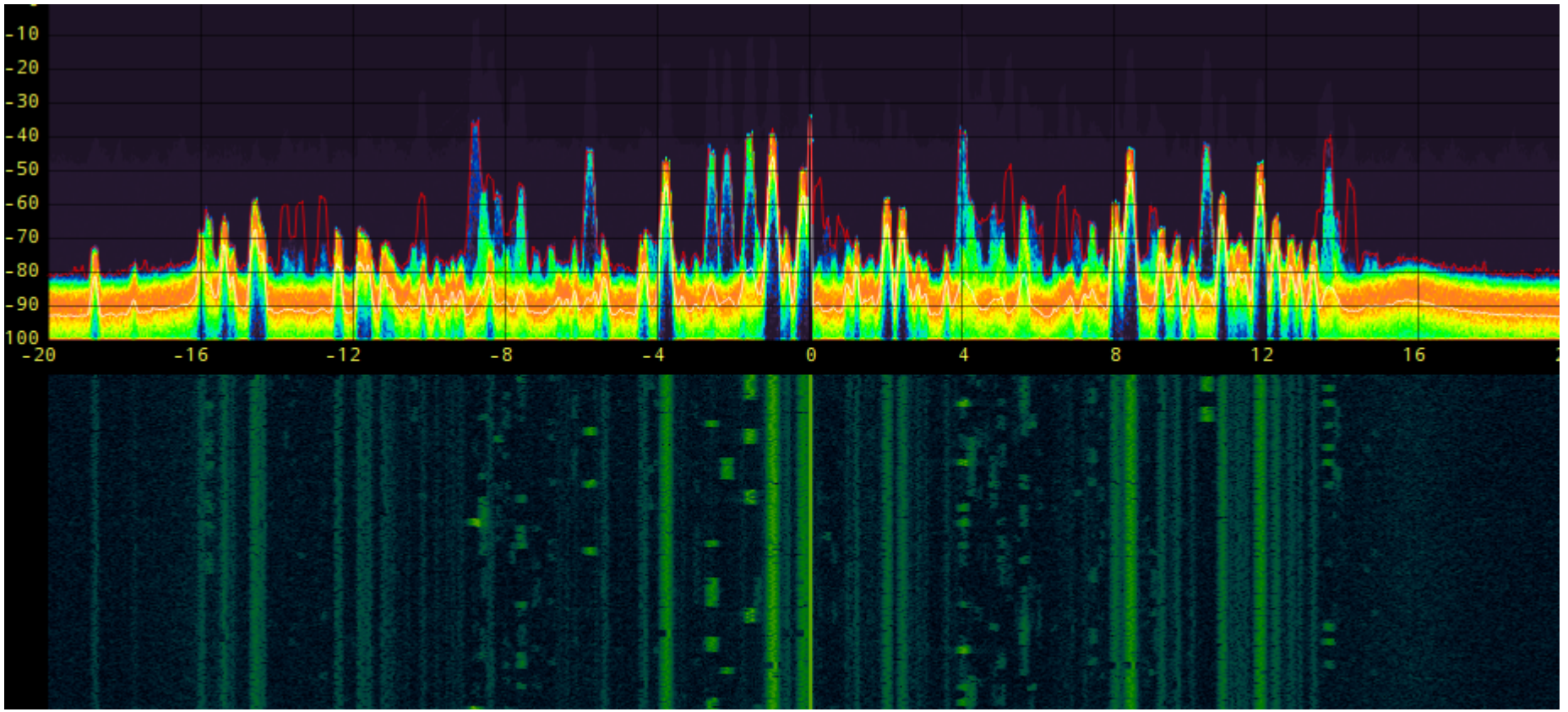
Introduction to Software Defined Radio



Pamela O'Shea, OWASP Melbourne App Sec Day 2017
@pamoshea @sdr_melbourne

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/UCLBloqxOXEj4fH7sTT5YULA (SDR Melbourne Channel)**

Contents

Hardware

- RTLSDR Dongle: start with one like this from eBay e.g. Realtek chip.
- Receive only
- Range: 64 - 1700 MHz approx
- Cost: $10 approx

Hardware

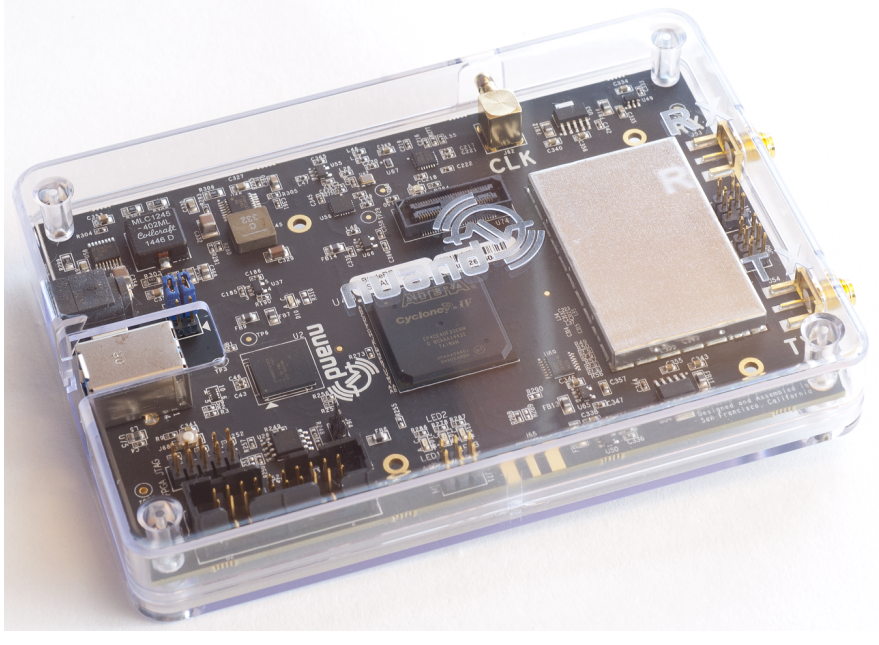
- RTLSDR Dongle: from rtlsdr.com
- Better components & cooling & bias tee
- Cost: $25 approx
- Worth the extra cost!!!

Hardware

- HackRF One
- Recieve and transmit
- Half duplex
- Range: 1 MHz - 6 GHz
- Cost: $400 approx

Hardware

- BladeRF
- Recieve and transmit
- Full duplex
- Range: 300MHz - 3.8GHz
- Cost: $500 approx



Hardware

- USRP e.g. USRP E310
- Recieve and transmit
- Full duplex
- Range: 70 MHz - 6 GHz
- FPGA
- Cost: $5000 approx

Common SDR Antennas

- Omnidirectional
- Directional (high gain)
- Passive
- Active (need power)

Whip Antenna

- General purpose
- Portable
- Not directional

Telescopic Antenna

- General purpose
- Portable
- Not directional

Discone Antenna

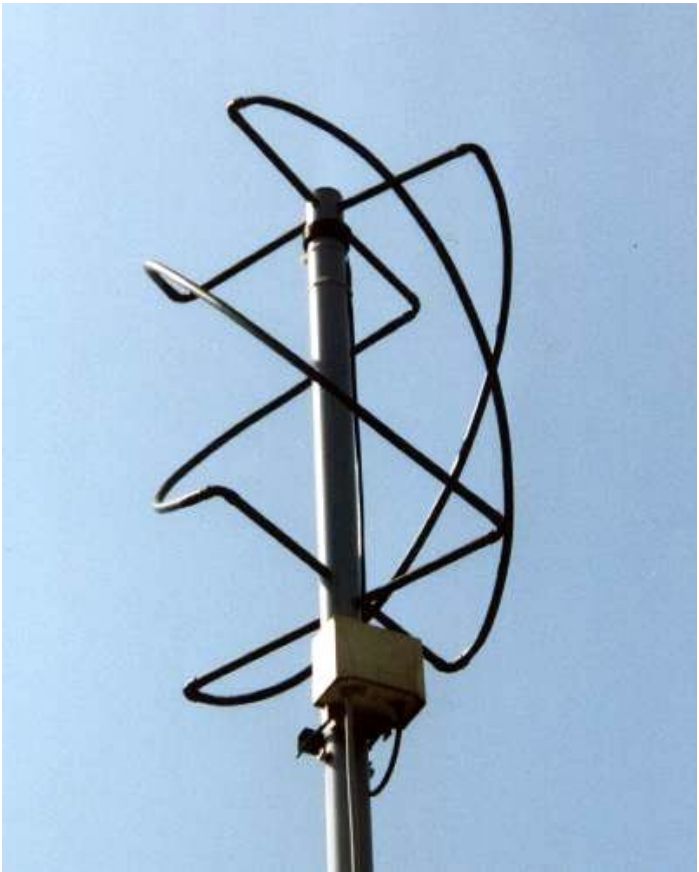
- General purpose
- Wideband
- Not directional

Turnstile Antenna

- Satelitte reception e.g. weather/NOAA

QFH Antenna

- QuadriFilar Helix
- Satelitte reception e.g. weather/NOAA



DIY Directional Antennas

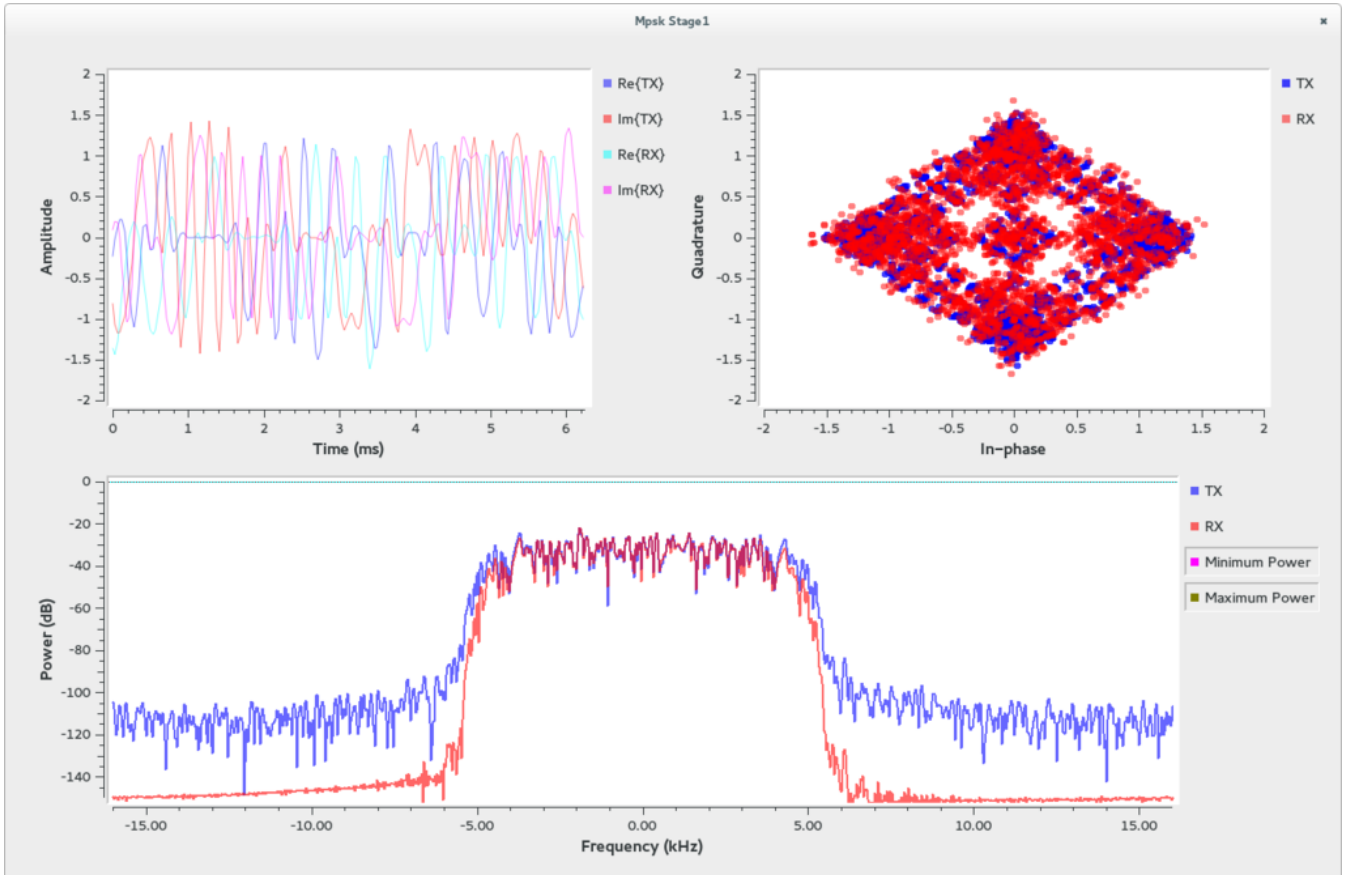
- Tape Measure

Satelitte DVB-S Antenna

- DVB-S digital video transmissions from International Space Station

Software

- GNU Radio: provides signal processing blocks to implement software-defined radios and signal-processing systems



Software

Linux

- GNU Radio Live Image
- Pentoo
- Ubuntu is highly recommended
- Install with aptitude for older stable version of gnu-radio
- Install with pybombs for latest versions
- Works on Raspberry Pi too!

Windows

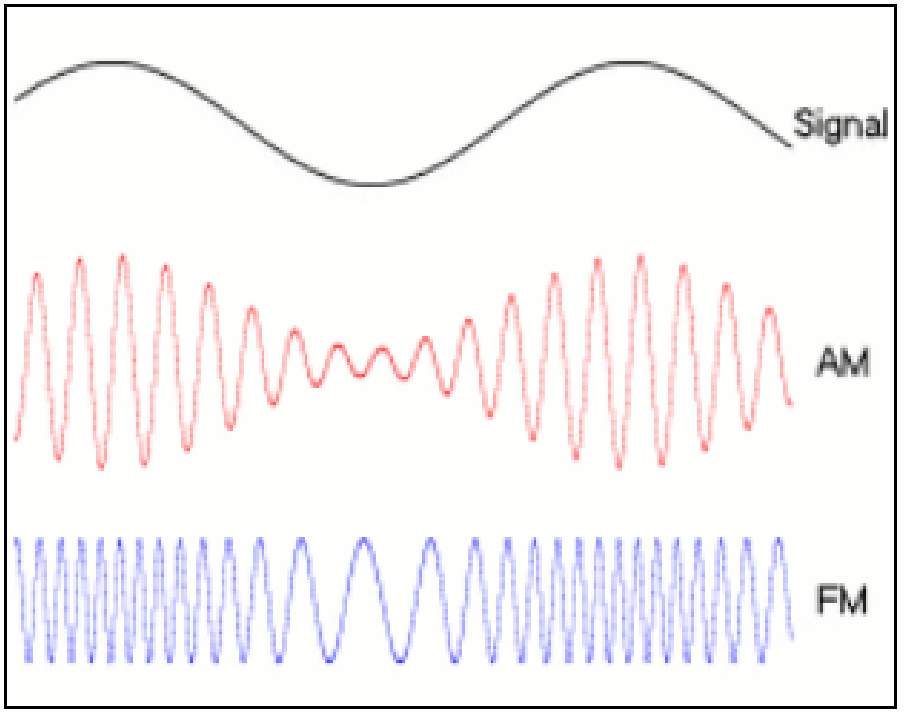
- SDR# is a good free tool of choice for Windows (same as gqrx on Linux)
- Check out Hak5 for tools on Windows

DSP intro

- Modulations
  - Amplitdue modulation
  - Frequency modulation
  - Phase modulation
- Sampling & Nyquist
- Filtering
  - Low Pass
  - High Pass
  - Finite Impulse Response (FIR)
  - Infinite Impulse Response (IIR)

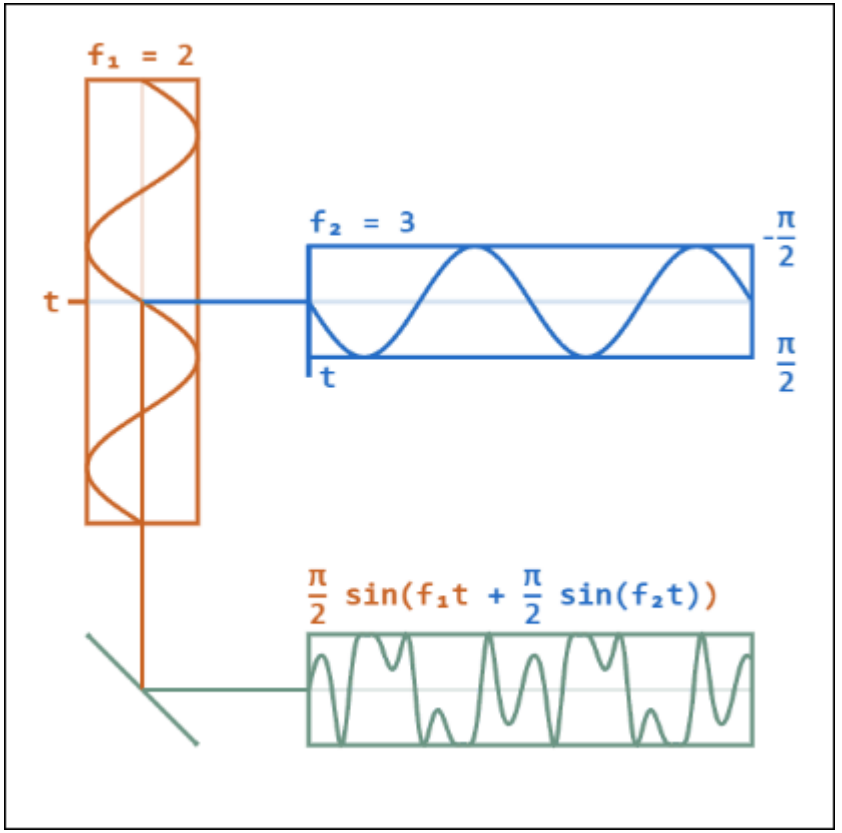
AM / FM Modulations

- An audio signal (top) may be carried by a carrier signal using AM or FM methods



Phase Modulation

- The modulating wave (blue) is modulating the carrier wave (red), resulting in the PM signal (green)

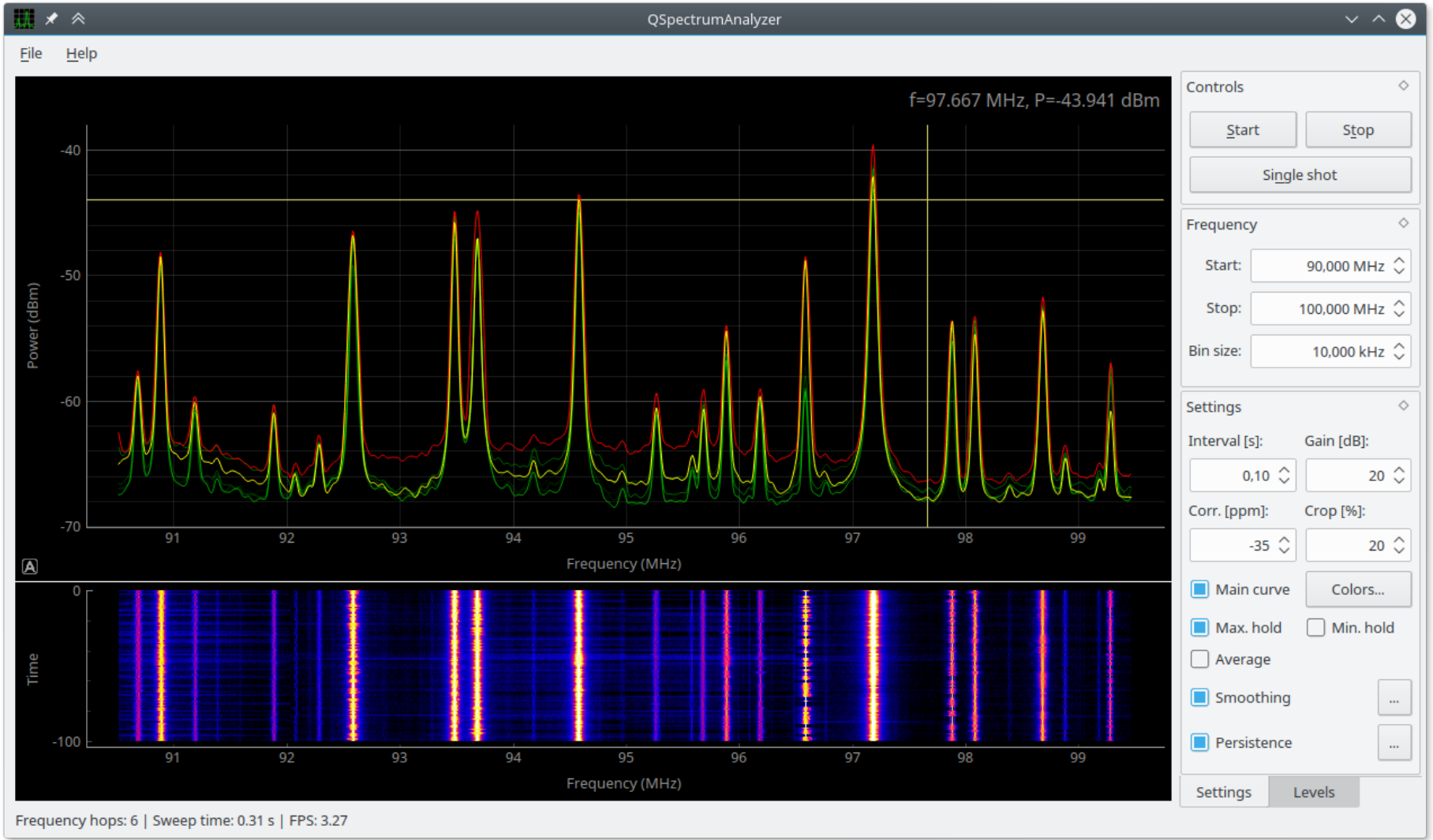


DSP intro

- Demos

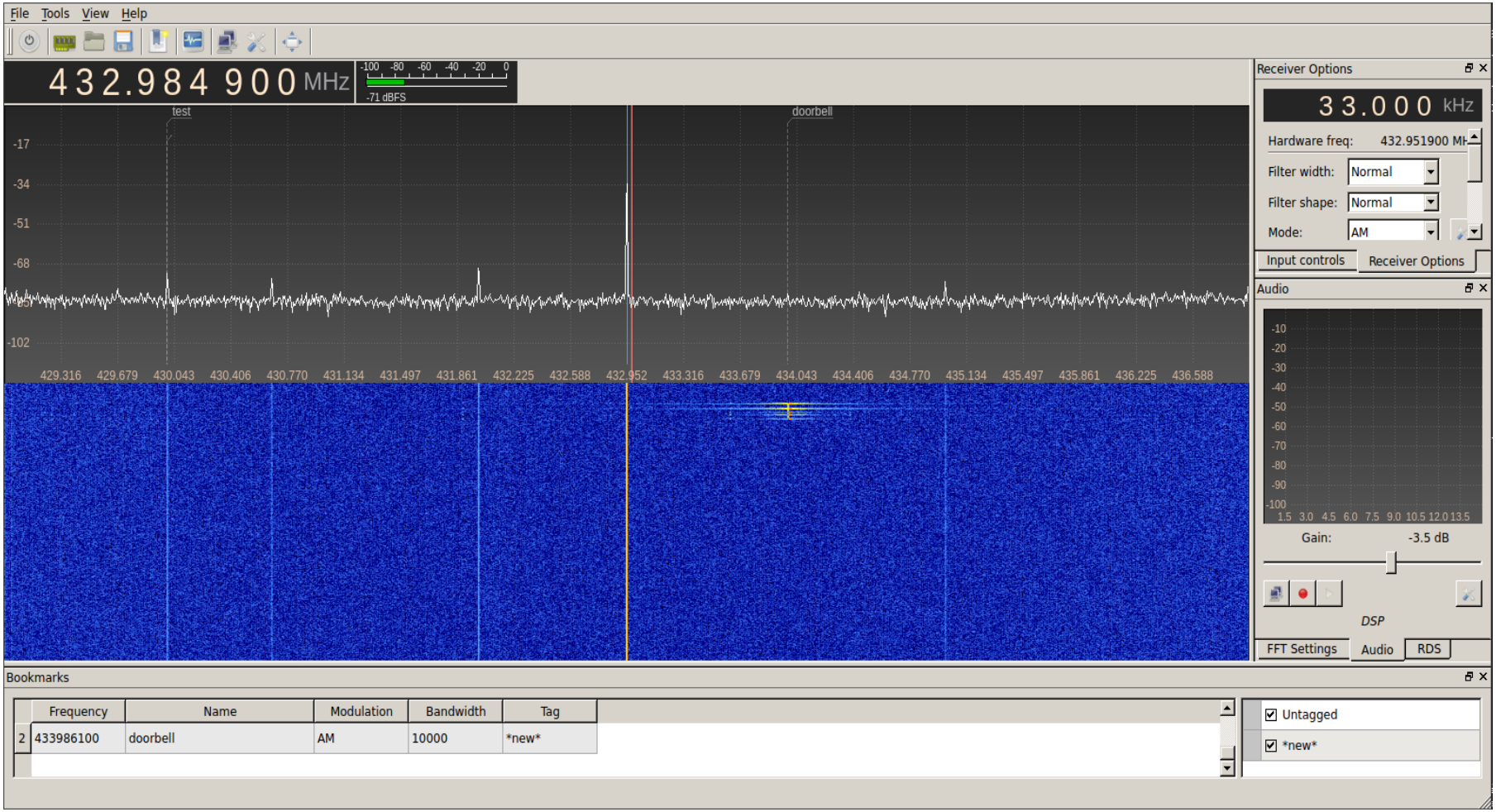
Frequency Scanning

- Demo



Remote Control Intro

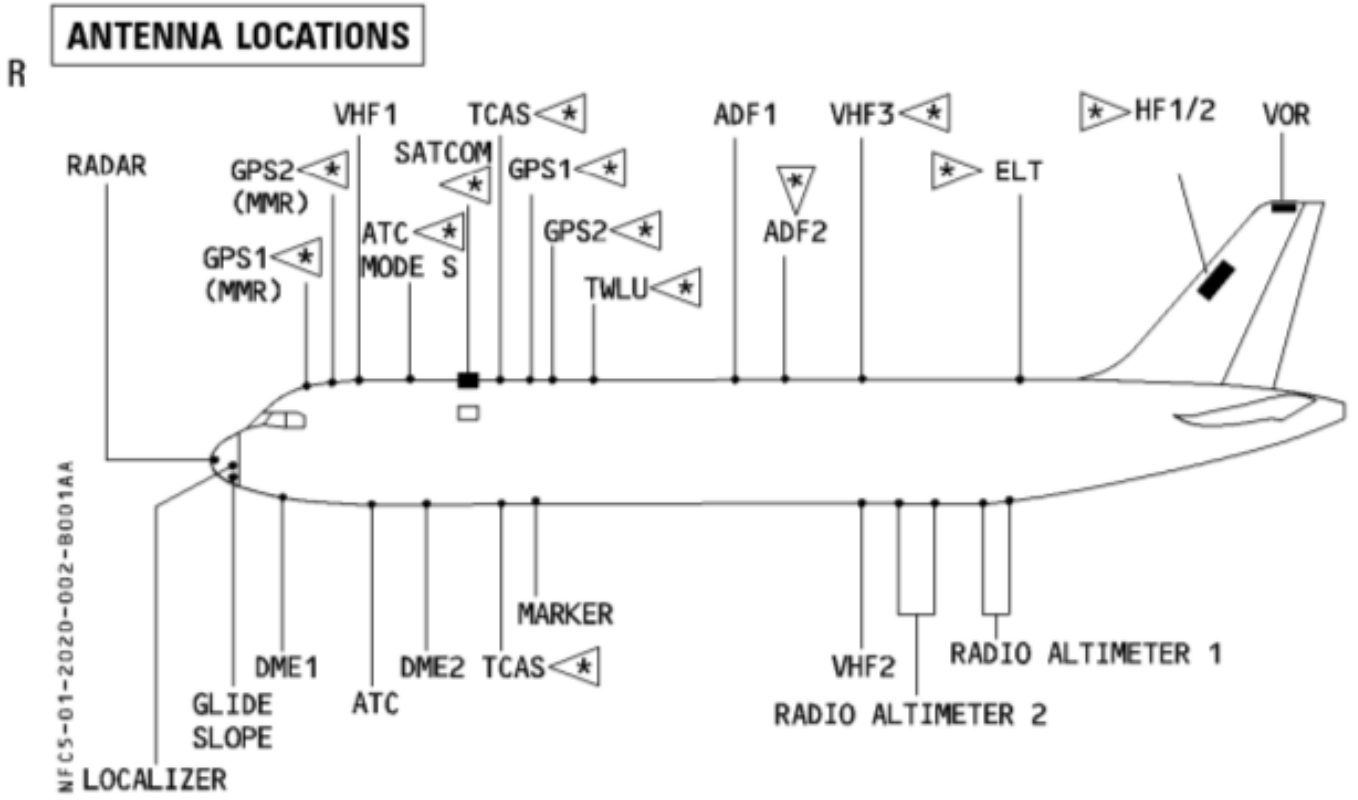
- Demo



Some Local Frequencies

- Demo

Airplanes

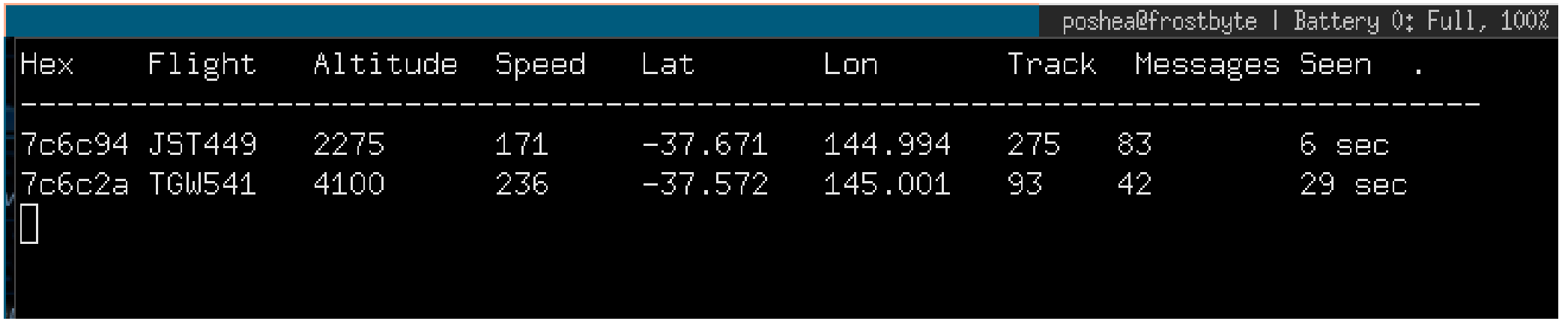

ANTENNA LOCATIONS
R
VHF1
TCAS
ADF1
VHF3
HF1/2
VOR
RADAR
GPS2
(MMR)
SATCOM
GPS1
ELT
ATC
MODE S
GPS2
ADF2
GPS1
(MMR)
TWLU
MARKER
DME1
DME2
TCAS
VHF2
RADIO ALTIMETER 1
GLIDE
SLOPE
ATC
RADIO ALTIMETER 2
LOCALIZER
NFC5-01-2020-002-B001AA

ADS-B

- **ADS-B:** 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)

dump1090

$ dump1090 --interactive --aggressive



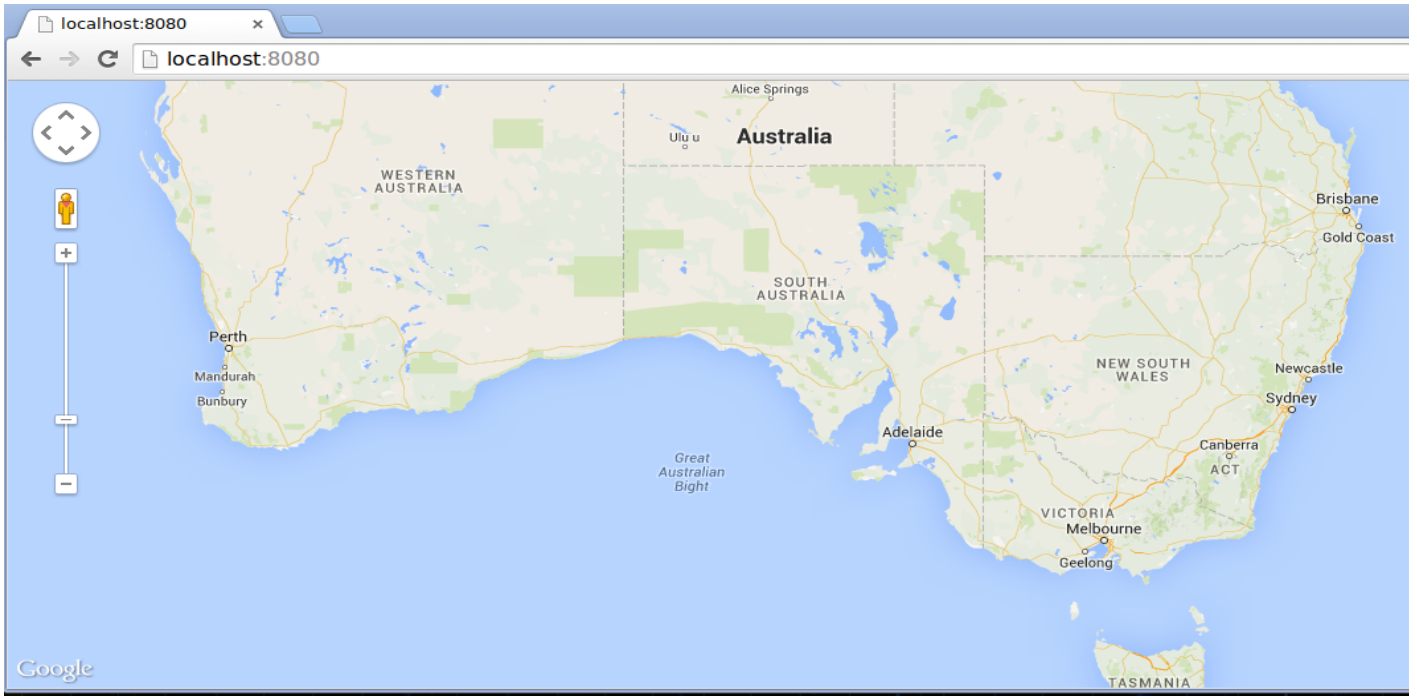
dump1090

```
$ dump1090 --interactive --aggressive --net
```

```
http://localhost:8080
```

dump1090

```
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
```



dump1090

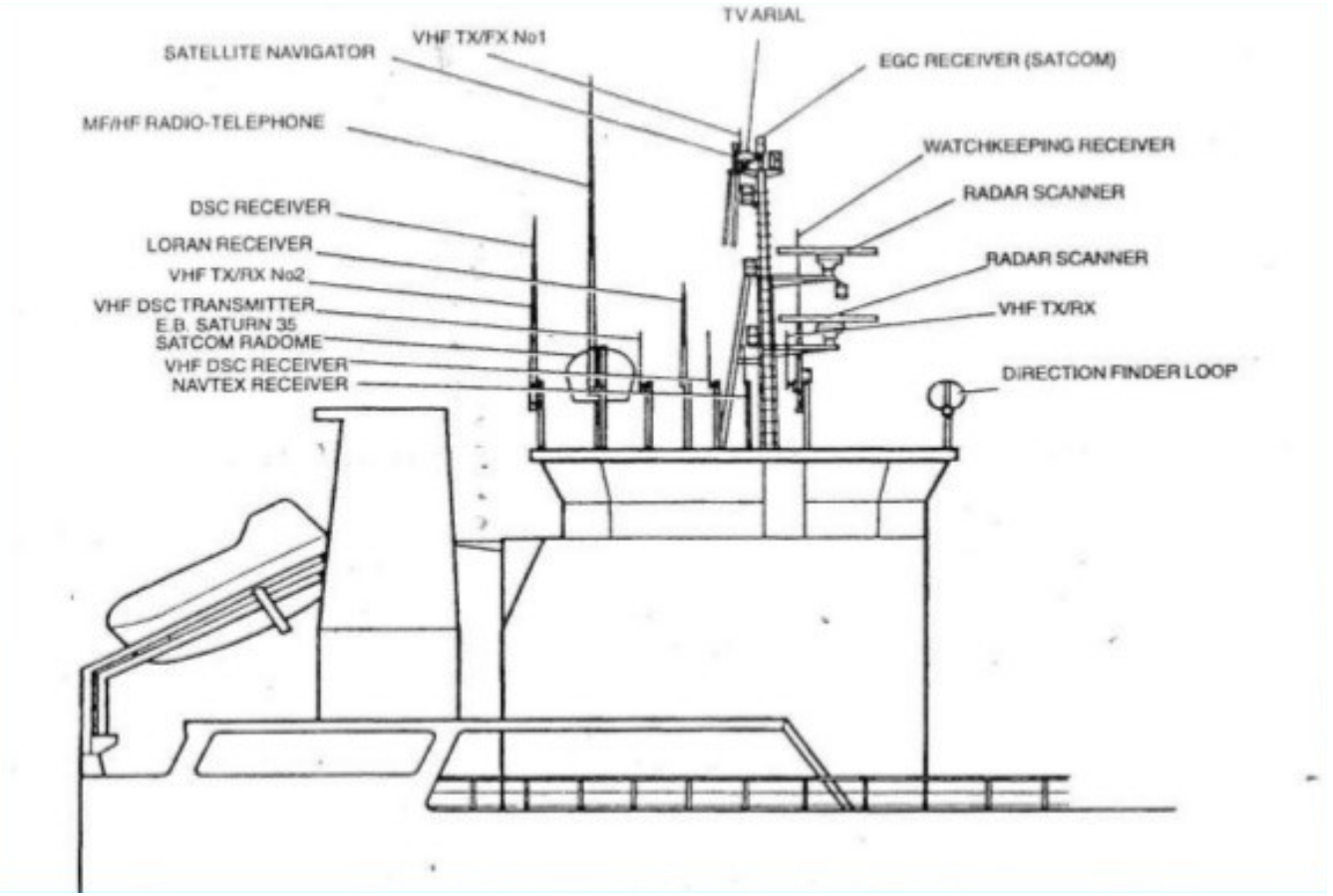
```
*8ce3b19f2f463e3c1d81330e61f8;
CRC: 0e61f8 (ok)
Single bit error fixed, bit 27953
DF 17: ADS-B message.
  Capability     : 4 (Level 2+3+4 (DF0,4,5,11,20,21,24,code7 - is on ground))
  ICAO Address   : e3b19f
  Extended Squitter  Type: 5
  Extended Squitter  Sub : 7
  Extended Squitter  Name: Surface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

modes_rx

$ 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)
```

Ships


TV ARIAL
VHF TX/FX No1
SATELLITE NAVIGATOR
EGC RECEIVER (SATCOM)
MF/HF RADIO-TELEPHONE
WATCHKEEPING RECEIVER
RADAR SCANNER
DSC RECEIVER
LORAN RECEIVER
RADAR SCANNER
VHF TX/RX No2
VHF DSC TRANSMITTER
VHF TX/RX
E.B. SATURN 35
SATCOM RADOME
VHF DSC RECEIVER
DIRECTION FINDER LOOP
NAVTEX RECEIVER

AIS

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

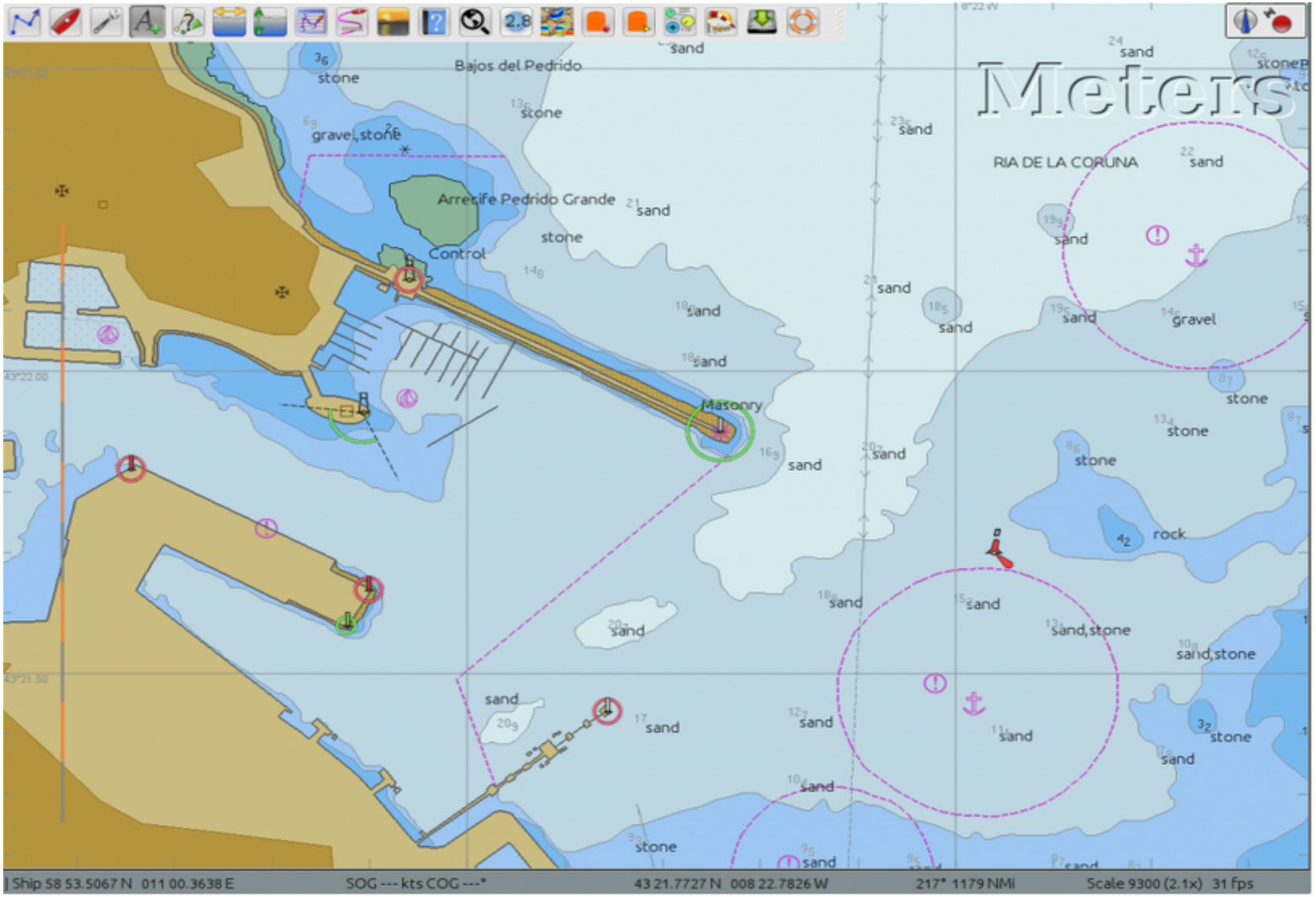
AIS

$ ais_rx -s osmocom

- Chart plotting tool: **opencpn**

  http://opencpn.org/ocpn/

AIS - opencpn


Bajos del Pedrido
Arrecife Pedrido Grande
Control
Masonry
RIA DE LA CORUNA
Meters
| Ship 58 53.5067 N 011 00.3638 E
SOG --- kts COG ---°
43 21.7727 N 008 22.7826 W
217° 1179 NMi
Scale 9300 (2.1x) 31 fps

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)

multimon-ng

- **$ gqrx**

Tune to a pager frequency

Filter: Wide

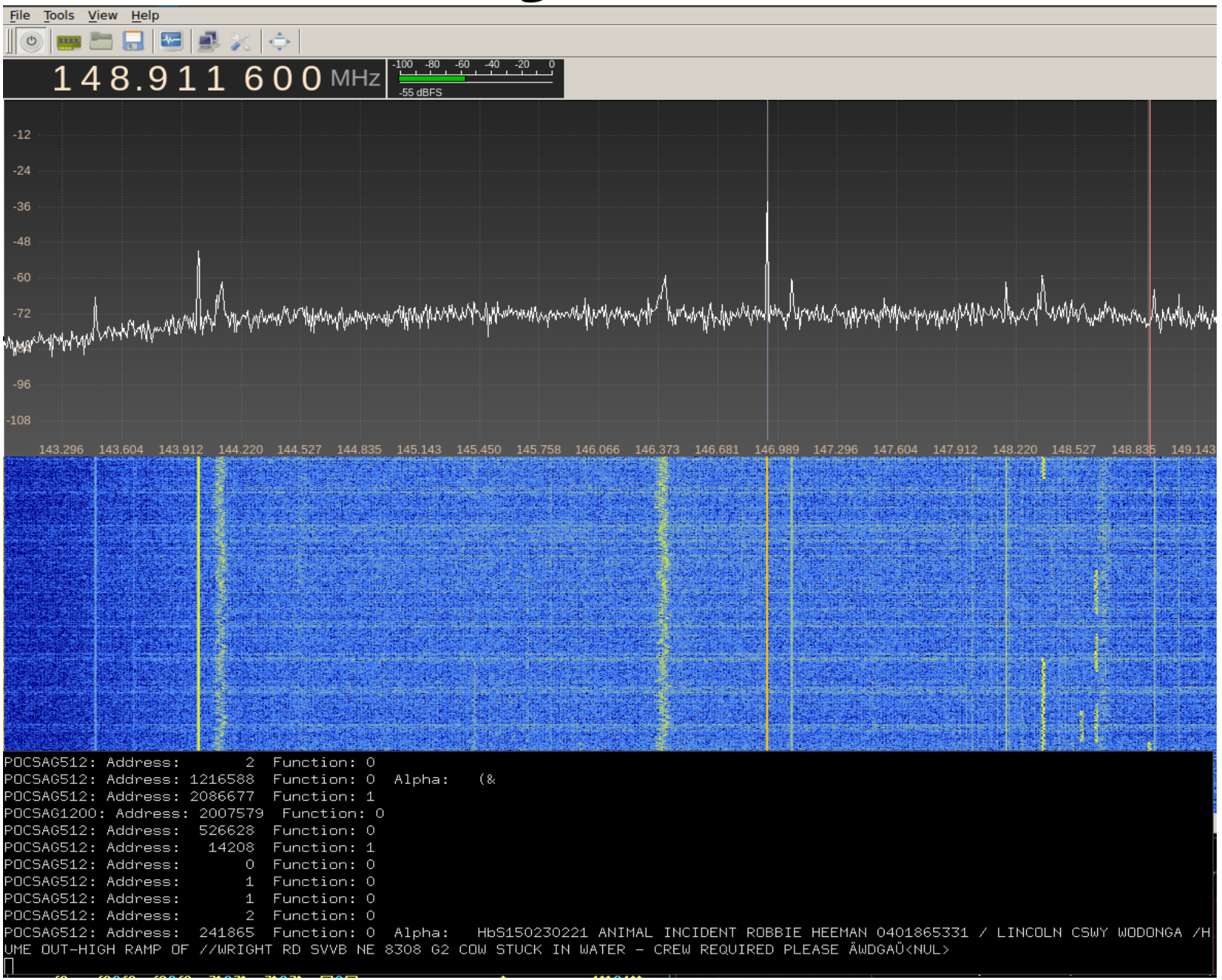
Mode: Narrow FM

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

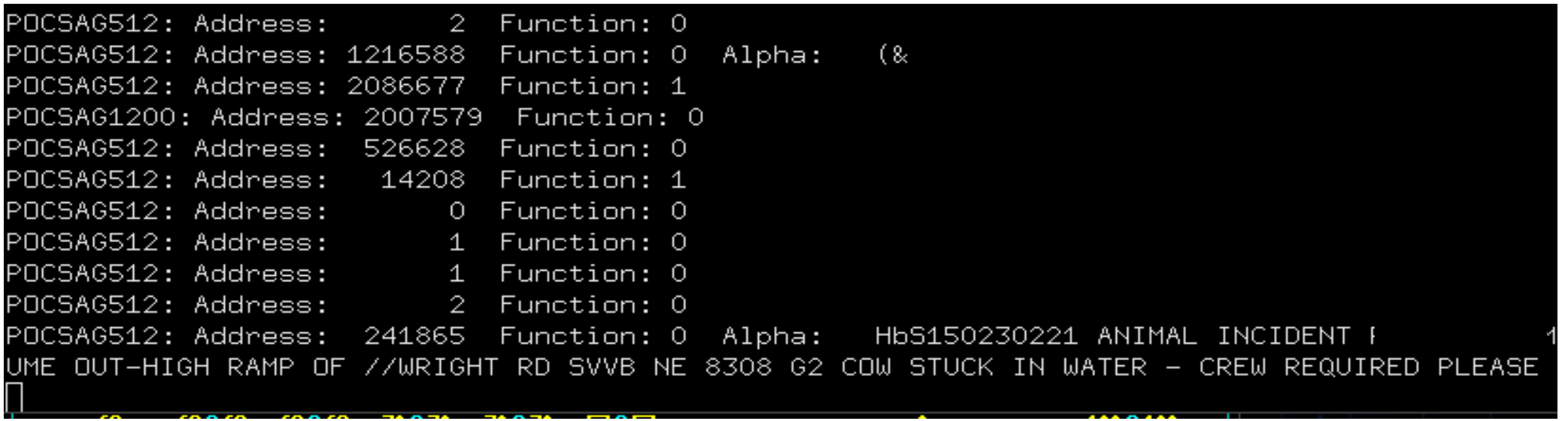
- **$ pauvcontrol**

Enable recording from internal sound card

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 ÂWDGAÜ<NUL>

Pagers


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
UME OUT-HIGH RAMP OF //WRIGHT RD SVVB NE 8308 G2 COW STUCK IN WATER - CREW REQUIRED PLEASE

Pagers

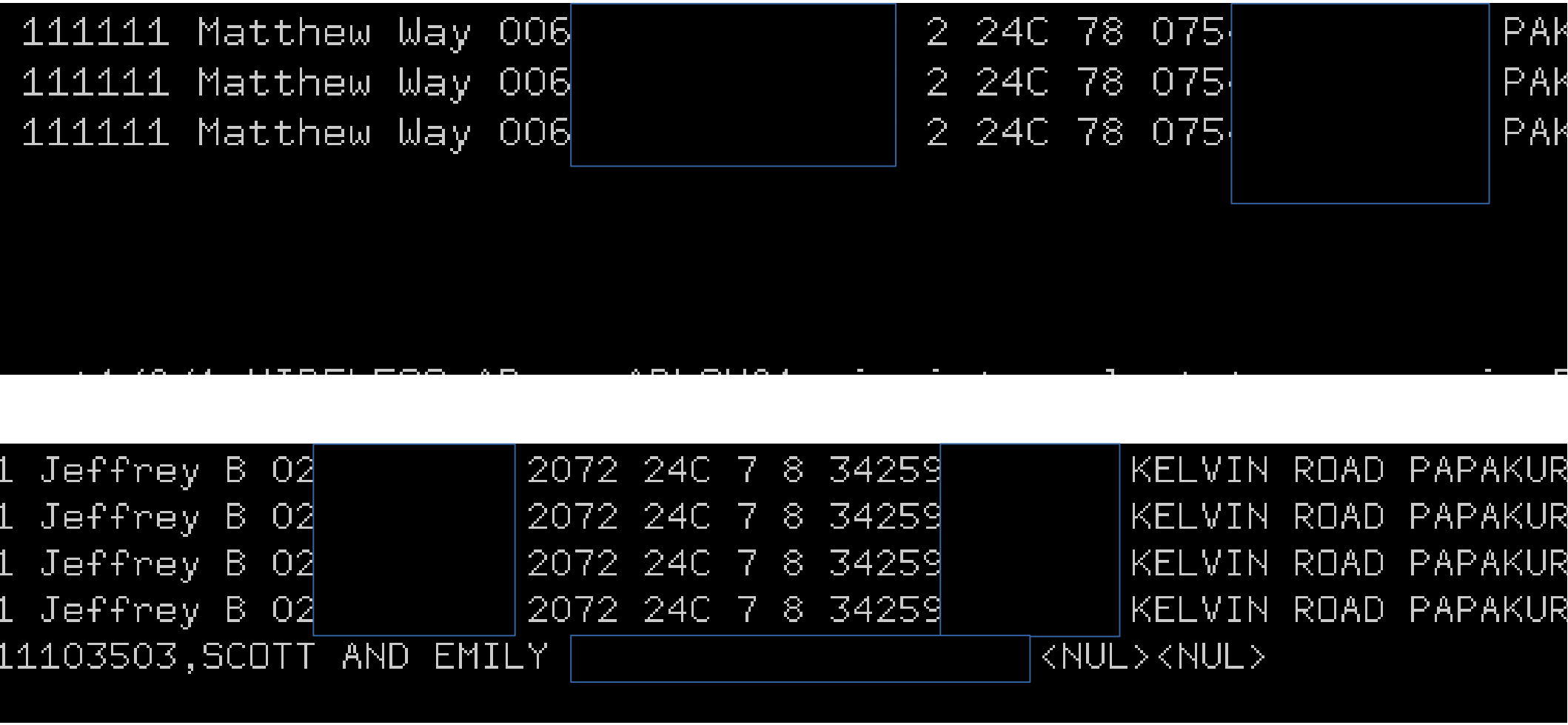
```
Alpha:   MLK P1-61 East Foyer Auto Door Push Button has changed state to: Open-Circuit Ta<NUL><NUL>



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



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

Pagers

```
7BDGS H T3 14:48 27/05 SAINT KENTIGERN TRUST 111111 Matthew [redacted] 207 2 24C 78 07545 [redacted] ROAD AUCKLAND * DPL CHECK OK
7BDGS H T3 14:48 27/05 SAINT KENTIGERN TRUST 111111 Matthew [redacted] 207 2 24C 78 07545 [redacted] ROAD AUCKLAND * DPL CHECK OK
7BDGS H T3 14:48 27/05 SAINT KENTIGERN TRUST 111111 Matthew [redacted] 207 2 24C 78 07545 [redacted] 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] ROAD PAPAKURA * DPL CHECK OK
7BDXX H T3 14:41 27/05 KELVIN ROAD SCHOOL 111111 Jeffrey B 02[redacted] 2072 24C 7 8 34259[redacted] ROAD PAPAKURA * DPL CHECK OK
7BDXX H T3 14:41 27/05 KELVIN ROAD SCHOOL 111111 Jeffrey B 02[redacted] 2072 24C 7 8 34259[redacted] ROAD PAPAKURA * DPL CHECK OK
7BDXX H T3 14:41 27/05 KELVIN ROAD SCHOOL 111111 Jeffrey B 02[redacted] 2072 24C 7 8 34259[redacted] ROAD PAPAKURA * DPL CHECK OK
J639247,MTB12,S31,:34 YAKTANGA WY MOUNT_BARKER:11103503,SCOTT AND EMILY[redacted],<NUL><NUL>
00:18 P260001.ADA
```

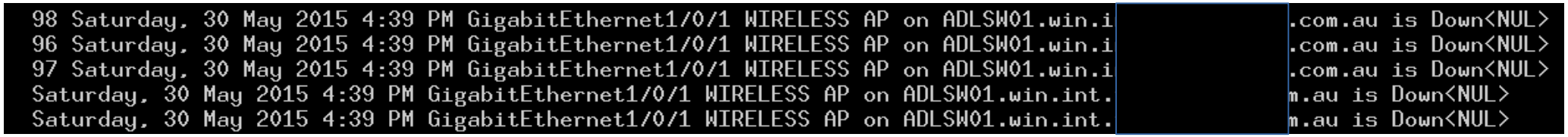
Pagers


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>

Pagers

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

Pagers

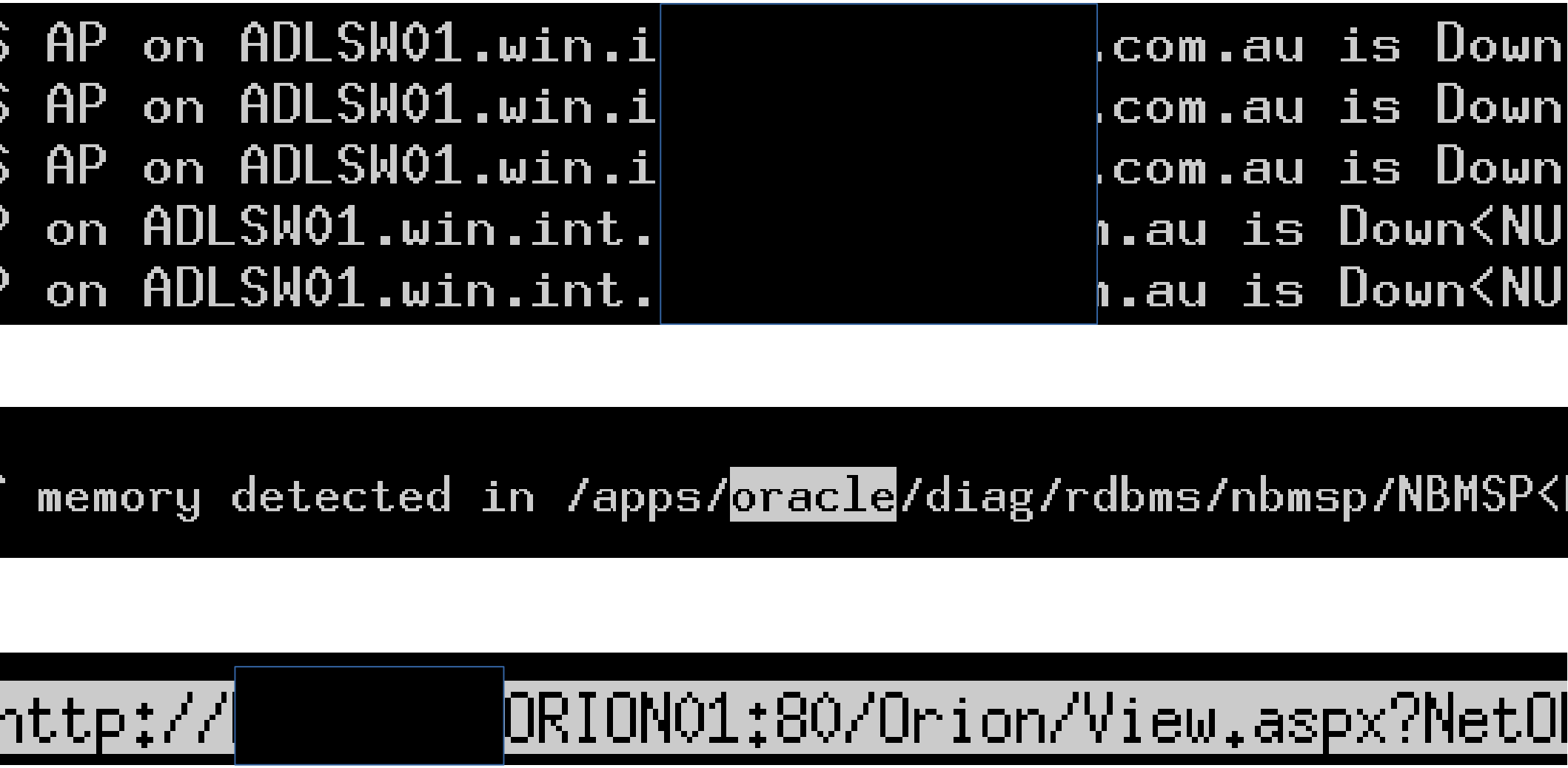

98 Saturday, 30 May 2015 4:39 PM GigabitEthernet1/0/1 WIRELESS AP on ADLSW01.win.i .com.au is Down<NUL>
96 Saturday, 30 May 2015 4:39 PM GigabitEthernet1/0/1 WIRELESS AP on ADLSW01.win.i .com.au is Down<NUL>
97 Saturday, 30 May 2015 4:39 PM GigabitEthernet1/0/1 WIRELESS AP on ADLSW01.win.i .com.au is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


Ä1/2Ü ÄRepeat #2Ü EM Event: Critical:NBMSP.arcbs .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

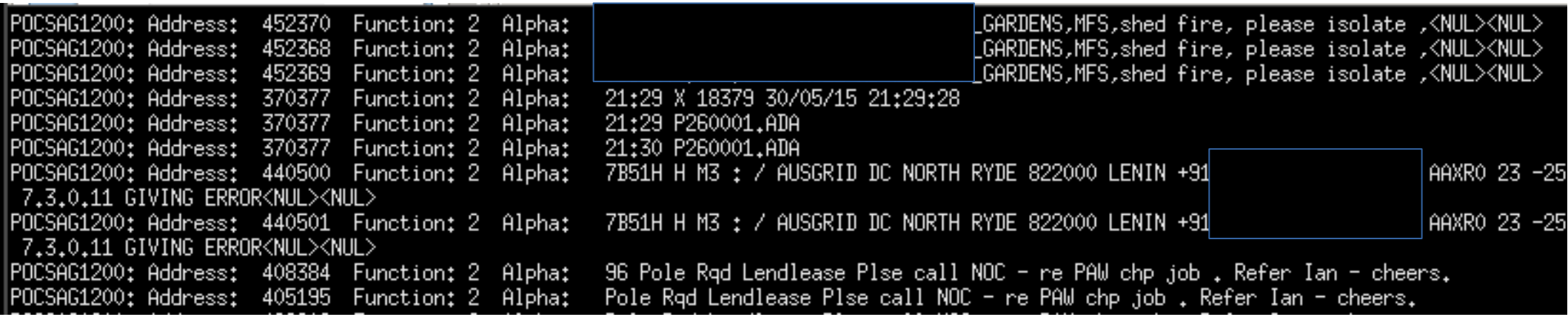

84 Saturday, 30 May 2015 5:02 PM
REA-EQX-SQLN1 100 % CPU - Top 10

http:/ -ORION01:80/Orion/View.aspx?NetObject=N:301<NUL>

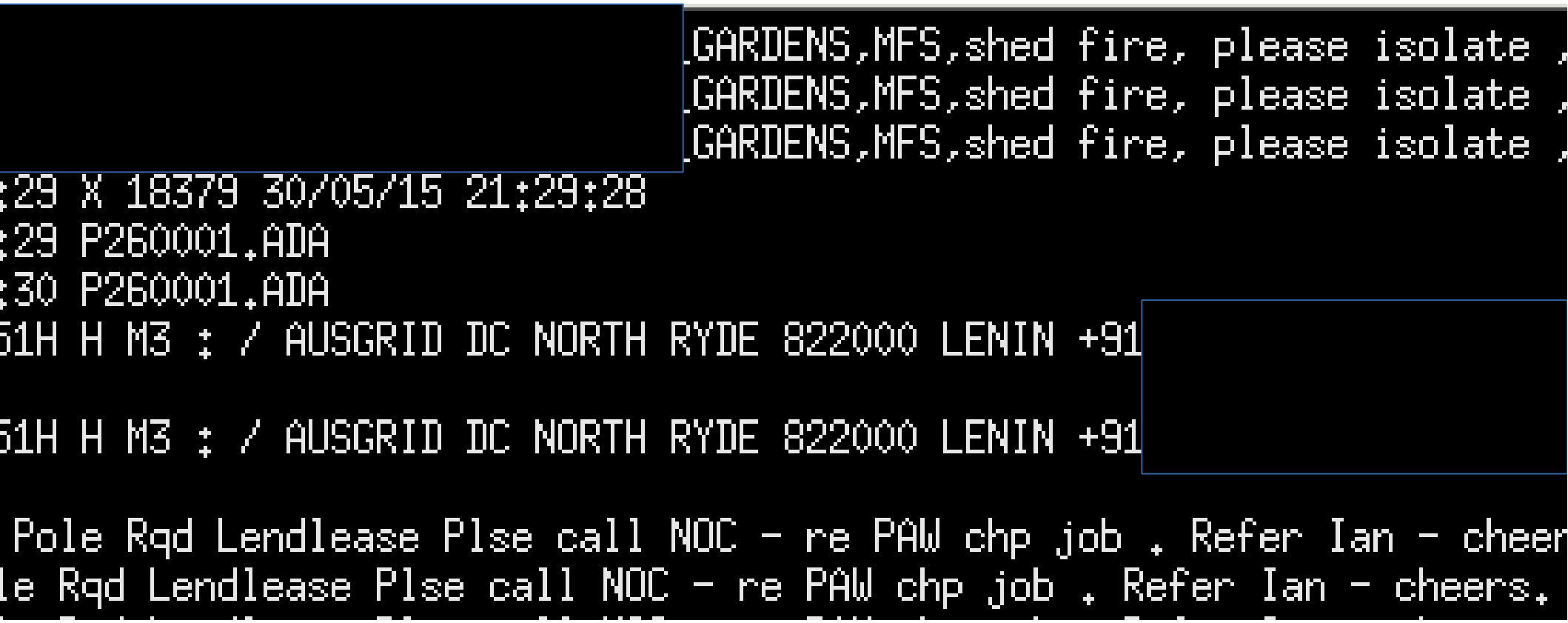
Pagers


AP on ADLSW01.win.i .com.au is Down
AP on ADLSW01.win.i .com.au is Down
AP on ADLSW01.win.i .com.au is Down
on ADLSW01.win.int. .au is Down<NU
on ADLSW01.win.int. .au is Down<NU
memory detected in /apps/oracle/diag/rdbms/nbmsp/NBMSP<
http://ORION01:80/Orion/View.aspx?NetO

Pagers


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.

Pagers


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.

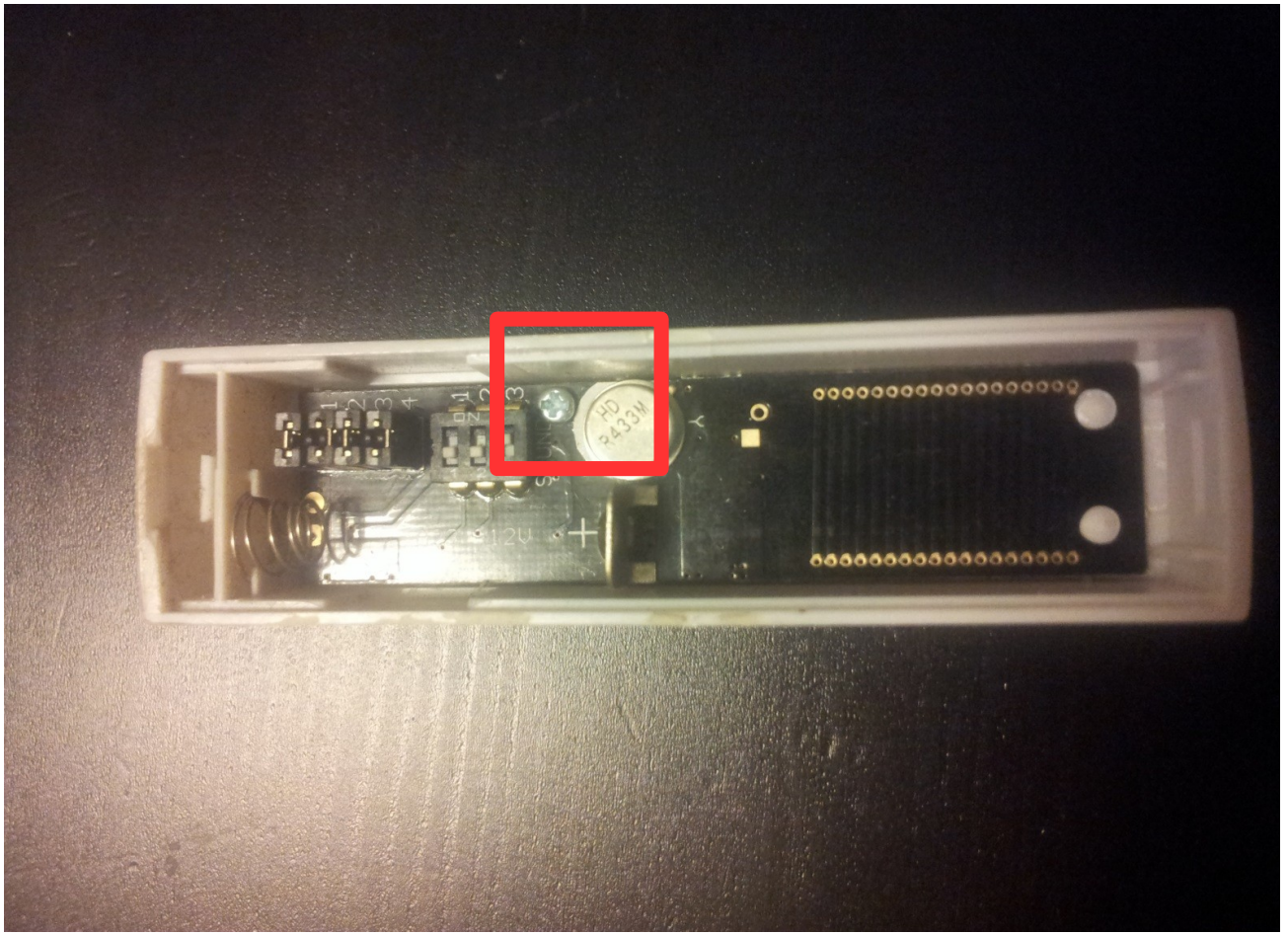
Remote Control Analysis

Remote Control Analysis

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

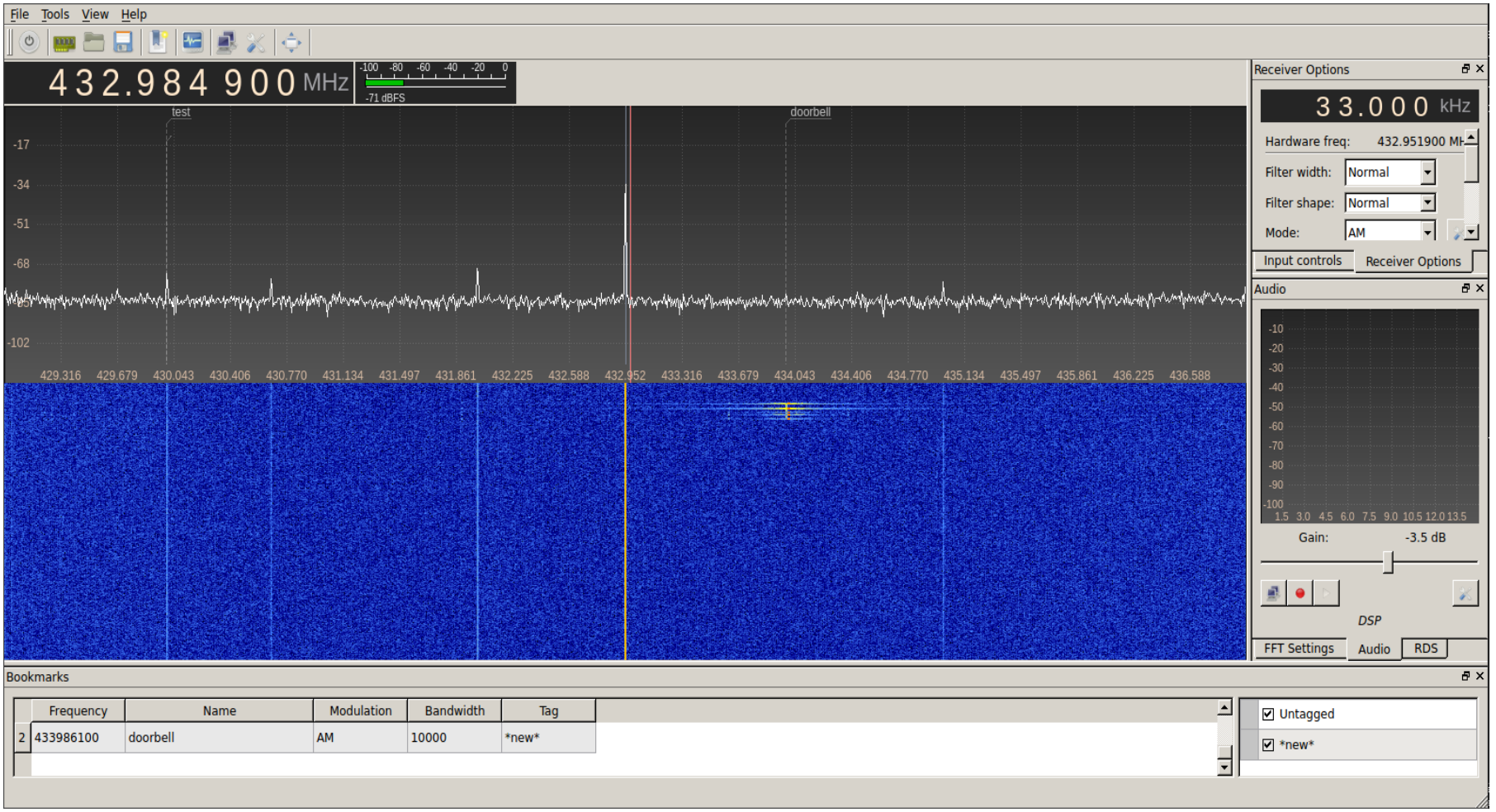
Remotes - Doorbells

1) Identify Frequency: 433Mhz (approx)



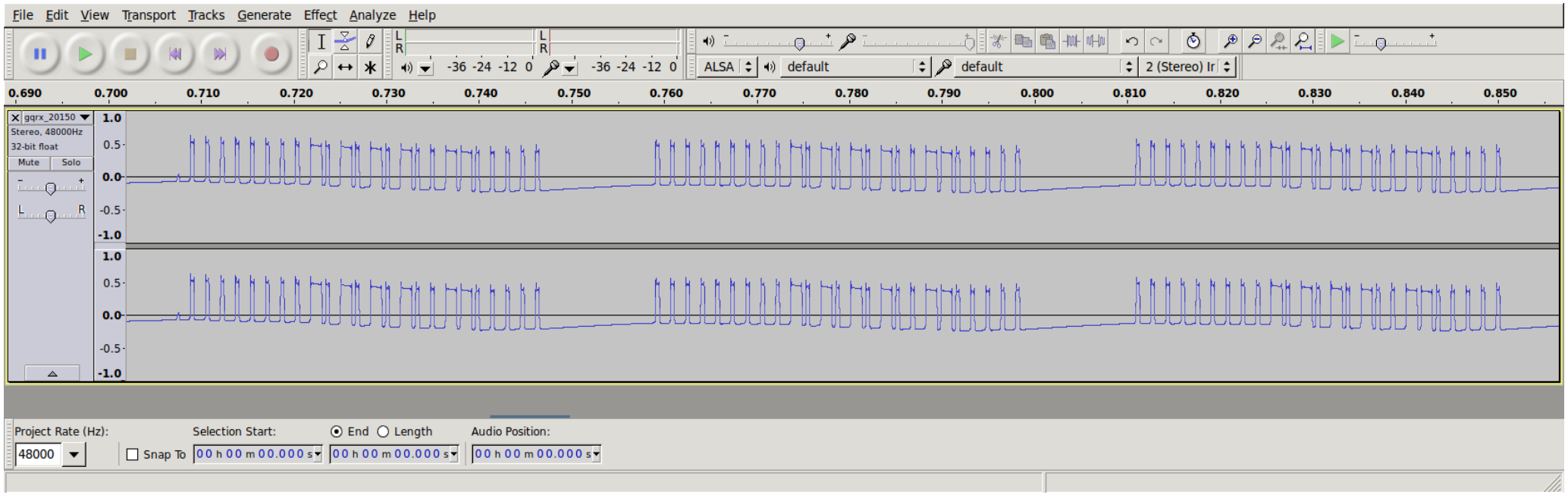
Remotes - Doorbells

2A) Identify Modulation: listening in GQRX



Remotes - Doorbells

2B) Open Recoding in Audacity



Remotes - Doorbells

- 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

Remotes - Doorbells

3) Capture Raw Data

- Check frequency in gqrx and record with a hackrf:
- **$ hackrf_transfer -r 433995700.raw -f 433995700**

Remotes - 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**

Questions

Time to try for yourself...