

# Software Defined Radio (SDR)

Dr. Mike Ham

# What is SDR?

- 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

What radio waves surround you?

# 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

USB RTL-SDR Kit

\$17.99 from Hak5 <http://hakshop.myshopify.com/collections/software-defined-radio/products/software-defined-radio-kit-rtl-sdr?variant=424034573>



# 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

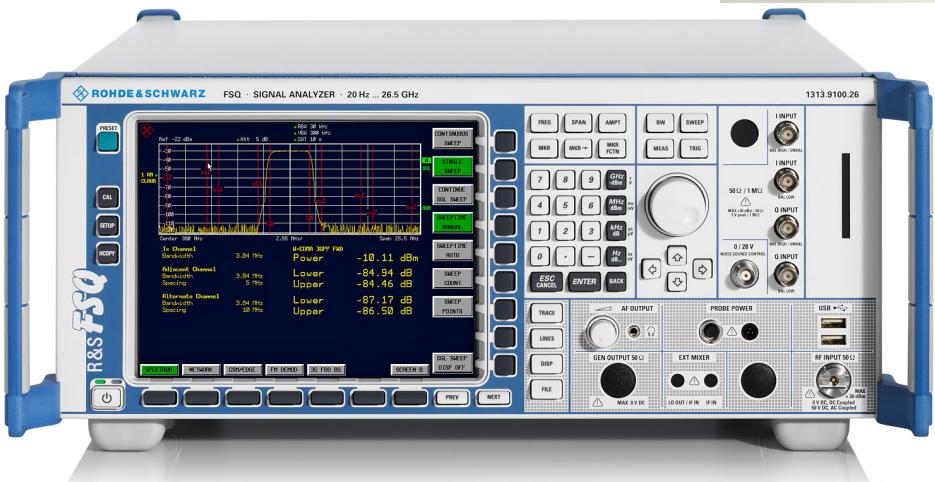
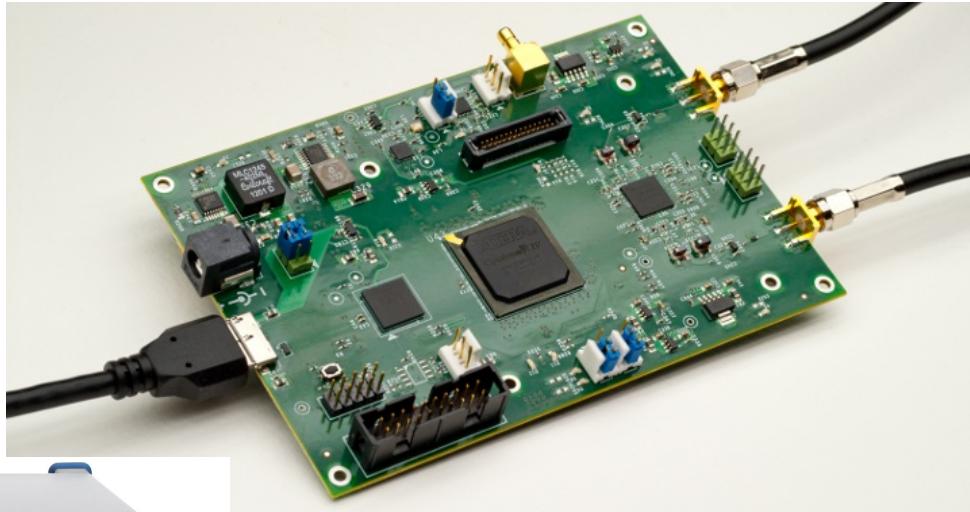
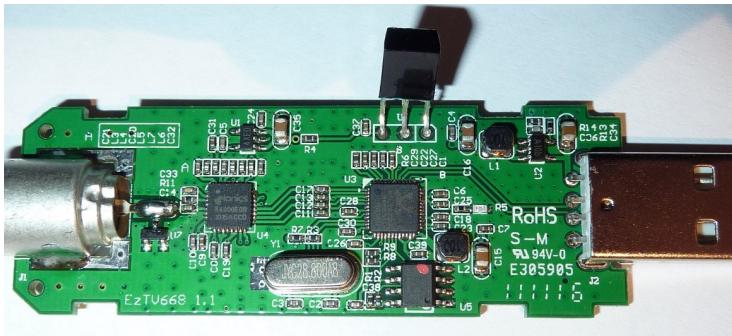
# Geeky Specs

- 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

# Driver Voodoo

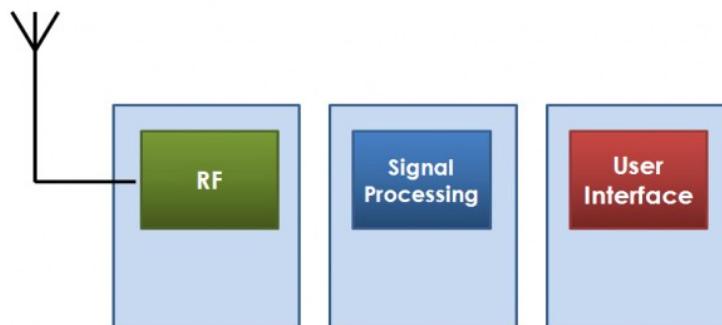
- Some really smart people have crafted a driver for these USB adapters to give us more control
- Driver – software that controls hardware
  - Your mouse, keyboard, printers, etc. all use them
  - Computer has to know how to speak the language of the hardware in order for it to work

# Other SDR Hardware

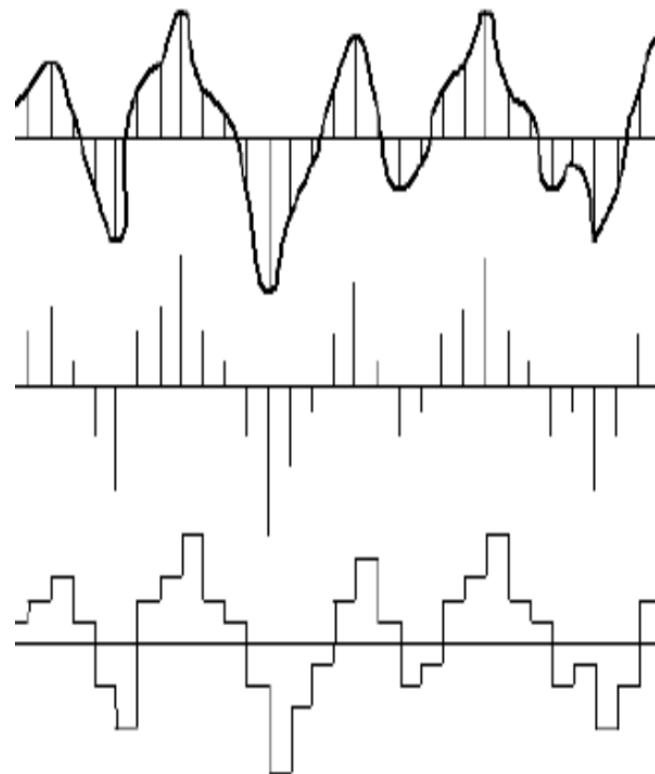


# How does SDR work?

- 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



# Installing

- Clone my script off of GitHub
- Change the script to be executable:  
**chmod +x sdr\_setup.sh**
- Run the script:  
**./sdr\_setup.sh**

# FM Radio

- Let's go for something normal first
- FM radio (these radios are supposed to do this out of the box)
  1. Choose **WFM** (wide-band FM radio)
  2. Set your frequency by clicking large numbers on top
    1. Local station KJAM is **103.1**
    2. The interface is a little touchy
  3. Click the play button and listen!

SDR# v1.0.0.1347 - IQ Imbalance: Gain = 1.000 Phase = 0.000°



000.103.100.000 ◀▶

▼ Source

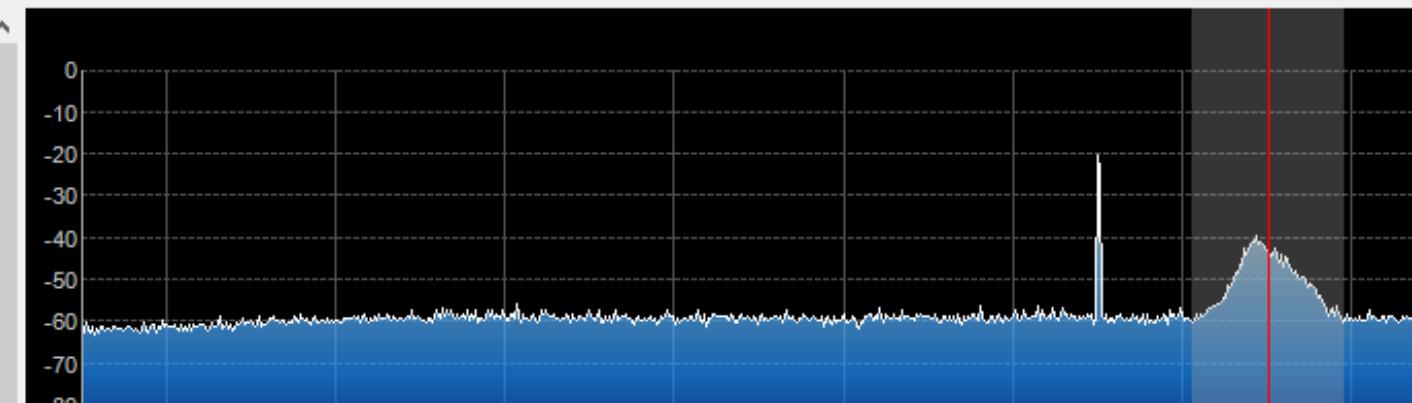
RTL-SDR (USB)

▼ Radio

- NFM     AM     LSB     USB
- WFM     DSB     CW     RAW

Shift

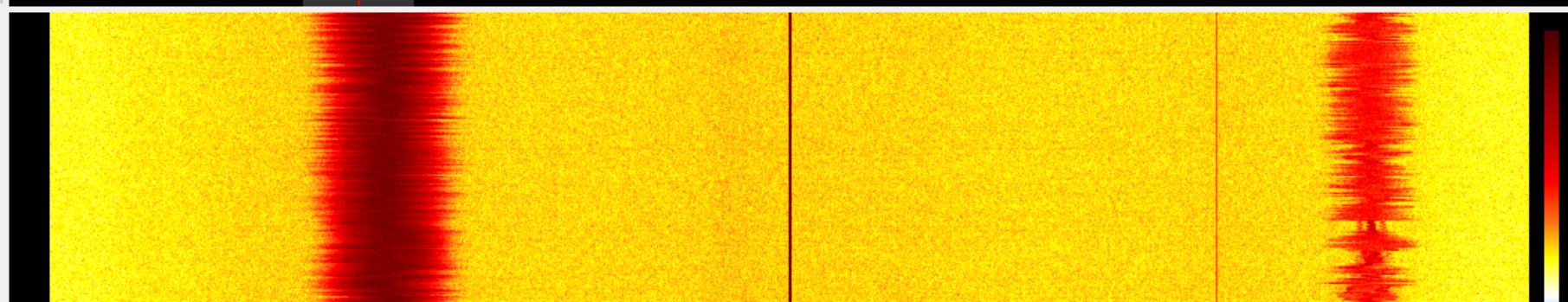
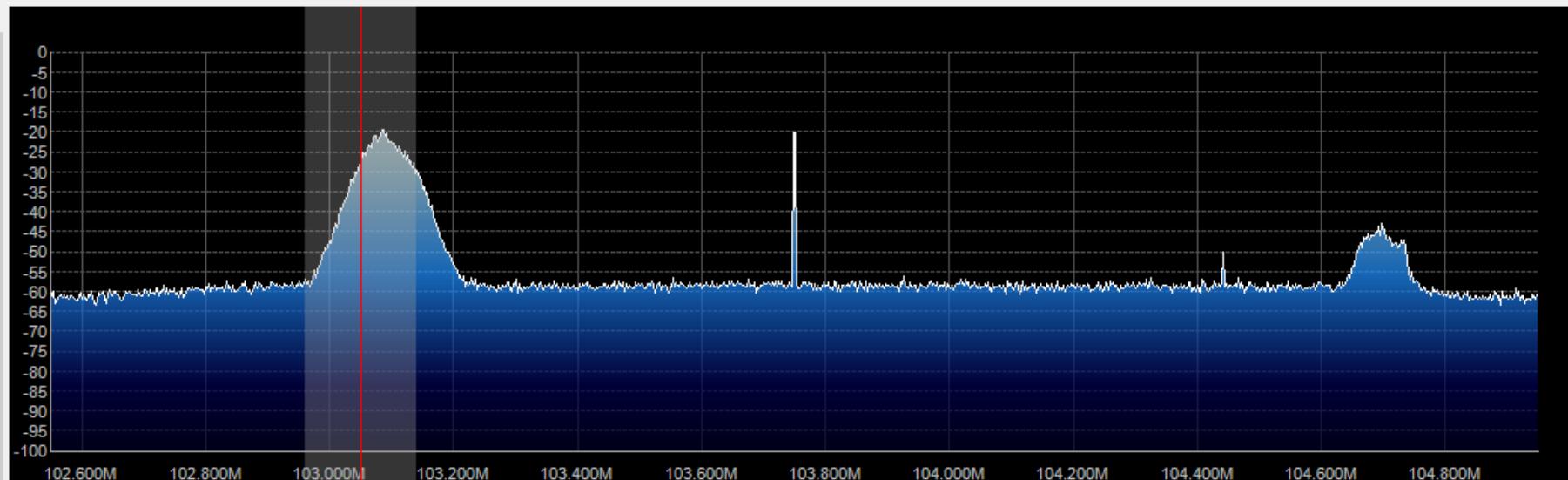
Filter



# Find me another station!

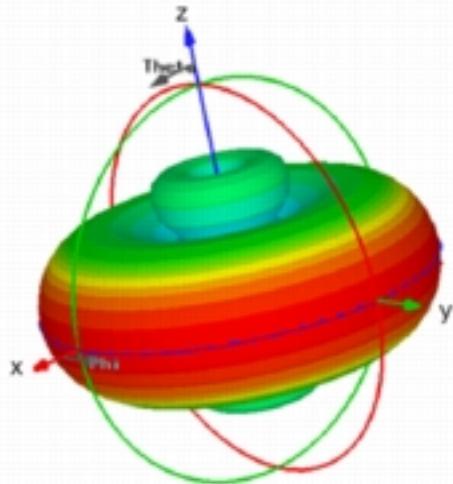
- I've given you a FM station to tune into
- SDR# shows us where we have strong signals in the current spectrum (WFM in our case)
  - Peaks more than likely will be other radio stations
- You can use the filters on the right-hand side to try and pick out different radio stations
  - Antenna position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

000.103.050.000 ◀▶

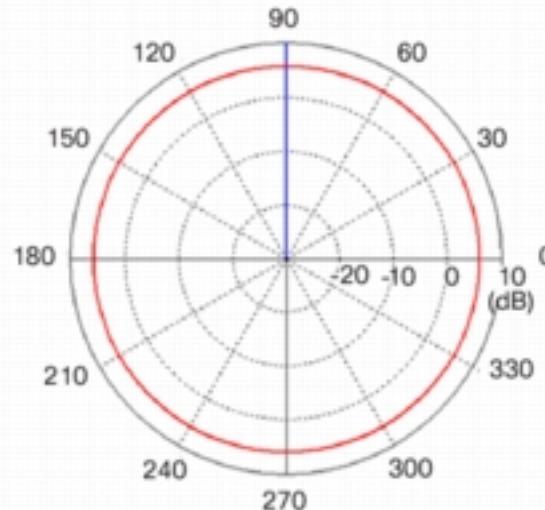


# Antenna Types

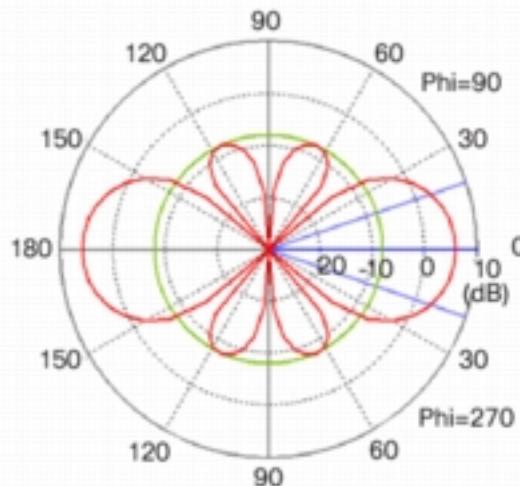
- Omnidirectional
  - Extends your range in all directions
- Directional
  - Let's you focus your signal in a particular direction
- Sensitivity – measured in dBi
  - dBi - gain of an antenna as referenced to an ISOTROPIC (omnidirectional) source
  - Remember, every 3 dBi = double the sensitivity



(a) 5.8 dBi Omni 3D Pattern

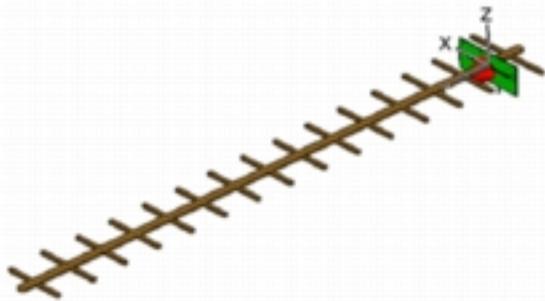


(b) 5.8 dBi Omni Azimuth Plane Pattern

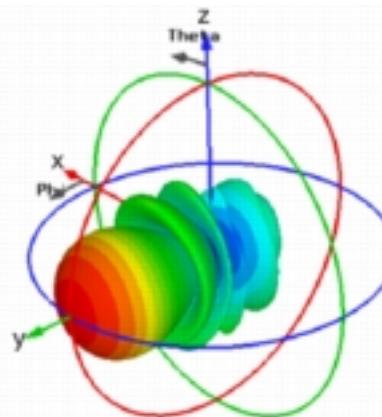


(c) 5.8 dBi Omni Elevation Plane Pattern

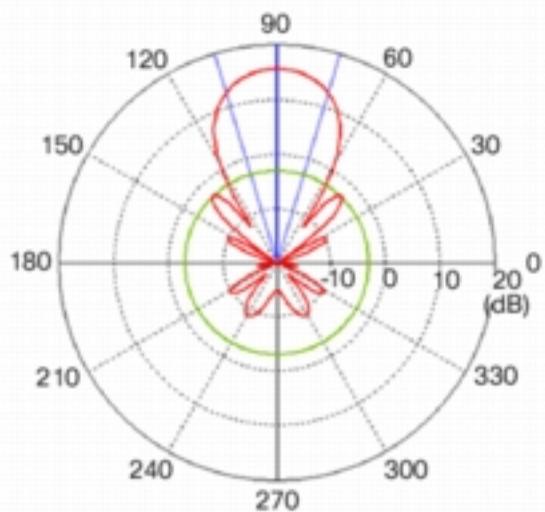




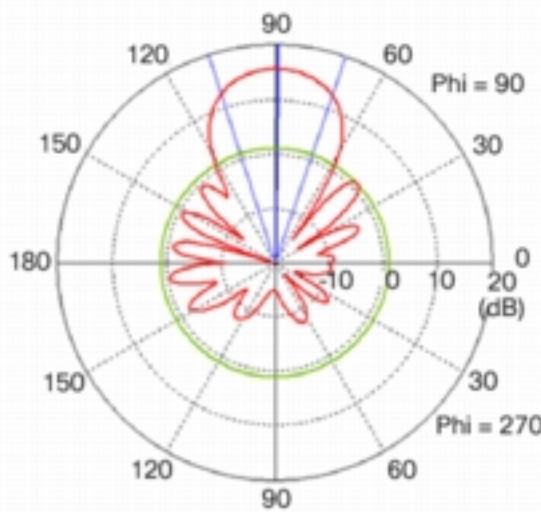
(a) Yagi Antenna Model



(b) Yagi Antenna 3D Radiation Pattern



(c) Yagi Antenna Azimuth Plane Pattern



(d) Yagi Antenna Elevation Plane Pattern

# Look at the Spectrum

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

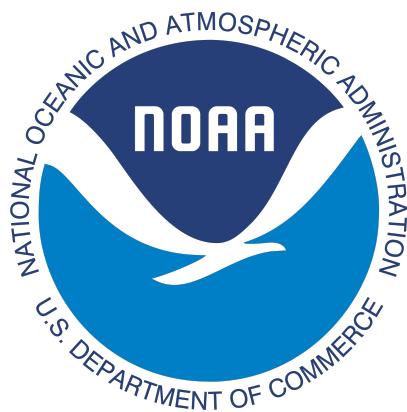
# How about Weather Radio

- 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

1. Find your nearest NOAA weather station frequency here:

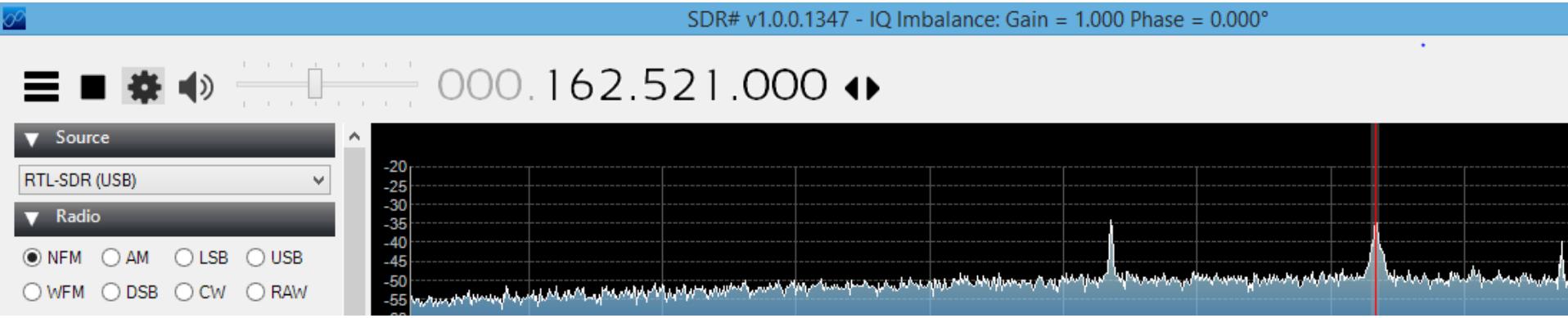
[http://www.nws.noaa.gov/nwr/coverage/country\\_coverage.html](http://www.nws.noaa.gov/nwr/coverage/country_coverage.html)

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

2. Type one of the frequencies into SDR#

# Tuning into Weather

3. 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 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



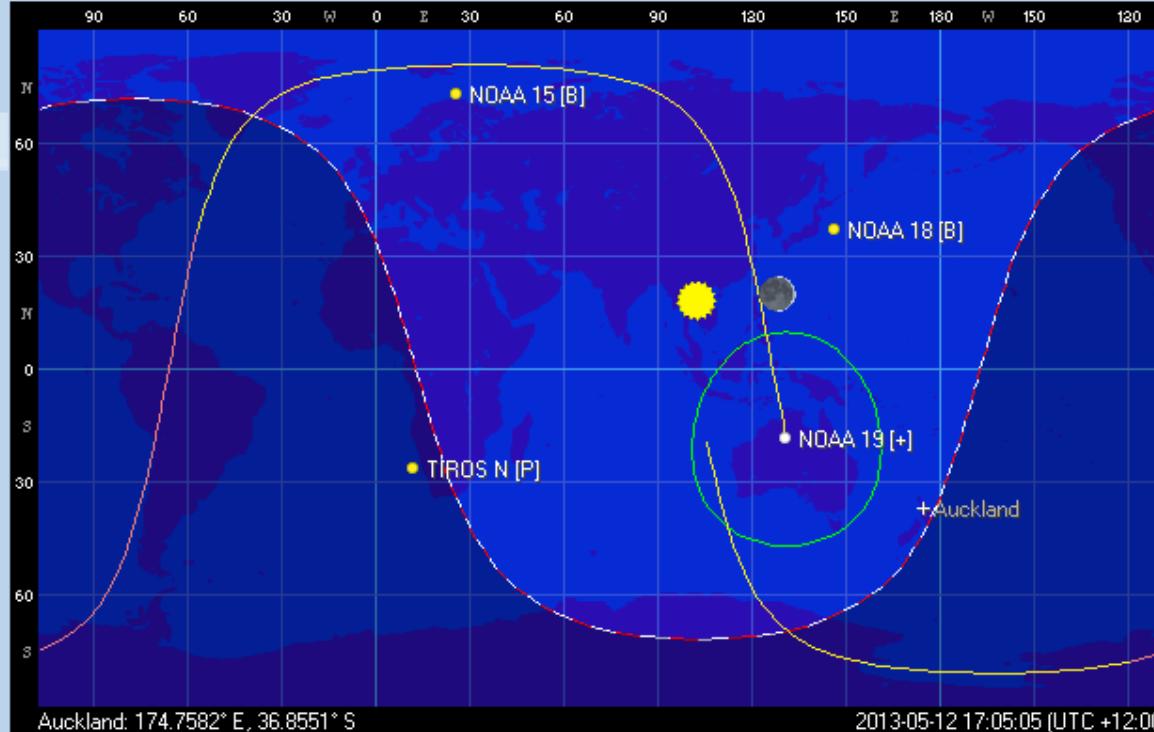
# Tracking Satellite

- 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



- 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	Dlink/MHz	Receive/doppler	Dlink mode
283.3	145.000	144.997686	FM-W
Elevation	Uplink/MHz	Transmit/doppler	Uplink mode
-11.7	145.000	145.002314	

DDE conversation with driver is NOT active

Driver:

Object:



SDR# RSDEV Freq v1.3.3 - IQ Imbalance: Gain = 0.956 Phase = -0.02°

Play Stop  IQ Stream  Wave file

Radio

NFM  AM  LSB  USB

WFM  DSB  CW-L  CW-U

Frequency

Center

Shift

Front end

Filter type

Filter bandwidth

Filter order

Squelch  CW/Shift

Step size

Snap to grid  12.5 kHz

Correct IQ  Swap I & Q

FM Stream  Mark Peaks

Audio

AF Gain

Samplerate

Input

Output

Latency (ms)

Filter Audio

AGC

Use AGC  Use Hard

Threshold (dB)

Decay (ms)

Slope (dB)

FFT Display

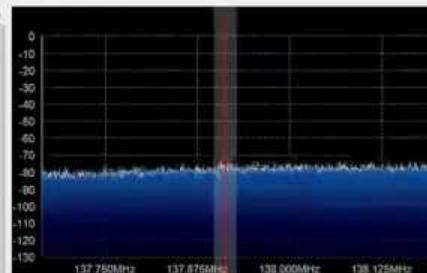
View

Window

Resolution

Gradient

S-Attack



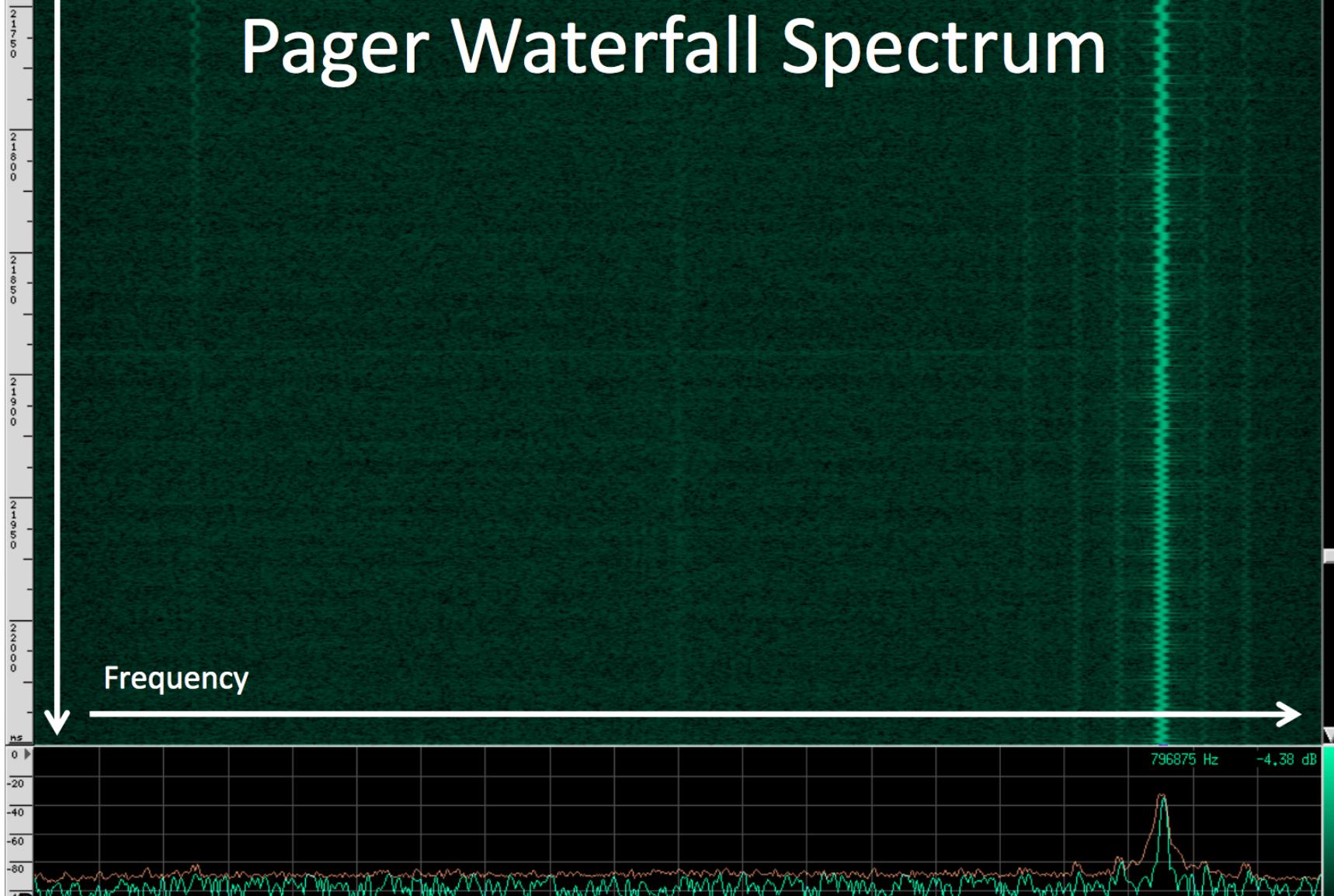
# Balint Seeber – Applications Specialist



Time

# Pager Waterfall Spectrum

Frequency



## Decoder 0

X

From beginning  
 From start offset

Invert  
 Invert first bit

Baudot  
 7-bit ASCII  
 8-bit ASCII  
 Swap endian-ness

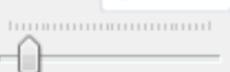
Highlight differences  
 Show decoded data  
 Accumulate data  
 Extra newline

Offset: 0  


Extend Offset

Sync settings

Show bits

Columns: 4  


Straight  Flip Flop  
 Diff  Diff (inverted)  
 Prev 0  Prev 1  
 Manchester 0 (IEEE)  
 Manchester 1 (orig)  
 Diff Man 0  BPM  
 Diff Man 1  BPS

Start bit  
 No stop bits Max bits: 4096  
 Stop bit  
 Two stop bits

Dump

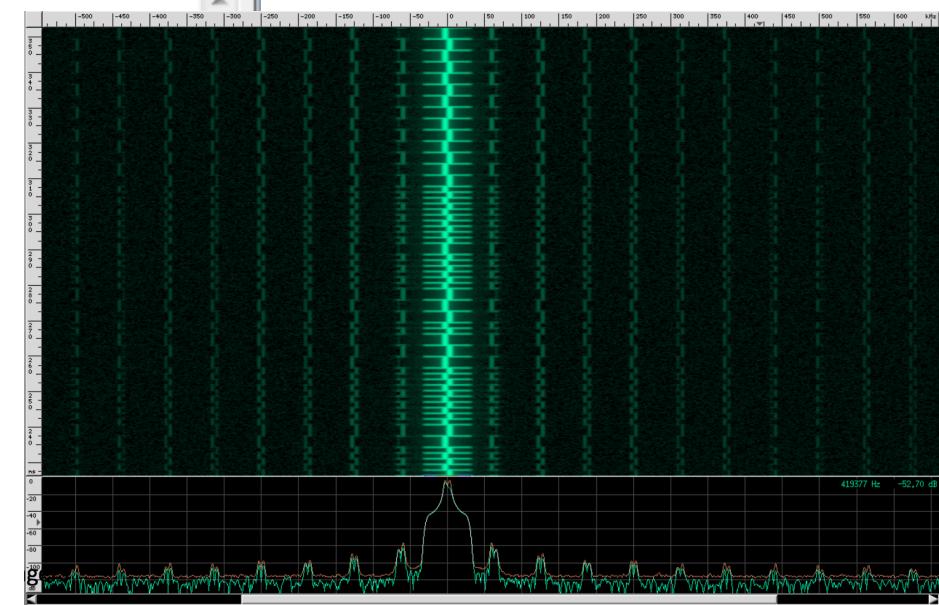
Clear

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>	...

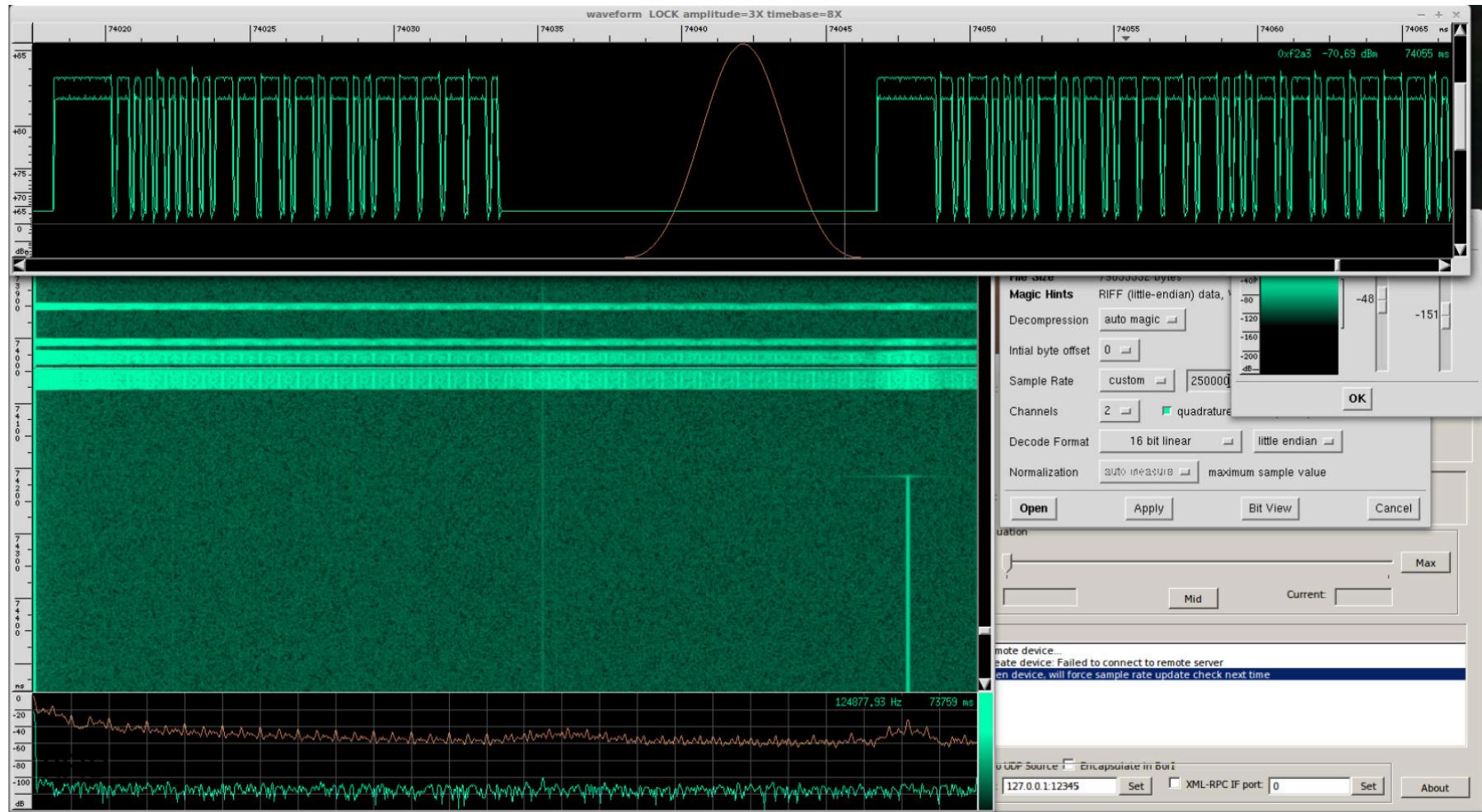
Sum: C1

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



# Jared Boon

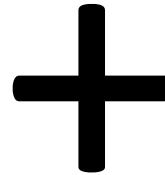
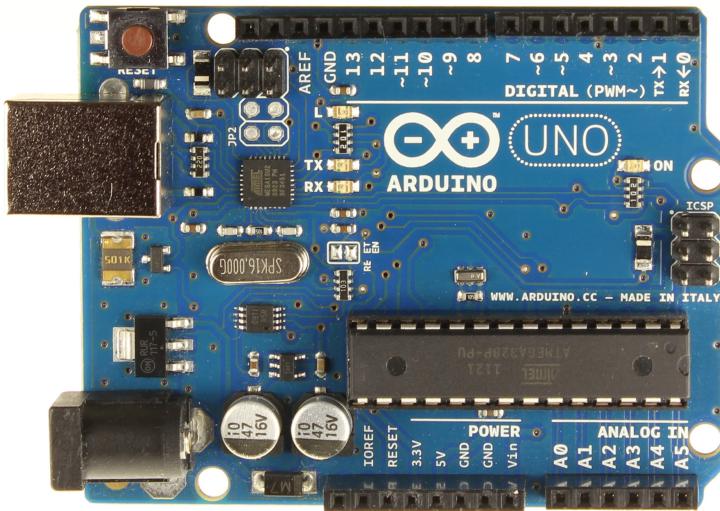
- Tire Pressure Monitoring System (TPMS)
- All cars in the US sold after 2008 have it
- We should know if one of our tires are low
- Guess what? There's no “wire” going into your tire to check the pressure, it's wireless ☺



# 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

# Pranks?



# More Ideas

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