

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 **Elionics 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

SEE SOMETHING NEW, EVERY DAY.

TAKE A LOOK

Search

All rt-sdr

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 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

amazon music 3 MONTHS FOR \$0.99 OFFER ENDS TOMORROW Starts at \$7.99/month after

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

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

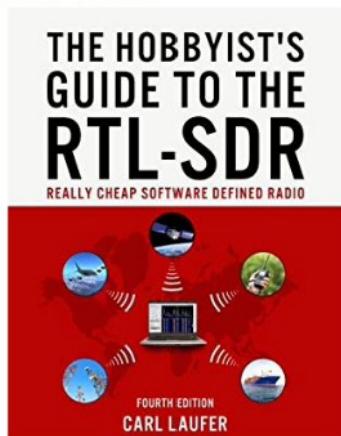
Other Sellers on Amazon

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

1st Edition

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

★★★★★ (216)



Format Paperback



\$23⁷⁰

\$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).

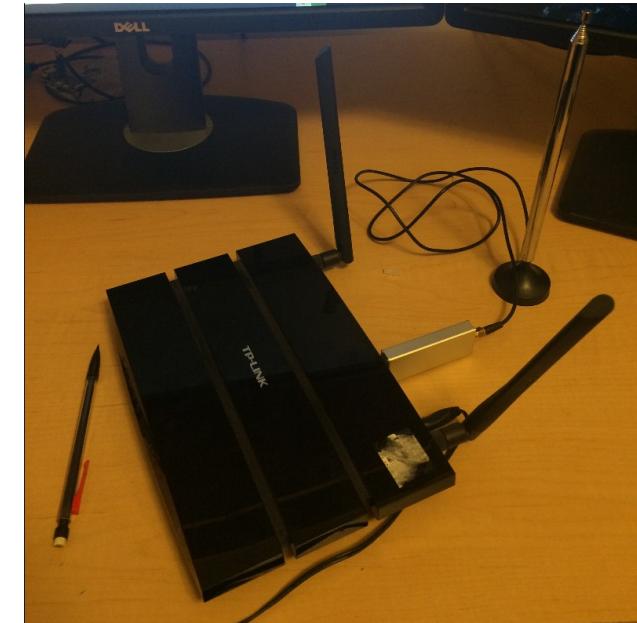
Embedded Linux Friendly



Android Apps



Raspberry Pi
Beagle Bone

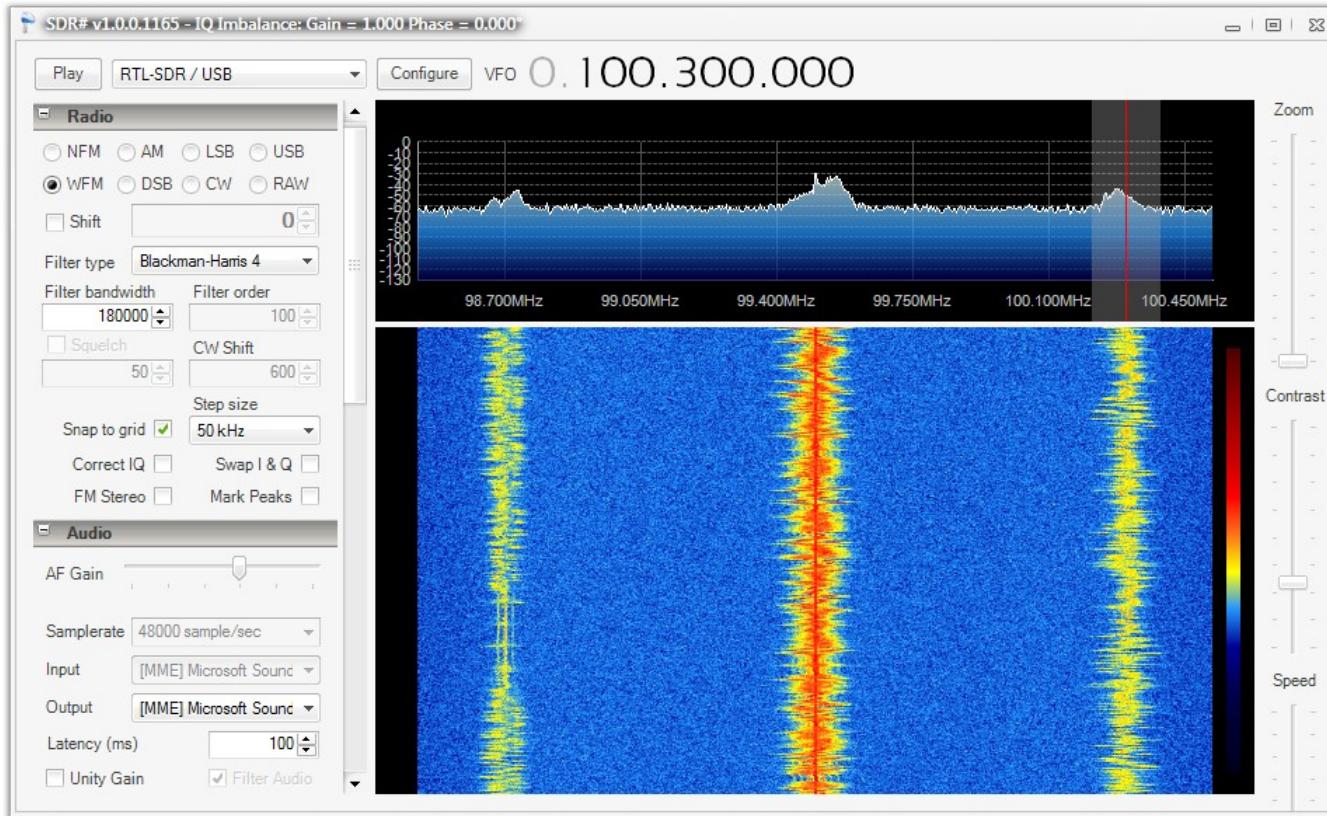


Wifi Router (OpenWrt)

Minimal Software Tools

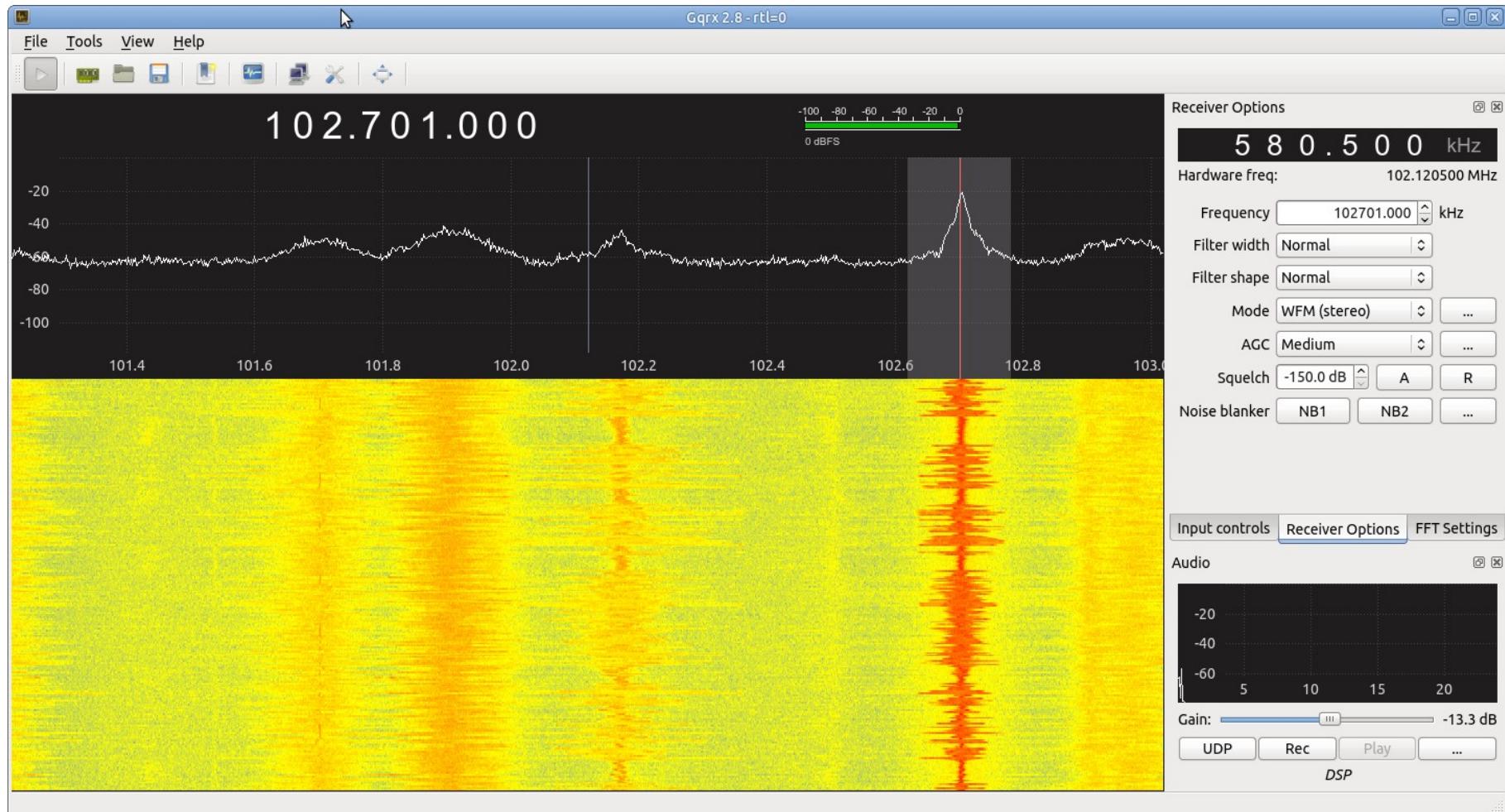
GUI Tuners

For Windows: SDR Sharp aka SDR#



GUI Tuners

For Linux: GQRX



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

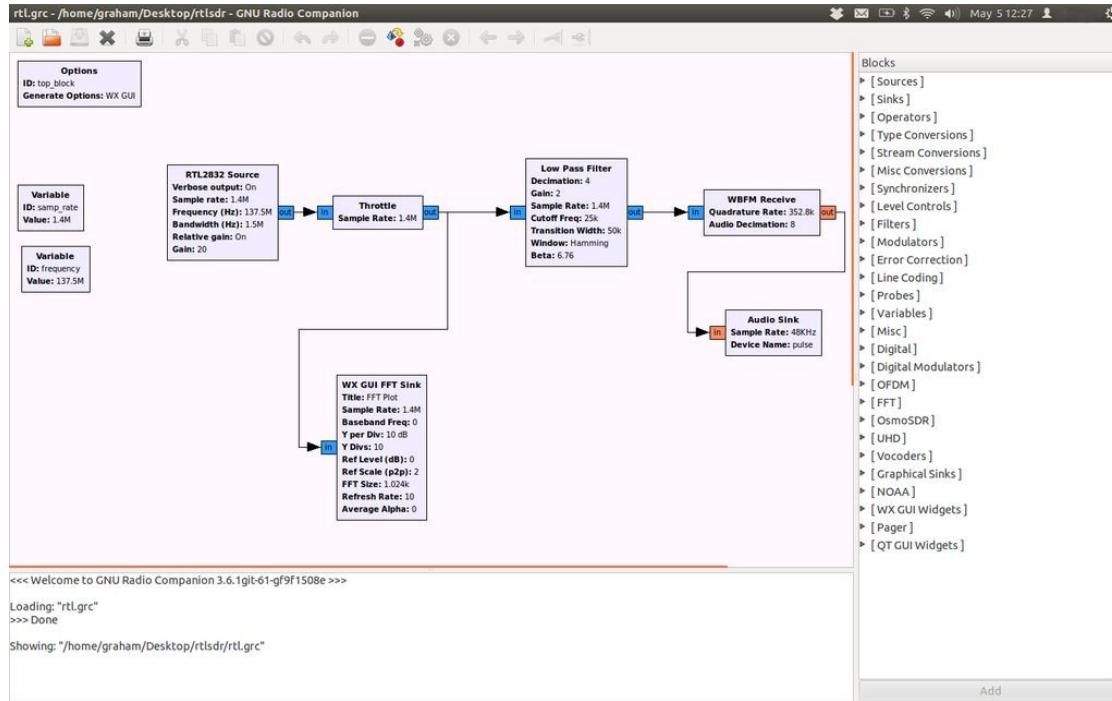
A lot of these tools already in Kali Linux. Radio flavors of Linux OS too (e.g. SigintOS <https://www.sigintos.com/>)



Very powerful, but steep learning curve

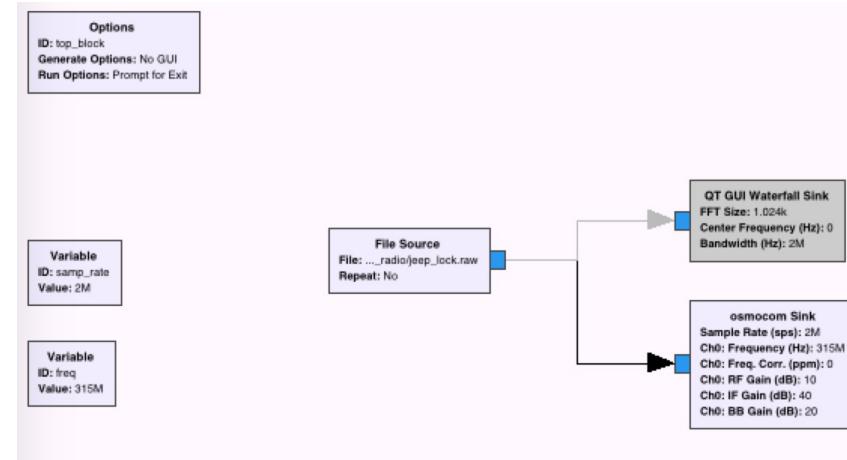
Simple FM Tuner

<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

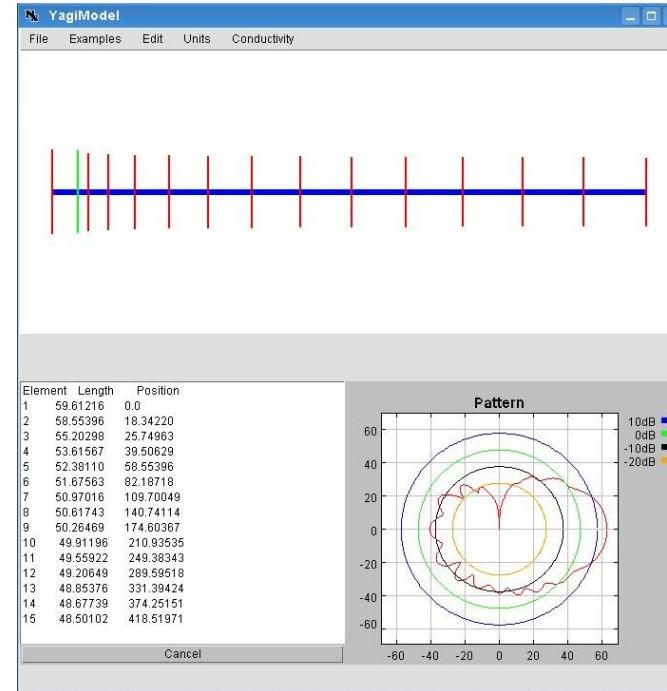


Copper wire from
Lowes or Home Depot

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 Tutorial: Receiv... +

https://www rtl-sdr com/rtl-sdr-tutorial-receiving-noaa-weather-satellite-images/

rtl-sdr

RTL-SDR.COM

RTL-SDR (RTL283U) and software defined radio news and projects. Also featuring Airspy, HackRF, FCD, SDRplay and more.

HOME ABOUT RTL-SDR QUICK START GUIDE FEATURED ARTICLES SOFTWARE SIGNAL ID WIKI FORUM RTL-SDR STORE GUIDE BOOK CONTACT

MAY 13, 2013

RTL-SDR TUTORIAL: RECEIVING NOAA WEATHER SATELLITE IMAGES

Everyday multiple NOAA weather satellites pass above you. Each NOAA weather satellite broadcasts an Automatic Picture Transmission (APT) signal, which contains a live weather image of your area. This combined with a good antenna, SDRSharp and a decoding program can be used to download and display these live images several times a day.

This tutorial will show you how to set up a NOAA weather satellite receiving station, which will allow you to gather several live weather satellite images each day. Most parts of this tutorial are also applicable to other software radios, such as the Funcube dongle and HackRF and Airspy, but the RTL-SDR is the cheapest option. Hardware radio scanners can also work, provided the radio has a large IF bandwidth (30 MHz).

Note that if you have success with this tutorial, you may also be interested in [decoding Meteor M N2 weather satellites](#) which provide much higher resolution images. Also, an alternative tutorial for decoding NOAA satellites that uses rtl_fm [can be found here](#).



P25 P1 DIGITAL VOICE DECODING
P25 P2 DECODING WITH OP25
TRUNKED RADIO FOLLOWING
POCSAG PAGER DECODING
TETRA VOICE DECODING
ANALYZING GSM SIGNALS
DRM RADIO DECODING
DECODING 433 MHZ ISM BAND WEATHER STATIONS

erberosSDR
ut Coherent RTL-SDR
RTL-SDR.com and Othernet
Passive Radar
irection Finding
Coming Soon
ck for more info

Facebook Twitter Google+ RSS

WEEKLY NEWSLETTER
Enter your email address...
Subscribe

SEARCH

RECENT POSTS
[SDRplay Spectrum Analyzer Software Updated to V1.0a](#)
[Othernet Dreamcatcher On Sale for Only \\$49](#)
[Building a Transmit/Receive Relay](#)

https://rtl-sdr.com/

RTL-SDR.com Blog

Select Categories to Security

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

Written by admin — Leave a comment — Posted in RTL-SDR, Security — Tagged with IoT, rtl-sdr, rtl2832, rtl2832u, security

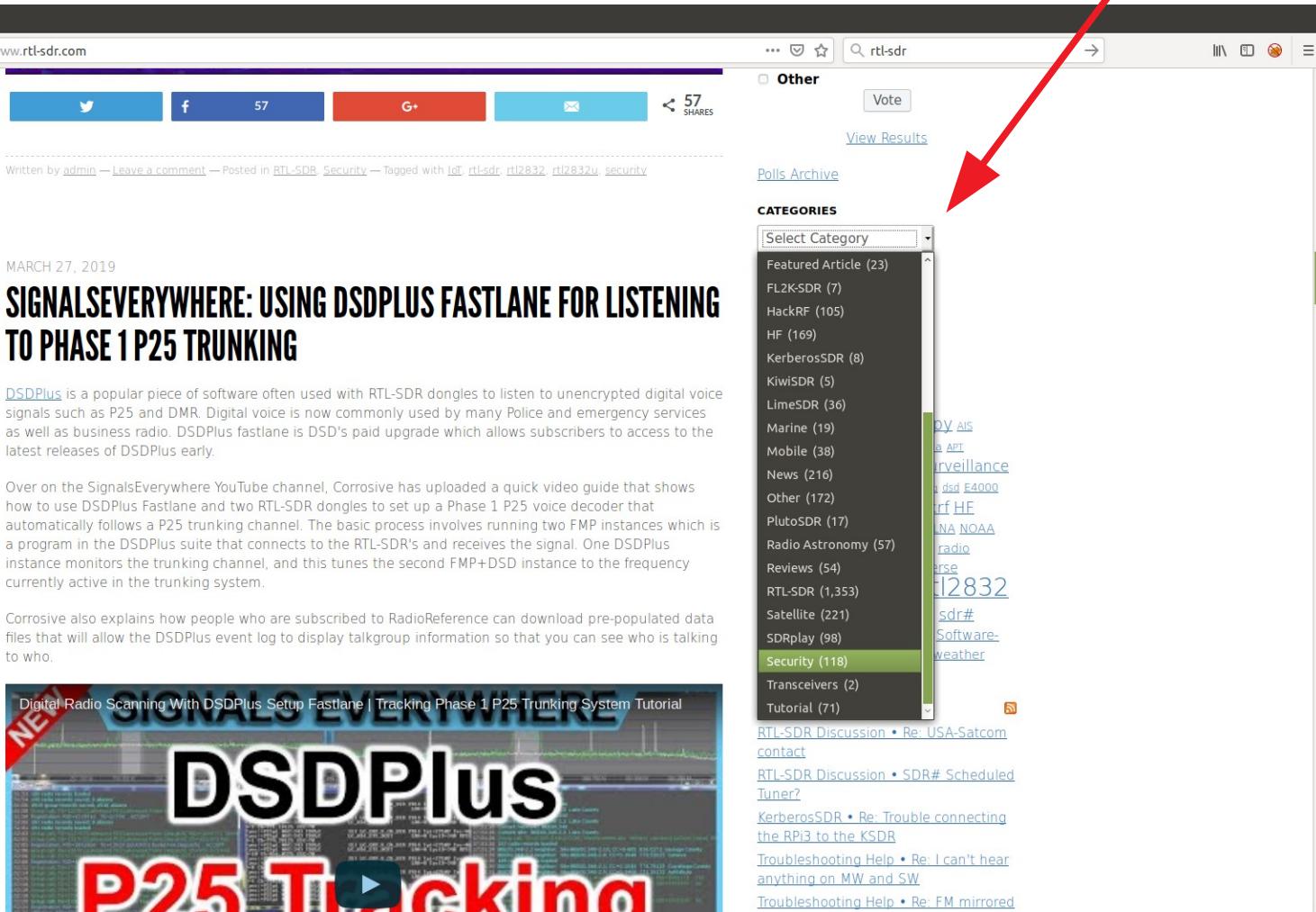
MARCH 27, 2019

SIGNALSEVERYWHERE: USING DSDPLUS FASTLANE FOR LISTENING TO PHASE 1 P25 TRUNKING

DSDPlus is a popular piece of software often used with RTL-SDR dongles to listen to unencrypted digital voice signals such as P25 and DMR. Digital voice is now commonly used by many Police and emergency services as well as business radio. DSDPlus fastlane is DSD's paid upgrade which allows subscribers to access to the latest releases of DSDPlus early.

Over on the SignalsEverywhere YouTube channel, Corrosive has uploaded a quick video guide that shows how to use DSDPlus Fastlane and two RTL-SDR dongles to set up a Phase 1 P25 voice decoder that automatically follows a P25 trunking channel. The basic process involves running two FMP instances which is a program in the DSDPlus suite that connects to the RTL-SDR's and receives the signal. One DSDPlus instance monitors the trunking channel, and this tunes the second FMP+DSD instance to the frequency currently active in the trunking system.

Corrosive also explains how people who are subscribed to RadioReference can download pre-populated data files that will allow the DSDPlus event log to display talkgroup information so that you can see who is talking to who.



The sidebar on the right contains a 'Categories' dropdown menu and a 'Polls Archive' section. The 'Categories' menu lists various topics with their counts: Featured Article (23), FL2K-SDR (7), HackRF (105), HF (169), KerberosSDR (8), KiwiSDR (5), LimeSDR (36), Marine (19), Mobile (38), News (216), Other (172), PlutoSDR (17), Radio Astronomy (57), Reviews (54), RTL-SDR (1,353), Satellite (221), SDRplay (98), **Security (118)**, Transceivers (2), Tutorial (71). Below the categories is a list of recent forum posts:

- RTL-SDR Discussion • Re: USA-Satcom contact
- RTL-SDR Discussion • SDR# Scheduled Tuner?
- KerberosSDR • Re: Trouble connecting the RPi3 to the KSDR
- Troubleshooting Help • Re: I can't hear anything on MW and SW
- Troubleshooting Help • Re: FM mirrored

Common Radio Frequencies

Some databases/frequencies are outdated/obsolete

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

The screenshot shows a web browser window with the title "Common Frequencies" and the URL "https://wiki.radioreference.com/index.php/Common_Frequencies". The page content is a hierarchical list of radio frequency categories:

- Common Consumer and Business
 - Cordless Microphones
 - Cordless Phone
 - Disaster Relief
 - Entertainment
 - Circuses
 - Sports
 - Stage Productions
 - Television and Motion Picture Production
 - Traveling Broadway Shows
 - World Wrestling Entertainment
 - Explosive Demolition
 - Fast Food
 - Arby's
 - Burger King
 - Dairy Queen
 - Dunkin Donuts
 - Hardee's
 - Kenny Rogers Roasters
 - Kentucky Fried Chicken
 - McDonald's
 - Taco Bell
 - Wendy's
 - White Castle
 - Hydrological/Meteorological Channels
 - Marine VHF Channels
 - Marine VHF Band Plans
 - Paging
 - Part 22 Paging Channels
 - Personal Radio Services
 - Citizens Band (CB)
 - Family Radio Service (FRS)
 - General Mobile Radio Service (GMRS)
 - FRS/GMRS combined channel chart
 - Multi-Use Radio Service (MURS)
 - Public Safety
 - 700 MHz Public Safety Band Plan
 - Common Public Safety
 - EMS
 - SECURE
 - Radio Control Frequencies
 - Red Cross - See Disaster Relief
 - SCADA
 - Stores

Digital Voice Comms

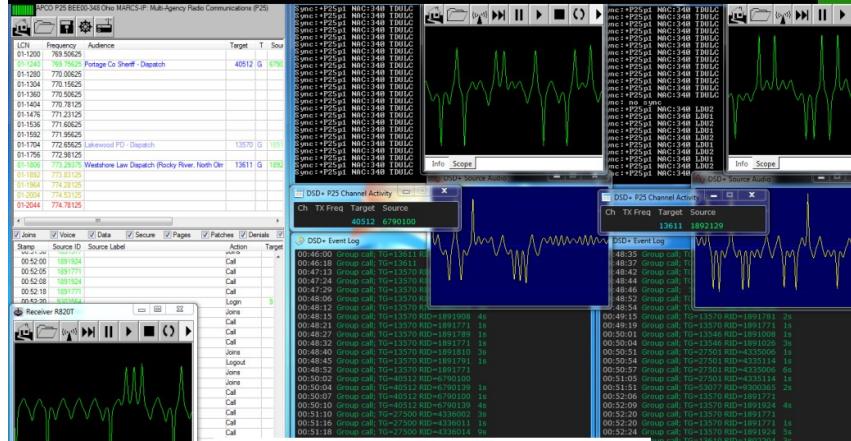
Police and Cordless Phones

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 Frequencies

Radioreference.com Reference Database

The screenshot shows the homepage of Radioreference.com. At the top, there's a navigation bar with links for LOGIN · REGISTER · MOBILE · HELP, social media icons for Facebook, Twitter, and Email, and a SEARCH bar. Below the navigation is the Radioreference.com logo and tagline "Your Complete Reference Source". A prominent banner for "THE UNIDEN SDS100" scanner is displayed, featuring the text "A Revolutionary New Scanner!" and a "Order Now!" button. The main content area has a large "Welcome to Radio Reference" banner with a background image of a radio tower and a green field. To the right of the banner, text states: "RadioReference.com is the world's largest radio communications data provider, featuring a complete frequency database, trunked radio system information, and FCC license data." It also mentions that registration is free and advanced features are available to Premium Subscribers. A "Click Here" link is provided for registration. Below the banner, there are four blue buttons: "Reference Database", "Discussion Forums", "Wiki Reference", and "Live Audio". A red arrow points from the left towards the "Reference Database" button. To the right of these buttons is a "News and Announcements" section listing five recent stories. Further down is an "Active Forum Threads" section with three listed threads. On the far right, there's a "Featured Item" section showing an image of the Uniden Bearcat SDS100 Police Scanner with its details and a descriptive paragraph.

News and Announcements

- 31 Dec 2018 Partial FCC shutdown
- 30 Dec 2018 Last of the scanners: Are police security measures and new technologies killing an American obsession?
- 28 Dec 2018 Communications outage disrupts 911 service in parts of the country
- 17 Dec 2018 New RadioReference Discussion Forums
- 03 Dec 2018 Satellites to Scan for Pirate Radio

[See all stories](#)

Active Forum Threads

- Scanning/troubleshooting Jefferson County/Boulder area 02 Jan 2019 by [jmblodgett](#)
- Trumbull County 02 Jan 2019 by [captmud](#)
- Scanner craziness ... 02 Jan 2019 by [mule1075](#)

Featured Item

Uniden Bearcat SDS100 Police Scanner

The All New Revolutionary Scanner!

This true I/Q Scanner is the first scanner to incorporate Software Defined Radio technology to provide incredible digital performance in even the most challenging RF environments. The SDS100's digital performance better than any other scanner in both simulcast and weak-signal environments. This is the first scanner to signal the end of the notorious digital trunking simulcast.

RadioReference Douglas County Results

Douglas County, Nebraska X + https://www.radioreference.com/apps/db/?ctid=1678 133% radio reference

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>

The screenshot shows a web browser window titled "FCC Search FCC Databases". The URL in the address bar is <https://www.fcc.gov/licensing-databases/search-fcc-databases>. The page content is organized into sections:

- Licensing & Databases** (highlighted in blue)
- [Overview](#)
- [About Licensing](#)
- [Databases](#) (highlighted in blue)
- [Fees](#)
- [Forms](#)
- [FCC Registration System \(CORES\)](#)
- [System Alerts & Notifications](#)

The main content area lists various search interfaces:

- Explore granular search interfaces into more than 40 specialized FCC databases such as radio call signs and equipment authorization.
- AM Radio Station Search
- Antenna Structure Registration – Application Search
- Antenna Structure Registration – Registration Search
- Cable Search
- Call Sign Query
- Children's Programming Report Search
- Consolidated Public Database System – Antenna Search
- Consolidated Public Database System – Application Search
- Consolidated Public Database System – EEO Filing Search
- Consolidated Public Database System – Ownership Report Search
- Consolidated Public Database System – Station Search
- Consumer Complaints Search
- Earth Station Location Search
- EAS Test Reporting System
- ECFS Search – Filings
- ECFS Search - Proceedings
- Electronic ARMSI Filing System
- Electronic Tariff Filing System Search
- Equipment Authorization Search
- Equipment Authorization System Grantee Search
- Equipment Authorization System Pending Application Search
- Equipment Authorization System Test Firm Search
- Experimental Licensing System - Call Sign Search
- Experimental Licensing System - Generic Search
- Experimental Licensing System - Point Radius Search
- FCC Registration Number Search
- FCC Search
- FM Radio Station Search
- Form 327 CARS License Search
- General Menu License Search – By Call Sign
- General Menu License Search – By File Number
- General Menu License Search – By Licensee
- General Menu License Search – By Parent/Child
- General Menu License Search – By Site/Frequency
- International Bureau Application Filing & Reporting System - Search
- Licensing and Management System Search

A red arrow points to the "General Menu License Search – By Site/Frequency" link. In the bottom right corner of the page, there is a small blue circular icon containing a white stick figure.



Site / Market / 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 NLongitude W

S

E

Licensee Name: Wildcard Search: Grant Date: From: Entering only a "From" value will search on licenses granted **prior** to the date.To: Expiration Date: From: If only a "From" date is entered the system will only retrieve records which expire **after** the date.
The date format is mm/dd/yyyyTo:

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.

Sarpy County Results

UP
BCP

Site / Frequency / Market							
Site: 2		Area of Operation: KMRA around a Fixed Location		City: OMAHA, NE		County: SARPY	
Frequency: 464.02500000 469.02500000						Coordinates: 41° 7' 51.6" N, 96° 8' 44.9" W	
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							
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: WNTVZ/6	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: WPOA330	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		Name: GRETNA, NE		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: WQA2496	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		Name: 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		Name: City: Omaha, NE		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 Search FCC Databases | F X +

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

Licensing & Databases

Overview

About Licensing

Databases

Fees

Forms

FCC Registration System (CORES)

System Alerts & Notifications

Explore granular search interfaces into more than 40 specialized FCC databases such as radio call signs and equipment authorization.

- AM Radio Station Search
- Antenna Structure Registration – Application Search
- Antenna Structure Registration – Registration Search
- Cable Search
- Call Sign Query
- Children's Programming Report Search
- Consolidated Public Database System – Antenna Search
- Consolidated Public Database System – Application Search
- Consolidated Public Database System – EEO Filing Search
- Consolidated Public Database System – Ownership Report Search
- Consolidated Public Database System – Station Search
- Consumer Complaints Search
- Earth Station Location Search
- EAS Test Reporting System
- ECFS Search – Filings
- ECFS Search - Proceedings
- Electronic ARMS Filing System
- Electronic Tariff Filing System Search
- Equipment Authorization Search
- Equipment Authorization System Grantee Search
- Equipment Authorization System Pending Application Search
- Equipment Authorization System Test Firm Search
- Experimental Licensing System - Call Sign Search
- Experimental Licensing System - Generic Search
- Experimental Licensing System - Point Radius Search
- FCC Registration Number Search
- FCC Search
- FM Radio Station Search
- Form 327 CARS License Search
- General Menu License Search – By Call Sign
- General Menu License Search – By File Number
- General Menu License Search – By Licensee
- General Menu License Search – By Parent/Child
- General Menu License Search – By Site/Frequency
- International Bureau Application Filing & Reporting System - Search
- Licensing and Management System Search



FCC ID Search

Equipment Authorization Search

FCC OET Authorization S X +

Federal Communications Co... (US) https://apps.fcc.gov/oetcf/eas/reports/GenericSearch.cfm

fcc search

Office of Engineering and Technology

OET Home Page FCC Site Map

Filing Options

- Grantee Registration
- Modify Grantee Information
- Reply to Grantee Name Change Correspondence
- Test Firm Accrediting Body Login
- Return to 159 / Pay for a Grantee registration

Reports

- Pending Application Status
- Authorization Search
- Grantee Search
- Pending Grantee Search
- TCB Search
- Test Firms
- Test Firm Accrediting Bodies
- Equipment Class/Rule Part List

Miscellaneous

- Get FRN
- Knowledge Database
- Hearing Aid Compatibility Status Reporting
- Measurement Procedures

Application Information:

Grantee Code: HYQ (First three or five characters of FCCID)

Product Code: 12BDM Exact Match (Remaining characters of FCCID)

Applicant Name:

Final Action Date Range (mm/dd/yyyy): to

Grant Comments:

Application Purpose:

Software Defined Radios:

FCC Approved Applications Only
TCB Approved Applications Only
Composite Applications Only

Grant Note: & & View Grant Note Descriptions

Test Firm:

Application Status: All Granted Statuses

Equipment Authorization Search

Equipment Information:

Equipment Class:

Frequency Range in MHz: to Exact Match

Necessary Bandwidth:

Emission Designator:

Frequency Tolerance: to Exact Match

Power Output (in Watts): to Exact Match

Rule Parts (up to three): & & Exact Match

Product Description:

Modular Type: Single Modular Approval
Limited Single Modular Approval
Split Modular Approval
Limited Split Modular Approval

OR show all modular OR show all non-modular

FCC ID Search (Alt)

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

The screenshot shows the FCC ID Search page. At the top, there's a navigation bar with links for About the FCC, Proceedings & Actions, Licensing & Databases, Reports & Research, News & Events, and For Consumers. Below the navigation is a breadcrumb trail: Home / Engineering & Technology / Laboratory Division / Equipment Authorization Approval Guide / FCC ID Search.

FCC ID Search Form:

FCC ID Search Form	
Help	Advanced Search
Grantee Code: (First three or five characters of FCCID)	
<input type="text" value="HYQ"/>	
Product Code: (Remaining characters of FCCID)	
<input type="text" value="12BDM"/>	
search	

Advanced Search

To perform an advanced search go to: <https://apps.fcc.gov/oetcf/eas/reports/GeneralSearch.cfm>. The advanced search permits search on a wide range of fields associated with an FCC ID to help find the information on a grant of certification.

FCC ID Search Instructions

- FCC ID numbers consists of two elements, a grantee code and an equipment product code. An FCC ID is assigned to all devices subject to certification.
- The grantee code, the first portion of the FCC ID, is either a three or five character alphanumeric string representing the Grantee/Applicant.
 - Grantee codes that begin with an alphabetic character (A-Z) of three characters in length. The second and third characters may be numbers or alphabetic characters.
 - Grantee codes that begin with a number (2-9) are five characters in length. The second through fifth

Sometimes Find FCC ID Online

e.g. Alarm Systems

RTL-SDR.COM

SimpliSafe

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 RFCA

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 Advanced Share

[eBay](#) > [Business & Industrial](#) > [Facility Maintenance & Safety](#) > [Surveillance & Alarm Equipment](#) > [Alarm Systems & Accessories](#) > [Alarm Control Panels & Keypads](#)

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

Buy It Now Add to cart Make Offer Watch

or Best Offer

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 DMP.COM [f](#) [t](#) [o](#) [in](#) [d](#) [v](#) @DMPALARMS

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
- Open/Close schedules with Closing Check
- Attrition Detection™ monitors system for arming activity
- Built-in English text programming from any keypad
- Arm Only, Ambush Code, and Temporary User Code

INTRUSION PANELS

COMPATIBILITY REFERENCE SHEET

Keypads 7000 Series Thinline Keypads 7000A Series Aquatite Keypads 7300 Series Icon Keypads 7800 Touchscreen Keypads 9000 Wireless Keypads 9800 Wireless Touchscreen Keypads	Monitoring center Receivers SCS-IP Security Control Receiver SCS-105 Single-Line DMP Serial 3 Receiver Compatible with Receivers that accept Standard CID, DMP Serial 3 or Network messaging	1142BC Two-Button Belt Clip Hold-up Transmitter 1144-4 Four-Button Key Fob 1144-ZP Two-Button Key Fob 1144-P One-Button Key Fob 1144-D Dual-Button Key Fob 1148 Personal Pendant 1154 Wireless Four-Zone Input Module	System Specifications Primary Power: 16.5 VAC, 40 VA transformer (Model 321) Secondary Power: 12 VDC Battery
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	SCS-VR (Virtual Receiver) software—only solution that runs on a server for network IP and cellular communications	1158 Wireless 8-Zone Input Module 116-4NS Wireless Smoke Detector with No Sounder 116-6 Wireless Smoke Ring 1183-135F Heat Detector 1183-135R Heat Detector 1184 Carbon Monoxide Detector	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)
Dealer Management Remote Link Programming software Tech APP Dealer Admin	DMP Wireless 1100 Receiver 1100I In-Line Receiver 1100H High-Power Receiver 1100R Repeater 1101 Universal Transmitter, Internal and External Contacts	738A Ademco 32-point Expansion Module 738I ITI 96-point Expansion Module 738Z+ Z-Wave Interface Module 738T Wireless Translator	Enclosures: Material Cold-rolled steel Model 340 (Gray) 12.75" W × 9.5" H × 2.75" D Model 349 (Gray) 12.25" W × 11.75" H × 3.25" D Model 340A (Gray Attack) 13.25" W × 11.3" H × 3.6" D
Cellular 263H HSPA+ Cellular Communicator (AT&T) 263H-CAN HSPA+ Cellular Communicator (AT&T) Canada 263LTE-L V LTE Verizon 263LTE-A LTE AT&T (Coming Soon) 380-400 Replacement Level 400 SIM Card (AT&T) 381-42 12' SMA Coax Cable Extension 381-25 25' SMA Cable Extension 383 External Antenna 384-1 5dBi Fiberglass Antenna 387-2 2dB Attack Enclosure Antenna 387-3 3dBi MEG Antenna	Accessories 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 Announcer 1119 Door Sounder 1121 Pet Immune PIR Motion Detector Wireless PIR 360 Ceiling Mount PIR Wall Mount Curtain PIR	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	
Intrusion Devices DMP is compatible with most standard wireless intrusion devices.	End User Management System Link™ Virtual Keypad.com Virtual Keypad App	FCC Part 15 ID: CCKPC0096 FCC Part 68 Registration ID: CCKAL00BX750 Industry Canada ID: 5151A-PC0096	

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

Google search results for "dmp 1122 fcc id". About 12,000 results found.

[PDF] 1122 wireless pir motion detector - Digital Monitoring Products
<https://buy.dmp.com/dmp/products/documents/LT-1647.pdf>

When programming the 1122 in the panel, refer to the panel programming ... the 1122 needs to sense before going into alarm. 11. Choose ... Use one 3.0V lithium battery, DMP Model CR123A, or FCC Part 15 Registration ID CCK1122.

1122 Wireless Alarm Sounder User Manual Manual Digital ... - FCC ID
[https://fccid.io/Digital Monitoring Products Inc 1122](https://fccid.io/Digital%20Monitoring%20Products%20Inc%201122)

Aug 1, 2017 - 1122 WIRELESS PIR MOTION DETECTOR Installation Guide PROGRAM ... All DMP 1100 Series Wireless Receivers and burglarly panels.

FCC ID CCK1122 Wireless Alarm Sounder by Digital Monitoring ...
[https://fccid.io/Digital Monitoring Products Inc](https://fccid.io/Digital%20Monitoring%20Products%20Inc)

FCC ID CCK1122 (CCK 1122) Wireless Alarm Sounder manufactured by Digital Monitoring Products Inc operating frequencies, user manual, ... Digital Monitoring Products Inc Wireless Alarm Sounder 1122. FCC ... Email: btucker@dmp.com ...

1122 Wireless Alarm Sounder Test Report EMC Digital ... - FCC ID
[https://fccid.io/Digital Monitoring Products Inc 1122](https://fccid.io/Digital%20Monitoring%20Products%20Inc%201122)

Aug 1, 2017 - Wireless Alarm Sounder Test Report details for FCC ID CCK1122 made by ... DMP FCC Part 15.247 max level 20 dB Model # - 1122PIR ...

[PDF] 1125 Motion Spec Sheet.pdf
www.alarmhow.net/manuals/DMP/Wireless/1125%20Motion%20Spec%20Sheet.pdf

Two-Way Supervised Wireless from DMP delivers unparalleled ... Seamless integration with DMP Command Processor™ FCC Part 15 Registration ID. Missing: 1122 | Must include: 1122

Digital Monitoring Products 1122 Installation Manual - ManualsLib
[https://www.manualslib.com/.../Security Sensors](https://www.manualslib.com/.../Security%20Sensors)

View and Download Digital Monitoring Products 1122 installation manual online. ... Use only a 3.0V lithium battery, DMP Model CR123A, or the ... Specifications Certifications Battery FCC Part 15 Registration ID CCK1122 Life Expectancy 3 ...

FCC OET Authorization Search Results for FCC ID CCK1122.

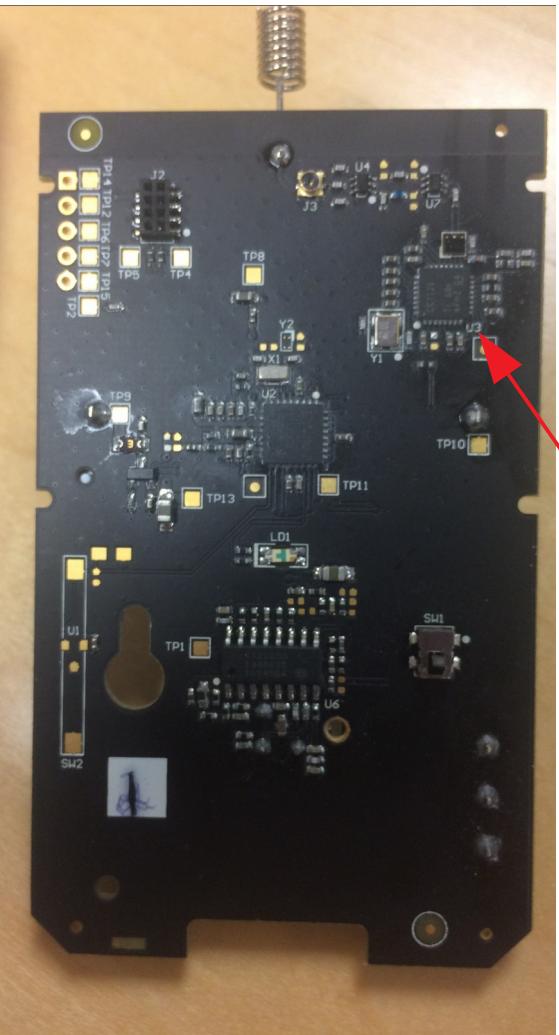
View Form	Display Exhibits	Grant	Corresp.	Name Conidence	Applicant	Address	City	State Country	Zip Code	FCC ID	Application Purpose	Final Action Date	Lower Frequency in MHz	Upper Frequency in MHz
Detail	Summary				Digital Monitoring Products Inc	2500 N. Partnership Boulevard Springfield MO United States	65803	CCK1122	Original Equipment	08/01/2017	905.6	924.4		

OET List Exhibits Report for FCC ID CCK1122.

View Attachment	Exhibit Type	Date Submitted to FCC	Display Type	Date Available
Letter of Agency	Cover Letter(s)	08/01/2017	pdf	08/01/2017
Confidentiality Request Letter	Cover Letter(s)	08/01/2017	pdf	08/01/2017
External Photos	External Photos	08/01/2017	pdf	08/01/2017
ID Label	ID Label/Location Info	08/01/2017	pdf	08/01/2017
Label Location	ID Label/Location Info	08/01/2017	pdf	08/01/2017
Internal Photos	Internal Photos	08/01/2017	pdf	08/01/2017
Test Report	Test Report	08/01/2017	pdf	08/01/2017
Test Setup Photos	Test Setup Photos	08/01/2017	pdf	08/01/2017
Manual	Users Manual	08/01/2017	pdf	08/01/2017

Internal Photos & Test Report has the good stuff

Internal Photos



DMP 1122 Wireless PIR Alarm System Recon

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:	<input checked="" type="checkbox"/> 902-928MHz	<input type="checkbox"/> 2400-2483.5MHz	<input type="checkbox"/> 5725-5850MHz
Measured Separation (kHz)	Limit (kHz)	Result	
362.18	74.1	Pass	
Limit:	<input checked="" type="checkbox"/> 25kHz	<input type="checkbox"/> 20dB channel bandwidth	<input type="checkbox"/> 2/3 of 20dB channel bandwidth
Span:	1 MHz		
RBW:	<input type="checkbox"/> 3kHz	<input checked="" type="checkbox"/> 10kHz	<input type="checkbox"/> 100kHz
VBW:	<input type="checkbox"/> 3kHz	<input checked="" type="checkbox"/> 30kHz	<input type="checkbox"/> 100kHz
		<input type="checkbox"/> other	kHz
		<input type="checkbox"/> other	kHz

3.4 Number of hopping frequencies

Frequency Range:	<input checked="" type="checkbox"/> 902-928MHz	<input type="checkbox"/> 2400-2483.5MHz	<input type="checkbox"/> 5725-5850MHz
Measured Number	Requirements	Result	
53	50	Pass	
Channel 20dB Bandwidth:	<input checked="" type="checkbox"/> <250kHz	<input type="checkbox"/> ≥250kHz	

3.5 Average time of occupancy of hopping frequency

Frequency Range:	<input checked="" type="checkbox"/> 902-928MHz	<input type="checkbox"/> 2400-2483.5MHz	<input type="checkbox"/> 5725-5850MHz
Measured / Calculated Time sec	Period sec	Limit sec	Result
0.3	20	0.4	Pass
Period:	<input type="checkbox"/> 10s	<input checked="" type="checkbox"/> 20s	<input type="checkbox"/> 30s
		<input checked="" type="checkbox"/> 0.4s multiplied by the channel number	
Channel 20dB Bandwidth:	<input checked="" type="checkbox"/> <250kHz	<input type="checkbox"/> ≥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	919.6391
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

Multiple Address System X SIG Signal Identification Wiki X + https://www.sigidwiki.com/wiki/Signal_Identification_Guide signal wiki ↗

FREQUENCY BANDS

VLF	LF	MF	HF	VHF	UHF
12	22	29	196	96	113

CATEGORIES

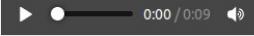
All Identified Signals			Unidentified Signals		
Military	Radar	Common/Active	Rare/Inactive	Amateur Radio	Commercial
Aviation	Marine	Analogue	Digital	Trunked Radio	Utility
Satellite	Navigation	Interfering Emissions	Requested	Numbers Stations	Time

Stats

Identified Signals in Database: **362**
Unidentified Signals to be Identified: **239**
Requested Signals: **52**

Recently Added Signals	Recently Updated Signals
<ul style="list-style-type: none">■ 2019-01-04 11:38:50 Unknown signal■ 2018-12-31 08:07:45 IMet-1 RS Radiosonde■ 2018-12-29 07:13:21 Possibly a RADAR?■ 2018-11-30 20:16:03 WSPR■ 2018-11-08 09:12:00 R580	<ul style="list-style-type: none">■ 2019-01-04 12:26:54 SIGFOX■ 2019-01-04 11:38:49 Unknown signal■ 2019-01-03 20:18:00 CIS MFSK-20 XPA■ 2019-01-01 12:06:05 Yaesu System Fusion■ 2018-12-31 08:18:45 IMet-1 RS Radiosonde

Signal ID Wiki

SIG Utility Signals - Signal Idx								
	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

SIG CompuLert - Signal Ideni X + https://www.sigidwiki.com/wiki/CompuLert 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

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

Video Examples [edit]

- Siren test (CompuLert signals can be heard as siren activates) [\(embed\)](#)
- Colerain, OH sirens [\(embed\)](#)

Additional Links [edit]

- KB9UKD Digital Modes [\(embed\)](#)
- American Signal Corporation, CompuLert System [\(embed\)](#)
- Wikipedia: American Signal Corporation (ASC) [\(embed\)](#)

Additional Images [edit]

Categories: Signal | Digital | UHF | Active | Utility

CompuLert

Frequencies 453.375 MHz
Frequency 453.375 MHz - 453.375 MHz
Range —

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

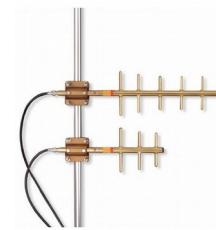


Siren Jack: <https://www.sirenjack.com/> (ATI Systems)

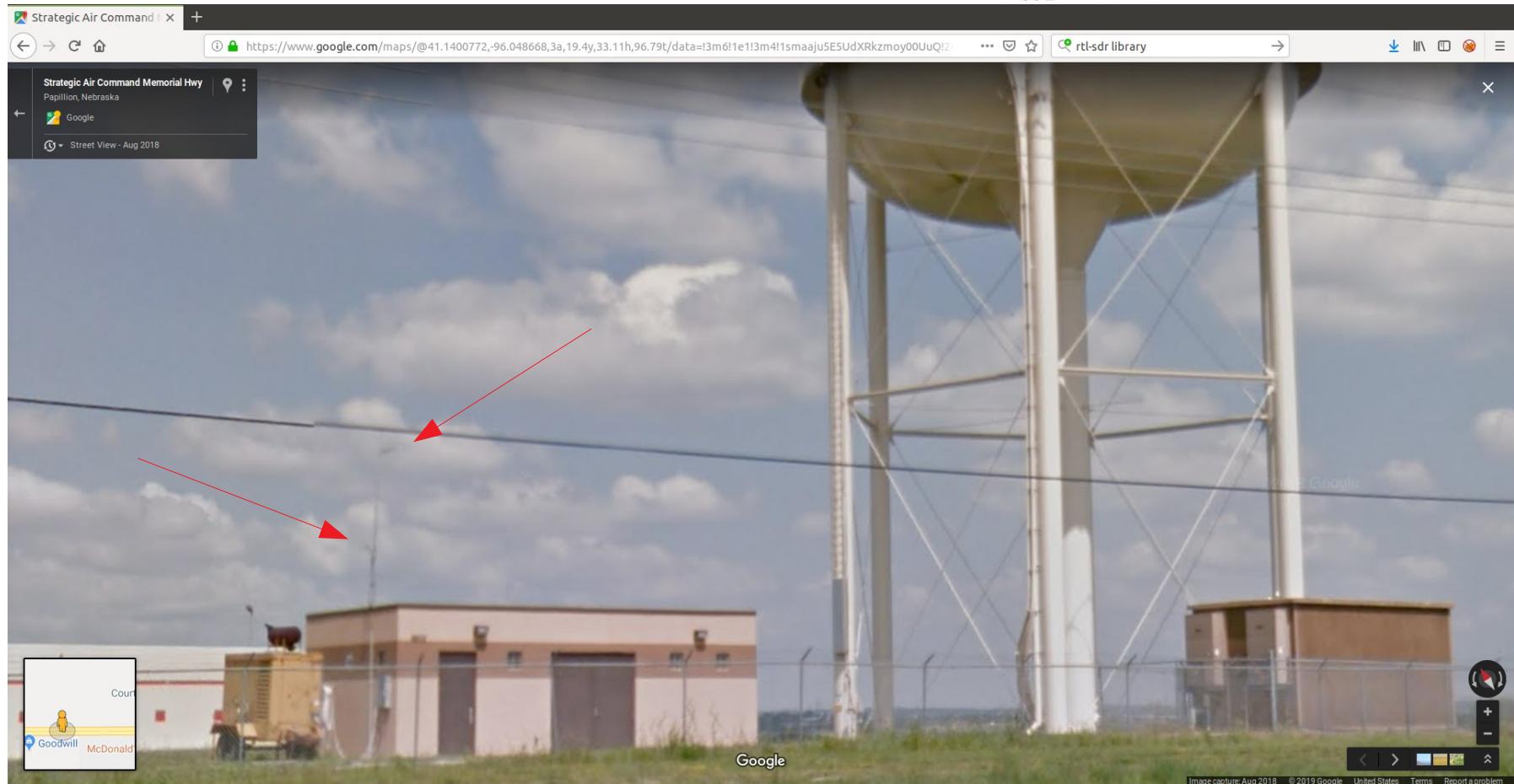
Utility Antennas Everywhere

MAS (Multiple Address Service) SCADA

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



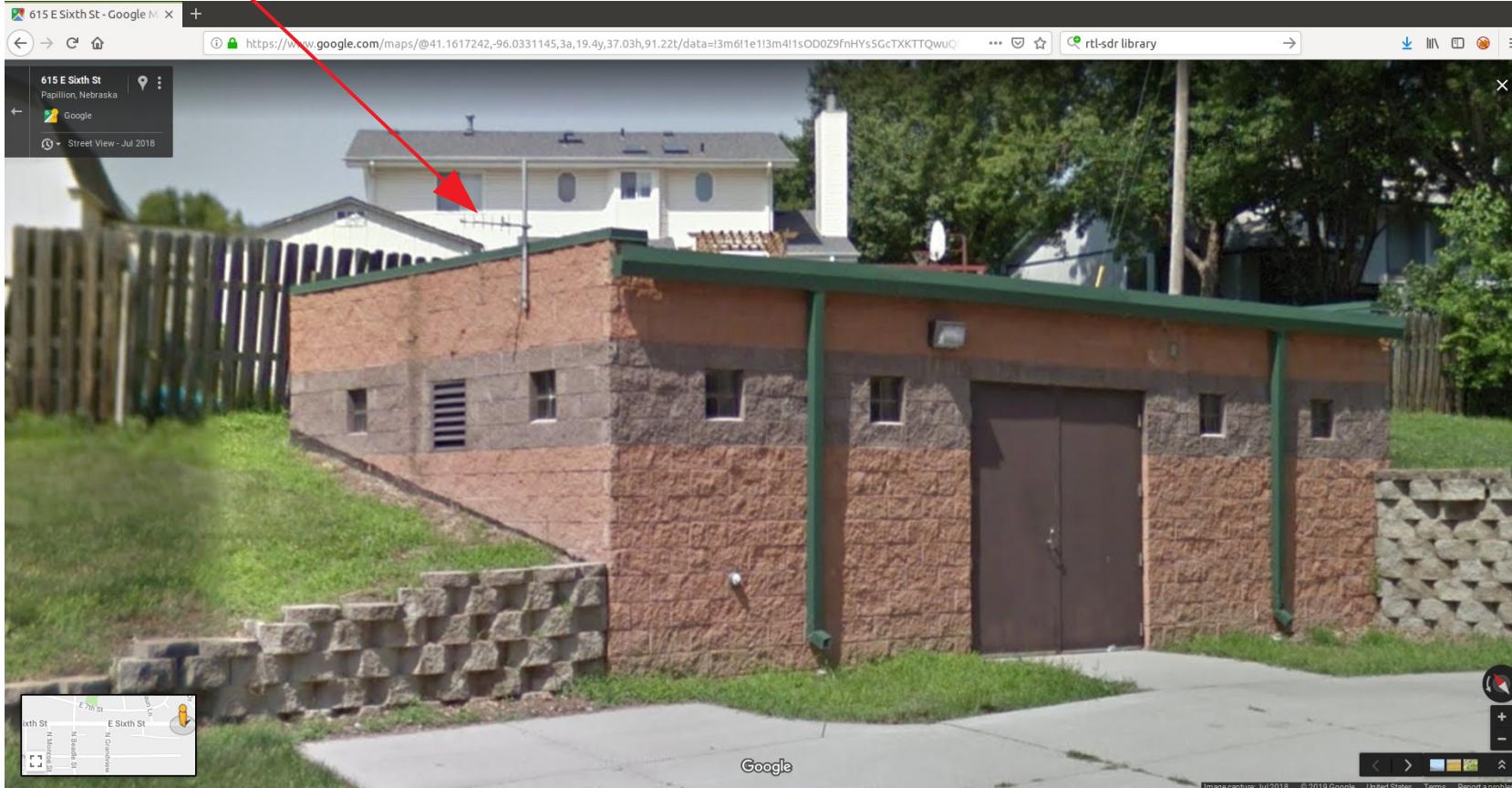
~900MHz Yagi



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/e_Sarpy-County-Appendix(reduced).pdf

81 of 178

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 186 th Street (South of Hwy 370)
Funding	General Fund (Sewer)
Year Completed	2010

Google Search:
Sarpy scada

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

Telemetry Antennas USGS Streamgage GOES15 Weather Satellite Uplink 401.8MHz

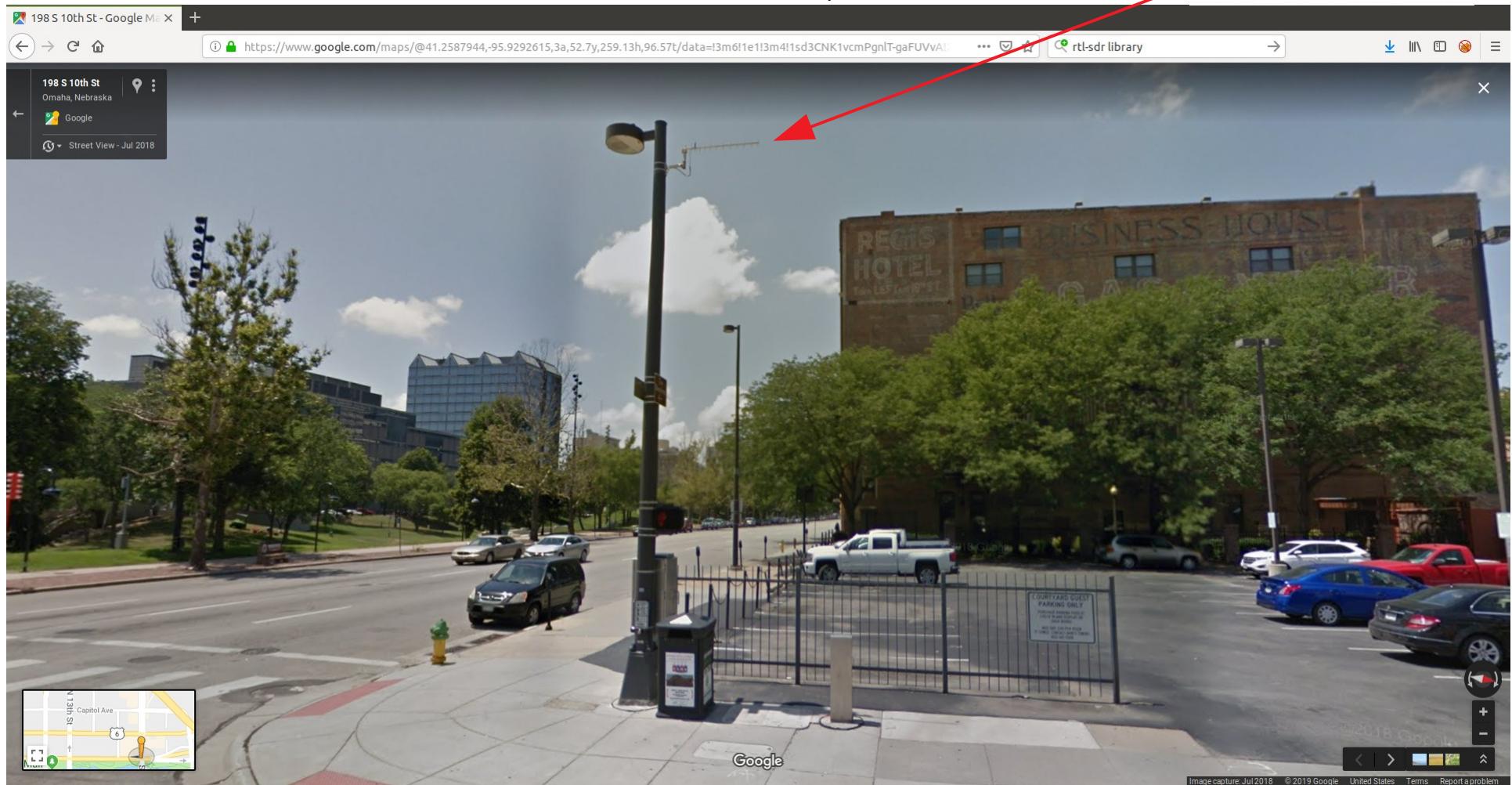


Omaha Traffic Lights

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



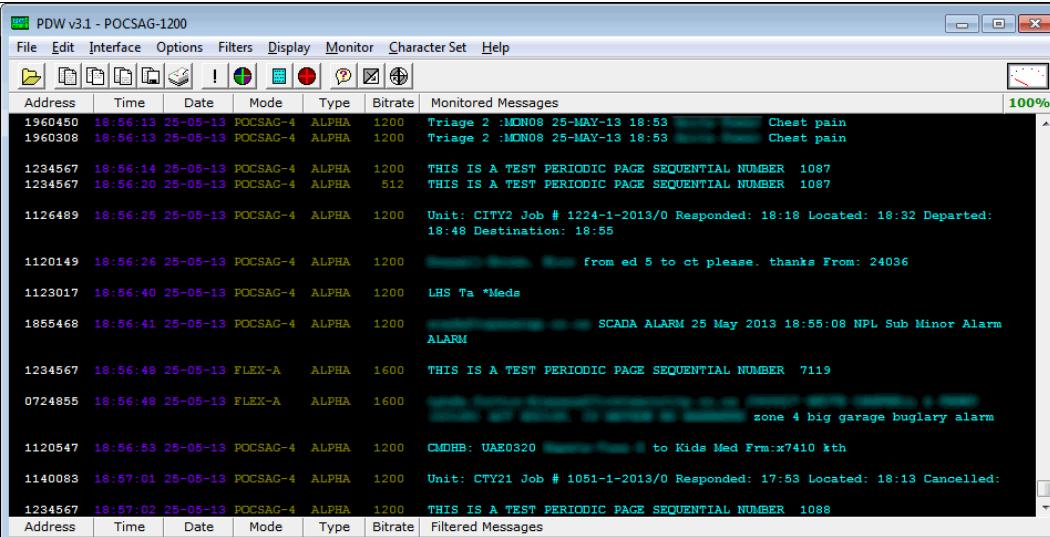
Buy on
ebay



A Google Street View screenshot showing a street scene in Omaha, Nebraska. The address 198 S 10th St is visible in the top left corner. A red arrow points from the Encom Serial Modem image to a street lamp post on the sidewalk. The post has an antenna mounted on it. In the background, there's a large brick building with a sign that reads "REGIS HOTEL" and "BUSINESS HOUSE". The sky is blue with some clouds. A small inset map in the bottom left corner shows the location relative to Capitol Ave and 10th St.

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 - wireless/pocsag_ambulance.wav
multimon-ng  (C) 1996/1997 by Tom Sailer HB9JNX/AE4WA
(C) 2012-2014 by Elias Oenal      Remote site: /home/www-data/wirelessness
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      ? scripts
POCSAG1200: Address: 1876594 Function: 1      ? software
POCSAG1200: Address: 1483379 Function: 1      ? training-common-sense
POCSAG1200: Address: 1309718 Function: 0 Numeric: 1 6.0U. 0.3785401.4663.5 2603.5.00
POCSAG1200: Address: 1309718 Function: 0 Alpha: AMBULANCE (2641104)<NULL>
POCSAG1200: Address: 1309718 Function: 0 Skyper: @LATK@MBD-US>'15300/3?
POCSAG1200: Address: 2010229 Function: 1      POCSAG-protocol.pdf
POCSAG1200: Address: 1712758 Function: 1      POCSAG-encoded.png
POCSAG1200: Address: 401702 Function: 2 Numeric: 663.5 2603.5.00
POCSAG1200: Address: 1089601 Function: 3      belgian_pager_multimon_ng_169.6mhz.png
POCSAG1200: Address: 177721 Function: 0 Numeric: -.U28061309]04.-4797-567[-3 7]UU10
POCSAG1200: Address: 177721 Function: 0 Alpha: ZW 01 : Ziekenwagen<NULL>
POCSAG1200: Address: 177721 Function: 0 Skyper: YV<US>/0<US>9<US>Yhdjdmv`fdm?
POCSAG1200: Address: 2044535 Function: 0      ARIEL
```

Multimon-ng for Linux

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

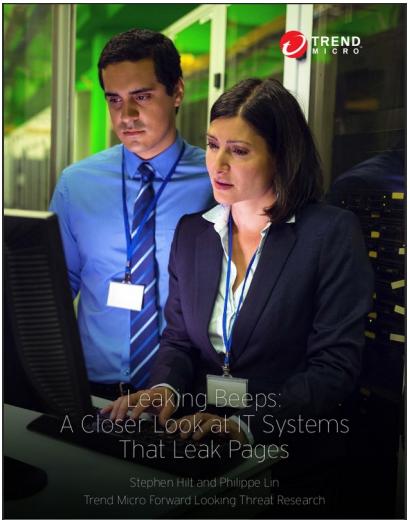
<https://tools.kali.org/wireless-attacks/multimon-ng>

<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



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

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

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

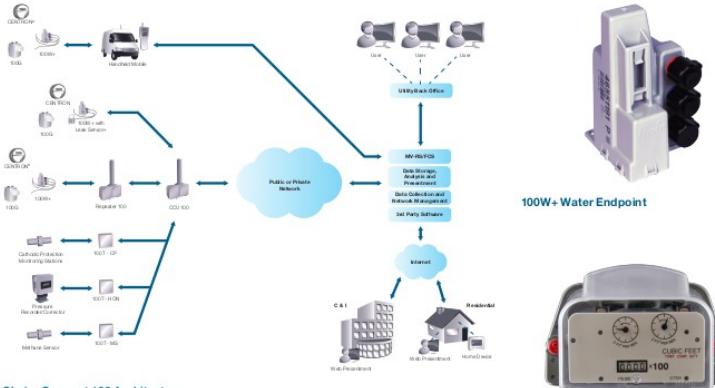
<https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-leaking-beeps-healthcare.pdf>

<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

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.



CCU 100



CENTRON C1SR Electricity Meter



100G DLN ERT Module



100W+ Water Endpoint

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



Smart Meter Cover RF
\$69.95
Smart Meter Cover RF...
Amazon.com



Smart Meter Cover
\$97.00
BioElectric Shie...
Amazon.com



Smart Meter Guard EMF
\$129.95
Amazon.com
★★★★★ (17)



Smart Meter Shield Radiation
\$29.95
eBay
★★★★★ (17)
Rank Shops



Utility Meters

RTLAMR Screenshot Smart (AMR) Meters

```
cobraboss@loonlake:~$ rtlamr rtlamr
16:13:42.809123 decode.go:45: CenterFreq: 912600155
16:13:42.810628 decode.go:46: SampleRate: 2359296
16:13:42.810651 decode.go:47: DataRate: 32768
16:13:42.810670 decode.go:48: ChipLength: 72
16:13:42.810688 decode.go:49: PreambleSymbols: 21
16:13:42.810705 decode.go:50: PreambleLength: 3024
16:13:42.810723 decode.go:51: PacketSymbols: 96
16:13:42.810741 decode.go:52: PacketLength: 13824
16:13:42.810762 decode.go:59: Protocols: scm
16:13:42.810780 decode.go:60: Preambles: 111110010101001100000
16:13:42.810800 main.go:114: GainCount: 29
{Time:2019-01-02T16:13:44.506 SCM:{ID:23908760 Type: 7 Tamper:{Phy:02 Enc:01} Consumption: 5113108 CRC:0x44AF}}
{Time:2019-01-02T16:13:45.168 SCM:{ID:65464279 Type: 7 Tamper:{Phy:02 Enc:01} Consumption: 386856 CRC:0x8837}}
{Time:2019-01-02T16:13:46.115 SCM:{ID:65598349 Type: 7 Tamper:{Phy:02 Enc:02} Consumption: 3167361 CRC:0xB8B7}}
{Time:2019-01-02T16:13:48.280 SCM:{ID:23952902 Type: 7 Tamper:{Phy:02 Enc:01} Consumption: 2152836 CRC:0x9682}}
{Time:2019-01-02T16:13:49.672 SCM:{ID:30441747 Type:13 Tamper:{Phy:00 Enc:00} Consumption: 48759 CRC:0x3CC4}}
{Time:2019-01-02T16:13:51.671 SCM:{ID:65749048 Type: 7 Tamper:{Phy:02 Enc:01} Consumption: 4606828 CRC:0x2664}}
{Time:2019-01-02T16:13:52.449 SCM:{ID:65717300 Type: 7 Tamper:{Phy:02 Enc:02} Consumption: 7748552 CRC:0x6570}}
{Time:2019-01-02T16:13:53.449 SCM:{ID:21489469 Type: 7 Tamper:{Phy:02 Enc:01} Consumption: 4575830 CRC:0x13EB}}
{Time:2019-01-02T16:13:54.447 SCM:{ID:65457695 Type: 7 Tamper:{Phy:02 Enc:01} Consumption: 2456027 CRC:0xA7B4}}
{Time:2019-01-02T16:13:54.503 SCM:{ID:65610246 Type: 7 Tamper:{Phy:00 Enc:03} Consumption: 7538850 CRC:0xF70B}}
{Time:2019-01-02T16:13:57.673 SCM:{ID:47517999 Type:12 Tamper:{Phy:03 Enc:00} Consumption: 766156 CRC:0x62B2}}
{Time:2019-01-02T16:13:58.004 SCM:{ID:39132296 Type:12 Tamper:{Phy:00 Enc:00} Consumption: 755800 CRC:0x817E}}
{Time:2019-01-02T16:13:58.391 SCM:{ID:46703184 Type:12 Tamper:{Phy:00 Enc:00} Consumption: 578188 CRC:0x1BF6}}
{Time:2019-01-02T16:13:59.112 SCM:{ID:59977459 Type: 7 Tamper:{Phy:02 Enc:01} Consumption: 5708416 CRC:0x4400}}
{Time:2019-01-02T16:14:01.446 SCM:{ID:47518025 Type:12 Tamper:{Phy:00 Enc:00} Consumption: 69336 CRC:0xA9AC}}
{Time:2019-01-02T16:14:02.060 SCM:{ID:23279959 Type: 7 Tamper:{Phy:02 Enc:01} Consumption: 9356747 CRC:0x9482}}
{Time:2019-01-02T16:14:02.558 SCM:{ID:46449412 Type:12 Tamper:{Phy:00 Enc:00} Consumption: 384140 CRC:0x19D7}}
{Time:2019-01-02T16:14:02.616 SCM:{ID:59977436 Type: 7 Tamper:{Phy:02 Enc:03} Consumption: 9291655 CRC:0x371E}}
{Time:2019-01-02T16:14:02.668 SCM:{ID:65393803 Type: 7 Tamper:{Phy:02 Enc:01} Consumption: 1473042 CRC:0x6ED3}}
{Time:2019-01-02T16:14:02.671 SCM:{ID:23951166 Type: 7 Tamper:{Phy:03 Enc:00} Consumption: 4306944 CRC:0xD86A}}
{Time:2019-01-02T16:14:03.227 SCM:{ID:65520412 Type: 7 Tamper:{Phy:03 Enc:01} Consumption: 8916746 CRC:0x7078}}
{Time:2019-01-02T16:14:03.338 SCM:{ID:65393664 Type: 7 Tamper:{Phy:02 Enc:01} Consumption: 8152051 CRC:0x0559}}
{Time:2019-01-02T16:14:05.446 SCM:{ID:65378577 Type: 7 Tamper:{Phy:02 Enc:01} Consumption: 3667019 CRC:0x0A14}}
{Time:2019-01-02T16:14:05.614 SCM:{ID:65717260 Type: 7 Tamper:{Phy:02 Enc:01} Consumption: 5751100 CRC:0xA9FD}}
{Time:2019-01-02T16:14:05.728 SCM:{ID:45423404 Type: 7 Tamper:{Phy:02 Enc:00} Consumption: 3146239 CRC:0xC26C}}
{Time:2019-01-02T16:14:06.169 SCM:{ID:23964070 Type: 7 Tamper:{Phy:01 Enc:01} Consumption: 2024140 CRC:0xAE8F}}
```

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/eldrac0/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 decrease the t nPress 'm' to toggle sound, or 'q'Current Time: 2018-01-15 18:34:19.021088
```

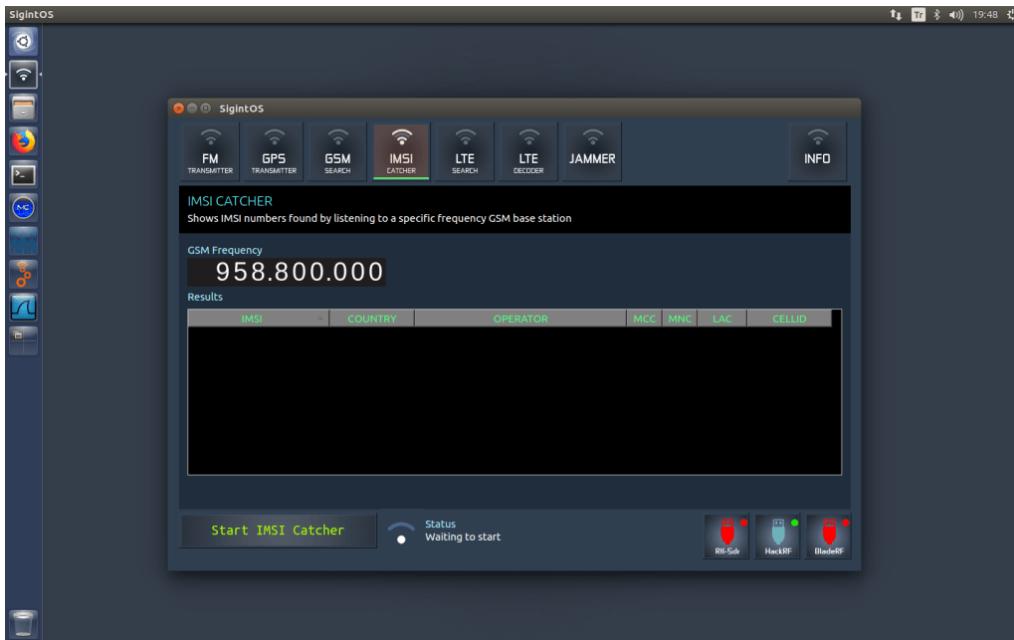
Wireless IDS & Tracking

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

HACKADAY

HOME BLOG HACKADAY.IO TINDIE HACKADAY PRIZE SUBMIT ABOUT

LTE IMSI CATCHER

by: Michael Uttmark 18 Comments May 30, 2017

camp.hsbp.org

Tracking Area Update Reject

- UE sends a Tracking Area Update Request
- Rogue eNodeB rejects it with cause 9

#9 (UE identity cannot be derived by the network);

The UE shall set the EPS update status to EU2 NOT UPDATED (and shall store it according to subclause 5.1.3.3) and shall delete any GUTI, last visited registered TAI, TAI list and the state EMM-DEREGISTERED.

<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/furrtrek/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>



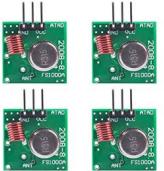
CC1110/CC1111 Dev Board, ~\$75

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>



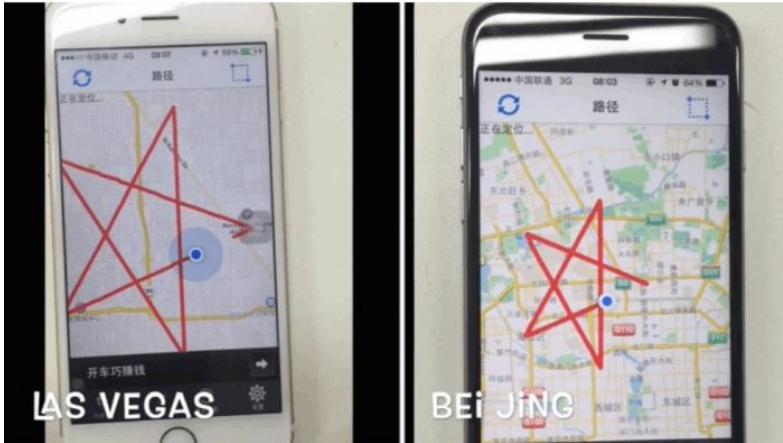
USB3 VGA Dongle (FL2000) HF – 157MHz ~ 1.7GHz, \$5

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

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

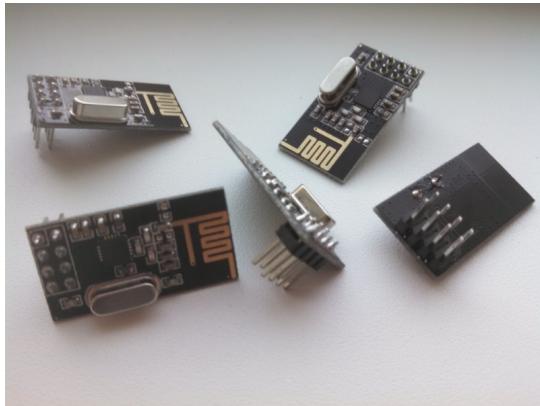
<https://www rtl-sdr.com/cheating-at-pokemon-go-with-a-hackrf-and-gps-spoofing/>

Drone Hacking

Or nRF24L01 sniffing

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/>

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

Exploit List

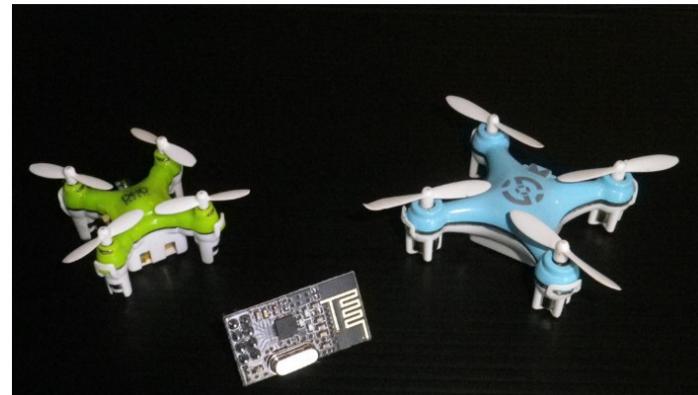
<https://medium.com/@swalters/how-can-drones-be-hacked-the-updated-list-of-vulnerable-drones-attack-tools-dd2e006d6809>

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.](#)



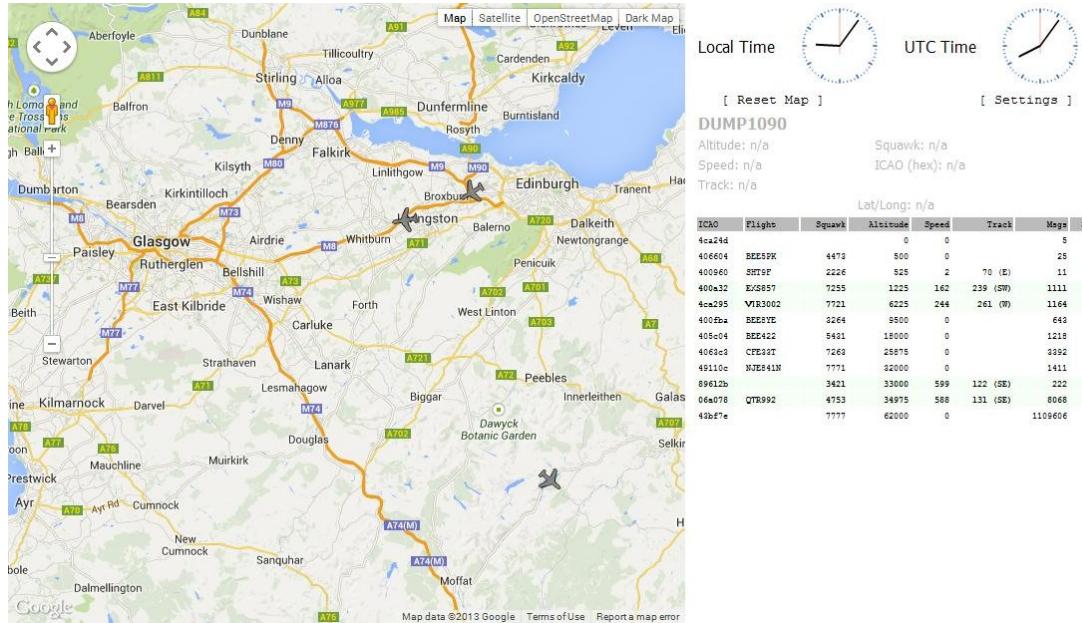
Aircraft Tracking

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	BEE267	19125					38	6845	0
400984	S	4622	EZE2BZ	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



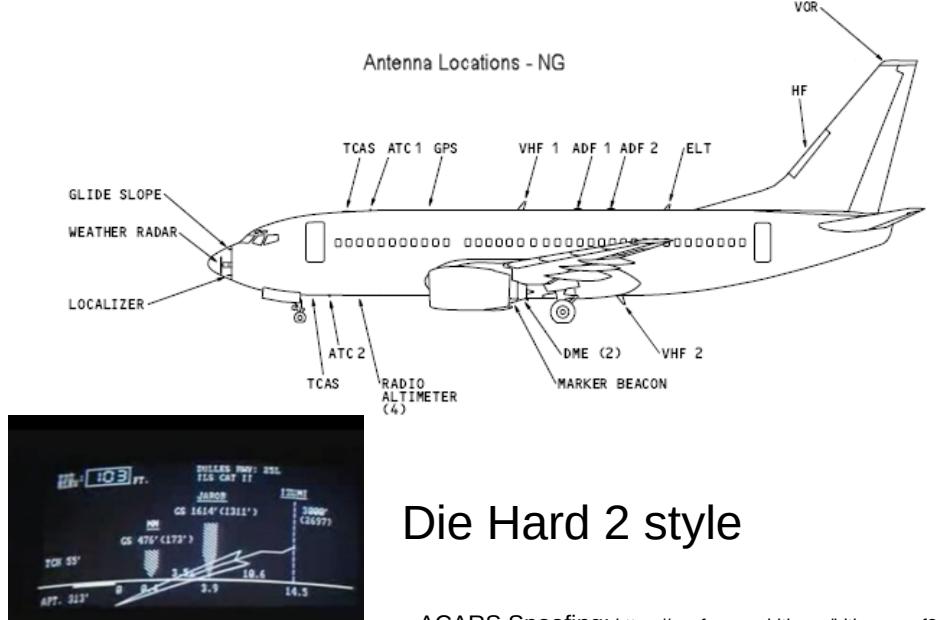
ADS-B Beacon Spoofing is easy: DoS Air Traffic Control Displays (RpiTx Throwie/Drone)

<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

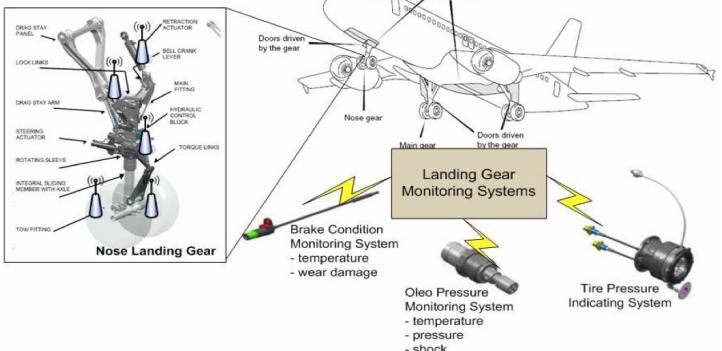
<https://www.iata.org/whatwedo/ops-infra/air-traffic-management/PublishingImages/Pages/radio-spectrum/aviation-usages-of-frequency-spectrum.pdf>

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

Bands	Frequency Spectrum	Aviation Usages	Types of Services	Remarks(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	ARNS	At risk - UK OfCom is proposing a shared use with wireless A/V system. Possible European-wide extension. IATA submitted comments.
	1 164 – 1 215 MHz	Airborne collision avoidance system (ACAS)	ARNS/RNSS	Note: Allocation for Earth-satellite link of ADS-B at WRC-15.
	1 215 – 1 400 MHz	DME/Global Navigation Satellite System (GNSS)	ARNS	GPS (L1)/GLONASS (L5)/Galileo (E5a)/BeiDou (B2a, B2)
	1 525 – 1 559 MHz	Primary Surveillance Radar (PSR)	ARNS	
	1 559 – 1 610 MHz	Satellite Communications (FANS)	MSS (space-Earth)	
	1 610 – 1 626.5 MHz	GNSS	ARNS/RNSS	GPS (L1), GLONASS
	1 626.5 – 1 660.5 MHz	Satellite Communications (Iridium)	AMS(R)S (s-, e-, =)	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.
	2 700 – 3 300 MHz	Satellite Communications (FANS)	MSS (earth-space)	This AMS(R)S allocation does not support civil aviation requirement.
UHF or S	3 400 – 4 200 MHz	PSR Metereological RADAR	ARNS RNS/RLS	
	4 200 – 4 400 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	5 000 – 5 250 MHz	Radio Altimeter Wireless Avionics Intra-Communications (WAIC)	ARNS	To monitor - Mobile phone requested adjacent frequency @ WRC-15.
	5 350 – 5 470 MHz	Microwave Landing System (MLS) UAS CNPC/Airport Surface Communication (AeroMACS)	AM(R)S/AMS(R)S	Allocation for WAIC at WRC-15.
	8 750 – 8 850 MHz	Airborne weather radar	ARNS/RLS	Also used for airborne ground mapping.
SHF or X	9 000 – 9 500 MHz	Precision Approach Radar (PAR)/Airborne weather radar/ASDE	ARNS/RNS	Also used for airborne ground mapping. Airborne Doppler radar is used to determine aircraft ground distance, speed and drift angle.
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/hitbseccf2013ams/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>

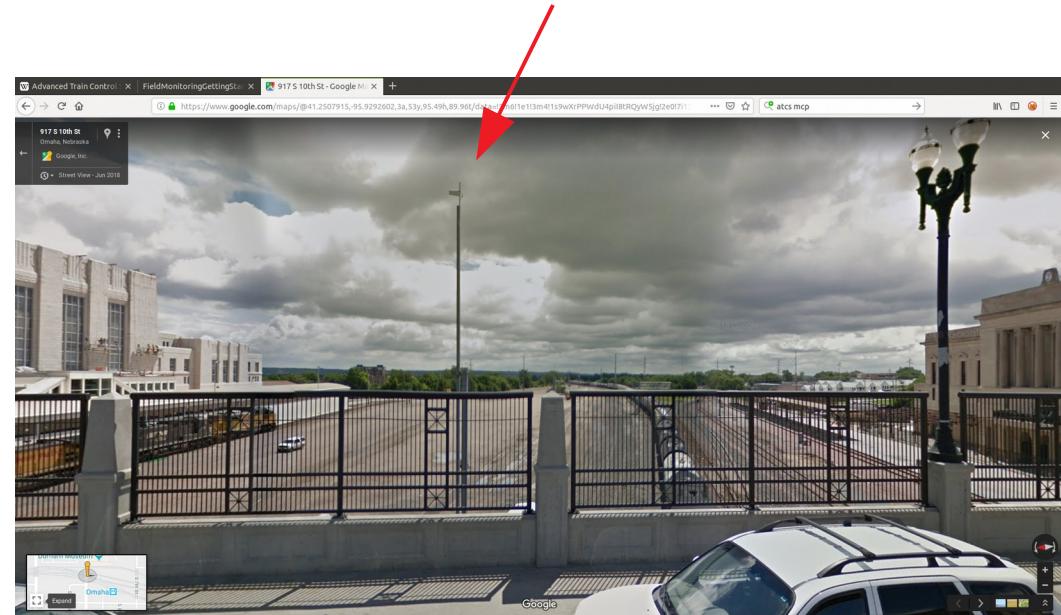
UP uses Genisys system.

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

ATCS Monitor - Ft Wayne

File Edit View Actions Configure Help

Type MCP Datagram User Data Received

9.2.11	Hadley	[40 00] 7RWK	2006/01/16 00:27:18
9.2.11	Union	[41] EGK,NWK	2006/01/16 00:27:18
9.2.11	Runnion	[10 00 00 00] 1NWK	2006/01/16 00:27:18
9.2.11	Piqua	[41] EGK,NWK	2006/01/16 00:27:18
9.2.11	Mike	[09 21 61 0E] 2EAK,1NWK,4LZK,2NWK,1EGK,1WAK,3NWK,4RWK,1LZK	2006/01/16 00:27:18
9.2.11	Piqua	[41] EGK,NWK	2006/01/16 00:27:22

Active MCP Window

Address	Name	Indications	ISeqErr	Controls	CSeqErr	Other	Last Packet
75502240290202	Union	1	0%				2006/01/16 00:27:18
75502240300202	Piqua	2	0%				2006/01/16 00:27:22
75502240320202	Mike	1	0%				2006/01/16 00:27:18
75502430020202	Runnion	1	0%				2006/01/16 00:27:18
75502430100202	Hadley	1	0%				2006/01/16 00:27:18

Packet Display

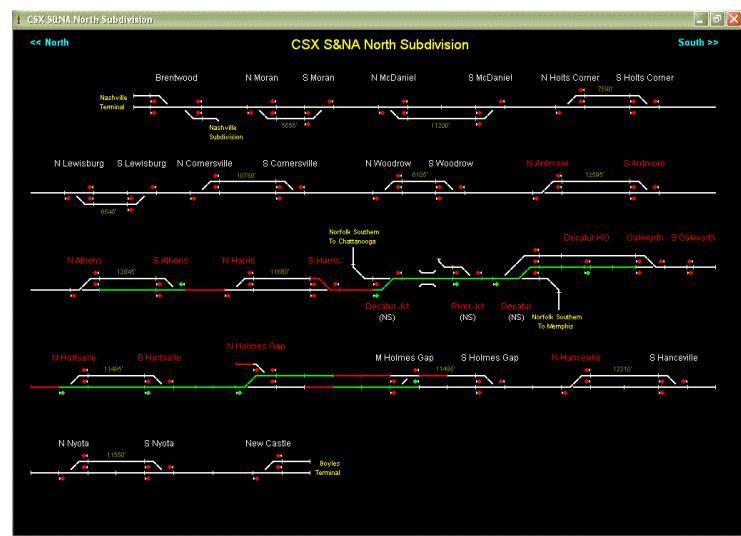
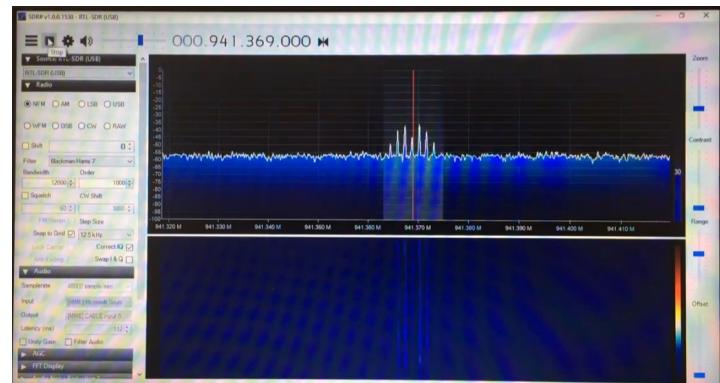
Wayside MCP: 75502430100202 (Hadley)

2006/01/16 00:27:18
NW Datagram (1) Inbound to Ground
Frame=36 GFI=6 Group=8 SSeq=124 R:
To Dispatch: 2550105243
Number=9.2.11 CODELINE_INDICATION,
Mnemonics="7RWK"
23 0C 05 9E D4 68 00 F8 00 EA 25 :
3A 1A A2 A2 00 66 02 02 12 8B 03 :
Wayside MCP: 75502240300202 (Piqua)

2006/01/16 00:27:22
NW Datagram (1) Inbound to Ground
Frame=35 GFI=6 Group=8 SSeq=93 R:
To Dispatch: 2550305224
Number=9.2.11 CODELINE_INDICATION,
Mnemonics="EGK,NWK"
23 14 05 CF 8F 68 00 BA 00 EA 25 :
4A 3A A2 A2 00 BA 02 02 12 8B 03 :

Monitoring

Errors: 1 of 7 (14%) 12:27 AM



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

UP Omaha Terminal

UP Omaha Terminal

Blair, Columbus, Omaha, and Falls City Subs

Voice Frequencies:

Blair, Falls City, and Omaha Subs - 160.740 (AAR 042)

Sioux City Sub - 161.175 (AAR 071)

Protocols:

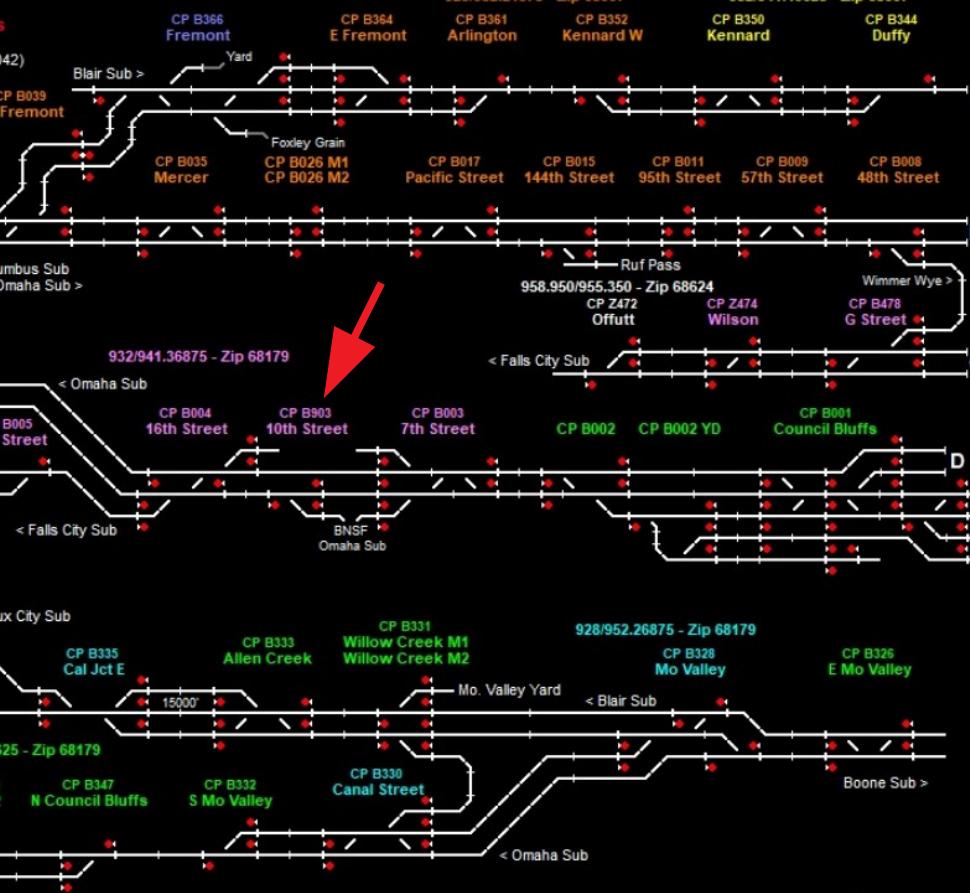
Zip 68179 - Genysis RFL

Zip 68007 & 68624 - Genysis 202T 1200

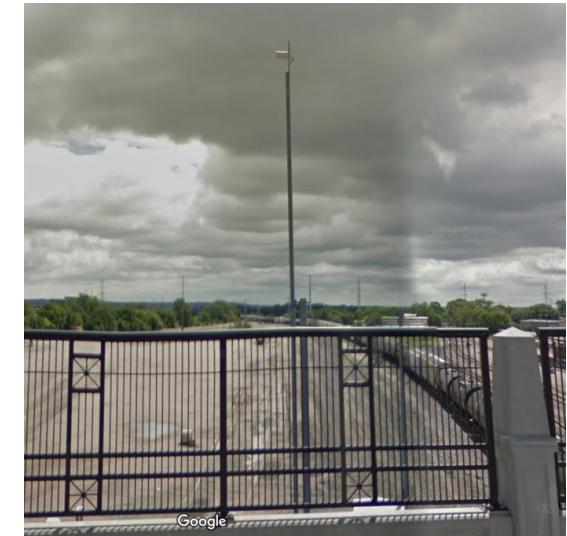
928/952.14375 - Zip 68624

CP B049 Best

CP B040



Updated 12/15/2016



On-board Train Telemetry

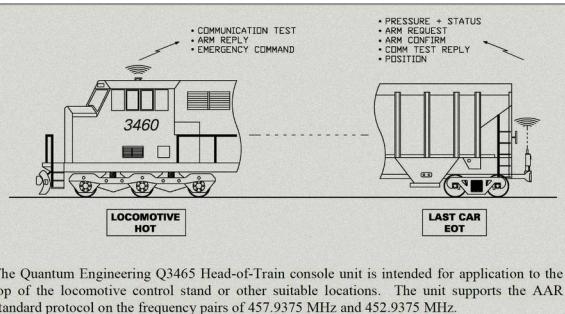
Transmits Brake Pressure &
Accidental Train Separation

~452MHZ



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	1	OK		0	1	NML	1	0
2014/02/01 19:56:12	0.5	EOT	44777		60	0	1	1	OK		0	1	NML	1	1
2014/02/01 19:56:15	0.5	EOT	44777		60	0	1	1	OK		0	1	NML	1	1
2014/02/01 19:56:17	0.4	EOT	43075		0	0	1	1	OK	20	1		NML	1	0
2014/02/01 19:56:23	0.4	EOT	76527		85	1	1	1	OK	30	1		NML	1	0
2014/02/01 19:56:27	0.4	EOT	76527		85	1	1	1	OK	30	1		NML	1	1
2014/02/01 19:56:31	0.4	EOT	76832		90	1	1	1	OK	0	1		NML	1	0
2014/02/01 19:56:35	0.4	EOT	76832		89	1	1	1	OK	0	1		NML	1	1
2014/02/01 19:57:11	0.3	EOT	44777		60	0	1	1	OK	0	1		NML	1	0
2014/02/01 19:57:13	0.3	EOT	43075		0	0	1	1	OK	20	1		NML	1	0
2014/02/01 19:57:28	0.3	EOT	76527		85	1	1	1	OK	30	1		NML	1	0
2014/02/01 19:57:37	0.3	EOT	76832		89	1	1	1	OK	0	1		NML	1	0
2014/02/01 19:58:10	0.2	EOT	44777		61	0	1	1	OK	0	1		NML	1	0

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



Rail Automation
Head of Train Device
Locomotive Onboard Equipment



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



Key Fob Hacking

RollJam

Rolling Code Remote Keyless Entry (RKE)

1) One-way RKE



rolling code N



verifies against window of valid codes

N-1
N
N+1
N+2
N+3
N+4

Jam & replay attack



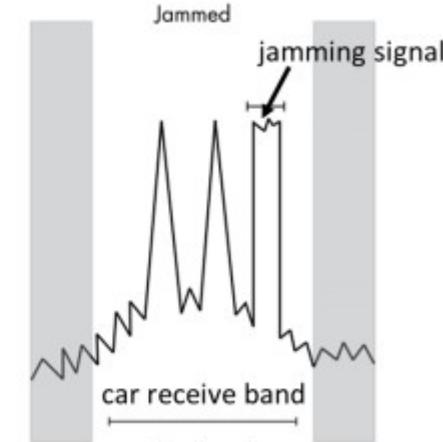
rolling code



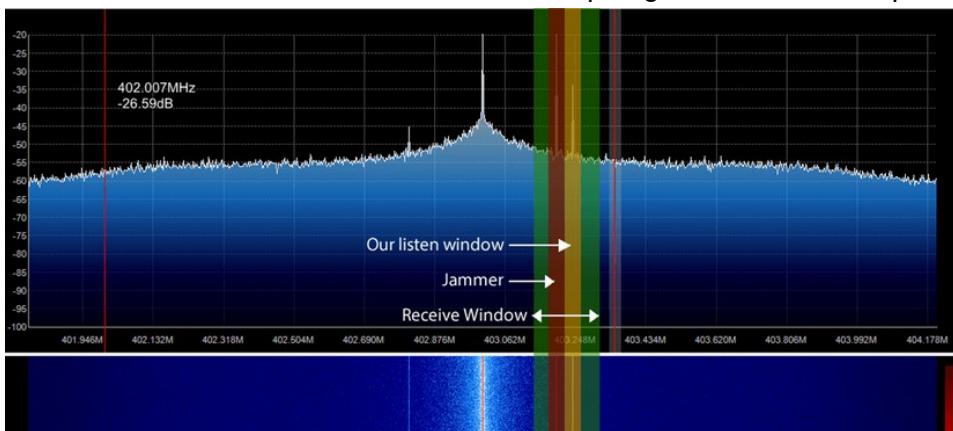
receive antenna



jamming signal / replay antenna



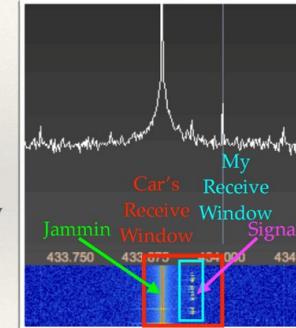
<https://github.com/trishmapow/rf-jam-replay>



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

Jam+Listen(1), Jam+Listen(2), Replay (1)

- ♦ Jam at slightly deviated frequency
- ♦ Receive at frequency with tight receive filter bandwidth to evade jamming
- ♦ User presses key but car can't read signal due to jamming
- ♦ User presses key again — you now have **two** rolling codes
- ♦ Replay first code so user gets into car, we still have second code



<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)



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

Robbed in seconds: Car-jammers in SA

2017-06-14 08:28

SHARE: [f](#) [t](#) [g+](#) [e](#)

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-jammering tactics in SA as well as valuable advice for motorists.

Signal Jamming



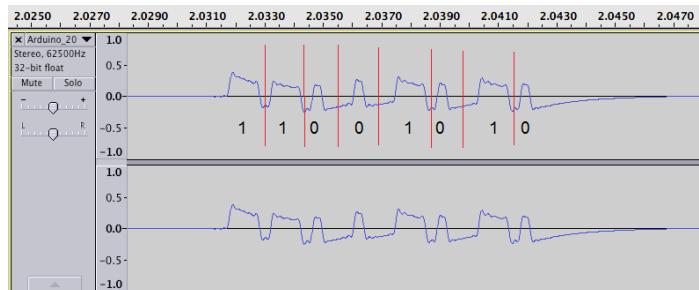
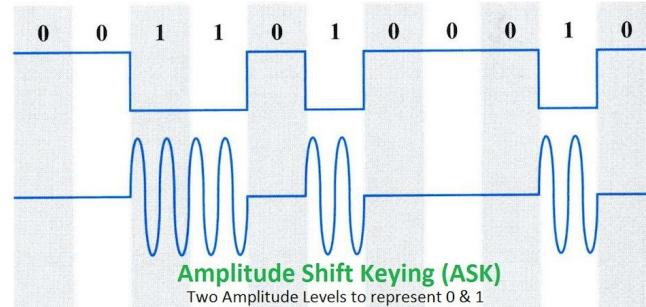
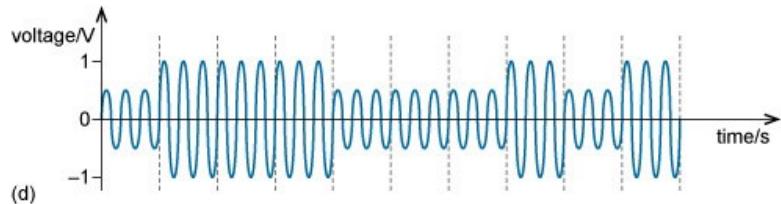
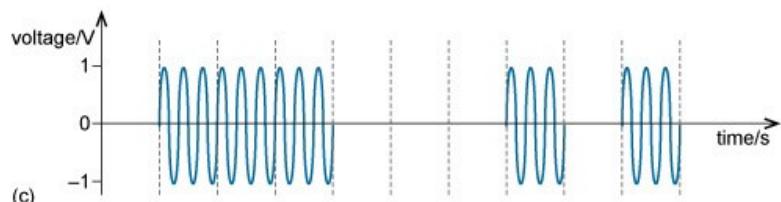
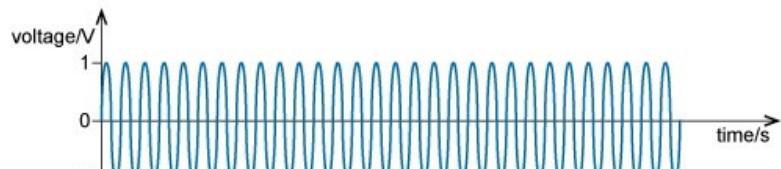
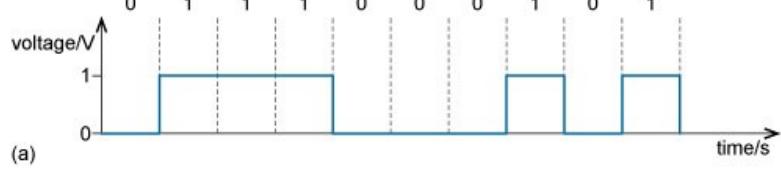
REMOTE-JAMMING IN SA: Another driver falls victim to theft in SA. Image: YouTube

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	[52] Bresser Thermo-/Hygro-Sensor 3CH
[02] Rubicson Temperature Sensor	[53] Springfield Temperature and Soil Moisture
[03] Prologue Temperature Sensor	[54] Oregon Scientific SL109H Remote Thermal Hygro Sensor
[04] Waveman Switch Transmitter	[55] Acurite 606TX Temperature Sensor
[05]* Steffen Switch Transmitter	[56] TFA pool temperature sensor
[06]* ELV EM 1000	[57] Kedsum Temperature & Humidity Sensor
[07]* ELV WS 2000	[58] blyss DCS-UK-WH (433.92 MHz)
[08] LaCrosse TX Temperature / Humidity Sensor	[59] Steelmate TPMS
[09]* Template decoder	[60] Schrader TPMS
[10]* Acurite 986 Rain Gauge	[61]* LightwaveRF
[11] Acurite 609TXC Temperature and Humidity Sensor	[62] Elro DB286A Doorbell
[12] Oregon Scientific Weather Sensor	[63] Efergy Optical
[13]* Mebus 433	[64] Honda Car Key
[14]* Intertechno 433	[65]* Template decoder
[15] KlikAanklikUlt Wireless Switch	[66] Fine Offset Electronics, XC0400
[16] AlectoVi Weather Sensor (Alecto WS3500 WS4500 Ventus W155/W044 Oregon	[67] Radiohead ASK
[17] Cardin S466-TX2	[68] Kerui PIR Sensor
[18] Fine Offset Electronics, WH2 Temperature/Humidity Sensor	[69] Fine Offset WH1050 Weather Station
[19] Nexus Temperature & Humidity Sensor	[70] Honeywell Door/Window Sensor
[20] Ambient Weather Temperature Sensor	[71] Maverick ET-732/733 BBQ Sensor
[21] Calibre RF-104 Sensor	[72]* RF+tech
[22]* X10 RF	[73] LaCrosse TX141-Bv2/TX141TH-Bv2 sensor
[23]* DSC Security Contact	[74] Acurite 00275rm,00276rm Temp/Humidity with optional probe
[24]* Brennenstuhl RCS 2044	[75] LaCrosse TX35DTH-IT Temperature sensor
[25] GT-WT-02 Sensor	[76] LaCrosse TX29IT Temperature sensor
[26] Danfoss CFR Thermostat	[77] Vaillant calorMatic 340f Central Heating Control
[27]* Energy Count 3000 (868.3 MHz)	[78] Fine Offset Electronics, WH25 Temperature/Humidity/Pressure Sensor
[28]* Valeo Car Key	[79] Fine Offset Electronics, WH0530 Temperature/Rain Sensor
[29] Chuango Security Technology	[80] IBIS beacon
[30] Generic Remote SC226x EV1527	[81] Oil Ultrasonic STANDARD FSK
[31] TFA-Twin-Plus-30.3049 and Ea2 BL999	[82] Citroen TPMS
[32] Fine Offset Electronics WH1080/WH3080 Weather Station	[83] oil Ultrasonic STANDARD ASK
[33] WT450	[84] Thermopro TP11 Thermometer
[34] LaCrosse WS-2310 Weather Station	[85] Solight TE44
[35] Esperanza EWS	[86] Wireless Smoke and Heat Detector GS 558
[36] Efergy e2 classic	[87] Generic wireless motion sensor
[37]* Inovalley kw9015b, TFA Dostmann 30.3161 (Rain and temperature sensor)	[88] Toyota TPMS
[38] Generic temperature sensor 1	[89] Ford TPMS
[39] WG-PB12V1	[90] Renault TPMS
[40] Acurite 592TXR Temp/Humidity, 5n1 Weather Station, 6045 Lightning	[91]* inFactory
[41] Acurite 986 Refrigerator / Freezer Thermometer	[92] FT-004-B Temperature Sensor
[42] HIDEKI TS04 Temperature, Humidity, Wind and Rain Sensor	[93] Ford Car Key
[43] Watchman Sonic / Apollo Ultrasonic / Beckett Rocket oil tank monitor	[94] Philips outdoor temperature sensor
[44] CurrentCost Current Sensor	[95] Schrader TPMS EG53MA4
[45] emonTx OpenEnergyMonitor	[96] Nexa
[46] HT680 Remote control	[97] Thermopro TP12 Thermometer
[47] S3318P Temperature & Humidity Sensor	[98] GE Color Effects
[48] Akhan 100F14 remote keyless entry	[99] X10 Security
[49] Quhwa	[100] Interlogix GE UTC Security Devices
[50] OSV1 Temperature Sensor	[101]* Dish remote 6.3
[51] Proove	
[52] Bresser Thermo-/Hygro-Sensor 3CH	

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>

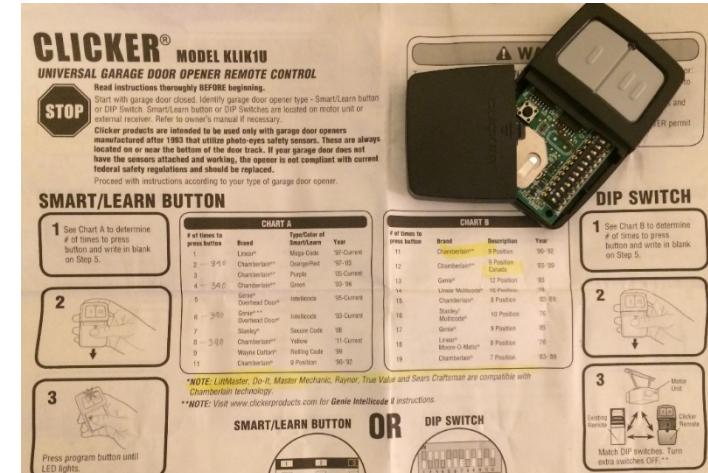
Simple OOK/ASK bruteforce library with custom checksums support <https://github.com/Ganapati/brOOKforce>

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/>

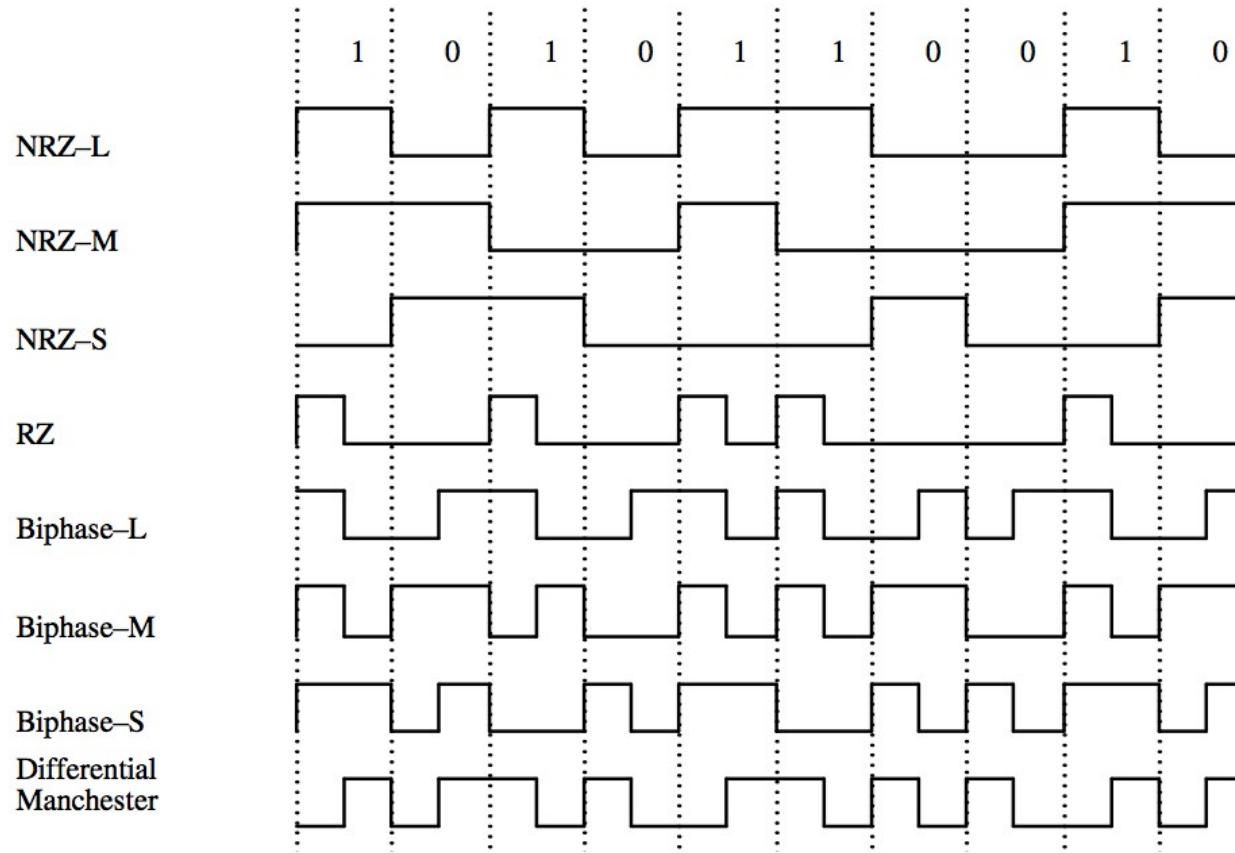


Universal Garage Remote
Sold at Walmart. Great learning tool



OOK Signal Decoding

If the signal is new/unknown, we have to determine line code format
How is the binary data being transmitted?



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/>

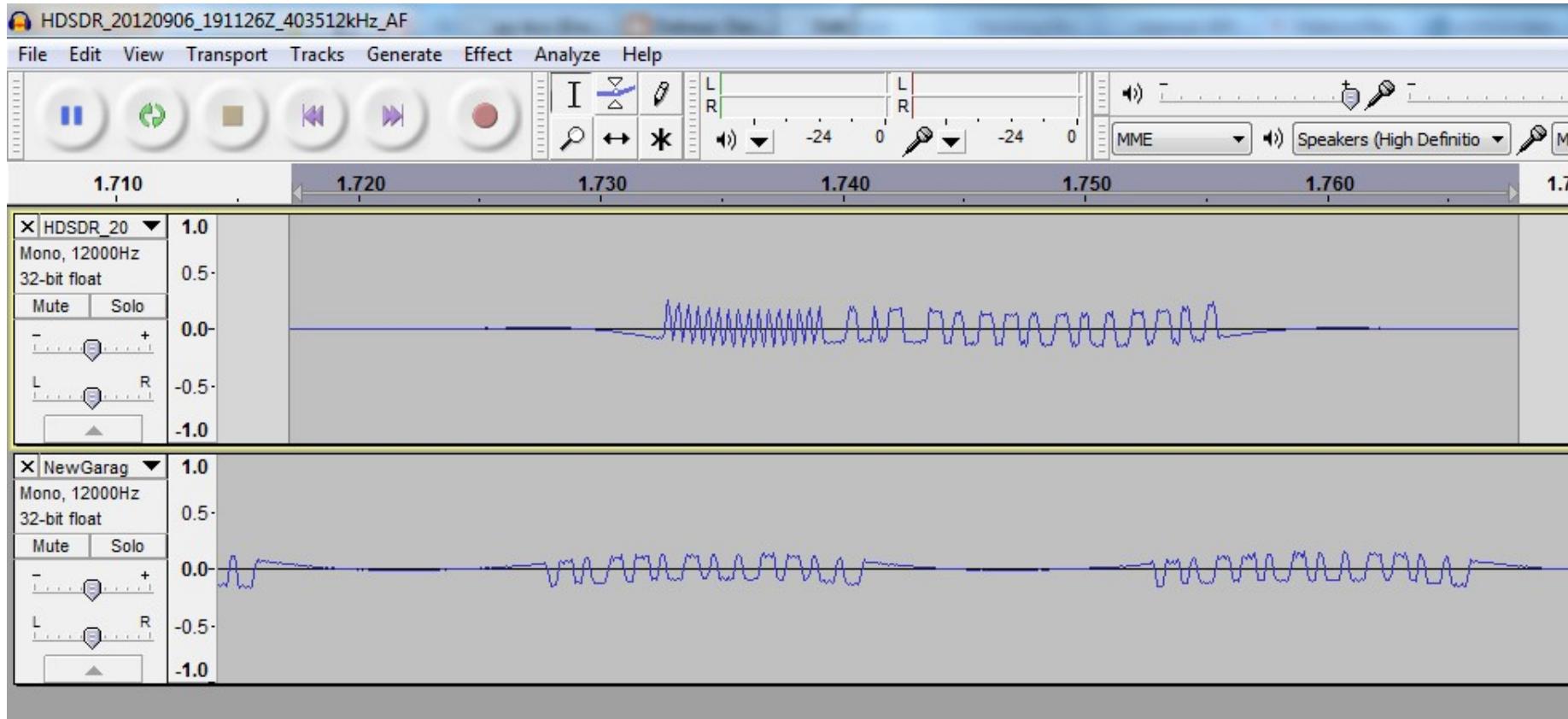
<https://www.andrewmohawk.com/2012/09/06/hacking-fixed-key-remotes/>

Audacity

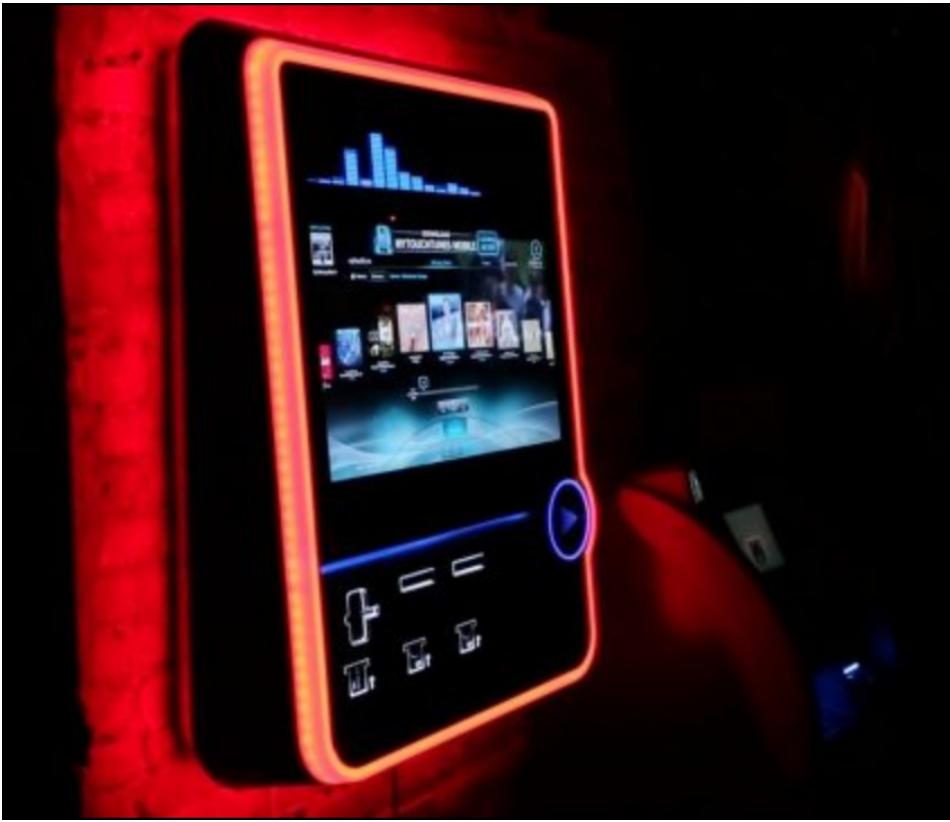
Demodulate signal (AM vs FM) and record to digital audio file (WAV)

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

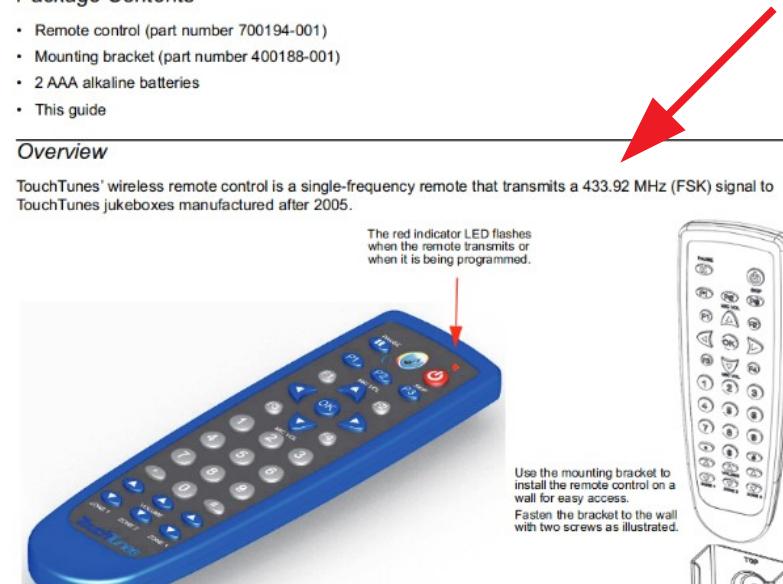
This guide explains the setup and operation of TouchTunes wireless remote control, P/N 700194-001.

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.



The red indicator LED flashes when the remote transmits or when it is being programmed.

Use the mounting bracket to install the remote control on a wall for easy access.
Fasten the bracket to the wall with two screws as illustrated.

(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

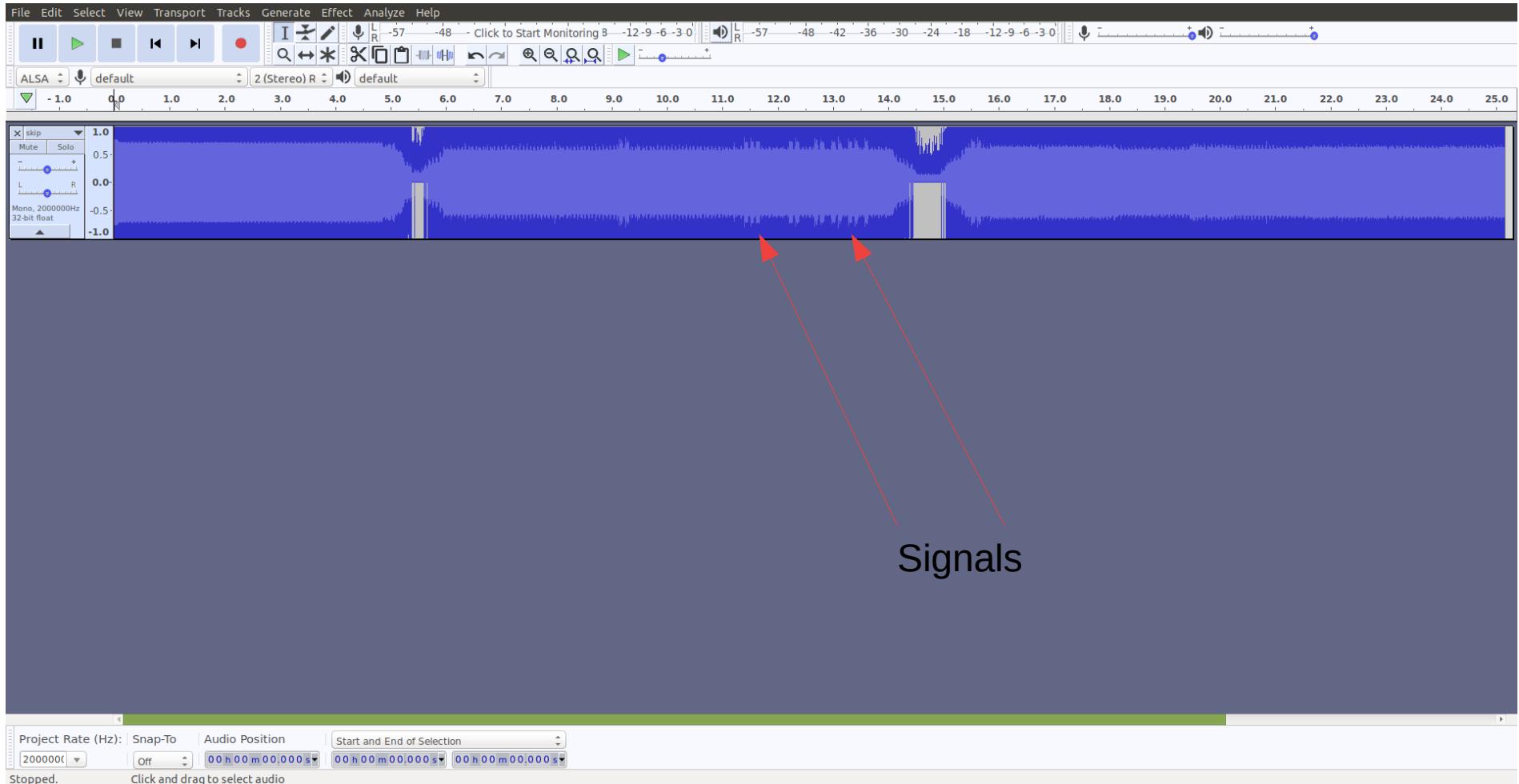
Prior to the “skip”, start recording 433.92 MHz on RasPi.

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

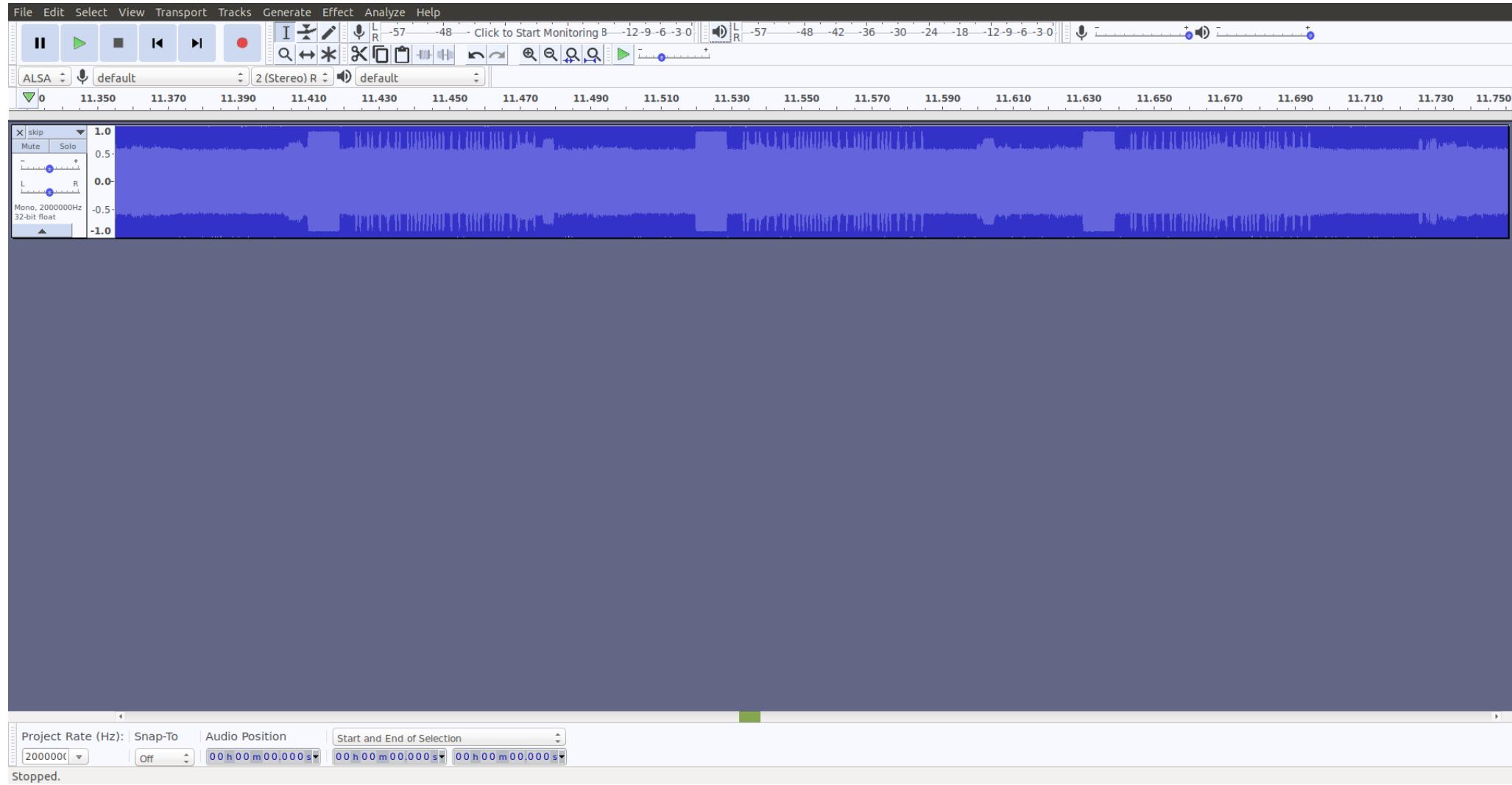


Reverse Engineer Signal

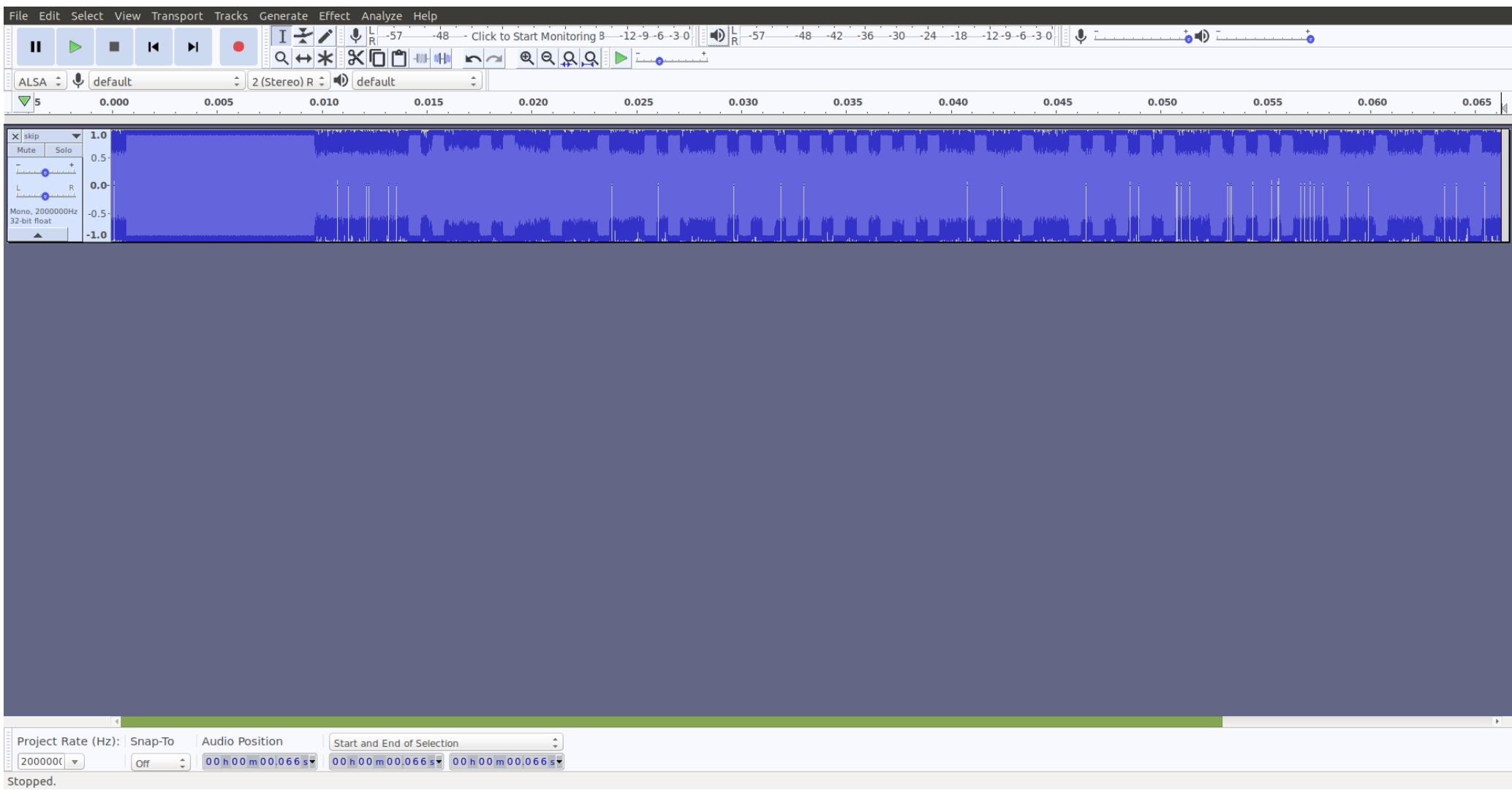
Examine wav file in Audacity or Baudline



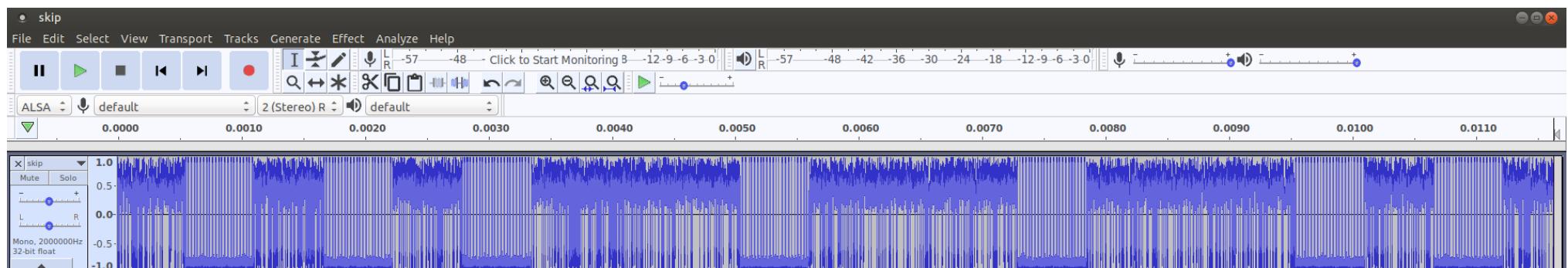
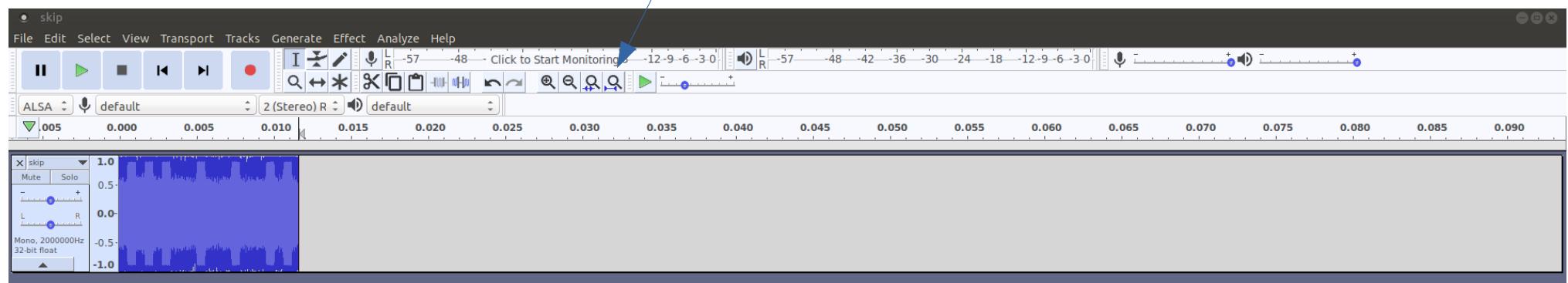
Zoomed In



Zoomed to single signal



Determine length of pulses & gaps (microseconds)



500ish microseconds



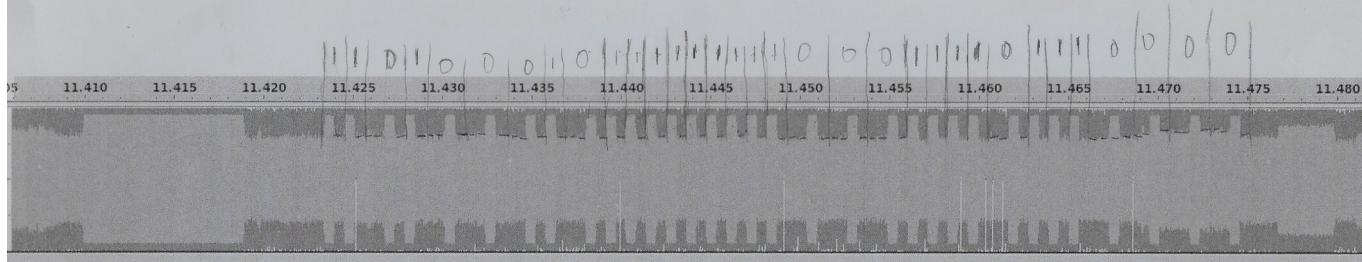
550-600ish microseconds

Manchester Encoding

1101000101111111100011101110000 P1
110100010111111110011010111001010 P2



P1 credit



$$1 = \boxed{\text{L}}$$

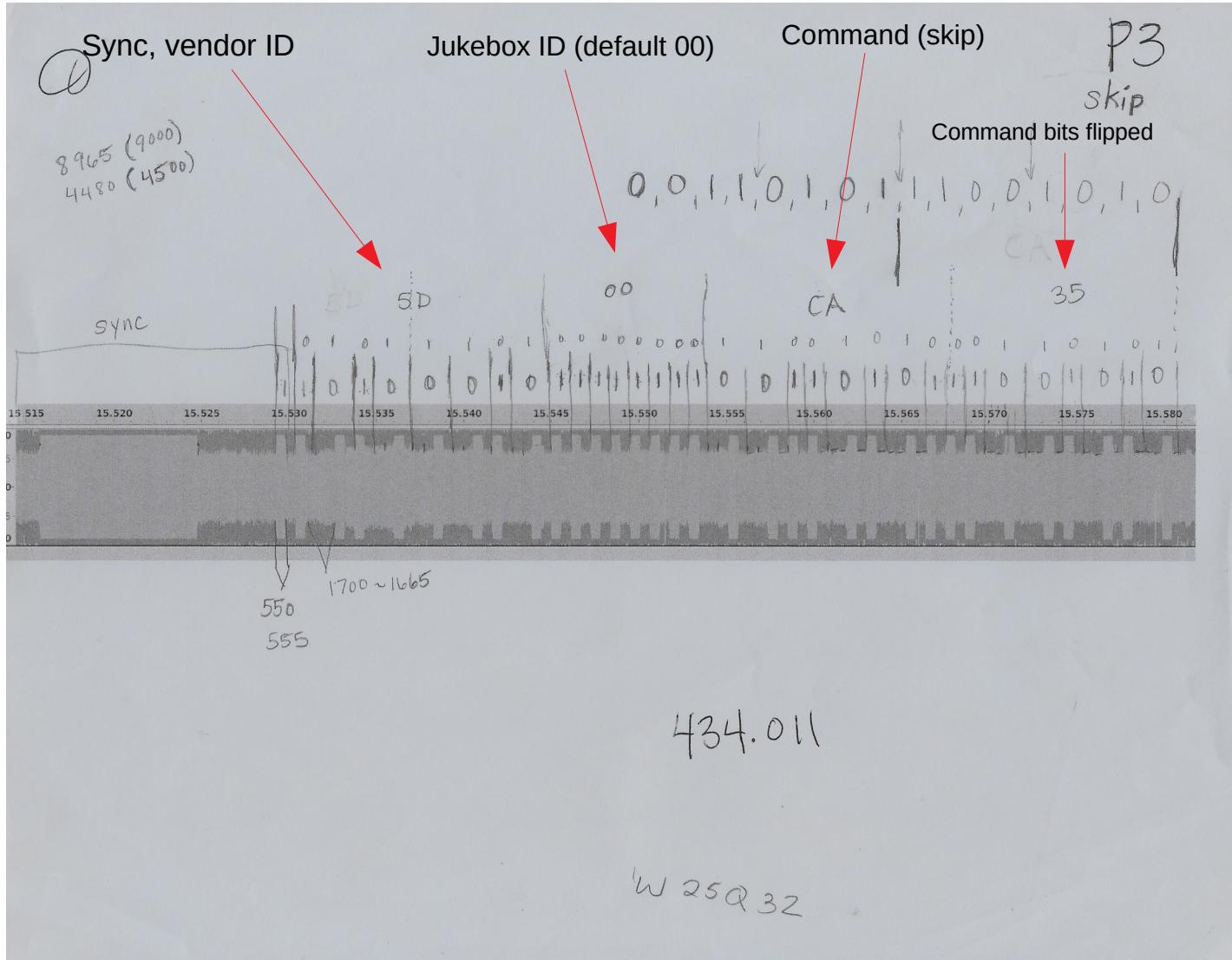
$$100 + 500 = 600$$

100 ft

microseconds

$$0 = \boxed{\text{H}}$$

-F



Arduino Hello World

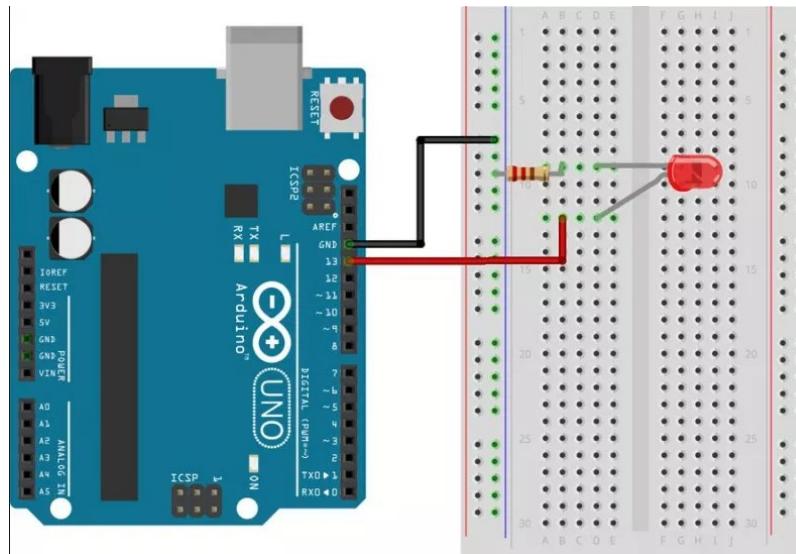
Blink LED

<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

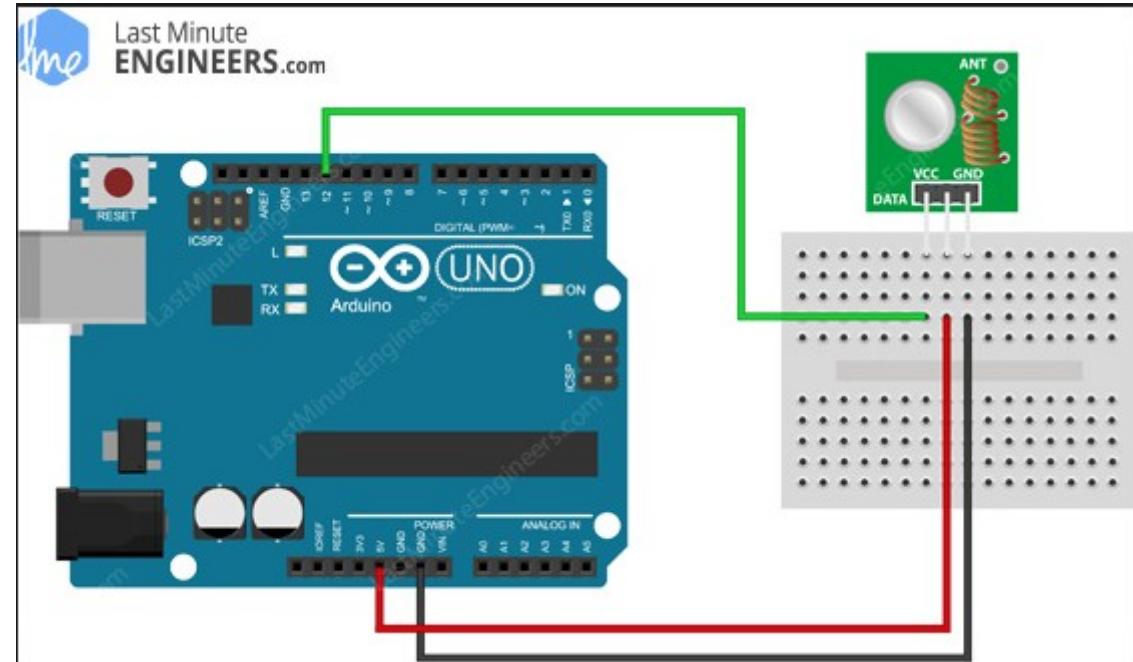
OFF



Arduino 433 Transmitter (Jukebox Clone)

```
*skip.c ✘
5
6 int main (void) {
7     int pin = 0; //GPIO pin 11 on RaspberryPi2
8     int try_limit = 3; //send code 3 times
9
10    if( wiringPiSetup() == -1 )
11        exit (1);
12    if( piHiPri( 99 ) == -1 )
13        exit (1);
14
15    pinMode( pin, OUTPUT );
16
17    for( int y = 0; y < 1; y++ ) {
18        for( int z = 0; z < try_limit; z++ ) {
19            int values[] =
20            {
21                1,1,0,1,0,0,0,1,0,
22                1,1,1,1,1,1,1,1,
23                0,0,1,1,0,0,1,1,1,0,0,1,0,1,0
24            };
25
26            int valueCount = 33;
27
28            digitalWrite( pin, HIGH );
29            delayMicroseconds( 8965 );
30            digitalWrite( pin, LOW );
31            delayMicroseconds( 4480 );
32
33            for( int x = 0; x < valueCount; x++ ) {
34                if( values[x] == 1 ) {
35                    digitalWrite( pin, HIGH );
36                    delayMicroseconds( 500 );
37                    digitalWrite( pin, LOW );
38                    delayMicroseconds( 585 );
39                }
34                else {
35                    digitalWrite( pin, LOW );
36                    delayMicroseconds( 1066 );
37                    digitalWrite( pin, HIGH );
38                    delayMicroseconds( 500 );
39                    digitalWrite( pin, LOW );
40                    delayMicroseconds( 585 );
41                }
42            }
43            digitalWrite( pin, LOW );
44            delayMicroseconds( 45000 );
45        }
46    }
47 }
48
49 }
```

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/furtek/portapack-havoc>

The Fonz: Touchtunes remote for RfCat

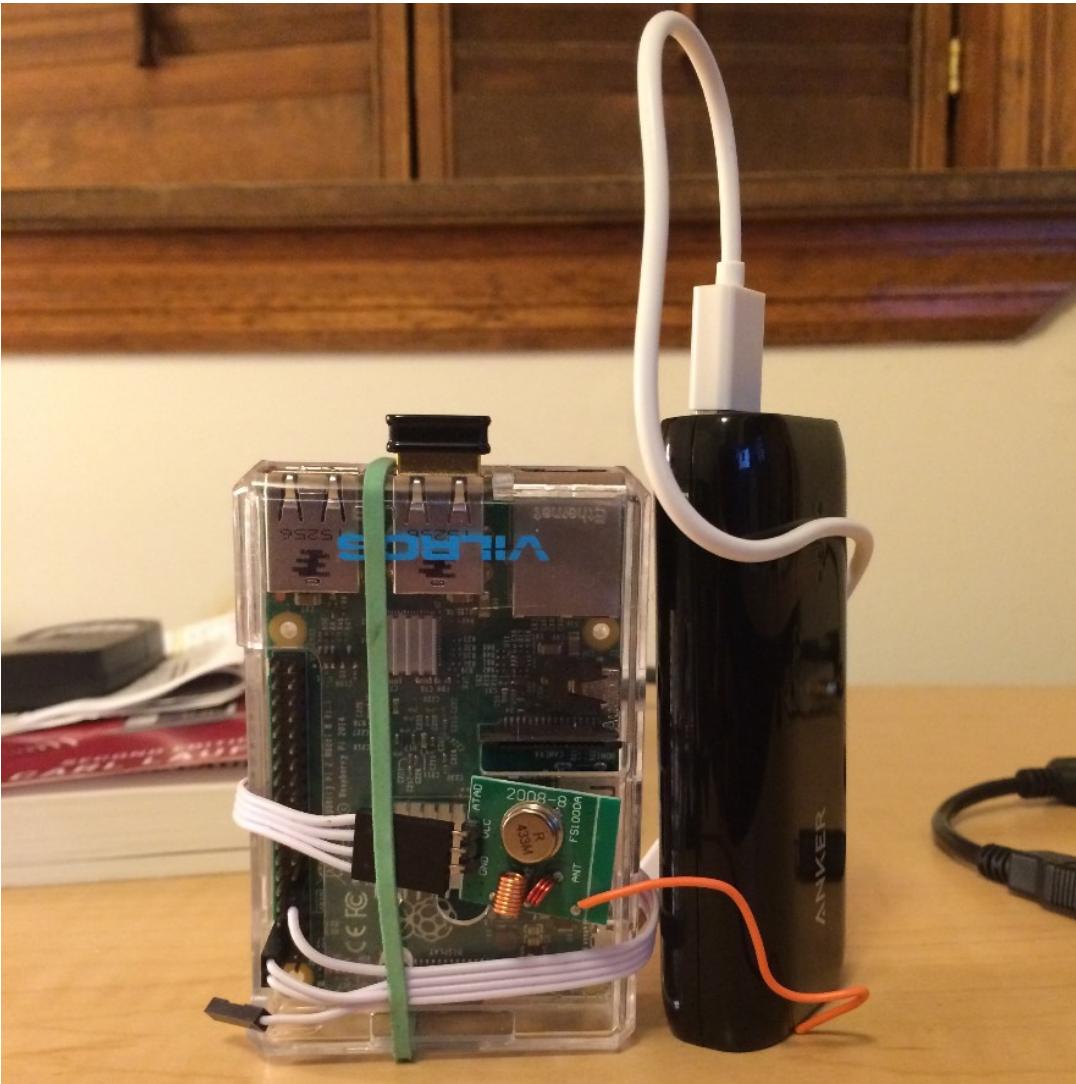
<https://github.com/notpike/The-Fonz>



```
// 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
    0x80, // 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/furtek/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

Correct my mistakes? (Baud not baud rate)