An Introduction to Software Defined Radio

Pamela O'Shea, @pamoshea

Contents

1. Hardware
2. Software
3. Planes
4. Ships
5. Pagers
6. Home devices

1. Hardware

- RTL-SDR Dongle: Great value receiver!
- Realtek RTL2832U/R820T Tuner Receiver
- Freq range: 24 MHz - 1.8 GHz
- Receive only
- $10 AUD

1. Hardware

- HackRF One
- Transmit & Receive
- Half Duplex
- Freq Range: 1 MHz - 6 GHz
- $520 AUD

1. Hardware

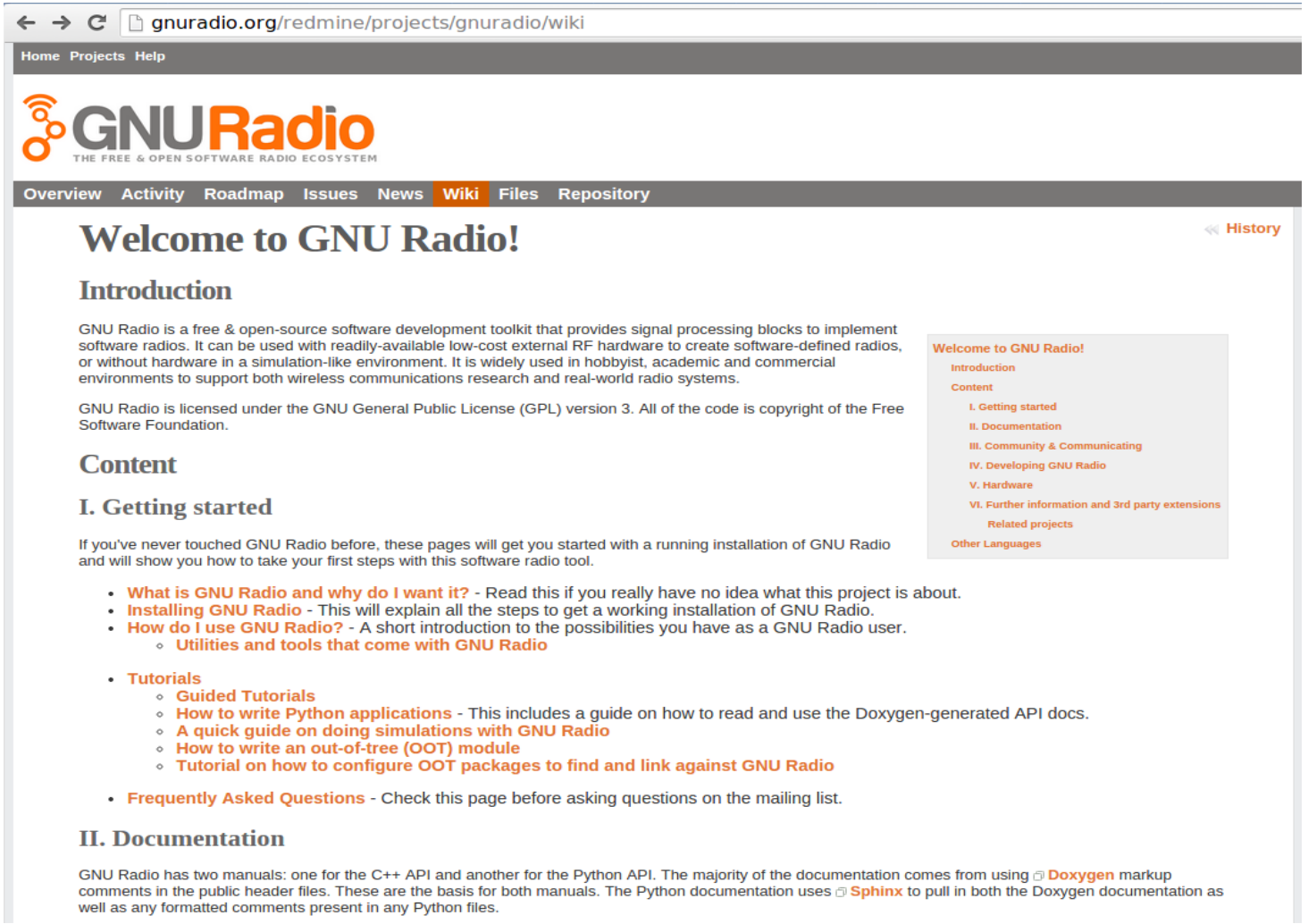
- HackRF One Portapack
- Add on
- Come see at our equipment table after the talks

1. Hardware

- USRP
- New model USRP E312
- Freq range: 70 MHz - 6 GHz
- $5,220 AUD

2. Software

- GNU RADIO



2. Software

- **Linux**
  - **GNU Radio Live:** https://gnuradio.org/redmine/projects/gnuradio/wiki/GNURadioLiveDVD
  - **Pentoo:** http://www.pentoo.ch
  - **Kali**: https://www.kali.org
  - **Ubuntu**: http://www.ubuntu.com
- **Windows**:
  - Not covering Windows this meetup 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. Software

- **GQRX** on Linux
- This is also supplied in our Live USB Dongles
- Tune into FM radio

3. Planes

3. Planes – ADSB

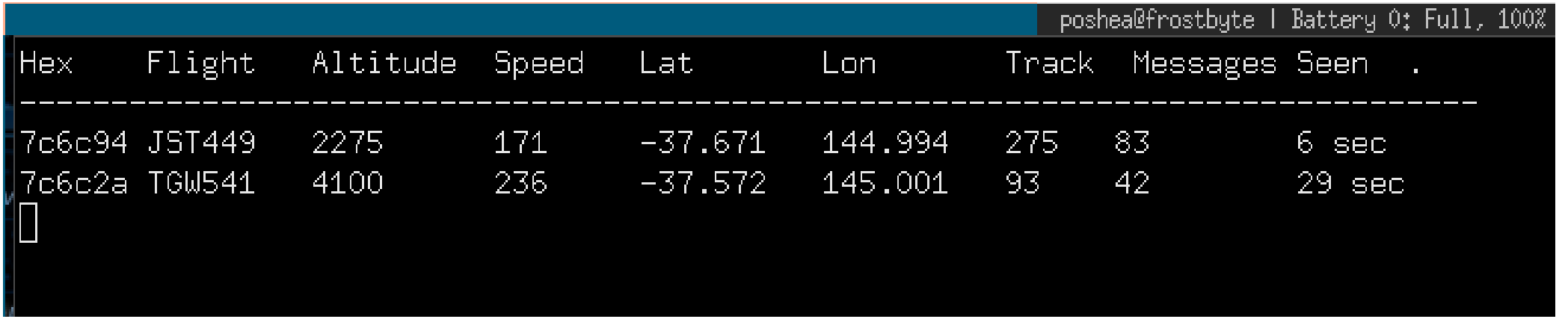
- **ADSB**: Automatic dependent surveillance – broadcast
- Radar replacement
- Aircraft gets position from satellite and broadcasts it for tracking
- No encryption or authentication
- 1090 Mhz (or 978 Mhz)

3. Planes – dump1090: list aircraft

- Tool: **dump1090**

  https://github.com/antirez/dump1090

  dump1090 --interactive --aggressive



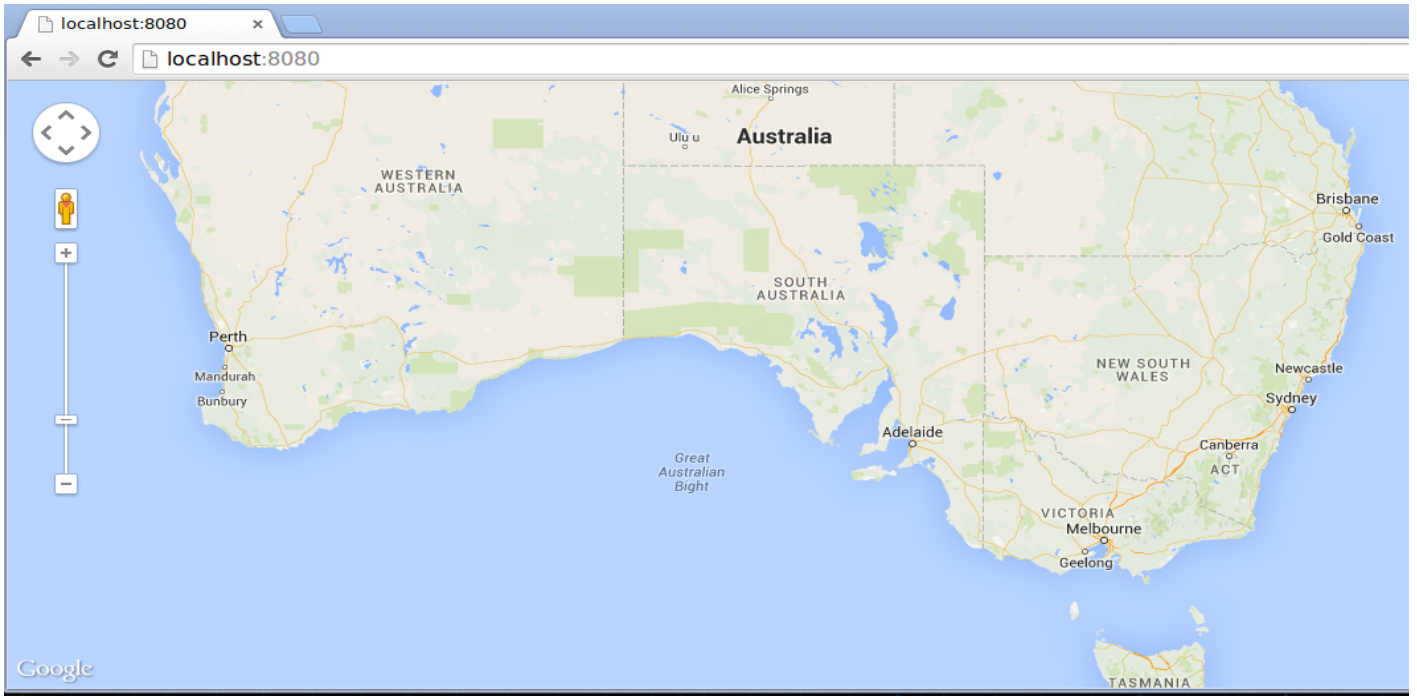
3. Planes – dump1090 Viewing on a Map

dump1090 --interactive --aggressive --net

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

3. Planes - dump1090: Viewing on a Map

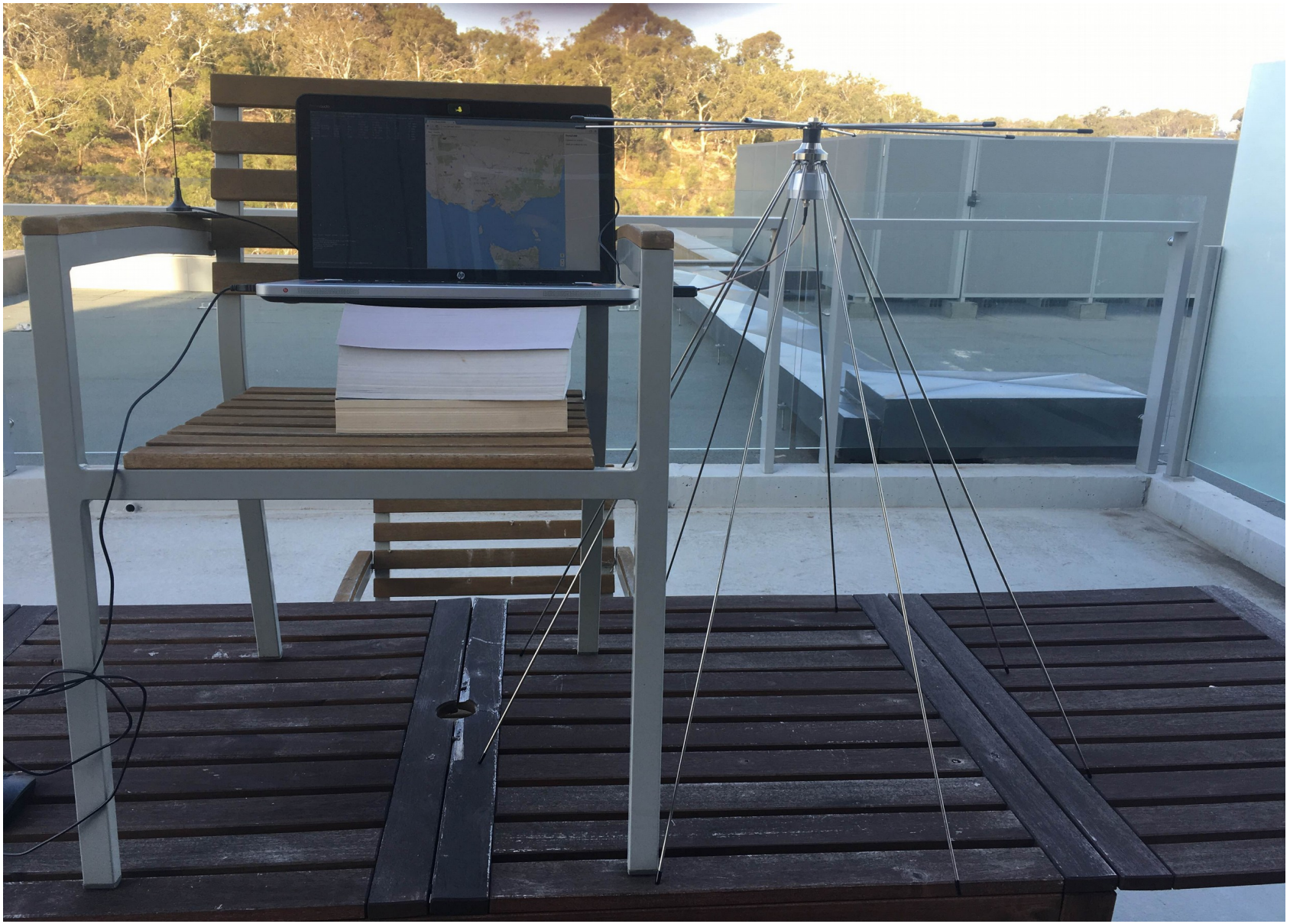
```
Hex    Flight   Altitude  Speed   Lat       Lon       Track  Messages Seen    .
--------------------------------------------------------------------------------
c319ce          0         0       0.000     0.000     0      1          32 sec
0c1a1f          0         0       0.000     0.000     0      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
```



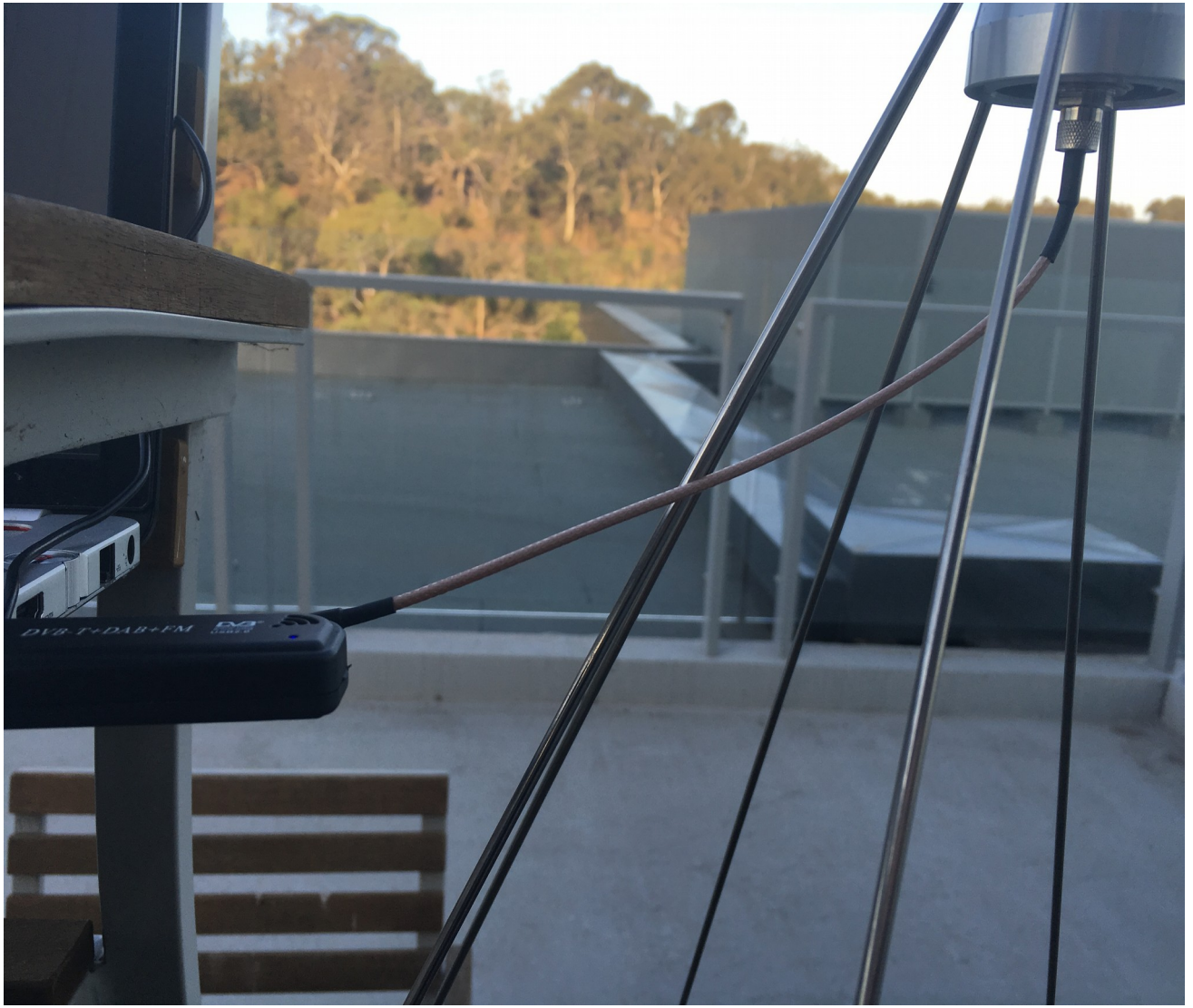
3. Planes – dump1090: Viewing messages

```
*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. Planes – Discone Antenna



3. Planes – Discone Antenna



3. Planes – Discone Antenna

3. Planes – Discone Antenna

3. Planes

[Video]

3. Planes

- The basic rubber ducky antenna with the RTL SDR will still give you great results
- Just make sure its in line of sight of the sky
- The higher the better
- Could even try with a drone and present your results here!

4. Ships

4. Ships - AIS

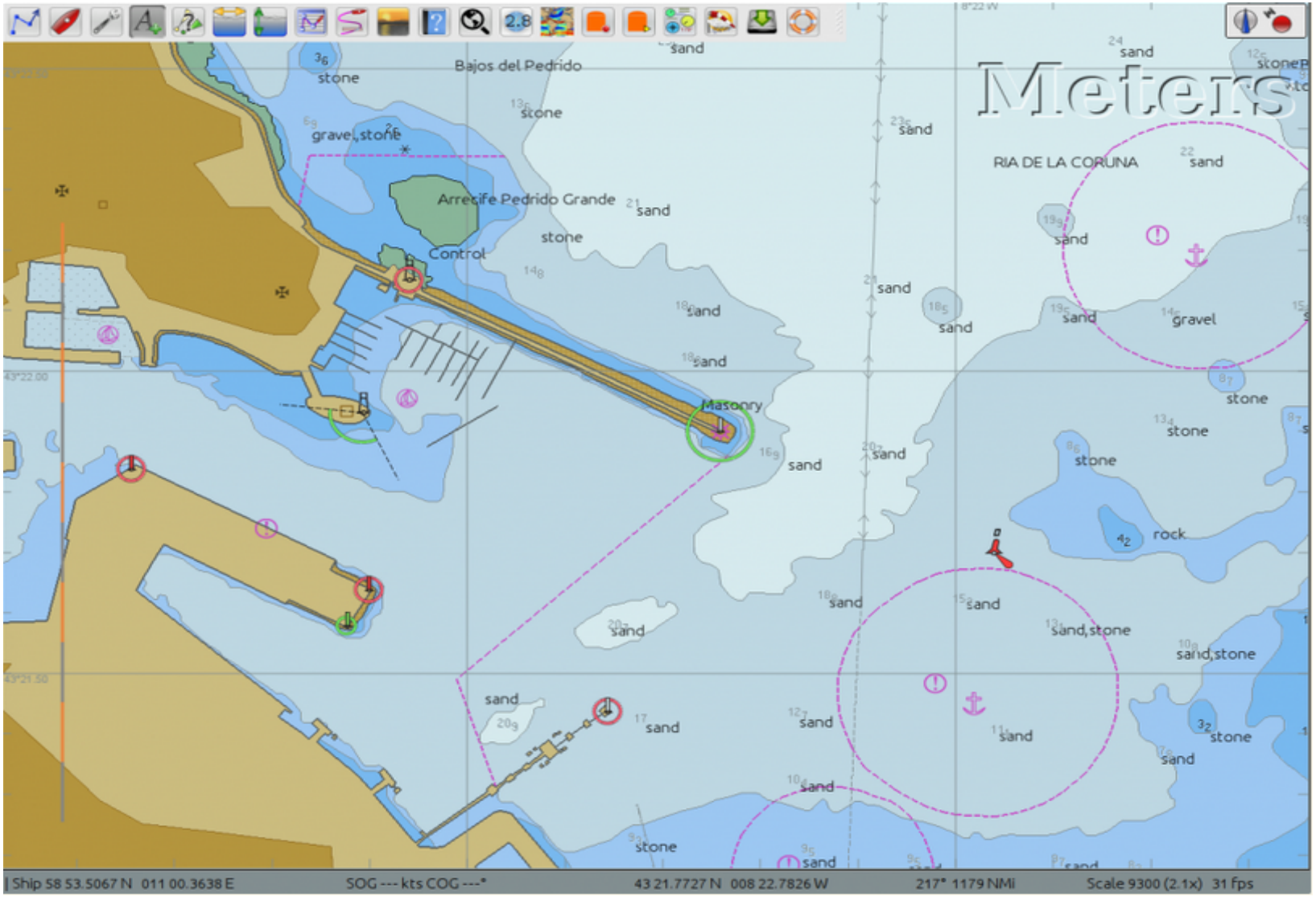
- AIS: Automatic Identification System
- Tracking systems for ships
- Location
- Messages
- Similar to ADS-B
- 162Mhz

4. Ships

- AIS receiver: **ais_rx**
  - https://github.com/bistromath/gr-ais/
  - ./ais_rx -s osmocom

- Chart plotting tool: **opencpn**
  - http://opencpn.org/ocpn/

4. Ships - opencpn



5. Pagers

5. 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)

5. Pagers – multimon-ng

- Tool: **multimon**

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

  1. **gqrx**: tune to a pager frequency

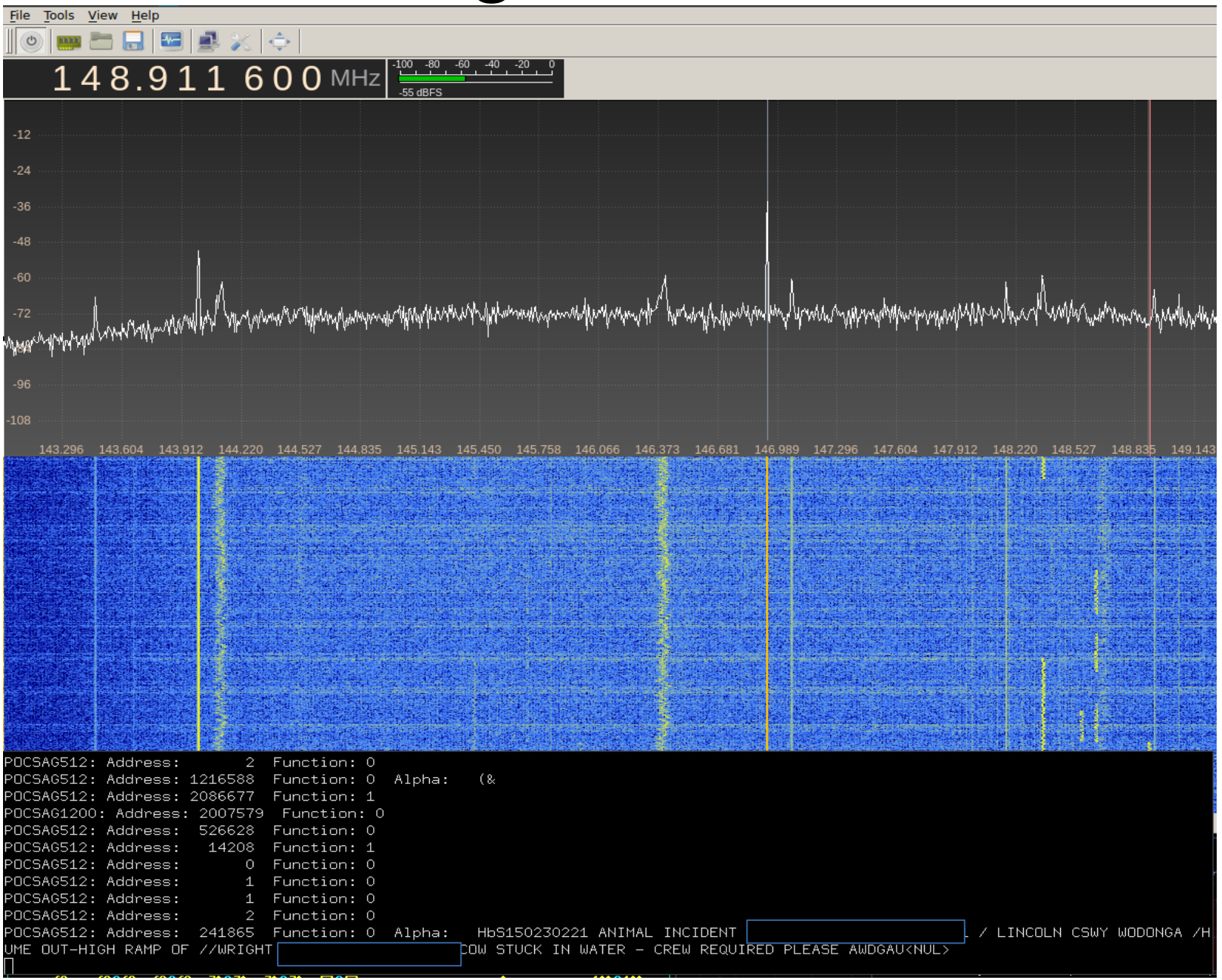
  Filter: Wide

  Mode: Narrow FM

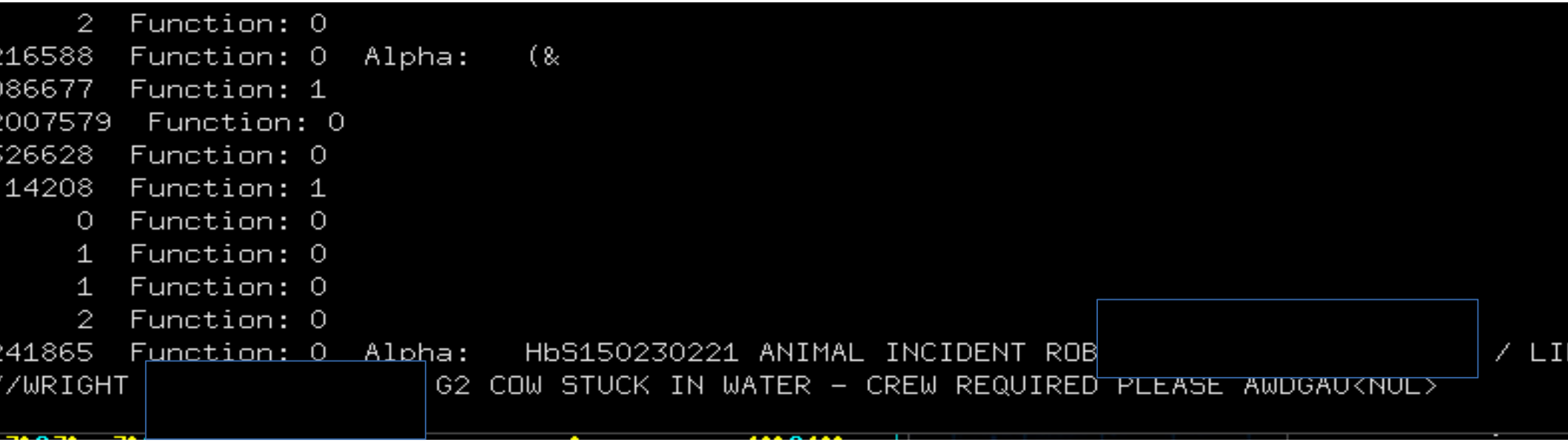
  2. **padsp multimon-ng** -a POCSAG512 -a POCSAG1200 -a POCSAG2400 -f alpha

  3. **pauvcontrol** – enable recording from internal sound card

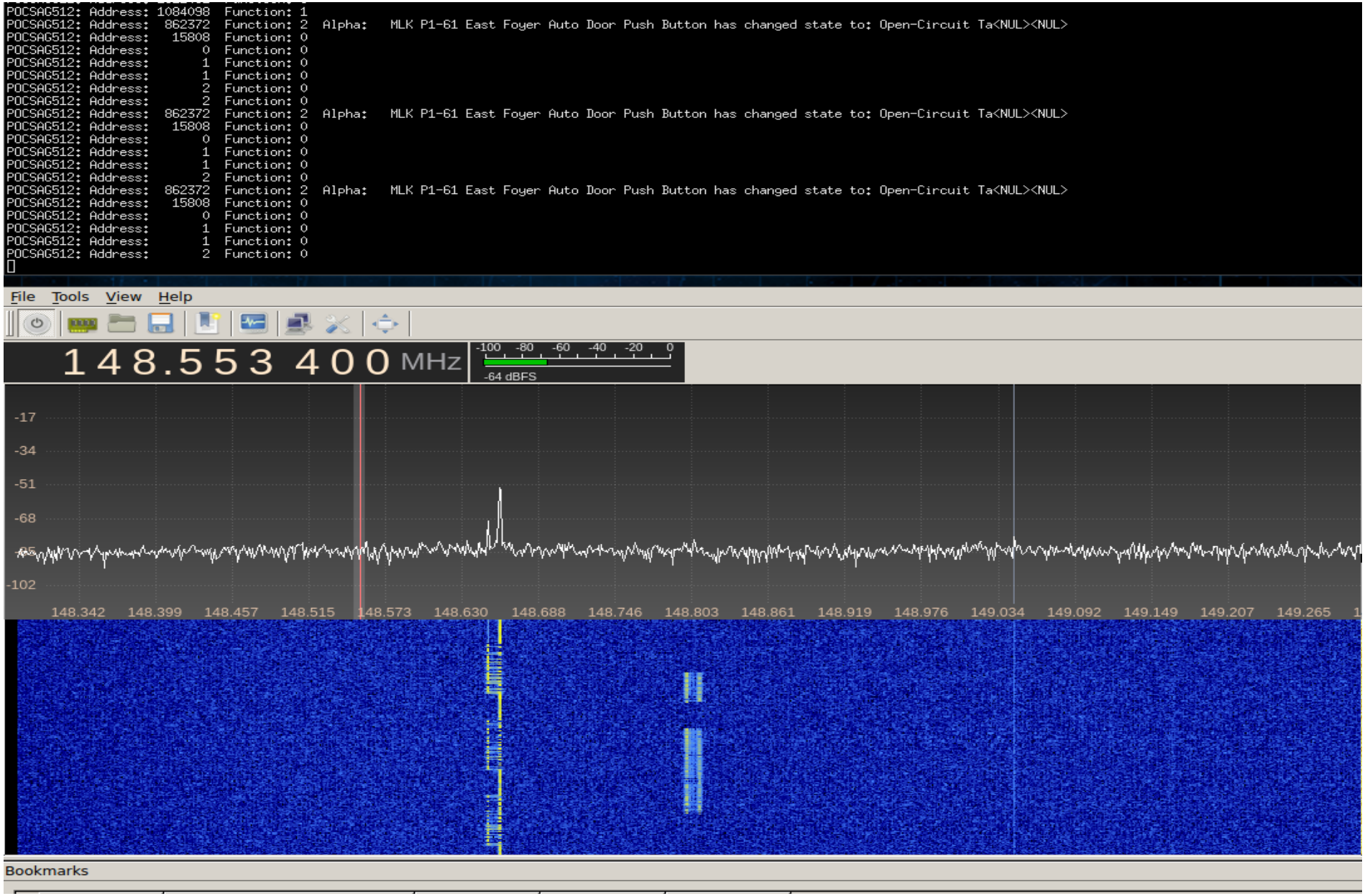
5. Pagers – VET


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 / LINCOLN CSWY WODONGA /H
UME OUT-HIGH RAMP OF //WRIGHT COW STUCK IN WATER - CREW REQUIRED PLEASE AWDGAU<NUL>

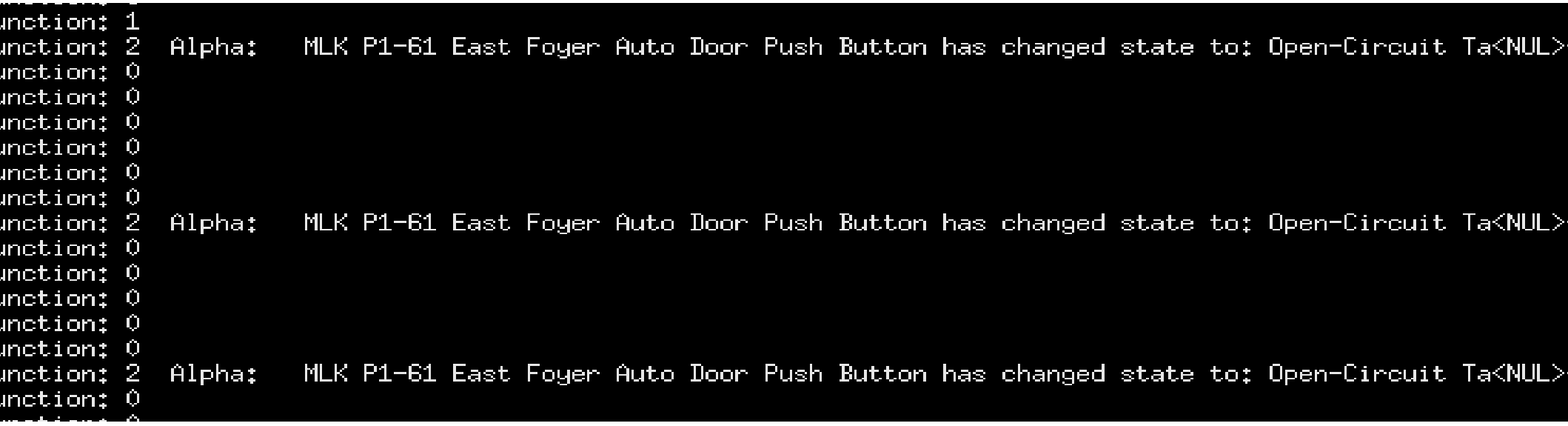
5. Pagers – VET (zoom-in)



5. Pagers – Doors



5. Pagers – Doors (zoom-in)

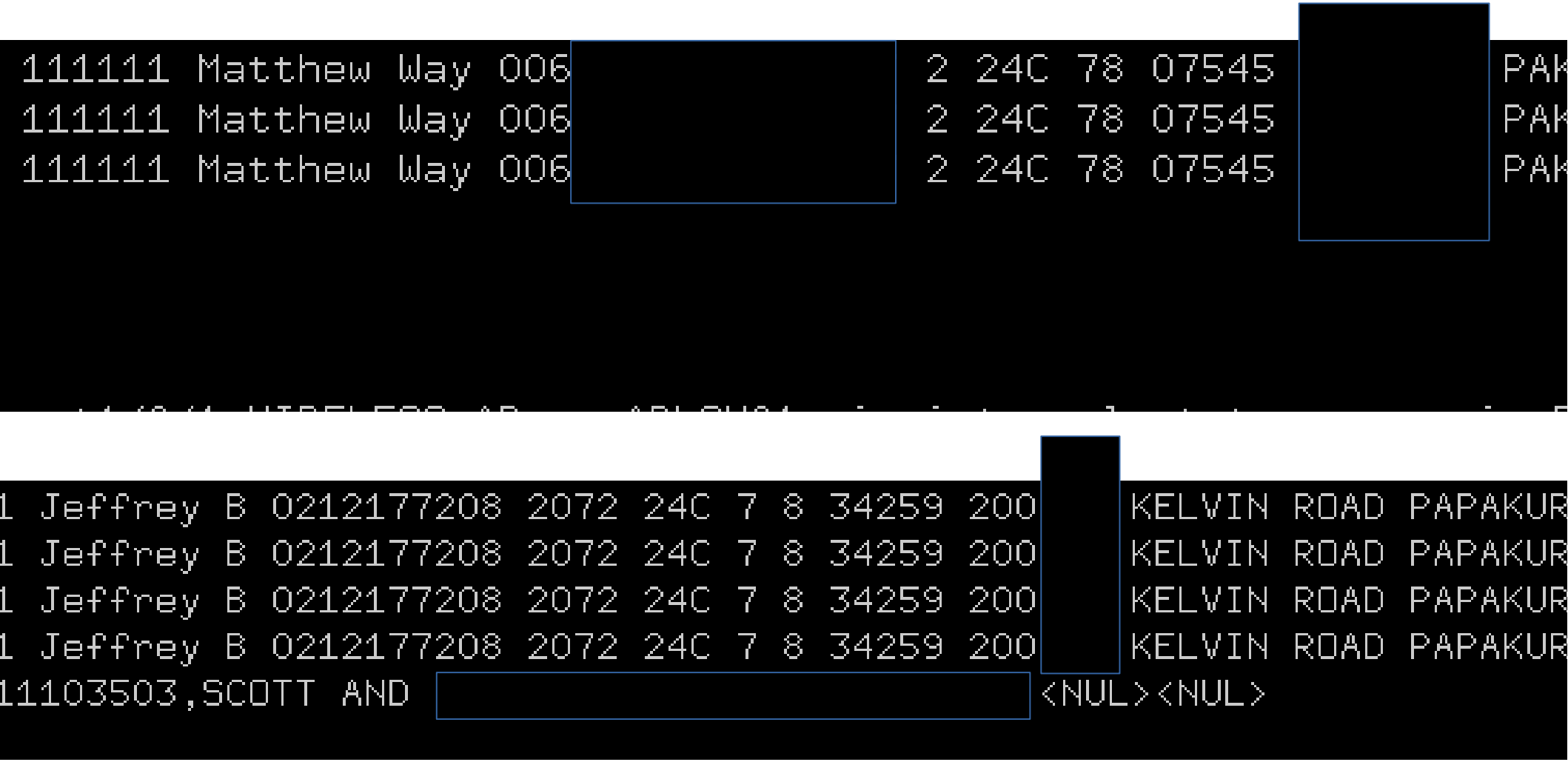


5. Pagers – Licence Plate Checks

```
7BDGS H T3 14:48 27/05 SAINT KENTIGERN TRUST 111111 Matthew [redacted] 24C 78 075[redacted]KURANGA ROAD AUCKLAND * DPL CHECK OK
7BDGS H T3 14:48 27/05 SAINT KENTIGERN TRUST 111111 Matthew [redacted] 24C 78 075[redacted]KURANGA ROAD AUCKLAND * DPL CHECK OK
7BDGS H T3 14:48 27/05 SAINT KENTIGERN TRUST 111111 Matthew [redacted] 24C 78 075[redacted]KURANGA 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 0212[redacted] 24C 7 8 34259 [redacted] ROAD PAPAKURA * DPL CHECK OK
7BDXX H T3 14:41 27/05 KELVIN ROAD SCHOOL 111111 Jeffrey B 0212[redacted] 24C 7 8 34259 [redacted] ROAD PAPAKURA * DPL CHECK OK
7BDXX H T3 14:41 27/05 KELVIN ROAD SCHOOL 111111 Jeffrey B 0212[redacted] 24C 7 8 34259 [redacted] ROAD PAPAKURA * DPL CHECK OK
7BDXX H T3 14:41 27/05 KELVIN ROAD SCHOOL 111111 Jeffrey B 0212[redacted] 24C 7 8 34259 [redacted] ROAD PAPAKURA * DPL CHECK OK
[redacted] MOUNT_BARKER:11103503,SCOTT AND[redacted]
```

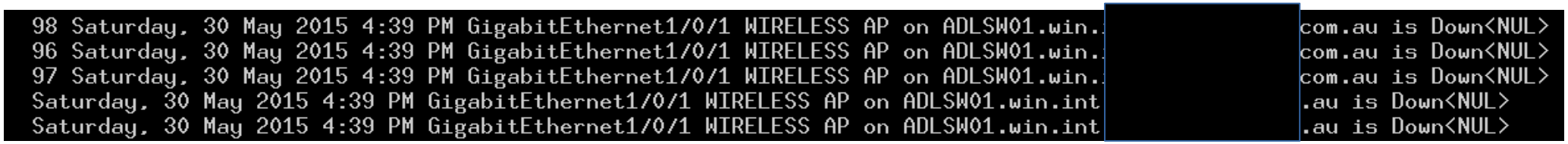
5. Pagers – Licence Plate Checks (zoom in)



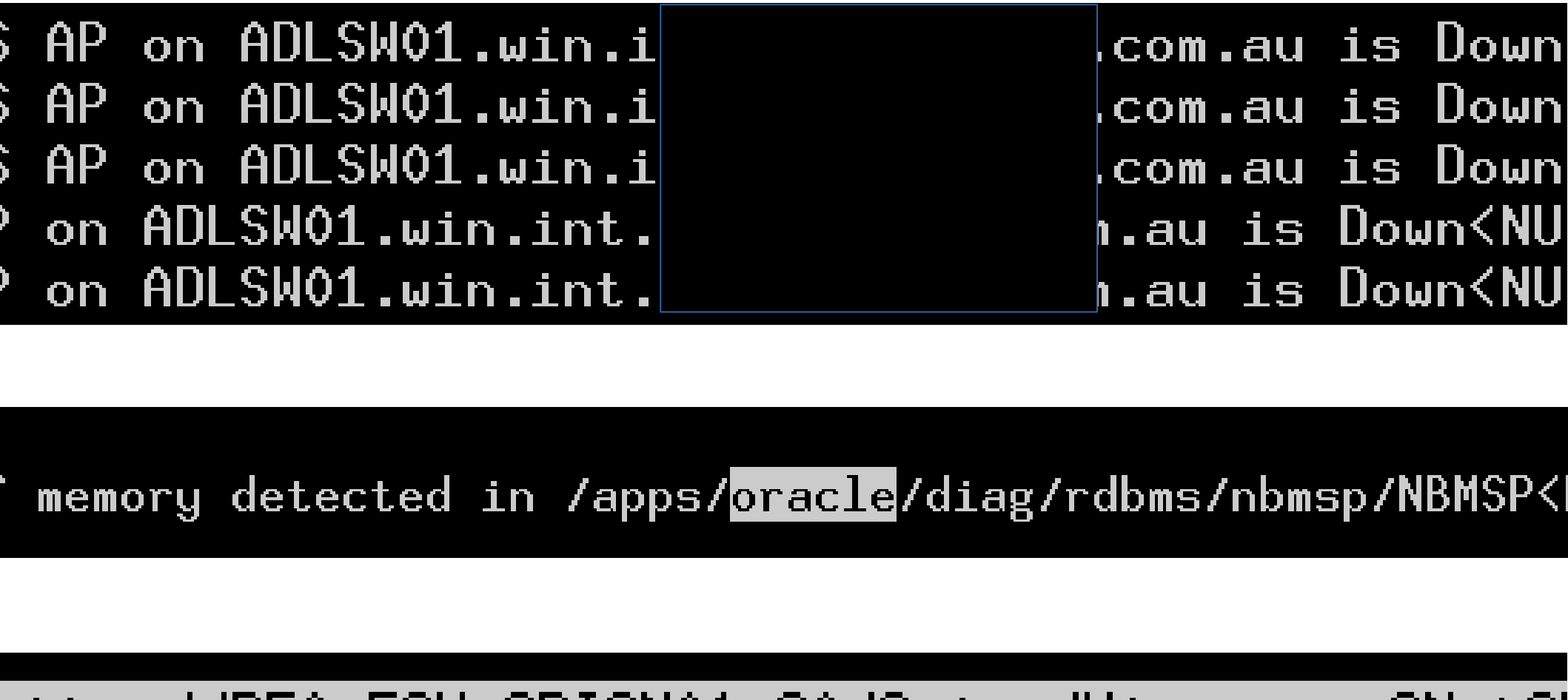
5. Pagers – Passcodes

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

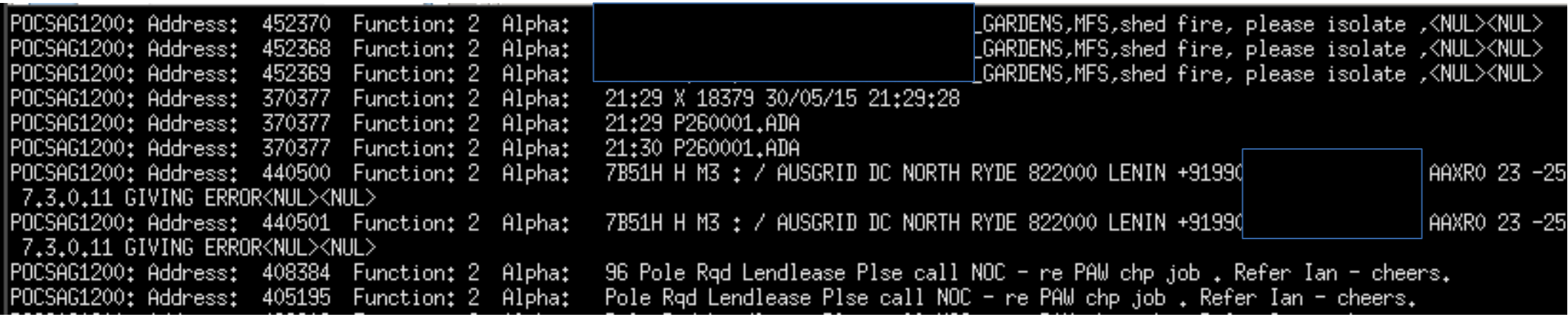
5. Pagers – Datacentre Servers



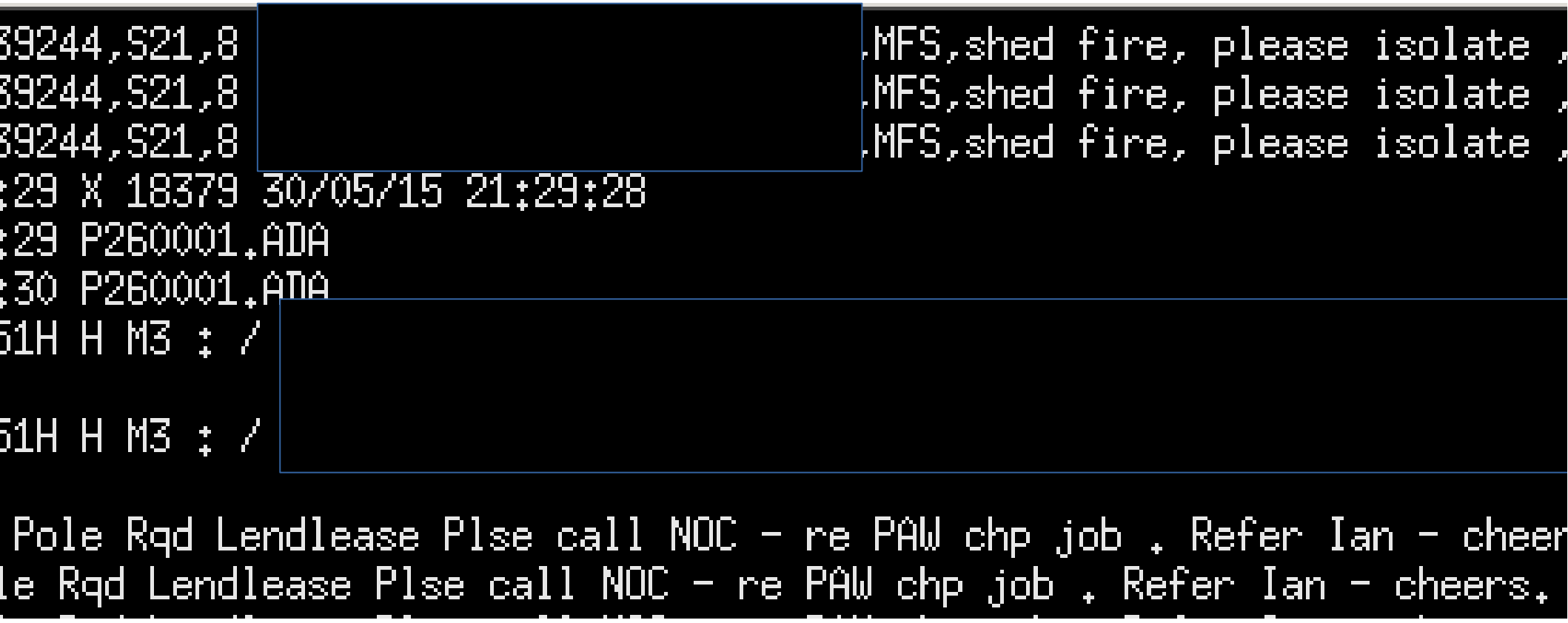
5. Pagers – Datacentre Servers (zoom in)



5. Pagers – Emergency Services



5. Pagers – Emergency Services (zoom in)



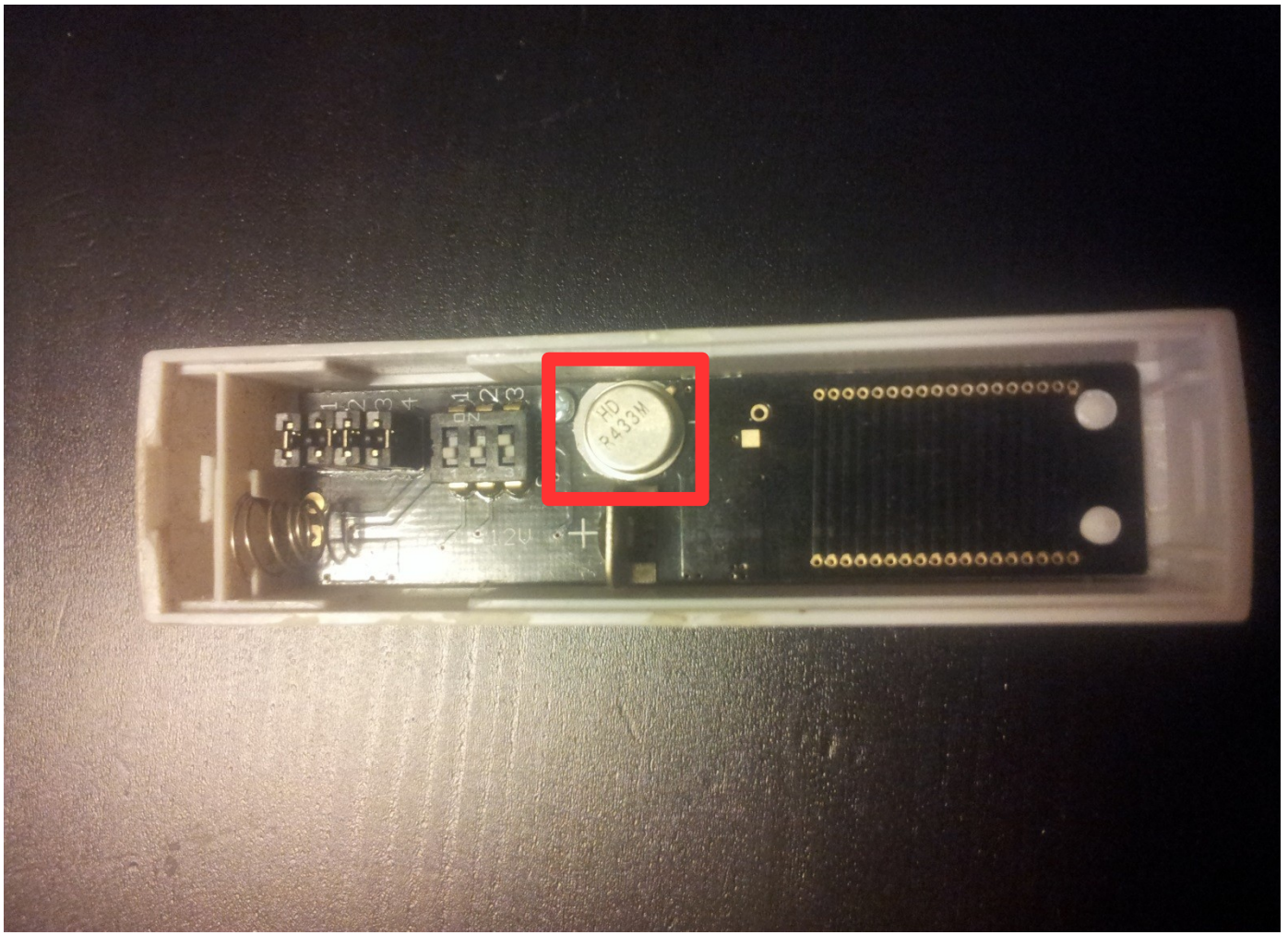
6. Home Devices

6. Home Devices

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

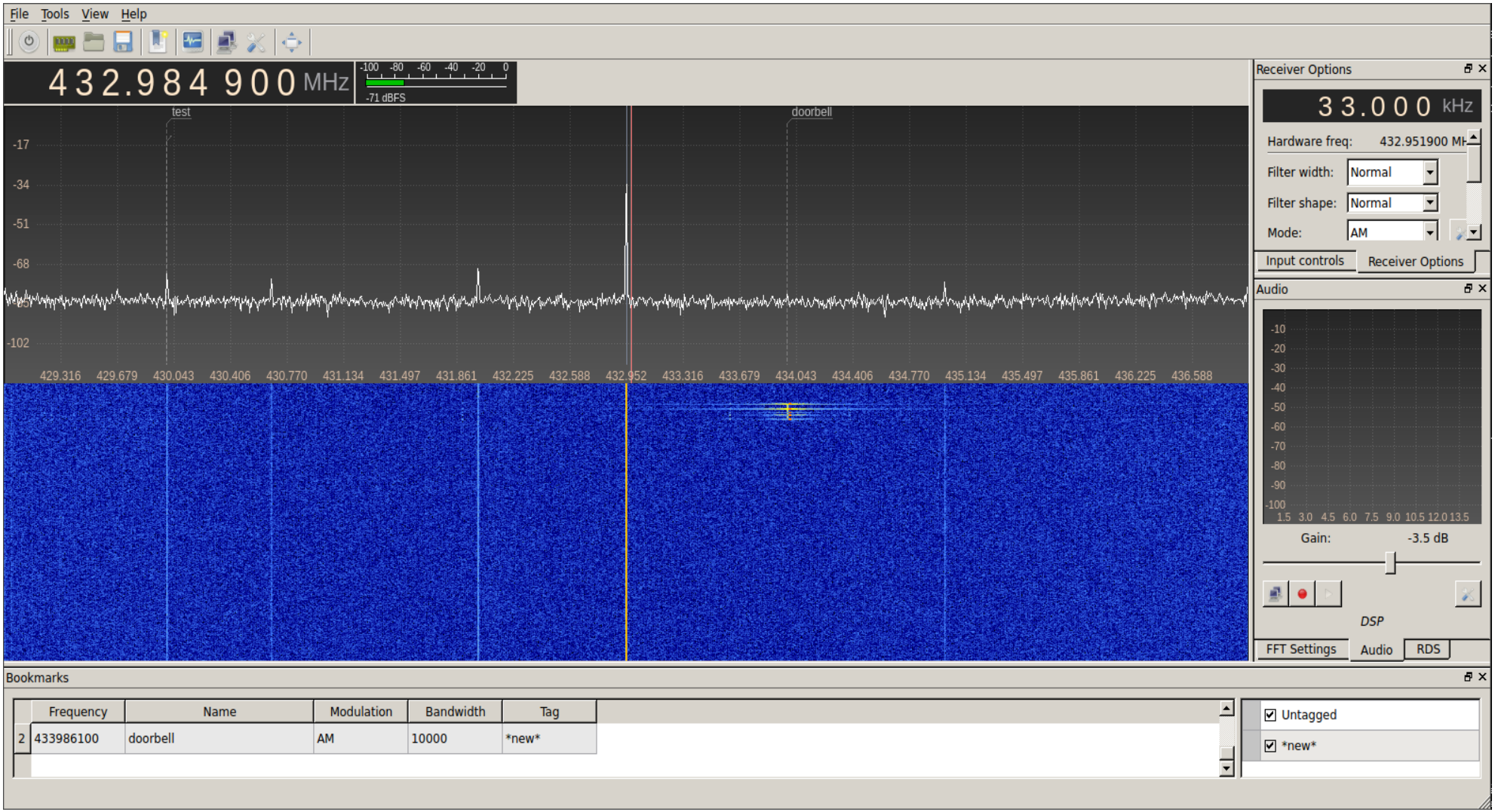
6. Home Devices - Doorbells

1) Identify Frequency: 433Mhz (approx)



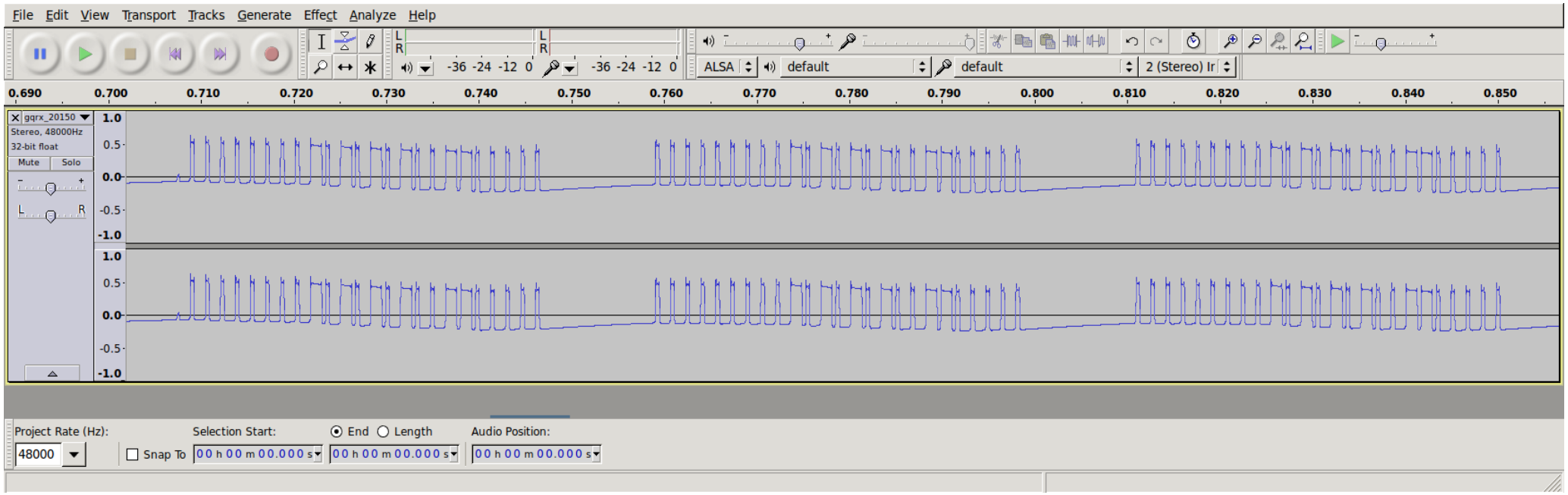
6. Home Devices - Doorbells

2A) Identify Modulation: listening in gqrx



6. Home Devices - Doorbells

2B) Open Recoding in Audacity



6. 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

6. Home Devices - Doorbells

3) Capture Raw Data

Check frequency in gqrx and record with a hackrf:

hackrf_transfer -r 433995700.raw -f 433995700

6. Home Devices - Doorbells

4) Replay without remote

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

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

Questions