hackrf sdr meets +613

Playing in Melbourne ISM with SDR

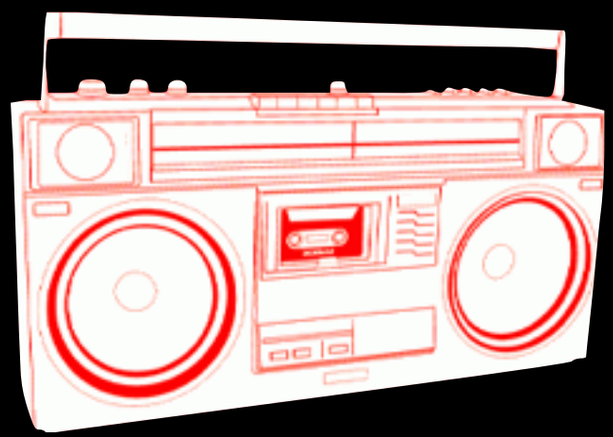
About us

- Neal “@y011” Wise
- Liam “@liamosaur” O

About presentation

- We backed HackRF on Kickstarter
  - Got two hackrf's as a result
- We tried to a lot (too much? meh…)
- There's so much to look at and too many good ideas
  - here are some of them

Quick SDR primer



plus

~=

hardware

software

SDRs I - Ham radio stuff

- Icom, KINETIC SBS*, Elecraft, FlexRadio, Soft Rocks boards (audio output) & others
- Many of these focus on ham radio bands

- Many of these implement ham-y stuff for DX*
- 2M, 10M, 20M, 40M, 80M etc.
- CW, etc. Used just like traditional ham radio rigs
- See awesome www.websdr.org
  (see you in a few hours)

SDRs II - "hacker friendly" stuff

- Ettus USRPs - Network & USB
- E4000/R820U DVB-T tuners - USB
- BladeRF - USB
- HackRF - USB
- Funcube - USB

Comparing SDR

device	Freq supported	Detail / Price in USD
Ettus USRPs	70MHz - 6GHz	- Network & USB / Badass / Expensive
RTL2832U	24MHz-1.7GHz	DVB-T tuners - “drifty” - E4000/ R820T - $10-$200
BladeRF	300MHz - 3.8GHz	full-duplex 28MHz, USB3, 2x2 MIMO ant. - $420 / FPGA model $615
HackRF	10MHz-6GHz	half-duplex 20MHz - $300

What's a HackRF

- Completely open sourced SDR
  - hardware
  - firmware
  - software and libraries
  - www.greatscottgadgets.com

HackRF

- why is this better than $20 RTL SDR or is it “as good” as ~$1k USD+ USRPs
- 10MHz*-6GHz
- up to 20MHz of bandwidth
- up to 20MHz sample rate

ASSURANCE

Hardware

SDR peripherals

Computer-controllable Scanners and other radios with audio output*

+

Software

libraries like
-librtlsdr
-libhackrf

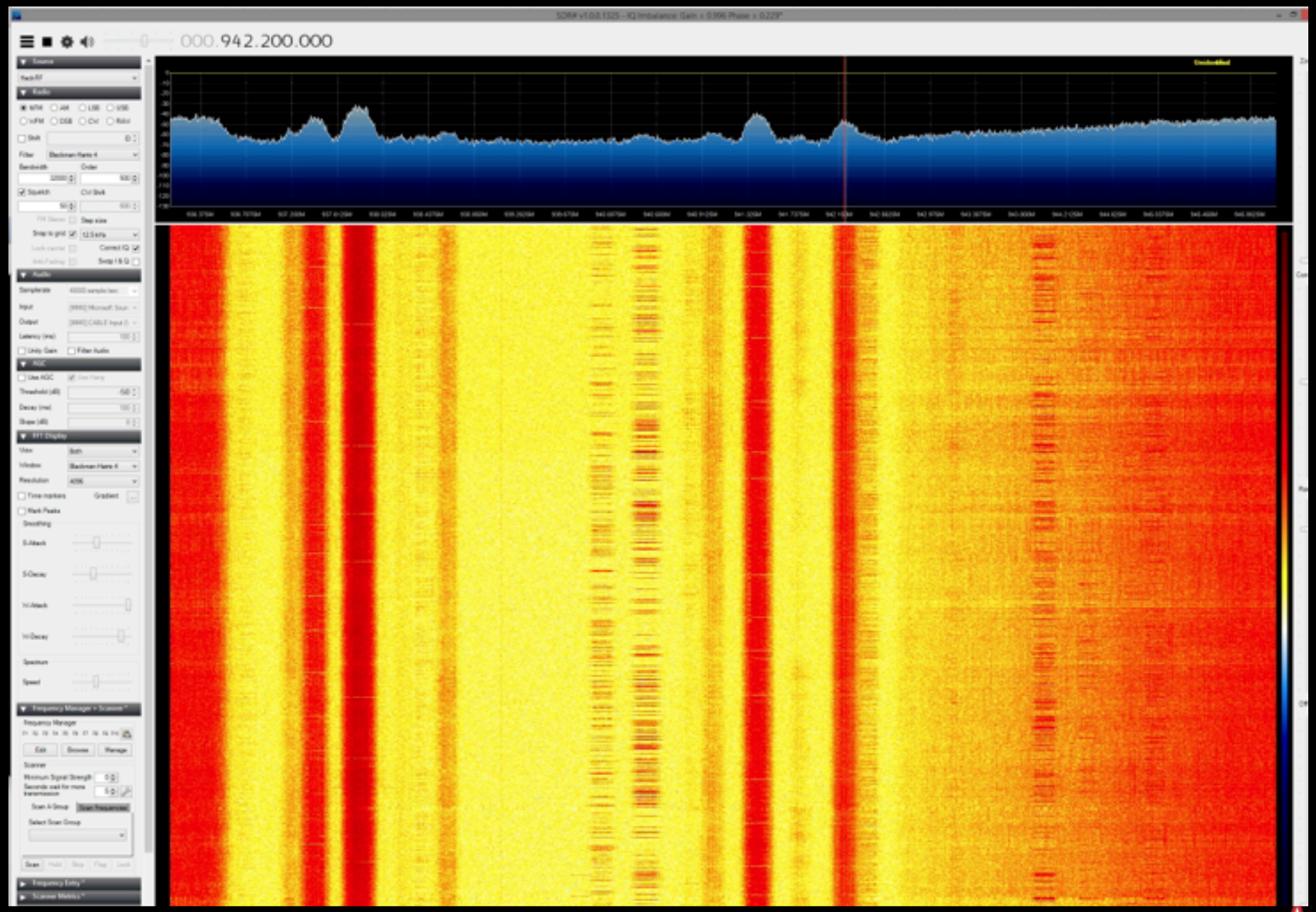
gnuradio

Front end radio console applications

=

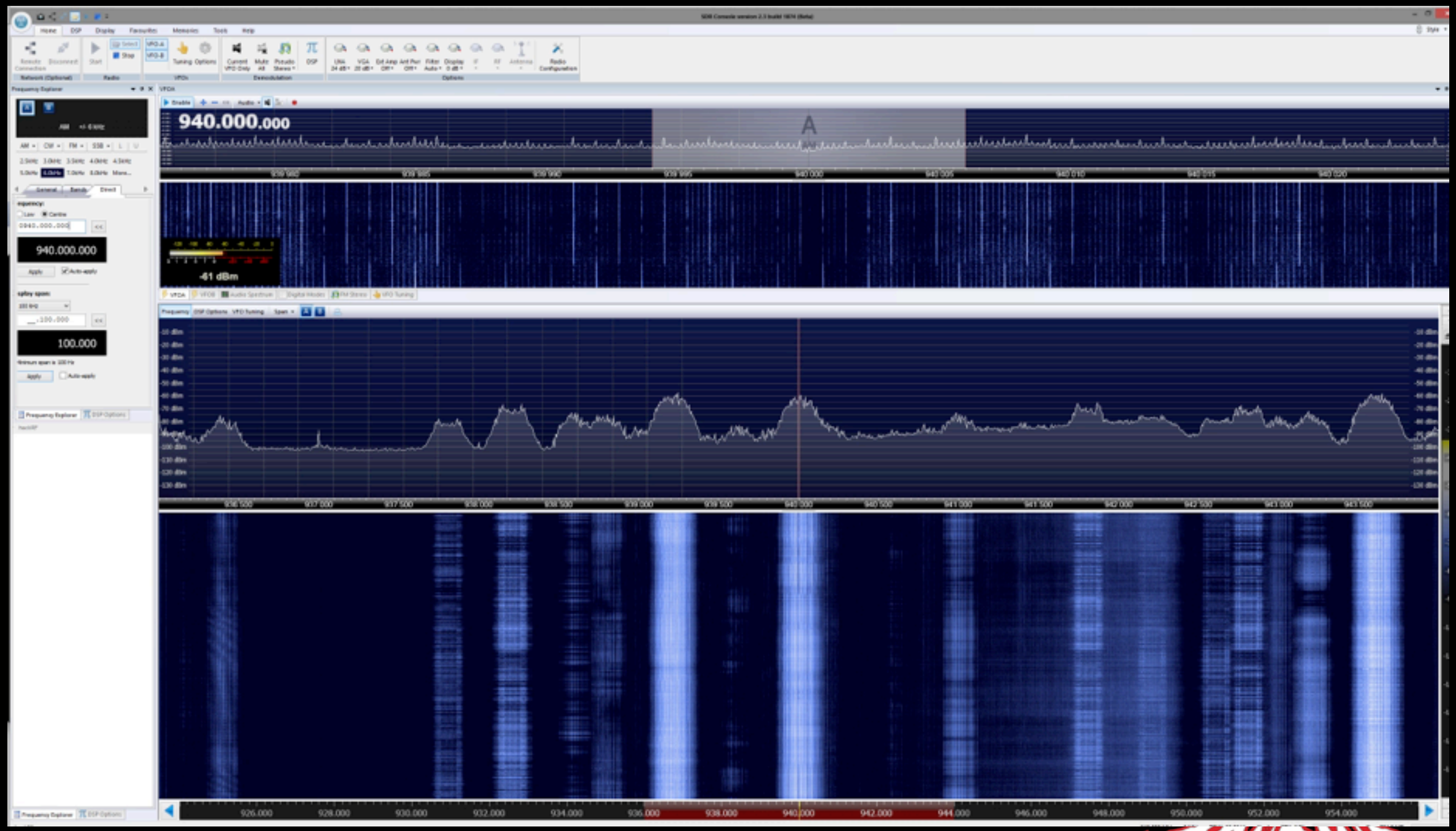
analog and digital voice, video & data

SDR front ends - SDR#



This was a presented video

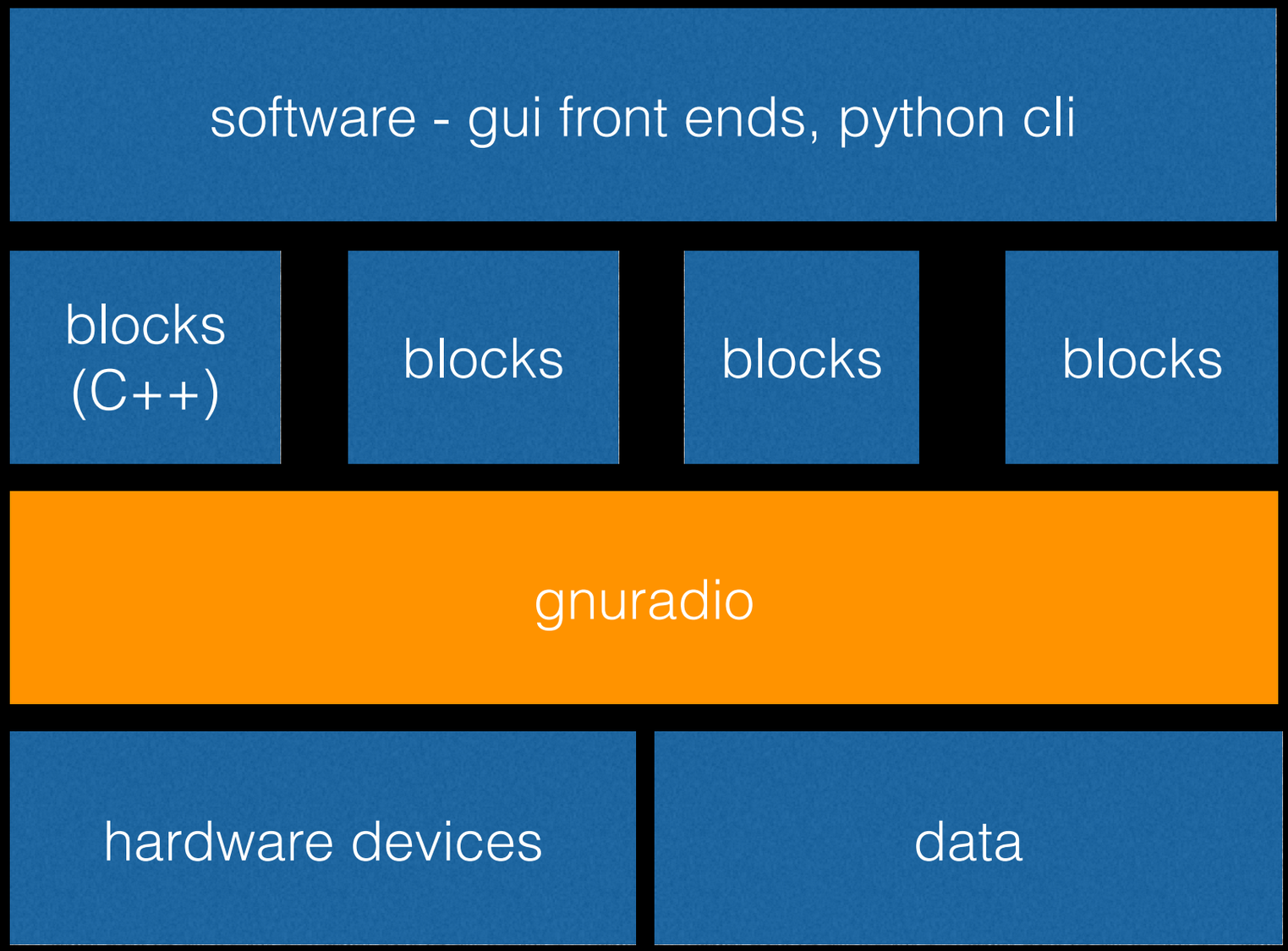
SDR Console



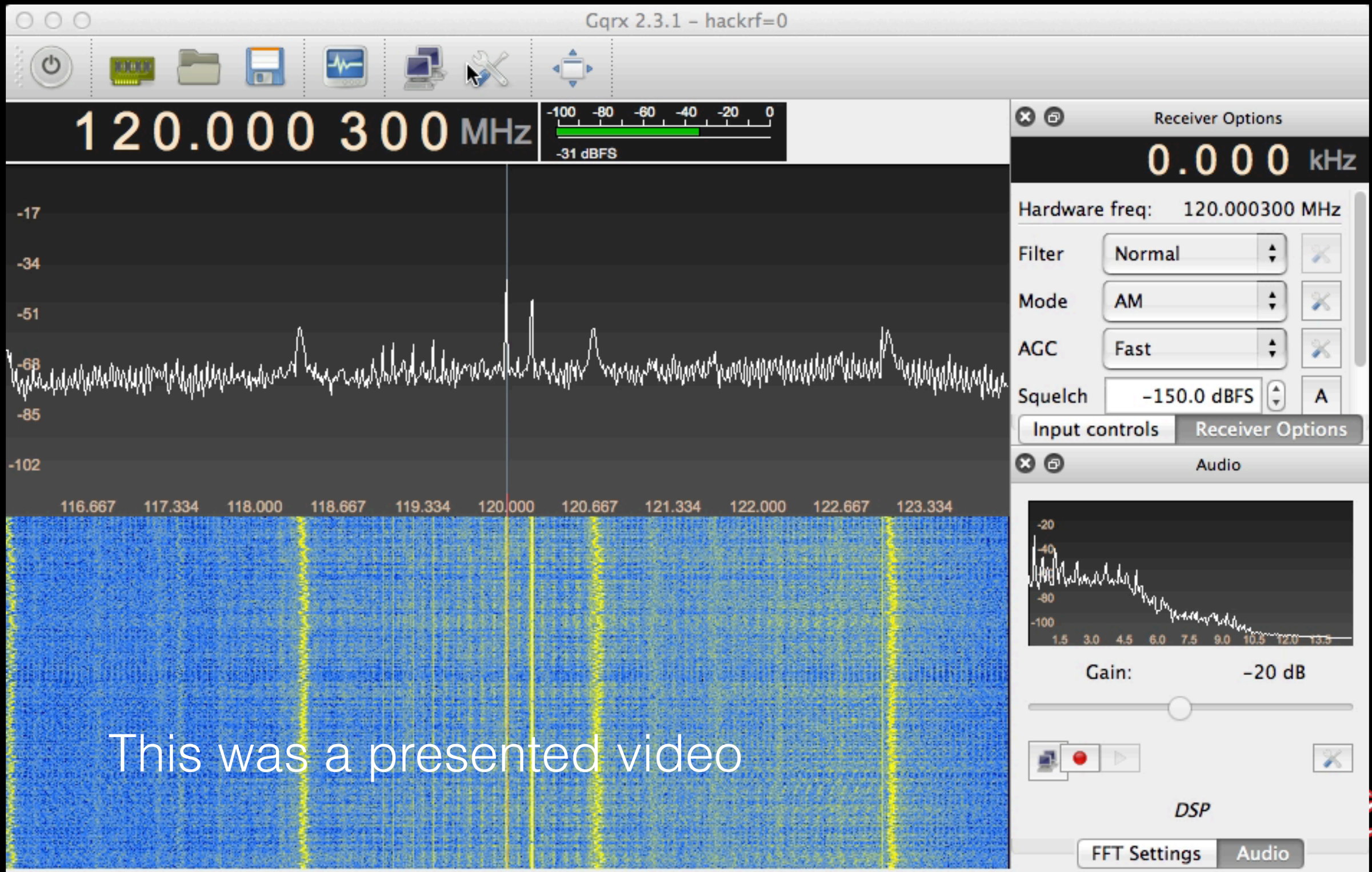
This was a presented video

ASSURANCE

An idiots* view of gnu radio



gqrx - “hello world” of SDR



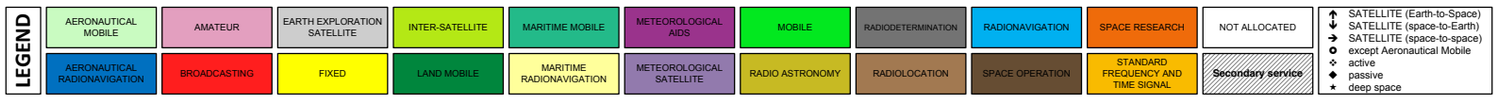
What's out there to be seen

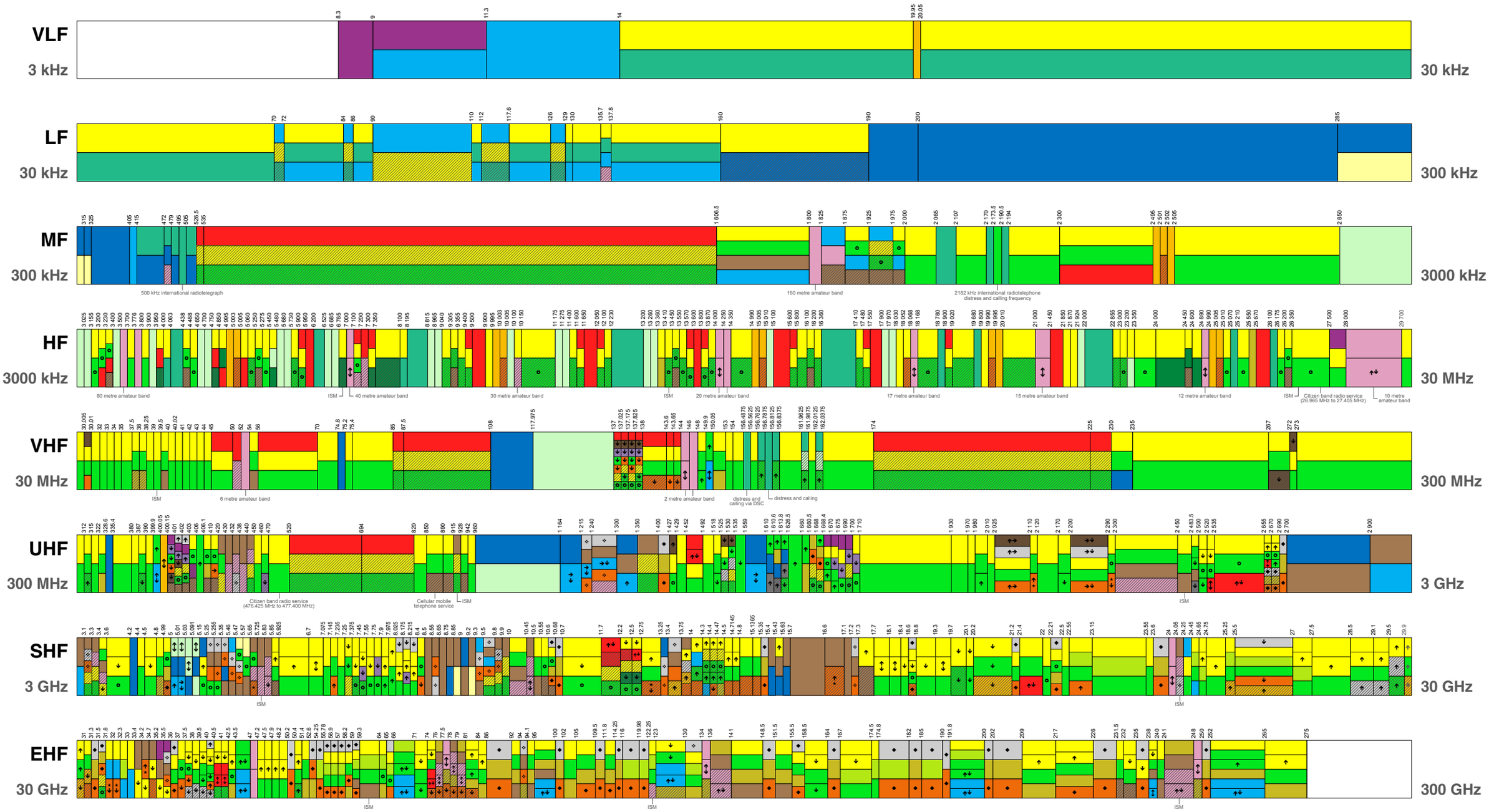
Australian radiofrequency spectrum

allocations chart

Australian Government

acma
Australian Communications and Media Authority





Demo

FM and AM modulated voice with gqrx

(these were local services
and the conference wireless mic)

Plane & Airport Stuff

- Airport - ATIS
- Planes - ADS-B / ACARS etc

ASSURANCE

Essendon Airport

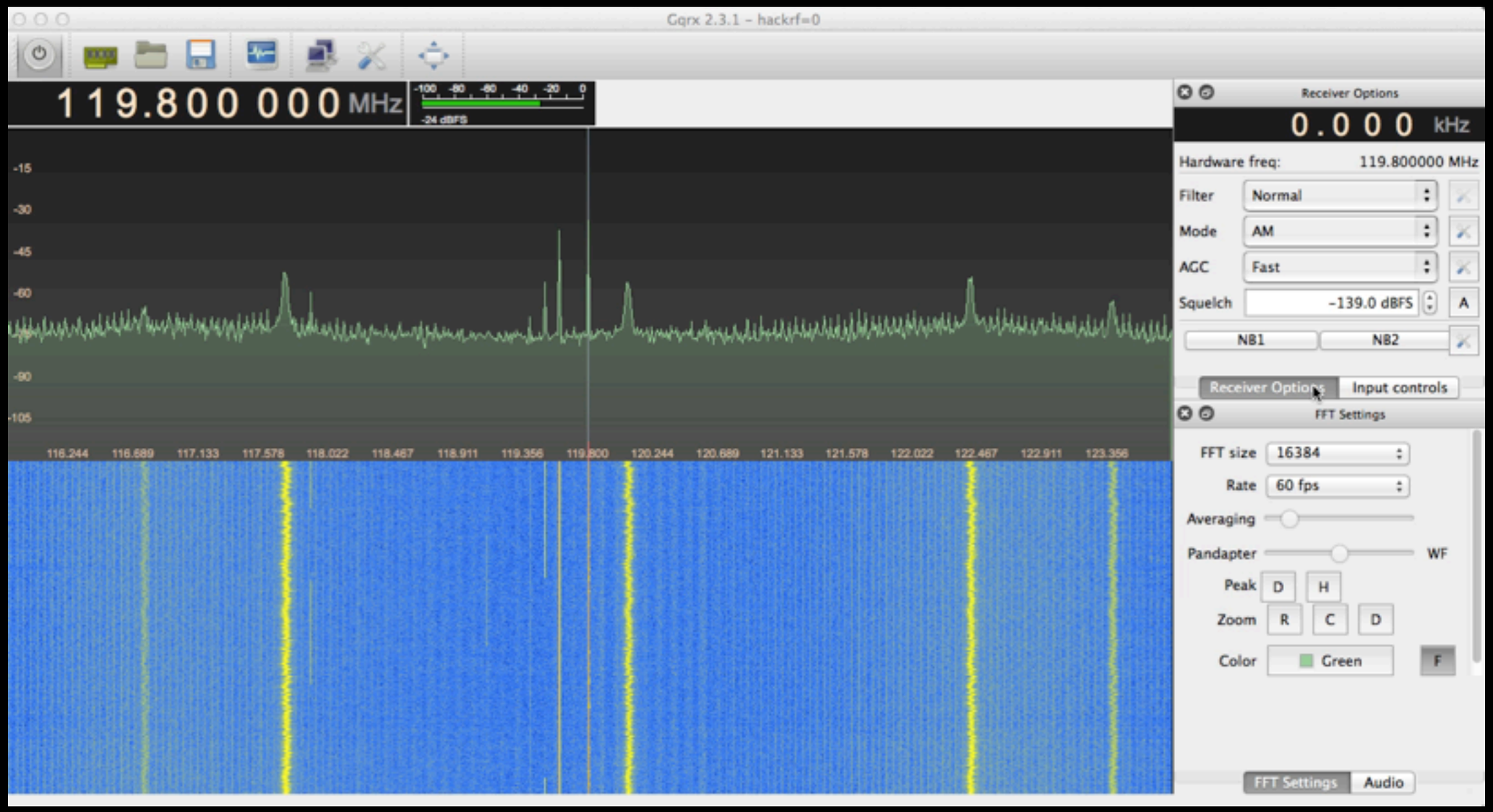
IATA: MEB ICAO: YMEN

What Freq/Mod	What is it
119.800 MHz AM	ATIS Essendon terminal information airport status and time in “zulu”
124.1 MHz AM	PAL
118.455 MHz AM	clearance delivery to startup for departure
135.7 MHz AM	inbound airways clearance

Are We Not YMEN?

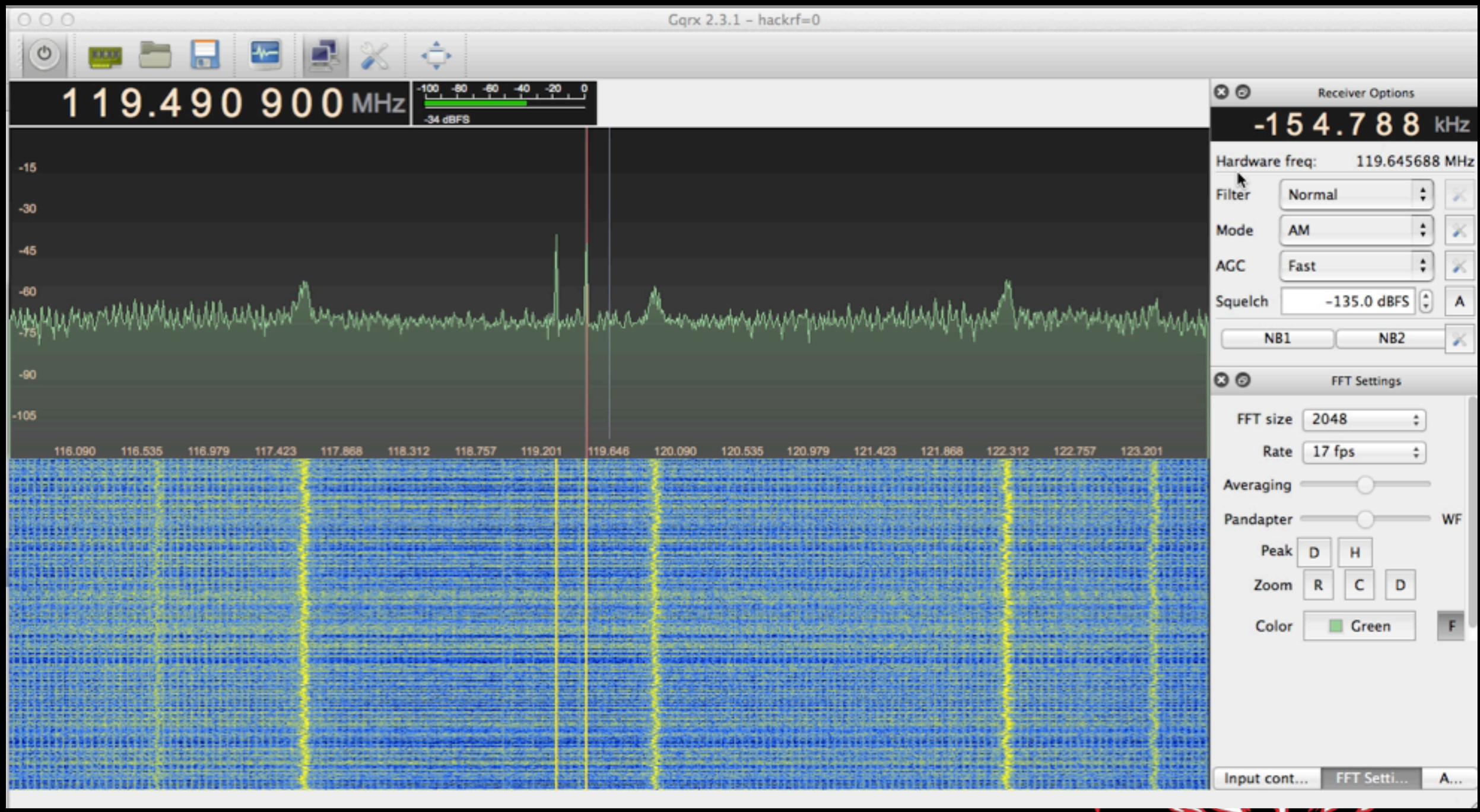
Essendon ATIS today

119.8 MHz



This was a presented video

Essendon ATIS - storms



Planes ADS-B Demo

ADS-B 1090MHz

ACARS 130.550MHz

[BEGIN_MESSAGE]----------

RX_IDX: 1
CRC: Correct
Timestamp: 25/09/2014 10:14
ACARS mode: M
Message label: H1 (Message to/from terminal)
Aircraft reg: .VH-VNG, flight id: TT0221
Aircraft: Airbus A320-232
Registration: VH-VNG
Mode-S ID: 7C6C2A
Airline: Tiger Airways Australia

Block id: 53, msg. no: D02A
Source: Digital Flight Data Acquisition Unit
Message content:-
#DFBA02/A32002,1,1/CCVH-VNG,SEP24,234353,YSSY,YMML,0221/
C106,77801,5000,43,0010,0,0100,42,X/CEN176,36007,258,779,6246,325,I21002/
CNN177,36031,258,780,6246,325/EC012741,19381,11387,73,38,38/EE013064,01892,01044,

[END_MESSAGE]----------

ACARS (rtl… cheating)

Cocoa1090

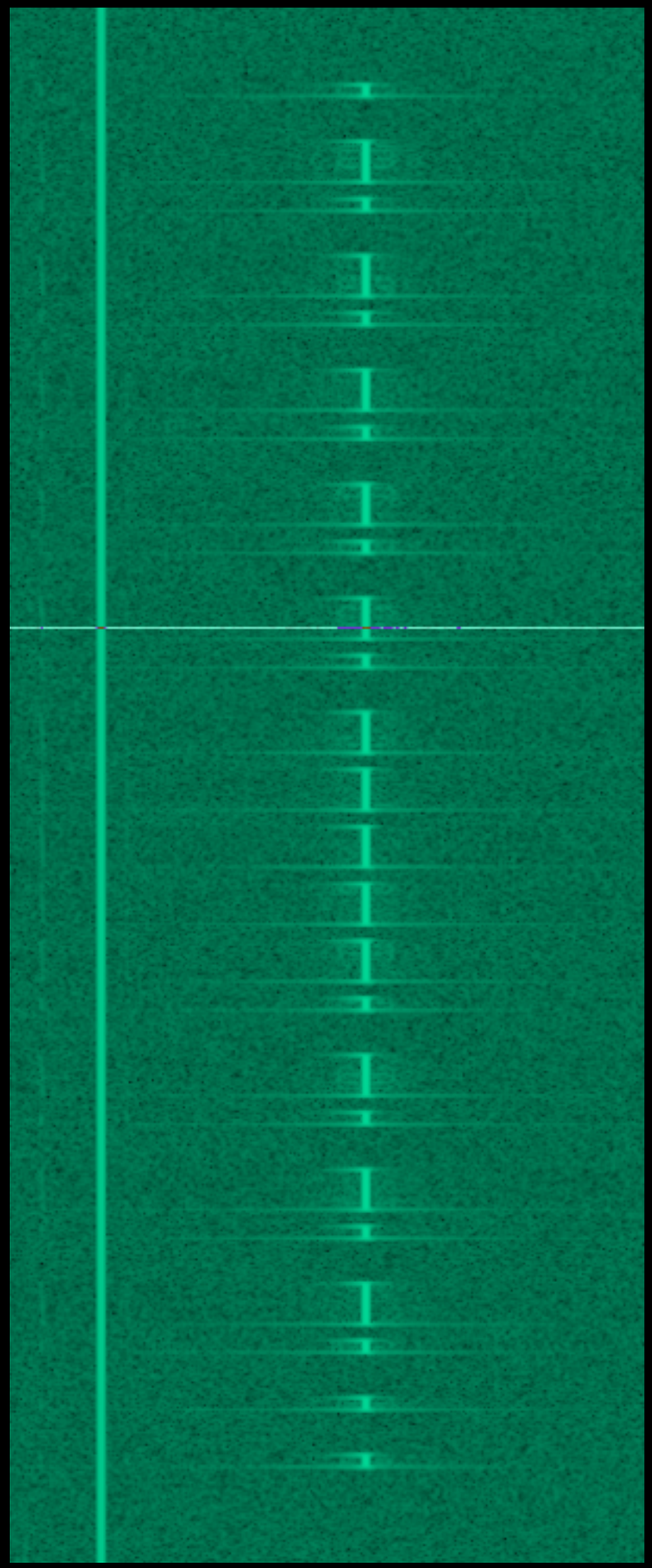
ICAO	TAIL	FLIGHT	ALTITUDE	SPEED	LAT	LON	TRACK	MESSAGES	SEEN	PLANE
8a03c2	-		33425	0	0	0	0	1	62	-
7501e9	-	XAX215	275	0	0	0	0	55	1	-
7c77f9	-	QFA609	11975	251	322.994	-39.2981	170	97	34	-
7c6b40	-	????????	275	0	0	0	0	10	75	-
7c6db8	-	QFA702	0	0	0	0	0	30	1	-
7c6d2c	-	VOZ816	6725	271	322.556	-21.937	272	362	1	-
7c8021	-	RXA3557	300	0	0	0	0	117	5	-
7c6c55	-	VOZ733	275	0	0	0	0	41	5	-
888081	-		0	0	0	0	0	2	9	-
7c801c	-	RXA3152	15025	295	322.857	-11.2857	51	51	67	-
7c6d93	-	QFA477	4625	211	322.544	-177.141	260	1033	0	-
7c6de8	-	QFA610	275	0	0	0	0	133	1	-
8a03c0	-	GIA717	275	0	0	0	0	99	1	-
7c6d28	-	VOZ319	5600	278	322.368	175.608	329	1302	1	-
7c6ddf	-	QFA674	250	122	322.34	-32.6981	171	1339	1	-
7c6de7	-	QFA796	300	0	0	0	0	95	0	-
7c5323	-	QFA29	275	0	0	0	0	110	1	-
7c6c52	-	VOZ1507	250	0	0	0	0	83	32	-
7c80fb	-	RXA3258	11125	218	322.561	-175.402	63	1166	7	-
7c6d2a	-	VOZ1291	11375	356	322.542	-38.6444	33	1443	0	-
7c6d7b	-	JST700	300	0	0	0	0	441	3	-
7c7746	-	TGW511	275	129	322.341	-177.545	171	421	28	-
7c6b35	-	JST612	28275	469	322.833	-145.511	52	621	31	-

Preamble: 17683 Demod: 138 Good CRC: 17 Bad CRC: 121 Fixed: 2 2 0 Frames/sec: 19 Fix 2

Demos - 433MHz

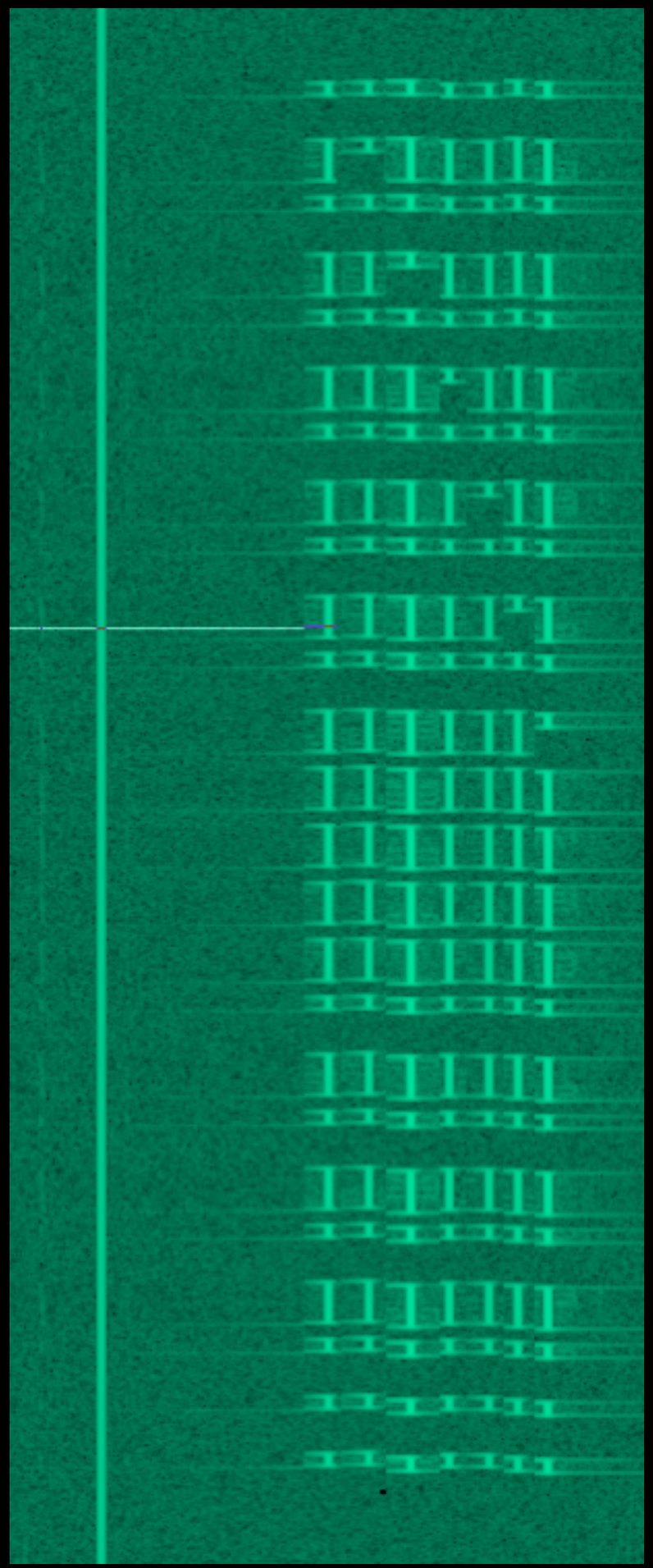
- 433MHz is way fun
- hackrf_transfer capture / playback

baudline



more doorbell

baudline redux



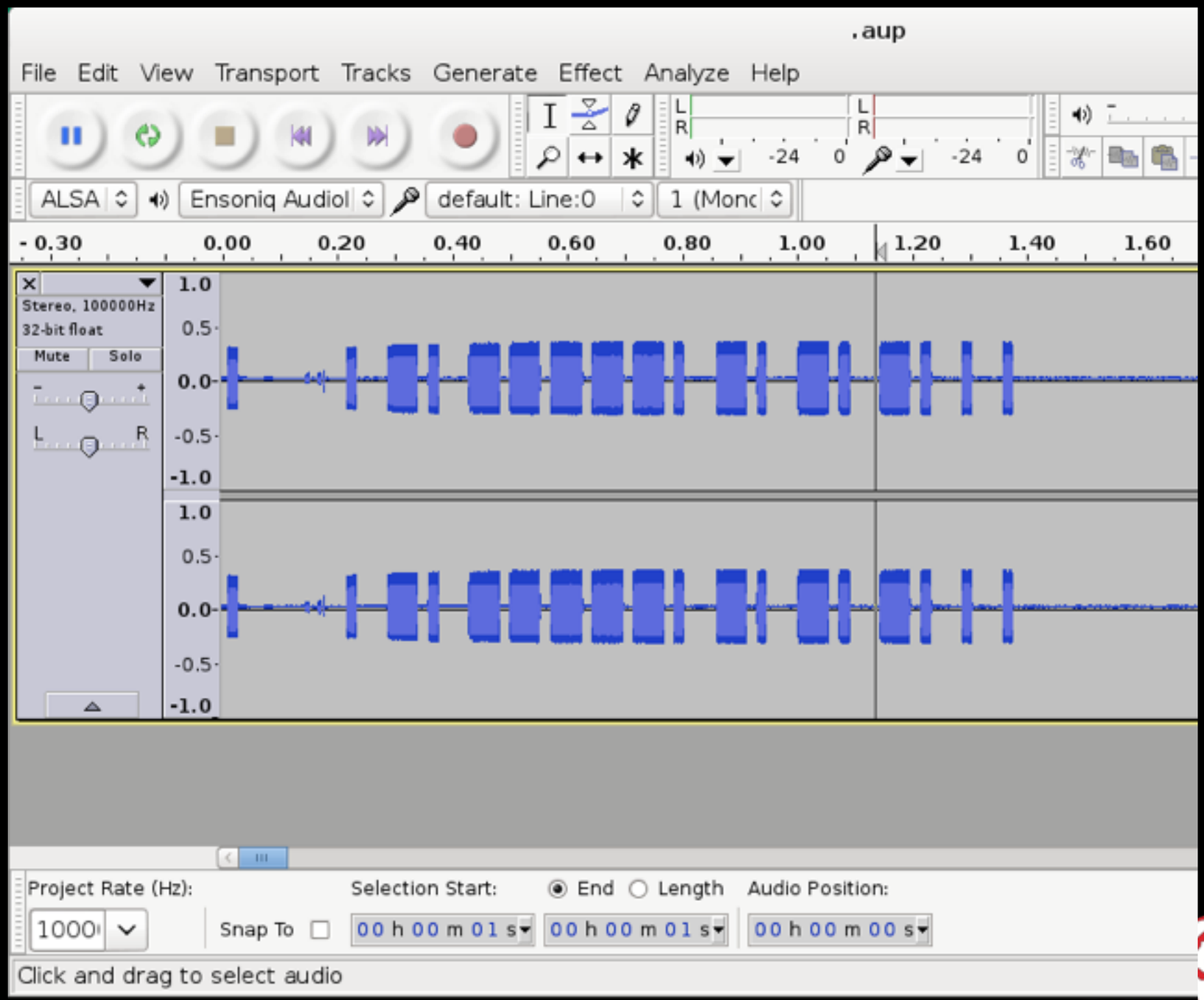
knick knocking 2014

ASSURANCE

the Right Way

- Pulse Width Demodulation to binary
- Generate binary codes for each possible dip switch combination
- Modulate codes onto carrier signal and transmit

the ~~Wrong~~ MAX POWER way



the ~~Wrong~~ MAX POWER.py way

```
output = open('output', 'wb')
repeatLimit = 6
for pattern in range(0, 64):
    for repeat in range(0, repeatLimit):
        shutil.copyfileobj(open('gap.raw','rb'), output)
        bitmask = 1
        while bitmask < 64:
            if pattern & bitmask:
                shutil.copyfileobj(open('one.raw','rb'), output)
            else:
                shutil.copyfileobj(open('zero.raw','rb'), output)
            bitmask = bitmask << 1
        shutil.copyfileobj(open('postamble.raw','rb'), output)
output.close()
```

Junk Demo

I got a fever, and the only prescription is more doorbell

Stuff we're working on

- Digital radio - gr-dsd, dsd.exe/ dsdplus.exe + SDR Console / SDR#
- Trunk radio systems - P25 (Hello Moto) & MPT 1327 (…)
- TramTracker and transport radio data
- Oh yeah and…

ASSURANCE

REDACTED

sorry this was research in
progress that we'll be continuing
(aka you should've been there…)

Securing radios?

- Gah… what do you mean?
- Spread Spectrum (Frequency Hopping etc) - Security through obscurity?
- For example some trunk radio systems in use use encryption

Questions?

Thanks!

- Thanks Chris, Marta & Ruxcon Crew!
- Greetz dr0nely, cynasty, snare, corrupt, wily, deathflu, ap613, boz0, codeine; dnoiz, #kiwicon & #ducksec crew _o<
- 9AM Tomorrow, get your hungover heads to see Dr Silvio