Hacking the Wireless World: Software Defined Radio Exploits

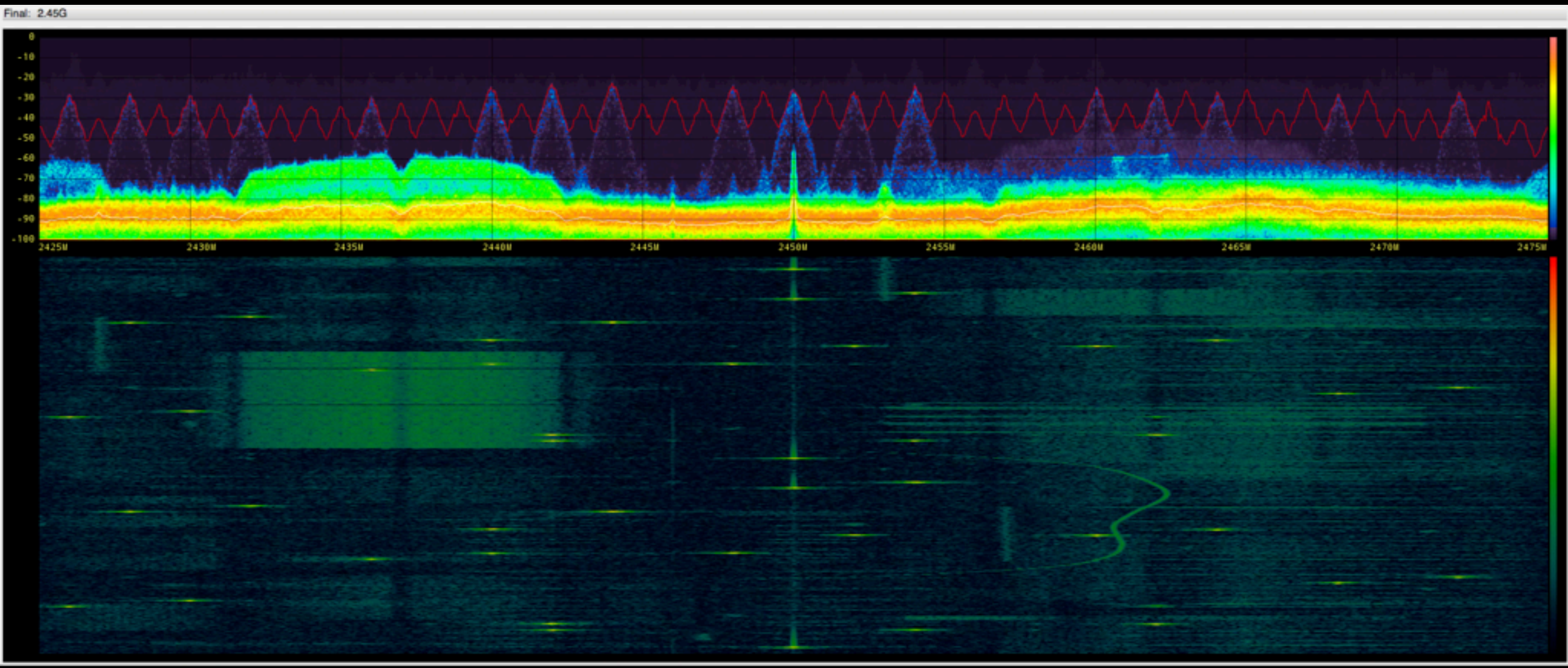
Balint Seeber
Director of Vulnerability Research
Bastille

What are we looking at?

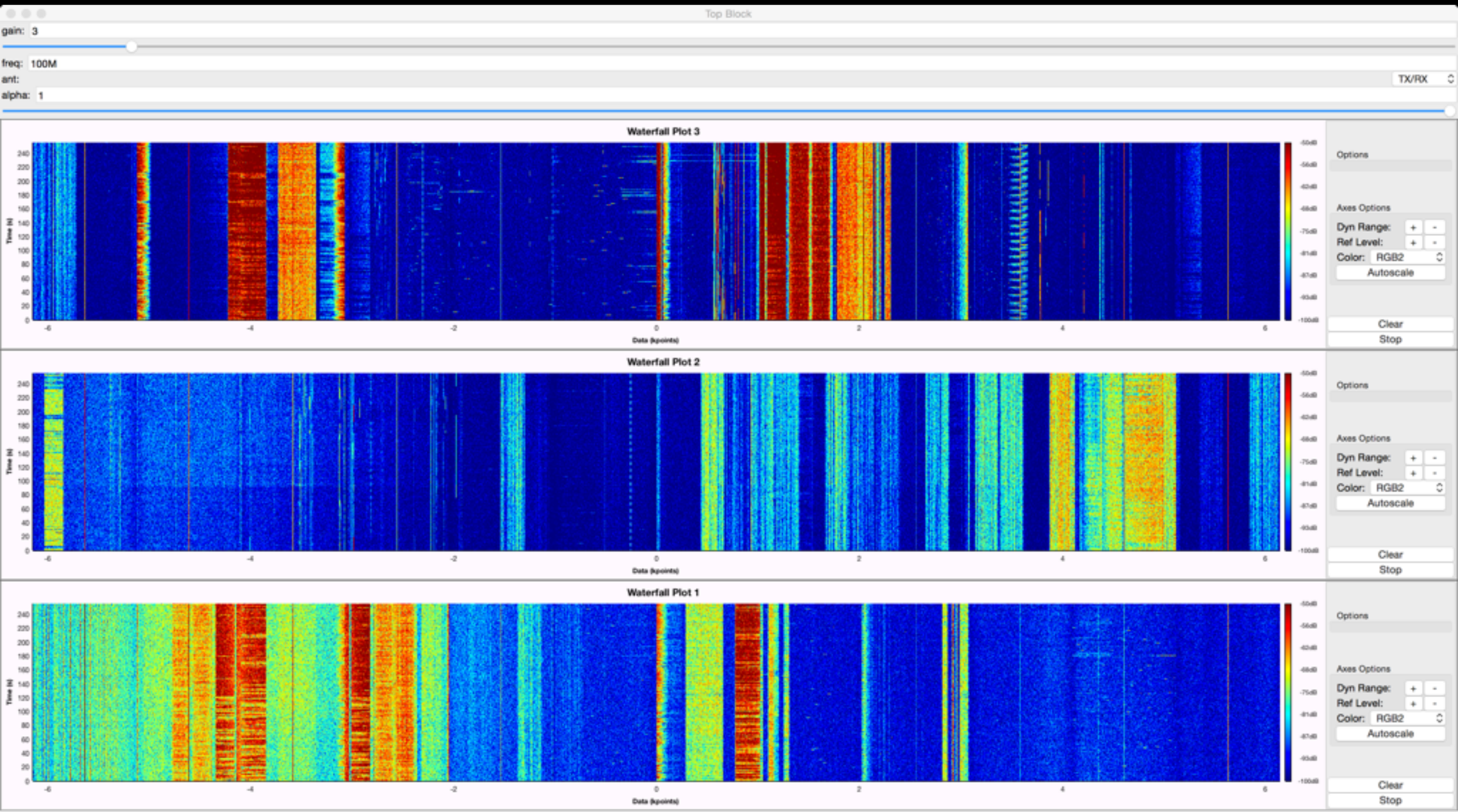
Overview

- The Radio Frequency Spectrum
- Aviation / INMARSAT Aero
- Drones / Airborne Surveillance
- New Signals

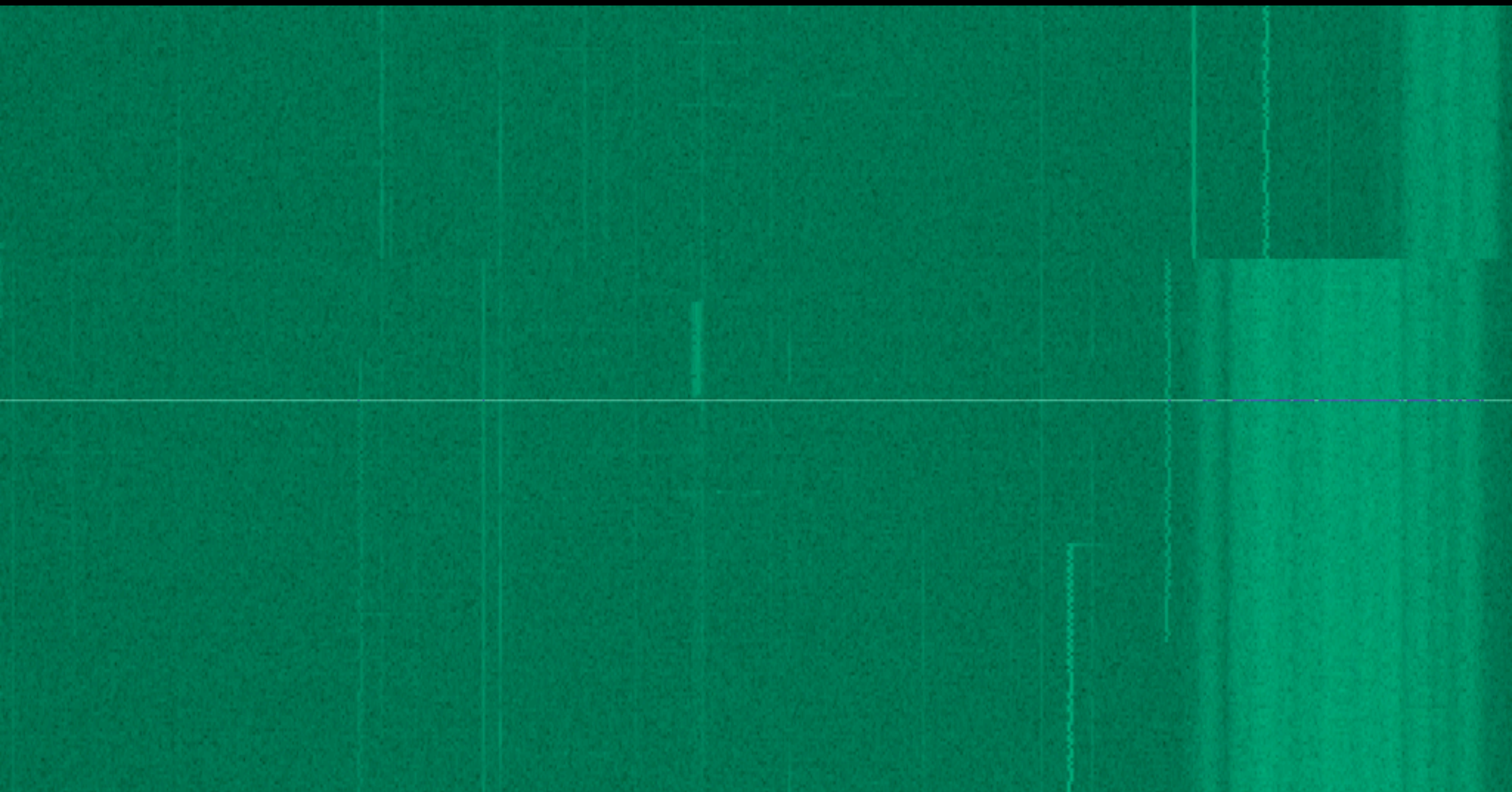
2.4 GHz ISM Band Activity



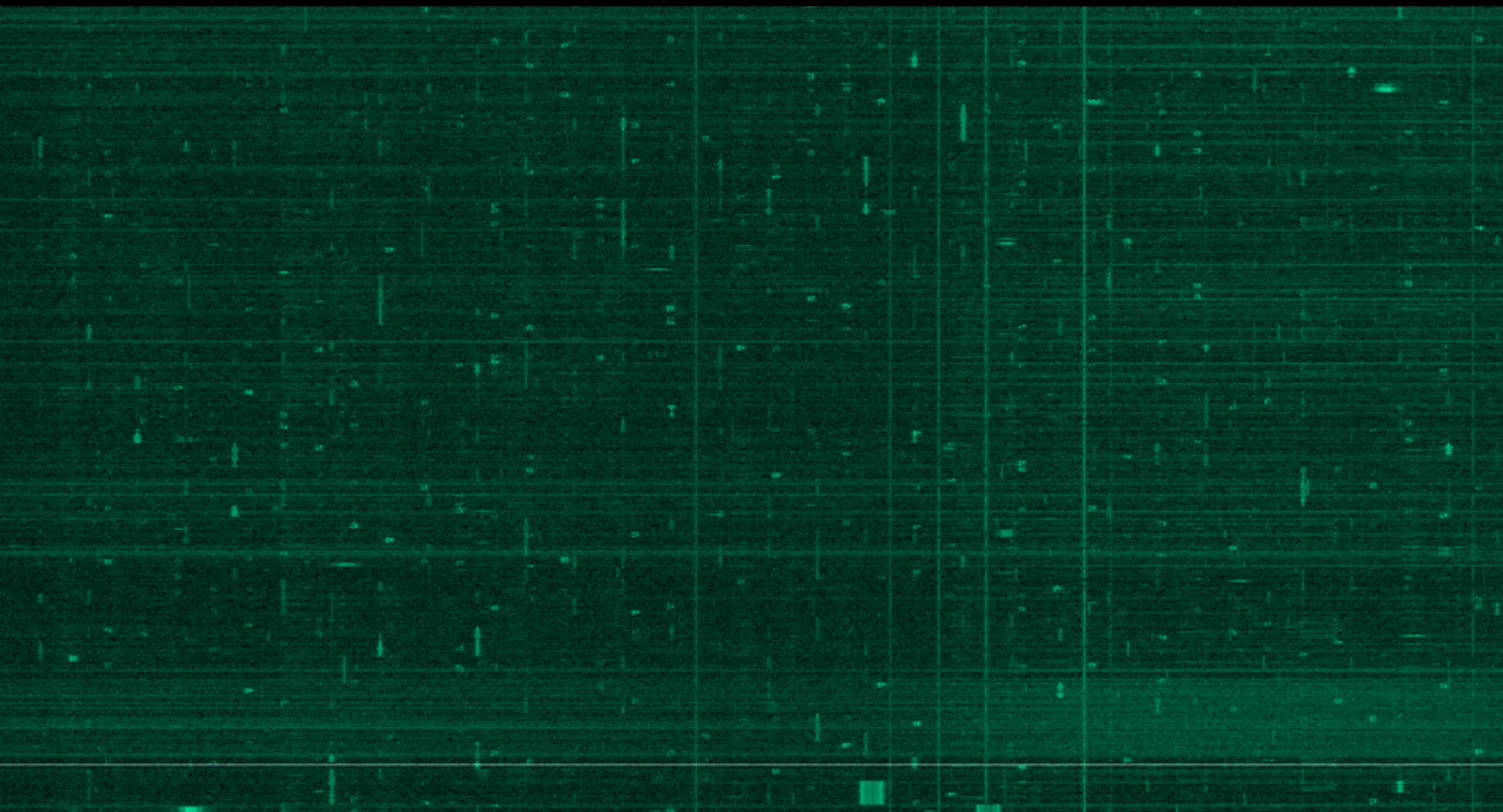
Wideband Activity: 50 MHz - 1.25 GHz



915 MHz ISM Band Activity

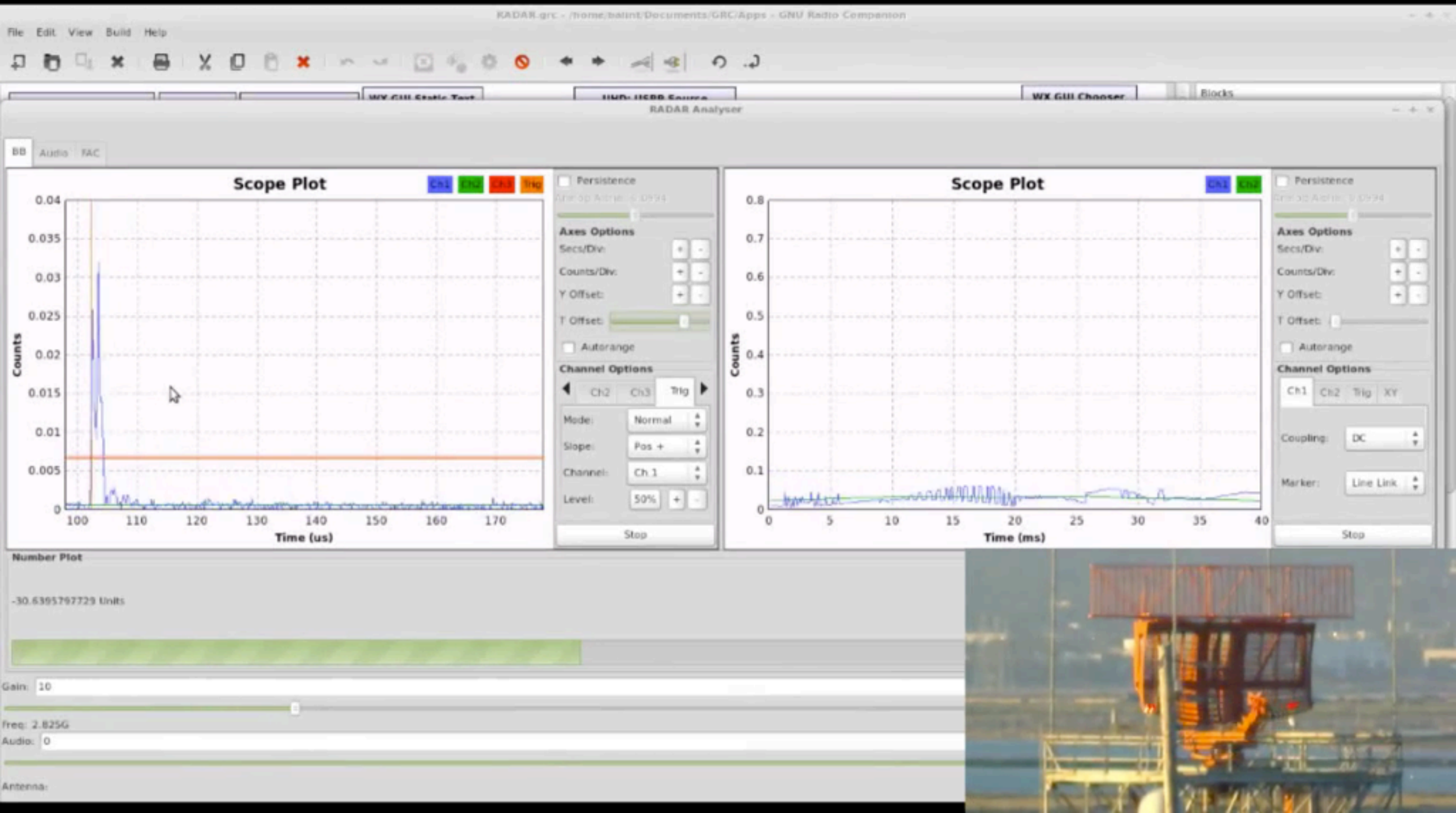


915 MHz ISM Band Activity



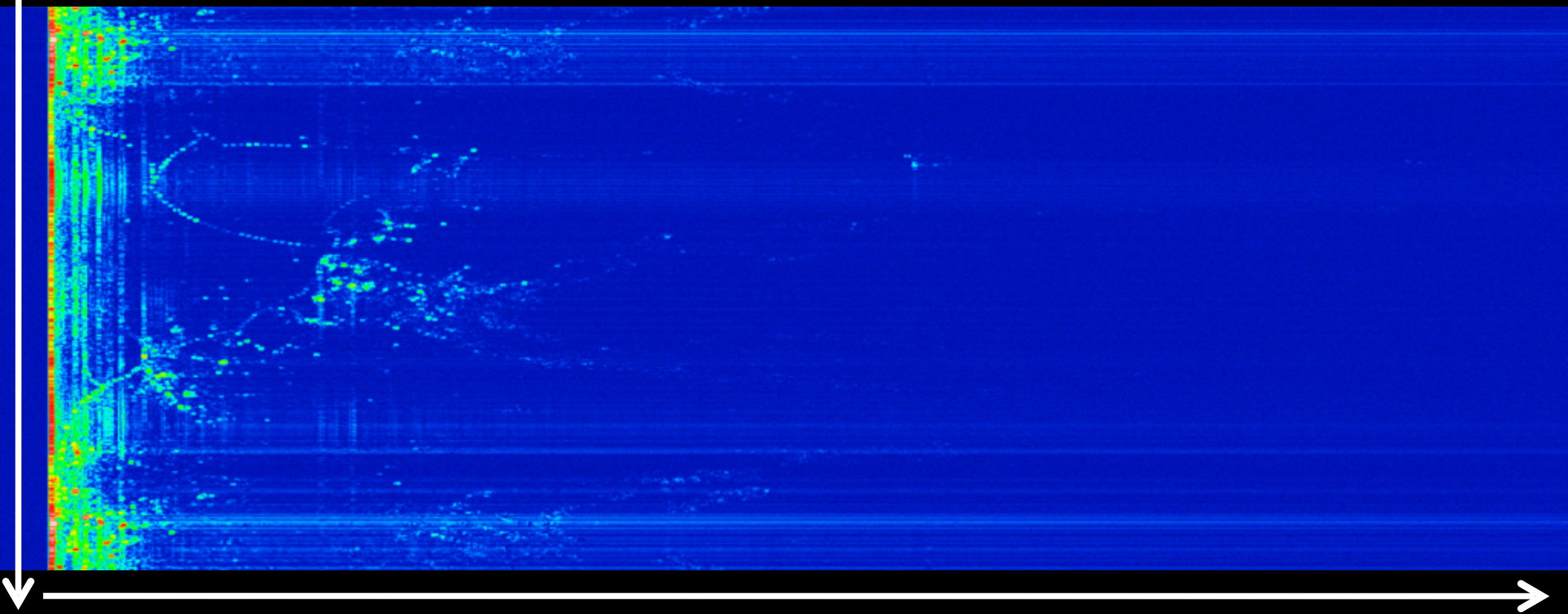
Aviation

Primary **S**urveillance **R**ADAR (PSR)



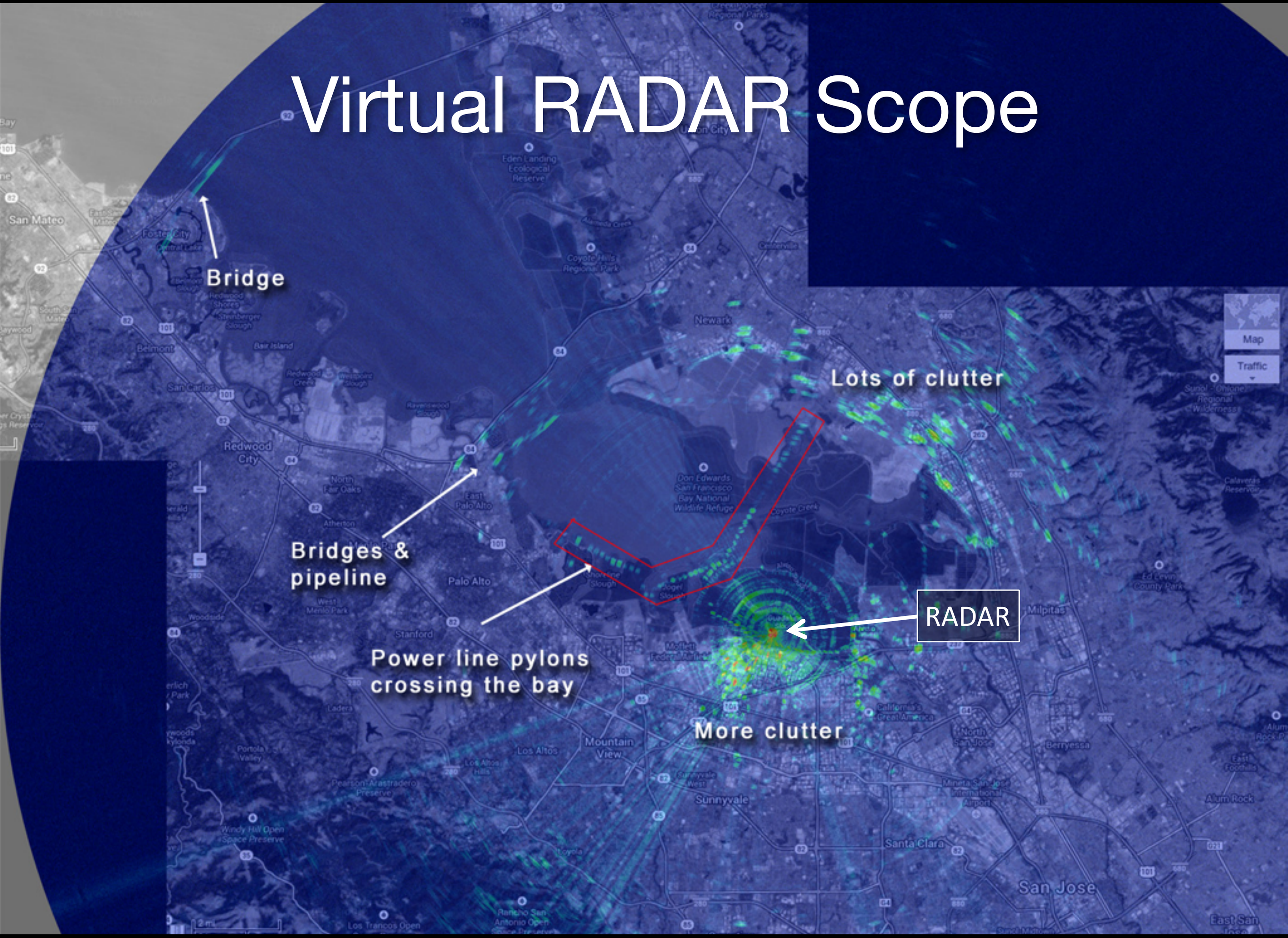
Raw RADAR Return Plot

Each scanline is synchronised to an emitted pulse



Scanline is amplitude of samples over time (also range of the return)

Virtual RADAR Scope



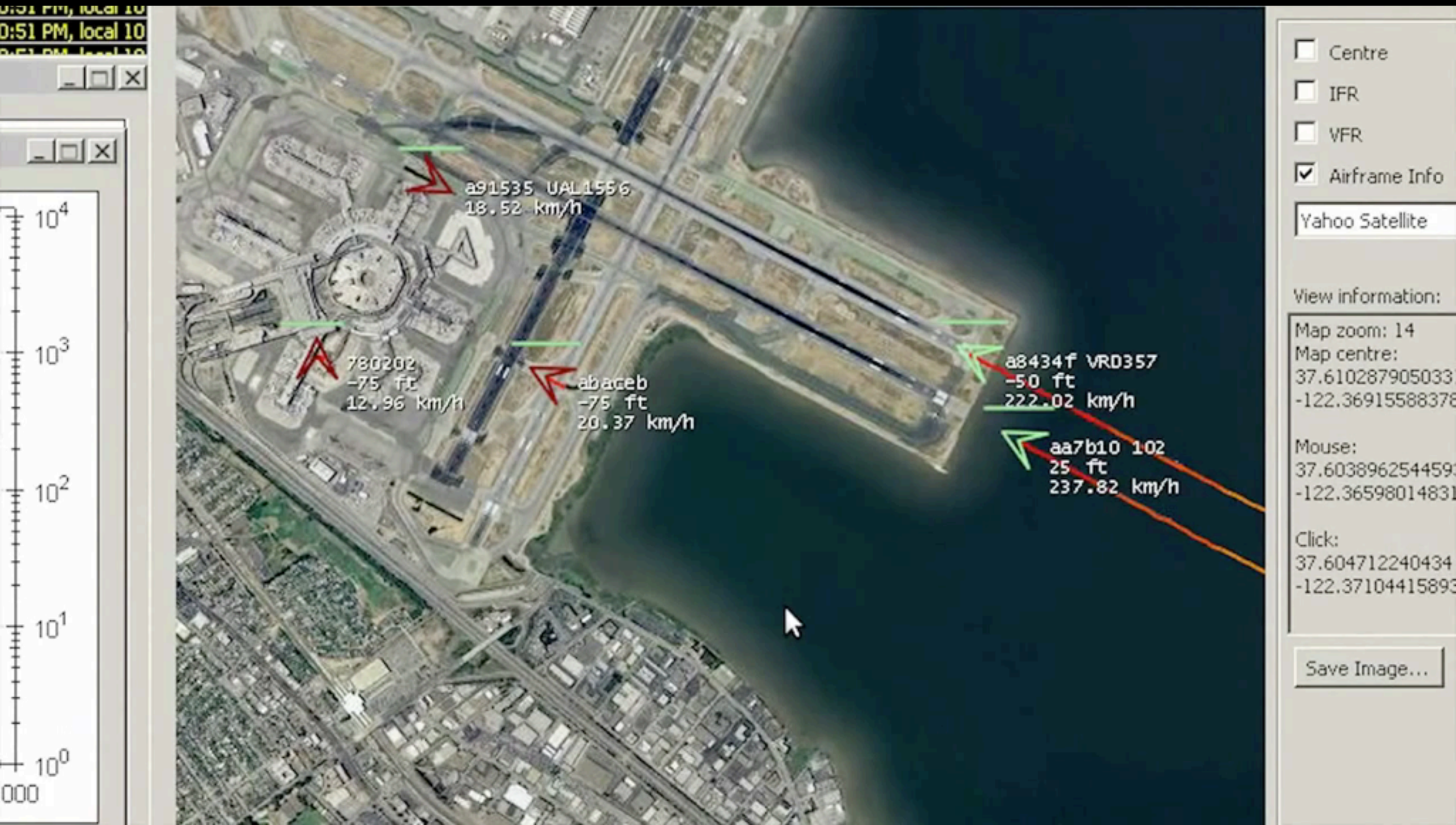

TCAS
Xpndr
High gain
SATCOM
Low-gain
VHF
HF
54A
54A
VHF
DME
ADF
EPIRB
Marker
RADAR Altimeter

A Typical 747 has…

31 radios

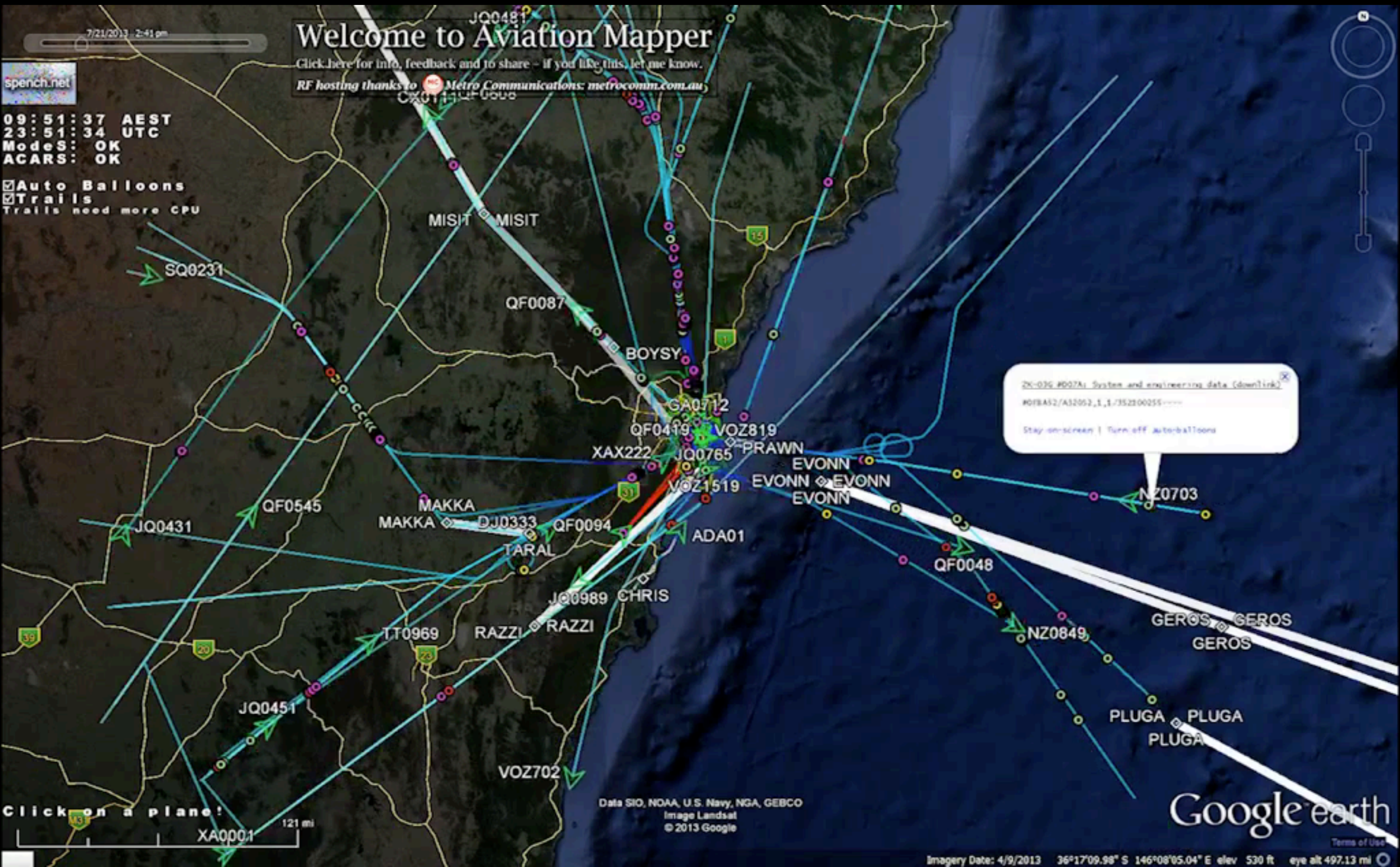
- 2 x 400 W voice HF
- 3 x 25 W voice/data VHF
- 2 x 100 W 9GHz RADARs
- 2 x GPS, 1.5GHz 60 W voice/data SATCOM
- 2 x 75MHz marker beacons
- 3 x VHF LOC localiser
- 3 x UHF glide slope
- 2 x LF ADF automatic direction finder
- 2 x VOR VHF omni-directional range
- 2 x 1GHz 600 W transponders
- 2 x 1GHz 700 W DME distance measuring equipment
- 3 x 500mW 4.3GHz radar altimeters
- 3 x 406MHz EPIRB

Landing at SFO



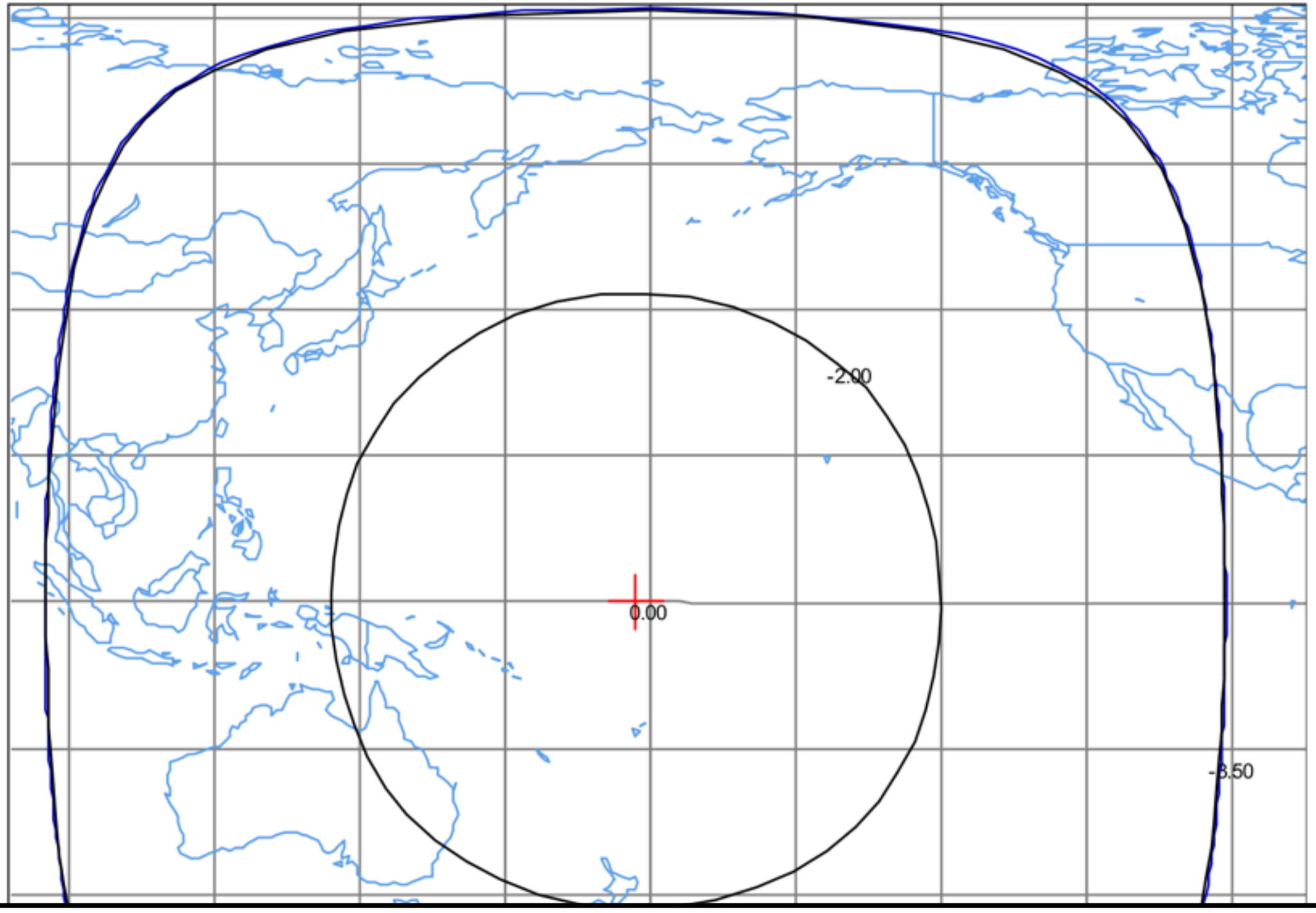
Takeoff at SFO (Cockpit View)

Combined Mode S & ACARS



‘Engineering’ Status Messages over ACARS

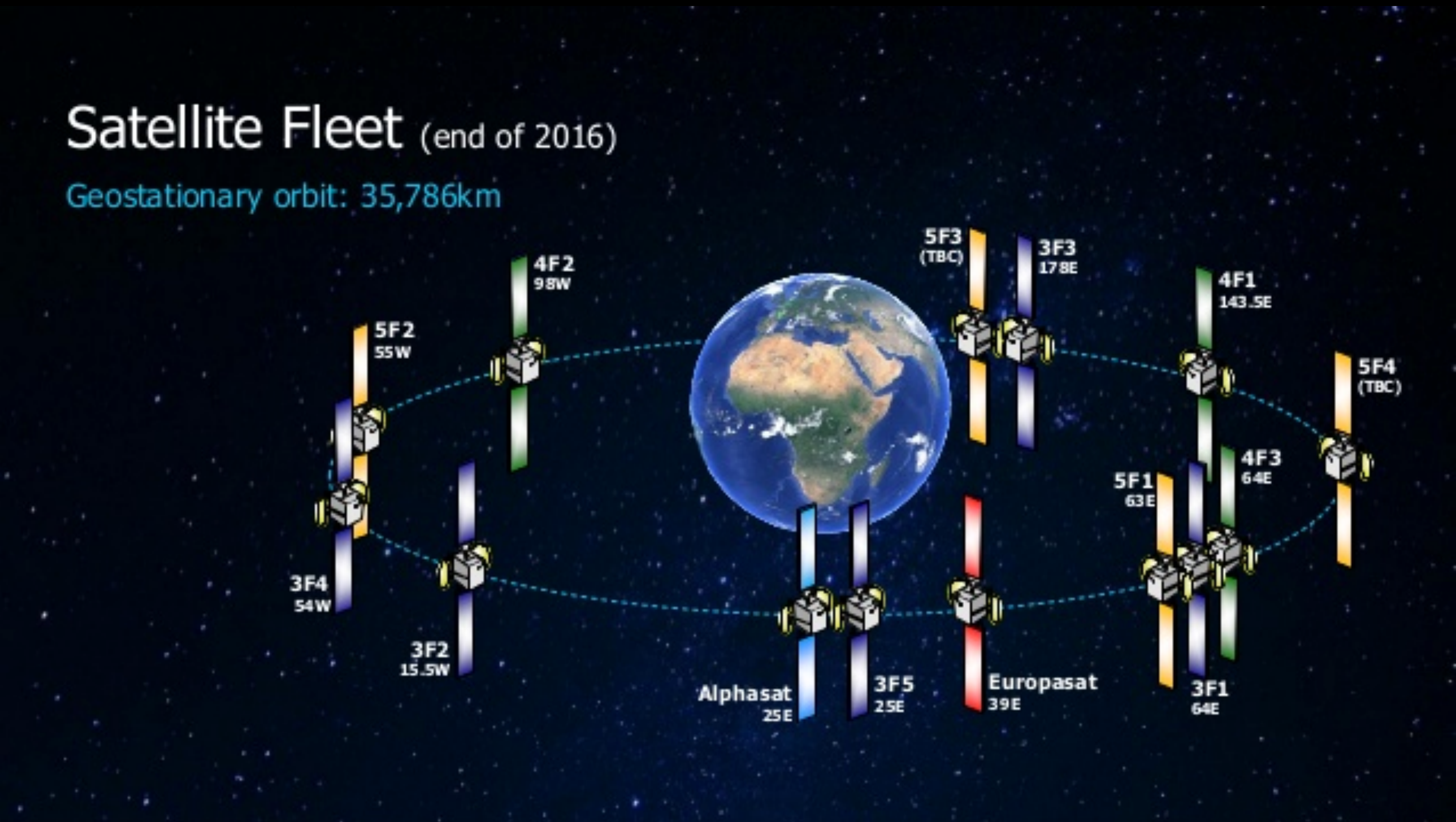
Waypoints Transmitted over ACARS

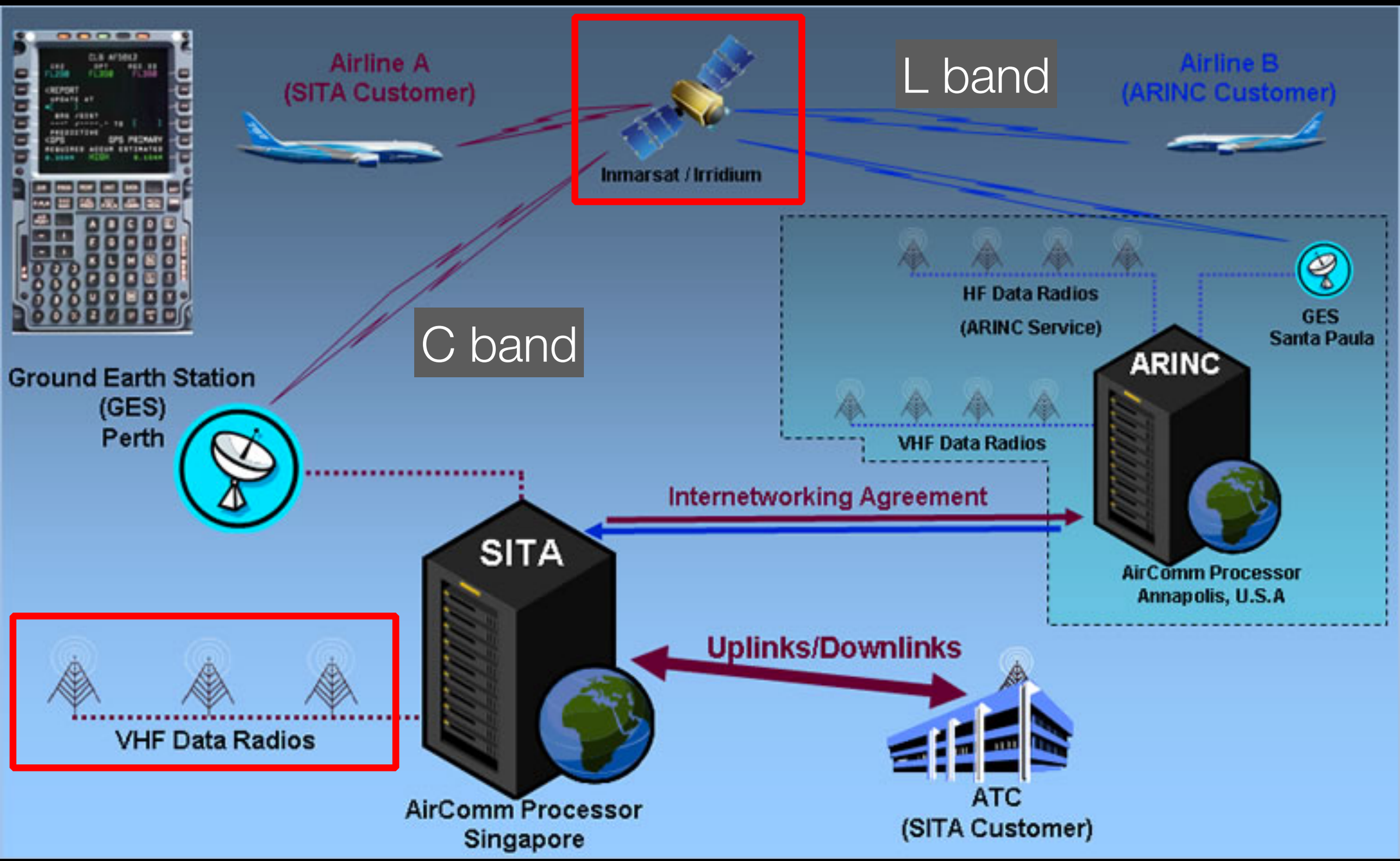


http://licensing.fcc.gov/cgi-bin/ws.exe/prod/ib/forms/attachment_menu.hts?id_app_num=68368&acct=263899&id_form_num=13&filing_key=-127644

INMARSAT-3

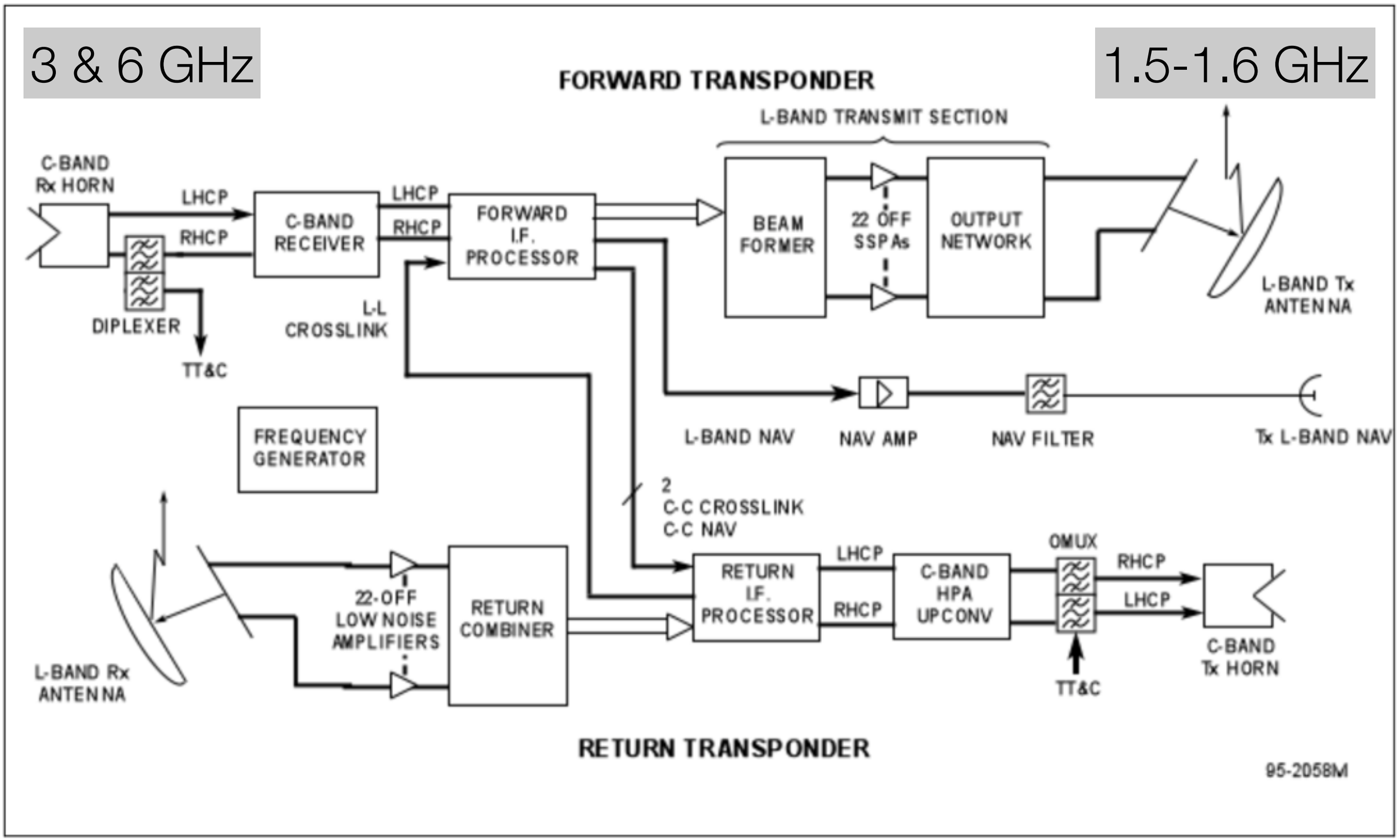
INMARSAT Geostationary Birds





http://members.optusnet.com.au/~cjr/introduction.htm

INMARSAT ‘Bent Pipe’ Transponders



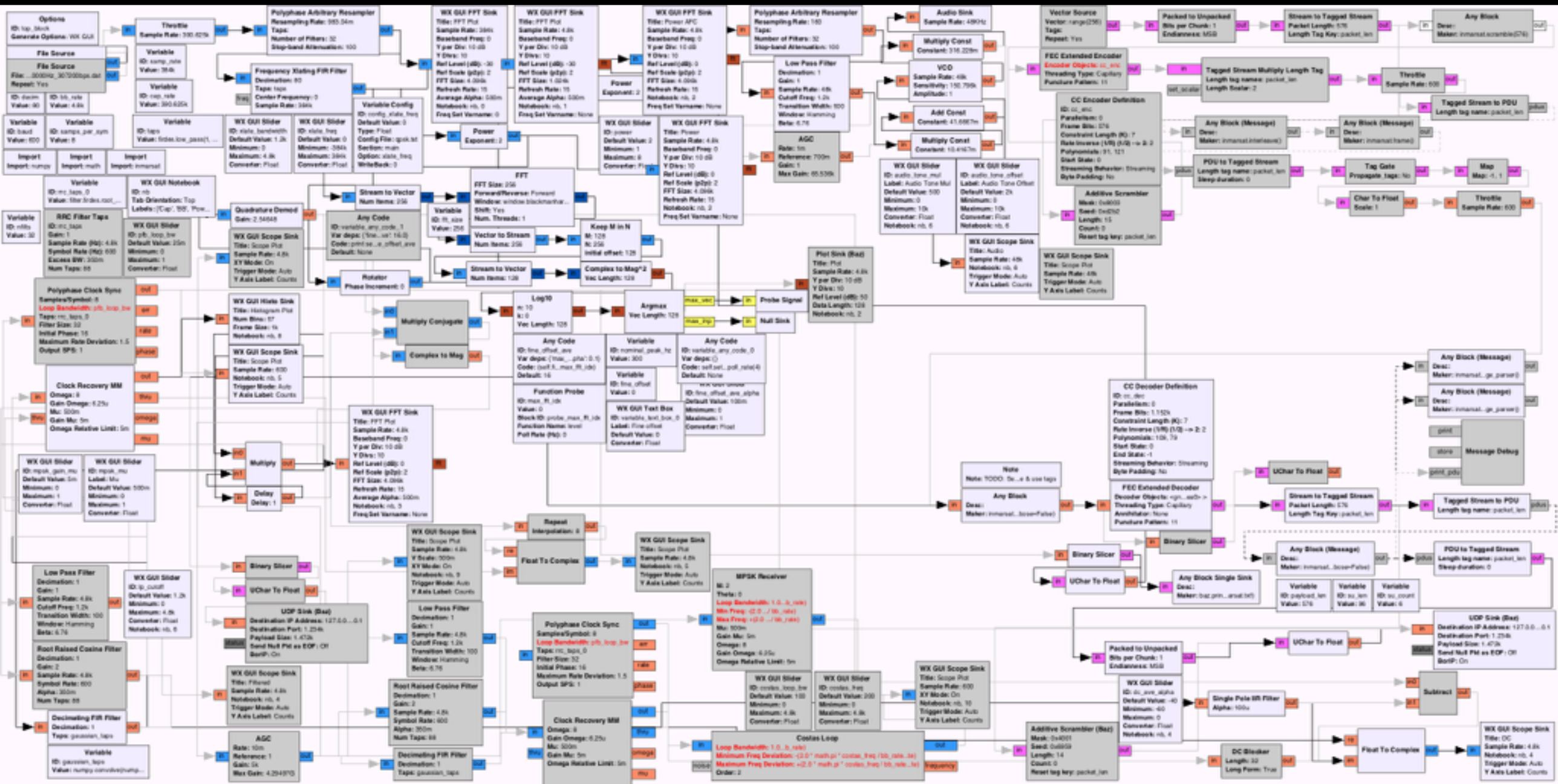

Bandpass Filter 1560MHz, 120MHz BW
LNA - Gain 14.8dB, NF 0.46dB
LHCP Helical Feed


LNA - 28dB gain?, 0.8dB NF ?

INMARSAT Aero

- **P Channel** - *coordination and timing begins here!*
  - Packet mode Time Division Multiplex (TDM)
  - Sent *to* aircraft, carries signalling & user data
- R Channel: random access signalling & user data, *from* aircraft
- T Channel: Reservation TDMA, *from* aircraft, for data transmission
- C Channel: Circuit-mode, *to & from* aircraft, carries voice and user data

The P Channel Flowgraph so far…

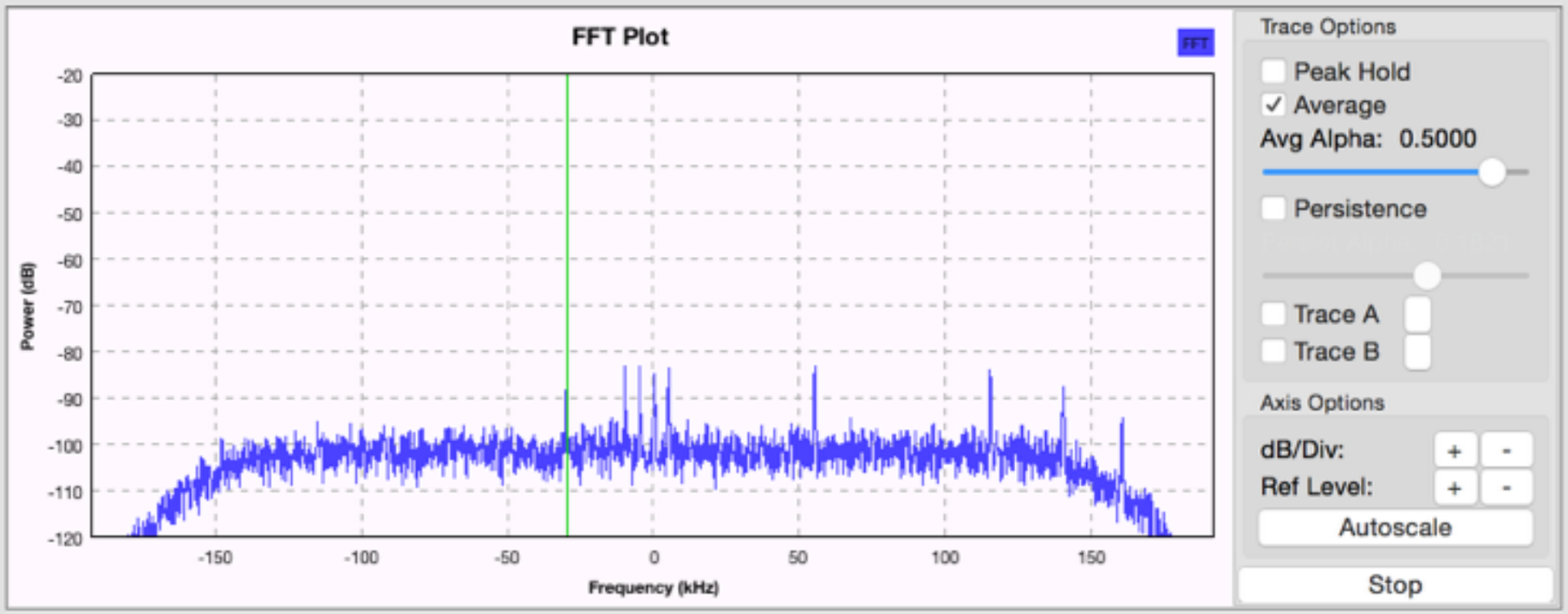


Top Block

xlate_freq: -29.6k

power: 2

Cap | BB | Power | Baud | Quad | Clock | Audio | FEC | Histo



Trace Options

Peak Hold

Average

Avg Alpha: 0.5000

Persistence

Trace A

Trace B

Axis Options

dB/Div: + -

Ref Level: + -

Autoscale

Stop

Mu: 500m

mpsk_gain_mu: 5m

lp_cutoff: 1.2k

Audio Tone Offset: 2k

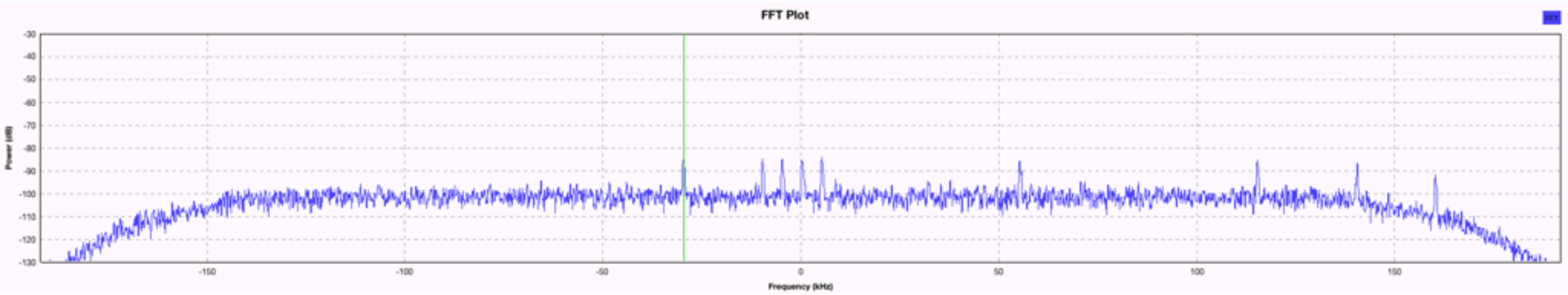
Audio Tone Mul: 500

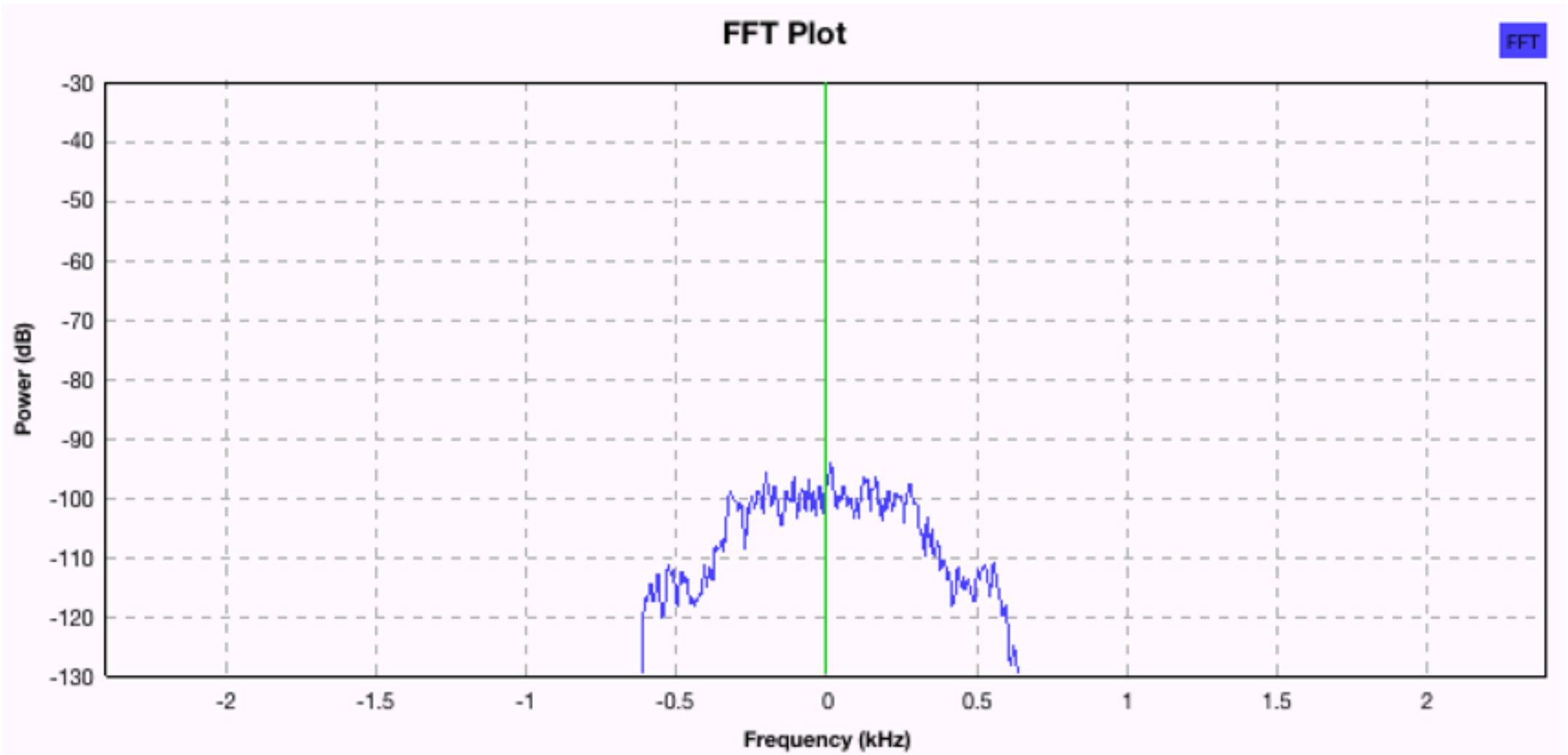
amp: -10

xlate_bandwidth: 1.2k

pfb_loop_bw: 25m

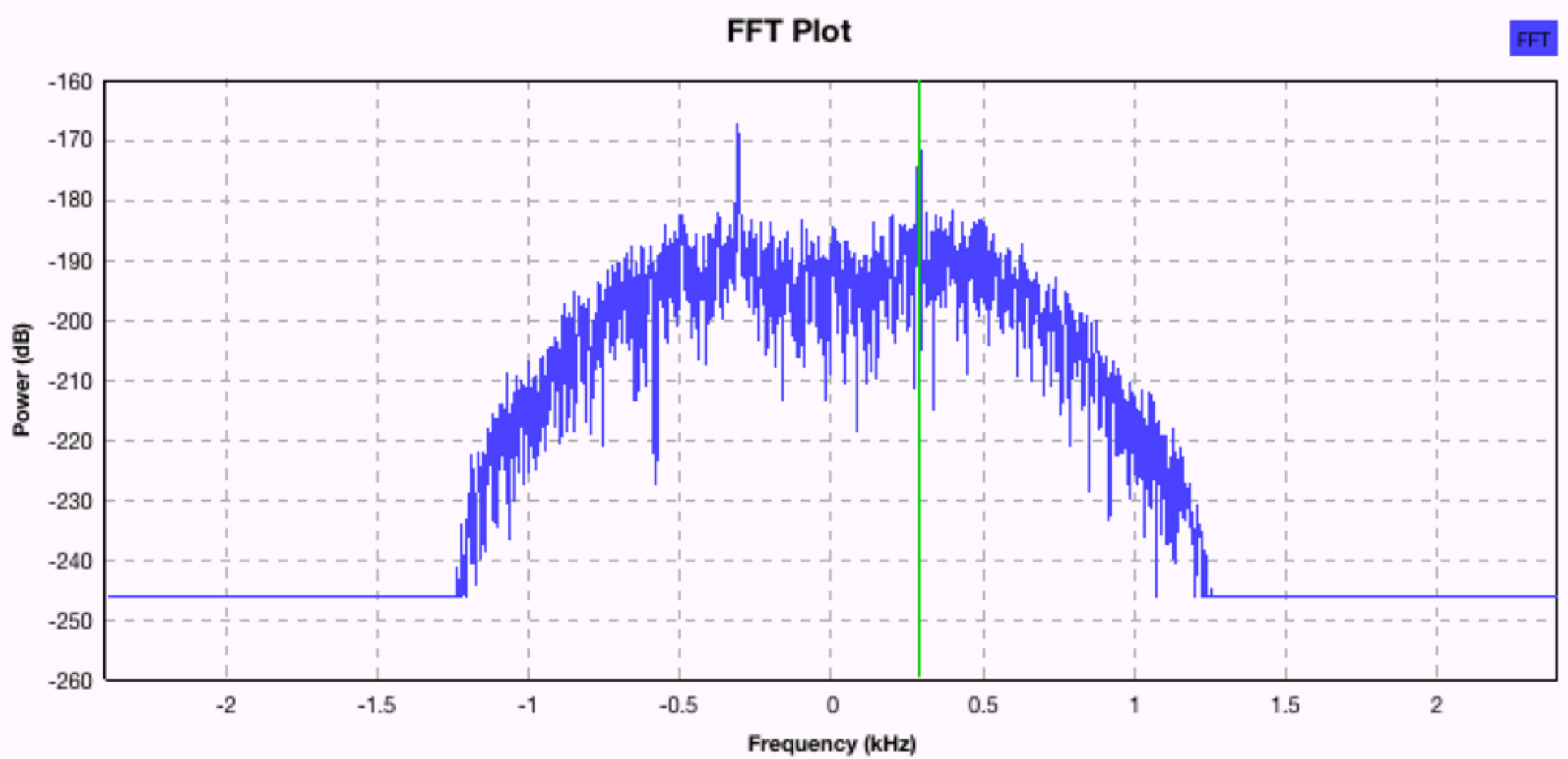
Channel Selection





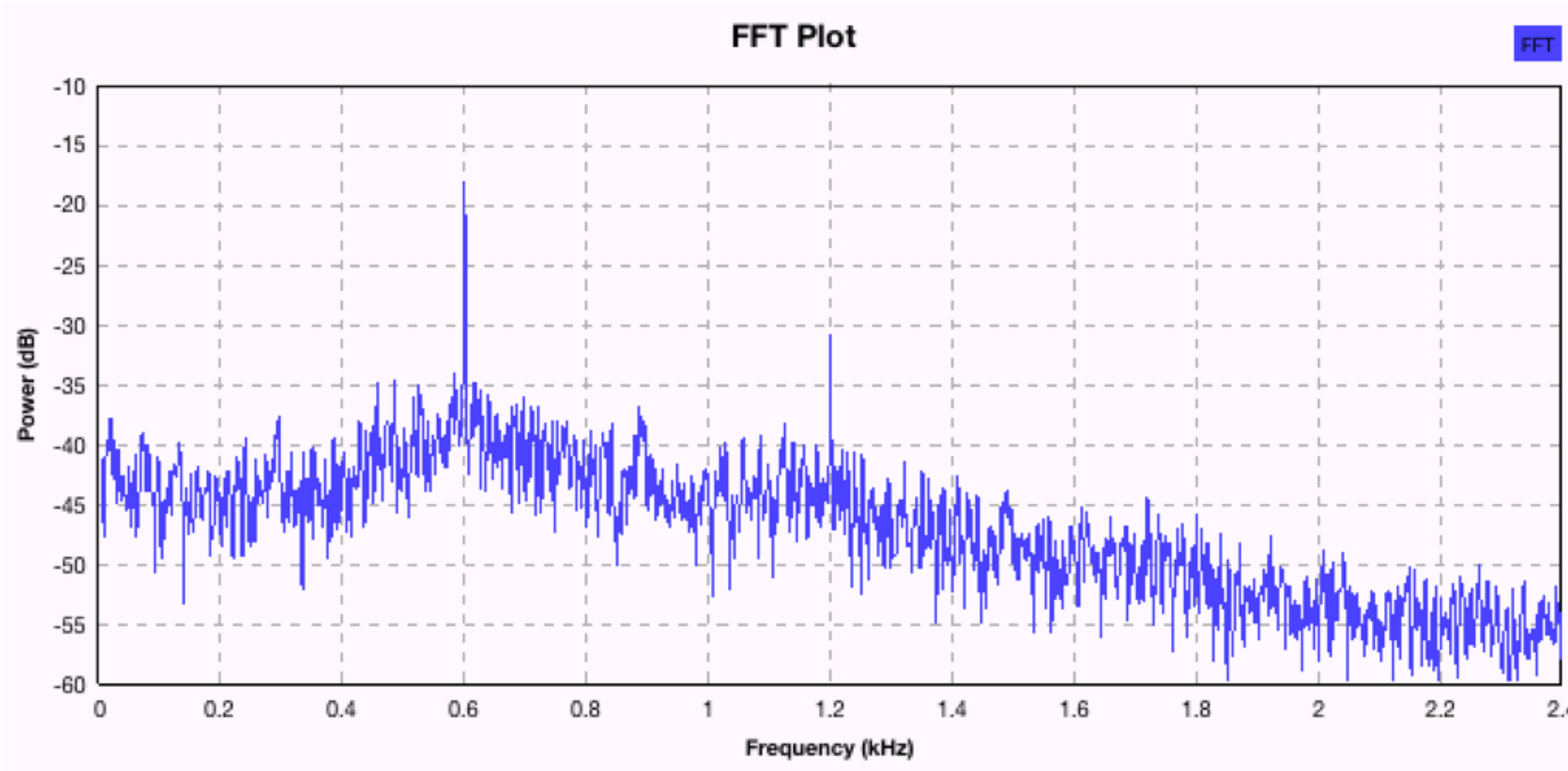
Modulation Type

- **G**aussian **M**inimum **S**hift **K**eying (GMSK): FFT of squared complex samples results in two peaks equidistant from 0



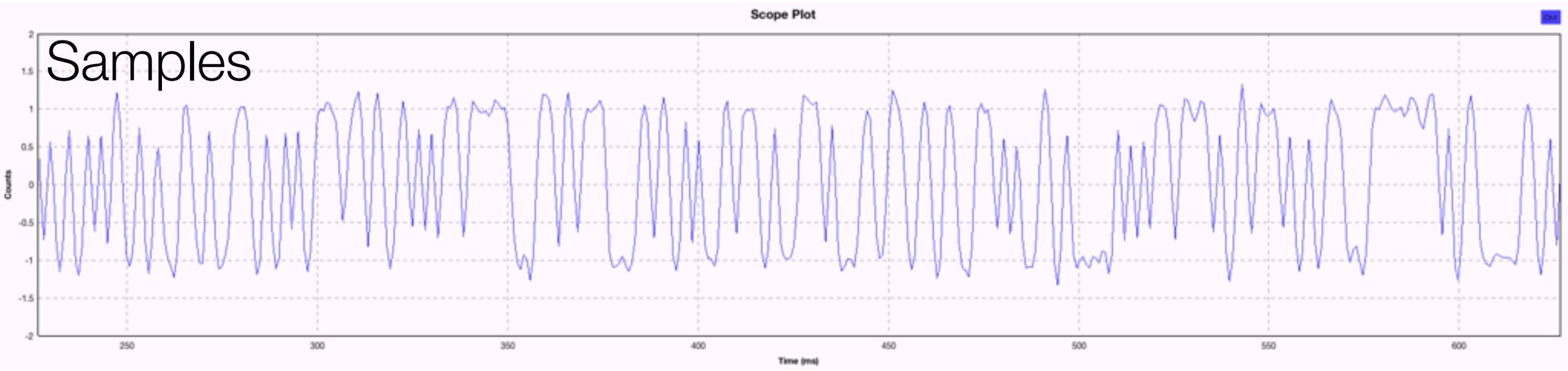
Symbol (Baud) Rate

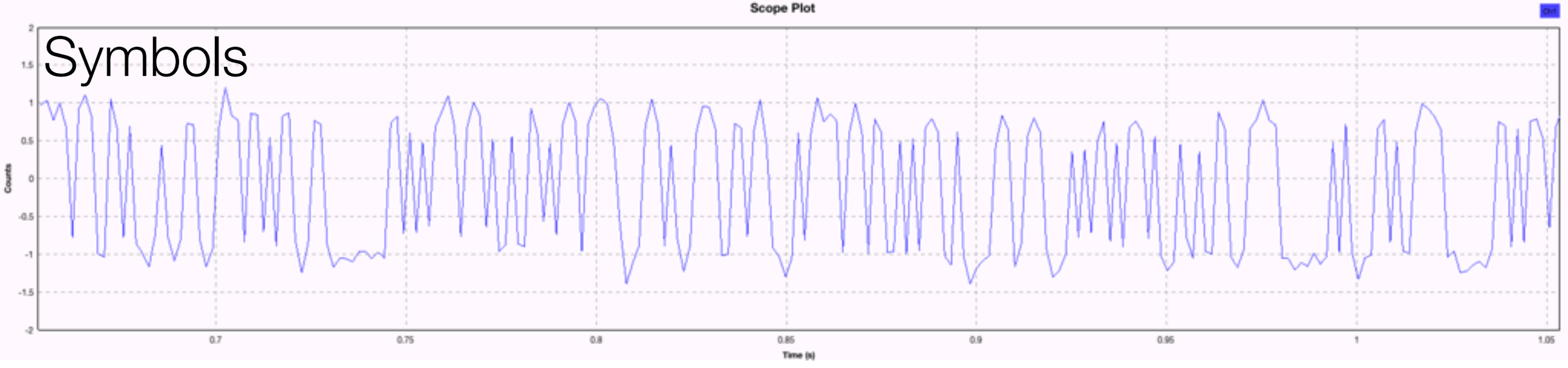
- Cyclostationary Analysis: rate is first peak in plot (600 bps, also distance between cyclo peaks)



Clock Recovery

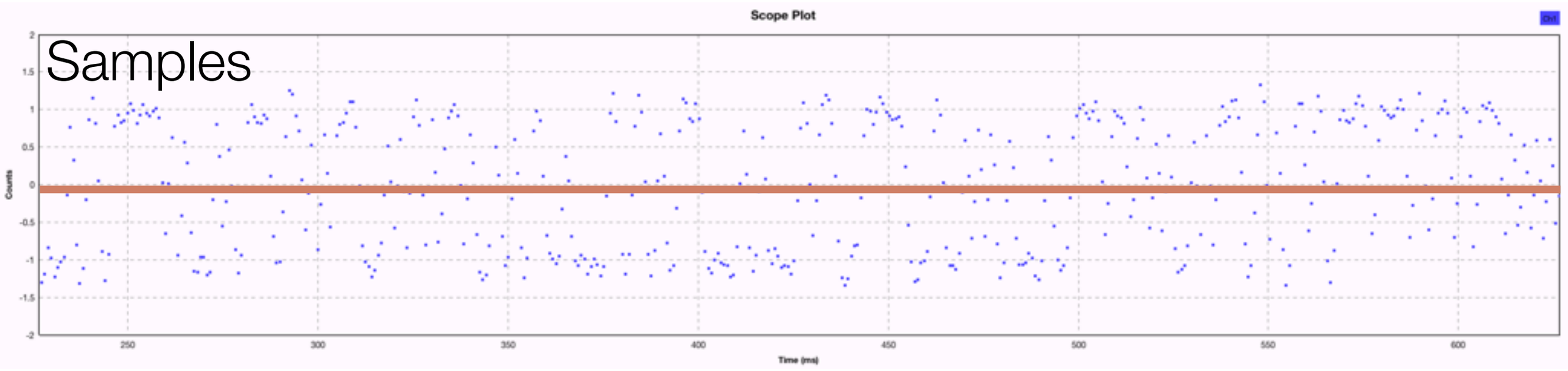
- Enough information to begin tracking symbols in channel (and output them to enable operation on bits)

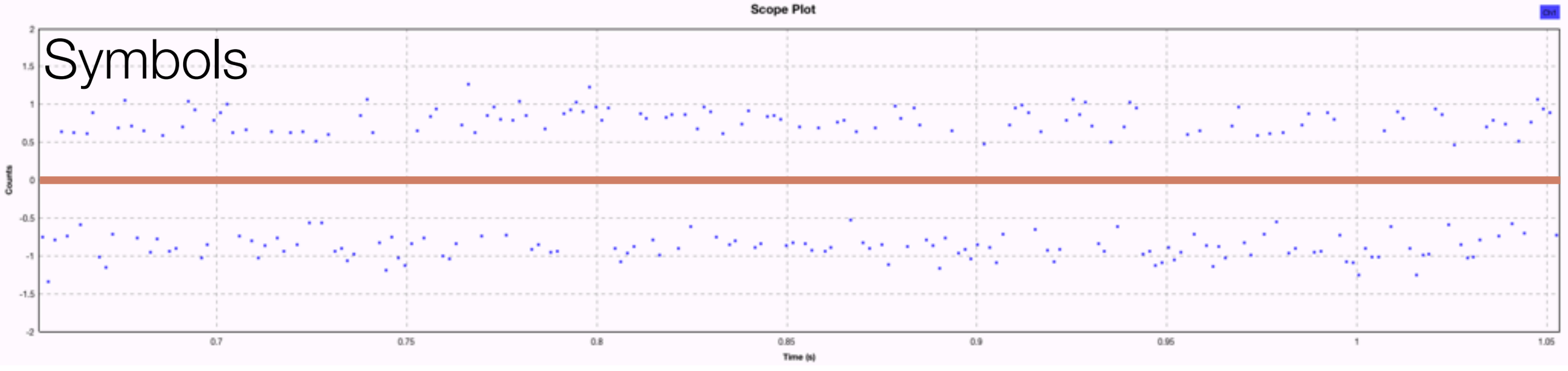




Clock Recovery Quality

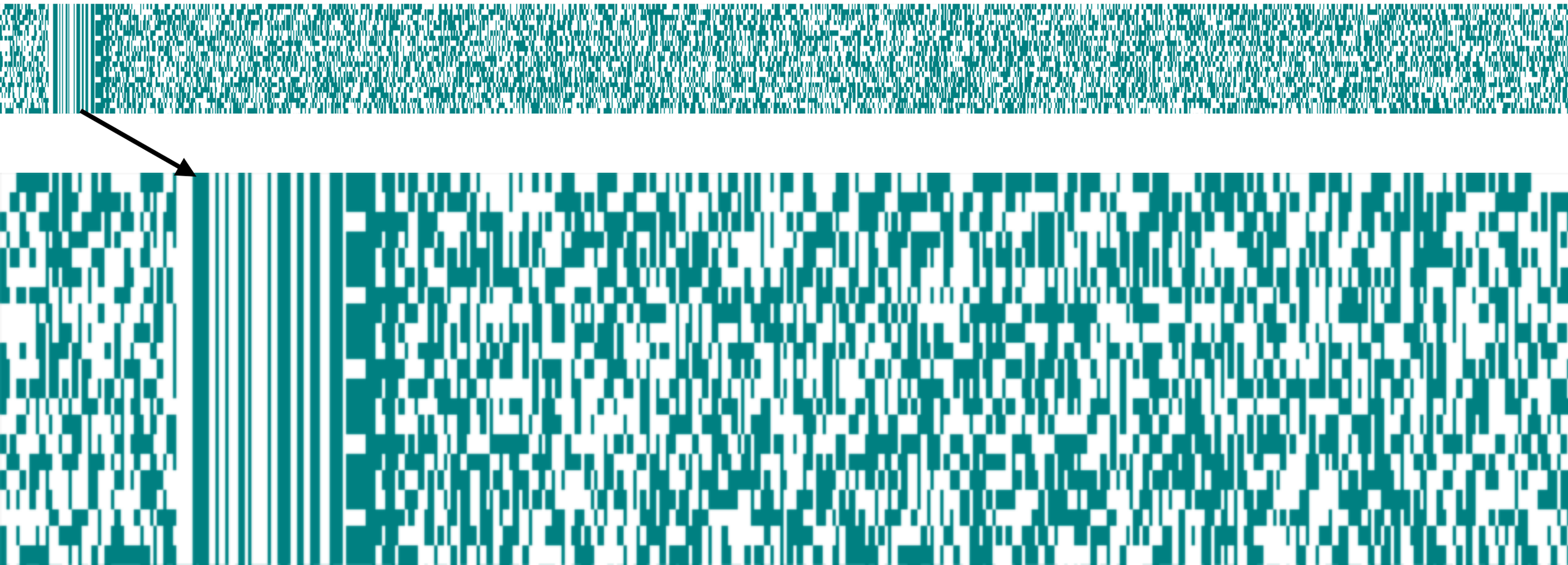
- Increased separation between symbols about 0





Frame Structure

- Search for repeating patterns in raster plot
  - 1200 bits wide (line up pattern vertically): unique word (sync), frame header, payload



Payload Encoding

- Appears ‘random’
- Generally data has gone through:
    1. Interleaving (protects against burst errors)
    2. **F**orward **E**rror **C**orrection (data redundancy)
    3. Scrambling (energy dispersal & clock recovery)
- Complex process - difficult to test each step individually

Payload Details

- RTFM

- Frame payload consists of multiple fixed-length Signal Units (number of SUs depends on data rate of channel, here 6 of 96 bits each)

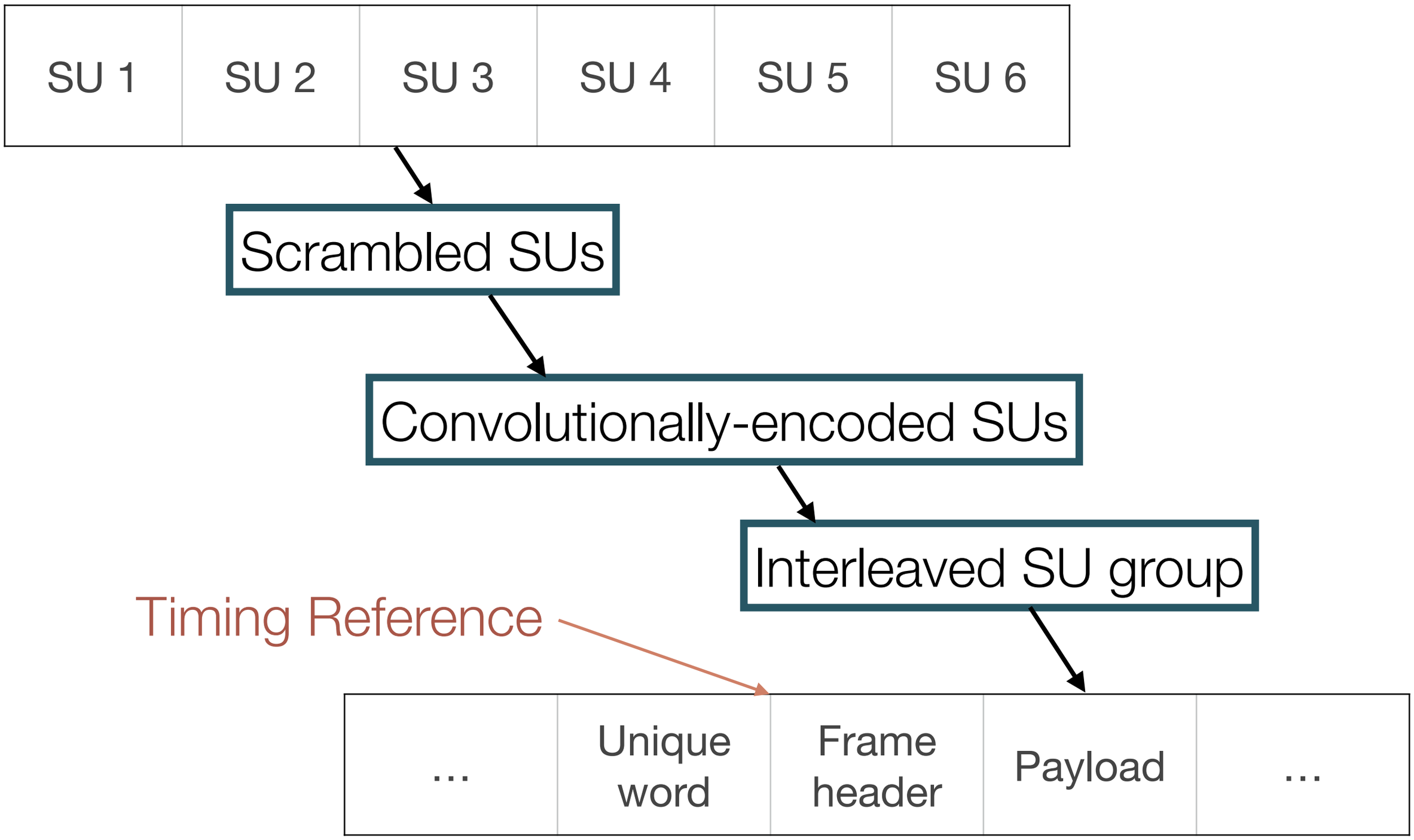
- For transmission, the entire SU group is:

    1. scrambled

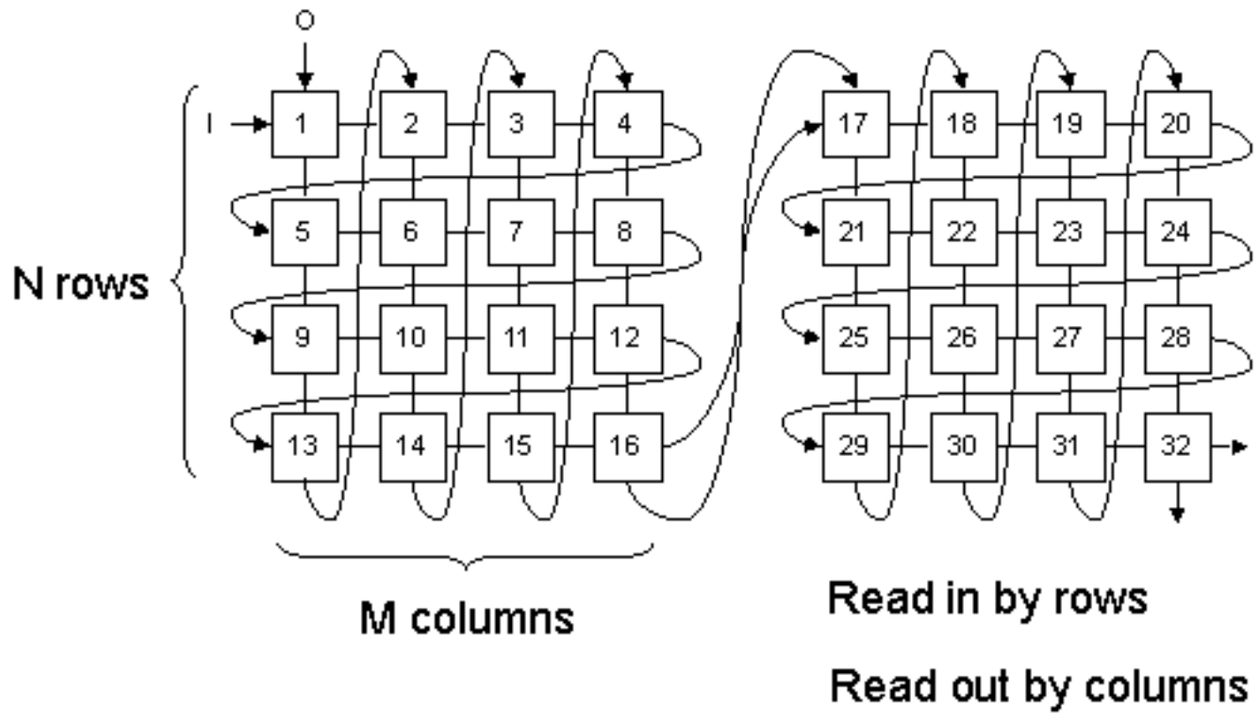
    2. 1/2-rate convolutionally encoded

    3. fed through an interleaver

Frame Details



#1: De-interleaving

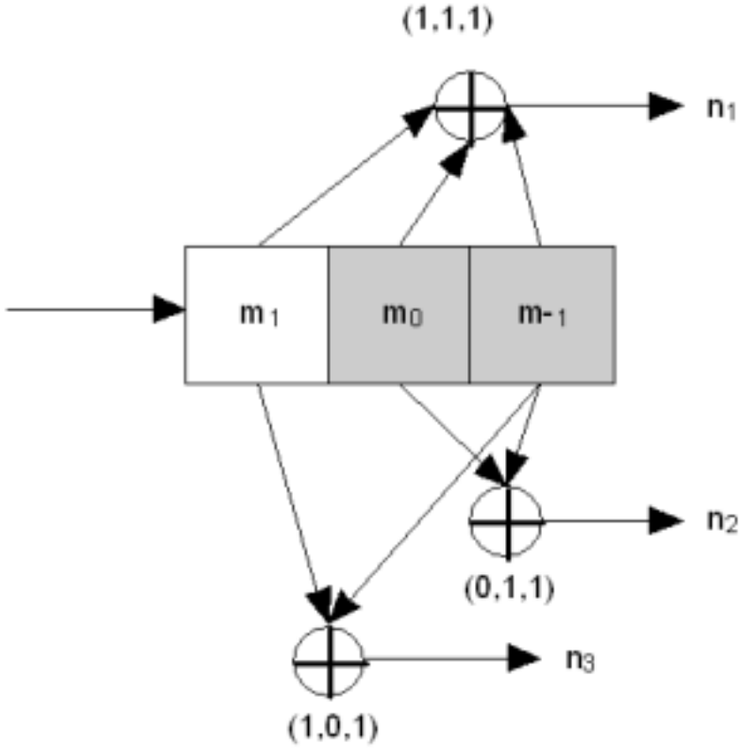


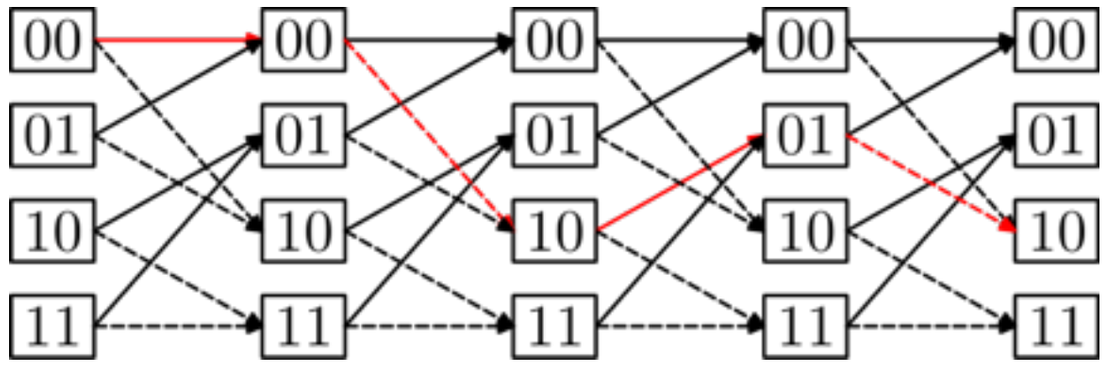
https://www.cl.cam.ac.uk/~jac22/otalks/rtpi/sld004.htm

#2: Convolutional (Viterbi) Decoding

- A convolutional code adds additional bits to a stream so that a receiver can correct errors

- Given received error-prone symbols, a Viterbi decoder will output the bits that represent the most likely path through a trellis matching the convolutional code

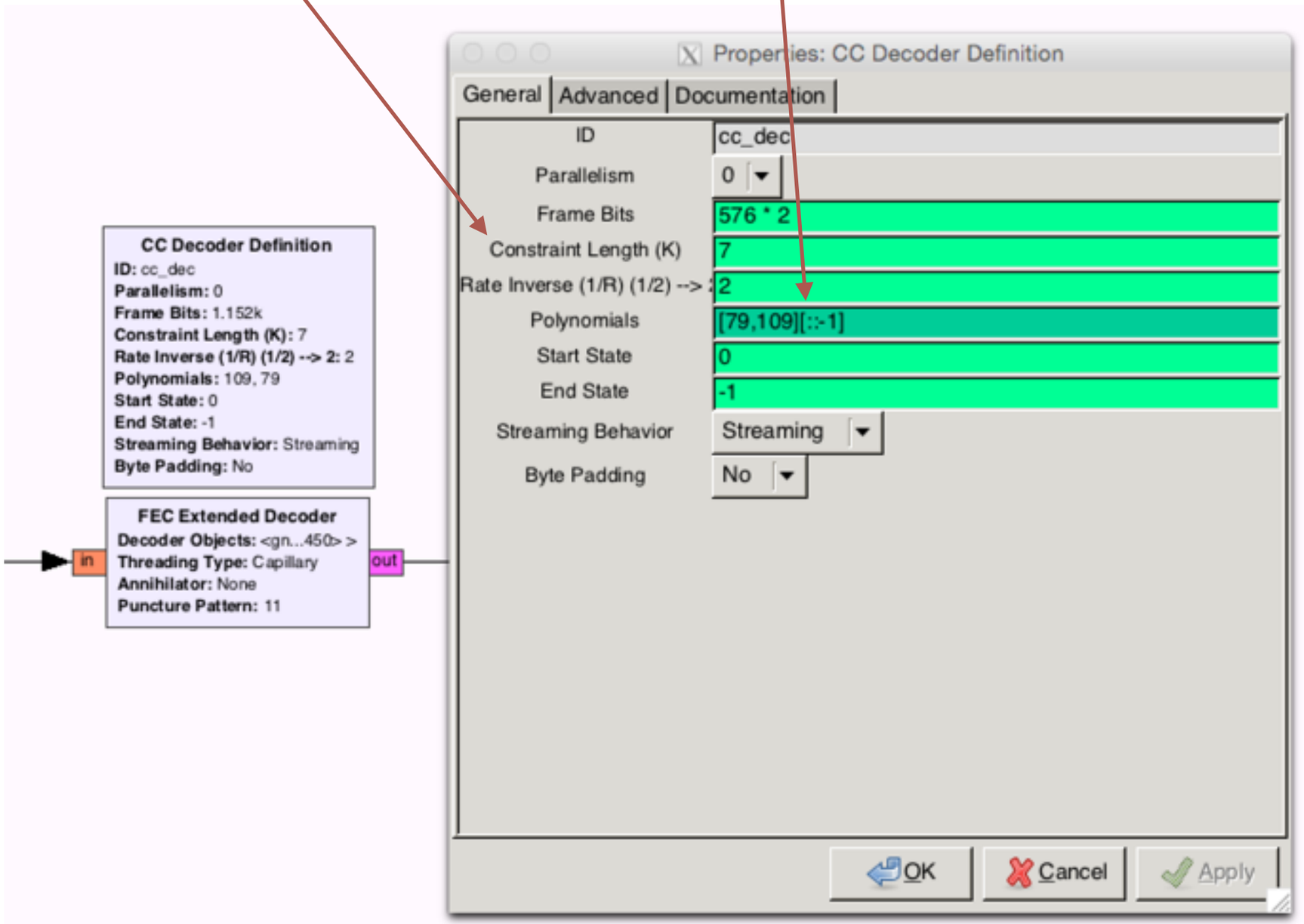




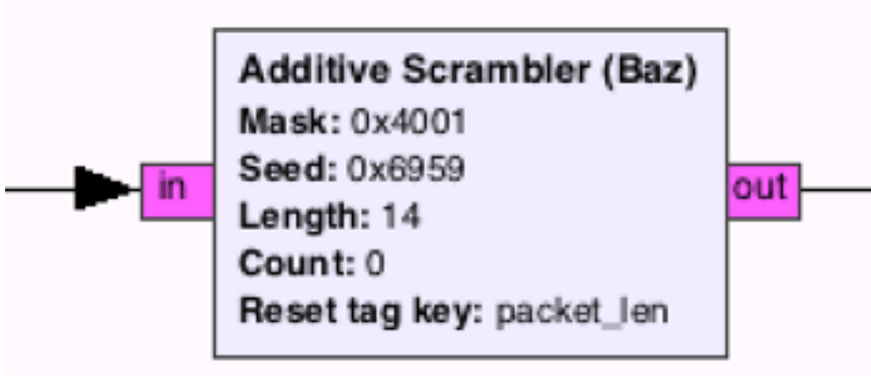
https://en.wikipedia.org/wiki/Convolutional_code

#2: Viterbi Decoder

- The NASA Voyager K=7 convolutional code is popular, and used here (gr-fec)

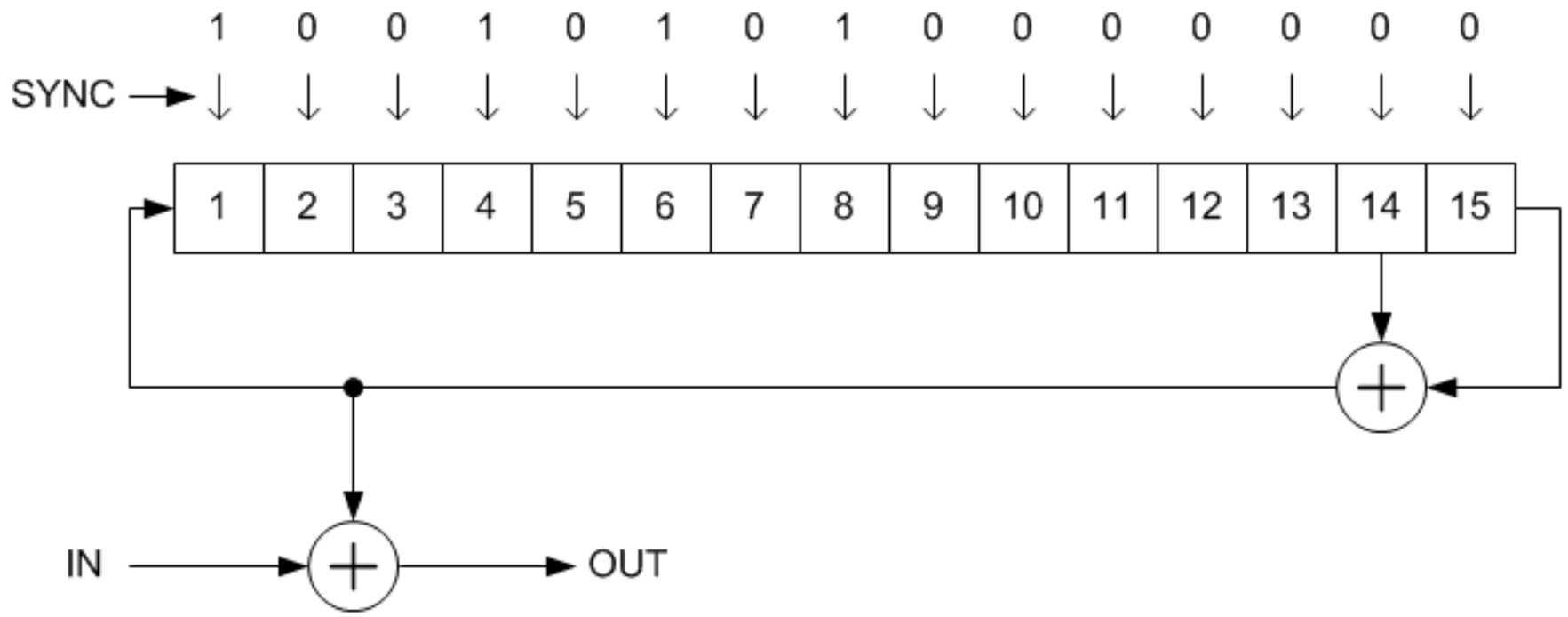


#3: De-scrambling



- Implemented as a Linear Feedback Shift Register
- Reset (sync'd) at the beginning of a new frame

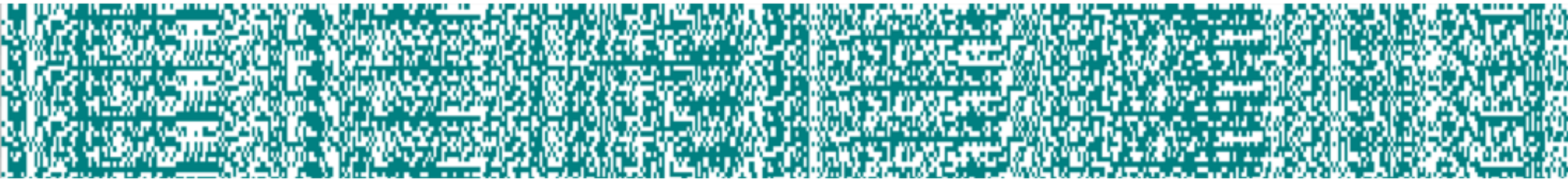
Example:



https://en.wikipedia.org/wiki/Scrambler

Validation

- Inspect raster plot of output to check if there is more structure:



- Compute CRC checksum to confirm correct decode: CRC-16-CCITT should yield **`f0b8`**

Decoding

71780a5b82751e60*ffff*1c75 f0b8 **ISU (User Data)**

62ae146182748e0000000eee f0b8 ACK

d676*d3542070616 7e520*01a8 f0b8 **User Data begins**

d576*2fae0d8a2fd33231*cbfb f0b8

d476*2f4ab0b031b52fc2*5cab f0b8

d376*b0322f46b0342f4f*8c67 f0b8

d276*31b5b0b00d8a2f43*7024 f0b8

d176*c1c4c44954494fce*4775 f0b8

d076*c14c2049ce464f526*db5 f0b8

11a9322582df000a84526d98 f0b8 Log on

40a9322582d831663856f222 f0b8 Channel control

c0d83781384a000000005331 f0b8

41a9322582d941063787551e f0b8 Channel control

c0d936c336b836c51101af14 f0b8

6271c274827d8e000000d259 f0b8 ACK

Decoding

cf76cdc154494fce2fae332f f0b8
ce760d8a2fc4b0324c2f7f34 f0b8
cd76ae2f542fae0d8a2f3719 f0b8
cc76c8b032b3b32fae2f10bd f0b8
cb764f31b6b0b02faec1be14 f0b8
ca76f2f2e97661ec20678197 f0b8
c97661f4e5206e756d624cd8 f0b8
c876e5f2ba0d8a2f4f31f556 f0b8
c776b6b0b02f5831b92f7d65 f0b8
c676450d8a2fd332b62f0091 f0b8
c5764f31b6b0b02fae0d2599 f0b8
c4768ac26167676167e576ea f0b8
c37620e3ec61e96d20e68b9d f0b8
c276eff220c8cbc720610933 f0b8
c176f2f2e97661ecba0db0a2 f0b8
c0768a2f9762917f0000f199 f0b8 **User Data ends**

User Data: ACARS Message

`2..B-KQKH1F- #T1O1600/X26/E

/S22/B02/O1600

/.Please arrive at the boarding gate at least/.

/O1500/X02/E/O1500

/S23/B02/X05/F04/O1500

minutes

/O1600/X12/ **before departure./.**

Late passengers may not be accepted for/.

travel.

Other Types of Messages: Notices

`2.N610FEA9YG,

AND H CLSD. TWY K CLSD,

BTWN RWY 33, AND TWY J.

TWY J CLSD, BTWN RWY

28R, AND TWY C. RWY 28L

ARRIVALS, EXPECT BACK

TAXI RWY 28R. CTN, PSNL

AND EQPT WORKING, EDGE

OF CLSD RWY 28R.

CAUTION, BIRDS NEAR

AIRPORT.

Other Types of Messages: Weather

```
METAR PACD 192153Z 36012KT 10SM SCT012
OVC060 08/08 A2931 RMK AO2

      RAE29 SLP924 P0001 T00830083
```

Other Types of Messages: AFN / CPDLC / ADS-C

```
@2.JA838JA0Y/ANCATYA.AFN/FMHJAL3,.JA838J,
86DA1E,212225/FAK0,PAZN/FARADS,0/FARATC,
004F0

P2.N620FEH1X- #MD/A6
OAKODYA.ADS.N620FE07030B000C010D010E0110010F
01799A

02.B-6535A6W/
UPGCAYA.ADS.B-6535080F13264825E41

2B-16705RAZQUTPEOCBR~1RA101192156
SA 19/21:54
```

Other Types of Messages: Scheduling

```
`2B-16708H1V- #T1:)DM01171719

/M99

/Q01

BR395/,/3SGN/,07:20/,T2/,C4/,On Time/./.

BR211/,/3BKK/,08:15/,T2/,C7/,On Time/./.

BR255/,/3DPS/,10:15/,T2/,C8/,On Time/./.

BR271/,/3MNL/,09:30/,T2/,C3/,On Time/./.

BR265/,/3PNH/,09:10/,
```

Other Types of Messages: ???

2.N610FEA9Z ...**ADVS YOU**

HAVE INFO G.5403

2.70042BC1B.ATSMCXA 192157

AGM

AN 70042B

- **NO PARTICIPATING TWIP**

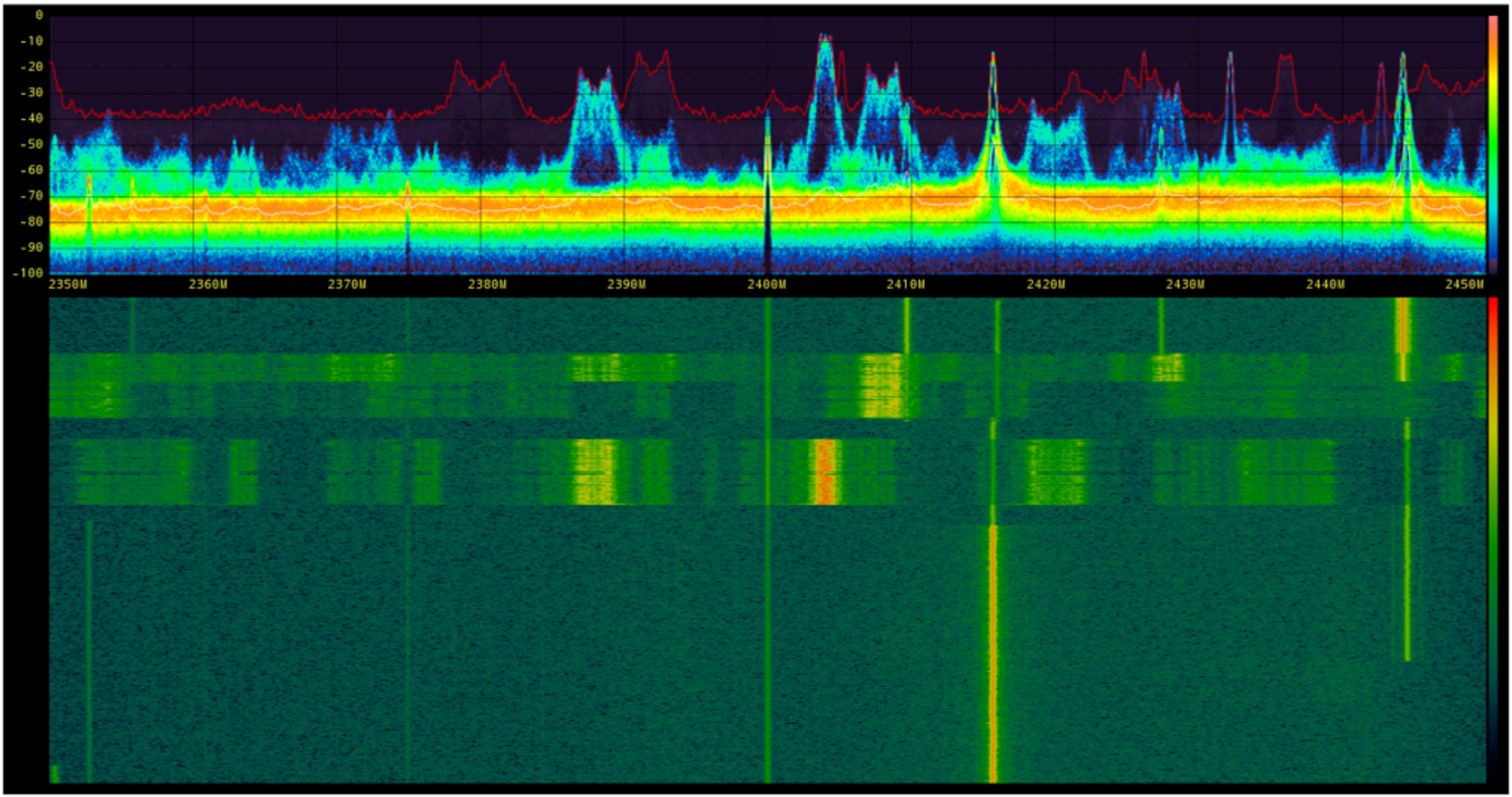
AIRPORT IN REQUEST

Drones & FPV

Hacking the Wireless World with #sdr

@spenchdotnet

2.4 GHz ISM Band Activity: Drone R/C



Frequency Management: Don't Wreck Your Neighbor's Drone

By Tyler Winegarner March 3rd, 2015 3:12 pm Category Electronics, Robotics

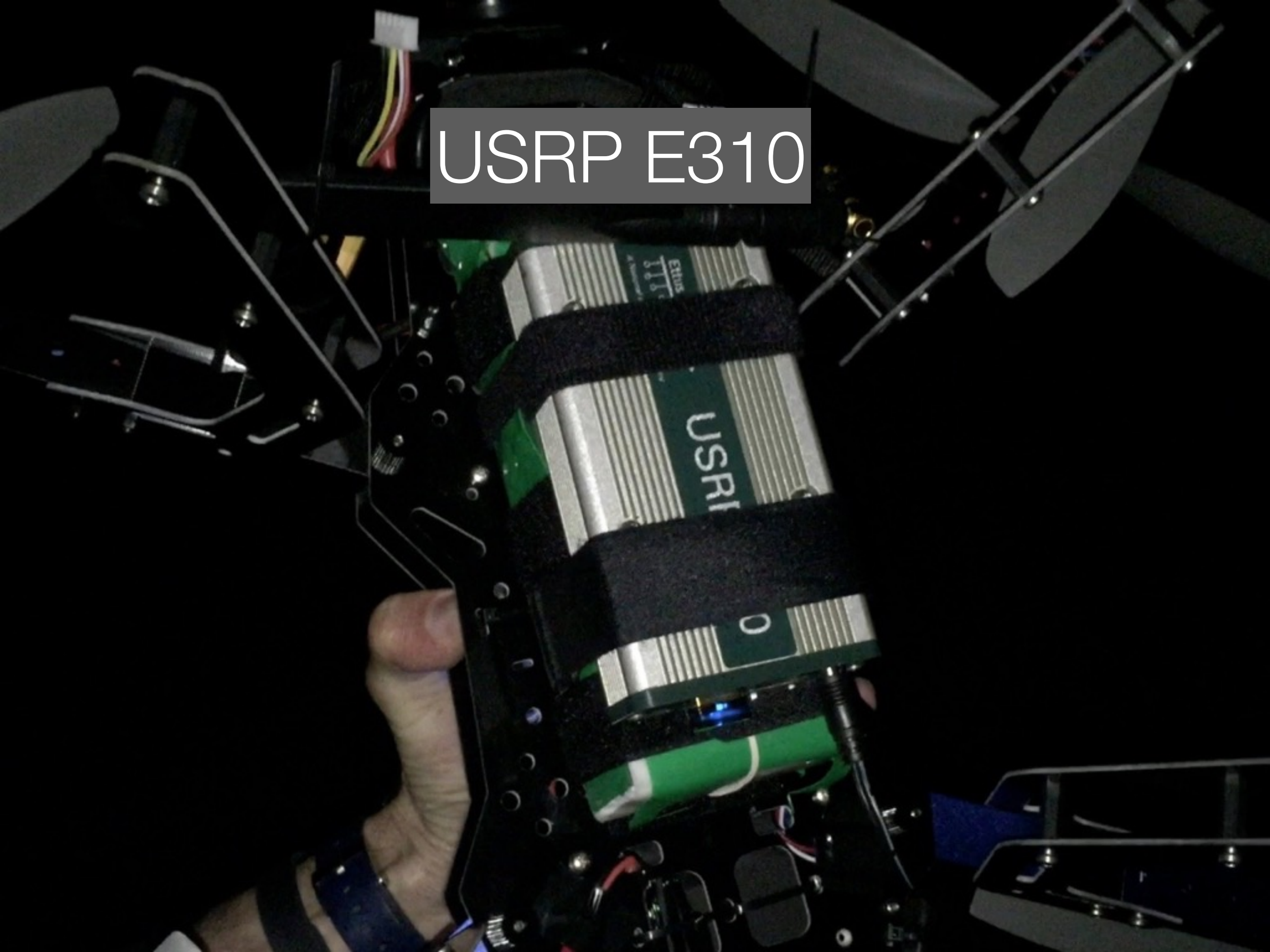
http://makezine.com/2015/03/03/frequency-management-dont-wreck-your-neighbors-drone/

What are we looking at?

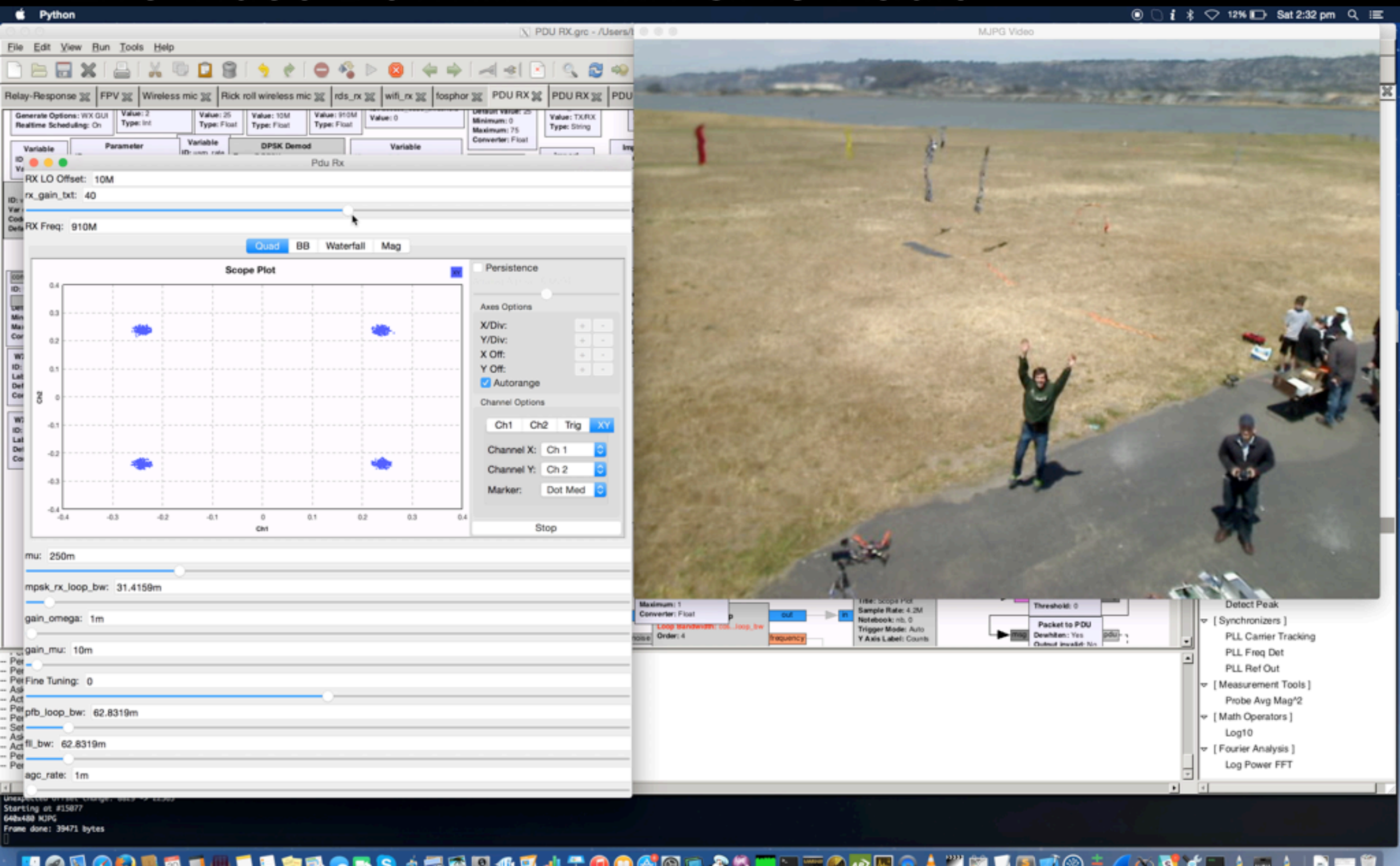
3D Robotics X8+


Webcam

USRP E310

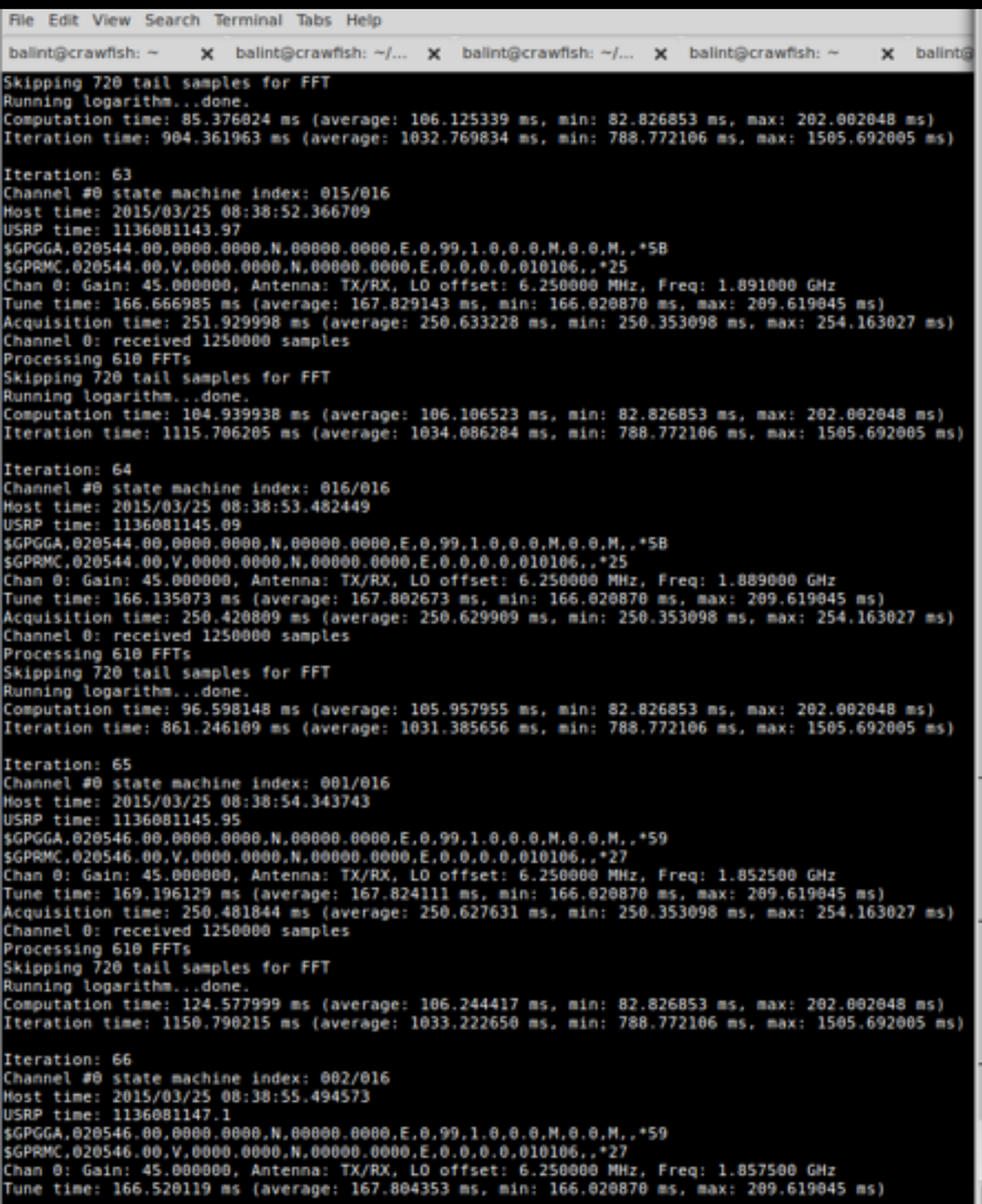


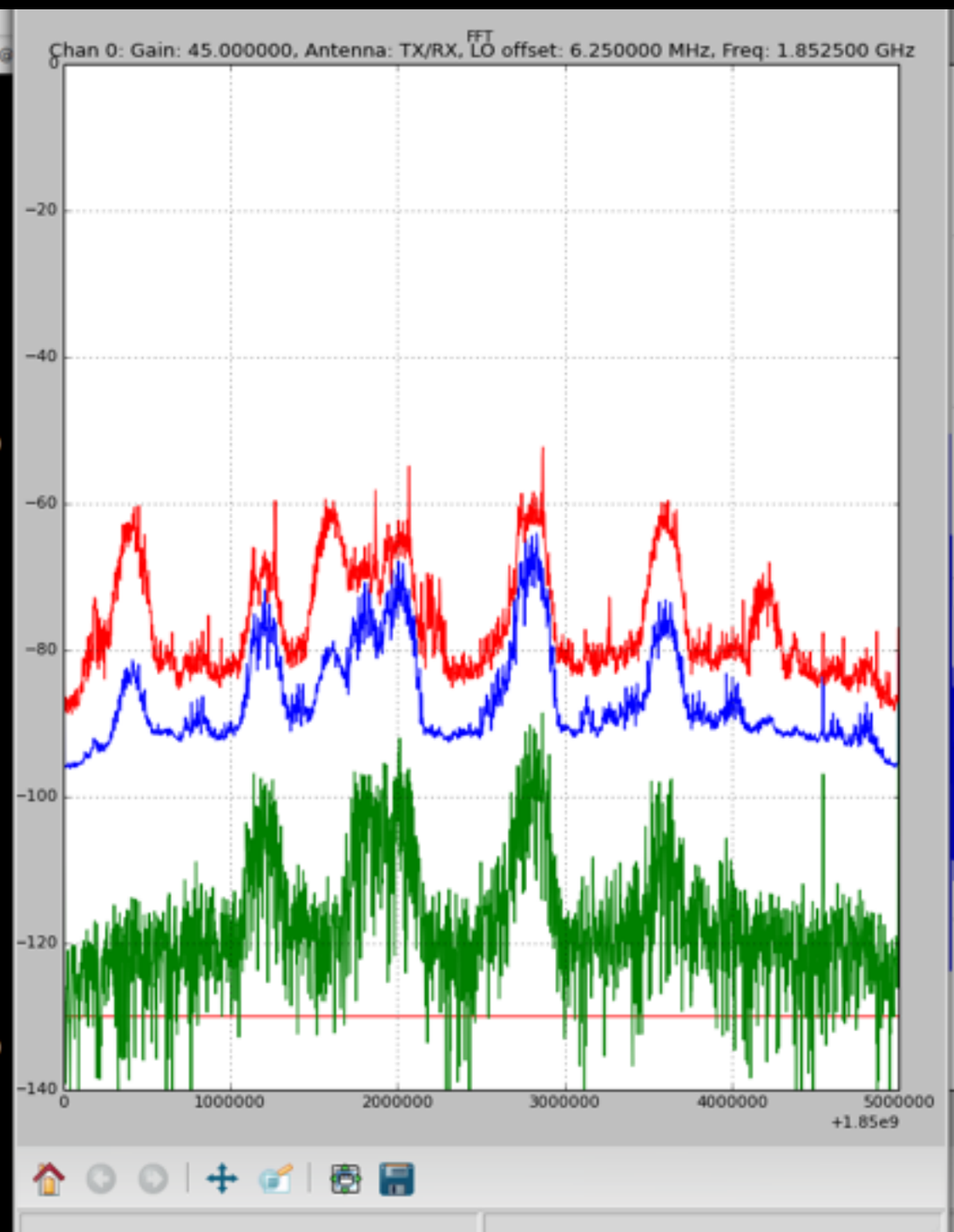
Live Video Downlink with GNU Radio

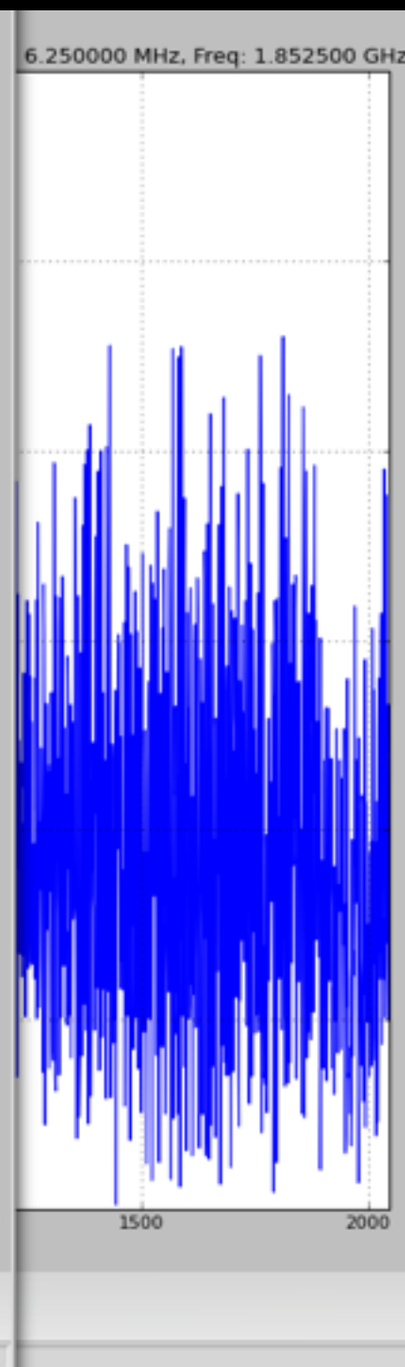


Live Video Downlink with GNU Radio

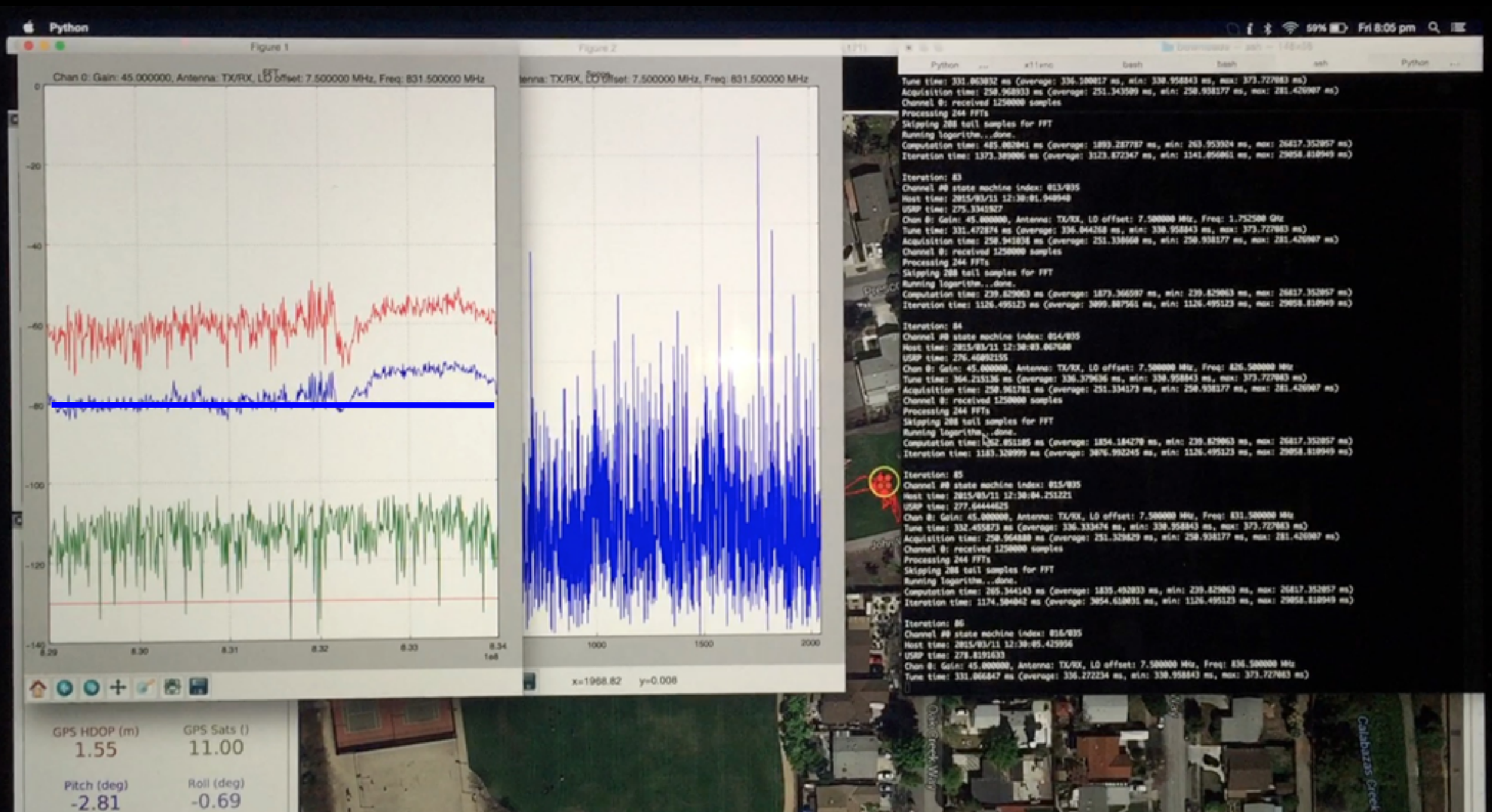
Spectrum Scanner



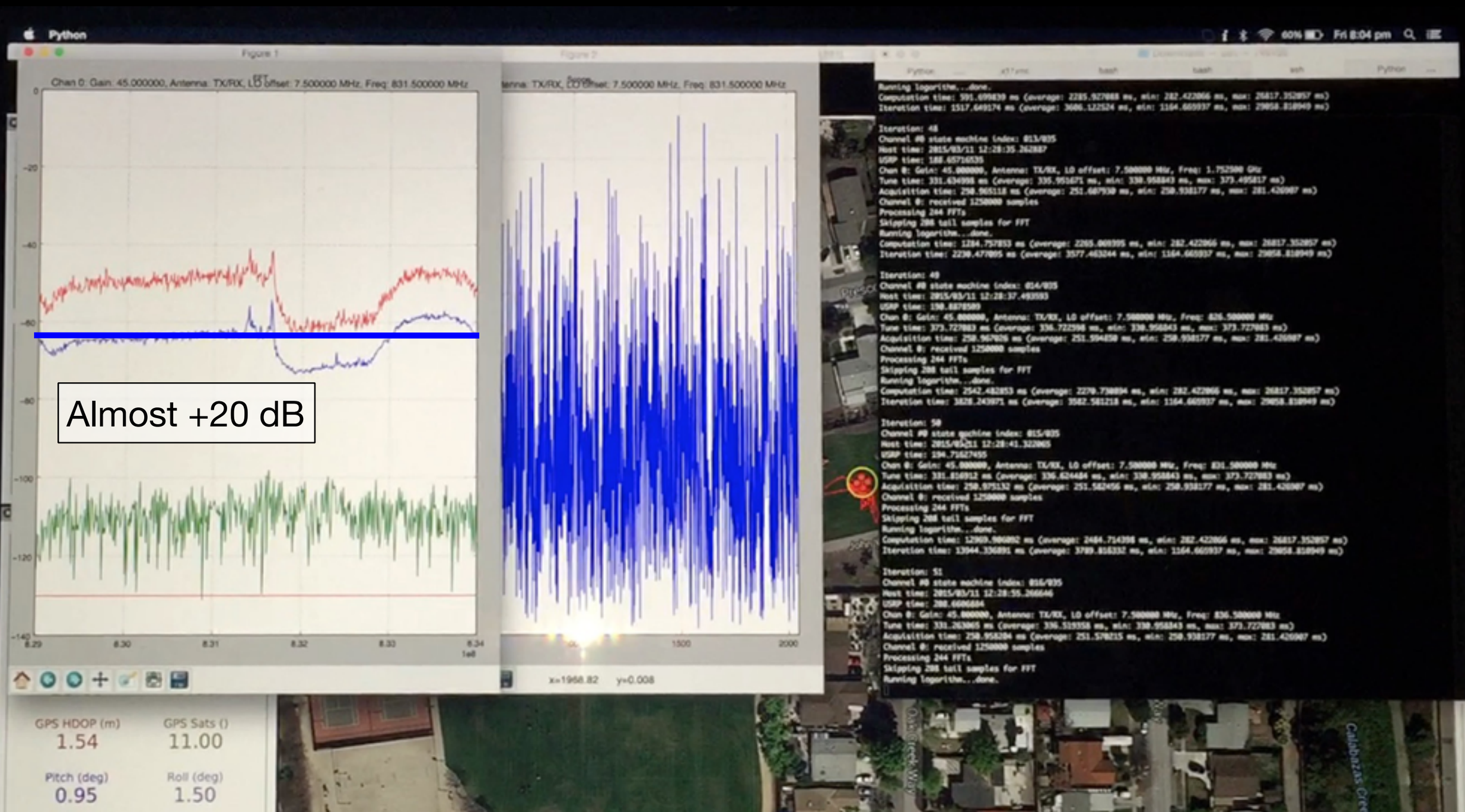




Ground-Level SNR



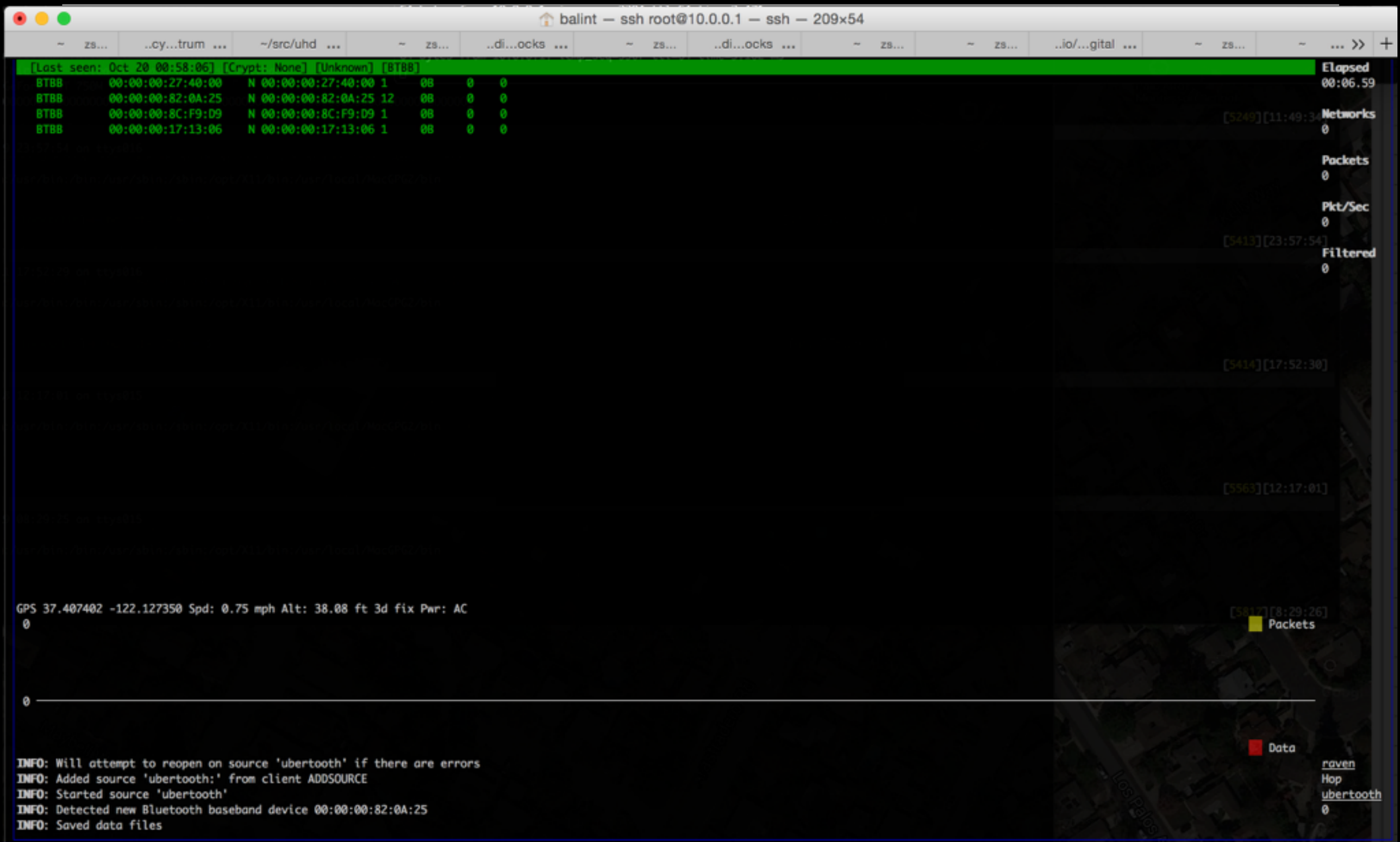
Airborne SNR



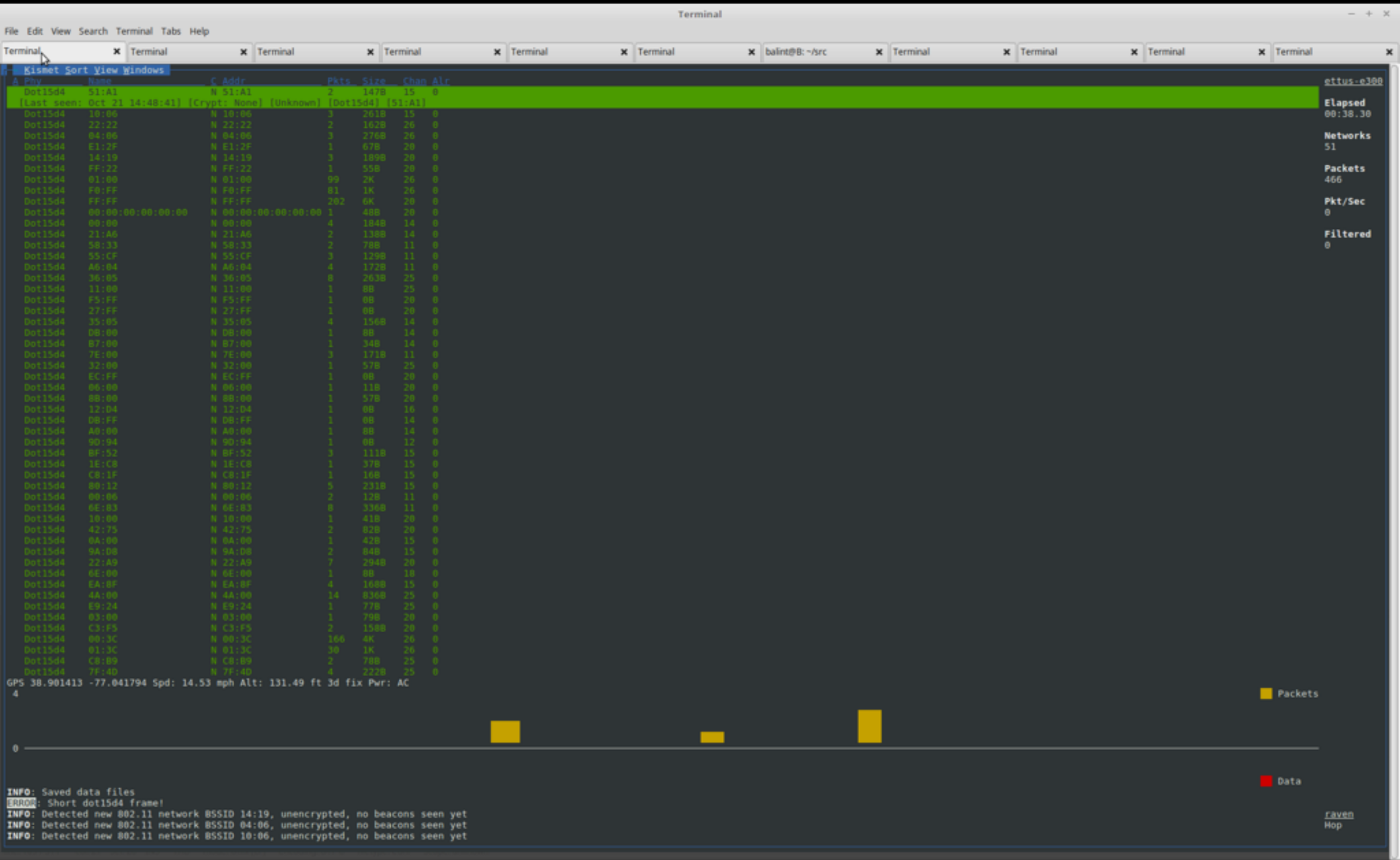
GSG Ubertooth dongle

Atmel RZRAVEN ZigBee dongle

Kismet with Ubertooth Plugin on E310

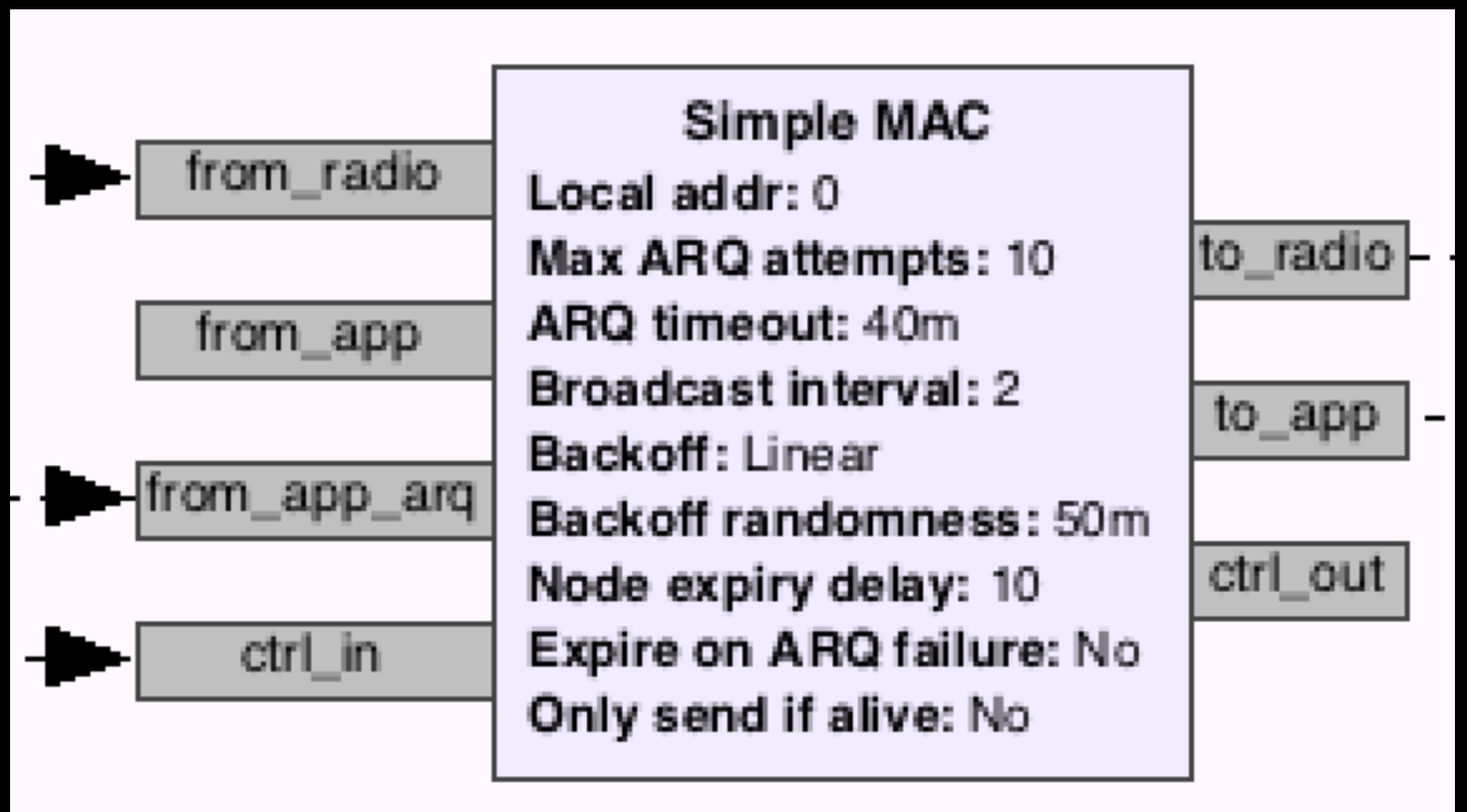


Kismet with ZigBee Plugin on E310



Backhaul

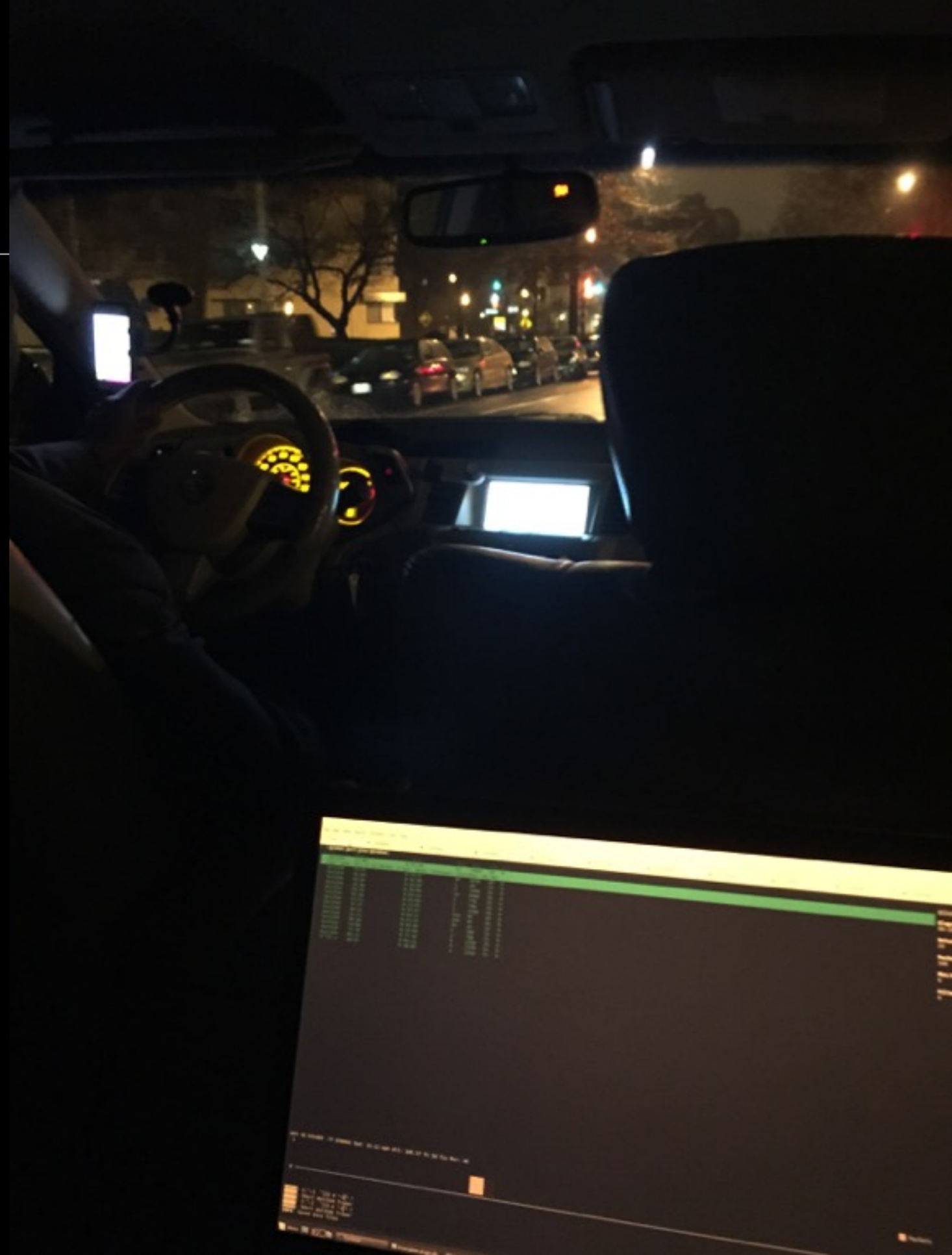
- None: Run unattended
- Wi-Fi: More 2.4 GHz ISM activity close to receiver & limited range
- Custom through SDR: greater range

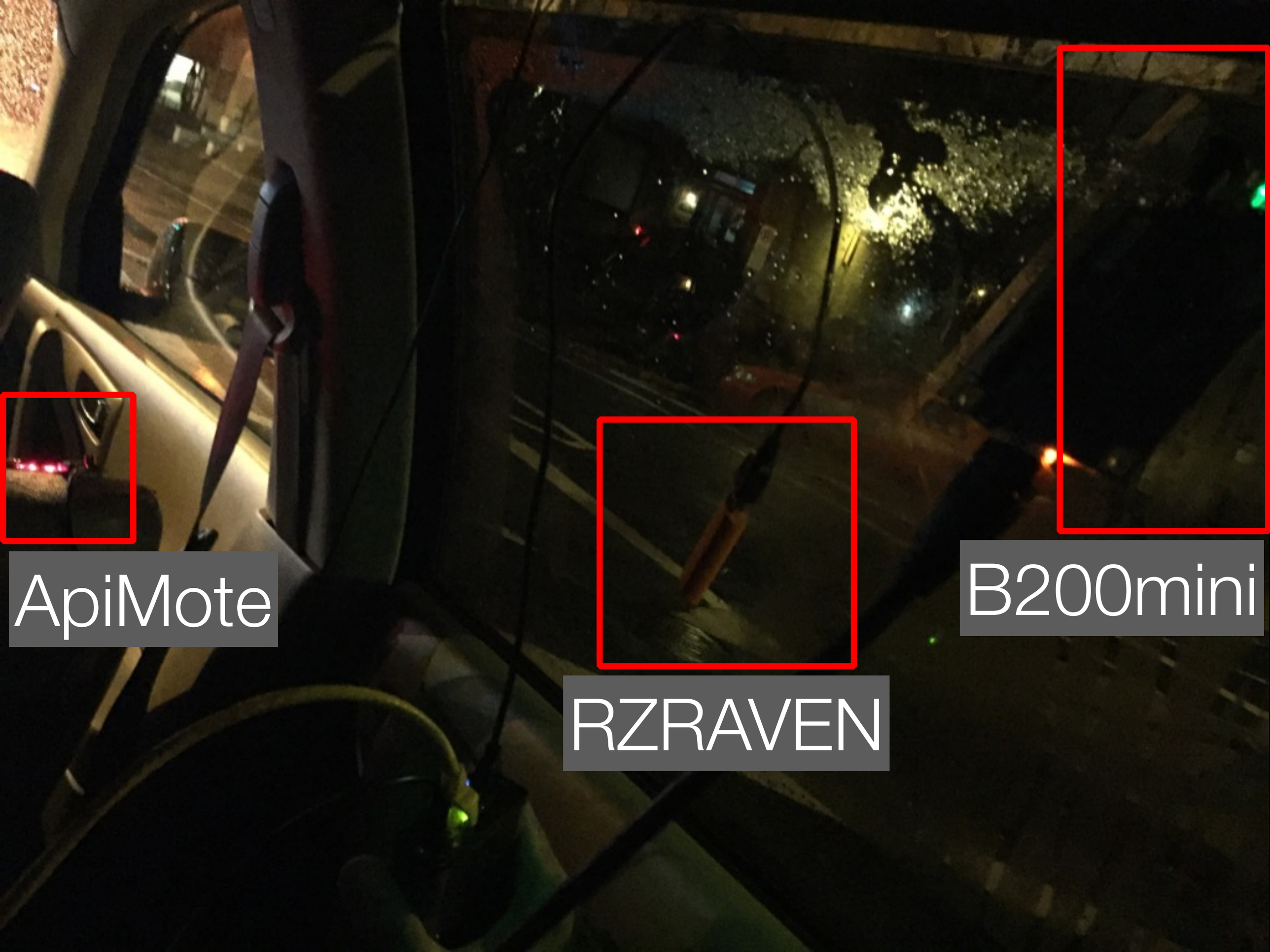


Airborne Platform

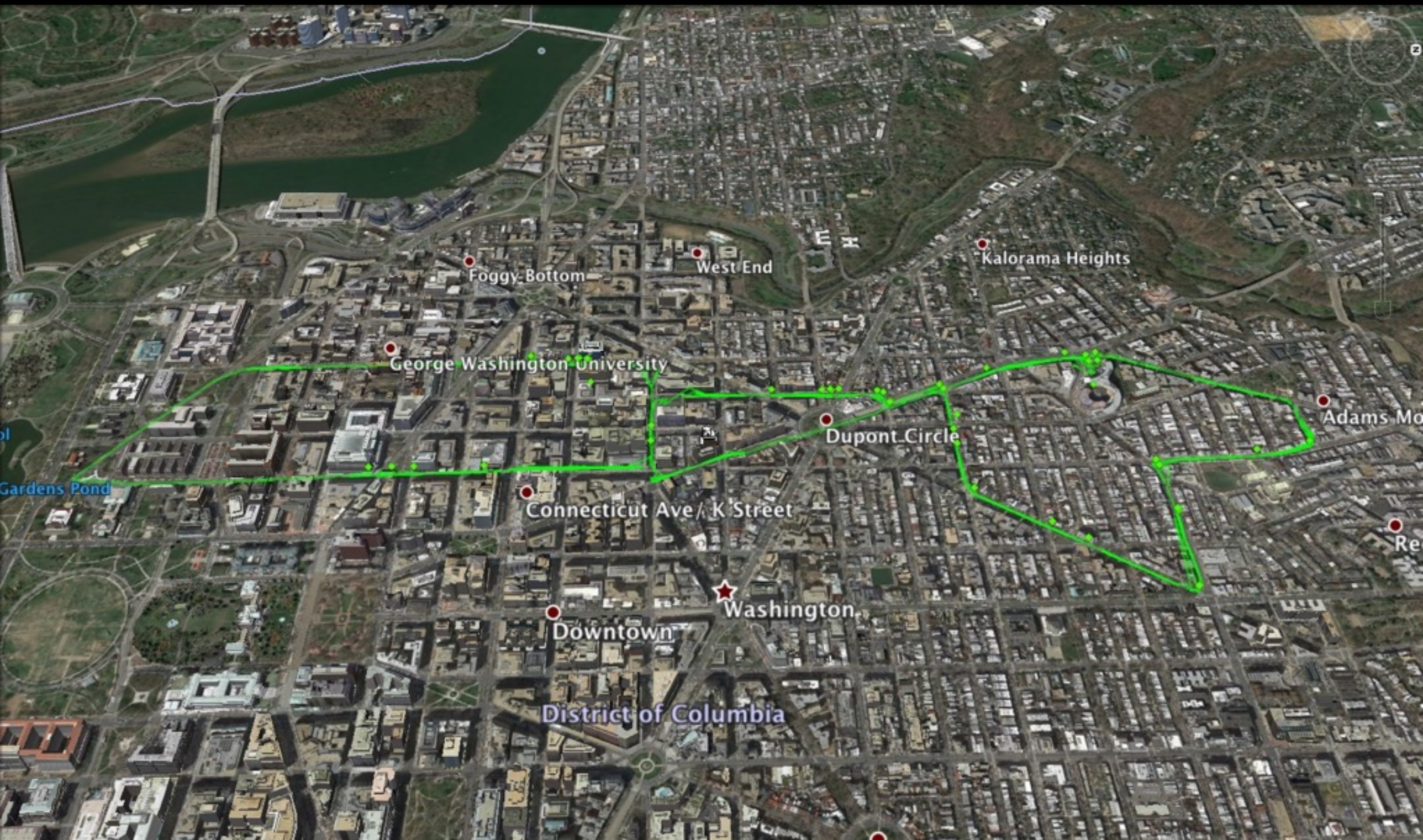
- Spectrum Monitoring & Recording
- Wi-Fi
- Bluetooth
- ZigBee
- Live Video
- Custom Backhaul

ZigBee Wardriving

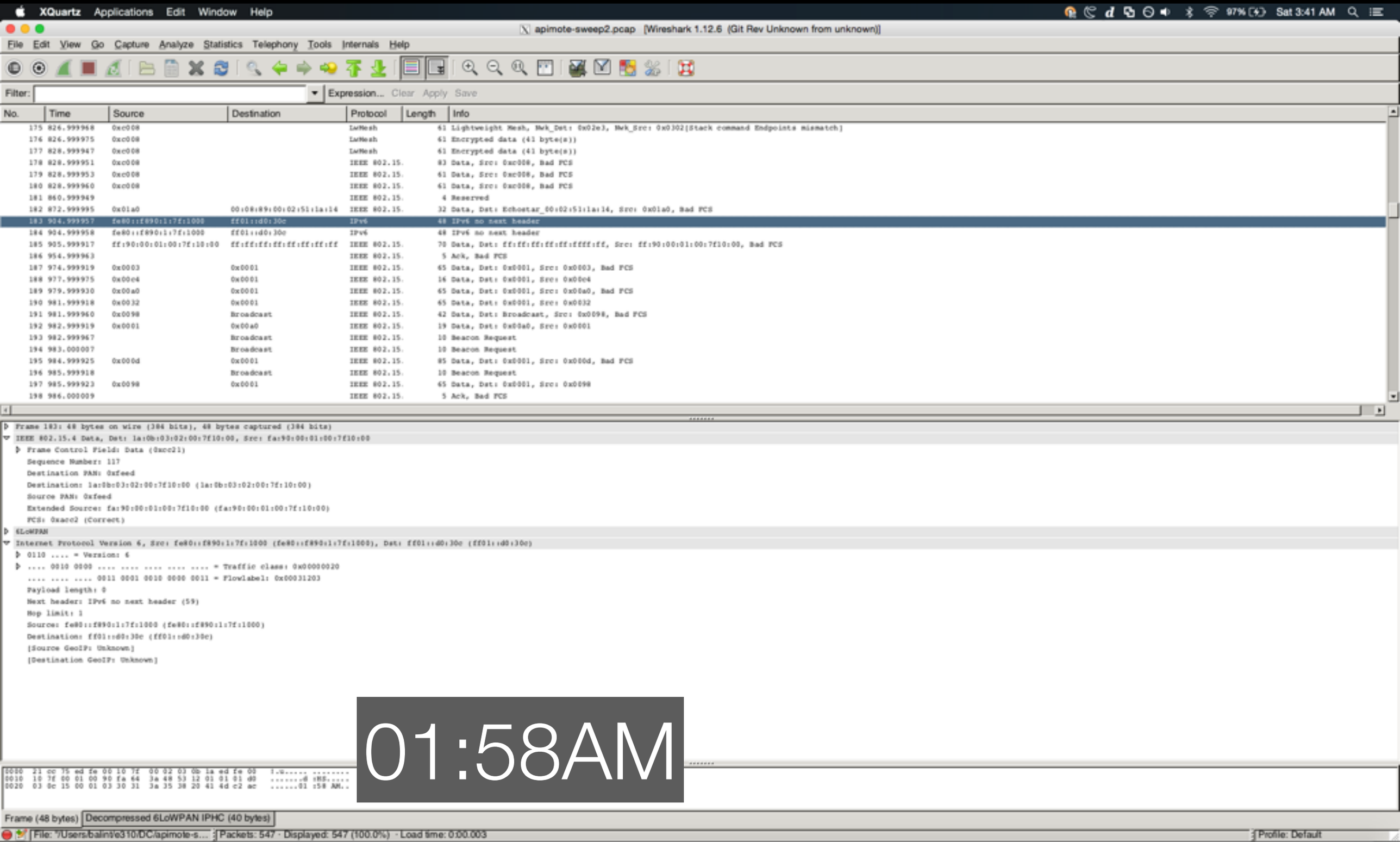



ApiMote
RZRAVEN
B200mini

ZigBee Wardriving

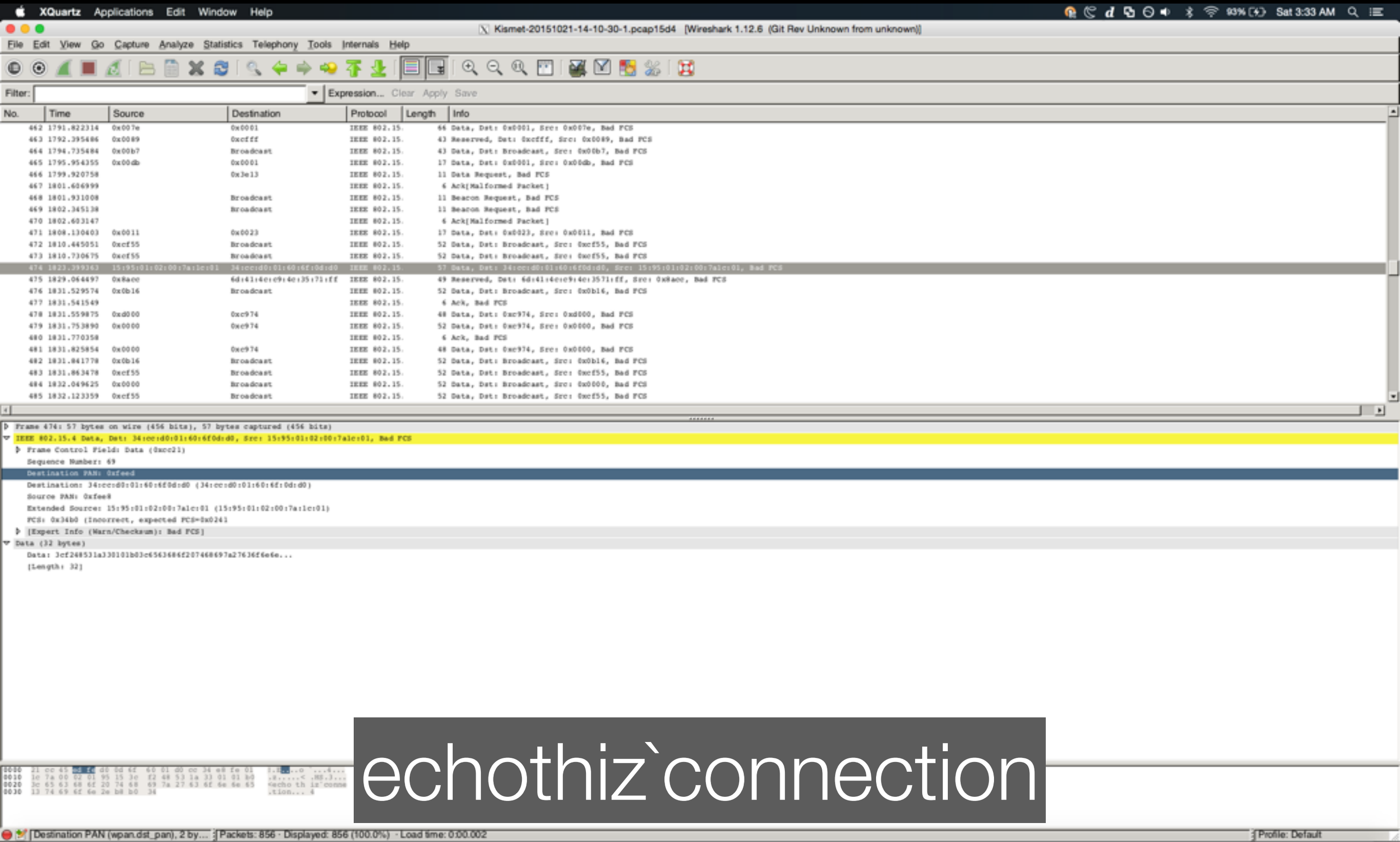


ZigBee Wardriving



01:58AM

ZigBee Wardriving



echothiz`connection

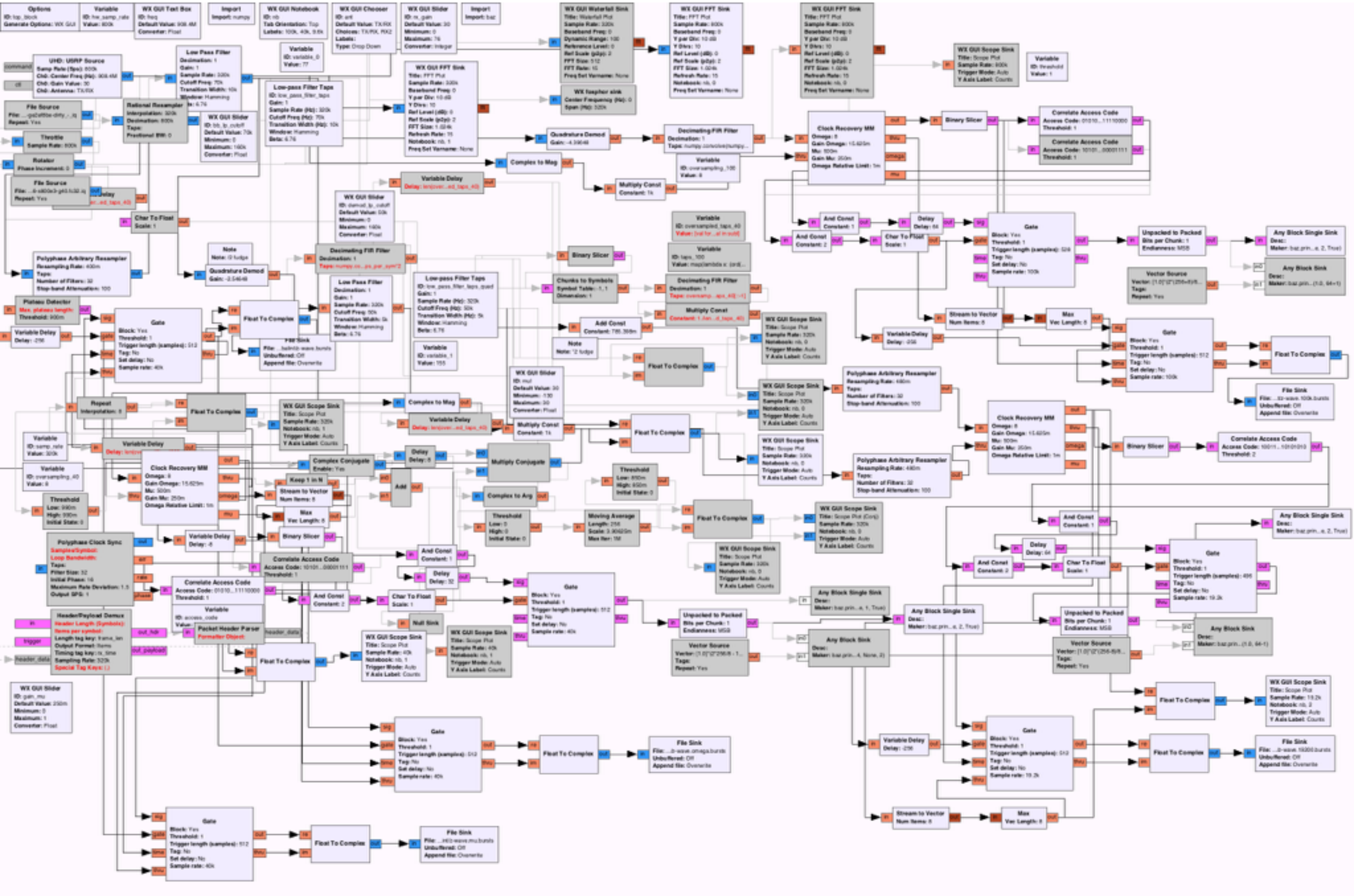
Other Signals

Z-Wave

- Home automation
- 908.4(2) MHz
- Three rates:
  - 9.6k
  - 40k
  - 100k

Z-Wave

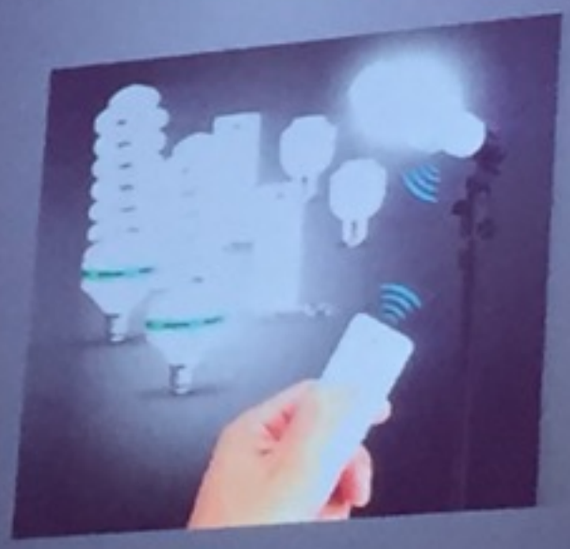

QuickTime Player File Edit View Window Help
Fri 3:46 PM
Z-Wave RX.grc - /Users/balint/Documents/GRC/Test - GNU Radio Companion
File Edit View Run Tools Help
wifi_rx-qt
Random raster speed test
Z-Wave RX
Baudline
fosphor
Conv
Top Block
rx_gain: 47
100k 40k 9.6k
Scope Plot
Persistence
Axes Options
Secs/Div:
Counts/Div:
Y Offset:
T Offset:
Autorange
Channel Options
Ch1 Ch2 Trig XY
Coupling: DC
Marker: Line Link
Stop
FFT Plot
Trace Options
Peak Hold
Average
Persistence
Trace A
Trace B
Axis Options
dB/Div:
Ref Level:
Autoscale
Stop
mul: 30
gain_mu: 250m
freq: 908.4M
demod_lp_cutoff: 50k
bb_lp_cutoff: 70k
ant: TX/RX
Options
Variable
WX GUI Text Box
Import
WX GUI Notebook
WX GUI Chooser
UHD: USRP Source
Low Pass Filter
Variable
Low-pass Filter Taps
File Source
Rational Resampler
WX GUI Slider
Throttle
Rotator
File Source
Char To Float
WX GUI Slider
Polyphase Arbitrary Resampler
Note
Quadrature Demod
Decimating FIR Filter
Low Pass Filter
Plateau Detector
Variable Delay
Gate
Float To Complex
File Sink
Repeat
Float To Complex
WX GUI Scope Sink
Variable
Stream Operators
Stream Tag Tools



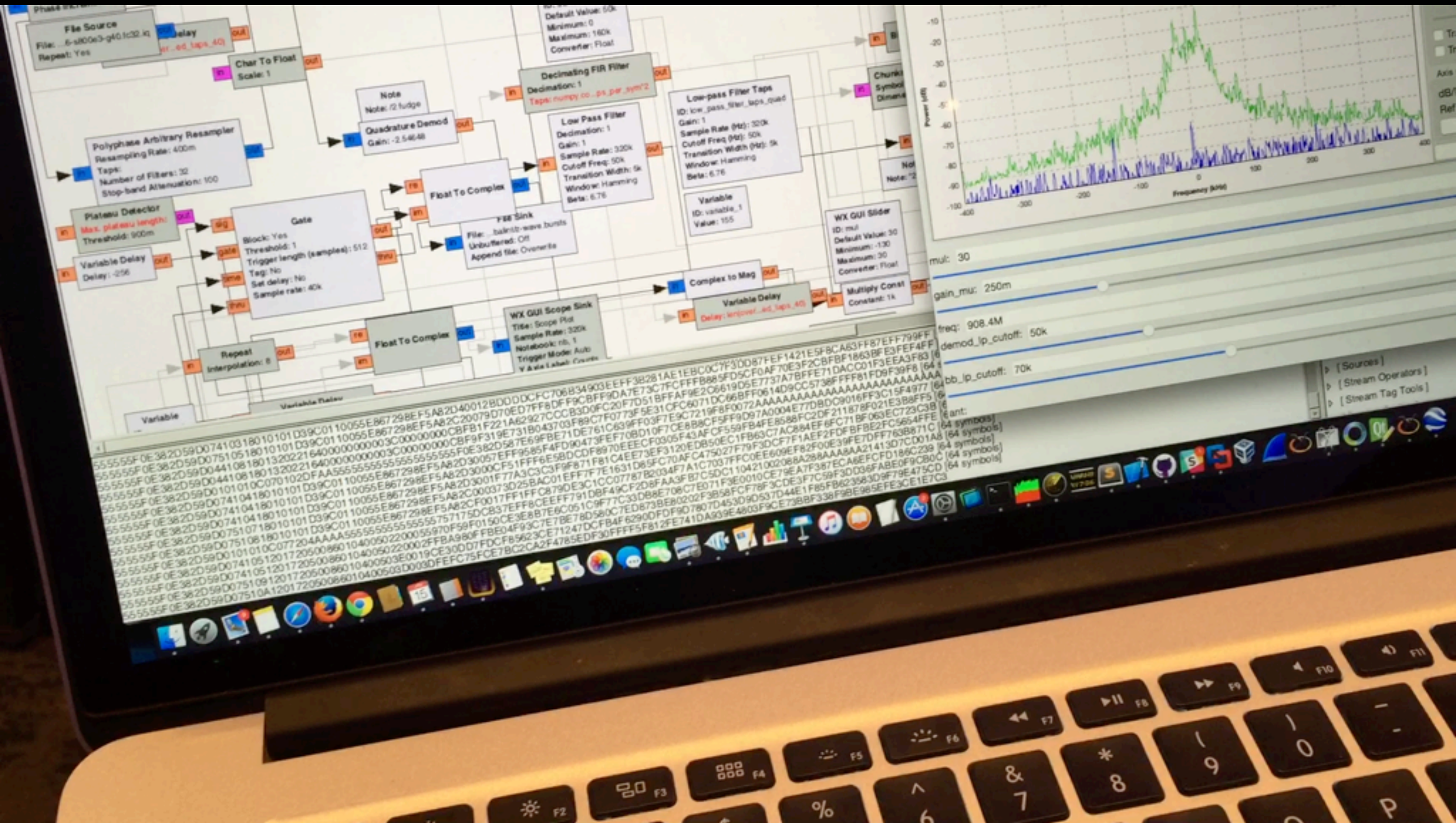
Options
Variable
WX GUI Text Box
Import
WX GUI Notebook
WX GUI Chooser
WX GUI Slider
WX GUI Waterfall Sink
WX GUI FFT Sink
WX GUI Scope Sink
UHD: USRP Source
Low Pass Filter
Low-pass Filter Taps
Rational Resampler
File Source
Throttle
Rotator
Char To Float
Polyphase Arbitrary Resampler
Plateau Detector
Variable Delay
Quadrature Demod
Decimating FIR Filter
Complex to Mag
Multiply Const
Clock Recovery MM
Binary Slicer
Correlate Access Code
And Const
Delay
Gate
Unpacked to Packed
Any Block Single Sink
Any Block Sink
Vector Source
Stream to Vector
Max
Float To Complex
File Sink
Chunks to Symbols
Add Const
Repeat
Complex Conjugate
Multiply Conjugate
Complex to Arg
Threshold
Moving Average
Keep 1 in N
Add
Polyphase Clock Sync
Header/Payload Demux
Packet Header Parser
Null Sink
Note

Breaking Bulbs

- Z-Wave is not the only smart energy protocol!
- 2.4 GHz
  - Wi-Fi
  - ZigBee
  - 6LoWPAN
  - WirelessHART
  - Bluetooth
- < 1 GHz
  - Z-Wave
  - Insteon
  - Lutron
  - Xodus
  - ...



Z-Wave


File Source
Repeat: Yes
Char To Float
Scale: 1
Note
Note: /21udge
Quadrature Demod
Gain: -2.54648
Decimating FIR Filter
Decimation: 1
Low Pass Filter
Decimation: 1
Gain: 1
Sample Rate: 320k
Cutoff Freq: 50k
Transition Width: 5k
Window: Hamming
Beta: 6.76
Low-pass Filter Taps
ID: low_pass_filter_taps_quad
Gain: 1
Sample Rate (Hz): 320k
Cutoff Freq (Hz): 50k
Transition Width (Hz): 5k
Window: Hamming
Beta: 6.76
Polyphase Arbitrary Resampler
Resampling Rate: 400m
Taps:
Number of Filters: 32
Stop-band Attenuation: 100
Plateau Detector
Max. plateau length:
Threshold: 900m
Variable Delay
Delay: -256
Gate
Block: Yes
Threshold: 1
Trigger length (samples): 512
Tag: No
Set delay: No
Sample rate: 40k
Float To Complex
File Sink
File: ...bal/rtl-wave.bursts
Unbuffered: Off
Append file: Overwrite
Variable
ID: variable_1
Value: 155
WX GUI Slider
ID: mul
Default Value: 30
Minimum: -130
Maximum: 30
Converter: Float
Multiply Const
Constant: 1k
Complex to Mag
Variable Delay
Repeat
Interpolation: 8
Float To Complex
WX GUI Scope Sink
Title: Scope Plot
Sample Rate: 320k
Notebook: nb, 1
Trigger Mode: Auto
Variable
Variable Delay
mul: 30
gain_mu: 250m
freq: 908.4M
demod_lp_cutoff: 50k
bb_lp_cutoff: 70k
[Sources]
[Stream Operators]
[Stream Tag Tools]

B200mini

Z-Wave around DC

555555F0EB1578020141010C0326021006F4F149DBCBBF29D4318B3AB0E28AAA32CB00F52E0115FF138C41156070576A259B421B16C
BECAA7AFB8E8F838EEE2A [64 symbols]

555555F1555555545D514F41D515555574144A15575554557D5D5D1C3555A5C5091DFDDD4455717C1D6191F455754755757479D4715
555515D55544545552C17 [64 symbols]

555545F0DD4265E5714546F71474FD5935260618144170D55555F0D7242DFF0850455890060AAF3AA969B53F732828EF19B1A046E2A
0AAA6A2EA22A8E4BAAAB8 [64 symbols]

555554F055045C555551555555555D5555D555D55557545545D51F0551A5555515155D555555555155D5C5539CF5171475FF914006D5
D6751F5DD554528461F1F [64 symbols]

5555557001516570C7C55479DBBAAAEA888AAF022816AAAEAAA2AEEBFBA0FE7C9D7D557C5C5755515557845025573F41F92080BAA22
E3F7E29DD555555515545 [64 symbols]

555555705725DF9C117E6FCB5667C3455550476C5D5A55554501DF5D60F20E4AA5066547FDD1D10FC75D7C42009CE5D497551551458
4259535E715C54007D1F1 [64 symbols]

555555F07D0F5DDF771387134E77D37F40F9280D237C455E6592E1E80544A54E5277911DF0D76051536553C5531355999C91C4173FE
6C952D730AA8EB8EA5E9A [64 symbols]

555554F05555554555714E7073FD8BF87BF0F6C20081C4CF8518E052EA41DA61F8EBCEDE6810DD3FA3928B31FD7AAC5BAA60F1889DB9
CA387D99EFF6996EFE216 [64 symbols]

555755F0D18CF24309530B0C18B0026F40B7A49C115183DE785BB71CD9C61F475185179D94A700EC50C68000020800050300C141C1C
1C02000700040683810008 [64 symbols]

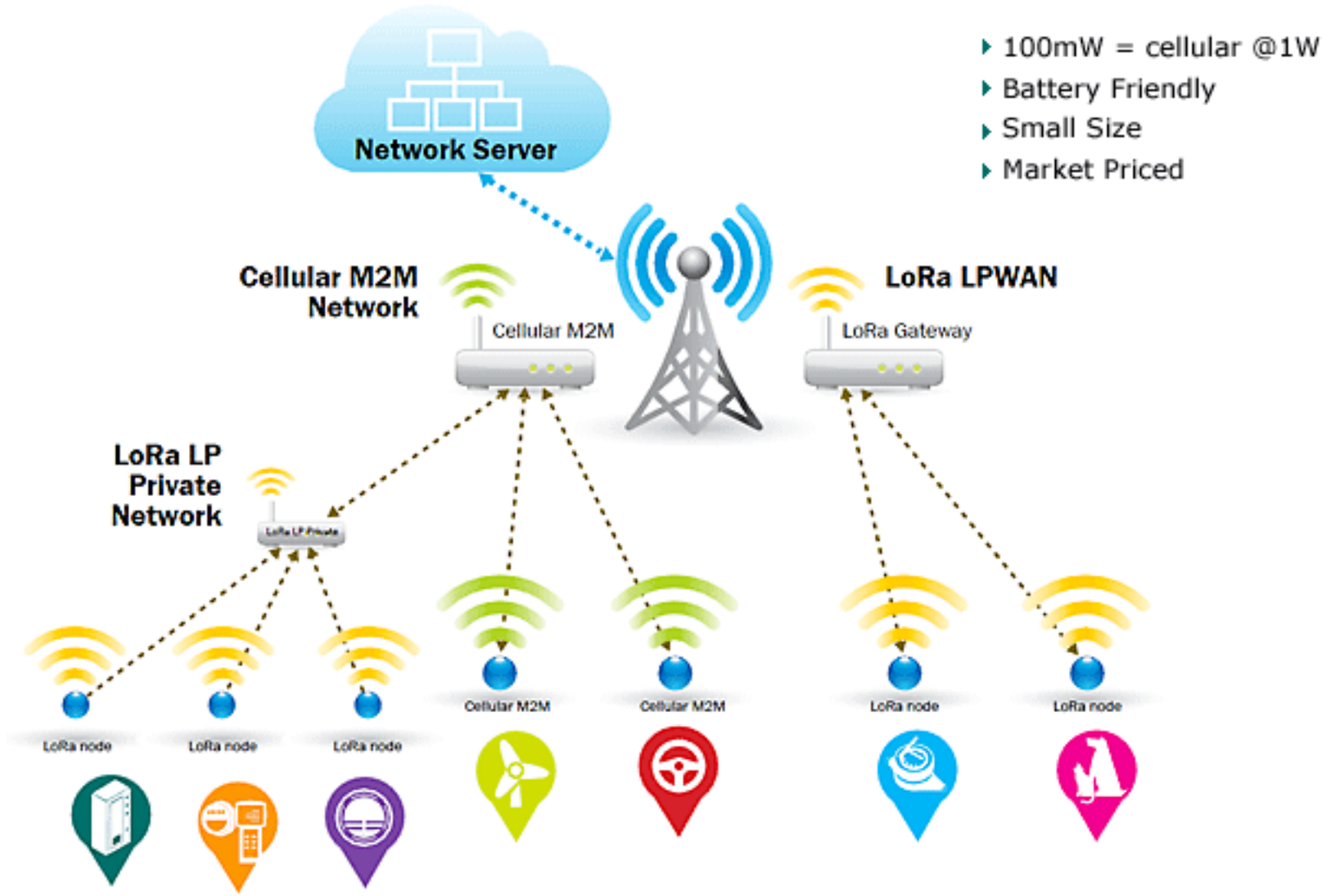
555555F0D18CE24208030B0A0909C1342E8002187CF020CBF63DD0089D7E6C6DC44278632A44357FC200B9C485EE1785F6CC47C21BA
786F255808E0FC4235C79 [64 symbols]

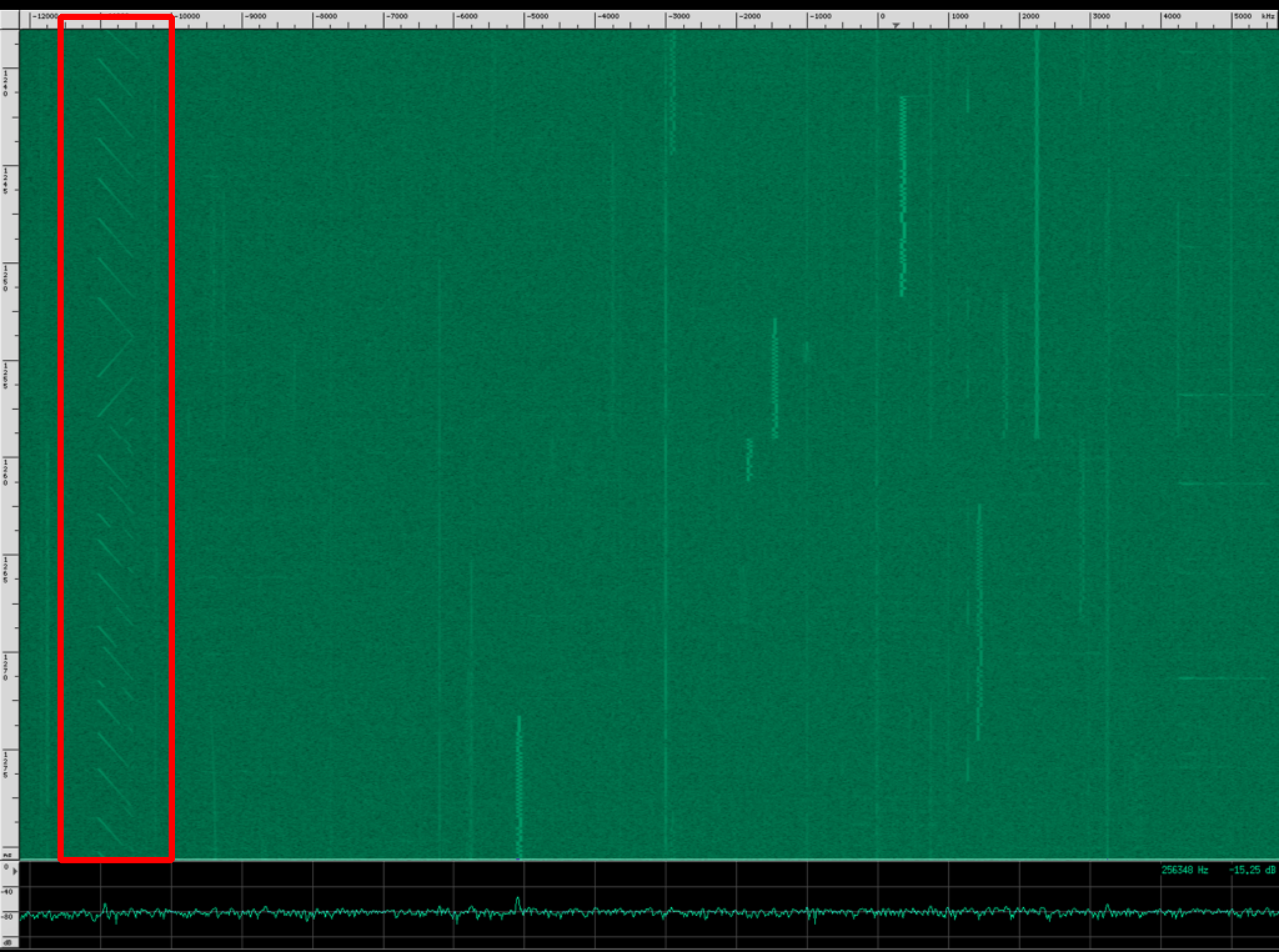
555555F0D18CE24208410D0D012003FF96517925490C33D0F4F1FA2FEF0AE332C3B69189E0A08D0054029FCCE66C3F308FD3945AE73
39F33DDC600222BC43F67 [64 symbols]

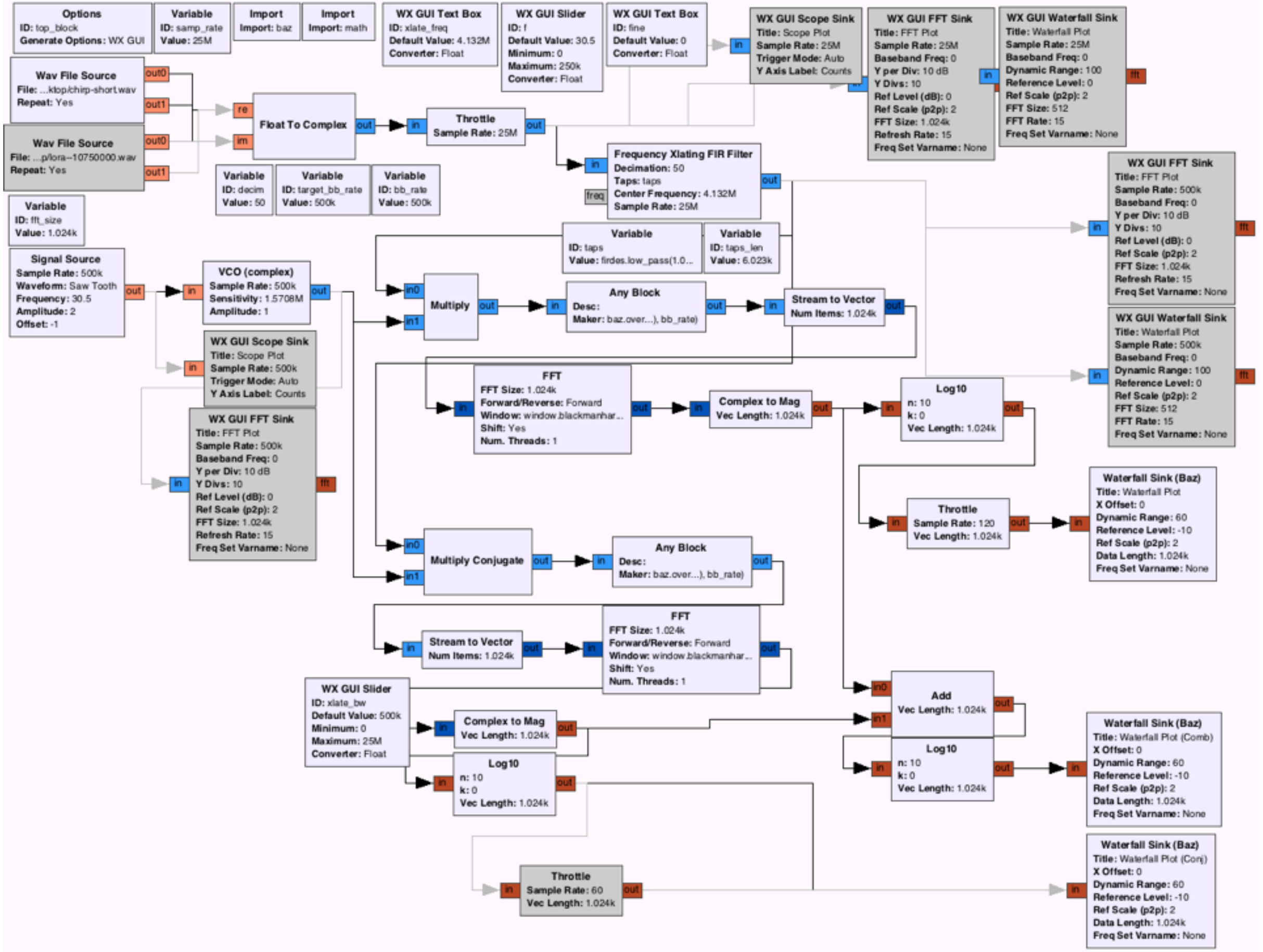
555555F0D18CE24208410D0D012003FF964E3C5021C31F7A60DC1F00DF00E4305DB9FFA1062E4F6B74F7CFFD4AEE8E18EF9EF429941
1D82901B29F201FFC0088 [64 symbols]

LoRa

- Chirp Spread Spectrum (CSS)
- 915 MHz ISM band
- UL & DL channels
- Variable bandwidth/ spreading factor
- Coexistence
- Replace GPRS?




-12000
-10000
-9000
-8000
-7000
-6000
-5000
-4000
-3000
-2000
-1000
0
1000
2000
3000
4000
5000
kHz
256348 Hz
-15.25 dB


Options
ID: top_block
Generate Options: WX GUI
Variable
ID: samp_rate
Value: 25M
Import
Import: baz
Import
Import: math
WX GUI Text Box
ID: xlate_freq
Default Value: 4.132M
Converter: Float
WX GUI Slider
ID: f
Default Value: 30.5
Minimum: 0
Maximum: 250k
Converter: Float
WX GUI Text Box
ID: fine
Default Value: 0
Converter: Float
WX GUI Scope Sink
Title: Scope Plot
Sample Rate: 25M
Trigger Mode: Auto
Y Axis Label: Counts
WX GUI FFT Sink
Title: FFT Plot
Sample Rate: 25M
Baseband Freq: 0
Y per Div: 10 dB
Y Divs: 10
Ref Level (dB): 0
Ref Scale (p2p): 2
FFT Size: 1.024k
Refresh Rate: 15
Freq Set Varname: None
WX GUI Waterfall Sink
Title: Waterfall Plot
Sample Rate: 25M
Baseband Freq: 0
Dynamic Range: 100
Reference Level: 0
Ref Scale (p2p): 2
FFT Size: 512
FFT Rate: 15
Freq Set Varname: None
Wav File Source
File: ...ktop/chirp-short.wav
Repeat: Yes
Wav File Source
File: ...p/lora--10750000.wav
Repeat: Yes
Float To Complex
Throttle
Sample Rate: 25M
Variable
ID: decim
Value: 50
Variable
ID: target_bb_rate
Value: 500k
Variable
ID: bb_rate
Value: 500k
Frequency Xlating FIR Filter
Decimation: 50
Taps: taps
Center Frequency: 4.132M
Sample Rate: 25M
Variable
ID: fft_size
Value: 1.024k
Variable
ID: taps
Value: firdes.low_pass(1.0...
Variable
ID: taps_len
Value: 6.023k
Signal Source
Sample Rate: 500k
Waveform: Saw Tooth
Frequency: 30.5
Amplitude: 2
Offset: -1
VCO (complex)
Sample Rate: 500k
Sensitivity: 1.5708M
Amplitude: 1
Multiply
Any Block
Desc:
Maker: baz.over...), bb_rate)
Stream to Vector
Num Items: 1.024k
WX GUI FFT Sink
Title: FFT Plot
Sample Rate: 500k
Baseband Freq: 0
Y per Div: 10 dB
Y Divs: 10
Ref Level (dB): 0
Ref Scale (p2p): 2
FFT Size: 1.024k
Refresh Rate: 15
Freq Set Varname: None
WX GUI Waterfall Sink
Title: Waterfall Plot
Sample Rate: 500k
Baseband Freq: 0
Dynamic Range: 100
Reference Level: 0
Ref Scale (p2p): 2
FFT Size: 512
FFT Rate: 15
Freq Set Varname: None
WX GUI Scope Sink
Title: Scope Plot
Sample Rate: 500k
Trigger Mode: Auto
Y Axis Label: Counts
WX GUI FFT Sink
Title: FFT Plot
Sample Rate: 500k
Baseband Freq: 0
Y per Div: 10 dB
Y Divs: 10
Ref Level (dB): 0
Ref Scale (p2p): 2
FFT Size: 1.024k
Refresh Rate: 15
Freq Set Varname: None
FFT
FFT Size: 1.024k
Forward/Reverse: Forward
Window: window.blackmanhar...
Shift: Yes
Num. Threads: 1
Complex to Mag
Vec Length: 1.024k
Log10
n: 10
k: 0
Vec Length: 1.024k
Throttle
Sample Rate: 120
Vec Length: 1.024k
Waterfall Sink (Baz)
Title: Waterfall Plot
X Offset: 0
Dynamic Range: 60
Reference Level: -10
Ref Scale (p2p): 2
Data Length: 1.024k
Freq Set Varname: None
Multiply Conjugate
Any Block
Desc:
Maker: baz.over...), bb_rate)
Stream to Vector
Num Items: 1.024k
FFT
FFT Size: 1.024k
Forward/Reverse: Forward
Window: window.blackmanhar...
Shift: Yes
Num. Threads: 1
WX GUI Slider
ID: xlate_bw
Default Value: 500k
Minimum: 0
Maximum: 25M
Converter: Float
Complex to Mag
Vec Length: 1.024k
Log10
n: 10
k: 0
Vec Length: 1.024k
Add
Vec Length: 1.024k
Log10
n: 10
k: 0
Vec Length: 1.024k
Waterfall Sink (Baz)
Title: Waterfall Plot (Comb)
X Offset: 0
Dynamic Range: 60
Reference Level: -10
Ref Scale (p2p): 2
Data Length: 1.024k
Freq Set Varname: None
Throttle
Sample Rate: 60
Vec Length: 1.024k
Waterfall Sink (Baz)
Title: Waterfall Plot (Conj)
X Offset: 0
Dynamic Range: 60
Reference Level: -10
Ref Scale (p2p): 2
Data Length: 1.024k
Freq Set Varname: None

Top Block

xlate_freq: 10.75M

fine: 0

f: 0

xlate_bw: 500k

Waterfall Plot (Comb)

Time (s)

Data (kpoints)

Waterfall Plot (Conj)

Waterfall Plot

Top Block

xlate_freq: 10.75M

fine: 0

f: 488.5

xlate_bw: 500k

Waterfall Plot (Comb)

Options

Axes Options

Dyn Range: + -

Ref Level: + -

Color: RGB2

Autoscale

Clear

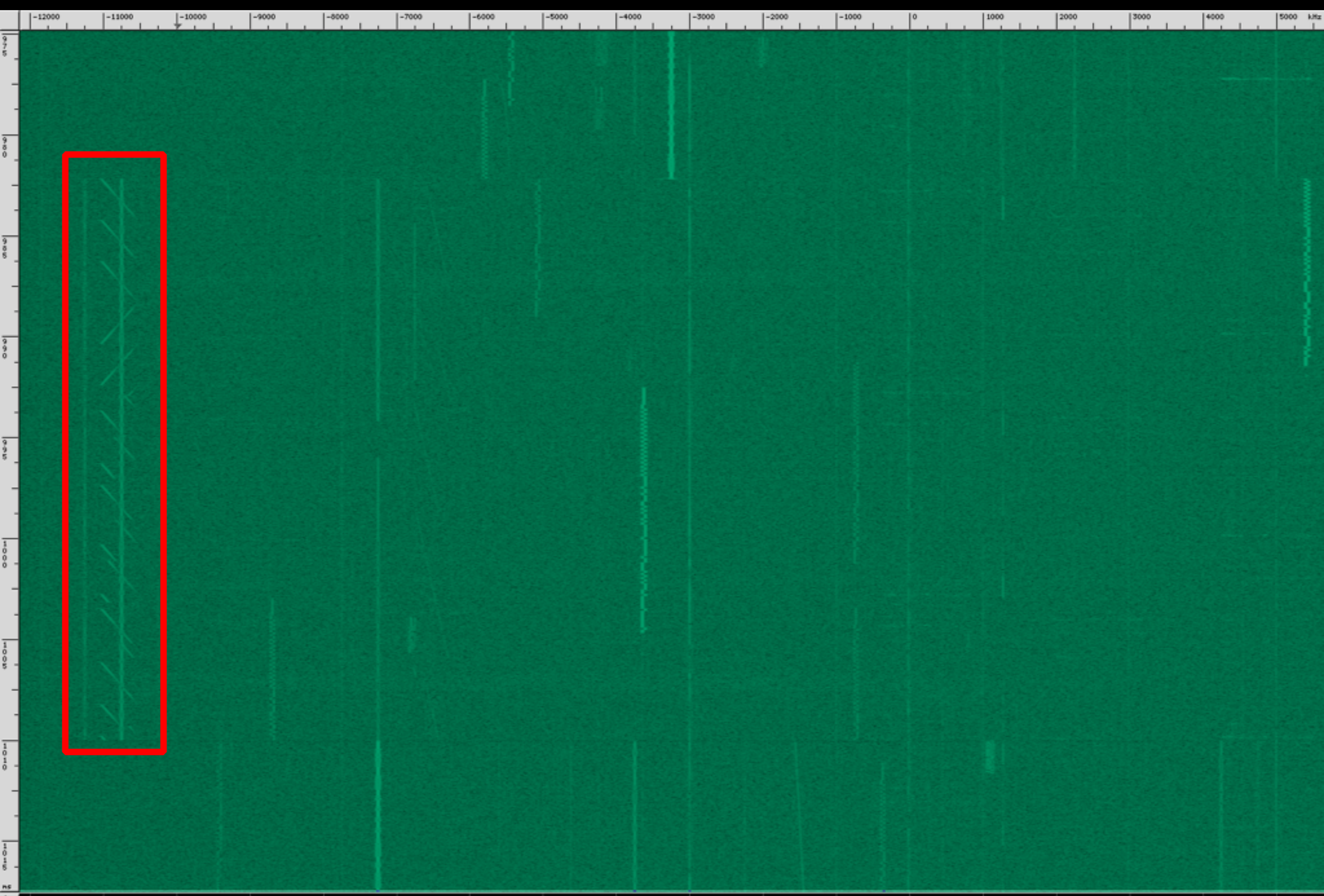
Stop

Waterfall Plot (Conj)

Waterfall Plot

Time (s)

Data (kpoints)


-12000
-11000
-10000
-9000
-8000
-7000
-6000
-5000
-4000
-3000
-2000
-1000
0
1000
2000
3000
4000
5000
kHz
ms
0
-40
-80
dB
-9985352 Hz
-140.00 dB

Top Block

xlate_freq: 10.75M

fine: 0

f: 0

xlate_bw: 500k

Waterfall Plot (Comb)

Time (s)

Data (kpoints)

Waterfall Plot (Conj)

Waterfall Plot

Top Block

xlate_freq: 10.75M

fine: 0

f: 488.5

xlate_bw: 500k

Waterfall Plot (Comb)

Time (s)

Data (kpoints)

Options

Axes Options

Dyn Range: + -

Ref Level: + -

Color: RGB2

Autoscale

Clear

Stop

Waterfall Plot (Conj)

Time (s)

Data (kpoints)

Options

Axes Options

Dyn Range: + -

Ref Level: + -

Color: RGB2

Autoscale

Clear

Stop

Waterfall Plot

Time (s)

Data (kpoints)

Options

Axes Options

Dyn Range: + -

Ref Level: + -

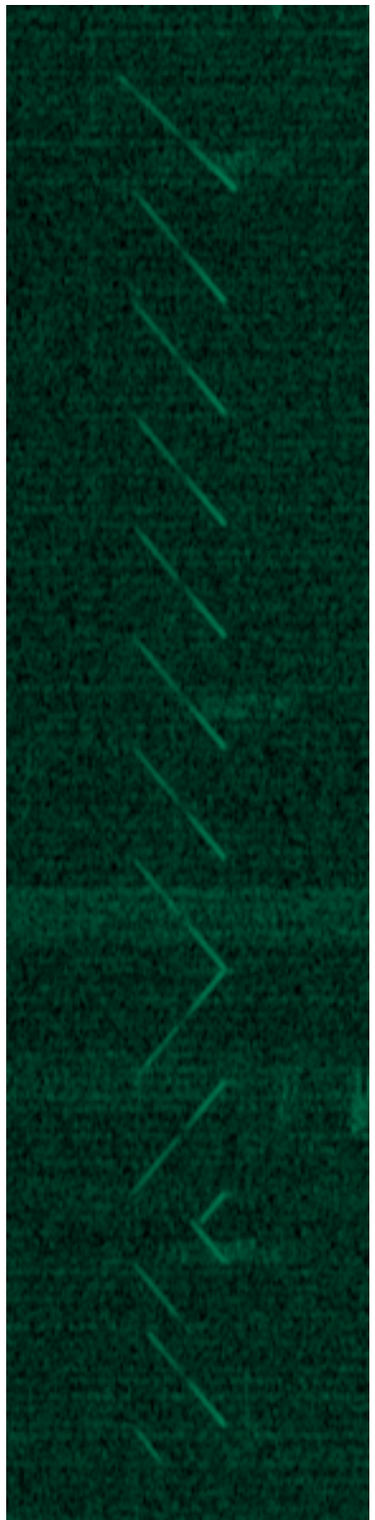
Color: RGB2

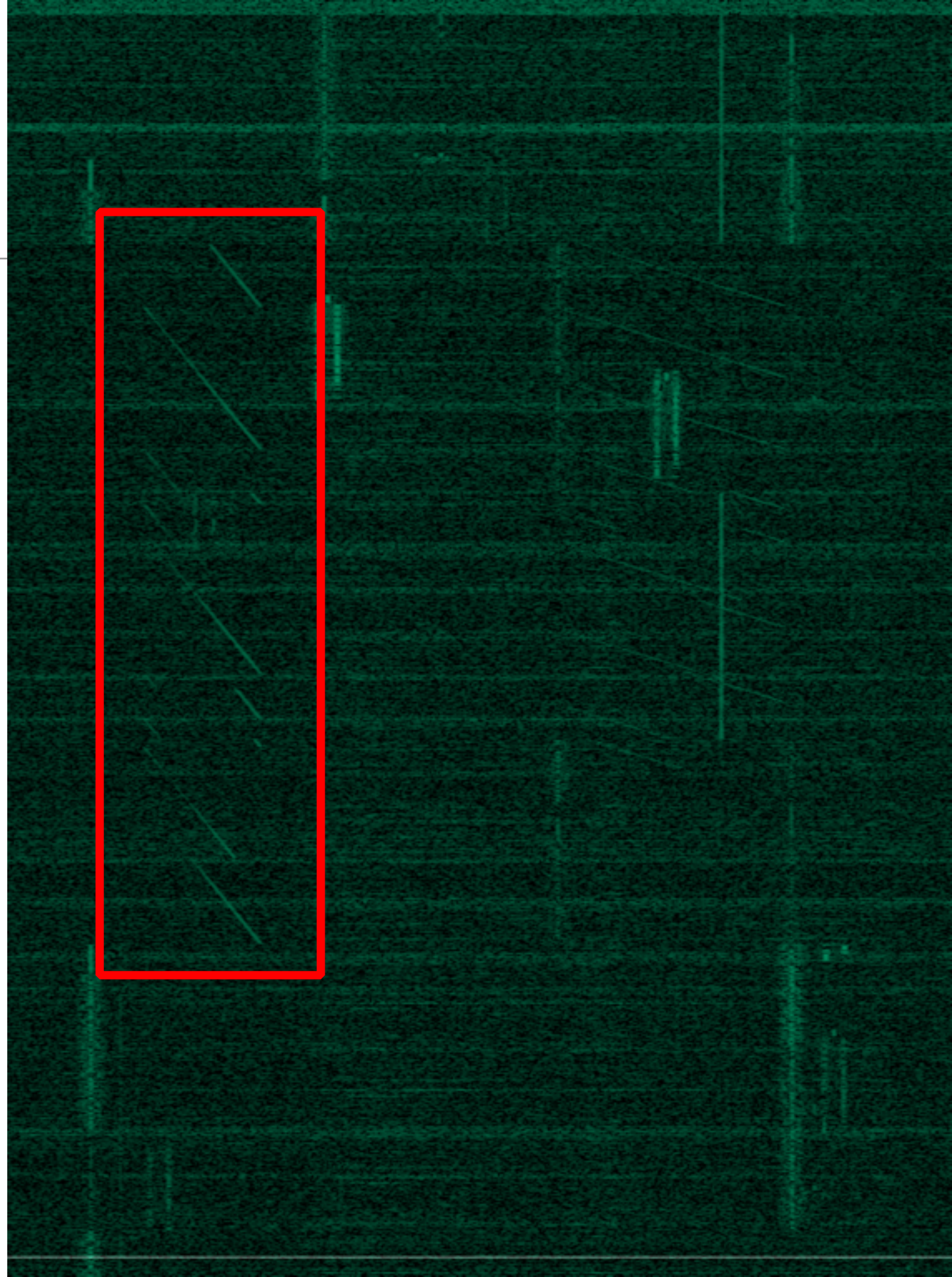
Autoscale

Clear

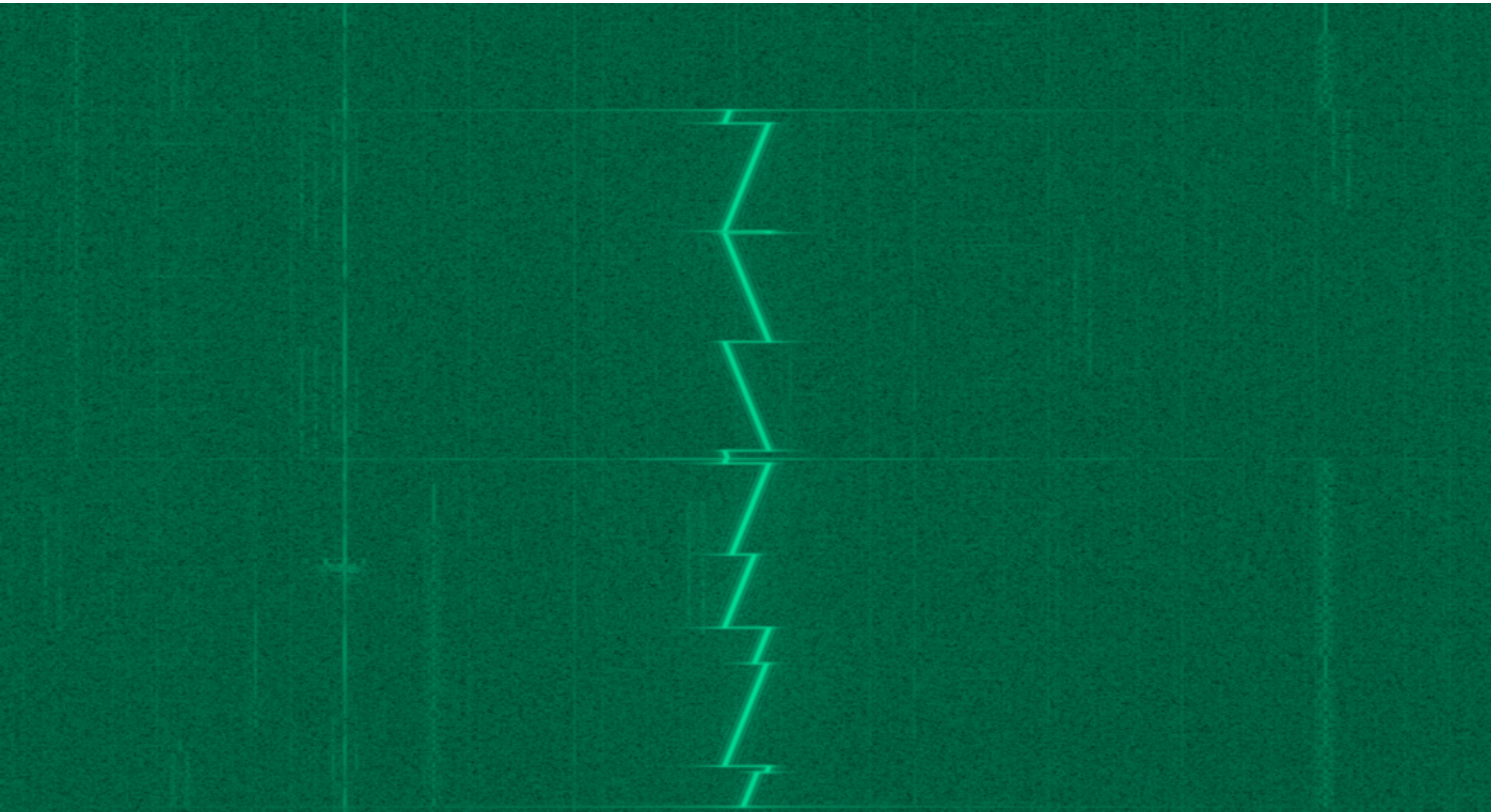
Stop

Other CSS?





Other CSS?



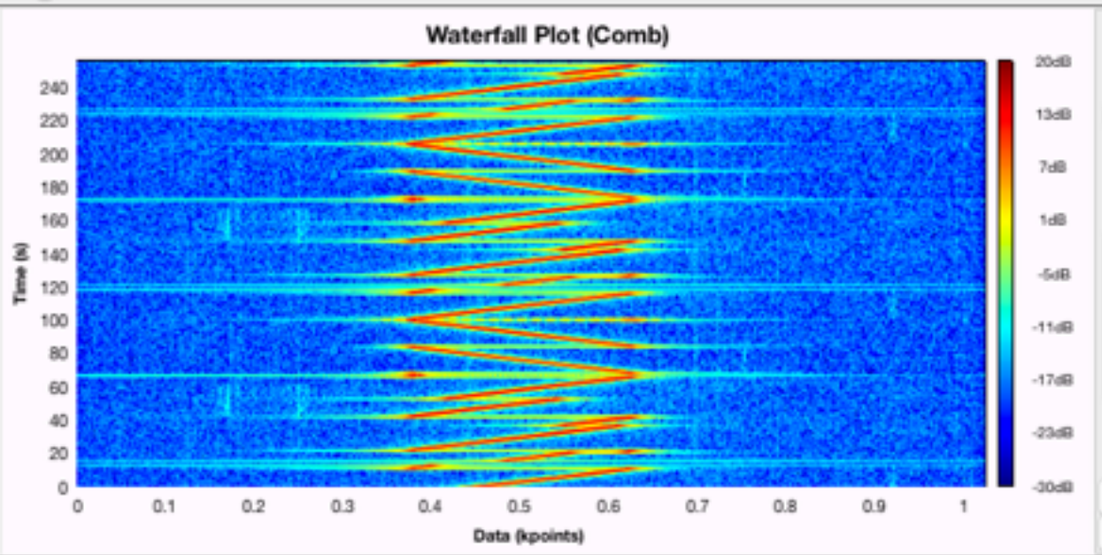
Top Block

xlate_freq: 4.132M

fine: 0

f: 0

xlate_bw: 500k



Optio

Axes

Dyn

Ref L

Colo

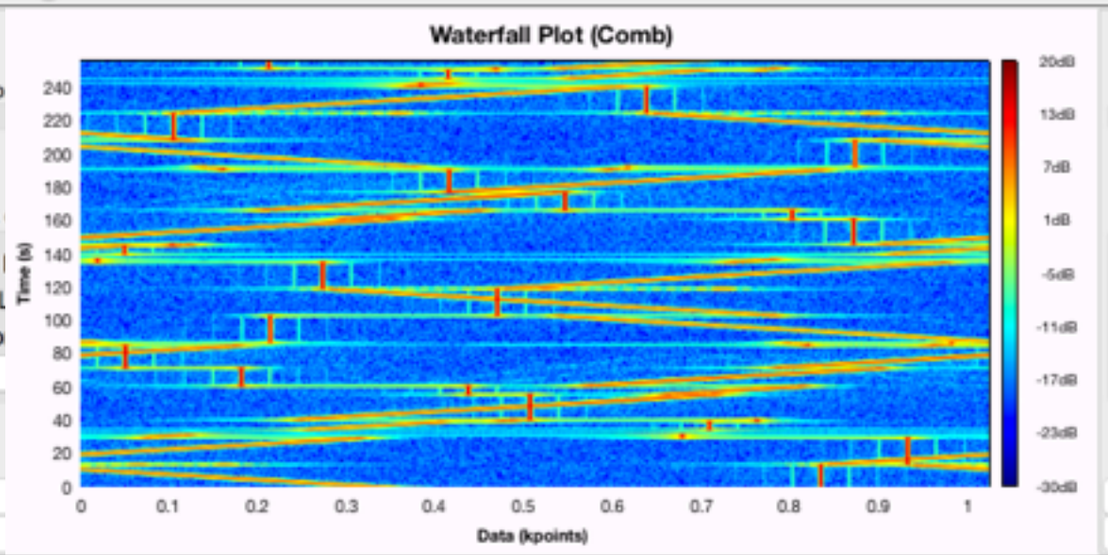
Top Block

xlate_freq: 4.132M

fine: 0

f: 30.5

xlate_bw: 500k



Options

Axes Options

Dyn Range: + -

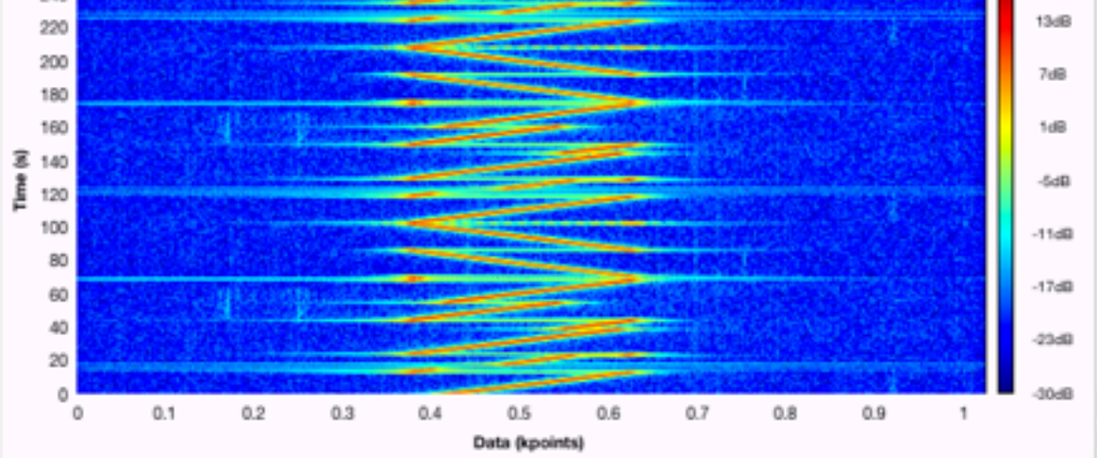
Ref Level: + -

Color: RGB2

Autoscale

Clear

Stop



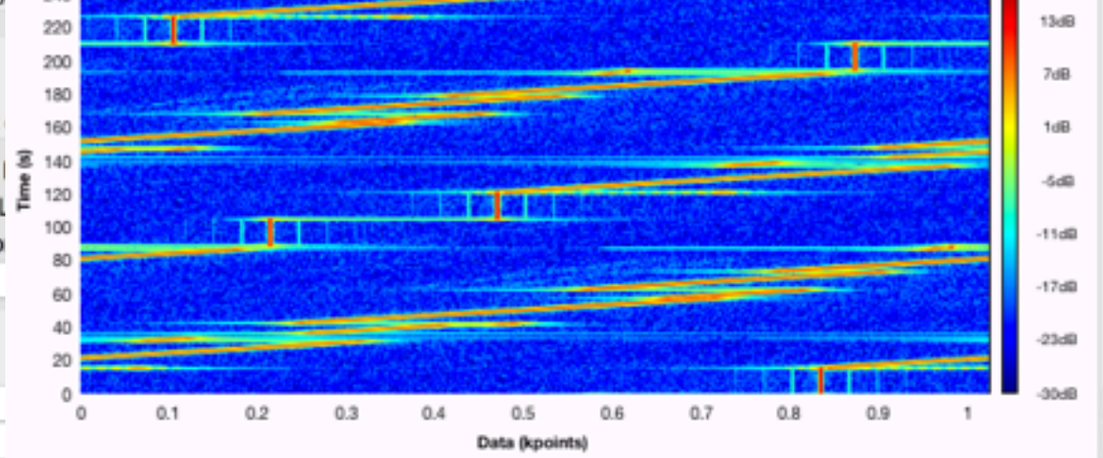
Optio

Axes

Dyn

Ref L

Colo



Options

Axes Options

Dyn Range: + -

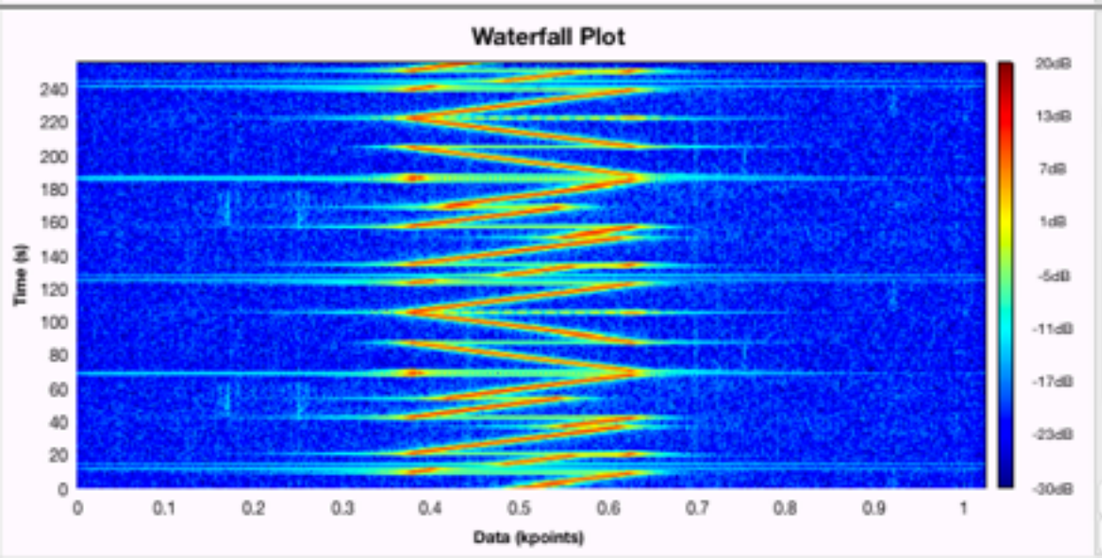
Ref Level: + -

Color: RGB2

Autoscale

Clear

Stop



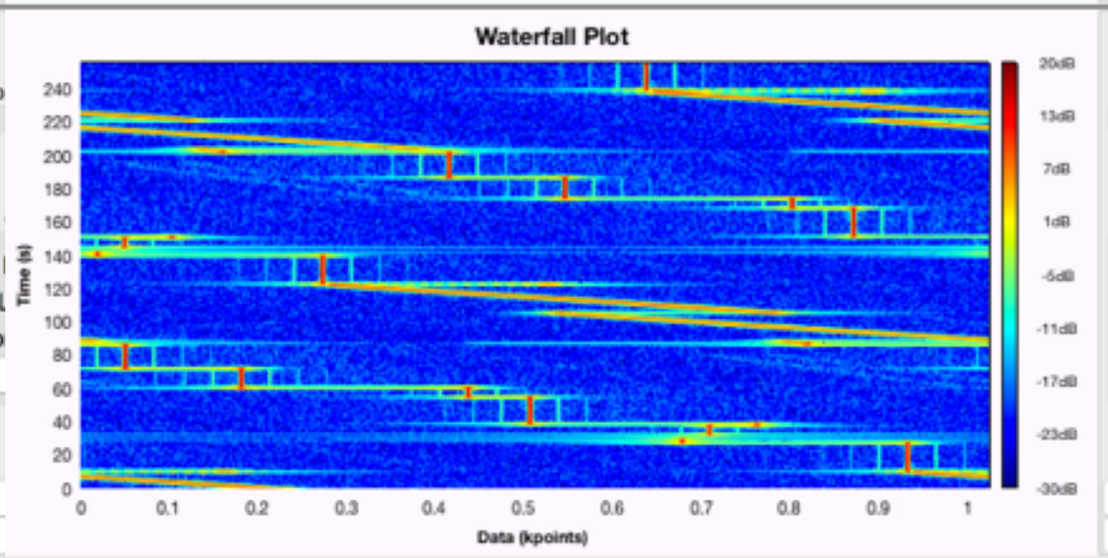
Optio

Axes

Dyn

Ref L

Colo



Options

Axes Options

Dyn Range: + -

Ref Level: + -

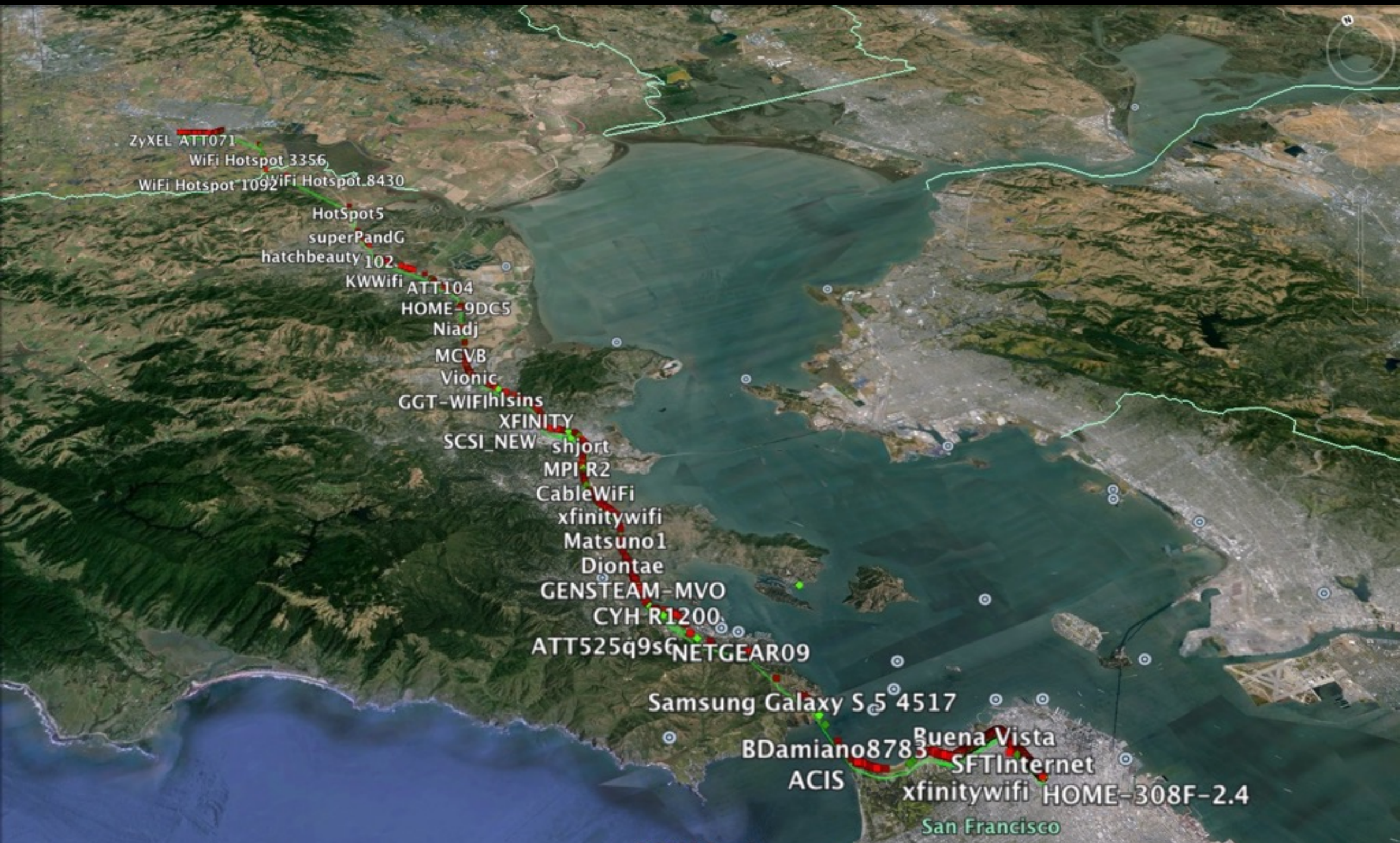
Color: RGB2

Autoscale

Clear

Stop

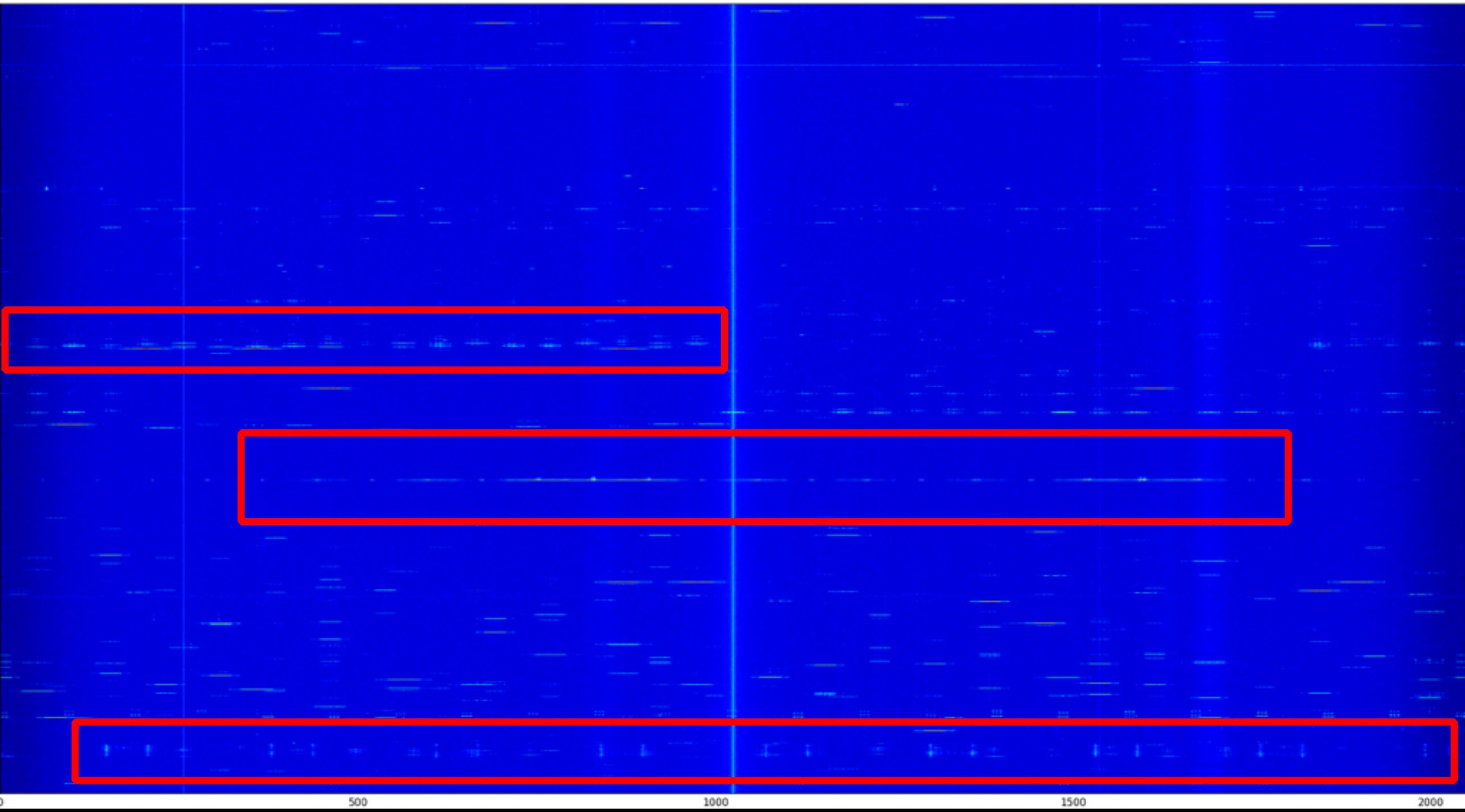
Spectrum Summary



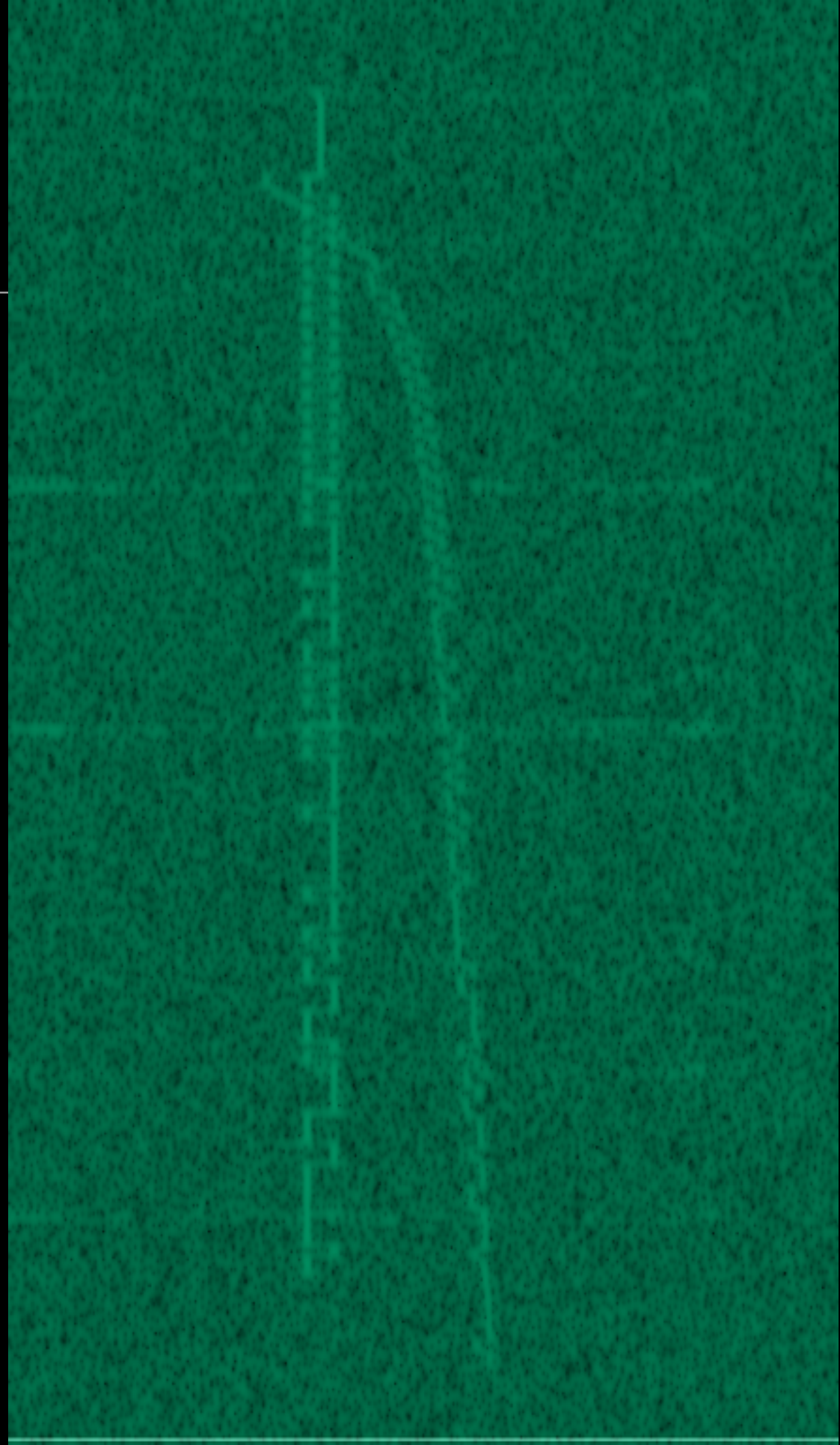
Spectrum Summary

Spectrum Summary

Spectrum Summary



Inebriated LO



OP25

Hacking the Wireless World with #sdr

@spenchdotnet

Op25 Grc

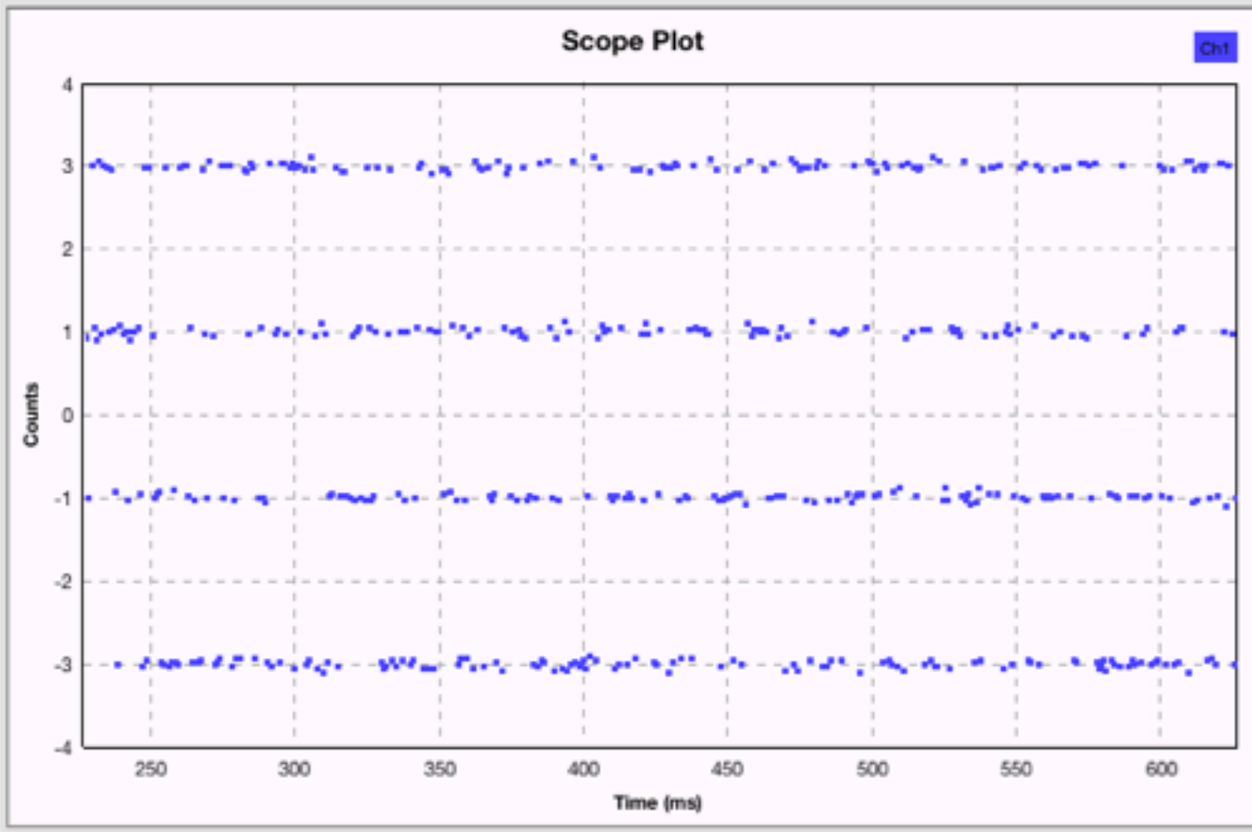
Fine Offset: 0

Xlate Offset: -19.3894k

Xlate BW: 24k

Verbose console logging

BB-1 | BB-2 | Xlate-1 | Xlate-2 | 4FSK | Dibits | Audio



Persistence

Analog Alpha: 0.0994

Axes Options

Secs/Div: + -

Counts/Div: + -

Y Offset: + -

T Offset:

Autorange

Channel Options

Ch1 | Trig

Coupling: DC

Marker: Dot Large

Stop

Output idle silence

Frequency: 469.45M

Auto tune: 0

Audio mul: 0

Final freq: 469.431M

DUID: LDU2

NAC: Default NAC

Source: 0x129712

Destination:

MFID: Standard MFID (pre-20

ALGID: DES-OFB

KID: 0x3780

MI: 0xb068e81a8eb86b6400

TGID: 0x0001

Gain: 20

Properties: OP25 Decoder (Simple)

General | Advanced | Documentation

ID	op25_decoder_simple_0
Key (hex)	
Key map (hex)	{0x3780: "C[redacted]4"}
Idle silence	No
Output traffic	Yes

```
LDU2: LSDW: 0xf301, valid
LDU2: 0 hamming errors, valid
LDU2: 0874 0535 013F 082E 07FF 02E2 061E 0010
LDU2: 08F4 03DC 0605 08A3 07FF 06ED 0361 0064
LDU2: 0935 0248 05EE 06A9 07FF 0578 014F 00DE
LDU2: 0935 014D 0DE1 024F 07FF 0557 05B9 00DA
LDU2: 0975 0908 09EA 0FD6 07FF 04C5 00F2 004C
LDU2: 096D 090C 0A39 04ED 07FF 07BC 024F 0020
LDU2: 0966 0CD2 06D3 0018 0400 037F 0128 00D5
LDU2: 0924 0FC1 09DB 0550 07FF 057A 04FF 00AA
LDU2: 09DD 0179 0D81 0C1C 06DE 0197 04CE 0046
LDU2:   AlgID: 0x81, KID: 0x3780, MI: ceed5275a045652600
DES:    1704 bits used from 28 iterations
```

```
LDU1: LSDW: 0xf83e, valid
LDU1: 0 hamming errors, valid
LDU1: LCF: 0x00, MFID: 0x00
LDU1: Emergency: 0x00, Reserved: 0x4000, TGID: 0x0001, Source: 0x129712
LDU1: 0855 0F42 05F5 0534 0400 0130 0466 00E2
LDU1: 00A2 05B3 0BFB 06B9 0033 016C 062C 00F0
LDU1: 082F 05F2 0161 0011 0400 0309 04FA 0060
LDU1: 08ED 019A 0732 065C 07FF 04AE 04C2 00BF
LDU1: 08EC 0358 0777 02A4 07FF 0649 05F8 009D
LDU1: 08AC 016C 01FE 0ED0 07FF 073A 05C6 00BA
LDU1: 0874 05F0 01DD 0168 07FF 0426 057C 0031
LDU1: 0874 04F6 07DD 0736 07FF 0403 01E6 00F8
LDU1: 082C 05B4 009F 0AC2 07FF 0785 06A0 00CD
```

Cyberspectrum: Bay Area Software Defined Radio

Change photo

Santa Clara, CA

Founded Nov 5, 2014

About us...

SDR Enthusiasts 234
Group reviews 3
Upcoming Meetups 1
Past Meetups 6
Our calendar

Welcome!

+ SCHEDULE A NEW MEETUP

Upcoming 1 | Past | Calendar

Cyberspectrum #6: San Francisco

Noisebridge
2169 Mission St, San Francisco, CA (map)

Tentative date! More details coming soon... If you wish to present, or would like to learn about a particular topic, please get in touch!

LEARN MORE

Hosted by: Balint Seeber (Organizer)

Wed Apr 29
6:30 PM
✓ I'M GOING
3 going
0 comments

Recent Meetups

What's new

✓ NEW RSVP

Chris Kuethe RSVPed Yes for Cyberspectrum #6: San Francisco
3 days ago

NEW MEMBER
Jabi Aguirre joined
3 days ago

NEW MEMBER

Phil joined
3 days ago

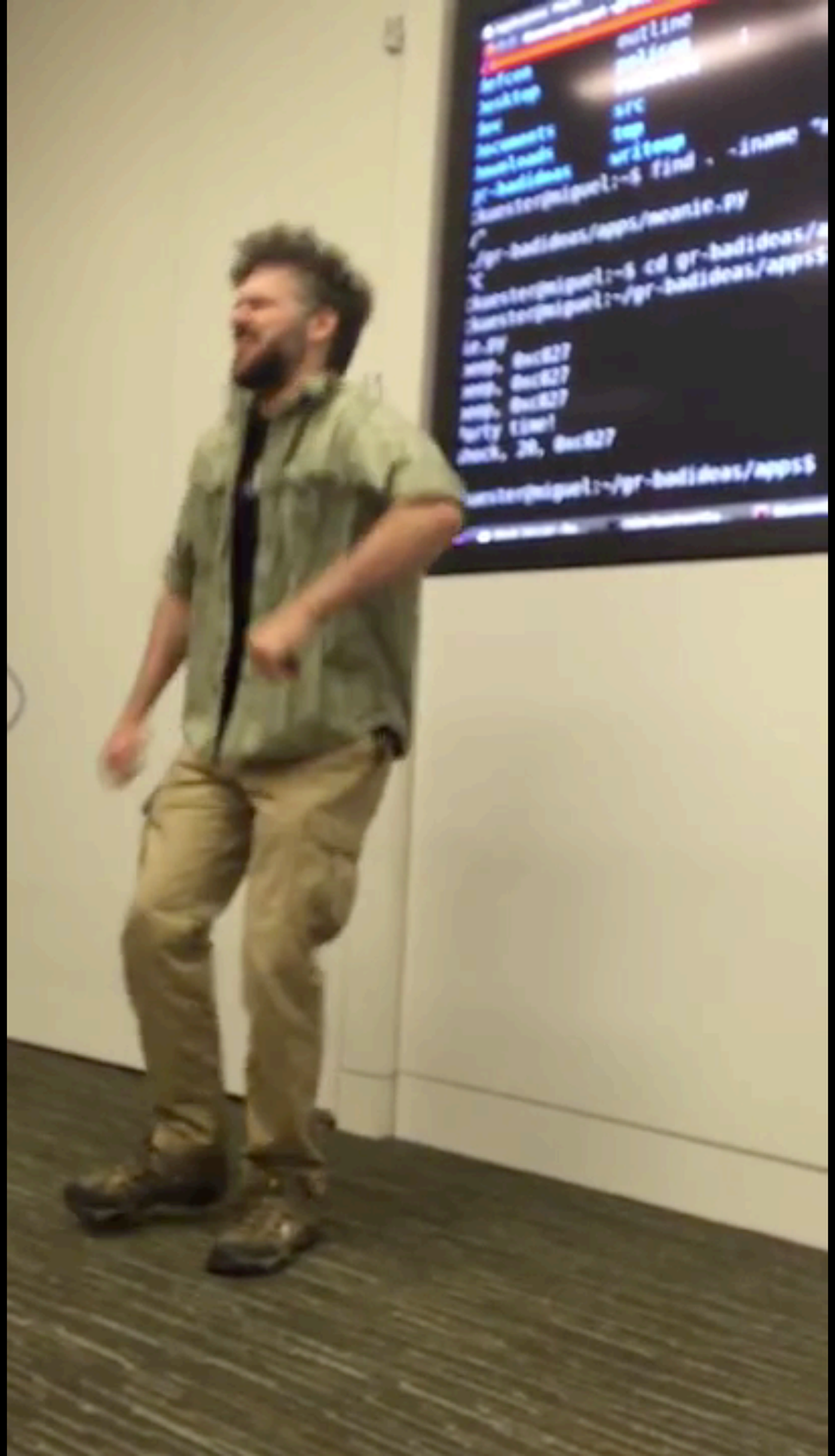
NEW MEMBER

Bene joined
4 days ago

✓ NEW RSVP

Samant Kumar RSVPed Yes for Cyberspectrum #6: San Francisco


Cyberspectrum #6


outline
src
tmp
writeup
~$ find . -iname "*
./gr-badideas/apps/weanie.py
~$ cd gr-badideas/apps
~/gr-badideas/apps$
0xc827
0xc827
0xc827
Party time!
duck, 20, 0xc827
~/gr-badideas/apps$

Thank you!

You can't protect what you can't see.

@spenchdotnet

balint@bastille.io

GitHub: balint256

GitHub: RFStorm

Bastille