Hacking the Wireless World: Software Defined Radio Exploits

Balint Seeber
Director of Vulnerability Research
Bastille

Overview

- Aviation
- RDS TMC
- Radio Direction Finding
- OP25
- IoT
- SATCOM
- ISEE-3 Reboot Mission

Aviation


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

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

Position

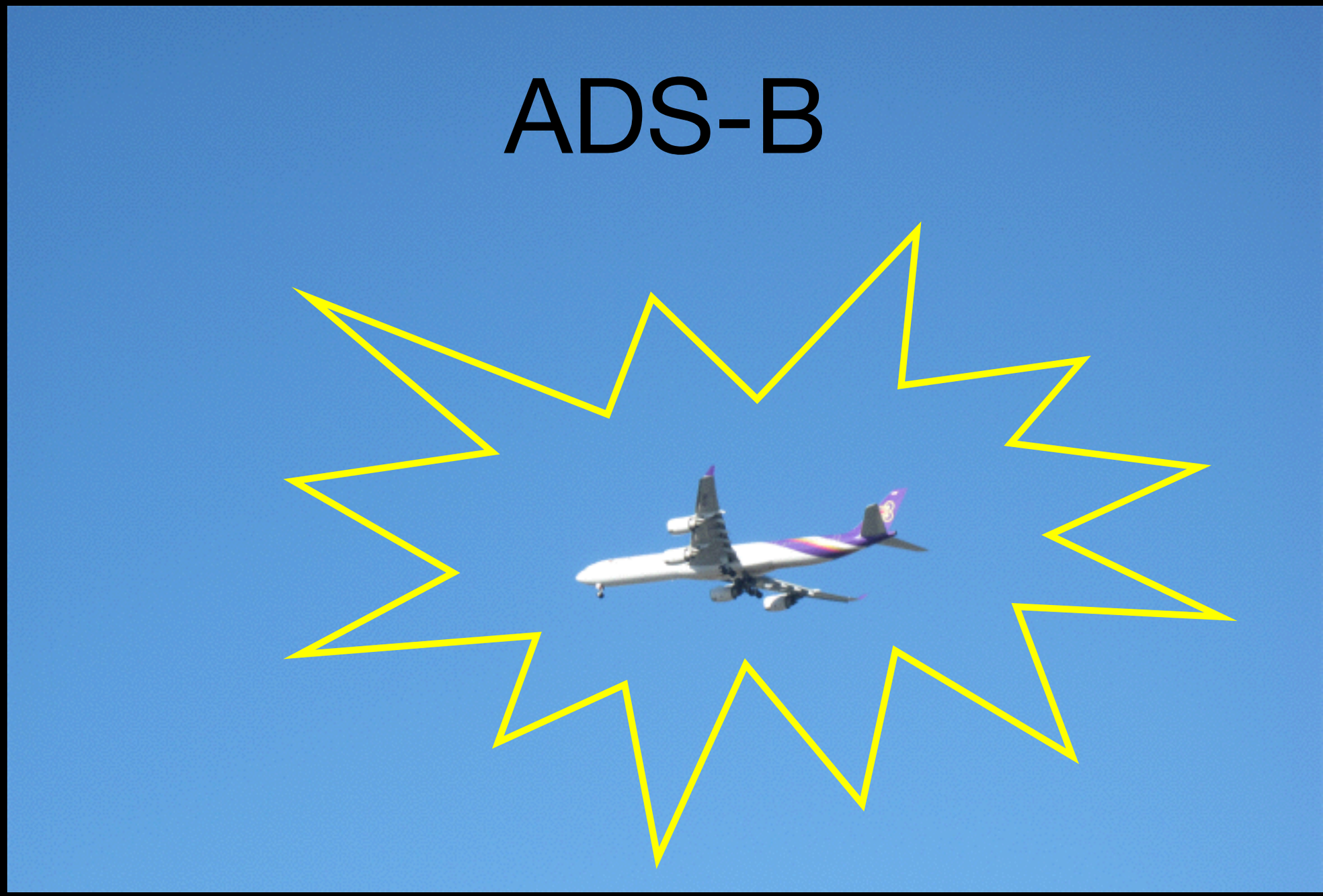
Heading

Altitude

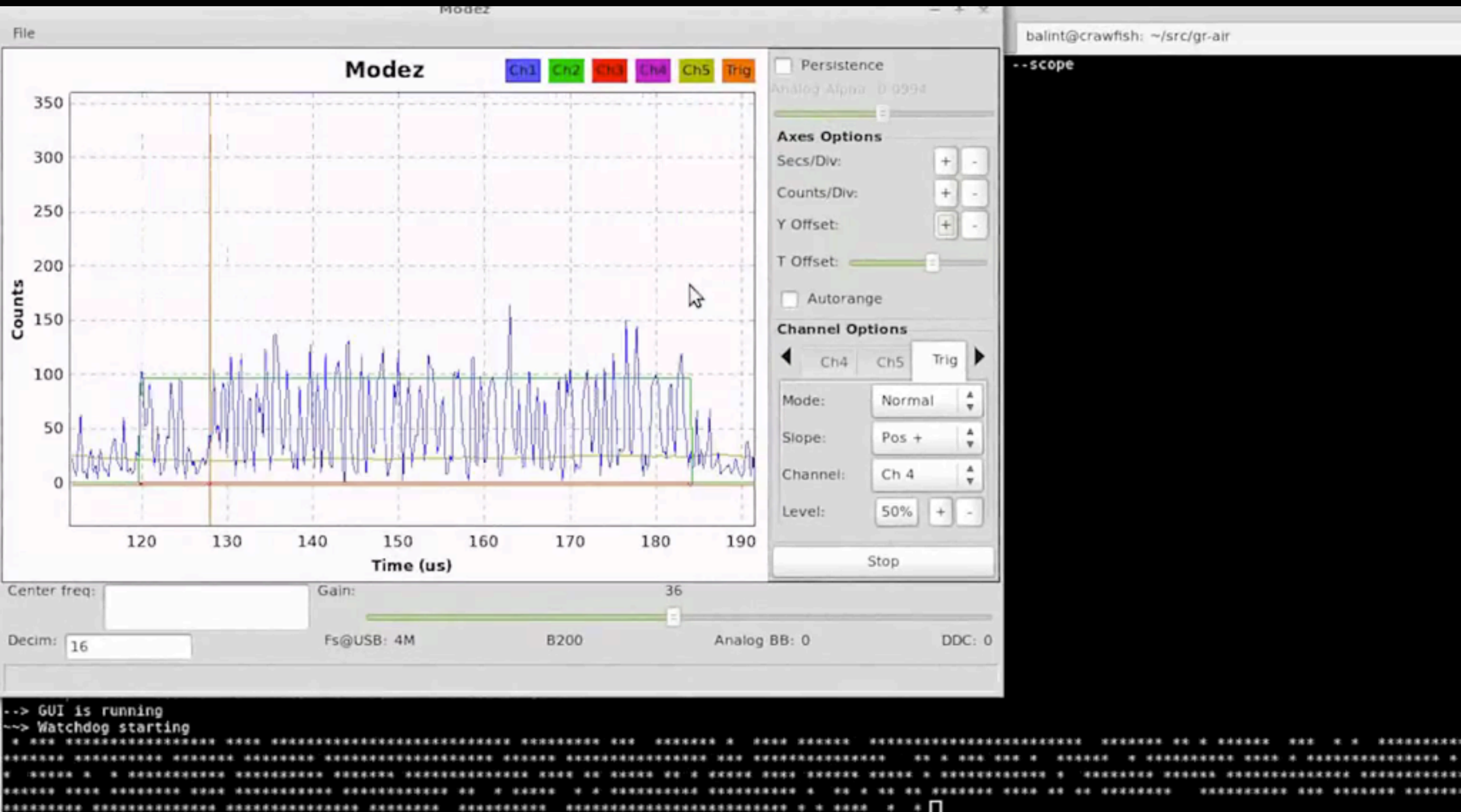
Vertical rate

Flight ID

Squawk code

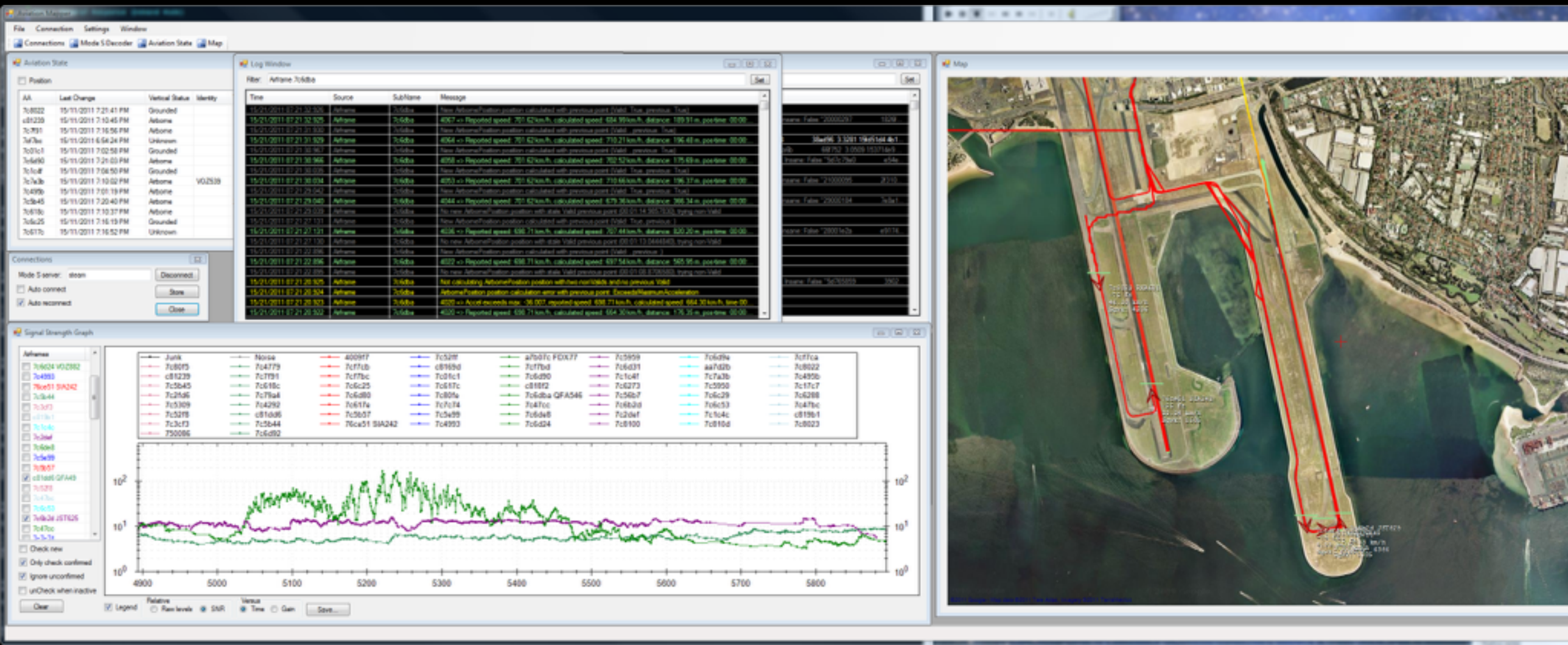


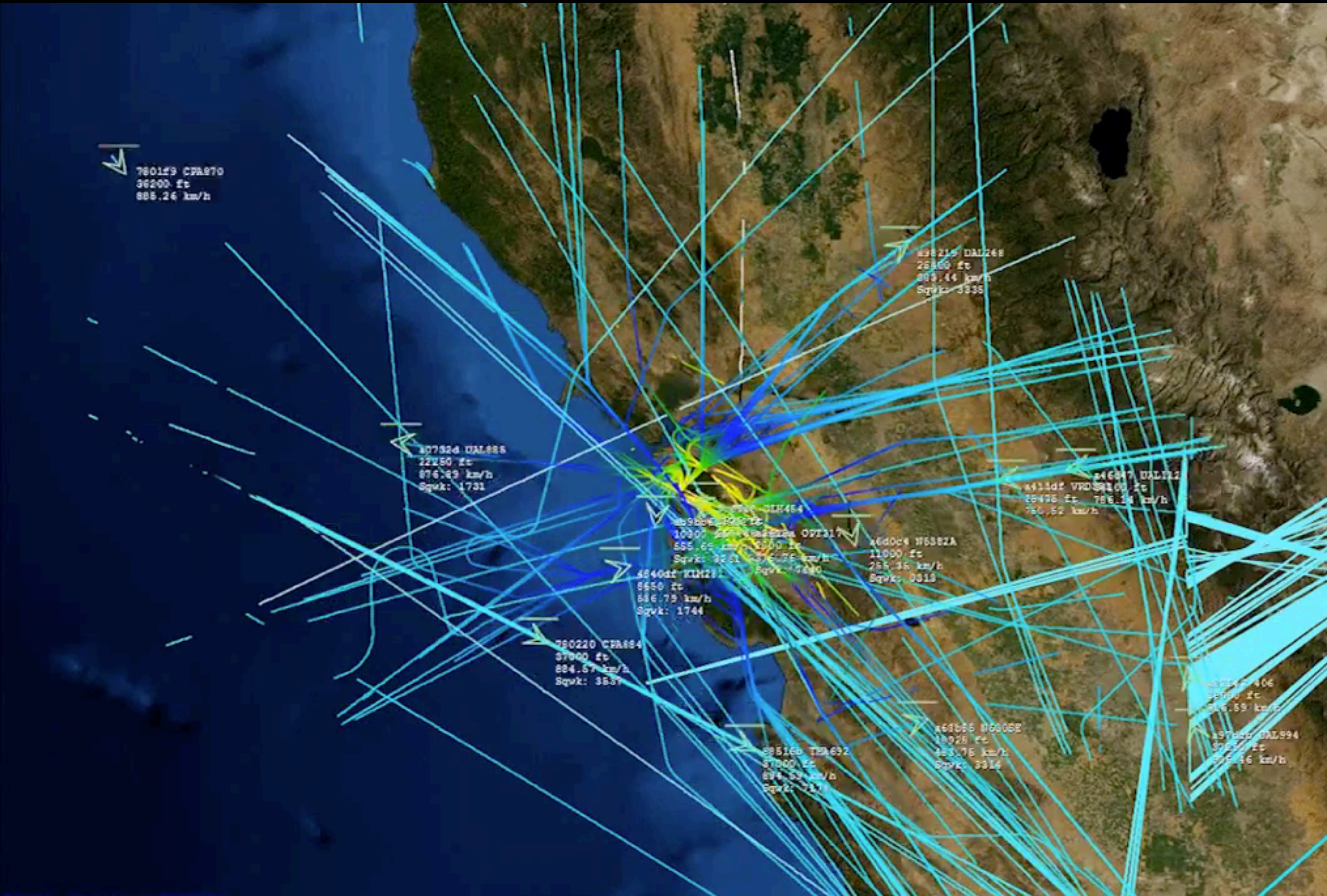
Mode S Decoder



Aviation **Map**per

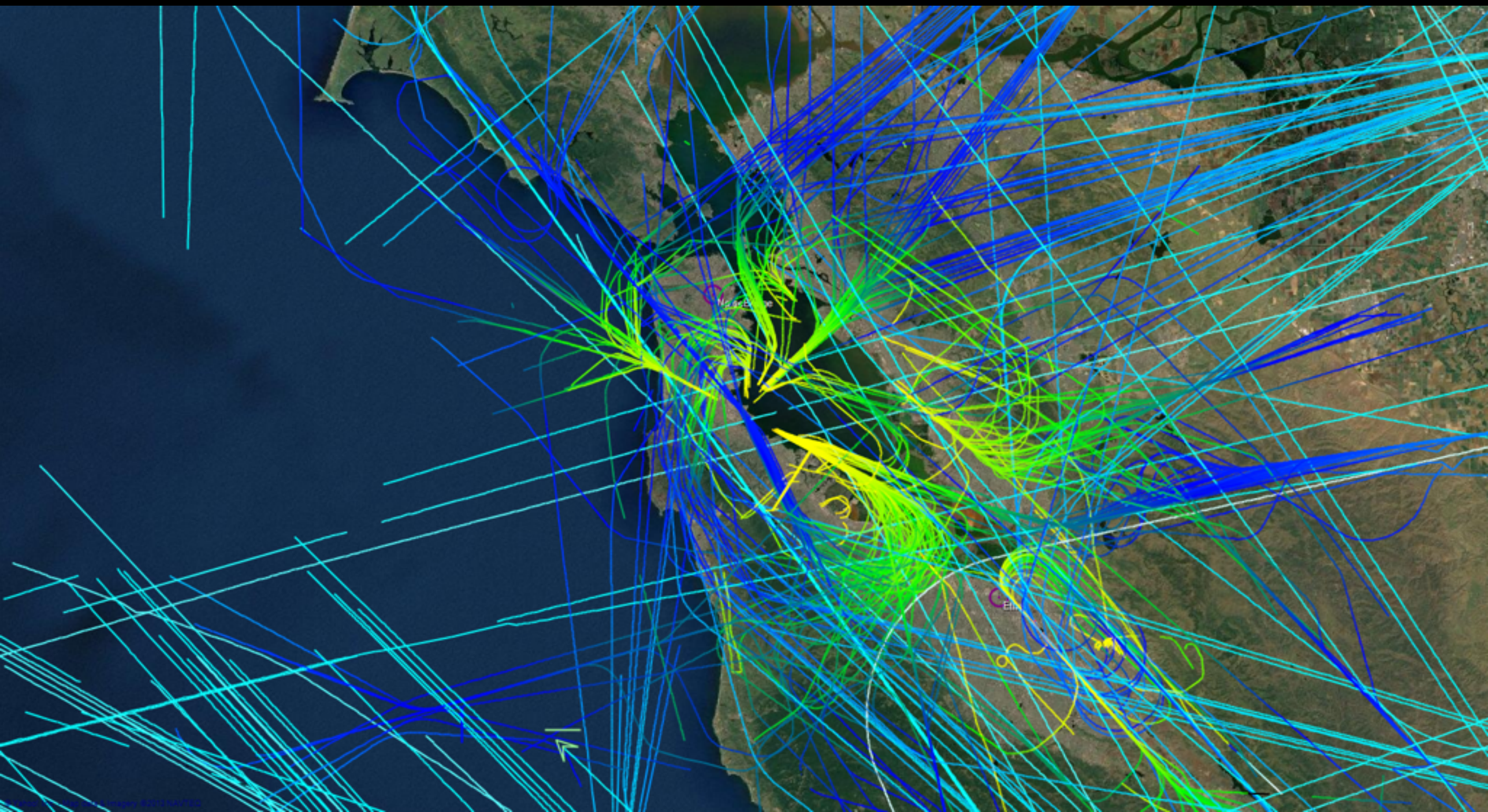
- Connects to Mode S decoder server
- Tracks & plots airframes, collects statistics
- Provides state server for web streaming



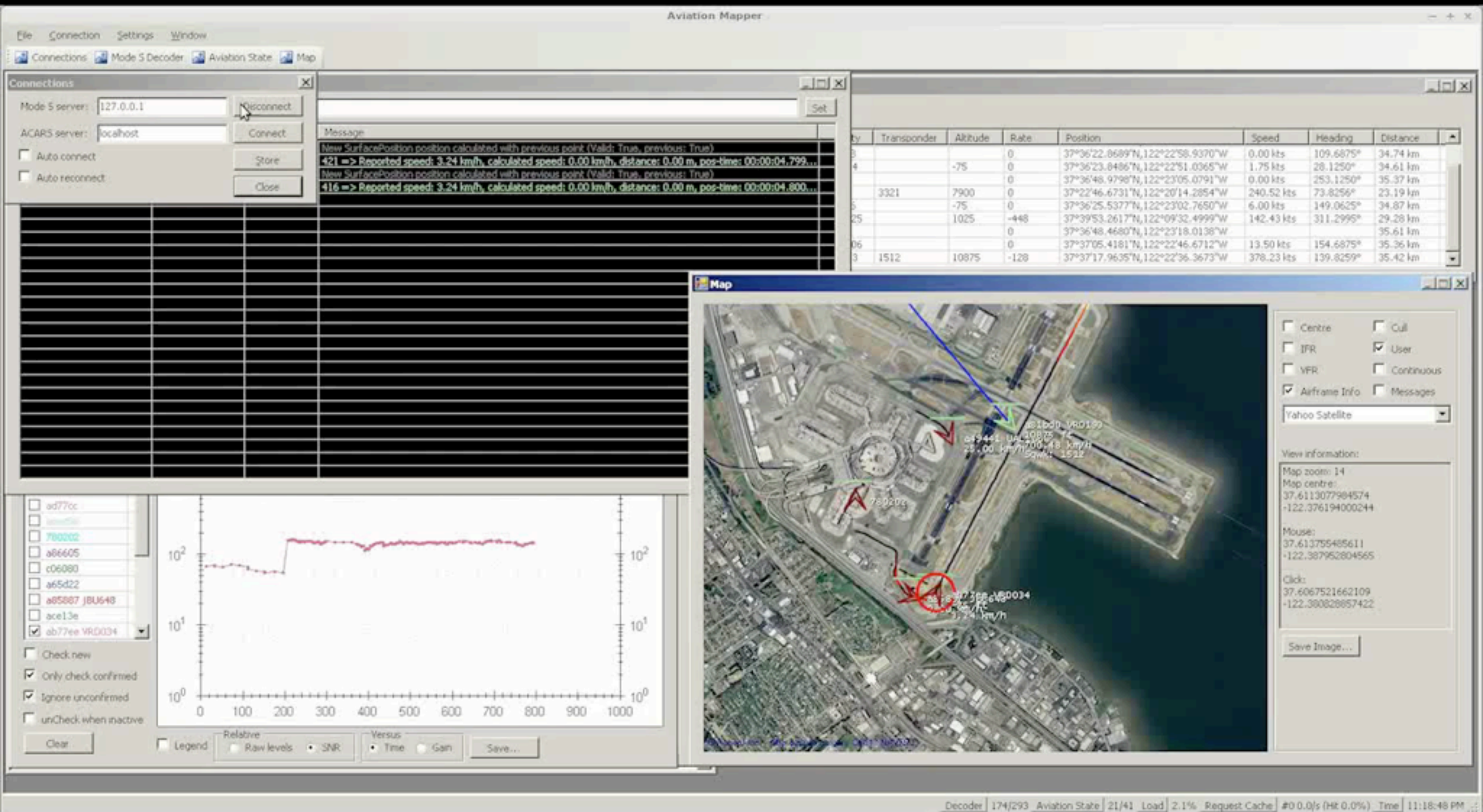


7801f9 CPA870
36200 ft
886.26 km/h
a07324 UAL885
22250 ft
876.69 km/h
Sqwk: 1731
4840df KLM281
8650 ft
686.79 km/h
Sqwk: 1744
780220 CPA884
37000 ft
884.57 km/h
a6d0c4 N6382A
11000 ft

Aircraft Trails with Colour-coded Altitude



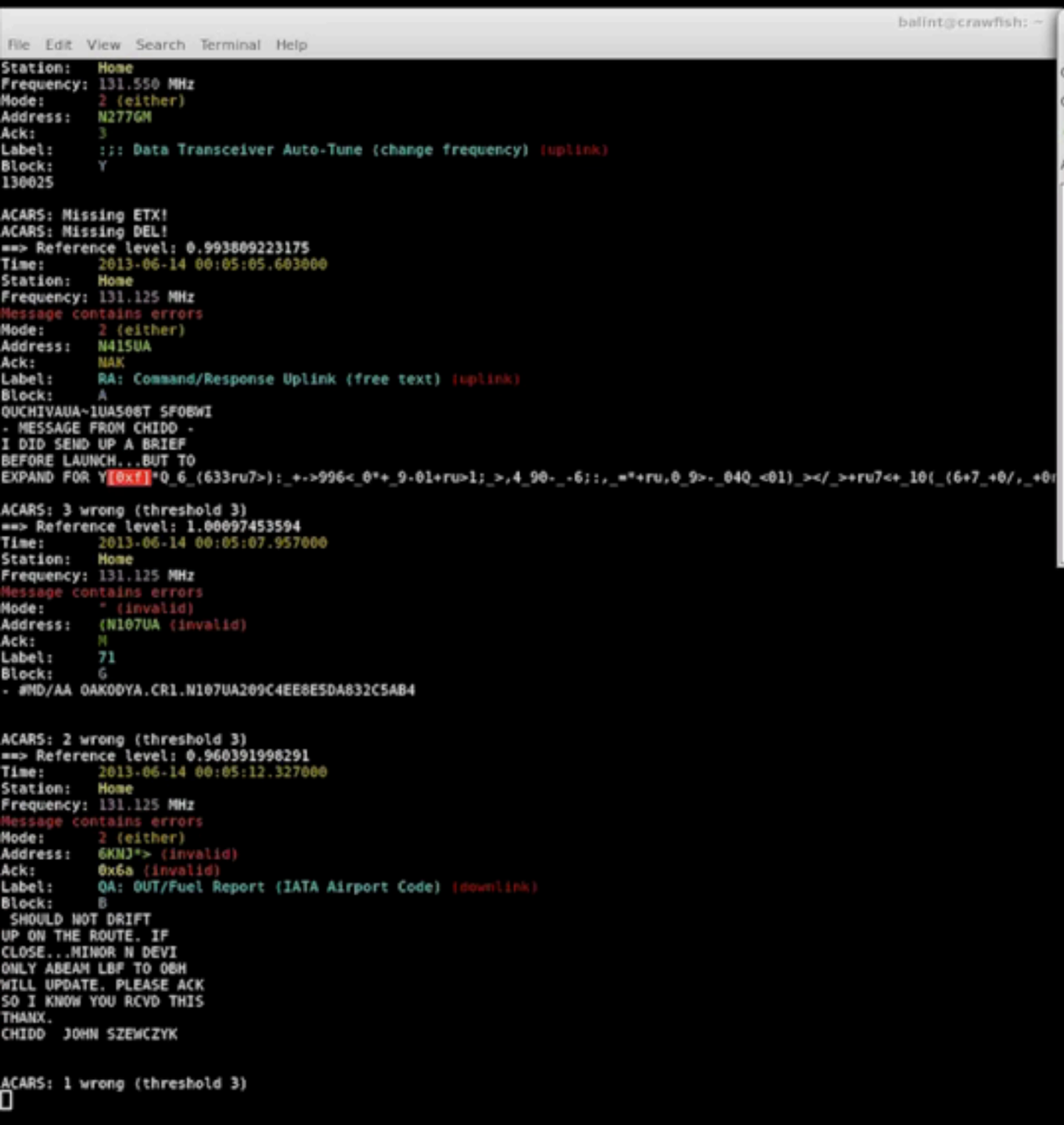
Takeoff at SFO



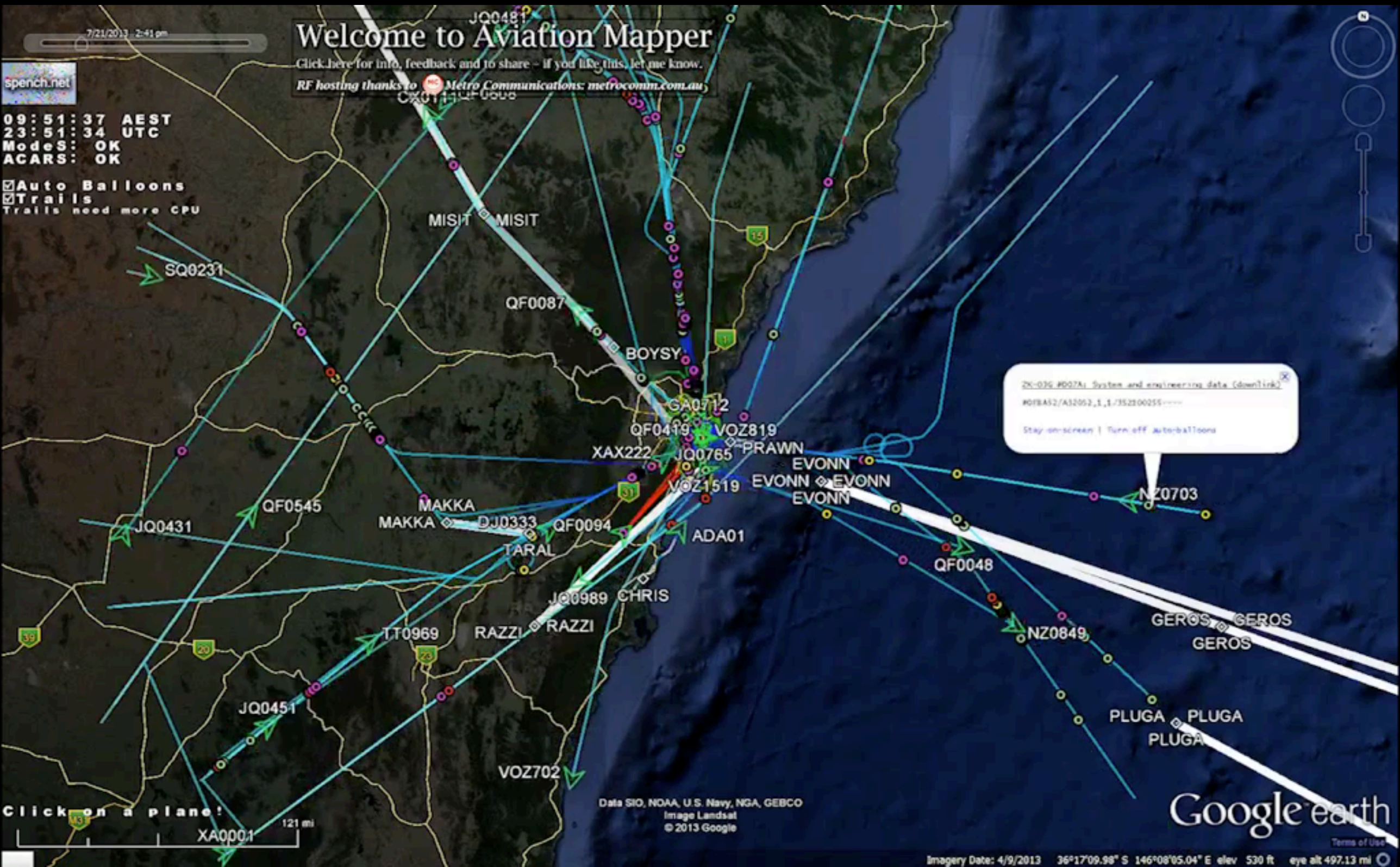
Takeoff at SFO

Takeoff at SFO (Cockpit View)

ACARS Decoder



Combined Mode S & ACARS



‘Engineering’ Status Messages over ACARS

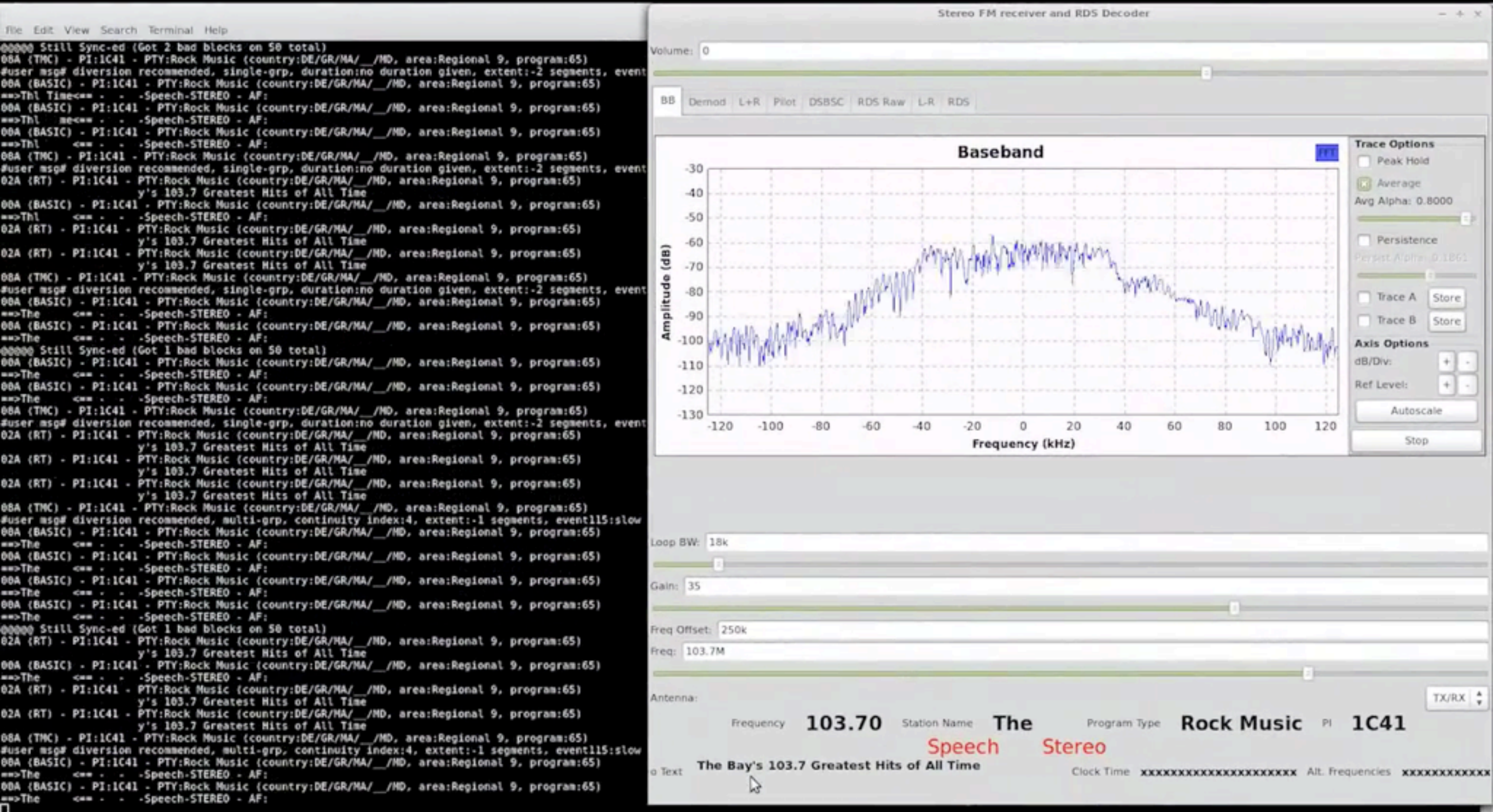
Waypoints Transmitted over ACARS

RDS TMC

Hacking the Wireless World with #sdr

@spenchdotnet

Stereo FM with RDS: Receiver



Radio Data Service

Traffic Message Channel

Traffic Message Channel

```
#user msg# single-grp, duration:15 minutes, diversion recommended, extent:-2 segments, event:74 [41]:traffic congestion, average speed of 50 km/h, location:1862
#user msg# single-grp, duration:15 minutes, diversion recommended, extent:-2 segments, event:74 [41]:traffic congestion, average speed of 50 km/h, location:1862
#user msg# single-grp, duration:15 minutes, diversion recommended, extent:-2 segments, event:74 [41]:traffic congestion, average speed of 50 km/h, location:1862
#user msg# single-grp, duration:15 minutes, diversion recommended, extent:2 segments, event:72 [39]:traffic congestion, average speed of 30 km/h, location:22340
#user msg# single-grp, duration:15 minutes, diversion recommended, extent:2 segments, event:72 [39]:traffic congestion, average speed of 30 km/h, location:22340
#user msg# single-grp, duration:15 minutes, diversion recommended, extent:2 segments, event:803 [823]:(Q sets of) construction work, location:62276
#user msg# single-grp, duration:15 minutes, diversion recommended, extent:2 segments, event:803 [823]:(Q sets of) construction work, location:62276
#user msg# single-grp, duration:15 minutes, diversion recommended, extent:1 segments, event:1120 [1592]:(Q probability of) sunny periods, location:58180
#user msg# single-grp, duration:15 minutes, diversion recommended, extent:1 segments, event:1120 [1592]:(Q probability of) sunny periods, location:58180
#user msg# single-grp, duration:15 minutes, diversion recommended, extent:1 segments, event:1120 [1592]:(Q probability of) sunny periods, location:58180
#user msg# single-grp, duration:15 minutes, diversion recommended, extent:2 segments, event:75 [42]:traffic congestion, average speed of 60 km/h, location:56133
#user msg# single-grp, duration:15 minutes, diversion recommended, extent:-3 segments, event:73 [40]:traffic congestion, average speed of 40 km/h, location:65344
#user msg# single-grp, duration:15 minutes, diversion recommended, extent:-3 segments, event:73 [40]:traffic congestion, average speed of 40 km/h, location:65344
#user msg# single-grp, duration:15 minutes, diversion recommended, extent:2 segments, event:76 [43]:traffic congestion, average speed of 70 km/h, location:53073
#user msg# single-grp, duration:15 minutes, diversion recommended, extent:-2 segments, event:74 [41]:traffic congestion, average speed of 50 km/h, location:63296
#user msg# single-grp, duration:15 minutes, diversion recommended, extent:-3 segments, event:76 [43]:traffic congestion, average speed of 70 km/h, location:51014
#user msg# single-grp, duration:15 minutes, diversion recommended, extent:-3 segments, event:76 [43]:traffic congestion, average speed of 70 km/h, location:51014
#user msg# single-grp, duration:15 minutes, diversion recommended, extent:-3 segments, event:76 [43]:traffic congestion, average speed of 70 km/h, location:62289
#user msg# single-grp, duration:15 minutes, diversion recommended, extent:-3 segments, event:76 [43]:traffic congestion, average speed of 70 km/h, location:51014
#user msg# single-grp, duration:15 minutes, diversion recommended, extent:-3 segments, event:76 [43]:traffic congestion, average speed of 70 km/h, location:62289
#user msg# single-grp, duration:15 minutes, diversion recommended, extent:-3 segments, event:76 [43]:traffic congestion, average speed of 70 km/h, location:62289
#user msg# single-grp, duration:15 minutes, diversion recommended, extent:-2 segments, event:75 [42]:traffic congestion, average speed of 60 km/h, location:53062
#user msg# single-grp, duration:15 minutes, diversion recommended, extent:-2 segments, event:73 [40]:traffic congestion, average speed of 40 km/h, location:838
#user msg# single-grp, duration:15 minutes, diversion recommended, extent:-2 segments, event:73 [40]:traffic congestion, average speed of 40 km/h, location:838
#user msg# single-grp, duration:15 minutes, diversion recommended, extent:-2 segments, event:73 [40]:traffic congestion, average speed of 40 km/h, location:838
#user msg# single-grp, duration:15 minutes, diversion recommended, extent:-2 segments, event:75 [42]:traffic congestion, average speed of 60 km/h, location:3910
#user msg# single-grp, duration:15 minutes, diversion recommended, extent:-2 segments, event:75 [42]:traffic congestion, average speed of 60 km/h, location:3910
#user msg# single-grp, duration:15 minutes, diversion recommended, extent:-2 segments, event:75 [42]:traffic congestion, average speed of 60 km/h, location:3910
#user msg# single-grp, duration:15 minutes, diversion recommended, extent:-1 segments, event:76 [43]:traffic congestion, average speed of 70 km/h, location:6978
#user msg# single-grp, duration:15 minutes, diversion recommended, extent:-1 segments, event:76 [43]:traffic congestion, average speed of 70 km/h, location:6978
#user msg# single-grp, duration:15 minutes, diversion recommended, extent:-2 segments, event:76 [43]:traffic congestion, average speed of 70 km/h, location:12114
#user msg# single-grp, duration:15 minutes, diversion recommended, extent:-2 segments, event:76 [43]:traffic congestion, average speed of 70 km/h, location:12114
#user msg# single-grp, duration:15 minutes, diversion recommended, extent:-2 segments, event:72 [39]:traffic congestion, average speed of 30 km/h, location:49990
#user msg# single-grp, duration:15 minutes, diversion recommended, extent:-2 segments, event:72 [39]:traffic congestion, average speed of 30 km/h, location:49990
#user msg# single-grp, duration:15 minutes, diversion recommended, extent:-4 segments, event:76 [43]:traffic congestion, average speed of 70 km/h, location:59208
#user msg# single-grp, duration:15 minutes, diversion recommended, extent:-4 segments, event:76 [43]:traffic congestion, average speed of 70 km/h, location:59208
#user msg# single-grp, duration:15 minutes, diversion recommended, extent:3 segments, event:75 [42]:traffic congestion, average speed of 60 km/h, location:838
#user msg# single-grp, duration:15 minutes, diversion recommended, extent:1 segments, event:1118 [0]: , location:5953
#user msg# single-grp, duration:15 minutes, diversion recommended, extent:1 segments, event:1118 [0]: , location:5953
```

Results

```
Location #  1 has     1 possible plain codes
  4603  11fb
Location #  2 has     1 possible plain codes
  4401  1131
Location #  3 has     1 possible plain codes
  4172  104c
Location #  4 has     1 possible plain codes
  5134  140e
Location #  5 has     1 possible plain codes
  4193  1061
Location #  6 has     1 possible plain codes
  4527  11af
Location #  7 has     1 possible plain codes
  4329  10e9
Location #  8 has     1 possible plain codes
  5611  15eb
Location #  9 has     1 possible plain codes
  4538  11ba
Location # 10 has     1 possible plain codes
  4303  10cf
Location # 11 has     1 possible plain codes
  4223  107f
Location # 12 has     1 possible plain codes
  4834  12e2
```

```
Encryption ID   2 has      2 possible keys
Encryption ID   3 has     15 possible keys
Encryption ID   4 has      5 possible keys
Encryption ID   5 has      4 possible keys
Encryption ID   6 has      3 possible keys
Encryption ID   7 has      5 possible keys
Encryption ID   8 has      7 possible keys
Encryption ID   9 has      2 possible keys
Encryption ID  10 has     34 possible keys
Encryption ID  11 has      1 possible keys
Encryption ID  13 has      4 possible keys
Encryption ID  15 has      2 possible keys
Encryption ID  17 has      2 possible keys
Encryption ID  18 has      3 possible keys
Encryption ID  20 has      3 possible keys
Encryption ID  21 has      4 possible keys
Encryption ID  22 has      6 possible keys
Encryption ID  24 has      1 possible keys
Encryption ID  25 has      3 possible keys
Encryption ID  26 has      5 possible keys
Encryption ID  27 has      3 possible keys
Encryption ID  28 has      1 possible keys
Encryption ID  30 has      2 possible keys
Encryption ID  31 has      4 possible keys
```

FM

101.9MHz ST RDS

SDR-FM!!

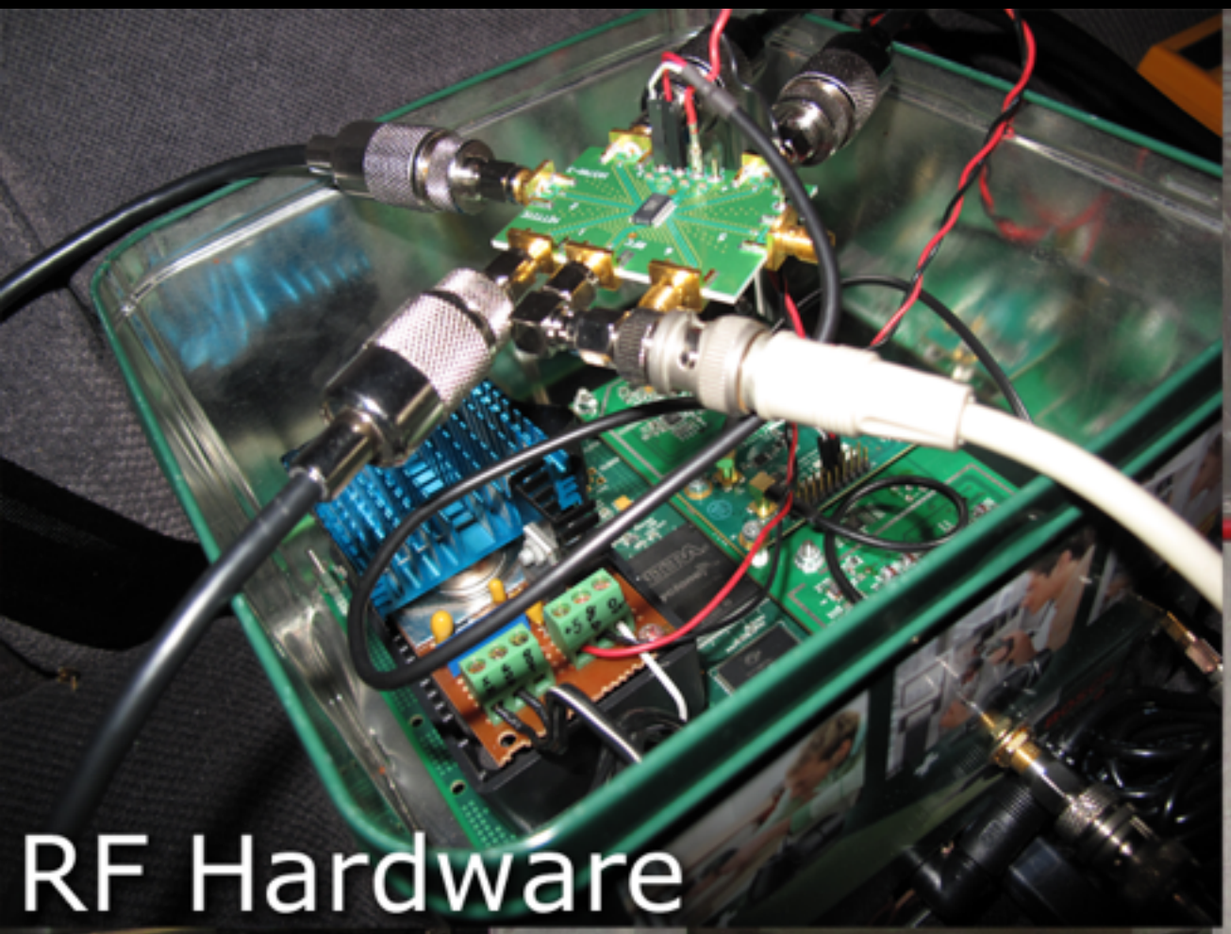
11 33

RDF

Hacking the Wireless World with #sdr

@spenchdotnet

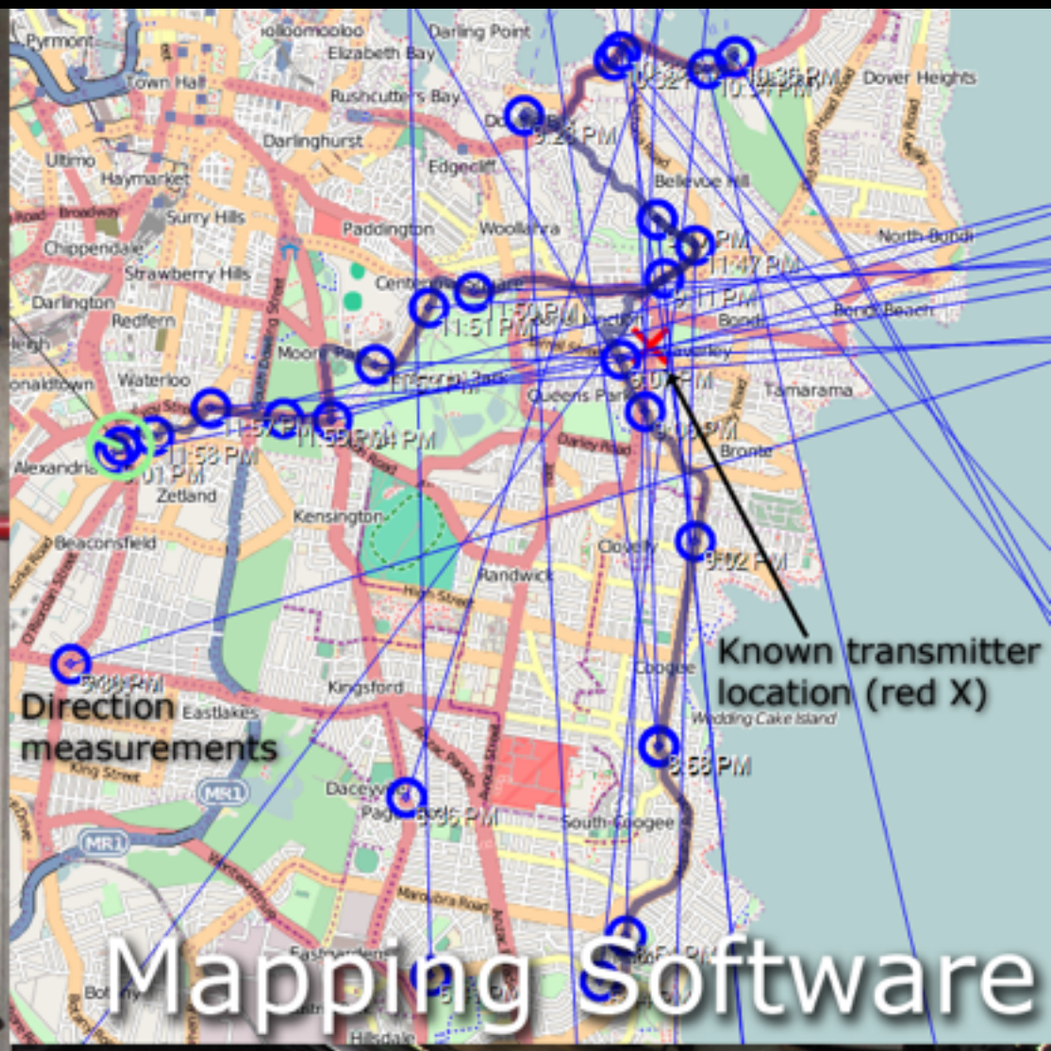
SDR Direction Finding



RF Hardware

Software-Defined Radio

Direction Finding



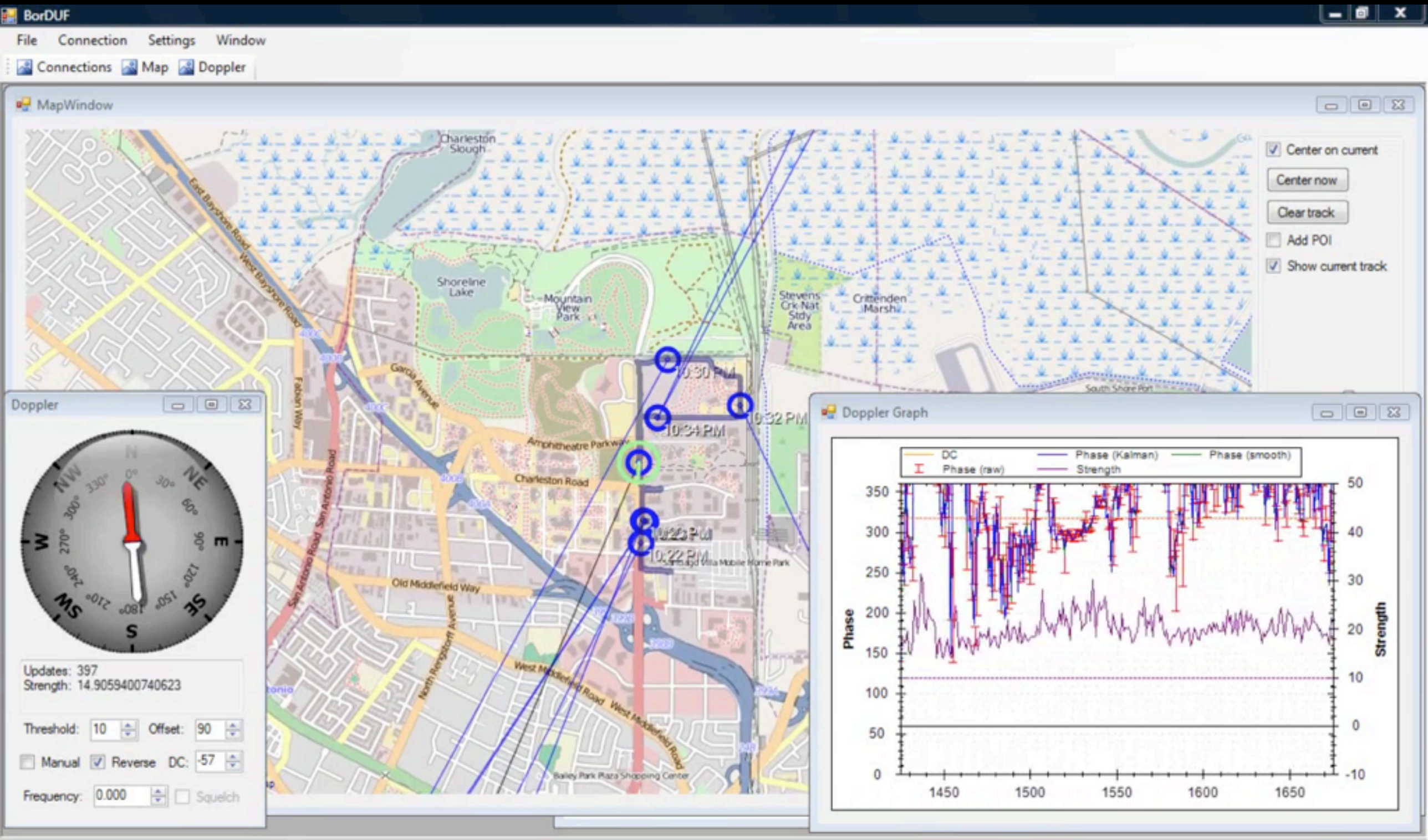
Mapping Software

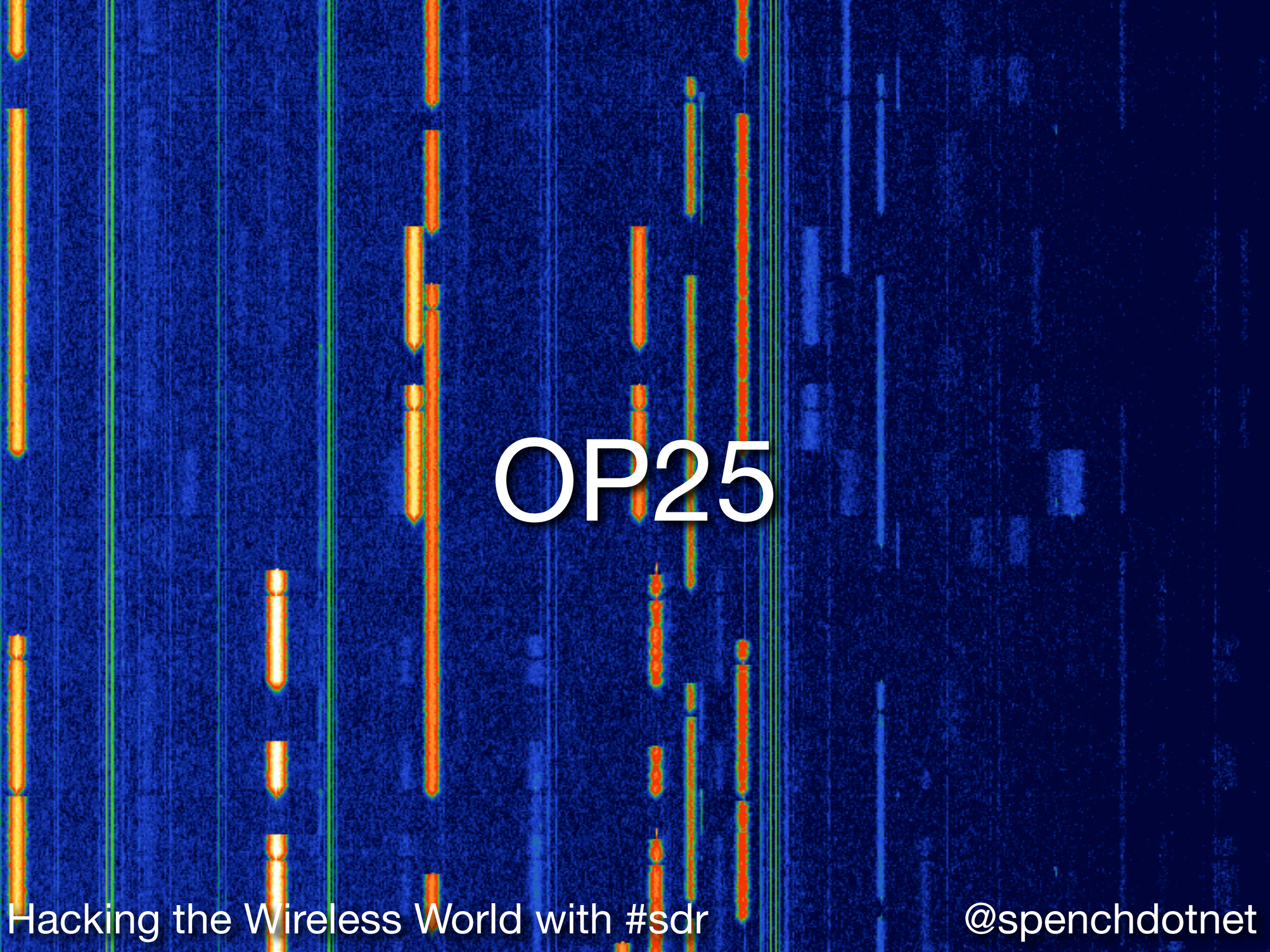
Antenna Array

The DUF-Mobile

Balint Seeber
http://spench.net/

Radio Direction Finding & Mapping




OP25
Hacking the Wireless World with #sdr
@spenchdotnet

Python

OP25.grc - /Users/balint/Documents/GRC/Apps - GNU Radio Companion

File Edit View Run Tools Help

OP25 | Z-Wave RX | Baudline-file | Baudline | Downconvert | WAV-to-CFile | WAV to CFile

Op25 Grc

Fine Offset: 0

Xlate Offset: -19.802k

Xlate BW: 24k

Verbose console logging

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

Scope Plot

Persistence

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: 770.25M

Auto tune: 0

Audio mul: 0

Final freq: 770.23M

DUID: LDU2 MFID: Standard MFID (pre-20

NAC: ALGID: Plain

Source: 0x129712 KID: 0x0000

Destination: MI: 0x00000000000000000

TGID: 0x0001

Gain: 20

message

[Misc]
Any Block (Message)
[None]
Message Callback
Message Relay
[Networking Tools]
Message Server
[Message Tools]
Tag to Message
Message Burst Source
Message Sink
Message Source
[Debug Tools]
Message Debug
Message Strobe
Message Strobe Random-Delay
[Foo]
Periodic Message Source
[ZeroMQ Interfaces]
ZMQ PUB Message Sink
ZMQ PULL Message Source
ZMQ PUSH Message Sink
ZMQ REP Message Sink
ZMQ REQ Message Source
ZMQ SUB Message Source

```
LDU2:    46 d9 c8 07 d8 f3 fc 09 fa 0c 17
LDU2: LSDW: 0xdfa2, valid
LDU2:    AlgID: 0x80, KID: 0x0000, MI: 00000000000000000
eserved: 0x0000, TGID: 0x0001, Source: 0x129712
LDU1:    4a bd 44 4b 36 89 ff d5 bb 52 60
LDU1:    4b 3d 85 20 e3 78 ff bc e7 a3 33
LDU1:    47 2a e8 a7 fd 6b c6 d7 a1 0f 70
LDU1:    4b c4 62 ec f2 c7 ff a2 d8 64 95
LDU1:    4b c5 6e 42 00 fb ff ac 1b b9 b4
LDU1:    4b c1 7c 53 5c ef ff 81 33 61 6b
LDU1:    4b d1 34 7c 2c 52 ff 8b f8 92 d4
LDU1:    4b 51 3e 5a d4 9c ff e2 13 ae cb
LDU1:    4b 51 3c 7e cc 12 ff e0 00 18 a2
LDU1: LSDW: 0x0802, valid
```

Python

OP25.grc - /Users/balint/Documents/GRC/Apps - GNU Radio Companion

File Edit View Run Tools Help

OP25 | Z-Wave RX | Baudline-file | Baudline | Downconvert | VCO | soho_tlm | ACARS RX | ATSC PN | ATSC resample | DSC jammer | FSK audio | usrp_rx_flex | WAV resample | WAV-to-CFile | WAV to CFile

Op25 Grc

Fine Offset: 0

Xlate Offset: -19.802k

Xlate BW: 24k

Verbose console logging

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

FFT Plot

Trace Options: Peak Hold; Average (Avg Alpha: 0.0667); Persistence; Trace A Store; Trace B Store

Axis Options: dB/Div: + -; Ref Level: + -; Autoscale; Stop

Frequency (MHz)

Output idle silence

Frequency: 770.25M

Auto tune: 0

Audio mul: 0

Final freq: 770.23M

DUID:	LDU1	MFID:	Standard MFID (pre-2(
NAC:		ALGID:	DES-OFB
Source:	0x129712	KID:	0x3780
Destination:		MI:	0x6f166d91ce5bd2f000
		TGID:	0x0001

Gain: 20

message

- [Misc]
  - Any Block (Message)
- [None]
  - Message Callback
  - Message Relay
- [Networking Tools]
  - Message Server
- [Message Tools]
  - Tag to Message
  - Message Burst Source
  - Message Sink
  - Message Source
- [Debug Tools]
  - Message Debug
  - Message Strobe
  - Message Strobe Random-Delay
- [Foo]
  - Periodic Message Source
- [ZeroMQ Interfaces]
  - ZMQ PUB Message Sink
  - ZMQ PULL Message Source
  - ZMQ PUSH Message Sink
  - ZMQ REP Message Sink
  - ZMQ REQ Message Source
  - ZMQ SUB Message Source

```
LDU2:    7a 02 f8 2e 7f 01 bf 84 69 61 58
LDU2:    7a 68 be b0 d1 8a ff e9 14 91 83
LDU2: LSDW: 0x037e, valid
LDU2:    AlgID: 0x81, KID: 0x3780, MI: 6f166d91ce5bd2f000
DES:     1704 bits used from 28 iterations

LDU1: 0 hamming errors, valid
LDU1:    73 5c e3 46 5c 3e ff f6 61 54 04
LDU1:    7b 54 94 34 1a 42 ff f2 e7 b9 09
LDU1:    7f 5d 06 83 28 89 ff f3 4f 56 7a
LDU1:    7f 55 16 19 7b 98 ff f3 9d 7e 75
LDU1:    82 ce 24 76 6d 25 ff ff 67 03 18
LDU1:    8e be a9 3b 66 04 ff fb 6c 7b f9
LDU1:    96 3e 20 41 7c 2f 80 08 49 21 84
LDU1: LSDW: 0x2c26, valid
```

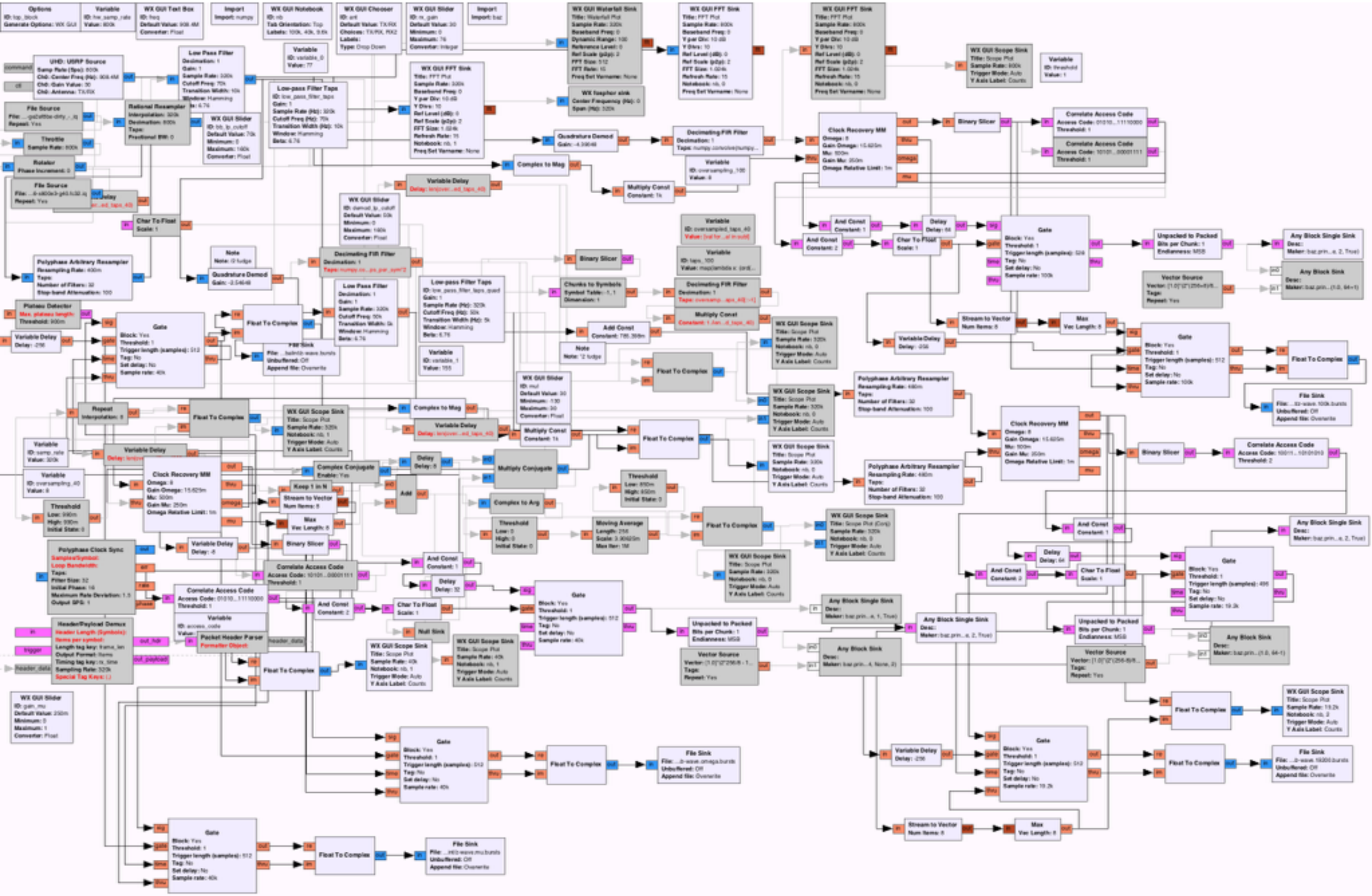
IoT

Z-Wave

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

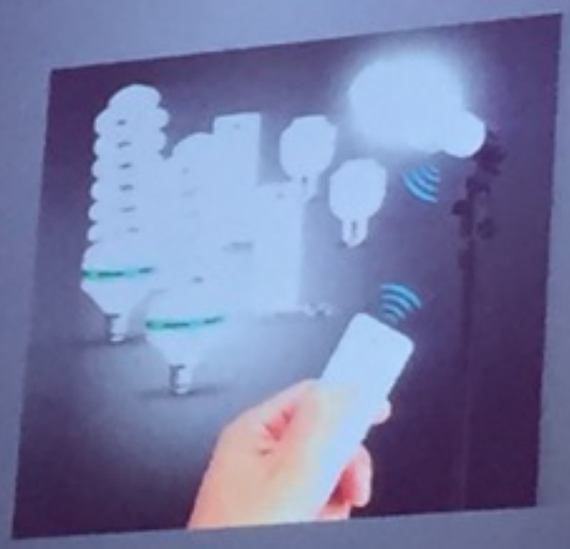
Z-Wave


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]

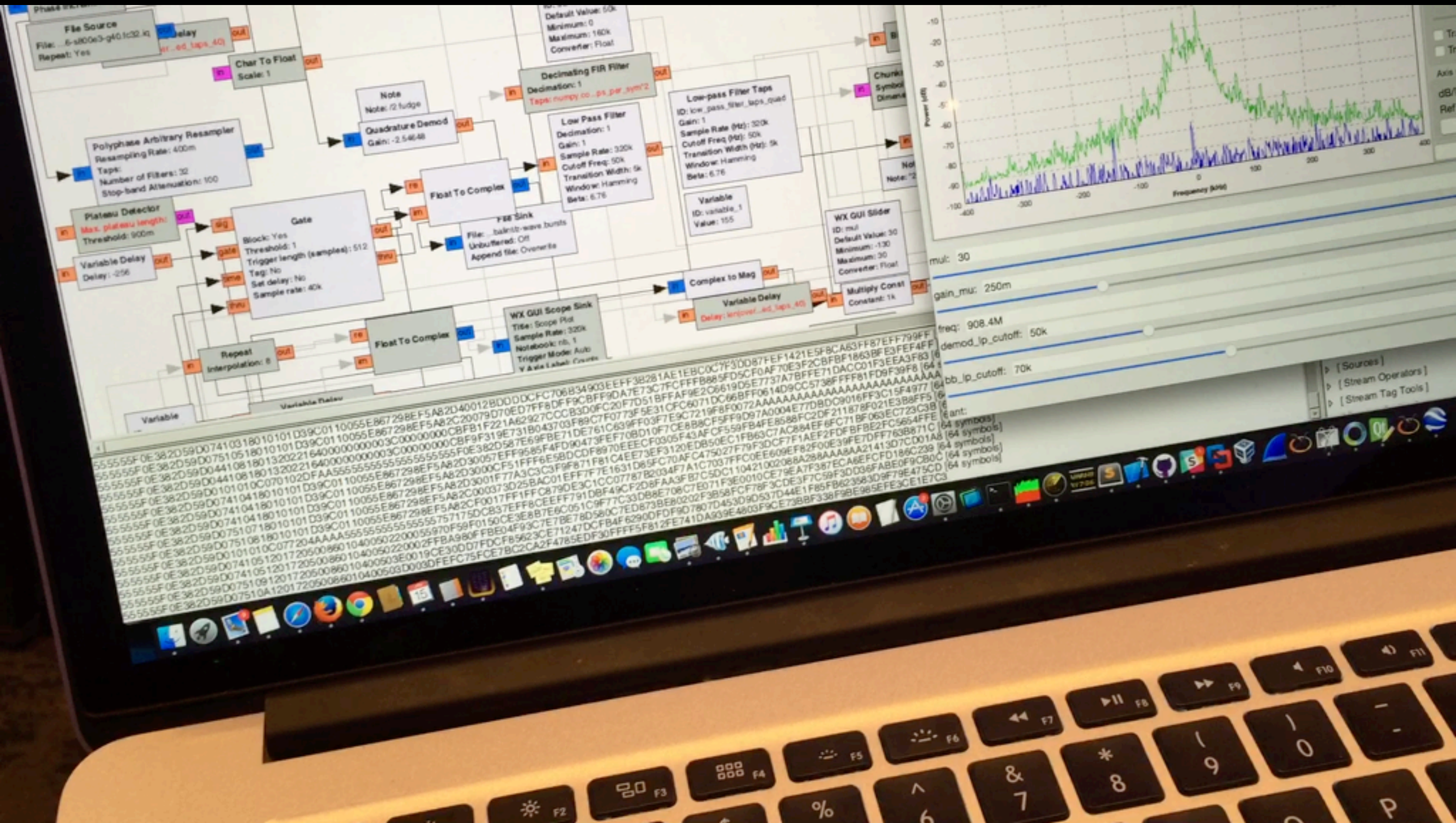

Options
ID: top_block
Generate Options: WX GUI
Variable
ID: hw_samp_rate
Value: 800k
WX GUI Text Box
ID: freq
Default Value: 908.4M
Converter: Float
Import
Import: numpy
WX GUI Notebook
ID: nb
Tab Orientation: Top
Labels: 100k, 40k, 9.6k
WX GUI Chooser
ID: ant
Default Value: TX/RX
Choices: TX/RX, RX2
Labels:
Type: Drop Down
WX GUI Slider
ID: rx_gain
Default Value: 30
Minimum: 0
Maximum: 76
Converter: Integer
Import
Import: baz
WX GUI Waterfall Sink
Title: Waterfall Plot
Sample Rate: 320k
Baseband Freq: 0
Dynamic Range: 100
Reference Level: 0
Ref Scale (pt2p): 2
FFT Size: 512
FFT Rate: 15
Freq Set Varname: None
WX GUI FFT Sink
Title: FFT Plot
Sample Rate: 800k
Baseband Freq: 0
Y per Div: 10 dB
Y Divs: 10
Ref Level (dB): 0
Ref Scale (pt2p): 2
FFT Size: 1.024k
Refresh Rate: 15
Notebook: nb, 0
Freq Set Varname: None
WX GUI FFT Sink
Title: FFT Plot
Sample Rate: 800k
Baseband Freq: 0
Y per Div: 10 dB
Y Divs: 10
Ref Level (dB): 0
Ref Scale (pt2p): 2
FFT Size: 1.024k
Refresh Rate: 15
Notebook: nb, 0
Freq Set Varname: None
WX GUI Scope Sink
Title: Scope Plot
Sample Rate: 800k
Trigger Mode: Auto
Y Axis Label: Counts
Variable
ID: threshold
Value: 1
UHD: USRP Source
Samp Rate (Sps): 800k
Ch0: Center Freq (Hz): 908.4M
Ch0: Gain Value: 30
Ch0: Antenna: TX/RX
Low Pass Filter
Decimation: 1
Gain: 1
Sample Rate: 320k
Cutoff Freq: 70k
Transition Width: 10k
Window: Hamming
Beta: 6.76
Variable
ID: variable_0
Value: 77
WX GUI Slider
ID: bb_lp_cutoff
Default Value: 70k
Minimum: 0
Maximum: 160k
Converter: Float
Low-pass Filter Taps
ID: low_pass_filter_taps
Gain: 1
Sample Rate (Hz): 320k
Cutoff Freq (Hz): 70k
Transition Width (Hz): 10k
Window: Hamming
Beta: 6.76
WX GUI FFT Sink
Title: FFT Plot
Sample Rate: 320k
Baseband Freq: 0
Y per Div: 10 dB
Y Divs: 10
Ref Level (dB): 0
Ref Scale (pt2p): 2
FFT Size: 1.024k
Refresh Rate: 15
Notebook: nb, 1
Freq Set Varname: None
WX freqchor sink
Center Frequency (Hz): 0
Span (Hz): 320k
Quadrature Demod
Gain: -4.34648
Decimating FIR Filter
Decimation: 1
Taps: numpy.conclove(numpy...
Variable
ID: oversampling_100
Value: 8
Clock Recovery MM
Omega: 8
Gain Omega: 15.625m
Mu: 500m
Gain Mu: 250m
Omega Relative Limit: 1m
Binary Slicer
Correlate Access Code
Access Code: 01010...11110000
Threshold: 1
Correlate Access Code
Access Code: 10101...00001111
Threshold: 1
File Source
File: ...gs2ut50e-dnfy_r...tq
Repeat: Yes
Rational Resampler
Interpolation: 320k
Decimation: 800k
Taps:
Fractional BW: 0
Throttle
Sample Rate: 800k
Rotator
Phase Increment: 0
File Source
File: ...6-s800e3-gt0.fc32.iq
Repeat: Yes
Variable Delay
Delay: ...er...ed_taps_40)
Complex to Mag
Variable Delay
Delay: len(over...ed_taps_40)
Multiply Const
Constant: 1k
Char To Float
Scale: 1
WX GUI Slider
ID: demod_lp_cutoff
Default Value: 50k
Minimum: 0
Maximum: 160k
Converter: Float
Note
Note: 0 fudge
Quadrature Demod
Gain: -2.54648
Decimating FIR Filter
Decimation: 1
Taps: numpy.co...ps_per_sym*2
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
Variable
ID: variable_1
Value: 155
Binary Slicer
Chunks to Symbols
Symbol Table: -1, 1
Dimension: 1
Decimating FIR Filter
Decimation: 1
Taps: oversamp...aps_40[::-1]
Multiply Const
Constant: 1.4en...d_taps_40)
Add Const
Constant: 785.398m
Note
Note: 12 fudge
Variable
ID: oversampled_taps_40
Value: [val for ...al in outs]
Variable
ID: taps_100
Value: map(lambda x: (int(...
Polyphase Arbitrary Resampler
Resampling Rate: 400m
Taps:
Number of Filters: 32
Stop-band Attenuation: 100
Plateau Detector
Max. plateau length: 900m
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: ...bsinb-wave.bursts
Unbuffered: Off
Append file: Overwrite
Repeat
Interpolation: 1
Float To Complex
WX GUI Scope Sink
Title: Scope Plot
Sample Rate: 320k
Notebook: nb, 1
Trigger Mode: Auto
Y Axis Label: Counts
Complex to Mag
Variable Delay
Delay: len(over...ed_taps_40)
WX GUI Slider
ID: mul
Default Value: 30
Minimum: -100
Maximum: 30
Converter: Float
Multiply Const
Constant: 1k
Float To Complex
Variable
ID: samp_rate
Value: 320k
Variable Delay
Delay: len(over...ed_taps_40)
Clock Recovery MM
Omega: 8
Gain Omega: 15.625m
Mu: 500m
Gain Mu: 250m
Omega Relative Limit: 1m
Complex Conjugate
Enable: Yes
Delay
Delay: 8
Add
Multiply Conjugate
Variable
ID: oversampling_40
Value: 8
Keep 1 in N
Stream to Vector
Num Items: 8
Max
Vec Length: 8
Threshold
Low: 990m
High: 990m
Initial State: 0
Complex to Arg
Threshold
Low: 0
High: 0
Initial State: 0
Moving Average
Length: 256
Scale: 3.90625m
Max Iter: 1M
Threshold
Low: 850m
High: 950m
Initial State: 0
Float To Complex
WX GUI Scope Sink
Title: Scope Plot
Sample Rate: 320k
Notebook: nb, 0
Trigger Mode: Auto
Y Axis Label: Counts
WX GUI Scope Sink
Title: Scope Plot
Sample Rate: 320k
Notebook: nb, 0
Trigger Mode: Auto
Y Axis Label: Counts
WX GUI Scope Sink
Title: Scope Plot (Corp)
Sample Rate: 320k
Notebook: nb, 0
Trigger Mode: Auto
Y Axis Label: Counts
Polyphase Arbitrary Resampler
Resampling Rate: 480m
Taps:
Number of Filters: 32
Stop-band Attenuation: 100
Polyphase Clock Sync
Samples/Symbol:
Loop Bandwidth:
Taps:
Filter Size: 32
Initial Phase: 16
Maximum Rate Deviation: 1.5
Output SPS: 1
Correlate Access Code
Access Code: 10101...00001111
Threshold: 1
And Const
Constant: 1
Delay
Delay: 32
Char To Float
Scale: 1
Correlate Access Code
Access Code: 01010...11110000
Threshold: 1
Variable
ID: access_code
Value: ...
And Const
Constant: 2
Null Sink
Header/Payload Demux
Header Length (Symbols):
Items per symbol:
Length tag key: frame_len
Output Format: Items
Timing tag key: rx_time
Sampling Rate: 320k
Special Tag Keys: ( )
Packet Header Parser
Formatter Object:
Float To Complex
WX GUI Scope Sink
Title: Scope Plot
Sample Rate: 40k
Notebook: nb, 1
Trigger Mode: Auto
Y Axis Label: Counts
WX GUI Scope Sink
Title: Scope Plot
Sample Rate: 40k
Notebook: nb, 1
Trigger Mode: Auto
Y Axis Label: Counts
Gate
Block: Yes
Threshold: 1
Trigger length (samples): 512
Tag: No
Set delay: No
Sample rate: 40k
Unpacked to Packed
Bits per Chunk: 1
Endianness: MSB
Vector Source
Vector: [1.0]*2*256+[-1...
Tags:
Repeat: Yes
Any Block Sink
Desc:
Maker: baz.prin...e, 2, True)
Any Block Sink
Desc:
Maker: baz.prin...4, None, 2)
WX GUI Slider
ID: gain_mu
Default Value: 250m
Minimum: 0
Maximum: 1
Converter: Float
Gate
Block: Yes
Threshold: 1
Trigger length (samples): 512
Tag: No
Set delay: No
Sample rate: 40k
Float To Complex
File Sink
File: ...0-wave_omega.bursts
Unbuffered: Off
Append file: Overwrite
Gate
Block: Yes
Threshold: 1
Trigger length (samples): 512
Tag: No
Set delay: No
Sample rate: 40k
Float To Complex
File Sink
File: ...t60-wave_mu.bursts
Unbuffered: Off
Append file: Overwrite
WX GUI Scope Sink
Title: Scope Plot
Sample Rate: 320k
Notebook: nb, 0
Trigger Mode: Auto
Y Axis Label: Counts
WX GUI Scope Sink
Title: Scope Plot
Sample Rate: 320k
Notebook: nb, 0
Trigger Mode: Auto
Y Axis Label: Counts
Polyphase Arbitrary Resampler
Resampling Rate: 480m
Taps:
Number of Filters: 32
Stop-band Attenuation: 100
Clock Recovery MM
Omega: 8
Gain Omega: 15.625m
Mu: 500m
Gain Mu: 250m
Omega Relative Limit: 1m
Binary Slicer
Correlate Access Code
Access Code: 10011...10100010
Threshold: 2
Any Block Single Sink
Desc:
Maker: baz.prin...e, 2, True)
And Const
Constant: 1
Delay
Delay: 64
And Const
Constant: 2
Char To Float
Scale: 1
Gate
Block: Yes
Threshold: 1
Trigger length (samples): 496
Tag: No
Set delay: No
Sample rate: 19.2k
Any Block Single Sink
Desc:
Maker: baz.prin...e, 2, True)
Any Block Sink
Desc:
Maker: baz.prin...(1.0, 64-1)
Unpacked to Packed
Bits per Chunk: 1
Endianness: MSB
Vector Source
Vector: [1.0]*2\256+8/8...
Tags:
Repeat: Yes
Variable Delay
Delay: -256
Gate
Block: Yes
Threshold: 1
Trigger length (samples): 512
Tag: No
Set delay: No
Sample rate: 19.2k
Float To Complex
WX GUI Scope Sink
Title: Scope Plot
Sample Rate: 19.2k
Notebook: nb, 2
Trigger Mode: Auto
Y Axis Label: Counts
Float To Complex
File Sink
File: ...0-wave_19200.bursts
Unbuffered: Off
Append file: Overwrite
Stream to Vector
Num Items: 8
Max
Vec Length: 8

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: r21udge
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
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
Variable
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]

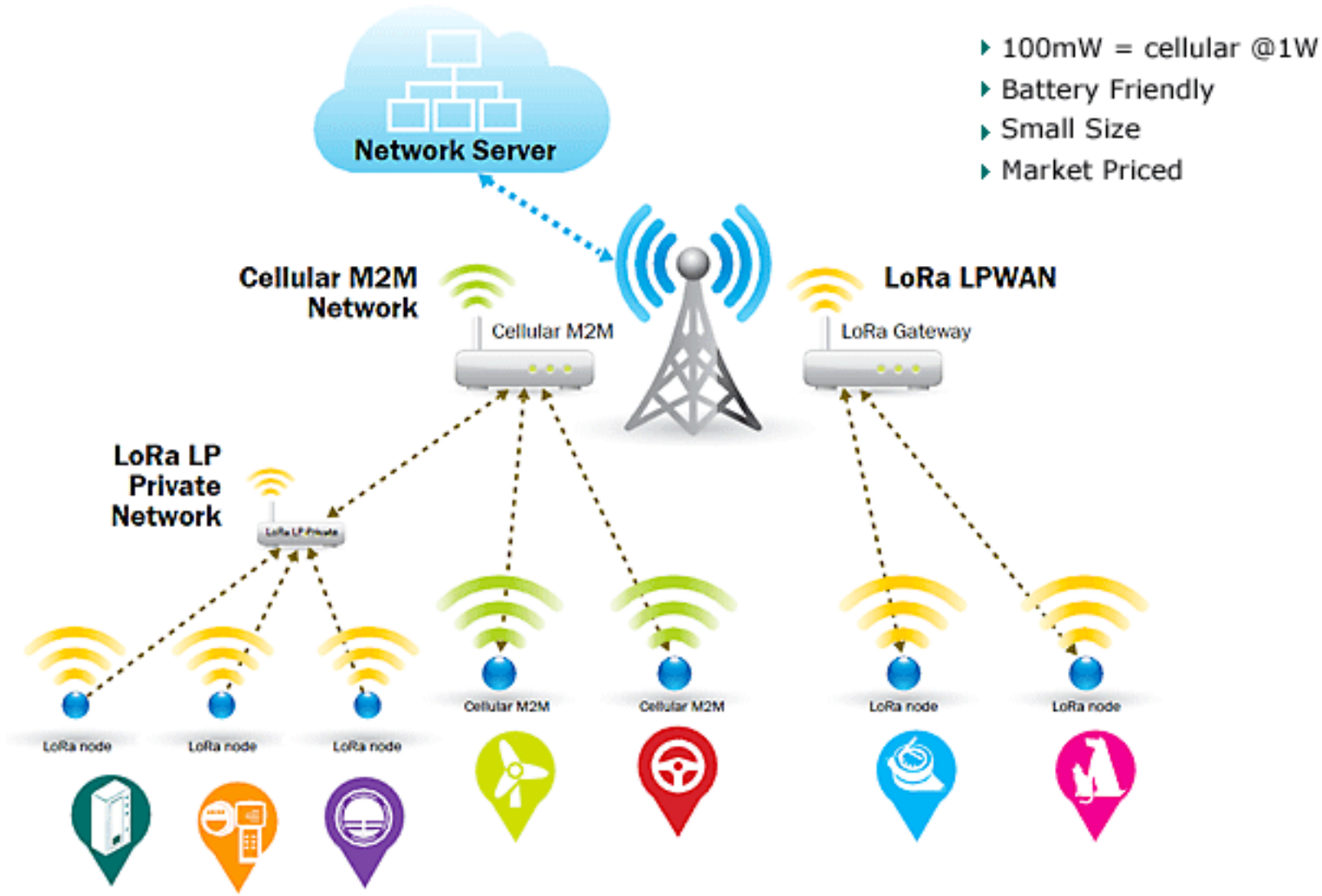
555555F0D18CE24208030B0A0909C1342E8002187CF020CBF63DD0089D7E6C6DC44278632A44357FC200B9C485EE1785F6CC47C21BA
786F255808E0FC4235C79 [64 symbols]

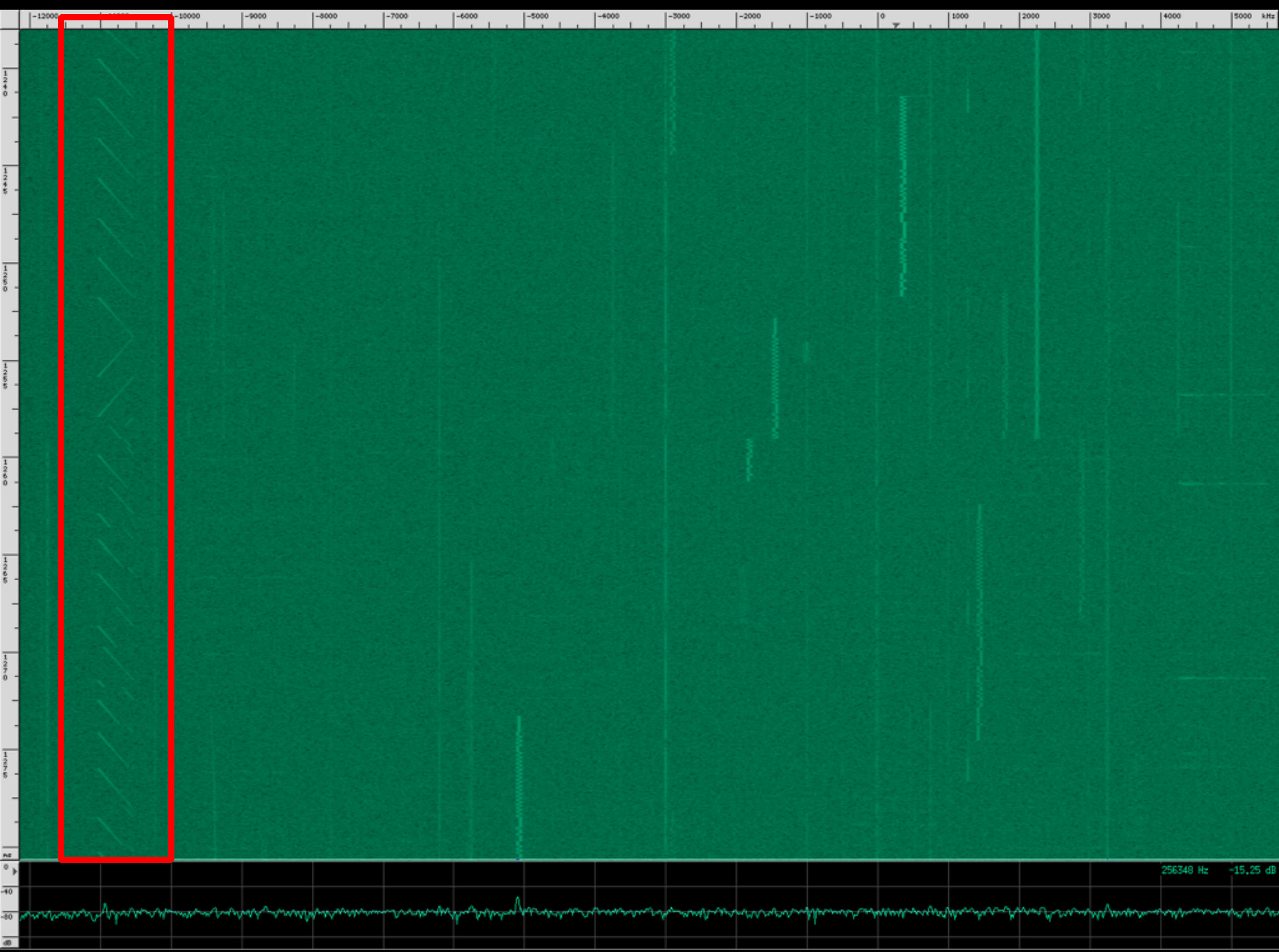
555555F0D18CE24208410D0D012003FF96517925490C33D0F4F1FA2FEF0AE332C3B69189E0A08D0054029FCCE66C3F308FD3945AE73
39F33DDC600222BC43F67 [64 symbols]

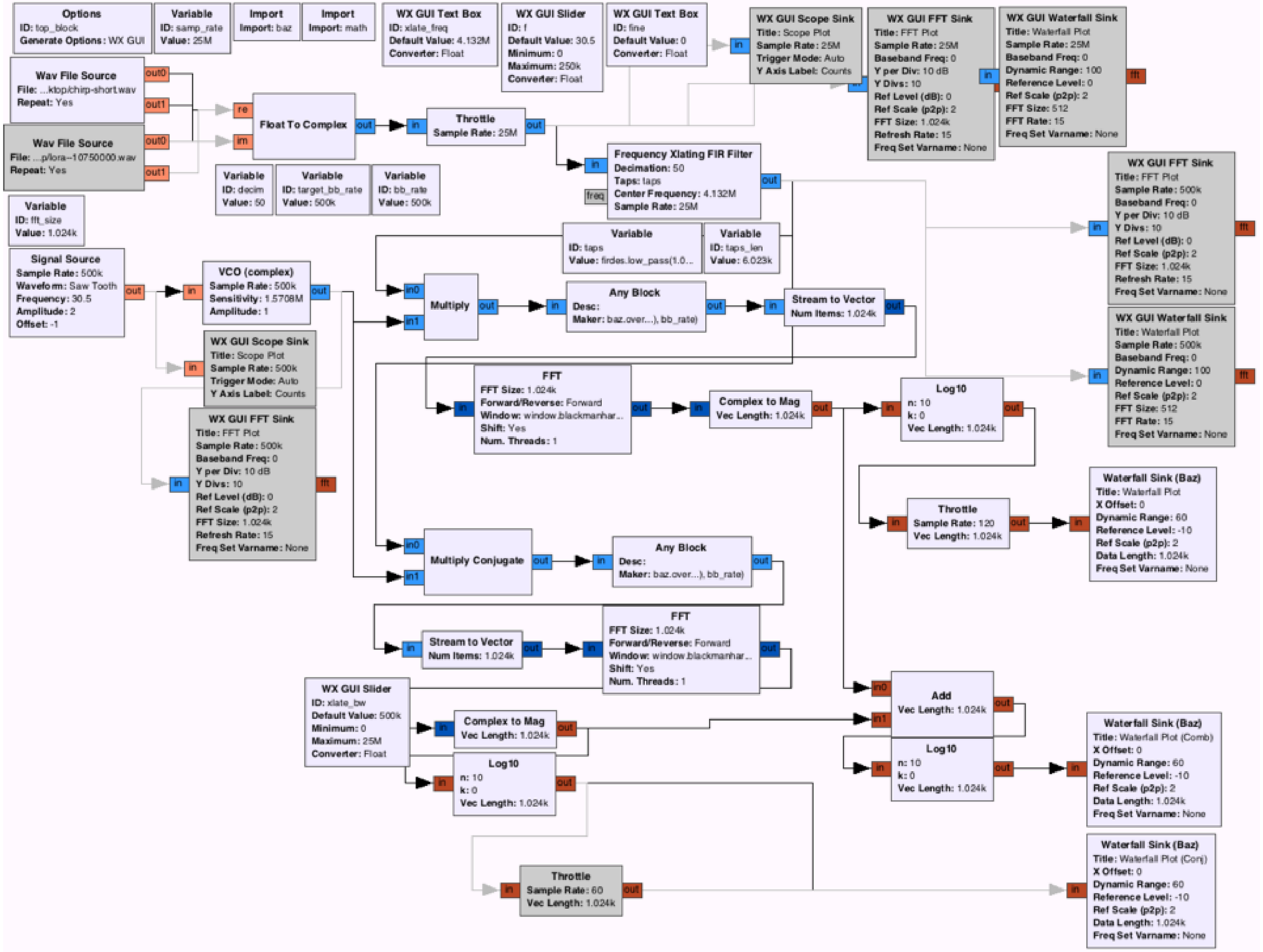
555555F0D18CE24208410D0D012003FF964E3C5021C31F7A60DC1F00DF00E4305DB9FFA1062E4F6B74F7CFFD4AEE8E18EF9EF429941
1D82901B29F201FFC0088 [64 symbols]

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
-40
-80
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

Data (kpoints)

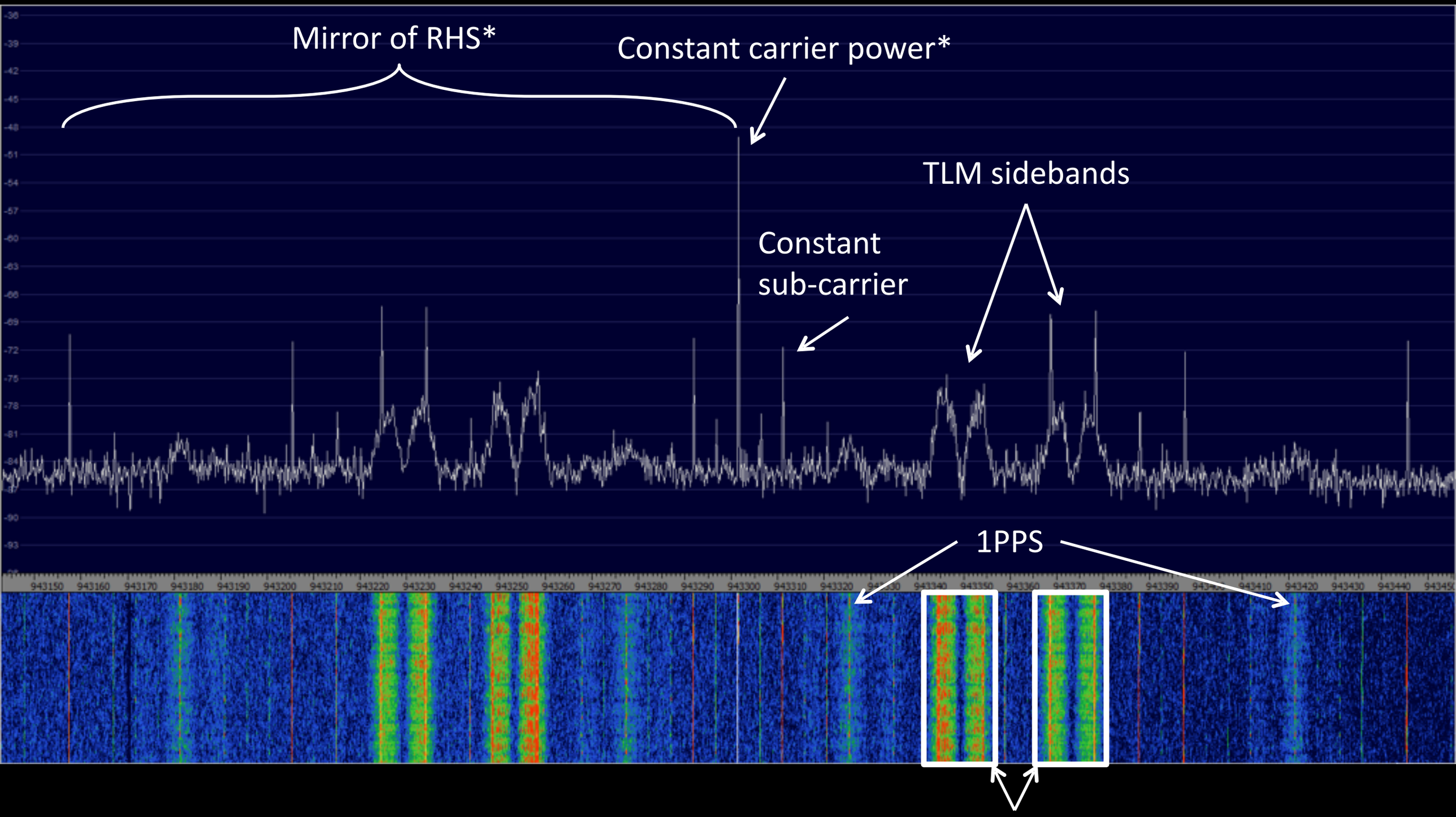
Blind Signal Analysis

What you need

Dish + LNB + power injector + USRP + GNU Radio

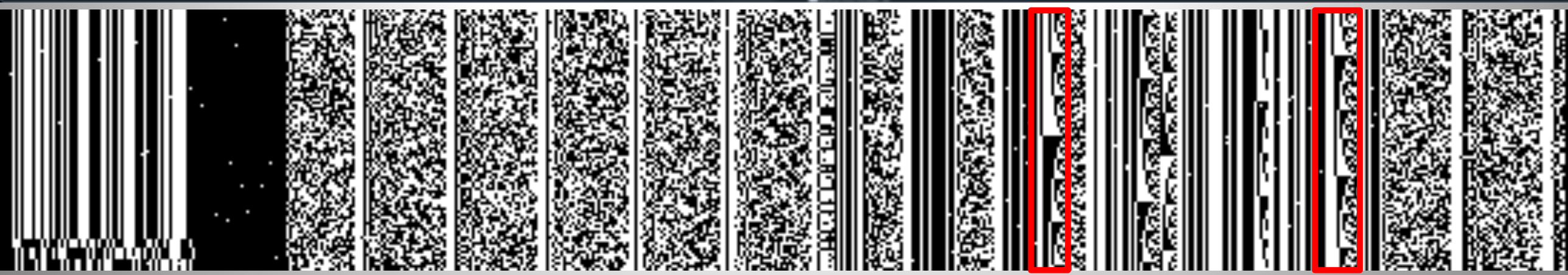
(set-top box with LNB-thru)

D1 TLM1: 12243.25 MHz

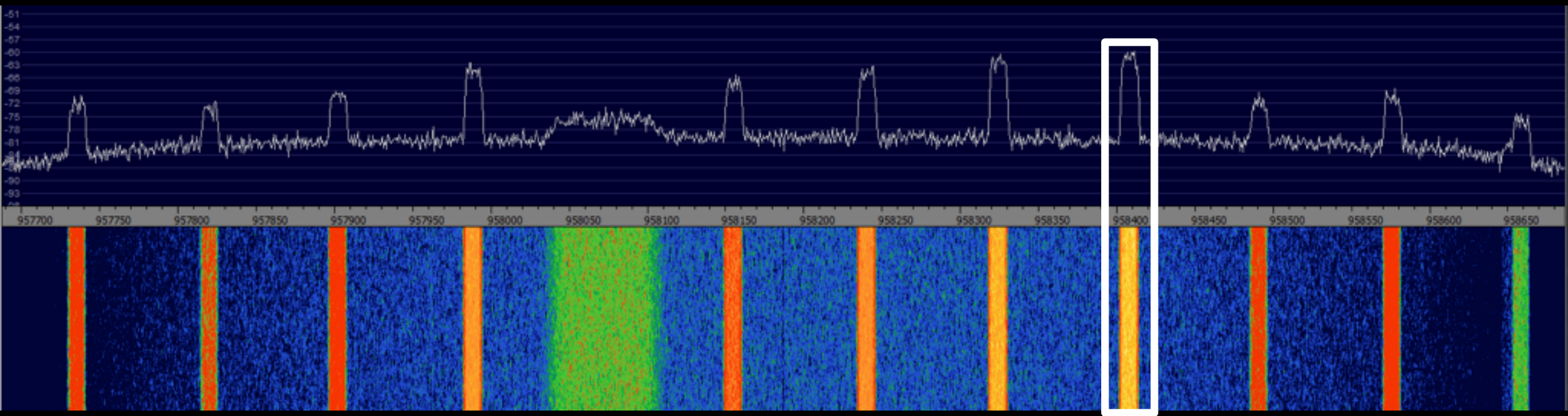


Beacon with **P**hase **M**odulation* (PM): 1PPS and two telemetry streams (sidebands)

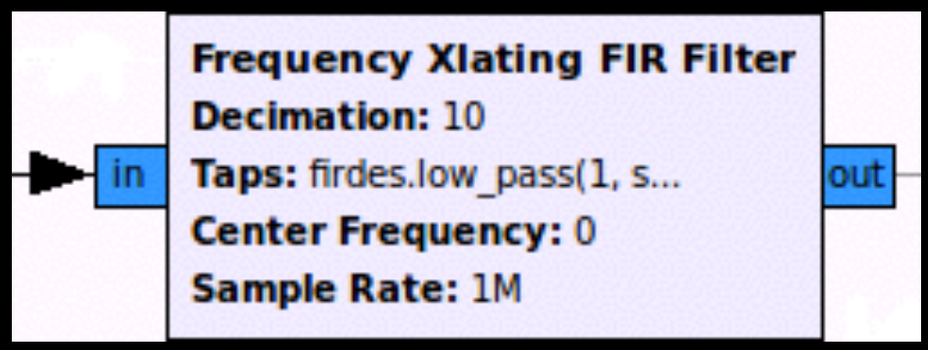
Visualisation



Let’s try one…

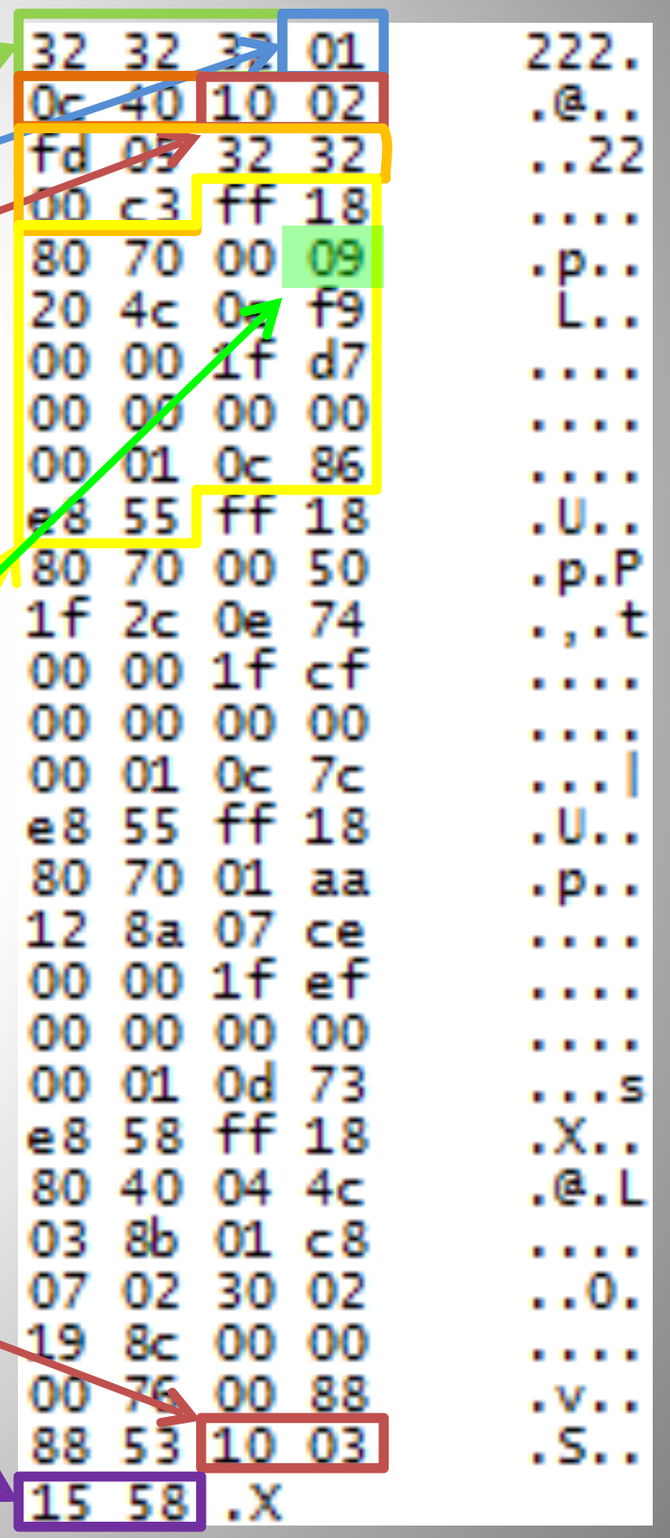


- Feed entire baseband spectrum into GR
- Perform ‘channel selection’ to isolate stream of interest (create new baseband centred on stream)

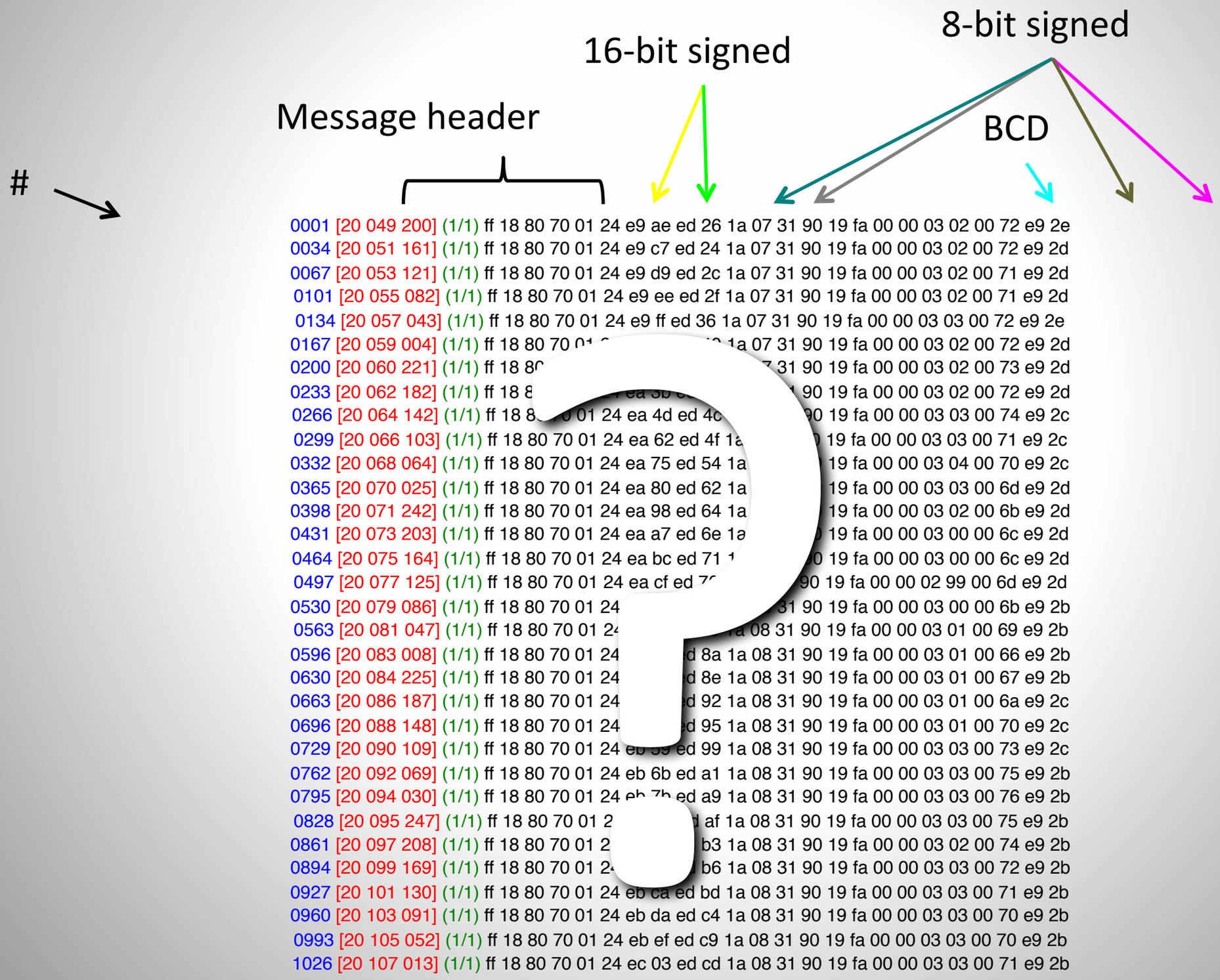


Frame analysis

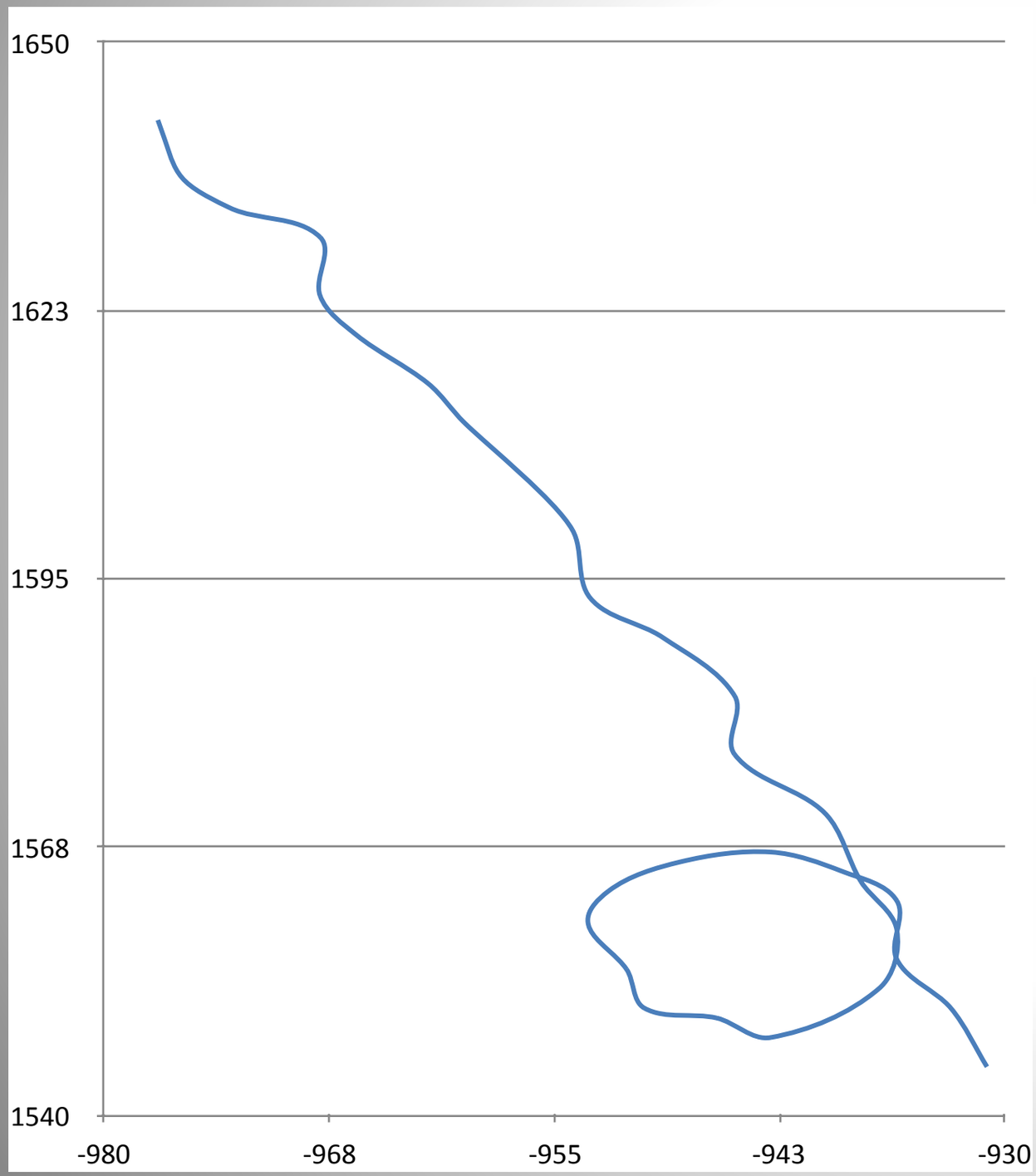
- Header
  - SYN SYN SYN (EBCDIC)
- Character-oriented encoding:
  - SOH
  - STX
  - ETX
  - CRC (CCITT-16)
- Numbers of fixed-length messages
  - Each contains an ID

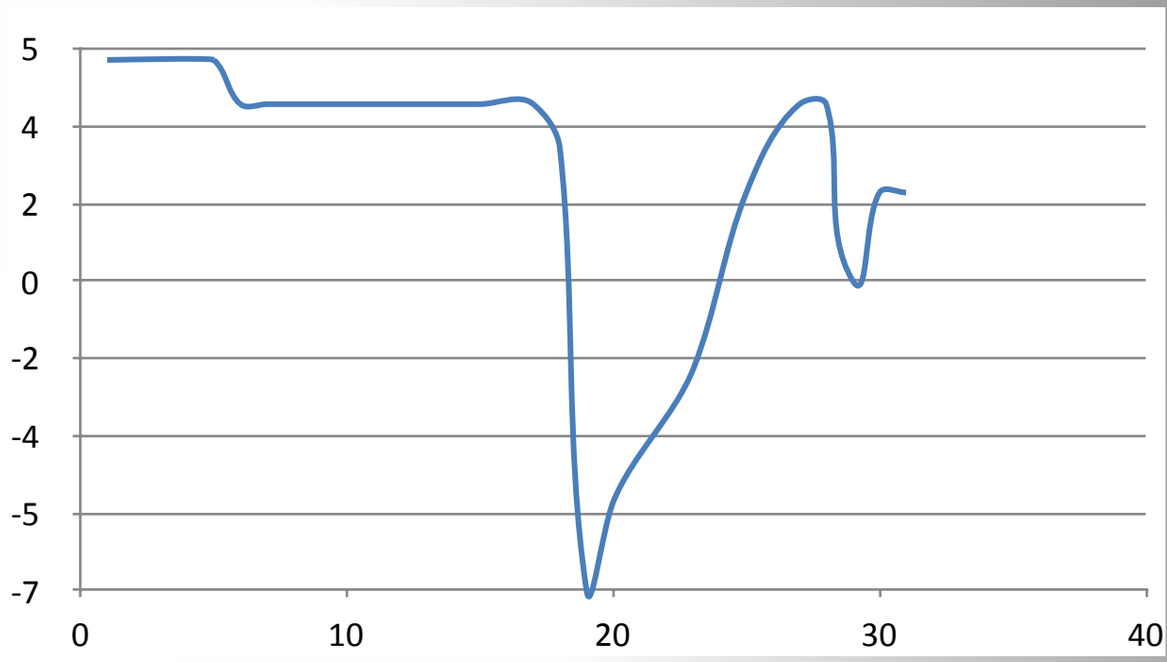


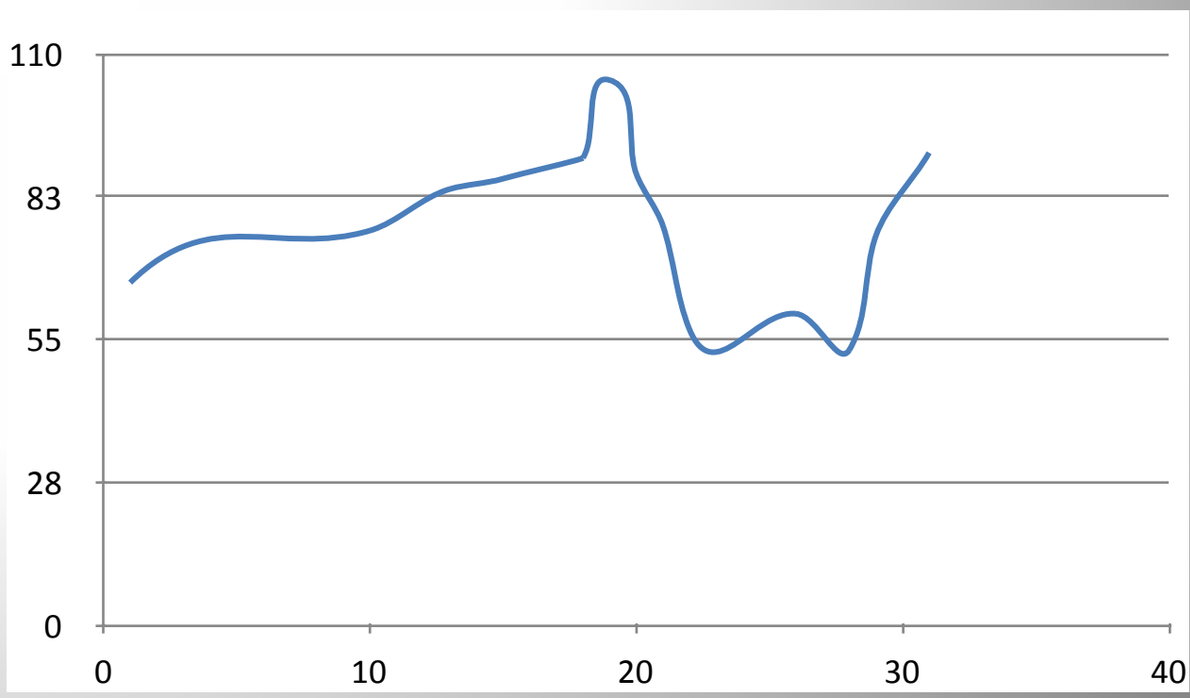
Un-pack & find patterns



Graphing the Data







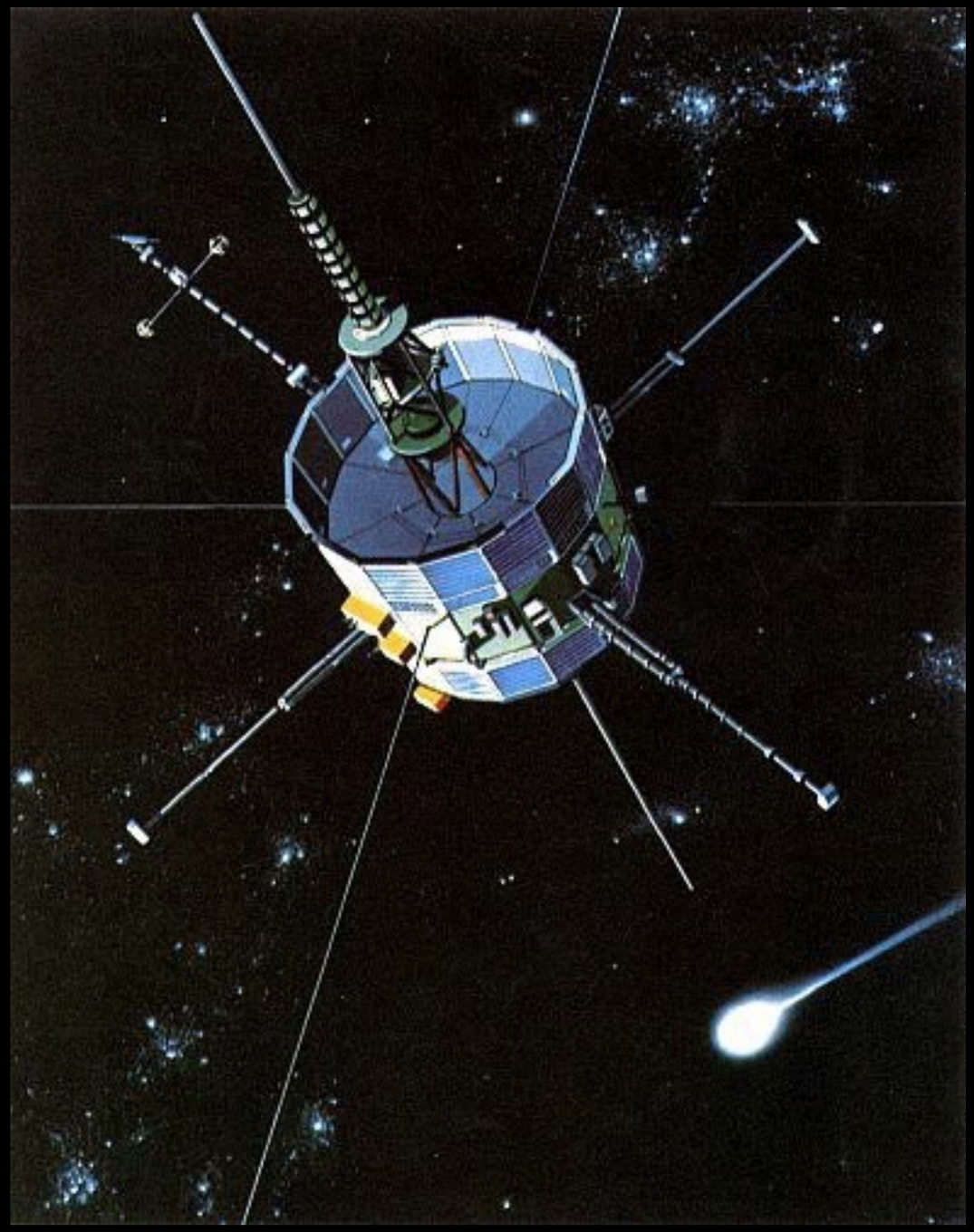
ISEE-3 Reboot Project

Hacking the Wireless World with #sdr

@spenchdotnet

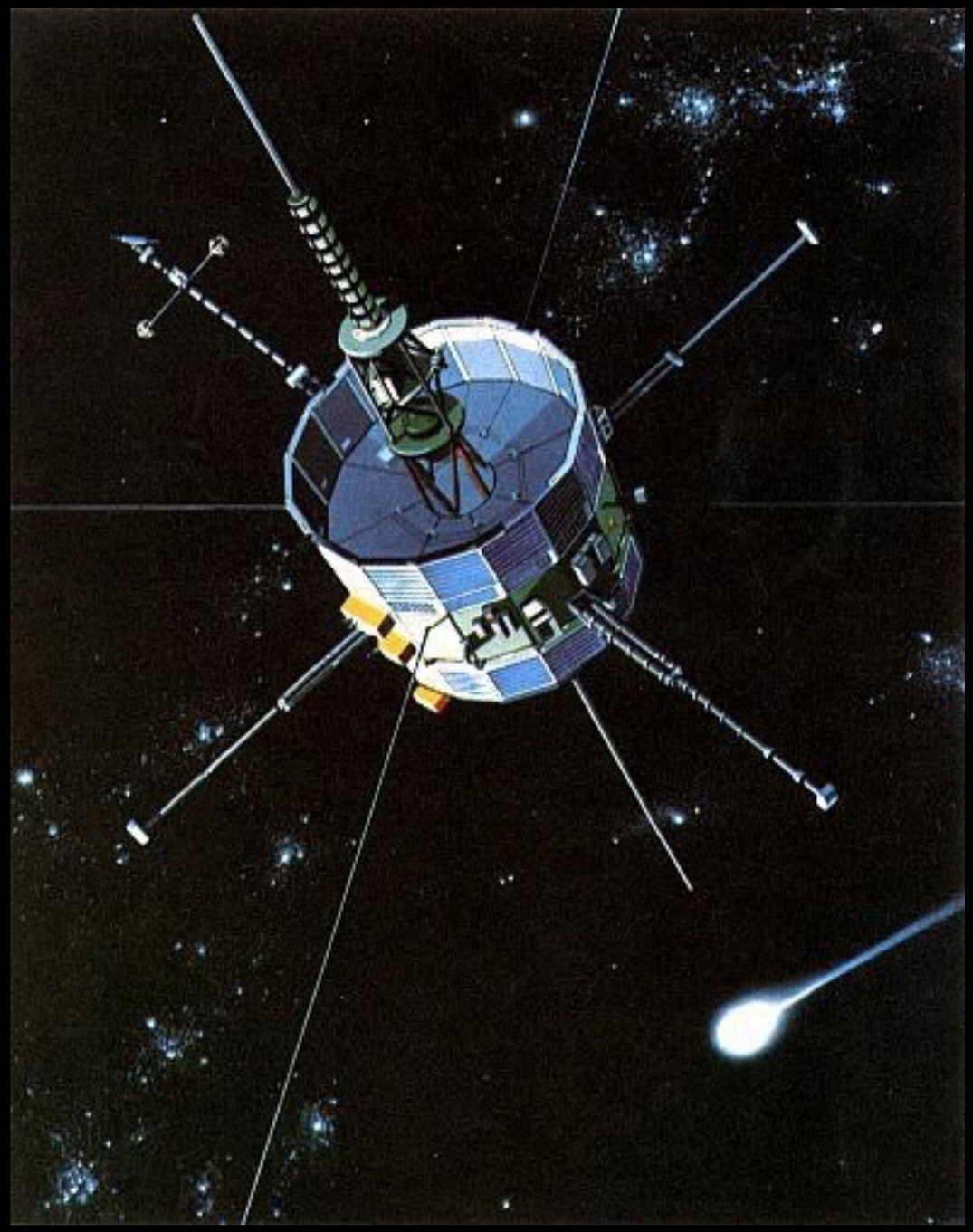
ISEE-3

- **I**nternational **S**un/**E**arth **E**xplorer 3
- Launched: August 12, 1978
- Heliocentric Orbit
- Study interaction between solar wind and Earth’s magnetic field



ISEE-3

- Renamed ICE: **I**nternational **C**ometary **E**xplorer
- First spacecraft in halo orbit at an Earth-Sun L1 (Lagrange point)
- First spacecraft to pass through tail of a comet (Giacobini-Zinner)



ISEE 3 MANEUVERS FROM LAUNCH TO HALO ORBIT TO COMET EXPLORATION

COMET HALLEY
3-28-86

COMET GIACOBINI-ZINNER
9-11-85

9-1-82

HALO ORBIT
6 MO. TRAVEL
5 YR. ORBIT

L1

6-10-82

MOON ORBIT

11-23-83

11-23-82

9-27-83

12-22-83

3-30-83

6-30-83

L2

2-8-83

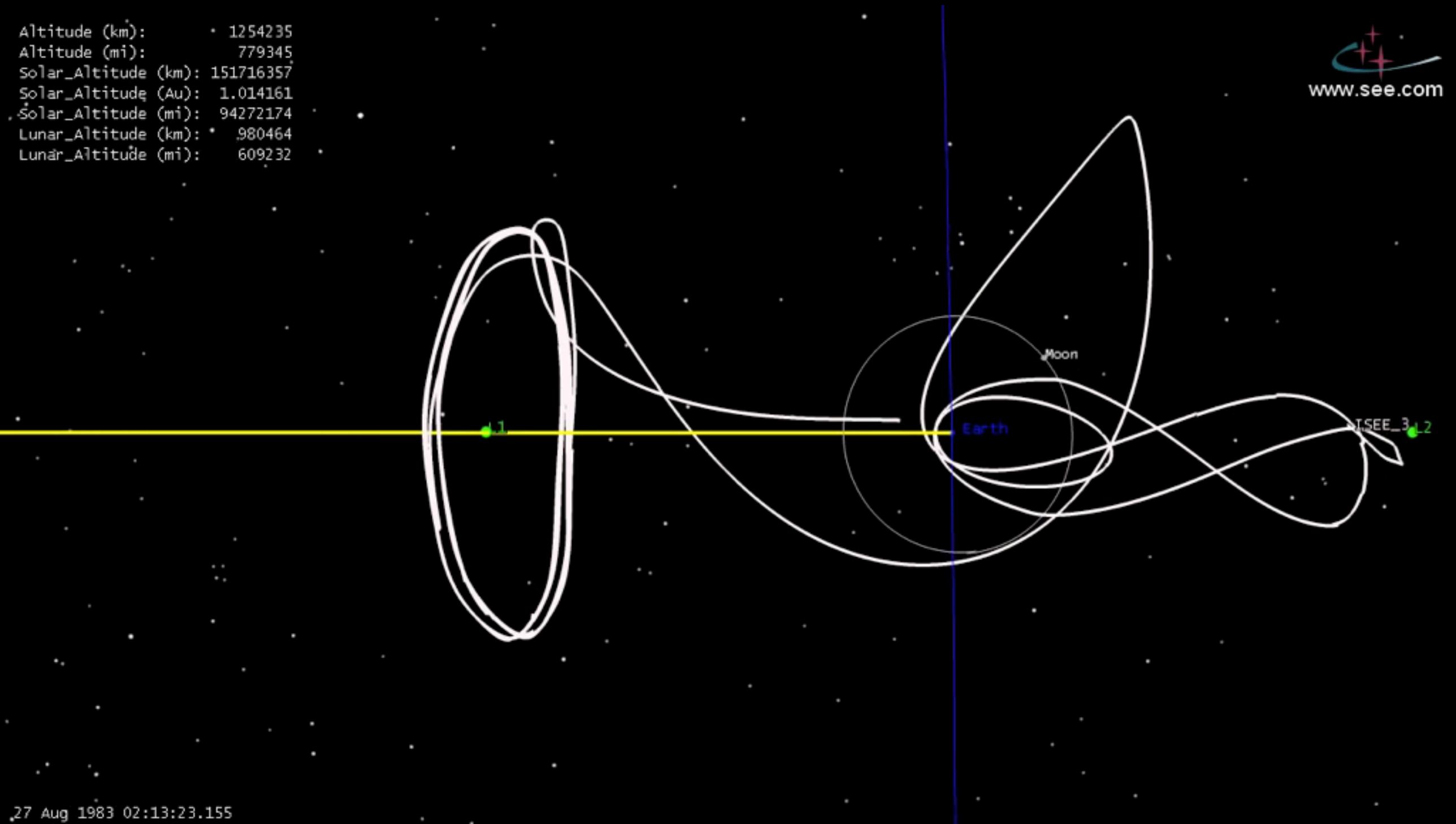
4-23-83

10-16-82

2012

DELTA 2914
LAUNCHED AUGUST 12, 1978

Slingshot Manoeuvre after Orbiting L1

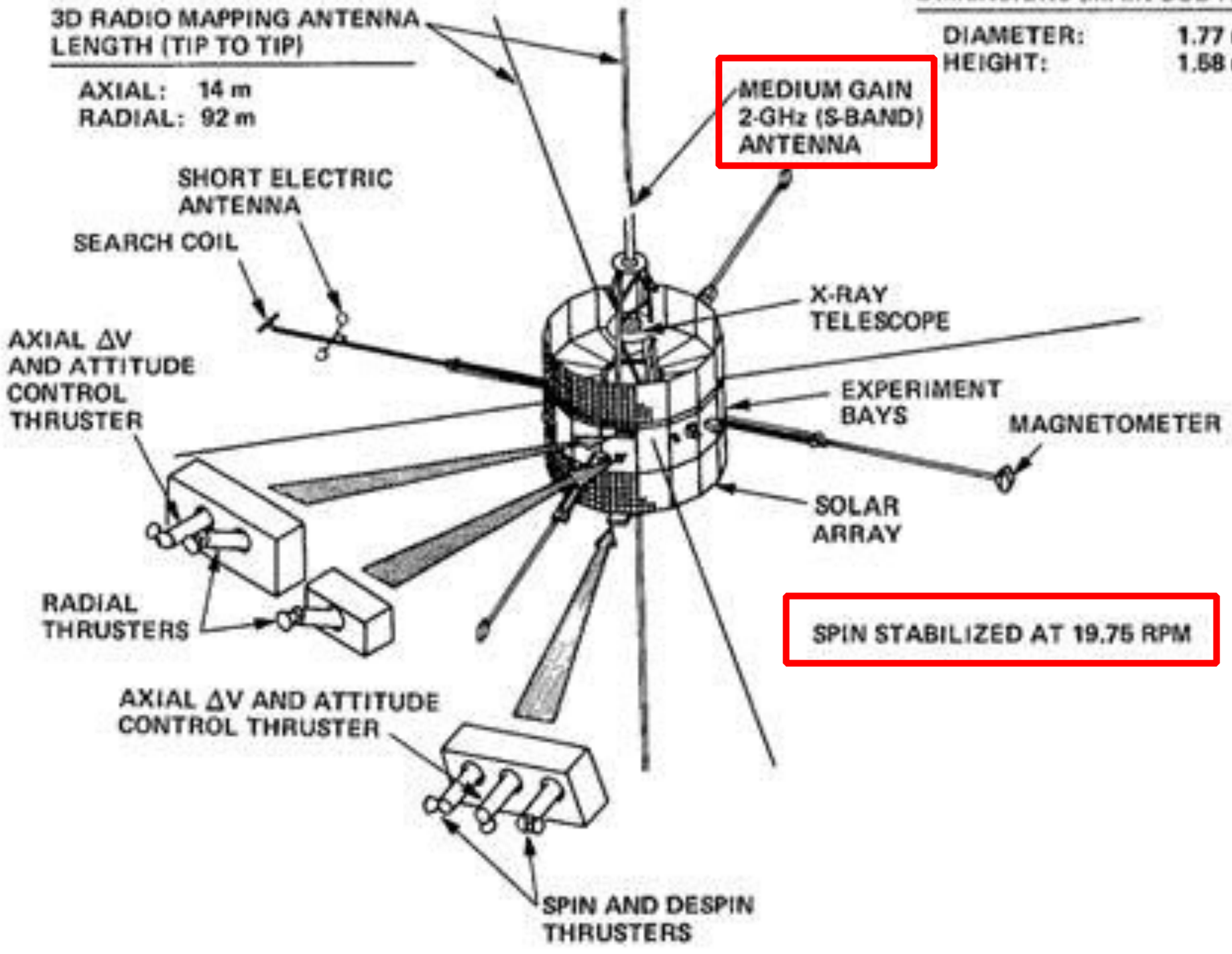


TOTAL S/C WEIGHT: 479 kg

EXPERIMENTS: 104 kg
HYDRAZINE: 89 kg

DIMENSIONS (MAIN BODY)

DIAMETER: 1.77 m
HEIGHT: 1.58 m

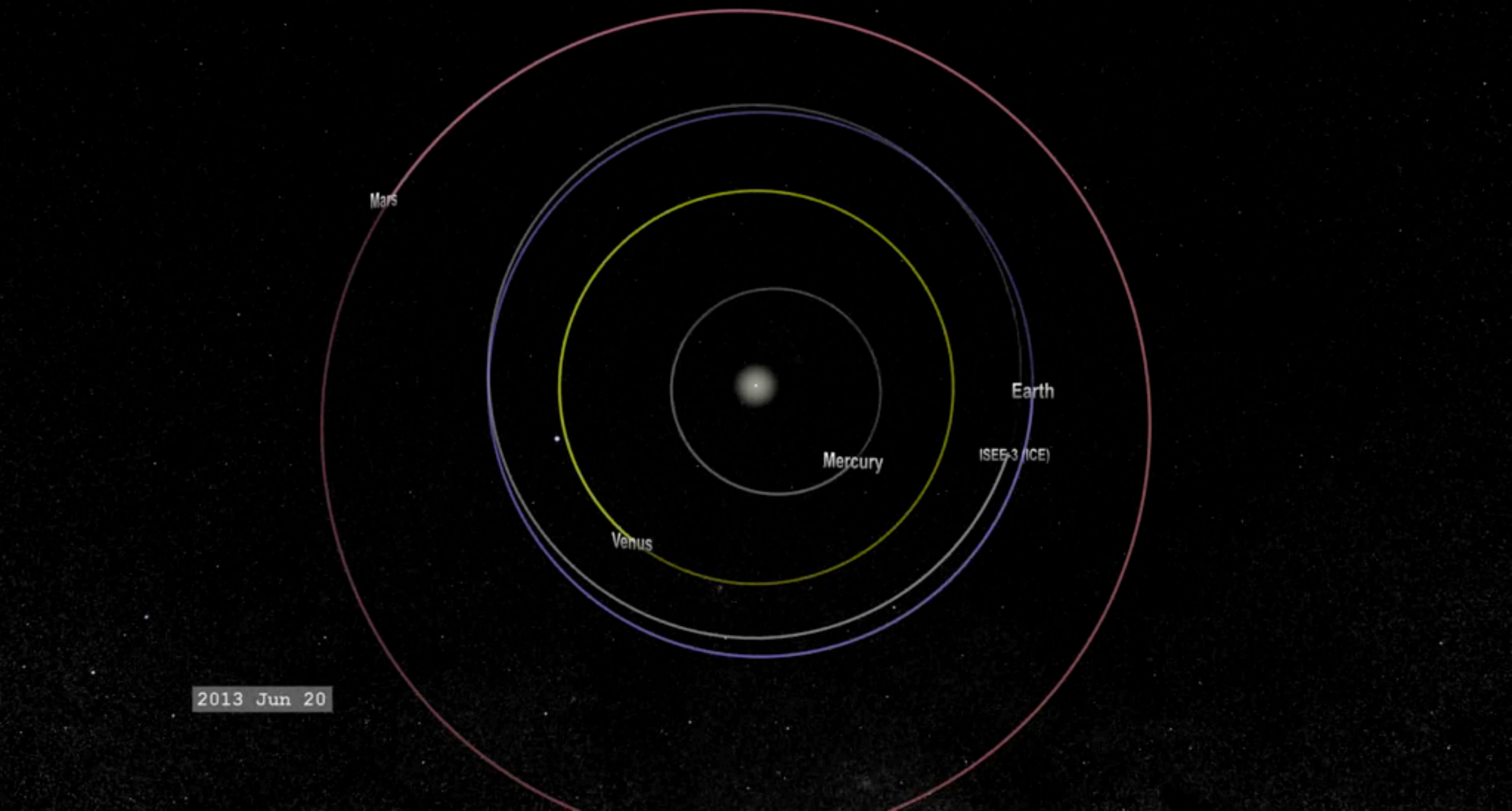


SPIN STABILIZED AT 19.75 RPM

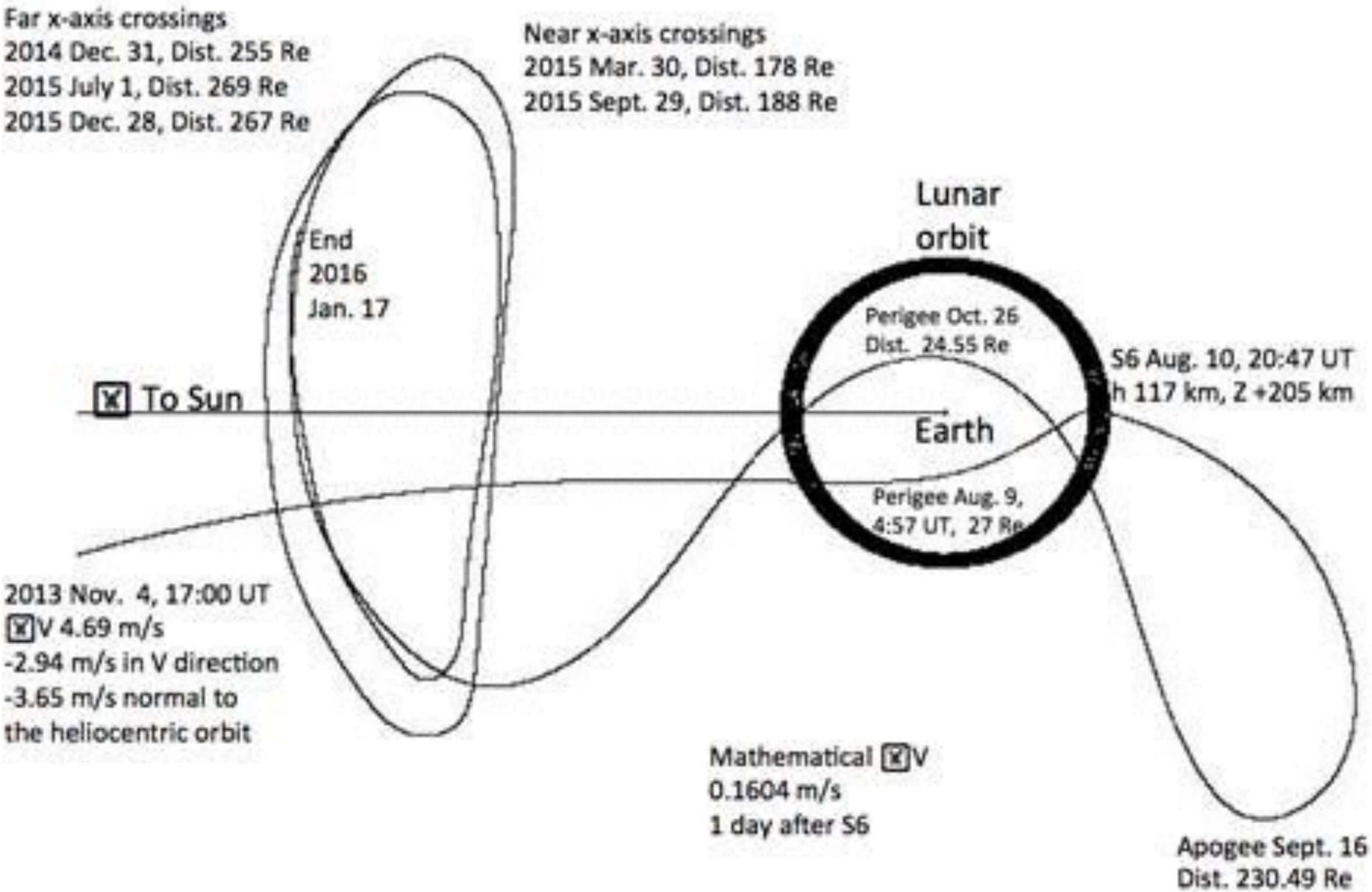
Old Telemetry Screen

```
ISEE-C;CPU1;  64;ACN;ORB 000;BUS V 28.29;ES CURR 1.34;NE CURR 6.69
OH   0.0; 0.000 RPM; 0.000 SEC;CMD CTR A;B  00; 79;S/C 037/22:24:49 (30261143)
S/C HSK; PAGE 4              RESET CTR A;B 640;639;GMT 074/22:18:00.115 78/03/15
-ATTITUDE AND ORBIT CONTROL SUBSYSTEM-  ---- HYDRAZINE PROPULSION SYSTEM ---
- ELECTRONICS A -   - ELECTRONICS B -   PRI HTRS 1/2  LOW   ACCL CTR 1/2  110
LOGIC PWR     ON   LOGIC PWR     ON    SEC HTRS 1/2  OFF   ACCL T 1/2   24.4
+28V PWR      ON   +28V PWR     OFF    ACL PWR 1/2  2.50 T PRI TK HTRS   OFF
TSL             010TSL 010010          PRI TK HTRS100100    SEC TK HTRS   OFF
SINIT 011100   OFF   SINIT 101110 100001 SEC TK101110 100111 LATCH VALVB   OFF
SECT WIDTH     360   SECT WIDTH    OFF  LATCH VALVA  OPEN  LATCH VALVD  OPEN
FIRINGS         36   FIRINGS        77  LATCH VALVC  CLOS  THERMO CPLF 346.2
RATIO FIRING   DIS   RATIO FIRING  DIS  THERMO CPL  248.6  TANK PRESS    2.4
THRUST RATI      2   THRUST RATI   114  TANK PRESS    2.7
MANEUVER      TERM   MANEUVER      INIT
MANEUV COMPL   NO   MANEUV COMPL  YES


                                                          FRAME NUMBER  173
```

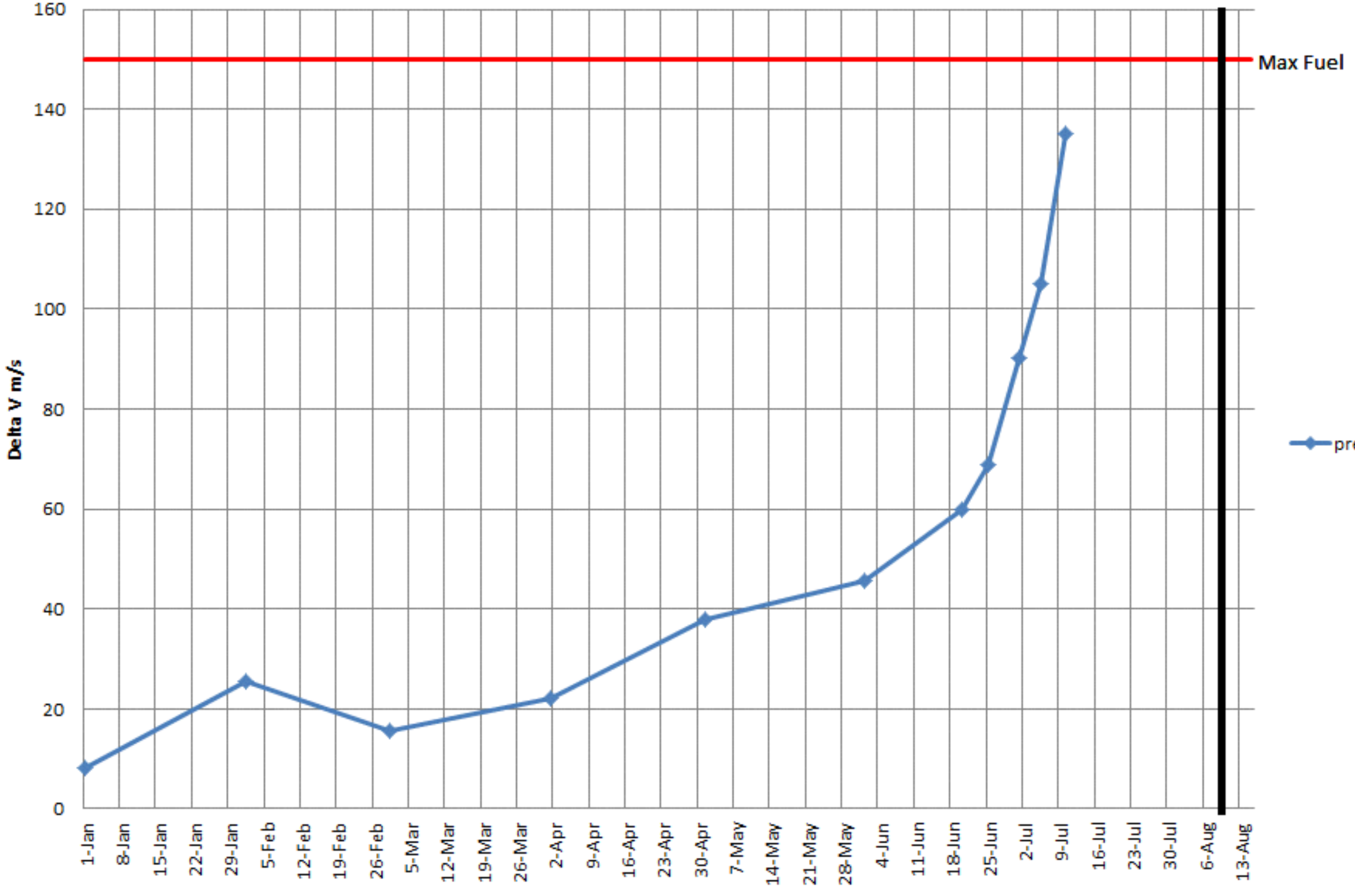
ISEE-3 Revisiting Earth



Success Case



Total Delta V Requirement to Bring ISEE-3 Back to L1

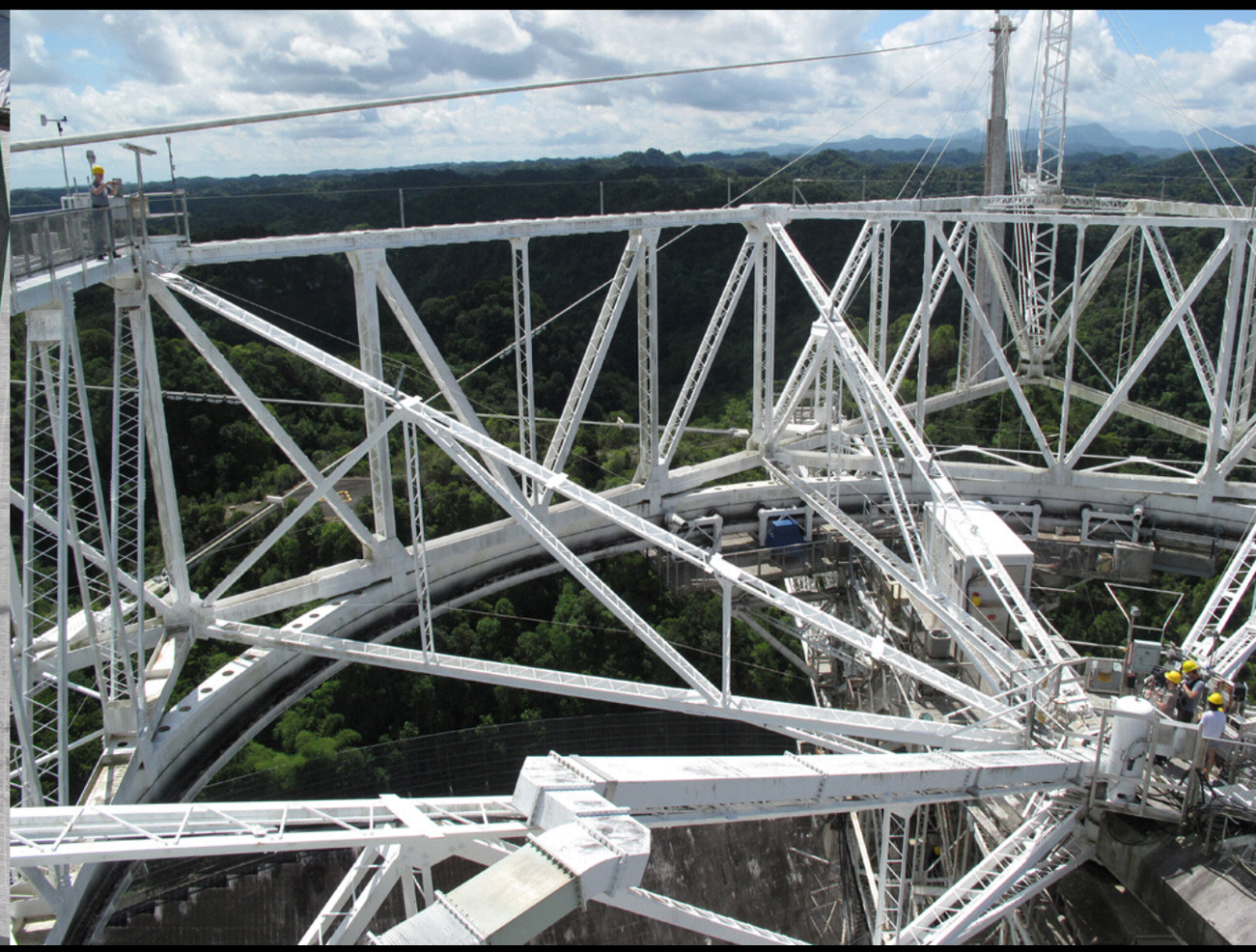


Python Real-time Tracker

```
UTC  : 2014-05-28 07:50:06.234132
Local: 2014-05-28 03:50:06.234096 (-4.0)

Lines: 471/2881 (2410 left)

Speed (km/s) : -3.4829406
Speed (m/s)  : -3482.9406368
Speed (km/hr): -12538.5862925

Dist (AU) : 0.10369466811595
Dist (km) : 15512501.553089

Light time (one-way) : 51.744135 s
Light time (two-way) : 103.488271 s

R.A.:  7.7720059526
Decl: +21.4076608943
(adjusted for light time)

Downlink frequencies:

2.270400000 GHz: 2.270426377 GHz (+26.377449 kHz)
2.217500000 GHz: 2.217525763 GHz (+25.762858 kHz)
```

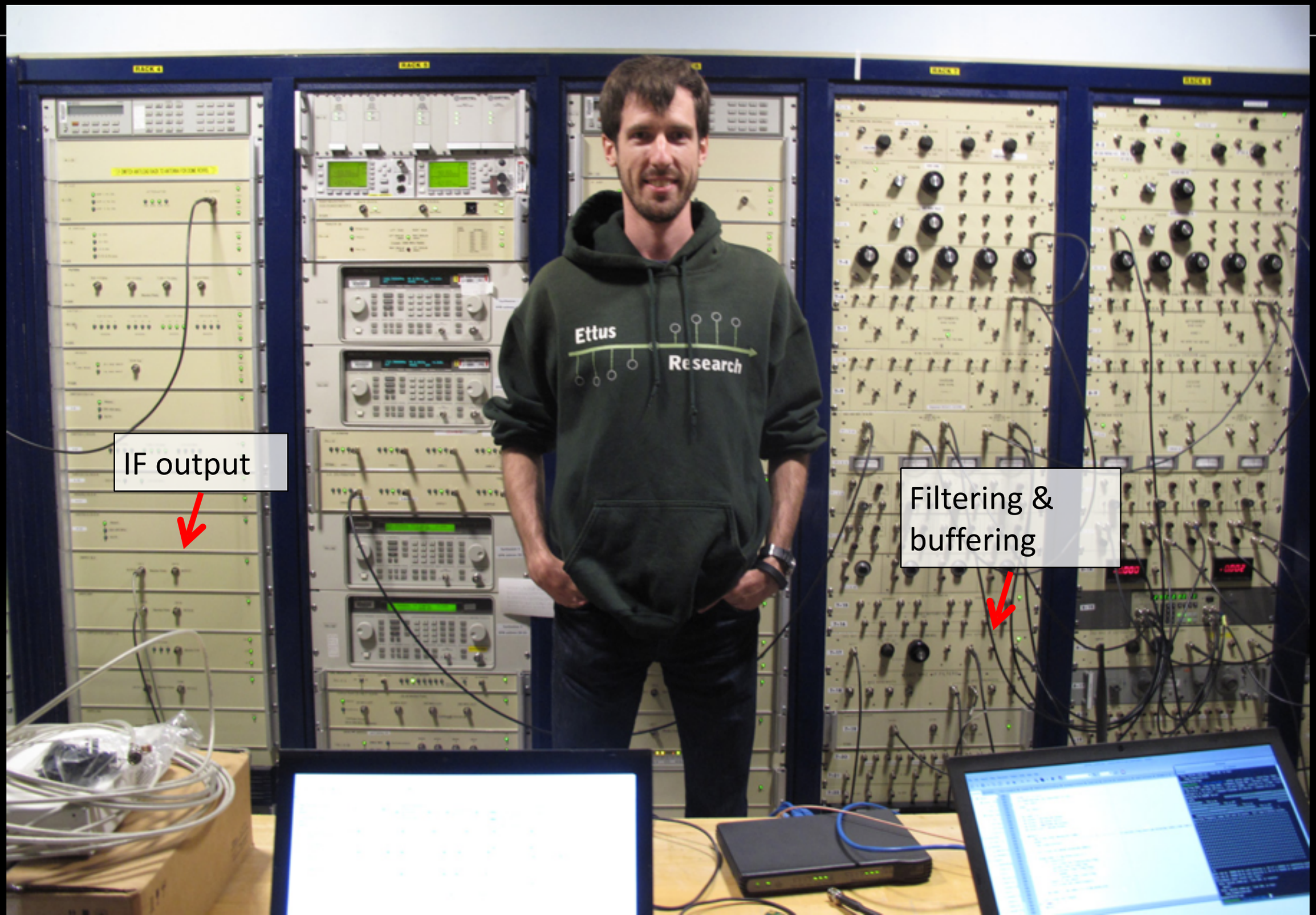
Arecibo Radio Observatory

View from Above

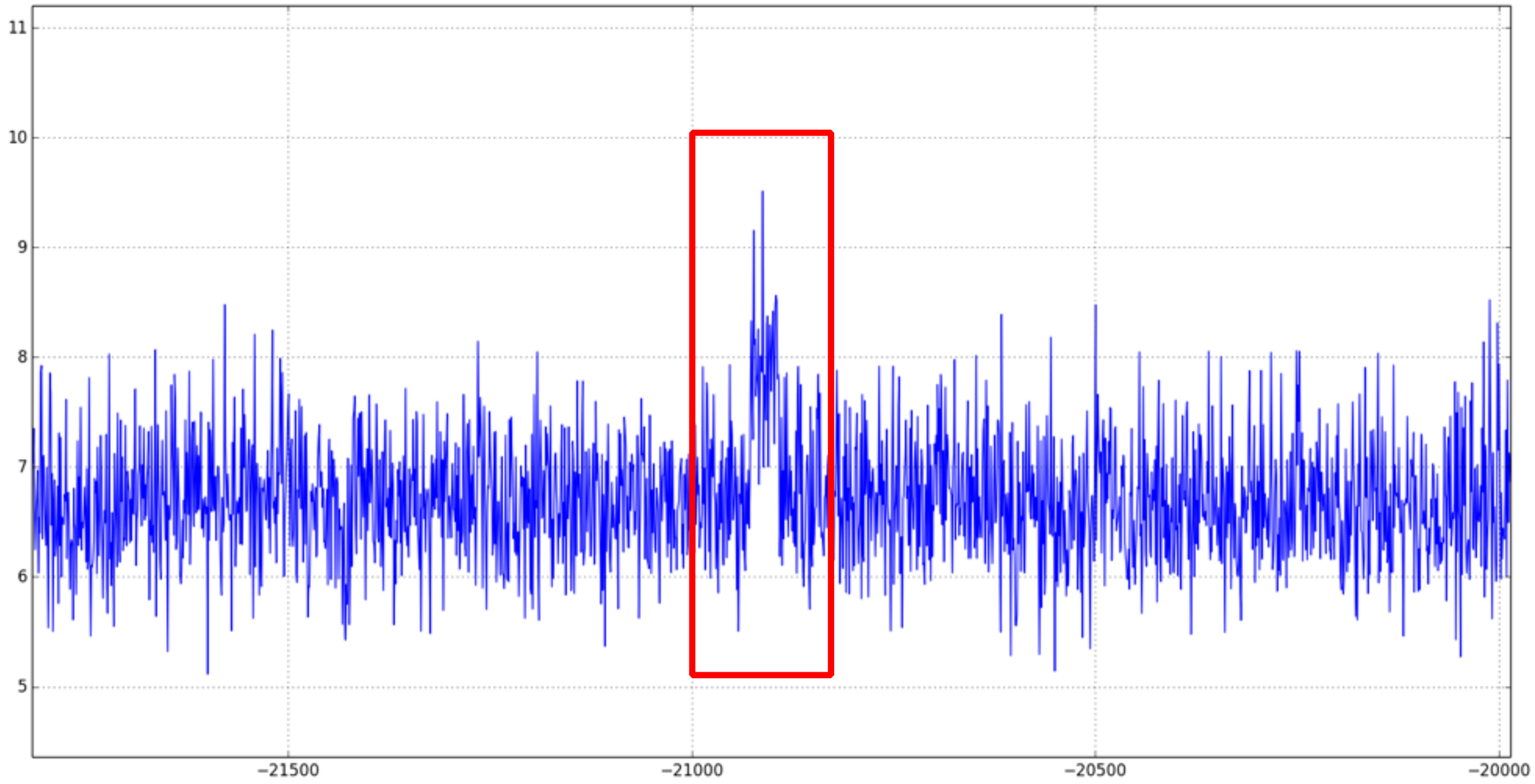


Ionospheric heaters

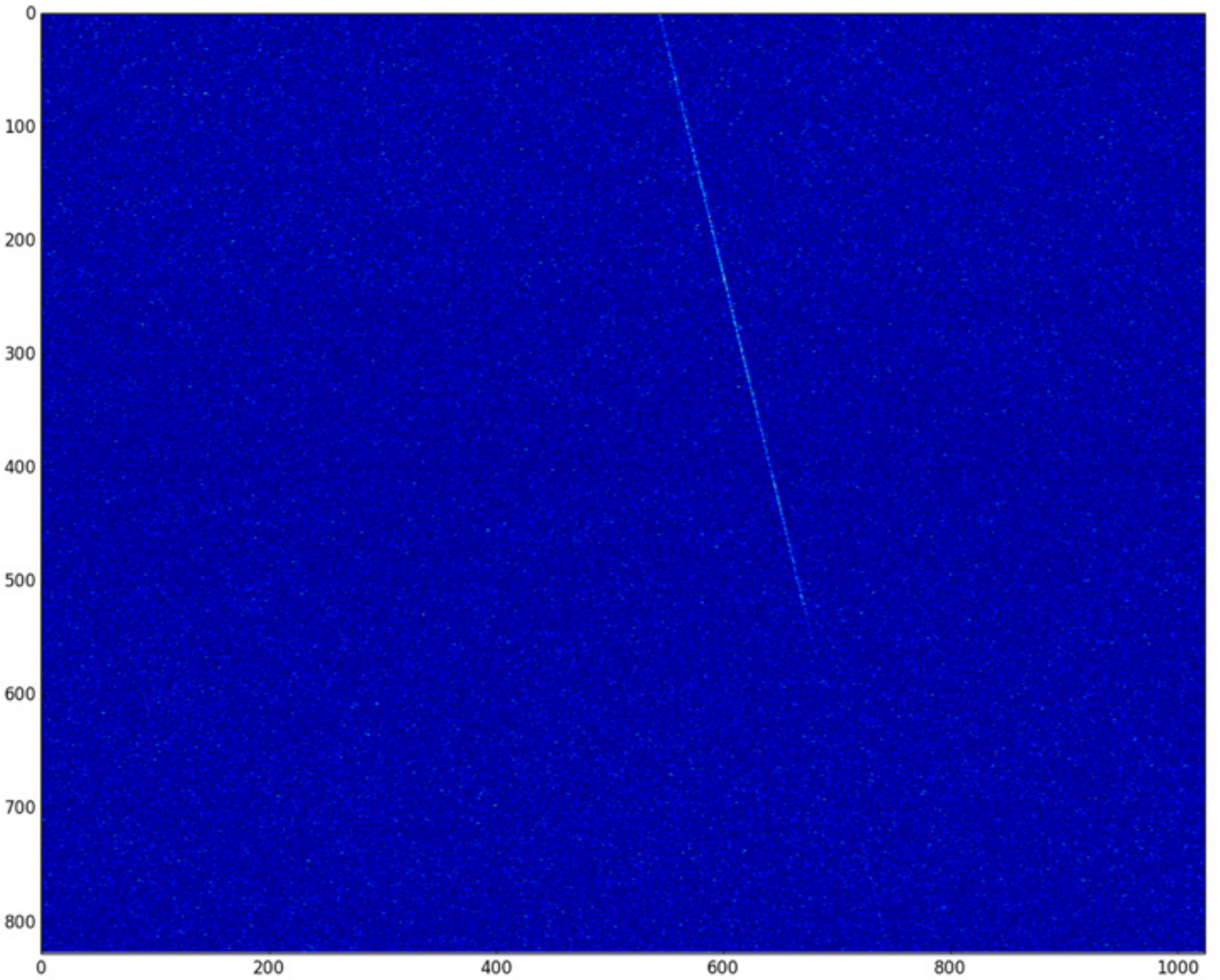
IF Panel



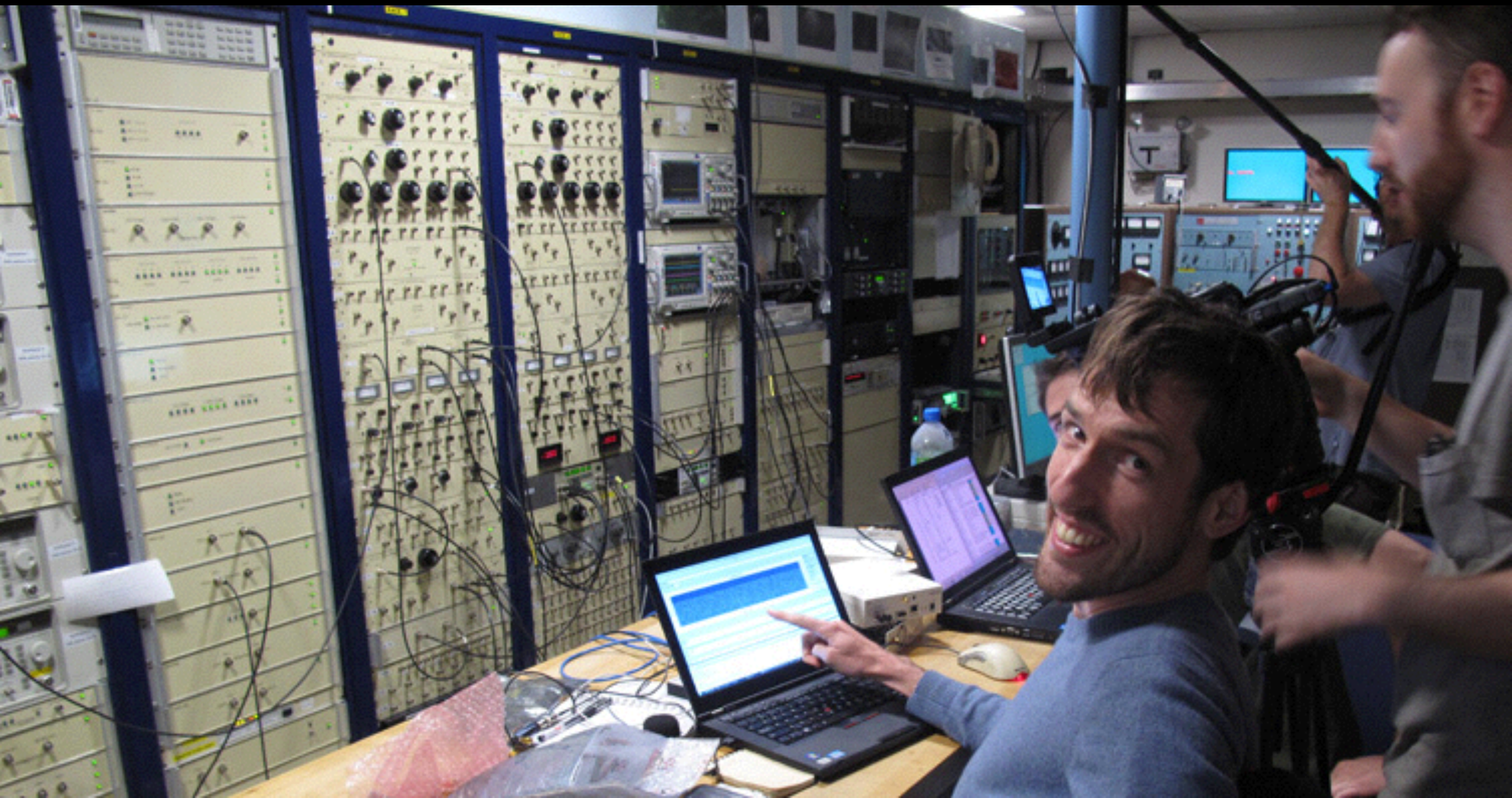
Weak Signal → Low RBW



numpy & matplotlib

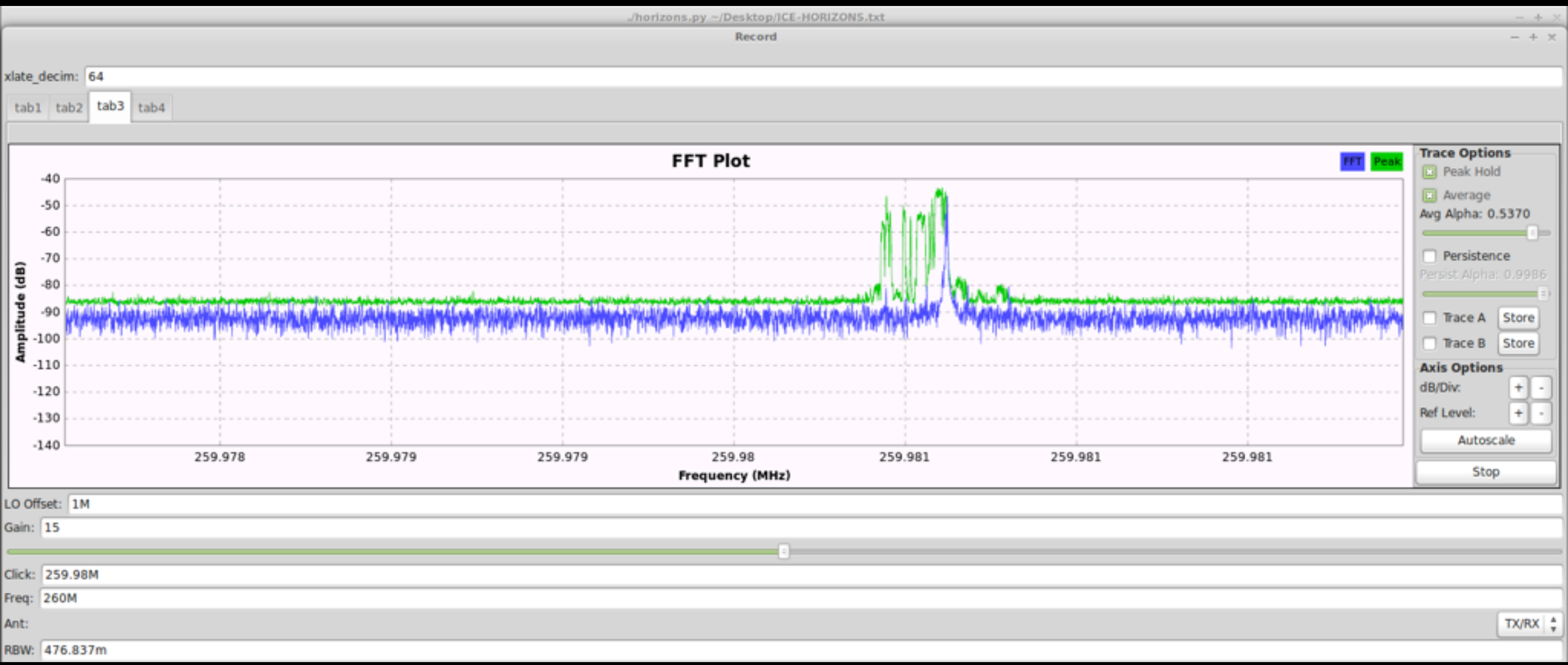


Receiving Unmodulated Carrier



After Improving Pointing

- ~45 dB C/N
- Moving peak below due to Doppler shift

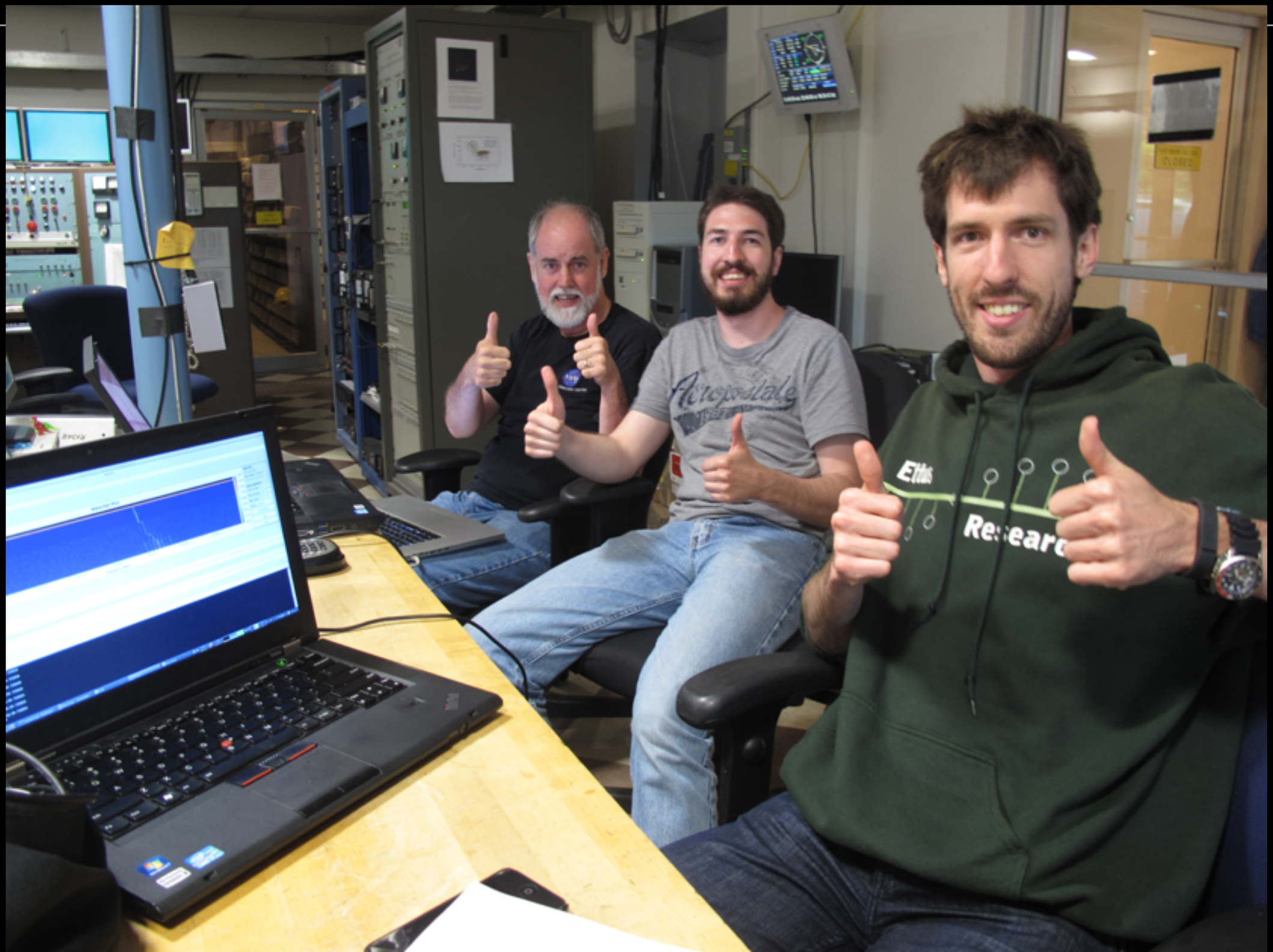


Media

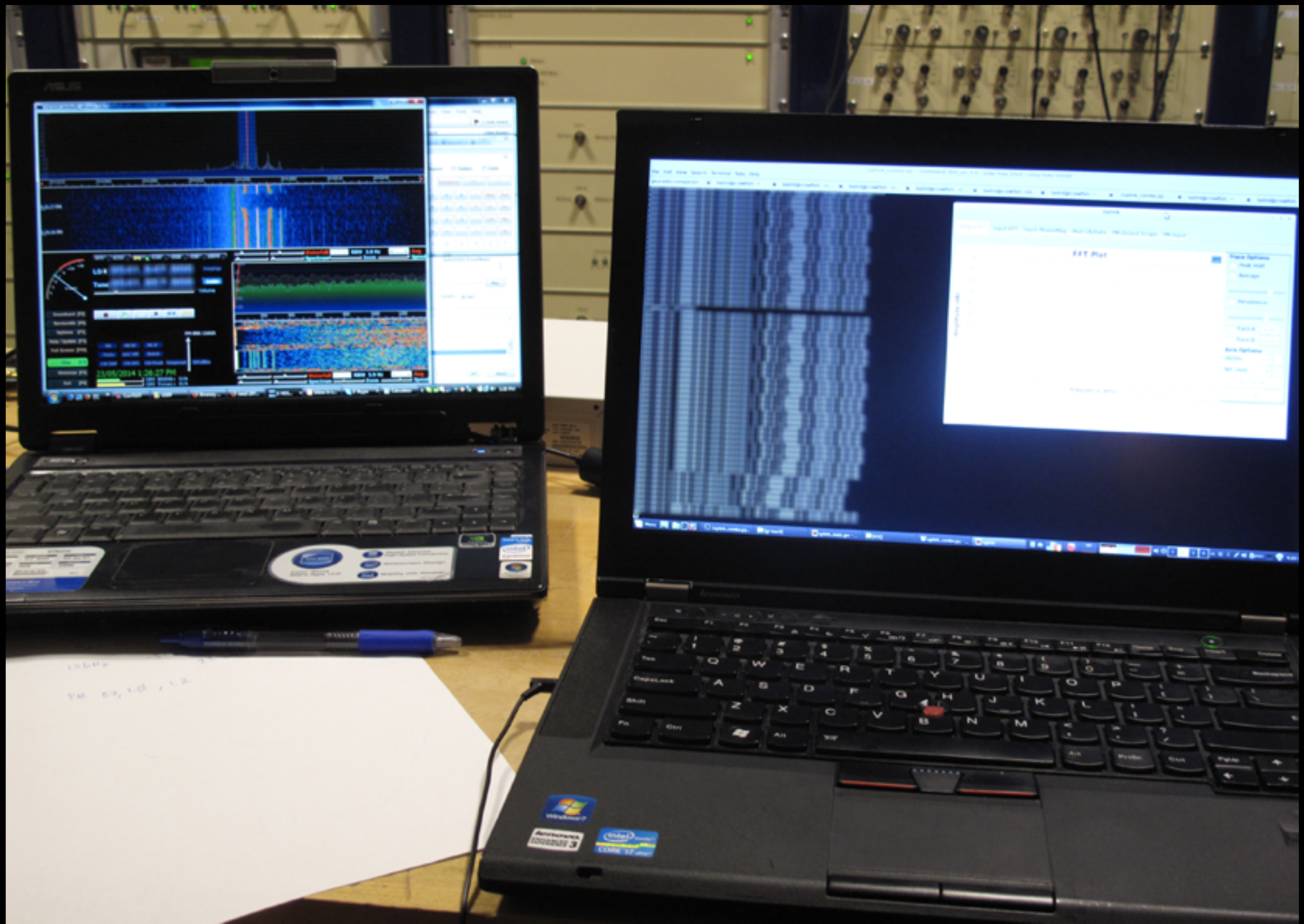
- Wide-spread coverage
- #ISEE3, @ISEE3Reboot, @EttusResearch, @spenchdotnet
- This particular photo has appeared on The Register, CBS News…

Preparing for Uplink

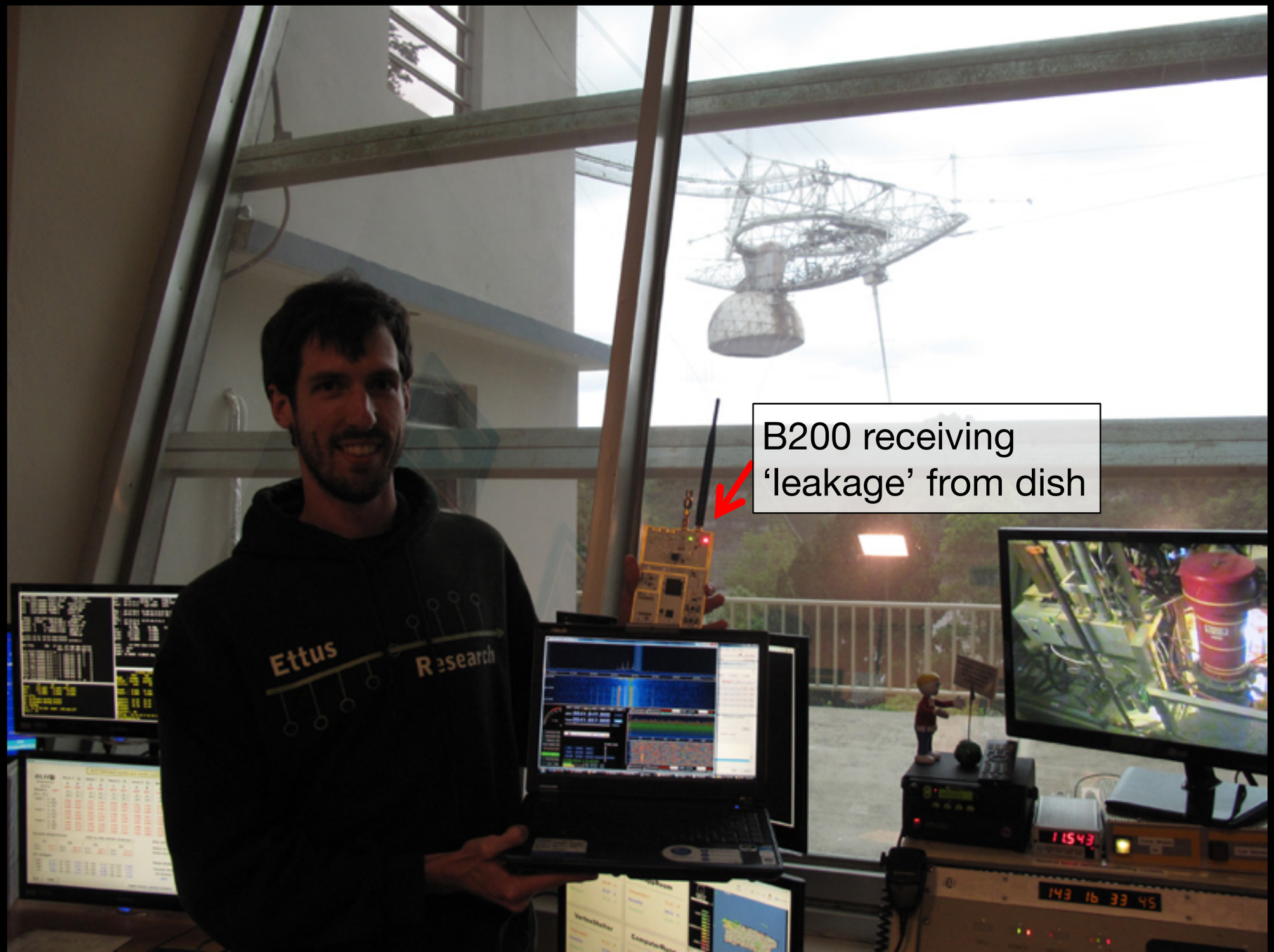
Fingers Crossed

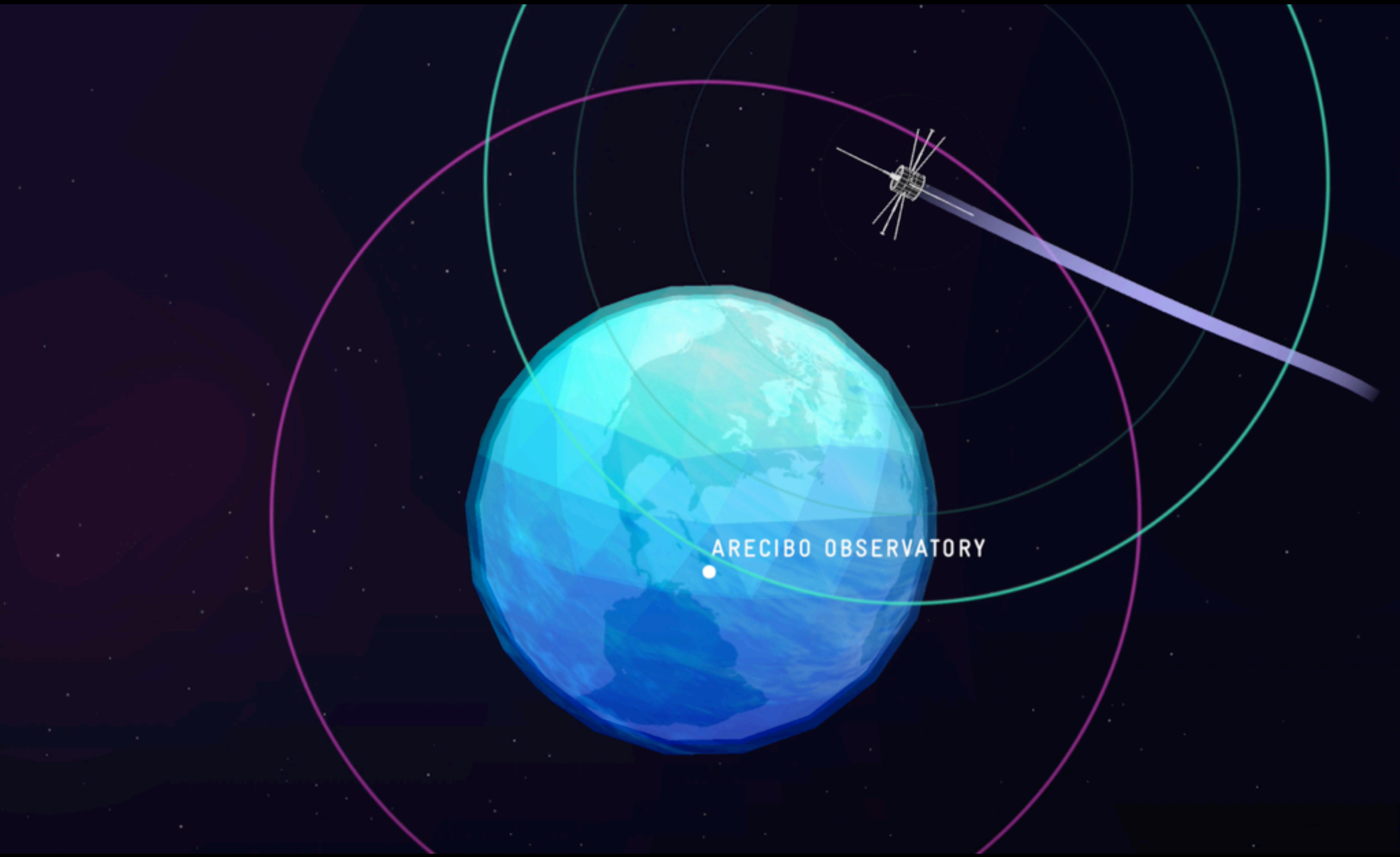


Transmission to Enable Telemetry



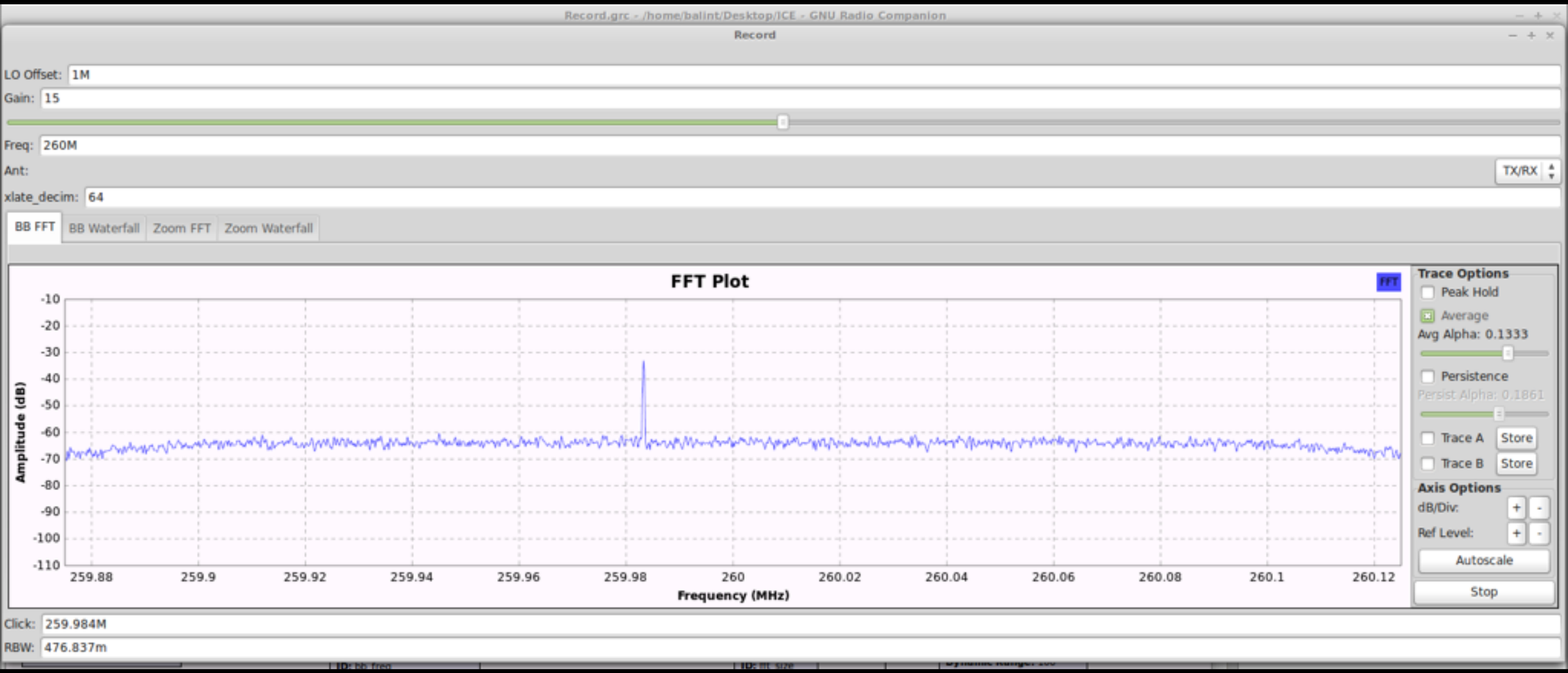
Verifying Transmitted Signal



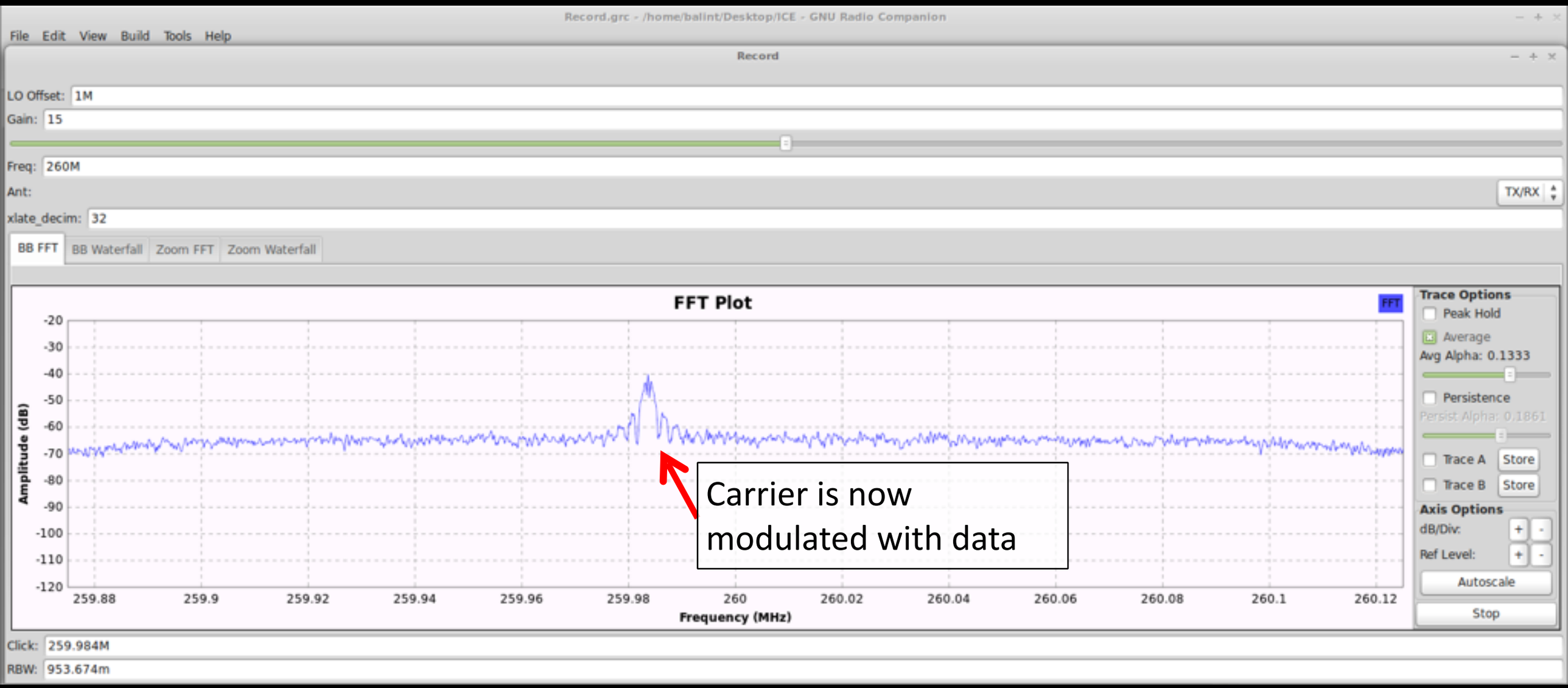

ARECIBO OBSERVATORY

Round-trip Suspense

Live Sampled Baseband

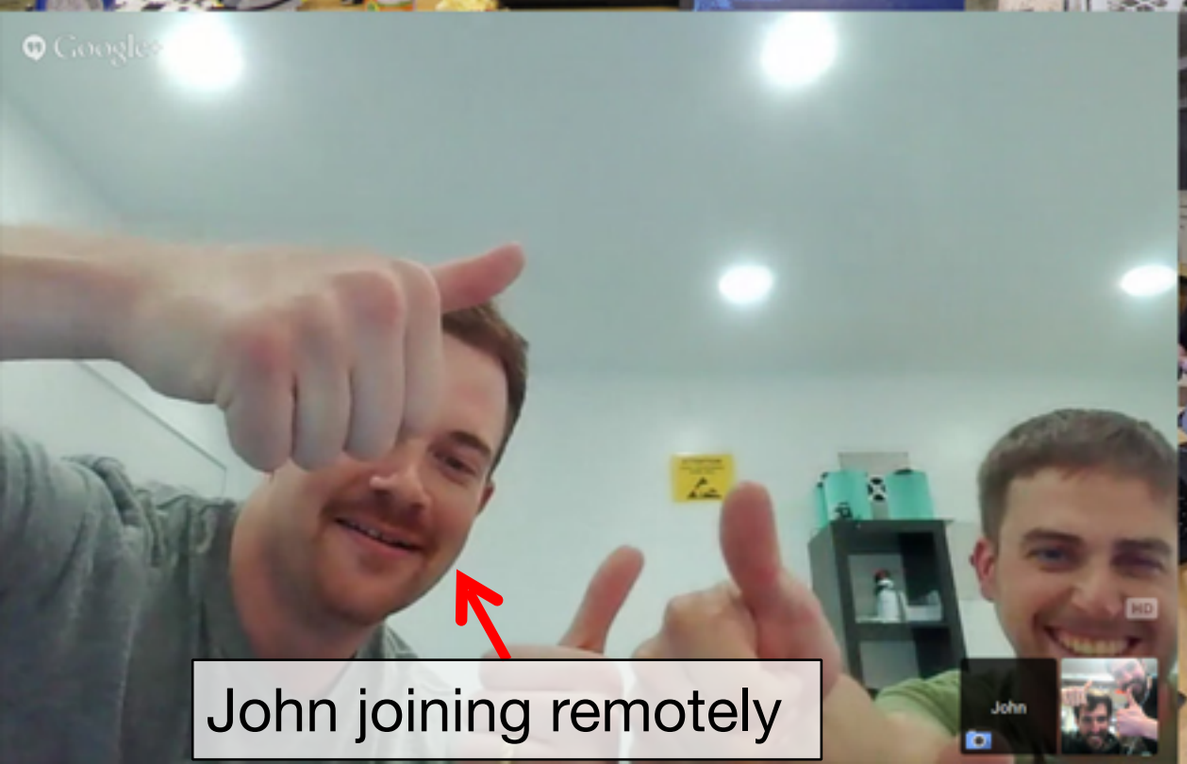


Live Sampled Baseband



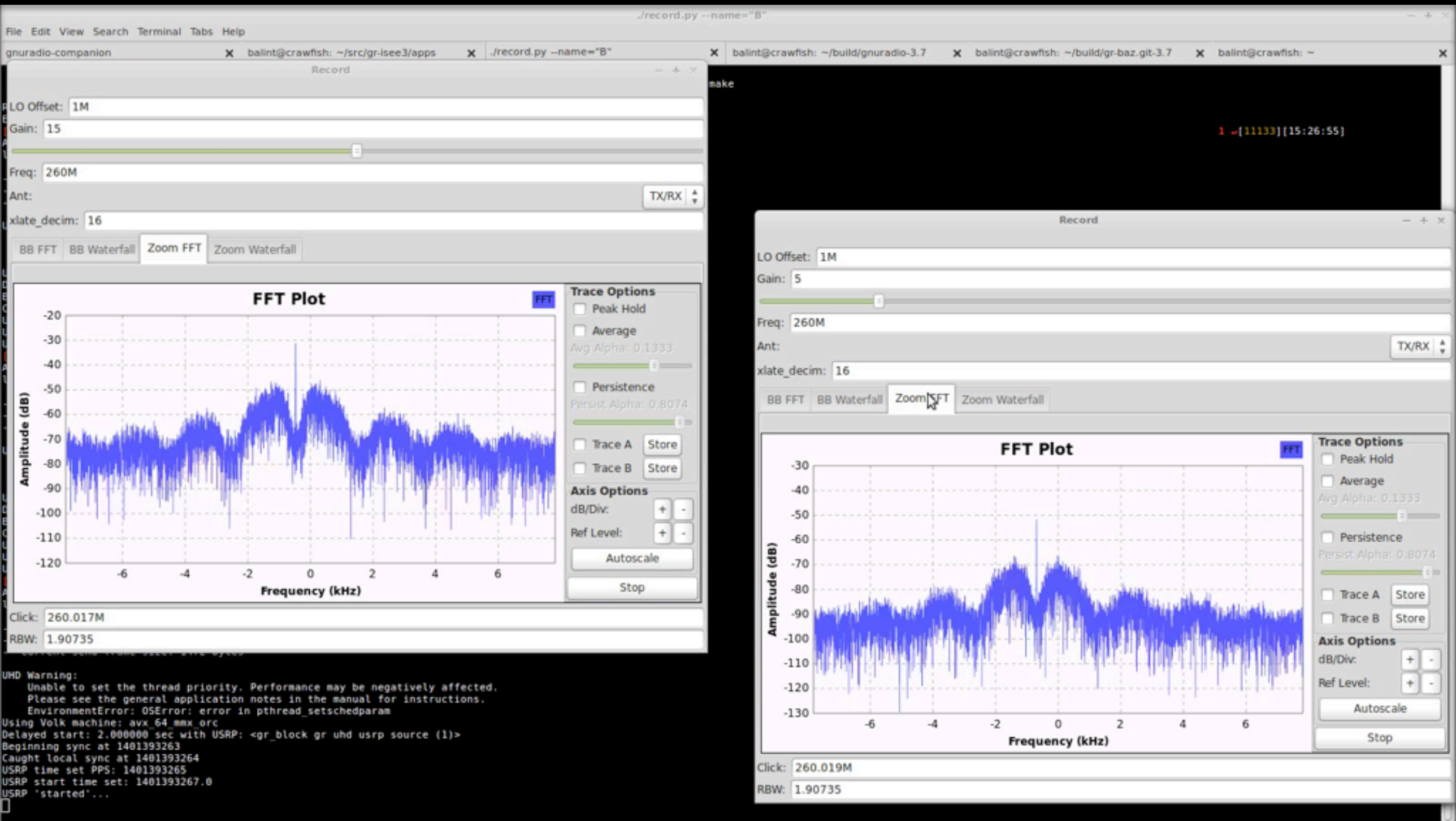
Celebration

Phil Perillat: lives and breathes the telescope



John joining remotely

Telemetry Modulated on Transponders A & B



PLL Loop BW: 10

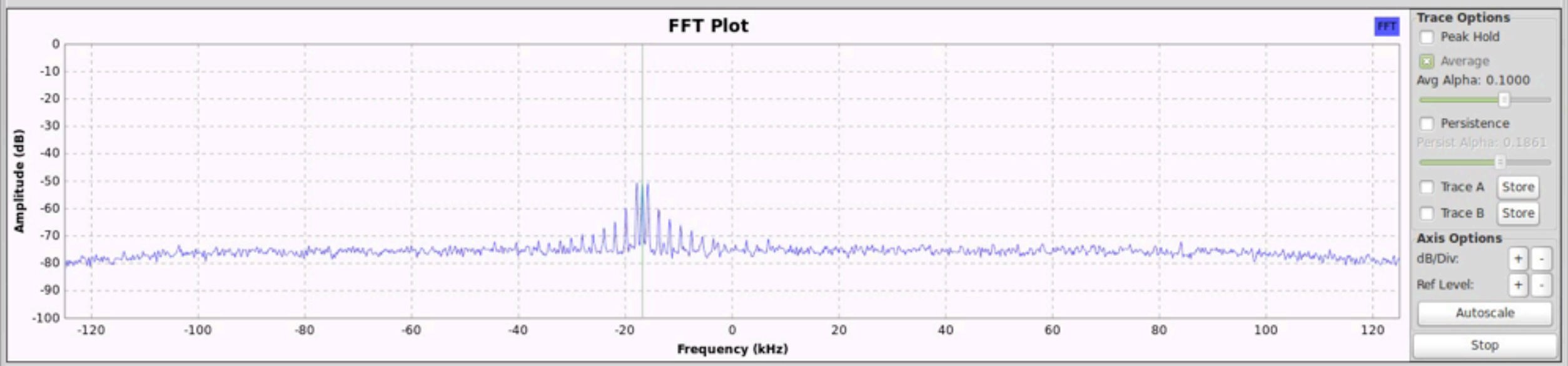
XLate Offset: -16.7798k

XLate BW: 3.75k

SC PLL Freq: 1k

SC PLL Loop BW: 100

FFT | Waterfall | BB FFT | BB Waterfall | PLL FFT | PLL Waterfall | Phase XY | Arg | Cyclo | Shaped | Clock | Sync | Costas | MPSK | Audio | Cyclo



Delay: 1

Audio Tone Offset: 3.5k

Audio Tone Mul: 200

PLL Loop BW: 10

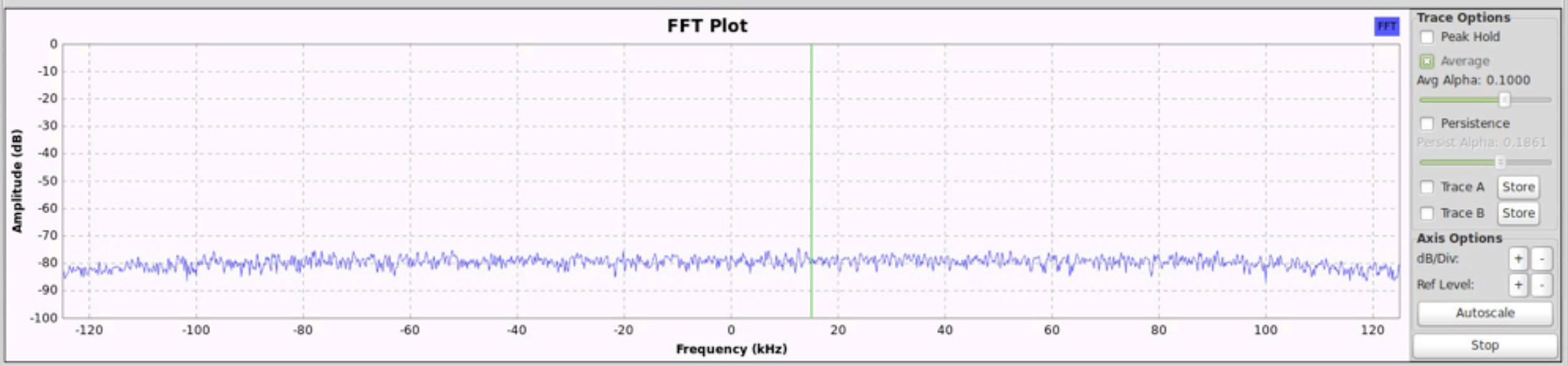
XLate Offset: 15.083k

XLate BW: 3.75k

SC PLL Freq: 1k

SC PLL Loop BW: 100

FFT | Waterfall | BB FFT | BB Waterfall | PLL FFT | PLL Waterfall | Phase XY | Arg | Cyclo | Shaped | Clock | Sync | Costas | MPSK | Audio | Cyclo

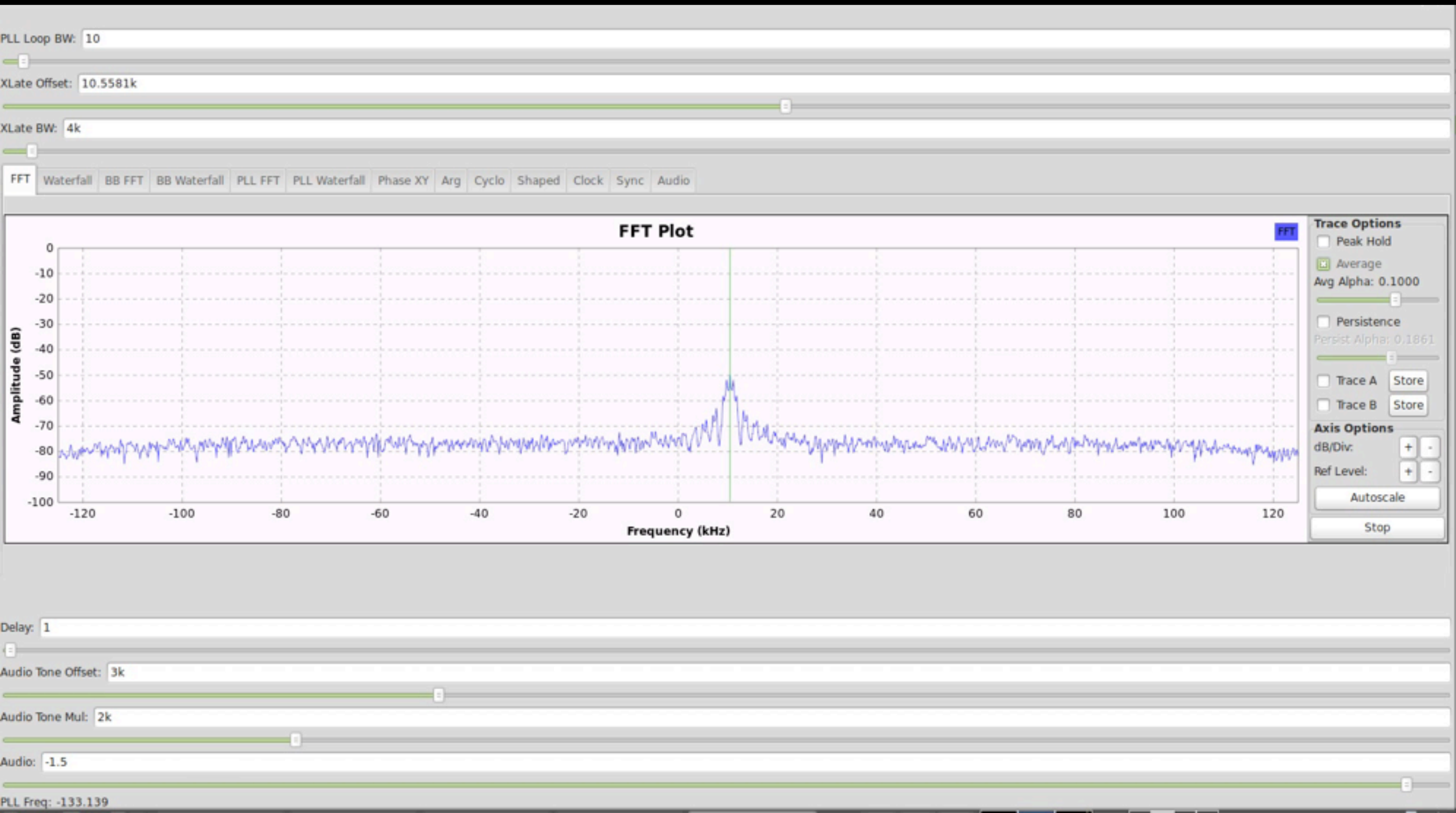


Delay: 1

Audio Tone Offset: 3.5k

Audio Tone Mul: 200

Telemetry Demodulation & Decoding (512 bps)

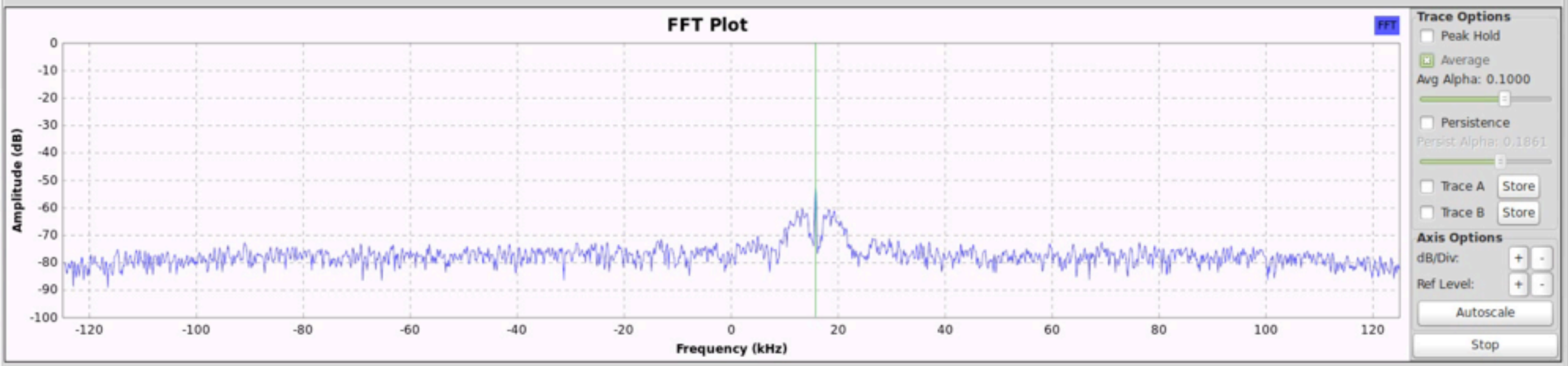


PLL Loop BW: 10

XLate Offset: 15.8371k

XLate BW: 18k

FFT | Waterfall | BB FFT | BB Waterfall | PLL FFT | PLL Waterfall | Phase XY | Arg | Cyclo | Shaped | Clock | Sync | Audio



Delay: 1

Audio Tone Offset: 8k

Audio Tone Mul: 5k

Audio: -1.5

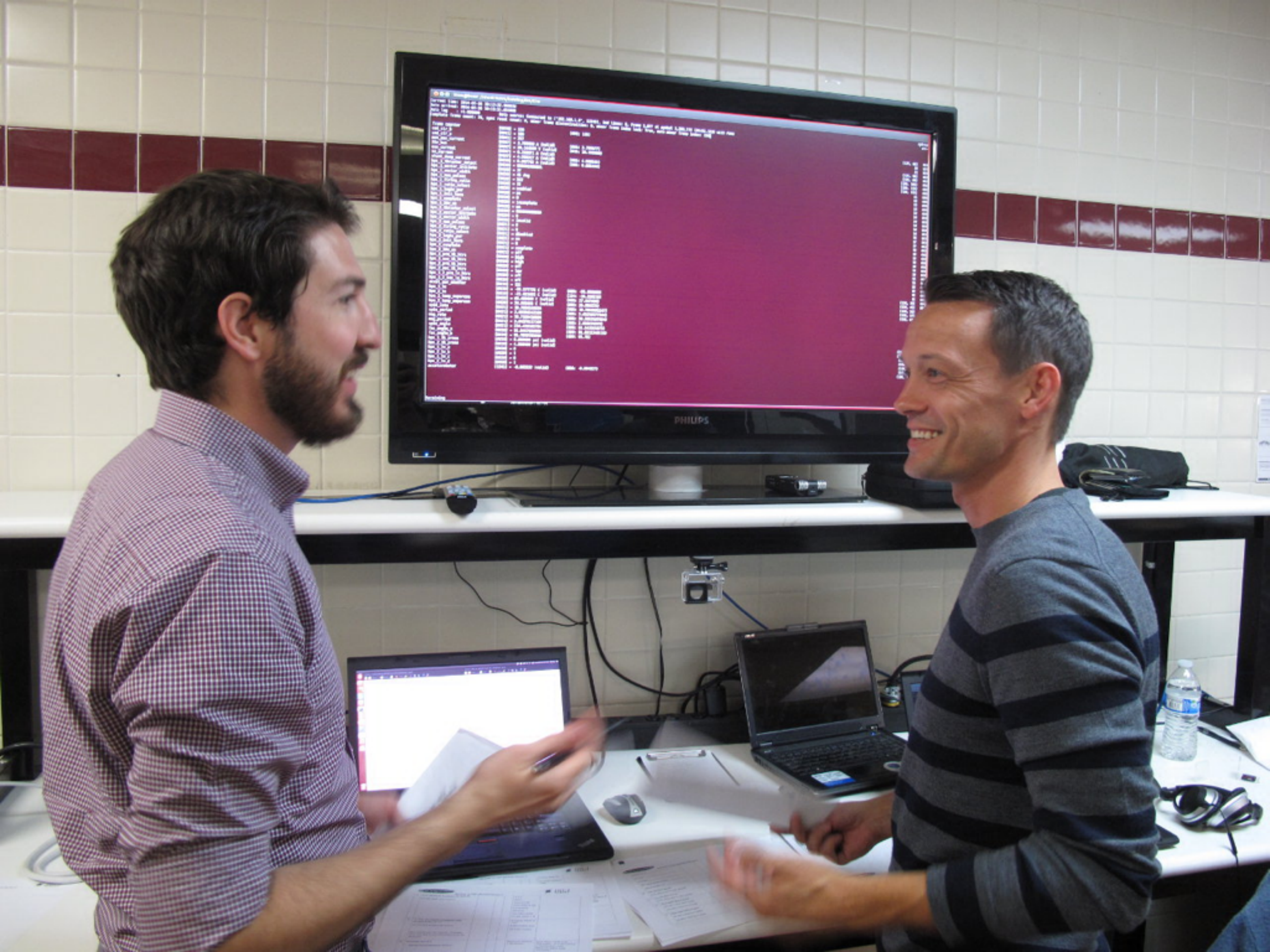
PLL Freq: -65.9914

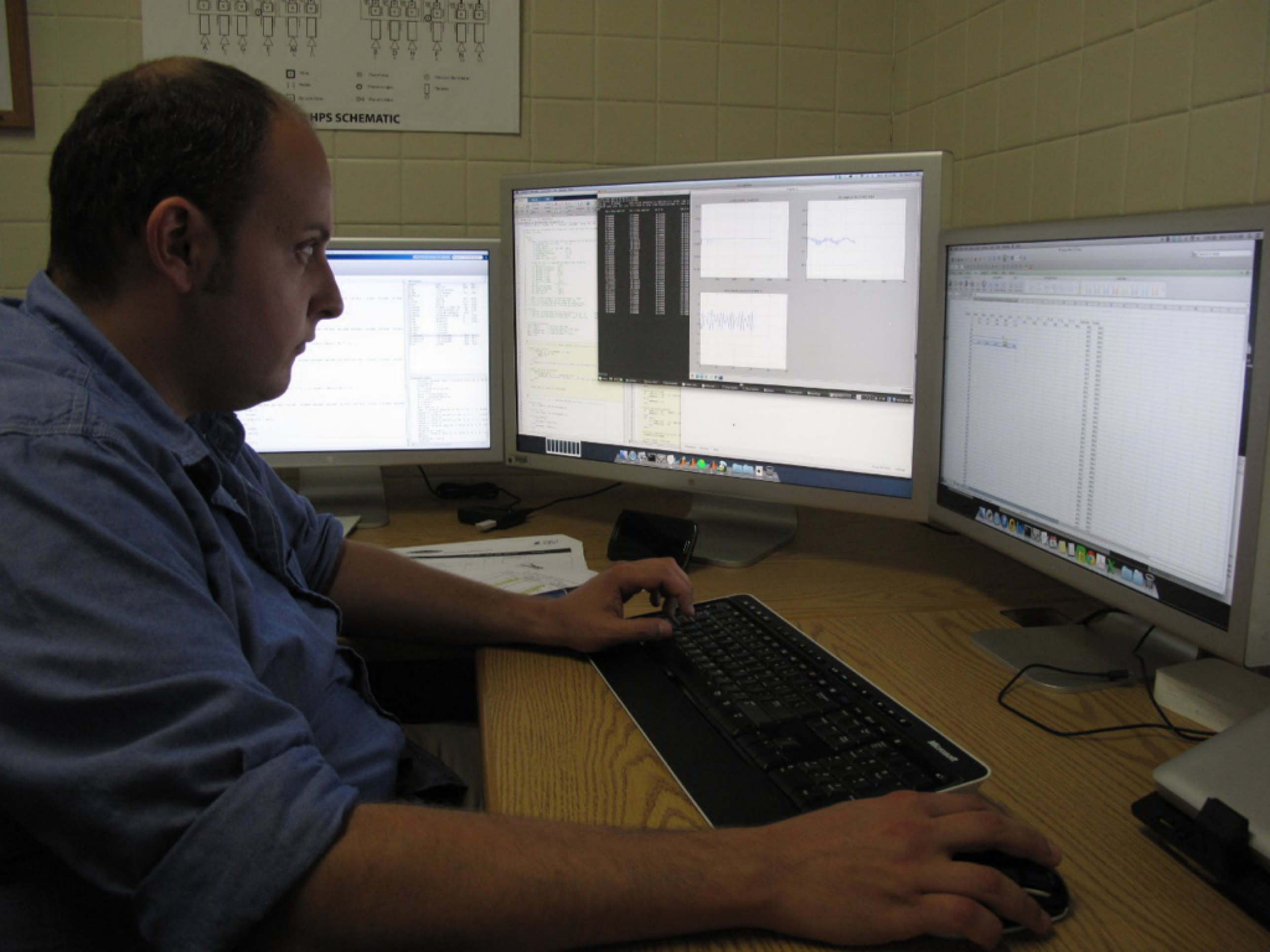
Propulsion System

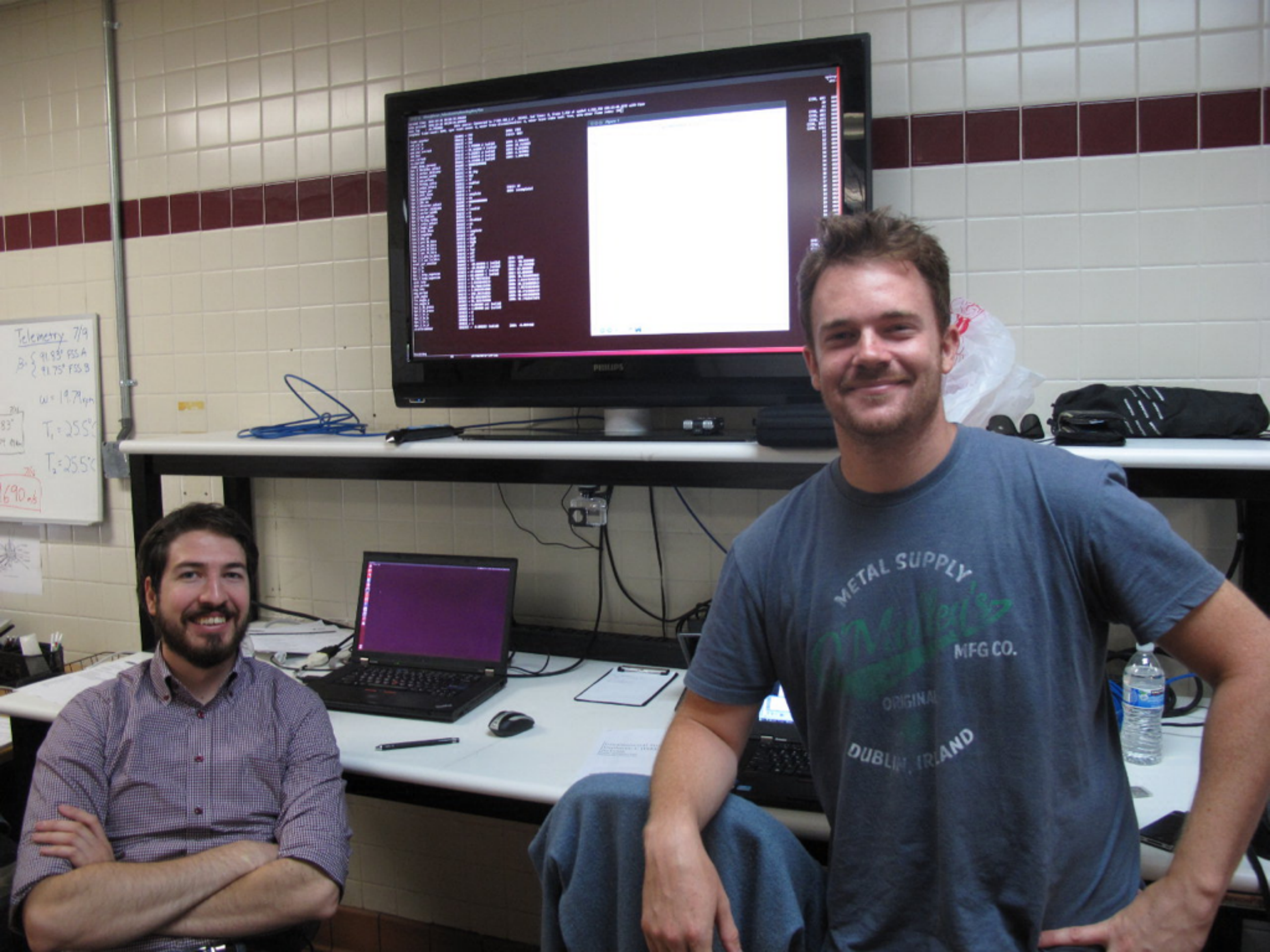
```
Current time: 2014-06-24 13:50:54.153003                                                                                                spinup
Data arrived: 2014-06-24 13:50:54.161531                                                                                                `st~
Data lag    : -0.008515         Data source: Rate: 1027, drops: 0000
Complete frame count: 9, sync reset count: 3, minor frame discontinuities: 5

 frame counter              [0012] = 136                        (001: 135)                                          (136, 60)   001
 cmd_ctr_b                  [0010] = 251                        (008: 96)                                                20   001
 cmd_ctr_a                  [0010] = 149                        (008: 0)                                                 21   000
 non_ess_current            [0015] = 3.951613 A (valid)         (004: 3.911290)                                     (136, 85)   000
 28v_bus                    [0016] = 28.144000 V (valid)        (008: 28.136000)                                    (136, 86)   000
 ess_current                [0015] = 0.233871 A (valid)         (002: 0.225806)                                     (136, 87)   000
 sa_current                 [0014] = 5.277778 A (valid)         (000: 5.158730)                                    (136, 101)   000
 shunt_dump_current         [0003] = 0.685484 A (valid)         (004: 0.887097)                                    (134, 121)   004
 hps_1_thruster_select      [0007] = 000000000000               (009: 010110000110)                                      11   001
 hps_1_sector_initiate      [0007] = 475                        (009: 252)                                               12   001
 hps_1_sector_width         [0007] = 2                          (009: 0)                                                 12   001
 hps_1_num_pulses           [0008] = 4                          (009: 2)                                                 13   001
 hps_1_firing_ratio         [0008] = 15                         (009: 1)                                                 14   001
 hps_1_ratio_select         [0008] = enabled                    (013: disabled)                                          14   001
 hps_1_logic_pwr            [0008] = on                         (016: off)                                               14   001
 hps_1_init_term            [0008] = 0                          (009: 1)                                                 14   001
 hps_1_complete             [0008] = incomplete                                                                          14   001
 hps_1_28v_on               [0008] = off                        (017: on)                                                14   001
 hps_2_thruster_select      [0007] = 000000000000               (009: 011111100100)                                      16   001
 hps_2_sector_initiate      [0007] = 0                          (008: 712)                                               17   001
 hps_2_sector_width         [0007] = 0                          (008: 3)                                                 17   001
 hps_2_num_pulses           [0007] = 0                          (008: 1078)                                              18   001
 hps_2_firing_ratio         [0006] = 0                          (015: 9)                                                 19   001
 hps_2_ratio_select         [0006] = disabled                   (015: enabled)                                           19   001
 hps_2_logic_pwr            [0006] = on                         (008: off)                                               19   001
 hps_2_init_term            [0006] = 0                          (015: 1)                                                 19   001
 hps_2_complete             [0006] = complete                   (008: incomplete)                                        19   001
 hps_2_28v_on               [0006] = off                        (008: on)                                                19   001
 hps_1_prm_tk_htrs          [0004] = off                                                                                 55   003
 hps_1_sec_tk_htrs          [0004] = low                        (003: off)                                               55   003
 hps_2_prm_tk_htrs          [0004] = off                        (011: low)                                               55   003
 hps_2_sec_tk_htrs          [0004] = low                        (003: off)                                               55   003
 hps_1_2_prm_ln_htrs        [0004] = low                        (003: off)                                               55   003
 hps_1_2_sec_ln_htrs        [0004] = low                        (003: off)                                               55   003
 accel_pwr_monitor          [0003] = 119                                                                          (136, 38)   001
 hps_1_tc                   [0003] = -55.088889 C (valid)       (001: -51.600000)                                 (136, 41)   001
 hps_2_tc                   [0003] = -10.810811 C (valid)                                                         (136, 51)   001
 hps_1_temp_supercom        [0005] = 1                          (005: 145)                                        (134, 57)   005
 hps_2_temp_supercom        [0004] = 1                          (012: 253)                                        (134, 67)   004
 spin_rate                  [0003] = 19.1595852499                                                                   35   007
 spin_period                [0003] = 3.13159179688                                                                   35   007
 mag_rate                   [0003] = 18.7810935769              (006: 19.2120075047)                                 39   006
 mag_period                 [0003] = 3.19470214844              (006: 3.123046875)                                   39   006
 spin_angle                 [0003] = 207.686910423              (007: 0.0)                                               35   007
 fss_angle                  [0004] = 91.6409684294              (001: Data out of expected range)                        58   001
 hps_1_tk_press             [0003] = 0.000000 psi (valid)                                                        (136, 115)   000
 hps_2_tk_press             [0003] = 4.800000 psi (valid)                                                        (136, 121)   000
 hps_1_lv_a                 [0004] = 0                                                                            (134, 61)   004
 hps_2_lv_b                 [0004] = 0                                                                            (134, 61)   004
 hps_1_lv_c                 [0004] = 0                                                                            (134, 61)   004
 hps_2_lv_d                 [0004] = 0                                                                            (134, 61)   004
 accelerometer              [0234] = 119                        (010: 221)                                        (137, 40)   000



Receiving
```

Live Telemetry from Bochum

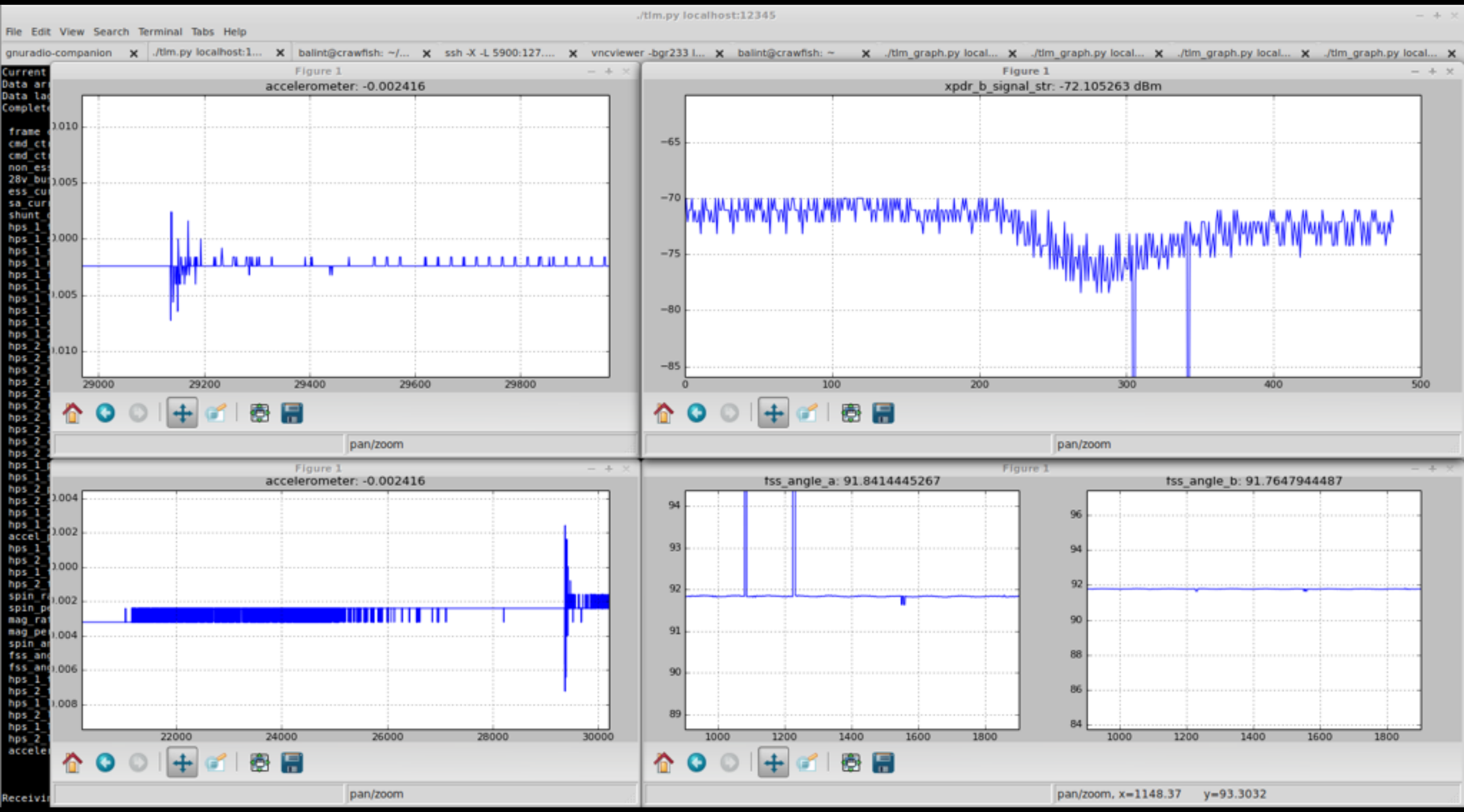
- Many thanks to our friends at AMSAT-DL


PHILIPS

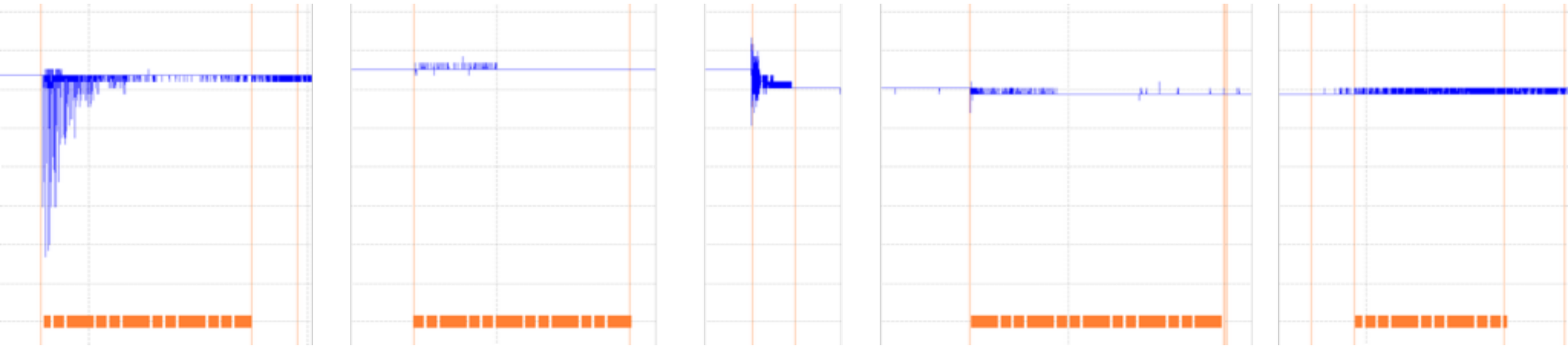

HPS SCHEMATIC


Telemetry 7/9
METAL SUPPLY
MFG CO.
ORIGINAL
DUBLIN, IRLAND

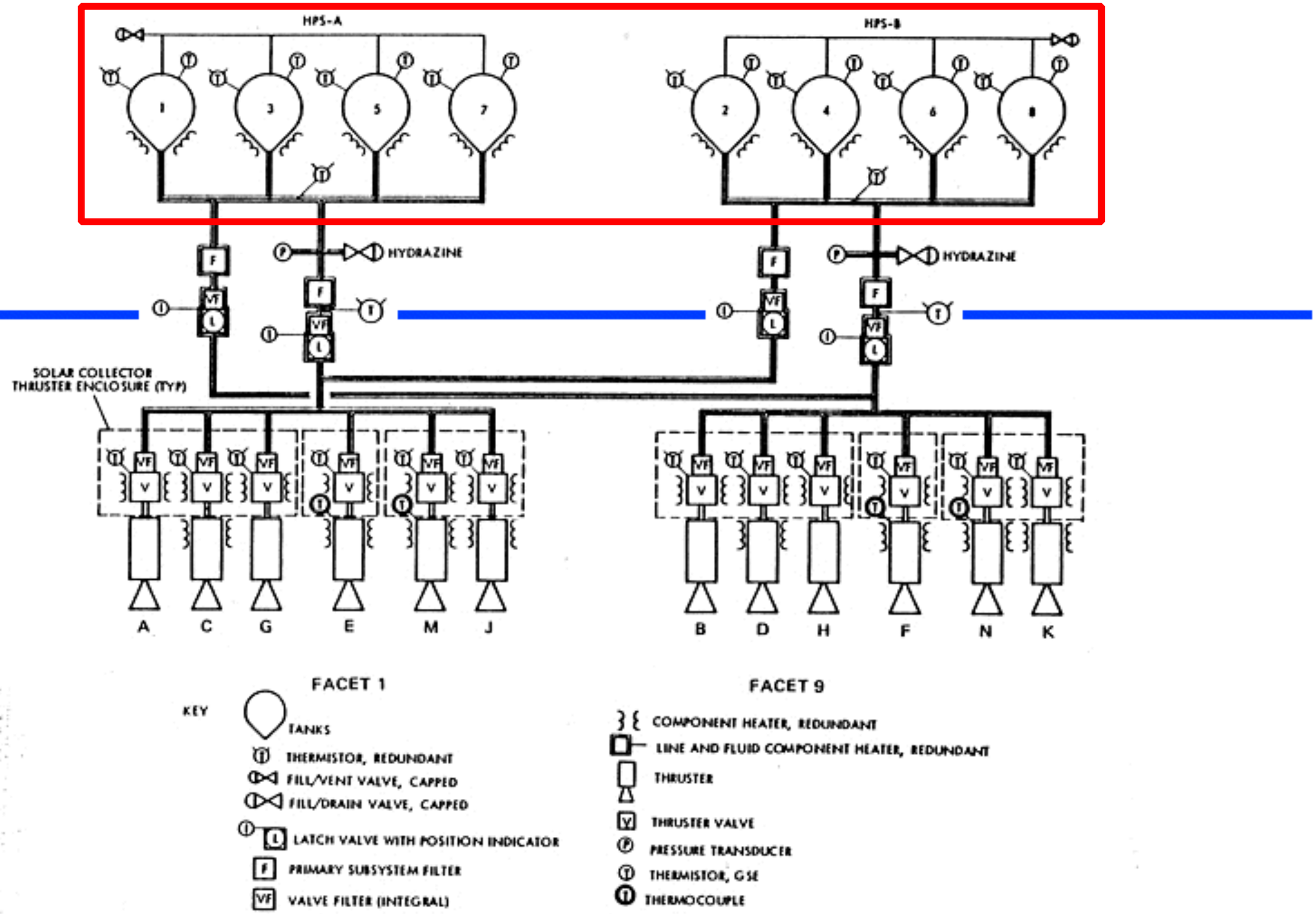
Telemetry During Thruster Firing



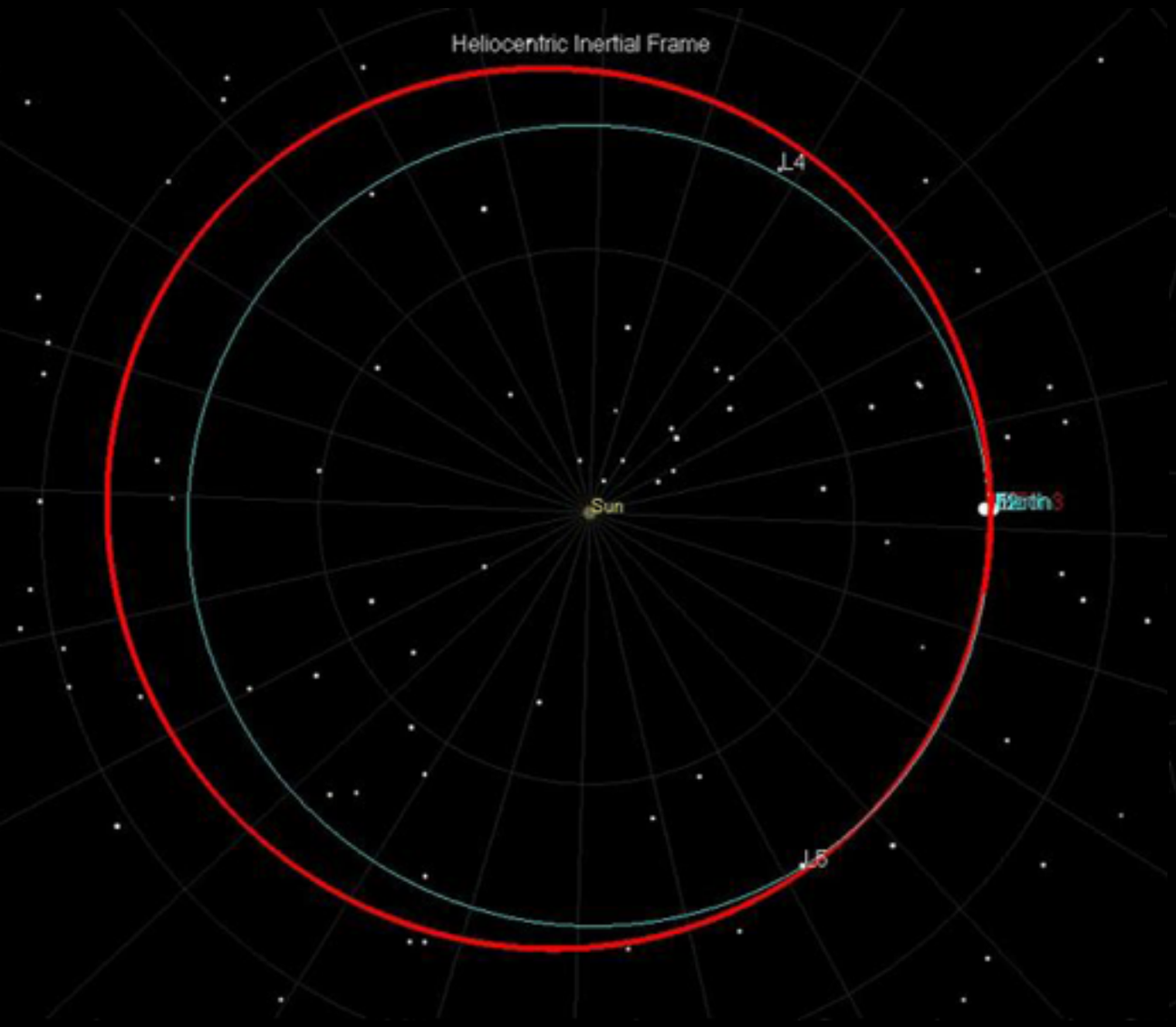
No Thrust

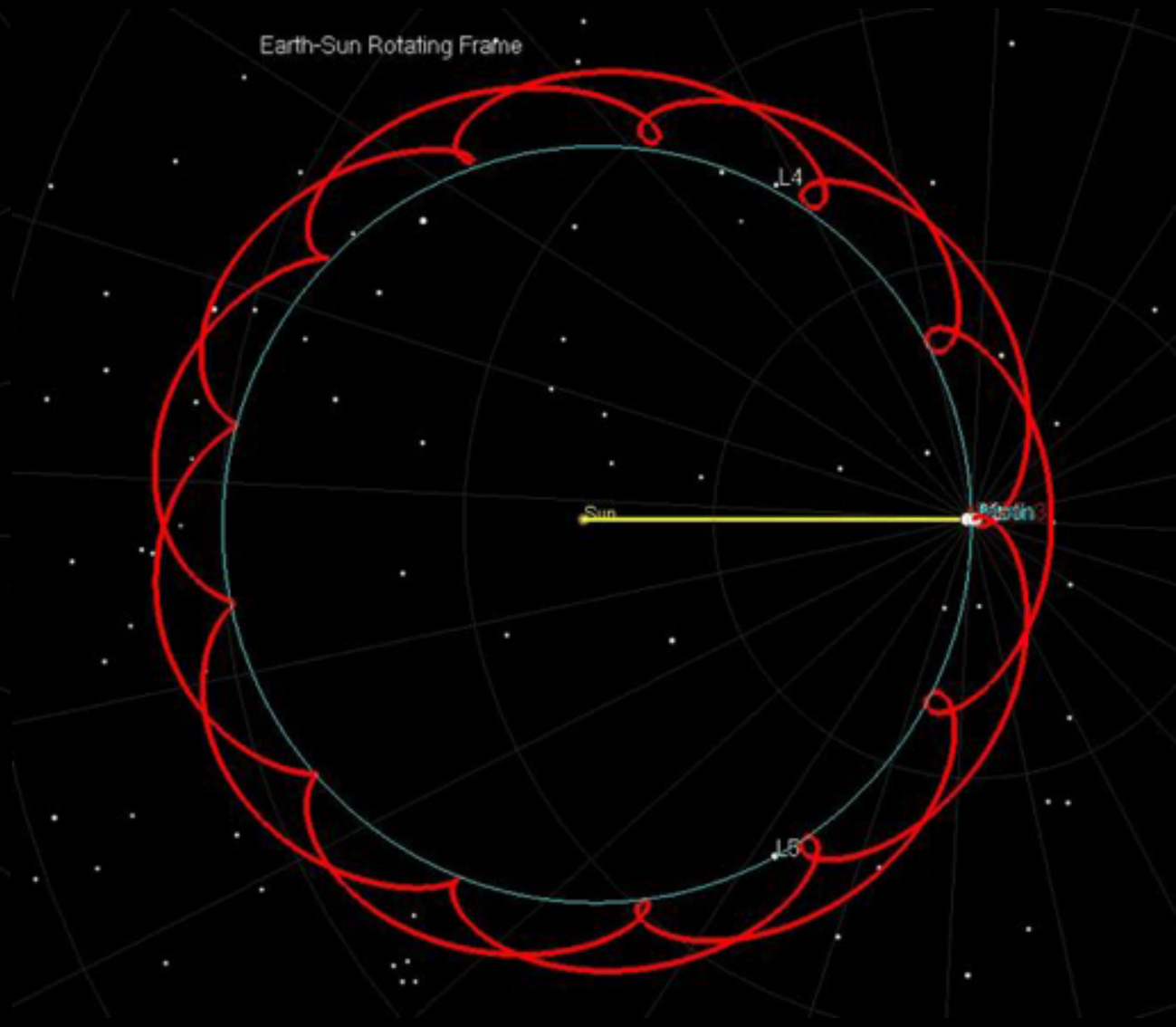


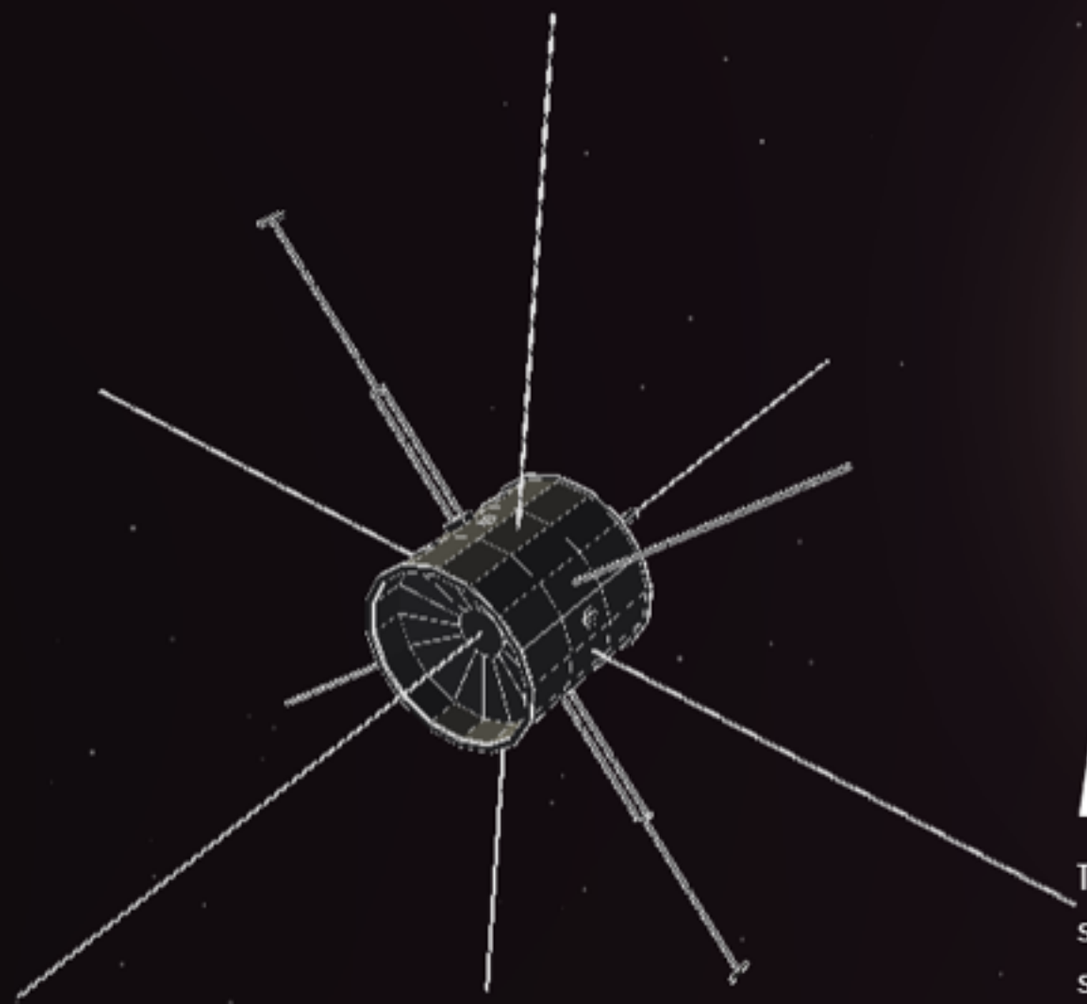
Hydrazine Propulsion System

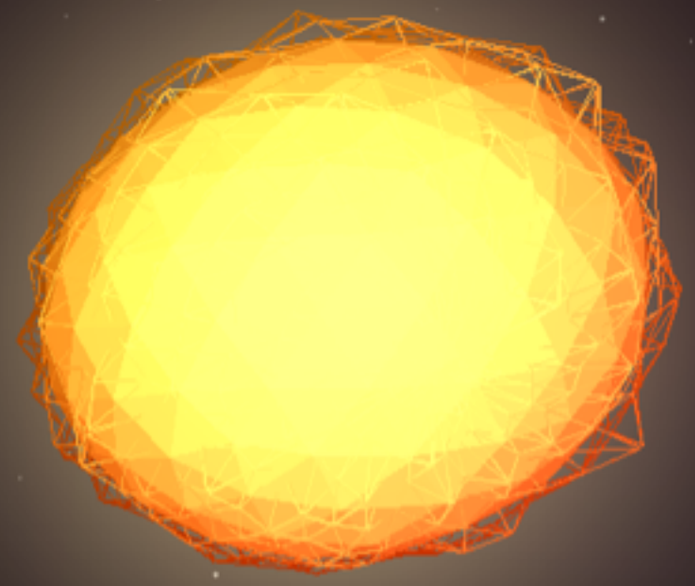


New Orbit


Heliocentric Inertial Frame
L4
Sun
Earth
L5


Earth-Sun Rotating Frame
L4
Sun
Earth
L5





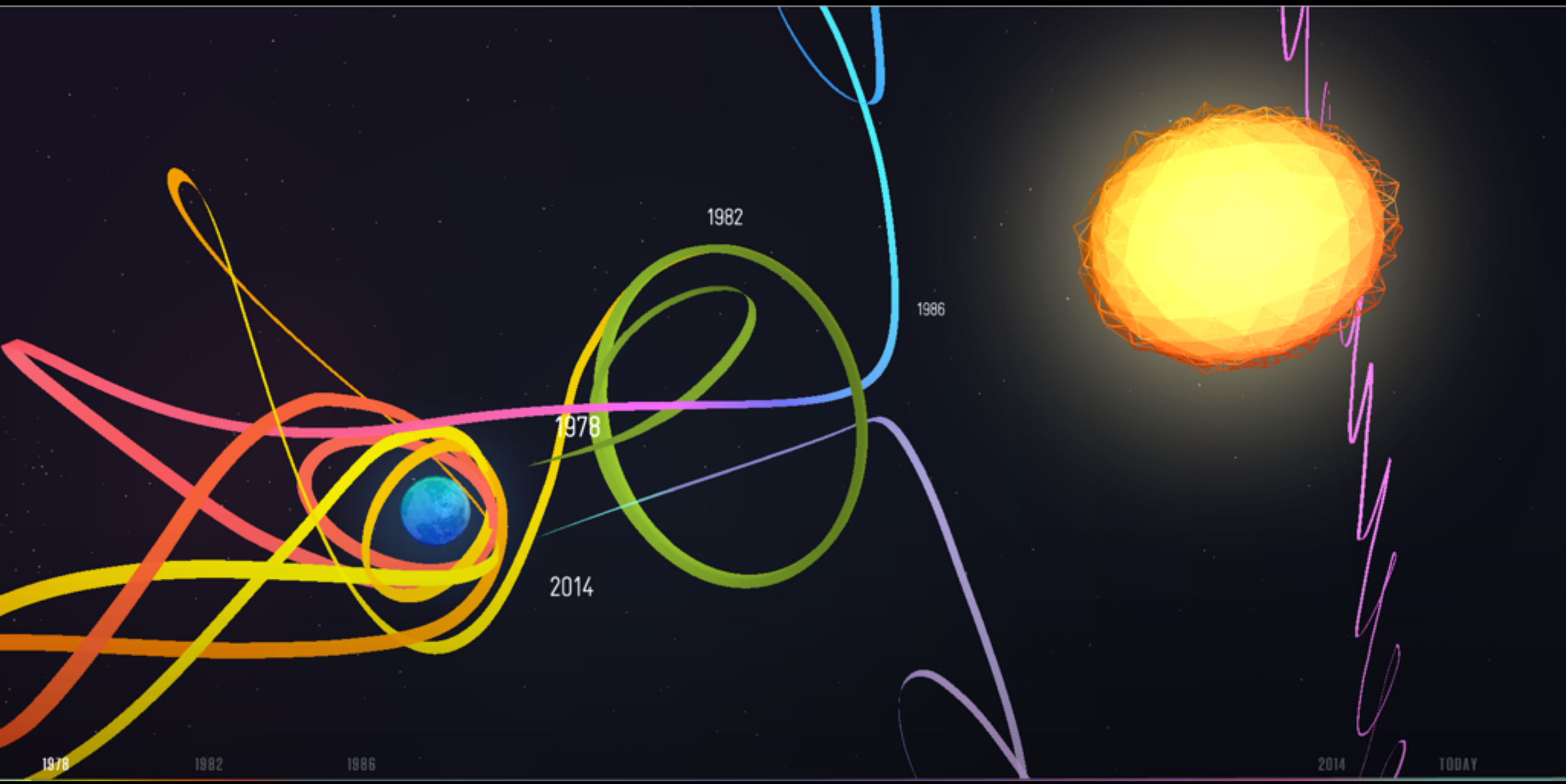
A SPACECRAFT FOR ALL

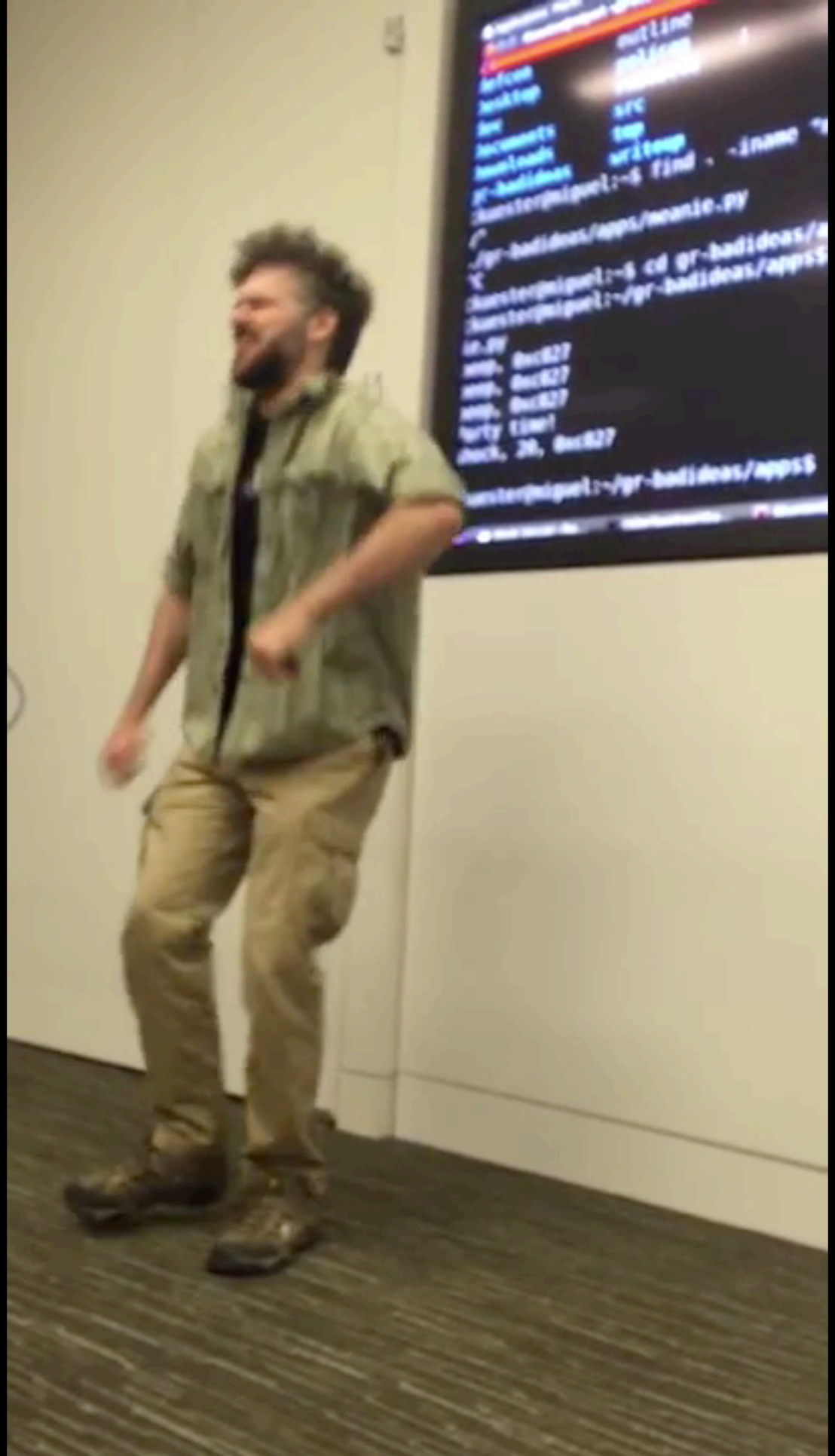
The ISEE-3 was launched to study the Sun in 1978, but ended up redefining space flight. Now it's on a new mission to become citizen science's first spacecraft, with data accessible by everyone.

SEE THE JOURNEY

SEE LIVE VIEW

www.spacecraftforall.com




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.net

GitHub: balint256

GitHub: BastilleResearch

Bastille