

0x01 Software Defined Radio (SDR)

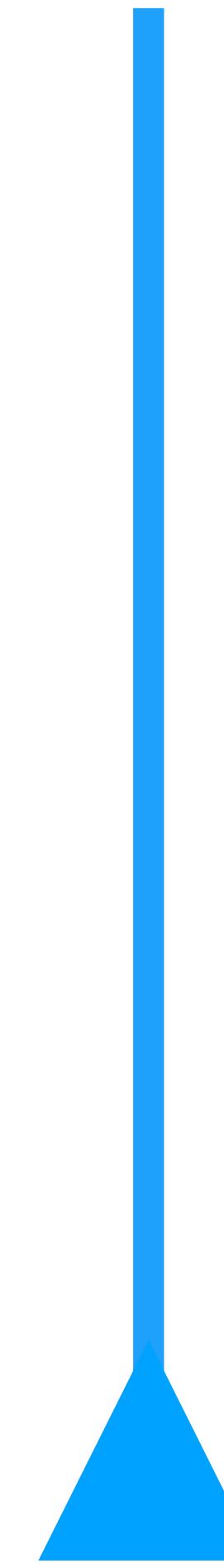
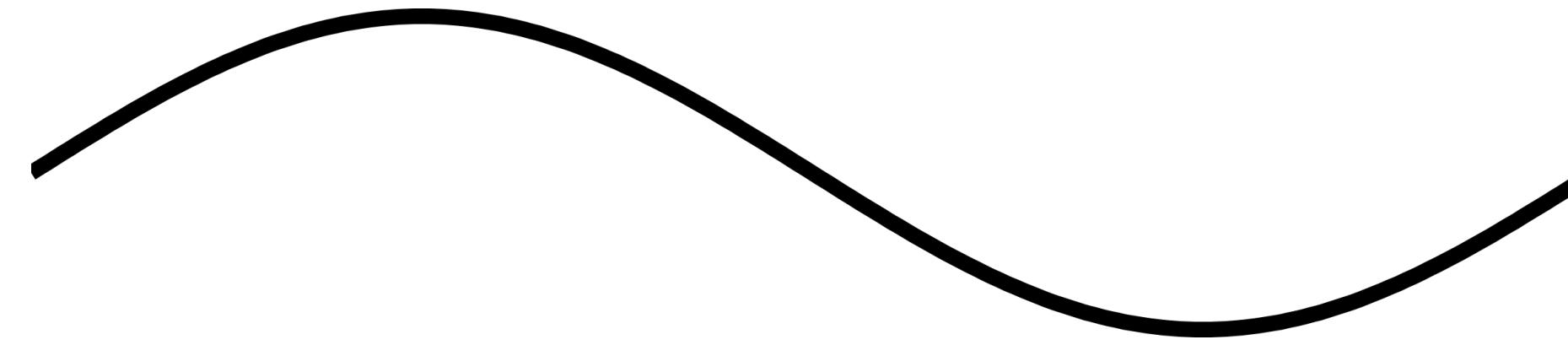
Dr. Mike Ham

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

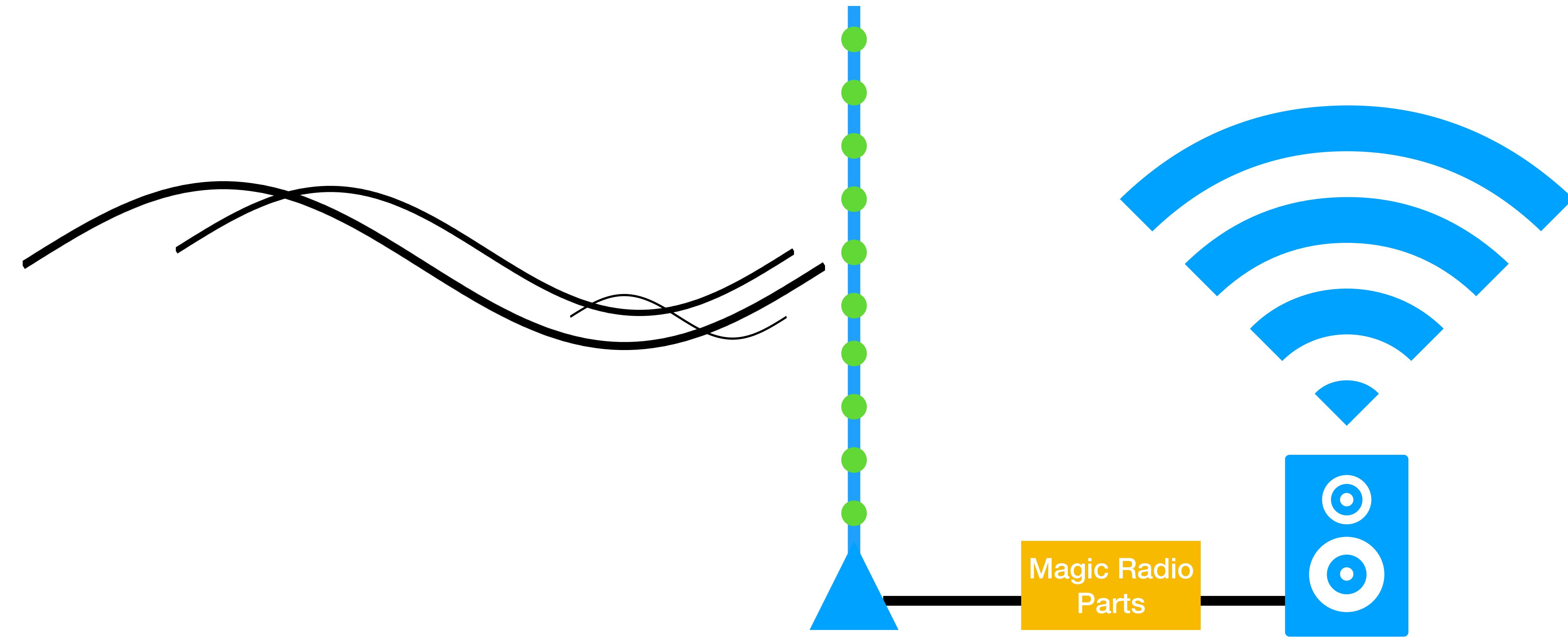
**What radio waves surround
you?**

Get creative!

Radio 101



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

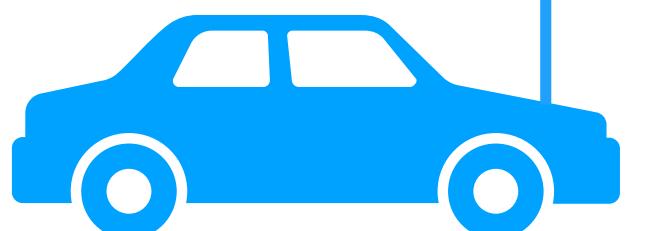
AM Radio Antenna

- Typical frequency around 1000kHz (kilohertz)
 - FM radio operates around 100MHz (megahertz)
 - $1 \text{ MHz} = 1000\text{kHz}$
- 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

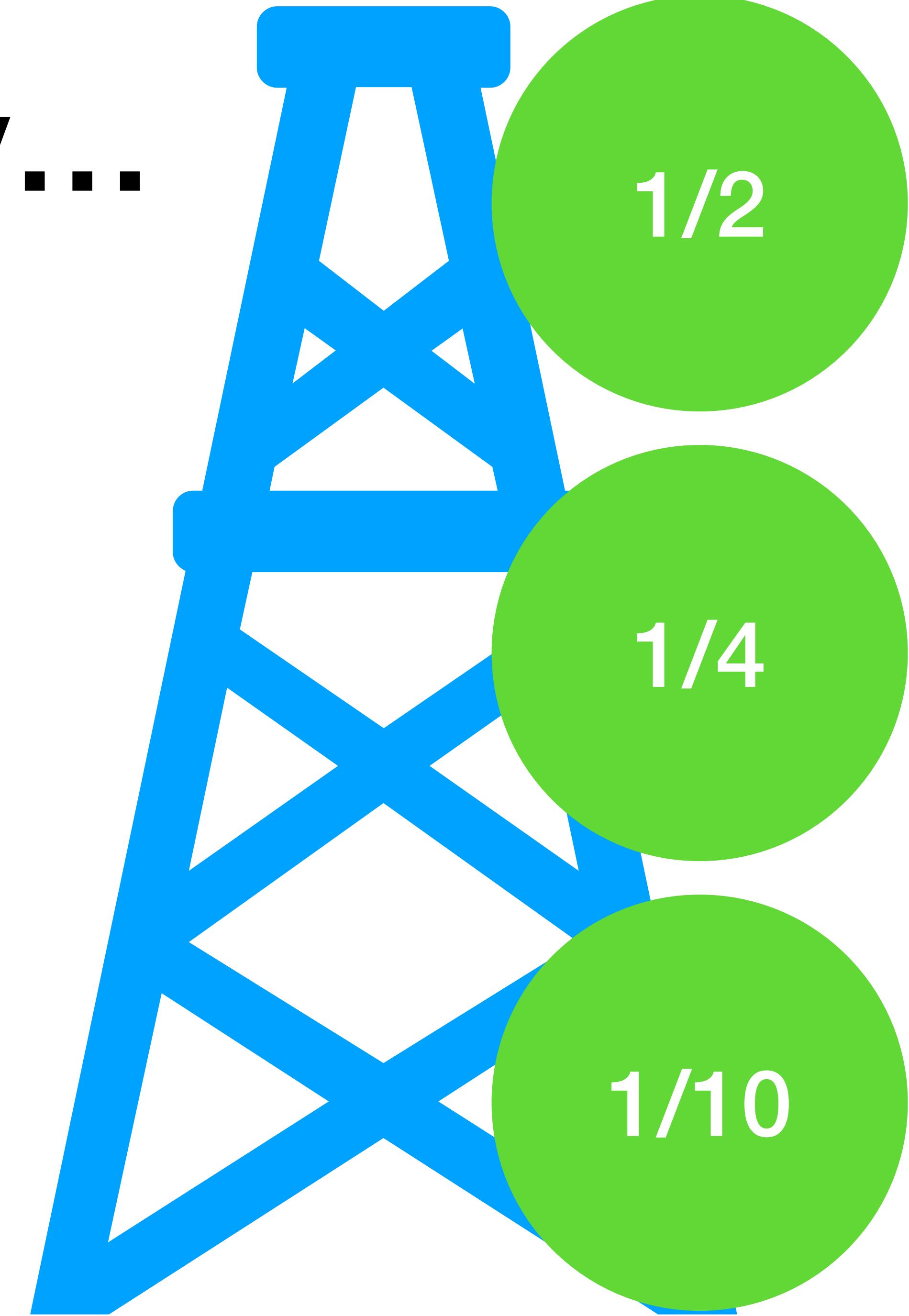
- Simple calculation: $m = 300 / \text{frequency MHz}$
 - If I tune into FM103.1, how long of an antenna do I need?
 - Remember, FM operates in megahertz (MHz)
 - $m \underline{\hspace{2cm}} = 300 / \underline{\hspace{2cm}}$
- What about AM radio which is kilohertz, let's say 1390kHz
 - $m = 300 / (\text{frequency kHz} / 1000)$
 - $m \underline{\hspace{2cm}} = 300 / \underline{\hspace{2cm}}$

AM - 215.83m (708.1ft)



FM 2.91m (9.55ft)

Oh my...

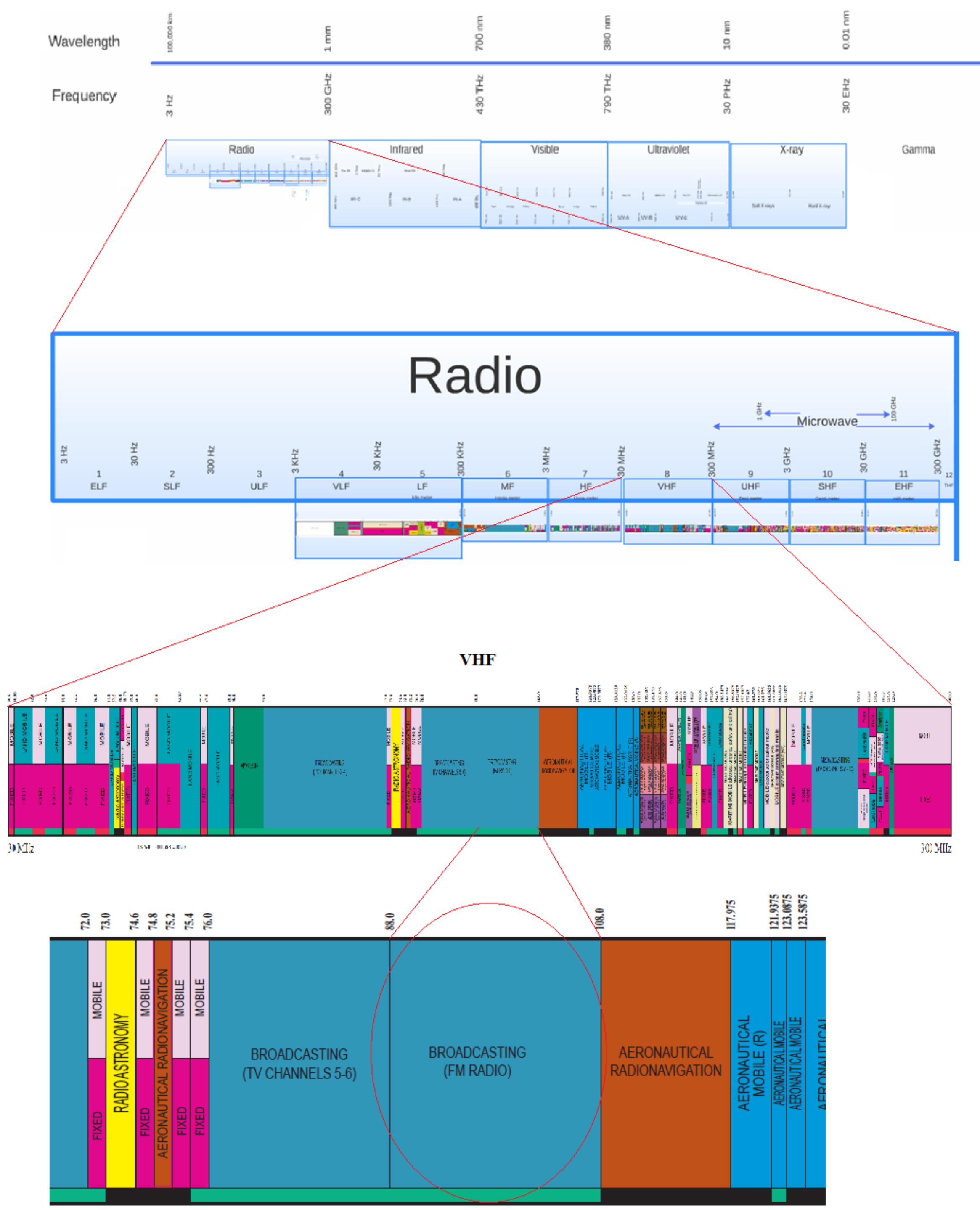


3Hz to 30EHz

3Hz to 3THz

30MHz to 300MHz

88MHz to 108MHz



US Frequency Allocations

- <https://www.ntia.doc.gov/files/ntia/publications/2003-allochrt.pdf>

UNITED STATES FREQUENCY ALLOCATIONS THE RADIO SPECTRUM



ACTIVITY CODE

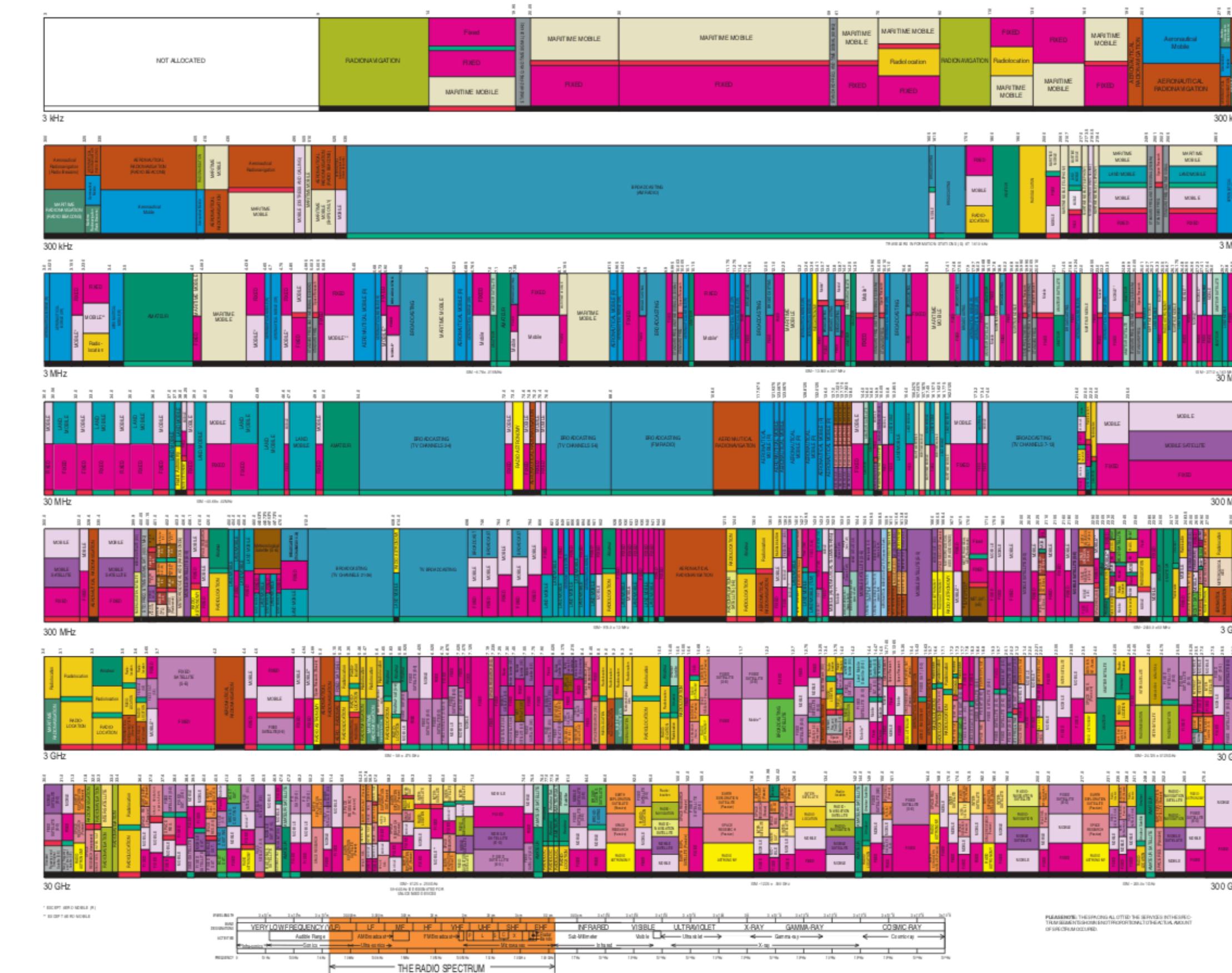
GOVERNMENT EXCLUSIVE	
NON-GOVERNMENT EXCLUSIVE	

ALLOCATION USAGE DESIGNATION

SERVICE	EXAMPLE	DESCRIPTION
Primary	FM102	Capital letters
Secondary	Mobile	For Capital with lower case letters

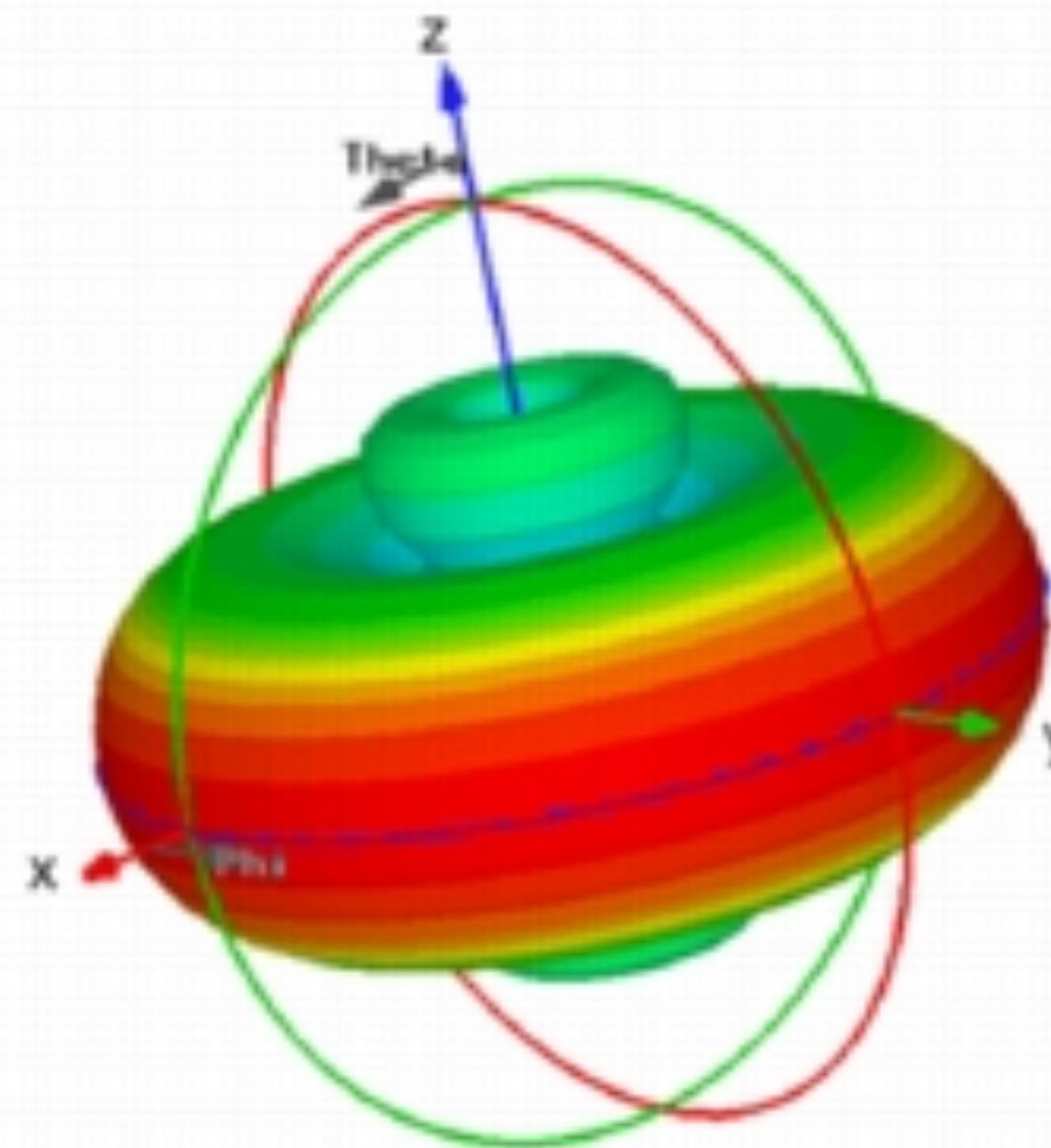
This chart is a key map showing the order of the Tables of Frequency Allocations used by the International Telecommunications Union (ITU) for Radio Frequency Allocation. The order of the tables is the same as in the Tables of Primary and Secondary. These tables are complete lists of allocations, some of which could be found in the Tables of Primary and Secondary. There are no complete lists of allocations, some of which could be found in the Tables of Primary and Secondary.

U.S. DEPARTMENT OF COMMERCE
National Telecommunications and Information Administration
Office of Spectrum Management
October 2003

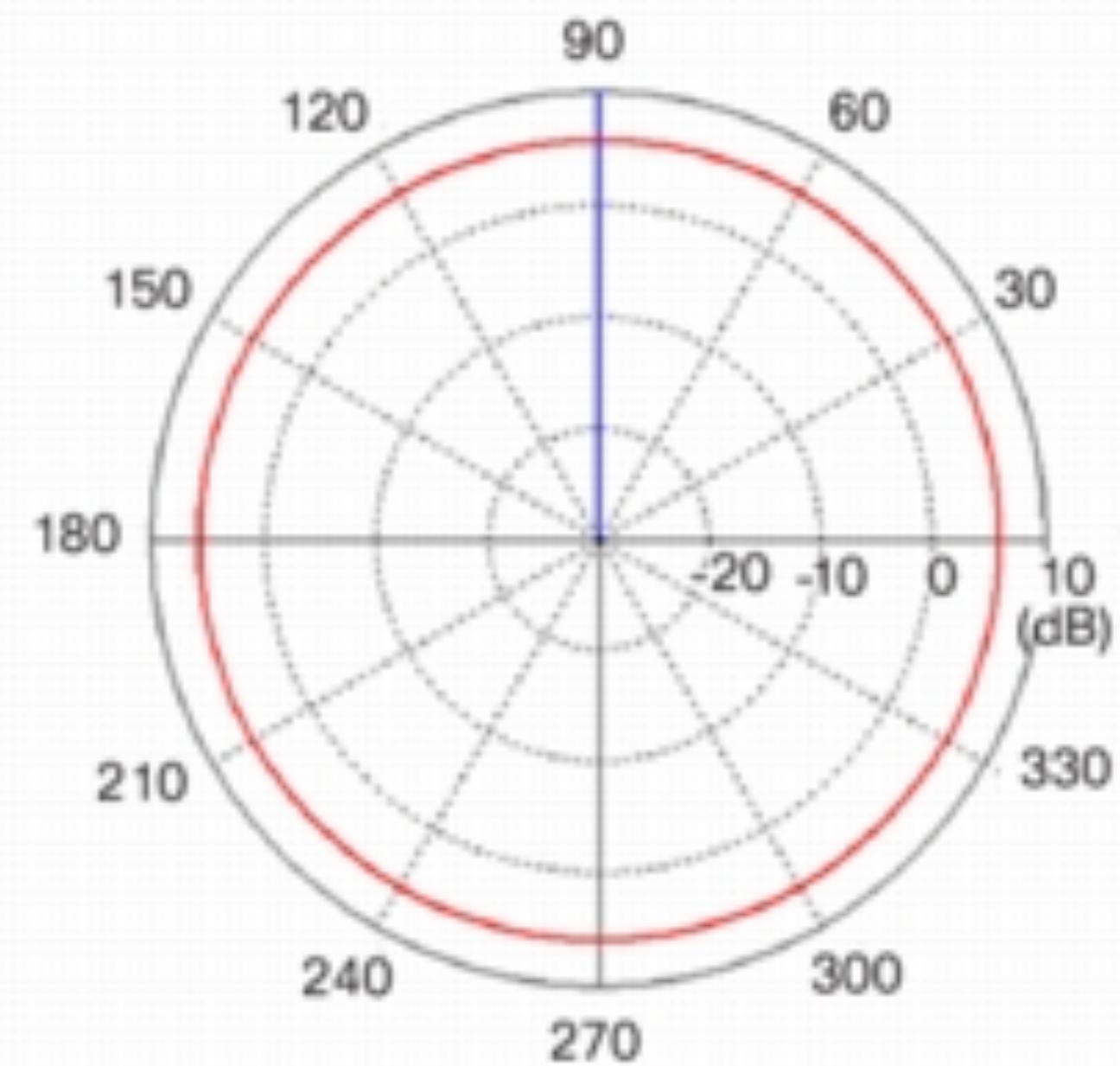


Antenna Types

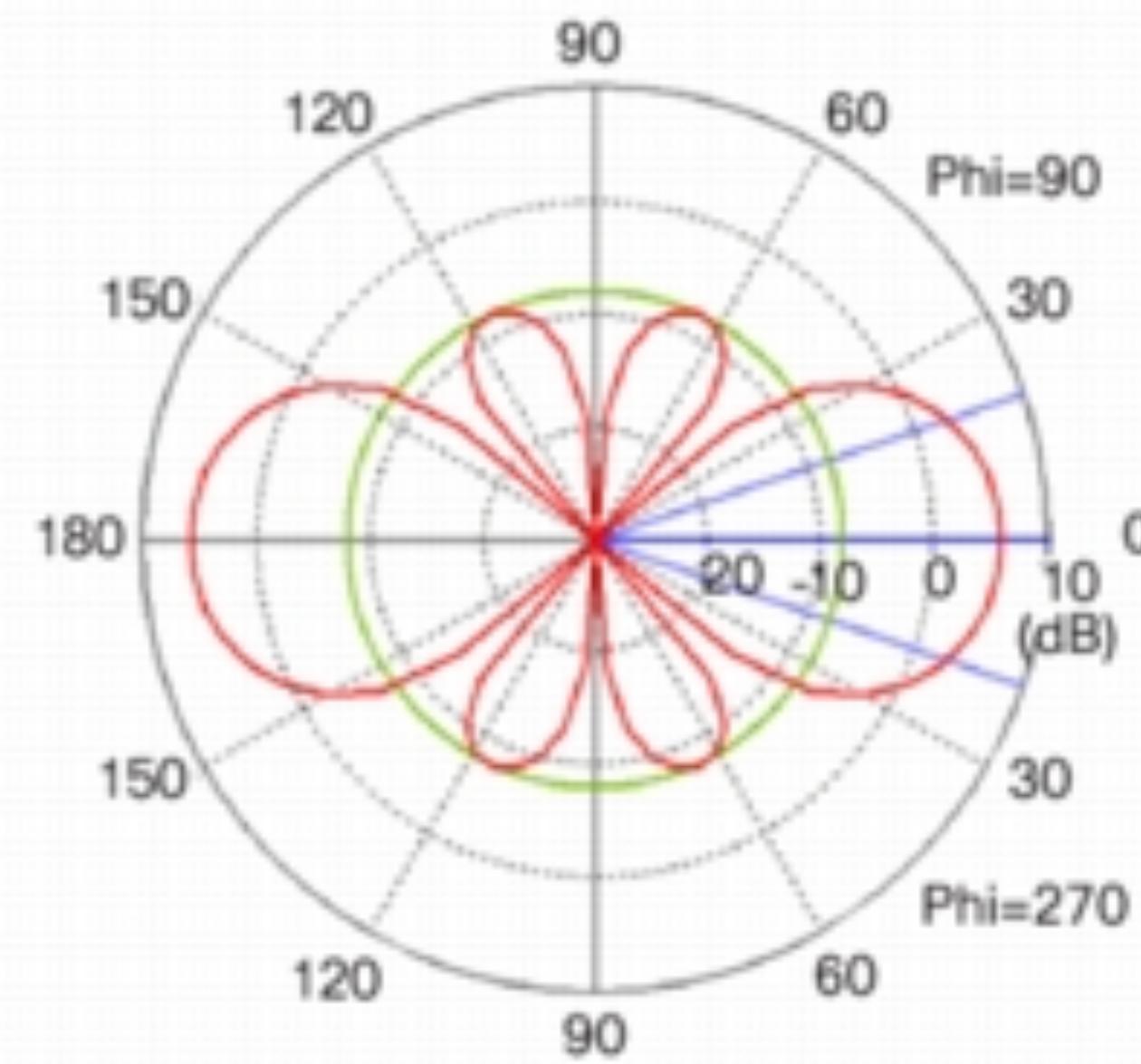
- Omnidirectional
 - Extends your range in all directions
- Directional
 - Let's you focus your signal in a particular direction
- Sensitivity – measured in dBi
 - dBi - gain of an antenna as referenced to an ISOTROPIC (omnidirectional) source
 - Remember, every 3 dBi = double the sensitivity



(a) 5.8 dBi Omni 3D Pattern

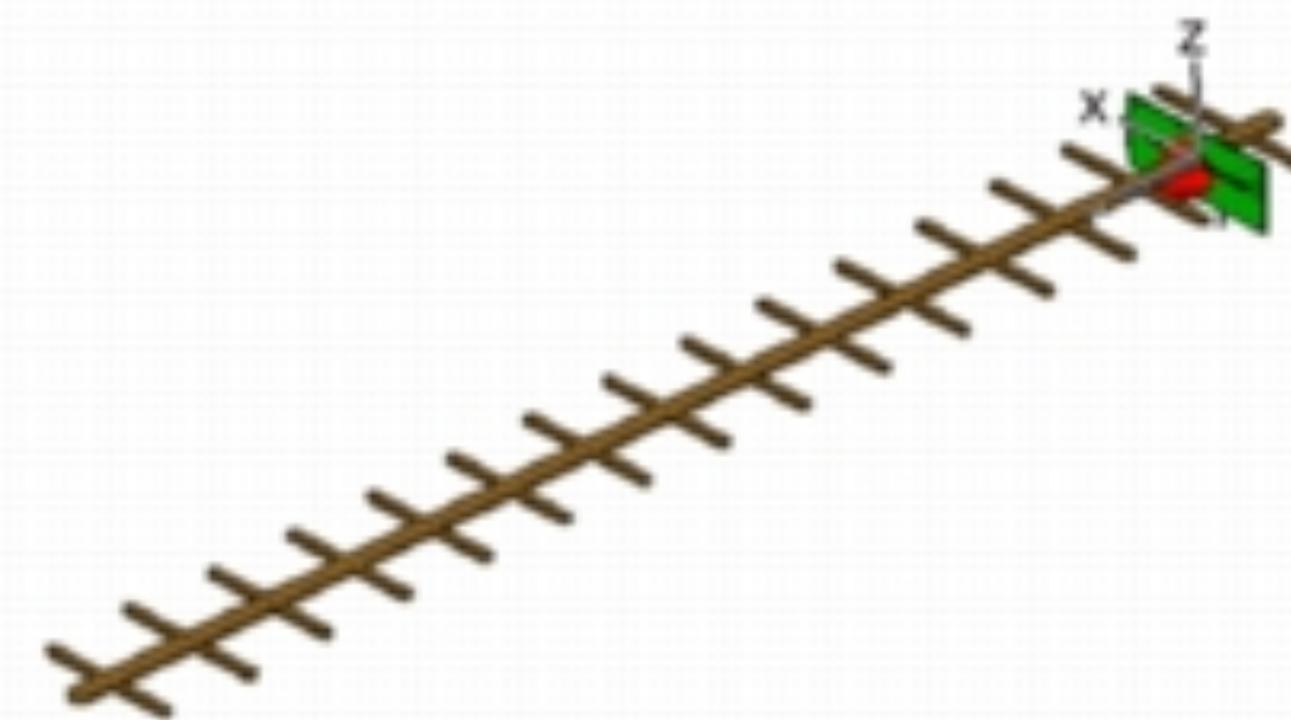


(b) 5.8 dBi Omni Azimuth Plane Pattern

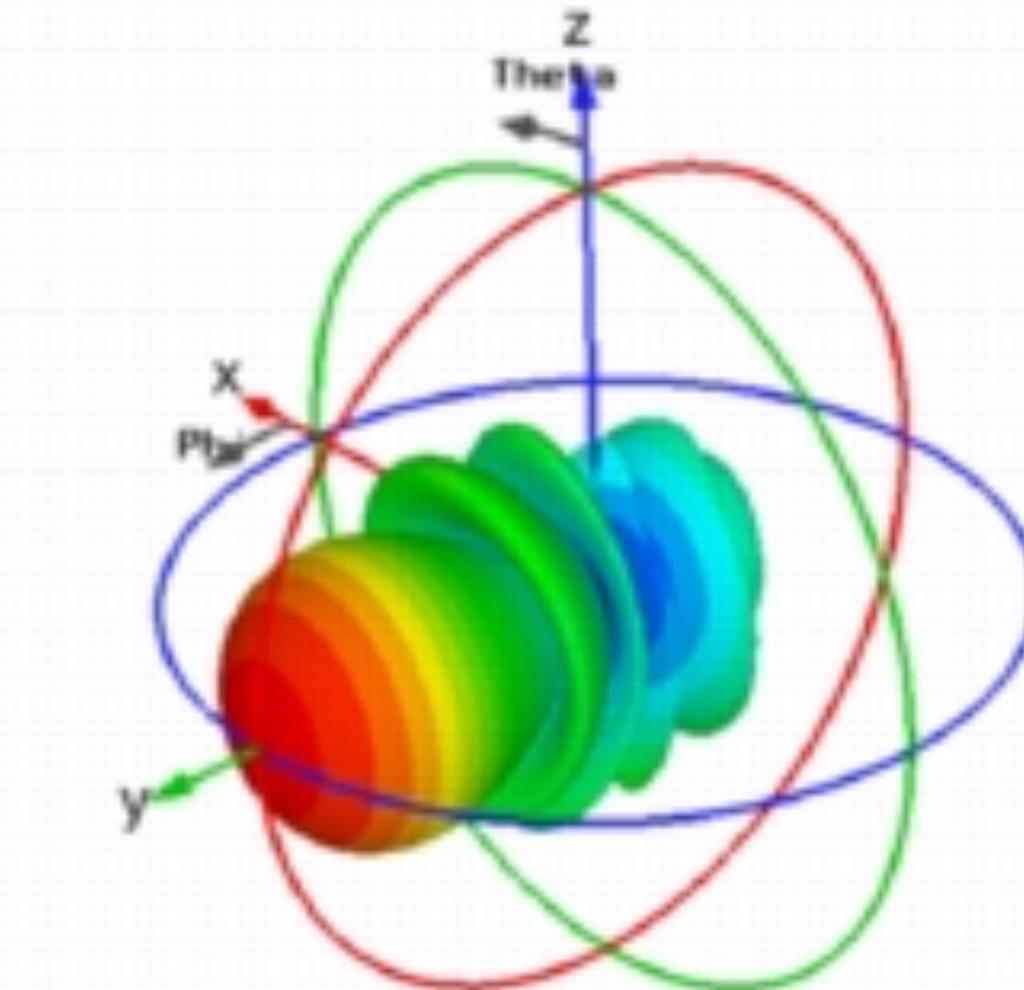


(c) 5.8 dBi Omni Elevation Plane Pattern

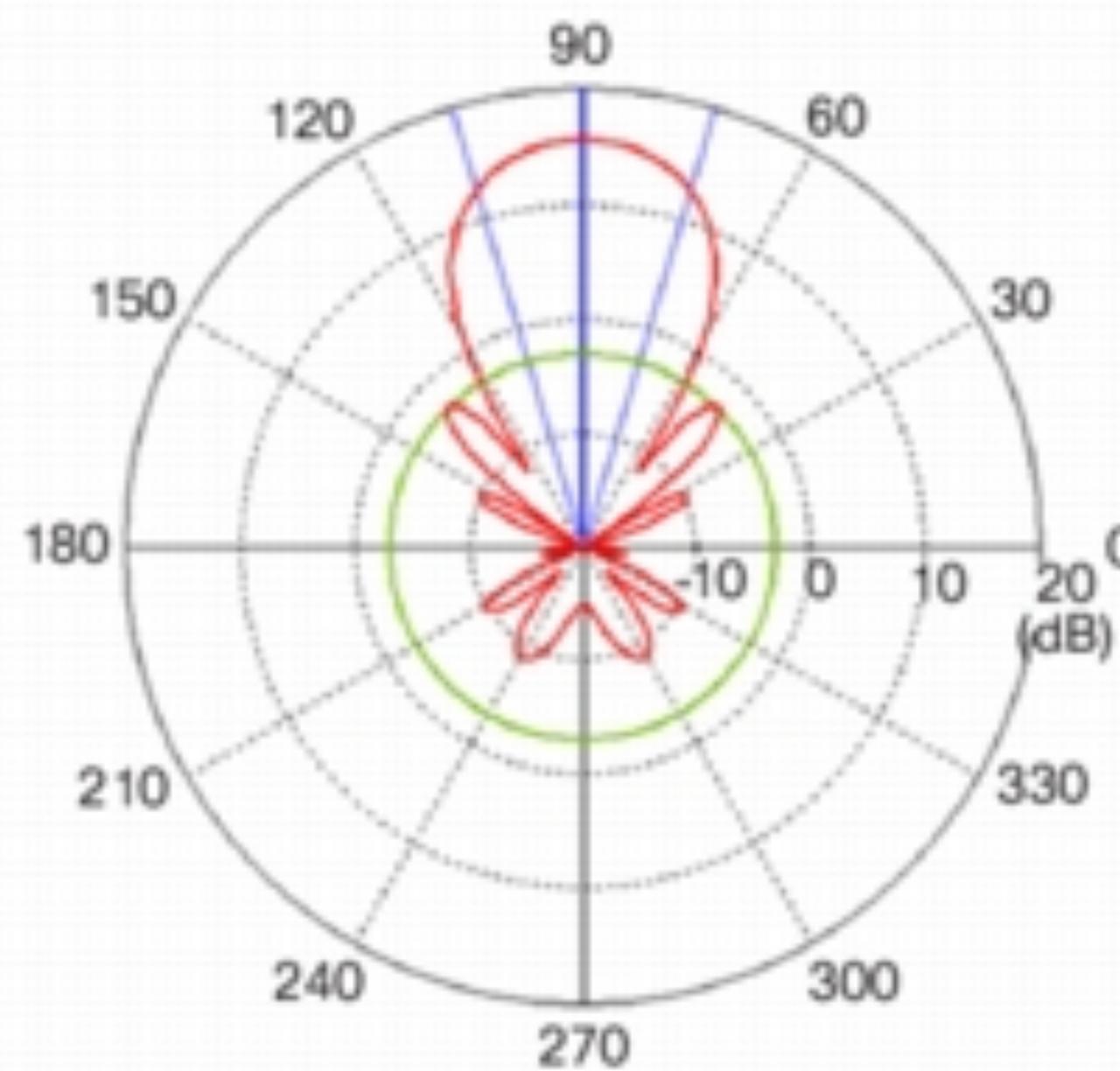




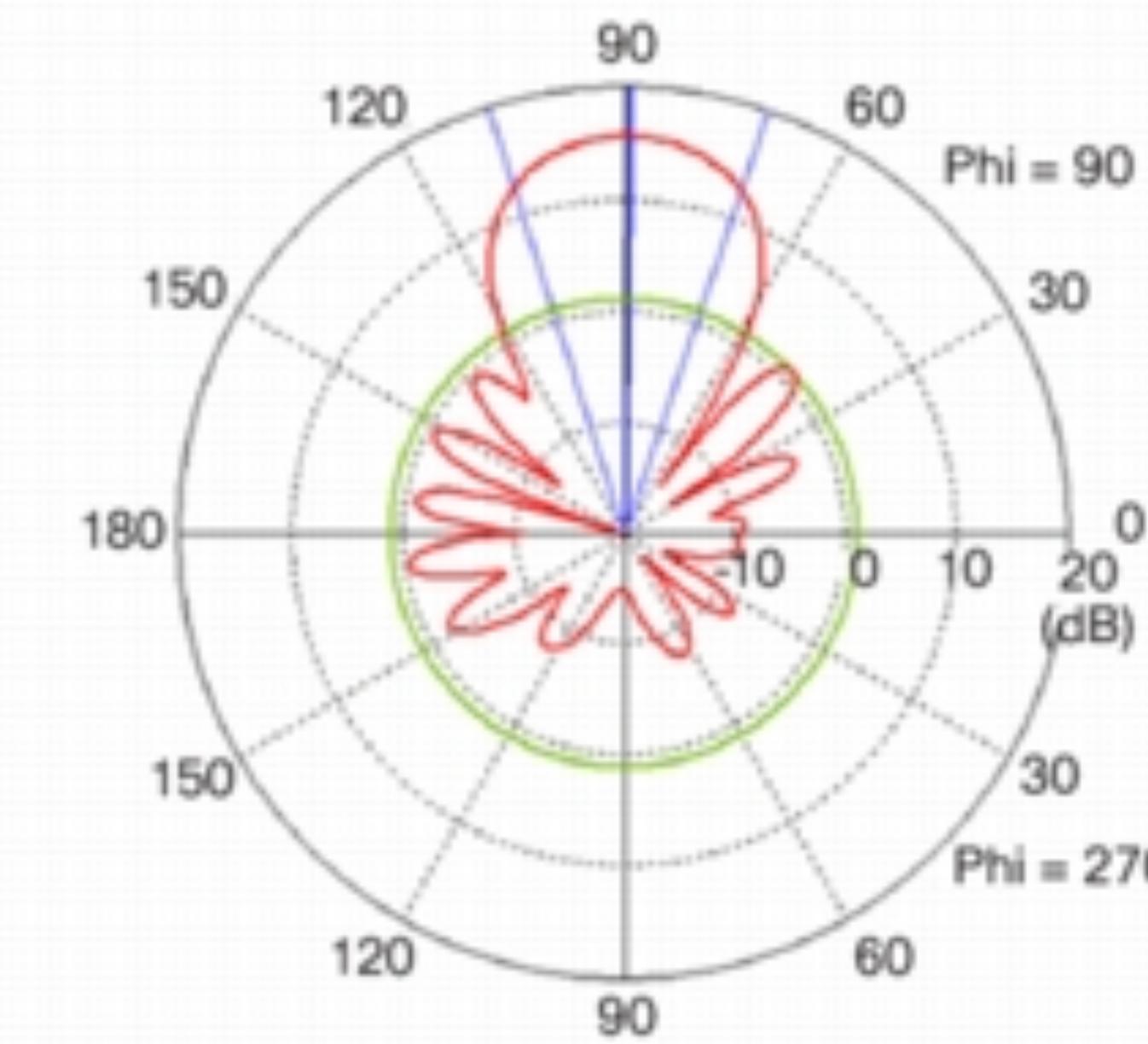
(a) Yagi Antenna Model



(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



What can SDR do?

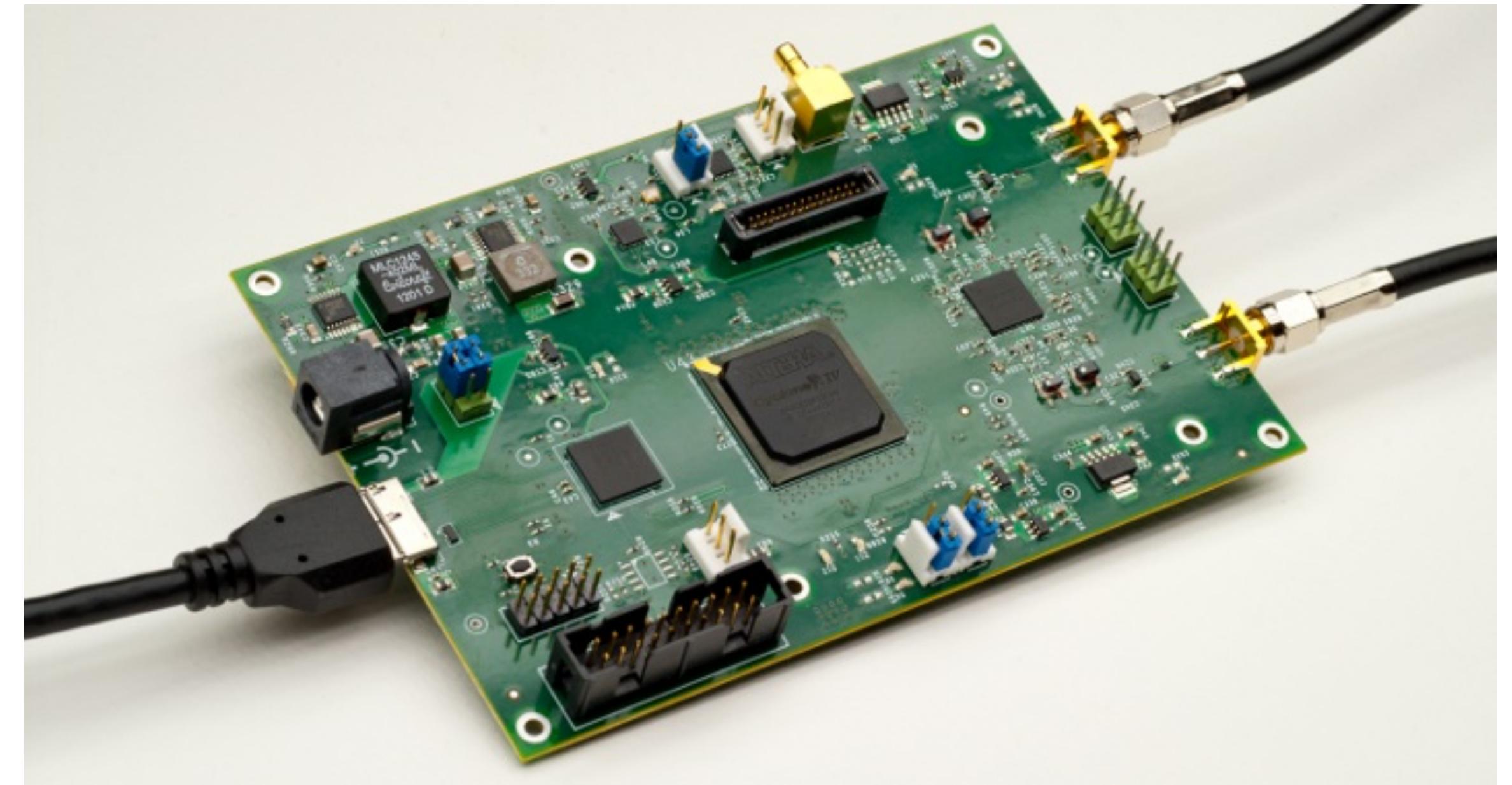
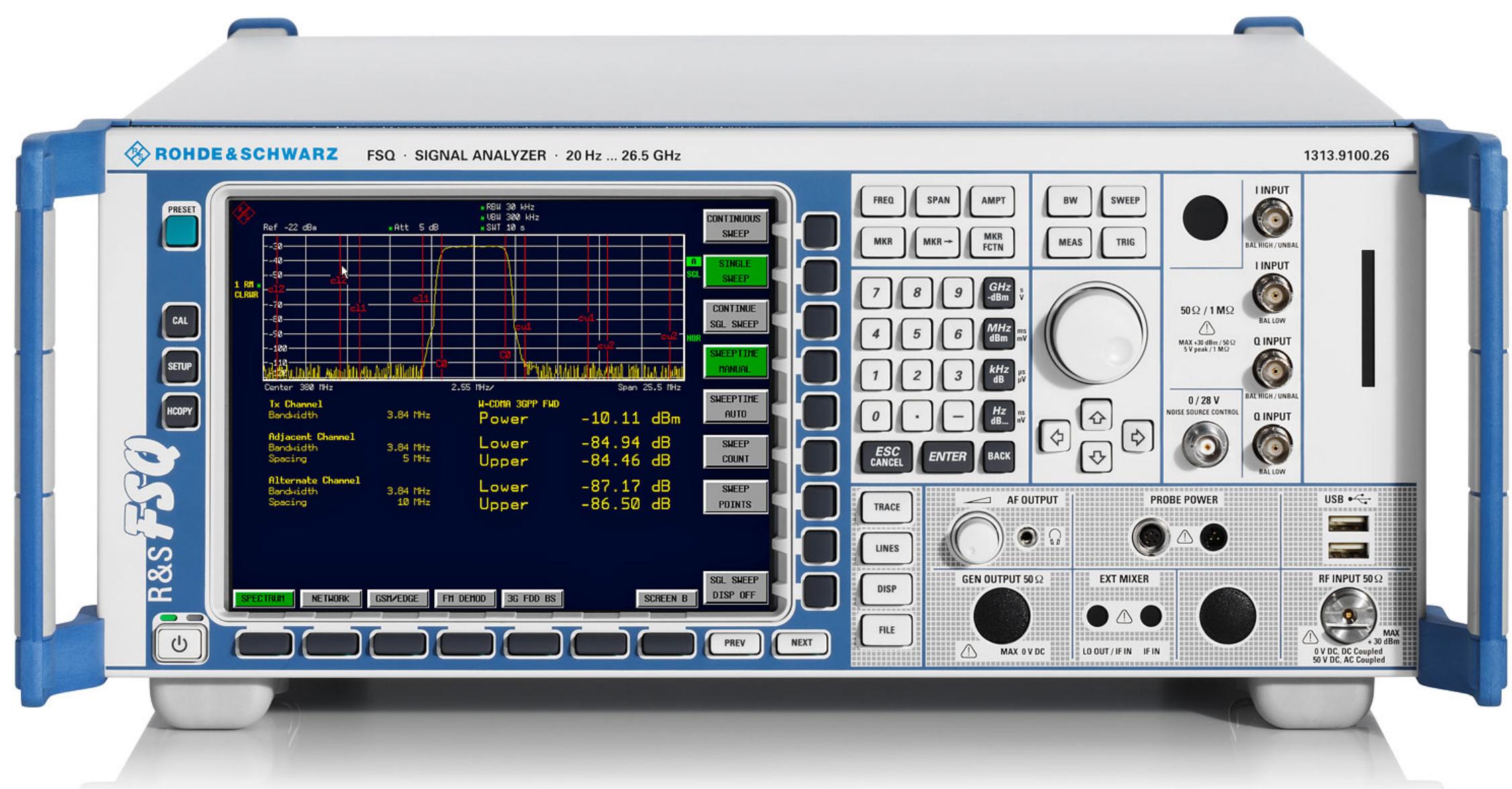
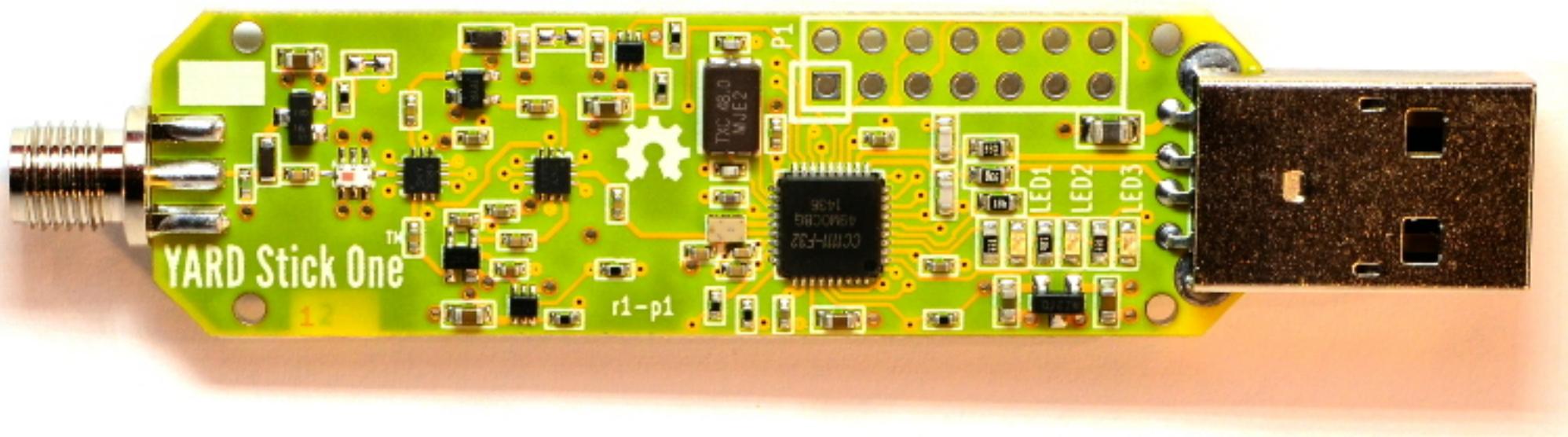
- This can be used as an AM / FM radio, a police scanner, air traffic control listener, etc.
- Receive images from weather satellites
- You're basically packet sniffing with radio
- Isn't that not legit to do?
 - Use common sense when doing stuff like this
 - The antennas you have can only receive not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



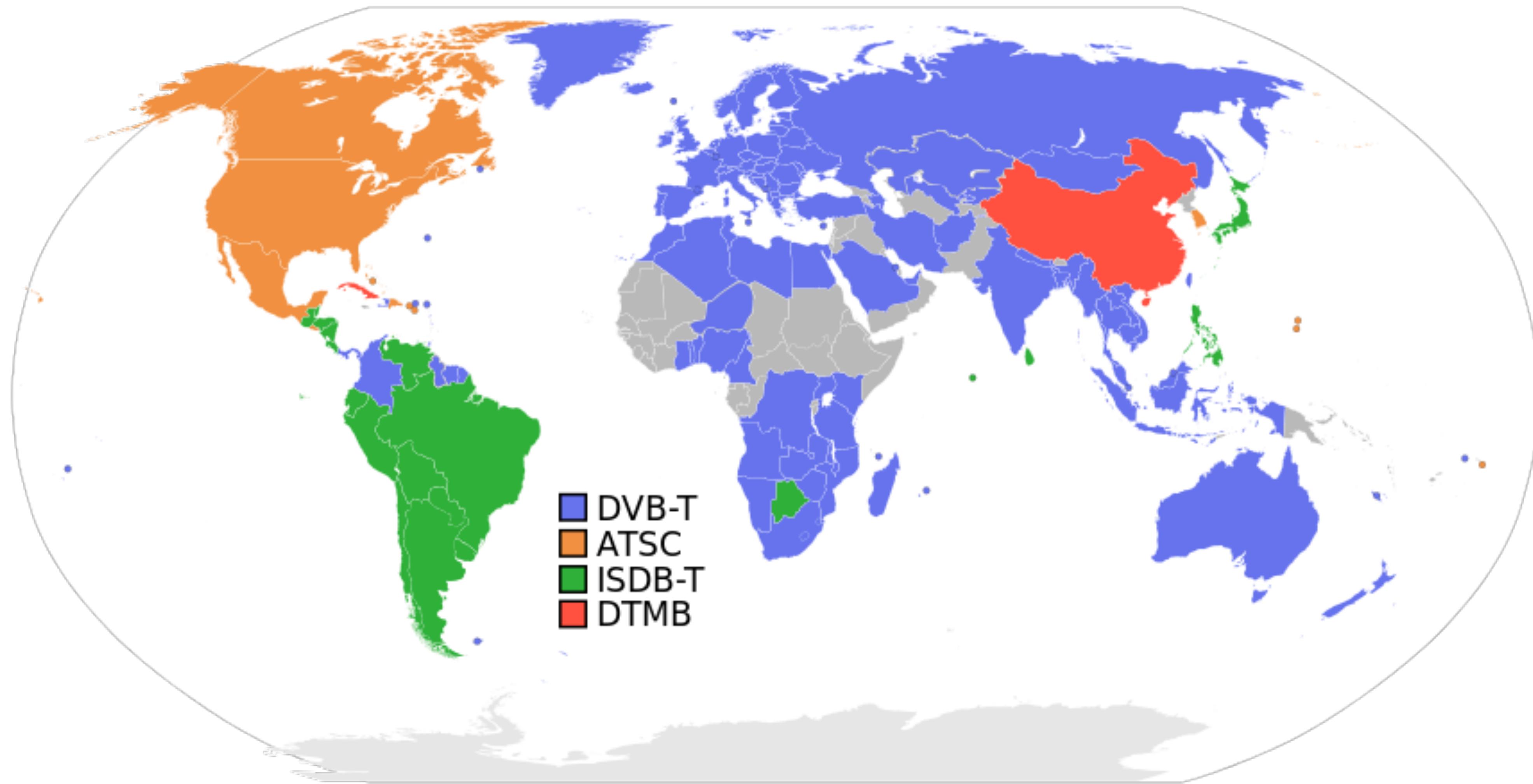
Geeky Specs

- 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?!

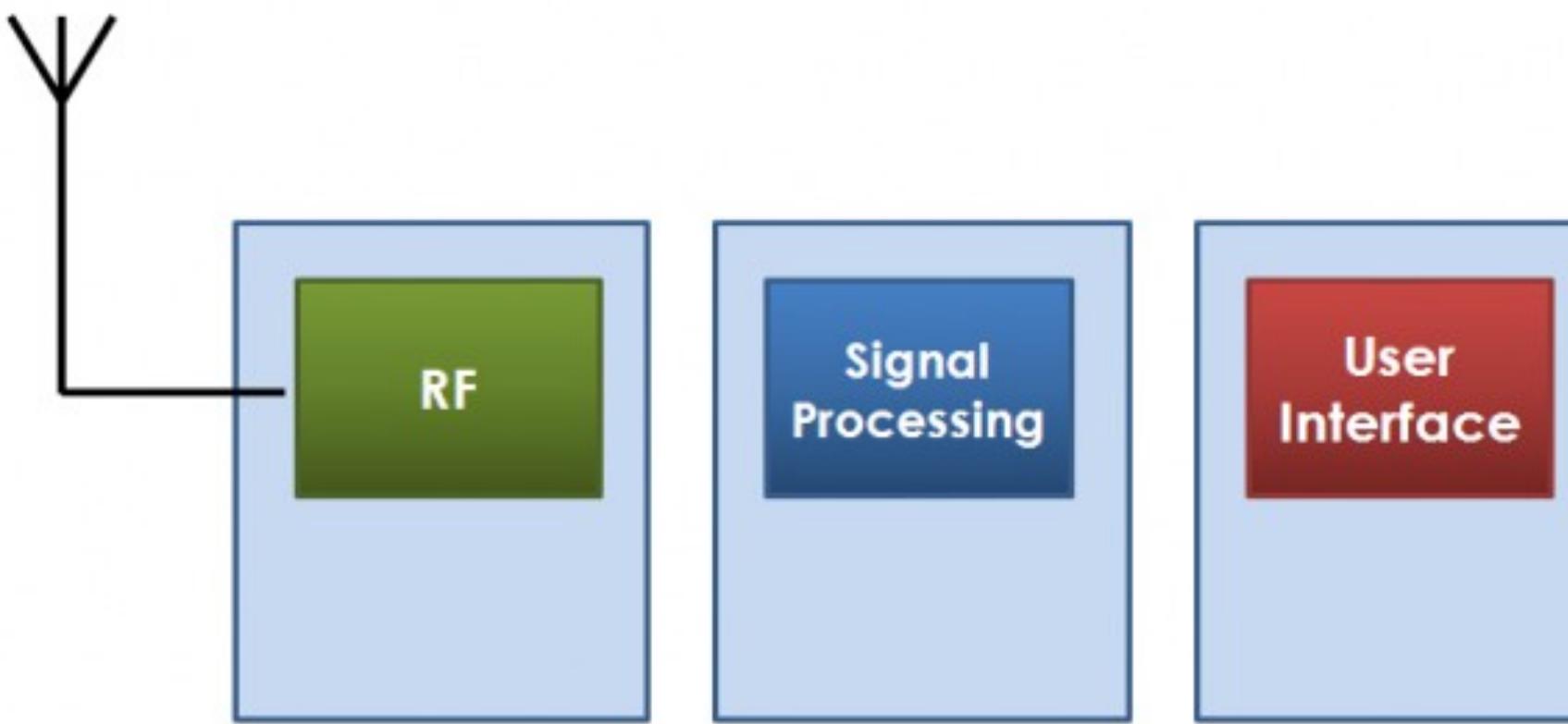


Driver Voodoo

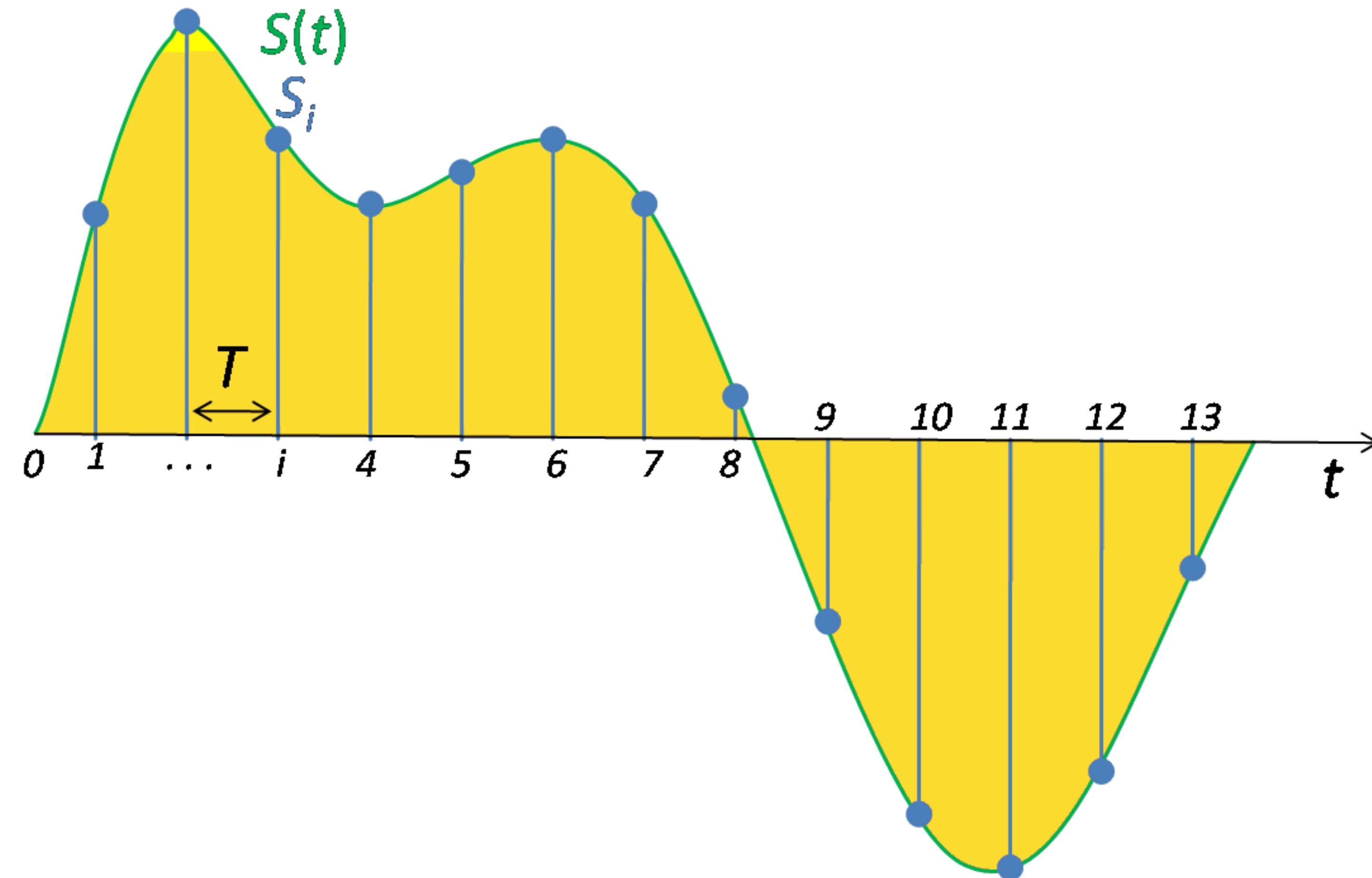
- Some really smart people have crafted a driver for these USB adapters to give us more control
- Driver – software that controls hardware
 - Your mouse, keyboard, printers, etc. all use them
 - Computer has to know how to speak the language of the hardware in order for it to work

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



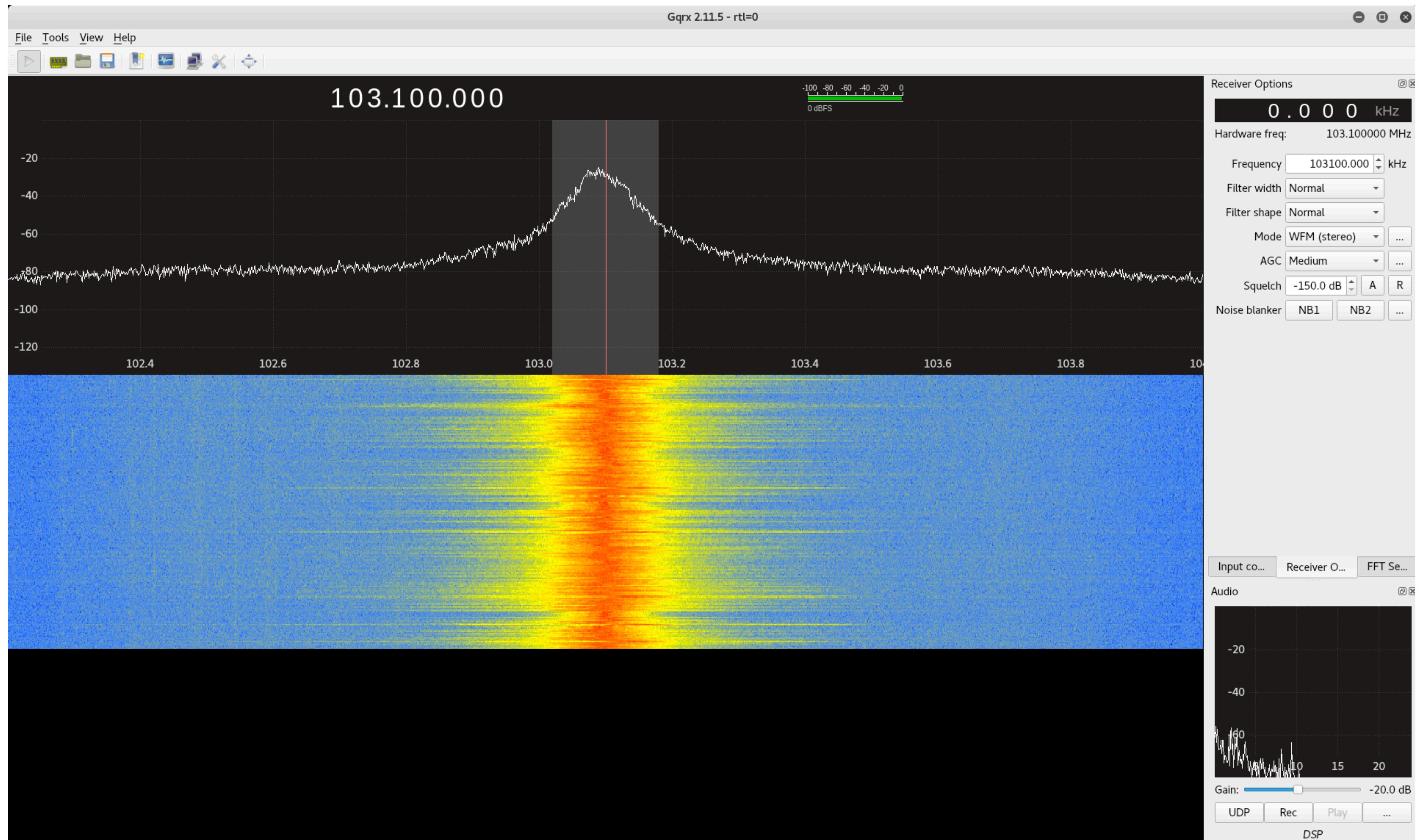
Original \rightarrow Sampled \rightarrow Reconstructed



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!

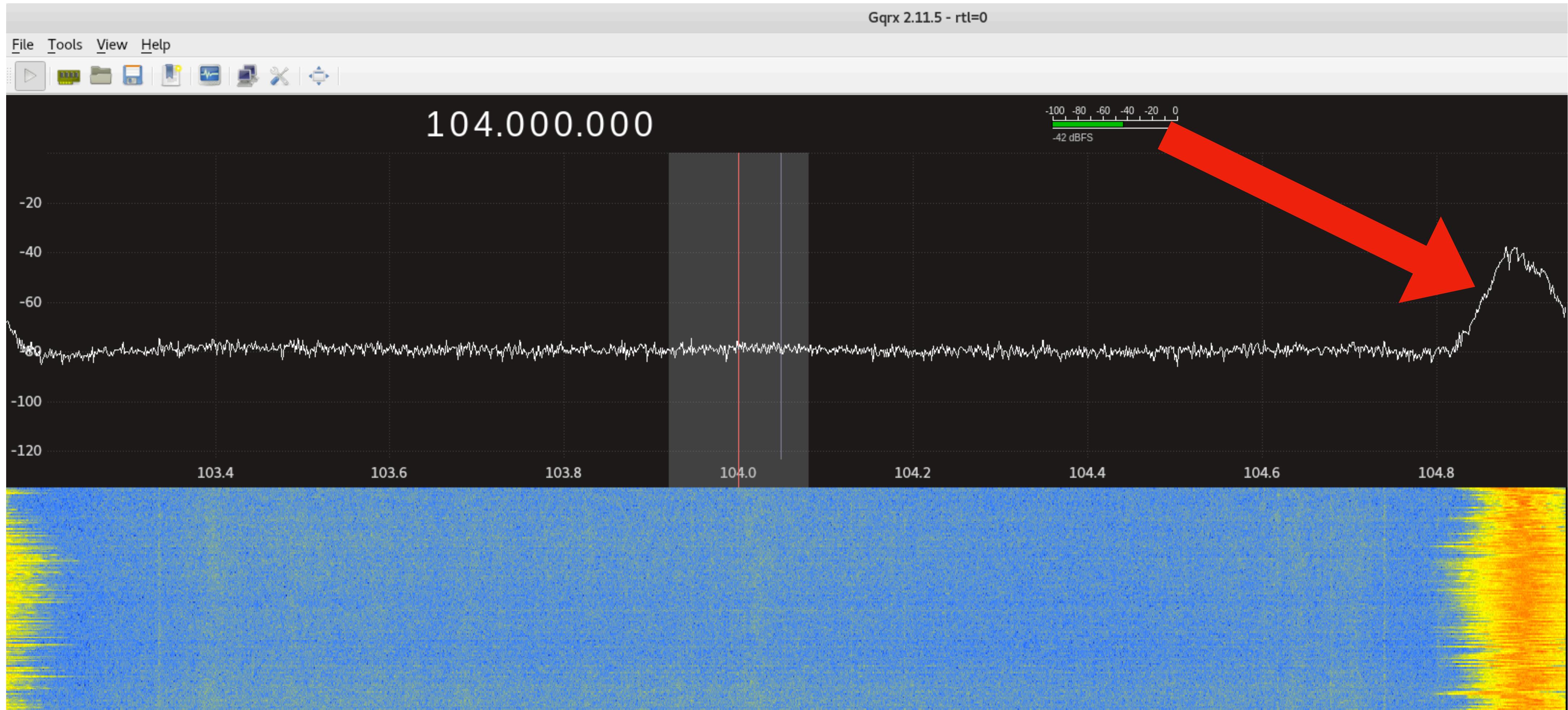
gqrx



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

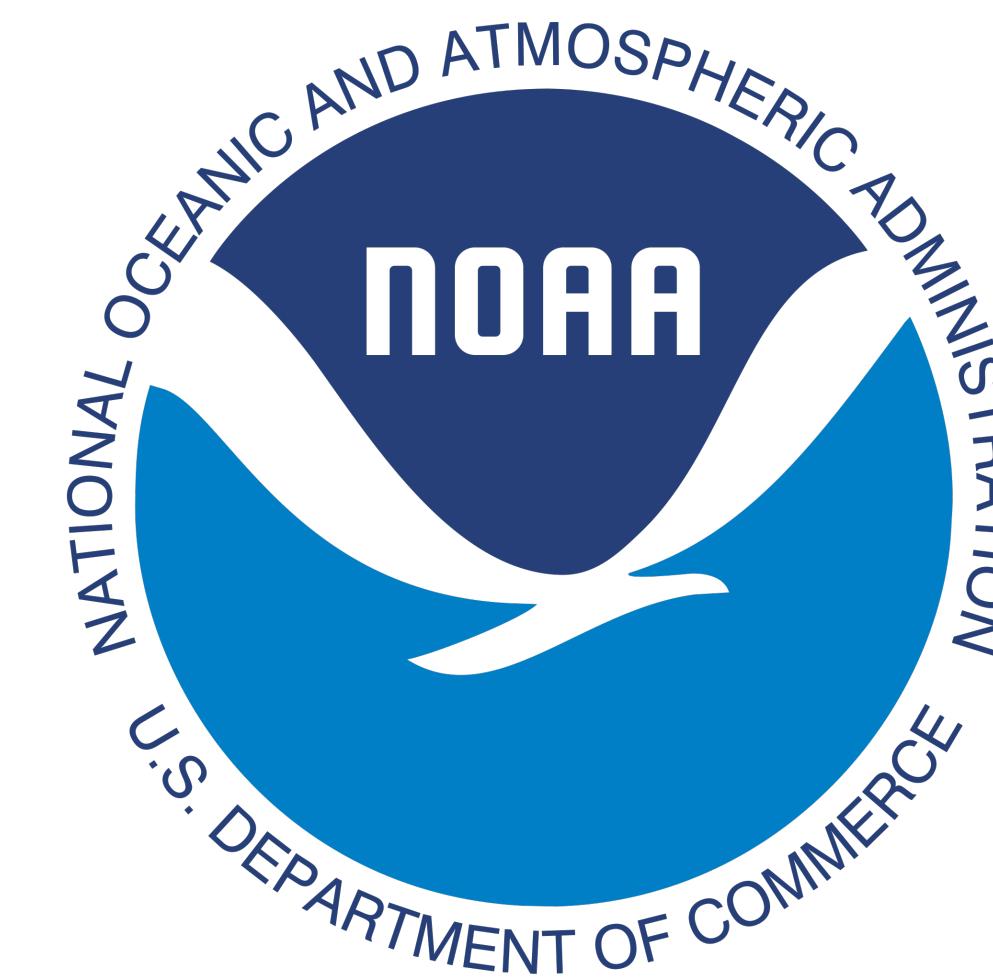
How about Weather Radio

- Most AM/FM radios can't tune into the same weather network
- We've probably all seen one of these...maybe at Grandparents?



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:
 - http://www.nws.noaa.gov/nwr/coverage/county_coverage.html

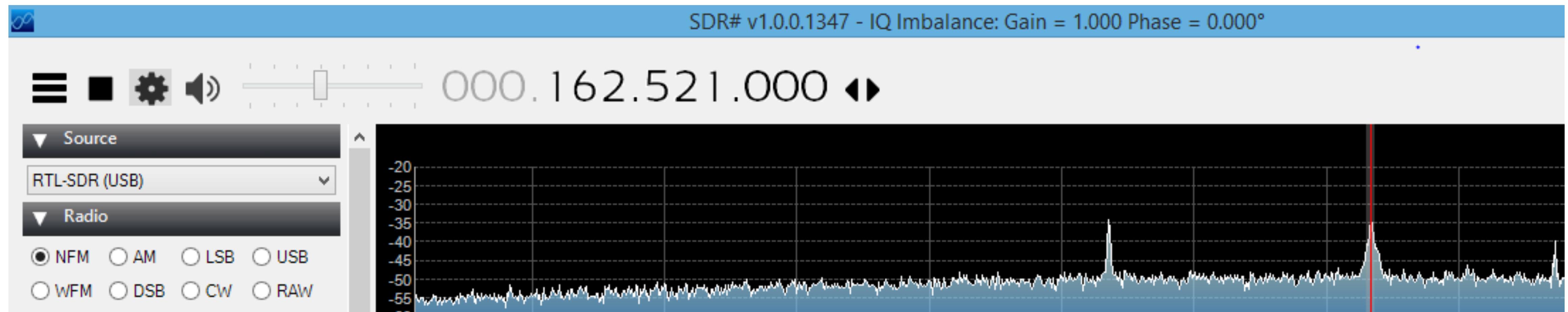
Kingsbury	046077	Arlington	KXI71	162.525	ALL
Kingsbury	046077	Wessington	WXM27	162.550	ALL
Lake	046079	Arlington	KXI71	162.525	ALL
Lake	046079	Sioux Falls	WXM28	162.400	ALL
Lawrence	046081	Lead	WXL23	162.525	ALL

- Type one of the frequencies into gqrx

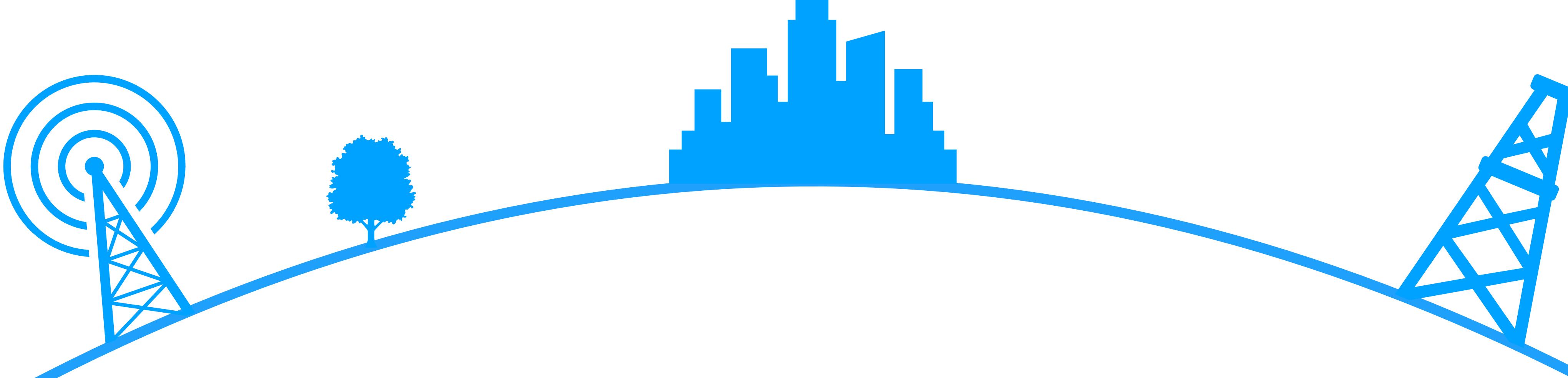
Tuning into Weather

- 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

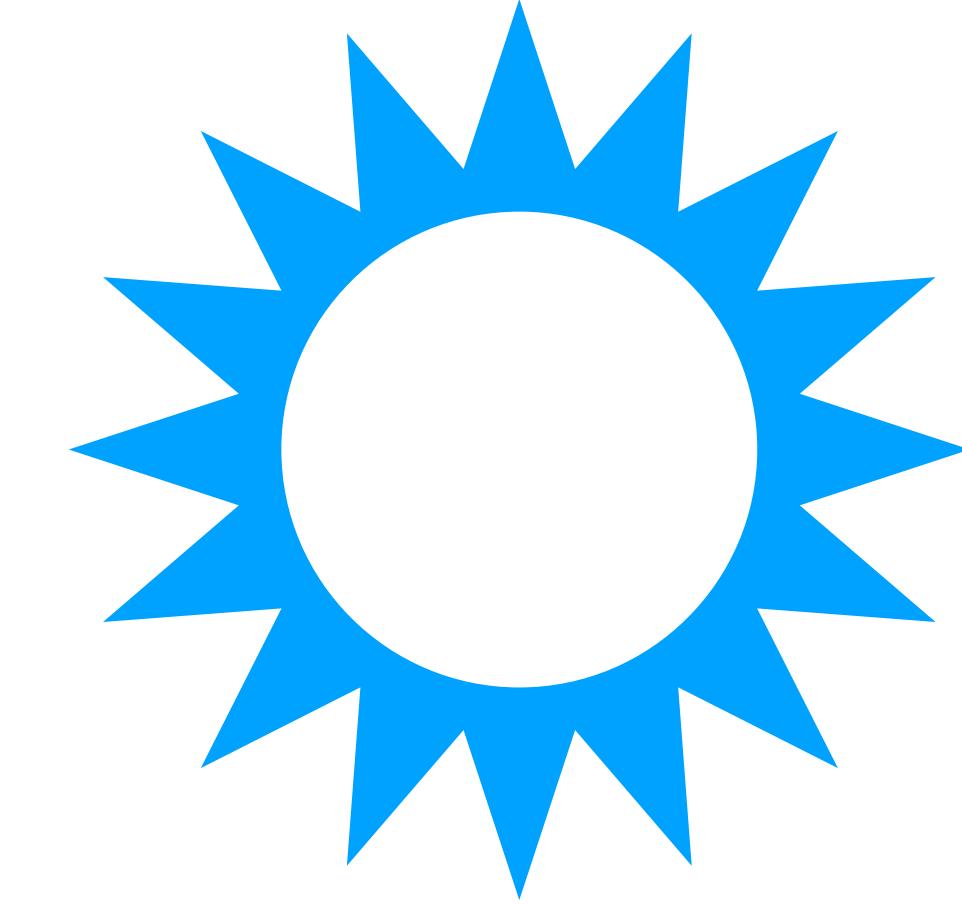
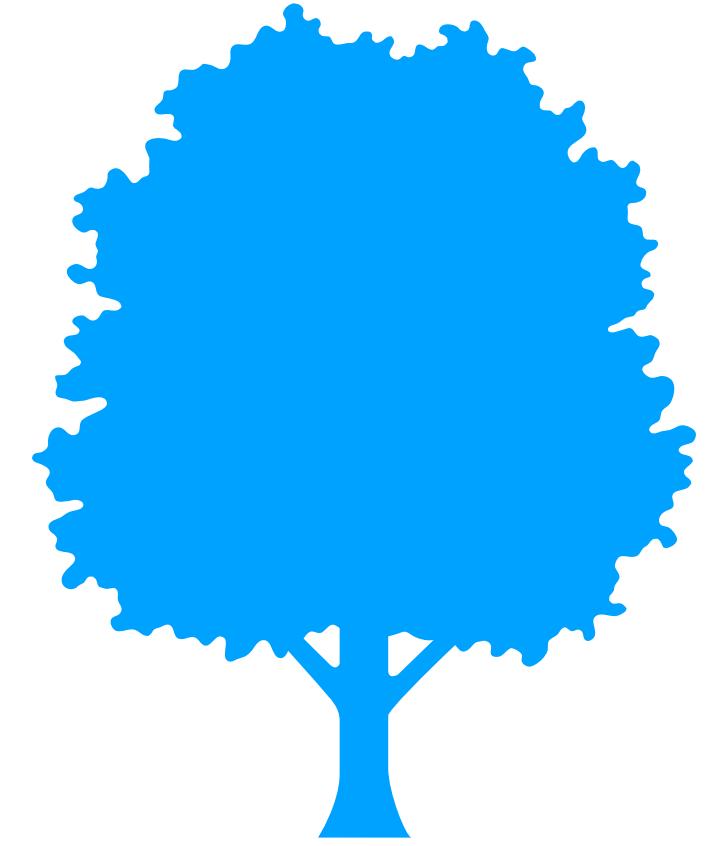
Weather Radio



Any Luck?



Weather Recording (Backup)



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

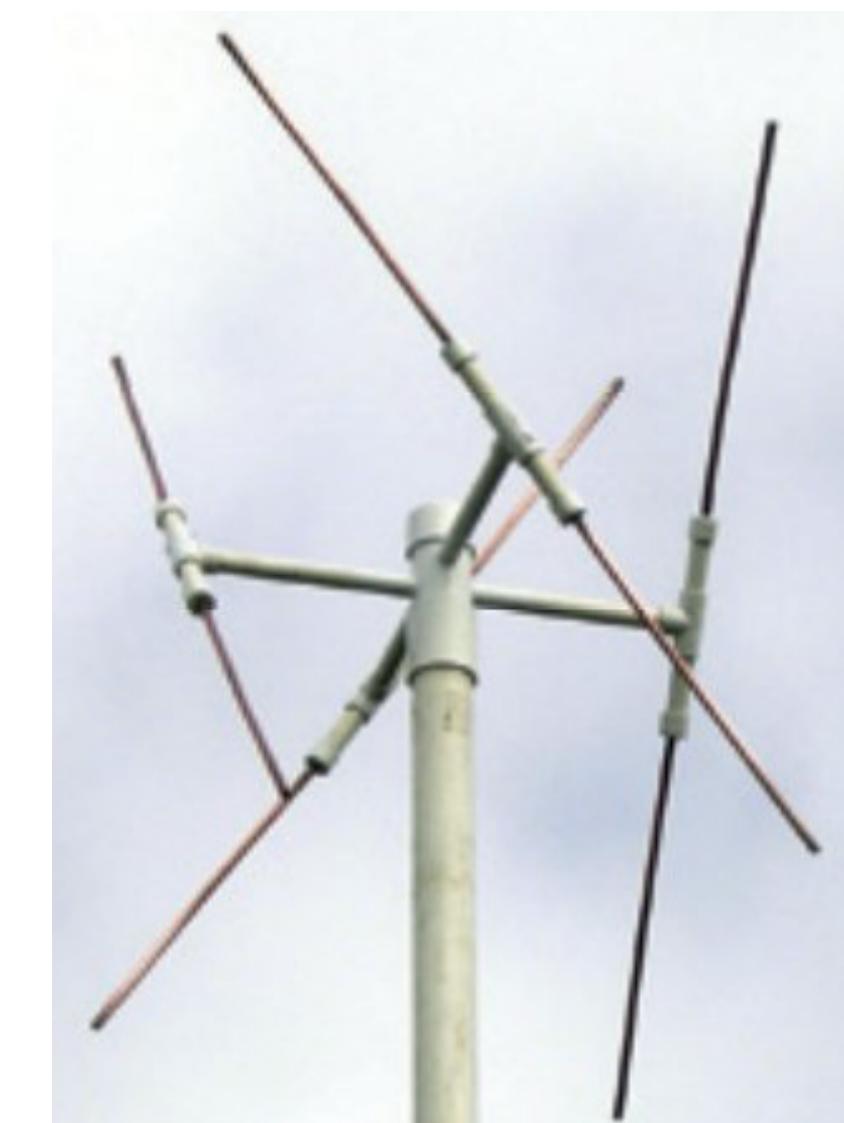
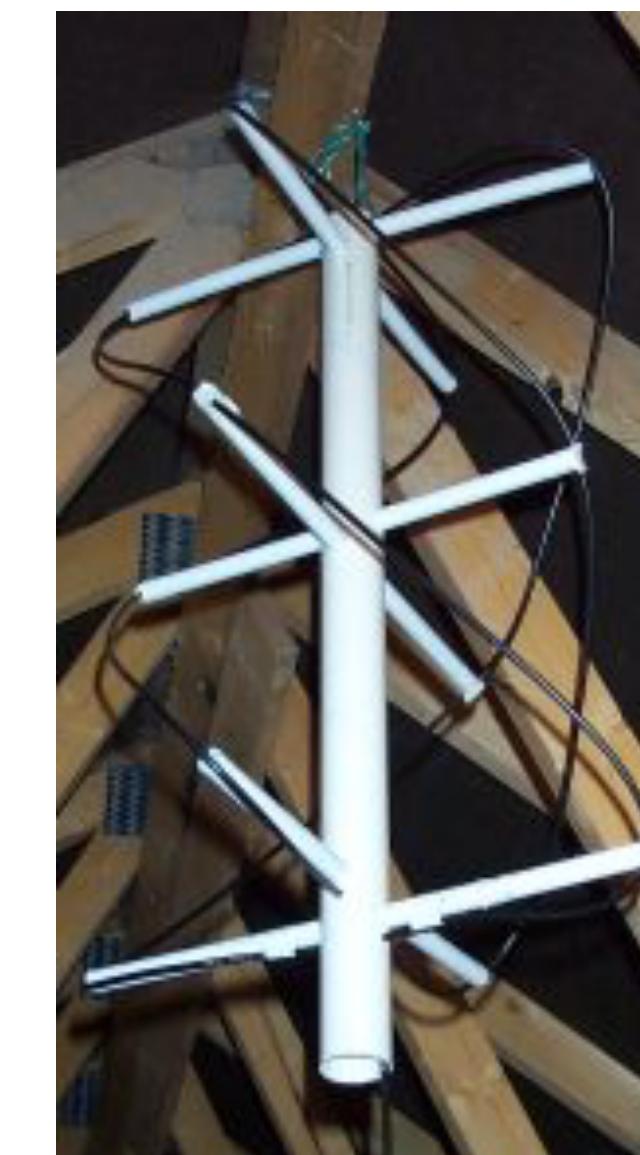
- Planes are very cool, but I like space a little better...
- How about gathering some information from satellites?
 - Our friends, the NOAA, have satellites sending images back for weather purposes
 - This gets a little more complicated though

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

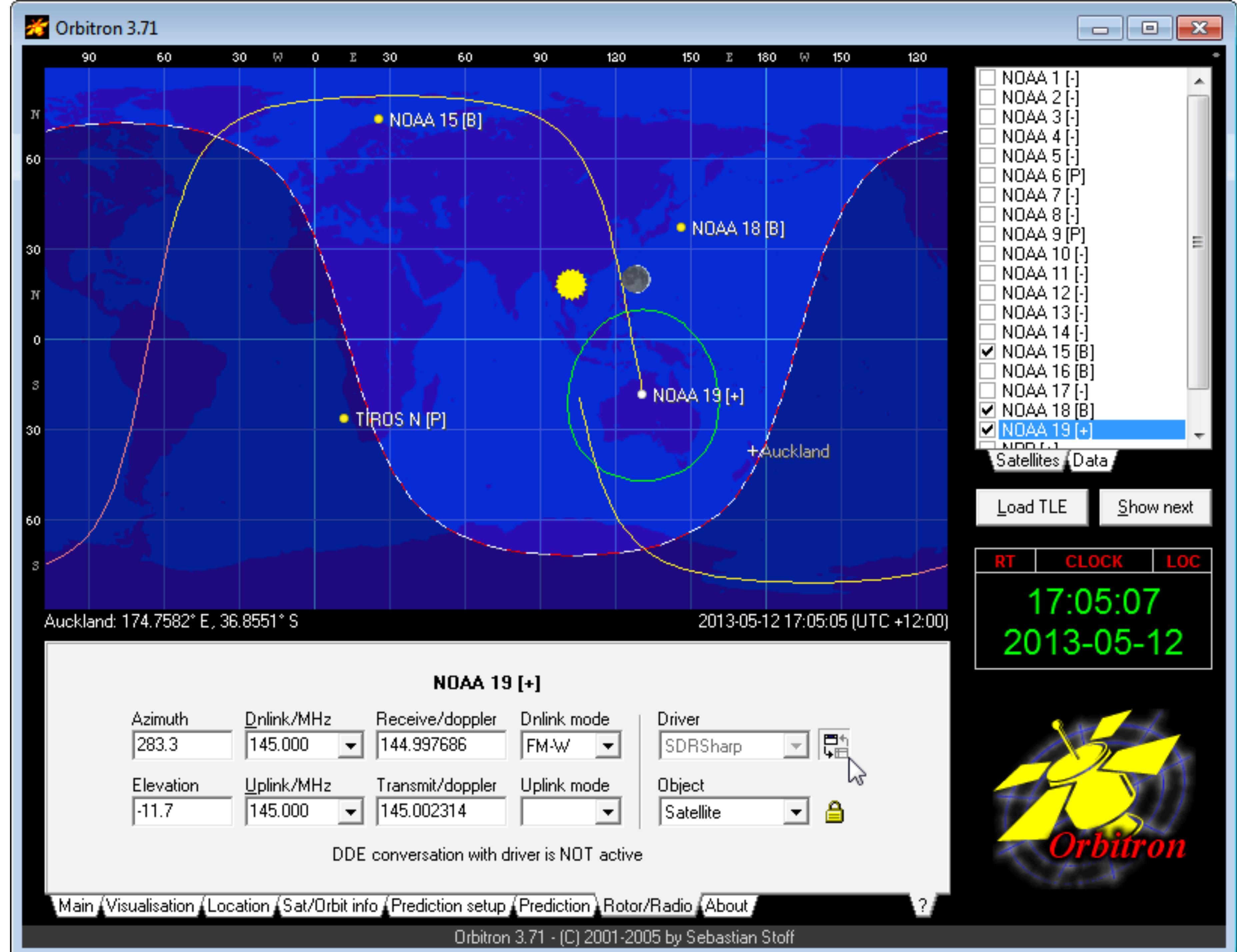


Tracking Satellite

- 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

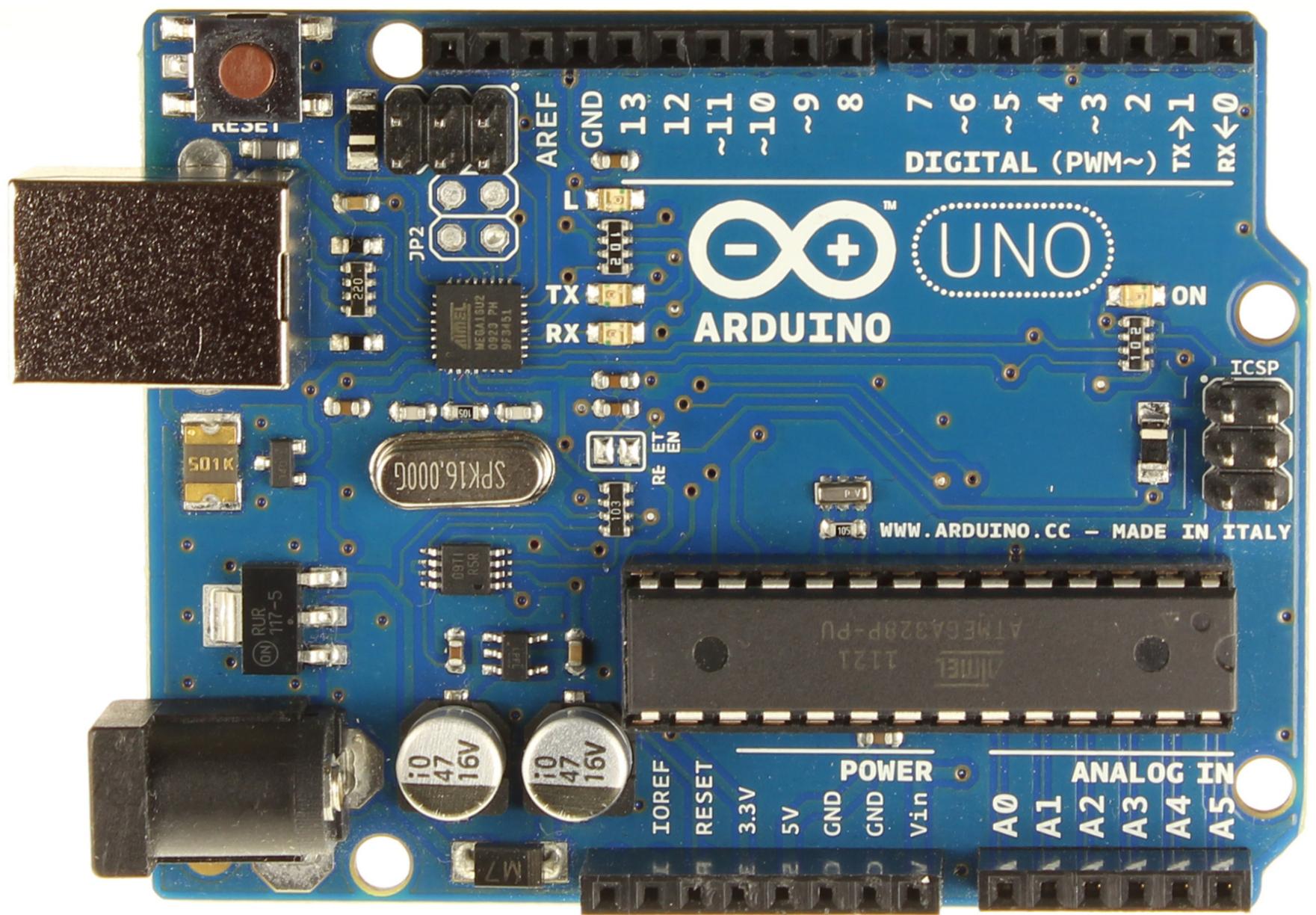
Decoding the Data

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





Pranks?



+



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

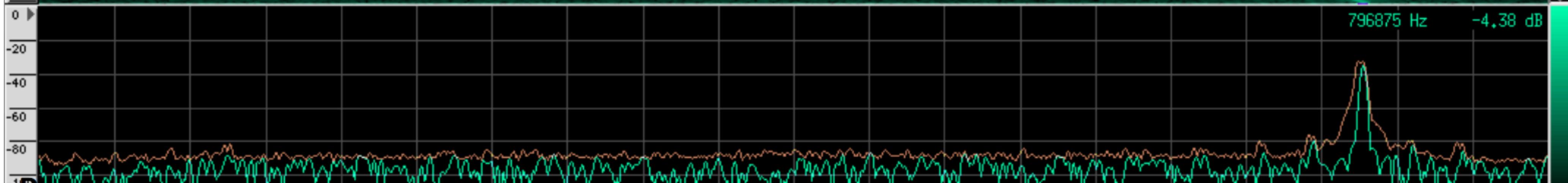
Balint Seeber – Applications Specialist



Time

Pager Waterfall Spectrum

Frequency



Decoder 0

From beginning Invert
 From start offset Baudot

 Offset: 7-bit ASCII Highlight differences
 Extend Offset Invert first bit 8-bit ASCII Show decoded data
 Sync settings Straight Flip Flop Accumulate data
 Show bits Diff Diff (inverted) Swap endian-ness

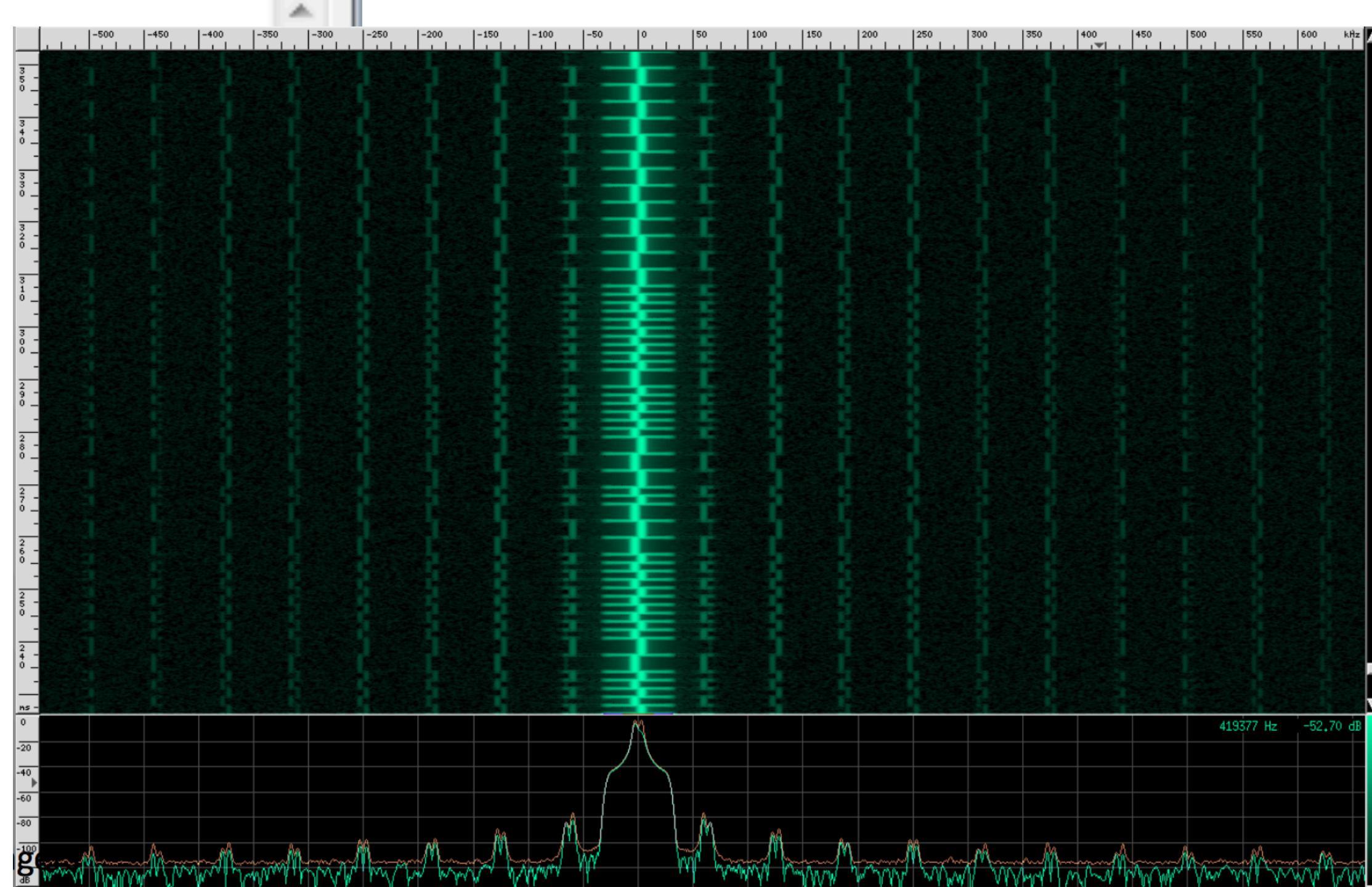
 Columns: Prev 0 Prev 1 Enforce control bits
 Manchester 0 (IEEE) Start bit
 Manchester 1 (orig) No stop bits Max bits:
 Diff Man 0 BPM Stop bit
 Diff Man 1 BPS Two stop bits

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>	

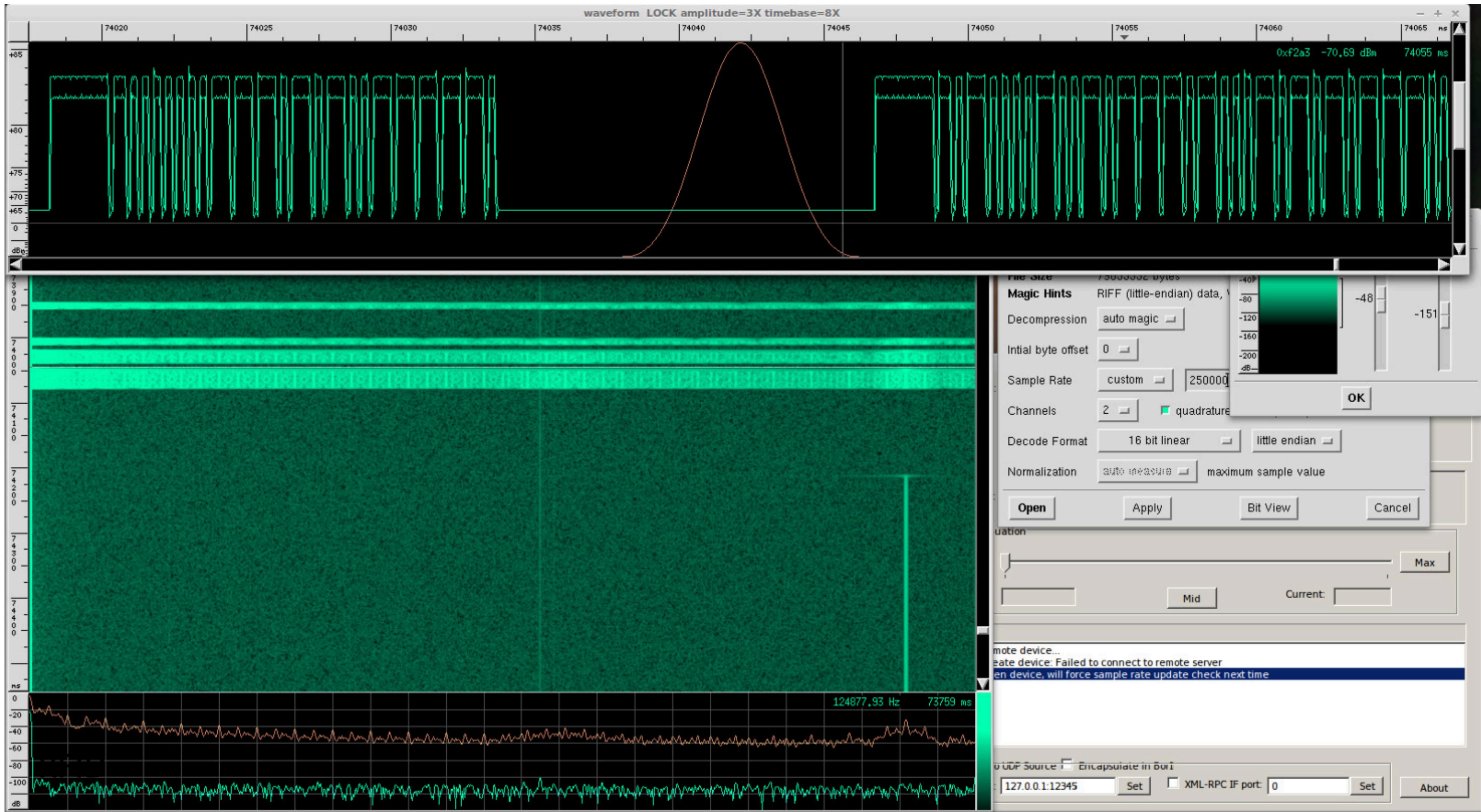
Sum: C1

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