# 0x01 Software Defined Radio (SDR)

Dr. Mike Ham

We’re going to use a computer to listen to radio waves.

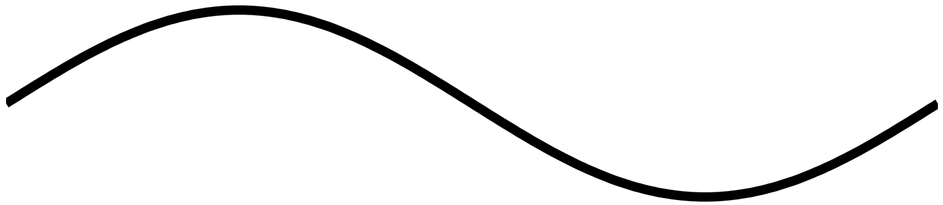
# What radio waves surround you?

# What radio waves surround you?

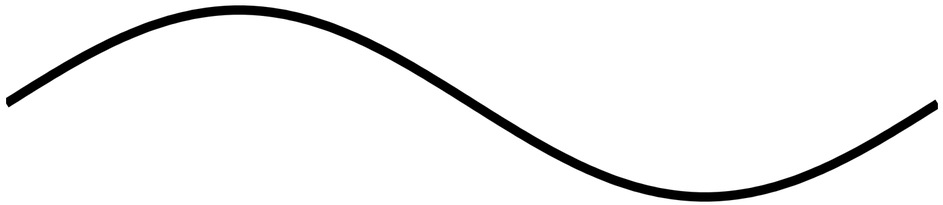
**Get creative!**

# Radio 101

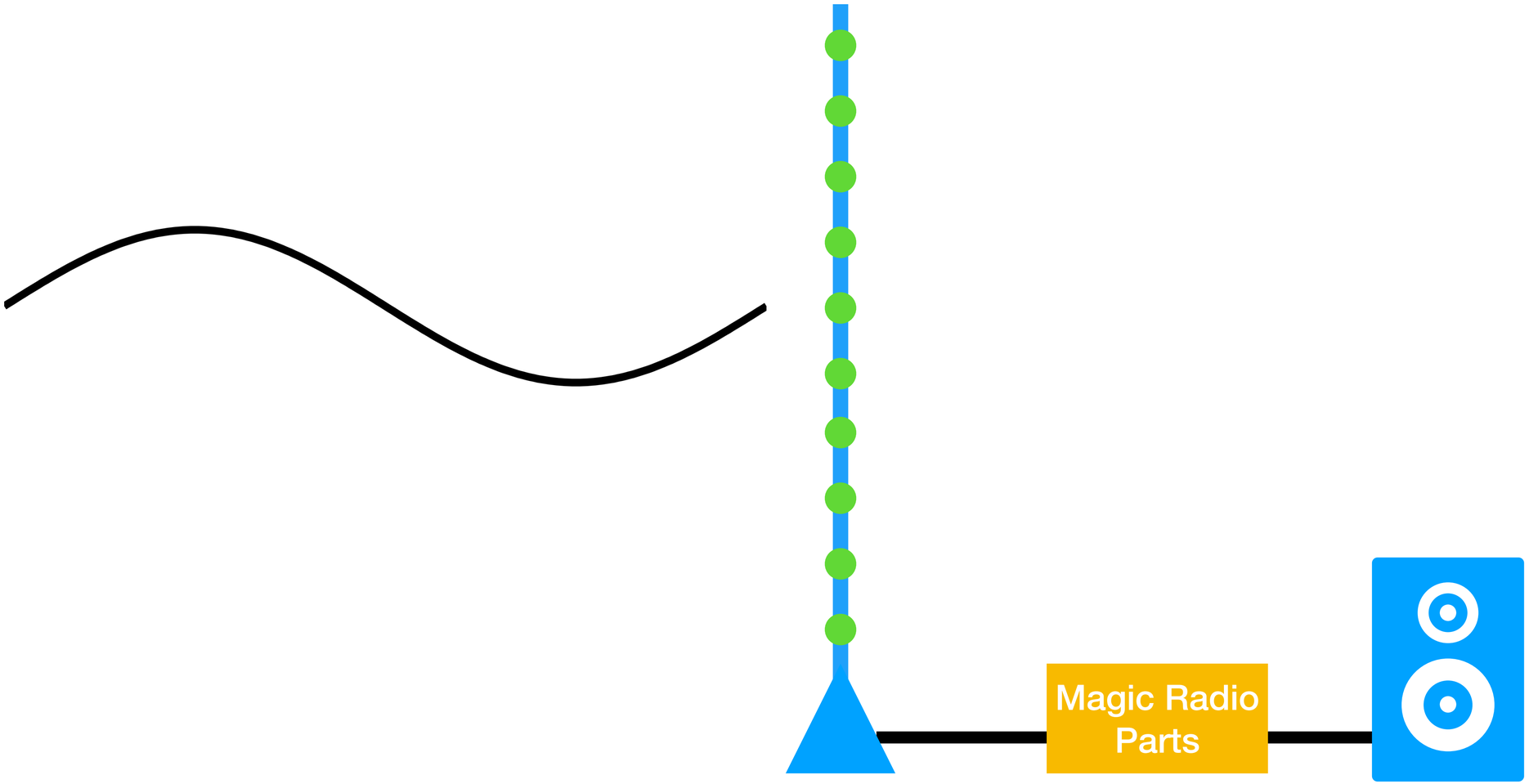
# Radio 101



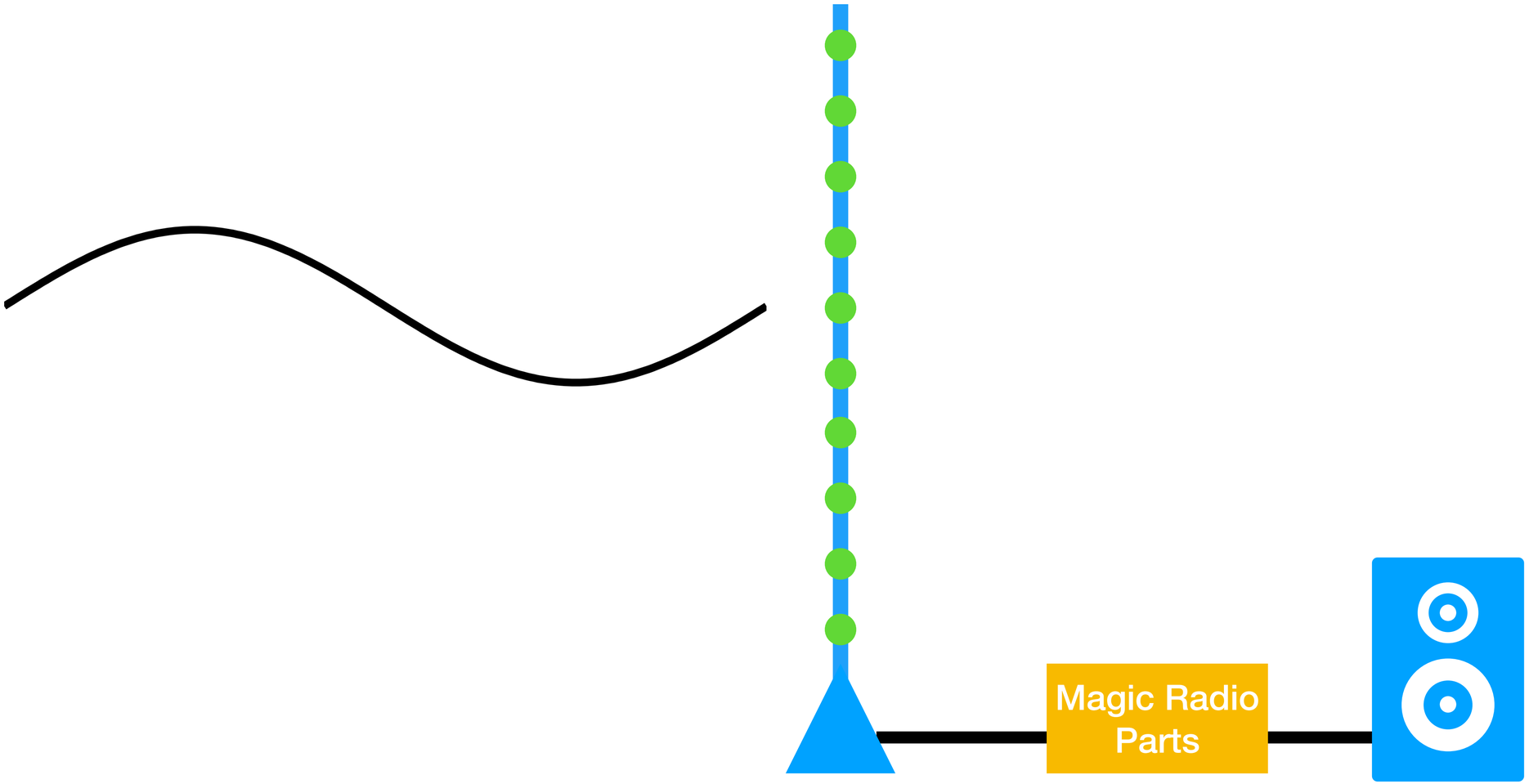
# Radio 101



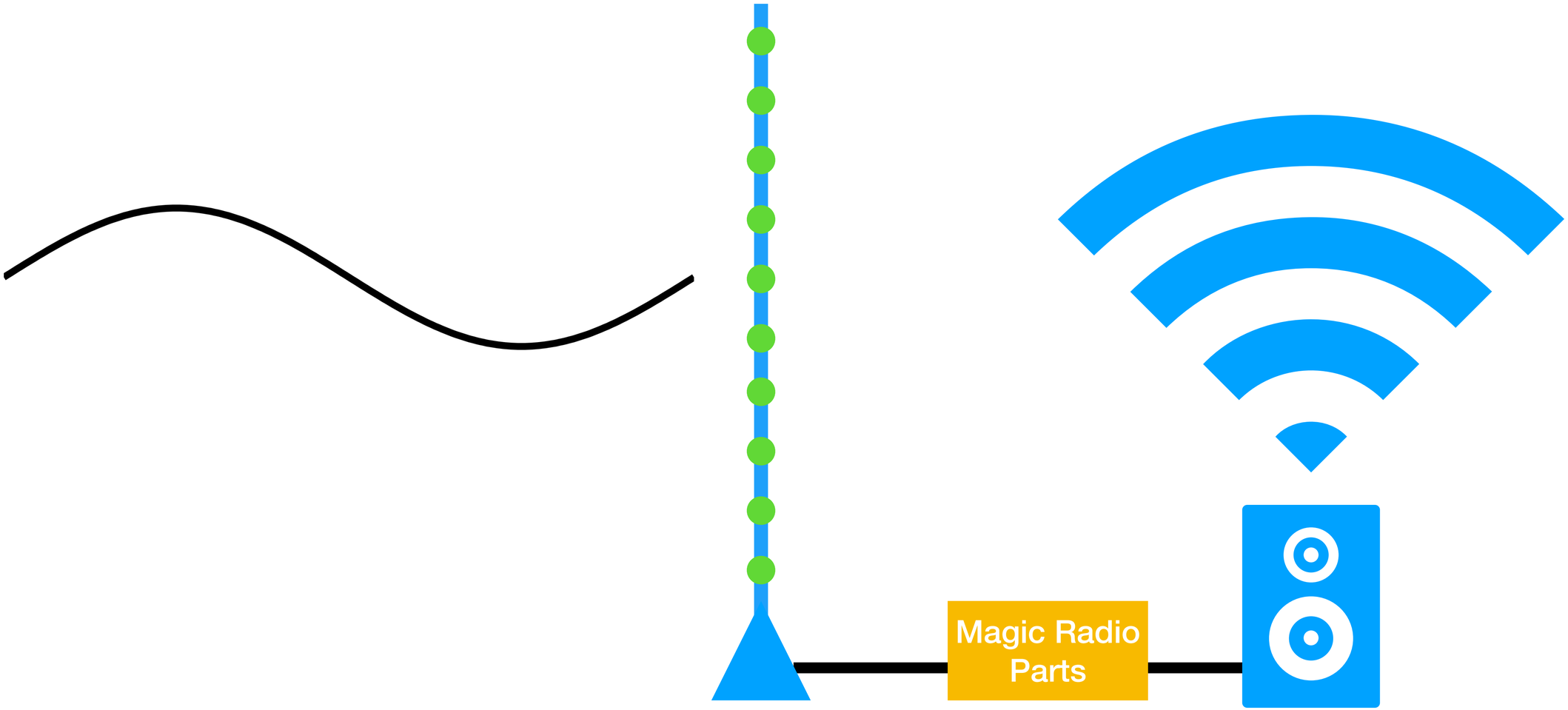
# Antenna



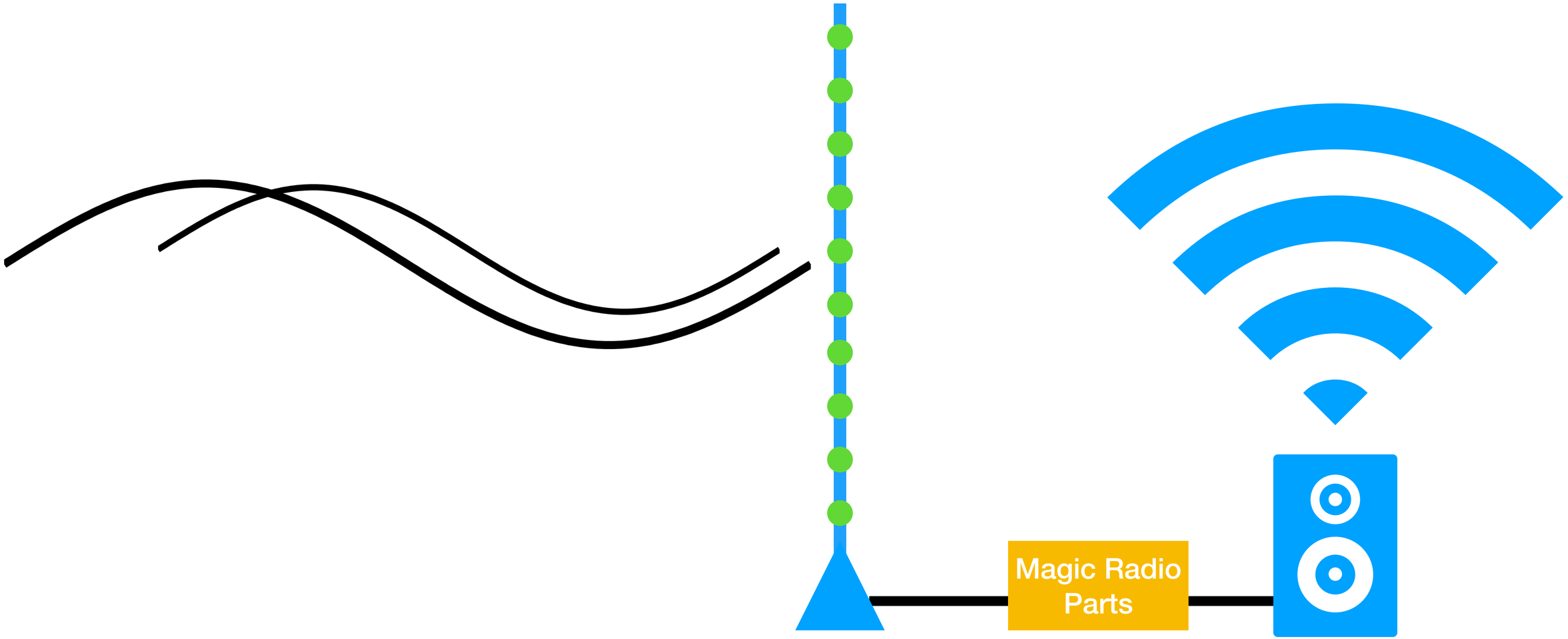
# Antenna



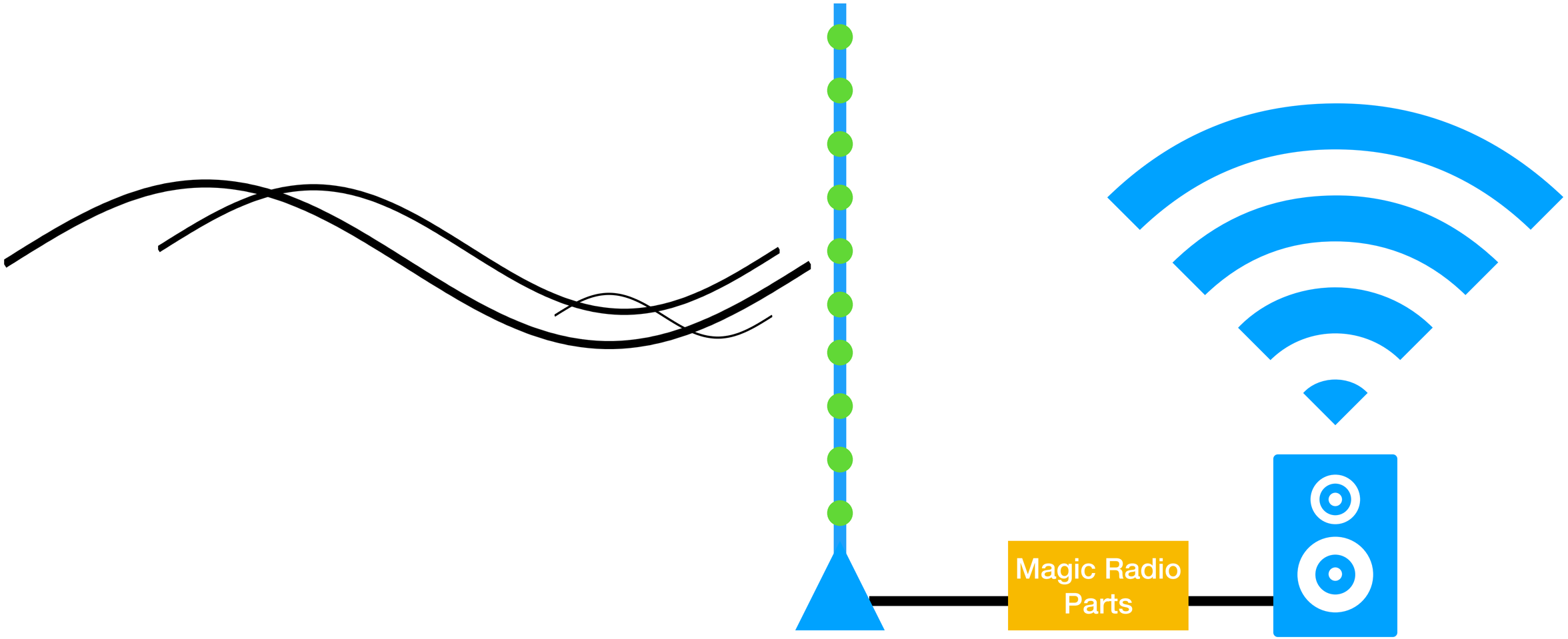
# Antenna



# Antenna

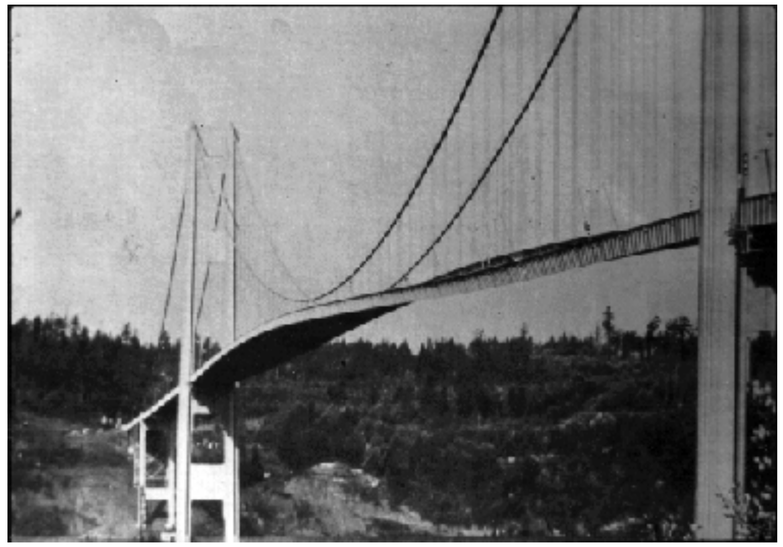


# Antenna



# One Antenna for All?

- The length and type are hugely important to what it can receive
- There is lots of physics and math involved in antenna design
- What we're looking for is a term called **resonance**
  - Pretty much where the antenna "vibrates" most efficiently
  - Largely determined by length



# AM Radio Antenna

- Typical frequency around 1000kHz (kilohertz)
  - FM radio operates around 100MHz (megahertz)
  - 1 MHz = 1000kHz
- All radio waves traverse the planet at the speed of light
  - Low frequency = big radio wave
  - High frequency = little radio wave
  - FM radio waves are roughly 100 times smaller than AM radio waves

# How Big

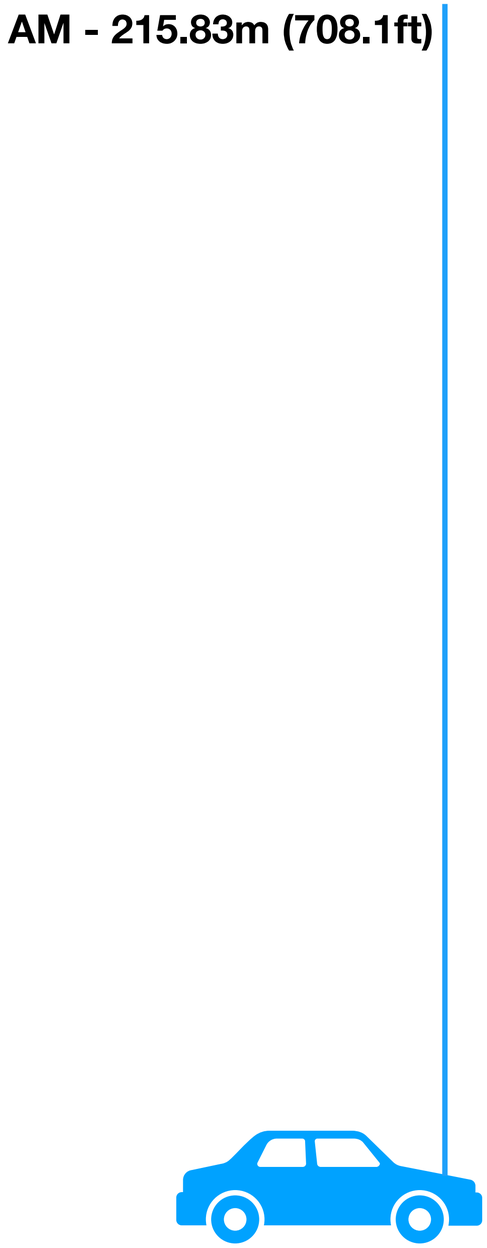
# How Big

- Simple calculation: m = 300 / frequency MHz
  - If I tune into FM103.1, how long of an antenna do I need?
  - Remember, FM operates in megahertz (MHz)
  - m_____ = 300 / _____

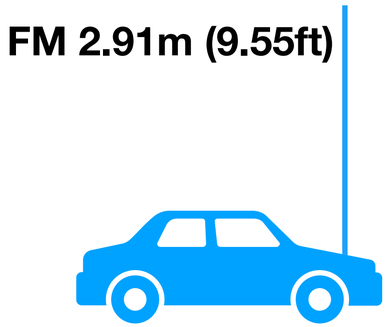
# How Big

- Simple calculation: m = 300 / frequency MHz
  - If I tune into FM103.1, how long of an antenna do I need?
  - Remember, FM operates in megahertz (MHz)
  - m_____ = 300 / _____
- What about AM radio which is kilohertz, let's say 1390kHz
  - m = 300 / (frequency kHz / 1000)
  - m_____ = 300 / _____

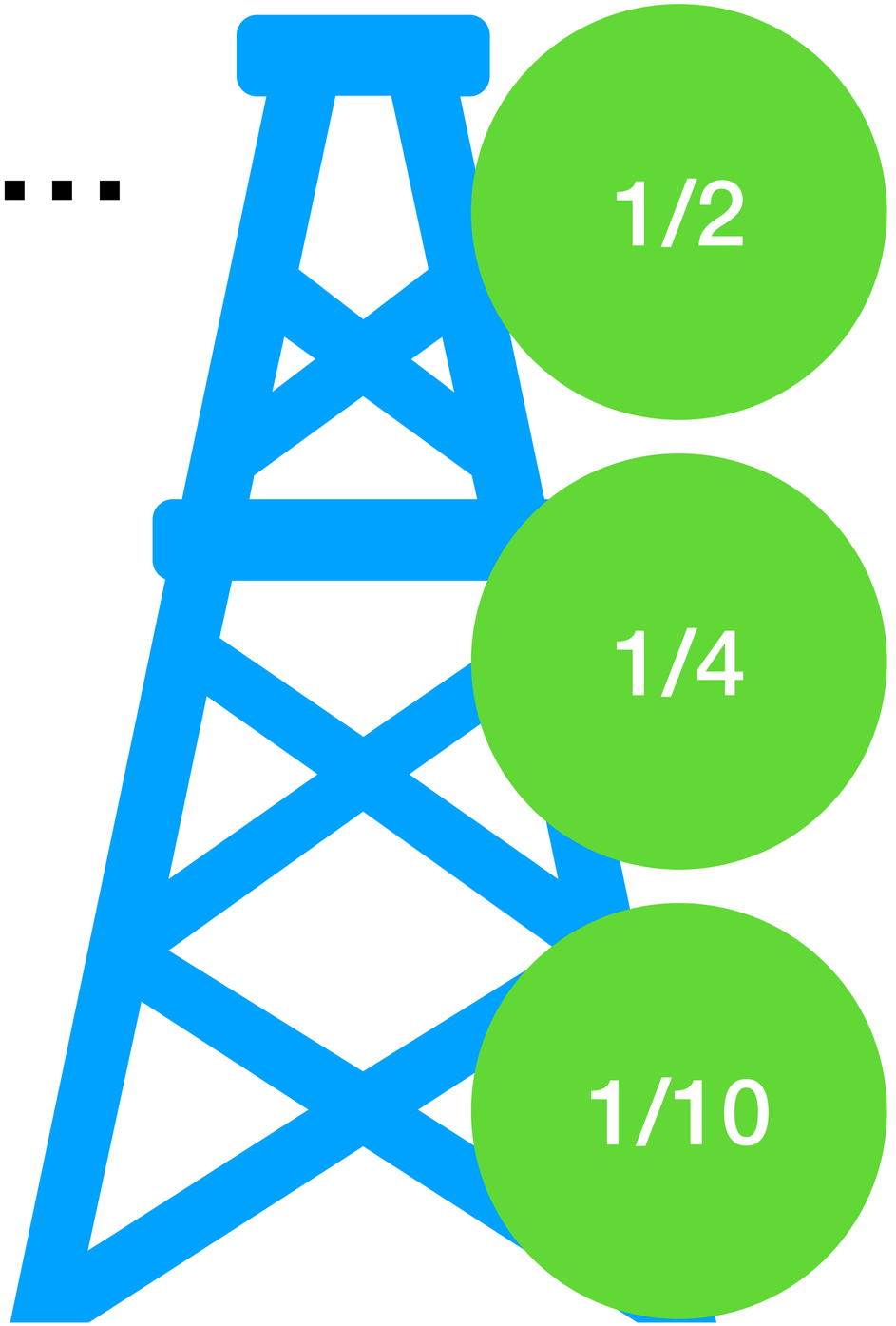
# Oh my…

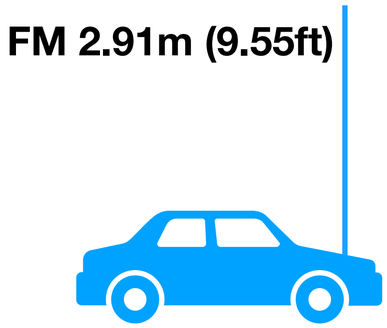


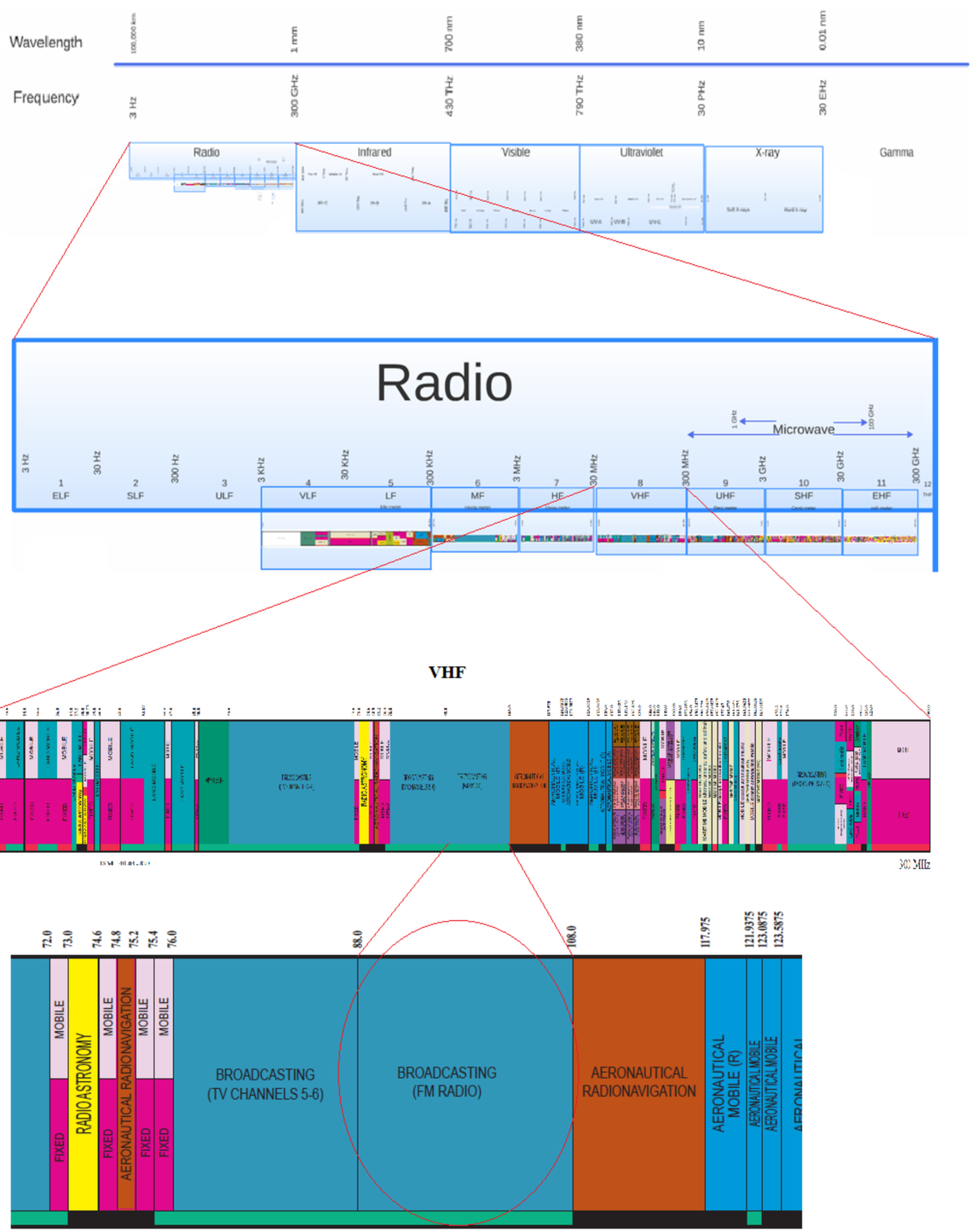
# Oh my…



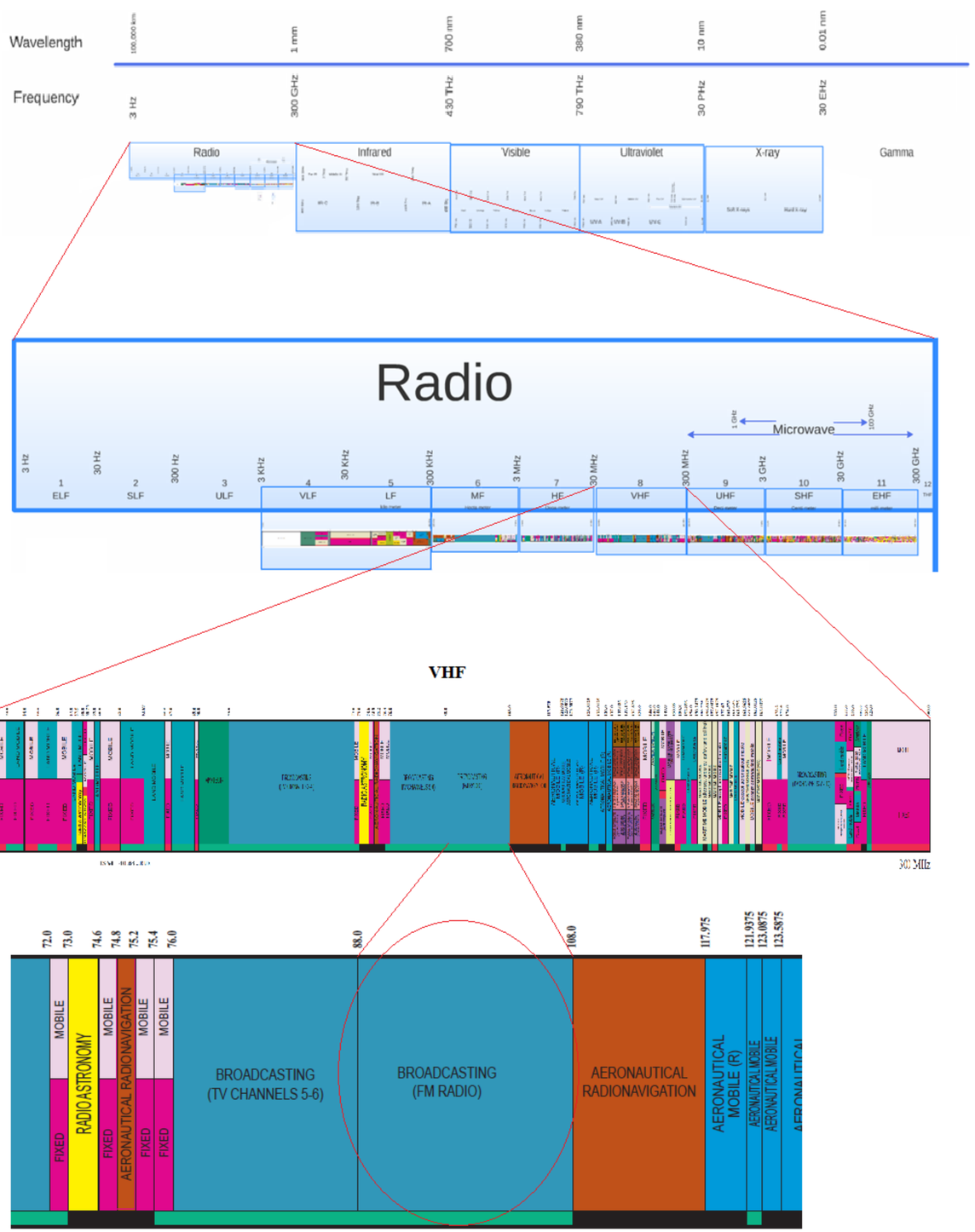
# Oh my…



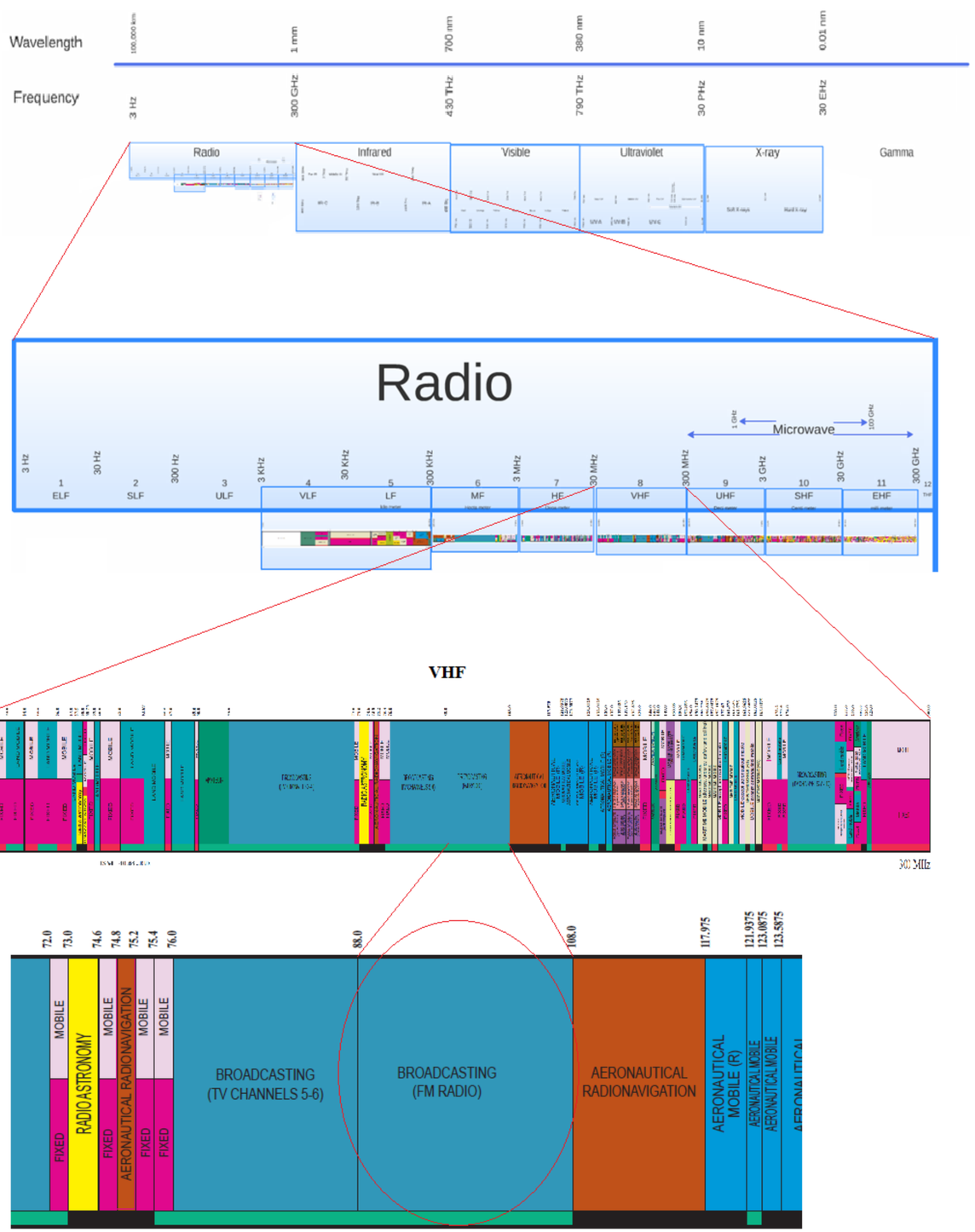

Wavelength
1 mm
700 nm
380 nm
10 nm
0.01 nm
Frequency
3 Hz
300 GHz
430 THz
790 THz
30 PHz
30 EHz
Radio
Infrared
Visible
Ultraviolet
X-ray
Gamma
Radio
Microwave
1 GHz
100 GHz
3 Hz
30 Hz
300 Hz
3 KHz
30 KHz
300 KHz
3 MHz
30 MHz
300 MHz
3 GHz
30 GHz
300 GHz
1 ELF
2 SLF
3 ULF
4 VLF
5 LF
6 MF
7 HF
8 VHF
9 UHF
10 SHF
11 EHF
12
VHF
30 MHz
72.0
73.0
74.6
74.8
75.2
75.4
76.0
88.0
108.0
117.975
121.9375
123.0875
123.5875
MOBILE
FIXED
RADIOASTRONOMY
MOBILE
FIXED
AERONAUTICAL RADIONAVIGATION
MOBILE
FIXED
MOBILE
BROADCASTING
(TV CHANNELS 5-6)
BROADCASTING
(FM RADIO)
AERONAUTICAL
RADIONAVIGATION
AERONAUTICAL
MOBILE (R)
AERONAUTICAL MOBILE
AERONAUTICAL MOBILE

# 3Hz to 30EHz


Wavelength
100,000 km
1 mm
700 nm
380 nm
10 nm
0.01 nm
Frequency
3 Hz
300 GHz
430 THz
790 THz
30 PHz
30 EHz
Radio
Infrared
Visible
Ultraviolet
X-ray
Gamma
Radio
Microwave
1 GHz
100 GHz
3 Hz
30 Hz
300 Hz
3 KHz
30 KHz
300 KHz
3 MHz
30 MHz
300 MHz
3 GHz
30 GHz
300 GHz
1 ELF
2 SLF
3 ULF
4 VLF
5 LF
6 MF
7 HF
8 VHF
9 UHF
10 SHF
11 EHF
12
VHF
30 MHz
72.0
73.0
74.6
74.8
75.2
75.4
76.0
88.0
108.0
117.975
121.9375
123.0875
123.5875
MOBILE
FIXED
RADIOASTRONOMY
MOBILE
FIXED
AERONAUTICAL RADIONAVIGATION
MOBILE
FIXED
MOBILE
BROADCASTING
(TV CHANNELS 5-6)
BROADCASTING
(FM RADIO)
AERONAUTICAL
RADIONAVIGATION
AERONAUTICAL
MOBILE (R)
AERONAUTICAL MOBILE
AERONAUTICAL MOBILE

3Hz to 30EHz

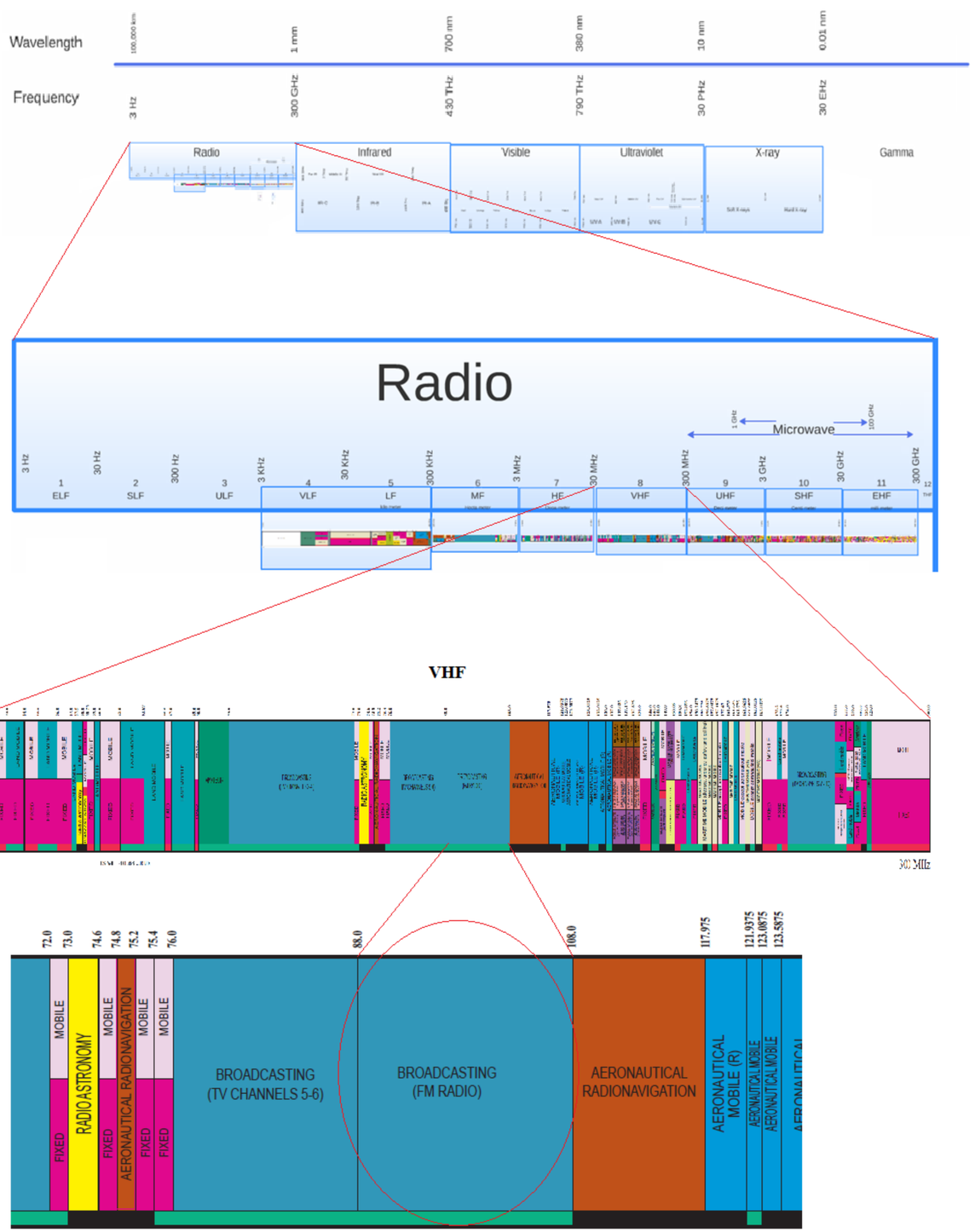
3Hz to 3THz



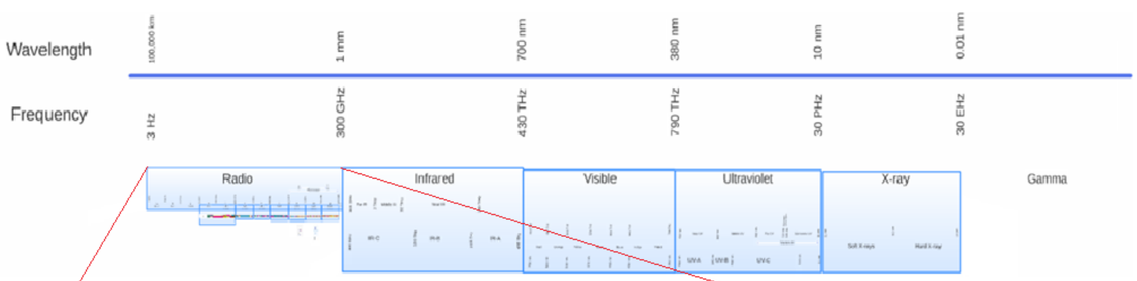
3Hz to 30EHz

3Hz to 3THz

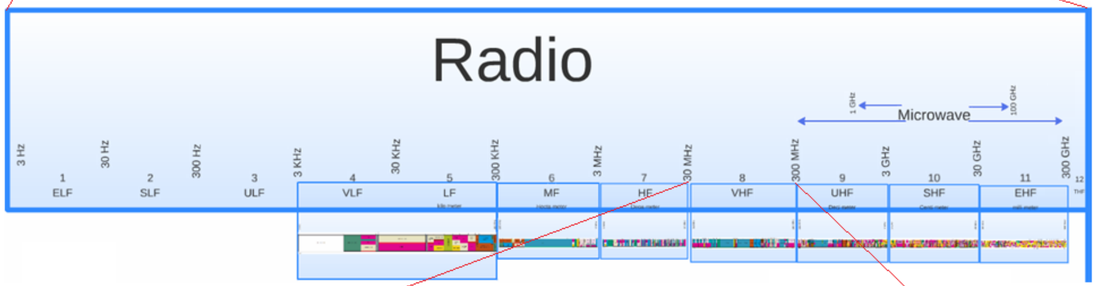
30MHz to 300MHz



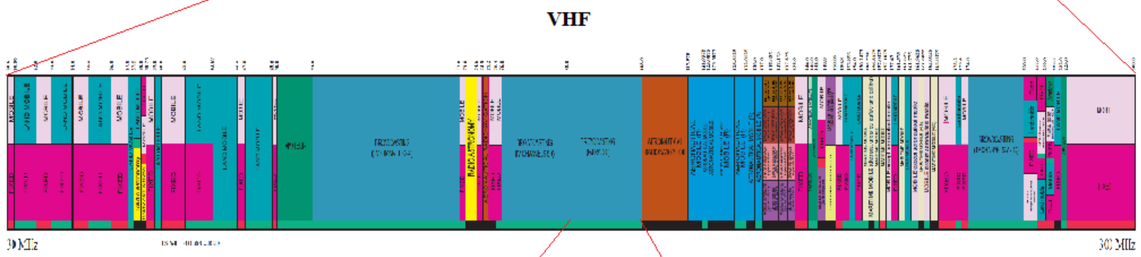
3Hz to 30EHz



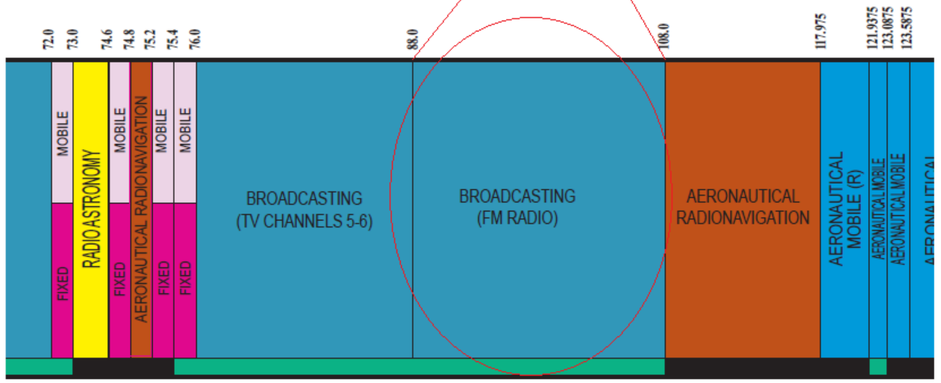

3Hz to 3THz




30MHz to 300MHz




88MHz to 108MHz



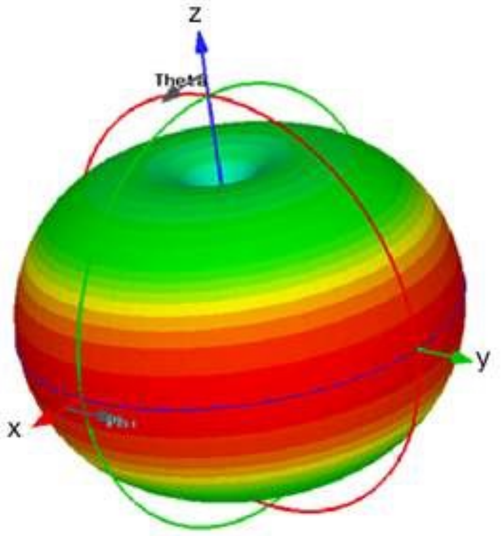
# US Frequency Allocations

- https://www.ntia.doc.gov/files/ntia/publications/january_2016_spectrum_wall_chart.pdf

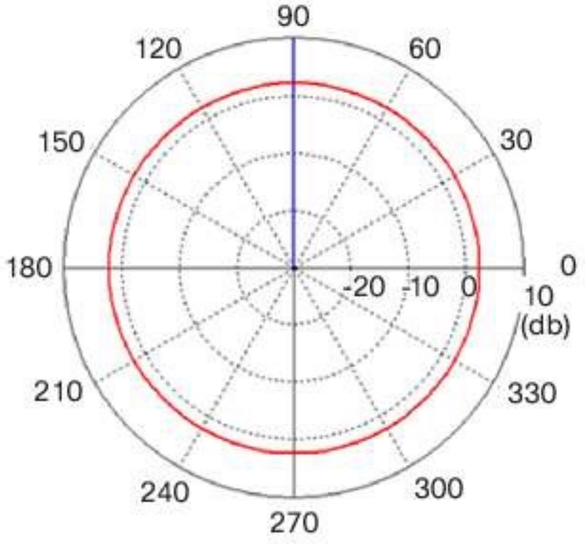
# Antenna Types

- Omnidirectional
  - Extends your range in all directions
- Directional
  - Let’s you focus your signal in a particular direction
- Sensitivity – measured in dBi
  - dBi - gain of an antenna as referenced to an ISOTROPIC (omnidirectional) source
  - Remember, every 3 dBi = double the sensitivity

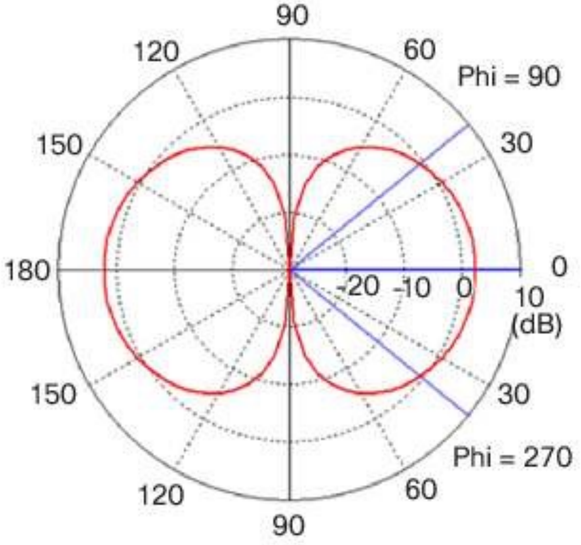

(a) Dipole Antenna Model



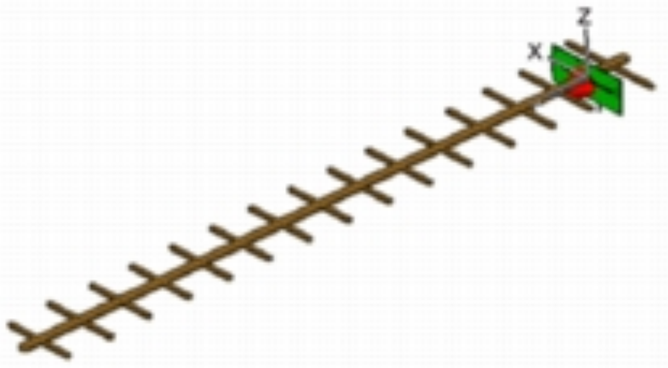

(b) Dipole 3D Radiation Pattern



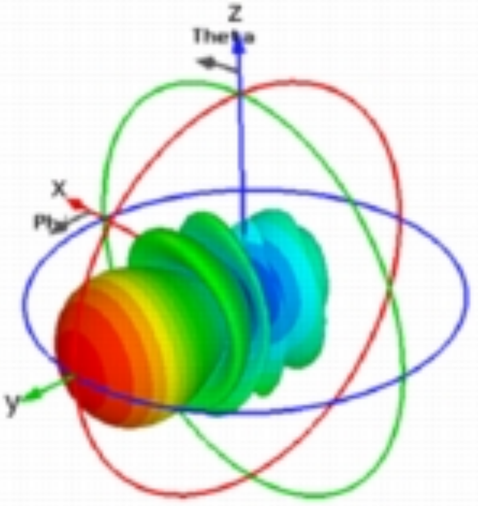

(c) Dipole Azimuth Plane Pattern



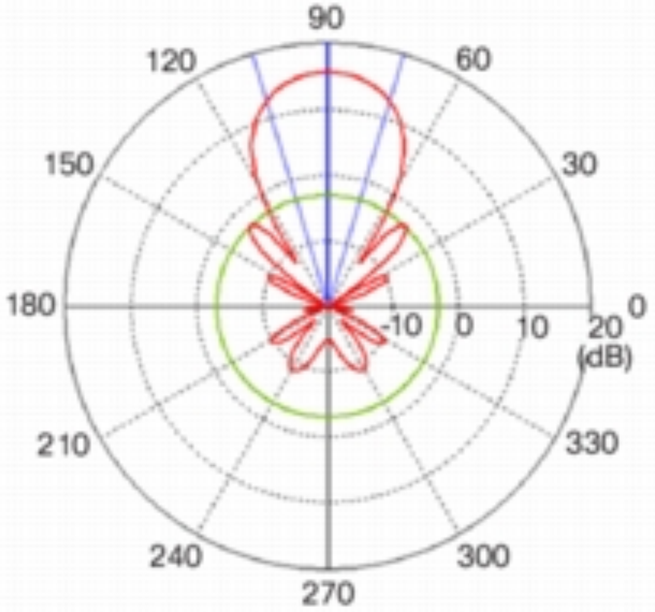

(d) Dipole Elevation Plane Pattern



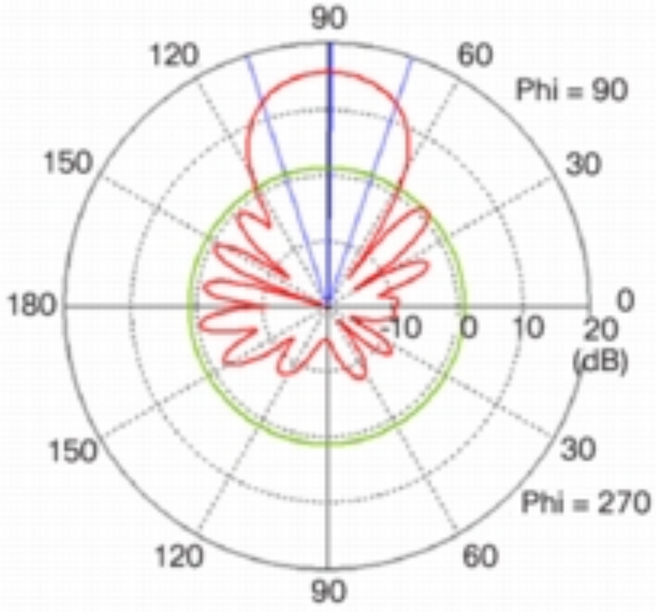

(a) Yagi Antenna Model




(b) Yagi Antenna 3D Radiation Pattern




(c) Yagi Antenna Azimuth Plane Pattern




(d) Yagi Antenna Elevation Plane Pattern

# What is SDR?

- Device that allows us to *understand* different signals received by a radio
- Effectively the goal is to remove the analog parts of a radio and do it all in software
    - Think about turning a knob on the radio and replacing that mechanism with software
- Rather than just being able to tune into one thing (e.g. FM radio), you can capture a wide array of bands

# FM Radio

# FM Radio

# FM Radio

# FM Radio

# FM Radio

# FM Radio

# FM Radio

# FM Radio

# FM Radio

# FM Radio

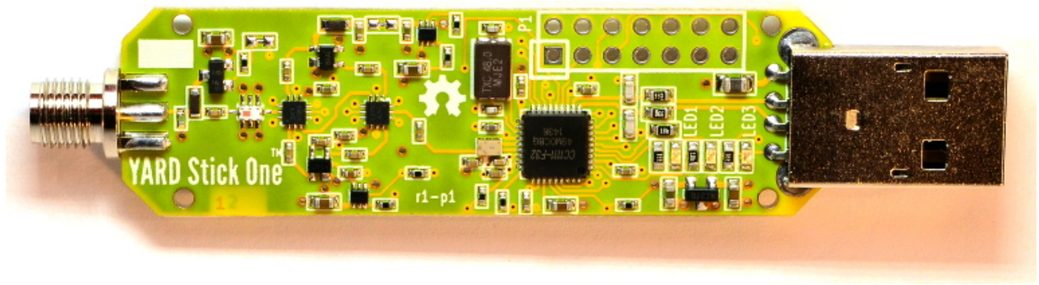
# What can SDR do?

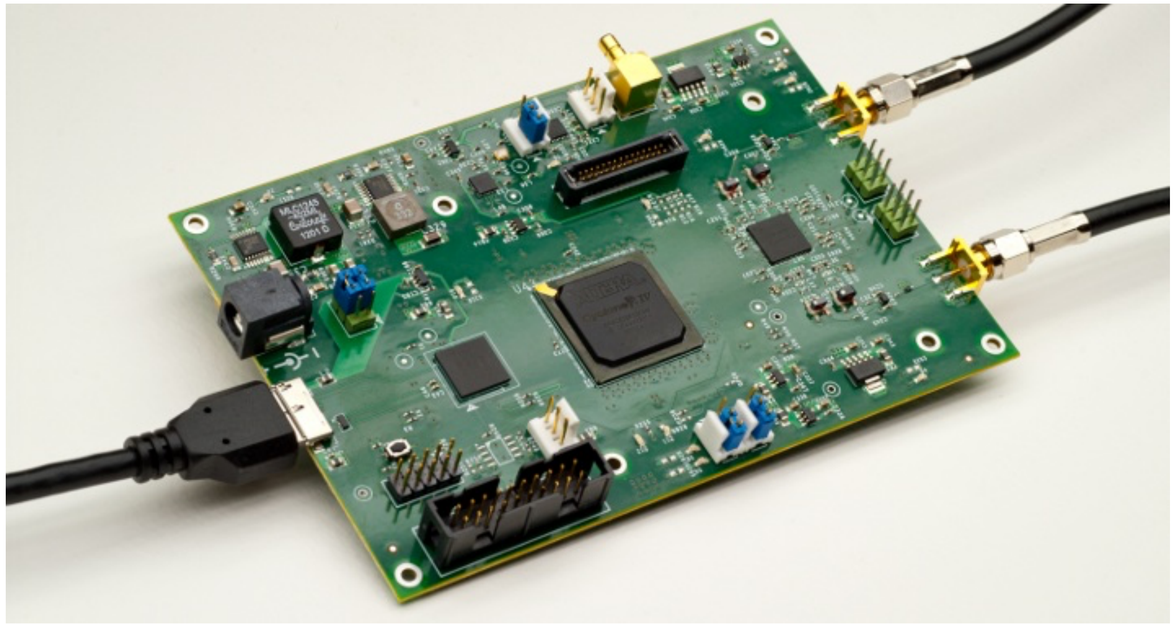
- This can be used as an AM / FM radio, a police scanner, air traffic control listener, etc.
- Receive images from weather satellites
- You’re basically packet sniffing with radio
- Isn’t that not legit to do?
  - Use common sense when doing stuff like this
  - The antennas you have can only receive not transmit so you’re ok here

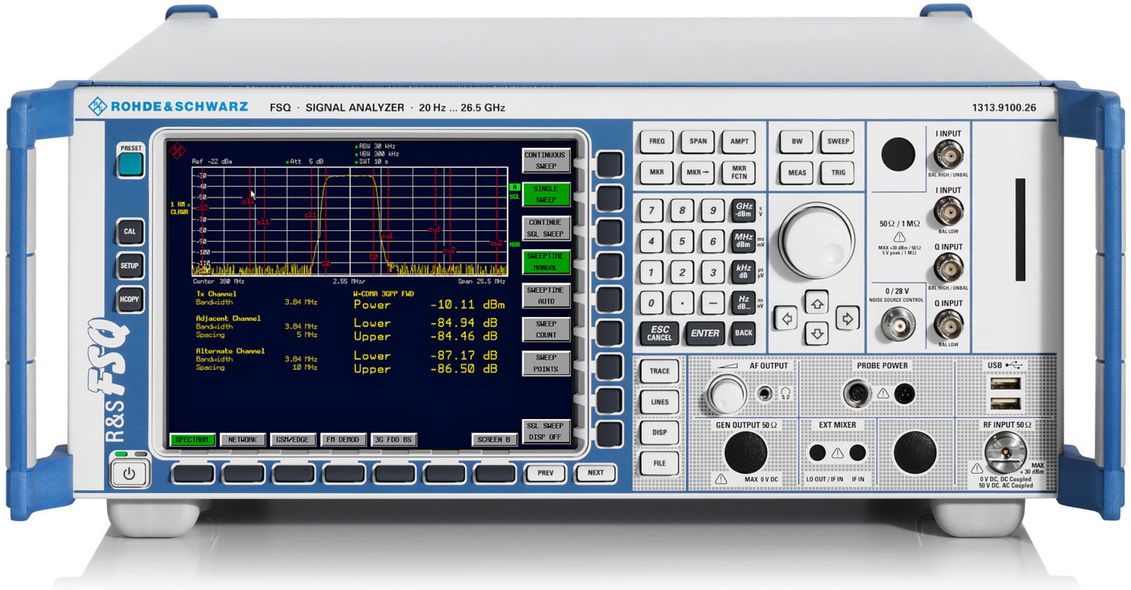
# The Hardware

- Software Defined Radio Receiver USB Stick
  - RTL2832 w/R820T
  - 24MHz to 1850MHz
- ~20 piece of hardware, can definitely get them cheaper if you shop around

# Other SDR Hardware





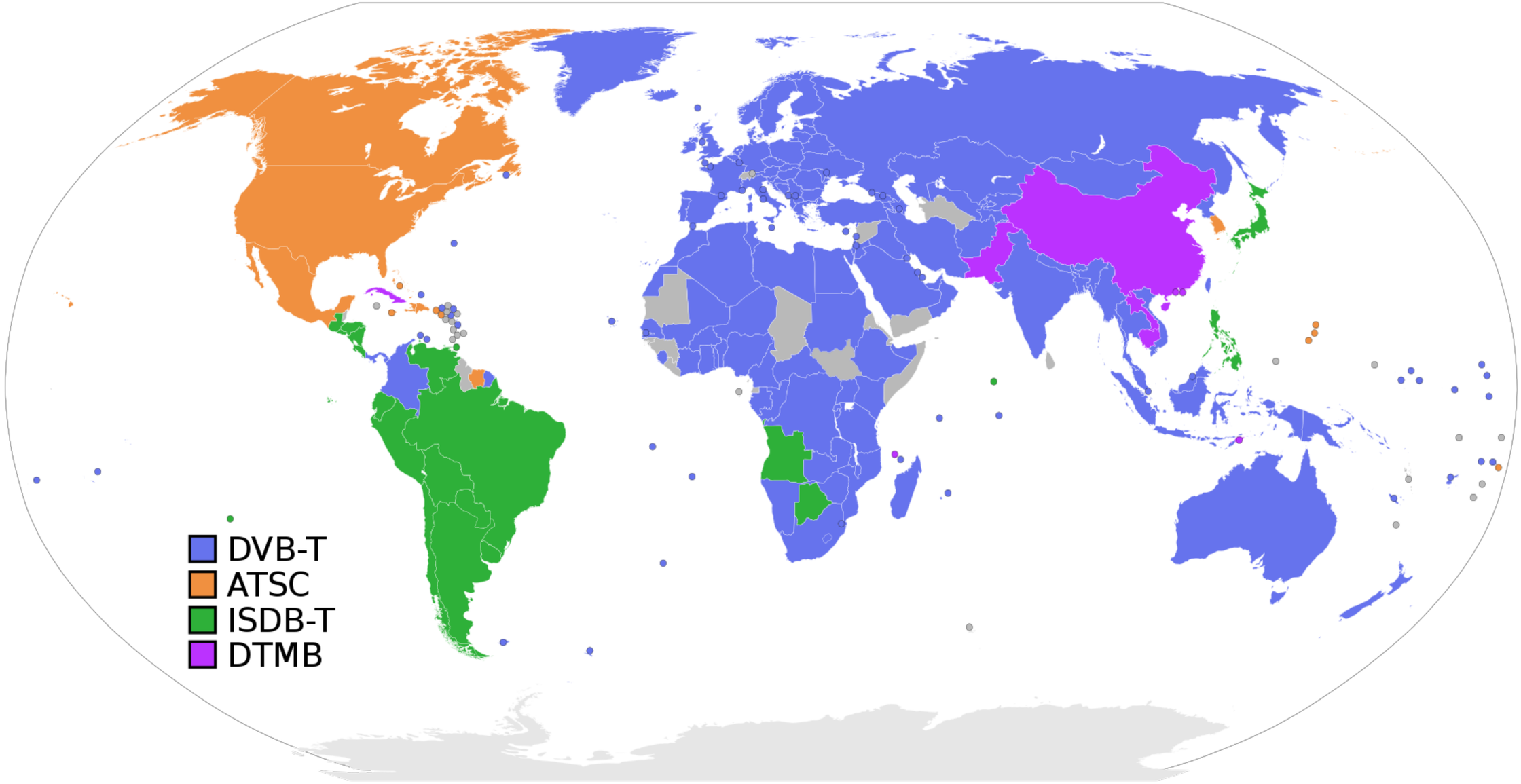
# Geeky Specs

- DVBT:48.25 ~863.25 MHZ
- FM radio: 87.5~108 MHZ
- DAB radio: L-Band-1452960~1490624 KHZ
- VHF—174928~ 239200 KHz
- Will work for both for software defined radio and DVB video capture (where available)
- Compatible with most SDR software. Approx range: 25MHz-1700MHz
- 6-8 MHz Bandwidth

# Intended Purpose

- This USB adapter is meant to allow users to record and watch digital TV on a computer
  - Still image snapshots, recording and playback, etc.
  - Play FM radio and DAB digital radio
- Realtek RTL2832U and R820T chipsets
  - With a little trickery, we can actually make these do a lot more

# TV?!



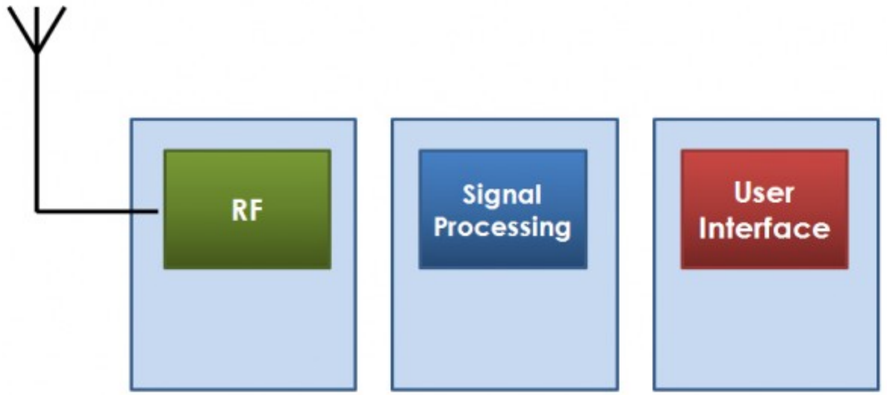
# Driver Voodoo

- Some really smart people have crafted a driver for these USB adapters to give us more control
- Driver – software that controls hardware
  - Your mouse, keyboard, printers, etc. all use them
  - Computer has to know how to speak the language of the hardware in order for it to work

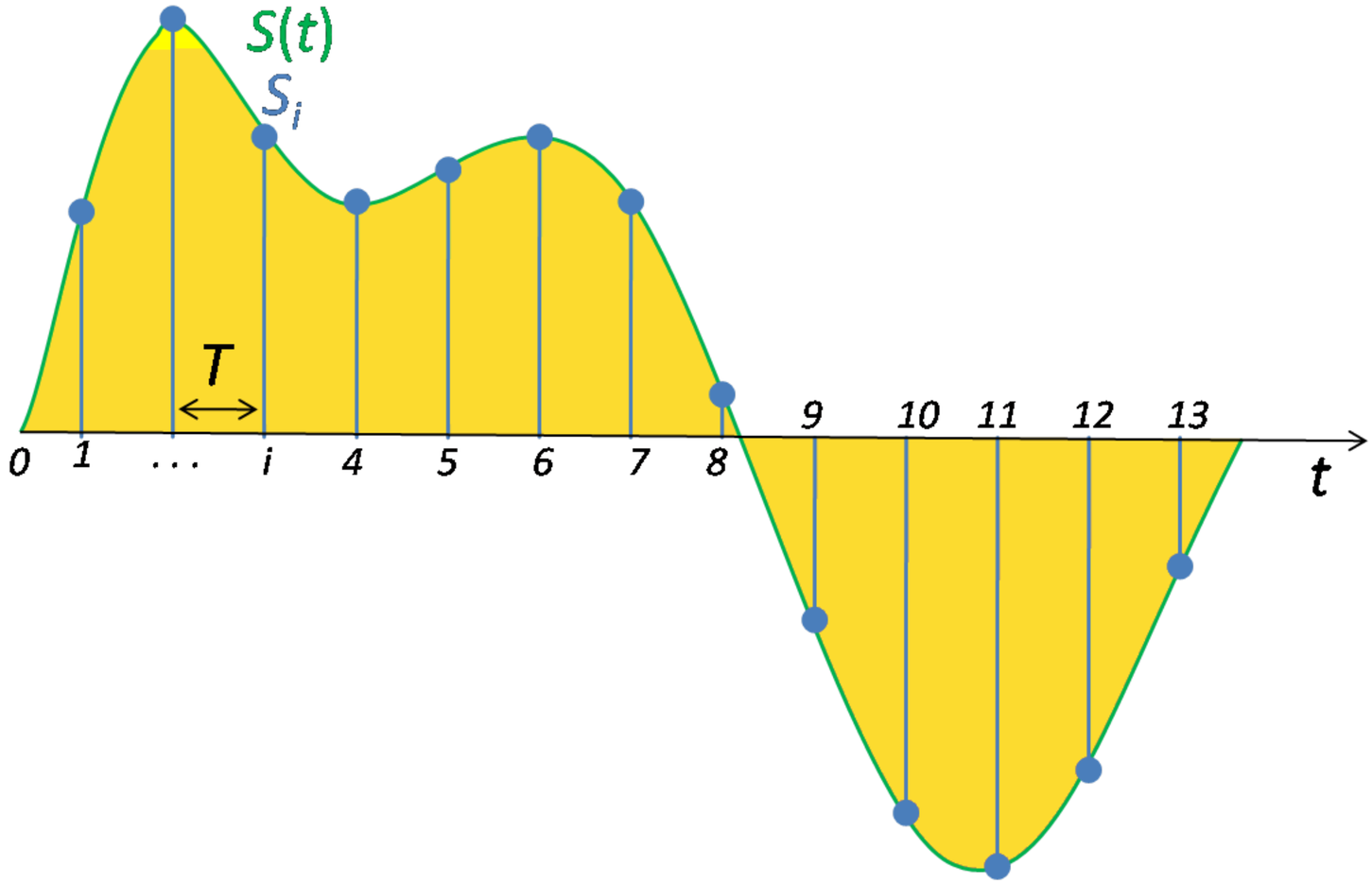
# How does SDR work?

- At a 10,000’ view, SDR converts the analog signals on the antenna into digital signals (1’s and 0’s)

- Using signal processing techniques, we can make that data more usable



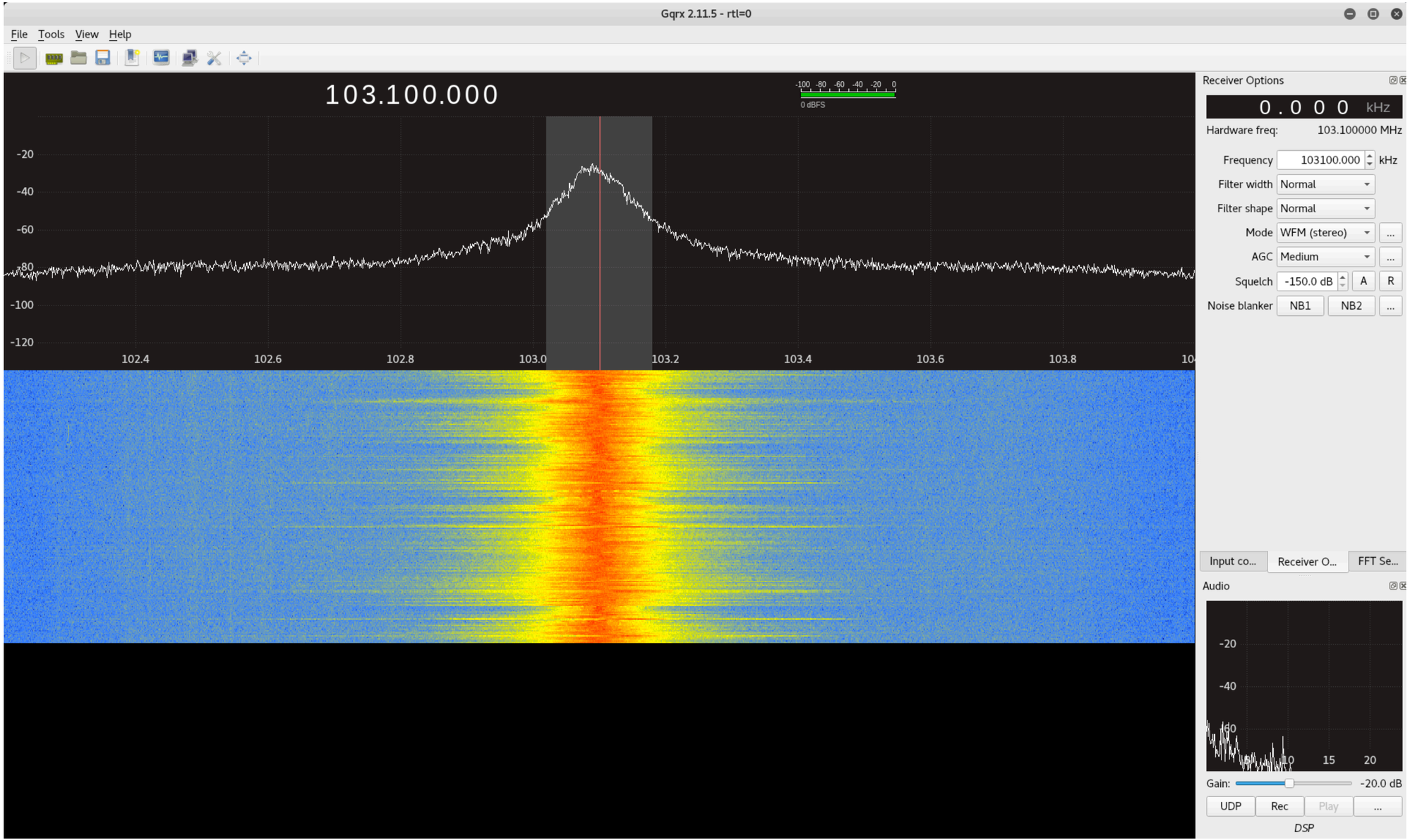
# Original —> Sampled —> Reconstructed



# FM Radio

- Let’s go for something normal first
- FM radio (these radios aren't supposed to do this out of the box)
- Choose WFM (wide-band FM radio)
- Set your frequency by clicking large numbers on top
  - Local station KJAM is 103.1
  - The interface is a little touchy
- Click the play button and listen!

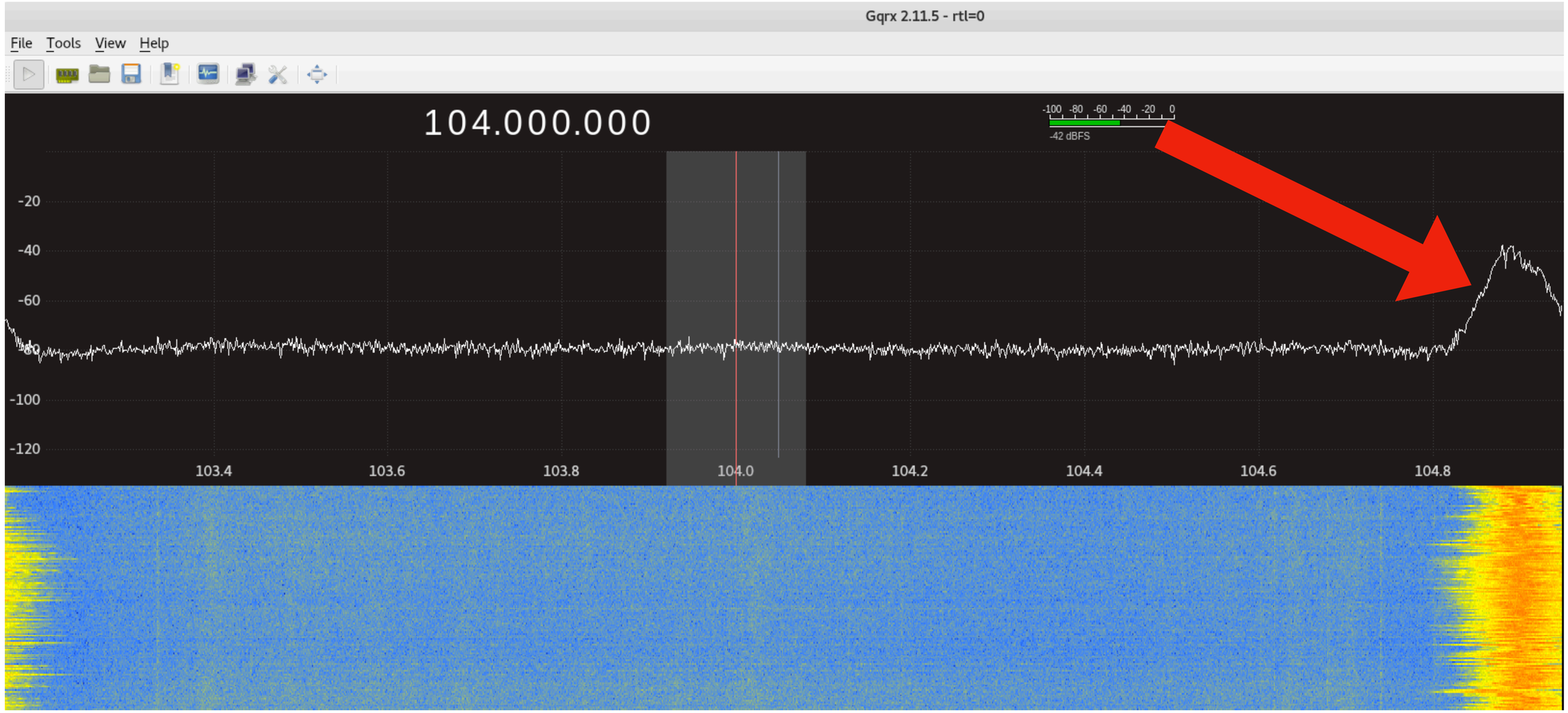
# gqrx


Gqrx 2.11.5 - rtl=0
File Tools View Help
103.100.000
-100 -80 -60 -40 -20 0
0 dBFS
-20
-40
-60
-80
-100
-120
102.4
102.6
102.8
103.0
103.2
103.4
103.6
103.8
Receiver Options
0.000 kHz
Hardware freq: 103.100000 MHz
Frequency 103100.000 kHz
Filter width Normal
Filter shape Normal
Mode WFM (stereo)
AGC Medium
Squelch -150.0 dB A R
Noise blanker NB1 NB2
Input co... Receiver O... FFT Se...
Audio
-20
-40
-60
10
15
20
Gain: -20.0 dB
UDP Rec Play
DSP

# Find me another station!

- I’ve given you a FM station to tune into
- gqrx shows us where we have strong signals in the current spectrum (WFM in our case)
    - Peaks more than likely will be other radio stations
- You can use the filters on the right-hand side to try and pick out different radio stations
    - Antenna position matters, make sure it stands upright, move to window if need be (they’re just little fellas)

# Another Station



# Look at the Spectrum

- If you adjust the contrast a bit, pinpointing signals becomes a little bit easier

# How about Weather Radio

- Most AM/FM radios can’t tune into the same weather network
- We’ve probably all seen one of these…
  - Older people
  - Rural/storm areas

# RTL-SDR Weather Station

- This is where SDR starts to get cool
- Our adapter shouldn’t be able to gather weather data, but we have special drivers
- NOAA – a big deal in the weather world

# Tuning into Weather

- Find your nearest NOAA weather station frequency here:
  - https://www.weather.gov/nwr/counties

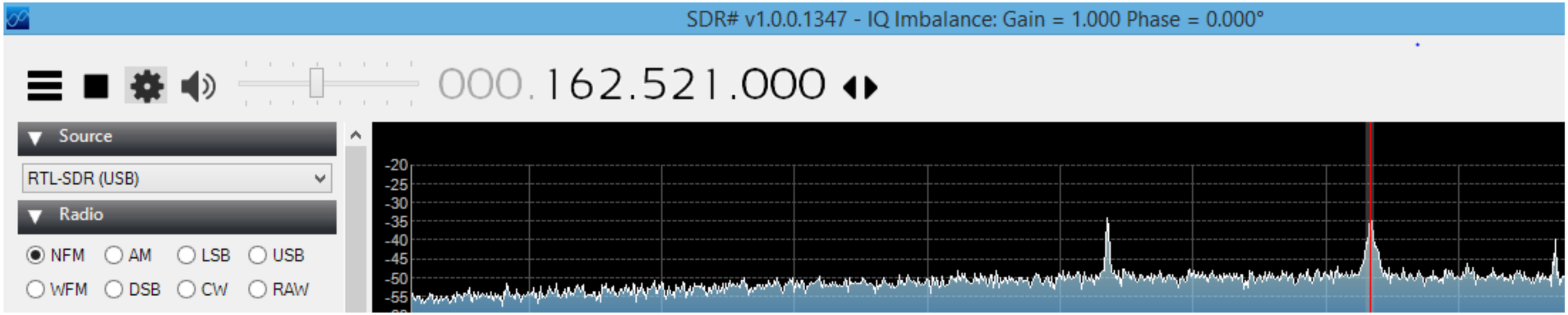
| | | | | | |
|---|---|---|---|---|---|
| Kingsbury | 046077 | Arlington | KXI71 | 162.525 | ALL |
| Kingsbury | 046077 | Wessington | WXM27 | 162.550 | ALL |
| Lake | 046079 | Arlington | KXI71 | 162.525 | ALL |
| Lake | 046079 | Sioux Falls | WXM28 | 162.400 | ALL |
| Lawrence | 046081 | Lead | WXL23 | 162.525 | ALL |

- Type one of the frequencies into gqrx

# Tuning into Weather

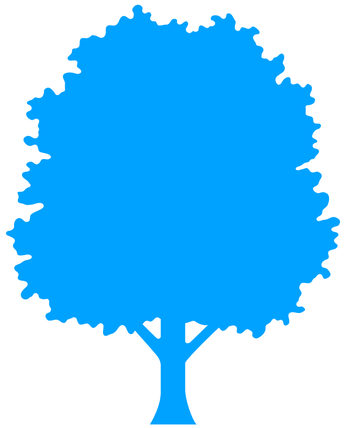
- The peak is much smaller/thinner than FM, we're dealing with narrow-band here.  Change the radio to NFM
- Note: NFM requires a little better signal, may not work well in a building
  - Even though NOAA says **162.525** look at your spectrum and see what your radio wants
  - Environmental factors affect signal

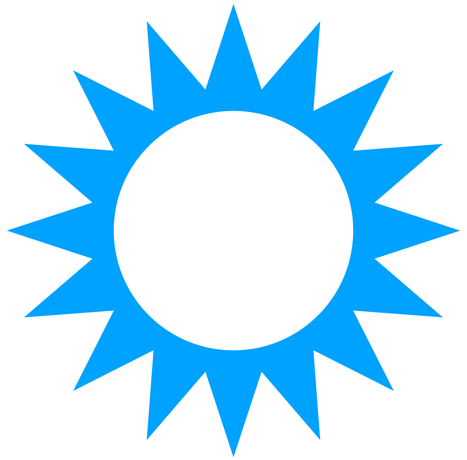
# Weather Radio



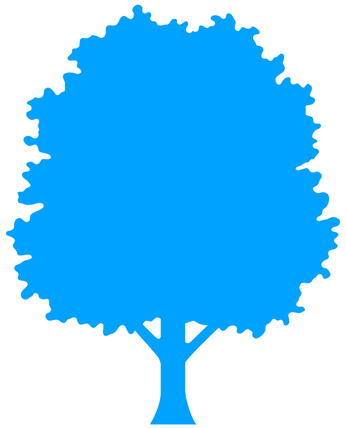
# Any Luck?

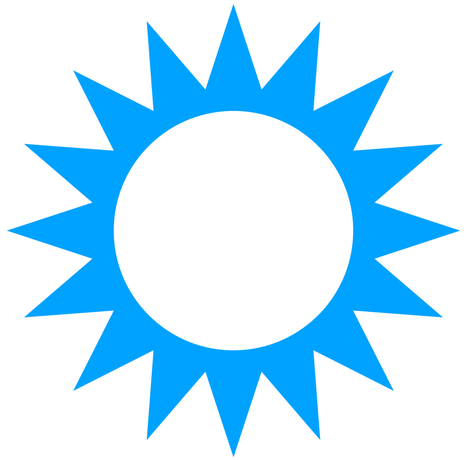
# Weather Recording (Backup)





# Weather Recording (Backup)





# Let’s talk Airplanes

- ADS-B - Automatic dependent surveillance – broadcast
  - Cooperative surveillance for tracking aircraft
- Aircraft determines its position and broadcasts it for safety measures
- Sent in clear text, they want people to read this so planes don’t crash

# Pieces of Software

- dump1090
  - Takes all of the ADSB data and decodes the packets (frames)

- Disclaimer: Madison is not a destination for many planes, fingers crossed one is passing over

# Don’t Stop at 30K Feet

- Planes are very cool, but I like space a little better…
- How about gathering some information from satellites?
  - Our friends, the NOAA, have satellites sending images back for weather purposes
- This gets a little more complicated though

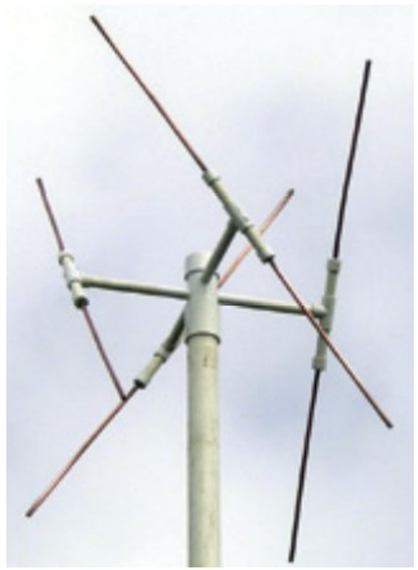
# Satellite Imagery

- Unfortunately, you need a different antenna than what we have
    - As satellites spin and tumble through space, their signals do not come in a completely linear fashion
- With a special antenna, you can gather “audio” from the satellites and save it off to a file

# Right Hand Circularly Polarized (RHCP)

- As the satellites broadcast their signal, they also rotate, rotating the signal polarization

- Satellite antennas are also designed to receive best from signals coming from the sky



# Tracking Satellite

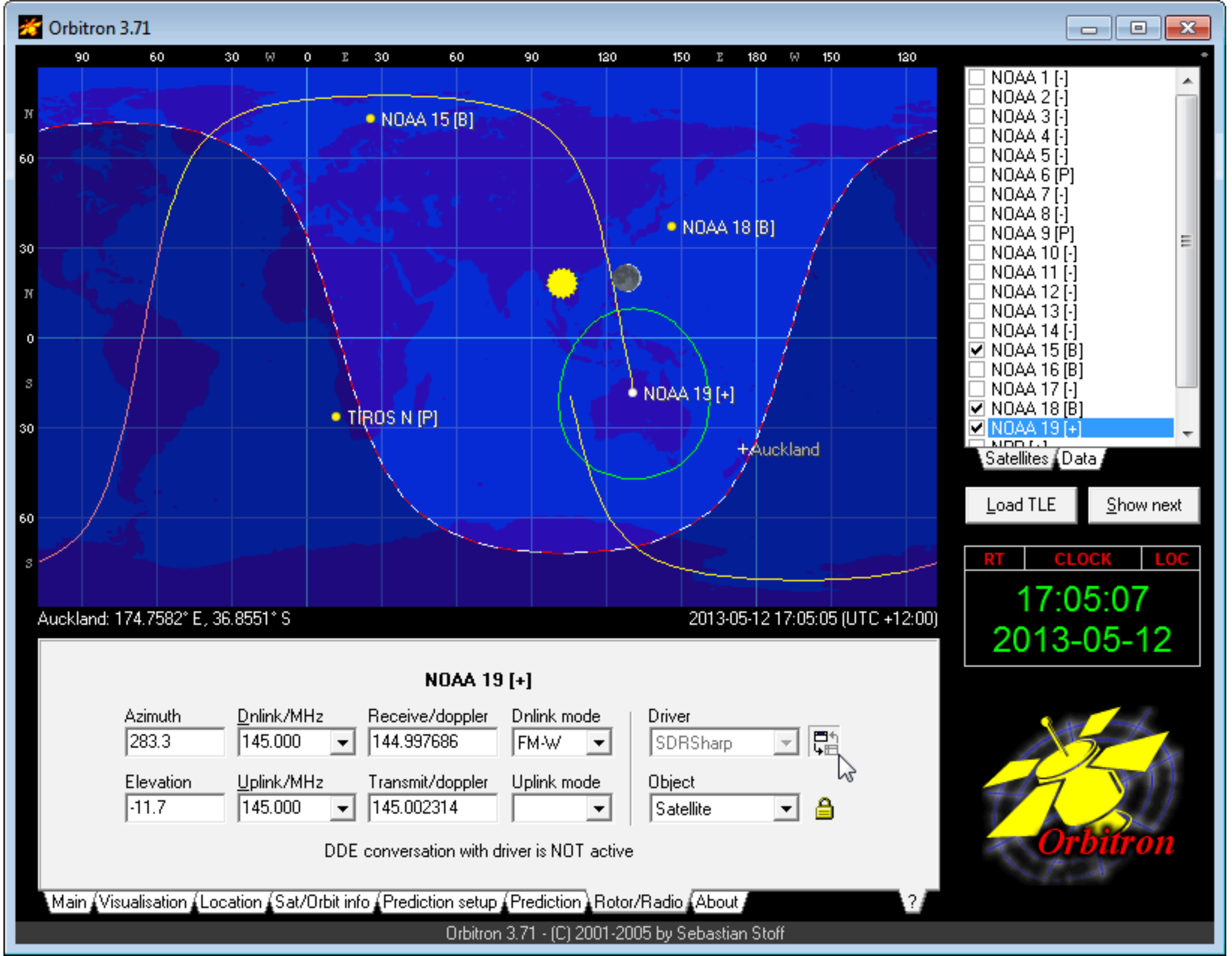
- Once the antenna is attached, if you tune into one of the following stations, you may start receiving the “audio”
  - NOAA 15 – 137.6200 MHz
  - NOAA 18 – 137.9125 MHz
  - NOAA 19 – 137.1000 MHz

# Tracking Satellite

- Once the antenna is attached, if you tune into one of the following stations, you may start receiving the “audio”
  - NOAA 15 – 137.6200 MHz
  - NOAA 18 – 137.9125 MHz
  - NOAA 19 – 137.1000 MHz

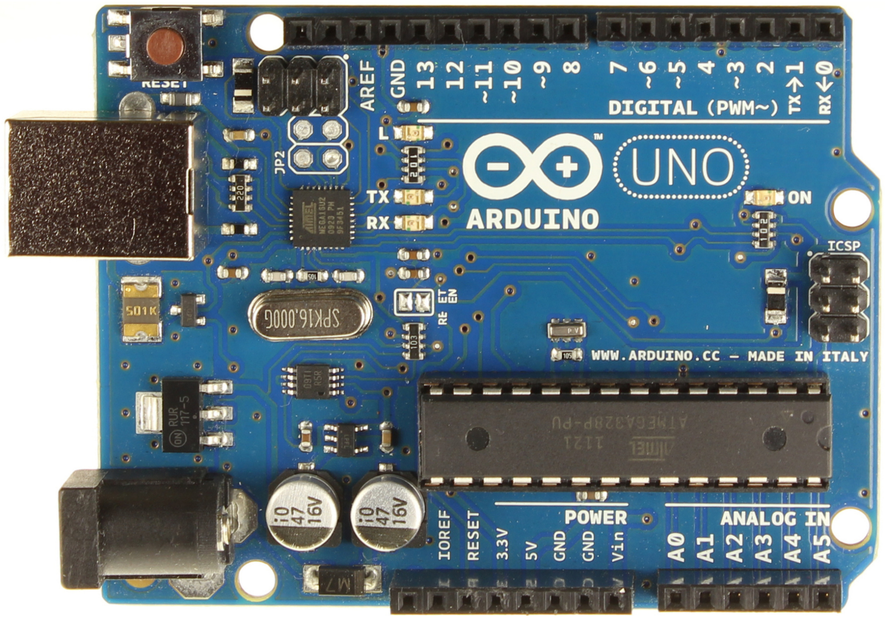
# Decoding the Data

- Through some complicated software, the 1’s and 0’s from the audio stream can be converted back into digital content
  - Orbitron
  - WXtoImg
- The result being satellite imagery and positioning


Orbitron 3.71
NOAA 15 [B]
NOAA 18 [B]
NOAA 19 [+]
TIROS N [P]
Auckland
Auckland: 174.7582° E, 36.8551° S
2013-05-12 17:05:05 (UTC +12:00)
NOAA 1 [-]
NOAA 2 [-]
NOAA 3 [-]
NOAA 4 [-]
NOAA 5 [-]
NOAA 6 [P]
NOAA 7 [-]
NOAA 8 [-]
NOAA 9 [P]
NOAA 10 [-]
NOAA 11 [-]
NOAA 12 [-]
NOAA 13 [-]
NOAA 14 [-]
NOAA 15 [B]
NOAA 16 [B]
NOAA 17 [-]
NOAA 18 [B]
NOAA 19 [+]
Satellites
Data
Load TLE
Show next
RT
CLOCK
LOC
17:05:07
2013-05-12
NOAA 19 [+]
Azimuth
283.3
Dnlink/MHz
145.000
Receive/doppler
144.997686
Dnlink mode
FM-W
Driver
SDRSharp
Elevation
-11.7
Uplink/MHz
145.000
Transmit/doppler
145.002314
Uplink mode
Object
Satellite
DDE conversation with driver is NOT active
Main
Visualisation
Location
Sat/Orbit info
Prediction setup
Prediction
Rotor/Radio
About
?
Orbitron 3.71 - (C) 2001-2005 by Sebastian Stoff


SDR# RSDEV Fork v1.3.1 - IQ Imbalance: Gain = 0.966 Phase = -0.16°
Play
Stop
IQ Stream
Wave file
Radio
NFM
AM
LSB
USB
WFM
DSB
CW-L
CW-U
Frequency
137,912,500
Center
138,695,797
Shift
-8,333
Front end
RTL-SDR / RTL2832U
Filter type
Blackman-Harris
Filter bandwidth
30000
Filter order
10
Squelch
CW Shift
Step size
Snap to grid
12.5 kHz
Correct IQ
Swap I & Q
Mark Peaks
Audio
AF Gain
Samplerate
48000 sample/sec
Input
[MME] Microsoft Sound M...
Output
[MME] Microsoft Sound M...
Latency (ms)
100
Filter Audio
AGC
Use AGC
Use Hang
Threshold (dB)
100
Decay (ms)
100
Slope (dB)
0
FFT Display
View
Both
Window
Blackman-Harris
Resolution
32768
Gradient
S-Attack
137.750MHz
137.875MHz
138.000MHz
138.125MHz
WXtoImg Recording
File
Satellite
Enhancements
Options
Projection
Image
Help
Image
Audio Files
Raw Images
Saved Images
Recording NOAA 18 (unprocessed data shown)...
2012-08-19 03:22 UTC
NOAA 18 Elev: 38.3° Azi: 18.3° 7:49 / 11:40
Recording NOAA 18 (northbound 59 E) on 137.9125 MHz from 03:14:27 UTC...
64%
50%

# Pranks?


DIGITAL (PWM~)
UNO
ARDUINO
ON
ICSP
WWW.ARDUINO.CC – MADE IN ITALY
POWER
ANALOG IN

+

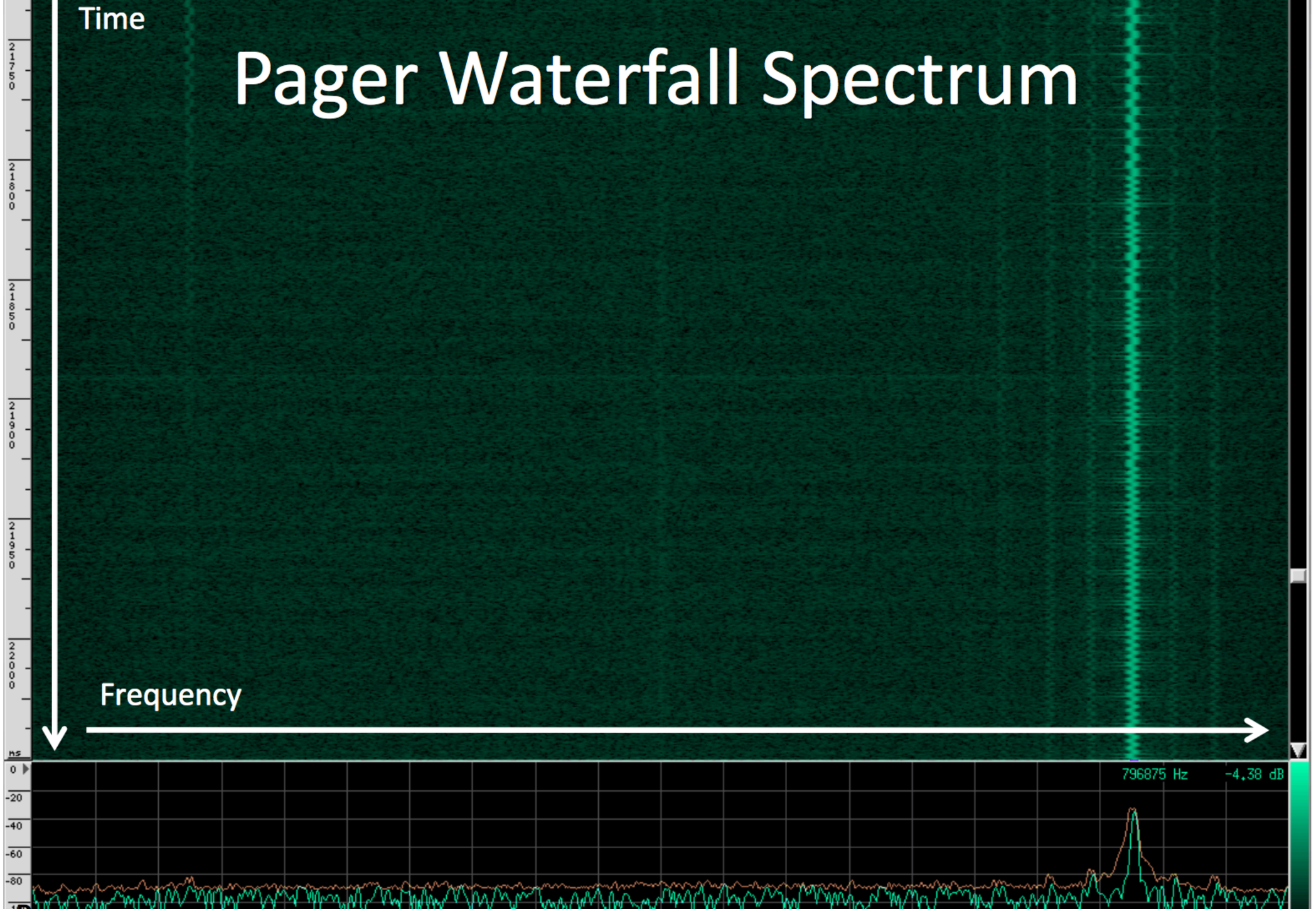
# Jared Boon

- Tire Pressure Monitoring System (TPMS)
- All cars in the US sold after 2008 have it
- We should know if one of our tires are low
- Guess what? There’s no “wire” going into your tire to check the pressure, it’s wireless ☺

# TPMS

- The signals have some really rudimentary protection on them, but Jared was able to demodulate them
- He could get each tire’s pressure from 30-50 feet away depending on the TPMS module
- Probably not a goldmine of information but interesting nonetheless

# Balint Seeber – Applications Specialist


Time
Pager Waterfall Spectrum
Frequency
796875 Hz
-4.38 dB

Decoder 0

- [ ] From beginning
- [x] From start offset

Offset: 0

- [ ] Extend Offset
- [x] Sync settings
- [x] Show bits

Columns: 4

- [ ] Invert
- [ ] Invert first bit
- [ ] Straight
- [ ] Flip Flop
- [ ] Diff
- [ ] Diff (inverted)
- [ ] Prev 0
- [ ] Prev 1
- [x] Manchester 0 (IEEE)
- [ ] Manchester 1 (orig)
- [ ] Diff Man 0
- [ ] BPM
- [ ] Diff Man 1
- [ ] BPS

- [ ] Baudot
- [ ] 7-bit ASCII
- [x] 8-bit ASCII
- [x] Swap endian-ness
- [x] Enforce control bits
- [ ] Start bit
- [x] No stop bits
- [ ] Stop bit
- [ ] Two stop bits

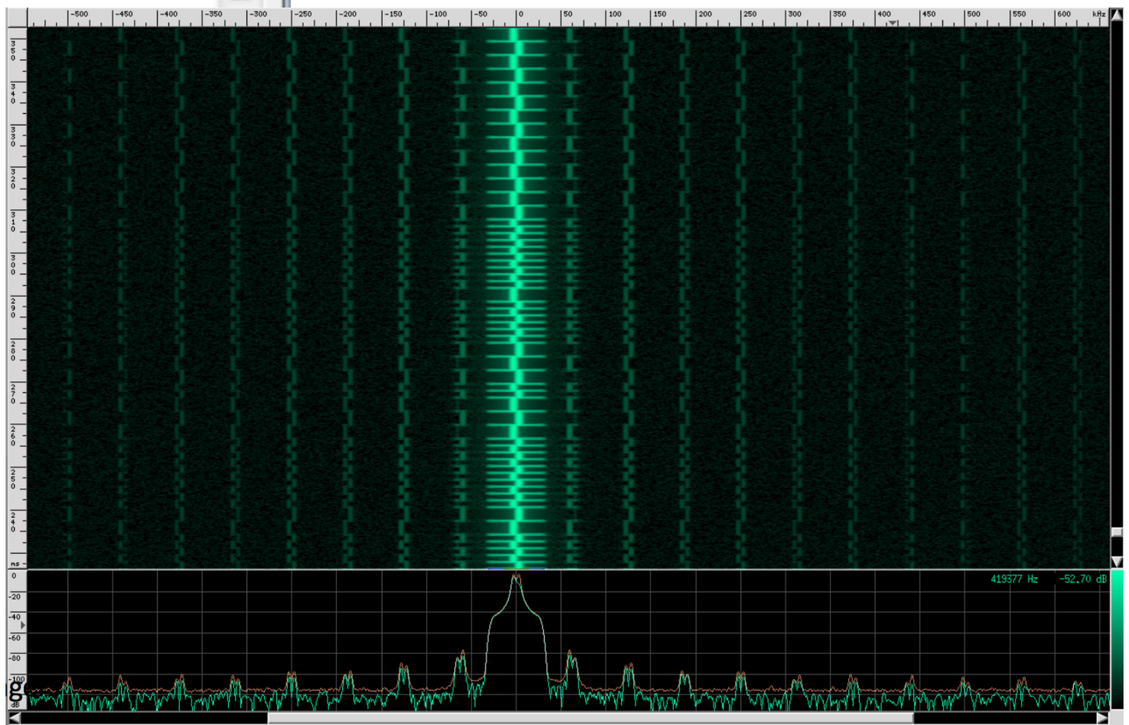
- [x] Highlight differences
- [ ] Show decoded data
- [ ] Accumulate data
- [ ] Extra newline

Max bits: 4096

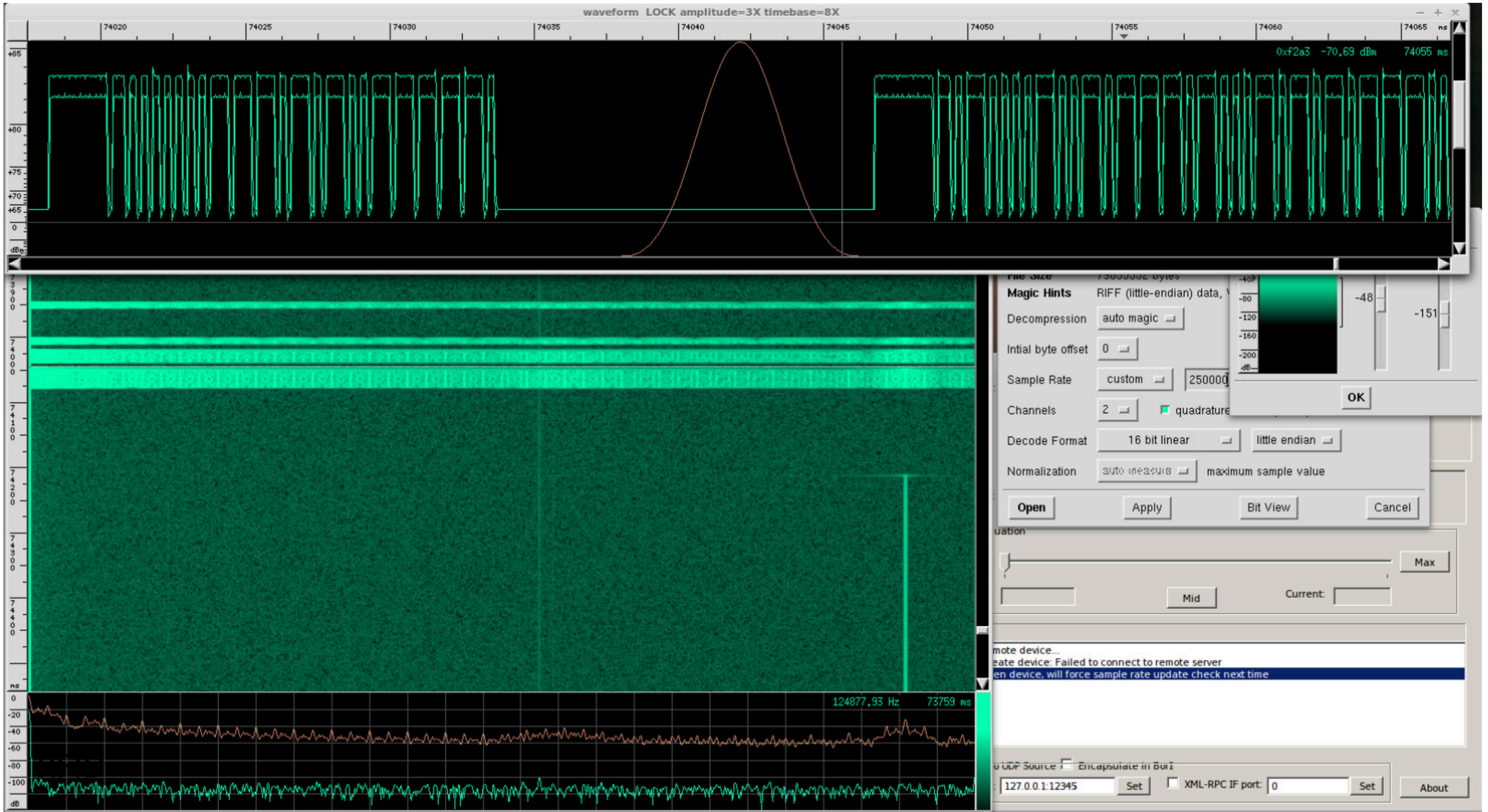
Dump Clear

```
000     10101010 10101010 10101010 11111100     aa aa aa fc     ....
004     00101101 00000010 00001000 00001100     2d 02 08 0c     -...
008     00000000 00000000 00000000 00000000     00 00 00 00     ....
012     00000000 10000001 11000001 0    00 81 c1 ...<7 left>

Sum: C1
LRC: FFFFFC42
CRC Poly D5 Start 00: 03
CRC Poly D5 Start FF: A9
CRC Poly AB Start 00: 2E
CRC Poly AB Start FF: 78
CRC Poly EA Start 00: DB
CRC Poly EA Start FF: 71
```



# Toyota Prius Keyless Entry



# More Ideas

- Building security badges
- Gated communities
- Doorbells
- Remote controlled power outlets