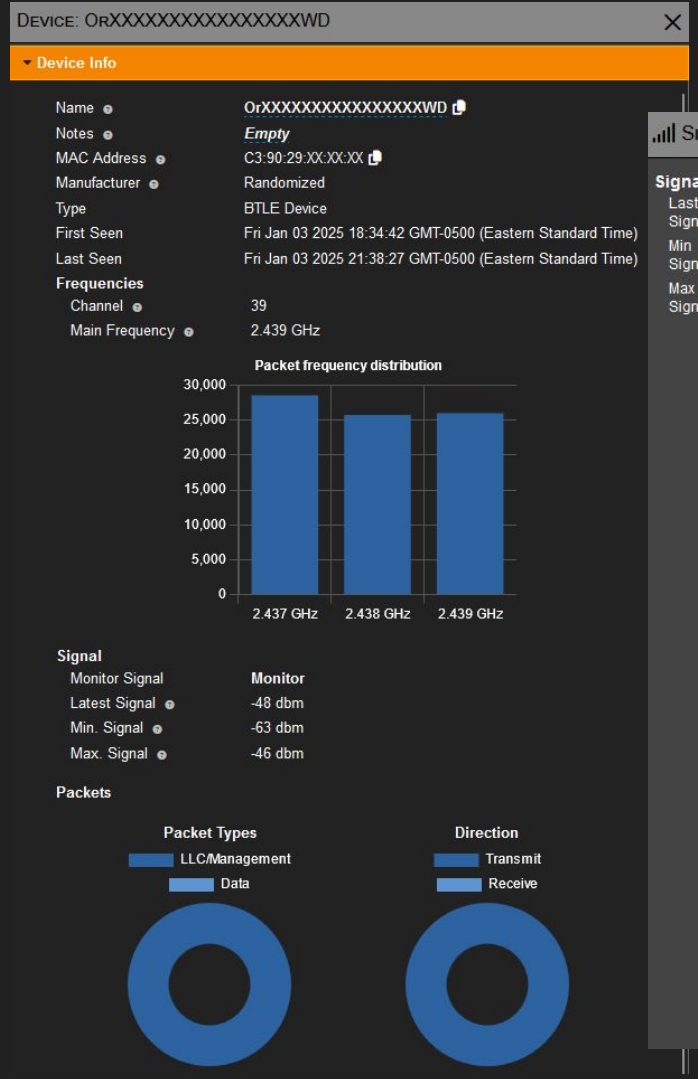
SSID: WaXXXXXXXXFi

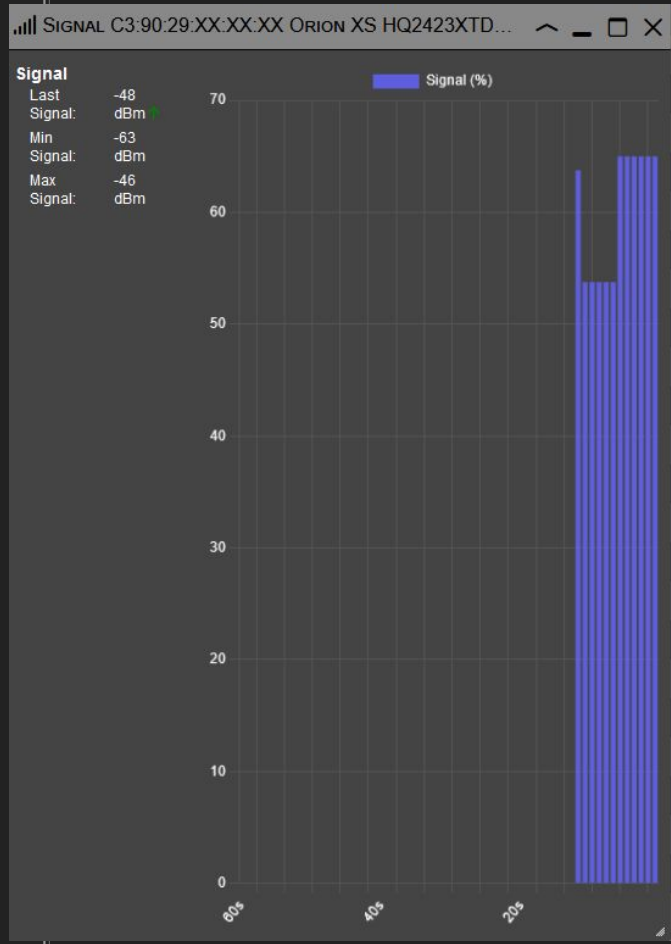
SSID	WaXXXXXXXXFi
Encryption	WPA3 WPA3-PSK WPA3-SAE AES-CCMP
MFP	Supported (802.11w)
Channel	11
HT Mode	HT20
Connected Stations	0
Channel Utilization	56.86%
Advertised Power	22dBm
First Seen	Jan 03 2025 18:34:44
Last Seen	Jan 03 2025 21:37:11
Beacon Rate	10/sec
Max. Rate	780 MBit/s
802.11d Country	US

Responded SSIDs

Kismet Wireless

BTLE Devices

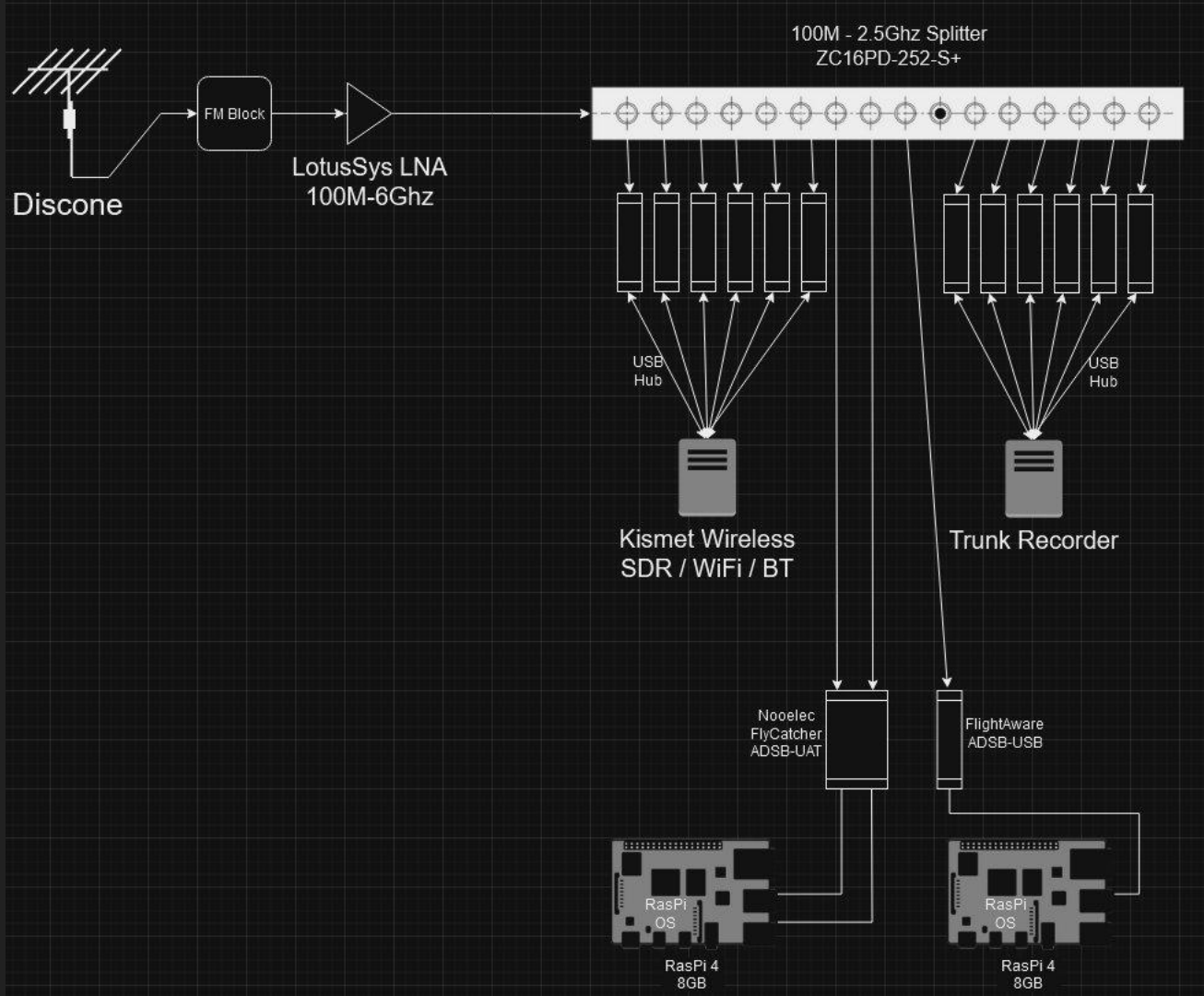




Advanced Build

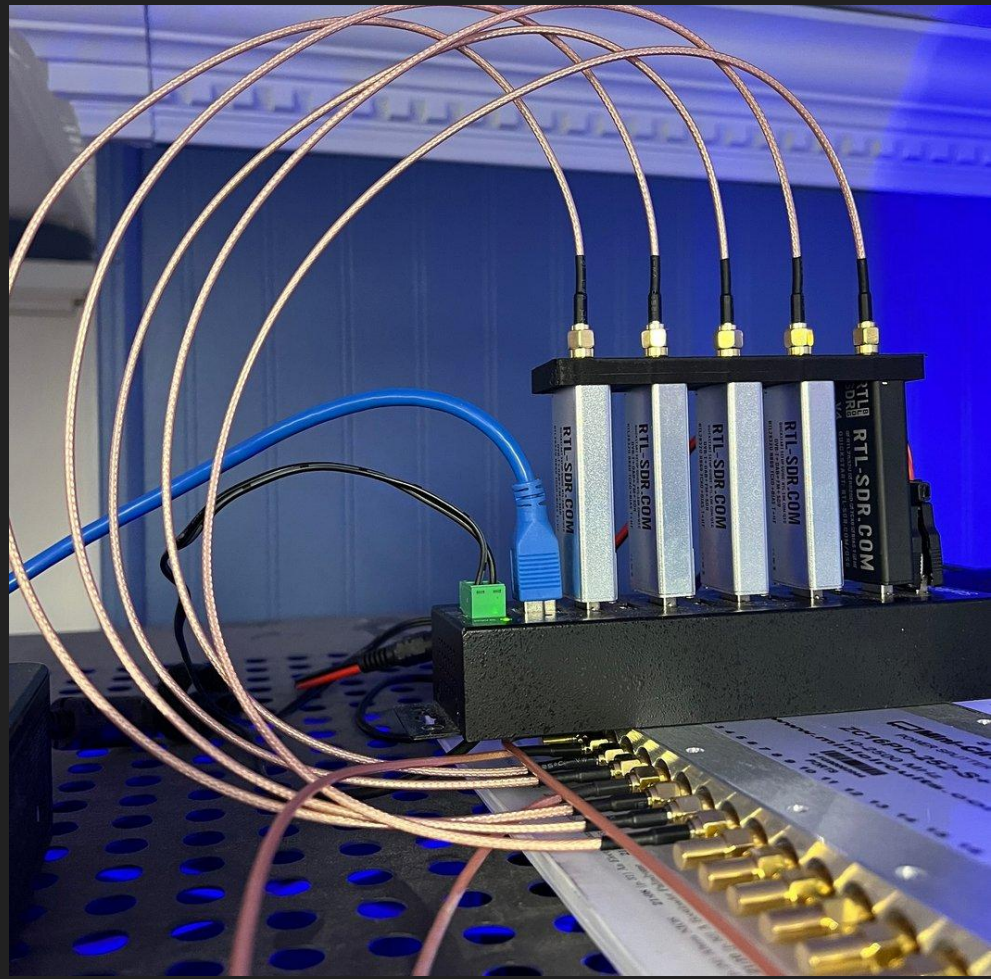
Wiring Diagram

- Parts List
  - Mini-Circuits 16 port splitter
  - RTL-SDR V3/V4
  - StarTech USB 10 port Powered USB 3.0 Powered Hub



Advanced Build

Suffolk P25 Trunk-Recorder



Closing

- Slides will be shared (check GitHub)
- Questions
- Go Be Radio Frequency Curious

Appendix

- RTL-SDR Devices
  - https://www.rtl-sdr.com/buy-rtl-sdr-dvb-t-dongles/
  - https://www.nooelec.com/store/sdr.html

- Multiple SDR Trunk Recorder
  - https://github.com/robotastic/trunk-recorder
  - Location for MY Build Configuration file for SCPD (and more)
    - https://github.com/busysignal/SCPD-TrunkRecorder

- Kismet Wireless
  - https://www.kismetwireless.net/download/
  - https://www.kismetwireless.net/docs/readme/intro/kismet/

- Kismet Wireless / WiFi / WarDrive Rig Systems
  - www.busysignal.io
  -