Hacking the Wireless World with Software Defined Radio – 2.0

Balint Seeber (Applications Specialist & SDR Evangelist)

balint@ettus.com
balint@spench.net
@spenchdotnet

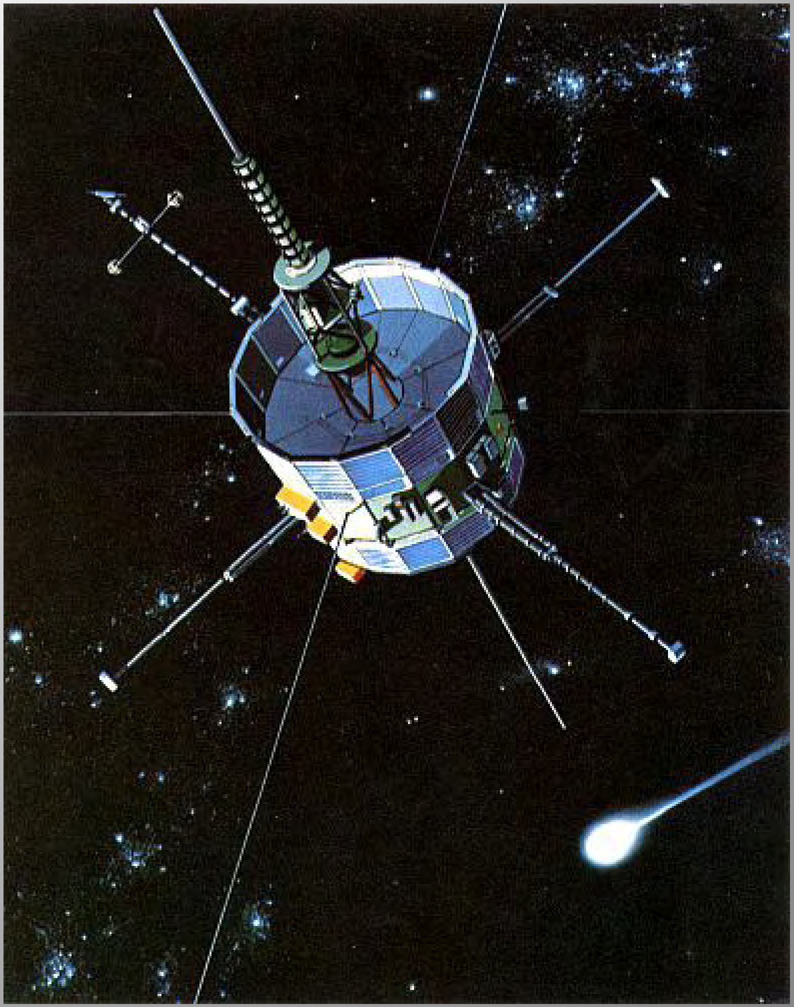
Ettus Research

Getting ready for some serious sampling by the Adriatic Sea

First day of visit to Italy...

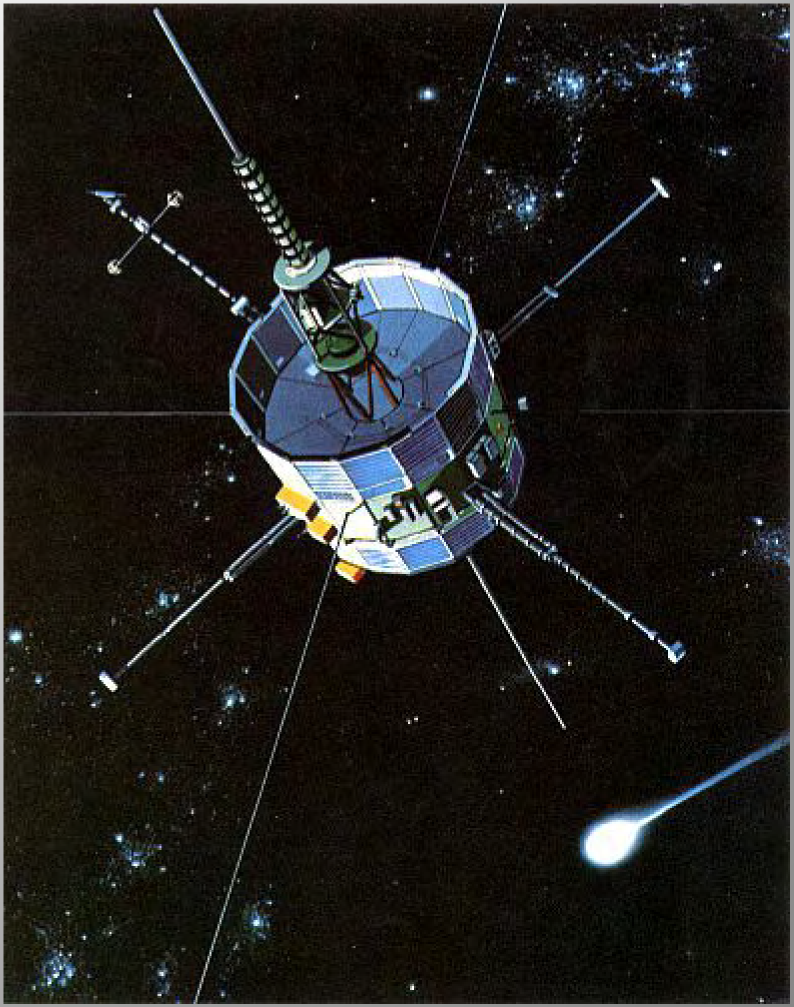
ISEE-3

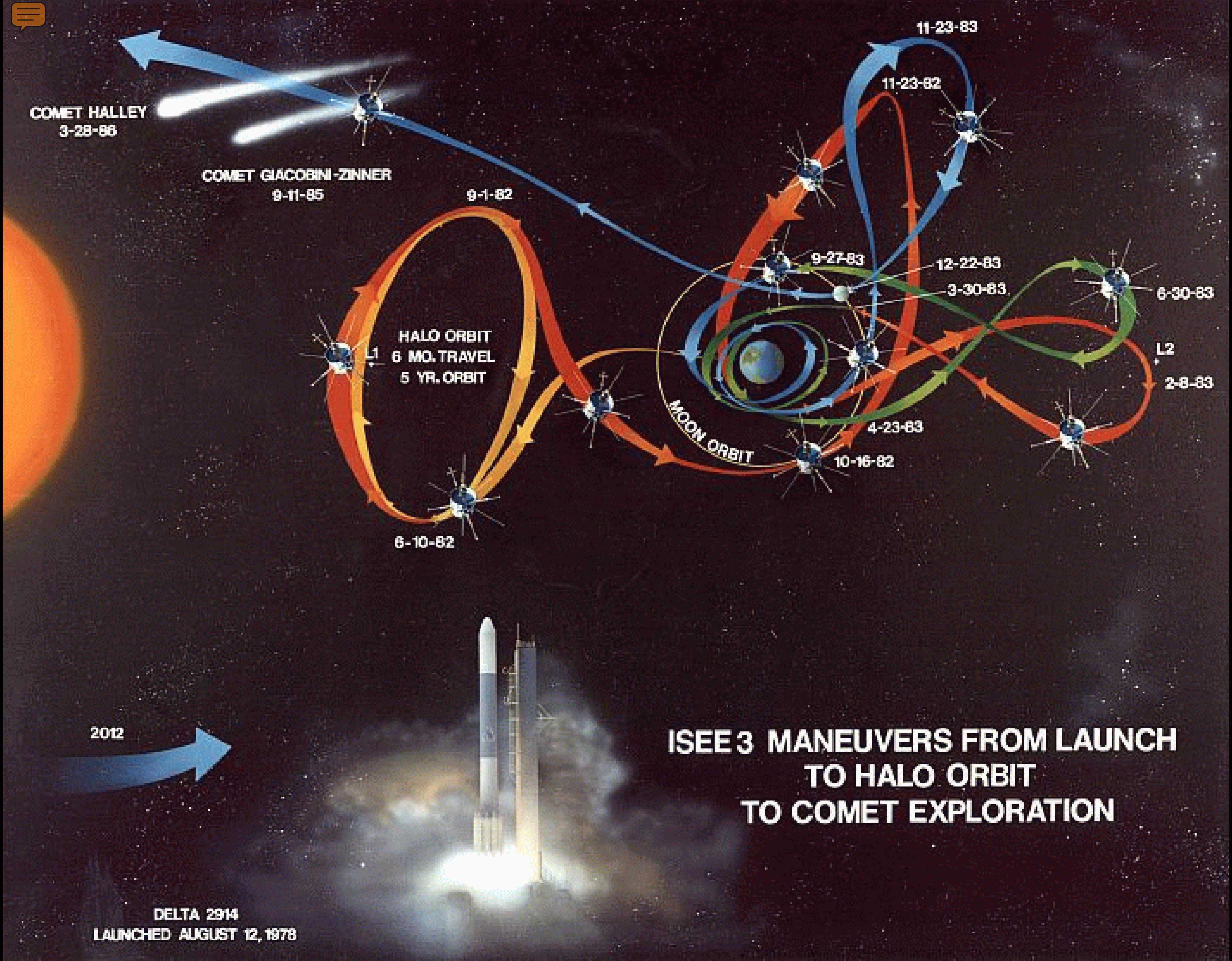
- **I**nternational **S**un/**E**arth **E**xplorer 3
- Launched: August 12, 1978
- Heliocentric Orbit
- Study interaction between solar wind and
  Earth’s magnetic field



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)

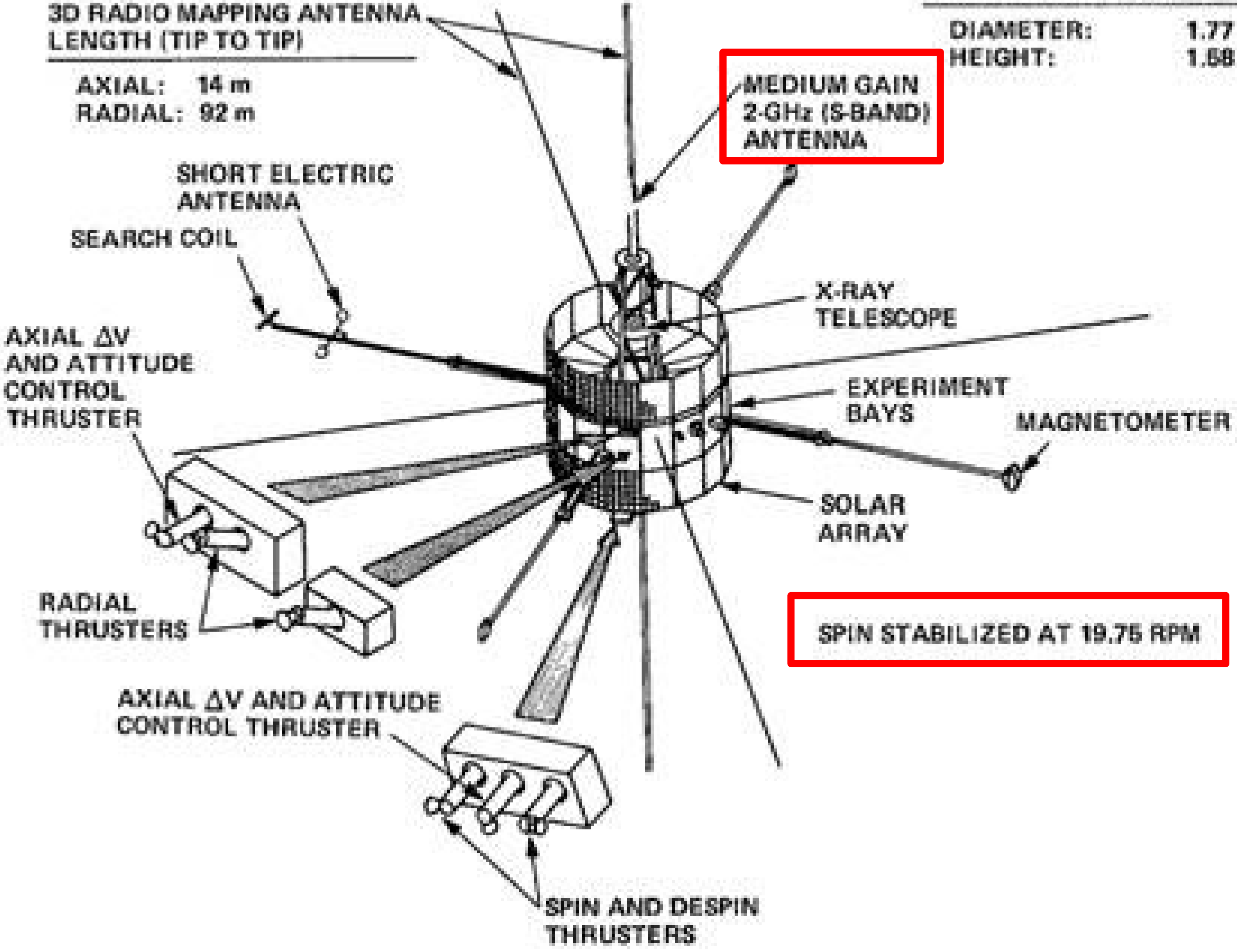




ISEE 3 MANEUVERS FROM LAUNCH
TO HALO ORBIT
TO COMET EXPLORATION

ISEE-3 ORIGINAL TRAJECTORY

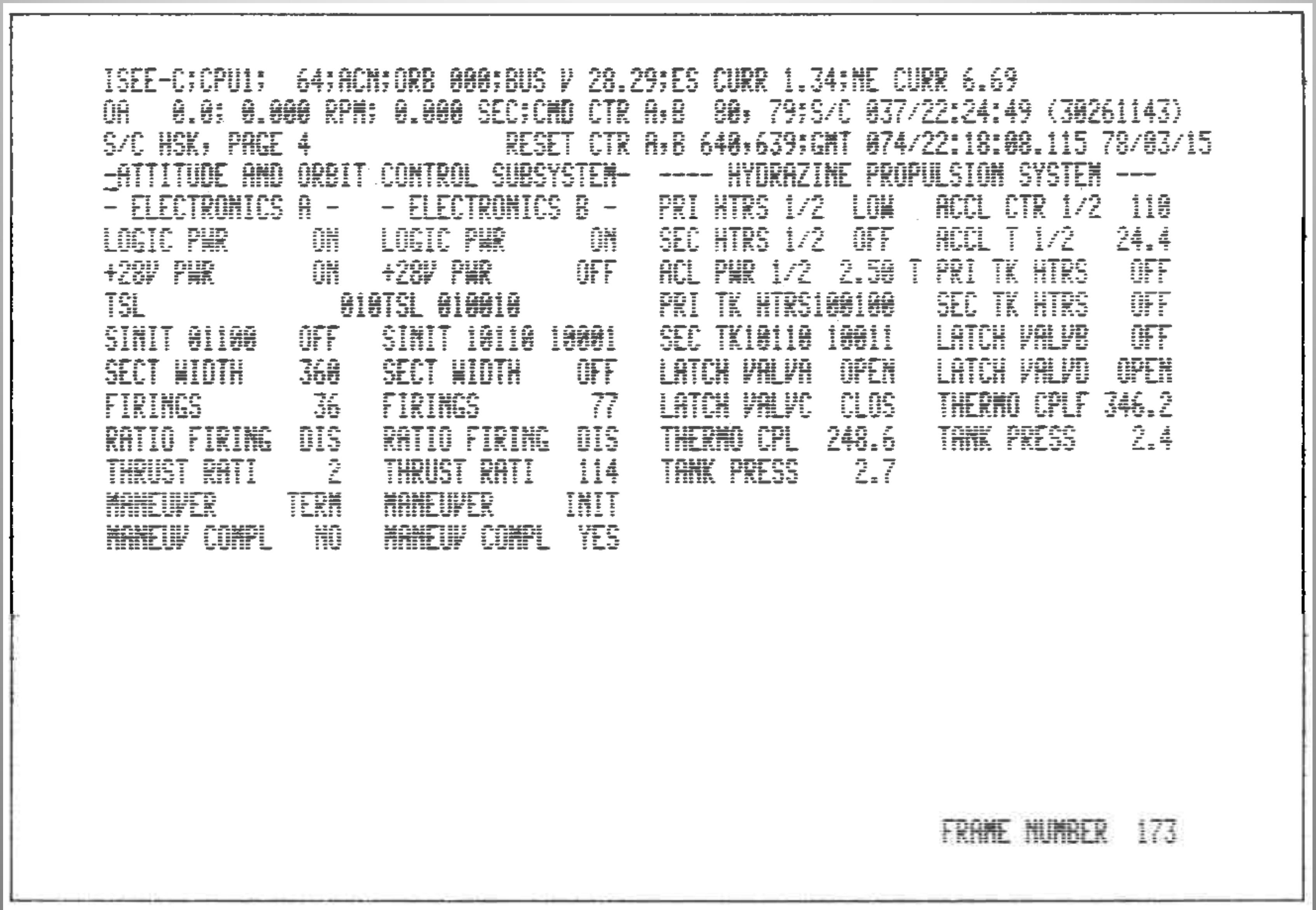
1978-1985



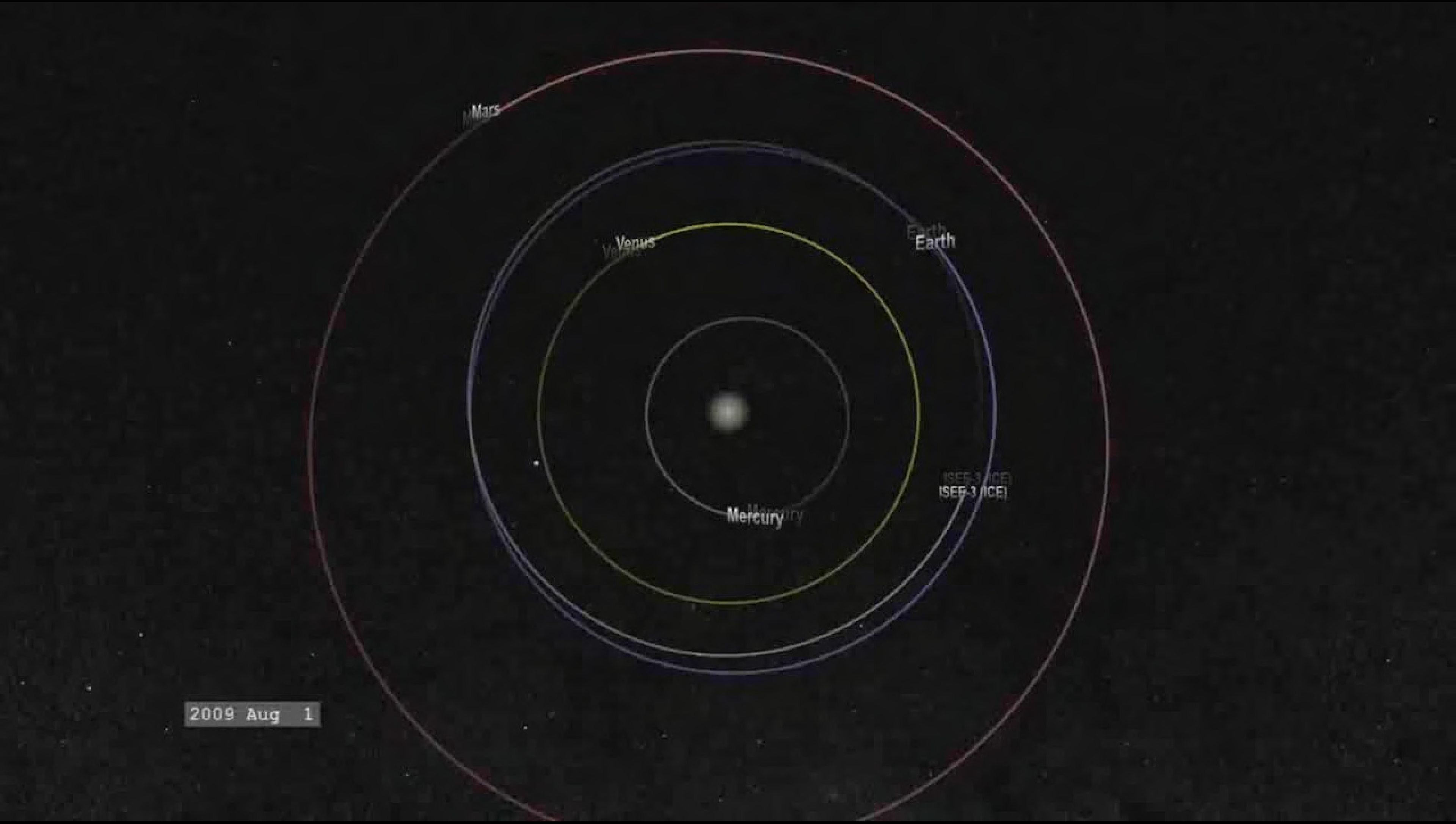
3D RADIO MAPPING ANTENNA LENGTH (TIP TO TIP)
AXIAL: 14 m
RADIAL: 92 m
MEDIUM GAIN 2-GHz (S-BAND) ANTENNA
SHORT ELECTRIC ANTENNA
SEARCH COIL
X-RAY TELESCOPE
AXIAL ΔV AND ATTITUDE CONTROL THRUSTER
EXPERIMENT BAYS
MAGNETOMETER
SOLAR ARRAY
RADIAL THRUSTERS
SPIN STABILIZED AT 19.75 RPM
AXIAL ΔV AND ATTITUDE CONTROL THRUSTER
SPIN AND DESPIN THRUSTERS

TOTAL S/C WEIGHT:	479 kg
EXPERIMENTS:	104 kg
HYDRAZINE:	89 kg
DIMENSIONS (MAIN BODY)	
DIAMETER:	1.77 m
HEIGHT:	1.58 m

Old Telemetry Screen



```
ISEE-C;CPU1;  64;ACN;ORB 000;BUS V 28.29;ES CURR 1.34;NE CURR 6.69
OA   0.0: 0.000 RPM: 0.000 SEC;CMD CTR A;B  80, 79;S/C 037/22:24:49 (30261143)
S/C HSK, PAGE 4              RESET CTR A;B 640,639;GMT 074/22:18:08.115 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 01100    OFF  SINIT 10110 10001   SEC TK10110 10011   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
```


Mars
Venus
Earth
ISEE-3 (ICE)
Mercury
2009 Aug 1

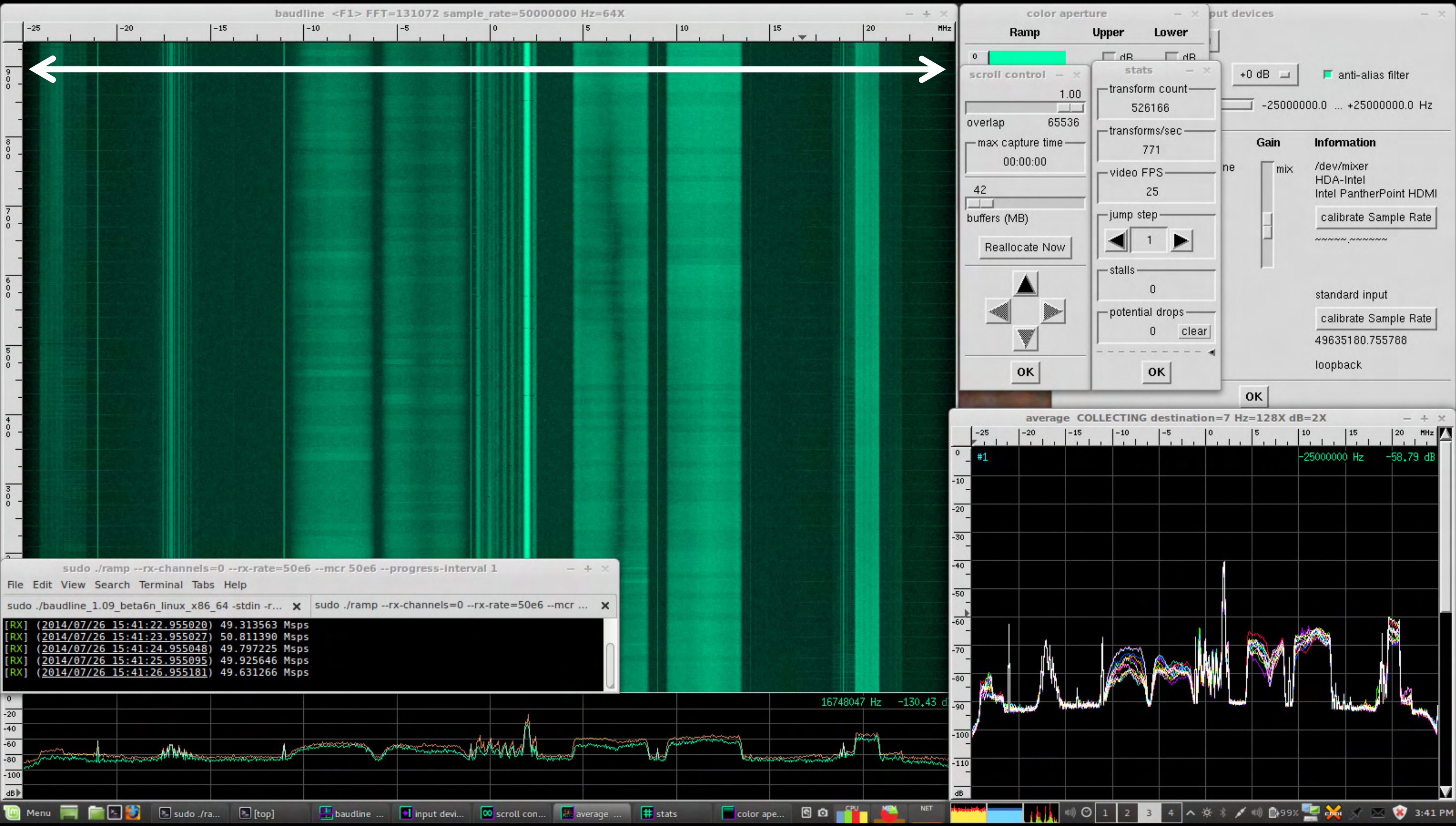
Overview

- Restaurant Pagers
- RDS TMC
- Primary Surveillance RADAR
- RFID
- ISEE-3

GNURadio

THE FREE & OPEN SOFTWARE RADIO ECOSYSTEM

50 MHz BW



sudo ./ramp --rx-channels=0 --rx-rate=50e6 --mcr 50e6 --progress-interval 1

sudo ./baudline_1.09_beta6n_linux_x86_64 -stdin -r... | sudo ./ramp --rx-channels=0 --rx-rate=50e6 --mcr ...

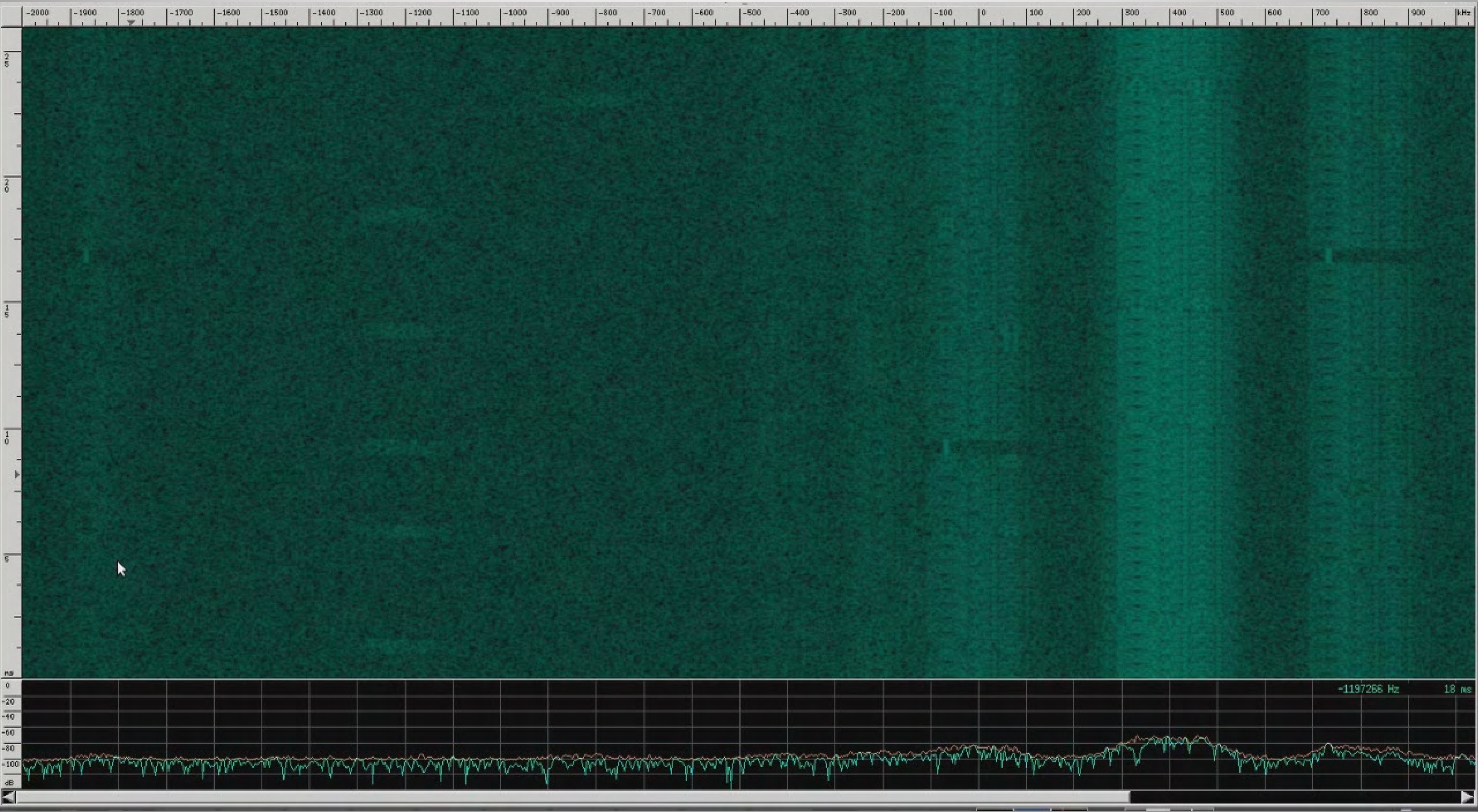
```
[RX] (2014/07/26 15:41:22.955020) 49.313563 Msps
[RX] (2014/07/26 15:41:23.955027) 50.811390 Msps
[RX] (2014/07/26 15:41:24.955048) 49.797225 Msps
[RX] (2014/07/26 15:41:25.955095) 49.925646 Msps
[RX] (2014/07/26 15:41:26.955181) 49.631266 Msps
```

scroll control: 1.00; overlap 65536; max capture time 00:00:00; buffers (MB) 42

stats: transform count 526166; transforms/sec 771; video FPS 25; jump step 1; stalls 0; potential drops 0

input devices: +0 dB; -25000000.0 ... +25000000.0 Hz; /dev/mixer HDA-Intel Intel PantherPoint HDMI; 49635180.755788

GSM BCCH & Traffic

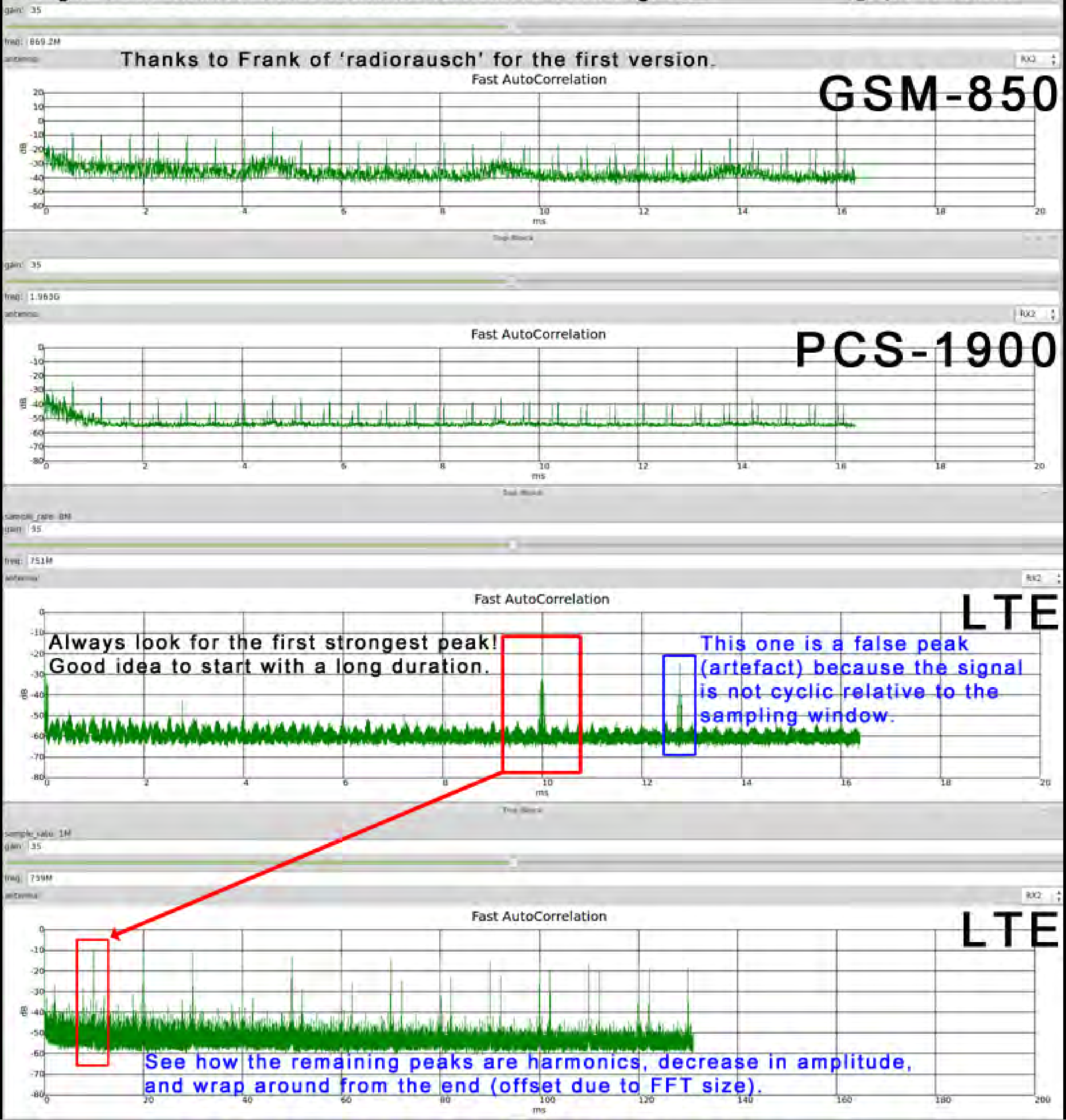


Dialplan

- 101 – Registration
  - Text back 4-to-10 digit number to register
- 411 – Info
- 600 – Echo Test
- 777 – Time
- 778 – ANI
- 2103 – Me

Using a USRP B210 & the Fast Auto-correlation Sink in gr-baz

@spenchdotnet



Thanks to Frank of ‘radiorausch’ for the first version.

GSM-850

PCS-1900

LTE

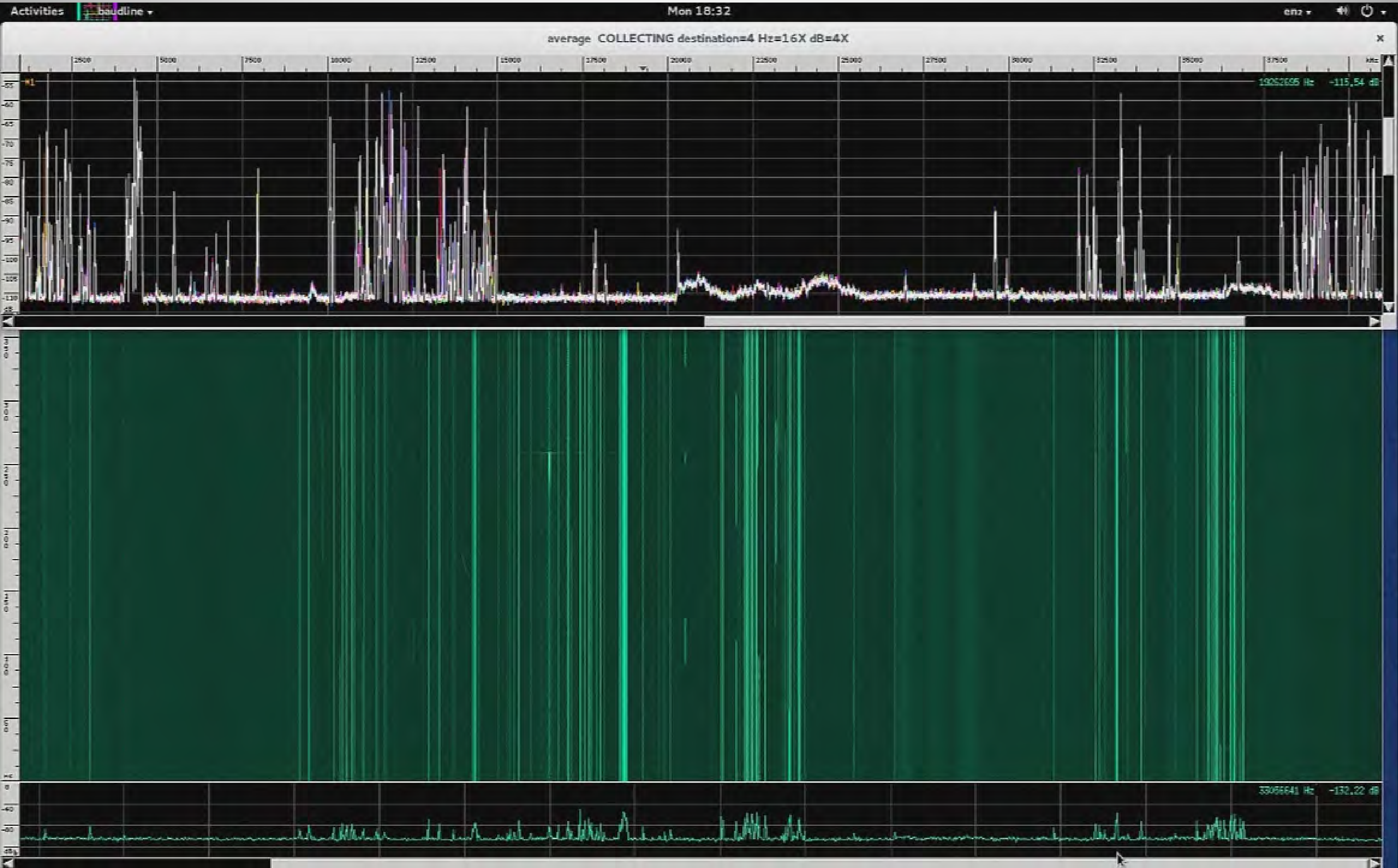
Always look for the first strongest peak!
Good idea to start with a long duration.

This one is a false peak (artefact) because the signal is not cyclic relative to the sampling window.

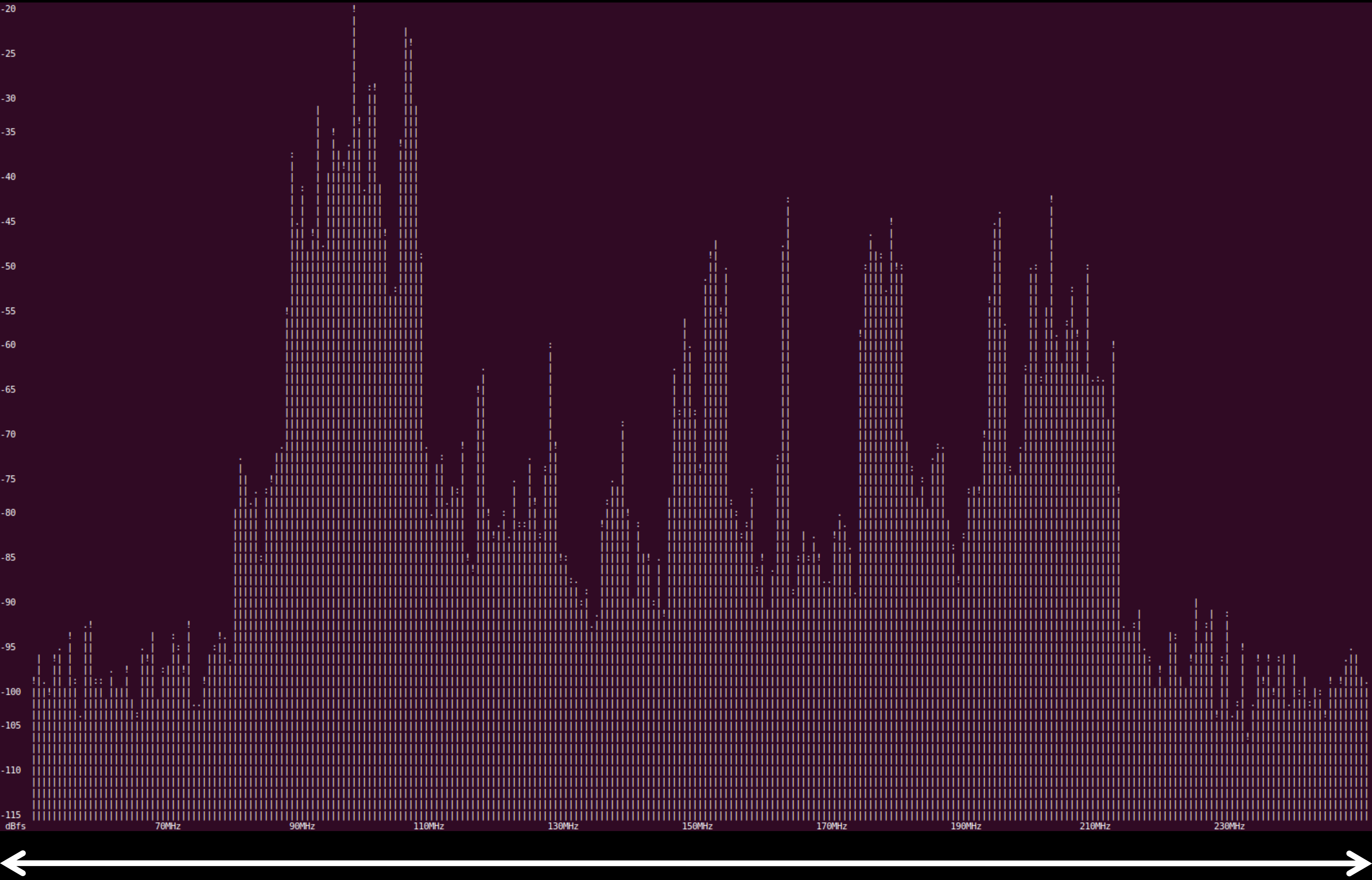
LTE

See how the remaining peaks are harmonics, decrease in amplitude, and wrap around from the end (offset due to FFT size).

400 MHz Band

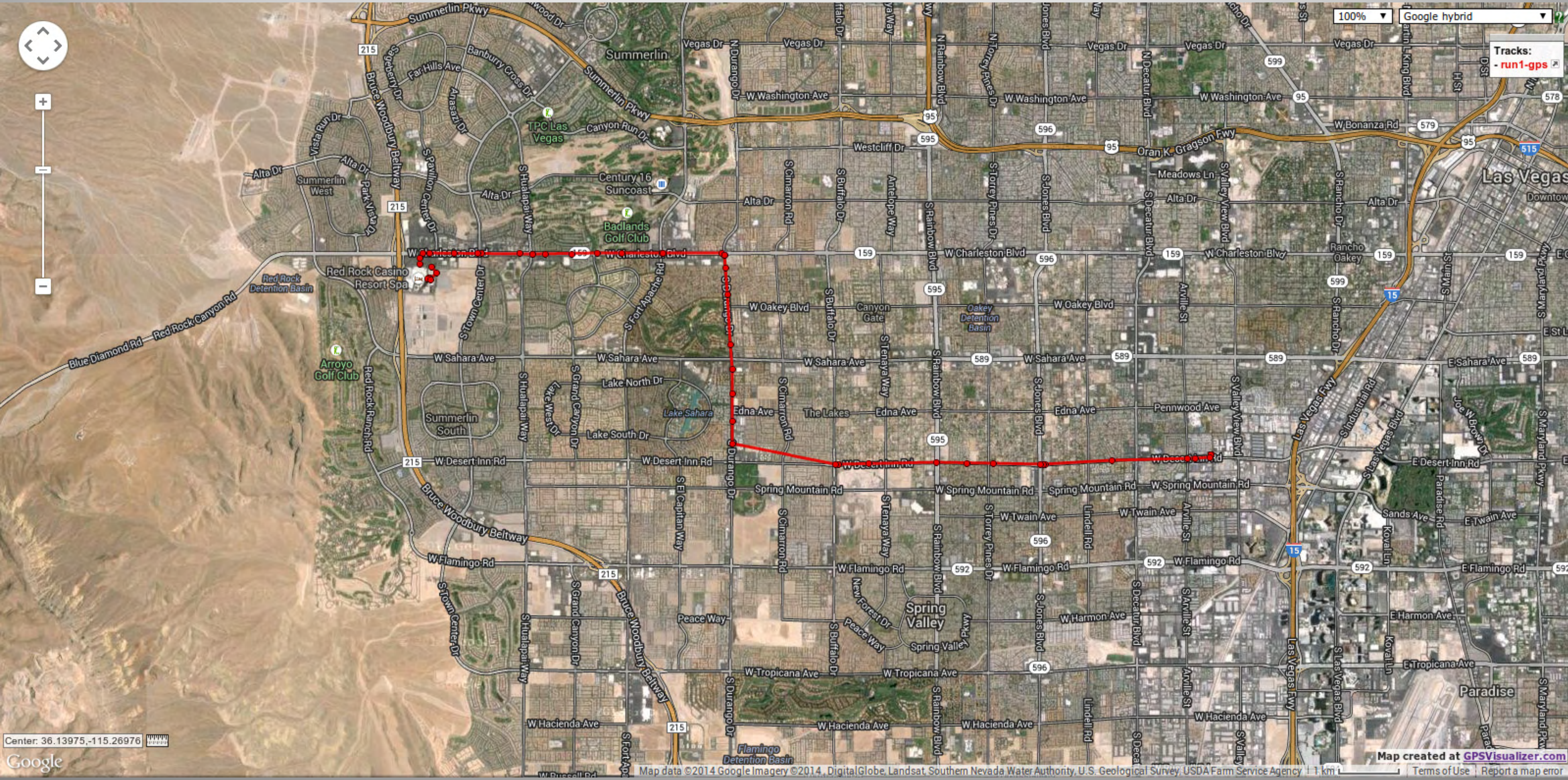


average COLLECTING destination=4 Hz=16X dB=4X

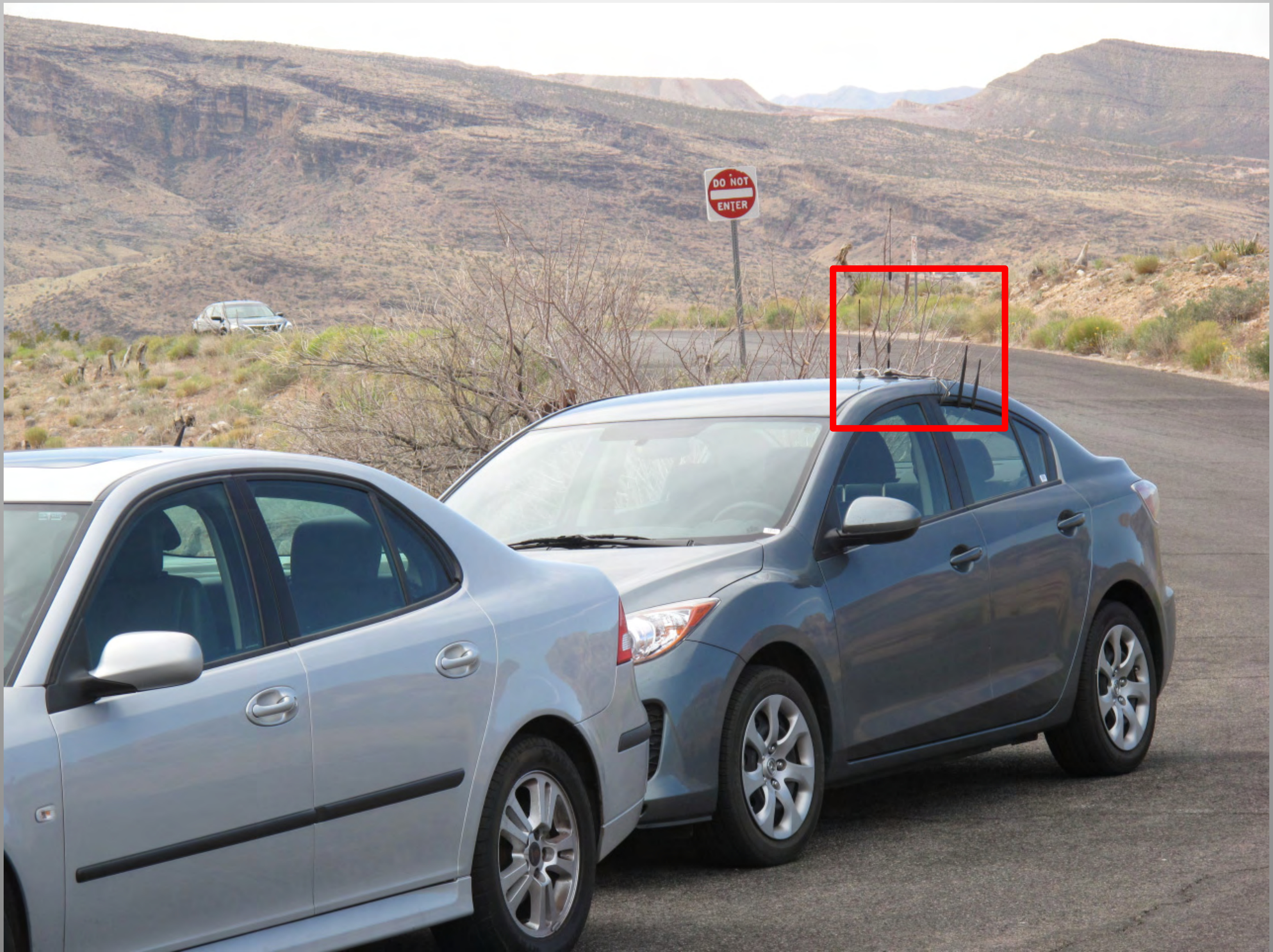


50 MHz – 250 MHz (200 Msps, 120 MHz RF BW)

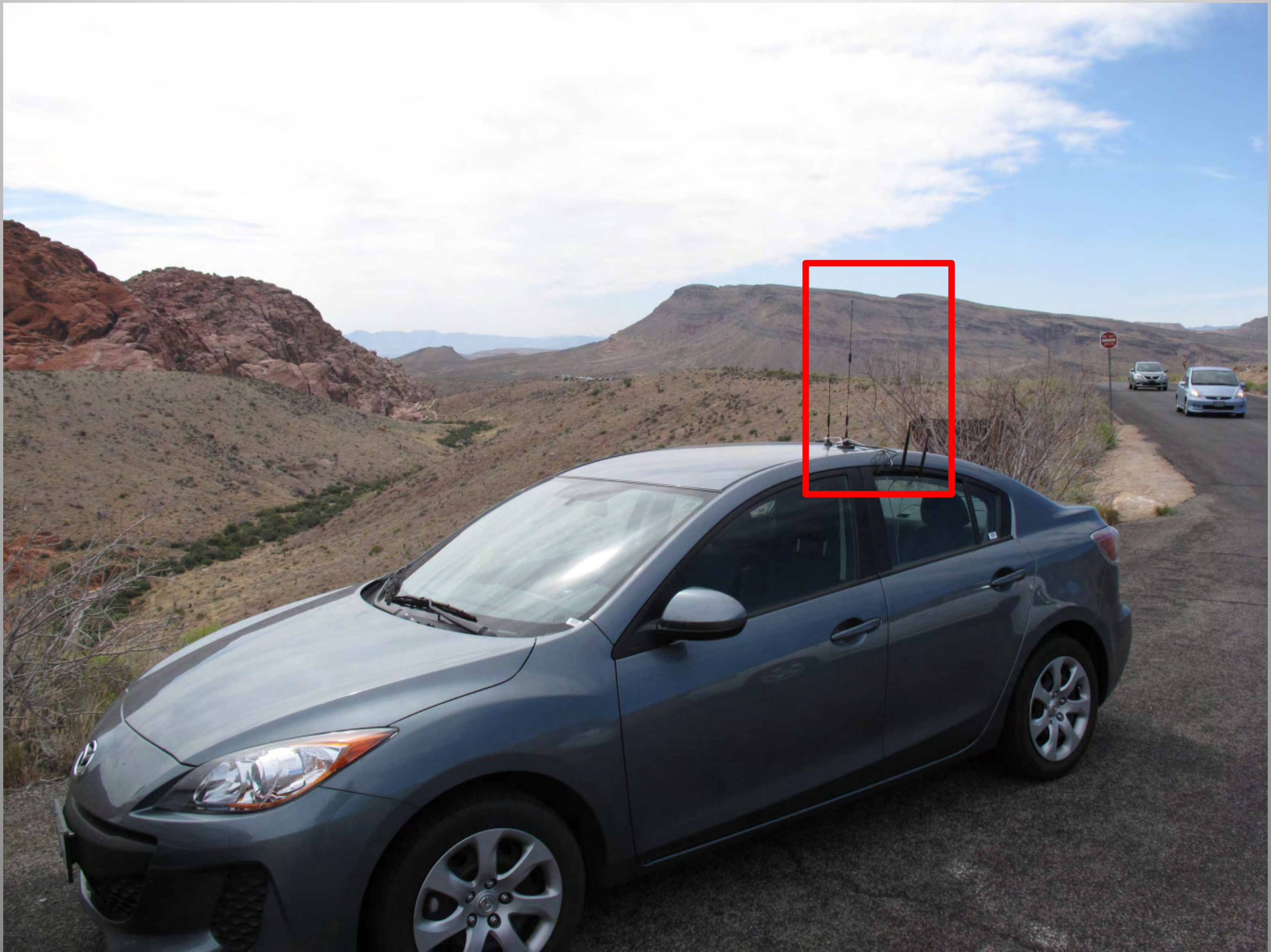
Spectrum Monitoring



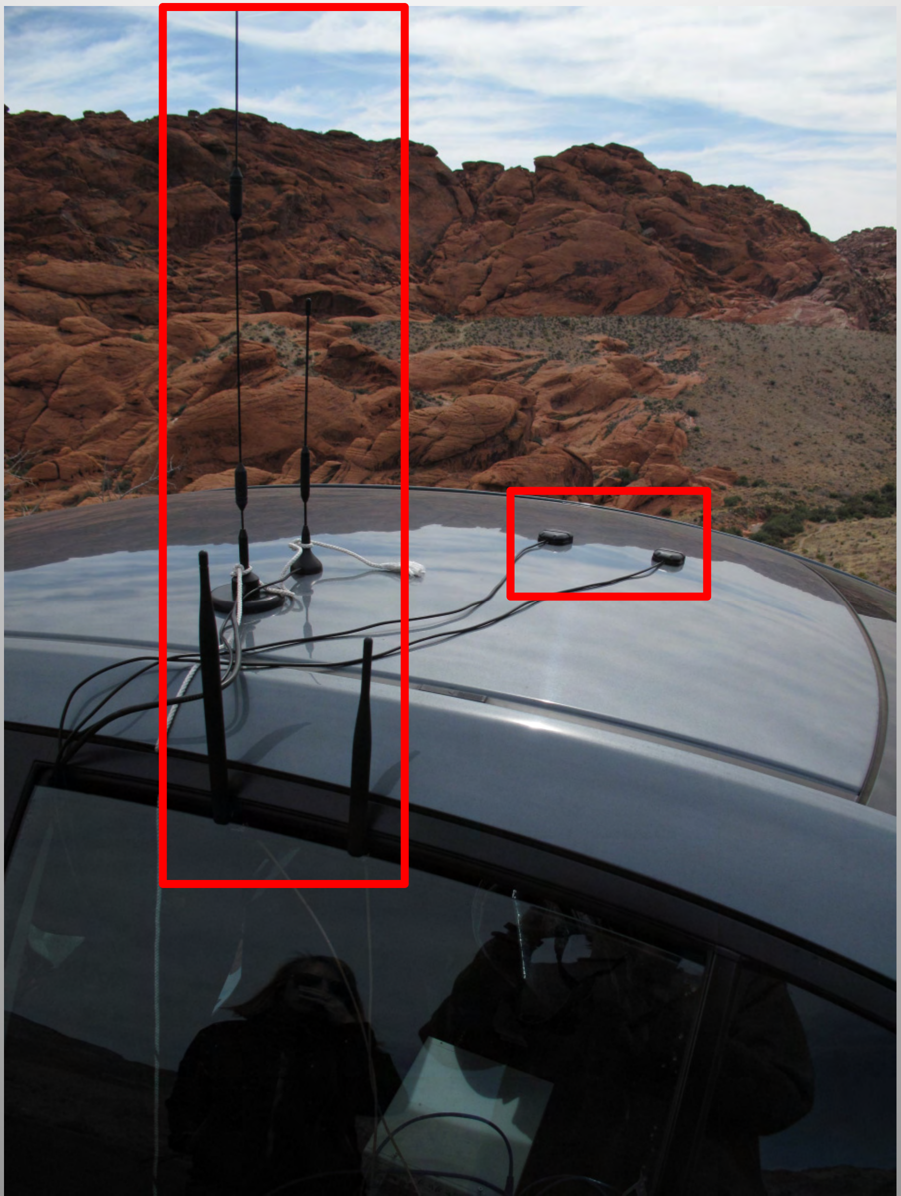
Spot the Antennas



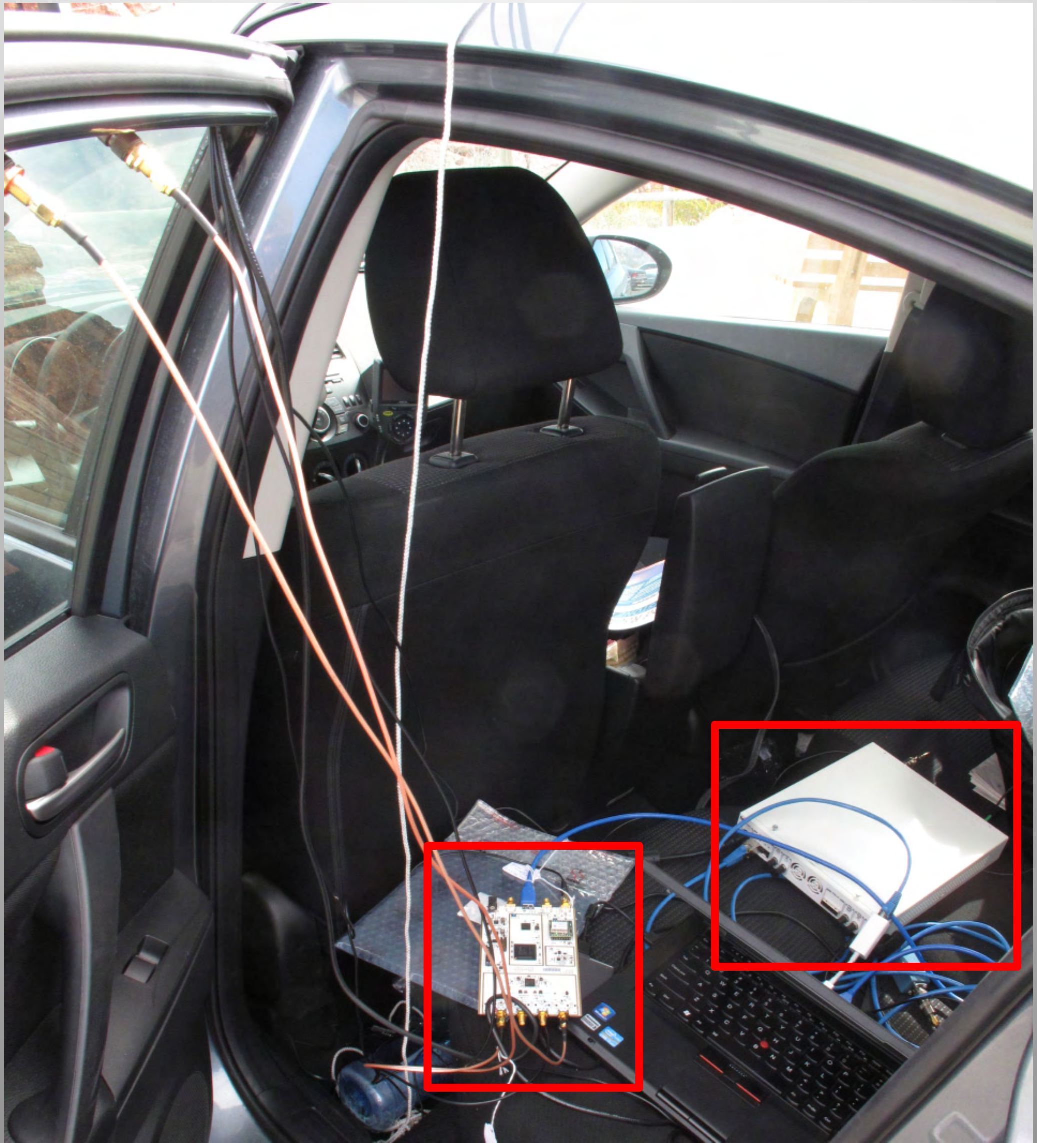
Spot the Antennas



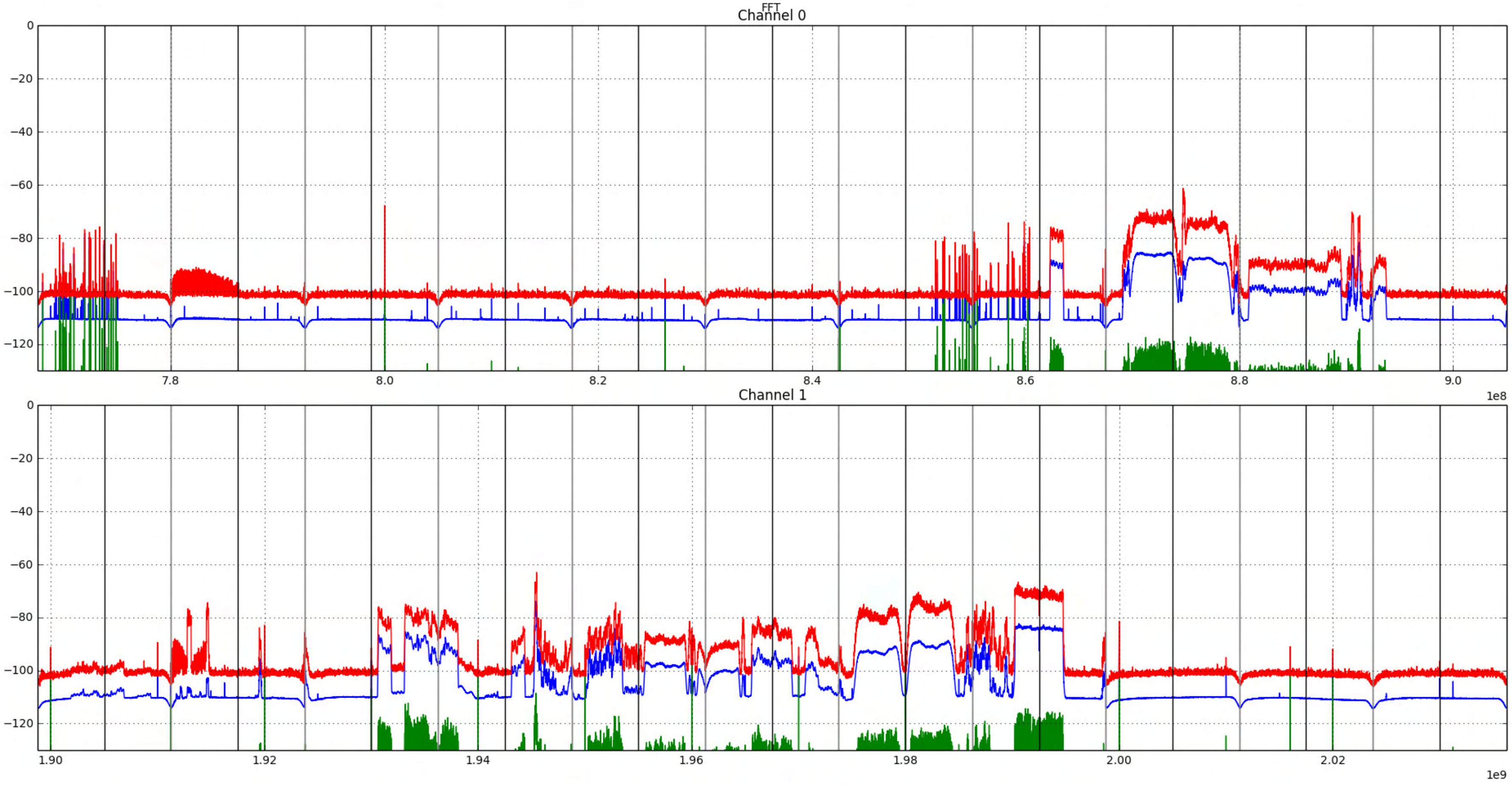
Spot the Antennas



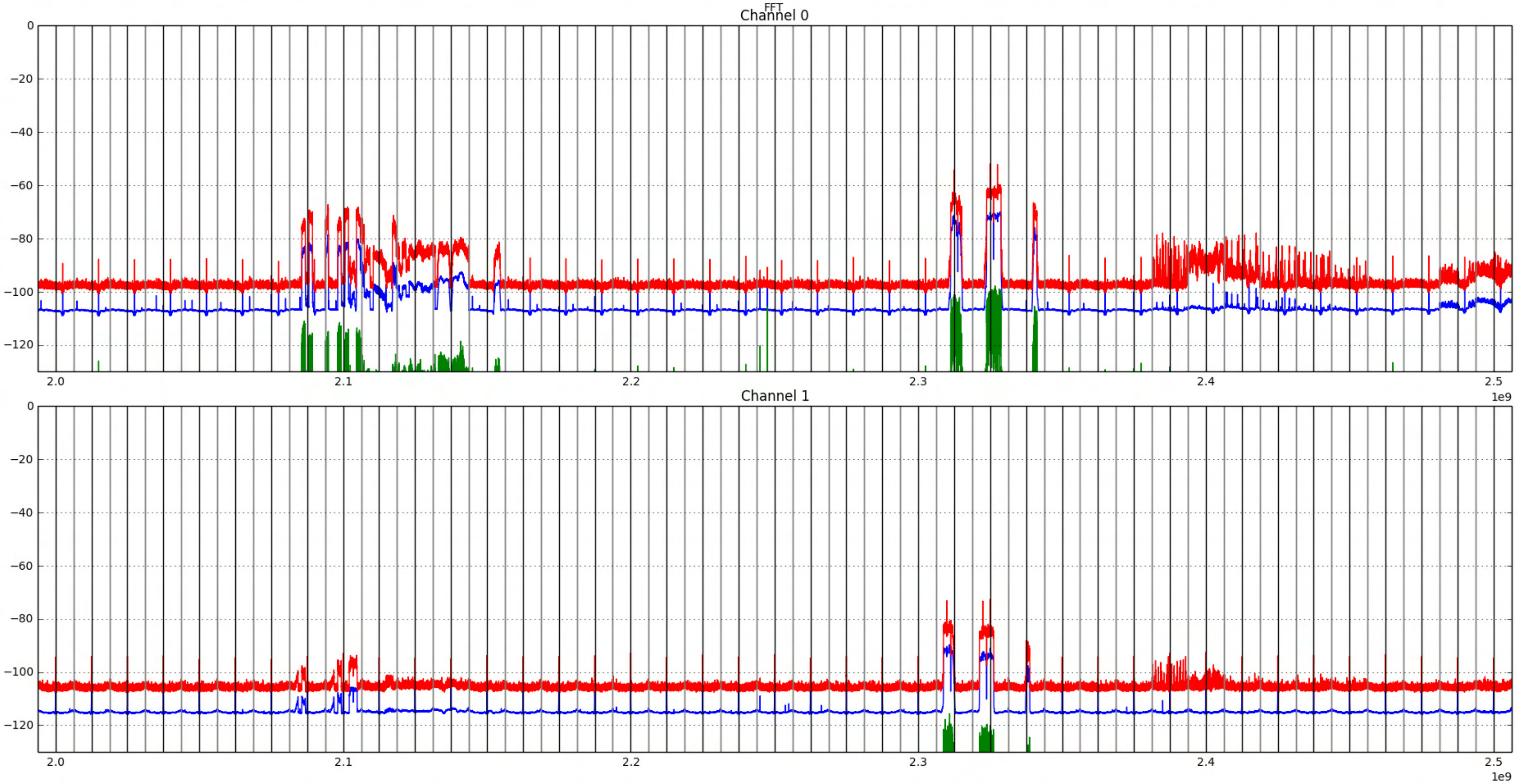
Spot the USRPs



Stitched FFTs

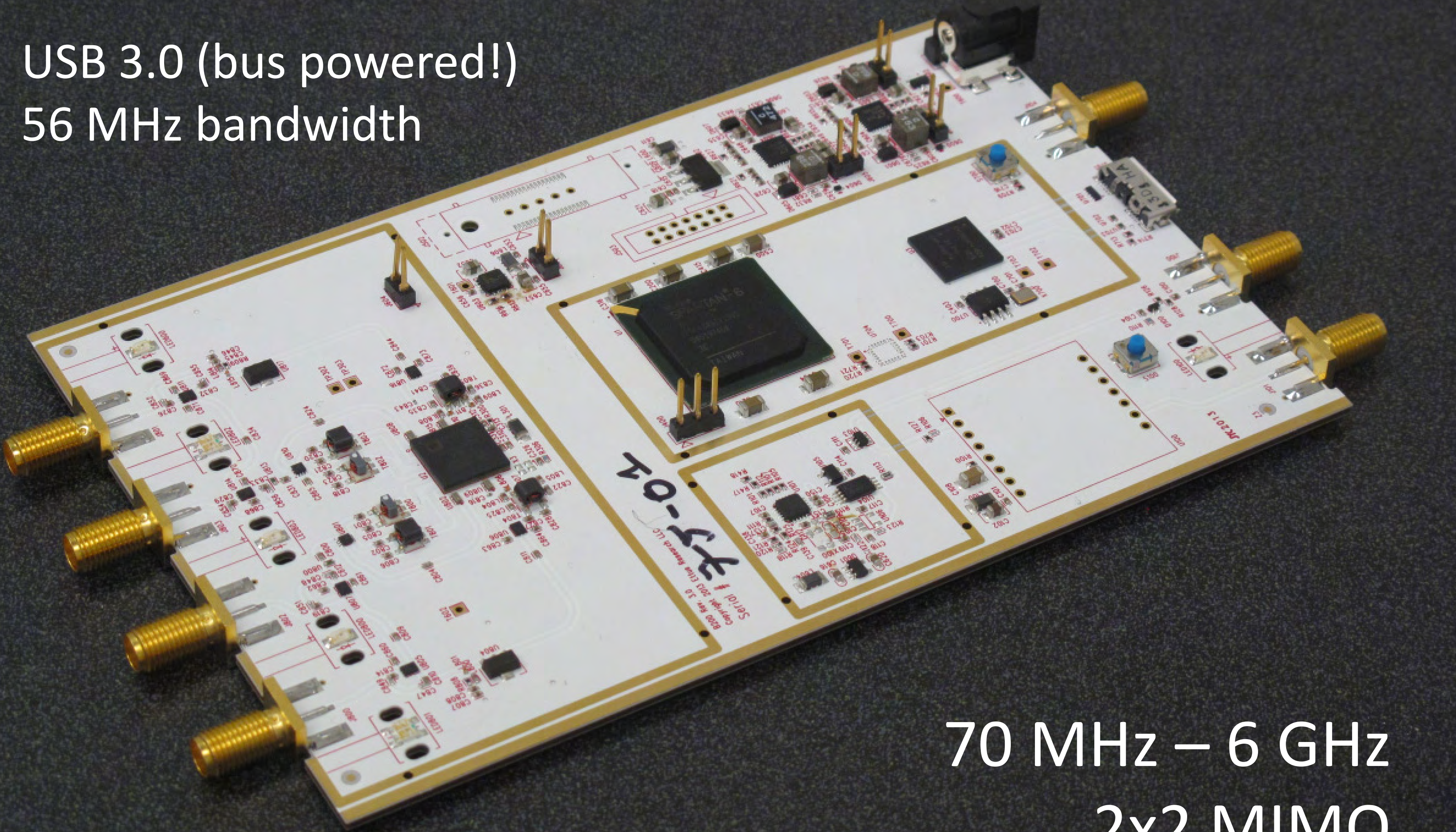


Stitched FFTs



USRP B200 & B210

USB 3.0 (bus powered!)
56 MHz bandwidth



70 MHz – 6 GHz
2x2 MIMO

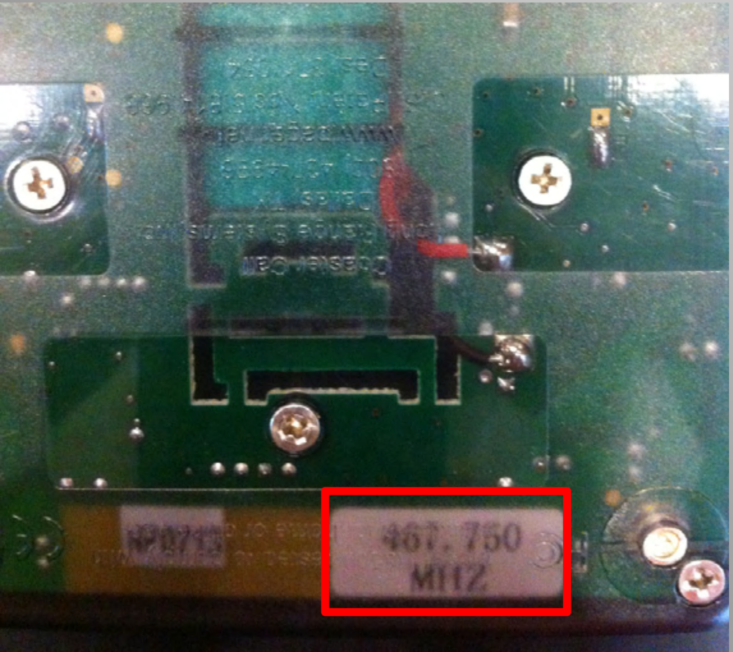
Restaurant Pagers

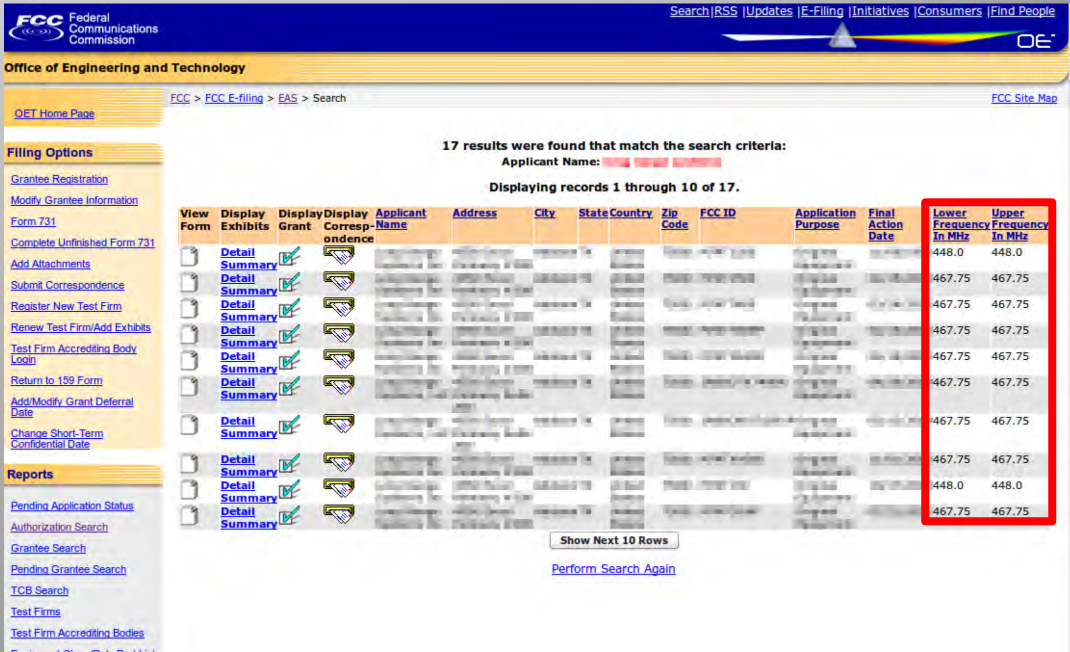
Your food is ready?

- Pagers inform waiting customer they can collect their order
  - Assuming their order is ready
- Order & collection rate should be ~same
  - Unless everyone is paged at once

Step 1: Frequency

- Either:
  - Find frequency label on the device
  - Find FCC ID on device and check online
  - Scan spectrum in likely ranges (e.g. 450-470 MHz)




FCC Federal Communications Commission
Search | RSS | Updates | E-Filing | Initiatives | Consumers | Find People
OET
Office of Engineering and Technology
FCC > FCC E-filing > EAS > Search
FCC Site Map
OET Home Page
Filing Options
Grantee Registration
Modify Grantee Information
Form 731
Complete Unfinished Form 731
Add Attachments
Submit Correspondence
Register New Test Firm
Renew Test Firm/Add Exhibits
Test Firm Accrediting Body Login
Return to 159 Form
Add/Modify Grant Deferral Date
Change Short-Term Confidential Date
Reports
Pending Application Status
Authorization Search
Grantee Search
Pending Grantee Search
TCB Search
Test Firms
Test Firm Accrediting Bodies

17 results were found that match the search criteria:
Applicant Name: [redacted]

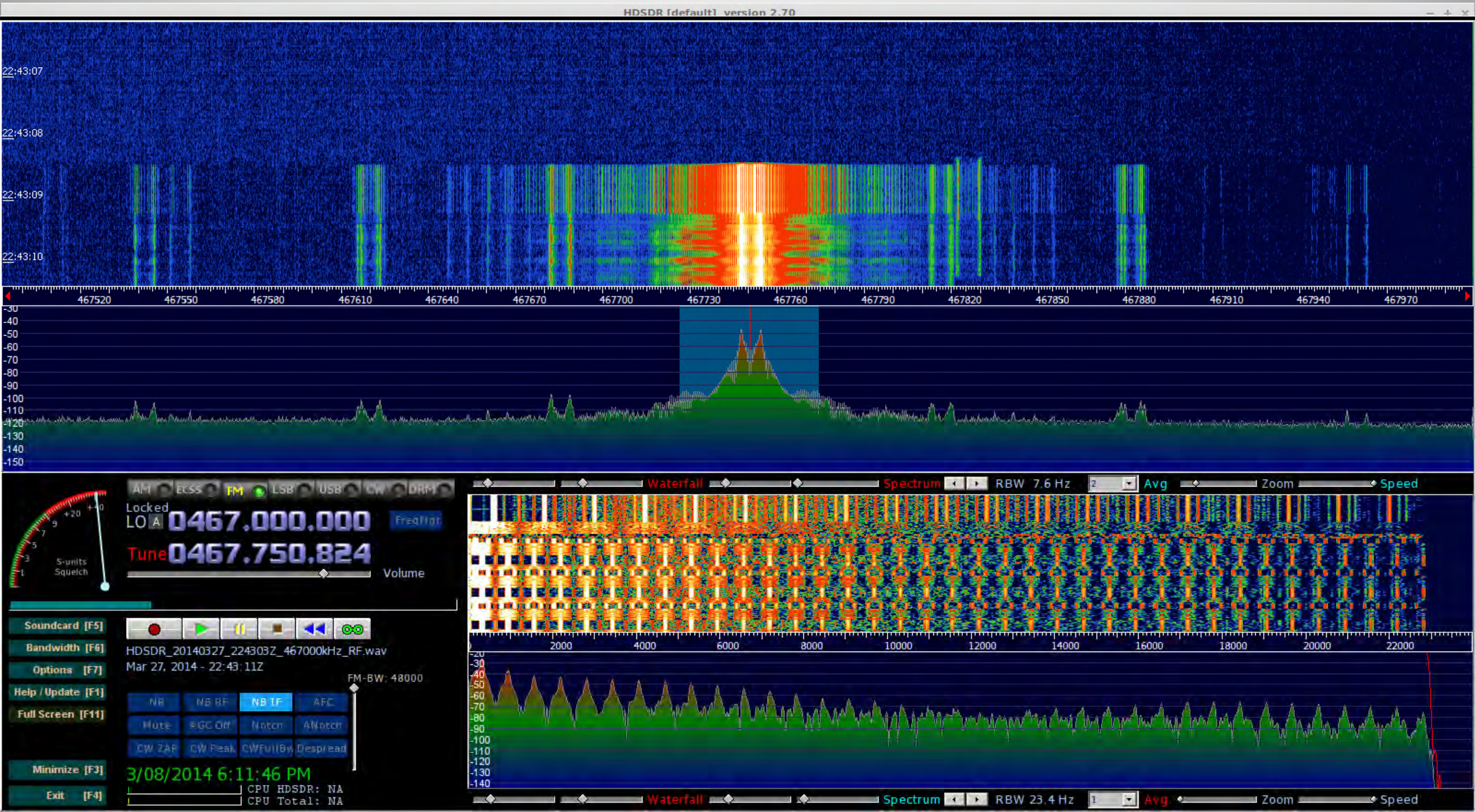
Displaying records 1 through 10 of 17.

View Form	Display Exhibits	Display Grant	Display Correspondence	Applicant Name	Address	City	State	Country	Zip Code	FCC ID	Application Purpose	Final Action Date	Lower Frequency In MHz	Upper Frequency In MHz
□	Detail Summary	✓	✉	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	448.0	448.0
□	Detail Summary	✓	✉	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	467.75	467.75
□	Detail Summary	✓	✉	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	467.75	467.75
□	Detail Summary	✓	✉	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	467.75	467.75
□	Detail Summary	✓	✉	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	467.75	467.75
□	Detail Summary	✓	✉	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	467.75	467.75
□	Detail Summary	✓	✉	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	467.75	467.75
□	Detail Summary	✓	✉	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	467.75	467.75
□	Detail Summary	✓	✉	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	448.0	448.0
□	Detail Summary	✓	✉	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	467.75	467.75

Show Next 10 Rows

Perform Search Again

Step 1: Frequency



HDSDR [default] version 2.70

Locked

LO A 0467.000.000

Tune 0467.750.824

HDSDR_20140327_224303Z_467000kHz_RF.wav

Mar 27, 2014 - 22:43:11Z

FM-BW: 48000

RBW 7.6 Hz

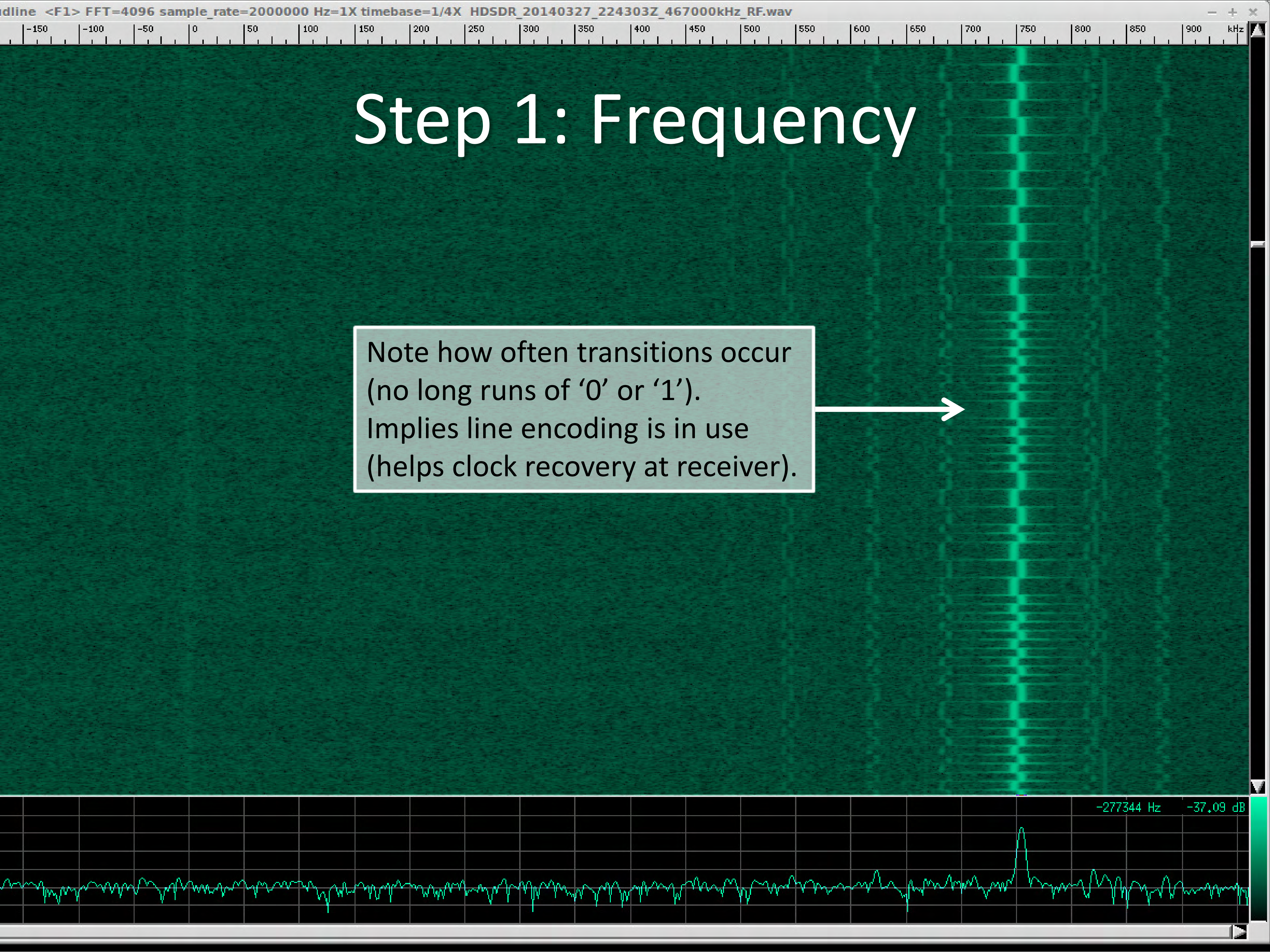
RBW 23.4 Hz

3/08/2014 6:11:46 PM

CPU HDSDR: NA

CPU Total: NA

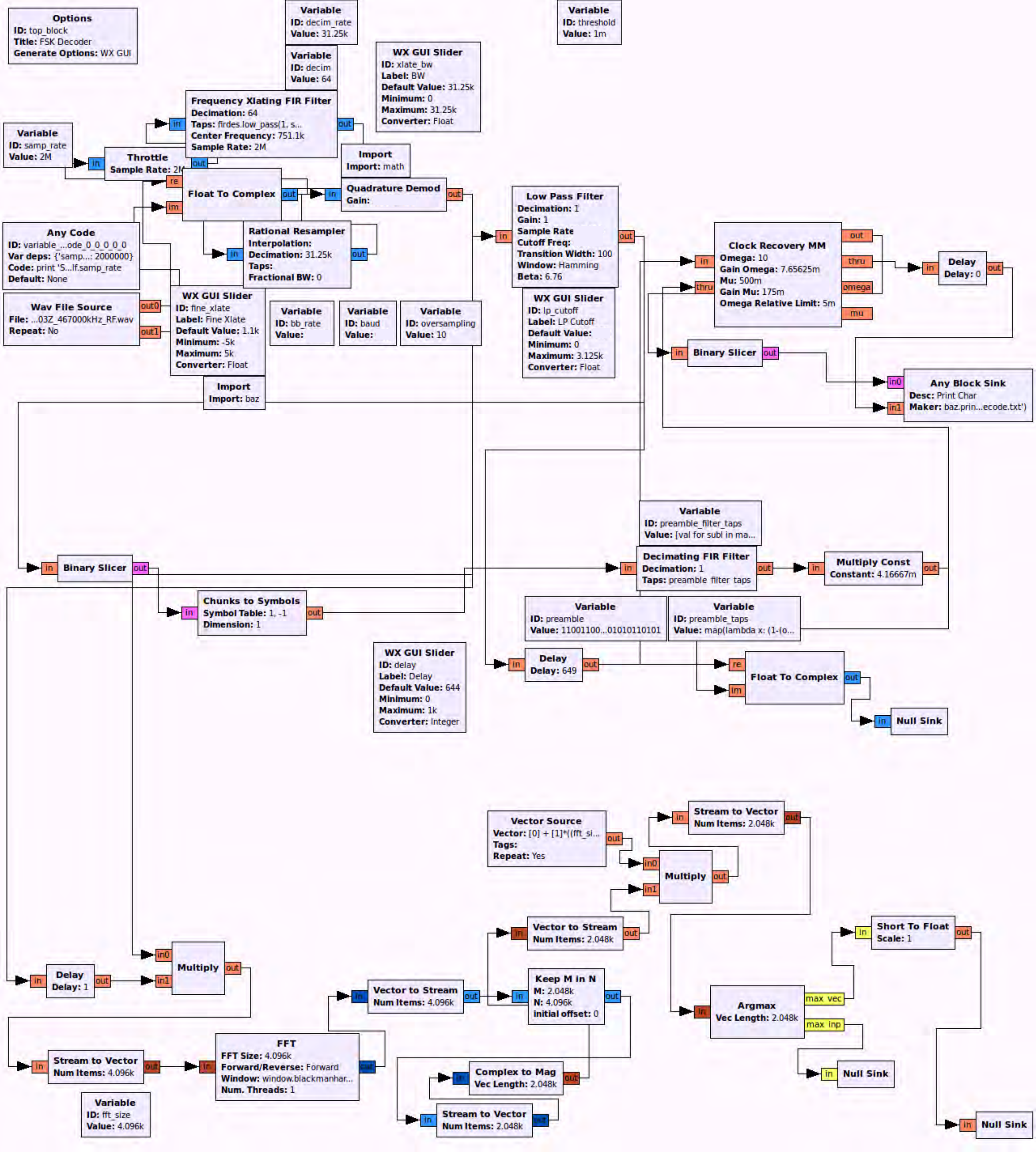
Step 1: Frequency



Note how often transitions occur (no long runs of ‘0’ or ‘1’).
Implies line encoding is in use (helps clock recovery at receiver).

dline <F1> FFT=4096 sample_rate=2000000 Hz=1X timebase=1/4X HDSDR_20140327_224303Z_467000kHz_RF.wav
-150
-100
-50
0
50
100
150
200
250
300
350
400
450
500
550
600
650
700
750
800
850
900
kHz
-277344 Hz
-37.09 dB

Flowgraph



Options
ID: top_block
Title: FSK Decoder
Generate Options: WX GUI

Variable
ID: decim_rate
Value: 31.25k

Variable
ID: decim
Value: 64

WX GUI Slider
ID: xlate_bw
Label: BW
Default Value: 31.25k
Minimum: 0
Maximum: 31.25k
Converter: Float

Variable
ID: threshold
Value: 1m

Frequency Xlating FIR Filter
Decimation: 64
Taps: firdes.low_pass(1, s...
Center Frequency: 751.1k
Sample Rate: 2M

Variable
ID: samp_rate
Value: 2M

Throttle
Sample Rate: 2M

Import
Import: math

Float To Complex

Quadrature Demod
Gain:

Low Pass Filter
Decimation: 1
Gain: 1
Sample Rate
Cutoff Freq:
Transition Width: 100
Window: Hamming
Beta: 6.76

Any Code
ID: variable_...ode_0_0_0_0_0
Var deps: {'samp...: 2000000}
Code: print 'S...lf.samp_rate
Default: None

Rational Resampler
Interpolation:
Decimation: 31.25k
Taps:
Fractional BW: 0

Clock Recovery MM
Omega: 10
Gain Omega: 7.65625m
Mu: 500m
Gain Mu: 175m
Omega Relative Limit: 5m

Delay
Delay: 0

Wav File Source
File: ...03Z_467000kHz_RF.wav
Repeat: No

WX GUI Slider
ID: fine_xlate
Label: Fine Xlate
Default Value: 1.1k
Minimum: -5k
Maximum: 5k
Converter: Float

Variable
ID: bb_rate
Value:

Variable
ID: baud
Value:

Variable
ID: oversampling
Value: 10

WX GUI Slider
ID: lp_cutoff
Label: LP Cutoff
Default Value:
Minimum: 0
Maximum: 3.125k
Converter: Float

Binary Slicer

Any Block Sink
Desc: Print Char
Maker: baz.prin...ecode.txt')

Import
Import: baz

Variable
ID: preamble_filter_taps
Value: [val for subl in ma...

Binary Slicer

Decimating FIR Filter
Decimation: 1
Taps: preamble_filter_taps

Multiply Const
Constant: 4.16667m

Chunks to Symbols
Symbol Table: 1, -1
Dimension: 1

Variable
ID: preamble
Value: 11001100...01010110101

Variable
ID: preamble_taps
Value: map(lambda x: (1-(o...

WX GUI Slider
ID: delay
Label: Delay
Default Value: 644
Minimum: 0
Maximum: 1k
Converter: Integer

Delay
Delay: 649

Float To Complex

Null Sink

Vector Source
Vector: [0] + [1]*((fft_si...
Tags:
Repeat: Yes

Stream to Vector
Num Items: 2.048k

Multiply

Vector to Stream
Num Items: 2.048k

Short To Float
Scale: 1

Delay
Delay: 1

Multiply

Vector to Stream
Num Items: 4.096k

Keep M in N
M: 2.048k
N: 4.096k
initial offset: 0

Argmax
Vec Length: 2.048k

Stream to Vector
Num Items: 4.096k

FFT
FFT Size: 4.096k
Forward/Reverse: Forward
Window: window.blackmanhar...
Num. Threads: 1

Complex to Mag
Vec Length: 2.048k

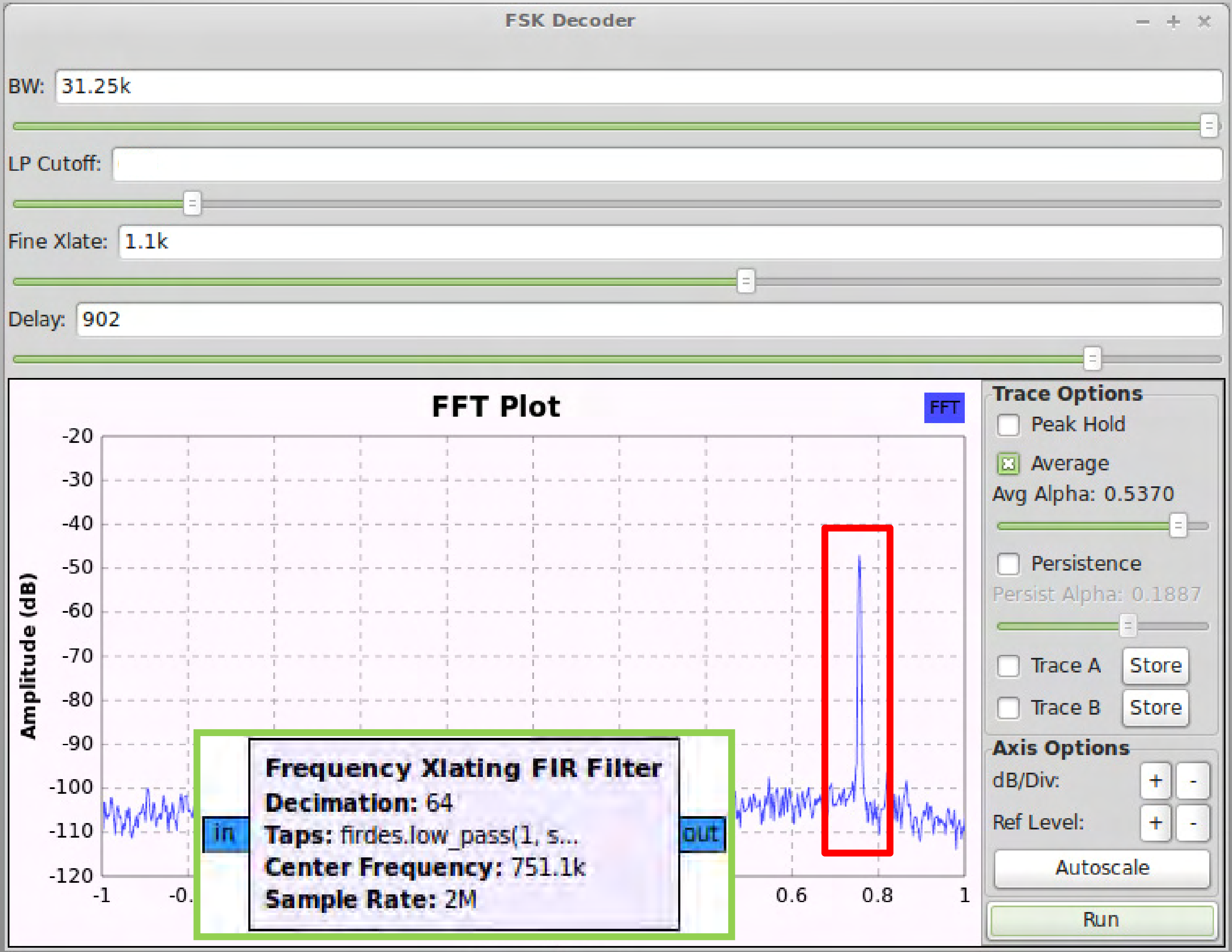
Null Sink

Variable
ID: fft_size
Value: 4.096k

Stream to Vector
Num Items: 2.048k

Null Sink

Step 2: Channel Selection



FSK Decoder

BW: 31.25k

LP Cutoff:

Fine Xlate: 1.1k

Delay: 902

Frequency Xlating FIR Filter
Decimation: 64
Taps: firdes.low_pass(1, s...
Center Frequency: 751.1k
Sample Rate: 2M

Trace Options

☐ Peak Hold

☒ Average

Avg Alpha: 0.5370

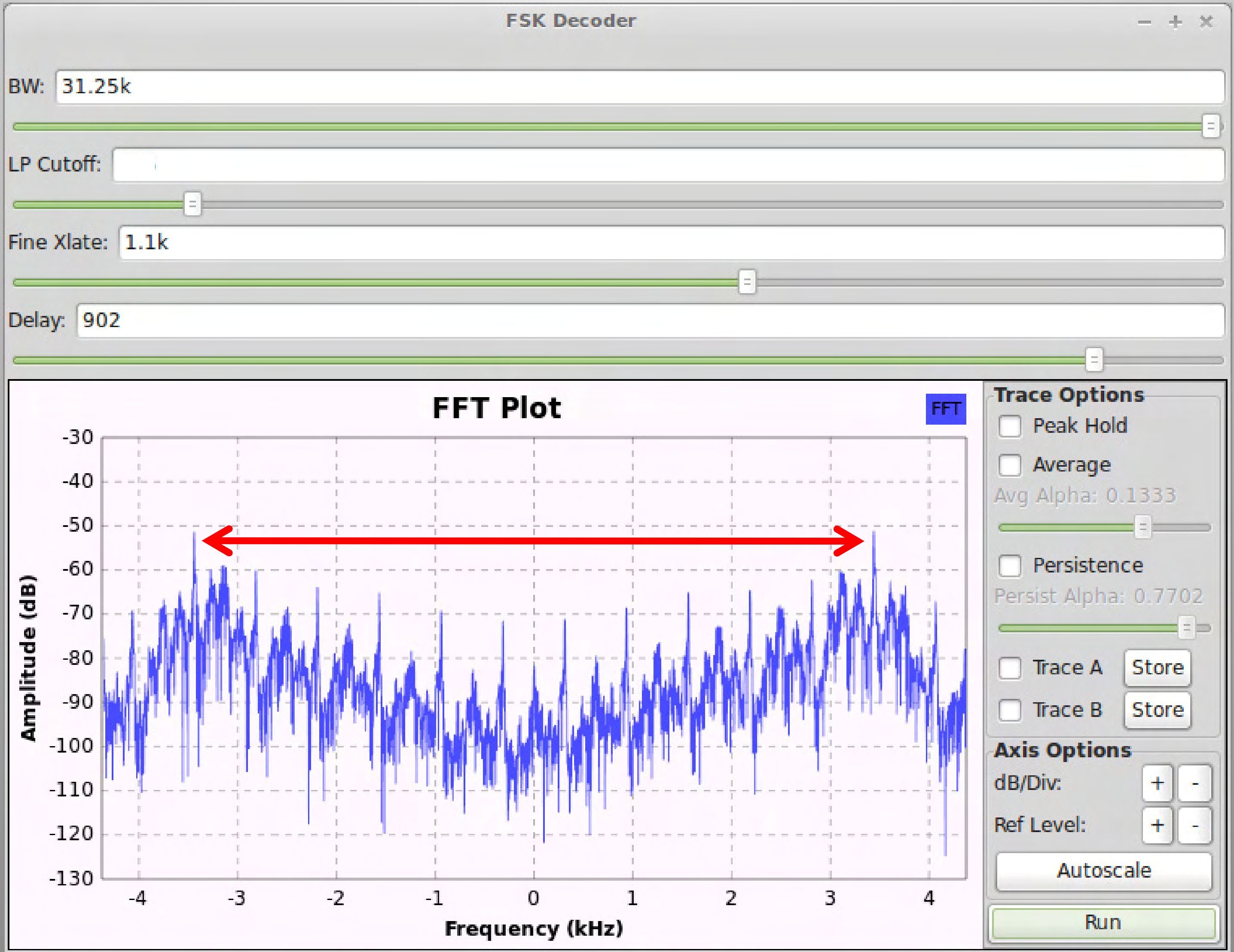
☐ Persistence

Persist Alpha: 0.1887

☐ Trace A

☐ Trace B

Step 3: FSK Deviation



FSK Decoder

BW: 31.25k

LP Cutoff:

Fine Xlate: 1.1k

Delay: 902

Trace Options

☐ Peak Hold

☐ Average

Avg Alpha: 0.1333

☐ Persistence

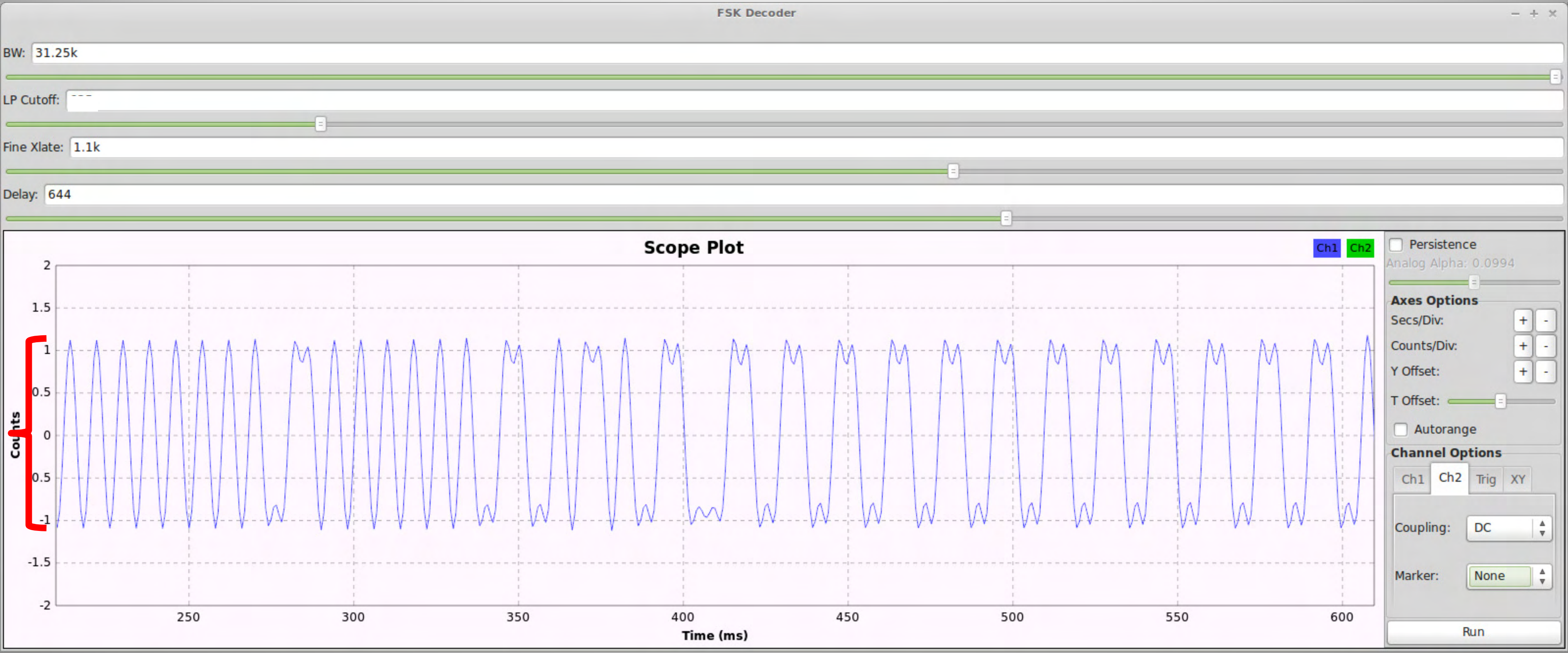
Persist Alpha: 0.7702

☐ Trace A

☐ Trace B

Axis Options

Step 4: Quadrature Demod



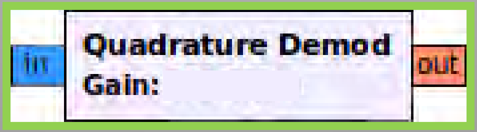
FSK Decoder

BW: 31.25k

LP Cutoff:

Fine Xlate: 1.1k

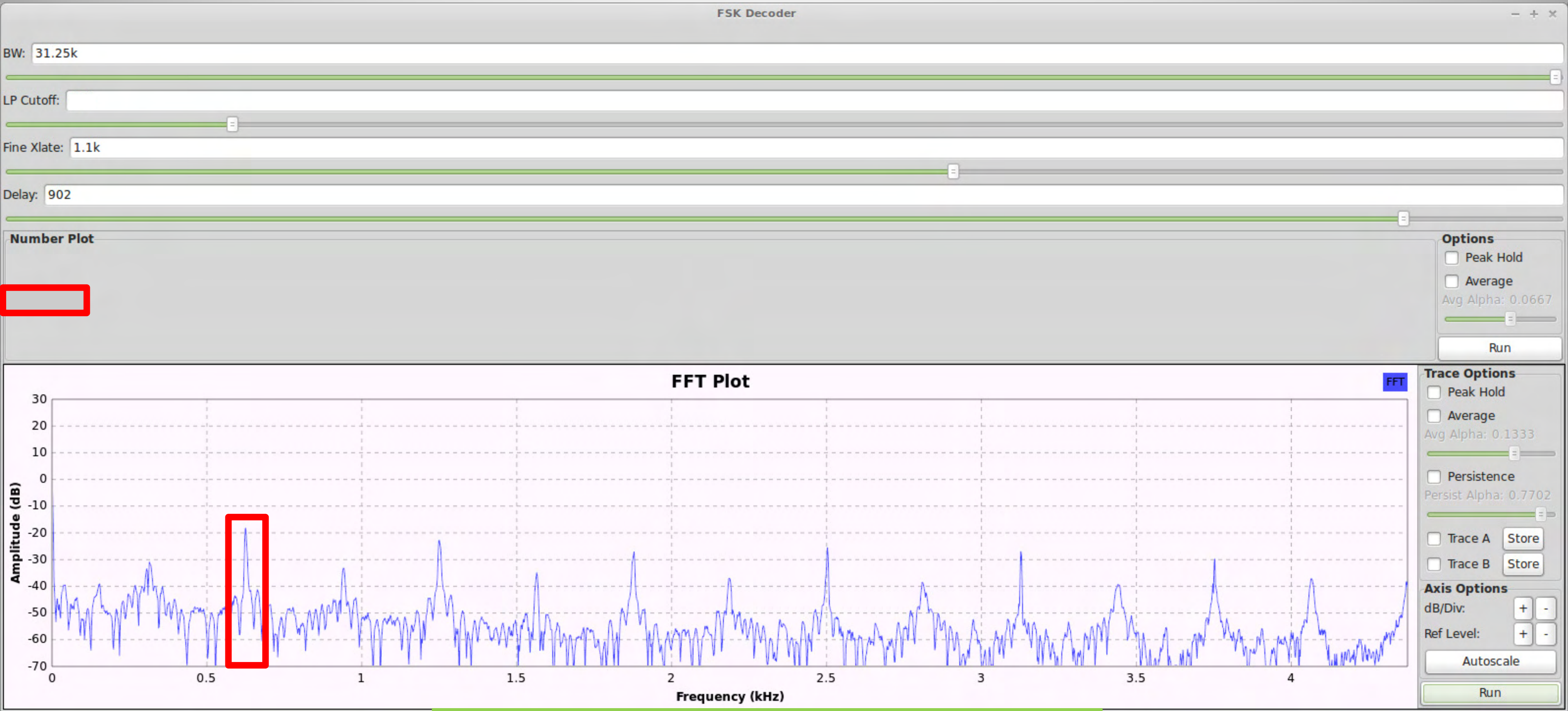
Delay: 644



Quadrature Demod

Gain:

Step 5: Baud Rate



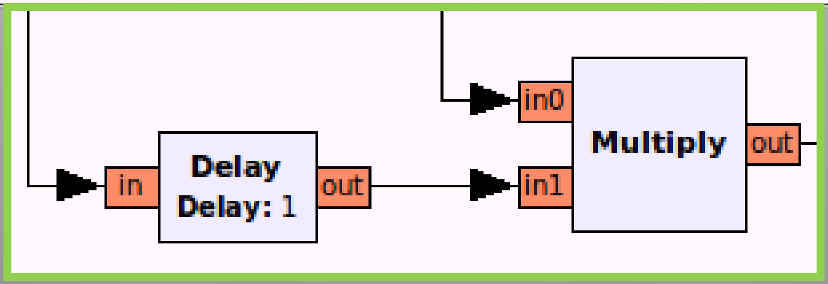
FSK Decoder

BW: 31.25k

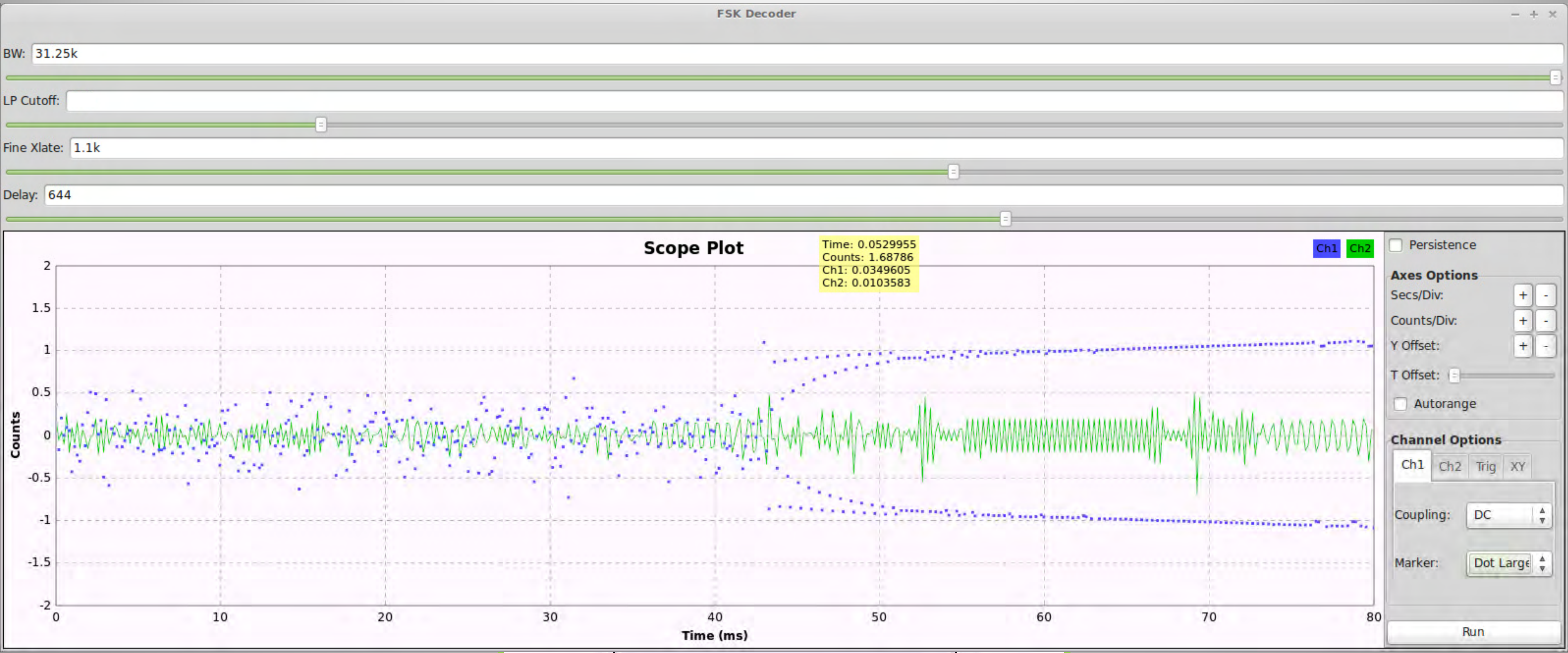
LP Cutoff:

Fine Xlate: 1.1k

Delay: 902



Step 5: Clock Recovery



BW: 31.25k

LP Cutoff:

Fine Xlate: 1.1k

Delay: 644

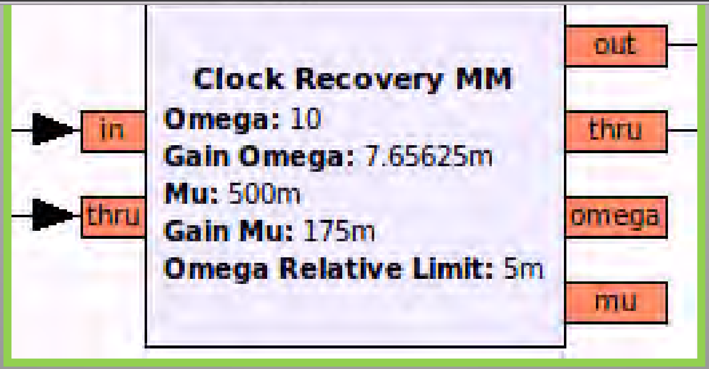
Time: 0.0529955
Counts: 1.68786
Ch1: 0.0349605
Ch2: 0.0103583

☐ Persistence

☐ Autorange

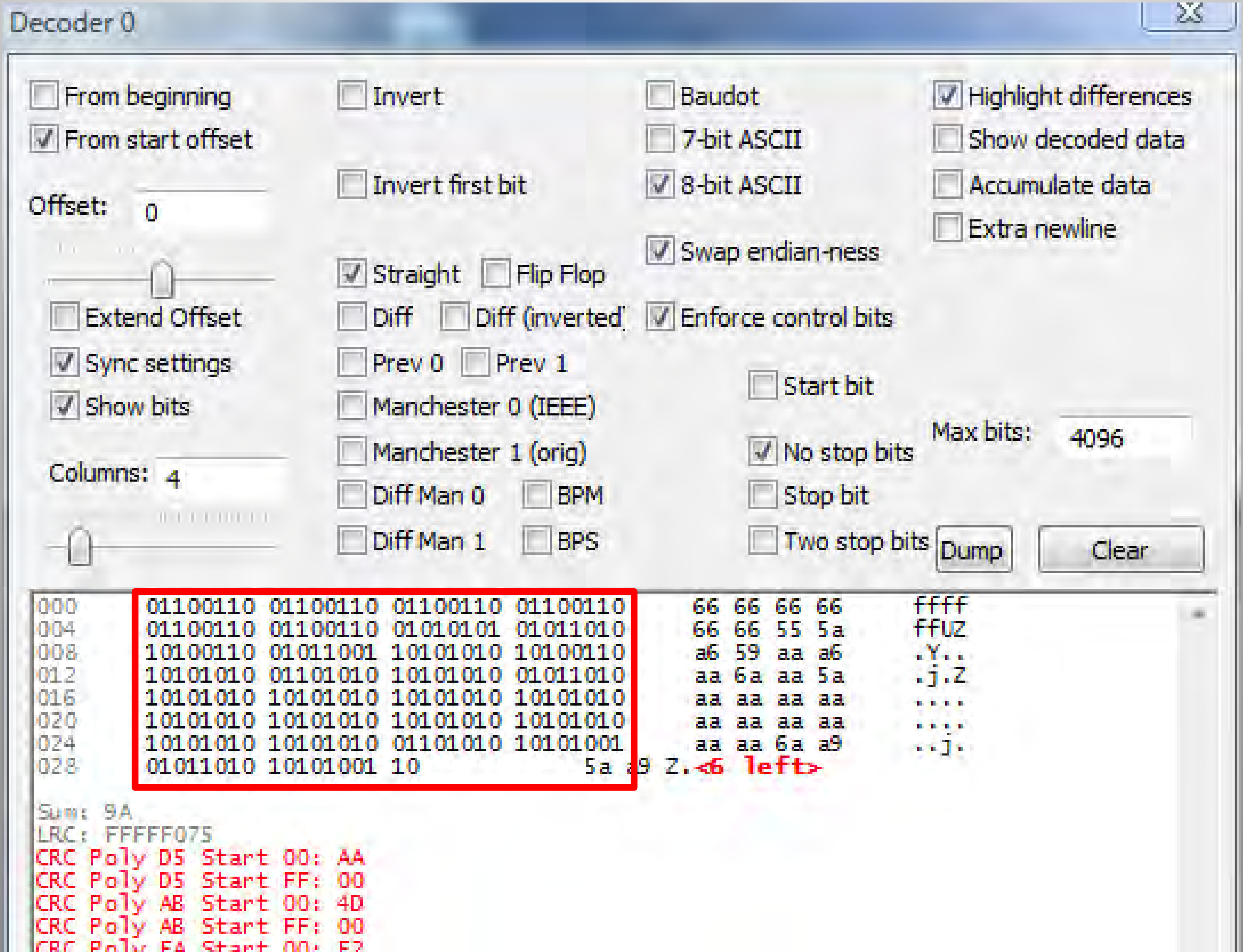
Coupling: DC

Marker: Dot Large



Clock Recovery MM
Omega: 10
Gain Omega: 7.65625m
Mu: 500m
Gain Mu: 175m
Omega Relative Limit: 5m

Step 6: Line Encoding



Decoder 0

☐ From beginning
☑ From start offset

Offset: 0

☐ Extend Offset
☑ Sync settings
☑ Show bits

Columns: 4

☐ Invert

☐ Invert first bit

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

☐ Baudot
☐ 7-bit ASCII
☑ 8-bit ASCII

☑ Swap endian-ness

☑ Enforce control bits

☐ Start bit

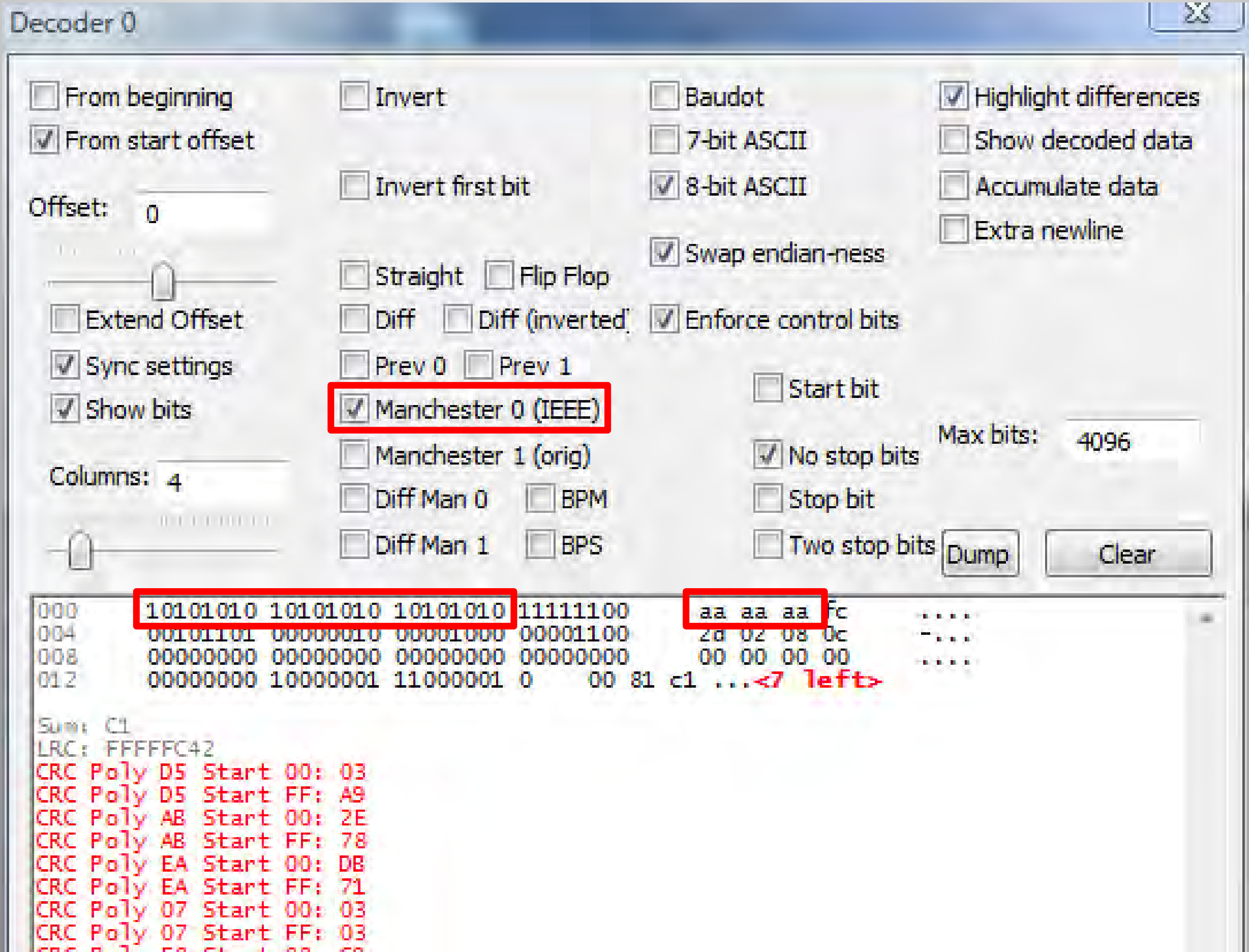
☑ No stop bits
☐ Stop bit
☐ Two stop bits

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

Max bits: 4096

```
000      01100110 01100110 01100110 01100110     66 66 66 66     ffff
004      01100110 01100110 01010101 01011010     66 66 55 5a     ffUZ
008      10100110 01011001 10101010 10100110     a6 59 aa a6     .Y..
012      10101010 01101010 10101010 01011010     aa 6a aa 5a     .j.Z
016      10101010 10101010 10101010 10101010     aa aa aa aa     ....
020      10101010 10101010 10101010 10101010     aa aa aa aa     ....
024      10101010 10101010 01101010 10101001     aa aa 6a a9     ..j.
028      01011010 10101001 10                5a a9 Z.<6 left>

Sum: 9A
LRC: FFFFF075
CRC Poly D5 Start 00: AA
CRC Poly D5 Start FF: 00
CRC Poly AB Start 00: 4D
CRC Poly AB Start FF: 00
CRC Poly EA Start 00: F2
```

Manchester Encoding



Decoder 0

☐ From beginning
☑ From start offset
Offset: 0
☐ Extend Offset
☑ Sync settings
☑ Show bits
Columns: 4

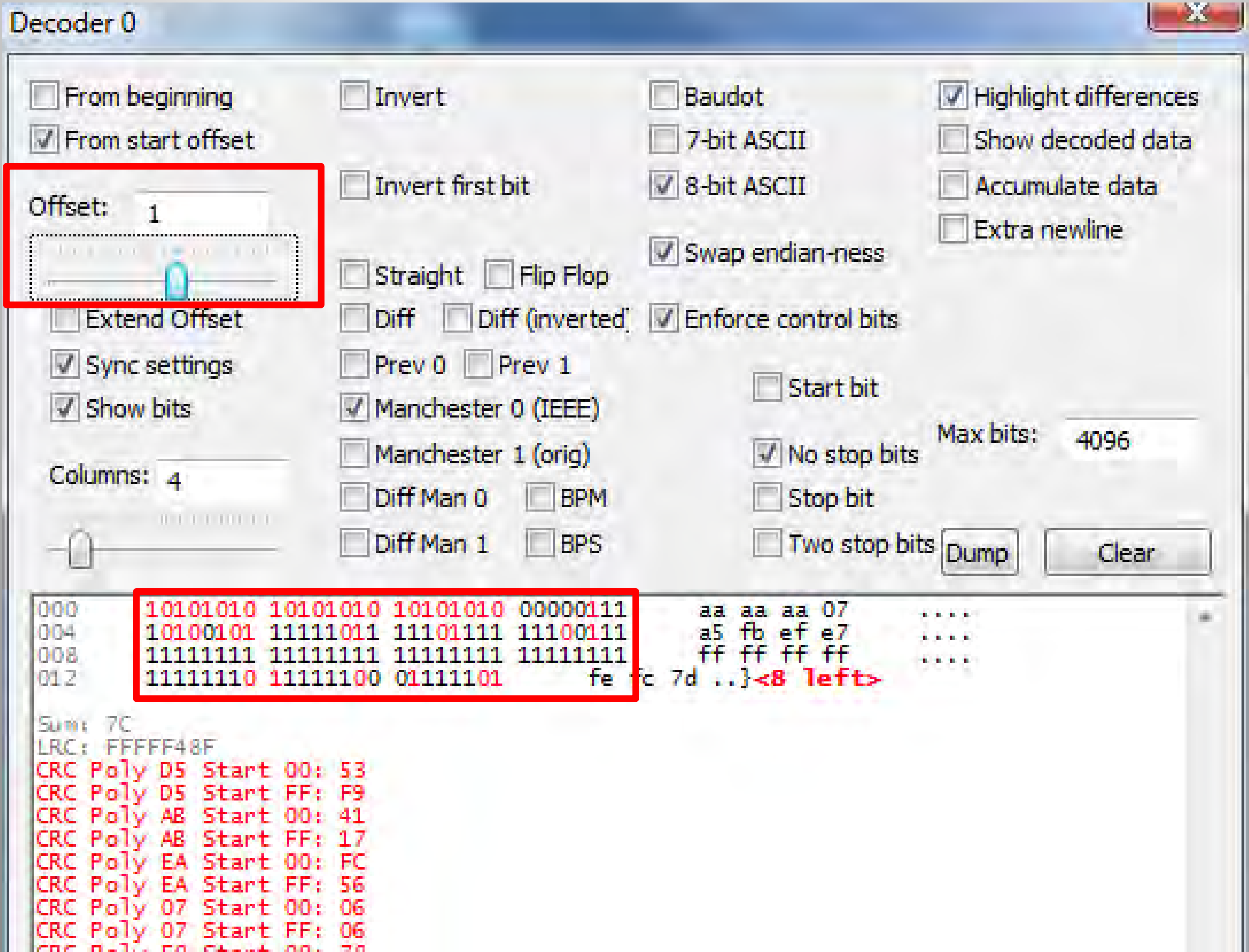
☐ Invert
☐ Invert first bit
☐ Straight ☐ Flip Flop
☐ Diff ☐ Diff (inverted)
☐ Prev 0 ☐ Prev 1
☑ Manchester 0 (IEEE)
☐ Manchester 1 (orig)
☐ Diff Man 0 ☐ BPM
☐ Diff Man 1 ☐ BPS

☐ Baudot
☐ 7-bit ASCII
☑ 8-bit ASCII
☑ Swap endian-ness
☑ Enforce control bits
☐ Start bit
☑ No stop bits
☐ Stop bit
☐ Two stop bits

☑ Highlight differences
☐ Show decoded data
☐ Accumulate data
☐ Extra newline
Max bits: 4096

```
000     10101010 10101010 10101010 11111100     aa aa aa fc     ....
004     00101101 00000010 00001000 00001100     2d 02 08 0c     -...
008     00000000 00000000 00000000 00000000     00 00 00 00     ....
012     00000000 10000001 11000001 0     00 81 c1 ...<7 left>

Sum: C1
LRC: FFFFFC42
CRC Poly D5 Start 00: 03
CRC Poly D5 Start FF: A9
CRC Poly AB Start 00: 2E
CRC Poly AB Start FF: 78
CRC Poly EA Start 00: DB
CRC Poly EA Start FF: 71
CRC Poly 07 Start 00: 03
CRC Poly 07 Start FF: 03
```

Manchester Violation



Decoder 0

☐ From beginning
☑ From start offset

Offset: 1

☐ Extend Offset
☑ Sync settings
☑ Show bits

Columns: 4

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

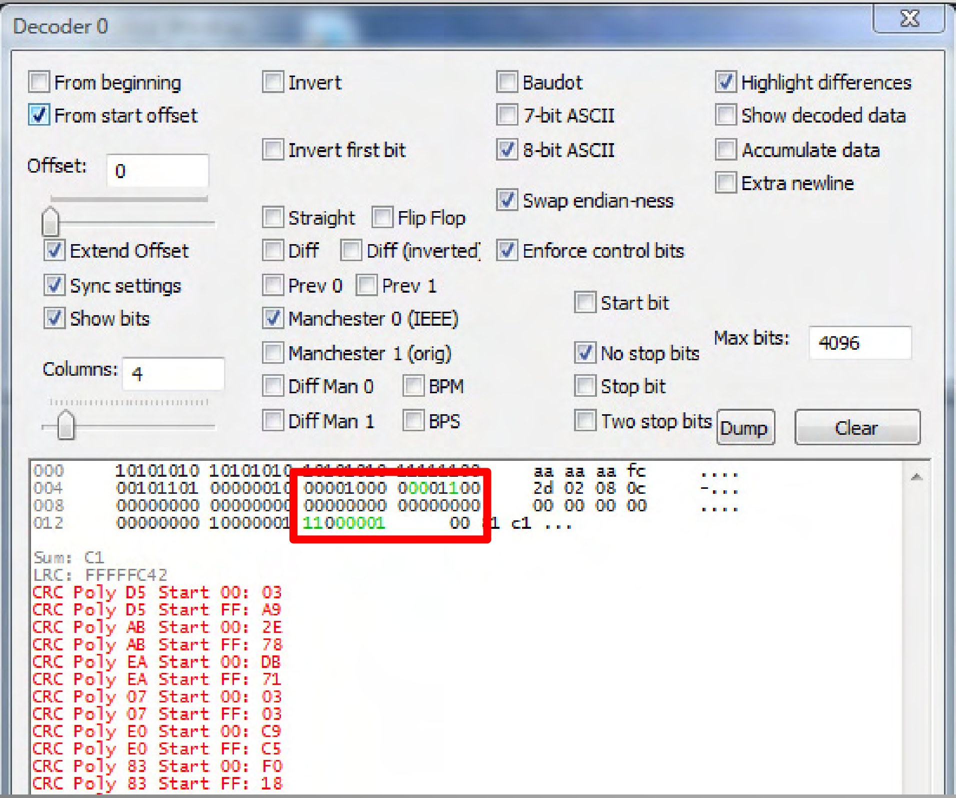
☐ Baudot
☐ 7-bit ASCII
☑ 8-bit ASCII
☑ Swap endian-ness
☑ Enforce control bits
☐ Start bit
☑ No stop bits
☐ Stop bit
☐ Two stop bits

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

Max bits: 4096

```
000     10101010 10101010 10101010 00000111      aa aa aa 07     ....
004     10100101 11111011 11101111 11100111      a5 fb ef e7     ....
008     11111111 11111111 11111111 11111111      ff ff ff ff     ....
012     11111110 11111100 01111101          fe fc 7d ..}<8 left>

Sum: 7C
LRC: FFFFF48F
CRC Poly D5 Start 00: 53
CRC Poly D5 Start FF: F9
CRC Poly AB Start 00: 41
CRC Poly AB Start FF: 17
CRC Poly EA Start 00: FC
CRC Poly EA Start FF: 56
CRC Poly 07 Start 00: 06
CRC Poly 07 Start FF: 06
```

Step 7: Compare Changing Bits



Decoder 0

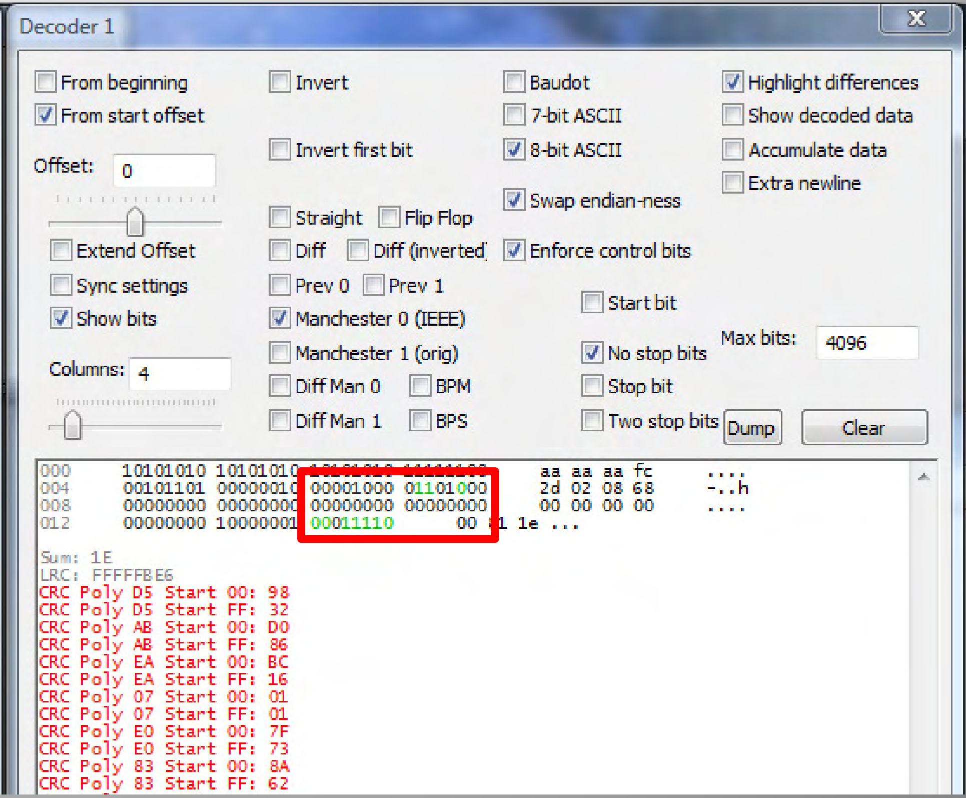
☐ From beginning
☑ From start offset
Offset: 0
☑ Extend Offset
☑ Sync settings
☑ Show bits
Columns: 4

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

☐ Baudot
☐ 7-bit ASCII
☑ 8-bit ASCII
☑ Swap endian-ness
☑ Enforce control bits
☐ Start bit
☑ No stop bits
☐ Stop bit
☐ Two stop bits

☑ Highlight differences
☐ Show decoded data
☐ Accumulate data
☐ Extra newline
Max bits: 4096

```
000     10101010 10101010 10101010 11111100     aa aa aa fc     ....
004     00101101 00000010 00001000 00001100     2d 02 08 0c     -...
008     00000000 00000000 00000000 00000000     00 00 00 00     ....
012     00000000 10000001 11000001          00 81 c1 ...

Sum: C1
LRC: FFFFFC42
CRC Poly D5 Start 00: 03
CRC Poly D5 Start FF: A9
CRC Poly AB Start 00: 2E
CRC Poly AB Start FF: 78
CRC Poly EA Start 00: DB
CRC Poly EA Start FF: 71
CRC Poly 07 Start 00: 03
CRC Poly 07 Start FF: 03
CRC Poly E0 Start 00: C9
CRC Poly E0 Start FF: C5
CRC Poly 83 Start 00: F0
CRC Poly 83 Start FF: 18
```



Decoder 1

☐ From beginning
☑ From start offset
Offset: 0
☐ Extend Offset
☐ Sync settings
☑ Show bits
Columns: 4

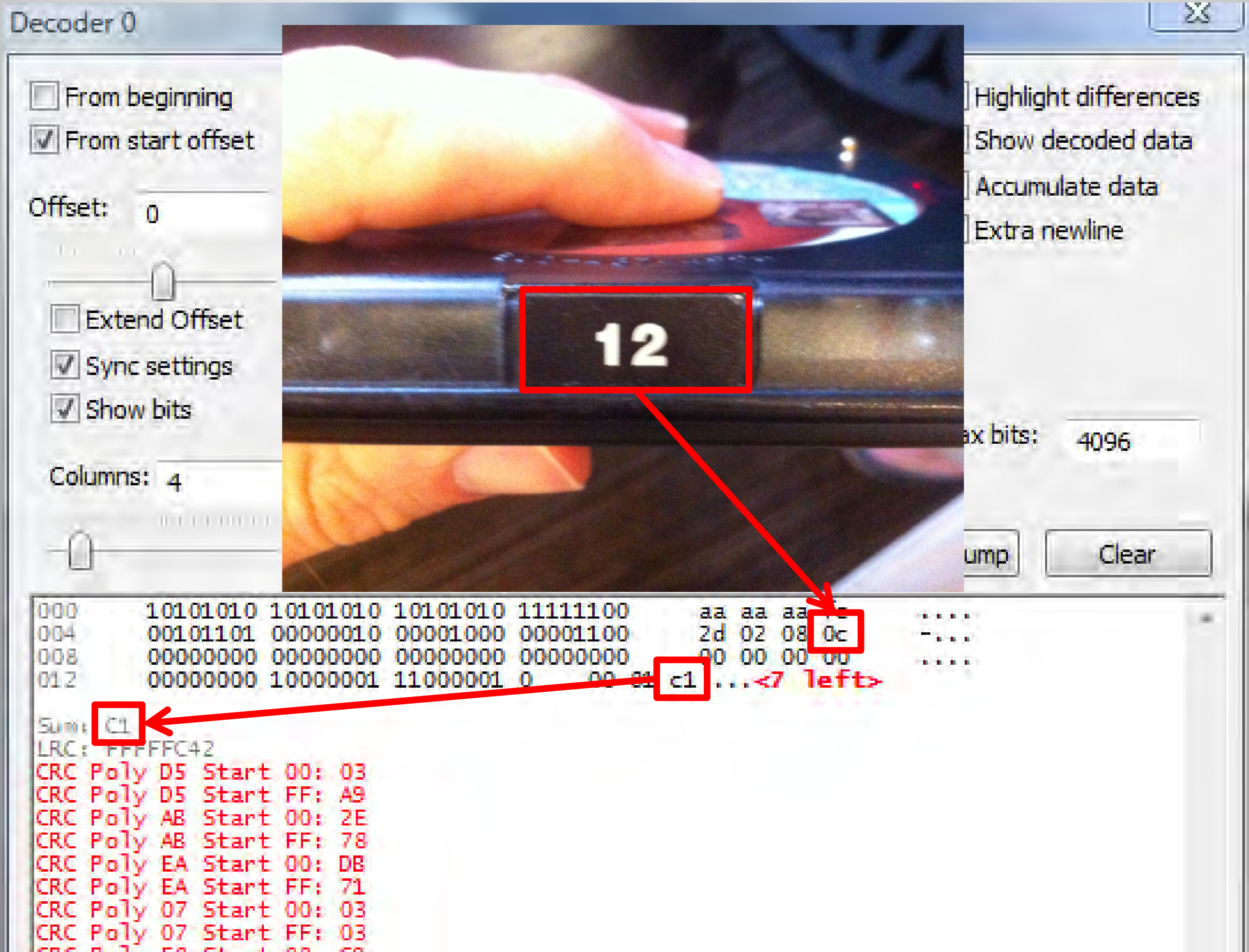
☐ Invert
☐ Invert first bit
☐ Straight ☐ Flip Flop
☐ Diff ☐ Diff (inverted)
☐ Prev 0 ☐ Prev 1
☑ Manchester 0 (IEEE)
☐ Manchester 1 (orig)
☐ Diff Man 0 ☐ BPM
☐ Diff Man 1 ☐ BPS

☐ Baudot
☐ 7-bit ASCII
☑ 8-bit ASCII
☑ Swap endian-ness
☑ Enforce control bits
☐ Start bit
☑ No stop bits
☐ Stop bit
☐ Two stop bits

☑ Highlight differences
☐ Show decoded data
☐ Accumulate data
☐ Extra newline
Max bits: 4096

```
000     10101010 10101010 10101010 11111100     aa aa aa fc     ....
004     00101101 00000010 00001000 01101000     2d 02 08 68     -..h
008     00000000 00000000 00000000 00000000     00 00 00 00     ....
012     00000000 10000001 00011110          00 81 1e ...

Sum: 1E
LRC: FFFFFBE6
CRC Poly D5 Start 00: 98
CRC Poly D5 Start FF: 32
CRC Poly AB Start 00: D0
CRC Poly AB Start FF: 86
CRC Poly EA Start 00: BC
CRC Poly EA Start FF: 16
CRC Poly 07 Start 00: 01
CRC Poly 07 Start FF: 01
CRC Poly E0 Start 00: 7F
CRC Poly E0 Start FF: 73
CRC Poly 83 Start 00: 8A
CRC Poly 83 Start FF: 62
```

Step 8: Finding the ID



☐ From beginning
☑ From start offset

Offset: 0

☐ Extend Offset
☑ Sync settings
☑ Show bits

Columns: 4

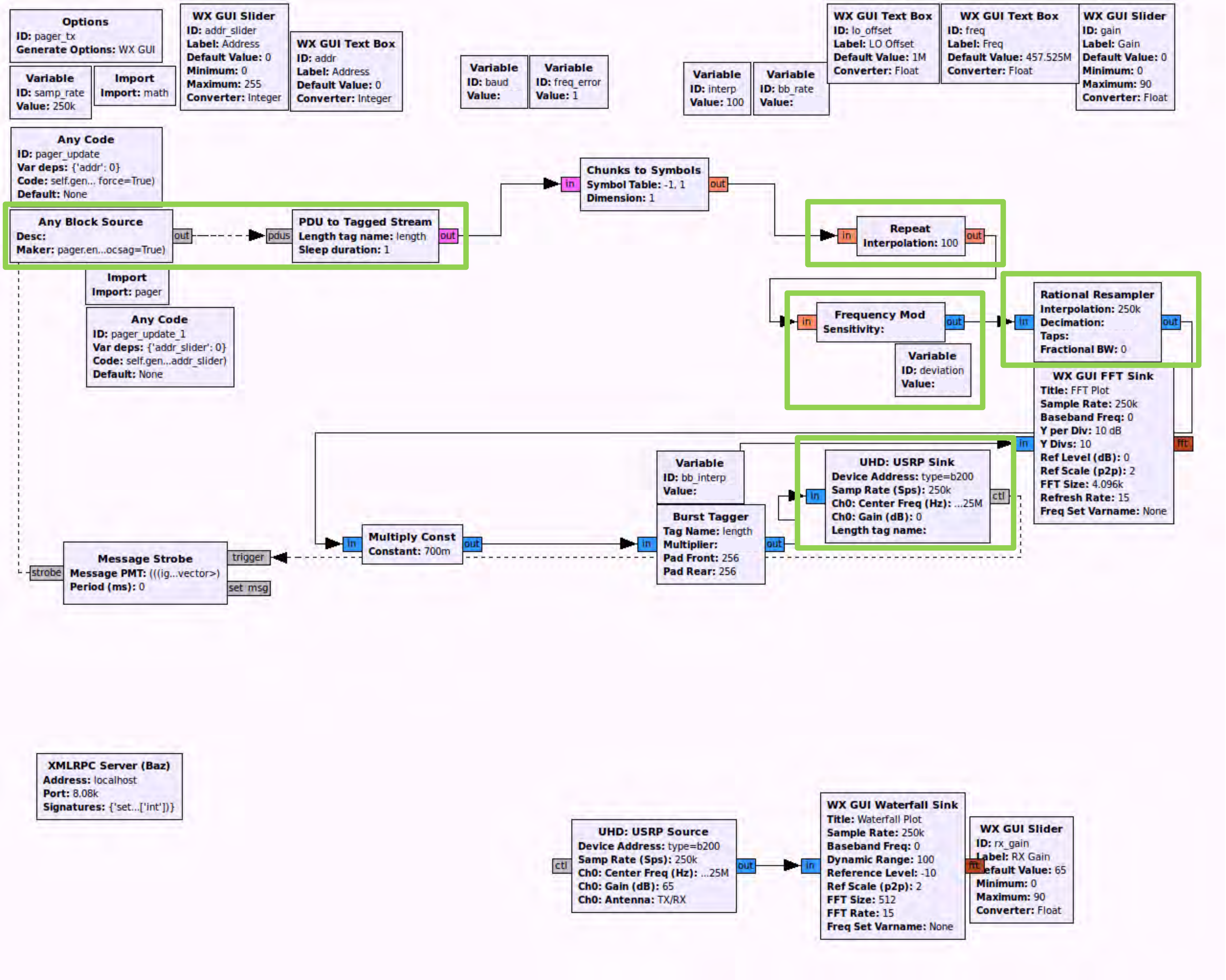
Highlight differences
Show decoded data
Accumulate data
Extra newline

ax bits: 4096

```
000      10101010 10101010 10101010 11111100      aa aa aa fc     ....
004      00101101 00000010 00001000 00001100      2d 02 08 0c     -...
008      00000000 00000000 00000000 00000000      00 00 00 00     ....
012      00000000 10000001 11000001 0       00 81 c1 ...<7 left>

Sum: C1
LRC: FFFFFC42
CRC Poly D5 Start 00: 03
CRC Poly D5 Start FF: A9
CRC Poly AB Start 00: 2E
CRC Poly AB Start FF: 78
CRC Poly EA Start 00: DB
CRC Poly EA Start FF: 71
CRC Poly 07 Start 00: 03
CRC Poly 07 Start FF: 03
```

Modulator

- Reverse the decoding process:
  1. Construct packet
     a) Preamble (wake up receiver)
     b) Magic header (sync & system ID)
     c) Pager number
     d) Checksum
  2. Interpolate (choose samples per bit)
  3. Frequency Modulate
  4. Apply pulse-shaping filter (*ideally*)
  5. Resample for transmitter



Options
ID: pager_tx
Generate Options: WX GUI

Variable
ID: samp_rate
Value: 250k

Import
Import: math

WX GUI Slider
ID: addr_slider
Label: Address
Default Value: 0
Minimum: 0
Maximum: 255
Converter: Integer

WX GUI Text Box
ID: addr
Label: Address
Default Value: 0
Converter: Integer

Variable
ID: baud
Value:

Variable
ID: freq_error
Value: 1

Variable
ID: interp
Value: 100

Variable
ID: bb_rate
Value:

WX GUI Text Box
ID: lo_offset
Label: LO Offset
Default Value: 1M
Converter: Float

WX GUI Text Box
ID: freq
Label: Freq
Default Value: 457.525M
Converter: Float

WX GUI Slider
ID: gain
Label: Gain
Default Value: 0
Minimum: 0
Maximum: 90
Converter: Float

Any Code
ID: pager_update
Var deps: {'addr': 0}
Code: self.gen... force=True)
Default: None

Chunks to Symbols
Symbol Table: -1, 1
Dimension: 1

Any Block Source
Desc:
Maker: pager.en...ocsag=True)

PDU to Tagged Stream
Length tag name: length
Sleep duration: 1

Repeat
Interpolation: 100

Import
Import: pager

Any Code
ID: pager_update_1
Var deps: {'addr_slider': 0}
Code: self.gen...addr_slider)
Default: None

Frequency Mod
Sensitivity:

Variable
ID: deviation
Value:

Rational Resampler
Interpolation: 250k
Decimation:
Taps:
Fractional BW: 0

WX GUI FFT Sink
Title: FFT Plot
Sample Rate: 250k
Baseband Freq: 0
Y per Div: 10 dB
Y Divs: 10
Ref Level (dB): 0
Ref Scale (p2p): 2
FFT Size: 4.096k
Refresh Rate: 15
Freq Set Varname: None

Variable
ID: bb_interp
Value:

UHD: USRP Sink
Device Address: type=b200
Samp Rate (Sps): 250k
Ch0: Center Freq (Hz): ...25M
Ch0: Gain (dB): 0
Length tag name:

Multiply Const
Constant: 700m

Burst Tagger
Tag Name: length
Multiplier:
Pad Front: 256
Pad Rear: 256

Message Strobe
Message PMT: (((ig...vector>)
Period (ms): 0

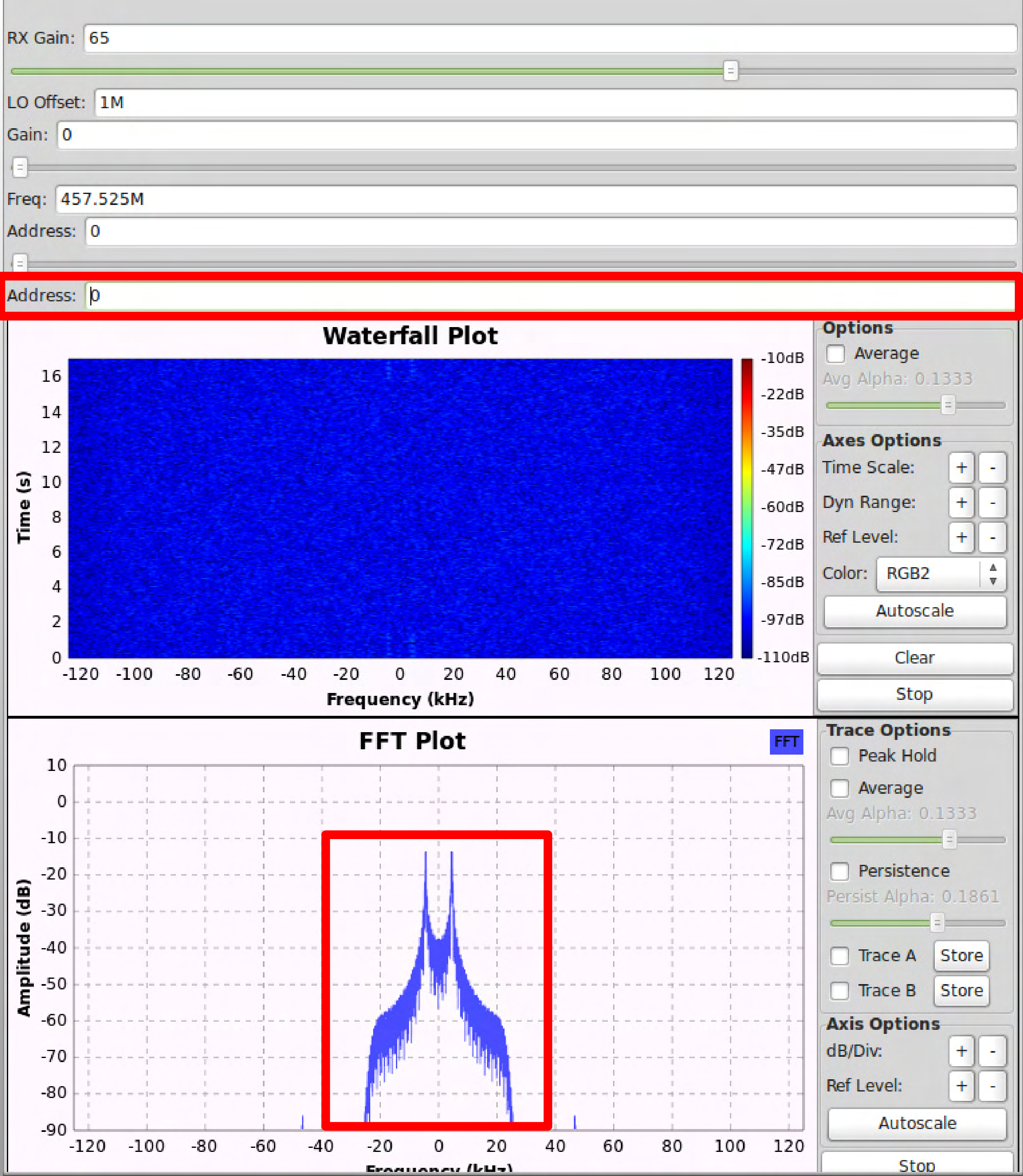
XMLRPC Server (Baz)
Address: localhost
Port: 8.08k
Signatures: {'set...['int']}}

UHD: USRP Source
Device Address: type=b200
Samp Rate (Sps): 250k
Ch0: Center Freq (Hz): ...25M
Ch0: Gain (dB): 65
Ch0: Antenna: TX/RX

WX GUI Waterfall Sink
Title: Waterfall Plot
Sample Rate: 250k
Baseband Freq: 0
Dynamic Range: 100
Reference Level: -10
Ref Scale (p2p): 2
FFT Size: 512
FFT Rate: 15
Freq Set Varname: None

WX GUI Slider
ID: rx_gain
Label: RX Gain
Default Value: 65
Minimum: 0
Maximum: 90
Converter: Float

Modulator



RX Gain: 65

LO Offset: 1M

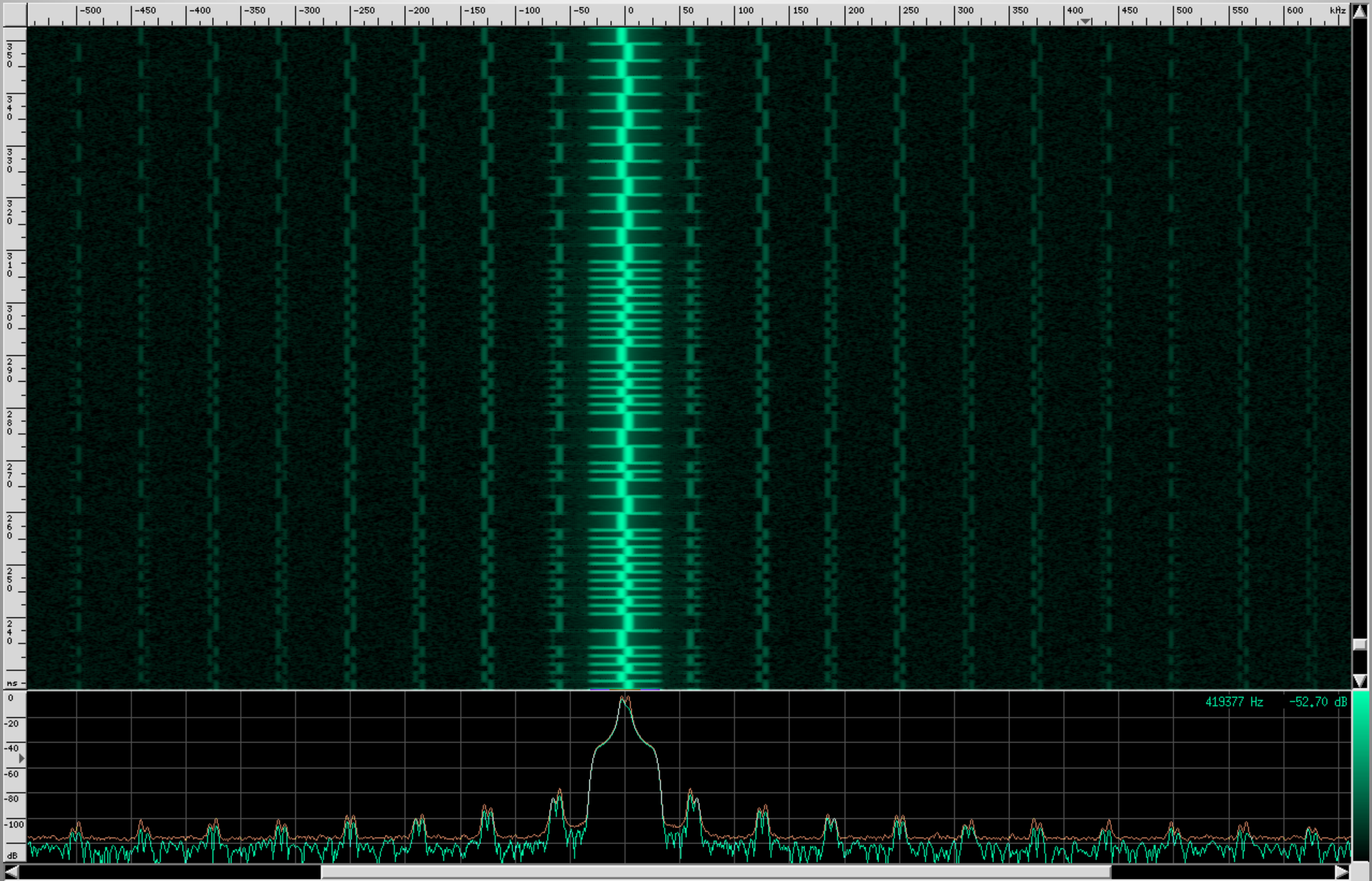
Gain: 0

Freq: 457.525M

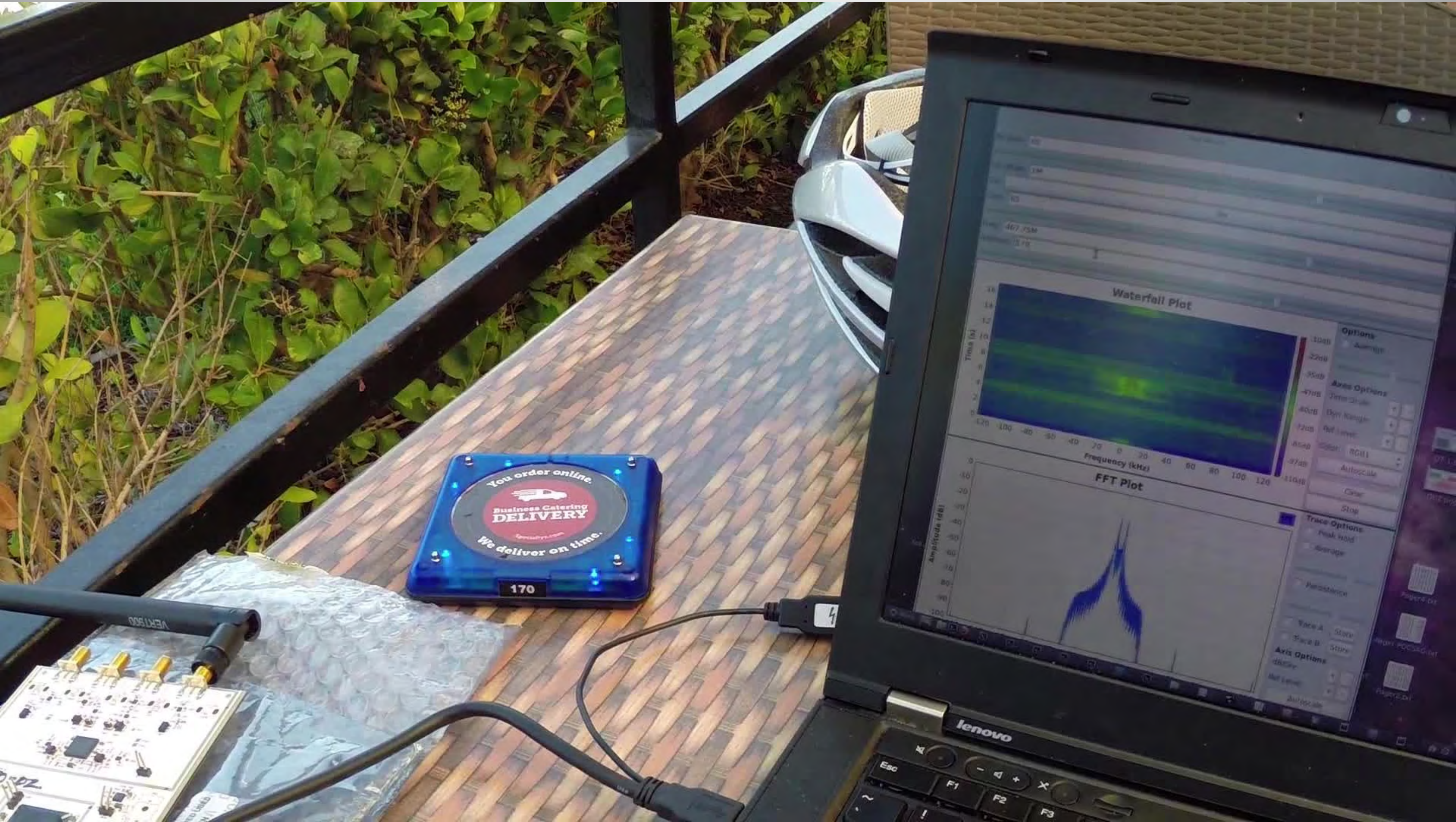
Address: 0

Address: 0

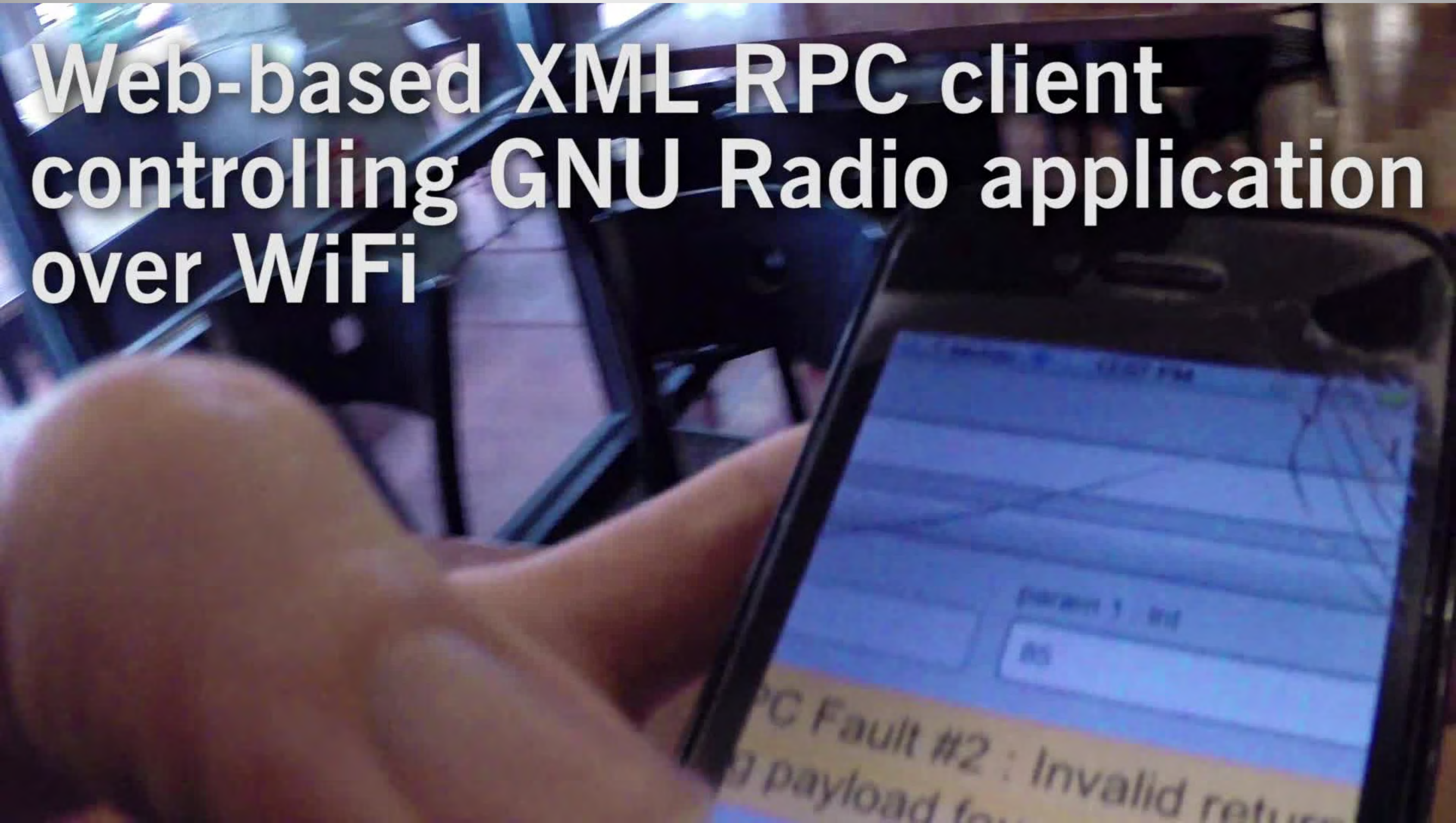
Modulator Output



Modulator

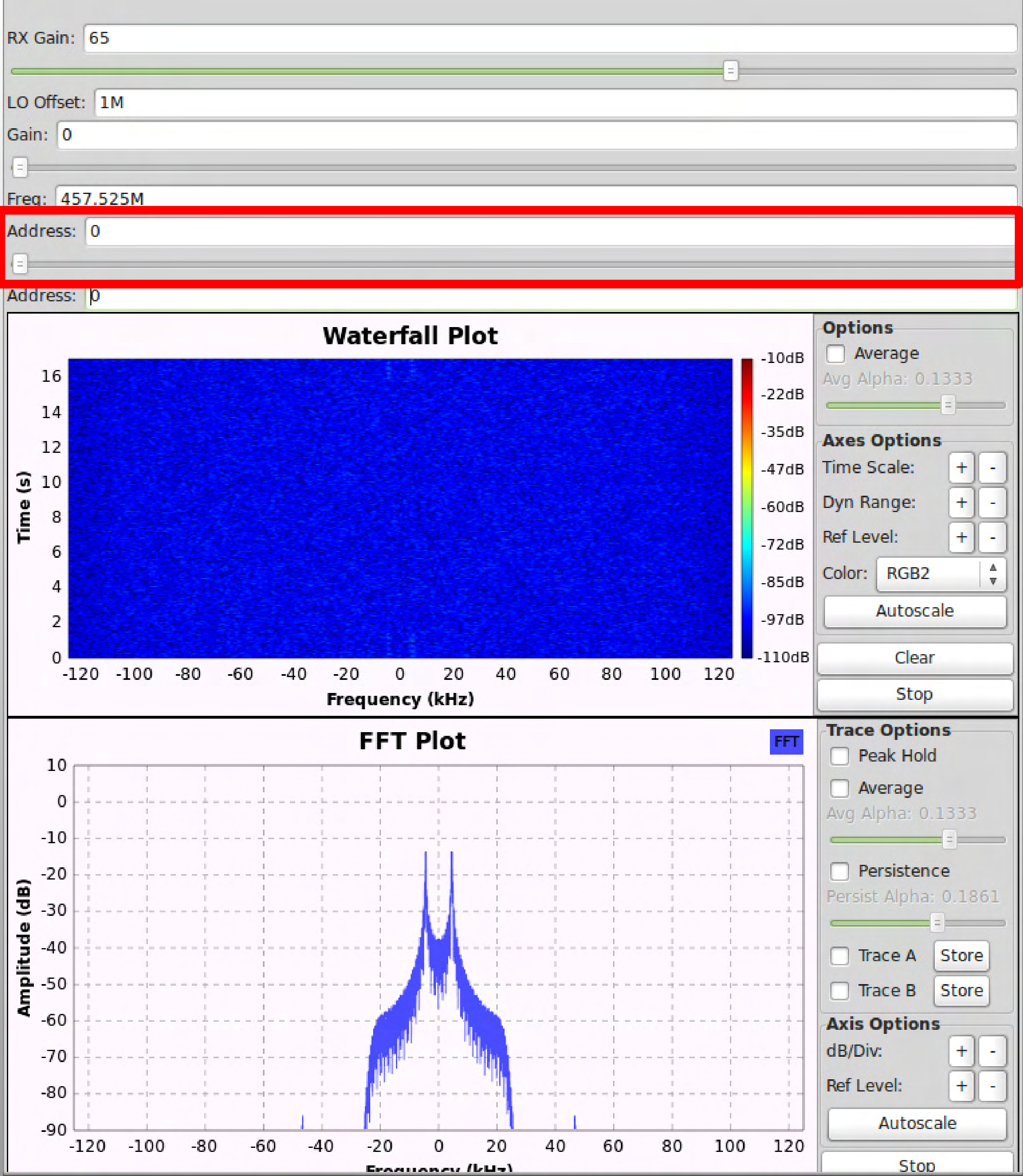

Waterfall Plot
Time (s)
Frequency (kHz)
FFT Plot
Amplitude (dB)
Options
Axis Options
Trace Options
Autoscale
Clear
Stop
You order online.
Business Catering DELIVERY
We deliver on time.
170
VERT900
lenovo

Remote Control



Web-based XML RPC client controlling GNU Radio application over WiFi

Slider



RX Gain: 65

LO Offset: 1M

Gain: 0

Freq: 457.525M

Address: 0

Address: 0

Avg Alpha: 0.1333

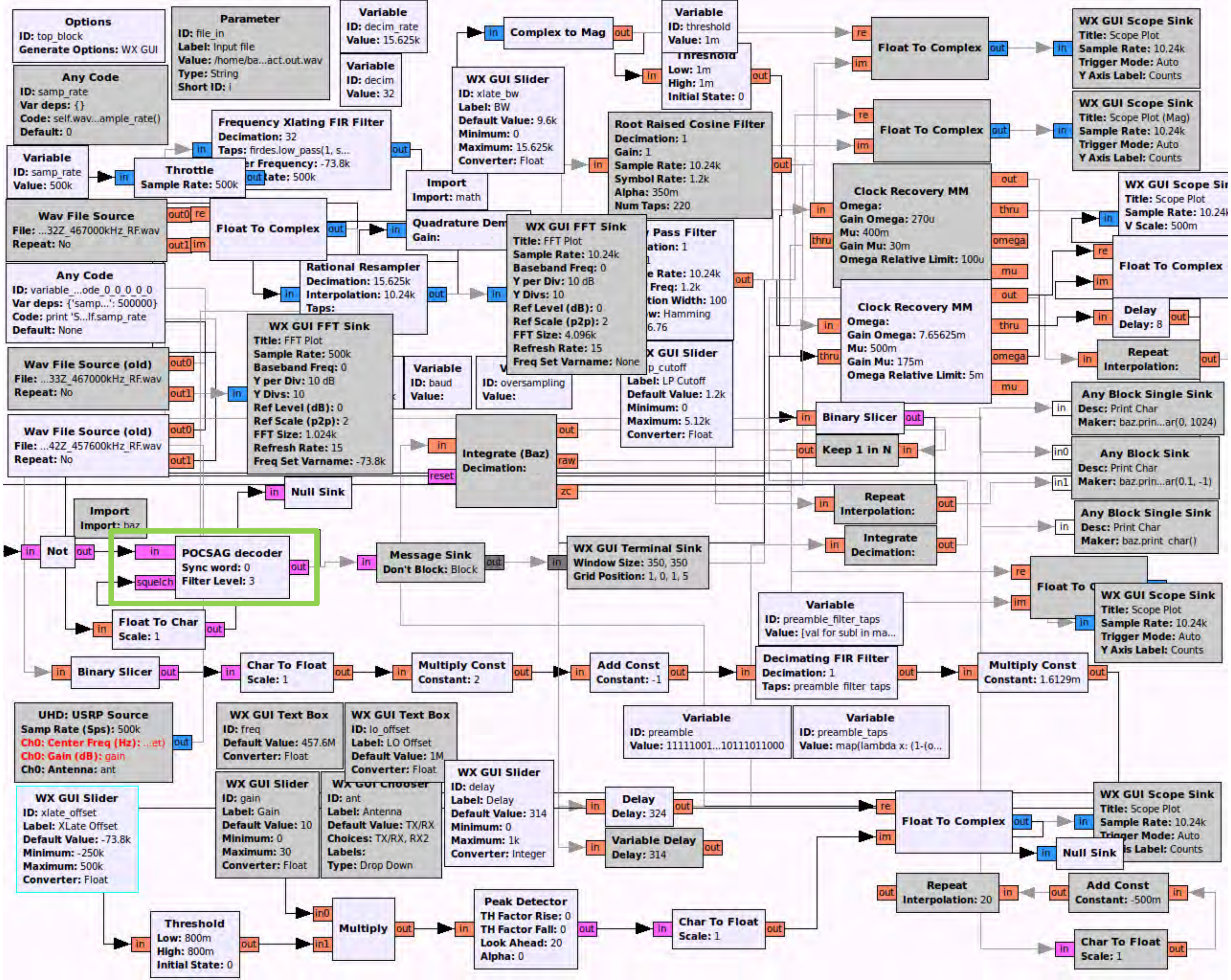
Color: RGB2

Avg Alpha: 0.1333

Persist Alpha: 0.1861

POCSAG

- Other restaurant pager systems adopt a standard
- Decode with gr-pocsag
  - – Modified to end frame decoding when squelch closes



Options
ID: top_block
Generate Options: WX GUI

Parameter
ID: file_in
Label: Input file
Value: /home/ba...act.out.wav
Type: String
Short ID: i

Variable
ID: decim_rate
Value: 15.625k

Variable
ID: decim
Value: 32

Any Code
ID: samp_rate
Var deps: {}
Code: self.wav...ample_rate()
Default: 0

Frequency Xlating FIR Filter
Decimation: 32
Taps: firdes.low_pass(1, s...
...er Frequency: -73.8k
...Rate: 500k

Variable
ID: samp_rate
Value: 500k

Throttle
Sample Rate: 500k

Wav File Source
File: ...32Z_467000kHz_RF.wav
Repeat: No

Float To Complex

Any Code
ID: variable_...ode_0_0_0_0
Var deps: {'samp...': 500000}
Code: print 'S...lf.samp_rate
Default: None

Rational Resampler
Decimation: 15.625k
Interpolation: 10.24k
Taps:

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: -73.8k

Wav File Source (old)
File: ...33Z_467000kHz_RF.wav
Repeat: No

Wav File Source (old)
File: ...42Z_457600kHz_RF.wav
Repeat: No

Complex to Mag

WX GUI Slider
ID: xlate_bw
Label: BW
Default Value: 9.6k
Minimum: 0
Maximum: 15.625k
Converter: Float

Import
Import: math

Quadrature Dem...
Gain:

WX GUI FFT Sink
Title: FFT Plot
Sample Rate: 10.24k
Baseband Freq: 0
Y per Div: 10 dB
Y Divs: 10
Ref Level (dB): 0
Ref Scale (p2p): 2
FFT Size: 4.096k
Refresh Rate: 15
Freq Set Varname: None

Variable
ID: baud
Value:

V...
ID: oversampling
Value:

Variable
ID: threshold
Value: 1m

Threshold
Low: 1m
High: 1m
Initial State: 0

Root Raised Cosine Filter
Decimation: 1
Gain: 1
Sample Rate: 10.24k
Symbol Rate: 1.2k
Alpha: 350m
Num Taps: 220

...Pass Filter
...ation: 1
...1
...e Rate: 10.24k
... Freq: 1.2k
...tion Width: 100
...w: Hamming
...6.76

...X GUI Slider
...p_cutoff
Label: LP Cutoff
Default Value: 1.2k
Minimum: 0
Maximum: 5.12k
Converter: Float

Integrate (Baz)
Decimation:

Null Sink

Float To Complex

Float To Complex

Clock Recovery MM
Omega:
Gain Omega: 270u
Mu: 400m
Gain Mu: 30m
Omega Relative Limit: 100u

Clock Recovery MM
Omega:
Gain Omega: 7.65625m
Mu: 500m
Gain Mu: 175m
Omega Relative Limit: 5m

Binary Slicer

Keep 1 in N

Repeat
Interpolation:

Integrate
Decimation:

WX GUI Scope Sink
Title: Scope Plot
Sample Rate: 10.24k
Trigger Mode: Auto
Y Axis Label: Counts

WX GUI Scope Sink
Title: Scope Plot (Mag)
Sample Rate: 10.24k
Trigger Mode: Auto
Y Axis Label: Counts

WX GUI Scope Si...
Title: Scope Plot
Sample Rate: 10.24k
V Scale: 500m

Float To Complex

Delay
Delay: 8

Repeat
Interpolation:

Any Block Single Sink
Desc: Print Char
Maker: baz.prin...ar(0, 1024)

Any Block Sink
Desc: Print Char
Maker: baz.prin...ar(0.1, -1)

Any Block Single Sink
Desc: Print Char
Maker: baz.print_char()

Import
Import: baz

Not

POCSAG decoder
Sync word: 0
Filter Level: 3

Message Sink
Don't Block: Block

WX GUI Terminal Sink
Window Size: 350, 350
Grid Position: 1, 0, 1, 5

Float To C...

WX GUI Scope Sink
Title: Scope Plot
Sample Rate: 10.24k
Trigger Mode: Auto
Y Axis Label: Counts

Variable
ID: preamble_filter_taps
Value: [val for subl in ma...

Float To Char
Scale: 1

Binary Slicer

Char To Float
Scale: 1

Multiply Const
Constant: 2

Add Const
Constant: -1

Decimating FIR Filter
Decimation: 1
Taps: preamble_filter_taps

Multiply Const
Constant: 1.6129m

UHD: USRP Source
Samp Rate (Sps): 500k
Ch0: Center Freq (Hz): ...et)
Ch0: Gain (dB): gain
Ch0: Antenna: ant

WX GUI Text Box
ID: freq
Default Value: 457.6M
Converter: Float

WX GUI Text Box
ID: lo_offset
Label: LO Offset
Default Value: 1M
Converter: Float

Variable
ID: preamble
Value: 11111001...10111011000

Variable
ID: preamble_taps
Value: map(lambda x: (1-(o...

WX GUI Slider
ID: xlate_offset
Label: XLate Offset
Default Value: -73.8k
Minimum: -250k
Maximum: 500k
Converter: Float

WX GUI Slider
ID: gain
Label: Gain
Default Value: 10
Minimum: 0
Maximum: 30
Converter: Float

WX GUI Chooser
ID: ant
Label: Antenna
Default Value: TX/RX
Choices: TX/RX, RX2
Labels:
Type: Drop Down

WX GUI Slider
ID: delay
Label: Delay
Default Value: 314
Minimum: 0
Maximum: 1k
Converter: Integer

Delay
Delay: 324

Variable Delay
Delay: 314

Float To Complex

WX GUI Scope Sink
Title: Scope Plot
Sample Rate: 10.24k
Trigger Mode: Auto
...is Label: Counts

Null Sink

Repeat
Interpolation: 20

Add Const
Constant: -500m

Threshold
Low: 800m
High: 800m
Initial State: 0

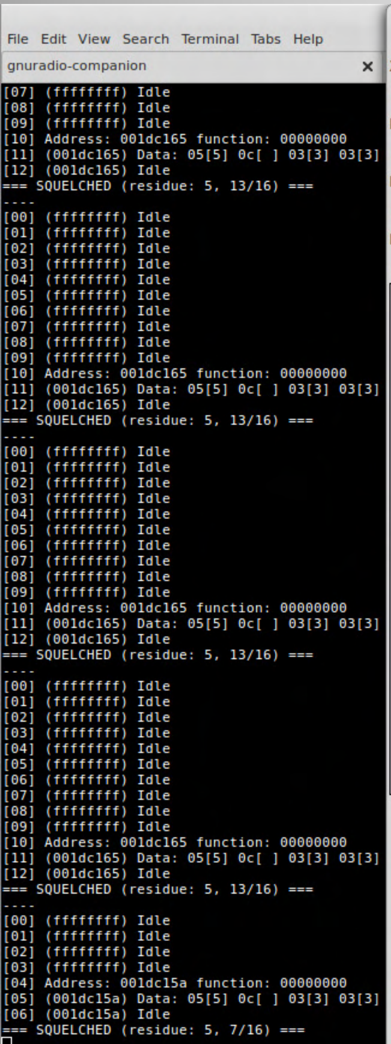
Multiply

Peak Detector
TH Factor Rise: 0
TH Factor Fall: 0
Look Ahead: 20
Alpha: 0

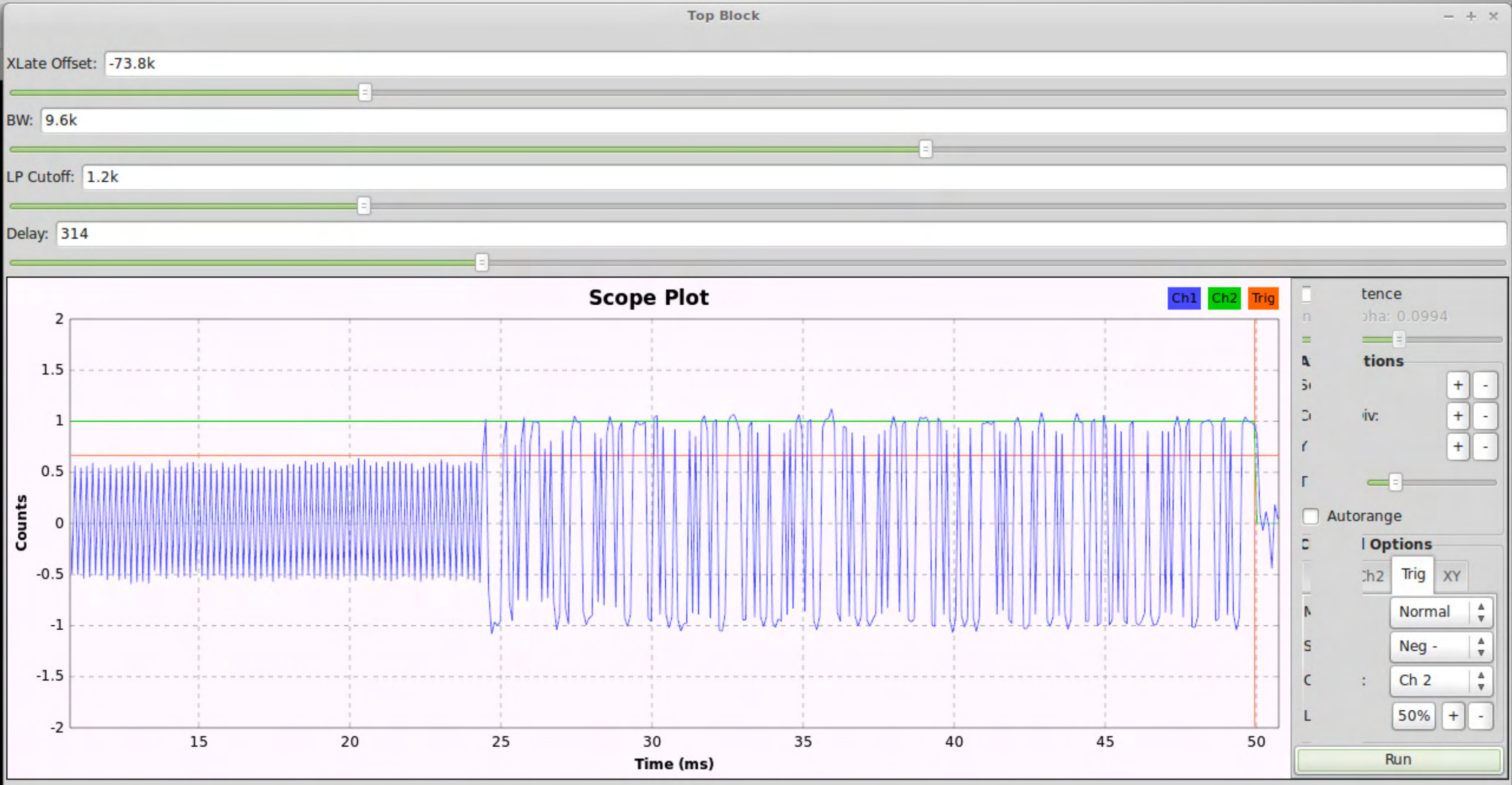
Char To Float
Scale: 1

Char To Float
Scale: 1

POCSAG Decode



```
[07] (ffffffff) Idle
[08] (ffffffff) Idle
[09] (ffffffff) Idle
[10] Address: 001dc165 function: 00000000
[11] (001dc165) Data: 05[5] 0c[ ] 03[3] 03[3]
[12] (001dc165) Idle
=== SQUELCHED (residue: 5, 13/16) ===
----
[00] (ffffffff) Idle
[01] (ffffffff) Idle
[02] (ffffffff) Idle
[03] (ffffffff) Idle
[04] (ffffffff) Idle
[05] (ffffffff) Idle
[06] (ffffffff) Idle
[07] (ffffffff) Idle
[08] (ffffffff) Idle
[09] (ffffffff) Idle
[10] Address: 001dc165 function: 00000000
[11] (001dc165) Data: 05[5] 0c[ ] 03[3] 03[3]
[12] (001dc165) Idle
=== SQUELCHED (residue: 5, 13/16) ===
----
[00] (ffffffff) Idle
[01] (ffffffff) Idle
[02] (ffffffff) Idle
[03] (ffffffff) Idle
[04] (ffffffff) Idle
[05] (ffffffff) Idle
[06] (ffffffff) Idle
[07] (ffffffff) Idle
[08] (ffffffff) Idle
[09] (ffffffff) Idle
[10] Address: 001dc165 function: 00000000
[11] (001dc165) Data: 05[5] 0c[ ] 03[3] 03[3]
[12] (001dc165) Idle
=== SQUELCHED (residue: 5, 13/16) ===
----
[00] (ffffffff) Idle
[01] (ffffffff) Idle
[02] (ffffffff) Idle
[03] (ffffffff) Idle
[04] (ffffffff) Idle
[05] (ffffffff) Idle
[06] (ffffffff) Idle
[07] (ffffffff) Idle
[08] (ffffffff) Idle
[09] (ffffffff) Idle
[10] Address: 001dc165 function: 00000000
[11] (001dc165) Data: 05[5] 0c[ ] 03[3] 03[3]
[12] (001dc165) Idle
=== SQUELCHED (residue: 5, 13/16) ===
----
[00] (ffffffff) Idle
[01] (ffffffff) Idle
[02] (ffffffff) Idle
[03] (ffffffff) Idle
[04] Address: 001dc15a function: 00000000
[05] (001dc15a) Data: 05[5] 0c[ ] 03[3] 03[3]
[06] (001dc15a) Idle
=== SQUELCHED (residue: 5, 7/16) ===
```



XLate Offset: -73.8k

BW: 9.6k

LP Cutoff: 1.2k

Delay: 314

POCSAG Frames

```
----
[00] Address: 001dc168 function: 00000000
[01] (001dc168) Data: 05[5] 0c[ ] 03[3] 03[3] 03[3]
[02] (001dc168) Idle
=== SQUELCHED (residue: 5) ===
----
[00] (ffffffff) Idle
[01] (ffffffff) Idle
[02] (ffffffff) Idle
[03] (ffffffff) Idle
[04] (ffffffff) Idle
[05] (ffffffff) Idle
[06] Address: 001dc15b function: 00000000
[07] (001dc15b) Data: 05[5] 0c[ ] 03[3] 03[3] 03[3]
[08] (001dc15b) Idle
=== SQUELCHED (residue: 5) ===
----
[00] (ffffffff) Idle
[01] (ffffffff) Idle
[02] (ffffffff) Idle
[03] (ffffffff) Idle
[04] (ffffffff) Idle
[05] (ffffffff) Idle
[06] Address: 001dc15b function: 00000000
[07] (001dc15b) Data: 05[5] 0c[ ] 03[3] 03[3] 03[3]
[08] (001dc15b) Idle
=== SQUELCHED (residue: 5) ===
```

POCSAG Frame

```
----
[00] (ffffffff) Idle
[01] (ffffffff) Idle
[02] (ffffffff) Idle
[03] (ffffffff) Idle
[04] (ffffffff) Idle
[05] (ffffffff) Idle
[06] Address: 001dc15b function: 00000000
[07] (001dc15b) Data: 05[5] 0c[ ] 03[3] 03[3] 03[3]
[08] (001dc15b) Idle
=== SQUELCHED (residue: 5) ===
```

5b = 01011011

Pager Frame Construction

- Preamble
- SYNC
- Address: System & Pager
  - Schedule address to appear in correct slot
  - Pad with IDLEs beforehand
- Pager action
- Trailing IDLE
- Apply BCH(31,21) ECC to each slot

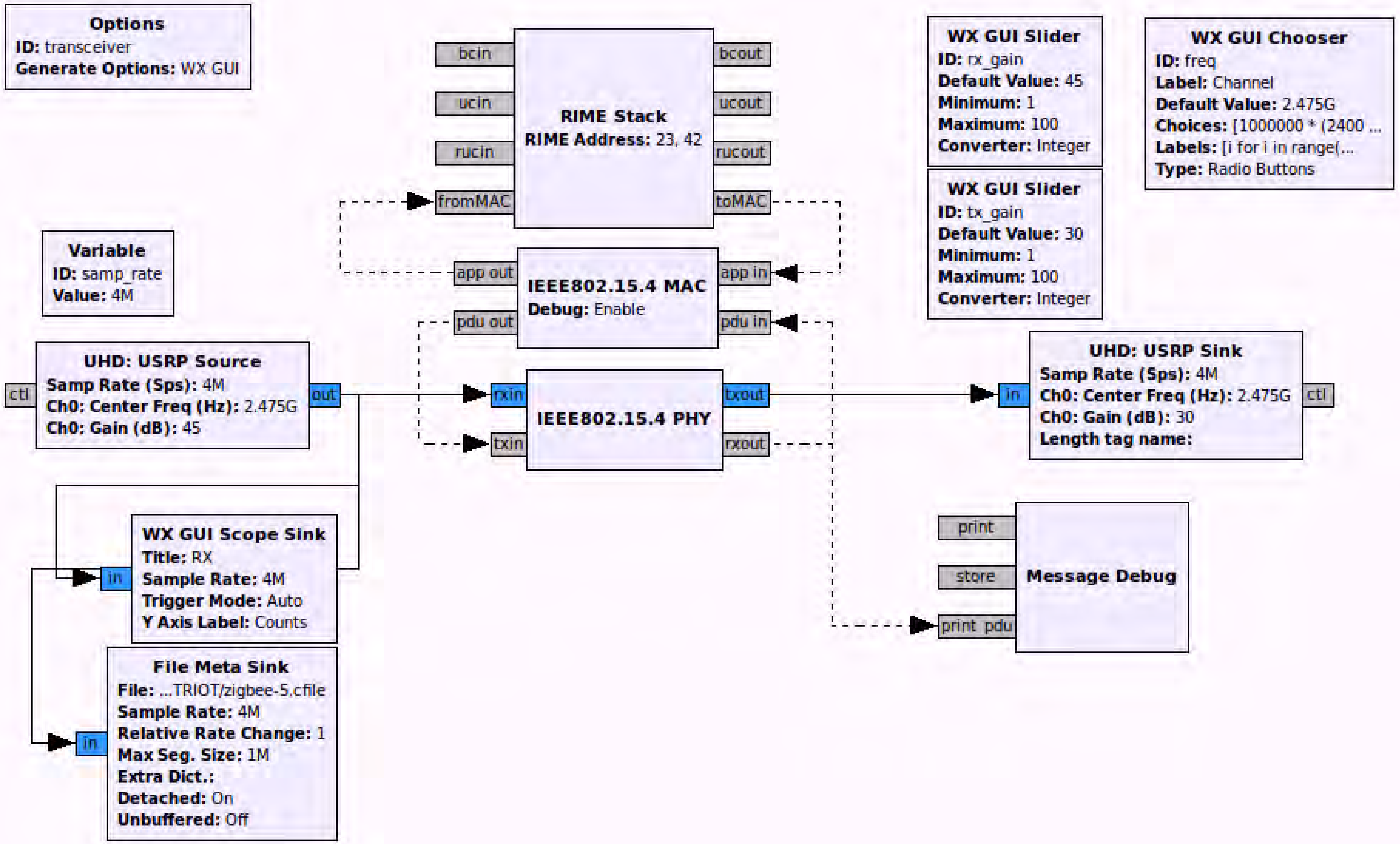
POCASG Modulator

ZigBee

- Roles reversed: pager unit transmits
- Pager unit has integrated RFID reader
- RFID chip stuck on underside of each table
- Placing pager unit on table transmits **pager** number and **table** number
- 2.4 GHz ISM band
- Decode with gr-ieee802-15-4

FCC ID: M746863 This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference and (2) this device must accept any interference received, including interference that may cause undesired operation.

ZigBee Transceiver



Options
ID: transceiver
Generate Options: WX GUI

Variable
ID: samp_rate
Value: 4M

UHD: USRP Source
Samp Rate (Sps): 4M
Ch0: Center Freq (Hz): 2.475G
Ch0: Gain (dB): 45

WX GUI Scope Sink
Title: RX
Sample Rate: 4M
Trigger Mode: Auto
Y Axis Label: Counts

File Meta Sink
File: ...TRIOT/zigbee-5.cfile
Sample Rate: 4M
Relative Rate Change: 1
Max Seg. Size: 1M
Extra Dict.:
Detached: On
Unbuffered: Off

RIME Stack
RIME Address: 23, 42

IEEE802.15.4 MAC
Debug: Enable

IEEE802.15.4 PHY

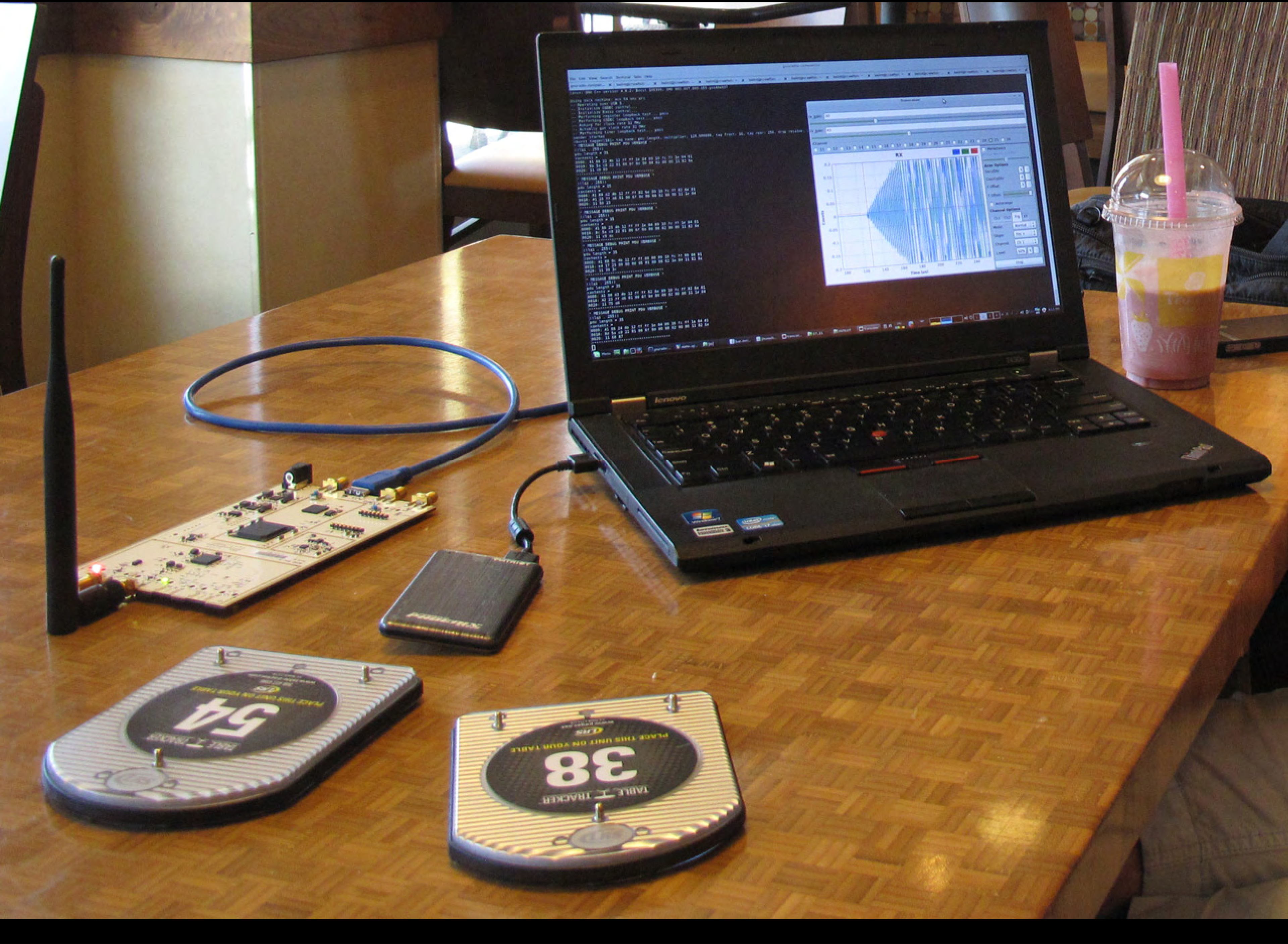
WX GUI Slider
ID: rx_gain
Default Value: 45
Minimum: 1
Maximum: 100
Converter: Integer

WX GUI Slider
ID: tx_gain
Default Value: 30
Minimum: 1
Maximum: 100
Converter: Integer

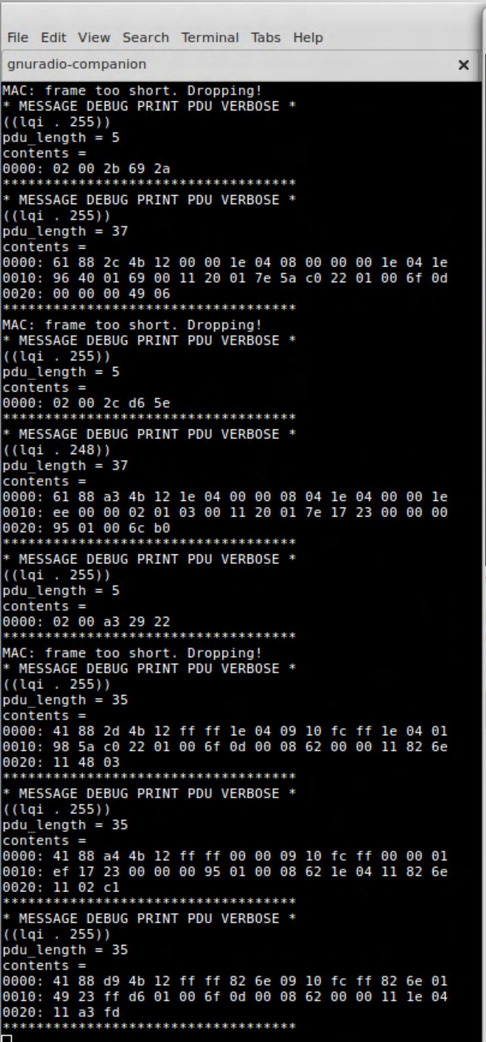
WX GUI Chooser
ID: freq
Label: Channel
Default Value: 2.475G
Choices: [1000000 * (2400 ...
Labels: [i for i in range(...
Type: Radio Buttons

UHD: USRP Sink
Samp Rate (Sps): 4M
Ch0: Center Freq (Hz): 2.475G
Ch0: Gain (dB): 30
Length tag name:

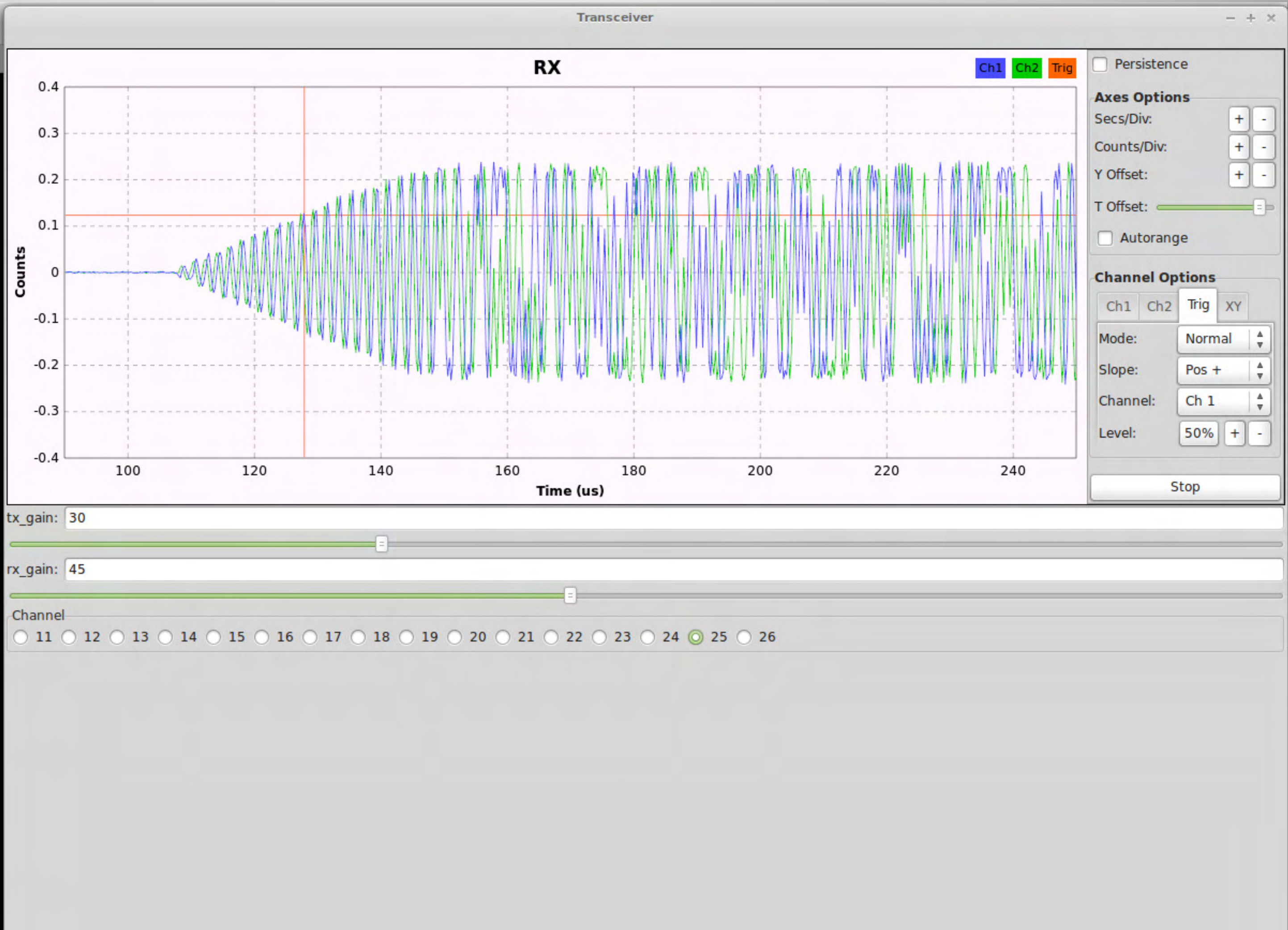
Message Debug


lenovo
ThinkPad
54
PLACE THIS UNIT ON YOUR TABLE
TABLE TRACKER
38
PLACE THIS UNIT ON YOUR TABLE
TABLE TRACKER

Decoded ZigBee



```
MAC: frame too short. Dropping!
* MESSAGE DEBUG PRINT PDU VERBOSE *
((lqi . 255))
pdu_length = 5
contents =
0000: 02 00 2b 69 2a
***********************************
* MESSAGE DEBUG PRINT PDU VERBOSE *
((lqi . 255))
pdu_length = 37
contents =
0000: 61 88 2c 4b 12 00 00 1e 04 08 00 00 00 1e 04 1e
0010: 96 40 01 69 00 11 20 01 7e 5a c0 22 01 00 6f 0d
0020: 00 00 00 49 06
***********************************
MAC: frame too short. Dropping!
* MESSAGE DEBUG PRINT PDU VERBOSE *
((lqi . 255))
pdu_length = 5
contents =
0000: 02 00 2c d6 5e
***********************************
* MESSAGE DEBUG PRINT PDU VERBOSE *
((lqi . 248))
pdu_length = 37
contents =
0000: 61 88 a3 4b 12 1e 04 00 00 08 04 1e 04 00 00 1e
0010: ee 00 00 02 01 03 00 11 20 01 7e 17 23 00 00 00
0020: 95 01 00 6c b0
***********************************
* MESSAGE DEBUG PRINT PDU VERBOSE *
((lqi . 255))
pdu_length = 5
contents =
0000: 02 00 a3 29 22
***********************************
MAC: frame too short. Dropping!
* MESSAGE DEBUG PRINT PDU VERBOSE *
((lqi . 255))
pdu_length = 35
contents =
0000: 41 88 2d 4b 12 ff ff 1e 04 09 10 fc ff 1e 04 01
0010: 98 5a c0 22 01 00 6f 0d 00 08 62 00 00 11 82 6e
0020: 11 48 03
***********************************
* MESSAGE DEBUG PRINT PDU VERBOSE *
((lqi . 255))
pdu_length = 35
contents =
0000: 41 88 a4 4b 12 ff ff 00 00 09 10 fc ff 00 00 01
0010: ef 17 23 00 00 00 95 01 00 08 62 1e 04 11 82 6e
0020: 11 02 c1
***********************************
* MESSAGE DEBUG PRINT PDU VERBOSE *
((lqi . 255))
pdu_length = 35
contents =
0000: 41 88 d9 4b 12 ff ff 82 6e 09 10 fc ff 82 6e 01
0010: 49 23 ff d6 01 00 6f 0d 00 08 62 00 00 11 1e 04
0020: 11 a3 fd
***********************************
```



□ Persistence

Secs/Div: + -

Counts/Div: + -

Y Offset: + -

T Offset:

□ Autorange

Mode: Normal

Slope: Pos +

Channel: Ch 1

Level: 50% + -

tx_gain: 30

rx_gain: 45

Channel

○ 11 ○ 12 ○ 13 ○ 14 ○ 15 ○ 16 ○ 17 ○ 18 ○ 19 ○ 20 ○ 21 ○ 22 ○ 23 ○ 24 ● 25 ○ 26

Decoded Pager

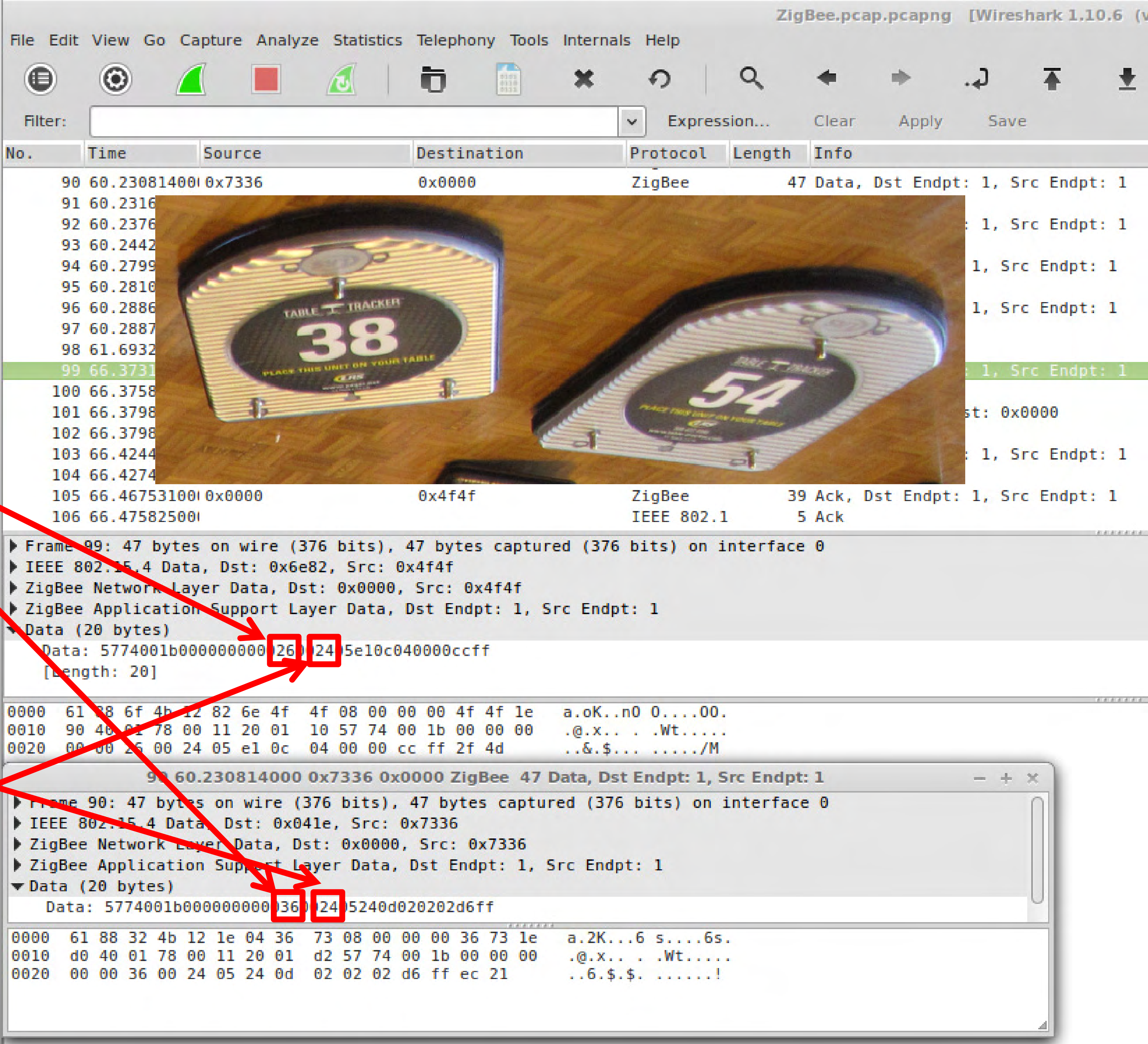
Pagers:

38 = 0x26

54 = 0x36

Table:

36 = 0x24


ZigBee.pcap.pcapng [Wireshark 1.10.6 (v
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save
TABLE TRACKER
38
PLACE THIS UNIT ON YOUR TABLE
54

```
No.   Time           Source    Destination  Protocol     Length Info
   90 60.23081400( 0x7336      0x0000       ZigBee           47 Data, Dst Endpt: 1, Src Endpt: 1
   91 60.2316                                                   : 1, Src Endpt: 1
   92 60.2376
   93 60.2442                                                   1, Src Endpt: 1
   94 60.2799
   95 60.2810                                                   1, Src Endpt: 1
   96 60.2886
   97 60.2887
   98 61.6932
   99 66.3731                                                   : 1, Src Endpt: 1
  100 66.3758                                                   st: 0x0000
  101 66.3798
  102 66.3798                                                   : 1, Src Endpt: 1
  103 66.4244
  104 66.4274
  105 66.46753100( 0x0000     0x4f4f       ZigBee           39 Ack, Dst Endpt: 1, Src Endpt: 1
  106 66.47582500(                          IEEE 802.1        5 Ack
```

```
▶ Frame 99: 47 bytes on wire (376 bits), 47 bytes captured (376 bits) on interface 0
▶ IEEE 802.15.4 Data, Dst: 0x6e82, Src: 0x4f4f
▶ ZigBee Network Layer Data, Dst: 0x0000, Src: 0x4f4f
▶ ZigBee Application Support Layer Data, Dst Endpt: 1, Src Endpt: 1
▼ Data (20 bytes)
    Data: 5774001b000000000026002405e10c040000ccff
    [Length: 20]

0000  61 88 6f 4b 12 82 6e 4f  4f 08 00 00 00 4f 4f 1e   a.oK..nO O....OO.
0010  90 40 01 78 00 11 20 01  10 57 74 00 1b 00 00 00   .@.x.. . .Wt.....
0020  00 00 26 00 24 05 e1 0c  04 00 00 cc ff 2f 4d      ..&.$... ...../M
```

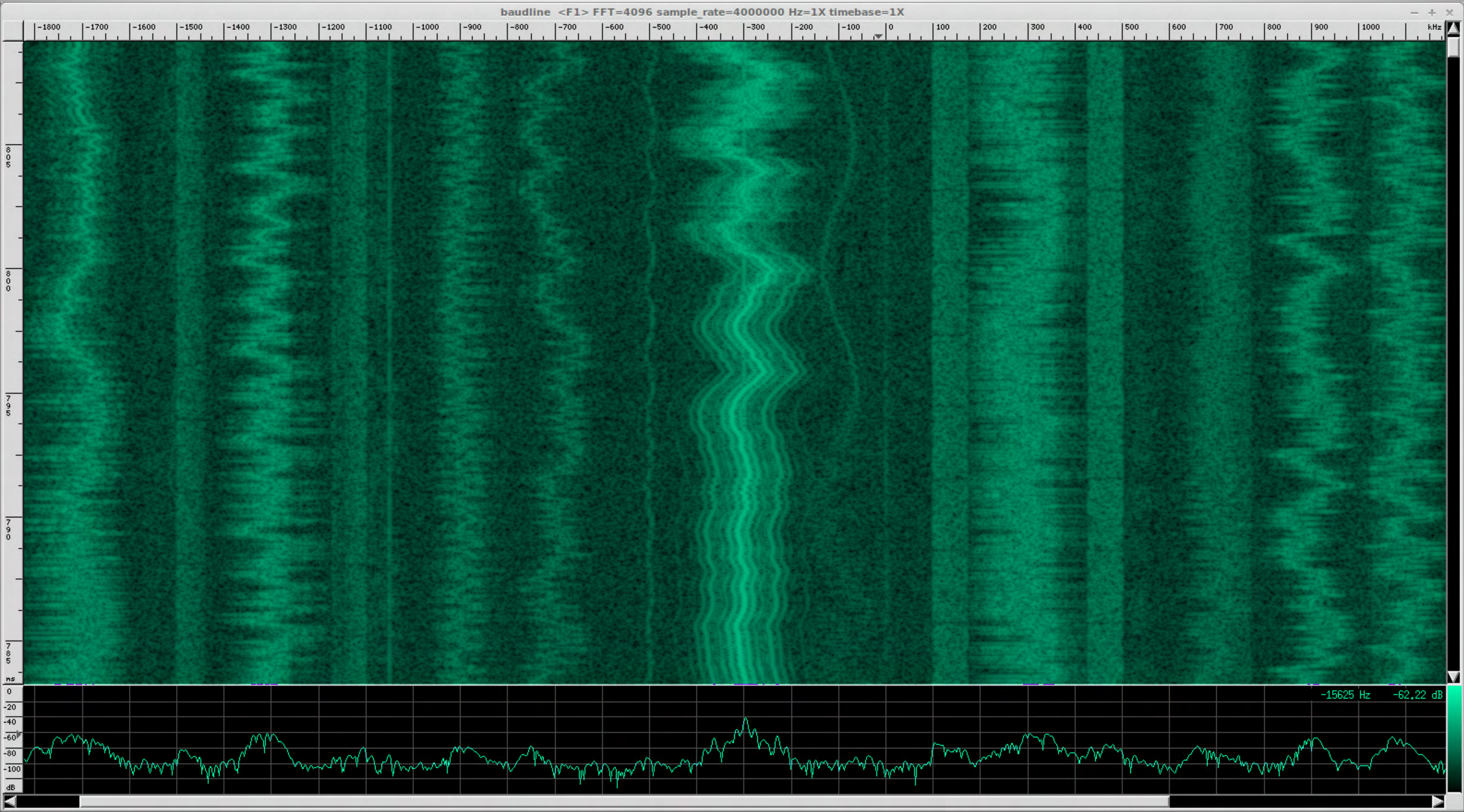
```
90 60.230814000 0x7336 0x0000 ZigBee  47 Data, Dst Endpt: 1, Src Endpt: 1
▶ Frame 90: 47 bytes on wire (376 bits), 47 bytes captured (376 bits) on interface 0
▶ IEEE 802.15.4 Data, Dst: 0x041e, Src: 0x7336
▶ ZigBee Network Layer Data, Dst: 0x0000, Src: 0x7336
▶ ZigBee Application Support Layer Data, Dst Endpt: 1, Src Endpt: 1
▼ Data (20 bytes)
    Data: 5774001b000000000036002405240d020202d6ff

0000  61 88 32 4b 12 1e 04 36  73 08 00 00 00 36 73 1e   a.2K...6 s....6s.
0010  d0 40 01 78 00 11 20 01  d2 57 74 00 1b 00 00 00   .@.x.. . .Wt.....
0020  00 00 36 00 24 05 24 0d  02 02 02 d6 ff ec 21      ..6.$.$. ......!
```

Hostage Pager

- Pagers get angry when system broadcast (beacon) is not heard within timeout
  - Flash & vibrate until they are returned within range
- Take a pager hostage by broadcasting beacon

RDS TMC

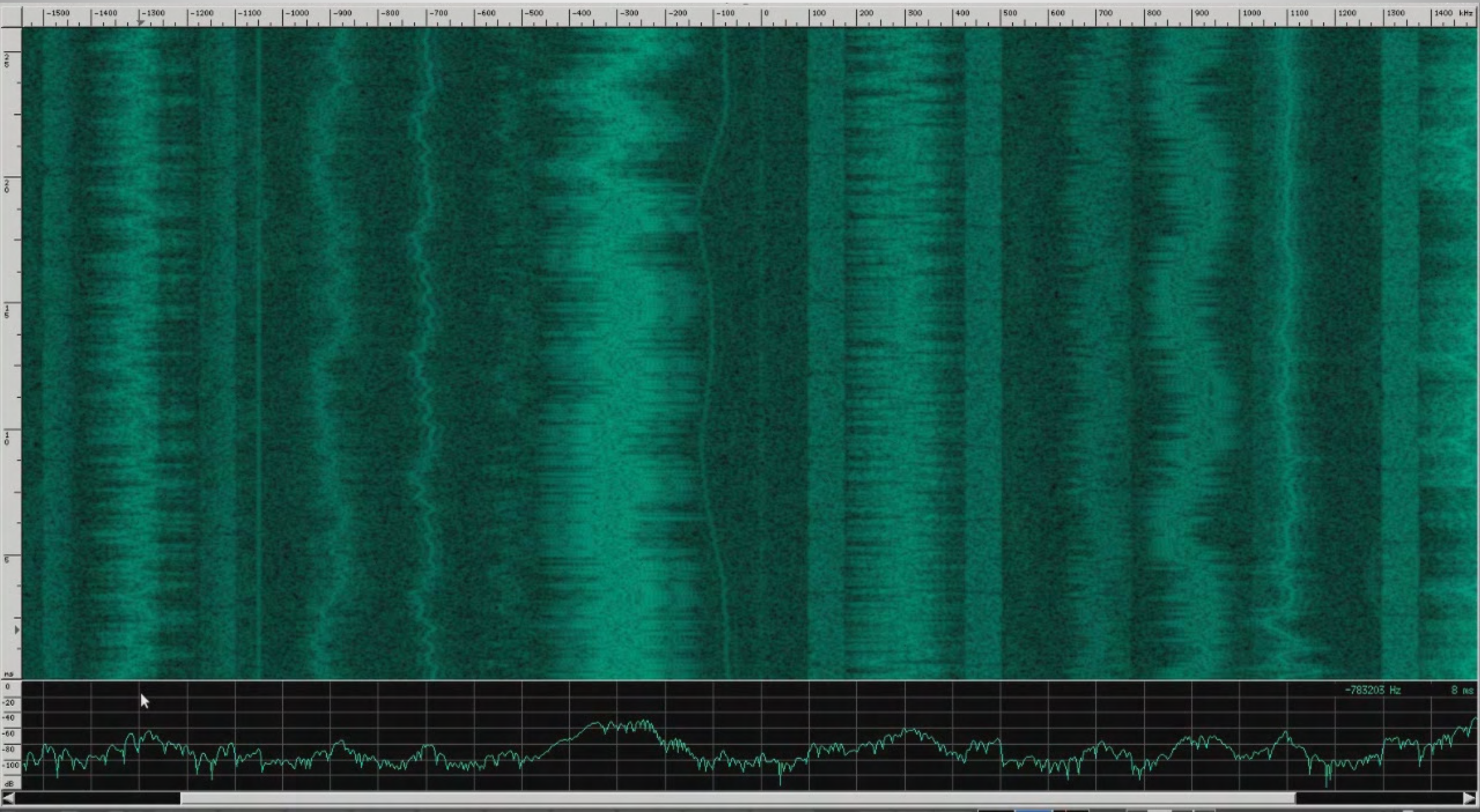
FM Broadcast Band

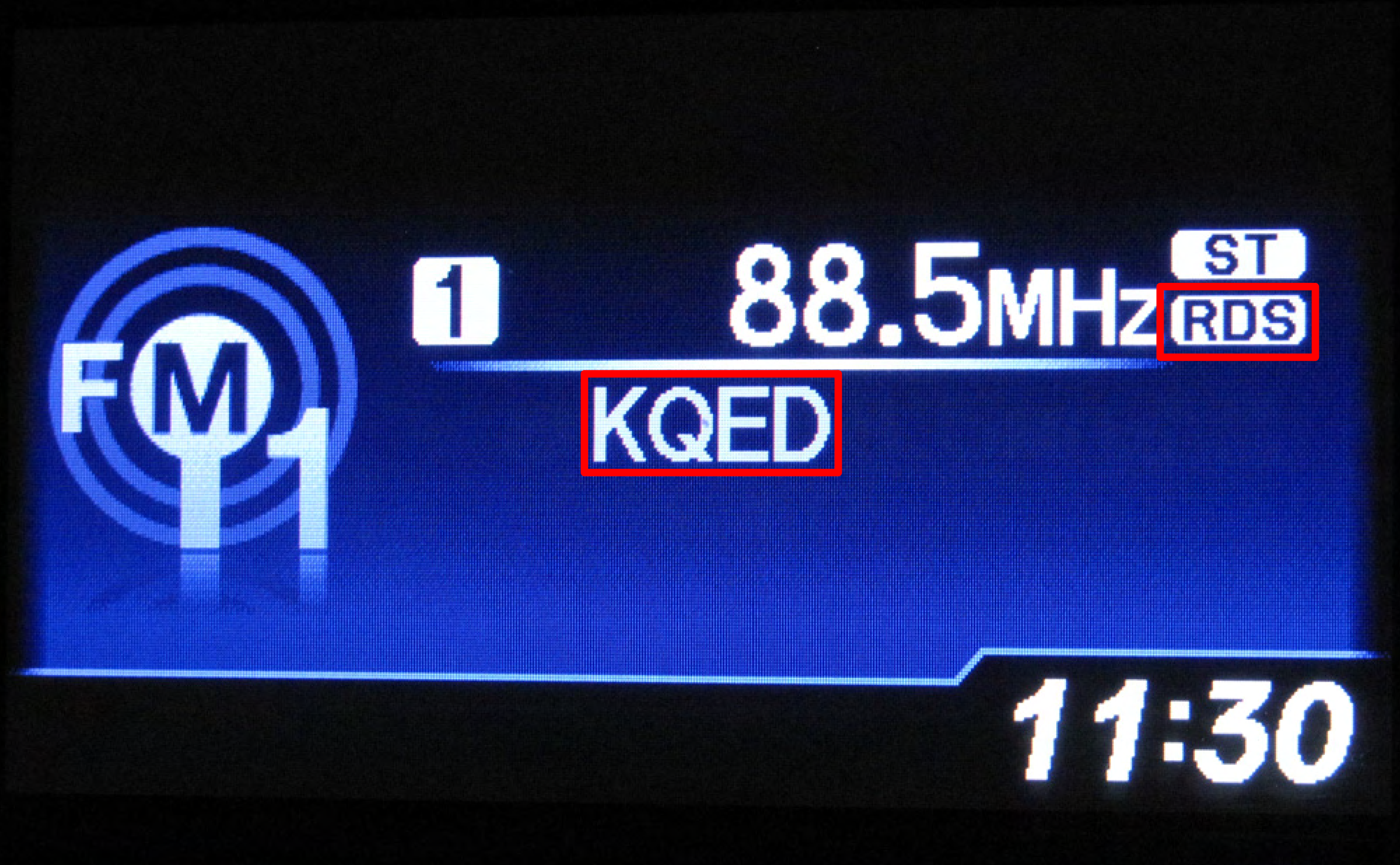


baudline <F1> FFT=4096 sample_rate=4000000 Hz=1X timebase=1X

-15625 Hz -62.22 dB

FM Broadcast Band



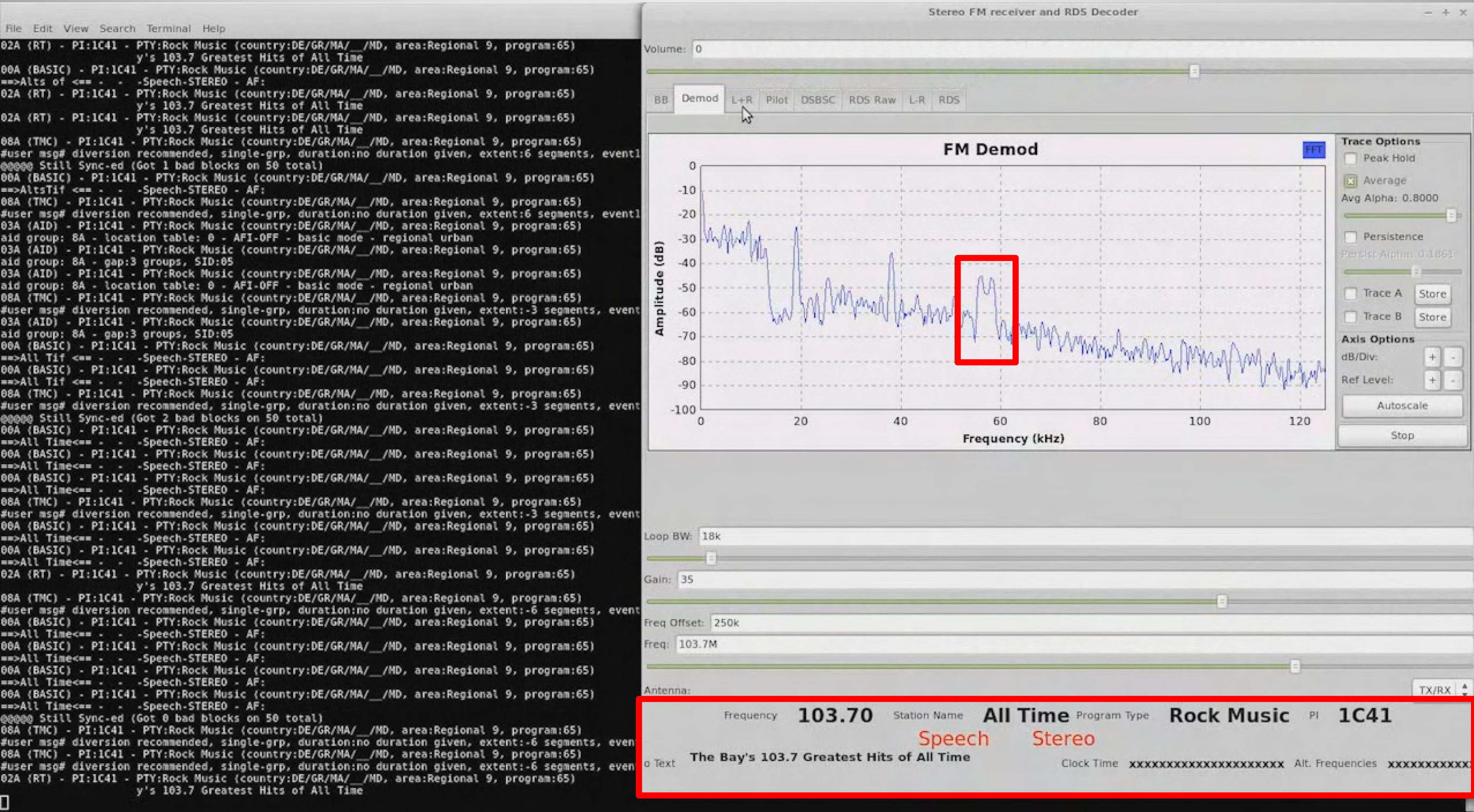

FM 1
1
88.5MHz
ST
RDS
KQED
11:30

Radio Data Service

- Subcarrier on commercial FM stations
- Not audible (filtered out)
- BPSK @ 1187.5 bps
- Listen & decode with gr-rds

Stereo FM with RDS: Receiver

Radio Data Service



```
02A (RT) - PI:1C41 - PTY:Rock Music (country:DE/GR/MA/__/MD, area:Regional 9, program:65)
                     y's 103.7 Greatest Hits of All Time
00A (BASIC) - PI:1C41 - PTY:Rock Music (country:DE/GR/MA/__/MD, area:Regional 9, program:65)
==>Alts of <== -  -  -Speech-STEREO - AF:
02A (RT) - PI:1C41 - PTY:Rock Music (country:DE/GR/MA/__/MD, area:Regional 9, program:65)
                     y's 103.7 Greatest Hits of All Time
02A (RT) - PI:1C41 - PTY:Rock Music (country:DE/GR/MA/__/MD, area:Regional 9, program:65)
                     y's 103.7 Greatest Hits of All Time
08A (TMC) - PI:1C41 - PTY:Rock Music (country:DE/GR/MA/__/MD, area:Regional 9, program:65)
#user msg# diversion recommended, single-grp, duration:no duration given, extent:6 segments, eventl
@@@@@ Still Sync-ed (Got 1 bad blocks on 50 total)
00A (BASIC) - PI:1C41 - PTY:Rock Music (country:DE/GR/MA/__/MD, area:Regional 9, program:65)
==>AltsTif <== -  -  -Speech-STEREO - AF:
08A (TMC) - PI:1C41 - PTY:Rock Music (country:DE/GR/MA/__/MD, area:Regional 9, program:65)
#user msg# diversion recommended, single-grp, duration:no duration given, extent:6 segments, eventl
03A (AID) - PI:1C41 - PTY:Rock Music (country:DE/GR/MA/__/MD, area:Regional 9, program:65)
aid group: 8A - location table: 0 - AFI-OFF - basic mode - regional urban
03A (AID) - PI:1C41 - PTY:Rock Music (country:DE/GR/MA/__/MD, area:Regional 9, program:65)
aid group: 8A - gap:3 groups, SID:05
03A (AID) - PI:1C41 - PTY:Rock Music (country:DE/GR/MA/__/MD, area:Regional 9, program:65)
aid group: 8A - location table: 0 - AFI-OFF - basic mode - regional urban
08A (TMC) - PI:1C41 - PTY:Rock Music (country:DE/GR/MA/__/MD, area:Regional 9, program:65)
#user msg# diversion recommended, single-grp, duration:no duration given, extent:-3 segments, event
03A (AID) - PI:1C41 - PTY:Rock Music (country:DE/GR/MA/__/MD, area:Regional 9, program:65)
aid group: 8A - gap:3 groups, SID:05
00A (BASIC) - PI:1C41 - PTY:Rock Music (country:DE/GR/MA/__/MD, area:Regional 9, program:65)
==>All Tif <== -  -  -Speech-STEREO - AF:
00A (BASIC) - PI:1C41 - PTY:Rock Music (country:DE/GR/MA/__/MD, area:Regional 9, program:65)
==>All Tif <== -  -  -Speech-STEREO - AF:
08A (TMC) - PI:1C41 - PTY:Rock Music (country:DE/GR/MA/__/MD, area:Regional 9, program:65)
#user msg# diversion recommended, single-grp, duration:no duration given, extent:-3 segments, event
@@@@@ Still Sync-ed (Got 2 bad blocks on 50 total)
00A (BASIC) - PI:1C41 - PTY:Rock Music (country:DE/GR/MA/__/MD, area:Regional 9, program:65)
==>All Time<== -  -  -Speech-STEREO - AF:
00A (BASIC) - PI:1C41 - PTY:Rock Music (country:DE/GR/MA/__/MD, area:Regional 9, program:65)
==>All Time<== -  -  -Speech-STEREO - AF:
00A (BASIC) - PI:1C41 - PTY:Rock Music (country:DE/GR/MA/__/MD, area:Regional 9, program:65)
==>All Time<== -  -  -Speech-STEREO - AF:
08A (TMC) - PI:1C41 - PTY:Rock Music (country:DE/GR/MA/__/MD, area:Regional 9, program:65)
#user msg# diversion recommended, single-grp, duration:no duration given, extent:-3 segments, event
00A (BASIC) - PI:1C41 - PTY:Rock Music (country:DE/GR/MA/__/MD, area:Regional 9, program:65)
==>All Time<== -  -  -Speech-STEREO - AF:
00A (BASIC) - PI:1C41 - PTY:Rock Music (country:DE/GR/MA/__/MD, area:Regional 9, program:65)
==>All Time<== -  -  -Speech-STEREO - AF:
02A (RT) - PI:1C41 - PTY:Rock Music (country:DE/GR/MA/__/MD, area:Regional 9, program:65)
                     y's 103.7 Greatest Hits of All Time
08A (TMC) - PI:1C41 - PTY:Rock Music (country:DE/GR/MA/__/MD, area:Regional 9, program:65)
#user msg# diversion recommended, single-grp, duration:no duration given, extent:-6 segments, event
00A (BASIC) - PI:1C41 - PTY:Rock Music (country:DE/GR/MA/__/MD, area:Regional 9, program:65)
==>All Time<== -  -  -Speech-STEREO - AF:
00A (BASIC) - PI:1C41 - PTY:Rock Music (country:DE/GR/MA/__/MD, area:Regional 9, program:65)
==>All Time<== -  -  -Speech-STEREO - AF:
00A (BASIC) - PI:1C41 - PTY:Rock Music (country:DE/GR/MA/__/MD, area:Regional 9, program:65)
==>All Time<== -  -  -Speech-STEREO - AF:
@@@@@ Still Sync-ed (Got 0 bad blocks on 50 total)
08A (TMC) - PI:1C41 - PTY:Rock Music (country:DE/GR/MA/__/MD, area:Regional 9, program:65)
#user msg# diversion recommended, single-grp, duration:no duration given, extent:-6 segments, even
08A (TMC) - PI:1C41 - PTY:Rock Music (country:DE/GR/MA/__/MD, area:Regional 9, program:65)
#user msg# diversion recommended, single-grp, duration:no duration given, extent:-6 segments, even
02A (RT) - PI:1C41 - PTY:Rock Music (country:DE/GR/MA/__/MD, area:Regional 9, program:65)
                     y's 103.7 Greatest Hits of All Time
```

Stereo FM receiver and RDS Decoder

Volume: 0

Loop BW: 18k

Gain: 35

Freq Offset: 250k

Freq: 103.7M

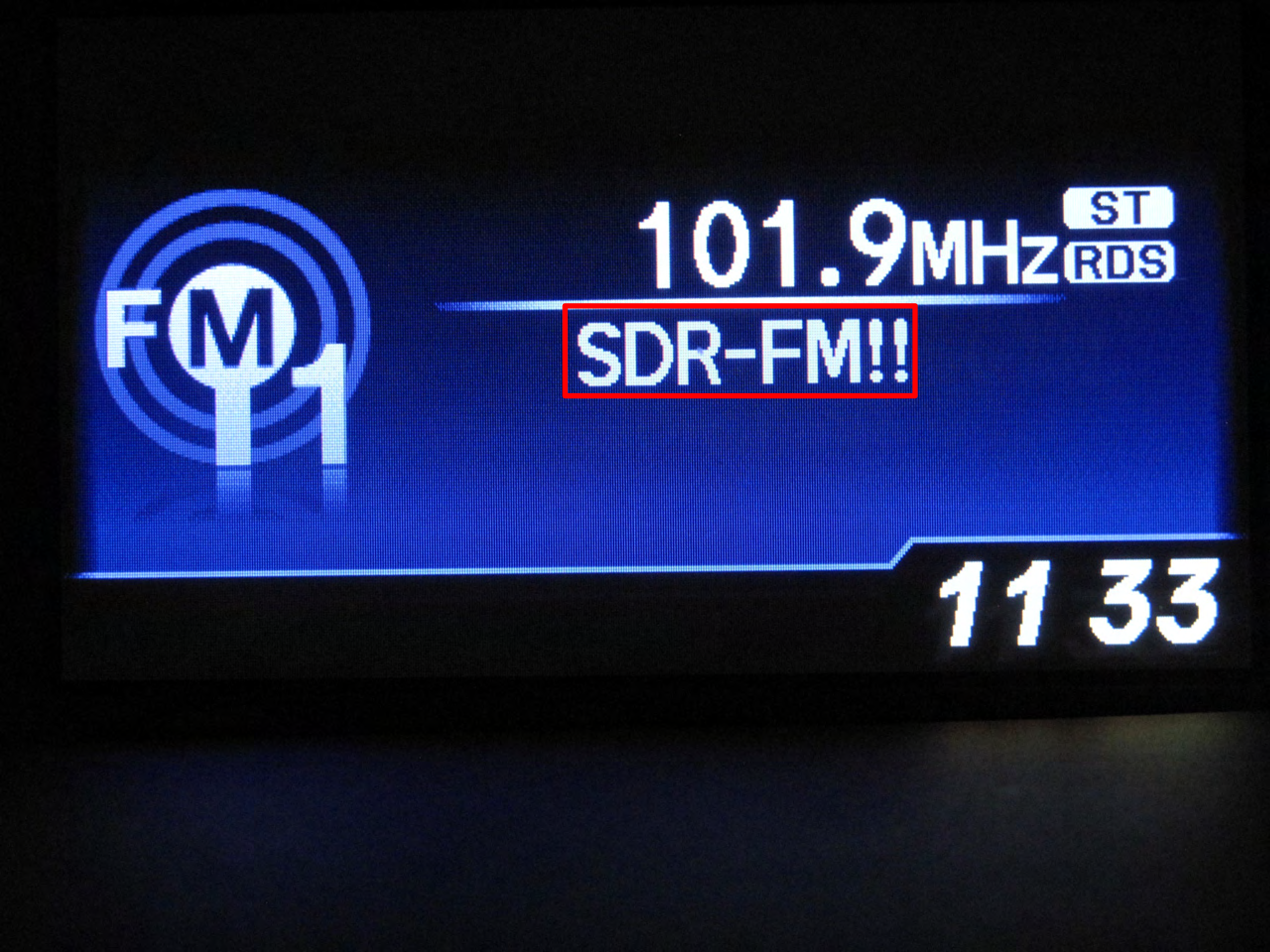
Antenna: TX/RX

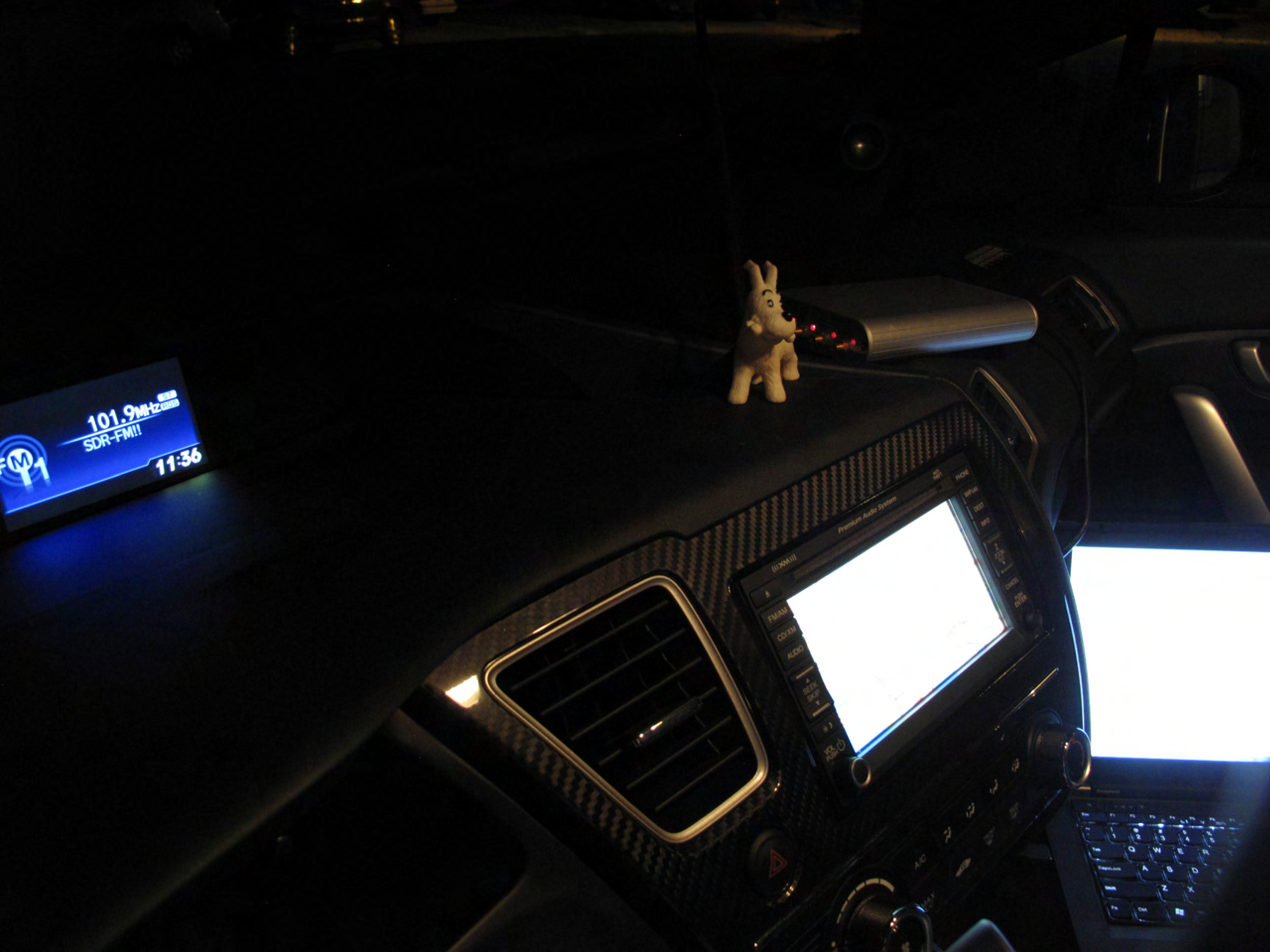
Frequency 103.70 Station Name All Time Program Type Rock Music PI 1C41

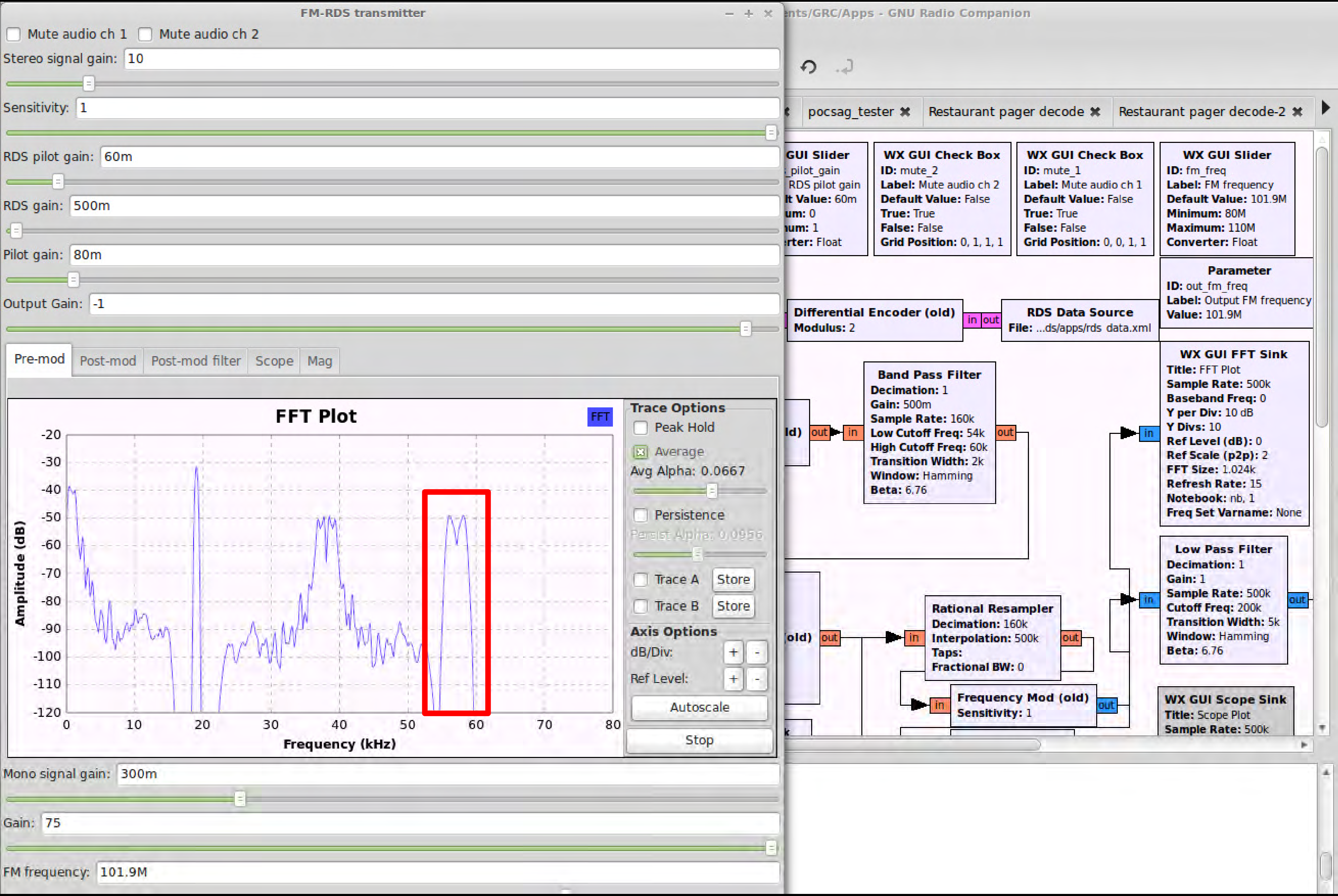
Speech Stereo

o Text The Bay's 103.7 Greatest Hits of All Time

Clock Time xxxxxxxxxxxxxxxxxxxxx Alt. Frequencies xxxxxxxxxxx


FM
1
101.9MHz
ST
RDS
SDR-FM!!
11 33


FM 1
101.9MHz
ST
RDS
SDR-FM!!
11:36
Premium Audio System
PHONE
MAP
DEST
INFO
ZOOM
CANCEL
PUSH ENTER
FM/AM
CD/XM
AUDIO
SEEK SKIP
VOL PUSH
A/C



FM-RDS transmitter

☐ Mute audio ch 1 ☐ Mute audio ch 2

Stereo signal gain: 10

Sensitivity: 1

RDS pilot gain: 60m

RDS gain: 500m

Pilot gain: 80m

Output Gain: -1

Mono signal gain: 300m

Gain: 75

FM frequency: 101.9M

GUI Slider
_pilot_gain
RDS pilot gain
lt Value: 60m
um: 0
um: 1
rter: Float

WX GUI Check Box
ID: mute_2
Label: Mute audio ch 2
Default Value: False
True: True
False: False
Grid Position: 0, 1, 1, 1

WX GUI Check Box
ID: mute_1
Label: Mute audio ch 1
Default Value: False
True: True
False: False
Grid Position: 0, 0, 1, 1

WX GUI Slider
ID: fm_freq
Label: FM frequency
Default Value: 101.9M
Minimum: 80M
Maximum: 110M
Converter: Float

Parameter
ID: out_fm_freq
Label: Output FM frequency
Value: 101.9M

Differential Encoder (old)
Modulus: 2

RDS Data Source
File: ...ds/apps/rds_data.xml

Band Pass Filter
Decimation: 1
Gain: 500m
Sample Rate: 160k
Low Cutoff Freq: 54k
High Cutoff Freq: 60k
Transition Width: 2k
Window: Hamming
Beta: 6.76

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
Notebook: nb, 1
Freq Set Varname: None

Low Pass Filter
Decimation: 1
Gain: 1
Sample Rate: 500k
Cutoff Freq: 200k
Transition Width: 5k
Window: Hamming
Beta: 6.76

Rational Resampler
Decimation: 160k
Interpolation: 500k
Taps:
Fractional BW: 0

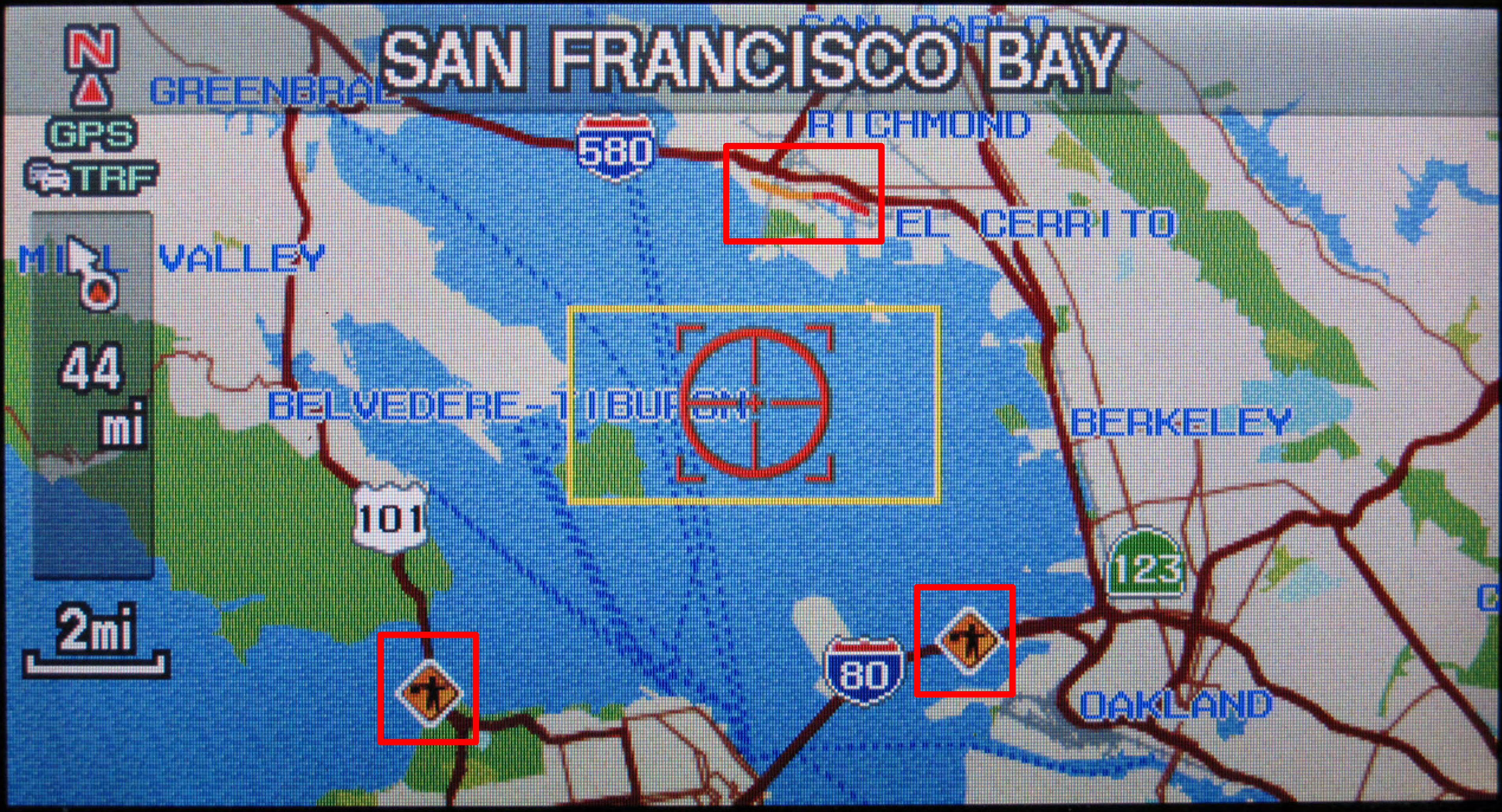
Frequency Mod (old)
Sensitivity: 1

WX GUI Scope Sink
Title: Scope Plot
Sample Rate: 500k

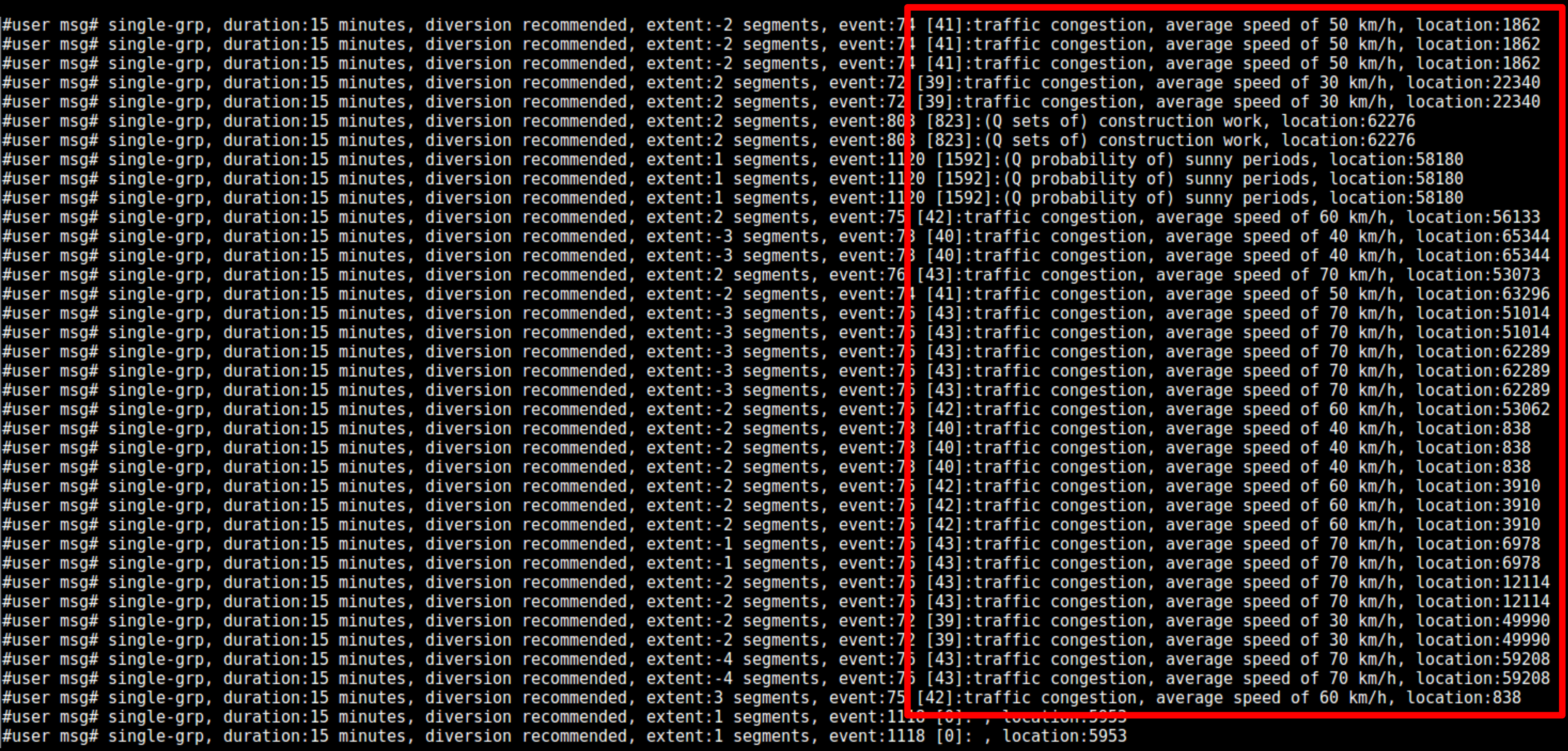
Traffic Message Channel

- Type 8A RDS group message
- Compact representation via look-up table:
  - Event
  - Location
  - Duration
- Examples:
  - Congestion
  - Accidents
  - Road work

Traffic Message Channel



Traffic Message Channel

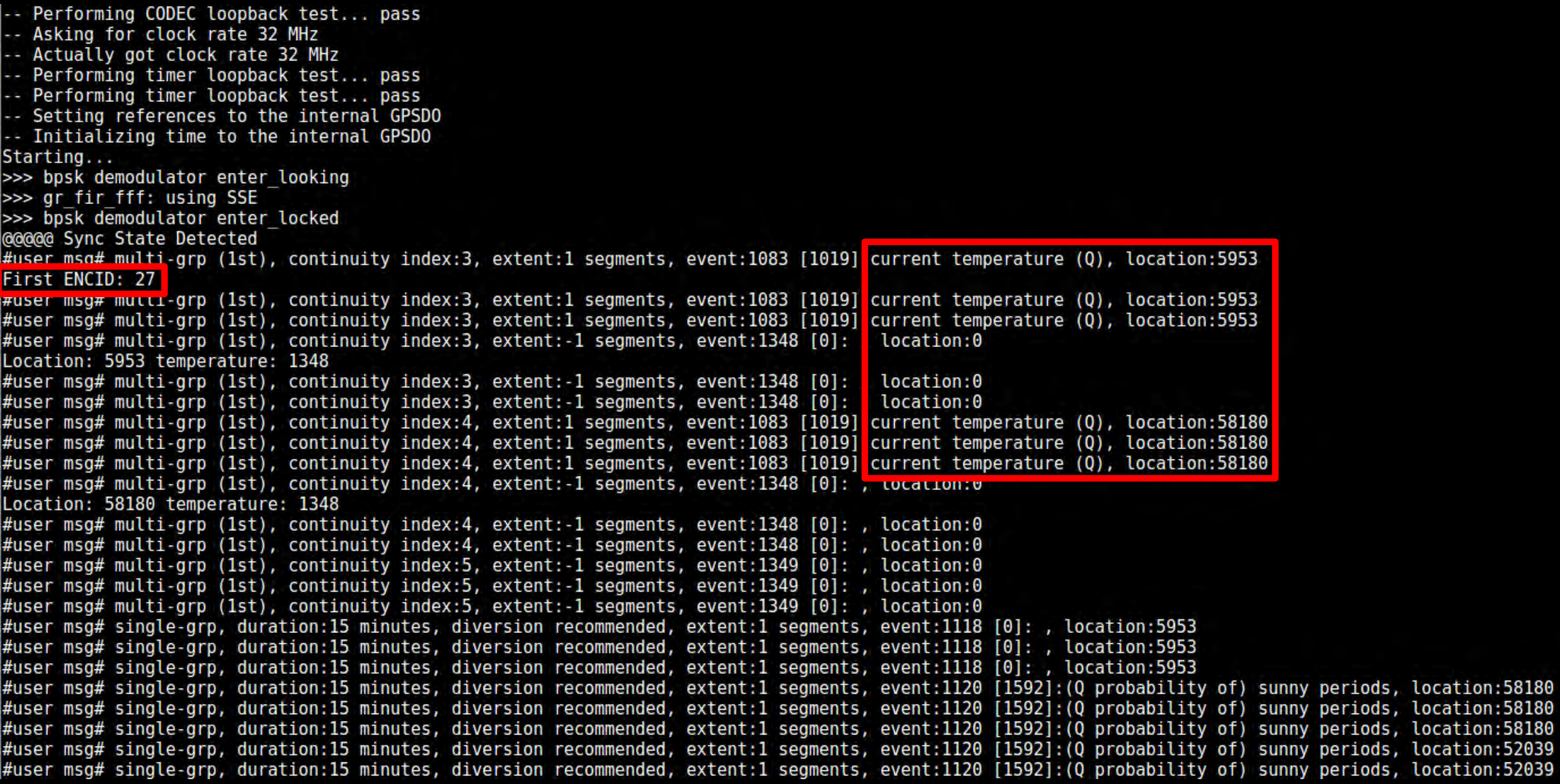


```
#user msg# single-grp, duration:15 minutes, diversion recommended, extent:-2 segments, event:74 [41]:traffic congestion, average speed of 50 km/h, location:1862
#user msg# single-grp, duration:15 minutes, diversion recommended, extent:-2 segments, event:74 [41]:traffic congestion, average speed of 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: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
```

Encrypted Location Codes

- Location codes: 16-bit for a given geographical area
- Encryption keys: 16-bit
- Schedule: One randomly chosen each day from 31 standard keys
- Receiver update: Key ID broadcast constantly

Daily Key ID

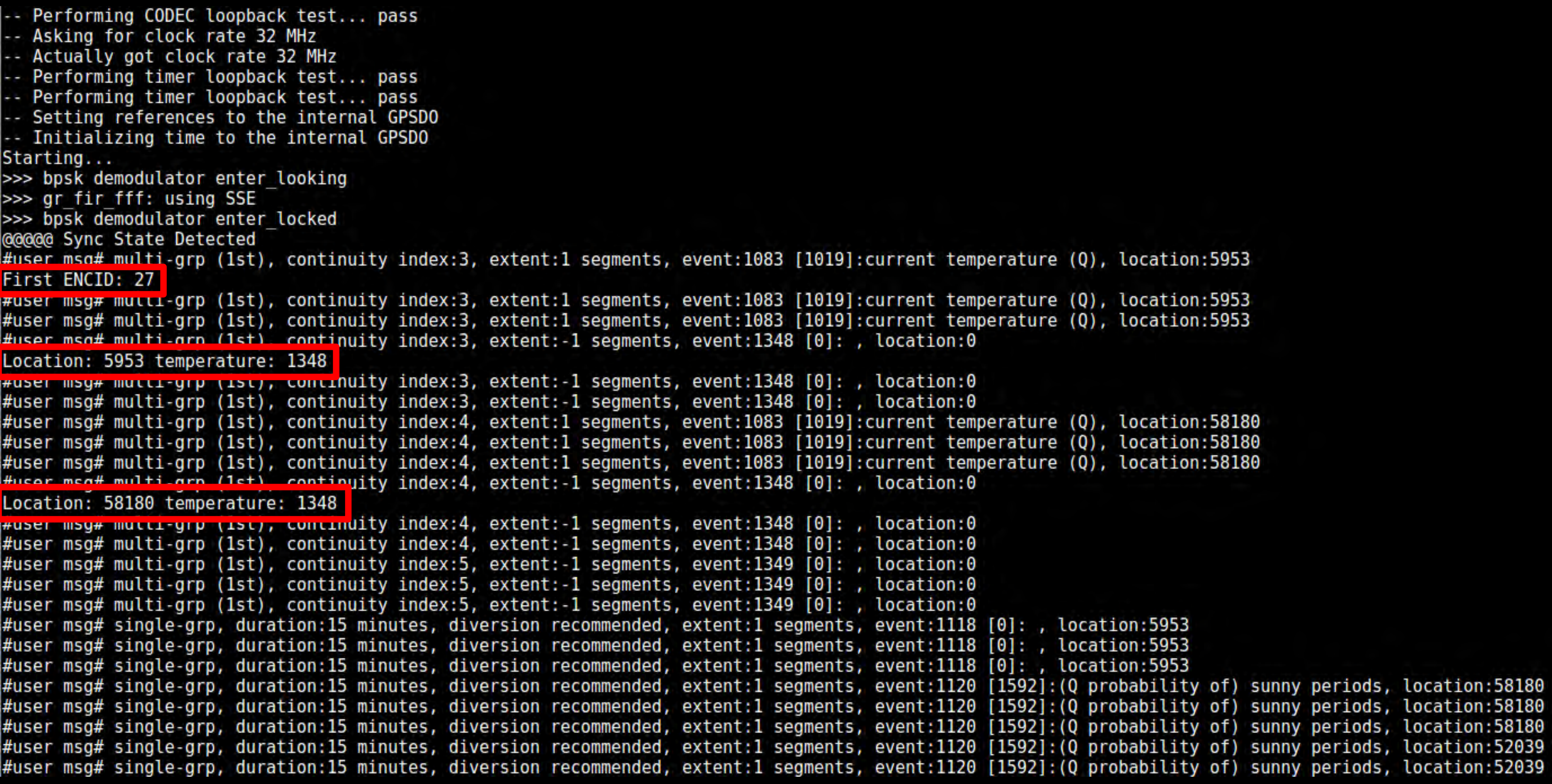


```
-- Performing CODEC loopback test... pass
-- Asking for clock rate 32 MHz
-- Actually got clock rate 32 MHz
-- Performing timer loopback test... pass
-- Performing timer loopback test... pass
-- Setting references to the internal GPSDO
-- Initializing time to the internal GPSDO
Starting...
>>> bpsk demodulator enter_looking
>>> gr_fir_fff: using SSE
>>> bpsk demodulator enter_locked
@@@@@ Sync State Detected
#user msg# multi-grp (1st), continuity index:3, extent:1 segments, event:1083 [1019] current temperature (Q), location:5953
First ENCID: 27
#user msg# multi-grp (1st), continuity index:3, extent:1 segments, event:1083 [1019] current temperature (Q), location:5953
#user msg# multi-grp (1st), continuity index:3, extent:1 segments, event:1083 [1019] current temperature (Q), location:5953
#user msg# multi-grp (1st), continuity index:3, extent:-1 segments, event:1348 [0]:   location:0
Location: 5953 temperature: 1348
#user msg# multi-grp (1st), continuity index:3, extent:-1 segments, event:1348 [0]:   location:0
#user msg# multi-grp (1st), continuity index:3, extent:-1 segments, event:1348 [0]:   location:0
#user msg# multi-grp (1st), continuity index:4, extent:1 segments, event:1083 [1019] current temperature (Q), location:58180
#user msg# multi-grp (1st), continuity index:4, extent:1 segments, event:1083 [1019] current temperature (Q), location:58180
#user msg# multi-grp (1st), continuity index:4, extent:1 segments, event:1083 [1019] current temperature (Q), location:58180
#user msg# multi-grp (1st), continuity index:4, extent:-1 segments, event:1348 [0]: , location:0
Location: 58180 temperature: 1348
#user msg# multi-grp (1st), continuity index:4, extent:-1 segments, event:1348 [0]: , location:0
#user msg# multi-grp (1st), continuity index:4, extent:-1 segments, event:1348 [0]: , location:0
#user msg# multi-grp (1st), continuity index:5, extent:-1 segments, event:1349 [0]: , location:0
#user msg# multi-grp (1st), continuity index:5, extent:-1 segments, event:1349 [0]: , location:0
#user msg# multi-grp (1st), continuity index:5, extent:-1 segments, event:1349 [0]: , location:0
#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
#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: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:1 segments, event:1120 [1592]:(Q probability of) sunny periods, location:52039
#user msg# single-grp, duration:15 minutes, diversion recommended, extent:1 segments, event:1120 [1592]:(Q probability of) sunny periods, location:52039
```

Patterns

- Always three unique temperature reports
  - Key: Event ID
  - Value: Location
- Group of three **Event ID**s always the ‘same’
- **Encrypted Location ID**s always the same for given **Enc ID**
- **Event ID**s identical for period of days/weeks
  - Can vary after some time, but ‘hidden’ (unobserved) value is always the same

‘Temperatures’



```
-- Performing CODEC loopback test... pass
-- Asking for clock rate 32 MHz
-- Actually got clock rate 32 MHz
-- Performing timer loopback test... pass
-- Performing timer loopback test... pass
-- Setting references to the internal GPSDO
-- Initializing time to the internal GPSDO
Starting...
>>> bpsk demodulator enter_looking
>>> gr_fir_fff: using SSE
>>> bpsk demodulator enter_locked
@@@@@ Sync State Detected
#user msg# multi-grp (1st), continuity index:3, extent:1 segments, event:1083 [1019]:current temperature (Q), location:5953
First ENCID: 27
#user msg# multi-grp (1st), continuity index:3, extent:1 segments, event:1083 [1019]:current temperature (Q), location:5953
#user msg# multi-grp (1st), continuity index:3, extent:1 segments, event:1083 [1019]:current temperature (Q), location:5953
#user msg# multi-grp (1st), continuity index:3, extent:-1 segments, event:1348 [0]: , location:0
Location: 5953 temperature: 1348
#user msg# multi-grp (1st), continuity index:3, extent:-1 segments, event:1348 [0]: , location:0
#user msg# multi-grp (1st), continuity index:3, extent:-1 segments, event:1348 [0]: , location:0
#user msg# multi-grp (1st), continuity index:4, extent:1 segments, event:1083 [1019]:current temperature (Q), location:58180
#user msg# multi-grp (1st), continuity index:4, extent:1 segments, event:1083 [1019]:current temperature (Q), location:58180
#user msg# multi-grp (1st), continuity index:4, extent:1 segments, event:1083 [1019]:current temperature (Q), location:58180
#user msg# multi-grp (1st), continuity index:4, extent:-1 segments, event:1348 [0]: , location:0
Location: 58180 temperature: 1348
#user msg# multi-grp (1st), continuity index:4, extent:-1 segments, event:1348 [0]: , location:0
#user msg# multi-grp (1st), continuity index:4, extent:-1 segments, event:1348 [0]: , location:0
#user msg# multi-grp (1st), continuity index:5, extent:-1 segments, event:1349 [0]: , location:0
#user msg# multi-grp (1st), continuity index:5, extent:-1 segments, event:1349 [0]: , location:0
#user msg# multi-grp (1st), continuity index:5, extent:-1 segments, event:1349 [0]: , location:0
#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
#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: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:1 segments, event:1120 [1592]:(Q probability of) sunny periods, location:52039
#user msg# single-grp, duration:15 minutes, diversion recommended, extent:1 segments, event:1120 [1592]:(Q probability of) sunny periods, location:52039
```

Patterns

Days →

Key ID (random each day)	K_1	K_2	K_2	K_3	…
Group Period	P_1	P_1	P_2	P_2	…
Hidden Plain 'Location'	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
L_1	evt(P_1, L_1) : enc(K_1, L_1)	evt(P_1, L_1) : enc(K_2, L_1)	evt(P_2, L_1) : enc(K_2, L_1)	evt(P_2, L_1) : enc(K_3, L_1)	…
L_2	evt(P_1, L_2) : enc(K_1, L_2)	evt(P_1, L_2) : enc(K_2, L_2)	evt(P_2, L_2) : enc(K_2, L_2)	evt(P_2, L_2) : enc(K_3, L_2)	…
L_3	evt(P_1, L_3) : enc(K_1, L_3)	evt(P_1, L_3) : enc(K_2, L_3)	evt(P_2, L_3) : enc(K_2, L_3)	evt(P_2, L_3) : enc(K_3, L_3)	…

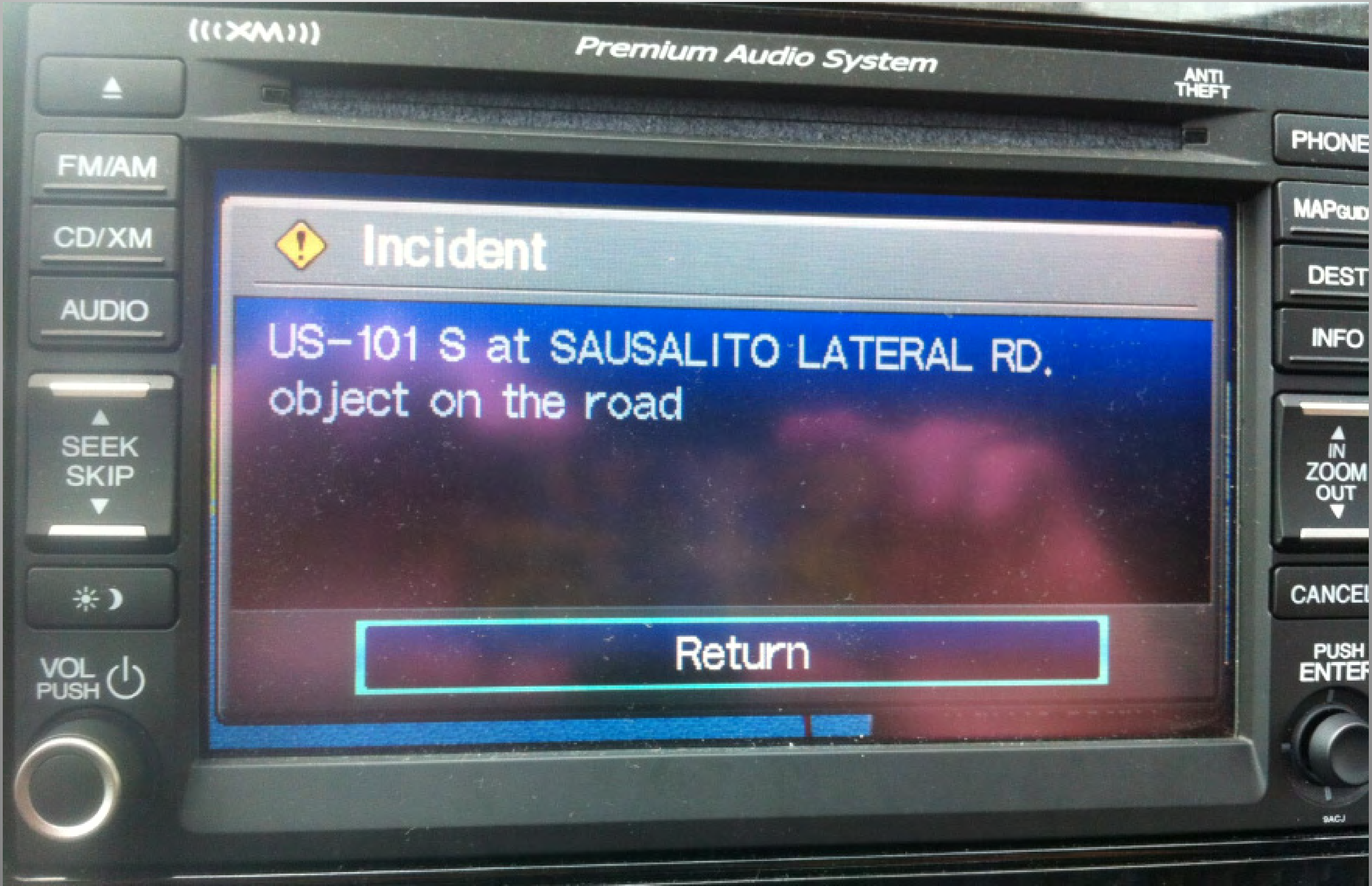
Transmitted over the air:

```
Event    = evt(period, plain location)
Location = enc(key of the day, plain location)
```

Security Analysis

- 16-bit is **very** short
- Identical group of ‘location codes’ are broadcast on a daily basis
  - Unknown but re-used plaintext
- ‘Singular’ events can be correlated from a trusted source
  - Known plaintext

Singular Event from Trusted Source



Incident

US-101 S at SAUSALITO LATERAL RD.
object on the road

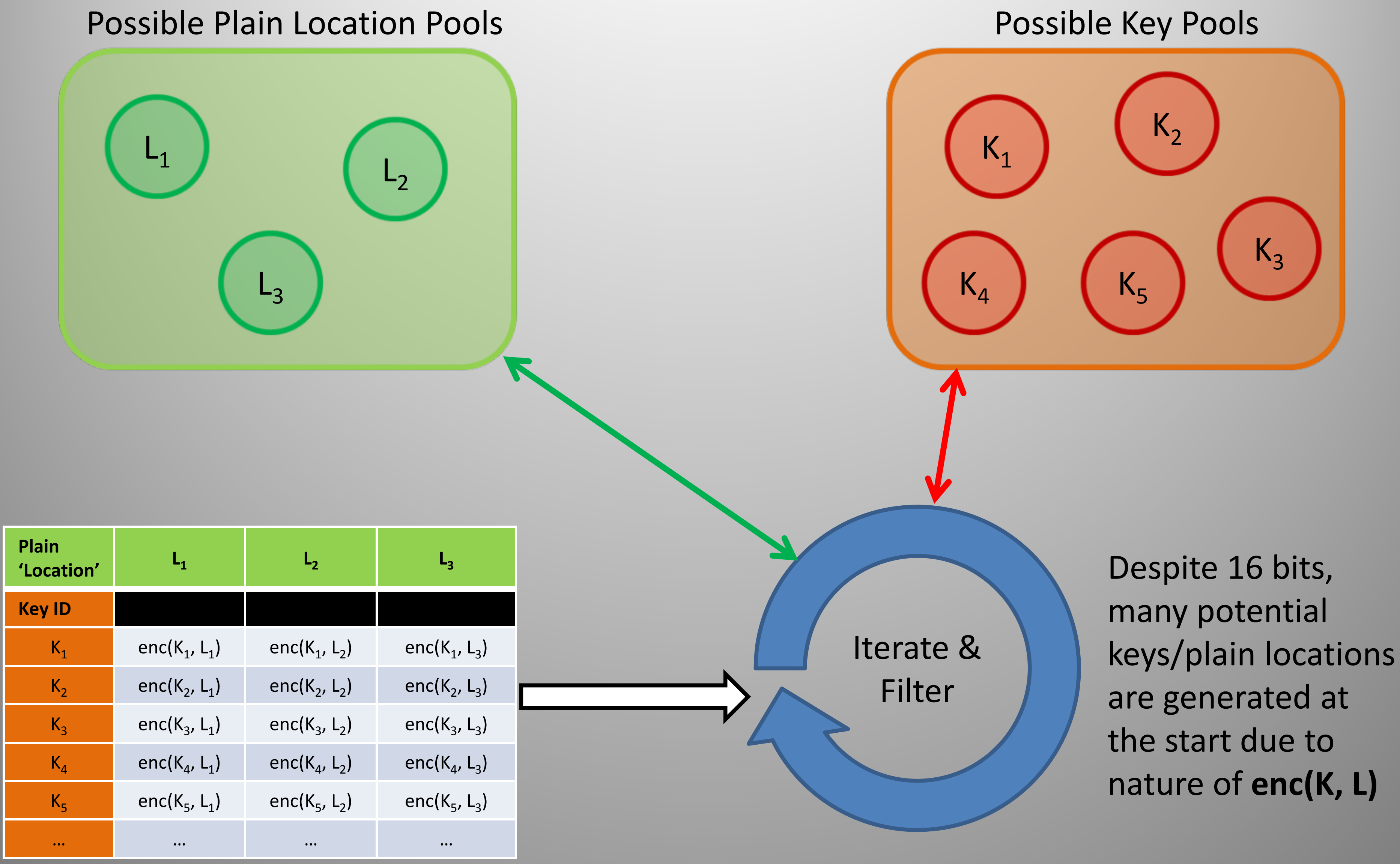
Return

Input Data

Plain 'Location'	**L_1**	**L_2**	**L_3**
Key ID	[redacted]	[redacted]	[redacted]
K_1	enc(K_1, L_1)	enc(K_1, L_2)	enc(K_1, L_3)
K_2	enc(K_2, L_1)	enc(K_2, L_2)	enc(K_2, L_3)
K_3	enc(K_3, L_1)	enc(K_3, L_2)	enc(K_3, L_3)
K_4	enc(K_4, L_1)	enc(K_4, L_2)	enc(K_4, L_3)
K_5	enc(K_5, L_1)	enc(K_5, L_2)	enc(K_5, L_3)
…	…	…	…

1. Bootstrap: find all possible plain locations & keys that result in enc(K_1, L_1)
2. Given those keys, find all possible plain locations recorded with that Key K_1 (i.e. L_2, L_3)
   - Remember pool of possible plain locations for each L & pool of possible keys for K
3. For each remaining K, repeat maintaining pool of possible keys for each K:
   - Find all possible keys given pool of possible plain locations for each L
   - Repeat, filtering pools until only one match remains
   - → Remove item from pool when enc(K, L) ≠ input data

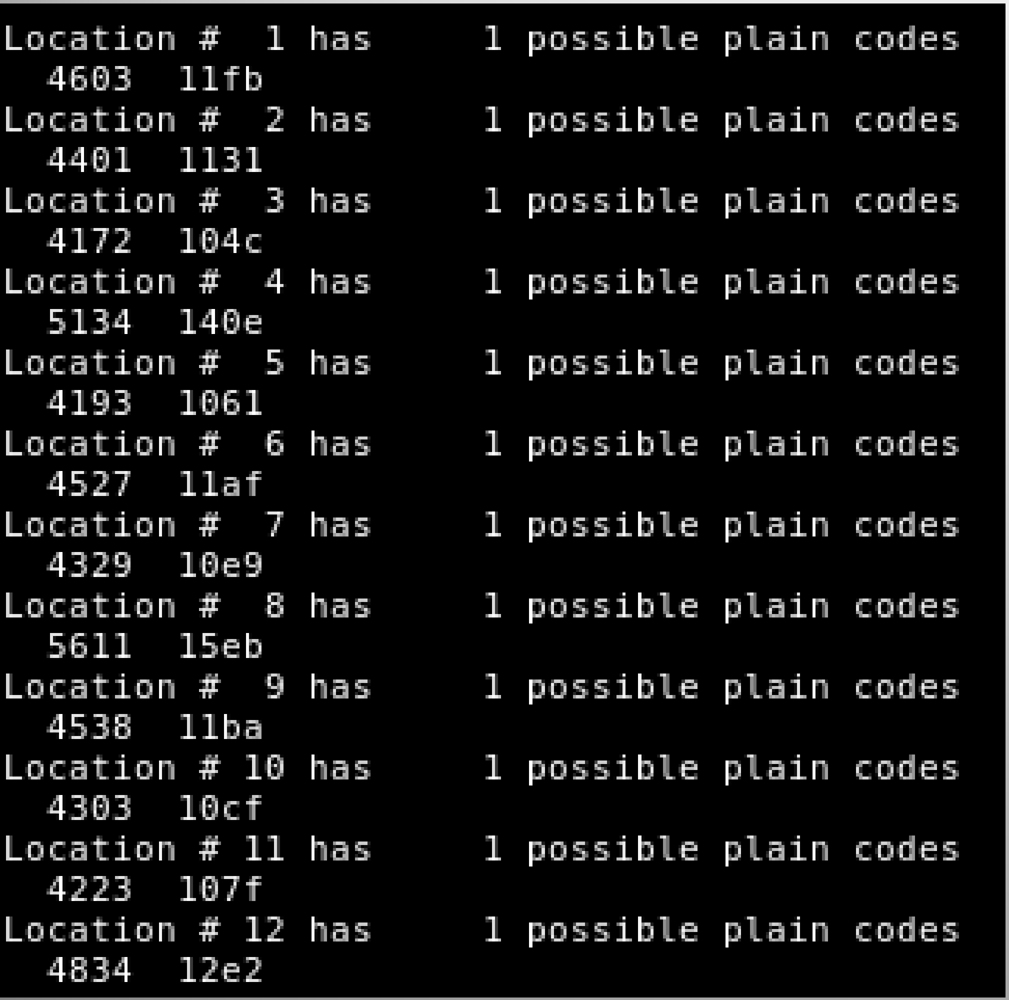
Algorithm



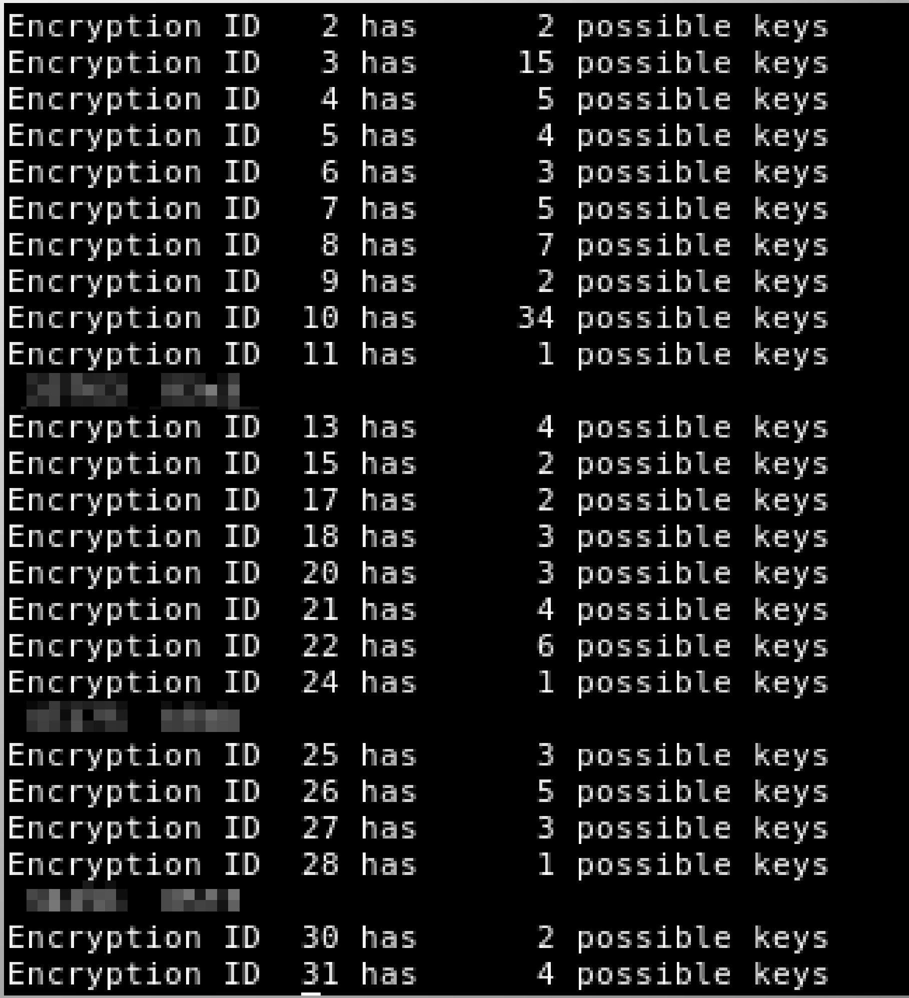
Plain 'Location'	L_1	L_2	L_3
Key ID			
K_1	enc(K_1, L_1)	enc(K_1, L_2)	enc(K_1, L_3)
K_2	enc(K_2, L_1)	enc(K_2, L_2)	enc(K_2, L_3)
K_3	enc(K_3, L_1)	enc(K_3, L_2)	enc(K_3, L_3)
K_4	enc(K_4, L_1)	enc(K_4, L_2)	enc(K_4, L_3)
K_5	enc(K_5, L_1)	enc(K_5, L_2)	enc(K_5, L_3)
…	…	…	…

Despite 16 bits, many potential keys/plain locations are generated at the start due to nature of **enc(K, L)**

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
 [redacted]
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
 [redacted]
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
 [redacted]
Encryption ID  30 has      2 possible keys
Encryption ID  31 has      4 possible keys
```

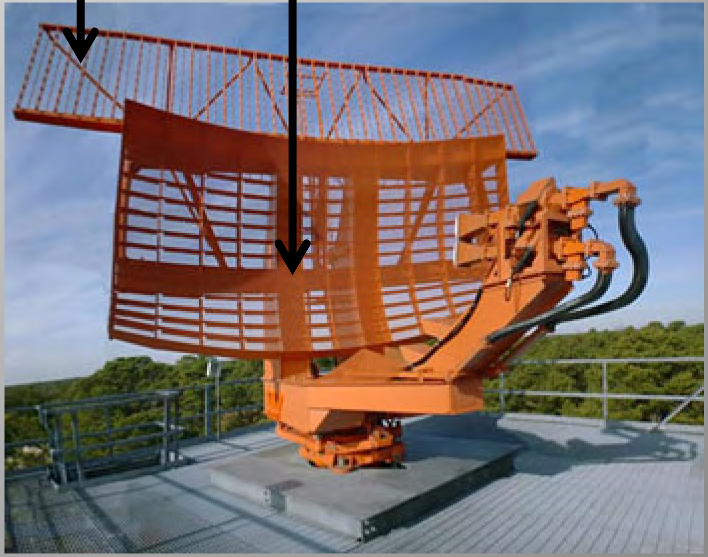
Results

- Convergence expedited by addition of ‘singular’ events
  - “vehicle fire(s)”
  - “flooding”
  - “object(s) on roadway {something that does not neccessarily block the road or part of it}”
- Even though multiple keys exist for a Key ID, with enough data plain location search yields one match!

Aviation RADAR

ATCRBS, PSR & SSR

- **A**ir **T**raffic **C**ontrol **R**adar **B**eacon **S**ystem
  - **P**rimary **S**urveillance **R**adar
  - **S**econdary **S**urveillance **R**adar

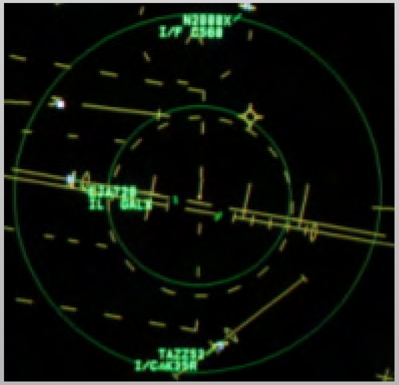


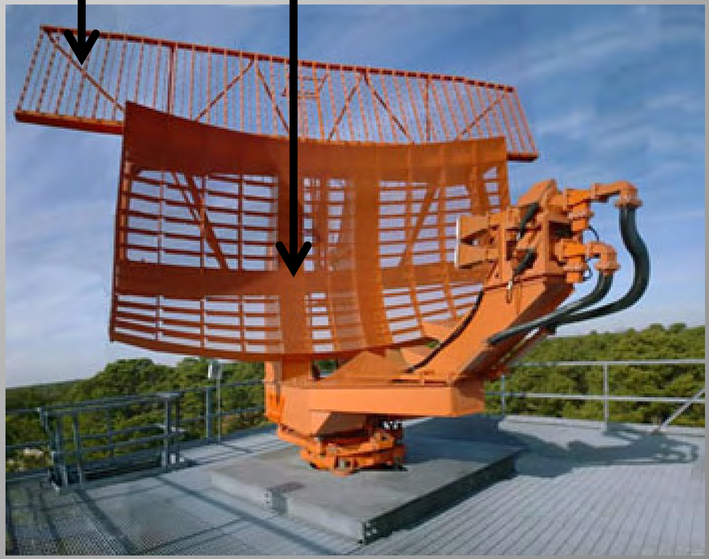
Primary:

- Traditional RADAR
- ‘Paints skins’ and listens for return
- Identifies and tracks primary targets, while ignoring ‘ground clutter’
- Range limited by RADAR equation ($\frac{1}{d^4}$)

ATCRBS, PSR & SSR

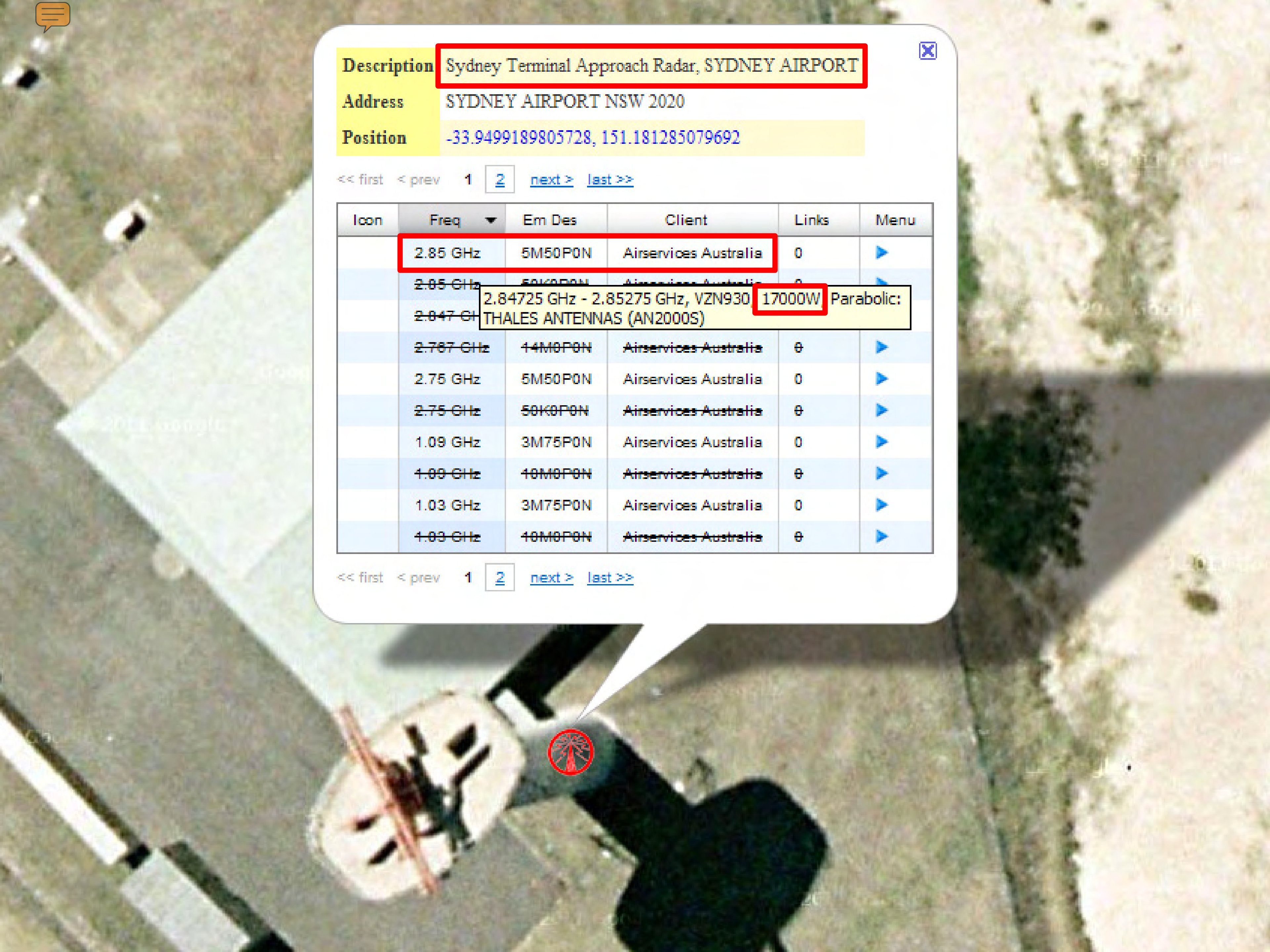
- **A**ir **T**raffic **C**ontrol **R**adar **B**eacon **S**ystem
  - **P**rimary **S**urveillance **R**adar
  - **S**econdary **S**urveillance **R**adar





Secondary:

- Directional radio
- Requires transponder
- Interrogates transponders, which reply with squawk code, altitude, etc.
- Increased range ($\frac{1}{d^2}$)



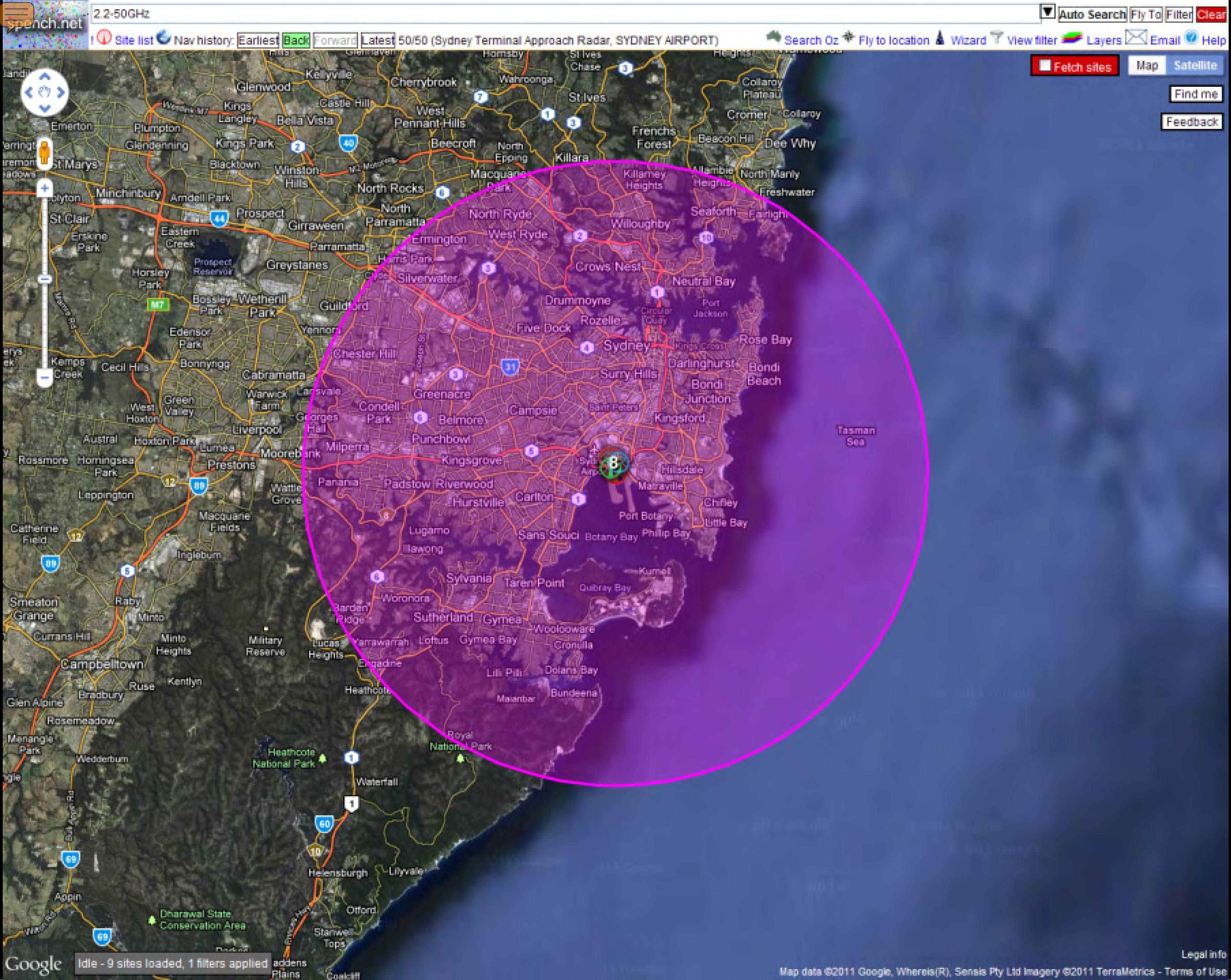
Description	Sydney Terminal Approach Radar, SYDNEY AIRPORT
Address	SYDNEY AIRPORT NSW 2020
Position	-33.9499189805728, 151.181285079692

<< first < prev 1 2 next > last >>

Icon	Freq	Em Des	Client	Links	Menu
	2.85 GHz	5M50P0N	Airservices Australia	0	▶
	~~2.85 GHz~~	~~50K0P0N~~	~~Airservices Australia~~	0	▶
	~~2.847 GH~~				
	~~2.767 GHz~~	~~14M0P0N~~	~~Airservices Australia~~	~~0~~	▶
	2.75 GHz	5M50P0N	Airservices Australia	0	▶
	~~2.75 GHz~~	~~50K0P0N~~	~~Airservices Australia~~	~~0~~	▶
	1.09 GHz	3M75P0N	Airservices Australia	0	▶
	~~1.09 GHz~~	~~10M0P0N~~	~~Airservices Australia~~	~~0~~	▶
	1.03 GHz	3M75P0N	Airservices Australia	0	▶
	~~1.03 GHz~~	~~10M0P0N~~	~~Airservices Australia~~	~~0~~	▶

2.84725 GHz - 2.85275 GHz, VZN930, 17000W, Parabolic: THALES ANTENNAS (AN2000S)

<< first < prev 1 2 next > last >>



2.2-50GHz

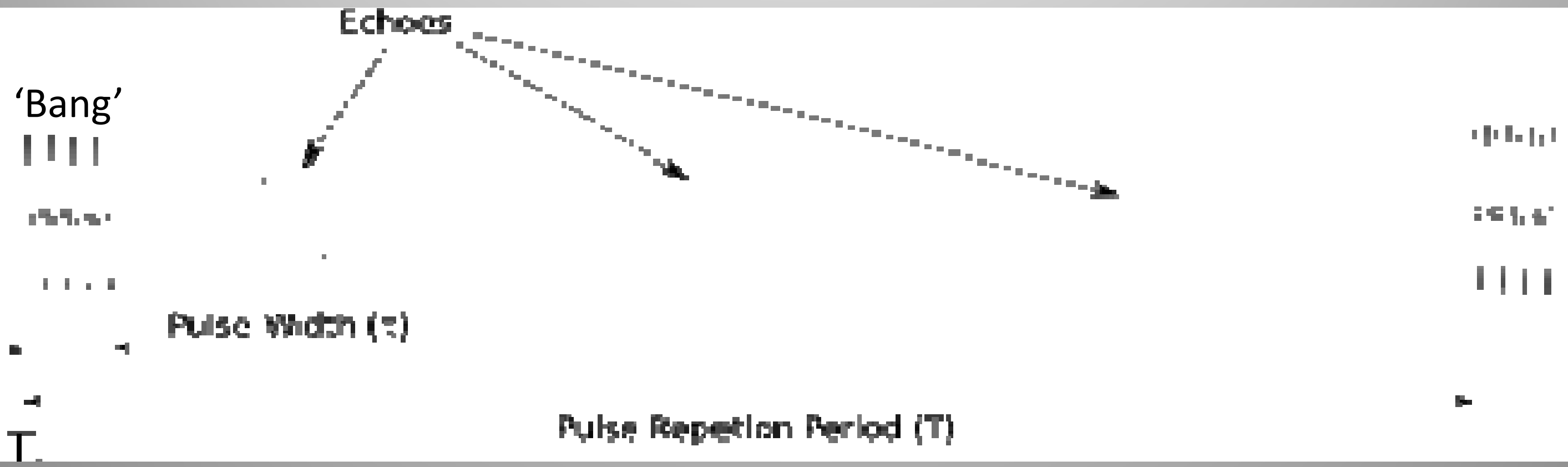
50/50 (Sydney Terminal Approach Radar, SYDNEY AIRPORT)

Idle - 9 sites loaded, 1 filters applied

Map data ©2011 Google, Whereis(R), Sensis Pty Ltd Imagery ©2011 TerraMetrics - Terms of Use

Primary Surveillance RADAR

- Transmits a ‘bang’ (the main pulse)
- Listens for returns (echoes)

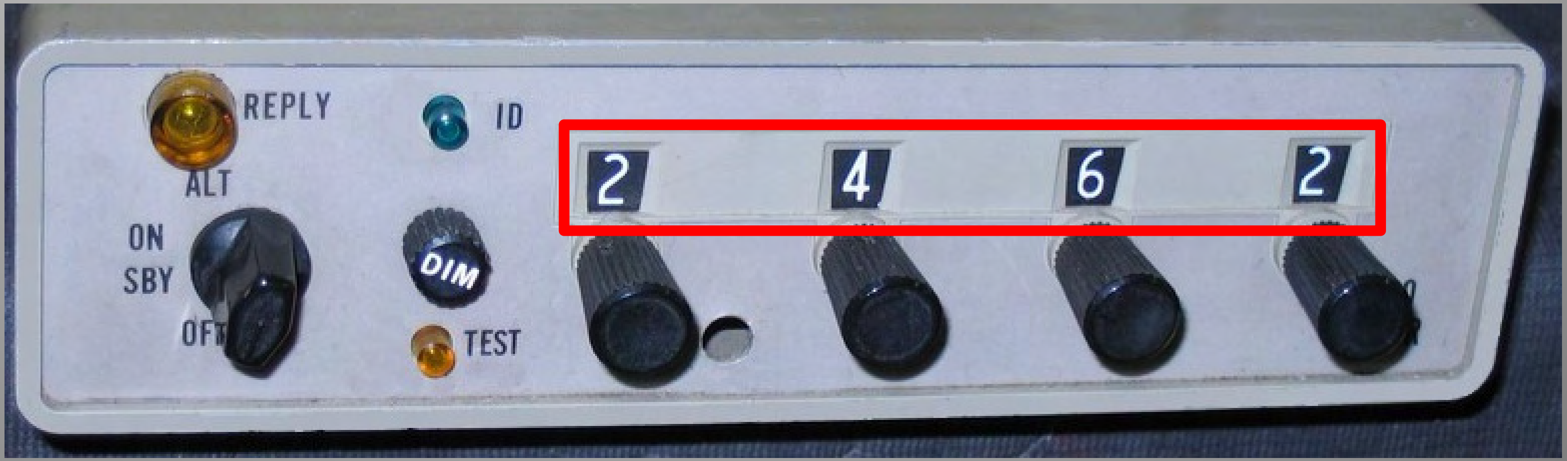


The Modes

- **A**: reply with squawk code
- **C**: reply with altitude

SSR

- **S**: enables **A**utomatic **D**ependant **S**urveillance-**B**roadcast (ADS-B), and the **A**ircraft/**T**raffic **C**ollision **A**voidance **S**ystem (ACAS/TCAS)



The Modes

- **A**: reply with squawk code
- **C**: reply with altitude

SSR

- **S**: enables **A**utomatic **D**ependant **S**urveillance-**B**roadcast (ADS-B), and the **A**ircraft/**T**raffic **C**ollision **A**voidance **S**ystem (ACAS/TCAS)

- Mode S not part of ATCRBS, but uses same radio hardware (same frequencies)
  - Increasing problem of channel congestion

Position

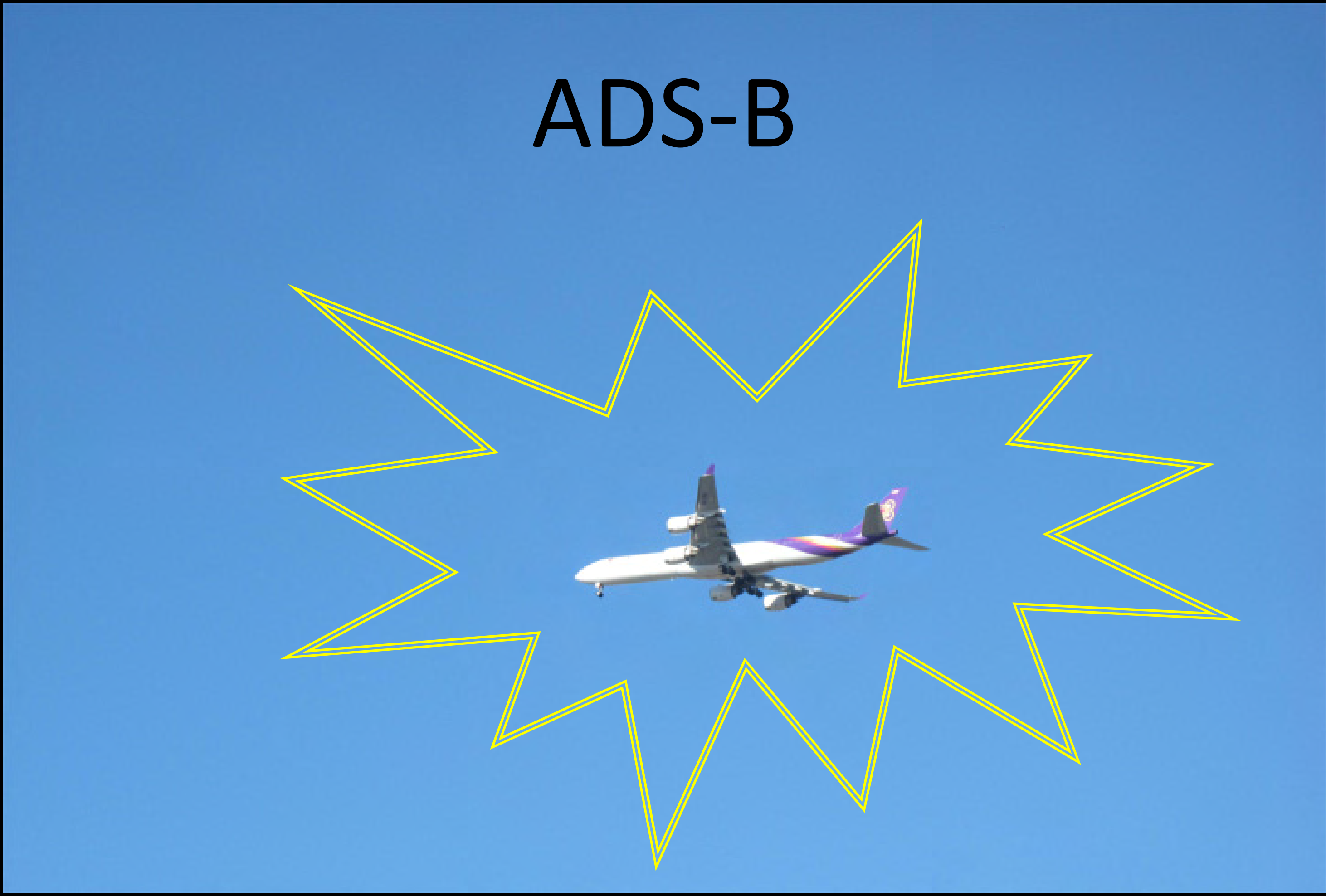
Heading

Altitude

Vertical rate

Flight ID

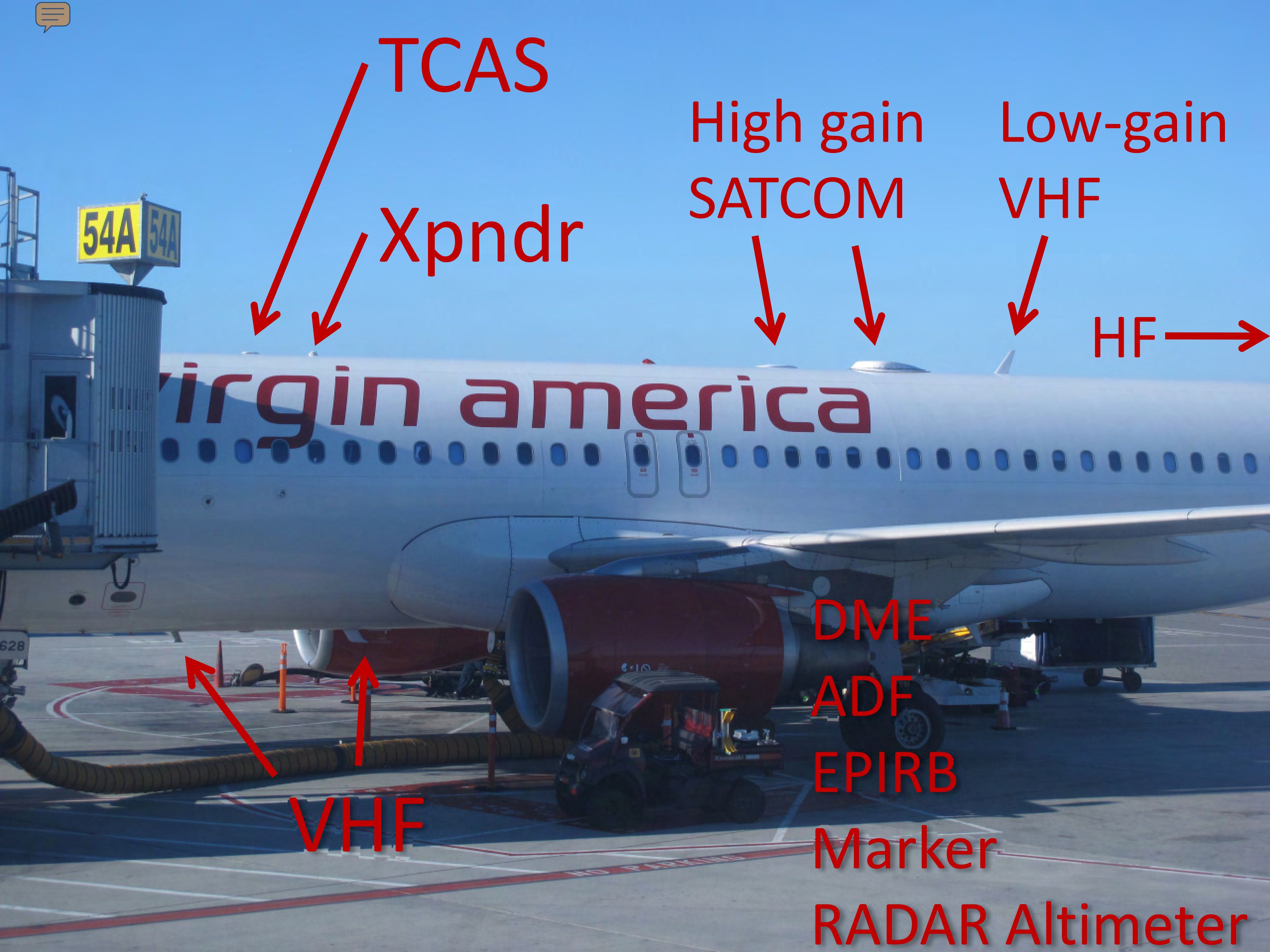
Squawk code



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



TCAS

Xpndr

High gain SATCOM

Low-gain VHF

HF

DME

ADF

EPIRB

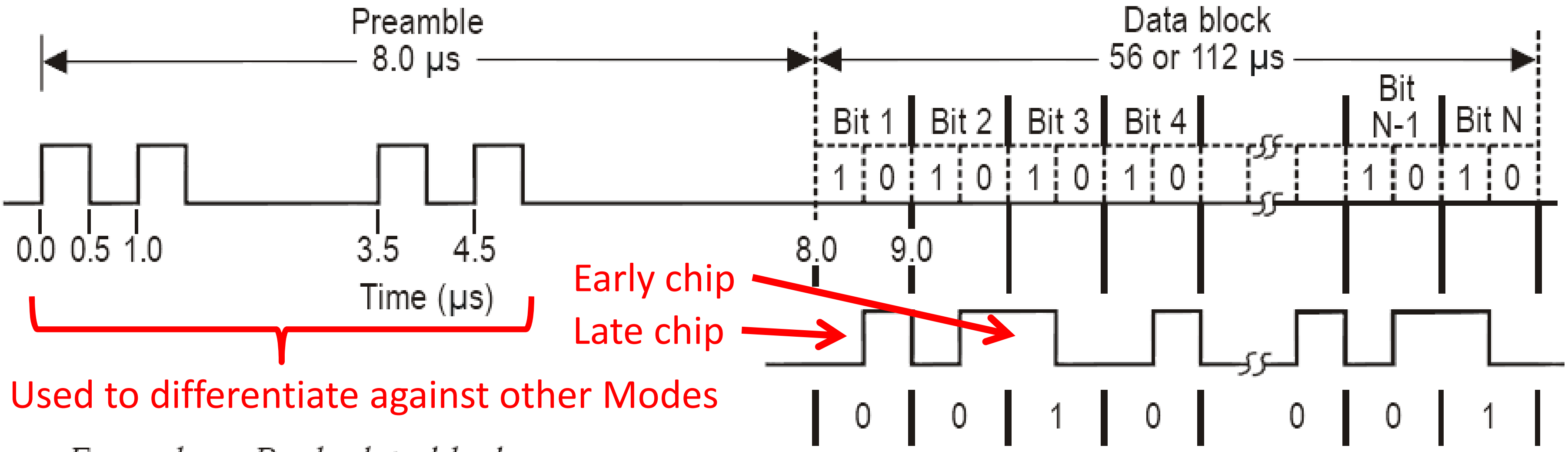
Marker

RADAR Altimeter

VHF

Mode S Response Encoding

- Data block is created & bits control position of pulses sent by transmitter



Early chip

Late chip

Used to differentiate against other Modes

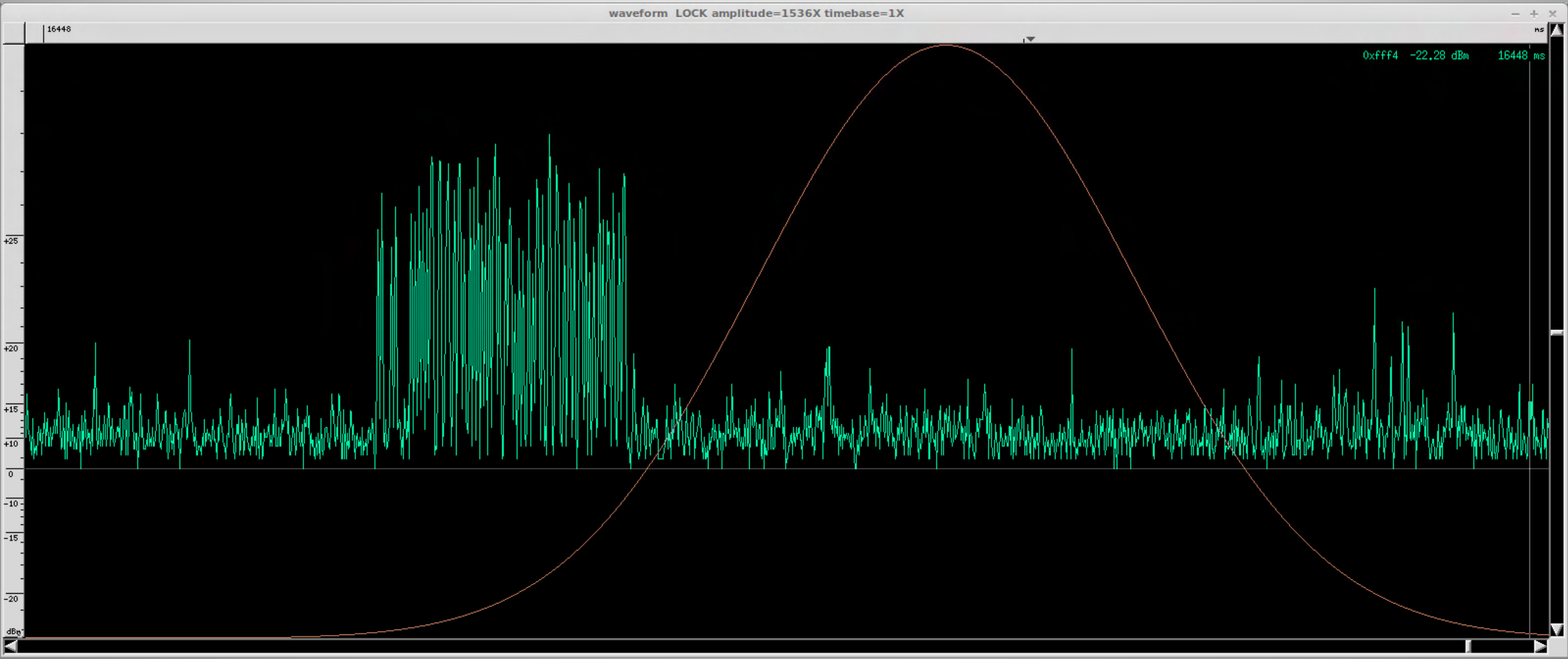
Example.— Reply data block corresponding to bit sequence 0010 001

Pulse Position Modulation (AM)

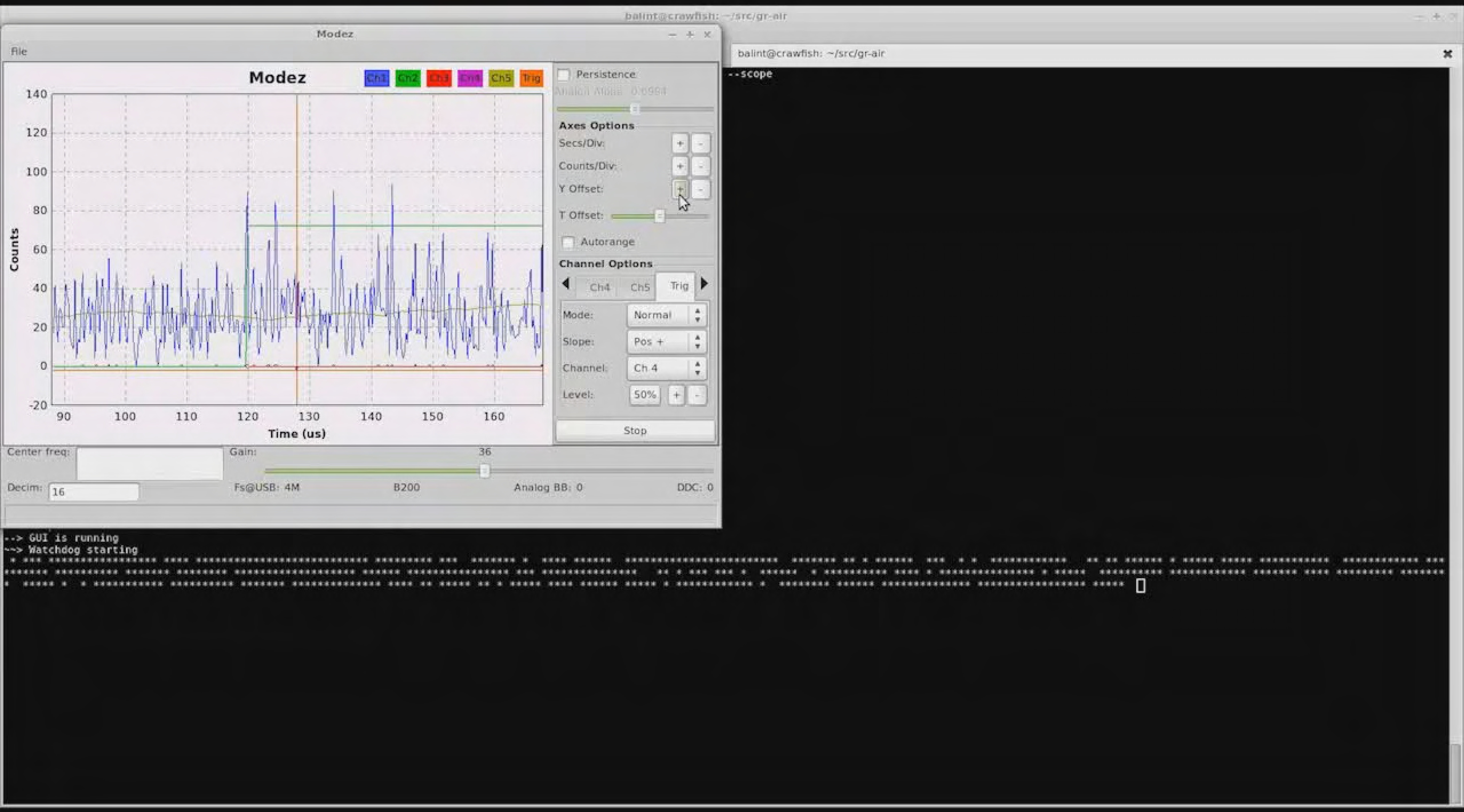
Pulse Position Modulation

- Pulse lasts **0.0000005 seconds** (0.5 μs)
- Need to sample signal at a **minimum of 2 MHz** (assuming you start sampling at precisely the right moment and stay synchronised)
- Requires high-bandwidth hardware and increased processing power
- Ideally, oversample to increase accuracy

Mode S Frame


waveform LOCK amplitude=1536X timebase=1X
16448
ms
0xfff4 -22.28 dBm
16448 ms
+25
+20
+15
+10
0
-10
-15
-20
dBm

Mode S Response: AM signal

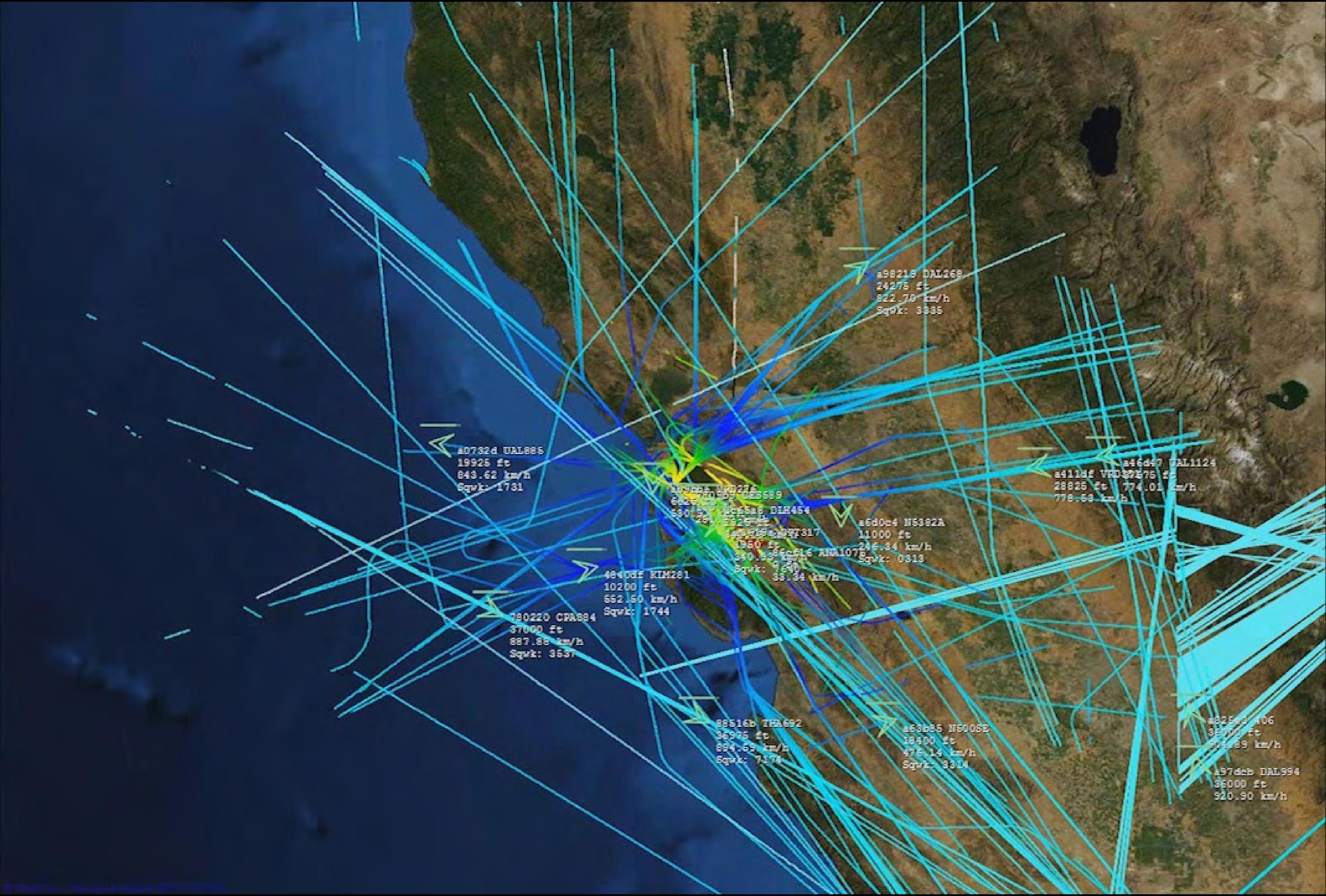


Mode: Normal
Slope: Pos +
Channel: Ch 4
Level: 50%

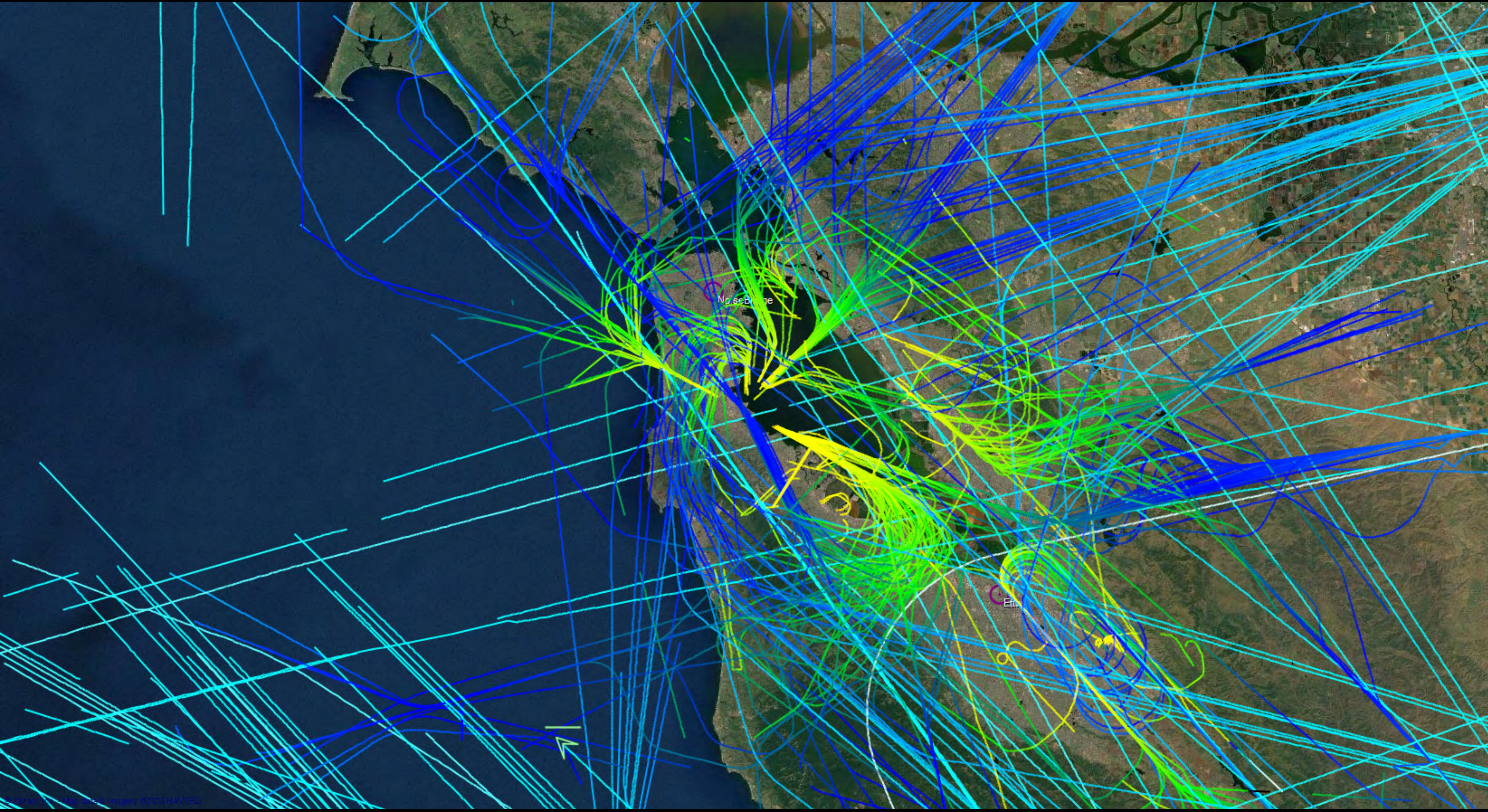
Center freq:
Gain: 36
Decim: 16
Fs@USB: 4M
B200
Analog BB: 0
DDC: 0

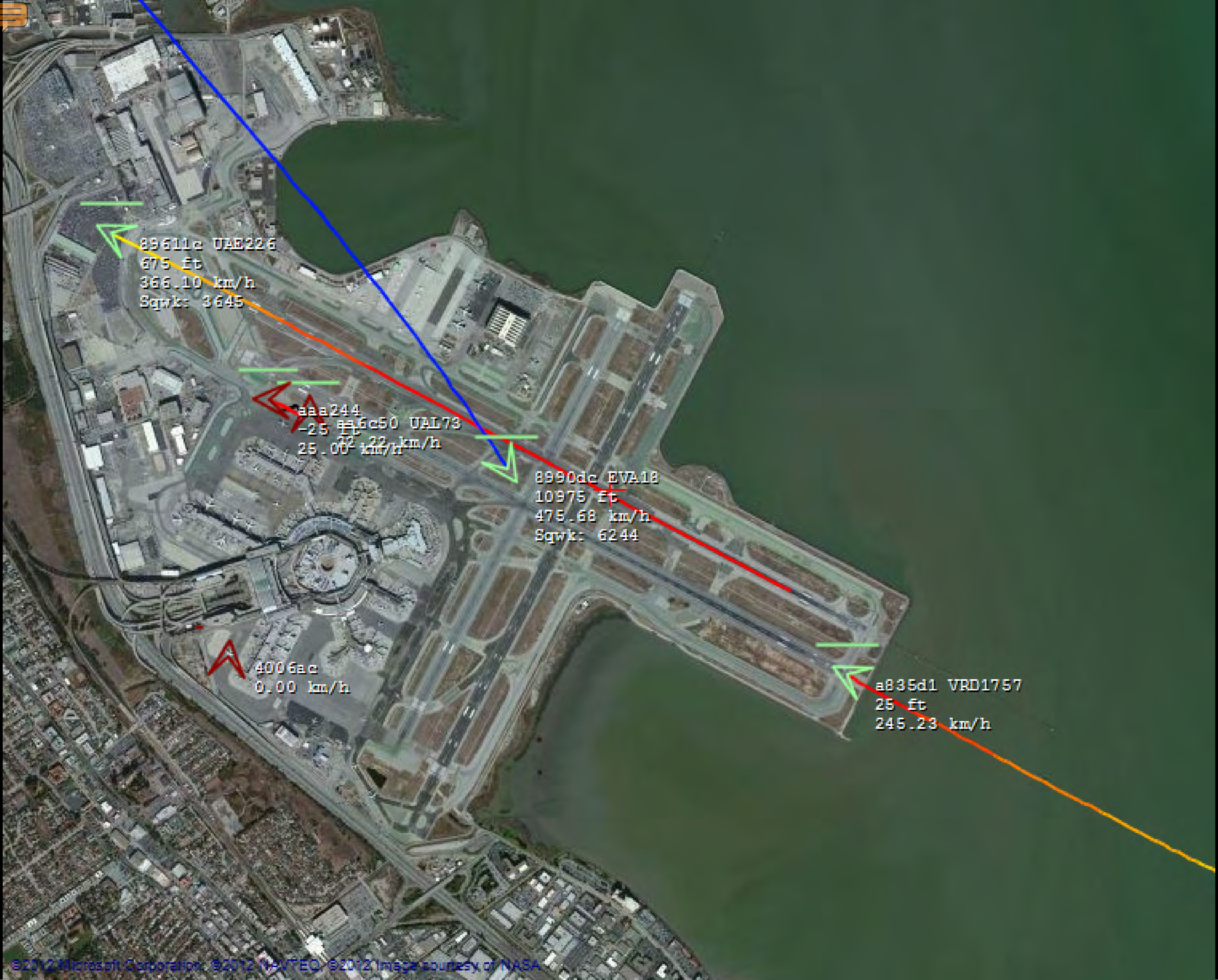
```
--scope
```

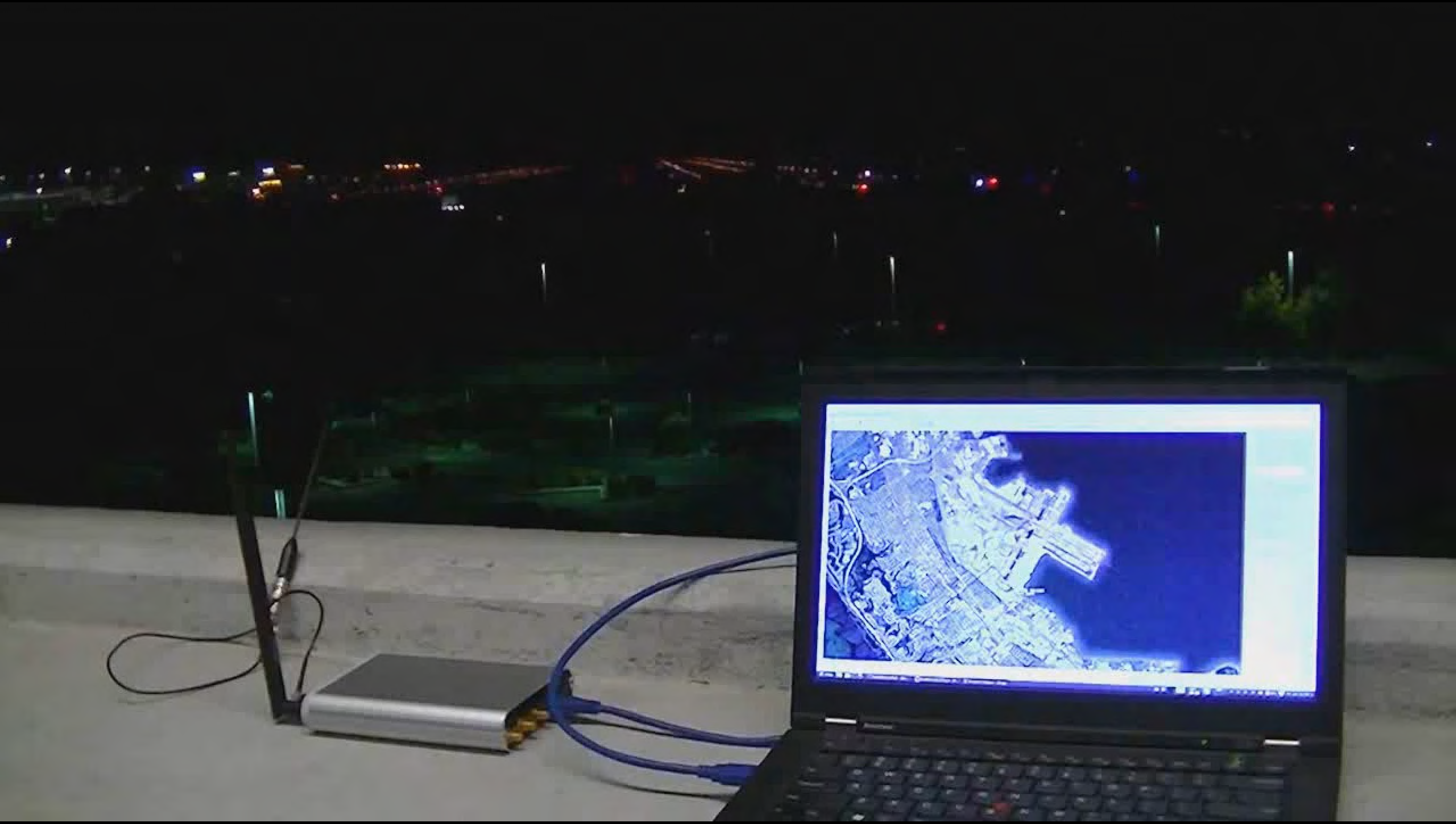
```
--> GUI is running
~~> Watchdog starting
 * *** **************** **** ************************** ********* ***  ******* *  **** ******  ************************  ******* ** * ******  ***  * *  ************   ** ** ****** * ***** ***** ***********  ************ ***
****** ********** ******* ******** ******************** ****** **************** *** **************   ** * *** *** *  ******  * ********** **** * *************** * *****  ********** ************ ******* **** ********* *******
*  ***** *  * *********** ********** ******* ************* **** ** ***** ** * ***** **** ****** ***** * ************ *  ******** ****** ************** ***************** *****
```



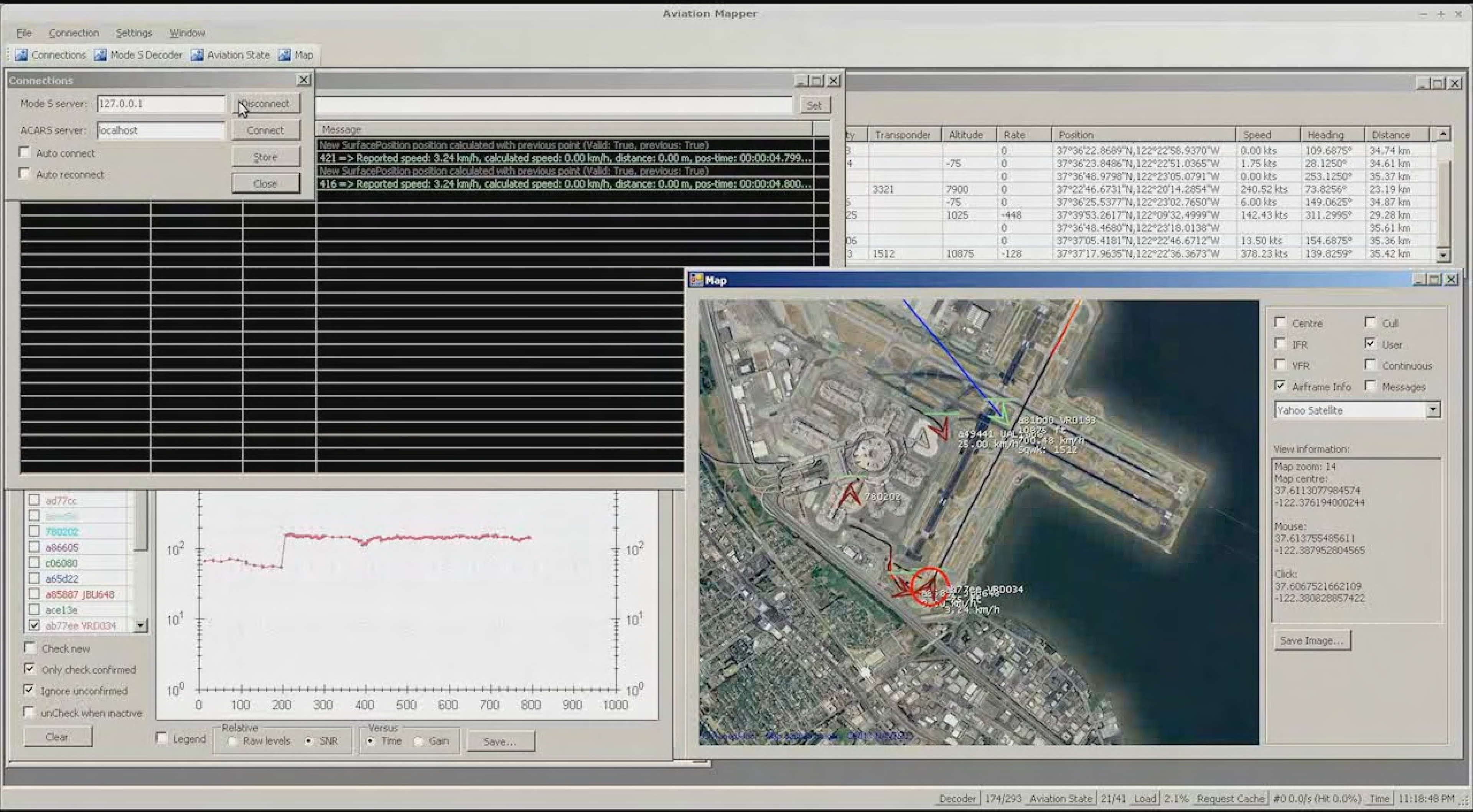
a98219 DAL268
24275 ft
822.70 km/h
Sqwk: 3385
a0732d UAL885
19925 ft
843.62 km/h
Sqwk: 1731
a46d47 UAL1124
a411df VRD
28825 ft 774.01 km/h
778.68 km/h
DLH454
a6d0c4 N5382A
11000 ft
246.34 km/h
Sqwk: 0313
AAL1078
33.34 km/h
4840df KLM281
10200 ft
652.50 km/h
Sqwk: 1744
780220 CPA884
37000 ft
887.88 km/h
Sqwk: 3537
88516b THA692
36975 ft
894.59 km/h
Sqwk: 7174
a63b85 N500SE
18400 ft
476.14 km/h
Sqwk: 3314
406
36000 ft
89 km/h
a97dcb DAL994
36000 ft
920.90 km/h


NoiseBridge
Etu
© Yahoo! Inc. - Map data & Imagery ©2013 NAVTEQ


89611c UAE226
675 ft
366.10 km/h
Sqwk: 3645
aaa244
-25 ft
25.00 km/h
aa6c50 UAL73
22.22 km/h
8990dc EVA18
10975 ft
475.68 km/h
Sqwk: 6244
4006ac
0.00 km/h
a835d1 VRD1757
25 ft
245.23 km/h
©2012 Microsoft Corporation, ©2012 NAVTEQ, ©2012 Image courtesy of NASA



a91535 UAL1556
18.52 km/h
a8434f VRD357
-125 ft
213.74 km/h
780202
-75 ft
12.96 km/h
abaceb
-75 ft
24.08 km/h
aa7b10 102
-100 ft
227.80 km/l
5887 BBU648
00 km/h



□ Auto connect
□ Auto reconnect

Message

```
New SurfacePosition position calculated with previous point (Valid: True, previous: True)
421 => Reported speed: 3.24 km/h, calculated speed: 0.00 km/h, distance: 0.00 m, pos-time: 00:00:04.799...
New SurfacePosition position calculated with previous point (Valid: True, previous: True)
416 => Reported speed: 3.24 km/h, calculated speed: 0.00 km/h, distance: 0.00 m, pos-time: 00:00:04.800...
```

ty	Transponder	Altitude	Rate	Position	Speed	Heading	Distance
3			0	37°36'22.8689"N,122°22'58.9370"W	0.00 kts	109.6875°	34.74 km
4		-75	0	37°36'23.8486"N,122°22'51.0365"W	1.75 kts	28.1250°	34.61 km
			0	37°36'48.9798"N,122°23'05.0791"W	0.00 kts	253.1250°	35.37 km
	3321	7900	0	37°22'46.6731"N,122°20'14.2854"W	240.52 kts	73.8256°	23.19 km
5		-75	0	37°36'25.5377"N,122°23'02.7650"W	6.00 kts	149.0625°	34.87 km
25		1025	-448	37°39'53.2617"N,122°09'32.4999"W	142.43 kts	311.2995°	29.28 km
			0	37°36'48.4680"N,122°23'18.0138"W			35.61 km
06			0	37°37'05.4181"N,122°22'46.6712"W	13.50 kts	154.6875°	35.36 km
3	1512	10875	-128	37°37'17.9635"N,122°22'36.3673"W	378.23 kts	139.8259°	35.42 km

□ ad77cc
□ [illegible]
□ 780202
□ a86605
□ c06080
□ a65d22
□ a85887 JBU648
□ ace13e
☑ ab77ee VRD034

□ Check new
☑ Only check confirmed
☑ Ignore unconfirmed
□ unCheck when inactive

□ Legend
Relative: ○ Raw levels ● SNR
Versus: ● Time ○ Gain

□ Centre
□ Cull
□ IFR
☑ User
□ VFR
□ Continuous
☑ Airframe Info
□ Messages

Yahoo Satellite

View information:

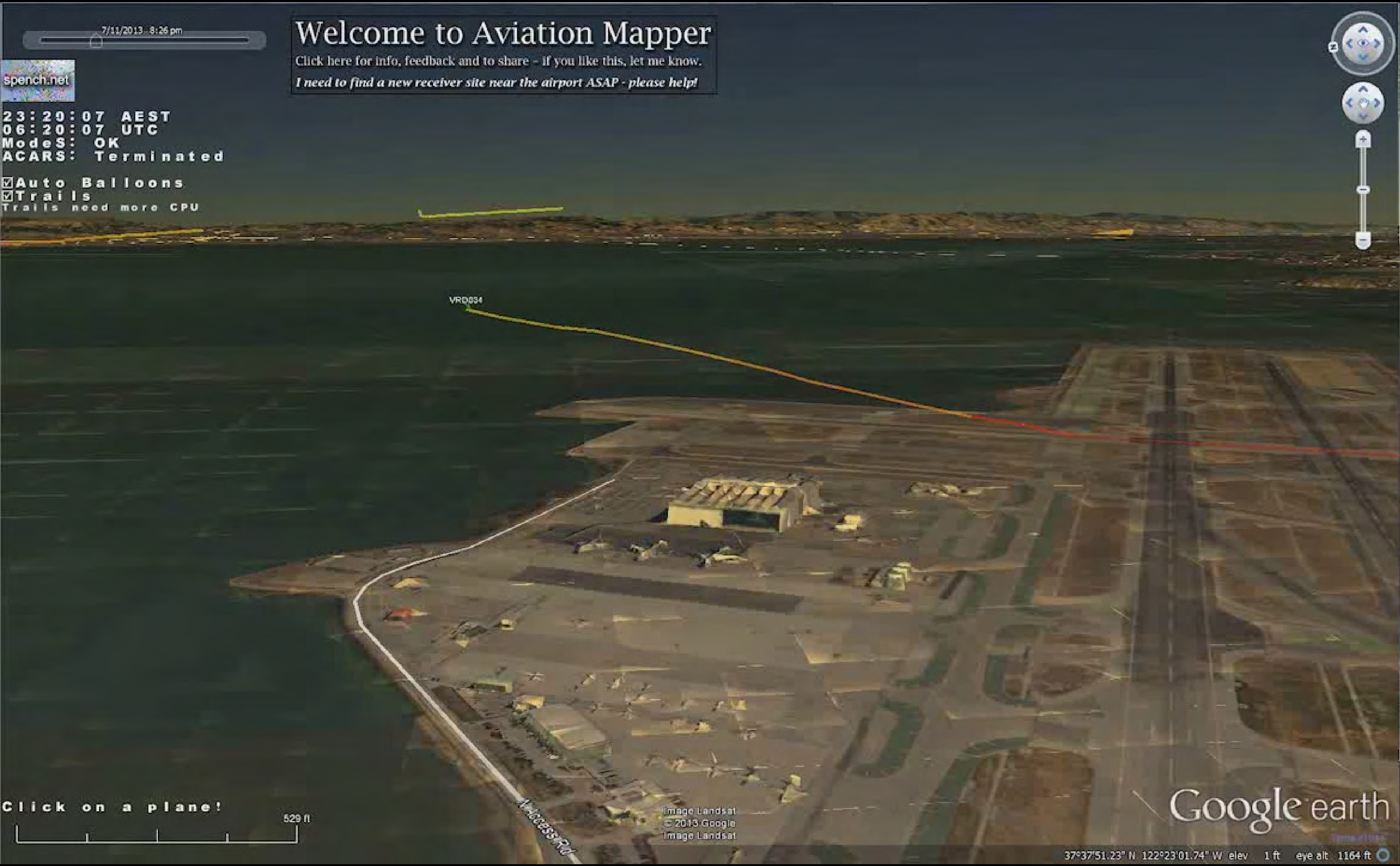
Map zoom: 14
Map centre:
37.6113077984574
-122.376194000244

Mouse:
37.613755485611
-122.387952804565

Click:
37.6067521662109
-122.380828857422

Decoder 174/293 Aviation State 21/41 Load 2.1% Request Cache #0 0.0/s (Hit 0.0%) Time 11:18:48 PM

ab77ee VRD034
225 ft
299.33 km/h
Sqwk: 1110
780202
a49441 UAL1606
27.78 km/h
a85687 JBU648
0.00 km/h



7/11/2013 8:26 pm

spench.net

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!

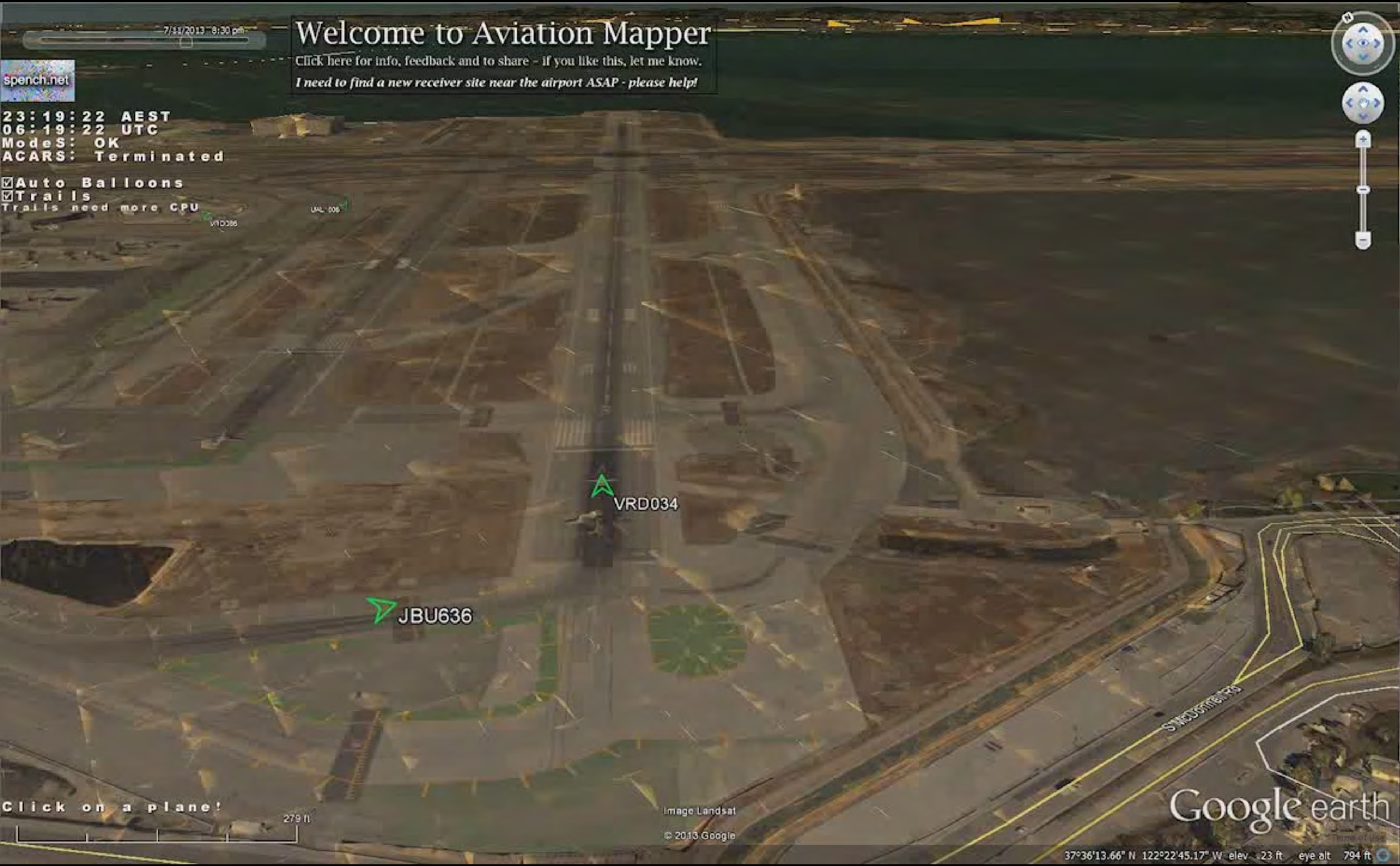
```
23:20:07 AEST
06:20:07 UTC
ModeS:  OK
ACARS:  Terminated
```

☑Auto Balloons
☑Trails
Trails need more CPU

Click on a plane!

Image Landsat
© 2013 Google
Image Landsat

37°37'51.23" N 122°23'01.74" W elev 1 ft eye alt 1164 ft



Welcome to Aviation Mapper

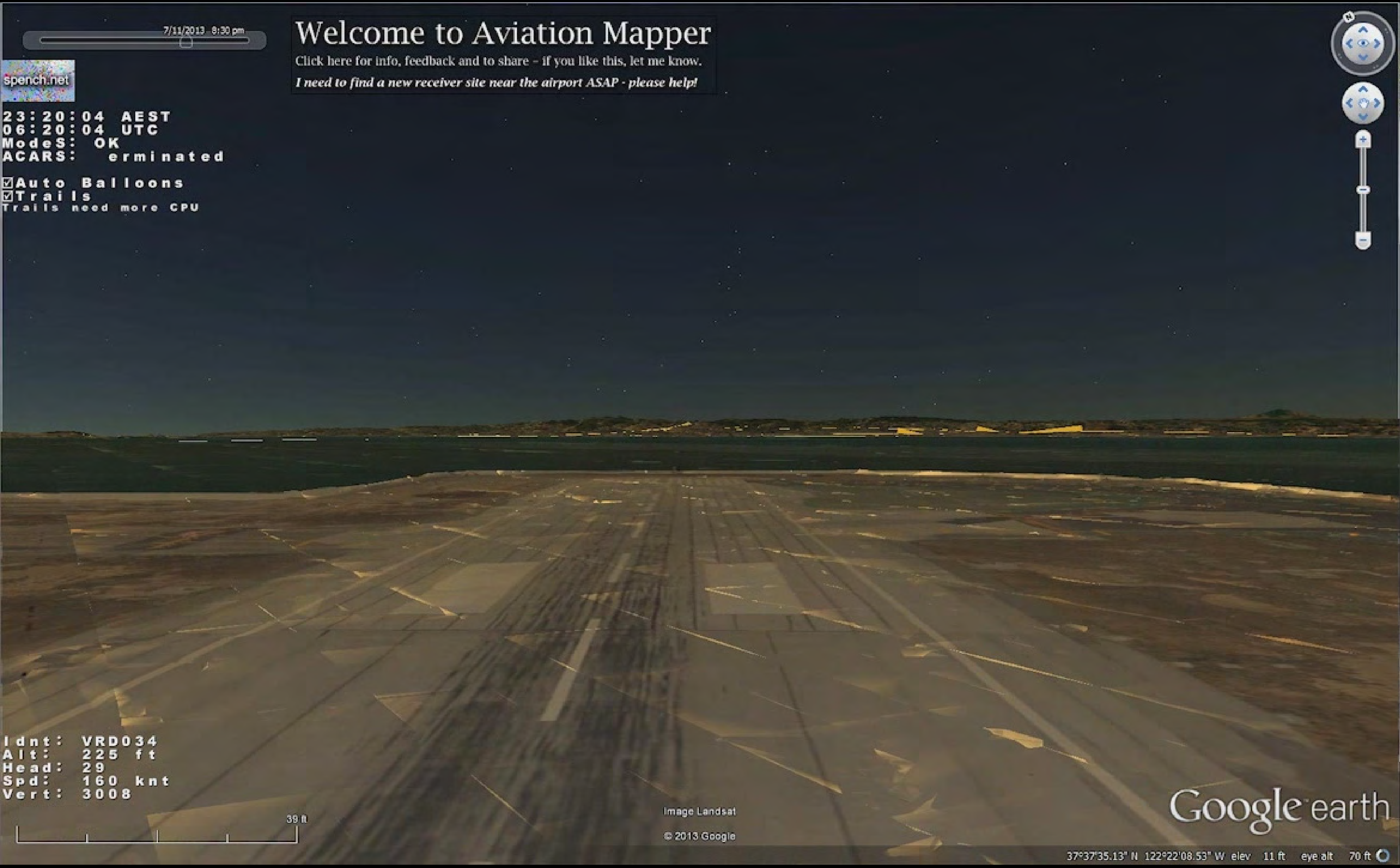
Click here for info, feedback and to share – if you like this, let me know.

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

23:19:22 AEST
06:19:22 UTC
ModeS: OK
ACARS: Terminated

☑Auto Balloons
☑Trails
Trails need more CPU

Click on a plane!



Welcome to Aviation Mapper

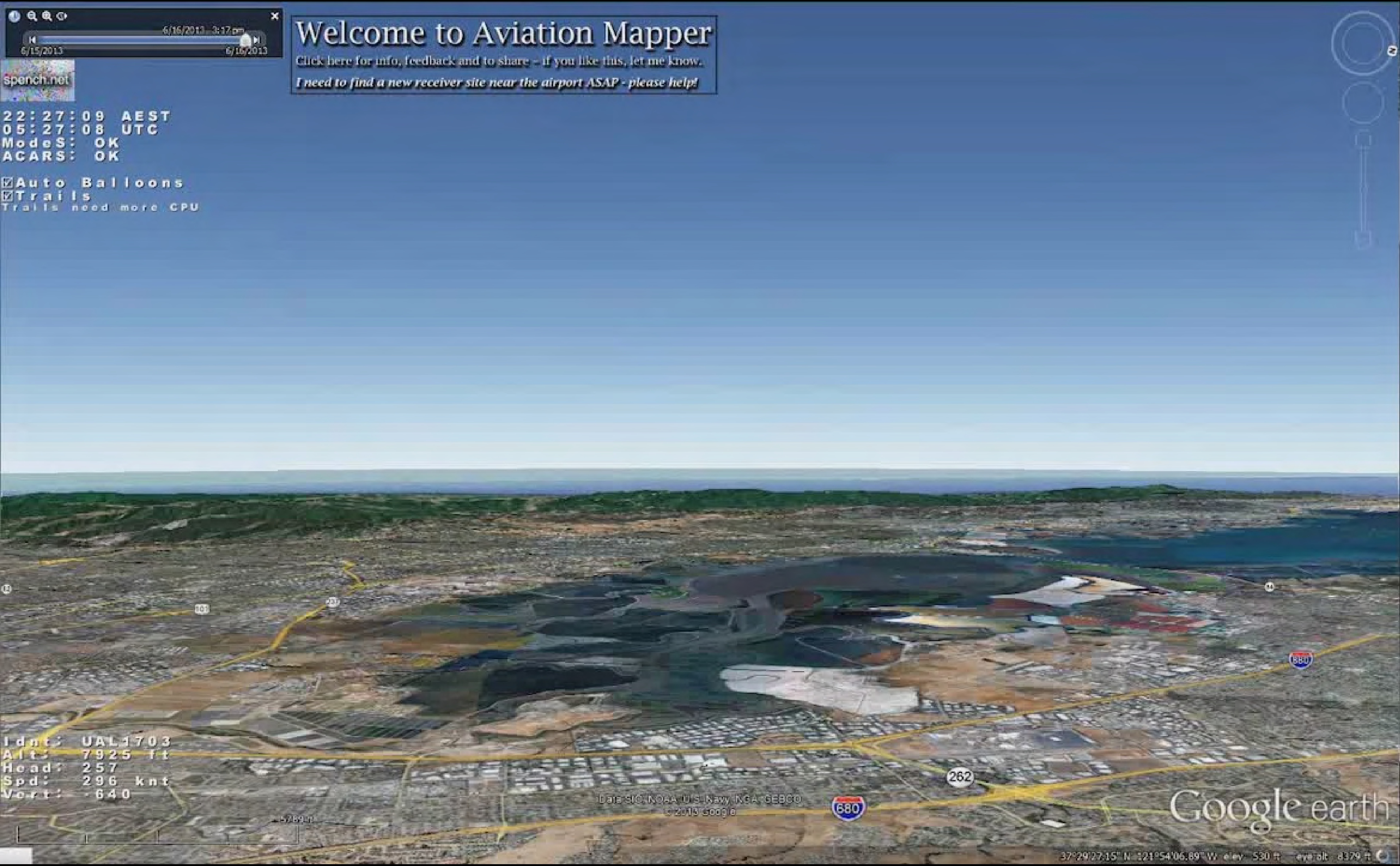
Click here for info, feedback and to share – if you like this, let me know.

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

```
23:20:04 AEST
06:20:04 UTC
ModeS:  OK
ACARS:   erminated

☑Auto Balloons
☑Trails
Trails need more CPU
```

```
Idnt:  VRD034
Alt:   225 ft
Head:  29
Spd:   160 knt
Vert:  3008
```

37°37'35.13" N 122°22'08.53" W elev 11 ft eye alt 70 ft



Welcome to Aviation Mapper

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

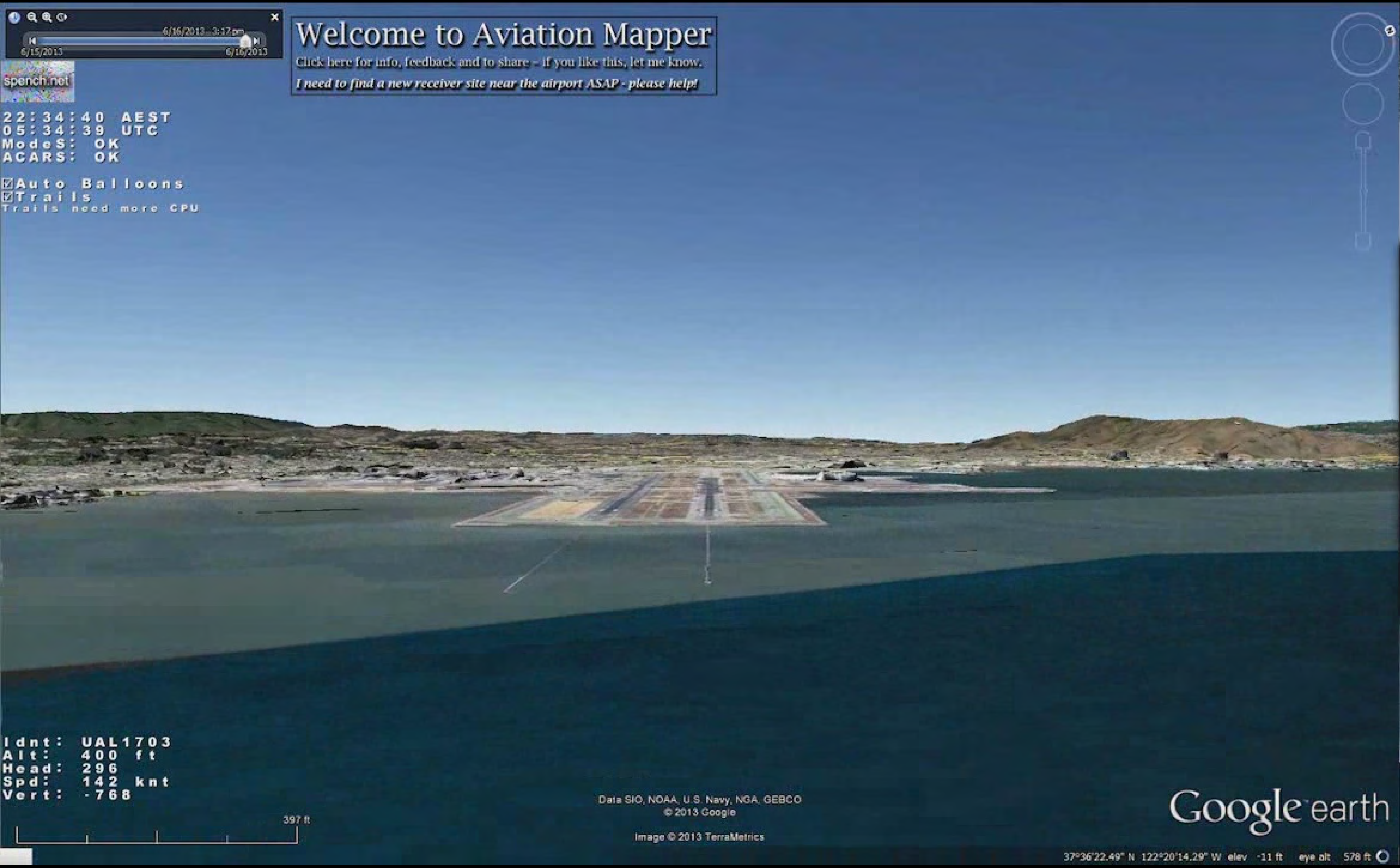
I need to find a new receiver site near the airport ASAP - please help!

```
22:27:09 AEST
05:27:08 UTC
ModeS:  OK
ACARS:  OK

☑Auto Balloons
☑Trails
Trails need more CPU
```

```
Idnt:   UAL1703
Alt:    7925 ft
Head:   257
Spd:    296 knt
Vert:   -640
```

Data SIO, NOAA, U.S. Navy, NGA, GEBCO
© 2013 Google

37°29'27.15" N 121°54'06.89" W elev 530 ft eye alt 8379 ft



Welcome to Aviation Mapper

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

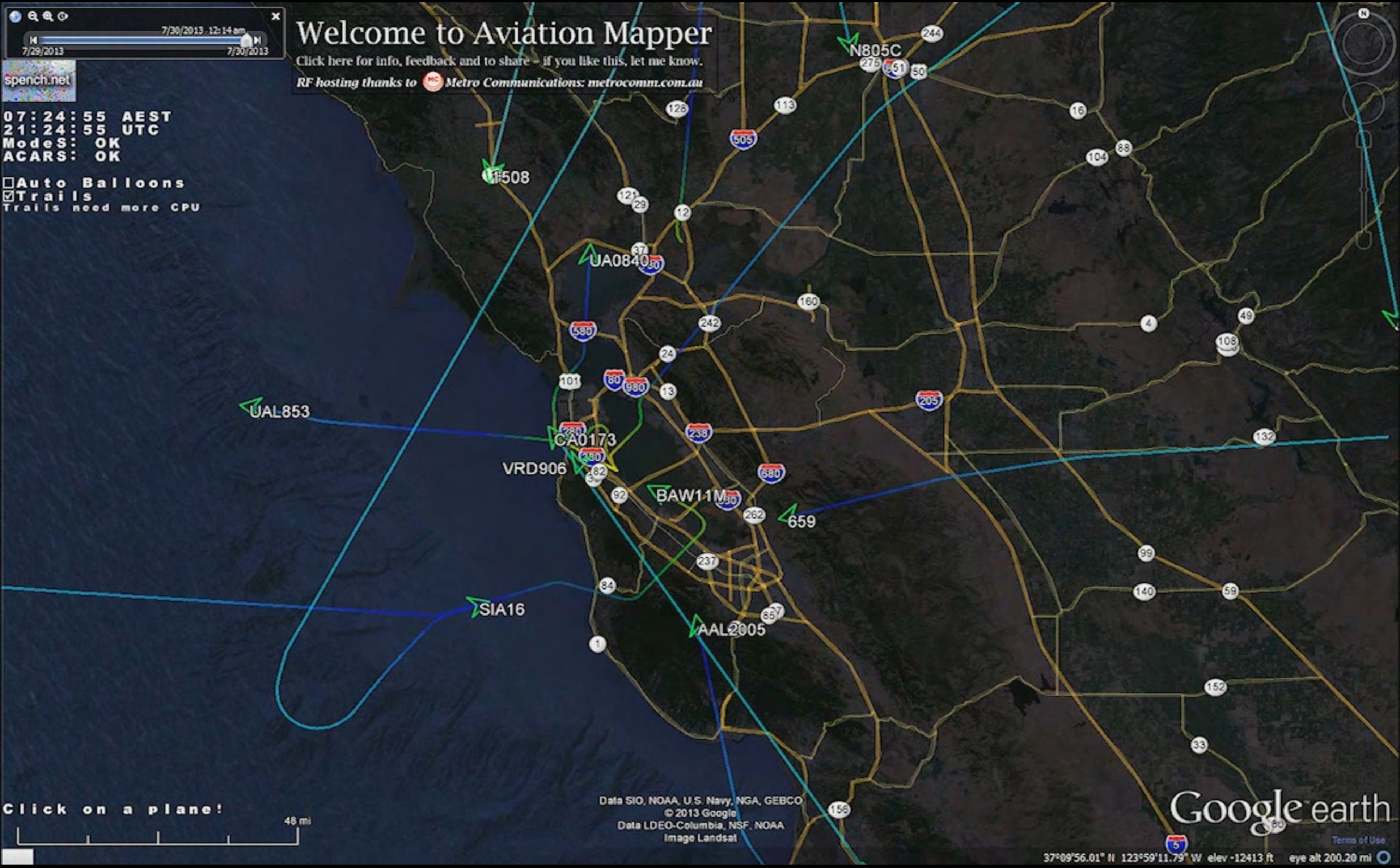
I need to find a new receiver site near the airport ASAP - please help!

22:34:40 AEST
05:34:39 UTC
ModeS: OK
ACARS: OK

☑Auto Balloons
☑Trails
Trails need more CPU

Idnt: UAL1703
Alt: 400 ft
Head: 296
Spd: 142 knt
Vert: -768

6/16/2013 3:17 pm
6/15/2013
6/16/2013
spench.net
397 ft
Data SIO, NOAA, U.S. Navy, NGA, GEBCO
© 2013 Google
Image © 2013 TerraMetrics
Google earth
37°36'22.49" N 122°20'14.29" W elev -11 ft eye alt 578 ft



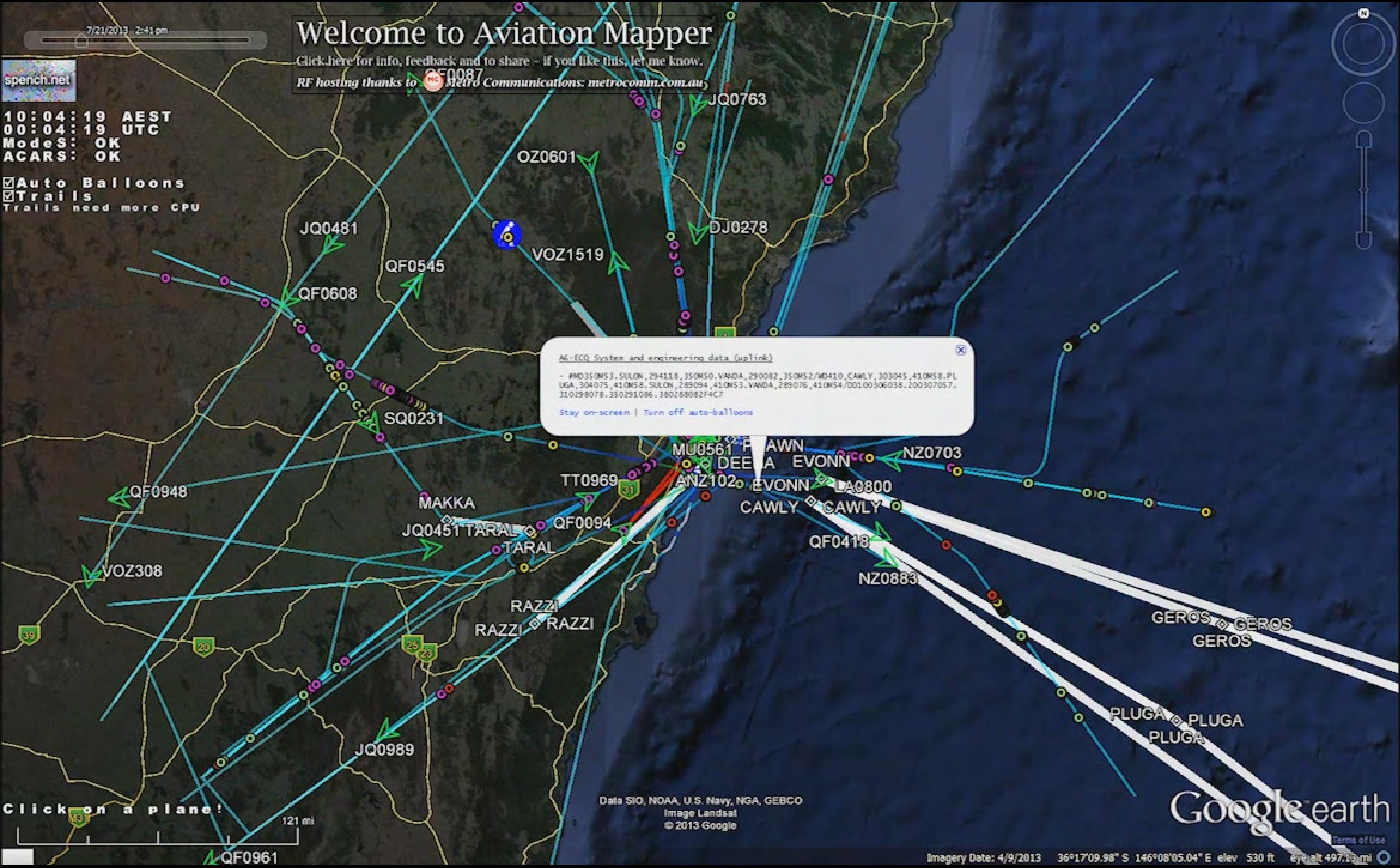
Welcome to Aviation Mapper

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

RF hosting thanks to Metro Communications: metrocomm.com.au

```
07:24:55 AEST
21:24:55 UTC
ModeS: OK
ACARS: OK
□Auto Balloons
☑Trails
Trails need more CPU
```

Click on a plane!



Welcome to Aviation Mapper

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

RF hosting thanks to Metro Communications: metrocomm.com.au

```
10:04:19 AEST
00:04:19 UTC
ModeS:  OK
ACARS:  OK
☑Auto Balloons
☑Trails
Trails need more CPU
```

A6-ECQ System and engineering data (uplink)

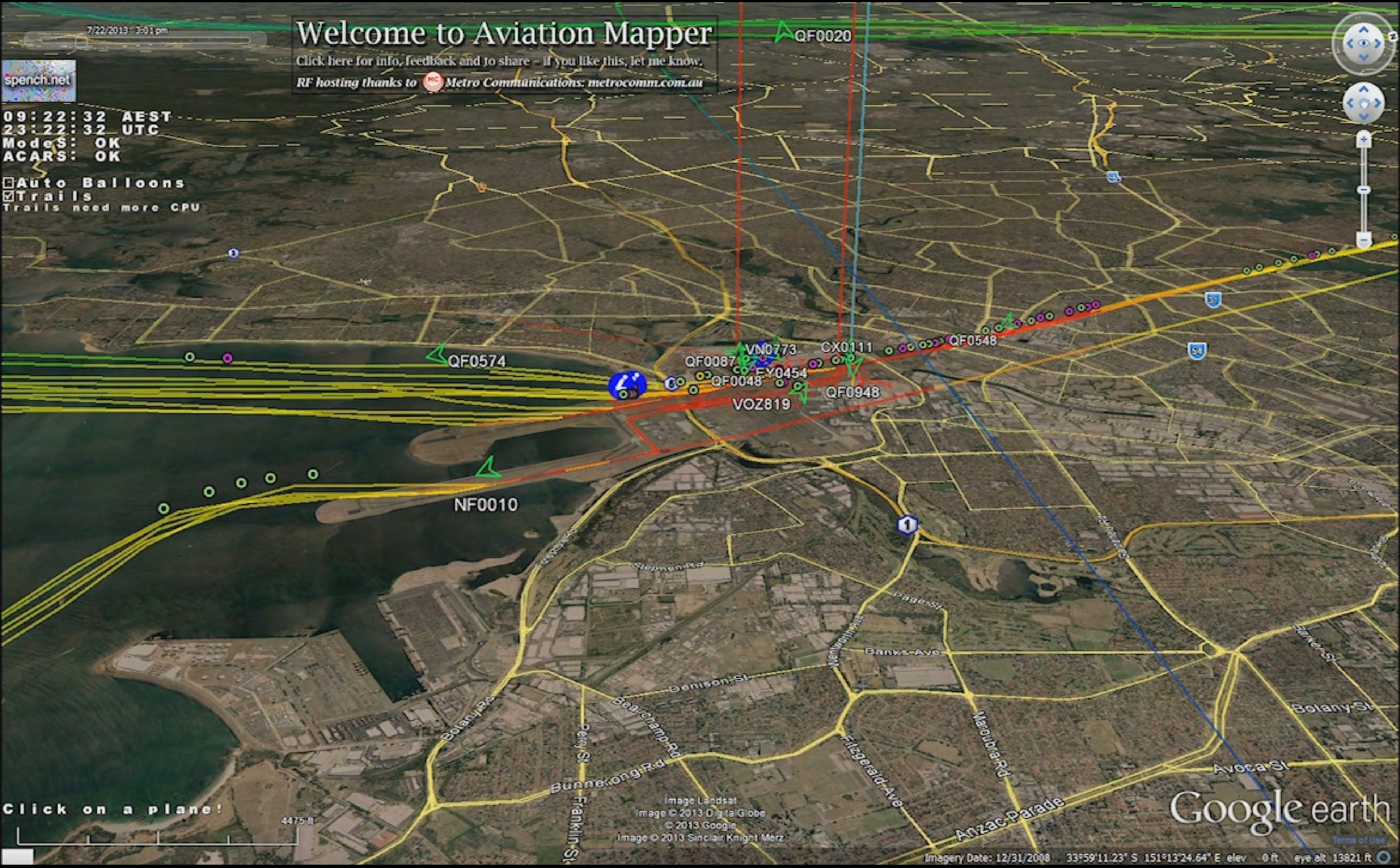
```
- #MD350M53.SULON,294118,350M50.VANDA,290082,350M52/MD410,CAWLY,303045,410M58.PL
UGA,304075,410M58.SULON,289094,410M53.VANDA,289076,410M54/DD100306038.200307057.
310298078.350291086.380288082F4C7
```

Stay on-screen | Turn off auto-balloons

Click on a plane!

Data SIO, NOAA, U.S. Navy, NGA, GEBCO
Image Landsat
© 2013 Google

Imagery Date: 4/9/2013   36°17'09.98" S 146°08'05.04" E elev 530 ft   eye alt 497.13 mi



Welcome to Aviation Mapper

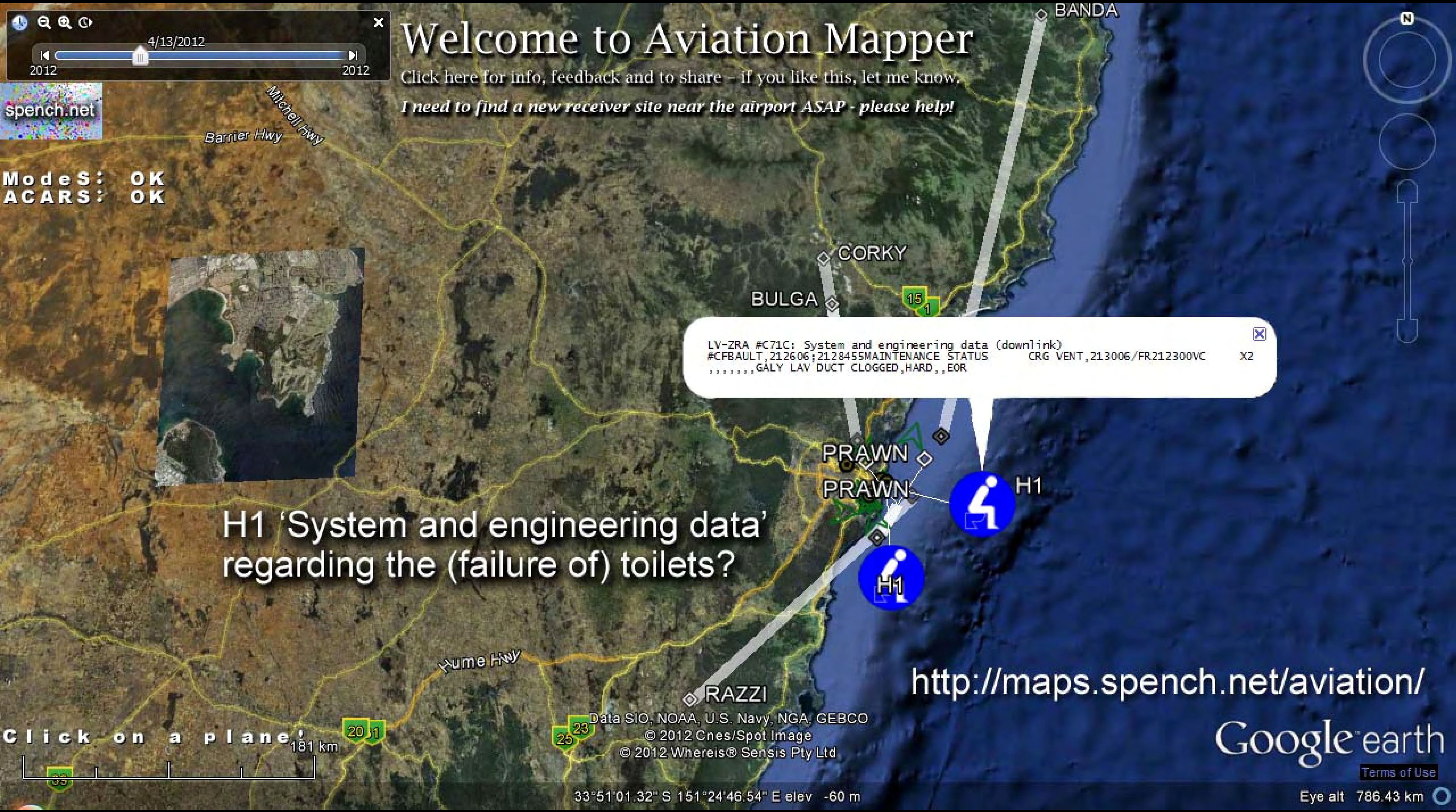
Click here for info, feedback and to share - if you like this, let me know.

RF hosting thanks to Metro Communications: metrocomm.com.au

```
09:22:32 AEST
23:22:32 UTC
ModeS:  OK
ACARS:  OK

□Auto Balloons
☑Trails
Trails need more CPU
```

Click on a plane!

Imagery Date: 12/31/2008   33°59'11.23" S 151°13'24.64" E elev 0 ft   eye alt 13821 ft

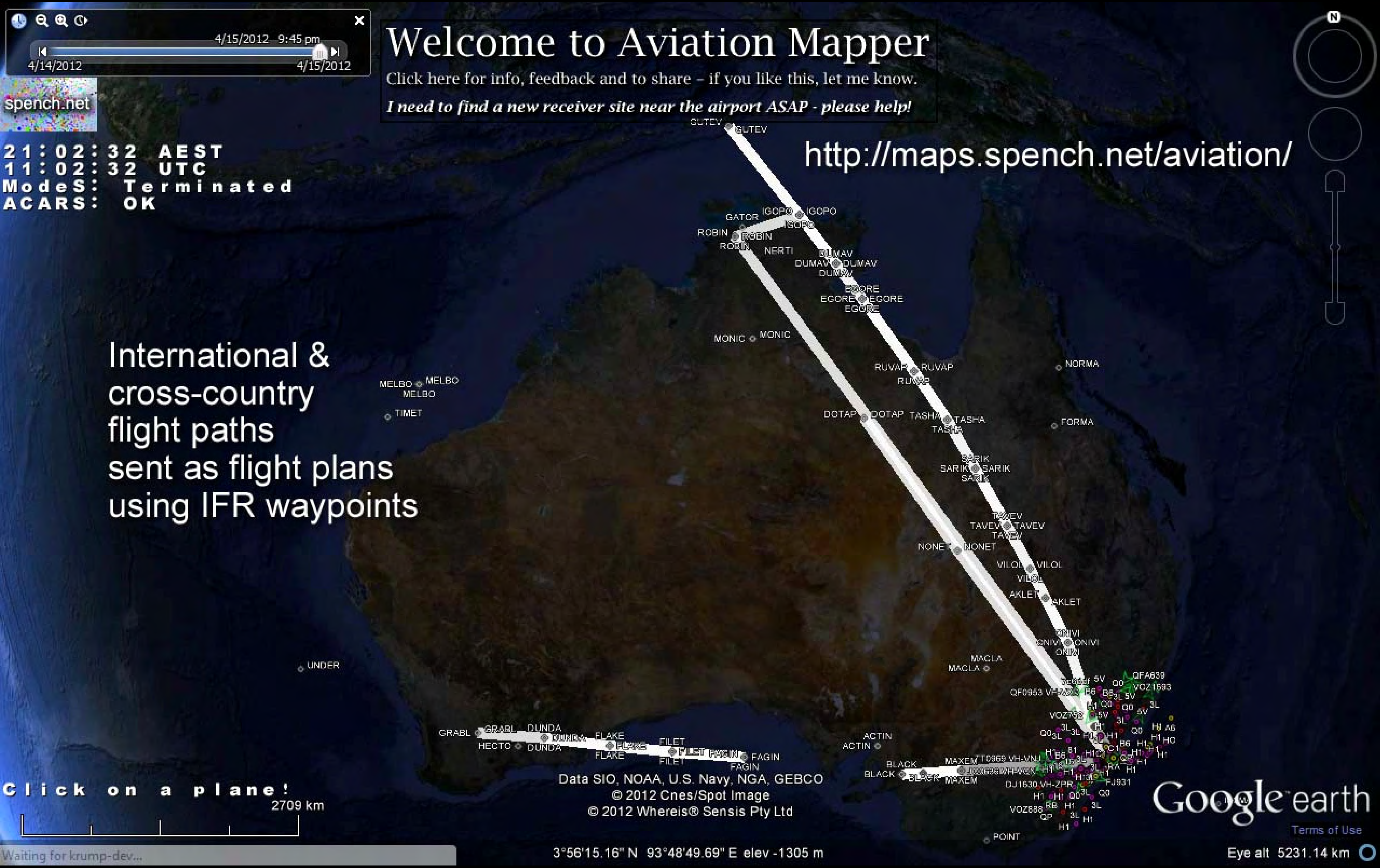


4/13/2012
2012
2012
spench.net
Welcome to Aviation Mapper
Click here for info, feedback and to share – if you like this, let me know.
I need to find a new receiver site near the airport ASAP - please help!
Mode S: OK
ACARS: OK
Mitchell Hwy
Barrier Hwy
BANDA
CORKY
BULGA
PRAWN
PRAWN
H1
H1
Hume Hwy
RAZZI
Click on a plane!
181 km
Data SIO, NOAA, U.S. Navy, NGA, GEBCO
© 2012 Cnes/Spot Image
© 2012 Whereis® Sensis Pty Ltd
Google earth
Terms of Use
33°51'01.32" S 151°24'46.54" E elev -60 m
Eye alt 786.43 km

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

H1 'System and engineering data' regarding the (failure of) toilets?

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



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/

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

4/15/2012 9:45 pm

4/14/2012 4/15/2012

spench.net

```
21:02:32 AEST
11:02:32 UTC
ModeS: Terminated
ACARS: OK
```

Click on a plane!

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

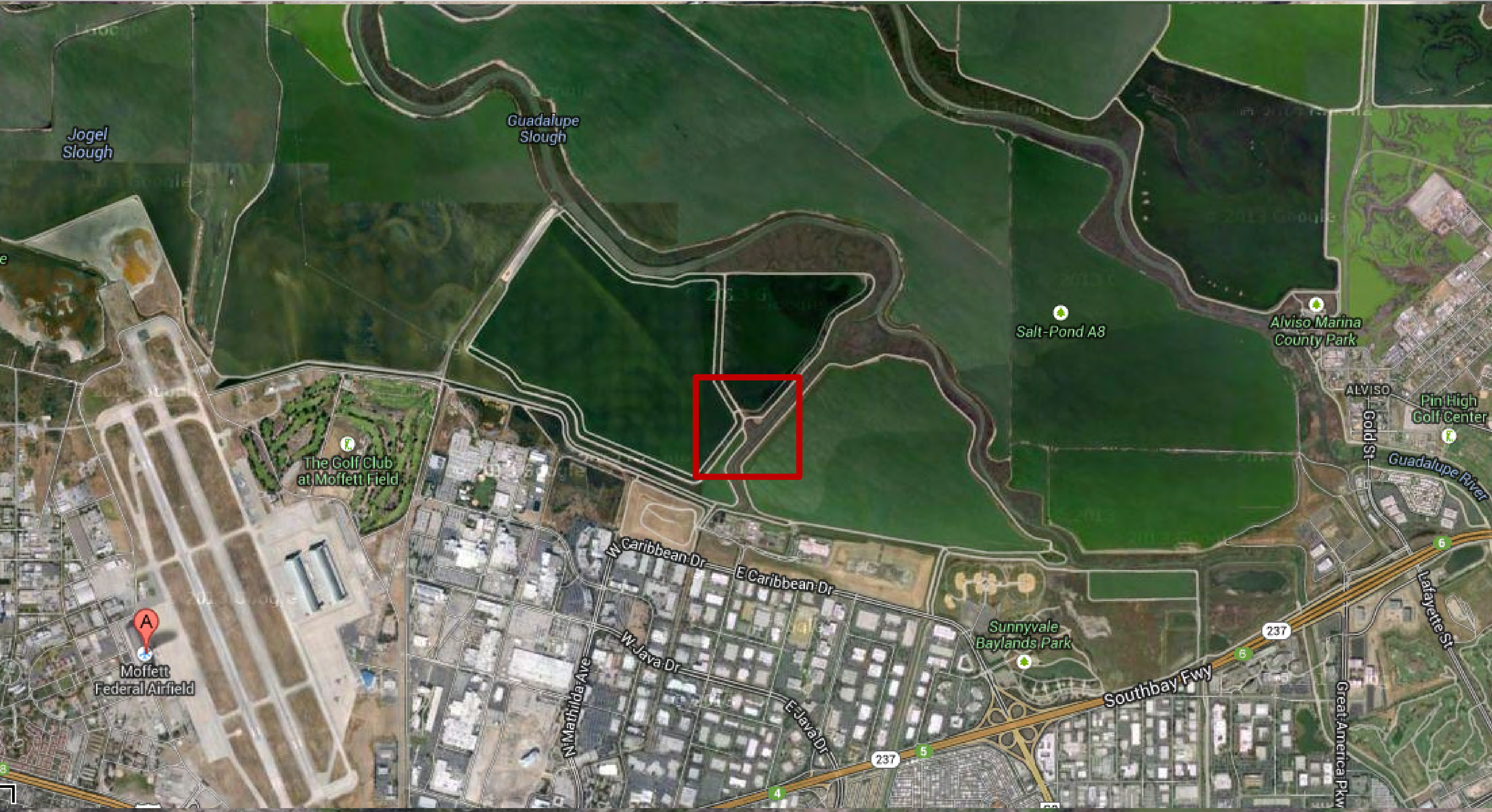
Waiting for krump-dev...

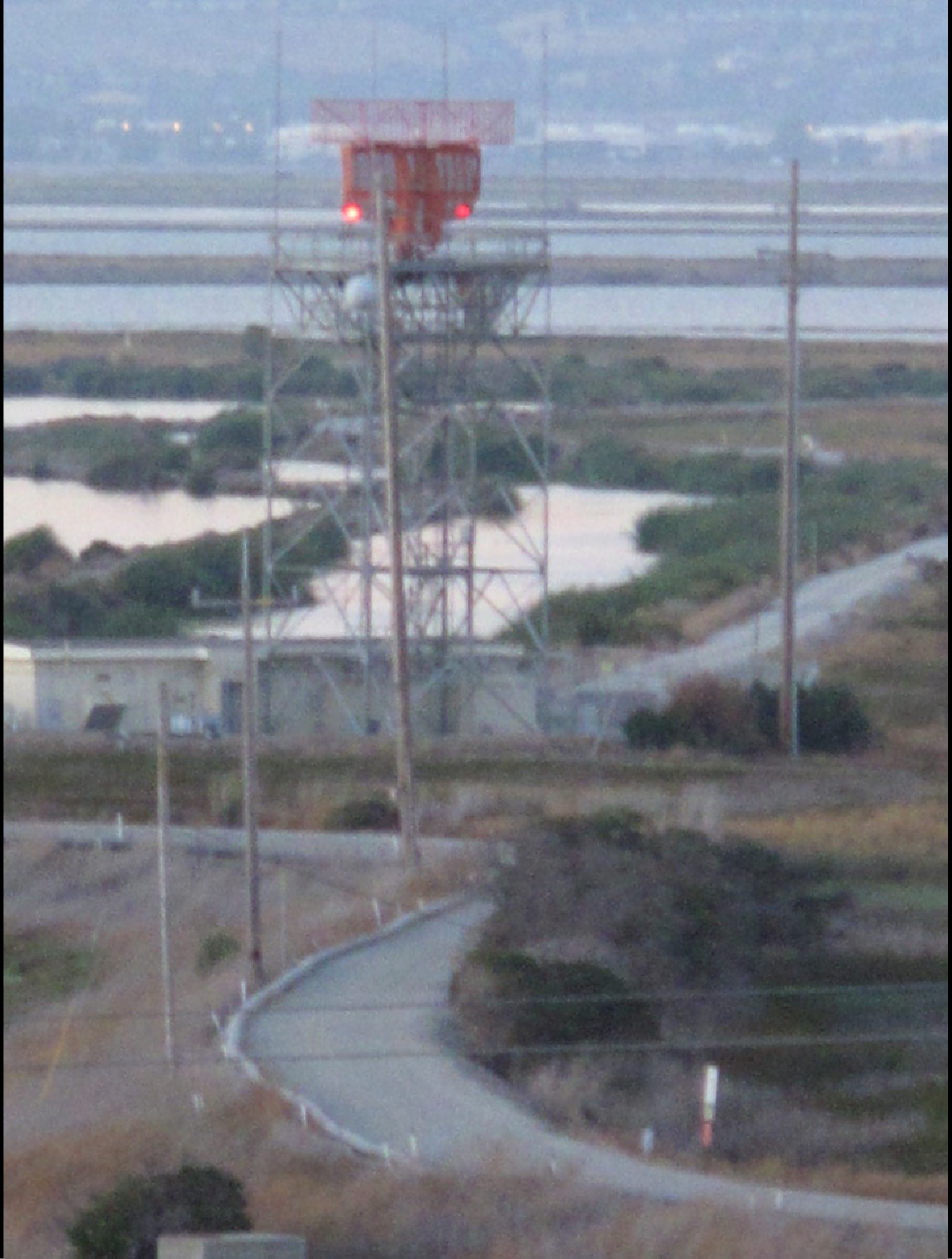
3°56'15.16" N 93°48'49.69" E elev -1305 m

Eye alt 5231.14 km

Primary Surveillance RADAR

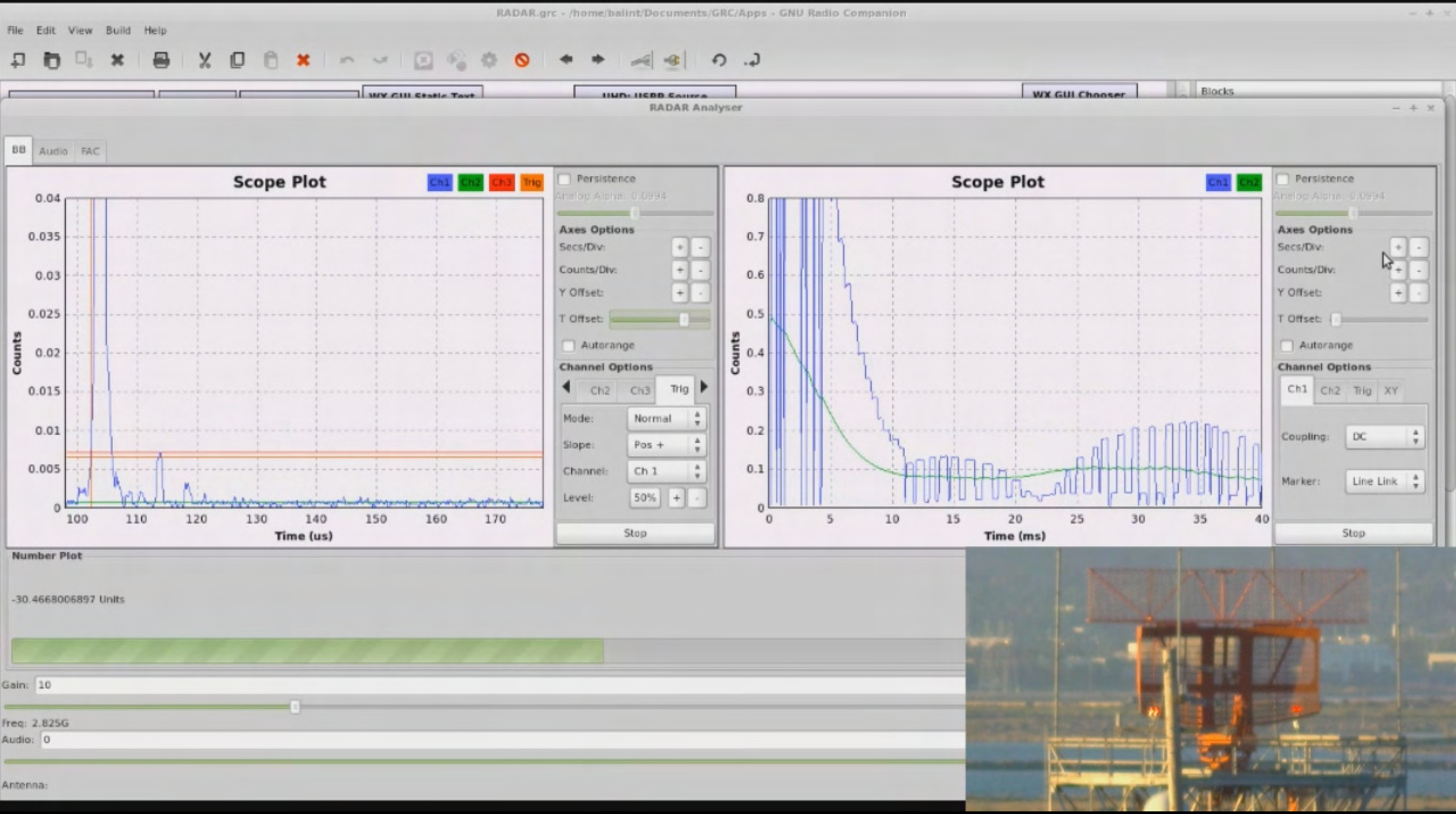
Moffett Field ASR-9





Primary Surveillance RADAR

Primary Surveillance RADAR



RADAR.grc - /home/balint/Documents/GRC/Apps - GNU Radio Companion

RADAR Analyser

Mode: Normal

Slope: Pos +

Channel: Ch 1

Level: 50%

Coupling: DC

Marker: Line Link

Number Plot

-30.4668006897 Units

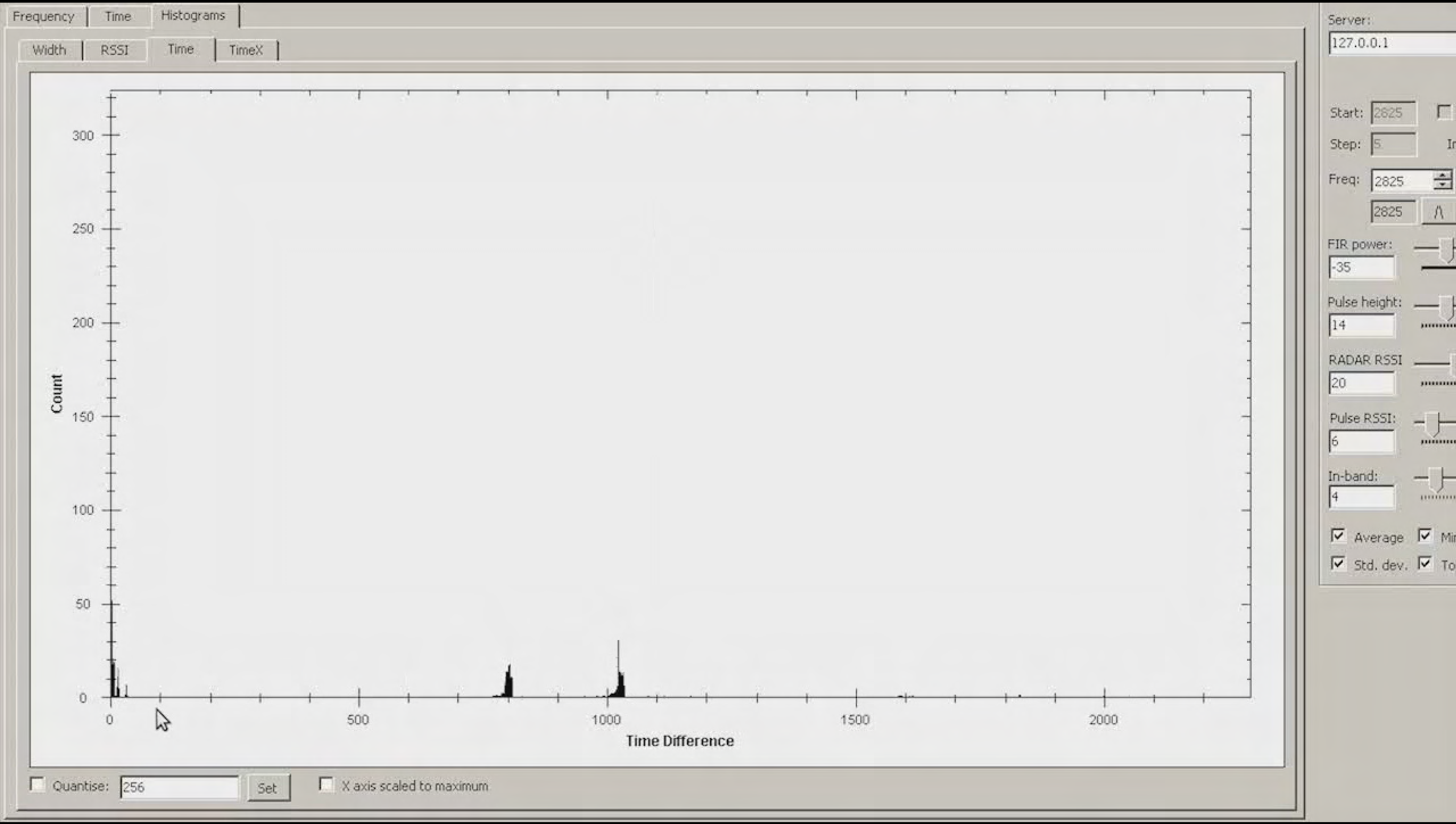
Gain: 10

Freq: 2.825G

Audio: 0

Antenna:

Primary Surveillance RADAR



Server: 127.0.0.1

Start: 2825 □

Step: 5

Freq: 2825

2825

FIR power: -35

Pulse height: 14

RADAR RSSI 20

Pulse RSSI: 6

In-band: 4

☑ Average ☑ Mi

☑ Std. dev. ☑ To

□ Quantise: 256

□ X axis scaled to maximum

Dual PRF Mode: Weather

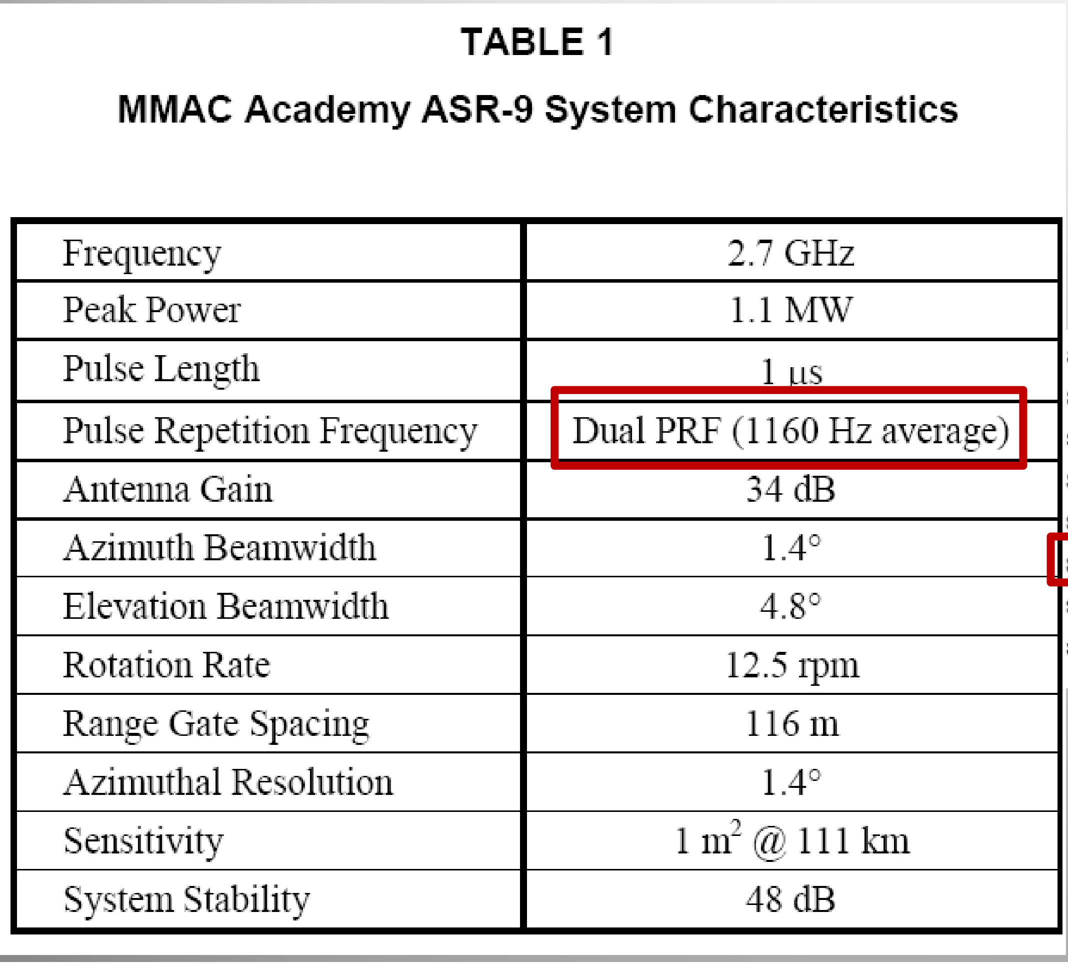
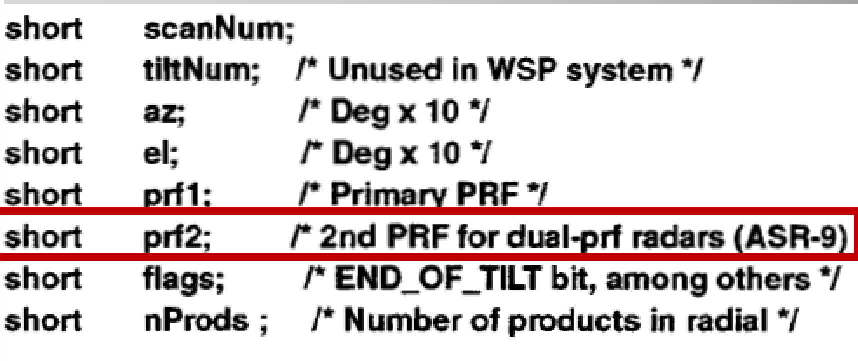


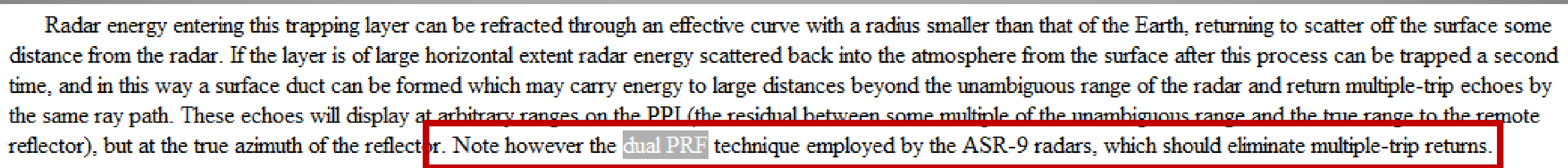
TABLE 1

MMAC Academy ASR-9 System Characteristics

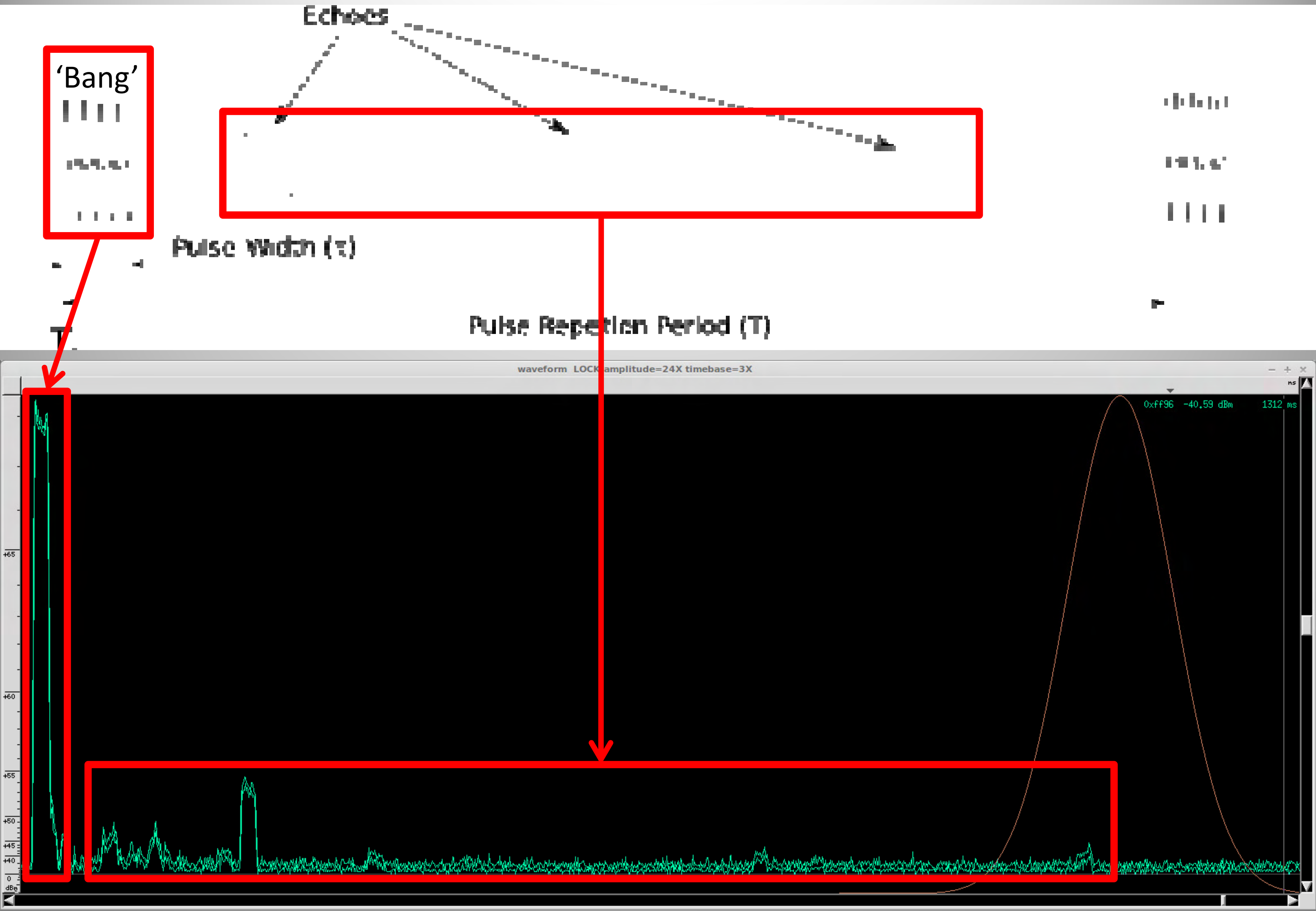
Frequency	2.7 GHz
Peak Power	1.1 MW
Pulse Length	1 µs
Pulse Repetition Frequency	Dual PRF (1160 Hz average)
Antenna Gain	34 dB
Azimuth Beamwidth	1.4°
Elevation Beamwidth	4.8°
Rotation Rate	12.5 rpm
Range Gate Spacing	116 m
Azimuthal Resolution	1.4°
Sensitivity	$1\ m^2$ @ 111 km
System Stability	48 dB



```
short     scanNum;
short     tiltNum;   /* Unused in WSP system */
short     az;        /* Deg x 10 */
short     el;        /* Deg x 10 */
short     prf1;      /* Primary PRF */
short     prf2;      /* 2nd PRF for dual-prf radars (ASR-9)
short     flags;     /* END_OF_TILT bit, among others */
short     nProds ;   /* Number of products in radial */
```



Radar energy entering this trapping layer can be refracted through an effective curve with a radius smaller than that of the Earth, returning to scatter off the surface some distance from the radar. If the layer is of large horizontal extent radar energy scattered back into the atmosphere from the surface after this process can be trapped a second time, and in this way a surface duct can be formed which may carry energy to large distances beyond the unambiguous range of the radar and return multiple-trip echoes by the same ray path. These echoes will display at arbitrary ranges on the PPI (the residual between some multiple of the unambiguous range and the true range to the remote reflector), but at the true azimuth of the reflector. Note however the dual PRF technique employed by the ASR-9 radars, which should eliminate multiple-trip returns.



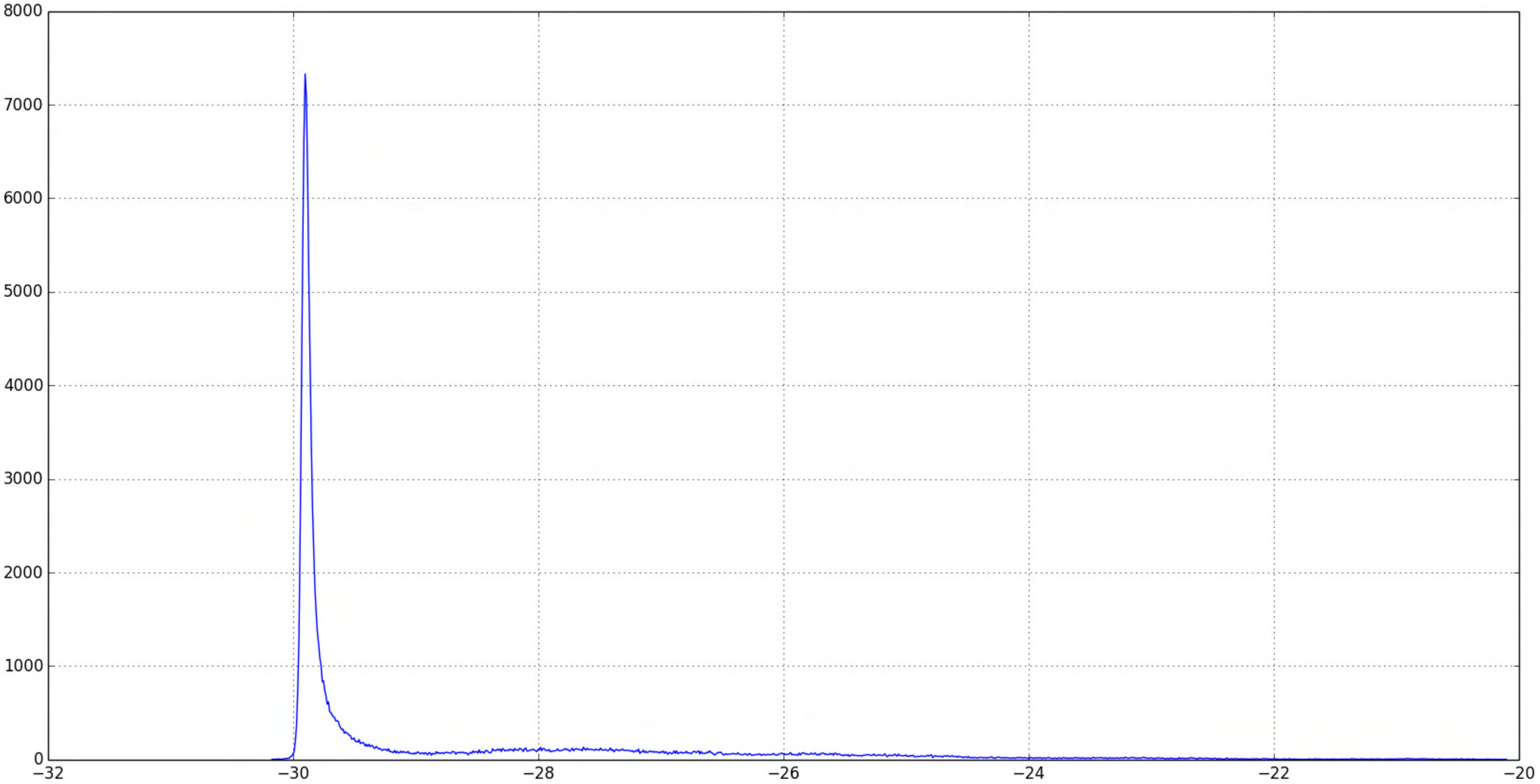
waveform LOCK amplitude=24X timebase=3X

0xff96 -40.59 dBm 1312 ms

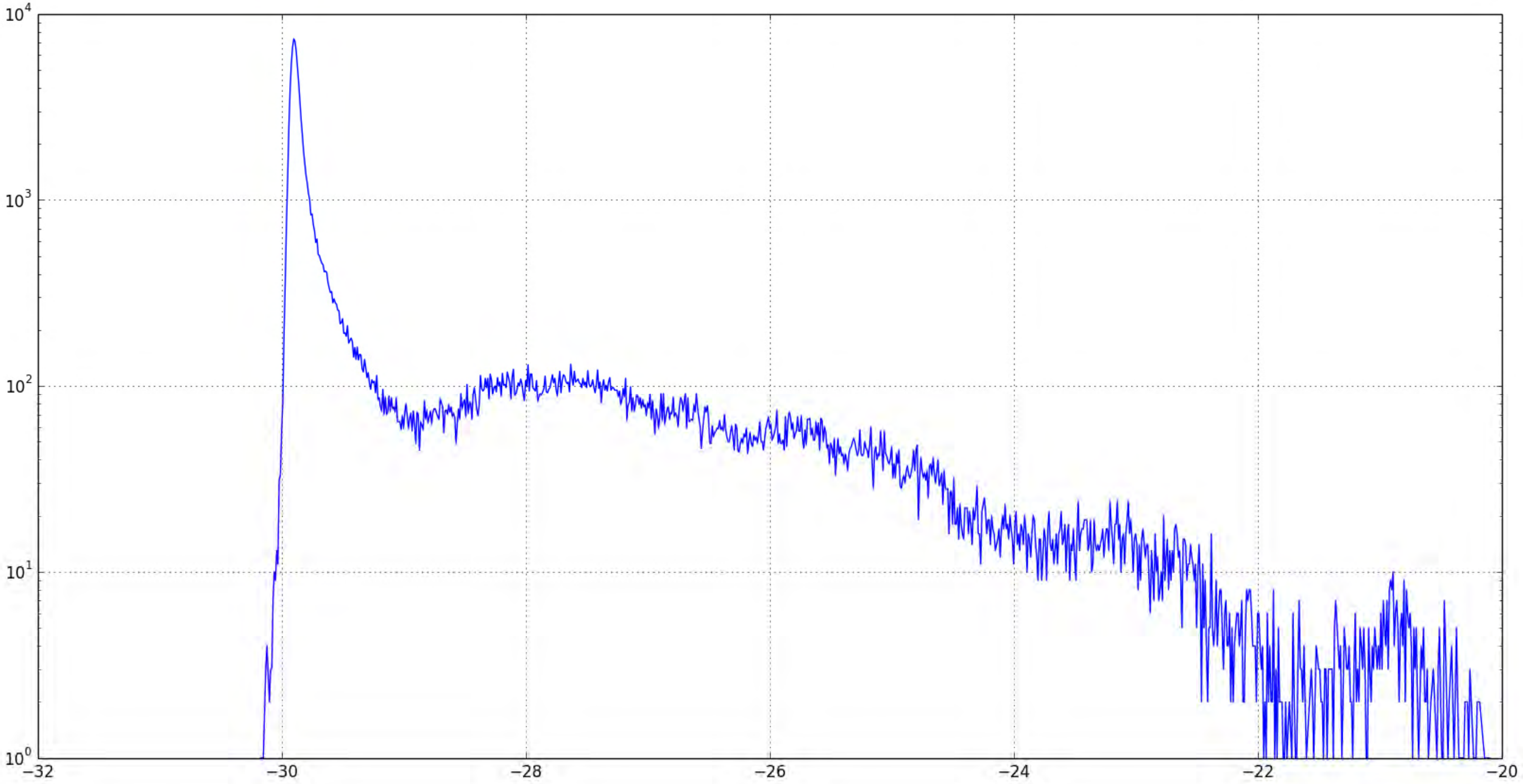
pple

GAP ATHLETIC
NATIONAL INSTRUMENTS

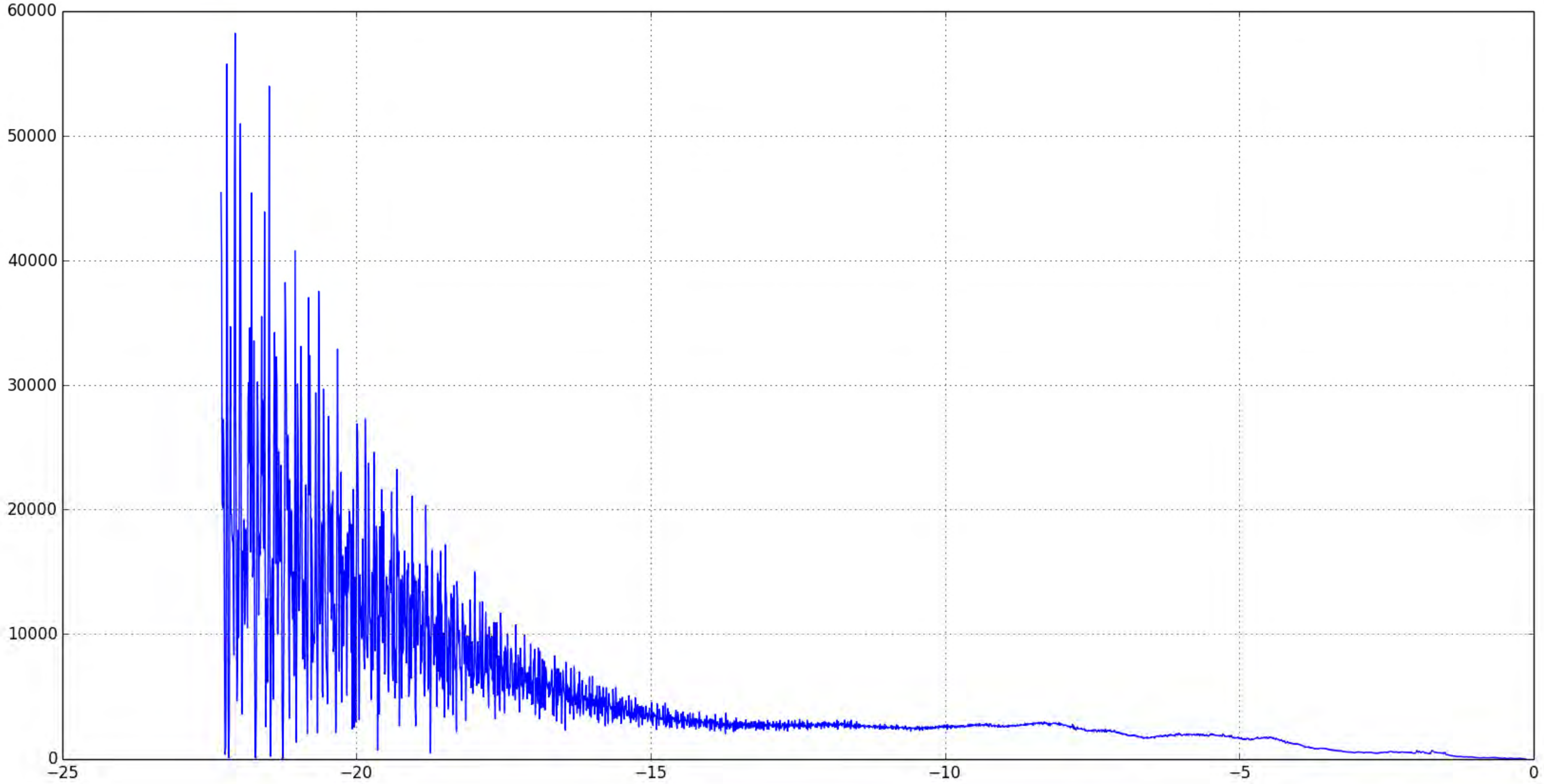
Magnitude Histogram



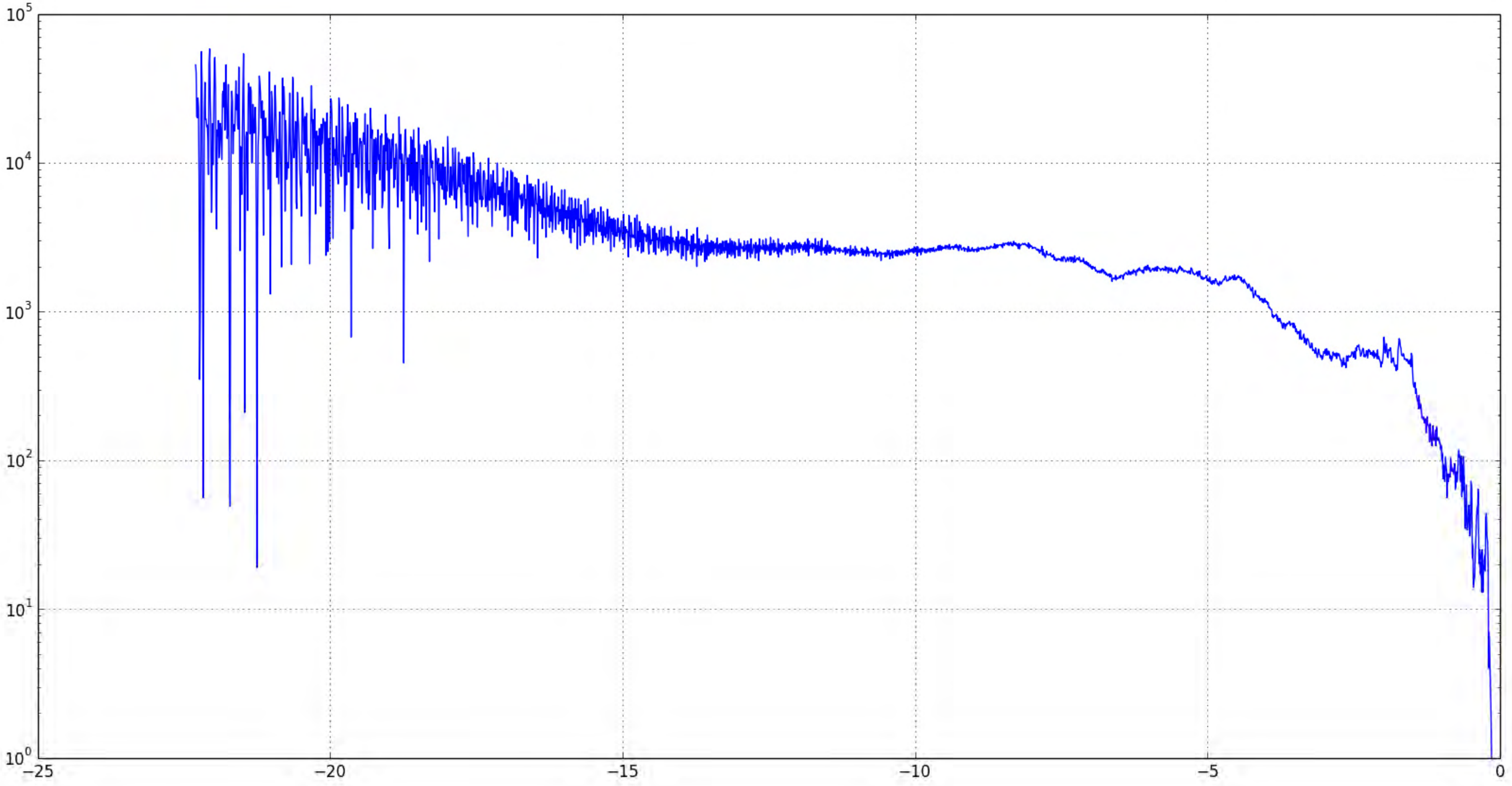
Magnitude Histogram



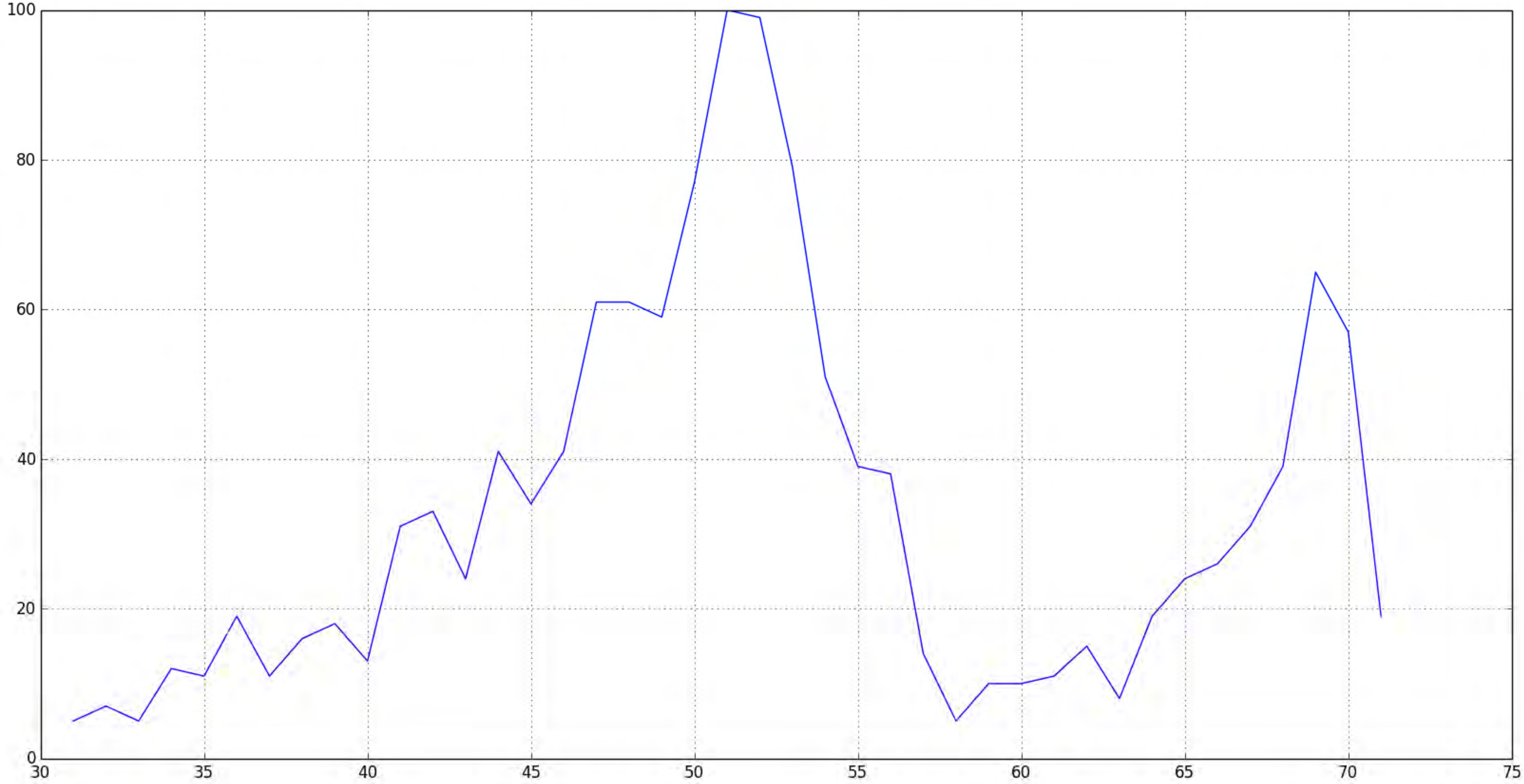
Above Noise Floor



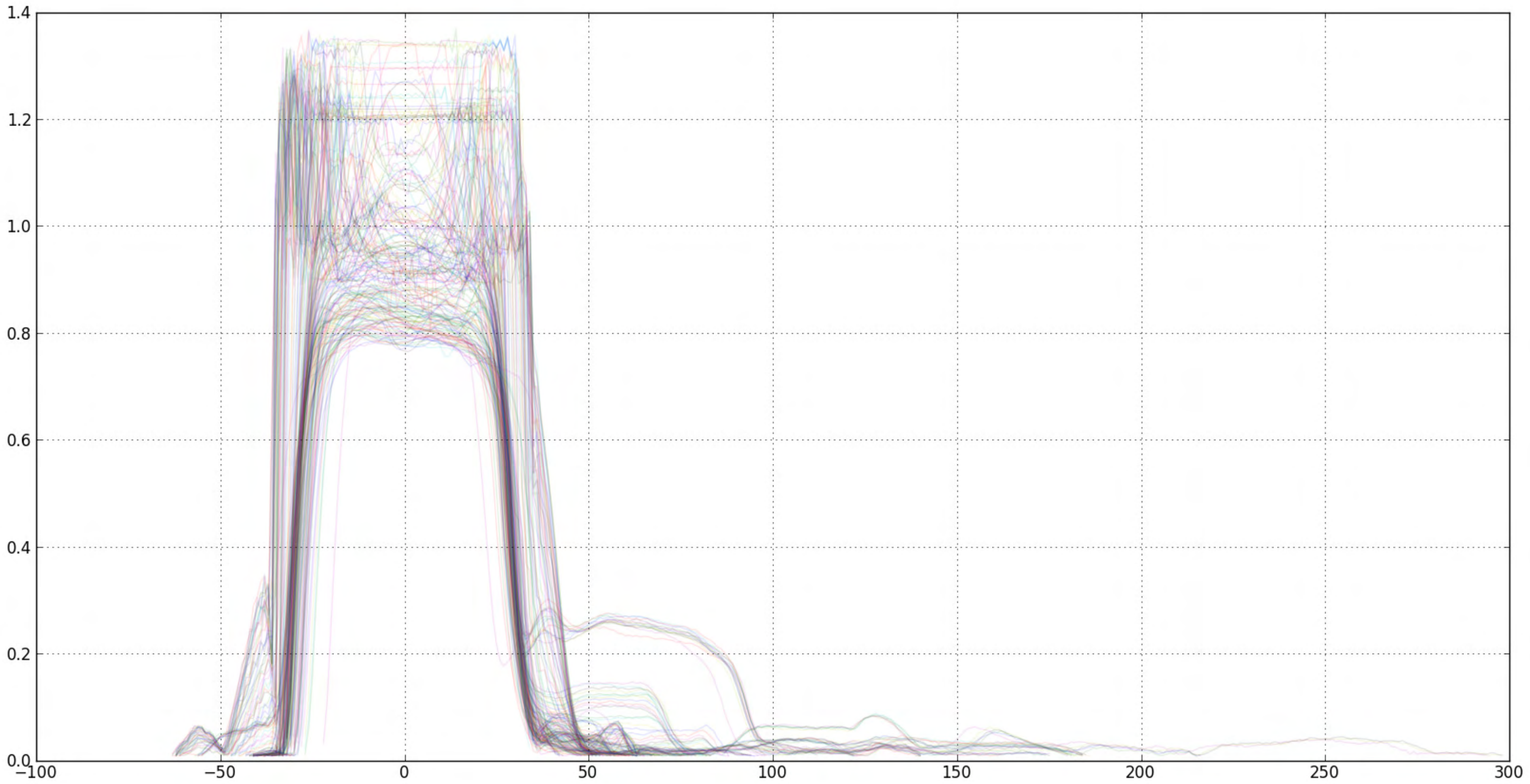
Above Noise Floor



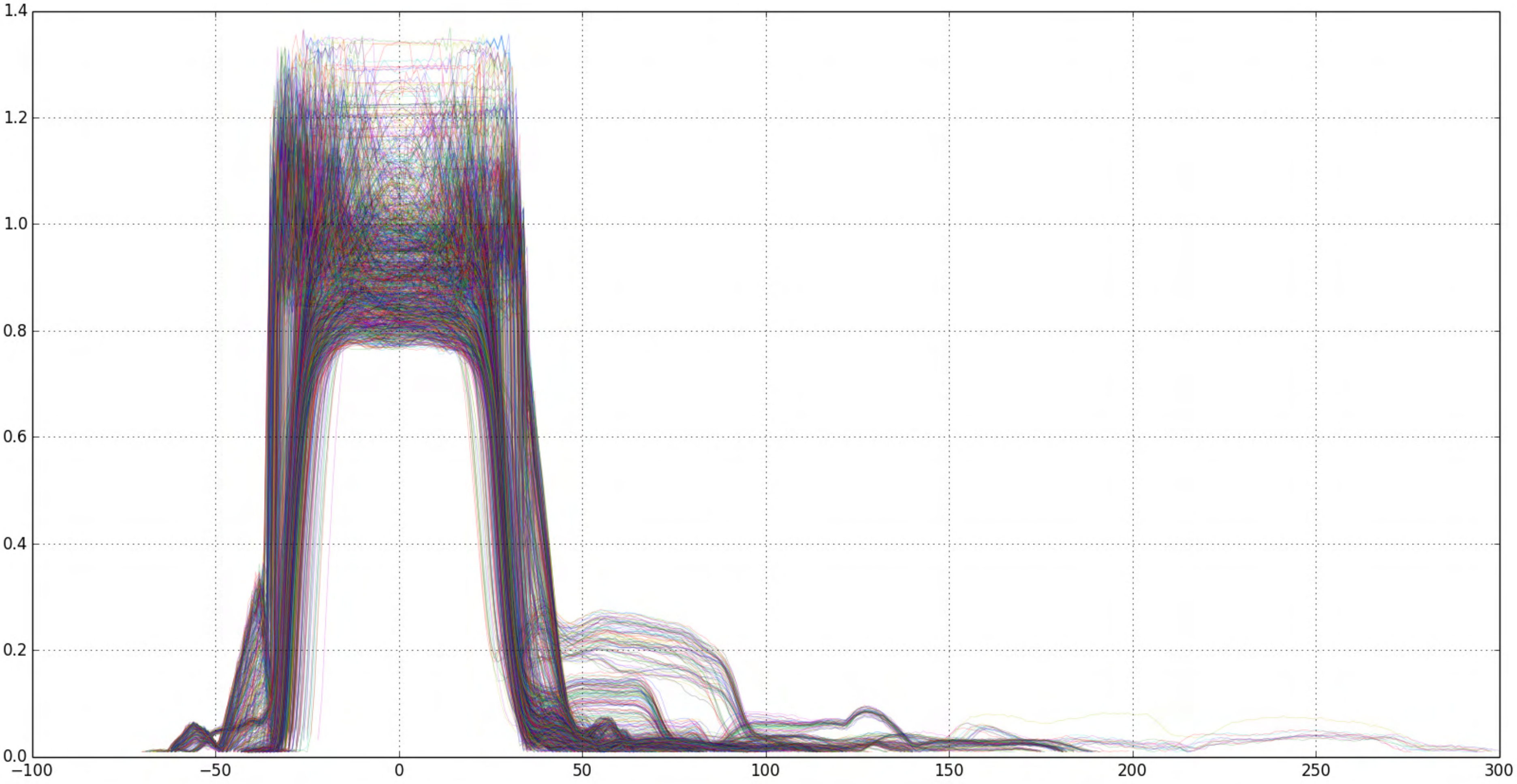
Pulse Length Histogram



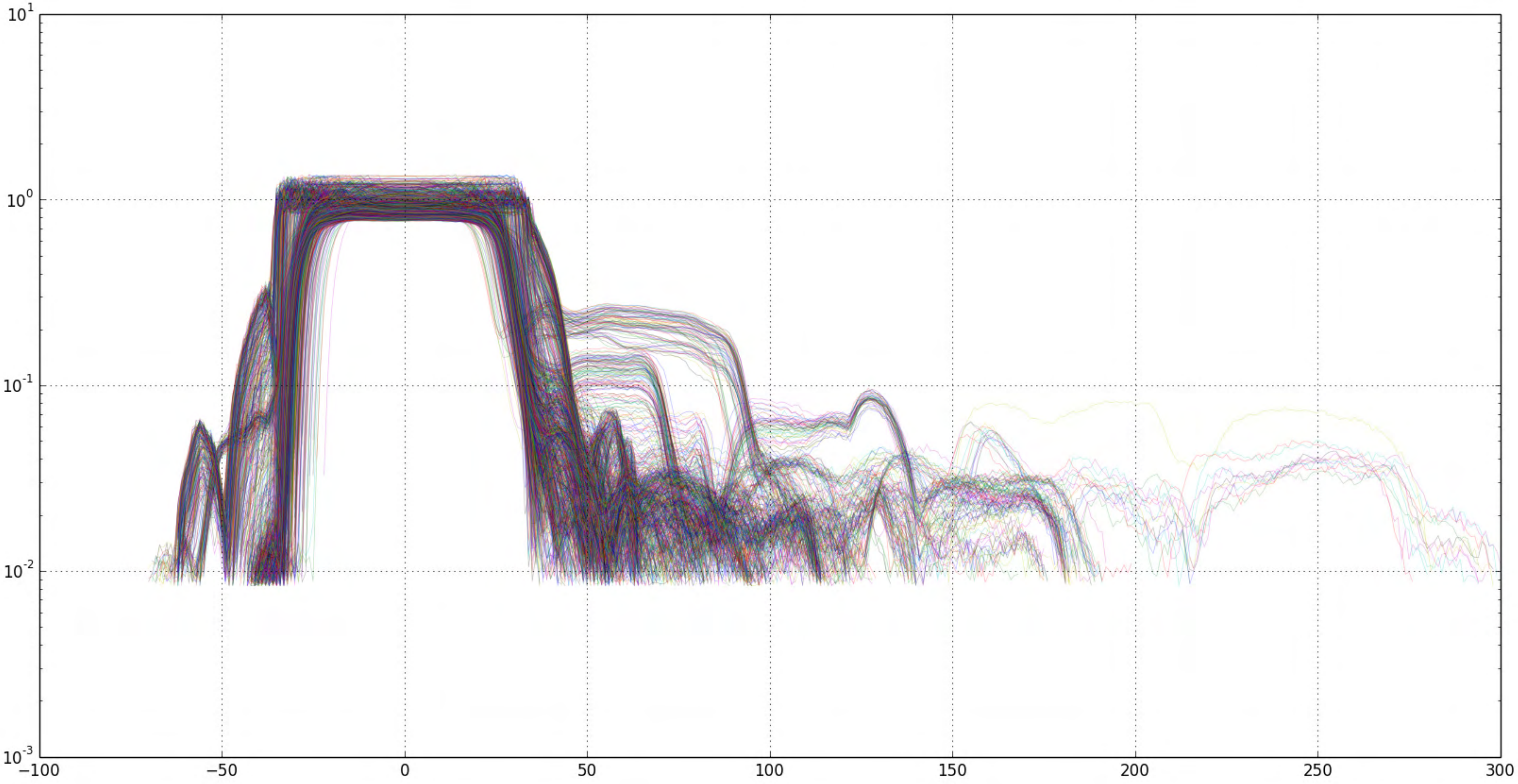
Pulse Envelope



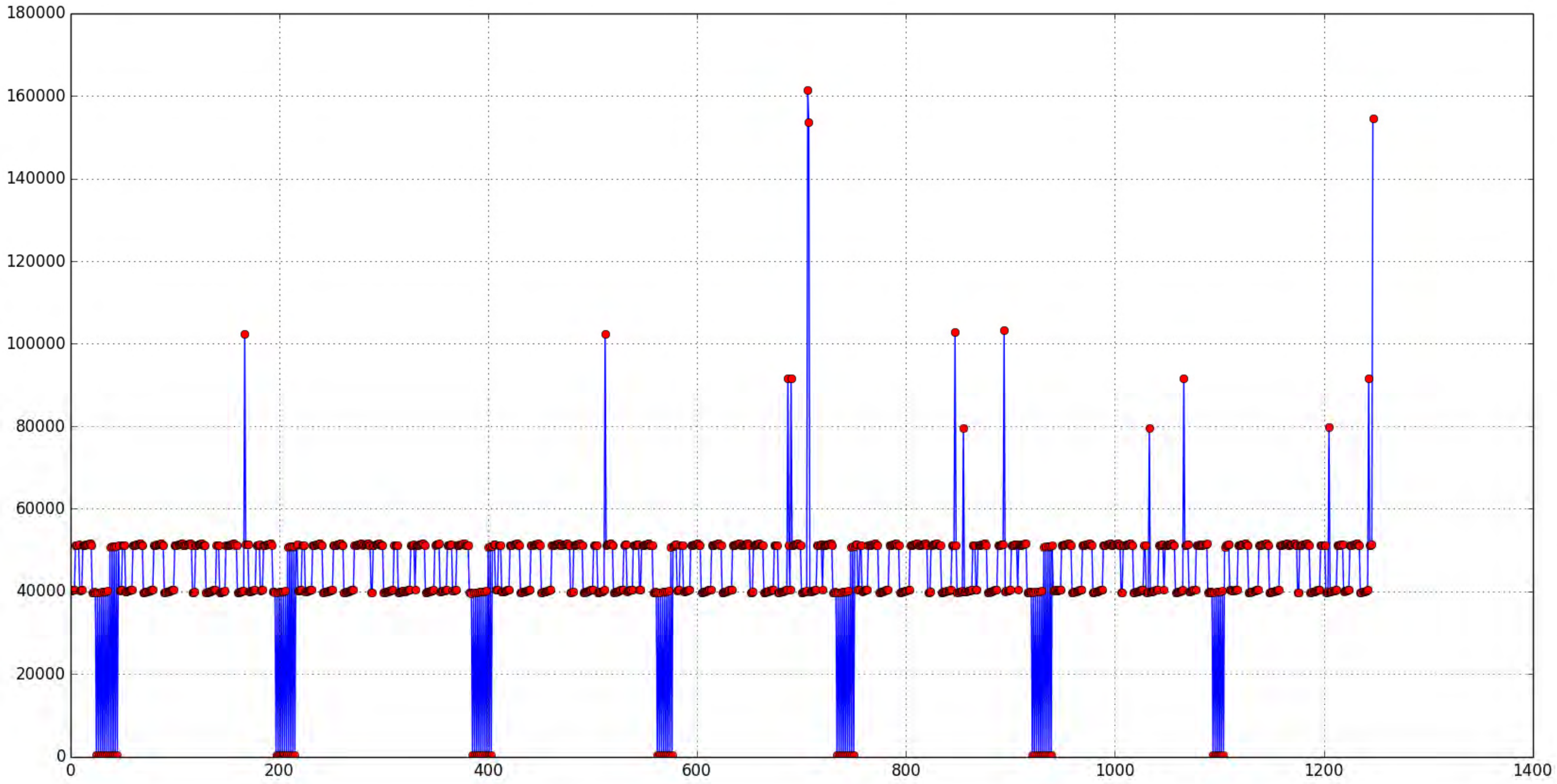
Pulse Envelope



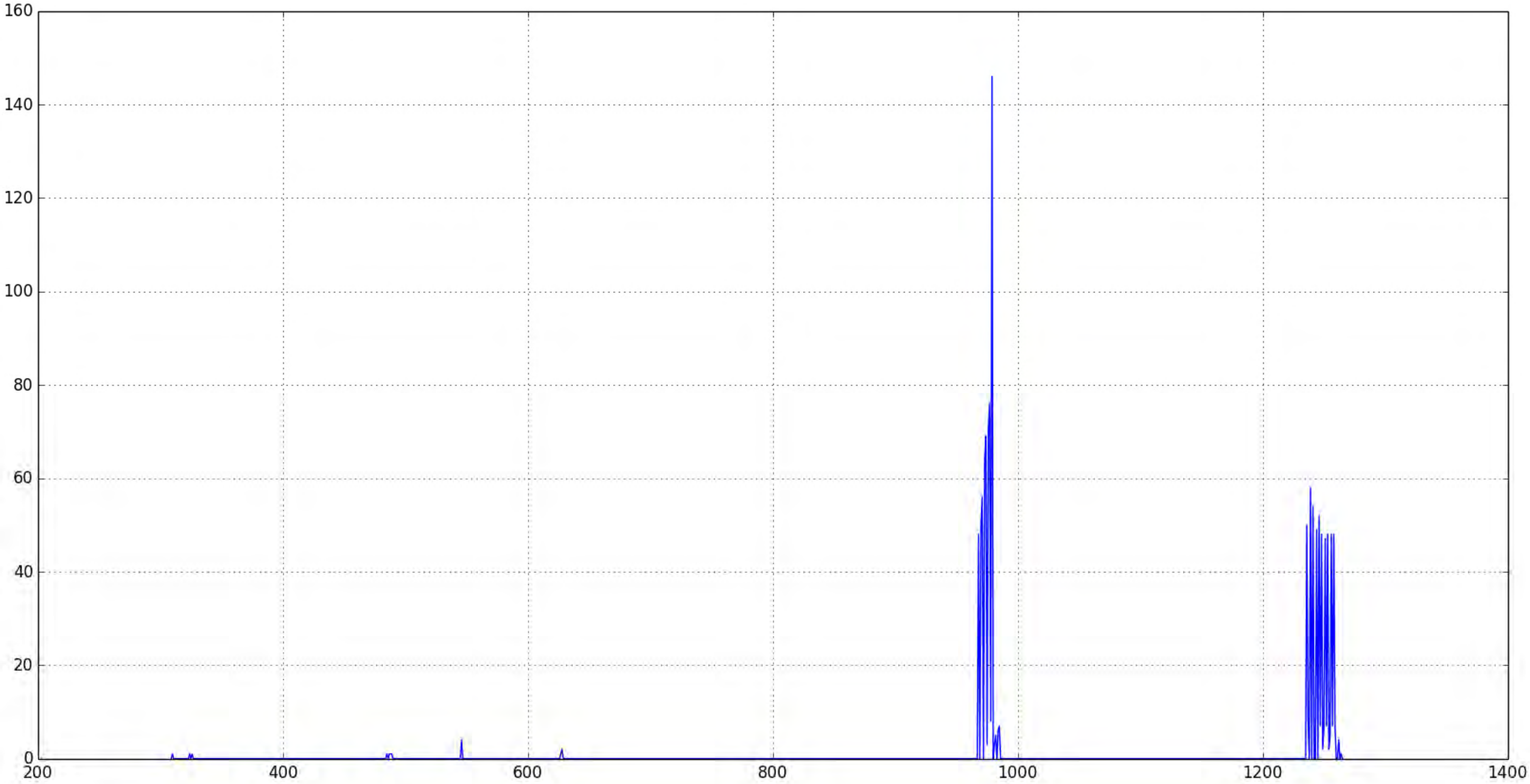
Pulse Envelope



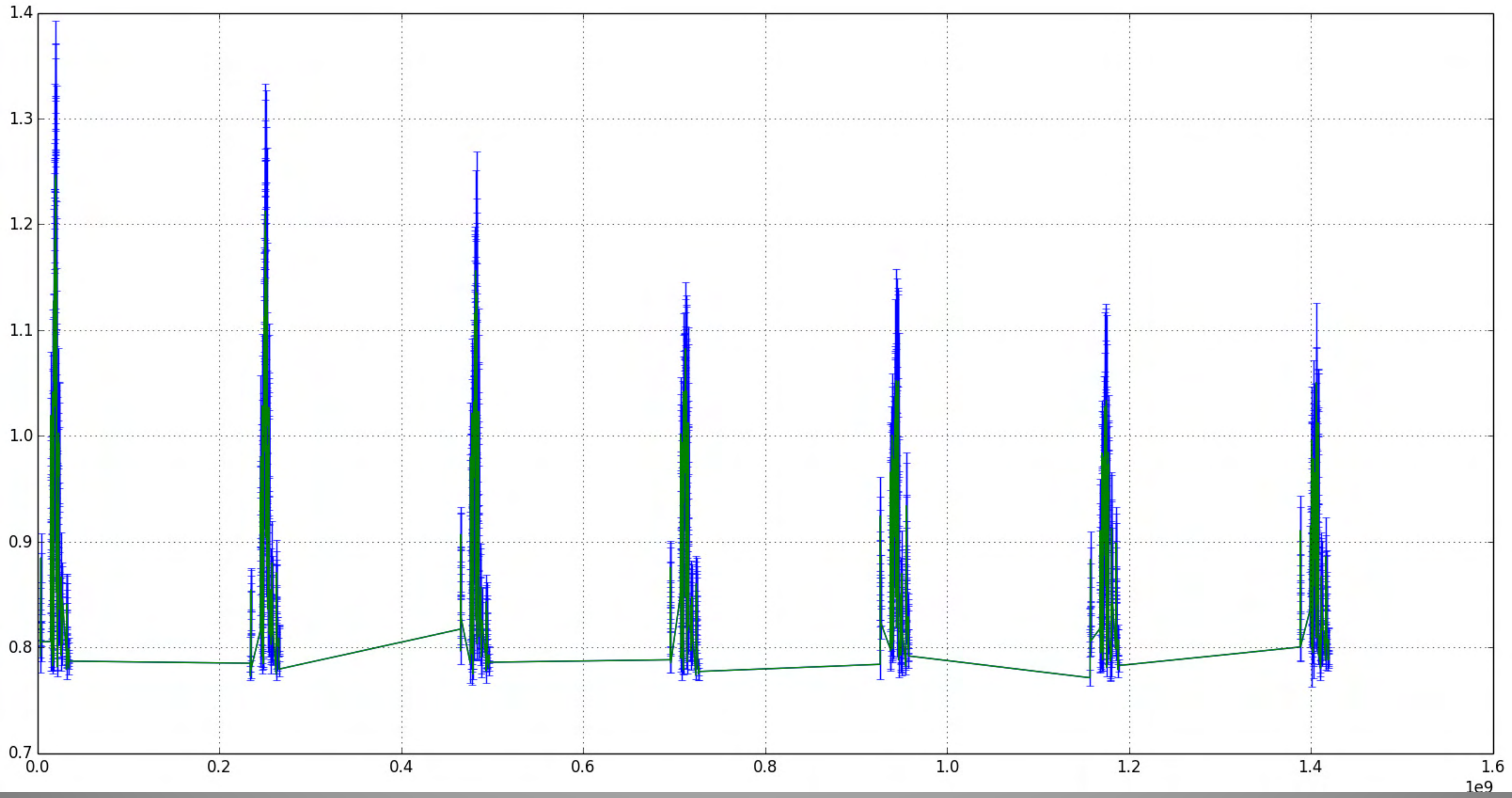
Strong Pulse Separation



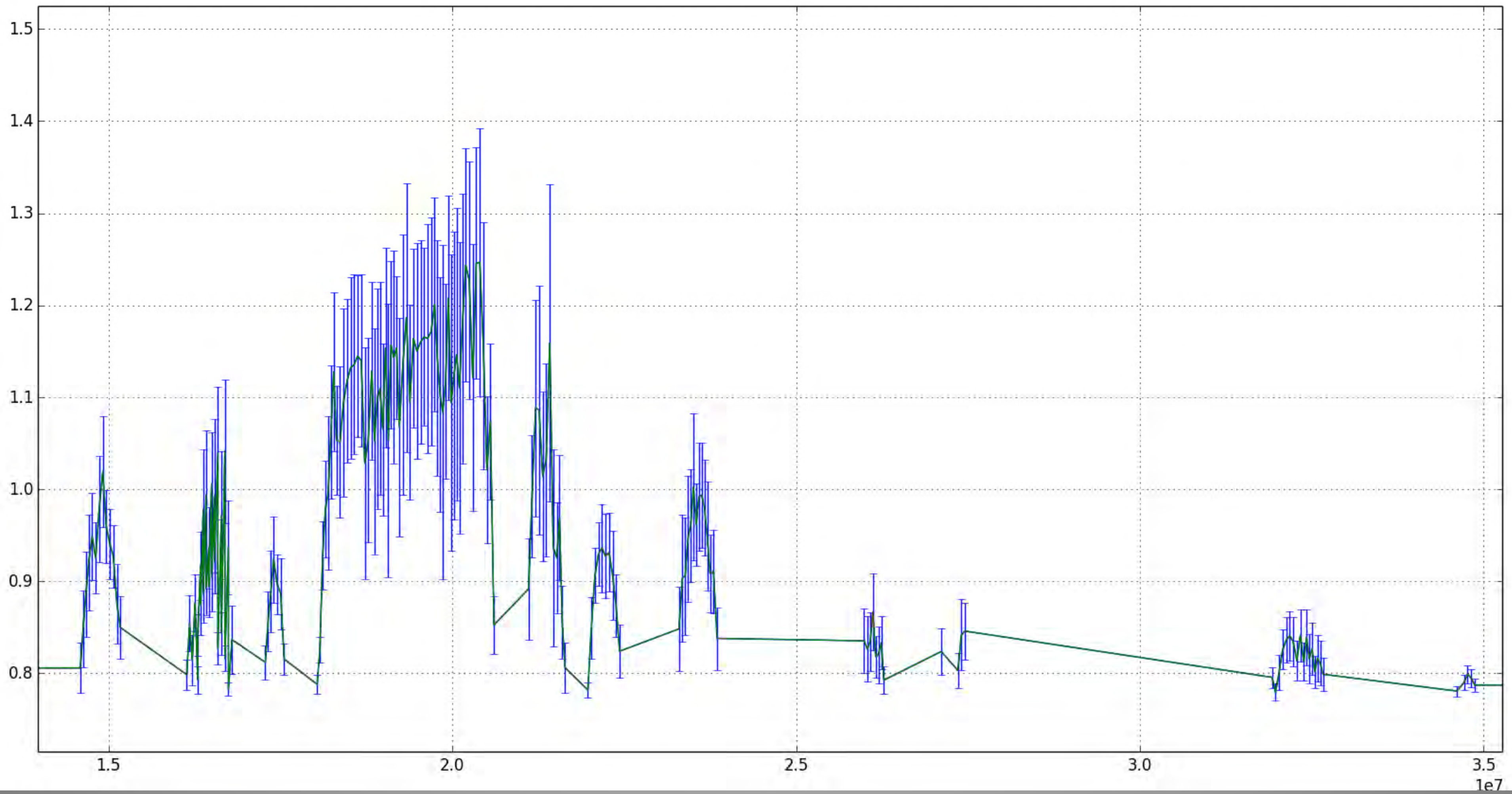
PRF Histogram



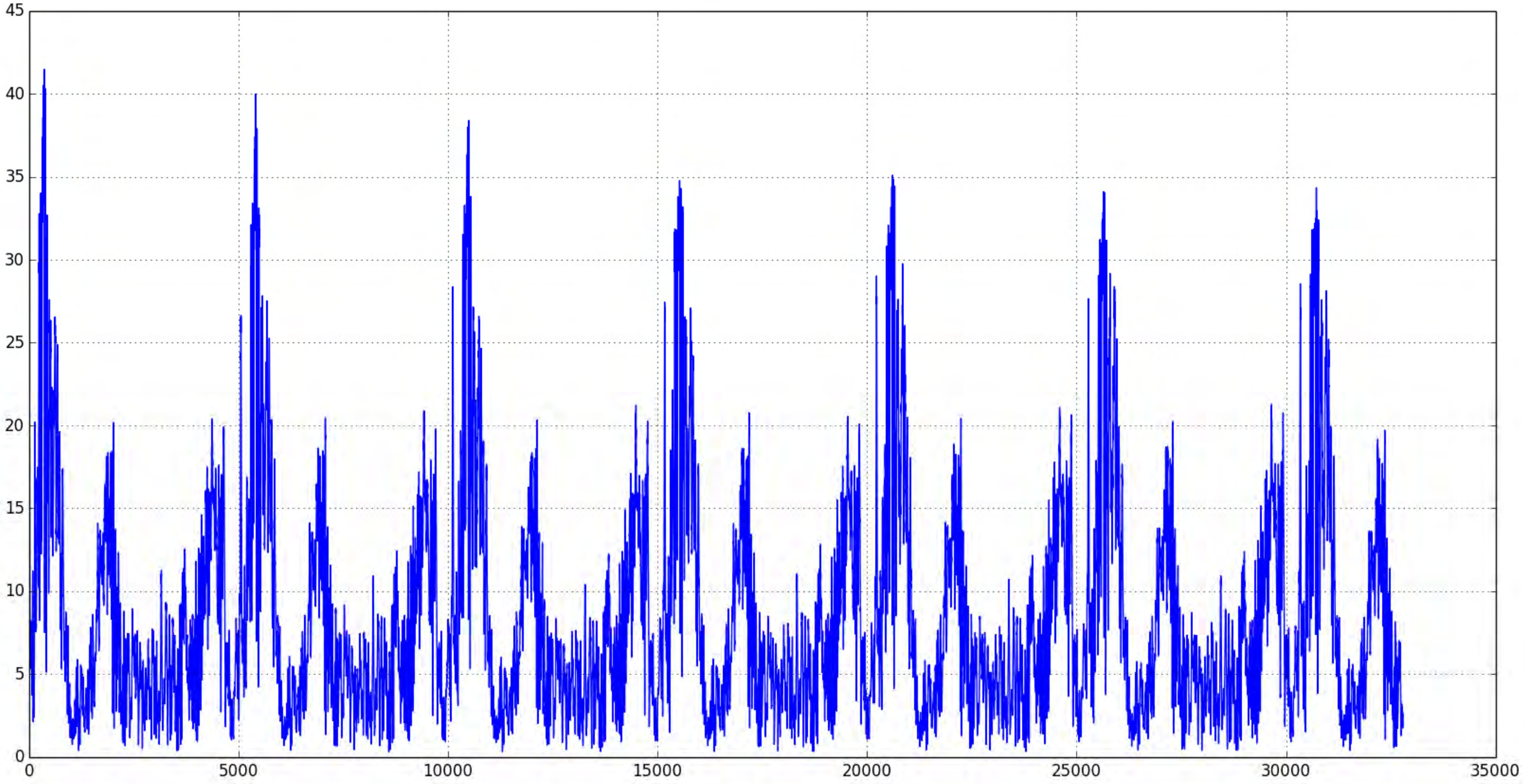
Strong Pulses vs. Time



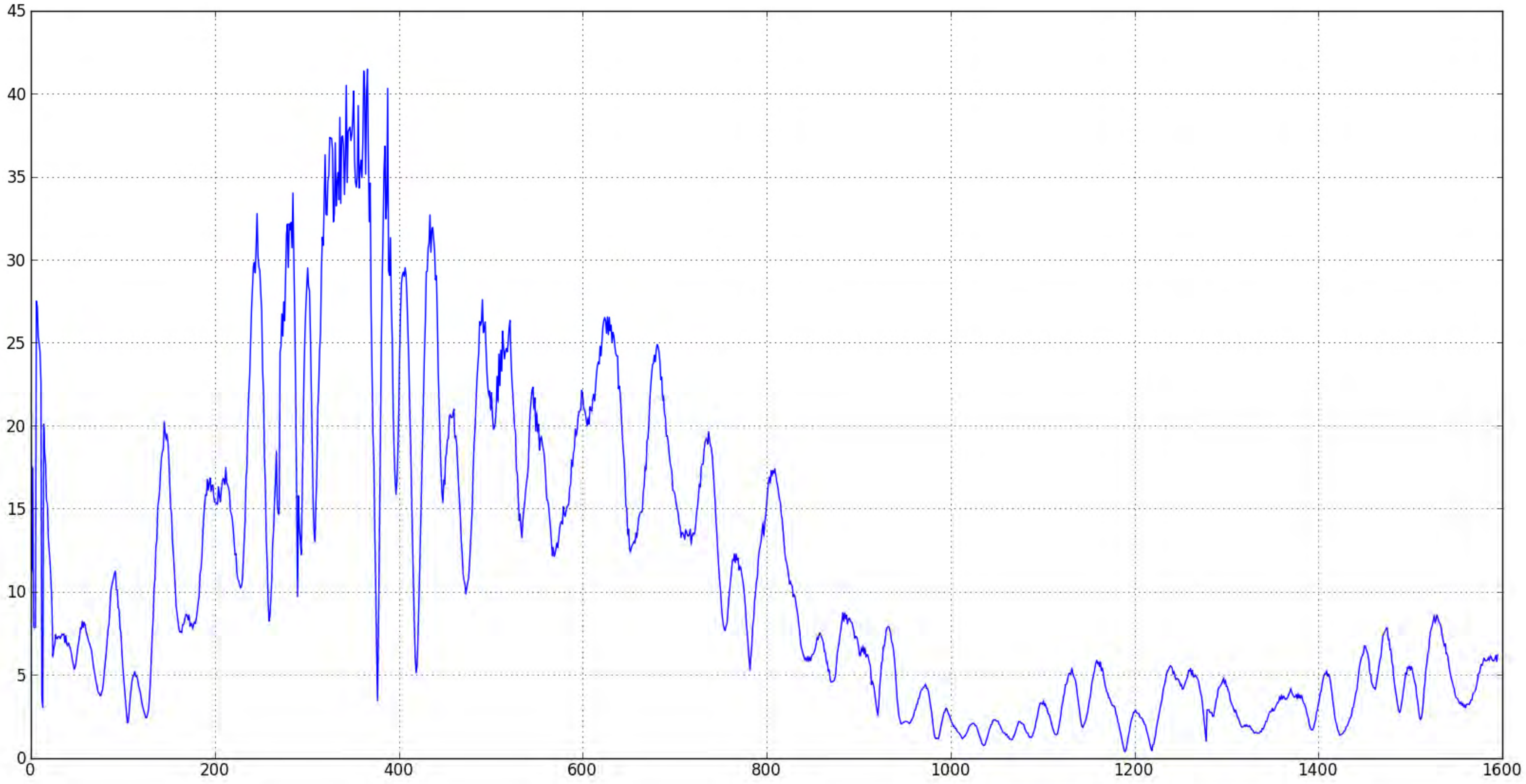
Strong Pulses vs. Time (zoomed)



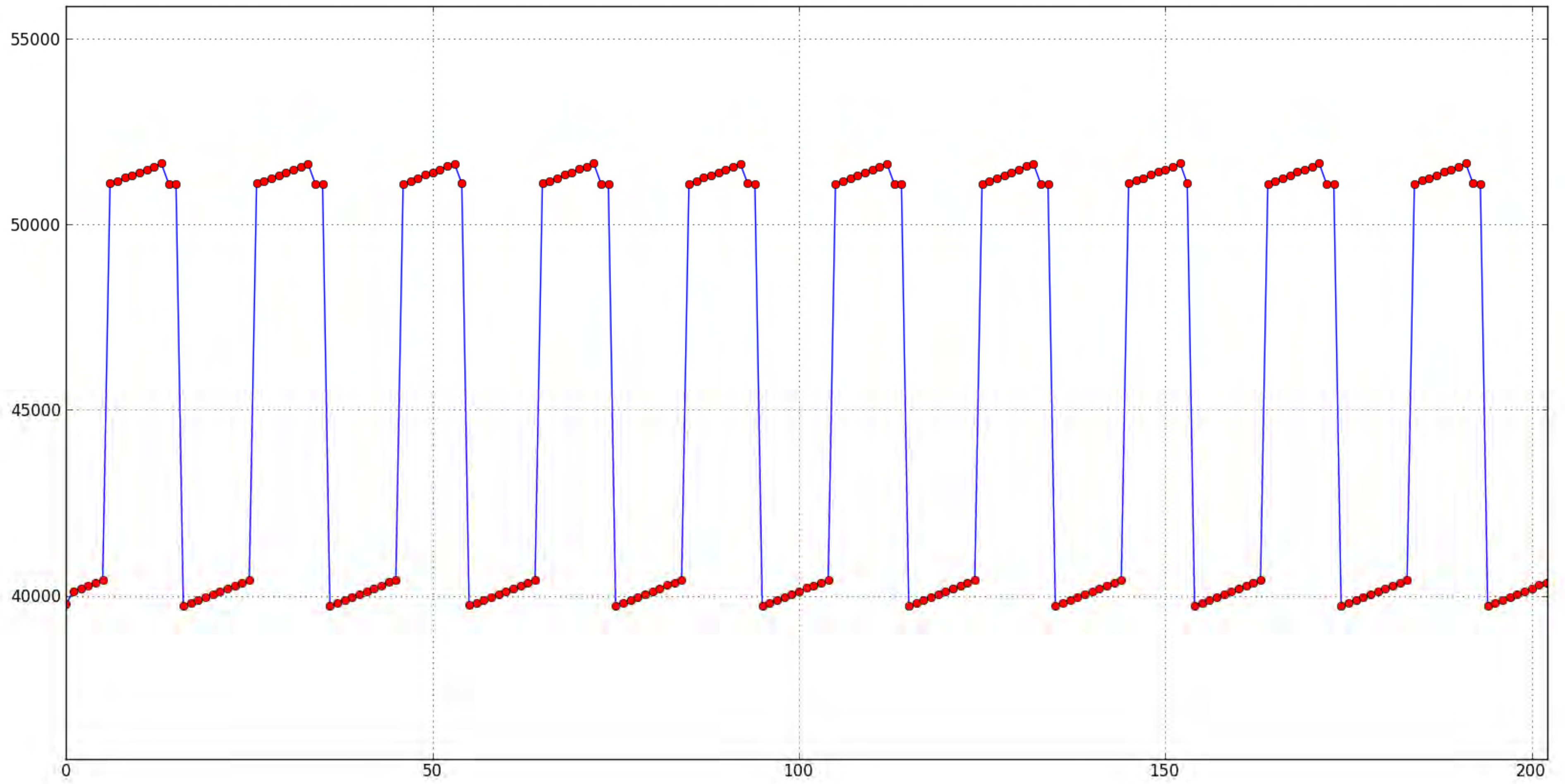
Pulse Power vs. Time



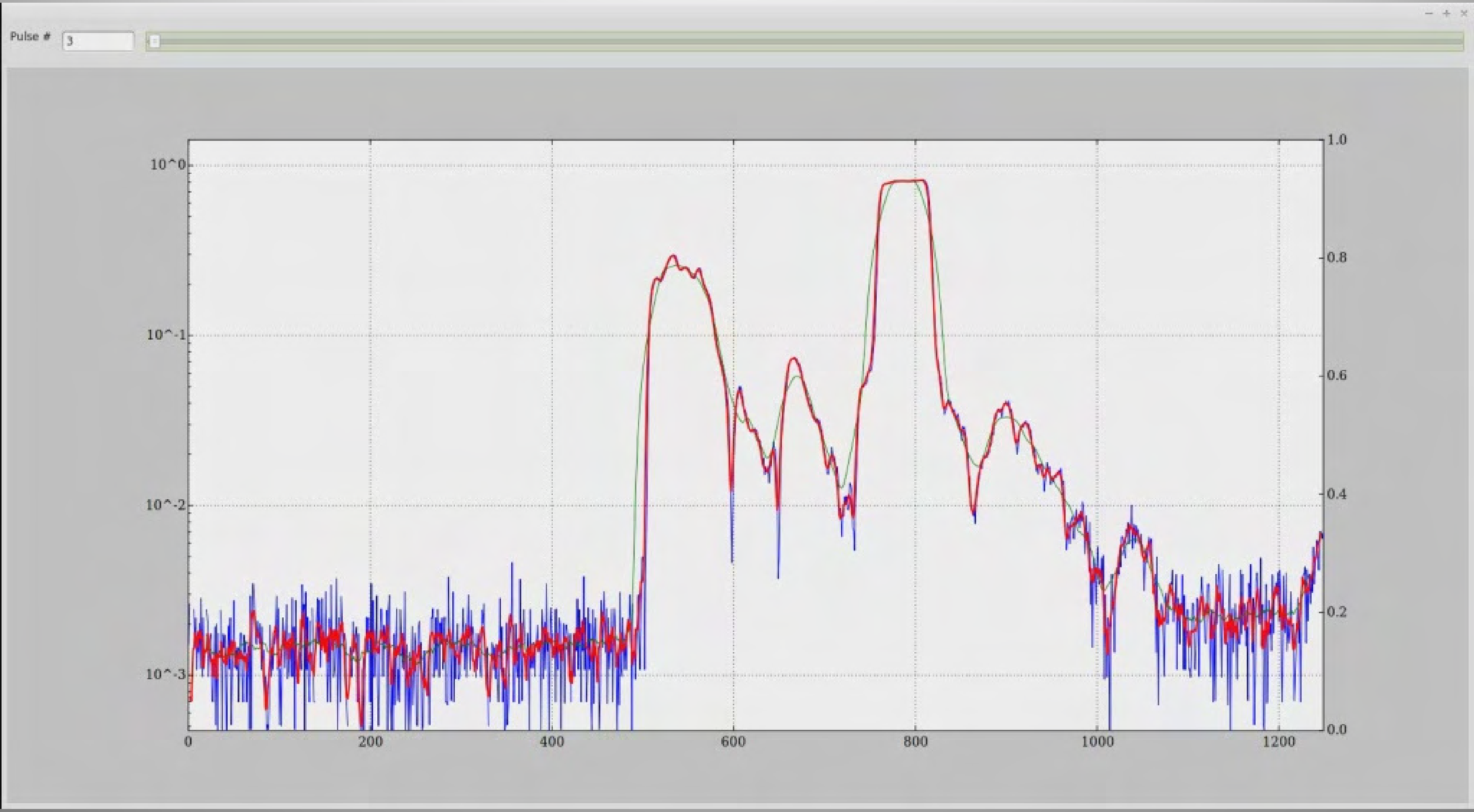
Pulse Power vs. Time (zoomed)



Distance Between Pulses

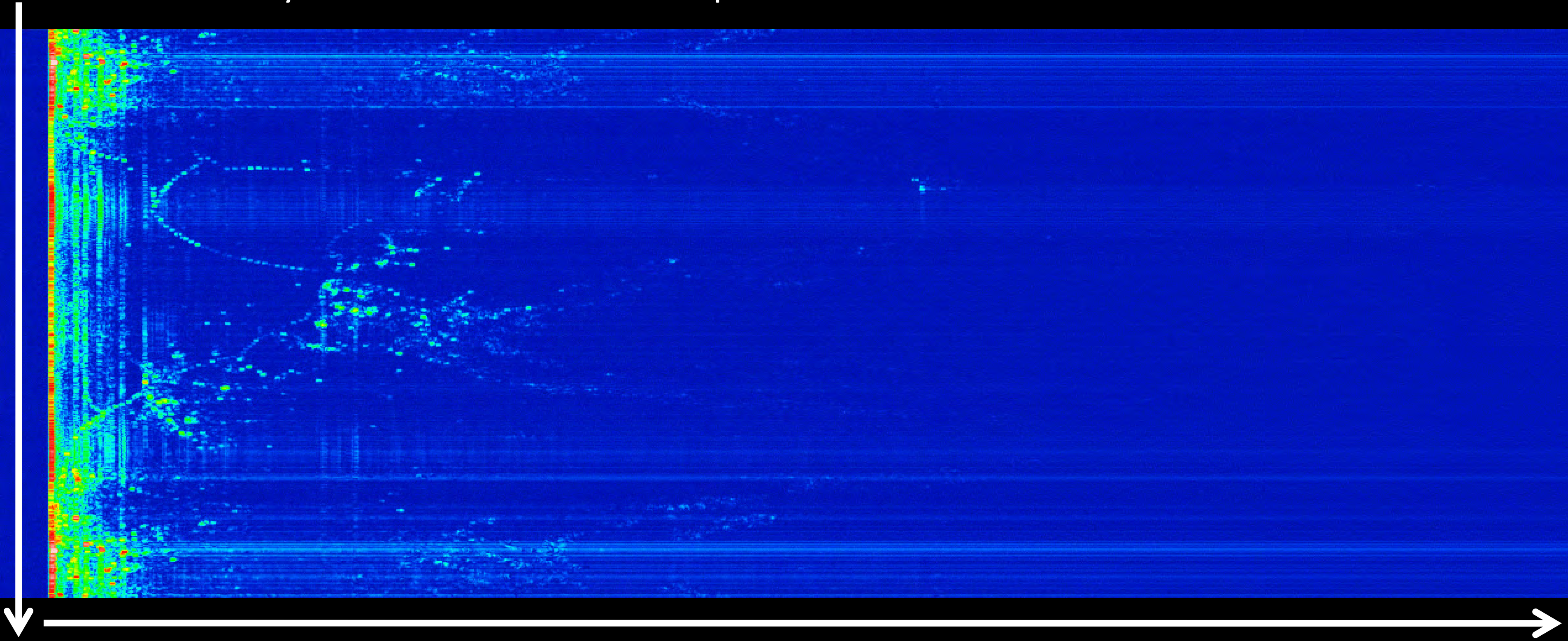


Pulse and echo power over time

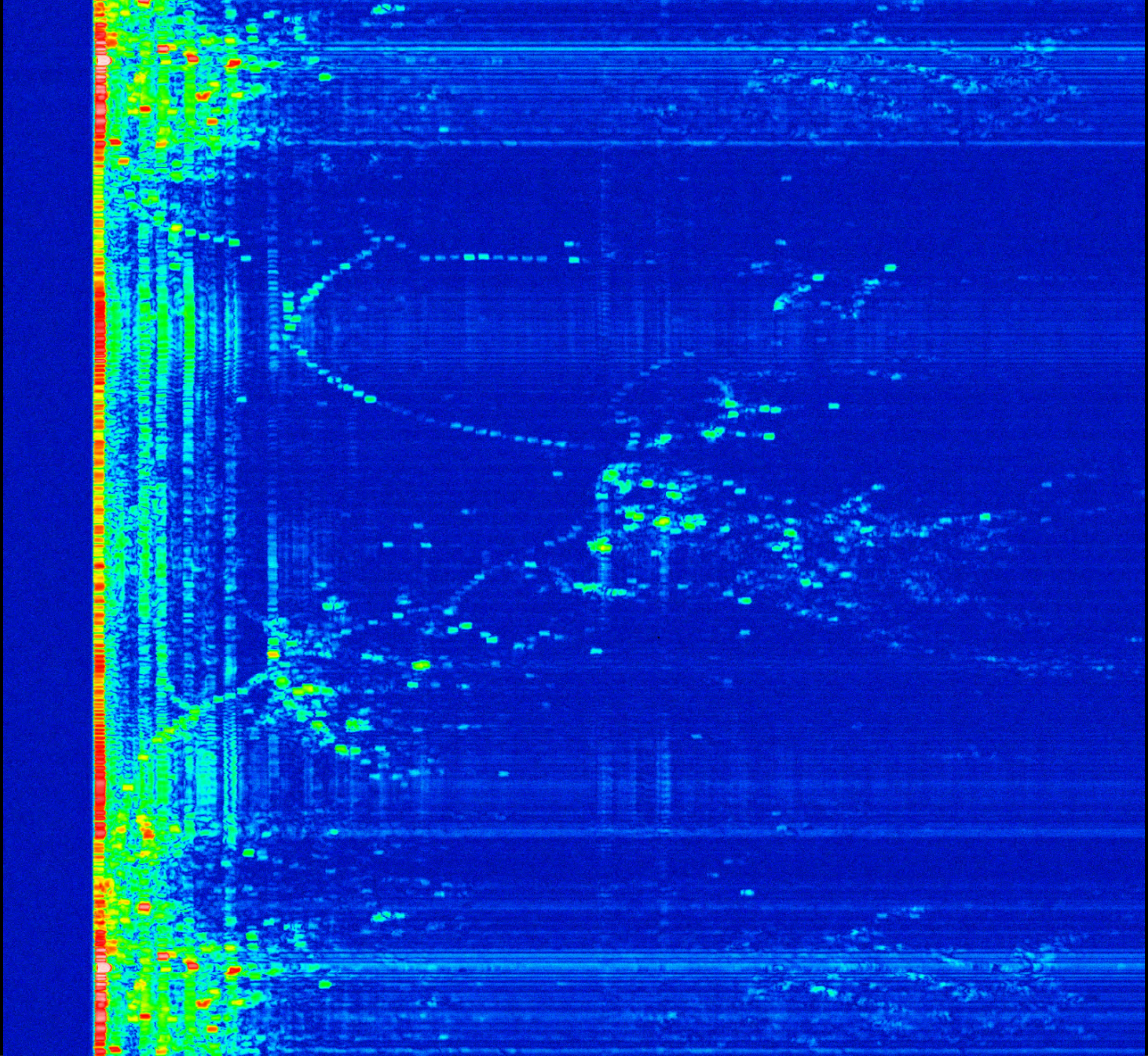


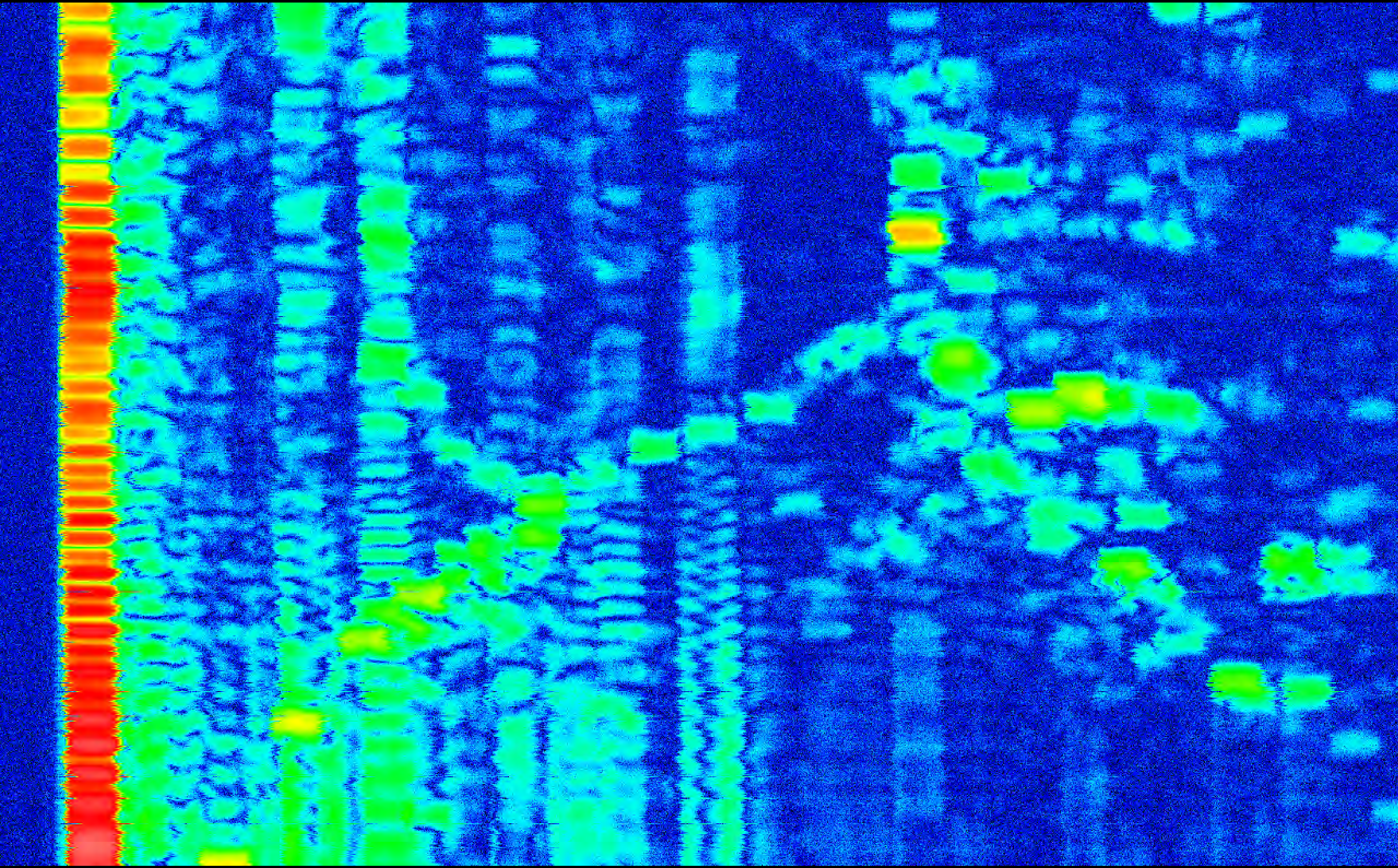
Raw RADAR Return Plot

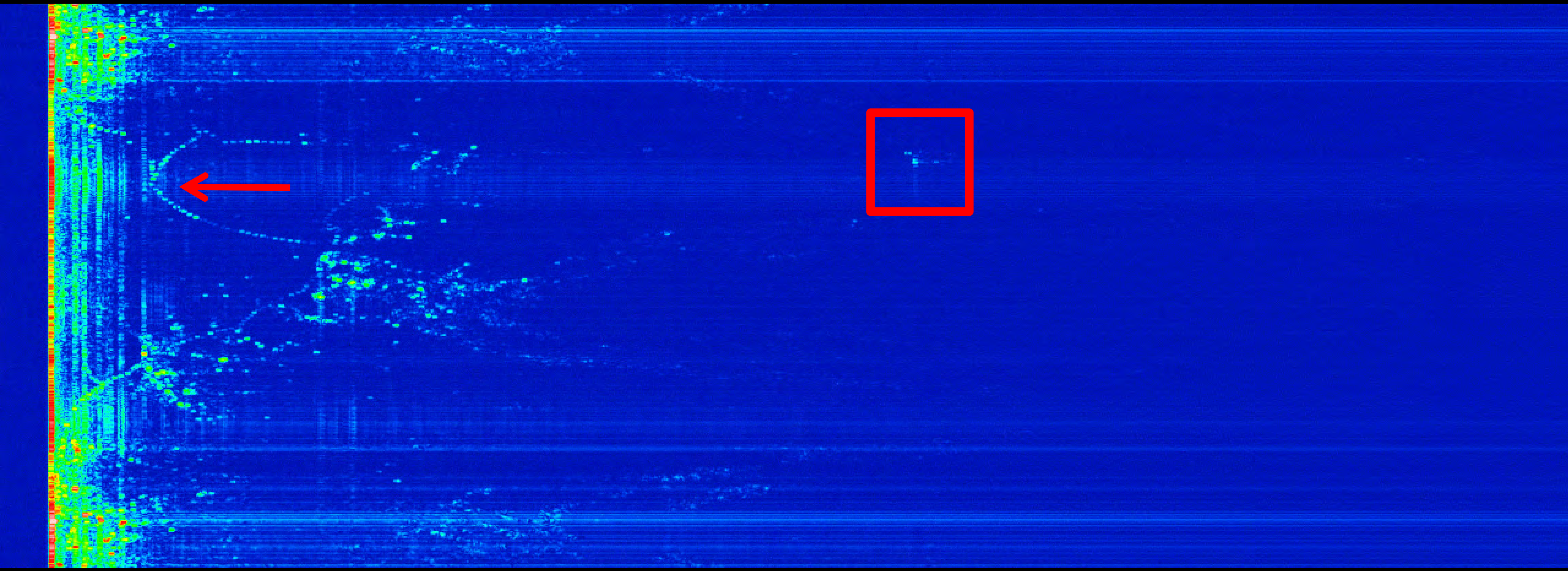
Each scanline is synchronised to an emitted pulse



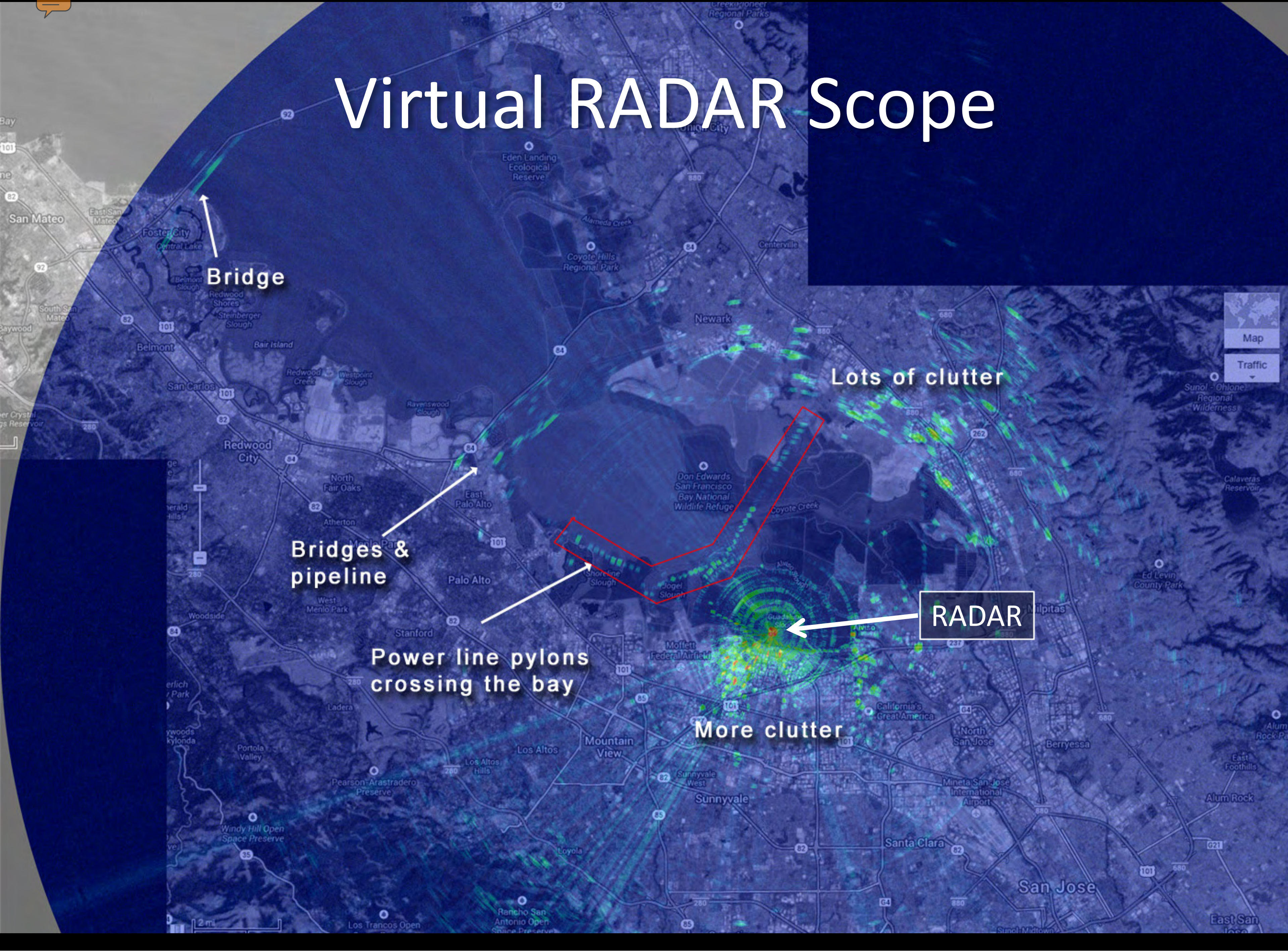
Scanline is amplitude of samples over time (also range of the return)

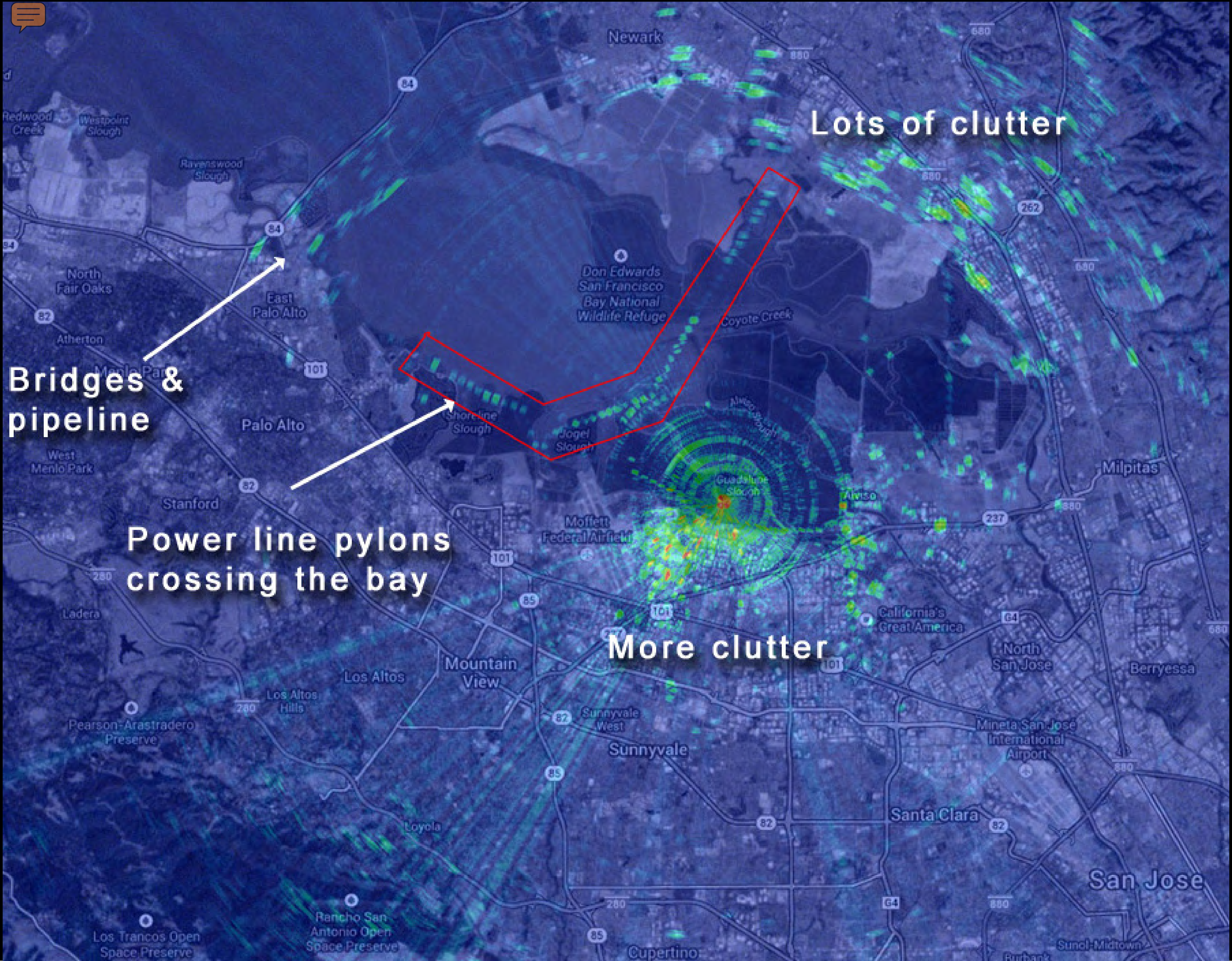






Virtual RADAR Scope



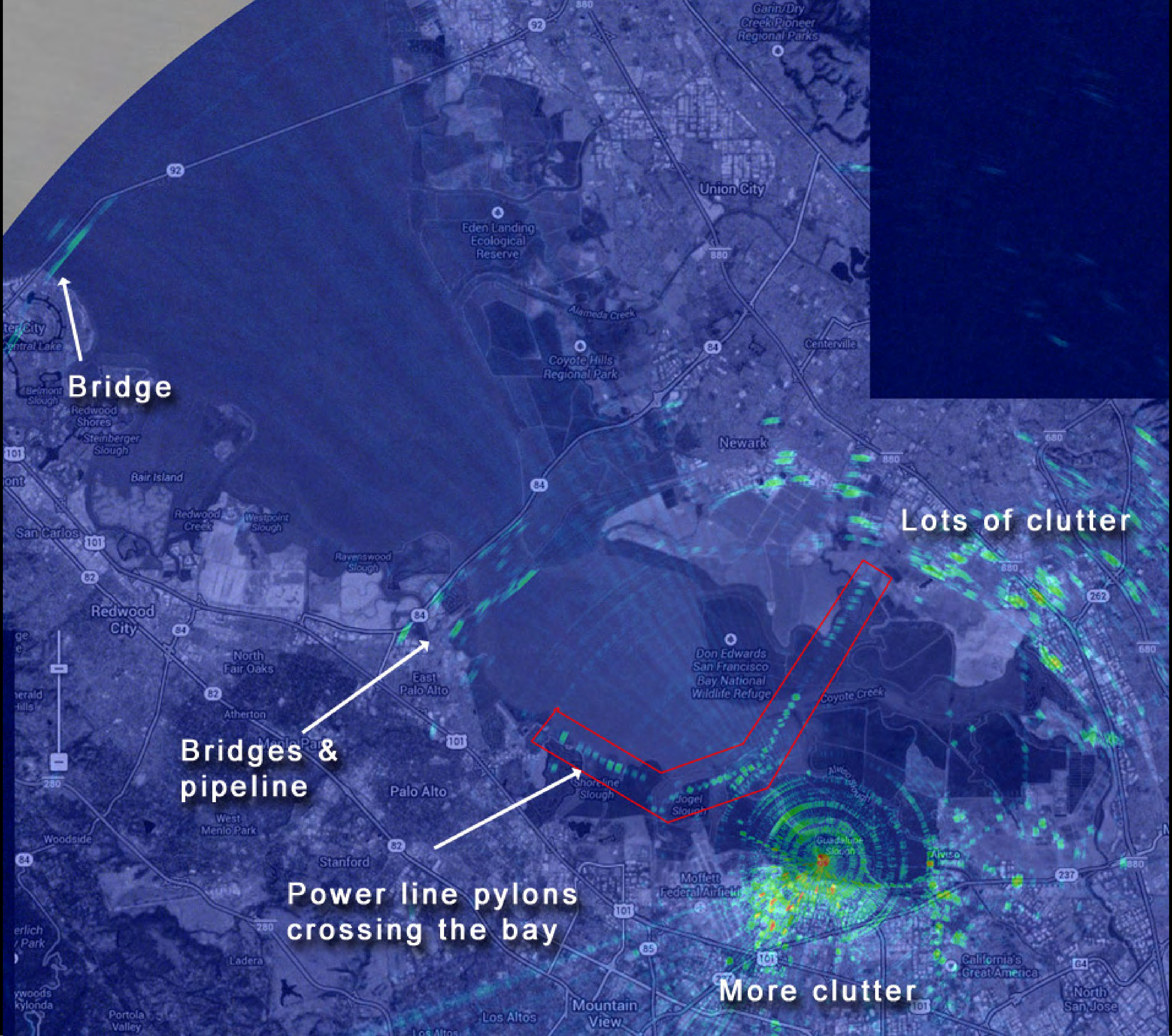


Lots of clutter

Bridges & pipeline

Power line pylons crossing the bay

More clutter



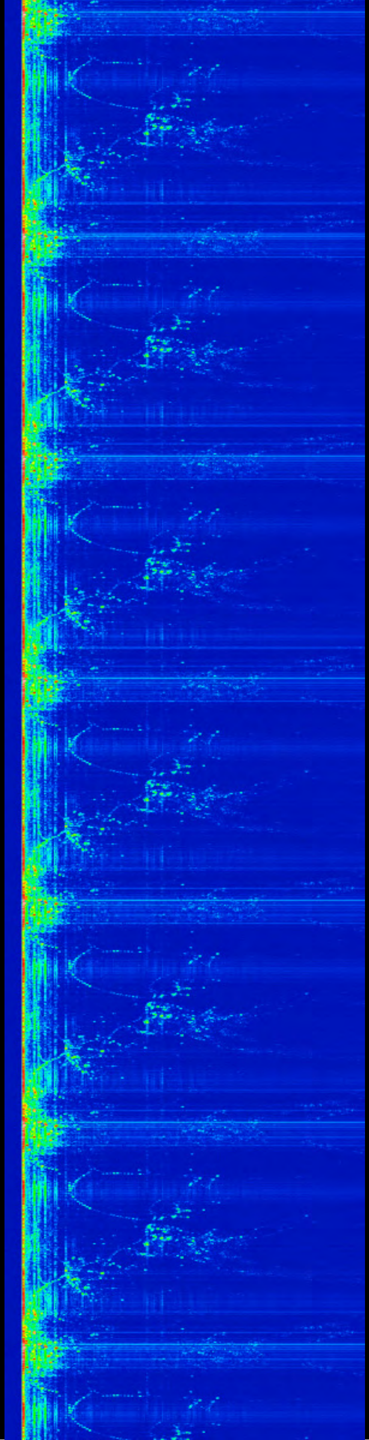
Bridge

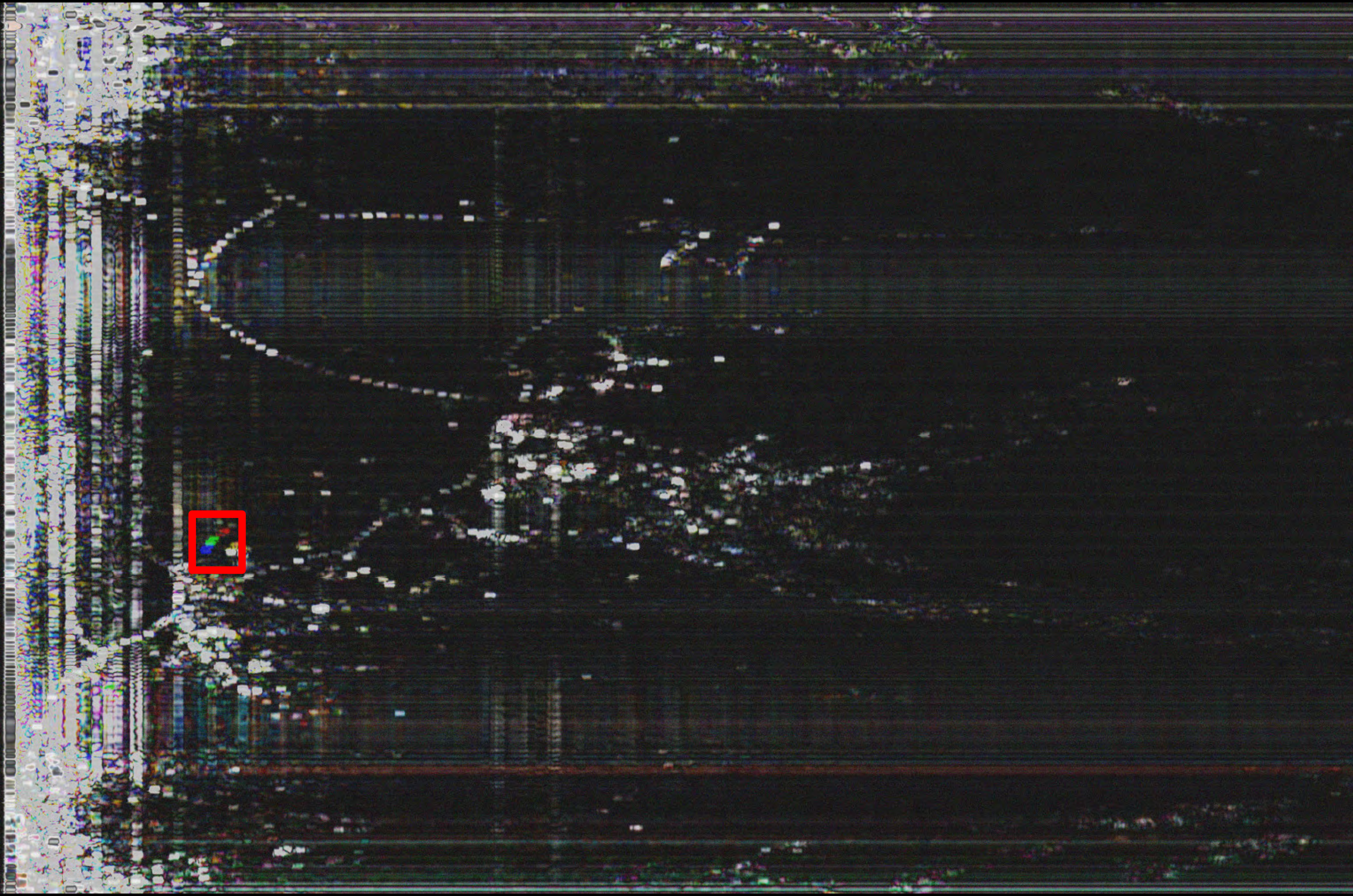
Bridges & pipeline

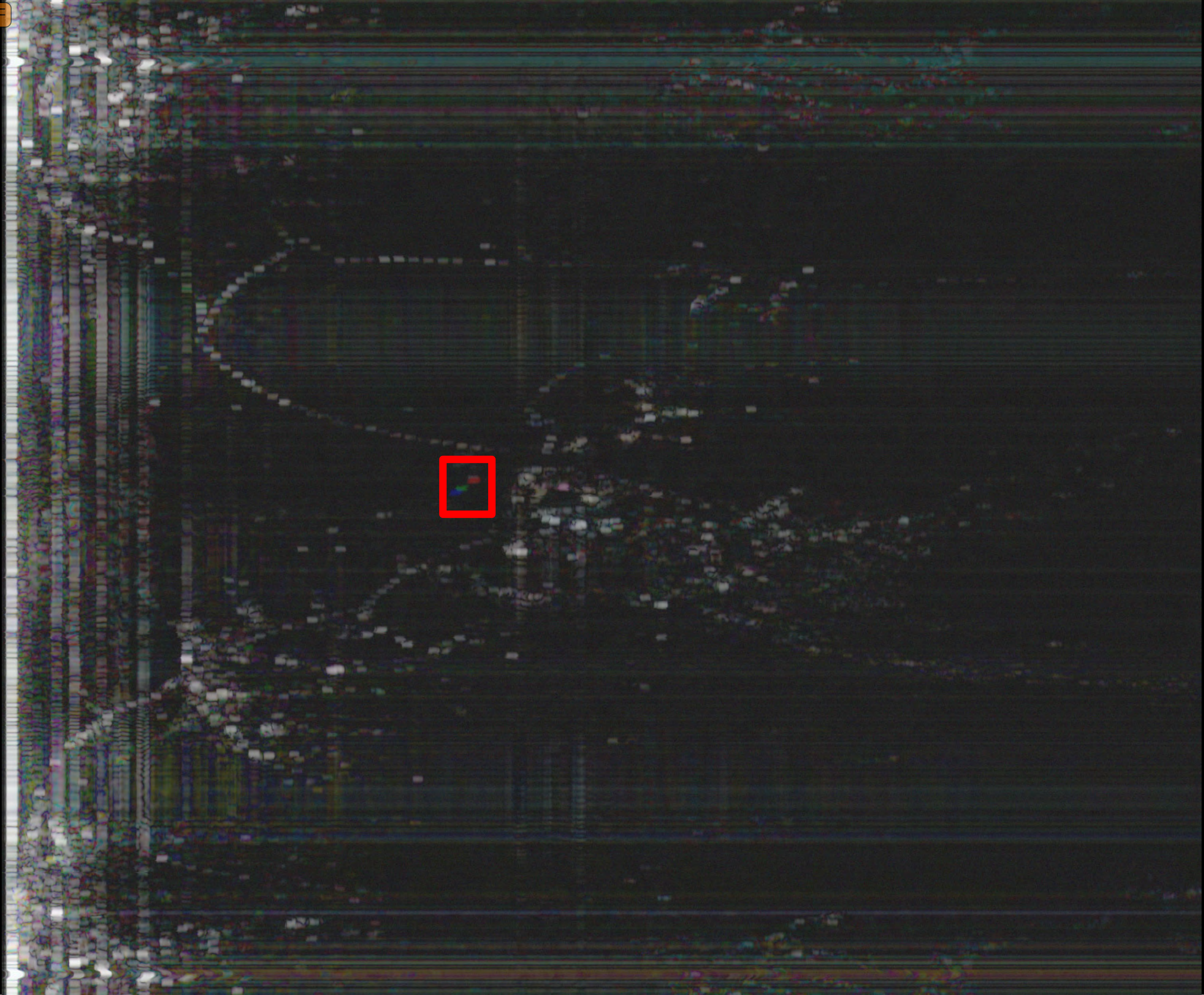
Power line pylons crossing the bay

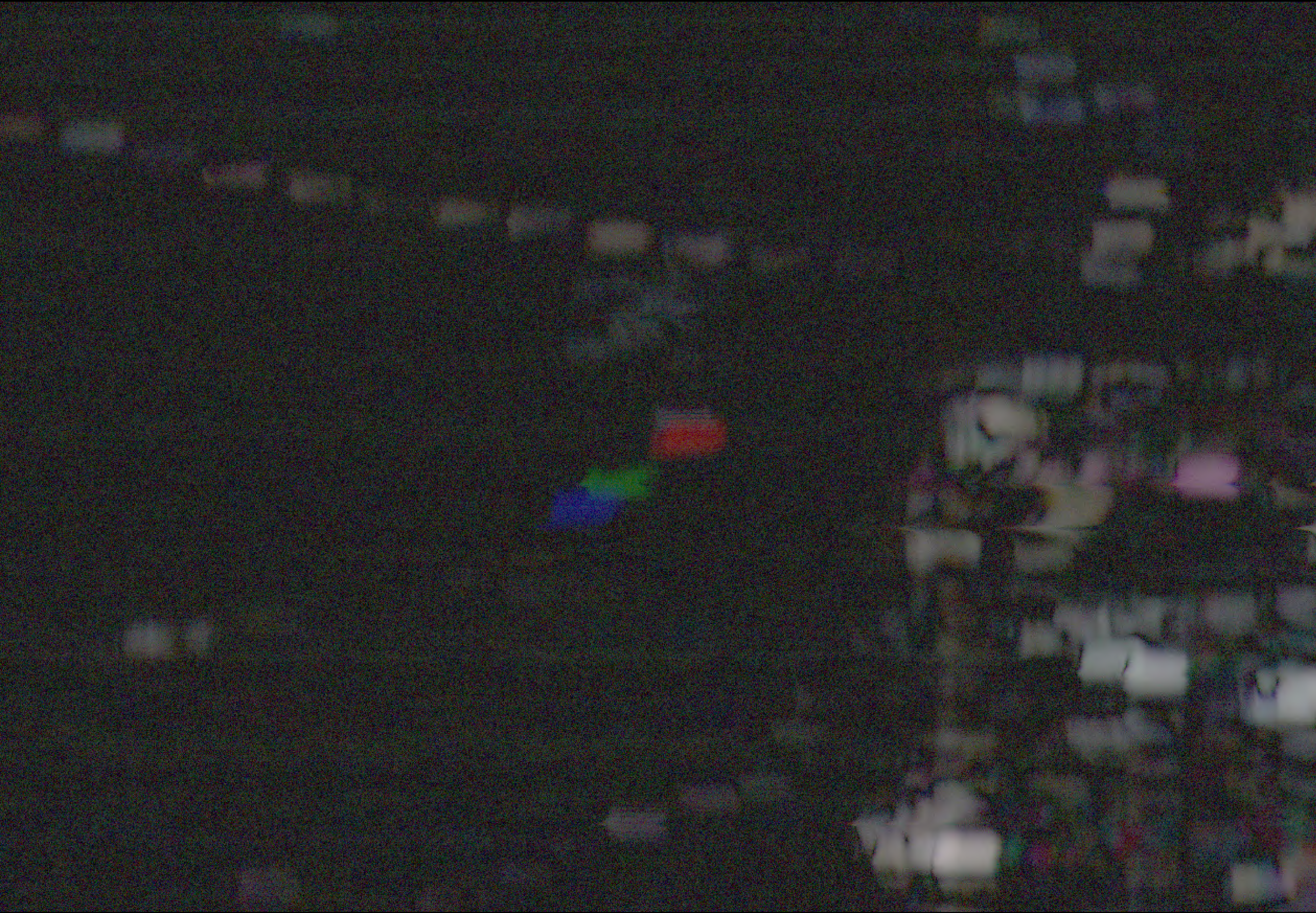
Lots of clutter

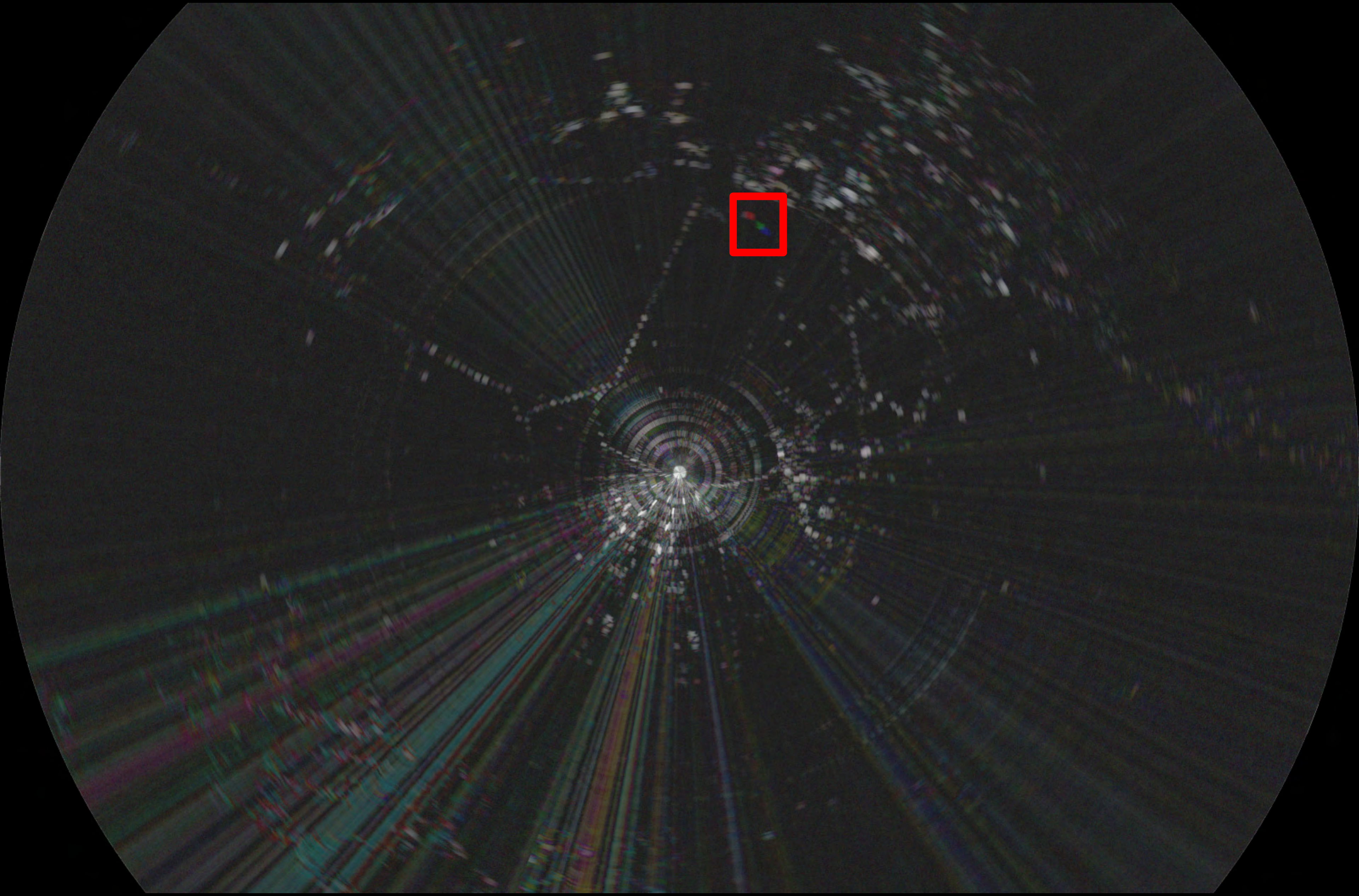
More clutter

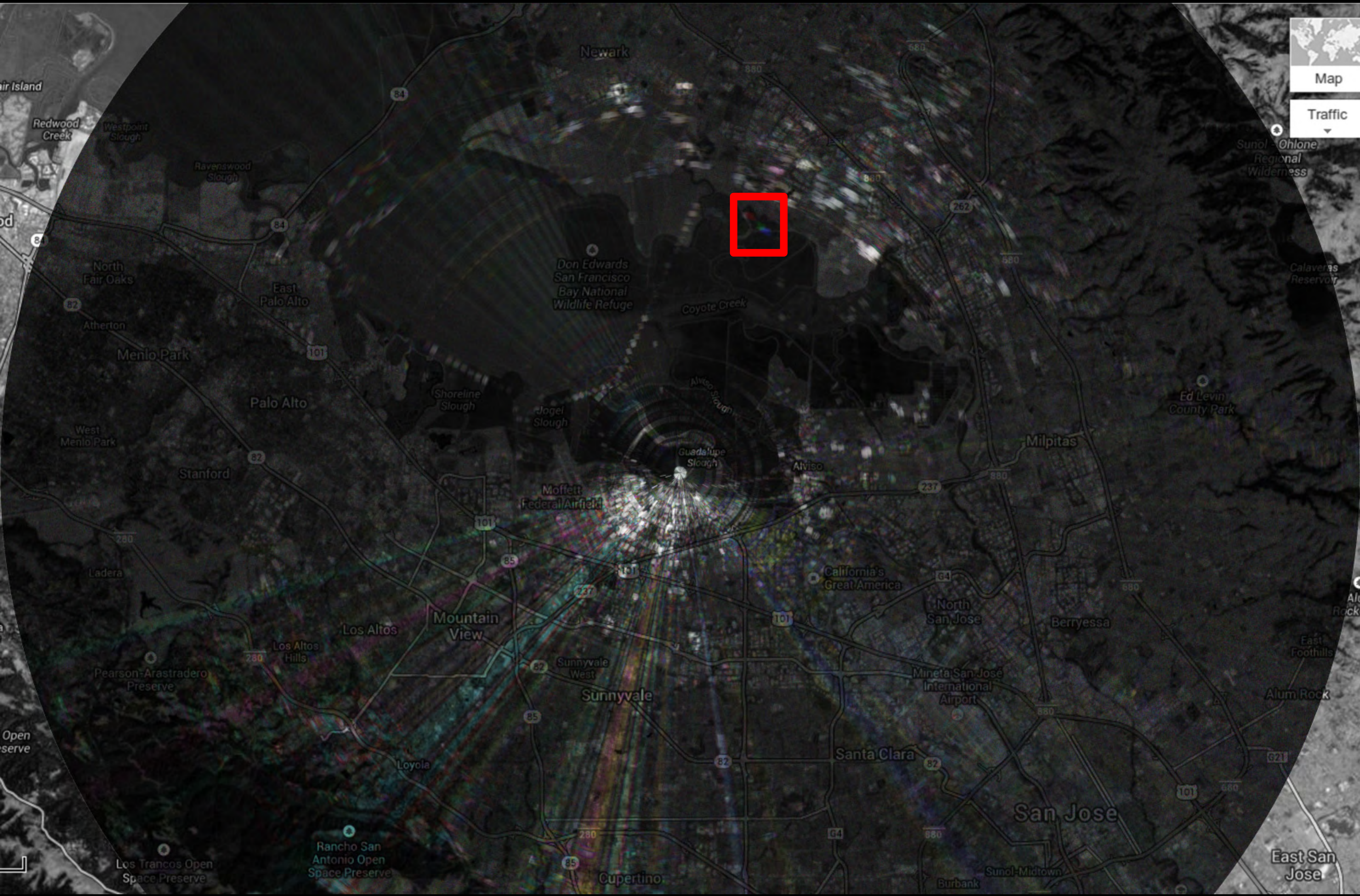




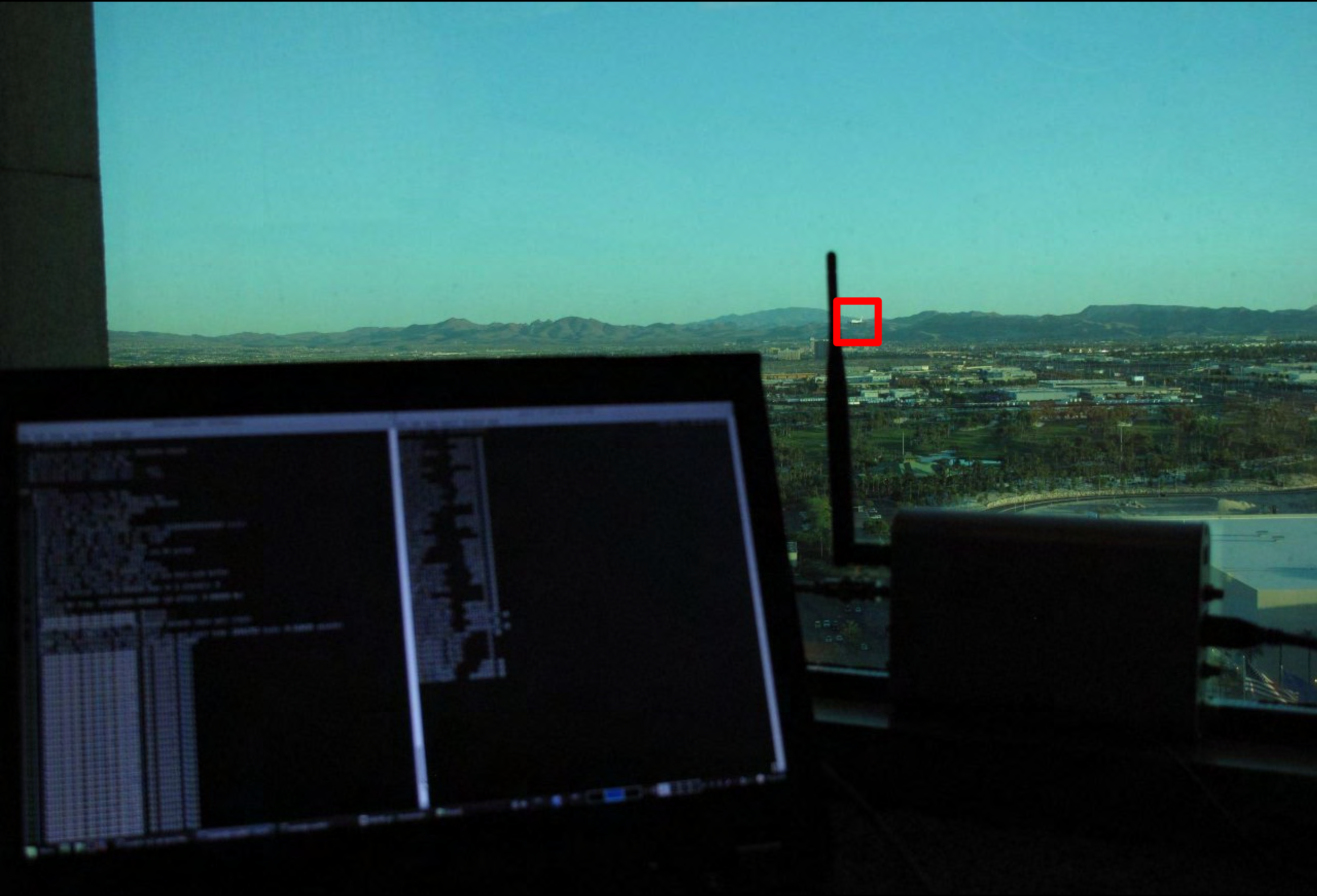




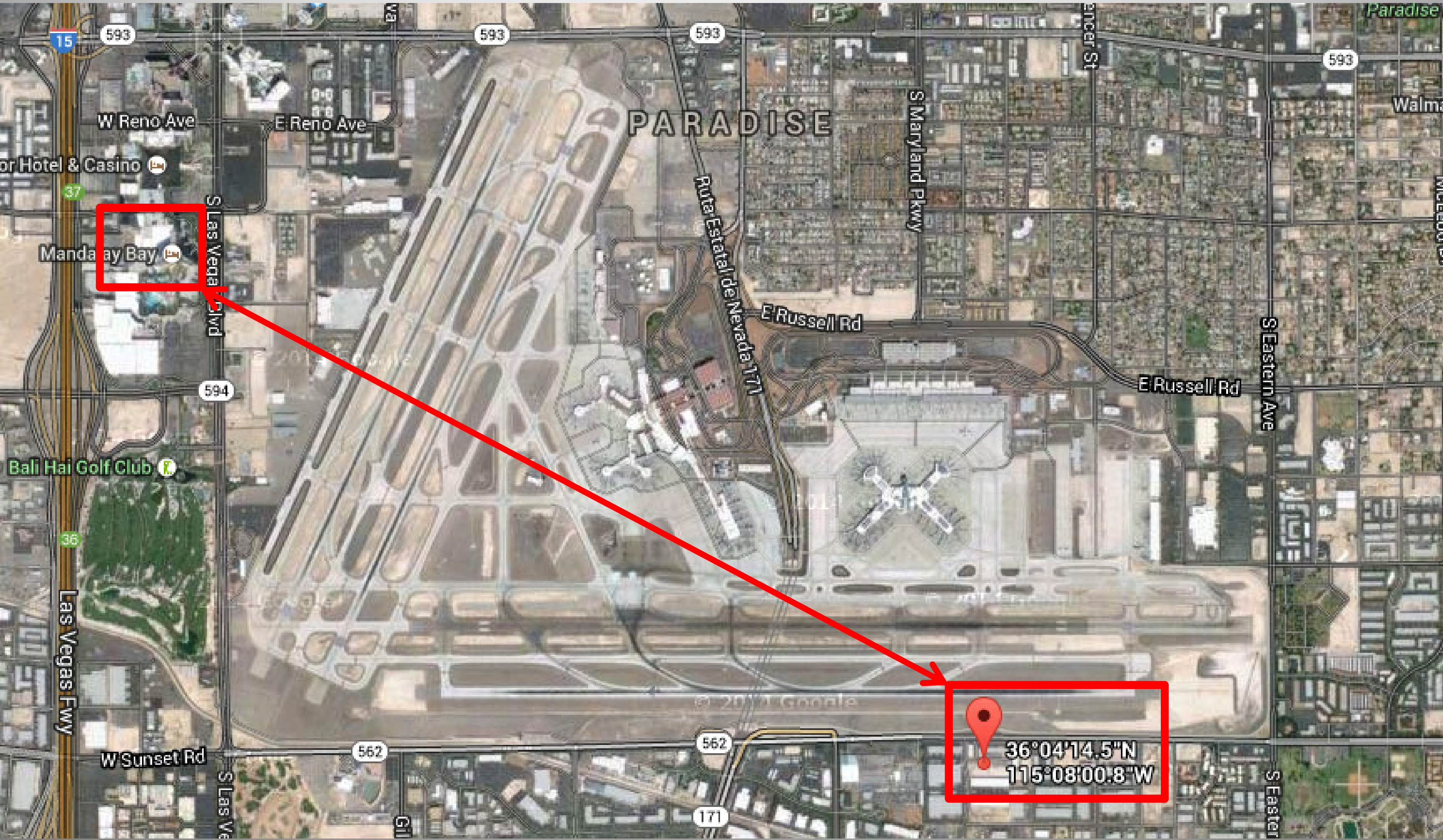



Map
Traffic
Newark
Redwood Creek
Westpoint Slough
Ravenswood Slough
North Fair Oaks
East Palo Alto
Atherton
Menlo Park
Palo Alto
West Menlo Park
Stanford
Don Edwards San Francisco Bay National Wildlife Refuge
Coyote Creek
Shoreline Slough
Jogel Slough
Alviso Slough
Guadalupe Slough
Alviso
Moffett Federal Airfield
Milpitas
Sunol - Ohlone Regional Wilderness
Calaveras Reservoir
Ed Levin County Park
Ladera
Los Altos
Los Altos Hills
Mountain View
Pearson-Arastradero Preserve
Sunnyvale West
Sunnyvale
California's Great America
North San Jose
Berryessa
East Foothills
Alum Rock
Mineta San José International Airport
Santa Clara
San Jose
Loyola
Rancho San Antonio Open Space Preserve
Los Trancos Open Space Preserve
Cupertino
Burbank
Sunol-Midtown
East San Jose
84
880
262
82
101
280
85
237
680
130
87
17

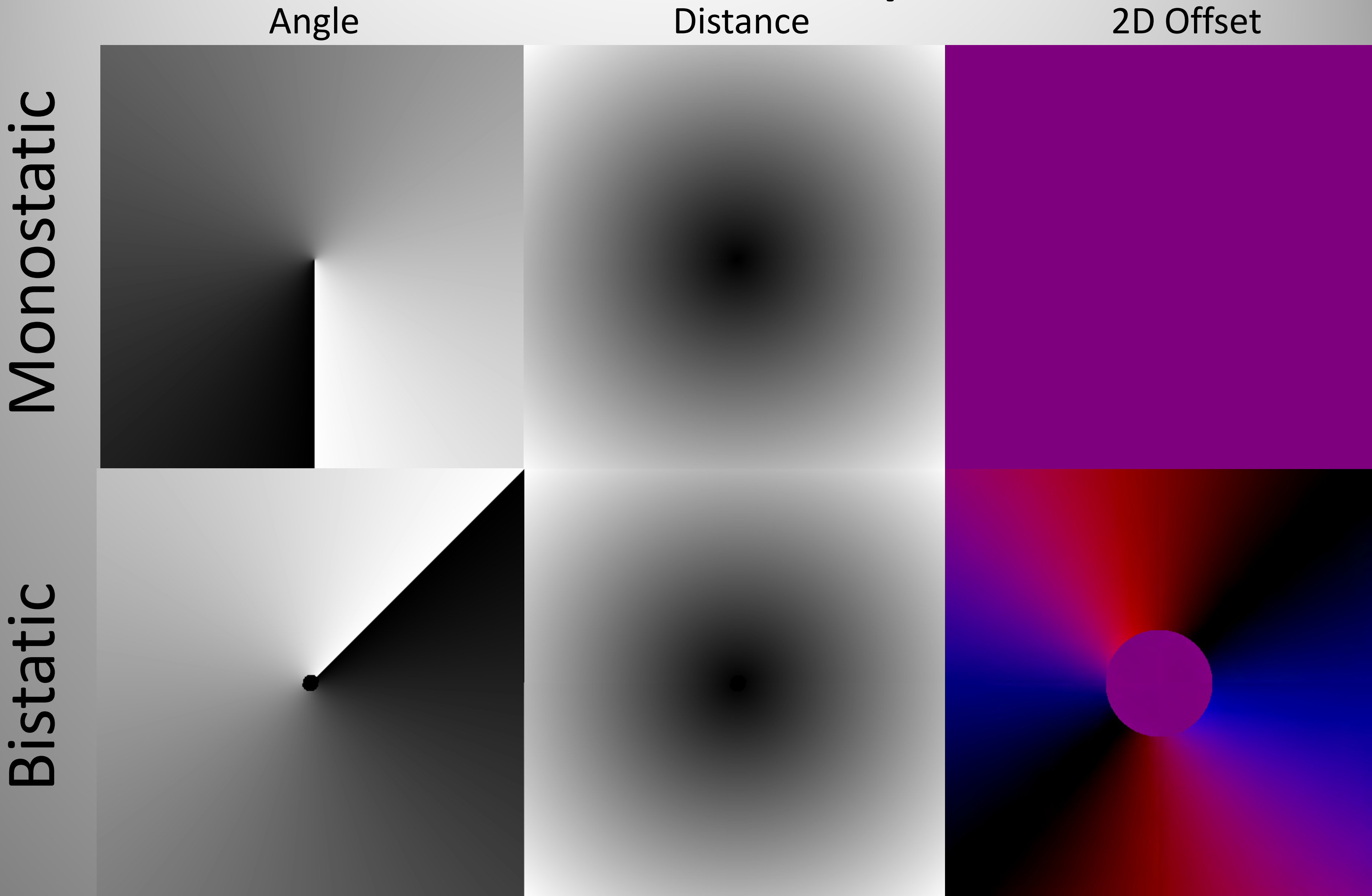
880
262
on Edwards
an Francisco
Bay National
ildlife Refuge
Coyote Creek

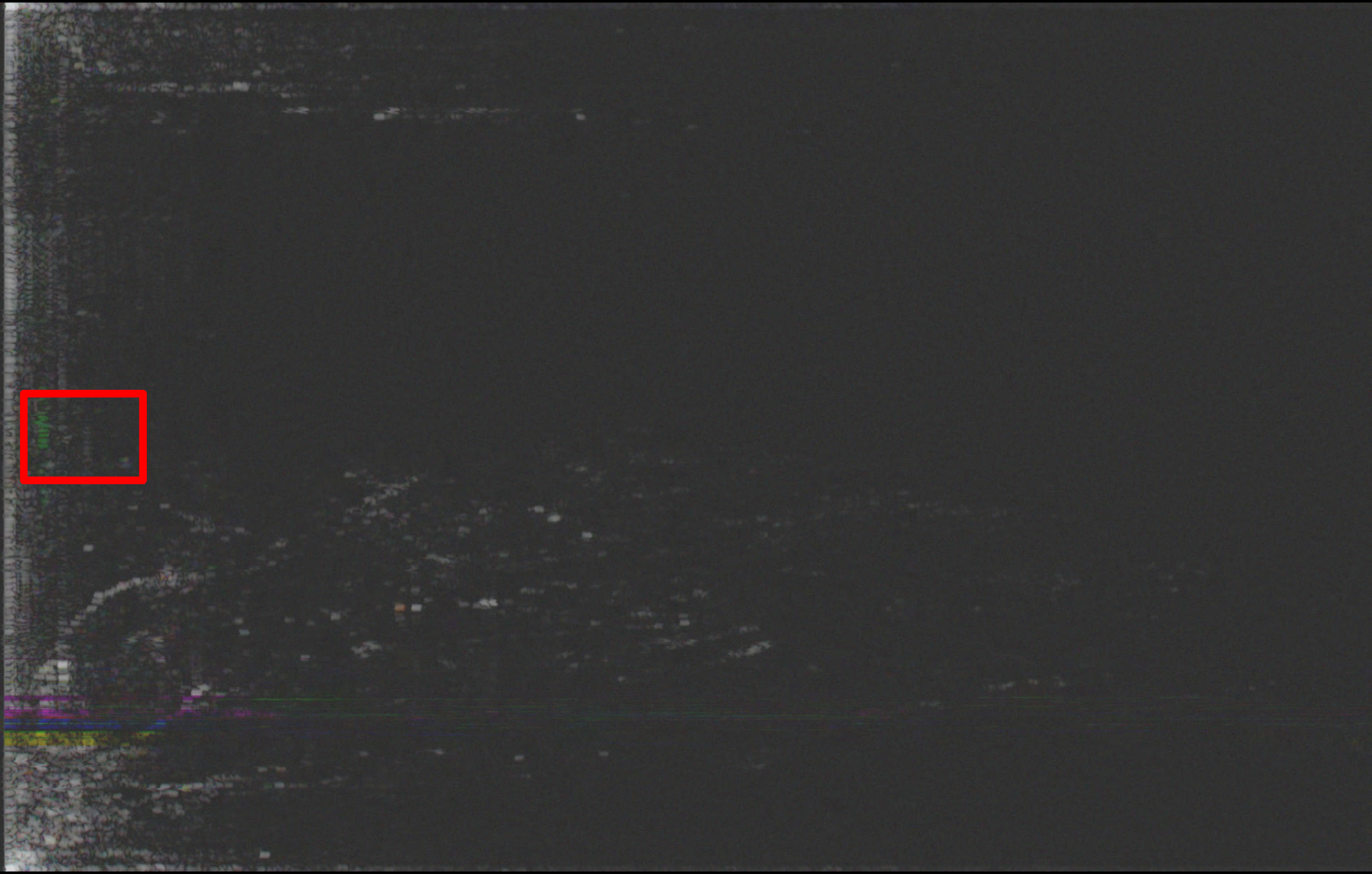


LAS ASR-9


15
593
593
593
593
Paradise
Walma
PARADISE
W Reno Ave
E Reno Ave
or Hotel & Casino
37
S Maryland Pkwy
Ruta Estatal de Nevada 171
S Las Vegas Blvd
Manda ay Bay
E Russell Rd
E Russell Rd
S Eastern Ave
594
Bali Hai Golf Club
36
Las Vegas Fwy
© 2014 Google
562
562
W Sunset Rd
S Las Ve
171
S Easter
36°04'14.5"N
115°08'00.8"W

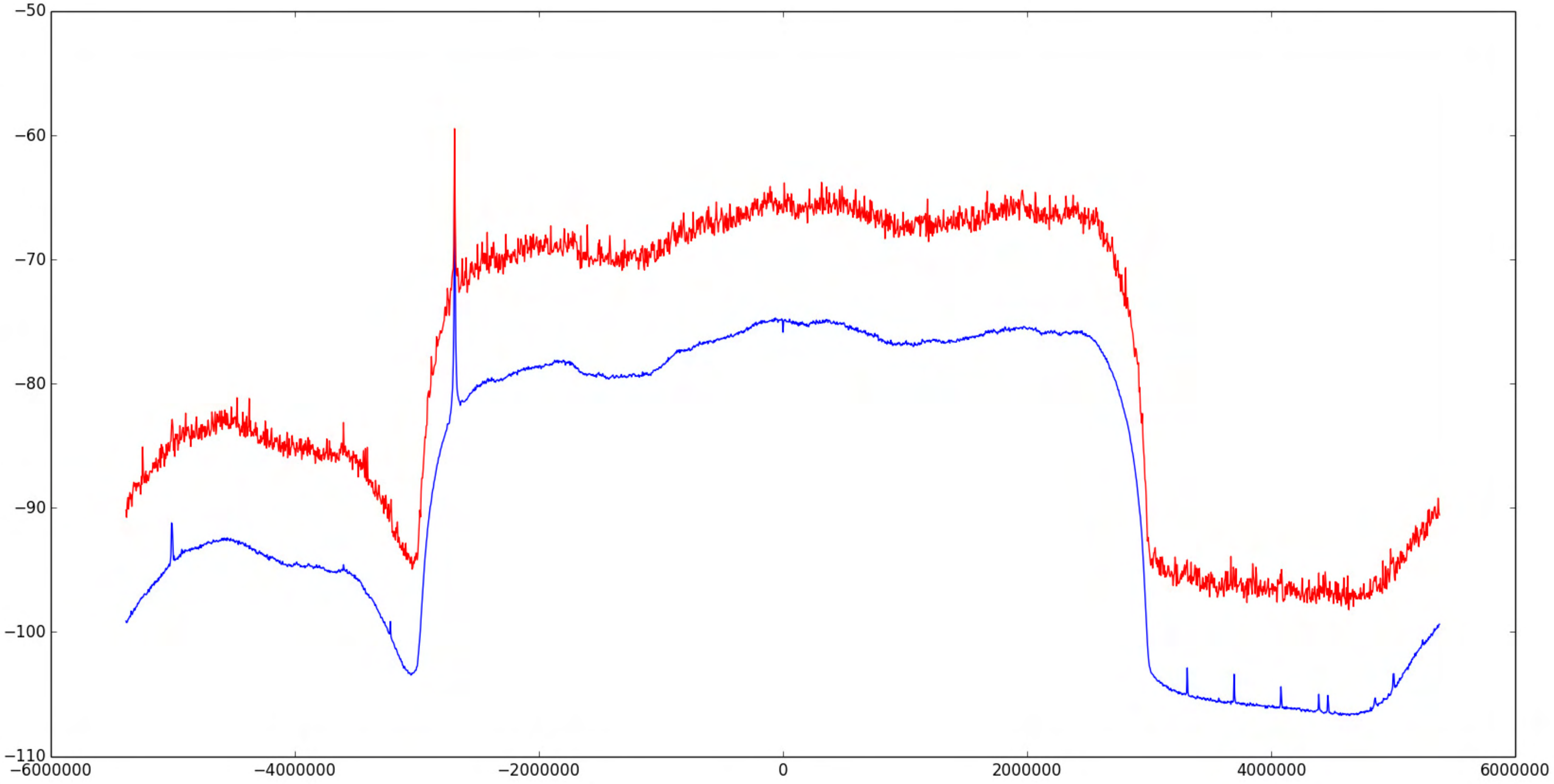
Distortion Map





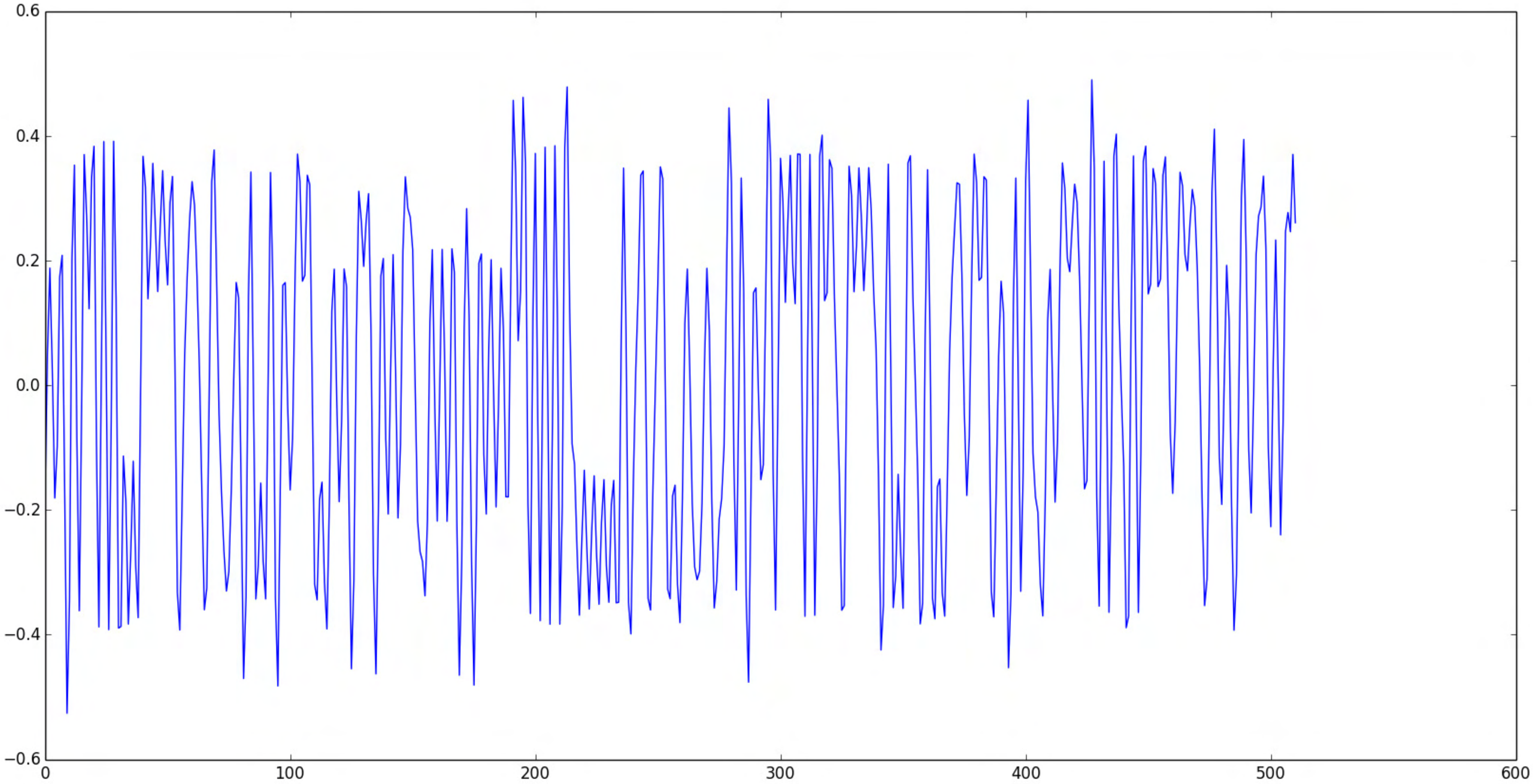
Multipath

ATSC

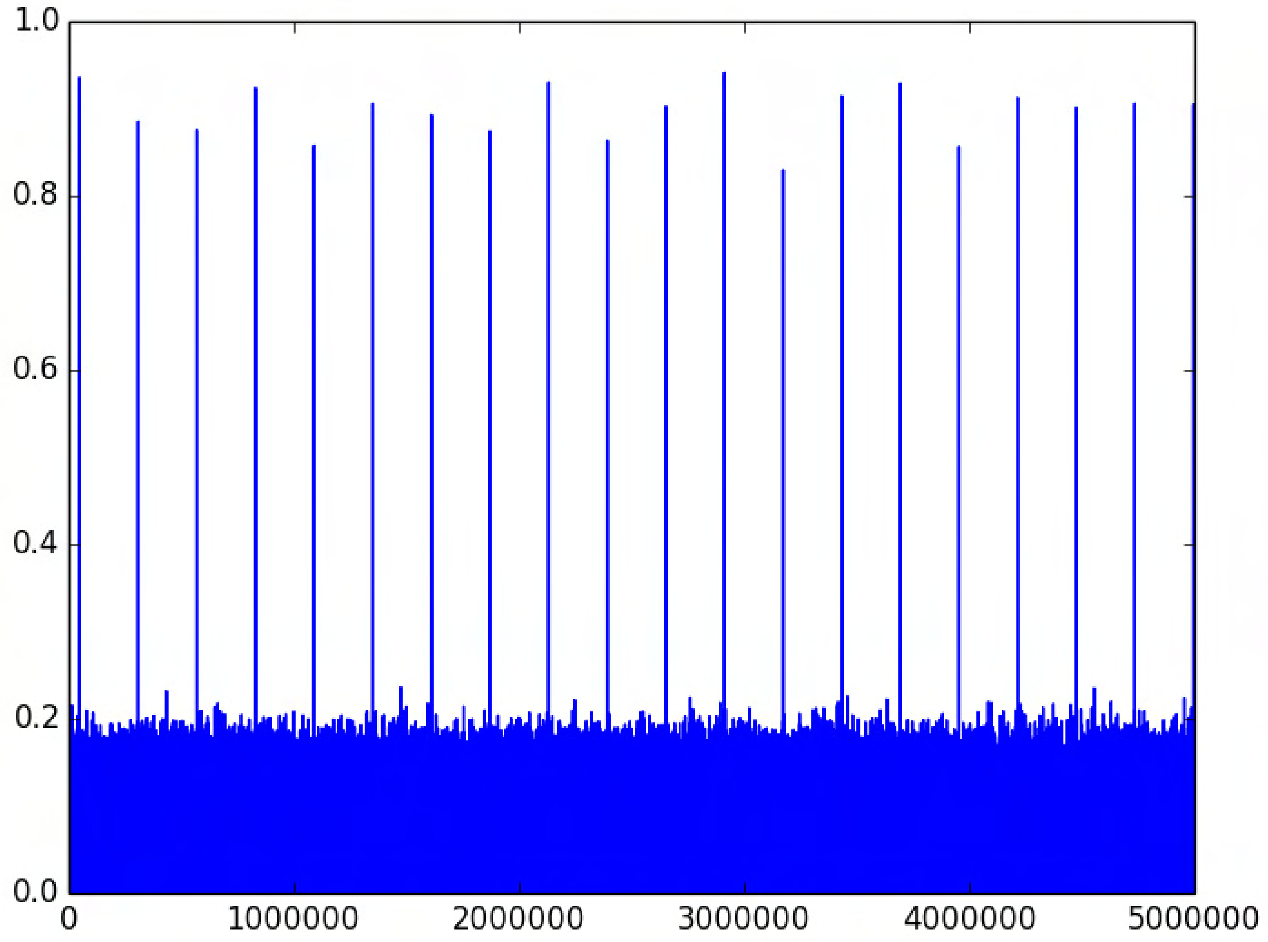


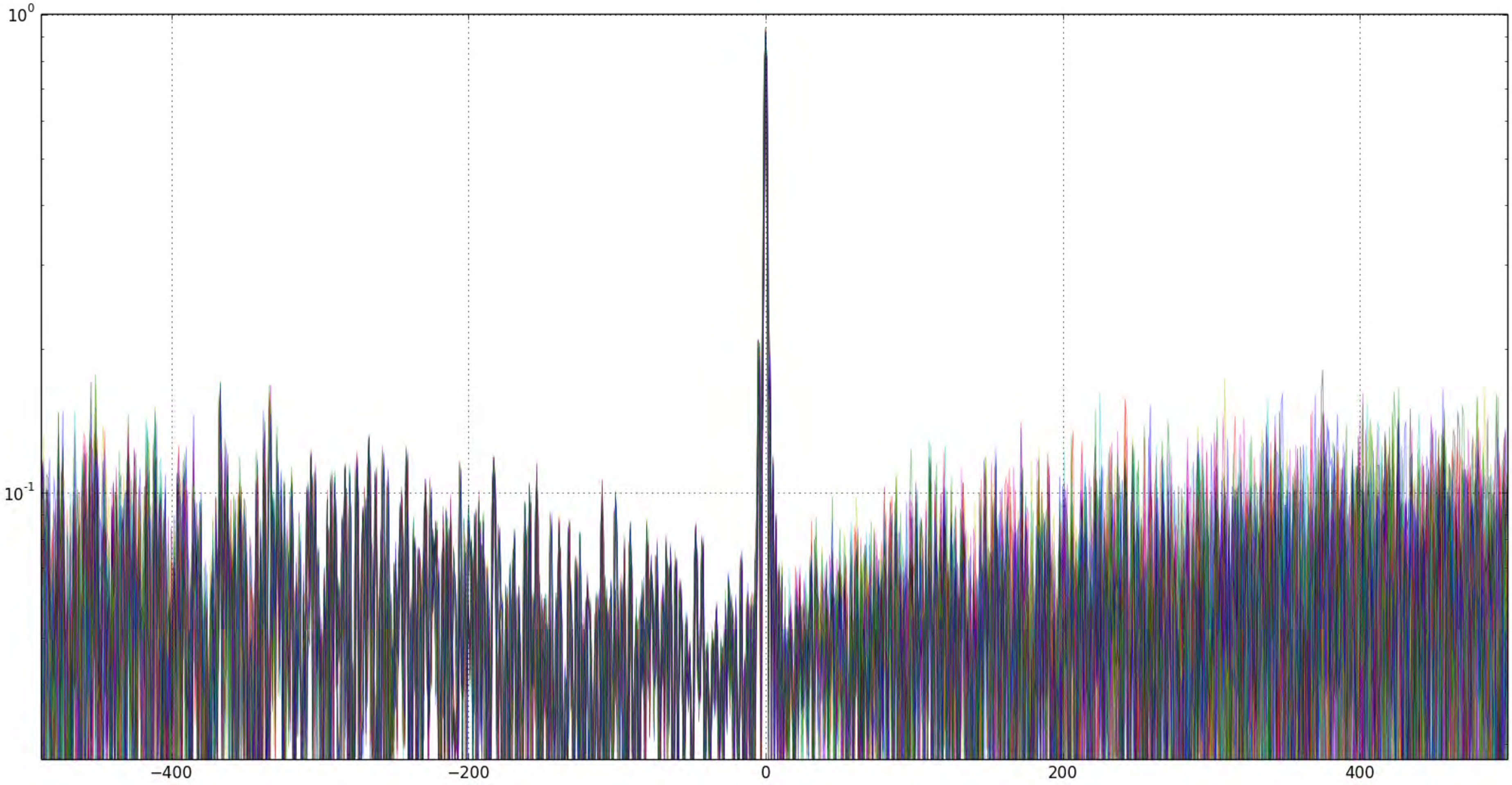
−50
−60
−70
−80
−90
−100
−110
−6000000
−4000000
−2000000
0
2000000
4000000
6000000

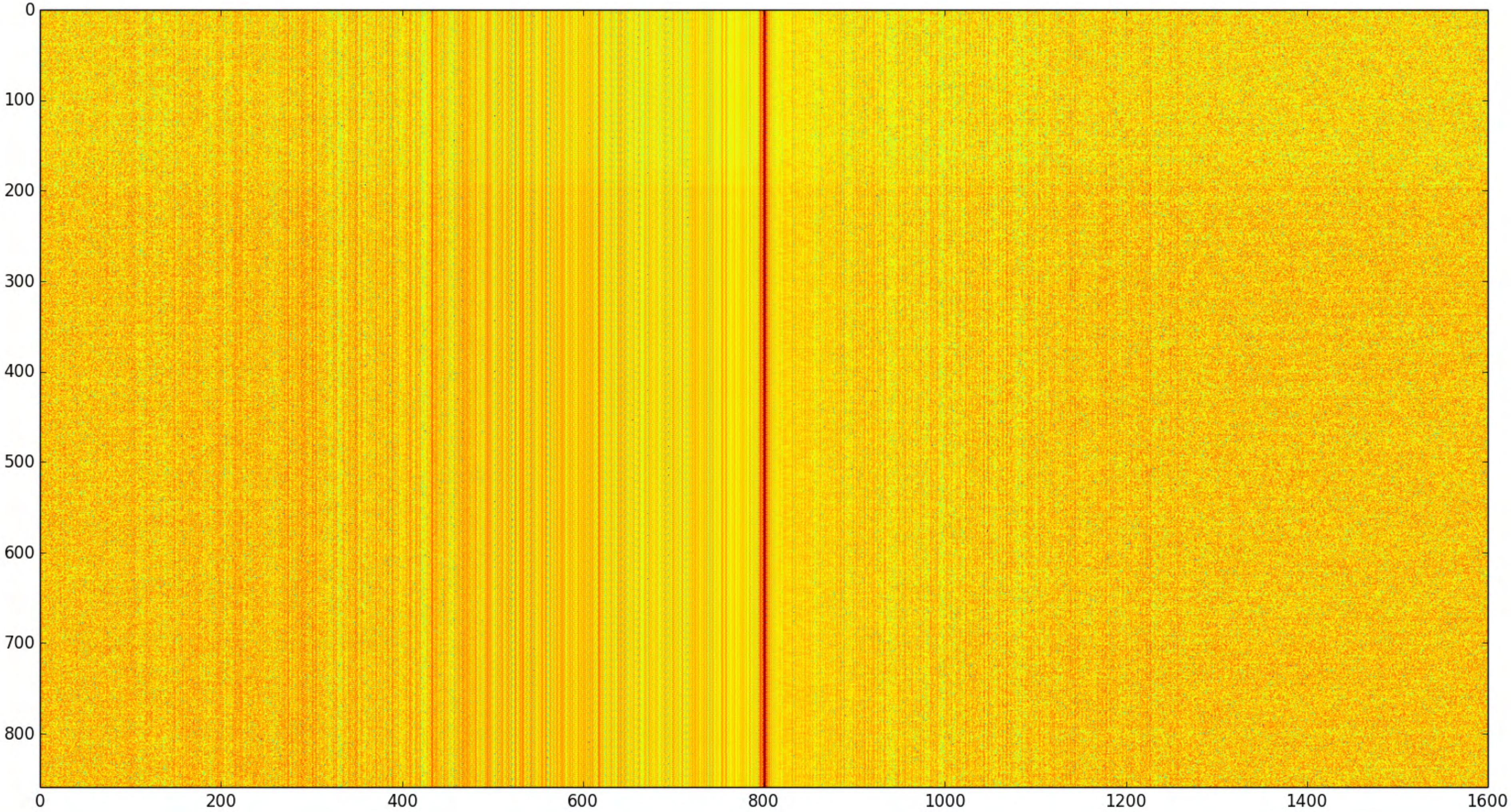
PN511

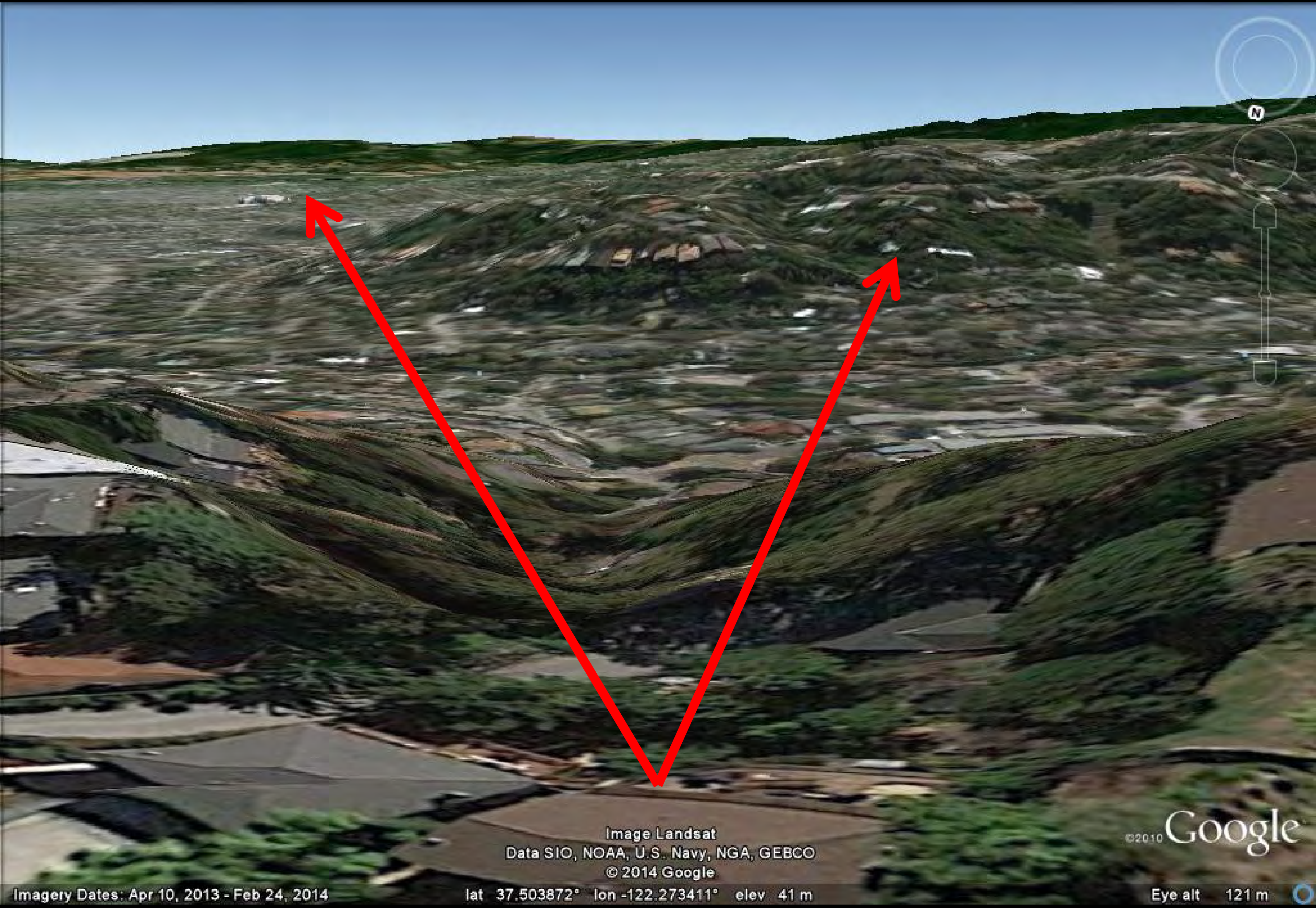


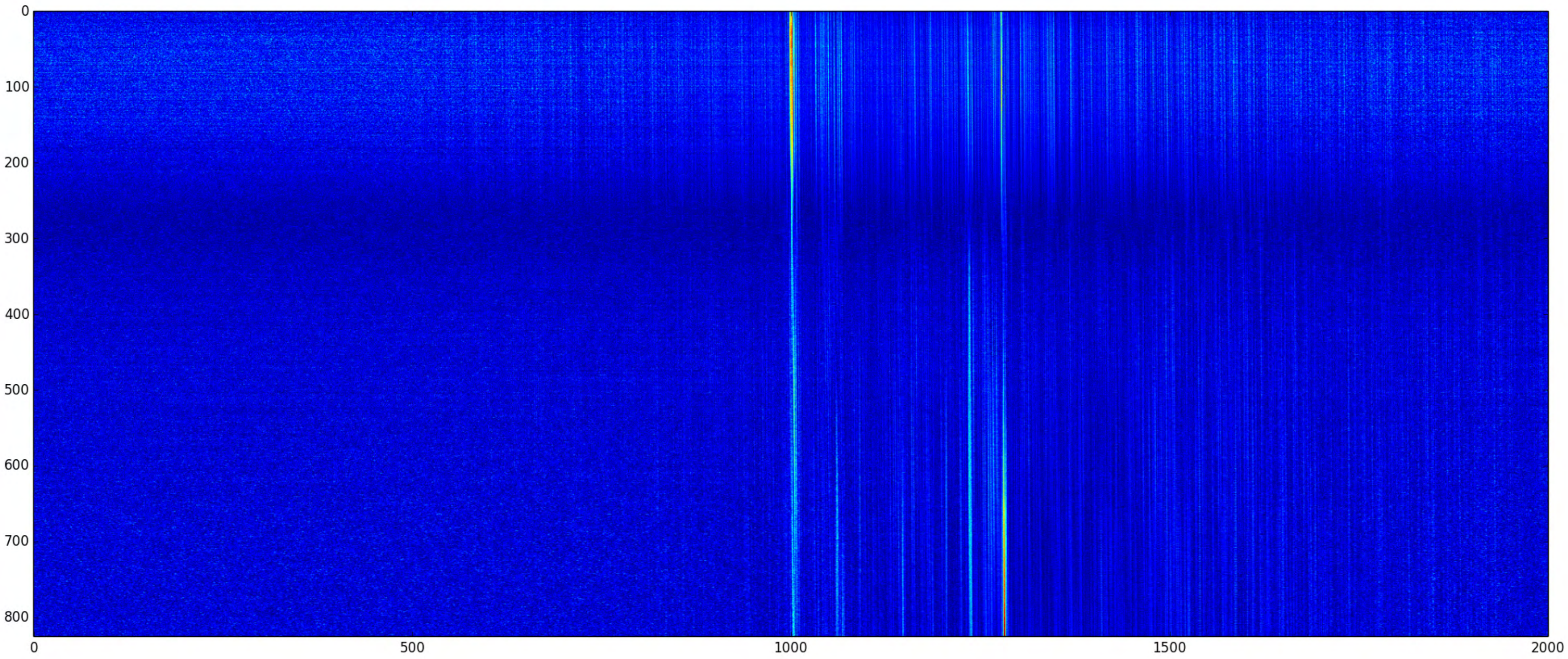
Correlation Peaks

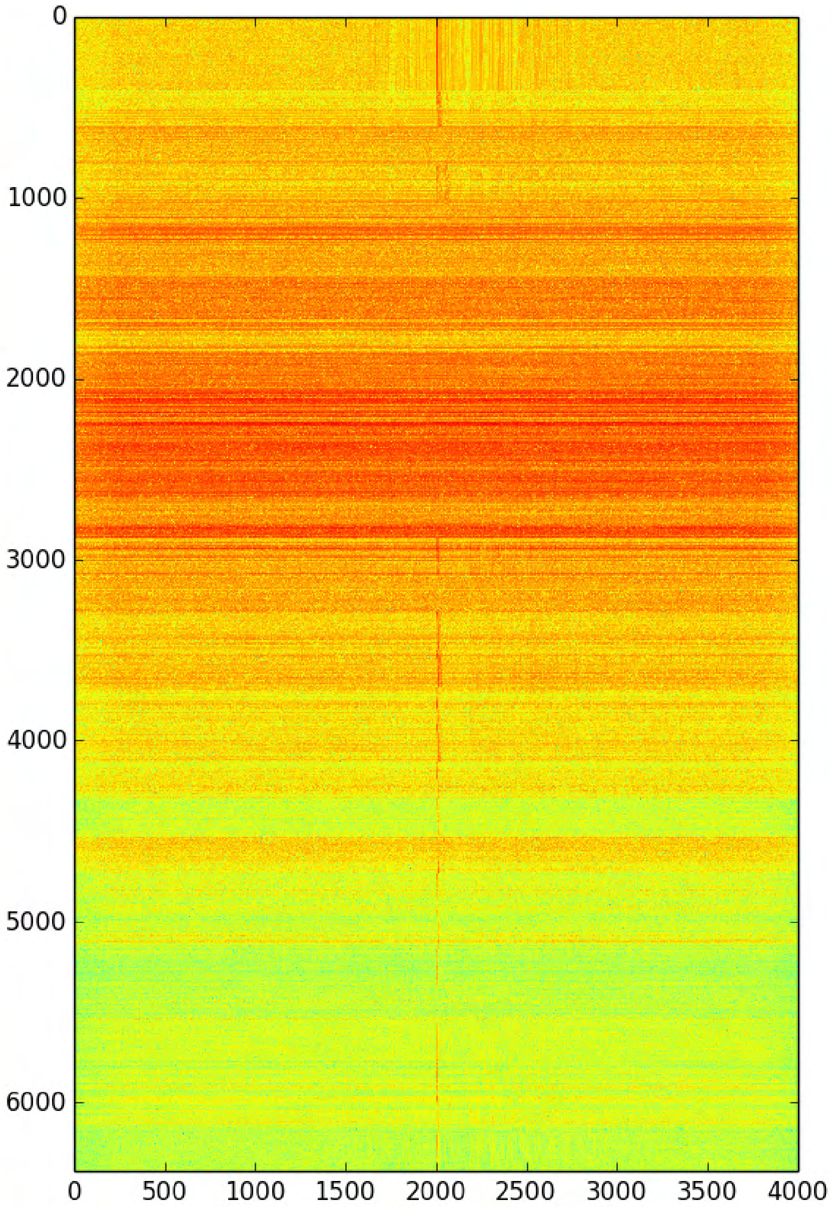


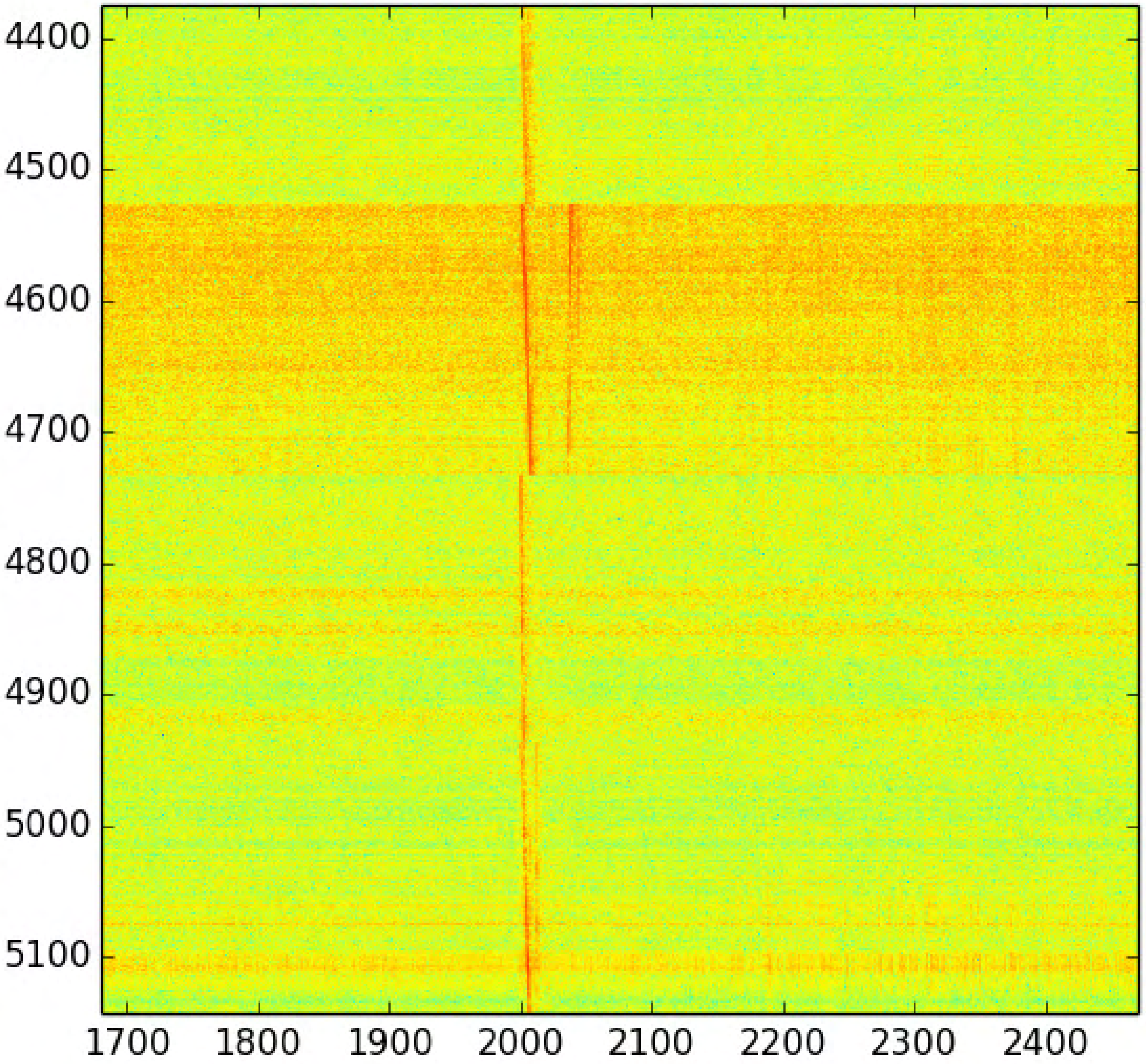

10^0
10^{-1}
−400
−200
0
200
400


0
100
200
300
400
500
600
700
800
0
200
400
600
800
1000
1200
1400
1600


N
Image Landsat
Data SIO, NOAA, U.S. Navy, NGA, GEBCO
© 2014 Google
©2010 Google
Imagery Dates: Apr 10, 2013 - Feb 24, 2014
lat 37.503872° lon -122.273411° elev 41 m
Eye alt 121 m


0
100
200
300
400
500
600
700
800
0
500
1000
1500
2000


0
1000
2000
3000
4000
5000
6000
0
500
1000
1500
2000
2500
3000
3500
4000


4400
4500
4600
4700
4800
4900
5000
5100
1700
1800
1900
2000
2100
2200
2300
2400

RFID

About FasTrak

FasTrak is the electronic toll system that allows customers to use any toll road, bridge, or express lane in California without stopping to pay. To participate, drivers must have a prepaid FasTrak account and a transponder properly installed on their windshield when they use a FasTrak toll road or

from a

accoun

Click he

Click h
accoun

1457950267

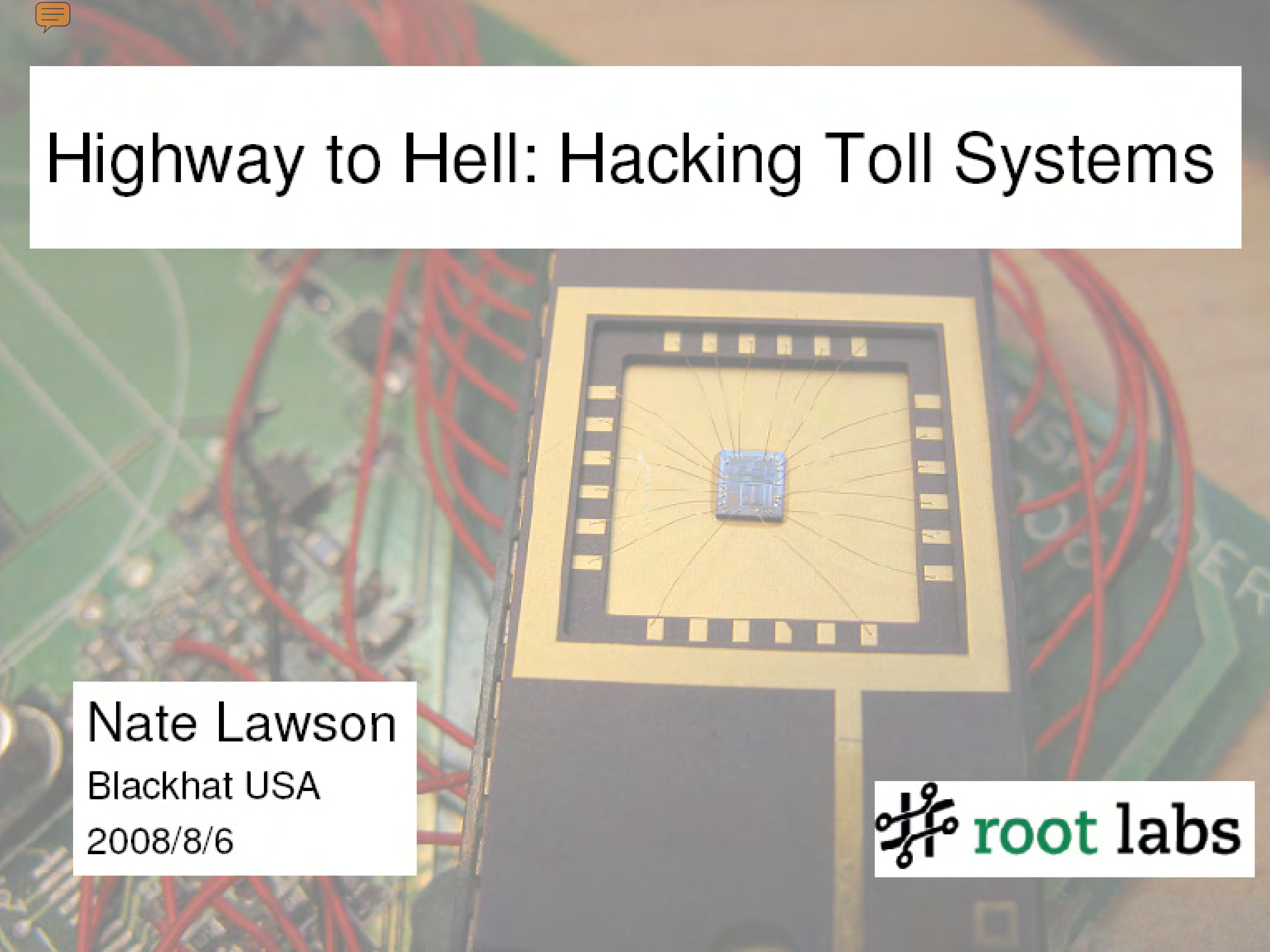
FASTRAK®

If found please return to:
FasTrak Customer Service Center
P.O. Box 26927
San Francisco, CA 94126
(877) 229-8655

RETURN
POSTAGE
GUARANTEED

FasTrak

- Traffic toll tag
  - Contains your ID
- Interrogation signal in 900 MHz ISM band
  - ‘Wake up’ signal activates tag
  - Pulse-Position Modulated payload
- Tag replies with backscatter modulation
  - Reflects transmitter’s RF energy (tiny amount)
  - Modulates reflection with Frequency Shift Keying



Highway to Hell: Hacking Toll Systems

Nate Lawson

Blackhat USA

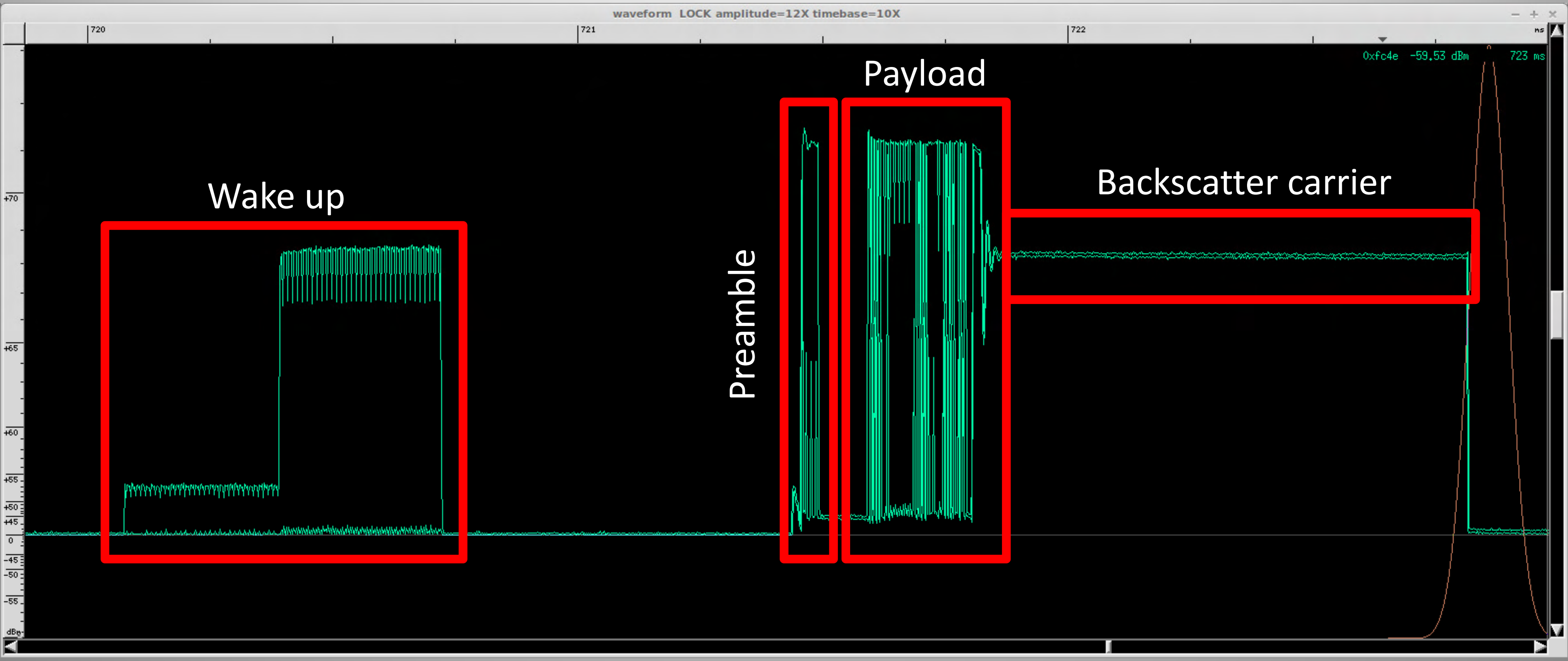
2008/8/6

root labs

LINCOLN
4.9 mi
0:10 to go
17.2mi
VOICE
19TH AVE
CANCEL
PUSH ENTER
A/C
MAX A/C
FRONT
REAR
RES +
CANCEL
- SET
0916.000.000
LO 0916.306.605
Tune 0916.306.605
T430s

Thank You for
NOT SMOKING
2
3
4
5

Interrogation Signal



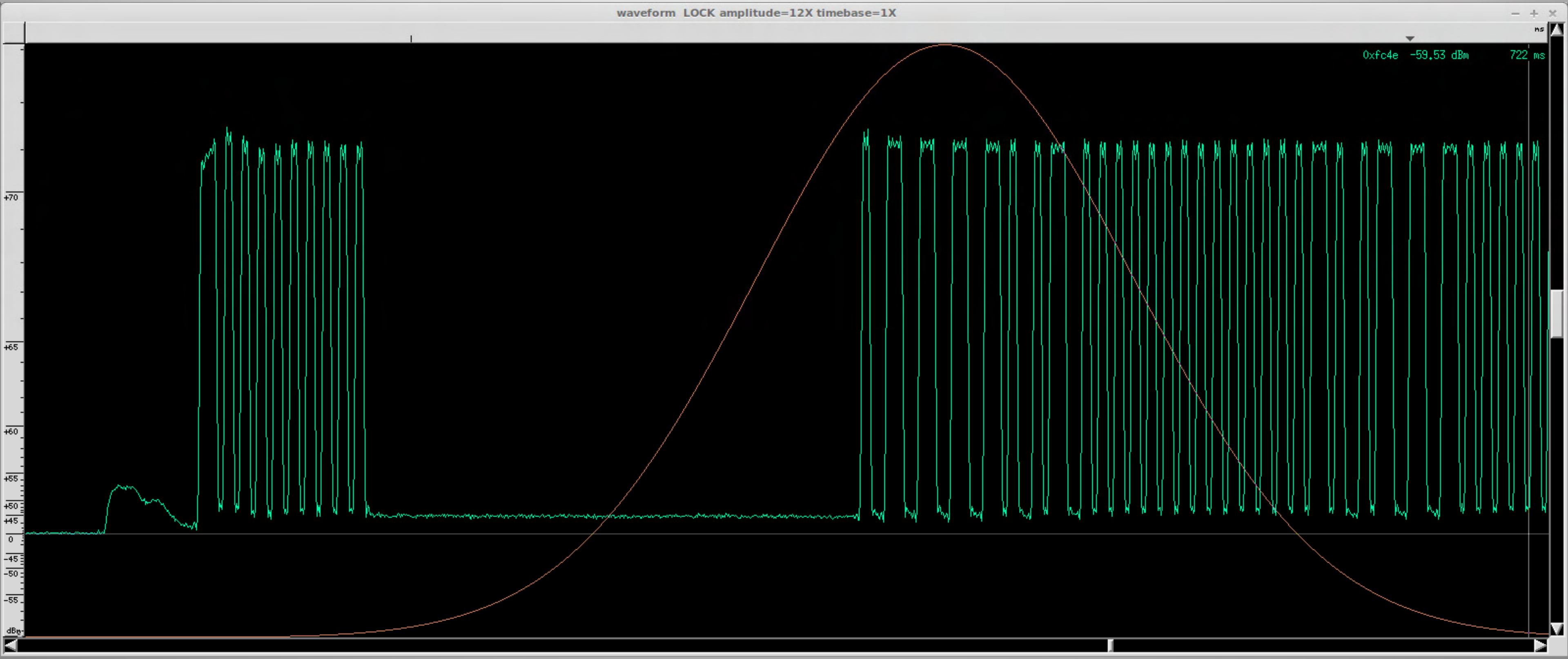
Wake up

Preamble

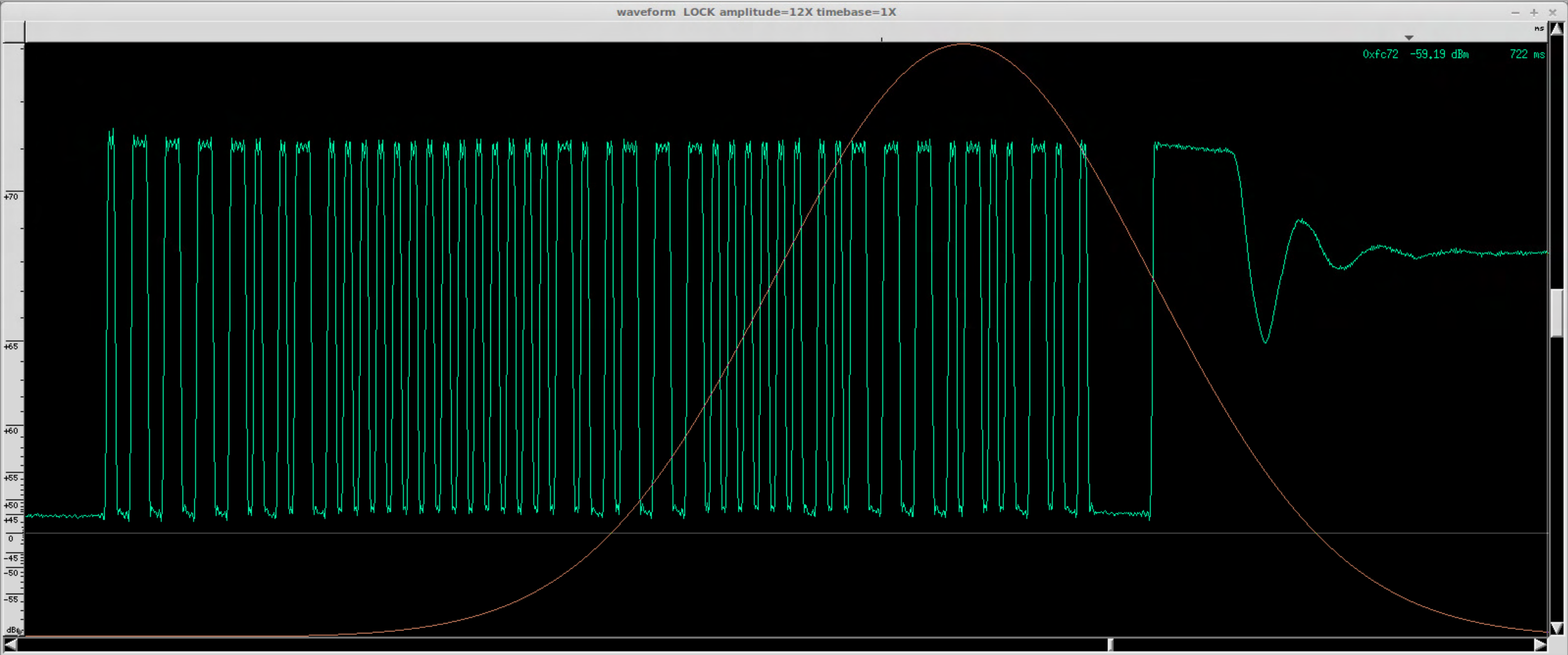
Payload

Backscatter carrier

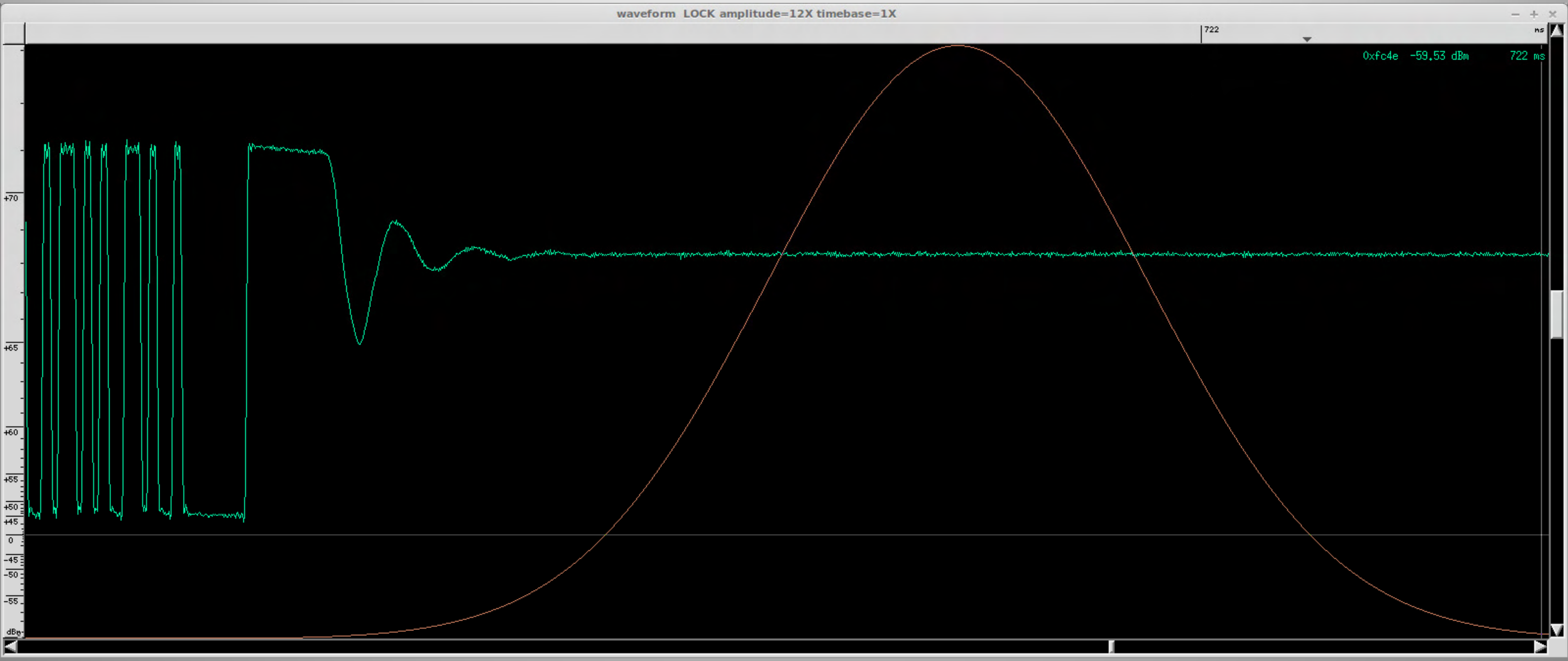
Wake Up/Preamble



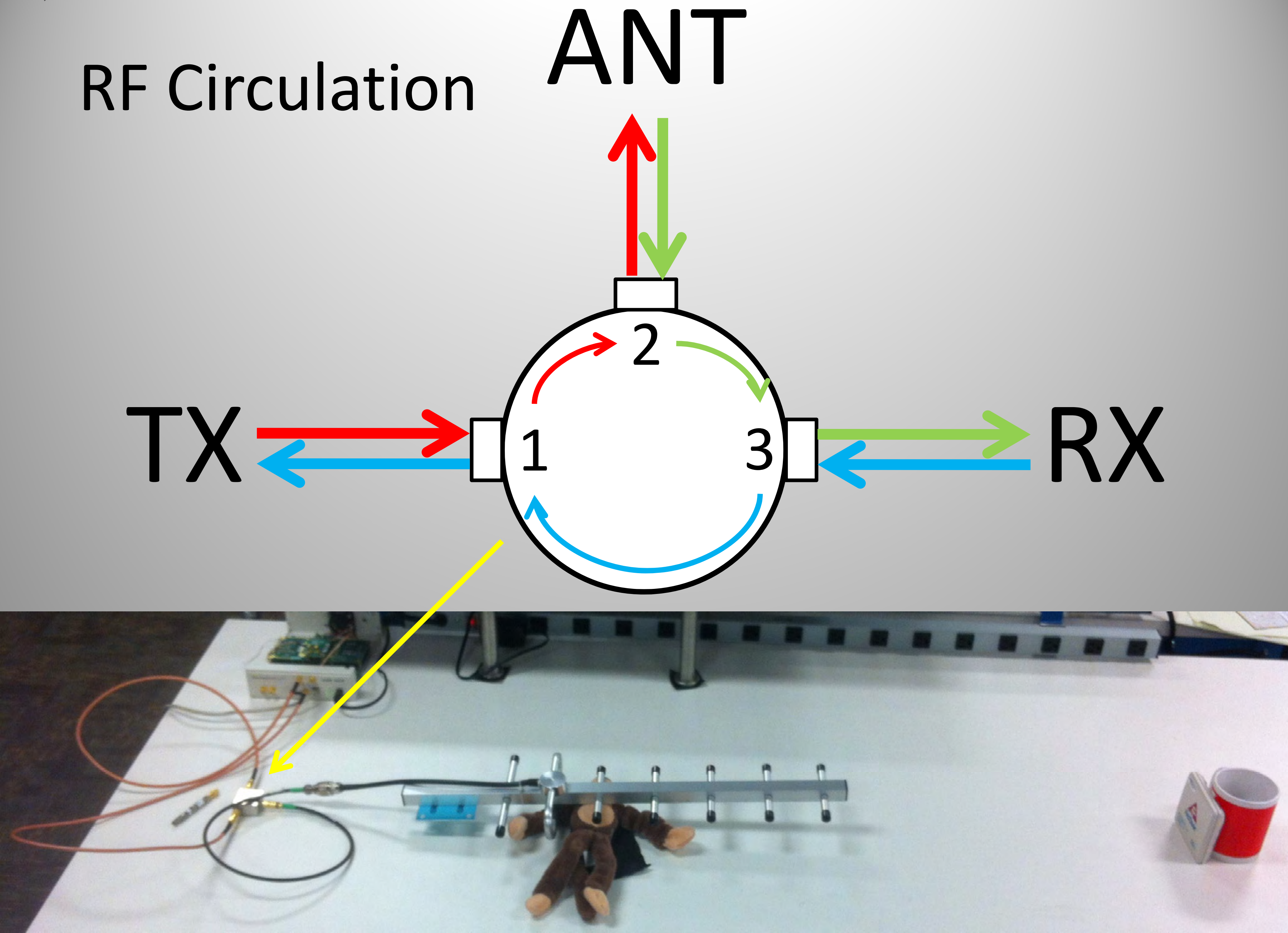
Interrogation Payload



Backscatter Carrier



RF Circulation



ANT

TX

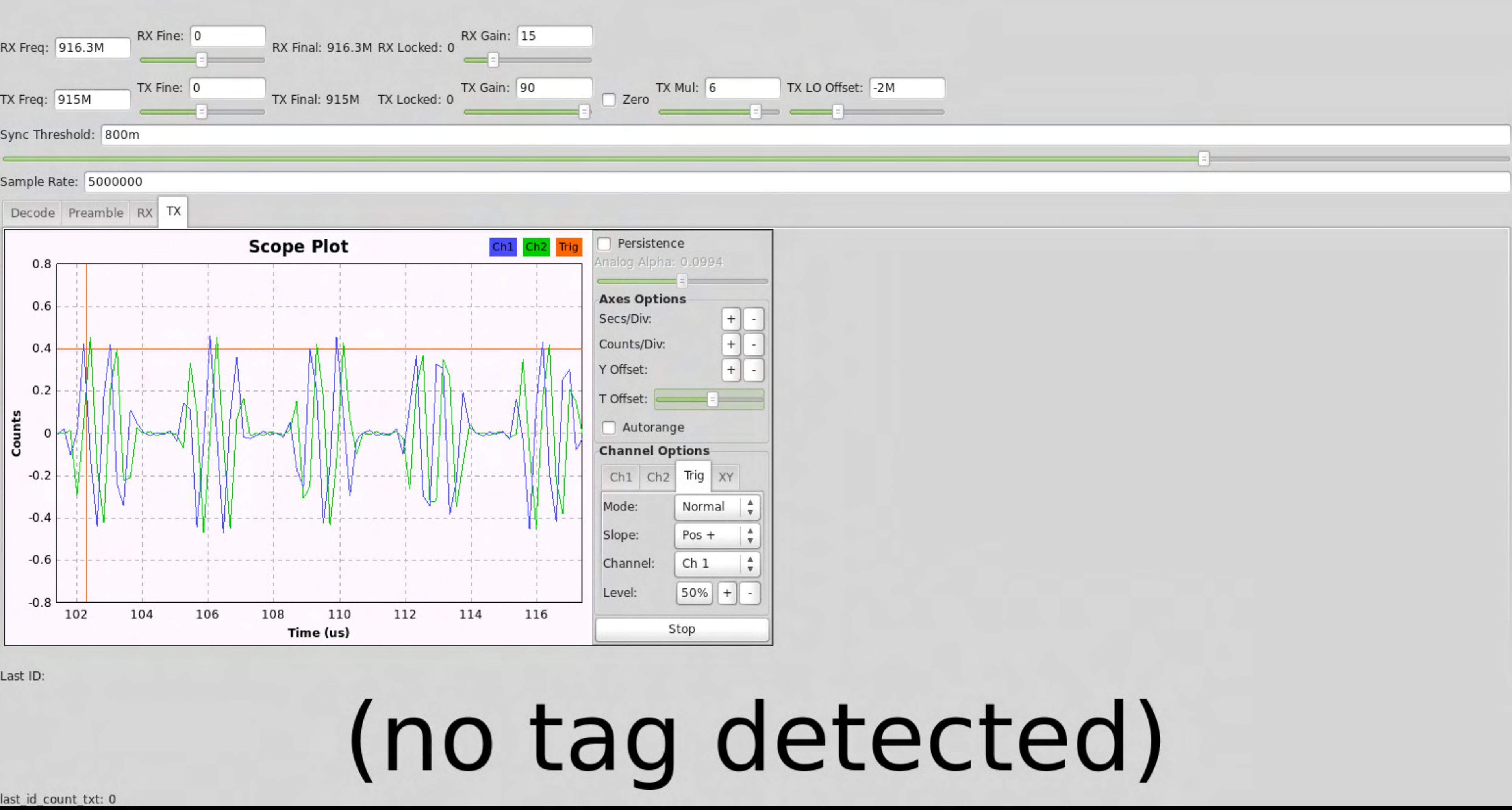
RX

2

1

3

Interrogation Signal



RX Freq: 916.3M
RX Fine: 0
RX Final: 916.3M
RX Locked: 0
RX Gain: 15

TX Freq: 915M
TX Fine: 0
TX Final: 915M
TX Locked: 0
TX Gain: 90
□ Zero
TX Mul: 6
TX LO Offset: -2M

Sync Threshold: 800m

Sample Rate: 5000000

□ Persistence
Analog Alpha: 0.0994

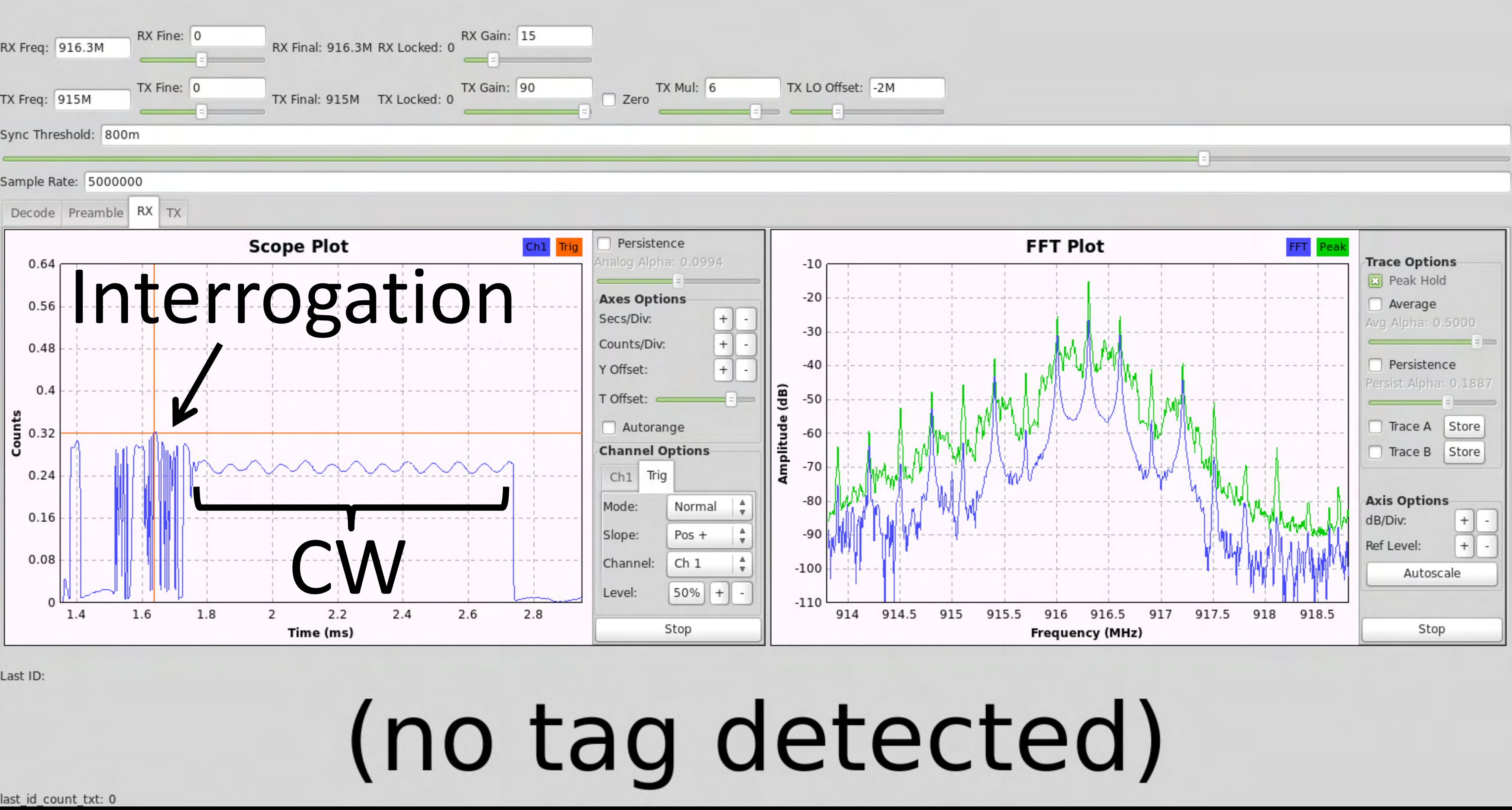
Mode: Normal
Slope: Pos +
Channel: Ch 1
Level: 50%

Last ID:

(no tag detected)

last_id_count_txt: 0

Received Signal



RX Freq: 916.3M RX Fine: 0 RX Final: 916.3M RX Locked: 0 RX Gain: 15

TX Freq: 915M TX Fine: 0 TX Final: 915M TX Locked: 0 TX Gain: 90 □ Zero TX Mul: 6 TX LO Offset: -2M

Sync Threshold: 800m

Sample Rate: 5000000

□ Persistence

Analog Alpha: 0.0994

□ Autorange

Mode: Normal

Slope: Pos +

Channel: Ch 1

Level: 50%

☒ Peak Hold

□ Average

Avg Alpha: 0.5000

□ Persistence

Persist Alpha: 0.1887

□ Trace A

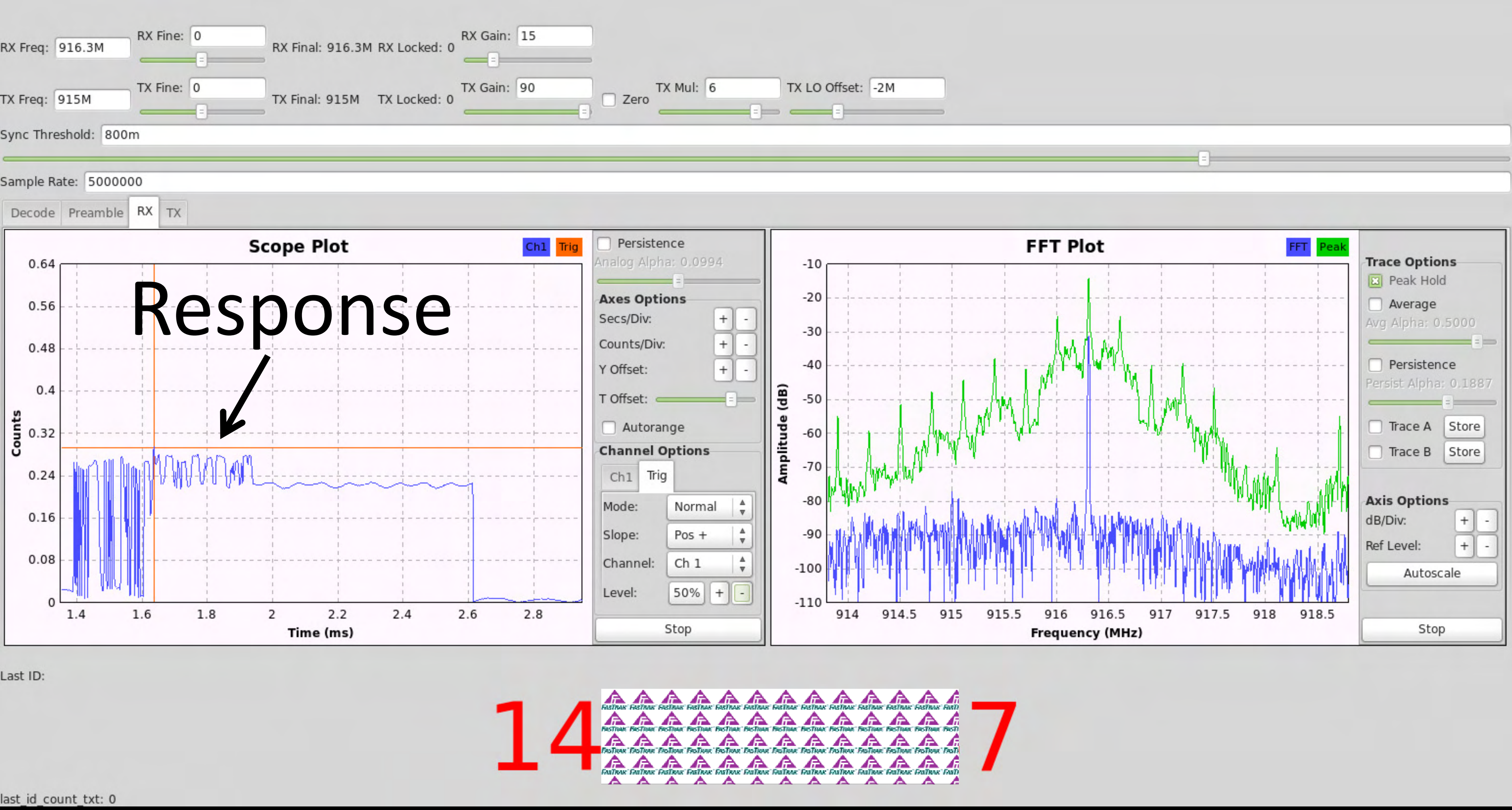
□ Trace B

Last ID:

last_id_count_txt: 0

(no tag detected)

Received Signal



RX Freq: 916.3M RX Fine: 0 RX Final: 916.3M RX Locked: 0 RX Gain: 15

TX Freq: 915M TX Fine: 0 TX Final: 915M TX Locked: 0 TX Gain: 90 □ Zero TX Mul: 6 TX LO Offset: -2M

Sync Threshold: 800m

Sample Rate: 5000000

□ Persistence
Analog Alpha: 0.0994

□ Autorange

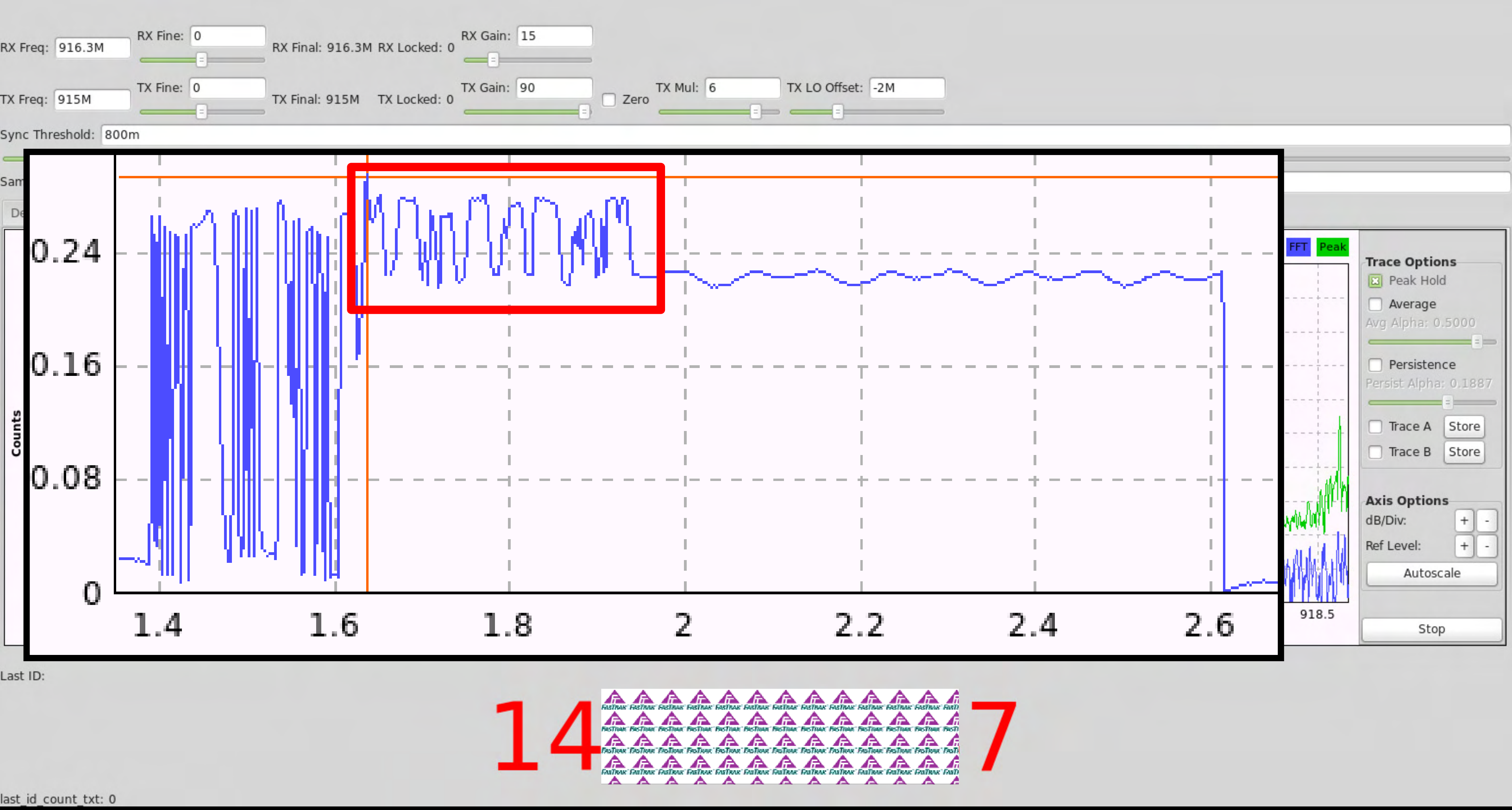
Mode: Normal
Slope: Pos +
Channel: Ch 1
Level: 50%

☒ Peak Hold
□ Average
Avg Alpha: 0.5000
□ Persistence
Persist Alpha: 0.1887
□ Trace A
□ Trace B

Last ID:

last_id_count_txt: 0

Received Signal



RX Freq: 916.3M RX Fine: 0 RX Final: 916.3M RX Locked: 0 RX Gain: 15

TX Freq: 915M TX Fine: 0 TX Final: 915M TX Locked: 0 TX Gain: 90 ☐ Zero TX Mul: 6 TX LO Offset: -2M

Sync Threshold: 800m

Trace Options

☒ Peak Hold

☐ Average

Avg Alpha: 0.5000

☐ Persistence

Persist Alpha: 0.1887

☐ Trace A

☐ Trace B

Axis Options

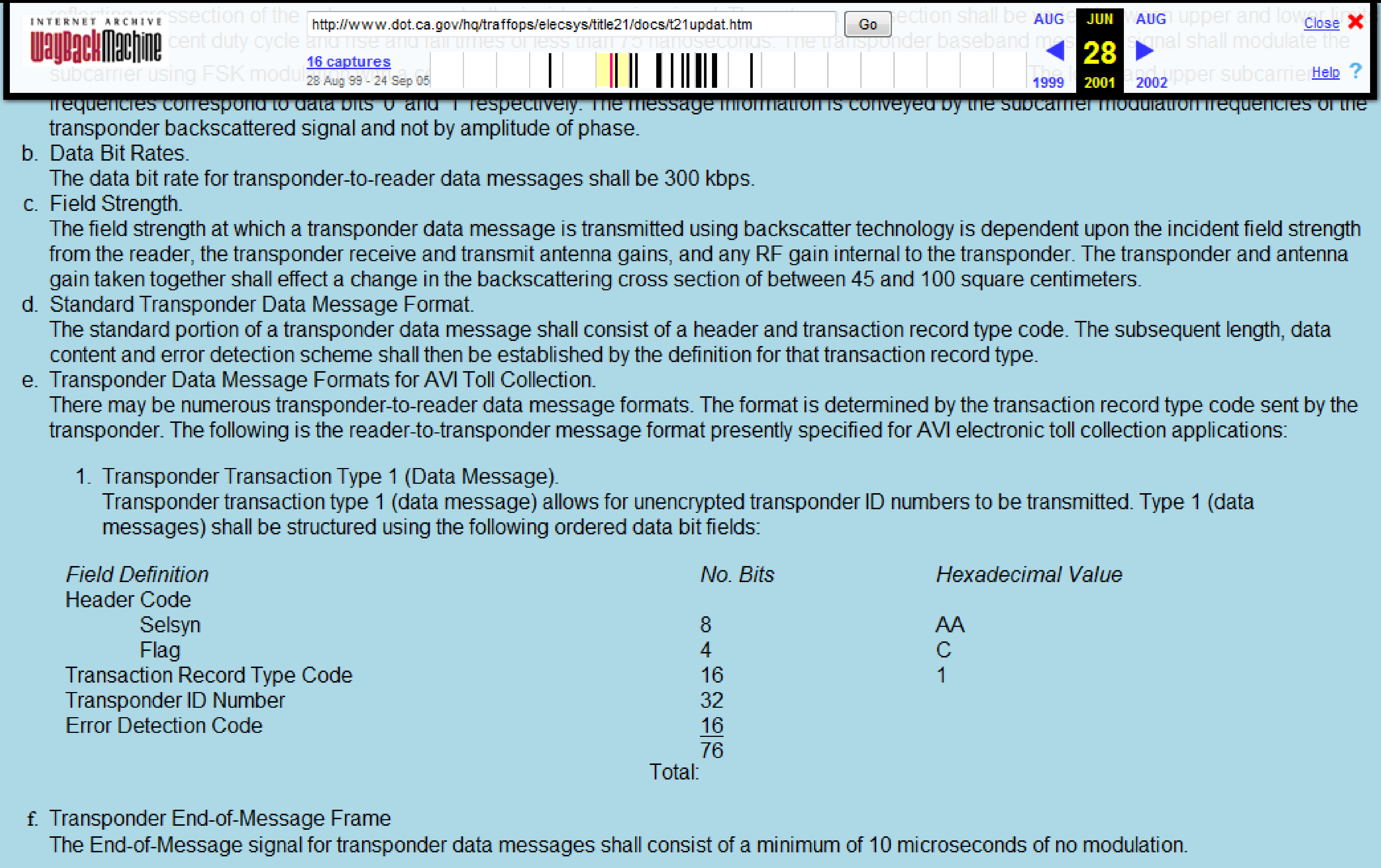
dB/Div:

Ref Level:

Last ID:

last_id_count_txt: 0

Title 21 Specification



reflecting crossection of the … section shall be … upper and lower limit … cent duty cycle and rise and fall times of less than 75 nanoseconds. The transponder baseband mes… signal shall modulate the subcarrier using FSK modul… with a ce… The l… and upper subcarrier frequencies correspond to data bits '0' and '1' respectively. The message information is conveyed by the subcarrier modulation frequencies of the transponder backscattered signal and not by amplitude of phase.

b. Data Bit Rates.
The data bit rate for transponder-to-reader data messages shall be 300 kbps.

c. Field Strength.
The field strength at which a transponder data message is transmitted using backscatter technology is dependent upon the incident field strength from the reader, the transponder receive and transmit antenna gains, and any RF gain internal to the transponder. The transponder and antenna gain taken together shall effect a change in the backscattering cross section of between 45 and 100 square centimeters.

d. Standard Transponder Data Message Format.
The standard portion of a transponder data message shall consist of a header and transaction record type code. The subsequent length, data content and error detection scheme shall then be established by the definition for that transaction record type.

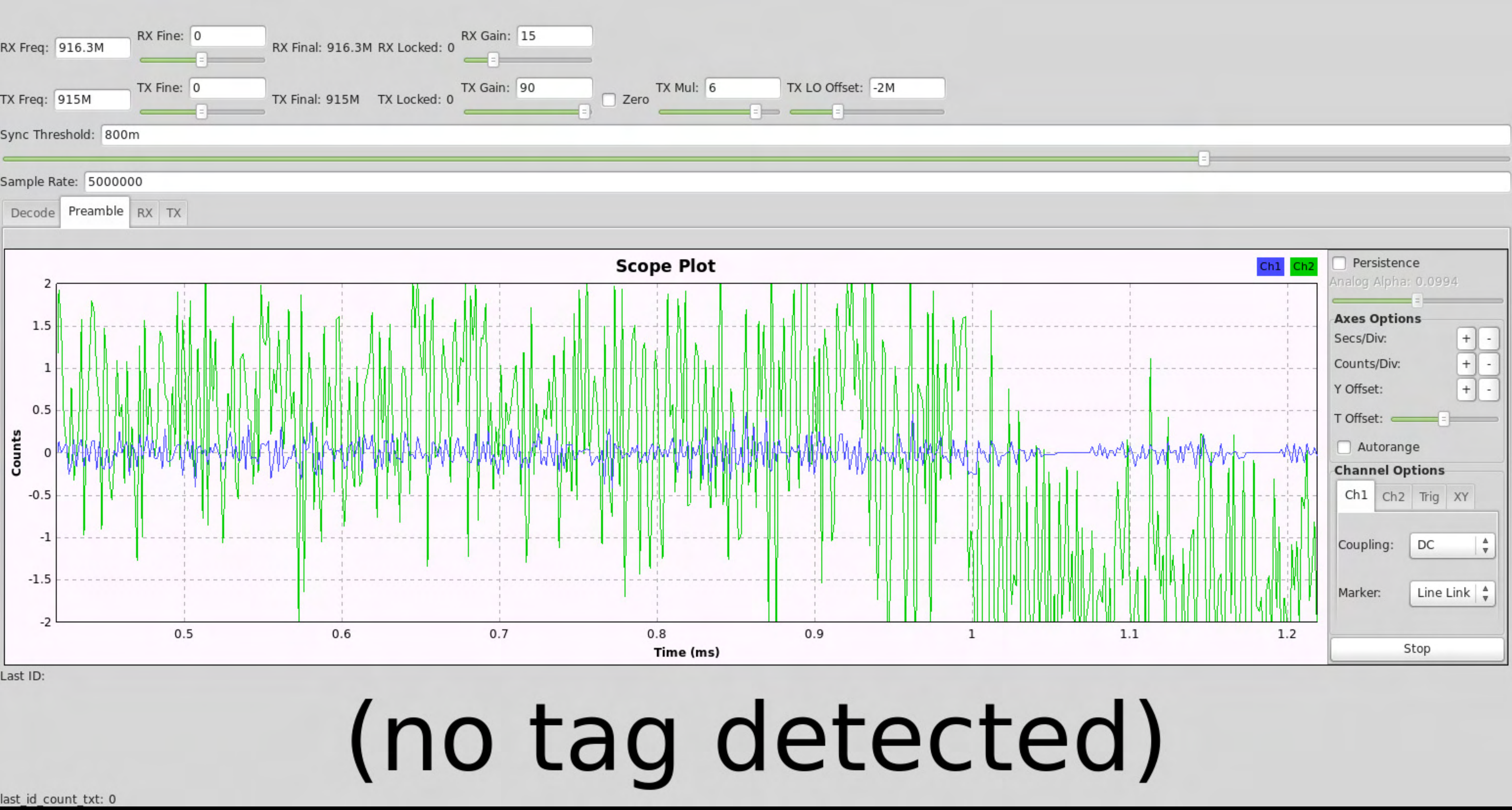
e. Transponder Data Message Formats for AVI Toll Collection.
There may be numerous transponder-to-reader data message formats. The format is determined by the transaction record type code sent by the transponder. The following is the reader-to-transponder message format presently specified for AVI electronic toll collection applications:

1. Transponder Transaction Type 1 (Data Message).
Transponder transaction type 1 (data message) allows for unencrypted transponder ID numbers to be transmitted. Type 1 (data messages) shall be structured using the following ordered data bit fields:

Field Definition	*No. Bits*	*Hexadecimal Value*
Header Code		
Selsyn	8	AA
Flag	4	C
Transaction Record Type Code	16	1
Transponder ID Number	32	
Error Detection Code	16	
Total:	76	

f. Transponder End-of-Message Frame
The End-of-Message signal for transponder data messages shall consist of a minimum of 10 microseconds of no modulation.

Preamble Detection



RX Freq: 916.3M
RX Fine: 0
RX Final: 916.3M RX Locked: 0
RX Gain: 15

TX Freq: 915M
TX Fine: 0
TX Final: 915M TX Locked: 0
TX Gain: 90
□ Zero
TX Mul: 6
TX LO Offset: -2M

Sync Threshold: 800m

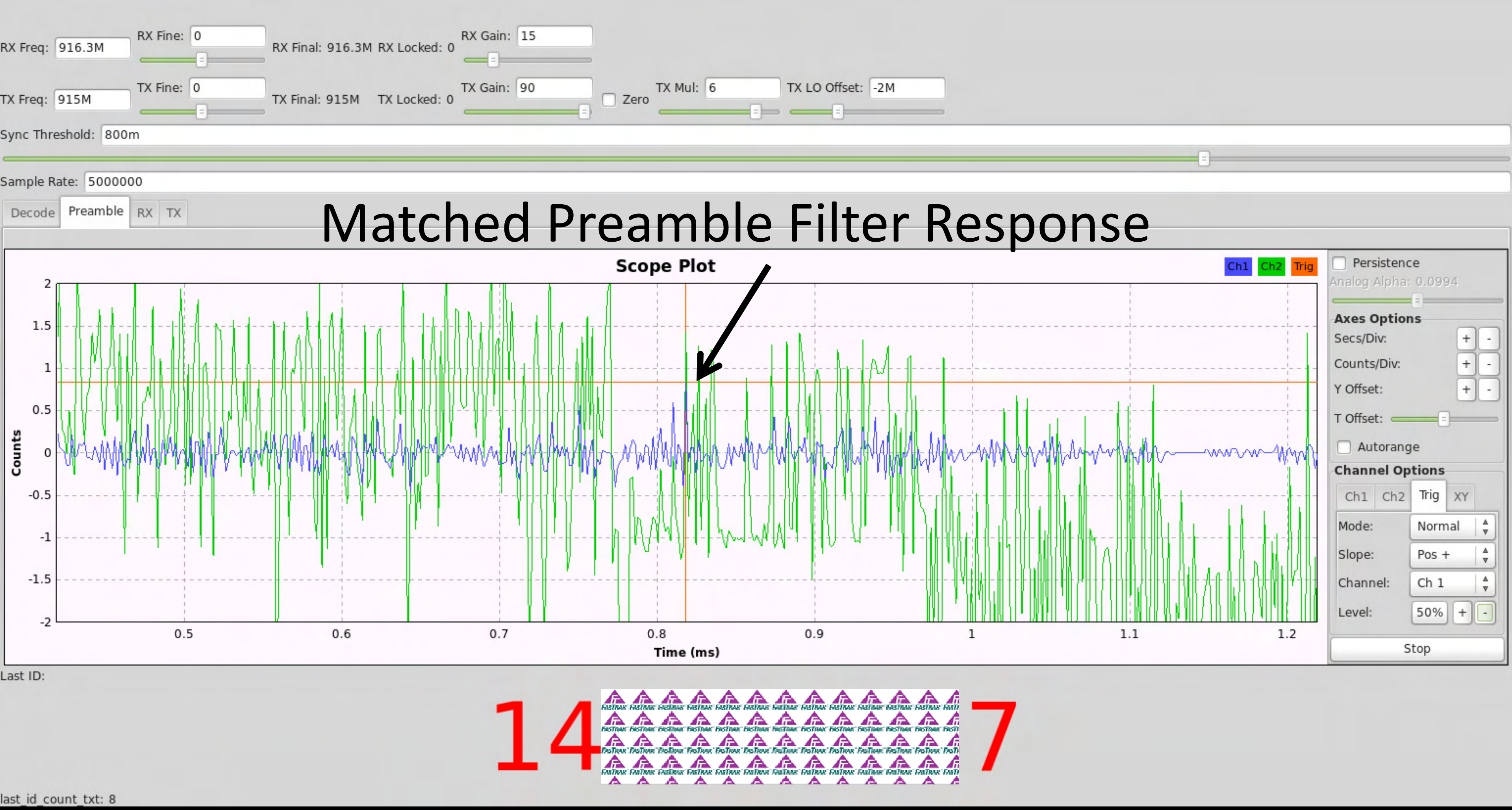
Sample Rate: 5000000

Last ID:

last_id_count_txt: 0

(no tag detected)

Preamble Detection



RX Freq: 916.3M

RX Fine: 0

RX Final: 916.3M RX Locked: 0

RX Gain: 15

TX Freq: 915M

TX Fine: 0

TX Final: 915M TX Locked: 0

TX Gain: 90

□ Zero

TX Mul: 6

TX LO Offset: -2M

Sync Threshold: 800m

Sample Rate: 5000000

Matched Preamble Filter Response

□ Persistence

Analog Alpha: 0.0994

Mode: Normal

Slope: Pos +

Channel: Ch 1

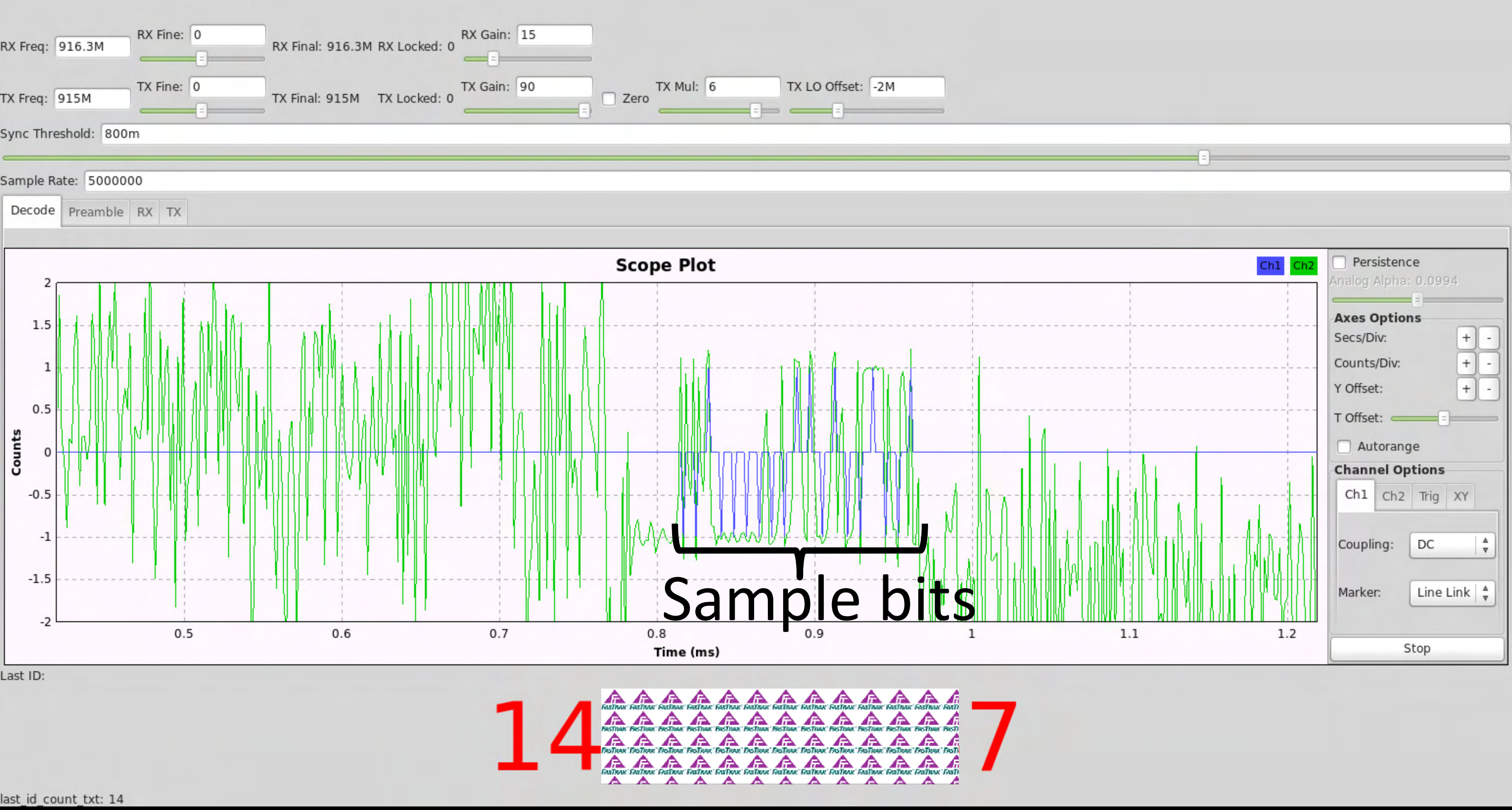
Level: 50%

Last ID:

14 7

last_id_count_txt: 8

Slicer Time!



RX Freq: 916.3M RX Fine: 0 RX Final: 916.3M RX Locked: 0 RX Gain: 15

TX Freq: 915M TX Fine: 0 TX Final: 915M TX Locked: 0 TX Gain: 90 □ Zero TX Mul: 6 TX LO Offset: -2M

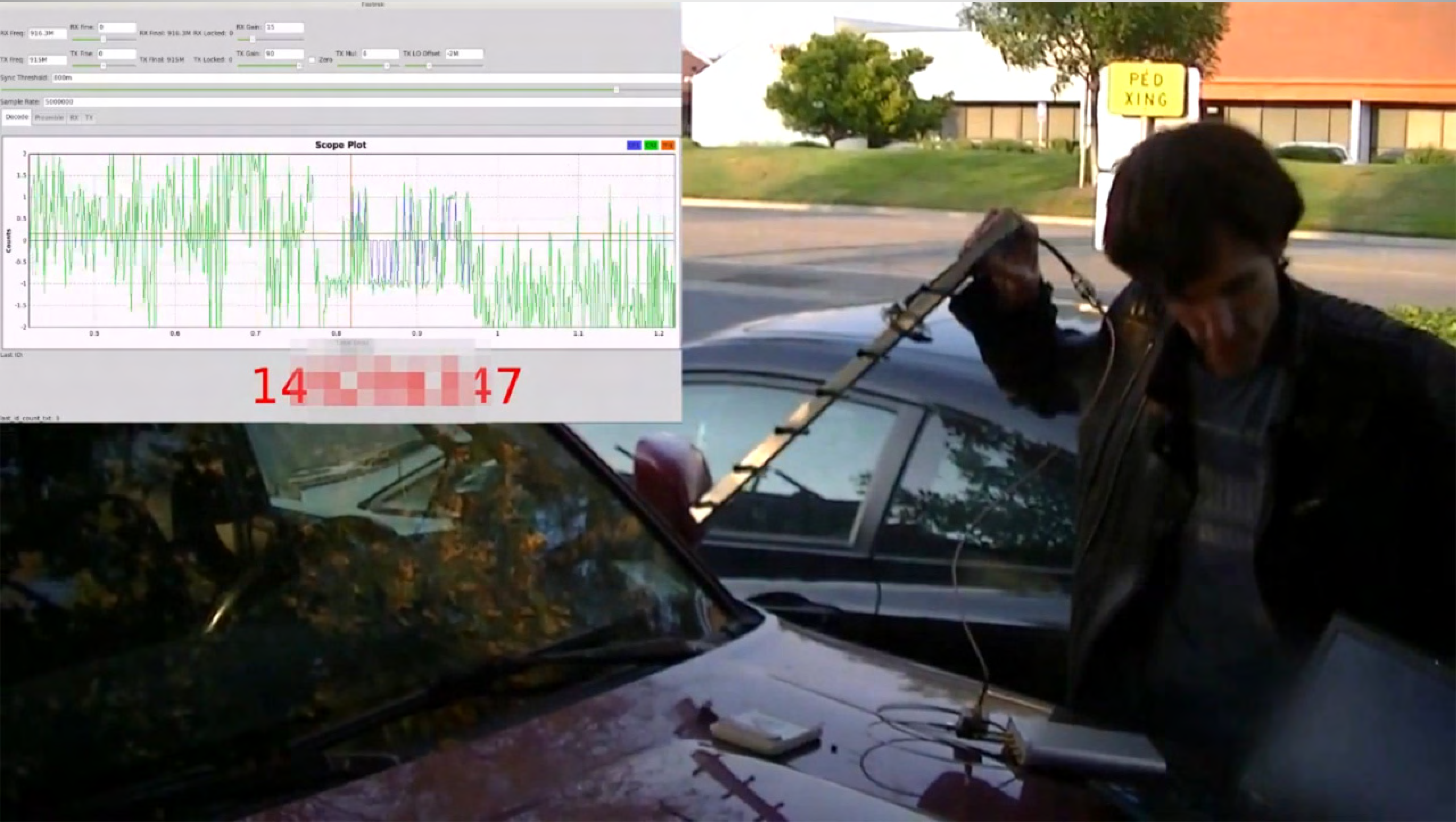
Sync Threshold: 800m

Sample Rate: 5000000

Last ID:

last_id_count_txt: 14

Reading a Tag Outside



RX Freq: 916.3M RX Fine: 0 RX Final: 916.3M RX Locked: 0 RX Gain: 15

TX Freq: 915M TX Fine: 0 TX Final: 915M TX Locked: 0 TX Gain: 90 □ Zero TX Mul: 6 TX LO Offset: -2M

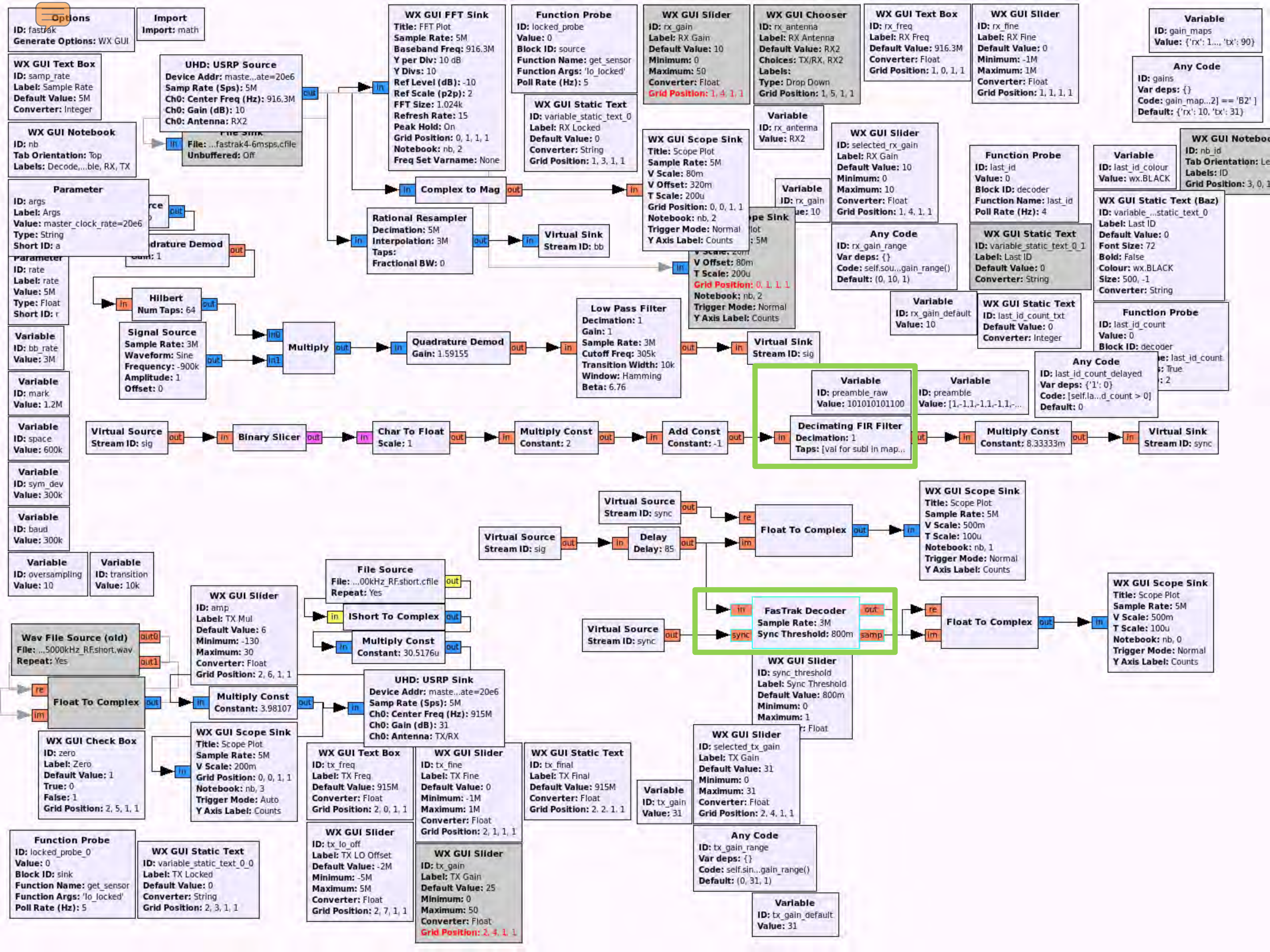
Sync Threshold: 800m

Sample Rate: 5000000

Last ID:

14[redacted]47

last_id_count_txt: 3



Options
ID: fastrak
Generate Options: WX GUI

Import
Import: math

WX GUI Text Box
ID: samp_rate
Label: Sample Rate
Default Value: 5M
Converter: Integer

UHD: USRP Source
Device Addr: maste...ate=20e6
Samp Rate (Sps): 5M
Ch0: Center Freq (Hz): 916.3M
Ch0: Gain (dB): 10
Ch0: Antenna: RX2

File Sink
File: ...fastrak4-6msps.cfile
Unbuffered: Off

WX GUI Notebook
ID: nb
Tab Orientation: Top
Labels: Decode,...ble, RX, TX

Parameter
ID: args
Label: Args
Value: master_clock_rate=20e6
Type: String
Short ID: a

Parameter
ID: rate
Label: rate
Value: 5M
Type: Float
Short ID: r

...drature Demod
...ain: 1

Hilbert
Num Taps: 64

Signal Source
Sample Rate: 3M
Waveform: Sine
Frequency: -900k
Amplitude: 1
Offset: 0

Multiply

Quadrature Demod
Gain: 1.59155

WX GUI FFT Sink
Title: FFT Plot
Sample Rate: 5M
Baseband Freq: 916.3M
Y per Div: 10 dB
Y Divs: 10
Ref Level (dB): -10
Ref Scale (p2p): 2
FFT Size: 1.024k
Refresh Rate: 15
Peak Hold: On
Grid Position: 0, 1, 1, 1
Notebook: nb, 2
Freq Set Varname: None

Complex to Mag

Rational Resampler
Decimation: 5M
Interpolation: 3M
Taps:
Fractional BW: 0

Virtual Sink
Stream ID: bb

Function Probe
ID: locked_probe
Value: 0
Block ID: source
Function Name: get_sensor
Function Args: 'lo_locked'
Poll Rate (Hz): 5

WX GUI Static Text
ID: variable_static_text_0
Label: RX Locked
Default Value: 0
Converter: String
Grid Position: 1, 3, 1, 1

WX GUI Slider
ID: rx_gain
Label: RX Gain
Default Value: 10
Minimum: 0
Maximum: 50
Converter: Float
Grid Position: 1, 4, 1, 1

WX GUI Chooser
ID: rx_antenna
Label: RX Antenna
Default Value: RX2
Choices: TX/RX, RX2
Labels:
Type: Drop Down
Grid Position: 1, 5, 1, 1

Variable
ID: rx_antenna
Value: RX2

WX GUI Text Box
ID: rx_freq
Label: RX Freq
Default Value: 916.3M
Converter: Float
Grid Position: 1, 0, 1, 1

WX GUI Slider
ID: rx_fine
Label: RX Fine
Default Value: 0
Minimum: -1M
Maximum: 1M
Converter: Float
Grid Position: 1, 1, 1, 1

Variable
ID: gain_maps
Value: {'rx': 1..., 'tx': 90}

Any Code
ID: gains
Var deps: {}
Code: gain_map...2] == 'B2']
Default: {'rx': 10, 'tx': 31}

WX GUI Scope Sink
Title: Scope Plot
Sample Rate: 5M
V Scale: 80m
V Offset: 320m
T Scale: 200u
Grid Position: 0, 0, 1, 1
Notebook: nb, 2
Trigger Mode: Normal
Y Axis Label: Counts

...pe Sink
...lot
...: 5M
V Scale: 20m
V Offset: 80m
T Scale: 200u
Grid Position: 0, 1, 1, 1
Notebook: nb, 2
Trigger Mode: Normal
Y Axis Label: Counts

Variable
ID: rx_gain
...e: 10

WX GUI Slider
ID: selected_rx_gain
Label: RX Gain
Default Value: 10
Minimum: 0
Maximum: 10
Converter: Float
Grid Position: 1, 4, 1, 1

Any Code
ID: rx_gain_range
Var deps: {}
Code: self.sou...gain_range()
Default: (0, 10, 1)

Variable
ID: rx_gain_default
Value: 10

Function Probe
ID: last_id
Value: 0
Block ID: decoder
Function Name: last_id
Poll Rate (Hz): 4

WX GUI Static Text
ID: variable_static_text_0_1
Label: Last ID
Default Value: 0
Converter: String

WX GUI Static Text
ID: last_id_count_txt
Default Value: 0
Converter: Integer

Variable
ID: last_id_colour
Value: wx.BLACK

WX GUI Notebo...
ID: nb_id
Tab Orientation: Le...
Labels: ID
Grid Position: 3, 0, 1...

WX GUI Static Text (Baz)
ID: variable_...static_text_0
Label: Last ID
Default Value: 0
Font Size: 72
Bold: False
Colour: wx.BLACK
Size: 500, -1
Converter: String

Function Probe
ID: last_id_count
Value: 0
Block ID: decoder
...e: last_id_count
...: True
...: 2

Any Code
ID: last_id_count_delayed
Var deps: {'1': 0}
Code: [self.la...d_count > 0]
Default: 0

Low Pass Filter
Decimation: 1
Gain: 1
Sample Rate: 3M
Cutoff Freq: 305k
Transition Width: 10k
Window: Hamming
Beta: 6.76

Virtual Sink
Stream ID: sig

Variable
ID: bb_rate
Value: 3M

Variable
ID: mark
Value: 1.2M

Variable
ID: space
Value: 600k

Variable
ID: sym_dev
Value: 300k

Variable
ID: baud
Value: 300k

Variable
ID: oversampling
Value: 10

Variable
ID: transition
Value: 10k

Virtual Source
Stream ID: sig

Binary Slicer

Char To Float
Scale: 1

Multiply Const
Constant: 2

Add Const
Constant: -1

Variable
ID: preamble_raw
Value: 101010101100

Decimating FIR Filter
Decimation: 1
Taps: [val for subl in map...

Variable
ID: preamble
Value: [1,-1,1,-1,1,-1,1,-...

Multiply Const
Constant: 8.33333m

Virtual Sink
Stream ID: sync

Virtual Source
Stream ID: sync

Virtual Source
Stream ID: sig

Delay
Delay: 85

Float To Complex

WX GUI Scope Sink
Title: Scope Plot
Sample Rate: 5M
V Scale: 500m
T Scale: 100u
Notebook: nb, 1
Trigger Mode: Normal
Y Axis Label: Counts

File Source
File: ...00kHz_RF.short.cfile
Repeat: Yes

IShort To Complex

Multiply Const
Constant: 30.5176u

Wav File Source (old)
File: ...5000kHz_RF.short.wav
Repeat: Yes

Float To Complex

WX GUI Slider
ID: amp
Label: TX Mul
Default Value: 6
Minimum: -130
Maximum: 30
Converter: Float
Grid Position: 2, 6, 1, 1

Multiply Const
Constant: 3.98107

UHD: USRP Sink
Device Addr: maste...ate=20e6
Samp Rate (Sps): 5M
Ch0: Center Freq (Hz): 915M
Ch0: Gain (dB): 31
Ch0: Antenna: TX/RX

Virtual Source
Stream ID: sync

FasTrak Decoder
Sample Rate: 3M
Sync Threshold: 800m

Float To Complex

WX GUI Scope Sink
Title: Scope Plot
Sample Rate: 5M
V Scale: 500m
T Scale: 100u
Notebook: nb, 0
Trigger Mode: Normal
Y Axis Label: Counts

WX GUI Slider
ID: sync_threshold
Label: Sync Threshold
Default Value: 800m
Minimum: 0
Maximum: 1
...r: Float

WX GUI Check Box
ID: zero
Label: Zero
Default Value: 1
True: 0
False: 1
Grid Position: 2, 5, 1, 1

WX GUI Scope Sink
Title: Scope Plot
Sample Rate: 5M
V Scale: 200m
Grid Position: 0, 0, 1, 1
Notebook: nb, 3
Trigger Mode: Auto
Y Axis Label: Counts

WX GUI Text Box
ID: tx_freq
Label: TX Freq
Default Value: 915M
Converter: Float
Grid Position: 2, 0, 1, 1

WX GUI Slider
ID: tx_fine
Label: TX Fine
Default Value: 0
Minimum: -1M
Maximum: 1M
Converter: Float
Grid Position: 2, 1, 1, 1

WX GUI Static Text
ID: tx_final
Label: TX Final
Default Value: 915M
Converter: Float
Grid Position: 2, 2, 1, 1

Variable
ID: tx_gain
Value: 31

WX GUI Slider
ID: selected_tx_gain
Label: TX Gain
Default Value: 31
Minimum: 0
Maximum: 31
Converter: Float
Grid Position: 2, 4, 1, 1

Any Code
ID: tx_gain_range
Var deps: {}
Code: self.sin...gain_range()
Default: (0, 31, 1)

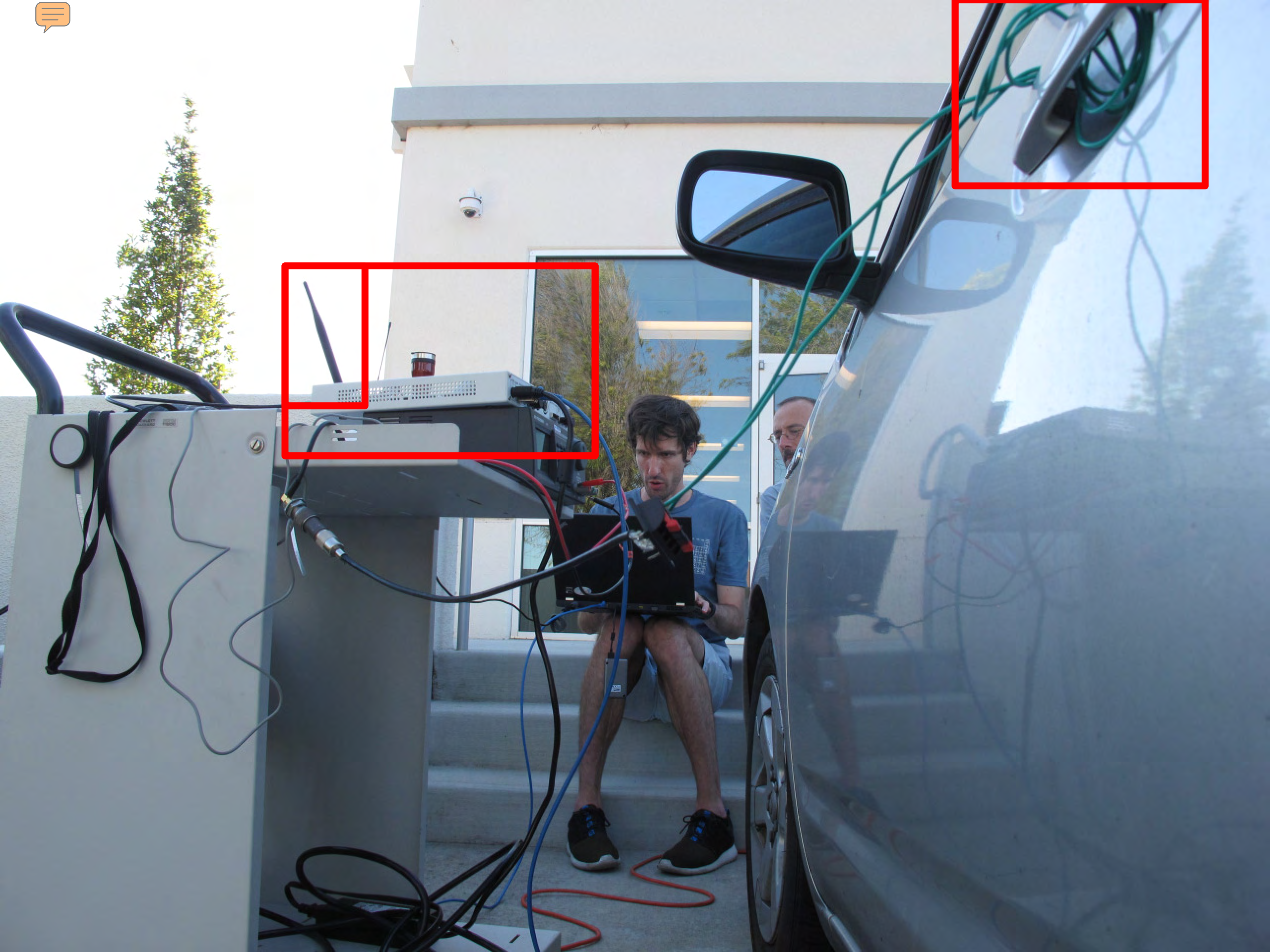
Variable
ID: tx_gain_default
Value: 31

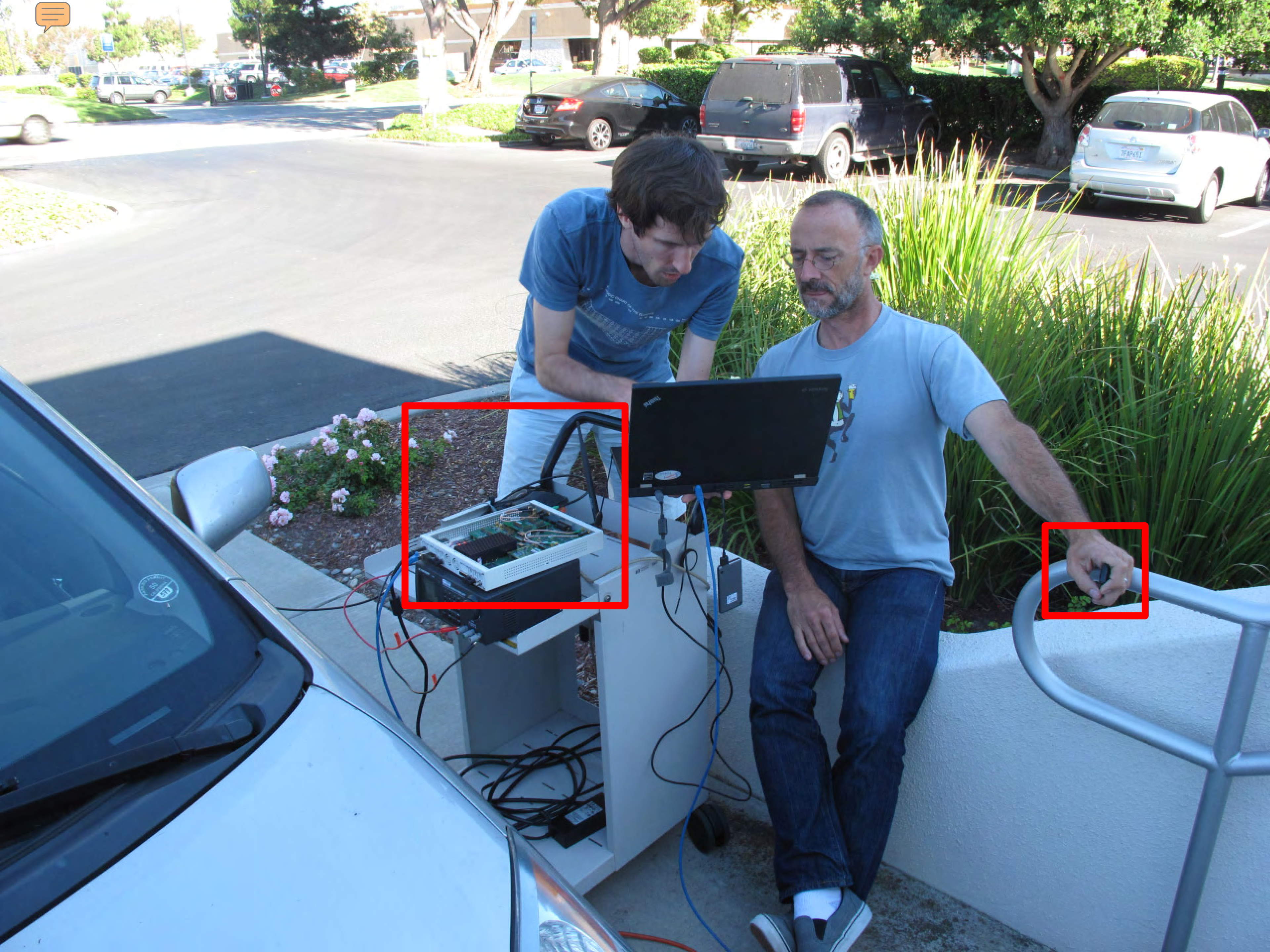
Function Probe
ID: locked_probe_0
Value: 0
Block ID: sink
Function Name: get_sensor
Function Args: 'lo_locked'
Poll Rate (Hz): 5

WX GUI Static Text
ID: variable_static_text_0_0
Label: TX Locked
Default Value: 0
Converter: String
Grid Position: 2, 3, 1, 1

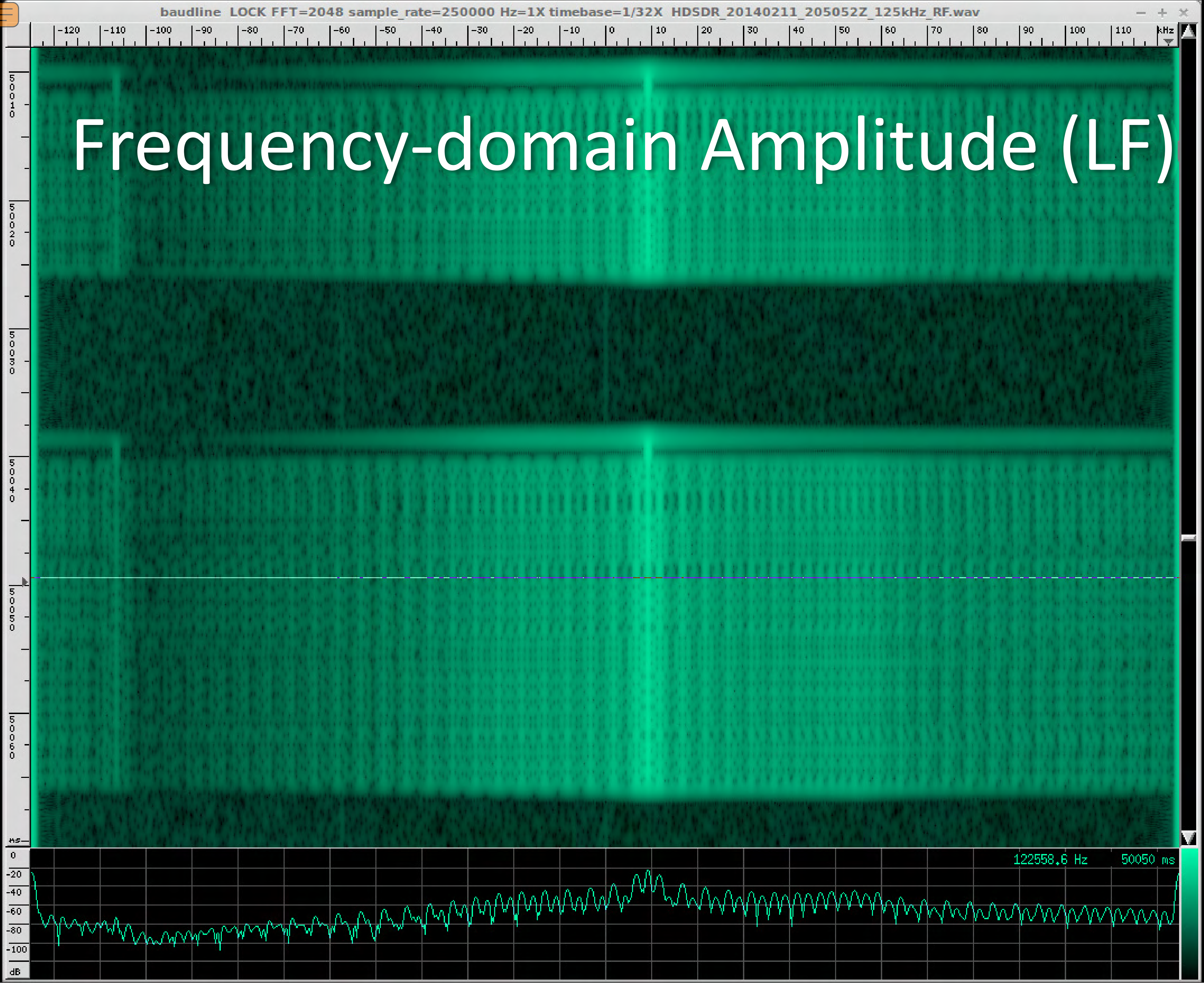
WX GUI Slider
ID: tx_lo_off
Label: TX LO Offset
Default Value: -2M
Minimum: -5M
Maximum: 5M
Converter: Float
Grid Position: 2, 7, 1, 1

WX GUI Slider
ID: tx_gain
Label: TX Gain
Default Value: 25
Minimum: 0
Maximum: 50
Converter: Float
Grid Position: 2, 4, 1, 1





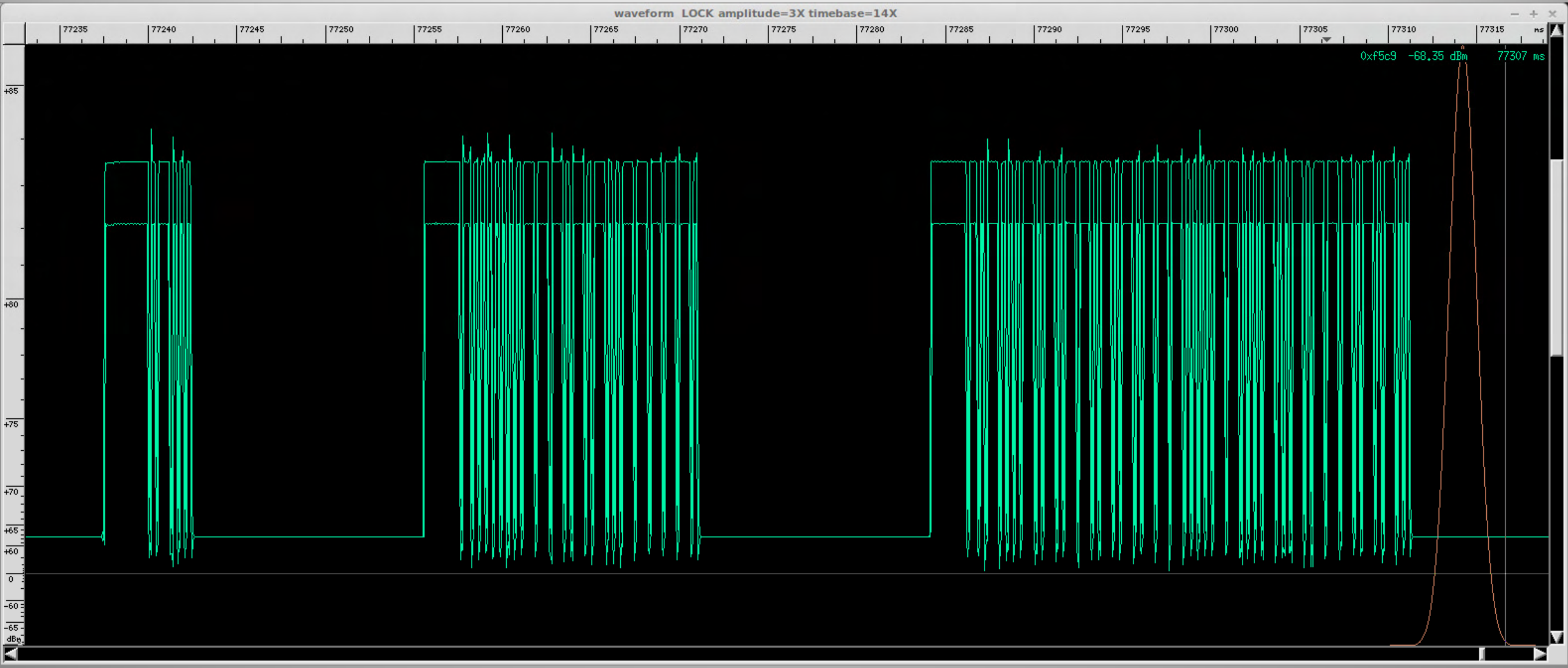
Frequency-domain Amplitude (LF)



baudline LOCK FFT=2048 sample_rate=250000 Hz=1X timebase=1/32X HDSDR_20140211_205052Z_125kHz_RF.wav

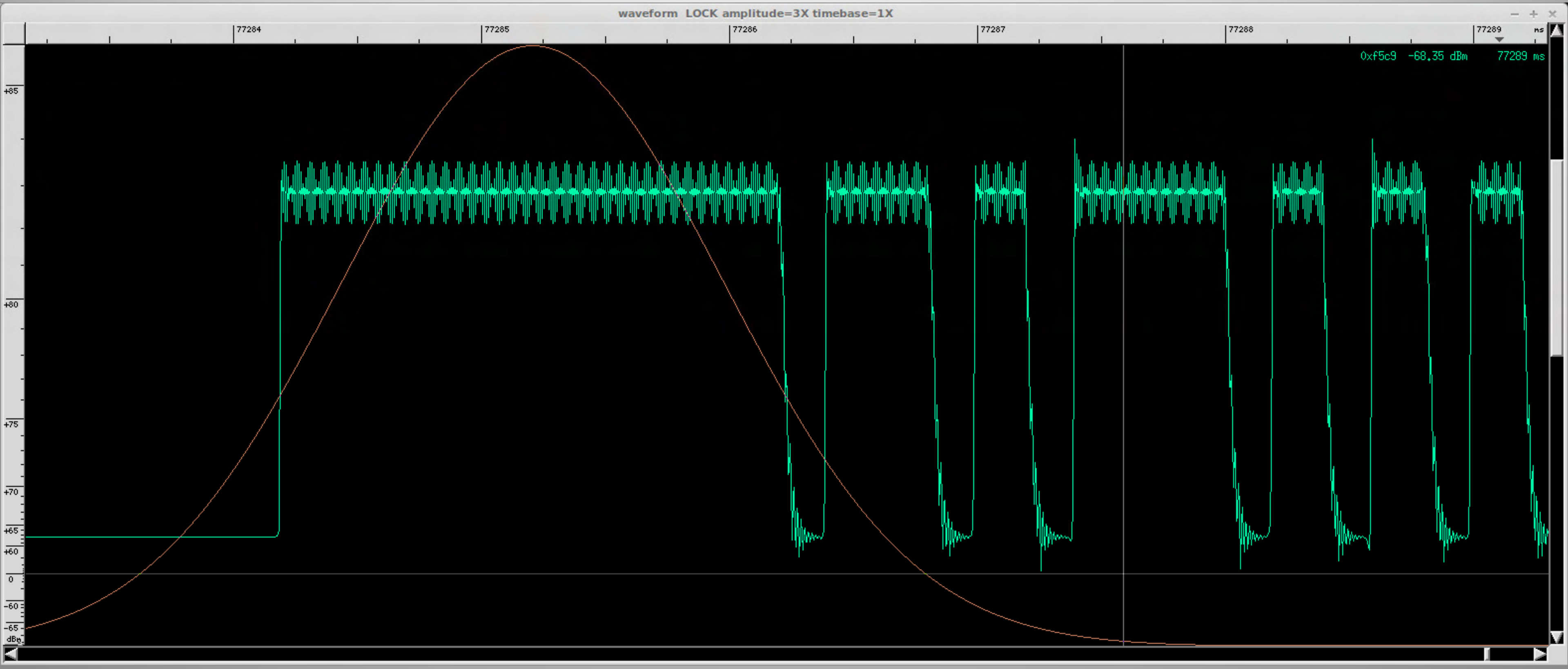
122558.6 Hz 50050 ms

Time-domain Amplitude (LF)



waveform LOCK amplitude=3X timebase=14X

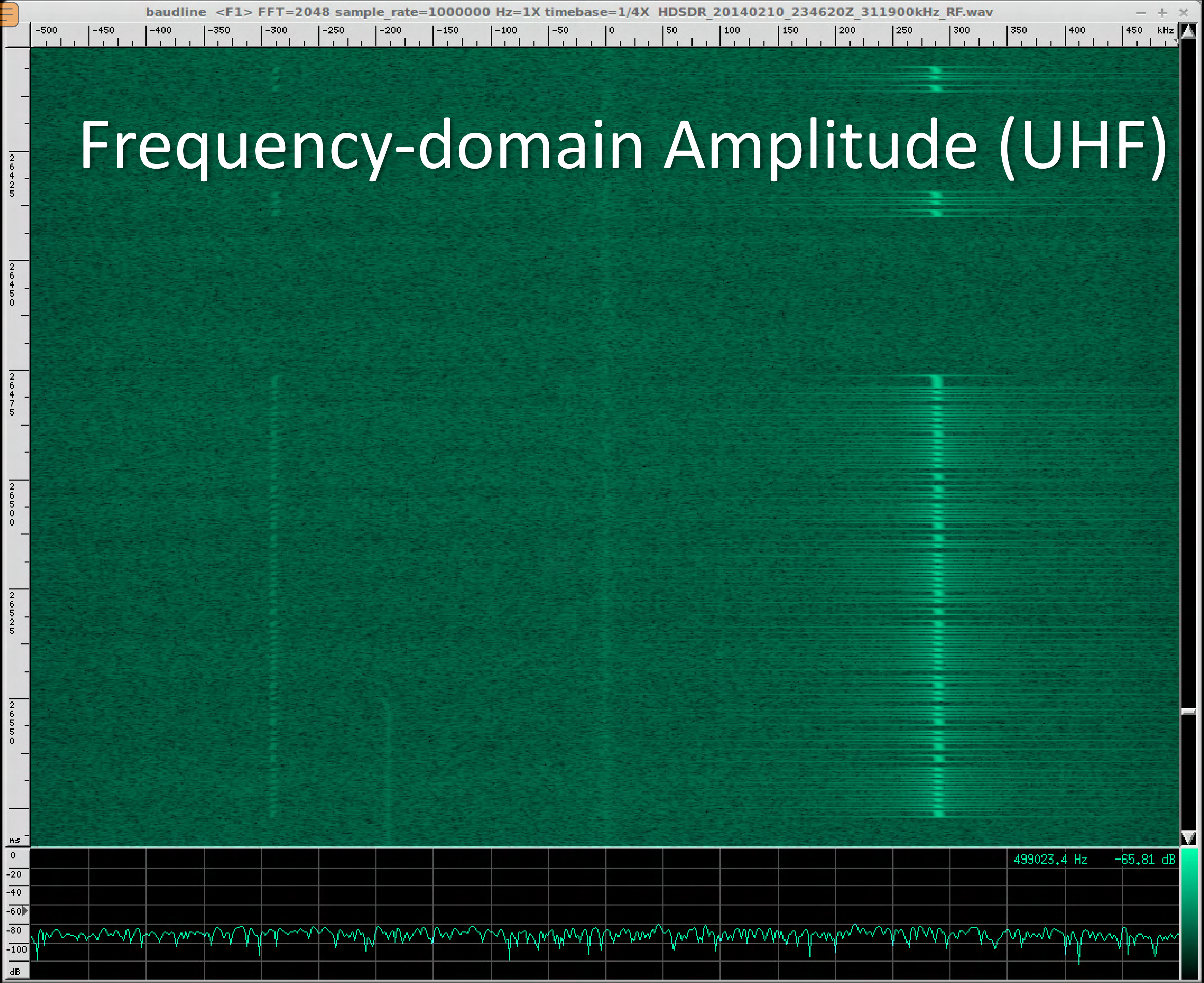
Time-domain Amplitude (LF)



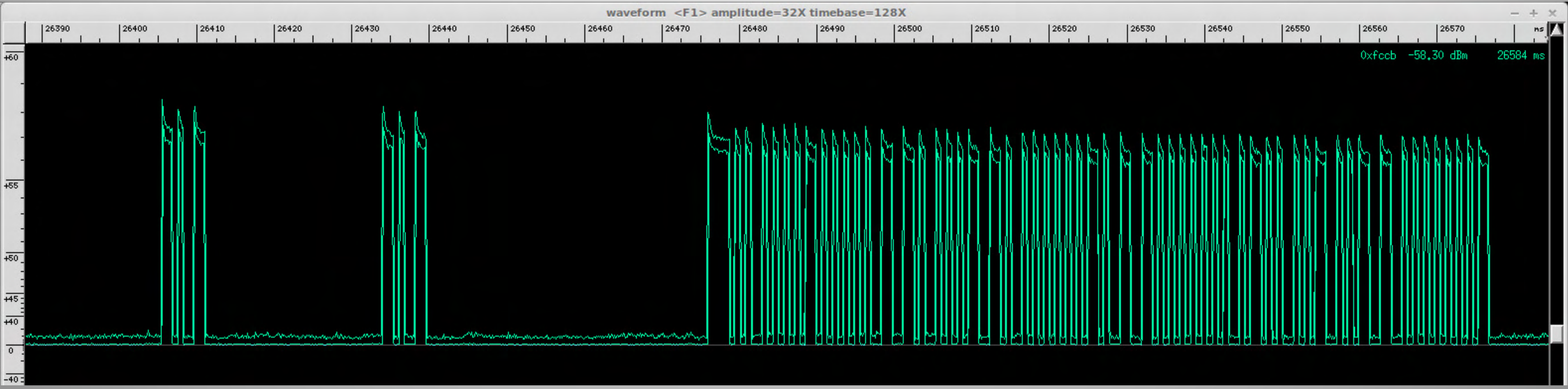
waveform LOCK amplitude=3X timebase=1X

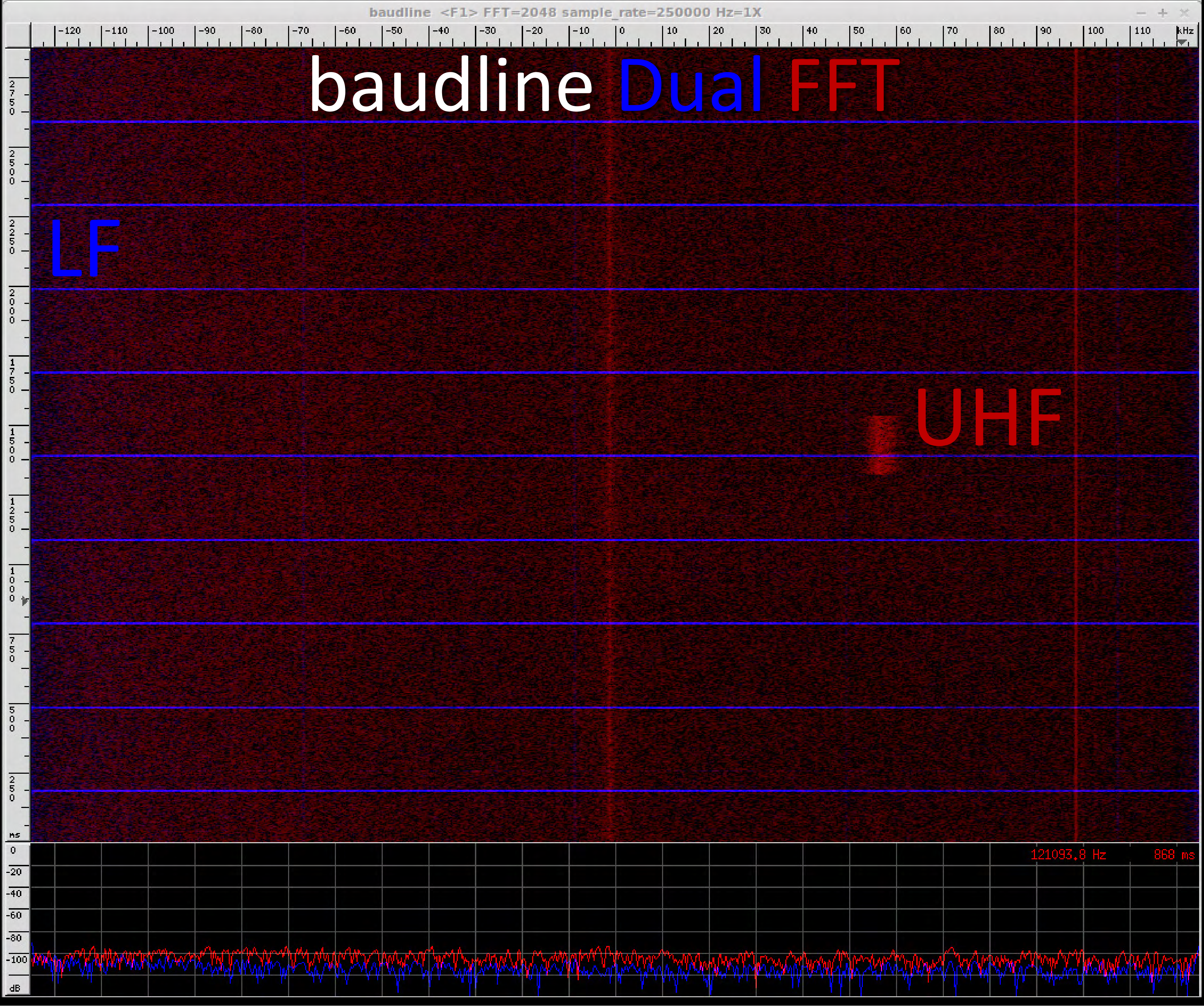
0xf5c9 -68.35 dBm 77289 ms

Frequency-domain Amplitude (UHF)



Time-domain Amplitude (UHF)



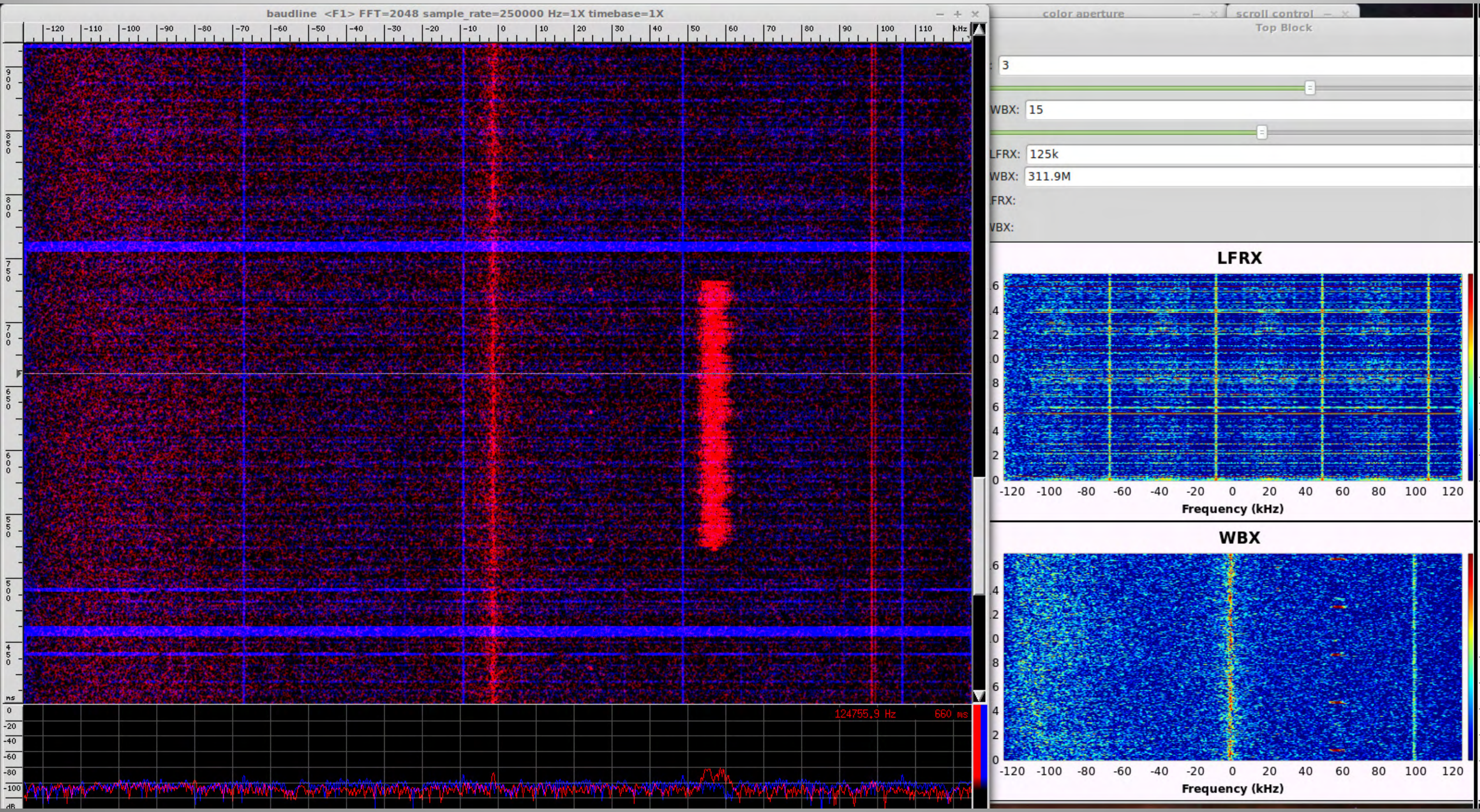


baudline <F1> FFT=2048 sample_rate=250000 Hz=1X

baudline Dual FFT

121093.8 Hz 868 ms

GNU Radio → baudline



baudline <F1> FFT=2048 sample_rate=250000 Hz=1X timebase=1X

Top Block

: 3

WBX: 15

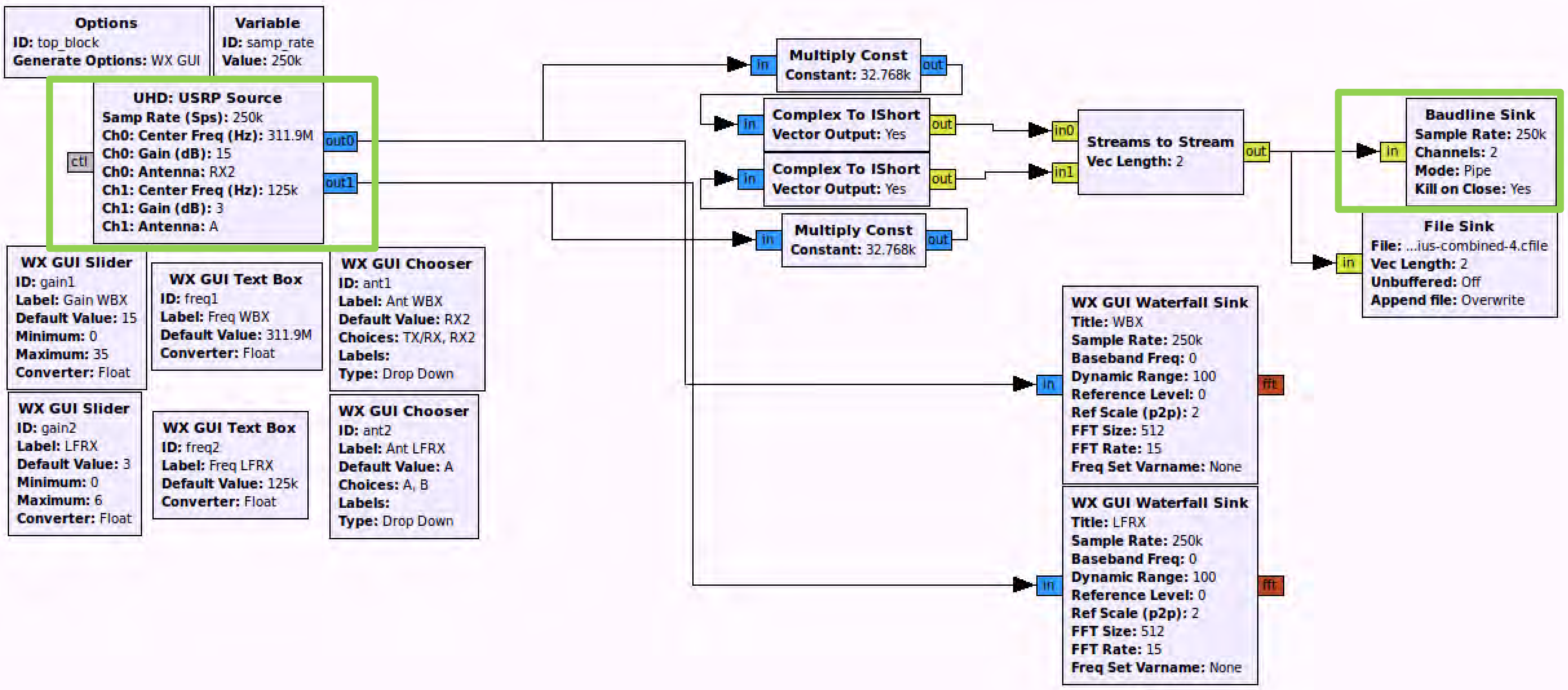
LFRX: 125k

WBX: 311.9M

FRX:

VBX:

GNU Radio + baudline



Options
ID: top_block
Generate Options: WX GUI

Variable
ID: samp_rate
Value: 250k

UHD: USRP Source
Samp Rate (Sps): 250k
Ch0: Center Freq (Hz): 311.9M
Ch0: Gain (dB): 15
Ch0: Antenna: RX2
Ch1: Center Freq (Hz): 125k
Ch1: Gain (dB): 3
Ch1: Antenna: A

Multiply Const
Constant: 32.768k

Complex To IShort
Vector Output: Yes

Complex To IShort
Vector Output: Yes

Multiply Const
Constant: 32.768k

Streams to Stream
Vec Length: 2

Baudline Sink
Sample Rate: 250k
Channels: 2
Mode: Pipe
Kill on Close: Yes

File Sink
File: ...ius-combined-4.cfile
Vec Length: 2
Unbuffered: Off
Append file: Overwrite

WX GUI Slider
ID: gain1
Label: Gain WBX
Default Value: 15
Minimum: 0
Maximum: 35
Converter: Float

WX GUI Text Box
ID: freq1
Label: Freq WBX
Default Value: 311.9M
Converter: Float

WX GUI Chooser
ID: ant1
Label: Ant WBX
Default Value: RX2
Choices: TX/RX, RX2
Labels:
Type: Drop Down

WX GUI Slider
ID: gain2
Label: LFRX
Default Value: 3
Minimum: 0
Maximum: 6
Converter: Float

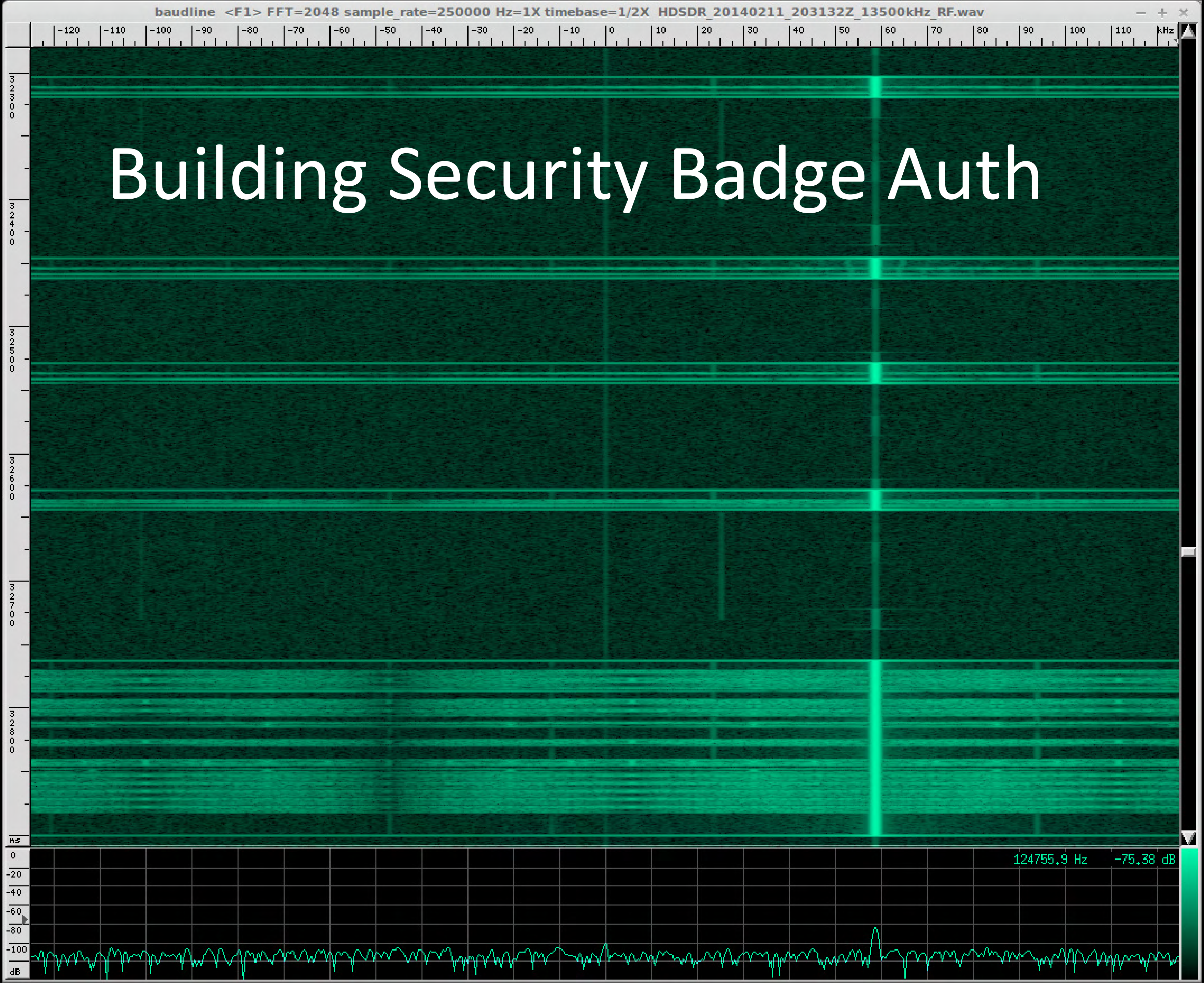
WX GUI Text Box
ID: freq2
Label: Freq LFRX
Default Value: 125k
Converter: Float

WX GUI Chooser
ID: ant2
Label: Ant LFRX
Default Value: A
Choices: A, B
Labels:
Type: Drop Down

WX GUI Waterfall Sink
Title: WBX
Sample Rate: 250k
Baseband Freq: 0
Dynamic Range: 100
Reference Level: 0
Ref Scale (p2p): 2
FFT Size: 512
FFT Rate: 15
Freq Set Varname: None

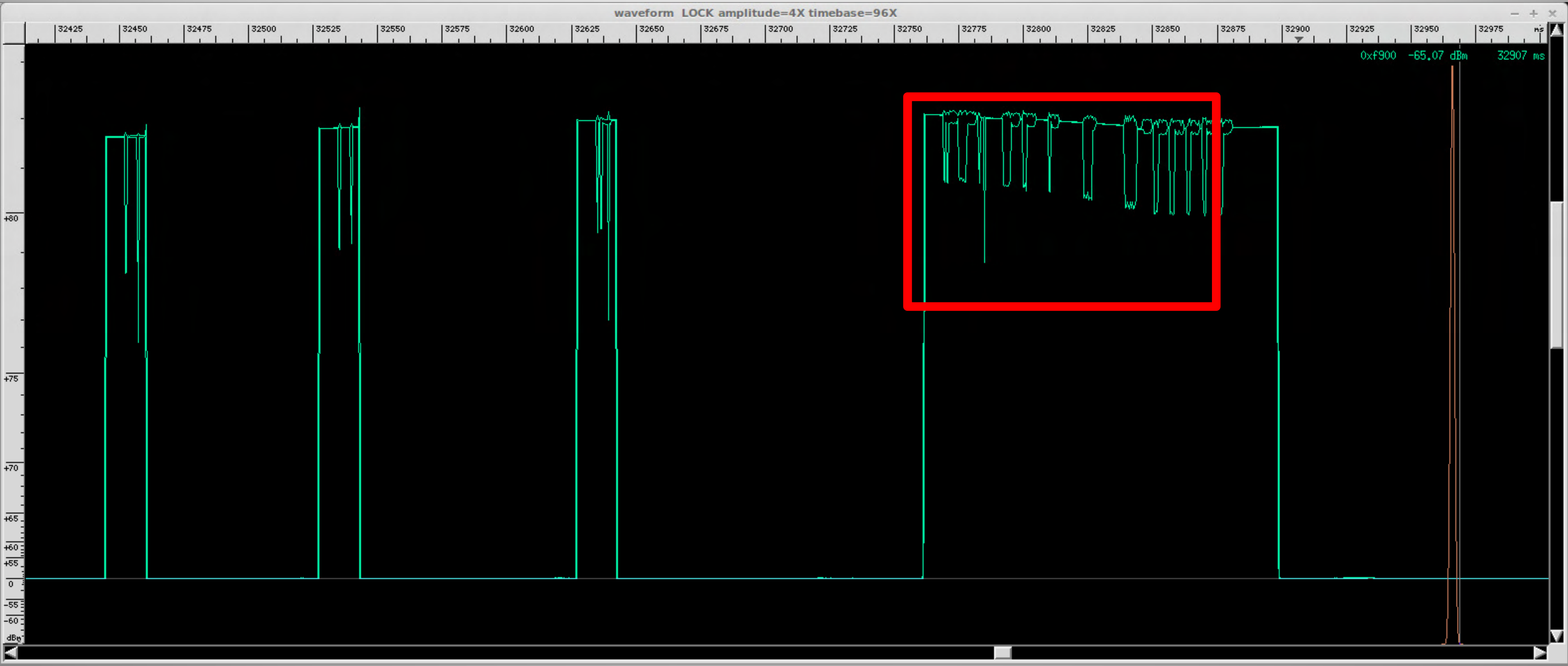
WX GUI Waterfall Sink
Title: LFRX
Sample Rate: 250k
Baseband Freq: 0
Dynamic Range: 100
Reference Level: 0
Ref Scale (p2p): 2
FFT Size: 512
FFT Rate: 15
Freq Set Varname: None

Building Security Badge Auth



baudline <F1> FFT=2048 sample_rate=250000 Hz=1X timebase=1/2X HDSDR_20140211_203132Z_13500kHz_RF.wav

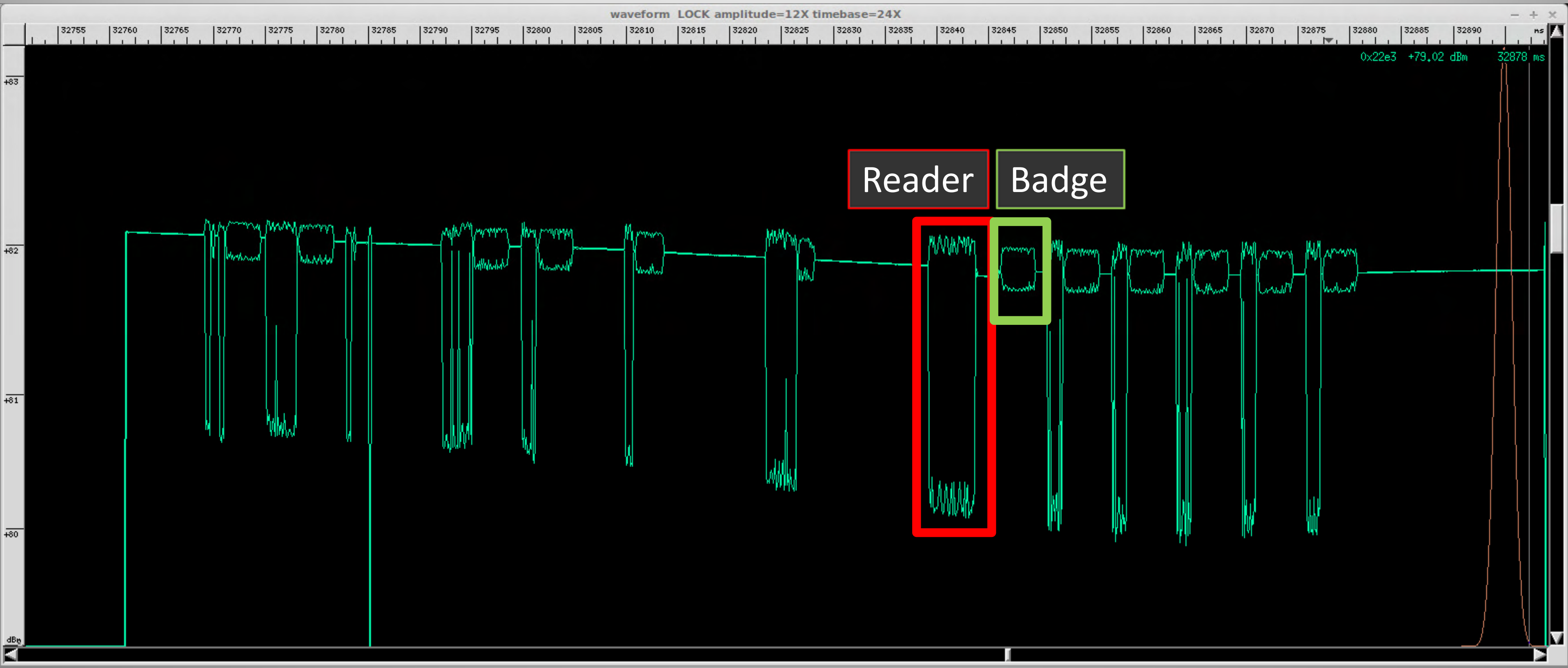
Time-domain Amplitude



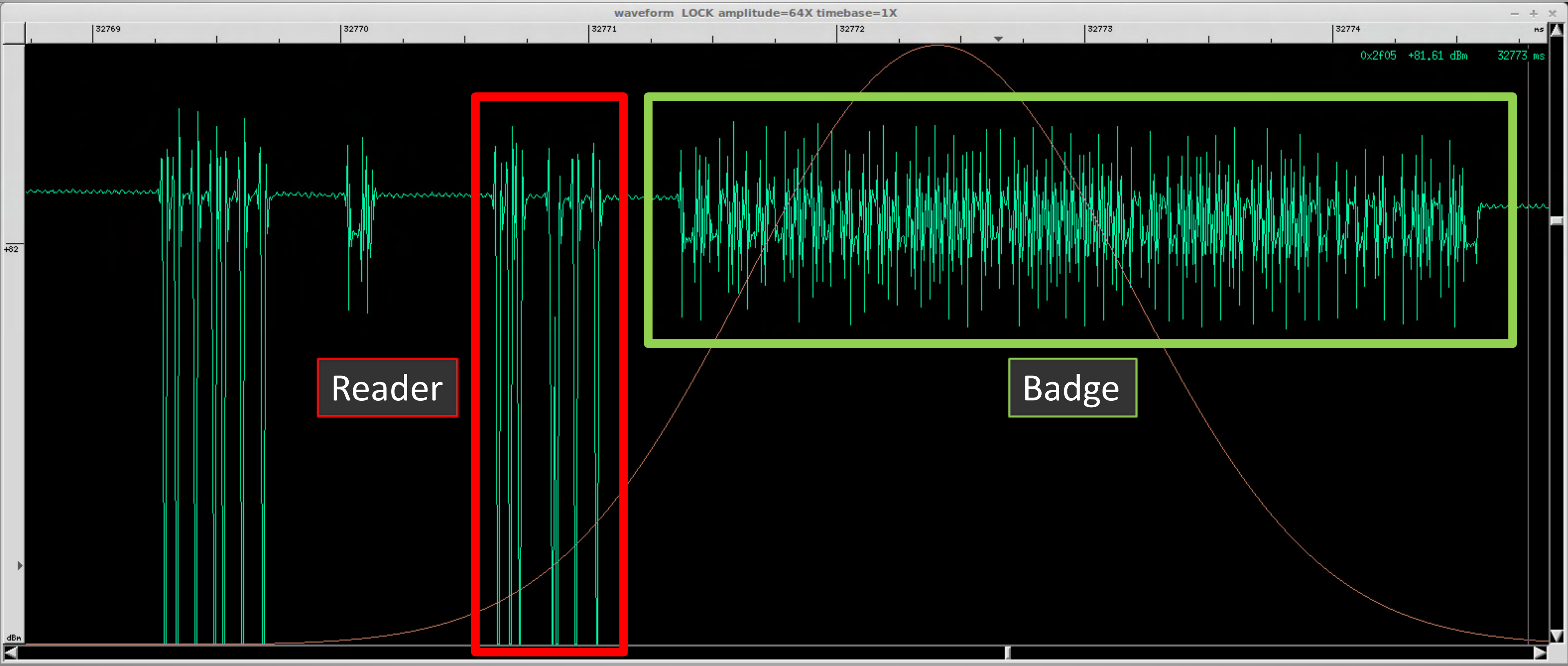
waveform LOCK amplitude=4X timebase=96X

0xf900 -65.07 dBm 32907 ms

Time-domain Amplitude



Time-domain Amplitude

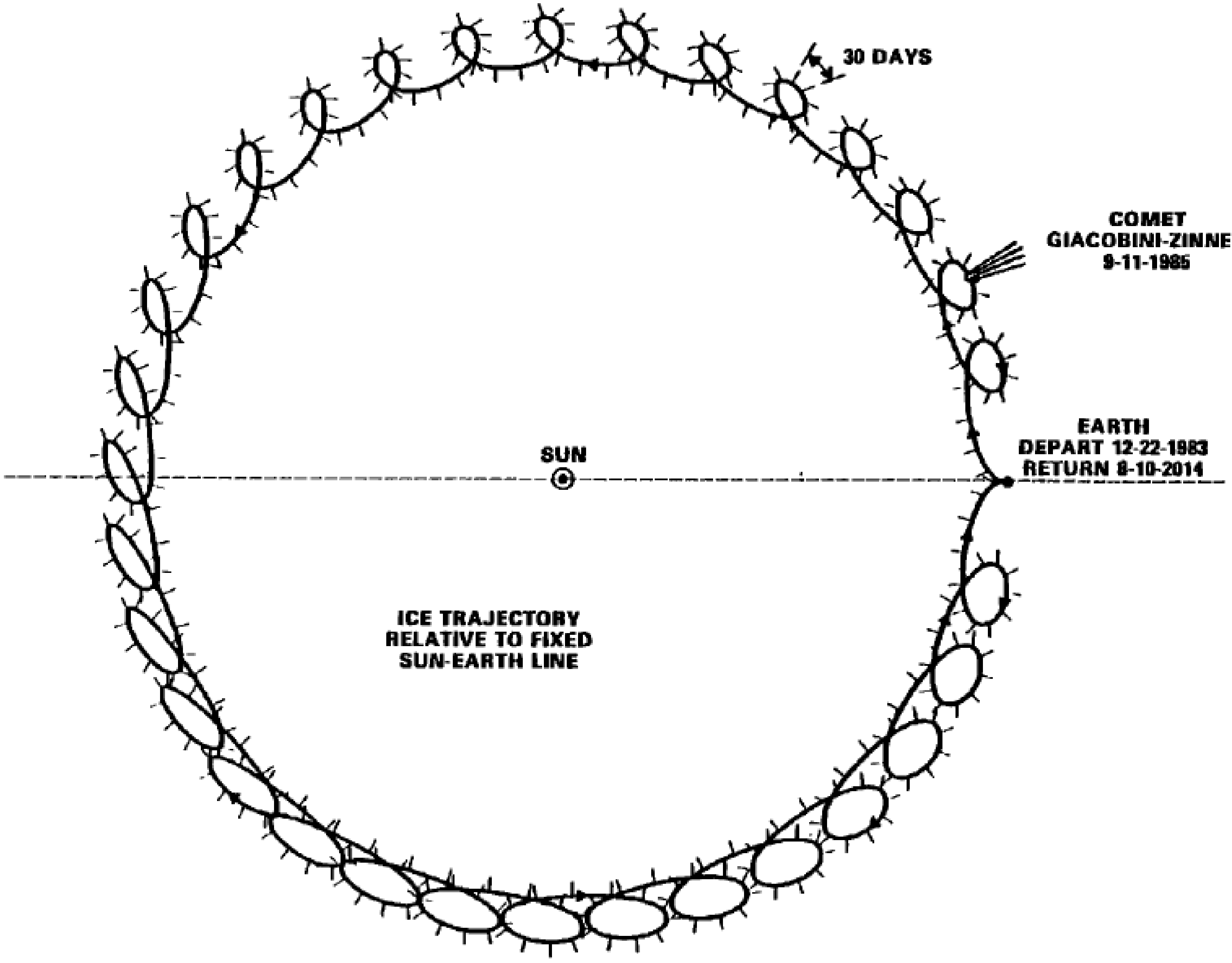

waveform LOCK amplitude=64X timebase=1X

0x2f05 +81.61 dBm 32773 ms

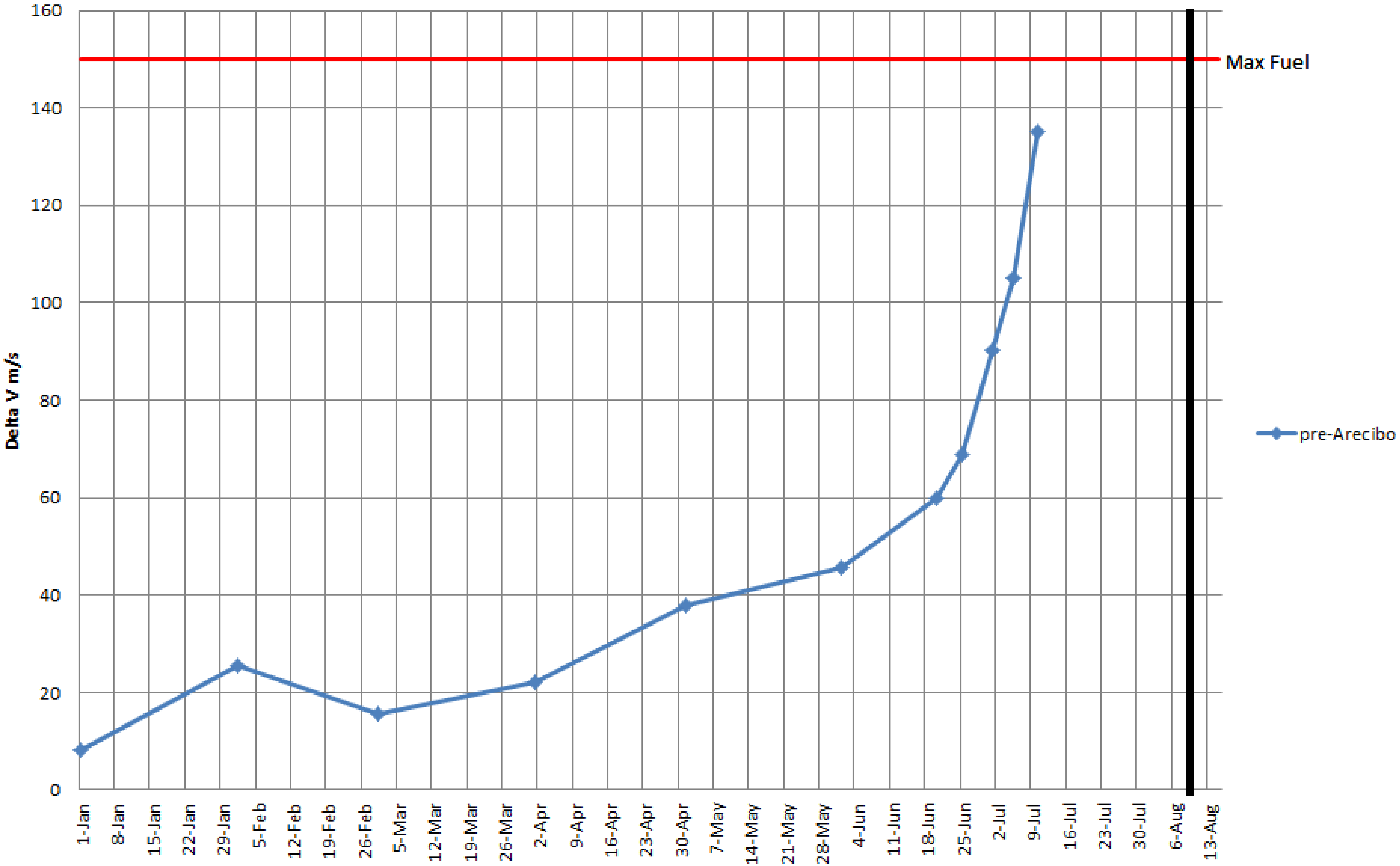
Reader

Badge

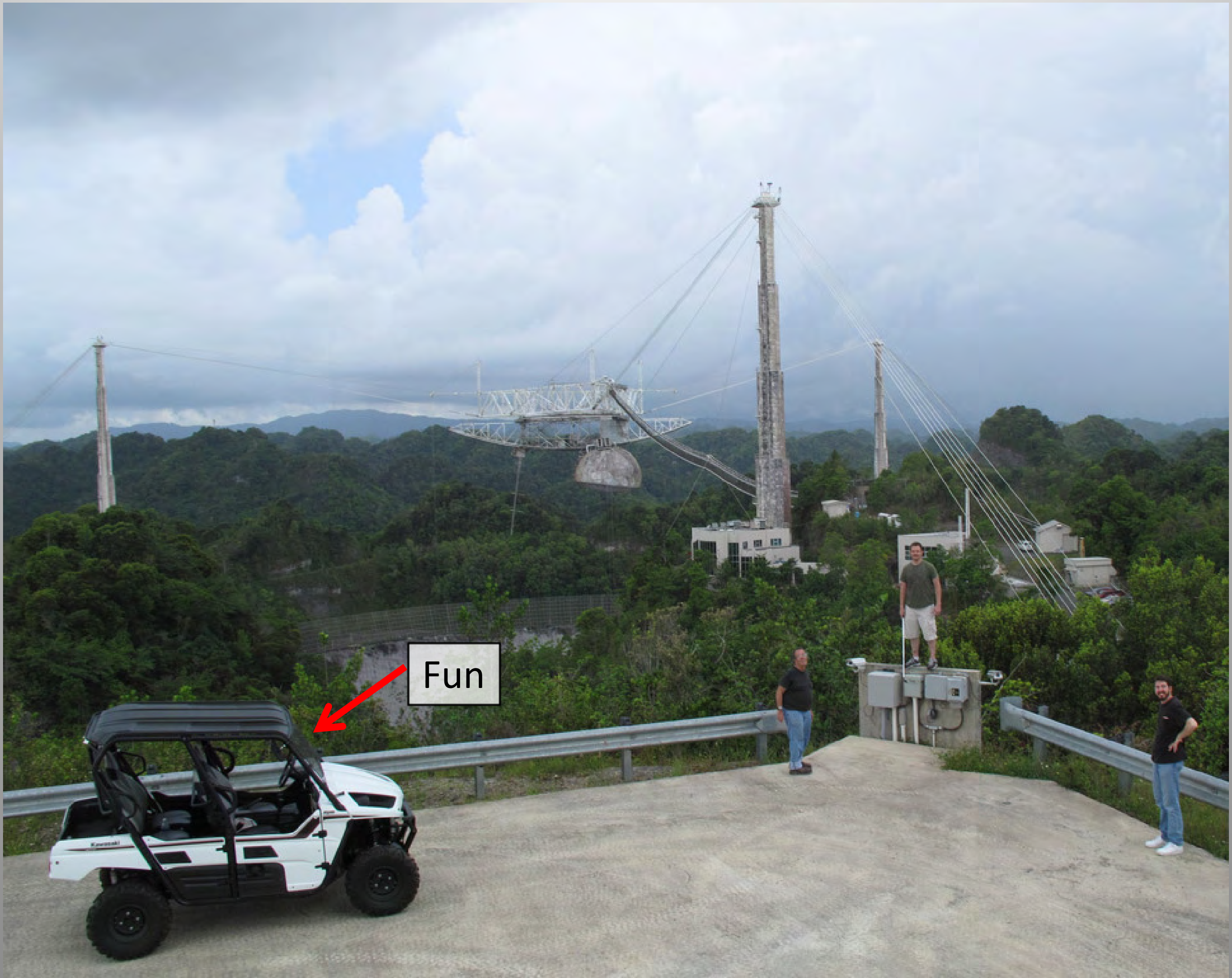
ISEE-3 Reboot Project


30 DAYS
COMET
GIACOBINI-ZINNER
9-11-1985
SUN
EARTH
DEPART 12-22-1983
RETURN 8-10-2014
ICE TRAJECTORY
RELATIVE TO FIXED
SUN-EARTH LINE

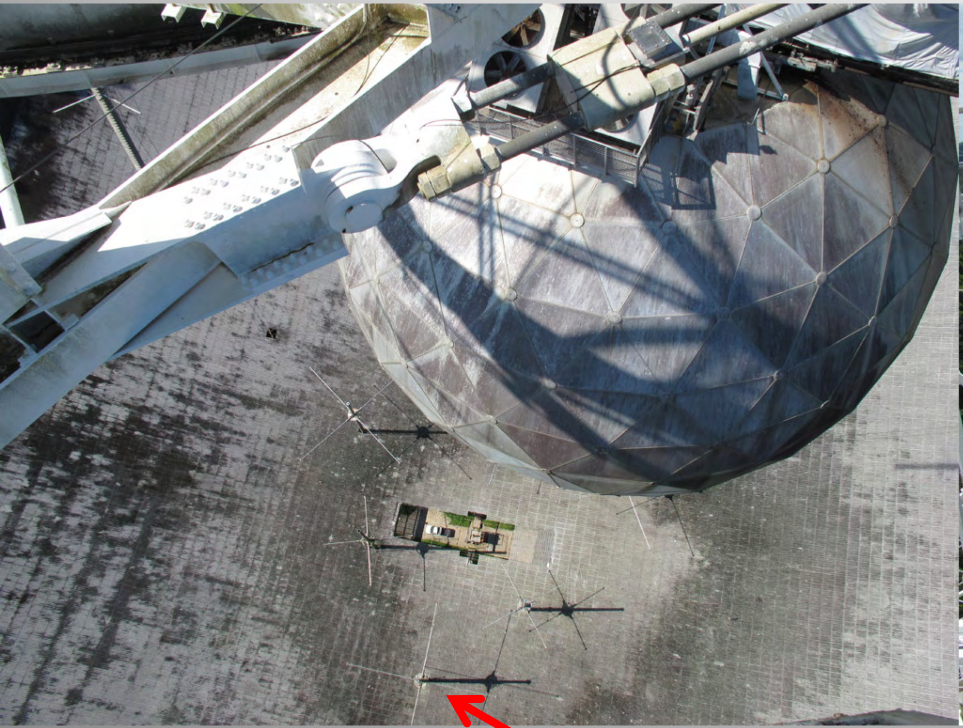
Total Delta V Requirement to Bring ISEE-3 Back to L1



Arecibo Radio Observatory

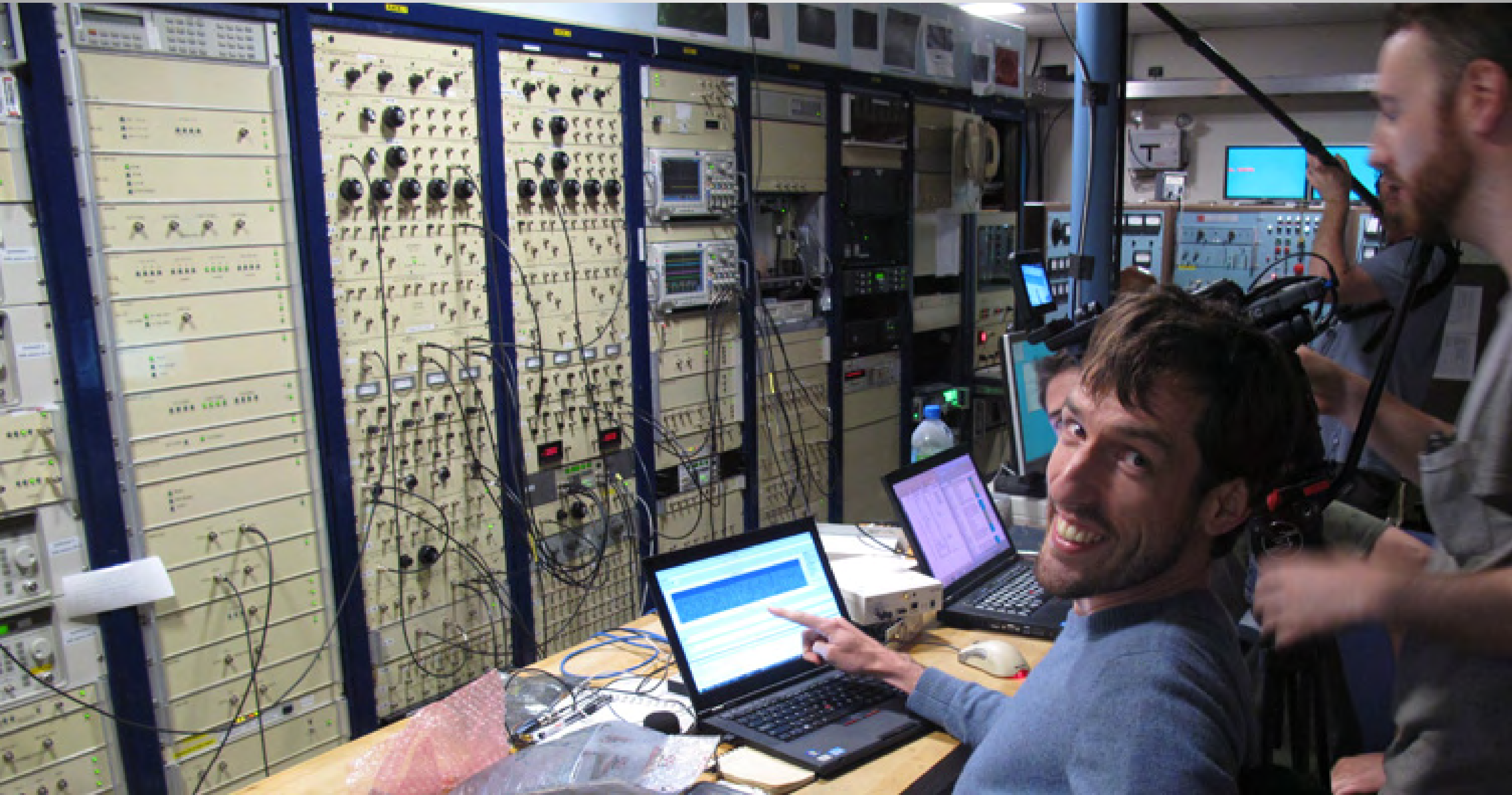


View from above

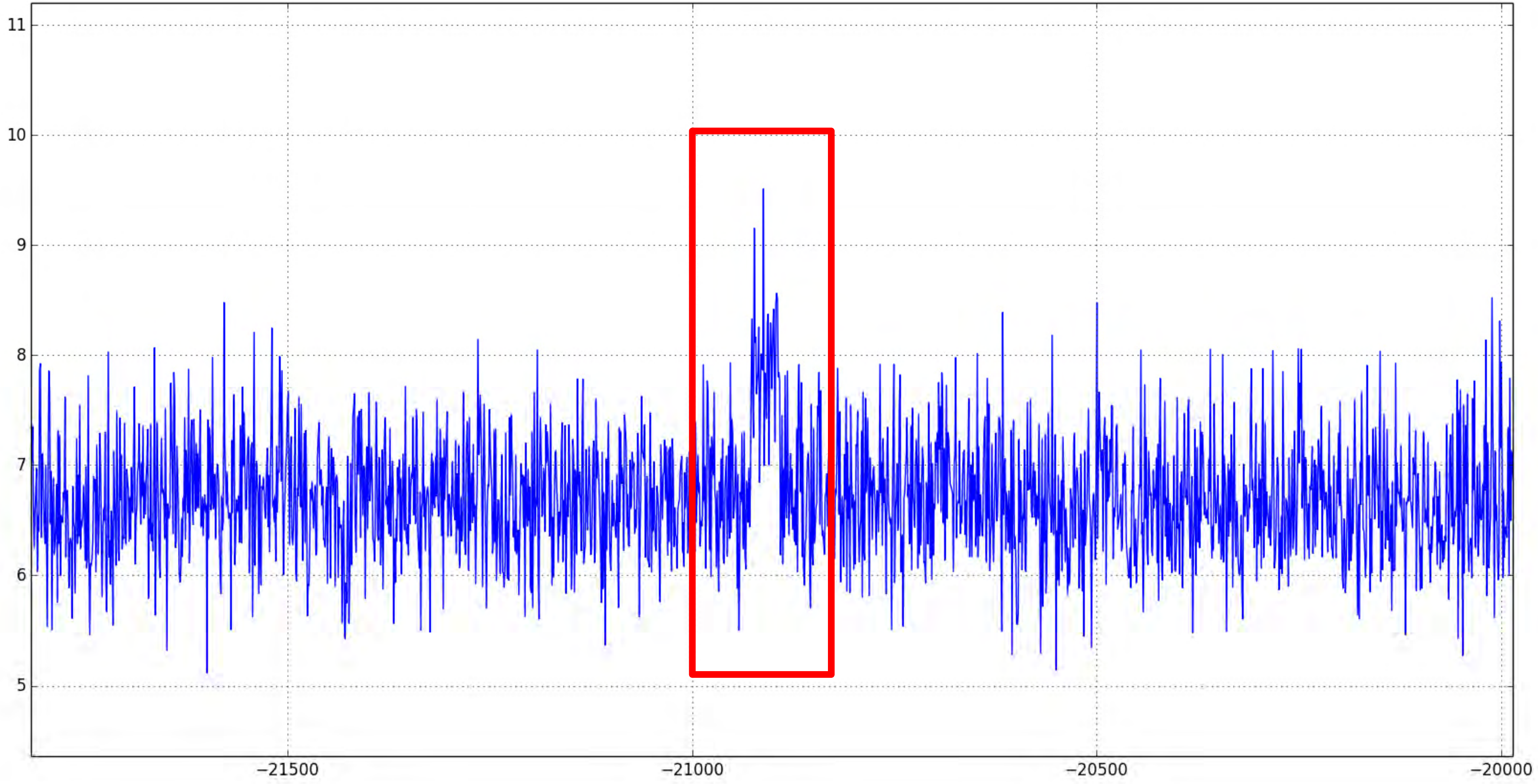


Ionospheric heaters

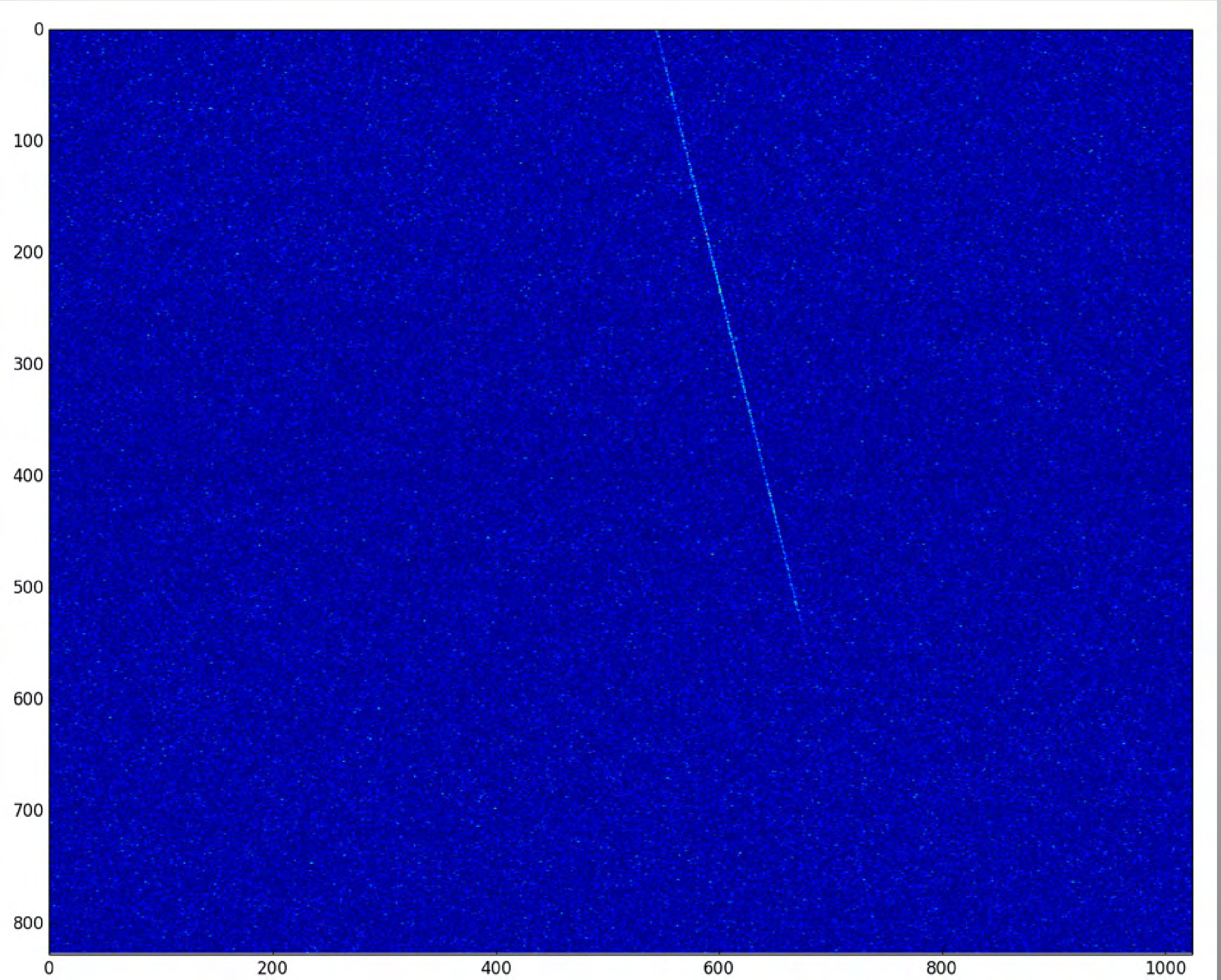
Still a good start…



Weak Signal → Low RBW

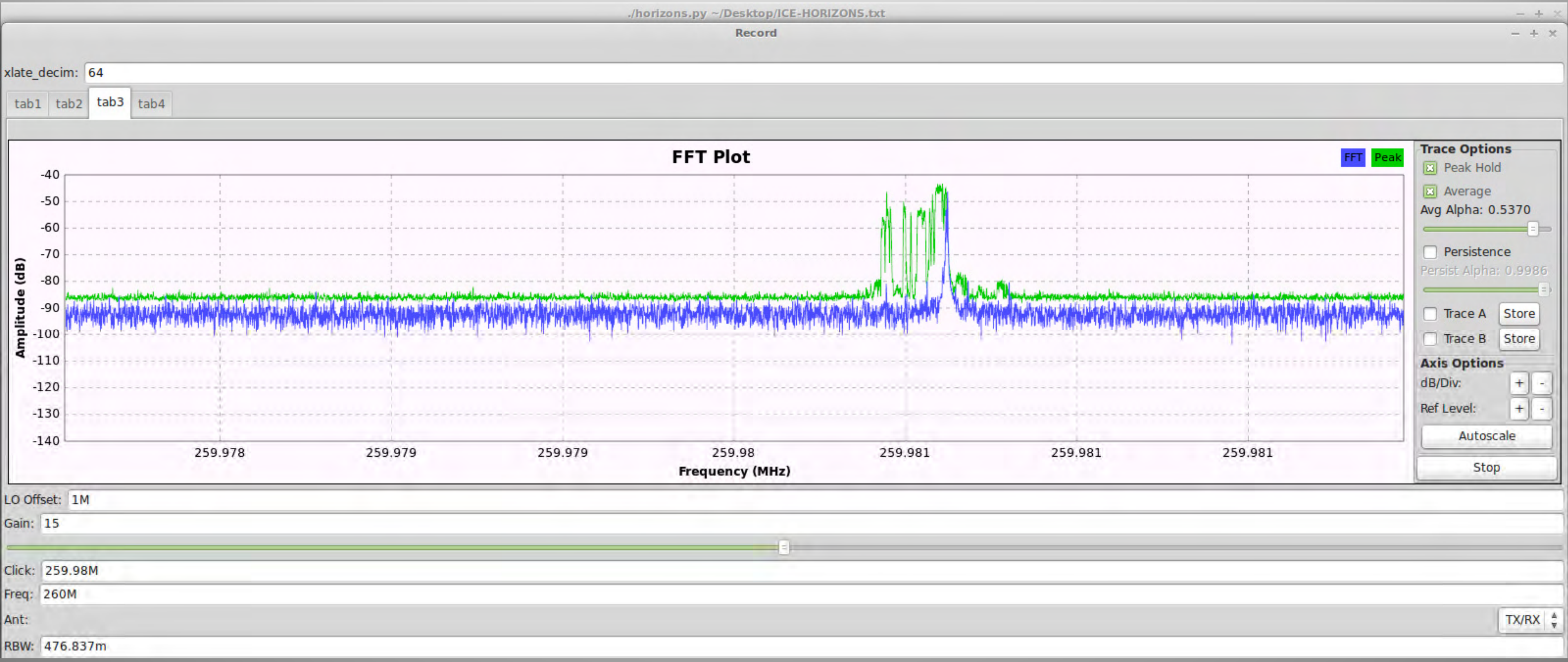


numpy & matplotlib



After Improving Pointing

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



xlate_decim: 64

☒ Peak Hold

☒ Average

Avg Alpha: 0.5370

☐ Persistence

Persist Alpha: 0.9986

☐ Trace A

☐ Trace B

dB/Div:

Ref Level:

LO Offset: 1M

Gain: 15

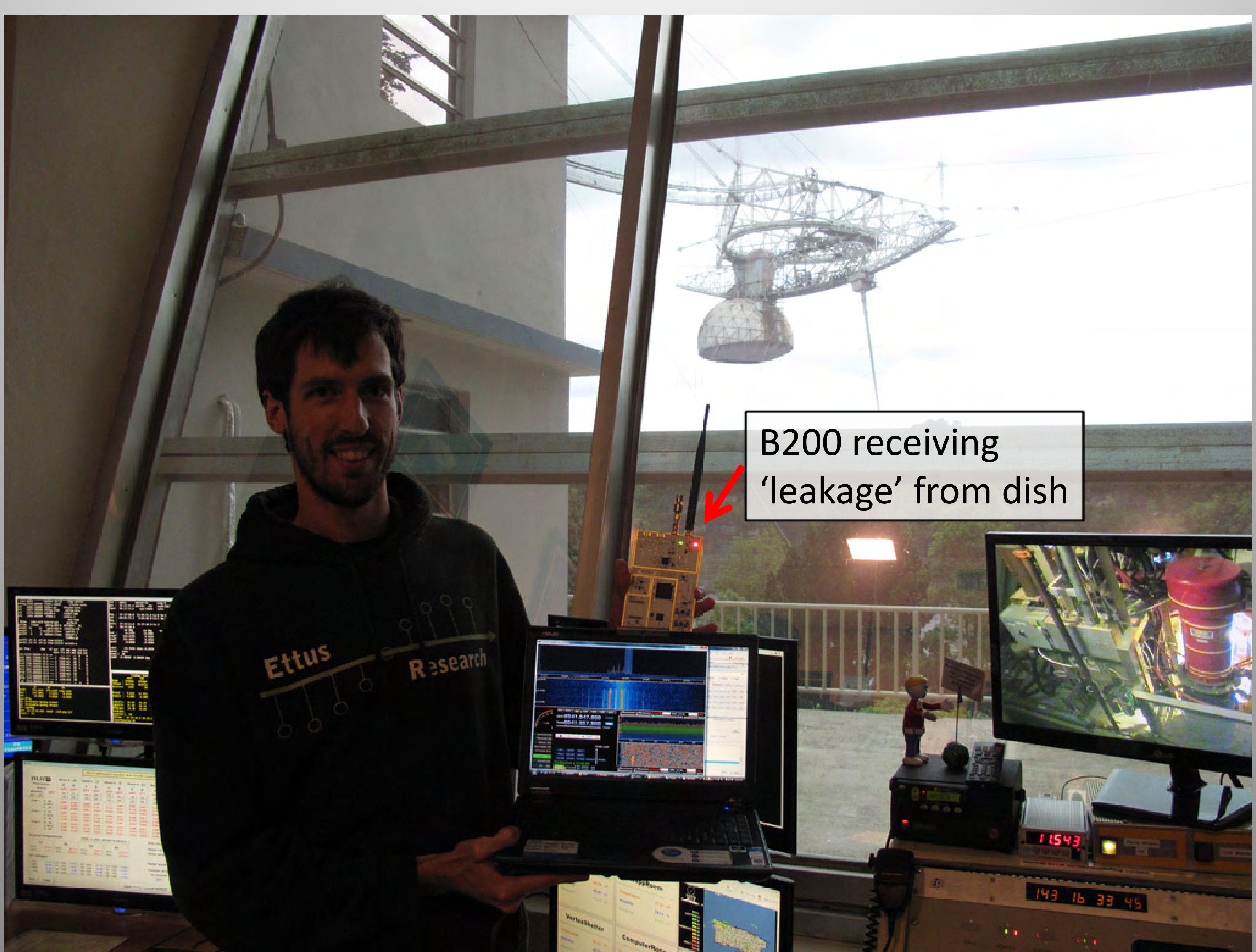
Click: 259.98M

Freq: 260M

Ant: TX/RX

RBW: 476.837m

Verifying Transmitted Signal

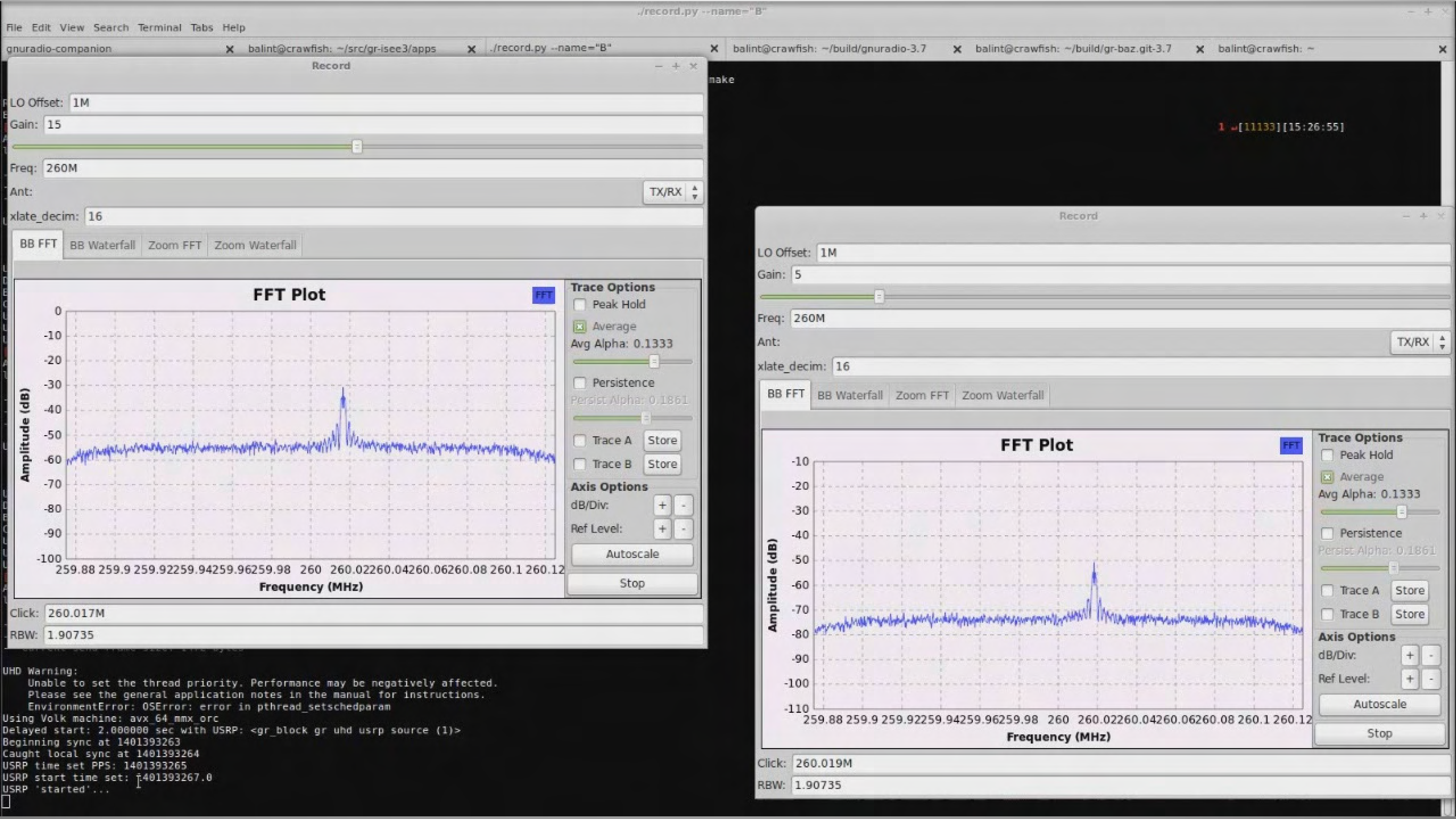


B200 receiving
‘leakage’ from dish

Moment of First Contact

Happy Dance

Dual Channel Recording



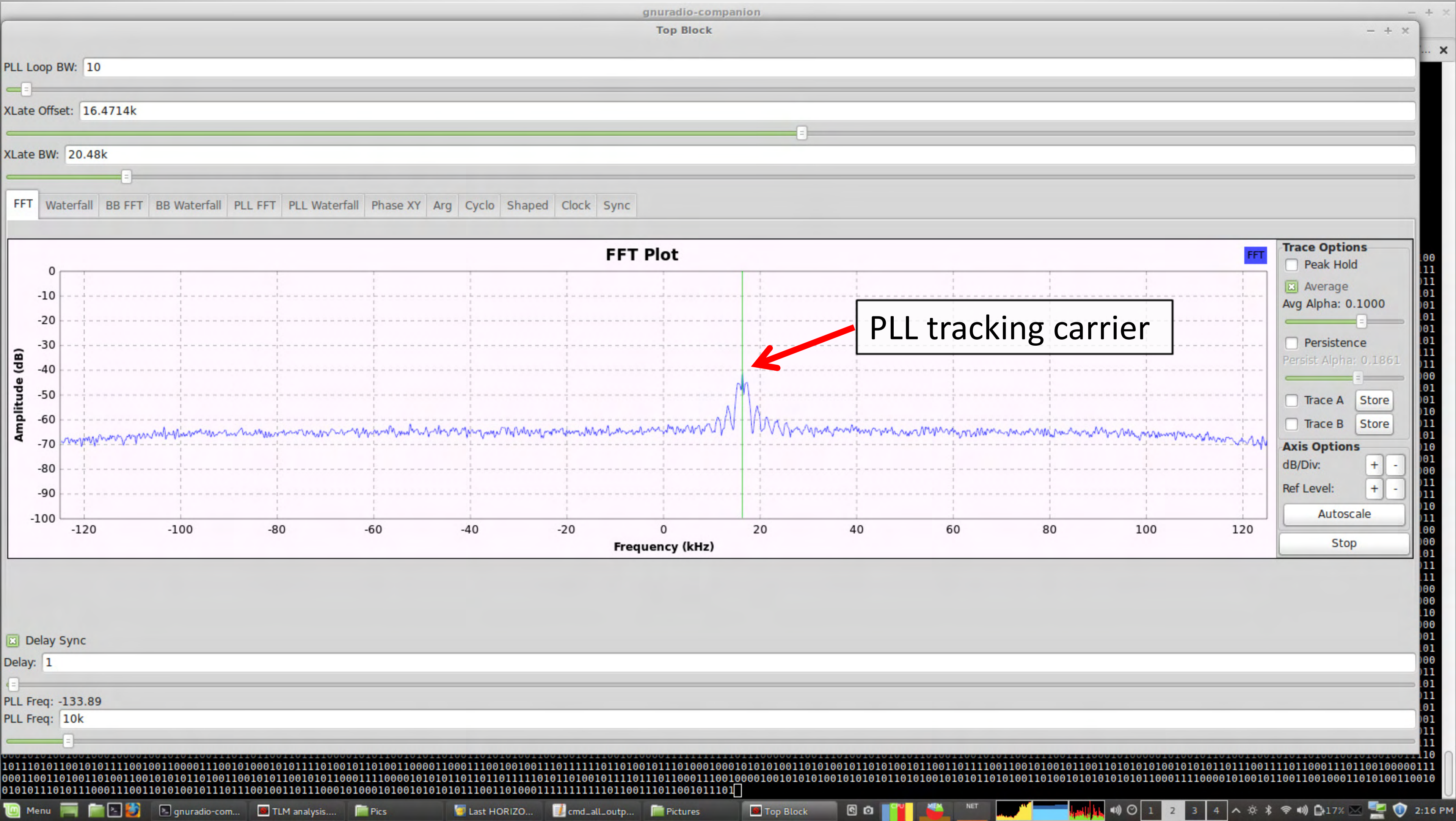
LO Offset: 1M
Gain: 15
Freq: 260M
Ant: TX/RX
xlate_decim: 16
☐ Peak Hold
☒ Average
Avg Alpha: 0.1333
☐ Persistence
Persist Alpha: 0.1861
☐ Trace A
☐ Trace B
Click: 260.017M
RBW: 1.90735

LO Offset: 1M
Gain: 5
Freq: 260M
Ant: TX/RX
xlate_decim: 16
☐ Peak Hold
☒ Average
Avg Alpha: 0.1333
☐ Persistence
Persist Alpha: 0.1861
☐ Trace A
☐ Trace B
Click: 260.019M
RBW: 1.90735

```
make

                                                     1 ↵[11133][15:26:55]
```

```
UHD Warning:
    Unable to set the thread priority. Performance may be negatively affected.
    Please see the general application notes in the manual for instructions.
    EnvironmentError: OSError: error in pthread_setschedparam
Using Volk machine: avx_64_mmx_orc
Delayed start: 2.000000 sec with USRP: <gr_block gr uhd usrp source (1)>
Beginning sync at 1401393263
Caught local sync at 1401393264
USRP time set PPS: 1401393265
USRP start time set: 1401393267.0
USRP 'started'...
```

Raw Captured Baseband



PLL Loop BW: 10

XLate Offset: 16.4714k

XLate BW: 20.48k

Delay Sync ☒

Delay: 1

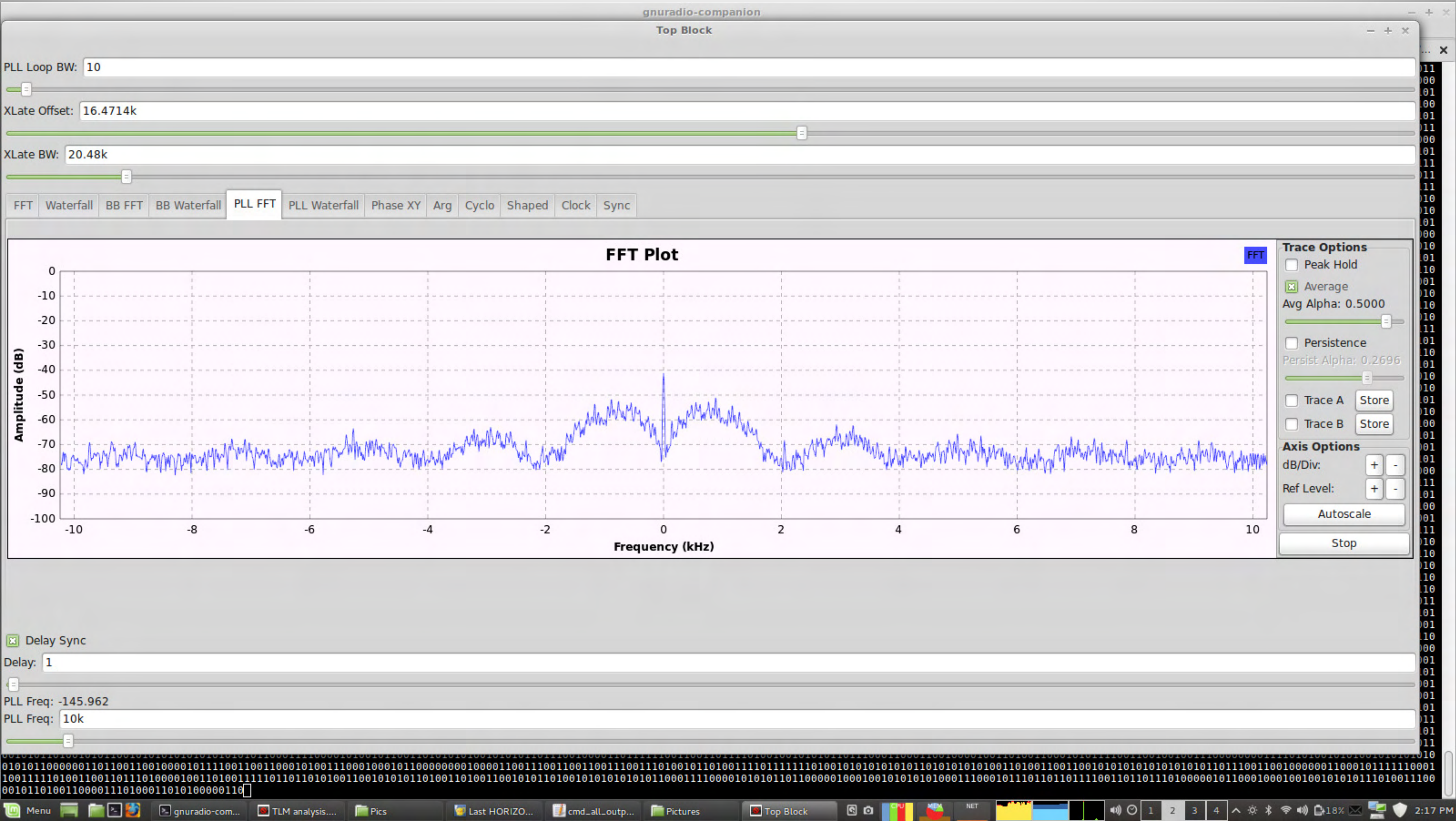
PLL Freq: -133.89

PLL Freq: 10k

```
1011101011001010111100100110000111001010001010111101001011010011000011000111001001001110111111101101001011101000100010101010011010100101101010010110010111100101011100111001011111001100101001011001101010101001010101101110011110110001110110010000011
0001100110100110100110010101011010011001010110010101100011110000101010110110110111111010110100101111011101100011100100001001010101001010101011010100101010110101001010011010010101010101100011110000101001011001100100011010100110001 0
010101110101110001110011010100101110111001001101110001010001010010101010111001101000111111111101100111011001011101
```

PLL tracking carrier

PLL Lock



PLL Loop BW: 10

XLate Offset: 16.4714k

XLate BW: 20.48k

☐ Peak Hold

☒ Average

Avg Alpha: 0.5000

☐ Persistence

Persist Alpha: 0.2696

☐ Trace A

☐ Trace B

☒ Delay Sync

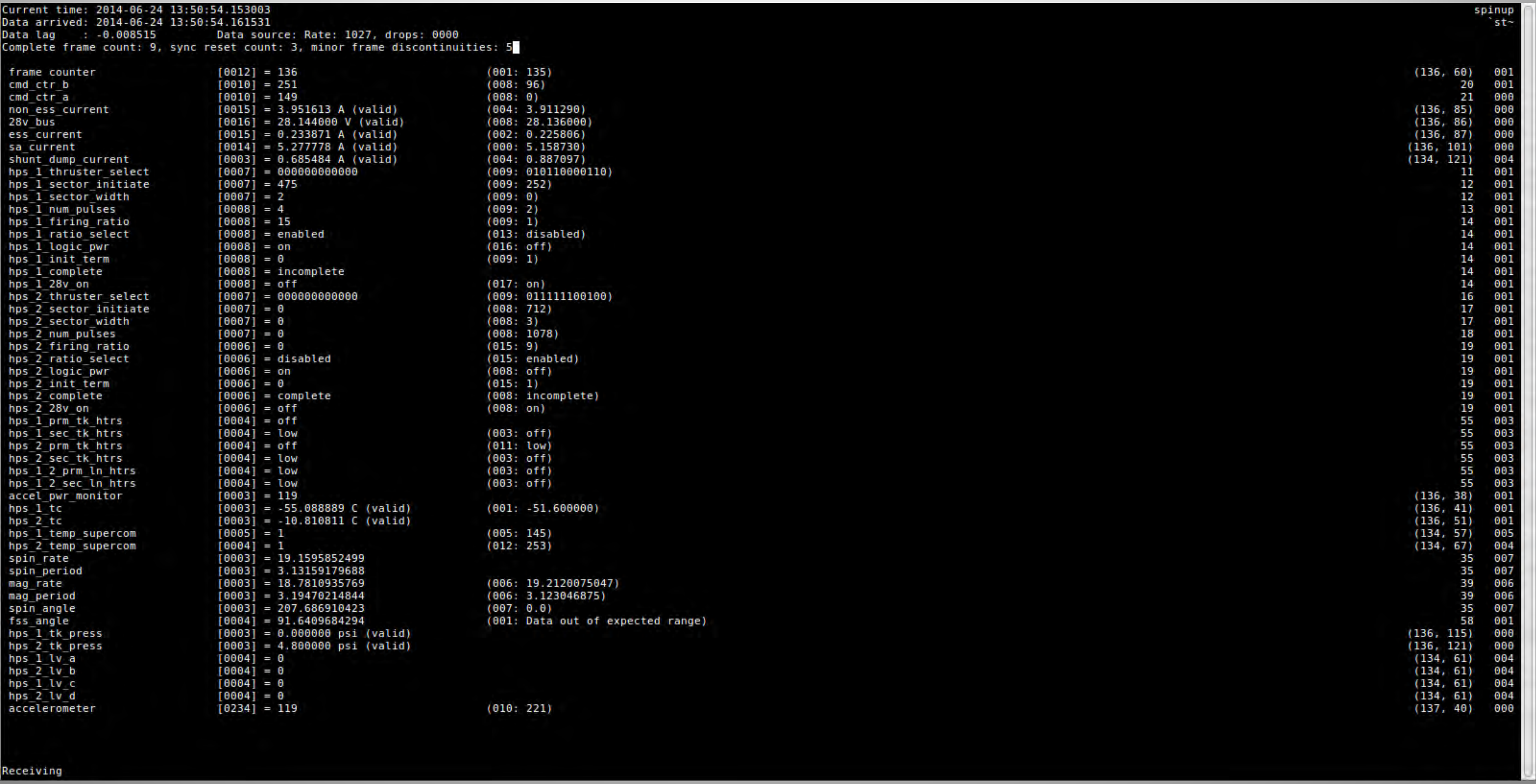
Delay: 1

PLL Freq: -145.962

PLL Freq: 10k

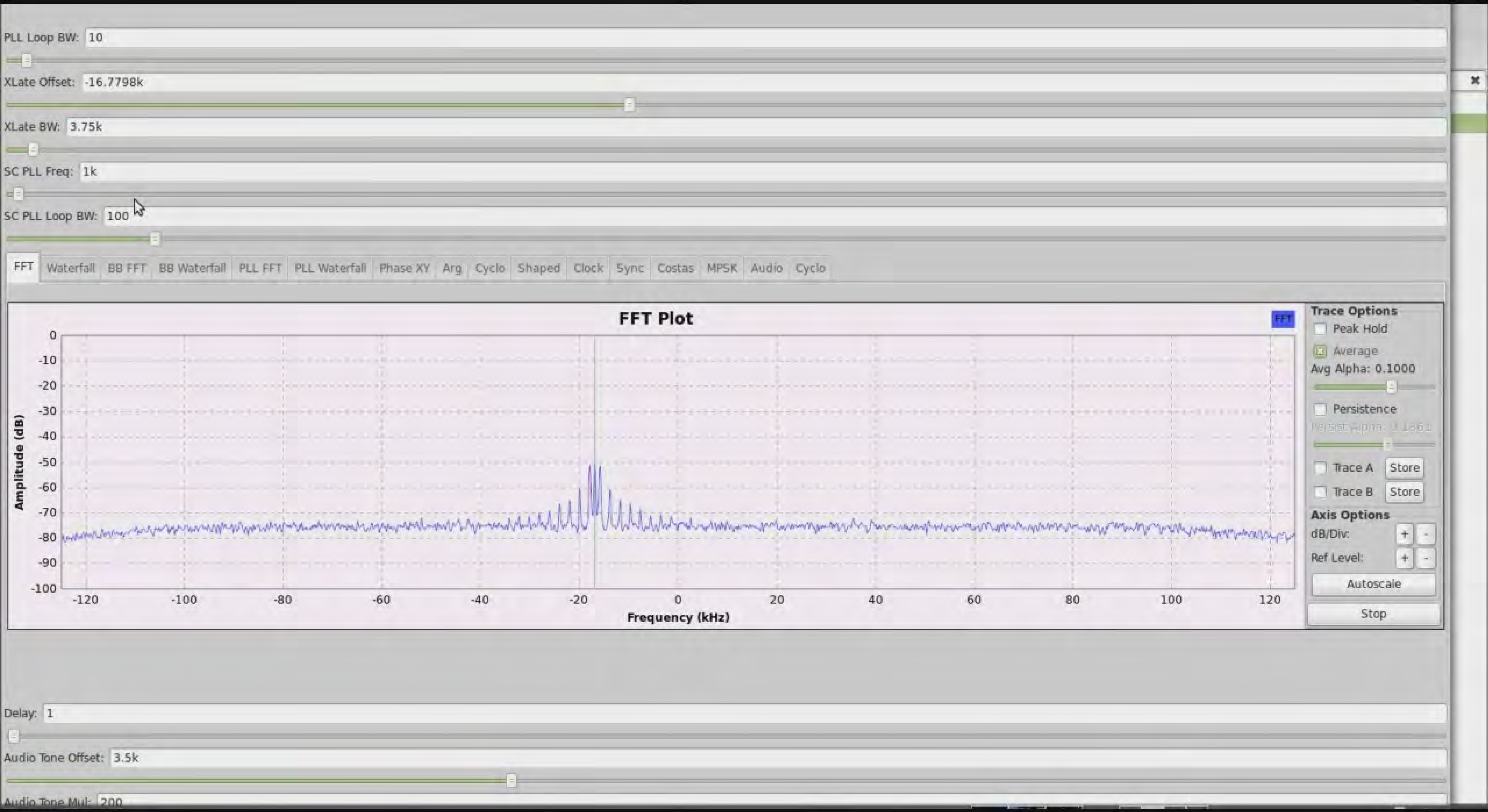
```
0101011000000110110011001000010111100110011000101001110001000101100000000010000110011100110011001110011101001011010011110111111101001010101010101101010101010011010011001100101010101010101011011100110010000001100010111110001
1001111101001100110111010000100110100111110110110101001100101010110100110100110010101101001010101010101100011110000101010110110000010001001010101010001110001011101101101111001101101111010000001011000100010010010101011101001110
00101101001100001110100011010100000110
```

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
```

Telemetry: 16 bps



PLL Loop BW: 10

XLate Offset: -16.7798k

XLate BW: 3.75k

SC PLL Freq: 1k

SC PLL Loop BW: 100

Delay: 1

Audio Tone Offset: 3.5k

Audio Tone Mul: 200

☐ Peak Hold

☒ Average

Avg Alpha: 0.1000

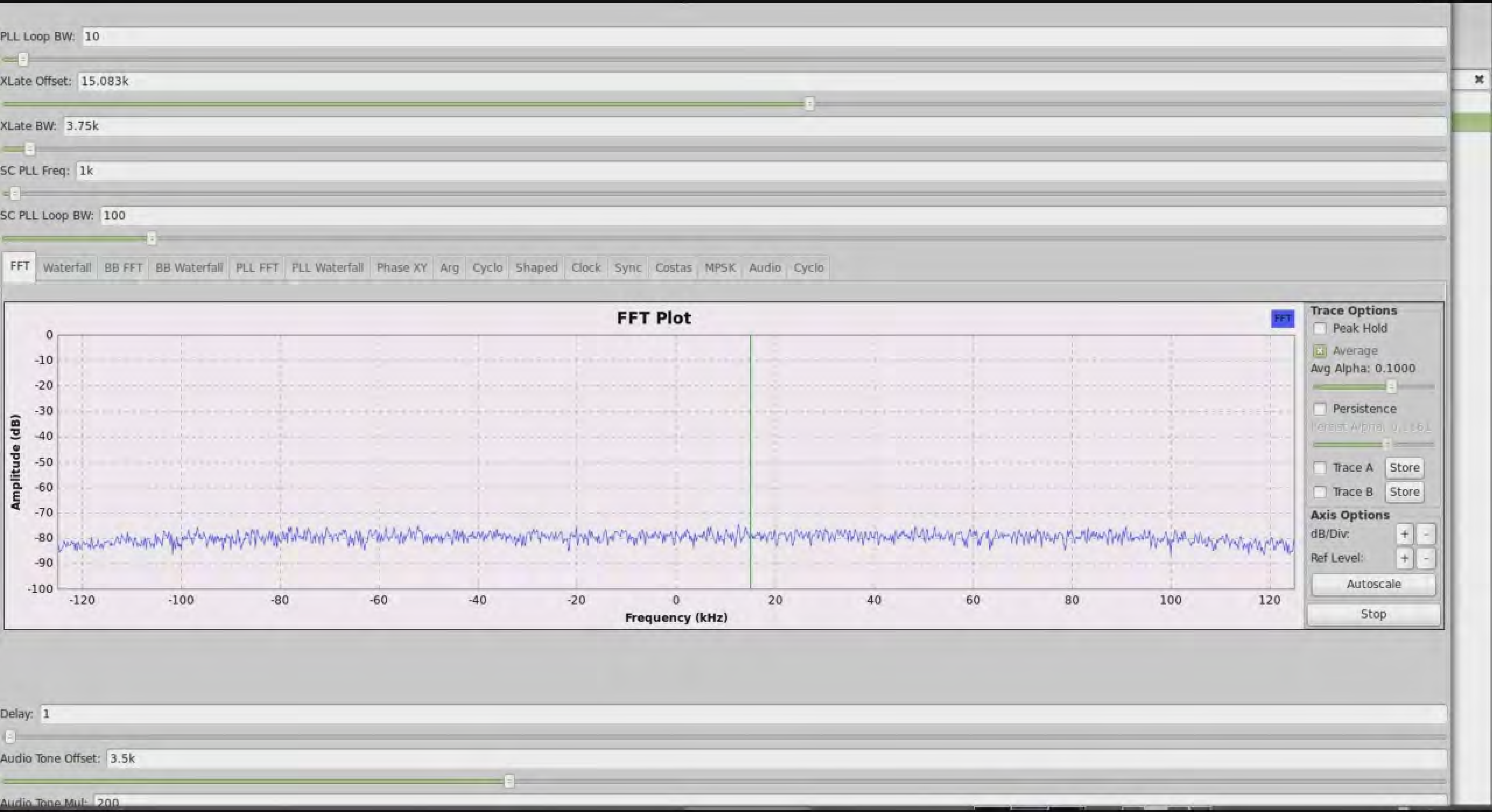
☐ Persistence

Persist Alpha: 0.1861

☐ Trace A

☐ Trace B

Telemetry: 64 bps



PLL Loop BW: 10

XLate Offset: 15.083k

XLate BW: 3.75k

SC PLL Freq: 1k

SC PLL Loop BW: 100

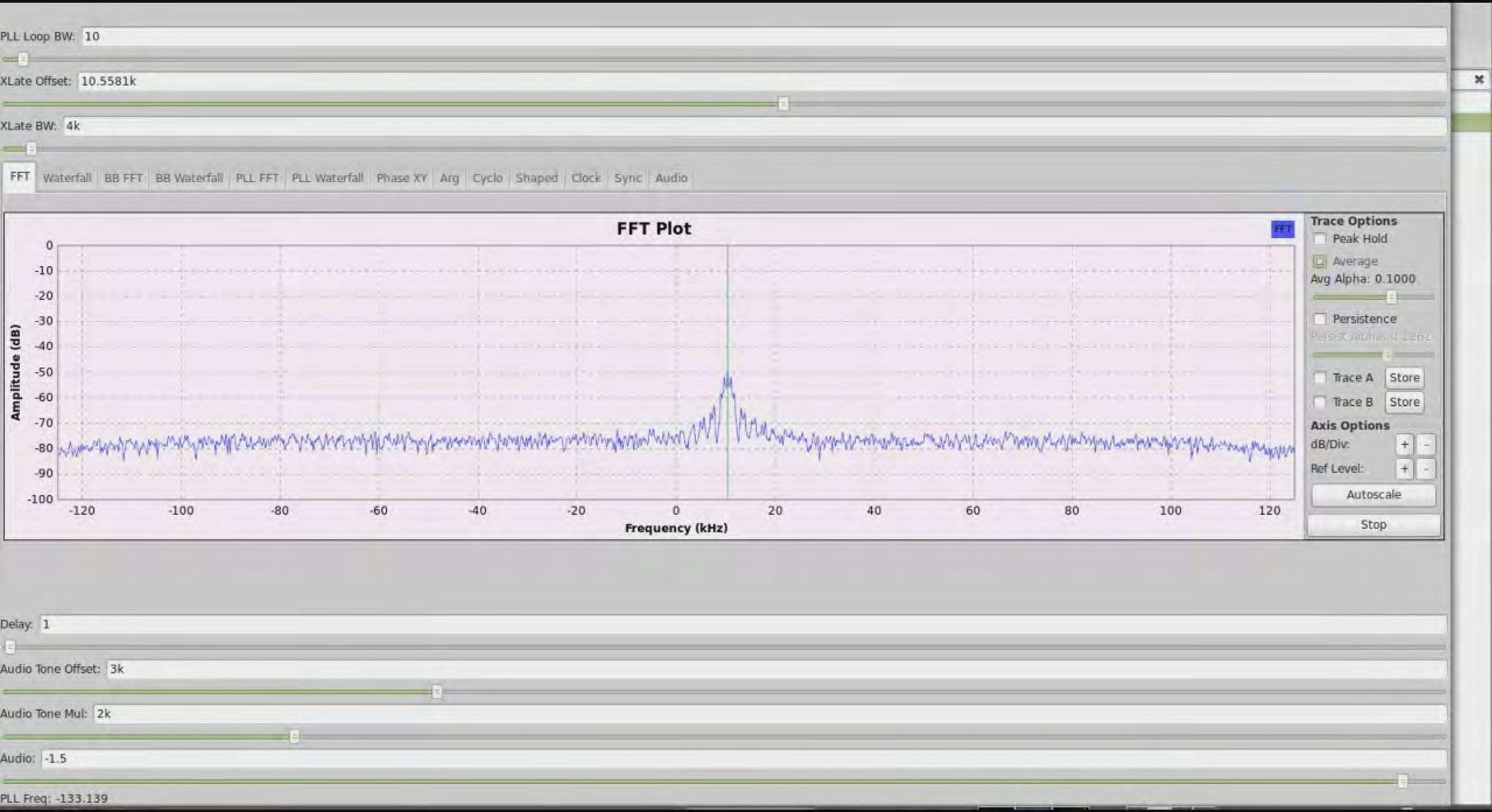
Avg Alpha: 0.1000

Delay: 1

Audio Tone Offset: 3.5k

Audio Tone Mul: 200

Telemetry: 512 bps



PLL Loop BW: 10

XLate Offset: 10.5581k

XLate BW: 4k

Delay: 1

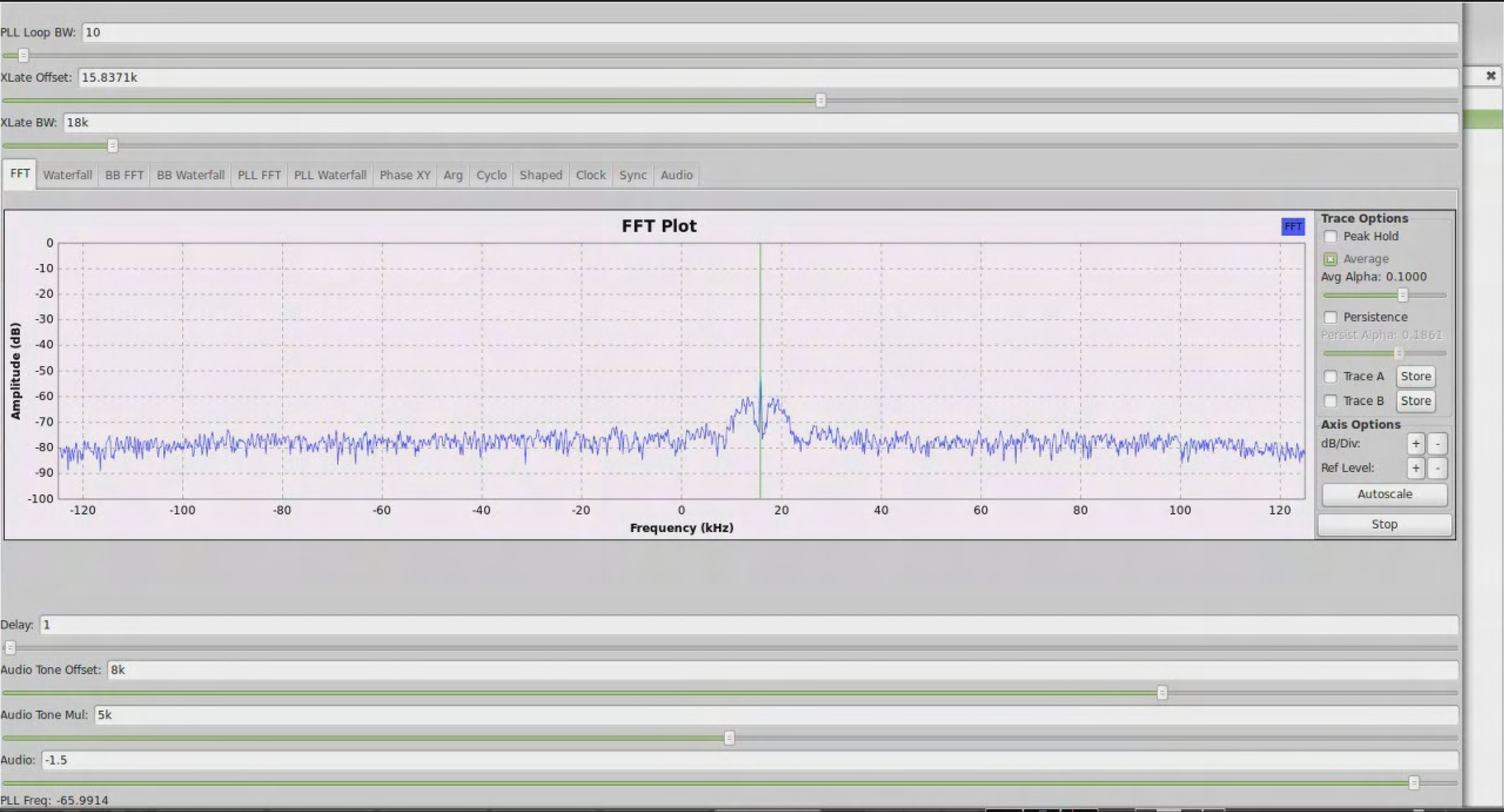
Audio Tone Offset: 3k

Audio Tone Mul: 2k

Audio: -1.5

PLL Freq: -133.139

Telemetry: 2048 bps



PLL Loop BW: 10

XLate Offset: 15.8371k

XLate BW: 18k

☐ Peak Hold

☒ Average

Avg Alpha: 0.1000

☐ Persistence

Persist Alpha: 0.1861

☐ Trace A

☐ Trace B

Delay: 1

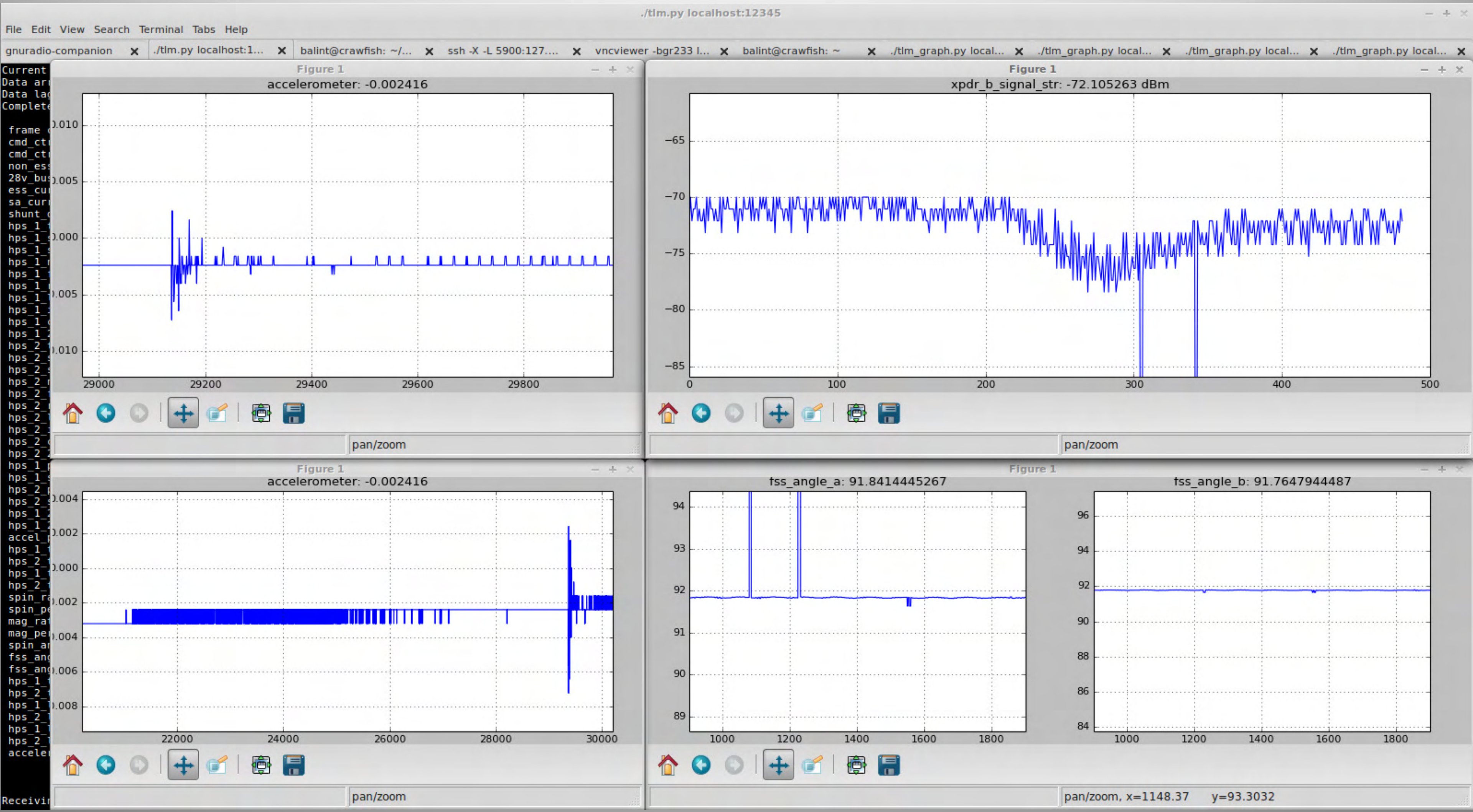
Audio Tone Offset: 8k

Audio Tone Mul: 5k

Audio: -1.5

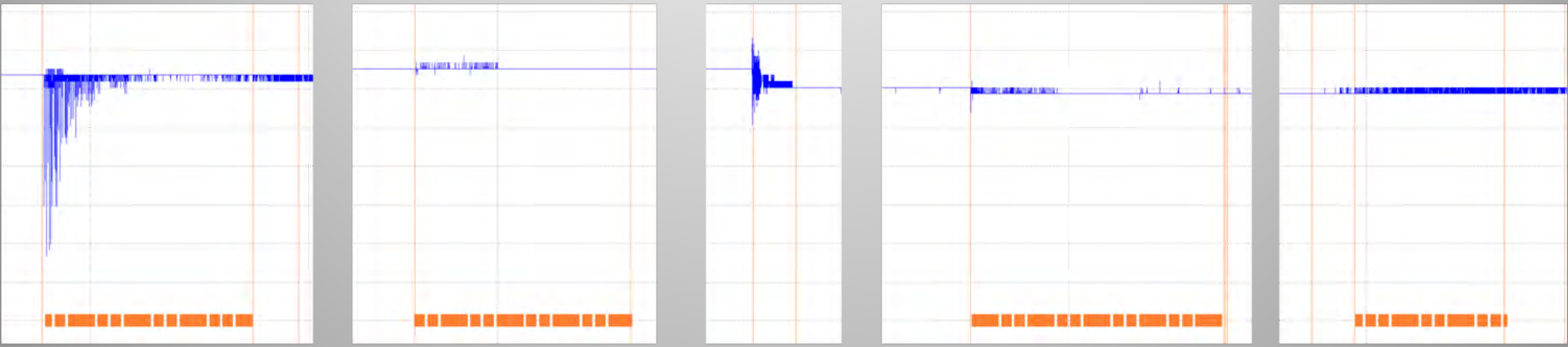
PLL Freq: -65.9914

Telemetry During Thruster Firing

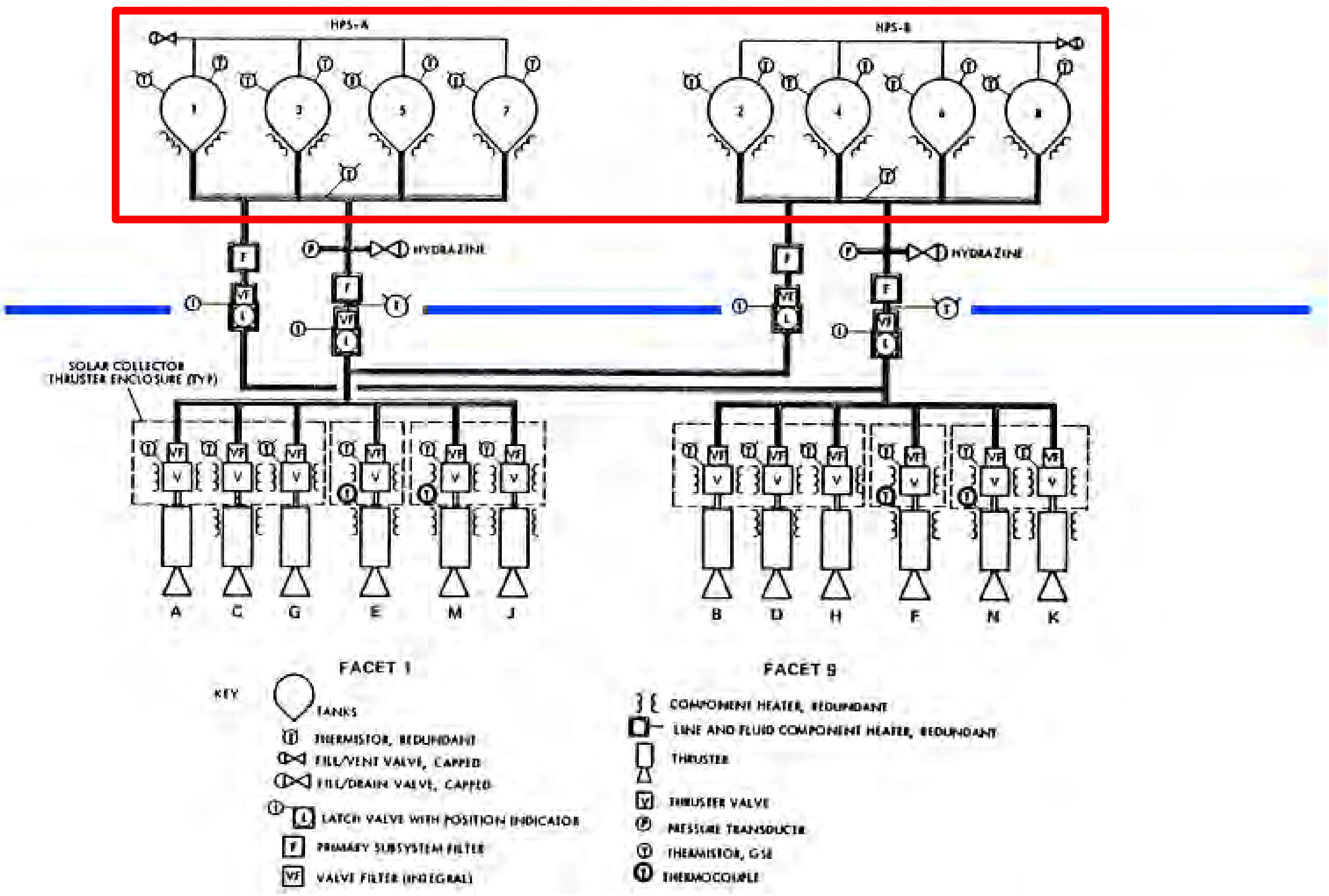


```
Current
Data ar
Data lag
Complete

 frame
 cmd_ct
 cmd_ct
 non_ess
 28v_bu
 ess_cu
 sa_curr
 shunt_
 hps_1_
 hps_1_
 hps_1_
 hps_1_
 hps_1_
 hps_1_
 hps_1_
 hps_1_
 hps_1_
 hps_1_
 hps_2_
 hps_2_
 hps_2_
 hps_2_
 hps_2_
 hps_2_
 hps_2_
 hps_2_
 hps_2_
 hps_2_
 hps_1_
 hps_1_
 hps_2_
 hps_2_
 hps_1_
 hps_1_
 accel_
 hps_1_
 hps_2_
 hps_1_
 hps_2_
 spin_ra
 spin_pe
 mag_ra
 mag_pe
 spin_a
 fss_an
 fss_an
 hps_1_
 hps_2_
 hps_1_
 hps_2_
 hps_1_
 hps_2_
 acceler

Receivi
```

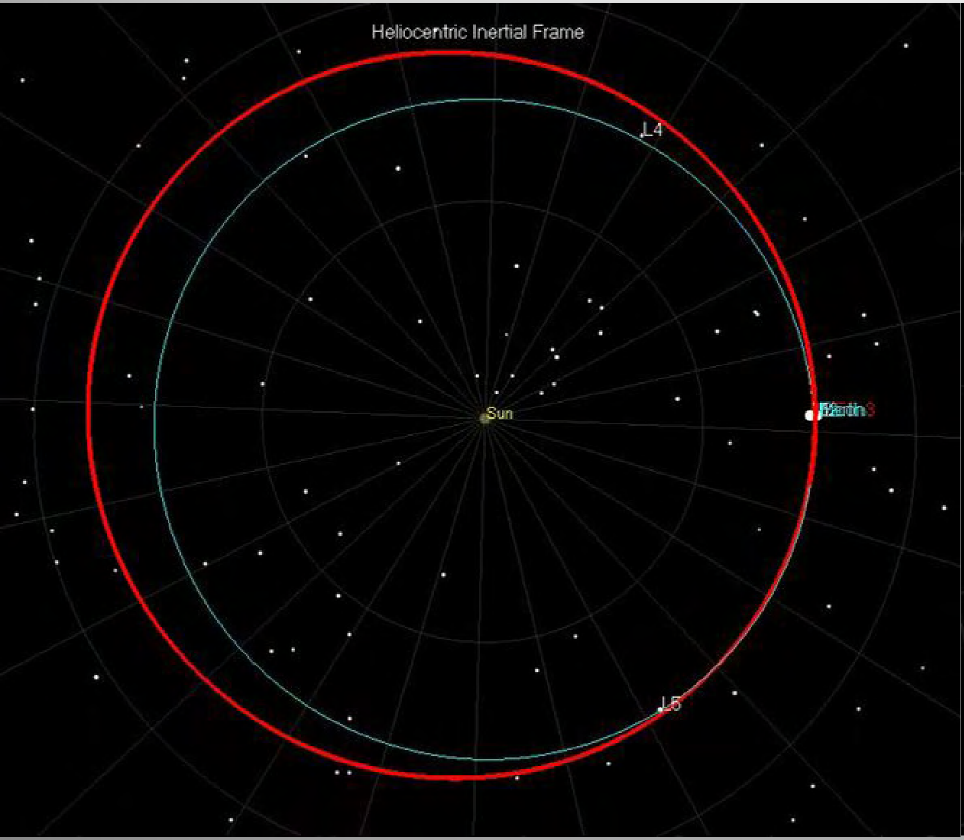
No Thrust

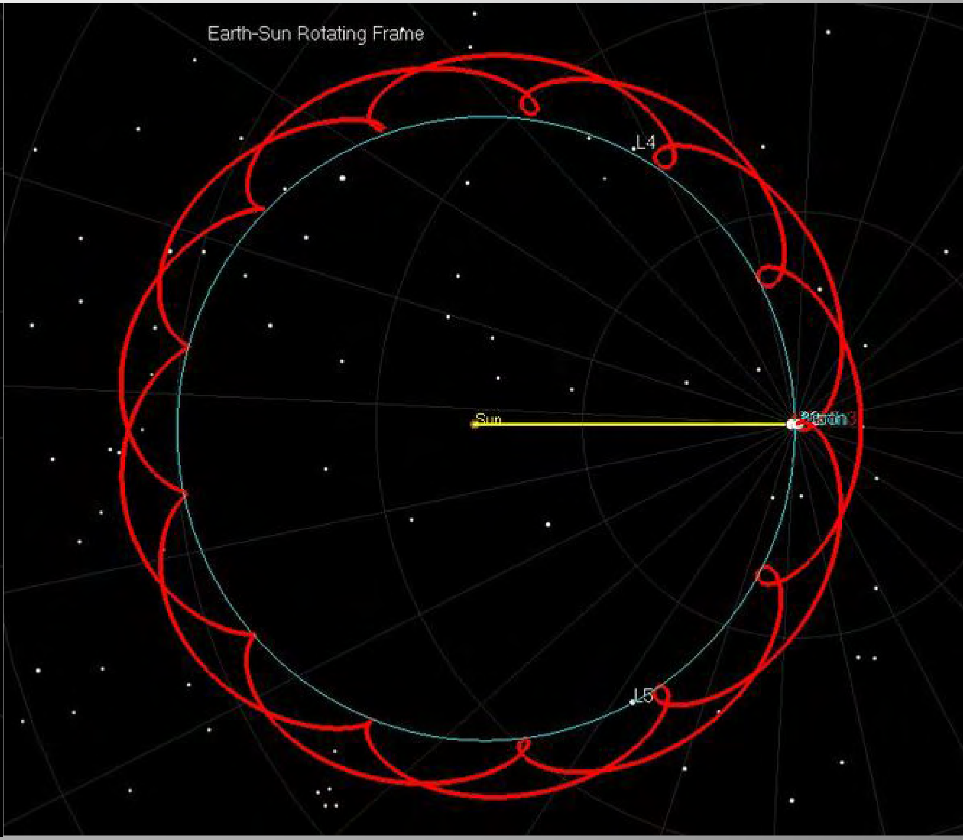


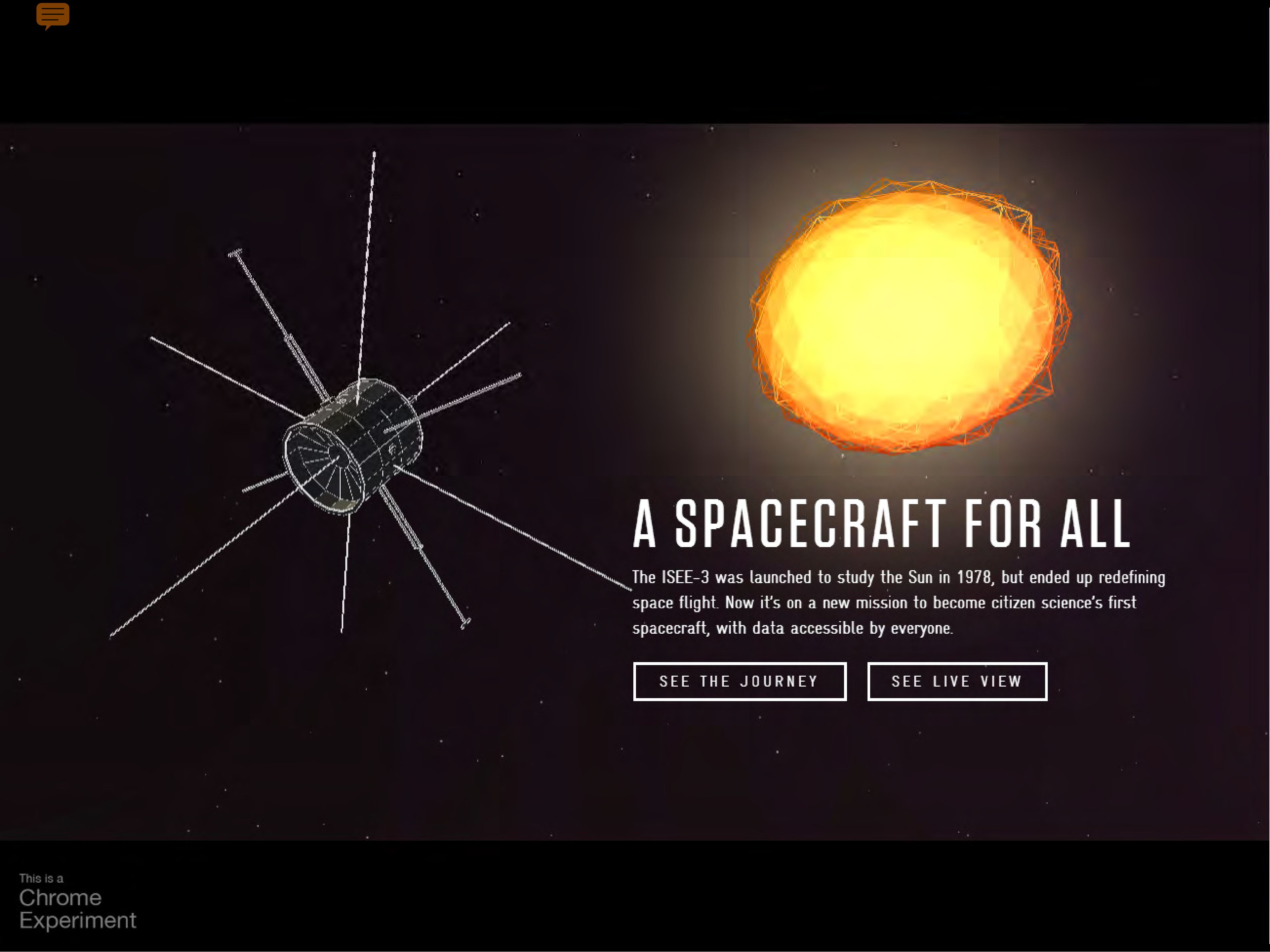
Hydrazine Propulsion System



New Orbit


Heliocentric Inertial Frame
L4
Sun
Earth
L5

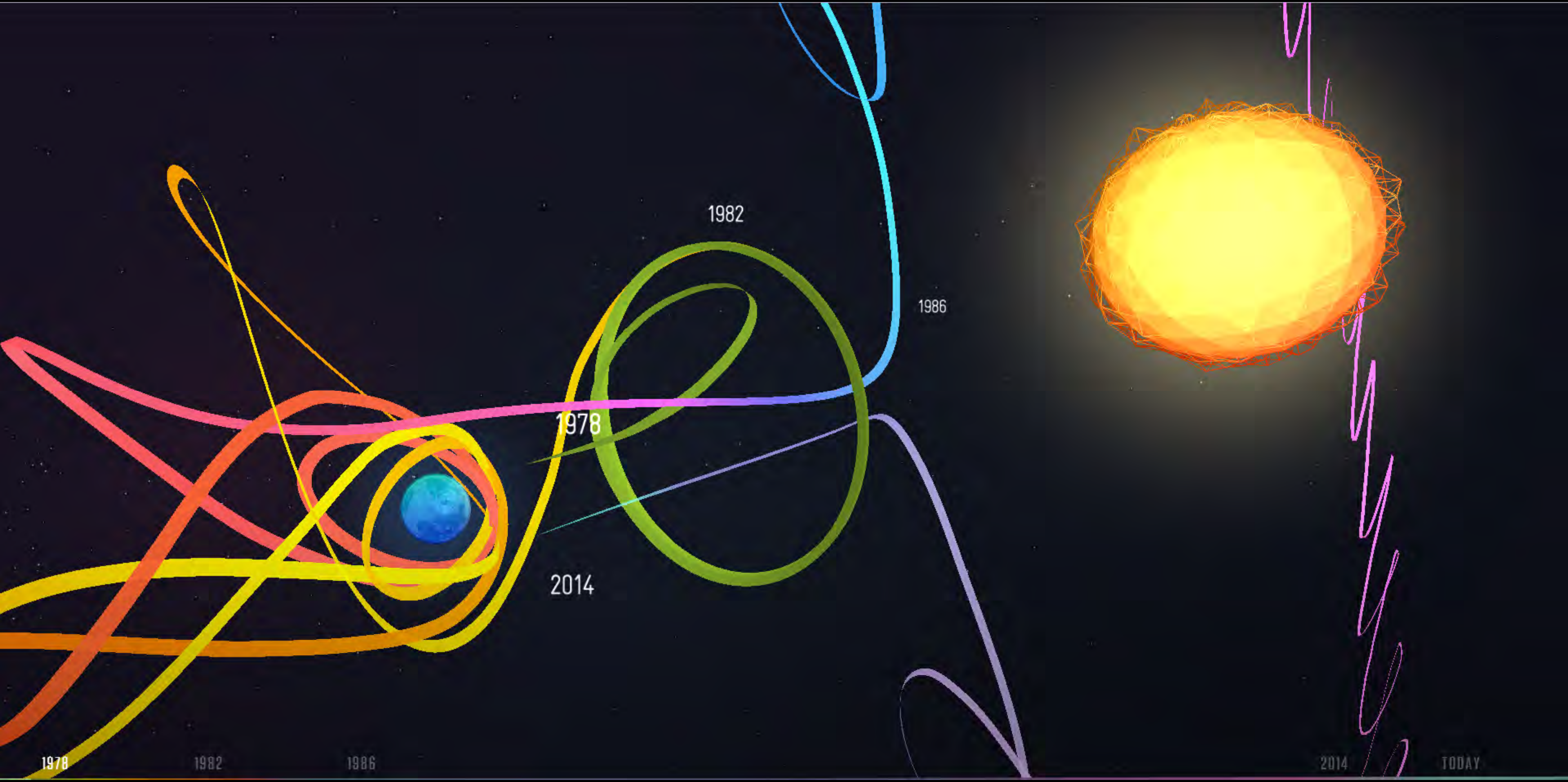

Earth-Sun Rotating Frame
L4
Sun
Earth
L5



A SPACECRAFT FOR ALL

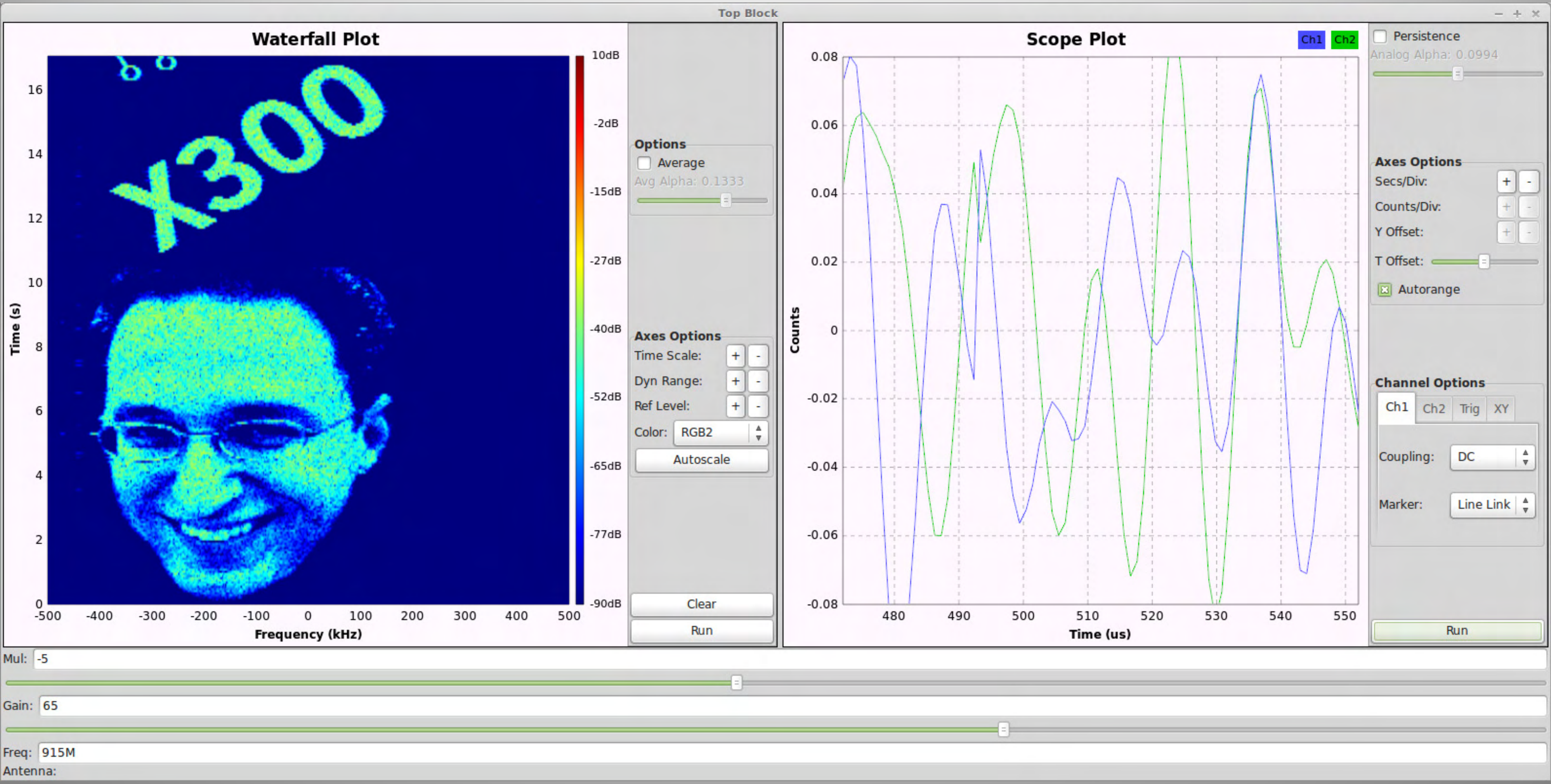
The ISEE-3 was launched to study the Sun in 1978, but ended up redefining space flight. Now it's on a new mission to become citizen science's first spacecraft, with data accessible by everyone.

www.spacecraftforall.com



oit
06

#cyberspectrum



Top Block

☐ Average
Avg Alpha: 0.1333

Color: RGB2

☐ Persistence
Analog Alpha: 0.0994

☒ Autorange

Coupling: DC

Marker: Line Link

Mul: -5

Gain: 65

Freq: 915M

Antenna:

http://wiki.spench.net/wiki/RF

http://spench.net/

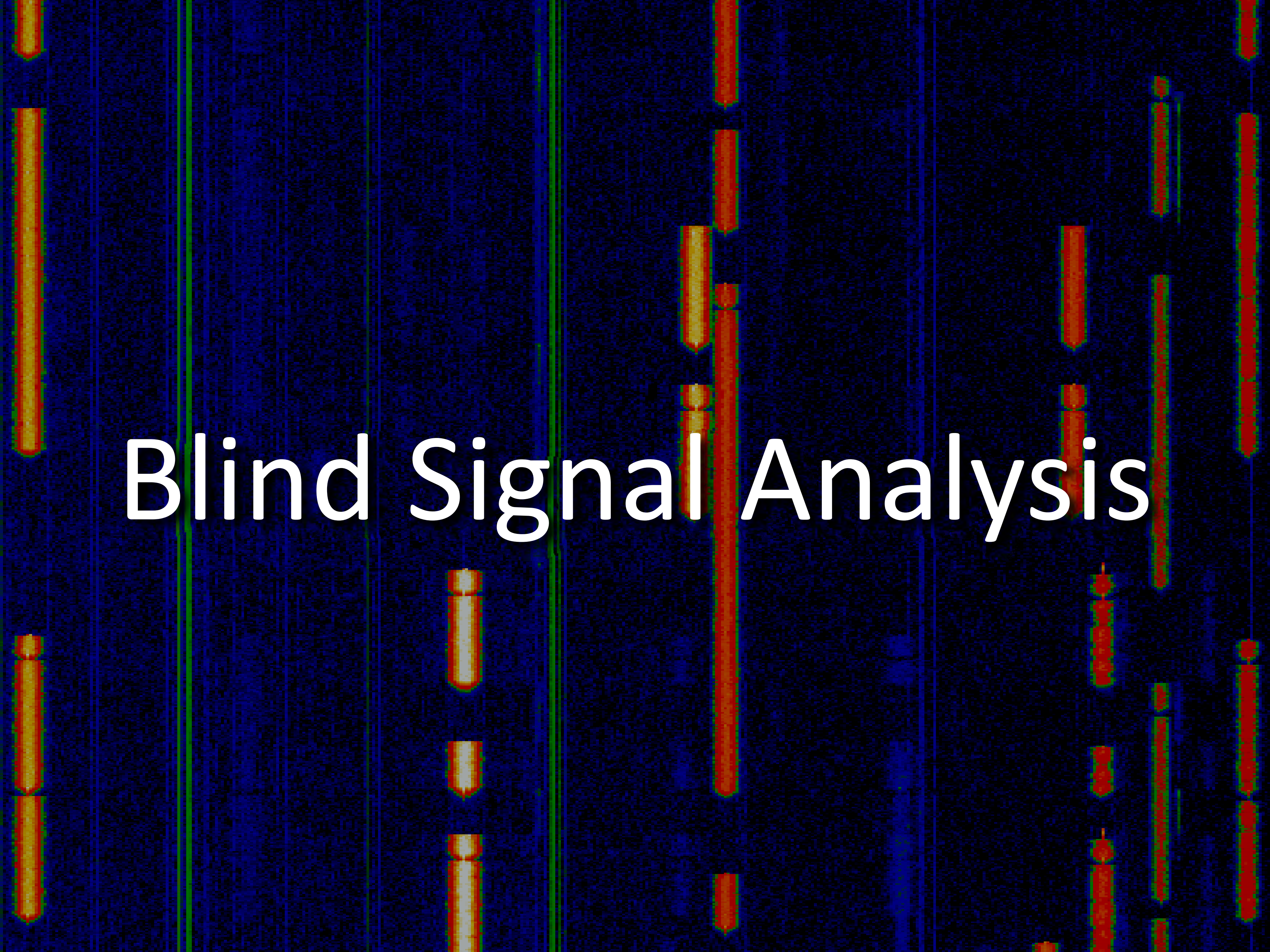
GitHub: balint256

balint@spench.net

balint@ettus.com

@spenchdotnet

Other Applications

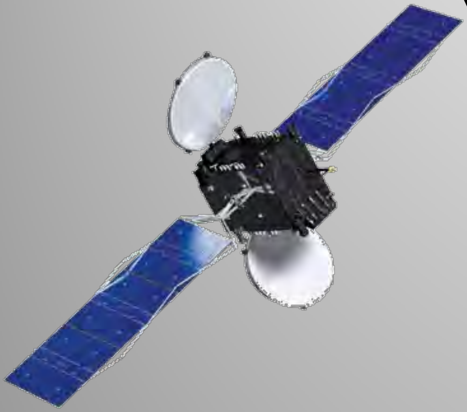


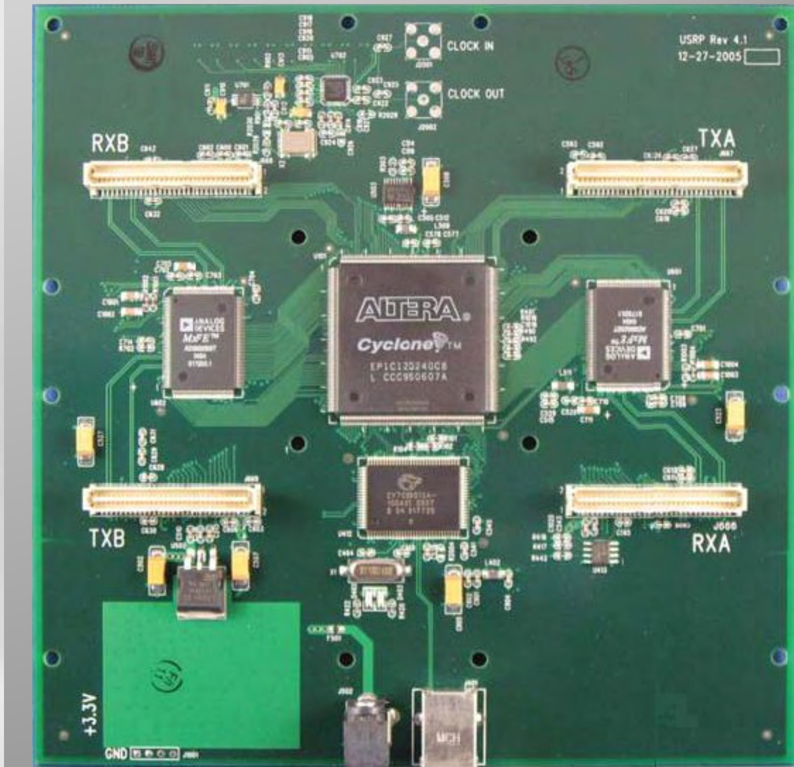
Blind Signal Analysis

What you need

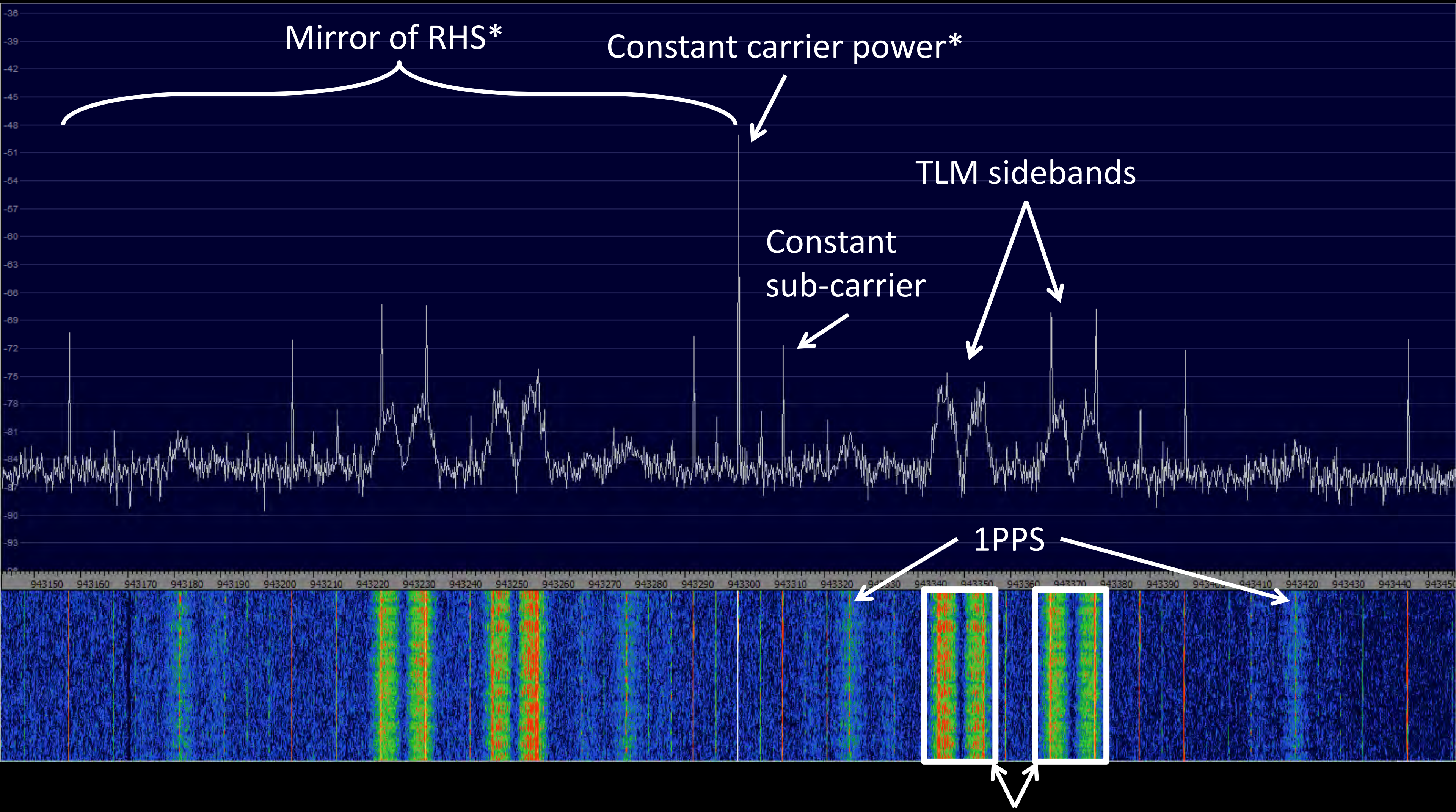
Dish + LNB + power injector + USRP + GNU Radio

(set-top box with LNB-thru)





D1 TLM1: 12243.25 MHz



Mirror of RHS*

Constant carrier power*

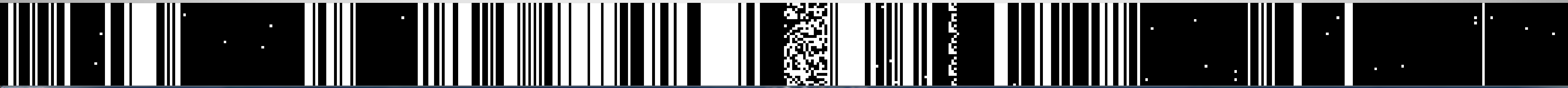
TLM sidebands

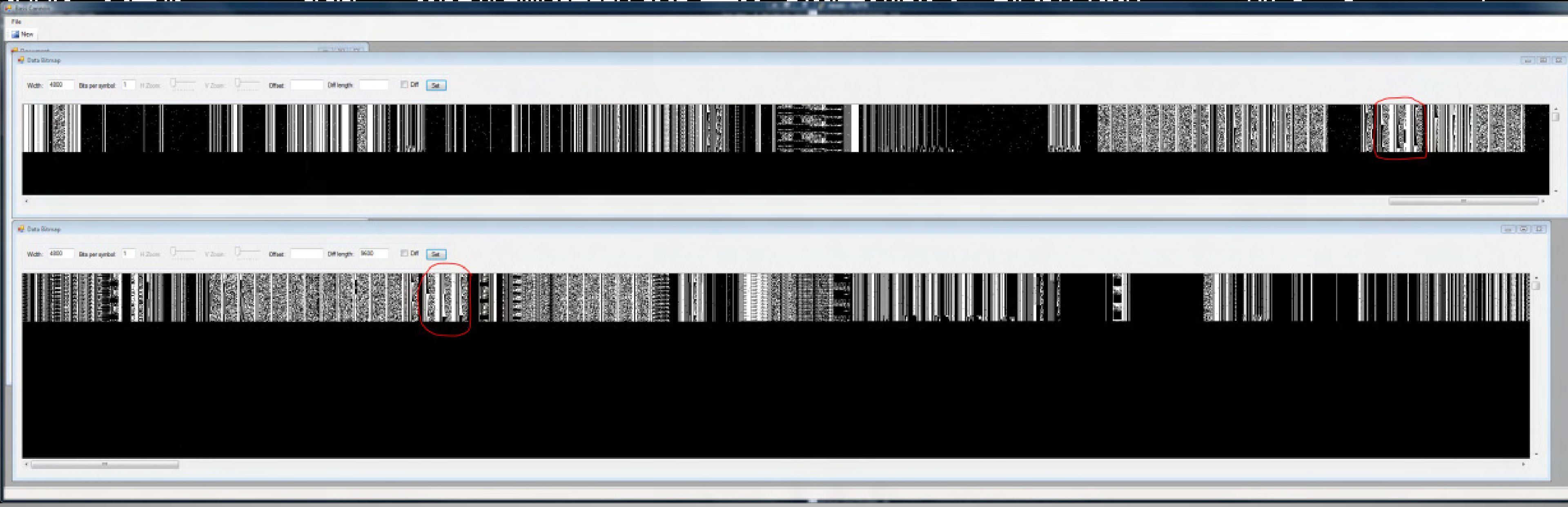
Constant sub-carrier

1PPS

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

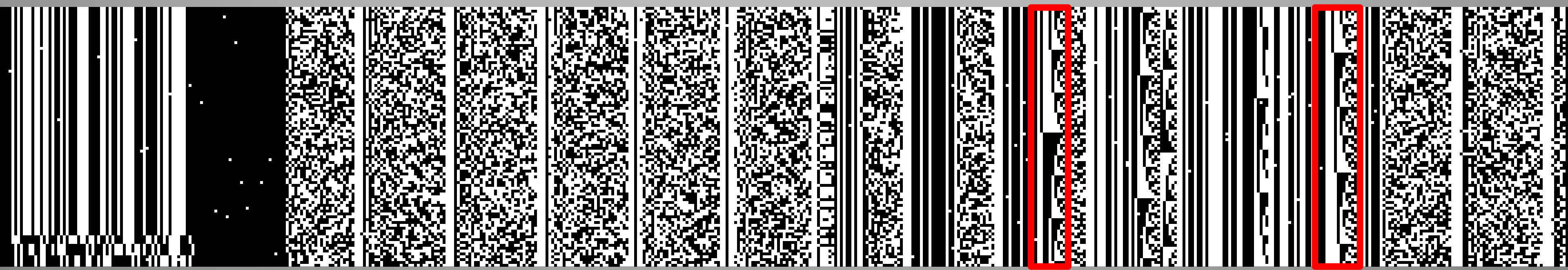
Visualisation



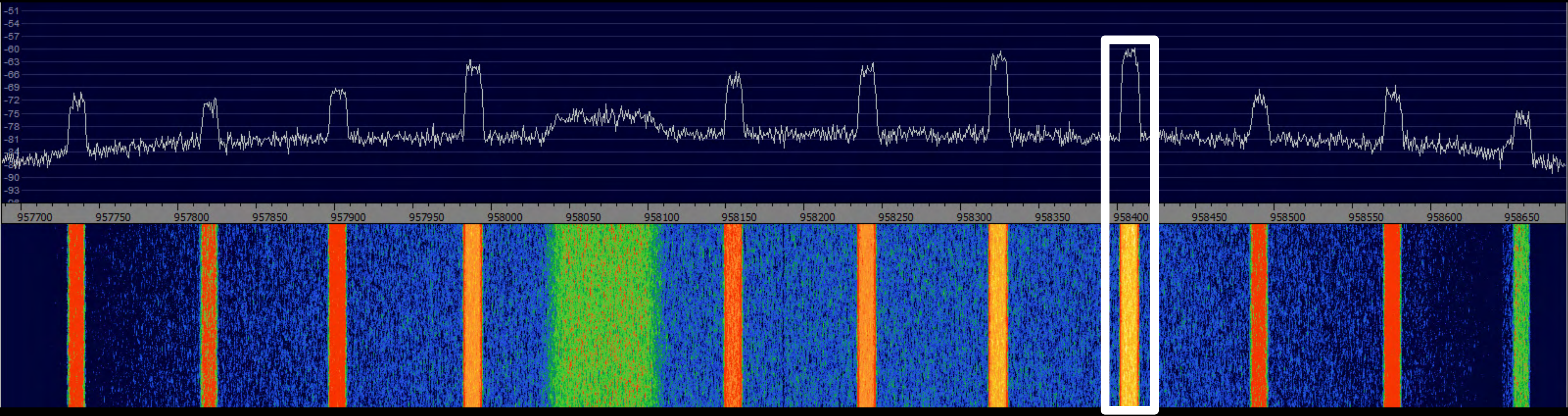


Width: 4800 Bits per symbol: 1 Offset: Diff length: □ Diff

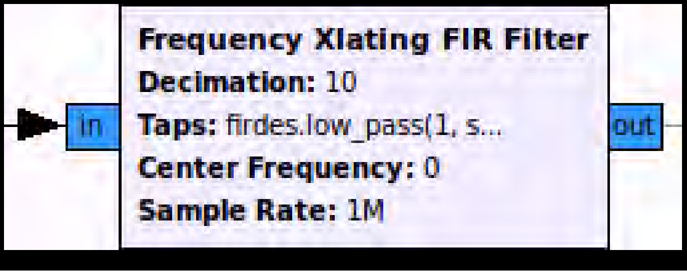
Width: 4800 Bits per symbol: 1 Offset: Diff length: 9600 □ Diff



Let’s try one…



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


Frequency Xlating FIR Filter

Decimation: 10

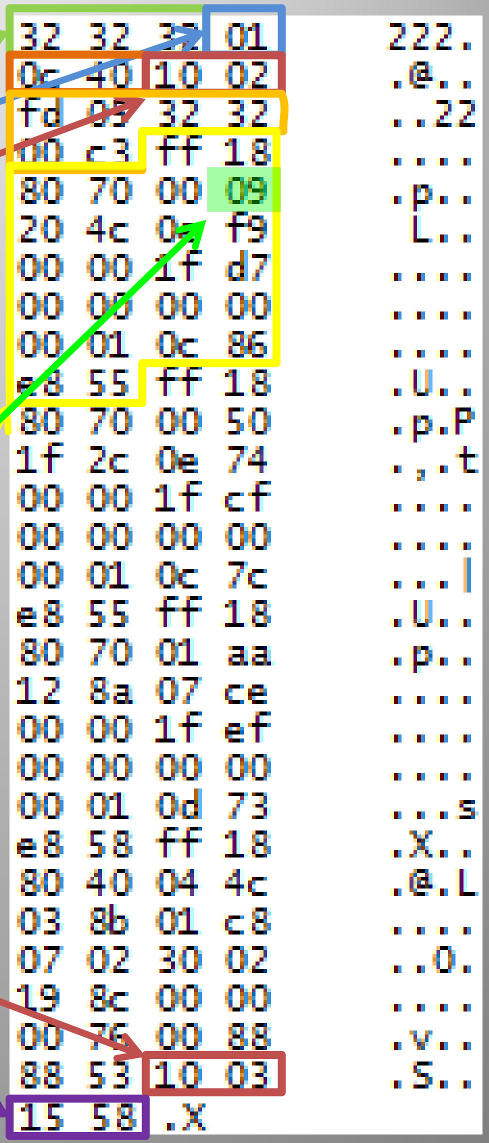
Taps: firdes.low_pass(1, s...

Center Frequency: 0

Sample Rate: 1M

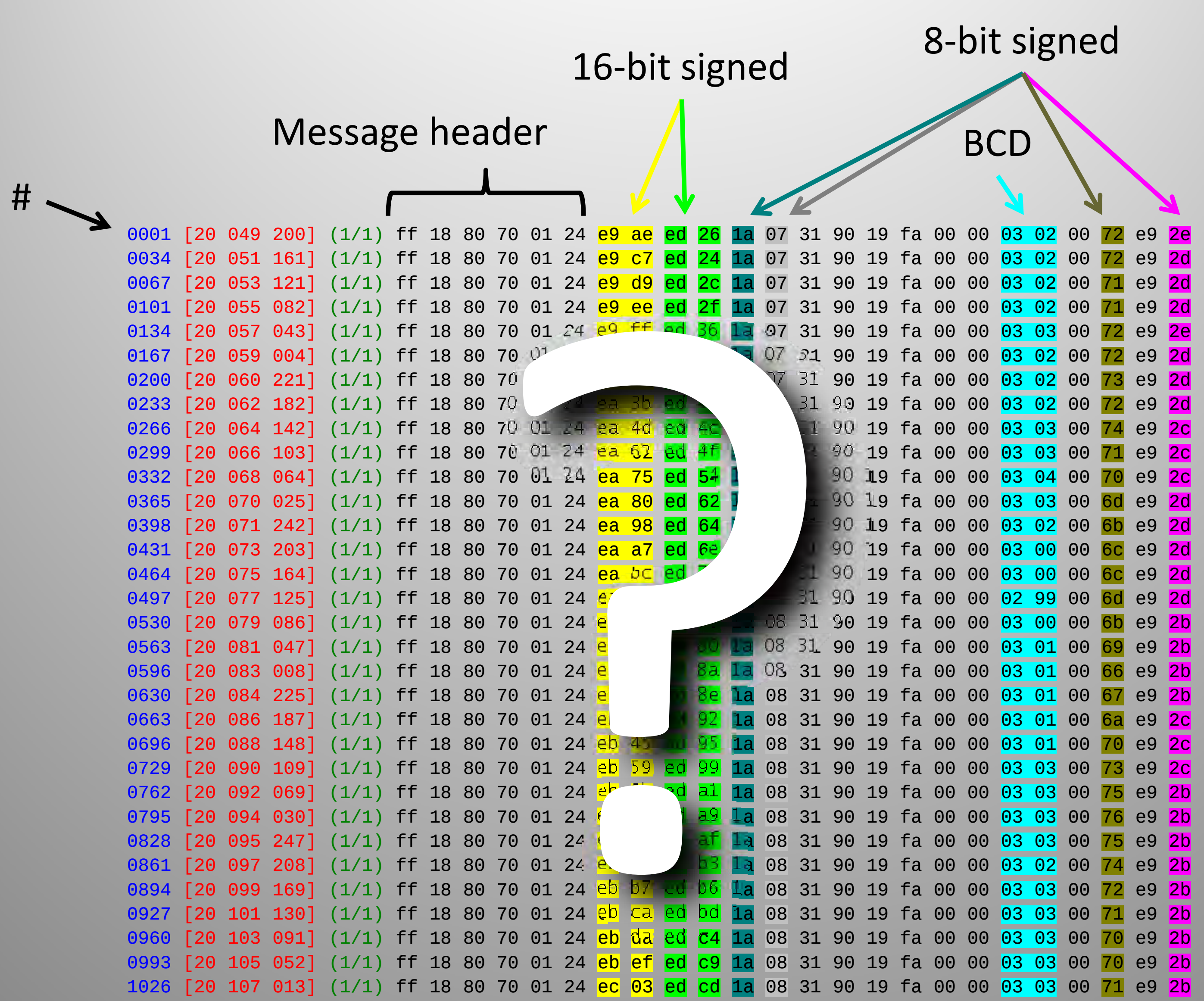
Frame analysis

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



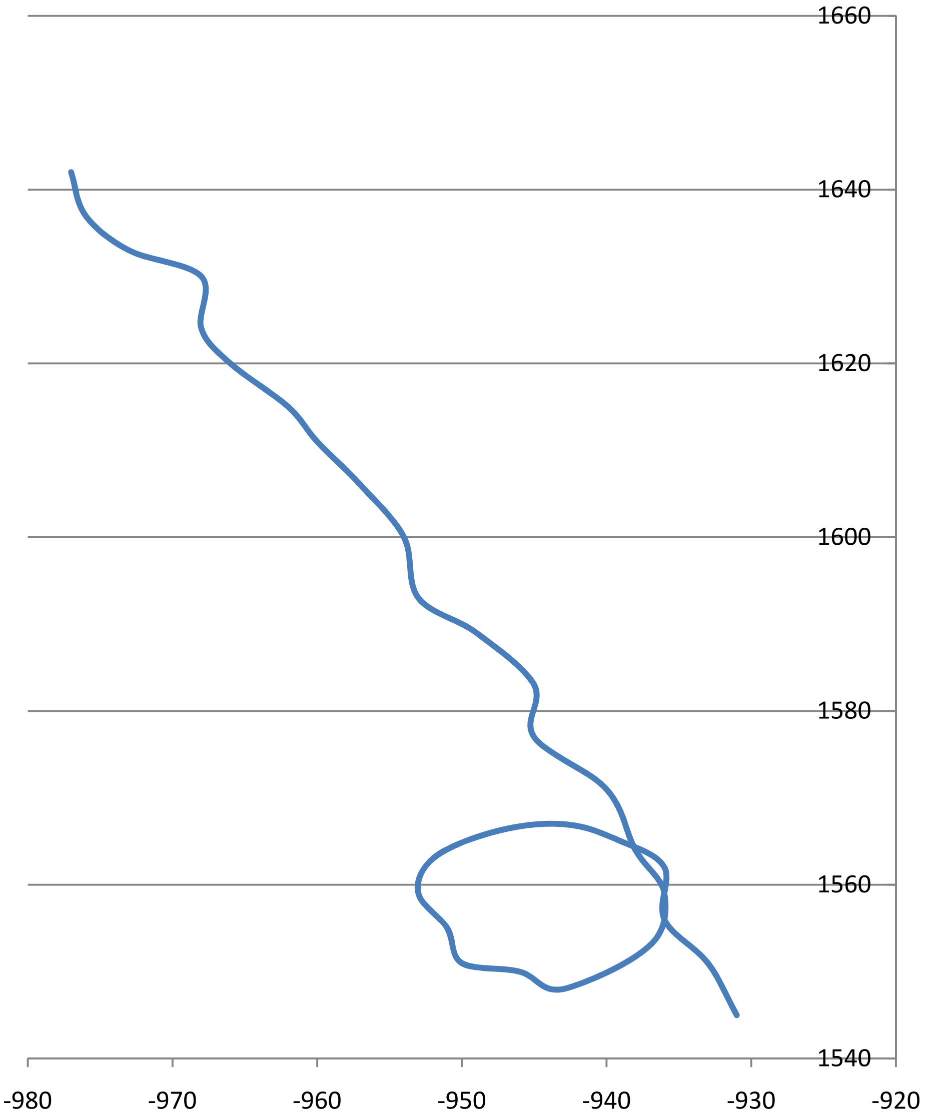
```
32 32 32 01        222.
0c 40 10 02        .@..
fd 03 32 32        ..22
00 c3 ff 18        ....
80 70 00 09        .p..
20 4c 0e f9         L..
00 00 1f d7        ....
00 00 00 00        ....
00 01 0c 86        ....
e8 55 ff 18        .U..
80 70 00 50        .p.P
1f 2c 0e 74        .,.t
00 00 1f cf        ....
00 00 00 00        ....
00 01 0c 7c        ...|
e8 55 ff 18        .U..
80 70 01 aa        .p..
12 8a 07 ce        ....
00 00 1f ef        ....
00 00 00 00        ....
00 01 0d 73        ...s
e8 58 ff 18        .X..
80 40 04 4c        .@.L
03 8b 01 c8        ....
07 02 30 02        ..0.
19 8c 00 00        ....
00 76 00 88        .v..
88 53 10 03        .S..
15 58 .X
```

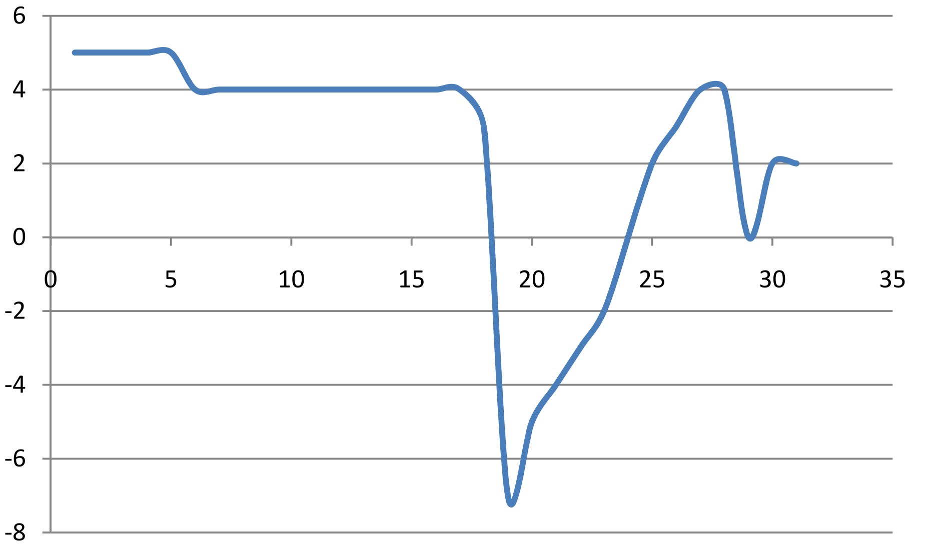
Un-pack & find patterns

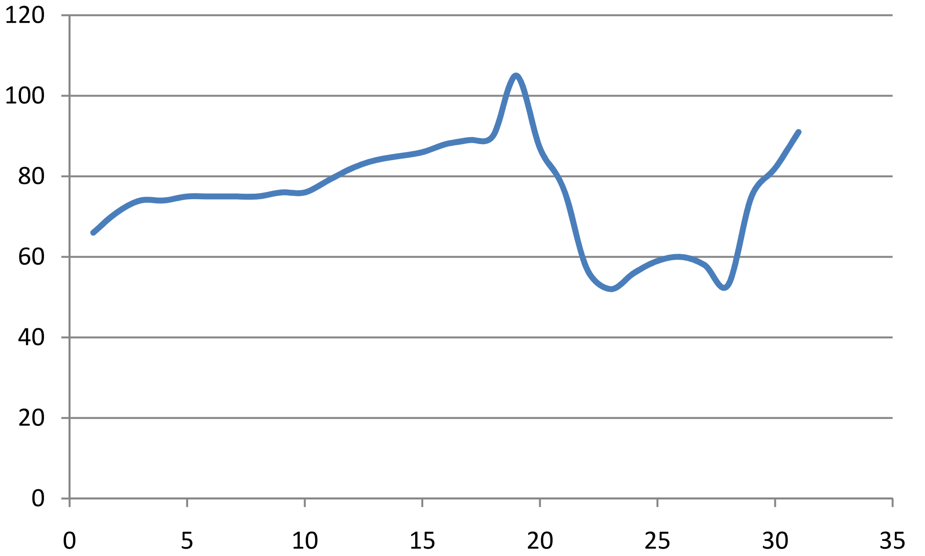


```
0001 [20 049 200] (1/1) ff 18 80 70 01 24 e9 ae ed 26 1a 07 31 90 19 fa 00 00 03 02 00 72 e9 2e
0034 [20 051 161] (1/1) ff 18 80 70 01 24 e9 c7 ed 24 1a 07 31 90 19 fa 00 00 03 02 00 72 e9 2d
0067 [20 053 121] (1/1) ff 18 80 70 01 24 e9 d9 ed 2c 1a 07 31 90 19 fa 00 00 03 02 00 71 e9 2d
0101 [20 055 082] (1/1) ff 18 80 70 01 24 e9 ee ed 2f 1a 07 31 90 19 fa 00 00 03 02 00 71 e9 2d
0134 [20 057 043] (1/1) ff 18 80 70 01 24 e9 ff ed 36 1a 07 31 90 19 fa 00 00 03 03 00 72 e9 2e
0167 [20 059 004] (1/1) ff 18 80 70 01 [illegible] [illegible] [illegible] [illegible] [illegible] 1a 07 31 90 19 fa 00 00 03 02 00 72 e9 2d
0200 [20 060 221] (1/1) ff 18 80 70 [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] 07 31 90 19 fa 00 00 03 02 00 73 e9 2d
0233 [20 062 182] (1/1) ff 18 80 70 [illegible] 24 ea 3b ed [illegible] [illegible] [illegible] 31 90 19 fa 00 00 03 02 00 72 e9 2d
0266 [20 064 142] (1/1) ff 18 80 70 01 24 ea 4d ed 4c [illegible] [illegible] 31 90 19 fa 00 00 03 03 00 74 e9 2c
0299 [20 066 103] (1/1) ff 18 80 70 01 24 ea 62 ed 4f [illegible] [illegible] [illegible] 90 19 fa 00 00 03 03 00 71 e9 2c
0332 [20 068 064] (1/1) ff 18 80 70 01 24 ea 75 ed 54 [illegible] [illegible] [illegible] 90 19 fa 00 00 03 04 00 70 e9 2c
0365 [20 070 025] (1/1) ff 18 80 70 01 24 ea 80 ed 62 [illegible] [illegible] [illegible] 90 19 fa 00 00 03 03 00 6d e9 2d
0398 [20 071 242] (1/1) ff 18 80 70 01 24 ea 98 ed 64 [illegible] [illegible] [illegible] 90 19 fa 00 00 03 02 00 6b e9 2d
0431 [20 073 203] (1/1) ff 18 80 70 01 24 ea a7 ed 6e [illegible] [illegible] [illegible] 90 19 fa 00 00 03 00 00 6c e9 2d
0464 [20 075 164] (1/1) ff 18 80 70 01 24 ea bc ed [illegible] [illegible] [illegible] 31 90 19 fa 00 00 03 00 00 6c e9 2d
0497 [20 077 125] (1/1) ff 18 80 70 01 24 [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] 31 90 19 fa 00 00 02 99 00 6d e9 2d
0530 [20 079 086] (1/1) ff 18 80 70 01 24 [illegible] [illegible] [illegible] [illegible] [illegible] 08 31 90 19 fa 00 00 03 00 00 6b e9 2b
0563 [20 081 047] (1/1) ff 18 80 70 01 24 [illegible] [illegible] [illegible] [illegible] 1a 08 31 90 19 fa 00 00 03 01 00 69 e9 2b
0596 [20 083 008] (1/1) ff 18 80 70 01 24 [illegible] [illegible] [illegible] 8a 1a 08 31 90 19 fa 00 00 03 01 00 66 e9 2b
0630 [20 084 225] (1/1) ff 18 80 70 01 24 [illegible] [illegible] [illegible] 8e 1a 08 31 90 19 fa 00 00 03 01 00 67 e9 2b
0663 [20 086 187] (1/1) ff 18 80 70 01 24 [illegible] [illegible] [illegible] 92 1a 08 31 90 19 fa 00 00 03 01 00 6a e9 2c
0696 [20 088 148] (1/1) ff 18 80 70 01 24 eb 45 [illegible] 95 1a 08 31 90 19 fa 00 00 03 01 00 70 e9 2c
0729 [20 090 109] (1/1) ff 18 80 70 01 24 eb 59 ed 99 1a 08 31 90 19 fa 00 00 03 03 00 73 e9 2c
0762 [20 092 069] (1/1) ff 18 80 70 01 24 eb [illegible] ed a1 1a 08 31 90 19 fa 00 00 03 03 00 75 e9 2b
0795 [20 094 030] (1/1) ff 18 80 70 01 24 [illegible] [illegible] [illegible] a9 1a 08 31 90 19 fa 00 00 03 03 00 76 e9 2b
0828 [20 095 247] (1/1) ff 18 80 70 01 24 [illegible] [illegible] [illegible] af 1a 08 31 90 19 fa 00 00 03 03 00 75 e9 2b
0861 [20 097 208] (1/1) ff 18 80 70 01 24 [illegible] [illegible] [illegible] b3 1a 08 31 90 19 fa 00 00 03 02 00 74 e9 2b
0894 [20 099 169] (1/1) ff 18 80 70 01 24 eb b7 ed b6 1a 08 31 90 19 fa 00 00 03 03 00 72 e9 2b
0927 [20 101 130] (1/1) ff 18 80 70 01 24 eb ca ed bd 1a 08 31 90 19 fa 00 00 03 03 00 71 e9 2b
0960 [20 103 091] (1/1) ff 18 80 70 01 24 eb da ed c4 1a 08 31 90 19 fa 00 00 03 03 00 70 e9 2b
0993 [20 105 052] (1/1) ff 18 80 70 01 24 eb ef ed c9 1a 08 31 90 19 fa 00 00 03 03 00 70 e9 2b
1026 [20 107 013] (1/1) ff 18 80 70 01 24 ec 03 ed cd 1a 08 31 90 19 fa 00 00 03 03 00 71 e9 2b
```

Graphing the Data

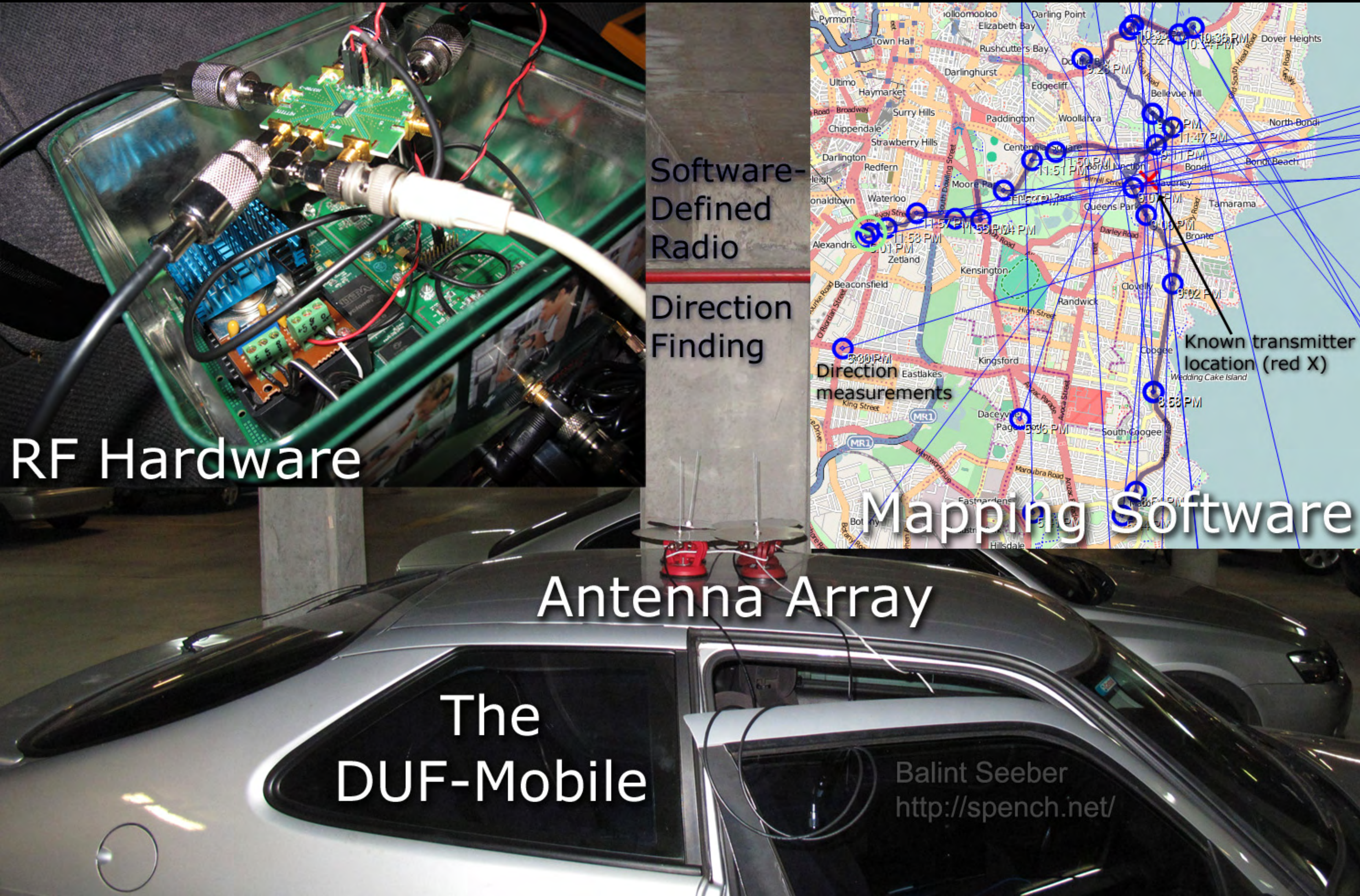




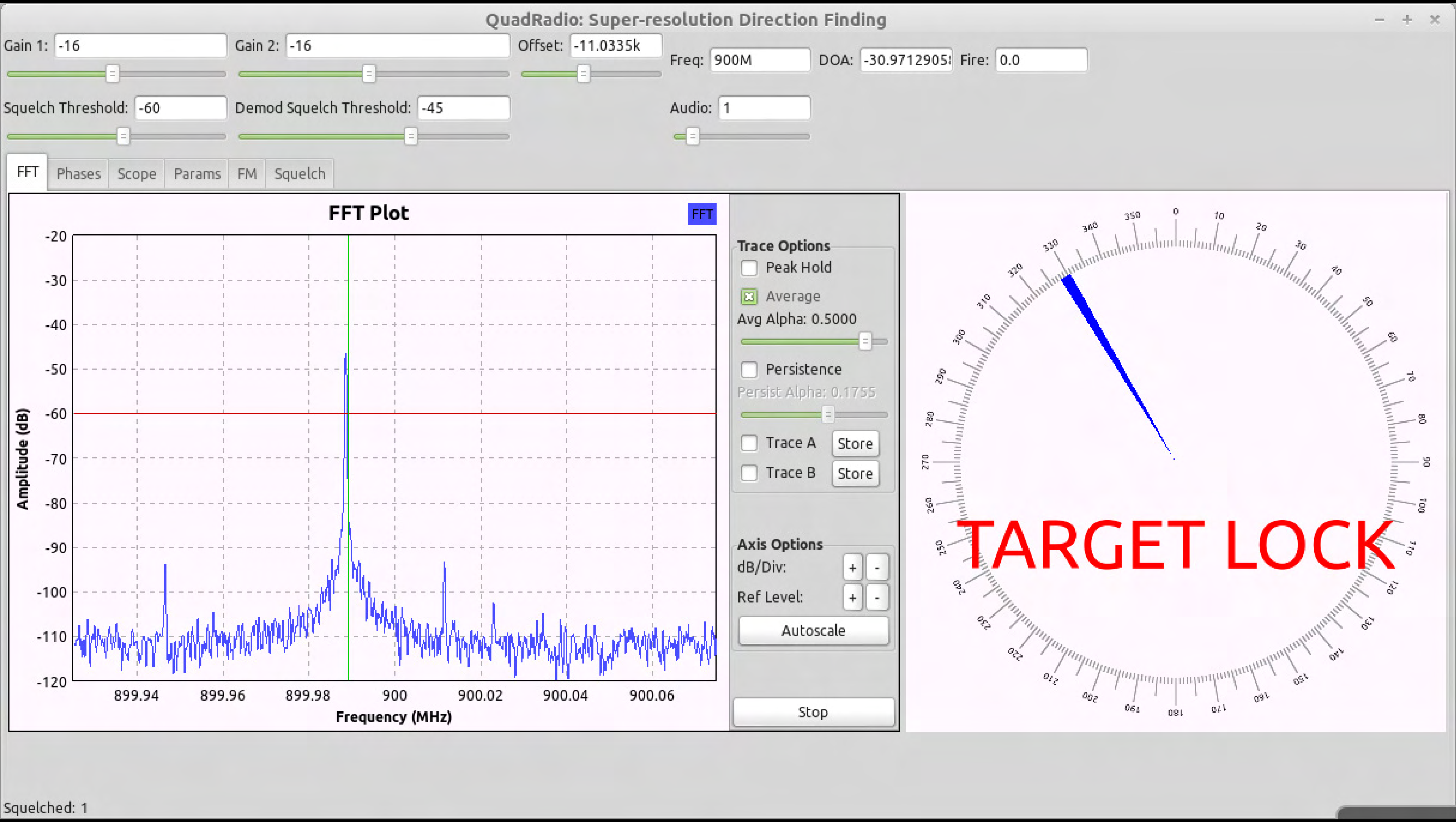


Software Defined Radio Direction Finding

SDR Direction Finding



Balint Seeber
http://spench.net/



QuadRadio: Super-resolution Direction Finding

Gain 1: -16

Gain 2: -16

Offset: -11.0335k

Freq: 900M

DOA: -30.9712905

Fire: 0.0

Squelch Threshold: -60

Demod Squelch Threshold: -45

Audio: 1

Trace Options

□ Peak Hold

☒ Average

Avg Alpha: 0.5000

□ Persistence

Persist Alpha: 0.1755

□ Trace A

□ Trace B

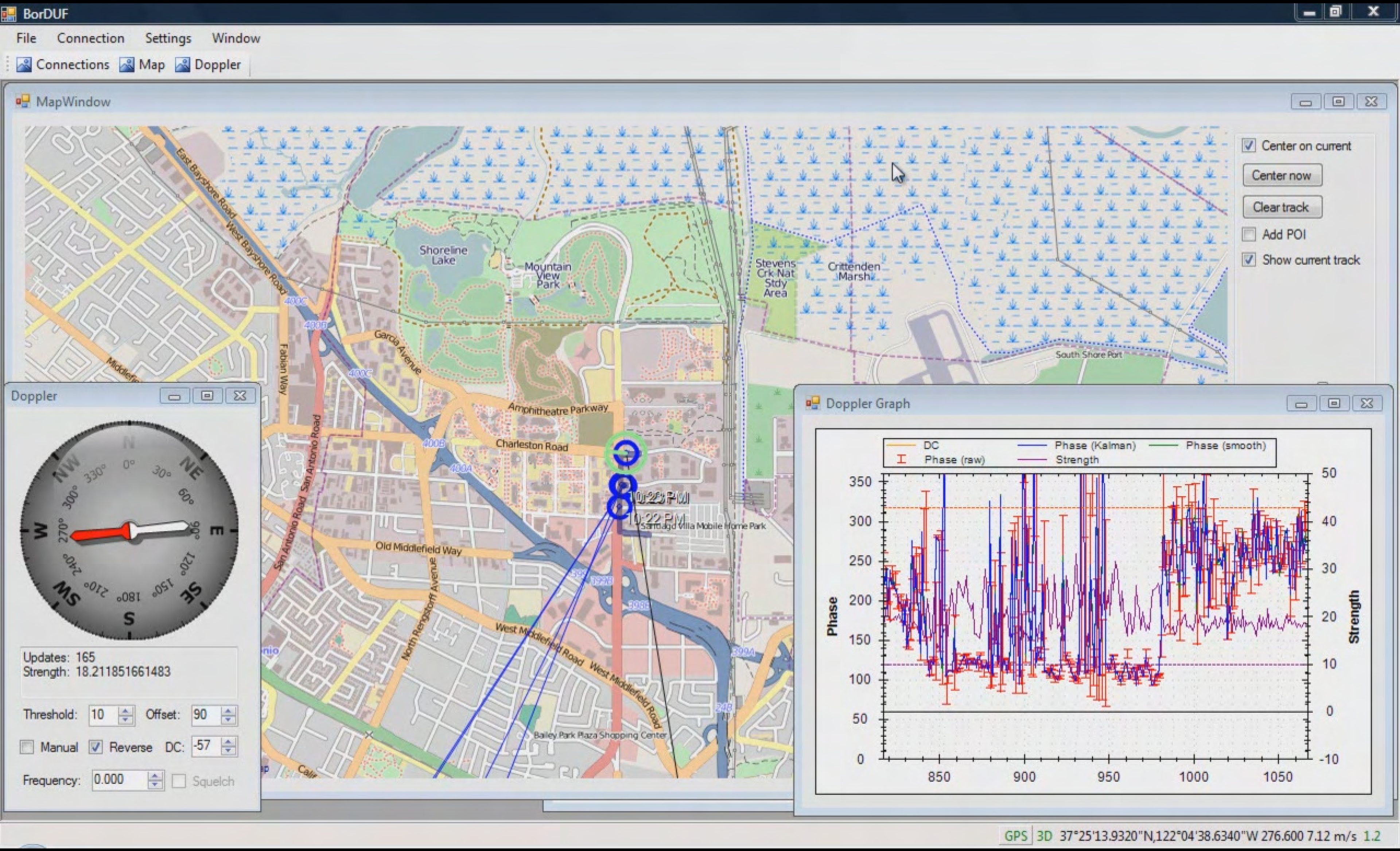
Axis Options

dB/Div:

Ref Level:

Squelched: 1

THIS
COMPANY
HAS WORKED
DAYS
WITHOUT A



BorDUF

☑ Center on current

☐ Add POI

☑ Show current track

Updates: 165
Strength: 18.211851661483

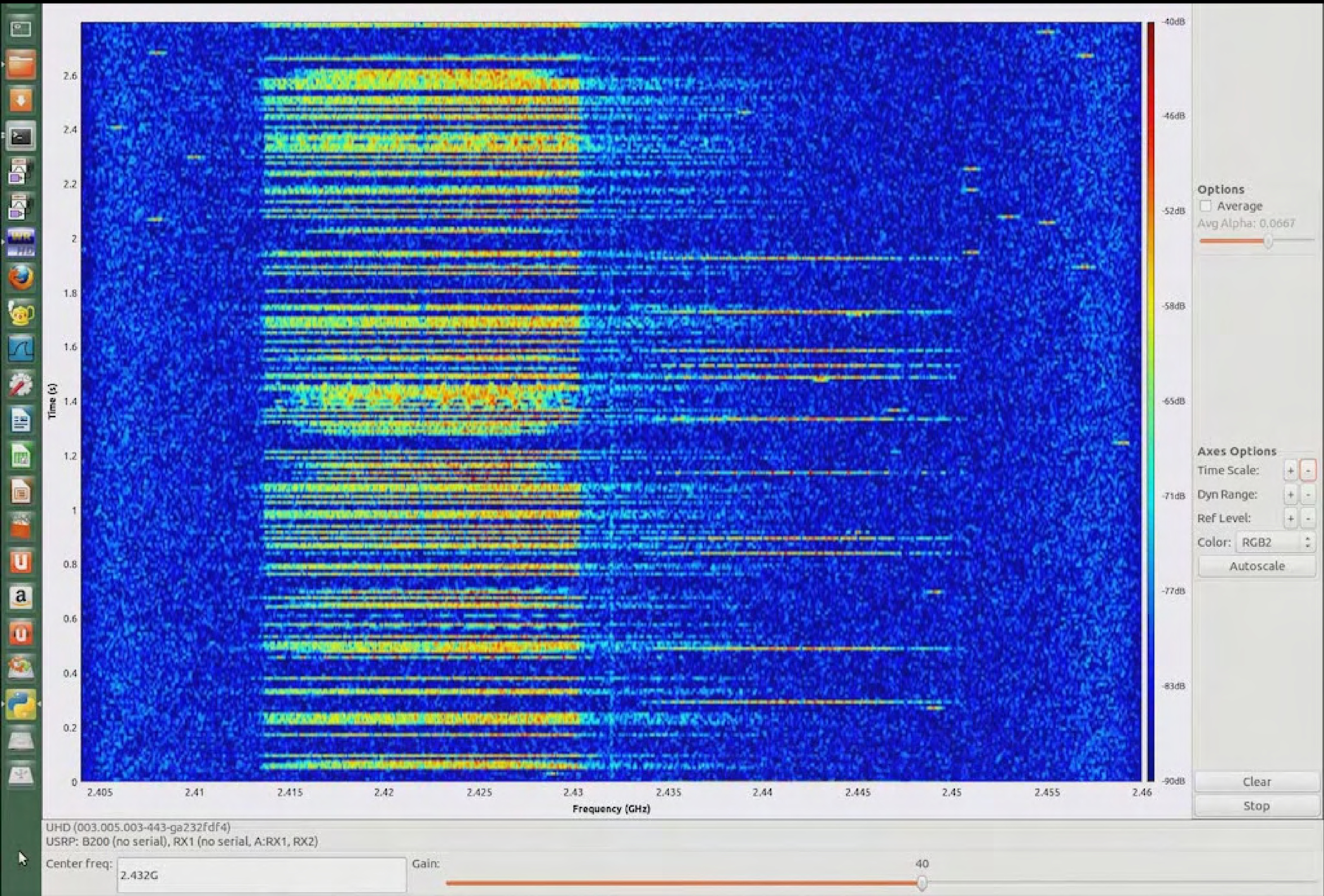
Threshold: 10 Offset: 90

☐ Manual ☑ Reverse DC: -57

Frequency: 0.000 ☐ Squelch

GPS 3D 37°25'13.9320"N,122°04'38.6340"W 276.600 7.12 m/s 1.2

Two WiFi channels, and then some…



UHD (003.005.003-443-ga232fdf4)
USRP: B200 (no serial), RX1 (no serial, A:RX1, RX2)

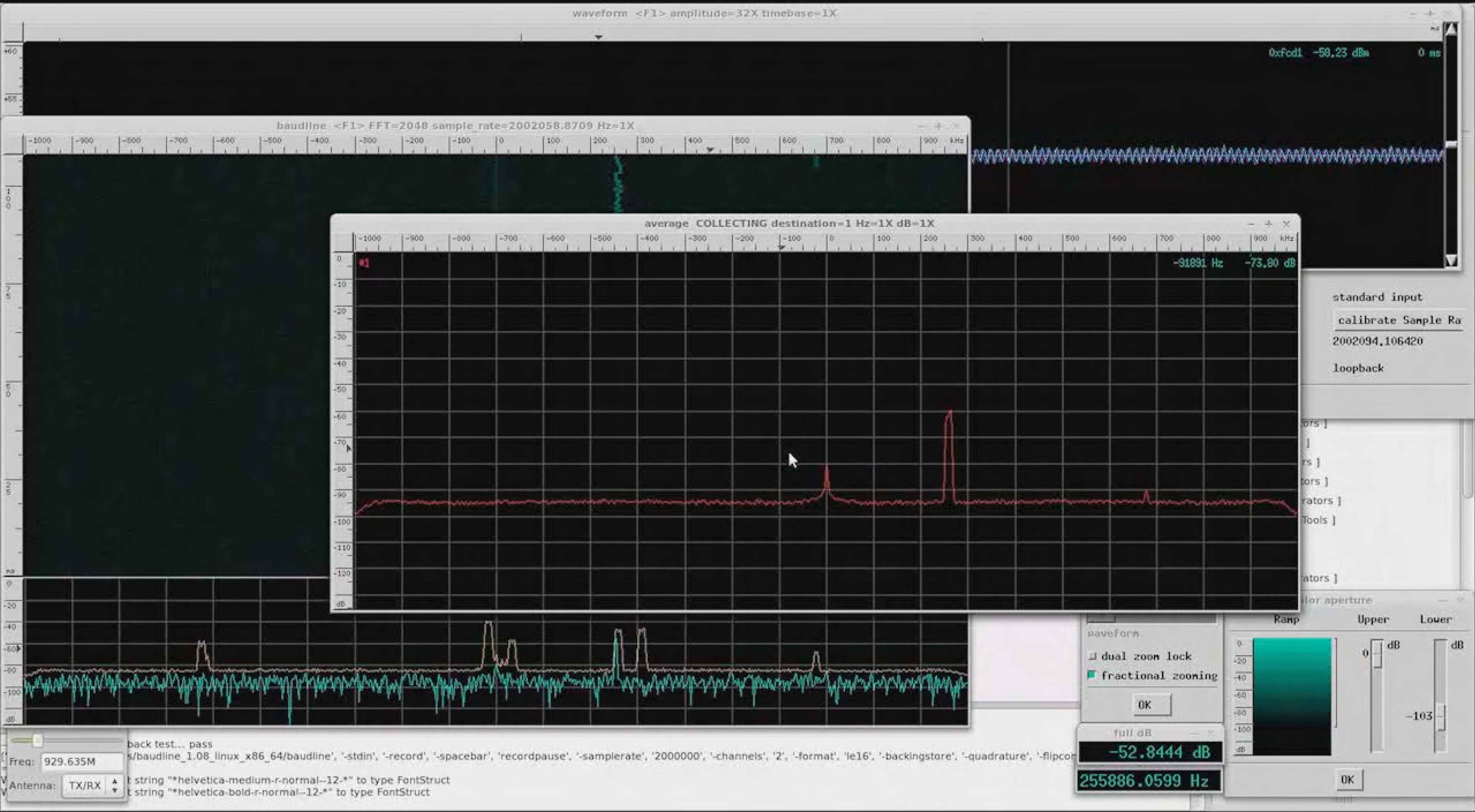
Center freq: 2.432G

Gain: 40

Color: RGB2

□ Average

FLEX Pagers & Baudline


waveform <F1> amplitude=32X timebase=1X
0xfcd1 -58.23 dBm 0 ms
baudline <F1> FFT=2048 sample_rate=2002058.8709 Hz=1X
average COLLECTING destination=1 Hz=1X dB=1X
-1000 -900 -800 -700 -600 -500 -400 -300 -200 -100 0 100 200 300 400 500 600 700 800 900 kHz
0 -10 -20 -30 -40 -50 -60 -70 -80 -90 -100 -110 -120 dB
#1
-91891 Hz -73.80 dB
standard input
calibrate Sample Ra
loopback
waveform
color aperture
Ramp
Upper
Lower
dB
OK
full dB

2002094.106420

□ dual zoom lock

☑ fractional zooming

Upper: 0 dB

Lower: -103 dB

-52.8444 dB

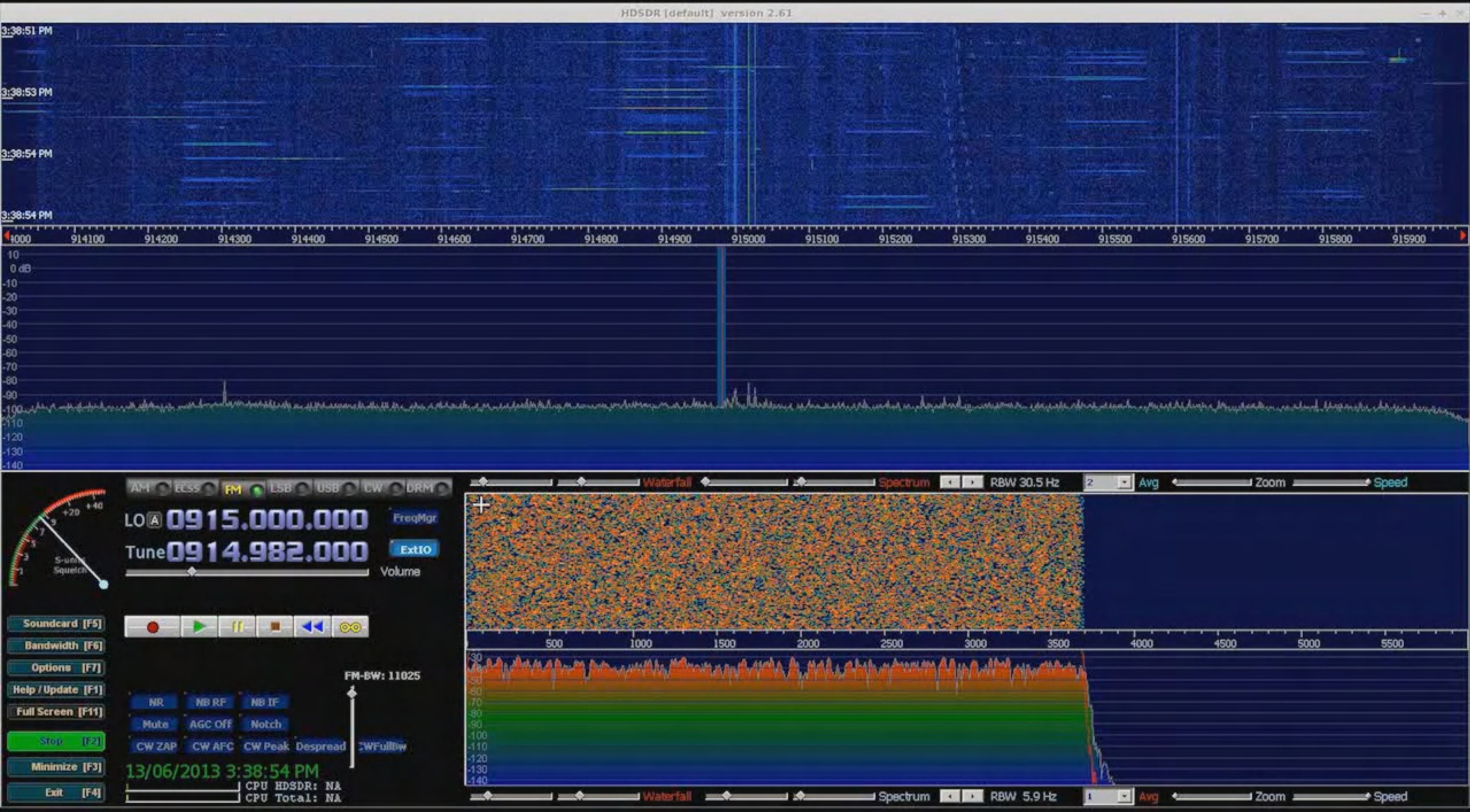
255886.0599 Hz

Freq: 929.635M

Antenna: TX/RX

```
back test... pass
s/baudline_1.08_linux_x86_64/baudline', '-stdin', '-record', '-spacebar', 'recordpause', '-samplerate', '2000000', '-channels', '2', '-format', 'le16', '-backingstore', '-quadrature', '-flipcor
t string "*helvetica-medium-r-normal--12-*" to type FontStruct
t string "*helvetica-bold-r-normal--12-*" to type FontStruct
```

900 MHz ISM – Smart Meters



HDSDR [default] version 2.61

LO 0915.000.000

Tune 0914.982.000

RBW 30.5 Hz

RBW 5.9 Hz

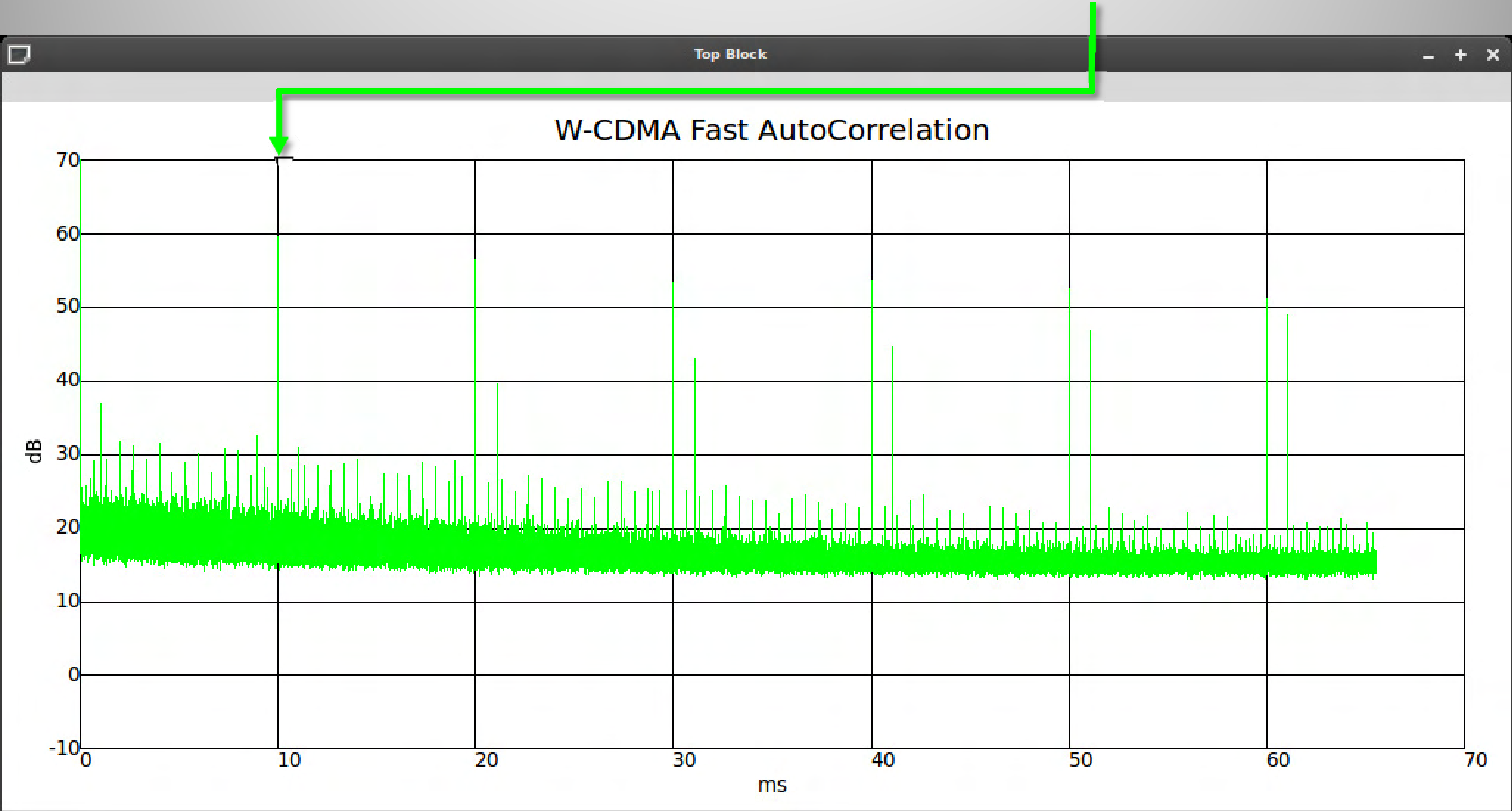
FM-BW: 11025

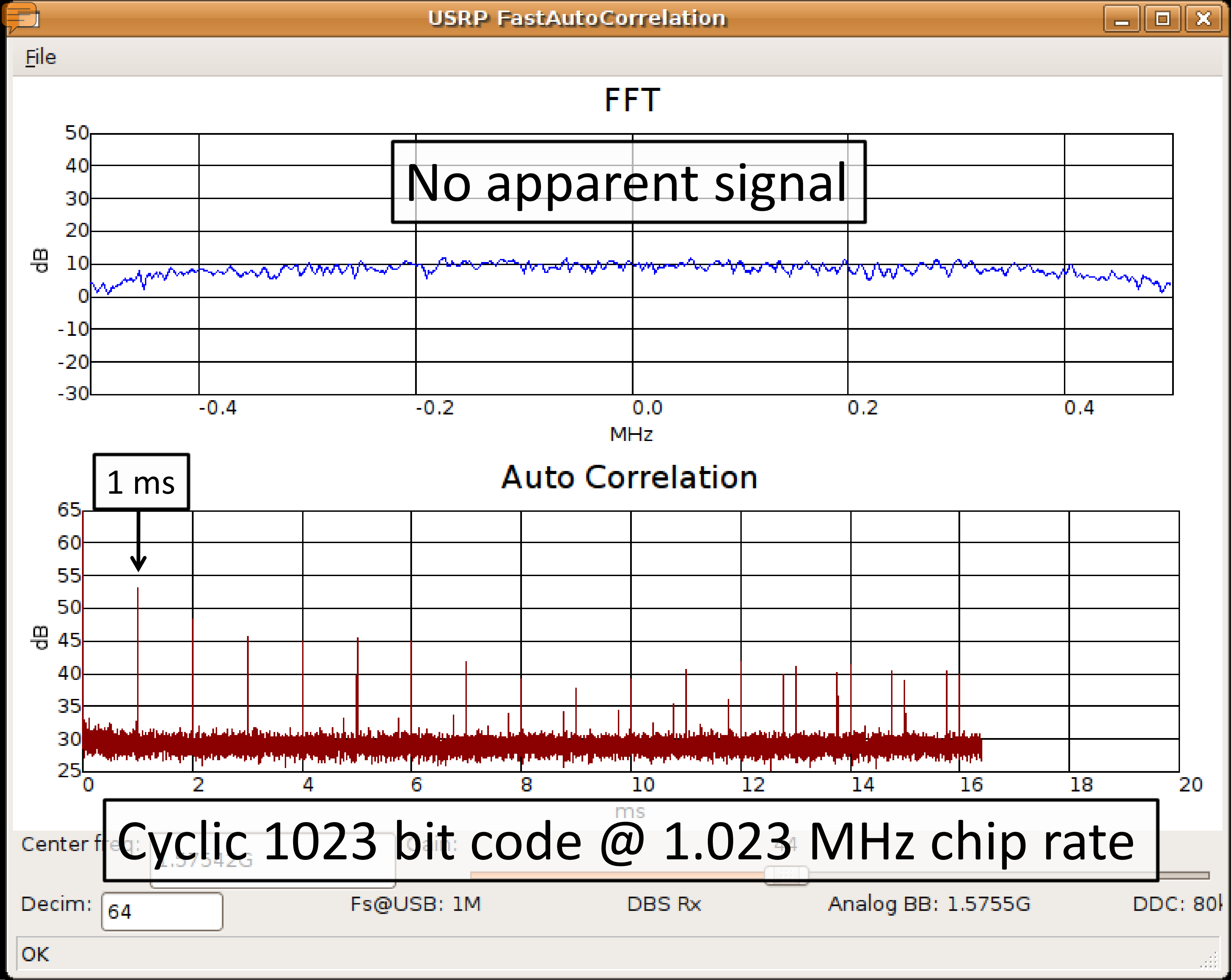
13/06/2013 3:38:54 PM

CPU HDSDR: NA
CPU Total: NA

3G W-CDMA

Signature of UMTS: repeating data in CPICH at 10 ms intervals





No apparent signal

1 ms

Cyclic 1023 bit code @ 1.023 MHz chip rate

Center freq: 1.57542G

Gain: 44

Decim: 64

Fs@USB: 1M

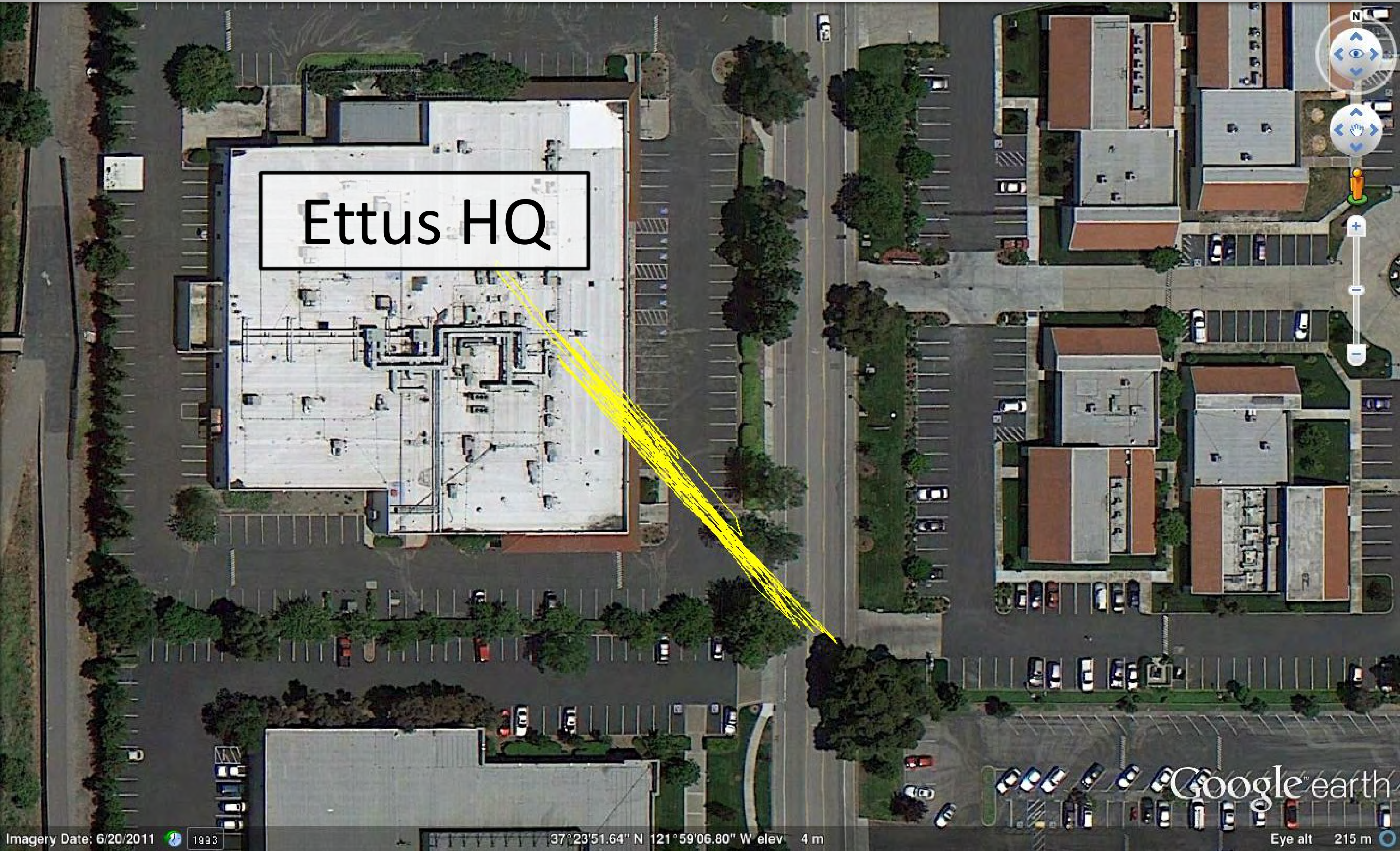
DBS Rx

Analog BB: 1.5755G

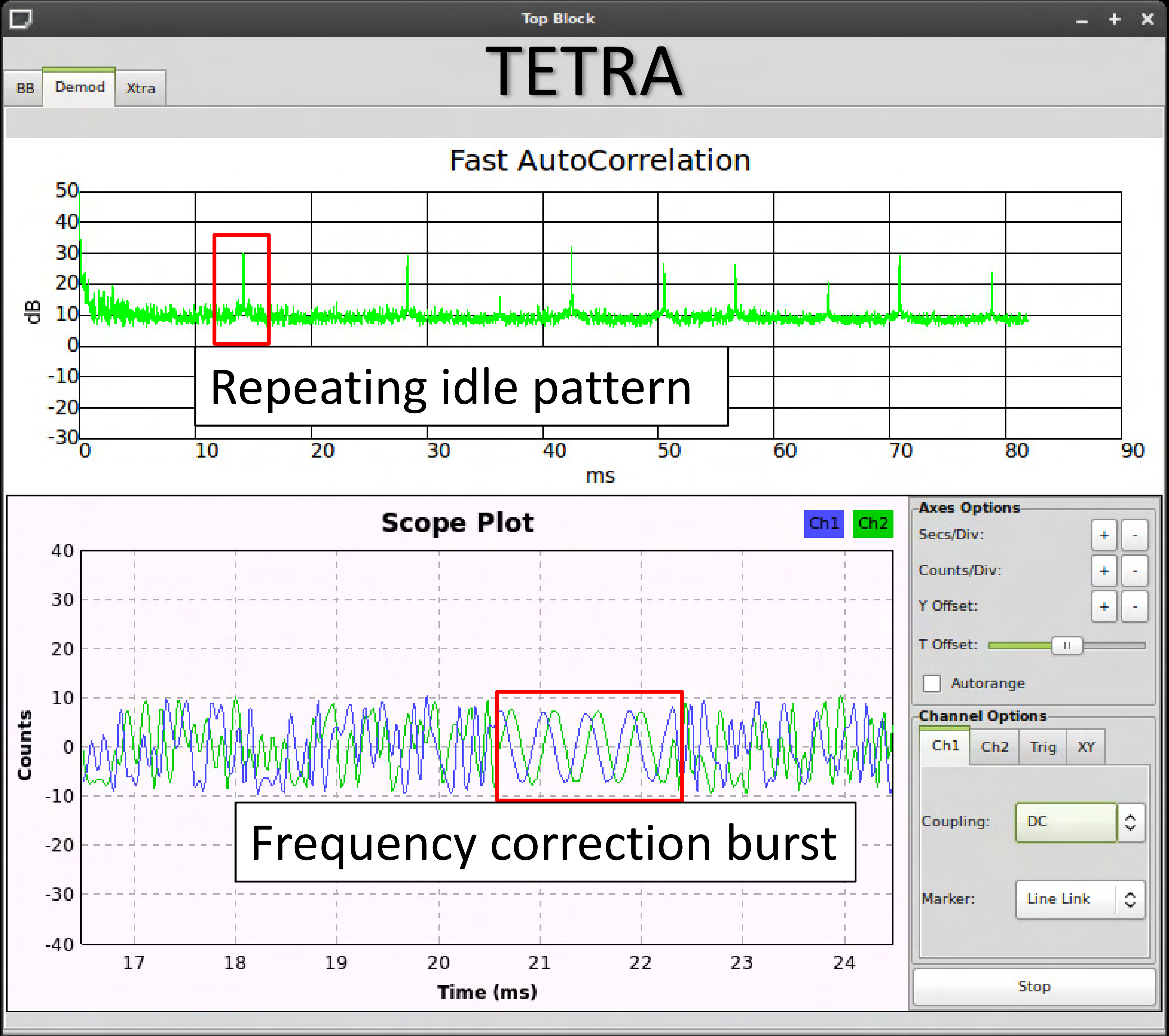
DDC: 80k

OK

gnss-sdr: Decoding L1



TETRA



Repeating idle pattern

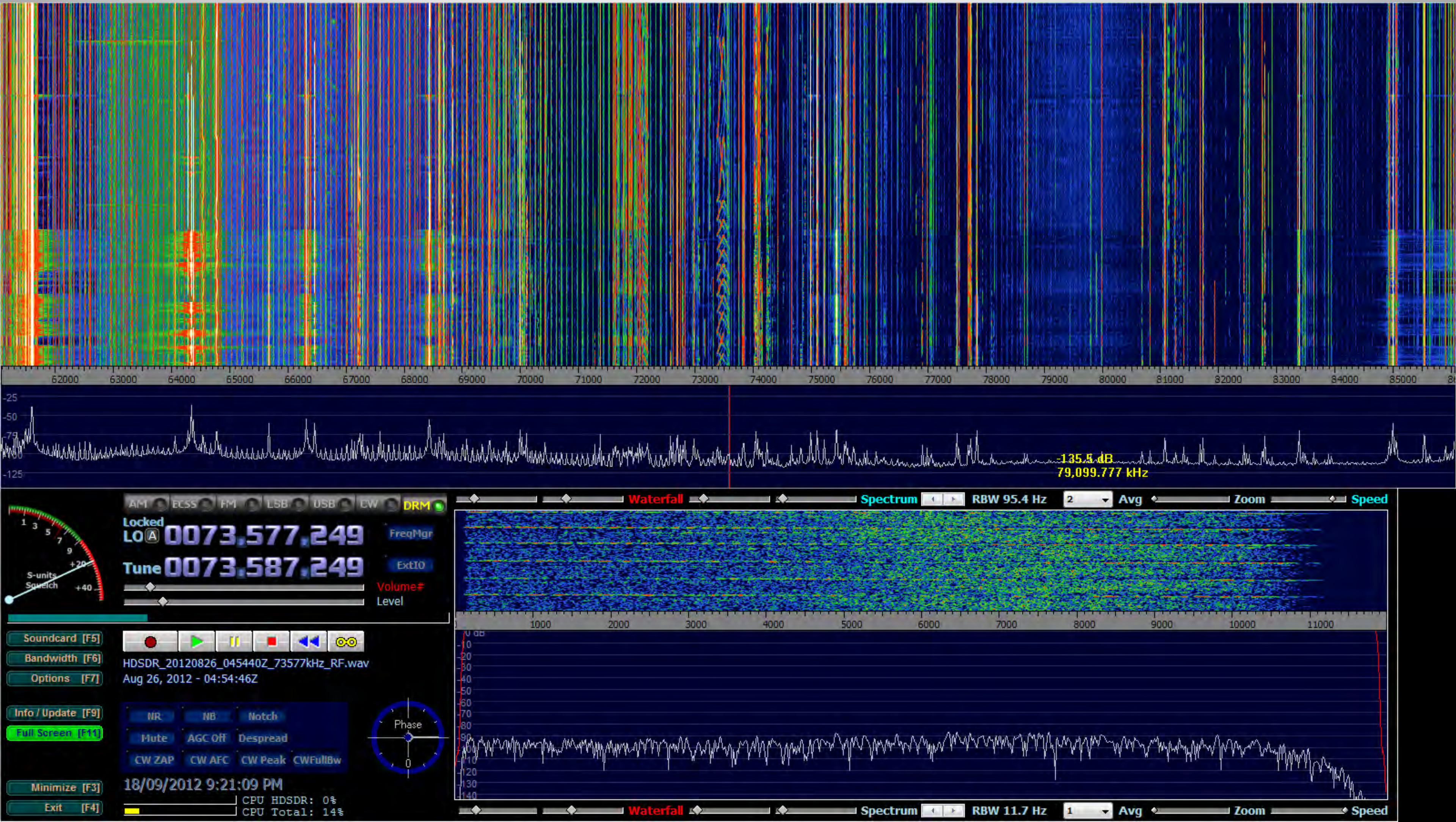
Frequency correction burst

□ Autorange

Coupling: DC

Marker: Line Link

The Entire HAM Band



Locked
LO A 0073.577.249
Tune 0073.587.249

HDSDR_20120826_045440Z_73577kHz_RF.wav
Aug 26, 2012 - 04:54:46Z

18/09/2012 9:21:09 PM

```
CPU HDSDR: 0%
CPU Total: 14%
```

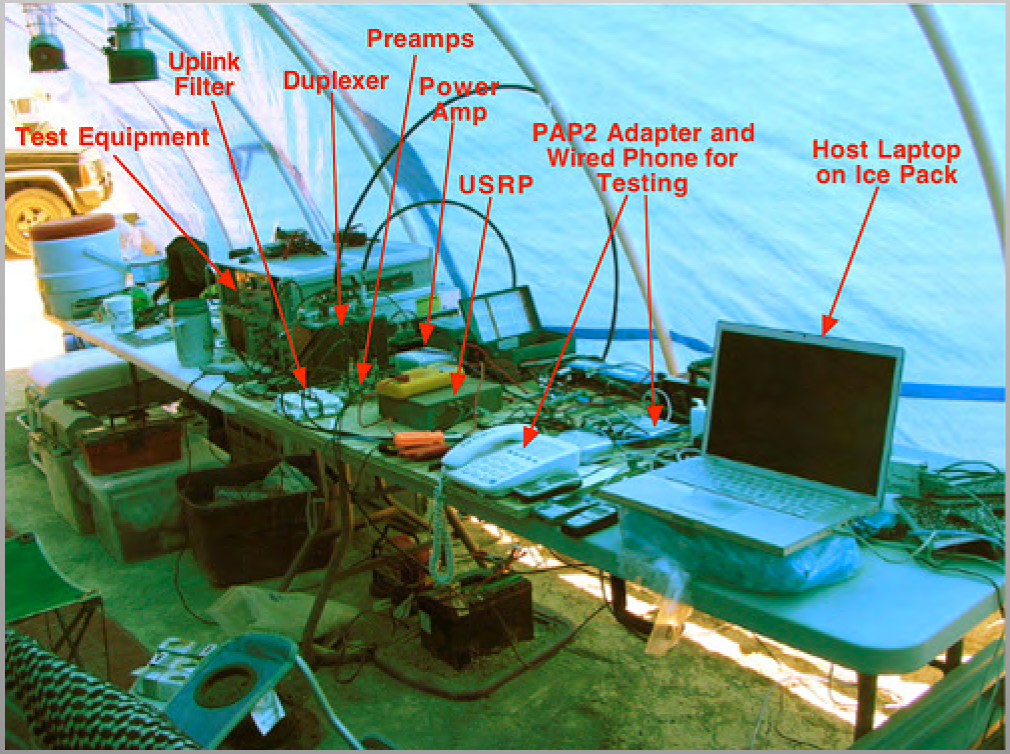
-135.5 dB
79,099.777 kHz

RBW 95.4 Hz 2 Avg

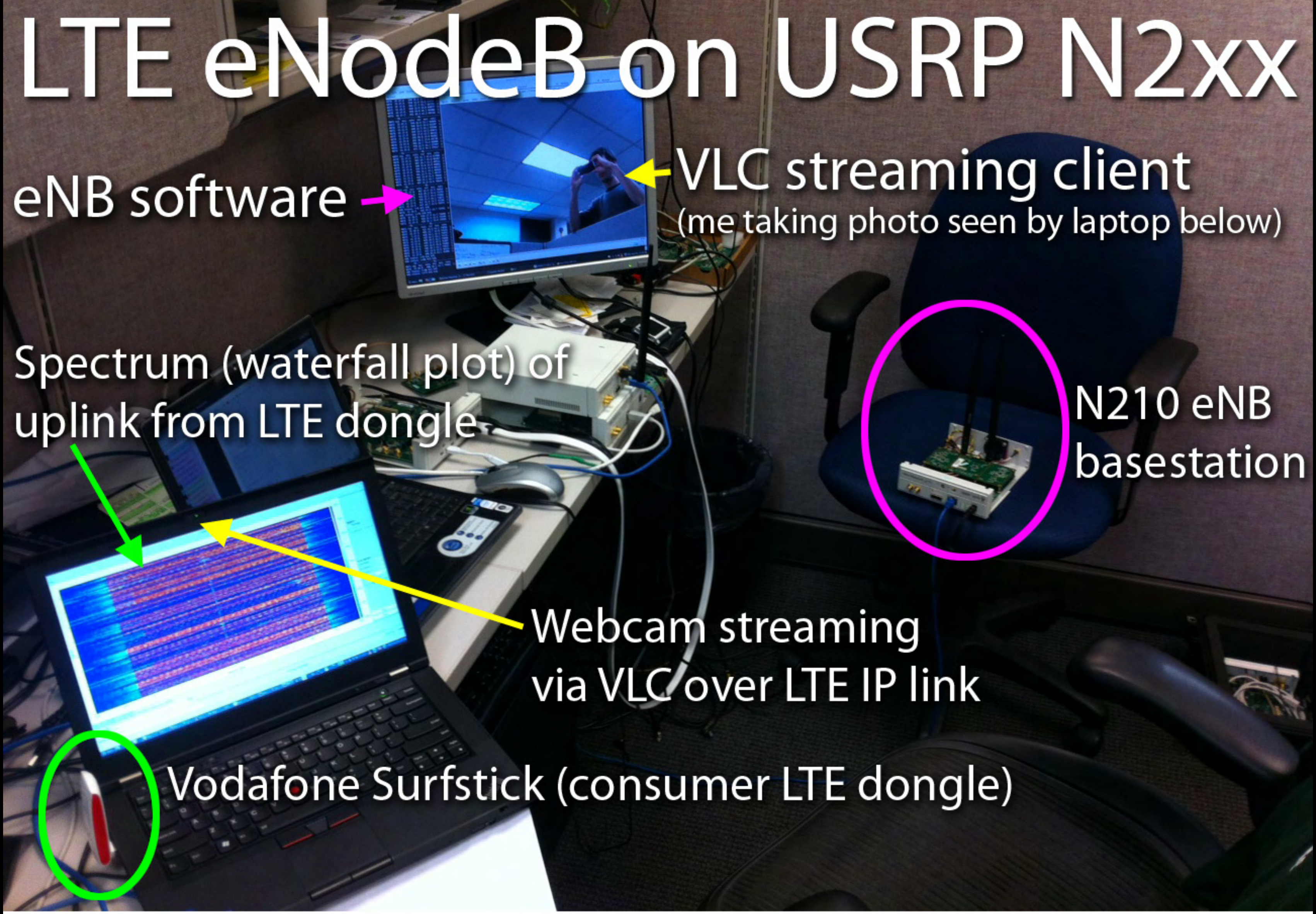
RBW 11.7 Hz 1 Avg

OpenBTS

- Open-source 2G GSM stack
  - Asterix softswitch (PBX)
  - VoIP backhaul



LTE eNodeB on USRP N2xx



eNB software

VLC streaming client
(me taking photo seen by laptop below)

Spectrum (waterfall plot) of uplink from LTE dongle

N210 eNB basestation

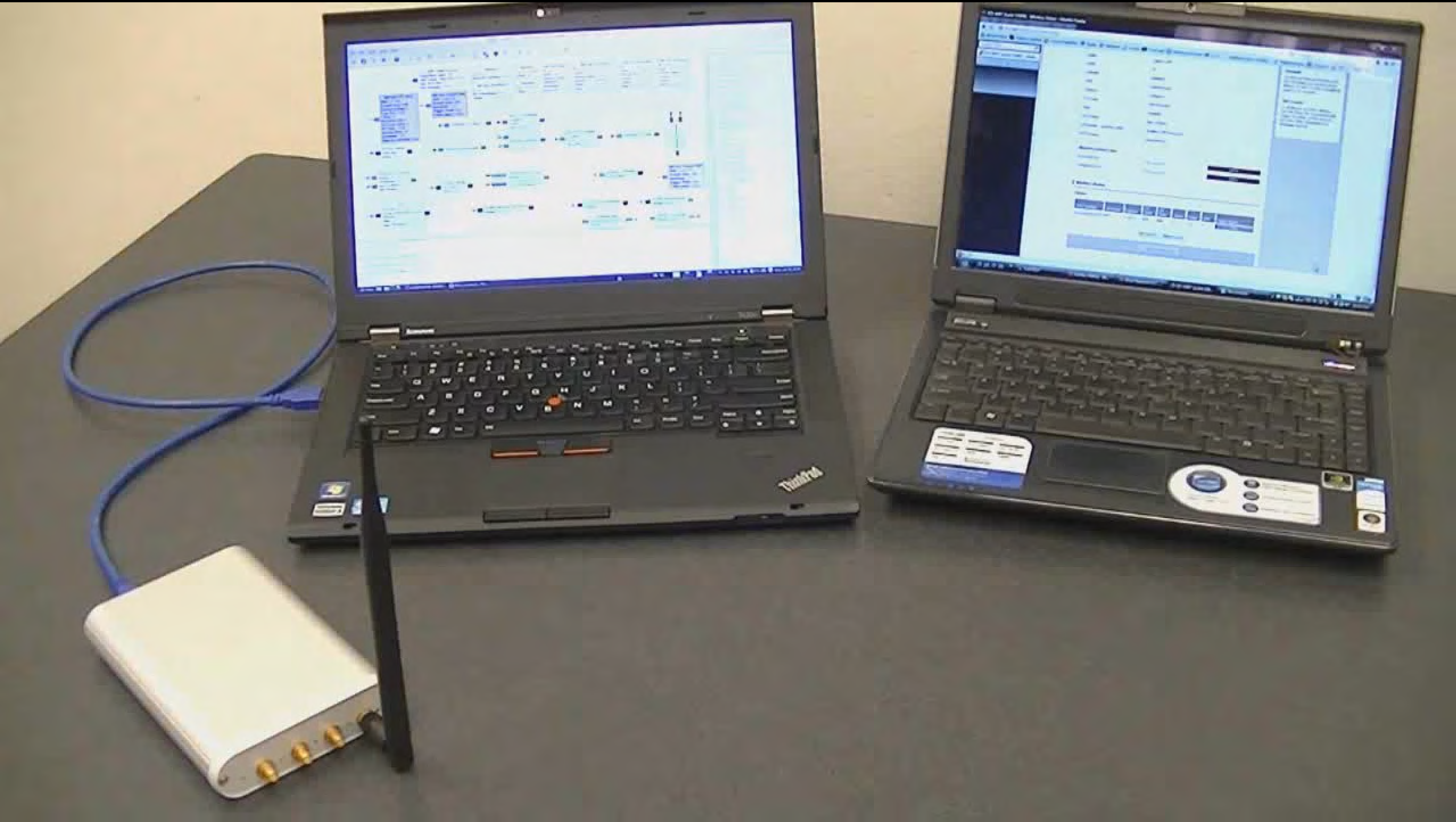
Webcam streaming via VLC over LTE IP link

Vodafone Surfstick (consumer LTE dongle)

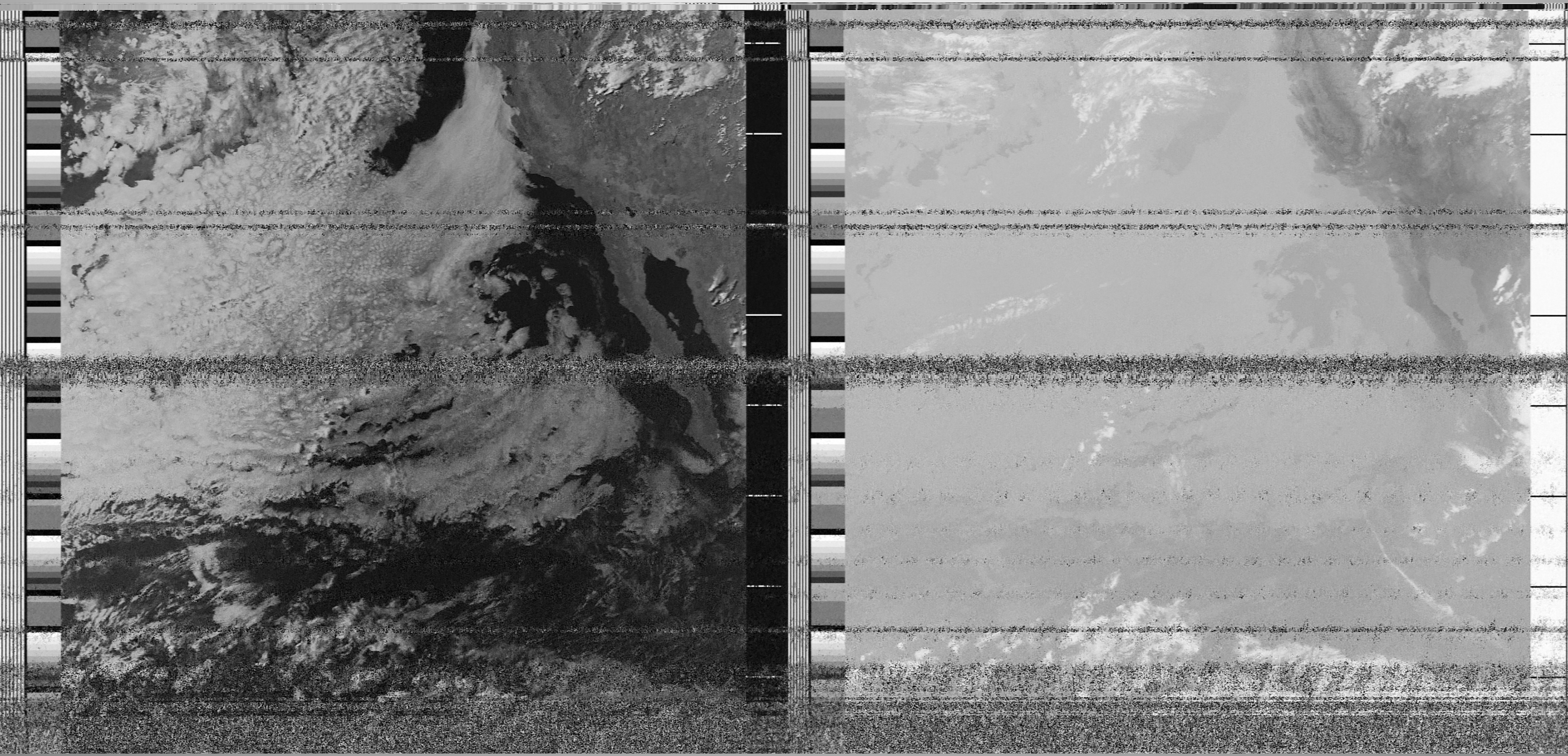
amarisoft

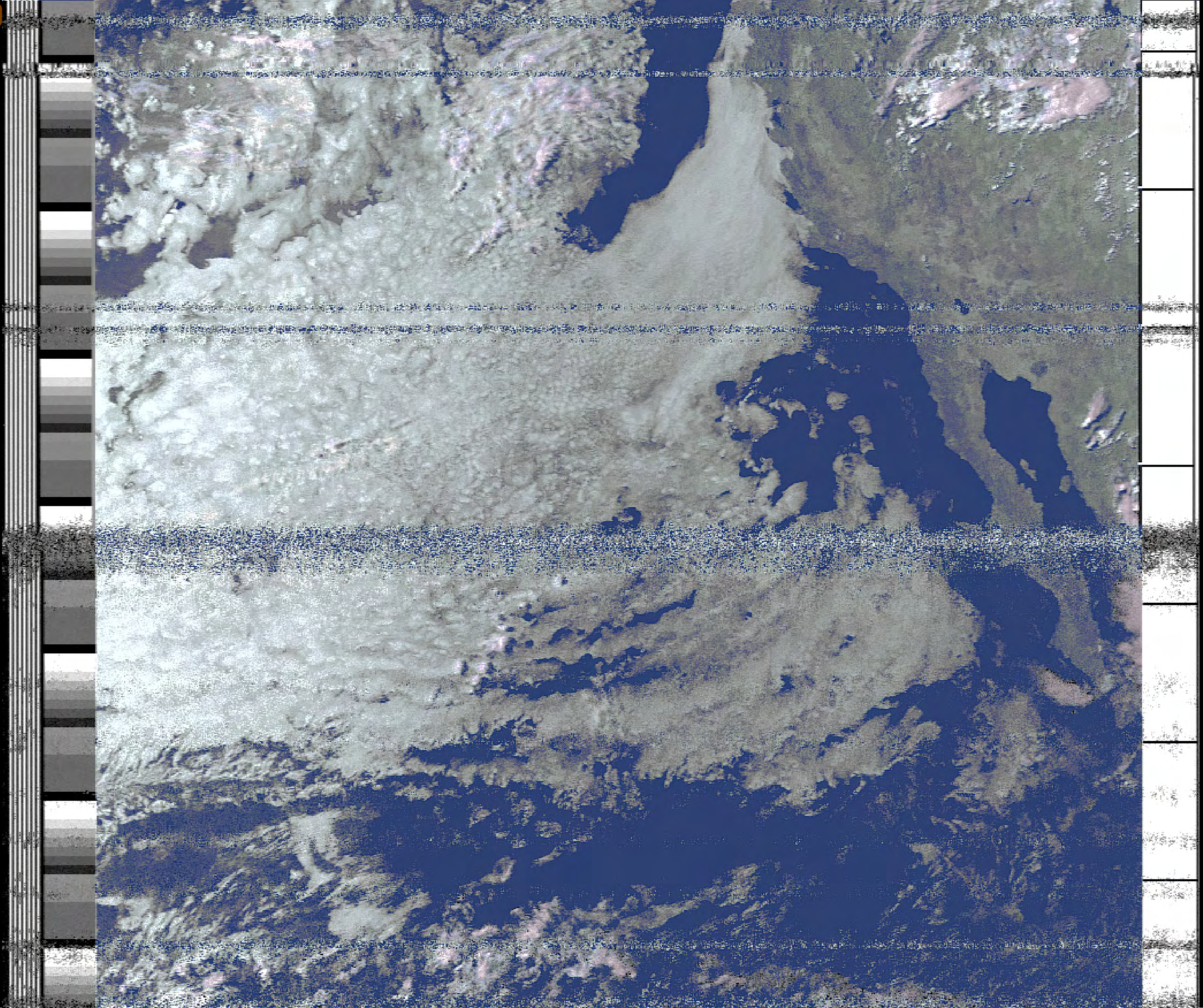
Ettus Research

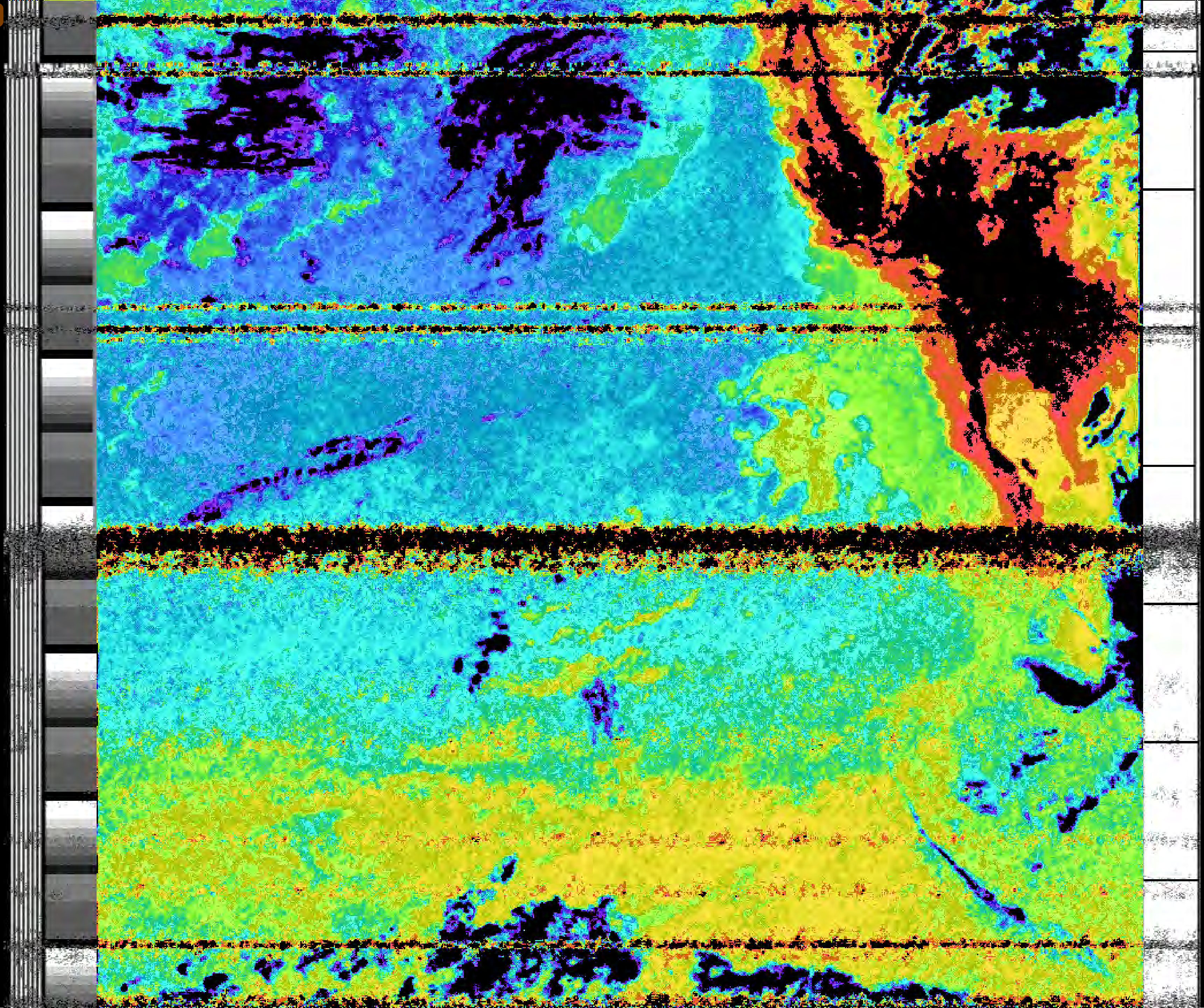
802.11agp (OFDM) Decoding



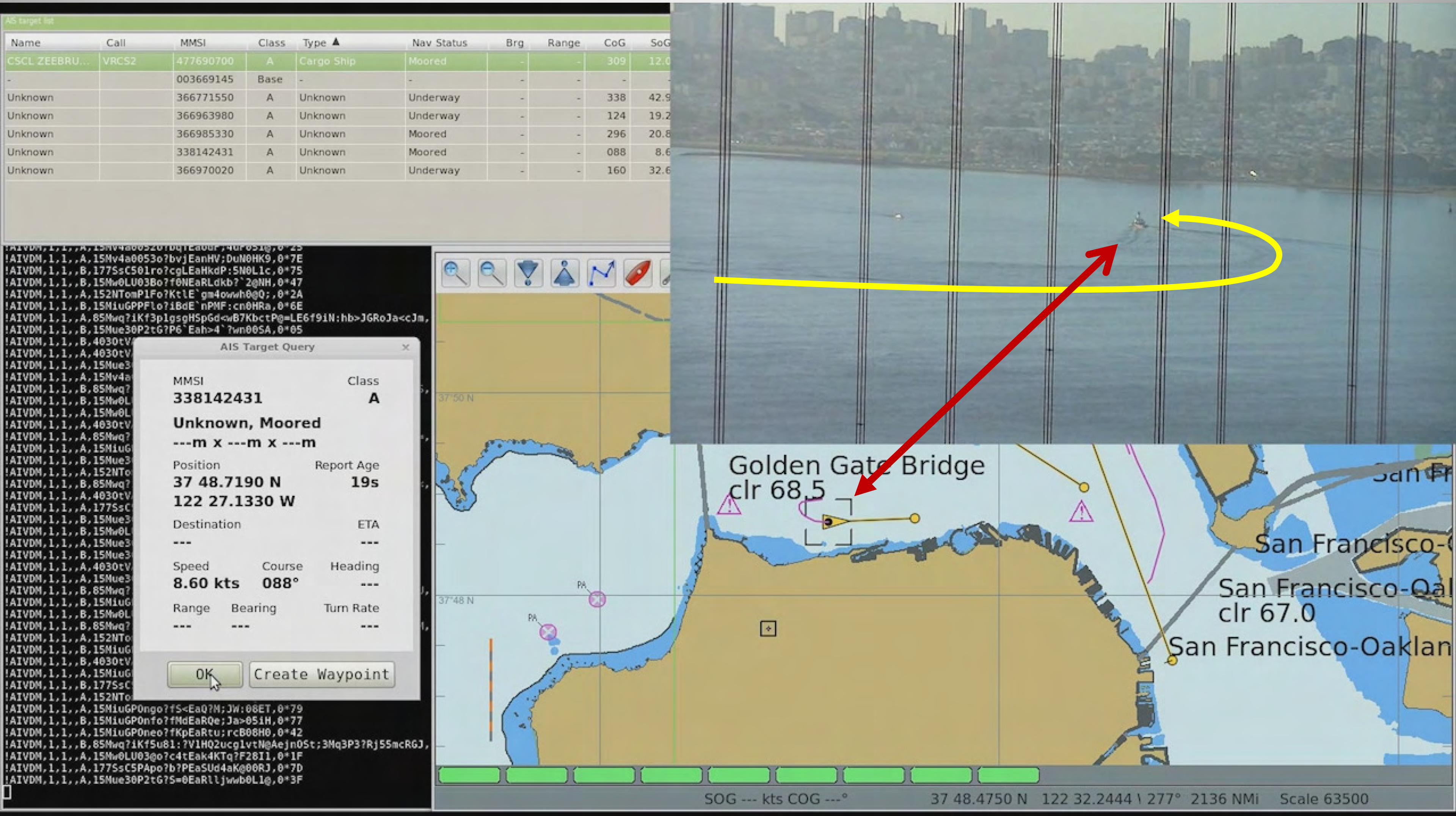
Automatic **P**icture **T**ransmission







Automatic Identification System



AIS target list

Name	Call	MMSI	Class	Type ▲	Nav Status	Brg	Range	CoG	SoG
CSCL ZEEBRU...	VRCS2	477690700	A	Cargo Ship	Moored	-	-	309	12.0
-		003669145	Base	-	-	-	-	-	-
Unknown		366771550	A	Unknown	Underway	-	-	338	42.9
Unknown		366963980	A	Unknown	Underway	-	-	124	19.2
Unknown		366985330	A	Unknown	Moored	-	-	296	20.8
Unknown		338142431	A	Unknown	Moored	-	-	088	8.6
Unknown		366970020	A	Unknown	Underway	-	-	160	32.6

```
!AIVDM,1,1,,A,15Mv4a0053o?bvjEanHV;DuN0HK9,0*7E
!AIVDM,1,1,,B,177SsC501ro?cgLEaHkdP:5N0L1c,0*75
!AIVDM,1,1,,B,15Mw0LU03Bo?f0NEaRLdkb?`2@NH,0*47
!AIVDM,1,1,,A,152NTomP1Fo?KtlE`gm4owwh0@Q;,0*2A
!AIVDM,1,1,,B,15MiuGPPFlo?iBdE`nPMF:cn0HRa,0*6E
!AIVDM,1,1,,A,85Mwq?iKf3plgsgHSpGd<wB7KbctP@=LE6f91N:hb>JGRoJa<cJm,
!AIVDM,1,1,,B,15Mue30P2tG?P6`Eah>4`?wn00SA,0*05
!AIVDM,1,1,,B,4030tV
!AIVDM,1,1,,A,4030tV
!AIVDM,1,1,,A,15Mue3
!AIVDM,1,1,,A,15Mv4a
!AIVDM,1,1,,B,85Mwq?
!AIVDM,1,1,,B,15Mw0L
!AIVDM,1,1,,A,15Mw0L
!AIVDM,1,1,,A,4030tV
!AIVDM,1,1,,A,85Mwq?
!AIVDM,1,1,,A,15MiuG
!AIVDM,1,1,,B,15Mue3
!AIVDM,1,1,,A,152NTo
!AIVDM,1,1,,B,85Mwq?
!AIVDM,1,1,,A,4030tV
!AIVDM,1,1,,A,177SsC
!AIVDM,1,1,,B,15Mue3
!AIVDM,1,1,,B,15Mw0L
!AIVDM,1,1,,A,15Mue3
!AIVDM,1,1,,B,15Mue3
!AIVDM,1,1,,A,4030tV
!AIVDM,1,1,,A,15Mue3
!AIVDM,1,1,,B,85Mwq?
!AIVDM,1,1,,B,15MiuG
!AIVDM,1,1,,B,15Mw0L
!AIVDM,1,1,,B,85Mwq?
!AIVDM,1,1,,A,152NTo
!AIVDM,1,1,,B,15MiuG
!AIVDM,1,1,,B,4030tV
!AIVDM,1,1,,A,15MiuG
!AIVDM,1,1,,B,177SsC
!AIVDM,1,1,,A,152NTo
!AIVDM,1,1,,A,15MiuGP0ngo?fS<EaQ?M;JW:08ET,0*79
!AIVDM,1,1,,B,15MiuGP0nfo?fMdEaRQe;Ja>05iH,0*77
!AIVDM,1,1,,A,15MiuGP0neo?fKpEaRtu;rcB08H0,0*42
!AIVDM,1,1,,B,85Mwq?iKf5u81:?V1HQ2ucglvtN@AejnOSt;3Mq3P3?Rj55mcRGJ,
!AIVDM,1,1,,A,15Mw0LU03@o?c4tEak4KTq?F28I1,0*1F
!AIVDM,1,1,,A,177SsC5PApo?b?PEaSUd4aK@00RJ,0*7D
!AIVDM,1,1,,A,15Mue30P2tG?S=0EaRlljwwb0L1@,0*3F
```

AIS Target Query

MMSI **338142431**	Class **A**

Unknown, Moored

---m x ---m x ---m

Position	Report Age
37 48.7190 N **122 27.1330 W**	**19s**

Destination	ETA
---	---

Speed	Course	Heading
8.60 kts	**088°**	---

Range	Bearing	Turn Rate
---	---	---

SOG --- kts COG ---°   37 48.4750 N   122 32.2444 \ 277°   2136 NMi   Scale 63500

23

SPORT
IANTS