Overview of Frugal Radio Spying

Receiving & transmitting radio signals with RTL-SDR & Arduino/RasPi GPIO pins

Around 2012

RTL2832U chipset designed to create affordable DVB-T TV USB dongles

DVB-T TV is Digital Video Broadcasting; antenna television format popular in Europe

Research of Antti Palosaari, Eric Fry and Osocom determined chipset could be accessed directly & could be tuned to 500kHz -- 1.7GHz

RTL-SDR Hardware varieties

What is the RTL-SDR frequency range?

This is dependent on the particular tuner variant used in the dongle, and the particular implementation. Some dongles, like our RTL-SDR Blog V3 also utilize the direct sampling mode which can enable reception below 28 MHz.

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

As you can see from the table, the **Elonics E4000** and **Rafael Micro R820T** dongles have the greatest frequency range.

https://www.rtl-sdr.com/about-rtl-sdr/
https://hackaday.com/2017/09/05/19-rtl-sdr-dongles-reviewed/

Amazon.com: RTL-SDR B

https://www.amazon.com/RTL-SDR-Blog-RTL2832U-Software-Telescopic/dp/B011HVUEME/ref=sr_1_3?ie=UTF8&qid=1546393387&sr=8-3&k

Search

amazon Try Prime

All rtl-sdr

New Year New You

Deliver to Bellevue 68123

Your Amazon.com Today's Deals Gift Cards Whole Foods Registry Sell Help

EN Hello. Sign in Account & Lists Orders Try Prime 0 Cart

All Electronics Deals Best Sellers TV & Video Audio & Home Theater Computers Camera & Photo Wearable Technology Car Electronics & GPS Portable Audio Cell Phones Office Electronics Musical Instruments New Arrivals Trade-In

‹ Back to search results for "rtl-sdr"

RTL-SDR Blog R820T2 RTL2832U 1PPM TCXO SMA Software Defined Radio with 2x Telescopic Antennas

by RTL-SDR Blog

4.1 out of 5 stars 593 customer reviews | 172 answered questions

Amazon's Choice for "rtl-sdr"

Price: $27.95 & FREE Shipping. Details

- Includes 1x RTL-SDR Blog brand R820T2 RTL2832U 1PPM TCXO HF Bias Tee SMA Dongle (V3), 1x portable multipurpose dipole antenna set. Dipole set includes 1x dipole base with 60cm RG174, 2x 23cm to 1m telescopic antenna, 2x 5cm to 13cm telescopic antenna, 1x 3m RG173 extension cable, 1x flex tripod mount, 1x suction cup mount.
- Great for many applications including general radio scanning, air traffic control, public safety radio, ADSB, ACARS, trunked radio, P25 digital voice, POCSAG, weather balloons, APRS, NOAA APT weather satellites, radio astronomy, meteor scatter monitoring, DAB, or for use as a low cost panadapter with a traditional ham radio.
- Several improvements over other brands including use of the R820T2 tuner, improved component tolerances, a 1 PPM temperature compensated oscillator (TCXO), SMA F connector, aluminium shielded case with thermal pad for passive cooling, activatable bias tee circuit and a much improved antenna set.
- Can tune from 500 kHz to 1.7 GHz and has up to 3.2 MHz of instantaneous bandwidth (2.4 MHz stable). (HF reception below 24 MHz in direct sampling mode). Please note RTL-SDR dongles are RX only.
- The multipurpose portable dipole kit is great for beginners! Use it either for terrestrial or satellite reception just by changing the orientation of the antenna. The mounts and extension cable allow you to temporarily place the antenna outside for improved reception.

Compare with similar items

Used & new (2) from $25.20 & FREE shipping.

SMA Adapter Connectivity Kit: 8 Adapters for NESDR (RTL-SDR) SMA Radios w/Case

Share 490+ Shares

$27.95

& FREE Shipping. Details

Want it Friday, Jan. 4? Choose Two-Day Shipping at checkout. Details

In Stock.

Sold by RTL-SDR Blog and Fulfilled by Amazon. Gift-wrap available.

Qty: 1

Add a Protection Plan:

4-Year Protection for $2.00

3-Year Protection for $1.62

Add to Cart

Turn on 1-Click ordering for this browser

Deliver to Bellevue 68123

Add to List

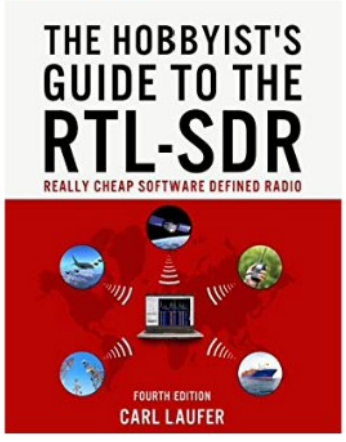
Other Sellers on Amazon

The Hobbyist's Guide to the RTL-SDR: Really Cheap Software Defined Radio

1st Edition

ISBN-13: 978-1514716694, **ISBN-10:** 1514716690

★★★★½ (216)



Format **Paperback** >

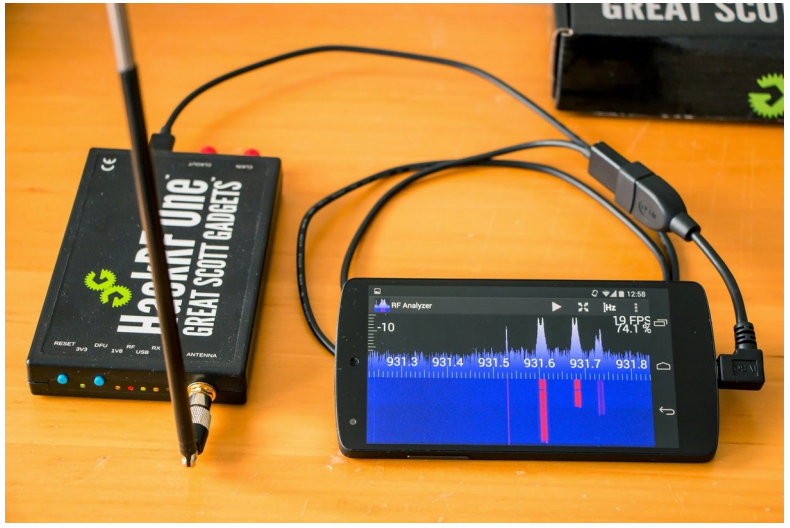
$23.70 ~~$24.95~~ *Save $1.25 (5%)*

What are some RTL-SDR Radio Scanner Applications?

The RTL-SDR can be used as a wide band radio scanner. Applications include:

- Use as a police radio scanner.
- Listening to EMS/Ambulance/Fire communications.
- Listening to aircraft traffic control conversations.
- Tracking aircraft positions like a radar with ADSB decoding.
- Decoding aircraft ACARS short messages.
- Scanning trunking radio conversations.
- Decoding unencrypted digital voice transmissions such as P25/DMR/D-STAR.
- Tracking maritime boat positions like a radar with AIS decoding.
- Decoding POCSAG/FLEX pager traffic.
- Scanning for cordless phones and baby monitors.
- Tracking and receiving meteorological agency launched weather balloon data.
- Tracking your own self launched high altitude balloon for payload recovery.
- Receiving wireless temperature sensors and wireless power meter sensors.
- Listening to VHF amateur radio.
- Decoding ham radio APRS packets.
- Watching analogue broadcast TV.
- Sniffing GSM signals.
- Using rtl-sdr on your Android device as a portable radio scanner.
- Receiving GPS signals and decoding them.
- Using rtl-sdr as a spectrum analyzer.
- Receiving NOAA weather satellite images.
- Listening to satellites and the ISS.
- Radio astronomy.
- Monitoring meteor scatter.
- Listening to FM radio, and decoding RDS information.
- Listening to DAB broadcast radio.
- Listening to and decoding HD-Radio (NRSC5).
- Use rtl-sdr as a panadapter for your traditional hardware radio.
- Decoding taxi mobile data terminal signals.
- Use rtl-sdr as a high quality entropy source for random number generation.
- Use rtl-sdr as a noise figure indicator.
- Reverse engineering unknown protocols.
- Triangulating the source of a signal.
- Searching for RF noise sources.
- Characterizing RF filters and measuring antenna SWR.
- Decoding Inmarsat STD-C EGC geosynchronous satellites.
- Listening to the ISS (International Space Station).

Embedded Linux Friendly



Android Apps

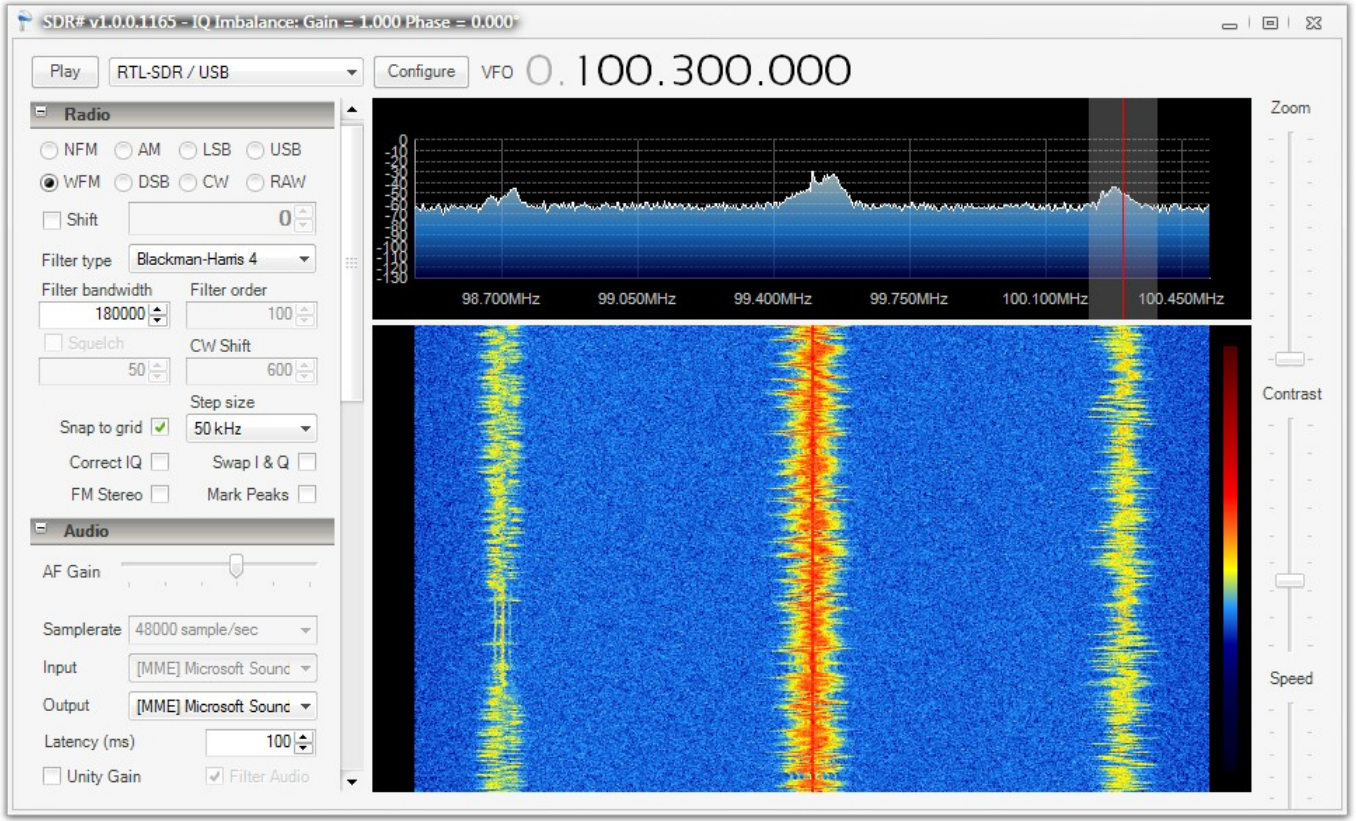
Raspberry Pi
Beagle Bone

Wifi Router (OpenWrt)

Minimal Software Tools

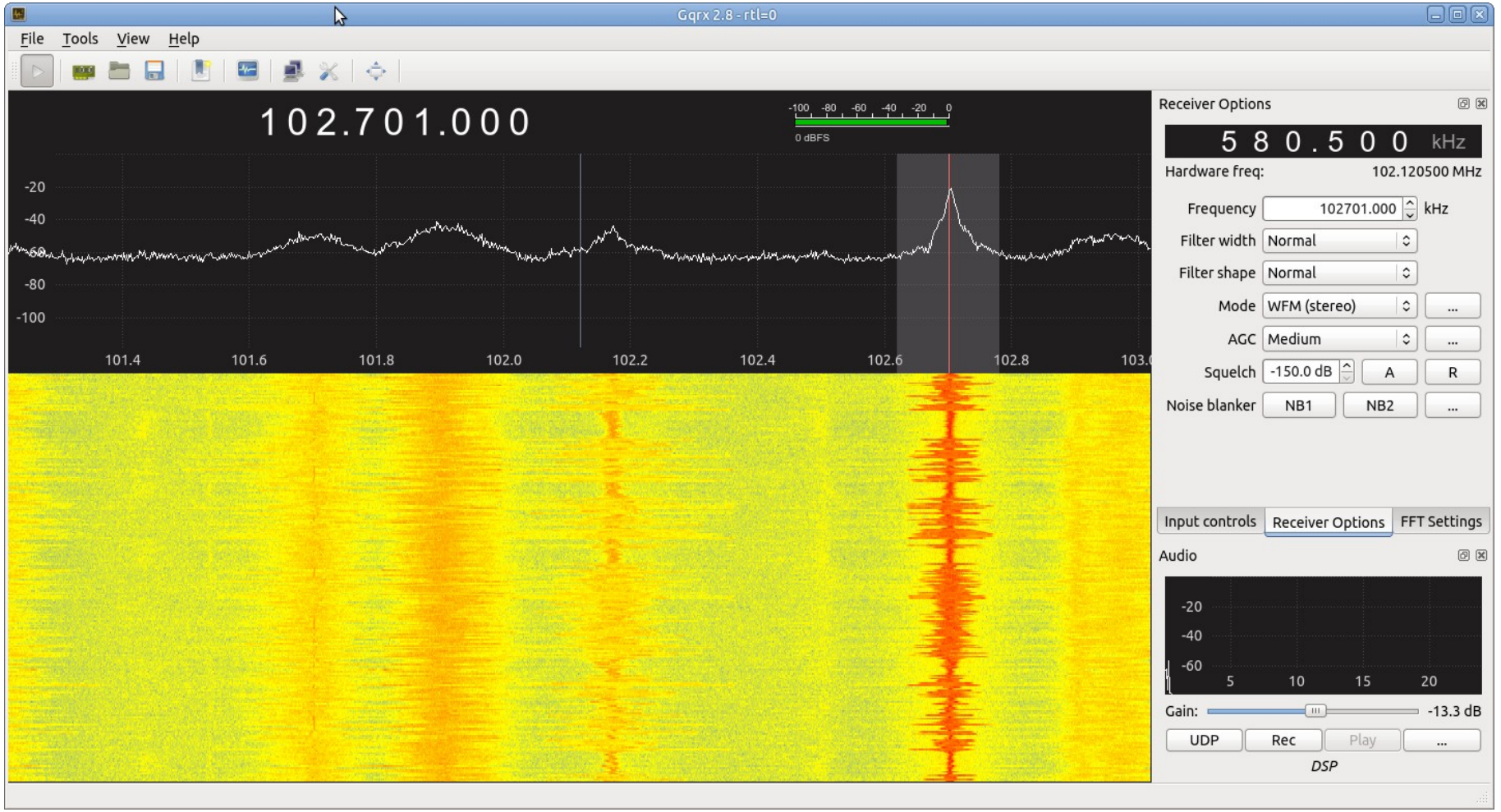
GUI Tuners

For Windows: SDR Sharp aka SDR#



https://airspy.com/download/

GUI Tuners
For Linux: GQRX



http://gqrx.dk/

https://www.bastibl.net/gqrx-for-digital-signals/

RTL-SDR Library (librtlsdr) & Command Line Executables

https://github.com/osmocom/rtl-sdr

rtl_test : benchmarking tool

rtl_eeprom : ROM programming tool, e.g. change default serial number

rtl_power : wideband spectrum monitor utility. Used for signal detection, e.g. bug detection, heat maps, reverse engineering

rtl_sdr : I/Q recorder (In-phase & Quadrature Phase data), “complete” radio signal. Used for replay attacks

rtl_tcp : stream raw radio signal (I/Q) over TCP/IP. Instead of running coaxial cable to antenna, run ethernet cable/wifi/active USB cable to antenna w/ RTL-SDR & embedded linux attached

rtl_fm : simple tuner & FM demodulator, pipe into Linux sox program to change sample rate & record to .wav file

A lot of these tools already in Kali Linux. Radio flavors of Linux OS too (e.g. SigintOS https://www.sigintos.com/)

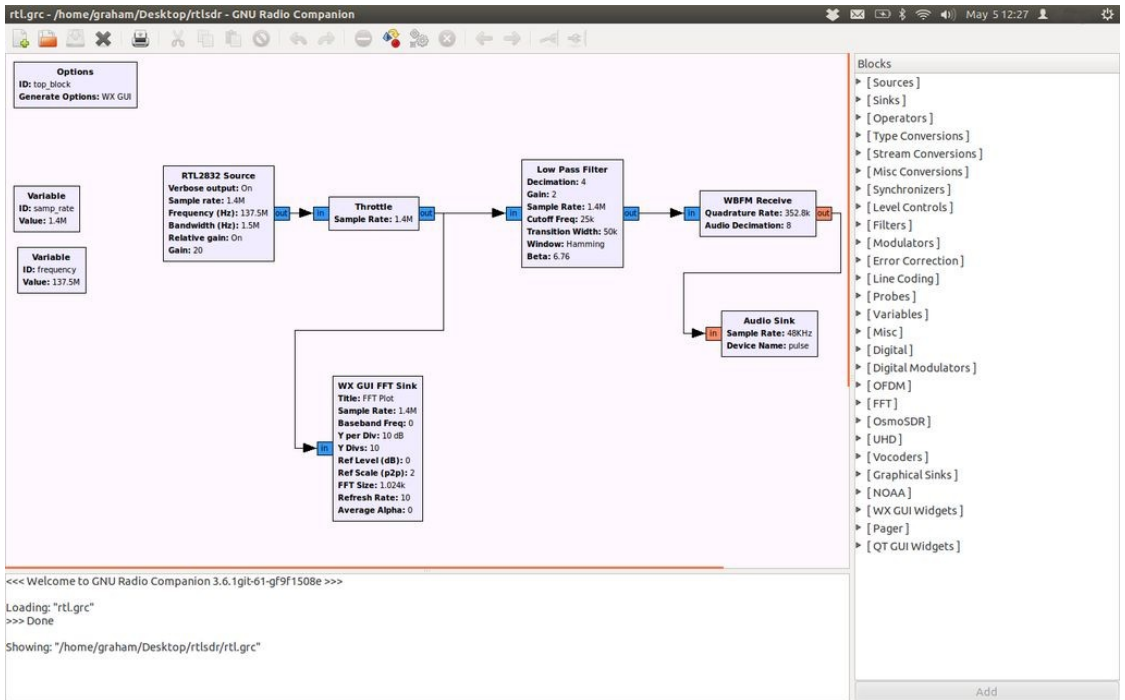
GNU Radio

THE FREE & OPEN SOFTWARE RADIO ECOSYSTEM

Very powerful, but steep learning curve

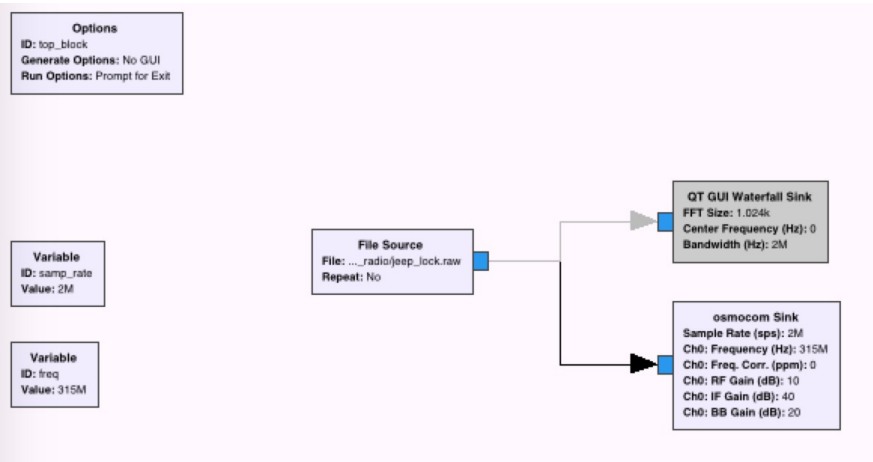
Simple FM Tuner

https://www.instructables.com/id/RTL-SDR-FM-radio-receiver-with-GNU-Radio-Companion/



Simple Replay Attack

https://calebmadrigal.com/hackrf-replay-attack-jeep/



Rftap: GNURadio → Wireshark

https://rftap.github.io/

Zigbee Example https://rftap.github.io/blog/2016/09/04/rftap-zigbee.html

DIY Antennas

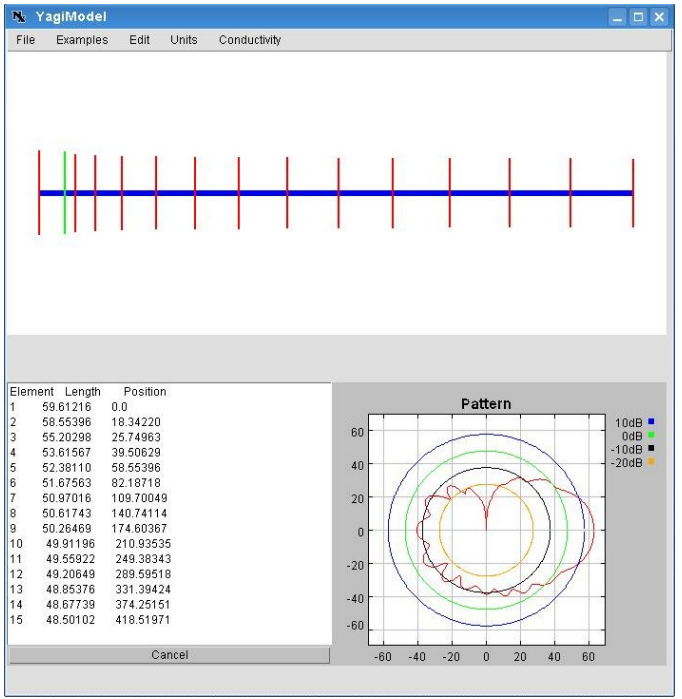
2.4GHz (wifi) & 1.6GHz (weather balloon) Yagi

Copper wire from
Lowes or Home Depot

SMA male connectors
(2.4GHz devices use RP-SMA!!! Do not mix up)

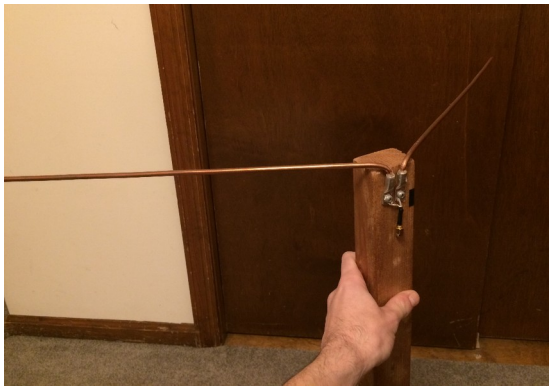
RG174 Coaxial Cable

Yagi Calculator for Target Frequency



http://fermi.la.asu.edu/ccli/applets/yagi/yagi.html
http://www.vk5dj.com/yagi.html

137MHz V-Dipole for Weather Satellites

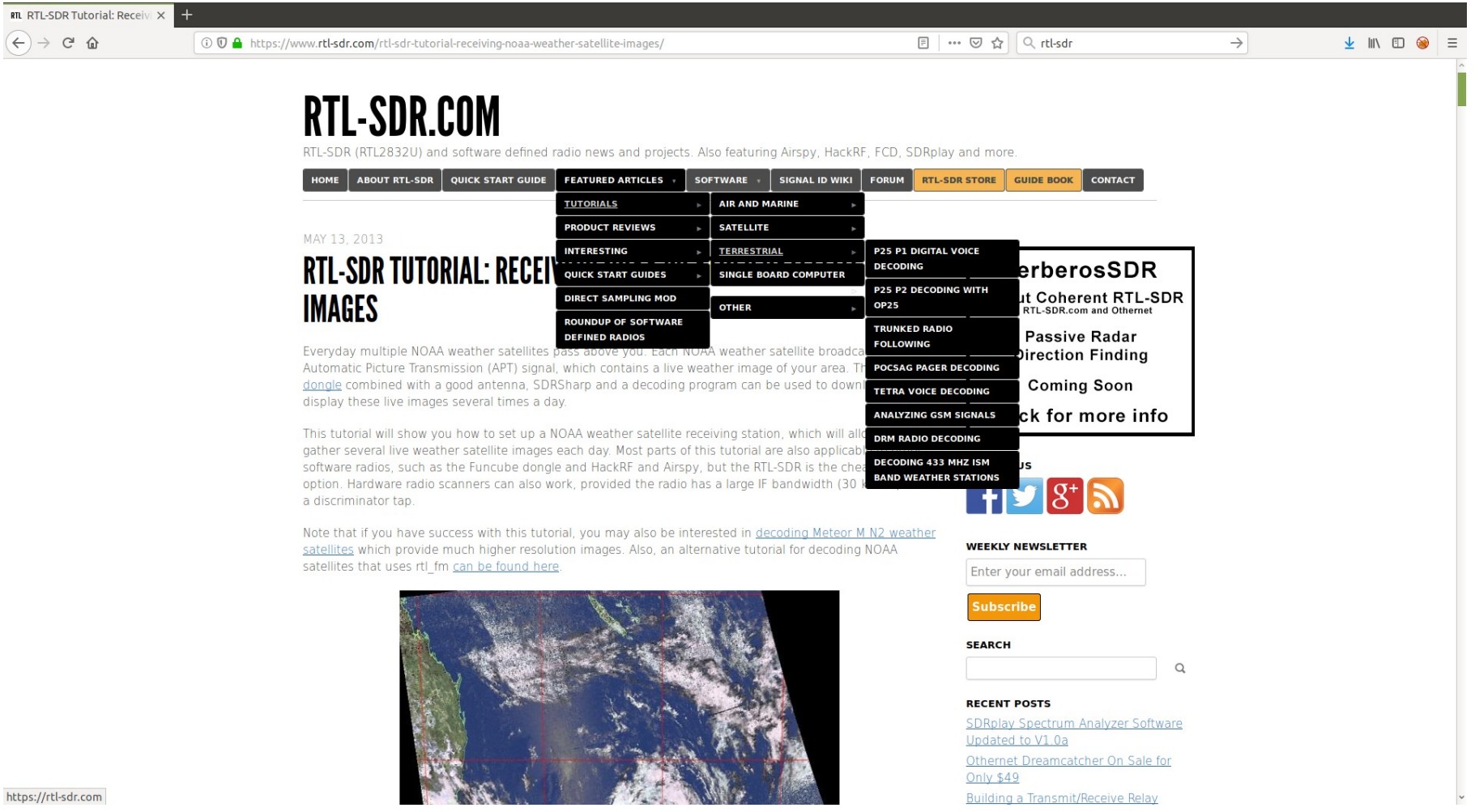


http://lna4all.blogspot.com/2017/02/diy-137-mhz-wx-sat-v-dipole-antenna.html

http://www.onlineconversion.com/frequency_wavelength.htm

RTL-SDR.com Blog

Best resource for all things RTL-SDR



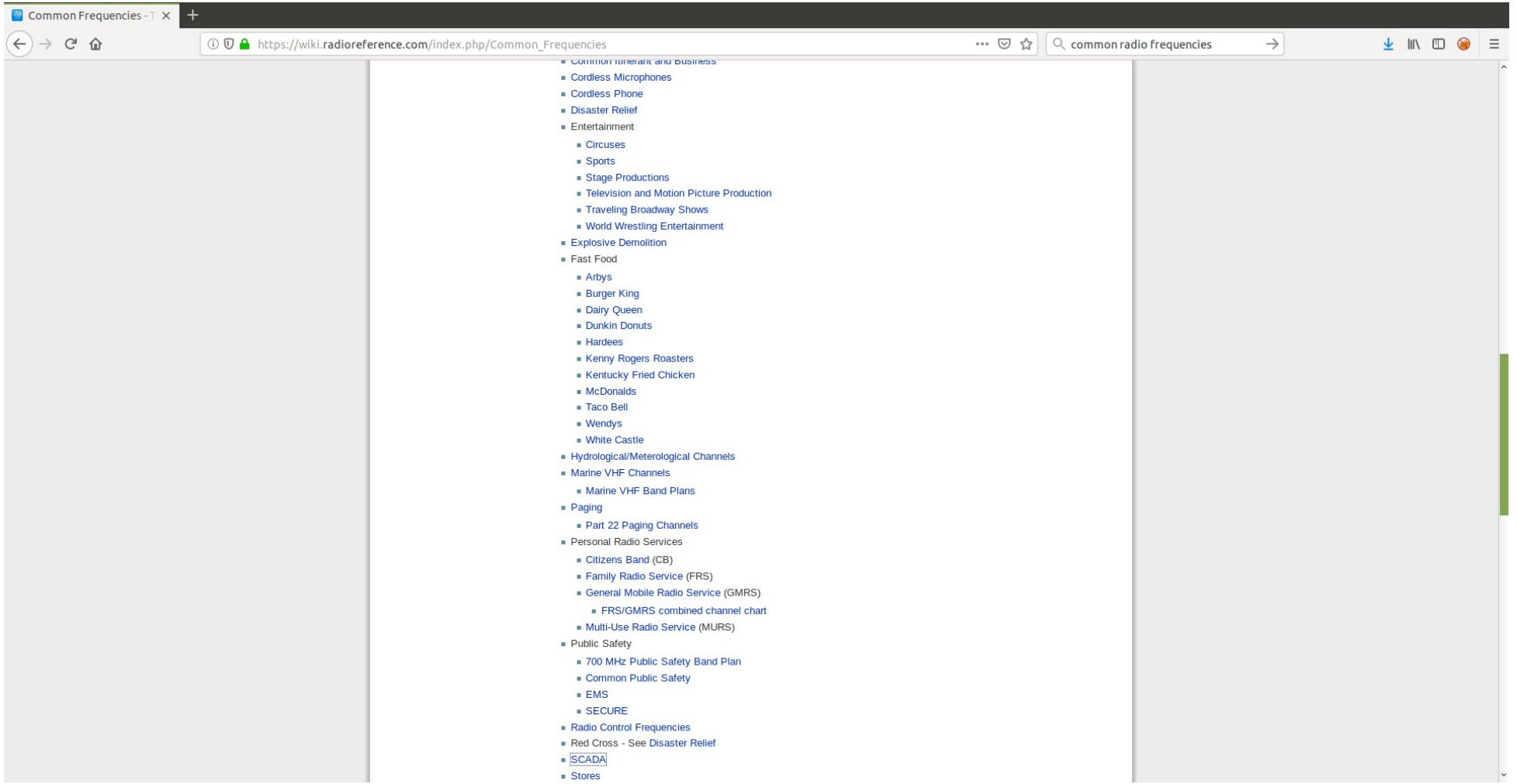
RTL-SDR.com Blog

Select Categories to Security

Common Radio Frequencies

Some databases/frequencies are outdated/obsolete

https://wiki.radioreference.com/index.php/Common_Frequencies



Digital Voice Comms

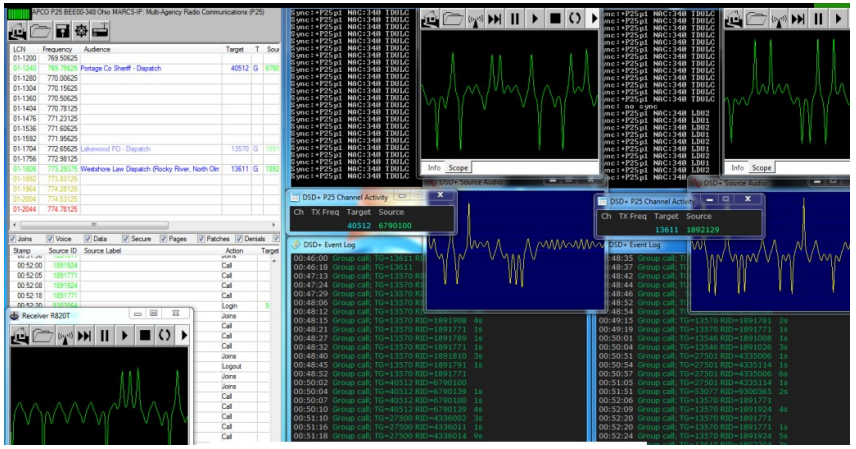
Police and Cordless Phones

Omaha Police uses P25 Trunking System (ORION)

https://www.radioreference.com/apps/db/?sid=2361

*need 2 RTL dongles (one for control channel)

https://www.jeffreykopcak.com/2014/12/12/p25-trunked-tracking-and-decoding-with-rtl-sdr-unitrunker-and-dsdplus/



Cordless Phones

DECT Protocol 900MHz, 1.9GHz, 5.8GHz

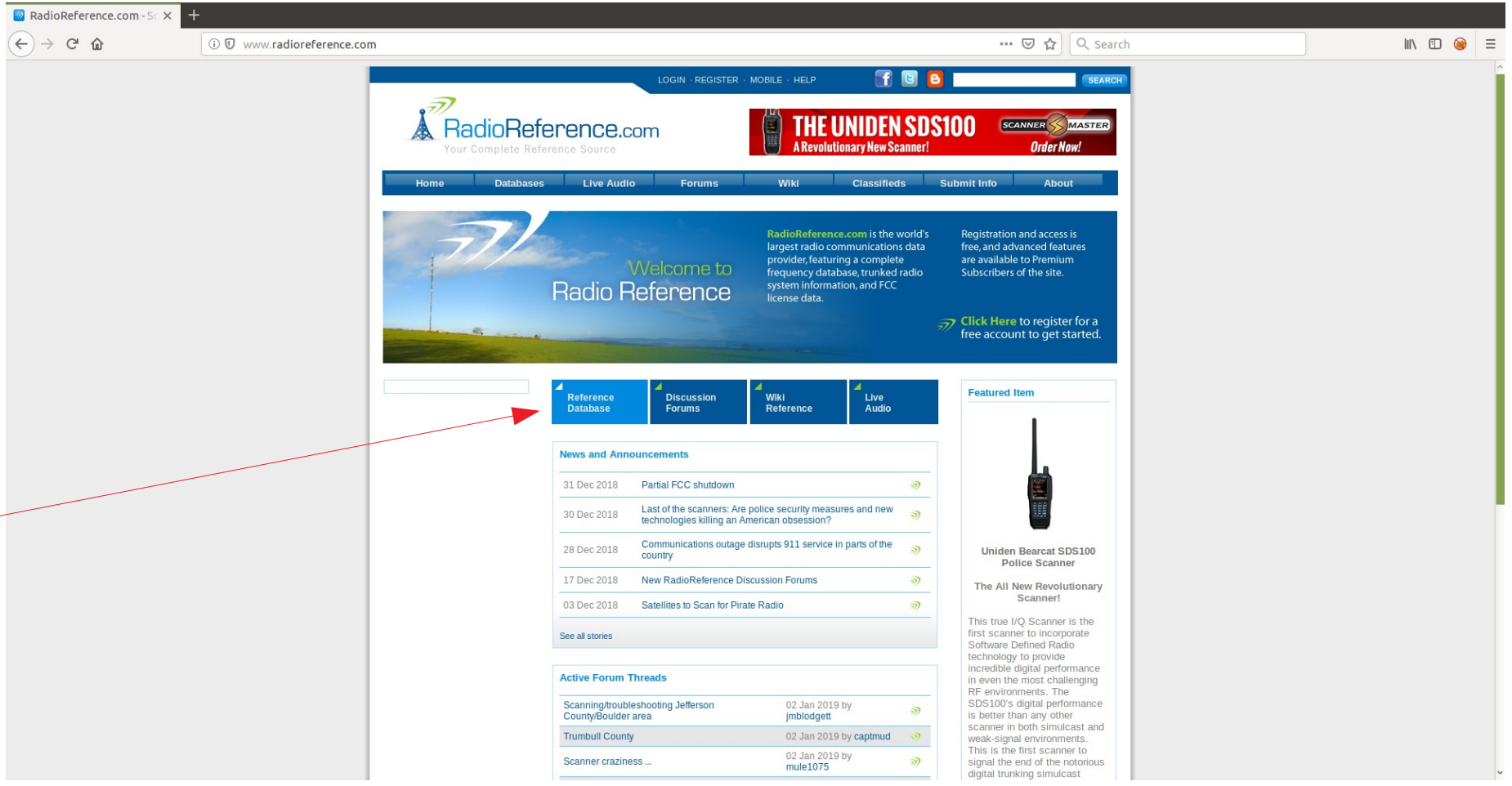
GR-DECT2: GNURadio DECT Audio Decoder

https://github.com/SignalsEverywhere/gr-dect2

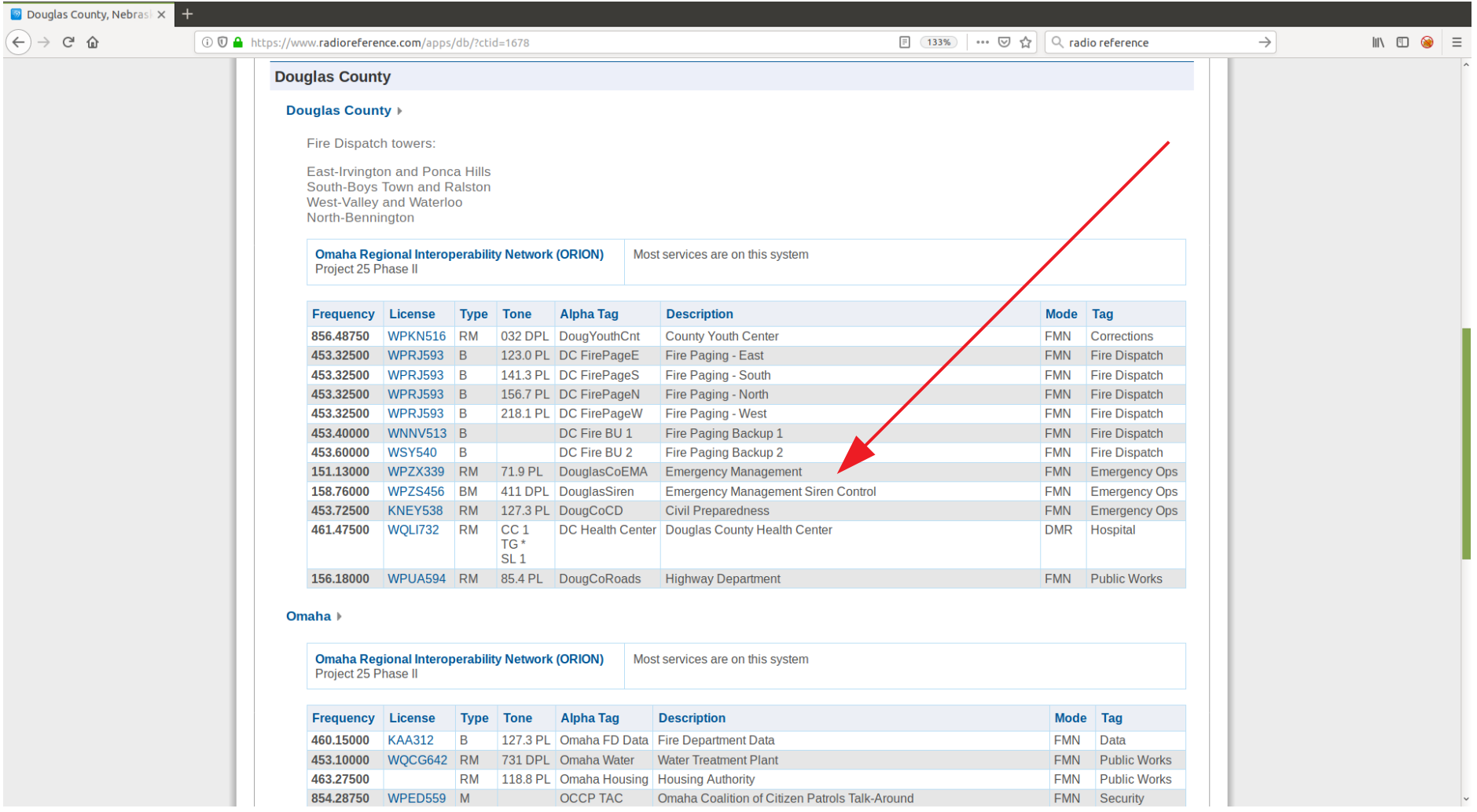
https://www.rtl-sdr.com/youtube-tutorial-eavesdropping-on-dect6-0-cordless-phones-with-a-hackrf-and-gr-dect2/

Finding Local Frequenices

Radioreference.com Reference Database



RadioReference Douglas County Results



Douglas County

Douglas County

Fire Dispatch towers:

East-Irvington and Ponca Hills
South-Boys Town and Ralston
West-Valley and Waterloo
North-Bennington

Omaha Regional Interoperability Network (ORION) Project 25 Phase II	Most services are on this system

Frequency	License	Type	Tone	Alpha Tag	Description	Mode	Tag
856.48750	WPKN516	RM	032 DPL	DougYouthCnt	County Youth Center	FMN	Corrections
453.32500	WPRJ593	B	123.0 PL	DC FirePageE	Fire Paging - East	FMN	Fire Dispatch
453.32500	WPRJ593	B	141.3 PL	DC FirePageS	Fire Paging - South	FMN	Fire Dispatch
453.32500	WPRJ593	B	156.7 PL	DC FirePageN	Fire Paging - North	FMN	Fire Dispatch
453.32500	WPRJ593	B	218.1 PL	DC FirePageW	Fire Paging - West	FMN	Fire Dispatch
453.40000	WNNV513	B		DC Fire BU 1	Fire Paging Backup 1	FMN	Fire Dispatch
453.60000	WSY540	B		DC Fire BU 2	Fire Paging Backup 2	FMN	Fire Dispatch
151.13000	WPZX339	RM	71.9 PL	DouglasCoEMA	Emergency Management	FMN	Emergency Ops
158.76000	WPZS456	BM	411 DPL	DouglasSiren	Emergency Management Siren Control	FMN	Emergency Ops
453.72500	KNEY538	RM	127.3 PL	DougCoCD	Civil Preparedness	FMN	Emergency Ops
461.47500	WQLI732	RM	CC 1 TG * SL 1	DC Health Center	Douglas County Health Center	DMR	Hospital
156.18000	WPUA594	RM	85.4 PL	DougCoRoads	Highway Department	FMN	Public Works

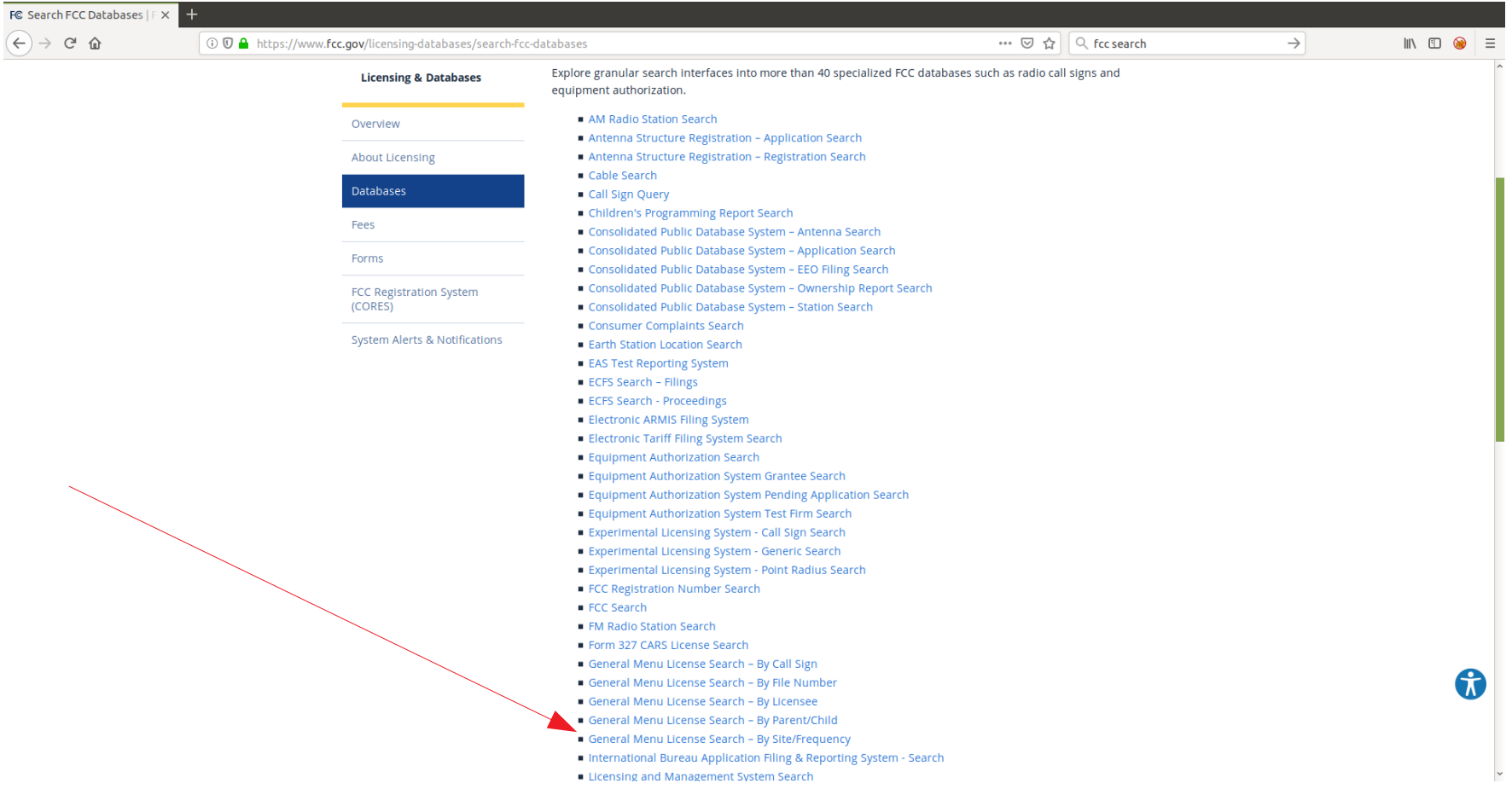
Omaha

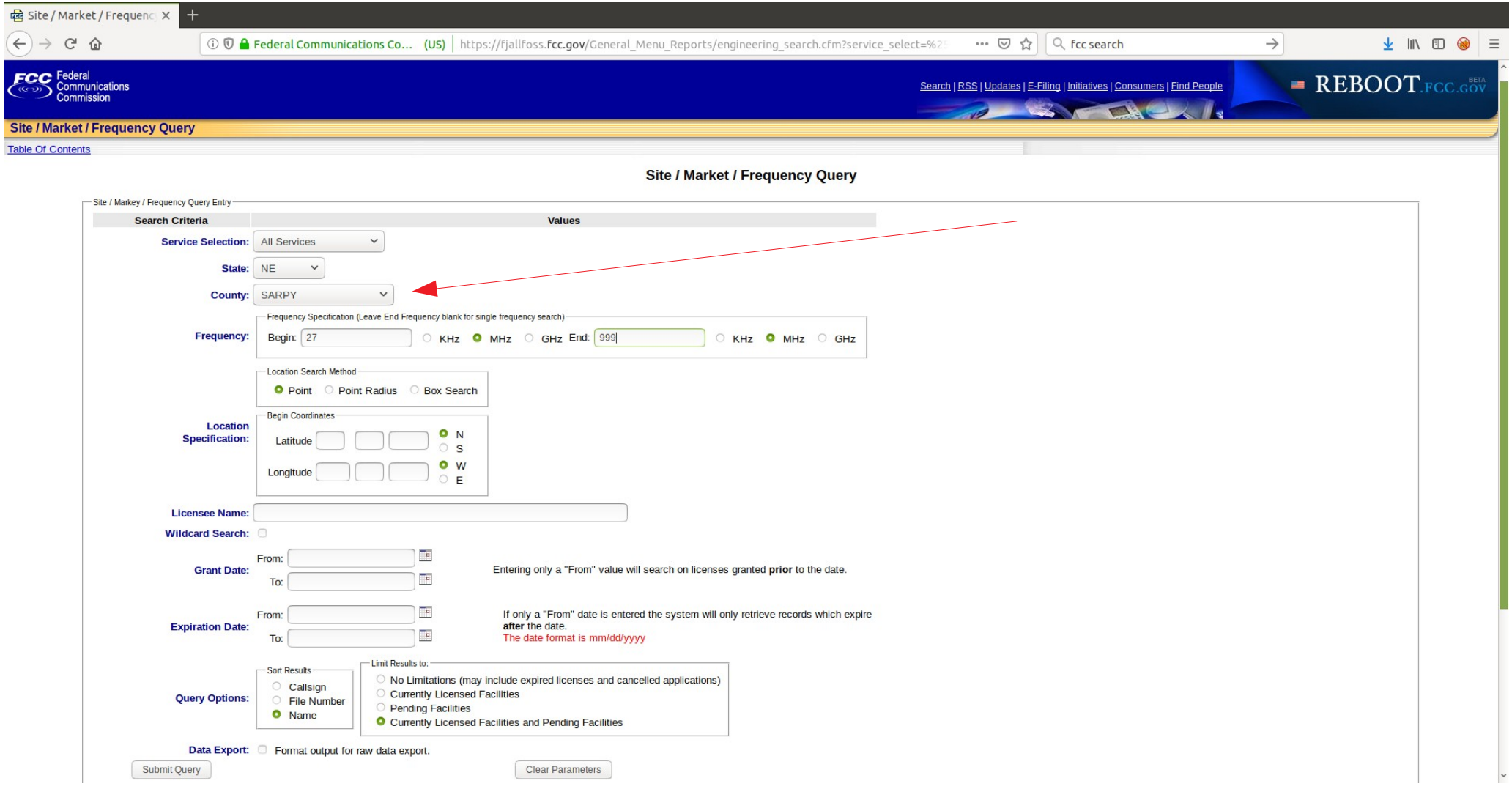
Omaha Regional Interoperability Network (ORION) Project 25 Phase II	Most services are on this system

Frequency	License	Type	Tone	Alpha Tag	Description	Mode	Tag
460.15000	KAA312	B	127.3 PL	Omaha FD Data	Fire Department Data	FMN	Data
453.10000	WQCG642	RM	731 DPL	Omaha Water	Water Treatment Plant	FMN	Public Works
463.27500		RM	118.8 PL	Omaha Housing	Housing Authority	FMN	Public Works
854.28750	WPED559	M		OCCP TAC	Omaha Coalition of Citizen Patrols Talk-Around	FMN	Security

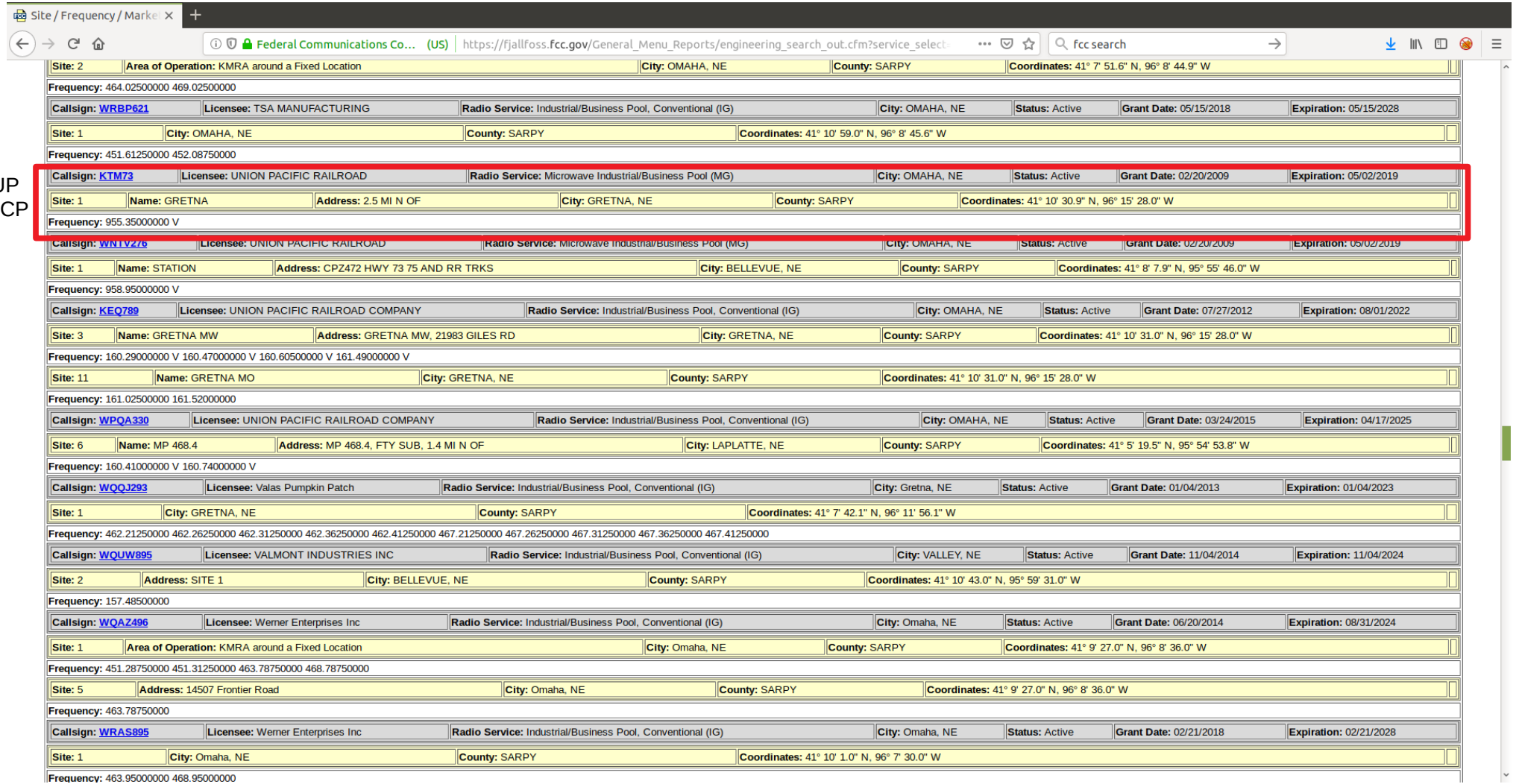
FCC General Menu License Search By Site/Frequency

https://www.fcc.gov/licensing-databases/search-fcc-databases




Site / Market / Frequenc
Federal Communications Co... (US)
https://fjallfoss.fcc.gov/General_Menu_Reports/engineering_search.cfm?service_select=%2
fcc search
FCC Federal Communications Commission
Search | RSS | Updates | E-Filing | Initiatives | Consumers | Find People
REBOOT.FCC.GOV BETA
Site / Market / Frequency Query
Table Of Contents
Site / Markey / Frequency Query
Site / Market / Frequency Query Entry
Search Criteria
Values
Service Selection:
All Services
State:
NE
County:
SARPY
Frequency Specification (Leave End Frequency blank for single frequency search)
Frequency:
Begin: 27
KHz MHz GHz
End: 999
KHz MHz GHz
Location Search Method
Point Point Radius Box Search
Location Specification:
Begin Coordinates
Latitude
N S
Longitude
W E
Licensee Name:
Wildcard Search:
Grant Date:
From:
To:
Entering only a "From" value will search on licenses granted prior to the date.
Expiration Date:
From:
To:
If only a "From" date is entered the system will only retrieve records which expire after the date.
The date format is mm/dd/yyyy
Query Options:
Sort Results
Callsign
File Number
Name
Limit Results to:
No Limitations (may include expired licenses and cancelled applications)
Currently Licensed Facilities
Pending Facilities
Currently Licensed Facilities and Pending Facilities
Data Export:
Format output for raw data export.
Submit Query
Clear Parameters

Sarpy County Results



Site / Frequency / Marke

Federal Communications Co... (US) https://fjallfoss.fcc.gov/General_Menu_Reports/engineering_search_out.cfm?service_select

fcc search

Site: 2 **Area of Operation:** KMRA around a Fixed Location **City:** OMAHA, NE **County:** SARPY **Coordinates:** 41° 7' 51.6" N, 96° 8' 44.9" W

Frequency: 464.02500000 469.02500000

Callsign: WRBP621 **Licensee:** TSA MANUFACTURING **Radio Service:** Industrial/Business Pool, Conventional (IG) **City:** OMAHA, NE **Status:** Active **Grant Date:** 05/15/2018 **Expiration:** 05/15/2028

Site: 1 **City:** OMAHA, NE **County:** SARPY **Coordinates:** 41° 10' 59.0" N, 96° 8' 45.6" W

Frequency: 451.61250000 452.08750000

UP BCP

Callsign: KTM73 **Licensee:** UNION PACIFIC RAILROAD **Radio Service:** Microwave Industrial/Business Pool (MG) **City:** OMAHA, NE **Status:** Active **Grant Date:** 02/20/2009 **Expiration:** 05/02/2019

Site: 1 **Name:** GRETNA **Address:** 2.5 MI N OF **City:** GRETNA, NE **County:** SARPY **Coordinates:** 41° 10' 30.9" N, 96° 15' 28.0" W

Frequency: 955.35000000 V

Callsign: WNTV276 **Licensee:** UNION PACIFIC RAILROAD **Radio Service:** Microwave Industrial/Business Pool (MG) **City:** OMAHA, NE **Status:** Active **Grant Date:** 02/20/2009 **Expiration:** 05/02/2019

Site: 1 **Name:** STATION **Address:** CPZ472 HWY 73 75 AND RR TRKS **City:** BELLEVUE, NE **County:** SARPY **Coordinates:** 41° 8' 7.9" N, 95° 55' 46.0" W

Frequency: 958.95000000 V

Callsign: KEQ789 **Licensee:** UNION PACIFIC RAILROAD COMPANY **Radio Service:** Industrial/Business Pool, Conventional (IG) **City:** OMAHA, NE **Status:** Active **Grant Date:** 07/27/2012 **Expiration:** 08/01/2022

Site: 3 **Name:** GRETNA MW **Address:** GRETNA MW, 21983 GILES RD **City:** GRETNA, NE **County:** SARPY **Coordinates:** 41° 10' 31.0" N, 96° 15' 28.0" W

Frequency: 160.29000000 V 160.47000000 V 160.60500000 V 161.49000000 V

Site: 11 **Name:** GRETNA MO **City:** GRETNA, NE **County:** SARPY **Coordinates:** 41° 10' 31.0" N, 96° 15' 28.0" W

Frequency: 161.02500000 161.52000000

Callsign: WPQA330 **Licensee:** UNION PACIFIC RAILROAD COMPANY **Radio Service:** Industrial/Business Pool, Conventional (IG) **City:** OMAHA, NE **Status:** Active **Grant Date:** 03/24/2015 **Expiration:** 04/17/2025

Site: 6 **Name:** MP 468.4 **Address:** MP 468.4, FTY SUB, 1.4 MI N OF **City:** LAPLATTE, NE **County:** SARPY **Coordinates:** 41° 5' 19.5" N, 95° 54' 53.8" W

Frequency: 160.41000000 V 160.74000000 V

Callsign: WQQJ293 **Licensee:** Valas Pumpkin Patch **Radio Service:** Industrial/Business Pool, Conventional (IG) **City:** Gretna, NE **Status:** Active **Grant Date:** 01/04/2013 **Expiration:** 01/04/2023

Site: 1 **City:** GRETNA, NE **County:** SARPY **Coordinates:** 41° 7' 42.1" N, 96° 11' 56.1" W

Frequency: 462.21250000 462.26250000 462.31250000 462.36250000 462.41250000 467.21250000 467.26250000 467.31250000 467.36250000 467.41250000

Callsign: WQUW895 **Licensee:** VALMONT INDUSTRIES INC **Radio Service:** Industrial/Business Pool, Conventional (IG) **City:** VALLEY, NE **Status:** Active **Grant Date:** 11/04/2014 **Expiration:** 11/04/2024

Site: 2 **Address:** SITE 1 **City:** BELLEVUE, NE **County:** SARPY **Coordinates:** 41° 10' 43.0" N, 95° 59' 31.0" W

Frequency: 157.48500000

Callsign: WQAZ496 **Licensee:** Werner Enterprises Inc **Radio Service:** Industrial/Business Pool, Conventional (IG) **City:** Omaha, NE **Status:** Active **Grant Date:** 06/20/2014 **Expiration:** 08/31/2024

Site: 1 **Area of Operation:** KMRA around a Fixed Location **City:** Omaha, NE **County:** SARPY **Coordinates:** 41° 9' 27.0" N, 96° 8' 36.0" W

Frequency: 451.28750000 451.31250000 463.78750000 468.78750000

Site: 5 **Address:** 14507 Frontier Road **City:** Omaha, NE **County:** SARPY **Coordinates:** 41° 9' 27.0" N, 96° 8' 36.0" W

Frequency: 463.78750000

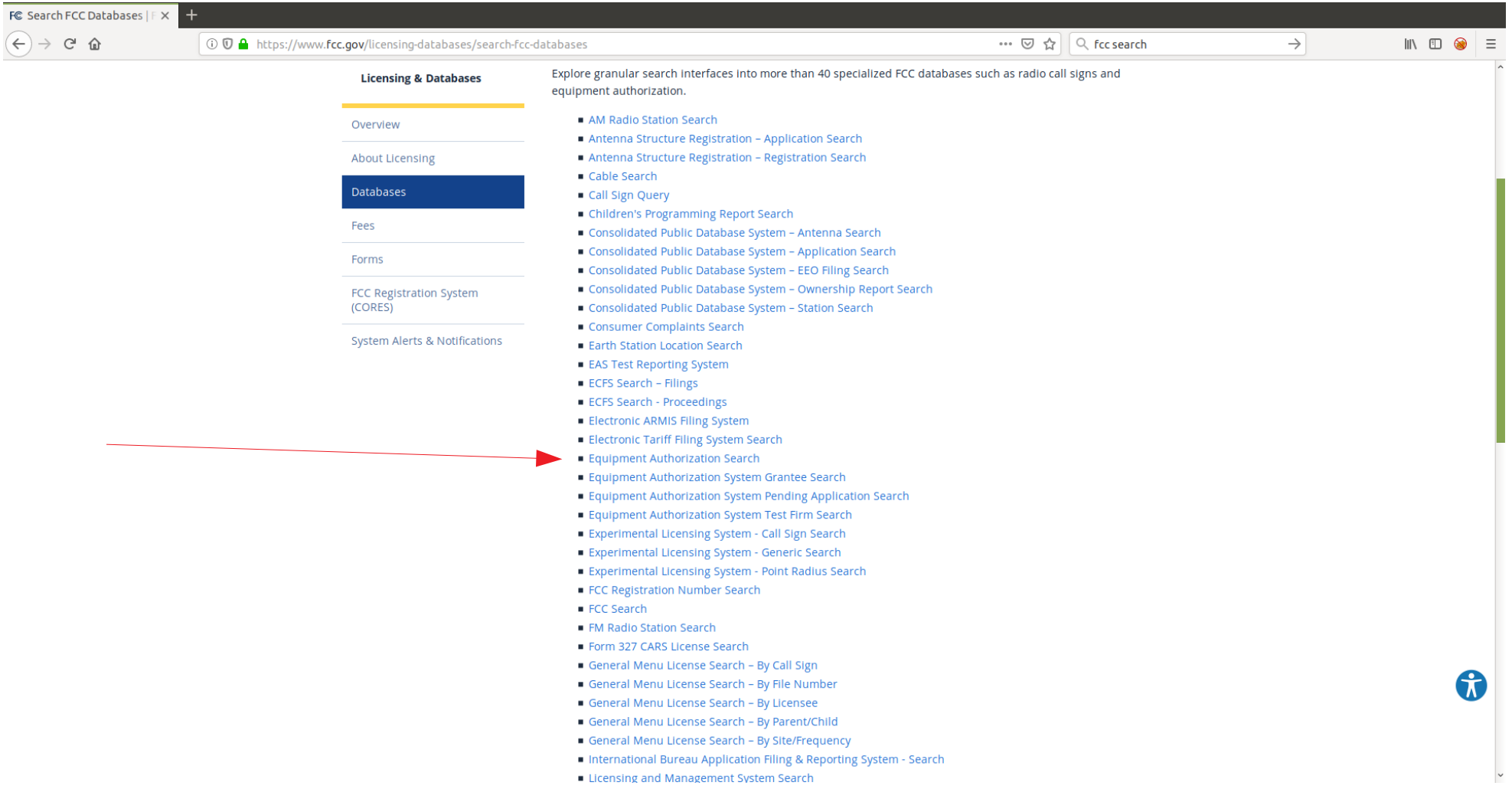
Callsign: WRAS895 **Licensee:** Werner Enterprises Inc **Radio Service:** Industrial/Business Pool, Conventional (IG) **City:** Omaha, NE **Status:** Active **Grant Date:** 02/21/2018 **Expiration:** 02/21/2028

Site: 1 **City:** Omaha, NE **County:** SARPY **Coordinates:** 41° 10' 1.0" N, 96° 7' 30.0" W

Frequency: 463.95000000 468.95000000

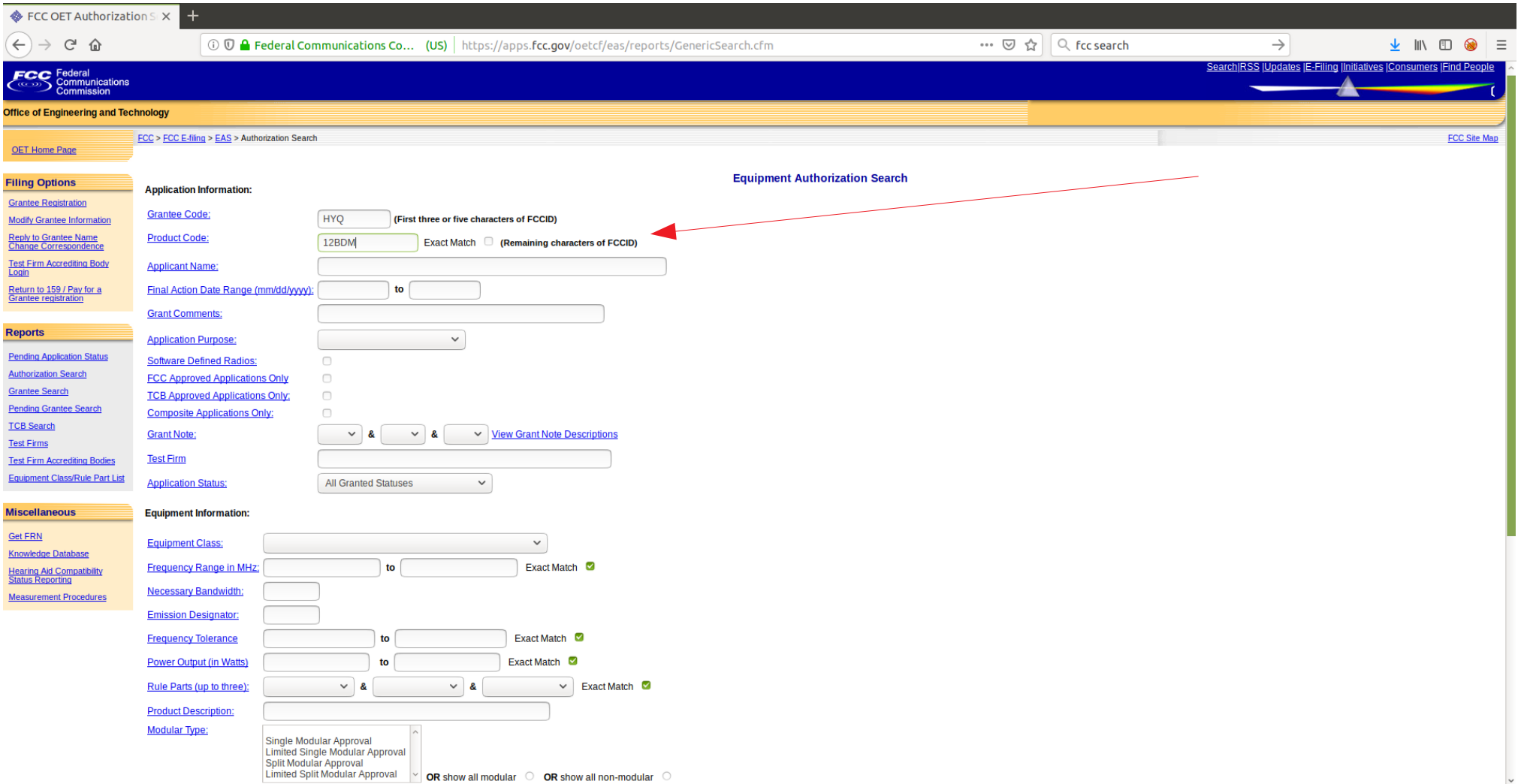
FCC ID Search

FCC ID Search



FCC ID Search

Equipment Authorization Search

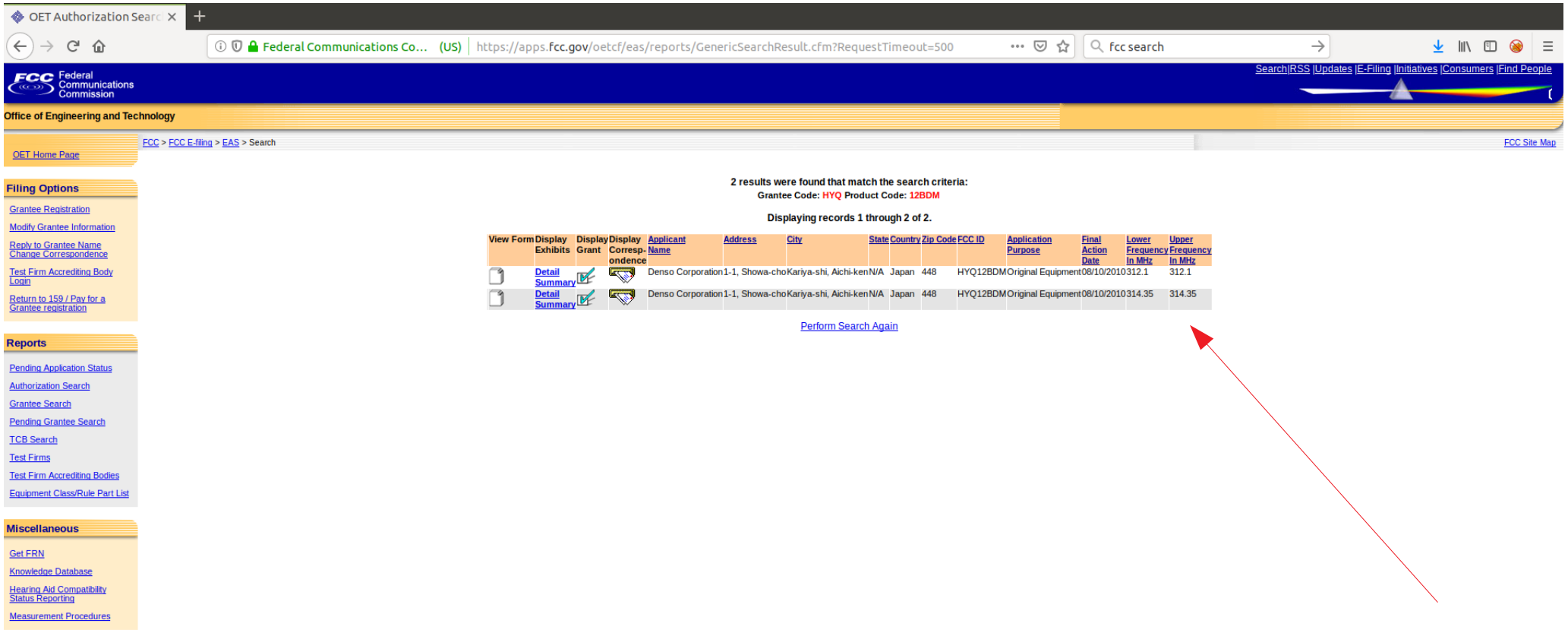


FCC ID Search (Alt)

https://www.fcc.gov/oet/ea/fccid

FCC ID Search

Equipment Authorization Search



Sometimes Find FCC ID Online
e.g. Alarm Systems

SimpliSafe

RTL-SDR.COM

RTL-SDR (RTL2832U) and software defined radio news and projects. Also featuring Airspy, HackRF, FCD, SDRplay a

HOME | ABOUT RTL-SDR | QUICK START GUIDE | FEATURED ARTICLES | SOFTWARE | SIGNAL ID WIKI | FORUM | RTL-SDR

MARCH 7, 2016

HACKING ALARM SYSTEMS WITH AN RTL-SDR AND RFCAT

Back in 2014 the author of boredhackerblog.blogspot.com did a final year project for his wireless security class on hacking home alarm systems. His presentation was titled "How we broke into your house". In his research the author used both an RTL-SDR and a simple RFcat wireless transmitter and performs a simple replay attack on a cheap $50 alarm system. His process for reverse engineering the alarm was essentially:

1. Look up the device frequency and listen to it with an RTL-SDR and SDR#.
2. Record the signal and visually study the waveform in Audacity.
3. Look up system part info and determine encoding type (e.g. ASK/OOK)
4. Determine the bit string and baud rate.
5. Program the RFcat to send the same disarm binary string.

Once again research like this shows that cheap home alarm systems have literally zero protections against wireless attacks. In a previous post we also showed how the popular Simplisafe wireless alarm system could be disarmed in a somewhat similar way.

DMP

Discovered the panel model from a google image search: “alarm panels”

SEi Omaha uses DMP

Security through Obscurity? Try ebay!

ebay Shop by category | Search for anything | All Categories | Search | Advanced

eBay › Business & Industrial › Facility Maintenance & Safety › Surveillance & Alarm Equipment › Alarm Systems & Accessories › Alarm Control Panels & Keypads | Share

DMP 7060n-w Thinline Series LCD Keypad NBR Keys No Zones White

Be the first to write a review | About this product

Brand new $49.62 | Make an offer: new (other)

Make an offer: new (other) ⓘ

$63.00

+ $8.20 Shipping

ebay MONEY BACK GUARANTEE

Buy It Now

Add to cart

or Best Offer

Make Offer

Watch

Get it by **Thursday, Mar 28** from San Marcos, California

- **New other (see details)** condition
- No returns, but backed by eBay Money back guarantee

"This item is unused, in factory packaging. Please view the photos."

See details

See all 2 best offer listings

Sold by electronicsrecyclersassociation (846)

98.9% Positive feedback

Contact seller

Finding Alarm System Frequencies

Googling the model number + “FCC ID”

DMP.COM @DMPALARMS

XT SERIES PANELS

XT30 and XT50 Panels

FEATURES

- Now with LTE
- Choose your preferred configuration for communications: network, dialer, cell, or Wi-Fi
- The XT30 has the capacity to expand up to 32 zones that can be a combination
- Variety of traditional metal enclosures available
- All/Perimeter, Home/Sleep/Away or up to six area systems
- 30 (XT30) / 99 (XT50) four-digit user codes with authority levels
- Door Access can be added with the 734 Wiegand module or DMP Thinline™ keypad with built-in proximity reader and relay
- Codeless arming/disarming with proximity reader
- Arm Only, Ambush Code, and Temporary User Code
- Built-in English text programming from any keypad
- Open/Close schedules with Closing Check
- Attrition Detection™ monitors system for arming activity

INTRUSION PANELS

COMPATIBILITY REFERENCE SHEET

Keypads

7000	Series Thinline Keypads
7000A	Series Aqualite Keypads
7300	Series Icon Keypads
7800	Touchscreen Keypads
9000	Wireless Keypads
9800	Wireless Touchscreen Keypads

Expansion Modules

708	Bus Extender
710	Bus Splitter/Repeater
711	Single Zone Expansion
712-8	8-zone Expansion
714	4-zone Class B Expansion
714-8	8-zone Class B Expansion
714-16	16-zone Class B Expansion
715	4-zone 2-wire Smoke Expansion
715-8	8-zone 2-wire Smoke Expansion
715-16	16-zone 2-wire Smoke Expansion

Cellular

263H	HSPA+ Cellular Communicator (AT&T)
263HCAN	HSPA+ Cellular Communicator (AT&T) Canada
263LTE-V	LTE Verizon
263LTE-A	LTE AT&T (Coming Soon)
380-400	Replacement Level 400 SIM Card (AT&T)
381-12	12' SMA Coax Cable Extension
381-25	25' SMA Cable Extension
383	External Antenna
387-1	3dB Fiberglass Antenna
387-2	2dB Attack Enclosure Antenna
387-3	3dB MEG Antenna

Intrusion Devices

DMP is compatible with most standa

Monitoring center Receivers

SCS-1R Security Control Receiver
SCS-105 Single-Line DMP Serial 3 Receiver Compatible with Receivers that accept Standard CID, DMP Serial 3 or Network messaging

SCS-VR (Virtual Receiver) software—only solution that runs on a server for network IP and cellular communications

Dealer Management

Remote Link Programming software
Tech APP
Dealer Admin

DMP Wireless

1100D	Receiver
1100DI	In-line Receiver
1100DH	High-Power Receiver
1100R	Repeater
1101	Universal Transmitter, Internal and External Contacts
1102	Universal Transmitter, External Contact
1103	Universal Transmitter, Internal and External Contact
1106	Universal Transmitter, Internal and External Contact
1107	Micro Window Transmitter
1114	Four-zone Expander
1115	Wireless Temperature Sensor and Flood Detector
1116	Relay Output
1117	LED Annunciator
1119	Door Sounder
1121	Pet Immune PIR Motion Detector
1122	Wireless PIR
1126R	360 Ceiling Mount PIR
1127C	Wall Mount Curtain PIR
1142BC	Two-Button Belt Clip Hold-up Transmitter
1144-4	Four-Button Key Fob
1144-2P	Two-Button Key Fob
1144-1P	One-Button Key Fob
1144-D	Dual-Button Key Fob
1148	Personal Pendant
1154	Wireless Four-Zone Input Module
1158	Wireless 8-Zone Input Module
1164NS	Wireless Smoke Detector with No Sounder
1166	Wireless Smoke Ring
1183-135F	Heat Detector
1183-135R	Heat Detector
1184	Carbon Monoxide Detector

Other Wireless

738A	Ademco 32-point Expansion Module
738I	ITI 96-point Expansion Module
738Z+	Z-Wave Interface Module
738T	Wireless Translator

Accessories

300	Four-wire Harness
307	Clip-on Tamper Switch
307-S	Screw-on Tamper Switch
335	Intrusion Siren
370	Lightning Suppressor
399	Programming Harness
300-9800-4	Four-wire Replacement Harness
861	Power Distribution Module

End User Management

System Link™
VirtualKeypad.com
Virtual Keypad App

Download on the App Store | GET IT ON Google Play

System Specifications

Primary Power:
16.5 VAC, 40 VA transformer
(Model 321)

Secondary Power:
12 VDC Battery

Outputs:

Auxiliary	500 mA at 12 VDC
Alarm	1.5 Amps at 12 VDC
Smoke	100 mA at 12 VDC
Annunciator(4)	50 mA each (switched ground)

Enclosures:

Material	Cold-rolled steel
Model 340 (Gray)	12.5" W × 9.5" H × 2.75" D
Model 349 (Gray)	12.25" W × 11.75" H × 3.125" D
Model 349A (Gray Attack)	13.25" W × 11.3" H × 3.6" D

Ordering information

Listings and Approvals

California State Fire Marshal (CSFM)
ETL:

ANSI/SIA CP-01-2010	False Alarm Reduction
ANSI/UL 1023	Household Burglar
ANSI/UL 985	Household Fire Warning
ANSI/UL 1635	Digital Burglar
ANSI/UL 1610	Central Station Burglar

FCC Part 15 ID: CCKPC0096
FCC Part 68 Registration ID CCKAL00BXT50
Industry Canada ID: 5131A-PC0096

Refer to the XT Series Installation Guide, Programming Guide and specific compli... ...ings for installation and programming requirements necessary to meet a particular approval.

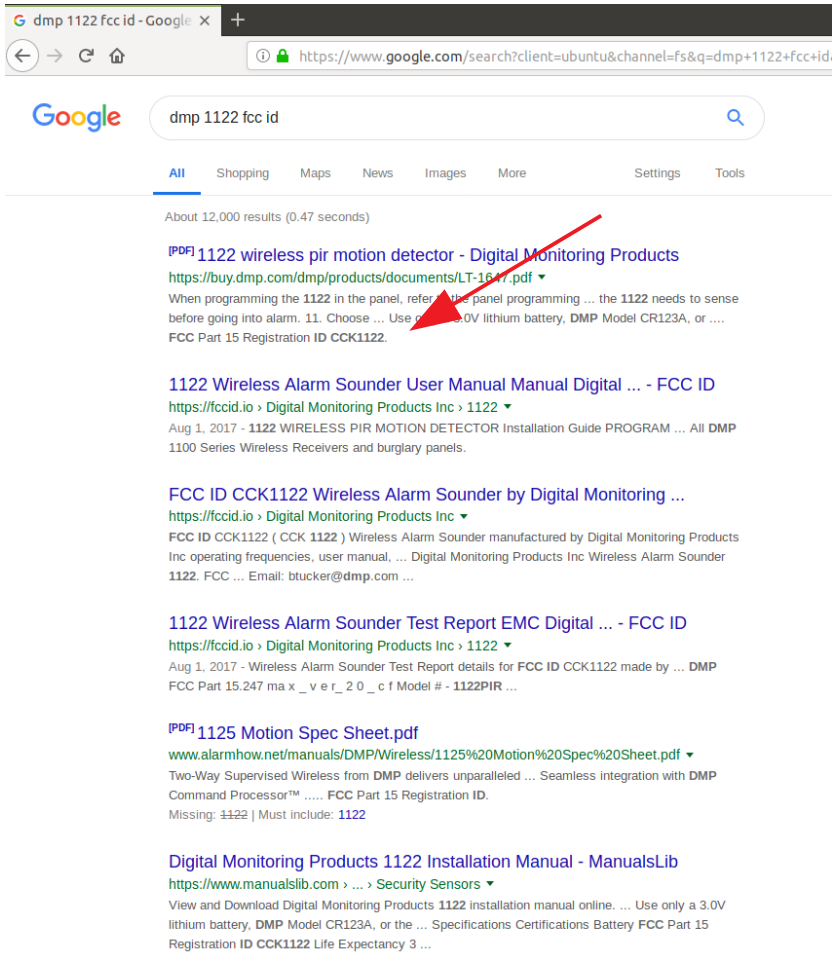
For additional information,

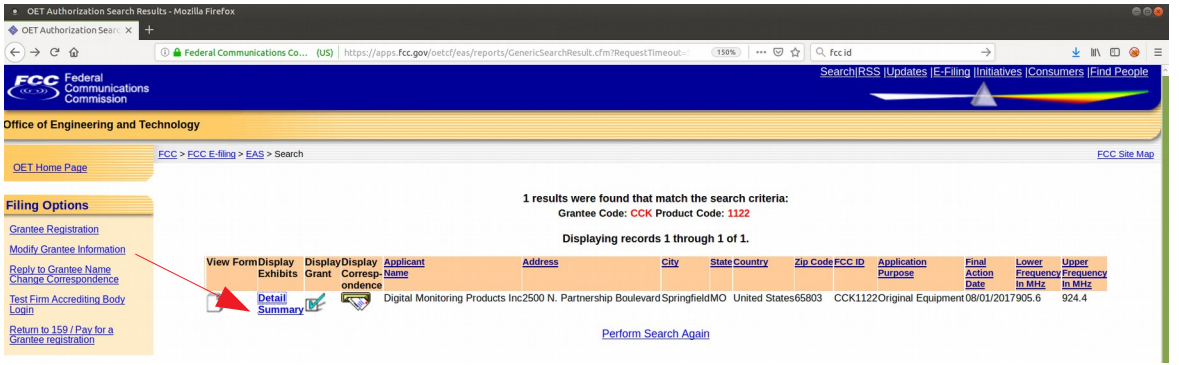
Searching the wireless accessories should give better results
DMP 1122 Wireless PIR FCC ID

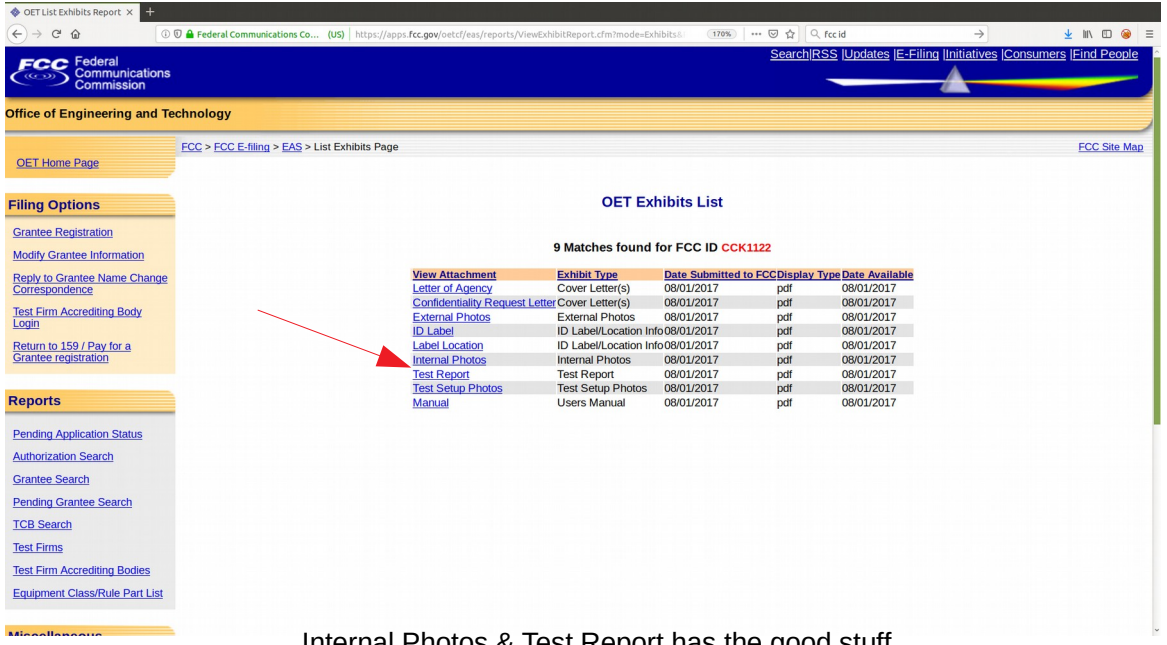
FCC ID for the RFID option.
Not interested in that

DPM Wireless PIR frequency

Alarm System Recon



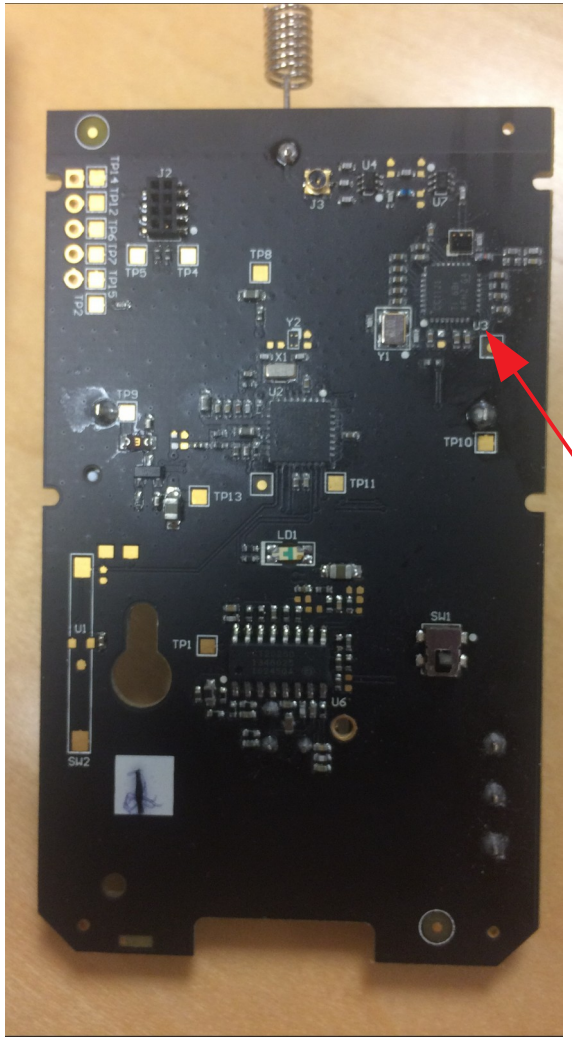




Internal Photos & Test Report has the good stuff

DMP 1122 Wireless PIR
Alarm System Recon

Internal Photos



Uses 900MHz Frequency Hopping

TI CC1121

Start Reverse Engineering With This Information

Frequency Hopping is complicated, but do-able,
Usually requires acquiring hardware through ebay

https://sandeen.net/wordpress/energy/neptune-rf-water-meter-frequency-hopping-pattern/

https://syssec.kaist.ac.kr/pub/2015/shin_wisa2015.pdf

http://thiébaud.fr/phy_xbee_p1.html

Test Report Info

3.2 Hopping channel carrier frequencies separation

Frequency Range:	☒ 902-928MHz	☐ 2400-2483.5MHz	☐ 5725-5850MHz
Measured Separation (kHz)	**Limit (kHz)**		**Result**
362.18	74.1		**Pass**
Limit:	☒ 25kHz ☐ 20dB channel bandwidth ☐ 2/3 of 20dB channel bandwidth		
Span:	1 MHz		
RBW:	☐ 3kHz ☒ 10kHz ☐ 100kHz ☐ other kHz		
VBW:	☐ 3kHz ☒ 30kHz ☐ 100kHz ☐ other kHz		

3.4 Number of hopping frequencies

Frequency Range:	☒ 902-928MHz	☐ 2400-2483.5MHz	☐ 5725-5850MHz
Measured Number	**Requirements**		**Result**
53	50		**Pass**
Channel 20dB Bandwidth:	☒ <250kHz ☐ ≥250kHz		

3.5 Average time of occupancy of hopping frequency

Frequency Range:	☒ 902-928MHz	☐ 2400-2483.5MHz	☐ 5725-5850MHz
Measured / Calculated Time sec	**Period sec**	**Limit sec**	**Result**
0.3	20	0.4	**Pass**
Period:	☐ 10s ☒ 20s ☐ 30s ☒ 0.4s multiplied by the channel number		
Channel 20dB Bandwidth:	☒ <250kHz ☐ ≥250kHz		

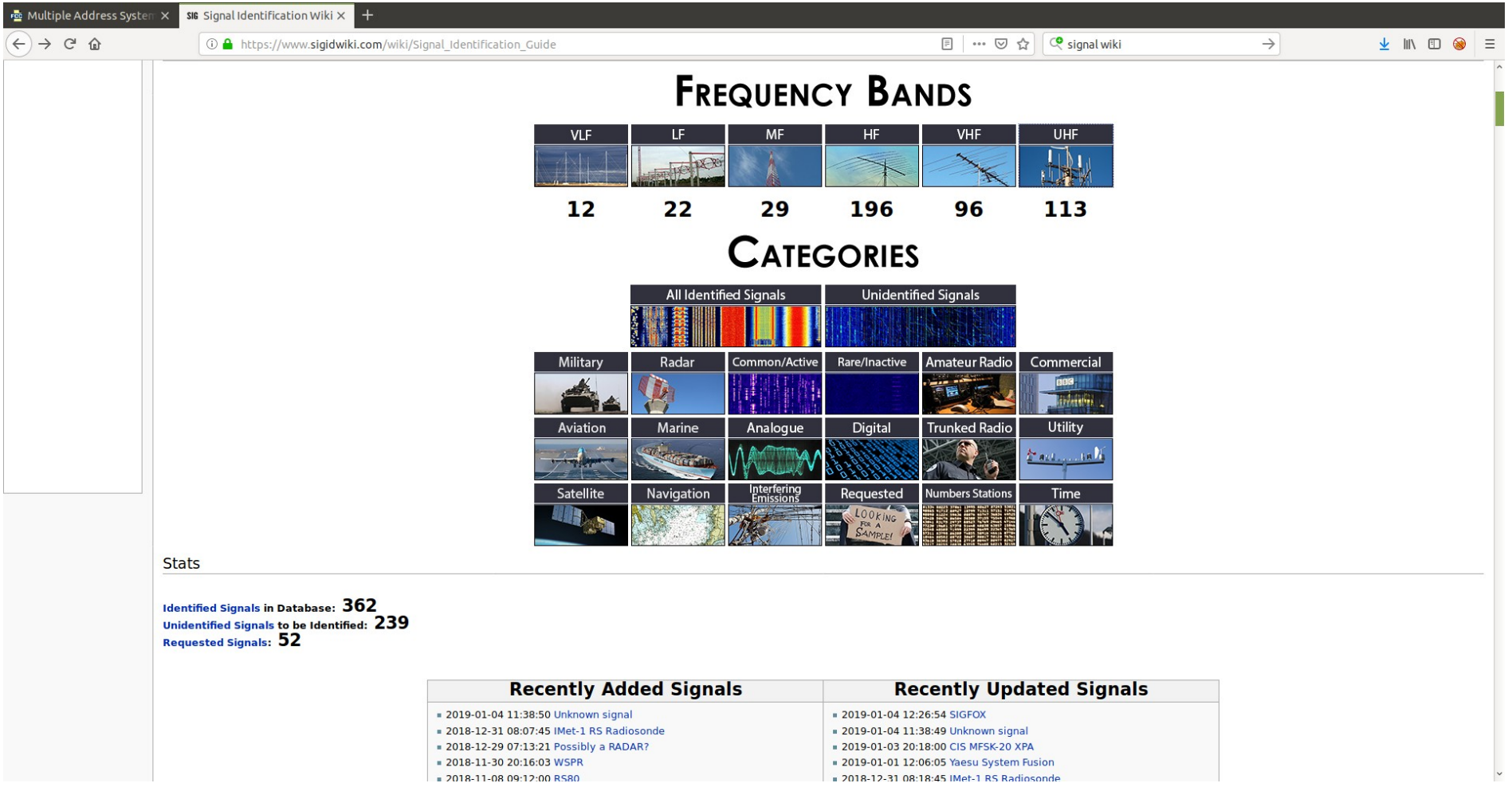
Pseudorandom hopping sequence
The system uses 61 hop channels. They are evenly spaced between 902.9729 MHz and

927.0271 MHz. They are listed, in order, below:

0	903.3257	18	911.4079	36	919.4901
1	903.7747	19	911.8569	37	919.9391
2	904.2237	20	912.3059	38	920.3881
3	904.6727	21	912.7549	39	920.8372
4	905.1217	22	913.2040	40	921.2862
5	905.5707	23	913.6530	41	921.7352
6	906.0198	24	914.1020	42	922.1842
7	906.4688	25	914.5510	43	922.6332
8	906.9178	26	915.0000	44	923.0822
9	907.3668	27	915.4490	45	923.5312
10	907.8158	28	915.8980	46	923.9802
11	908.2648	29	916.3470	47	924.4293
12	908.7138	30	916.7960	48	924.8783
13	909.1628	31	917.2451	49	925.3273
14	909.6119	32	917.6941	50	925.7763
15	910.0609	33	918.1431	51	926.2253
16	910.5099	34	918.5921	52	926.6743
17	910.9589	35	919.0411		

Signals Everywhere

Signal Identification Guide Database

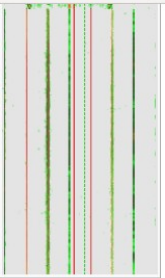
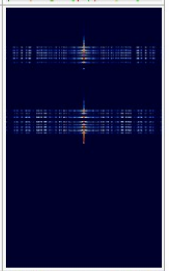
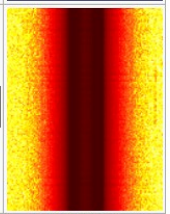
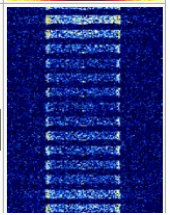


Signal ID Wiki

Multiple Address Syste | Utility Signals - Signal Ide

https://www.sigidwiki.com/wiki/Category:Utility

signal wiki

Supervisory Control And Data Acquisition (SCADA)	Supervisory Control And Data Acquisition (SCADA) is a control system architecture that is used in industrial applications for computerized automated systems. Wireless telemetry is used on RTU's to send data to control units for operators to utilize.	413 MHz — 950 MHz	FM	FSK	12 kHz		0:00 / 0:09	
Tire Pressure Monitoring System (TPMS)	TPMS (Tire-Pressure Monitoring System), more specifically Direct TPMS (dTPMS), is a system that uses pressure sensors to monitor tire pressure on vehicles.	315 MHz — 434 MHz	AM	FSK	100 kHz	Worldwide	0:00 / 0:00	
Toyota Car Key	Wireless entry rolling code car key.	315 MHz — 433 MHz	AM		40 kHz	Worldwide	0:00 / 0:00	
Vaisala RS41-SG Weather Balloon (Radiosonde)	Weather balloon (radiosonde) telemetry data.	400 MHz — 410 MHz	NFM	GFSK	4.8 kHz	Worldwide	0:00 / 0:00	

Signal ID Wiki

Compulert System

ASC Tempest T-128 (CSC-960)

Omaha Tornado Sirens

SIGIDWIKI.COM
SIGNAL IDENTIFICATION GUIDE

navigation
- Home Page
- All Identified Signals
- Unidentified Signals
- Recent changes
- Random page
- Add a Signal Entry
- RTL-SDR Blog
- Artemis 2

search
Search
Go Search

tools
- What links here
- Related changes
- Special pages
- Printable version
- Permanent link
- Page information
- Browse properties

page | discussion | edit with form | edit | history

CompuLert

Low speed FSK telemetry to monitor and control warning sirens that are used to warn the public of threats such as tsunamis, severe weather, chemical spills and civil emergencies.

Compulert was developed by Alerting Communicators of America (ACA), now named American Signal Corporation (ASC). It is a SCADA-based proprietary FSK protocol used to manage and monitor warning sirens in an area.

Contents [hide]
1 Samples
2 Video Examples
3 Additional Links
4 Additional Images

Samples [edit]

Sample 1: Compulert Telemetry

0:00 / 0:00

Sample 2: compulert(prob.) on public safety line

0:00 / 0:00

Video Examples [edit]

- Siren test (Compulert signals can be heard as siren activates)
- Colerain, OH sirens

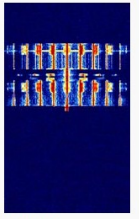
Additional Links [edit]

- KB9UKD Digital Modes
- Americal Signal Corporation, CompuLert System
- Wikipedia: American Signal Corporation (ASC)

Additional Images [edit]

Categories: Signal | Digital | UHF | Active | Utility

CompuLert



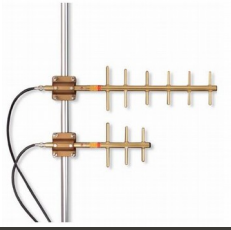
Frequencies	453.375 MHz
Frequency Range	453.375 MHz - 453.375 MHz
Mode	NFM
Modulation	FSK
ACF	—
Bandwidth	5 kHz
Location	Worldwide
Short Description	Low speed FSK telemetry to monitor and control warning sirens that are used to warn the public of threats such as tsunamis, severe weather, chemical spills and civil emergencies.
I/Q Raw Recording	—
Audio Sample	0:00 / 0:00

Siren Jack: https://www.sirenjack.com/ (ATI Systems)

Utility Antennas Everywhere

MAS (Multiple Address Service) SCADA

https://shmoo.gitbook.io/2016-shmoocon-proceedings/build_it/10_reverse-engineering-wireless-scada-systems



~900MHz Yagi

Utility Antennas Everywhere

Water Utility. SCADA yagi

Usually proprietary protocol

Sarpy County Appendix - 6_Sarpy-County-Appendix(reduced).pdf - Mozilla Firefox

https://jeo.com/sites/default/files/inline-files/6_Sarpy-County-Appendix(reduced).pdf

81 of 178 — Automatic Zoom

MITIGATION STRATEGY

Completed Mitigation Actions

Description	SCADA System for Water/Wastewater System
Analysis	Centralized computer control system which monitors and controls critical utilities/infrastructure components
Goal/Objective	Goal 3/Objective 3.6
Hazard(s) Addressed	All
Location	Eight Locations, Lift Station at 186th Street (South of Hwy 370)
Funding	General Fund (Sewer)
Year Completed	2010

615 E Sixth St - Google Maps

https://www.google.com/maps/@41.1617242,-96.0331145,3a,19.4y,37.03h,91.22t/data=!3m6!1e1!3m4!1sOD0Z9fnHYs5GcTXKTTQwuQ!

rtl-sdr library

615 E Sixth St
Papillion, Nebraska
Google
Street View - Jul 2018

Google

Image capture: Jul 2018 © 2019 Google United States Terms Report a problem

Google Search: Sarpy scada

Search government invoices, assessments, proposals, etc. for vendor & equipment info

Telemetry Antennas

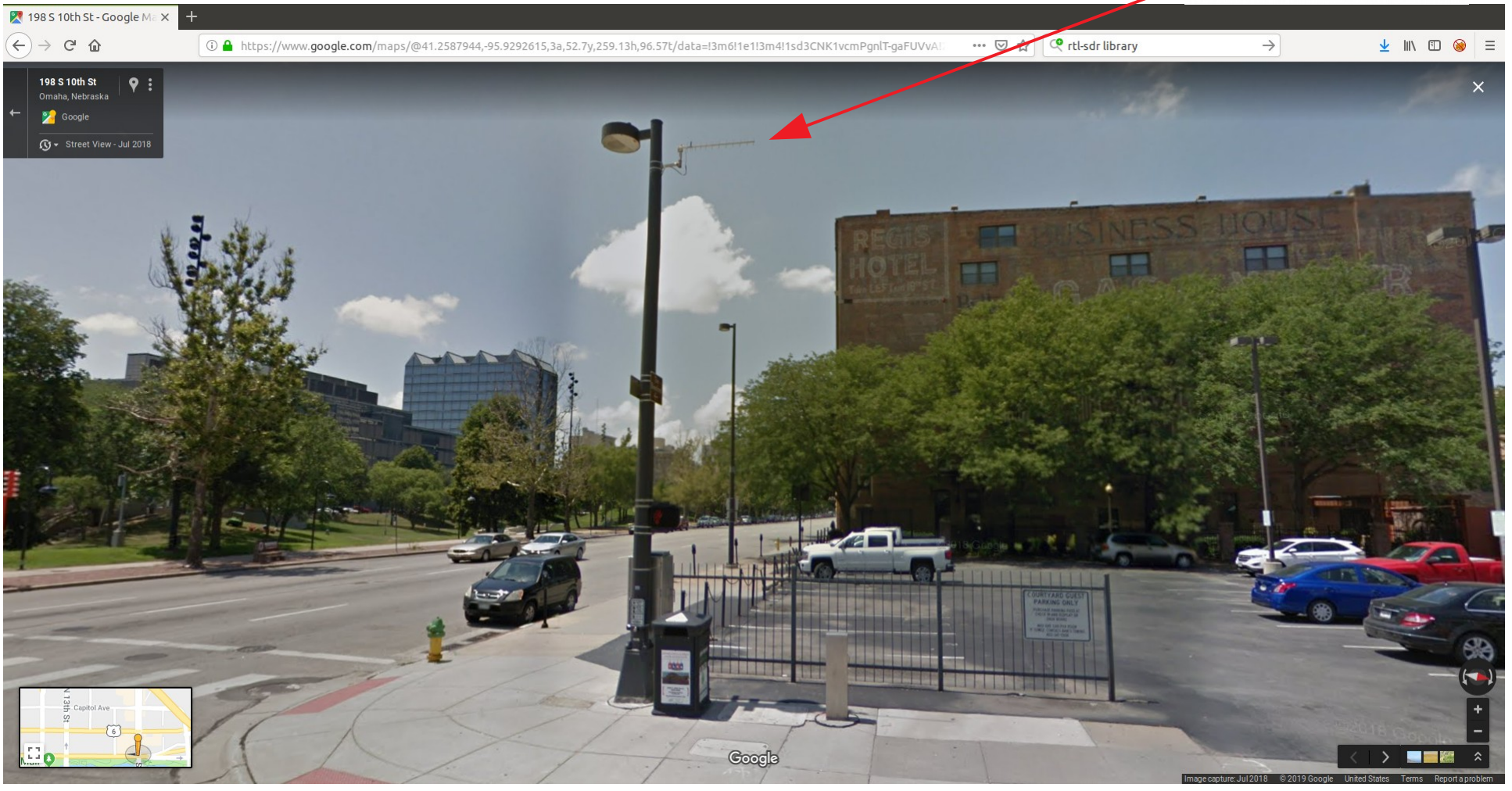
USGS Streamgage

GOES15 Weather Satellite Uplink 401.8MHz

Omaha Traffic Lights

Encom Serial Modem (Model 5200)
~900MHZ Frequency Hopping
Centracs Advanced Traffic Management System
and Wapiti Traffic View Software

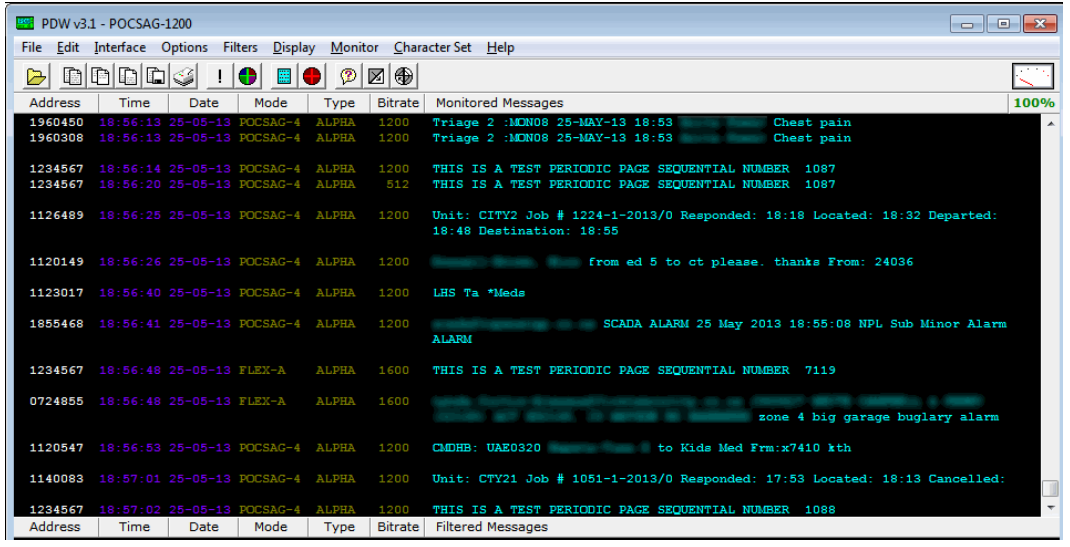
Buy on ebay



Pager Interception

SCADA & Hospital networks still use

POCSAG & FLEX protocol ~900-930MHZ



PDW software for Windows

https://www.discriminator.nl/pdw/index-en.html

https://www.rtl-sdr.com/rtl-sdr-tutorial-pocsag-pager-decoding/

```
audio  sox -t wav be-pager-pocsec.wav -esigned-integer -b16 -r 22050 -t raw - | multimon-ng
-a POCSAG512 -a POCSAG1200 -a POCSAG2400 -
multimon-ng  (C) 1996/1997 by Tom Sailer HB9JNX/AE4WA
             (C) 2012-2014 by Elias Oenal
available demodulators: POCSAG512 POCSAG1200 POCSAG2400 EAS UFSK1200 CLIPFSK FMSFSK AFSK1200 AF
SK2400 AFSK2400_2 AFSK2400_3 HAPN4800 FSK9600 DTMF ZVEI1 ZVEI2 ZVEI3 DZVEI PZVEI EEA EIA CCIR M
ORSE_CW DUMPCSV
Enabled demodulators: POCSAG512 POCSAG1200 POCSAG2400
POCSAG1200: Address: 1876594  Function: 1
POCSAG1200: Address: 1483379  Function: 1
POCSAG1200: Address: 1309718  Function: 0  Numeric: 1 6.0U.  0.3785401.4663.5 2603.5.00
POCSAG1200: Address: 1309718  Function: 0  Alpha:   AMBULANCE (Z641104)<NUL>
POCSAG1200: Address: 1309718  Function: 0  Skyper:  @LATK@MBD<US>'15300/3(?
POCSAG1200: Address: 2010229  Function: 1
POCSAG1200: Address: 1712758  Function: 1
POCSAG1200: Address:  401702  Function: 2  Numeric: 663.5 2603.5.00
POCSAG1200: Address: 1089601  Function: 3
POCSAG1200: Address:  177721  Function: 0  Numeric: .-U28061309]04.-4797-567[-3 7]2UU10
POCSAG1200: Address:  177721  Function: 0  Alpha:   ZW 01 : Ziekenwagen<NUL>
POCSAG1200: Address:  177721  Function: 0  Skyper:  YV<US>/0<US>9<US>Yhdjdmv`fdm?
POCSAG1200: Address: 2044535  Function: 0
```

Multimon-ng for Linux

https://github.com/EliasOenal/multimon-ng

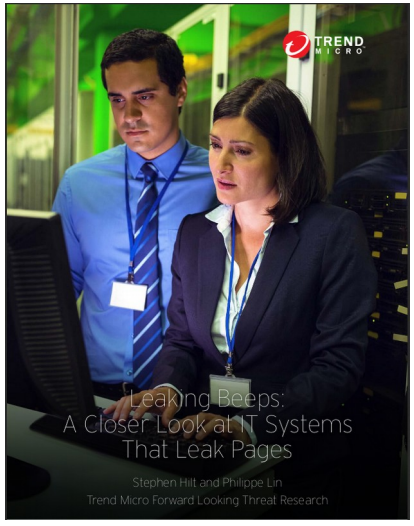
https://tools.kali.org/wireless-attacks/multimon-ng

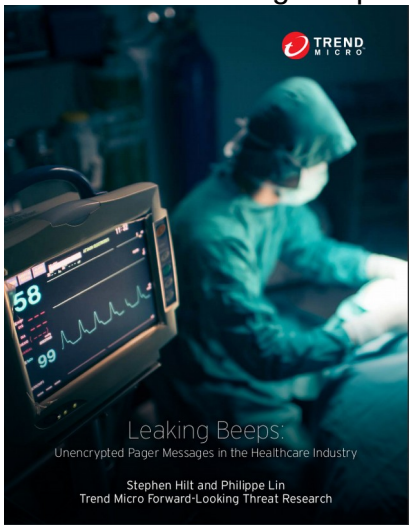
https://www.bastibl.net/pocsag/

https://www.rtl-sdr.com/pagermon-a-browser-based-app-for-displaying-pager-messages-from-multimon-ng/

Pager Interception

Leaking Beeps White Papers





Spoofing Pages

Lots of information can be seen from sniffing pager messages. However, it is also possible to inject your own pages if you have basic information about the systems in use. Without encryption and authentication, pager messages are easy to spoof as there is no way to verify that the messages are sent from trusted and known sources.

To test these theories, we bought some pagers to simulate the sending of pager messages. The goal was to send pages that were created by the researchers and prove that valid pagers would receive crafted messages from SDR. The simulation was done in a secure environment so it would not affect any existing pager systems.

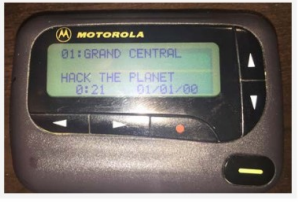


Figure 3. Test pager receiving test messages

Protected Health Information

The table below shows statistics of protected health information (PHI) or sensitive information that were observed during the span of the research:

Email	805,609	28%
Medical terms	647,745	23%
English names	510,313	18%
Syndromes / Diagnosis	399,862	14%
Medicine on FDA drug list	164,117	6%
Phone numbers	124,949	4%
Date of birth, age, gender	110,708	4%
Medical reference number	90,124	3%
URL	6,371	0%

Table 1: Distribution of PHI seen during the span of the research

https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp_leaking-beeps-industrial.pdf

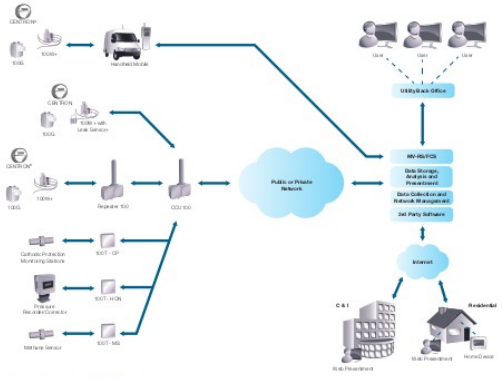
https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-leaking-beeps-healthcare.pdf

https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-leaking-beeps-a-closer-look-at-it-systems-that-leak-pages.pdf

Utility Meters

OPPD uses Itron ChoiceConnect

~900MHz ISM Band



ChoiceConnect 100 Architecture

100W+ Water Endpoint

100G DLN ERT Module

CENTRON C1SR Electricity Meter

CCU 100

HOW

ChoiceConnect offers energy and water utilities a wide array of operational, customer service and asset management benefits because of the advanced capabilities provided by its suite of products.

Endpoints

The power of ChoiceConnect starts with electricity, gas and water endpoints, such as the HP CENTRON, 100G and 100W+. These are coupled with the enhanced data collection systems that utilize Itron's proven ERT technology to communicate data to the utility. Our radio-based 900 MHz endpoints for electric, gas and water utilities are offered with different power levels and communication options to meet specific deployment requirements. The 100G and 100W+ also feature optional enhanced security with the addition of authentication and encryption. Accurate and cost-effective, ChoiceConnect endpoints offer proven reliability with an unmatched 20 year battery life and are rugged enough to withstand even the harshest environments. ChoiceConnect endpoints are easy to install and compatible with all leading water and gas meter manufacturers.

Leveraging our communication technologies, we extend the value of data collection out into utilities' distribution systems, integrating with acoustic sensors for proactive leak detection. Our 100T series for gas utilities remotely monitors for line pressure and temperature, cathodic protection and methane leaks for preemptive maintenance and enhanced safety. Our Leak Sensor+ for water utilities acoustically monitors for leaks, protecting water revenue and catching small leaks before they become costly mains breaks.

Fixed Network Collector CCU 100

The CCU 100 (also known as a collector) is the main collection point for the ChoiceConnect Fixed Network and reads data from Itron electricity meters, gas and water endpoints. The CCU 100 gathers consumption, daily or hourly meter reads, and other information from endpoints and communicates it back to the utility over a public or private network. When used with the Fixed Network Repeater 100 the coverage territory per CCU 100 is extended. It also manages the collection, processing and storage of endpoint data and can support two-way functionality to the endpoint. Equipped with a backup battery, the CCU100's adaptable design allows for a wide range of installation options, utilizing either AC, DC or solar power.

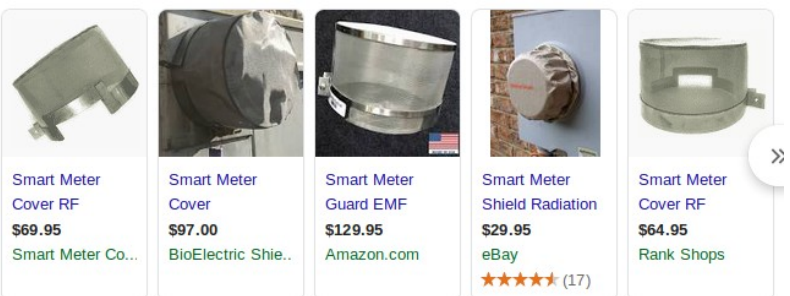
Easily decoded with RTLAMR on Linux

https://github.com/bemasher/rtlamr

https://www.rtl-sdr.com/rtlamr-rtl-sdr-receiver-900mhz-ism-smart-meters/

https://www.mathworks.com/help/comm/examples/automatic-meter-reading.html

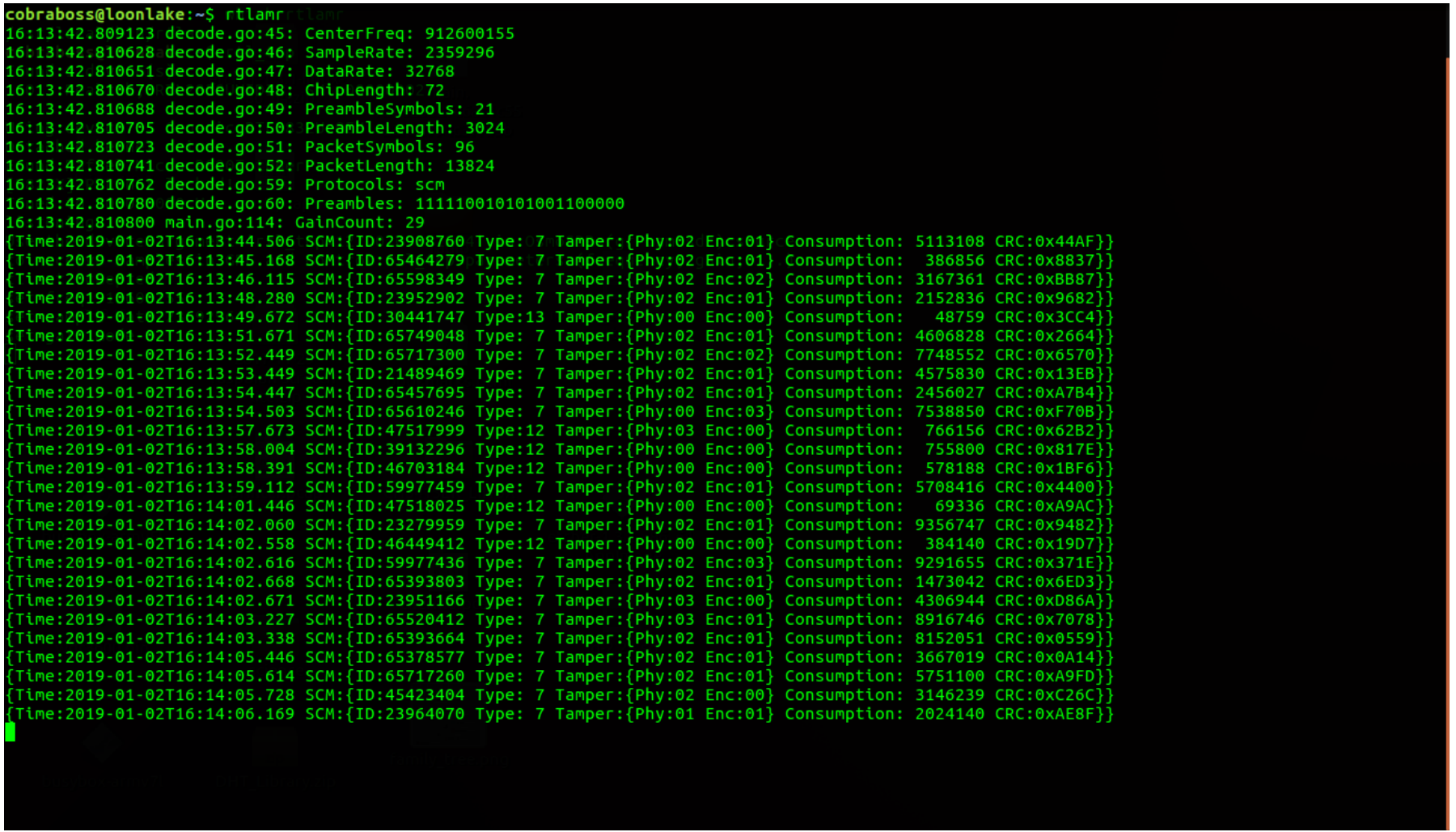
FCC ID: SK9C1A-3



Utility Meters

RTLAMR Screenshot

Smart (AMR) Meters



Wireless IDS & Tracking

RTLSDR-Scanner w/ GPS receiver

for RF direction finding (wardriving for radio)

https://github.com/EarToEarOak/RTLSDR-Scanner

https://wjmccann.github.io/blog/2018/04/06/Wardriving-433

https://www.rtl-sdr.com/updates-power-line-noise-detector-driveby-system/

Bug Detection & Proximity Alarms

Salamandra for Linux

https://github.com/eldraco/Salamandra

https://www.rtl-sdr.com/salamandra-detecting-and-locating-spy-microphones-with-an-rtl-sdr/

https://www.rtl-sdr.com/creating-an-rf-proximity-alarm-with-an-rtl-sdr/

Finding Spy Bugs with an RTL-SDR & Salamandra

```
Location Signal (the more, the closer)
DateTime (Amount of peaks) [Top Freq Detected MHz] Histogram
2018-01-15 18:33:28 (  2) [148.49]: ##
2018-01-15 18:33:34 (  2) [118.73]: ##
2018-01-15 18:33:34 (  2) [148.49]: ##
2018-01-15 18:33:39 (  1) [118.73]: #
2018-01-15 18:33:39 (  2) [148.49]: ##
2018-01-15 18:33:45 (  5) [118.77]: #####
2018-01-15 18:33:45 (  2) [148.49]: ##
2018-01-15 18:33:51 (  5) [118.79]: #####
2018-01-15 18:33:51 (  2) [148.49]: ##
2018-01-15 18:33:56 (  7) [118.78]: #######
2018-01-15 18:33:56 (  2) [148.49]: ##
2018-01-15 18:34:02 (  2) [148.49]: ##
2018-01-15 18:34:07 (  2) [148.49]: ##
2018-01-15 18:34:13 (  2) [148.49]: ##
2018-01-15 18:34:19 (  2) [148.49]: ##

Status: Detecting...    Threshold: 0.0      Sound: True    Min Freq: 100. Max
Freq: 200' to increase the threshold (less sensitivity), 'S' to decresase the t
hPress 'm' to toggle sound, or 'q'Current Time: 2018-01-15 18:34:19.021088
```

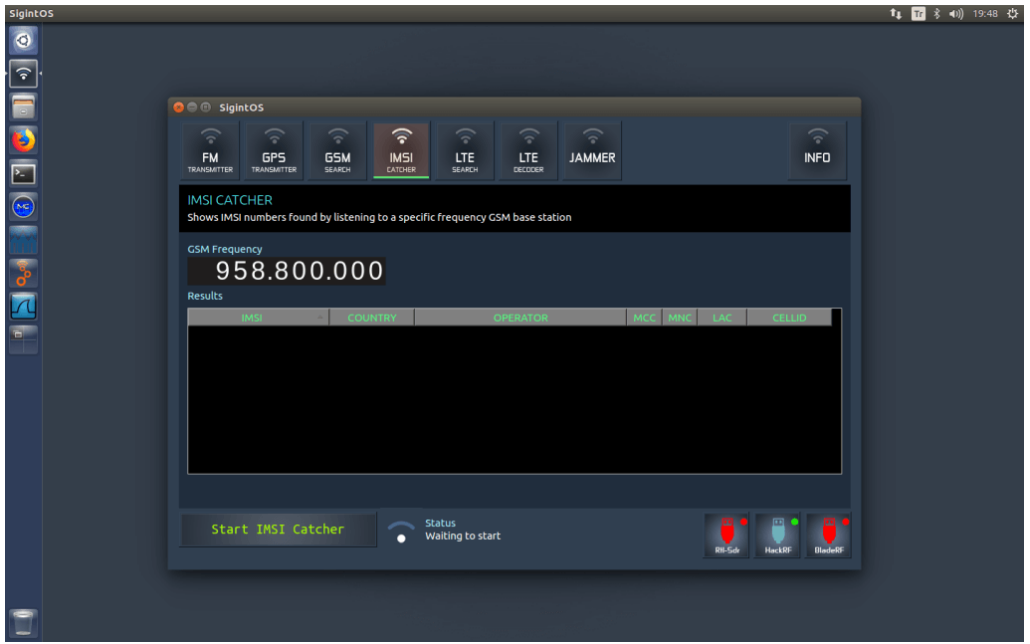
Wireless IDS & Tracking

LTE IMSI Catcher
aka Dirtbox, StingRay

** rtl-sdr must have transmit capability

SigIntOS claims to have catcher

Probably pay a license fee



https://www.rtl-sdr.com/sigintos-a-linux-distro-for-signal-intelligence/

https://www.sigintos.com/

A few researchers claim success

https://hackaday.com/2017/05/30/lte-imsi-catcher/

https://www.blackhat.com/docs/eu-15/materials/eu-15-Borgaonkar-LTE-And-IMSI-Catcher-Myths-wp.pdf

rogerpiquerasjover.net/LTE_security_TakeDownCon.pdf

Transmitting boards

For Rich People

HackRF One, 1 MHz – 6 GHz, ~$300

https://github.com/mossmann/hackrf/wiki/Software-Support

CLONING & SPOOFING TOOLS https://github.com/furrtek/portapack-havoc

Adalm PlutoSDR, 325 MHz – 3.8GHz, ~$150

*capable of 70 MHz - 6GHz

Yardstick One, ~280 MHz – 960 MHz, ~$120

https://github.com/atlas0fd00m/rfcat

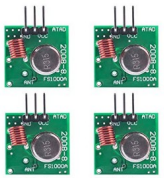
CC1110/CC1111 Dev Board, ~$75

Transmitting boards

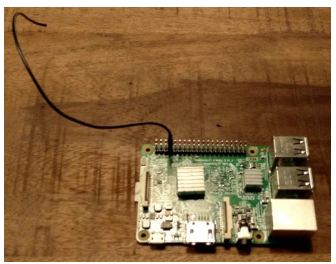
For Poor People

CC1101 chipset, requires microcontroller, ~$10

https://github.com/morethanuser/RFkitten



Freq. Specific 315/433MHz, ~$1 each



RpiTx, 5KHz – 1500MHz, Free

https://github.com/F5OEO/rpitx

USB3 VGA Dongle (FL2000) HF – 157MHz ~ 1.7GHz, $5

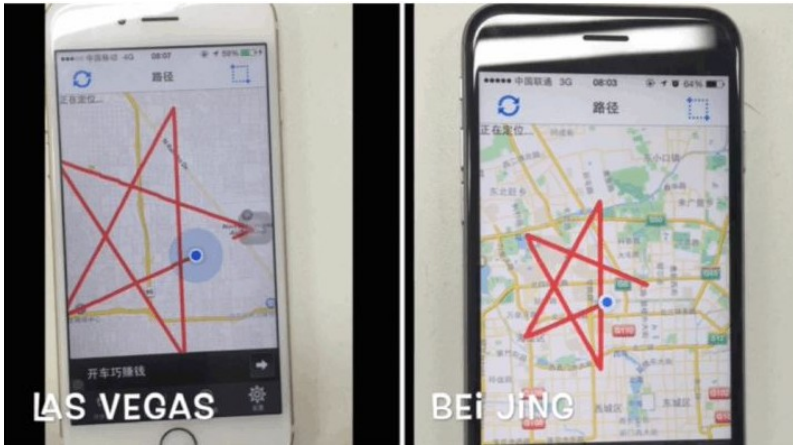
https://osmocom.org/projects/osmo-fl2k/wiki

Funtenna Exploit: https://arstechnica.com/information-technology/2015/08/funtenna-software-hack-turns-a-laser-printer-into-a-covert-radio/

GPS Spoofing & Jamming

1575 MHz and 1023 MHz

https://github.com/osqzss/gps-sdr-sim



JULY 19, 2018

USING A HACKRF TO SPOOF GPS NAVIGATION IN CARS AND DIVERT DRIVERS

https://www.rtl-sdr.com/using-a-hackrf-to-spoof-gps-navigation-in-cars-and-divert-drivers/

JULY 20, 2016

CHEATING AT POKÉMON GO WITH A HACKRF AND GPS SPOOFING

https://www.rtl-sdr.com/cheating-at-pokemon-go-with-a-hackrf-and-gps-spoofing/

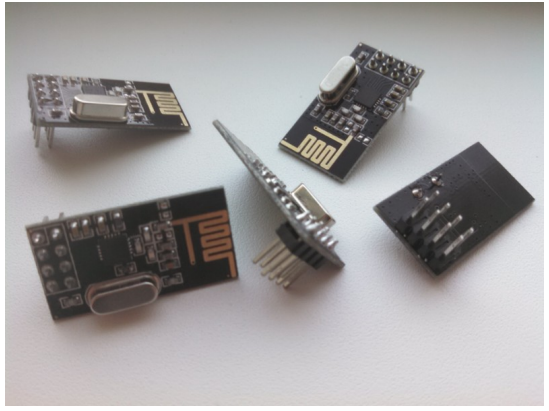
Drone Hacking

Or nRF24L01 sniffing

https://github.com/omriiluz/NRF24-BTLE-Decoder

nRF24L01 2.4GHz

http://blog.ptsecurity.com/2016/06/phd-vi-how-they-stole-our-drone.html



Also used in various Joysticks, Remotes, Keyboards, Mice, CrazyRadio

https://samy.pl/keysweeper/#sn

https://www.bitcraze.io/2015/06/sniffing-crazyflies-radio-with-hackrf-blue/

Exploit List

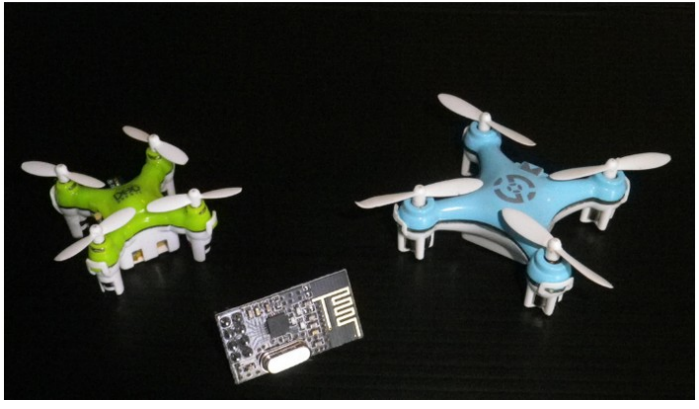
https://medium.com/@swalters/how-can-drones-be-hacked-the-updated-list-of-vulnerable-drones-attack-tools-dd2e006d6809

DeviationTX NRF24L01 Hijack

Attack type: Hijack (Bind before owner , overpower fixed freq/fixed ID)

Vulnerable drone: Most toy drones from Attop, Bayang, Cheerson, Eachine, Floueron, Hisky, JJRC, JD, Syma & WLToys) Complete list.

References: DeviationTX with $5 nrf24l01 module the universal drone remote.



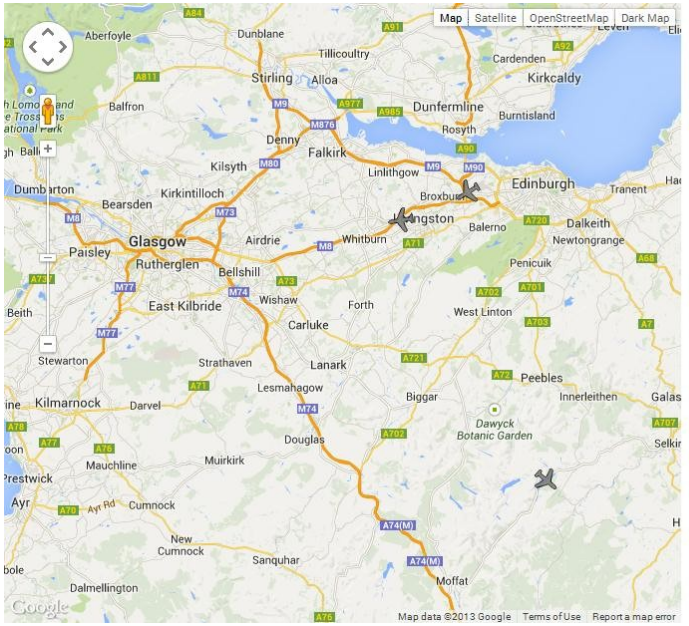
Aircraft Tracking

ADS-B Beacons on 1090MHz

Dump1090

https://github.com/antirez/dump1090

Hex	Mode	Sqwk	Flight	Alt	Spd	Hdg	Lat	Long	Sig	Msgs	Ti-
400e14	S	7315	EZY43PT	37000	419	353			5	42	0
406099	S	7634	CFE59G	38000					5	17	2
484cb6	S	6264	KLM65G	36325	413	297	55.844	-0.518	5	88	0
406a2e	S	7615	GMA104T	28000					4	100	2
400fba	S	5431	BEE1VB	5350					35	733	0
4ca281	S	7322	VIR3007	33175	396	336	54.564	-2.611	12	946	0
400ad1	S	7607		20025					7	208	0
400721	S	4246	LOG47LU	8550					30	955	0
400c5c	S	1444		27025					5	95	32
40610e	S	7330	BEE3FU	24000					9	583	0
400cb9	S	7732	LOG79ES	14500					11	922	0
4012d2	S	5466	LOG34YT	7100					6	83	5
405633	S	6254	EZY44NH	19425	387	149	55.408	-4.174	6	3039	13
400617	S	3416	TCX61EF	21550	439	108	55.364	-3.253	16	5062	0
405f79	S	4477	BEE767	19125					38	6845	0
400984	S	4622	EZE28Z	21475					12	3243	0
4ca73d	S	4244	RYR6699	3250	156	279	56.017	-3.135	81	6853	0
400987	S	4621	EZE76LK	23475					11	6841	0
400691	S	7762	BAW9CG	32675	458	317	56.386	-4.997	11	16051	0
4066d1	S	2227	TOM296	33225	488	151	54.700	-3.405	8	8244	0
4008fb	S	7655	LOG74HR	17600					10	5627	0
491304	S	7646	CSDXD	40000					8	5268	0



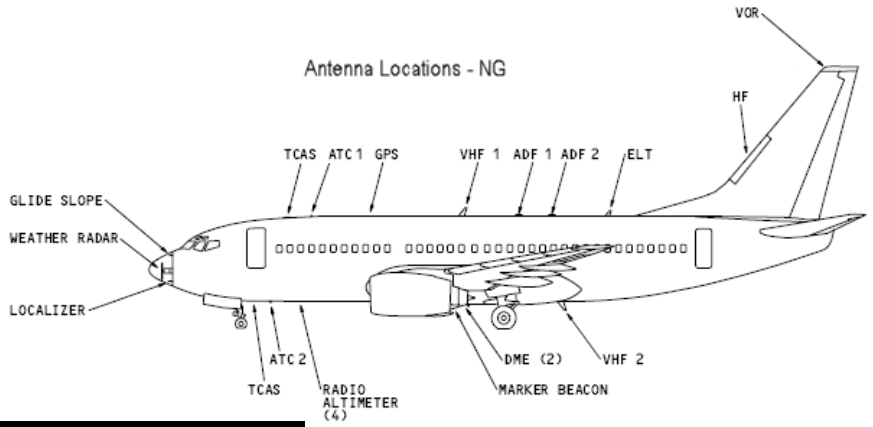
ADS-B Beacon Spoofing is easy: DoS Air Traffic Control Displays (RpiTx Throwie/Drone)

https://github.com/lyusupov/ADSB-Out

https://www.rtl-sdr.com/transmitting-ads-b-hackrf-receiving-rtl-sdr/

Aircraft Potential Attack Vectors?

Easy to sneak a transmitter on-board



Die Hard 2 style

https://www.iata.org/whatwedo/ops-infra/air-traffic-management/PublishingImages/Pages/radio-spectrum/aviation-usages-of-frequency-spectrum.pdf

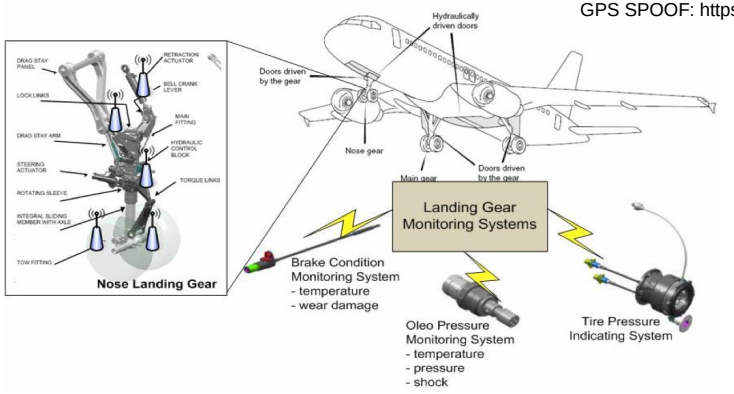
Aviation Usages of Frequency Spectrum (updated 5 January 2016 – Post WRC-2015)

Red text: ATM Infrastructure – Communication
Blue text: ATM Infrastructure – Navigation
Green text: ATM Infrastructure –Surveillance
Purple text: Avionics and Airborne equipment

Bands	Frequency Spectrum	Aviation Usages	Types of Services	Remark(s)
LF & MF	130 – 535 kHz	Non-Directional Beacon (NDB)	ARNS	
HF	2 850 – 22 000 kHz	Air-ground communication (HF voice and data)	AM(R)S	
	3 023 & 5 680 kHz	Search and Rescue	AM(R)S	
VHF	74.8 – 75.2 MHz	Marker Beacon	ARNS	
	108 – 117.975 MHz	VOR/ILS localizer GBAS/VDL Mode 4	ARNS AM(R)S	
	117.975 – 137 MHz	Air-ground and air-air communications (VHF voice and data)	AM(R)S	
	121.5, 123.1 & 243 MHz	Emergency distress frequency	AM(R)S	
UHF	328.6 – 335.4 MHz	ILS glide path	ARNS	
	406-406.1	Emergency locator transmitter (ELT)	MSS	
UHF or L	960 – 1 164 MHz	Distance Measuring Equipment (DME) TACAN Future LDACS	ARNS AM(R)S	***At risk*** - UK OfCom is proposing a shared use with wireless A/V system for big events. Possible European-wide extension. IATA submitted comments.
	978 MHz	Universal Access Transceiver (UAT)	AM(R)S	
	1 020 - 1 040 MHz and 1 080 – 1 100 MHz	Secondary Surveillance Radar (SSR) 1090 Extended Squitter ADS-B Airborne collision avoidance system (ACAS)	ARNS	***At risk*** - UK OfCom is proposing a shared use with wireless A/V system. Possible European-wide extension. IATA submitted comments. Note: Allocation for Earth-satellite link of ADS-B at WRC-15.
	1 164 – 1 215 MHz	DME/Global Navigation Satellite System (GNSS)	ARNS/RNSS	GPS (L5)/GLONASS (L5)/Galileo (E5a)/Beidou (B2a, B2)
	1 215 – 1 400 MHz	Primary Surveillance Radar (PSR)	ARNS	
	1 525 – 1 559 MHz	Satellite Communications (FANS)	MSS (space-Earth)	
	1 559 – 1 610 MHz	GNSS	ARNS/RNSS	GPS (L1), GLONASS ***At risk*** - LightSquared is aggressively lobbying US FCC for 1525 – 1545 MHz (MSS Downlink), 1610-1626.5 MHz (LEO) and 1626.5-1660.5 MHz (MSS Uplink). This may interfere with GPS (L1). IATA submitted joint comments.
	1 610 – 1 626.5 MHz	Satellite Communications (IRIDIUM)	AMS(R)S (s-E, E-s)	This AMS(R)S allocation does not support civil aviation requirement.
	1 626.5 – 1 660.5 MHz	Satellite Communications (FANS)	MSS(Earth-space)	
UHF or S	2 700 – 3 300 MHz	PSR Meteorological RADAR	ARNS RNS/RLS	
	3 400 – 4 200 MHz	Satellite Feeder Links to ATS Services in Africa		***To monitor*** - WRC-15 agreed on a better regulatory protection for FSS in Africa. Effectiveness to be seen. An educational campaign may be needed.
SHF or C	4 200 – 4 400 MHz	Radio Altimeter Wireless Avionics Intra-Communications (WAIC)	ARNS	***To monitor*** - Mobile phone requested adjacent frequency @ WRC-15. Allocation for WAIC at WRC-15.
	5 000 - 5 250 MHz	Microwave Landing System (MLS) UAS CNPC/Airport Surface Communication (AeroMACS)	ARNS AM(R)S/AMS(R)S	WRC-12 allocation. ***To monitor*** - For WRC-15 allocation see Note 1.
	5 350 - 5 470 MHz	Airborne weather radar	ARNS	Also used for airborne ground mapping.
SHF or X	8 750 - 8 850 MHz	Airborne Doppler radar	ARNS/RLS	Also used for airborne ground mapping. Airborne Doppler radar is used to determine aircraft ground distance, speed and drift angle.
	9 000 - 9 500 MHz	Precision Approach Radar (PAR)/Airborne weather radar/ASDE	ARNS/RNS	
SHF or Ku	13.25 - 13.4 GHz	Airborne Doppler radar	ARNS	
	15.4 - 15.7 GHz	PAR/Airborne weather radar/ASDE	ARNS/RLS	
SHF or K	24.25 - 24.65 GHz	ASDE	RNS	
SHF or Ka	31.8-33.4 GHz	ASDE/Airborne radar	RNS	

ACARS Spoofing: https://conference.hitb.org/hitbsecconf2013ams/materials/D1T1%20-%20Hugo%20Teso%20-%20Aircraft%20Hacking%20-%20Practical%20Aero%20Series.pdf

GPS SPOOF: https://www.nj.com/news/2013/08/man_fined_32000_for_blocking_newark_airport_tracking_system.html



Wireless Avionics Intra-Communications

(WAIC)

4.2 – 4.4 GHz

Redundant Safety Sensors Communicating Within the Plane

https://waic.avsi.aero/

Union Pacific

ATCS

Advanced Train Control System : Ensure safety by monitoring track status

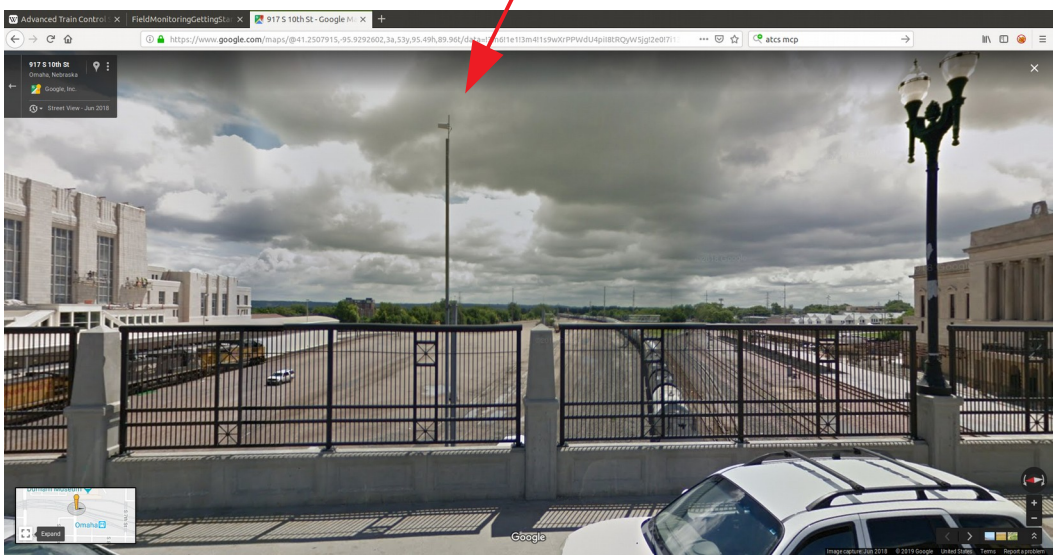
http://atcswiki-beta.greatlakesnetworking.net/index.php/FieldMonitoringGettingStarted

UP uses Genisys system.

Similar to MAS SCADA.

http://grouper.ieee.org/groups/railtransit/wg14/WEI%20Specification.pdf
https://w3.usa.siemens.com/mobility/us/en/freight-rail/rail-automation/field-service-group/Documents/MANUALS/COM-00-94-03A.1.pdf

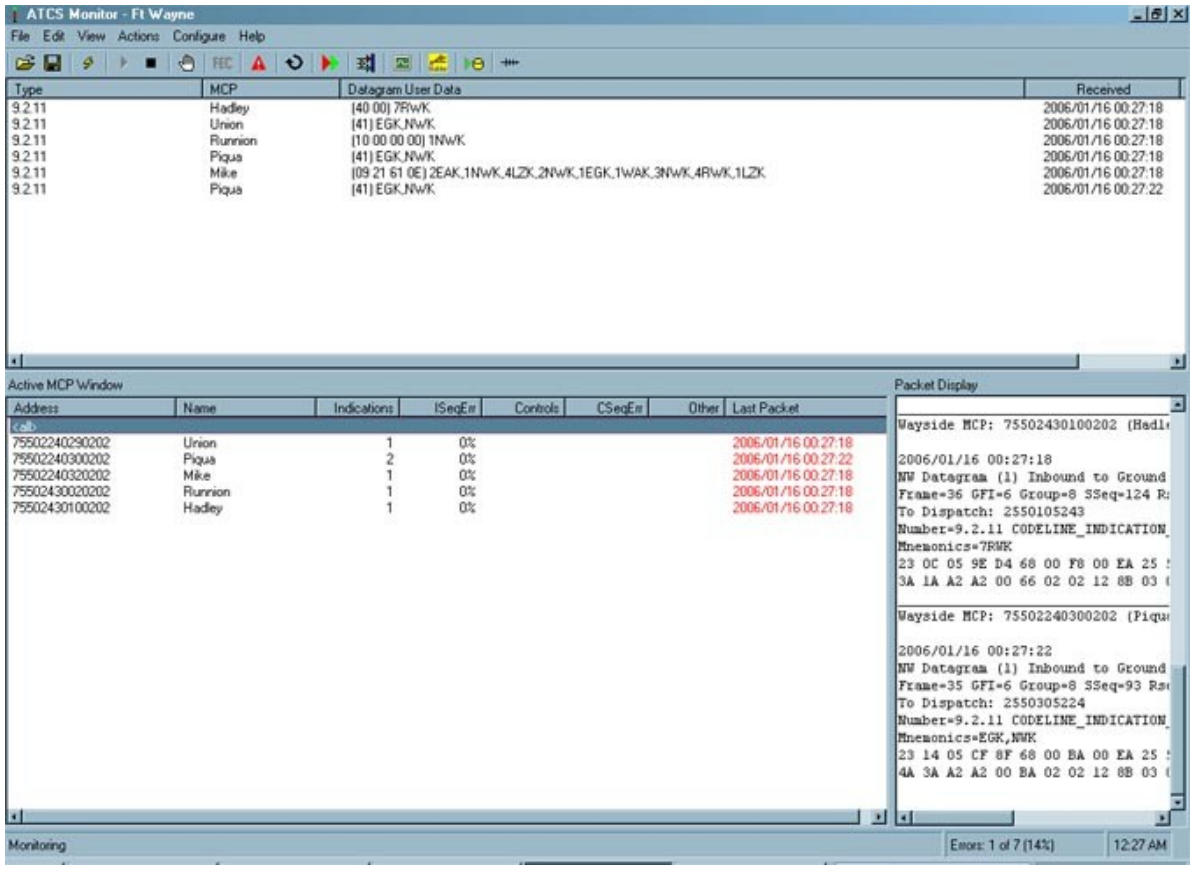
Base antenna (BCP) polls remote yagi antennas (M/WCP)

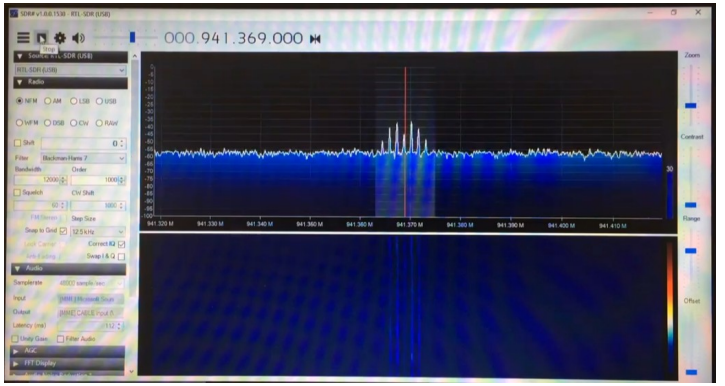


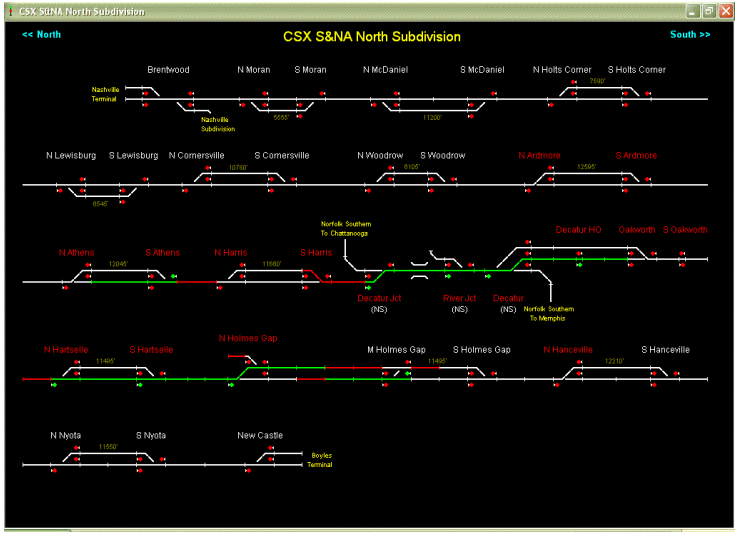
ATCS Monitor

Windows only. Tune SDR# to BCP/MCP frequency & pipe audio out to ATCSMonitor software

http://atcswiki-beta.greatlakesnetworking.net/index.php/Main_Page





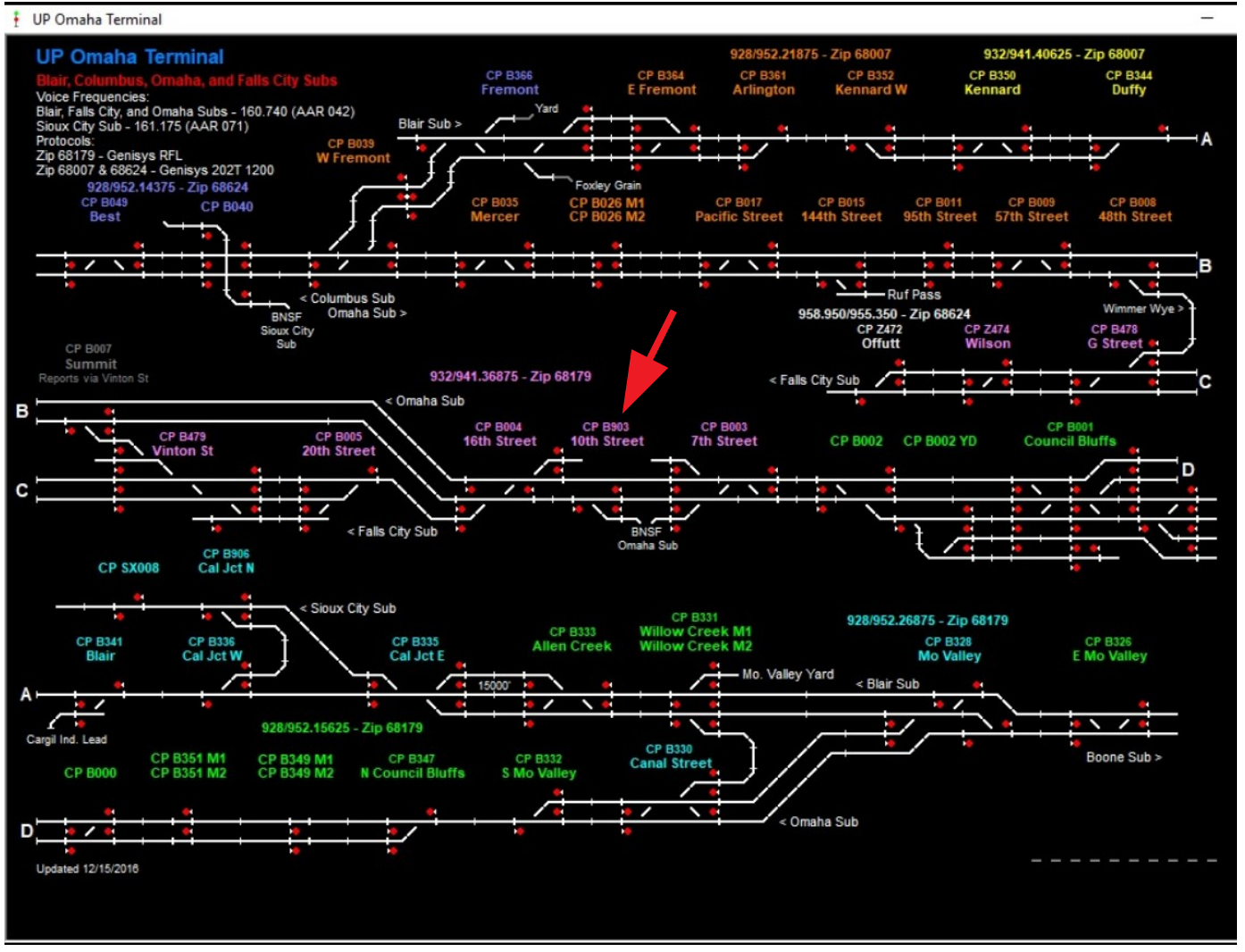


Monitor Train activity in energy producing areas

e.g. Oil production/movement → Market Prediction

FCC fines clandestine train tracking company http://trn.trains.com/news/news-wire/2016/09/27-aei-reader-update

ATCS Omaha Map



On-board Train Telemetry

Transmits Brake Pressure & Accidental Train Separation

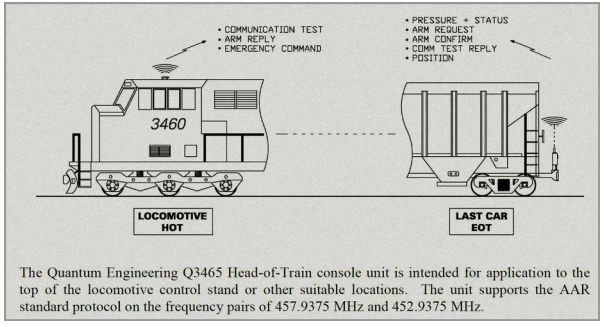
~452MHZ

SoftEOT

File Monitor Packets Tools Help

Time Received	SIG	SRC	ID	RR	SYMB	BP	MOT	MRK	BATST	BATCU	TRB	CMD	TYP	VLV	CNF
2014/02/01 19:52:06	0.2	EOT	44777			60	0	1	OK	0	1		NML	1	0
2014/02/01 19:52:24	0.6	HOT	76527									SRQ	NML		
2014/02/01 19:52:31	0.4	HOT	77830									SRQ	NML		
2014/02/01 19:52:32	0.6	HOT	76832									SRQ	NML		
2014/02/01 19:53:33	0.2	HOT	26376									SRQ	NML		
2014/02/01 19:54:00	0.2	HOT	99999									SRQ	NML		
2014/02/01 19:54:10	0.2	HOT	44777									SRQ	NML		
2014/02/01 19:54:26	0.4	HOT	76527									SRQ	NML		
2014/02/01 19:54:32	0.2	HOT	77830									SRQ	NML		
2014/02/01 19:55:31	0.1	HOT	26376									SRQ	NML		
2014/02/01 19:56:11	0.5	EOT	44777			61	0	1	OK	0	1		NML	1	0
2014/02/01 19:56:12	0.5	EOT	44777			60	0	1	OK	0	1		NML	1	1
2014/02/01 19:56:15	0.5	EOT	44777			60	0	1	OK	0	1		NML	1	1
2014/02/01 19:56:17	0.4	EOT	43075			0	0	1	OK	20	1		NML	1	0
2014/02/01 19:56:23	0.4	EOT	76527			85	1	1	OK	30	1		NML	1	0
2014/02/01 19:56:27	0.4	EOT	76527			85	1	1	OK	30	1		NML	1	1
2014/02/01 19:56:31	0.4	EOT	76832			90	1	1	OK	0	1		NML	1	0
2014/02/01 19:56:35	0.4	EOT	76832			89	1	1	OK	0	1		NML	1	1
2014/02/01 19:57:11	0.3	EOT	44777			60	0	1	OK	0	1		NML	1	0
2014/02/01 19:57:13	0.3	EOT	43075			0	0	1	OK	20	1		NML	1	0
2014/02/01 19:57:28	0.3	EOT	76527			85	1	1	OK	30	1		NML	1	0
2014/02/01 19:57:37	0.3	EOT	76832			89	1	1	OK	0	1		NML	1	0
2014/02/01 19:58:10	0.2	EOT	44777			61	0	1	OK	0	1		NML	1	0

https://groups.yahoo.com/neo/groups/SoftEOT/info



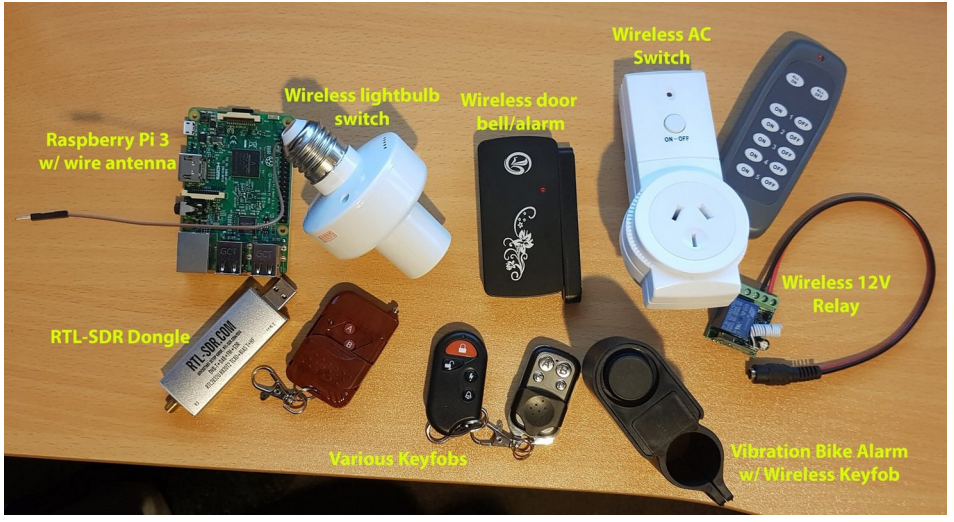
The Quantum Engineering Q3465 Head-of-Train console unit is intended for application to the top of the locomotive control stand or other suitable locations. The unit supports the AAR standard protocol on the frequency pairs of 457.9375 MHz and 452.9375 MHz.

I'd like to know: Can we get the train to stop in a remote location if the engineer thinks the brake pressure is failing?
Disrupt traffic, hijack, sabotage, steal cargo

Key Fob / Remote Control / Sensor Hacking

Fixed Code Remotes: Old Garage Doors
Gated Communities (DoorKing)
Remote Controls
Tornado Sirens (DTMF Tones)

Replay Attack: Simply record signal with RTL_SDR or Tuner (GQRX)
Replay signal with RpiTX

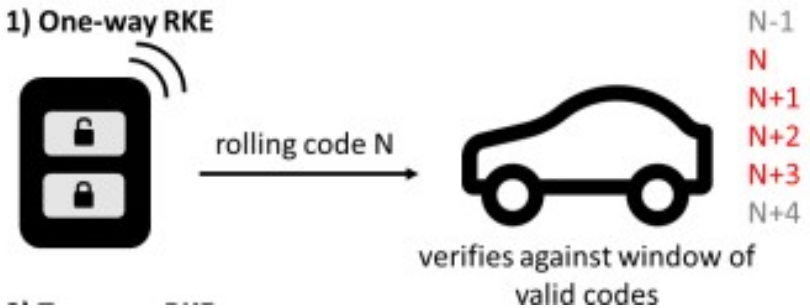


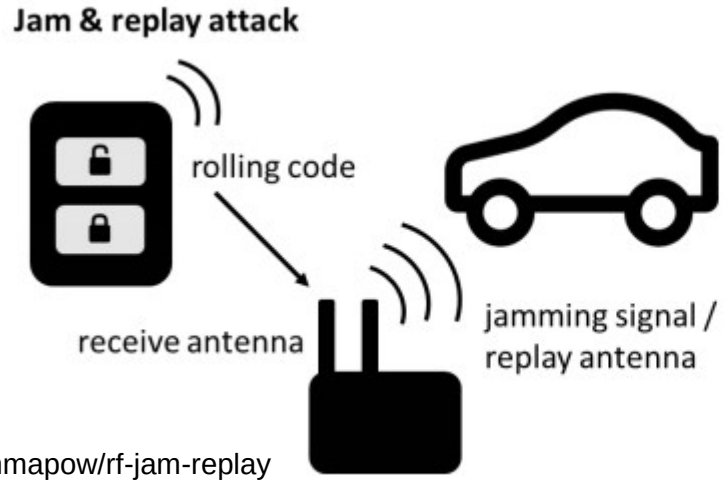
https://www.rtl-sdr.com/tutorial-replay-attacks-with-an-rtl-sdr-raspberry-pi-and-rpitx/

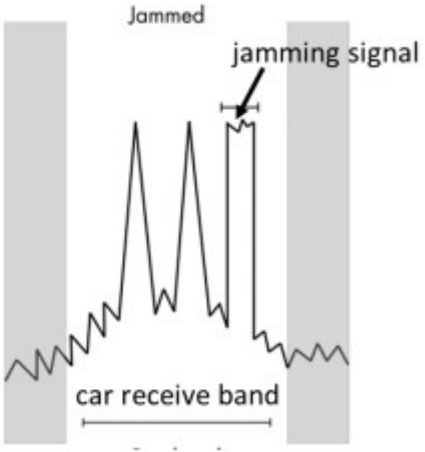
Key Fob Hacking

RollJam

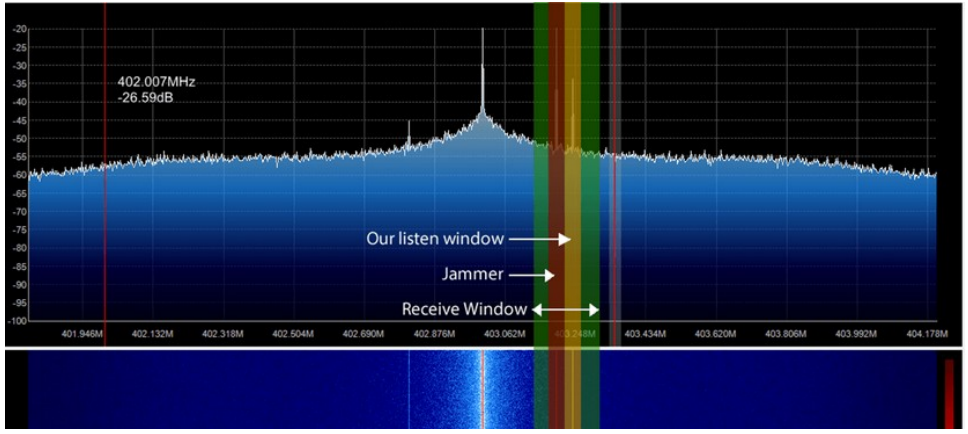
Rolling Code Remote Keyless Entry (RKE)



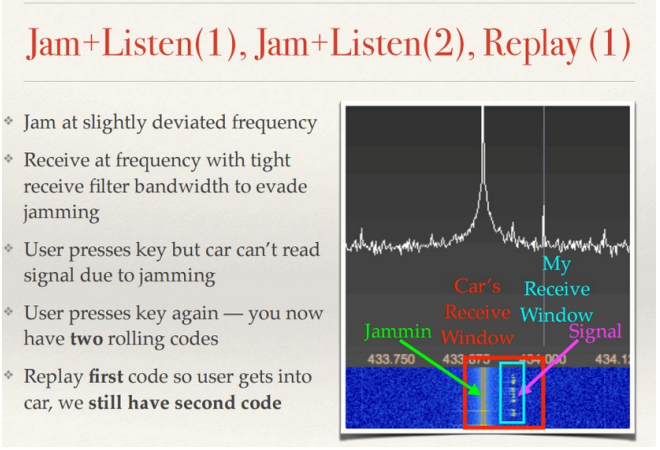




https://github.com/trishmapow/rf-jam-replay



https://www.andrewmohawk.com/2016/02/05/bypassing-rolling-code-systems/



https://www.rtl-sdr.com/breaking-into-cars-wirelessly-with-a-32-homemade-device-called-rolljam/

Key Fob Hacking

~~RollJam~~

Just Jam

Common in South Africa.

Key Fobs use 433MHz (315/390 in US)

Jam with cheap handheld transceiver (e.g. Baofeng)

Robbed in seconds: Car-jammers in SA

2017-06-14 08:28

SHARE:

Johannesburg - South Africa is one of the world's hot spots for hijacking and vehicle theft. Alarmingly, many car owners are also robbed of their possessions by criminals breaking into vehicles.

A growing trend among criminals is the use of car-remote jamming; a technique used by criminals whereby a signal blocks attempts to lock your vehicle via your alarm remote.

We've included videos revealing car-jamming tactics in SA as well as valuable advice for motorists.

Signal Jamming

REMOTE-JAMMING IN SA: Another driver falls victim to theft in SA. *Image: YouTube*

Lazy & unconcerned drivers don't notice the car never locked

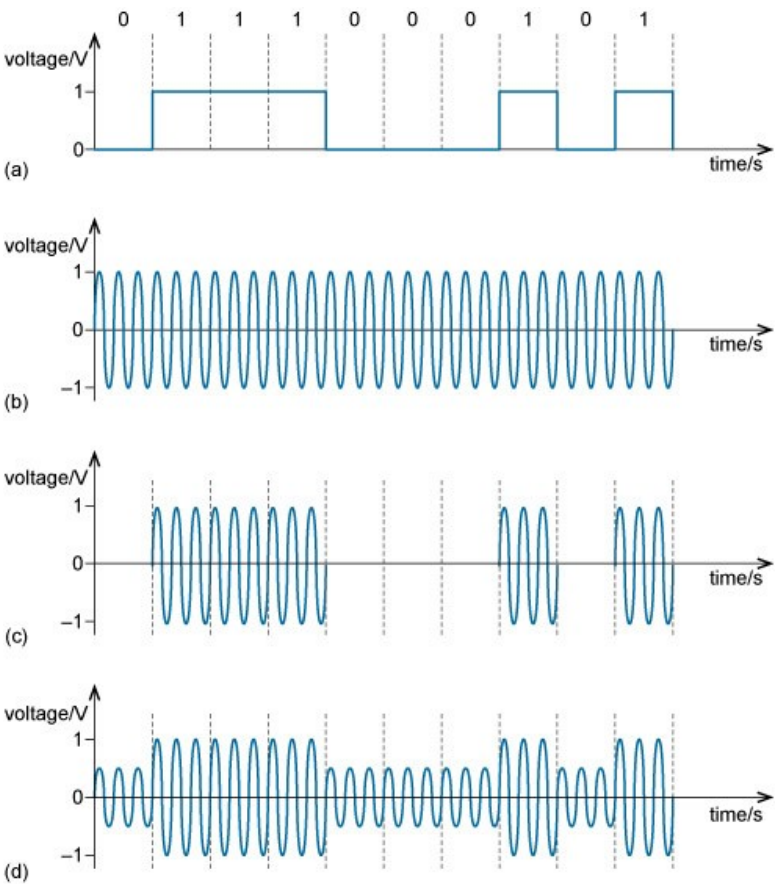
Once inside the car, capture the garage door signal.
Send the signal to my partner/RpiTx waiting at the home address

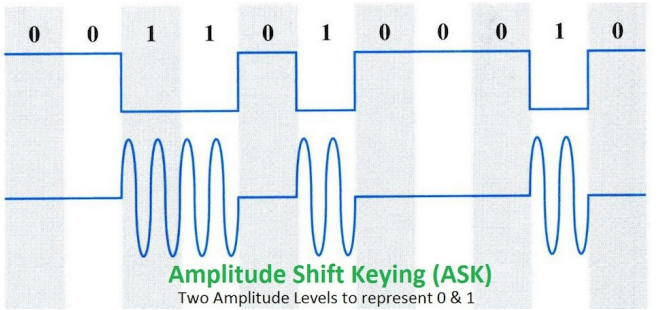
Signal Decoding

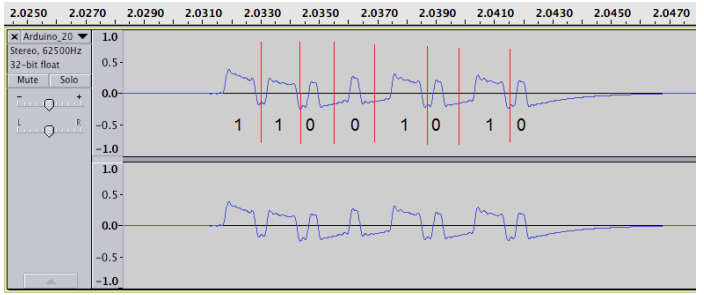
OOK / ASK

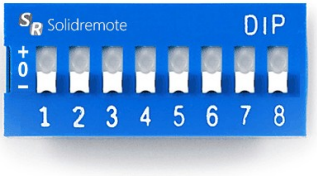
On-Off Keying / Amplitude Shift Keying

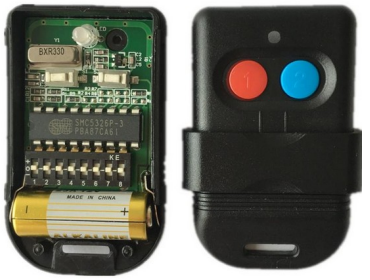
Used in a lot of remotes & sensors, transmitting lightweight data (few bytes)











Sensors & Remote Controls

Some signal formats are already decoded/known

RTL_433 Program performs automatic decode

https://github.com/merbanan/rtl_433

```
Supported device protocols:
    [01]* Silvercrest Remote Control
    [02]  Rubicson Temperature Sensor
    [03]  Prologue Temperature Sensor
    [04]  Waveman Switch Transmitter
    [05]* Steffen Switch Transmitter
    [06]* ELV EM 1000
    [07]* ELV WS 2000
    [08]  LaCrosse TX Temperature / Humidity Sensor
    [09]* Template decoder
    [10]* Acurite 896 Rain Gauge
    [11]  Acurite 609TXC Temperature and Humidity Sensor
    [12]  Oregon Scientific Weather Sensor
    [13]* Mebus 433
    [14]* Intertechno 433
    [15]  KlikAanKlikUit Wireless Switch
    [16]  AlectoV1 Weather Sensor (Alecto WS3500 WS4500 Ventus W155/W044 Oregon
    [17]  Cardin S466-TX2
    [18]  Fine Offset Electronics, WH2 Temperature/Humidity Sensor
    [19]  Nexus Temperature & Humidity Sensor
    [20]  Ambient Weather Temperature Sensor
    [21]  Calibeur RF-104 Sensor
    [22]* X10 RF
    [23]* DSC Security Contact
    [24]* Brennenstuhl RCS 2044
    [25]  GT-WT-02 Sensor
    [26]  Danfoss CFR Thermostat
    [27]* Energy Count 3000 (868.3 MHz)
    [28]* Valeo Car Key
    [29]  Chuango Security Technology
    [30]  Generic Remote SC226x EV1527
    [31]  TFA-Twin-Plus-30.3049 and Ea2 BL999
    [32]  Fine Offset Electronics WH1080/WH3080 Weather Station
    [33]  WT450
    [34]  LaCrosse WS-2310 Weather Station
    [35]  Esperanza EWS
    [36]  Efergy e2 classic
    [37]* Inovalley kw9015b, TFA Dostmann 30.3161 (Rain and temperature sensor)
    [38]  Generic temperature sensor 1
    [39]  WG-PB12V1
    [40]  Acurite 592TXR Temp/Humidity, 5n1 Weather Station, 6045 Lightning
    [41]  Acurite 986 Refrigerator / Freezer Thermometer
    [42]  HIDEKI TS04 Temperature, Humidity, Wind and Rain Sensor
    [43]  Watchman Sonic / Apollo Ultrasonic / Beckett Rocket oil tank monitor
    [44]  CurrentCost Current Sensor
    [45]  emonTx OpenEnergyMonitor
    [46]  HT680 Remote control
    [47]  S3318P Temperature & Humidity Sensor
    [48]  Akhan 100F14 remote keyless entry
    [49]  Quhwa
    [50]  OSv1 Temperature Sensor
    [51]  Proove
    [52]  Bresser Thermo-/Hygro-Sensor 3CH
```

```
    [52]  Bresser Thermo-/Hygro-Sensor 3CH
    [53]  Springfield Temperature and Soil Moisture
    [54]  Oregon Scientific SL109H Remote Thermal Hygro Sensor
    [55]  Acurite 606TX Temperature Sensor
    [56]  TFA pool temperature sensor
    [57]  Kedsum Temperature & Humidity Sensor
    [58]  blyss DC5-UK-WH (433.92 MHz)
    [59]  Steelmate TPMS
    [60]  Schrader TPMS
    [61]* LightwaveRF
    [62]  Elro DB286A Doorbell
    [63]  Efergy Optical
    [64]  Honda Car Key
    [65]* Template decoder
    [66]  Fine Offset Electronics, XC0400
    [67]  Radiohead ASK
    [68]  Kerui PIR Sensor
    [69]  Fine Offset WH1050 Weather Station
    [70]  Honeywell Door/Window Sensor
    [71]  Maverick ET-732/733 BBQ Sensor
    [72]* RF-tech
    [73]  LaCrosse TX141-Bv2/TX141TH-Bv2 sensor
    [74]  Acurite 00275rm,00276rm Temp/Humidity with optional probe
    [75]  LaCrosse TX35DTH-IT Temperature sensor
    [76]  LaCrosse TX29IT Temperature sensor
    [77]  Vaillant calorMatic 340f Central Heating Control
    [78]  Fine Offset Electronics, WH25 Temperature/Humidity/Pressure Sensor
    [79]  Fine Offset Electronics, WH0530 Temperature/Rain Sensor
    [80]  IBIS beacon
    [81]  Oil Ultrasonic STANDARD FSK
    [82]  Citroen TPMS
    [83]  Oil Ultrasonic STANDARD ASK
    [84]  Thermopro TP11 Thermometer
    [85]  Solight TE44
    [86]  Wireless Smoke and Heat Detector GS 558
    [87]  Generic wireless motion sensor
    [88]  Toyota TPMS
    [89]  Ford TPMS
    [90]  Renault TPMS
    [91]* inFactory
    [92]  FT-004-B Temperature Sensor
    [93]  Ford Car Key
    [94]  Philips outdoor temperature sensor
    [95]  Schrader TPMS EG53MA4
    [96]  Nexa
    [97]  Thermopro TP12 Thermometer
    [98]  GE Color Effects
    [99]  X10 Security
    [100]  Interlogix GE UTC Security Devices
    [101]* Dish remote 6.3
```

Fixed Remote (Dip Switch) Hacking

Replay attack, but must be in proximity during a button push

If the signal encoding (line code) style is known, then brute force DIP code

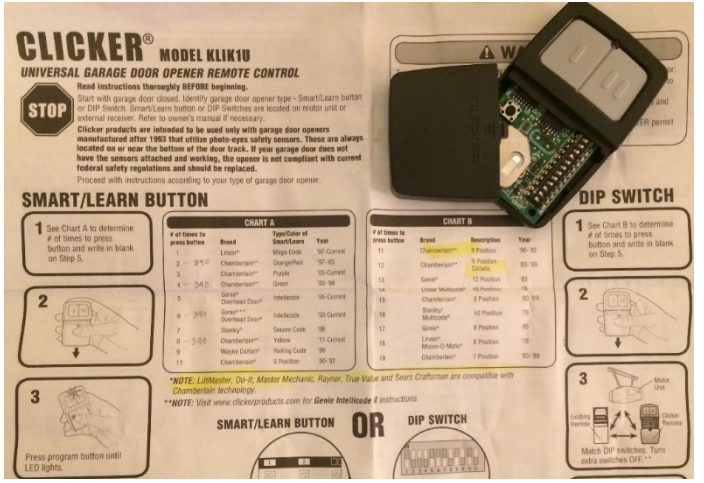
RfCat firmware has several tools:

- Helper scripts for RfCat devices https://github.com/AndrewMohawk/RfCatHelpers
- Simple OOK/ASK bruteforce library with custom checksums support https://github.com/Ganapati/brOOKforce
- Brute force/de Bruijn script for triggering an ook rf device with a rfcat dongle https://github.com/exploitagency/github-rfpwnon

Samy Kamkar's Open Sesame
http://samy.pl/opensesame/

Universal Garage Remote

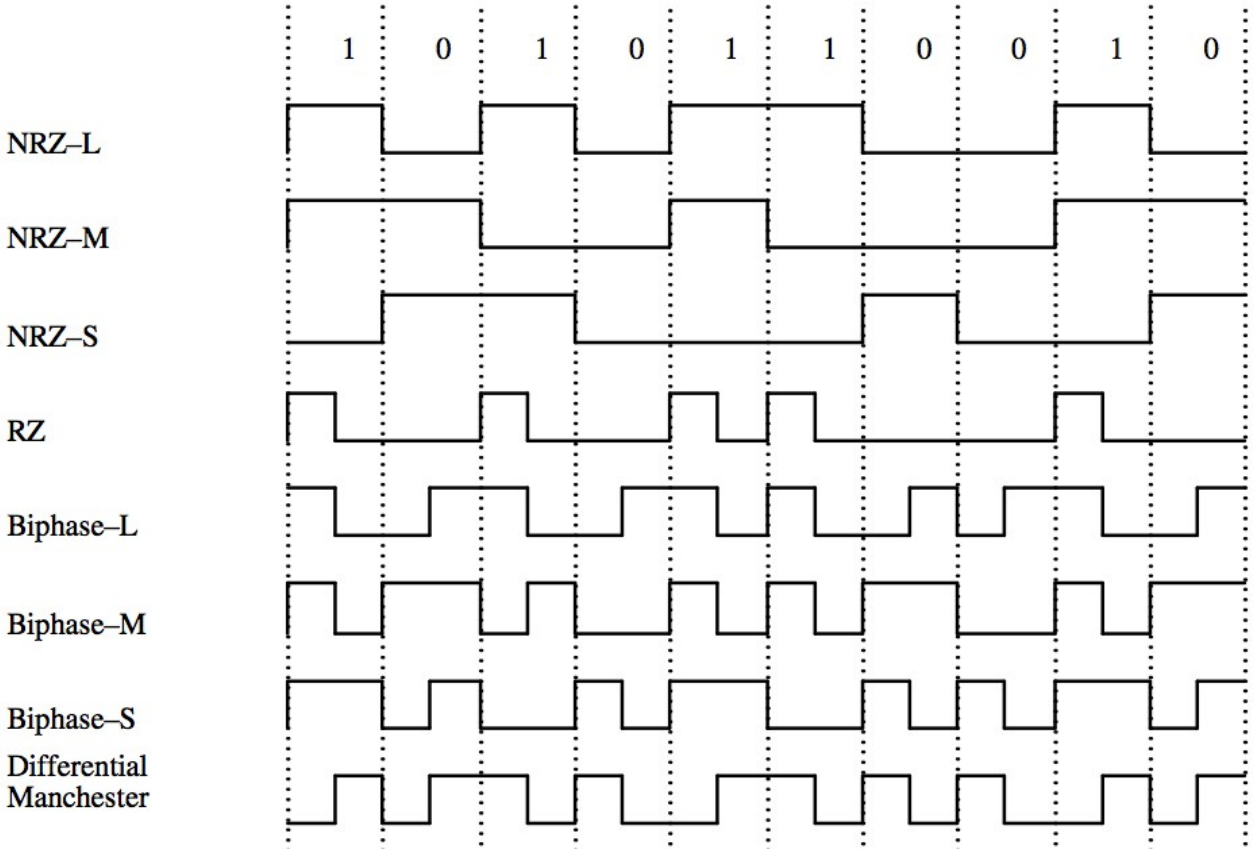
Sold at Walmart. Great learning tool



OOK Signal Decoding

If the signal is new/unknown, we have to determine line code format

How is the binary data being transmitted?



https://en.wikipedia.org/wiki/Line_code

OOK/ASK Reverse Engineering Tools

RTL_433: analyze mode

https://github.com/merbanan/rtl_433

Universal Radio Hacker: demodulation, custom decodes, fuzzing

https://github.com/jopohl/urh

RFSec-ToolKit: collection of tools. Baudline, ooktools, Inspectrum, rtl_433

https://github.com/cn0xroot/RFSec-ToolKit

CRC RevEng: CRC (checksum) cracking

http://reveng.sourceforge.net/

Audacity: Digital audio editor. Manually view signal via WAV file

https://www.audacityteam.org/

OOK Decode Examples

https://www.rtl-sdr.com/wp-content/uploads/2016/12/ASK_erhard_e_tutorial.pdf

https://addie.bike/tech/2018/07/13/garage-door-hack.html

https://foo-manroot.github.io/post/gnuradio/sdr/2018/01/15/gnuradio-ook-transmit.html

https://medium.com/@eoindcoolest/decoding-a-garage-door-opener-with-an-rtl-sdr-5a47292e2bda

https://www.securitysift.com/ook-signal-decoding-replay/

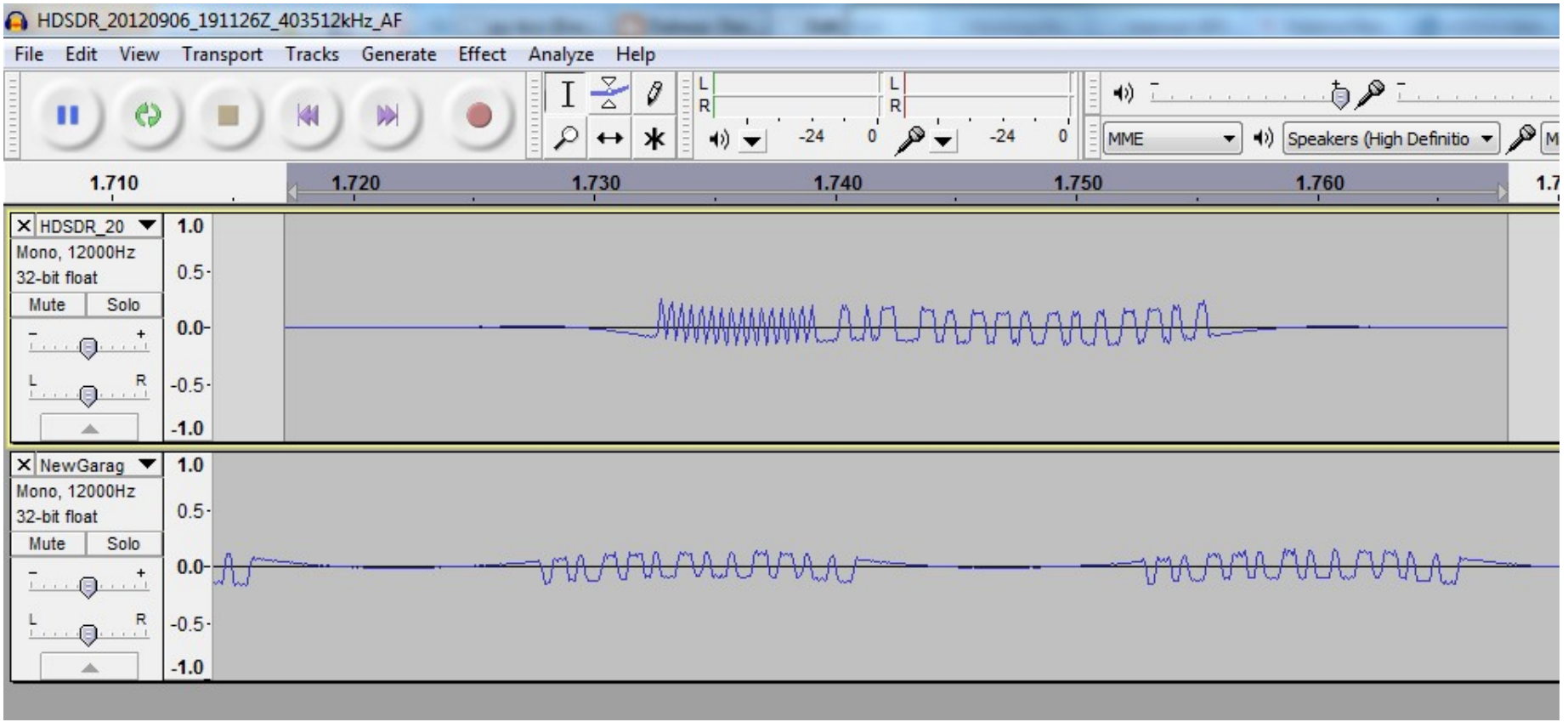
https://www.andrewmohawk.com/2012/09/06/hacking-fixed-key-remotes/

Audacity

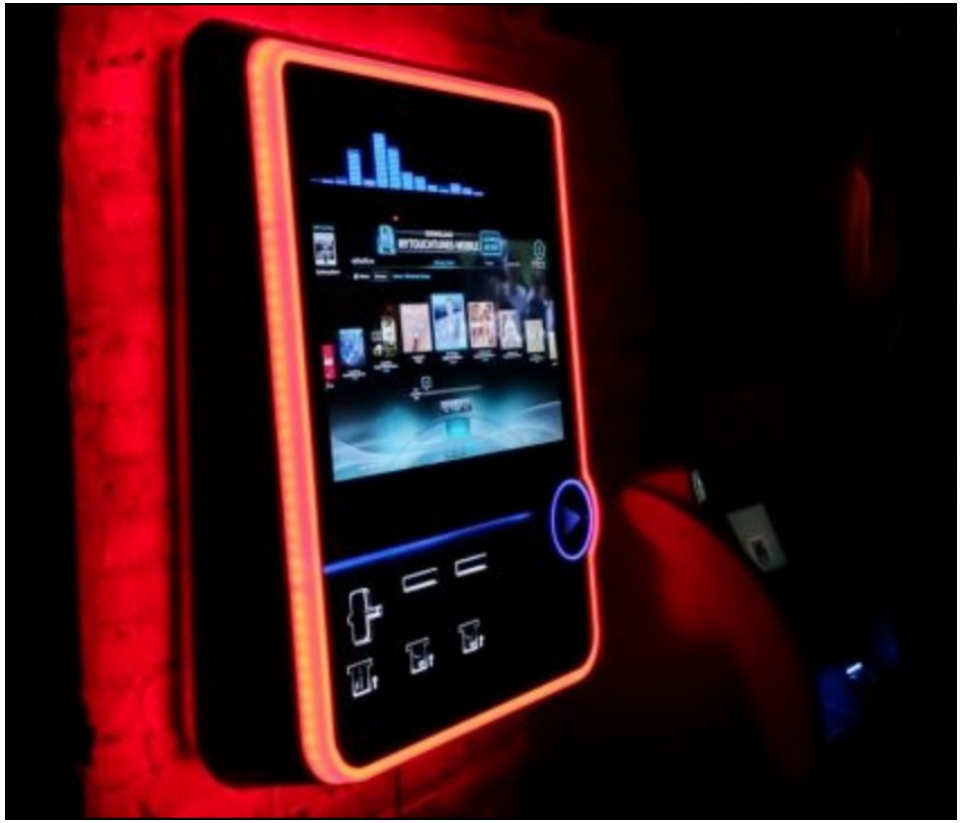
Demodulate signal (AM vs FM) and record to digital audio file (WAV)

Linux CLI: rtl_fm -M am -f 433920000 -s 2000000 - | sox -t raw -r 2000000 -e signed-integer -b 16 -c 1 -V1 – capture.wav

https://samy.pl/dingdong/



Touchtunes Jukebox Remote Control



April 2016
900303-001 Rev. 03

TouchTunes

Single-Frequency Remote Control User Guide

About This Guide

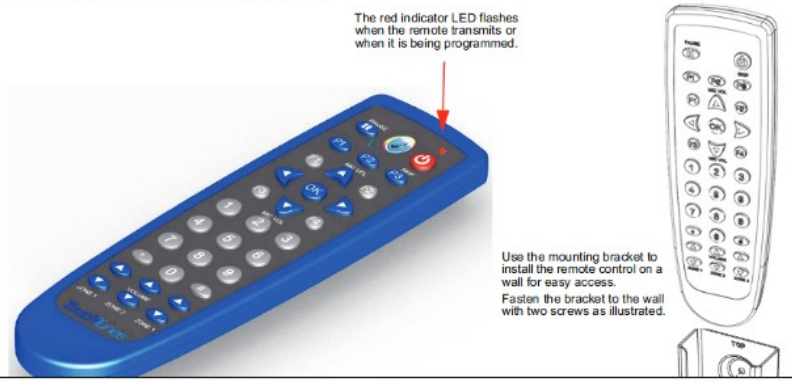
This guide explains the setup and operation of TouchTunes wireless remote control, P/N 700194-001.

Package Contents

- Remote control (part number 700194-001)
- Mounting bracket (part number 400188-001)
- 2 AAA alkaline batteries
- This guide

Overview

TouchTunes' wireless remote control is a single-frequency remote that transmits a 433.92 MHz (FSK) signal to TouchTunes jukeboxes manufactured after 2005.



(ASK not FSK)

http://productwarranty.touchtunes.com/download/attachments/1179814/900303-001-Remote%20Control%20User%20Guide-R01.pdf?version=2&modificationDate=1493044681000&api=v2

“Skip Song” Signal Intercept

Attach RTL-SDR, wifi adapter, & battery pack to Raspberry Pi w/ rtl_fm installed

Tether RasPi to smart phones hotspot/wifi network. SSH

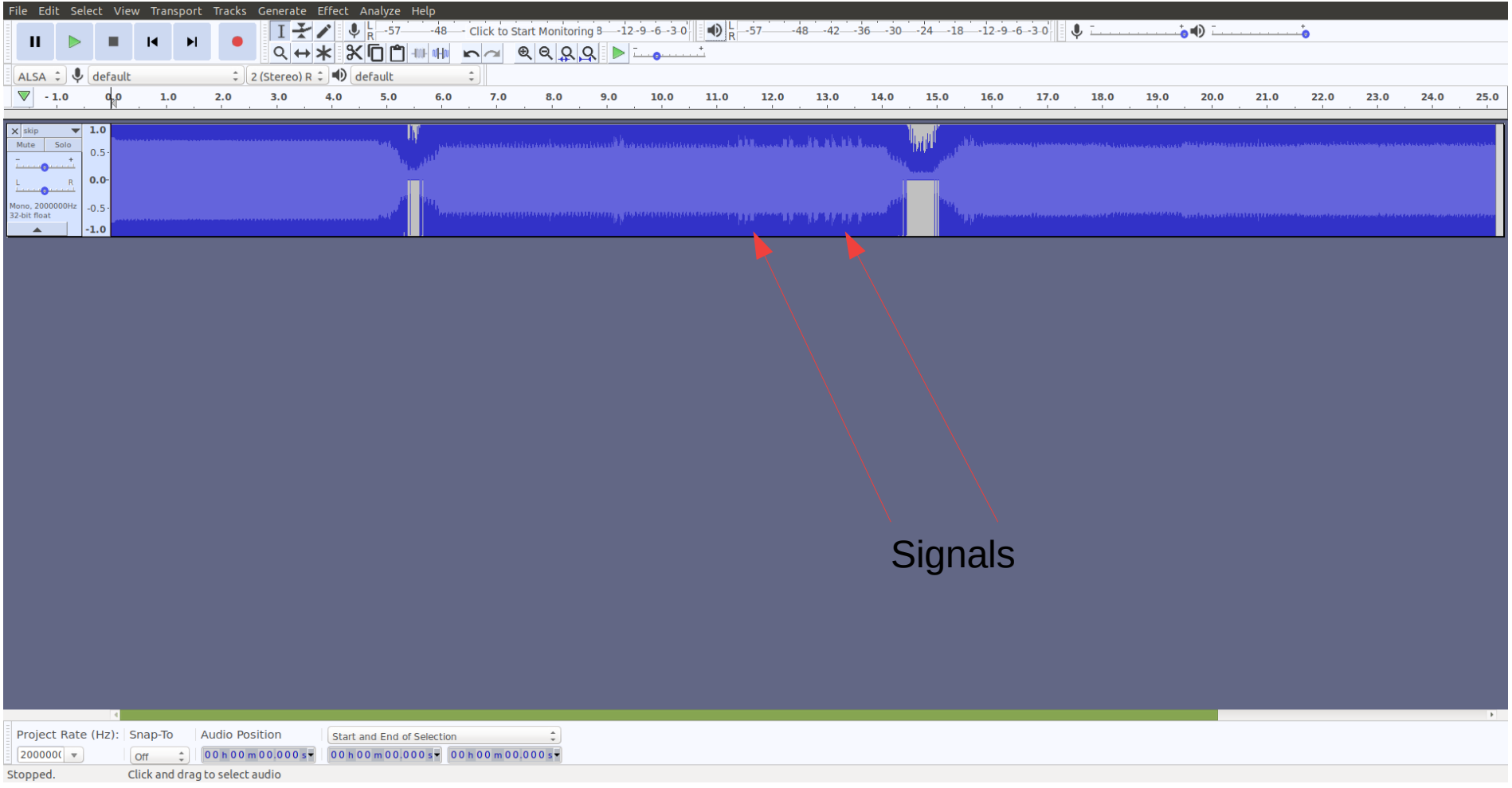
Hangout at dive bar during dead hours. Play a bad song & ask the bartender to skip

Prior to the “skip”, start recording 433.92 MHz on RasPi.

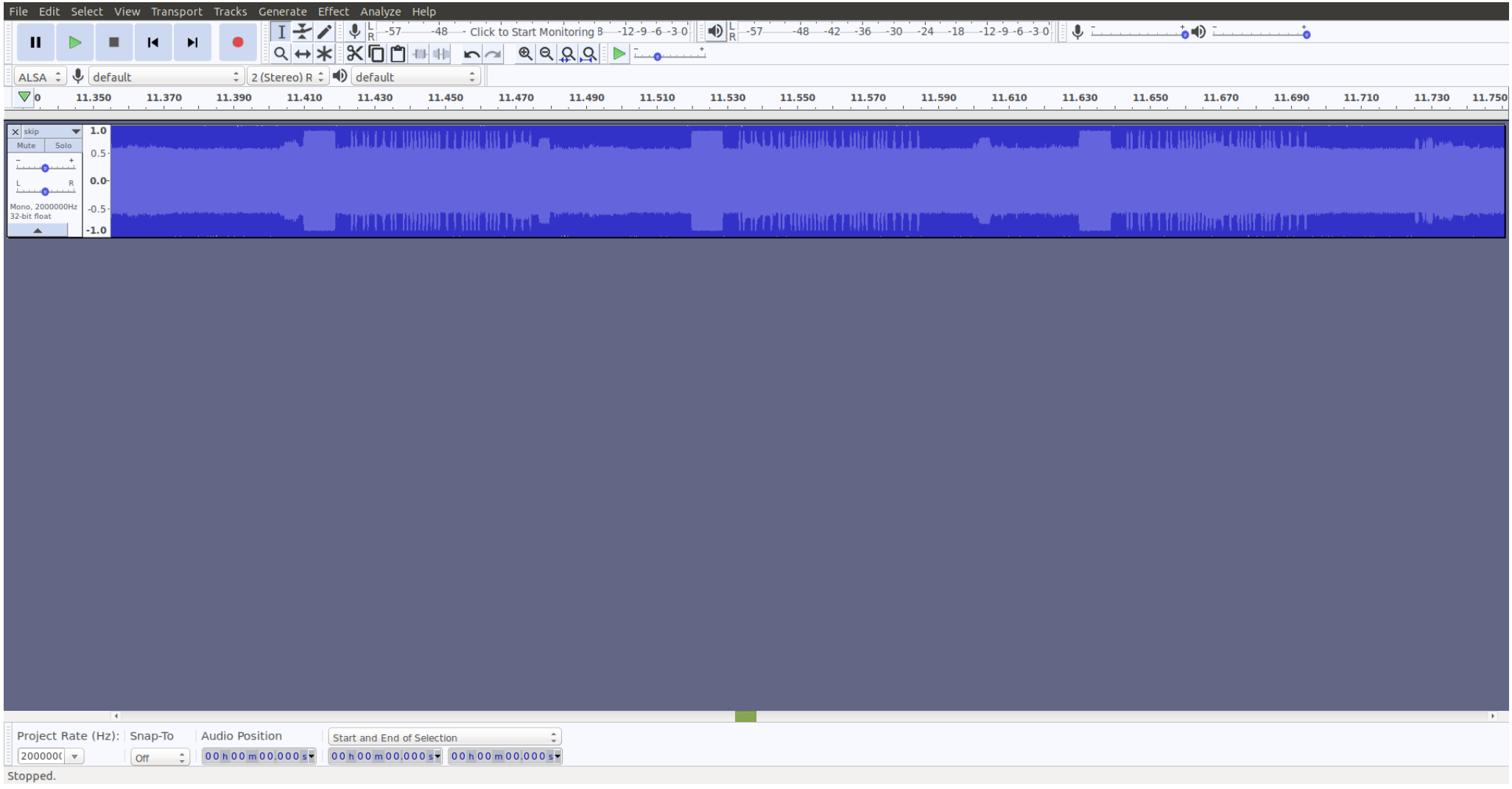
Command: rtl_fm -M am -f 433920000 -s 2000000 - | sox -t raw -r 2000000 -e signed-integer -b 16 -c 1 -V1 – capture.wav

Reverse Engineer Signal

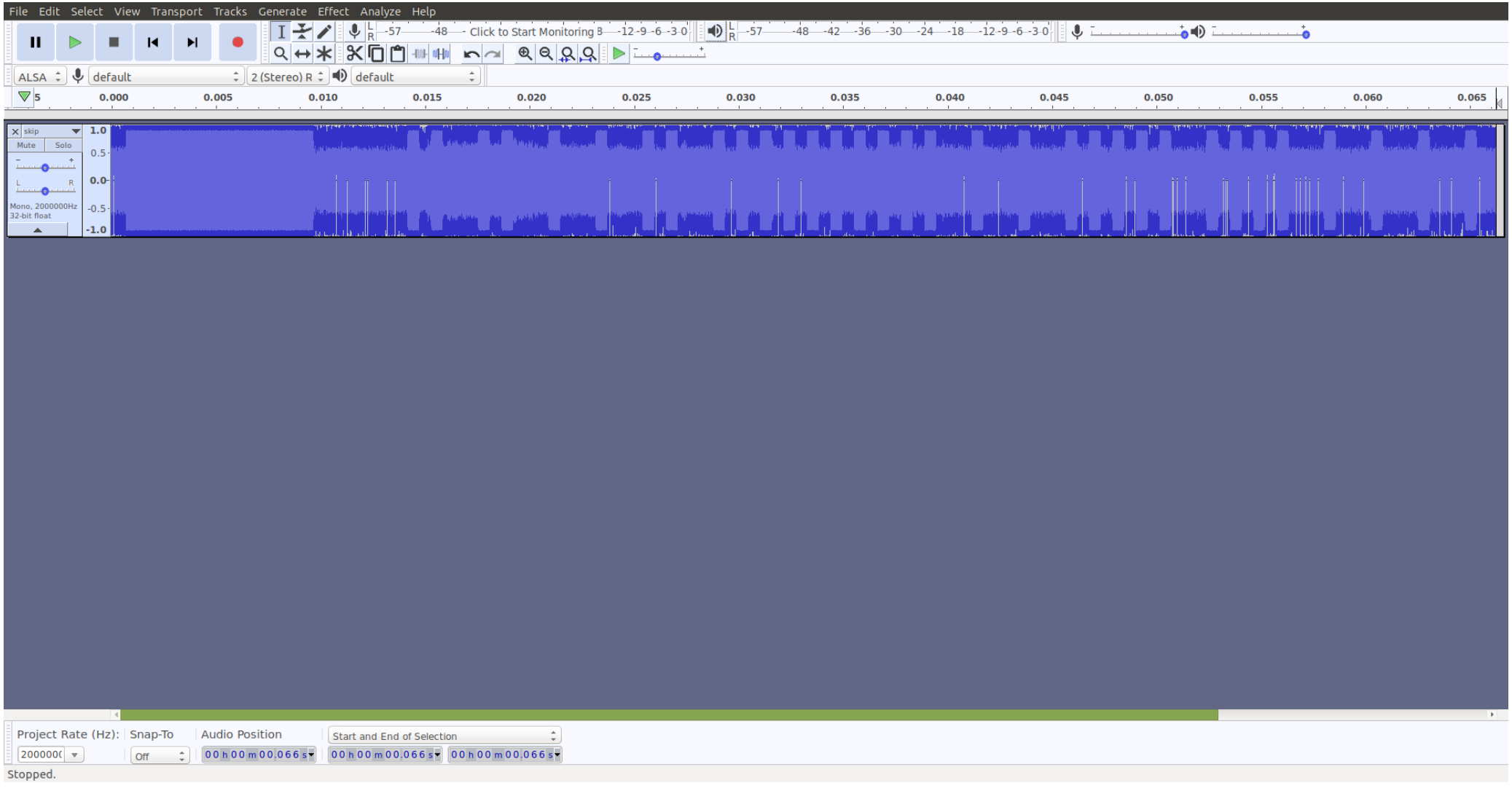
Examine wav file in Audacity or Baudline



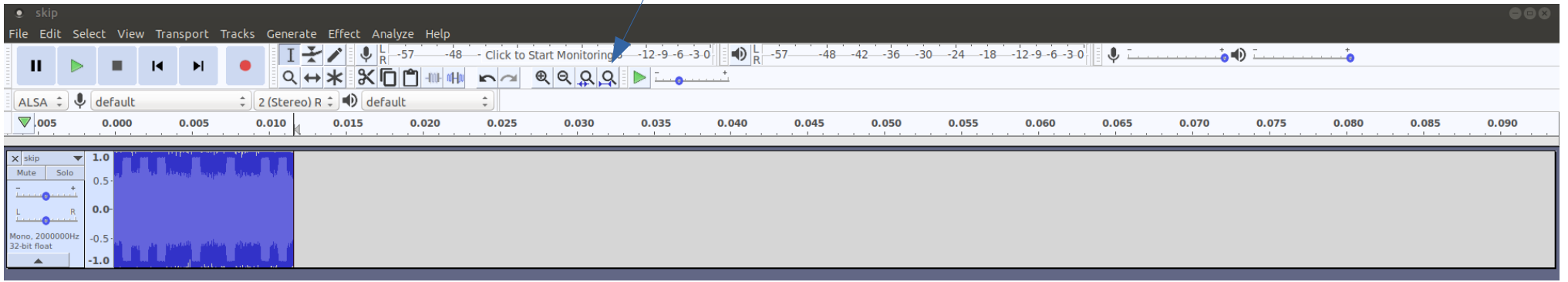
Zoomed In

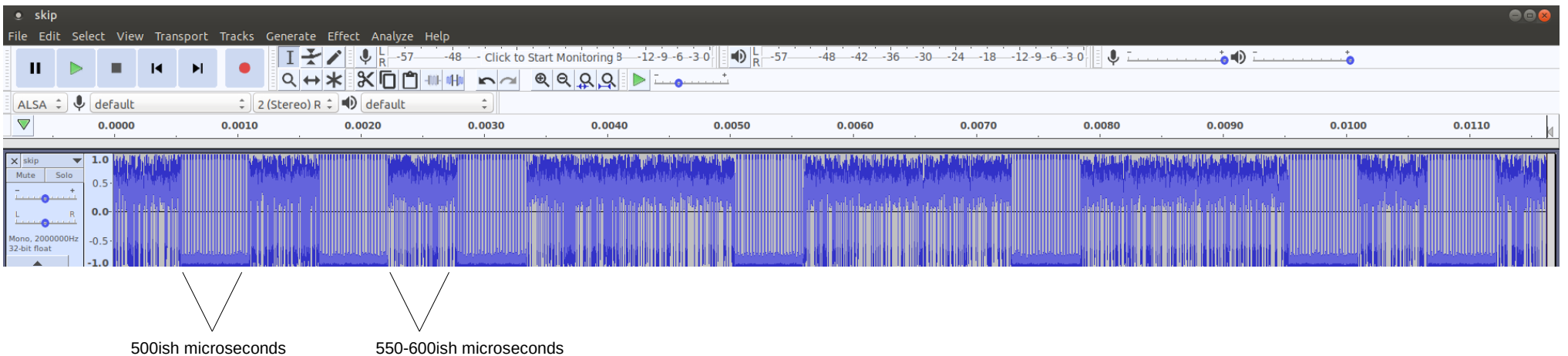

File Edit Select View Transport Tracks Generate Effect Analyze Help
Click to Start Monitoring
ALSA
default
2 (Stereo) R
default
11.350 11.370 11.390 11.410 11.430 11.450 11.470 11.490 11.510 11.530 11.550 11.570 11.590 11.610 11.630 11.650 11.670 11.690 11.710 11.730 11.750
skip
Mute
Solo
Mono, 2000000Hz
32-bit float
1.0
0.5
0.0
-0.5
-1.0
Project Rate (Hz):
Snap-To
Audio Position
Start and End of Selection
Off
00 h 00 m 00,000 s
Stopped.

Zoomed to single signal

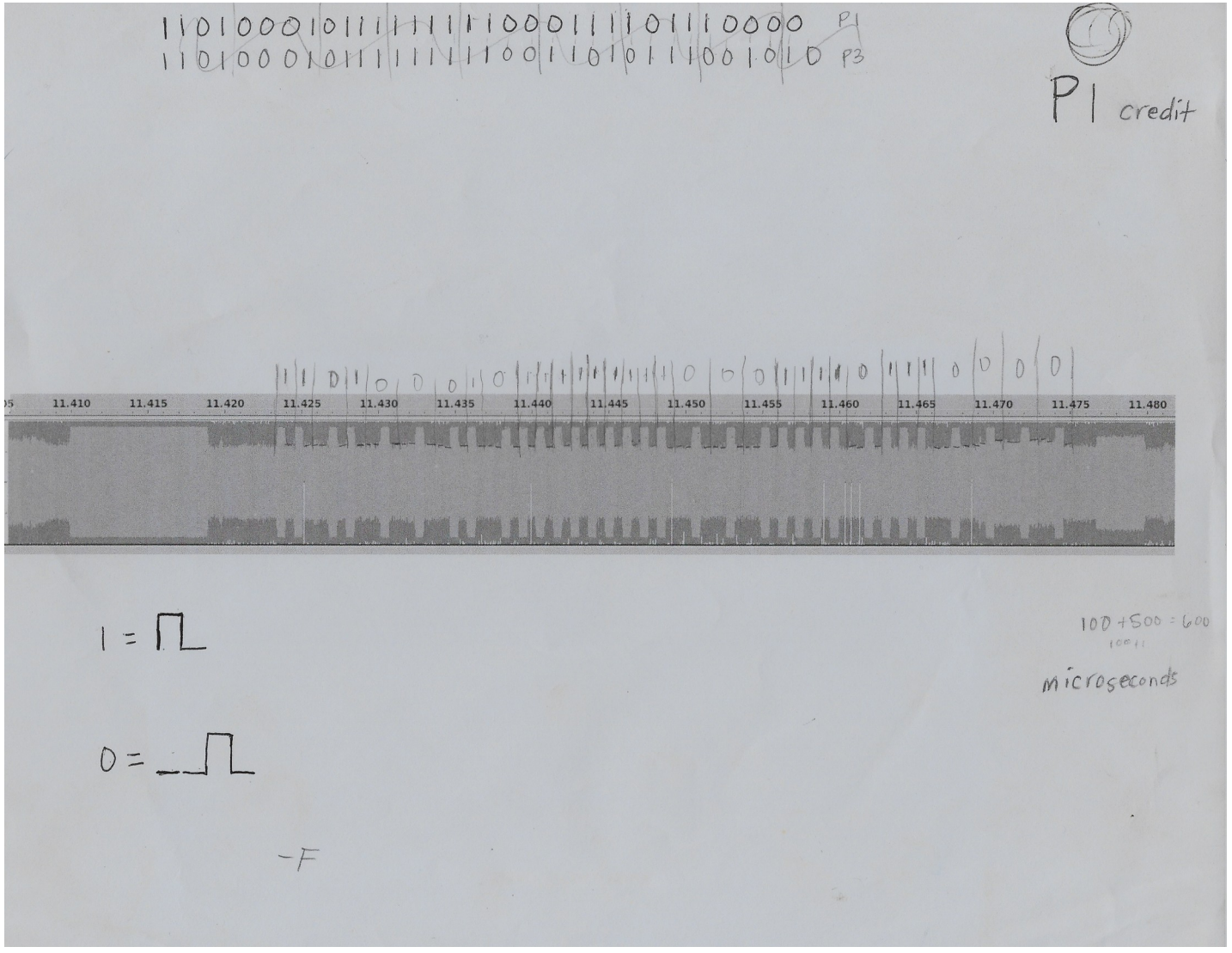


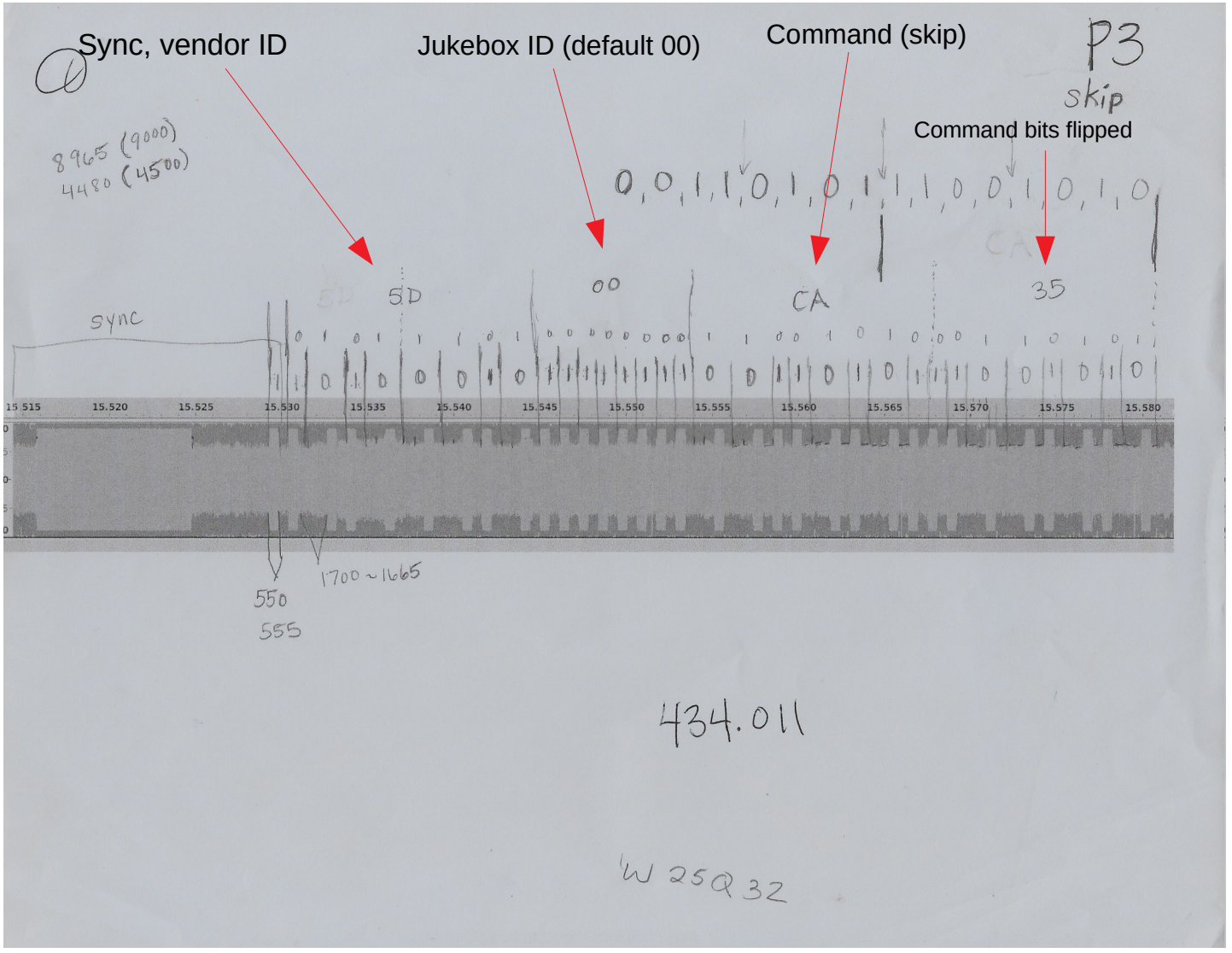
Determine length of pulses & gaps (microseconds)





Manchester Encoding




Sync, vendor ID
Jukebox ID (default 00)
Command (skip)
P3
skip
Command bits flipped
8965 (9000)
4480 (4500)
0,0,1,1,0,1,0,1,1,1,0,0,1,0,1,0
5D
00
CA
35
sync
15.515
15.520
15.525
15.530
15.535
15.540
15.545
15.550
15.555
15.560
15.565
15.570
15.575
15.580
550
555
1700 ~ 1665
434.011
W 25 Q 32

Arduino Hello World

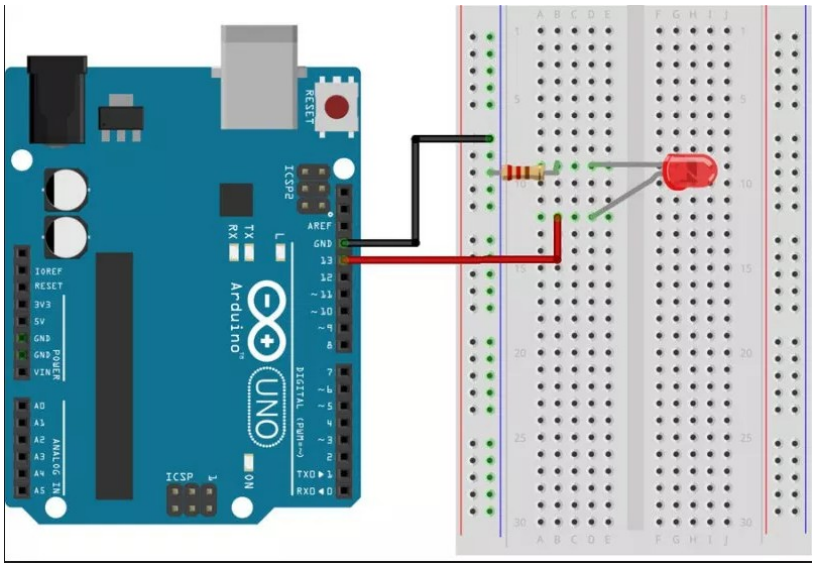
Blink LED

https://www.arduino.cc/en/tutorial/blink

```
void setup() {
  // initialize digital pin LED_BUILTIN as an output.
  pinMode(LED_BUILTIN, OUTPUT);
}

// the loop function runs over and over again forever
void loop() {
  digitalWrite(LED_BUILTIN, HIGH);   // turn the LED on (HIGH is the voltage level)
  delay(1000);                       // wait for a second
  digitalWrite(LED_BUILTIN, LOW);    // turn the LED off by making the voltage LOW
  delay(1000);                       // wait for a second
}
```

ON

OFF

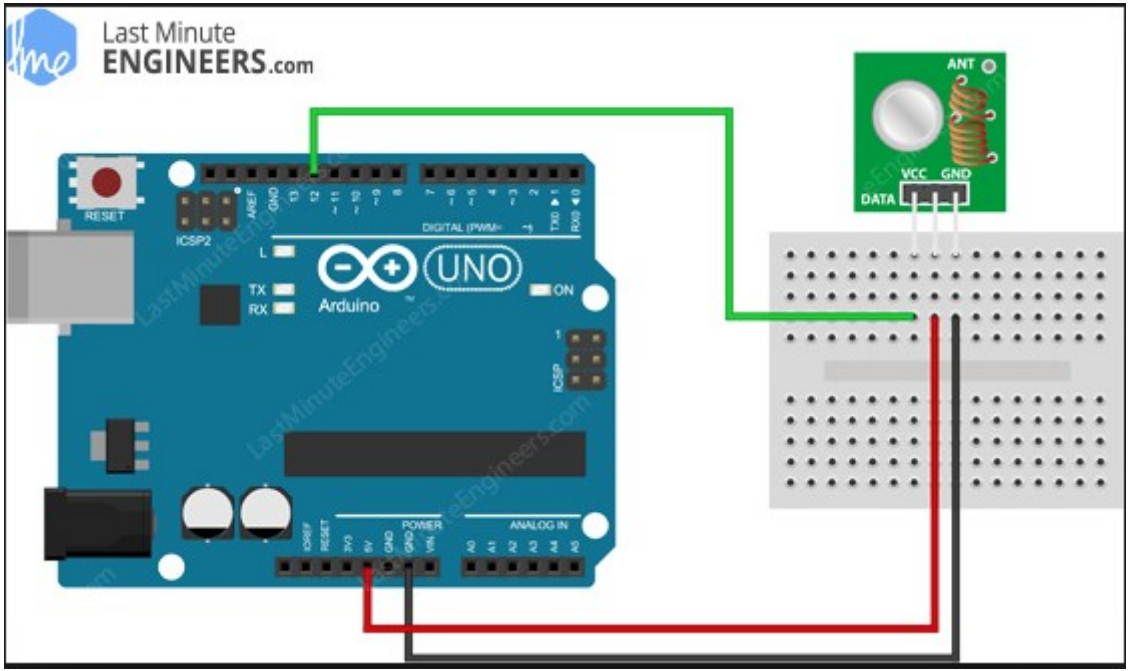


Arduino 433 Transmitter (Jukebox Clone)

*skip.c

```c

int main (void) {
    int pin = 0; //GPIO pin 11 on RaspberryPi2
    int try_limit = 3; //send code 3 times

    if( wiringPiSetup() == -1 )
        exit (1);
    if( piHiPri( 99 ) == -1 )
        exit (1);

    pinMode( pin, OUTPUT );

    for( int y = 0; y < 1; y++ ) {
        for( int z = 0; z < try_limit; z++ ) {
            int values[] =
            {
                1,1,0,1,0,0,0,1,0,
                1,1,1,1,1,1,1,1,
                0,0,1,1,0,1,0,1,1,1,0,0,1,0,1,0
            };

            int valueCount = 33;

            digitalWrite( pin, HIGH );
            delayMicroseconds( 8965 );
            digitalWrite( pin, LOW );
            delayMicroseconds( 4480 );

            for( int x = 0; x < valueCount; x++ ) {
                if( values[x] == 1 ) {
                    digitalWrite( pin, HIGH );
                    delayMicroseconds( 500 );
                    digitalWrite( pin, LOW );
                    delayMicroseconds( 585 );
                }
                else {
                    digitalWrite( pin, LOW );
                    delayMicroseconds( 1066 );
                    digitalWrite( pin, HIGH );
                    delayMicroseconds( 500 );
                    digitalWrite( pin, LOW );
                    delayMicroseconds( 585 );
                }
            }
            digitalWrite( pin, LOW );
            delayMicroseconds( 45000 );
        }
    }
```

RasPi example. Arduino is same concept



https://lastminuteengineers.com/433mhz-rf-wireless-arduino-tutorial/

Other Jukebox commands(volume, pause) available online

HackRf PortaPack & Havoc Firmware

https://github.com/furrtek/portapack-havoc

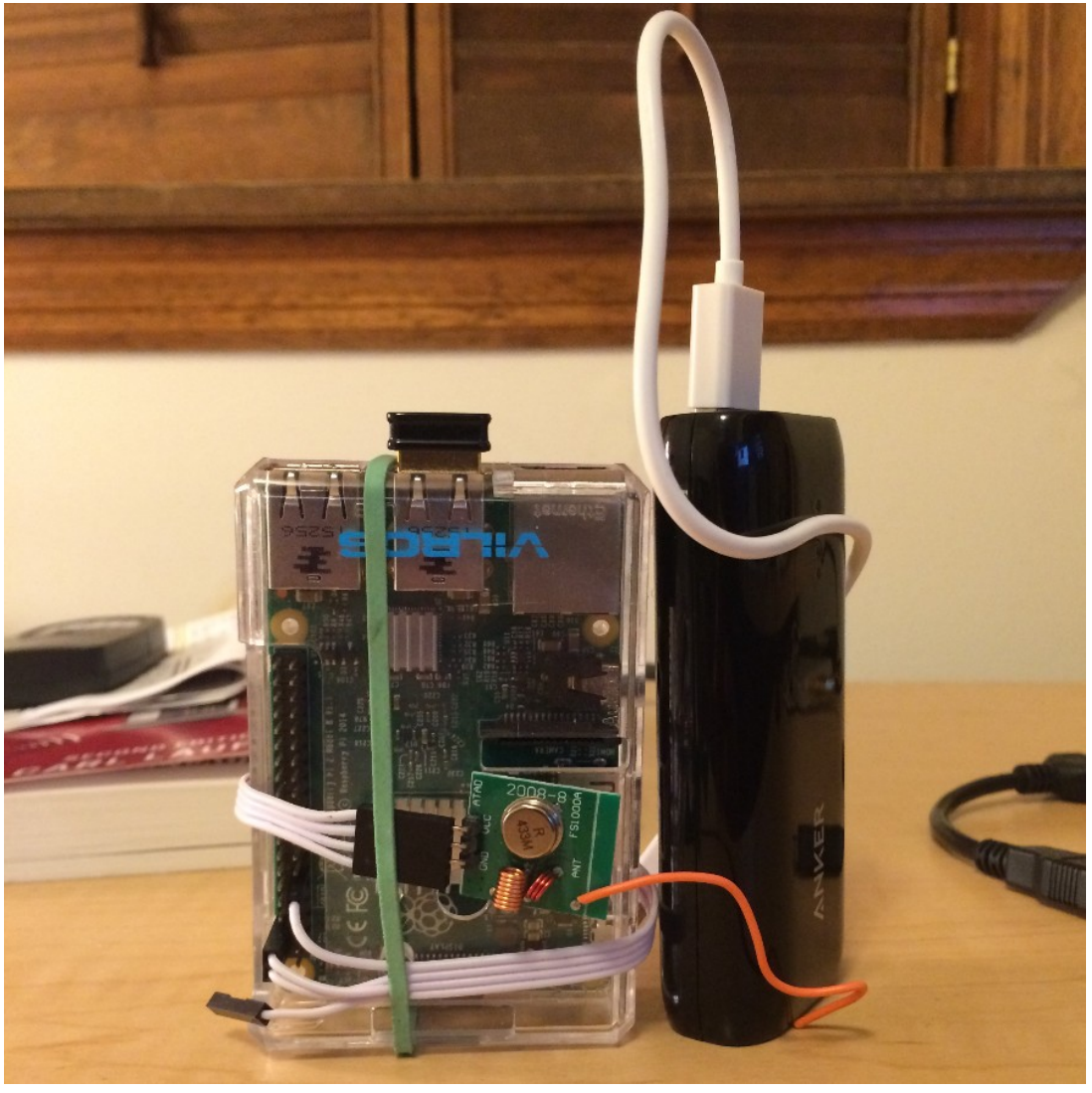
The Fonz: Touchtunes remote for RfCat

https://github.com/notpike/The-Fonz


```
// Each 16bit button code is actually 8bit followed by its complement
const uint8_t button_codes[32] = {
        0x32,   // Pause
        0x78,   // On/Off
        0x70,   // P1
        0x60,   // P2
        0xCA,   // P3
        0x20,   // F1
        0xF2,   // Up
        0xA0,   // F2
        0x84,   // Left
        0x44,   // OK
        0xC4,   // Right
        0x30,   // F3
        0x80,   // Down
        0xB0,   // F4
        0xF0,   // 1
        0x08,   // 2
        0x88,   // 3
        0x48,   // 4
        0xC8,   // 5
        0x28,   // 6
        0xA8,   // 7
        0x68,   // 8
        0xE8,   // 9
        0x18,   // Music_Karaoke
        0x98,   // 0
        0x58,   // Lock_Queue
        0xD0,   // Zone 1 Vol+
        0x90,   // Zone 2 Vol+
        0xC0,   // Zone 3 Vol+
        0x50,   // Zone 1 Vol-
        0x10,   // Zone 2 Vol-
        0x40,   // Zone 3 Vol-
```

https://github.com/furrtek/portapack-havoc/blob/master/firmware/application/apps/ui_touchtunes.hpp

The Jukebox is Yours Now



Demo

Gqrx (tuning)
Dump1090 (airplanes)
Rtlamr (smart meters)
Multimon-ng (pagers)
Rtl_433 (sensors)

Questions

Correst my mistakes? (Baud not baud rate)