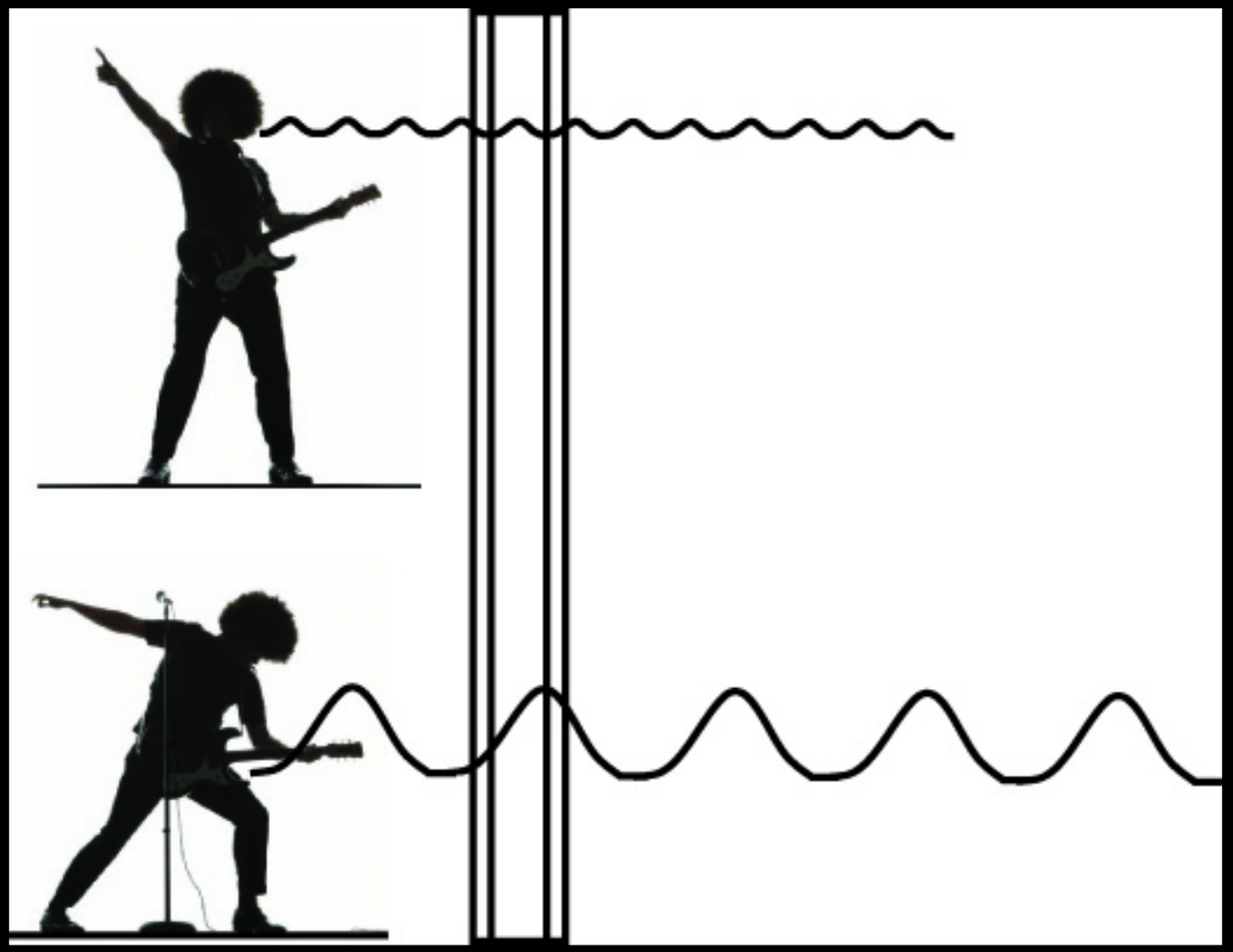
DC423 SDR Basics

My Antenna has more gain

@tothehilt && @synackpwn

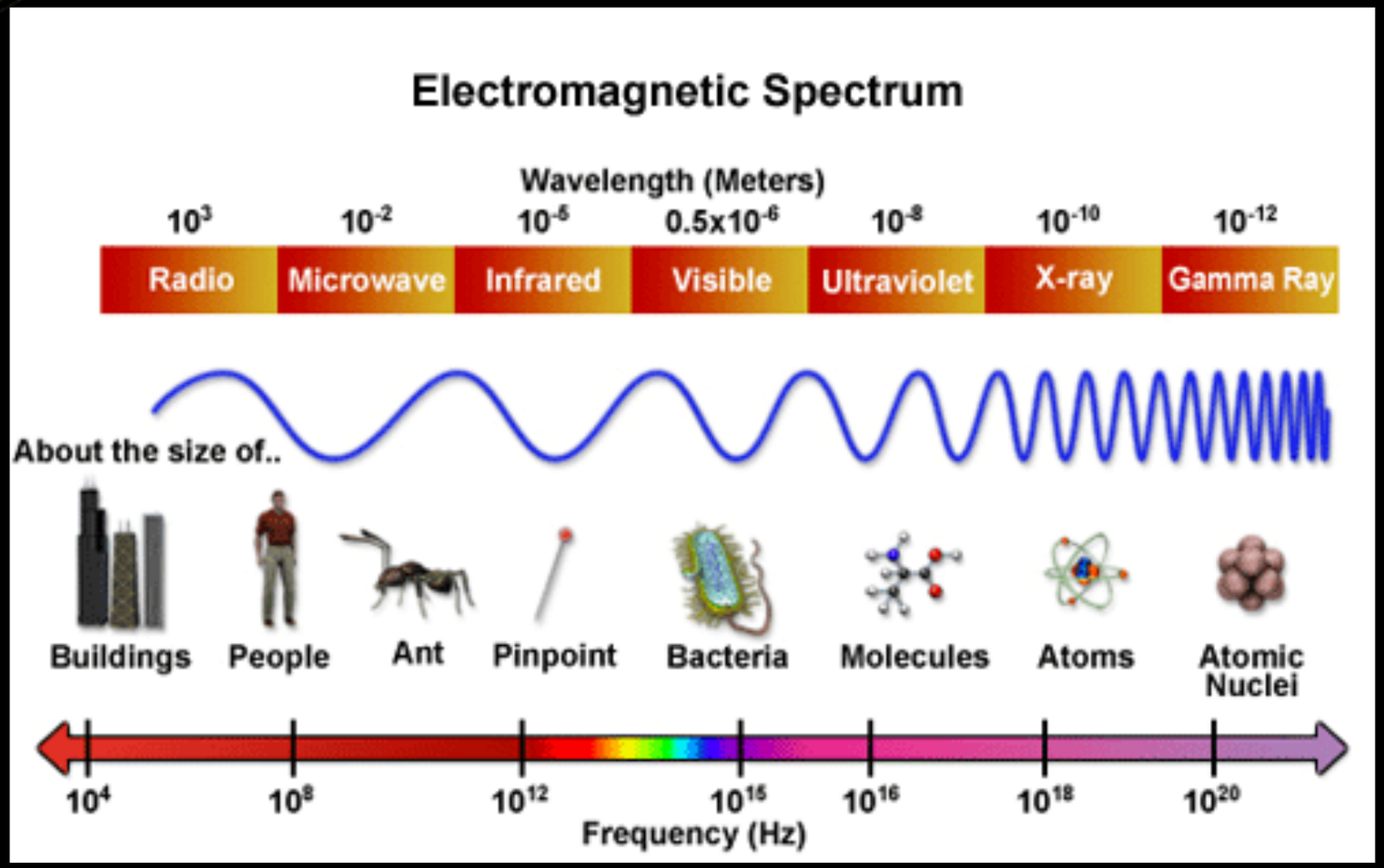
Sound Waves



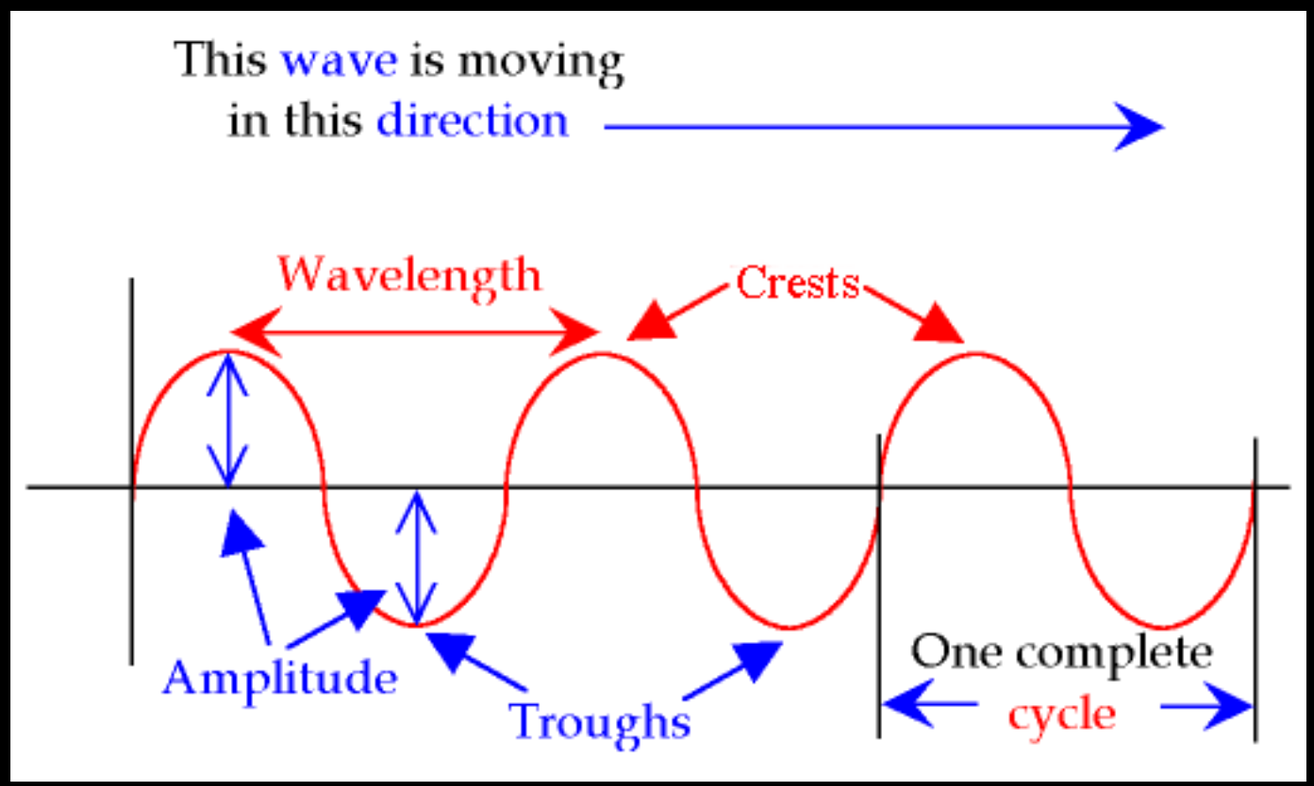
Radio Waves

- Radio Waves
- Electricity flowing into the transmitter antenna makes electrons vibrate up and down it, producing radio waves.
- The radio waves travel through the air at the speed of light.
- When the waves arrive at the receiver antenna, they make electrons vibrate inside it. This produces an electric current that recreates the original signal.

Radio Waves


Electromagnetic Spectrum
Wavelength (Meters)
10^3
10^-2
10^-5
0.5x10^-6
10^-8
10^-10
10^-12
Radio
Microwave
Infrared
Visible
Ultraviolet
X-ray
Gamma Ray
About the size of..
Buildings
People
Ant
Pinpoint
Bacteria
Molecules
Atoms
Atomic Nuclei
10^4
10^8
10^12
10^15
10^16
10^18
10^20
Frequency (Hz)

Radio Waves

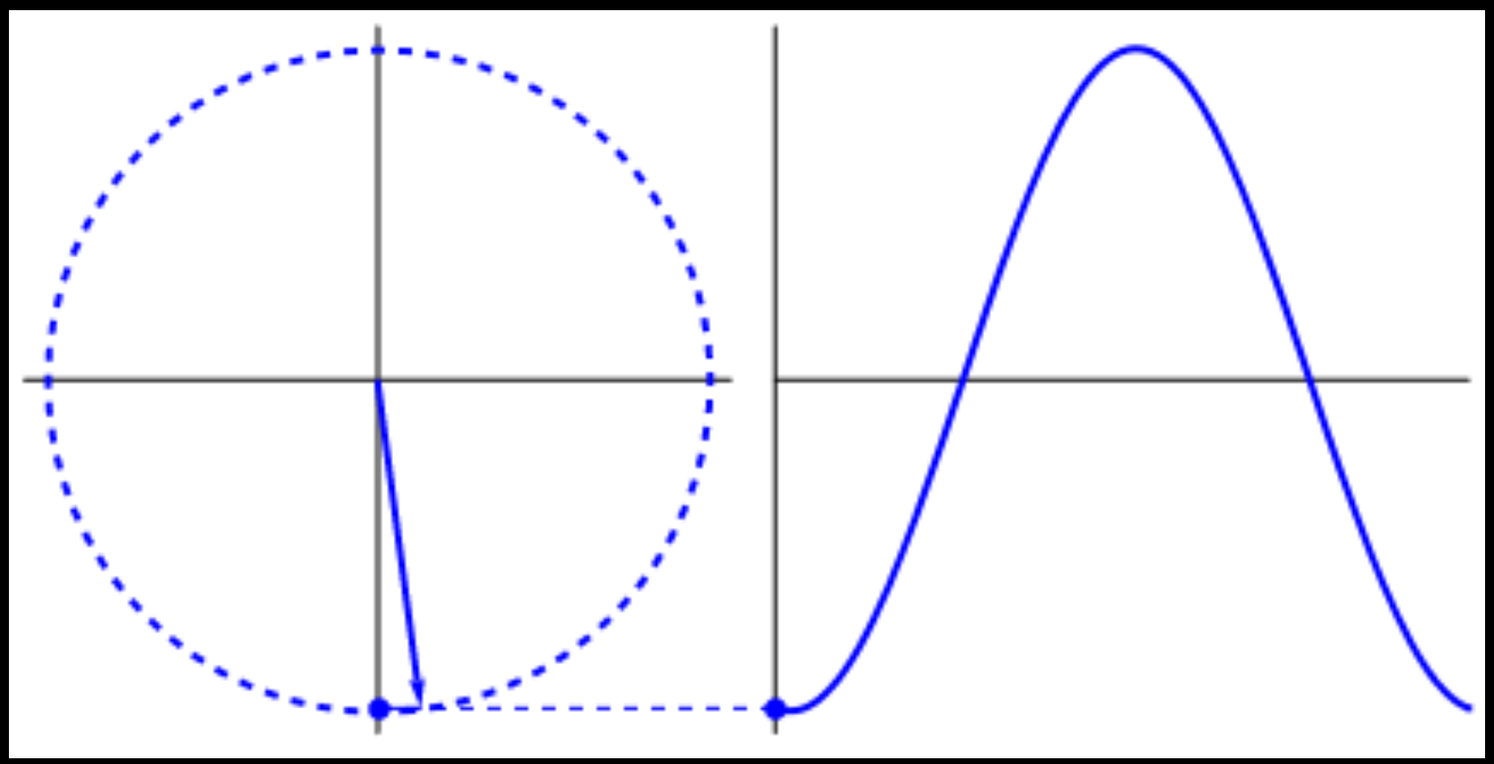

This wave is moving
in this direction
Wavelength
Crests
Amplitude
Troughs
One complete
cycle

$$v = f \lambda$$

- Frequency tells us how many waves are passing a point per second, the inverse of time.
- Wavelength tells us the length of those waves in metres, almost like a displacement.
- If we multiply these two together, we are really multiplying 1/s and m… which gives us m/s, the velocity of the wave!

v = velocity of the wave (m/s)
f = frequency (Hz)
λ = wavelength (m)
$v = f \lambda$

$$v = f \lambda$$



$$v = f \lambda$$

- MATH SO HARD MY HEAD HURTS
  - If 105.5 MHz is our local rock station, assuming we are in a vacuum how many feet is the wavelength
  - (Everyone look at @melangeabuser for the Answer)

$$v = f \lambda$$

- MATH SO HARD MY HEAD HURTS
  - m = 300000000/105500000
  - ~ 9.3 Feet (2.8 Meters)

SDR

- Dafuq is it?
- Why should I care?
- But Isn’t that illegal?

SDR

- Dafuq is it?
- Software-defined radio (SDR) is a radio communication system where components that have been typically implemented in hardware (e.g. mixers, filters, amplifiers, modulators/demodulators, detectors, etc.) are instead implemented by means of software on a personal computer or embedded system. While the concept of SDR is not new, the rapidly evolving capabilities of digital electronics render practical many processes which used to be only theoretically possible. (sauce wikipedia)

SDR

- Why should I care?
  - Because its super cool and everyone will be jealous of you.

SDR

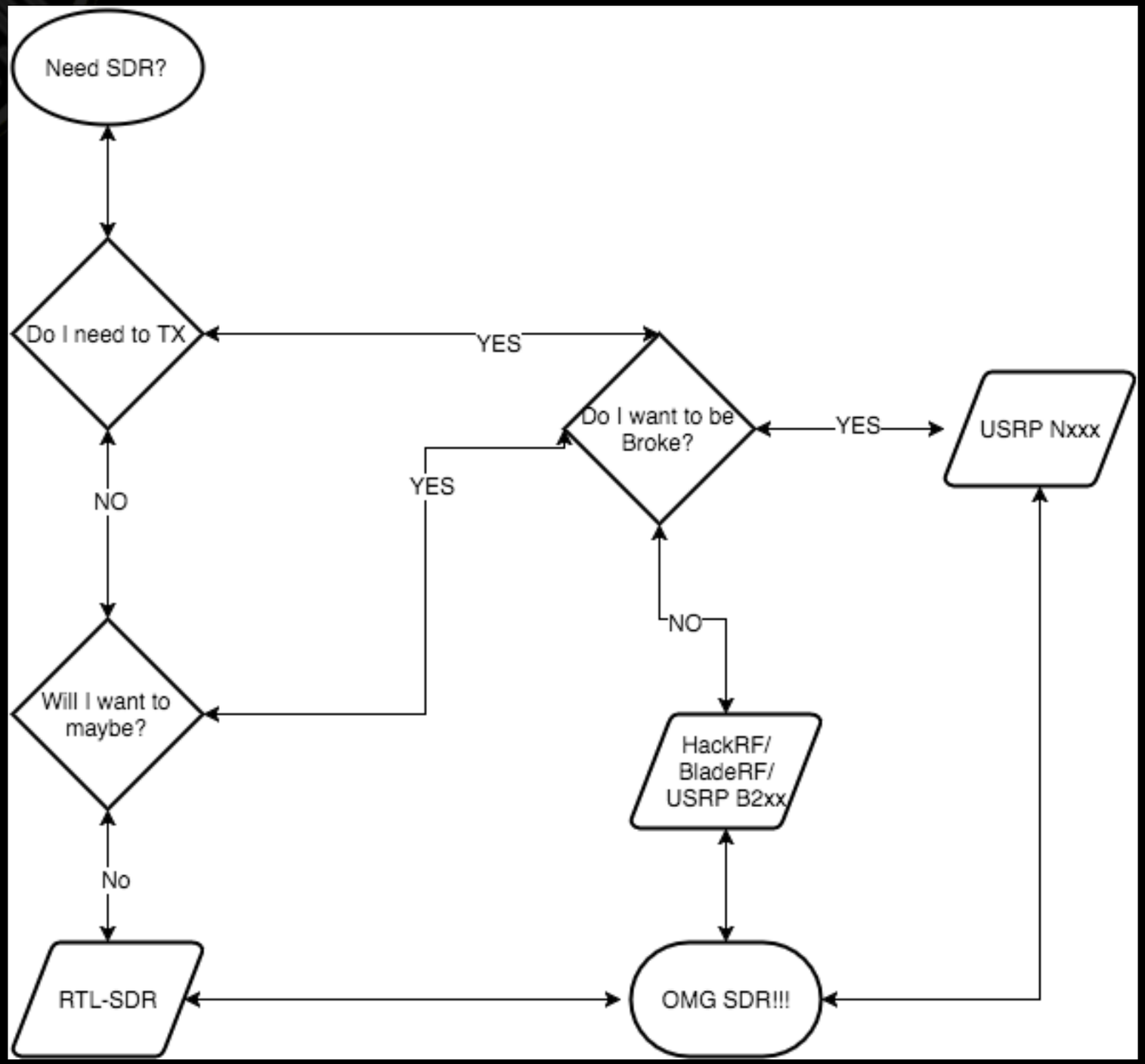
- But isn’t that illegal?
  - Well that depends. Really…

But What do I need?

- A SDR Device.
  - RTL-SDR
  - HackRF
  - BladeRF
  - USRP
- Some SDR Software
  - SDR# - Windows
  - HDSDR - Windows or Wine
  - GQRX - *nix
- A lot of time to kill with GNURadio
  - Seriously a lot of time because this is still a pain to deal with if you want to go past just watching and listening to basics.

But What do I need?

But What do I need?



What to do with SDR

What to do with SDR

What to do with SDR

What to do with SDR

What to do with SDR

What to do with SDR

Who can SDR?

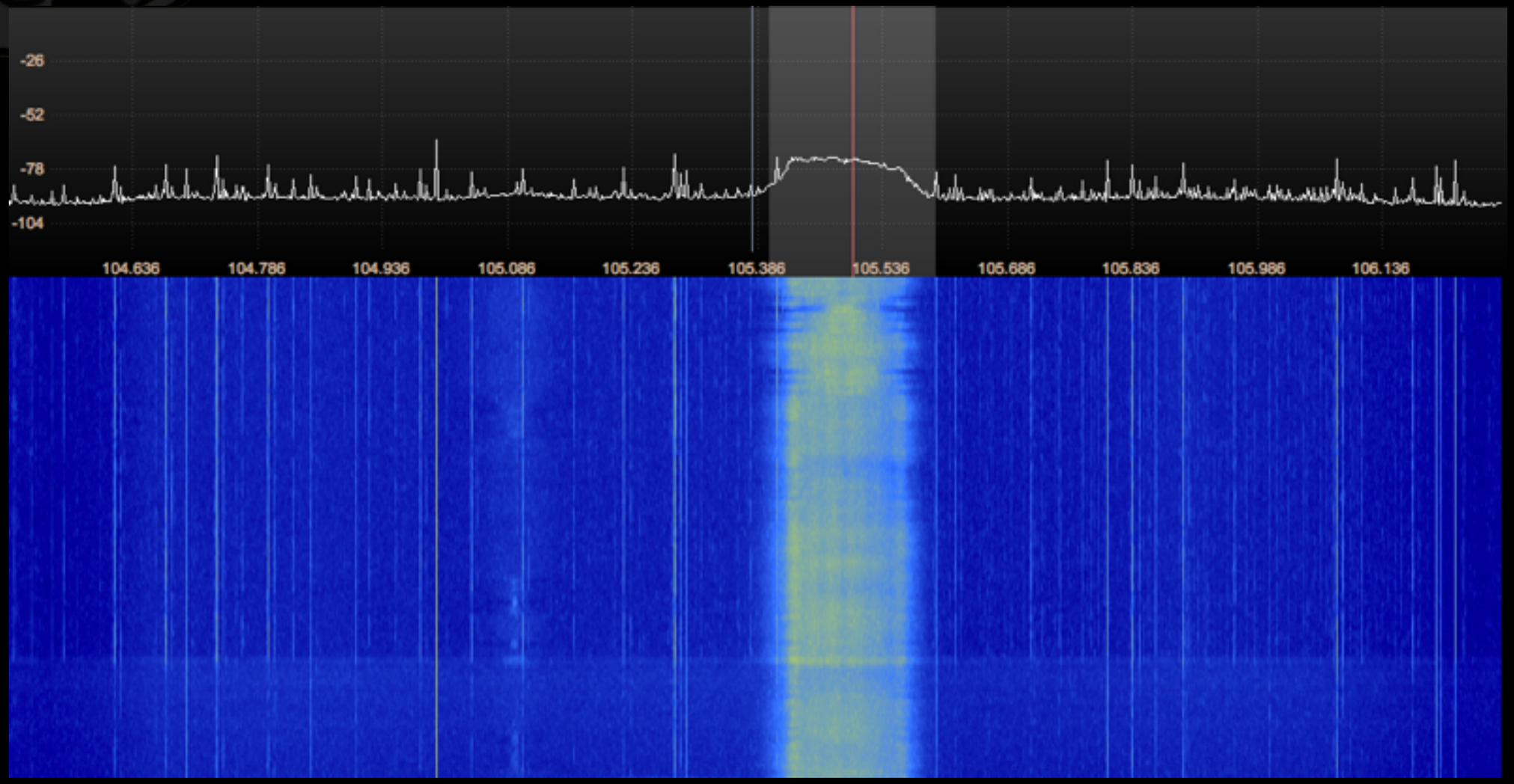
Anyone Can SDR

- BUT WITH ALL THIS WHERE DO I START?!?!

Listen to FM Radio

- Why?
- No boom box required.
- Makes you feel cool and can impress friends.
- Can even listen on bands that your silly boombox wouldn’t tune to.

Listen to FM Radio



Listen to FM Radio

DEMO TIME!!!!!!111ONE!!

Use:

http://gqrx.dk/

http://airspy.com/download/

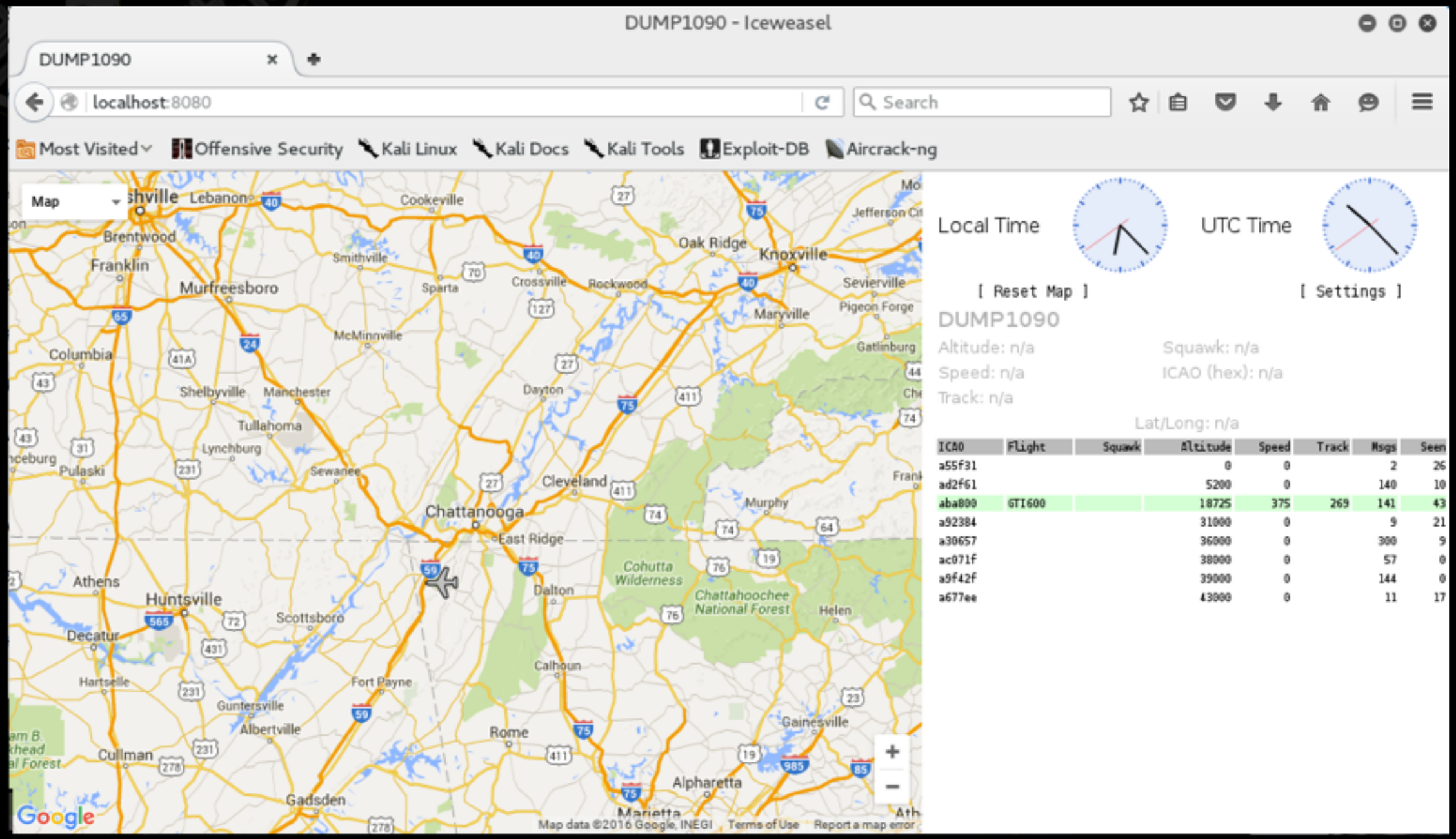
Fly It Sideways

- Why?
- Prove @sidragon1 is full of shit
- Cooler than listening to FM Radio
- Can wow your friends about how awesome you are at tracking planes.

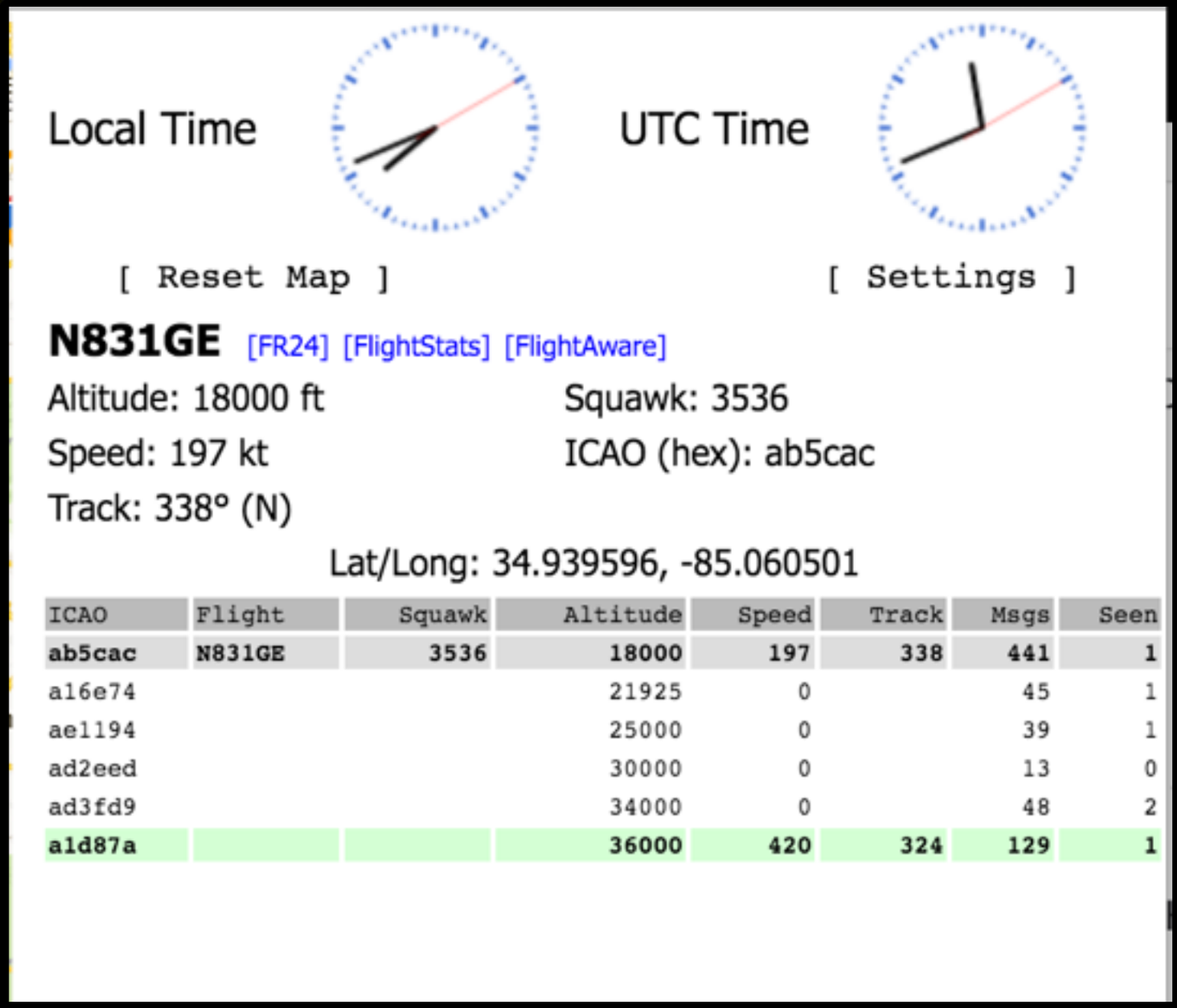
Fly it Sideways

```
Hex     Mode  Sqwk  Flight   Alt    Spd  Hdg    Lat      Long   Sig  Msgs   Ti|
-------------------------------------------------------------------------------
A915F3  S                    26600                              10    21    1
A677EE  S     1440  N516CC   43000  451  345   34.996  -85.225   20   402    0
AC071F  S                    38025                               7   198    0
A92384  S                    31000  491  143                     8    46   17
```

Fly it Sideways



Fly it Sideways



ICAO	Flight	Squawk	Altitude	Speed	Track	Msgs	Seen
ab5cac	**N831GE**	**3536**	**18000**	**197**	**338**	**441**	**1**
a16e74			21925	0		45	1
ae1194			25000	0		39	1
ad2eed			30000	0		13	0
ad3fd9			34000	0		48	2
a1d87a			**36000**	**420**	**324**	**129**	**1**

Fly it Sideways

N831GE
(Track inbound flight)
GESE LLC · WILMINGTON DE (registration)

Fulton County (KFTY – info)	Chicago/Rockford Intl (KRFD – info)
Atlanta, GA	Chicago/Rockford, IL
07:13PM EDT	***09:15PM CDT***
Scheduled: 06:00PM EDT	Scheduled: 08:03PM CDT

Other flights between these airports

28 min | 2 hr 33 min

Duration: 3 hours

Sunday, April 3, 2016

Status	*En Route* (84 sm down; 549 sm to go) (track log & graph)
Aircraft	Beechcraft Baron (58) (twin-piston) (BE58/G – photos)
Speed	196 kts (planned: 210 kts) (graph)
Altitude	18,000 feet (planned: 18,000 feet) (graph)
Distance	Direct: 633 sm Planned: 637 sm
Route	NOONE GQO (Decode)

Get notified of this flight's activity →

ACTIVITY LOG

Want a full history search for N831GE dating back to 1998? Buy now. Get it within one hour.

Fly it Sideways

DEMO Goes Here

USE:

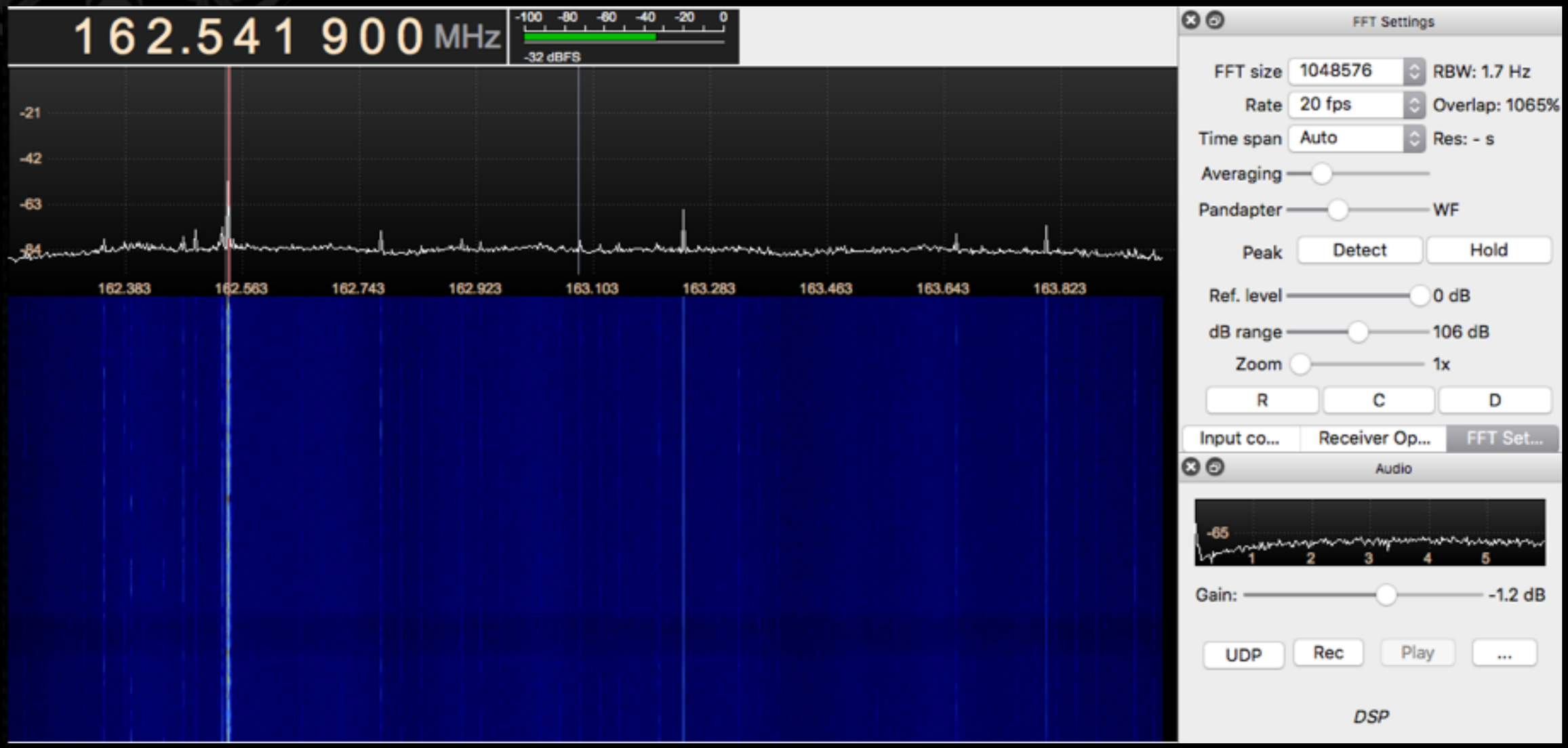
https://github.com/antirez/dump1090

In case of emergency

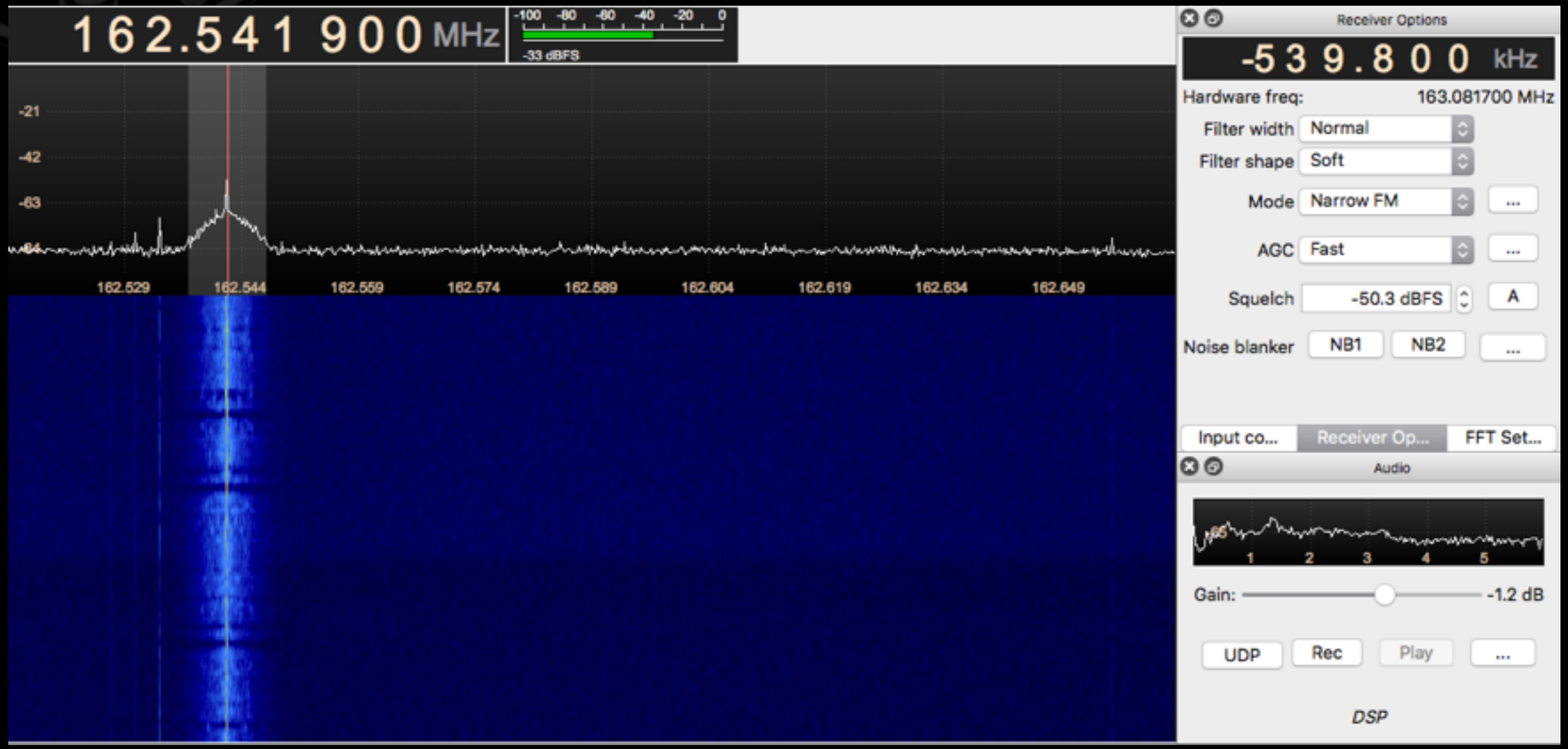
- Why?
- Weather Radios are $30+ dollars
- Hackers in closets already have their computers with them

In case of emergency

In case of emergency



In case of emergency



In case of emergency

DEMO Goes Here

Use:

http://gqrx.dk/

http://airspy.com/download/

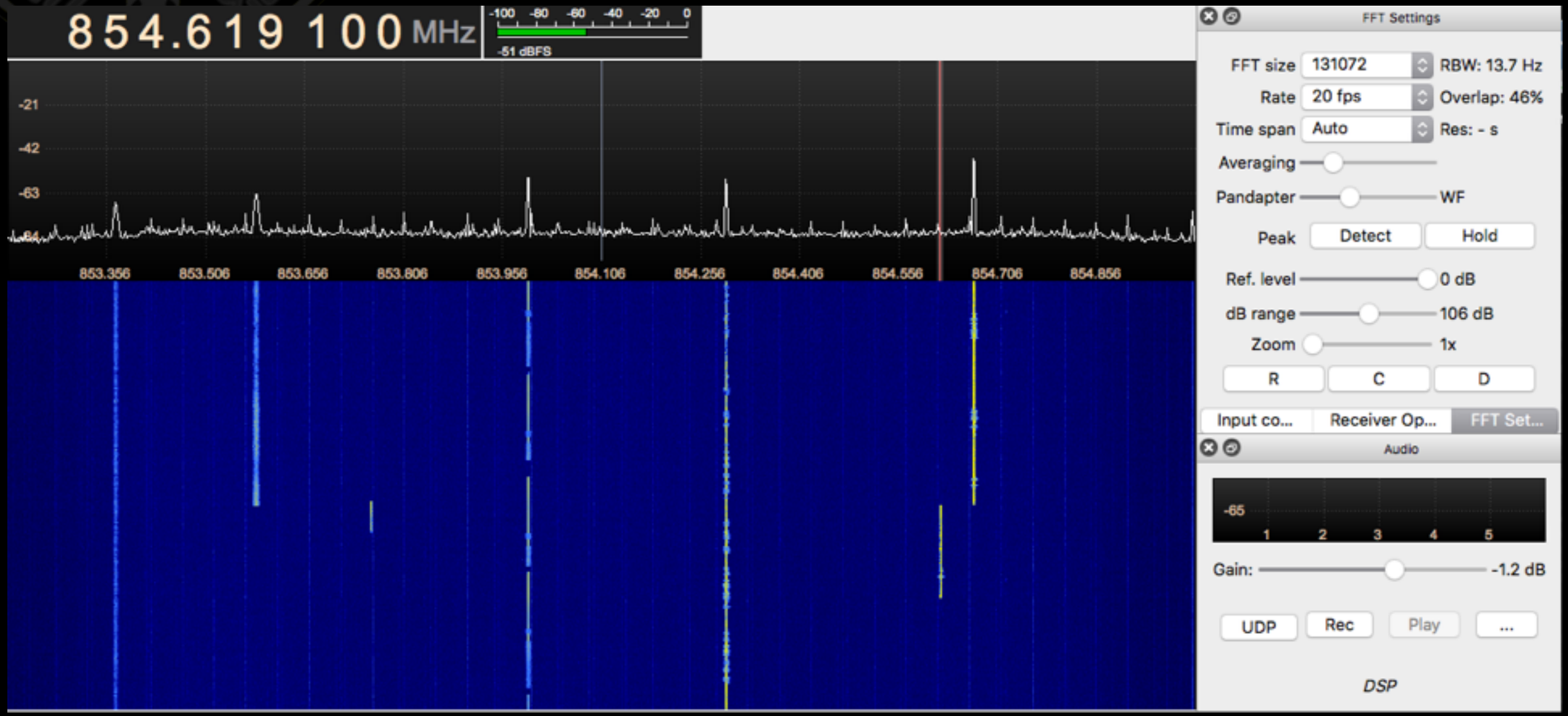
10-31 In Progress

- Why?
  - Ferguson…

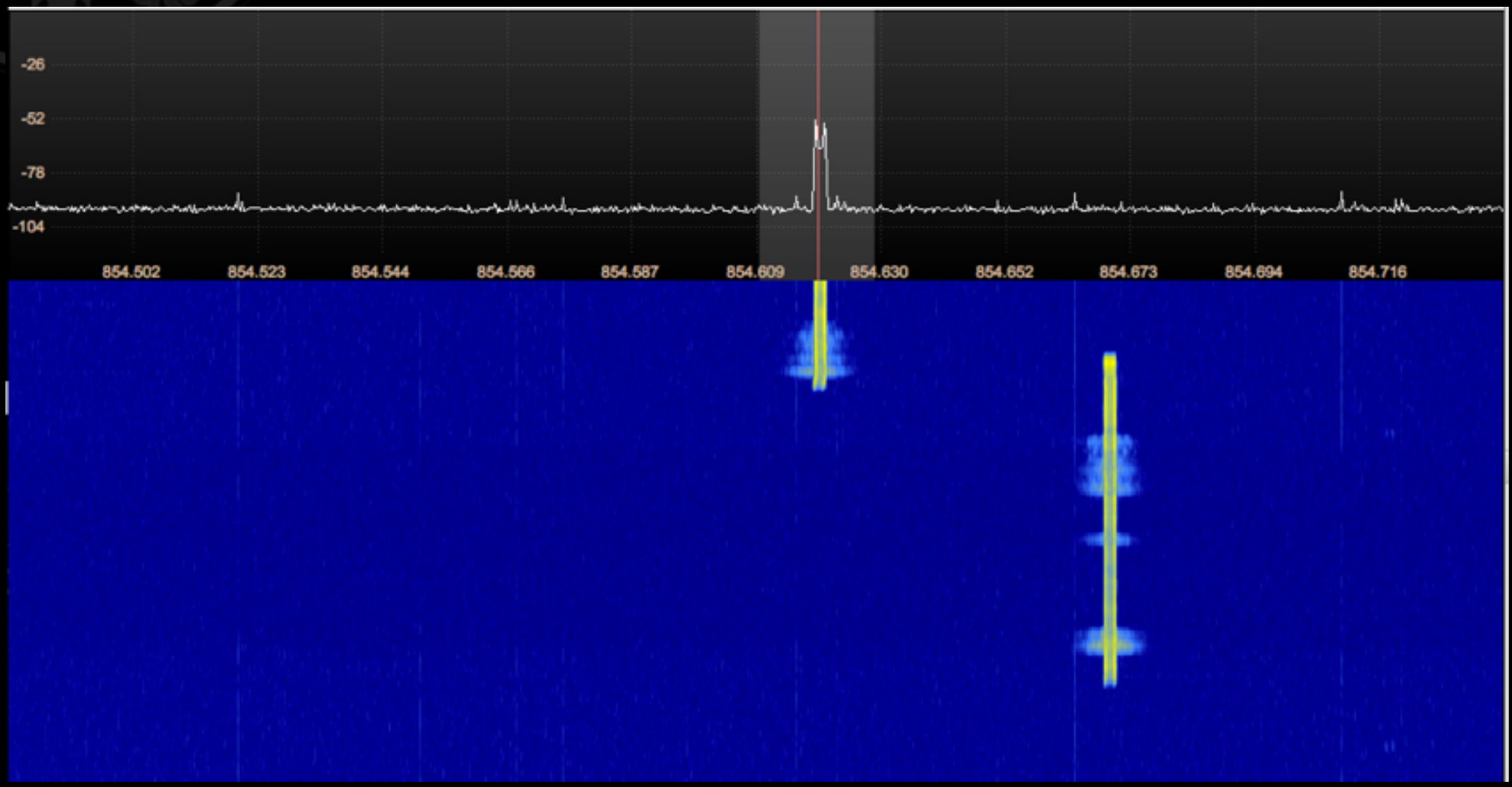
10-31 In Progress

- Police channels are publicly available and depends on region.
- Most police bands are narrow band FM or P25 encoded.

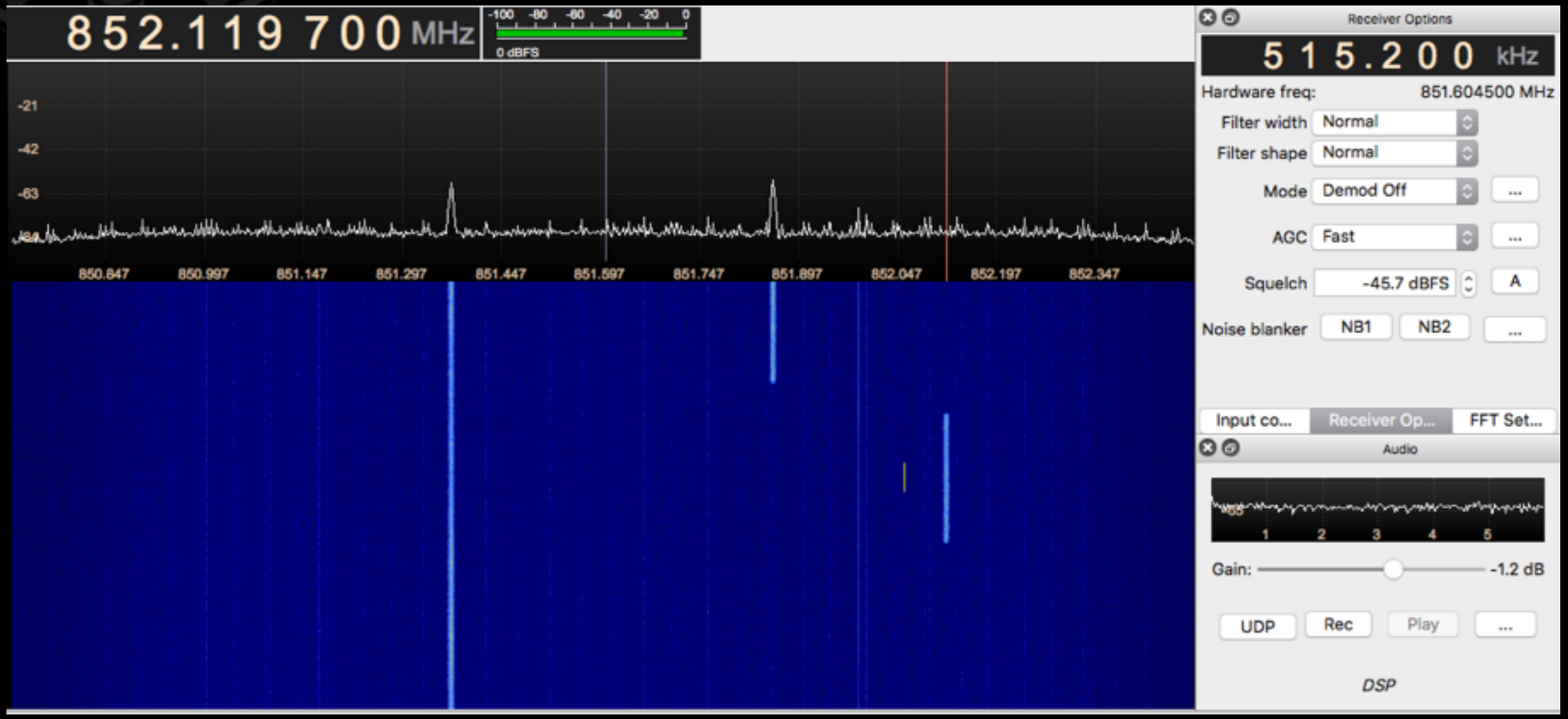
10-31 In progress



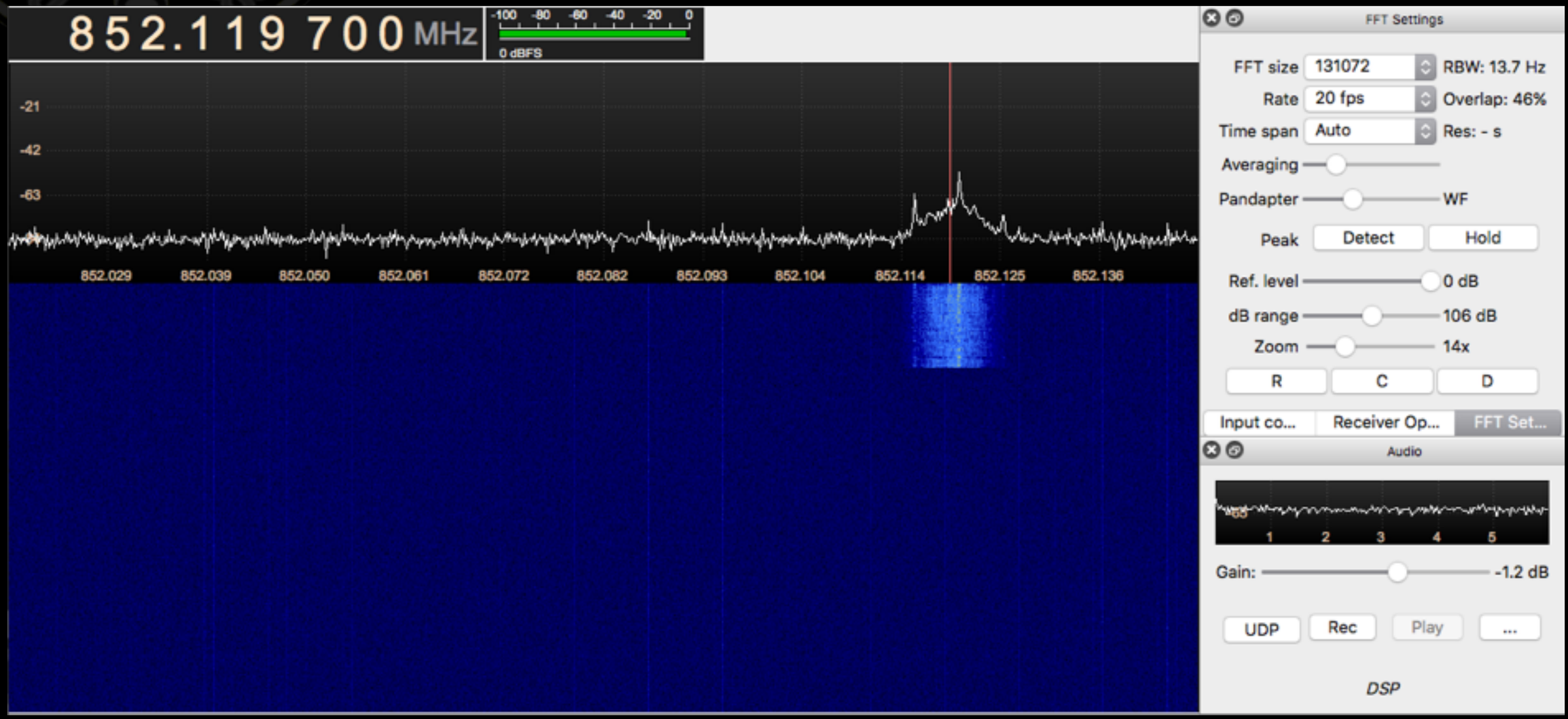
10-31 In progress



10-31 In progress



10-31 In Progress



10-31 In Progress

DEMO Goes Here

Use:

http://gqrx.dk/

https://github.com/szechyjs/dsd