



Hacking the Wireless World: Software Defined Radio Exploits

Balint Seeber
Director of Vulnerability Research

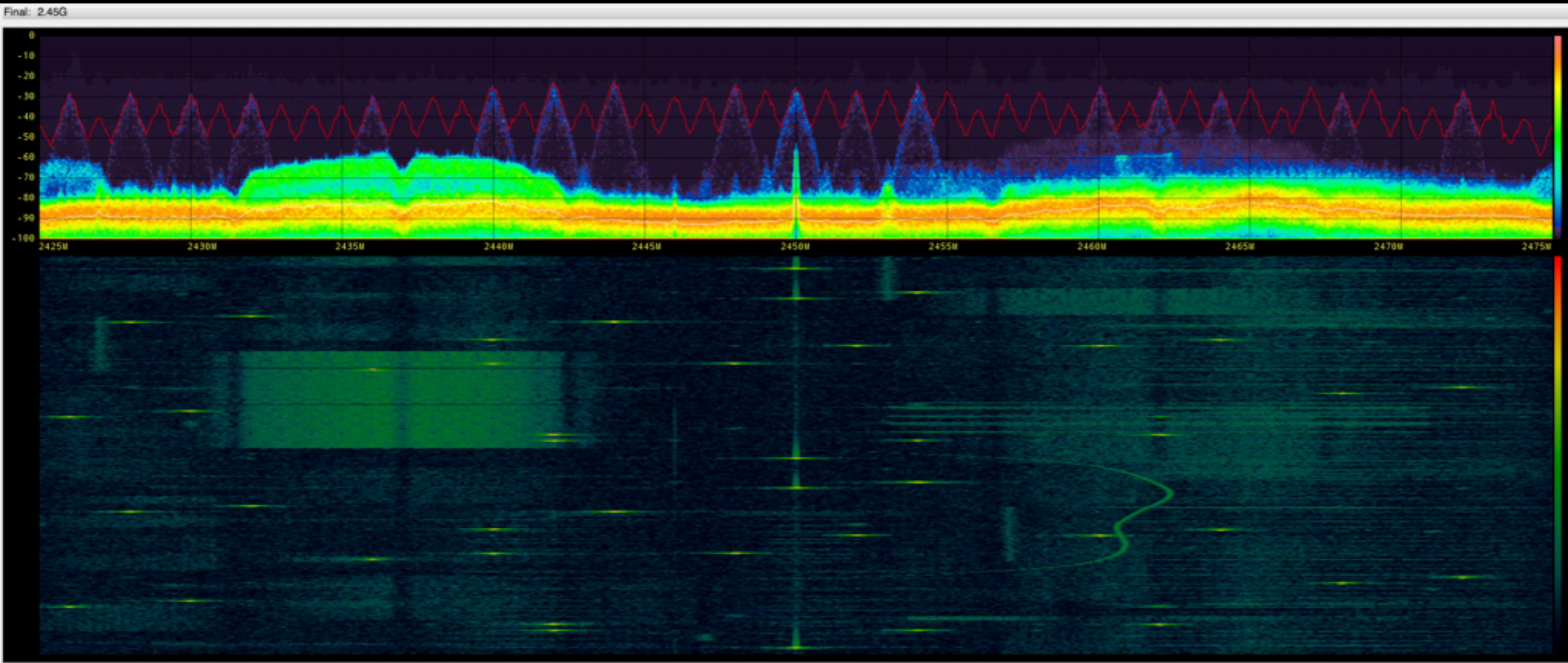
Bastille

What are we looking at?

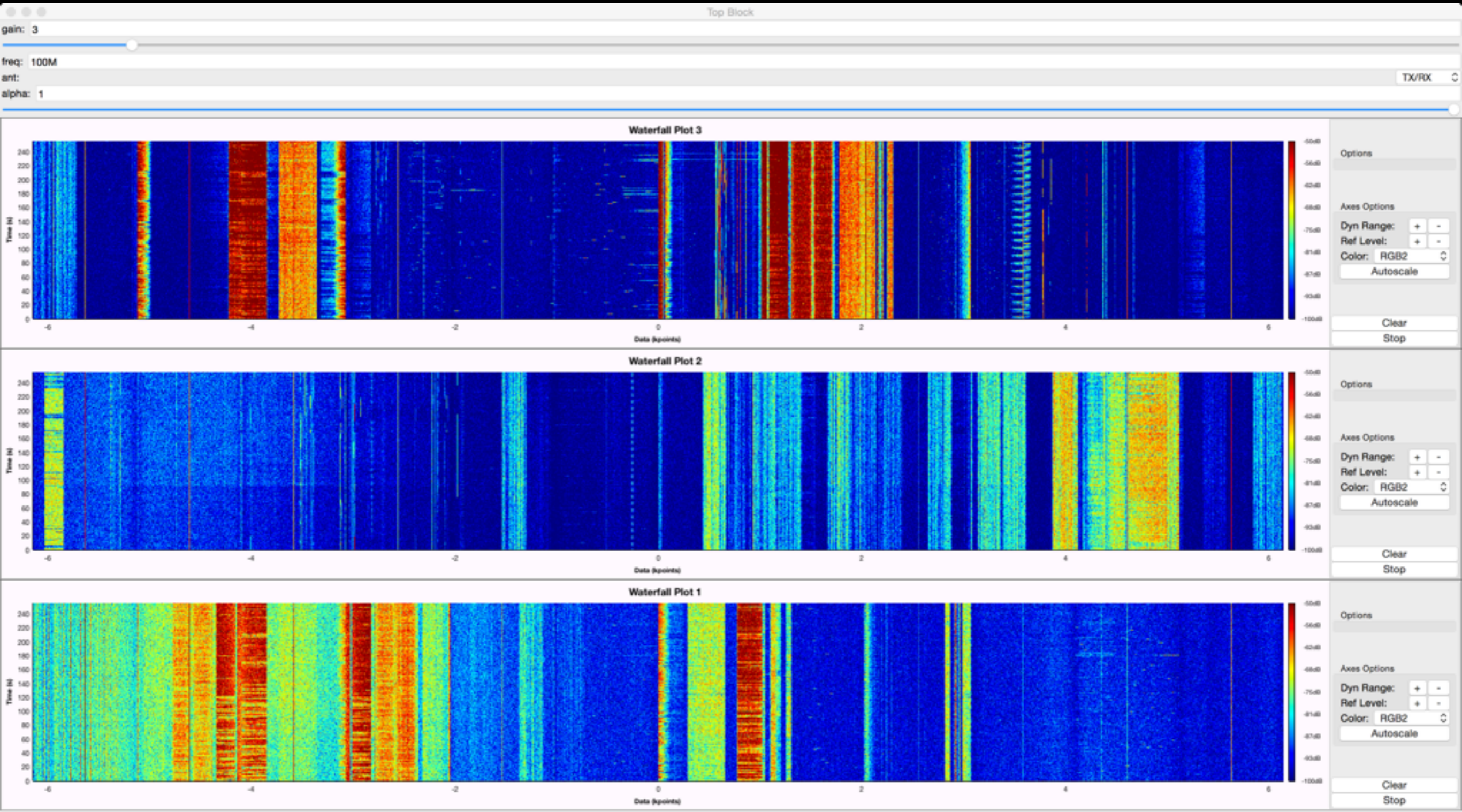
Overview

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

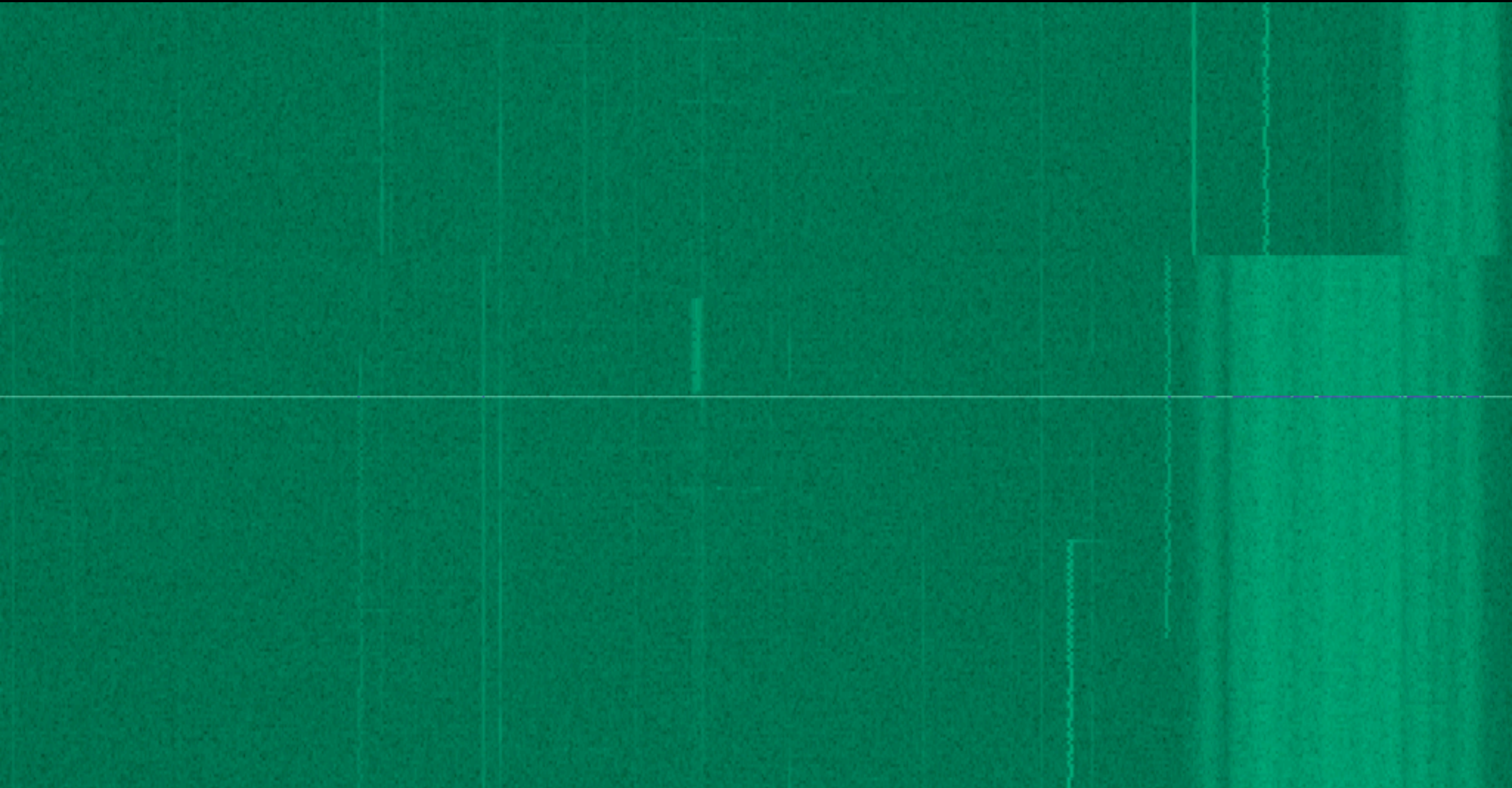
2.4 GHz ISM Band Activity



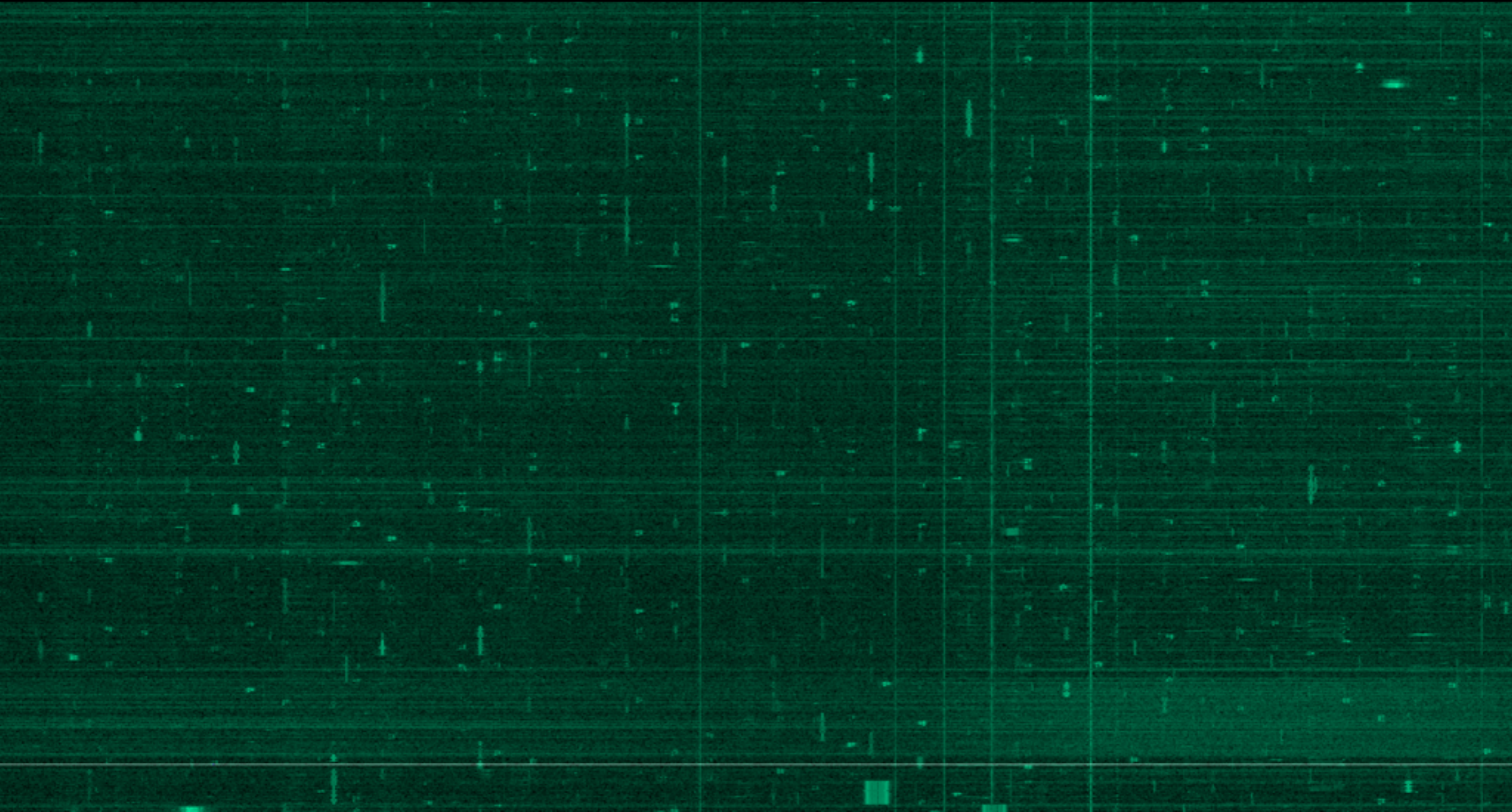
Wideband Activity: 50 MHz - 1.25 GHz



915 MHz ISM Band Activity

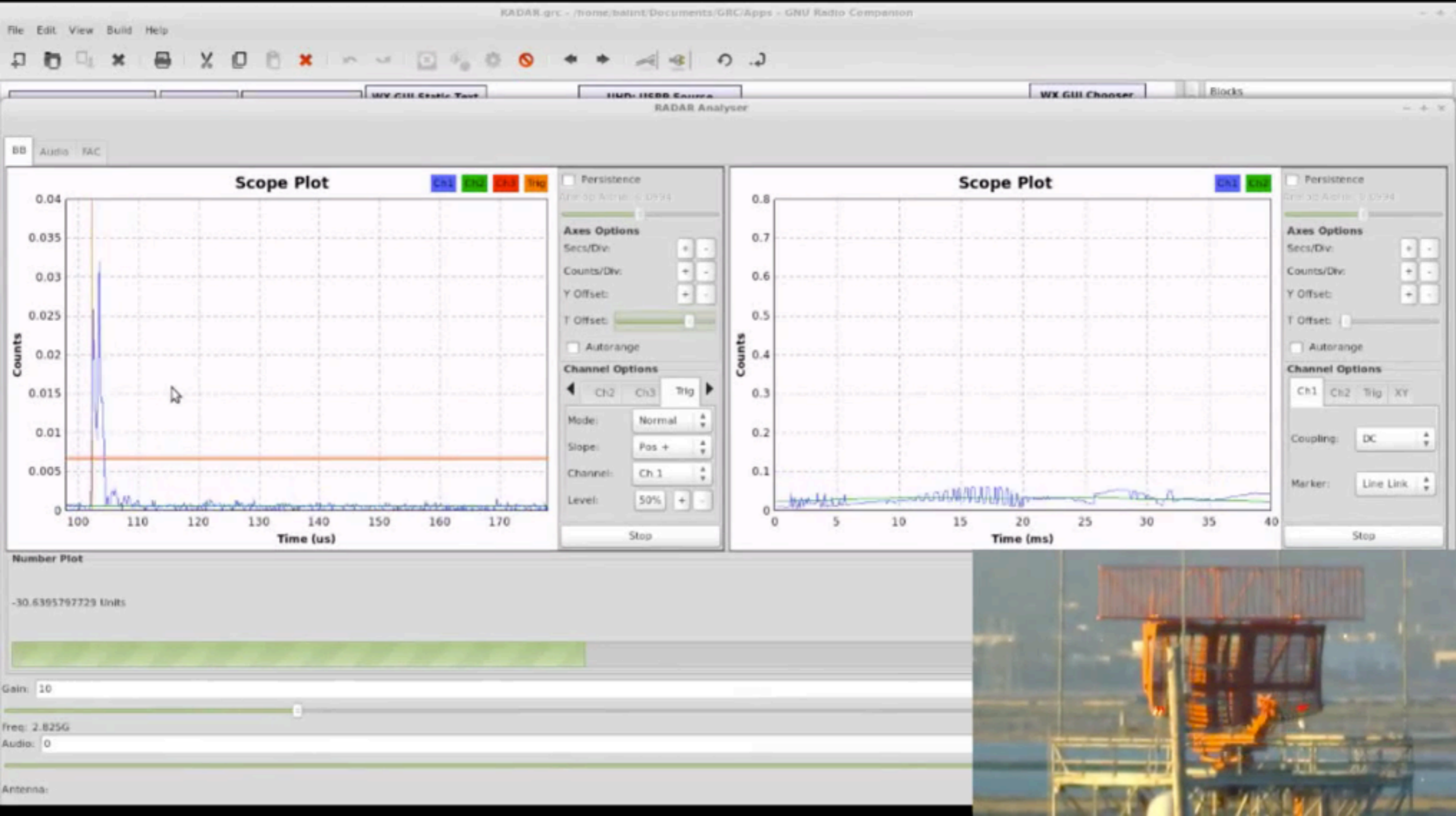


915 MHz ISM Band Activity



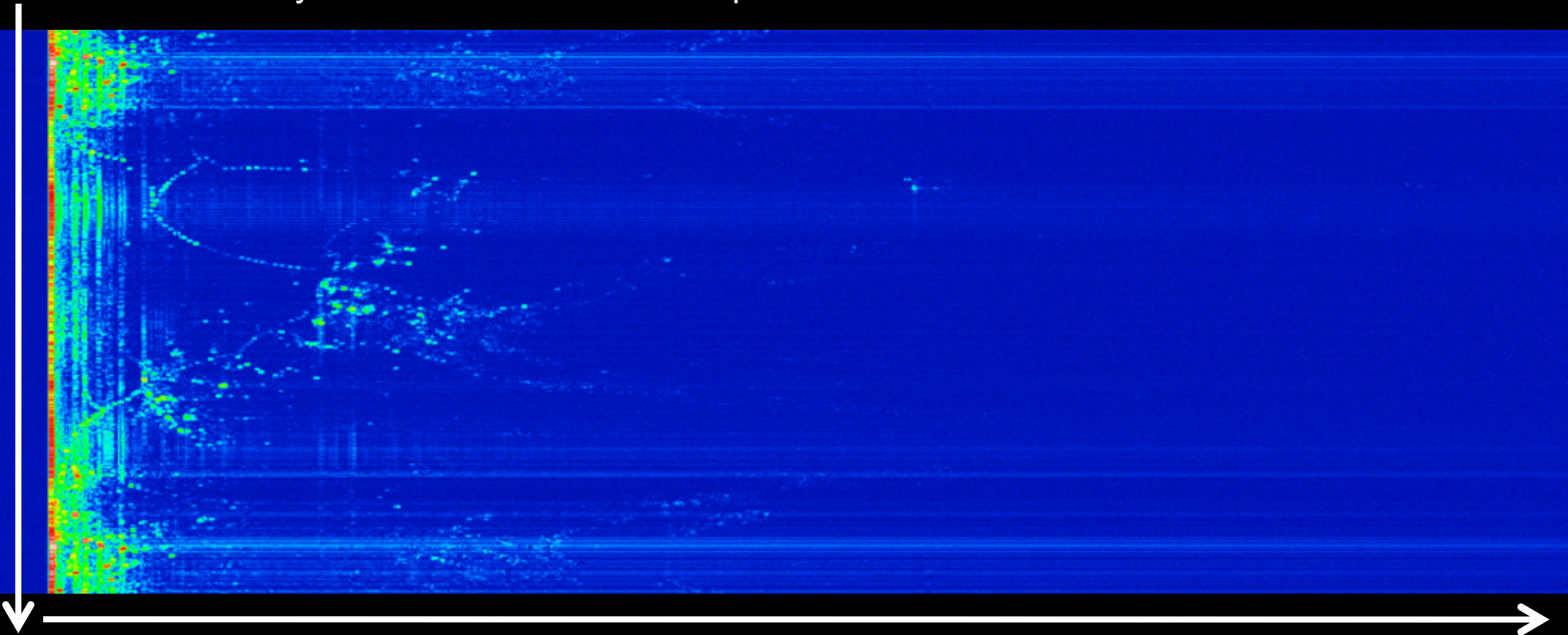
Aviation

Primary Surveillance RADAR (PSR)



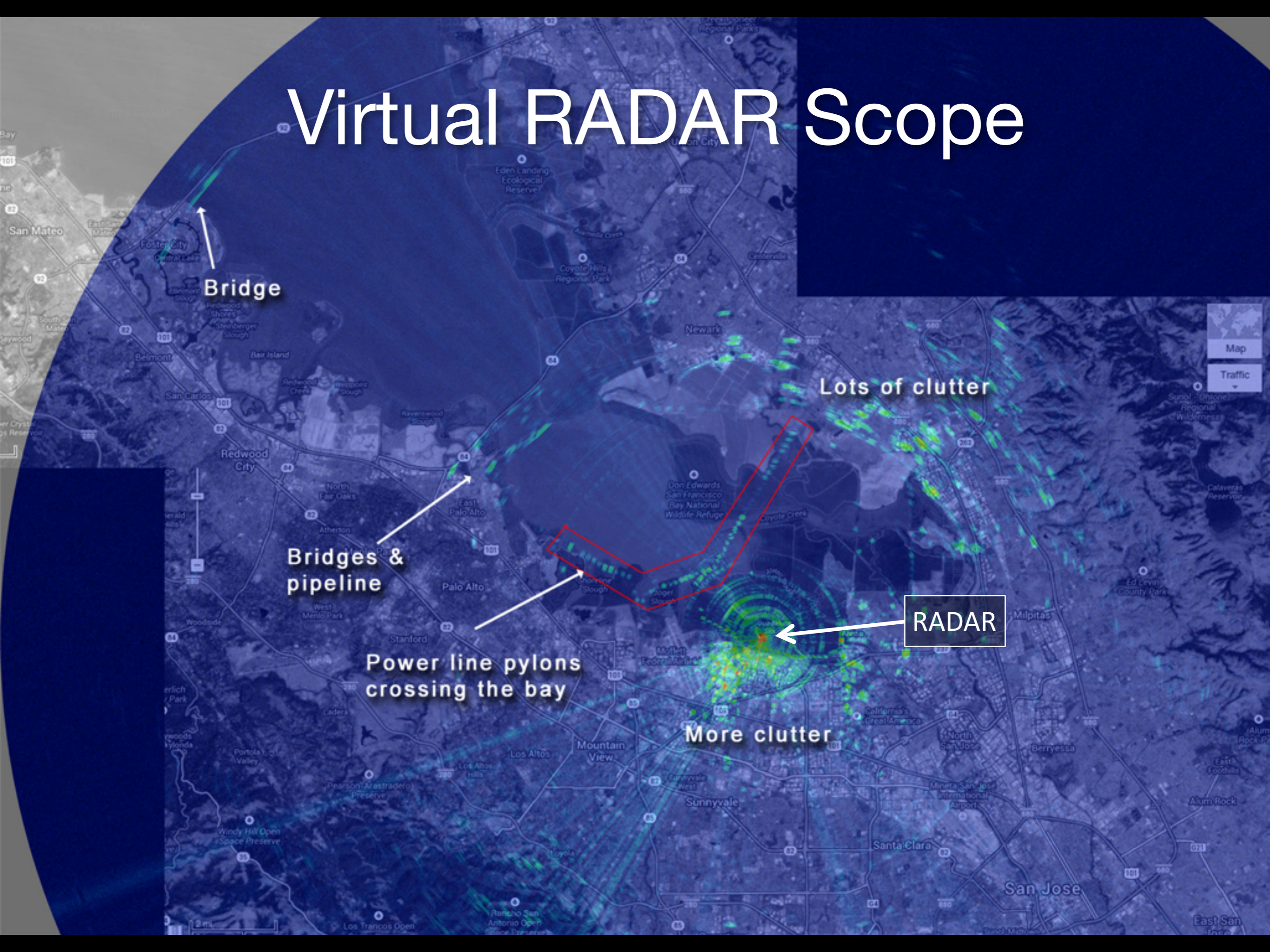
Raw RADAR Return Plot

Each scanline is synchronised to an emitted pulse



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

Virtual RADAR Scope



Bridge

Bridges & pipeline

Power line pylons crossing the bay

Lots of clutter

RADAR

More clutter



TCAS

Xpndr

High gain
SATCOM

Low-gain
VHF

HF →

DME

ADF

EPIRB

Marker

RADAR Altimeter

VHF

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

0:51 PM, local 10
0:51 PM, local 10
0:51 PM, local 10

10⁴
10³
10²
10¹
10⁰
000



- Centre
- IFR
- VFR
- Airframe Info

Yahoo Satellite

View information:

Map zoom: 14
Map centre:
37.610287905033
-122.36915588378

Mouse:
37.603896254459
-122.36598014831

Click:
37.604712240434
-122.37104415893

Save Image...

Takeoff at SFO (Cockpit View)

7/11/2013 - 8:30 pm

Welcome to Aviation Mapper

Click here for info, feedback and to share - If you like this, let me know.

I need to find a new receiver site near the airport ASAP - please help!

spen.ch.net

23:19:26 AEST
06:19:26 UTC
Modes: OK
ACARS: Terminated

Auto Balloons
 Trails
Trails need more CPU



Idnt: VRD034
Alt: -50 ft
Head: 28
Spd: 29 knt
Vert:

VRD034

13 ft

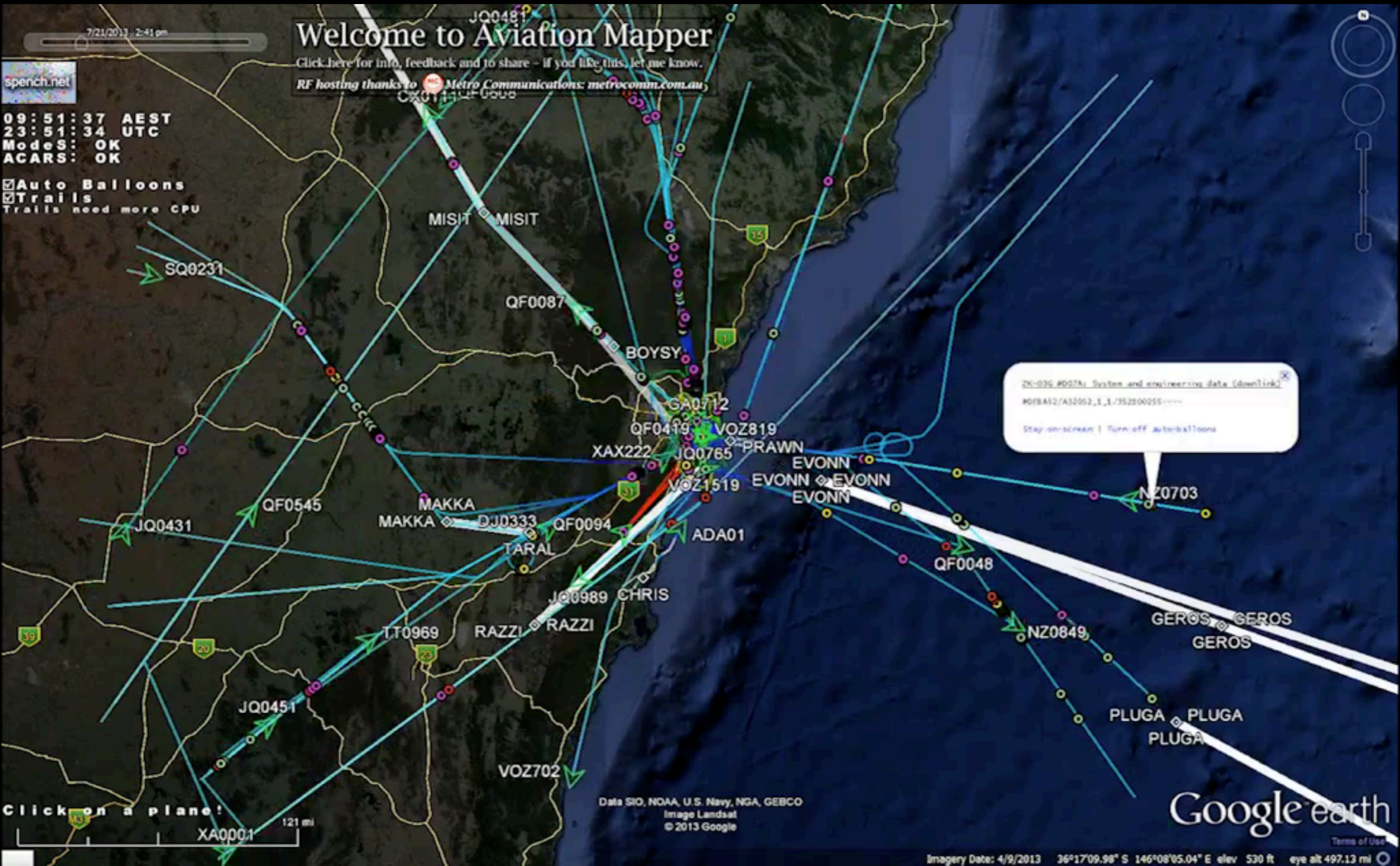
Image Landsat

© 2013 Google

Google earth

37°36'28.34" N 122°22'49.76" W elev 12 ft eye alt 31 ft

Combined Mode S & ACARS



'Engineering' Status Messages over ACARS

The screenshot displays the Aviation Mapper interface. At the top left, a timeline shows the date 4/13/2012. A search bar contains 'spench.net'. The status bar indicates 'Mode S: OK' and 'ACARS: OK'. The main map shows a coastal region of Australia with several airports marked: BANDA, CORKY, BULGA, PRAWN, PRAWN, and RAZZI. A white information box is open over the PRAWN airport, displaying the following ACARS message:

```
LV-ZRA #C71C: System and engineering data (downlink)
#CFBAULT,212606;2128455MAINTENANCE STATUS      CRG VENT,213006/FR212300VC      X2
.....GALY LAV DUCT CLOGGED,HARD,,ECR
```

Below the message box, a text overlay asks: "H1 'System and engineering data' regarding the (failure of) toilets?". At the bottom left, a scale bar indicates "Click on a plane" with a distance of 181 km. The bottom right corner shows the URL <http://maps.spench.net/aviation/> and the Google Earth logo. The bottom status bar displays coordinates: 33°51'01.32" S 151°24'46.54" E elev -60 m and an eye alt of 786.43 km.

Waypoints Transmitted over ACARS

4/15/2012 - 9:45 pm
4/14/2012 4/15/2012

Welcome to Aviation Mapper

Click here for info, feedback and to share - if you like this, let me know.

I need to find a new receiver site near the airport ASAP - please help!

<http://maps.spench.net/aviation/>

spench.net

21:02:32 AEST
11:02:32 UTC
Mode S: Terminated
ACARS: OK

International & cross-country flight paths sent as flight plans using IFR waypoints

Click on a plane!

2709 km

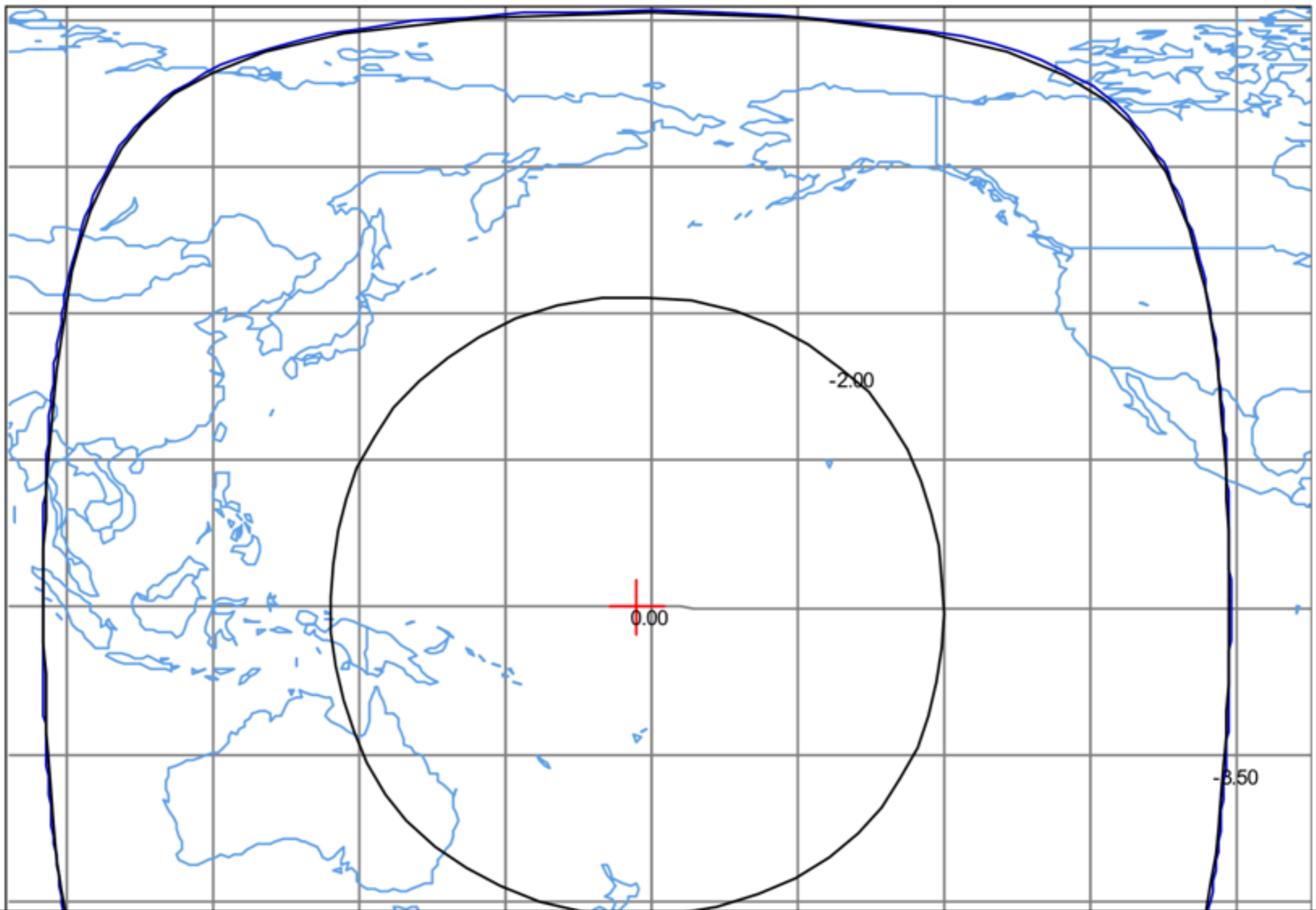
Data SIO, NOAA, U.S. Navy, NGA, GEBCO
© 2012 Cnes/Spot Image
© 2012 Whereis® Sensis Pty Ltd

3°56'15.16" N 93°48'49.69" E elev -1305 m

Google earth

Terms of Use

Eye alt 5231.14 km



[http://licensing.fcc.gov/cgi-bin/ws.exe/prod/ib/forms/
attachment_menu.hts?](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](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

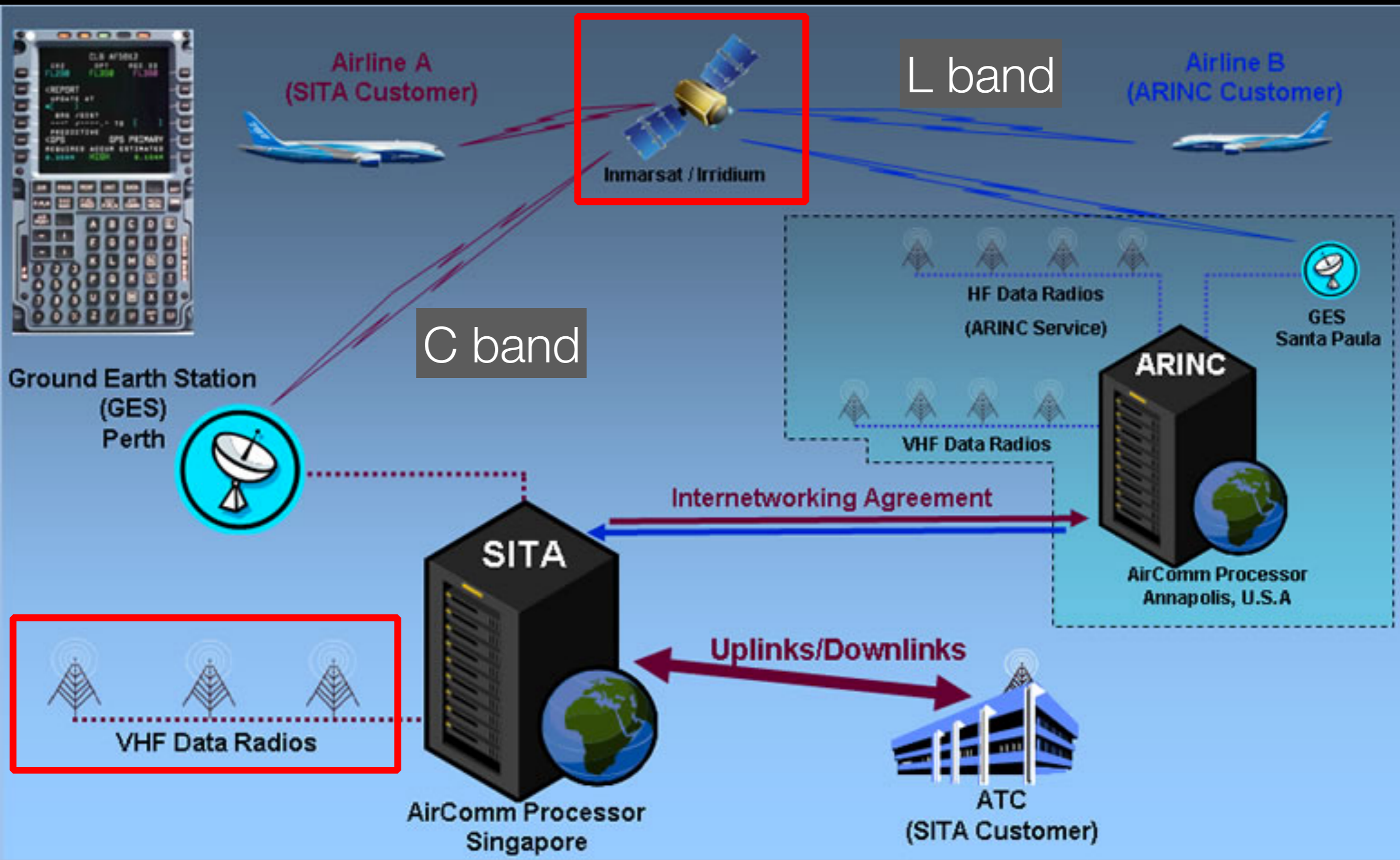


INMARSAT Geostationary Birds

Satellite Fleet (end of 2016)

Geostationary orbit: 35,786km

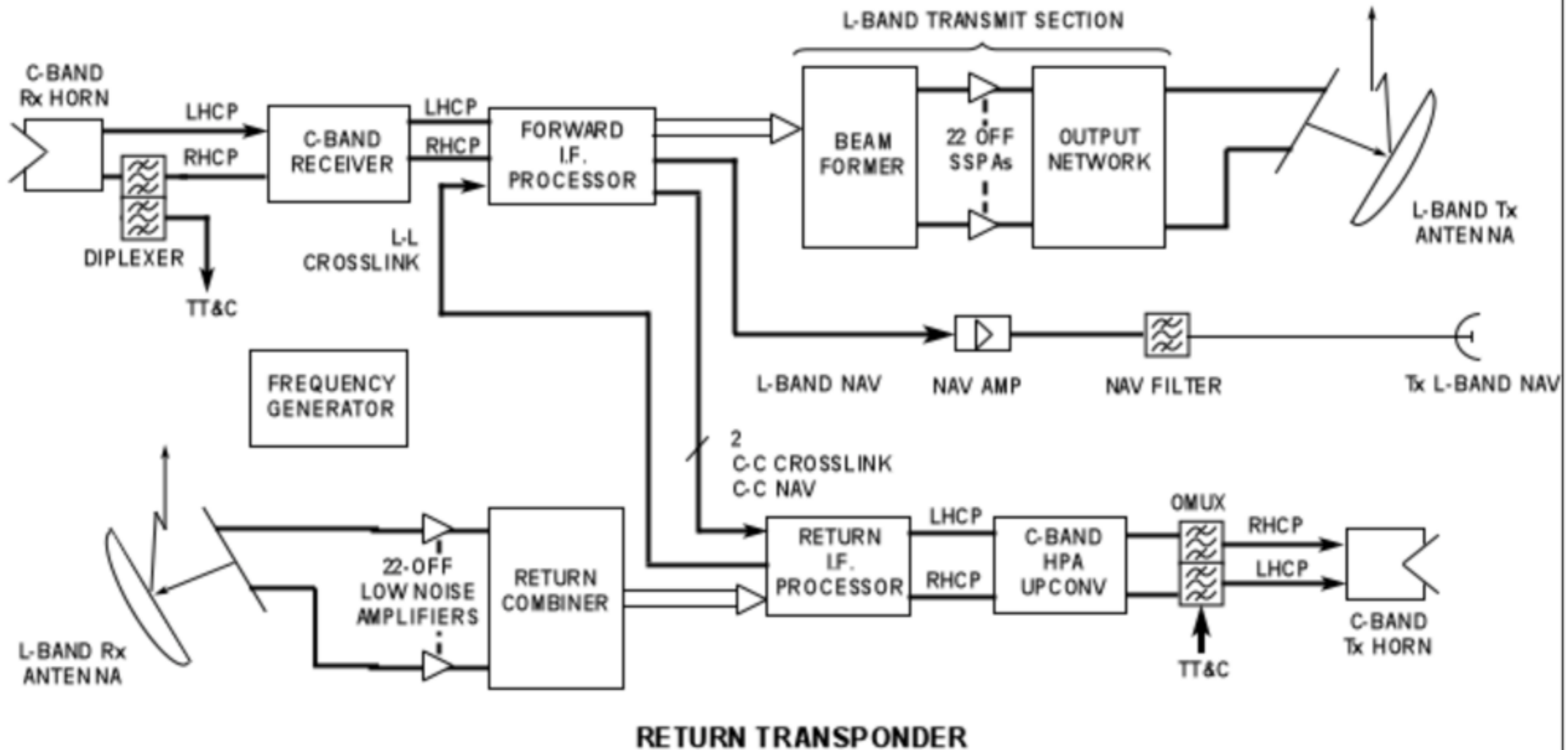




INMARSAT 'Bent Pipe' Transponders

3 & 6 GHz

1.5-1.6 GHz





Bandpass Filter 1560MHz, 120MHz BW

LNA - Gain 14.8dB, NF 0.46dB

LHCP Helical Feed



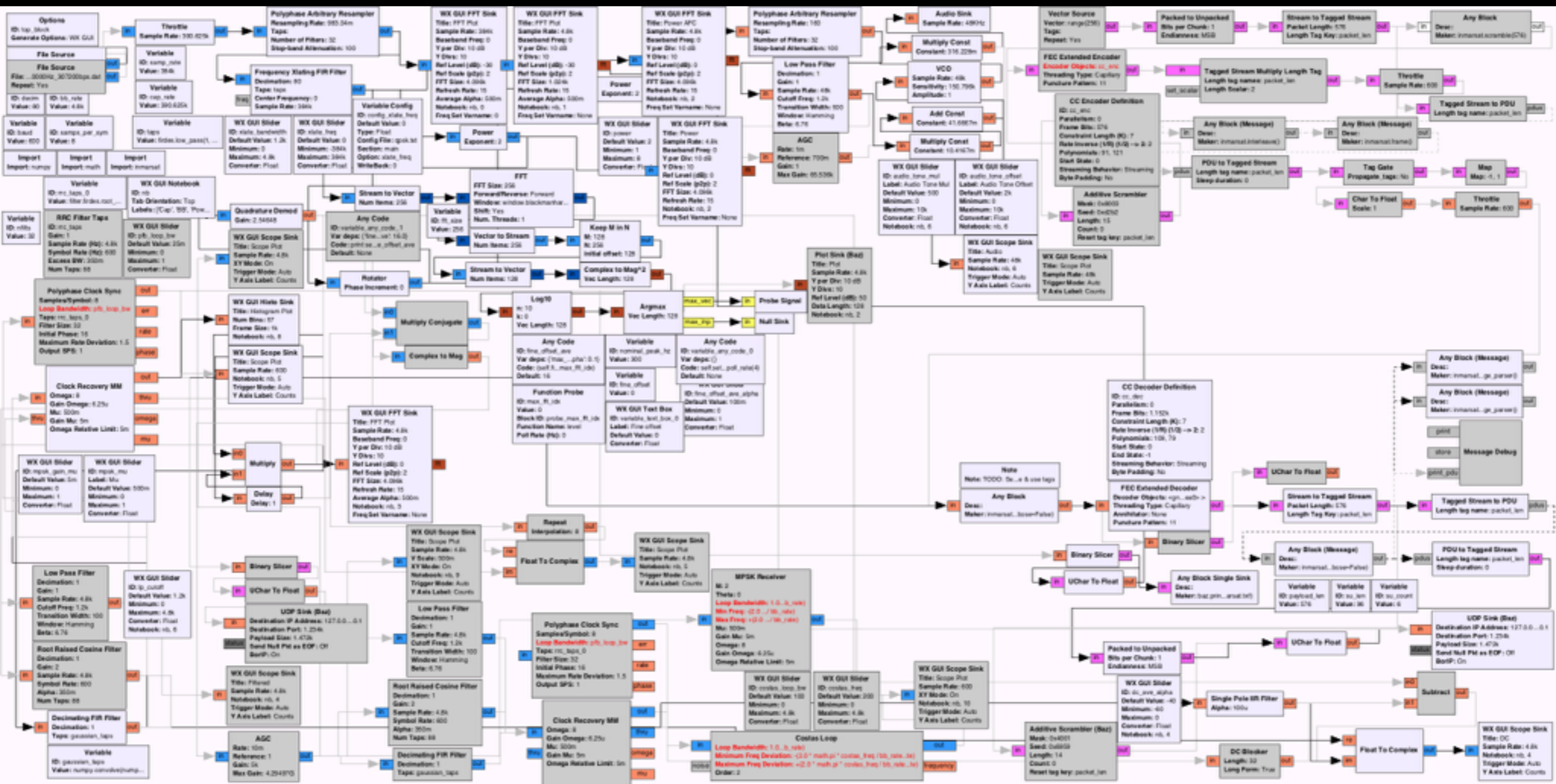


LNA - 28dB gain?, 0.8dB NF?

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

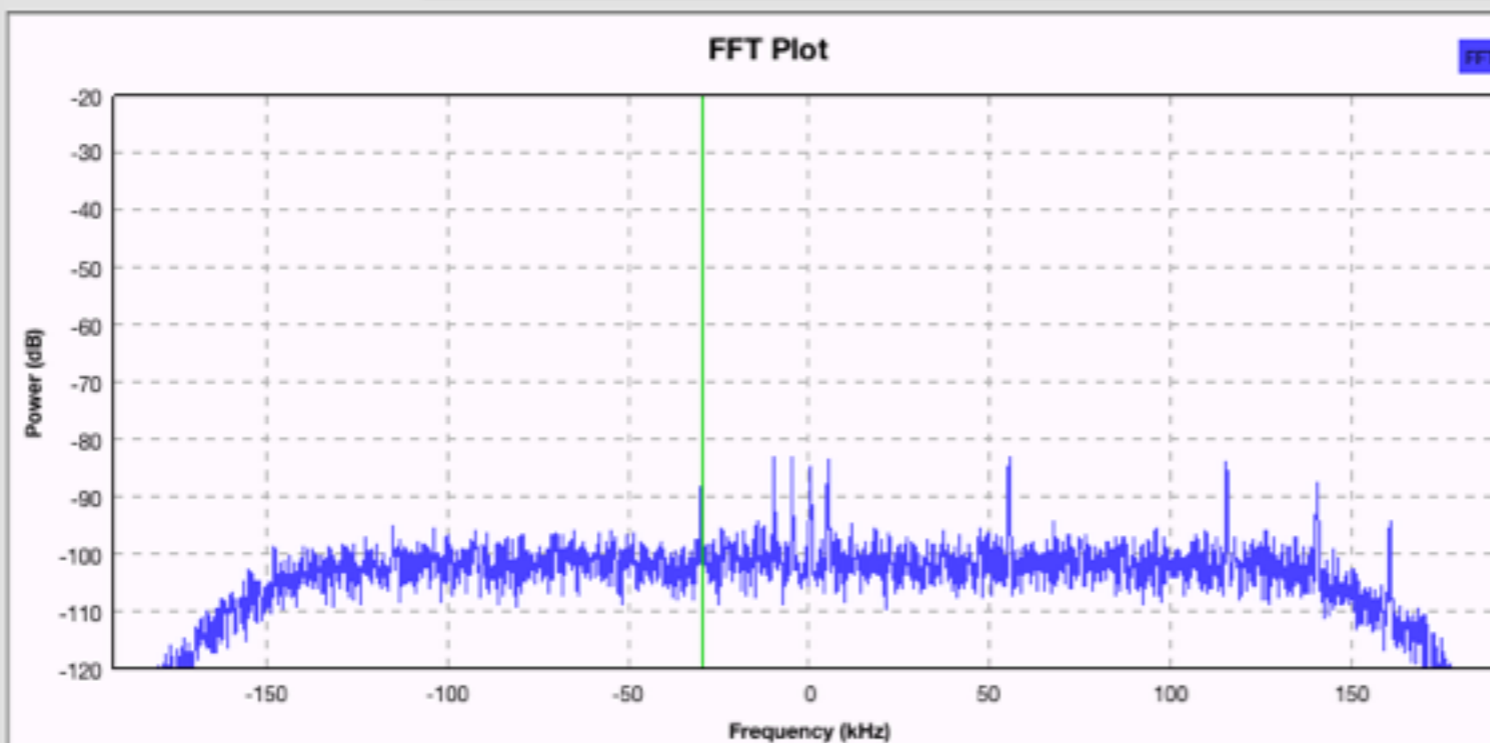
The P Channel Flowgraph so far...



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

Axis Options

dB/Div: + -

Ref Level: + -

Autoscale

Stop

Mu: 500m

m-psk_gain_mu: 5m

lp_cutoff: 1.2k

Audio Tone Offset: 2k

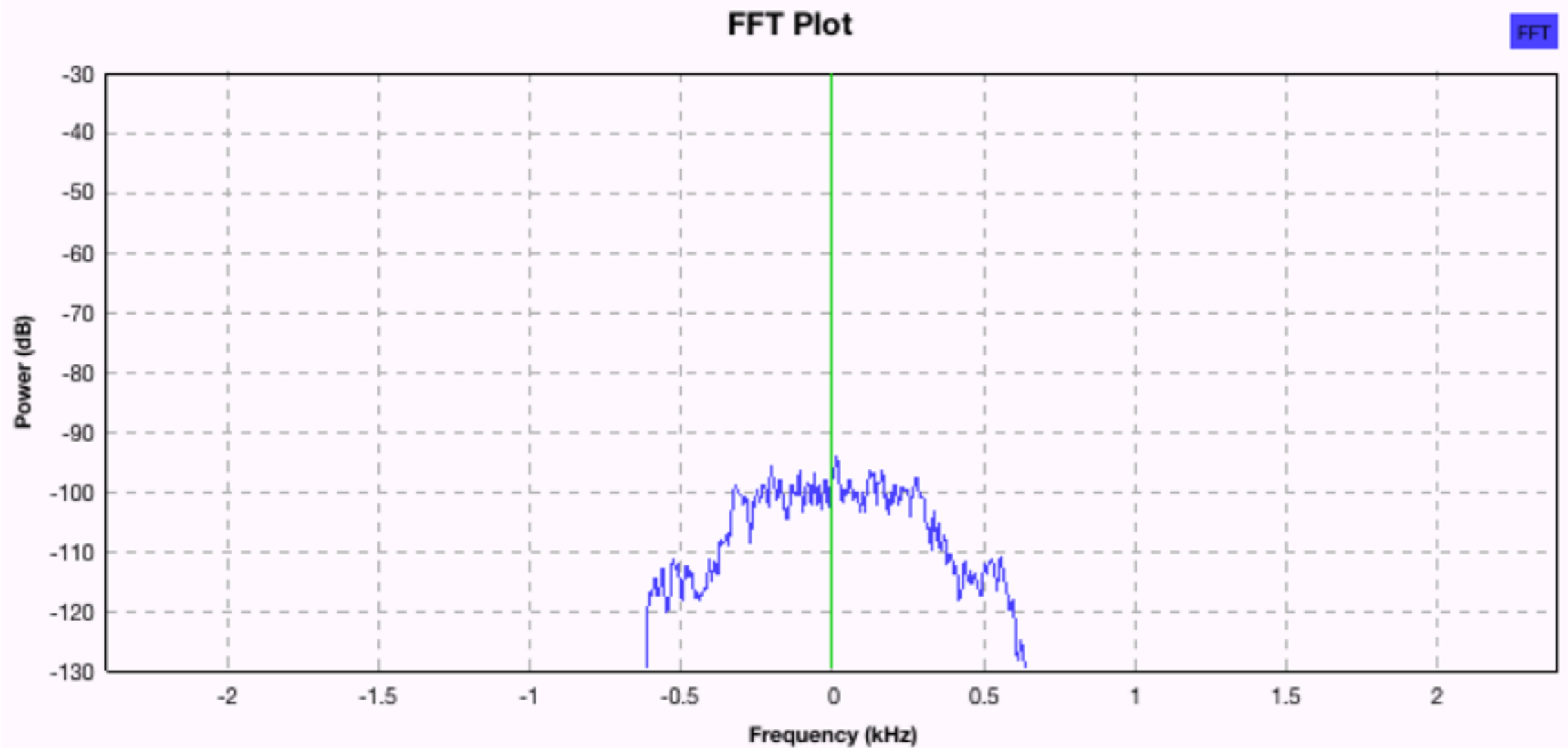
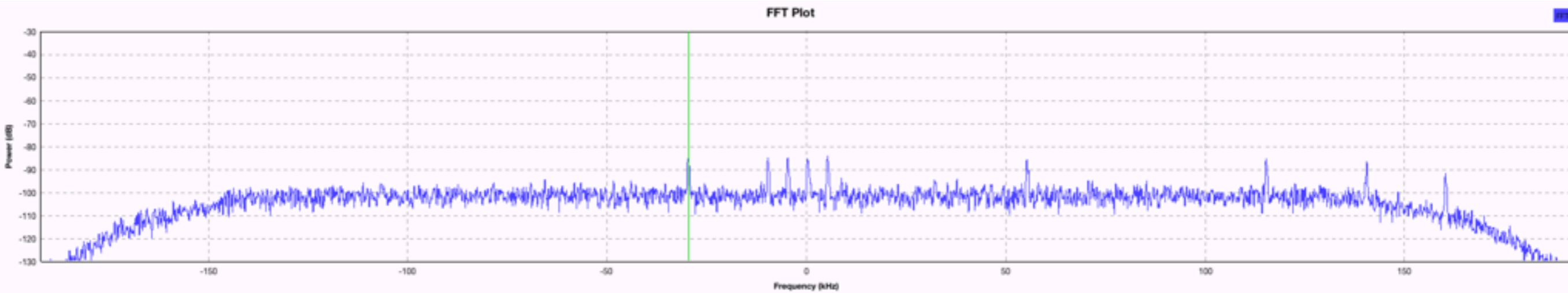
Audio Tone Mul: 500

amp: -10

xlate_bandwidth: 1.2k

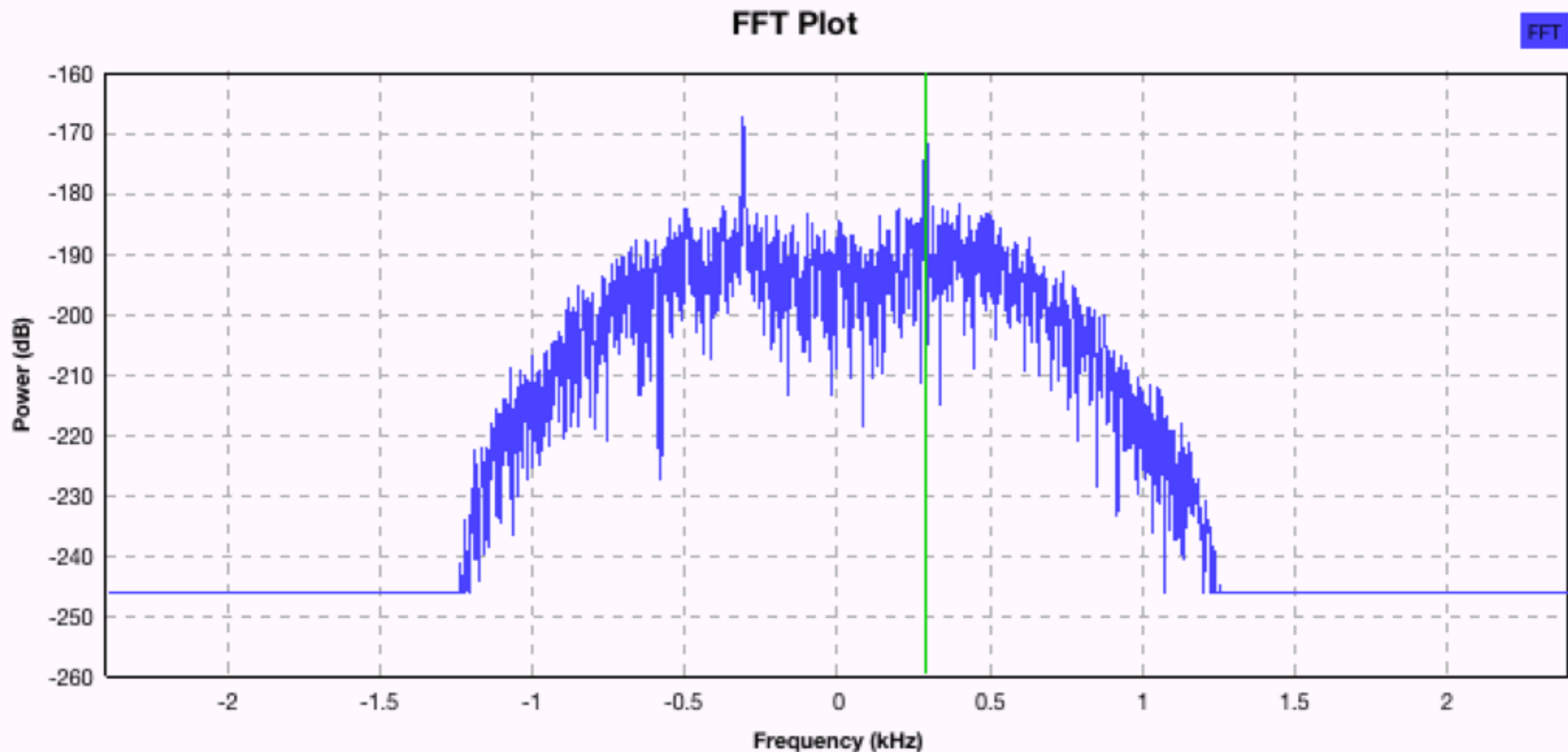
pfb_loop_bw: 25m

Channel Selection



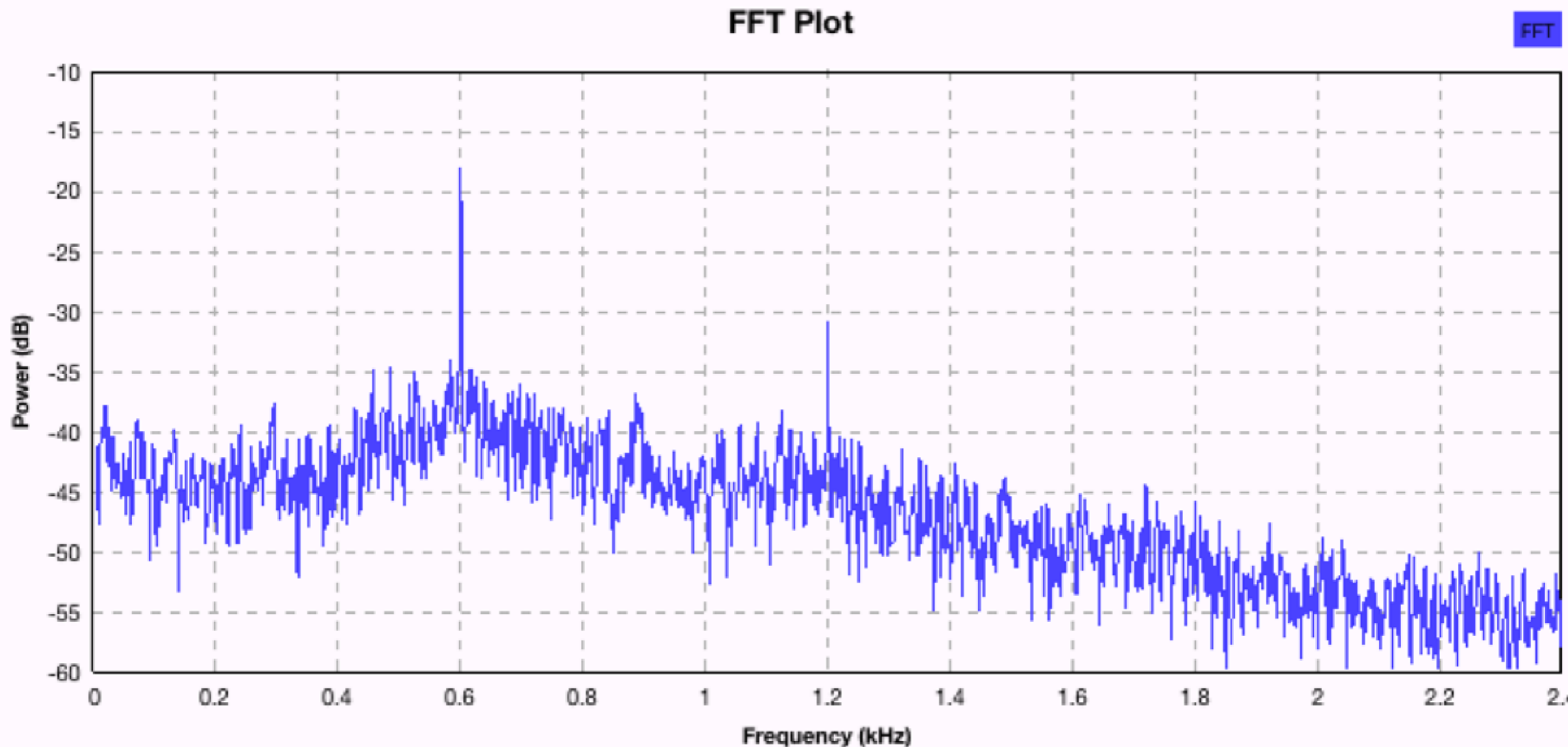
Modulation Type

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



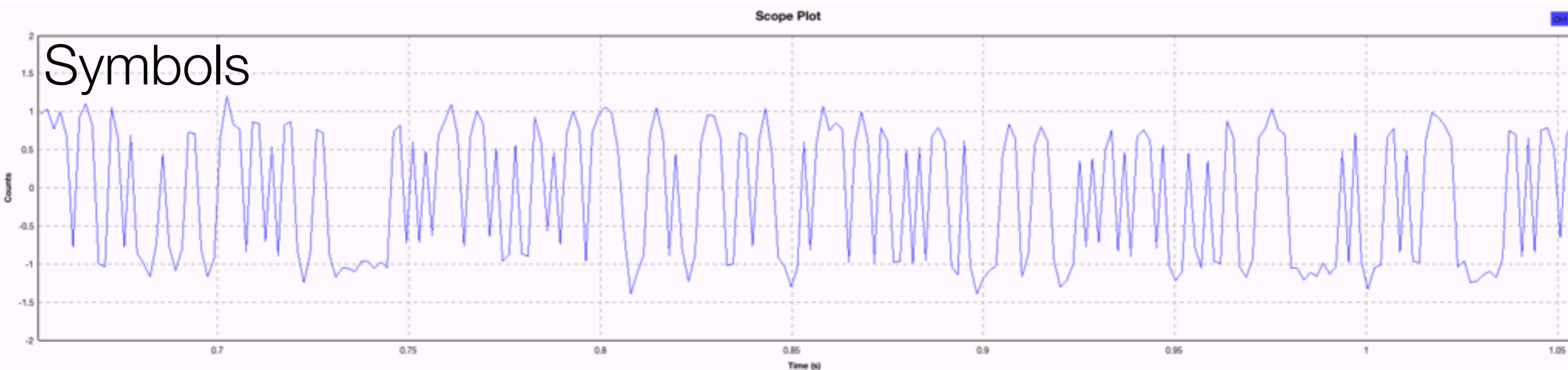
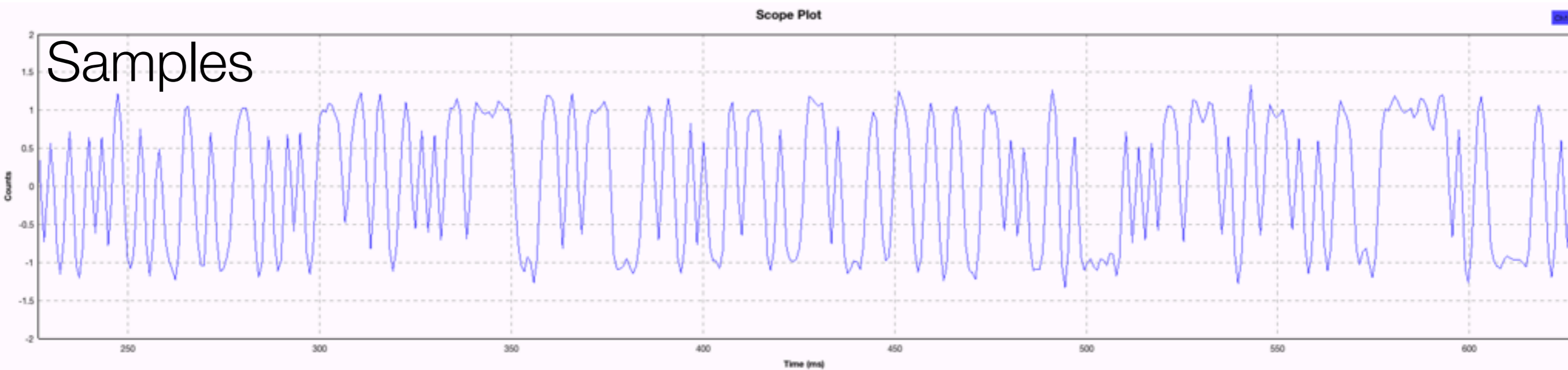
Symbol (Baud) Rate

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



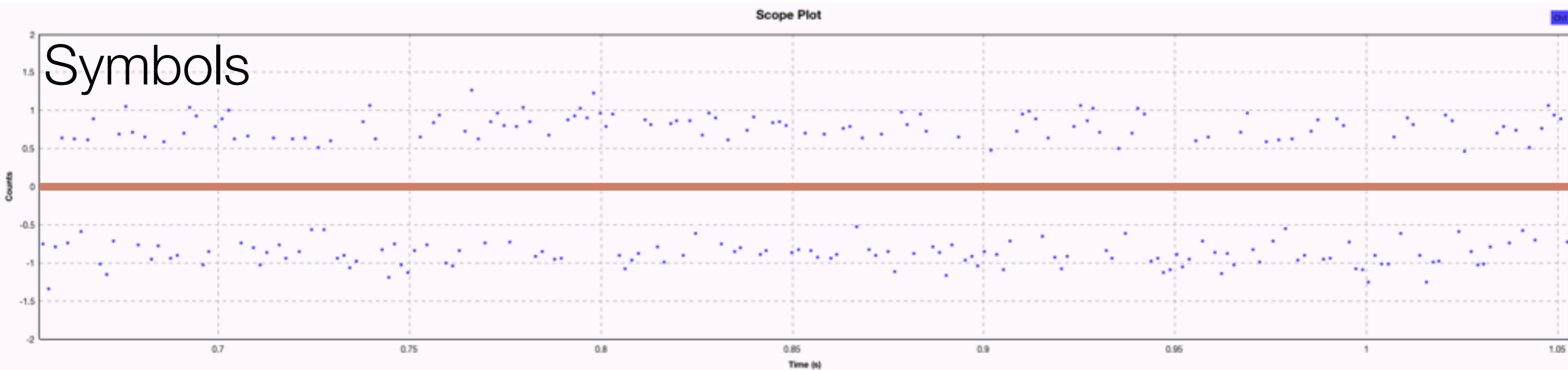
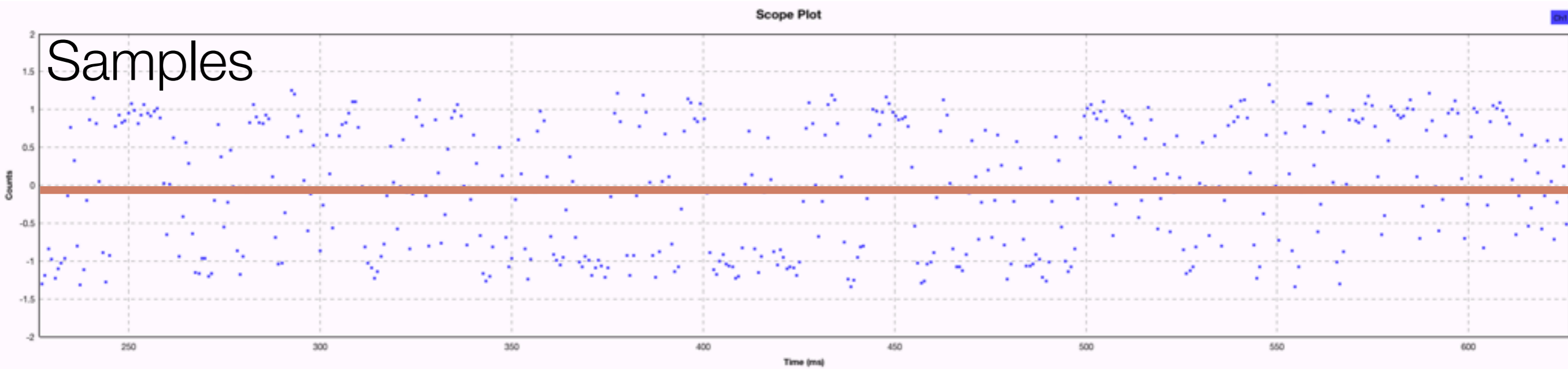
Clock Recovery

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



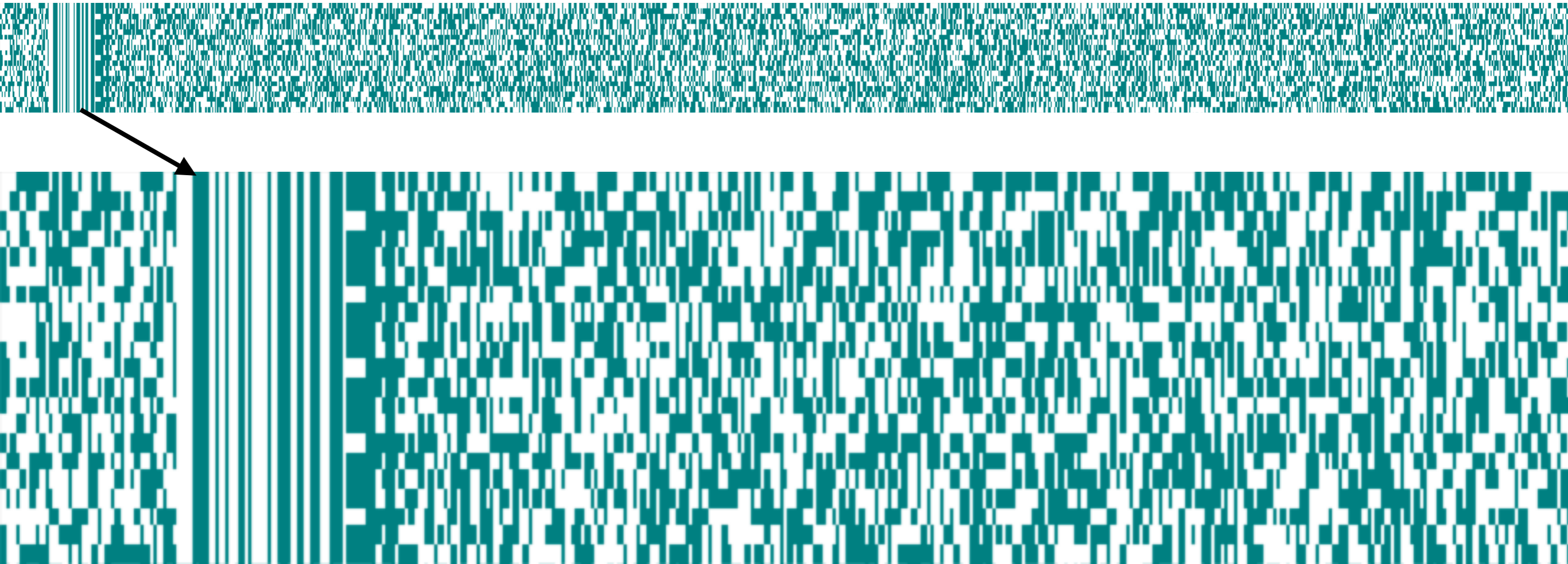
Clock Recovery Quality

- Increased separation between symbols about 0



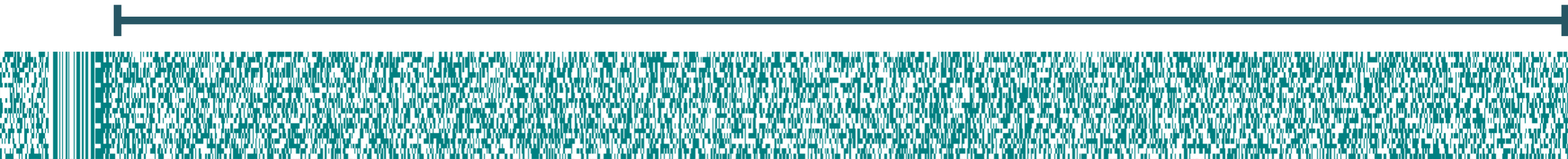
Frame Structure

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



Payload Encoding

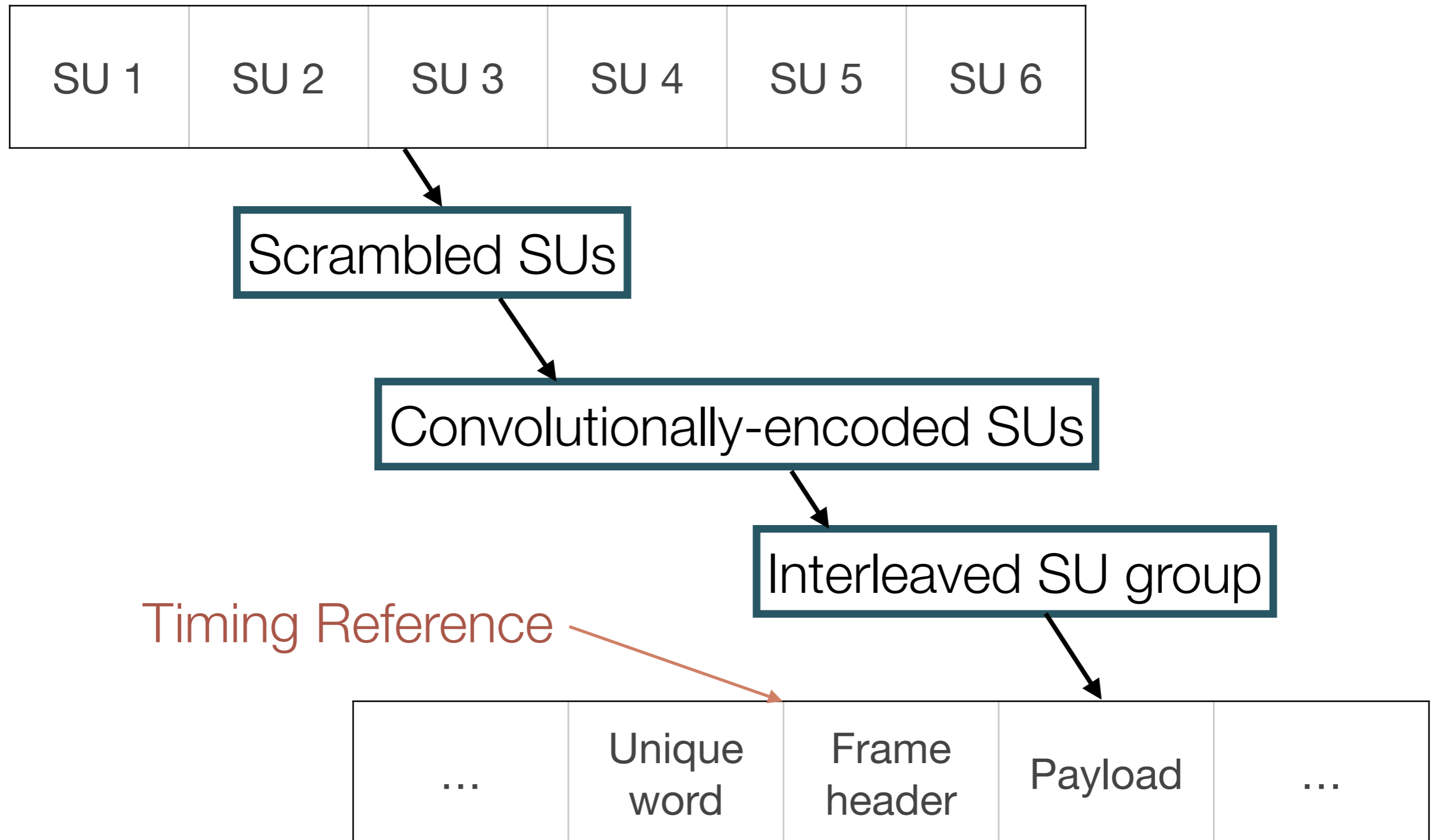
- Appears 'random'
- Generally data has gone through:
 1. Interleaving (protects against burst errors)
 2. **F**orward **E**rror **C**orrection (data redundancy)
 3. Scrambling (energy dispersal & clock recovery)
- Complex process - difficult to test each step individually



Payload Details

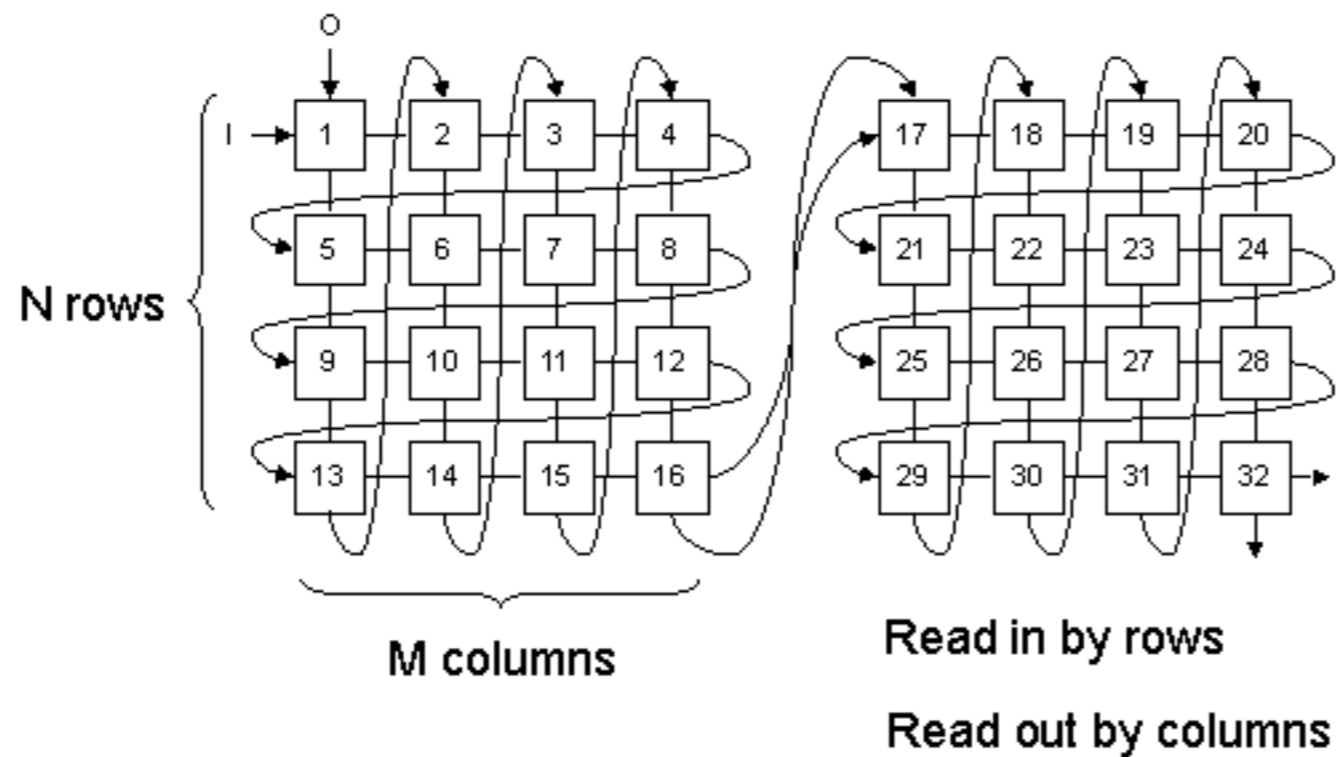
- RTFM
- Frame payload consists of multiple fixed-length Signal Units (number of SUs depends on data rate of channel, here 6 of 96 bits each)
- For transmission, the entire SU group is:
 1. scrambled
 2. 1/2-rate convolutionally encoded
 3. fed through an interleaver

Frame Details



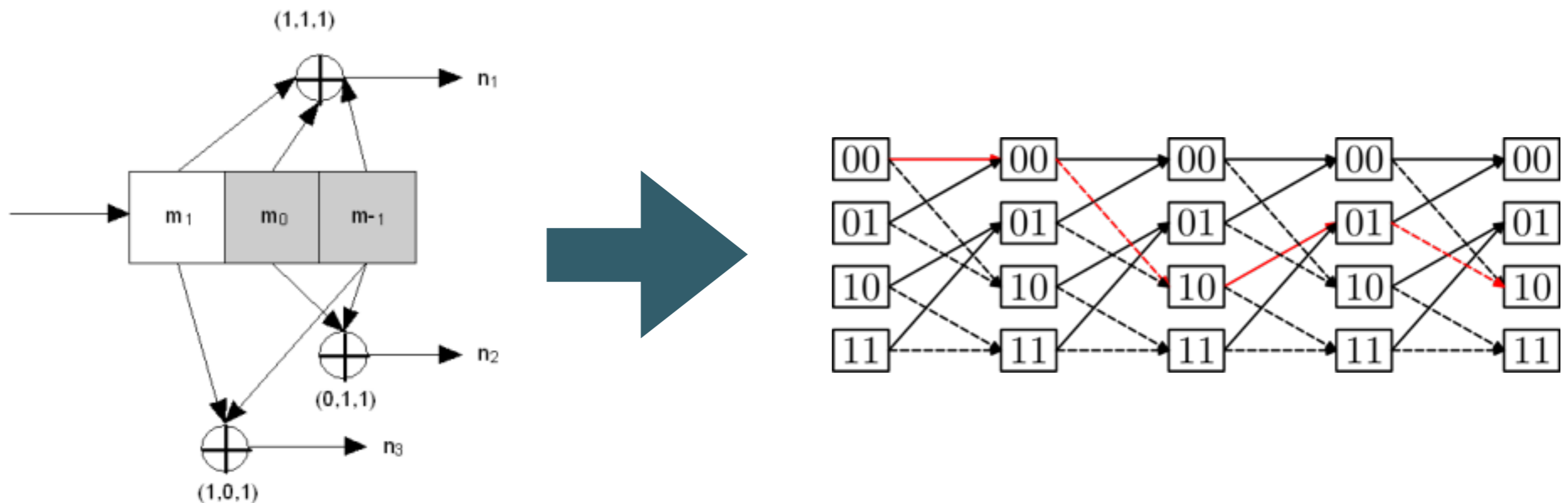
#1: De-interleaving

An example interleaver



#2: Convolutional (Viterbi) Decoding

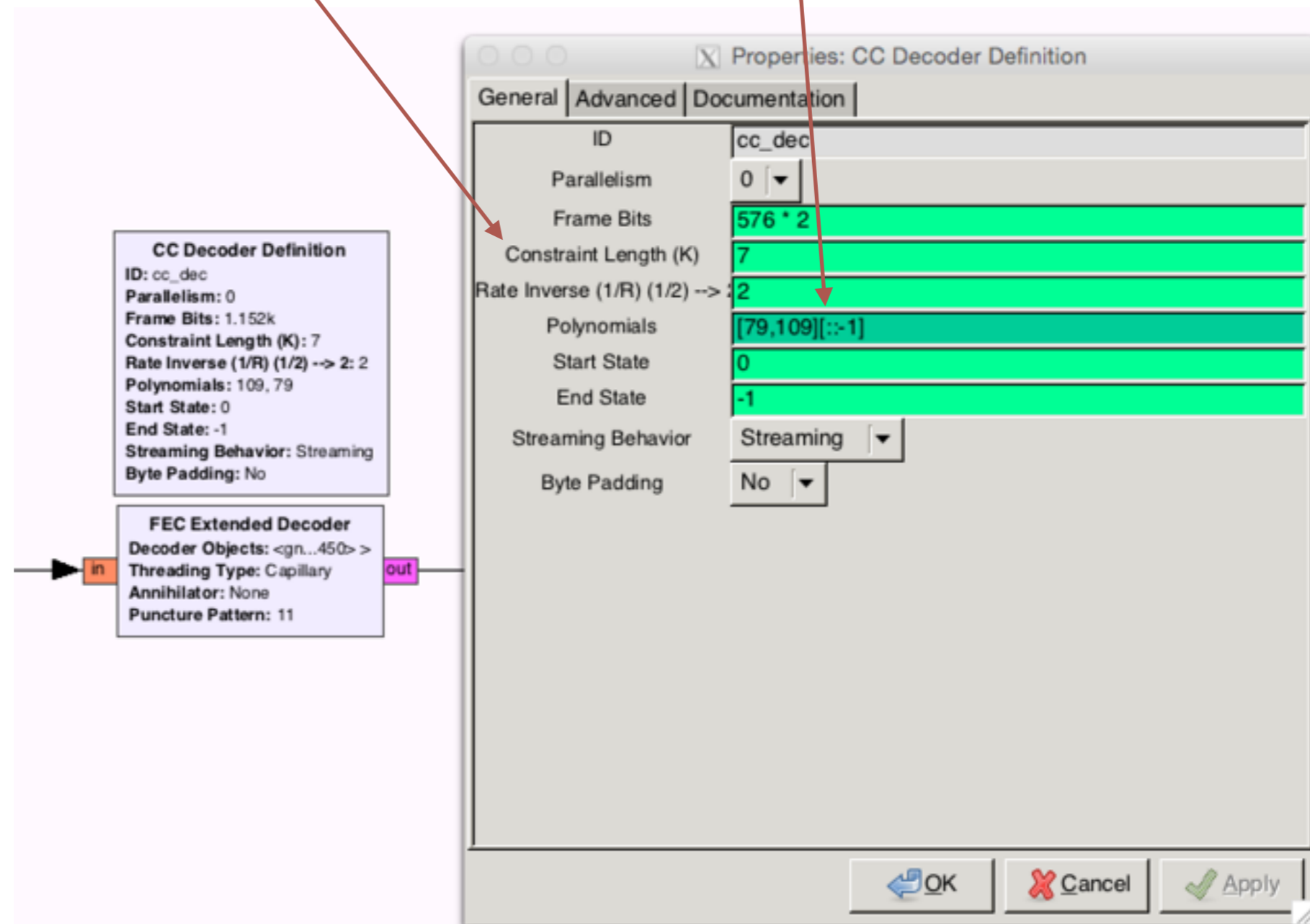
- A convolutional code adds additional bits to a stream so that a receiver can correct errors
- Given received error-prone symbols, a Viterbi decoder will output the bits that represent the most likely path through a trellis matching the convolutional code



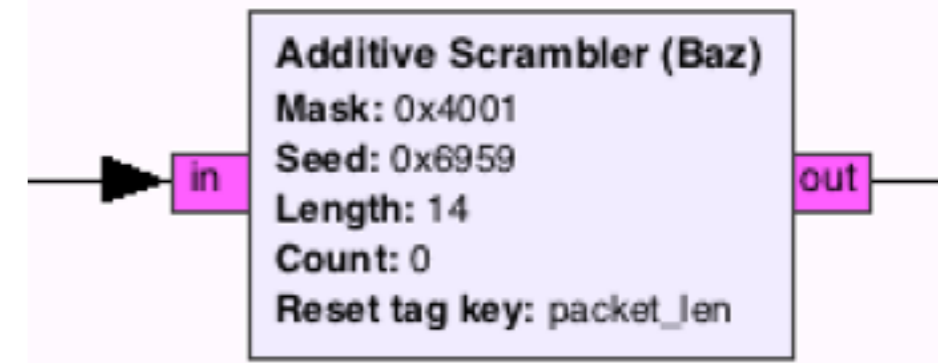
https://en.wikipedia.org/wiki/Convolutional_code

#2: Viterbi Decoder

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

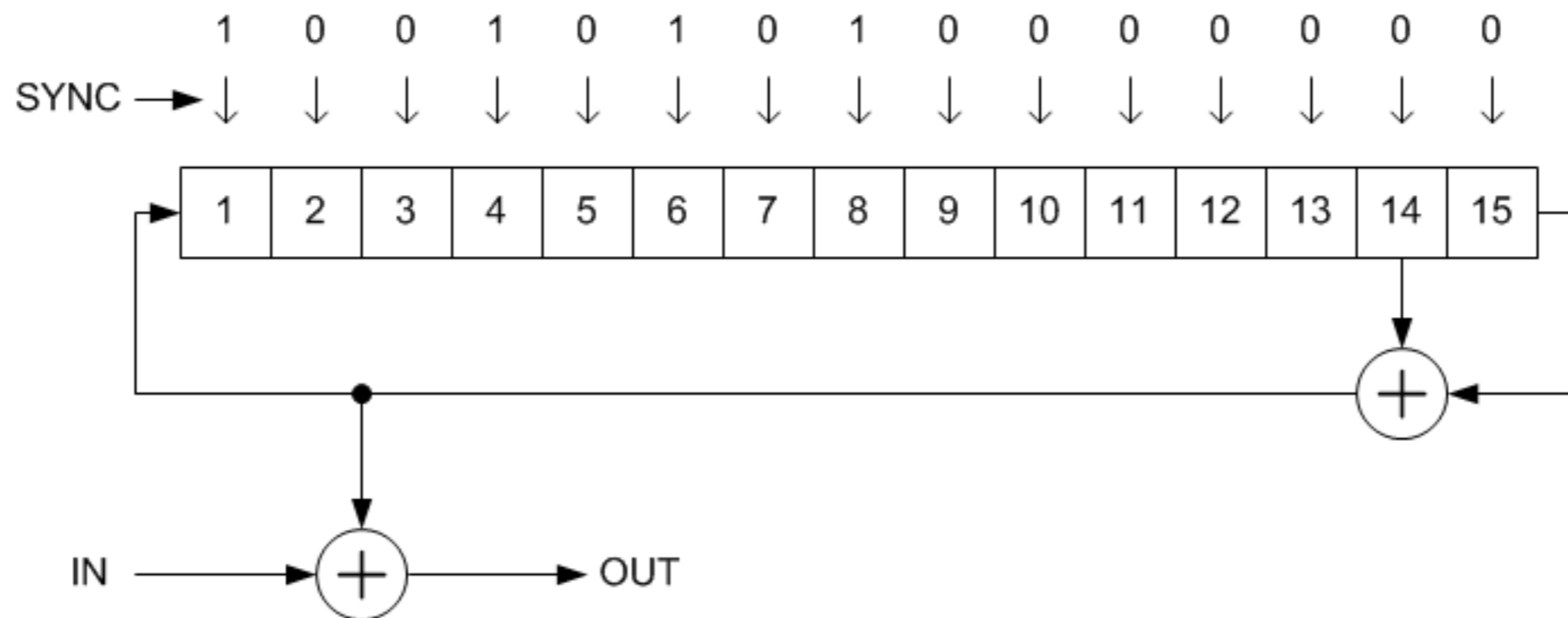


#3: De-scrambling



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

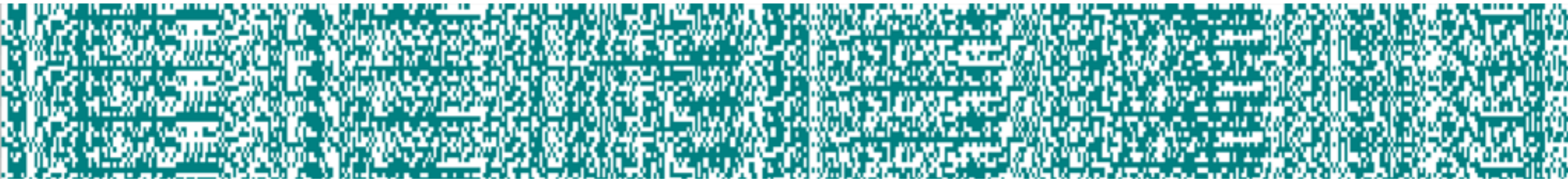
Example:



<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

71	780a5b82751e60ffff1c75	f0b8	ISU (User Data)
	62ae146182748e00000000eee	f0b8	ACK
d6	76d35420706167e52001a8	f0b8	User Data begins
d5	762fae0d8a2fd33231cbfb	f0b8	
d4	762f4ab0b031b52fc25cab	f0b8	
d3	76b0322f46b0342f4f8c67	f0b8	
d2	7631b5b0b00d8a2f437024	f0b8	
d1	76c1c4c44954494fce4775	f0b8	
d0	76c14c2049ce464f526db5	f0b8	
	11a9322582df000a84526d98	f0b8	Log on
	40a9322582d831663856f222	f0b8	Channel control
	c0d83781384a000000005331	f0b8	
	41a9322582d941063787551e	f0b8	Channel control
	c0d936c336b836c51101af14	f0b8	
	6271c274827d8e0000000d259	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- #T101600/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

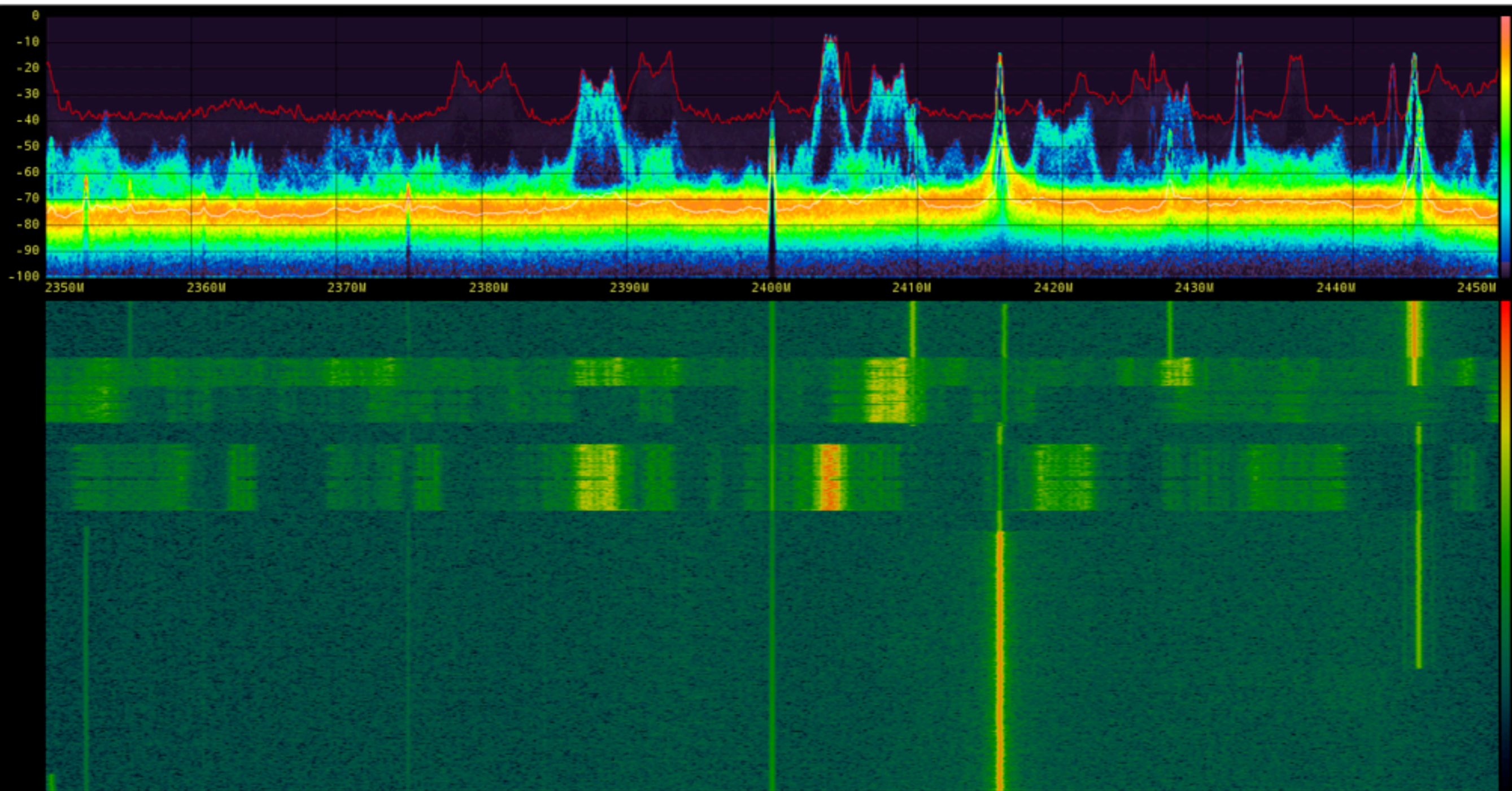
AN 70042B

– **NO PARTICIPATING TWIP**

AIRPORT IN REQUEST








Drones & FPV

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

 Share  Tweet 89  Reddit  Share 28  Pin it  Submit  Email



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

What are we looking at?

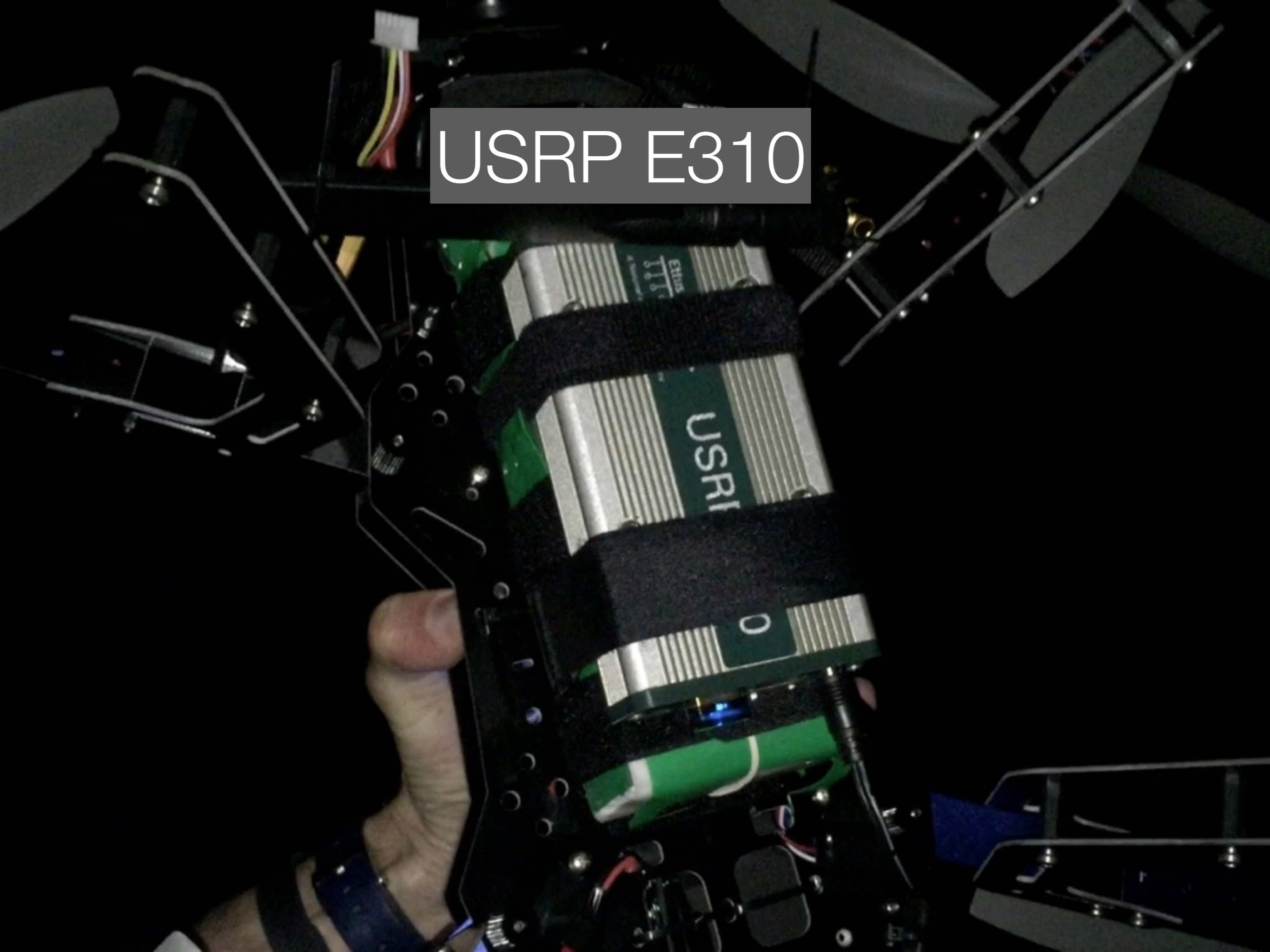
3D Robotics X8+





Webcam

USRP E310



Live Video Downlink with GNU Radio

The image displays the GNU Radio GUI interface for a live video downlink. The interface is split into several sections:

- Control Panel:** Located at the top left, it contains various knobs and sliders for adjusting parameters. Key parameters include:
 - RX LO Offset: 10M
 - rx_gain_bxt: 40
 - RX Freq: 910M
 - mu: 250m
 - mfsk_rx_loop_bw: 31.4159m
 - gain_omega: 1m
 - gain_mu: 10m
 - Per Fine Tuning: 0
 - perfb_loop_bw: 62.8319m
 - perfb_bw: 62.8319m
 - agc_rate: 1m
- Scope Plot:** A central plot showing the received signal. The plot is titled "Scope Plot" and displays a constellation diagram with four clusters of blue dots. The axes are labeled "Ch1" (horizontal) and "Ch2" (vertical), both ranging from -0.4 to 0.4. The plot is set to "XY" mode.
- Video Window:** On the right side, a window titled "MJPG Video" displays a live feed of a field. The video shows a large, open field with a paved path. Several people are visible, including one person in a green jacket with their arms raised. A drone is flying in the field. The video is being processed by a "Packet to PDU" block.
- Block Diagram:** At the bottom, a block diagram shows the signal flow. It includes a "Scope Plot" block, a "Packet to PDU" block, and a "Detect Peak" block. The "Scope Plot" block has a sample rate of 4.2M and a notebook number of 0. The "Packet to PDU" block has a threshold of 0 and is set to "Deassert: Yes" and "Output Inverted: No".

Live Video Downlink with GNU Radio



Spectrum Scanner

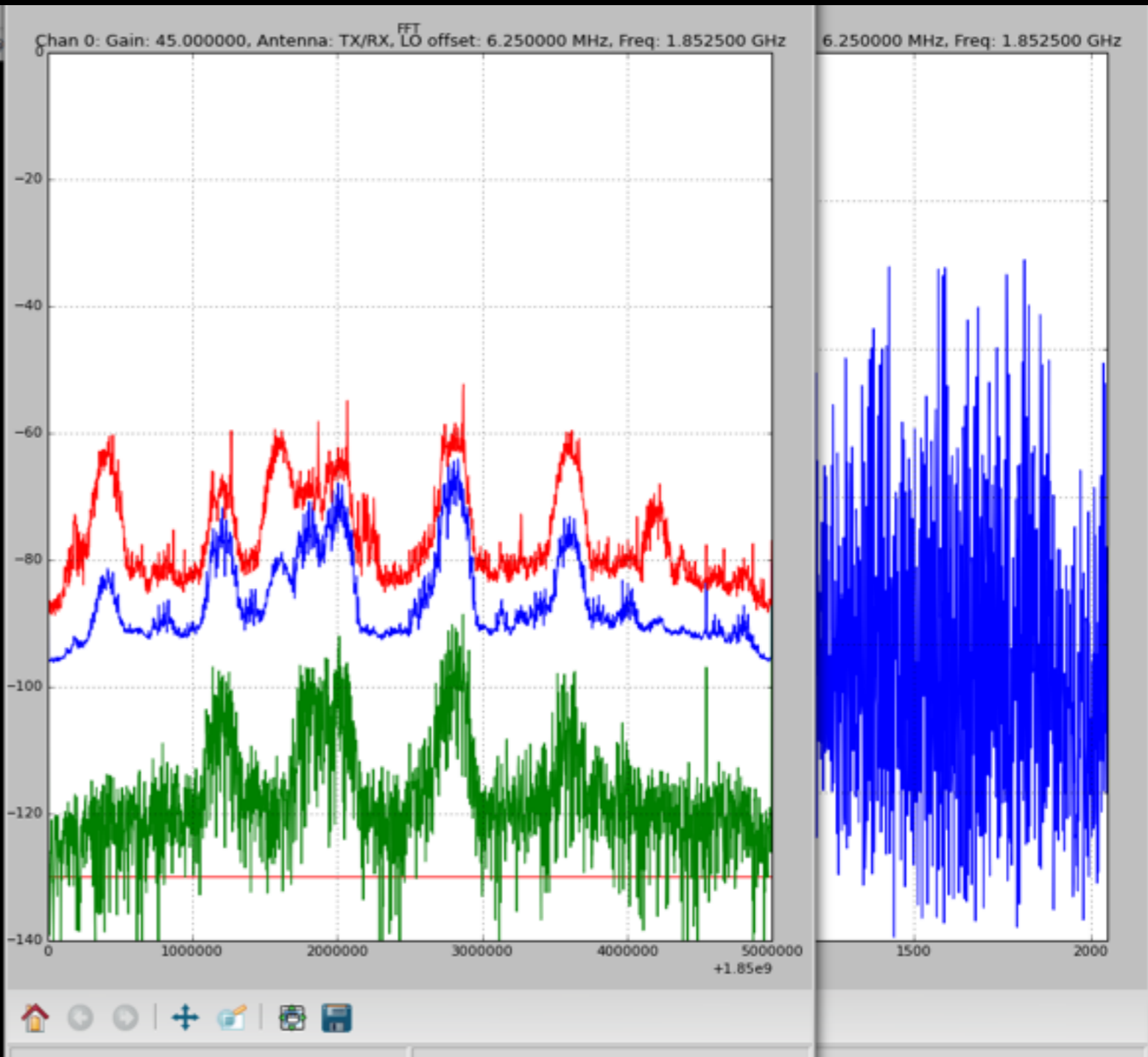
```
File Edit View Search Terminal Tabs Help
balint@crawfish: ~ x balint@crawfish: ~/... x balint@crawfish: ~/... x balint@crawfish: ~ x balint@crawfish: ~
Skipping 720 tail samples for FFT
Running logarithm...done.
Computation time: 85.376024 ms (average: 106.125339 ms, min: 82.826853 ms, max: 202.002048 ms)
Iteration time: 904.361963 ms (average: 1032.769834 ms, min: 788.772106 ms, max: 1505.692005 ms)

Iteration: 63
Channel #0 state machine index: 015/016
Host time: 2015/03/25 08:38:52.366709
USRP time: 1136081143.97
$GPGGA,020544.00,0000.0000,N,00000.0000,E,0.99,1.0,0.0,M,0.0,M,,*5B
$GPRMC,020544.00,V,0000.0000,N,00000.0000,E,0.0,0.0,010106.0,*25
Chan 0: Gain: 45.000000, Antenna: TX/RX, LO offset: 6.250000 MHz, Freq: 1.891000 GHz
Tune time: 166.666985 ms (average: 167.829143 ms, min: 166.020870 ms, max: 209.619045 ms)
Acquisition time: 251.929998 ms (average: 250.633228 ms, min: 250.353098 ms, max: 254.163027 ms)
Channel 0: received 1250000 samples
Processing 610 FFTs
Skipping 720 tail samples for FFT
Running logarithm...done.
Computation time: 104.939938 ms (average: 106.106523 ms, min: 82.826853 ms, max: 202.002048 ms)
Iteration time: 1115.706205 ms (average: 1034.086284 ms, min: 788.772106 ms, max: 1505.692005 ms)

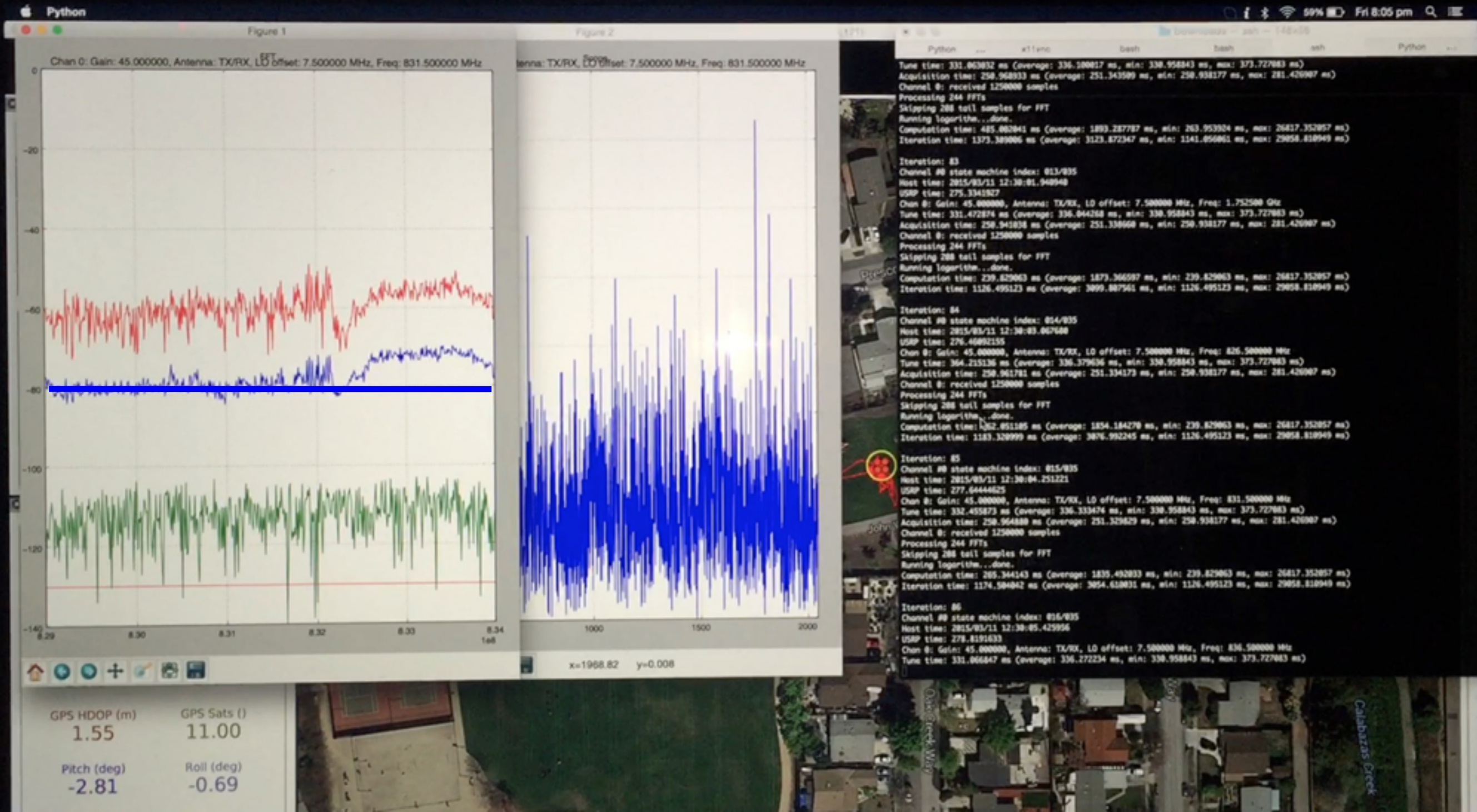
Iteration: 64
Channel #0 state machine index: 016/016
Host time: 2015/03/25 08:38:53.482449
USRP time: 1136081145.09
$GPGGA,020544.00,0000.0000,N,00000.0000,E,0.99,1.0,0.0,M,0.0,M,,*5B
$GPRMC,020544.00,V,0000.0000,N,00000.0000,E,0.0,0.0,010106.0,*25
Chan 0: Gain: 45.000000, Antenna: TX/RX, LO offset: 6.250000 MHz, Freq: 1.889000 GHz
Tune time: 166.135073 ms (average: 167.802673 ms, min: 166.020870 ms, max: 209.619045 ms)
Acquisition time: 250.420809 ms (average: 250.629909 ms, min: 250.353098 ms, max: 254.163027 ms)
Channel 0: received 1250000 samples
Processing 610 FFTs
Skipping 720 tail samples for FFT
Running logarithm...done.
Computation time: 96.598148 ms (average: 105.957955 ms, min: 82.826853 ms, max: 202.002048 ms)
Iteration time: 861.246109 ms (average: 1031.385656 ms, min: 788.772106 ms, max: 1505.692005 ms)

Iteration: 65
Channel #0 state machine index: 001/016
Host time: 2015/03/25 08:38:54.343743
USRP time: 1136081145.95
$GPGGA,020546.00,0000.0000,N,00000.0000,E,0.99,1.0,0.0,M,0.0,M,,*59
$GPRMC,020546.00,V,0000.0000,N,00000.0000,E,0.0,0.0,010106.0,*27
Chan 0: Gain: 45.000000, Antenna: TX/RX, LO offset: 6.250000 MHz, Freq: 1.852500 GHz
Tune time: 169.196129 ms (average: 167.824111 ms, min: 166.020870 ms, max: 209.619045 ms)
Acquisition time: 250.481844 ms (average: 250.627631 ms, min: 250.353098 ms, max: 254.163027 ms)
Channel 0: received 1250000 samples
Processing 610 FFTs
Skipping 720 tail samples for FFT
Running logarithm...done.
Computation time: 124.577999 ms (average: 106.244417 ms, min: 82.826853 ms, max: 202.002048 ms)
Iteration time: 1150.790215 ms (average: 1033.222650 ms, min: 788.772106 ms, max: 1505.692005 ms)

Iteration: 66
Channel #0 state machine index: 002/016
Host time: 2015/03/25 08:38:55.494573
USRP time: 1136081147.1
$GPGGA,020546.00,0000.0000,N,00000.0000,E,0.99,1.0,0.0,M,0.0,M,,*59
$GPRMC,020546.00,V,0000.0000,N,00000.0000,E,0.0,0.0,010106.0,*27
Chan 0: Gain: 45.000000, Antenna: TX/RX, LO offset: 6.250000 MHz, Freq: 1.857500 GHz
Tune time: 166.520119 ms (average: 167.804353 ms, min: 166.020870 ms, max: 209.619045 ms)
```

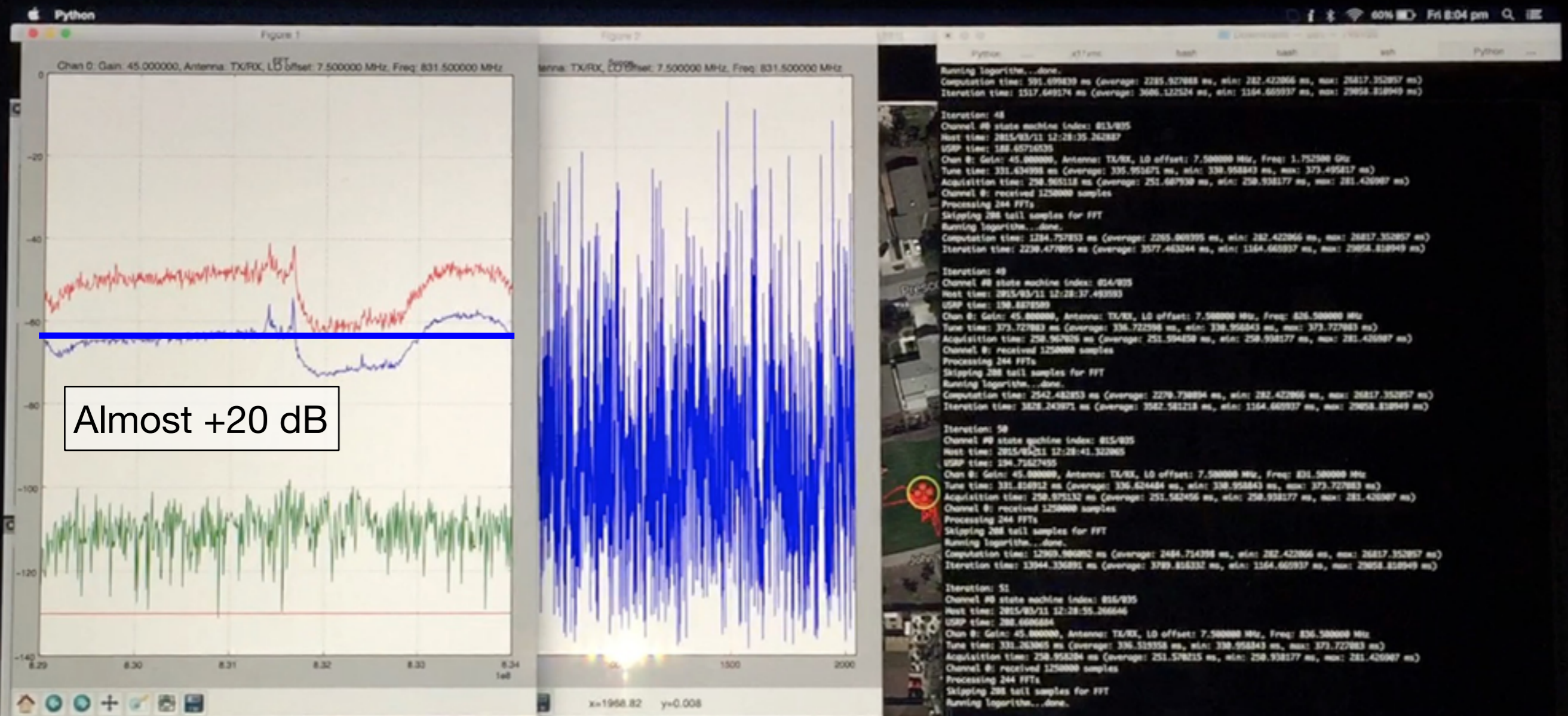


Ground-Level SNR



GPS HDOP (m) 1.55
GPS Sats (i) 11.00
Pitch (deg) -2.81
Roll (deg) -0.69

Airborne SNR



```
Running logarithm...done.
Computation time: 391.699839 ms (average: 2285.927883 ms, min: 282.422866 ms, max: 26817.352857 ms)
Iteration time: 1517.649174 ms (average: 3086.122524 ms, min: 1164.665937 ms, max: 29858.818949 ms)

Iteration: 48
Channel #0 state machine index: 813/835
Next time: 2815/03/11 12:28:35.262887
USRP time: 188.65716539
Chan 0: Gain: 45.800000, Antenna: TX/RX, LO offset: 7.500000 MHz, Freq: 1.752500 GHz
Tune time: 331.634998 ms (Coverage: 335.955671 ms, min: 338.958843 ms, max: 373.495817 ms)
Acquisition time: 258.965118 ms (average: 251.667938 ms, min: 258.938177 ms, max: 281.426967 ms)
Channel 0: received 1250000 samples
Processing 244 FFTs
Skipping 288 tail samples for FFT
Running logarithm...done.
Computation time: 1284.757853 ms (average: 2285.808395 ms, min: 282.422866 ms, max: 26817.352857 ms)
Iteration time: 2228.477895 ms (average: 3577.463244 ms, min: 1164.665937 ms, max: 29858.818949 ms)

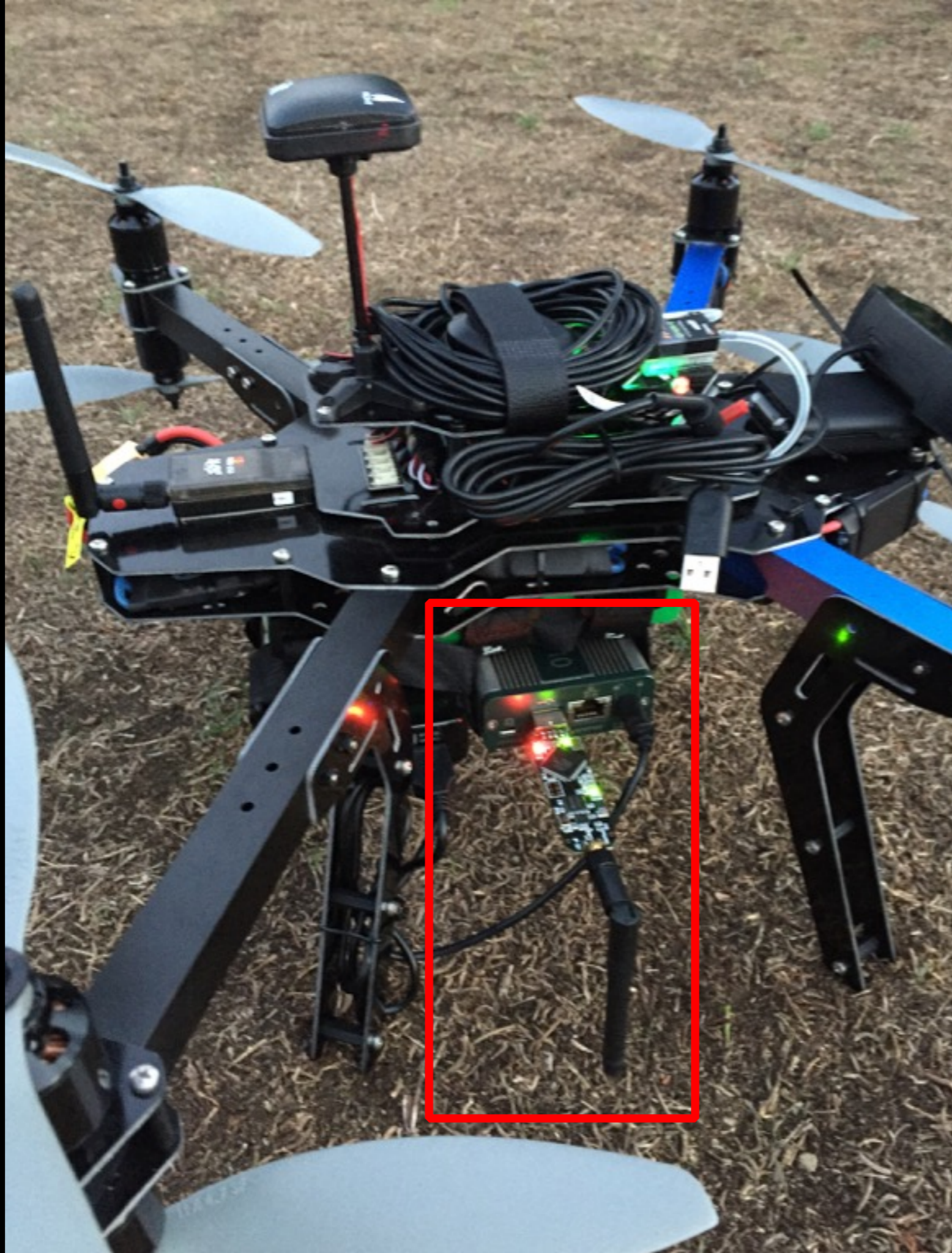
Iteration: 49
Channel #0 state machine index: 814/835
Next time: 2815/03/11 12:28:37.493393
USRP time: 158.8878589
Chan 0: Gain: 45.800000, Antenna: TX/RX, LO offset: 7.500000 MHz, Freq: 826.500000 MHz
Tune time: 373.727883 ms (Coverage: 336.624484 ms, min: 338.958843 ms, max: 373.727883 ms)
Acquisition time: 258.967826 ms (average: 251.594528 ms, min: 258.938177 ms, max: 281.426967 ms)
Channel 0: received 1250000 samples
Processing 244 FFTs
Skipping 288 tail samples for FFT
Running logarithm...done.
Computation time: 2542.482853 ms (average: 2278.738894 ms, min: 282.422866 ms, max: 26817.352857 ms)
Iteration time: 3428.243971 ms (average: 3542.581218 ms, min: 1164.665937 ms, max: 29858.818949 ms)

Iteration: 50
Channel #0 state machine index: 815/835
Next time: 2815/03/11 12:28:41.322865
USRP time: 194.71627495
Chan 0: Gain: 45.800000, Antenna: TX/RX, LO offset: 7.500000 MHz, Freq: 831.500000 MHz
Tune time: 331.828912 ms (Coverage: 336.624484 ms, min: 338.958843 ms, max: 373.727883 ms)
Acquisition time: 258.975132 ms (average: 251.582456 ms, min: 258.938177 ms, max: 281.426967 ms)
Channel 0: received 1250000 samples
Processing 244 FFTs
Skipping 288 tail samples for FFT
Running logarithm...done.
Computation time: 12989.986882 ms (average: 2484.714398 ms, min: 282.422866 ms, max: 26817.352857 ms)
Iteration time: 13944.336891 ms (average: 3789.816332 ms, min: 1164.665937 ms, max: 29858.818949 ms)

Iteration: 51
Channel #0 state machine index: 816/835
Next time: 2815/03/11 12:28:55.266646
USRP time: 288.6686884
Chan 0: Gain: 45.800000, Antenna: TX/RX, LO offset: 7.500000 MHz, Freq: 826.500000 MHz
Tune time: 331.263065 ms (Coverage: 336.533358 ms, min: 338.958843 ms, max: 373.727883 ms)
Acquisition time: 258.958284 ms (average: 251.578215 ms, min: 258.938177 ms, max: 281.426967 ms)
Channel 0: received 1250000 samples
Processing 244 FFTs
Skipping 288 tail samples for FFT
Running logarithm...done.
```

GPS HDOP (m) 1.54
GPS Sats (I) 11.00
Pitch (deg) 0.95
Roll (deg) 1.50







GSG Ubertooth dongle



Atmel RZRAVEN ZigBee dongle

Kismet with ZigBee Plugin on E310

Terminal

File Edit View Search Terminal Tabs Help

Terminal x Terminal x Terminal x Terminal x Terminal x Terminal x Terminal x Terminal x Terminal x Terminal x Terminal x Terminal x

Kismet Sort View Windows

A	Chy	Name	C	Addr	Pkts	Size	Chan	Alr	
Dot15d4	51:A1	N 51:A1			2	147B	15	0	ettus-e300
[Last seen: Oct 21 14:48:41] [Crypt: None] [Unknown] [Dot15d4] [51:A1]									
Dot15d4	10:06	N 10:06			3	261B	15	0	Elapsed 00:38.30
Dot15d4	22:22	N 22:22			2	162B	26	0	Networks 51
Dot15d4	04:06	N 04:06			3	276B	26	0	Packets 466
Dot15d4	E1:2F	N E1:2F			1	67B	20	0	Pkt/Sec 0
Dot15d4	14:19	N 14:19			3	189B	20	0	Filtered 0
Dot15d4	FF:22	N FF:22			1	55B	20	0	
Dot15d4	01:00	N 01:00			99	2K	26	0	
Dot15d4	F0:FF	N F0:FF			81	1K	26	0	
Dot15d4	FF:FF	N FF:FF			202	6K	20	0	
Dot15d4	00:00:00:00:00:00	N 00:00:00:00:00:00			1	48B	20	0	
Dot15d4	00:00	N 00:00			4	184B	14	0	
Dot15d4	21:A6	N 21:A6			2	138B	14	0	
Dot15d4	58:33	N 58:33			2	78B	11	0	
Dot15d4	55:CF	N 55:CF			3	129B	11	0	
Dot15d4	A6:04	N A6:04			4	172B	11	0	
Dot15d4	36:05	N 36:05			8	263B	25	0	
Dot15d4	11:00	N 11:00			1	8B	25	0	
Dot15d4	F5:FF	N F5:FF			1	8B	20	0	
Dot15d4	27:FF	N 27:FF			1	8B	20	0	
Dot15d4	35:05	N 35:05			4	156B	14	0	
Dot15d4	0B:00	N 0B:00			1	8B	14	0	
Dot15d4	87:00	N 87:00			1	34B	14	0	
Dot15d4	7E:00	N 7E:00			3	171B	11	0	
Dot15d4	32:00	N 32:00			1	57B	25	0	
Dot15d4	EC:FF	N EC:FF			1	8B	20	0	
Dot15d4	06:00	N 06:00			1	11B	20	0	
Dot15d4	8B:00	N 8B:00			1	57B	20	0	
Dot15d4	12:04	N 12:04			1	8B	16	0	
Dot15d4	0B:FF	N 0B:FF			1	8B	14	0	
Dot15d4	A0:00	N A0:00			1	8B	14	0	
Dot15d4	90:94	N 90:94			1	8B	12	0	
Dot15d4	BF:52	N BF:52			3	111B	15	0	
Dot15d4	1E:CB	N 1E:CB			1	37B	15	0	
Dot15d4	C8:1F	N C8:1F			1	16B	15	0	
Dot15d4	80:12	N 80:12			5	231B	15	0	
Dot15d4	00:06	N 00:06			2	12B	11	0	
Dot15d4	6E:83	N 6E:83			8	336B	11	0	
Dot15d4	10:00	N 10:00			1	41B	20	0	
Dot15d4	42:75	N 42:75			2	82B	20	0	
Dot15d4	0A:00	N 0A:00			1	42B	15	0	
Dot15d4	9A:00	N 9A:00			2	84B	15	0	
Dot15d4	22:A9	N 22:A9			7	294B	20	0	
Dot15d4	6E:00	N 6E:00			1	8B	18	0	
Dot15d4	EA:8F	N EA:8F			4	168B	15	0	
Dot15d4	4A:00	N 4A:00			14	836B	25	0	
Dot15d4	E9:24	N E9:24			1	77B	25	0	
Dot15d4	03:00	N 03:00			1	79B	20	0	
Dot15d4	C3:F5	N C3:F5			2	158B	20	0	
Dot15d4	00:3C	N 00:3C			166	4K	26	0	
Dot15d4	01:3C	N 01:3C			30	1K	26	0	
Dot15d4	C8:89	N C8:89			2	78B	25	0	
Dot15d4	7F:4D	N 7F:4D			4	222B	25	0	

GPS 38.901413 -77.041794 Spd: 14.53 mph Alt: 131.49 ft 3d fix Pwr: AC

4

Packets

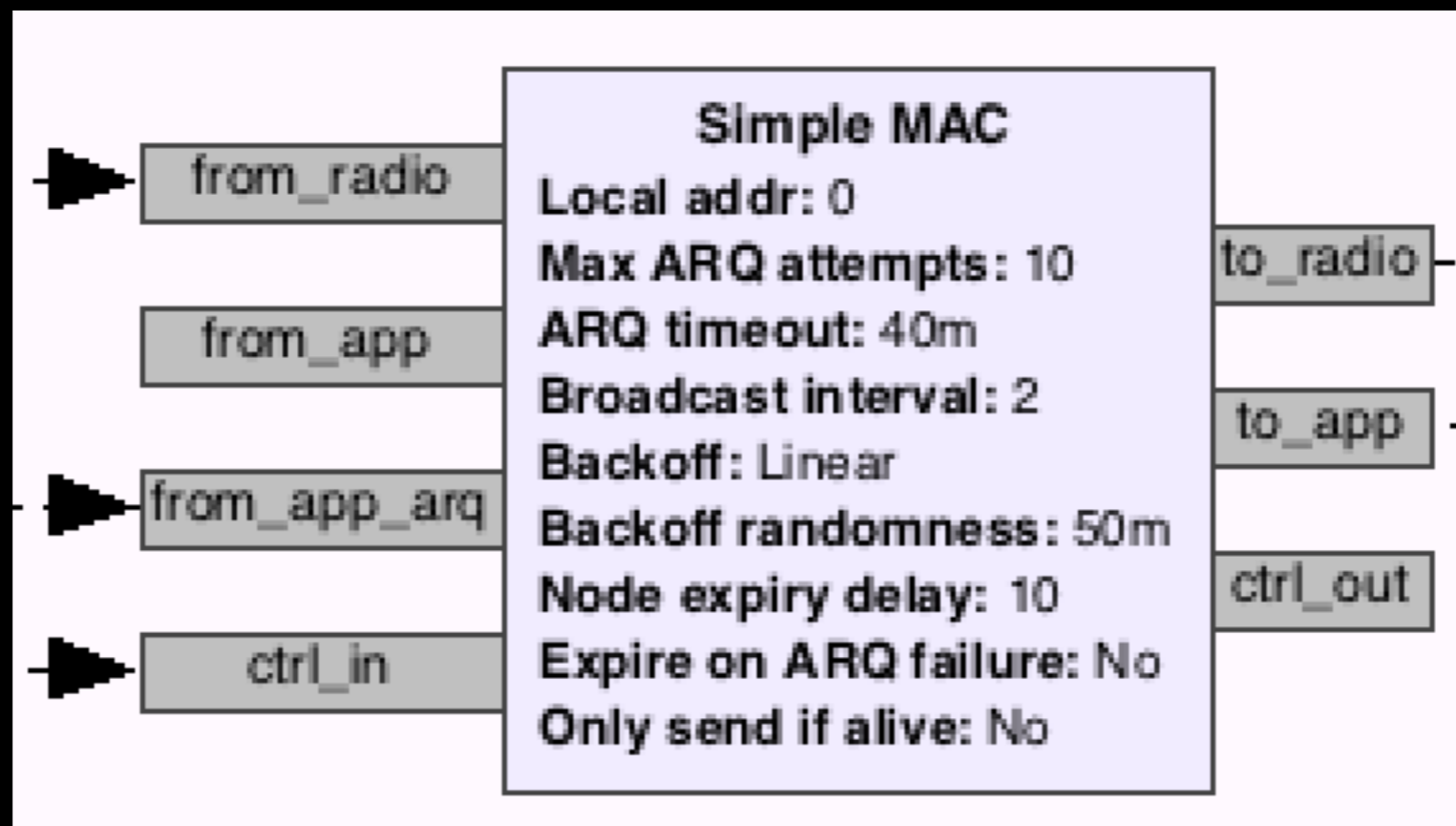
Data

INFO: Saved data files
ERROR: Short dot15d4 frame!
INFO: Detected new 802.11 network BSSID 14:19, unencrypted, no beacons seen yet
INFO: Detected new 802.11 network BSSID 04:06, unencrypted, no beacons seen yet
INFO: Detected new 802.11 network BSSID 10:06, unencrypted, no beacons seen yet

raven
Hop

Backhaul

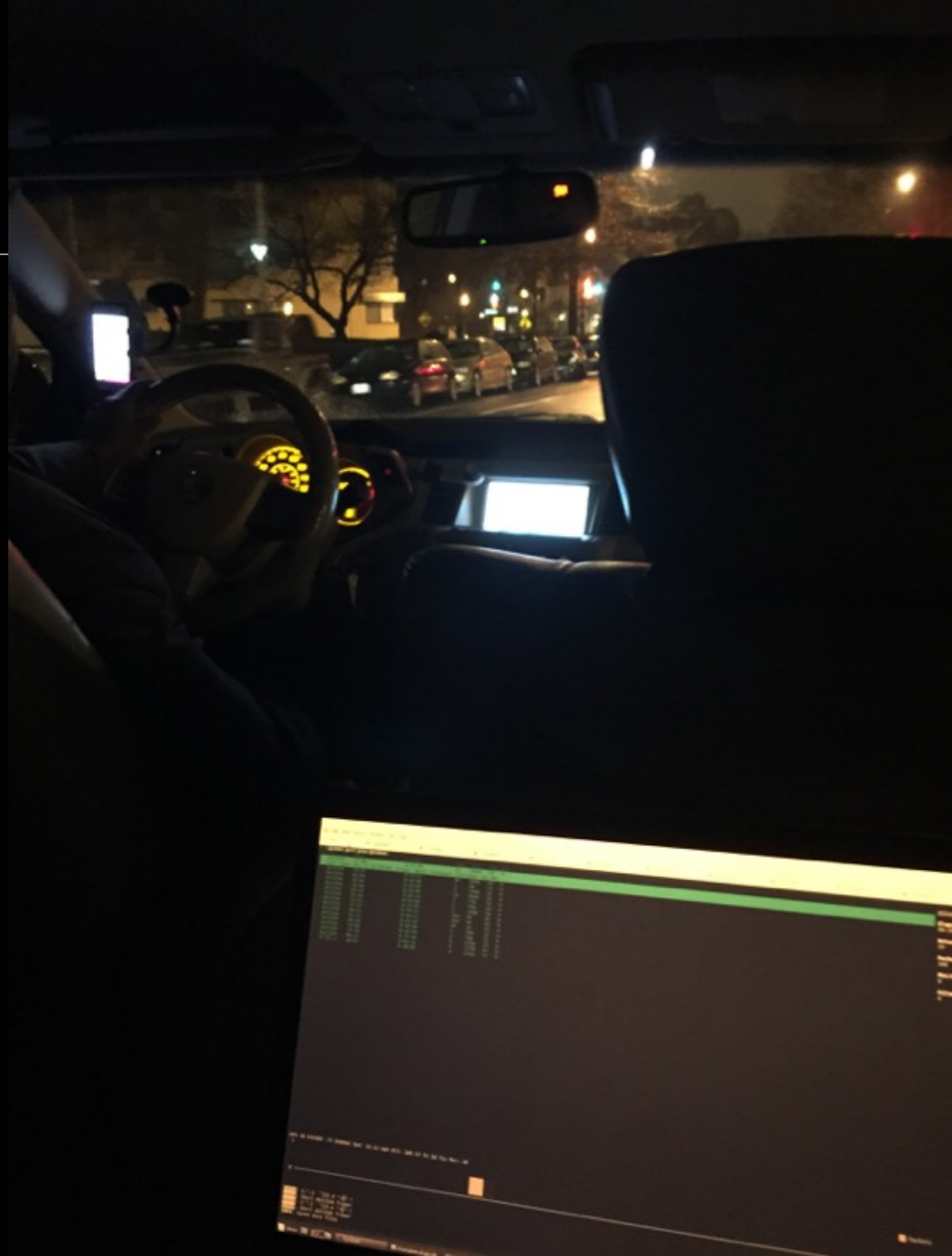
- None: Run unattended
- Wi-Fi: More 2.4 GHz ISM activity close to receiver & limited range
- Custom through SDR: greater range

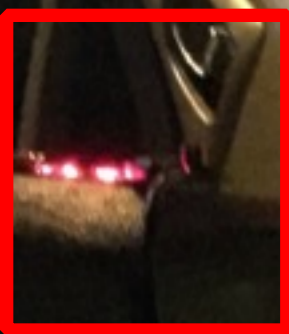


Airborne Platform

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

ZigBee Wardriving

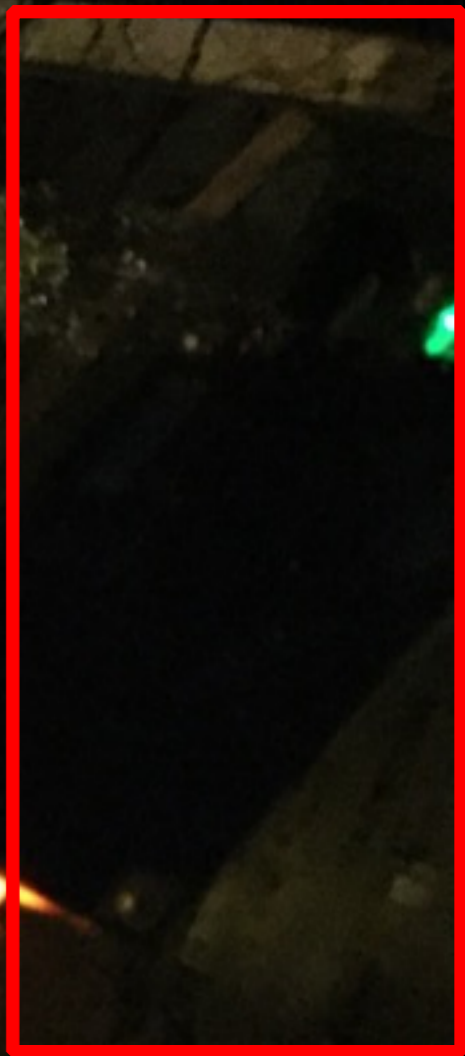




ApiMote



RZRAVEN



B200mini

ZigBee Wardriving

The image shows a Wireshark capture of ZigBee traffic. The main pane displays a list of frames with columns for No., Time, Source, Destination, Protocol, Length, and Info. The selected frame (No. 183) is expanded to show its details:

- Frame 183: 48 bytes on wire (384 bits), 48 bytes captured (384 bits)
- IEEE 802.15.4 Data, Dat: la:0b:03:02:00:7f:10:00, Src: fa:90:00:01:00:7f:10:00
 - Frame Control Field: Data (0x0c21)
 - Sequence Number: 117
 - Destination PAN: 0xfeed
 - Destination: la:0b:03:02:00:7f:10:00 (la:0b:03:02:00:7f:10:00)
 - Source PAN: 0xfeed
 - Extended Source: fa:90:00:01:00:7f:10:00 (fa:90:00:01:00:7f:10:00)
 - FCS: 0x0c21 (Correct)
 - 6LoWPAN
 - Internet Protocol Version 6, Src: fe80::f890:1:7f:1000 (fe80::f890:1:7f:1000), Dst: ff01::d0:30c (ff01::d0:30c)
 - 0110 = Version: 6
 - 0010 0000 = Traffic class: 0x00000020
 - 0011 0001 0010 0000 0011 = Flowlabel: 0x00031203
 - Payload length: 0
 - Next header: IPv6 no next header (59)
 - Hop limit: 1
 - Source: fe80::f890:1:7f:1000 (fe80::f890:1:7f:1000)
 - Destination: ff01::d0:30c (ff01::d0:30c)
 - [Source GeoIP: Unknown]
 - [Destination GeoIP: Unknown]

At the bottom of the interface, a hex dump shows the raw bytes of the frame, and a status bar indicates: Frame (48 bytes) | Decompressed 6LoWPAN IPHC (40 bytes) | File: /Users/balint/e310/DC/apimote-s... | Packets: 547 - Displayed: 547 (100.0%) - Load time: 0:00:00.3 | Profile: Default

01:58AM

ZigBee Wardriving

The image shows a Wireshark capture of ZigBee traffic. The main pane displays a list of captured packets. Packet 474 is highlighted in yellow and expanded in the details pane. The details pane shows the following information:

- Frame 474: 57 bytes on wire (456 bits), 57 bytes captured (456 bits)
- IEEE 802.15.4 Data, Dst: 34:cc:d0:01:60:6f:0d:d0, Src: 15:95:01:02:00:7a:1c:01, Bad FCS
- Frame Control Field: Data (0x0c21)
- Sequence Number: 69
- Destination PAN: 0xfeed
- Destination: 34:cc:d0:01:60:6f:0d:d0 (34:cc:d0:01:60:6f:0d:d0)
- Source PAN: 0xfee8
- Extended Source: 15:95:01:02:00:7a:1c:01 (15:95:01:02:00:7a:1c:01)
- FCS: 0x34b0 (Incorrect, expected FCS=0x0241)
- [Expert Info (Warn/Checksum): Bad FCS]
- Data (32 bytes)
- Data: 3cf248531a338101b03c6563686f207468697a27636f6e...
- [Length: 32]

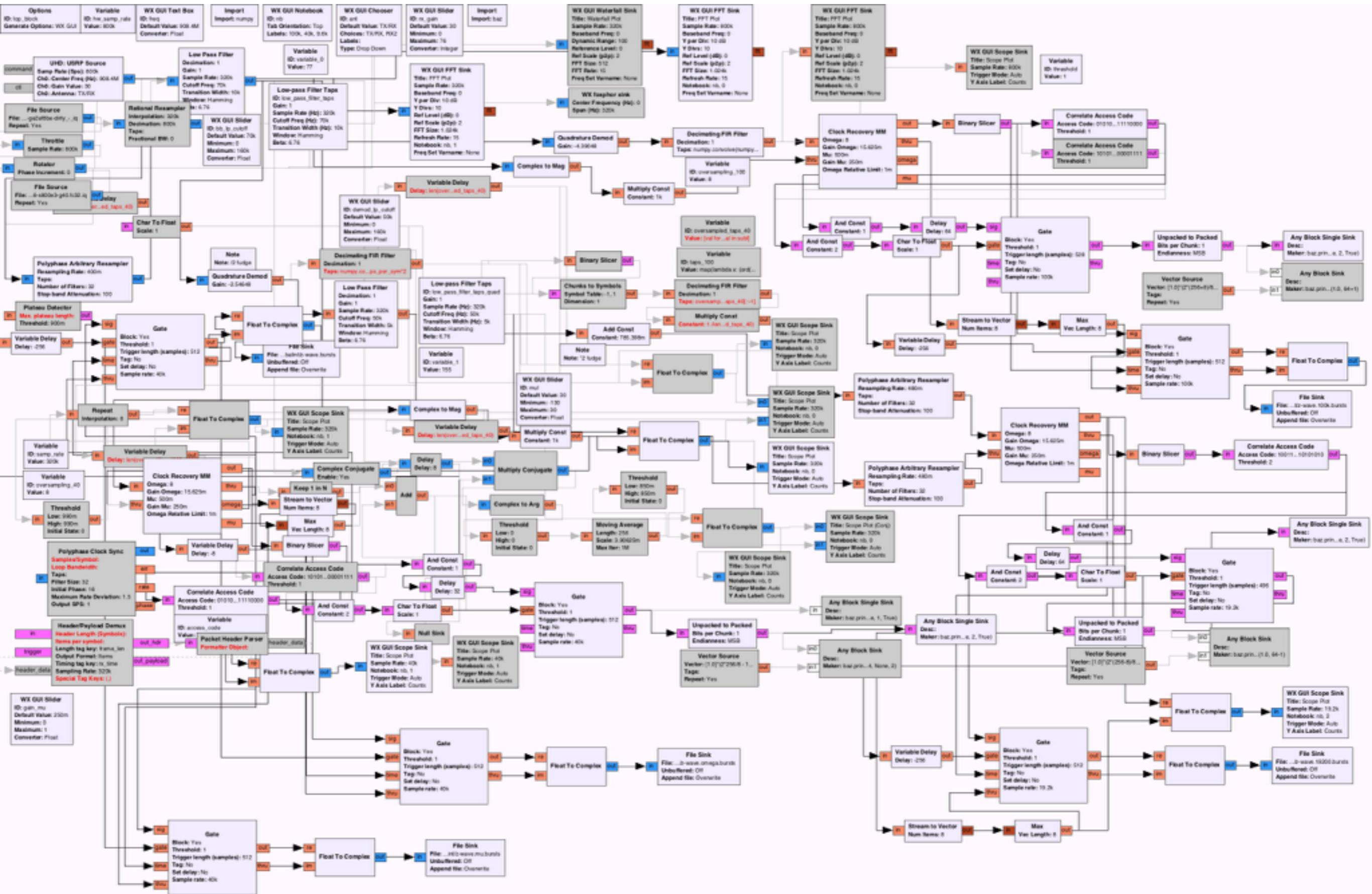
At the bottom of the image, there is a dark grey box with the text "echothiz`connection" in white. The status bar at the very bottom shows "Destination PAN (wpan.dst_pan), 2 by... | Packets: 856 - Displayed: 856 (100.0%) - Load time: 0:00:00.2 | Profile: Default".

Other Signals

Z-Wave

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

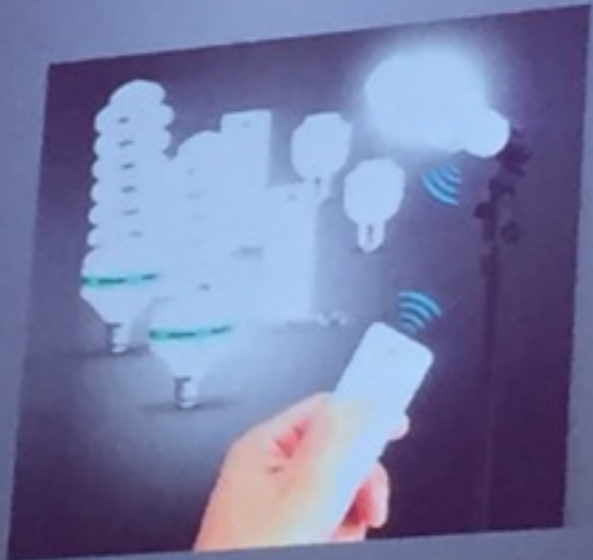




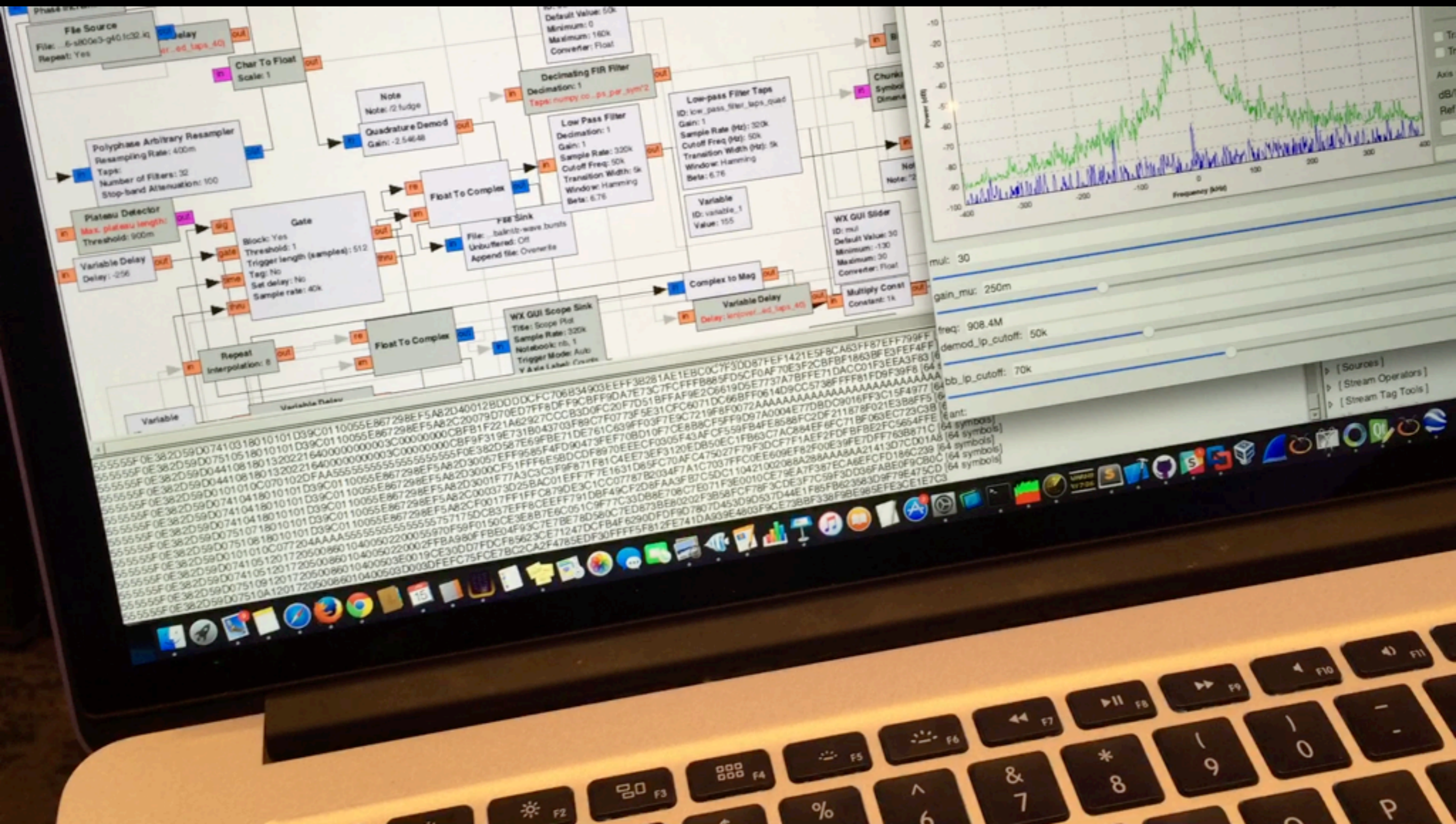
Breaking Bulbs



- 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





B200mini

Z-Wave around DC

55555F0EB1578020141010C0326021006F4F149DBCBBF29D4318B3AB0E28AAA32CB00F52E0115FF138C41156070576A259B421B16C
BECAA7AFB8E8F838EEE2A [64 symbols]

55555F155555545D514F41D515555574144A15575554557D5D5D1C3555A5C5091DFDDD4455717C1D6191F455754755757479D4715
555515D55544545552C17 [64 symbols]

555545F0DD4265E5714546F71474FD5935260618144170D55555F0D7242DFF0850455890060AAF3AA969B53F732828EF19B1A046E2A
0AAA6A2EA22A8E4BAAAB8 [64 symbols]

555554F055045C5555515555555D5555D555D55557545545D51F0551A5555515155D55555555155D5C5539CF5171475FF914006D5
D6751F5DD554528461F1F [64 symbols]

555557001516570C7C55479DBBAAEA888AAF022816AAAEAAA2AEEBFBA0FE7C9D7D557C5C5755515557845025573F41F92080BAA22
E3F7E29DD55555515545 [64 symbols]

55555705725DF9C117E6FCB5667C3455550476C5D5A55554501DF5D60F20E4AA5066547FDD1D10FC75D7C42009CE5D497551551458
4259535E715C54007D1F1 [64 symbols]

55555F07D0F5DDF771387134E77D37F40F9280D237C455E6592E1E80544A54E5277911DF0D76051536553C5531355999C91C4173FE
6C952D730AA8EB8EA5E9A [64 symbols]

555554F0555554555714E7073FD8BF87BF0F6C20081C4CF8518E052EA41DA61F8EBCED6810DD3FA3928B31FD7AAC5BAA60F1889DB9
CA387D99EFF6996EFE216 [64 symbols]

555755F0D18CF24309530B0C18B0026F40B7A49C115183DE785BB71CD9C61F475185179D94A700EC50C68000020800050300C141C1C
1C0200070004068381008 [64 symbols]

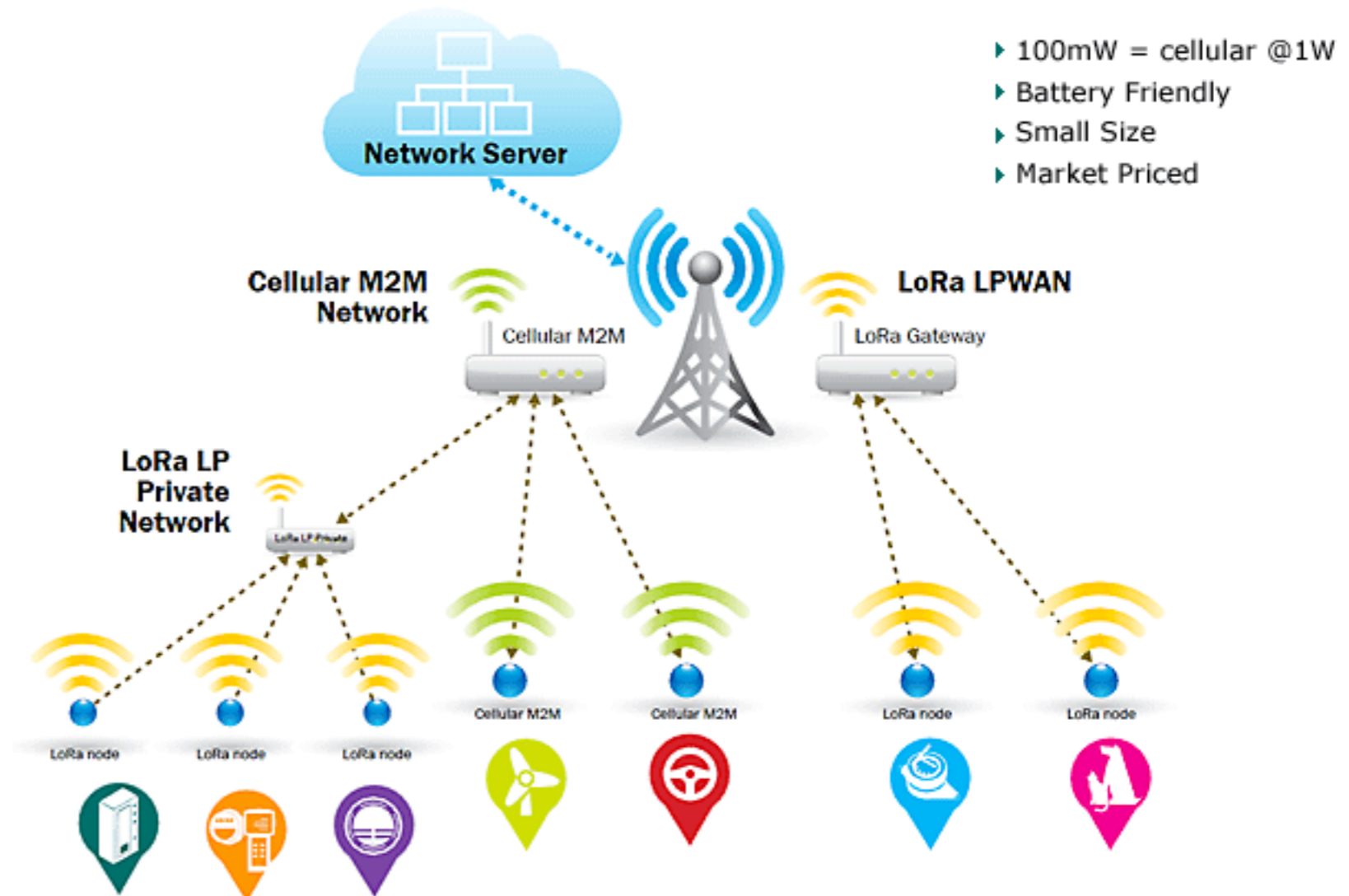
55555F0D18CE24208030B0A0909C1342E8002187CF020CBF63DD0089D7E6C6DC44278632A44357FC200B9C485EE1785F6CC47C21BA
786F255808E0FC4235C79 [64 symbols]

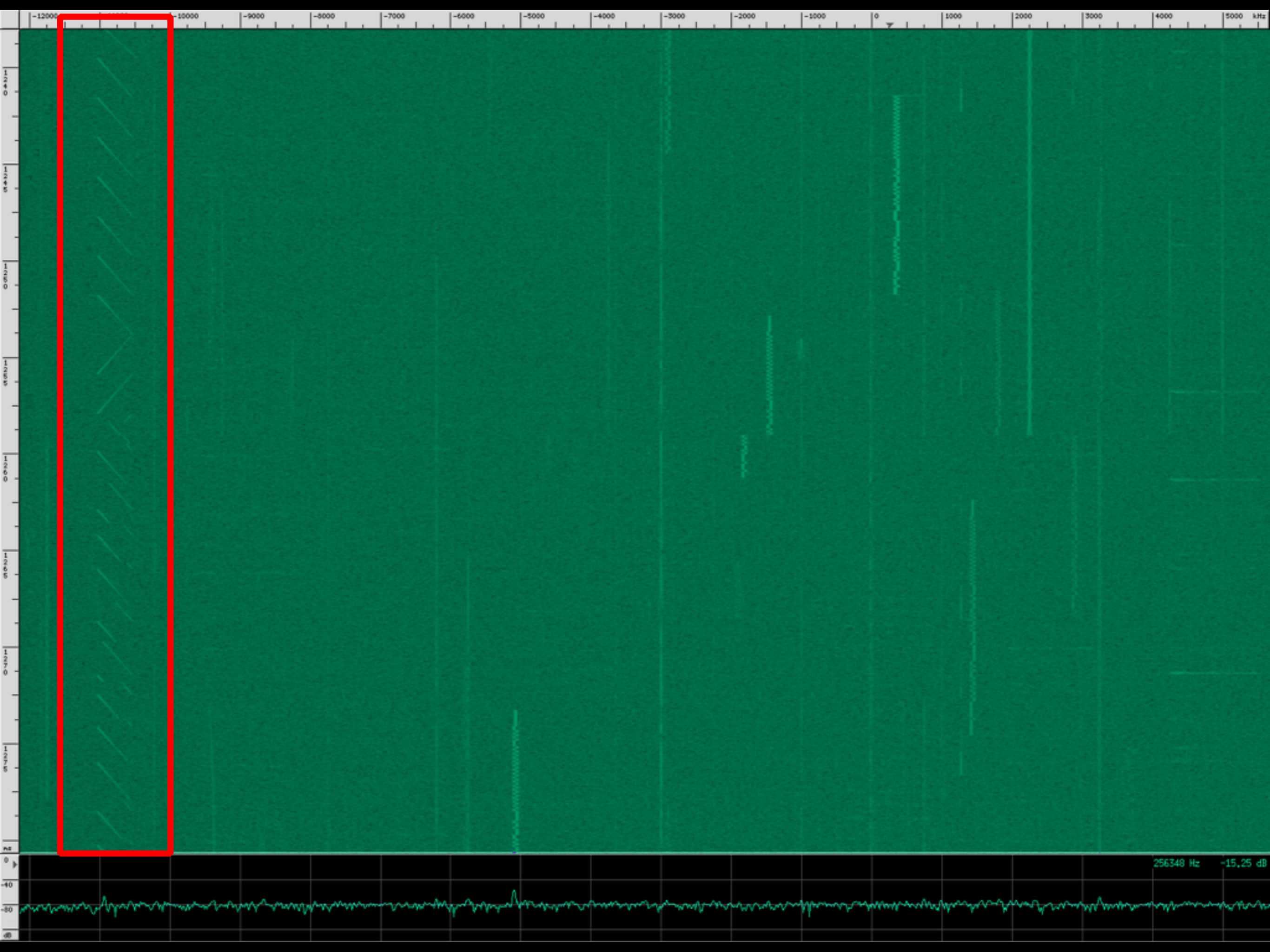
55555F0D18CE24208410D0D012003FF96517925490C33D0F4F1FA2FEF0AE332C3B69189E0A08D0054029FCCE66C3F308FD3945AE73
39F33DDC600222BC43F67 [64 symbols]

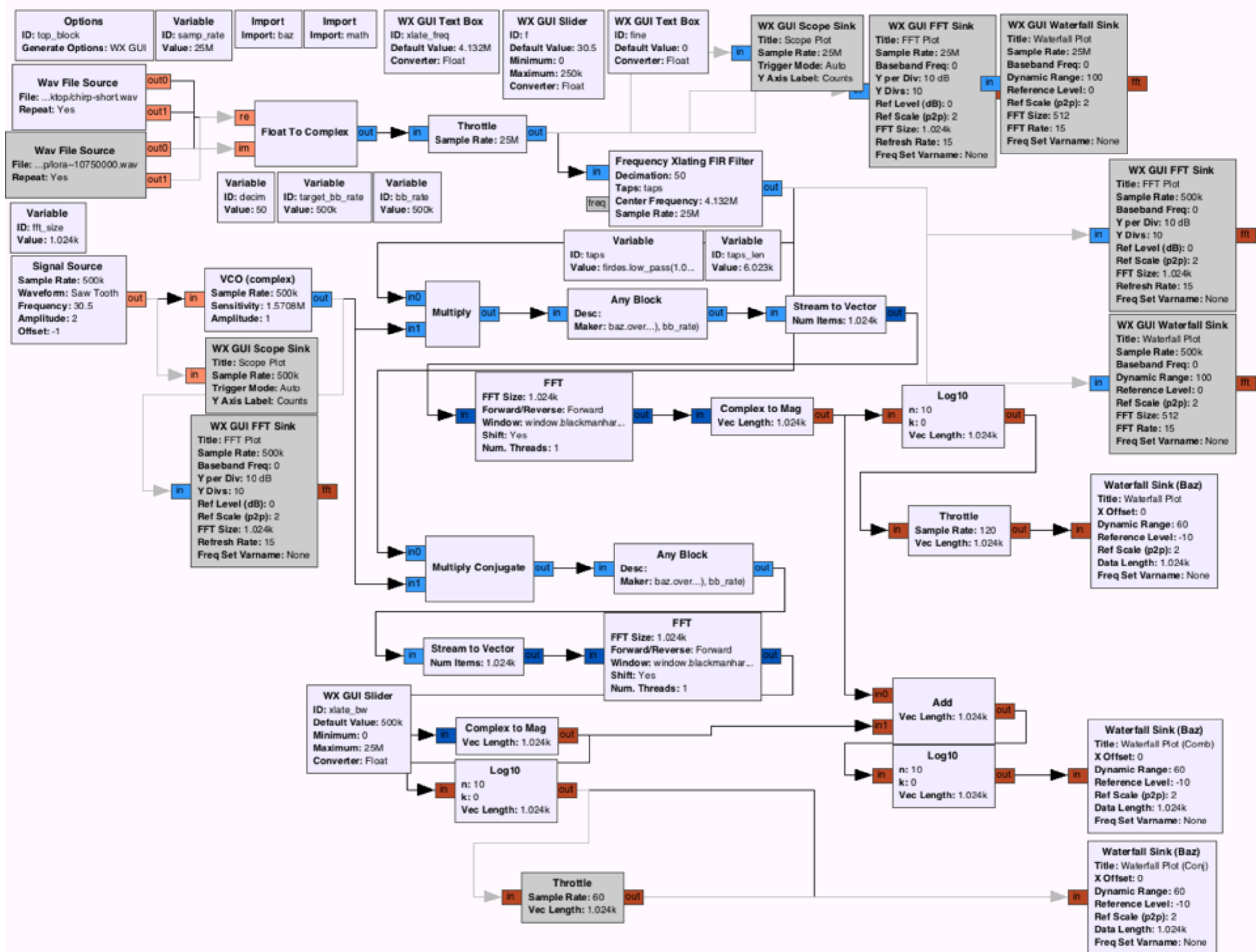
55555F0D18CE24208410D0D012003FF964E3C5021C31F7A60DC1F00DF00E4305DB9FFA1062E4F6B74F7CFFD4AEE8E18EF9EF429941
1D82901B29F201FFC0088 [64 symbols]

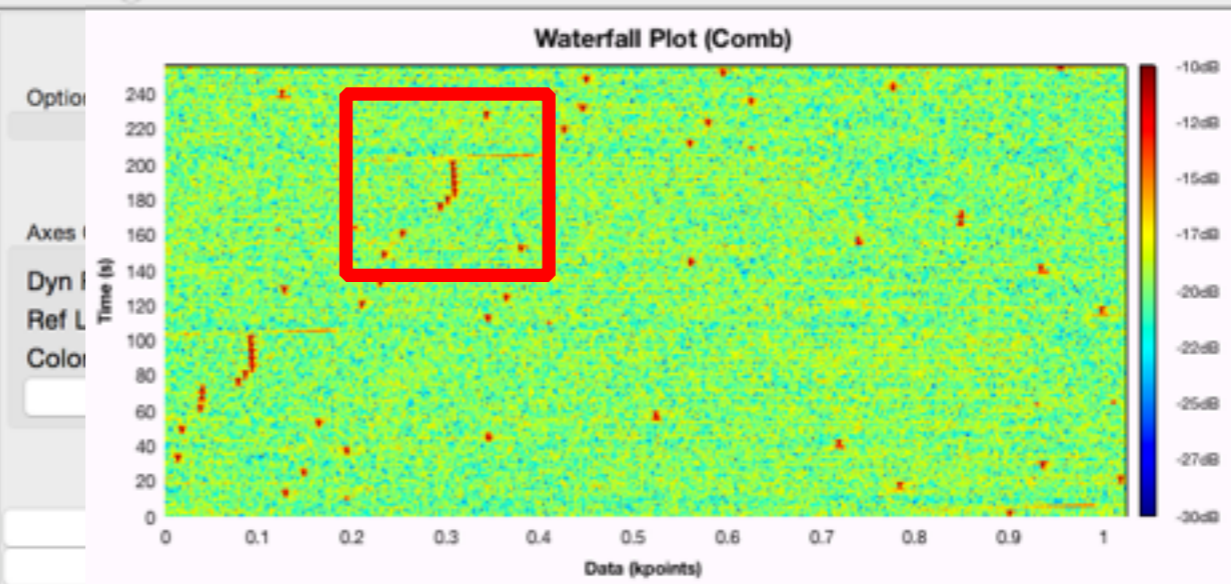
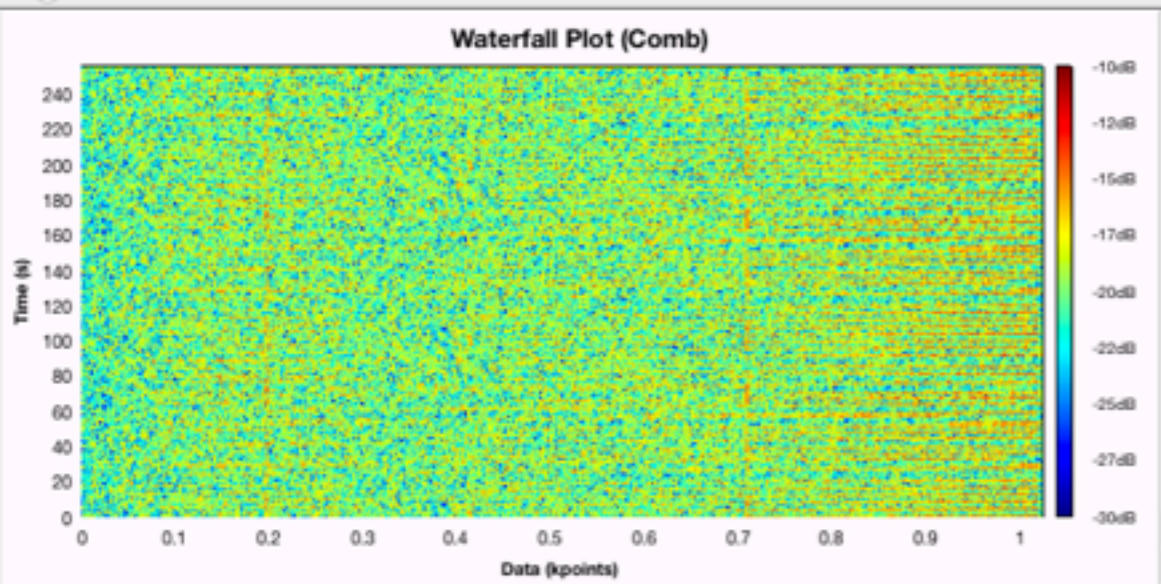
LoRa

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









Options

Axes Options

Dyn Range: + -

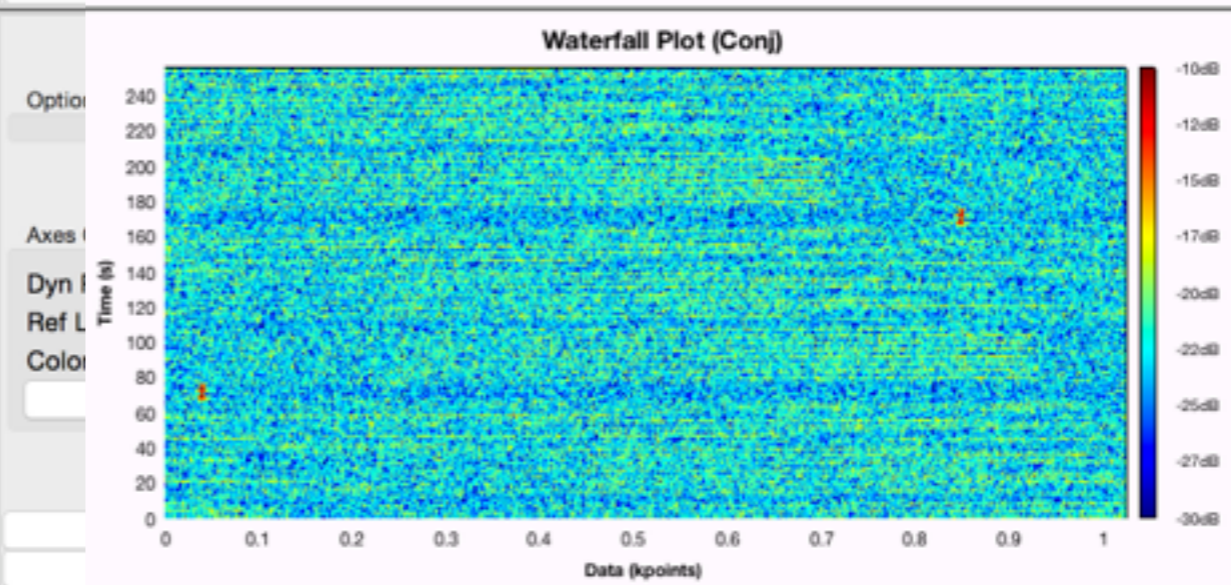
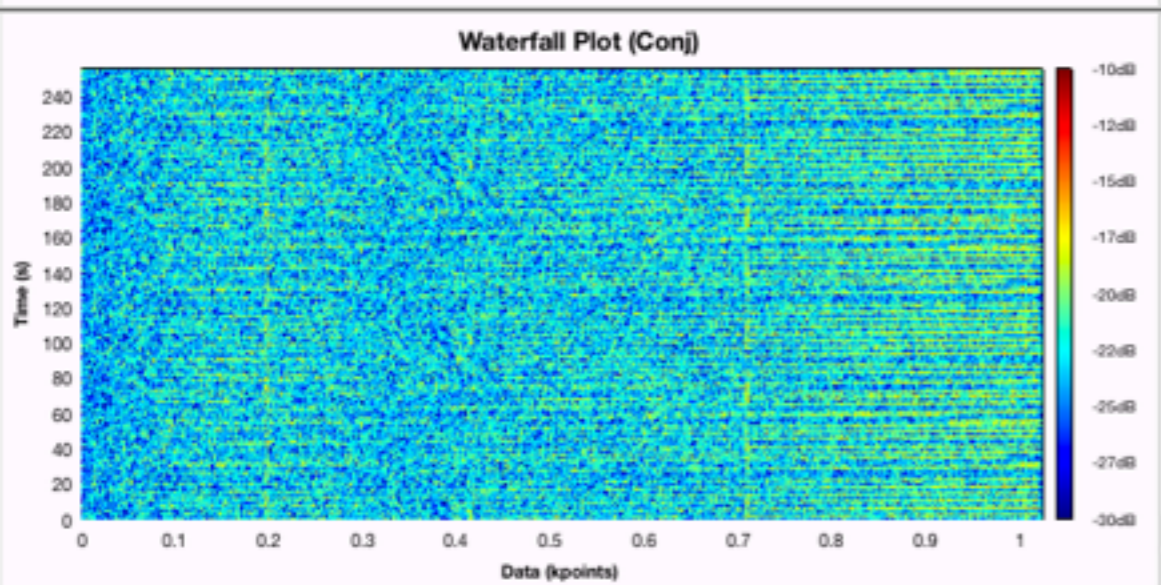
Ref Level: + -

Color: RGB2

Autoscale

Clear

Stop



Options

Axes Options

Dyn Range: + -

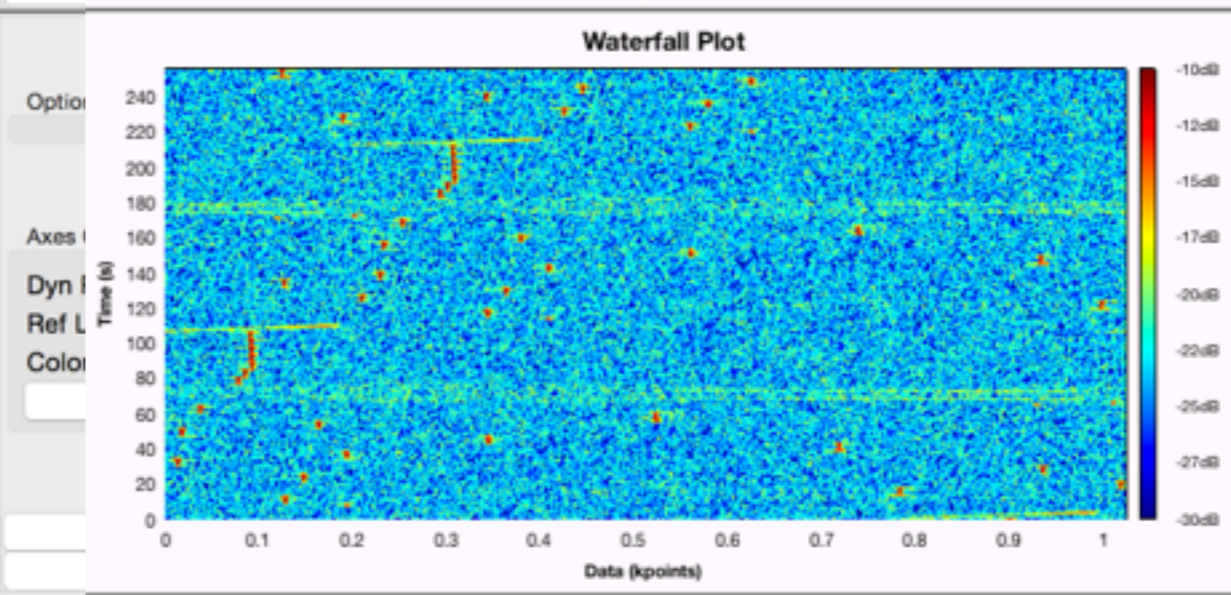
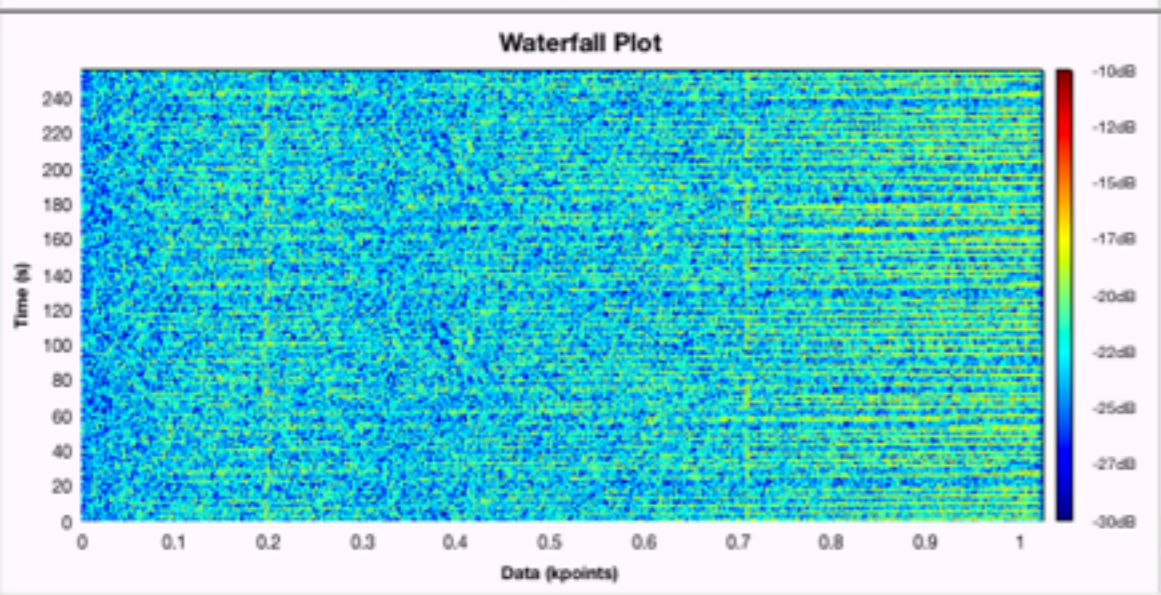
Ref Level: + -

Color: RGB2

Autoscale

Clear

Stop



Options

Axes Options

Dyn Range: + -

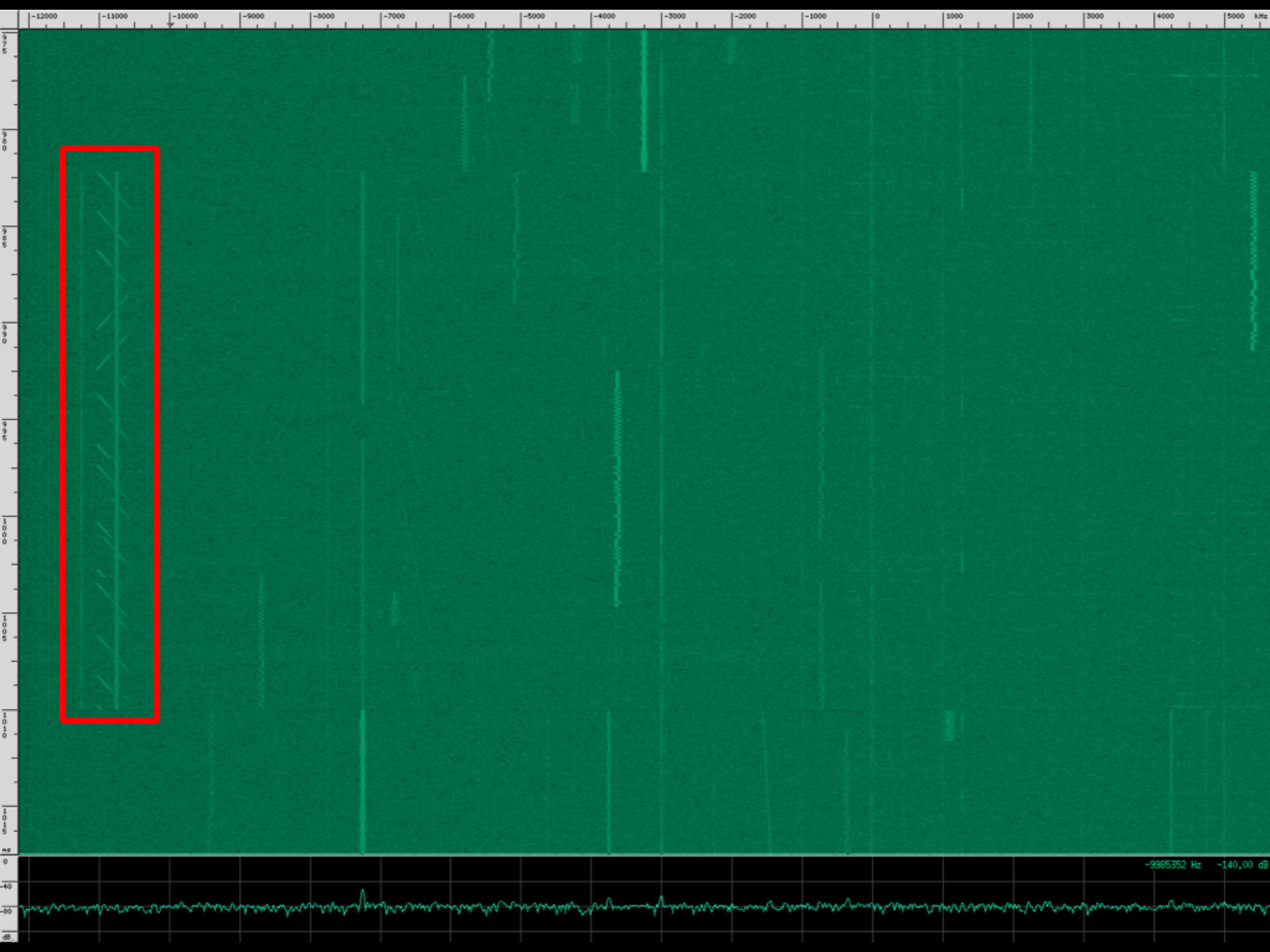
Ref Level: + -

Color: RGB2

Autoscale

Clear

Stop

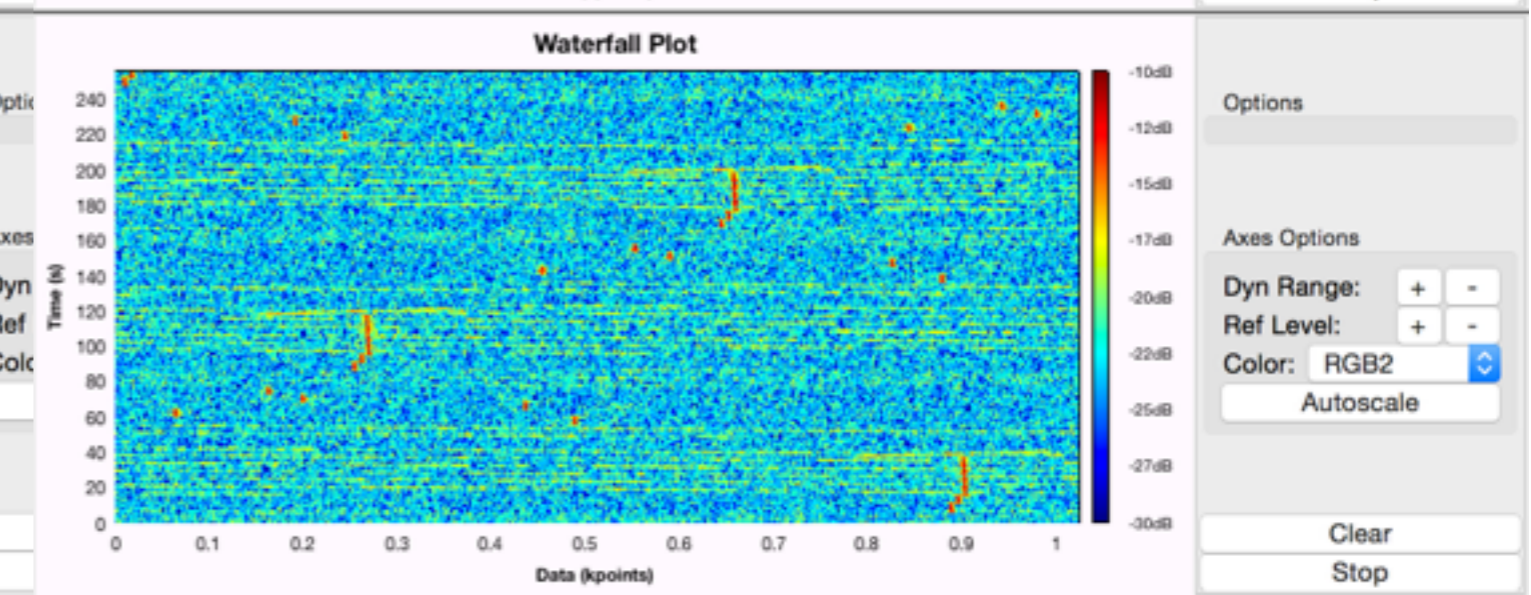
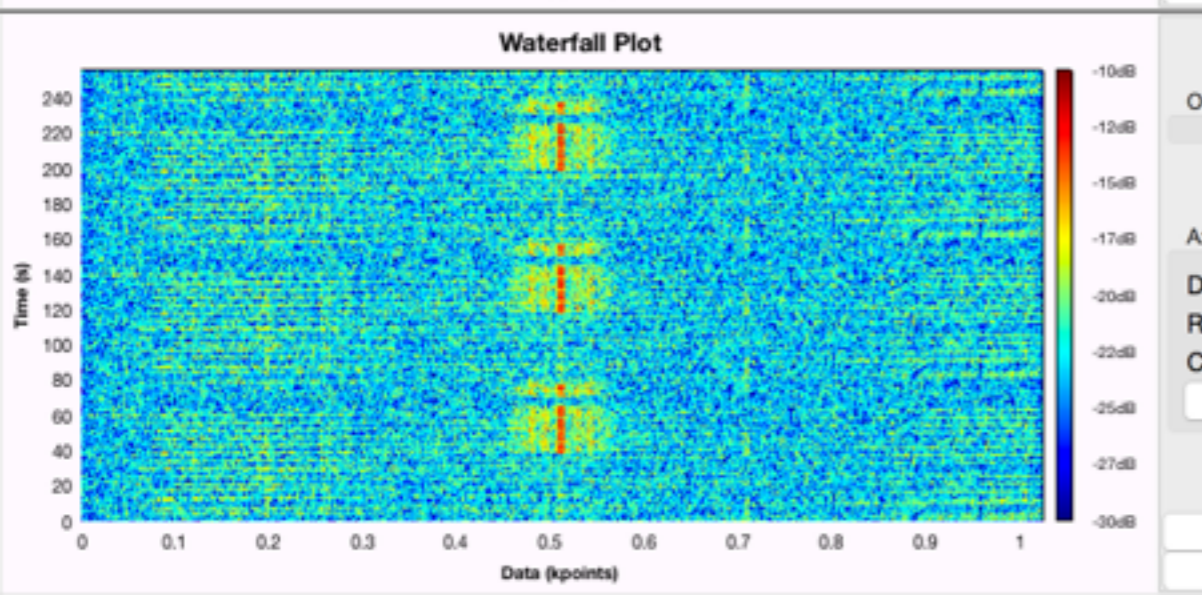
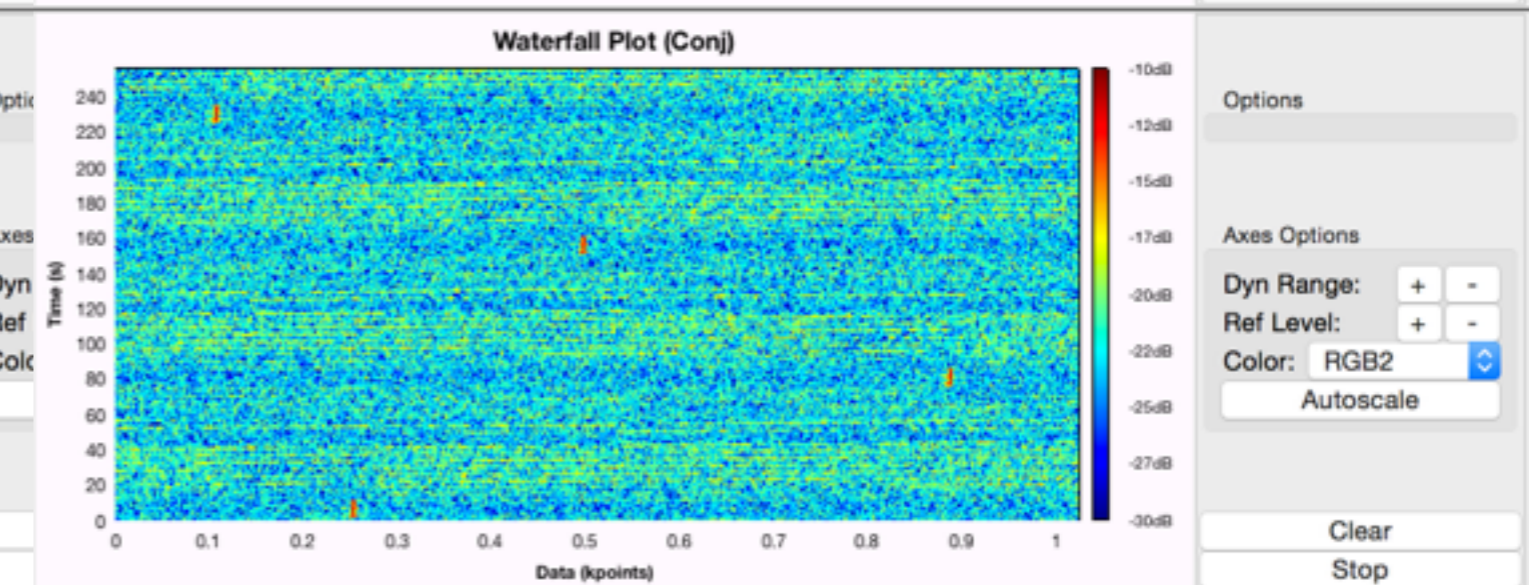
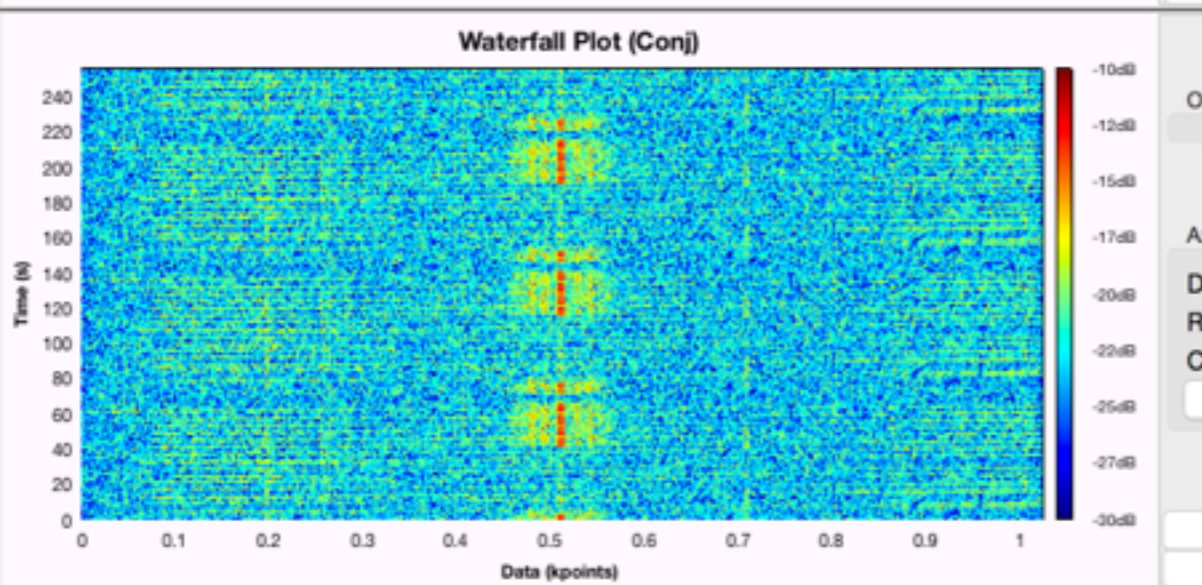
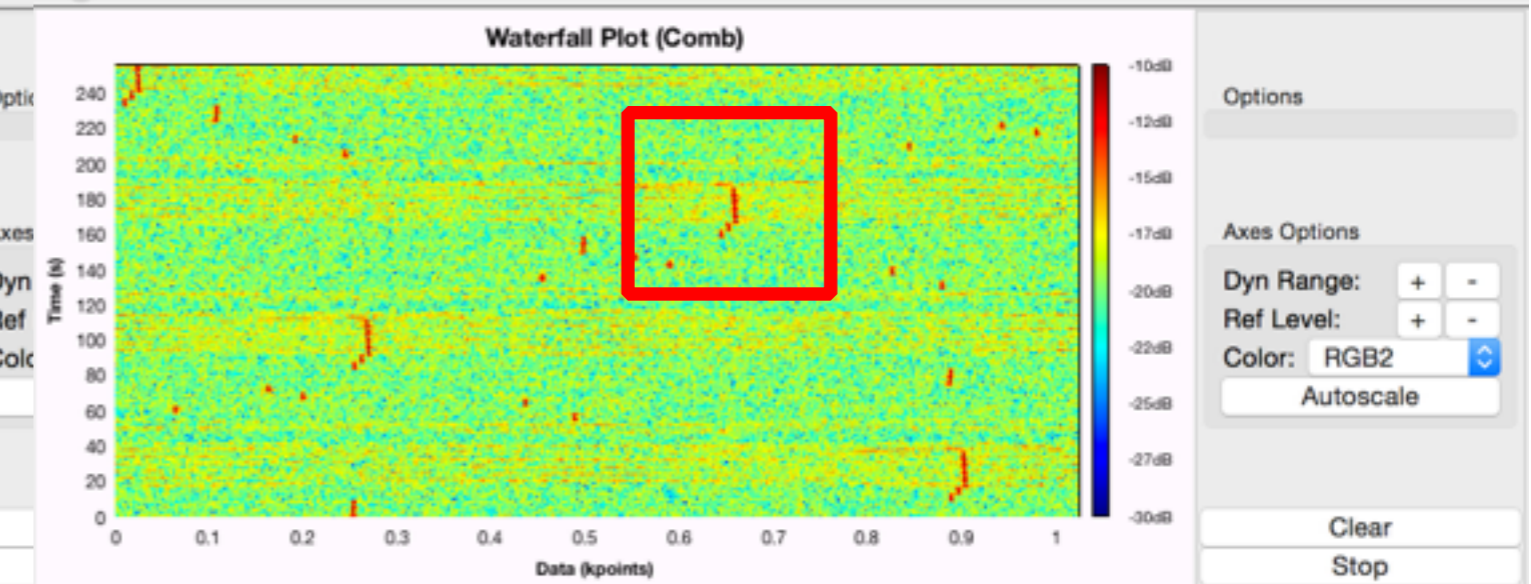
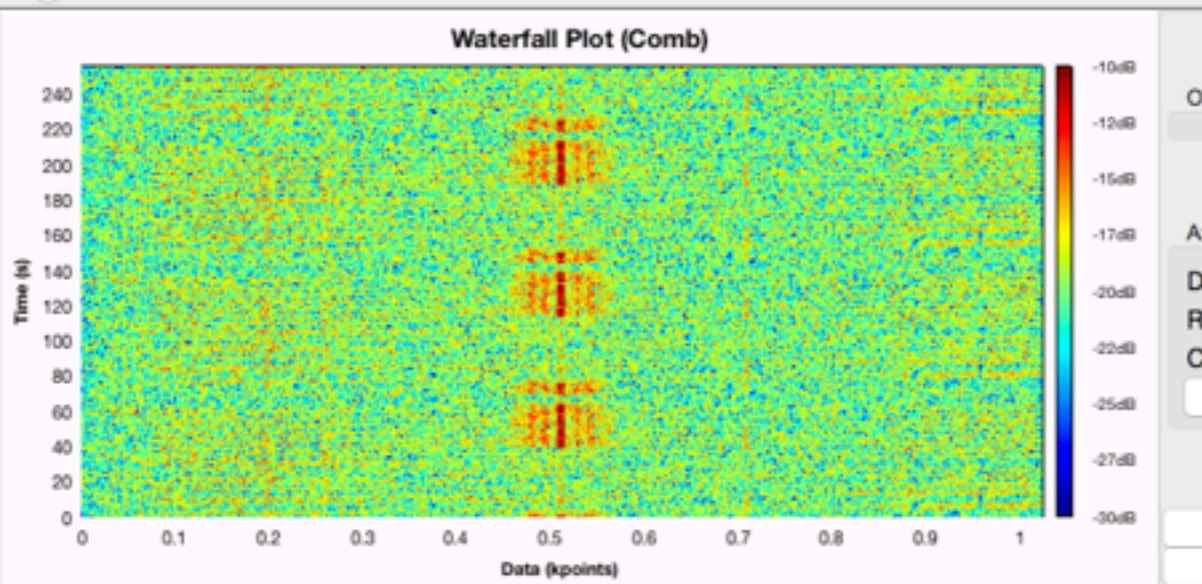


Top Block

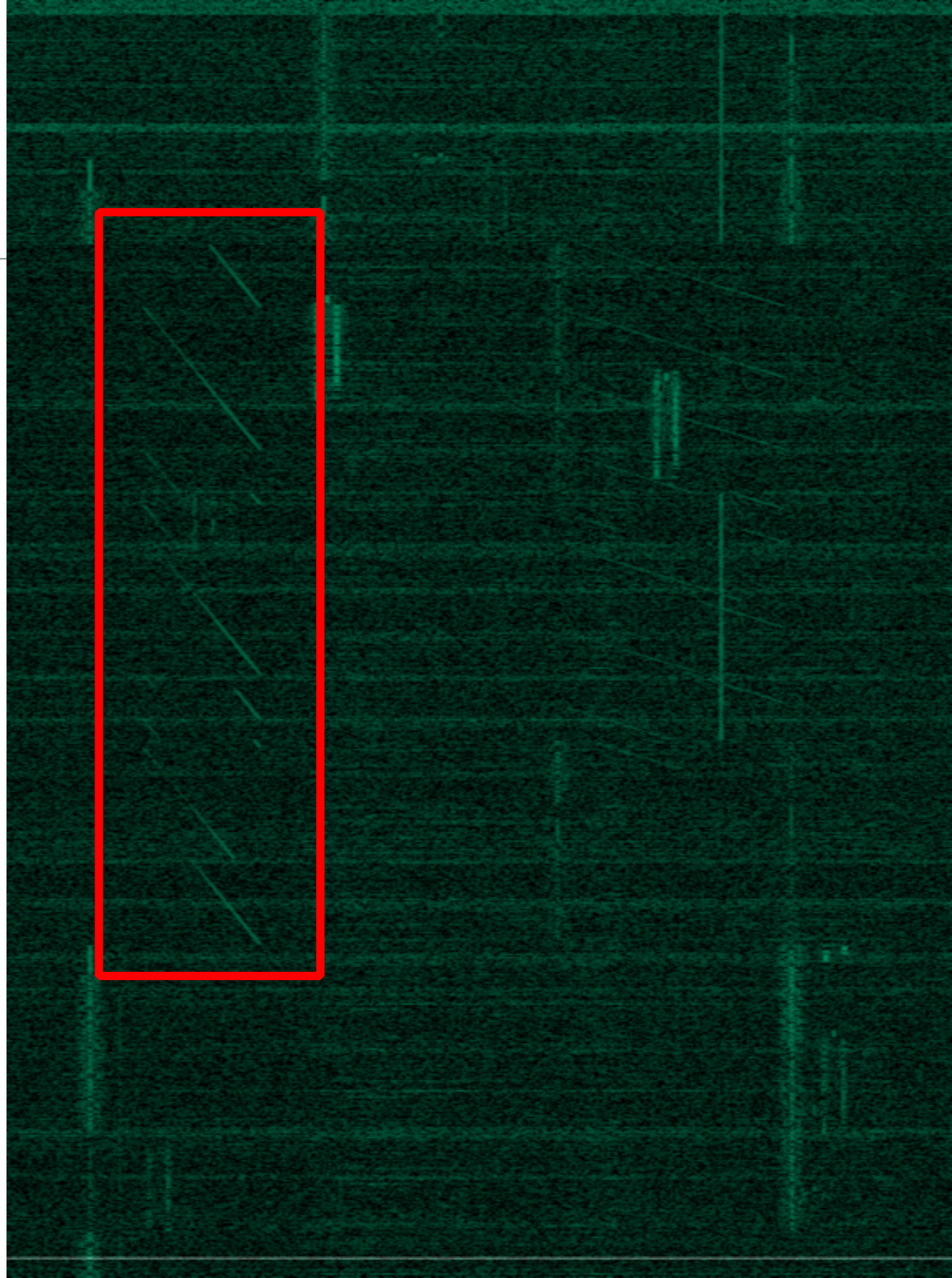
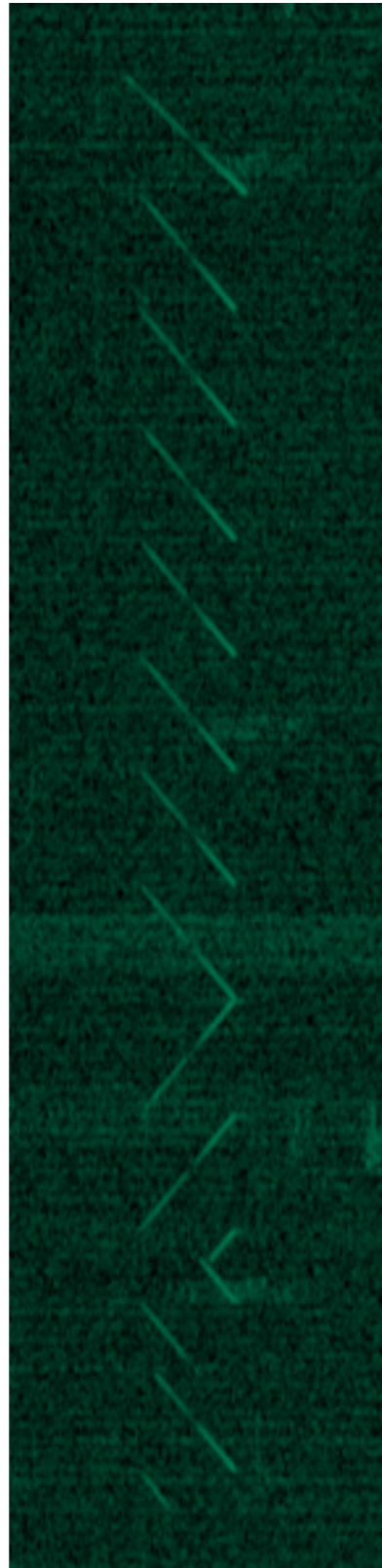
xlate_freq: 10.75M
fine: 0
f: 0
xlate_bw: 500k

Top Block

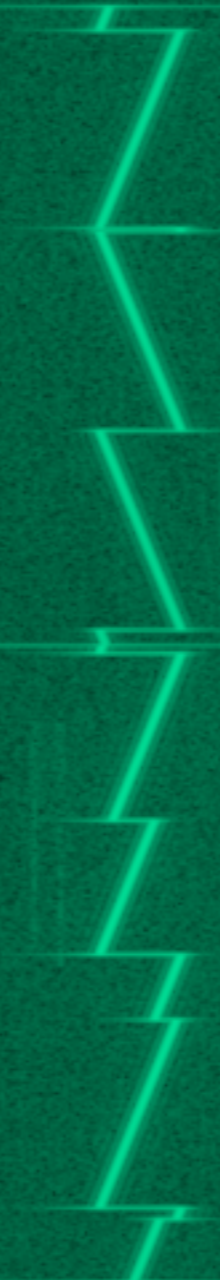
xlate_freq: 10.75M
fine: 0
f: 488.5
xlate_bw: 500k

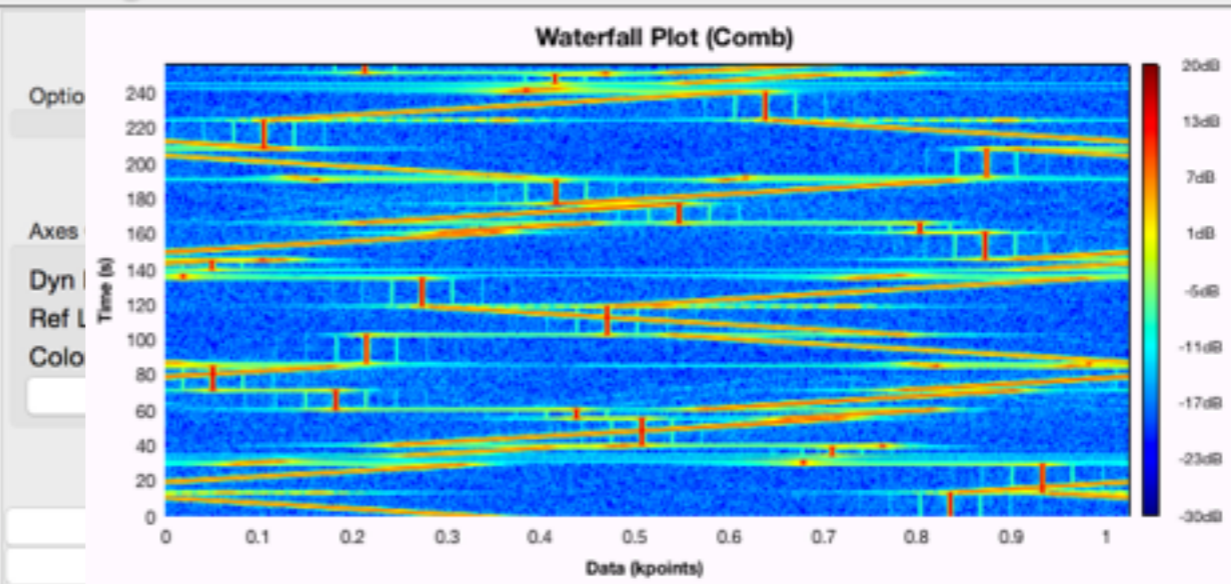
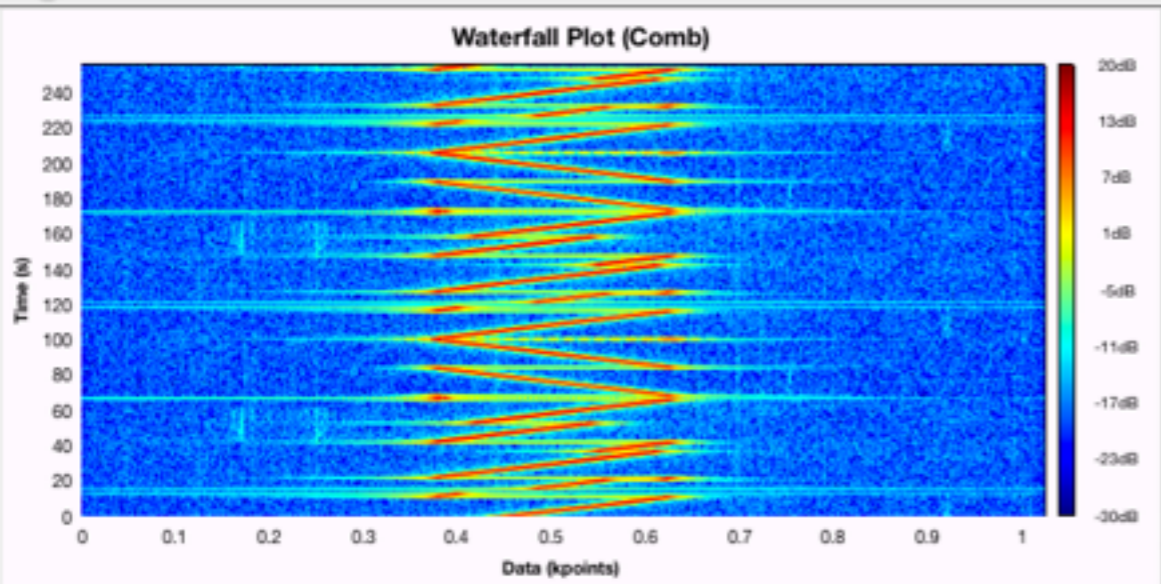


Other CSS?



Other CSS?





Options

Axes Options

Dyn Range: + -

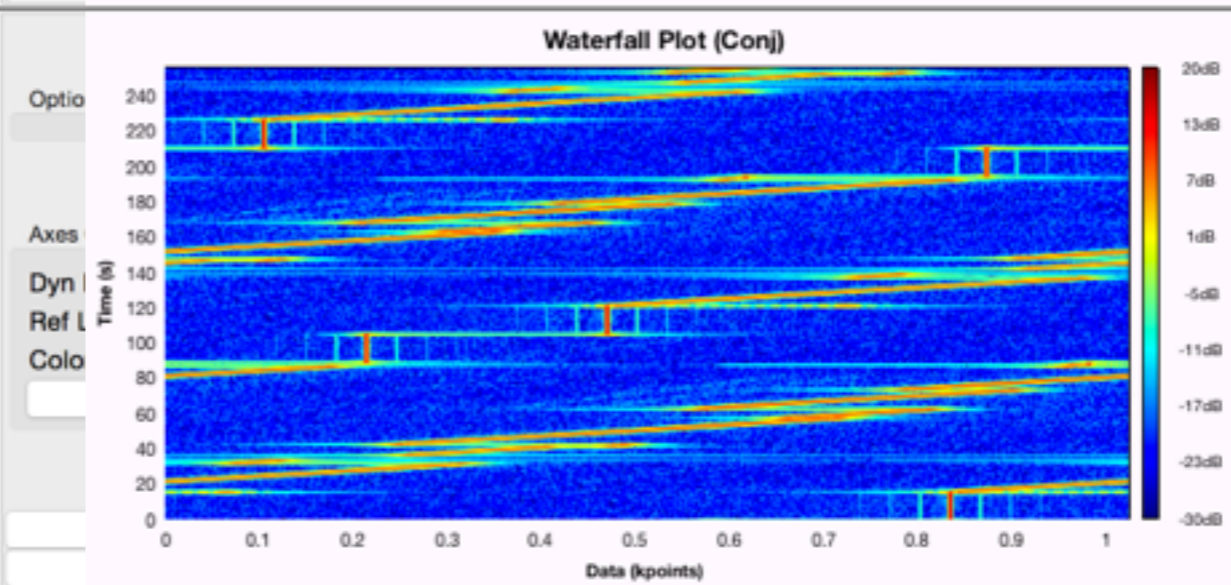
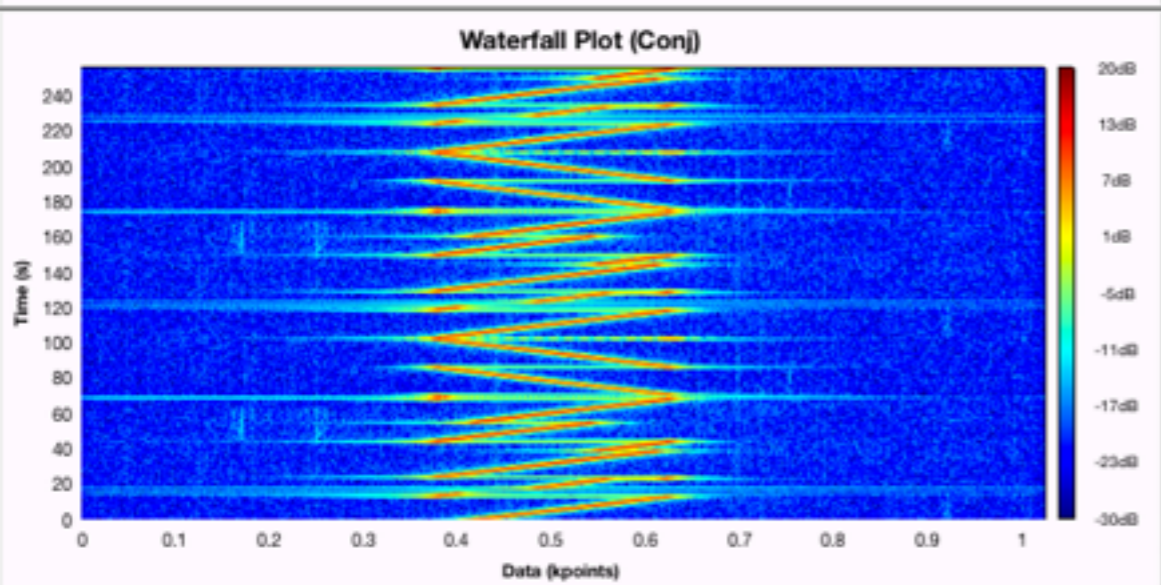
Ref Level: + -

Color: RGB2

Autoscale

Clear

Stop



Options

Axes Options

Dyn Range: + -

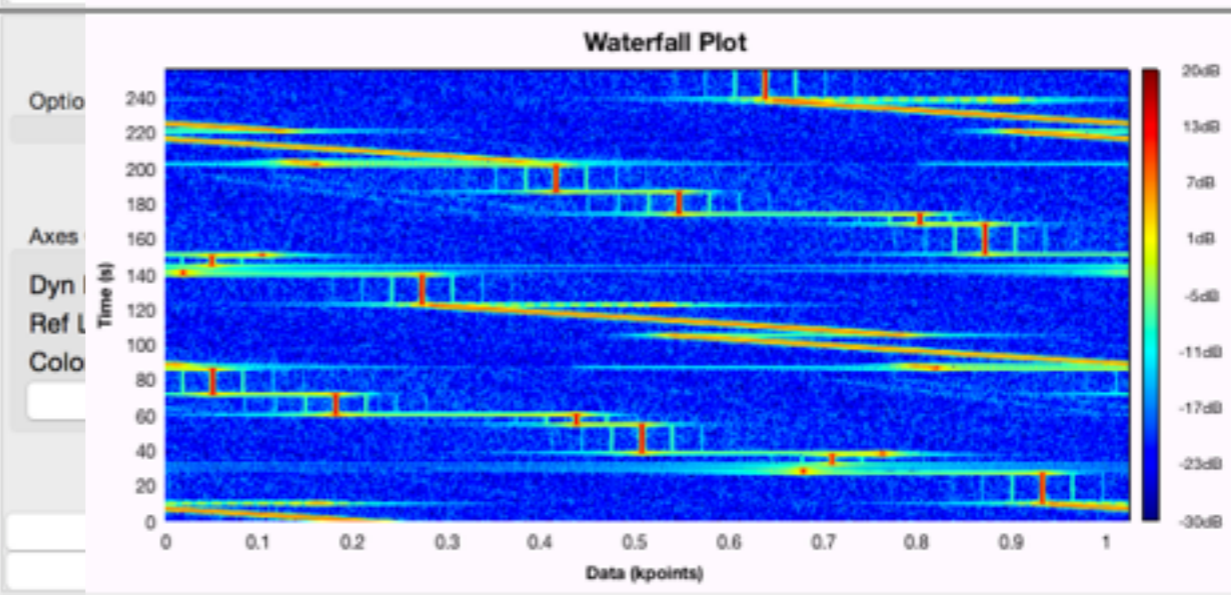
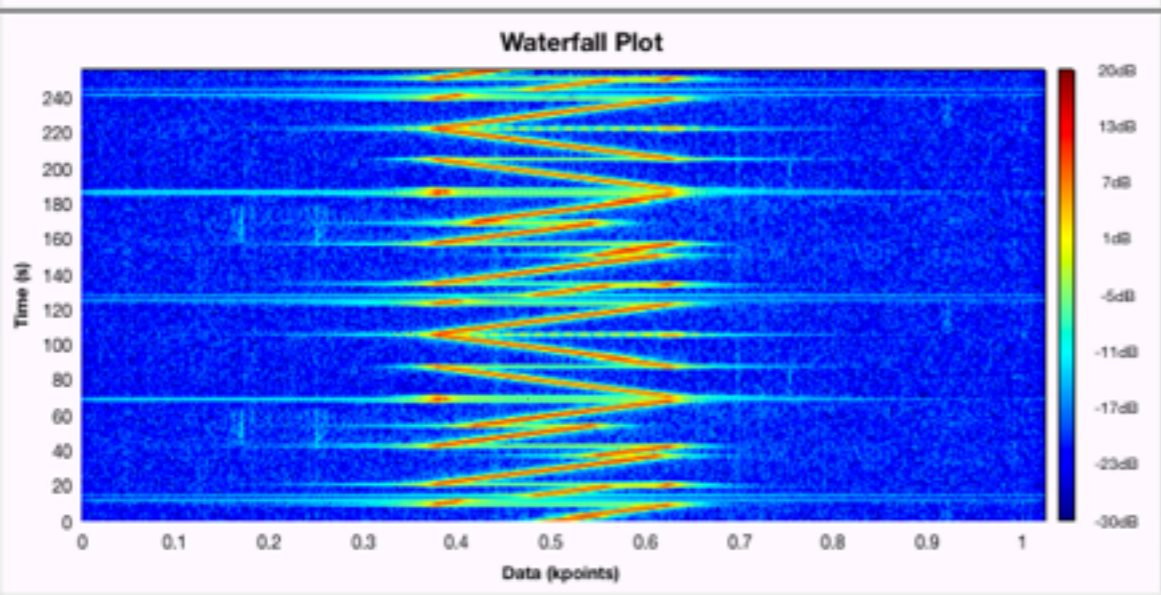
Ref Level: + -

Color: RGB2

Autoscale

Clear

Stop



Options

Axes Options

Dyn Range: + -

Ref Level: + -

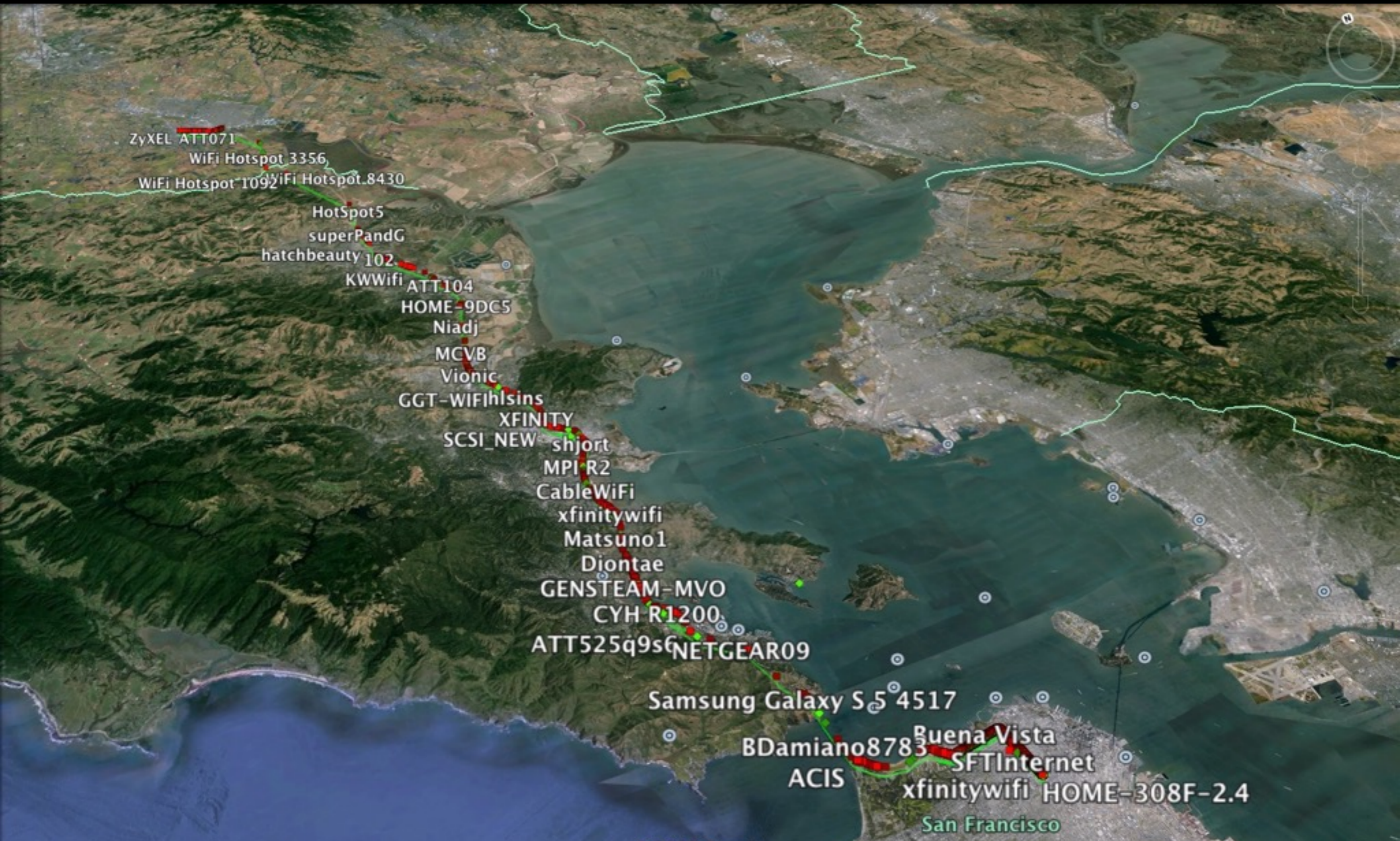
Color: RGB2

Autoscale

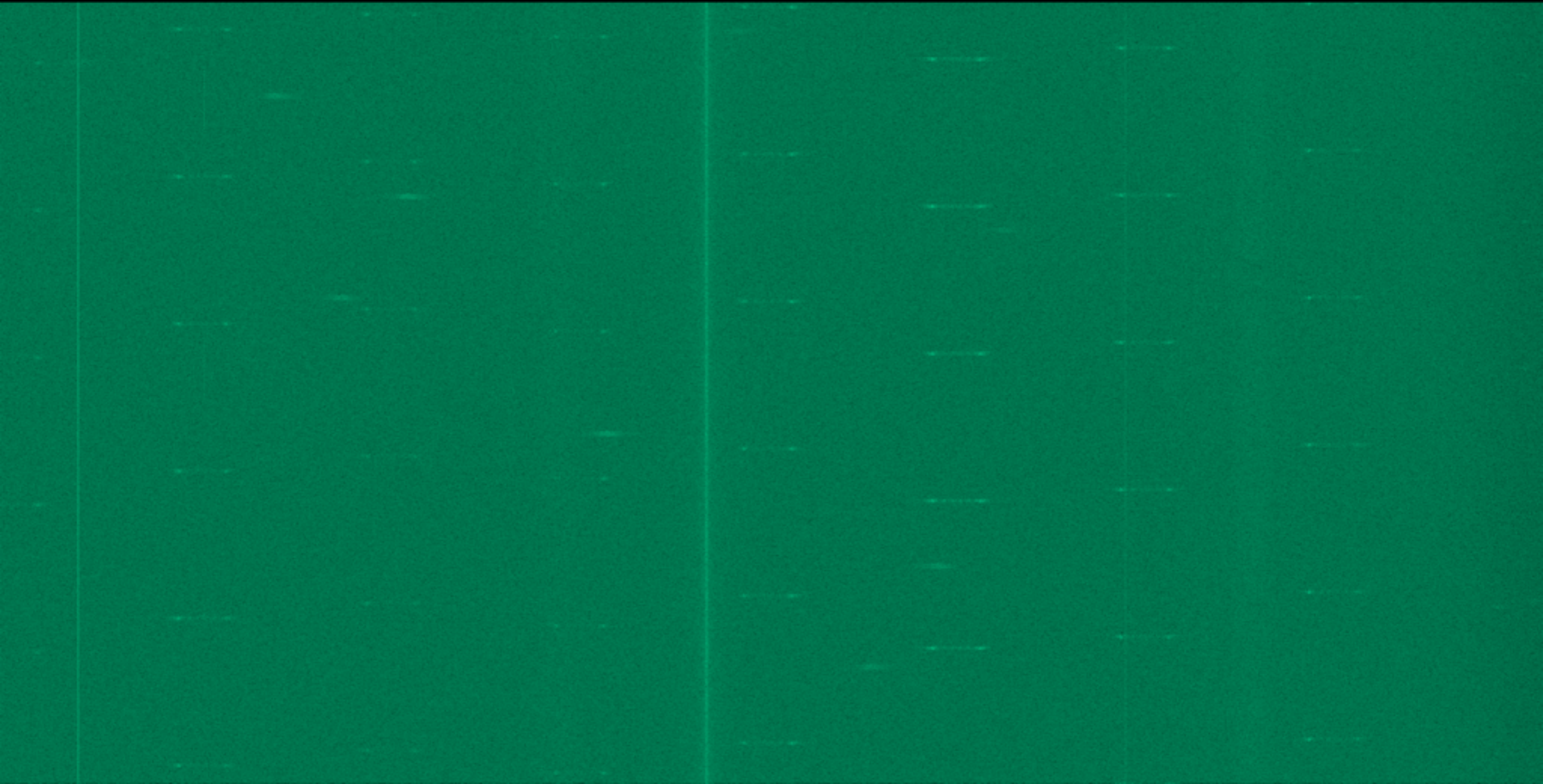
Clear

Stop

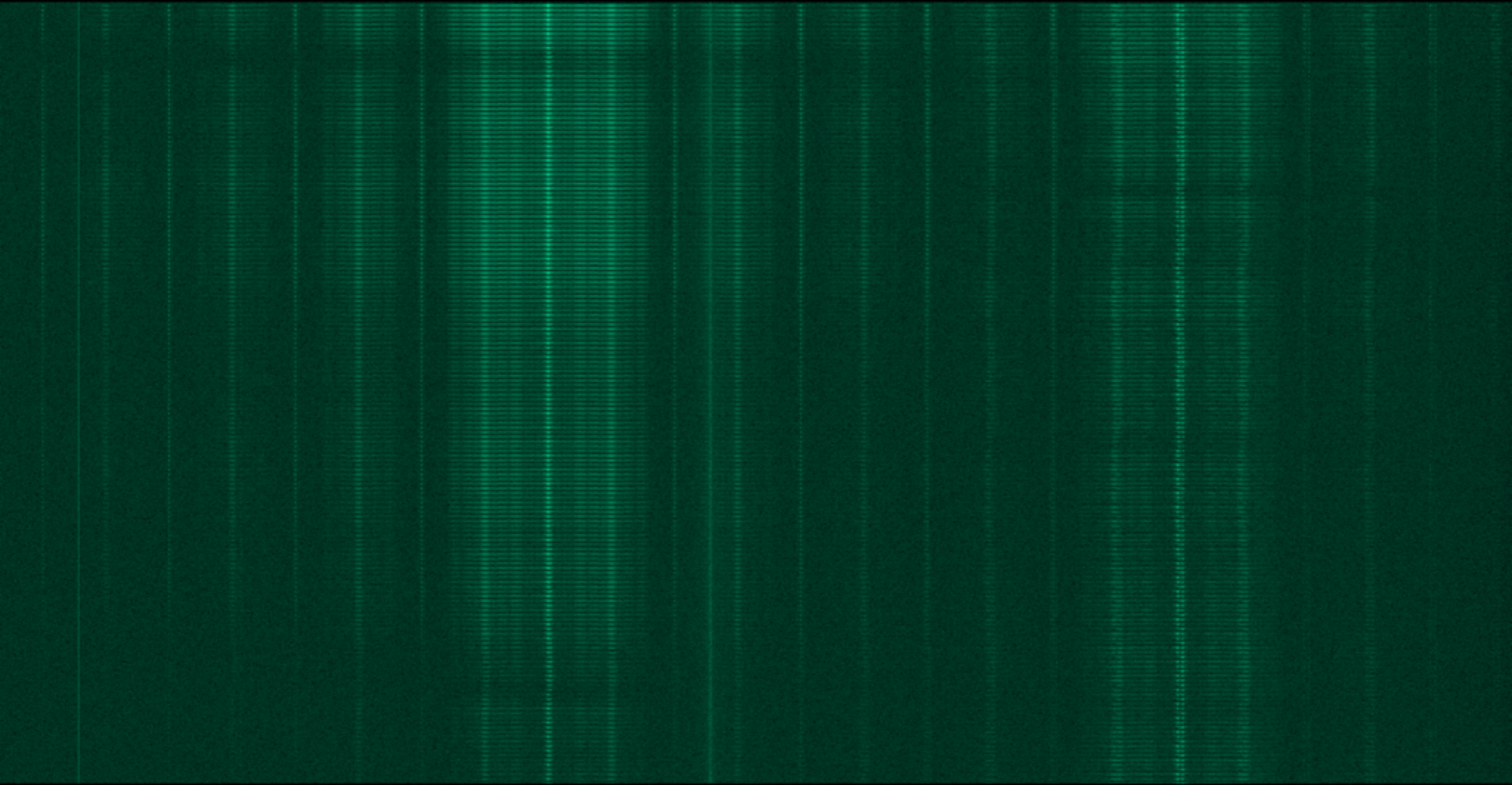
Spectrum Summary



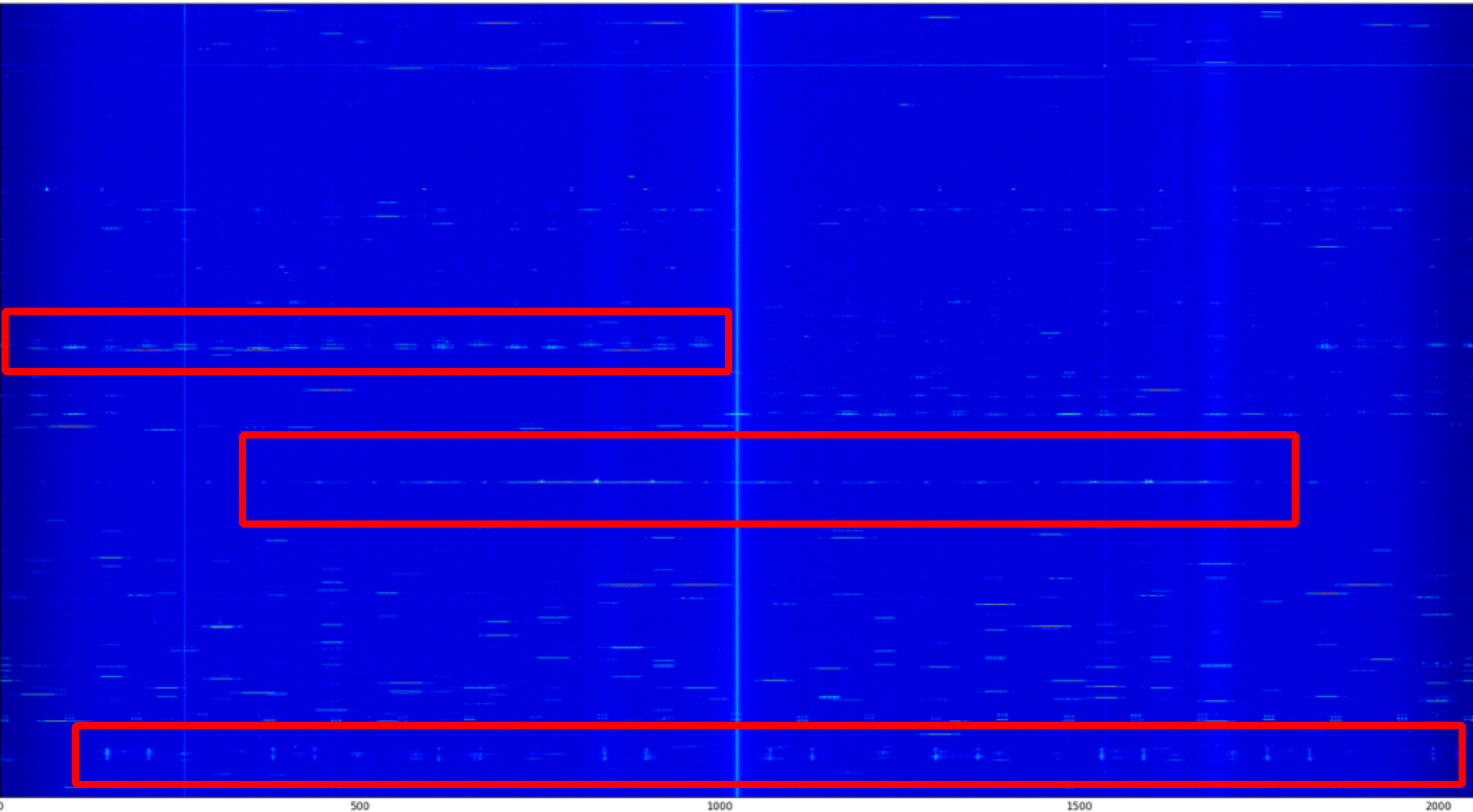
Spectrum Summary



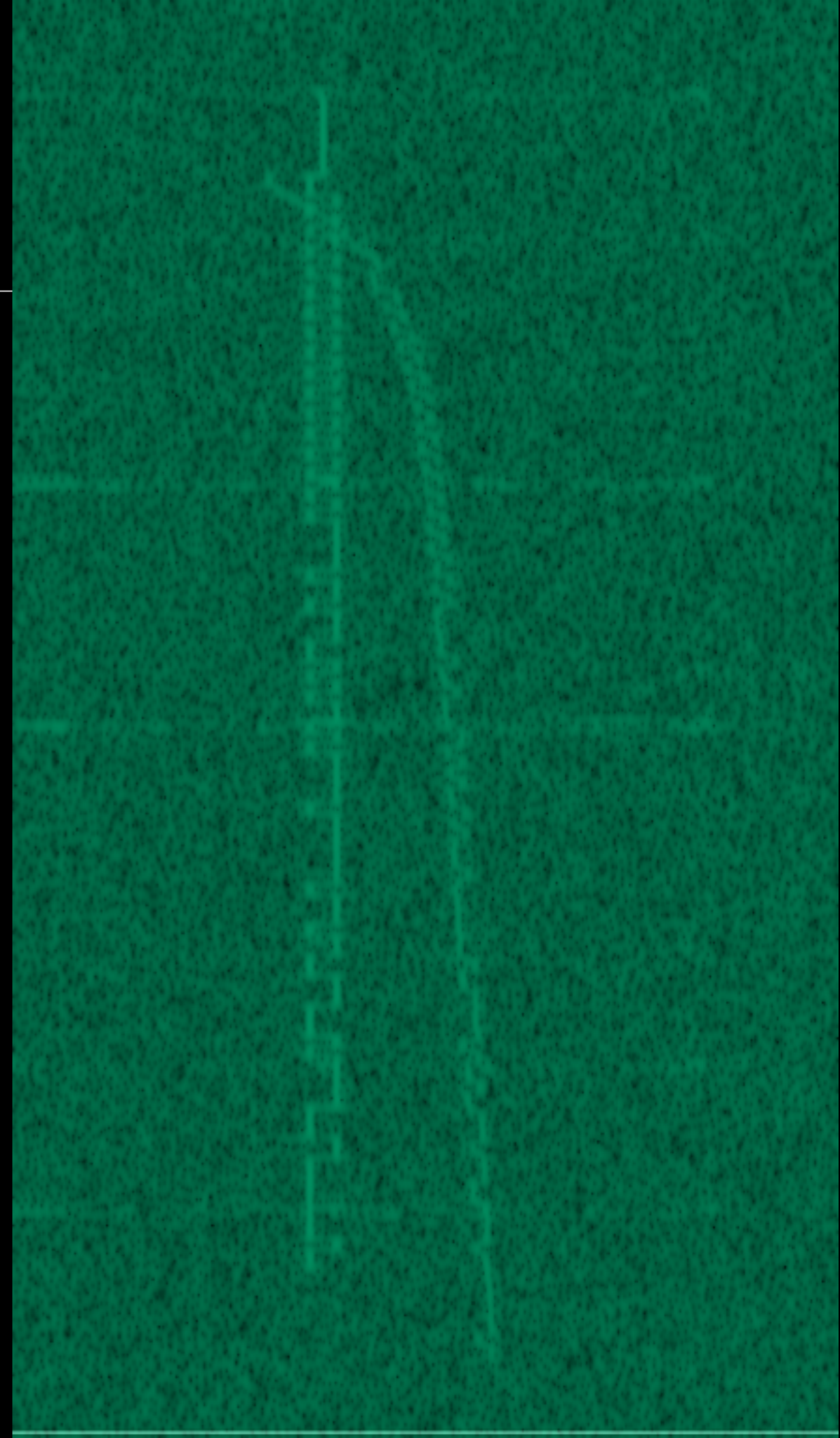
Spectrum Summary

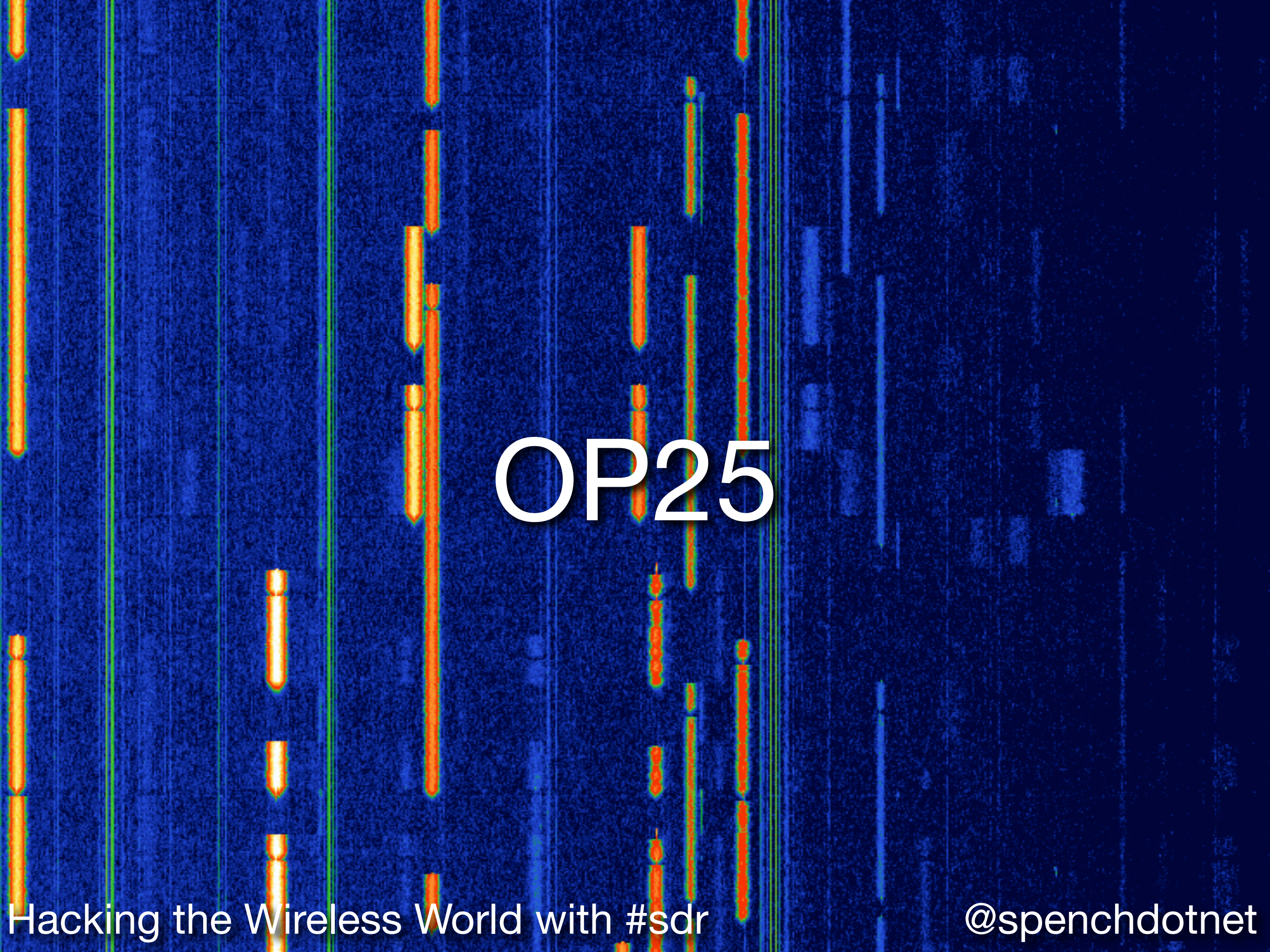


Spectrum Summary



Inebriated LO





OP25

Hacking the Wireless World with #sdr

@spenchnet

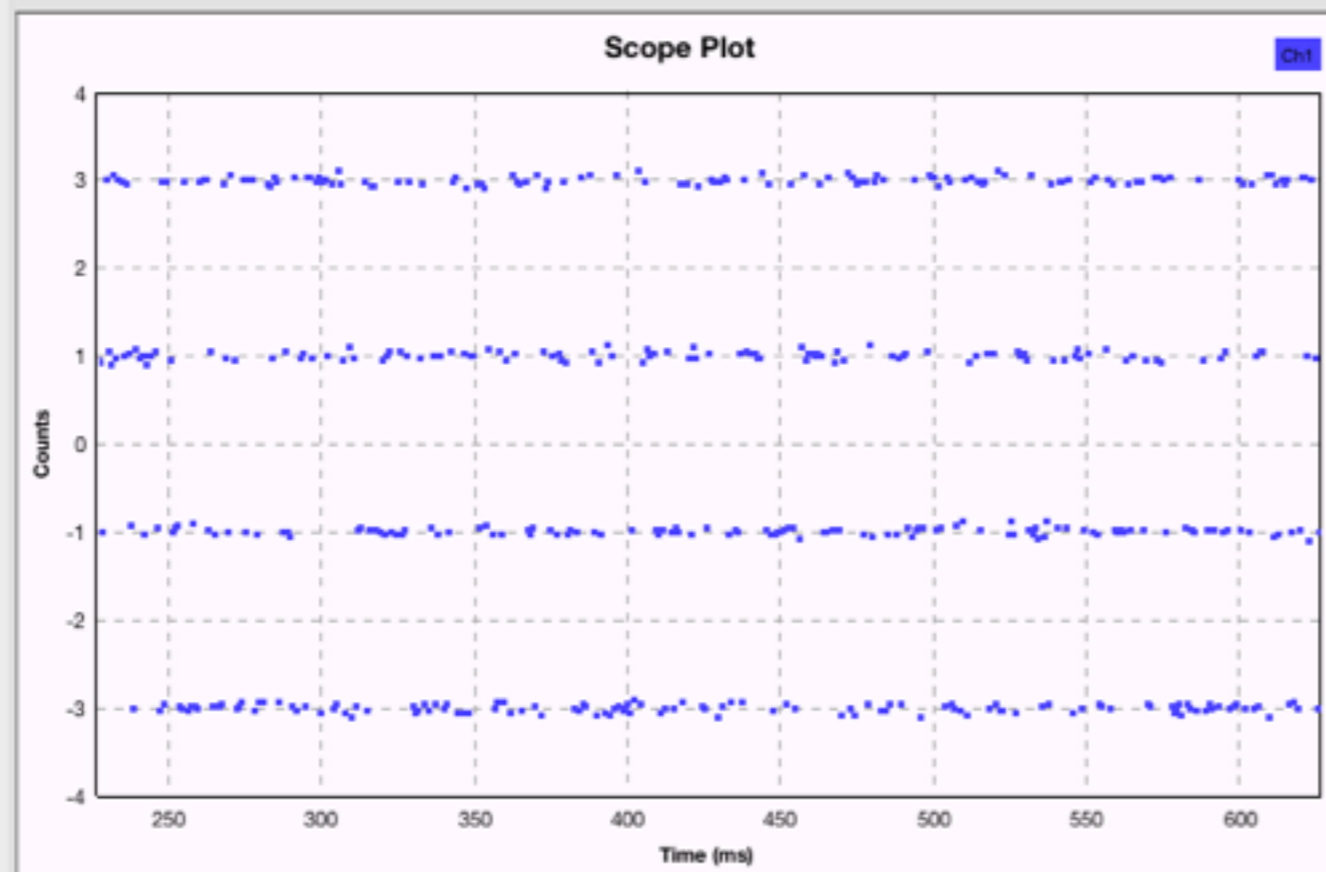
Fine Offset: 0

Xlate Offset: -19.3894k

Xlate BW: 24k

Verbose console logging

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



Persistence
Analog Alpha: 0.0004

Axes Options

Secs/Div: + -

Counts/Div: + -

Y Offset: + -

T Offset: [Slider]

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

MFID: Standard MFID (pre-20

NAC: Default NAC

ALGID: DES-OFB

Source: 0x129712

KID: 0x3780

Destination:

MI: 0xb068e81a8eb86b6400

TGID: 0x0001

Gain: 20

Properties: OP25 Decoder (Simple)

General

Advanced

Documentation

ID

op25_decoder_simple_0

Key (hex)

Key map (hex)

Idle silence

Output traffic

[Redacted]

{0x3780: "C [Redacted] 4"}

No

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
```

This

This

Cyberspectrum: Bay Area Software Defined Radio

Home Members Sponsors Photos Pages Discussions More

Group tools My profile



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

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](#)

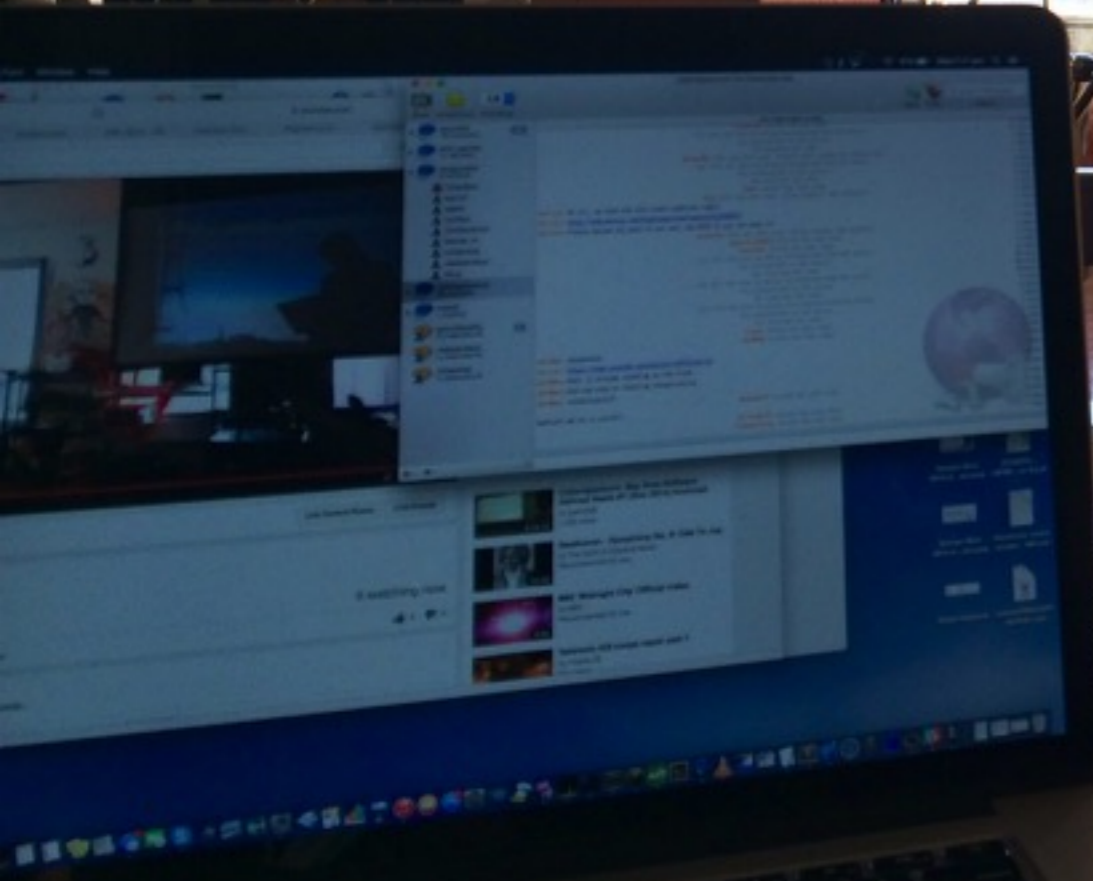
RSVPed Yes for
Cyberspectrum #6: San Francisco

6 days ago

Recent Meetups



Cyberspectrum #6



Thank you!



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

@spenchnet
balint@bastille.io

GitHub: balint256
GitHub: RFStorm

Bastille