RTL-SDR & GNU Radio

::Fabio, IZ5XRC ::Francesco, IW5EKN

"Serata a tema" - ARI Firenze
26 Febbraio 2015

Parte II

Uso & Esperimenti

Quale RTL-SDR possiedo ?

Quale RTL-SDR possiedo ?

Tuner	Frequency range
Elonics E4000	52 - 2200 MHz with a gap from 1100 MHz to 1250 MHz (varies)
Rafael Micro R820T	24 - 1766 MHz
Rafael Micro R828D	24 - 1766 MHz
Fitipower FC0013	22 - 1100 MHz (FC0013B/C, FC0013G has a separate L-band input, which is unconnected on most sticks)
Fitipower FC0012	22 - 948.6 MHz
FCI FC2580	146 - 308 MHz and 438 - 924 MHz (gap in between)

FULL LIST @ https://www.reddit.com/r/RTLSDR/comments/s6ddo/rtlsdr_compatibility_list_v2_work_in_progress/

VID	PID	Tuner	Device Name
0x0bda	0x2832	all of them	Generic RTL2832U (e.g. hama nano)
0x0bda	0x2838	E4000	ezcap USB 2.0 DVB-T/DAB/FM dongle
0x0ccd	0x00a9	FC0012	Terratec Cinergy T Stick Black (rev 1)
0x0ccd	0x00b3	FC0013	Terratec NOXON DAB/DAB+ USB dongle (rev 1)
0x0ccd	0x00d3	E4000	Terratec Cinergy T Stick RC (Rev.3)
0x0ccd	0x00e0	E4000	Terratec NOXON DAB/DAB+ USB dongle (rev 2)
0x185b	0x0620	E4000	Compro Videomate U620F
0x185b	0x0650	E4000	Compro Videomate U650F
0x1f4d	0xb803	FC0012	GTek T803
0x1f4d	0xc803	FC0012	Lifeview LV5TDeluxe

http://sdr.osmocom.org/trac/wiki/rtl-sdr

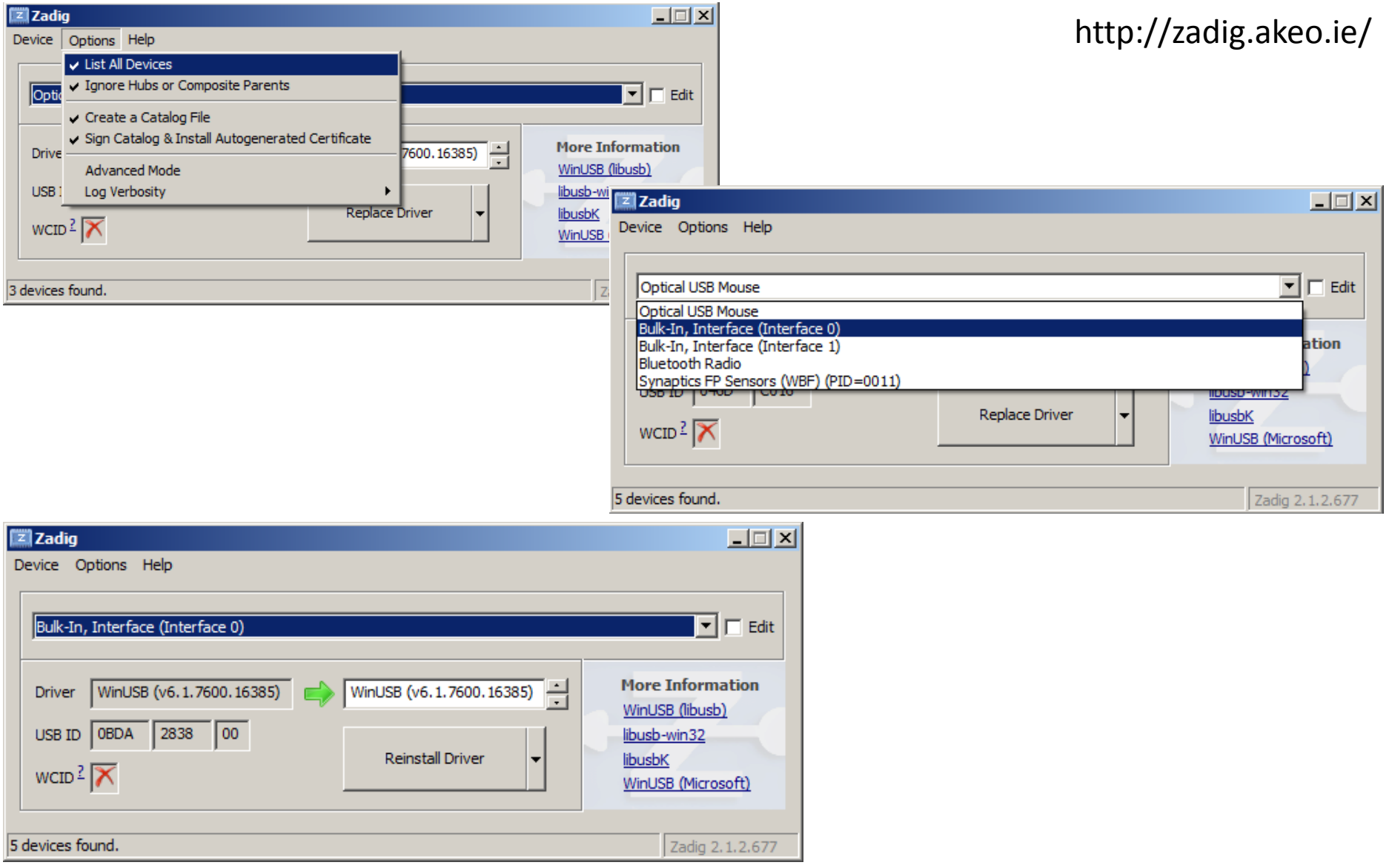
Quale RTL-SDR possiedo ?

VID	PID	Tuner	Device Name
0x0bda	0x2832	all of them	Generic RTL2832U (e.g. hama nano)
0x0bda	0x2838	E4000	ezcap USB 2.0 DVB-T/DAB/FM dongle
0x0ccd	0x00a9	FC0012	Terratec Cinergy T Stick Black (rev 1)
0x0ccd	0x00b3	FC0013	Terratec NOXON DAB/DAB+ USB dongle (rev 1)
0x0ccd	0x00d3	E4000	Terratec Cinergy T Stick RC (Rev.3)
0x0ccd	0x00e0	E4000	Terratec NOXON DAB/DAB+ USB dongle (rev 2)
0x185b	0x0620	E4000	Compro Videomate U620F
0x185b	0x0650	E4000	Compro Videomate U650F
0x1f4d	0xb803	FC0012	GTek T803
0x1f4d	0xc803	FC0012	Lifeview LV5TDeluxe

```
fjalar@fjalar:~$ lsusb
Bus 001 Device 004: ID 0bda:2838 Realtek Semiconductor Corp. RTL2838 DVB-T
Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
Bus 005 Device 001: ID 1d6b:0001 Linux Foundation 1.1 root hub
Bus 004 Device 002: ID 093a:2510 Pixart Imaging, Inc. Optical Mouse
Bus 004 Device 001: ID 1d6b:0001 Linux Foundation 1.1 root hub
Bus 003 Device 001: ID 1d6b:0001 Linux Foundation 1.1 root hub
Bus 002 Device 002: ID 0930:0508 Toshiba Corp. Integrated Bluetooth HCI
Bus 002 Device 001: ID 1d6b:0001 Linux Foundation 1.1 root hub
fjalar@fjalar:~$
```

"sudo rmmod dvb_usb_rtl28xxu rtl2832"

Installazione Driver Zadig – Osmocom/GNU-Radio



http://zadig.akeo.ie/

Installazione Osmocom/GNU Radio

$ wget http://www.sbrac.org/files/build-gnuradio && chmod a+x ./build-gnuradio && ./build-gnuradio

```
-- ######################################################
-- # gr-osmosdr enabled components
-- ######################################################
--   * Python support
--   * Osmocom IQ Imbalance Correction
--   * sysmocom OsmoSDR
--   * FUNcube Dongle
--   * FUNcube Dongle Pro+
--   * IQ File Source
--   * Osmocom RTLSDR
--   * RTLSDR TCP Client
--   * Ettus USRP Devices
--   * Osmocom MiriSDR
--   * HackRF Jawbreaker
--   * nuand bladeRF
--   * RFSPACE Receivers
--
-- ######################################################
-- # gr-osmosdr disabled components
-- ######################################################
```

```
fjalar@fjalar:~$ rtl_test
Found 1 device(s):
  0:  Realtek, RTL2838UHIDIR, SN: 00000001

Using device 0: Generic RTL2832U OEM
Found Rafael Micro R820T tuner
Supported gain values (29): 0.0 0.9 1.4 2.7 3.7 7.7 8.7 12.5 14.4 15.7 16.6 19.7 20.7 22.9 25.4 28.0 29.7 32.8 33.8 36.4 37.2 38.6 40.2 42.1 43.4 43.9 44.5 48.0 49.6
Sampling at 2048000 S/s.

Info: This tool will continuously read from the device, and report if
samples get lost. If you observe no further output, everything is fine.

Reading samples in async mode...
```

Linux Live + GNU Radio

https://gnuradio.org/redmine/projects/gnuradio/wiki/GNURadioLiveDVD

GNURadio
THE FREE & OPEN SOFTWARE RADIO ECOSYSTEM

Panoramica | Attività | Roadmap | Segnalazioni | Notizie | Wiki | File | Repository

GNU Radio Live SDR Environment

Cronologia

The GNU Radio Live SDR Environment, produced by Corgan Labs, is a bootable Ubuntu Linux DVD or USB drive image, with GNU Radio and third party software pre-installed. It is designed for quick and easy testing and experimentation with GNU Radio without having to make any permanent modifications to a PC or laptop. It does not, however, provide for permanent installation.

It is supplied as an ISO image to be downloaded and burned onto a recordable DVD disc or copied to a USB flash drive using a utility such as the Ubuntu Startup Disk Creator (Ubuntu Linux OS) or Unetbootin (Windows, MacOS, Linux). Creating a USB drive from the image will provide much faster booting and operation, and allow making changes and storing files. Finally, the ISO image may be booted within a virtual environment such as VirtualBox, QEMU/kvm, VMware, or Parallels.

Current Stable Release

This version of the ISO image is based on the latest stable release of GNU Radio, 3.7.9, and the stable releases of third party software at that time:

http://s3-dist.gnuradio.org/ubuntu-14.04.3-desktop-amd64-gnuradio-3.7.9.torrent

The use of Bittorrent reduces the load on the GNU Radio web server and lowers project bandwidth costs.

If a Bittorrent client is not available or its use is restricted, you may download the ISO image file by choosing from one of the following mirror sites:

http://s3-dist.gnuradio.org/ubuntu-14.04.3-desktop-amd64-gnuradio-3.7.9.iso
http://eu1-dist.gnuradio.org/s3/ubuntu-14.04.3-desktop-amd64-gnuradio-3.7.9.iso
http://eu2-dist.gnuradio.org/ubuntu-14.04.3-desktop-amd64-gnuradio-3.7.9.iso

Oppure: www.pentoo.ch

Experiments - Kalibrate

Linux source: https://github.com/steve-m/kalibrate-rtl
Windows : http://rtlsdr.org/files/kalibrate-win-release.zip

Per prima cosa si scansiona la banda, in questo caso GSM900 con il comando:

```
kal -g 7.7 -s GSM900
kal -g 7.7 -c 10 -d 0
```

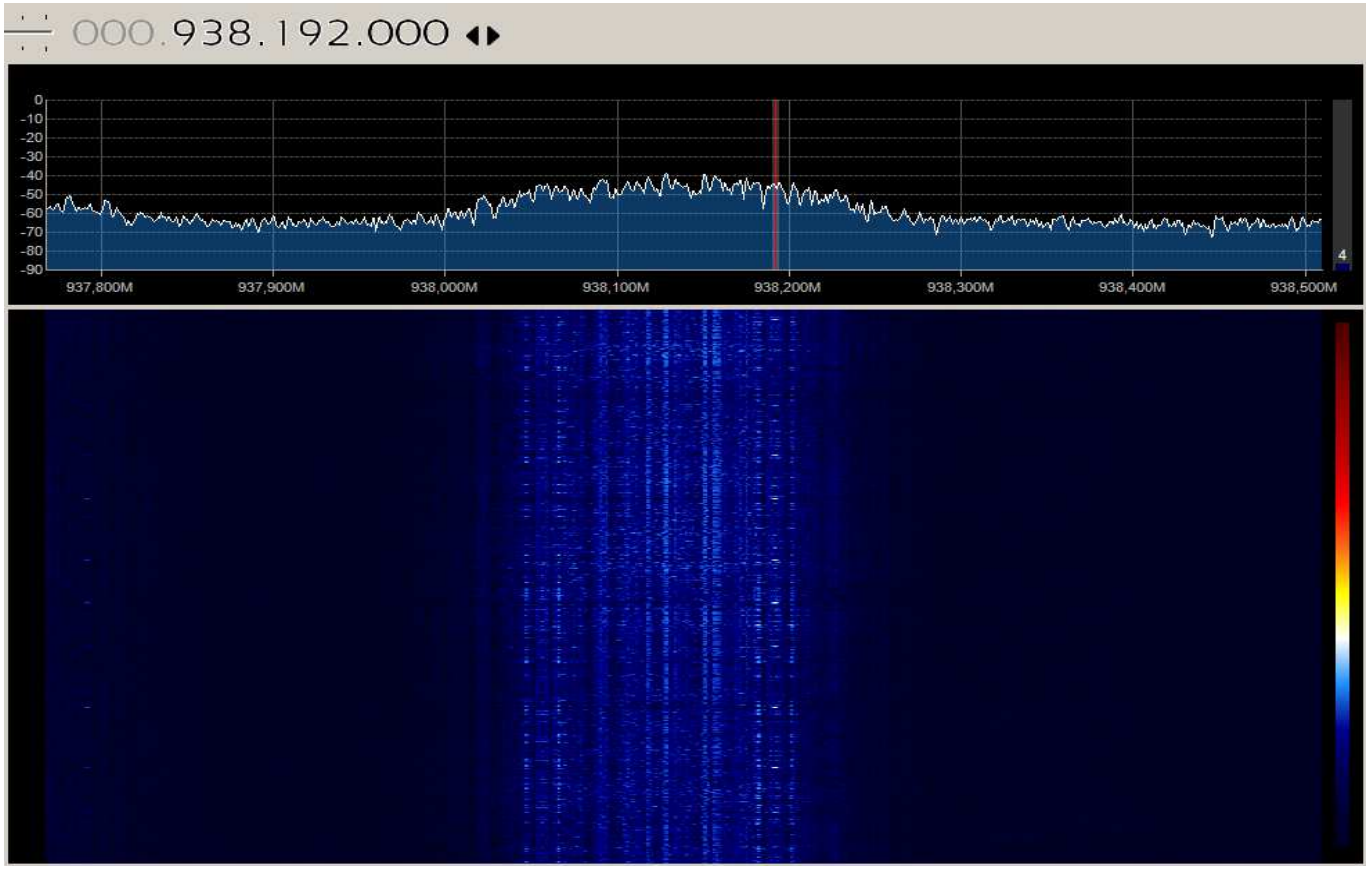
```
Found 1 device(s):
  0:  ezcap USB 2.0 DVB-T/DAB/FM dongle

Using device 0: ezcap USB 2.0 DVB-T/DAB/FM dongle
Found Rafael Micro R820T tuner
Exact sample rate is: 270833.002142 Hz
Setting gain: 7.7 dB
meh: Scanning for GSM-900 base stations.
GSM-900:
        chan: 1 (935.2MHz + 6.661kHz)   power: 285048.27
        chan: 10 (937.0MHz + 39.597kHz) power: 114406.80
        chan: 14 (937.8MHz + 38.844kHz) power: 71646.16
        chan: 21 (939.2MHz + 5.507kHz)  power: 82177.60
        chan: 25 (940.0MHz + 5.602kHz)  power: 113436.02
        chan: 27 (940.4MHz + 5.668kHz)  power: 39707.24
        chan: 38 (942.6MHz + 38.826kHz) power: 59826.82
        chan: 42 (943.4MHz + 39.078kHz) power: 242235.66
        chan: 44 (943.8MHz + 39.188kHz) power: 182702.23
        chan: 53 (945.6MHz + 6.040kHz)  power: 313829.17
        chan: 55 (946.0MHz + 6.097kHz)  power: 186234.85
        chan: 56 (946.2MHz + 5.711kHz)  power: 80134.95
        chan: 106 (956.2MHz + 37.846kHz)        power: 207237.49
        chan: 117 (958.4MHz + 4.601kHz) power: 357743.58
```

$$PPM = \frac{0.039597\ MHz}{937.0\ MHZ}$$

$$\approx 42\ PPM$$

Experiments – GSM FCCH



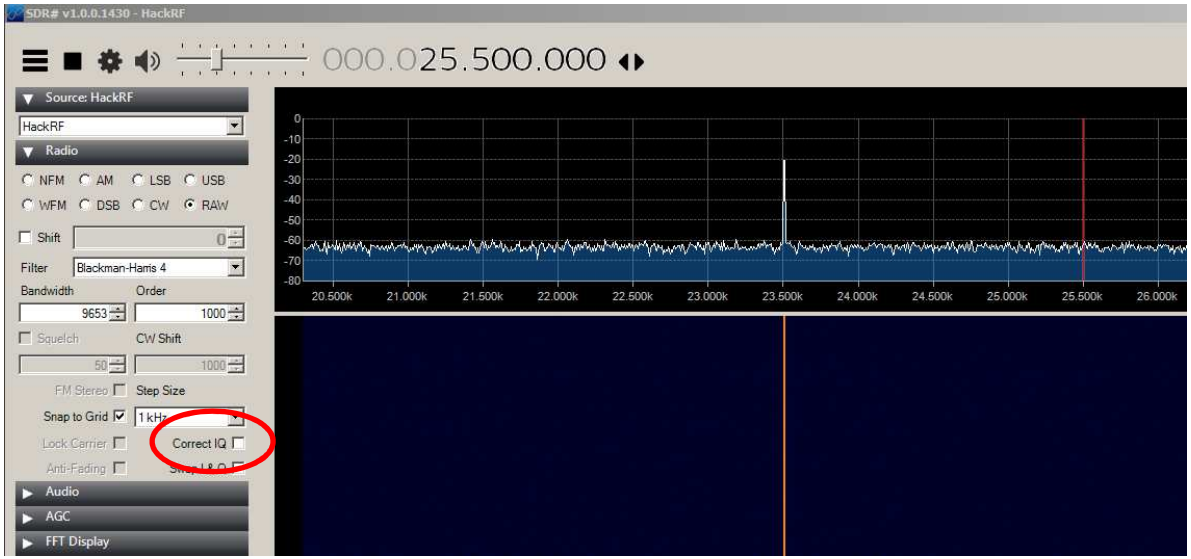
Band: GSM-900
Channel: 16
Uplink: 893.2 MHz
Downlink: 938.2 MHz

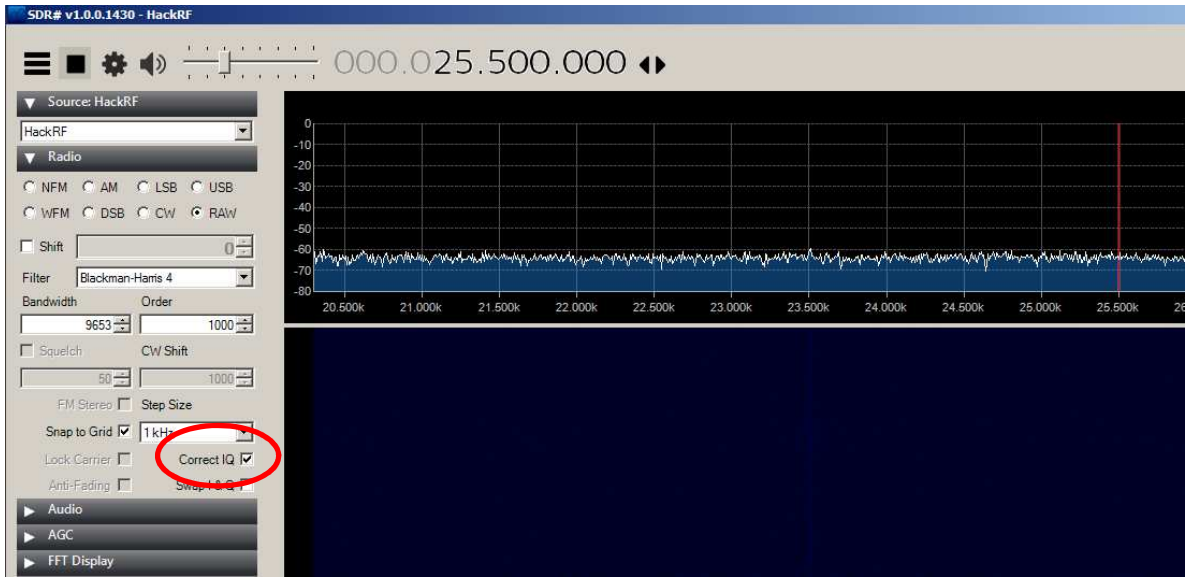
FCCH = Carrier+67.7kHz

$$PPM = \frac{(938192000 - \mathbf{938267700})}{938192000} \cdot 1e6 \approx -80.7\ ppm$$

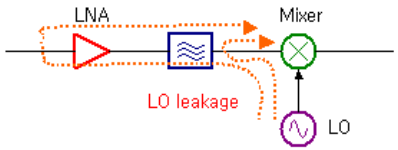
https://gnuradio.org/redmine/attachments/115/all_gsm_channels_arfcn.txt

Experiments – DC offset + IQ Imbalance





DC Offset:
È legato a fenomeni denominati "self-mixing" causati da L.O. leakage

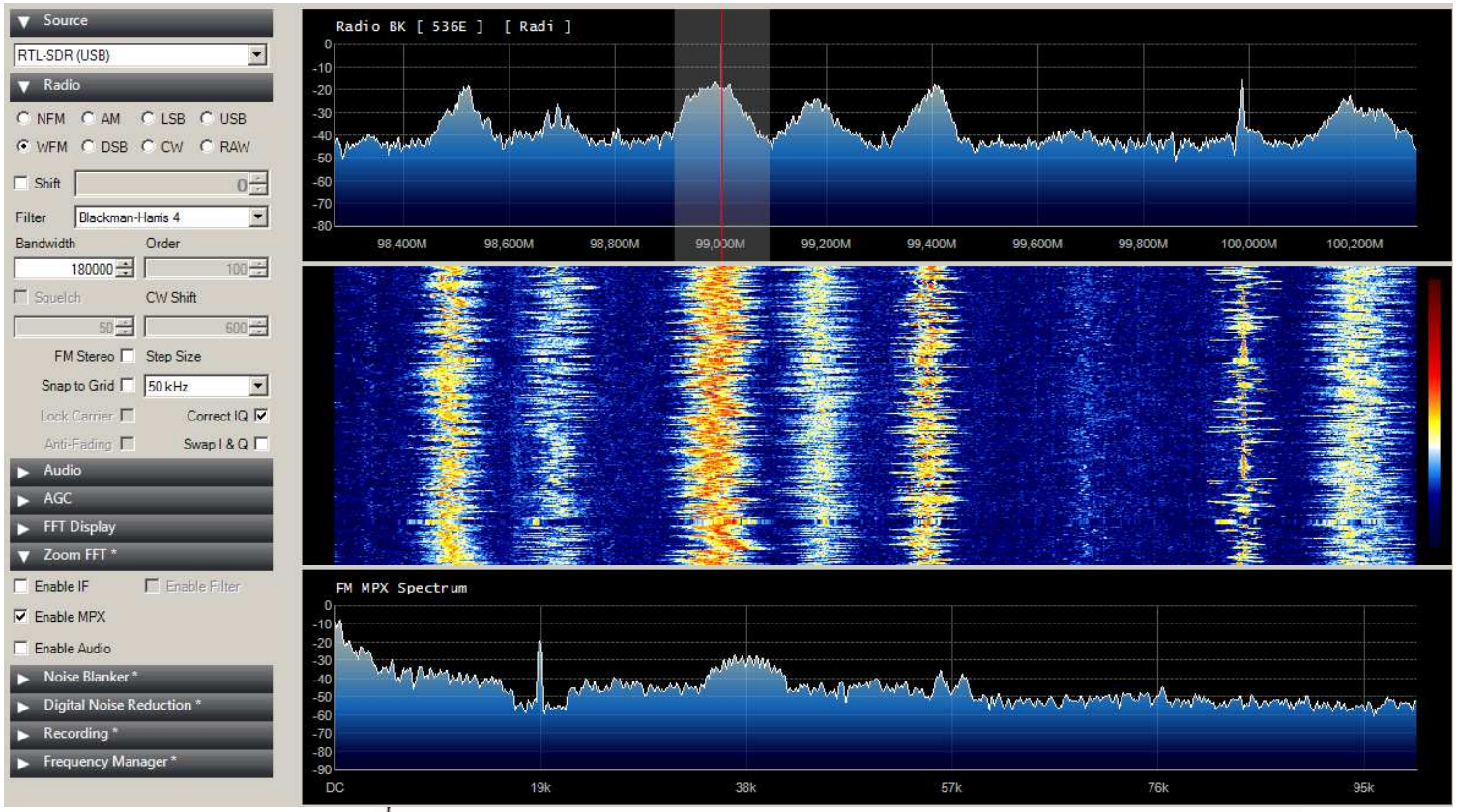


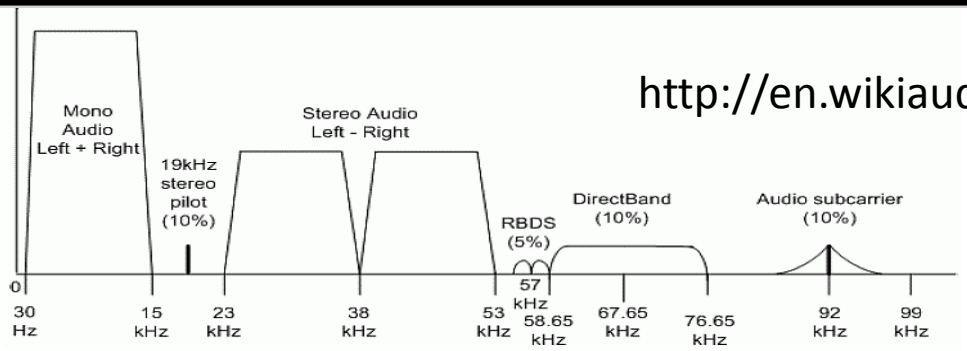
IQ Imbalance:
È legato a sbilanciamenti per diverso guadagno e relazione di fase tra le componenti I e Q (non esatta differenza di fase di 90°)

EFFETTO SULLO SPETTRO

DC Offset -> Picco DC
IQ Imbalance -> "Immagini"

Experiments – WFM + RDS

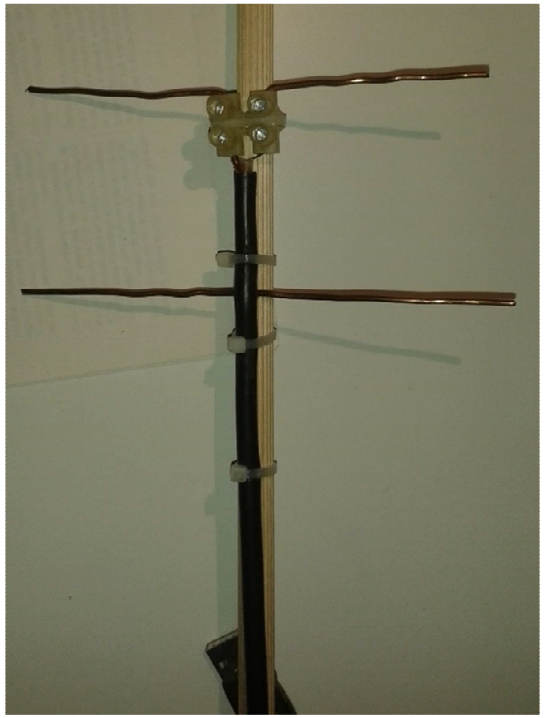


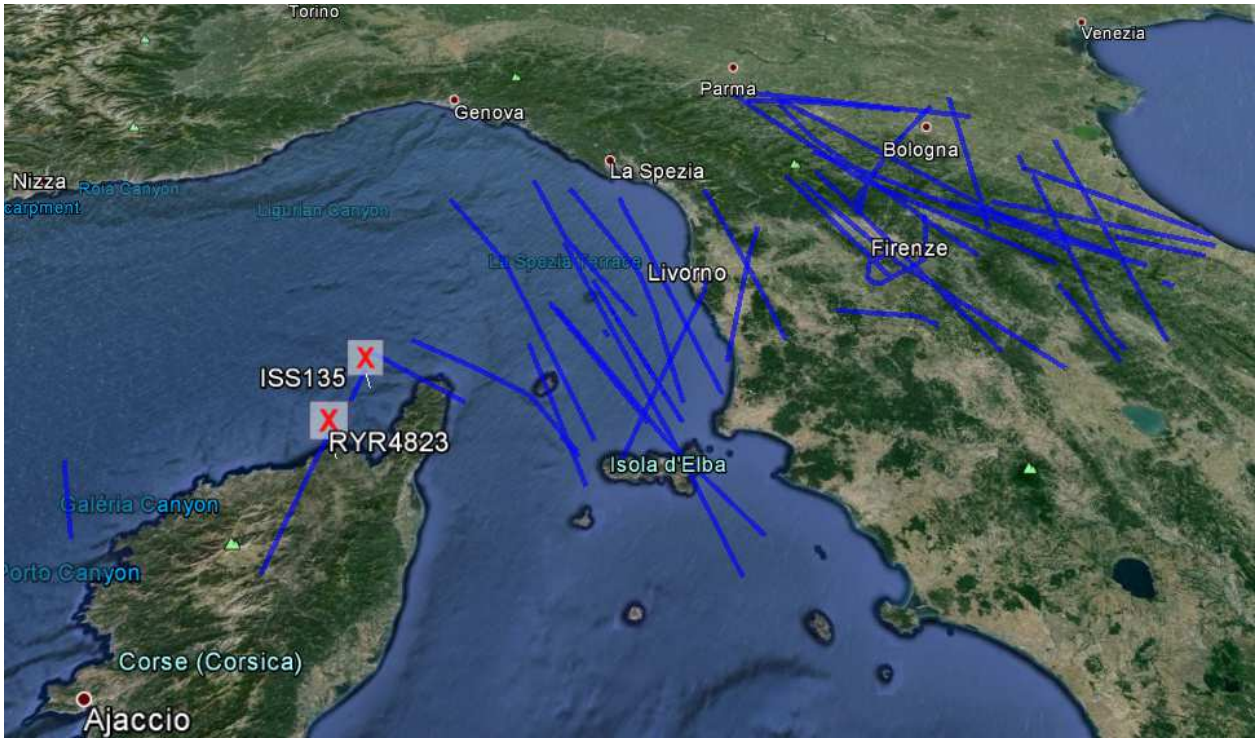


http://en.wikiaudio.org/FM_broadcasting

Experiments - dump1090 + 1090MHz Antenna

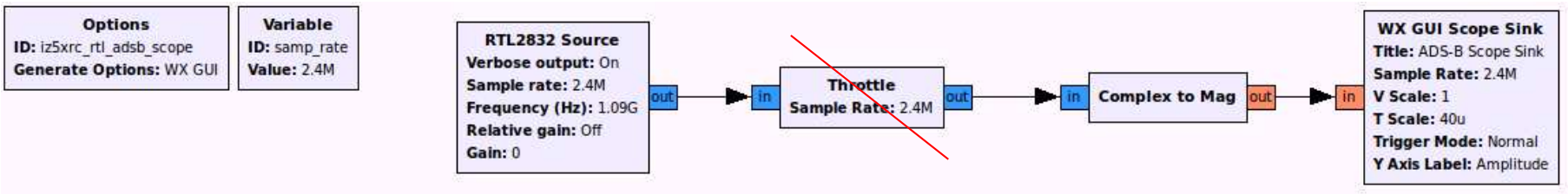
https://github.com/antirez/dump1090 → Linux
http://globe-s.eu/download/rtl1090imu.exe → WIN

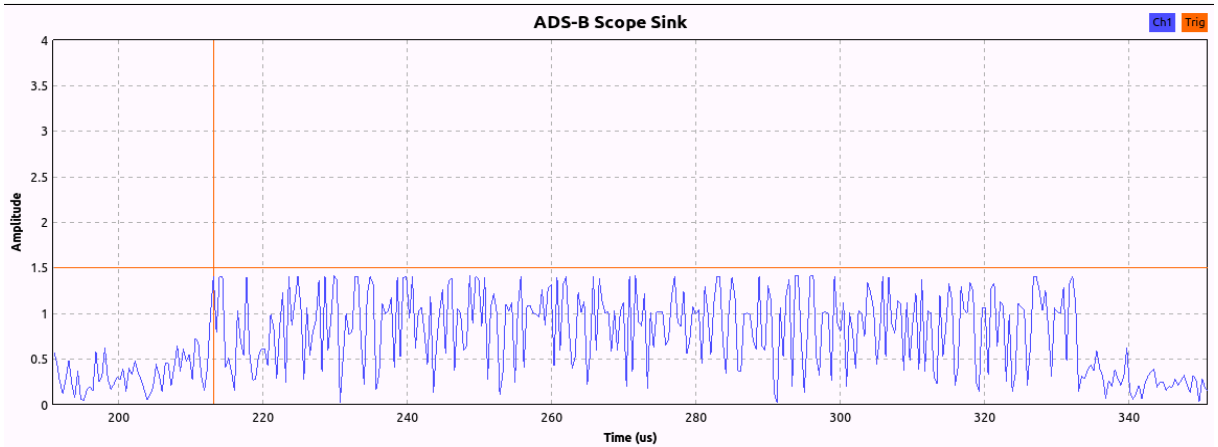




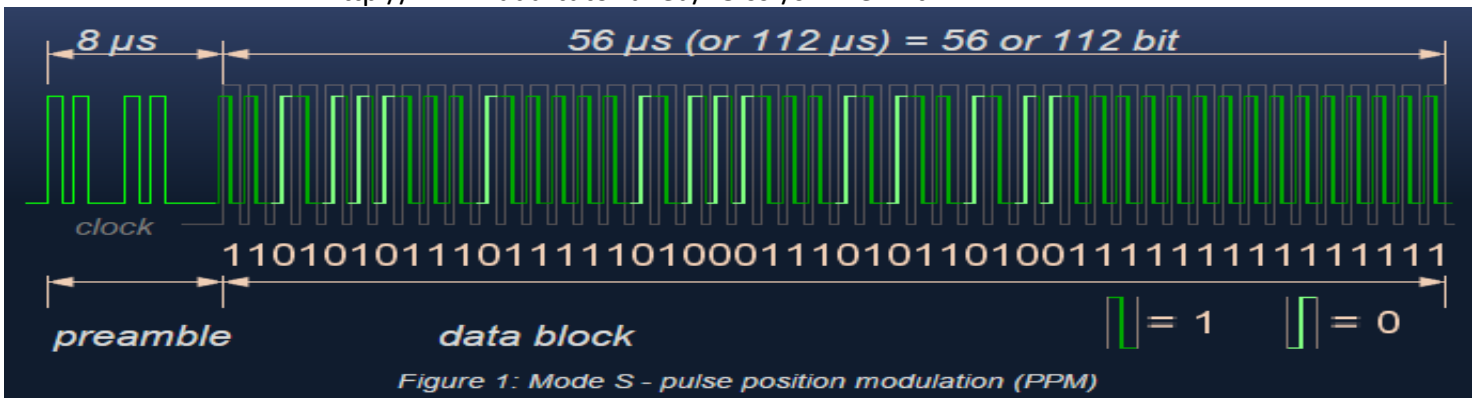
Hex	Flight	Altitude	Speed	Lat	Lon	Track	Messages	Seen .
3949e7	AFR012	36000	488	52.765	-1.250	324	124	20 sec
4caaec	REA264B	1000	104	52.483	-1.781	144	67	39 sec
405545		26900	0	0.000	0.000	0	112	0 sec
406769		2050	0	0.000	0.000	0	60	17 sec
49124b		33000	0	0.000	0.000	0	415	0 sec

Experiments - ADS-B GNU Radio Flowgraph

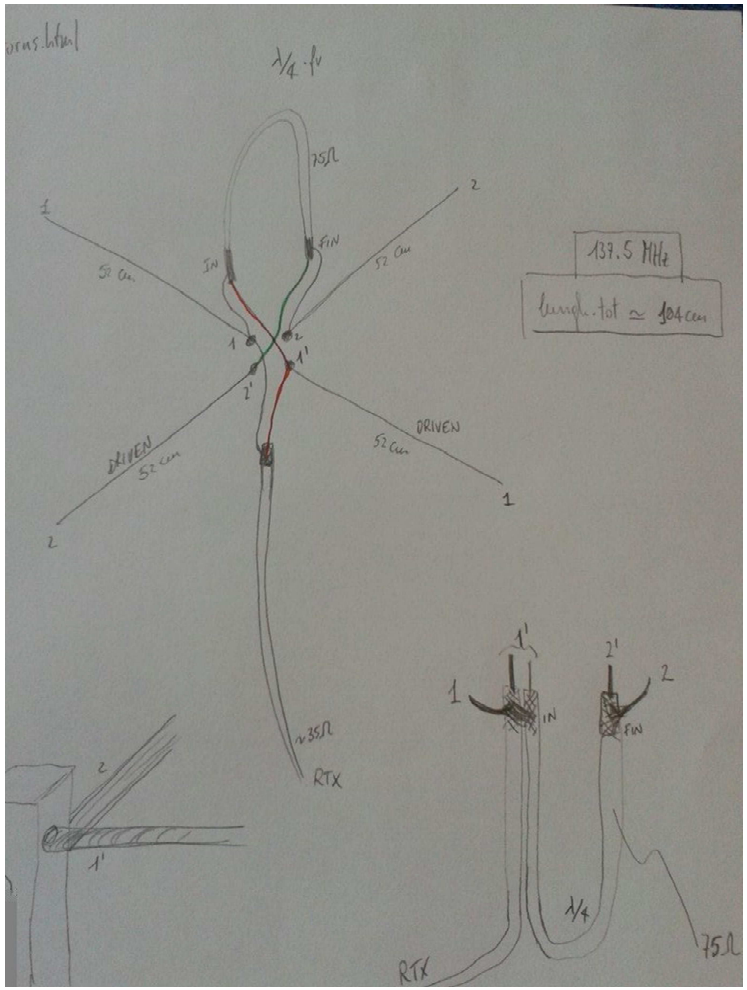


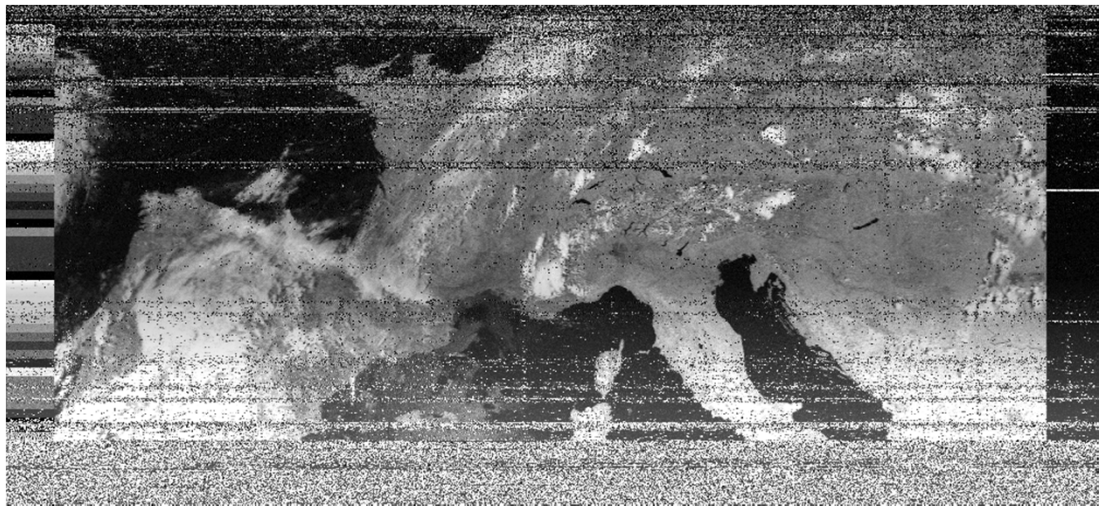


http://www.radartutorial.eu/13.ssr/sr24.en.html



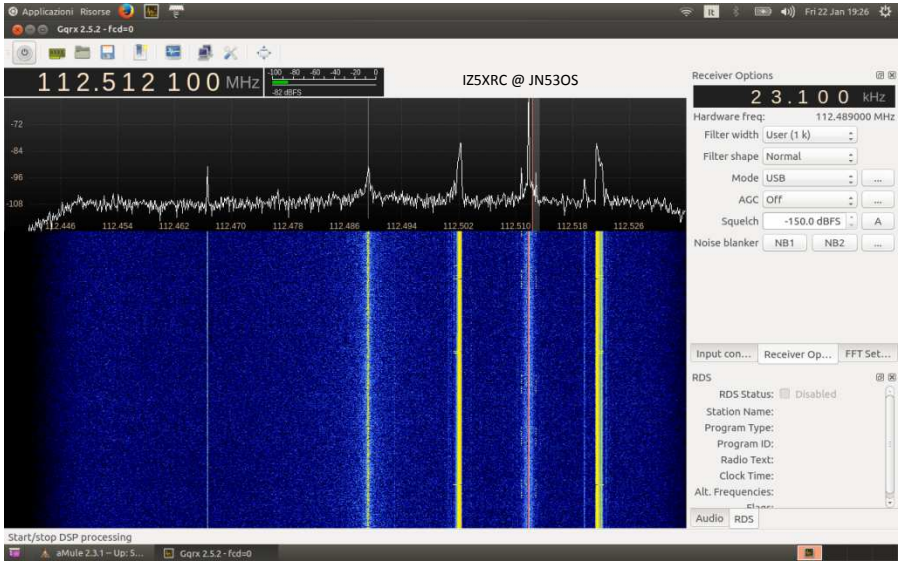
Experiments - NOAA 19 Overhead pass – WX Sat APT

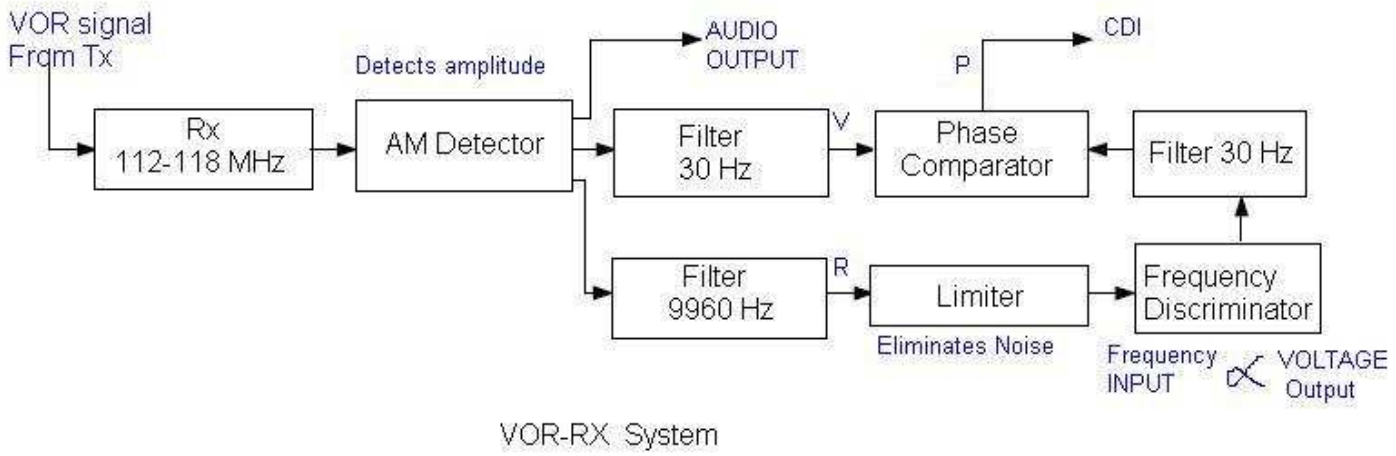




Experiments – VOR PRT

https://en.wikipedia.org/wiki/Radio_navigation#/media/File:VOR_DME_BUB.JPG



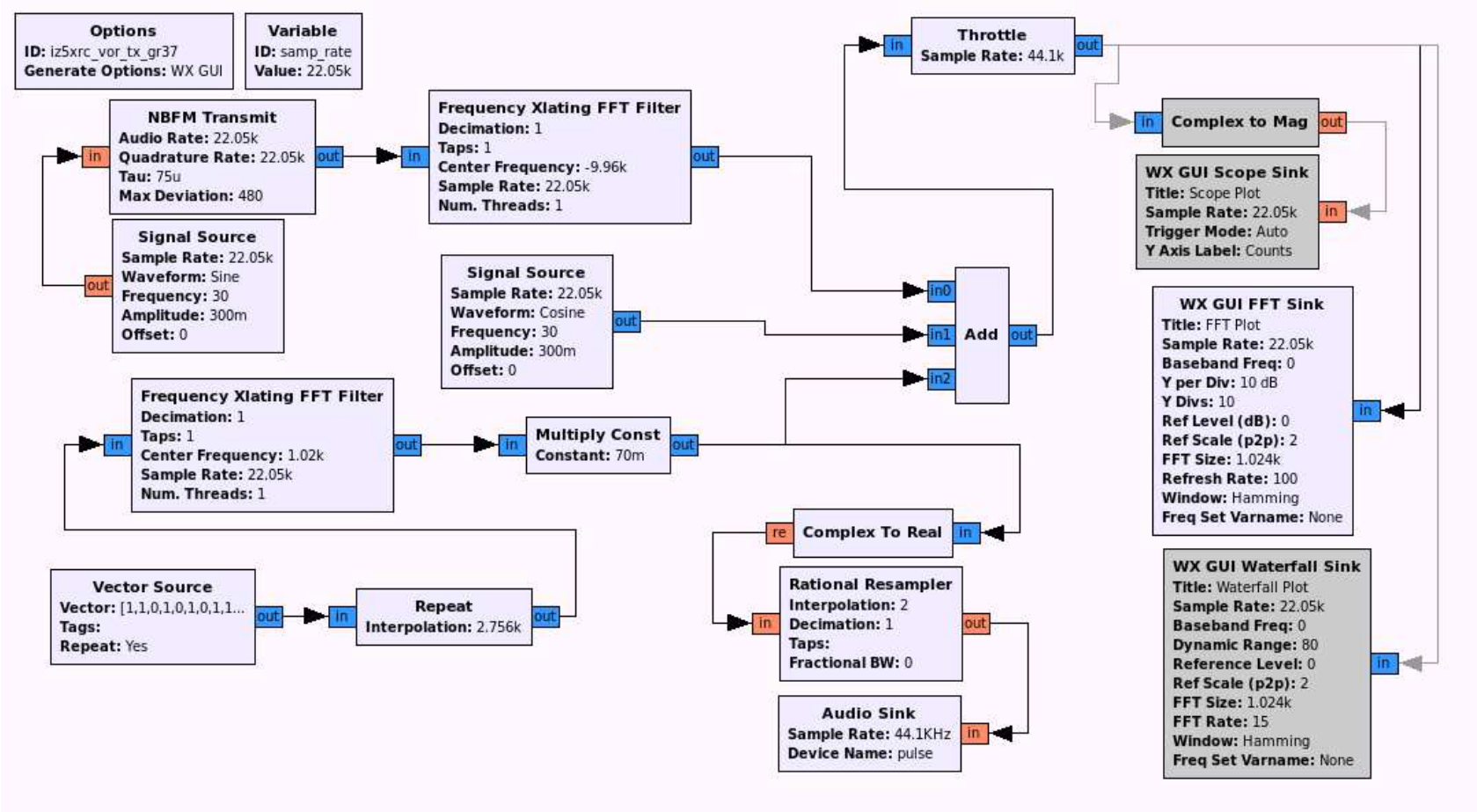


VOR-RX System

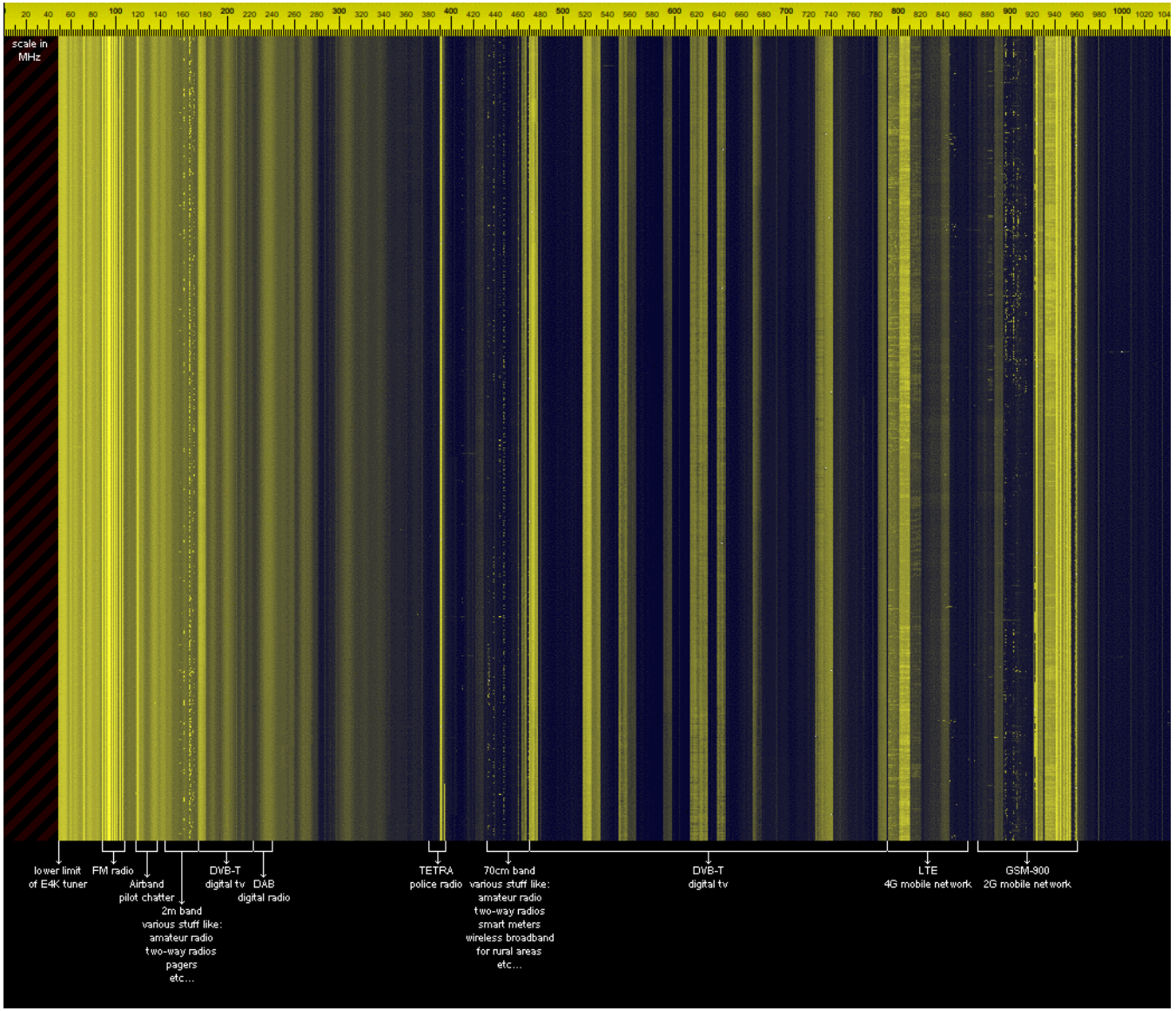
http://www.rfwireless-world.com/Terminology/VOR-VHF-Omnidirectional-Range.html

Experiments – VOR TX

GNURadio VOR TX – IZ5XRC



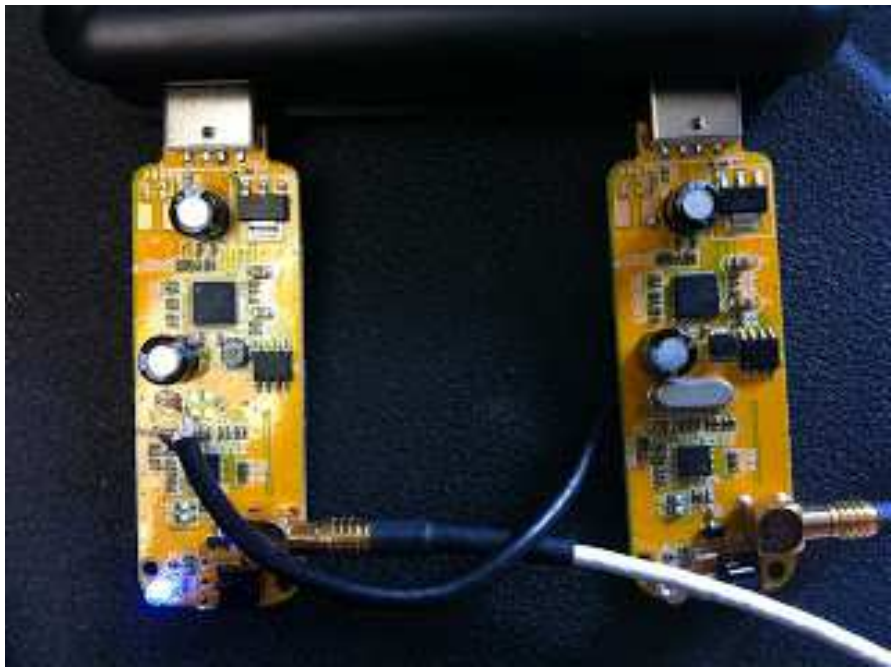
Experiments – RTL_POWER

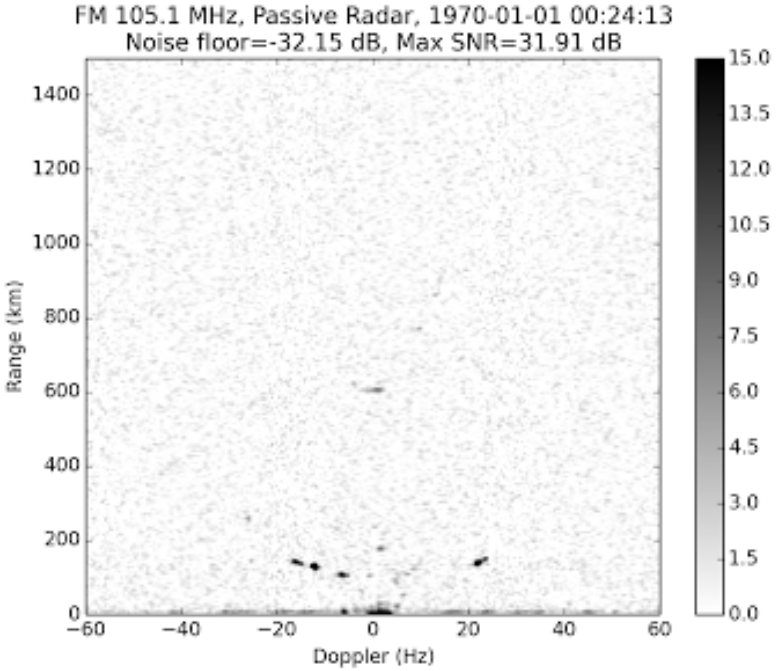


http://kmkeen.com/rtl-power/

Experiments – Passive Radar

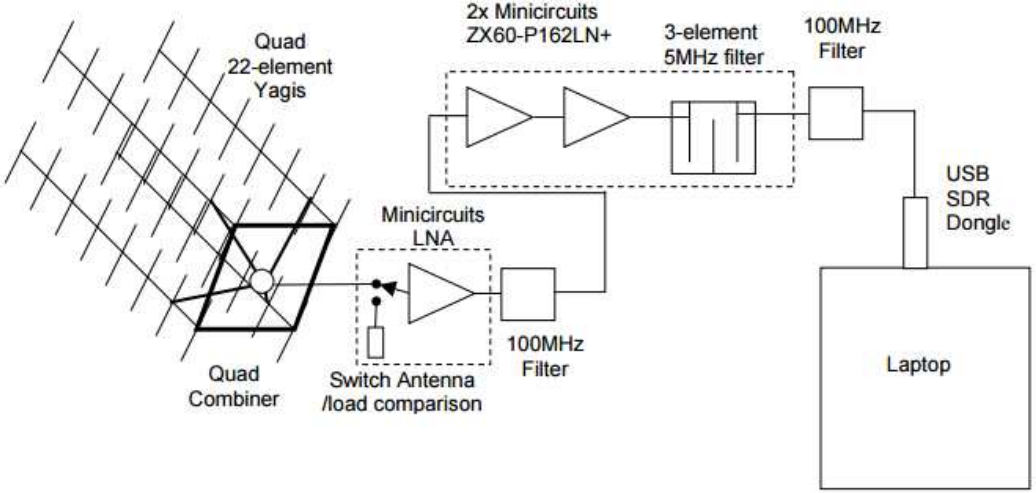
http://kaira.sgo.fi/2013/09/16-dual-channel-coherent-digital.html
http://kaira.sgo.fi/2013/09/passive-radar-with-16-dual-coherent.html

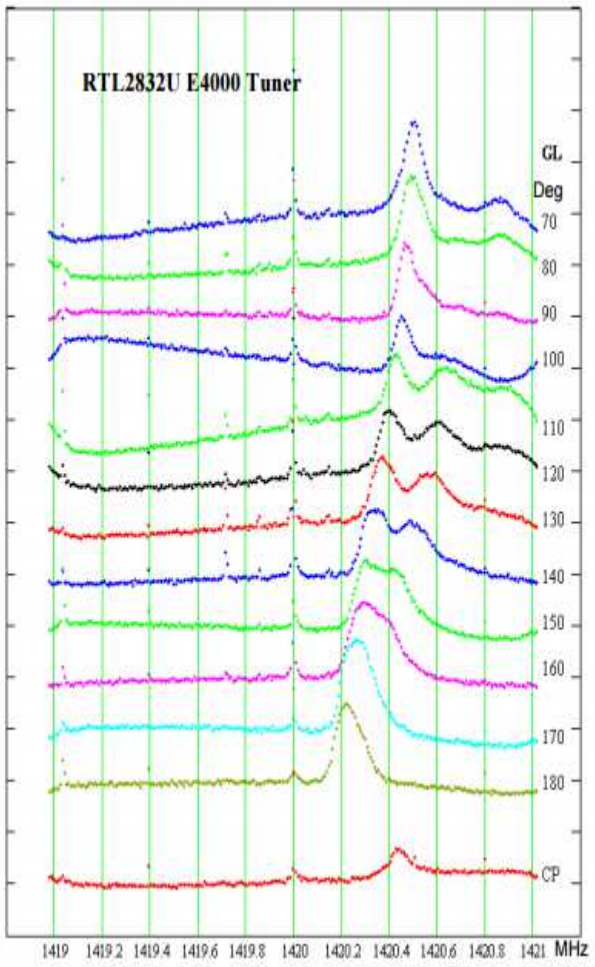




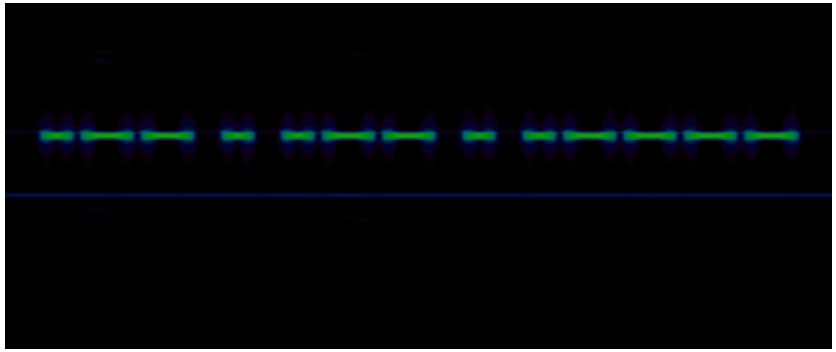
Experiments – Radio Astronomia

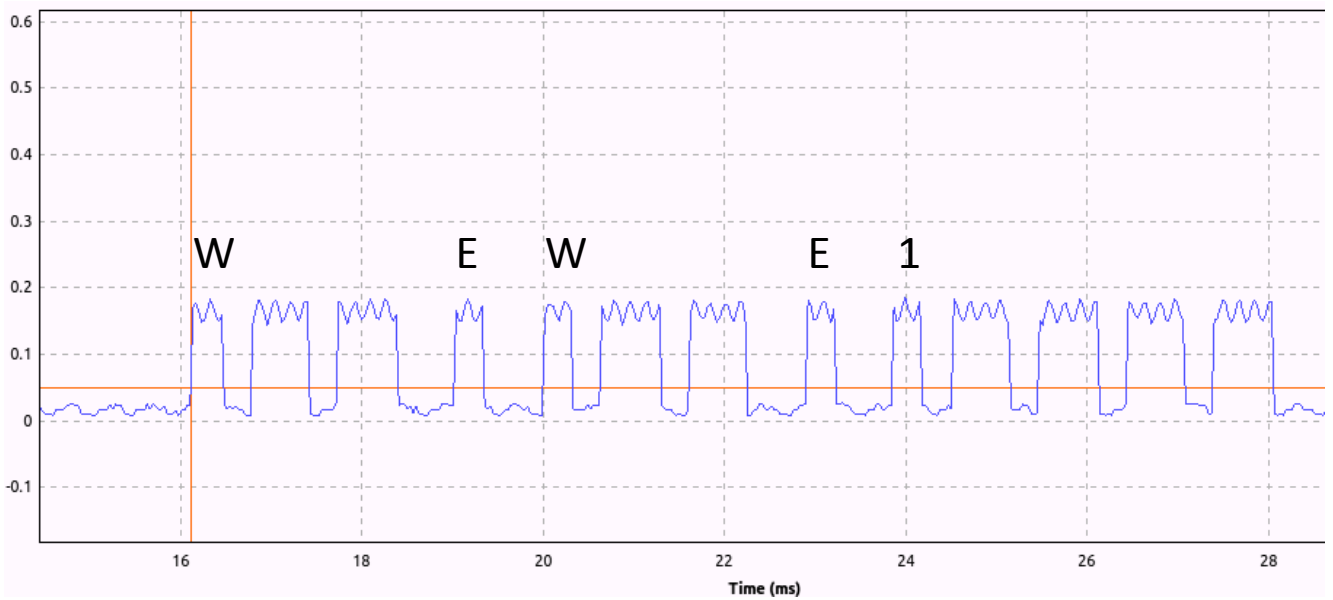
http://www.y1pwe.co.uk/RAProgs/HLRrtl2U.pdf



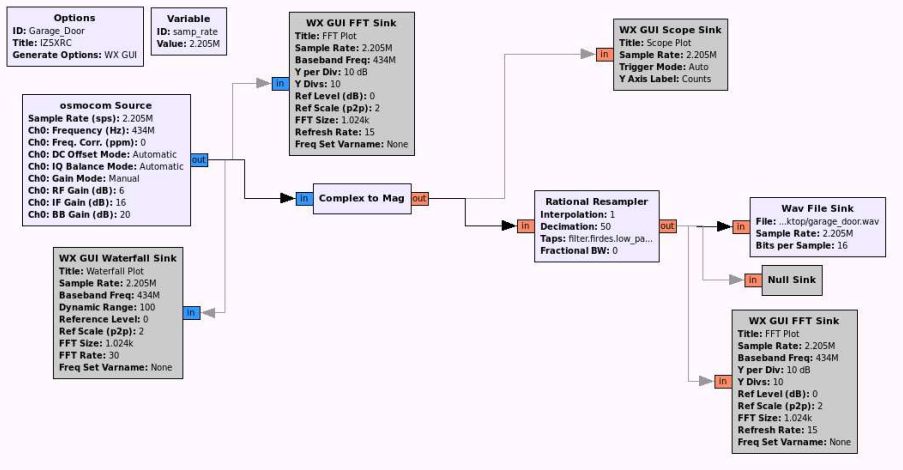


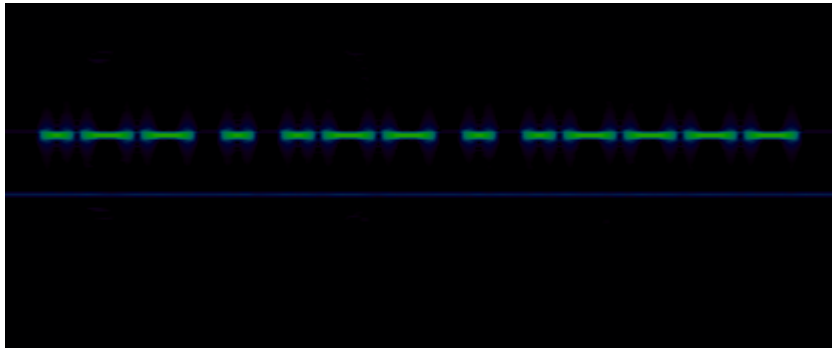
Experiments – OOK... CW ?

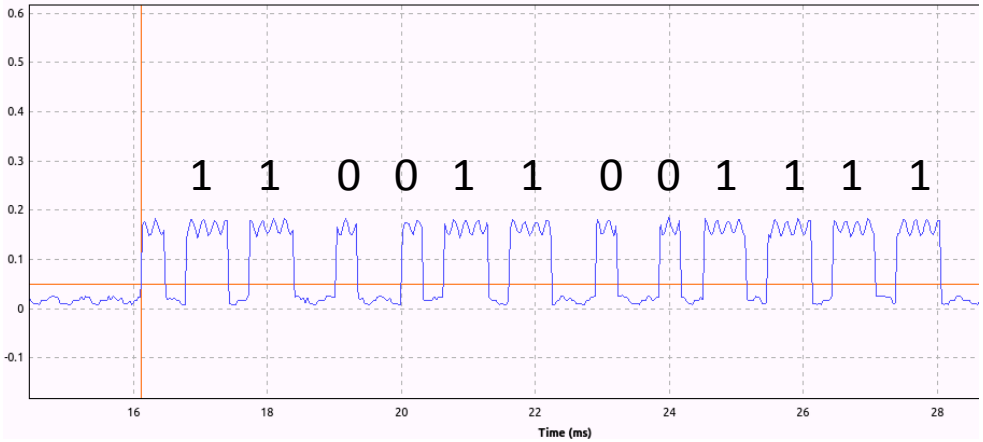




Experiments – No…. Key Fob + Garage Door!!!





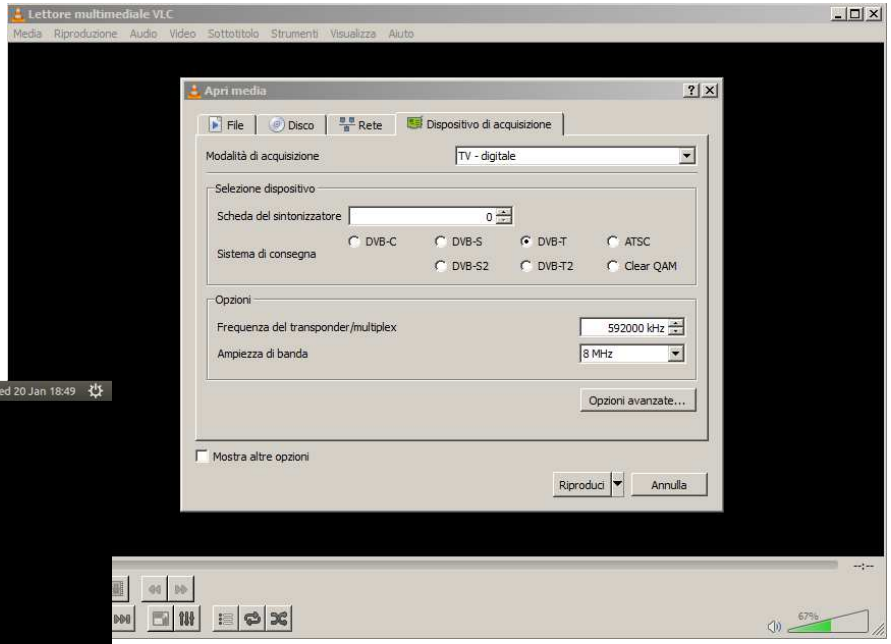


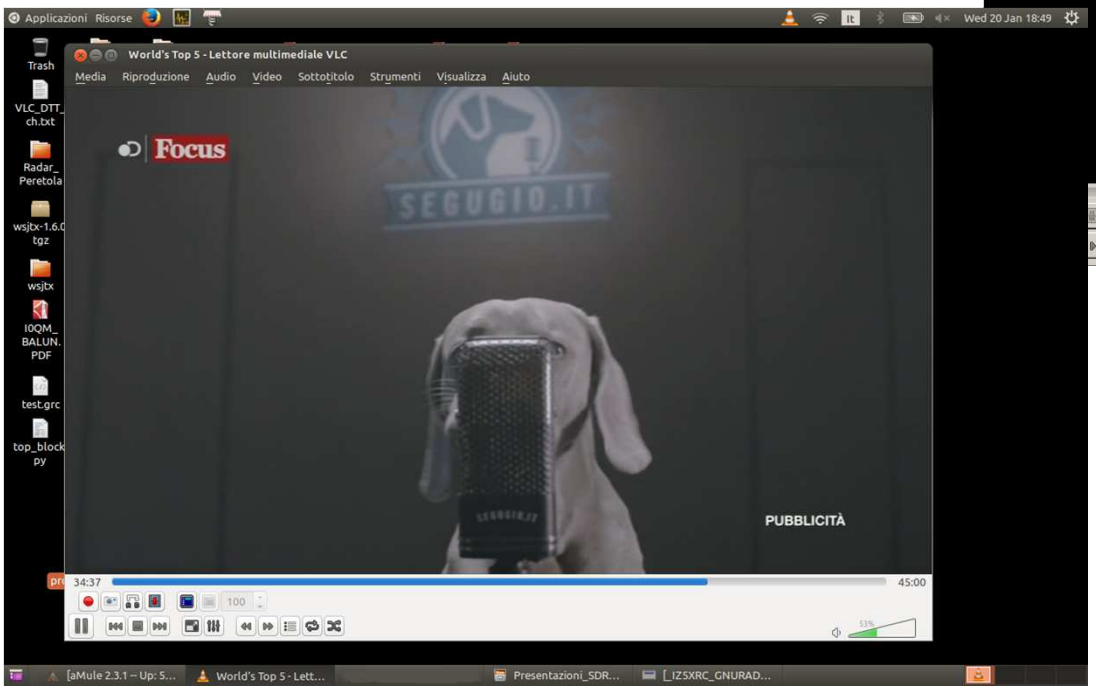
Experiments – DVB-T 1/2

`http://wirbel.htpc-forum.de/w_scan/w_scan-20141122.tar.bz2`

Riga di comando:

```
$ w_scan -ft -c IT -L > vlc_channels.xspf
$ vlc vlc_channels.xspf
```



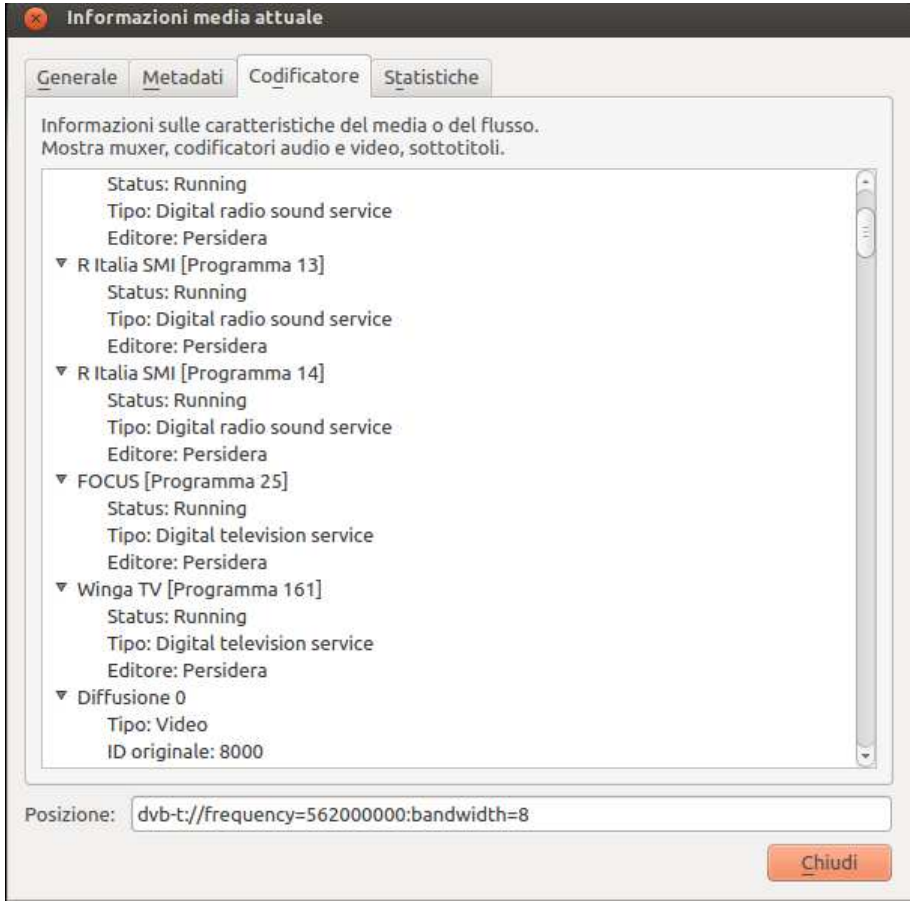


Experiments – DVB-T 2/2

…oppure creare un file di nome ‘prova.m3u’ che contiene :

```
dvb-t://frequency=490000000:bandwidth=8
```

aprire il file con VLC e selezionare dai menù: **strumenti -> Informazioni codificatore**



Con le info che appaiono si può creare
un altro file ‘programmi.m3u’:

```
#EXTM3U
#EXTINF:0,RAIUNO
#EXTVLCOPT:program=3401
dvb-t://frequency=490000000:bandwidth=8
```

Basta ripetere la sezione evidenziata in celeste
per tutti i programmi che interessano

Risorse Internet

http://sdr.osmocom.org/trac/wiki/rtl-sdr

Known Apps

The following 3rd party applications and libraries are successfully using either librtlsdr directly or the corresponding gnuradio source (gr-osmosdr):

Name	Type	Author	URL
gr-pocsag	GRC Flowgraph	Marcus Leech	https://www.cgran.org/browser/projects/gr-pocsag/trunk
multimode RX (try first!)	GRC Flowgraph	Marcus Leech	https://www.cgran.org/browser/projects/multimode/trunk
simple_fm_rvc	GRC Flowgraph	Marcus Leech	https://www.cgran.org/browser/projects/simple_fm_rcv/trunk
python-librtlsdr	Python Wrapper	David Basden	https://github.com/dbasden/python-librtlsdr
pyrtlsdr	Python Wrapper	Roger	https://github.com/roger-/pyrtlsdr
rtlsdr-waterfall	Python FFT GUI	Kyle Keen	https://github.com/keenerd/rtlsdr-waterfall
Wireless Temp. Sensor RX	Gnuradio App	Kevin Mehall	https://github.com/kevinmehall/rtlsdr-433m-sensor
QtRadio	SDR GUI	Andrea Montefusco et al.	http://napan.ca/ghpsdr3/index.php/RTL-SDR
gqrx	SDR GUI	Alexandru Csete	https://github.com/csete/gqrx
rtl_fm	SDR CLI	Kyle Keen	merged in librtlsdr master
SDR#	SDR GUI	Youssef Touil	http://sdrsharp.com/ and Windows Guide or Linux Guide
tetra_demod_fft	Trunking RX	osmocom team	osmosdr-tetra_demod_fft.py and the HOWTO
airprobe	GSM sniffer	osmocom team et al	http://git.gnumonks.org/cgi-bin/gitweb.cgi?p=airprobe.git
gr-smartnet (WIP)	Trunking RX	Nick Foster	http://www.reddit.com/r/RTLSDR/comments/us3yo/rtlsdr_smartnet/ Notes from the author
gr-air-modes	ADS-B RX	Nick Foster	https://www.cgran.org/wiki/gr-air-modes call with --rtlsdr option
Linrad	SDR GUI	Leif Asbrink (SM5BSZ)	http://www.nitehawk.com/sm5bsz/linuxdsp/hware/rtlsdr/rtlsdr.htm DAGC changes were applied to librtlsdr master
gr-ais (fork)	AIS RX	Nick Foster Antoine Sirinelli Christian Gagneraud	https://github.com/chgans/gr-ais
GNSS-SDR	GPS RX (Realtime!)	Centre Tecnològic de Telecomunicacions de Catalunya	Documentation and http://www.gnss-sdr.org
LTE-Cell-Scanner	LTE Scanner / Tracker	James Peroulas Evrytania LLC	http://www.evrytania.com/lte-tools https://github.com/Evrytania/LTE-Cell-Scanner

www.rtl-sdr.com

www.reddit.com/r/RTLSDR

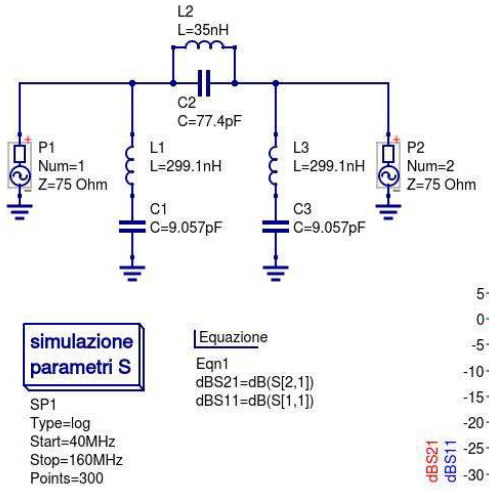
https://github.com/josemariaaraujo/ExtIO_RTL

FILTRI

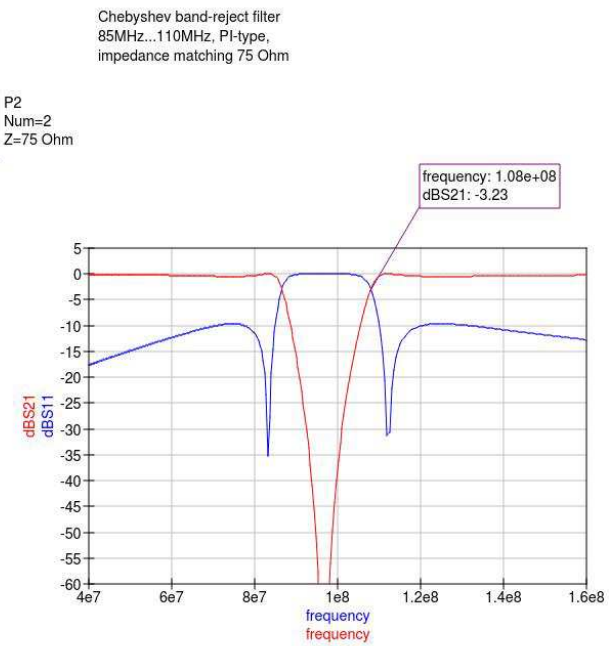
E’ consigliato l’uso di filtri per l’abbattimento delle broadcast FM

COAX STUB

Filtro Stop Band

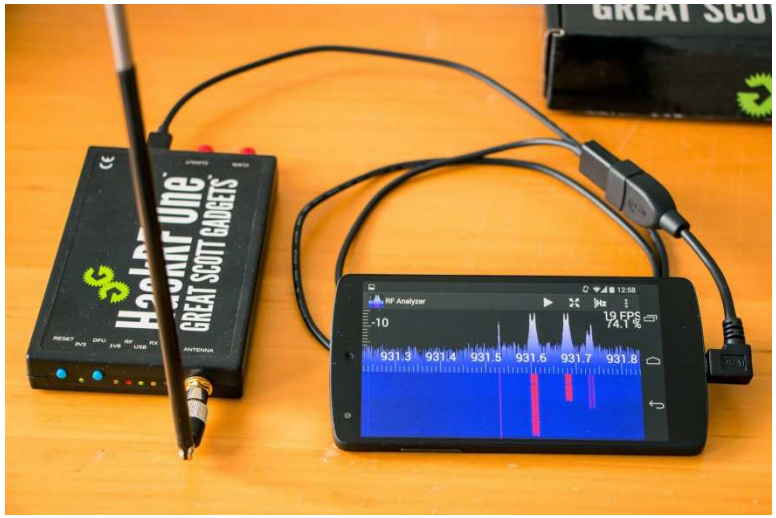


QucsFilter



Non Solo RX

https://greatscottgadgets.com/hackrf/



http://www.ettus.com/product/details/UB200-KIT

Michael Ossmann ----> http://greatscottgadgets.com/sdr/ lezioni sulle SDR

http://www.icomamerica.com/en/products/amateur/hf/7300/default.aspx

Dimostrazioni Live

Grazie