Software Defined Radio (SDR)

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.
- Receiver 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 USD 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

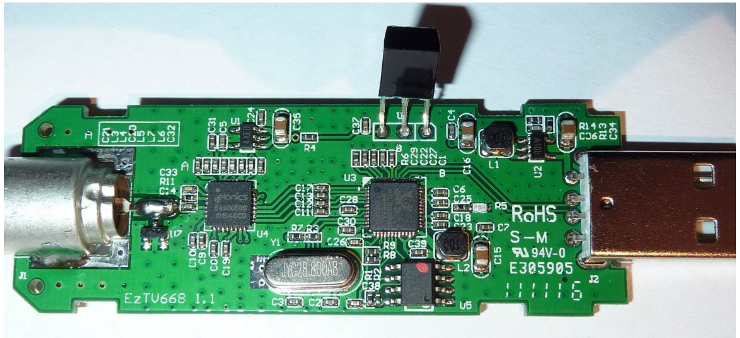
Geeky Specs

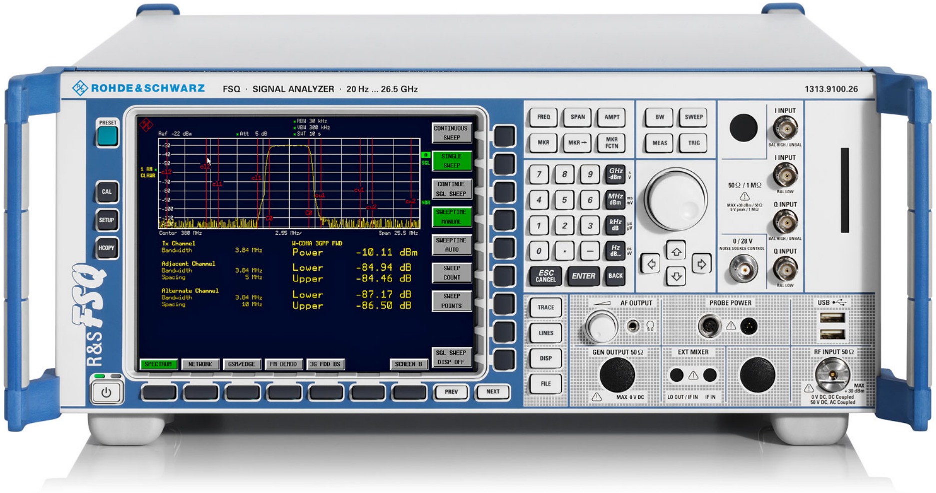
- DVBT:48.25 ~863.25 MHZ
- FM radio: 87.5~108 MHZ
- DAB radio: L-Band-1452960~1490624 KHZ
- VHF—174928~ 239200 KHz
- Will work for both for software defined radio and DVB video capture (where available)
- Compatible with most SDR software. Approx range: 25MHz-1700MHz
- 6-8 MHz Bandwidth

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

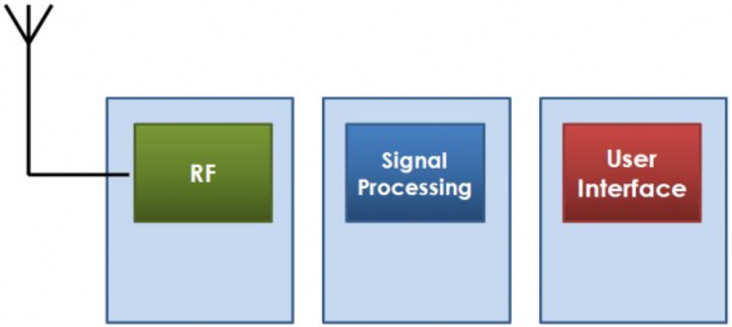
Other SDR Hardware



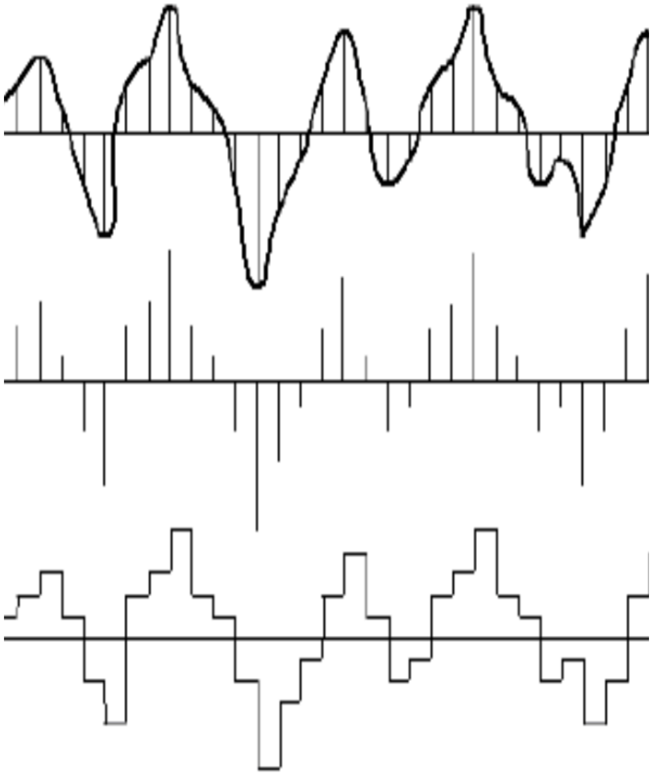


How does SDR work?

- 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

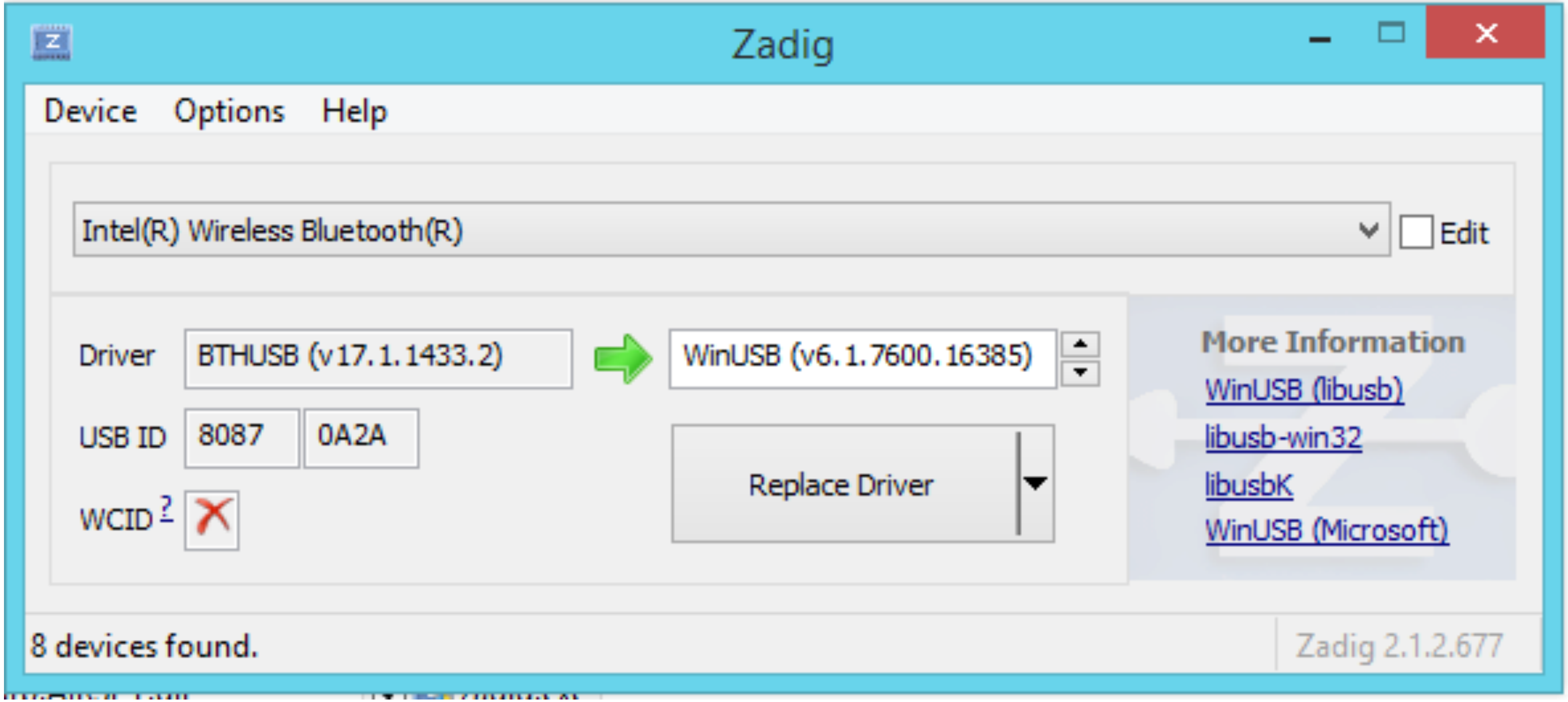


Original → Sampled → Reconstructed



Activity: Update Driver

1. Plug the USB dongle into your computer
2. Open up the **sdrsharp** folder and run **zadig.exe**
3. Under **Options** click **List All Devices**
4. Change the drop-down menu to read **RTL2838UHIDIR**
5. Click on **Replace Driver**



Intel(R) Wireless Bluetooth(R) □ Edit

Driver BTHUSB (v17.1.1433.2) → WinUSB (v6.1.7600.16385)

USB ID 8087 0A2A

WCID ? ✗

8 devices found.

Zadig 2.1.2.677

So what exactly did we do?

- Remember, this hardware was intended to do two basic things: TV/Radio
- We want to look at other airwaves, so we had to replace the way Windows talked to the hardware with a more advanced language
  - Going from talking to a dog to an engineer

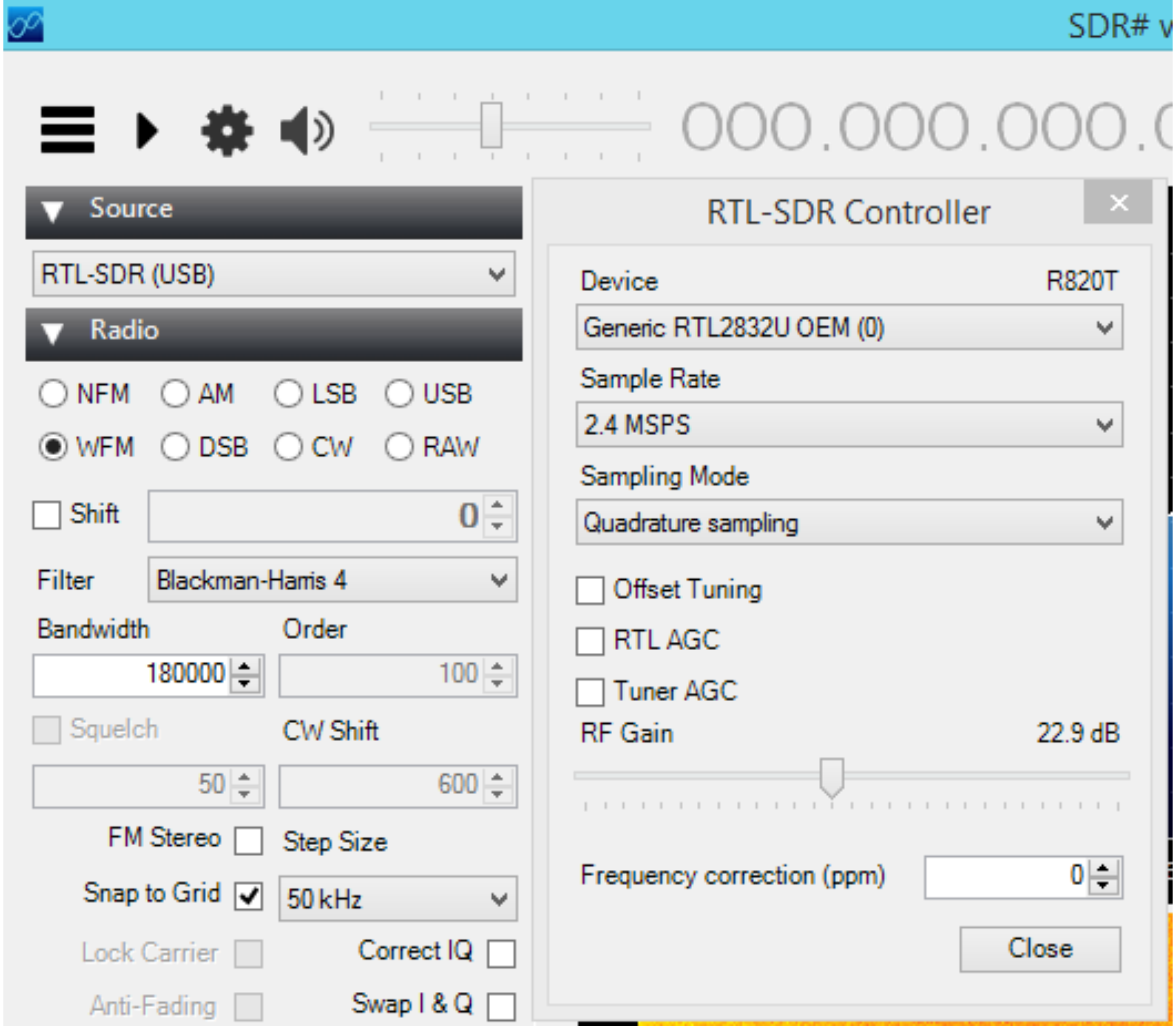
SDR#

Software Defined Radio

- Now that Windows can control the USB dongle a little more extensively, we need software
- Lot's of packages exist for Windows and Linux
- SDR# is the go-to for basic SDR
- It's already installed for you, but for your reference: http://sdrsharp.com/#sdrsharp

Open up SDR#

1. Double-click on **SDRSharp.exe**
2. Underneath **Source** choose **RTL-SDR (USB)**
3. Click on the Gear (**Configure**) and set the gain about half-way up
   – By default the RF gain is set at zero. A gain of zero will probably receive nothing but very strong broadcast FM



RTL-SDR (USB)

○ NFM ○ AM ○ LSB ○ USB
● WFM ○ DSB ○ CW ○ RAW

□ Shift 0

Filter: Blackman-Harris 4

Bandwidth: 180000

Order: 100

□ Squelch: 50

CW Shift: 600

FM Stereo □

Snap to Grid ☑

Step Size: 50 kHz

Lock Carrier □

Correct IQ □

Anti-Fading □

Swap I & Q □

RTL-SDR Controller

Device: R820T

Generic RTL2832U OEM (0)

Sample Rate: 2.4 MSPS

Sampling Mode: Quadrature sampling

□ Offset Tuning

□ RTL AGC

□ Tuner AGC

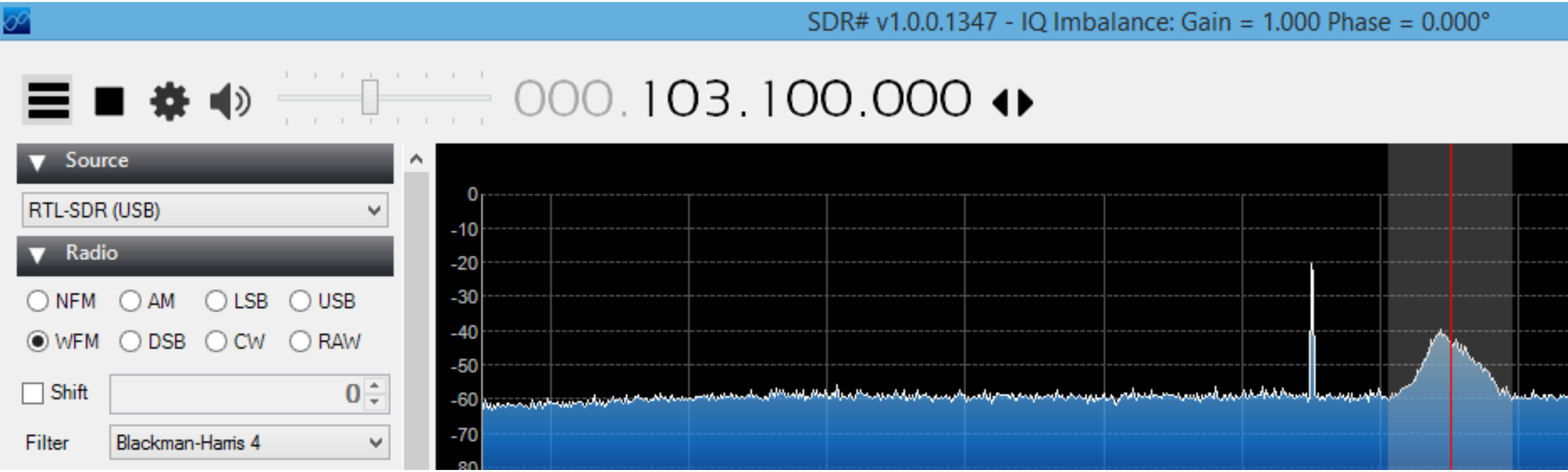
RF Gain: 22.9 dB

Frequency correction (ppm): 0

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

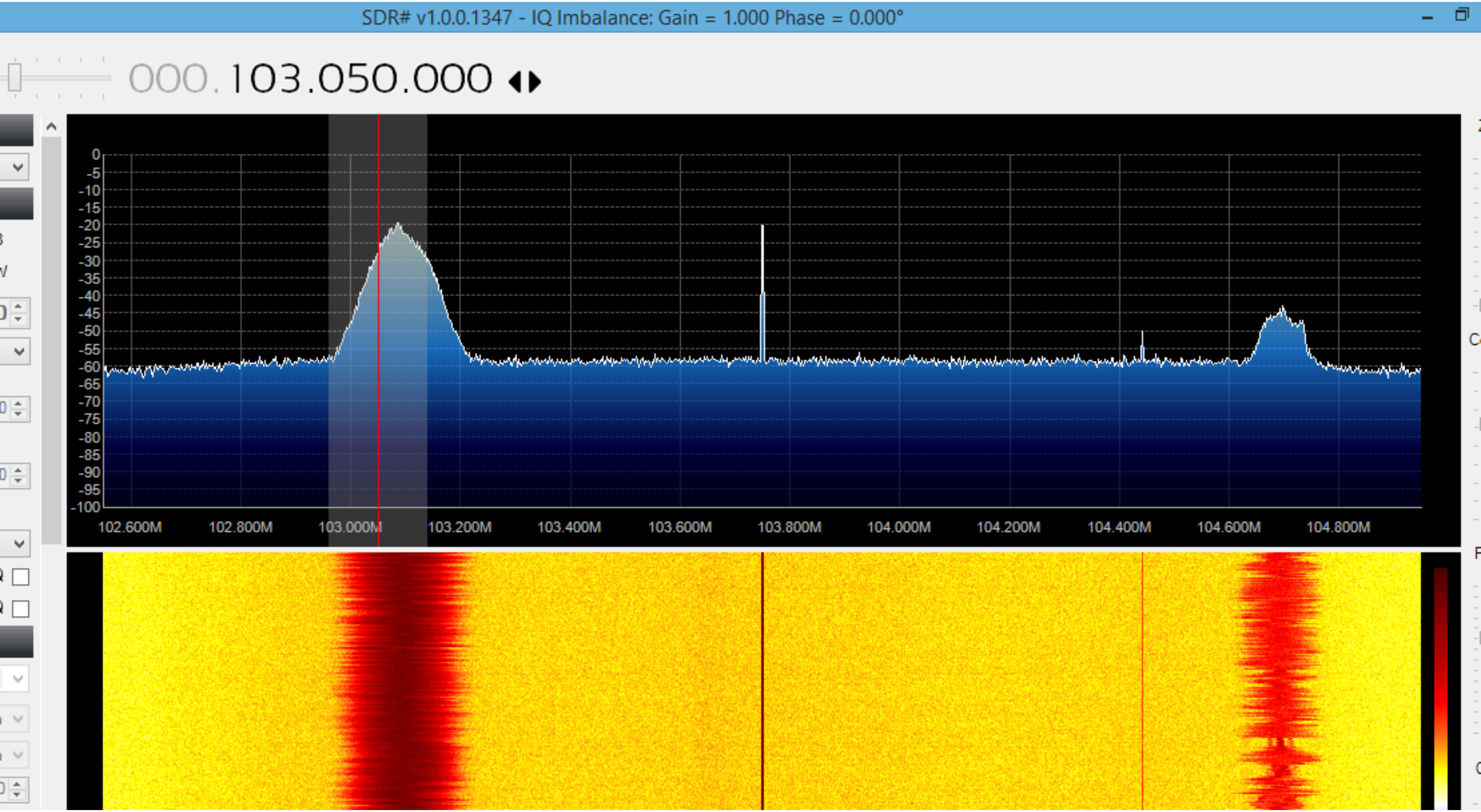
● WFM ○ DSB ○ CW ○ RAW

□ Shift 0

Filter Blackman-Harris 4

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)

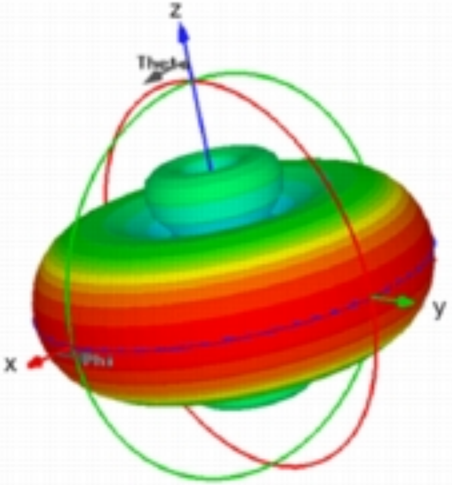


SDR# v1.0.0.1347 - IQ Imbalance: Gain = 1.000 Phase = 0.000°

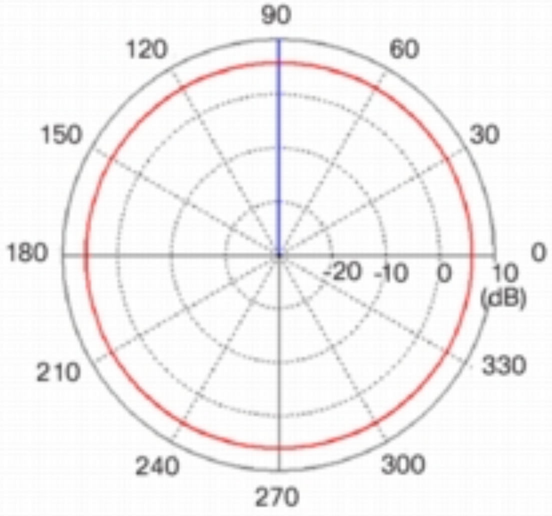
000.103.050.000

Antenna Types

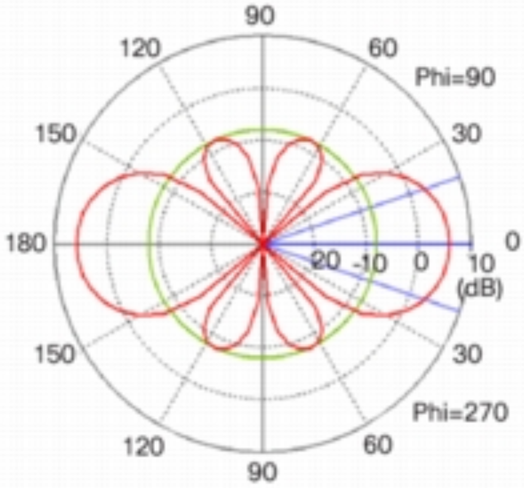
- Omnidirectional
  - Extends your range in all directions
- Directional
  - Let's you focus your signal in a particular direction
- Sensitivity – measured in dBi
  - dBi - gain of an antenna as referenced to an ISOTROPIC (omnidirectional) source
  - Remember, every 3 dBi = double the sensitivity



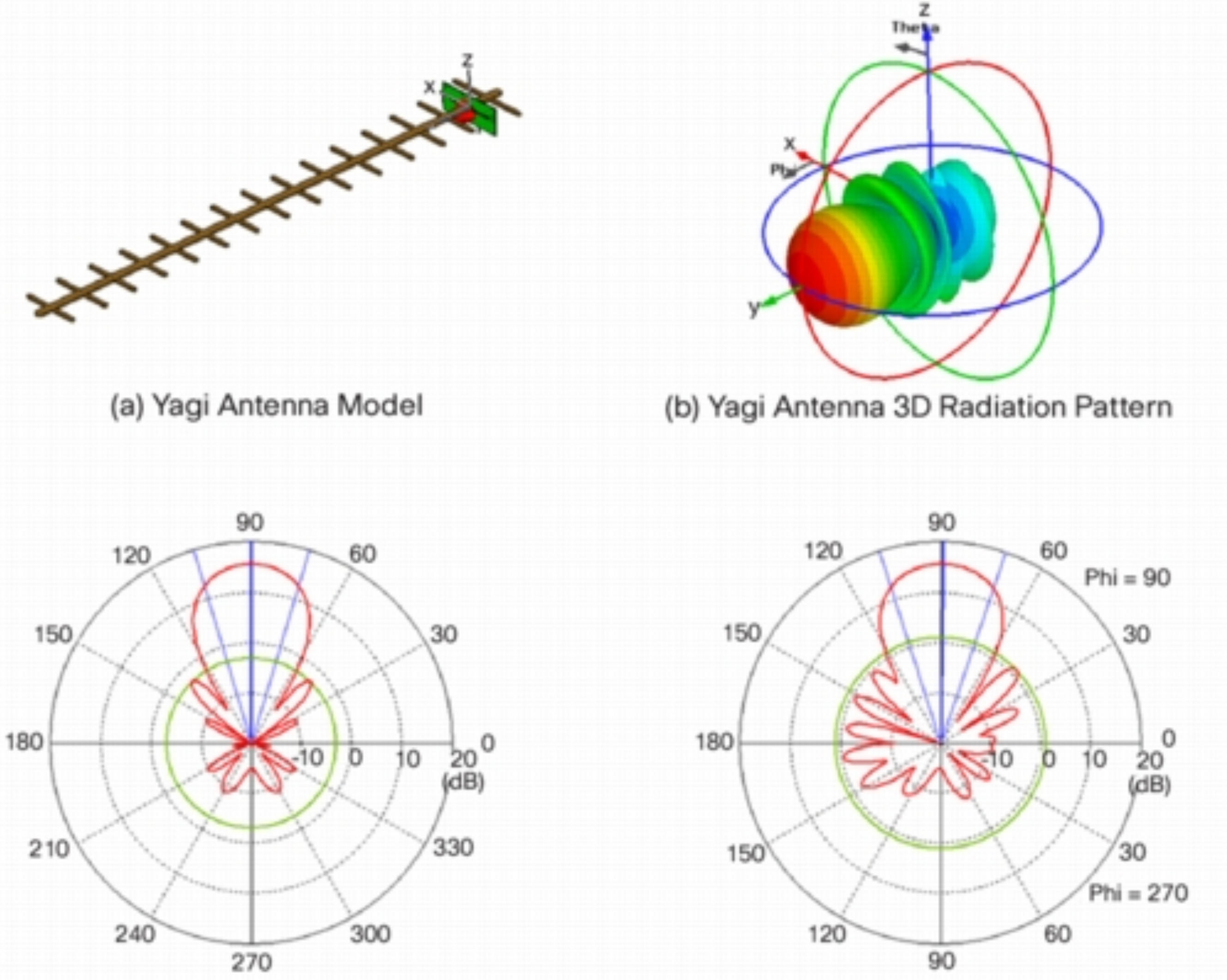
(a) 5.8 dBi Omni 3D Pattern



(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

Can you find me AM radio?

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?

MIDLAND
NOAA
SNOOZE
TORNADO
ALERT
12:05
7CH
S.A.M.E. DIGITAL WEATHER / ALL HAZARDS ALERT RADIO WITH AM FM

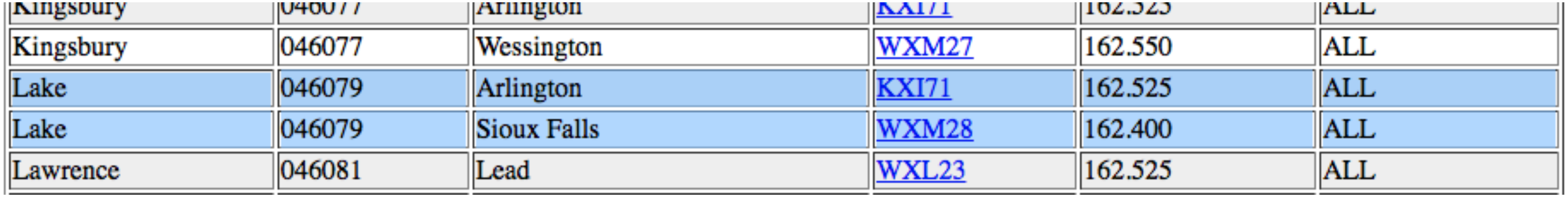
RTL-SDR Weather Station

- 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

NATIONAL OCEANIC AND ATMOSPHERIC ADMINISTRATION
NOAA
U.S. DEPARTMENT OF COMMERCE

Tuning into Weather

1. Find your nearest NOAA weather station frequency here: http://www.nws.noaa.gov/nwr/coverage/county_coverage.html



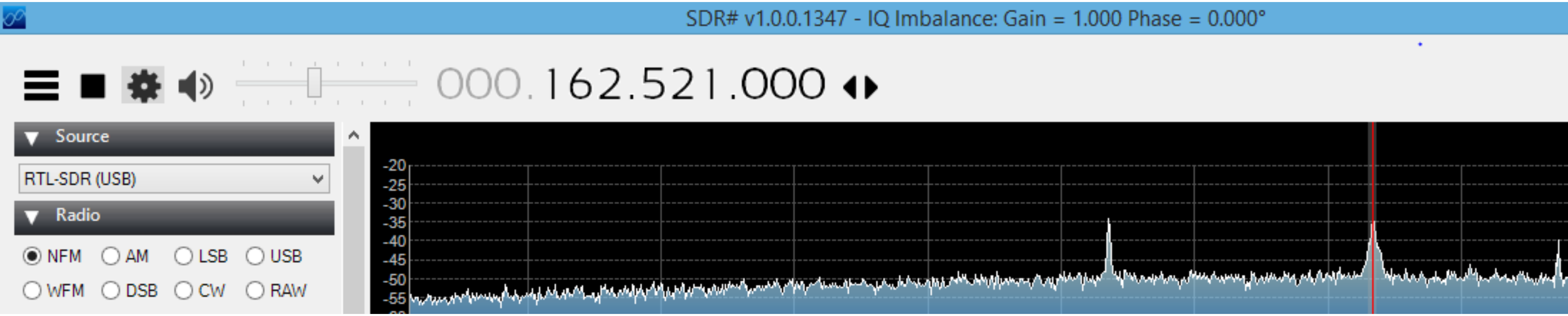
Kingsbury	046077	Arlington	KXI71	162.525	ALL
Kingsbury	046077	Wessington	WXM27	162.550	ALL
Lake	046079	Arlington	KXI71	162.525	ALL
Lake	046079	Sioux Falls	WXM28	162.400	ALL
Lawrence	046081	Lead	WXL23	162.525	ALL

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



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

000.162.521.000

▼ Source

RTL-SDR (USB)

▼ Radio

● NFM ○ AM ○ LSB ○ USB
○ WFM ○ DSB ○ CW ○ RAW

Weather Recording (Backup)

Let’s talk Airplanes

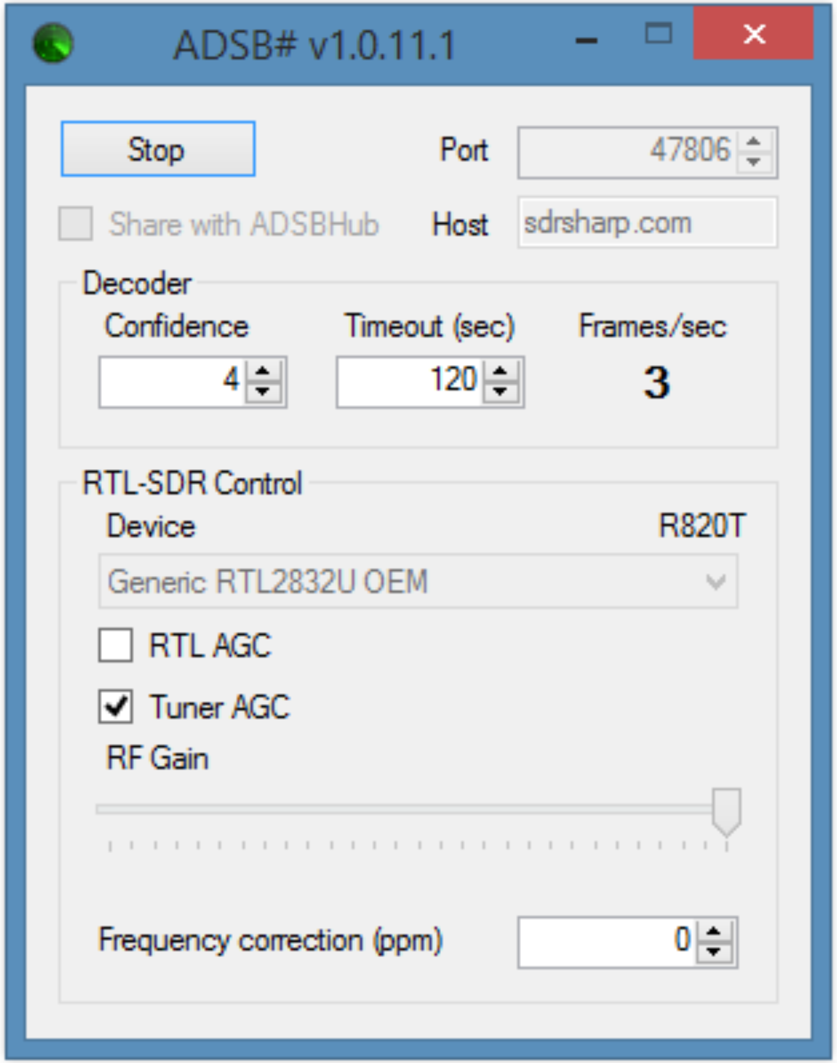
- ADS-B - Automatic dependent surveillance – broadcast
  - Cooperative surveillance for tracking aircraft
- Aircraft determines its position and broadcasts it for safety measures
- Sent in clear text, they want people to read this so planes don’t crash

Two Pieces of Software

- ADSB#
  - Takes all of the ADSB data and decodes the packets (frames)
- ADSB Scope
  - Plots the data gained from ADSB# to a nice map
- **Disclaimer**: Madison is not a destination for many planes, fingers crossed one is passing over

ADSB

1. It's already sitting in your sdrsharp folder
2. When the GUI opens, click **Start**
    1. You may need to allow access through your firewall (ADSB Scope will connect this way)
3. Download ADSB Scope - http://www.sprut.de/electronic/pic/projekte/adsb/adsb_all.zip
4. Extract ADSB Scope into your sdrsharp folder (or wherever, just remember where)



Port 47806

□ Share with ADSBHub

Host sdrsharp.com

Decoder

Confidence	Timeout (sec)	Frames/sec
4	120	3

RTL-SDR Control

Device R820T

Generic RTL2832U OEM

□ RTL AGC

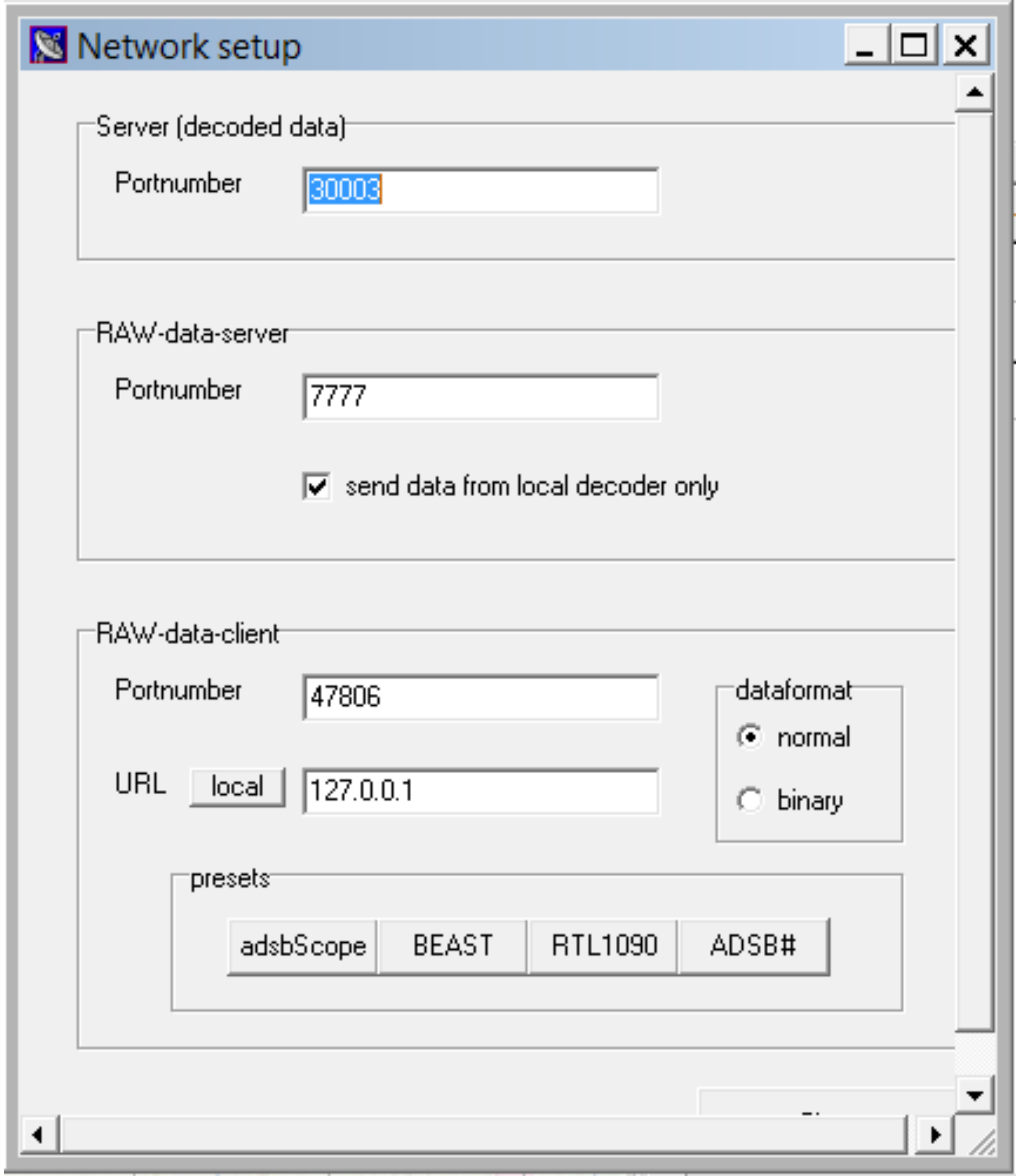
☑ Tuner AGC

RF Gain

Frequency correction (ppm) 0

ADSB Scope

5. Launch **adsbscope27_256** and change your location on the map
6. Once you found your spot, click **Navigation → set Receiver Location** and then **OK**
7. Click **other → Network setup**
8. Make sure the Portnumber matches ADSB# and the URL is set to **127.0.0.1**
9. Click **Close**



Network setup

Server (decoded data)

Portnumber 30003

RAW-data-server

Portnumber 7777

☑ send data from local decoder only

RAW-data-client

Portnumber 47806

URL 127.0.0.1

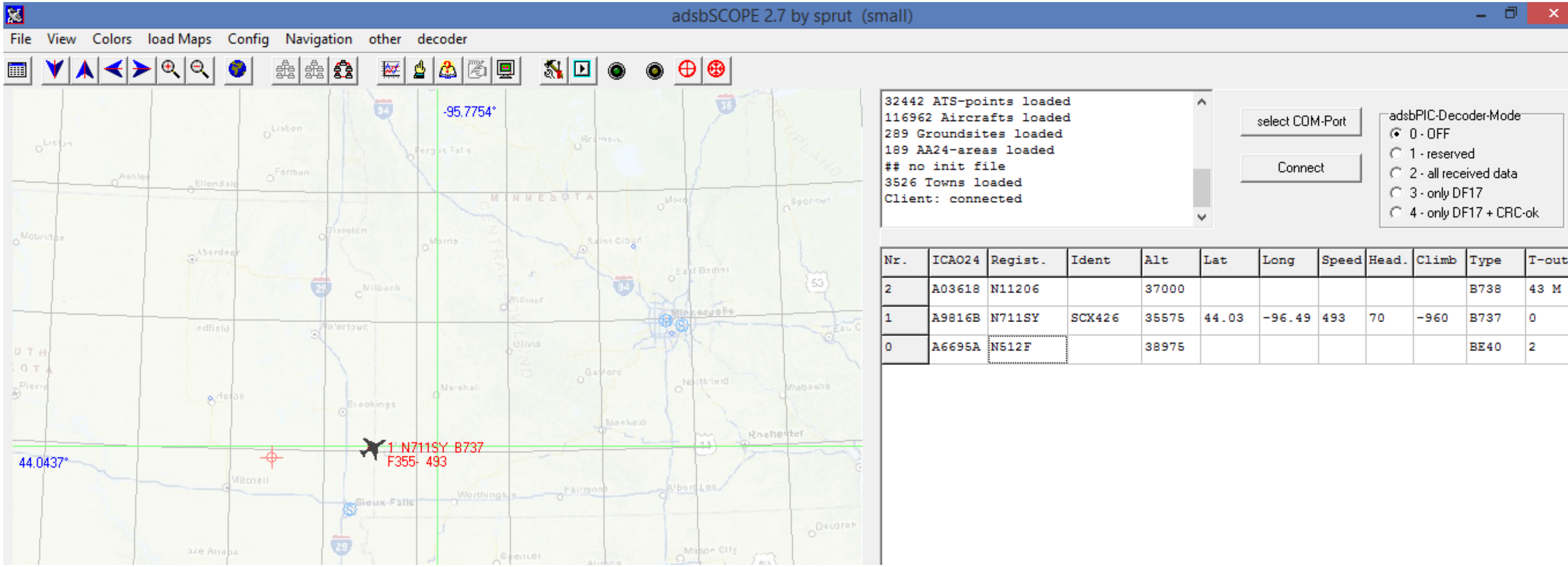
dataformat

● normal

○ binary

ADSB Scope

10. Go to **other → Network → Raw-data Client active**
11. Wait, hopefully a plane will fly over!

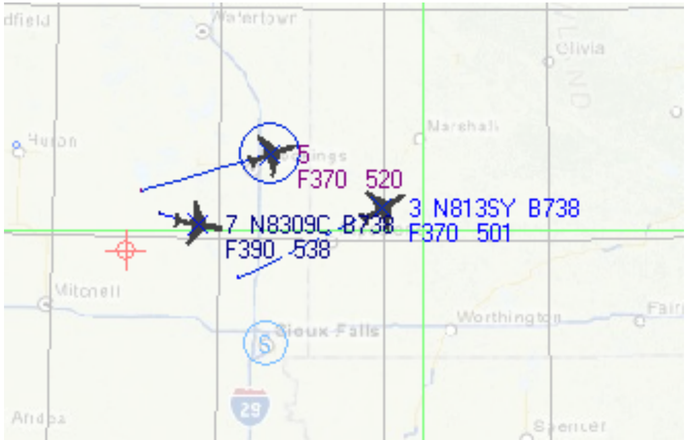


```
32442 ATS-points loaded
116962 Aircrafts loaded
289 Groundsites loaded
189 AA24-areas loaded
## no init file
3526 Towns loaded
Client: connected
```

adsbPIC-Decoder-Mode

- ● 0 - OFF
- ○ 1 - reserved
- ○ 2 - all received data
- ○ 3 - only DF17
- ○ 4 - only DF17 + CRC-ok

Nr.	ICAO24	Regist.	Ident	Alt	Lat	Long	Speed	Head.	Climb	Type	T-out
2	A03618	N11206		37000						B738	43 M
1	A9816B	N711SY	SCX426	35575	44.03	-96.49	493	70	-960	B737	0
0	A6695A	N512F		38975						BE40	2



Don’t Stop at 30K Feet

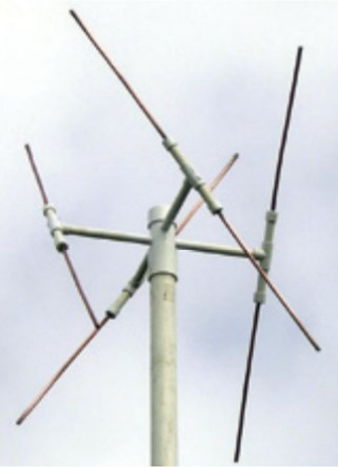
- Planes are very cool, but I like space a little better…
- How about gathering some information from satellites?
  - Our friends, the NOAA, have satellites sending images back for weather purposes
- This gets a little more complicated though

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

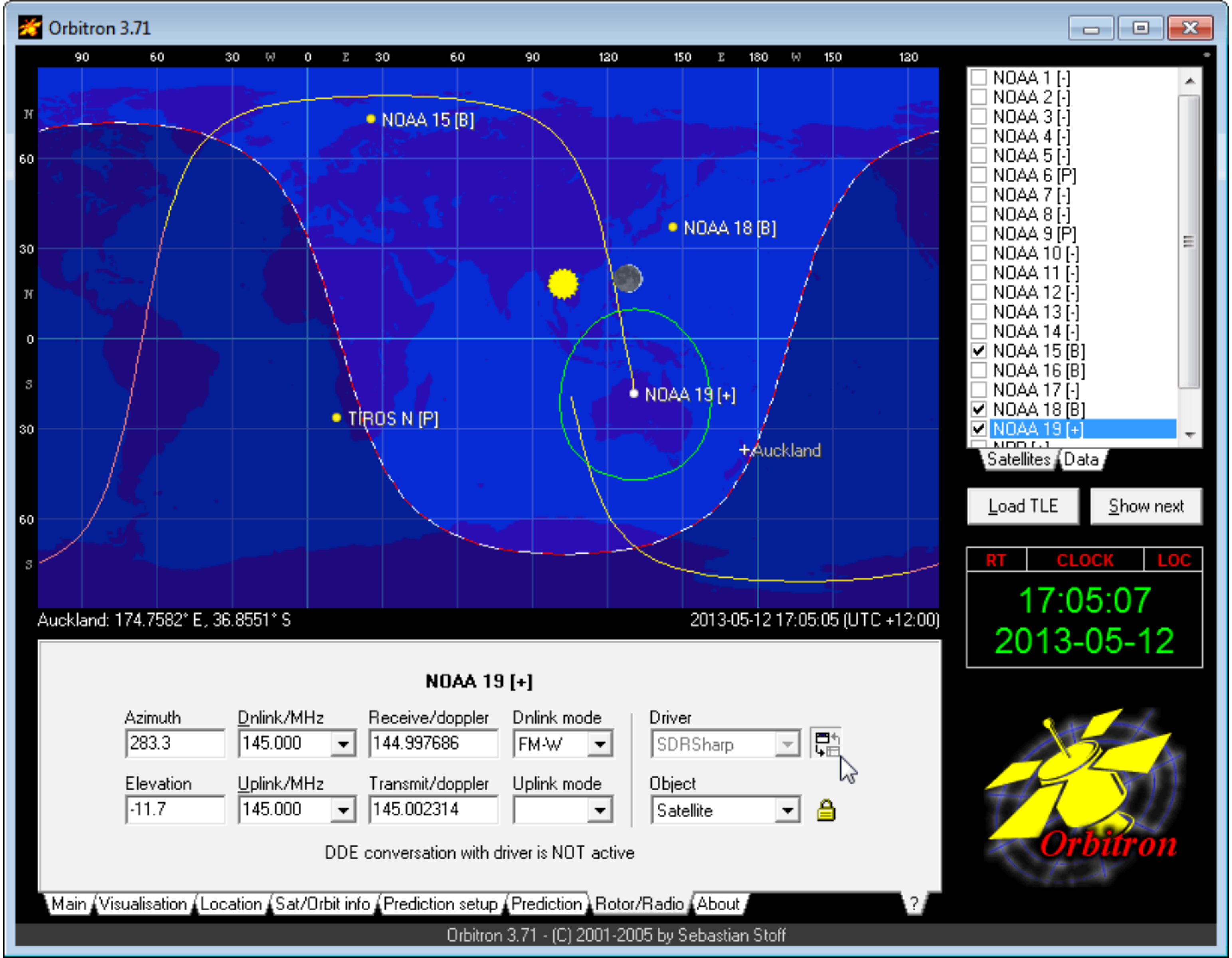


Tracking Satellite

- 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
  - WXtoImg
- 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 [+]

Auckland: 174.7582° E, 36.8551° S

2013-05-12 17:05:05 (UTC +12:00)

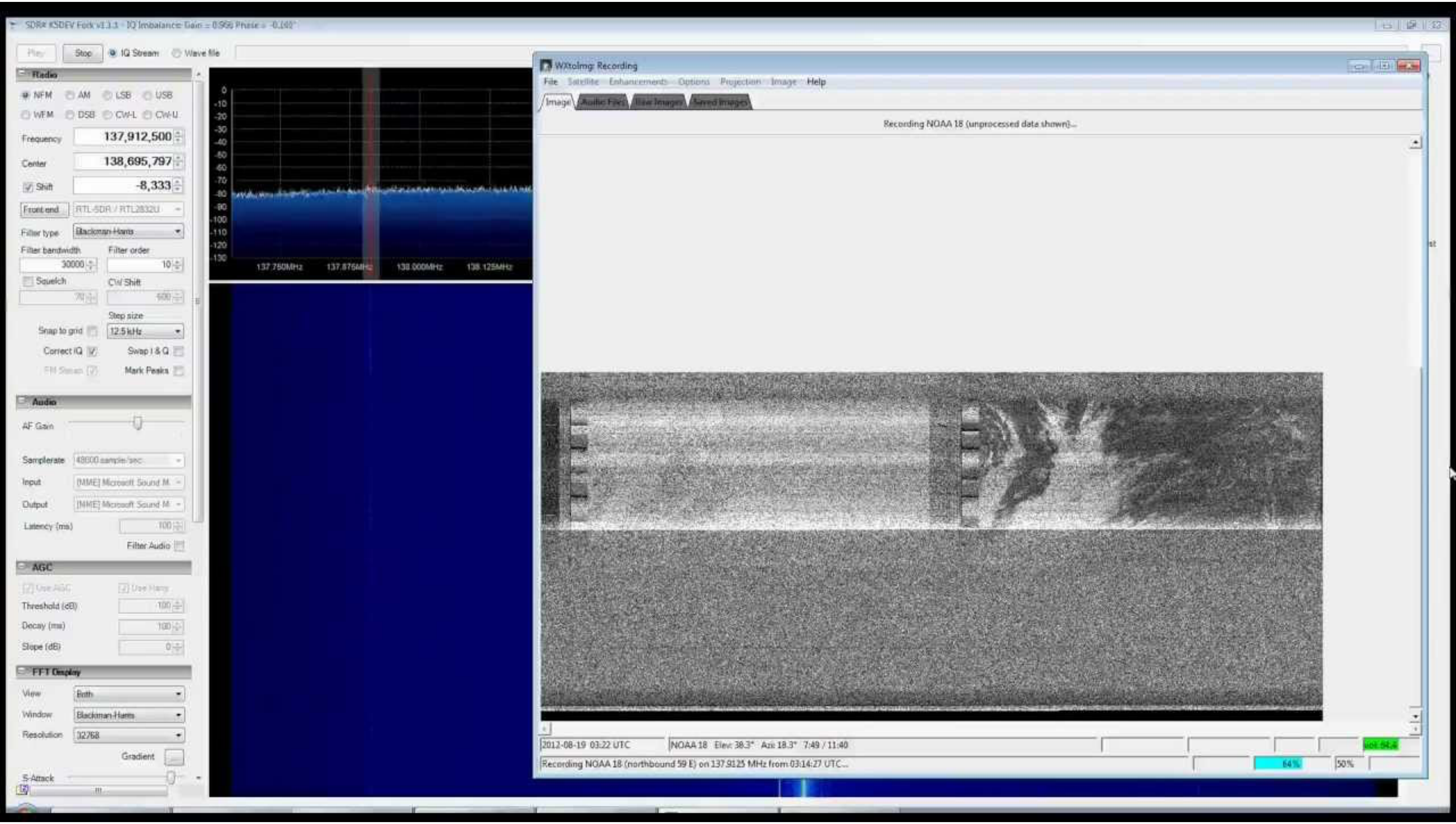
17:05:07
2013-05-12

NOAA 19 [+]

Azimuth: 283.3
Elevation: -11.7
Dnlink/MHz: 145.000
Uplink/MHz: 145.000
Receive/doppler: 144.997686
Transmit/doppler: 145.002314
Dnlink mode: FM-W
Uplink mode:
Driver: SDRSharp
Object: Satellite

DDE conversation with driver is NOT active

Orbitron 3.71 - (C) 2001-2005 by Sebastian Stoff



SDR# KSDEV Fork v1.3.3 - IQ Imbalance: Gain = 0.966 Phase = -0.160°

● 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 70 CW Shift 600

Step size 12.5 kHz

Snap to grid □

Correct IQ ☑ Swap I & Q □

FM Stereo ☑ 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

WXtoImg: Recording

Recording NOAA 18 (unprocessed data shown)...

2012-08-19 03:22 UTC

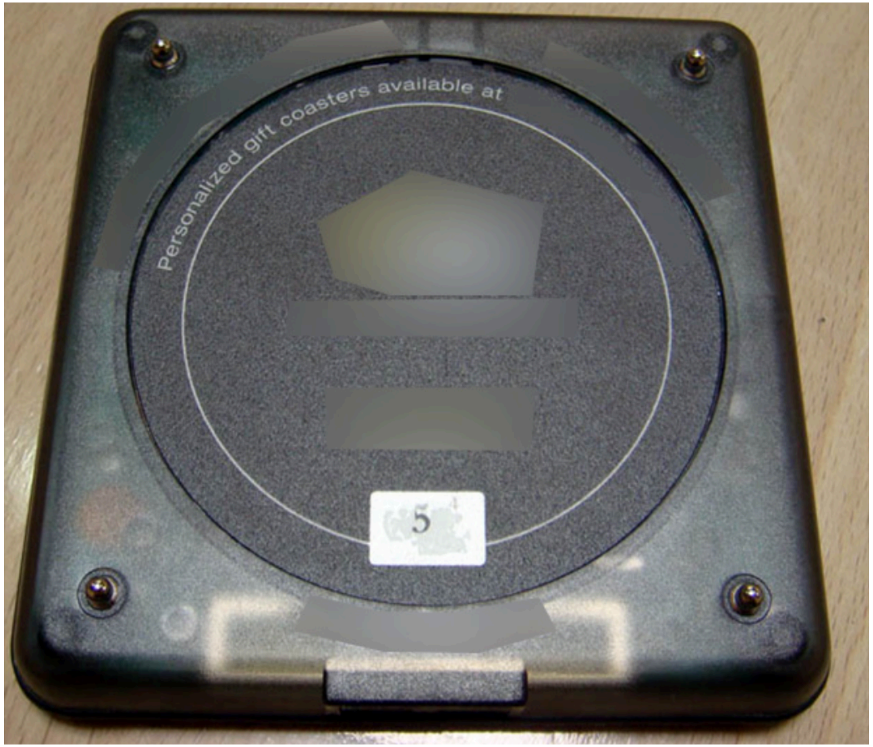
NOAA 18 Elev: 38.3° Azi: 18.3° 7:49 / 11:40

Recording NOAA 18 (northbound 59 E) on 137.9125 MHz from 03:14:27 UTC...

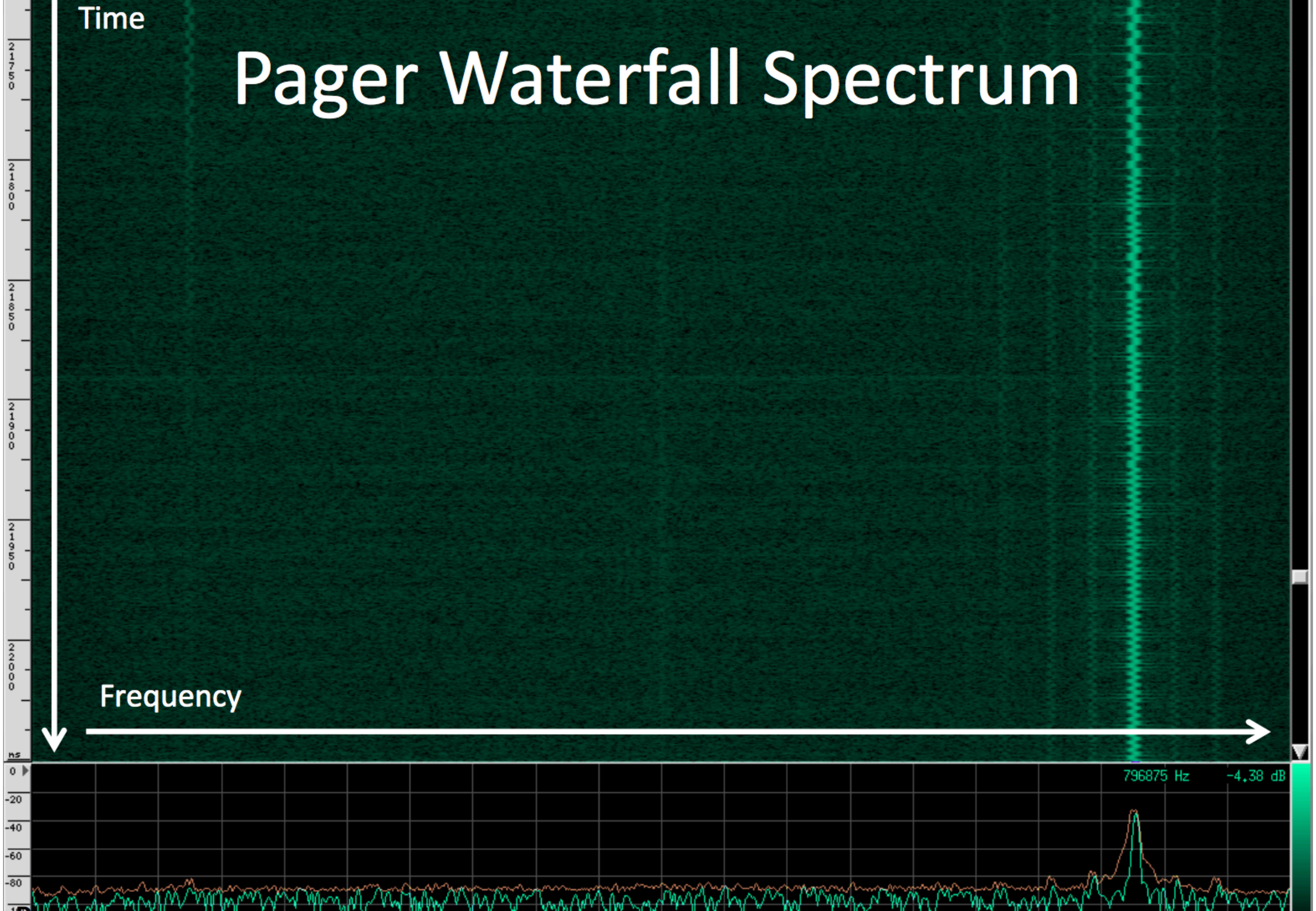
64%

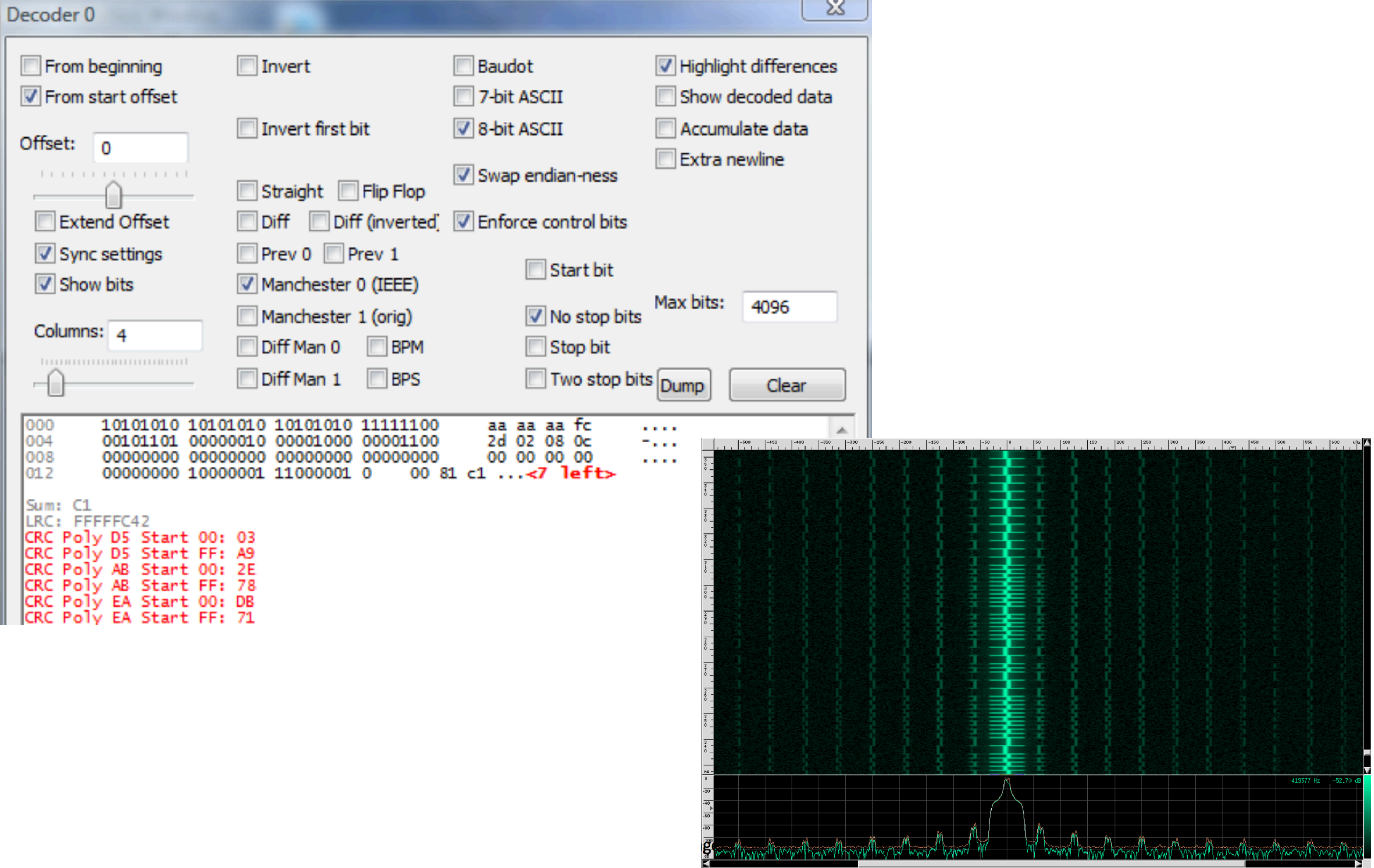
50%

Balint Seeber – Applications Specialist



Pager Waterfall Spectrum





Decoder 0

☐ From beginning
☑ From start offset

Offset: 0

☐ Extend Offset
☑ Sync settings
☑ Show bits

Columns: 4

☐ Invert

☐ Invert first bit

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

☐ Baudot
☐ 7-bit ASCII
☑ 8-bit ASCII

☑ Swap endian-ness

☑ Enforce control bits

☐ Start bit

☑ No stop bits
☐ Stop bit
☐ Two stop bits

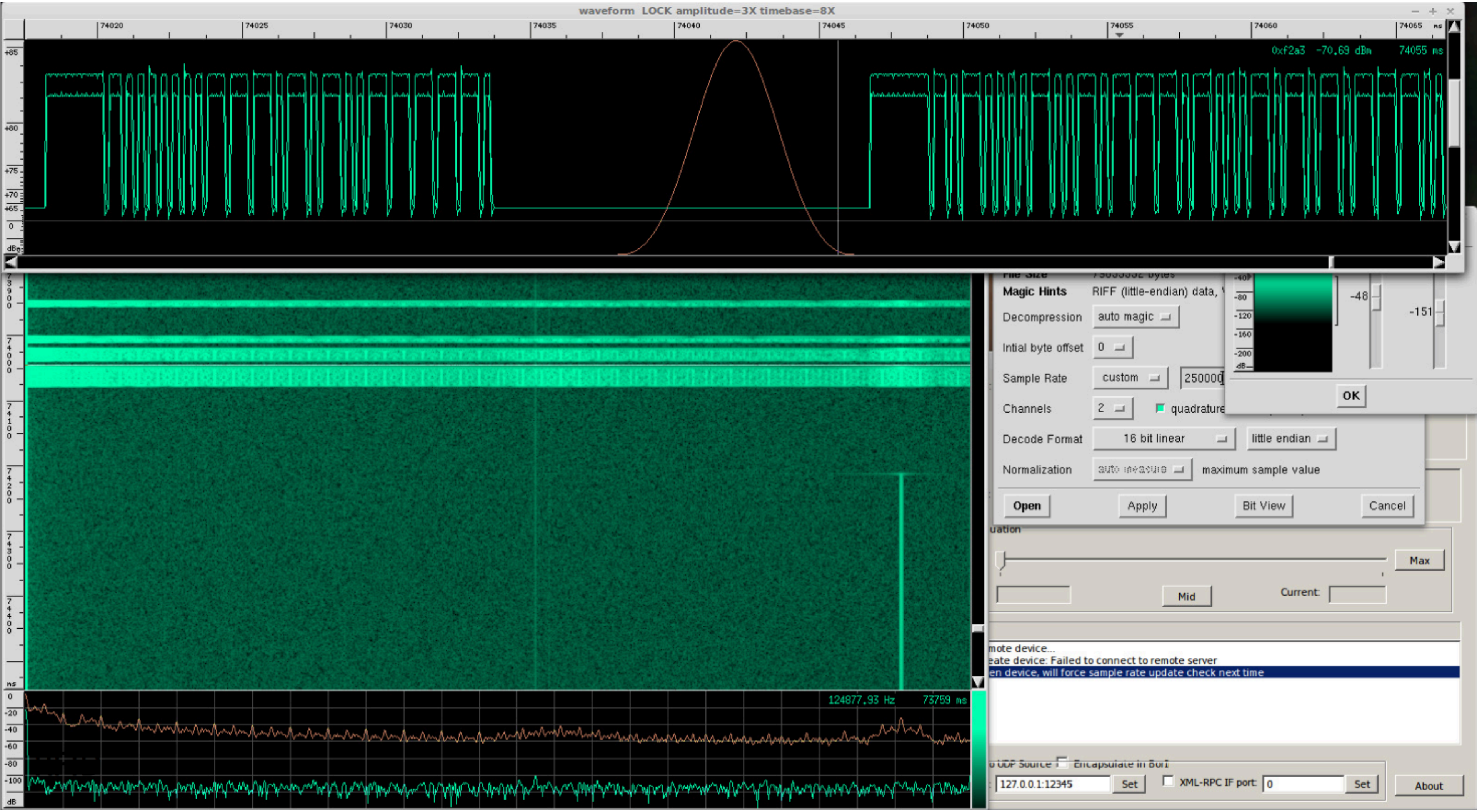
☑ Highlight differences
☐ Show decoded data
☐ Accumulate data
☐ Extra newline

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
```



waveform LOCK amplitude=3X timebase=8X

0xf2a3 -70.69 dBm 74055 ms

124877.93 Hz 73759 ms

File Size 75055552 bytes

Magic Hints RIFF (little-endian) data,

Decompression auto magic

Intial byte offset 0

Sample Rate custom 250000

Channels 2 ☑ quadrature

Decode Format 16 bit linear little endian

Normalization auto measure maximum sample value

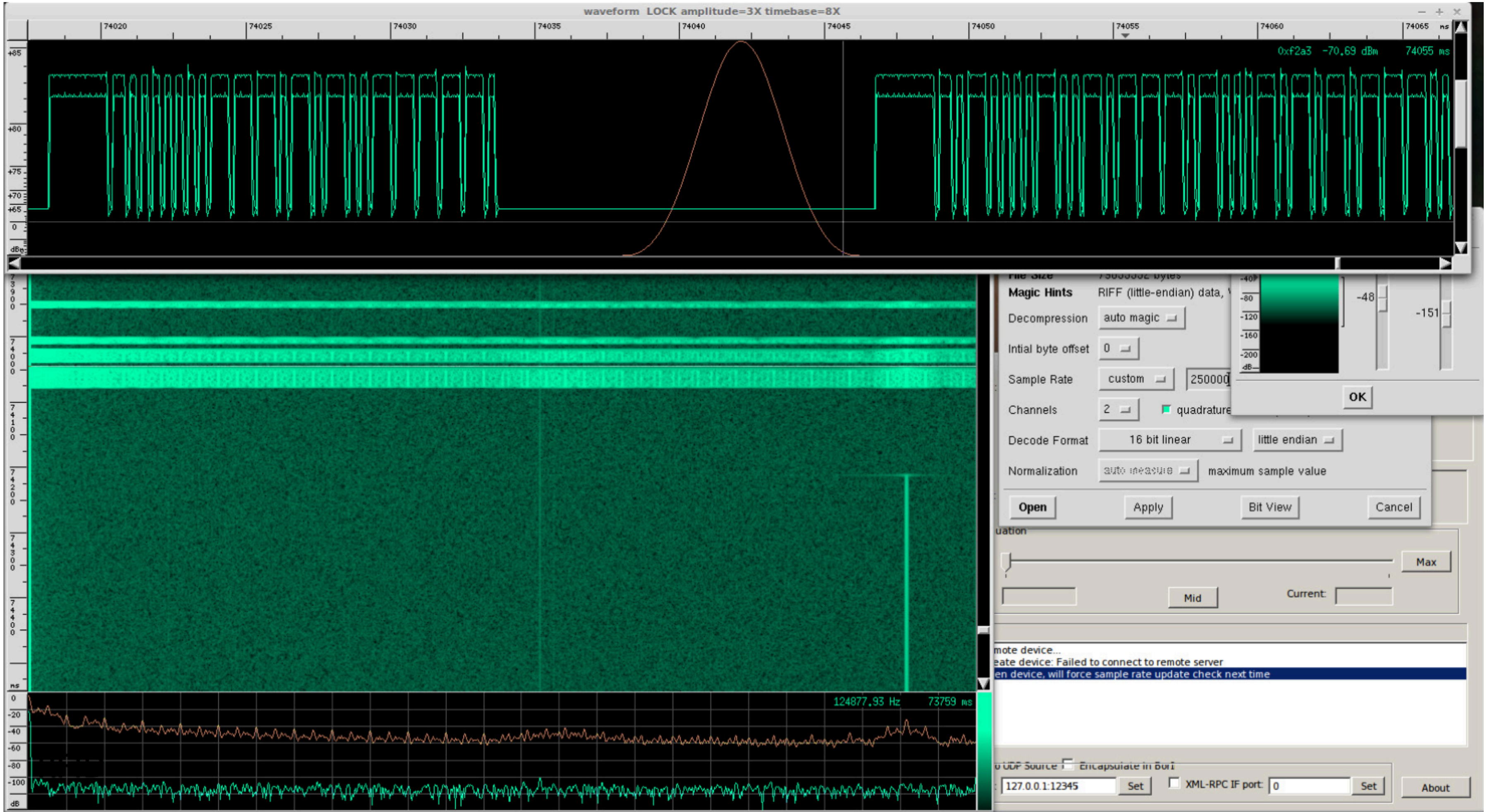
```
mote device...
eate device: Failed to connect to remote server
en device, will force sample rate update check next time
```

UDP Source □ Encapsulate in BorI

127.0.0.1:12345

□ XML-RPC IF port: 0

Toyota Prius Keyless Entry



waveform LOCK amplitude=3X timebase=8X

0xf2a3 -70.69 dBm 74055 ms

124877.93 Hz 73759 ms

Magic Hints RIFF (little-endian) data,

Decompression: auto magic

Intial byte offset: 0

Sample Rate: custom 250000

Channels: 2 ☑ quadrature

Decode Format: 16 bit linear, little endian

Normalization: auto measure maximum sample value

```
mote device...
eate device: Failed to connect to remote server
en device, will force sample rate update check next time
```

Current:

127.0.0.1:12345

□ XML-RPC IF port: 0

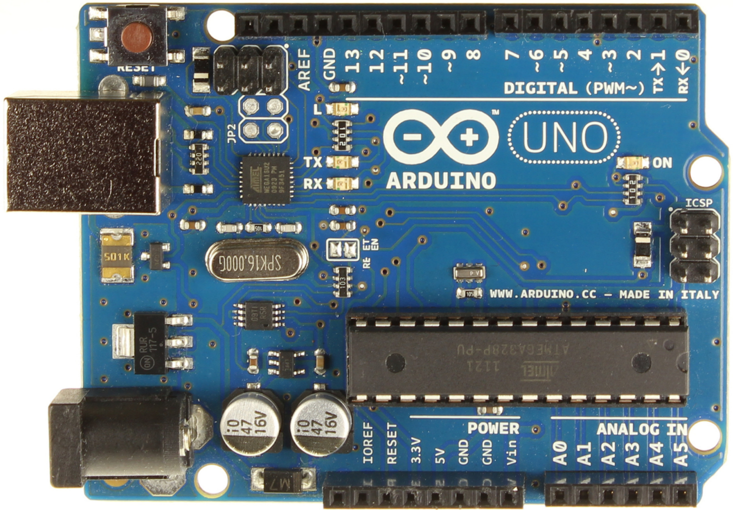
Jared Boon

- 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?


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

+

More Ideas

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