



DAKOTA STATE
UNIVERSITY®

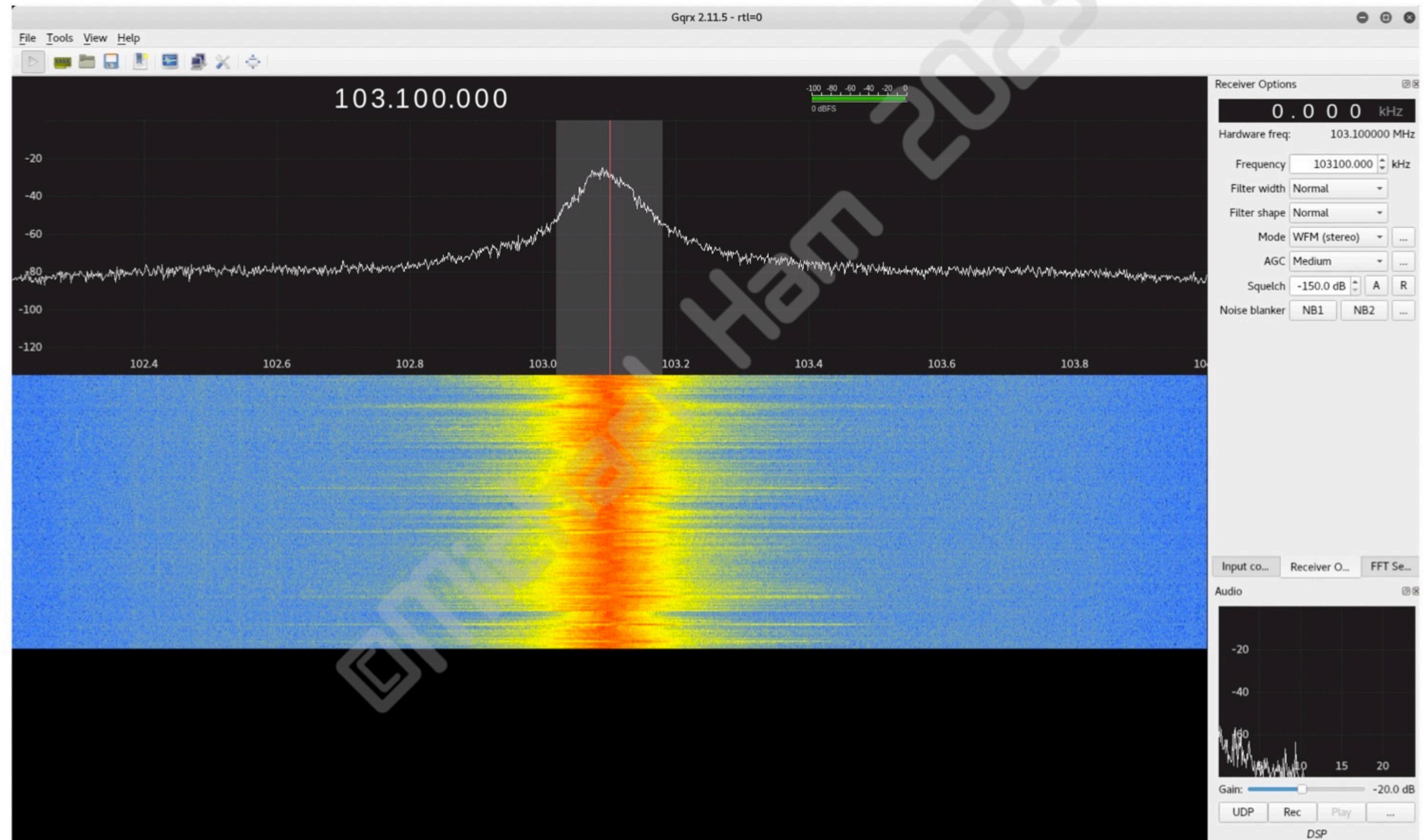
0x02 SDR Discovery

Dr. Mike Ham

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!

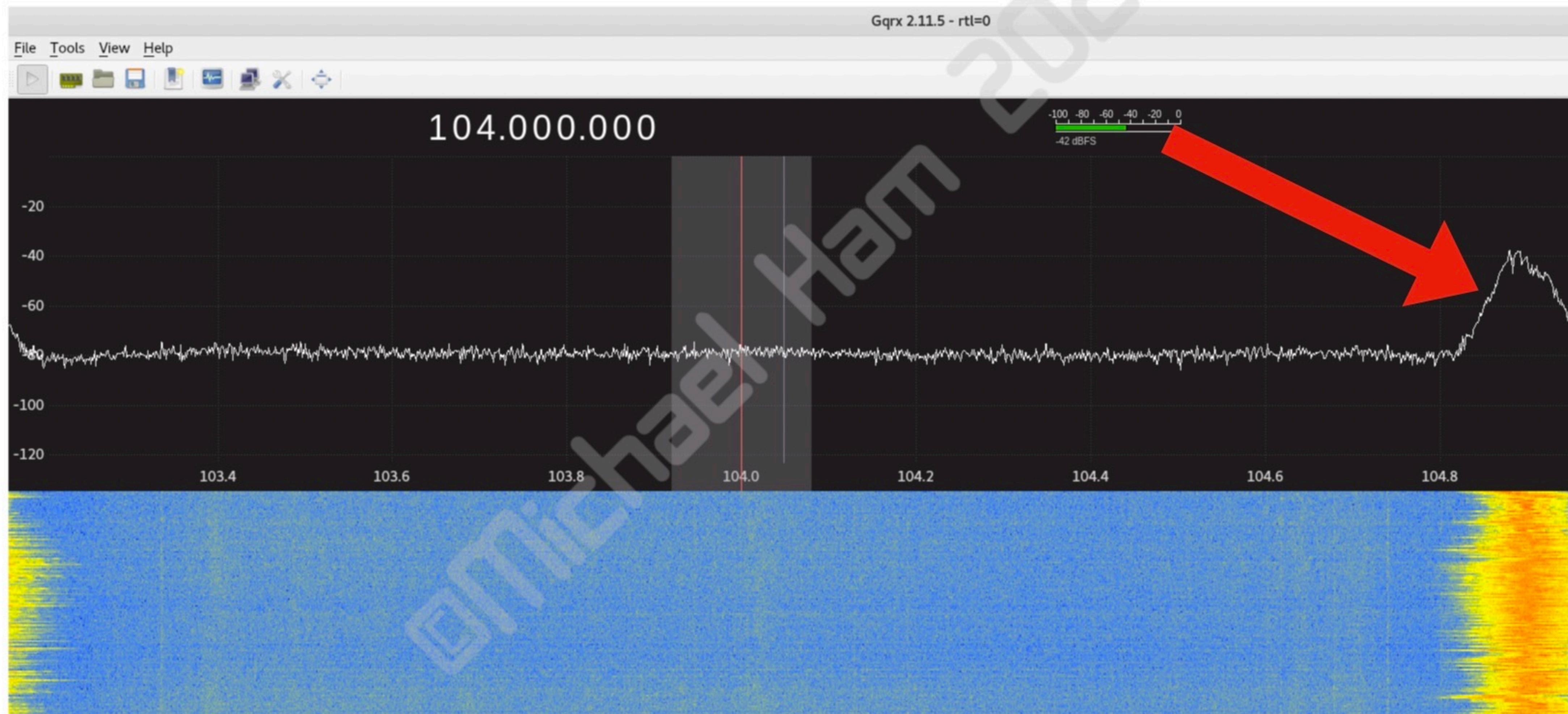
gqrx



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? idk



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

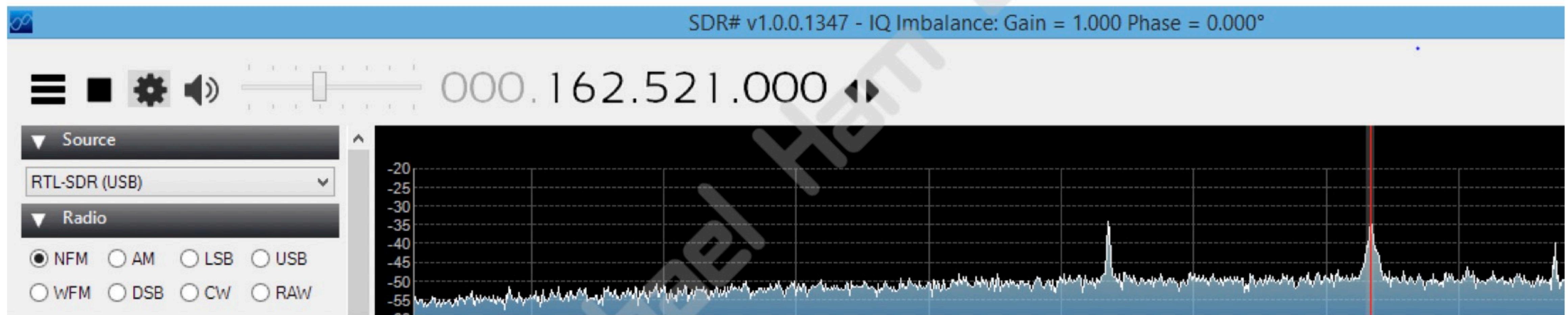
Kingsbury	046077	Arlington	KXI71	162.525	ALL
Kingsbury	046077	Wessington	WXM27	162.550	ALL
Lake	046079	Arlington	KXI71	162.525	ALL
Lake	046079	Sioux Falls	WXM28	162.400	ALL
Lawrence	046081	Lead	WXL23	162.525	ALL

- Type one of the frequencies into gqrx

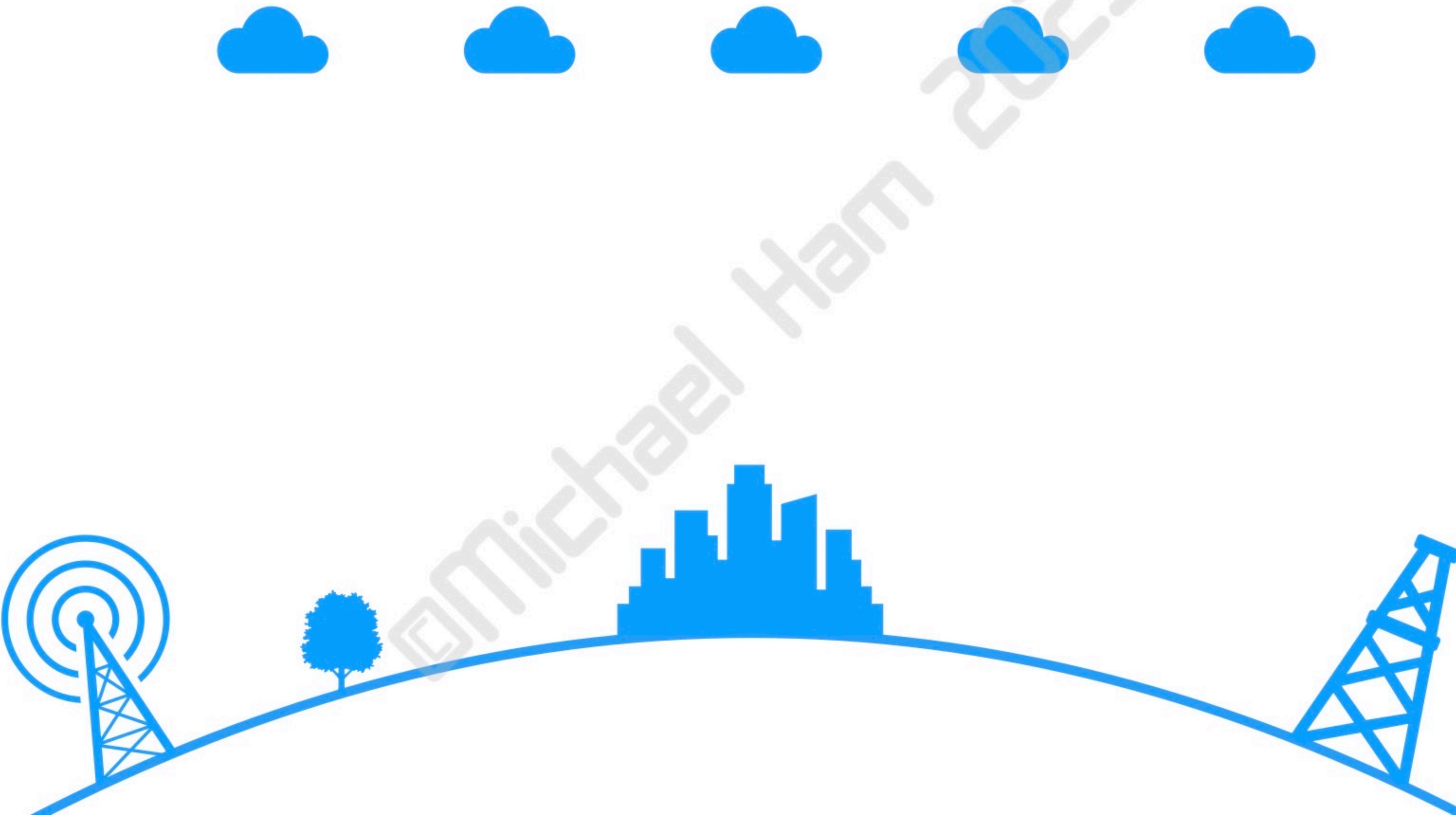
Tuning into Weather

- 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

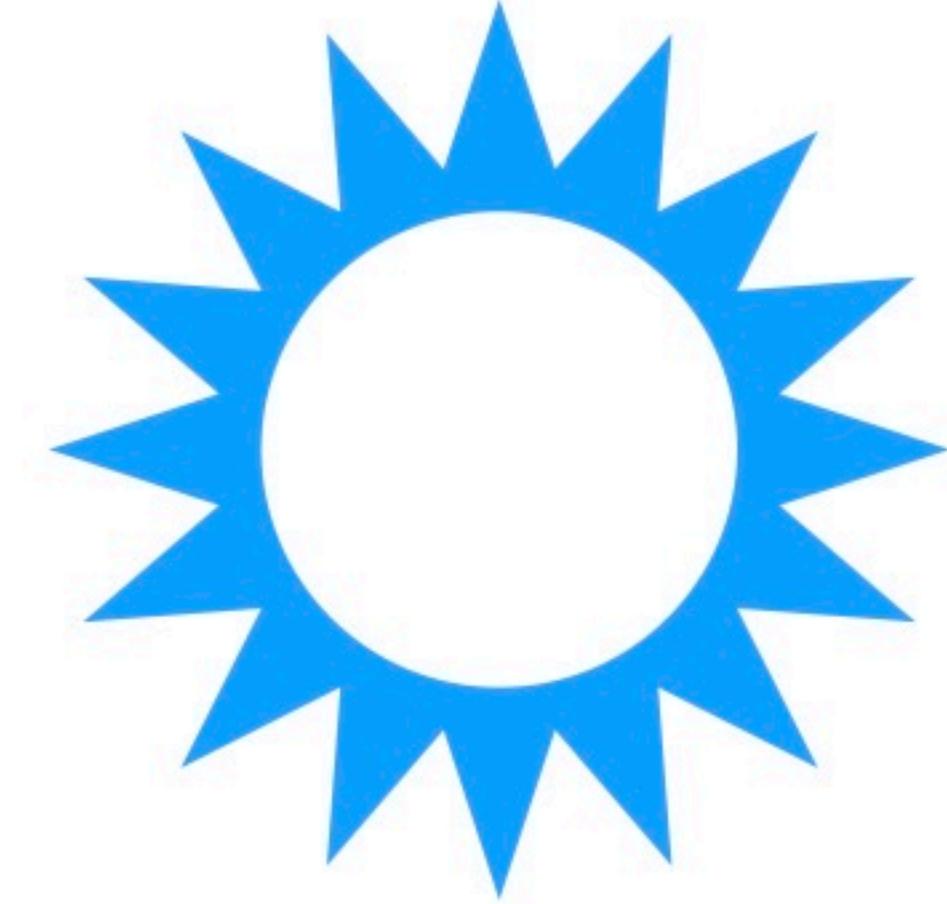
Weather Radio



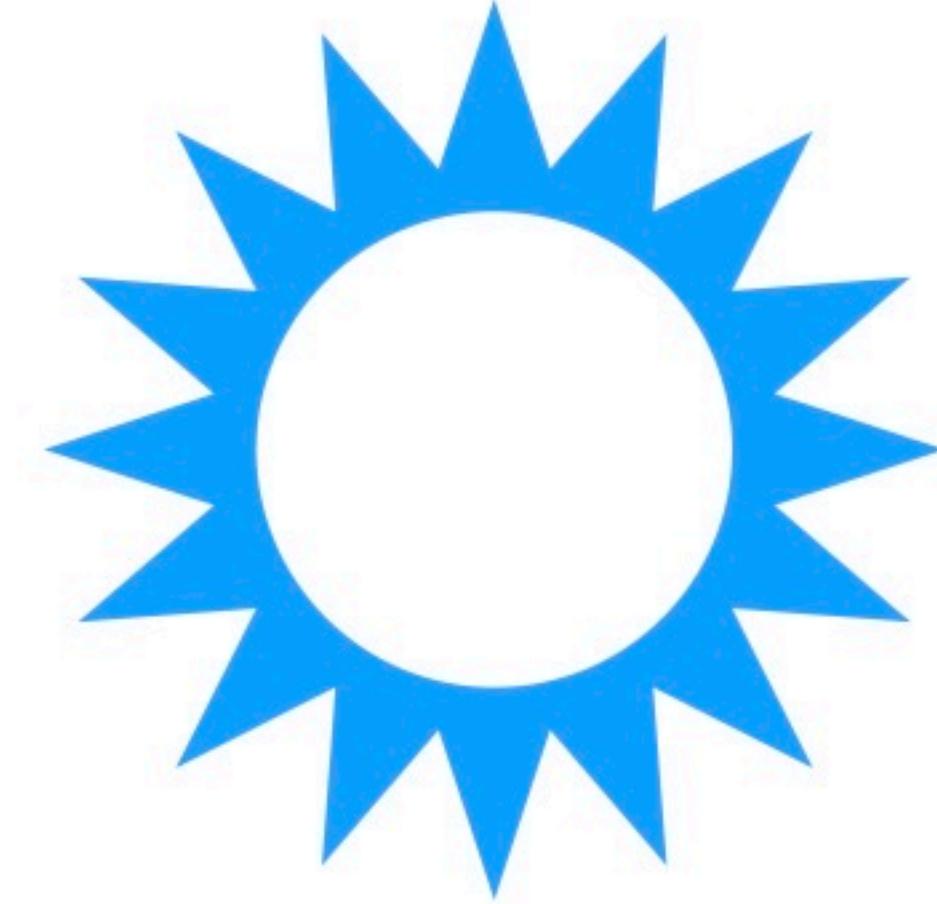
Any Luck?



Weather Recording (Backup)



Weather Recording (Backup)



Let's talk Airplanes

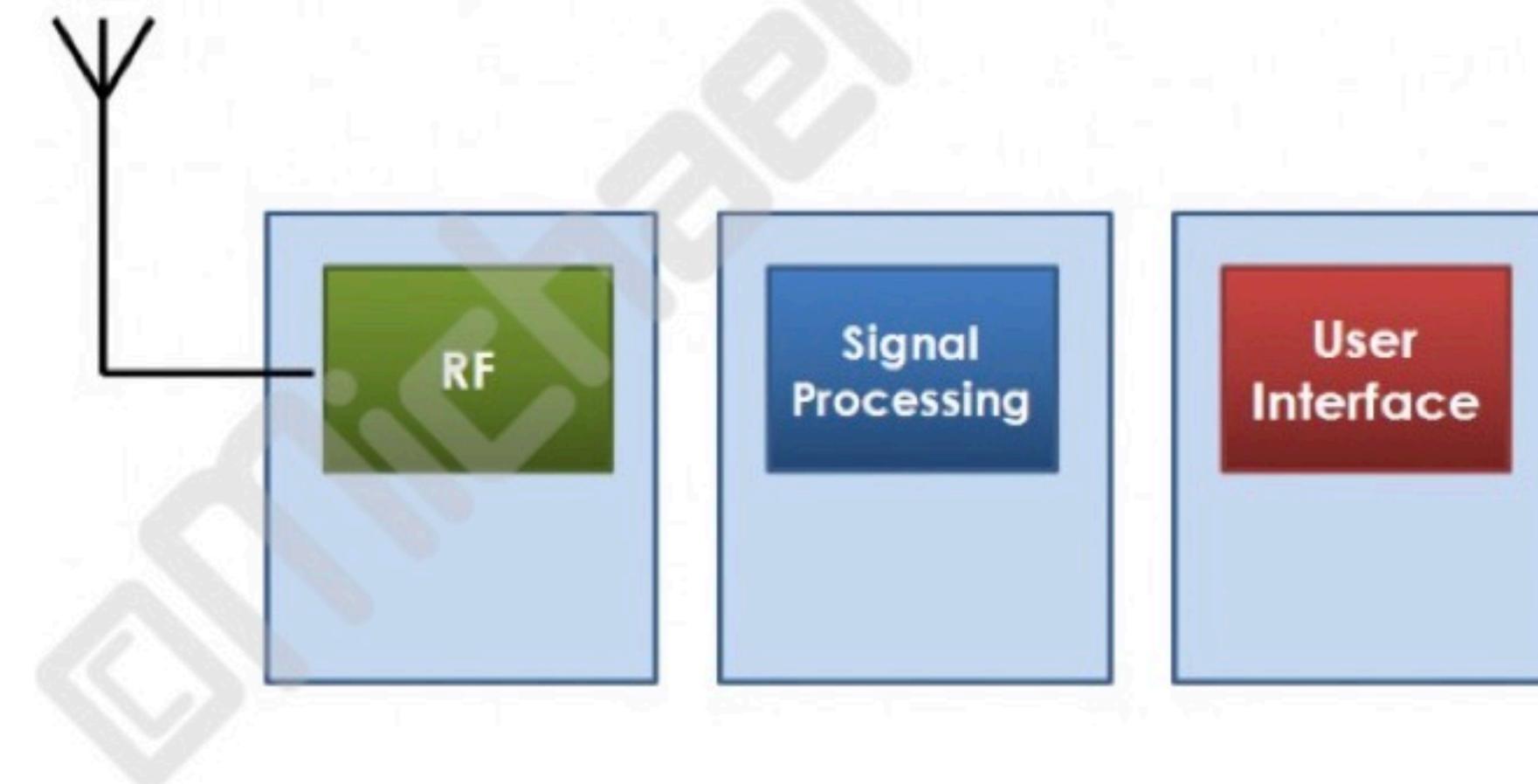
- ADS-B - Automatic dependent surveillance – broadcast
 - Cooperative surveillance for tracking aircraft
 - Aircraft determines its position and broadcasts it for safety measures
 - Sent in clear text, they want people to read this so planes don't crash

Pieces of Software

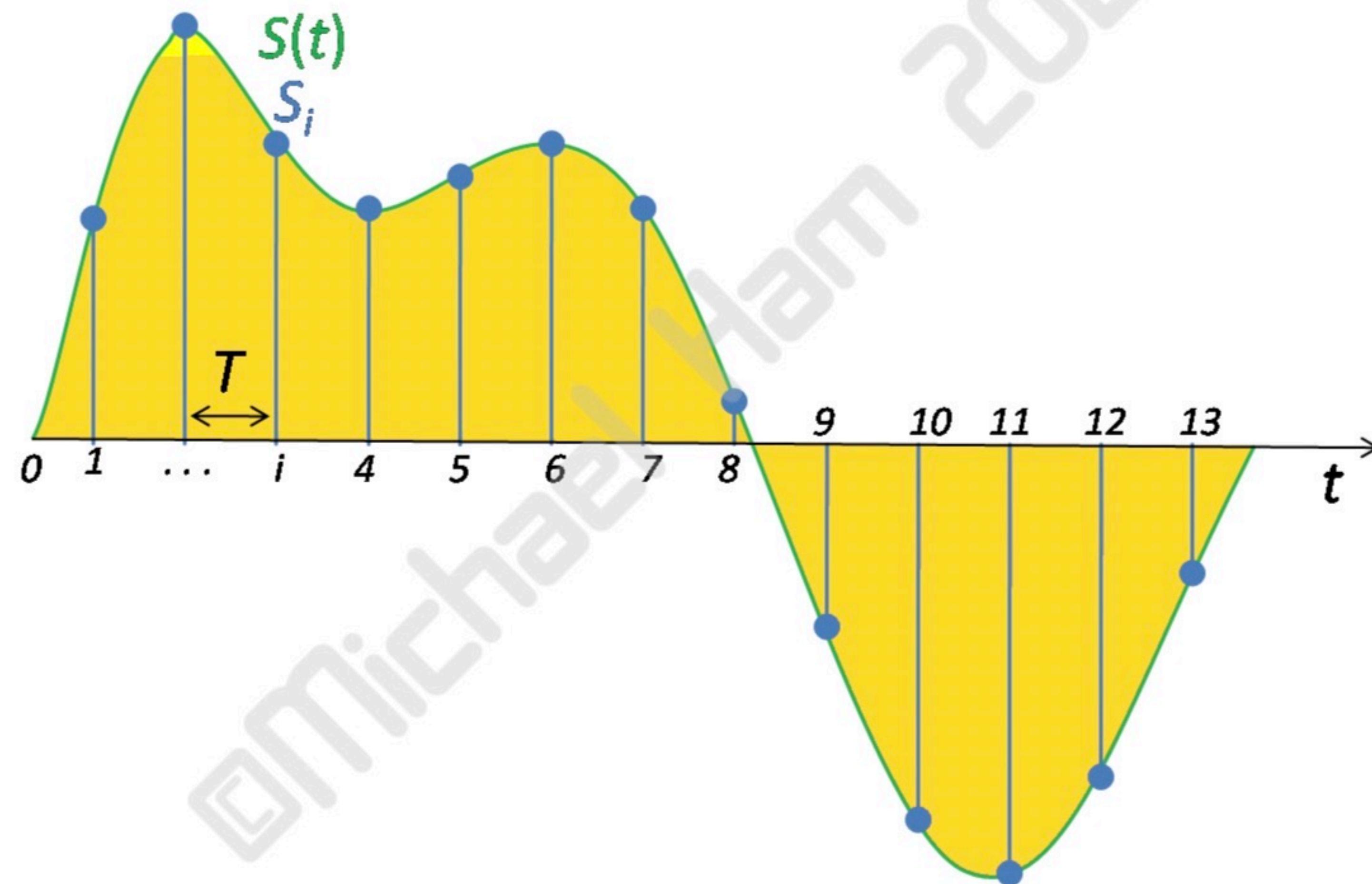
- dump1090
 - Takes all of the ADSB data and decodes the packets (frames)
 - 1090 MHz
- Disclaimer: Madison is not a destination for many planes, fingers crossed one is passing over

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



Michael Jackson
Ideas

2023

Don't Stop at 30K Feet

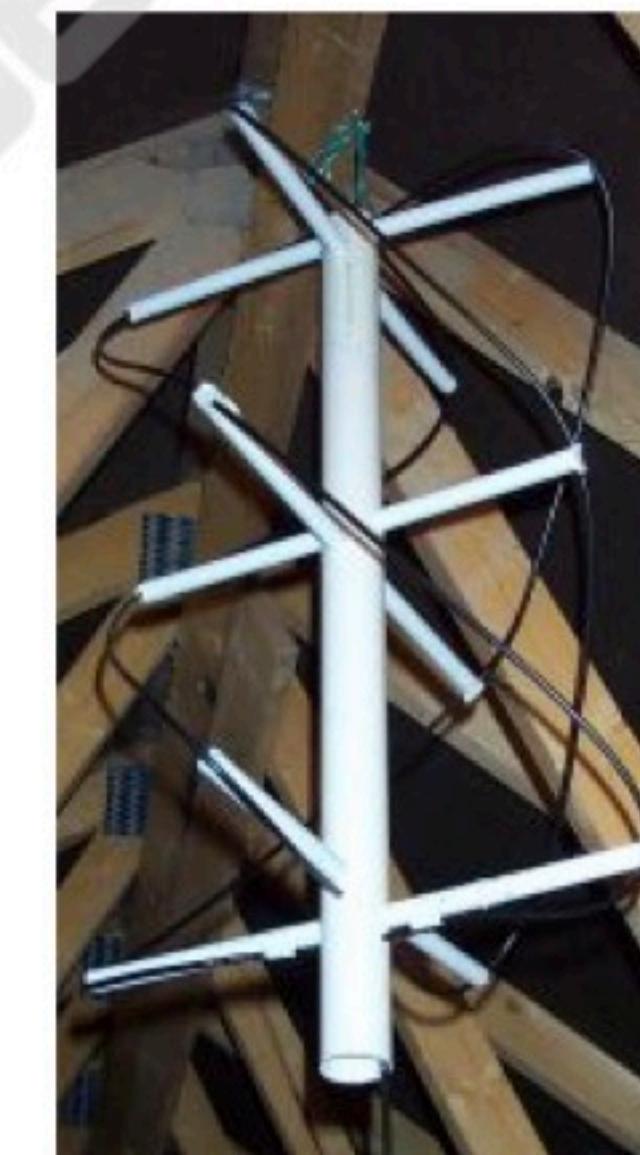
- Planes are very cool, but I like space a little better...
- How about gathering some information from satellites?
 - Our friends, the NOAA, have satellites sending images back for weather purposes
 - This gets a little more complicated though

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

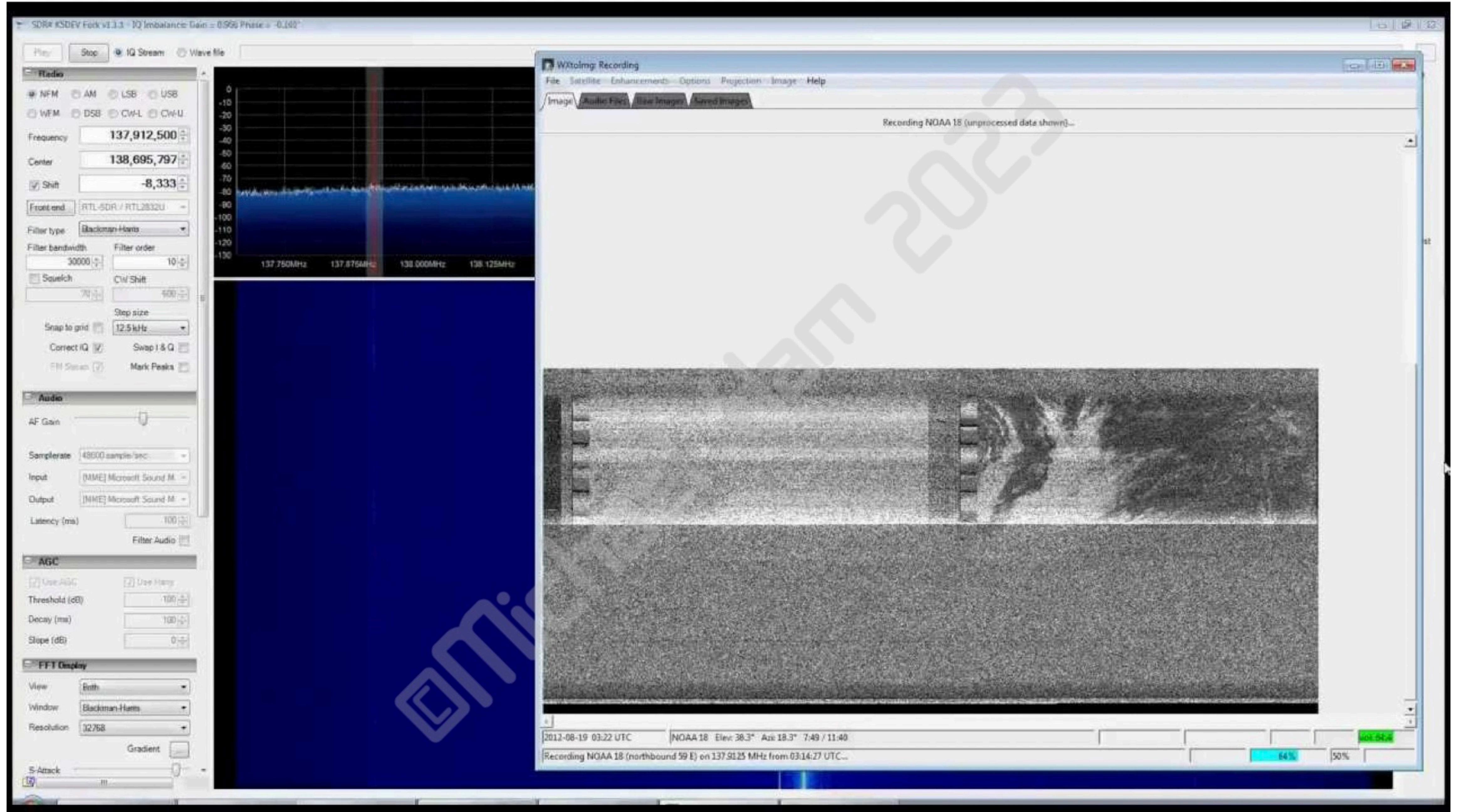


Tracking Satellite

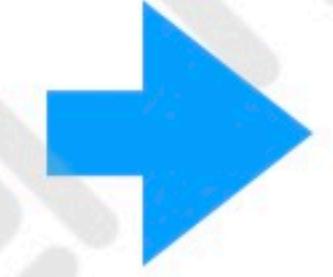
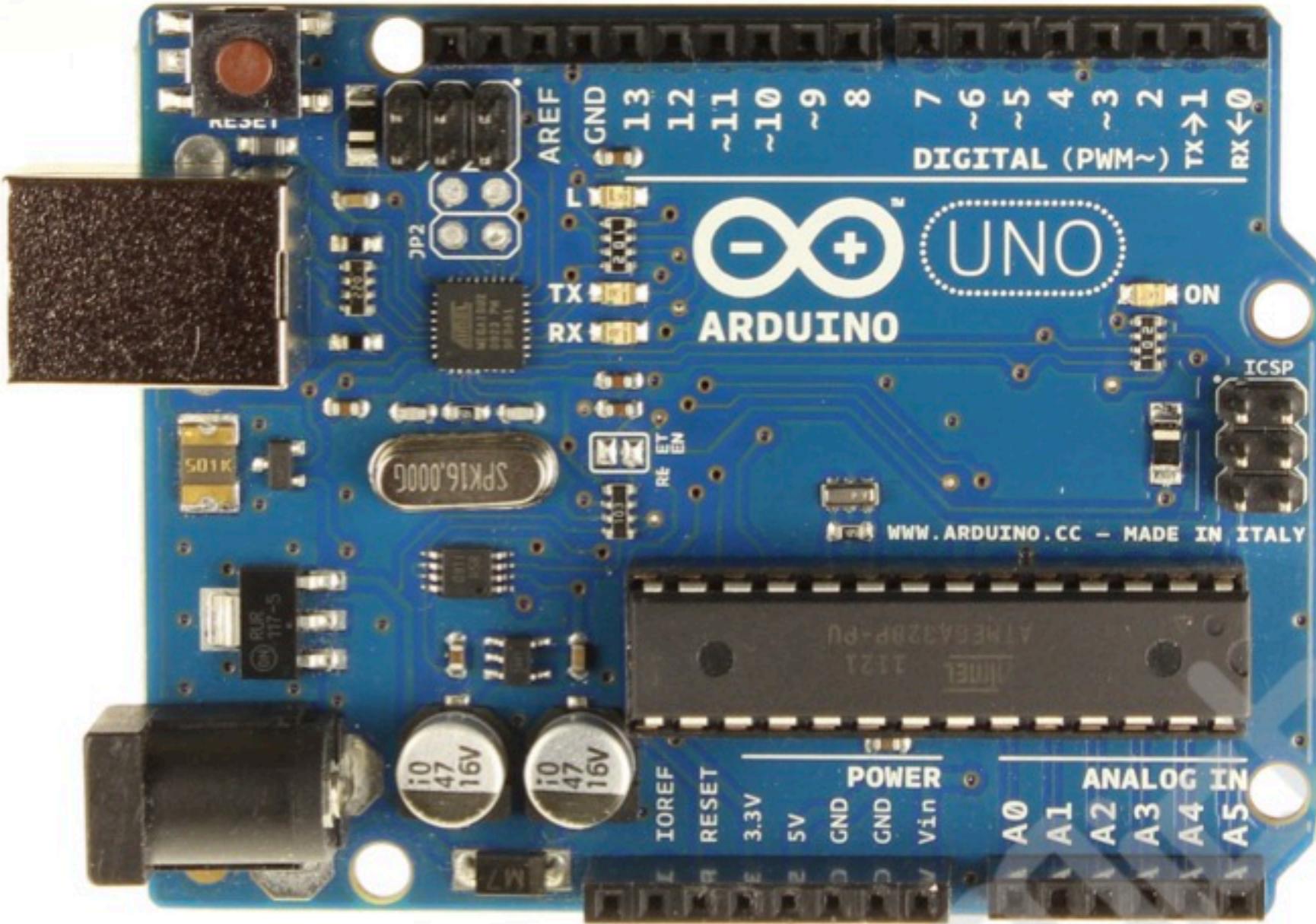
- Once the antenna is attached, if you tune into one of the following stations, you may start receiving the “audio”
 - NOAA 15 – 137.6200 MHz
 - NOAA 18 – 137.9125 MHz
 - NOAA 19 – 137.1000 MHz

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



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

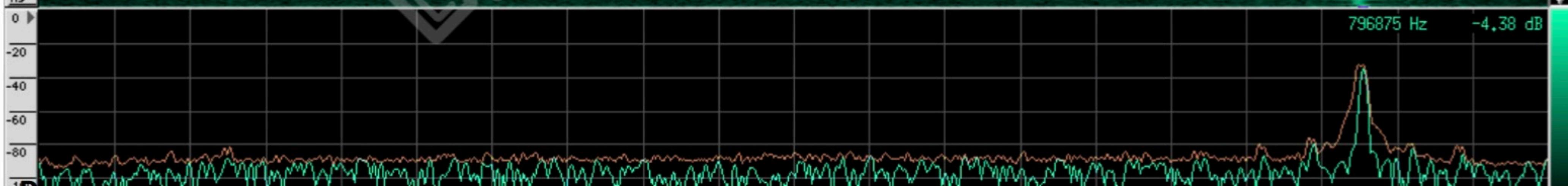
Balint Seeber – Applications Specialist



Time

Pager Waterfall Spectrum

Frequency



Decoder 0

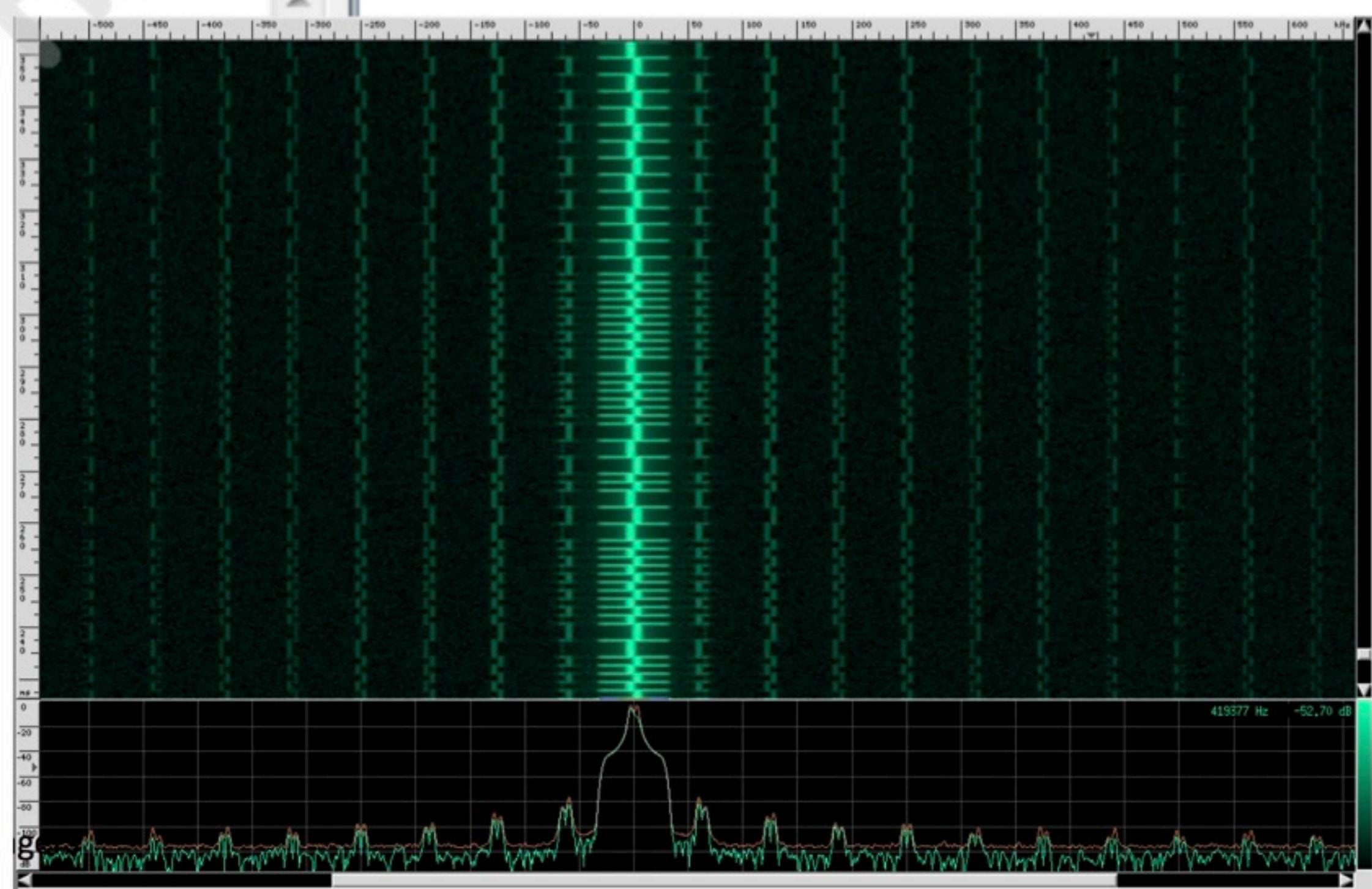
From beginning Invert Baudot Highlight differences
 From start offset 7-bit ASCII Show decoded data
Offset: Invert first bit 8-bit ASCII Accumulate data
 Extend Offset Straight Flip Flop Swap endian-ness
 Sync settings Diff Diff (inverted) Enforce control bits
 Show bits Prev 0 Prev 1 Start bit
Columns: Manchester 0 (IEEE) No stop bits Max bits:
 Manchester 1 (orig) Stop bit
 Diff Man 0 BPM Two stop bits **Dump** **Clear**
 Diff Man 1 BPS

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>	

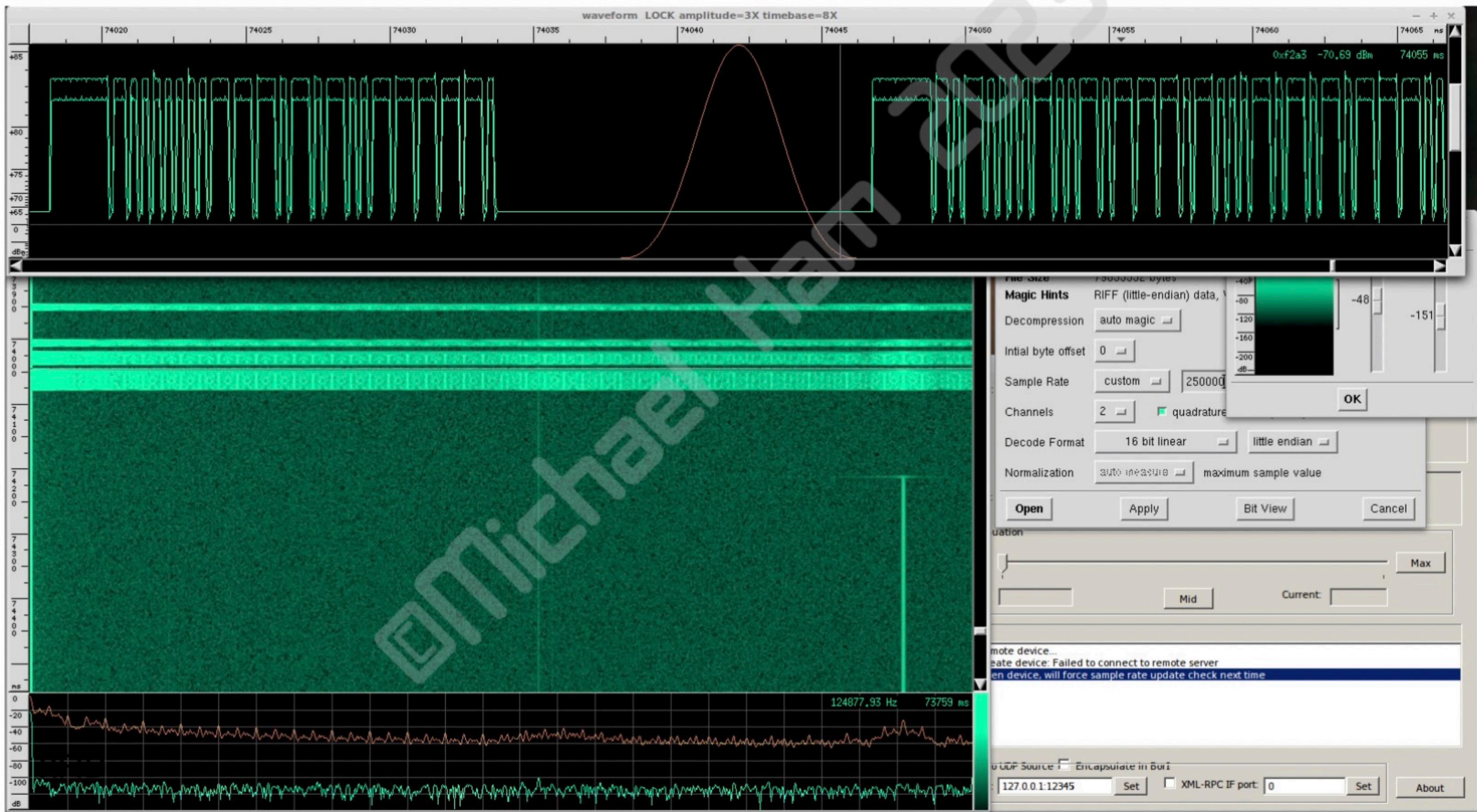
Sum: C1

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