An Introduction to Software Defined Radio

Pamela O'Shea, OWASP Melbourne App Sec Day, 17th September 2016
Twitter: @0xsh_

Cyberspectrum Melbourne

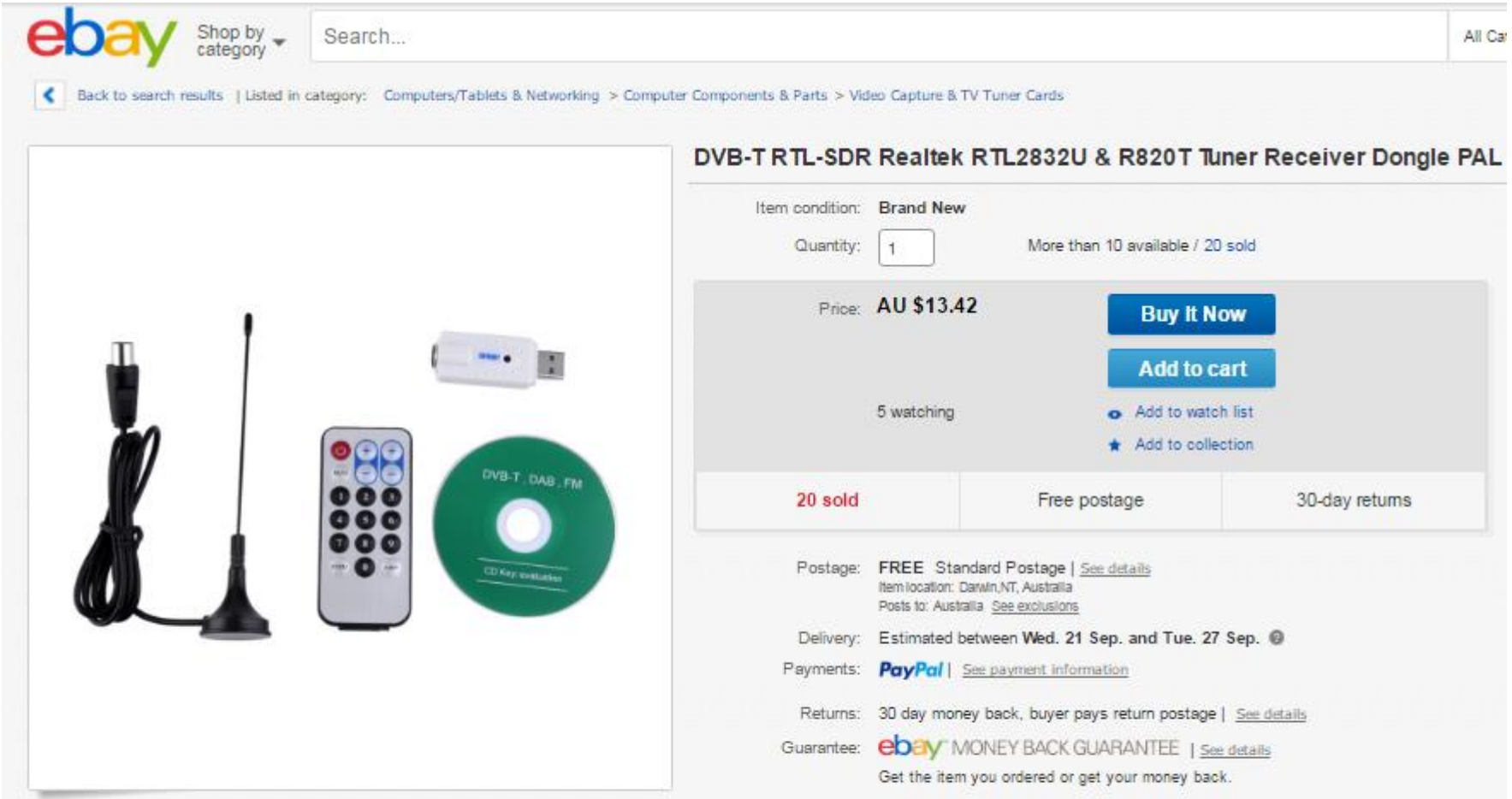
Twitter	**@sdr_melbourne**
Email	**sdr.melbourne@gmail.com**
Slack	**sdr-melbourne.slack.com (email for an invite)**
Meetup	**https://www.meetup.com/Cyberspectrum-Melbourne**
Blog	**http://randomkeystrokes.com/category/sdr/**
Github	**https://github.com/sdr-melbourne**
YouTube	**https://www.youtube.com/channel/UCLBloqxOXEj4fH7s ULA (SDR Melbourne Channel)**

Contents

1. Hardware/Software
2. Planes
3. Ships
4. Pagers
5. Home devices
6. Scanning the ground
7. Scanning on the move
8. Scanning the sky
9. GSM

1a. Hardware

- RTL-SDR Dongle: Great value receiver!
- Start one like this e.g. Realtek chip.

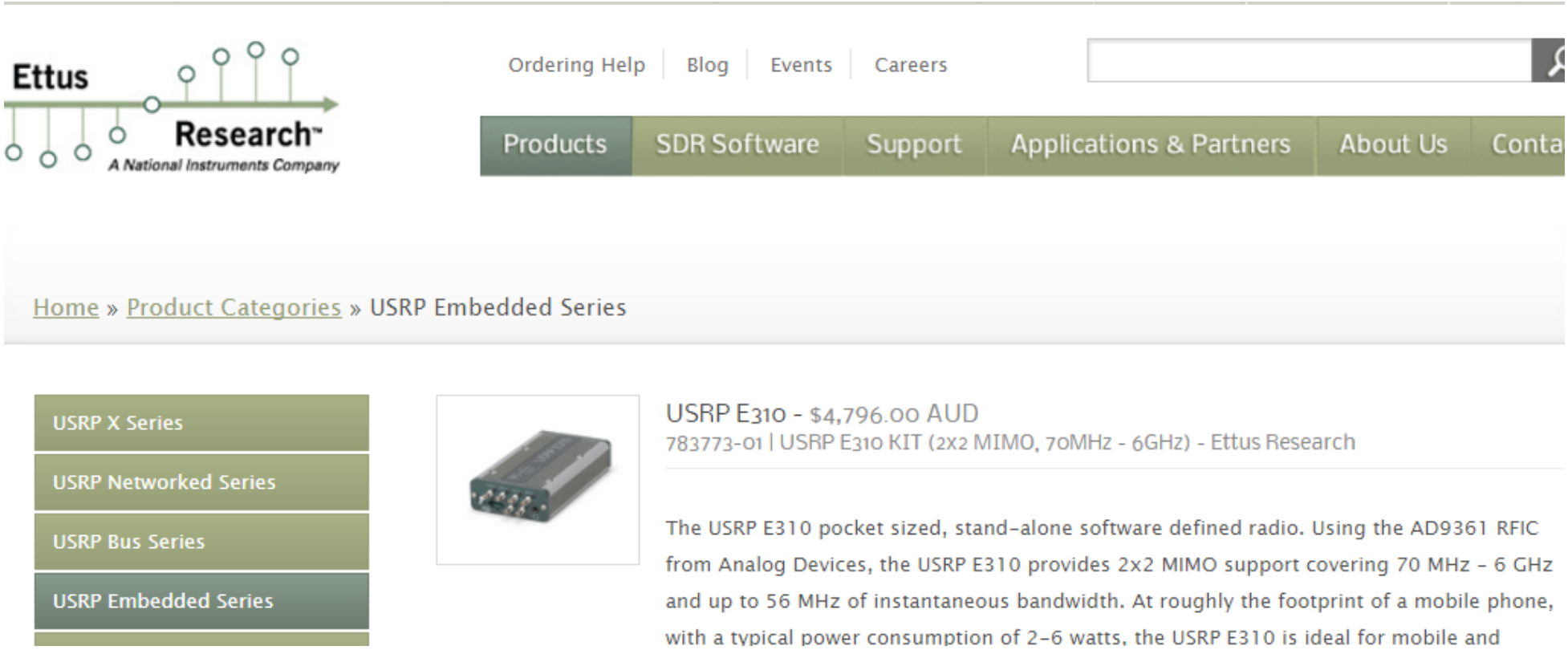


1a. Hardware

- HackRF One: Greater bandwidth, also transmits

1a. Hardware

- USRF: Greater bandwidths, bigger league.



1b. Software

- GNU RADIO

gnuradio.org/redmine/projects/gnuradio/wiki

Home Projects Help

GNURadio
THE FREE & OPEN SOFTWARE RADIO ECOSYSTEM

Overview Activity Roadmap Issues News Wiki Files Repository

History

Welcome to GNU Radio!

Introduction

GNU Radio is a free & open-source software development toolkit that provides signal processing blocks to implement software radios. It can be used with readily-available low-cost external RF hardware to create software-defined radios, or without hardware in a simulation-like environment. It is widely used in hobbyist, academic and commercial environments to support both wireless communications research and real-world radio systems.

GNU Radio is licensed under the GNU General Public License (GPL) version 3. All of the code is copyright of the Free Software Foundation.

Content

I. Getting started

If you've never touched GNU Radio before, these pages will get you started with a running installation of GNU Radio and will show you how to take your first steps with this software radio tool.

- What is GNU Radio and why do I want it? - Read this if you really have no idea what this project is about.
- Installing GNU Radio - This will explain all the steps to get a working installation of GNU Radio.
- How do I use GNU Radio? - A short introduction to the possibilities you have as a GNU Radio user.
  - Utilities and tools that come with GNU Radio
- Tutorials
  - Guided Tutorials
  - How to write Python applications - This includes a guide on how to read and use the Doxygen-generated API docs.
  - A quick guide on doing simulations with GNU Radio
  - How to write an out-of-tree (OOT) module
  - Tutorial on how to configure OOT packages to find and link against GNU Radio
- Frequently Asked Questions - Check this page before asking questions on the mailing list.

II. Documentation

GNU Radio has two manuals: one for the C++ API and another for the Python API. The majority of the documentation comes from using Doxygen markup comments in the public header files. These are the basis for both manuals. The Python documentation uses Sphinx to pull in both the Doxygen documentation as well as any formatted comments present in any Python files.

1b. Software

- **Linux**
  - GNU Radio have VM image, or use
  - Ubuntu is distro of choice for radio currently
  - Install with aptitude for older stable version of gnu-radio
  - Install with pybombs for latest versions
  - Works on Raspberry Pi too!

- Windows:
  - Not covering Windows here but SDR# is a good free tool of choice for Windows (same as gqrx on Linux)
  - Lots of easy to use tools on Windows
  - Check out Hak5 for tools on Windows

2. Planes

2. Planes – ADSB

- **ADSB**: Automatic dependent surveillance – broadcast
- Radar replacement
- Aircraft gets position from satellite and broadcasts it for tracking
- No encryption or authentication
- 1090 Mhz (or 978 Mhz)

2. Planes – dump1090: list aircraft

- Tool: **Dump1090**

  https://github.com/antirez/dump1090

  $ dump1090 --interactive --aggressive

```
posheal@frostbyte | Battery 0: Full, 100%
Hex    Flight   Altitude  Speed   Lat       Lon       Track  Messages Seen  .
--------------------------------------------------------------------------------
7c6c94 JST449   2275      171     -37.671   144.994   275    83       6 sec
7c6c2a TGW541   4100      236     -37.572   145.001   93     42       29 sec
```

2. Planes – modes_rx

- Tool: **modes_rx**

  https://github.com/bistromath/gr-air-modes

  $ apt-get install gr-air-modes

  $ modes_rx -d -P use -s osmocom

```
pi@raspberrypi:~ $ modes_rx -d -s osmocom -P
linux; GNU C++ version 4.9.1; Boost_105500; UHD_003.007.003-0-unknown

gr-osmosdr 0.1.3 (0.1.3) gnuradio 3.7.5
built-in source types: file osmosdr fcd rtl rtl_tcp uhd miri hackrf bladerf rfsp
ace airspy
Using FUNcube Dongle V2.0 (hw:1)
gr::log :INFO: audio source - Audio source arch: alsa
Opened: hw:1
Using Volk machine: neon_hardfp_orc
Dongle sucessfully initialized
Result of Action :+++++
FCDAPP 20.03
 Lna gain enabled
 Mixer gain enabled
If gain set to: 15
Set Frequency to: 1.09e+09 Hz, corrected to: 1090000000 Hz
If gain set to: 34
Gain is 34
Rate is 4000000
(-28 0.00000000) Type 5 (short surveillance ident reply) from ed4696 with ident
3326 (SPI ALERT)
```

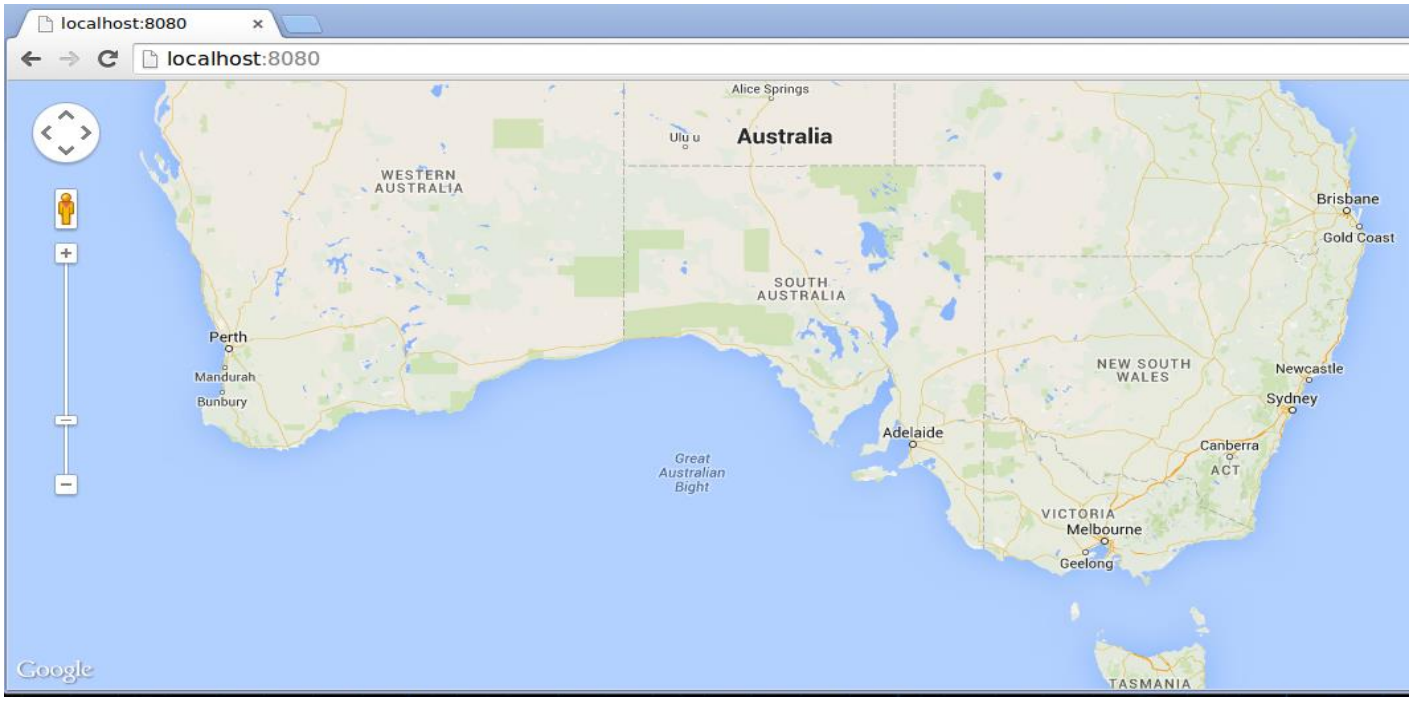
2. Planes – dump1090 Viewing on a Map

$ dump1090 --interactive --aggressive --net

Open browser on **http://localhost:8080** for map

2. Planes - dump1090: Viewing on a Map

```
Hex    Flight   Altitude  Speed   Lat       Lon       Track  Messages Seen   .
--------------------------------------------------------------------------------
c319ce          0         0       0.000     0.000     0      1        32 sec
0c1a1f          0         0       0.000     0.000     0      1        37 sec
bdf973          0         0       0.000     0.000     0      1        41 sec
cb09bf          0         0       0.000     0.000     0      1        52 sec
```



2. Planes – dump1090: Viewing messages

```
*8ce3b19f2f463e3c1d81330e61f8;
CRC: 0e61f8 (ok)
Single bit error fixed, bit 27953
DF 17: ADS-B message.
  Capability     : 4 (Level 2+3+4 (DF0,4,5,11,20,21,24,code7 - is on ground))
  ICAO Address   : e3b19f
  Extended Squitter  Type: 5
  Extended Squitter  Sub : 7
  Extended Squitter  Name: Surface Position
    Unrecognized ME type: 5 subtype: 7

*888a7fbe2e7e50c939f662bc85ce;
CRC: bc85ce (ok)
Single bit error fixed, bit 27999
DF 17: ADS-B message.
  Capability     : 0 (Level 1 (Survillance Only))
  ICAO Address   : 8a7fbe
  Extended Squitter  Type: 5
  Extended Squitter  Sub : 6
  Extended Squitter  Name: Surface Position
    Unrecognized ME type: 5 subtype: 6

*8d2b1817222070fcbda253d4f78d;
CRC: d4f78d (ok)
Single bit error fixed, bit 18760
DF 17: ADS-B message.
  Capability     : 5 (Level 2+3+4 (DF0,4,5,11,20,21,24,code7 - is on airborne))
  ICAO Address   : 2b1817
  Extended Squitter  Type: 4
  Extended Squitter  Sub : 2
  Extended Squitter  Name: Aircraft Identification and Category
    Aircraft Type  : Aircraft Type A
    Identification : HGC??ZIS

*890a3ed27f7750e80dc3620f309b;
CRC: 0f309b (ok)
Single bit error fixed, bit 27486
DF 17: ADS-B message.
  Capability     : 1 (Level 2 (DF0,4,5,11))
  ICAO Address   : 0a3ed2
  Extended Squitter  Type: 15
  Extended Squitter  Sub : 7
  Extended Squitter  Name: Airborne Position (Baro Altitude)
    F flag   : even
    T flag   : non-UTC
    Altitude : 22725 feet
    Latitude : 29702 (not decoded)
    Longitude: 115554 (not decoded)
```

3. Ships

3. Ships - AIS

- AIS: Automatic Identification System
- Tracking systems for ships
- Location
- Messages
- Similar to ADS-B
- 162Mhz

3. Ships

- Tool: **ais_rx**

  https://github.com/bistromath/gr-ais/

  $ ./ais_rx -s osmocom

- Chart plotting tool: **opencpn**

  http://opencpn.org/ocpn/

3. Ships - opencpn

4. Pagers

4. Pagers - POCSAG

- POCSAG: Post Office Code Standardisation Advisory Group
- Other pager protocols include FLEX
- Australia uses:
    - 148.3375 MHz (VHF)
    - 450.375 MHz (UHF)
    - 450.325 MHz (UHF)

4. Pagers – multimon-ng

- Tool: **multimon**

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

1. $ **gqrx**

   Tune to a pager frequency

   Filter: Wide

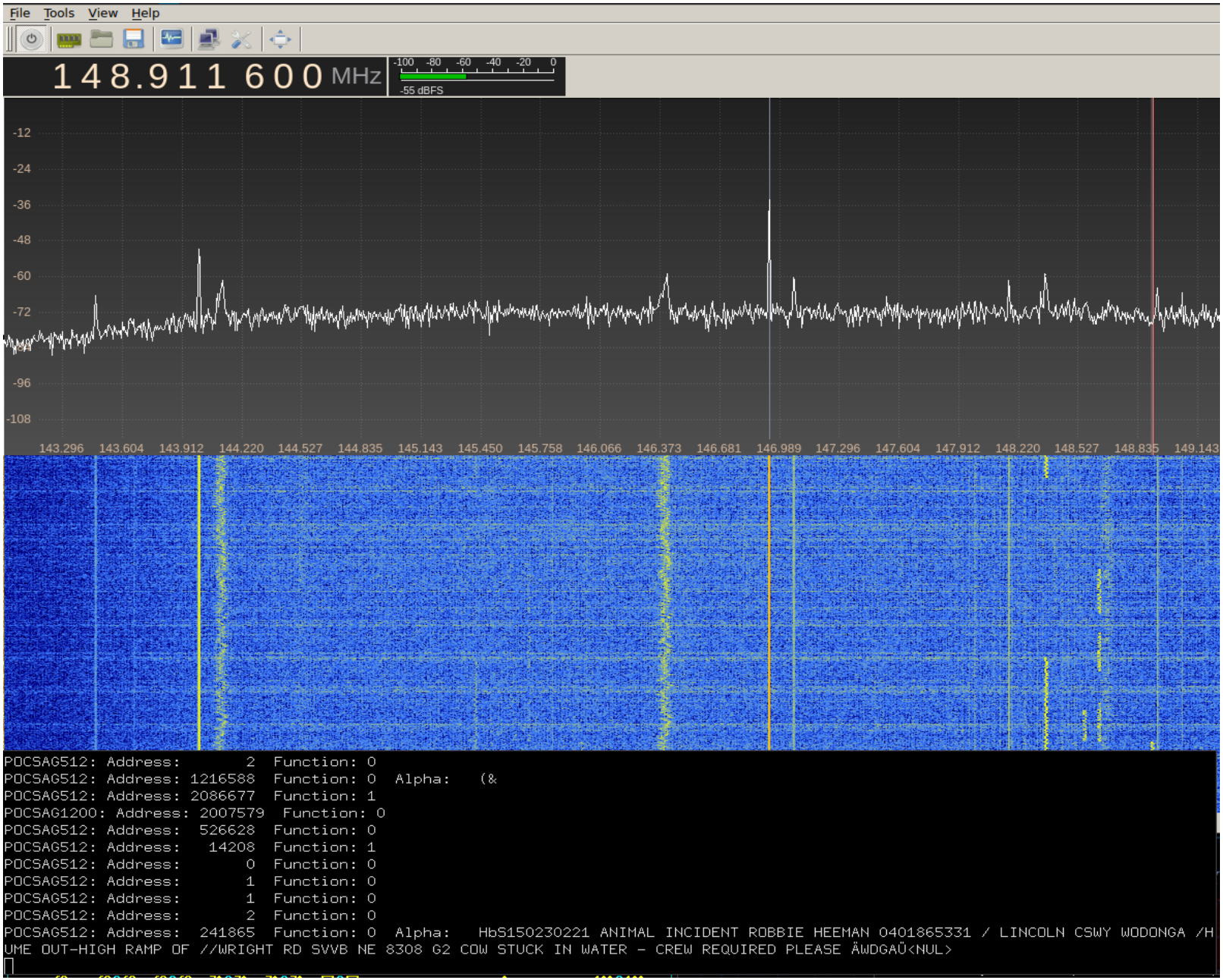
   Mode: Narrow FM

2. **$ padsp multimon-ng -a POCSAG512 -a POCSAG1200 -a POCSAG2400 -f alpha**

3. $ **pauvcontrol**

   enable recording from internal sound card

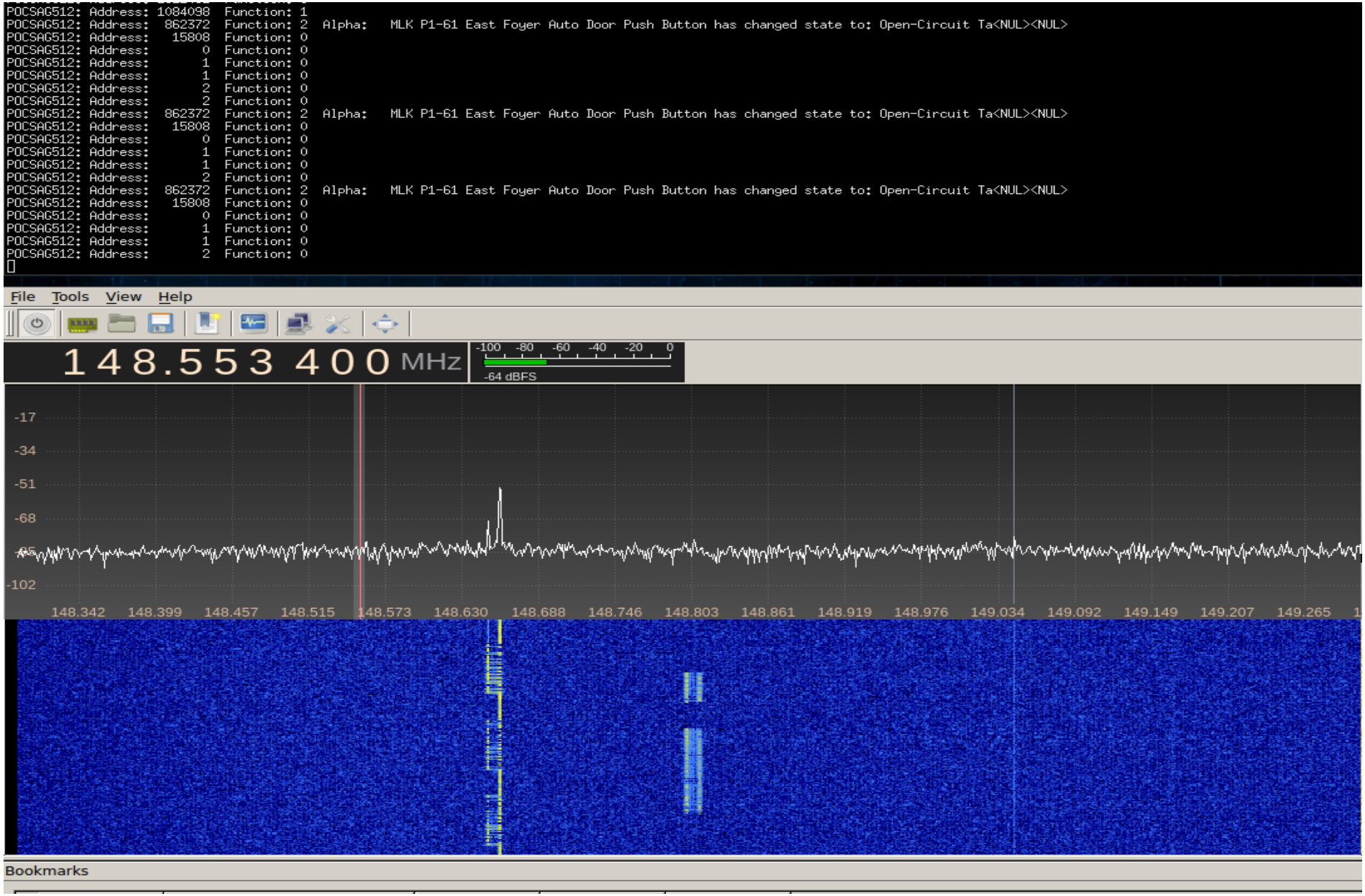
4. Pagers


File Tools View Help
148.911 600 MHz
-100 -80 -60 -40 -20 0
-55 dBFS
-12
-24
-36
-48
-60
-72
-96
-108
143.296 143.604 143.912 144.220 144.527 144.835 145.143 145.450 145.758 146.066 146.373 146.681 146.989 147.296 147.604 147.912 148.220 148.527 148.835 149.143
POCSAG512: Address: 2 Function: 0
POCSAG512: Address: 1216588 Function: 0 Alpha: (&
POCSAG512: Address: 2086677 Function: 1
POCSAG1200: Address: 2007579 Function: 0
POCSAG512: Address: 526628 Function: 0
POCSAG512: Address: 14208 Function: 1
POCSAG512: Address: 0 Function: 0
POCSAG512: Address: 1 Function: 0
POCSAG512: Address: 1 Function: 0
POCSAG512: Address: 2 Function: 0
POCSAG512: Address: 241865 Function: 0 Alpha: HbS150230221 ANIMAL INCIDENT ROBBIE HEEMAN 0401865331 / LINCOLN CSWY WODONGA /H
UME OUT-HIGH RAMP OF //WRIGHT RD SVVB NE 8308 G2 COW STUCK IN WATER - CREW REQUIRED PLEASE ÄWDGAÜ<NUL>

4. Pagers (zoom-in)

```
     2  Function: 0
216588  Function: 0  Alpha:   (&
086677  Function: 1
2007579  Function: 0
526628  Function: 0
14208  Function: 1
     0  Function: 0
     1  Function: 0
     1  Function: 0
     2  Function: 0
241865  Function: 0  Alpha:   HbS150230221 ANIMAL INCIDENT                    5331 / LI
/WRIGHT RD SVVB NE 8308 G2 COW STUCK IN WATER - CREW REQUIRED PLEASE ÄWDGAÜ<NUL>
```

4. Pagers – Doors

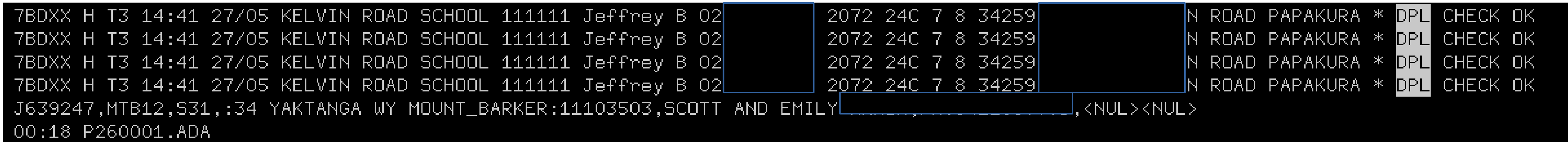


4. Pagers – Doors (zoom-in)

```
unction: 1
unction: 2  Alpha:   MLK P1-61 East Foyer Auto Door Push Button has changed state to: Open-Circuit Ta<NUL>
unction: 0
unction: 0
unction: 0
unction: 0
unction: 0
unction: 0
unction: 2  Alpha:   MLK P1-61 East Foyer Auto Door Push Button has changed state to: Open-Circuit Ta<NUL>
unction: 0
unction: 0
unction: 0
unction: 0
unction: 0
unction: 2  Alpha:   MLK P1-61 East Foyer Auto Door Push Button has changed state to: Open-Circuit Ta<NUL>
unction: 0
```

4. Pagers – Licence Plate Checks

```
7BDGS H T3 14:48 27/05 SAINT KENTIGERN TRUST 111111 Matthew [redacted] [redacted] 207 2 24C 78 07545 [redacted] AKURANGA ROAD AUCKLAND * DPL CHECK OK
7BDGS H T3 14:48 27/05 SAINT KENTIGERN TRUST 111111 Matthew 207 2 24C 78 07545 AKURANGA ROAD AUCKLAND * DPL CHECK OK
7BDGS H T3 14:48 27/05 SAINT KENTIGERN TRUST 111111 Matthew 207 2 24C 78 07545 AKURANGA ROAD AUCKLAND * DPL CHECK OK
20:21 P260001.ADA
20:22 P260001.ADA
20:23 P260001.ADA
20:24 P260001.ADA
```



```
7BDXX H T3 14:41 27/05 KELVIN ROAD SCHOOL 111111 Jeffrey B 02[redacted] 2072 24C 7 8 34259[redacted]N ROAD PAPAKURA * DPL CHECK OK
7BDXX H T3 14:41 27/05 KELVIN ROAD SCHOOL 111111 Jeffrey B 02 2072 24C 7 8 34259 N ROAD PAPAKURA * DPL CHECK OK
7BDXX H T3 14:41 27/05 KELVIN ROAD SCHOOL 111111 Jeffrey B 02 2072 24C 7 8 34259 N ROAD PAPAKURA * DPL CHECK OK
7BDXX H T3 14:41 27/05 KELVIN ROAD SCHOOL 111111 Jeffrey B 02 2072 24C 7 8 34259 N ROAD PAPAKURA * DPL CHECK OK
J639247,MTB12,S31,:34 YAKTANGA WY MOUNT_BARKER:11103503,SCOTT AND EMILY[redacted],<NUL><NUL>
00:18 P260001.ADA
```

4. Pagers – Licence Plate Checks (zoom in)

```
111111 Matthew Way 006                2 24C 78 075                PAK
111111 Matthew Way 006                2 24C 78 075                PAK
111111 Matthew Way 006                2 24C 78 075                PAK
```

```
1 Jeffrey B 02          2072 24C 7 8 34259          KELVIN ROAD PAPAKUR
1 Jeffrey B 02          2072 24C 7 8 34259          KELVIN ROAD PAPAKUR
1 Jeffrey B 02          2072 24C 7 8 34259          KELVIN ROAD PAPAKUR
1 Jeffrey B 02          2072 24C 7 8 34259          KELVIN ROAD PAPAKUR
11103503,SCOTT AND EMILY                    <NUL><NUL>
```

4. Pagers – Passcodes

```
500498  Function: 2  Alpha:   key safe located on the Right hand side of the front door - code is 1926<NUL
```

“key safe located on the Right hand side of the front door – code is 1926”

4. Pagers – Datacentre Servers

```
98 Saturday, 30 May 2015 4:39 PM GigabitEthernet1/0/1 WIRELESS AP on ADLSW01.win.i[redacted].com.au is Down<NUL>
96 Saturday, 30 May 2015 4:39 PM GigabitEthernet1/0/1 WIRELESS AP on ADLSW01.win.i[redacted].com.au is Down<NUL>
97 Saturday, 30 May 2015 4:39 PM GigabitEthernet1/0/1 WIRELESS AP on ADLSW01.win.i[redacted].com.au is Down<NUL>
Saturday, 30 May 2015 4:39 PM GigabitEthernet1/0/1 WIRELESS AP on ADLSW01.win.int.[redacted]m.au is Down<NUL>
Saturday, 30 May 2015 4:39 PM GigabitEthernet1/0/1 WIRELESS AP on ADLSW01.win.int.[redacted]m.au is Down<NUL>
```

```
Ä1/2Ü ÄRepeat #2Ü EM Event: Critical:NBMSP.arcbs[redacted].org.au_NBMSP-cluster_NBMSP_3 - Out of memory detected in /apps/oracle/diag/rdbms/nbmsp/NBMSP<NUL>
17:59 X 18365 30/05/15 17:59:28
18:01 P260001.ADA
```

```
84 Saturday, 30 May 2015 5:02 PM<br/>REA-EQX-SQLN1 100 % CPU - Top 10<br/><br/>http:/[redacted]-ORION01:80/Orion/View.aspx?NetObject=N:301<NUL>
```

4. Pagers – Datacentre Servers (zoom in)

```
S AP on ADLSW01.win.i[redacted].com.au is Down
S AP on ADLSW01.win.i[redacted].com.au is Down
S AP on ADLSW01.win.i[redacted].com.au is Down
P on ADLSW01.win.int.[redacted].au is Down<NU
P on ADLSW01.win.int.[redacted].au is Down<NU
```

```
memory detected in /apps/oracle/diag/rdbms/nbmsp/NBMSP<
```

```
http://[redacted]ORION01:80/Orion/View.aspx?NetOb
```

4. Pagers – Emergency Services

```
POCSAG1200: Address:  452370  Function: 2  Alpha:                                  _GARDENS,MFS,shed fire, please isolate ,<NUL><NUL>
POCSAG1200: Address:  452368  Function: 2  Alpha:                                  _GARDENS,MFS,shed fire, please isolate ,<NUL><NUL>
POCSAG1200: Address:  452369  Function: 2  Alpha:                                  _GARDENS,MFS,shed fire, please isolate ,<NUL><NUL>
POCSAG1200: Address:  370377  Function: 2  Alpha:   21:29 X 18379 30/05/15 21:29:28
POCSAG1200: Address:  370377  Function: 2  Alpha:   21:29 P260001.ADA
POCSAG1200: Address:  370377  Function: 2  Alpha:   21:30 P260001.ADA
POCSAG1200: Address:  440500  Function: 2  Alpha:   7B51H H M3 : / AUSGRID DC NORTH RYDE 822000 LENIN +91                AAXRO 23 -25
 7.3.0.11 GIVING ERROR<NUL><NUL>
POCSAG1200: Address:  440501  Function: 2  Alpha:   7B51H H M3 : / AUSGRID DC NORTH RYDE 822000 LENIN +91                AAXRO 23 -25
 7.3.0.11 GIVING ERROR<NUL><NUL>
POCSAG1200: Address:  408384  Function: 2  Alpha:   96 Pole Rqd Lendlease Plse call NOC - re PAW chp job . Refer Ian - cheers.
POCSAG1200: Address:  405195  Function: 2  Alpha:   Pole Rqd Lendlease Plse call NOC - re PAW chp job . Refer Ian - cheers.
```

4. Pagers – Emergency Services (zoom in)

```
GARDENS,MFS,shed fire, please isolate
GARDENS,MFS,shed fire, please isolate
GARDENS,MFS,shed fire, please isolate
29 X 18379 30/05/15 21:29:28
29 P260001,ADA
30 P260001,ADA
51H H M3 : / AUSGRID DC NORTH RYDE 822000 LENIN +91

51H H M3 : / AUSGRID DC NORTH RYDE 822000 LENIN +91

Pole Rqd Lendlease Plse call NOC - re PAW chp job . Refer Ian - cheer
le Rqd Lendlease Plse call NOC - re PAW chp job . Refer Ian - cheers.
```

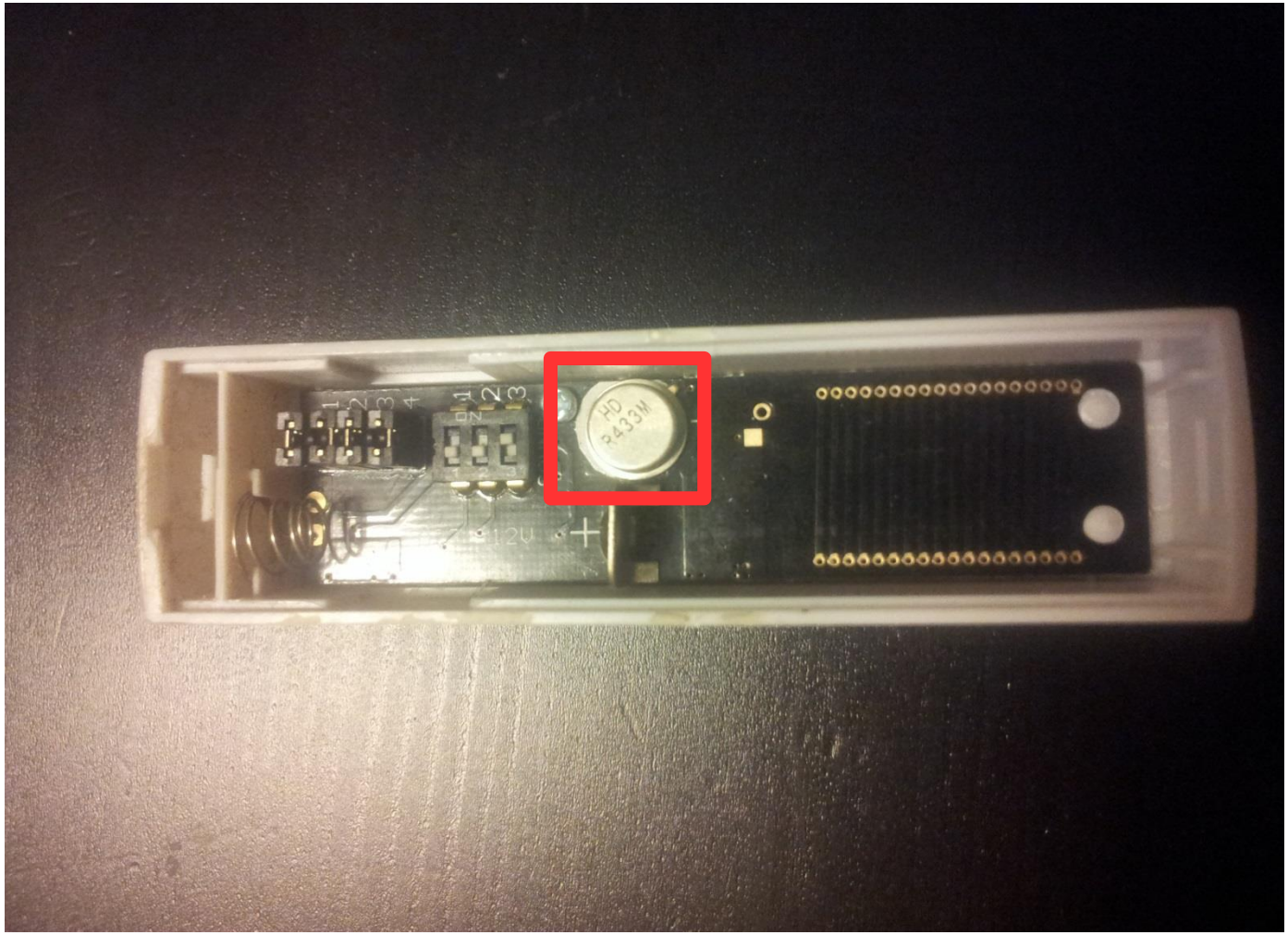
5. Home Devices

5. Home Devices

- **Doorbells**
- Garage doors
- Baby monitors
- Home automation
- Smart Meters

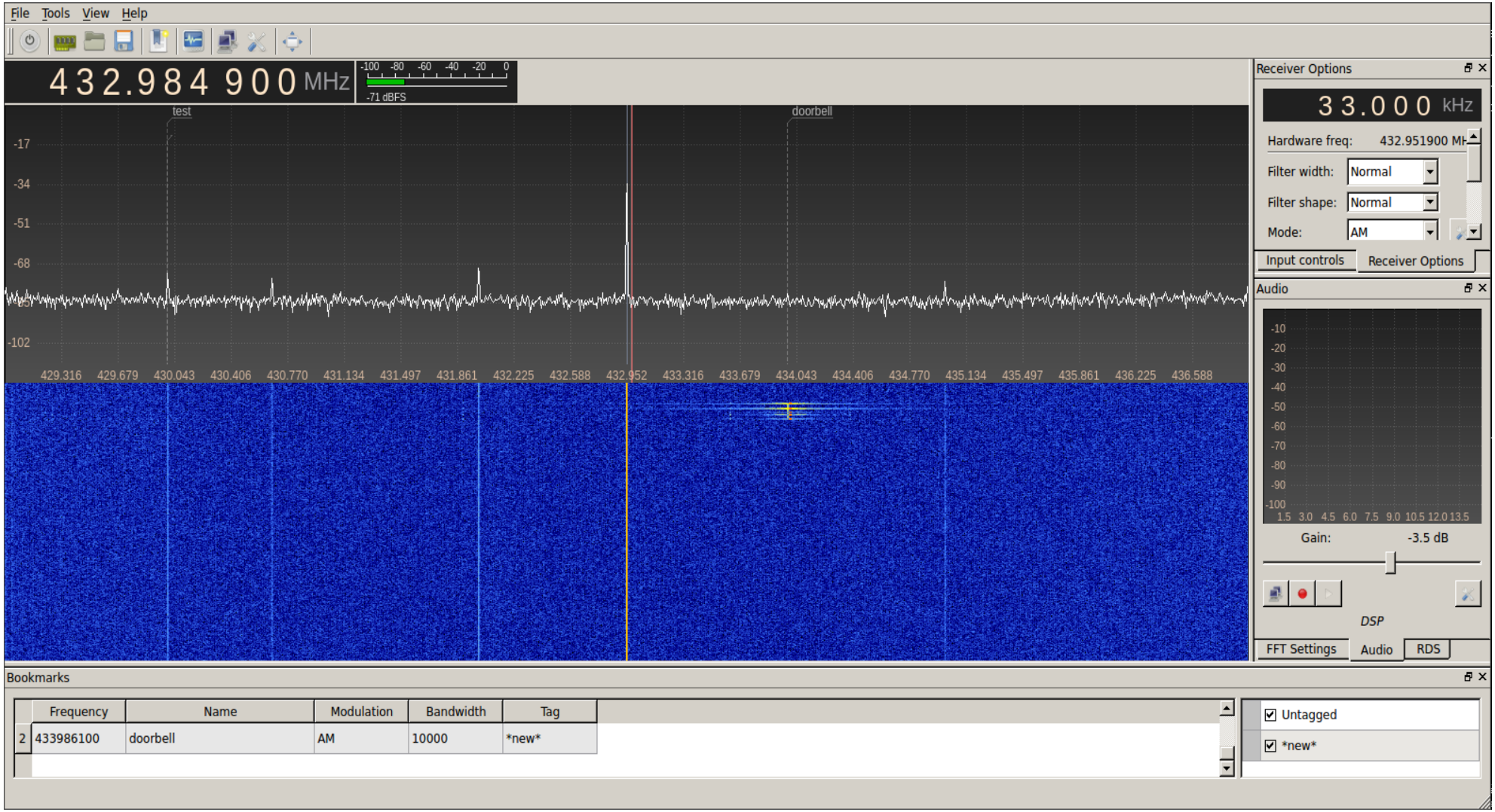
5. Home Devices - Doorbells

1) Identify Frequency: 433Mhz (approx)



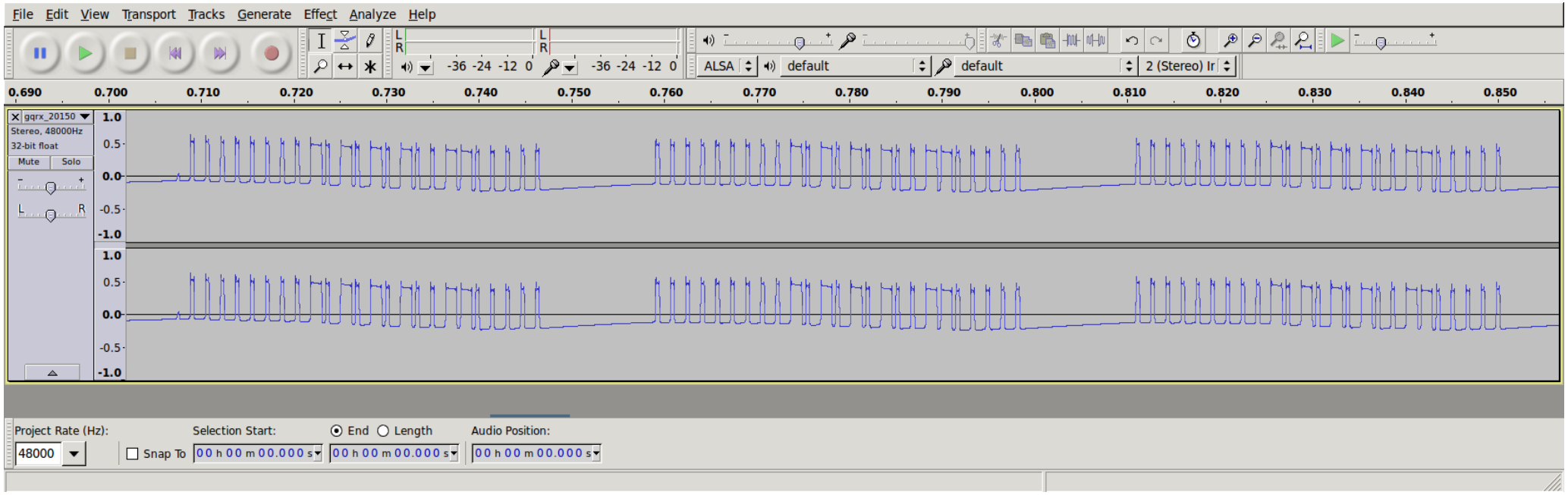
5. Home Devices - Doorbells

2A) Identify Modulation: listening in GQRX



5. Home Devices - Doorbells

2B) Open Recoding in Audacity



5. Home Devices - Doorbells

2B) Open Recoding in Audacity…

- We can clearly see ON/OFF (0 = OFF, 1 = ON): **Amplitude Modulation**
- Shorter pulses are 1, Longer pulses are consecutive ones
- OOK – On Off Shifting Keying

5. Home Devices - Doorbells

3) Capture Raw Data

Check frequency in gqrx and record with a hackrf:

$ hackrf_transfer -r 433995700.raw -f 433995700

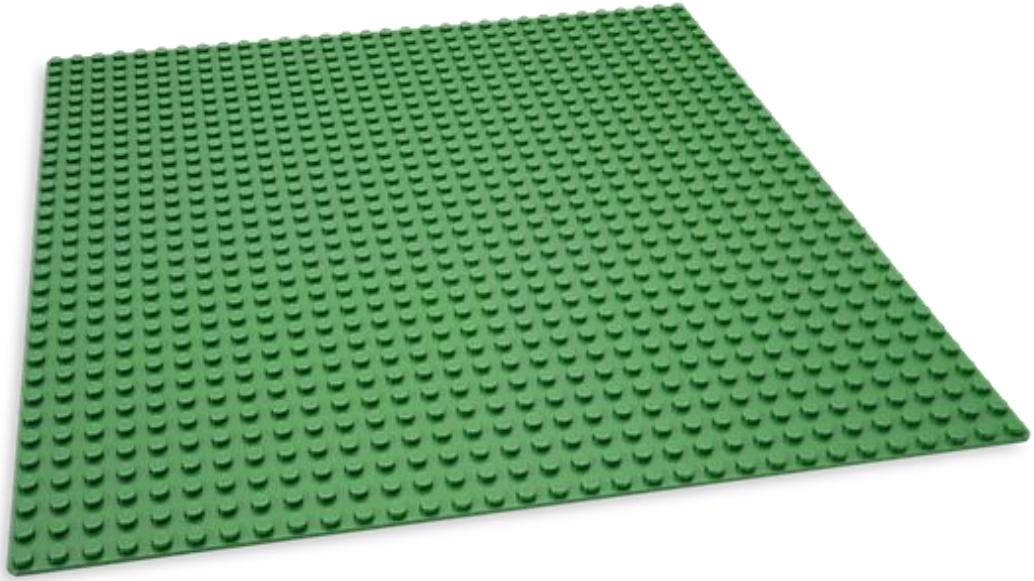
5. Home Devices - Doorbells

4) Replay without remote

Shift the frequency for transmission down 100Khz to avoid the carrier spike in middle of our signal

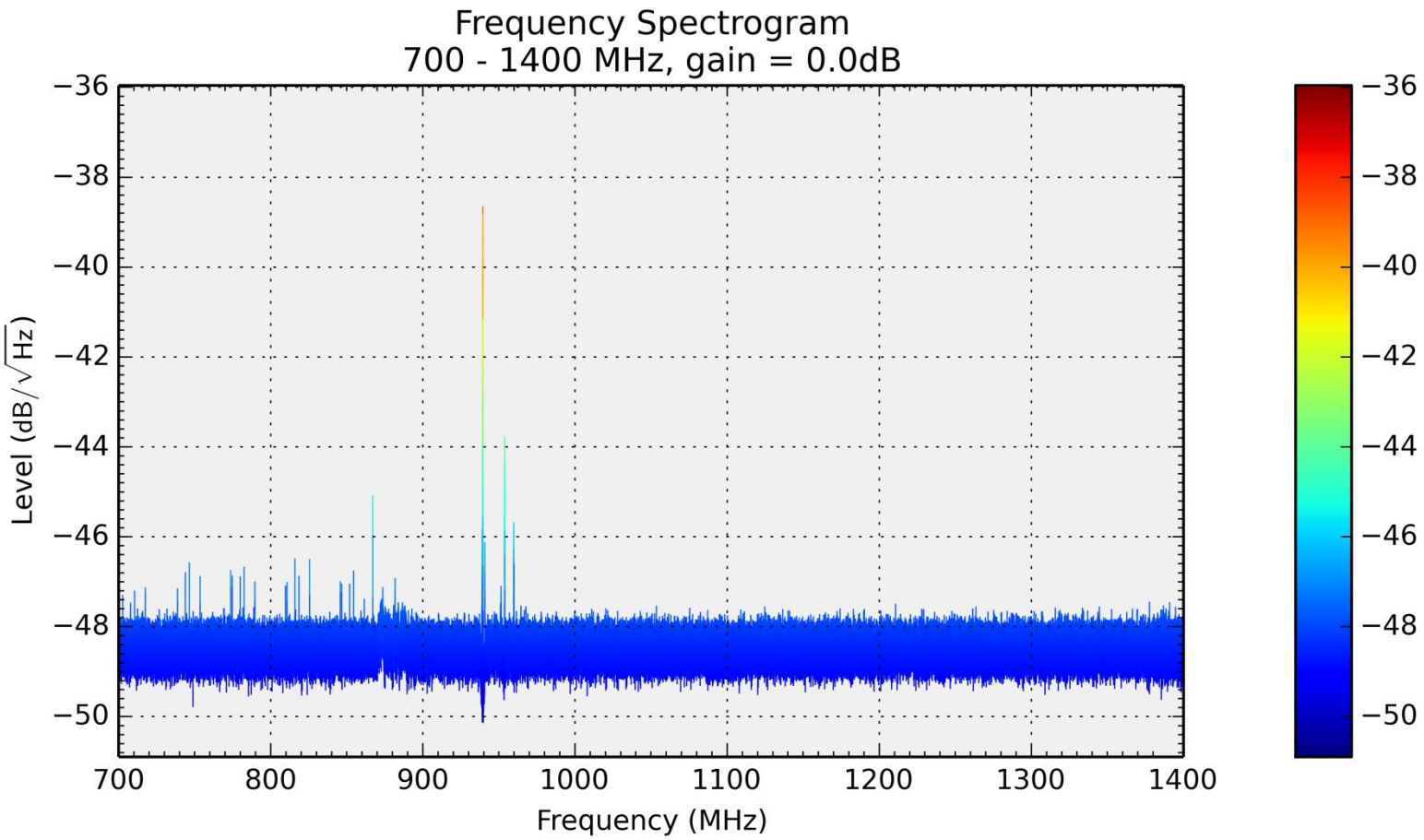
$ hackrf_transfer -t 433985700.raw -f 433985700 -x 20

6. Scanning the ground



6. Scanning the ground

- Tool: **rtlsdr-scanner**



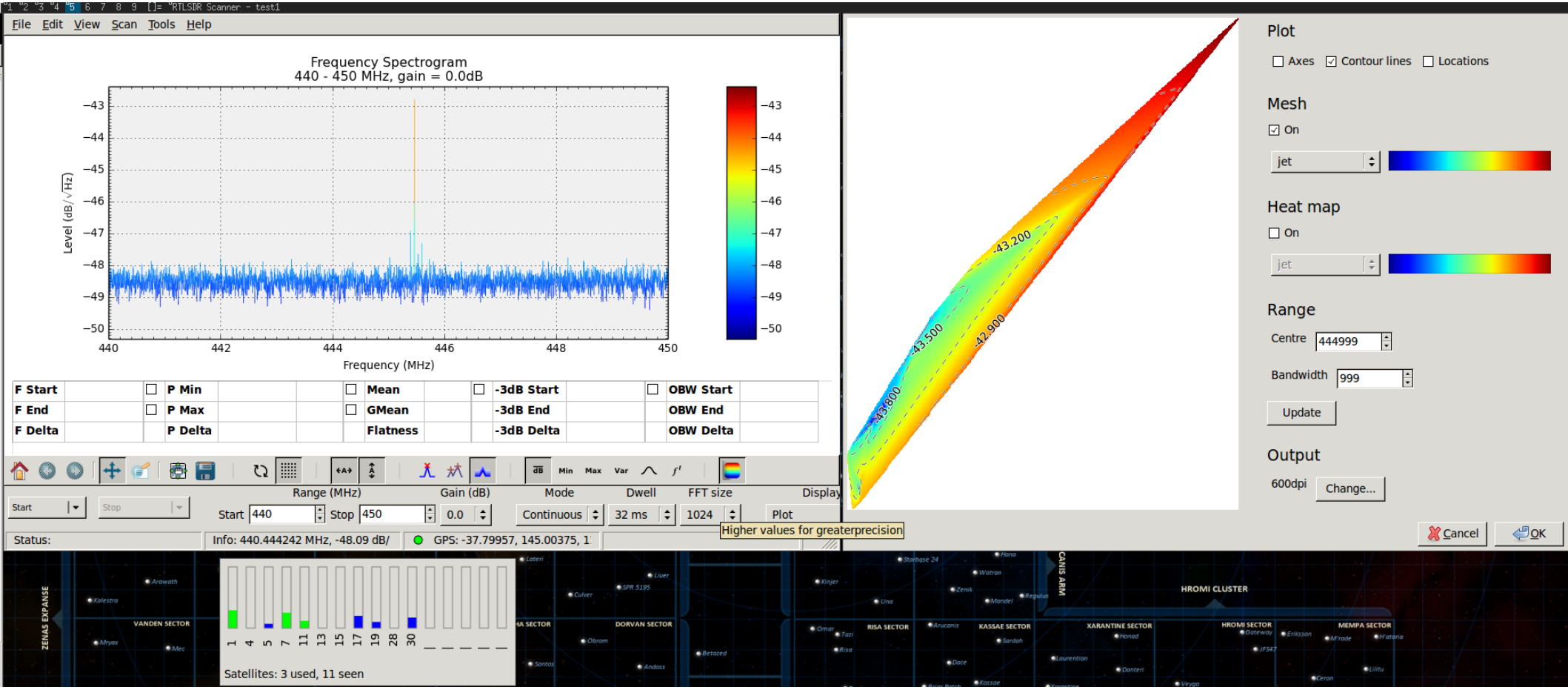
7. Scanning on the move

7. Scanning on the Move

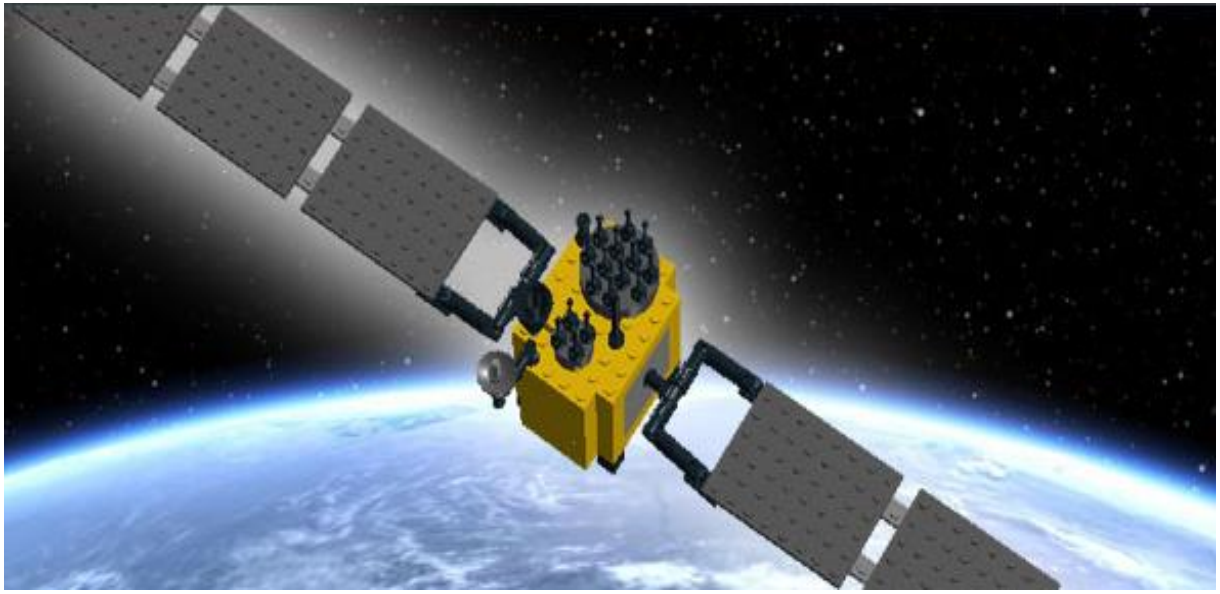
- rtlsdr-scanner
- Adding GPS
- Raspberry pi(es)
- Some antennae

7. Scanning on the Move

- Add GPS

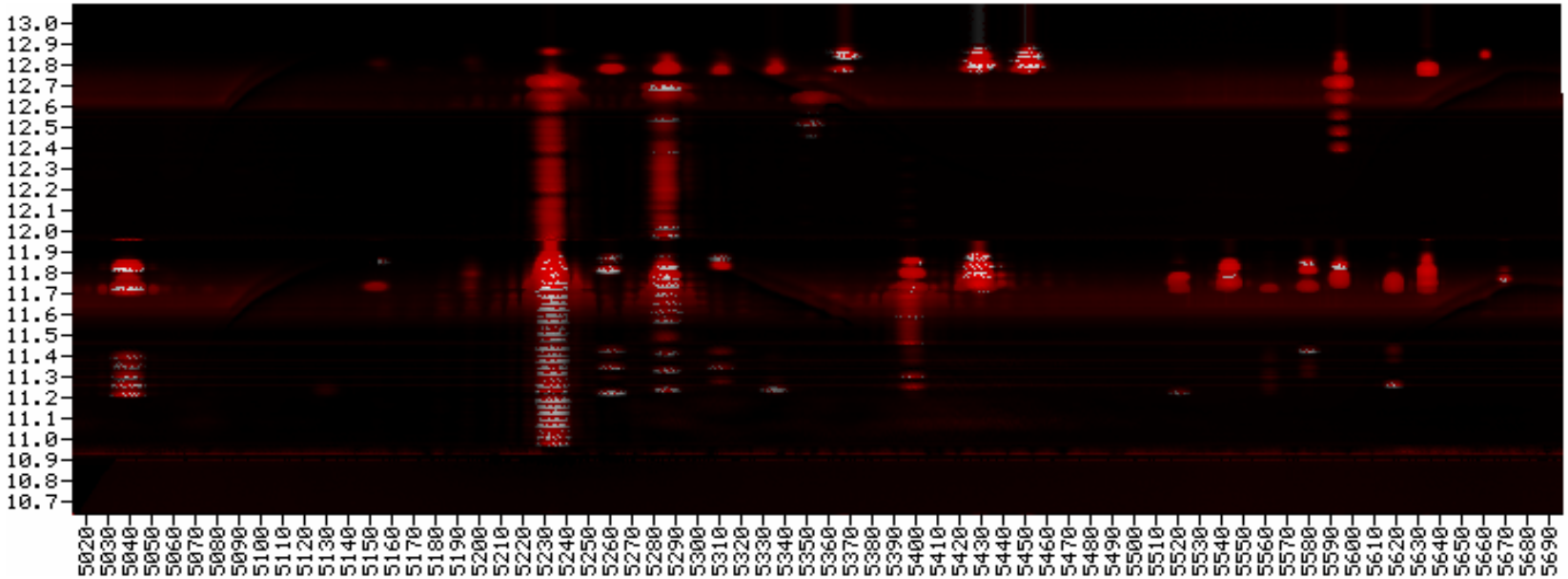


8. Scanning the sky



8. Scanning the sky

1.2m dish, motor, satmap



9. GSM

9a. GSM: Looking at control channels on downlink only

- Requirements:
  - hackrf
  - hackrf kalibrate
  - gnuradio-companion
  - gr-gsm
  - gqrx
  - wireshark

9a. GSM: Looking at control channels on downlink only

- Links:
  - hackrf kalibrate: https://github.com/scateu/kalibrate-hackrf.git
  - gr-gsm: https://github.com/ptrkrysik/gr-gsm.git
  - guide: https://z4ziggy.wordpress.com/2015/05/17/sniffing-gsm-traffic-with-hackrf/

9a. GSM: Looking at control channels on downlink only

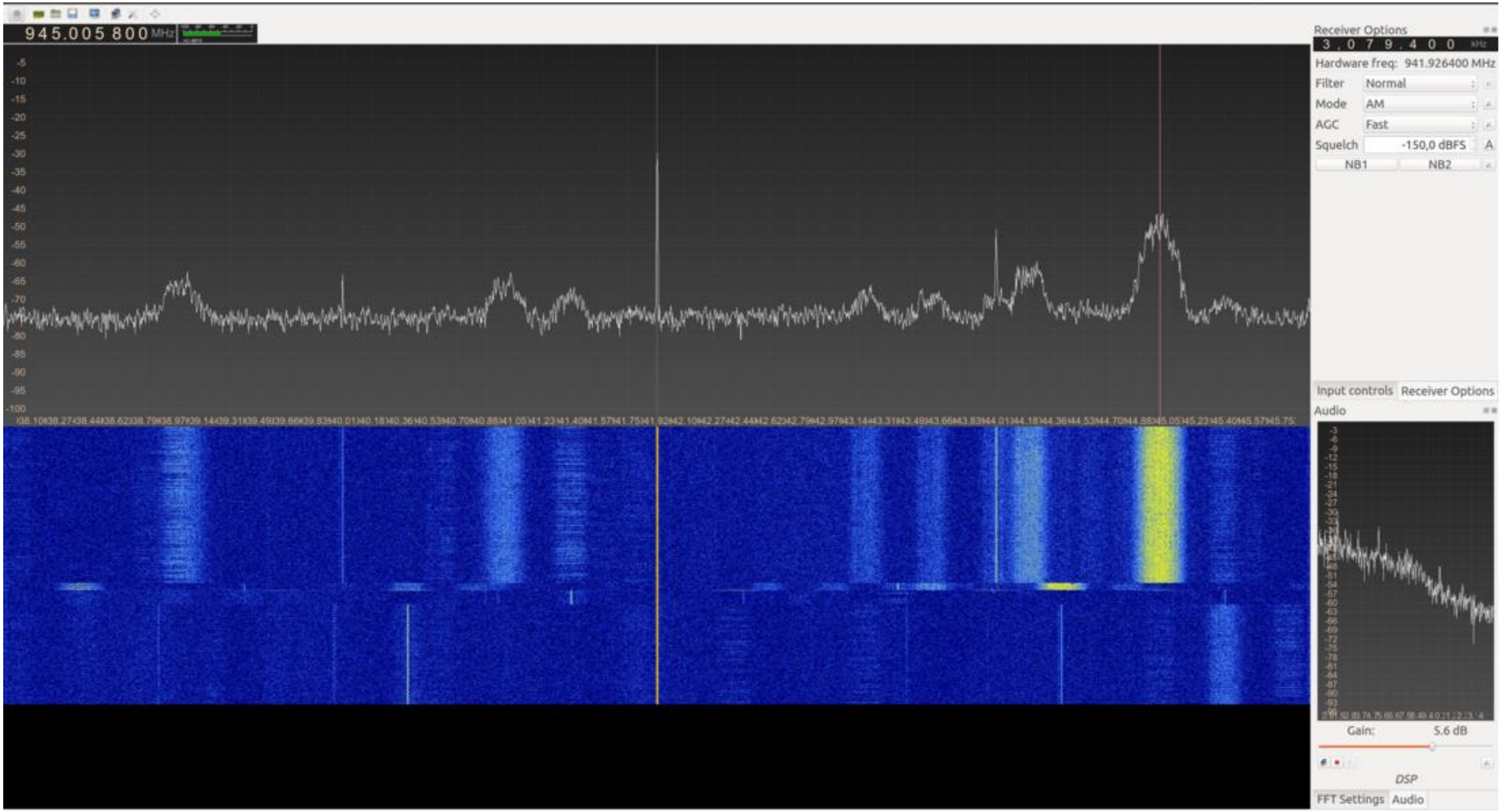
- 1. Finding GSM frequencies with kalibrate tool:

$ ./kal -s GSM900 -g 40 -l 40

```
kal: Scanning for GSM-900 base stations.
GSM-900:
        chan: 71 (949.2MHz + 32.326kHz) power: 2565731.98
        chan: 72 (949.4MHz + 7.165kHz)  power: 2644332.31
        chan: 104 (955.8MHz + 32.334kHz)        power: 2097247.66
        chan: 105 (956.0MHz + 7.332kHz) power: 2184371.47
        chan: 106 (956.2MHz - 17.806kHz)        power: 2219039.12
        chan: 107 (956.4MHz - 39.680kHz)        power: 2325130.00
        chan: 119 (958.8MHz + 22.870kHz)        power: 1615921.07
        chan: 120 (959.0MHz - 1.880kHz) power: 1693397.83
        chan: 121 (959.2MHz + 2.137kHz) power: 1681418.44
        chan: 122 (959.4MHz + 32.330kHz)        power: 1672177.79
        chan: 123 (959.6MHz - 17.795kHz)        power: 1738497.54
        chan: 124 (959.8MHz - 17.745kHz)        power: 1725323.52
```

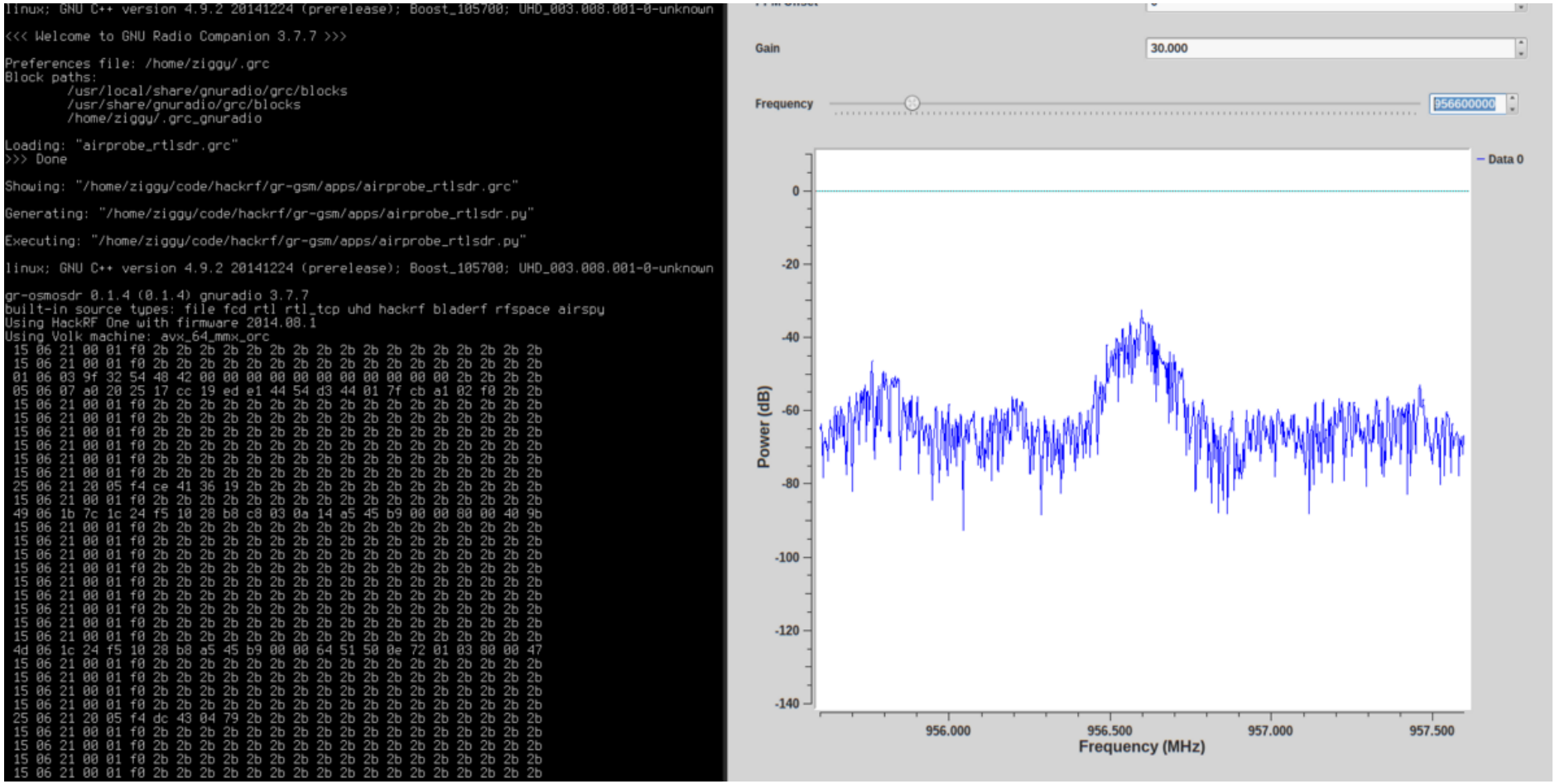
9a. GSM: Looking at control channels on downlink only

- 2. Check frequency is active in GQRX



9a. GSM: Looking at control channels on downlink only

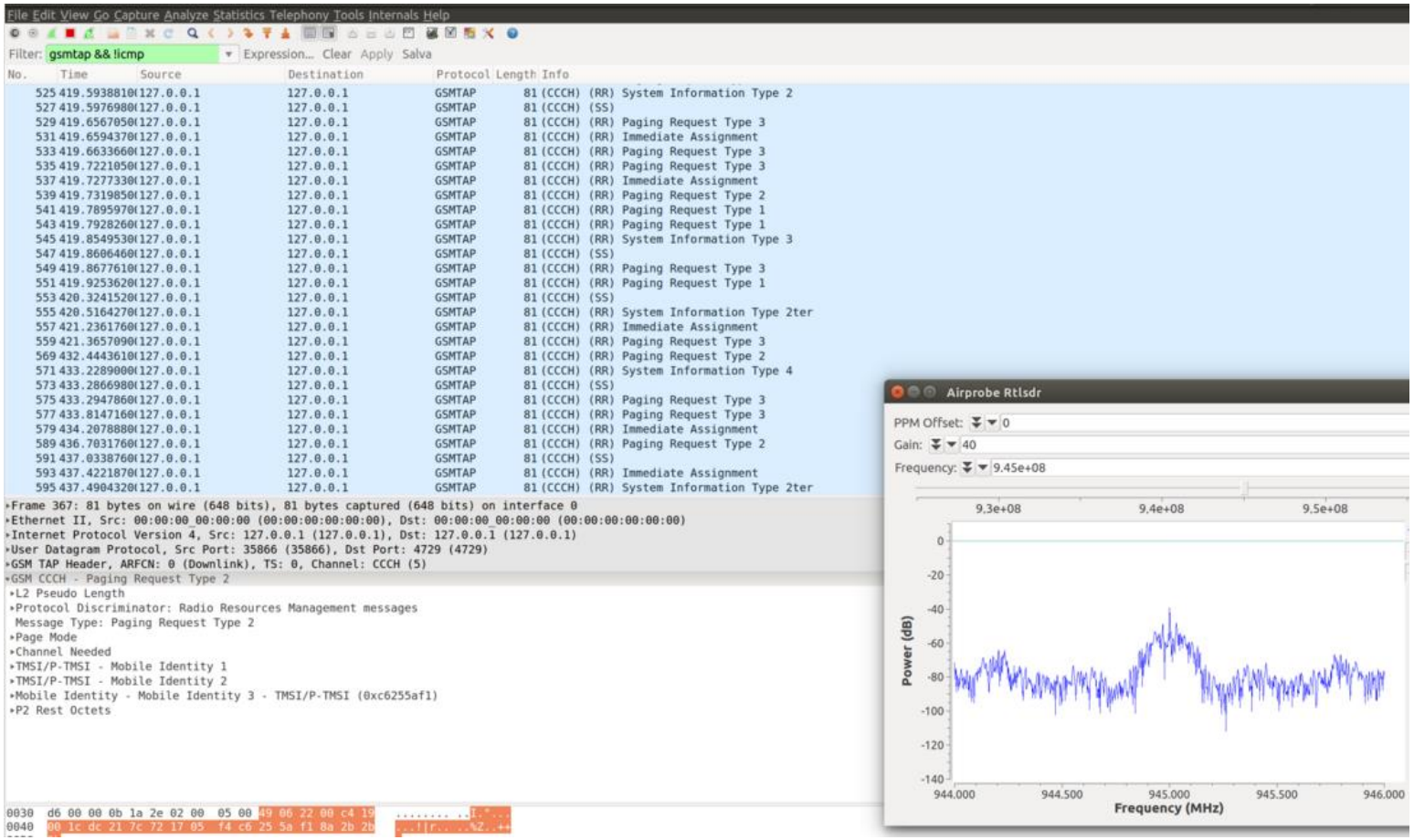
- 3. Use gr-gsm (airprobe_rtlsdr.grc) against our discovered freq



9a. GSM: Looking at control channels on downlink only

- 4. View the local interface in Wireshark

$ sudo wireshark -k -Y 'gsmtap && !icmp' -i lo



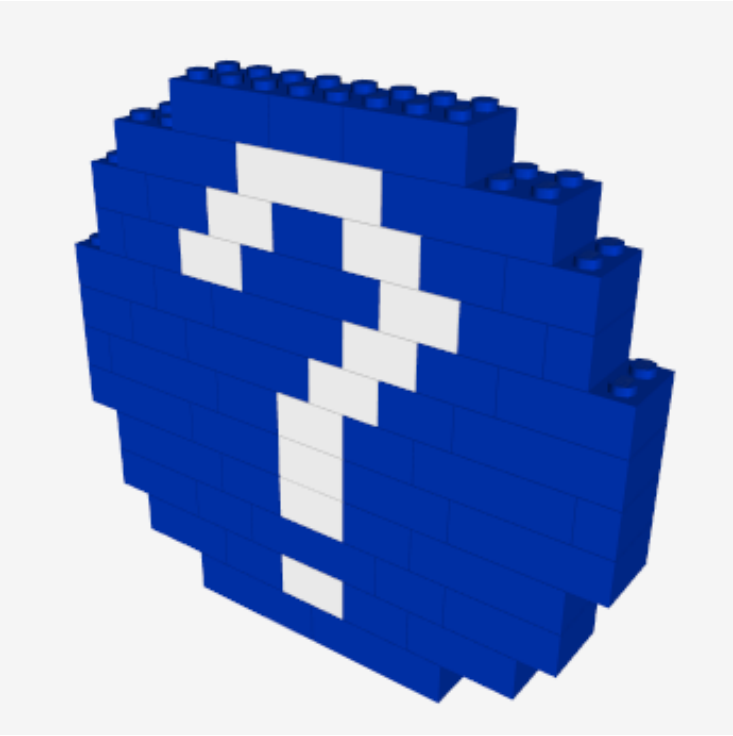
9b. GSM: Decrypting Your Calls & SMS

- Requirements:
  - Osmocom BB firmware on compatible phones x 4 (2 uplinks, 2 downlinks)
  - HLR lookup
  - Sending a Silent SMS
  - Airprobe
  - Kraken + A5/1 rainbow tables

9b. GSM: Decrypting Your Calls & SMS

- Links:
  - http://osmocom.org/
  - CCC Talk: https://www.youtube.com/watch?v=ZrbatnnRxFc
  - Slides: https://events.ccc.de/congress/2010/Fahrplan/attachments/1783_101228.27C3.GSM-Sniffing.Nohl_Munaut.pdf

Questions



Melbourne Meetup Group

- Join our Melbourne SDR meetup group (Cyberspectrum Melbourne)
- We have a slack channel – ask us any questions you may have or trouble with installing/getting tools going
- See you at the next meetup!
- @sdr_melbourne, @0xsh_

Cyberspectrum Melbourne

Twitter	**@sdr_melbourne**
Email	**sdr.melbourne@gmail.com**
Slack	**sdr-melbourne.slack.com (email for an invite)**
Meetup	**https://www.meetup.com/Cyberspectrum-Melbourne**
Blog	**http://randomkeystrokes.com/category/sdr/**
Github	**https://github.com/sdr-melbourne**
YouTube	**https://www.youtube.com/channel/UCLBloqxOXEj4fH7s ULA (SDR Melbourne Channel)**