SNIFFING THE AIRWAVES WITH RTL-SDR

YASHIN MEHABOOBE

ARCANUMX

#WHOAMI?

- Security researcher, OpenSecurity
- Organiser, Defcon Kerala
- Likes hardware hacking, malware analysis and CTFs
- Invited to Kaspersky CyberConference, Nullcon, c0c0n, Toorcon San Diego and Defcon Kerala and Bangalore

Radio 101

- You have a transmitter and receiver
- Signals are encoded into a sine wave
- Frequency of the sine wave is different for different transmitters
- Antennas used for extending the range

Radio 102

- What's important:
  - Modulation
  - Frequency range
  - Transmitting power

Modulation

- Amplitude modulation
- Frequency modulation
- Phase modulation

Status of Security in Radio

- Security is low
- Encryption support exists but is not utilized
- Easily Sniffable
- Hardware for sniffing usually expensive
- Security through obscurity

BEFORE SDRS

- MIXERS, FILTERS WERE ALL IMPLEMENTED IN HARDWARE
- DIFFERENT RADIOS FOR DIFFERENT FREQUENCIES
- SINGULAR PURPOSE

Enter the SDR

- Most components implemented in software.
- Allows you to choose the filter, amplifiers and detectors
- Use soundcard as ADC.
- Ranges from cheap (RTL-SDR) to expensive (USRP)

VARIOUS TYPES OF SDR

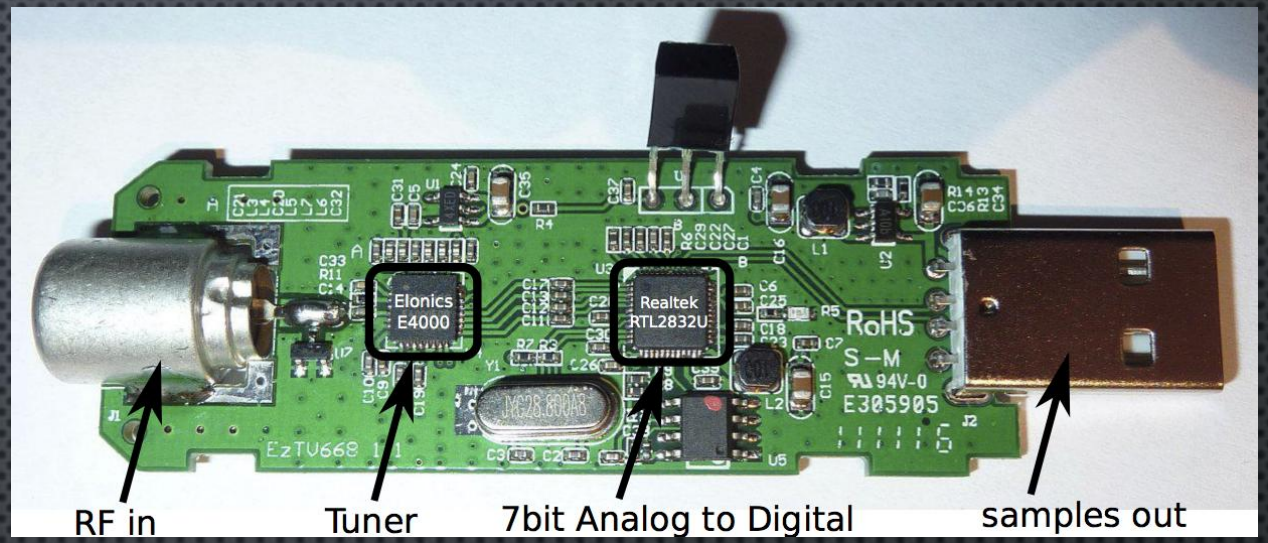
- HackRF
- BladeRF
- USRP
- Softrock
- RTL-SDR

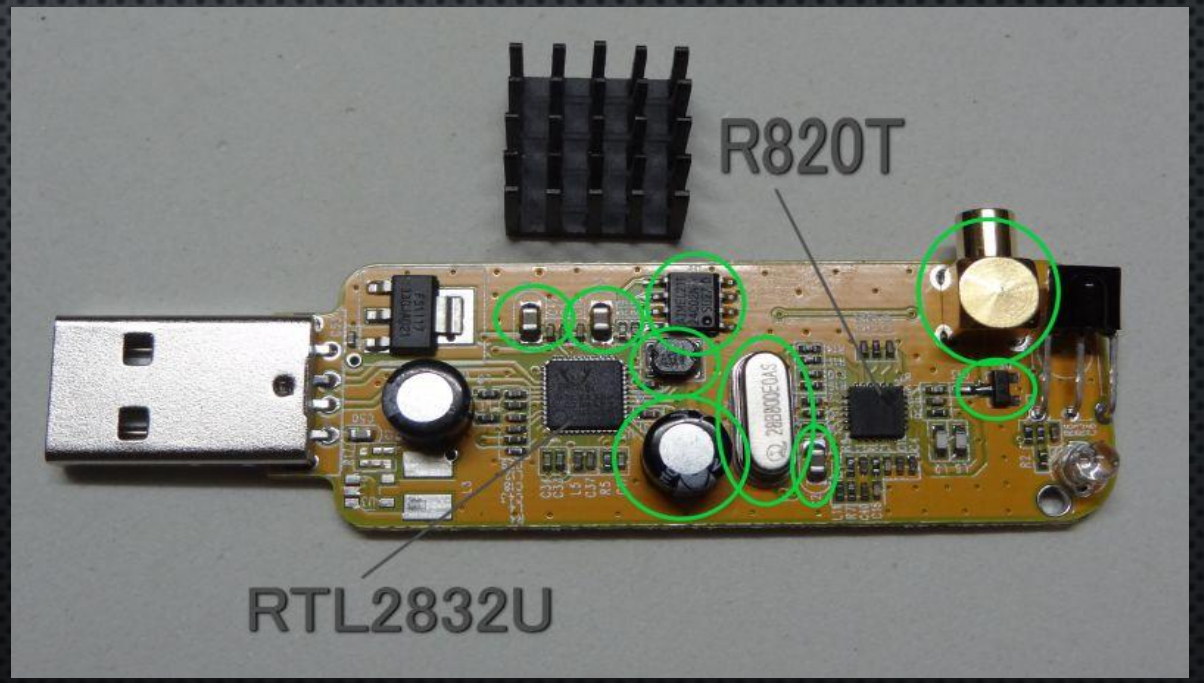
Enter the RTL-SDR

- Discovered by eric fry
- Found that RTL2832U gives raw I/Q
- Cheap ($14-$20)
- Good frequency range (~25Mhz to ~1700Mhz)
- Currently compatible with a lot of software

RTL SDR TYPES

- Mainly two types:
  - Elonics e4000 Chipset (rare)
    - Best for reception
    - 64-1700MHz
    - Slightly more expensive
  - Realtek R280T Chipset
    - Easier to find
    - 24Mhz to 1850 Mhz
    - Cheaper
    - Slightly less sensitive





What can you do with it?

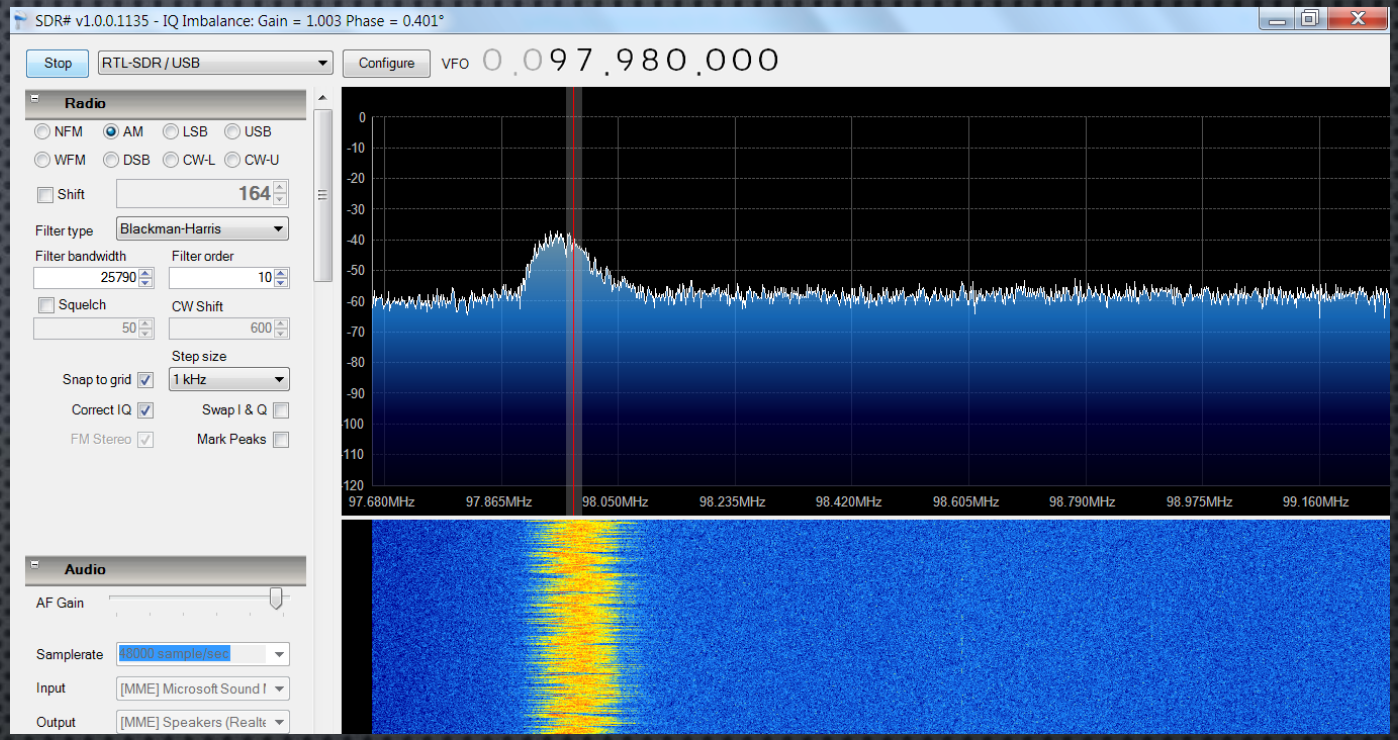
- Listen to anything in the compatible frequency range
- Use upconverters and downconverters to receive above and below
- Listen to GSM, GPS, NOAA satellite images, Tire pressure monitors and more
- Easy access to the world of SDR

"Software" Defined Radio

- Lot of software popped up after rtlsdr
- Many preexisting ones were patched with support
- Some are really difficult to set up (*cough*GNURadio*cough*)
- Kali >1.05 / Pentoo
- Would still need to reinstall rtlsdr library

SDR#

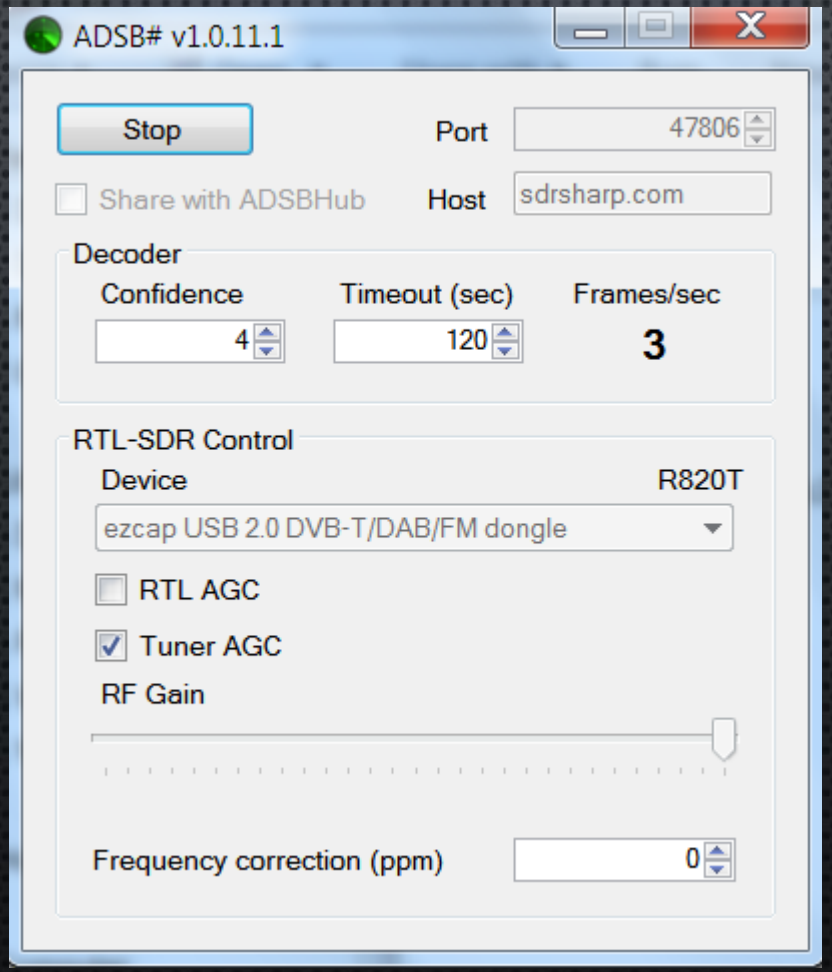
- Windows only
- Easy to use
- Zadig drivers
- Plugin friendly
- Recommeneded: Use the install script



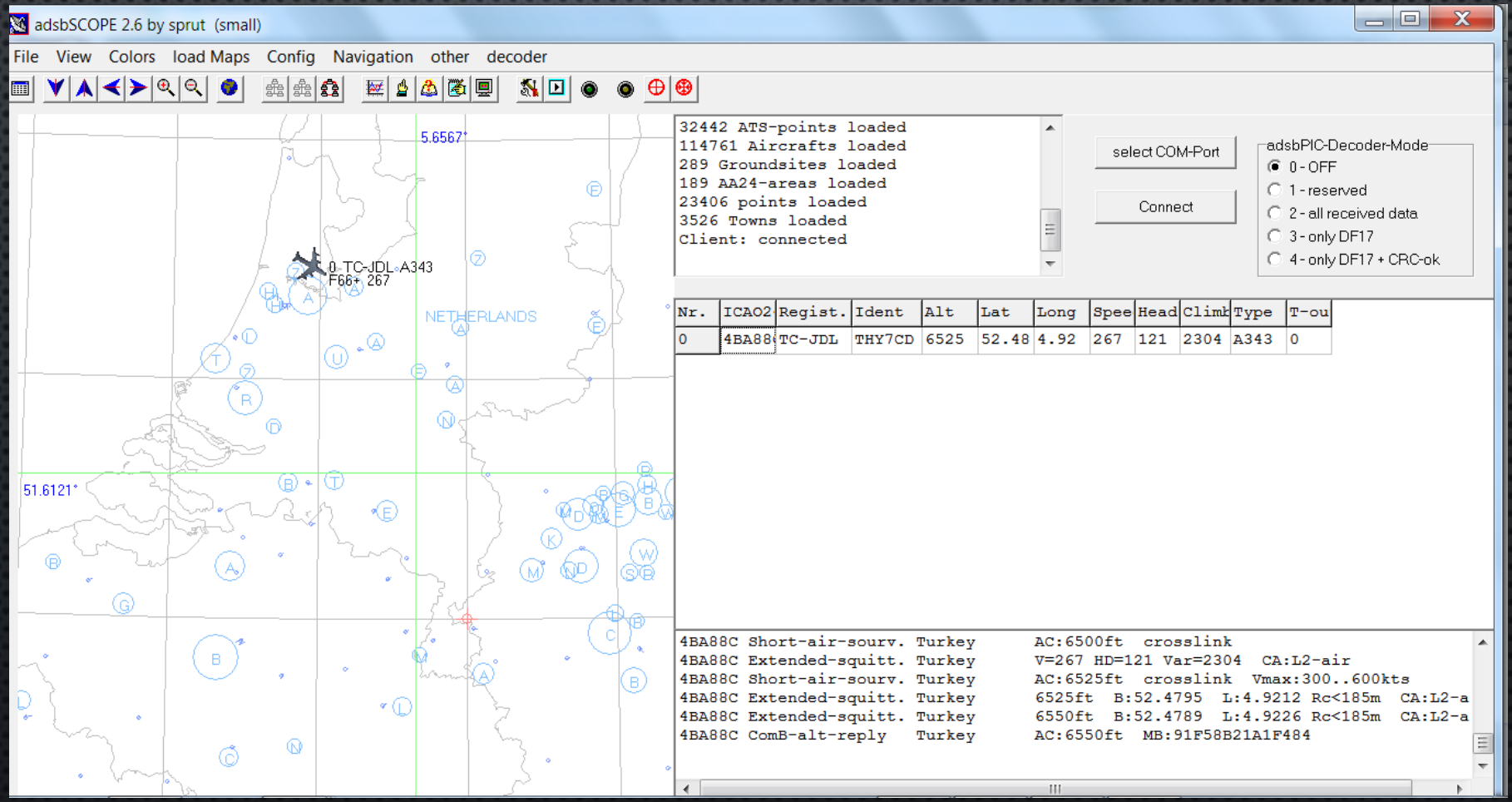
ADSB

- **Automatic dependent surveillance-broadcast**
- 1090 mhz
- Use dump1090,adsbsharp or similar
- Tranmits location,altitude, speed, heading etc
- Collinear,discone, vertically polarized antenna, ground plane, J pole

ADSBSHARP


ADSB# v1.0.11.1
Stop
Port
47806
Share with ADSBHub
Host
sdrsharp.com
Decoder
Confidence
Timeout (sec)
Frames/sec
4
120
3
RTL-SDR Control
Device
R820T
ezcap USB 2.0 DVB-T/DAB/FM dongle
RTL AGC
Tuner AGC
RF Gain
Frequency correction (ppm)
0

ADSB SCOPE

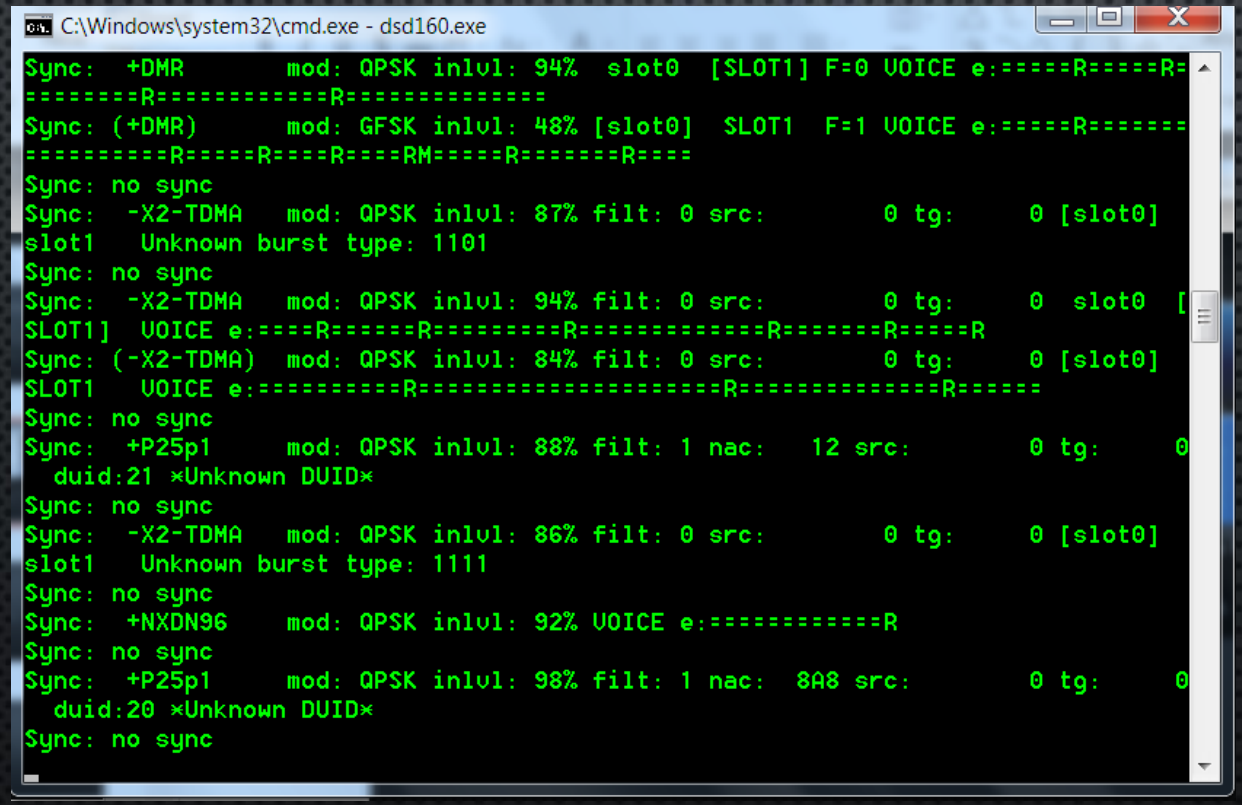

adsbSCOPE 2.6 by sprut (small)
File View Colors load Maps Config Navigation other decoder
32442 ATS-points loaded
114761 Aircrafts loaded
289 Groundsites loaded
189 AA24-areas loaded
23406 points loaded
3526 Towns loaded
Client: connected
select COM-Port
Connect
adsbPIC-Decoder-Mode
0 - OFF
1 - reserved
2 - all received data
3 - only DF17
4 - only DF17 + CRC-ok
5.6567°
51.6121°
NETHERLANDS
0 TC-JDL A343
F68+ 267
Nr. ICAO2 Regist. Ident Alt Lat Long Spee Head Climb Type T-ou
0 4BA88 TC-JDL THY7CD 6525 52.48 4.92 267 121 2304 A343 0
4BA88C Short-air-sourv. Turkey AC:6500ft crosslink
4BA88C Extended-squitt. Turkey V=267 HD=121 Var=2304 CA:L2-air
4BA88C Short-air-sourv. Turkey AC:6525ft crosslink Vmax:300..600kts
4BA88C Extended-squitt. Turkey 6525ft B:52.4795 L:4.9212 Rc<185m CA:L2-a
4BA88C Extended-squitt. Turkey 6550ft B:52.4789 L:4.9226 Rc<185m CA:L2-a
4BA88C ComB-alt-reply Turkey AC:6550ft MB:91F58B21A1F484

DSD

- Digital speech recorder
- Walkie talkies
- P25 radios
- etc

```
Digital Speech Decoder 1.6.0 beta with Auto P25 & DMR Filter
mbelib version 1.2.4
Audio In/Out Device: /dev/dsp
Sync:  -X2-TDMA   mod: QPSK inlvl:  7% filt: 0 src:       0 tg:     0 [slot0]
slot1   Unknown burst type: 1101
```

DSD RUNNING ON WINDOWS



RTL1090


OPEN
RTL1090 - (c) jetvision.de - B:103
BETA
1090.000 MHz
STOP
ICAO C/S ALT..MCP V/S GS TT SSR G*456^ SG MSGS
4CA5B0 AZA121 F076>090 +25 281 086 3173 *... 7 57
List
Table
Stats
I/SI
>10 >20 >40 >80 >120 >180
UDP BS TCP HTTP
78 ms 1/sec THR: -79db [8] Port:31001 A/C: 1 R820T-00000001

GNU Radio

- Difficult to install and configure
- Versatile and one of the most powerful
- Block architecture
- Sources produce data
- Sinks allow you to save or display outputs
- Using gr3.6.5

RTL_SDR CODEBASE

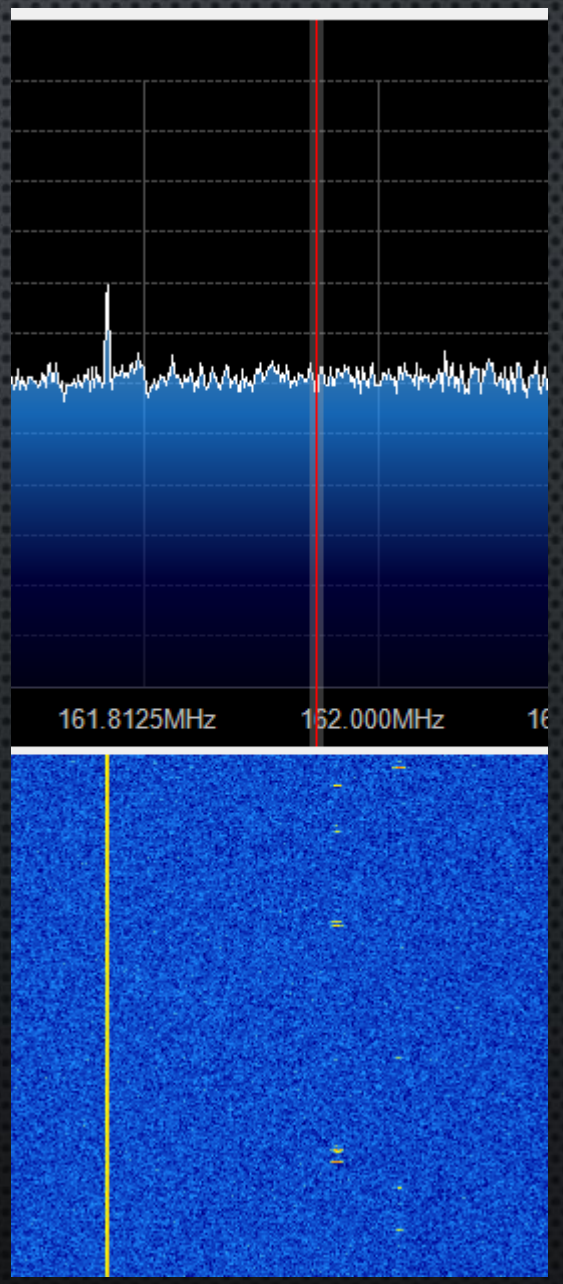
- Testing the presence and perform basic SDR output/transfer
- Rtl_fm (Basic fm receiver)
- Rtl_test (tests if the device is attached)
- Rtl_sdr (raw I/Q data)
- Rtl_tcp (to transmit raw I/Q)
- Kalis rtl-sdr will need to be reinstalled

GQRX

- Similar functionality to sdrsharp
- Preinstalled in kali
- FFT + Waterfall display
- Built on top of gnuradio
- Allows remote control

AIS

- Automatic identification system
- Two channels : Channel 87 (161. 975 Mhz) and Channel 88 (162.025 Mhz)
- Heard as blips
- Can be fed via virtualaudio cable to AISMON or shipplotter
- Sound heard as blips



ACARS

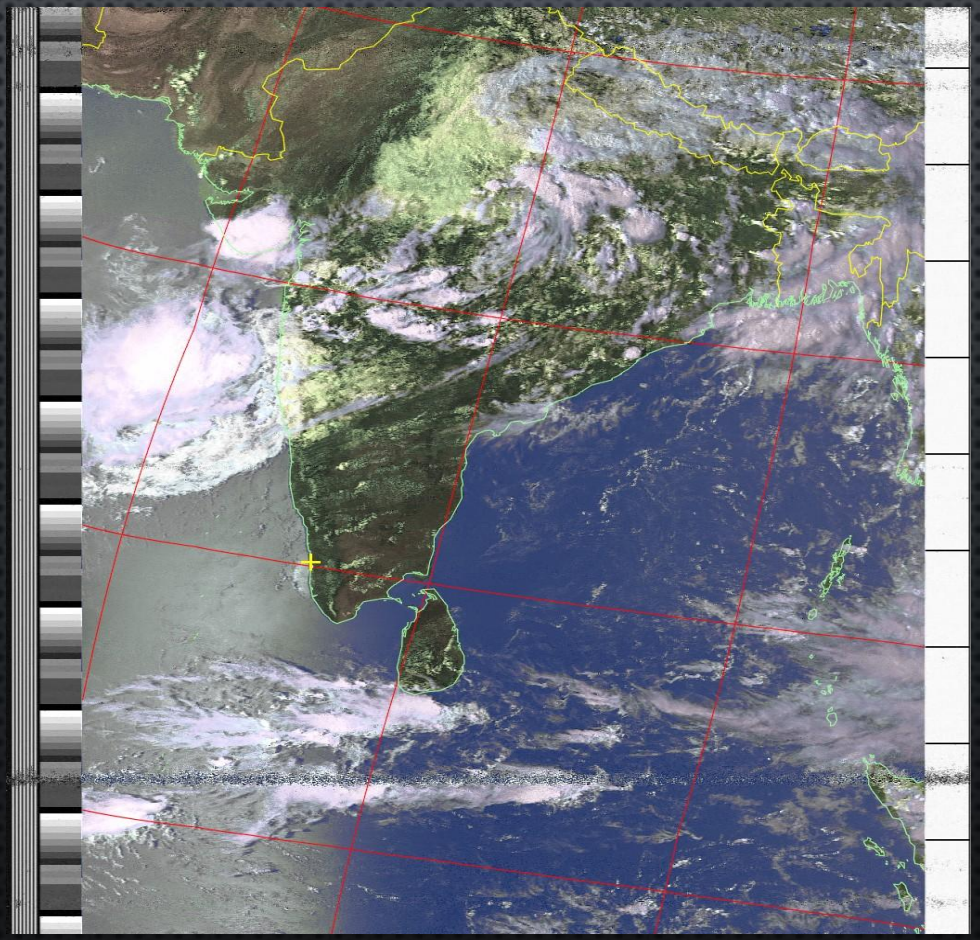
- **Aircraft Communications Addressing and Reporting System**
- **~133 Mhz**. Varies regionwise
- Usually don't contain location information (unlike ADS-B)
- used in avionics systems (seems gibberish)
- Audio piping method to decode
- Antenna: J Pole, Discone, colinear

NOAA SATELLITES

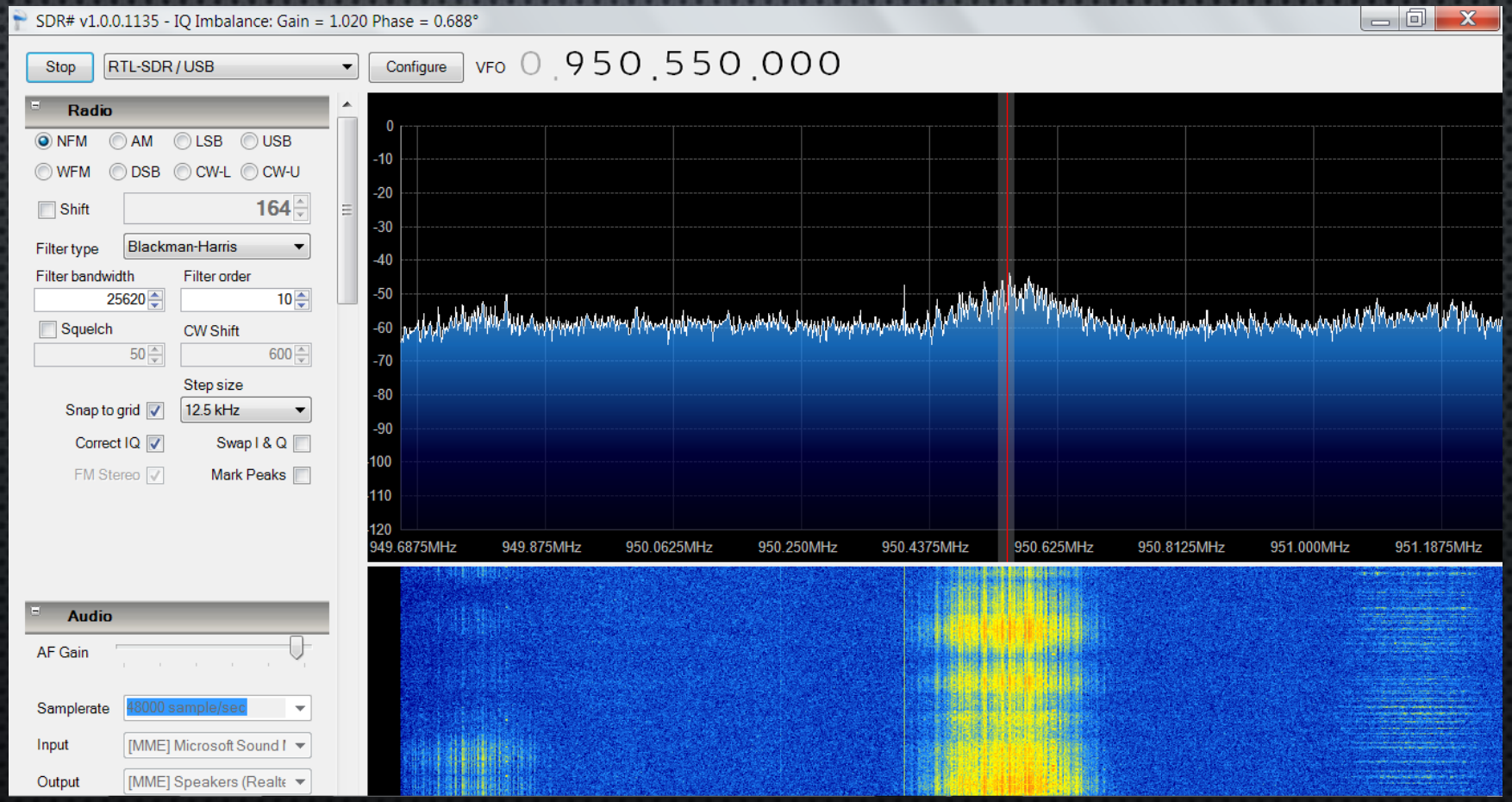
- Weather image satellites
- Circularly polarized antenna required
- Works at 137 mhz
- Software: Orbitron, wxtoimg, vb-cable, sdrsharp
- Antennaes: Ground plane, turnstile,QFH

GP ANTENNA USED

NOAA IMAGE



GSM


SDR# v1.0.0.1135 - IQ Imbalance: Gain = 1.020 Phase = 0.688°
Stop
RTL-SDR / USB
Configure
VFO
0.950.550.000
Radio
NFM
AM
LSB
USB
WFM
DSB
CW-L
CW-U
Shift
164
Filter type
Blackman-Harris
Filter bandwidth
25620
Filter order
10
Squelch
50
CW Shift
600
Step size
Snap to grid
12.5 kHz
Correct IQ
Swap I & Q
FM Stereo
Mark Peaks
Audio
AF Gain
Samplerate
48000 sample/sec
Input
[MME] Microsoft Sound
Output
[MME] Speakers (Realte
0
-10
-20
-30
-40
-50
-60
-70
-80
-90
-100
-110
-120
949.6875MHz
949.875MHz
950.0625MHz
950.250MHz
950.4375MHz
950.625MHz
950.8125MHz
951.000MHz
951.1875MHz

Identifying signals

- Identify using the waterfall
- Identify the modulation used
- Frequency tells you a lot
- Also strength of the signal

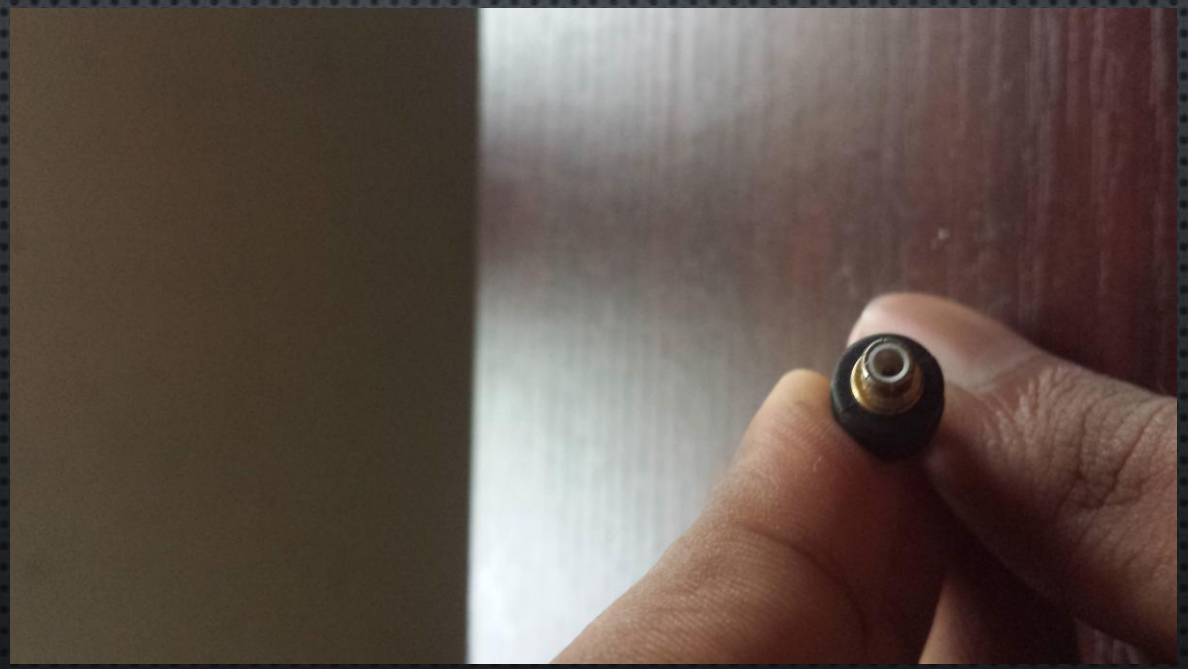
Modifications

- Interference limiting
- New antennas
- LNA

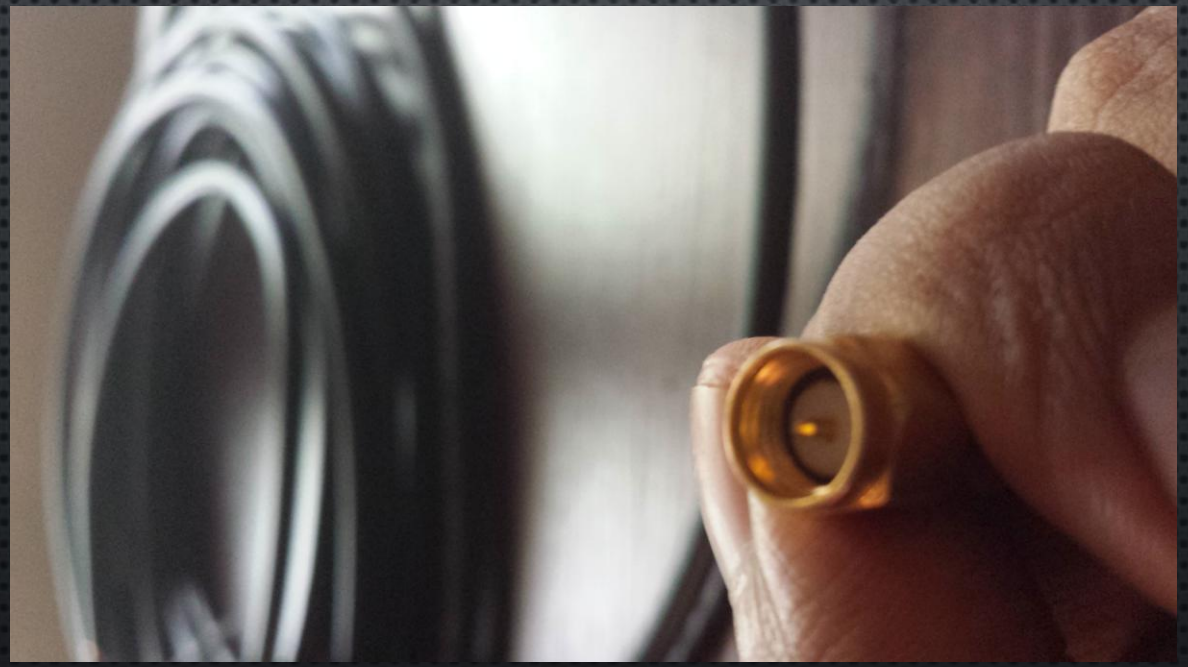
ANTENNAS

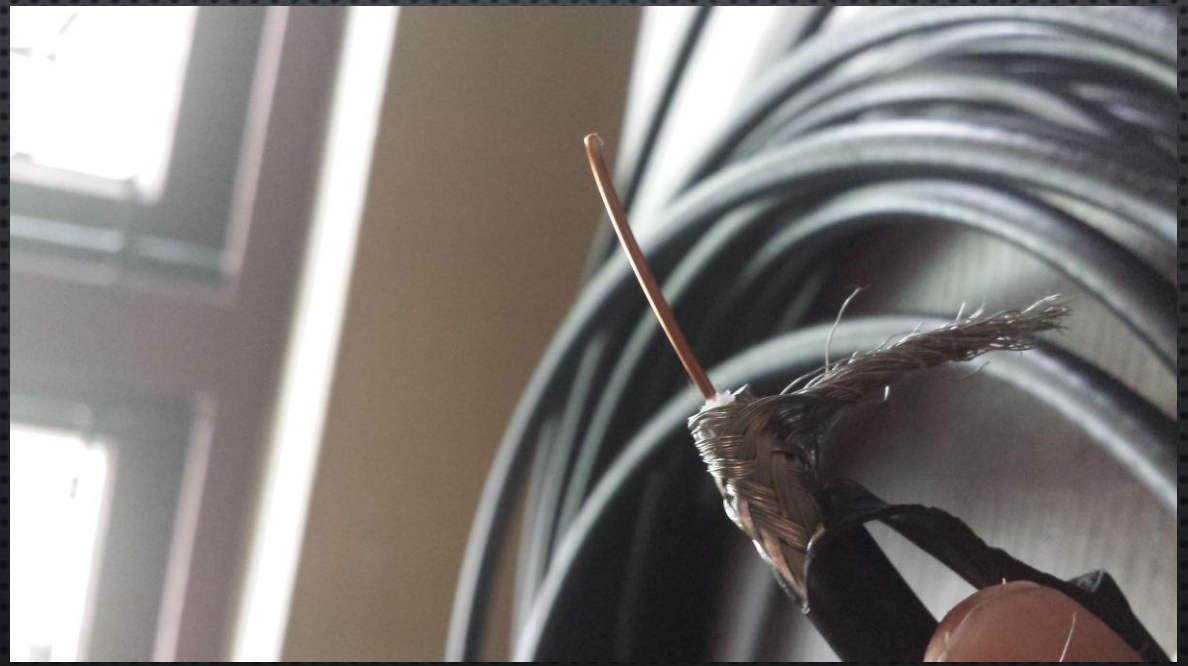
- Ground plane
- discone

MCX CONNECTOR



SMA CONNECTOR

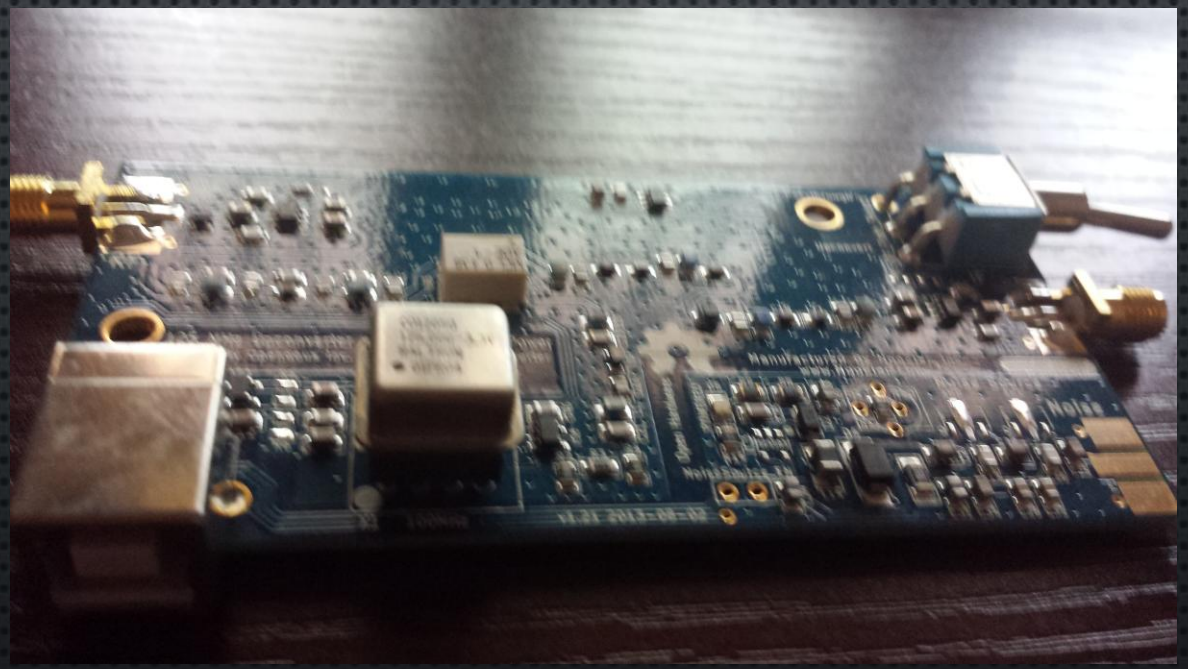




Upconverters

- Upconverters allow you to listen to frequencies below the RTL SDR range
- Nooelec ham it up upconverter is a good choice
- Pass through and upconvert may be mixed
- Connect power and sdr

HAM IT UP



GOTCHAS

- Version of GRC
- Rtlsdr module blacklisting
- Antenna
- Interference
- Wrong frequencies

So what about TX?

- Use hackrf
- RFCAT is a low cost alternative
- BladeRF
- Generic 433 mhz transmitters

Sniffing with other hardware

- NRF24L01+ allows you to sniff BLE
- RFCat is good for sniffing and replaying
- Ubertooth one

THANK YOU!