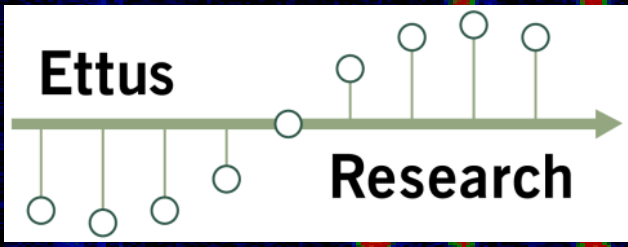
Notes and links in PDF comments on each slide

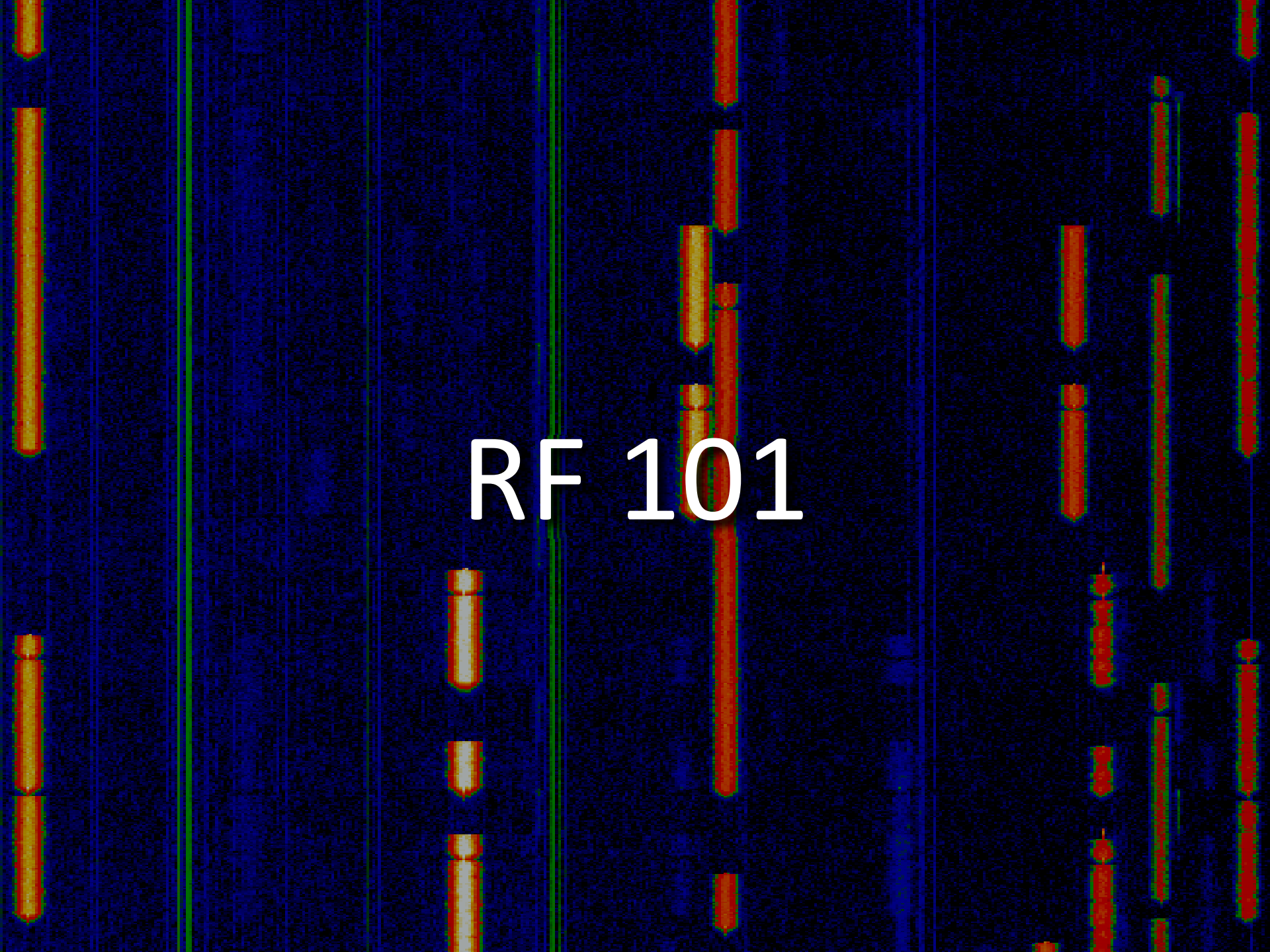
Hacking the Wireless World with Software Defined Radio – 2.0

Balint Seeber
Applications Specialist & SDR Evangelist
balint@ettus.com
balint@spench.net @spenchdotnet



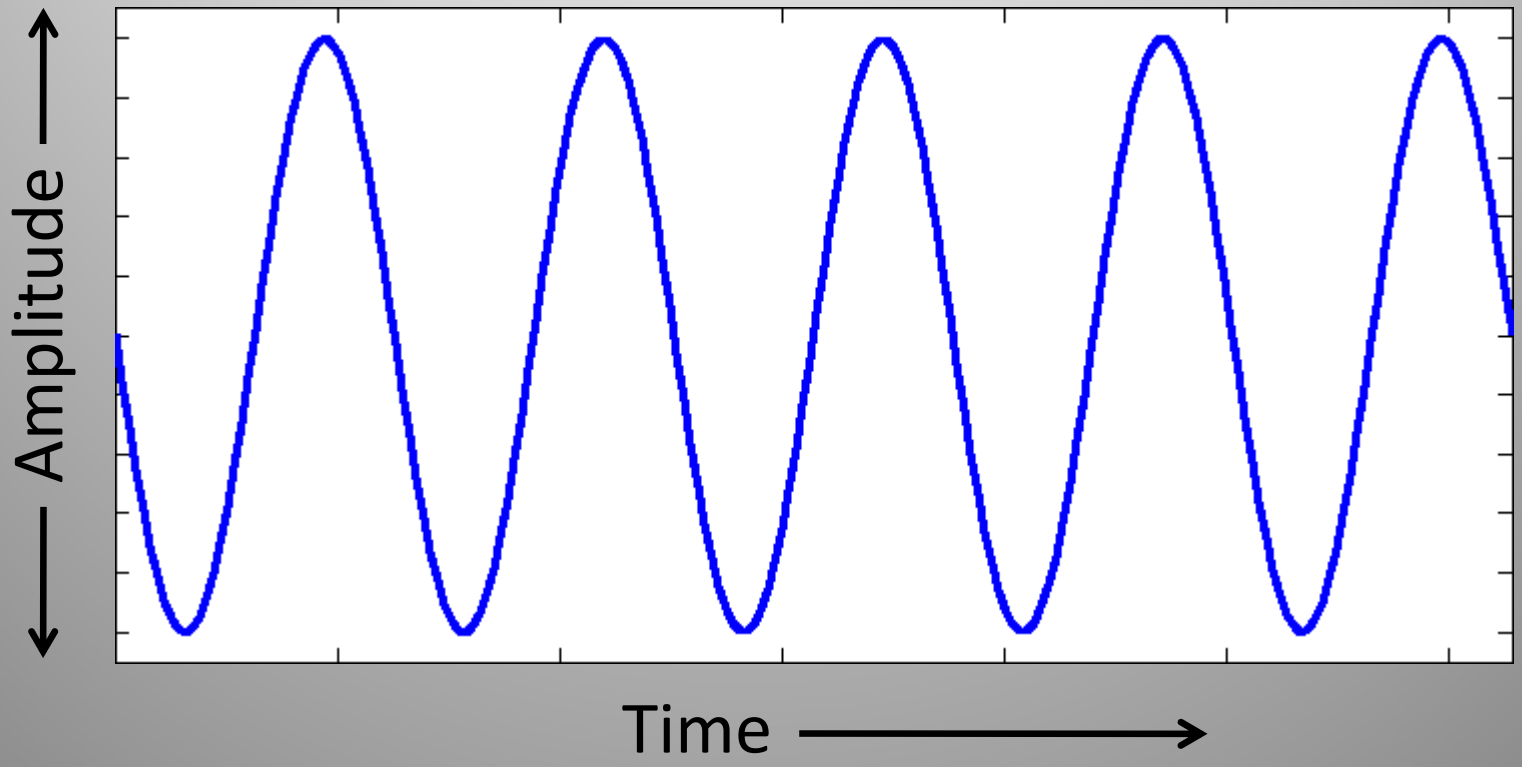
Overview

- RF 101
- Aviation RADAR
  - Secondary Surveillance RADAR
  - Primary Surveillance RADAR
- Pagers
- RDS TMC
- FasTrak
- Blind Signal Analysis
- Direction Finding


RF 101

Transmitting Data

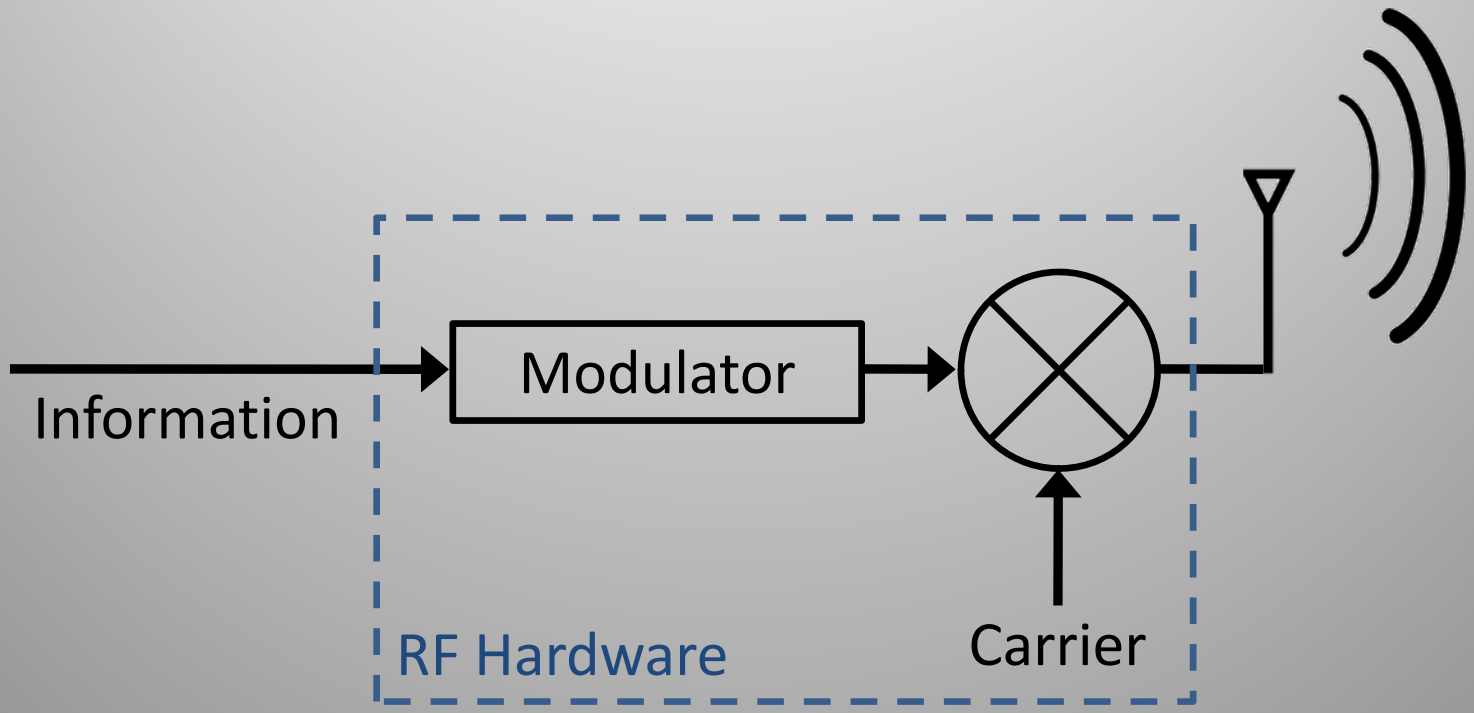
- Radio (carrier) wave must be modulated to convey information



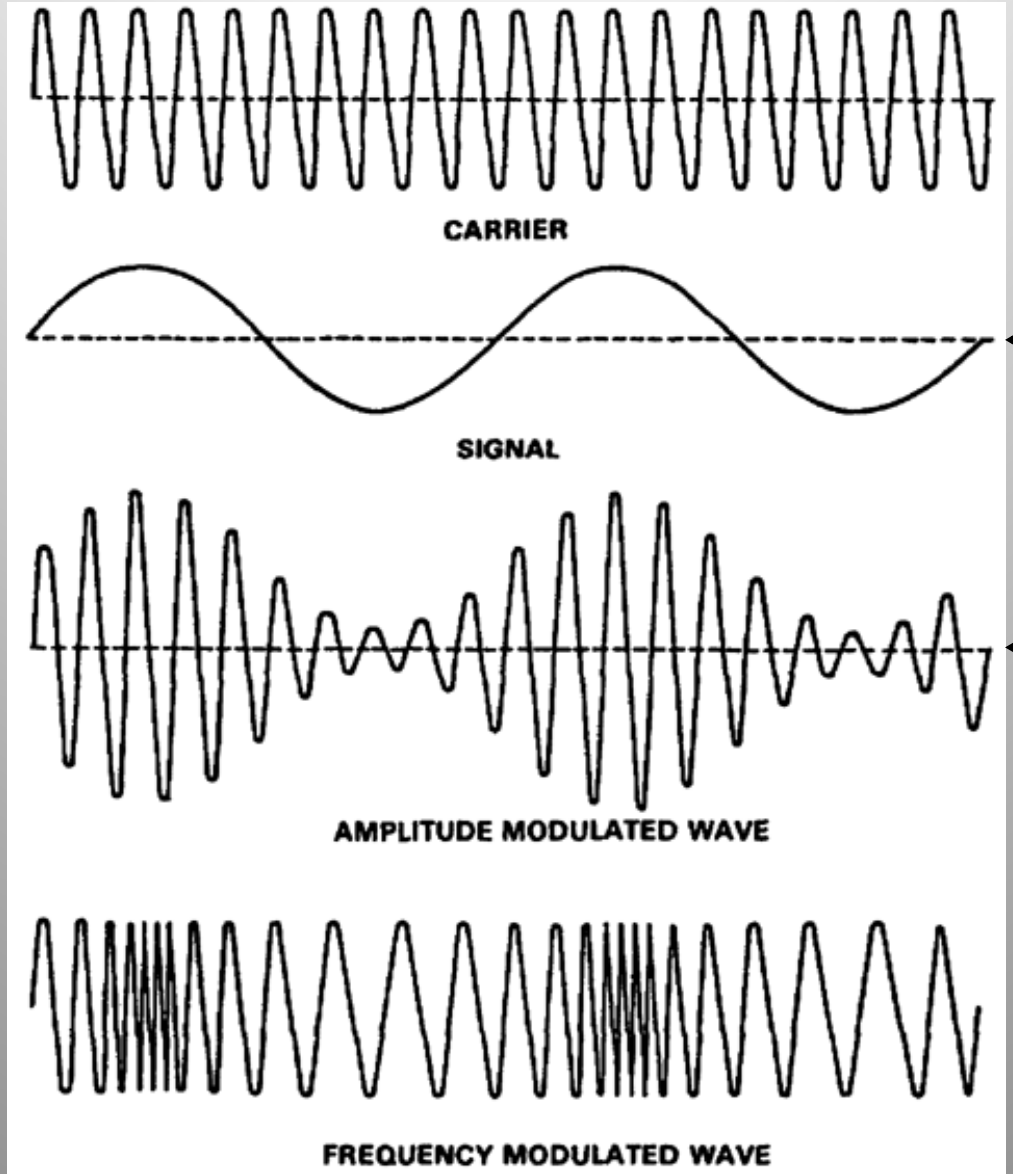
Transmitting Data

- Radio (carrier) wave must be modulated to convey information
- OOK (**O**n-**O**ff **K**eying)
  - Presence/absence of a signal
- COFDM (**C**oded **O**rthogonal **F**requency-**D**ivision **M**ultiplexing)
  - WiFi, DVB, DAB, WiMAX, UWB, 4G, ADSL, PLC

Transmitting Data



AM & FM: In the Time Domain

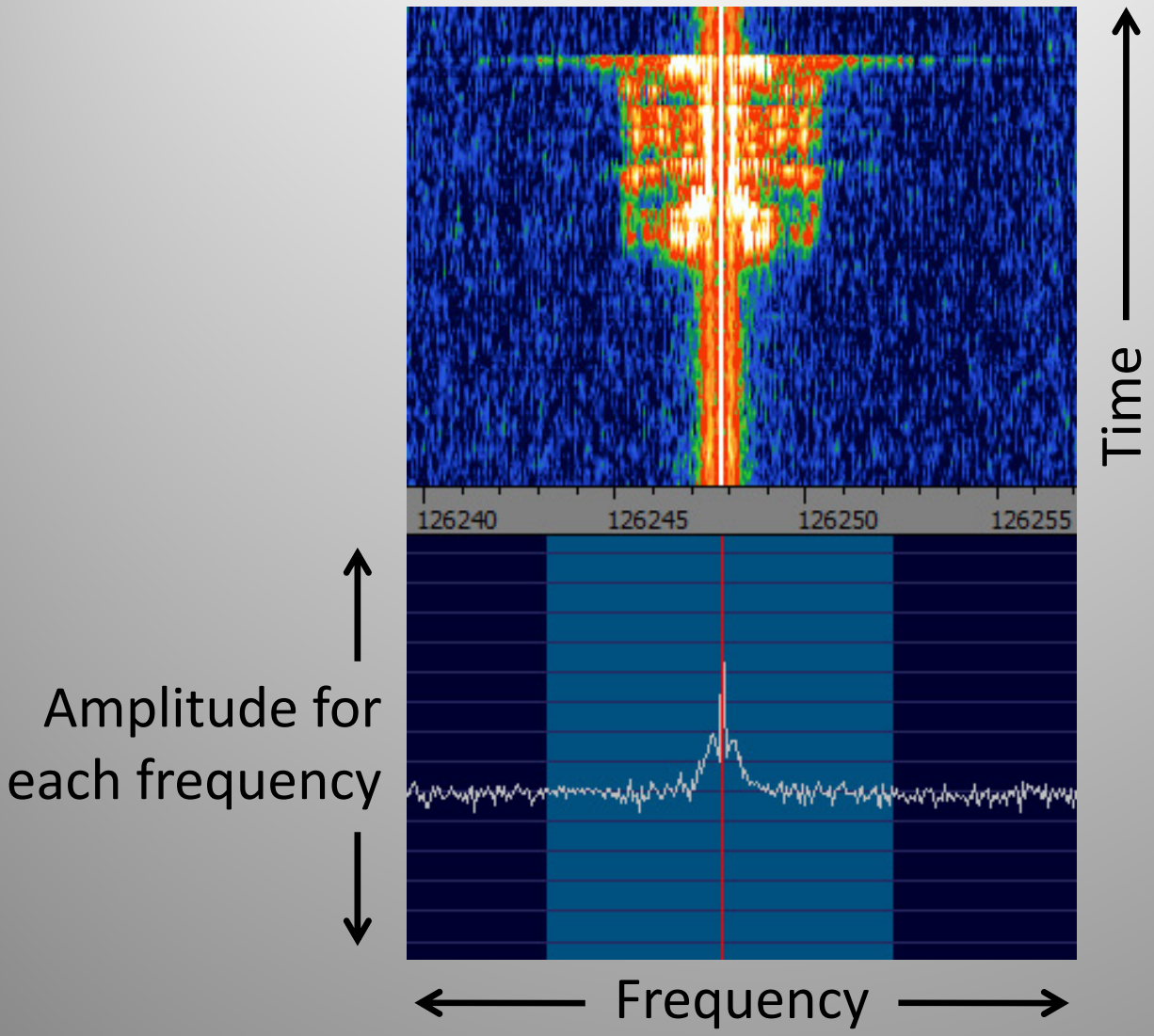


Analog or digital information

Constant amplitude

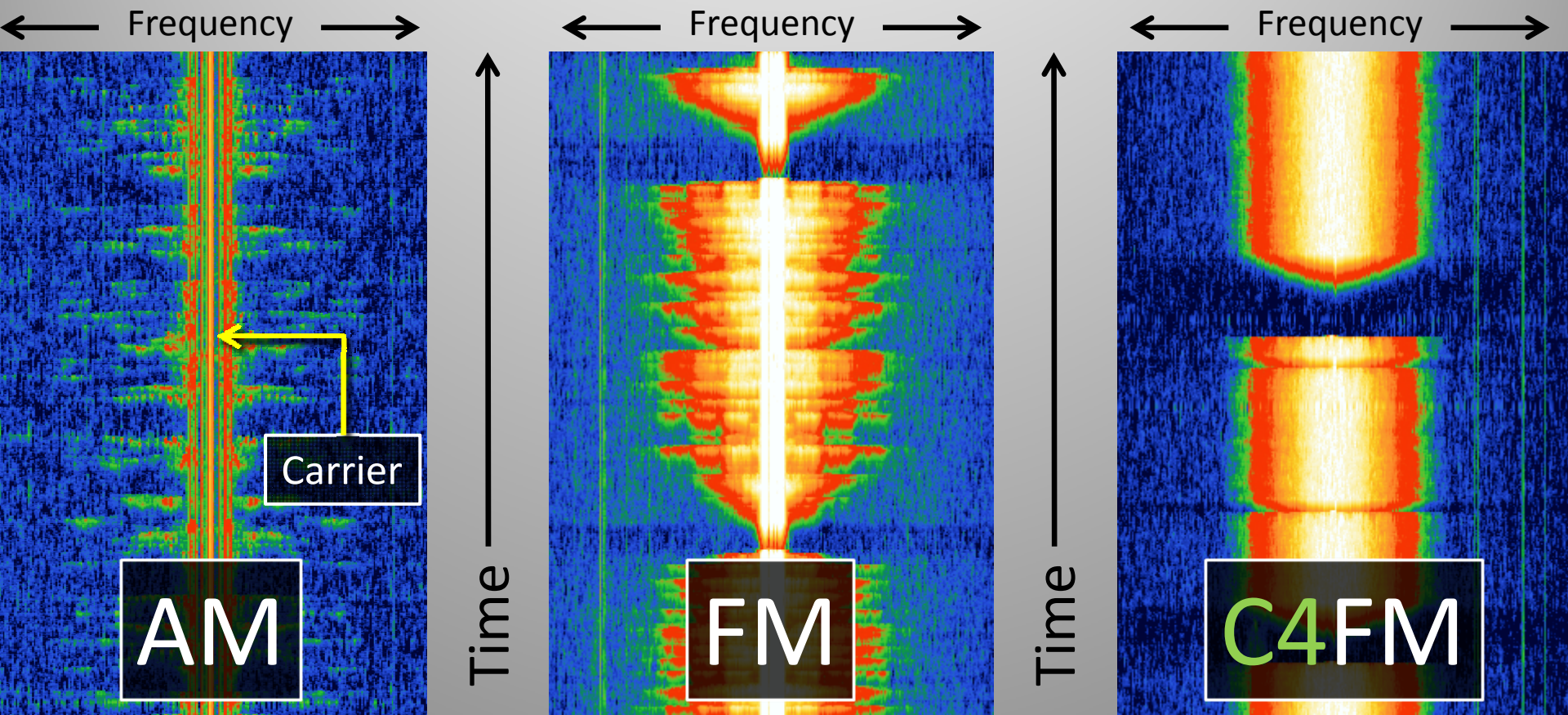
Constant frequency

In the Frequency Domain



Modulation

- Modulation technique defines how the signal will look on the spectrum

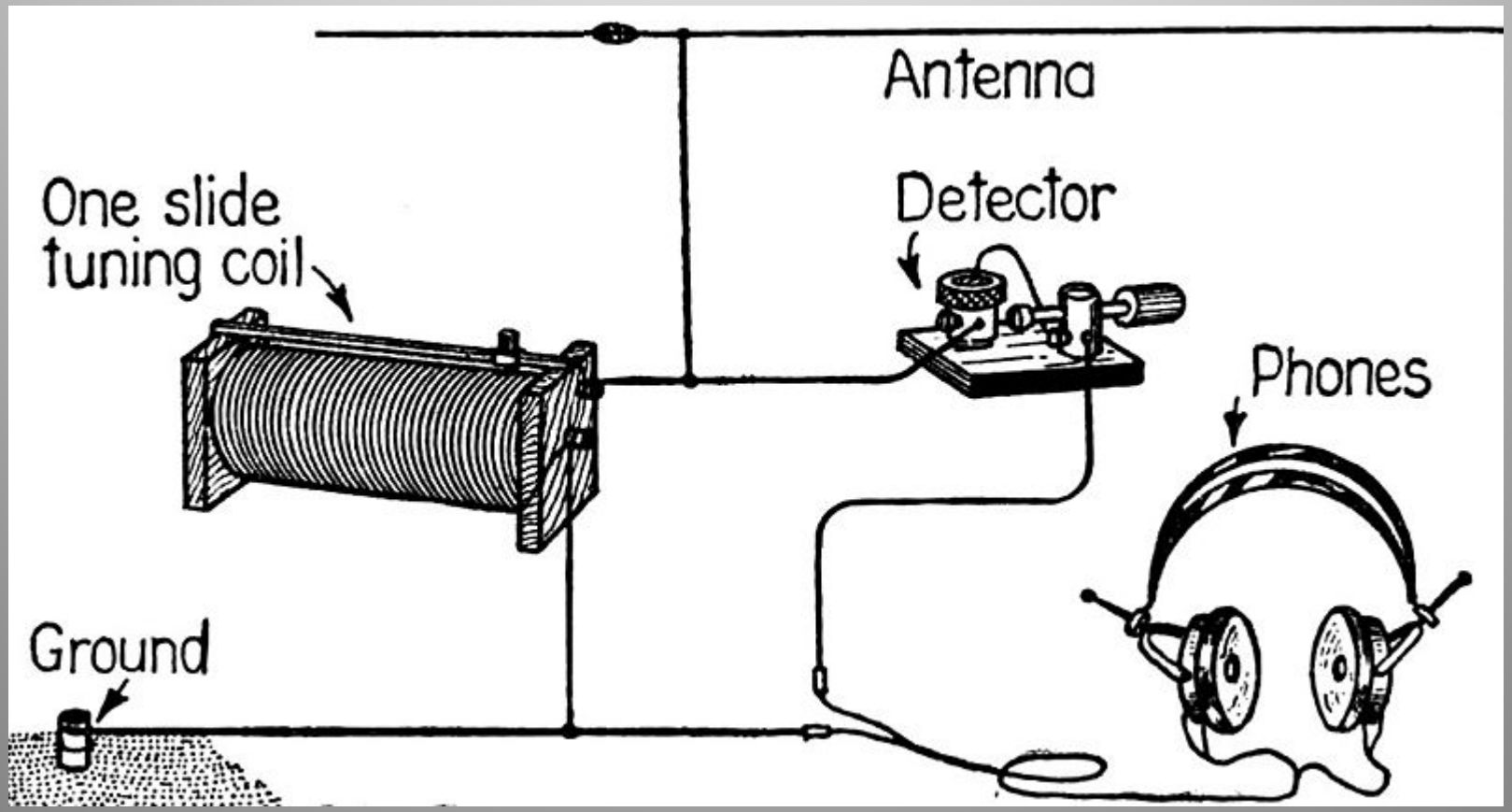


Hardware

- Crystal set receiver
  - Powerful AM transmissions

Hardware

- Crystal set receiver
  - Powerful AM transmissions

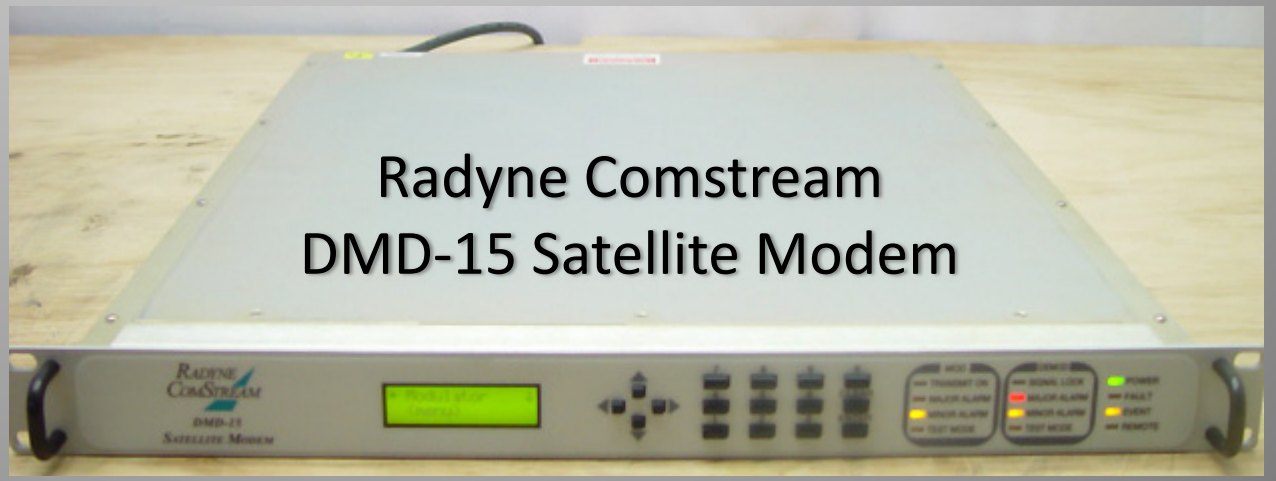


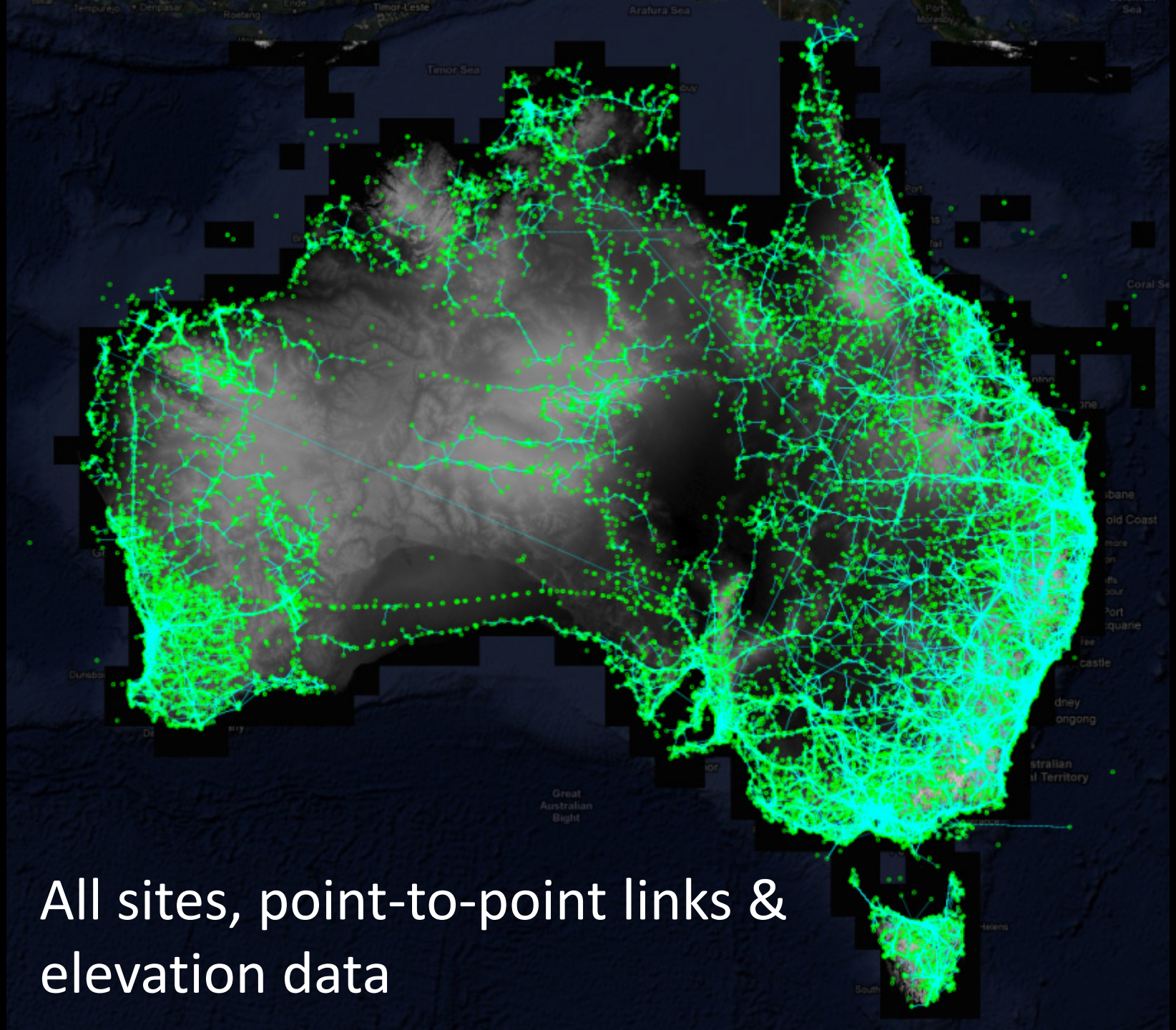
Hardware

- Crystal set receiver
  - Powerful AM transmissions
- More advanced hardware to handle increasingly complex modulation schemes
  - FM, stereo FM, microwave, digital…

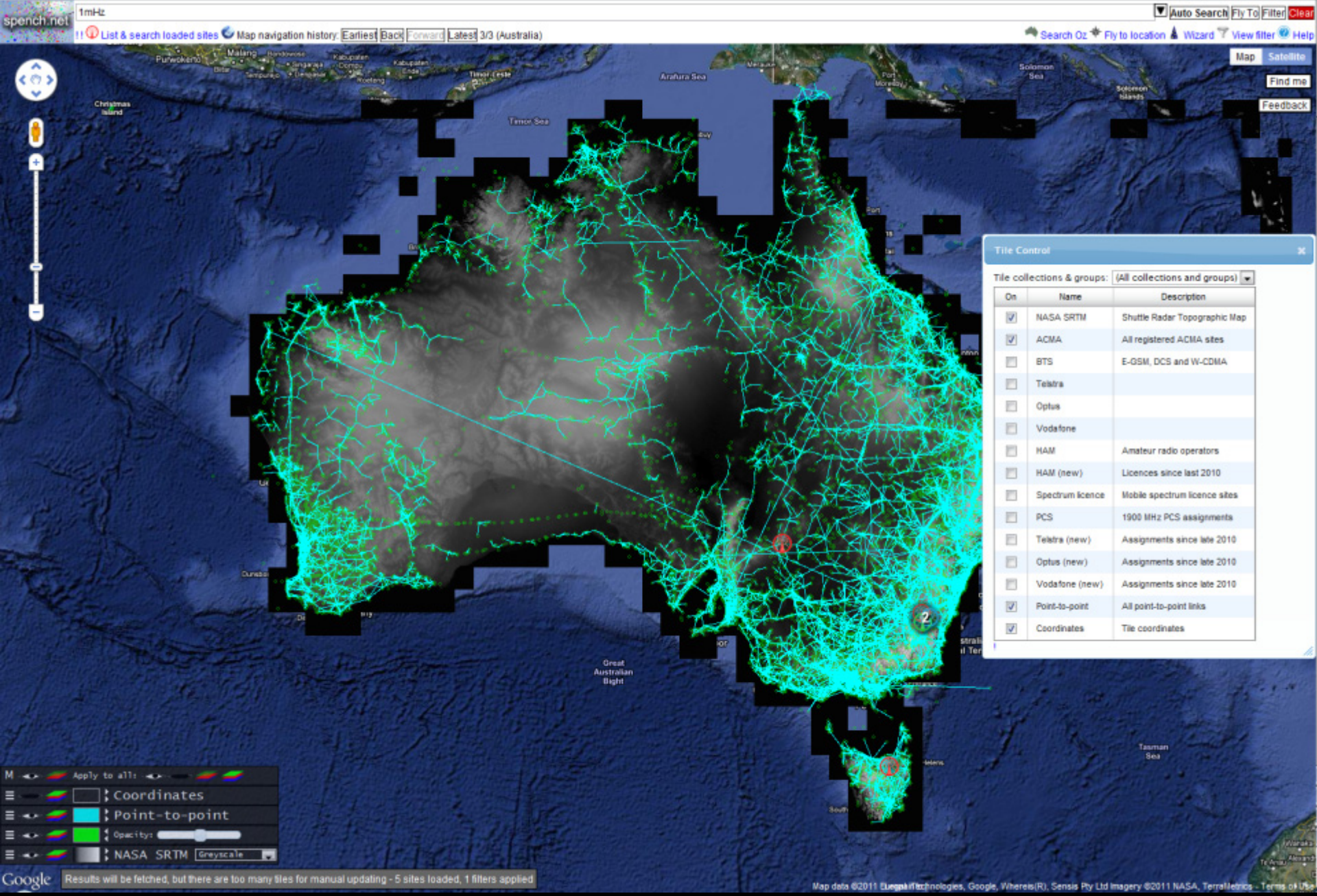
Modulation in Hardware

- **MO**dulation and **DE-M**odulation traditionally performed in hardware
- 'Black box' implementation
  - Not re-configurable
- Modern digital hardware allows more flexibility

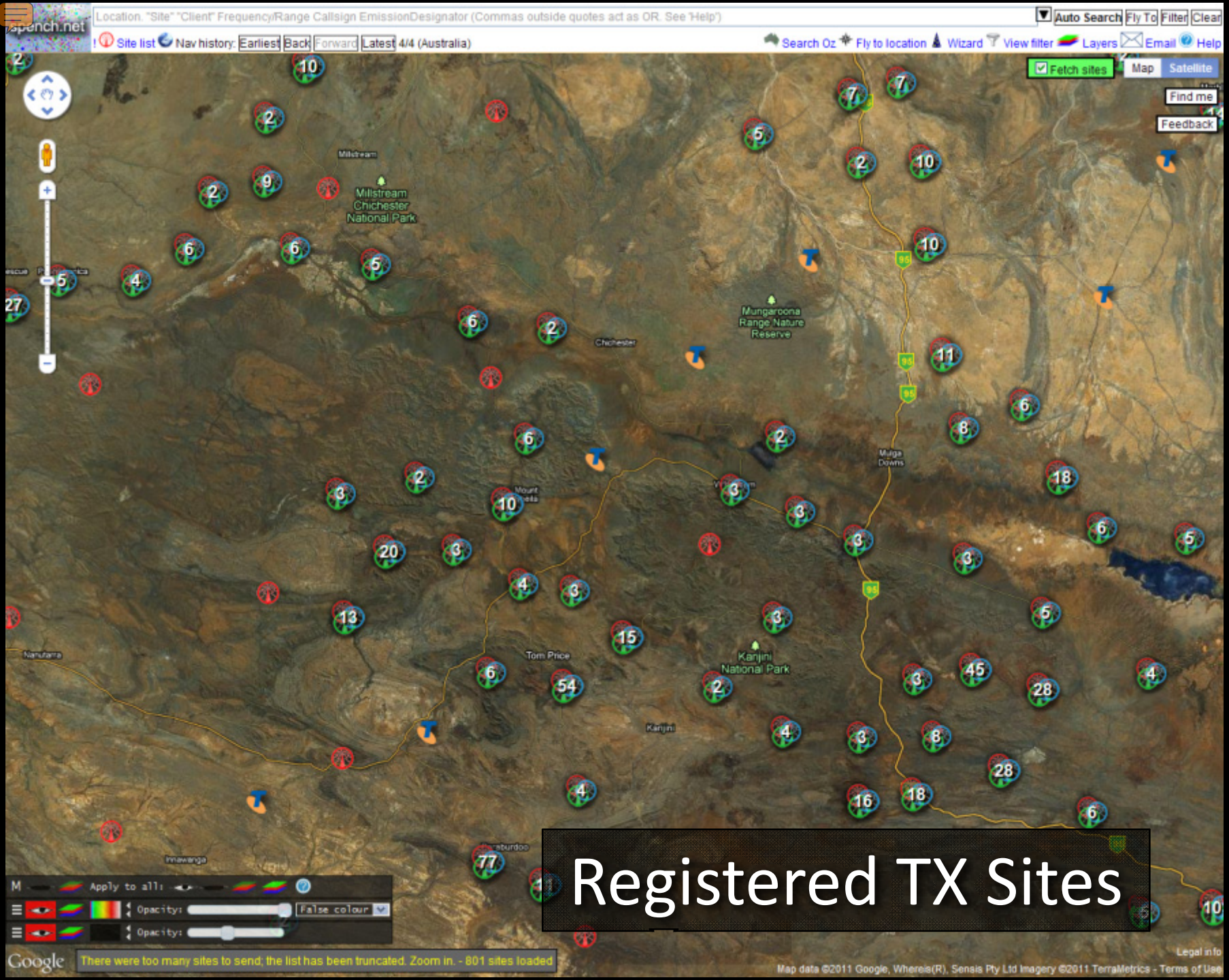




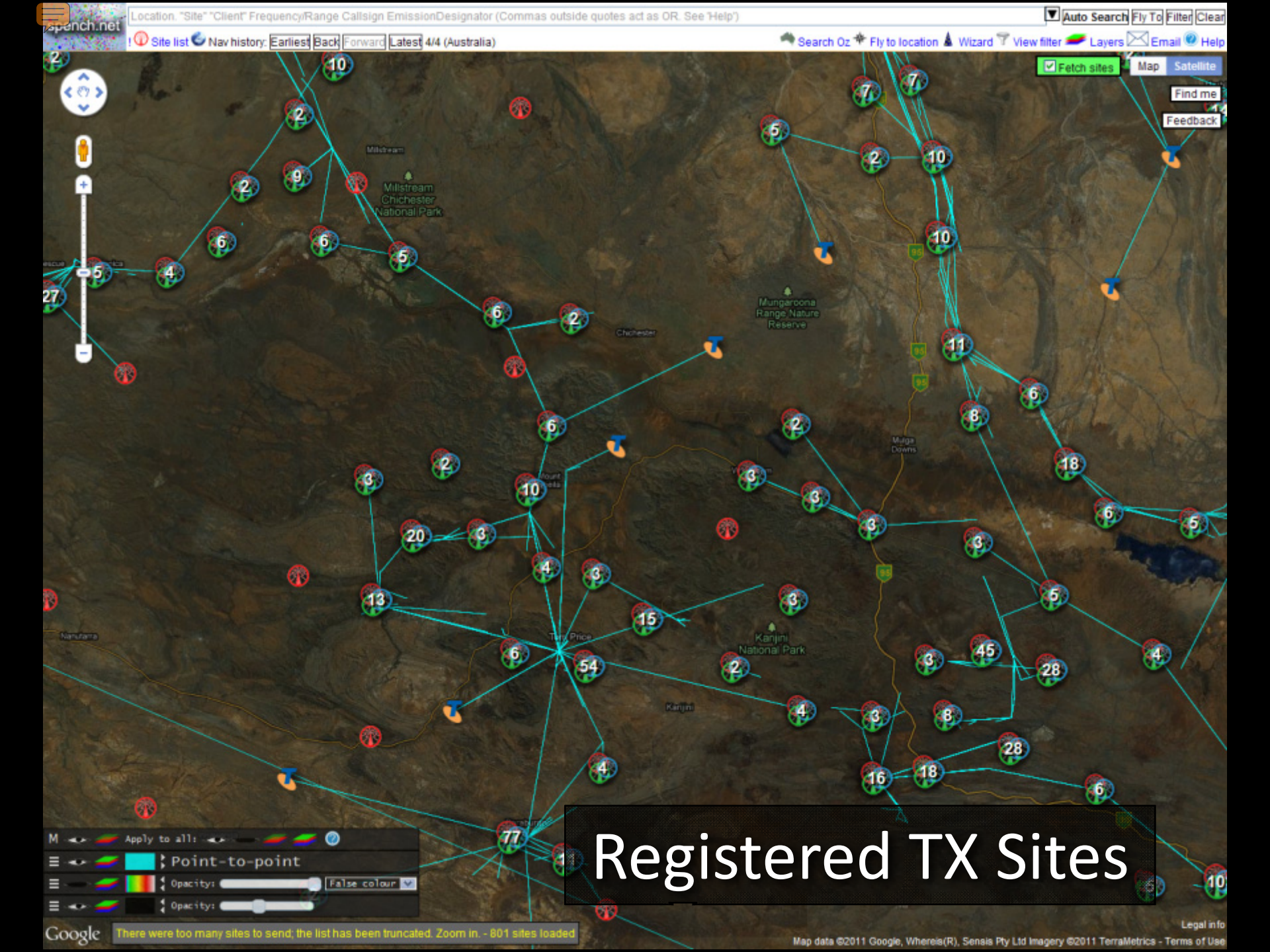
All sites, point-to-point links & elevation data

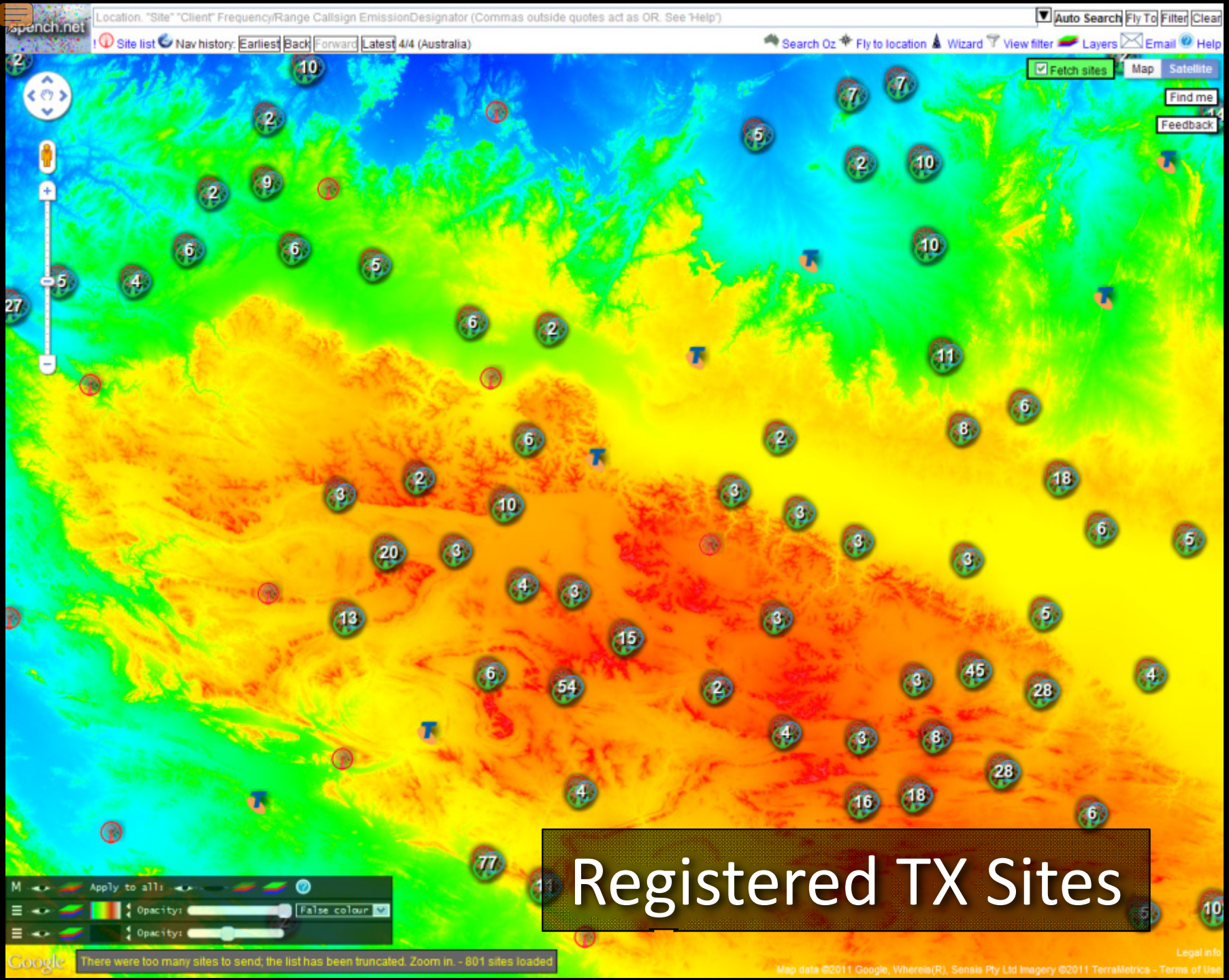


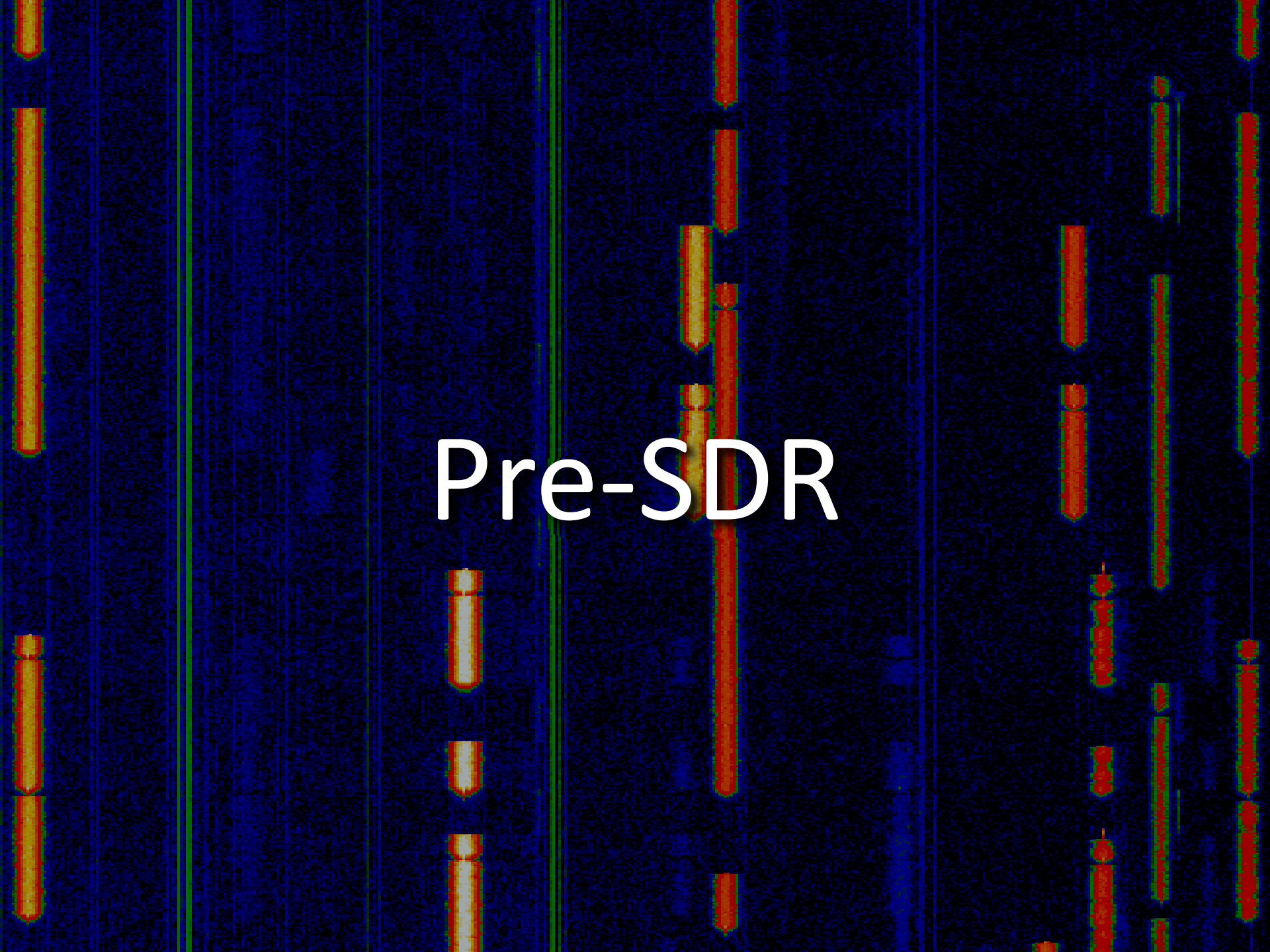
The RFMap web interface



Registered TX Sites


Location. "Site" "Client" Frequency/Range Callsign EmissionDesignator (Commas outside quotes act as OR. See 'Help')
Auto Search
Fly To
Filter
Clear
Site list
Nav history:
Earliest
Back
Forward
Latest
4/4 (Australia)
Search Oz
Fly to location
Wizard
View filter
Layers
Email
Help
Fetch sites
Map
Satellite
Find me
Feedback
Millstream Chichester National Park
Mungaroona Range Nature Reserve
Kanjini National Park
Apply to all:
Point-to-point
Opacity:
False colour
Opacity:
There were too many sites to send; the list has been truncated. Zoom in. - 801 sites loaded
Legal info
Map data ©2011 Google, Whereis(R), Sensis Pty Ltd Imagery ©2011 TerraMetrics - Terms of Use
Registered TX Sites


Location, "Site" "Client" Frequency/Range Callsign EmissionDesignator (Commas outside quotes act as OR. See 'Help')
Auto Search
Fly To
Filter
Clear
Site list
Nav history:
Earliest
Back
Forward
Latest
4/4 (Australia)
Search Oz
Fly to location
Wizard
View filter
Layers
Email
Help
Fetch sites
Map
Satellite
Find me
Feedback
Apply to all:
Opacity:
False colour
Opacity:
There were too many sites to send; the list has been truncated. Zoom in. - 801 sites loaded
Google
Map data ©2011 Google, Whereis(R), Sensis Pty Ltd Imagery ©2011 TerraMetrics - Terms of Use
Registered TX Sites


Pre-SDR


YAESU
FRA-7700
YAESU FRT-7700
YAESU FRG-9600
REALISTIC
300 CHANNEL
YAESU COMMUNICATIONS RECEIVER FRG-8800
POWER
PHONES
REC
SQUELCH
TONE
AF GAIN
FINE
M CH
ATT
Book of WHY
BIBLICAL ART
MICHELANGELO
RENAISSANCE
GAUDI
DEAN
Romeo and Juliet
King Henry V
Twelfth Night
Othello
OXFORD Children's Pocket Book of Knowledge
JAMES DAY

The Mystery Signal

Rate at which ‘messages’ were transmitted varied throughout the day:

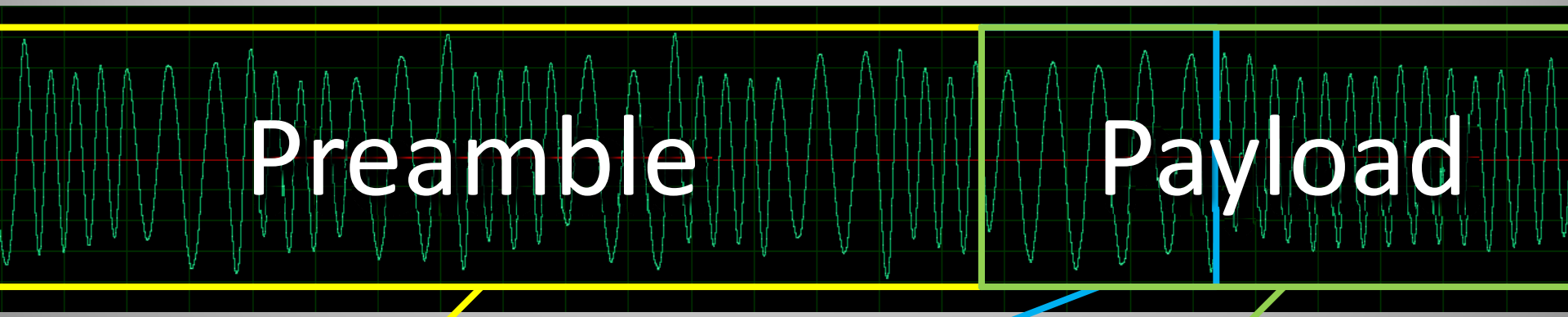
correlates with increased daytime activity.

Received RF signal → audio → sampled by soundcard → streamed across network

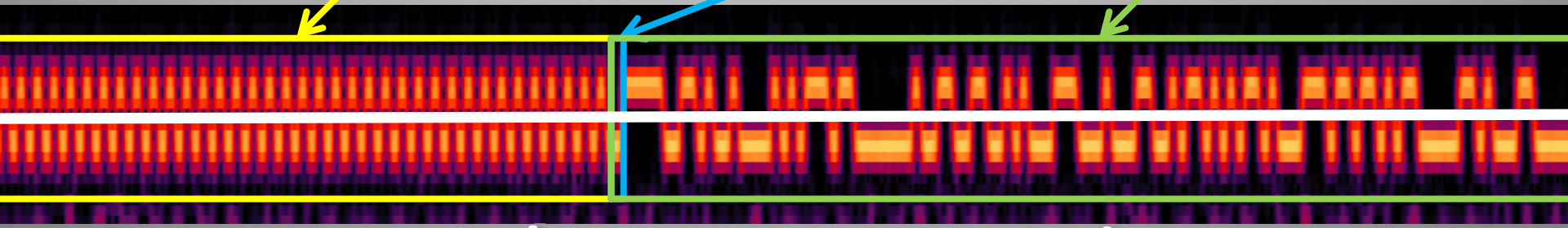
Step One: Look at the signal

Radio is already set to receive N-FM (narrowband frequency modulated signal)

Signal in the time domain (voltage vs. time):



Signal in the frequency domain (intensity of frequency bins vs. time):

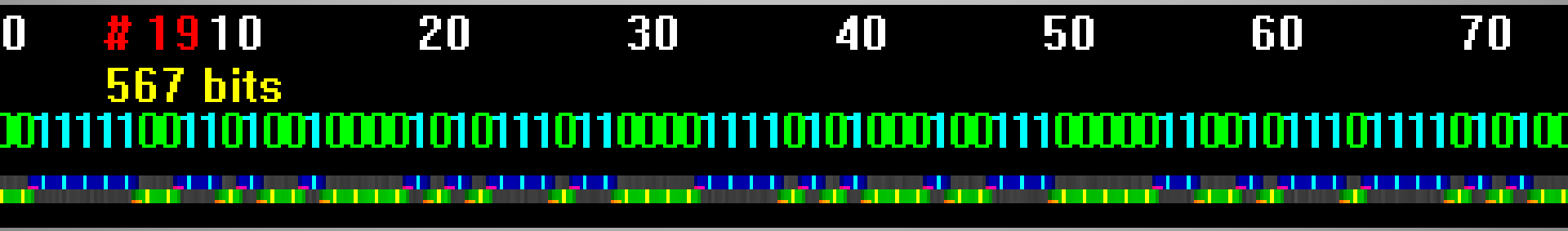


IT’S SLICER TIME!

Step Two: FFT of 2FSK → Bitstream

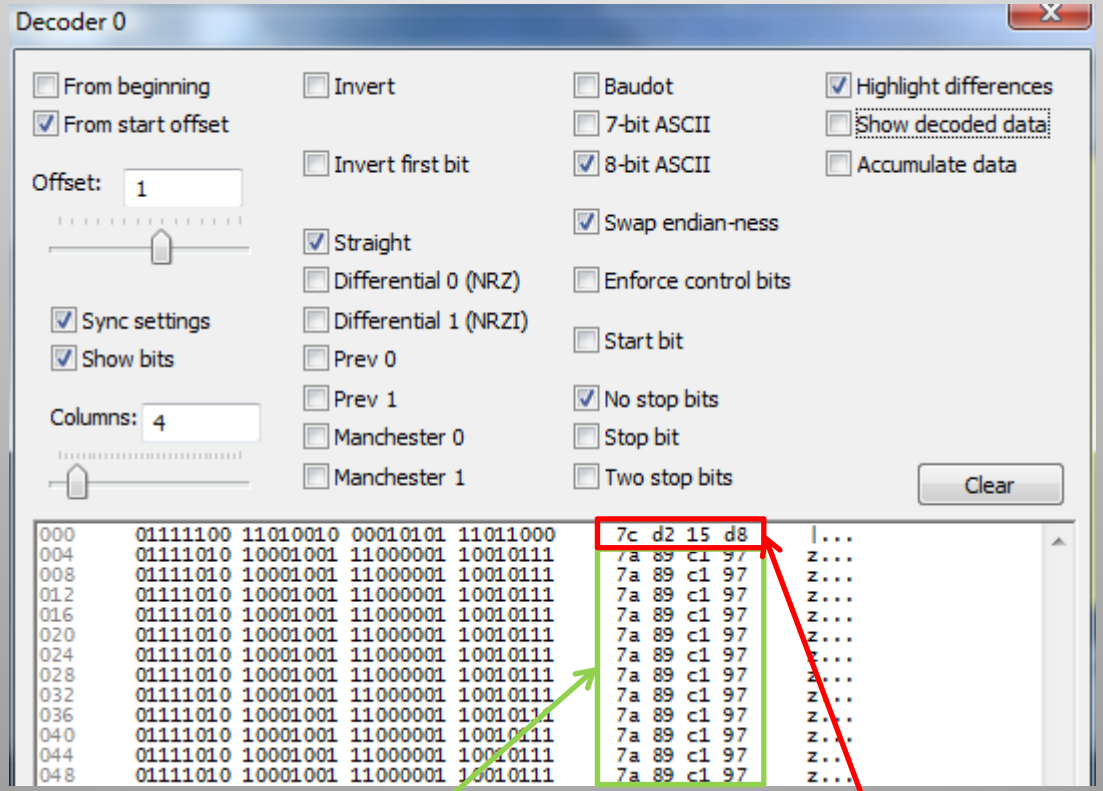
- Lock on two frequencies (**F**requency **S**hift **K**eying)
- Sample intensity of each at regular interval (baud rate)
- Pick which is the strongest:

low = 0 bit, high = 1 bit



Step Three: Data → Information

- The most difficult part, so try all combinations



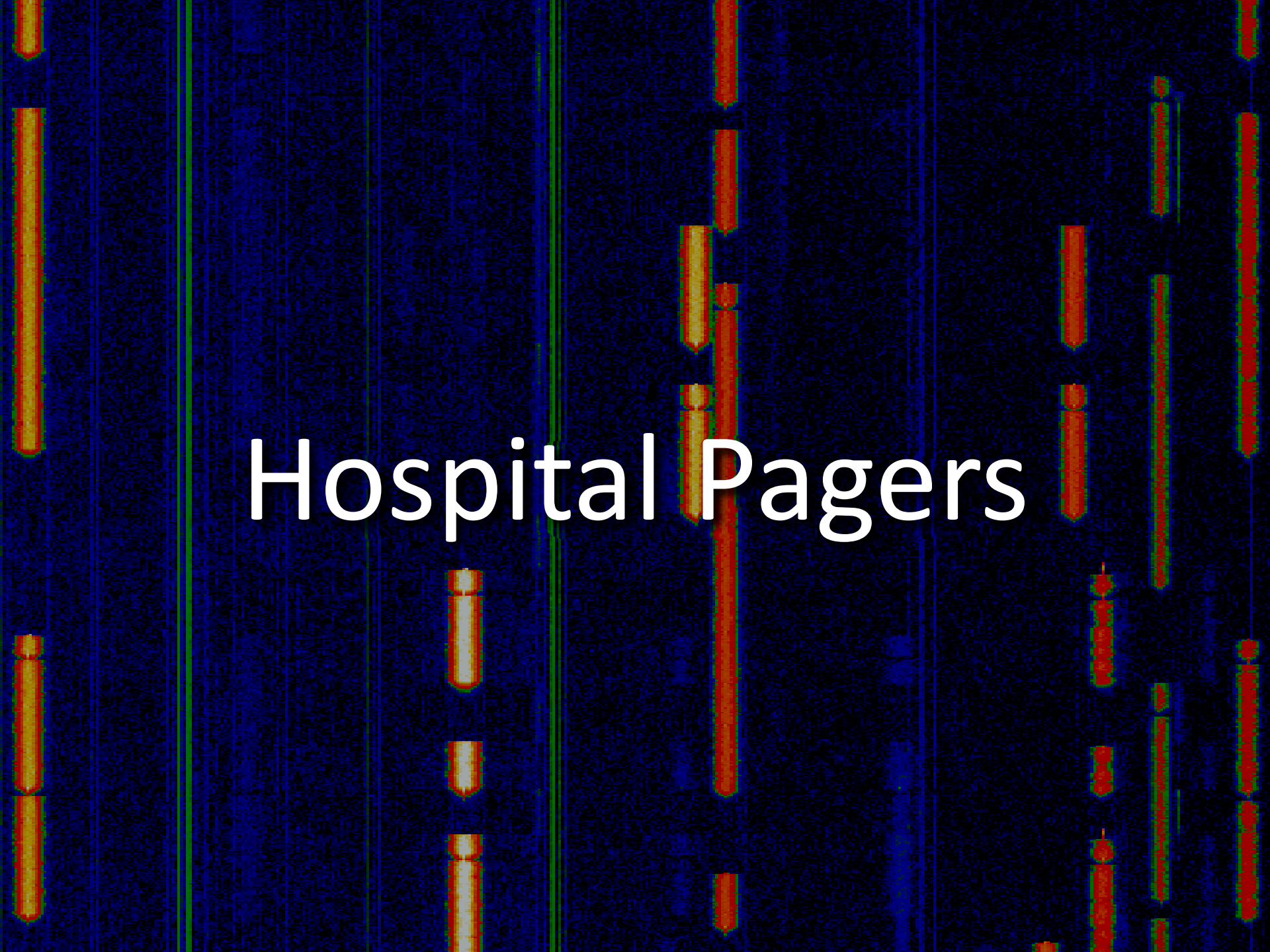
Wikipedia says:

Code words are transmitted in batches that consist of a sync codeword, defined in the standard as 0x7CD215D8, followed by 16 others containing the data. Any unused code words are filled with the idle value of 0x7A89C197. In practice other values are sometimes used to indicate sync and idle.

POCSAG!

- "**P**ost **O**ffice **C**ode **S**tandardization **A**dvisory **G**roup"
- Standard decoding software didn't work
- Key: recognisable sequence of bits when idle

→Look for known codewords/repeated bit strings


Hospital Pagers

Hospital Pager Systems

- High power, better penetration than mobiles
- Personnel carry small pagers, each with ID mapped to **R**adio **I**dentity **C**ode
- Mostly numeric pages with phone extension
- Sent via software on any computer at hospital
- Address to multiple recipients, automatically sent to each once
- Delivery not guaranteed

Frequencies

- Shared frequency: 148.1375 MHz (standard)
- Private systems in 800/900MHz band:

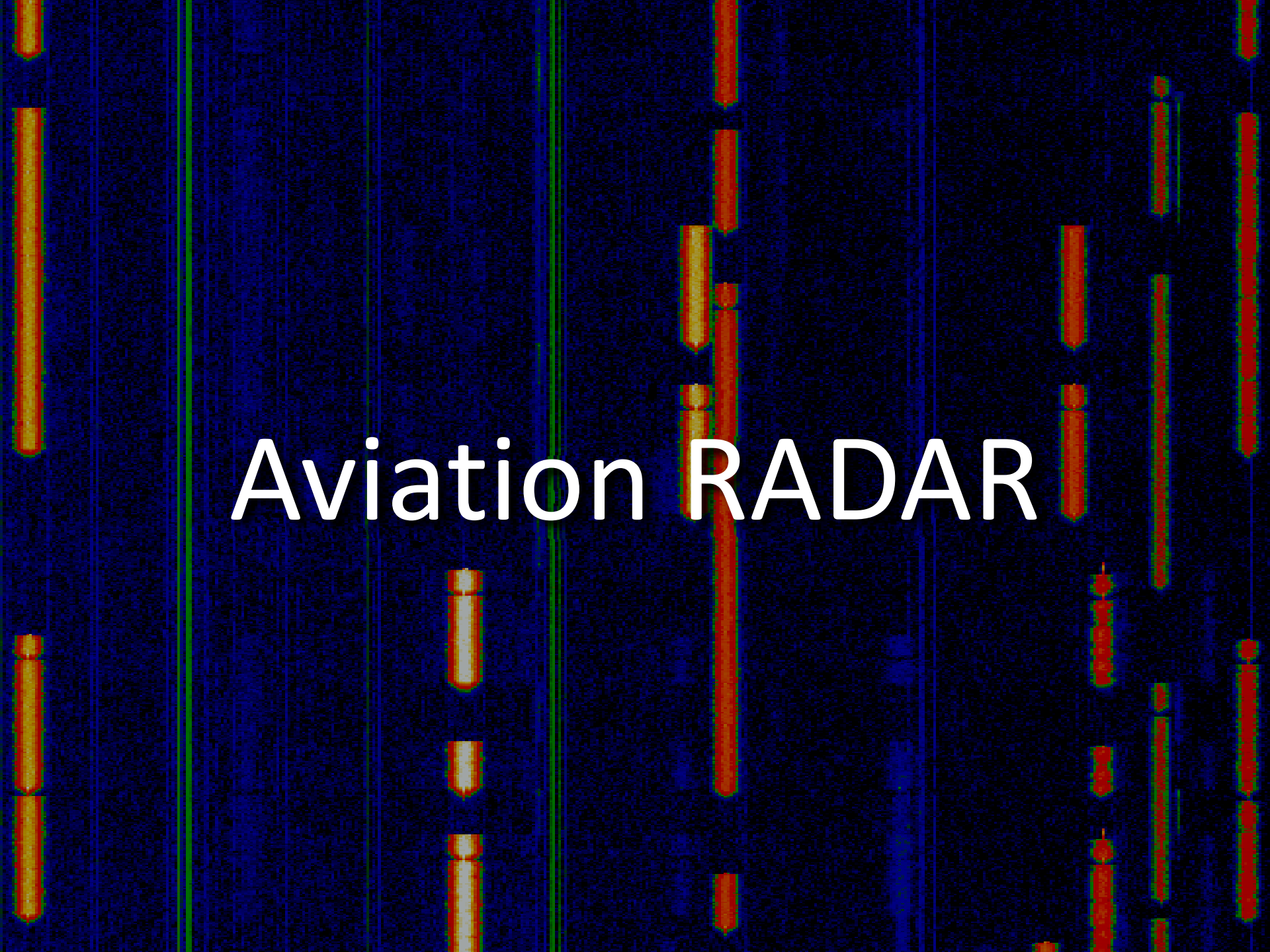
  Non-standard FSK ignored by decoders


Description E Block Royal Alfred Princes Hospital Missenden Rd, CAMPERDOWN
Address CAMPERDOWN NSW 2050
Position -33.8894079360502, 151.18276526855
<< first < prev 1 2 3 next > last >>
Icon Freq Em Des Client Links Menu
148.1375 MHz 16K0F2D Sydney West Area Health Service 22
929.41875 MHz 10K1F3E Sydney West Area Health Service 1
929.26875 MHz 10K1F3E Sydney West Area Health Service 1
853.06875 MHz 10K1F3E Sydney West Area Health Service 1
853.26875 MHz 10K1F3E Sydney West Area Health Service 1
853.41875 MHz 10K1F3E Sydney West Area Health Service 1
461.06875 MHz 10K1F2D Sydney West Area Health Service 1
857.4125 MHz 16K0F2D Sydney West Area Health Service 1
857.4125 MHz 16K0F2D Sydney West Area Health Service 1
857.4125 MHz 16K0F2D Sydney West Area Health Service 1
<< first < prev 1 2 3 next > last >>
Golygosh
St John's College
McDonald's
Missenden Rd
King George V Memorial Hospital For Mothers & Babies
Royal Prince Alfred Hospital
Royal Prince Alfred Hospital Helipad
Medical Society Bookshop
Blackburn Circuit
Cadigal Ln

On RFMap


Fetch sites
Map
Satellite
Find me
Feedback
Sydney West Area Health Service
Idle - 50 sites loaded, 2 filters applied
Map data ©2011 Google, Whereis(R), Sensis Pty Ltd Imagery ©2011 TerraMetrics - Terms of Use
Legal info

Sensitive Information


Aviation RADAR

ATCRBS, PSR & SSR

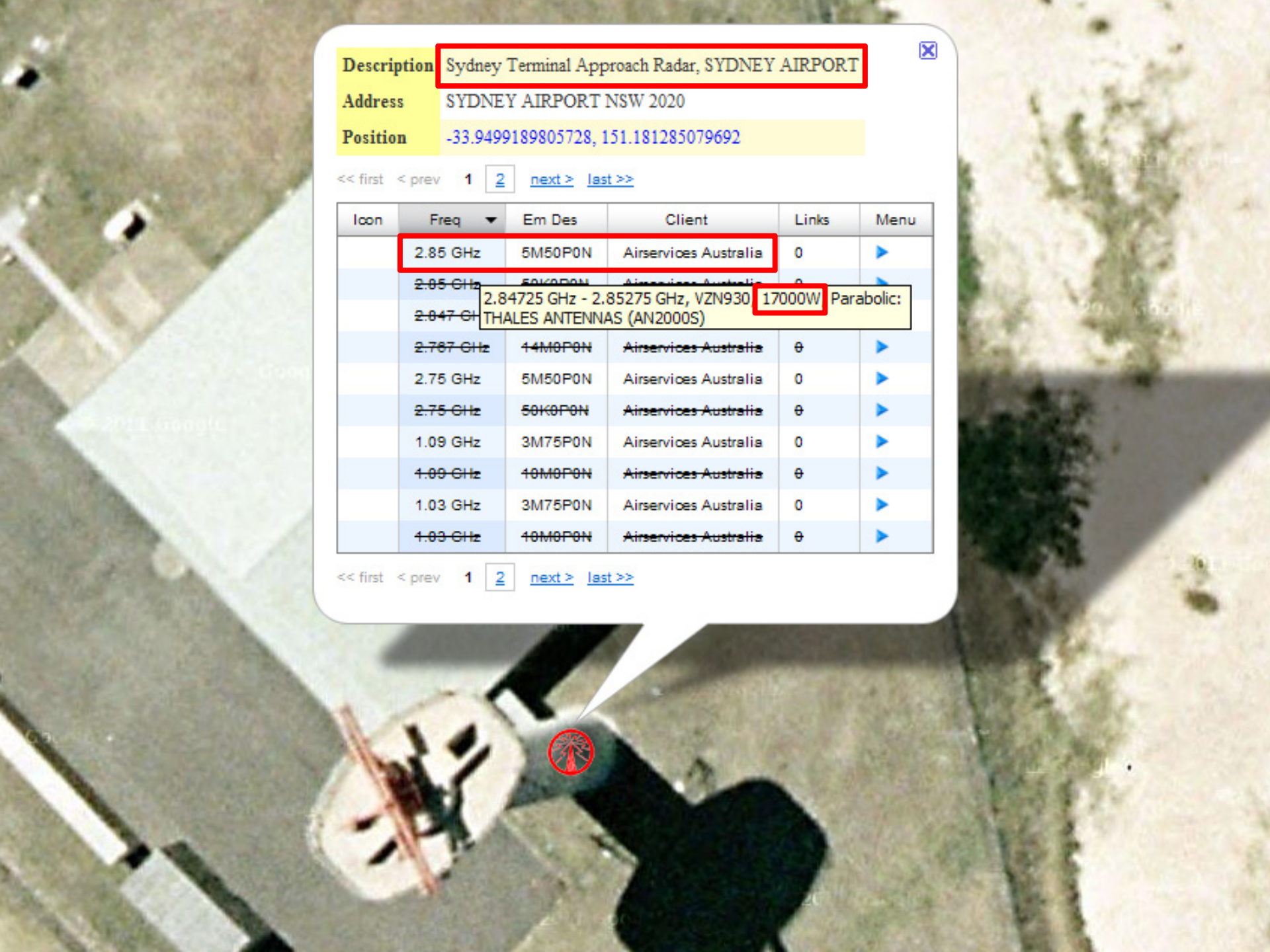
- **A**ir **T**raffic **C**ontrol **R**adar **B**eacon **S**ystem
  - **P**rimary **S**urveillance **R**adar
  - **S**econdary **S**urveillance **R**adar

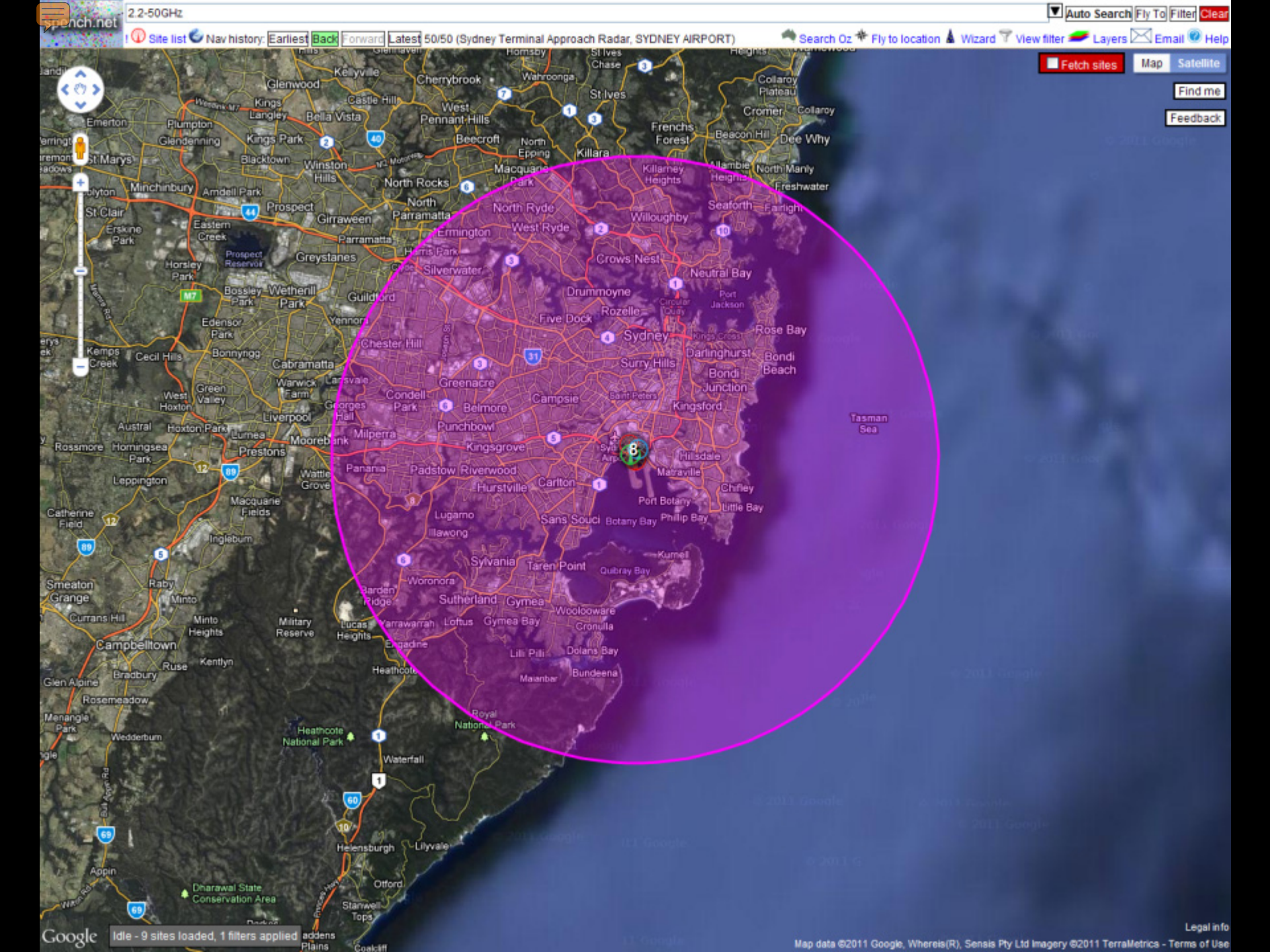
Primary:
- Traditional RADAR
- 'Paints skins' and listens for return
- Identifies and tracks primary targets, while ignoring 'ground clutter'
- Range limited by RADAR equation ($\frac{1}{d^4}$)

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

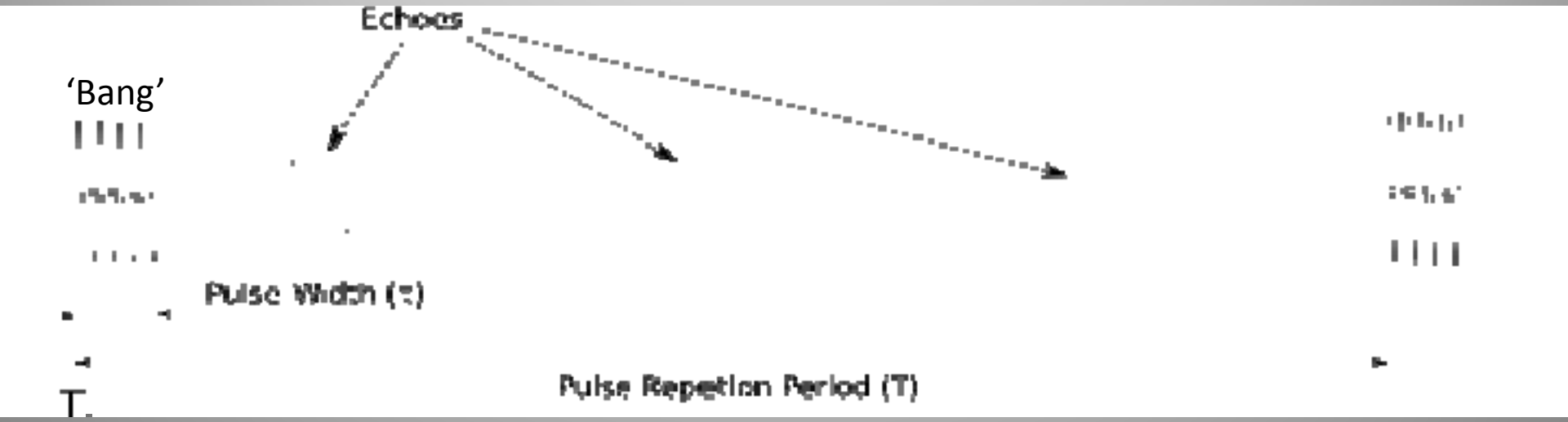
Secondary:
- Directional radio
- Requires transponder
- Interrogates transponders, which reply with squawk code, altitude, etc.
- Increased range ($\frac{1}{d^2}$)


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
2.84725 GHz - 2.85275 GHz, VZN930 17000W Parabolic:
THALES ANTENNAS (AN2000S)
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
<< first < prev 1 2 next > last >>


2.2-50GHz
Auto Search
Fly To
Filter
Clear
Site list
Nav history:
Earliest
Back
Forward
Latest
50/50 (Sydney Terminal Approach Radar, SYDNEY AIRPORT)
Search Oz
Fly to location
Wizard
View filter
Layers
Email
Help
Fetch sites
Map
Satellite
Find me
Feedback
Sydney
Parramatta
Liverpool
Campbelltown
Penrith
Blacktown
Hornsby
Manly
Bondi Beach
Tasman Sea
Royal National Park
Heathcote National Park
Dharawal State Conservation Area
Google
Idle - 9 sites loaded, 1 filters applied
Legal info
Map data ©2011 Google, Whereis(R), Sensis Pty Ltd Imagery ©2011 TerraMetrics - Terms of Use

Primary **S**urveillance **R**ADAR

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

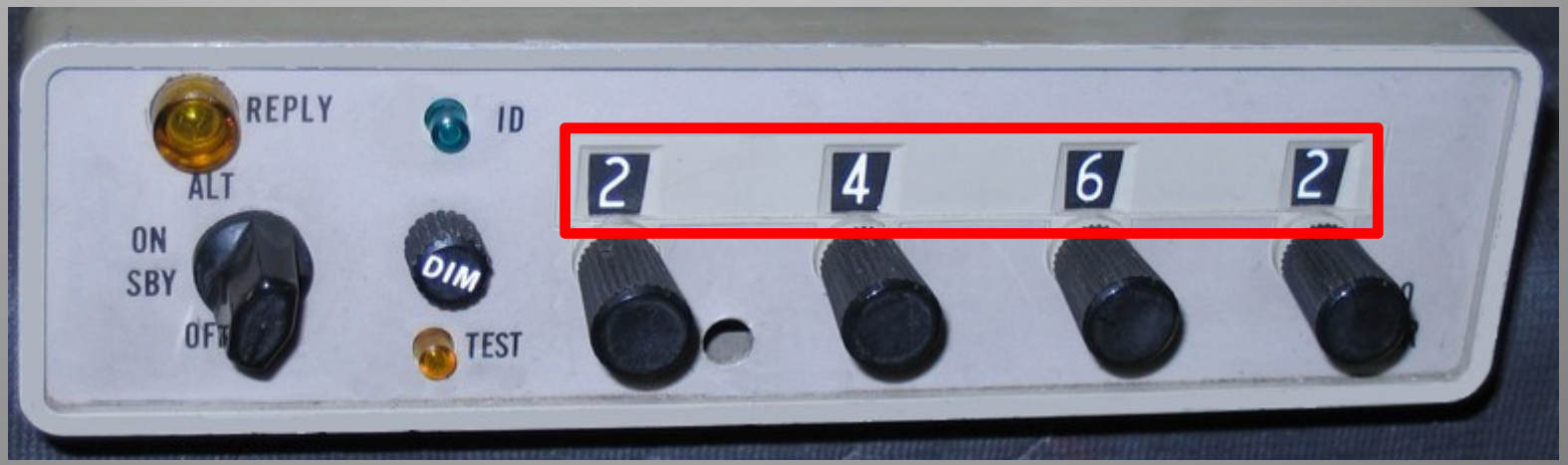


The Modes

- **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

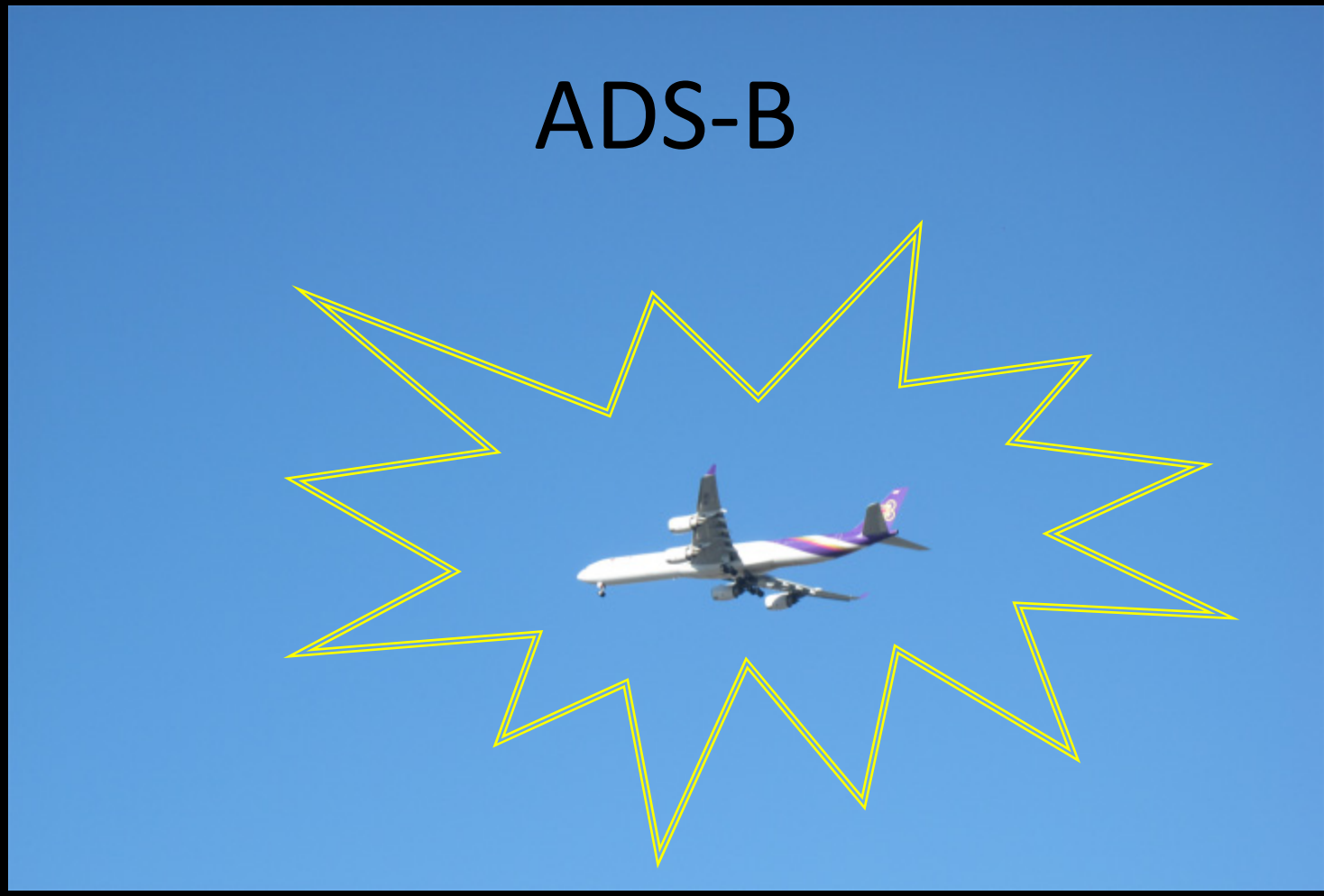
Heading

Altitude

Vertical rate

Flight ID

Squawk code



ATC

Uplink:
“All call” / Altitude request

Downlink:
Airframe ID / Altitude response (air-to-ground)

Mode S TX/RX: Linked to ATC (can be at airport, or remote)

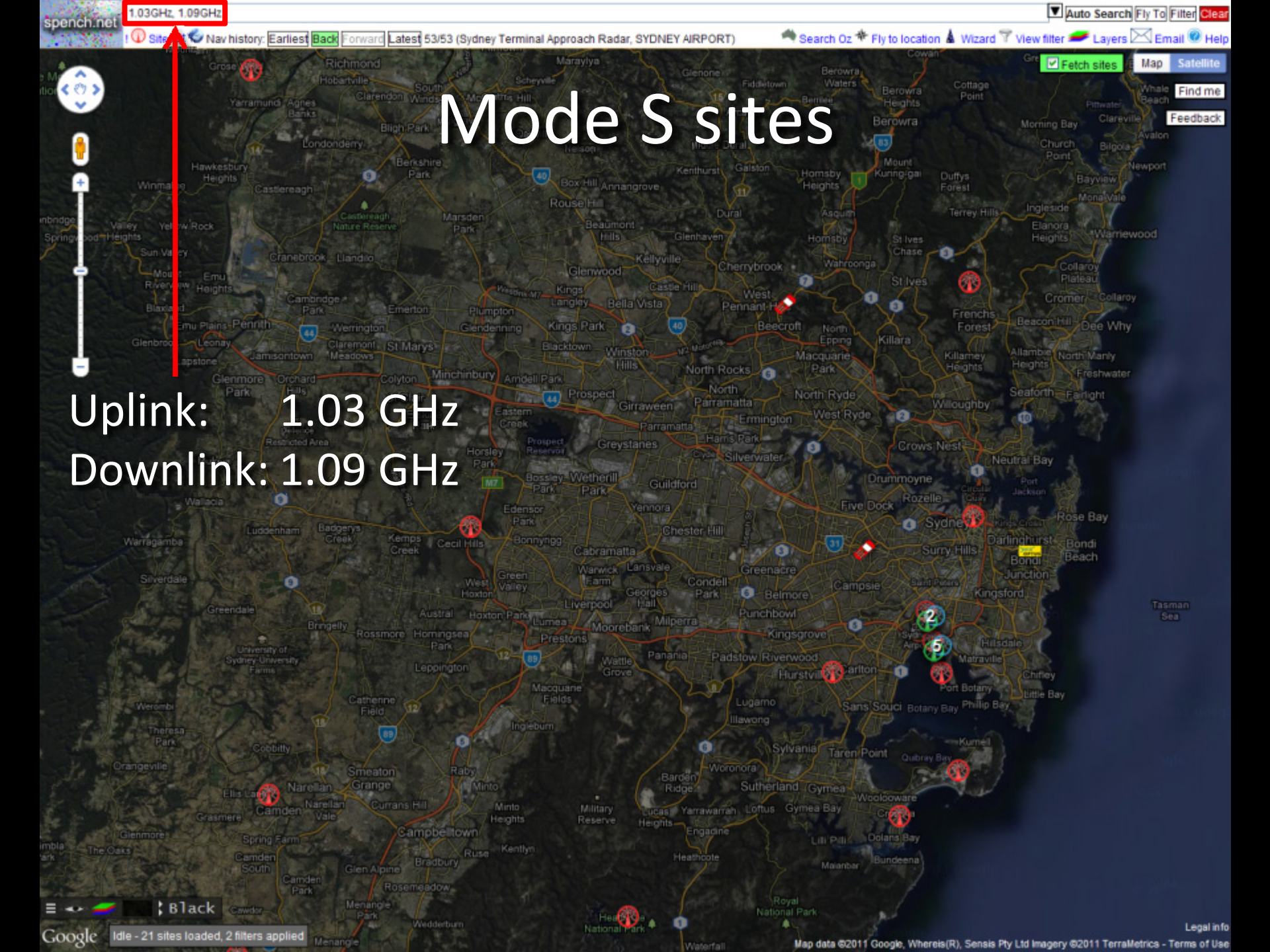
ACAS/TCAS

"PULL UP"

"TRAFFIC"

Altitude request

Altitude response (air-to-air)


spench.net
1.03GHz, 1.09GHz
Auto Search
Fly To
Filter
Clear
Site list
Nav history:
Earliest
Back
Forward
Latest
53/53 (Sydney Terminal Approach Radar, SYDNEY AIRPORT)
Search Oz
Fly to location
Wizard
View filter
Layers
Email
Help
Fetch sites
Map
Satellite
Find me
Feedback
Mode S sites
Uplink: 1.03 GHz
Downlink: 1.09 GHz
Black
Google
Idle - 21 sites loaded, 2 filters applied
Legal info
Map data ©2011 Google, Whereis(R), Sensis Pty Ltd Imagery ©2011 TerraMetrics - Terms of Use

A Typical 747 has…

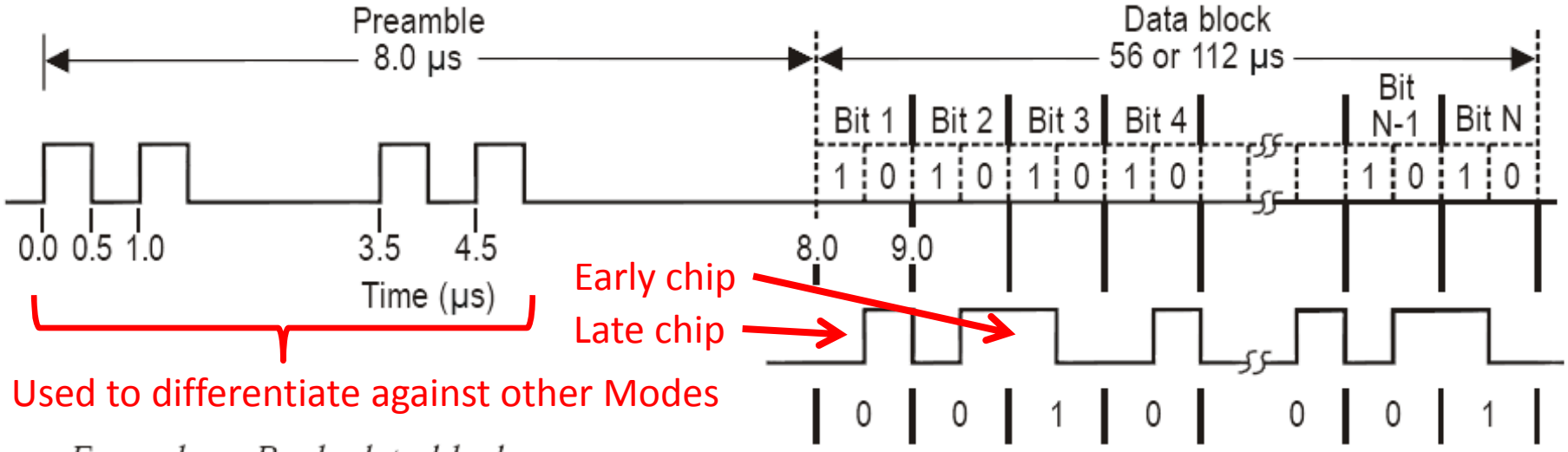
31 radios

- 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
54A
54A
VHF
DME
ADF
EPIRB
Marker
RADAR Altimeter

Mode S Response Encoding

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

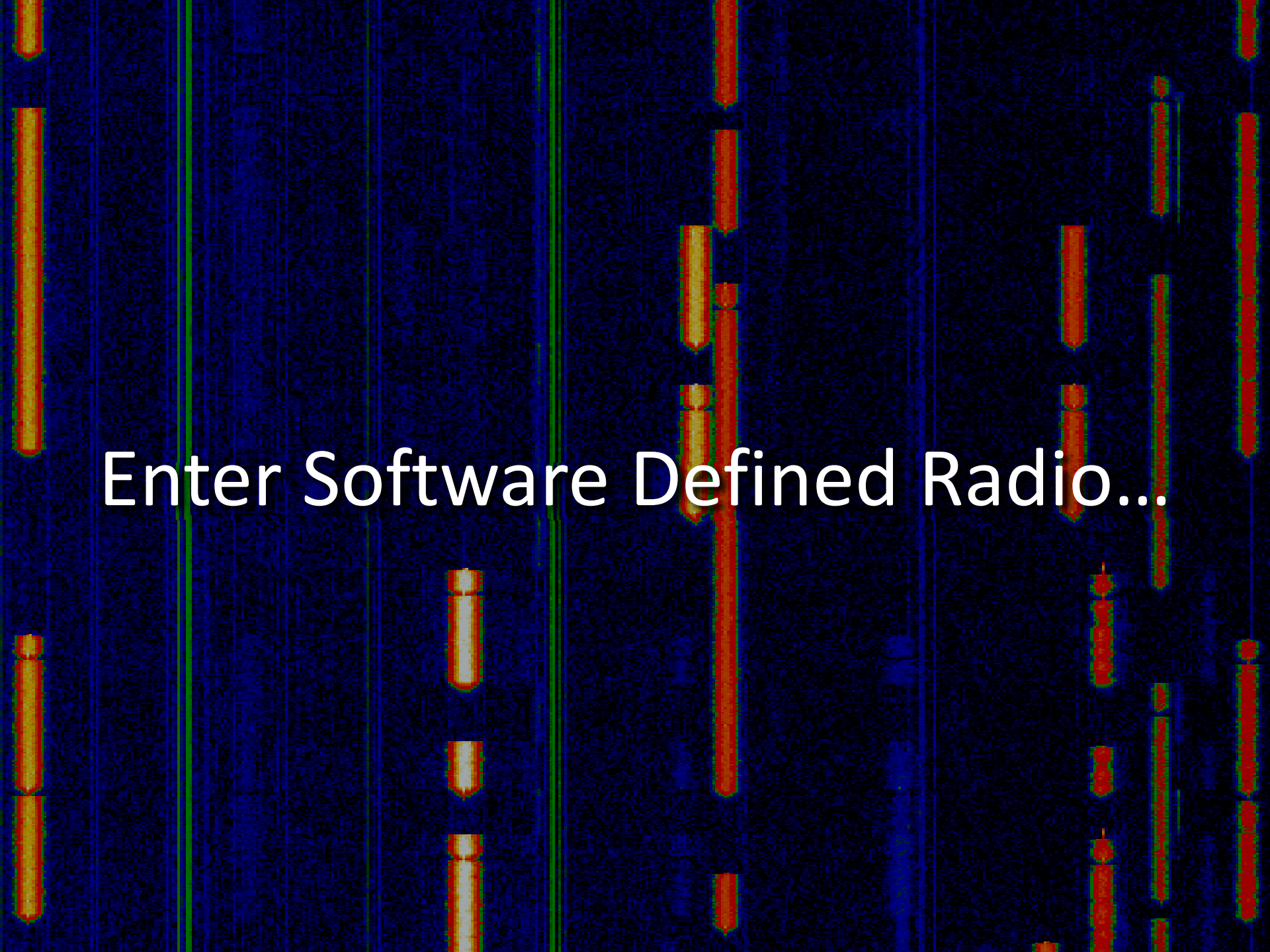


Example.— Reply data block corresponding to bit sequence 0010 001

Pulse Position Modulation (AM)

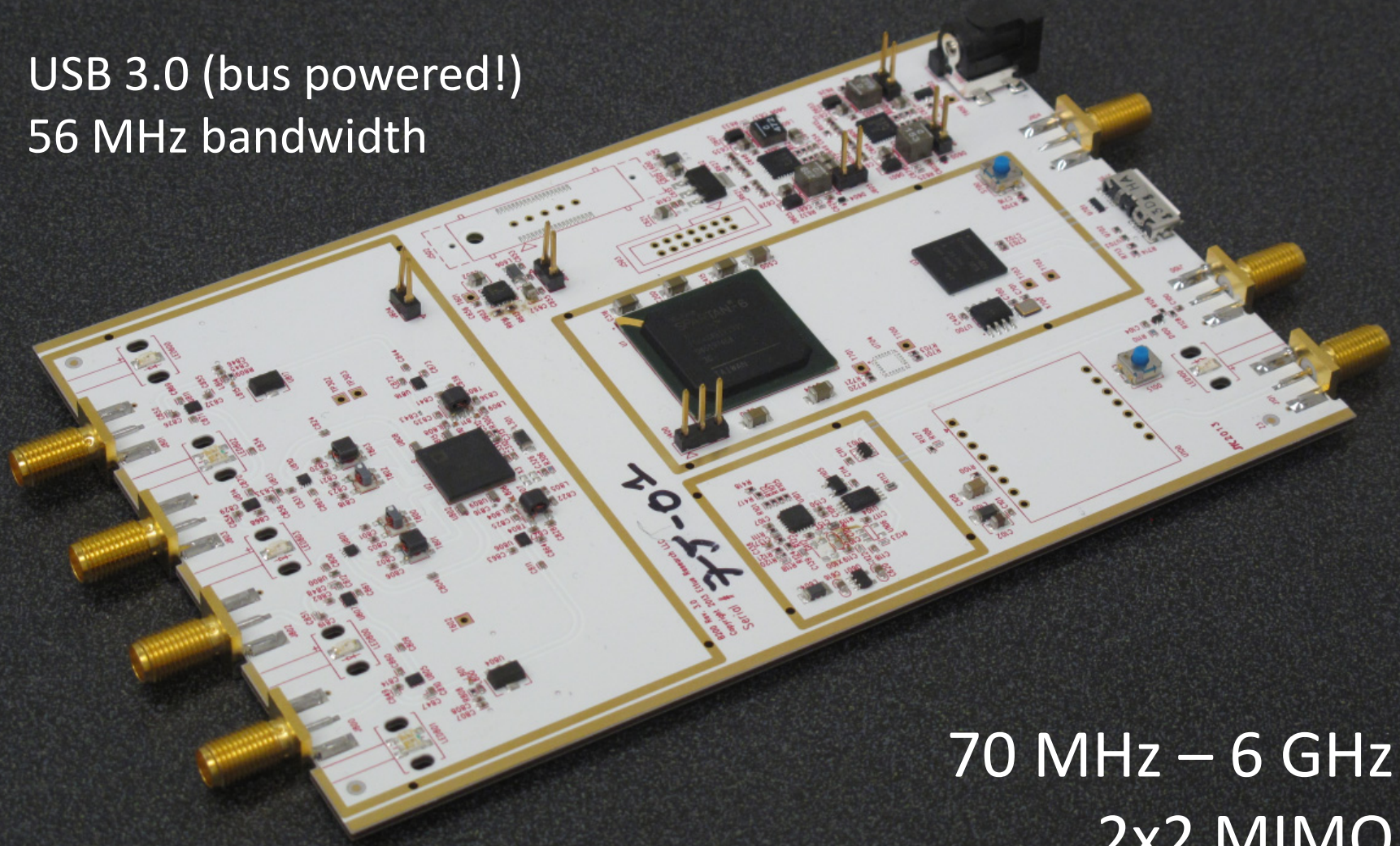
Pulse Position Modulation

- Pulse lasts **0.0000005 seconds** ($0.5\ \mu s$)
- 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


Enter Software Defined Radio…

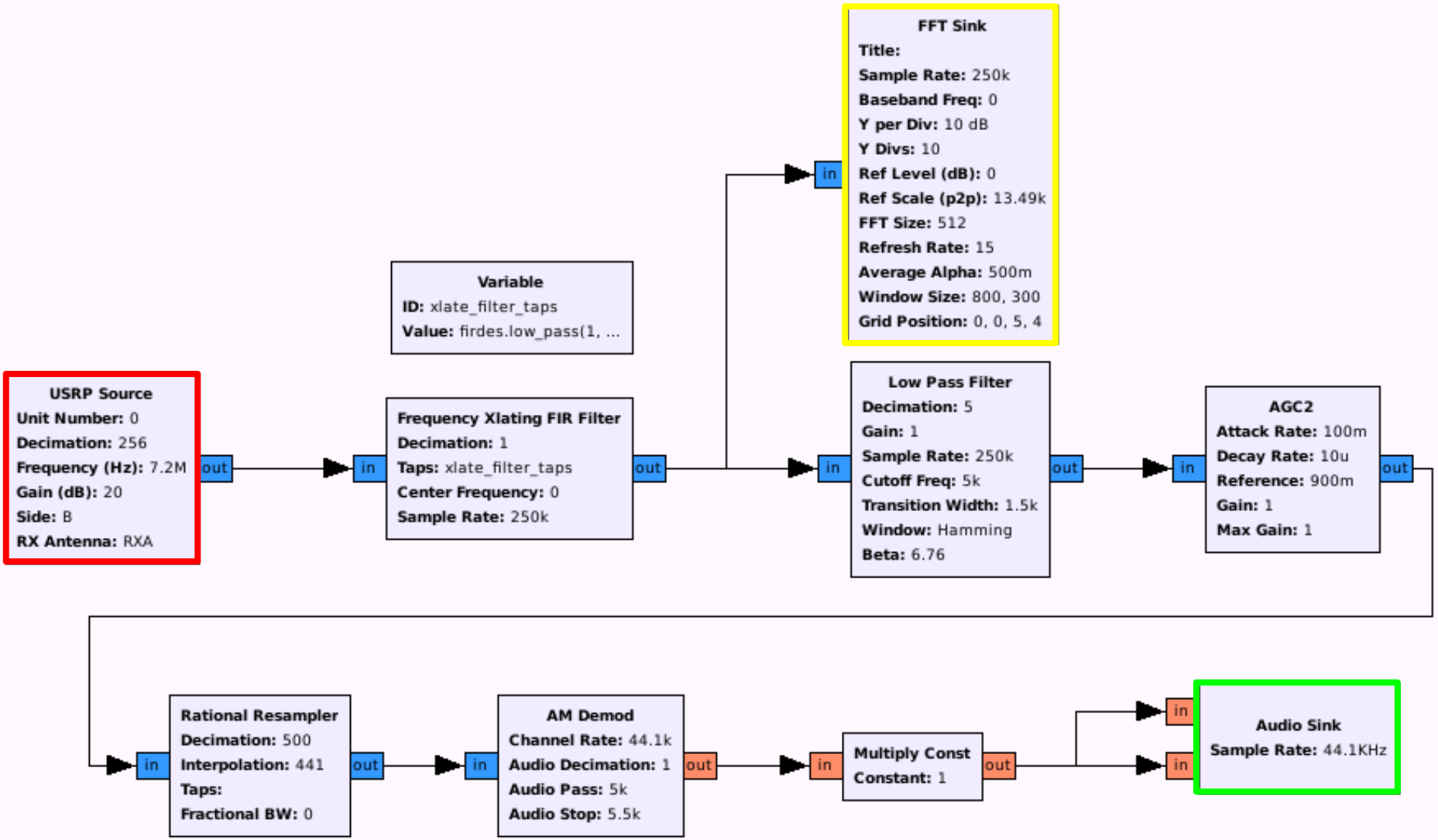
USRP B200 & B210

USB 3.0 (bus powered!)
56 MHz bandwidth

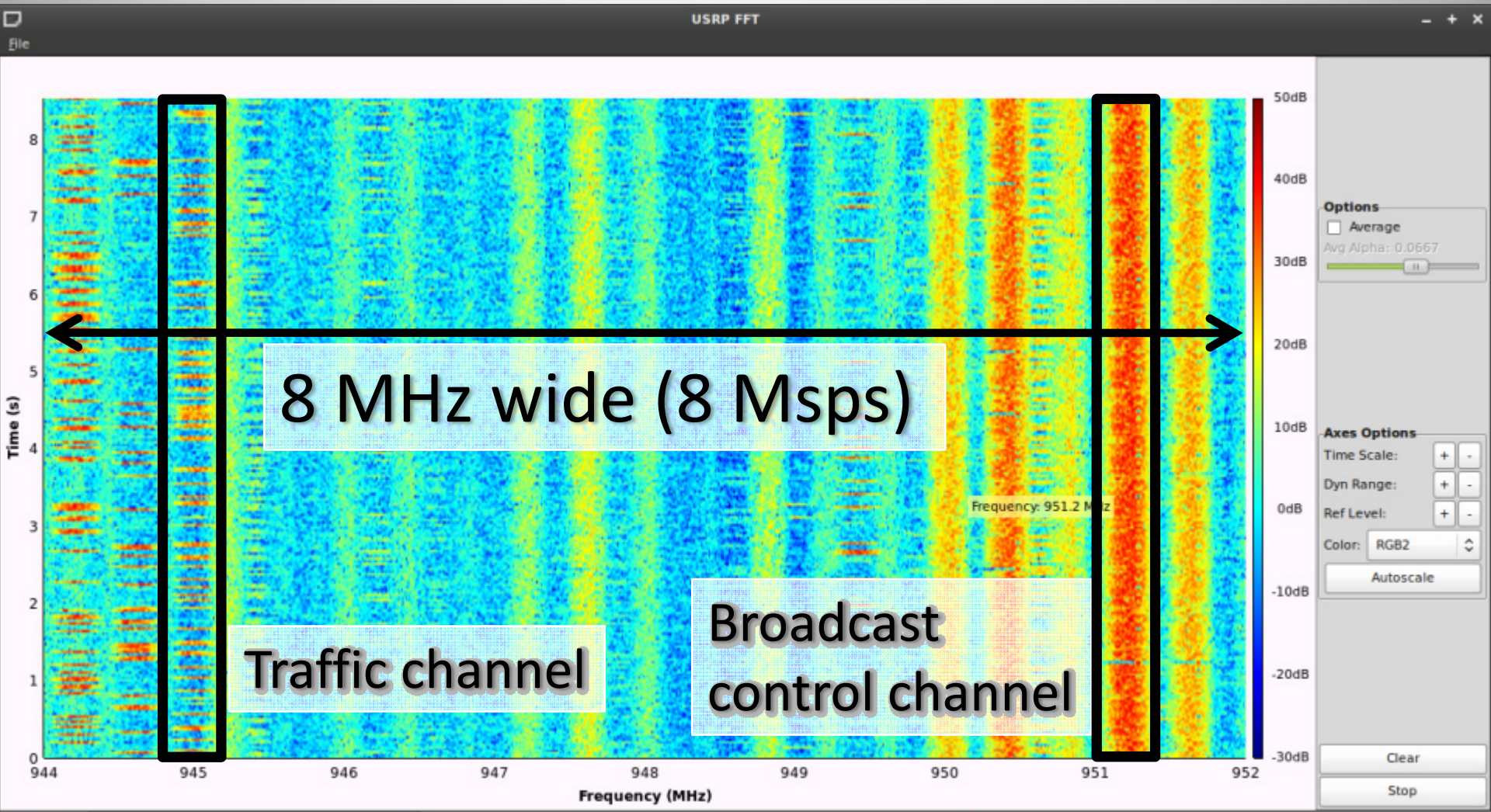


70 MHz – 6 GHz
2x2 MIMO

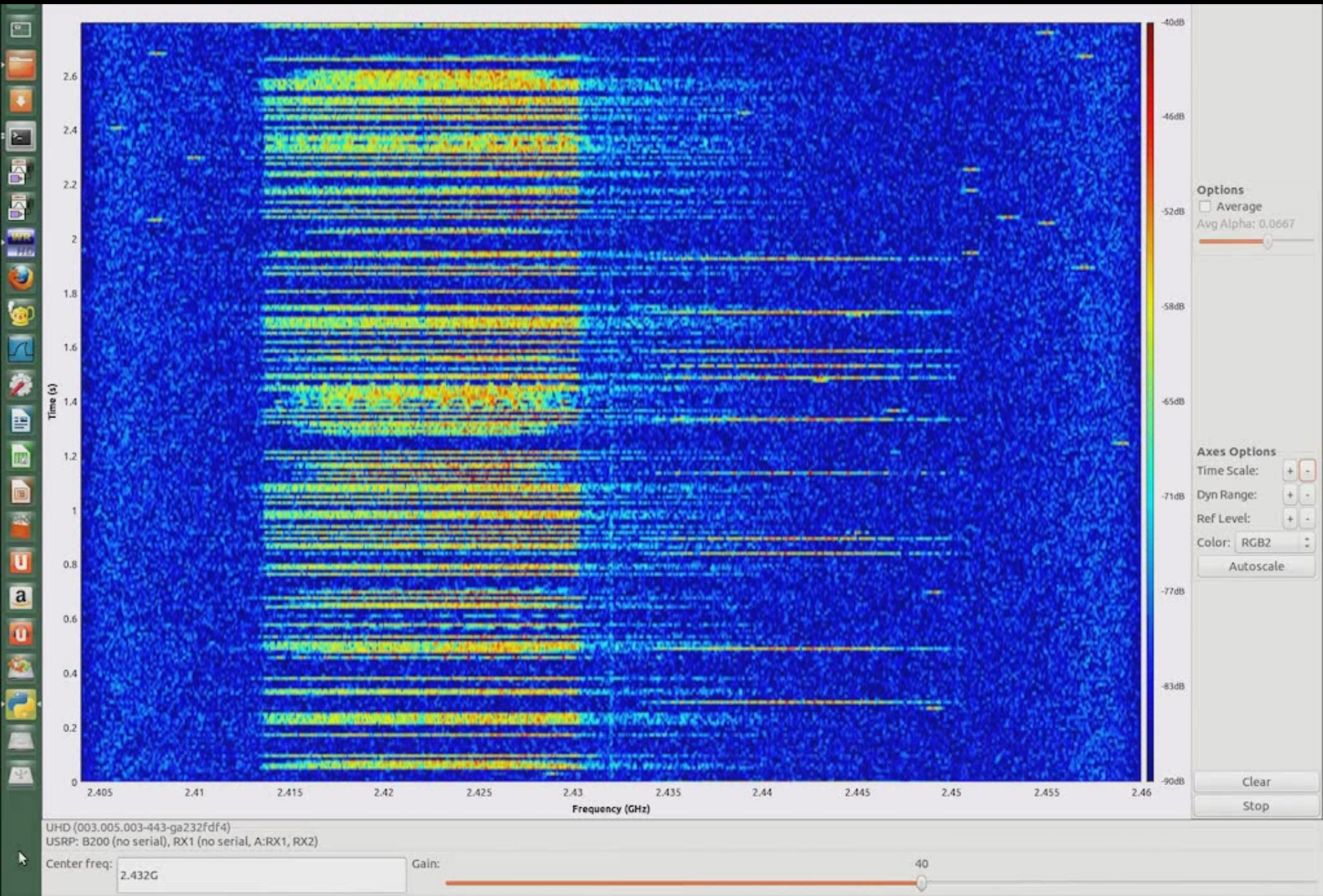
GNU Radio Companion



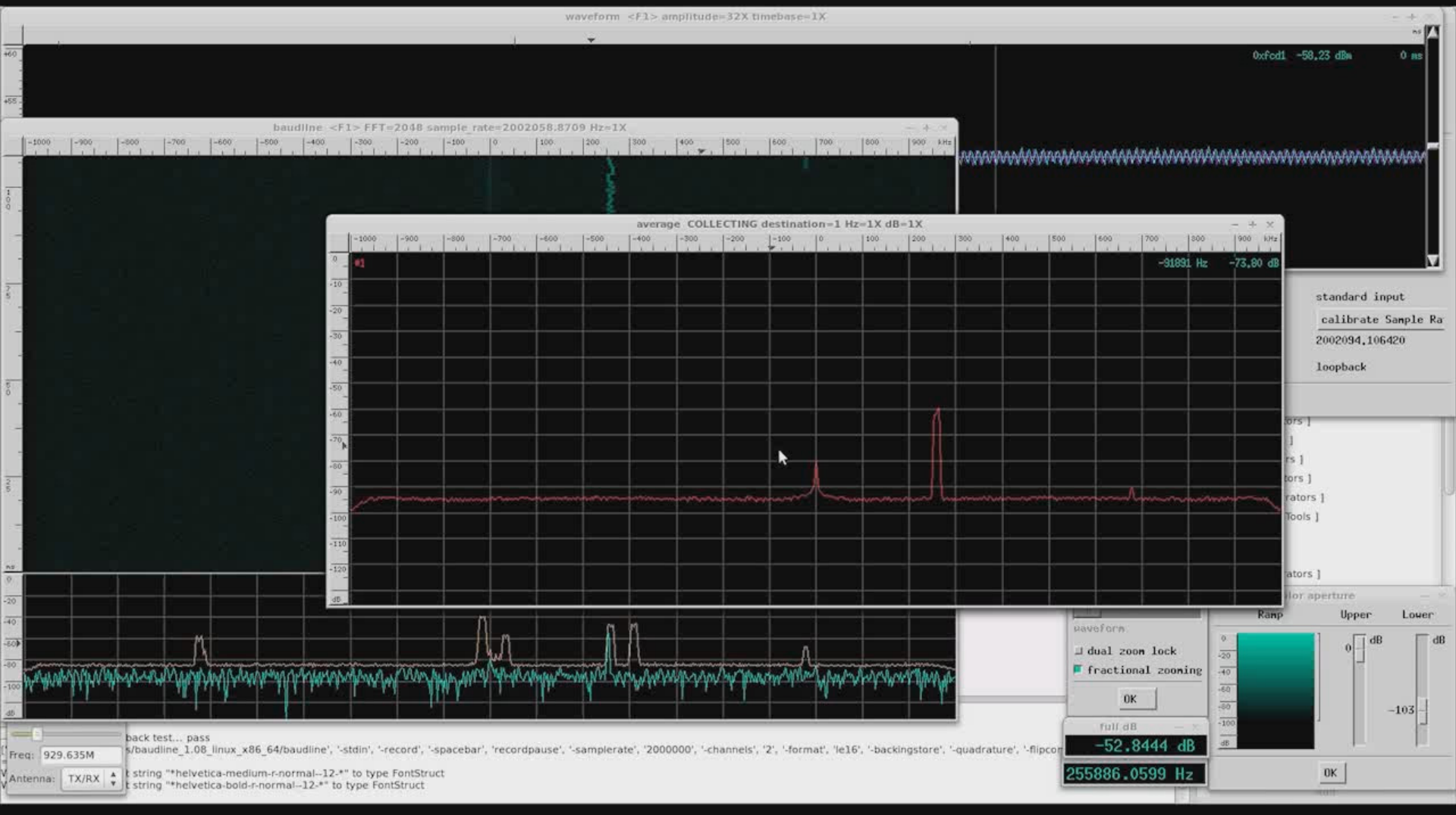
2G GSM Waterfall



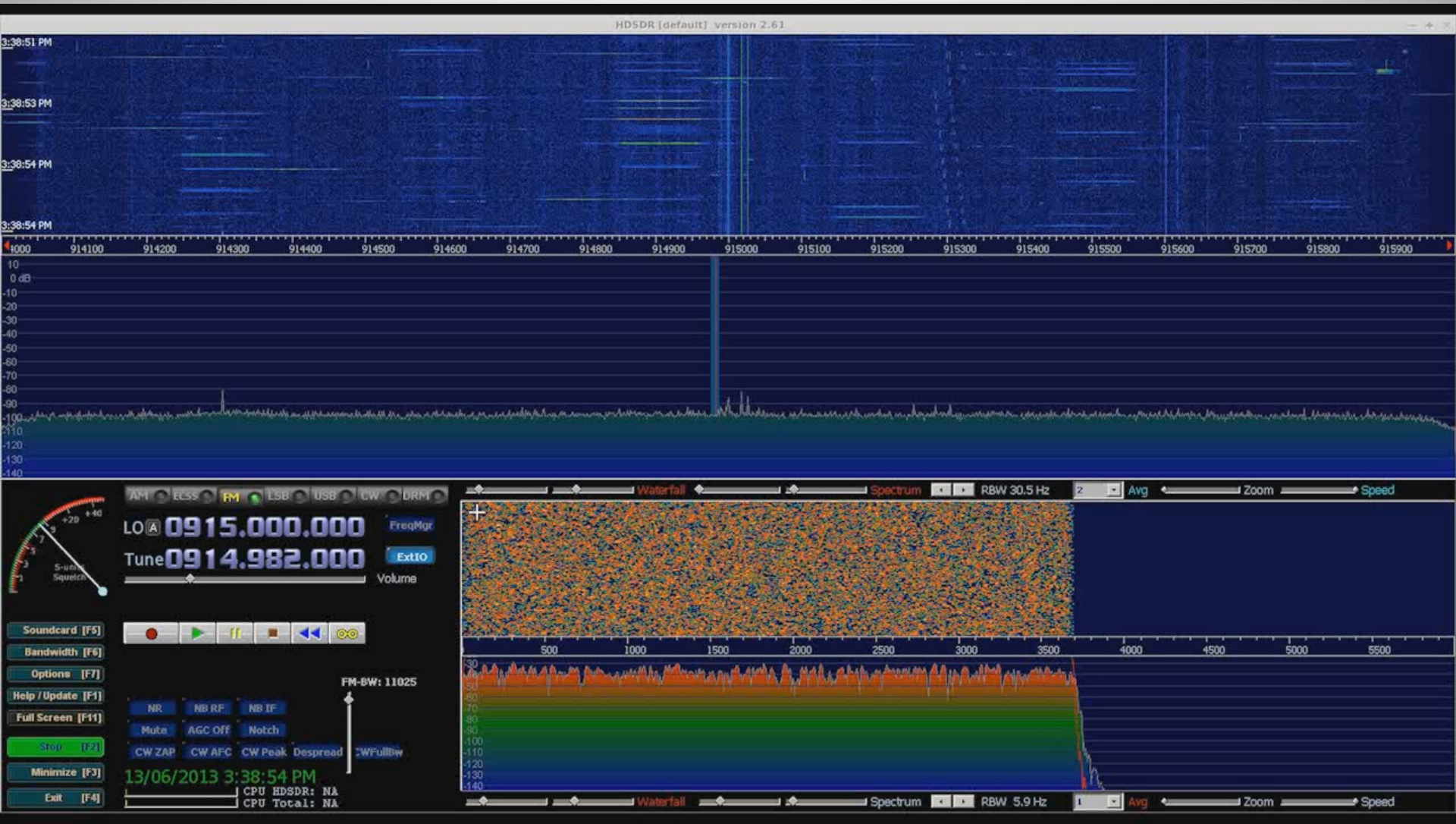
Two WiFi channels, and then some…



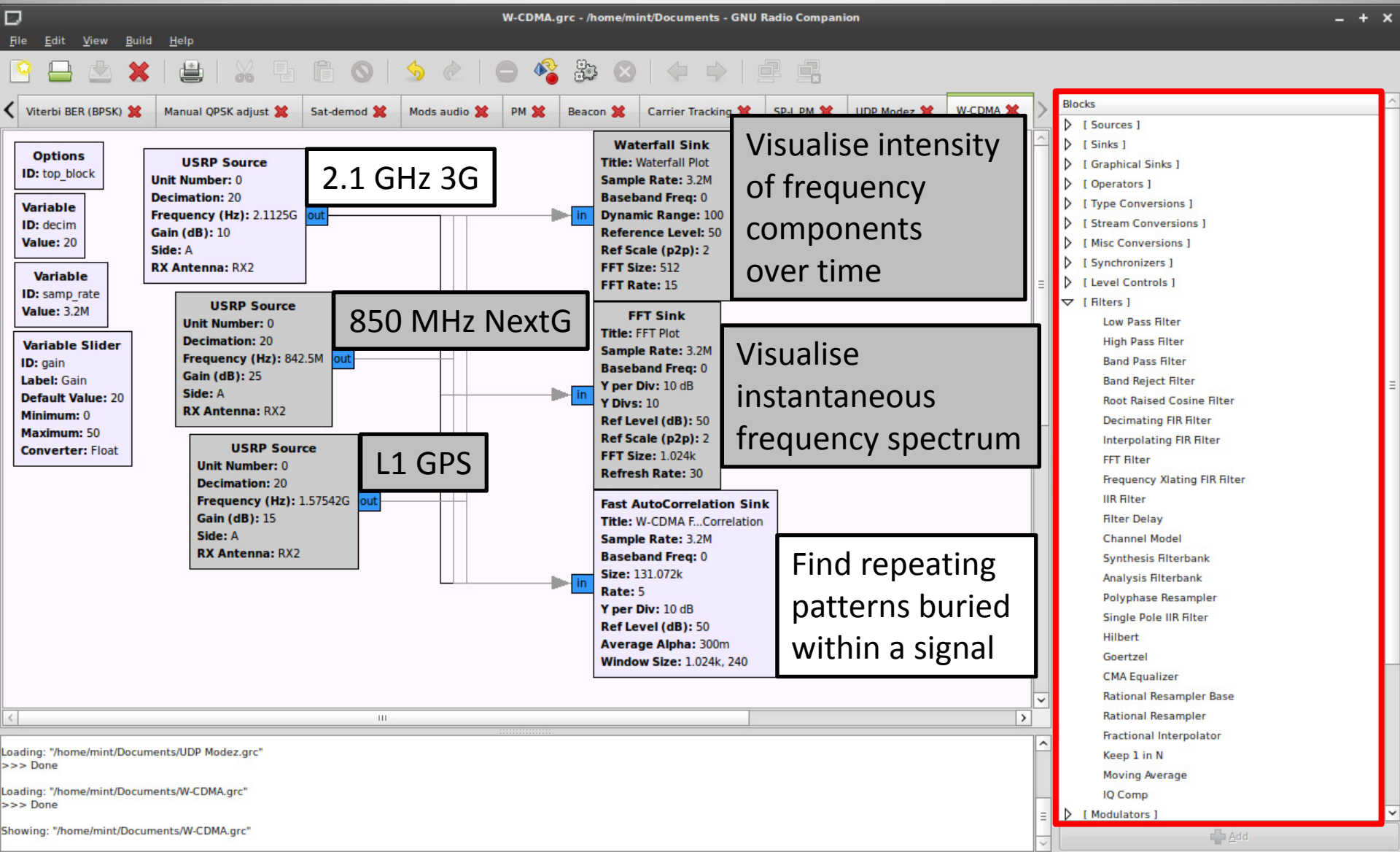
FLEX Pagers & Baudline



900 MHz ISM – Smart Meters

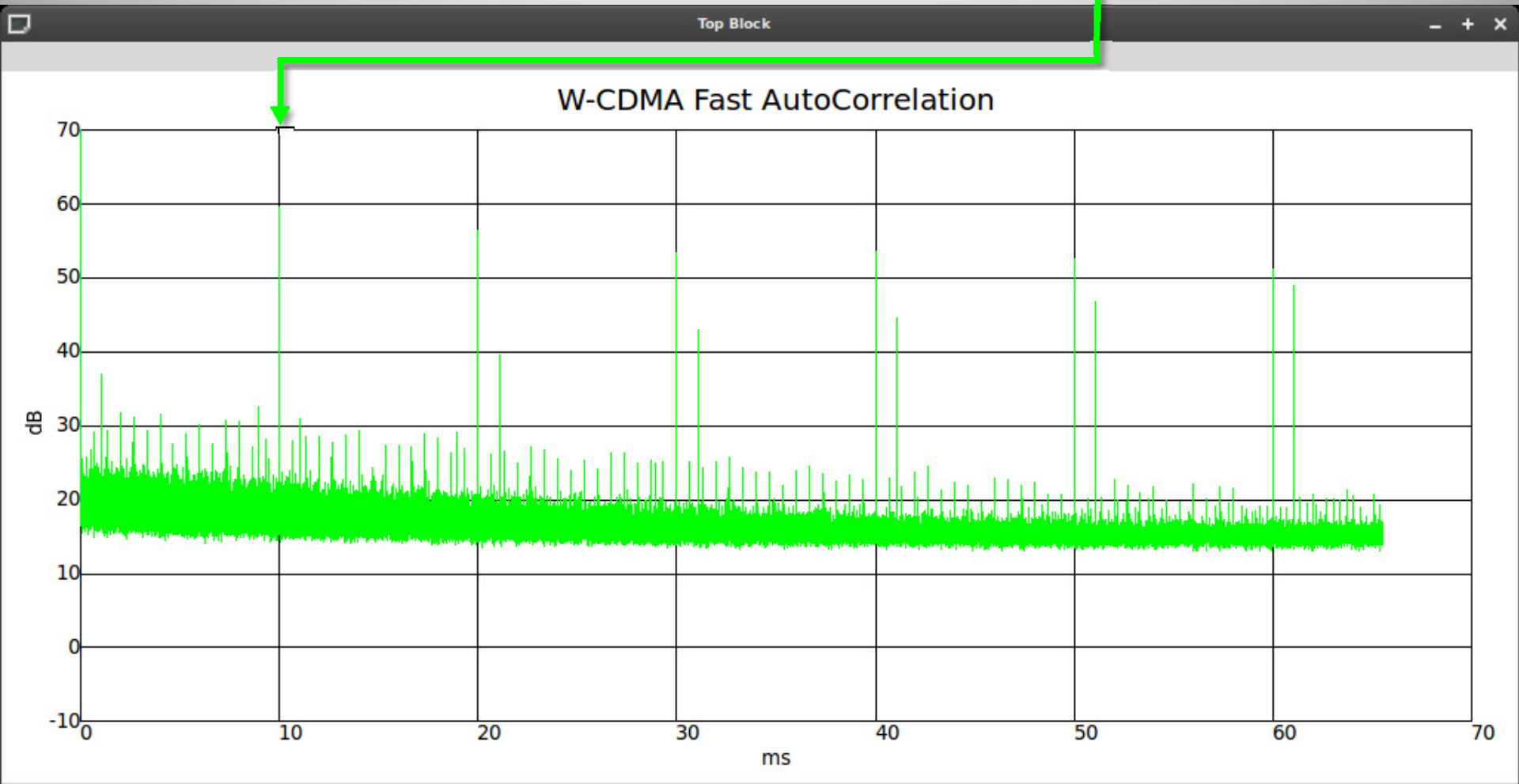


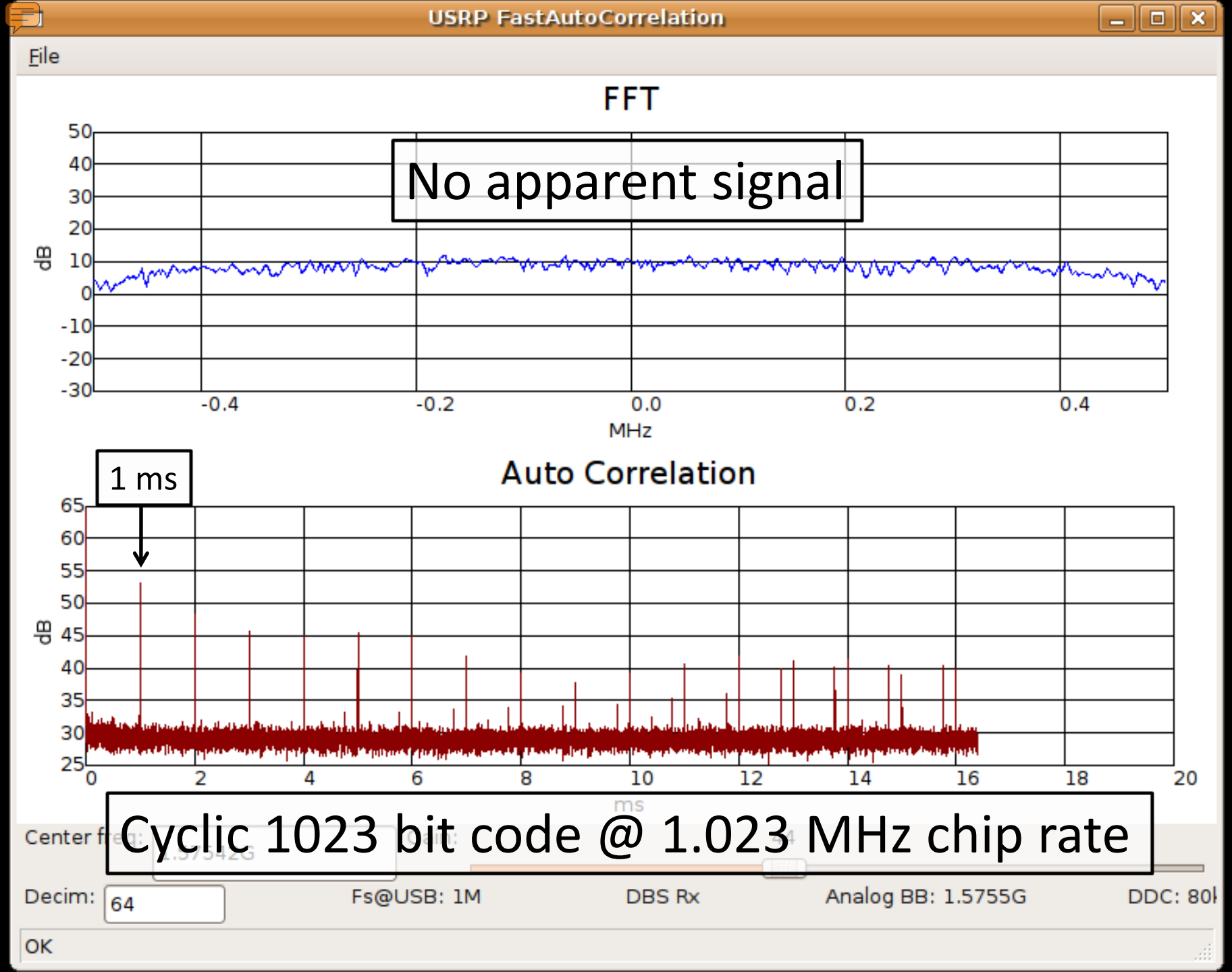
CDMA Detection with GRC



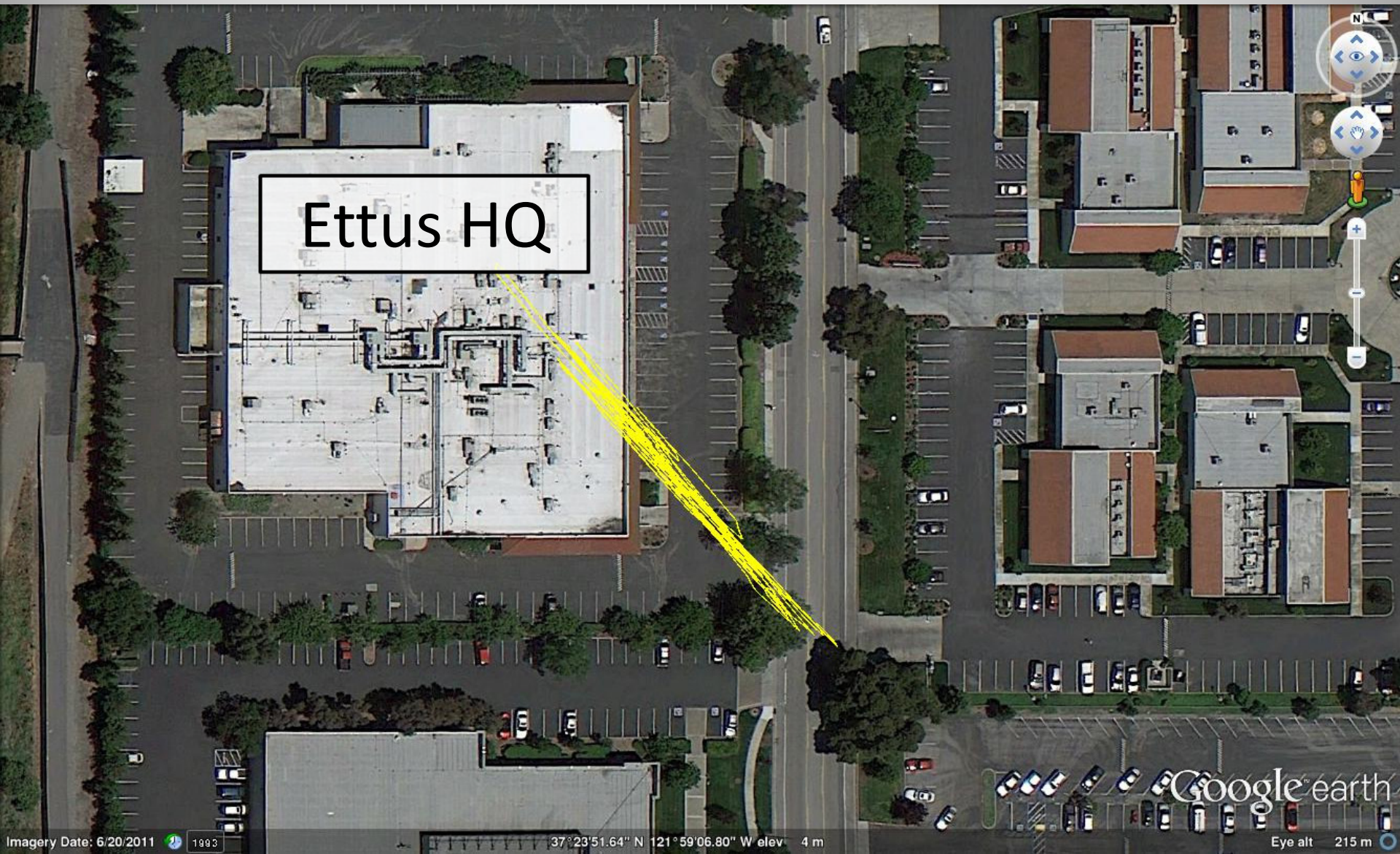
3G W-CDMA

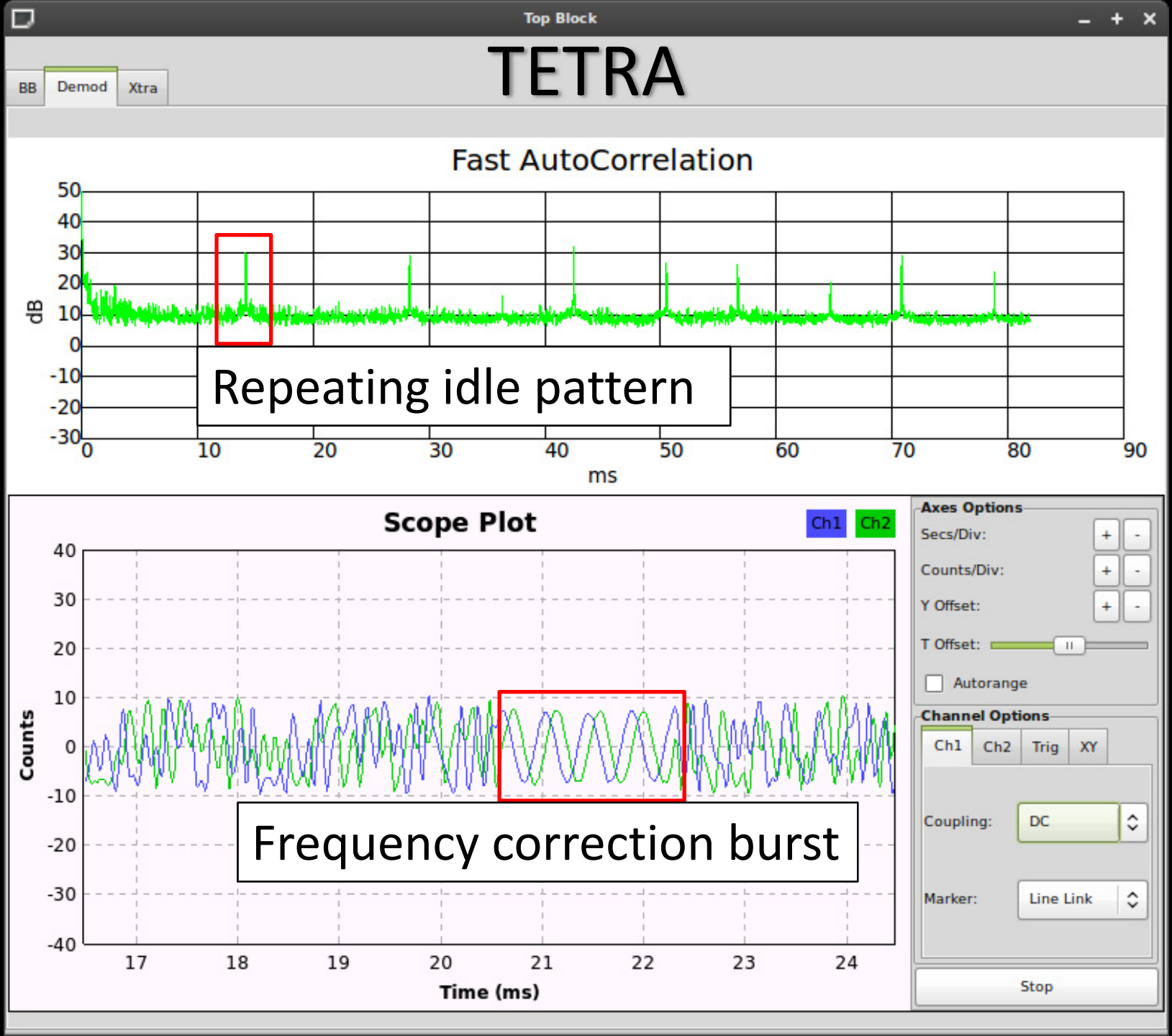
Signature of UMTS: repeating data in CPICH at 10 ms intervals




USRP FastAutoCorrelation
File
FFT
No apparent signal
50
40
30
20
10
0
-10
-20
-30
dB
-0.4
-0.2
0.0
0.2
0.4
MHz
1 ms
Auto Correlation
65
60
55
50
45
40
35
30
25
dB
0
2
4
6
8
10
12
14
16
18
20
ms
Cyclic 1023 bit code @ 1.023 MHz chip rate
Center freq:
Decim:
64
Fs@USB: 1M
DBS Rx
Analog BB: 1.5755G
DDC: 80k
OK

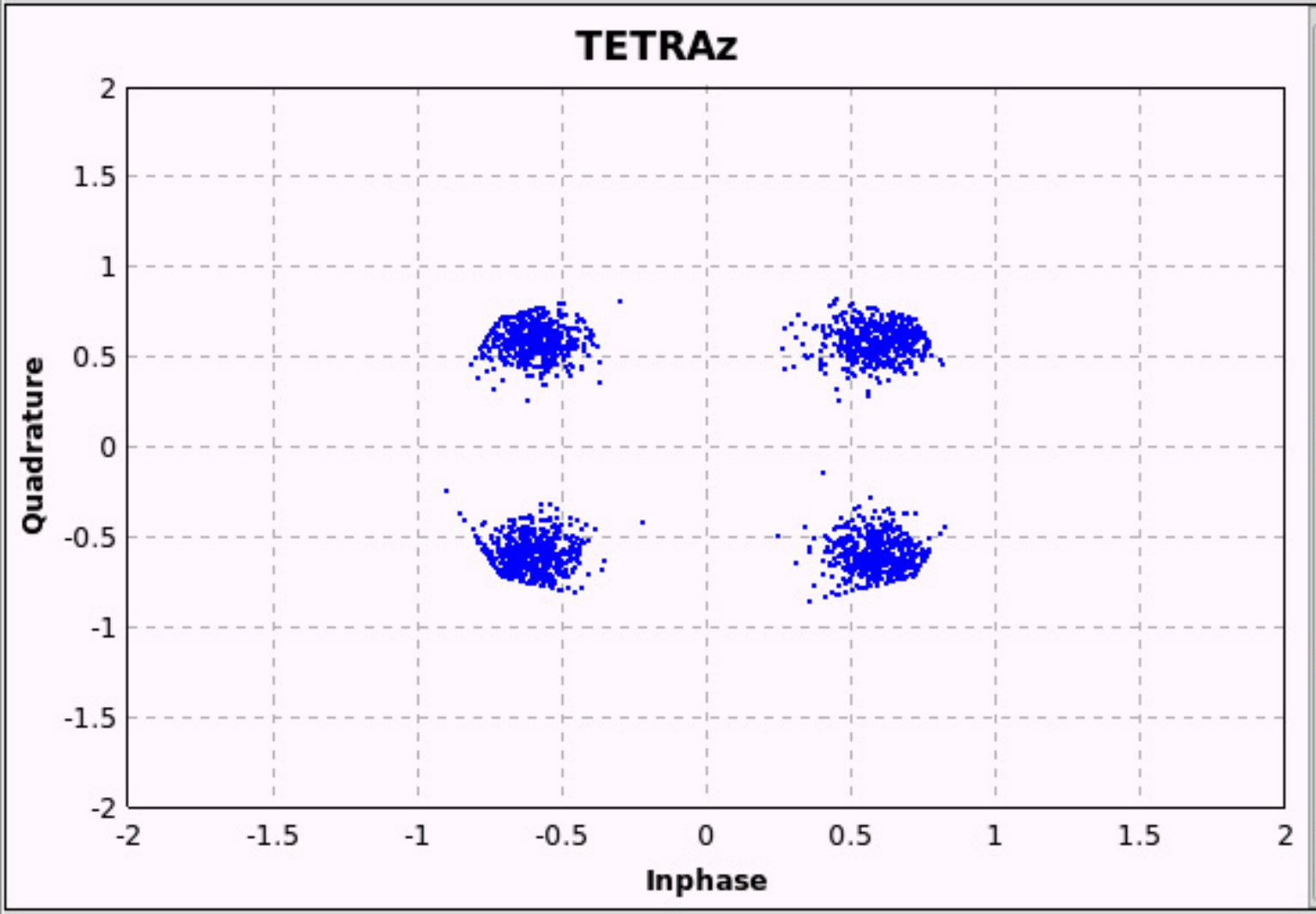
gnss-sdr: Decoding L1




Top Block
TETRA
BB
Demod
Xtra
Fast AutoCorrelation
dB
ms
Repeating idle pattern
Scope Plot
Ch1
Ch2
Counts
Time (ms)
Frequency correction burst
Axes Options
Secs/Div:
Counts/Div:
Y Offset:
T Offset:
Autorange
Channel Options
Ch1
Ch2
Trig
XY
Coupling:
DC
Marker:
Line Link
Stop

Top Block

BB | Demod | Xtra



Options

Alpha: 10m

Gain Mu: 50m

Marker: Dot Medium

Stop

TETRA

Sat Demod

BB | Scope | Demod | Pow | Cyclo | FAC | # | Quad | Mag | Test

Symbol rate (fine): 0

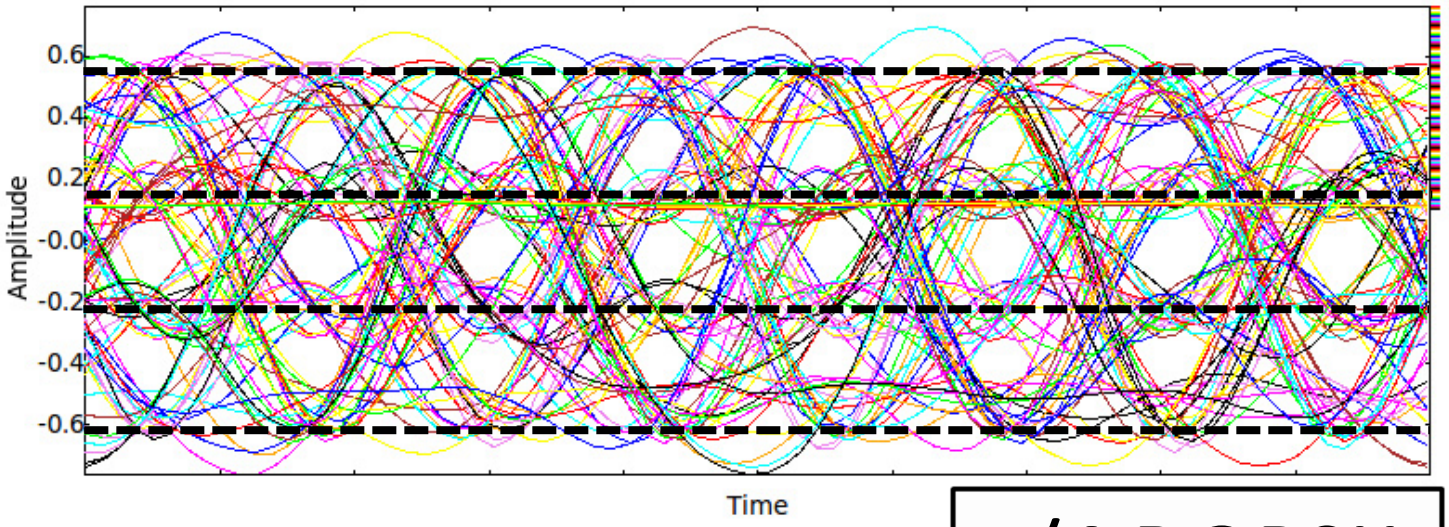
Symbol rate (coarse): 0

Symbol rate: 18000

Samples per symbol: 80

Num plots: 100

Data Scope



π/4 DQPSK

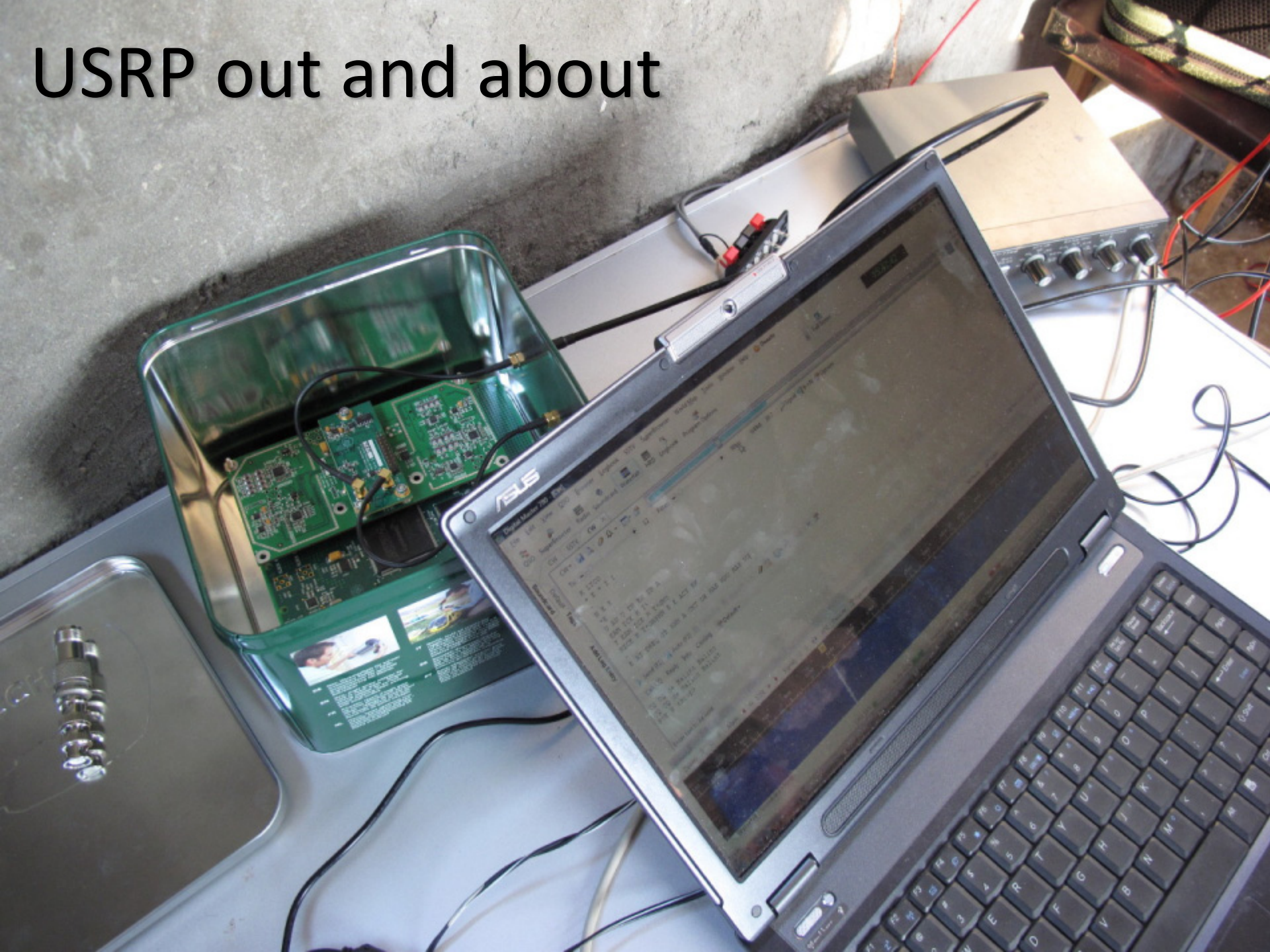
Fine Offset: 0

Coarse offset: 0

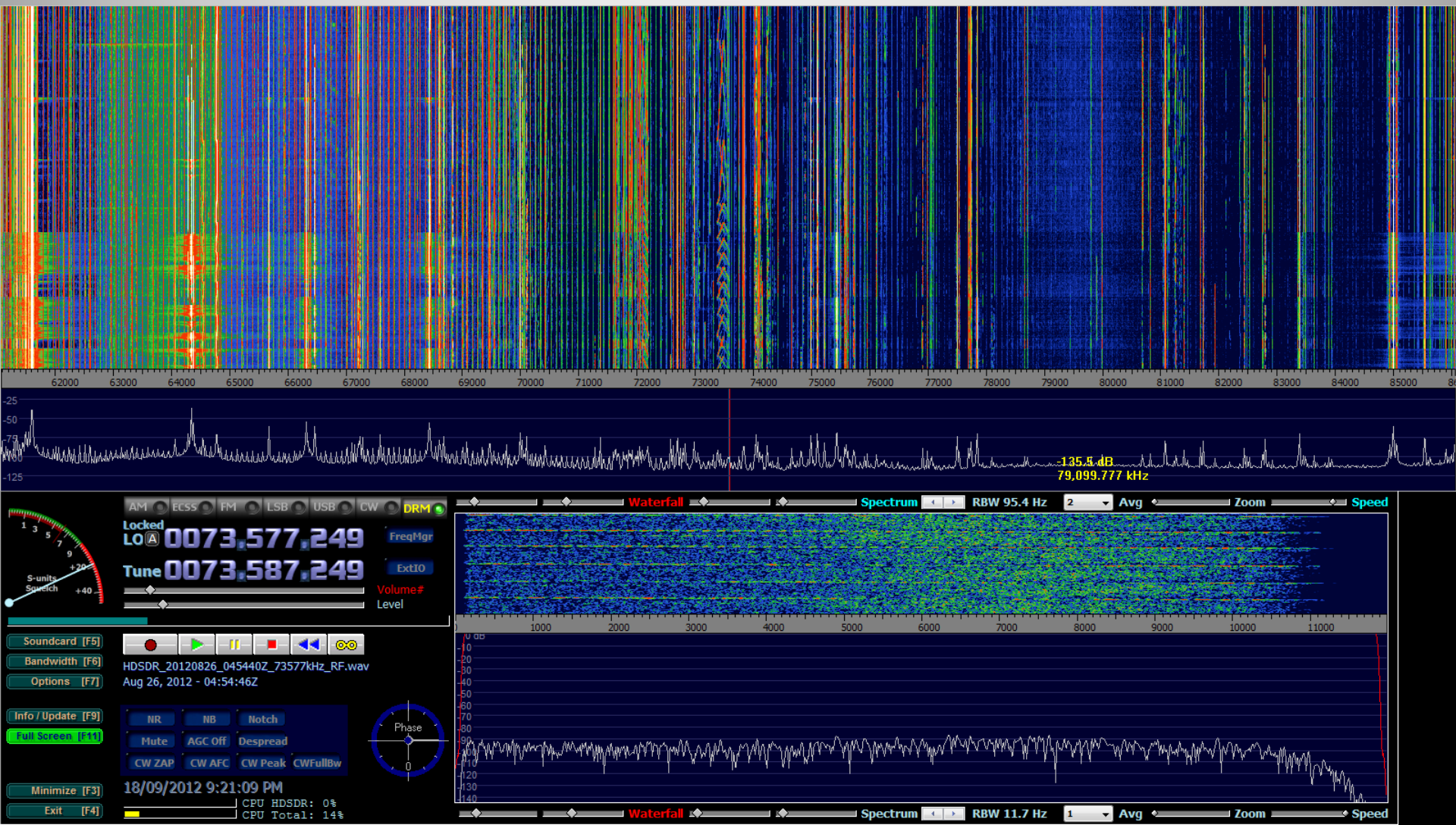
Xlate Offset: 117.708k

Xlate BW: 34.4375k

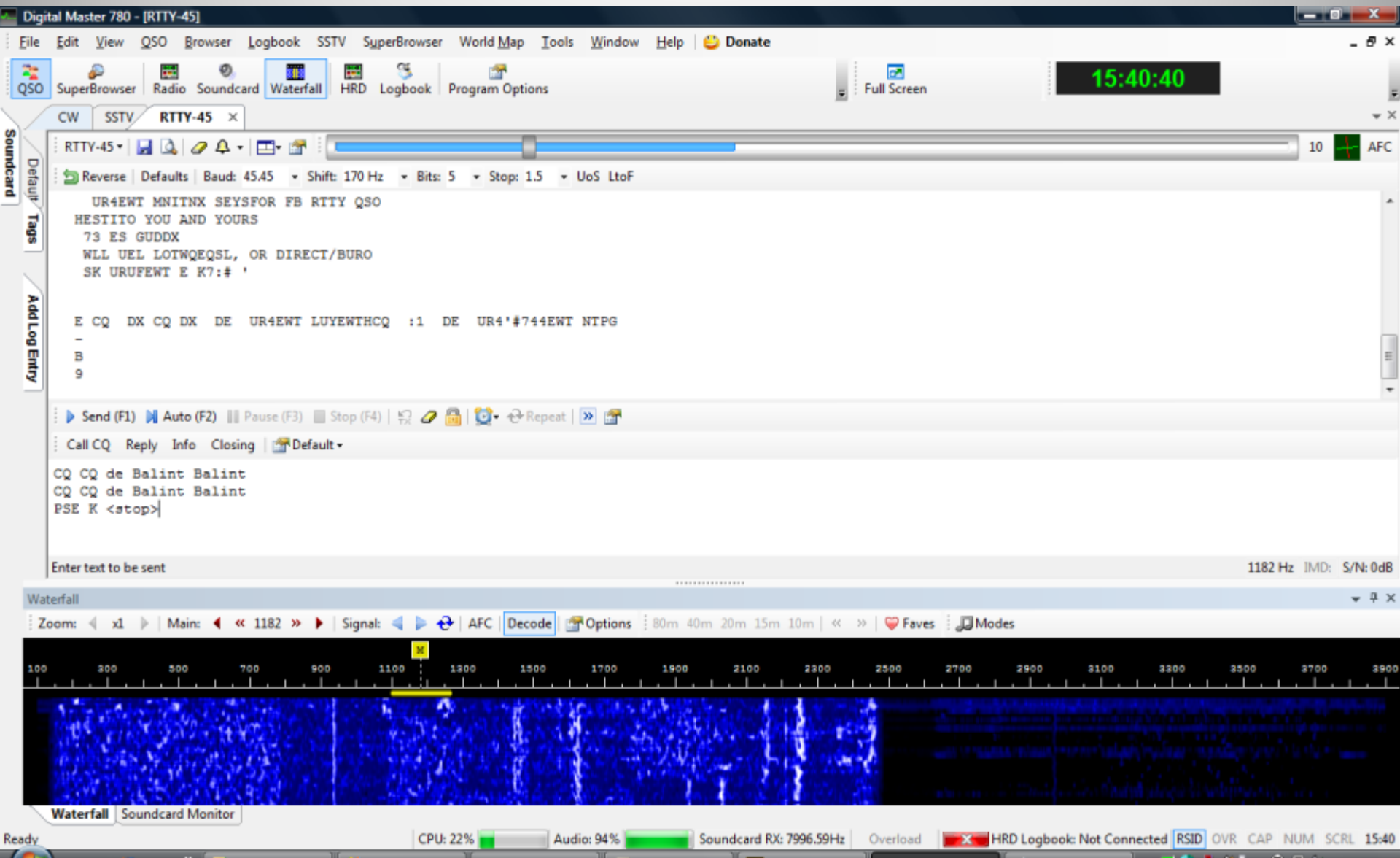
USRP out and about



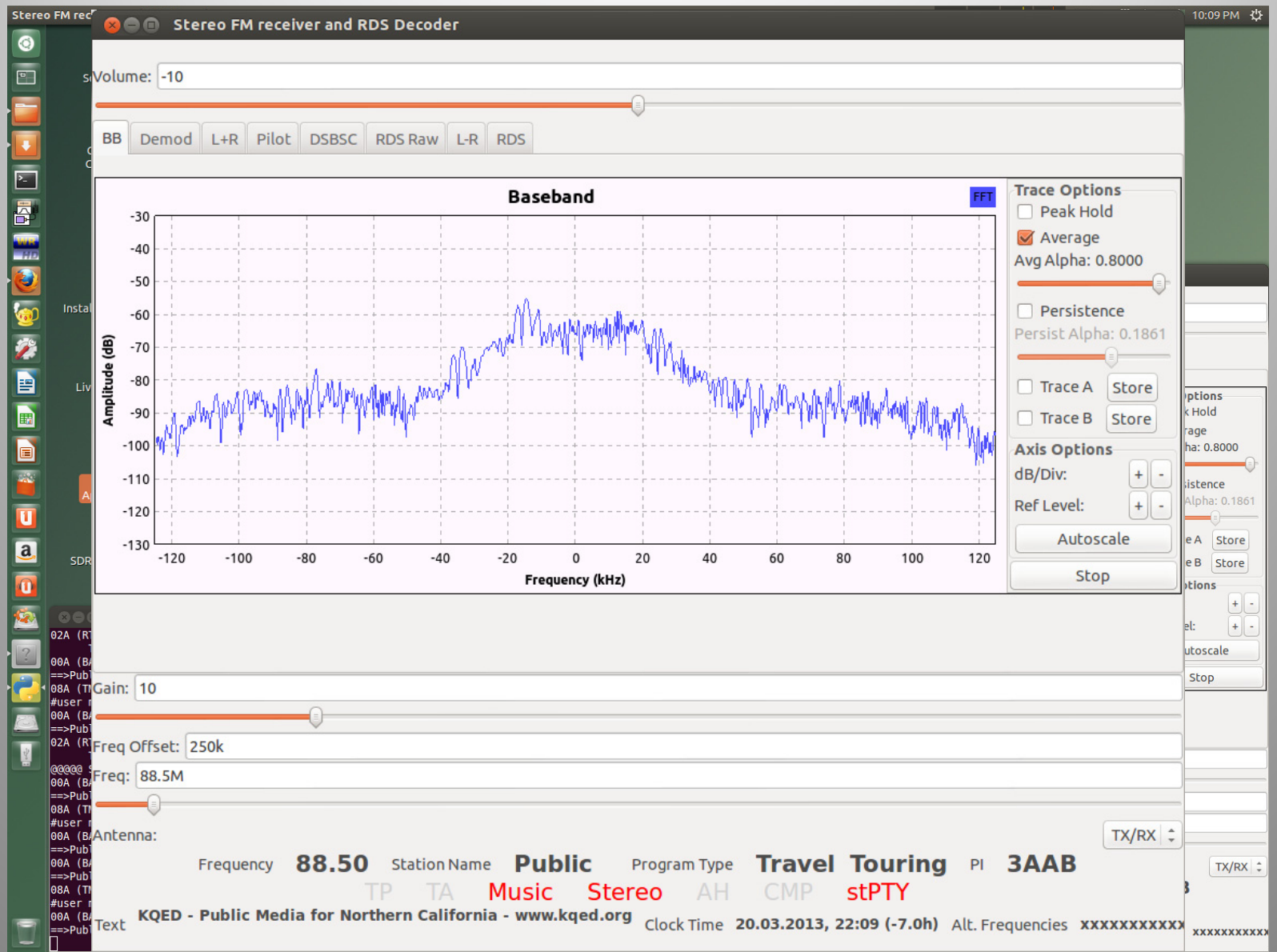
The Entire HAM Band



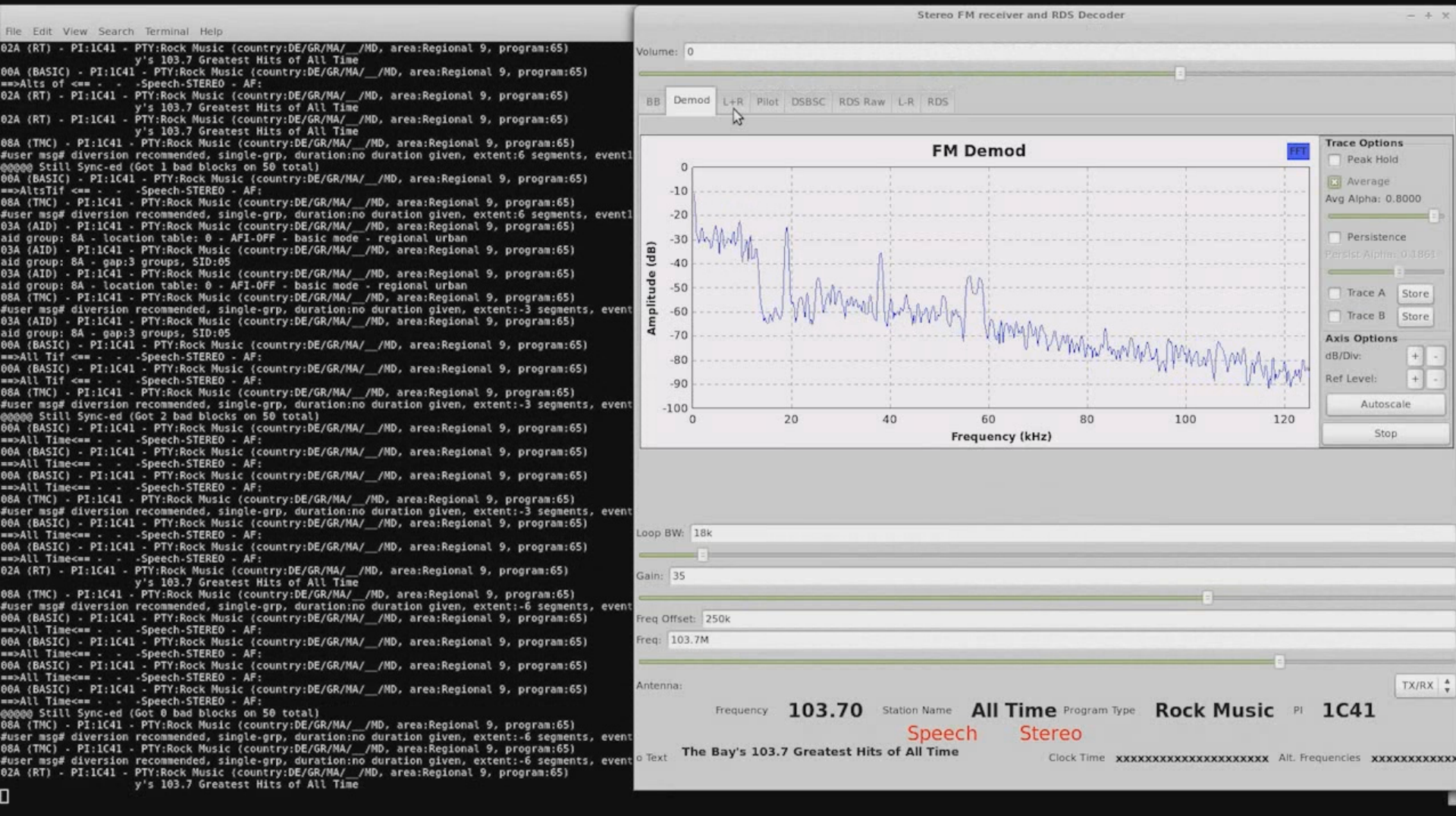
Amateur Digital Modes



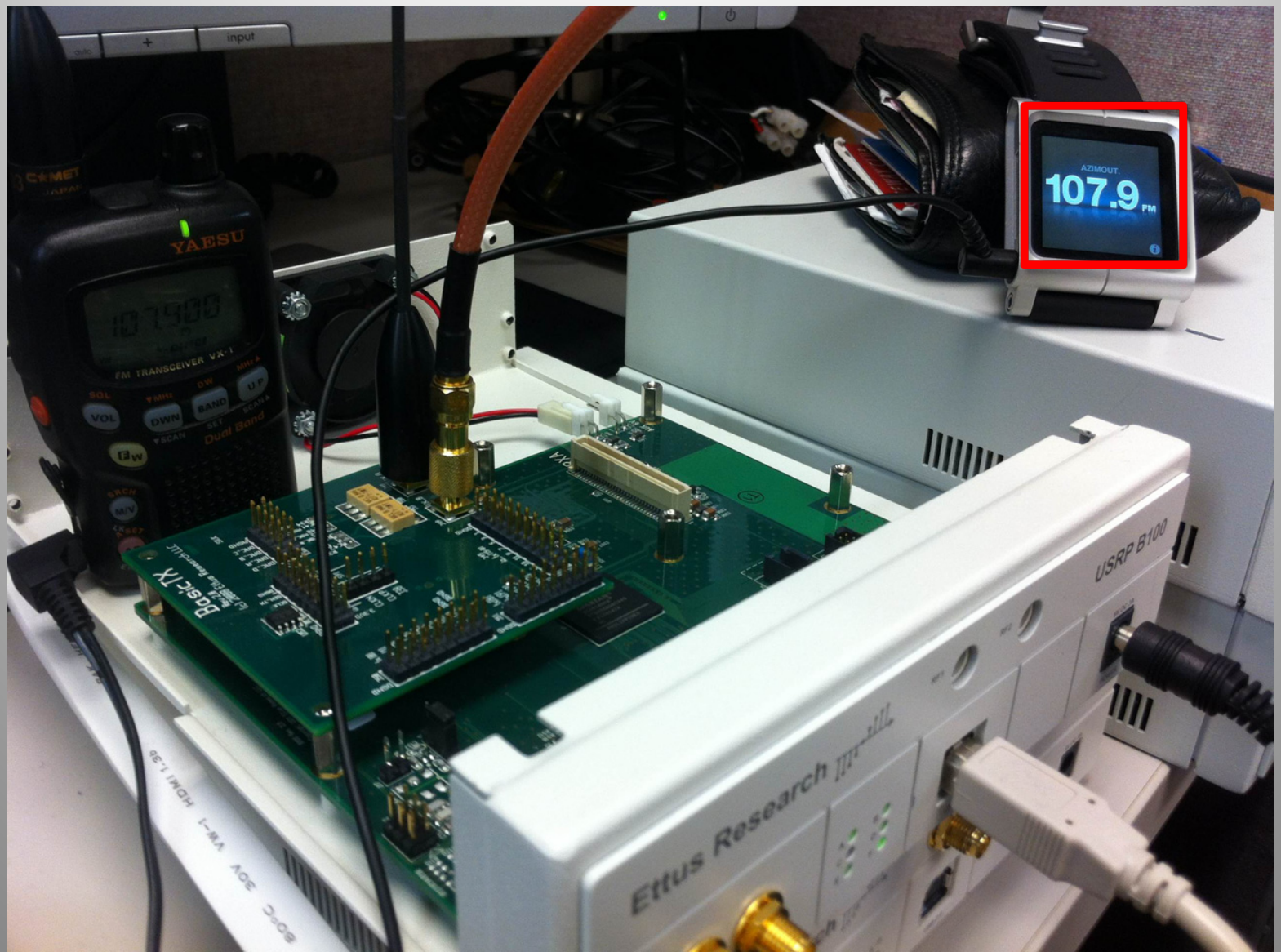
Stereo FM with RDS: Receiver



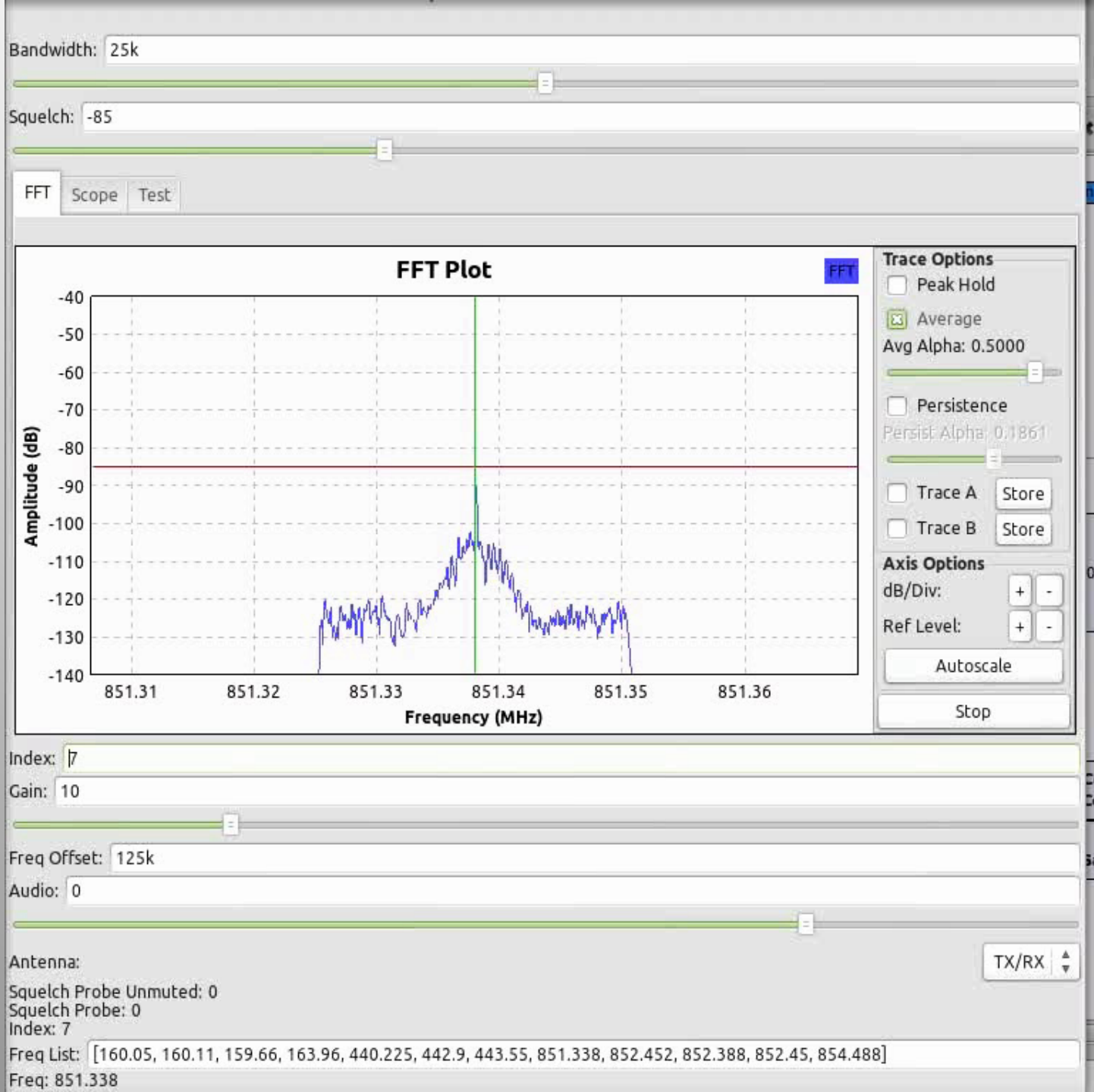
Stereo FM with RDS: Receiver



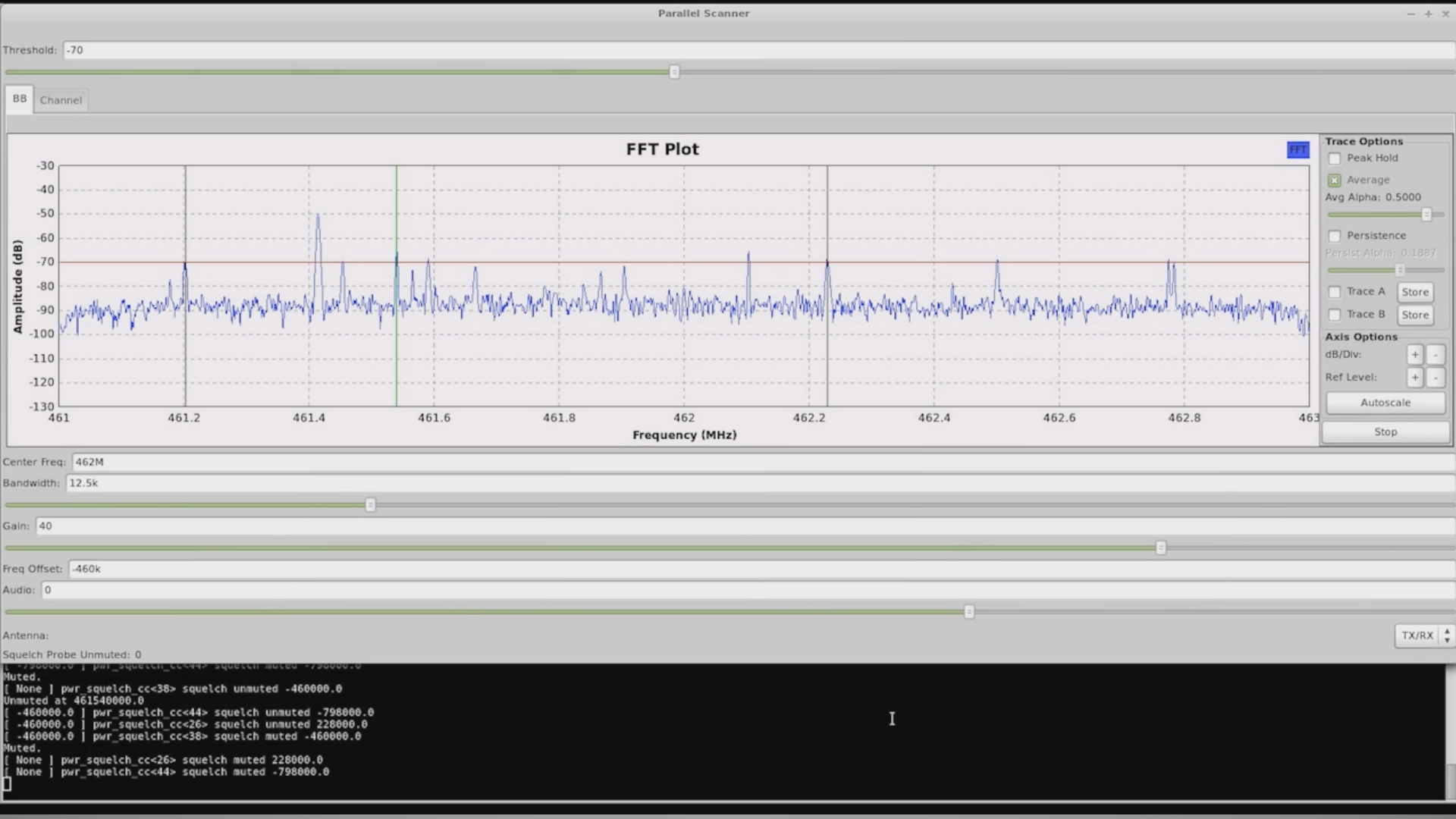
Stereo FM with RDS: Transmitter



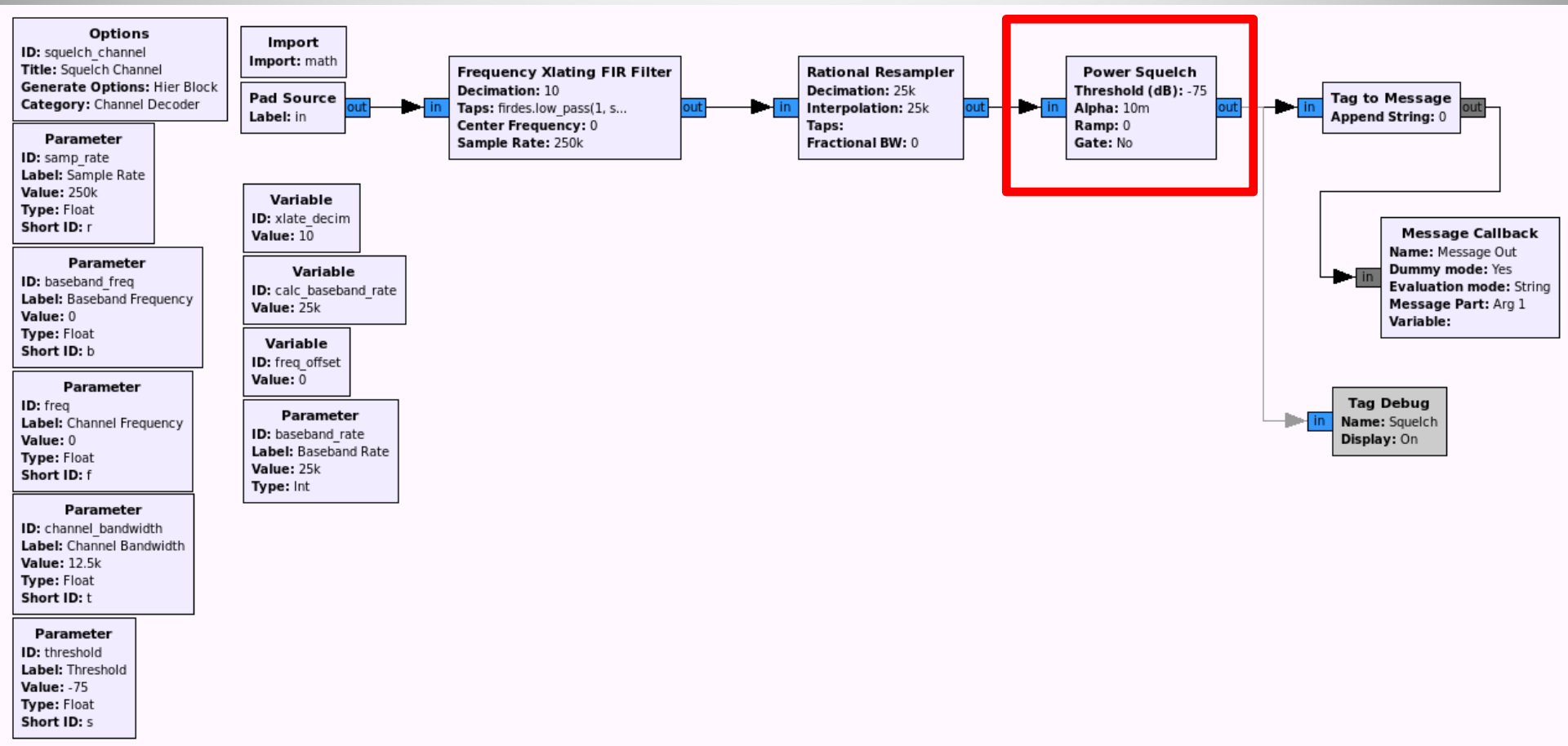
Sequential Scanning



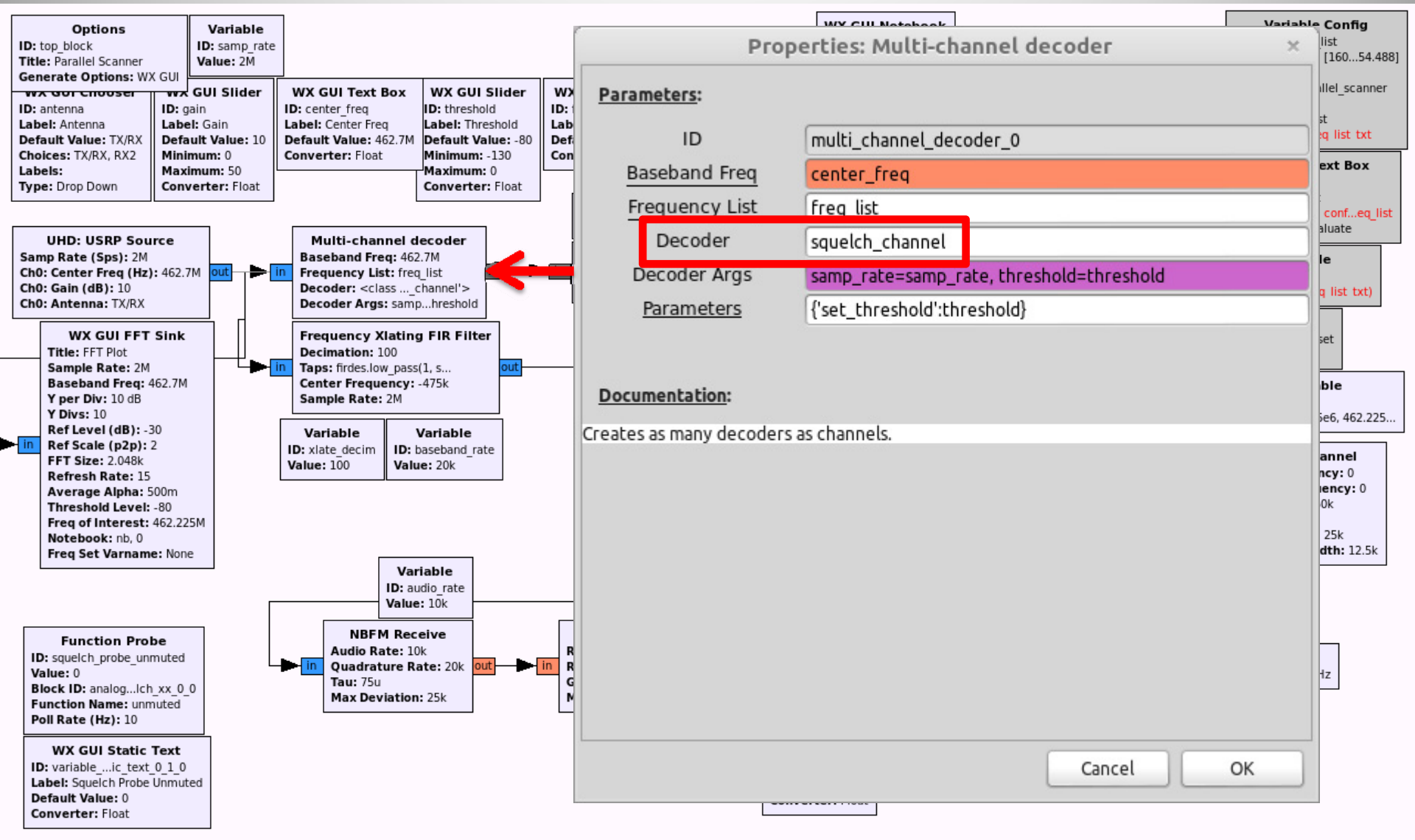
Parallel Decoding



Parallel Decoding: 1

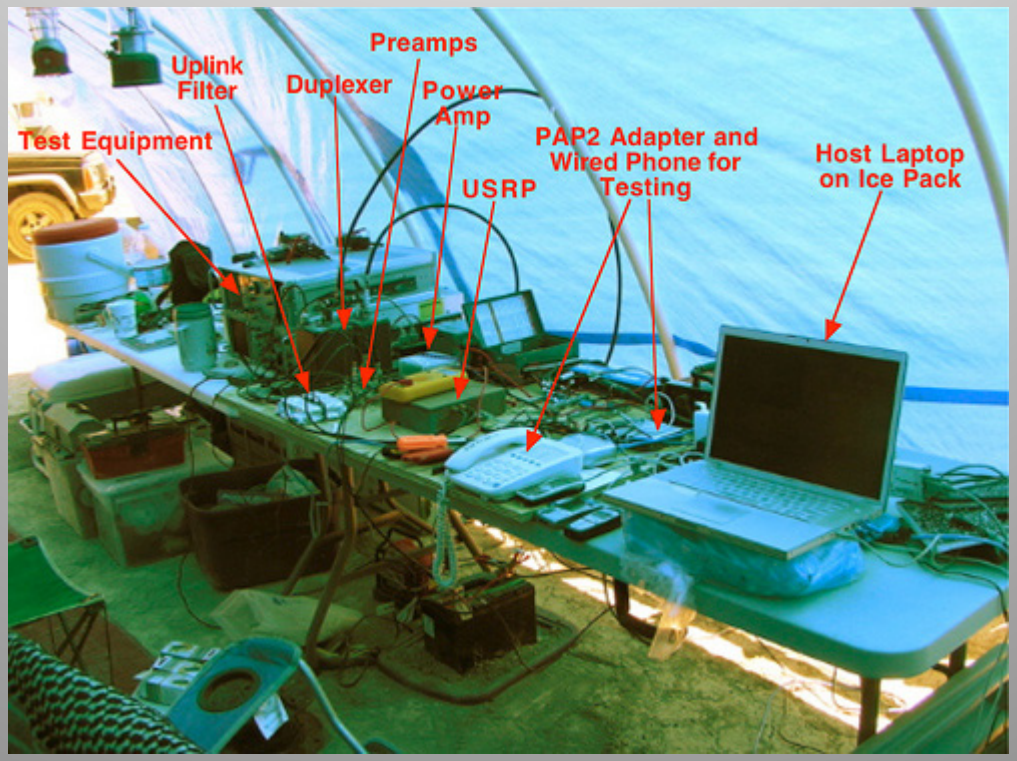


Parallel Decoding: N

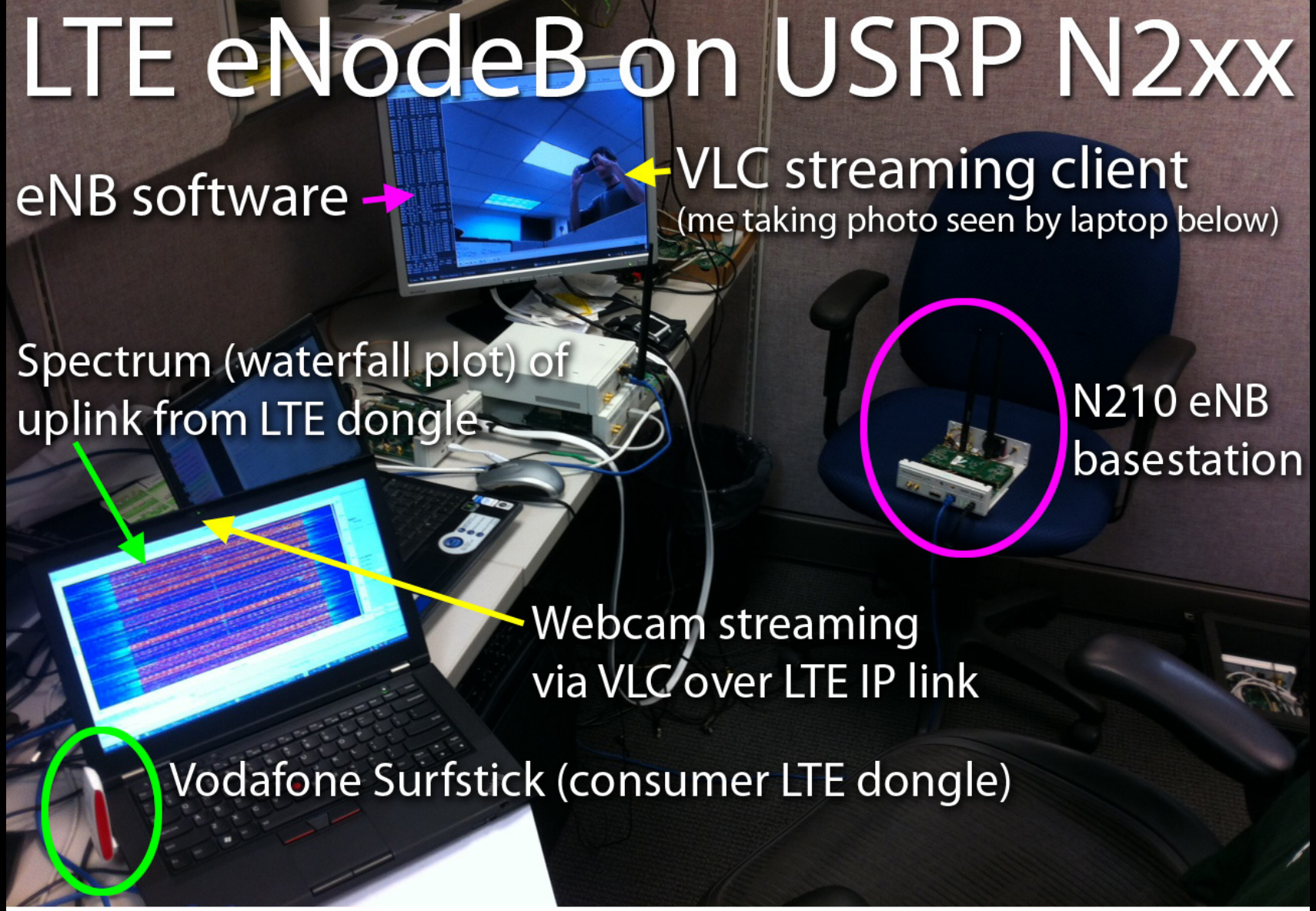


OpenBTS

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



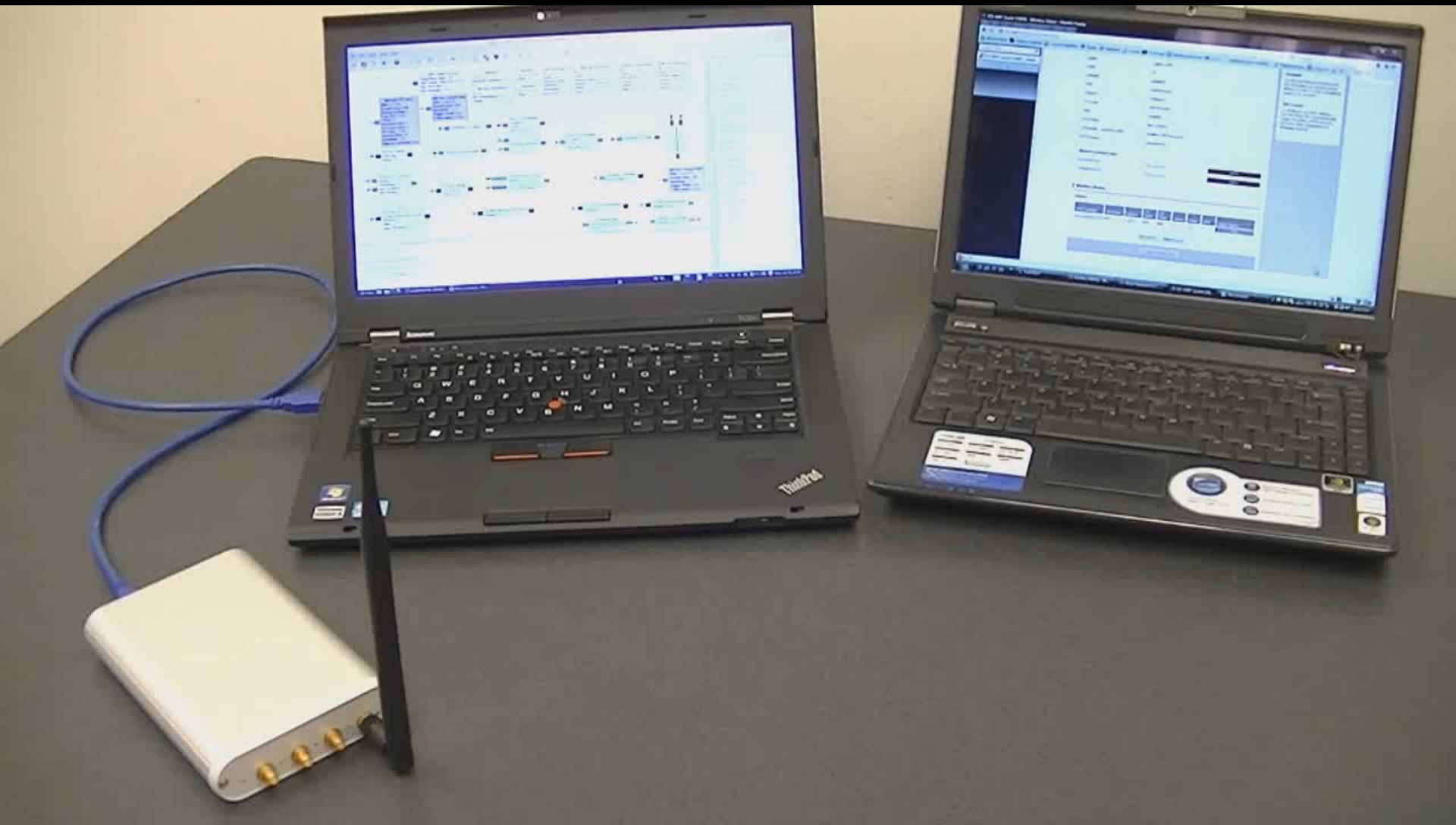
LTE eNodeB on USRP N2xx



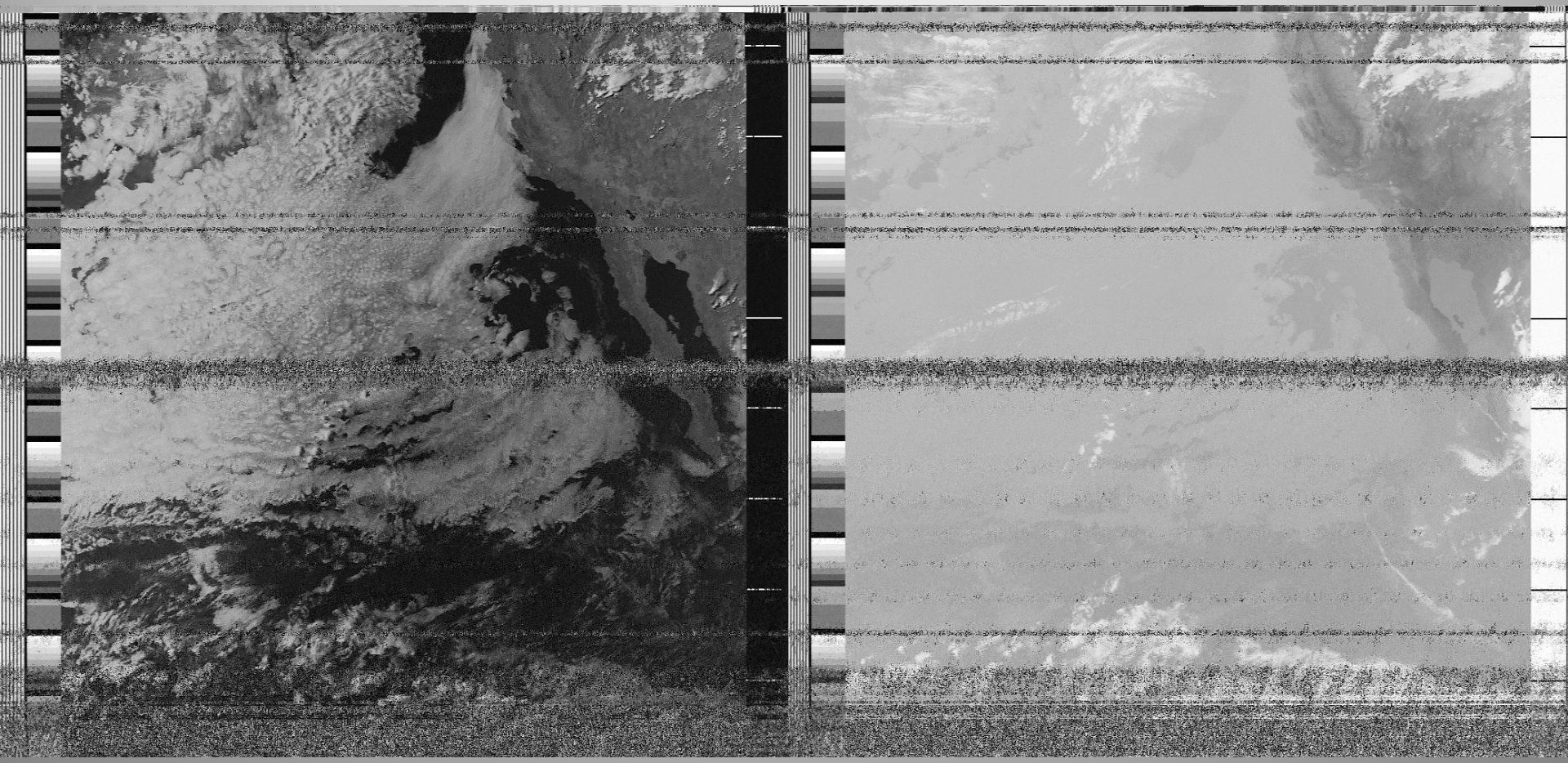
amarisoft

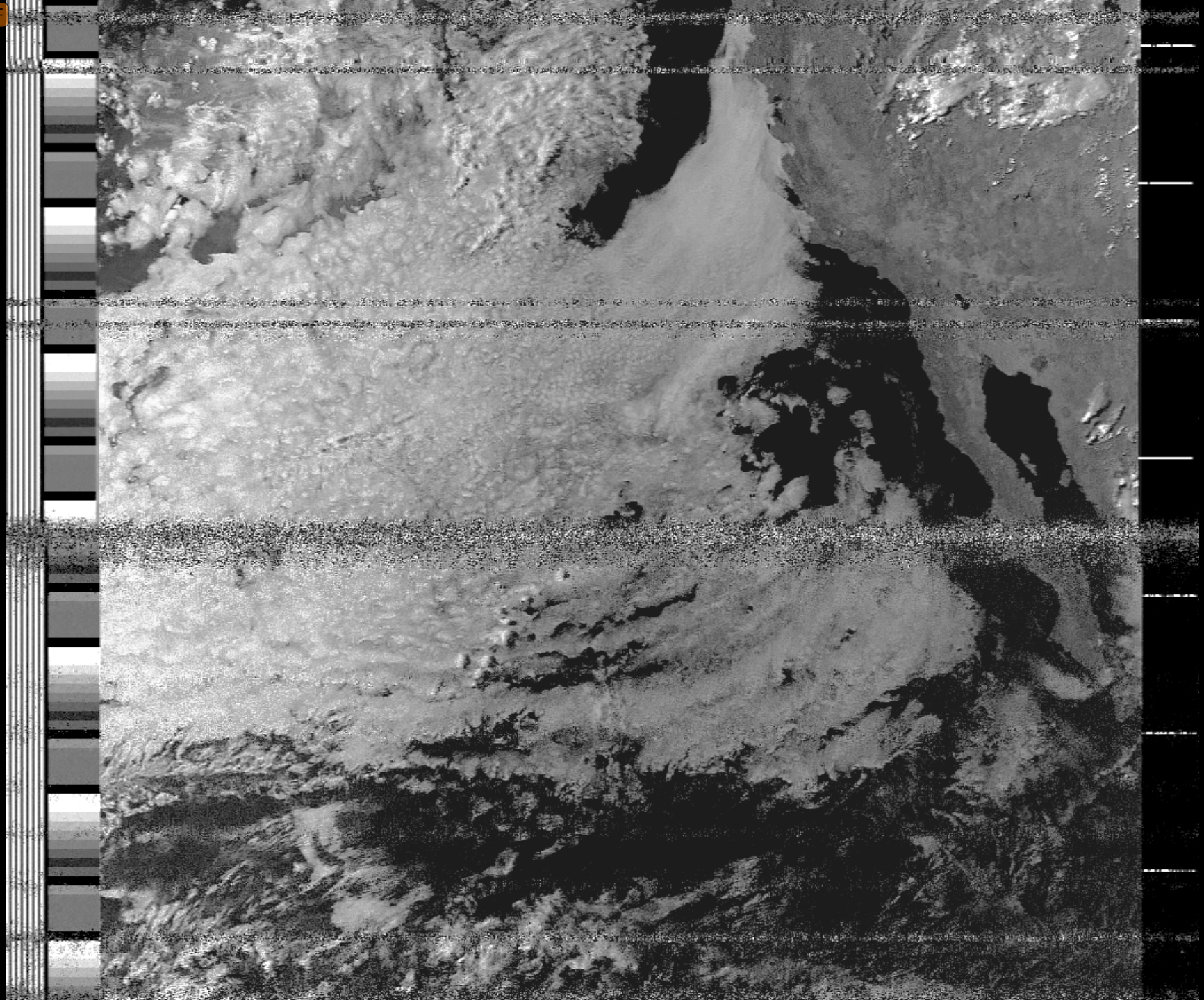
Ettus Research

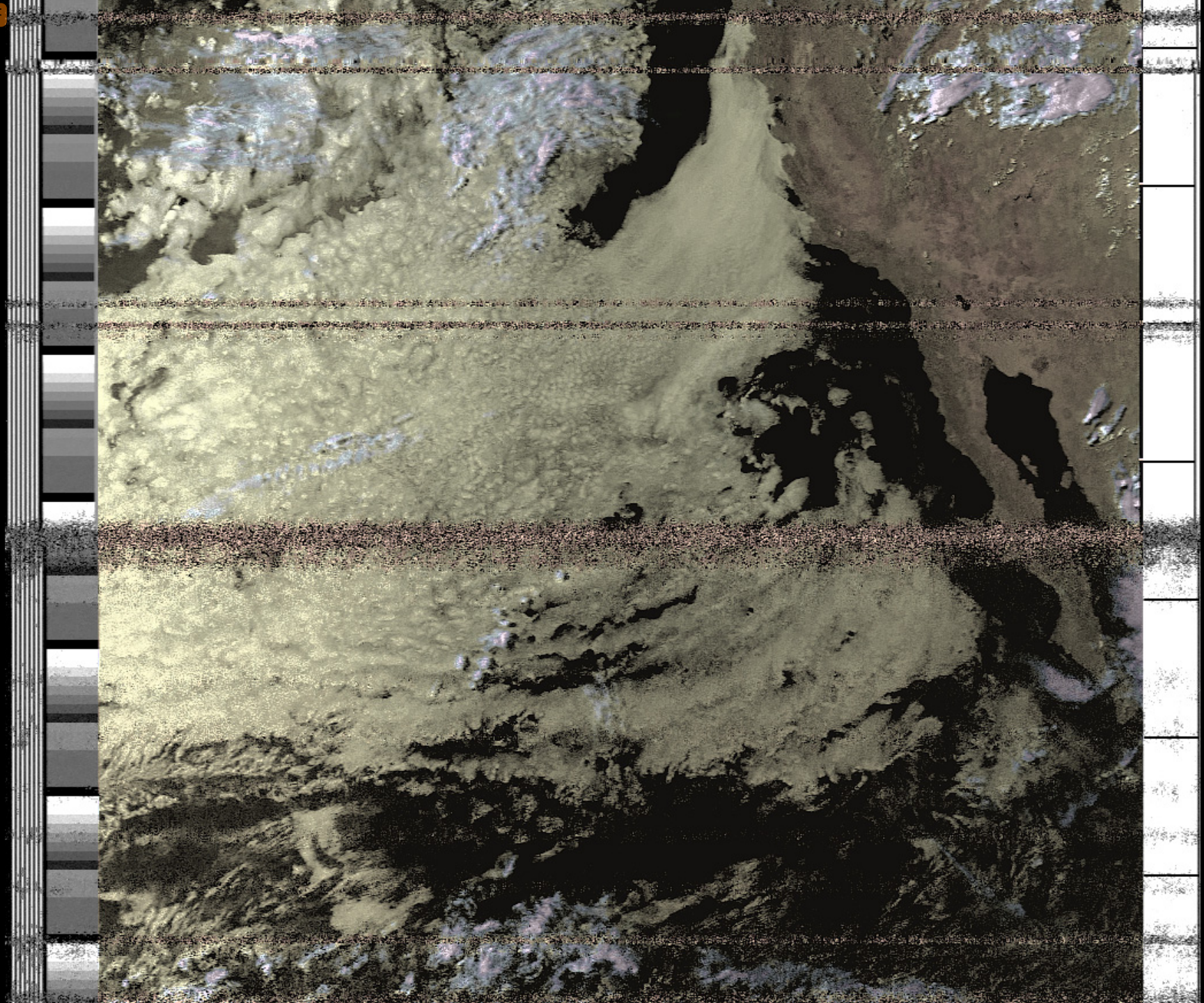
802.11agp (OFDM) Decoding

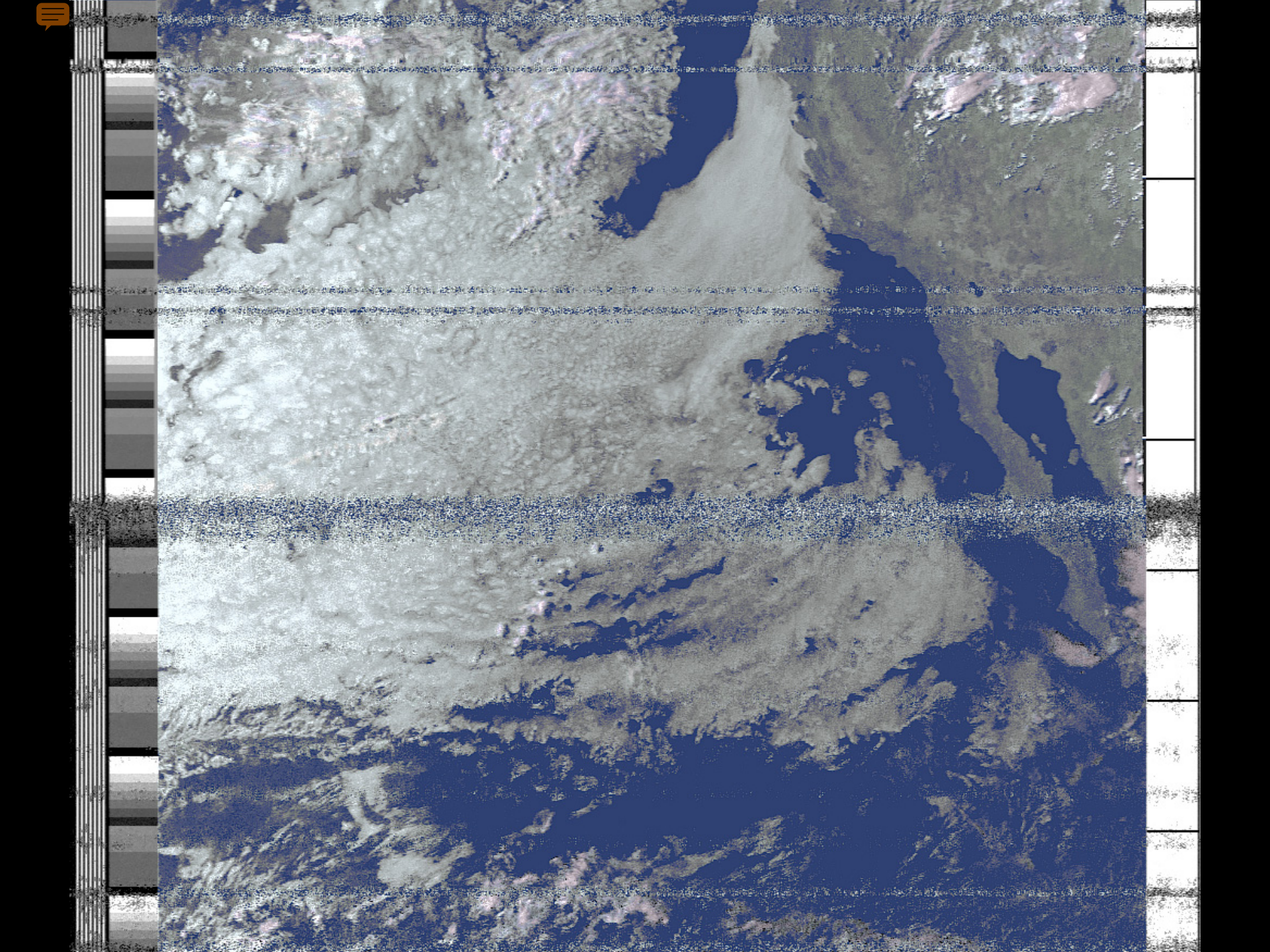


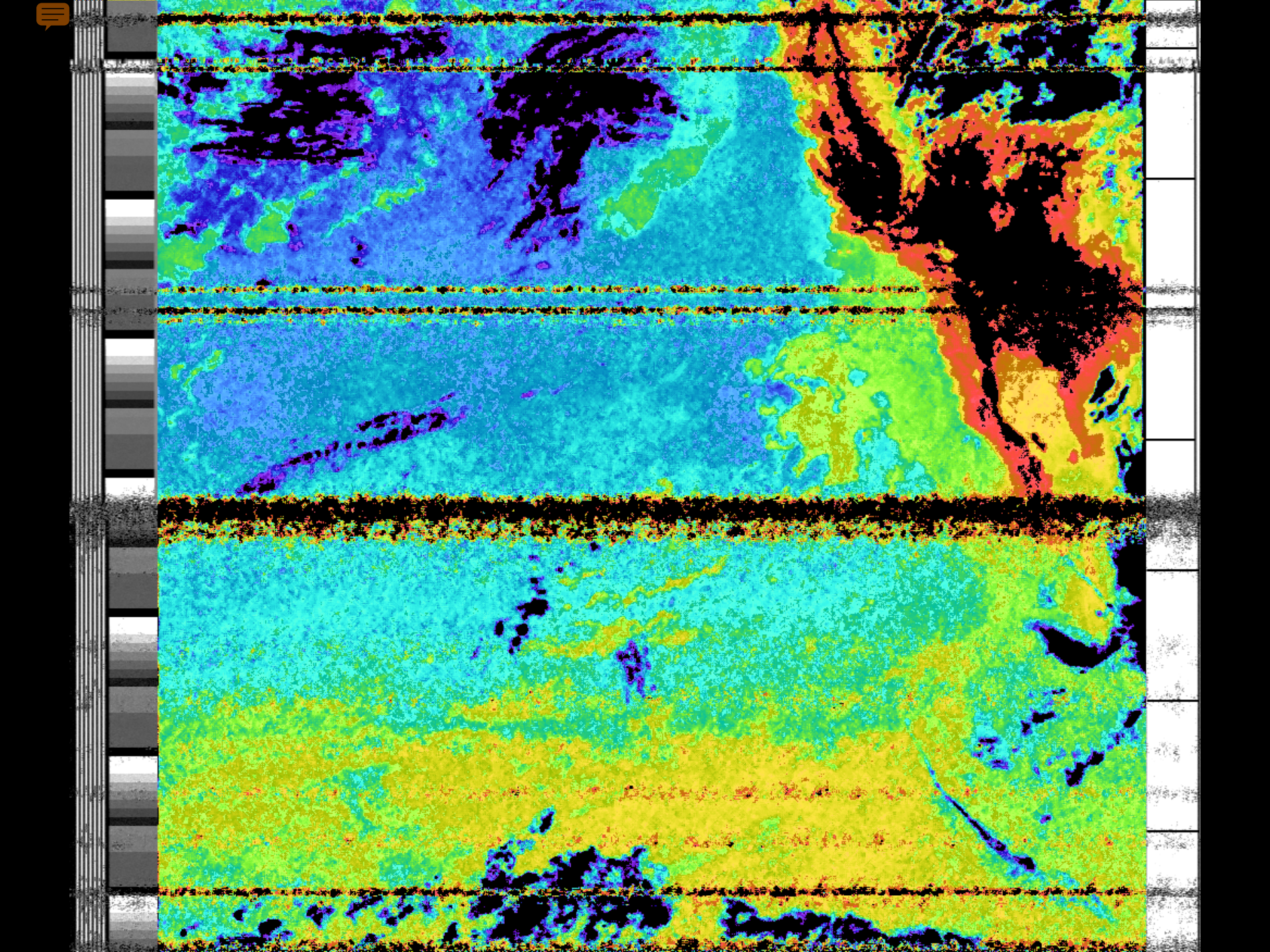
Automatic **P**icture **T**ransmission

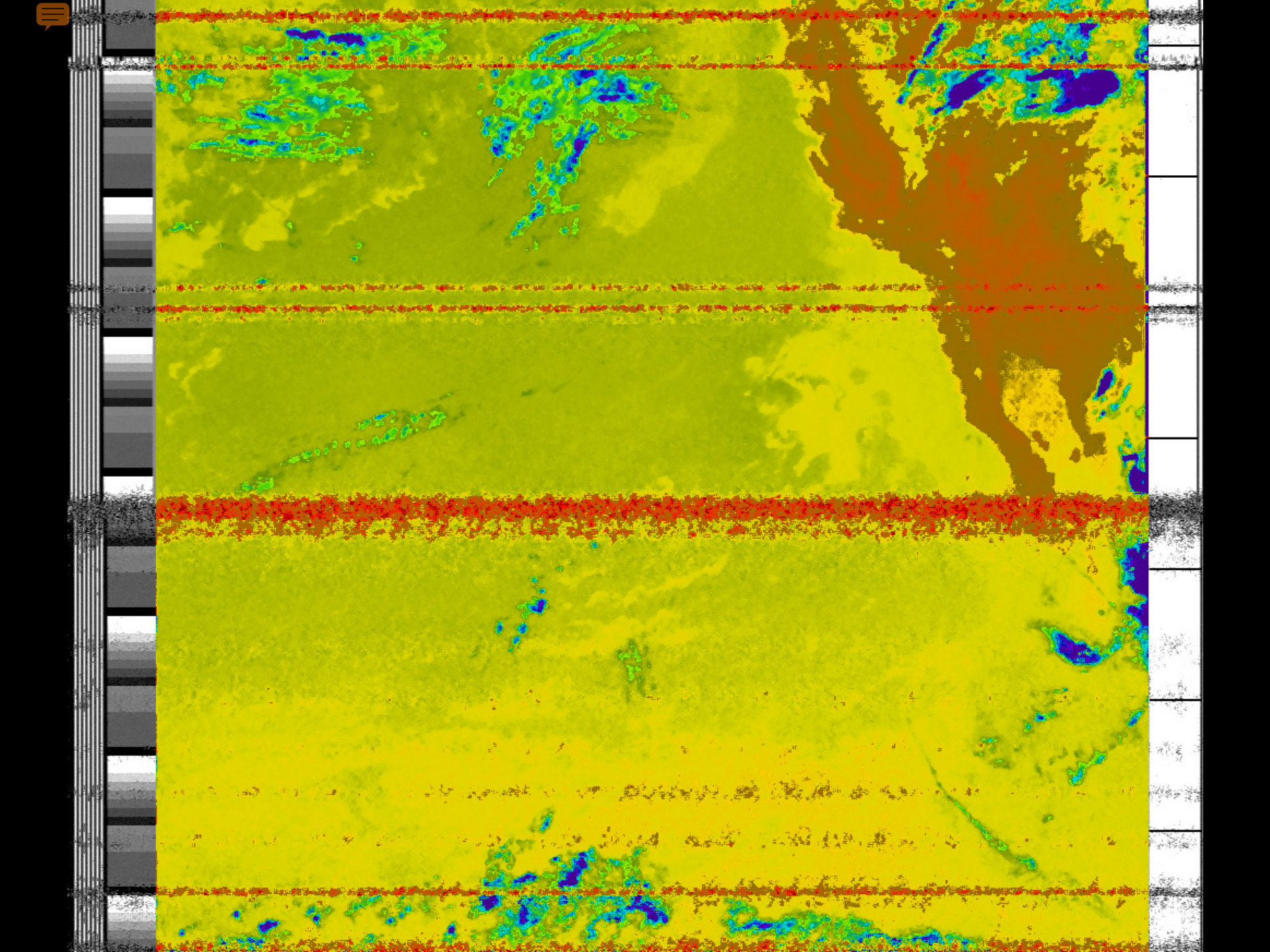




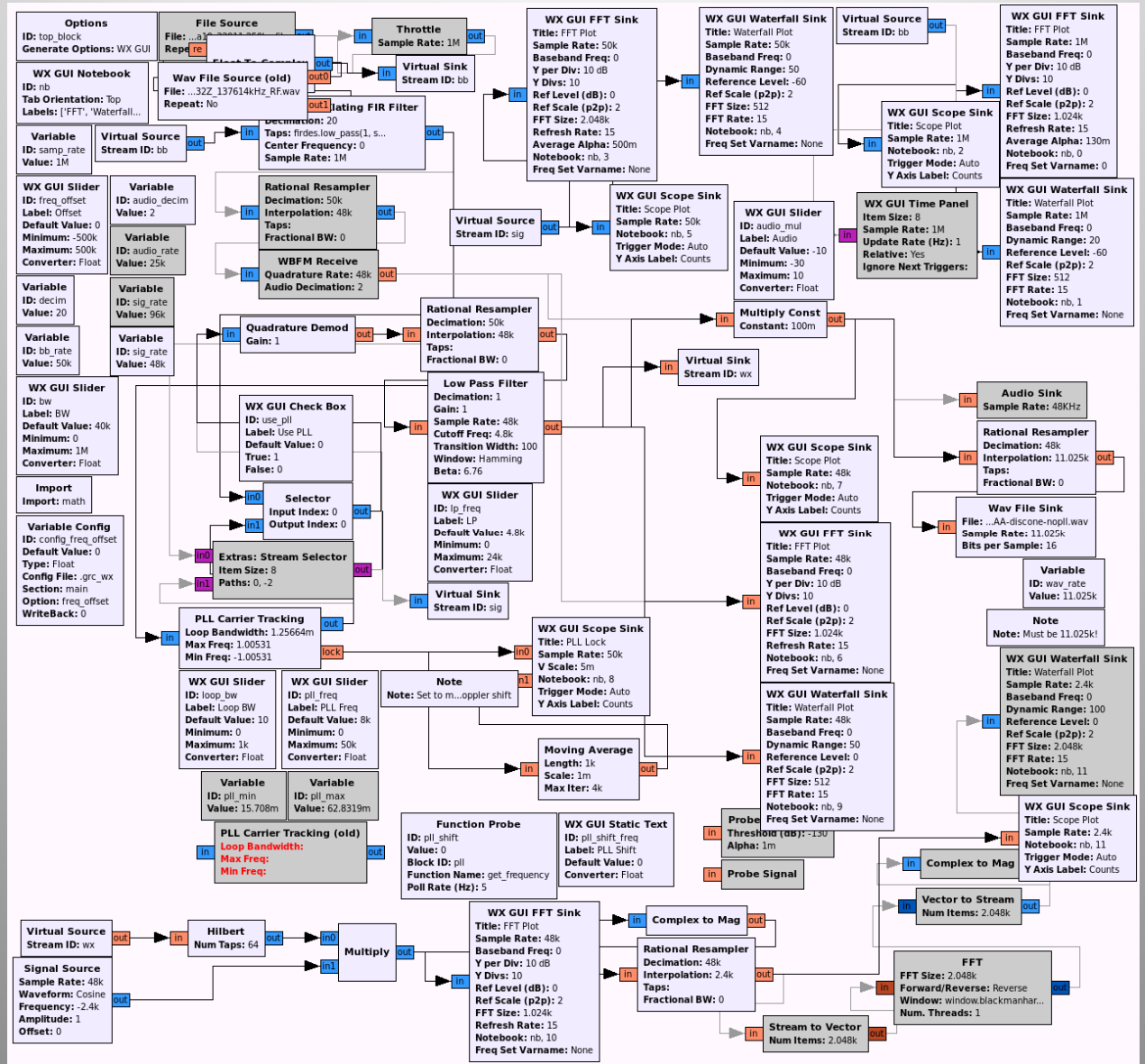




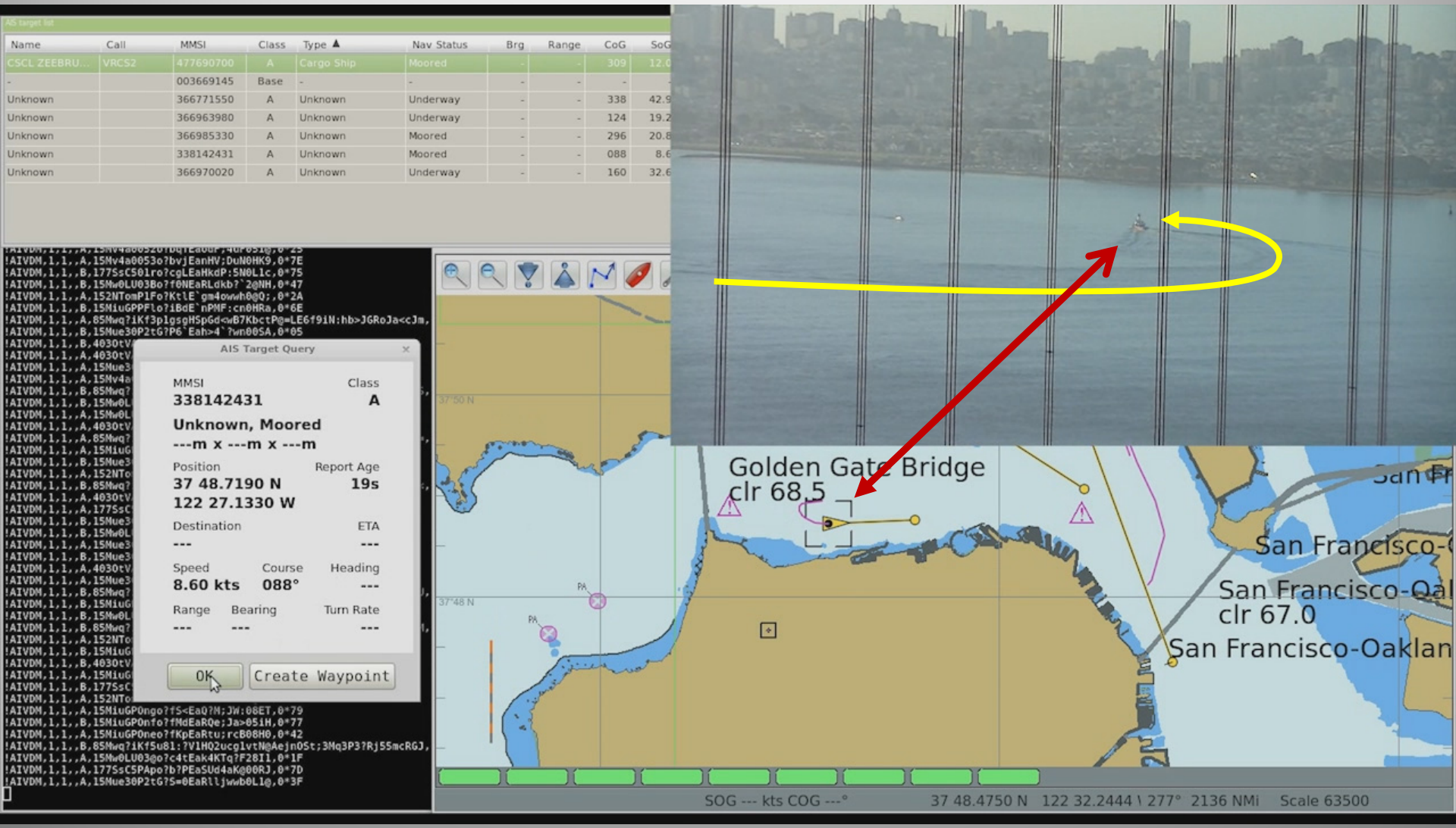




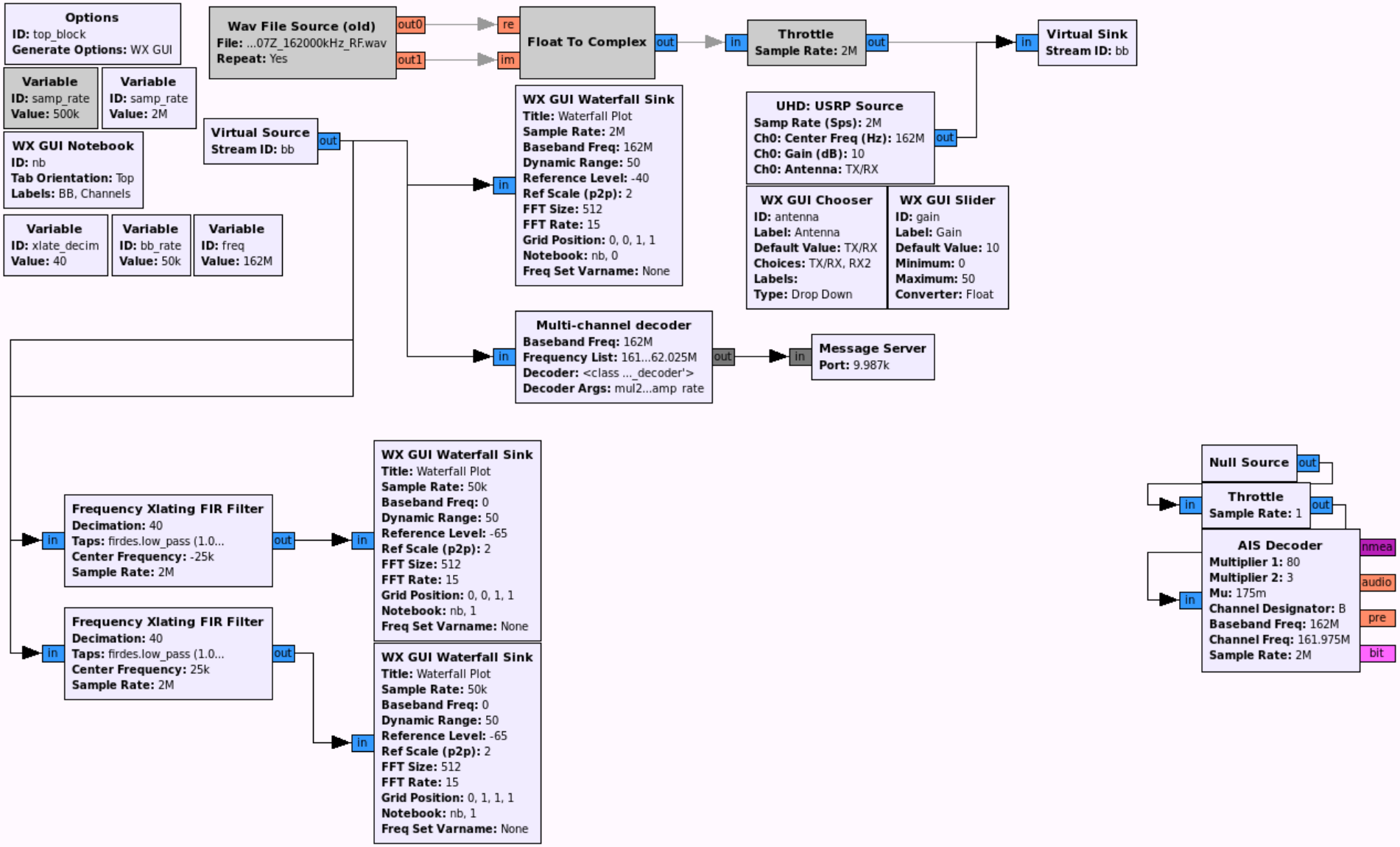
APT Baseband Processing



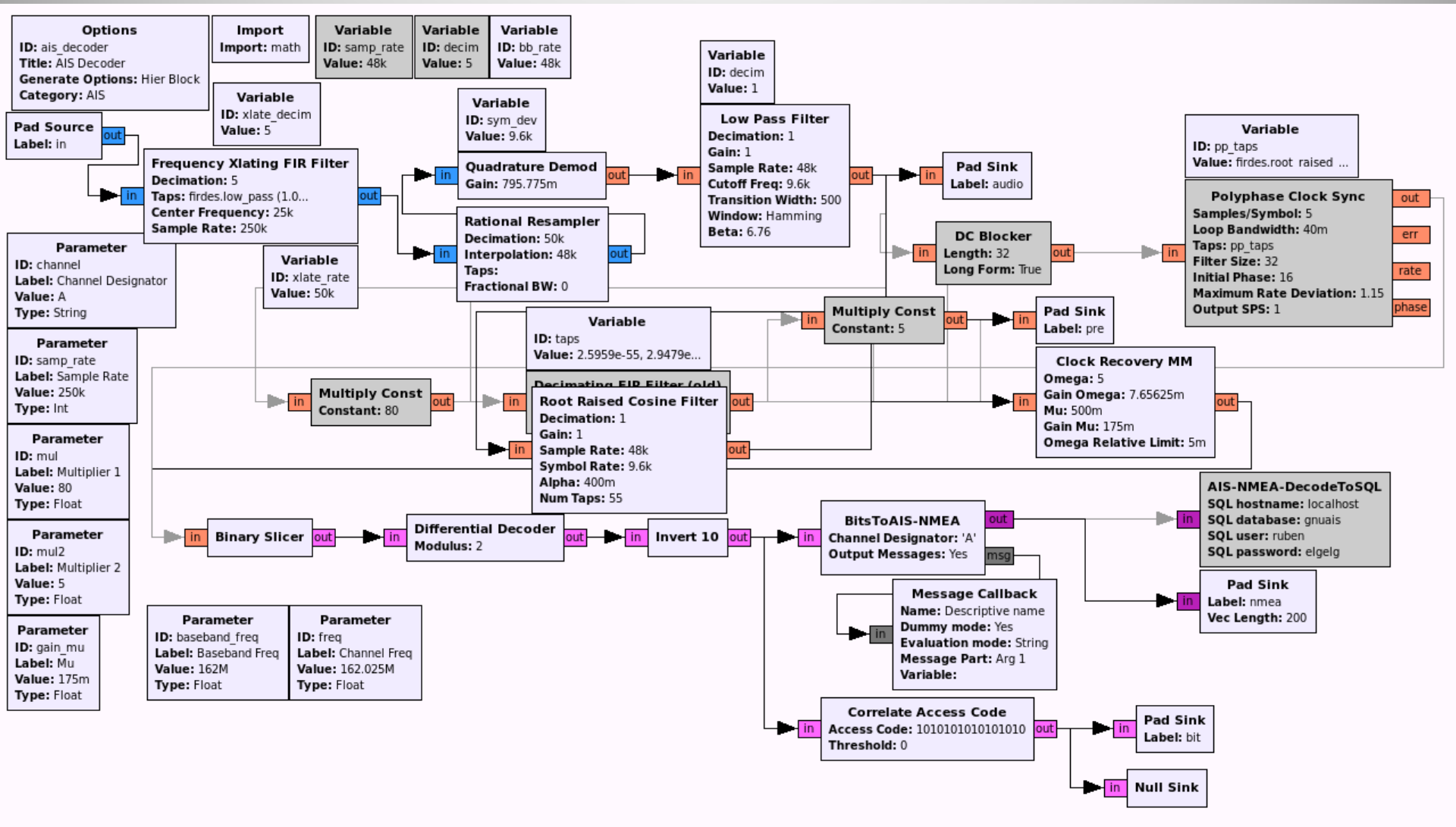
Automatic Identification System



AIS Multi-channel Decoder



AIS Channel Decoder

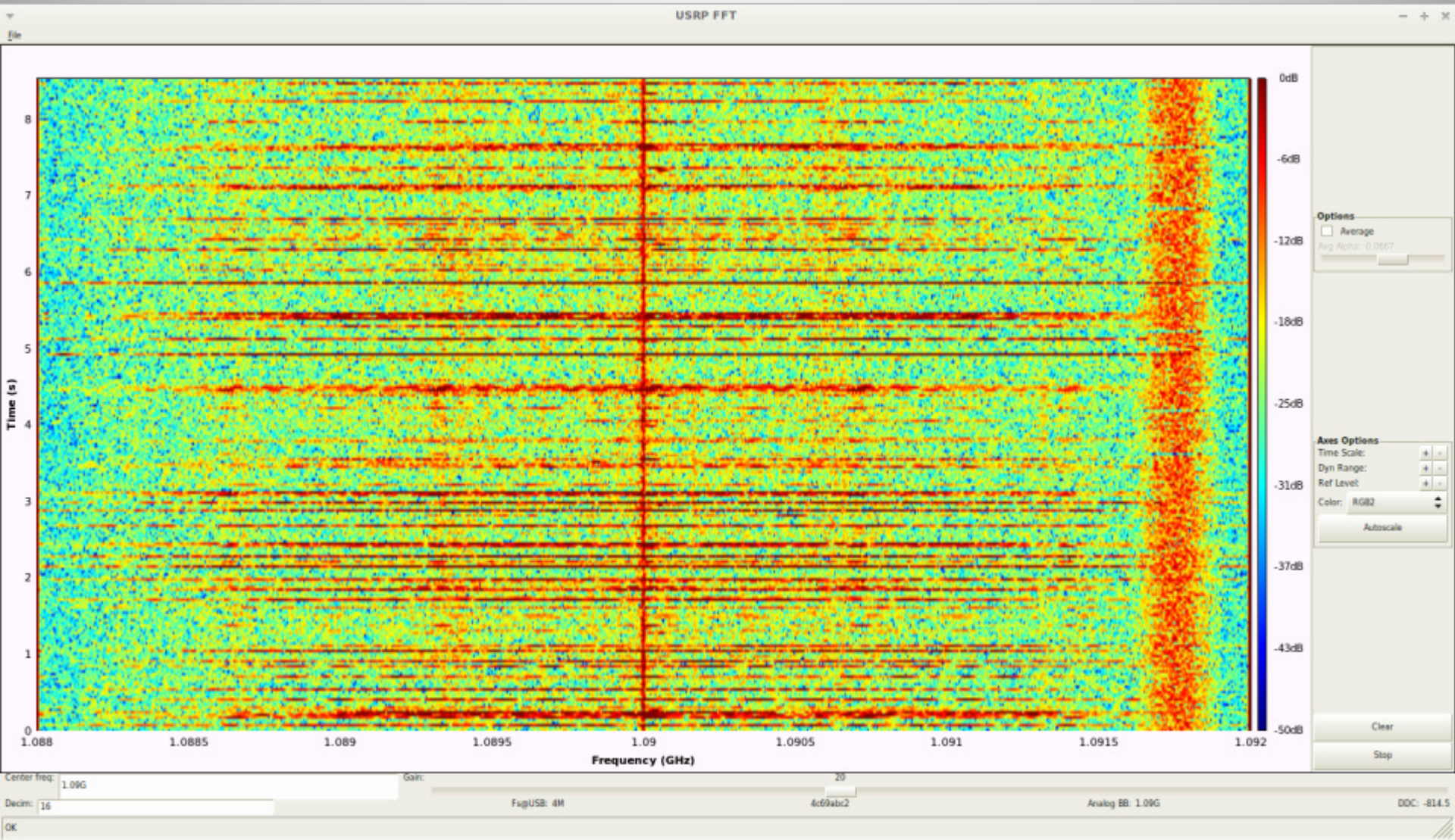


Other Applications of SDR

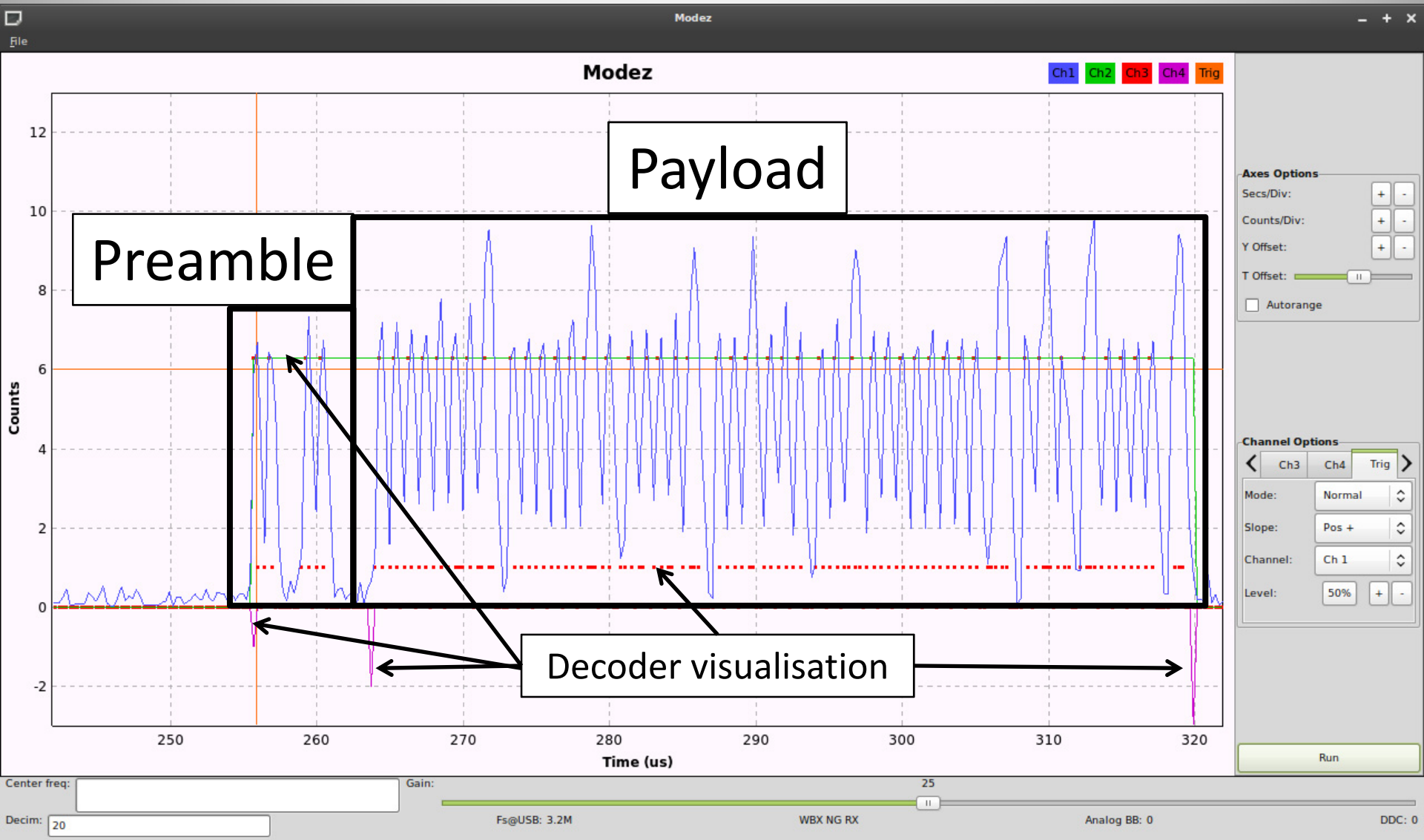
- Radio astronomy
- Passive radar
- DVB-S decoder
- Tracking pedestrian foot traffic in shopping malls

- Much more…

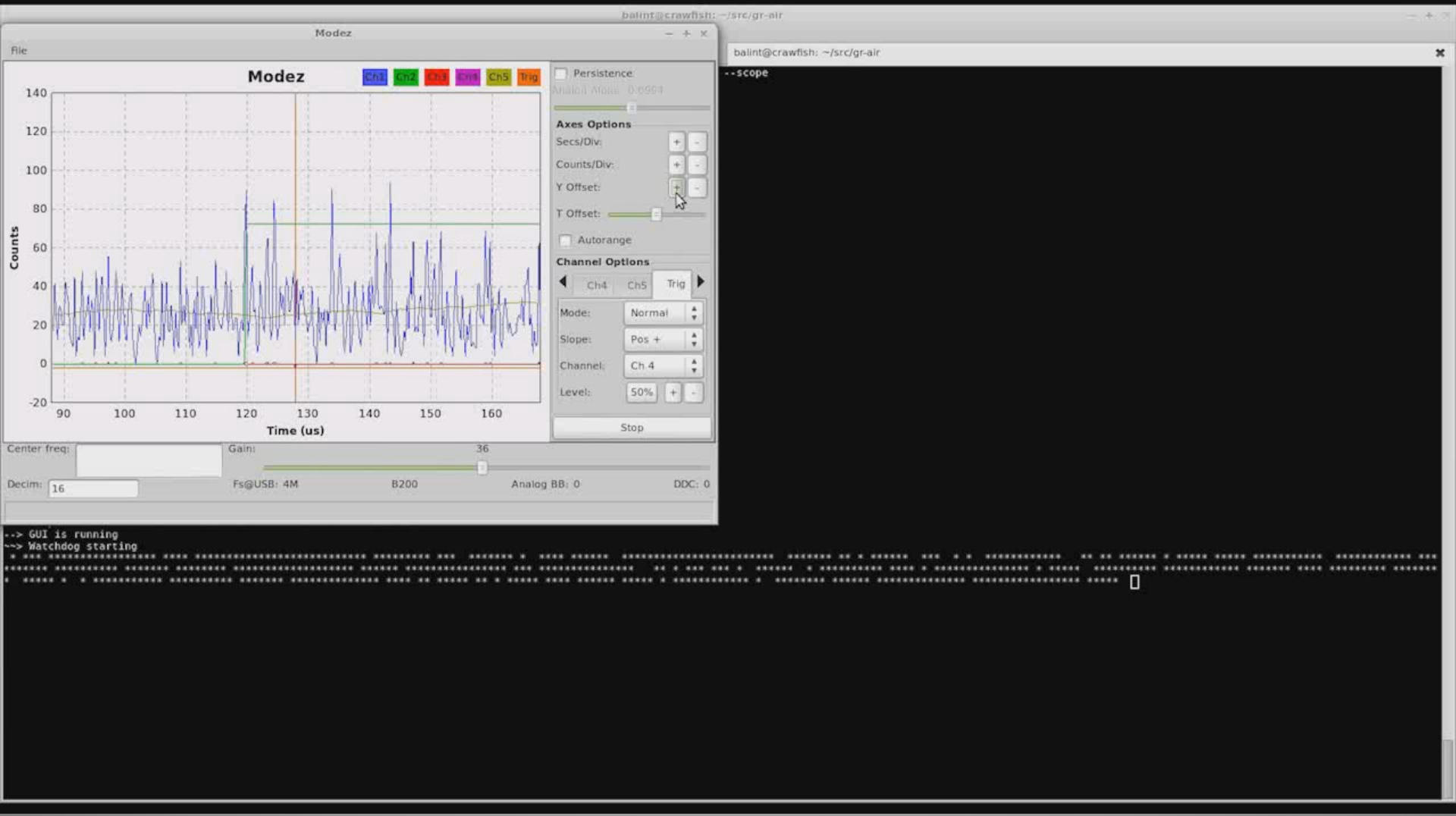
Mode S Waterfall



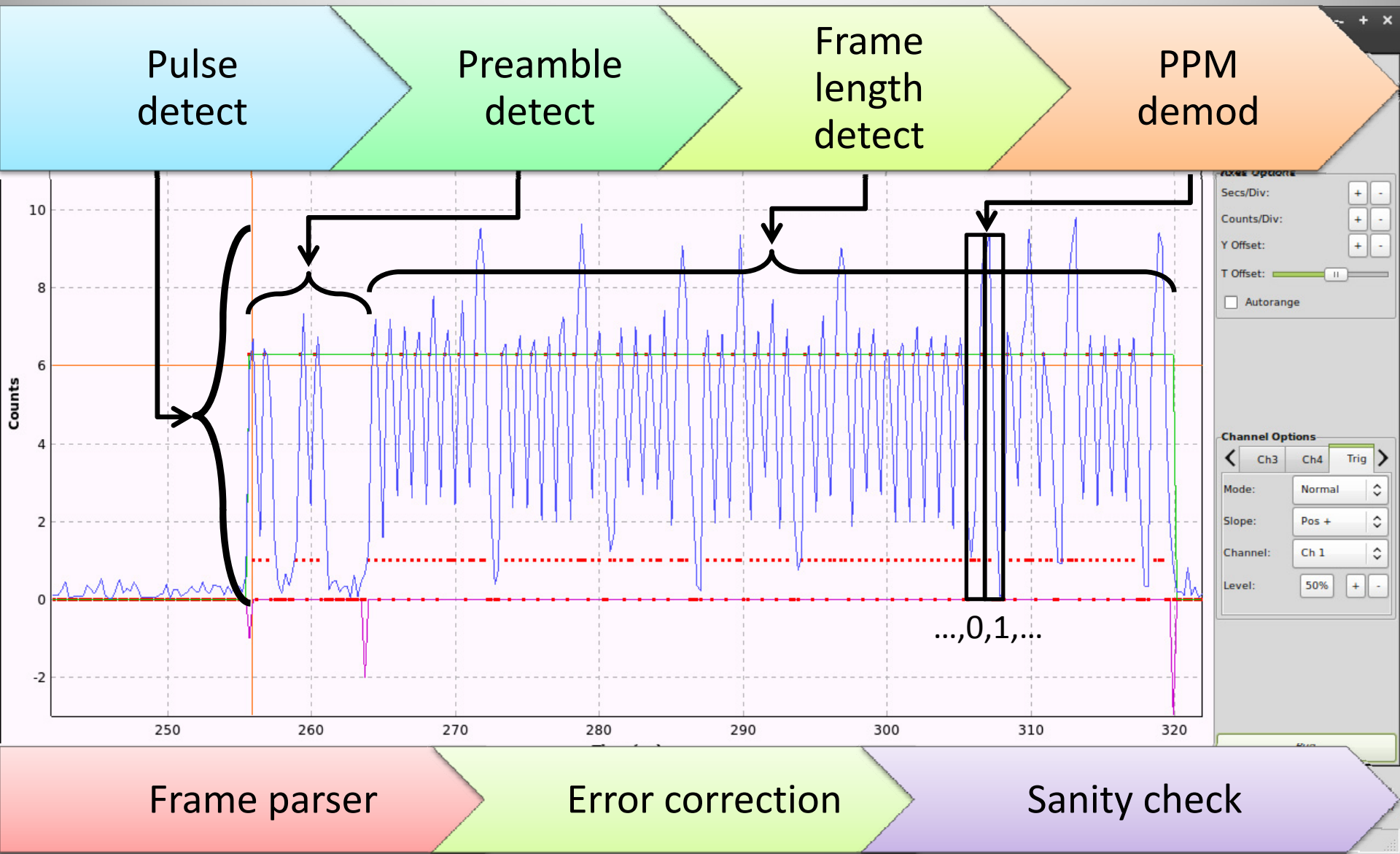
Mode S Response: AM signal



Mode S Response: AM signal



Mode S Decoder Structure



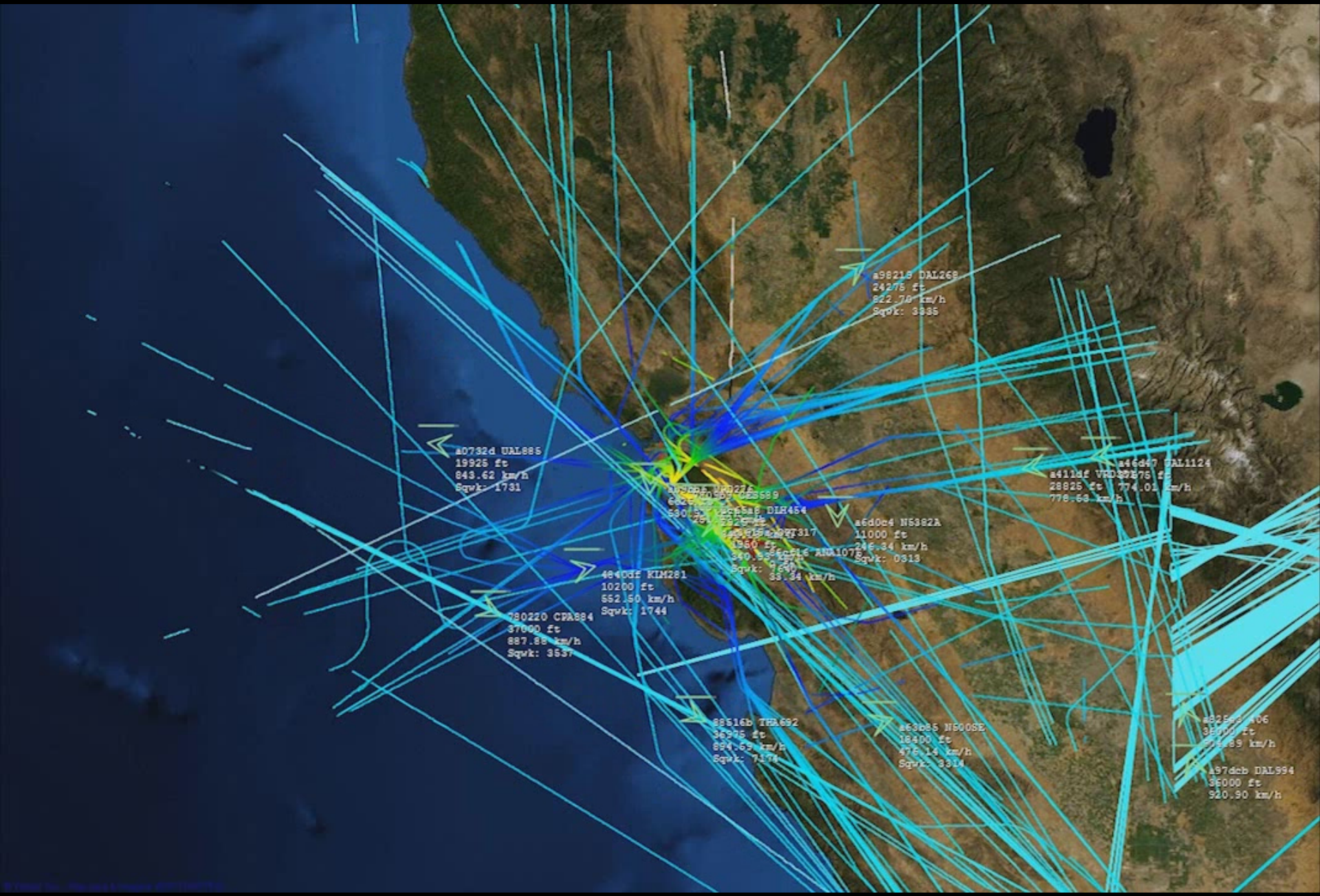
Secondary Surveillance RADAR

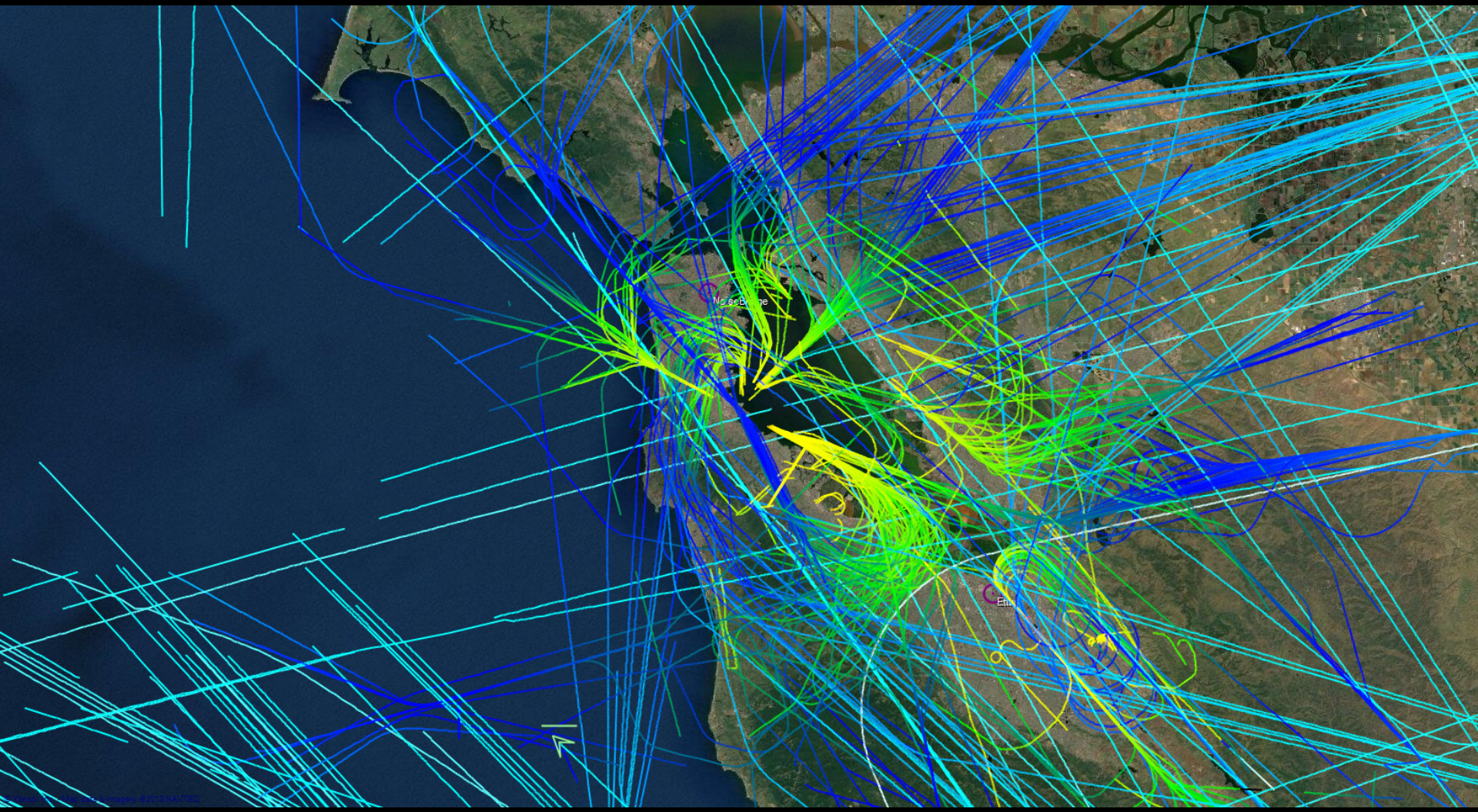
Mode S Frame Types

- Several **D**ownlink **F**ormats (DF)
  - Short/long frames (56/112 bits)
- Contains **A**irframe **A**ddress (AA)
  - 24-bit transponder address allocated by ICAO
- Appended CRC
  - ‘Normal’ mode (syndrome = 0)
  - Address overlaid mode (syndrome = AA)
- DF 11: All call, 5/20: Identity (squawk code), 0/4/16/20: Altitude…

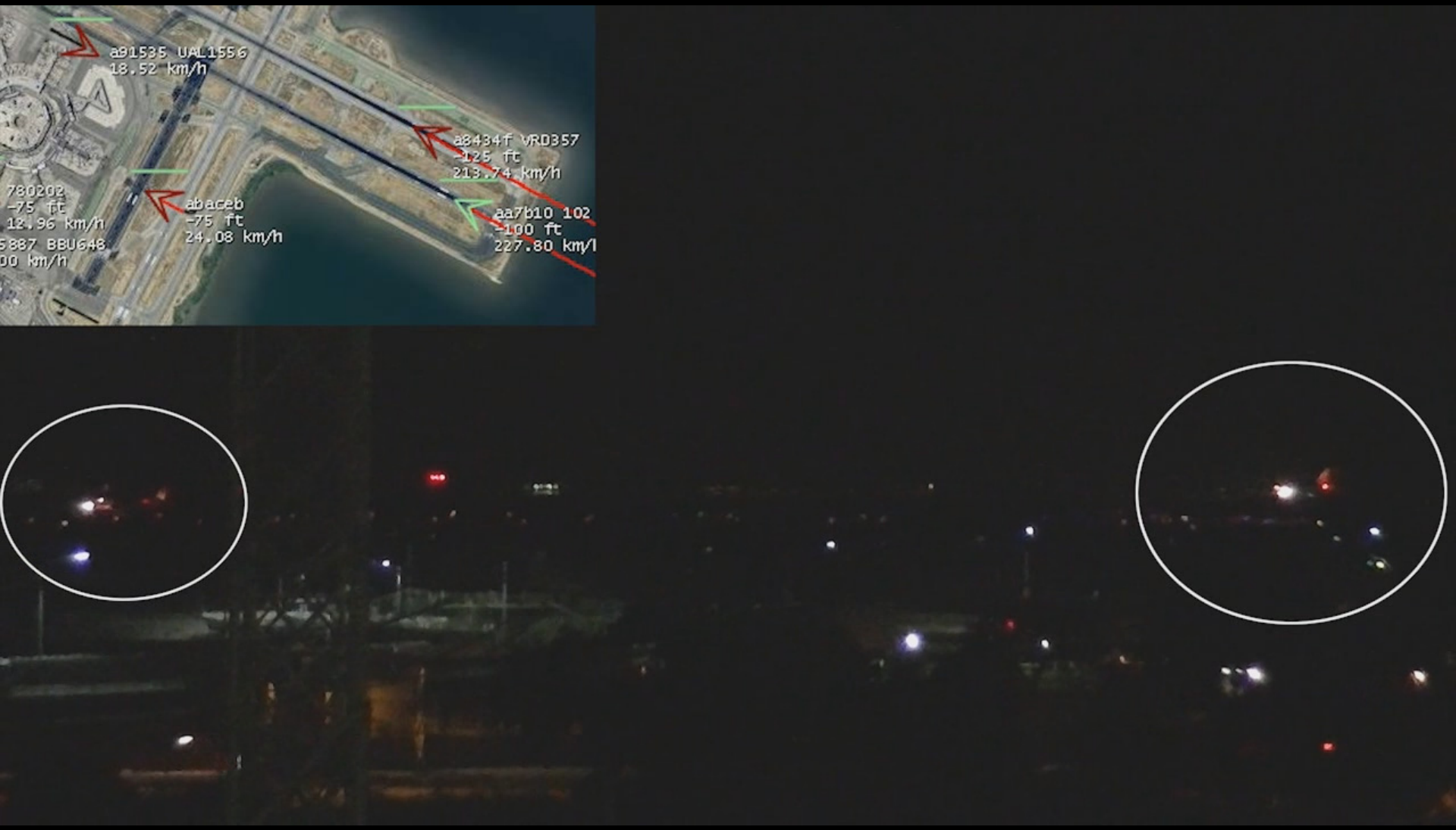
ADS-B: **E**xtended **S**quitter

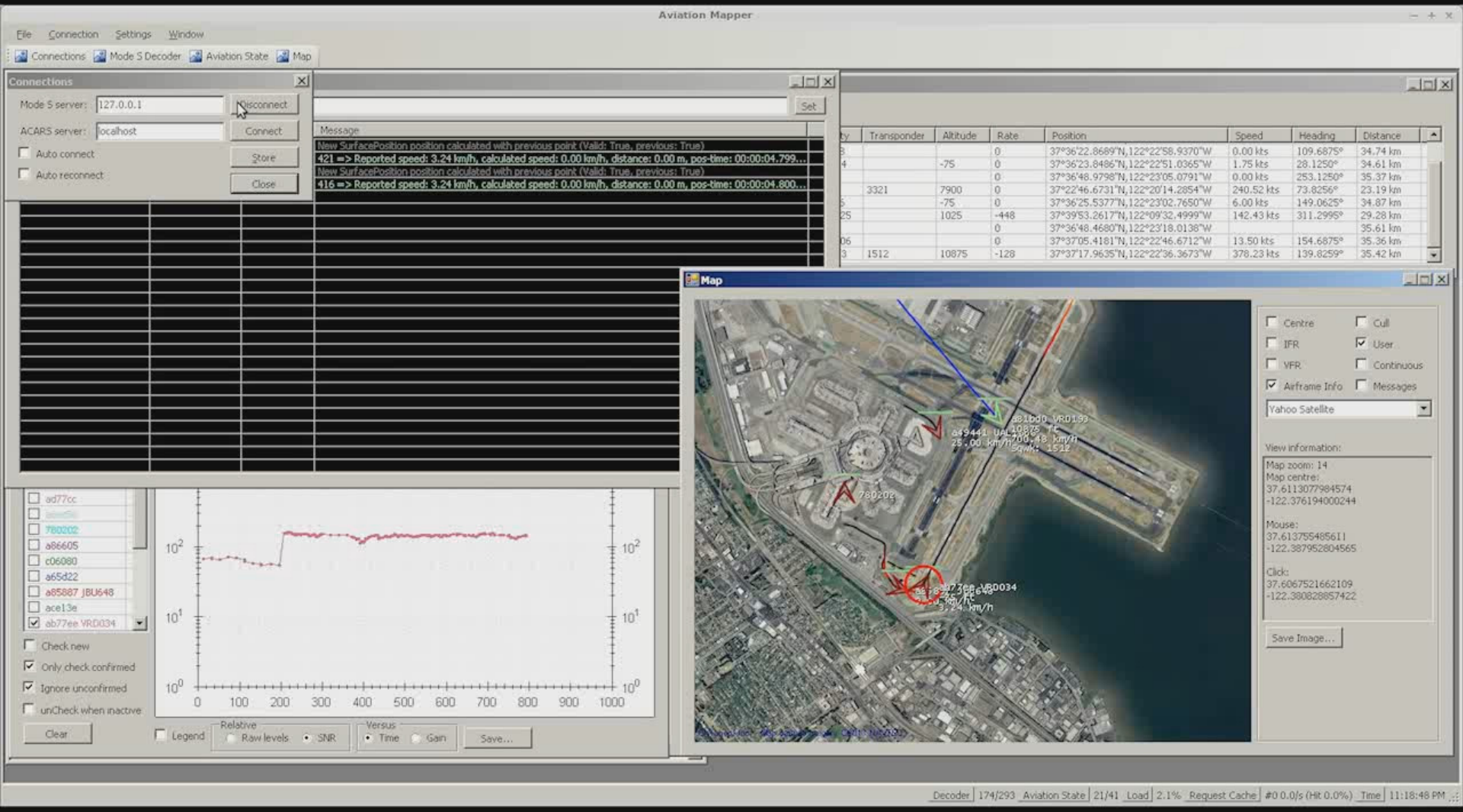
- Several ES types (DF 17):
  - Standard: position, altitude, heading, vertical rate, flight ID, transponder code
  - System information
  - Aircraft capabilities/status (e.g. autopilot enabled)
  - Aircraft intent
  - Traffic information
  - TCAS resolution advisories (“Pull up!”)


a98218 DAL268
24275 ft
822.70 km/h
Sqwk: 3335
a0732d UAL885
19925 ft
843.62 km/h
Sqwk: 1731
a46d47 UAL1124
a411df VRD32875
28825 ft
774.01 km/h
778.69 km/h
a6d0c4 N5382A
11000 ft
246.34 km/h
Sqwk: 0313
484cdf KLM281
10200 ft
552.50 km/h
Sqwk: 1744
780220 CPA884
37000 ft
887.88 km/h
Sqwk: 3537
88516b THA692
36975 ft
894.69 km/h
Sqwk: 7174
a63b85 N500SE
18400 ft
476.14 km/h
Sqwk: 3314
a97dcb DAL994
36000 ft
920.90 km/h

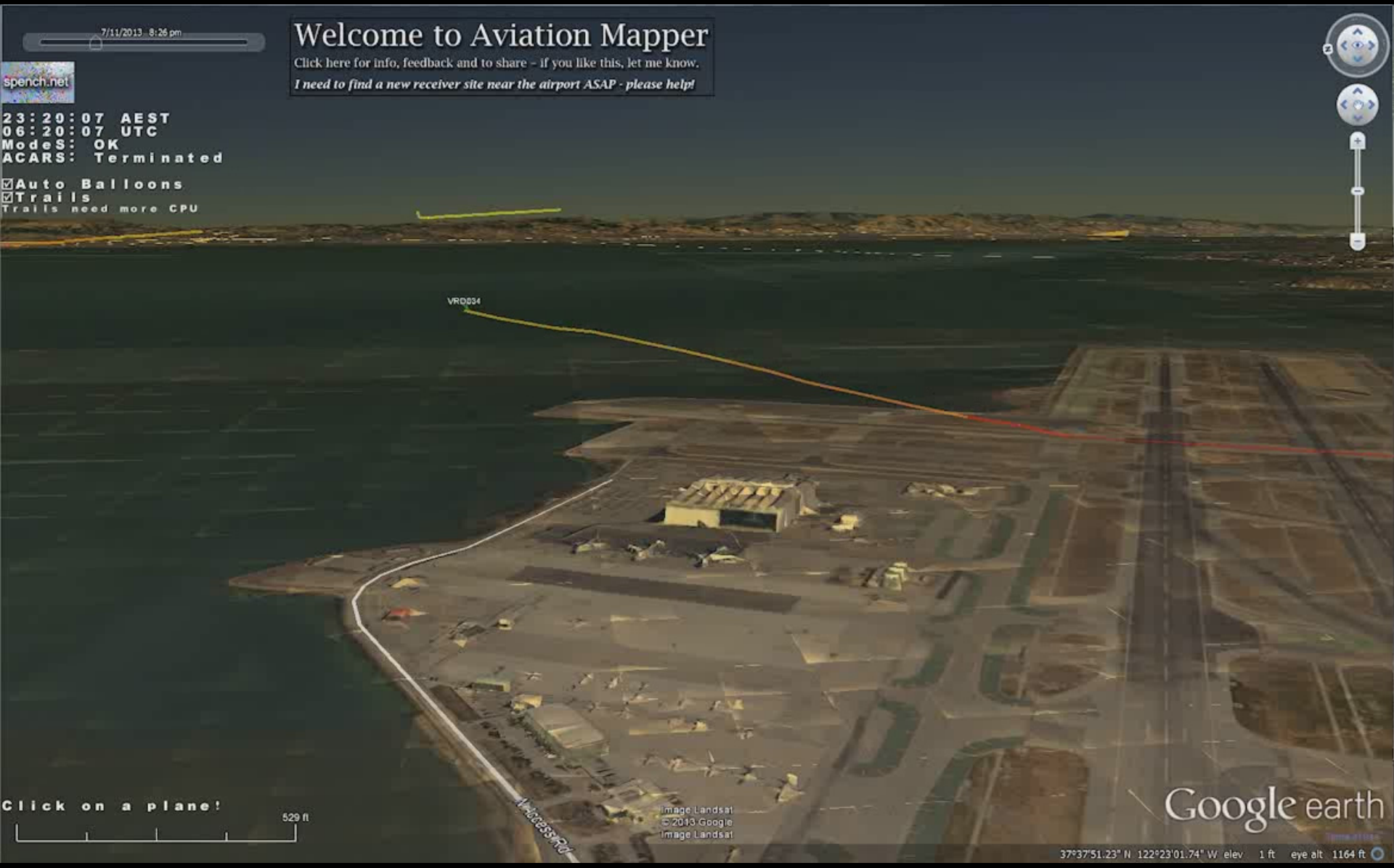



89611c UAE226
675 ft
366.10 km/h
Sqwk: 3645
aaa244
-25 ft
25.00 km/h
aa6c50 UAL73
22 ft
22 km/h
8990dc EVA18
10975 ft
475.68 km/h
Sqwk: 6244
4006ac
0.00 km/h
a835d1 VRD1757
25 ft
245.23 km/h
©2012 Microsoft Corporation, ©2012 NAVTEQ, ©2012 Image courtesy of NASA


a81535 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/h

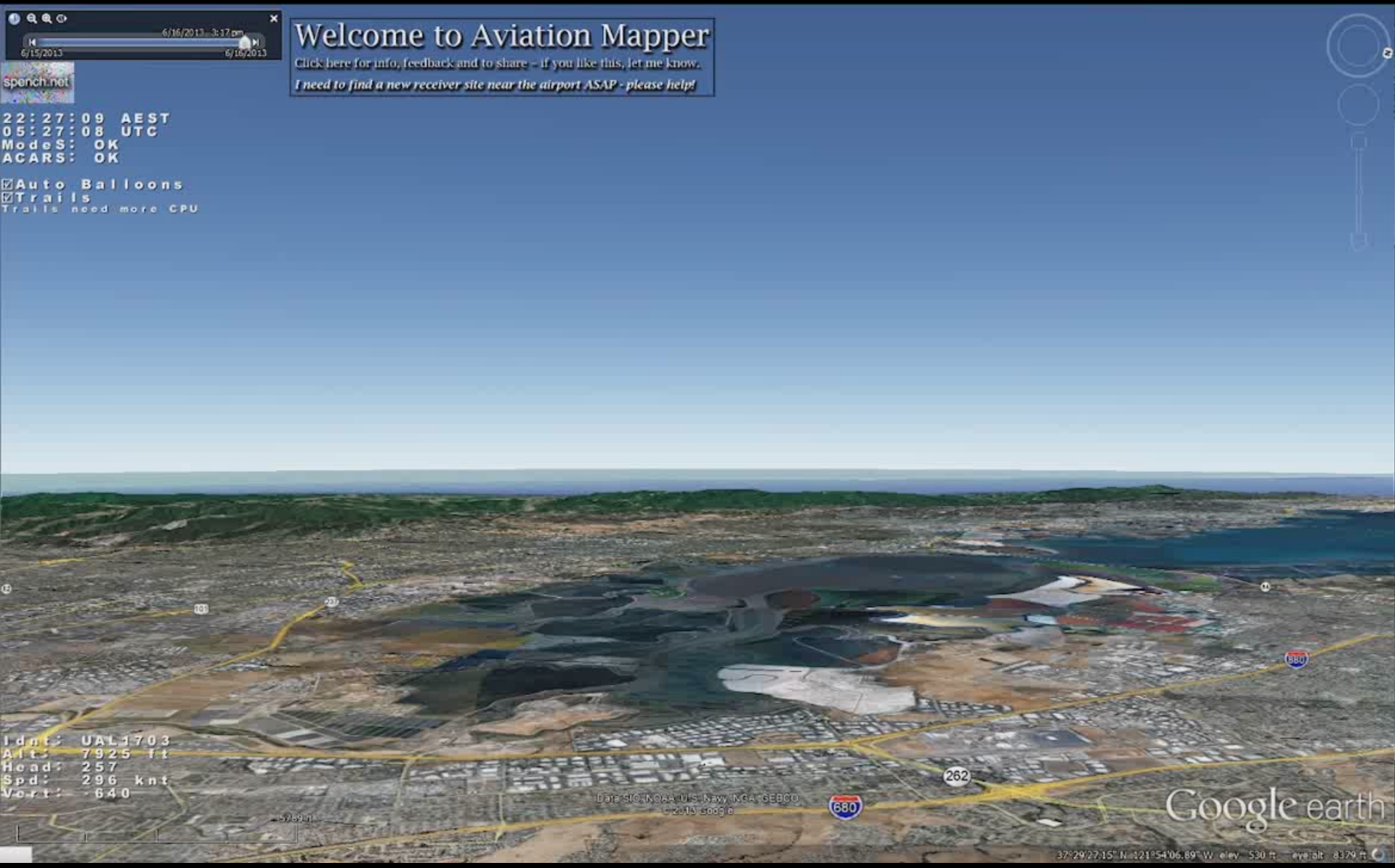

Aviation Mapper
File
Connection
Settings
Window
Connections
Mode S Decoder
Aviation State
Map
Connections
Mode S server:
127.0.0.1
Disconnect
ACARS server:
localhost
Connect
Auto connect
Auto reconnect
Store
Close
Set
Message
New SurfacePosition position calculated with previous point (Valid: True, previous: 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...
Transponder
Altitude
Rate
Position
Speed
Heading
Distance
37°36'22.8689"N,122°22'58.9370"W 0.00 kts 109.6875° 34.74 km
-75 37°36'23.8486"N,122°22'51.0365"W 1.75 kts 28.1250° 34.61 km
37°36'48.9798"N,122°23'05.0791"W 0.00 kts 253.1250° 35.37 km
3321 7900 37°22'46.6731"N,122°20'14.2854"W 240.52 kts 73.8256° 23.19 km
-75 37°36'25.5377"N,122°23'02.7650"W 6.00 kts 149.0625° 34.87 km
1025 -448 37°39'53.2617"N,122°09'32.4999"W 142.43 kts 311.2995° 29.28 km
37°36'48.4680"N,122°23'18.0138"W 35.61 km
37°37'05.4181"N,122°22'46.6712"W 13.50 kts 154.6875° 35.36 km
1512 10875 -128 37°37'17.9635"N,122°22'36.3673"W 378.23 kts 139.8259° 35.42 km
Map
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
Save Image...
ad77cc
780202
a86605
c06080
a65d22
a85887 JBU648
ace13e
ab77ee VRD034
Check new
Only check confirmed
Ignore unconfirmed
unCheck when inactive
Clear
Legend
Relative
Raw levels
SNR
Versus
Time
Gain
Save...
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
a49441 UAL1606
27.78 km/h
780202
a85687 JBU648
0.00 km/h


7/11/2013 8:26 pm
Welcome to Aviation Mapper
Click here for info, feedback and to share - if you like this, let me know.
I need to find a new receiver site near the airport ASAP - please help!
spench.net
23:20:07 AEST
06:20:07 UTC
ModeS: OK
ACARS: Terminated
Auto Balloons
Trails
Trails need more CPU
VRD034
Click on a plane!
529 ft
Image Landsat
© 2013 Google
Image Landsat
Google earth
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!
spench.net
23:19:22 AEST
06:19:22 UTC
ModeS: OK
ACARS: Terminated
Auto Balloons
Trails
Trails need more CPU
VRD034
JBU636
Click on a plane!
279 ft
Image Landsat
© 2013 Google
Google earth
37°36'13.66" N 122°22'45.17" W elev 23 ft eye alt 794 ft


7/11/2013 8:30 pm
spench.net
23:20:04 AEST
06:20:04 UTC
ModeS: OK
ACARS: erminated
Auto Balloons
Trails
Trails need more CPU
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!
Idnt: VRD034
Alt: 225 ft
Head: 29
Spd: 160 knt
Vert: 3008
39 ft
Image Landsat
© 2013 Google
Google earth
37°37'35.13" N 122°22'08.53" W elev 11 ft eye alt 70 ft

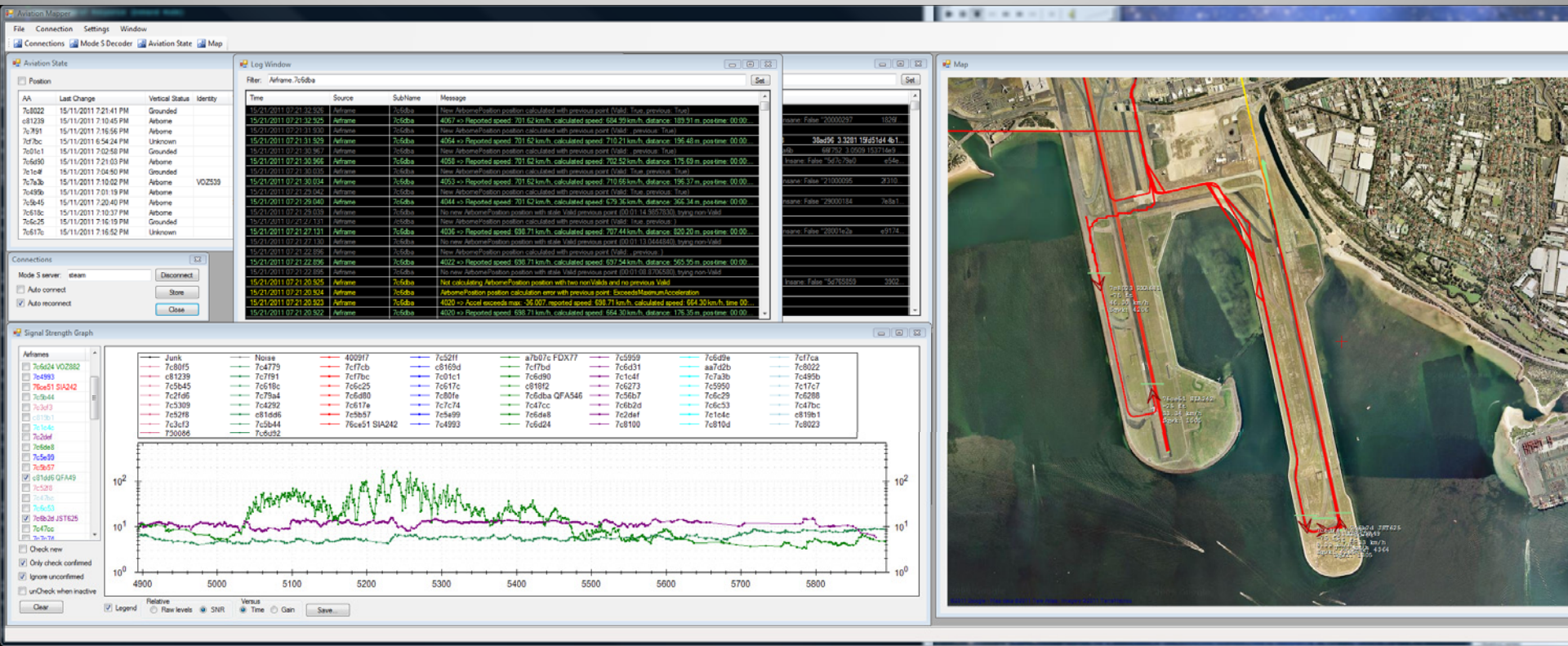

6/16/2013 3:17 pm
6/15/2013
6/16/2013
spench.net
Welcome to Aviation Mapper
Click here for info, feedback and to share - if you like this, let me know.
I need to find a new receiver site near the airport ASAP - please help!
22:27:09 AEST
05:27:08 UTC
ModeS: OK
ACARS: OK
Auto Balloons
Trails
Trails need more CPU
Idnt: UAL1703
Alt: 7925 ft
Head: 257
Spd: 296 knt
Vert: -640
Google earth


6/16/2013 3:17 pm
6/15/2013
6/16/2013
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!
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
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
7/30/2013 12:14 am
7/29/2013
7/30/2013
spench.net
07:24:55 AEST
21:24:55 UTC
ModeS: OK
ACARS: OK
Auto Balloons
Trails
Trails need more CPU
N805C
UA0840
UAL853
CA0173
VRD906
BAW11M
659
SIA16
AAL2005
Click on a plane!
48 mi
Data SIO, NOAA, U.S. Navy, NGA, GEBCO
© 2013 Google
Data LDEO-Columbia, NSF, NOAA
Image Landsat
Google earth
Terms of Use
37°09'56.01" N 123°59'11.79" W elev -12413 ft eye alt 200.20 mi

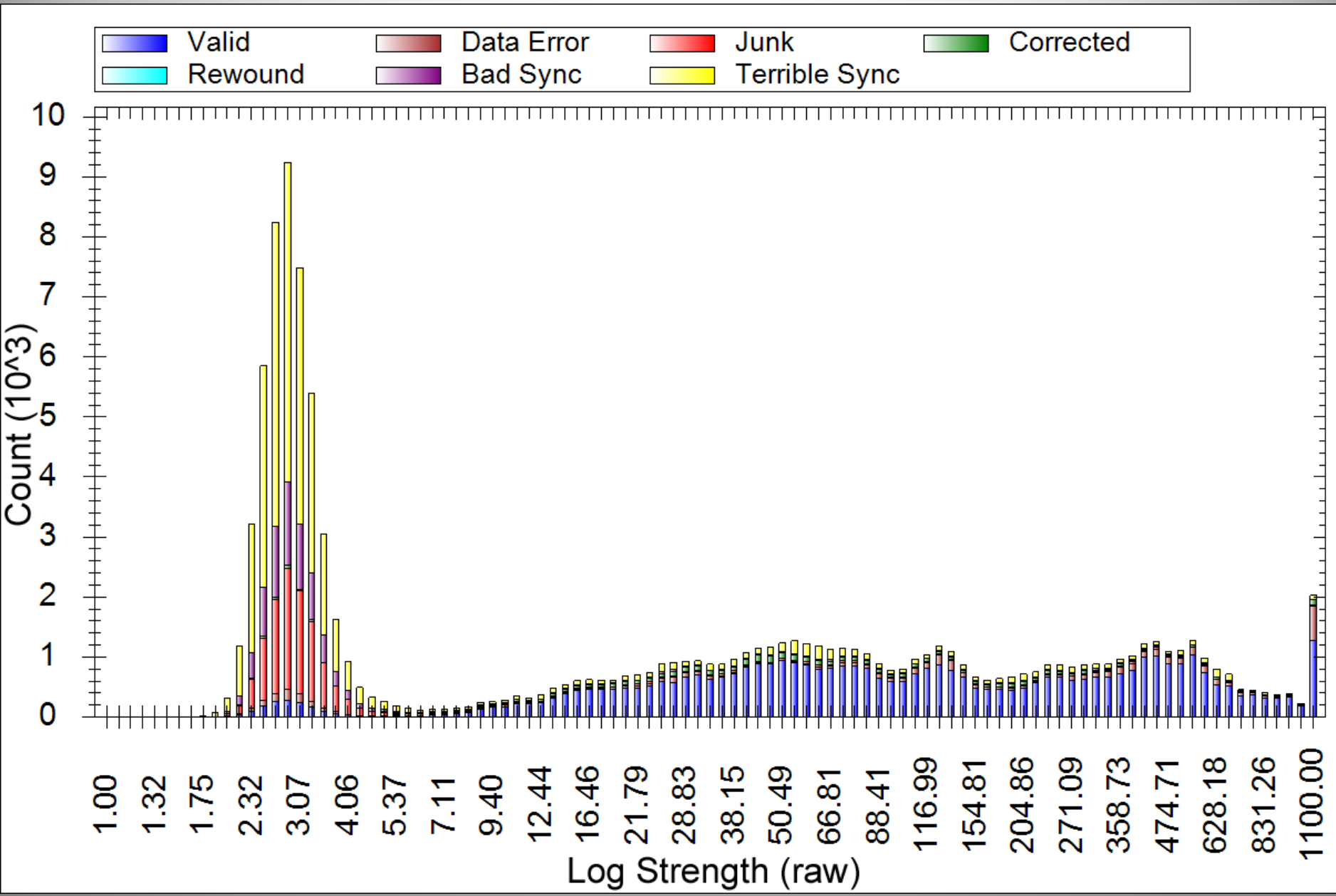
Aviation Mapper

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

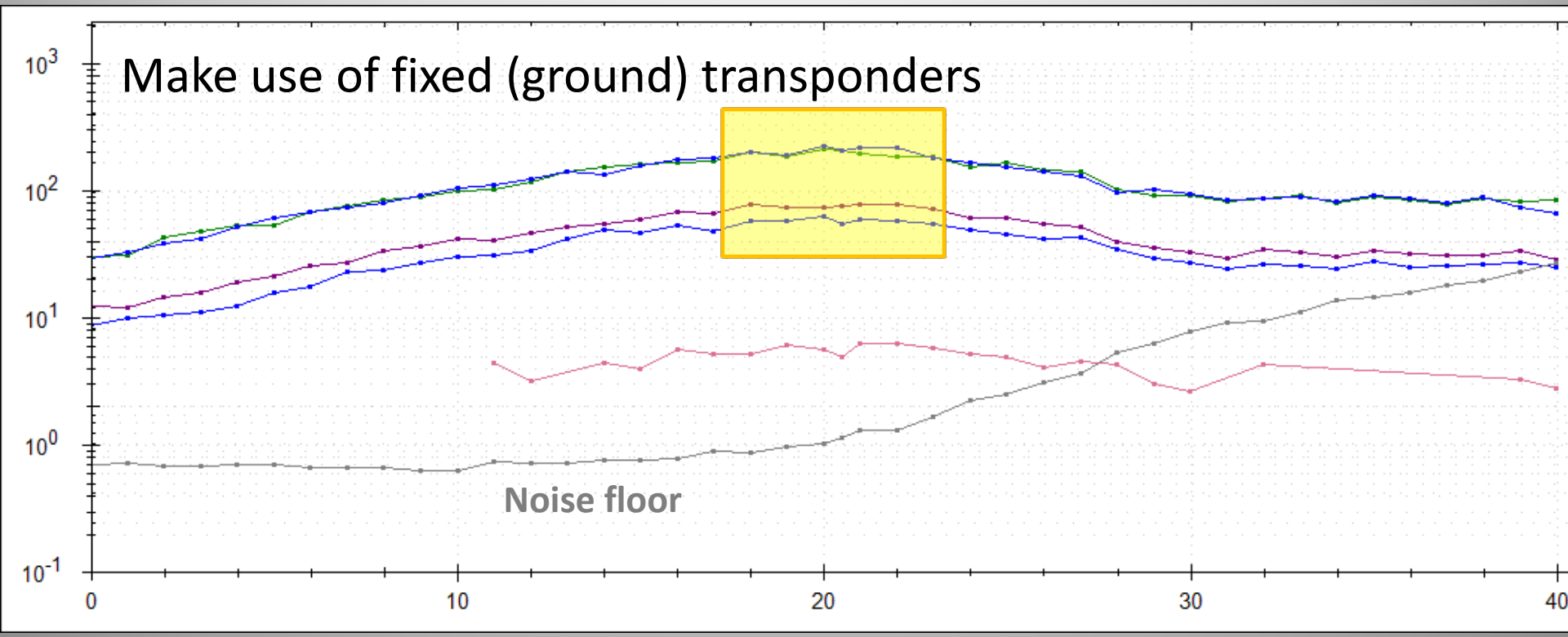


Modez Mk I


7c8031 RXA674
0 ft
61.20 km/h
Sqwk: 3707
7c810d RXA838
0 ft
64.80 km/h
Sqwk: 1041
7cf3d1
42350 ft
111.60 km/h
7c6d38 VOZ973
0 ft
0.00 km/h
Sqwk: 1452
Ground vehicle with Mode S!
(inspecting perimeter?)
©2011 Google - Map data ©2011 Tele Atlas, Imagery ©2011 TerraMetrics

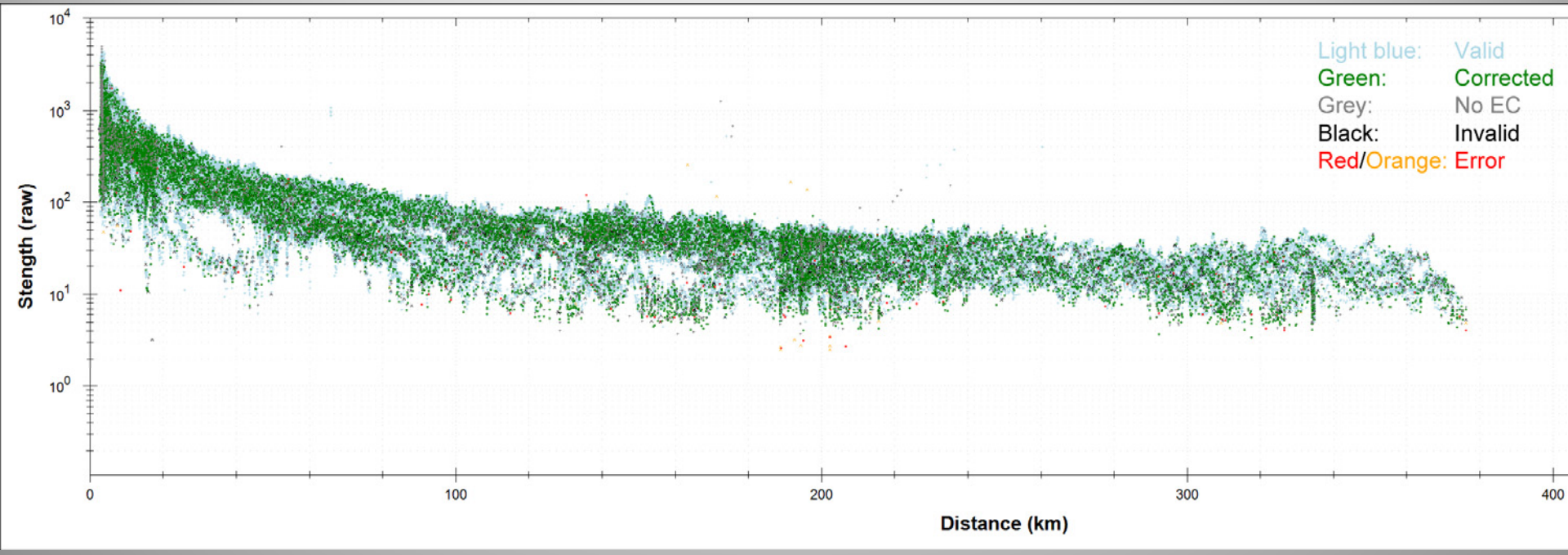

Valid
Data Error
Junk
Corrected
Rewound
Bad Sync
Terrible Sync
Count (10^3)
0
1
2
3
4
5
6
7
8
9
10
1.00
1.32
1.75
2.32
3.07
4.06
5.37
7.11
9.40
12.44
16.46
21.79
28.83
38.15
50.49
66.81
88.41
116.99
154.81
204.86
271.09
358.73
474.71
628.18
831.26
1100.00
Log Strength (raw)

SNR vs. Gain

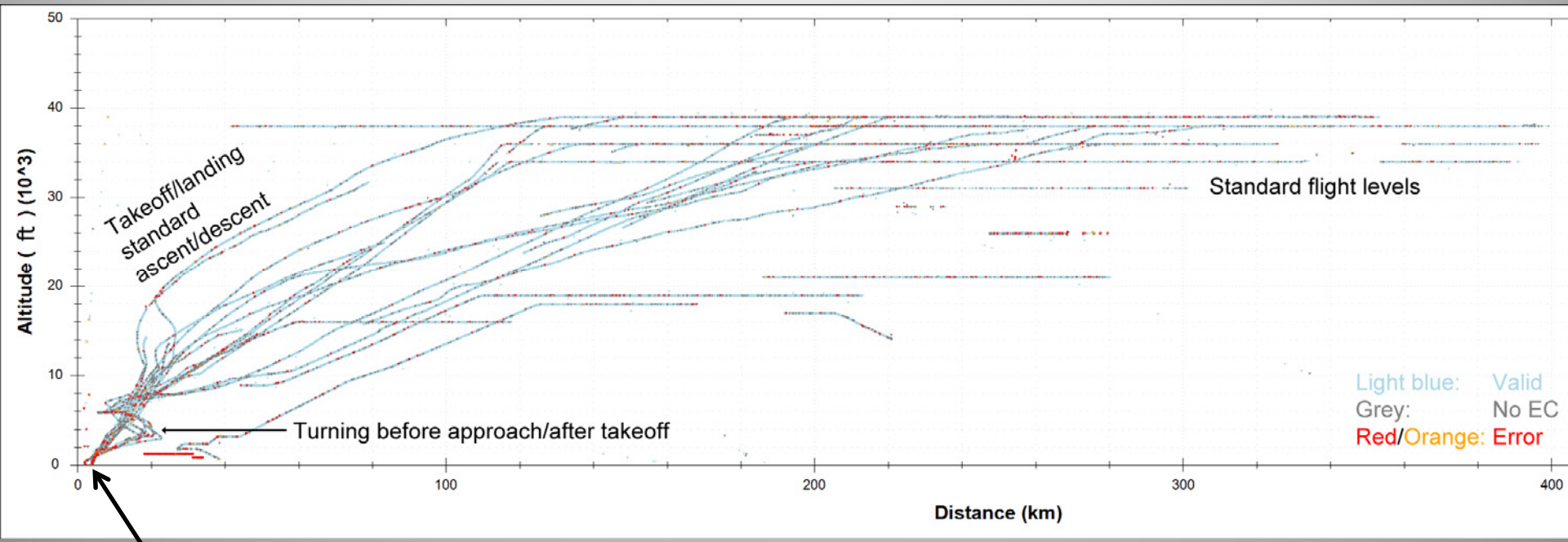


Change USRP/WBX gain

Strength vs. Distance

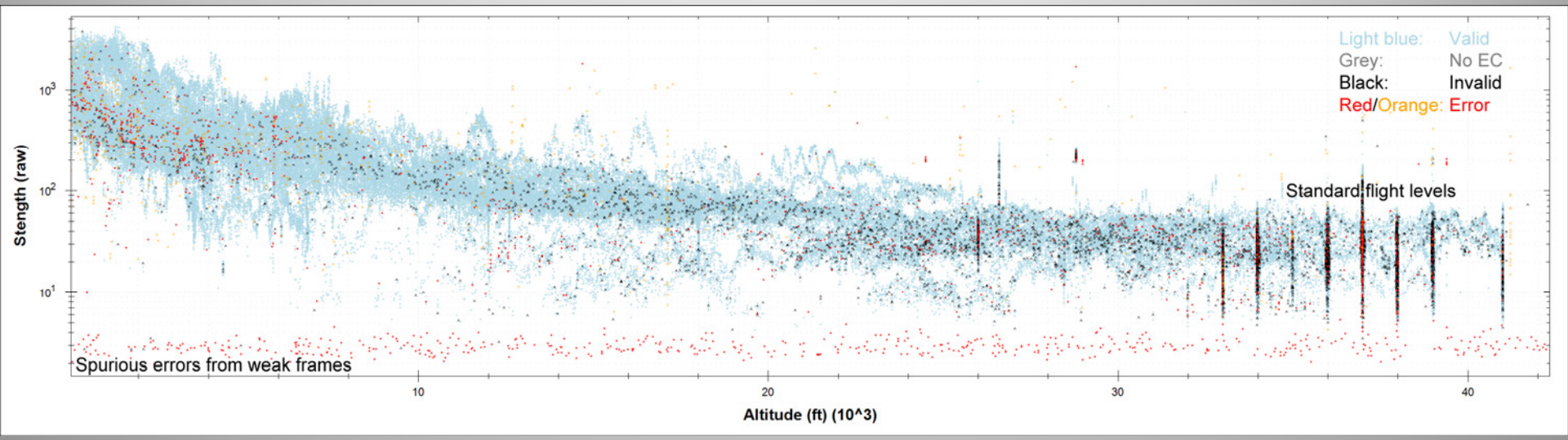


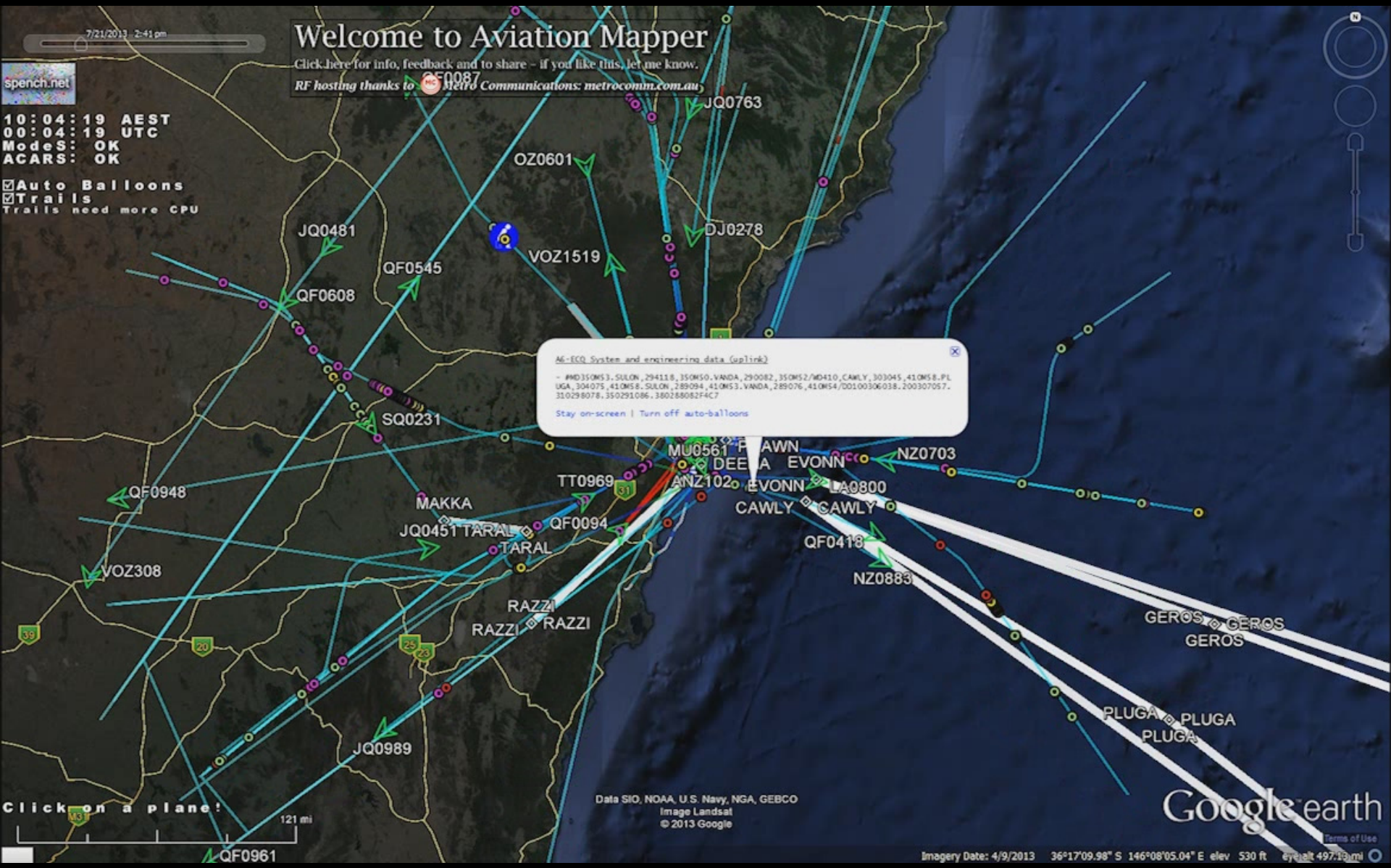
Altitude vs. Distance



Helps to live close to the airport

Strength vs. Altitude




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
7/21/2013 2:41 pm
spench.net
10:04:19 AEST
00:04:19 UTC
ModeS: OK
ACARS: OK
Auto Balloons
Trails
Trails need more CPU
QF0087
JQ0763
OZ0601
JQ0481
DJ0278
VOZ1519
QF0545
QF0608
SQ0231
A6-ECQ System and engineering data (uplink)
- #MD350NS3.SULON,294118,350NS0.VANDA,290082,350NS2/WD410,CAWLY,303045,410NS8.PLUGA,304075,410NS8.SULON,289094,410NS3.VANDA,289076,410NS4/DD100306038.200307057.310298078.350291086.380288082F4C7
Stay on-screen | Turn off auto-balloons
MU0561
DEEWA
EVONN
NZ0703
ANZ102
LA0800
CAWLY
QF0948
TT0969
MAKKA
JQ0451
TARAL
QF0094
QF0418
VOZ308
NZ0883
RAZZI
GEROS
PLUGA
JQ0989
Click on a plane!
121 mi
QF0961
Data SIO, NOAA, U.S. Navy, NGA, GEBCO
Image Landsat
© 2013 Google
Google earth
Terms of Use
Imagery Date: 4/9/2013 36°17'09.98" S 146°08'05.04" E elev 530 ft

ACARS

- **A**ircraft **C**ommunication **a**nd **R**eporting **S**ystem
- ‘Text messaging’ for aircraft
- Wide-reaching network
  - VHF ground stations
  - HF datalink
  - SATCOM
- Manual and automated messages between:
  - Cockpit, ATC, airline ops & airport ground staff
  - Avionics/engines, airline maintenance & equipment (engine) manufactures

Streaming

- Listening to primary & secondary frequencies
- Decoded, combined, JSON-ified & served

```
Time:       2011-11-15 22:42:17.894000
Station:    Home
Frequency:  131.55 MHz
Mode:       S (downlink, LCN: 19)
Address:    VH-OJD
Ack:        NAK
Label:      H1: System and engineering data
Block:      6
Message #:  C15A
Flight ID:  QF0021
#CFB/BLVBOCR.



 A RPT20 PG1  L-APU REAL
 B VH-OJD 15NOV11 1142 QFA21   YSSY/RJAA 685-2270-011 RR-508 ES


 1  489 100.0  92.8
 2  GND
 3    OPEN
 4  OFF 0.83
 5  OFF 100
 6   ON  ON 226 226
 7


Time:       2011-11-15 22:42:18.111000
Station:    Home
Frequency:  131.55 MHz
Mode:       s (uplink, LCN: 19)
Address:    A6-ECV
Ack:        7
Label:      _<DEL>: General Response (Demand Mode)
Block:      P


Time:       2011-11-15 22:42:22.203000
Station:    Home
Frequency:  131.55 MHz
Mode:       S (downlink, LCN: 19)
Address:    VH-OJD
Ack:        NAK
Label:      H1: System and engineering data
Block:      7
Message #:  C15B
Flight ID:  QF0021
#CFB  NORM 14.1
 8    OPEN  20
 9   ON  28
 10  ON 202
 11    MES 32 32
 12 NORM  70  70
 13   OPEN  53  53
 14 102
 15   94  61   0
 16  2266 CHG  2
 17  1760 27
 18 15NOV11 11:42:13
 19
```

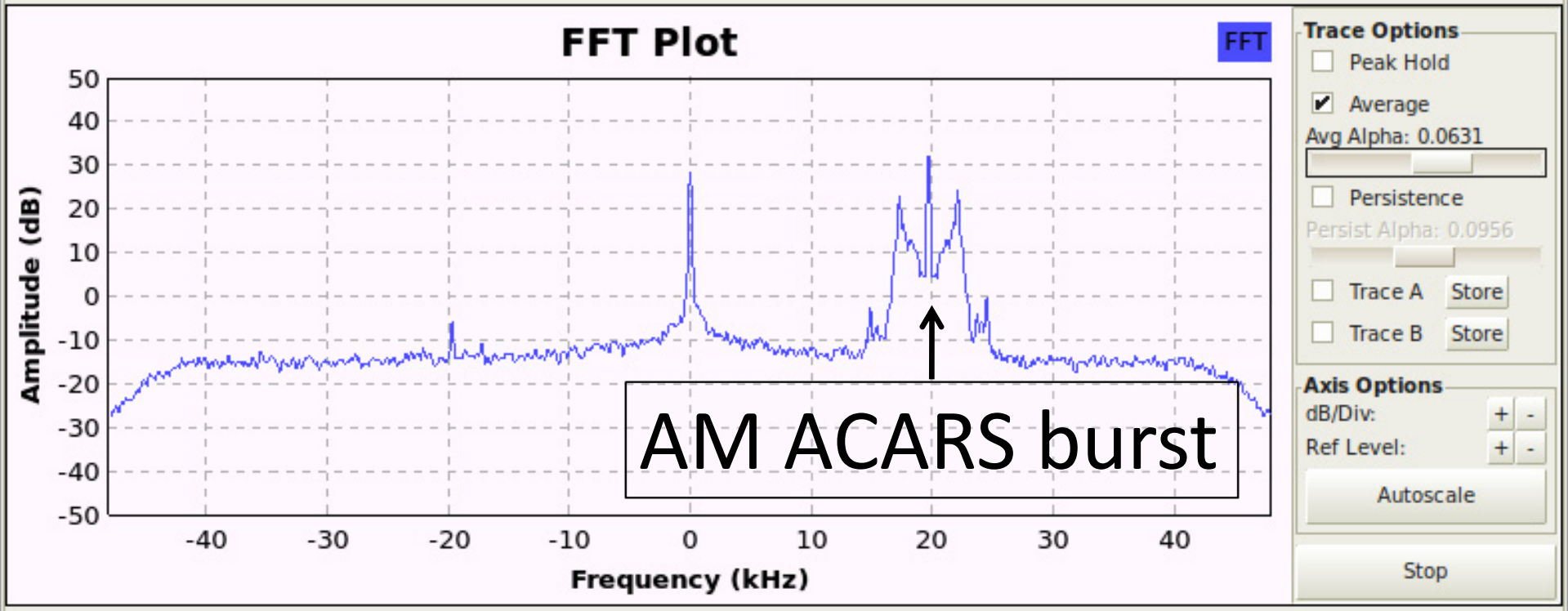
Acars Gui

xlate_fine: 0

xlate_coarse: 20k

xlate_bw: 8k

Main | PLL | AGC | Xlate | BB | Levels



Trace Options

Peak Hold

Average

Avg Alpha: 0.0631

Persistence

Persist Alpha: 0.0956

Trace A Store

Trace B Store

Axis Options

dB/Div: + -

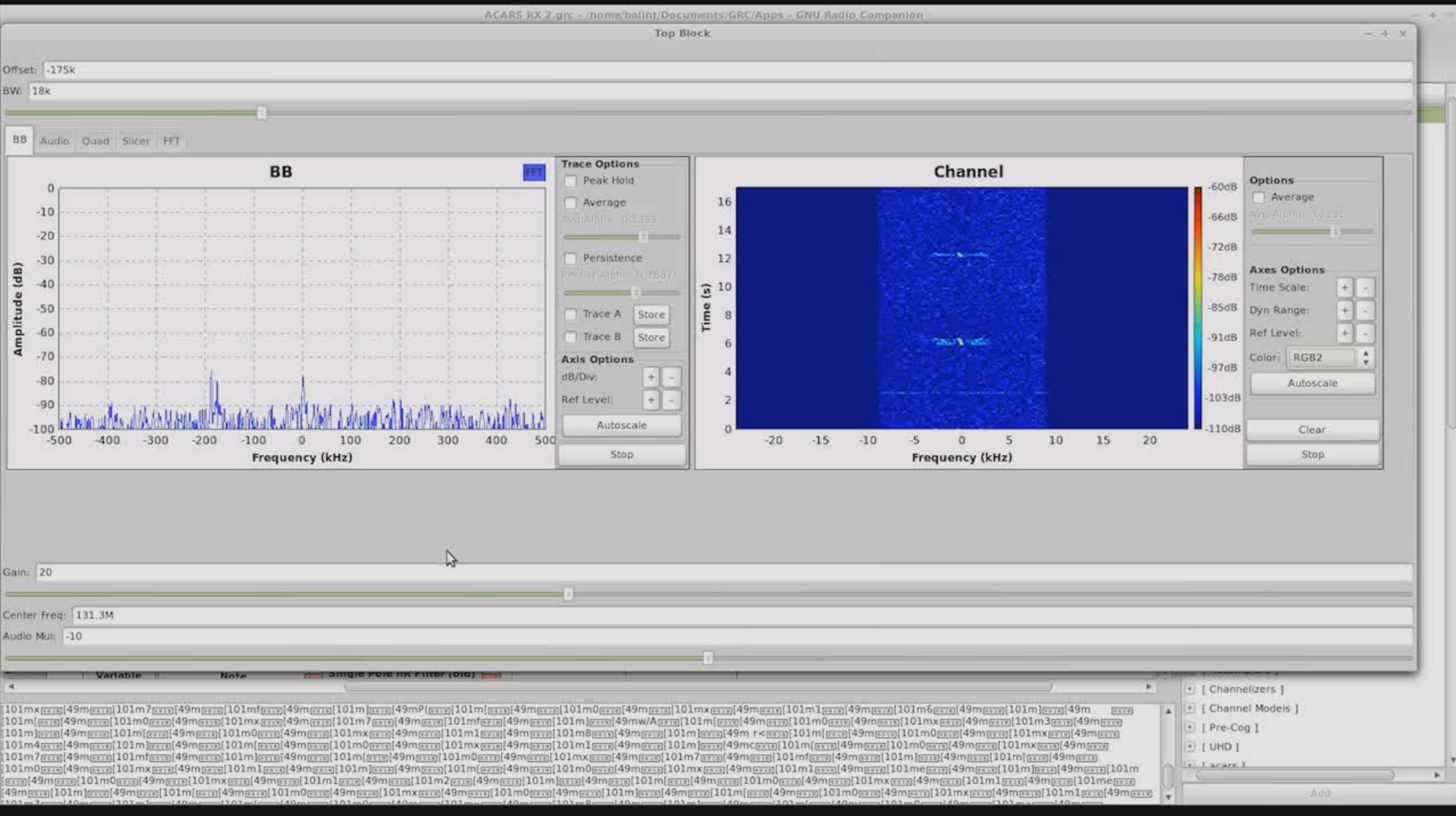
Ref Level: + -

Autoscale

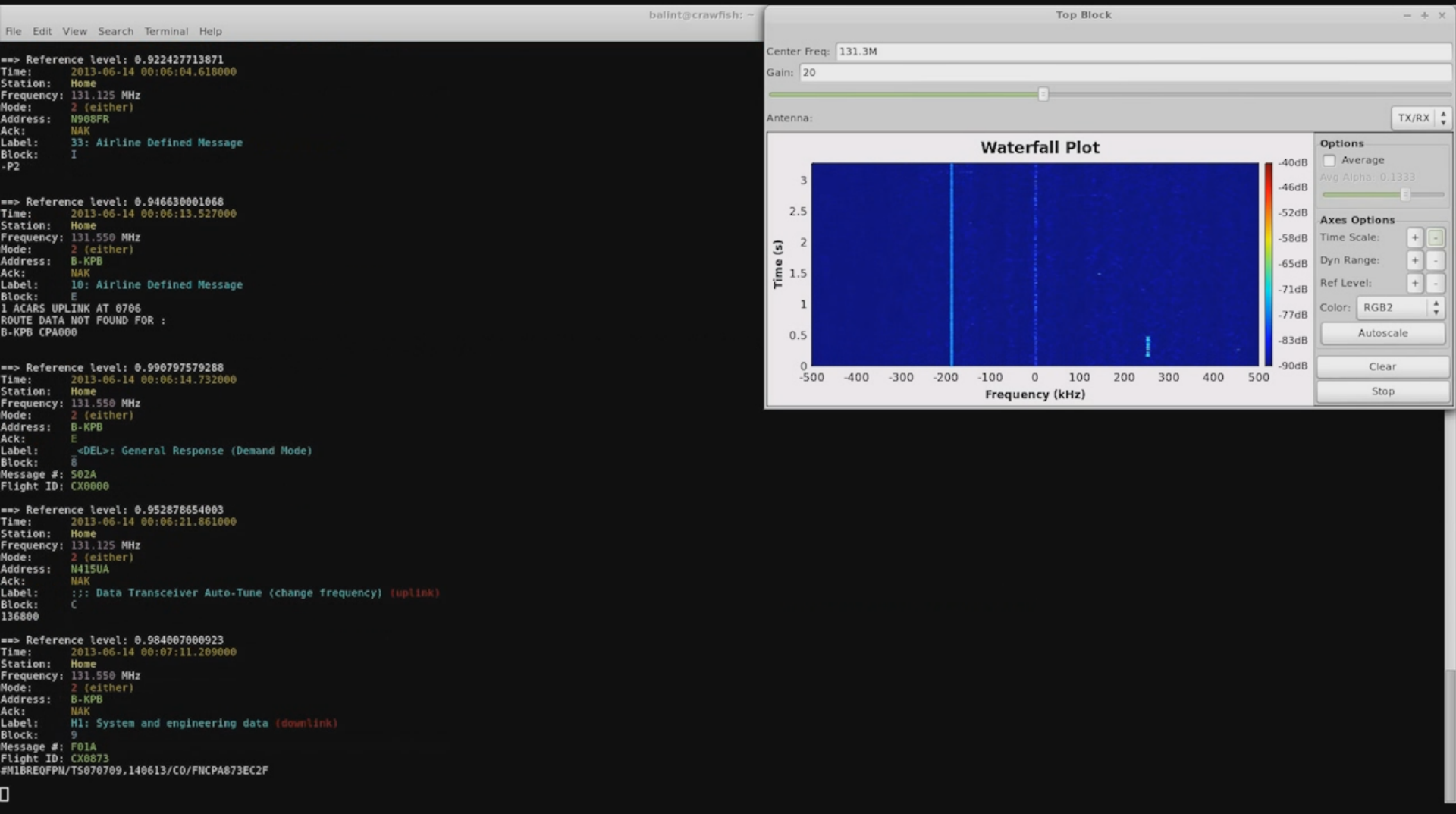
Stop

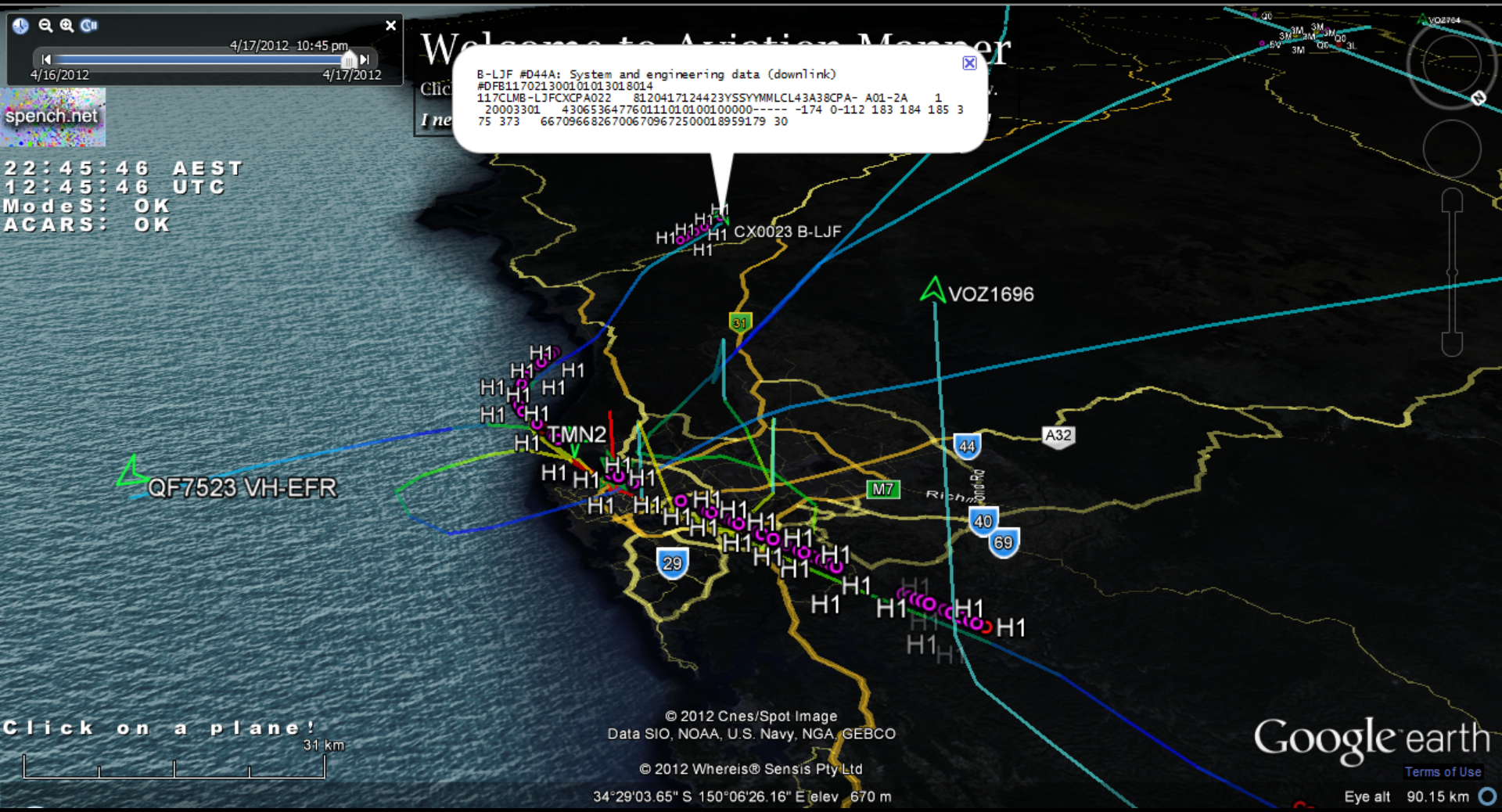
am_bw: 5k

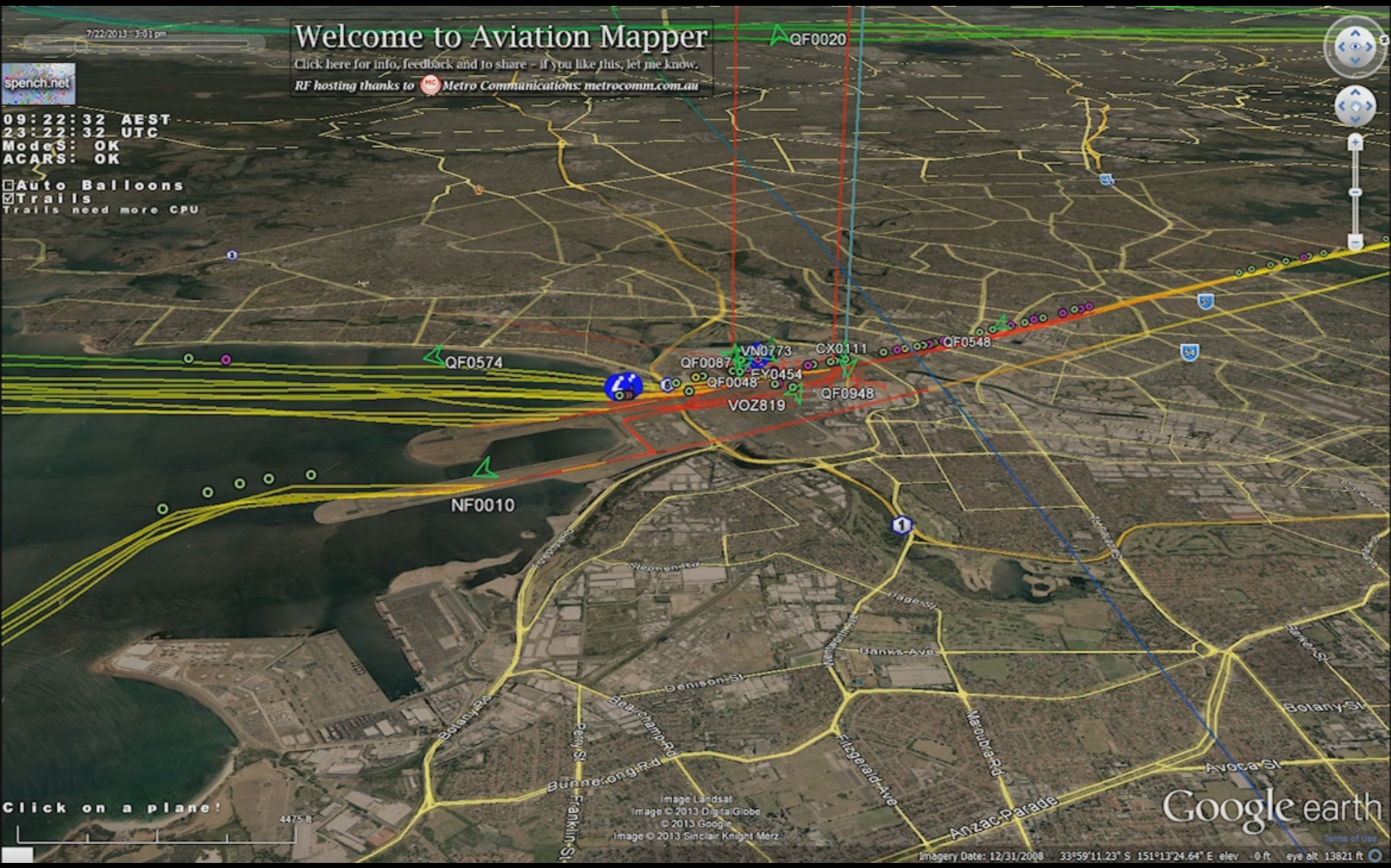
Multi-channel ACARS Decoder



Multi-channel ACARS Decoder




4/17/2012 10:45 pm
4/16/2012
4/17/2012
spench.net
22:45:46 AEST
12:45:46 UTC
ModeS: OK
ACARS: OK
B-LJF #D44A: System and engineering data (downlink)
#DFB1170213001010130180l4
117CLMB-LJFCXCPA022 8120417124423YSSYYMMLCL43A38CPA- A01-2A 1
20003301 430653647760111010100100000----- -174 0-112 183 184 185 3
75 373 66709668267006709672500018959179 30
CX0023 B-LJF
VOZ1696
QF7523 VH-EFR
TMN2
H1
31
44
A32
M7
40
69
29
Click on a plane!
31 km
© 2012 Cnes/Spot Image
Data SIO, NOAA, U.S. Navy, NGA, GEBCO
© 2012 Whereis® Sensis Pty Ltd
34°29'03.65" S 150°06'26.16" E elev 670 m
Google earth
Terms of Use
Eye alt 90.15 km


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
7/22/2013 3:01 pm
spench.net
09:22:32 AEST
23:22:32 UTC
Mode S: OK
ACARS: OK
Auto Balloons
Trails
Trails need more CPU
QF0020
QF0574
QF0087
VN0773
CX0111
QF0548
EY0454
QF0048
QF0948
VOZ819
NF0010
Click on a plane!
4475 ft
Image Landsat
Image © 2013 DigitalGlobe
© 2013 Google
Image © 2013 Sinclair Knight Merz
Google earth
Imagery Date: 12/31/2008 33°59'11.23" S 151°13'24.64" E elev 0 ft eye alt 13821 ft

Examples

```
Time:      2011-11-16 09:12:24.073000
Station:   Home
Frequency: 131.55 MHz
Mode:      s (uplink, LCN: 19)
Address:   9M-MPO
Ack:       NAK
Label:     31: Airline Defined Message
Block:     W
S
1. TOILET CC1-INOP
2. ROW 30-31 DEFG-CARPET FLOOR VERY WET
2. GALLEY 3-CART LIFT FLOODED
```

Examples

```
Time:       2011-11-16 09:49:00.255000
Station:    Home
Frequency:  131.45 MHz
Mode:       2 (either)
Address:    VN-A375
Ack:        NAK
Label:      H1: System and engineering data (downlink)
Block:      4
Message #:  C12A
Flight ID:  VN0773
#CFB.1/MPF/ANVN-A375/FIHVN773
/DM111115224900NOV1514042244PFR1/DAVVTS/DSYSSY/FR383141VSC
1,,,,,,,LAV 37,HARD,140505;237346CIDS1  1,,,,,,,DEU A
(200RH2),HARD,140505;383141VSC    1,,,,,,,LAV 53,HARD,174906;
```

Examples

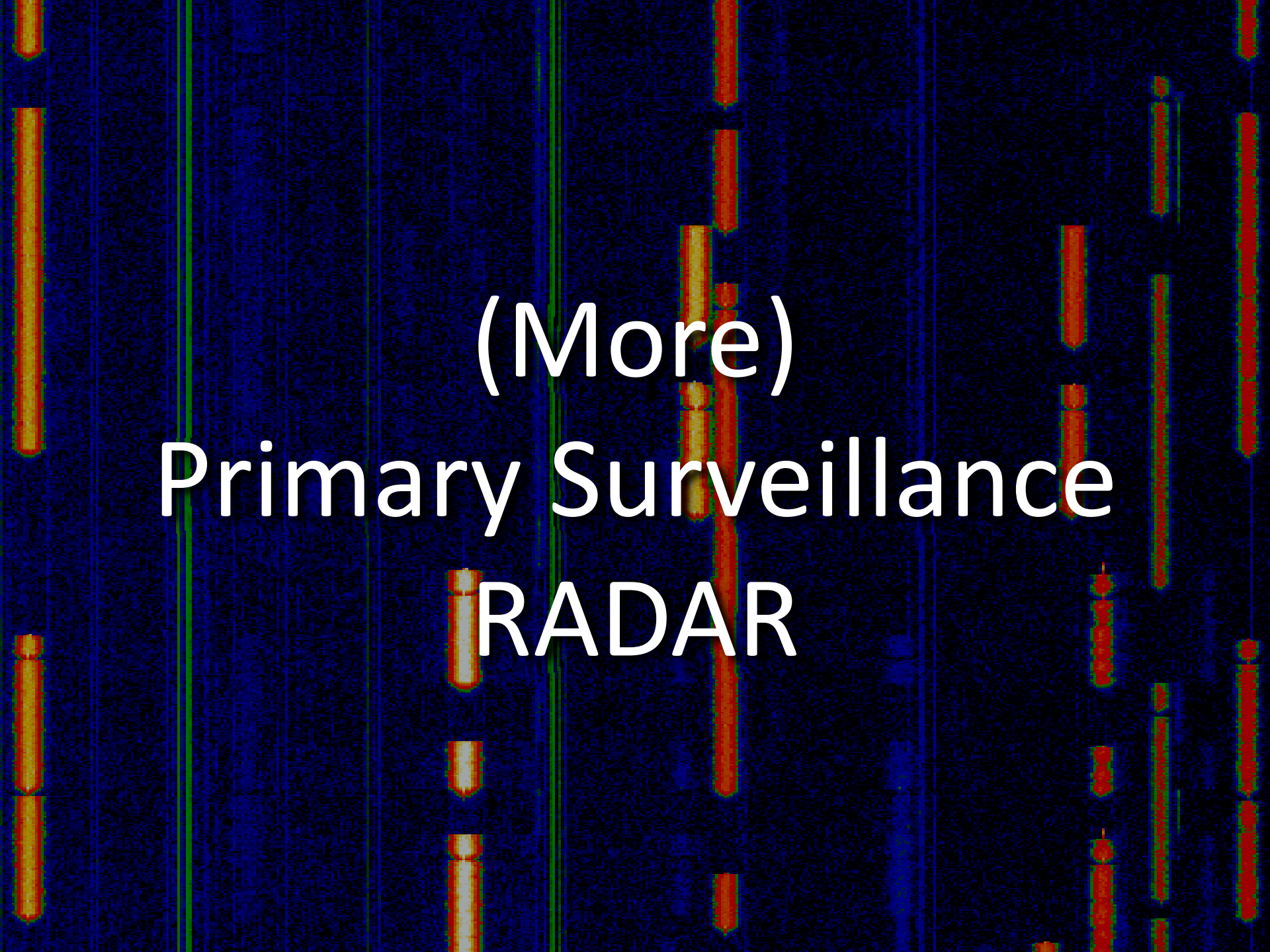
```
Time:       2011-11-16 09:49:06.844000
Station:    Home
Frequency:  131.45 MHz
Mode:       2 (either)
Address:    VN-A375
Ack:        NAK
Label:      H1: System and engineering data (downlink)
Block:      5
Message #:  C12B
Flight ID:  VN0773
#CFB383141VSC    1,,,,,,,LAV 61,HARD,202806;344137WXR2
1,,,,,,,WXR MOUNTING TRAY (5SQ),INTERMITTENT,203506,EOR
```


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!
4/13/2012
2012
2012
spench.net
Mitchell Hwy
Barrier Hwy
ModeS: OK
ACARS: OK
BANDA
CORKY
BULGA
LV-ZRA #C71C: System and engineering data (downlink)
#CFBAULT,212606;2128455MAINTENANCE STATUS CRG VENT,213006/FR212300VC X2
,,,,,,,GALY LAV DUCT CLOGGED,HARD,,EOR
PRAWN
PRAWN
H1
H1
H1 'System and engineering data' regarding the (failure of) toilets?
Kume Hwy
RAZZI
http://maps.spench.net/aviation/
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


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
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
GUTEV
GATOR
IGOPO
ROBIN
NERTI
DUMAV
EGORE
MONIC
RUVAP
NORMA
MELBO
TIMET
DOTAP
TASHA
FORMA
SARIK
TAVEV
NONET
VILOL
AKLET
ONIVI
MACLA
UNDER
GRABL
DUNDA
HECTO
FLAKE
FILET
FAGIN
ACTIN
BLACK
MAXEM
POINT
Data SIO, NOAA, U.S. Navy, NGA, GEBCO
© 2012 Cnes/Spot Image
© 2012 Whereis® Sensis Pty Ltd
Click on a plane!
2709 km
Waiting for krump-dev...
3°56'15.16" N 93°48'49.69" E elev -1305 m
Google earth
Terms of Use
Eye alt 5231.14 km

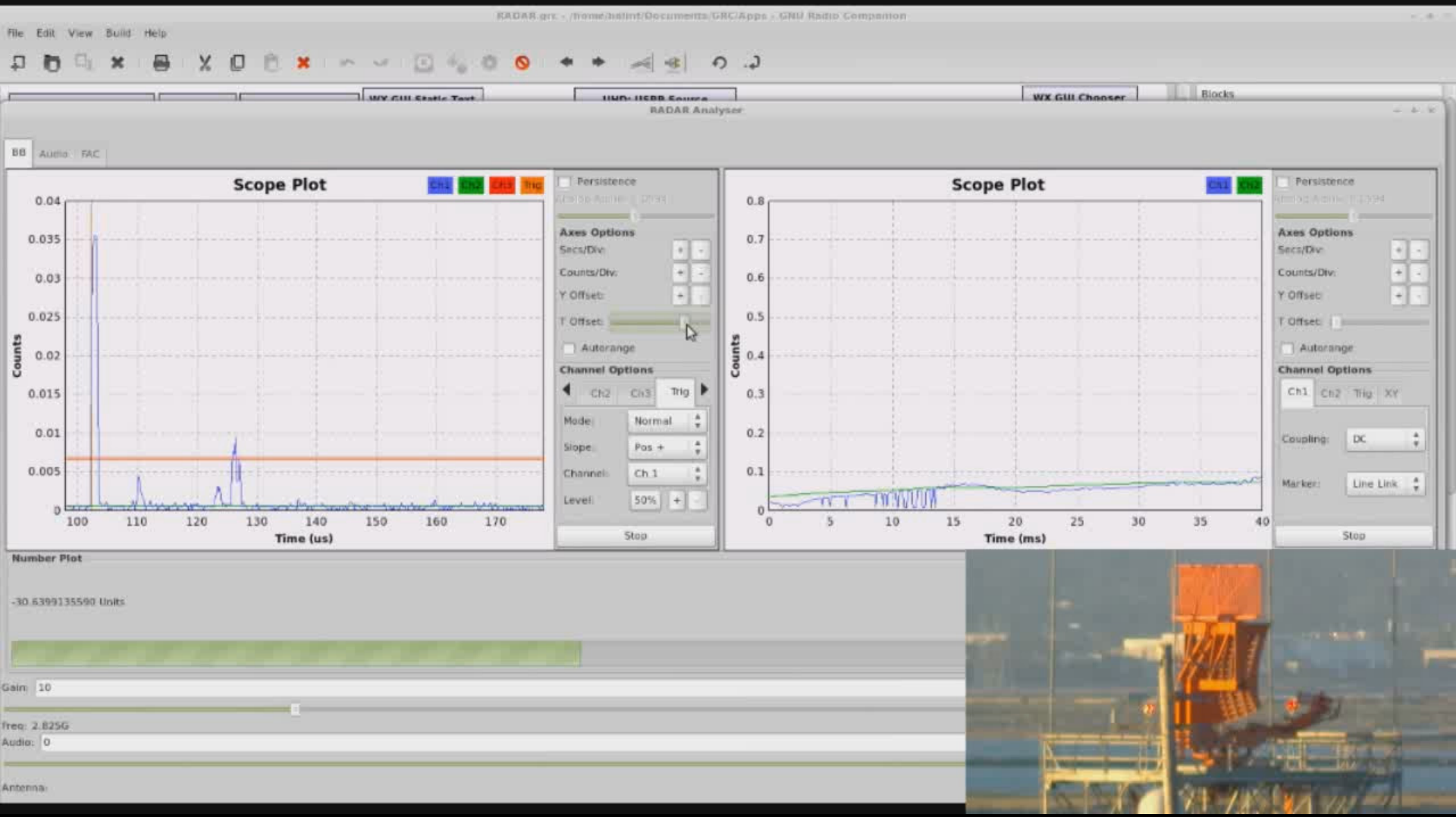
What about no ADS-B?

- No position reports
- Signal is high bandwidth
- Multiple remote USRPs can be sync'd with GPSDO
- Perform multilateration on non-ADS-B ('plain old' Mode S)
- Calculate position from TDOA

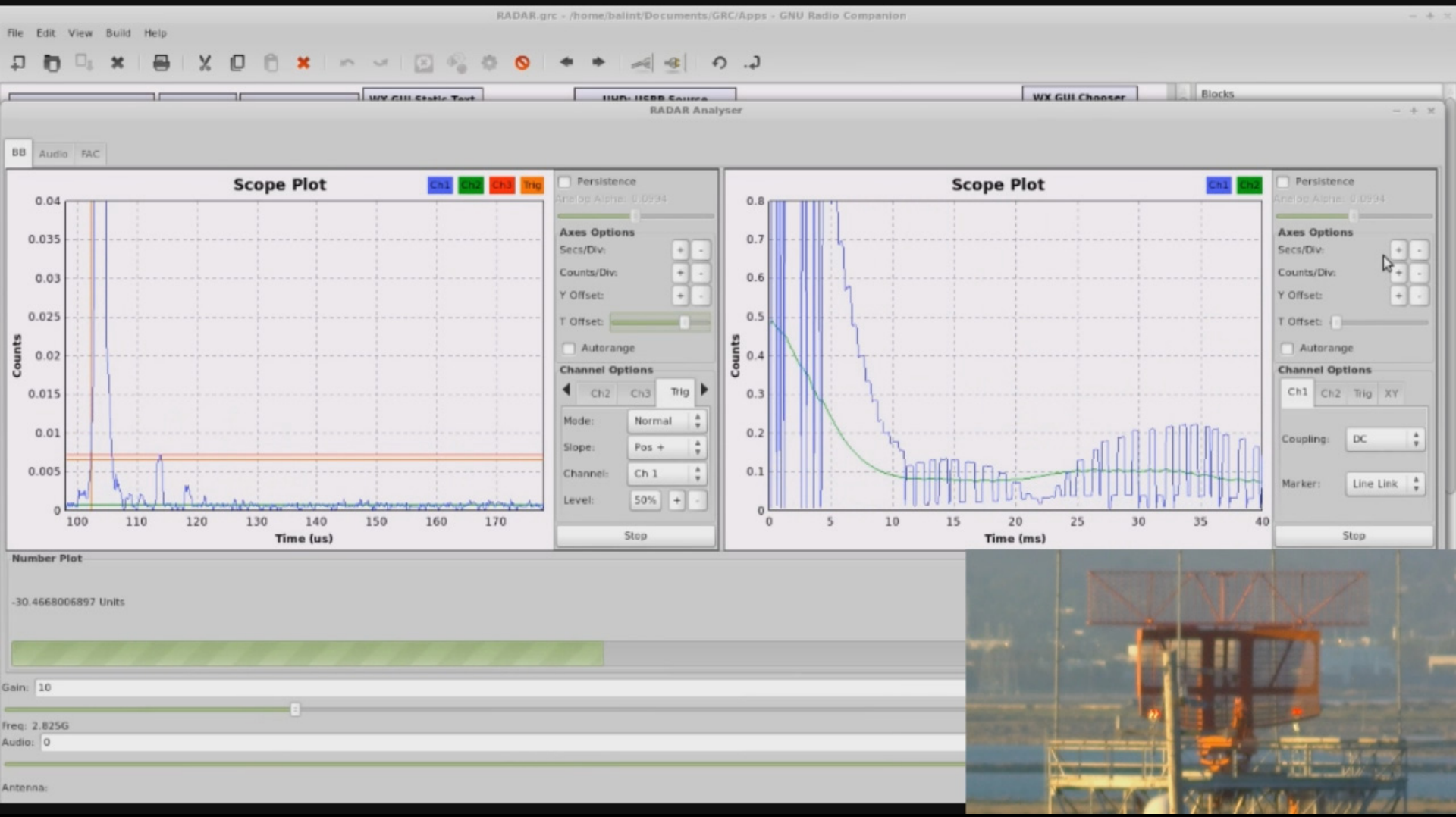

(More)
Primary Surveillance
RADAR

Moffett Field ASR-9

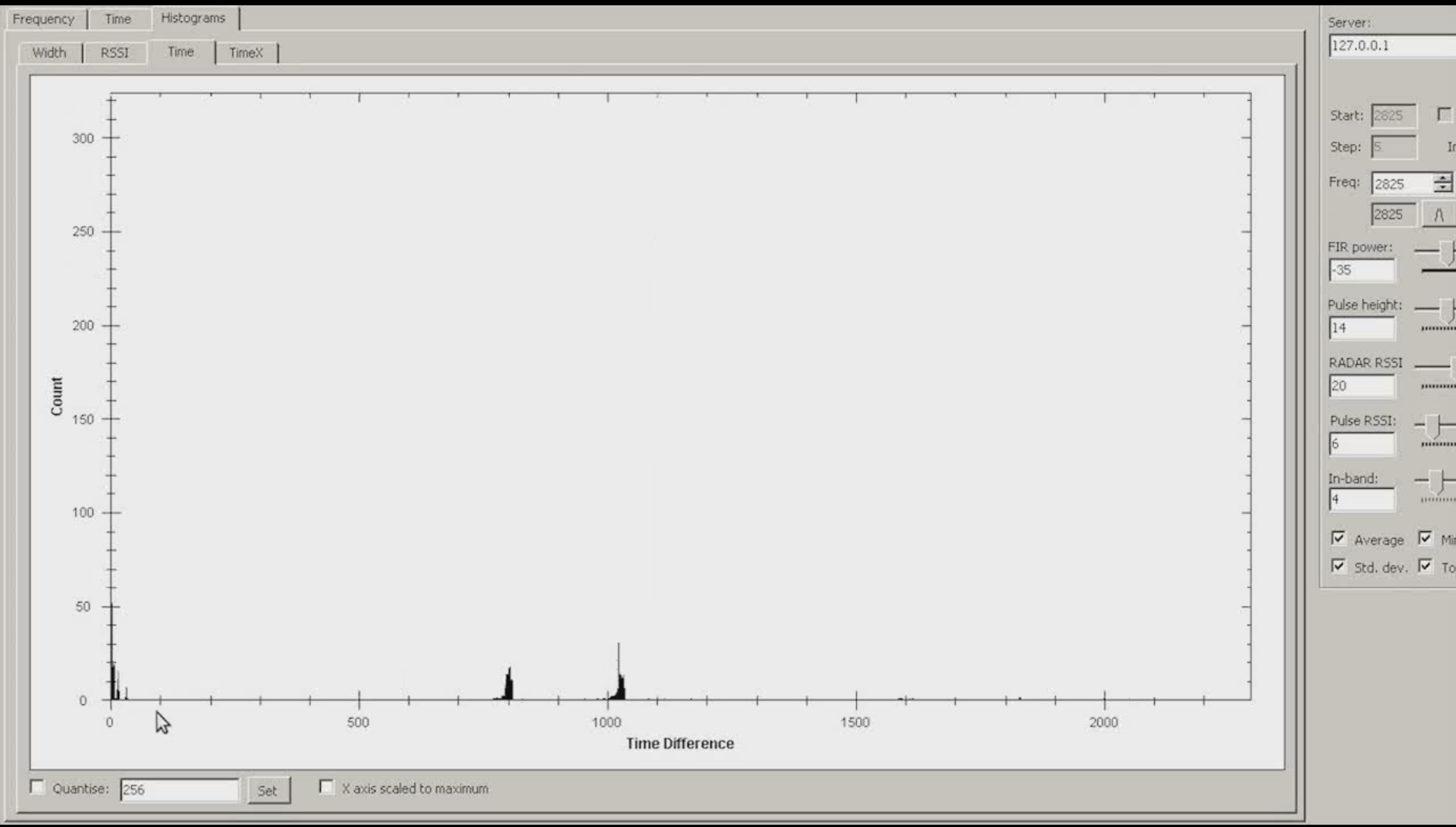
Primary Surveillance RADAR



Primary Surveillance RADAR



Primary Surveillance RADAR



Dual PRF Mode: Weather

TABLE 1

MMAC Academy ASR-9 System Characteristics

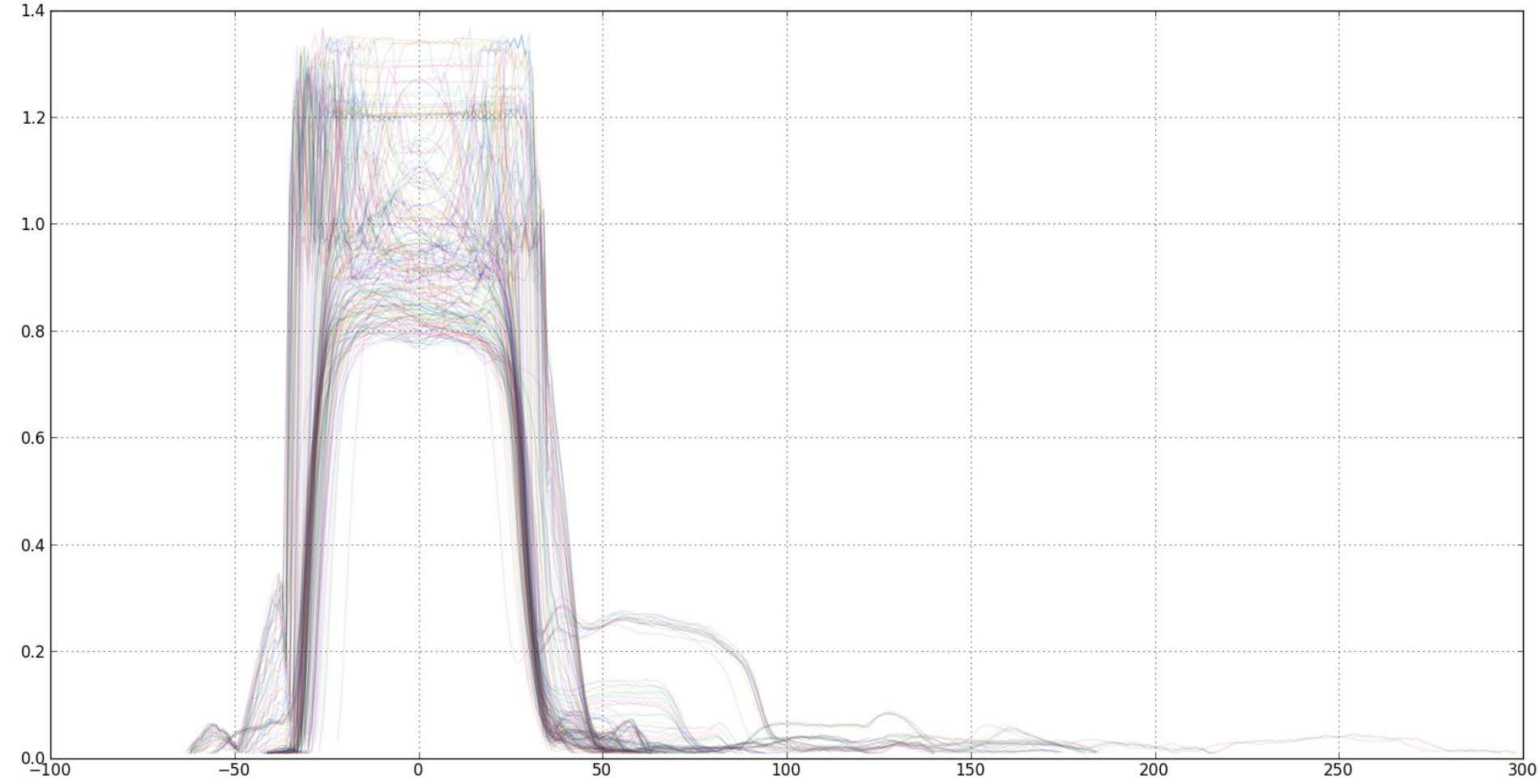
Frequency	2.7 GHz
Peak Power	1.1 MW
Pulse Length	1 μs
Pulse Repetition Frequency	Dual PRF (1160 Hz average)
Antenna Gain	34 dB
Azimuth Beamwidth	1.4°
Elevation Beamwidth	4.8°
Rotation Rate	12.5 rpm
Range Gate Spacing	116 m
Azimuthal Resolution	1.4°
Sensitivity	1 m^2 @ 111 km
System Stability	48 dB

```
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 */
```

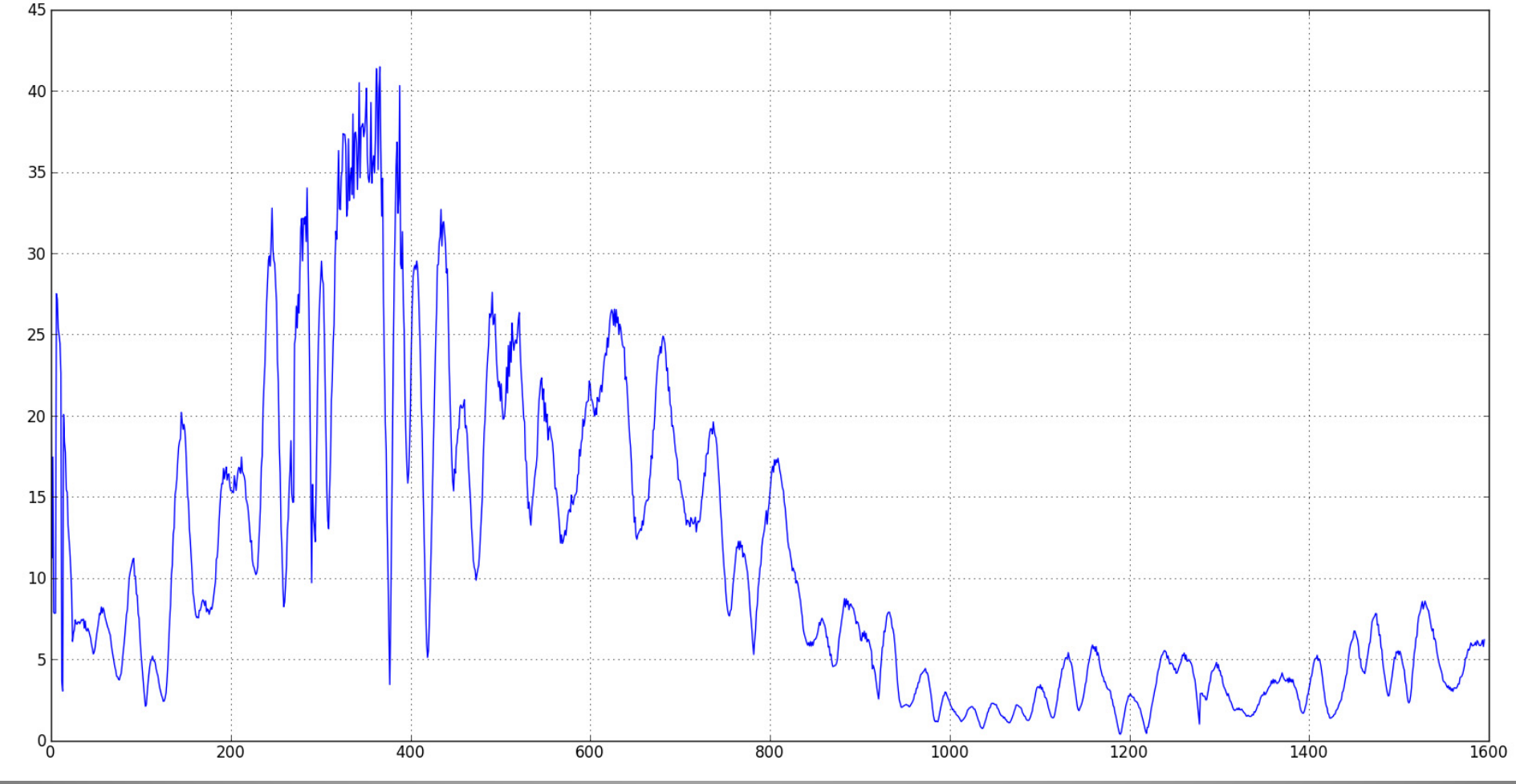
Radar energy entering this trapping layer can be refracted through an effective curve with a radius smaller than that of the Earth, returning to scatter off the surface some distance from the radar. If the layer is of large horizontal extent radar energy scattered back into the atmosphere from the surface 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.

Capture at 50 Msps to RAM

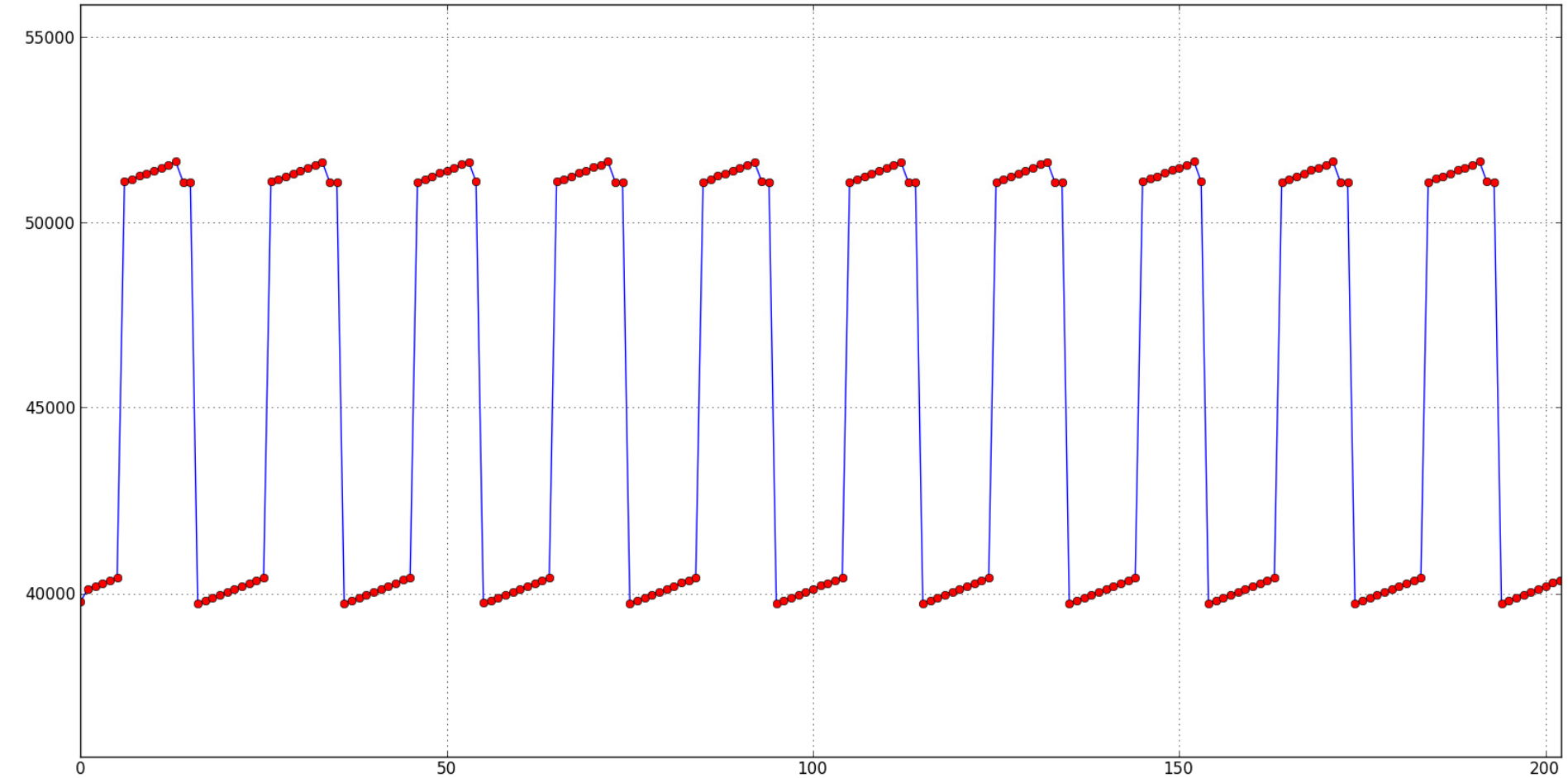
Pulse Envelope



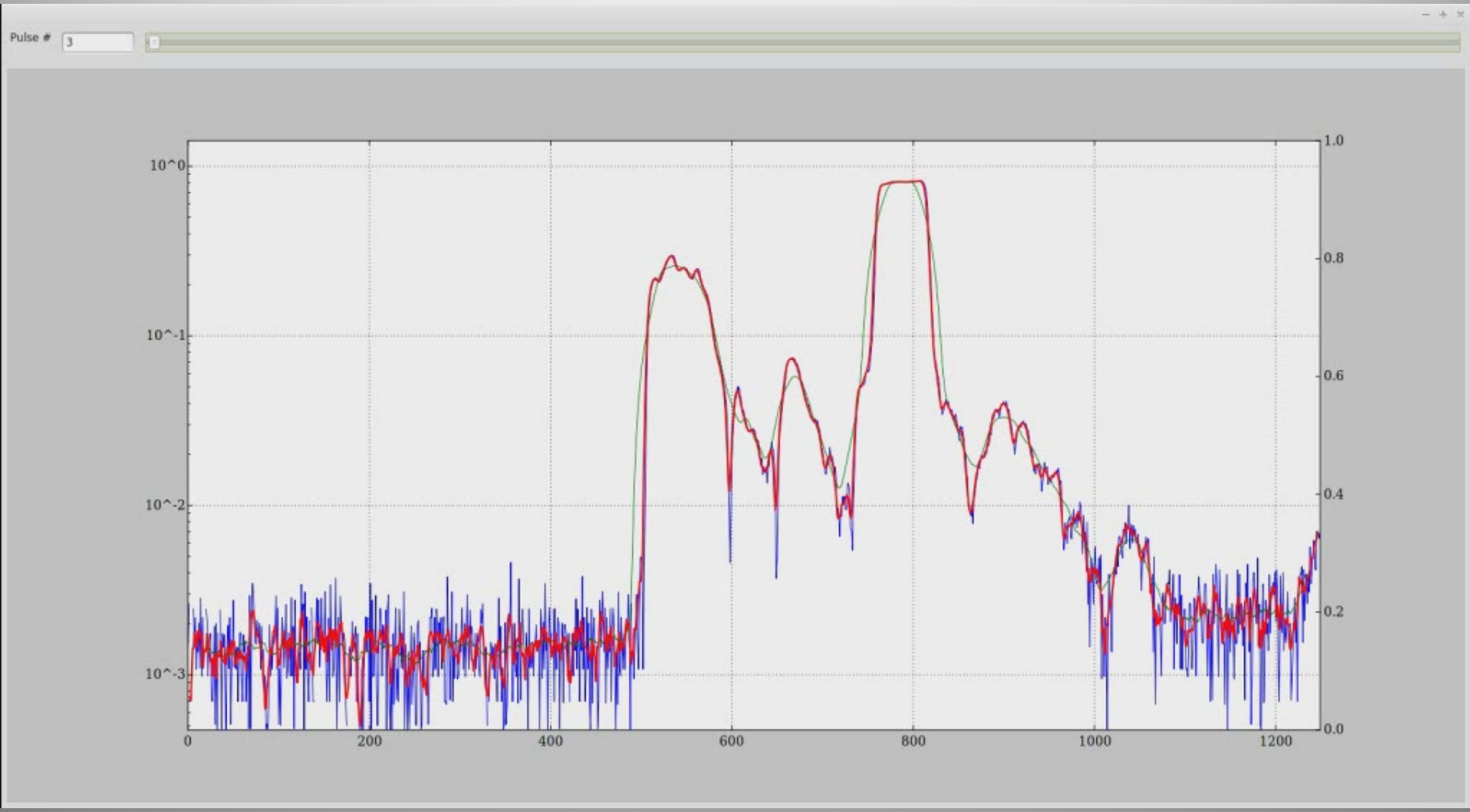
Pulse Power vs. Time

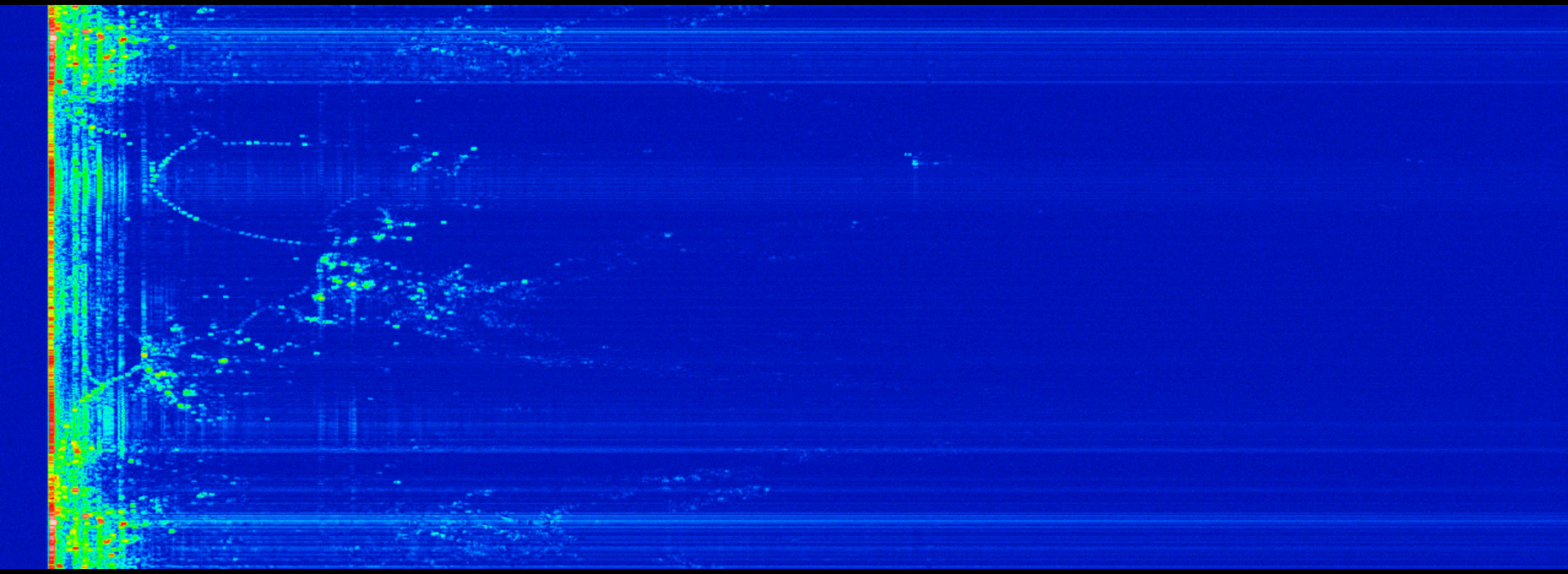


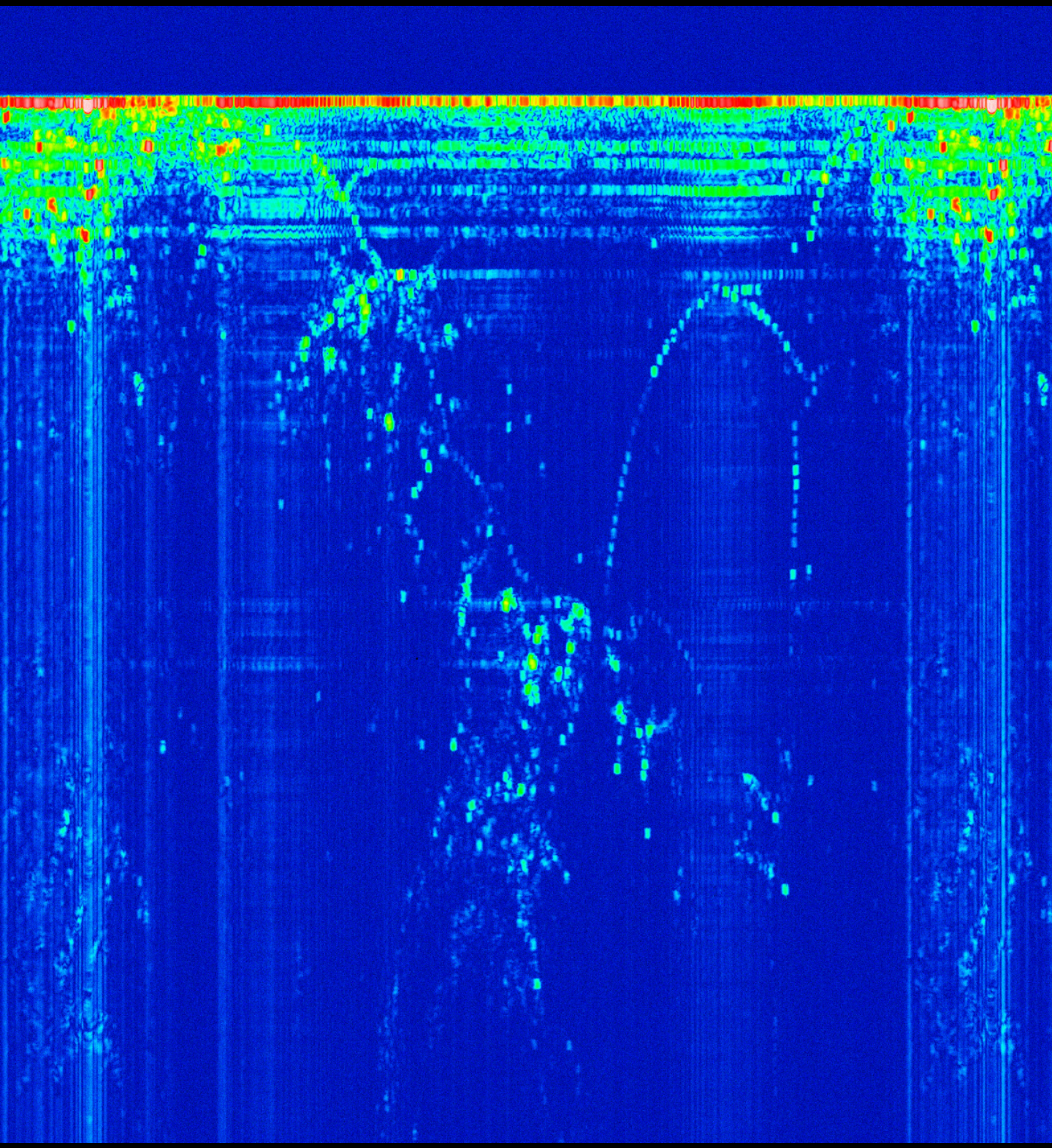
Distance Between Pulses

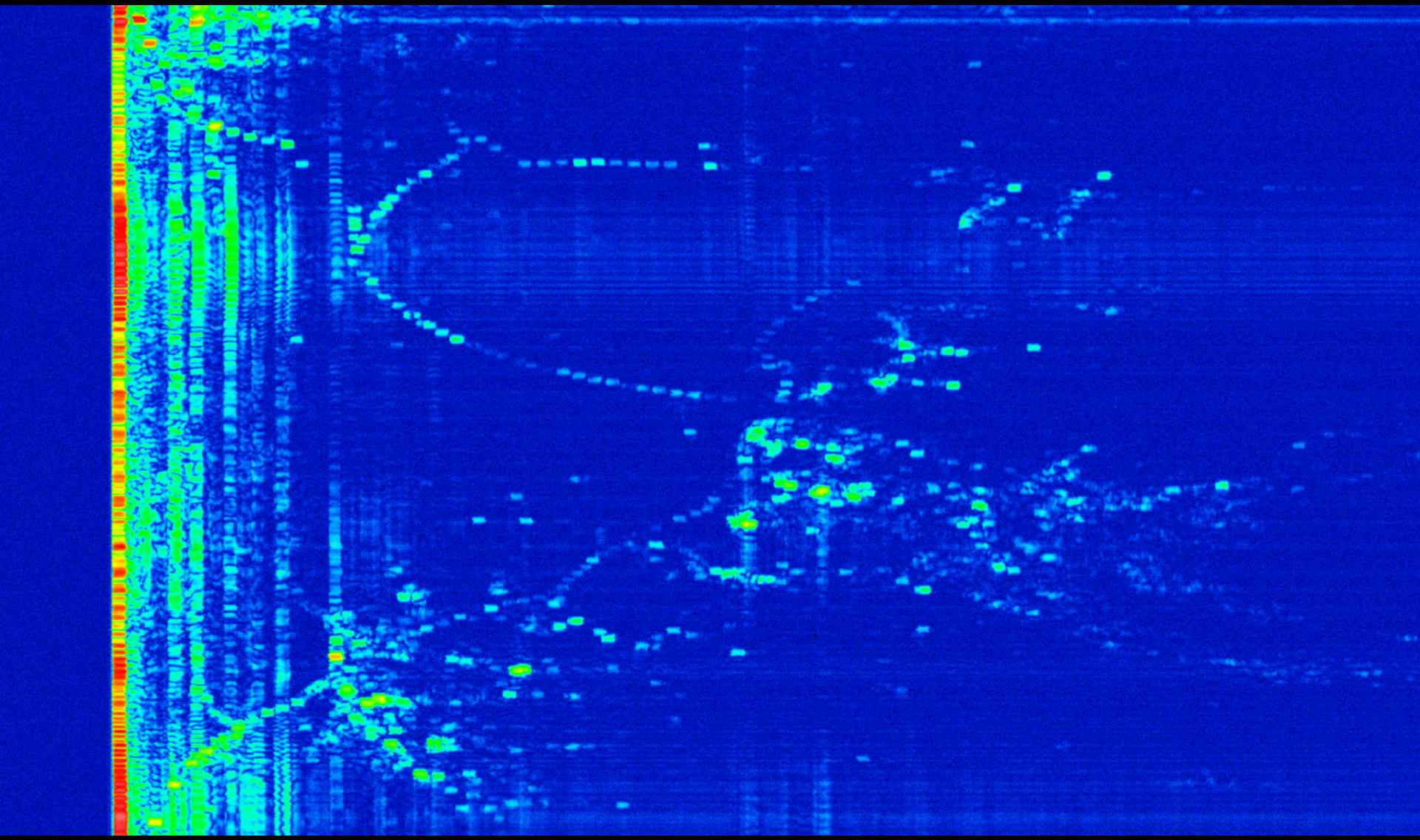


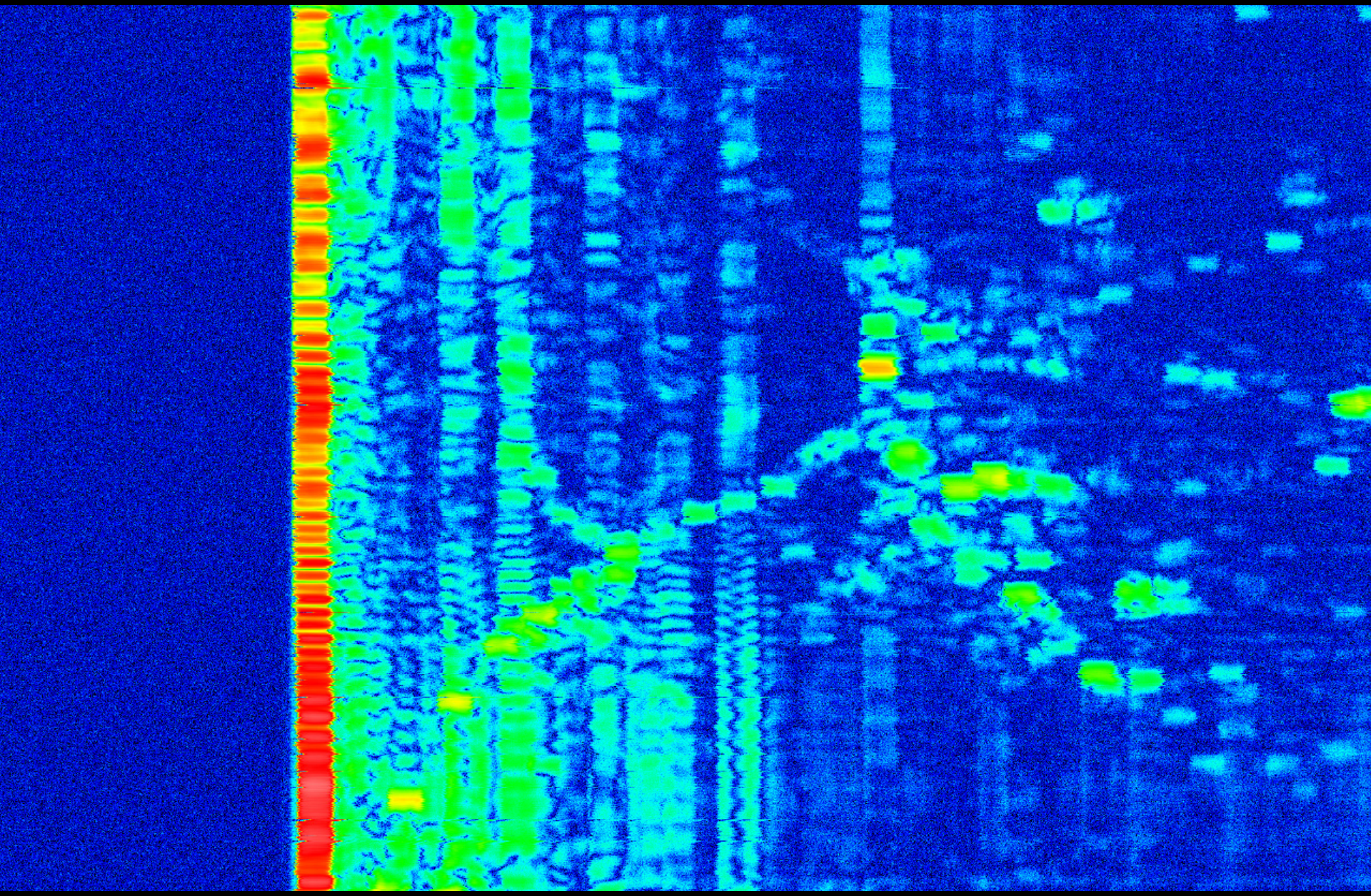
Pulse and echo power over time

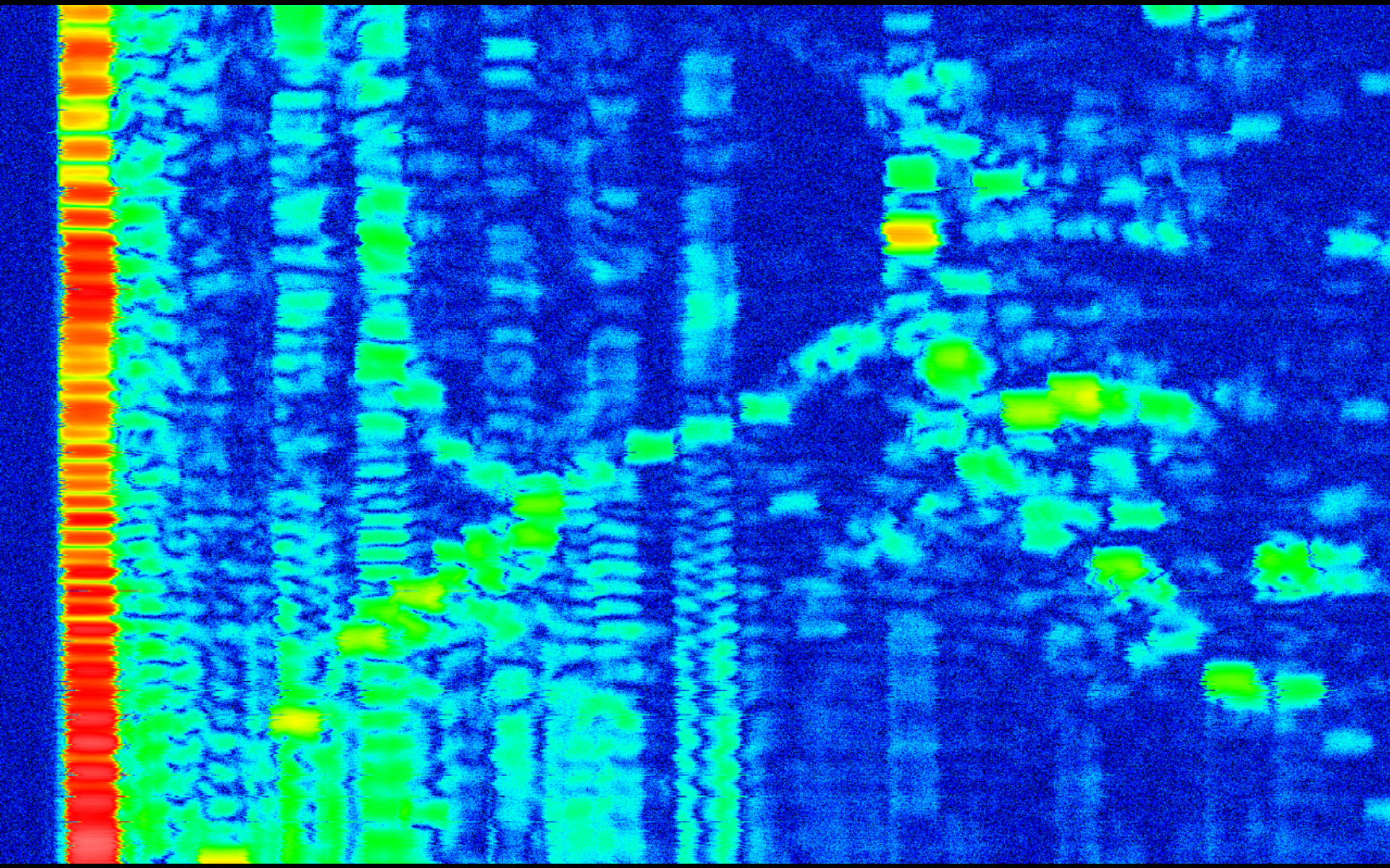


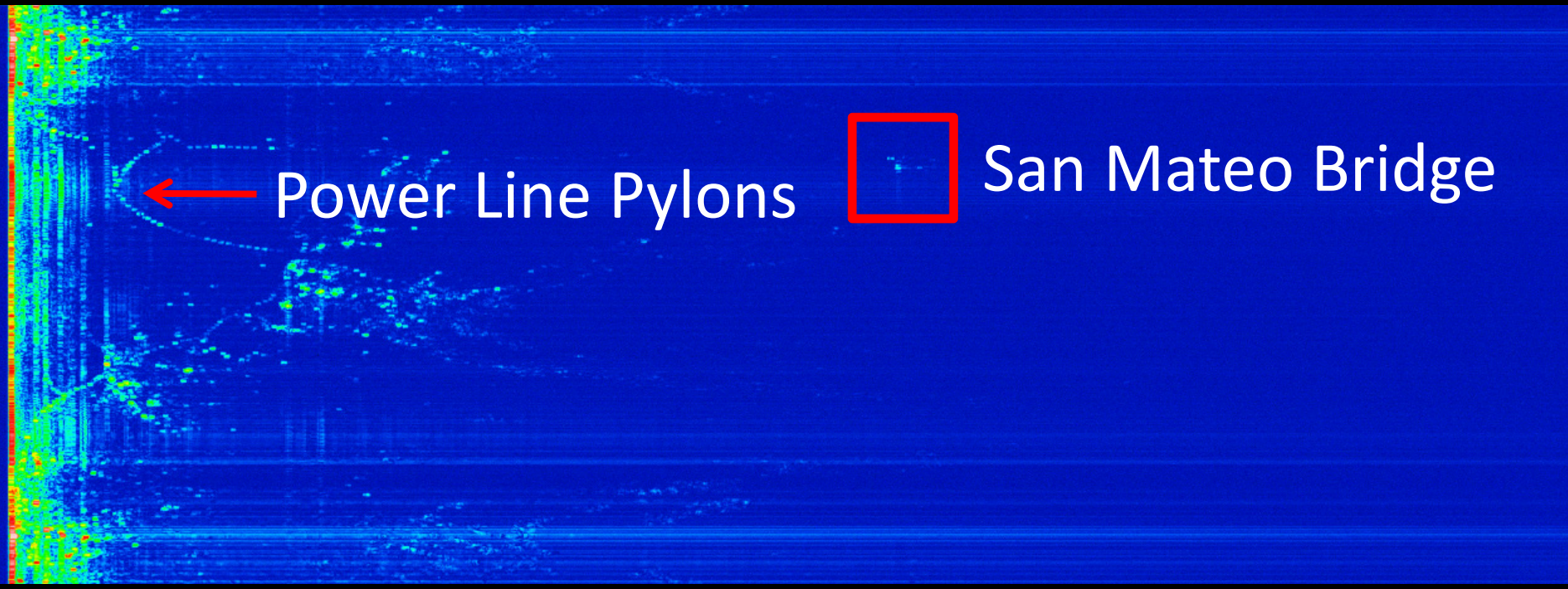




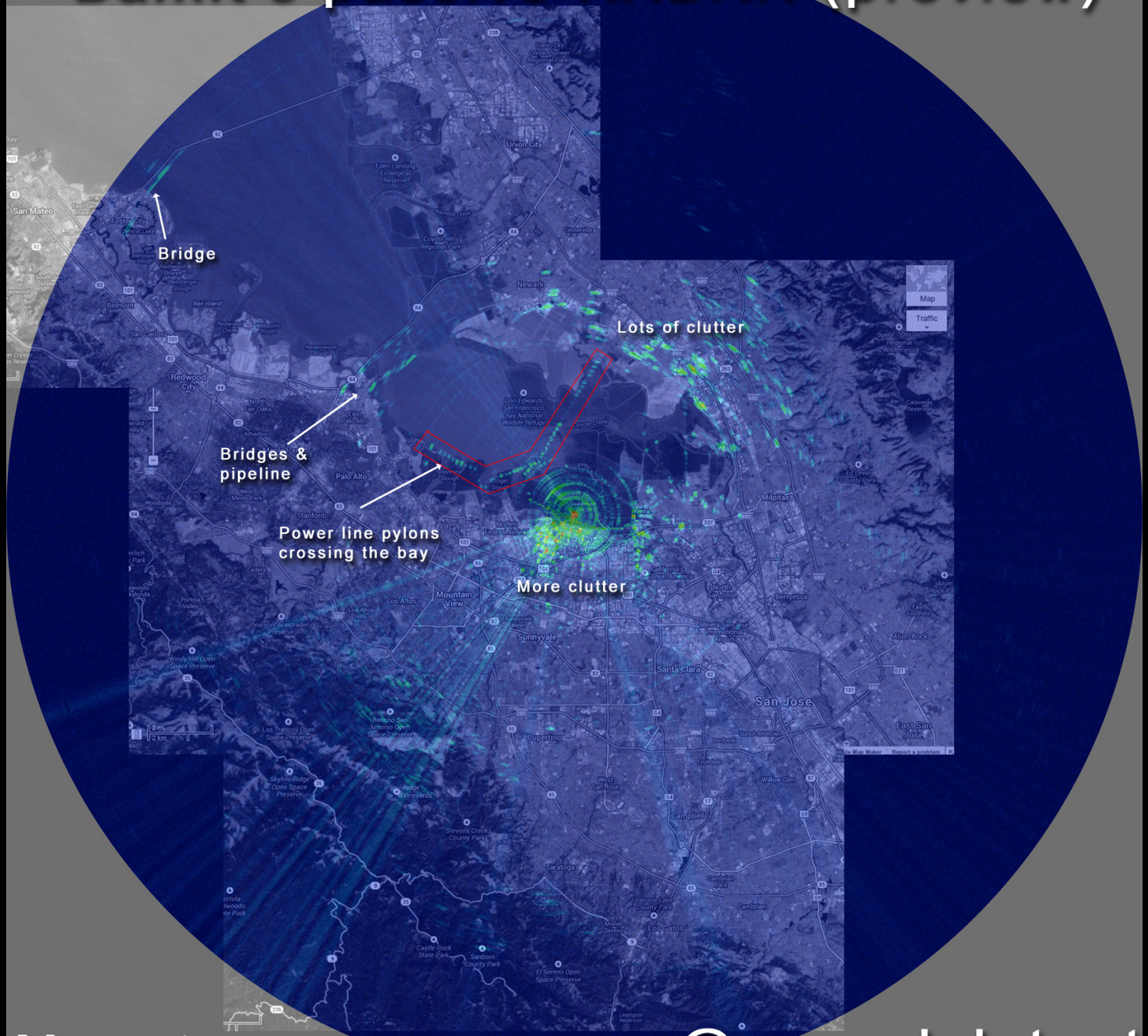






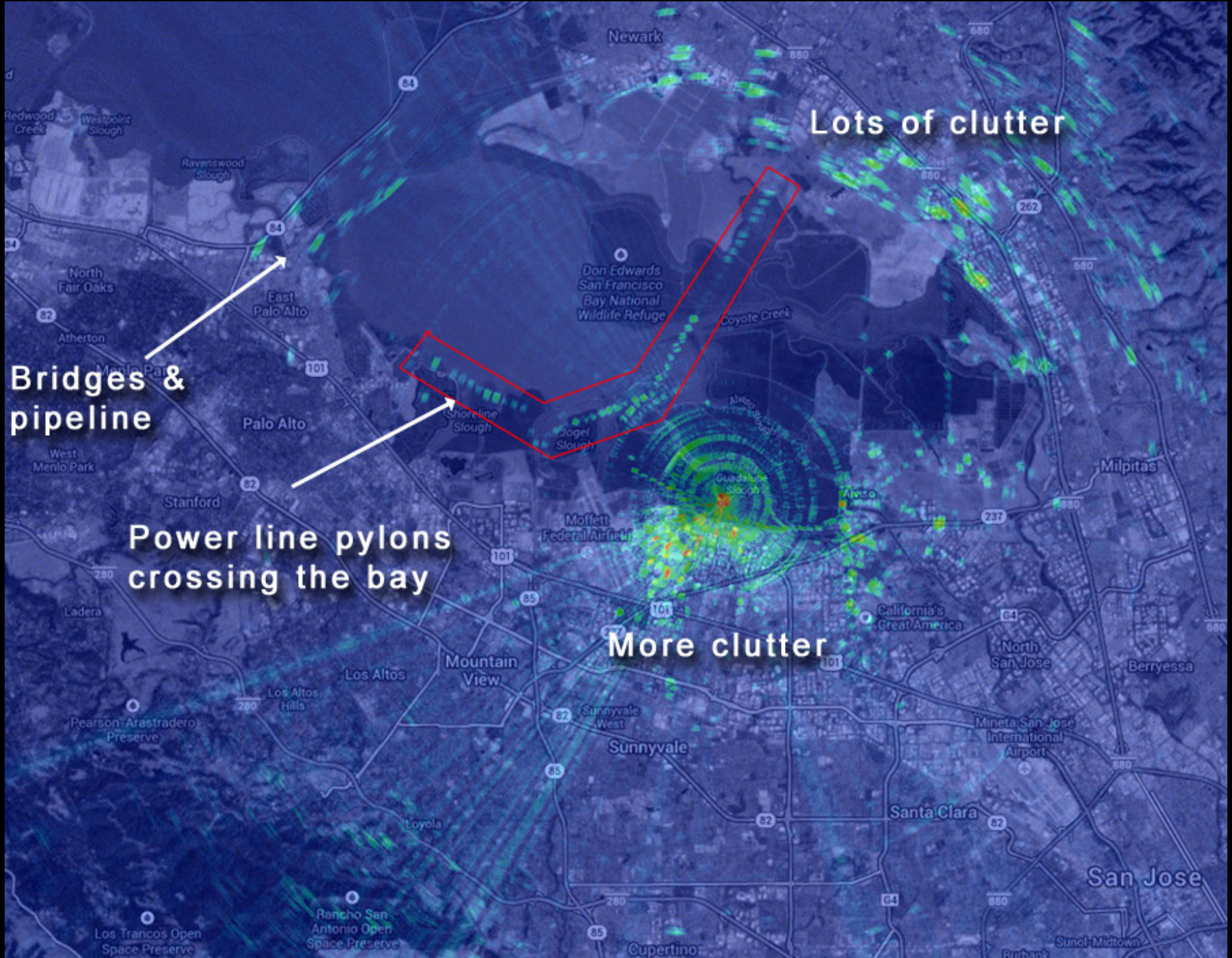

Power Line Pylons
San Mateo Bridge

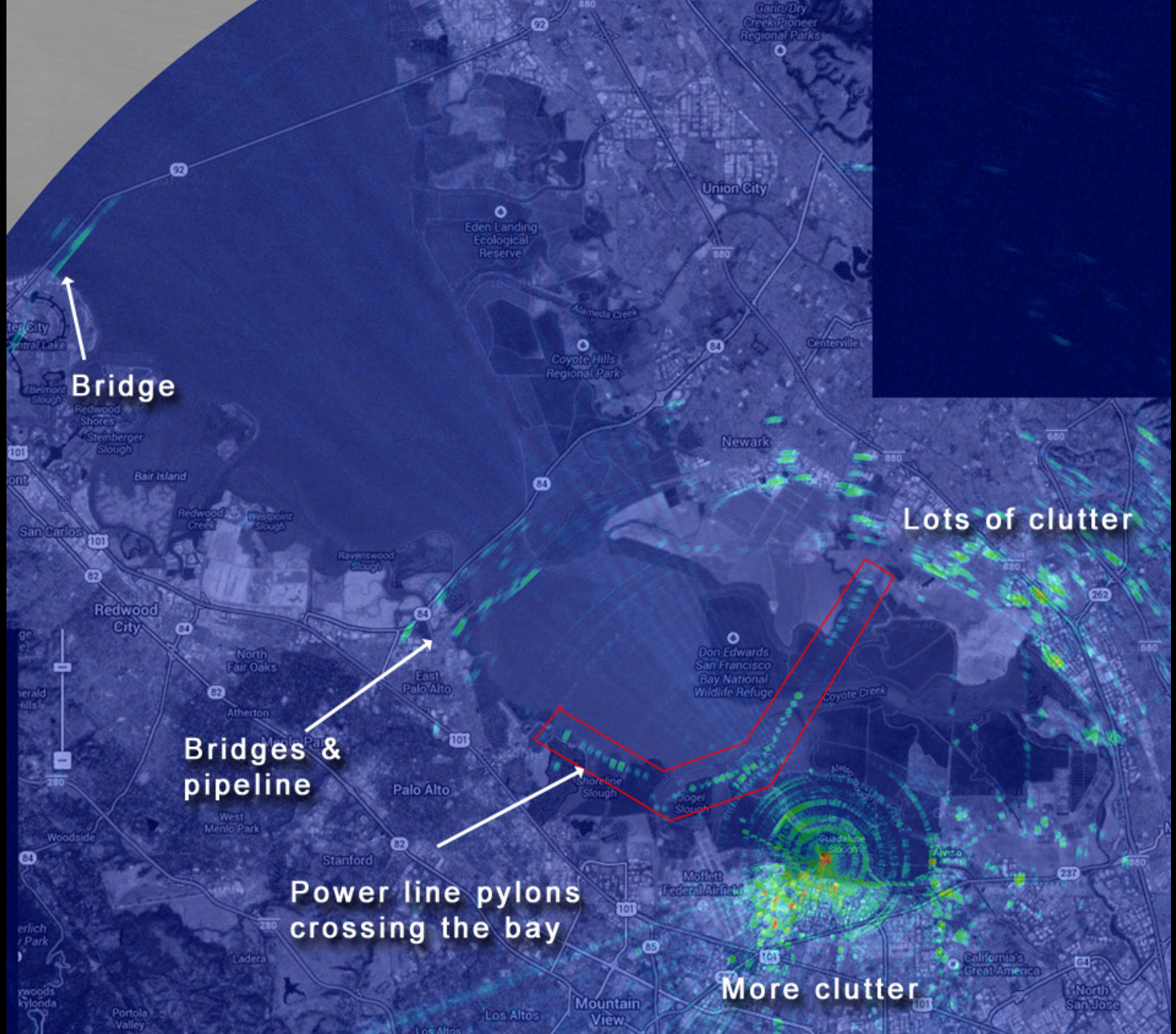
Balint's passive RADAR (preview)



More to come...

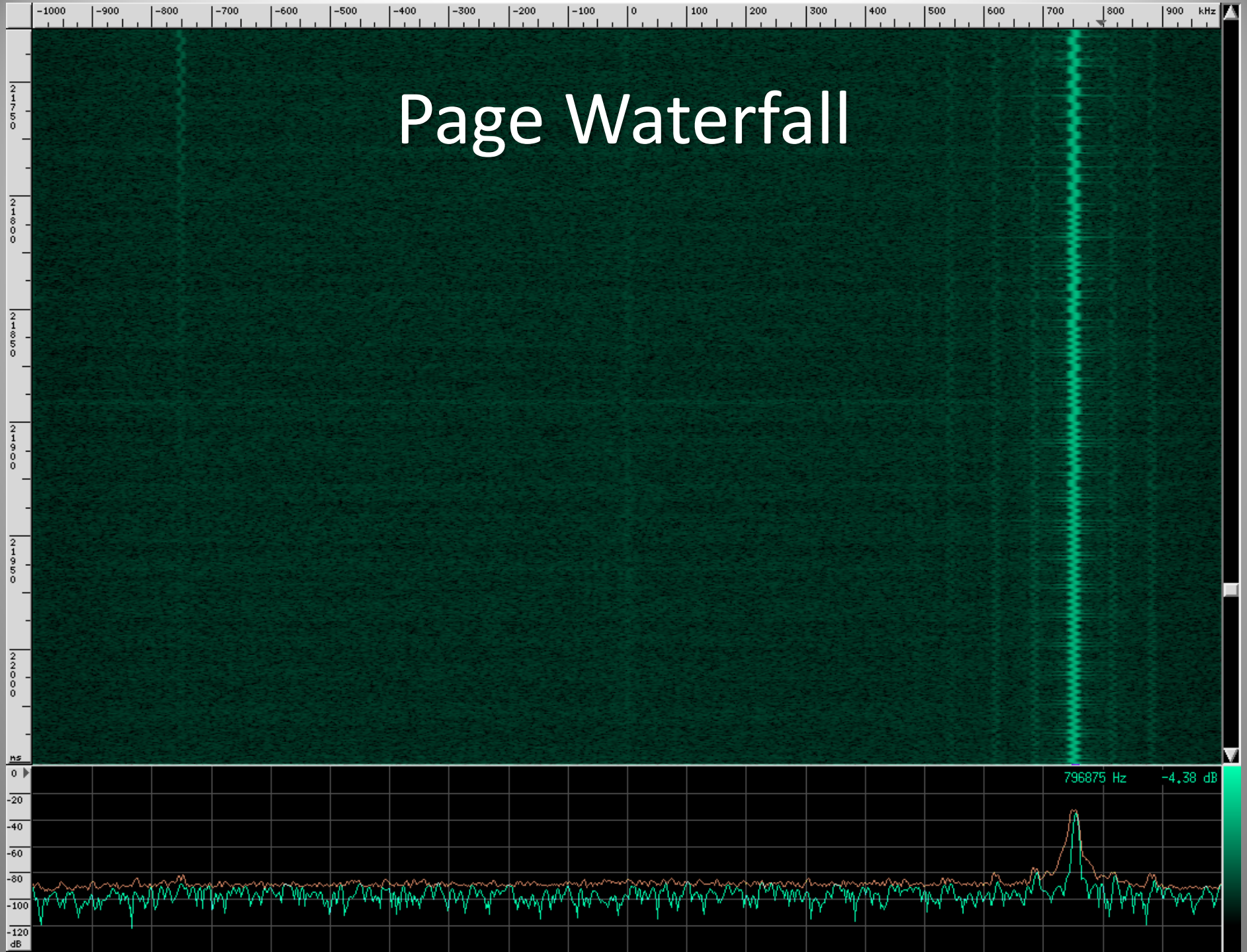
@spenchdotnet


Lots of clutter
Bridges & pipeline
Power line pylons crossing the bay
More clutter
Newark
Don Edwards San Francisco Bay National Wildlife Refuge
Coyote Creek
Palo Alto
Stanford
Moffett Federal Airfield
Mountain View
Los Altos
Sunnyvale
Santa Clara
San Jose
Milpitas
Alviso
California's Great America
Mineta San Jose International Airport
Cupertino
Loyola
Pearson-Arastradero Preserve
Los Trancos Open Space Preserve
Rancho San Antonio Open Space Preserve
Ladera
Los Altos Hills
Sunnyvale West
North San Jose
Berryessa
Sunol-Midtown
Redwood Creek
Westpoint Slough
Ravenswood Slough
North Fair Oaks
East Palo Alto
Atherton
Menlo Park
West Menlo Park
Shoreline Slough
Jogel Slough
Guadalupe Slough
Alviso Slough

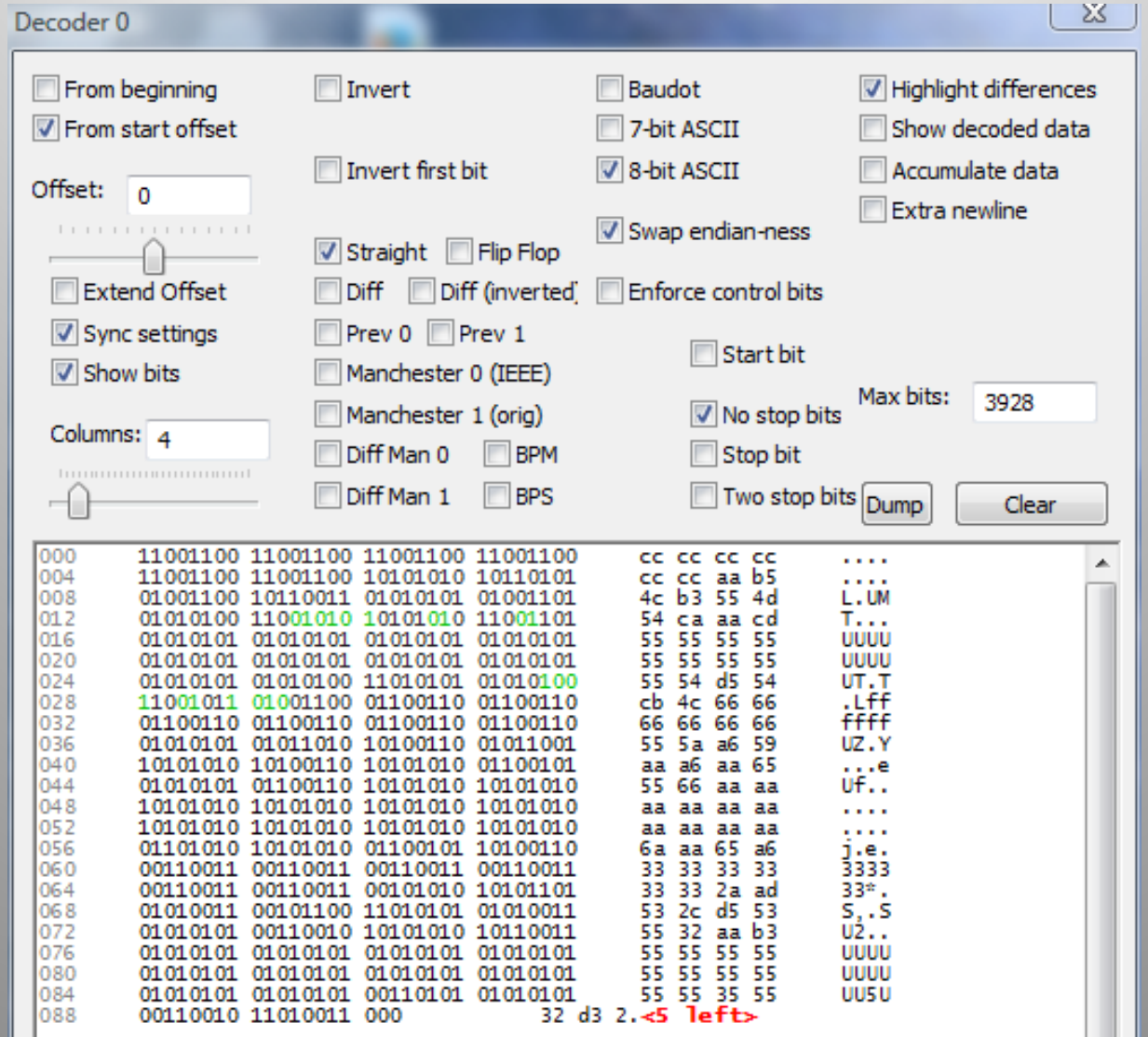

Bridge
Lots of clutter
Bridges &
pipeline
Power line pylons
crossing the bay
More clutter
Union City
Eden Landing
Ecological
Reserve
Coyote Hills
Regional Park
Newark
Redwood
City
Palo Alto
Stanford
Menlo Park
East
Palo Alto
Don Edwards
San Francisco
Bay National
Wildlife Refuge
Mountain
View
Los Altos
Moffett
Federal Airfield
Alviso
Ladera
Woodside
Portola
Valley
San Carlos
Redwood
Shores
Bair Island
North
Fair Oaks
Atherton
West
Menlo Park
Centerville
Coyote Creek
Shoreline
Slough
Guadalupe
Slough
Alameda Creek
Ravenswood
Slough
Redwood
Creek
Westpoint
Slough
Steinberger
Slough
Belmont
Slough
Gann/Dry
Creek Pioneer
Regional Parks
California's
Great America
North
San Jose

Restaurant Pagers

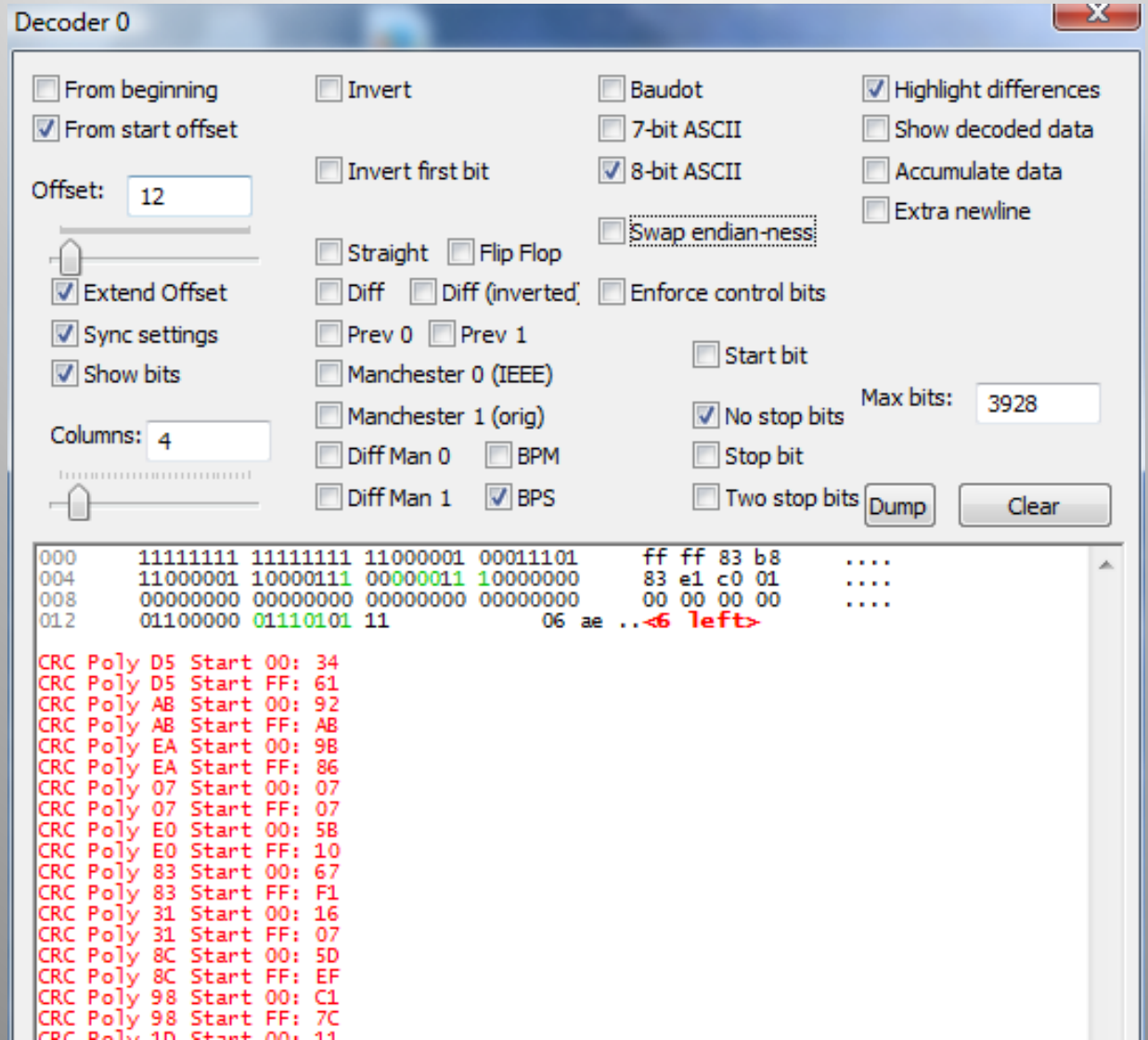
Another Kind of Pager


-1000
-900
-800
-700
-600
-500
-400
-300
-200
-100
0
100
200
300
400
500
600
700
800
900
kHz
Page Waterfall
ns
0
-20
-40
-60
-80
-100
-120
dB
796875 Hz
-4.38 dB

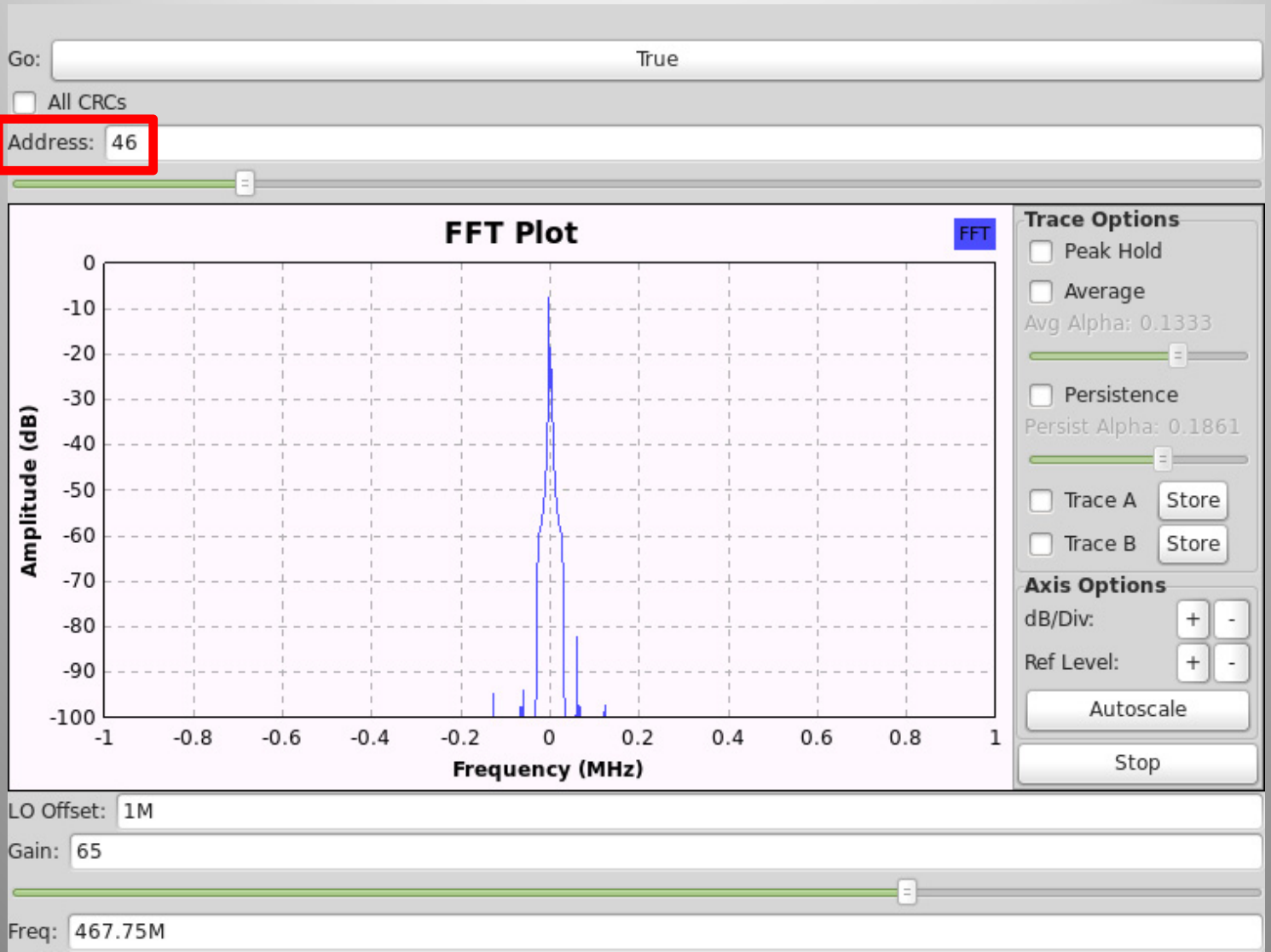
Line Encoding



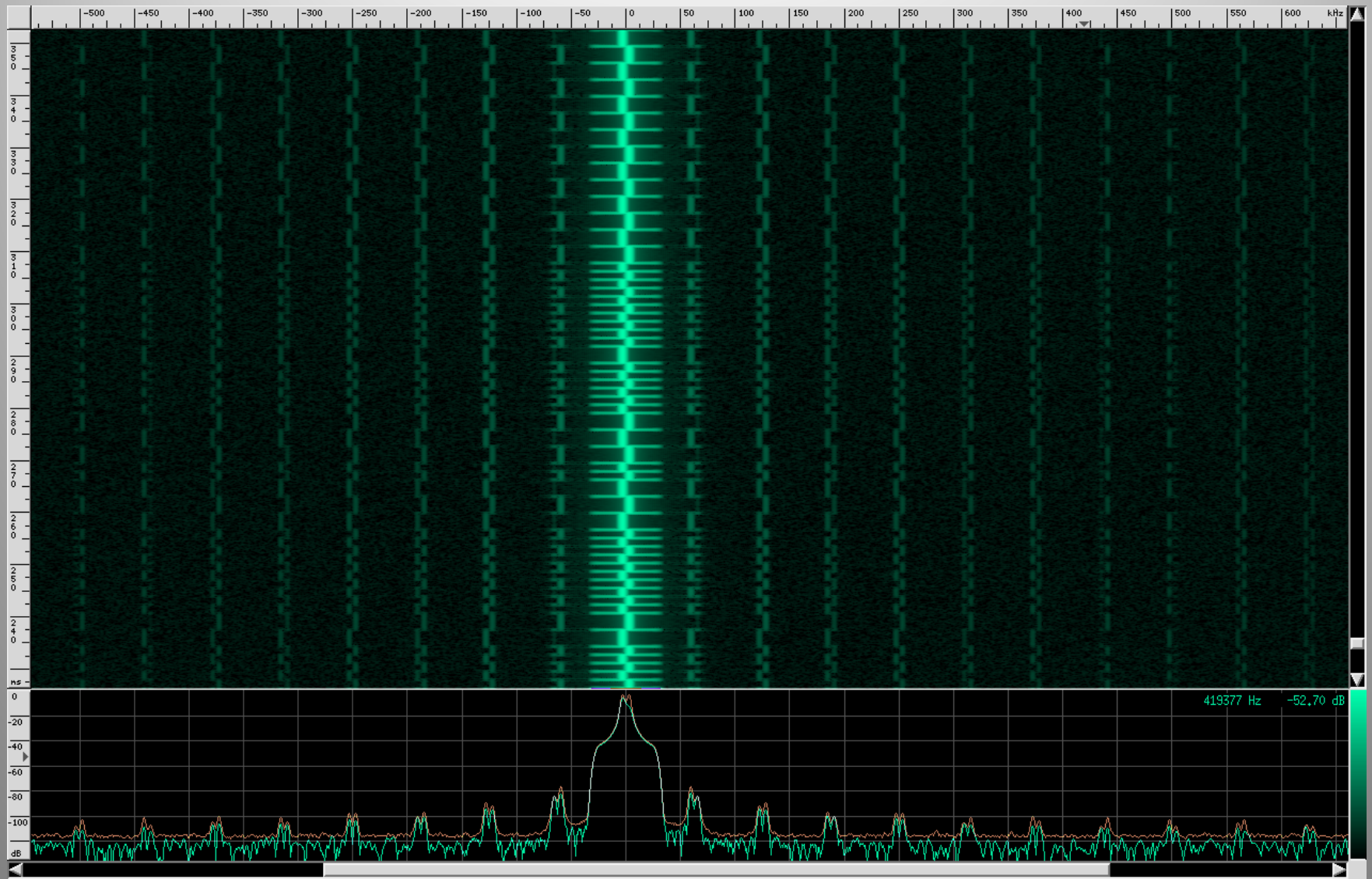
Manchester Encoding

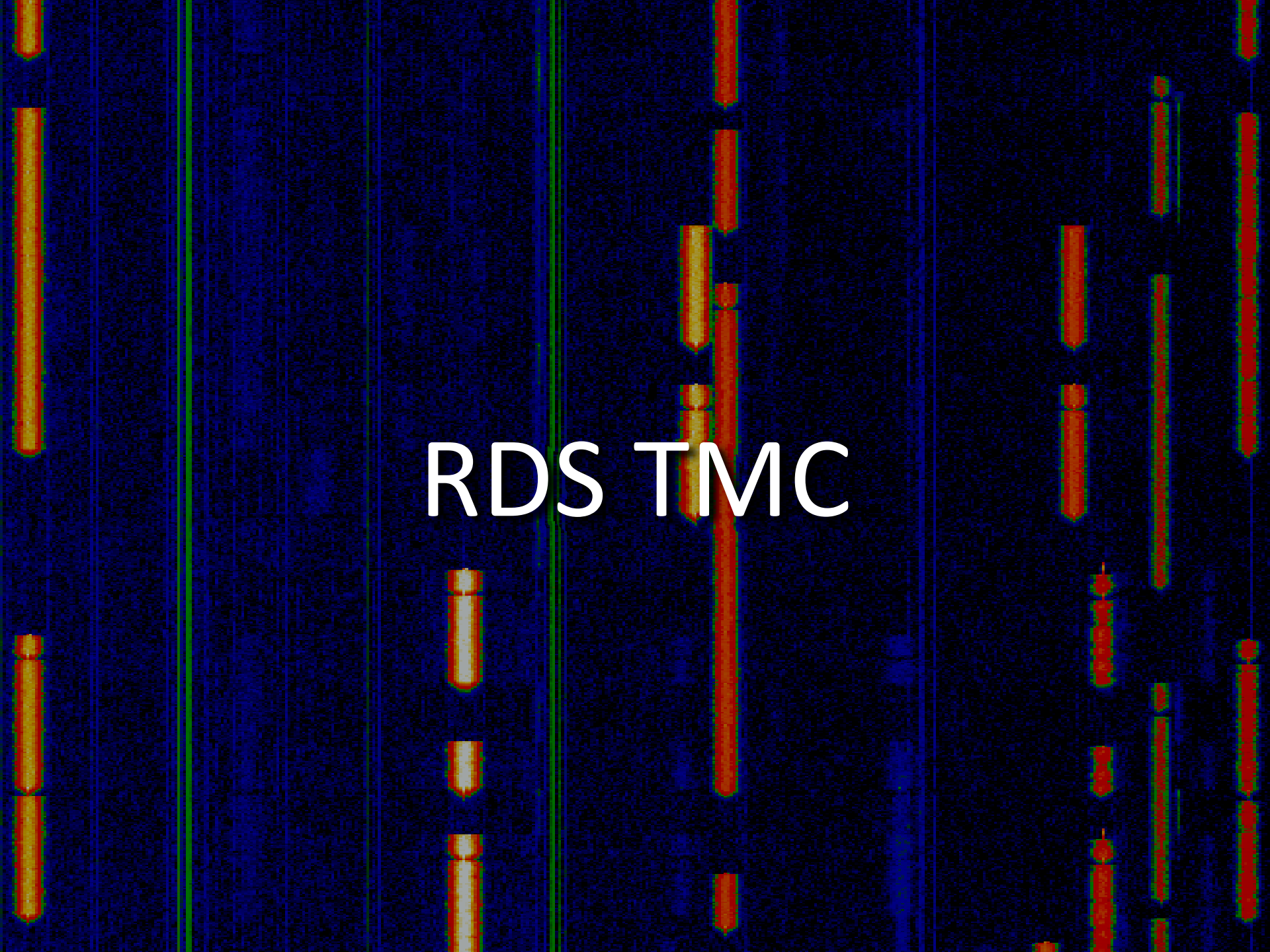


Modulator

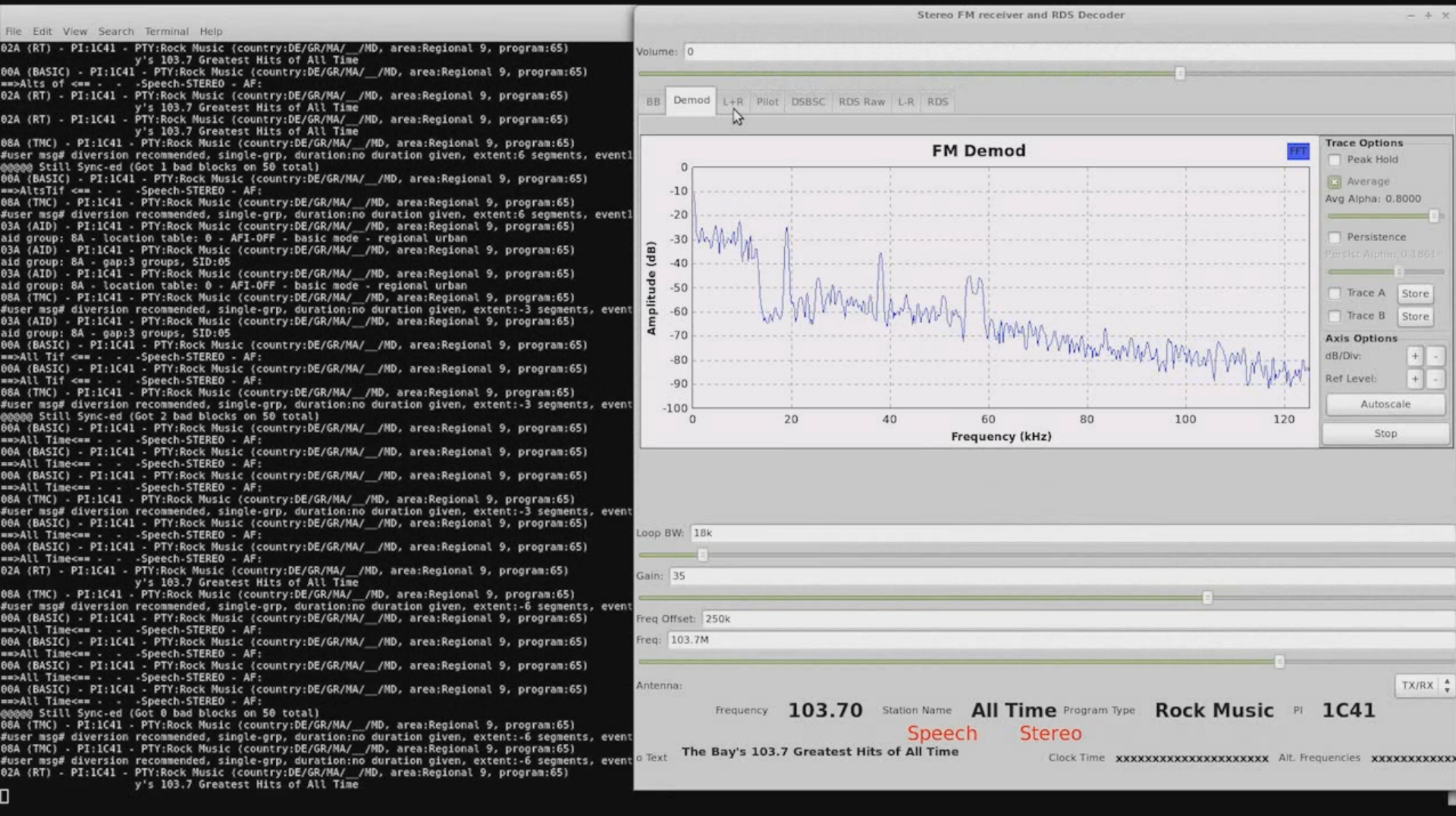

Go:
True
All CRCs
Address: 46
FFT Plot
FFT
Amplitude (dB)
0
-10
-20
-30
-40
-50
-60
-70
-80
-90
-100
-1
-0.8
-0.6
-0.4
-0.2
0
0.2
0.4
0.6
0.8
1
Frequency (MHz)
Trace Options
Peak Hold
Average
Avg Alpha: 0.1333
Persistence
Persist Alpha: 0.1861
Trace A
Store
Trace B
Store
Axis Options
dB/Div:
+
-
Ref Level:
+
-
Autoscale
Stop
LO Offset: 1M
Gain: 65
Freq: 467.75M

Modulator Output




RDS TMC

Traffic Message Channel



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

Security Analysis

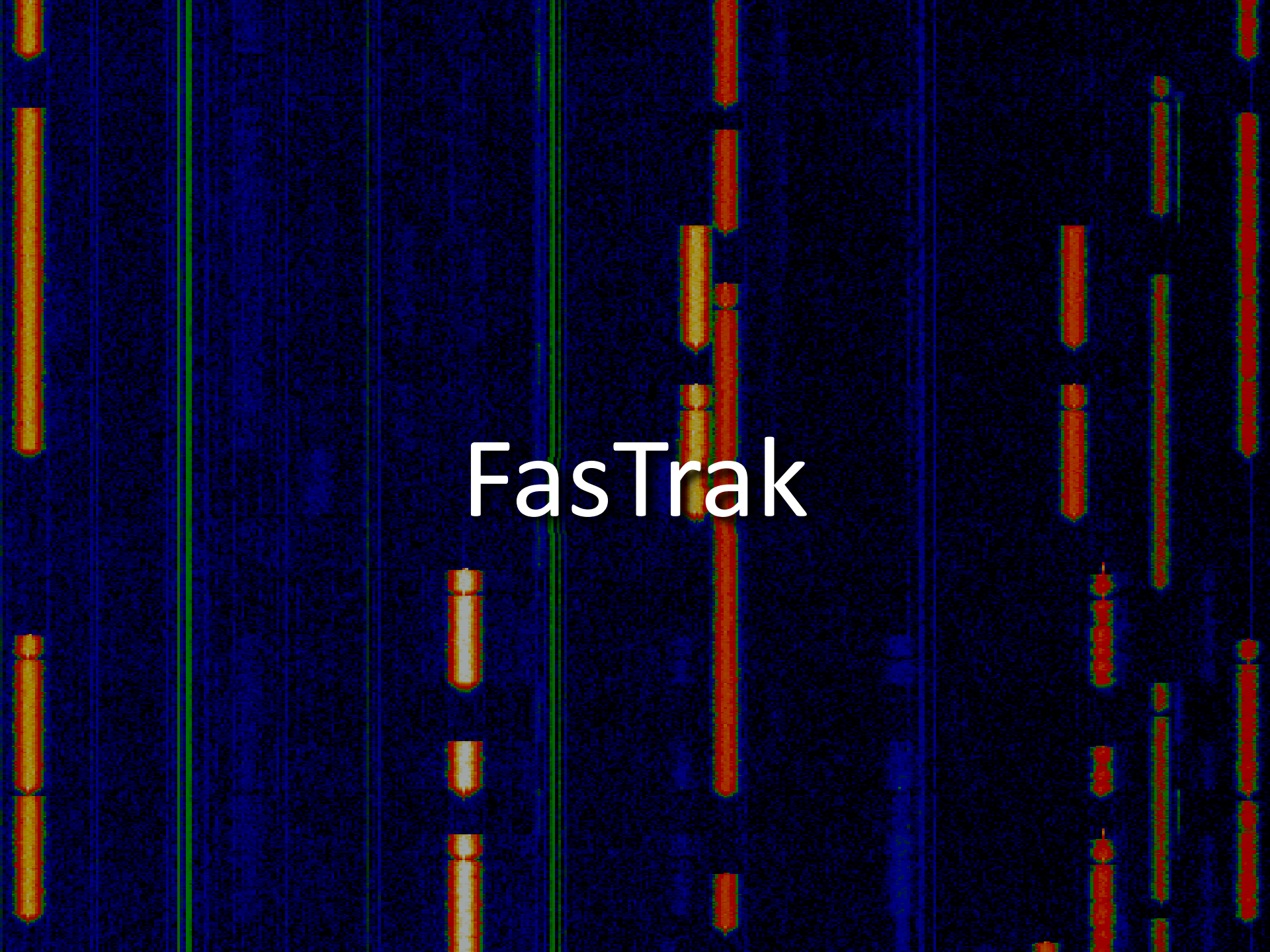
- 16-bit is **very** short
- Known location codes are broadcast on a daily basis
  - Unknown but re-used plaintext
- ‘Singular’ events can be correlated from a trusted source
  - Known plaintext

Trusted Source

Brute Force Search

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


FasTrak

511
Click. Call. Connect.

FasTrak

My Account Contact Us

FasTrak®

- About FasTrak
- FAQ
- How to Use I-15 Express Lanes
- South Bay Expressway
- Customer Service Centers

Get FasTrak

San Diego Toll Roads

News and Events

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

My FasTrak Account

I-15 Express Lanes

South Bay Expressway

Commute

DATA (D:)

2:04 AM

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

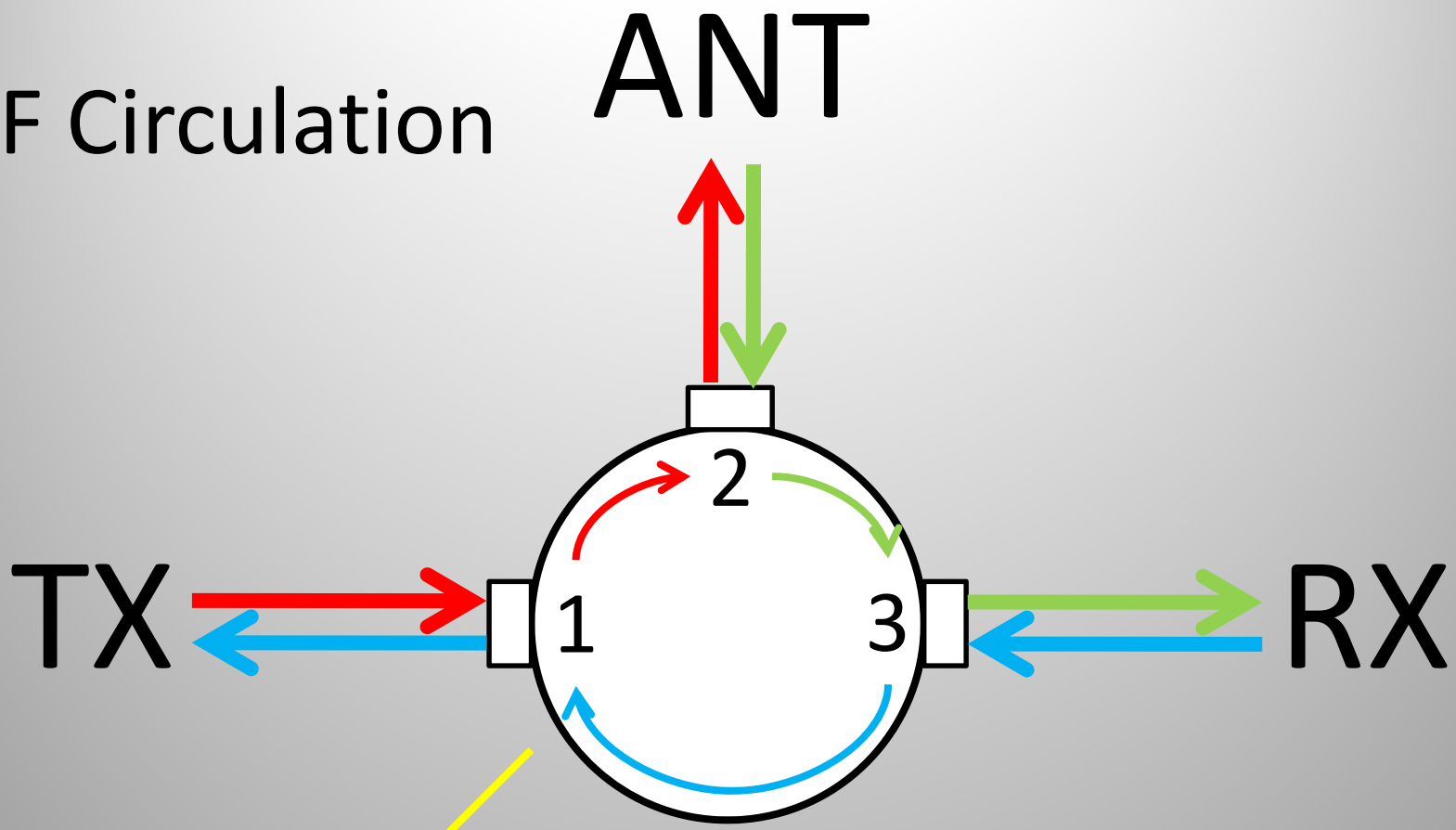
FasTrak

- 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

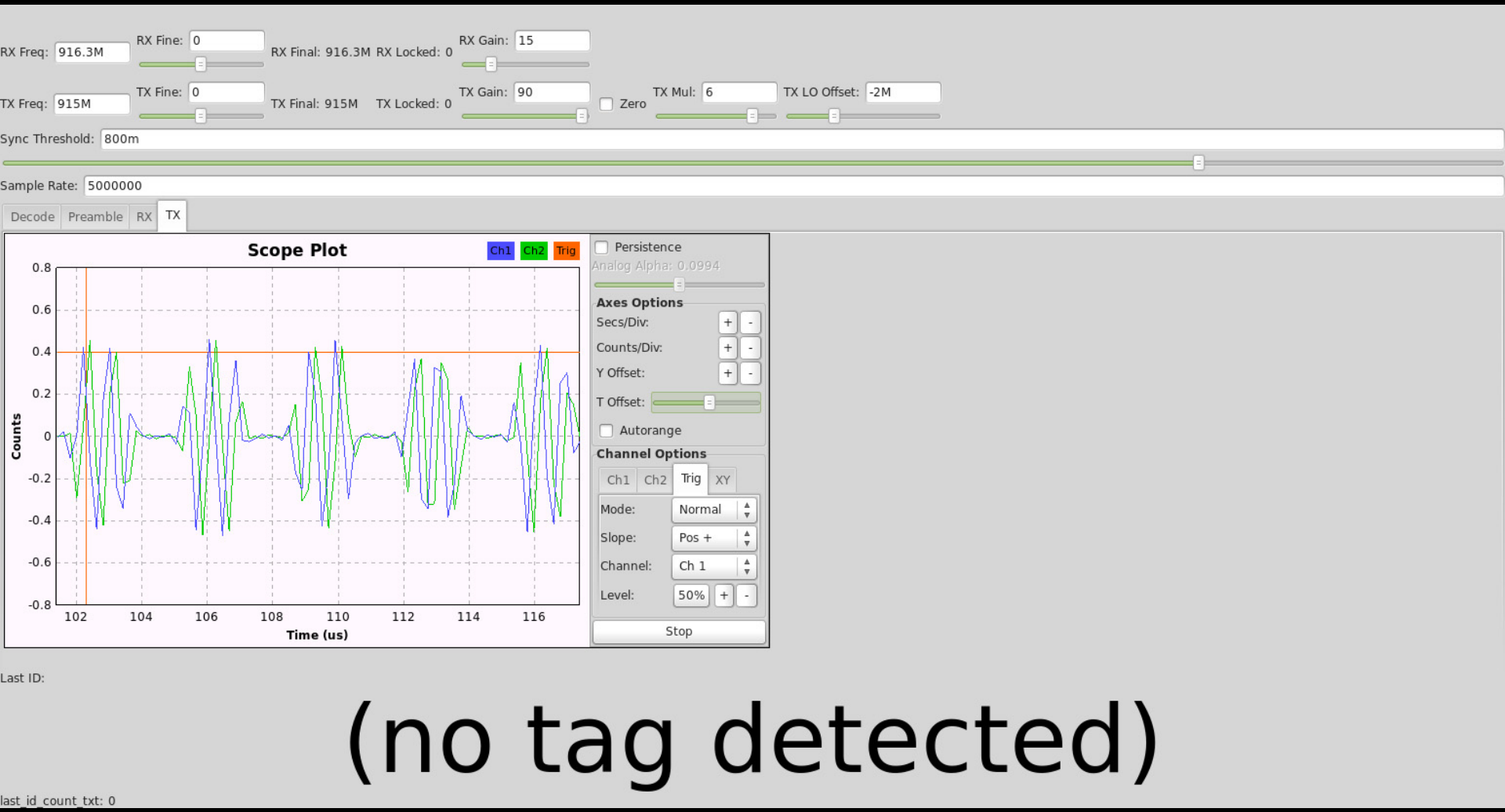

LINCOLN
19TH AVE
A/C
MAX A/C
RES
CANCEL
SET
LO 0916.000.000
Tune 0916.306.605


Thank You for
NOT SMOKING

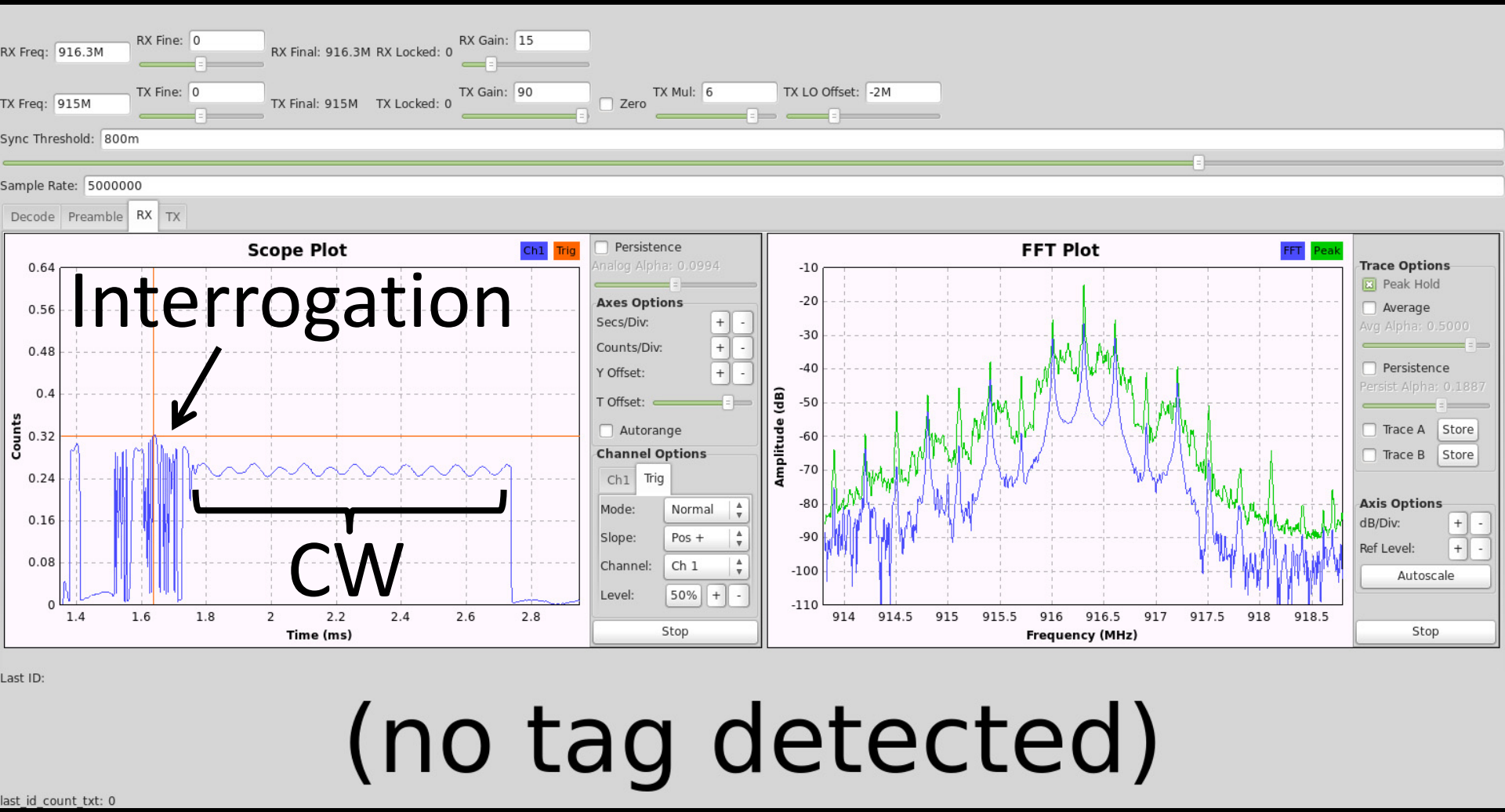
RF Circulation



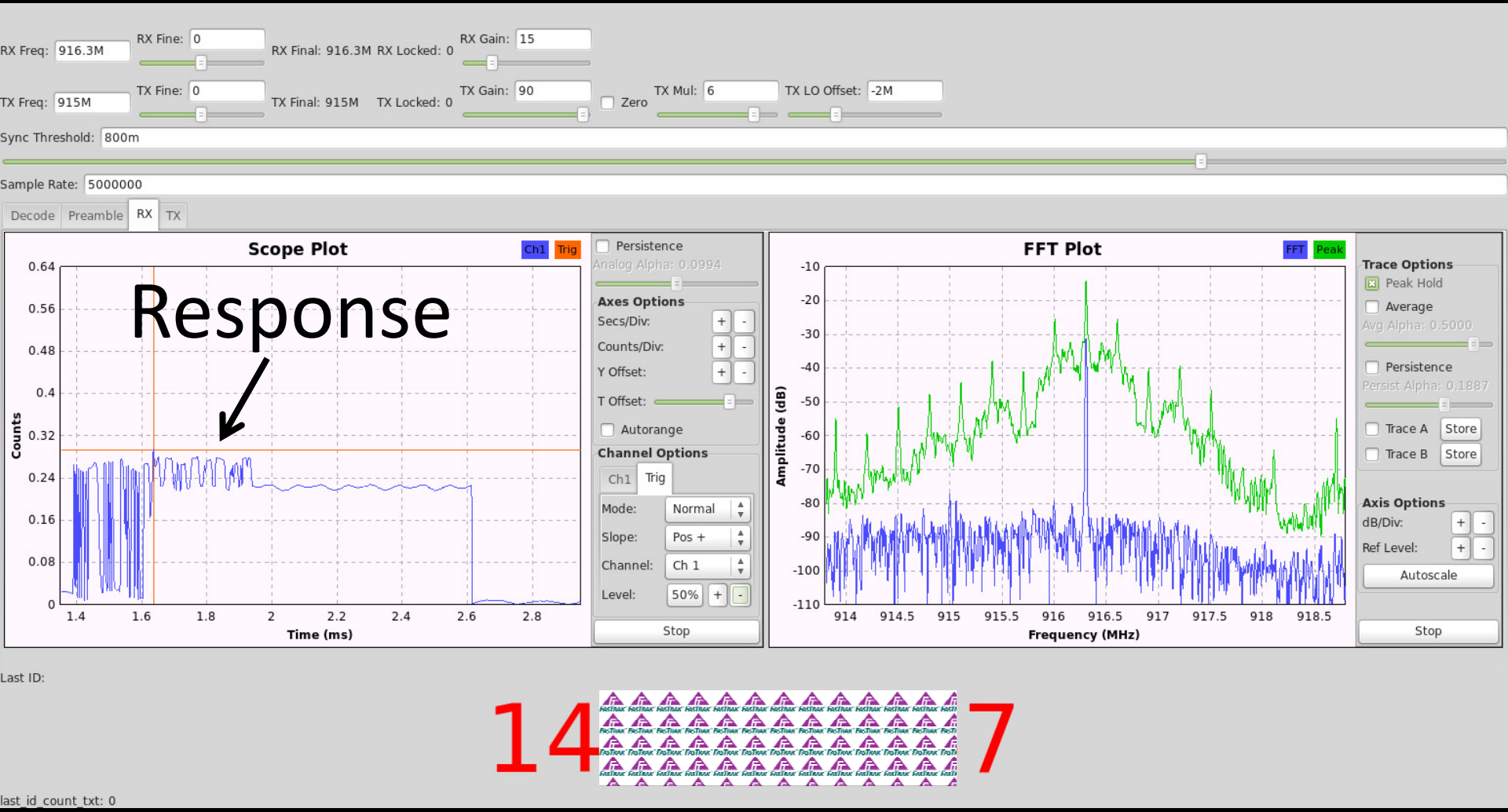
Interrogation Signal



Received Signal



Received Signal



Title 21 Specification

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.

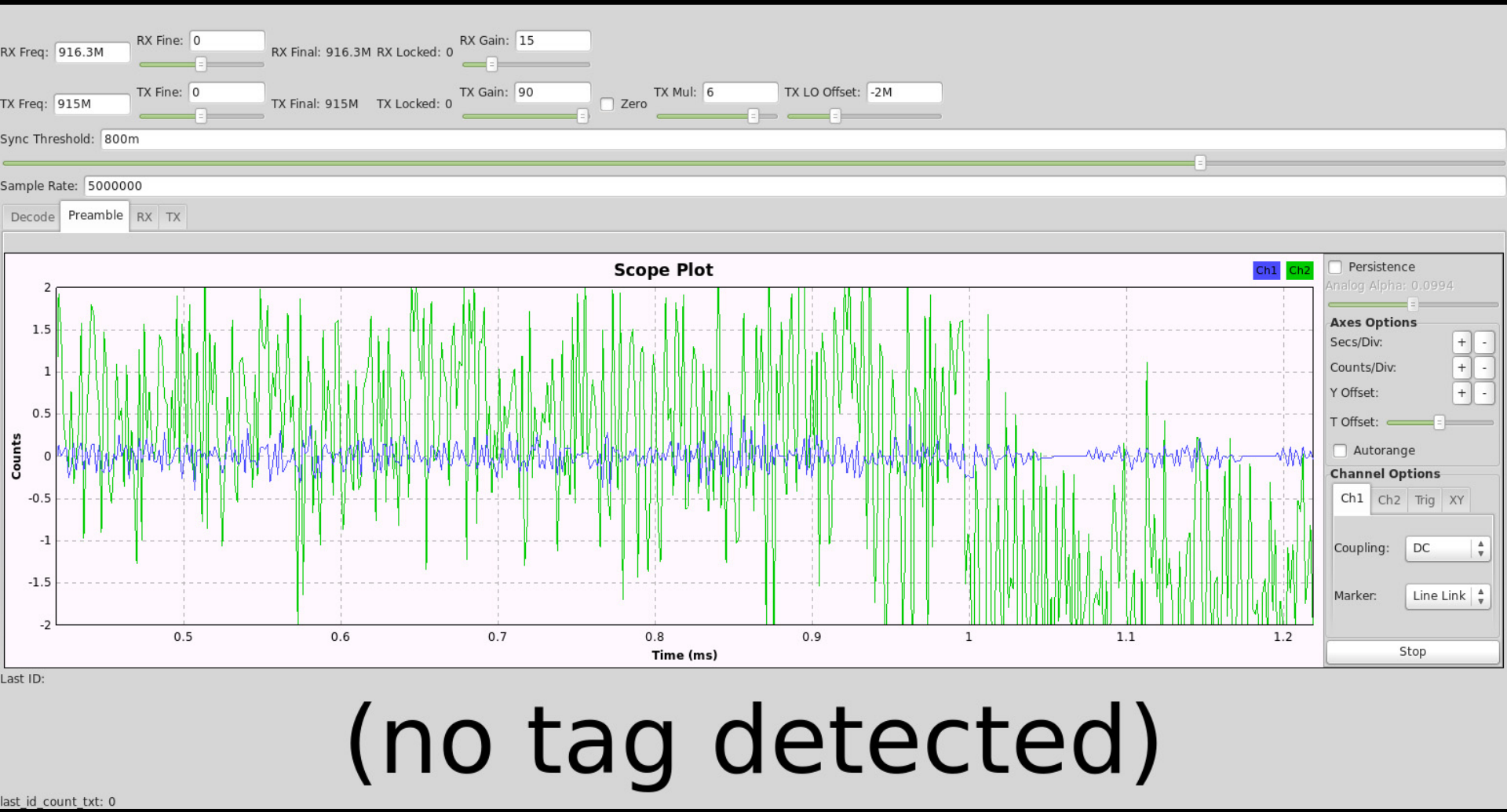
e. Transponder Data Message Formats for AVI Toll Collection.
There may be numerous transponder-to-reader data message formats. The format is determined by the transaction record type code sent by the transponder. The following is the reader-to-transponder message format presently specified for AVI electronic 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	
	76	
	Total:	

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.

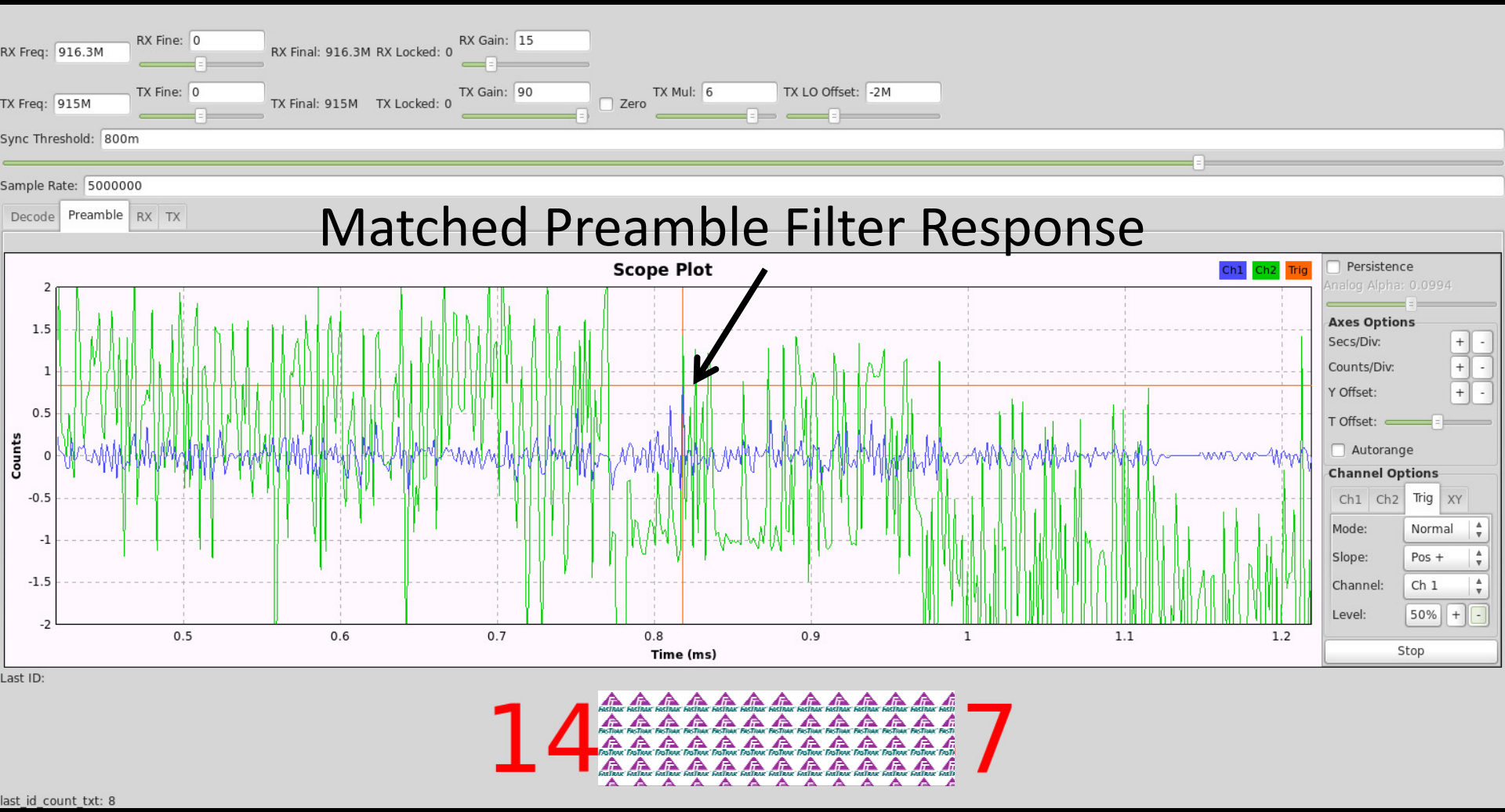
Preamble Detection



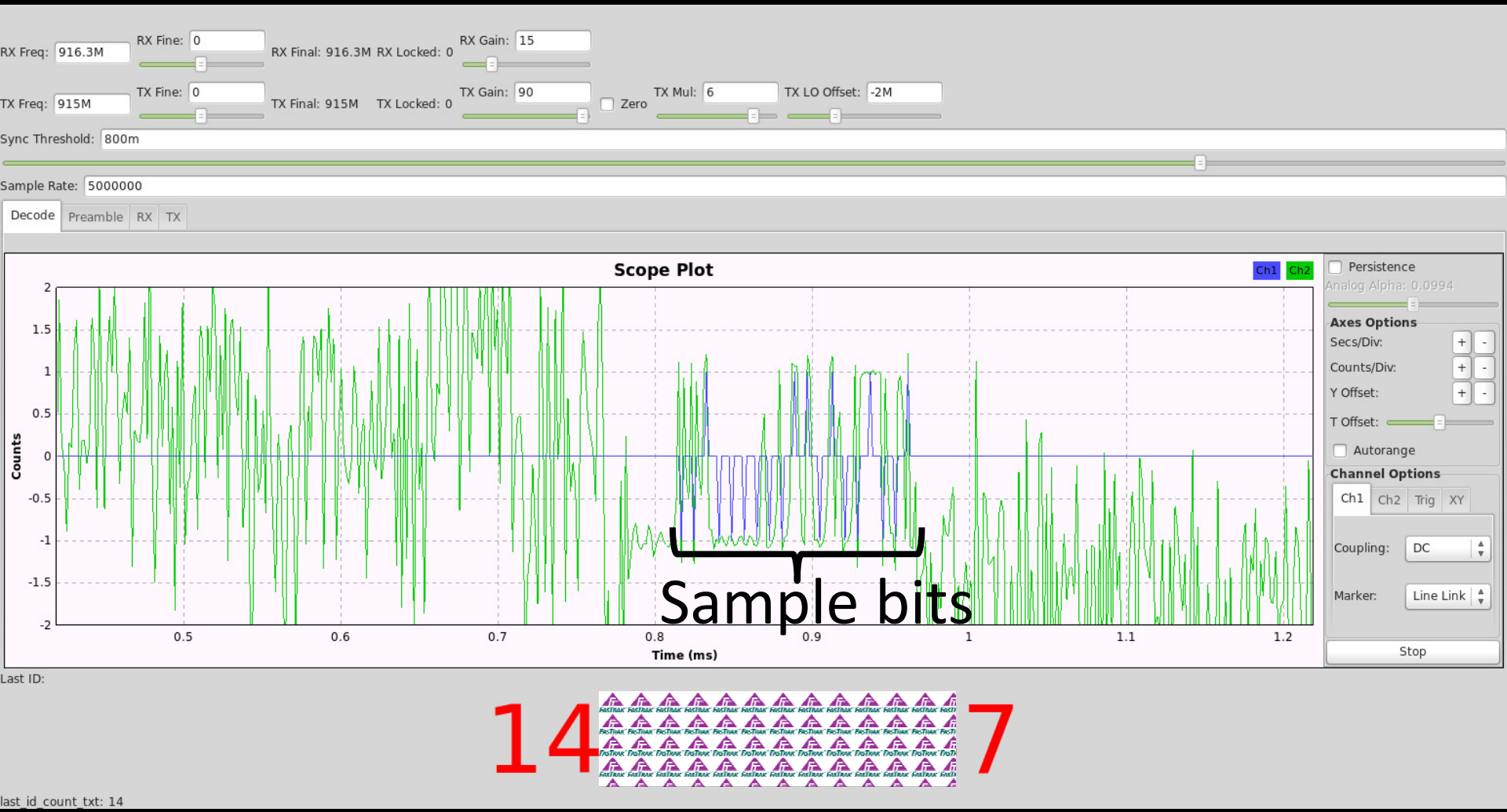
(no tag detected)

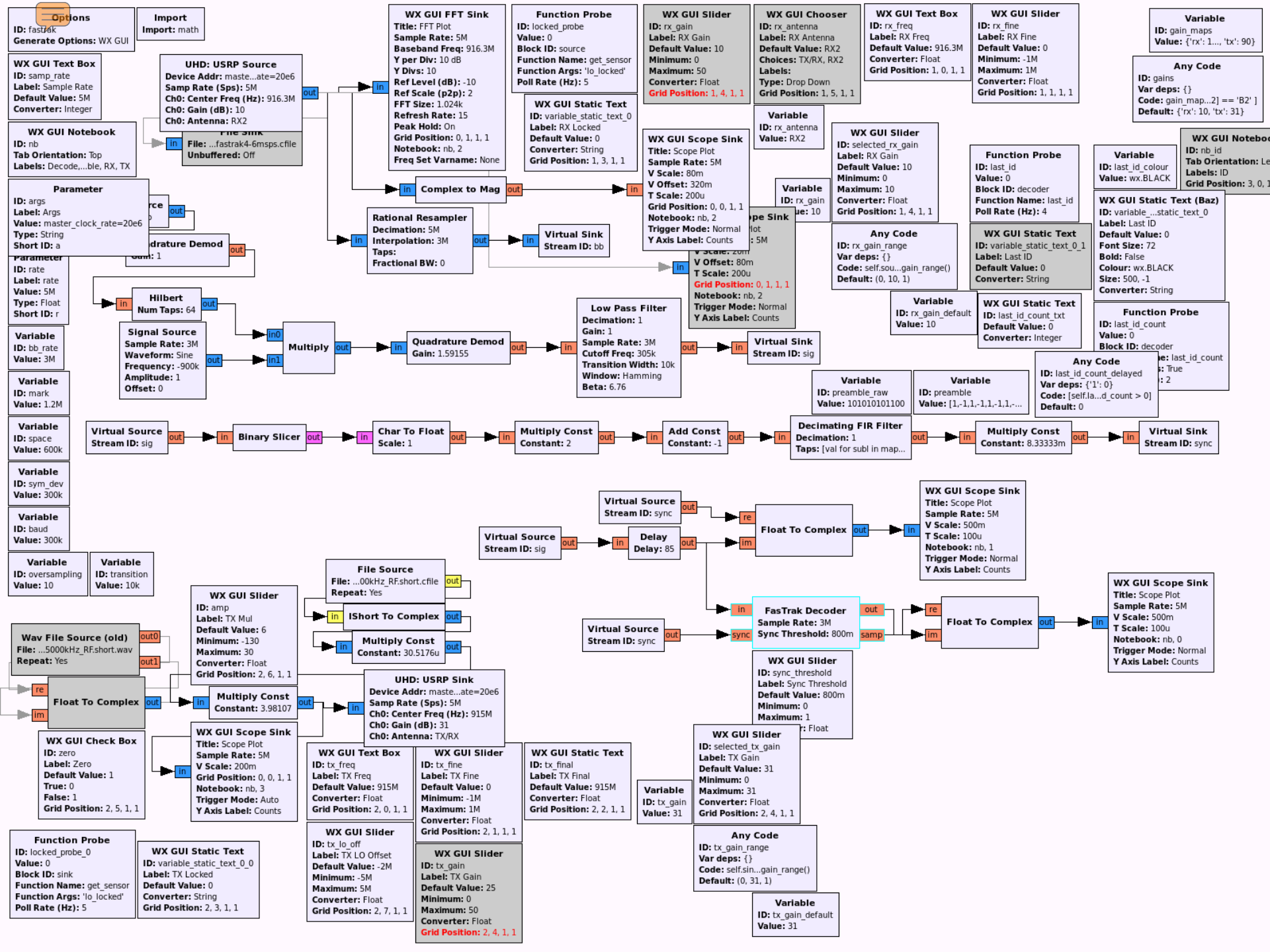
last_id_count_txt: 0

Preamble Detection

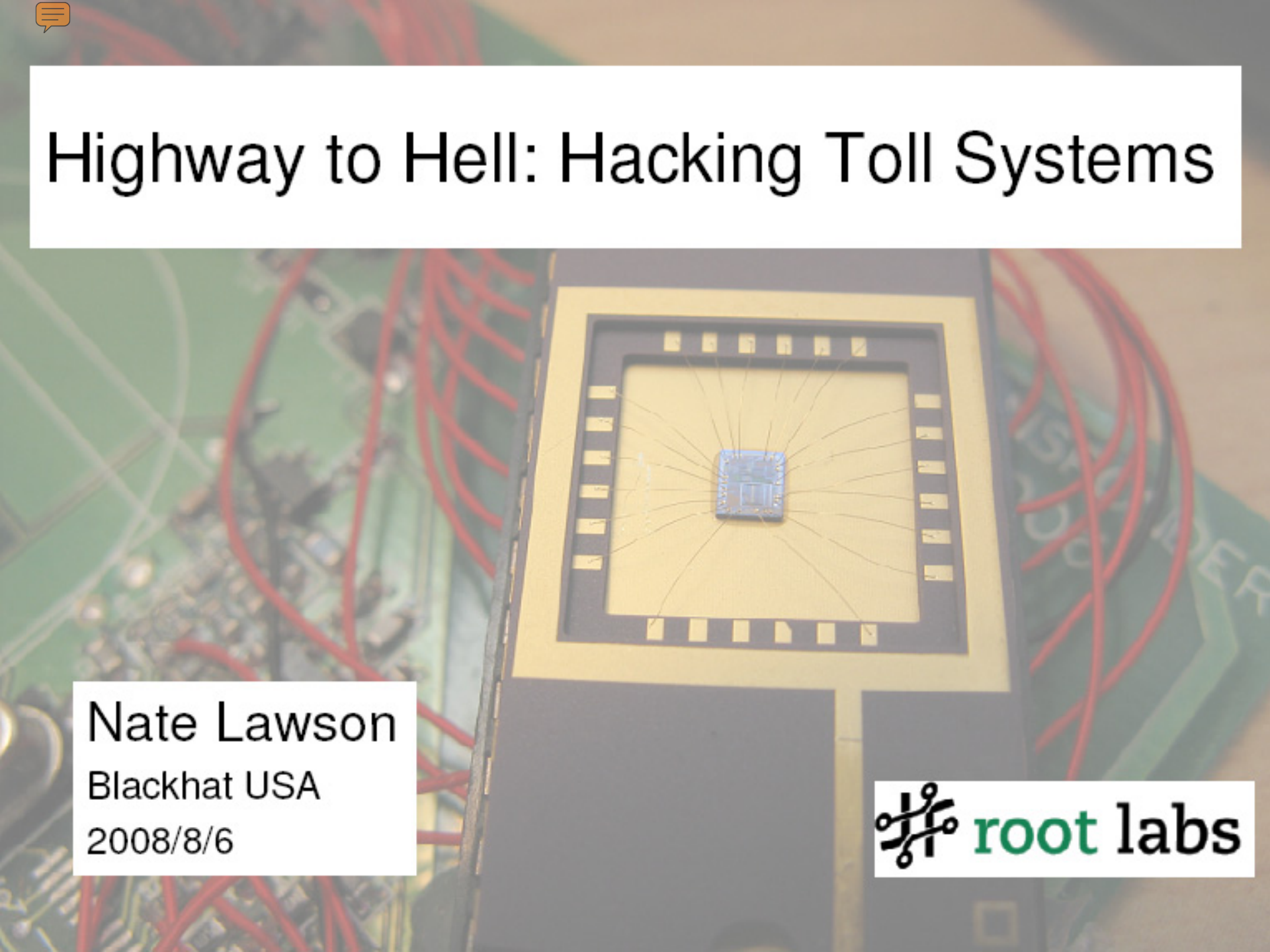


Slicer Time!


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
Decode
Preamble
RX
TX
Scope Plot
Ch1
Ch2
Counts
Time (ms)
Sample bits
Persistence
Analog Alpha: 0.0994
Axes Options
Secs/Div:
Counts/Div:
Y Offset:
T Offset:
Autorange
Channel Options
Ch1
Ch2
Trig
XY
Coupling:
DC
Marker:
Line Link
Stop
Last ID:
14
7
last_id_count_txt: 14


Options
ID: fastrak
Generate Options: WX GUI
Import
Import: math
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
Function Probe
ID: locked_probe
Value: 0
Block ID: source
Function Name: get_sensor
Function Args: 'lo_locked'
Poll Rate (Hz): 5
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
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}
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
Any Code
ID: gains
Var deps: {}
Code: gain_map...2] == 'B2']
Default: {'rx': 10, 'tx': 31}
WX GUI Notebook
ID: nb
Tab Orientation: Top
Labels: Decode,...ble, RX, TX
File Sink
File: ...fastrak4-6msps.cfile
Unbuffered: Off
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 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
Variable
ID: rx_antenna
Value: RX2
Variable
ID: rx_gain
Value: 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
Function Probe
ID: last_id
Value: 0
Block ID: decoder
Function Name: last_id
Poll Rate (Hz): 4
Variable
ID: last_id_colour
Value: wx.BLACK
WX GUI Notebo
ID: nb_id
Tab Orientation: Le
Labels: ID
Grid Position: 3, 0, 1
Parameter
ID: args
Label: Args
Value: master_clock_rate=20e6
Type: String
Short ID: a
Complex to Mag
Rational Resampler
Decimation: 5M
Interpolation: 3M
Taps:
Fractional BW: 0
Virtual Sink
Stream ID: bb
Any Code
ID: rx_gain_range
Var deps: {}
Code: self.sou...gain_range()
Default: (0, 10, 1)
WX GUI Static Text
ID: variable_static_text_0_1
Label: Last ID
Default Value: 0
Font Size: 72
Bold: False
Colour: wx.BLACK
Size: 500, -1
Converter: String
WX GUI Static Text (Baz)
ID: variable_...static_text_0
Label: Last ID
Default Value: 0
Converter: String
Variable
ID: rx_gain_default
Value: 10
WX GUI Static Text
ID: last_id_count_txt
Default Value: 0
Converter: Integer
Function Probe
ID: last_id_count
Value: 0
Block ID: decoder
Parameter
ID: rate
Label: rate
Value: 5M
Type: Float
Short ID: r
Hilbert
Num Taps: 64
Signal Source
Sample Rate: 3M
Waveform: Sine
Frequency: -900k
Amplitude: 1
Offset: 0
Multiply
Quadrature Demod
Gain: 1.59155
Low Pass Filter
Decimation: 1
Gain: 1
Sample Rate: 3M
Cutoff Freq: 305k
Transition Width: 10k
Window: Hamming
Beta: 6.76
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: preamble_raw
Value: 101010101100
Variable
ID: preamble
Value: [1,-1,1,-1,1,-1,1,-...
Any Code
ID: last_id_count_delayed
Var deps: {'1': 0}
Code: [self.la...d_count > 0]
Default: 0
Virtual Source
Stream ID: sig
Binary Slicer
Char To Float
Scale: 1
Multiply Const
Constant: 2
Add Const
Constant: -1
Decimating FIR Filter
Decimation: 1
Taps: [val for subl in map...
Multiply Const
Constant: 8.33333m
Virtual Sink
Stream ID: sync
Variable
ID: oversampling
Value: 10
Variable
ID: transition
Value: 10k
Virtual Source
Stream ID: sync
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
WX GUI Slider
ID: amp
Label: TX Mul
Default Value: 6
Minimum: -130
Maximum: 30
Converter: Float
Grid Position: 2, 6, 1, 1
Wav File Source (old)
File: ...5000kHz_RF.short.wav
Repeat: Yes
Float To Complex
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
FasTrak Decoder
Sample Rate: 3M
Sync Threshold: 800m
WX GUI Slider
ID: sync_threshold
Label: Sync Threshold
Default Value: 800m
Minimum: 0
Maximum: 1
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
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
Variable
ID: tx_gain
Value: 31
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

Highway to Hell: Hacking Toll Systems

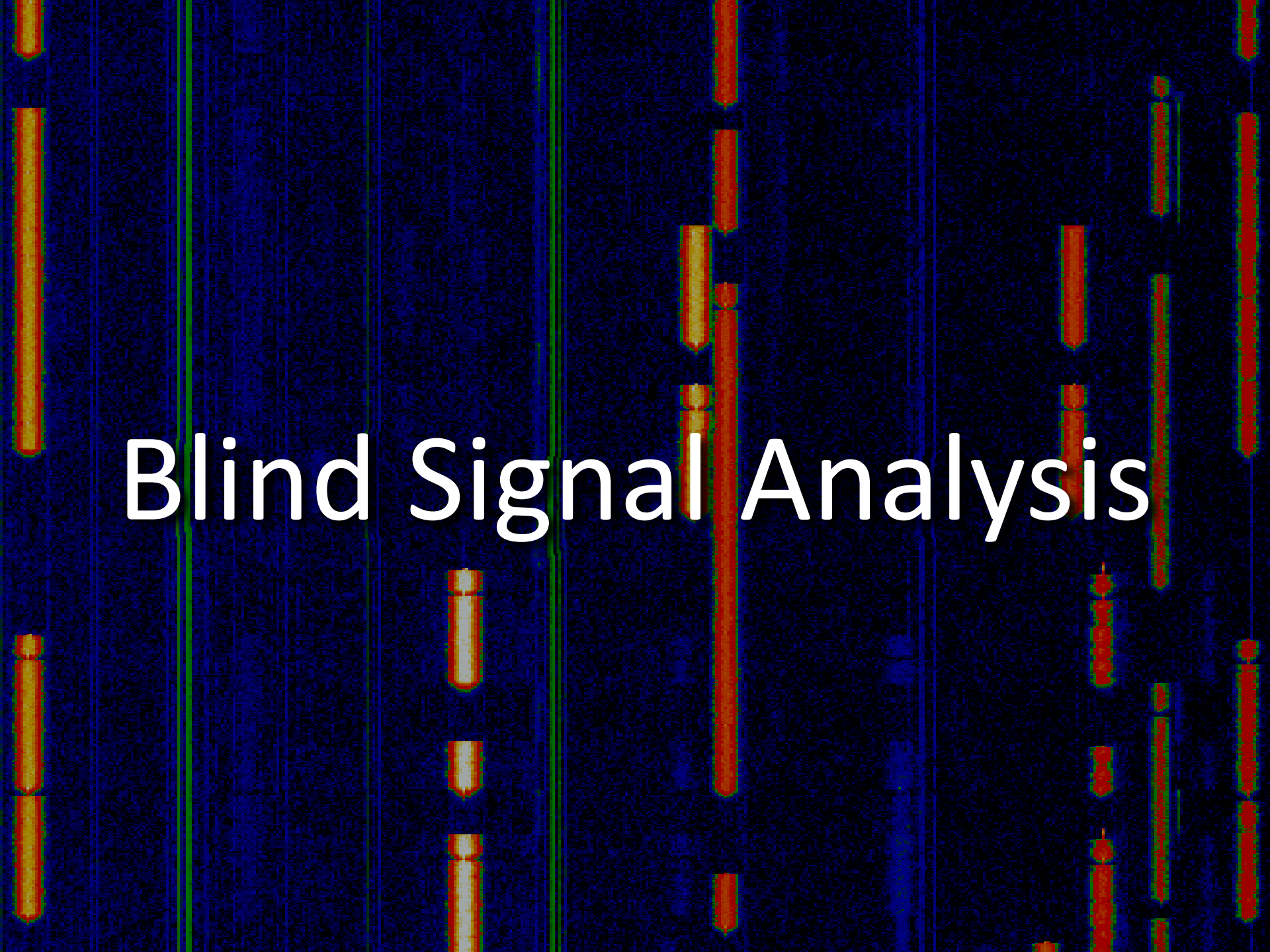


Nate Lawson

Blackhat USA

2008/8/6

root labs


Blind Signal Analysis

Recap

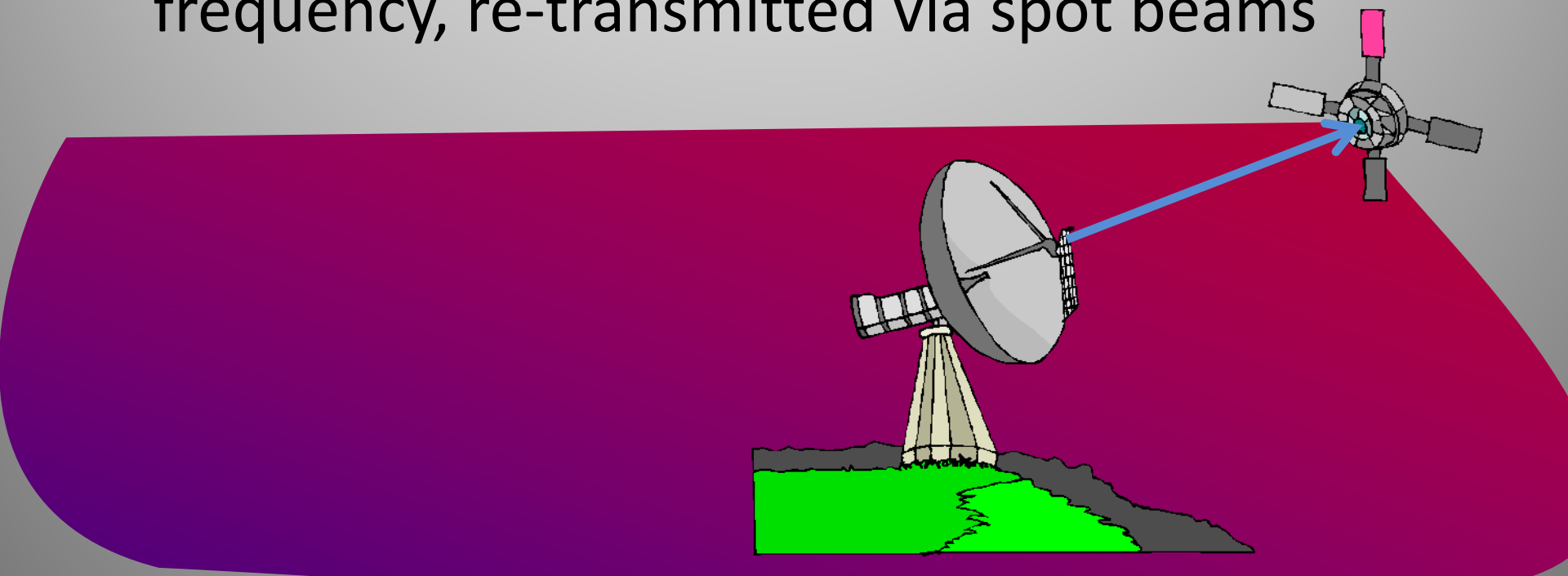
- Lots of different types of satellites
- Variables:
  - Purpose: comms, weather, MIL, amateur
  - Payload: transponders, cameras/sensors
  - Orbit: **L**ow **E**arth **O**rbit, geostationary (geosync)
  - Frequencies: uplink, downlink, beacon, command
- Two categories:
  - **Intelligent**: communication with on-board systems
  - **Dumb**: relay information with linear transponders

Wide-area re-broadcast

- RF megaphone (e.g. satellite TV)
- Single dish sends beam on uplink to satellite

Wide-area re-broadcast

- RF megaphone (e.g. satellite TV)
- Single dish sends beam on uplink to satellite
- Linear transponder shifts raw RF to downlink frequency, re-transmitted via spot beams



Wide-area re-broadcast

- RF megaphone (e.g. satellite TV)
- Single dish sends beam on uplink to satellite
- Linear transponder shifts raw RF to downlink frequency, re-transmitted via spot beams
- Cover any entire country

Wide-area re-broadcast

- RF megaphone (e.g. satellite TV)
- Single dish sends beam on uplink to satellite
- Linear transponder shifts raw RF to downlink frequency, re-transmitted via spot beams
- Cover any entire country

- Linear transponders are **dumb**: re-broadcast anything onto coverage area

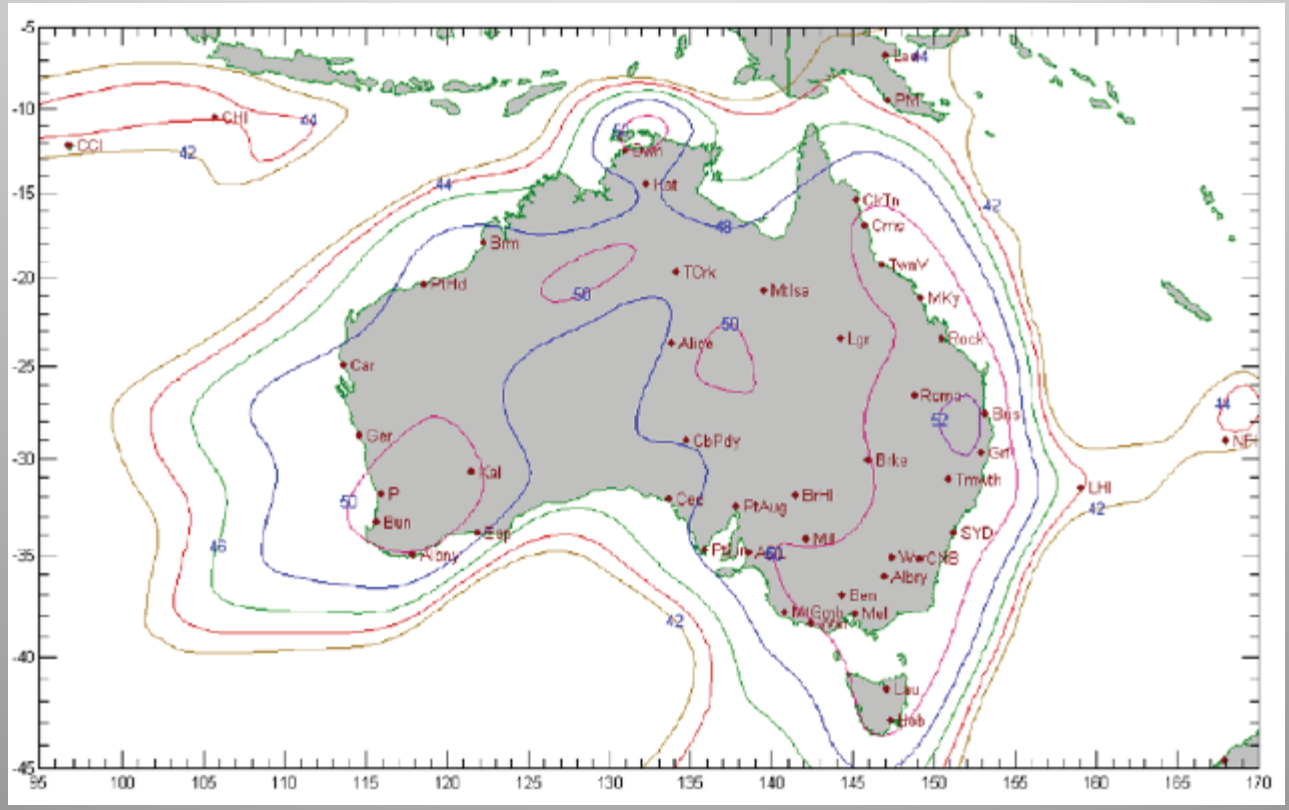
TT&C and UPC

- **T**elemetry, **T**racking and **C**ommand
- Need to be able to send commands to satellite
  - Change payload configuration
    - Multiplexing
    - Switch between redundant systems
    - Orbit
- Check on health of satellite/payload
  - Beacon + telemetry
- Measure affect of weather (combat rain fade)
  - **U**plink **P**ower **C**ontrol
  - Turn up transmitter power (keep at min. = save $$$)

Optus D1

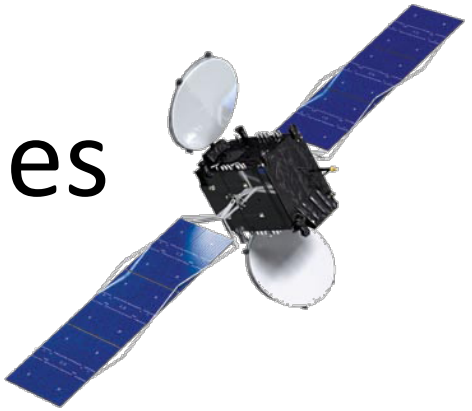
- 24 Ku band transponders
  - Multiplexed spot beams service Aus and NZ
  - Uplink: 14.0 - 14.5 GHz
  - Downlink: 12.25 - 12.75 GHz
  - Bandwidth: 54 MHz
- Mainly TV (wideband DVB-S)
  - ABC, SBS, Se7en, Nin9, SkyNZ
- Some other (narrowband) things…

FNA Beam Coverage

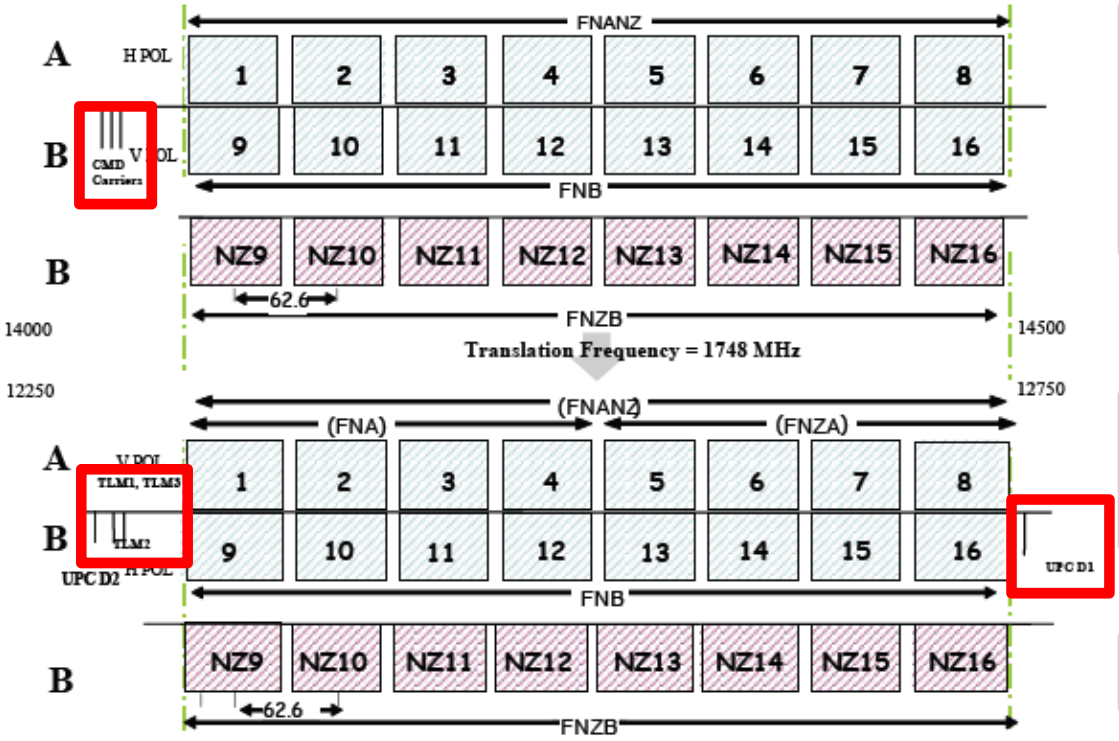


Effective **I**sotropic **R**adiated **P**ower (EIRP)

D1 Channel Frequencies



Uplink



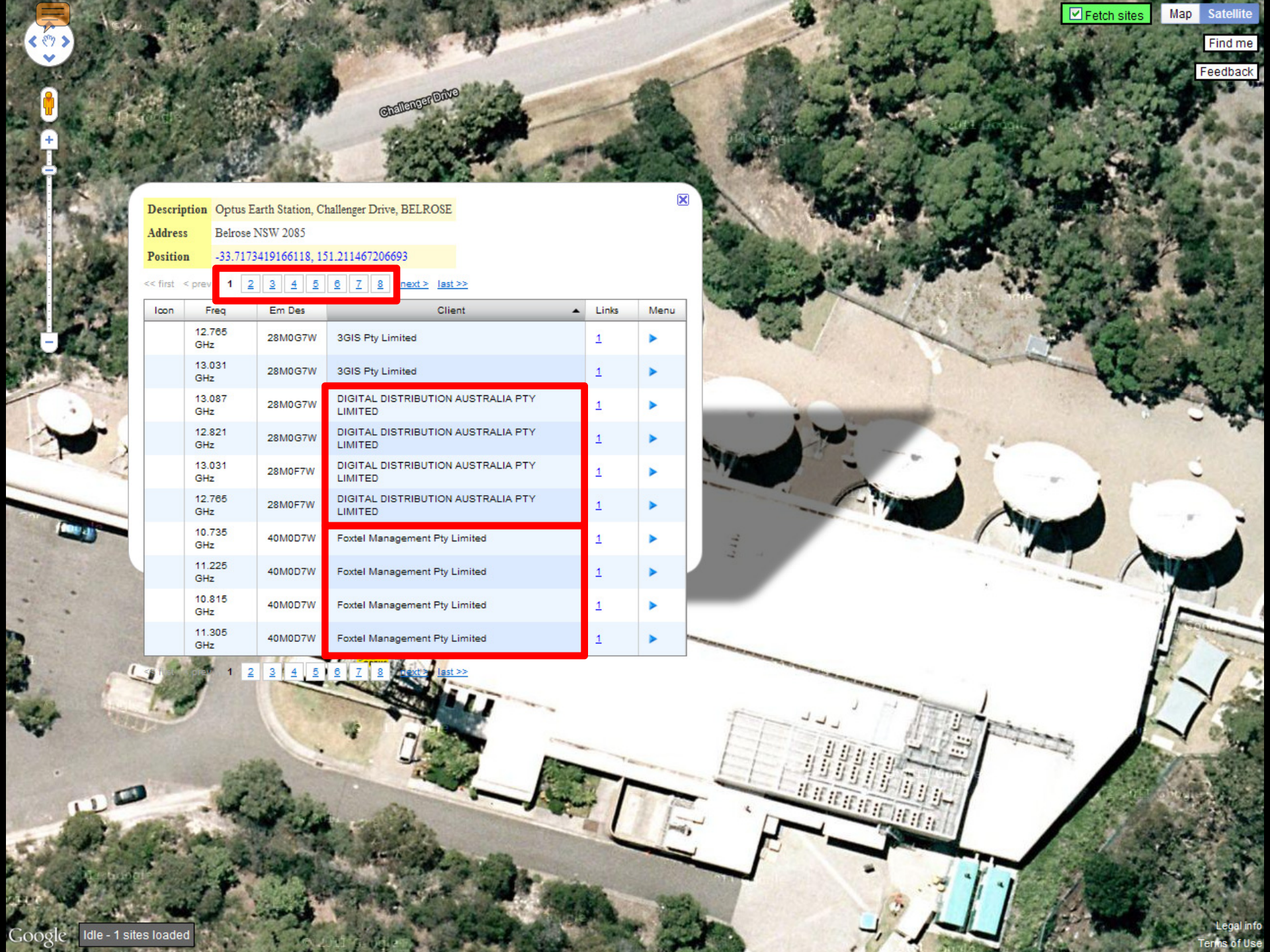
FSS Australia Centre Frequencies (MHz)		
Channel	Uplink	Downlink
1	14029.90	12281.90
2	14092.50	12344.50
3	14155.10	12407.10
4	14217.70	12469.70
5	14280.30	12532.30
6	14342.90	12594.90
7	14405.50	12657.50
8	14468.10	12720.10
9	14029.90	12281.90
10	14092.50	12344.50
11	14155.10	12407.10
12	14217.70	12469.70
13	14280.30	12532.30
14	14342.90	12594.90
15	14405.50	12657.50
16	14468.10	12720.10
TLM1		12243.25
TLM2		12245.25
TLM3		12243.25
UPC		12749.50

FSS NZ Centre Frequencies (MHz)		
Channel	Uplink	Downlink
NZ9	14029.90	12281.90
NZ10	14092.50	12344.50
NZ11	14155.10	12407.10
NZ12	14217.70	12469.70
NZ13	14280.30	12532.30
NZ14	14342.90	12594.90
NZ15	14405.50	12657.50
NZ16	14468.10	12720.10

D1

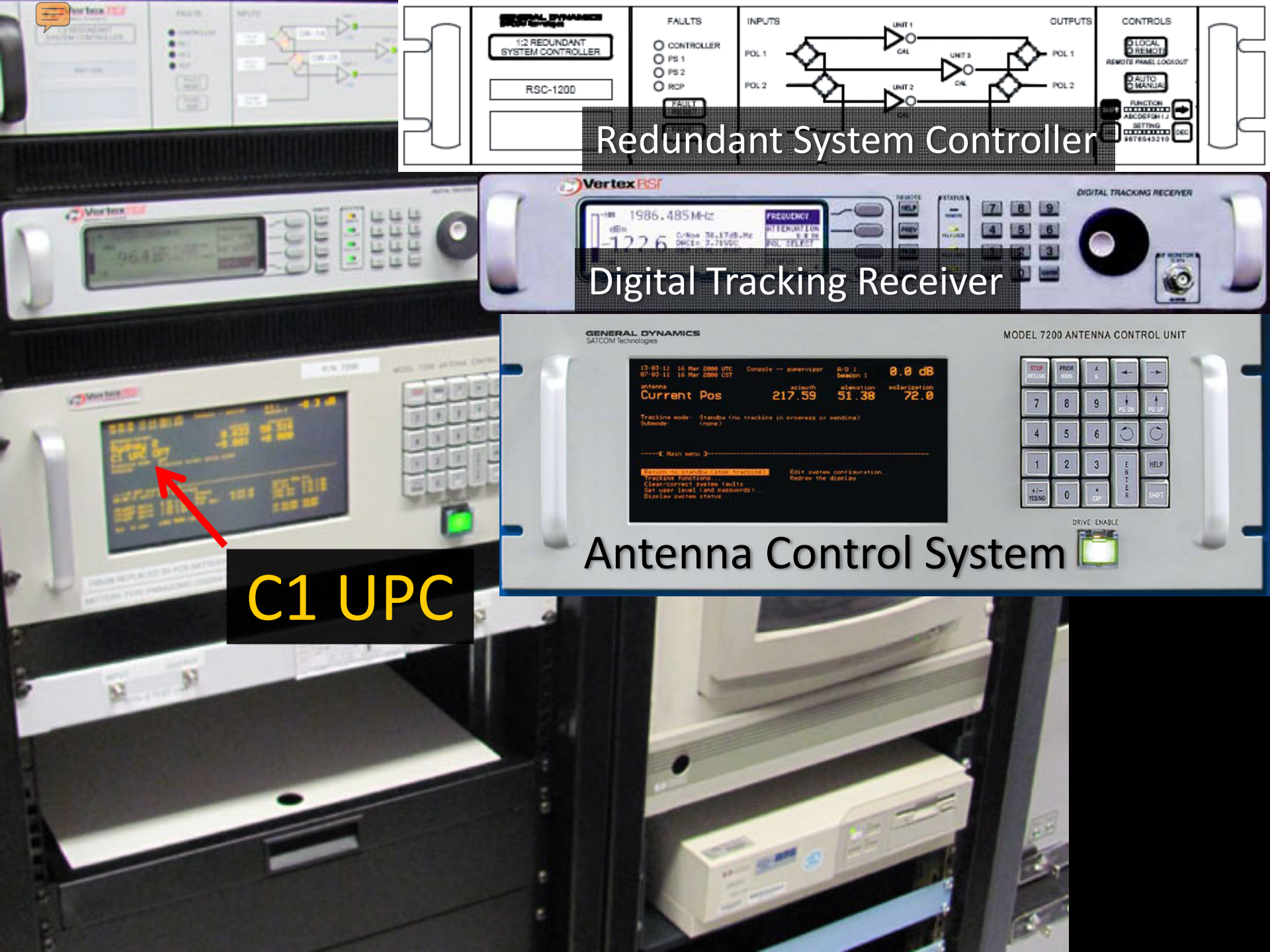
Downlink

Optus Earth Station
Belrose, Sydney


Fetch sites
Map
Satellite
Find me
Feedback
Challenger Drive
Description Optus Earth Station, Challenger Drive, BELROSE
Address Belrose NSW 2085
Position -33.7173419166118, 151.211467206693
<< first < prev 1 2 3 4 5 6 7 8 next > last >>
Icon | Freq | Em Des | Client | Links | Menu
12.765 GHz | 28M0G7W | 3GIS Pty Limited | 1
13.031 GHz | 28M0G7W | 3GIS Pty Limited | 1
13.087 GHz | 28M0G7W | DIGITAL DISTRIBUTION AUSTRALIA PTY LIMITED | 1
12.821 GHz | 28M0G7W | DIGITAL DISTRIBUTION AUSTRALIA PTY LIMITED | 1
13.031 GHz | 28M0F7W | DIGITAL DISTRIBUTION AUSTRALIA PTY LIMITED | 1
12.765 GHz | 28M0F7W | DIGITAL DISTRIBUTION AUSTRALIA PTY LIMITED | 1
10.735 GHz | 40M0D7W | Foxtel Management Pty Limited | 1
11.225 GHz | 40M0D7W | Foxtel Management Pty Limited | 1
10.815 GHz | 40M0D7W | Foxtel Management Pty Limited | 1
11.305 GHz | 40M0D7W | Foxtel Management Pty Limited | 1
1 2 3 4 5 6 7 8 next > last >>
Google
Idle - 1 sites loaded
Legal info
Terms of Use

Spot the satellite modem

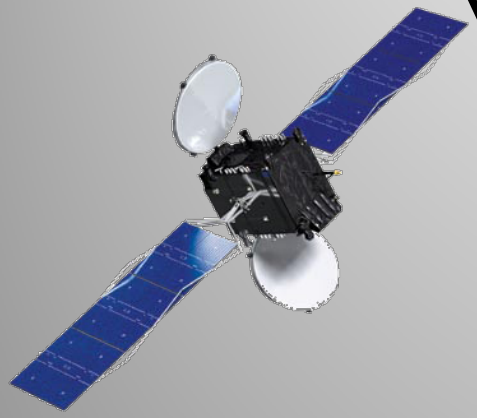
Radyne Comstream Satellite Modem DMD-15

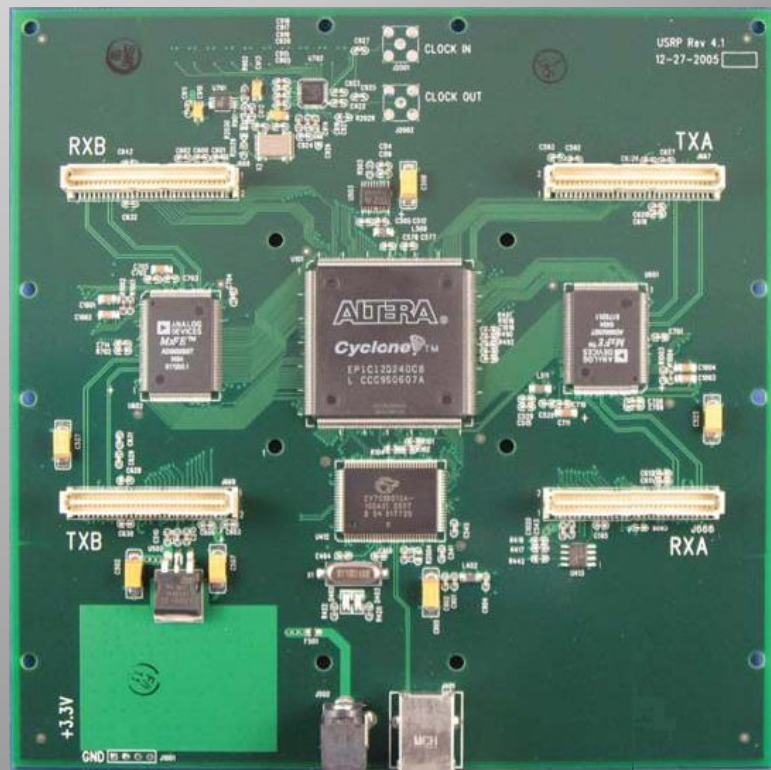

1:2 REDUNDANT SYSTEM CONTROLLER
RSC-1200
FAULTS
CONTROLLER
PS 1
PS 2
RCP
INPUTS
OUTPUTS
POL 1
POL 2
CONTROLS
LOCAL
REMOTE
AUTO
MANUAL
Redundant System Controller
Vertex RSI
DIGITAL TRACKING RECEIVER
1986.485 MHz
FREQUENCY
ATTENUATION
POL SELECT
Digital Tracking Receiver
GENERAL DYNAMICS
SATCOM Technologies
MODEL 7200 ANTENNA CONTROL UNIT
Current Pos
217.59
51.38
72.0
0.0 dB
DRIVE ENABLE
Antenna Control System
C1 UPC

What you need

Dish + LNB + power injector + USRP + GNU Radio

(set-top box with LNB-thru)





Low **N**oise **B**lock down-converter

Subtract 11.3 GHz from downlink frequency: 950 - 1450 MHz

Ku Band High Power TM Transmitters

Applications

- Satellite TC&R subsystems
- Telemetry and ranging transmission and modulation

Main features

- Ku Band
- Compatible with most of bus interfaces (command & telemetry formats)
- Power supplies 22 to 100V
- High power output, 8W EOL, 10W BOL (through SSPA)
- Flight Proven design
- Modulation Index selection
  - By Command
  - Automatic according to modulating tones number

Technologies

- Microwave Integrated Circuit
- Surface Mount Printed Circuit Board
- Thick Film Hybrid

Background

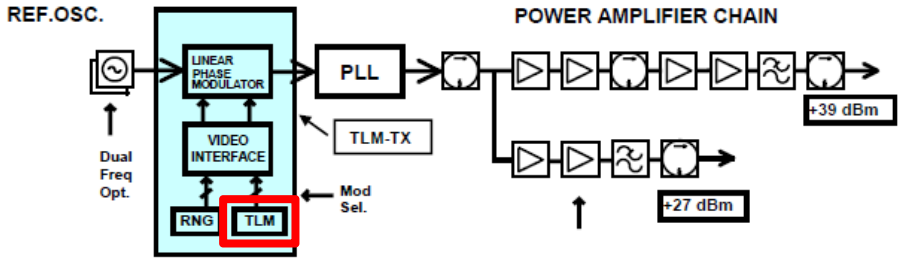
- AMC 14 - AMC 15 - AMC 16
- BSAT 2 A - BSAT 2 B
- BSAT 2 C
- BSAT3A
- ECHOSTAR 10
- ECHOSTAR 7
- GE 2A (NIMIQ2)
- HORIZON 2
- JCSAT 10
- JCSAT 11
- JCSAT 9
- NEWSKIES 6
- NEWSKIES 7
- OPTUS D1
- OPTUS D2
- Panamsat 11
- RAINBOW
- Thor2

Technical Description

- The unit consists of two modules:
  - MPLL module
  - Baseplate module

- The baseplate module houses the DC/DC converter board, which supplies the power voltages to the RF section, and the telemetry interface board, and the Solid State Power Amplifier (SSPA).
- The MPLL module includes all the microwave and RF circuitry to generate and modulate the Ku-band carrier. The modulation inputs interface is implemented on the Telemetry Interface board that is usually tailored on customer's requirements
- The reference crystal oscillator generates a frequency at about 100 MHz, depending on the exact transmitter frequency. The design is based upon a grounded-base configuration with an AT-cut quartz crystal resonator, oscillating in overtone mode. An analog thermal compensation network is implemented.
- Modulation indices may be selected by commands or, as option, automatic selection may be implemented. In this case a specific circuit keeps constant the total power of the modulation signal in presence of one, two or three input signals, in whatever combination
- The signal level emerging from the loop is about +10dBm. The following medium power Ku-band amplifier chain provides +27 dBm power level; it composed by three single ended stages using GaAs FET devices. The following SSPA, delivering 8W E.O.L. power level, is a single ended design, based on two power GaAs FET devices
- As an option, the unit can be equipped with an extra, independent amplifier chain, having an output power up to 0.5 W E.O.L. In this case the transmitter unit can operate in two functional modes: low power mode (0.5W), with high power output isolated (<-30dBm) and high power mode (8W), with low power output isolated (-15dBm)

Ku Band High Power Telemetry Transmitter Block Diagram



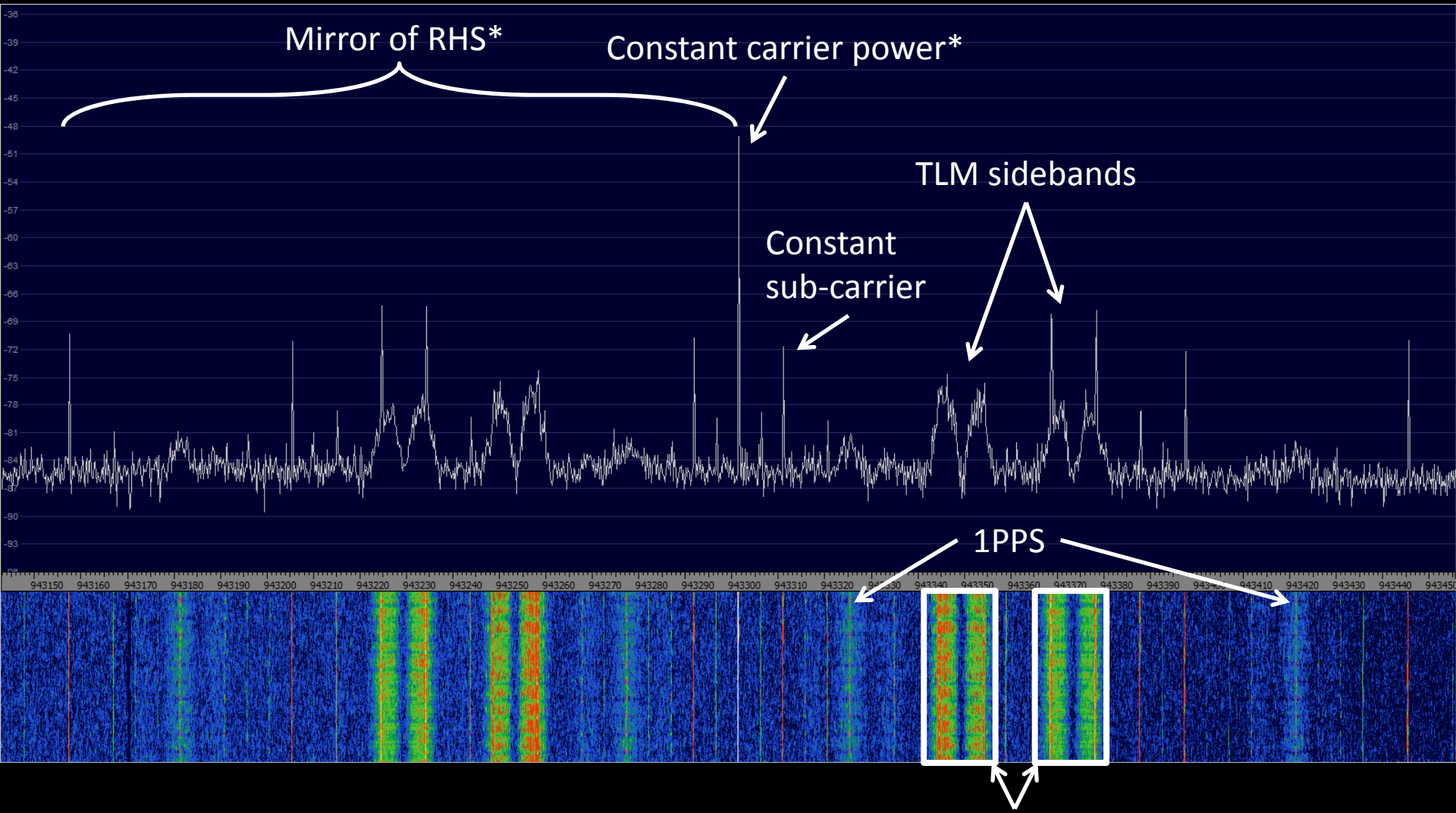
Main Performances

Output Frequency	10.7 – 12.7 GHz
Frequency Stability	± 10 ppm Std Stability Opt ± 5 ppm High Stability Opt
Output Power Level Extra Output	≥ 38.5 dBm (7W) EOL, up to 40dBm (10W) BOL (25C) ≥ 27 dBm EOL Dual Power Opt
Output Phase Noise	< 4 deg_{rms} @ 10 Hz to 1 MHz
PM modulation index	Up to 2.4 radpk
Mod.Index Selection	By command Automatic according to mod.tones number
Modulation Linearity	± 3%
Modulation Op.Mode	TM1, TM2, RNG1, RNG2, RNGS + TMs
DC/DC converter	55/71V – 22/43V (16Vpp max in the range for best efficiency)
Command Interface	HLC
Qualification Temp. Range	-25 / +65 °C

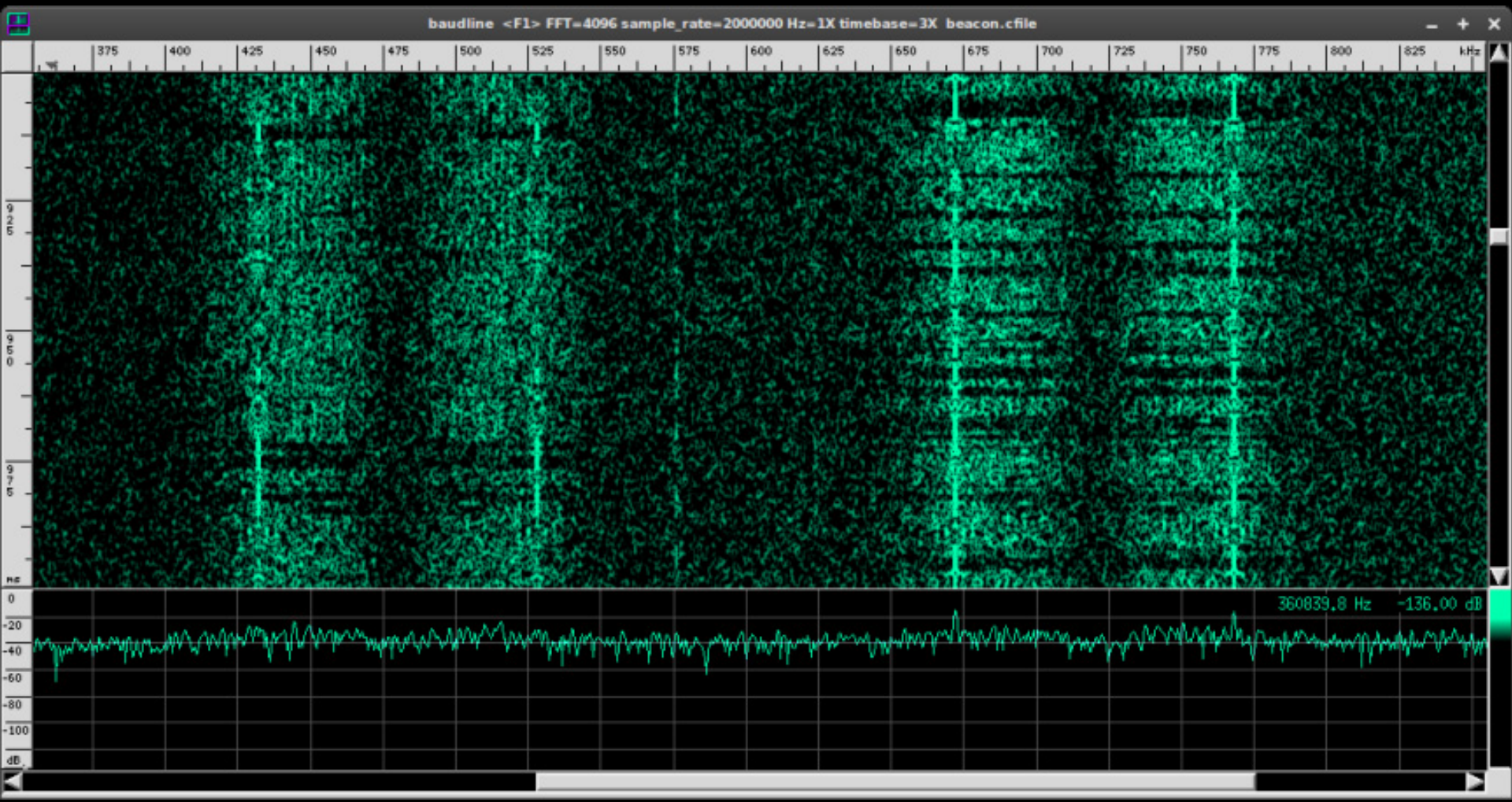
Mass, Dimensions and Consumption

DC Power Consumption	High power mode Low power mode	<55W <18W (Dual Power Opt)
Mass Properties	< 2 kg	
Outline Dimensions	250 x 130 x 80 mm	

D1 TLM1: 12243.25 MHz



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


baudline <F1> FFT=4096 sample_rate=2000000 Hz=1X timebase=3X beacon.cfile
375
400
425
450
475
500
525
550
575
600
625
650
675
700
725
750
775
800
825
kHz
360839.8 Hz -136.00 dB
0
-20
-40
-60
-80
-100
dB

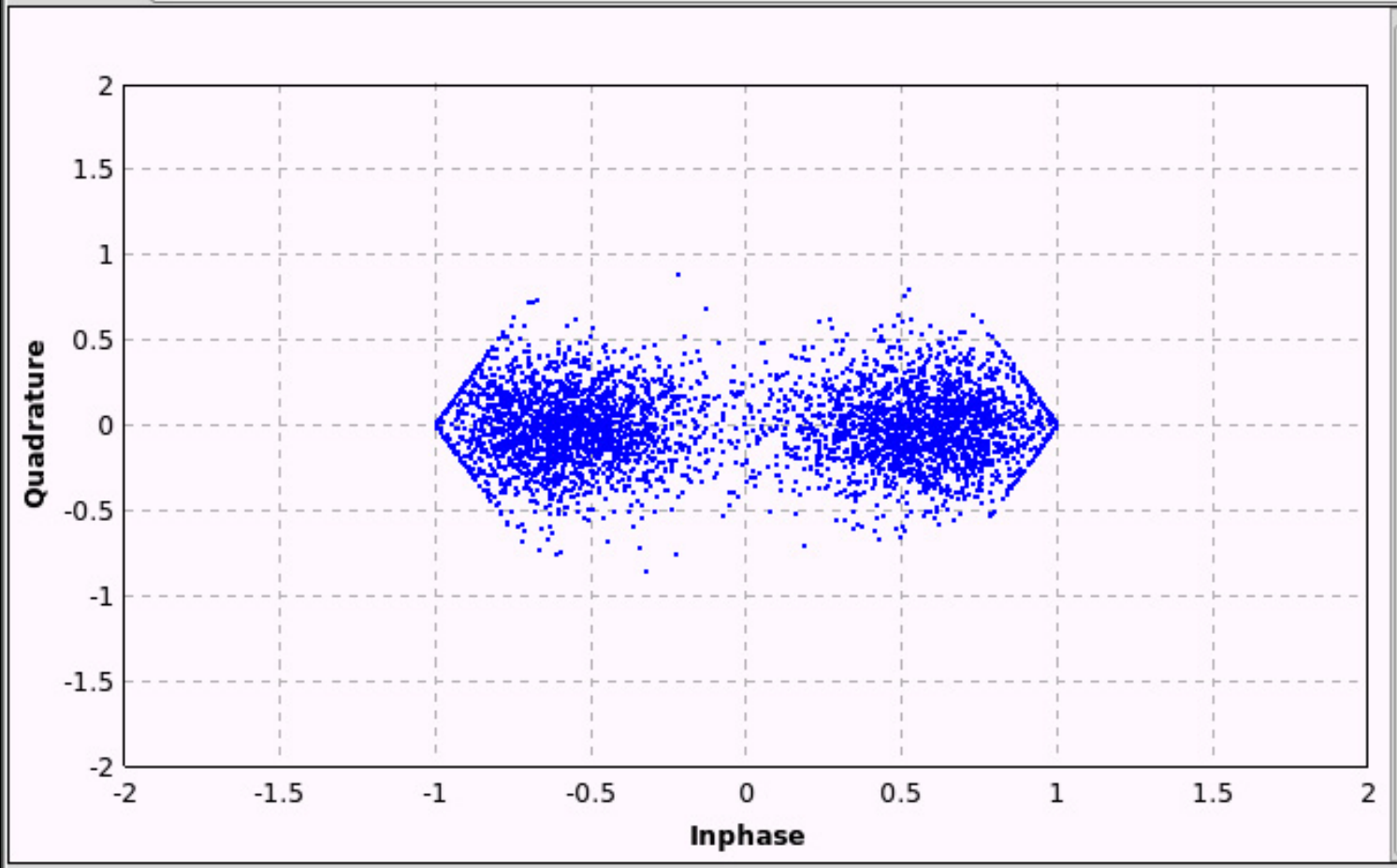
Top Block

BB | Scope | Demod | Pow | Cyclo | FAC | # | Quad | Mag | Test

Symbol rate (fine): 0

sym_rate_coarse: 0

Symbol rate: 9600



Options

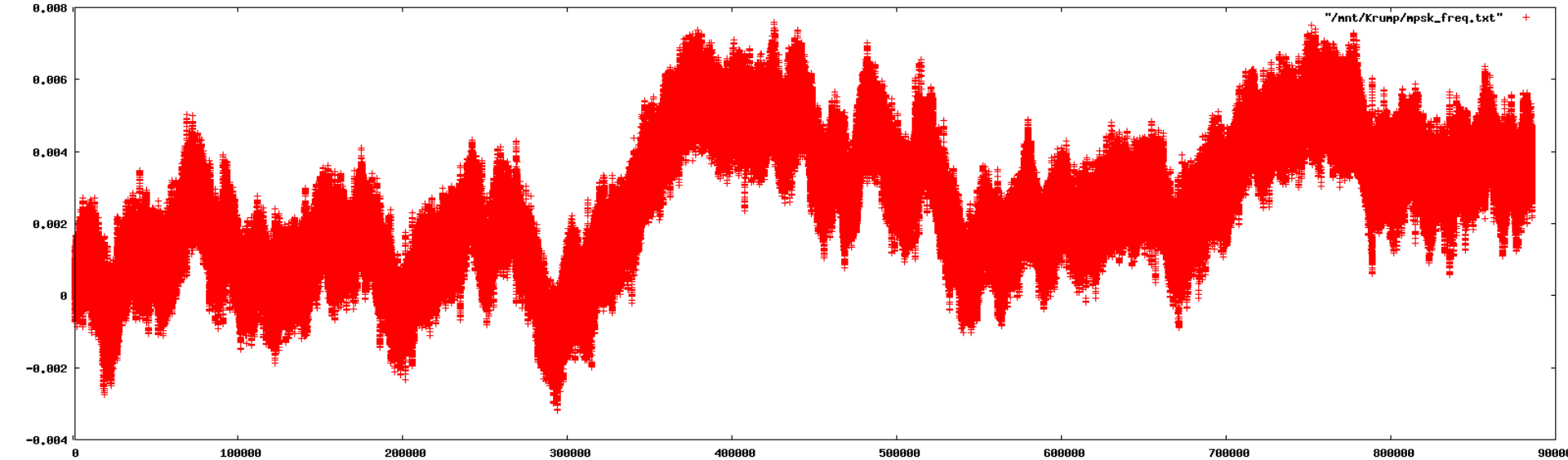
Alpha: 5m

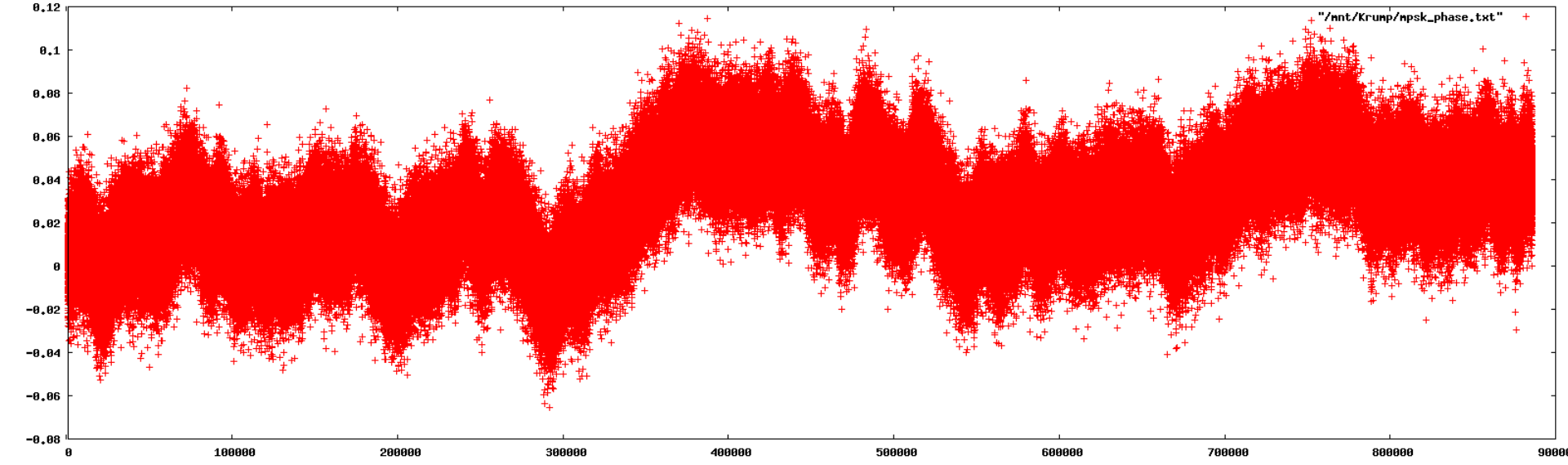
Gain Mu: 5m

Marker: Dot Medium

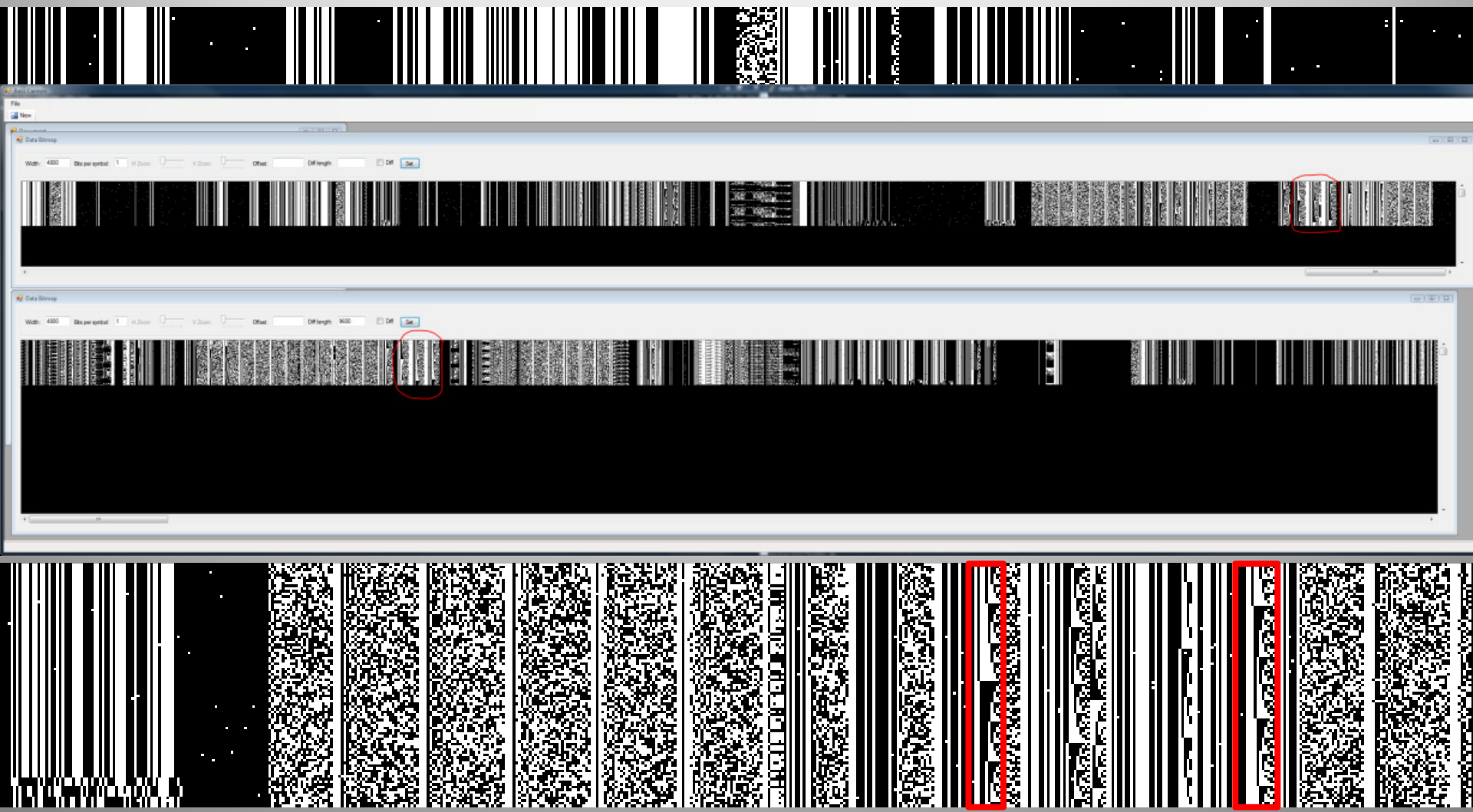
Run

PSK Debug Output



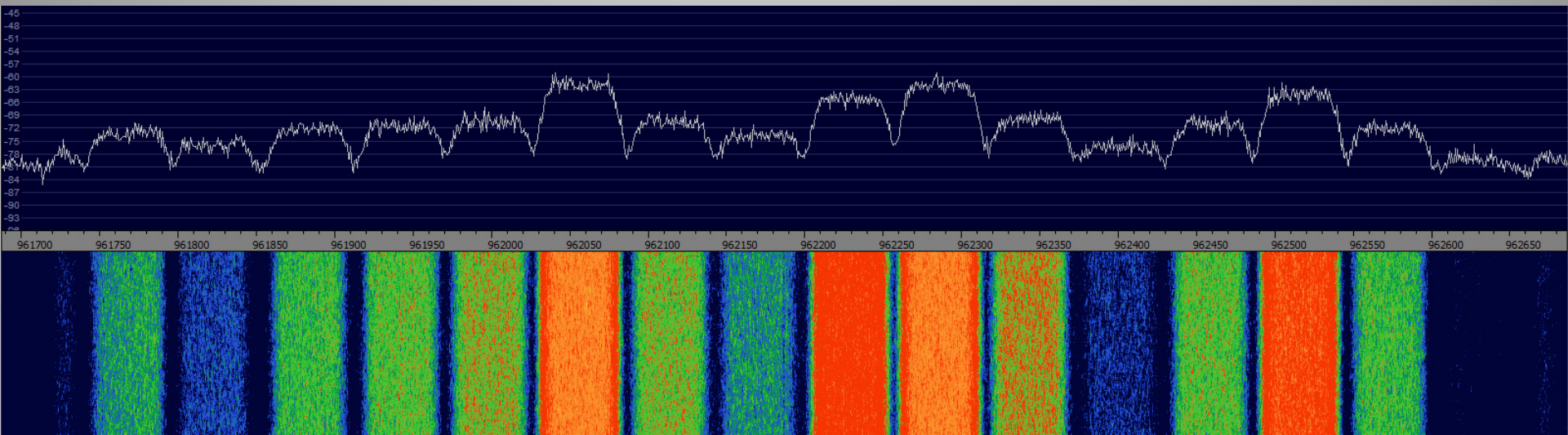


Visualisation



Data Streams

- All sorts of continuous streams of varying bandwidth
- Streams created by manipulating raw data to optimise for transmission over long distance
- Receiver must be able to lock on and decode

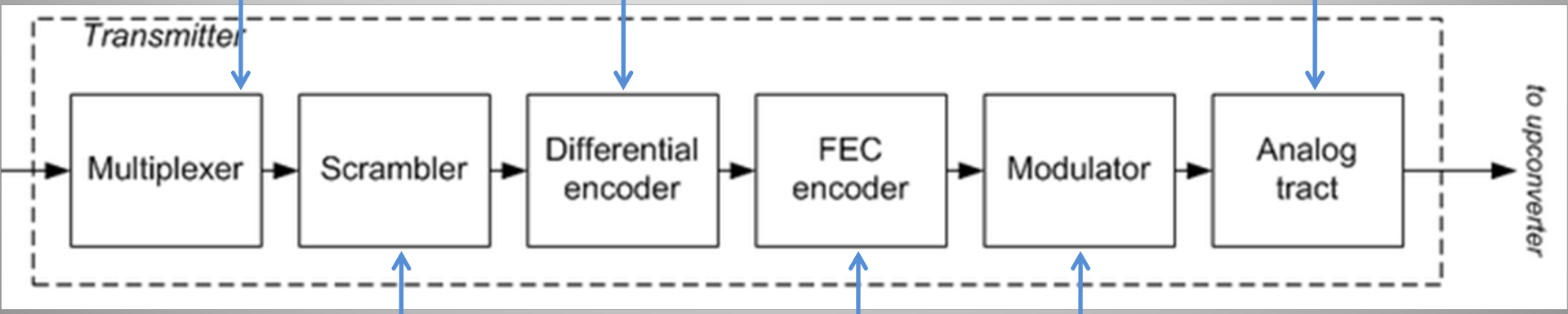


Modulation: pick your parameters

Support multiple data streams, drop-and-insert

Encode changes in data (receiver can be non-coherent)

Create signal suitable for uplink



Make data appear random (increase entropy of structured data)

Turn binary into symbols for baseband RF (0/1 → combinations of waves)

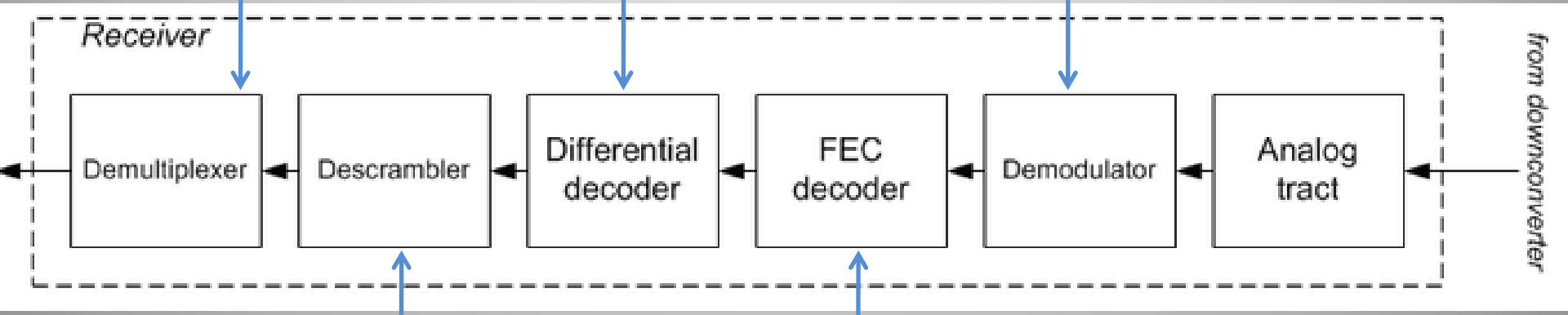
Protect integrity of data (corruption from noise on channel)

Demodulation: easy when you know

Are there multiple streams?
How are they multiplexed?

Is it differential, or
what defines a 0/1?

What is the modulation?
Symbol rate? Require coherence?
What is the phase difference?
Need to conjugate complex plane?



Possible to determine if it is scrambled
(calculate stats), but what is the scrambler?
Is it additive or multiplicative?
How is it synchronised?

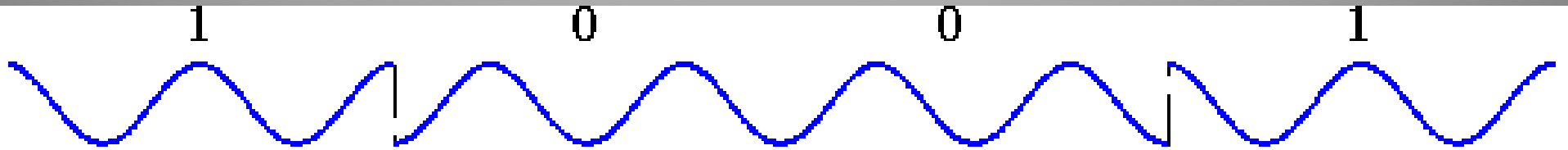
Which FEC(s) is used?
Is it a concatenated code?
What is the code rate?
What is the block size?
How is it synchronised?

If you don’t know…

- Try the most common/default options (RTFMM):
  - Modulation: **P**hase **S**hift **K**eying (BPSK, QPSK)
  - Convolutional code: NASA, K=7 (Voyager Probe)
  - Scrambler: IESS-803 (**I**ntelsat **B**usiness **S**ervice)
- Still need to try each combination of:
  - Differential decoding, synchronisation offset, symbol mapping
- Best option is to try every permutation automatically
- Assuming decent SNR, low **B**it **E**rror **R**ate is an indicator you’re heading the right way!

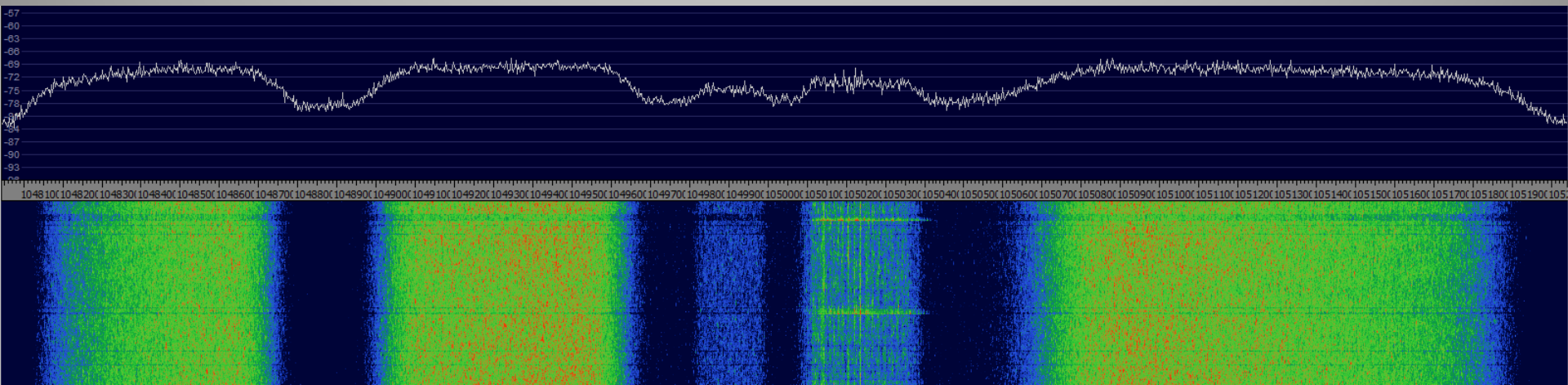
Aside: PSK, Symbols & Bits

- PSK uses changes in phase of a signal (carrier) to convey data
- Demodulator detects phase changes and outputs symbols
- Order of PSK determines # bits in 1 symbol
  - Many bits/symbol thanks to imaginary numbers (I/Q)
- Raw bit rate = symbol rate x (# bits/symbol)
  - Binary PSK (BPSK): 1 bit/symbol
  - Quaternary PSK (QPSK): 2 bits/symbol
  - 8PSK: 3 bits/symbol, etc…

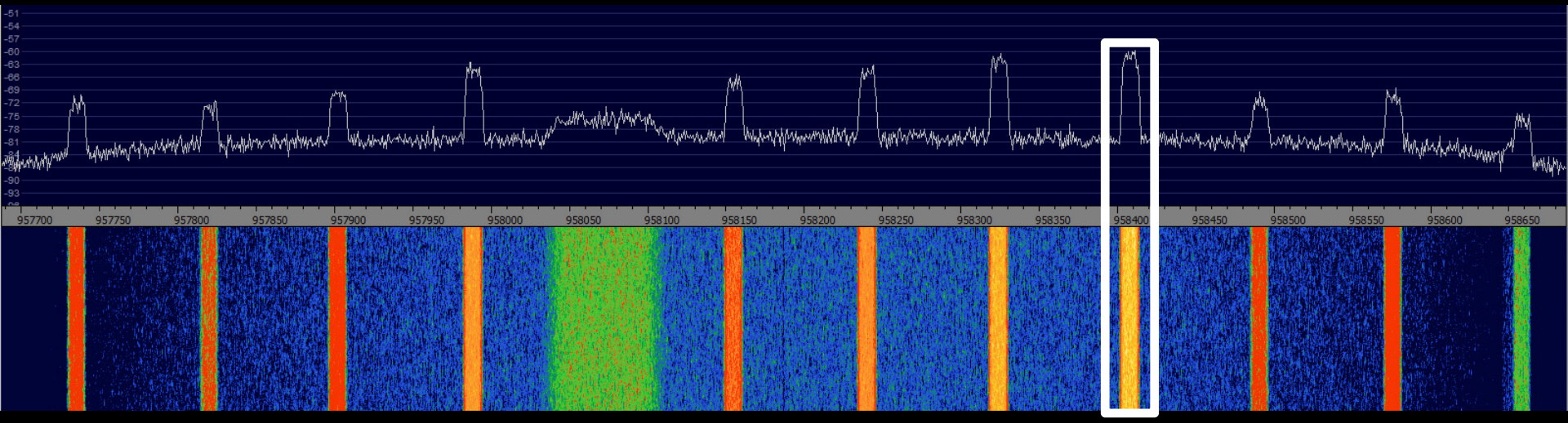


Determining modulation & rate

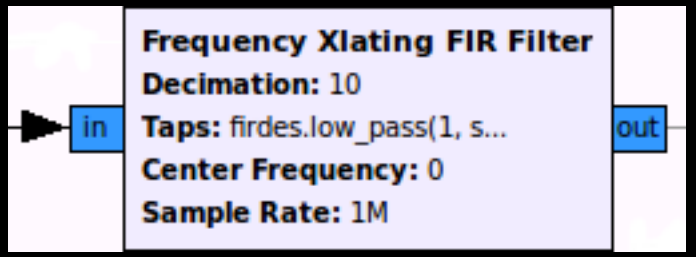
- Assuming PSK, easy to determine:
  - Modulation order: multiply the signal by itself
  - Symbol rate: multiply the signal by a lagged version of itself (cyclostationary analysis)
- Only a few GR blocks required do this



Let’s try one…

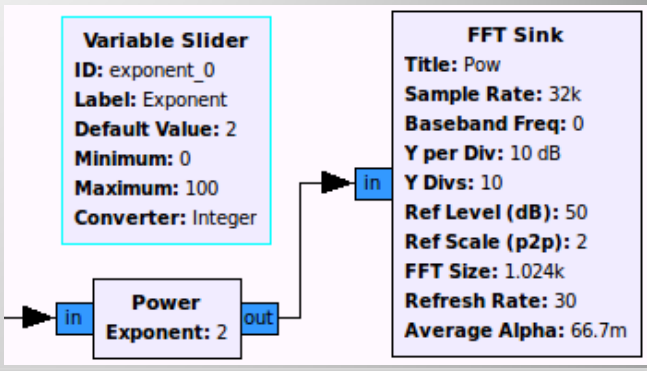


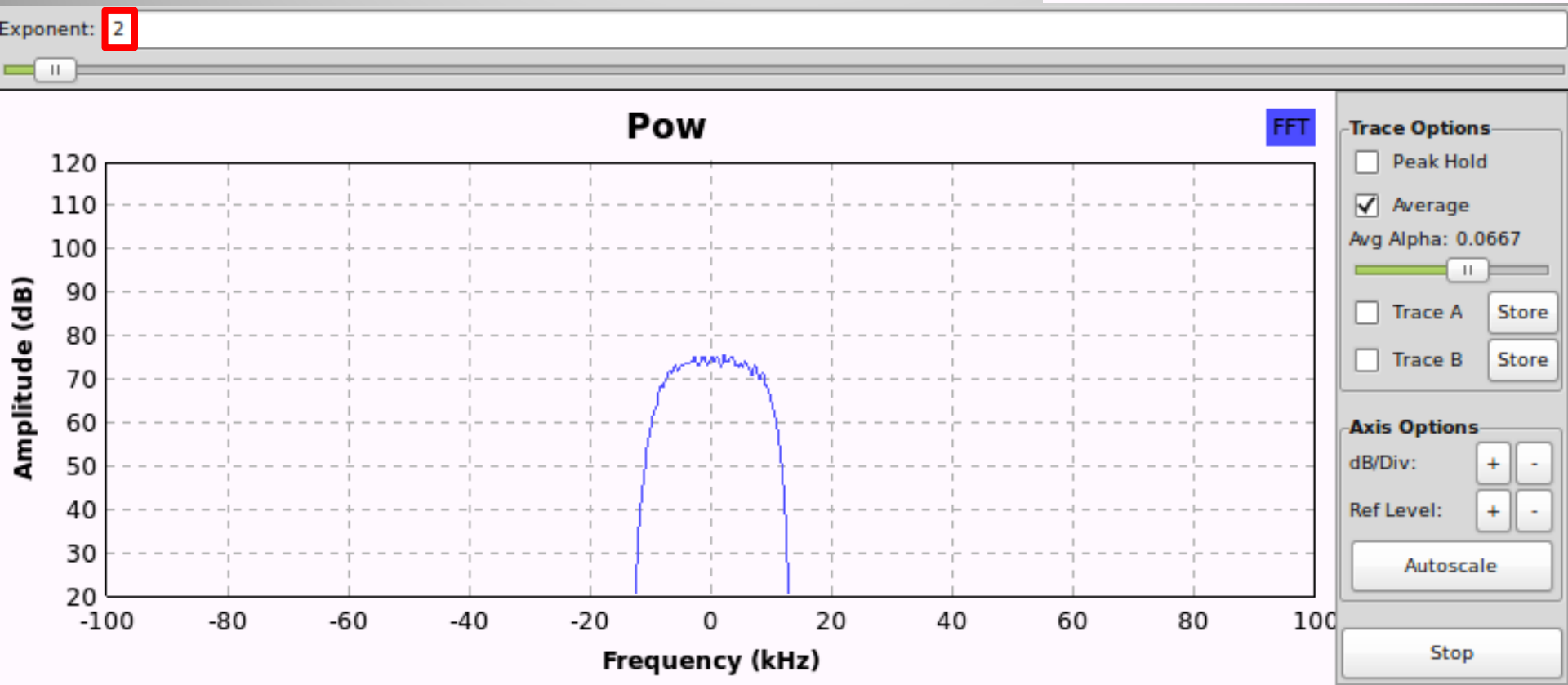
- Feed entire baseband spectrum into GR
- Perform ‘channel selection’ to isolate stream of interest (create new baseband centred on stream)



Determine PSK order

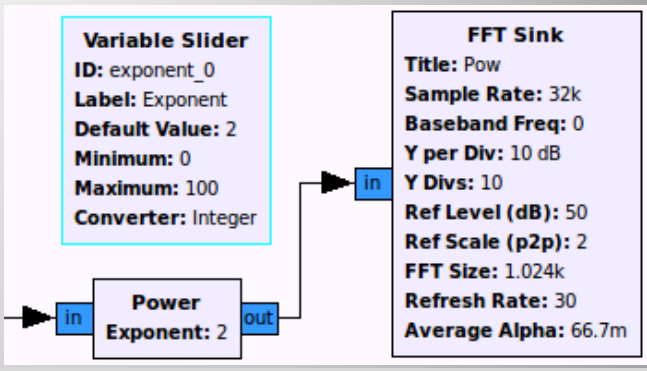
- Start at 2 and go up
- Stop when spike appears

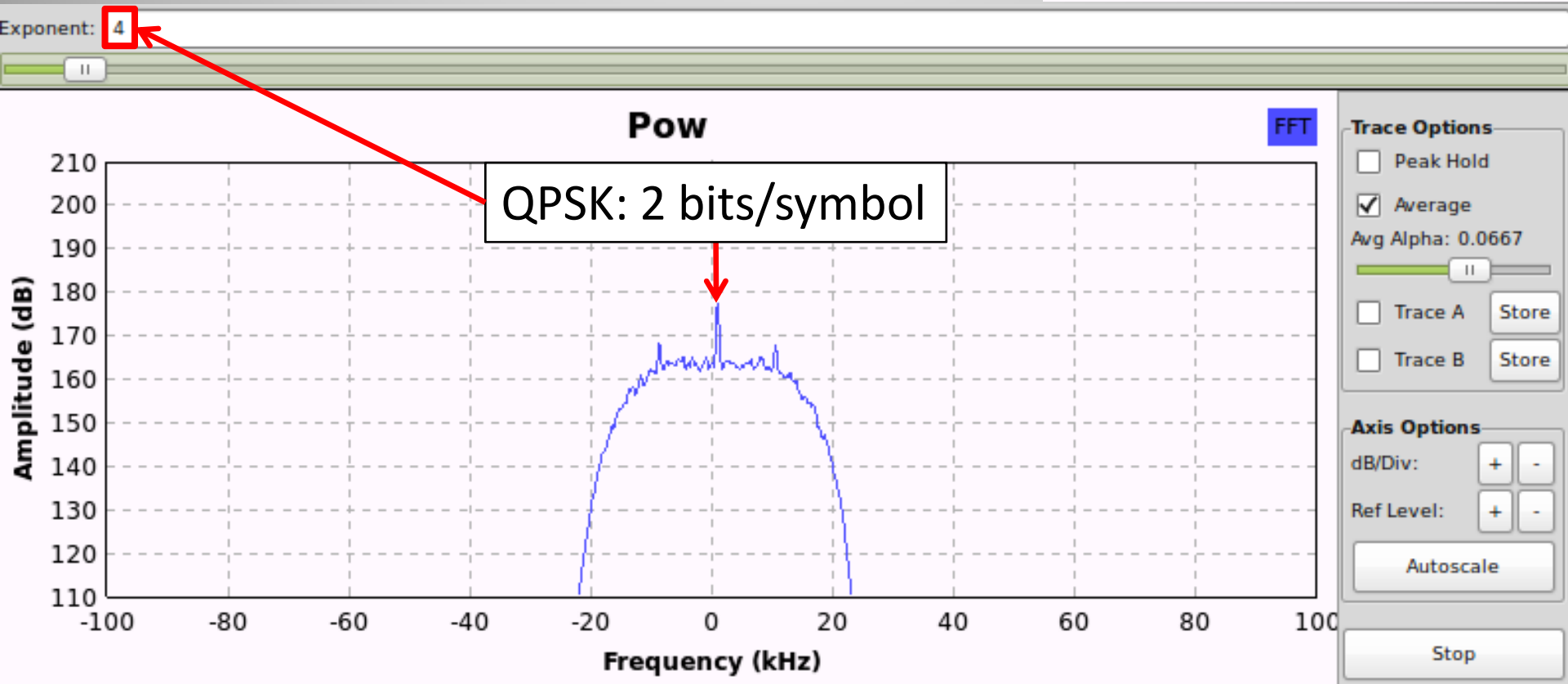




Determine PSK order

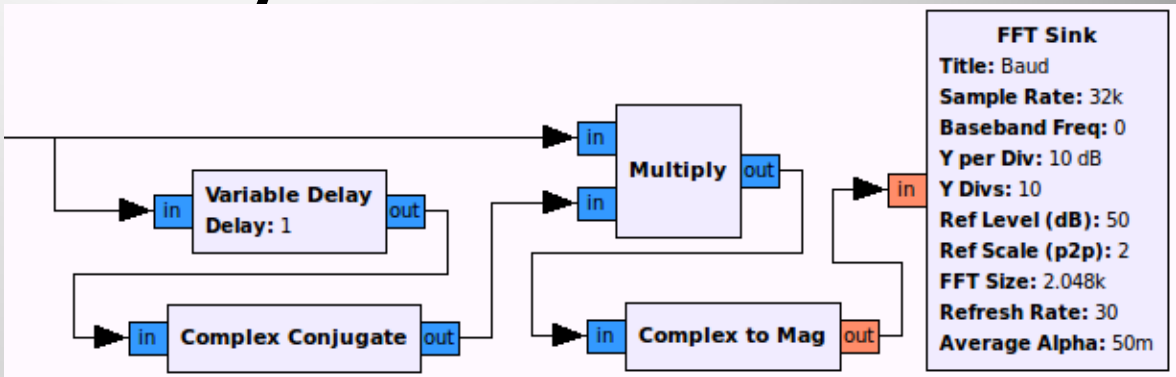
- Start at 2 and go up
- Stop when spike appears



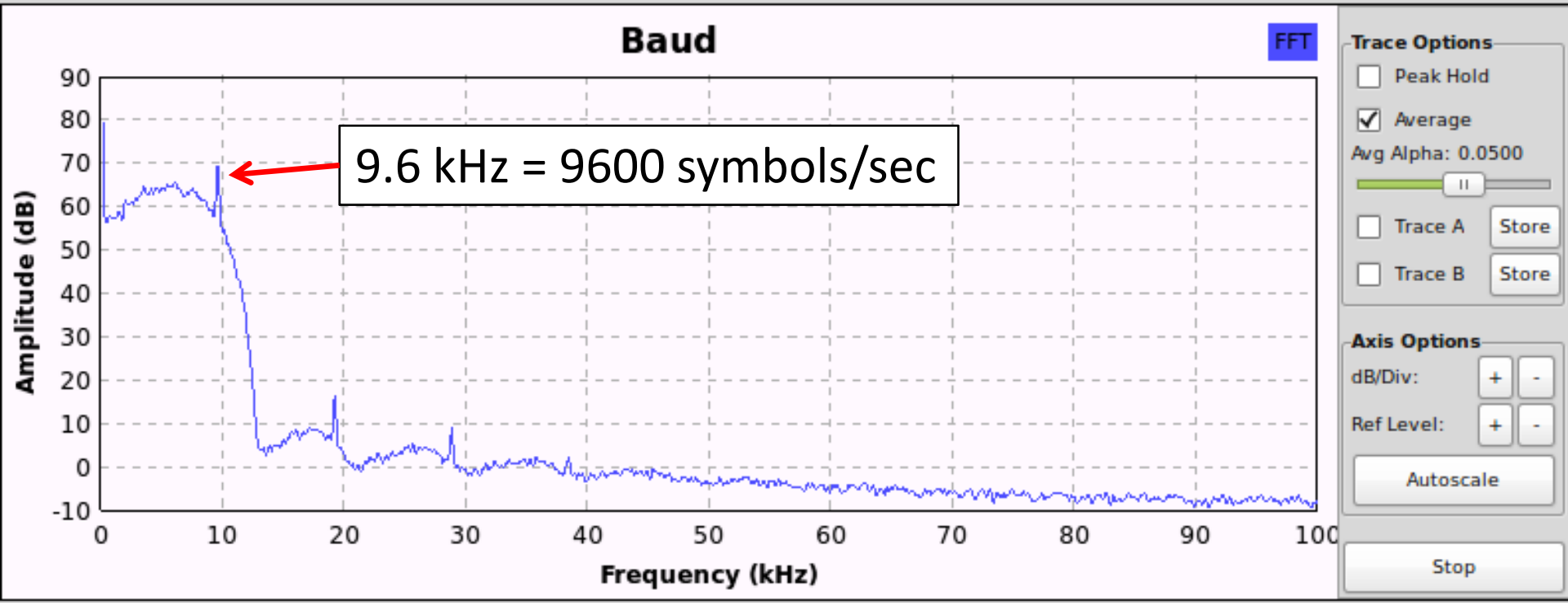


Determine Symbol Rate

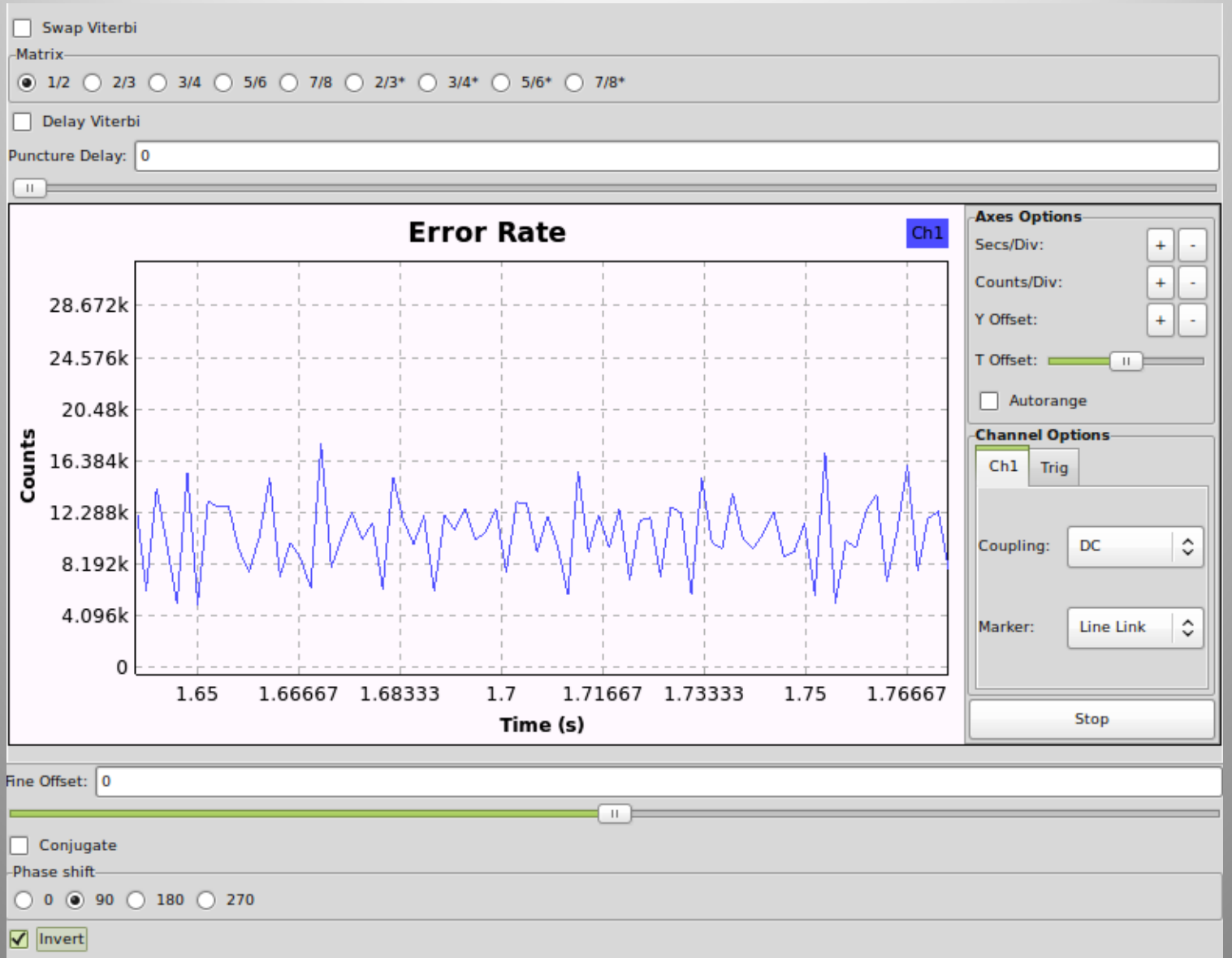
- Find first peak



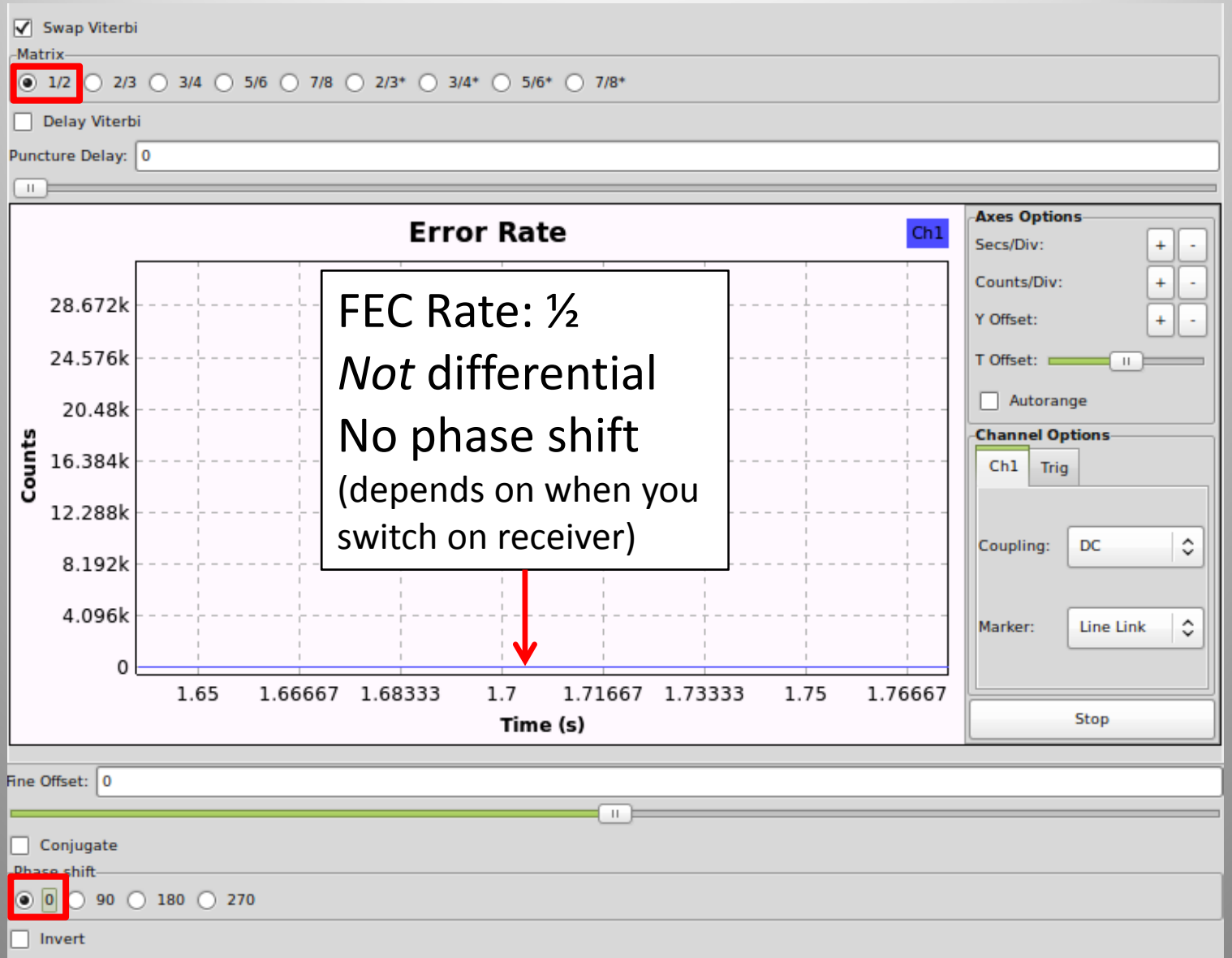
Nominal samples per symbol: 2



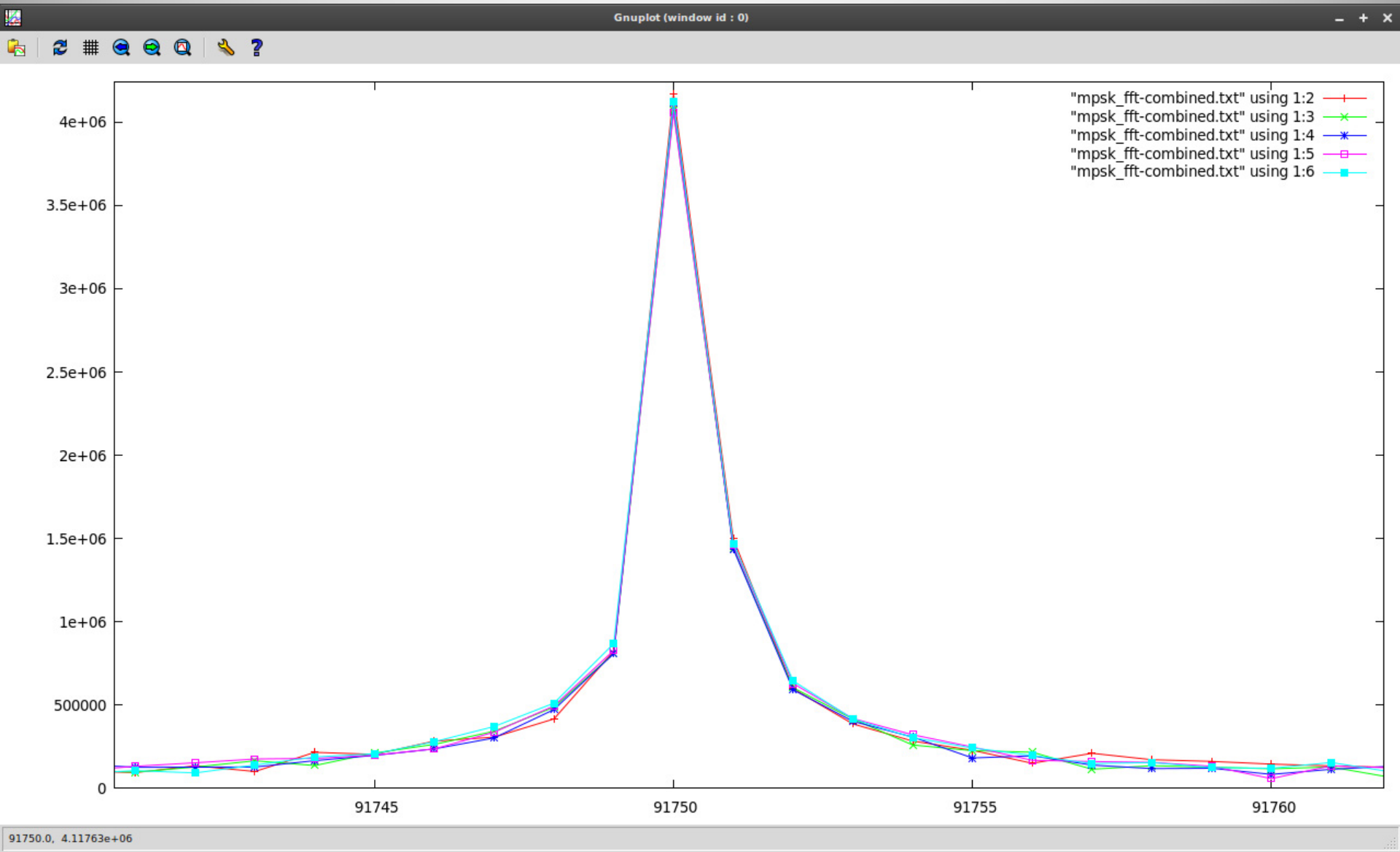
Try synchronisation & FEC

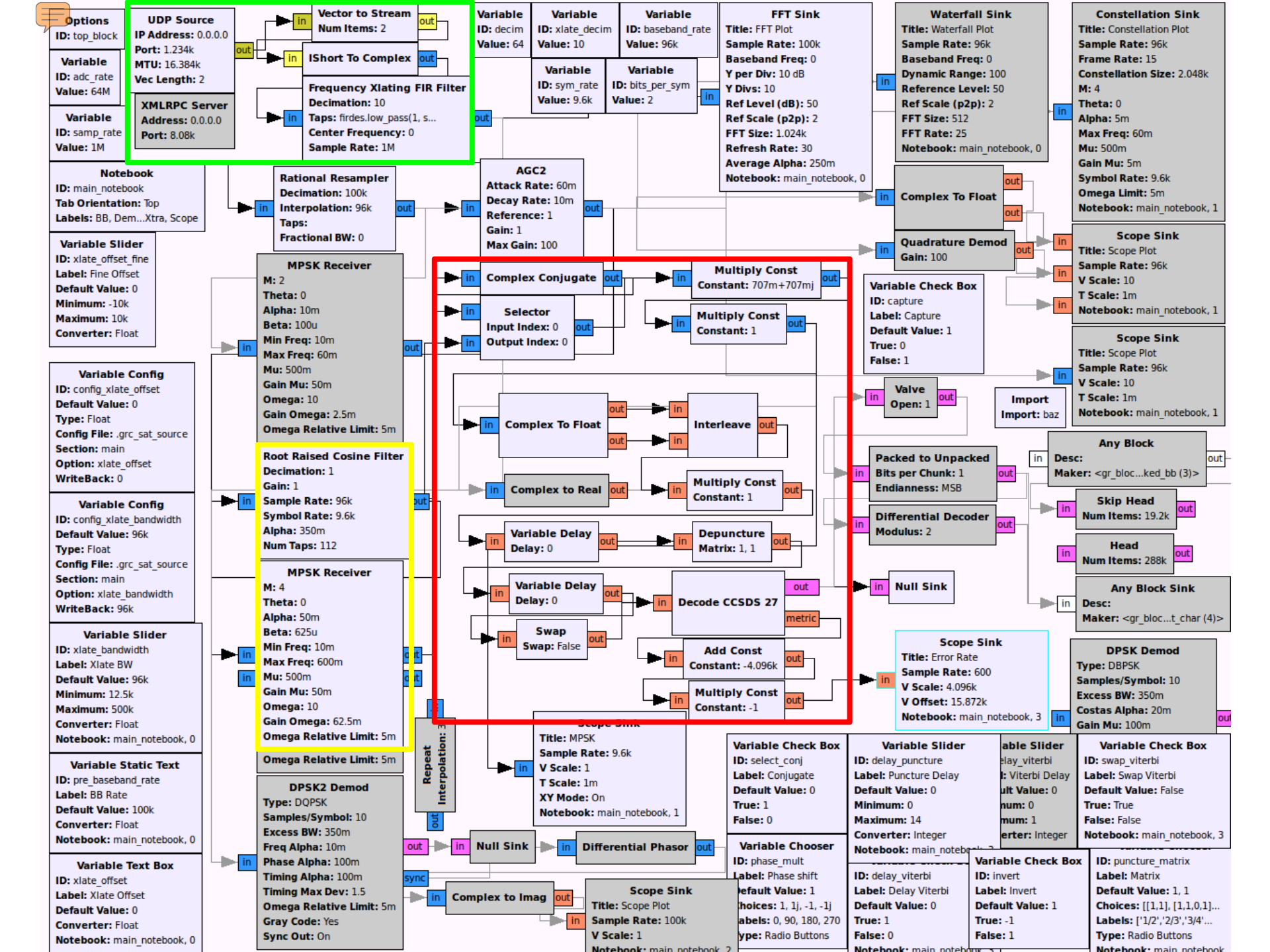


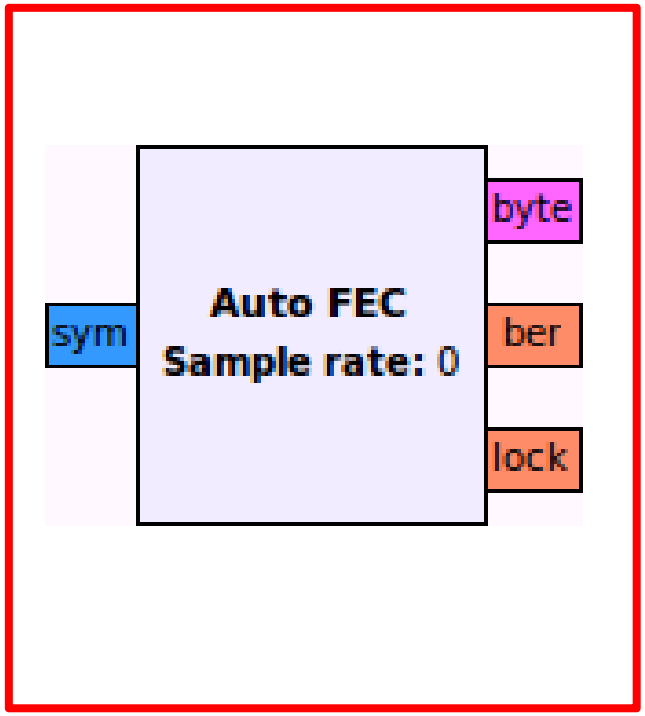
Try synchronisation & FEC



Find Precise Symbol Rate




Options
ID: top_block
UDP Source
IP Address: 0.0.0.0
Port: 1.234k
MTU: 16.384k
Vec Length: 2
XMLRPC Server
Address: 0.0.0.0
Port: 8.08k
Vector to Stream
Num Items: 2
IShort To Complex
Frequency Xlating FIR Filter
Decimation: 10
Taps: firdes.low_pass(1, s...
Center Frequency: 0
Sample Rate: 1M
Variable
ID: decim
Value: 64
Variable
ID: xlate_decim
Value: 10
Variable
ID: baseband_rate
Value: 96k
Variable
ID: sym_rate
Value: 9.6k
Variable
ID: bits_per_sym
Value: 2
FFT Sink
Title: FFT Plot
Sample Rate: 100k
Baseband Freq: 0
Y per Div: 10 dB
Y Divs: 10
Ref Level (dB): 50
Ref Scale (p2p): 2
FFT Size: 1.024k
Refresh Rate: 30
Average Alpha: 250m
Notebook: main_notebook, 0
Waterfall Sink
Title: Waterfall Plot
Sample Rate: 96k
Baseband Freq: 0
Dynamic Range: 100
Reference Level: 50
Ref Scale (p2p): 2
FFT Size: 512
FFT Rate: 25
Notebook: main_notebook, 0
Constellation Sink
Title: Constellation Plot
Sample Rate: 96k
Frame Rate: 15
Constellation Size: 2.048k
M: 4
Theta: 0
Alpha: 5m
Max Freq: 60m
Mu: 500m
Gain Mu: 5m
Symbol Rate: 9.6k
Omega Limit: 5m
Notebook: main_notebook, 1
Variable
ID: adc_rate
Value: 64M
Variable
ID: samp_rate
Value: 1M
Notebook
ID: main_notebook
Tab Orientation: Top
Labels: BB, Dem...Xtra, Scope
Rational Resampler
Decimation: 100k
Interpolation: 96k
Taps:
Fractional BW: 0
AGC2
Attack Rate: 60m
Decay Rate: 10m
Reference: 1
Gain: 1
Max Gain: 100
Complex To Float
Quadrature Demod
Gain: 100
Scope Sink
Title: Scope Plot
Sample Rate: 96k
V Scale: 10
T Scale: 1m
Notebook: main_notebook, 1
Variable Slider
ID: xlate_offset_fine
Label: Fine Offset
Default Value: 0
Minimum: -10k
Maximum: 10k
Converter: Float
MPSK Receiver
M: 2
Theta: 0
Alpha: 10m
Beta: 100u
Min Freq: 10m
Max Freq: 60m
Mu: 500m
Gain Mu: 50m
Omega: 10
Gain Omega: 2.5m
Omega Relative Limit: 5m
Complex Conjugate
Selector
Input Index: 0
Output Index: 0
Multiply Const
Constant: 707m+707mj
Multiply Const
Constant: 1
Variable Check Box
ID: capture
Label: Capture
Default Value: 1
True: 0
False: 1
Valve
Open: 1
Import
Import: baz
Variable Config
ID: config_xlate_offset
Default Value: 0
Type: Float
Config File: .grc_sat_source
Section: main
Option: xlate_offset
WriteBack: 0
Complex To Float
Interleave
Complex to Real
Multiply Const
Constant: 1
Variable Delay
Delay: 0
Depuncture
Matrix: 1, 1
Packed to Unpacked
Bits per Chunk: 1
Endianness: MSB
Differential Decoder
Modulus: 2
Any Block
Desc:
Maker: <gr_bloc...ked_bb (3)>
Skip Head
Num Items: 19.2k
Head
Num Items: 288k
Any Block Sink
Desc:
Maker: <gr_bloc...t_char (4)>
Root Raised Cosine Filter
Decimation: 1
Gain: 1
Sample Rate: 96k
Symbol Rate: 9.6k
Alpha: 350m
Num Taps: 112
Variable Config
ID: config_xlate_bandwidth
Default Value: 96k
Type: Float
Config File: .grc_sat_source
Section: main
Option: xlate_bandwidth
WriteBack: 96k
MPSK Receiver
M: 4
Theta: 0
Alpha: 50m
Beta: 625u
Min Freq: 10m
Max Freq: 600m
Mu: 500m
Gain Mu: 50m
Omega: 10
Gain Omega: 62.5m
Omega Relative Limit: 5m
Variable Delay
Delay: 0
Decode CCSDS 27
Swap
Swap: False
Null Sink
Add Const
Constant: -4.096k
Multiply Const
Constant: -1
Scope Sink
Title: Error Rate
Sample Rate: 600
V Scale: 4.096k
V Offset: 15.872k
Notebook: main_notebook, 3
DPSK Demod
Type: DBPSK
Samples/Symbol: 10
Excess BW: 350m
Costas Alpha: 20m
Gain Mu: 100
Variable Slider
ID: xlate_bandwidth
Label: Xlate BW
Default Value: 96k
Minimum: 12.5k
Maximum: 500k
Converter: Float
Notebook: main_notebook, 0
Omega Relative Limit: 5m
Repeat
Interpolation: 3
Scope Sink
Title: MPSK
Sample Rate: 9.6k
V Scale: 1
T Scale: 1m
XY Mode: On
Notebook: main_notebook, 1
Variable Check Box
ID: select_conj
Label: Conjugate
Default Value: 0
True: 1
False: 0
Variable Slider
ID: delay_puncture
Label: Puncture Delay
Default Value: 0
Minimum: 0
Maximum: 14
Converter: Integer
Notebook: main_notebook, 2
Variable Check Box
ID: swap_viterbi
Label: Swap Viterbi
Default Value: False
True: True
False: False
Notebook: main_notebook, 3
Variable Static Text
ID: pre_baseband_rate
Label: BB Rate
Default Value: 100k
Converter: Float
Notebook: main_notebook, 0
DPSK2 Demod
Type: DQPSK
Samples/Symbol: 10
Excess BW: 350m
Freq Alpha: 10m
Phase Alpha: 100m
Timing Alpha: 100m
Timing Max Dev: 1.5
Omega Relative Limit: 5m
Gray Code: Yes
Sync Out: On
Null Sink
Differential Phasor
Variable Chooser
ID: phase_mult
Label: Phase shift
Default Value: 1
Choices: 1, 1j, -1, -1j
Labels: 0, 90, 180, 270
Type: Radio Buttons
Variable Check Box
ID: delay_viterbi
Label: Delay Viterbi
Default Value: 0
True: 1
False: 0
Variable Check Box
ID: invert
Label: Invert
Default Value: 1
True: -1
False: 1
Variable Text Box
ID: xlate_offset
Label: Xlate Offset
Default Value: 0
Converter: Float
Notebook: main_notebook, 0
Complex to Imag
Scope Sink
Title: Scope Plot
Sample Rate: 100k
V Scale: 1
Notebook: main_notebook, 2
ID: puncture_matrix
Label: Matrix
Default Value: 1, 1
Choices: [[1,1], [1,1,0,1]...
Labels: ['1/2','2/3','3/4'...
Type: Radio Buttons
Notebook: main_notebook


Auto FEC
Sample rate: 0
sym
byte
ber
lock

Auto FEC

```
Creating Auto-FEC:
    sample_rate:                800000
    ber_threshold:              2048
    ber_smoothing:              0.01
    ber_duration:               8192
    ber_sample_decimation:      1
    settling_period:  4096
    pre_lock_duration:          8192

De-puncturer relative rate: 1.000000
==> Using throttle at sample rate: 800000
==> Using lock throttle rate: 50000
Auto-FEC thread started: Thread-1
Skipping initial samples while MPSK receiver locks: 4096

Reached excess BER limit: 11437.1352901 , locked: False , current puncture matrix: 0 , total samples
    received: 12289
    Applying lock value: 0
Beginning search...
    Applying rotation: 1j

Reached excess BER limit: 11870.4144919 , locked: False , current puncture matrix: 0 , total samples
    received: 24586
    Applying rotation: 1
    Applying conjugation: 0

Locking current XForm
=====================================================
```

FEC locked: 1/2

```
=====================================================
    Applying lock value: 1
```

Demodulated & error-corrected

- Symbol rate = 9600 symbols/sec
- Pre-FEC raw bit rate = 19200 bits/sec
- Post-FEC raw bit rate = 9600 bits/sec (½ rate)

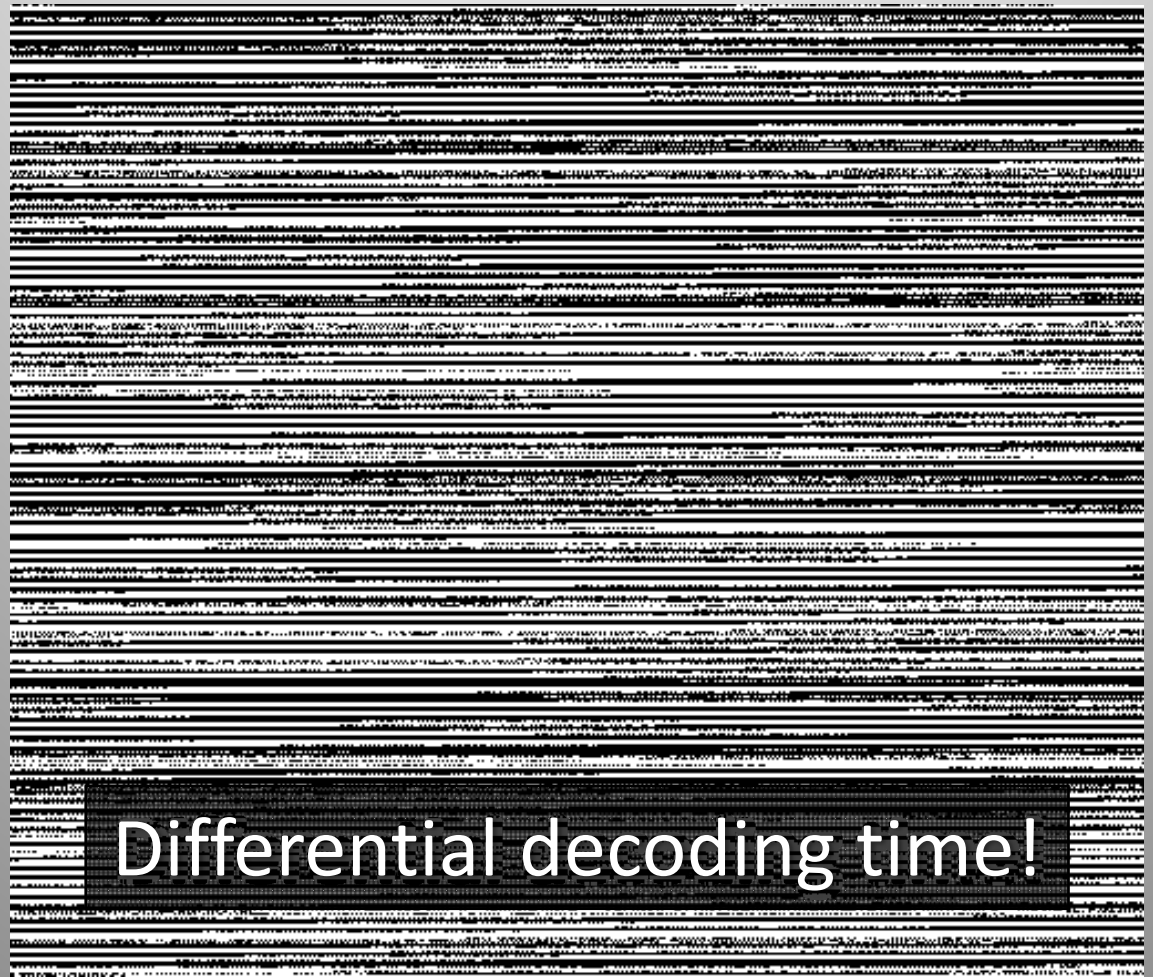
- Visualise data: look for additional clues
  - Differential encoding
  - Scrambling
  - Structure

Visualisation

- Raw data (0: black, 1: white)

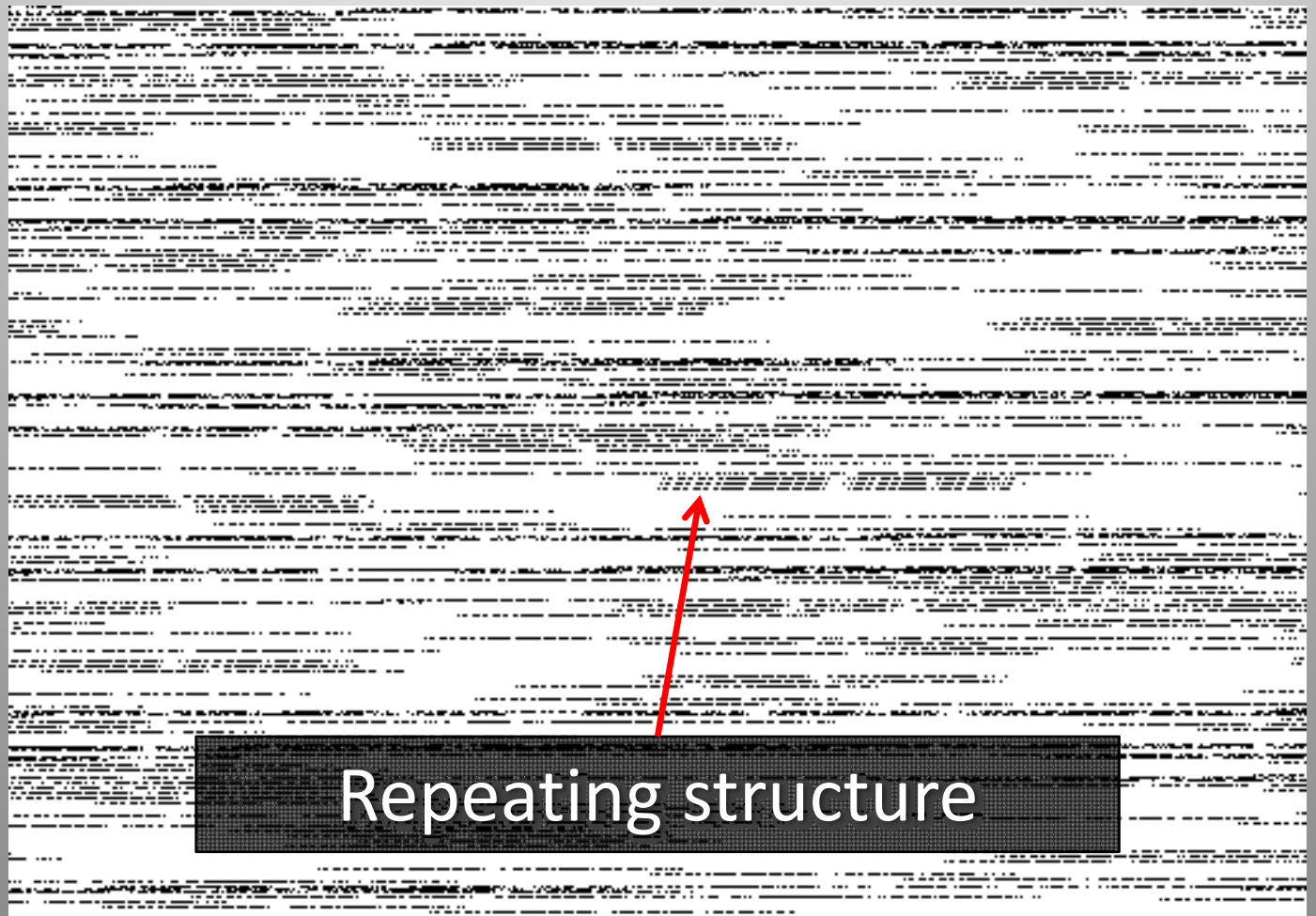
De-scrambled

- Better, but long runs of 0s and 1s (not ideal)



Diff. decoded & de-scrambled

- Structured, asynchronous packets of data!



Pattern Search

```
44 bits #0002-0002[+0000, /0000]: 00000001000011101000000010001011101111111011 (dfdd1017080)
44 bits #0002-0002[+0000, /0000]: 00000001100000011111000010111101010101111111 (feabd0f8180)
44 bits #0002-0002[+0000, /0000]: 00000001100001011111000010111101010101111111 (feabd0fa180)
44 bits #0004-0004[+0000, /0000]: 00000001100000110000100010111101010101111111 (feabd10c180)

43 bits #0000-0005[+0001, /0000]: 01101111001100000010011001100010000011000000 (1846640cf6)

42 bits #0002-0002[+0000, /0000]: 00000001100100011101001100001100001000000000 (430cb8980)
42 bits #0002-0002[+0000, /0000]: 00000001000001000010000001100110110000000010 (10366042080)
42 bits #0002-0002[+0000, /0000]: 00000001100100010001101100000011111000000000 (7c0d88980)
42 bits #0001-0003[+0000, /0000]: 00000001000011101000000010001011011111111110 (1fdd1017080)
42 bits #0003-0003[+0000, /0000]: 00000001100010011101001100001100001000000000 (430cb9180)
42 bits #0000-0004[+0002, /0000]: 00000011000001100001000101111010101011111111 (3f55e8860c0)

41 bits #0002-0002[+0000, /0000]: 00000001000011001001110000100111110000000000 (3e4393080)
41 bits #0003-0003[+0000, /0000]: 00000001000101001001110000001111110000000000 (3f0392880)
41 bits #0001-0003[+0000, /0000]: 00000001000011101000000011110101110000000001 (1036f017080)
41 bits #0000-0003[+0001, /0000]: 00000010000111010000000100010111011111111110 (fee880b840)
41 bits #0000-0004[+0002, /0000]: 00000001000011101000000010100000010101111111 (1f505017080)
41 bits #0006-0006[+0000, /0000]: 00000001000001000010000001011111110000000000 (3fa042080)

40 bits #0002-0002[+0000, /0000]: 11000010001011111001010000010001100000000 (18829f443)
40 bits #0002-0002[+0000, /0000]: 01100001011111110101000010001100000000111 (e0310afe86)
40 bits #0002-0002[+0000, /0000]: 00000001000011101000000010001011001111111 (fcd1017080)
40 bits #0002-0002[+0000, /0000]: 00011101001011001101000000100011000000001 (81881674b8)
40 bits #0000-0003[+0001, /0000]: 00000010000111010000000011110111011000000001 (81b780b840)
40 bits #0000-0003[+0001, /0000]: 00000011000100111010011000011000001000000000 (21865c8c0)
40 bits #0001-0004[+0000, /0000]: 00000001000011101000000010001011101111111111 (fdd1017080)
40 bits #0001-0004[+0000, /0000]: 00000001000011101000000011111011011000000000 (36f017080)
40 bits #0001-0005[+0000, /0000]: 00000001000011101000000010100000010101111111 (f505017080)
40 bits #0006-0006[+0000, /0000]: 00000001000001000010000001011111110000000000 (1fa042080)

39 bits #0002-0002[+0000, /0000]: 11111010010111001111010000100011000000000 (c42f3a5f)
39 bits #0002-0002[+0000, /0000]: 00100000011111111010010111000010111111111 (7f43a5fc04)
39 bits #0002-0002[+0000, /0000]: 00000001010101010010001101000111100000001 (41e2c4aa80)
39 bits #0002-0002[+0000, /0000]: 01110100101110011010000001000110000000010 (2062059d2e)
39 bits #0002-0002[+0000, /0000]: 01111101001011100111101000010001100000000 (1885e74be)
39 bits #0002-0002[+0000, /0000]: 01011010010111000110000000100011000000000 (c4063a5a)
39 bits #0000-0003[+0001, /0000]: 00000010001010010011100000011111000000000 (1f81c9440)
39 bits #0000-0004[+0001, /0000]: 00000010000111010000000100010111011111111 (7ee880b
39 bits #0000-0004[+0001, /0000]: 00000010000111010000000111101101100000000 (1b780b8
39 bits #0000-0005[+0002, /0000]: 00000010000111010000000101000001010111111 (7a8280b
39 bits #0000-0006[+0004, /0000]: 00000010000010000100000010111111110000000 (1fd0210
39 bits #0166-0172[+0000, /0000]: 11111110011000100110001001100100000000 (9919197

38 bits #0002-0002[+0000, /0000]: 01001000101110100001100001000110000000 (62185d12
38 bits #0002-0002[+0000, /0000]: 11110100101111011110100001000110000001 (206217bd
38 bits #0002-0002[+0000, /0000]: 00011000010111001011010000100011000000 (c42d3a18)
38 bits #0002-0002[+0000, /0000]: 00110000101111100110100001000110000000 (62167d0c)
38 bits #0001-0003[+0000, /0000]: 00000001010101010010001101000111100000 (1e2c4aa80)
38 bits #0000-0003[+0001, /0000]: 11111010010111001111010000100011000000 (c42f3a5f)
38 bits #0000-0003[+0001, /0000]: 01110100101110011010000001000110000001 (2062059d2e)
38 bits #0000-0006[+0004, /0000]: 00000010000010000100000010111111000000 (fd021040)
38 bits #0000-0172[+0166, /0000]: 111111010011000100110001001100100000000 (4c8c8cbf)

37 bits #0002-0002[+0000, /0000]: 11101100000001110101101100000001000000 (40dae037)
37 bits #0002-0002[+0000, /0000]: 10110100101111101101000001000110000000 (6205bd2d)
37 bits #0002-0002[+0000, /0000]: 00000001111011000010111001101011111111 (1fd6743780)
37 bits #0000-0003[+0001, /0000]: 00000010101010100100011010000111100000 (f1625540)
37 bits #0000-0010[+0008, /0000]: 00000001000001000010000001011111111010 (bfa042080)
37 bits #0000-0010[+0008, /0000]: 00000001000001000010000001011111110110 (dfa042080)
37 bits #0000-0010[+0008, /0000]: 00000001000001000010000001011111110001 (11fa042080)
```

- Search for repeating strings of bits
- Try to find frame header
- Clue: sudden increase in # of occurrences

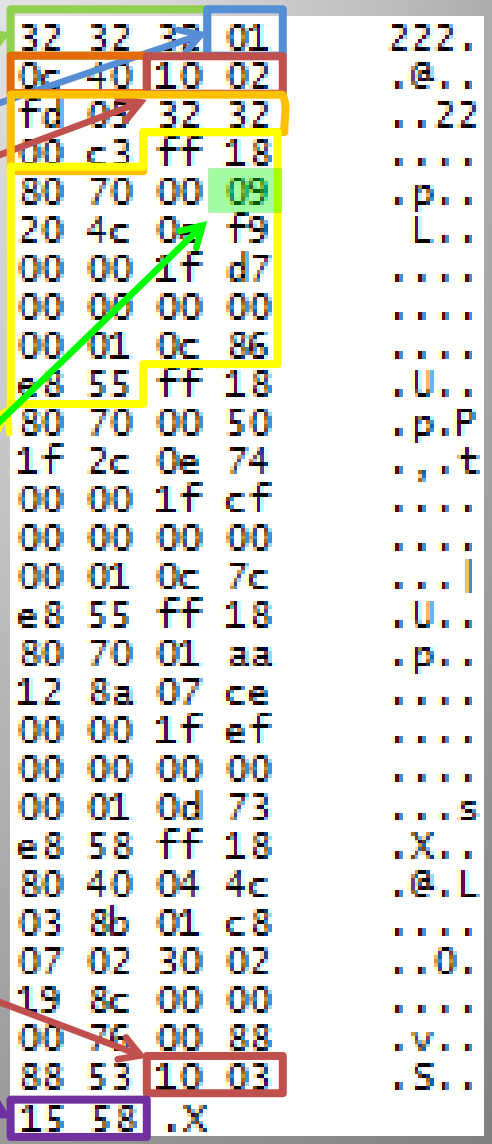
```
38 bits #0000-0006[+0004, /0000]: 00000010000010000100000010111111000000 (fd021040)
38 bits #0000-0172[+0166, /0000]: 111111010011000100110001001100100000000 (4c8c8cbf)

37 bits #0002-0002[+0000, /0000]: 11101100000001110101101100000001000000 (40dae037)
37 bits #0002-0002[+0000, /0000]: 10110100101111101101000001000110000000 (6205bd2d)
```

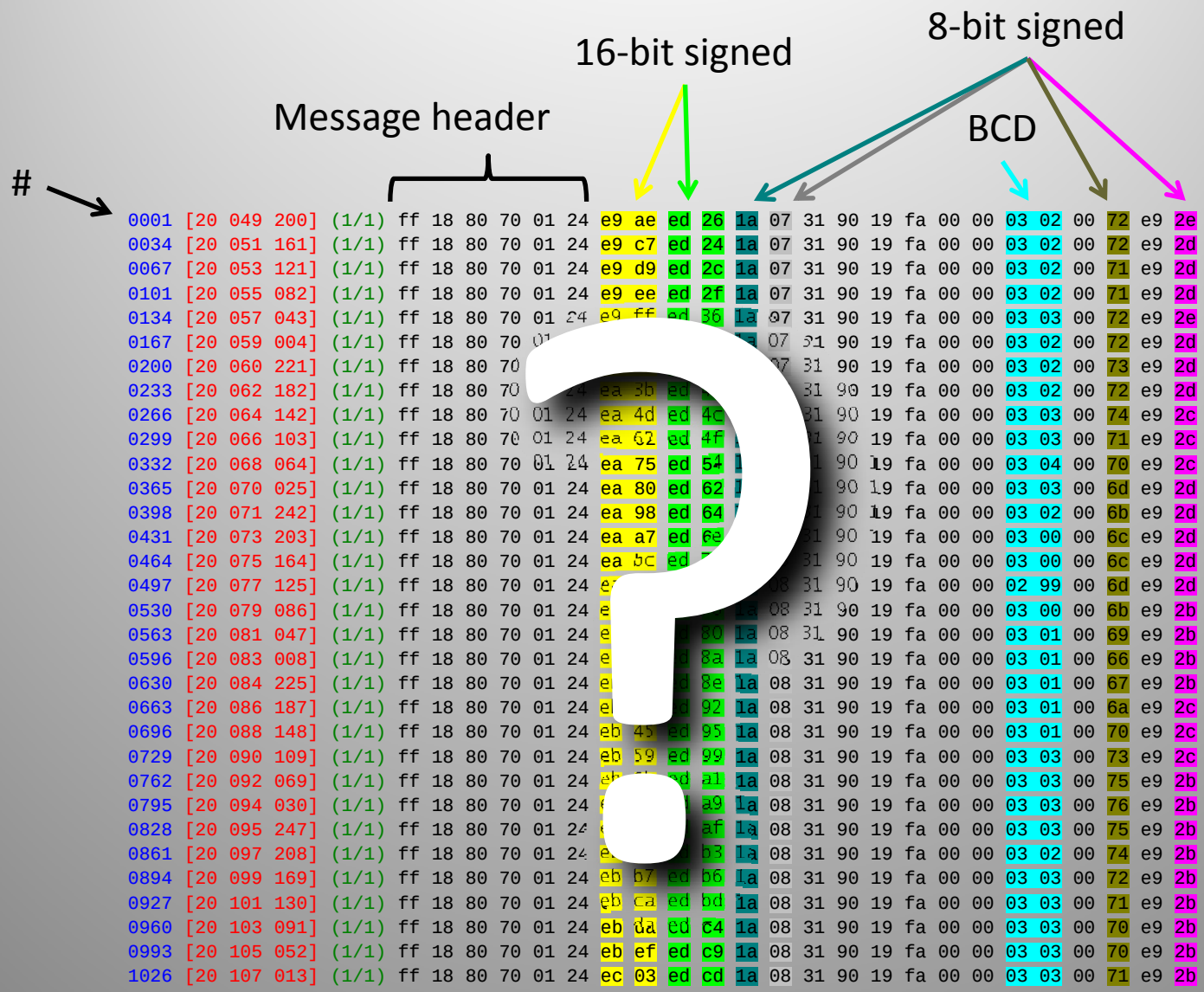
Preceding 1s are just part of ‘idle’ stream when no data is being sent

Frame analysis

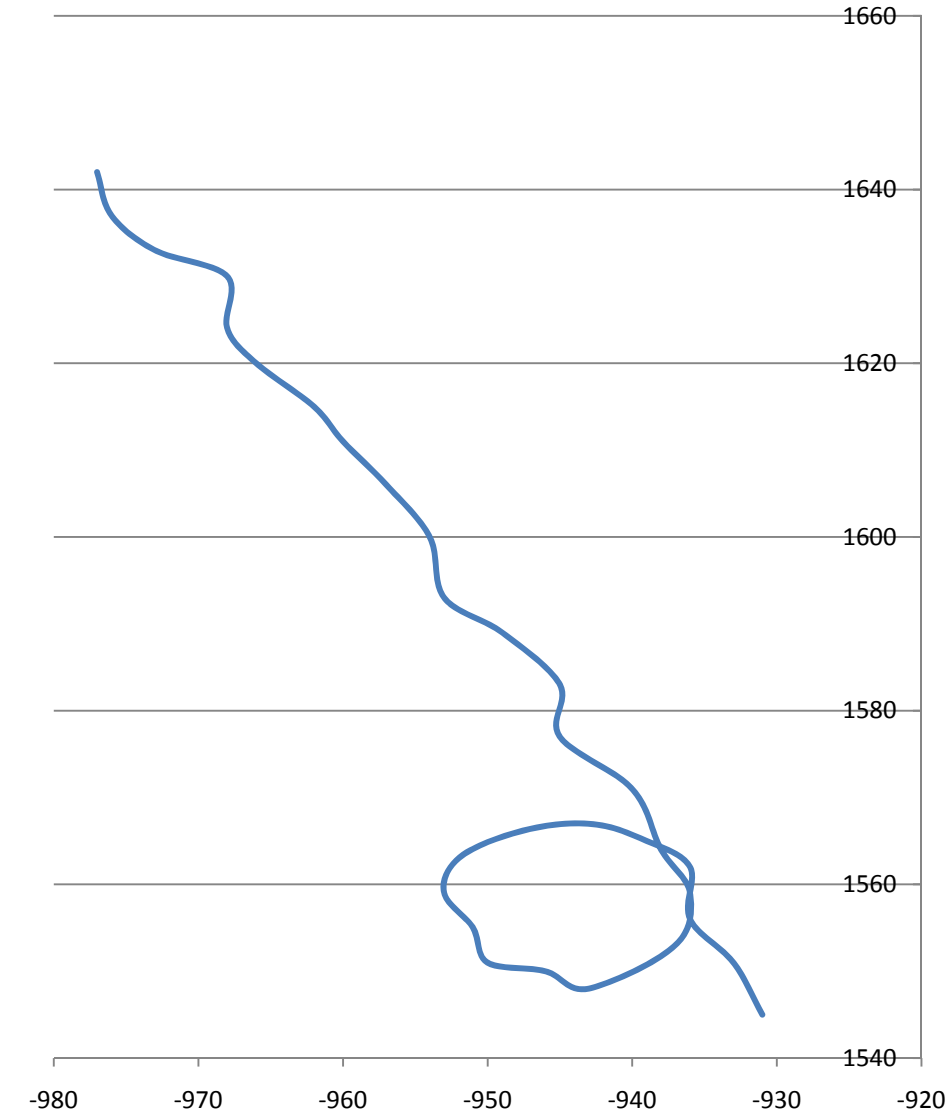
- Header
  - SYN SYN SYN (EBCDIC)
- Character-oriented encoding:
  - SOH
  - STX
  - ETX
  - CRC (CCITT-16)
- Numbers of fixed-length messages
  - Each contains an ID

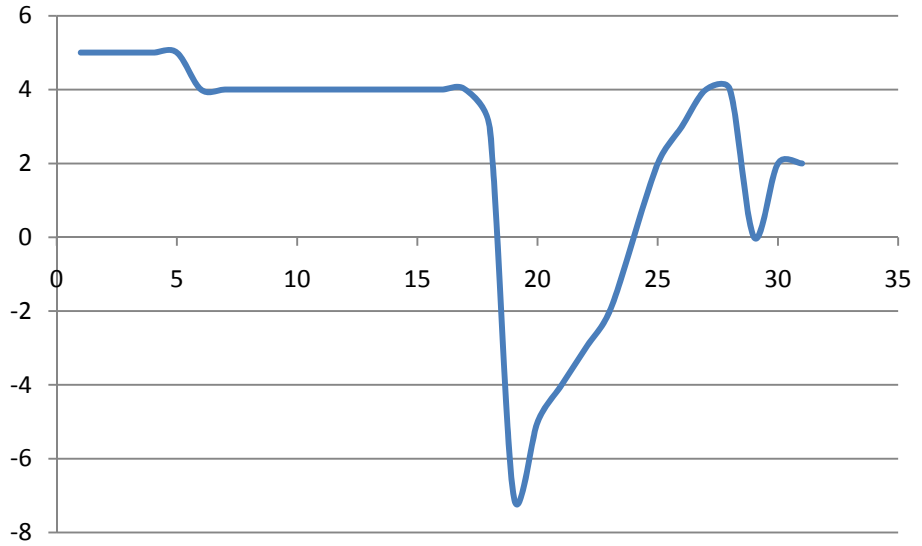


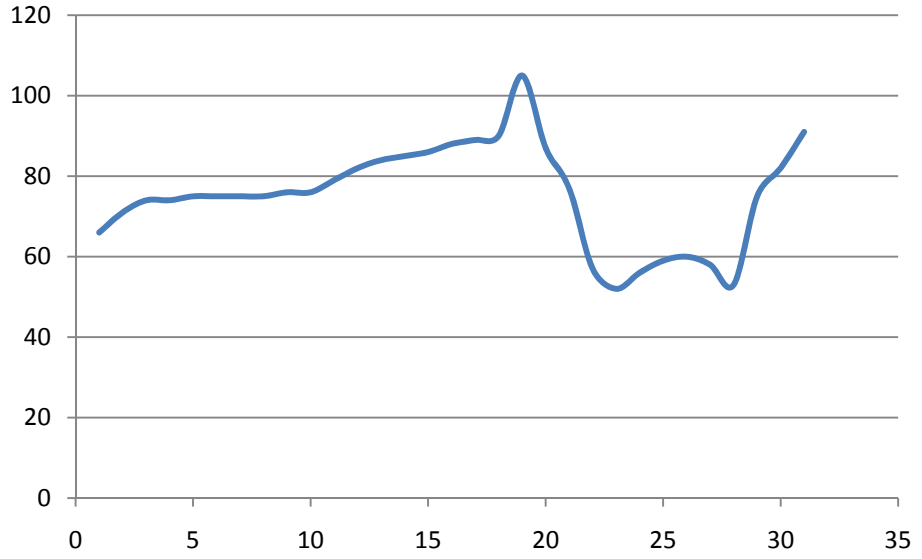
Un-pack & find patterns



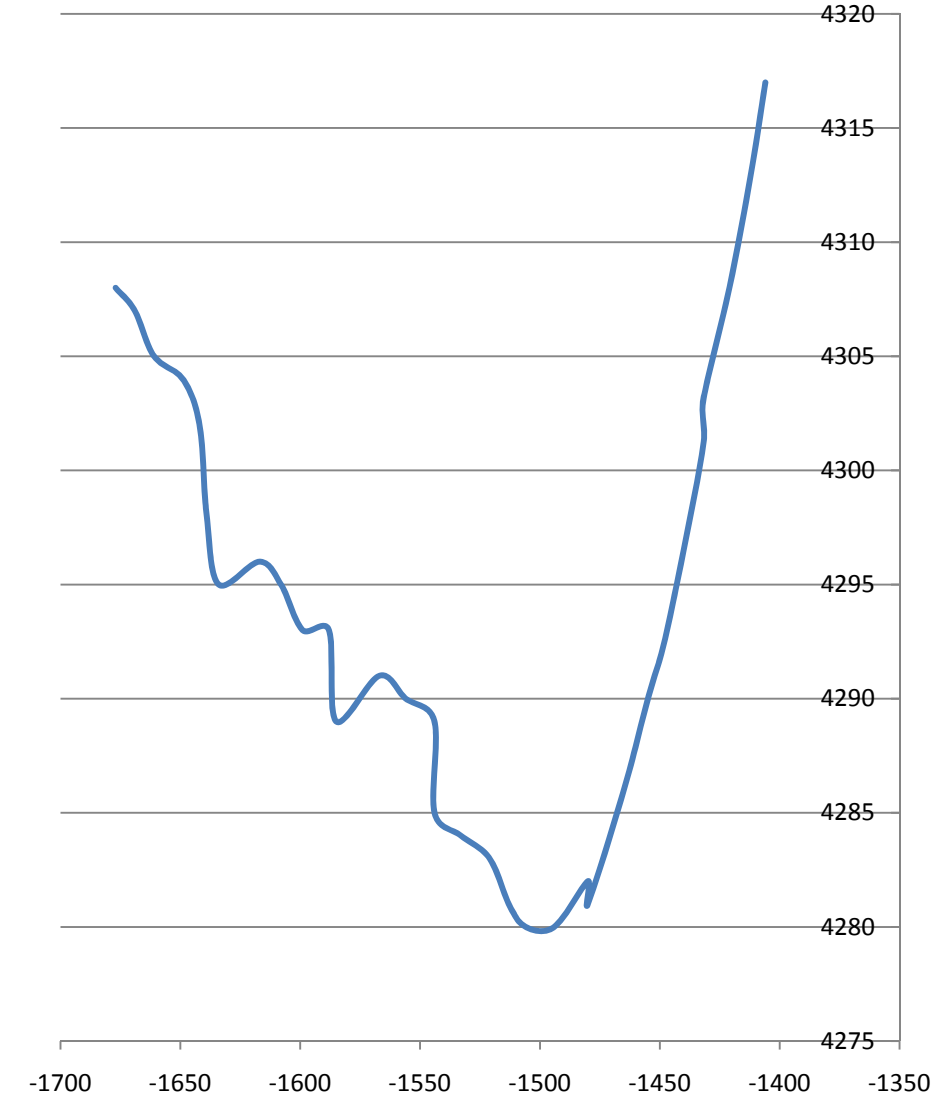
Graphing the Data

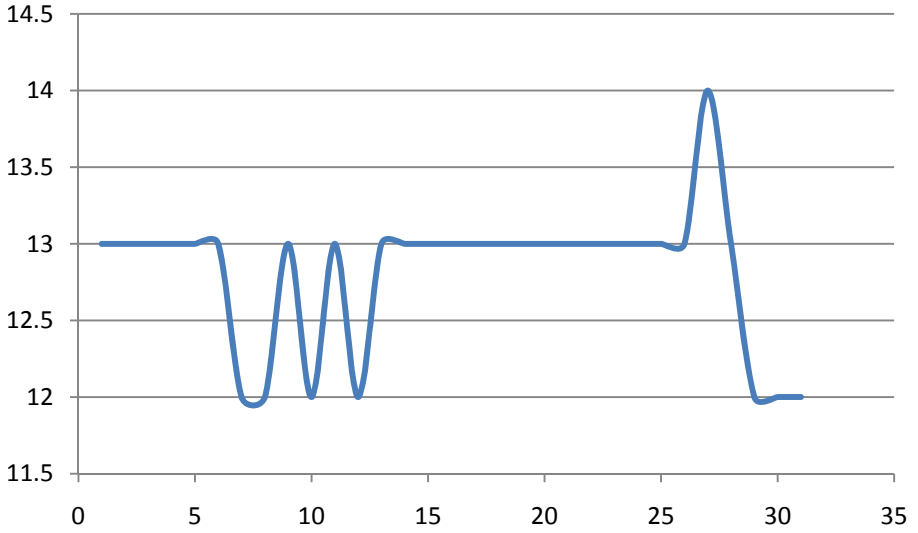


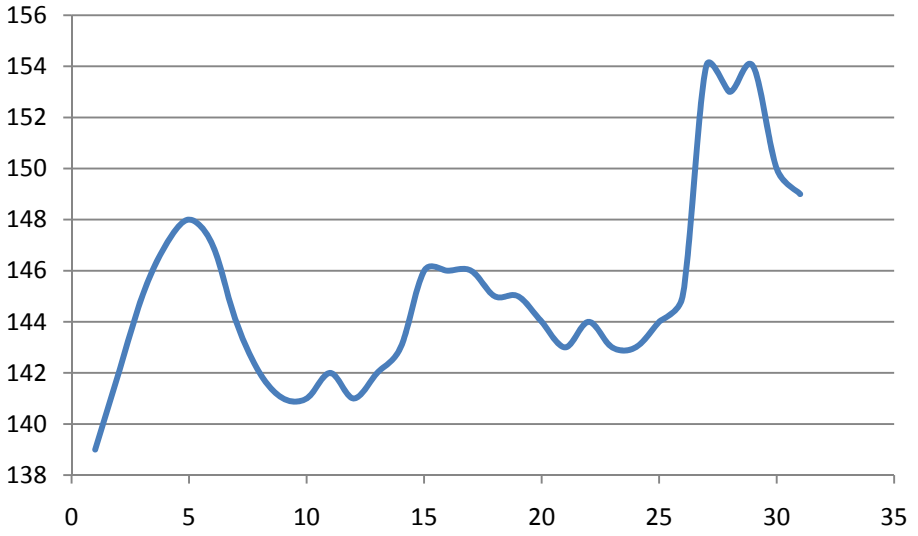


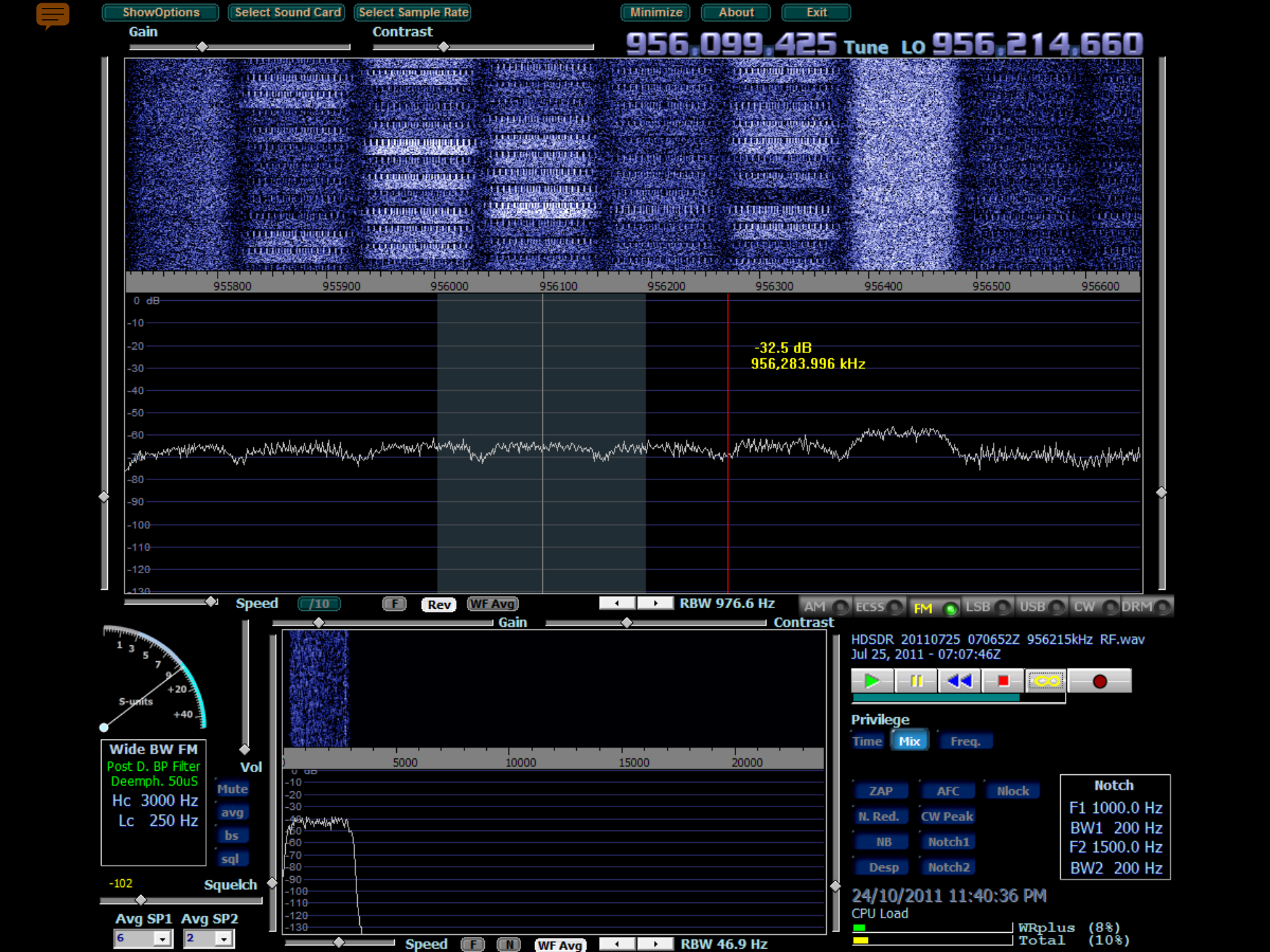


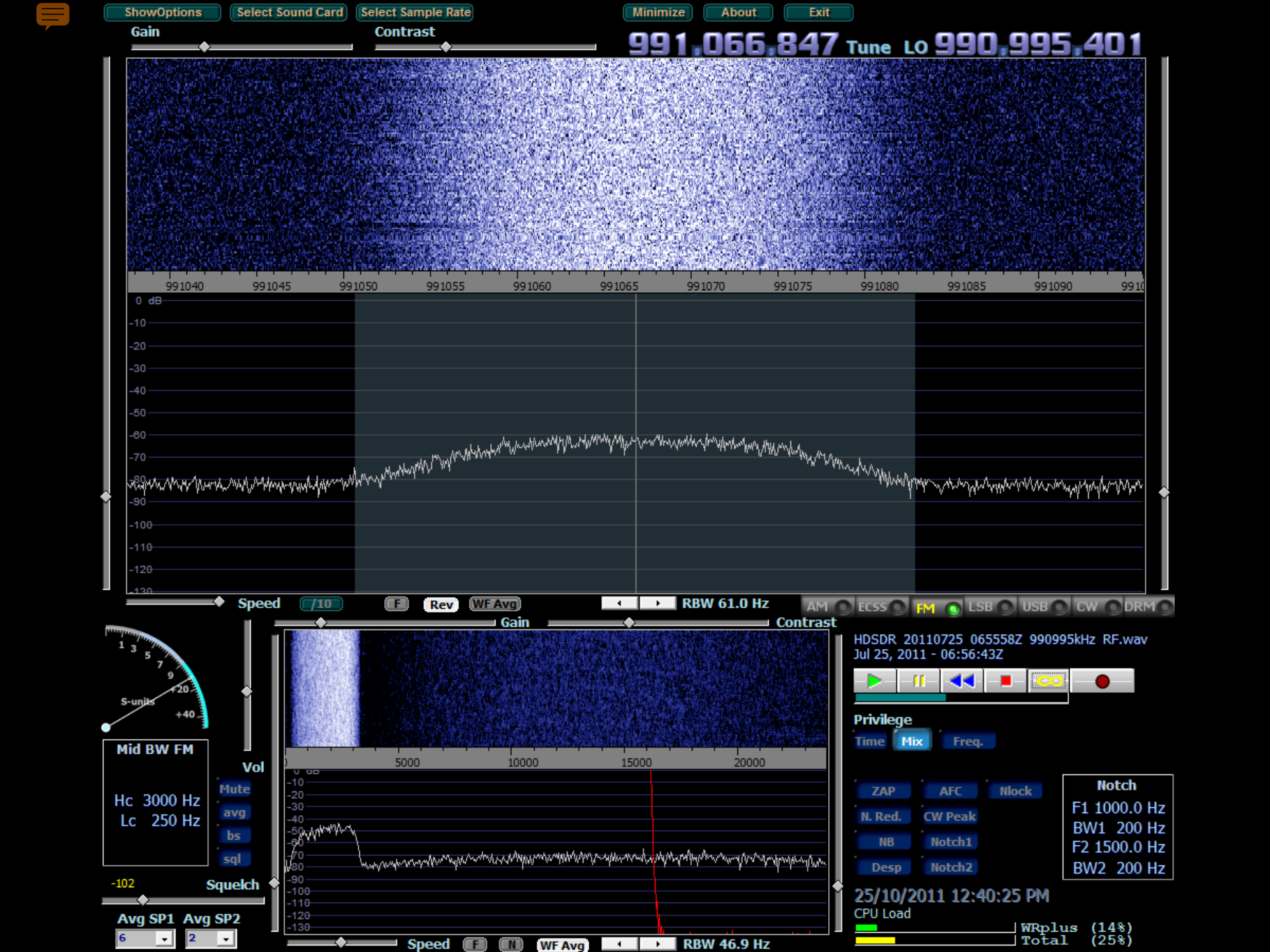
Graphing the Data



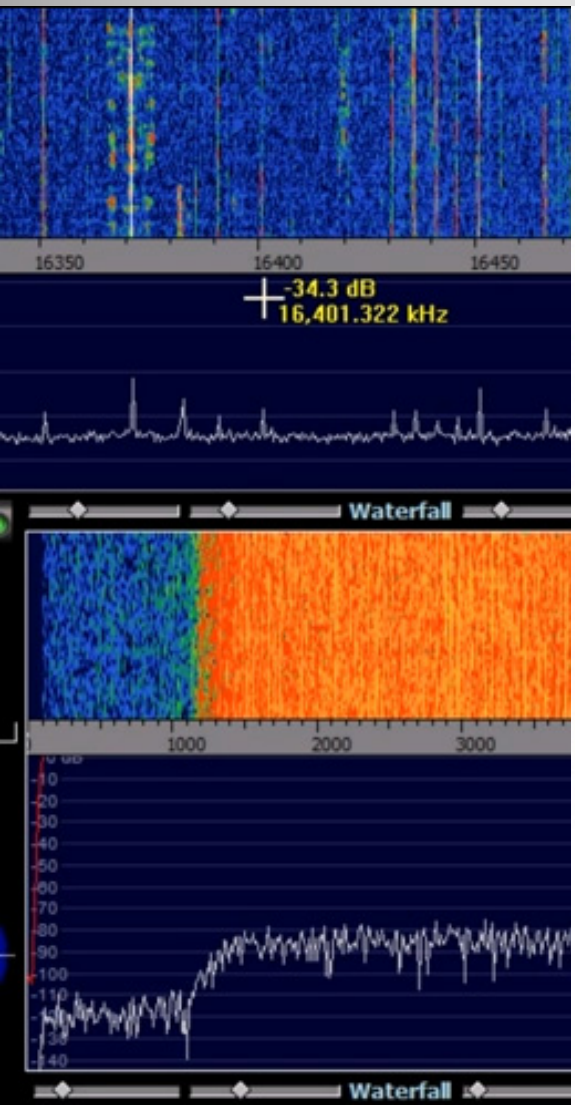





ShowOptions
Select Sound Card
Select Sample Rate
Minimize
About
Exit
Gain
Contrast
956.099.425 Tune LO 956.214.660
955800
955900
956000
956100
956200
956300
956400
956500
956600
0 dB
-10
-20
-30
-40
-50
-60
-70
-80
-90
-100
-110
-120
-130
-32.5 dB
956,283.996 kHz
Speed
/10
F
Rev
WF Avg
RBW 976.6 Hz
AM
ECSS
FM
LSB
USB
CW
DRM
S-units
1
3
5
7
9
+20
+40
Wide BW FM
Post D. BP Filter
Deemph. 50uS
Hc 3000 Hz
Lc 250 Hz
Vol
Mute
avg
bs
sql
-102
Squelch
Avg SP1
Avg SP2
6
2
Gain
Contrast
5000
10000
15000
20000
Speed
F
N
WF Avg
RBW 46.9 Hz
HDSDR 20110725 070652Z 956215kHz RF.wav
Jul 25, 2011 - 07:07:46Z
Privilege
Time
Mix
Freq.
ZAP
AFC
Nlock
N. Red.
CW Peak
NB
Notch1
Desp
Notch2
Notch
F1 1000.0 Hz
BW1 200 Hz
F2 1500.0 Hz
BW2 200 Hz
24/10/2011 11:40:36 PM
CPU Load
WRplus (8%)
Total (10%)


ShowOptions
Select Sound Card
Select Sample Rate
Minimize
About
Exit
Gain
Contrast
991,066,847 Tune LO 990,995,401
991040
991045
991050
991055
991060
991065
991070
991075
991080
991085
991090
0 dB
-10
-20
-30
-40
-50
-60
-70
-80
-90
-100
-110
-120
Speed
/10
F
Rev
WF Avg
RBW 61.0 Hz
AM
ECSS
FM
LSB
USB
CW
DRM
Gain
Contrast
5000
10000
15000
20000
Speed
F
N
WF Avg
RBW 46.9 Hz
S-units
Mid BW FM
Hc 3000 Hz
Lc 250 Hz
Vol
Mute
avg
bs
sql
-102
Squelch
Avg SP1
Avg SP2
HDSDR 20110725 065558Z 990995kHz RF.wav
Jul 25, 2011 - 06:56:43Z
Privilege
Time
Mix
Freq.
ZAP
AFC
Nlock
N. Red.
CW Peak
NB
Notch1
Desp
Notch2
Notch
F1 1000.0 Hz
BW1 200 Hz
F2 1500.0 Hz
BW2 200 Hz
25/10/2011 12:40:25 PM
CPU Load
WRplus (14%)
Total (25%)

STANAG 4285



STANAG-4285

STANAG-4285 is specified by the NATO (North Atlantic Treaty Organization) Military Agency for Standardization in "Characteristics of 1200 / 2400 / 3600 Bits per Second Single Tone Modulators / Demodulators for HF Radio Links" (16. February 1989).

Parameter	Value
Frequency range	HF
Operation modes	Broadcast/Simplex FEC
Modulation	8-PSK
Center frequency	1800 Hz
Symbol rate	2400 Bd
Receiver settings	DATA, CW, LSB or USB
Input format(s)	AF, IF

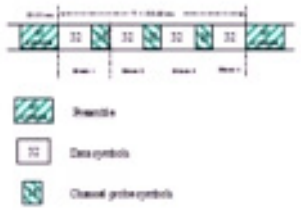
The modulation technique used in this mode consists of phase shift keying (8-PSK) of a single tone sub-carrier of 1800 Hz. The modulation speed (symbol rate) is always 2400 Bd.

Using different M-PSK modulations and FEC (Forward Error Correction) coding rates, serial binary user information (raw data) accepted at the line side input can be transmitted at different user data rates.

STANAG 4285 single tone waveform has the following characteristics which may be selected from **Options |Frame Format...**:

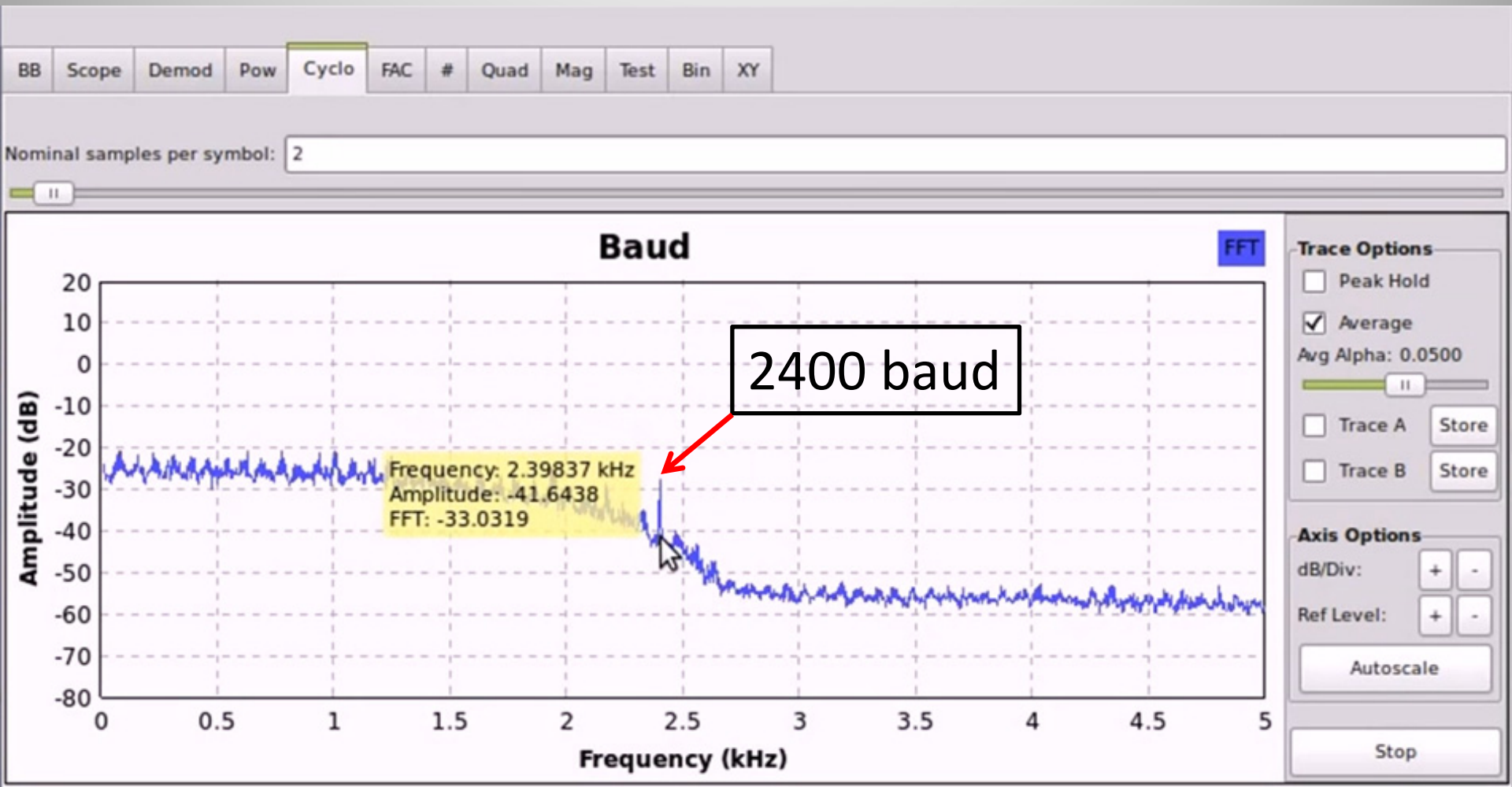
Baud Rate	User data rate (bps)	User data rate (bps)	FEC coding rate	Interleaver	No. of unknown 8-phase symbols (User Data)	No. of known 8-phase symbols (Channel Probe)
2400	2400	3 (8-PSK)	2 / 3	SHORT or LONG	32	16
2400	1200	2 (QPSK)	1 / 2	SHORT or LONG	32	16
2400	600	1 (BPSK)	1 / 2	SHORT or LONG	32	16
2400	300	1 (BPSK)	1 / 4	SHORT or LONG	32	16
2400	150	1 (BPSK)	1 / 8	SHORT or LONG	32	16
2400	75	1 (BPSK)	1 / 16	SHORT or LONG	32	16
2400	3600	3 (8-PSK)	No coding	ZERO	32	16
2400	2400	2 (QPSK)	No coding	ZERO	32	16
2400	1200	1 (BPSK)	No coding	ZERO	32	16

The user data is transmitted using a continuous frame structure. Each frame begins with a 33.33 ms preamble containing 80 symbols, the next 176 symbols are divided into four 32-symbol data segments and three 16-symbol channel probe segments.



At the end of transmission, a certain bit-pattern (in hexadecimal notation, 4B65A5B2, MSB first) is sent to mark the end of message (EOM). The

STANAG 4285


BB
Scope
Demod
Pow
Cyclo
FAC
#
Quad
Mag
Test
Bin
XY
Nominal samples per symbol:
2
Baud
FFT
2400 baud
Frequency: 2.39837 kHz
Amplitude: -41.6438
FFT: -33.0319
Amplitude (dB)
Frequency (kHz)
Trace Options
Peak Hold
Average
Avg Alpha: 0.0500
Trace A
Store
Trace B
Store
Axis Options
dB/Div:
Ref Level:
Autoscale
Stop

80 (preamble) +
4 x 32 (data) +
3 x 16 (channel probe)
@ 2400 bps
= **106.66 ms**

Fine Offset: 0

Coarse offset: 0

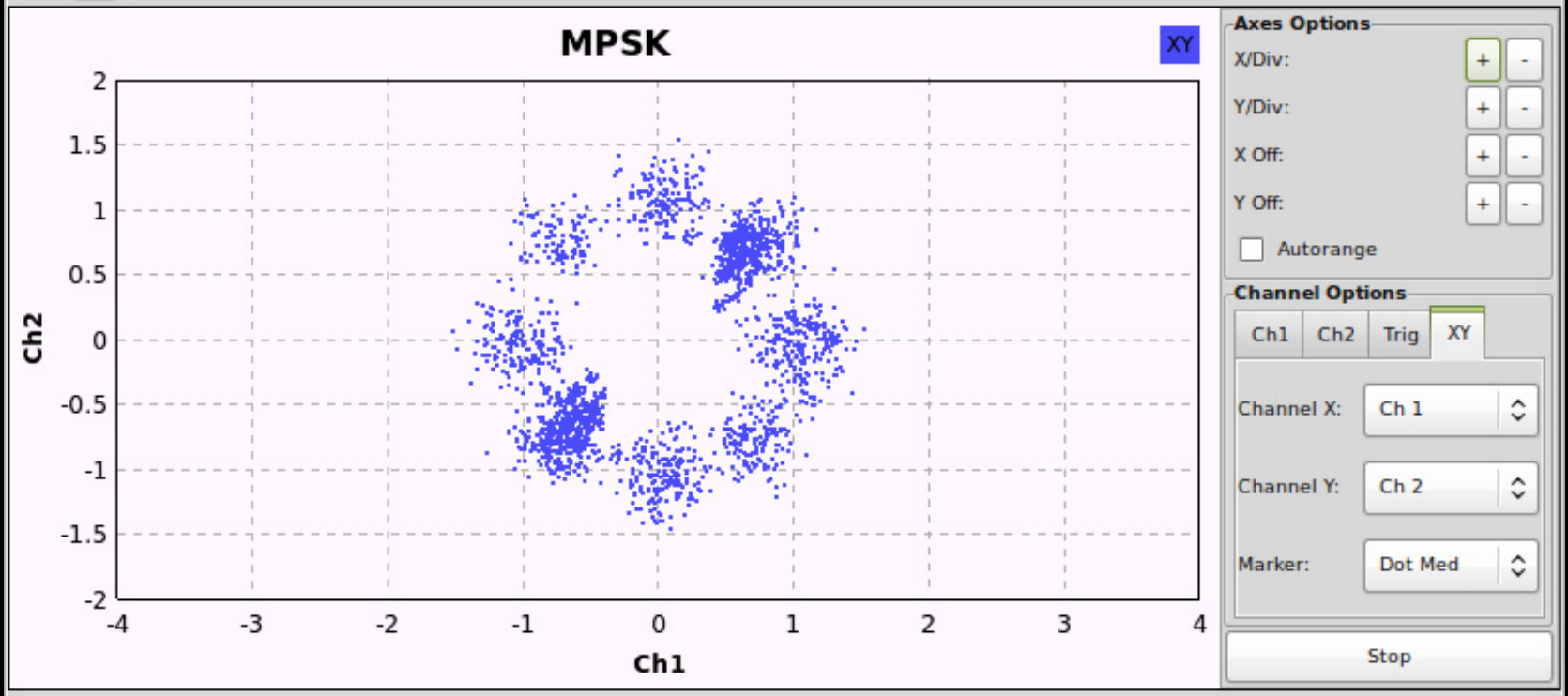
Xlate Offset: -306.325k

Xlate BW: 5k

BB | Demod | Xtra | Eye | Histo | FEC | PSK | FAC

Gain Mu: 10.481m

Alpha: 20.96m



Axes Options

X/Div: + -

Y/Div: + -

X Off: + -

Y Off: + -

Autorange

Channel Options

Ch1 | Ch2 | Trig | XY

Channel X: Ch 1

Channel Y: Ch 2

Marker: Dot Med

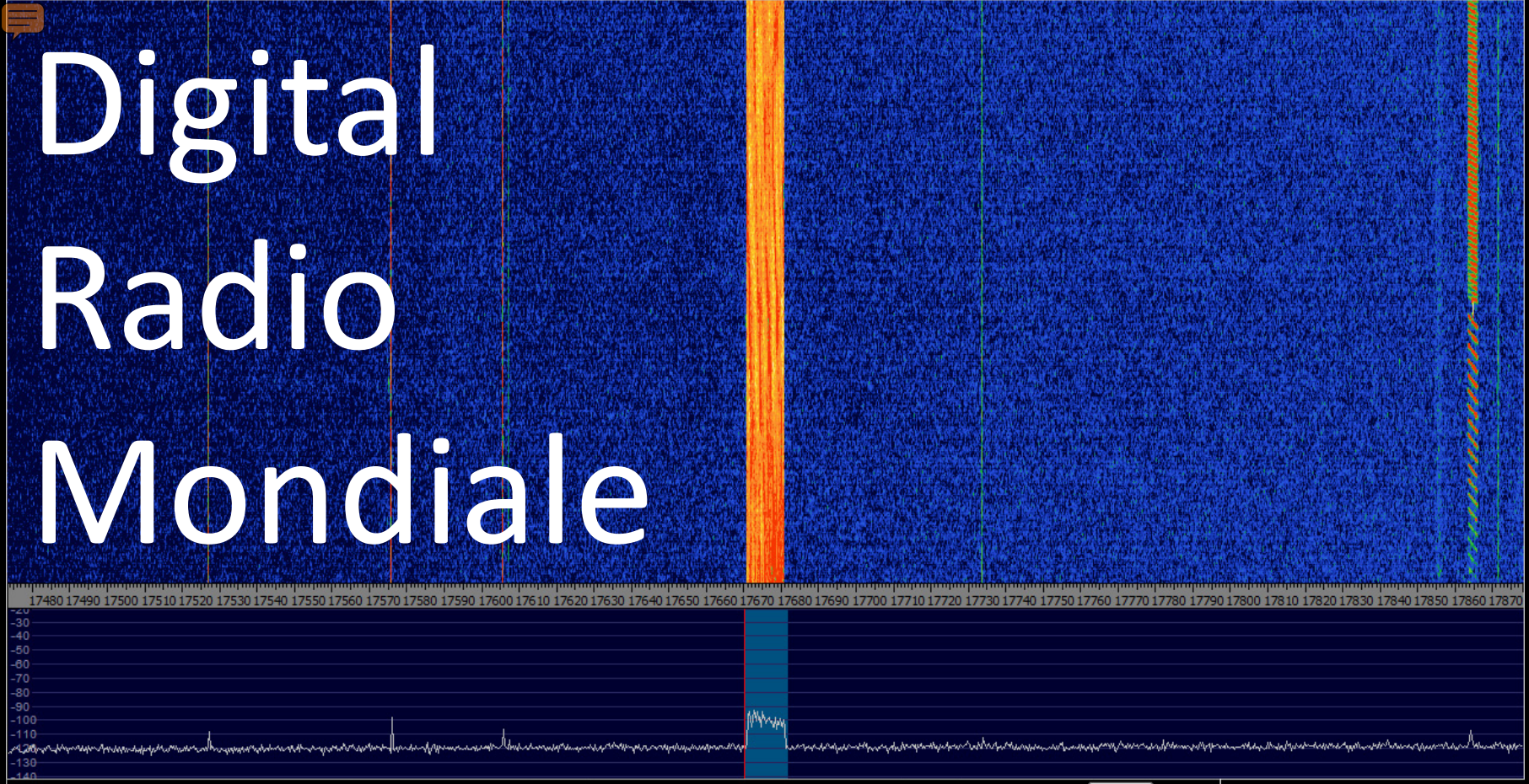
Stop

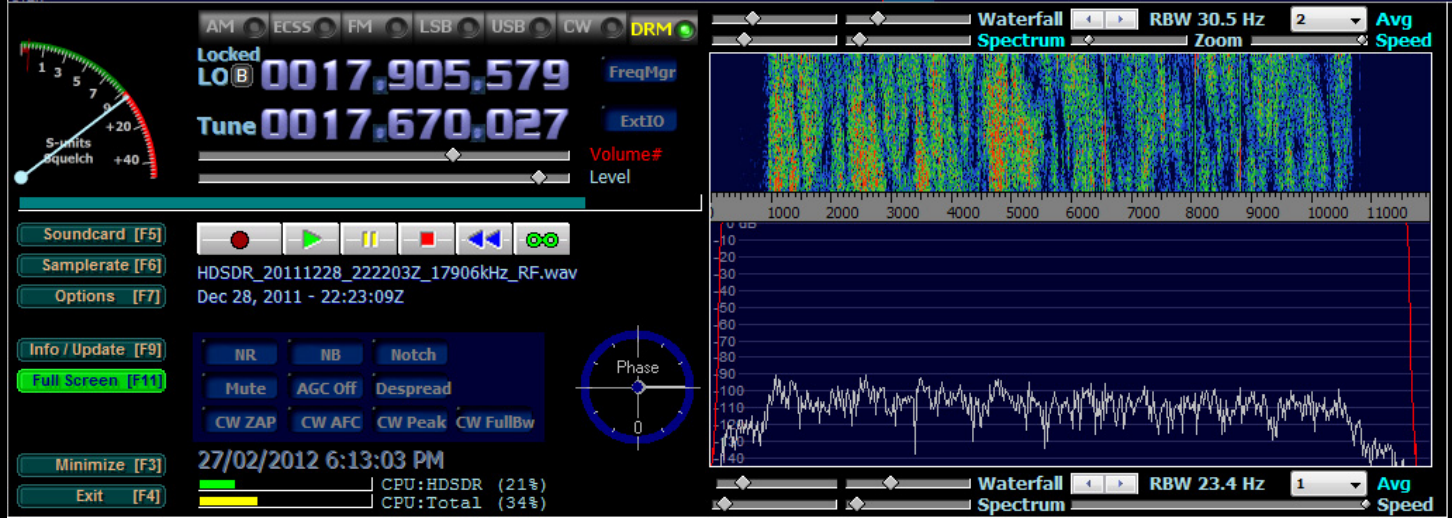
Fine Offset: 0

Xlate Offset: -306.325k

Xlate BW: 5k

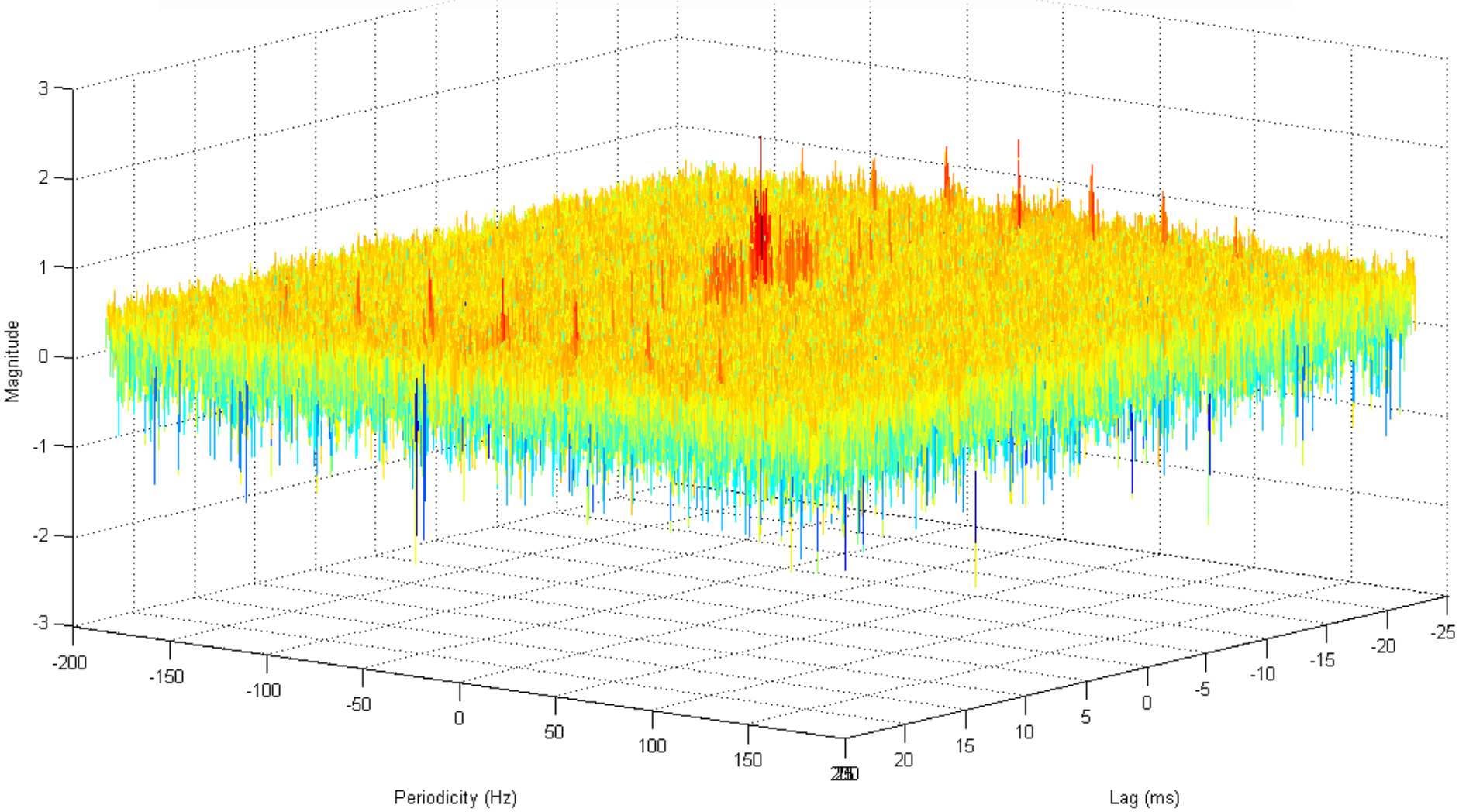
Digital Radio Mondiale



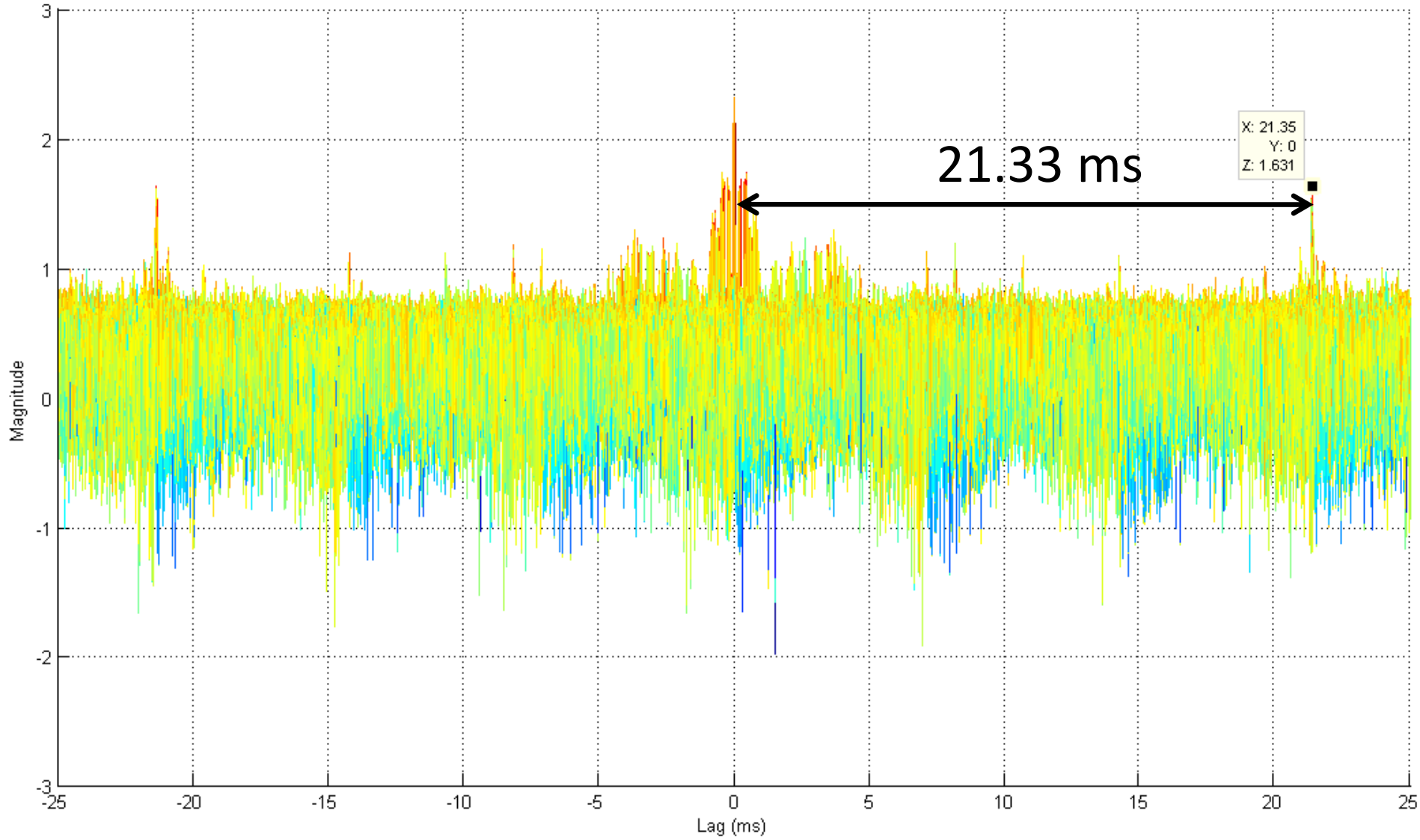


Cyclic Autocorrelation Function

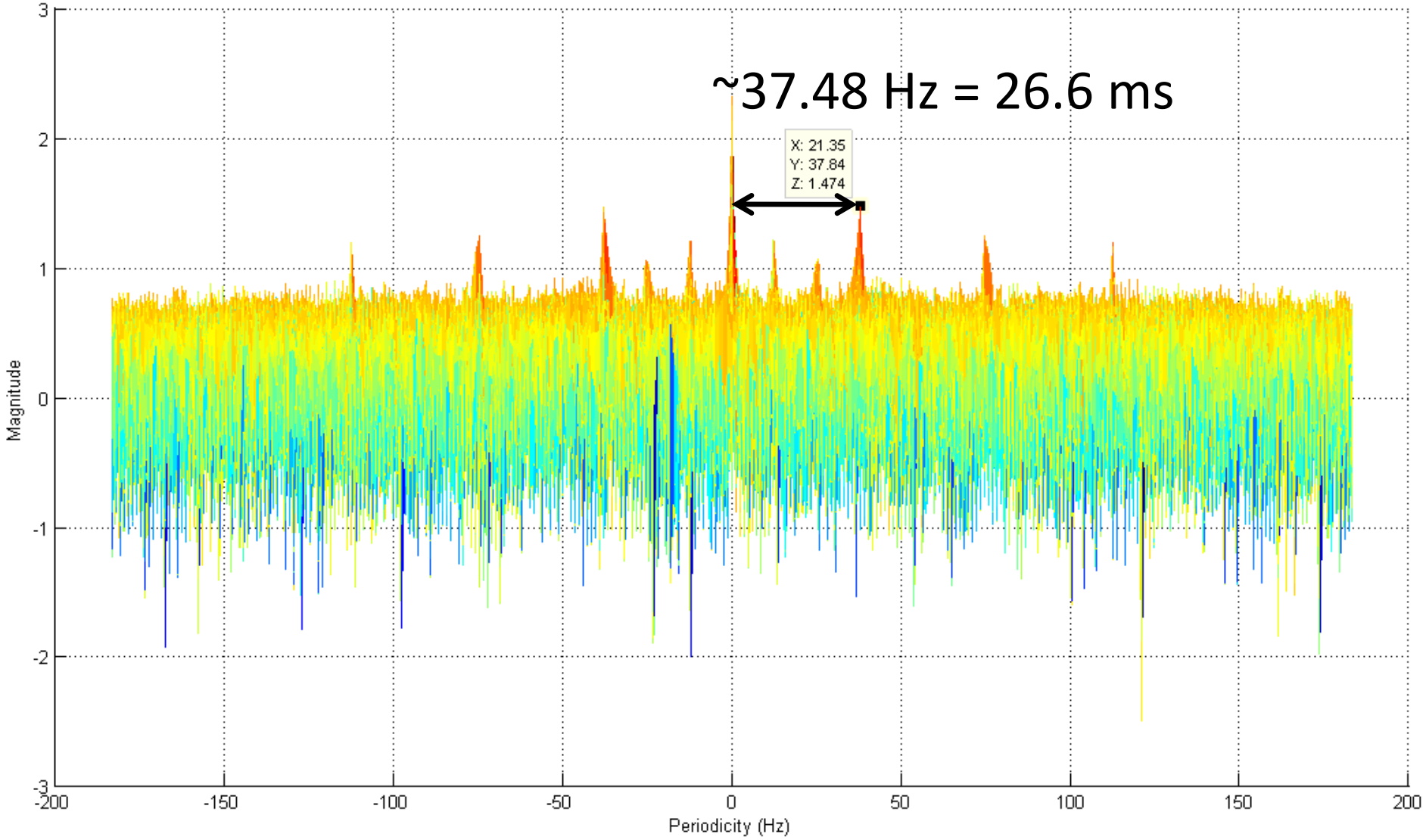
Han, Sohn & Moung,"A Blind OFDM Detection and Identification Method Based on Cyclostationarity for Cognitive Radio Application"



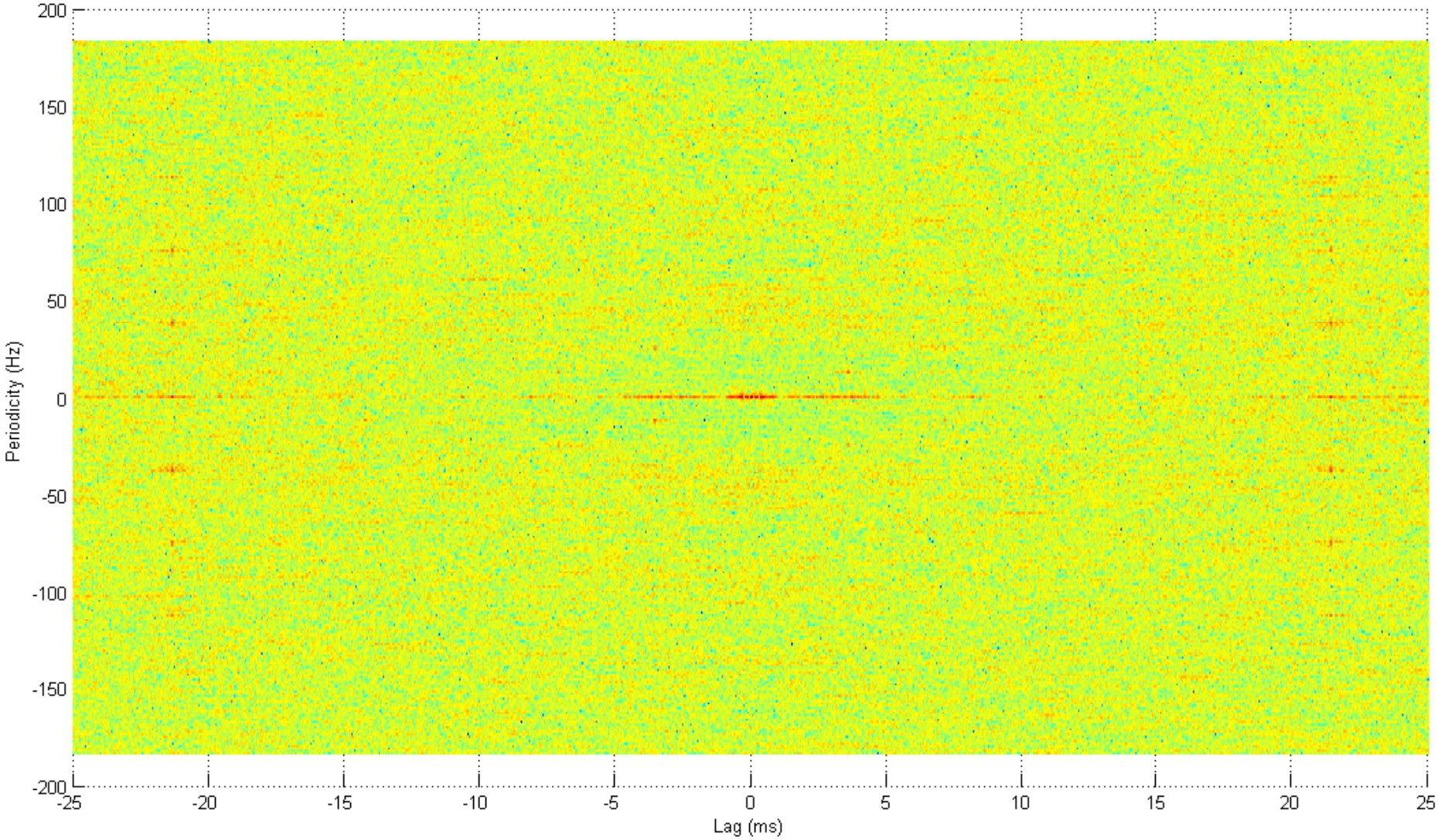
Un-guarded Symbol Time

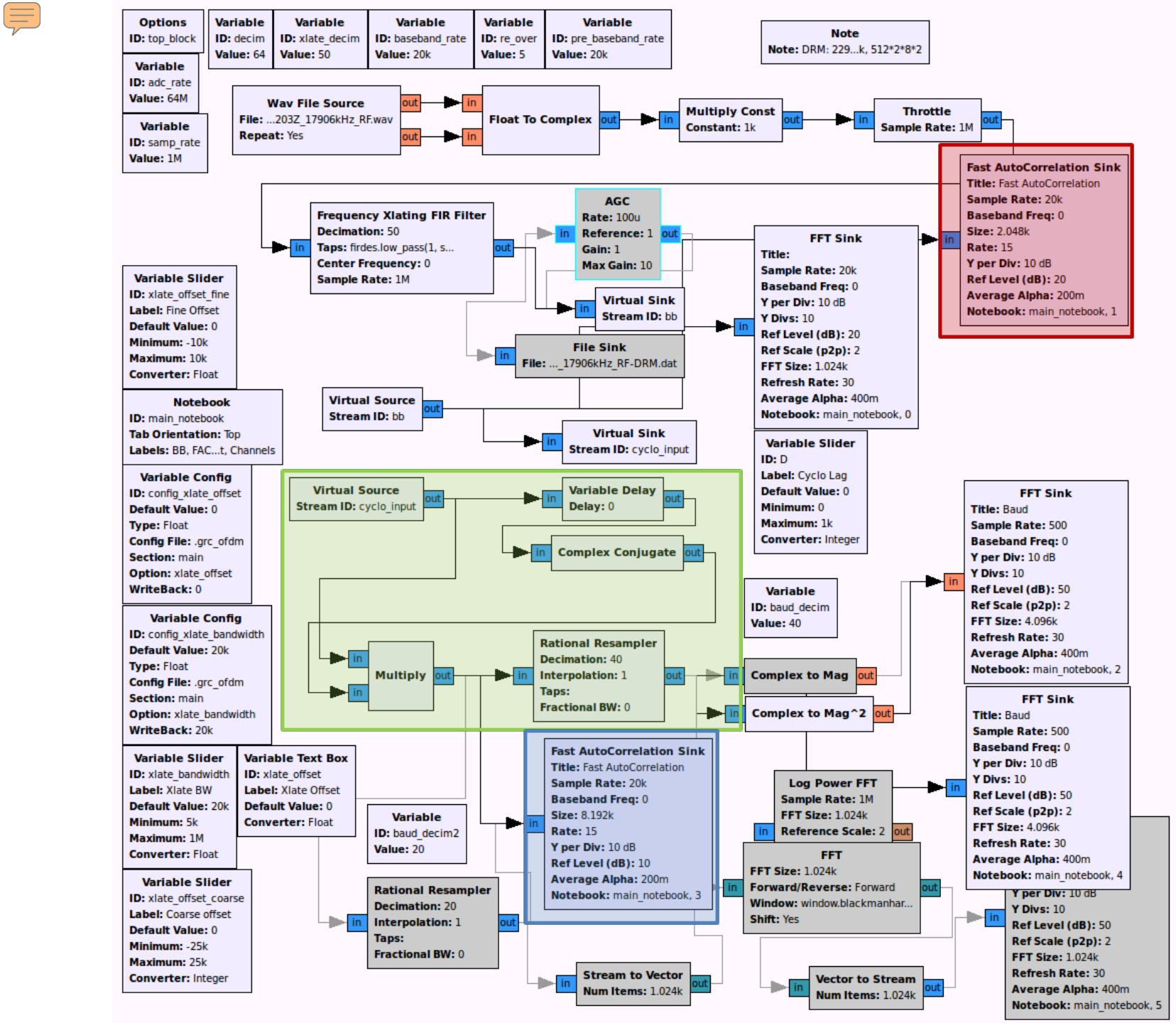


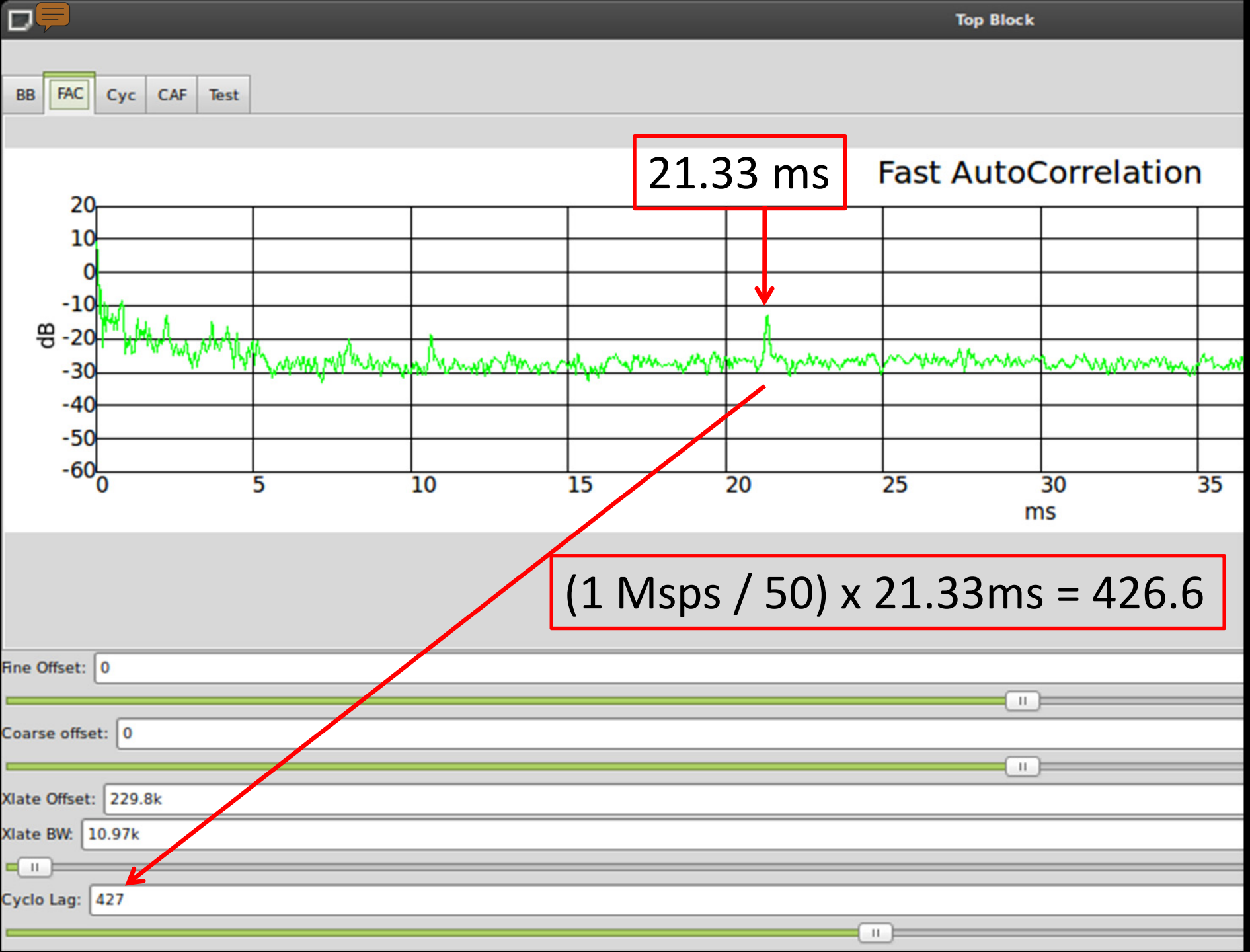
Total Symbol Duration



Top-down DRM Symmetry

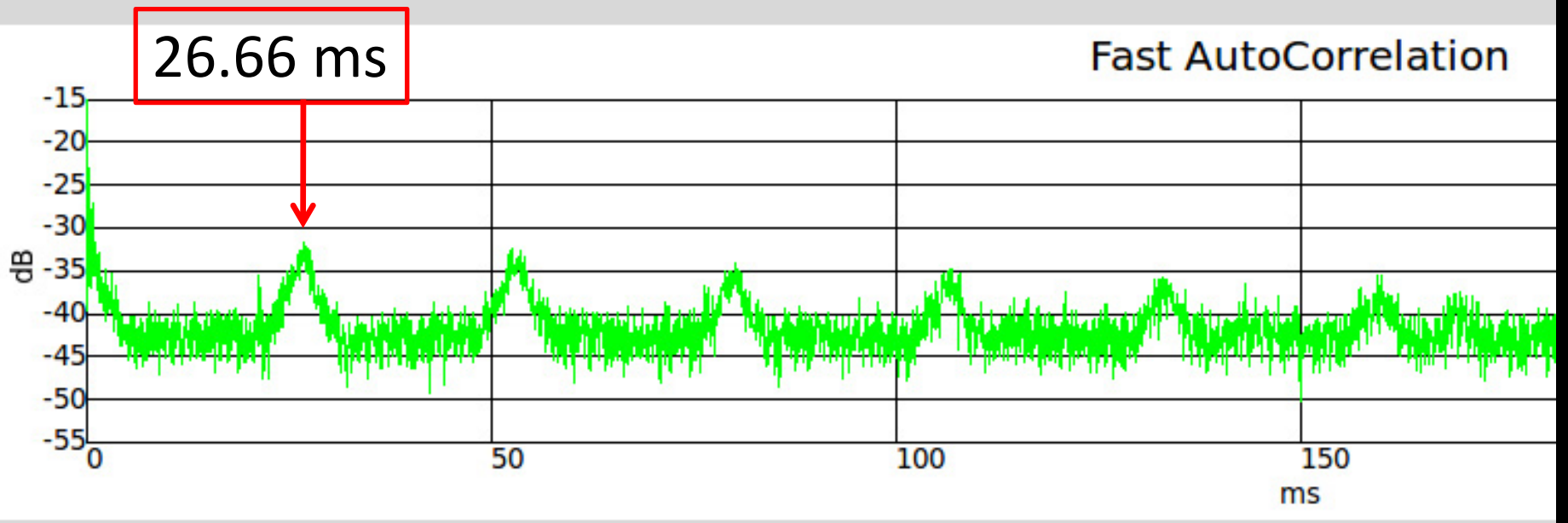



Options
ID: top_block
Variable
ID: decim
Value: 64
Variable
ID: xlate_decim
Value: 50
Variable
ID: baseband_rate
Value: 20k
Variable
ID: re_over
Value: 5
Variable
ID: pre_baseband_rate
Value: 20k
Note
Note: DRM: 229...k, 512*2*8*2
Variable
ID: adc_rate
Value: 64M
Variable
ID: samp_rate
Value: 1M
Wav File Source
File: ...203Z_17906kHz_RF.wav
Repeat: Yes
out
out
in
in
Float To Complex
out
in
Multiply Const
Constant: 1k
out
in
Throttle
Sample Rate: 1M
out
Fast AutoCorrelation Sink
Title: Fast AutoCorrelation
Sample Rate: 20k
Baseband Freq: 0
Size: 2.048k
Rate: 15
Y per Div: 10 dB
Ref Level (dB): 20
Average Alpha: 200m
Notebook: main_notebook, 1
Frequency Xlating FIR Filter
Decimation: 50
Taps: firdes.low_pass(1, s...
Center Frequency: 0
Sample Rate: 1M
AGC
Rate: 100u
Reference: 1
Gain: 1
Max Gain: 10
Virtual Sink
Stream ID: bb
File Sink
File: ..._17906kHz_RF-DRM.dat
FFT Sink
Title:
Sample Rate: 20k
Baseband Freq: 0
Y per Div: 10 dB
Y Divs: 10
Ref Level (dB): 20
Ref Scale (p2p): 2
FFT Size: 1.024k
Refresh Rate: 30
Average Alpha: 400m
Notebook: main_notebook, 0
Variable Slider
ID: xlate_offset_fine
Label: Fine Offset
Default Value: 0
Minimum: -10k
Maximum: 10k
Converter: Float
Notebook
ID: main_notebook
Tab Orientation: Top
Labels: BB, FAC...t, Channels
Virtual Source
Stream ID: bb
Virtual Sink
Stream ID: cyclo_input
Variable Slider
ID: D
Label: Cyclo Lag
Default Value: 0
Minimum: 0
Maximum: 1k
Converter: Integer
Variable Config
ID: config_xlate_offset
Default Value: 0
Type: Float
Config File: .grc_ofdm
Section: main
Option: xlate_offset
WriteBack: 0
Virtual Source
Stream ID: cyclo_input
Variable Delay
Delay: 0
Complex Conjugate
Variable
ID: baud_decim
Value: 40
FFT Sink
Title: Baud
Sample Rate: 500
Baseband Freq: 0
Y per Div: 10 dB
Y Divs: 10
Ref Level (dB): 50
Ref Scale (p2p): 2
FFT Size: 4.096k
Refresh Rate: 30
Average Alpha: 400m
Notebook: main_notebook, 2
Variable Config
ID: config_xlate_bandwidth
Default Value: 20k
Type: Float
Config File: .grc_ofdm
Section: main
Option: xlate_bandwidth
WriteBack: 20k
Multiply
Rational Resampler
Decimation: 40
Interpolation: 1
Taps:
Fractional BW: 0
Complex to Mag
Complex to Mag^2
Variable Slider
ID: xlate_bandwidth
Label: Xlate BW
Default Value: 20k
Minimum: 5k
Maximum: 1M
Converter: Float
Variable Text Box
ID: xlate_offset
Label: Xlate Offset
Default Value: 0
Converter: Float
Fast AutoCorrelation Sink
Title: Fast AutoCorrelation
Sample Rate: 20k
Baseband Freq: 0
Size: 8.192k
Rate: 15
Y per Div: 10 dB
Ref Level (dB): 10
Average Alpha: 200m
Notebook: main_notebook, 3
Log Power FFT
Sample Rate: 1M
FFT Size: 1.024k
Reference Scale: 2
FFT Sink
Title: Baud
Sample Rate: 500
Baseband Freq: 0
Y per Div: 10 dB
Y Divs: 10
Ref Level (dB): 50
Ref Scale (p2p): 2
FFT Size: 4.096k
Refresh Rate: 30
Average Alpha: 400m
Notebook: main_notebook, 4
Variable
ID: baud_decim2
Value: 20
FFT
FFT Size: 1.024k
Forward/Reverse: Forward
Window: window.blackmanhar...
Shift: Yes
Variable Slider
ID: xlate_offset_coarse
Label: Coarse offset
Default Value: 0
Minimum: -25k
Maximum: 25k
Converter: Integer
Rational Resampler
Decimation: 20
Interpolation: 1
Taps:
Fractional BW: 0
Stream to Vector
Num Items: 1.024k
Vector to Stream
Num Items: 1.024k
Y per Div: 10 dB
Y Divs: 10
Ref Level (dB): 50
Ref Scale (p2p): 2
FFT Size: 1.024k
Refresh Rate: 30
Average Alpha: 400m
Notebook: main_notebook, 5


Top Block
BB
FAC
Cyc
CAF
Test
21.33 ms
Fast AutoCorrelation
dB
20
10
0
-10
-20
-30
-40
-50
-60
0
5
10
15
20
25
30
35
ms
(1 Msps / 50) x 21.33ms = 426.6
Fine Offset:
0
Coarse offset:
0
Xlate Offset:
229.8k
Xlate BW:
10.97k
Cyclo Lag:
427

Top Block

BB | FAC | Cyc | CAF | Test | Channels



Fine Offset: 0

Coarse offset: 0

Xlate Offset: 229.8k

Xlate BW: 10.97k

Cyclo Lag: 427

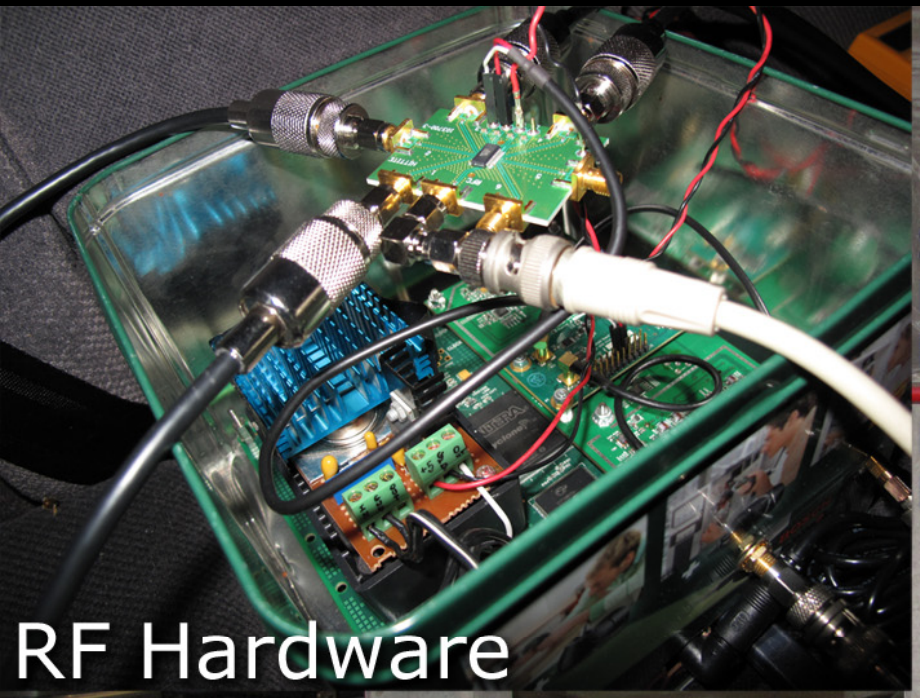
DRM Class B

Modulation property	Value
Un-guarded symbol time	**21.33 ms**
Sub-carrier spacing	46 7/8 Hz
Guard interval	5.33 ms
Total symbol duration	**26.66 ms**
Guard interval ratio	1/4
Symbols per frame	15

1 / (21.33 ms)


Software Defined
Radio Direction Finding

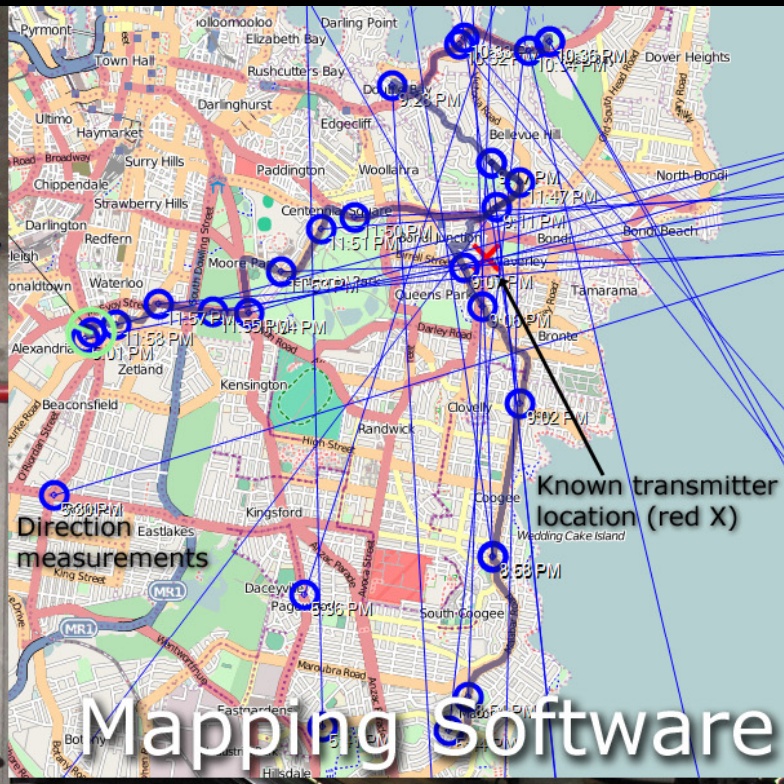
SDR Direction Finding



RF Hardware

Software-Defined Radio

Direction Finding



Mapping Software

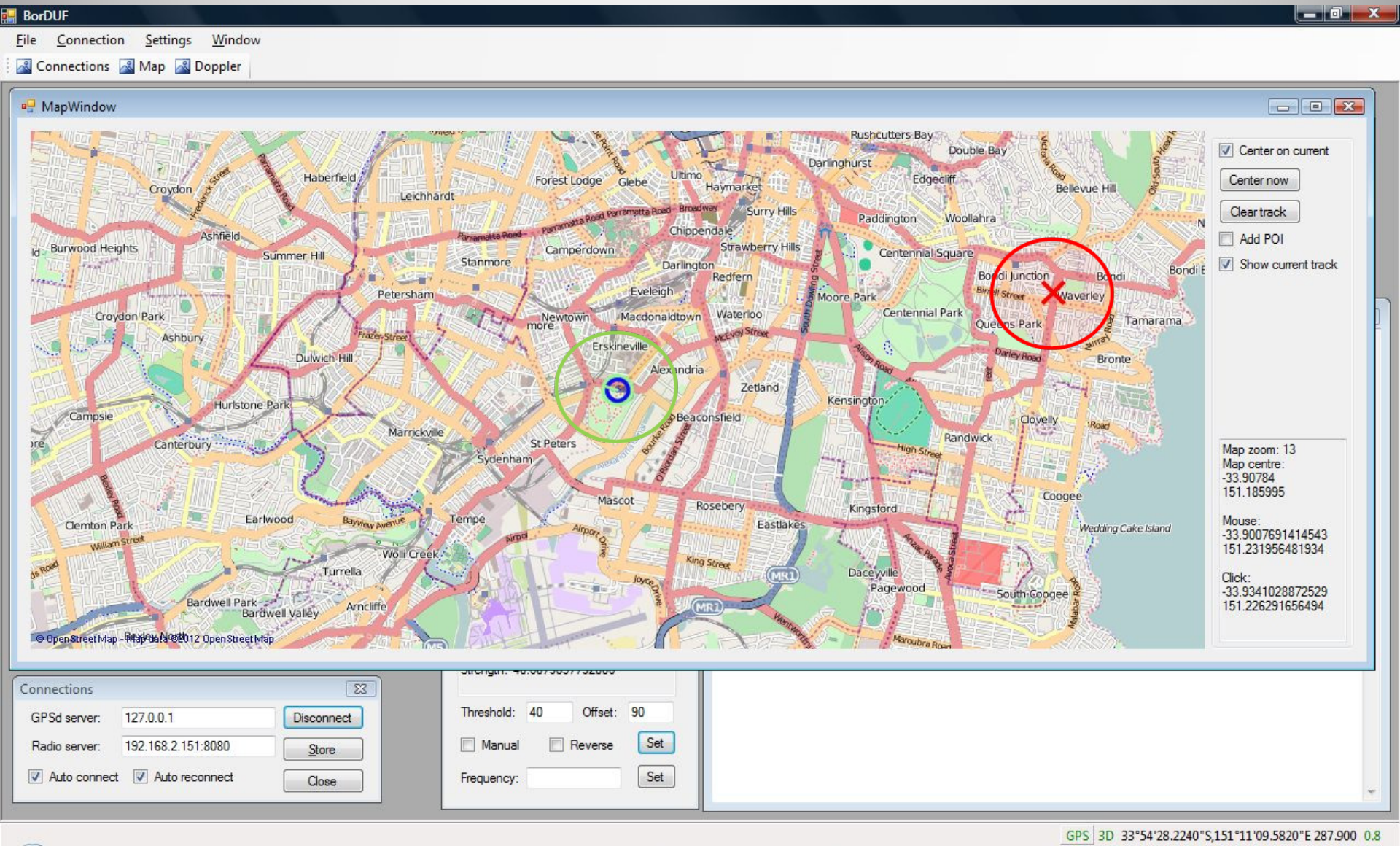
Antenna Array

The DUF-Mobile

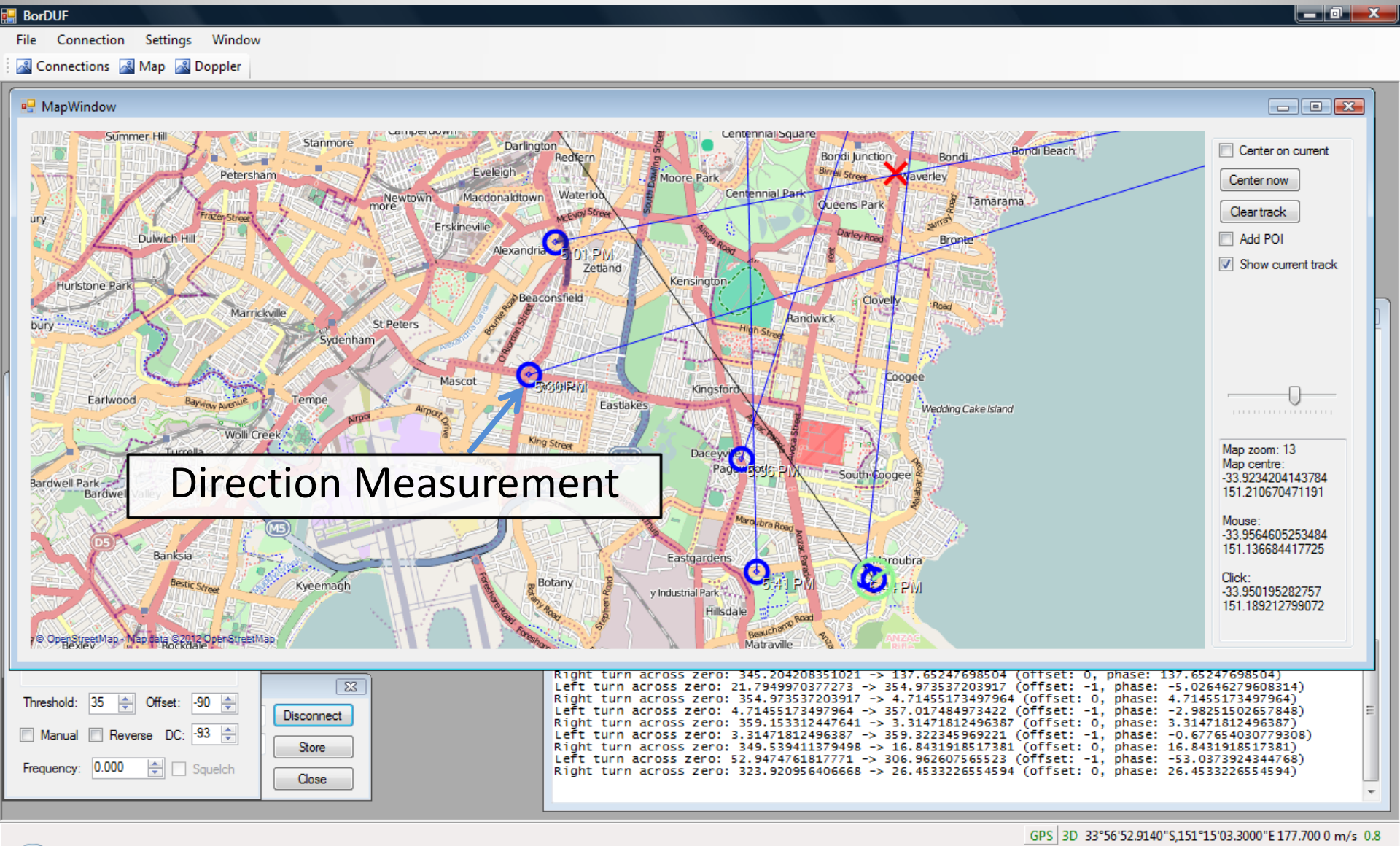
Balint Seeber
http://spench.net/


Antenna
Array

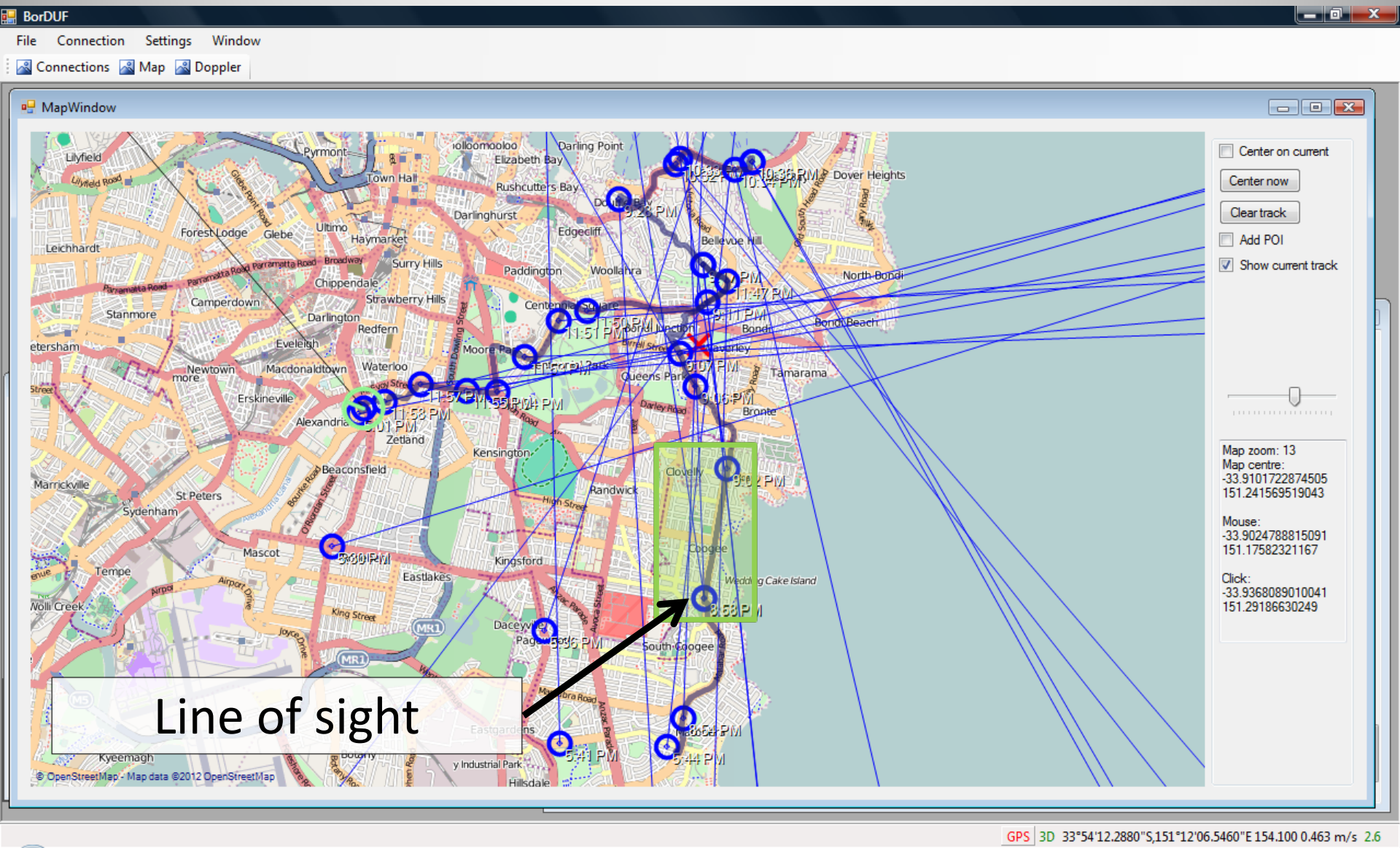
Start


BorDUF
File
Connection
Settings
Window
Connections
Map
Doppler
MapWindow
Center on current
Center now
Clear track
Add POI
Show current track
Map zoom: 13
Map centre:
-33.90784
151.185995
Mouse:
-33.9007691414543
151.231956481934
Click:
-33.9341028872529
151.226291656494
Connections
GPSd server:
127.0.0.1
Disconnect
Radio server:
192.168.2.151:8080
Store
Auto connect
Auto reconnect
Close
Threshold:
40
Offset:
90
Manual
Reverse
Set
Frequency:
Set
GPS
3D
33°54'28.2240"S,151°11'09.5820"E 287.900
0.8

Drive


BorDUF
File
Connection
Settings
Window
Connections
Map
Doppler
MapWindow
Center on current
Center now
Clear track
Add POI
Show current track
Map zoom: 13
Map centre:
-33.9234204143784
151.210670471191
Mouse:
-33.9564605253484
151.136684417725
Click:
-33.950195282757
151.189212799072
Direction Measurement
Threshold: 35
Offset: -90
Manual
Reverse
DC: -93
Frequency: 0.000
Squelch
Disconnect
Store
Close
Right turn across zero: 345.204208351021 -> 137.65247698504 (offset: 0, phase: 137.65247698504)
Left turn across zero: 21.7949970377273 -> 354.973537203917 (offset: -1, phase: -5.02646279608314)
Right turn across zero: 354.973537203917 -> 4.71455173497964 (offset: 0, phase: 4.71455173497964)
Left turn across zero: 4.71455173497964 -> 357.017484973422 (offset: -1, phase: -2.98251502657848)
Right turn across zero: 359.153312447641 -> 3.31471812496387 (offset: 0, phase: 3.31471812496387)
Left turn across zero: 3.31471812496387 -> 359.322345969221 (offset: -1, phase: -0.677654030779308)
Right turn across zero: 349.539411379498 -> 16.8431918517381 (offset: 0, phase: 16.8431918517381)
Left turn across zero: 52.9474761817771 -> 306.962607565523 (offset: -1, phase: -53.0373924344768)
Right turn across zero: 323.920956406668 -> 26.4533226554594 (offset: 0, phase: 26.4533226554594)
GPS 3D 33°56'52.9140"S,151°15'03.3000"E 177.700 0 m/s 0.8

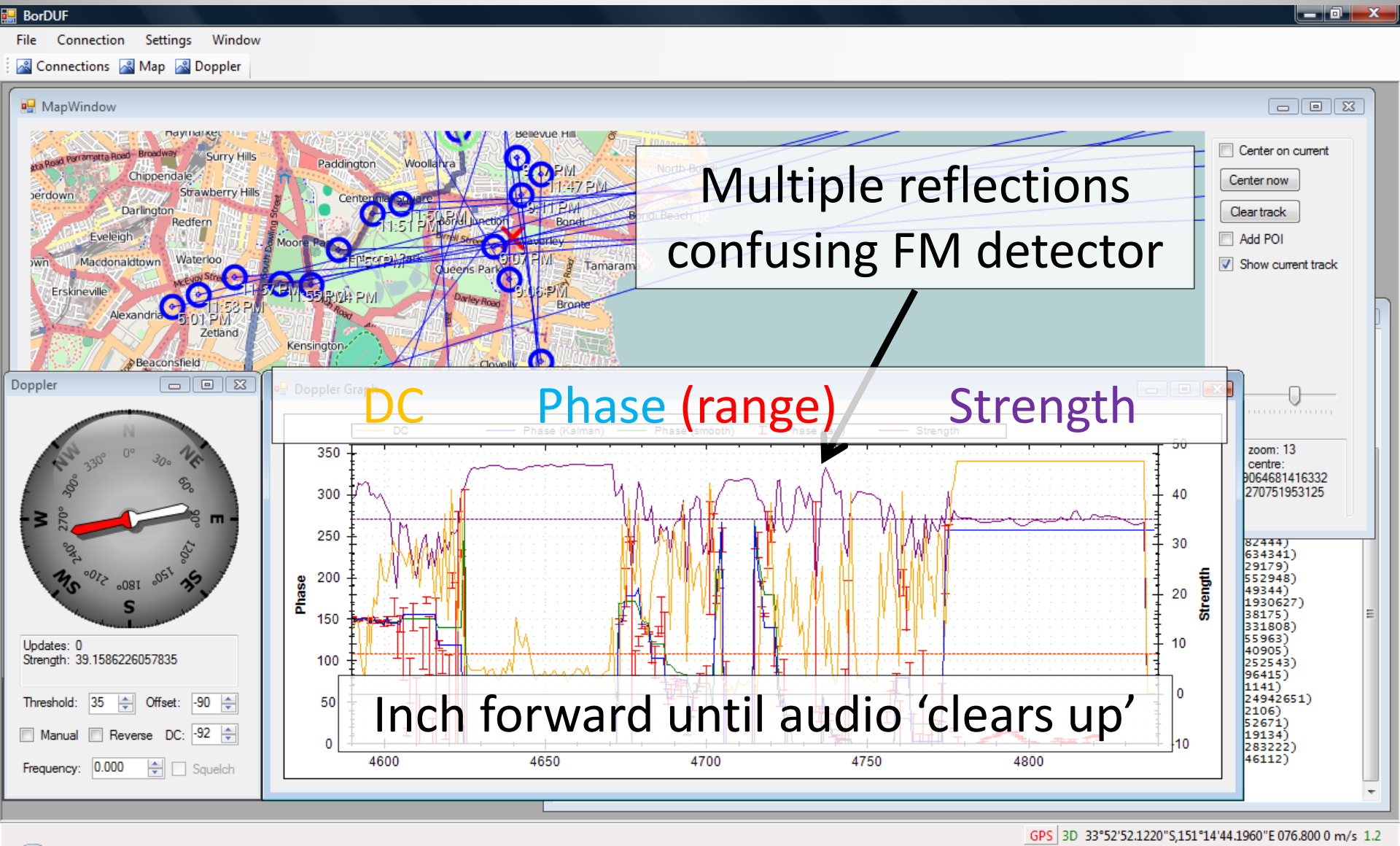
Complications: Coogee



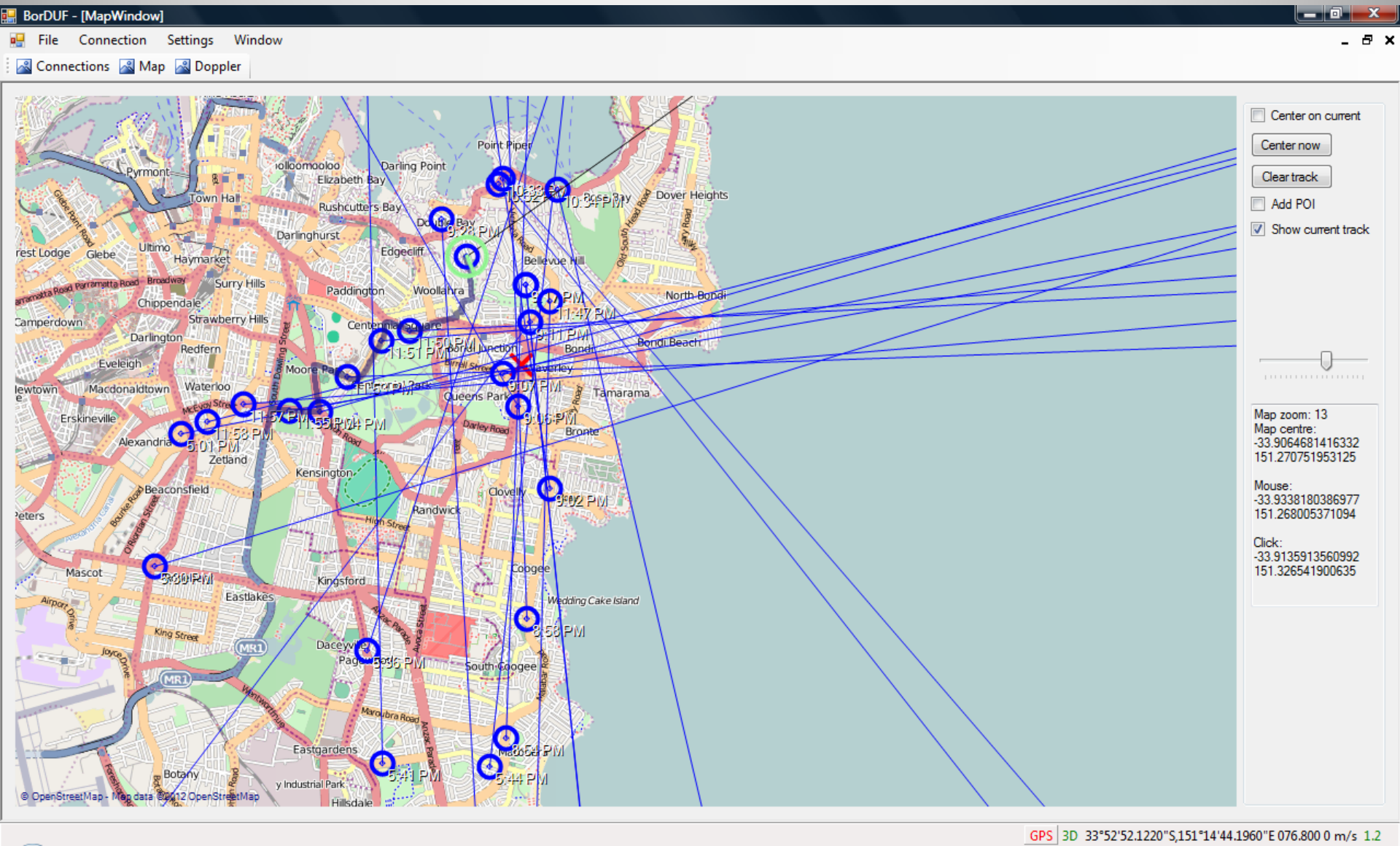
Complications

- Line-Of-Sight
  - Beware of reflections
    - Descending into ‘valley’…

Listen: Multipath



Done

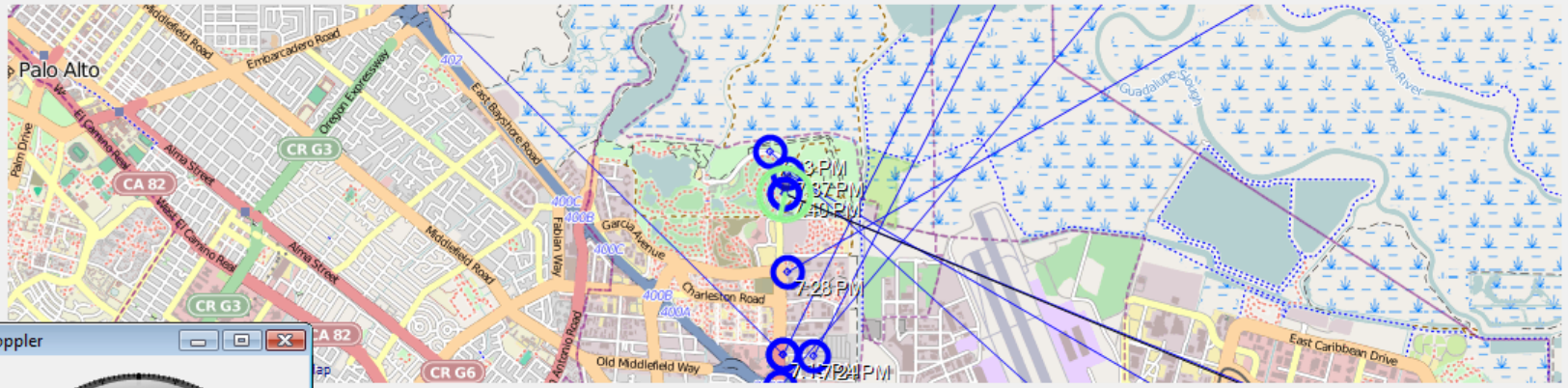

BorDUF - [MapWindow]
File
Connection
Settings
Window
Connections
Map
Doppler
Center on current
Center now
Clear track
Add POI
Show current track
Map zoom: 13
Map centre:
-33.9064681416332
151.270751953125
Mouse:
-33.9338180386977
151.268005371094
Click:
-33.9135913560992
151.326541900635
Point Piper
Darling Point
Elizabeth Bay
Rushcutters Bay
Double Bay
Rose Bay
Dover Heights
Darlinghurst
Edgecliff
Bellevue Hill
North Bondi
Paddington
Woollahra
Surry Hills
Chippendale
Strawberry Hills
Darlington
Redfern
Eveleigh
Waterloo
Macdonaldtown
Erskineville
Alexandria
Zetland
Kensington
Beaconsfield
Randwick
Clovelly
Coogee
Bondi Junction
Bondi
Bondi Beach
Tamarama
Bronte
Queens Park
Waverley
Pyrmont
Town Hall
Haymarket
Ultimo
Glebe
Centennial Park
Moore Park
Mascot
Eastlakes
Kingsford
Eastgardens
Botany
Hillsdale
South Coogee
Wedding Cake Island
© OpenStreetMap - Map data ©2012 OpenStreetMap
GPS 3D 33°52'52.1220"S,151°14'44.1960"E 076.800 0 m/s 1.2

BorDUF

File Connection Settings Window

Connections Map Doppler

MapWindow



Center on current

Center now

Clear track

Add POI

Show current track

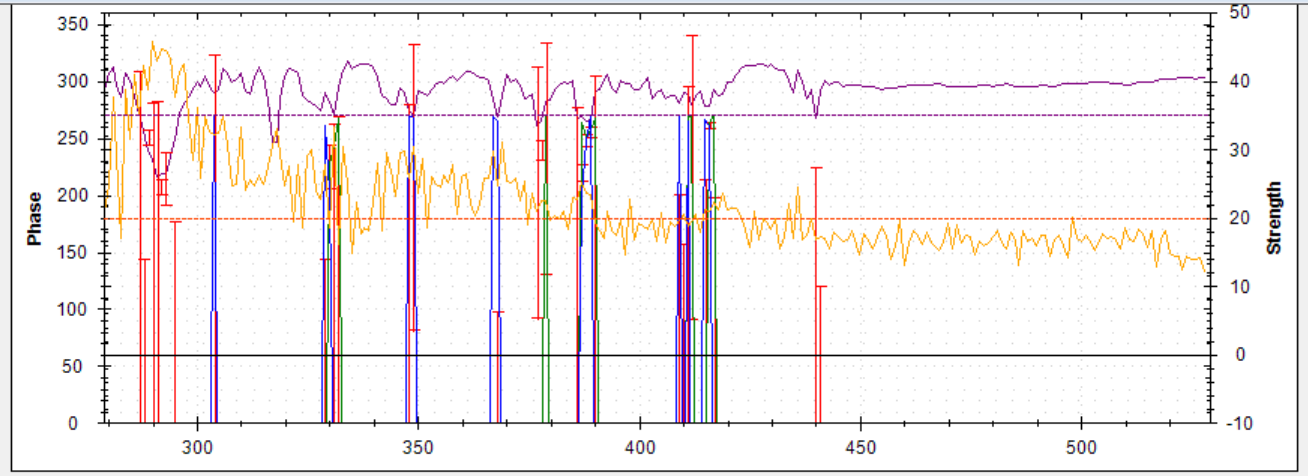
Doppler

Updates: 43
Strength: 40.4121494123098

Threshold: 35 Offset: -90

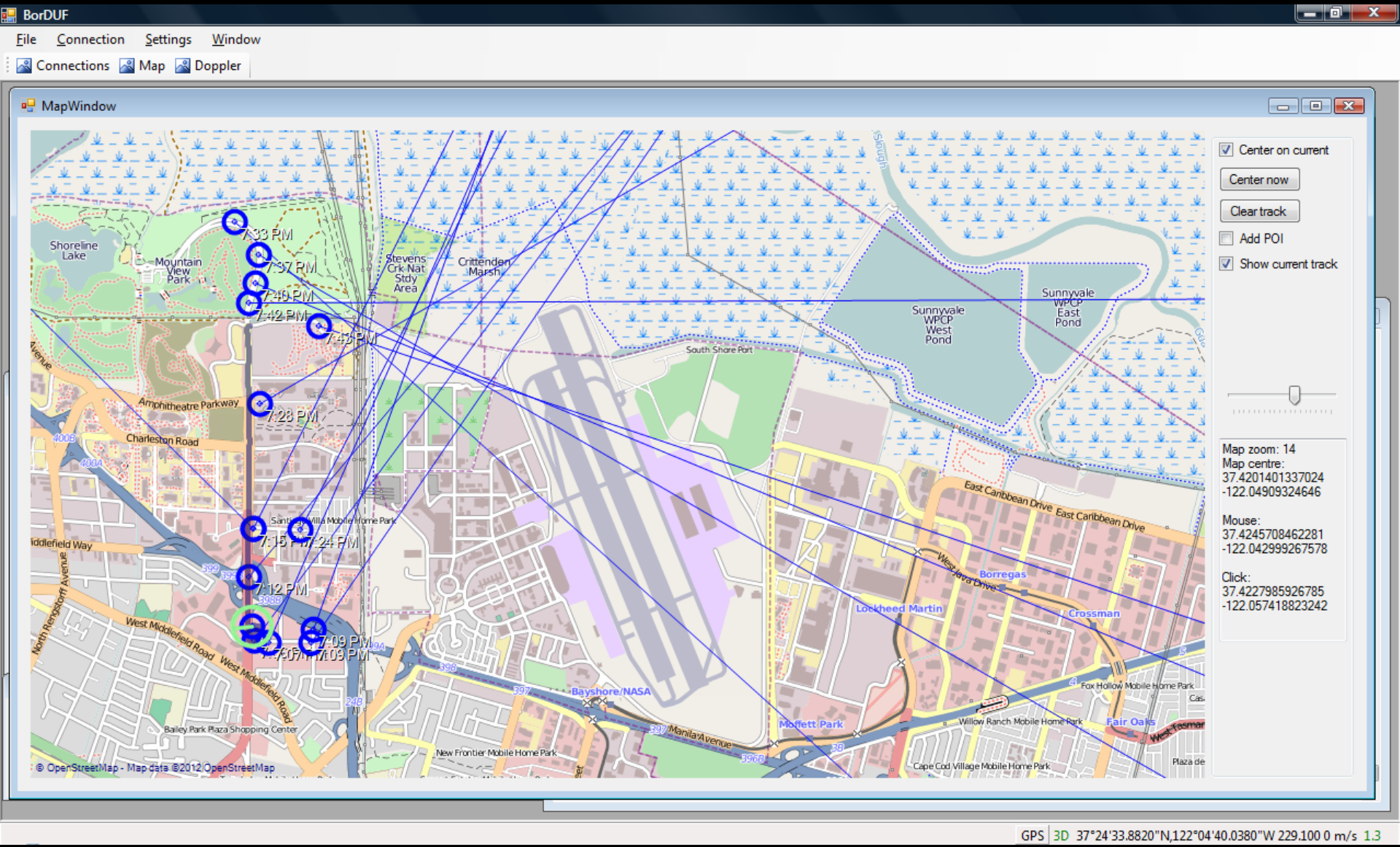
Manual Reverse DC: -80

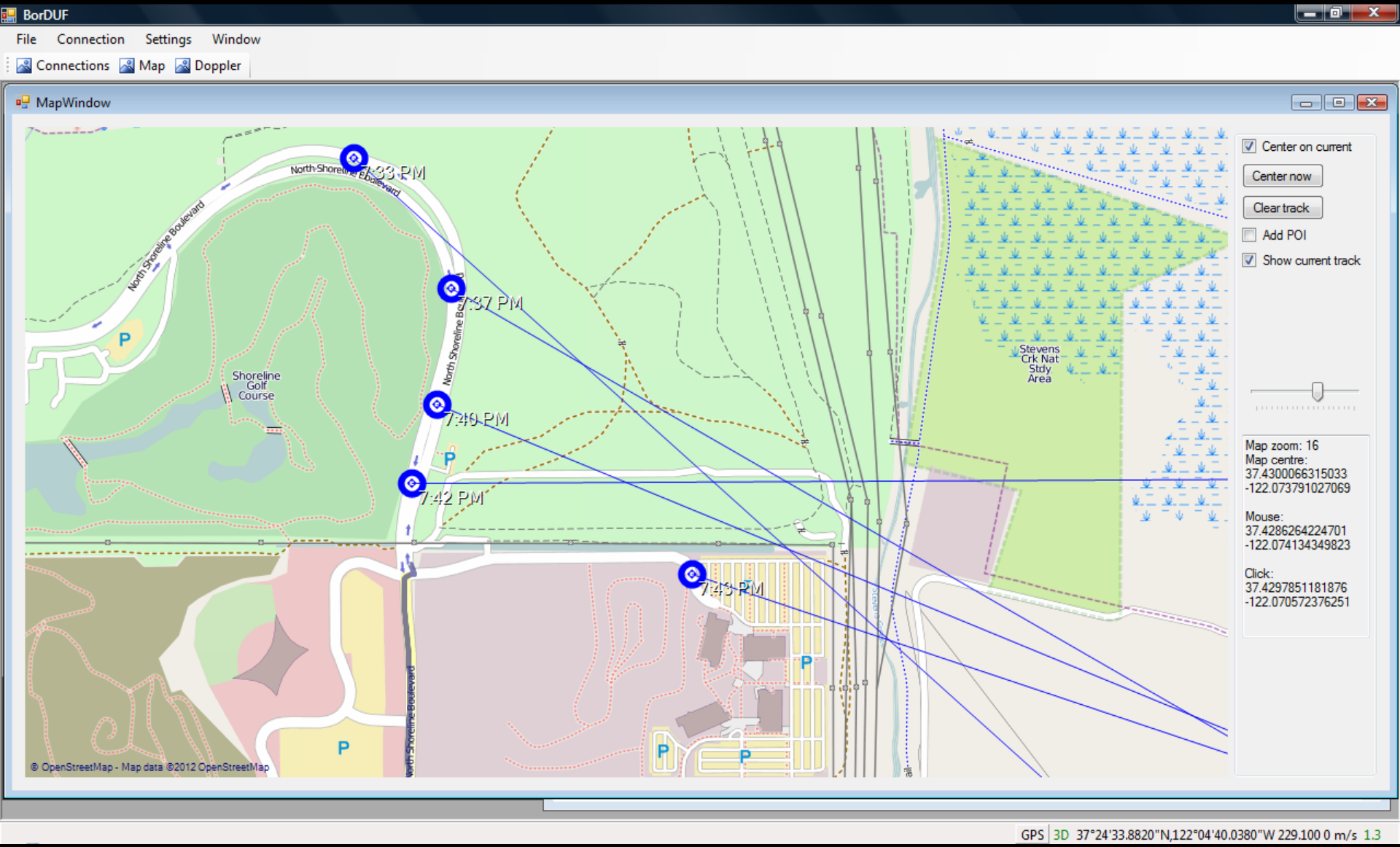
Frequency: 0.000 Squelch

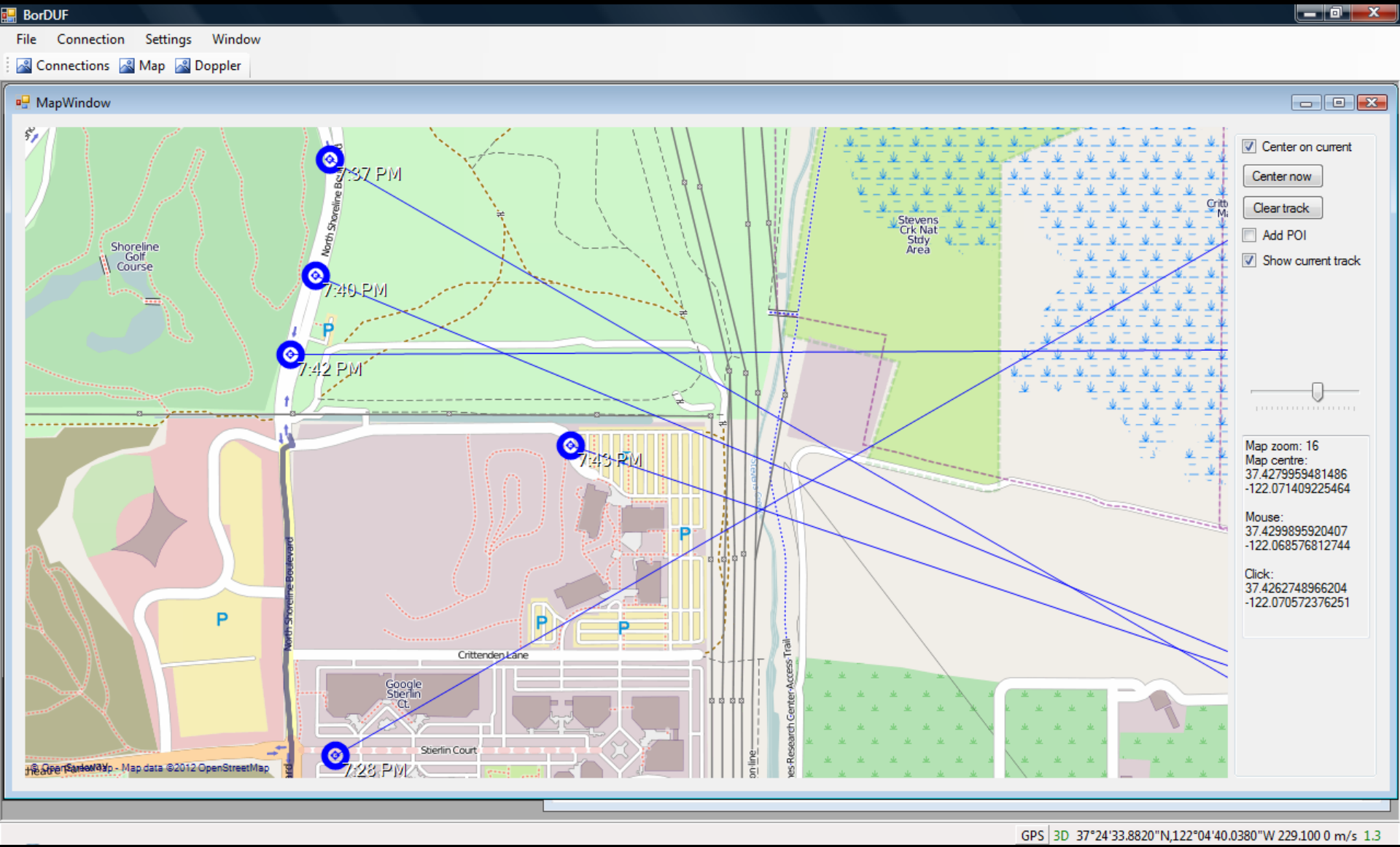


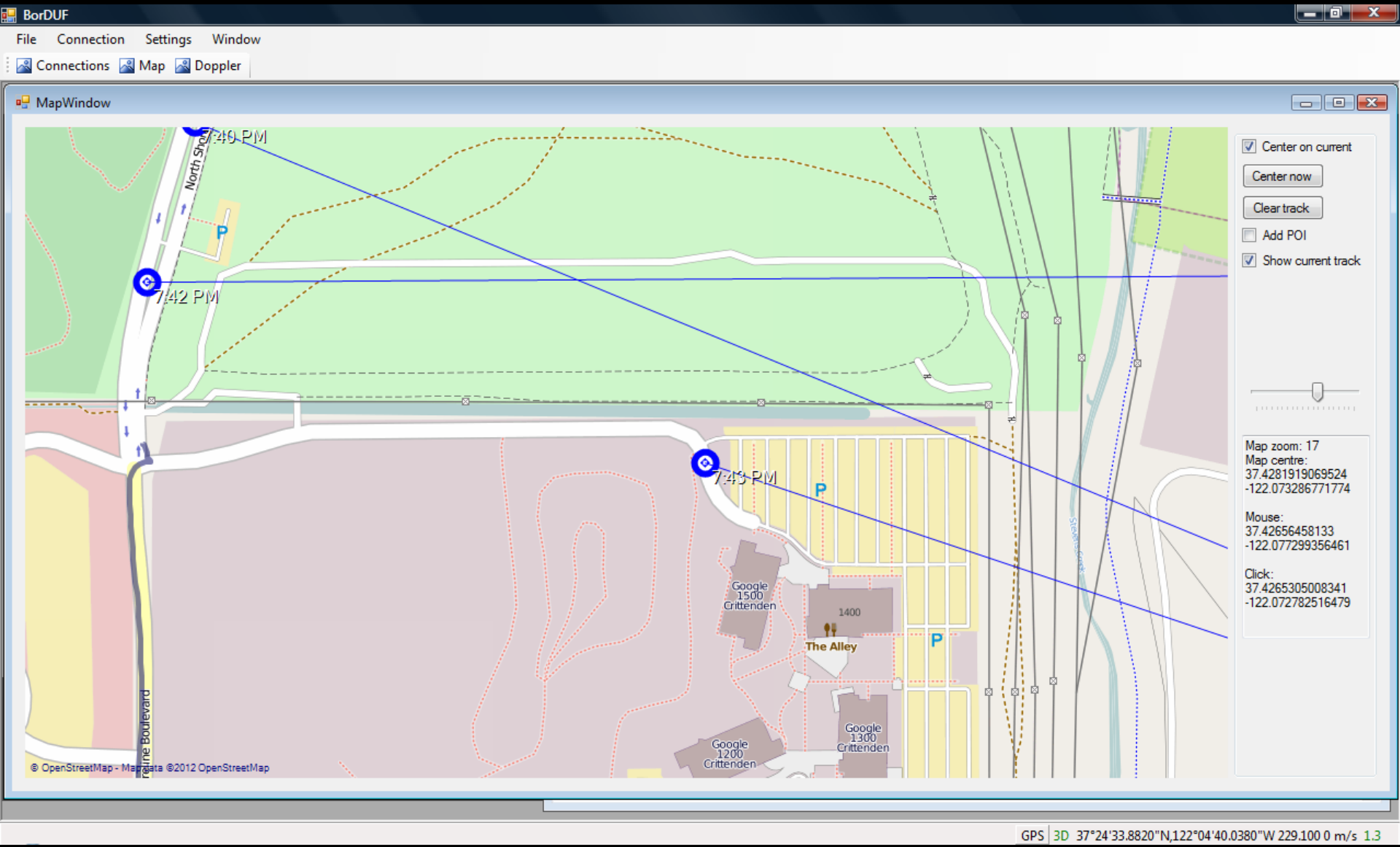
2659342)
59)
78497395)
259419)
839766286)
893056)
096886375)
540519)
7677959504)
670448)
5722486)
2116244659)
2228148)
086838732202)
6525021)
1750909972)
70712956)
27751085)
6156612)
5107070131)

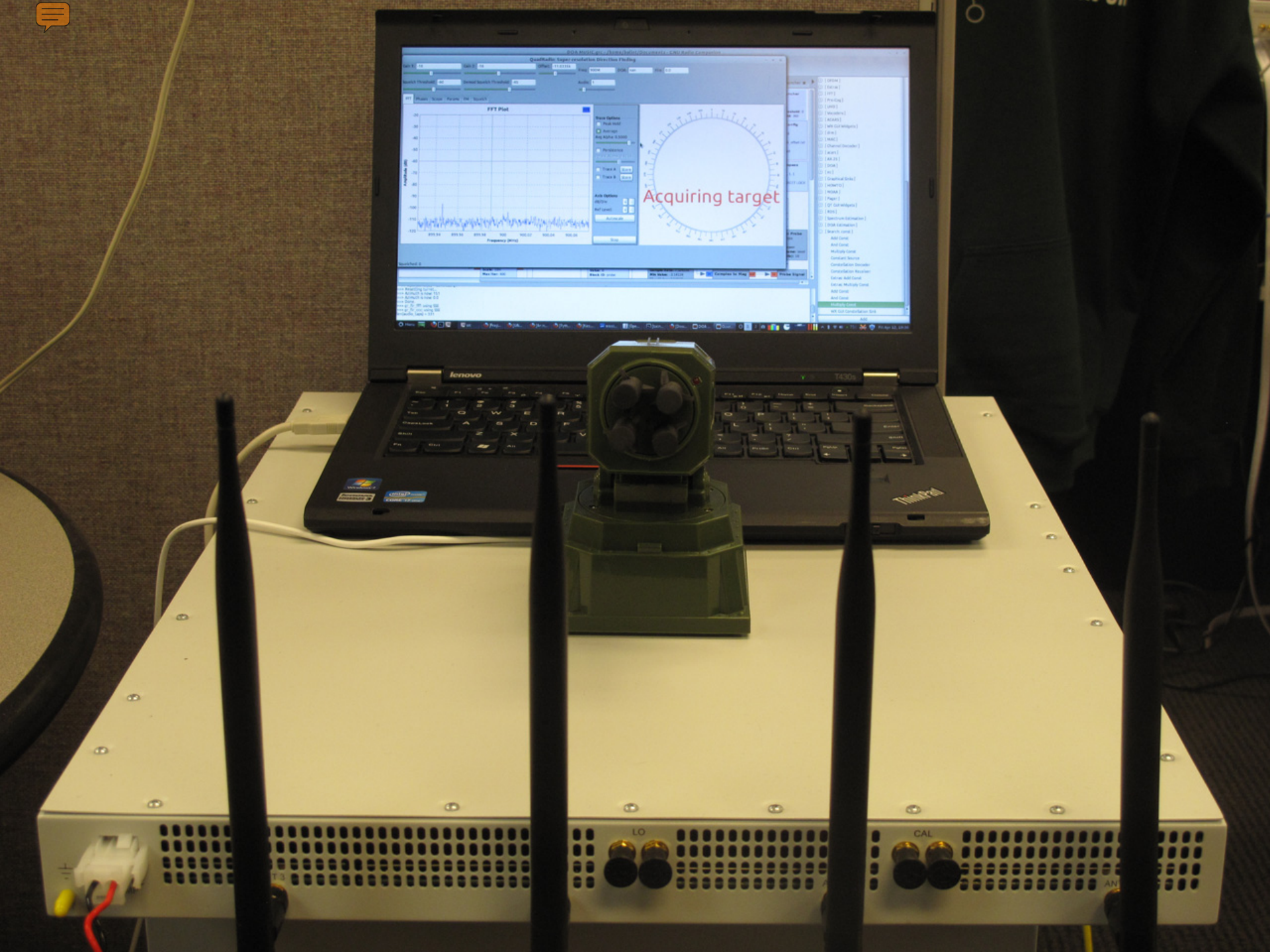
GPS 3D 37°25'50.7540"N,122°04'39.0180"W 197.400 0 m/s 1.1

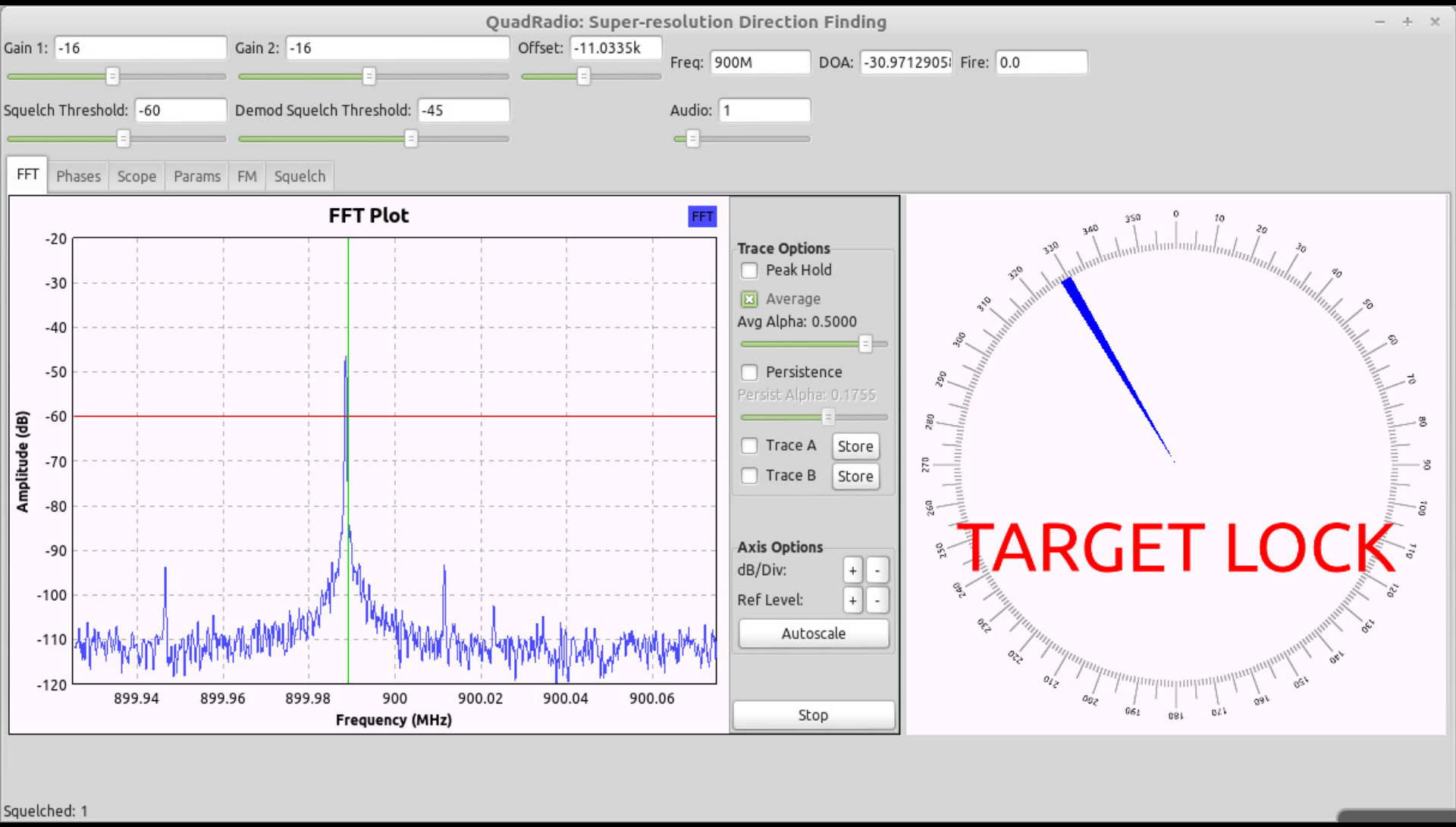

BorDUF
File
Connection
Settings
Window
Connections
Map
Doppler
MapWindow
Center on current
Center now
Clear track
Add POI
Show current track
Map zoom: 14
Map centre:
37.4201401337024
-122.04909324646
Mouse:
37.4245708462281
-122.042999267578
Click:
37.4227985926785
-122.057418823242
7:33 PM
7:37 PM
7:39 PM
7:42 PM
7:45 PM
7:28 PM
7:15 PM
7:24 PM
7:12 PM
7:09 PM
Shoreline Lake
Mountain View Park
Stevens Crk Nat Stdy Area
Crittenden Marsh
Sunnyvale WPCP West Pond
Sunnyvale WPCP East Pond
South Shore Port
Amphitheatre Parkway
Charleston Road
East Caribbean Drive
West Middlefield Road
Bayshore/NASA
Moffett Park
Lockheed Martin
Borregas
Crossman
Fair Oaks
Manila Avenue
Bailey Park Plaza Shopping Center
New Frontier Mobile Home Park
Willow Ranch Mobile Home Park
Fox Hollow Mobile Home Park
Cape Cod Village Mobile Home Park
© OpenStreetMap - Map data ©2012 OpenStreetMap
GPS 3D 37°24'33.8820"N,122°04'40.0380"W 229.100 0 m/s 1.3

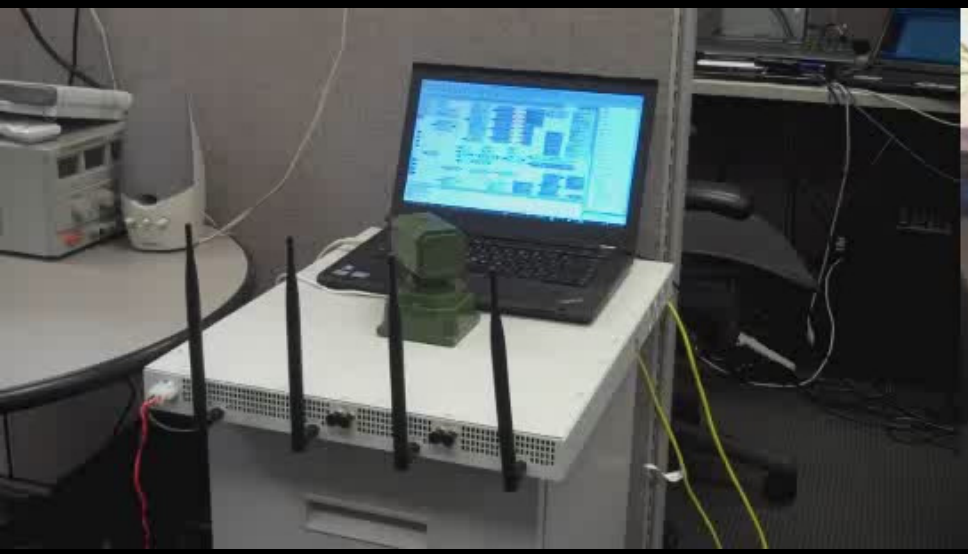

BorDUF
File
Connection
Settings
Window
Connections
Map
Doppler
MapWindow
7:33 PM
7:37 PM
7:40 PM
7:42 PM
7:45 PM
North Shoreline Boulevard
Shoreline Golf Course
Stevens Crk Nat Stdy Area
Center on current
Center now
Clear track
Add POI
Show current track
Map zoom: 16
Map centre:
37.4300066315033
-122.073791027069
Mouse:
37.4286264224701
-122.074134349823
Click:
37.4297851181876
-122.070572376251
© OpenStreetMap - Map data ©2012 OpenStreetMap
GPS 3D 37°24'33.8820"N,122°04'40.0380"W 229.100 0 m/s 1.3

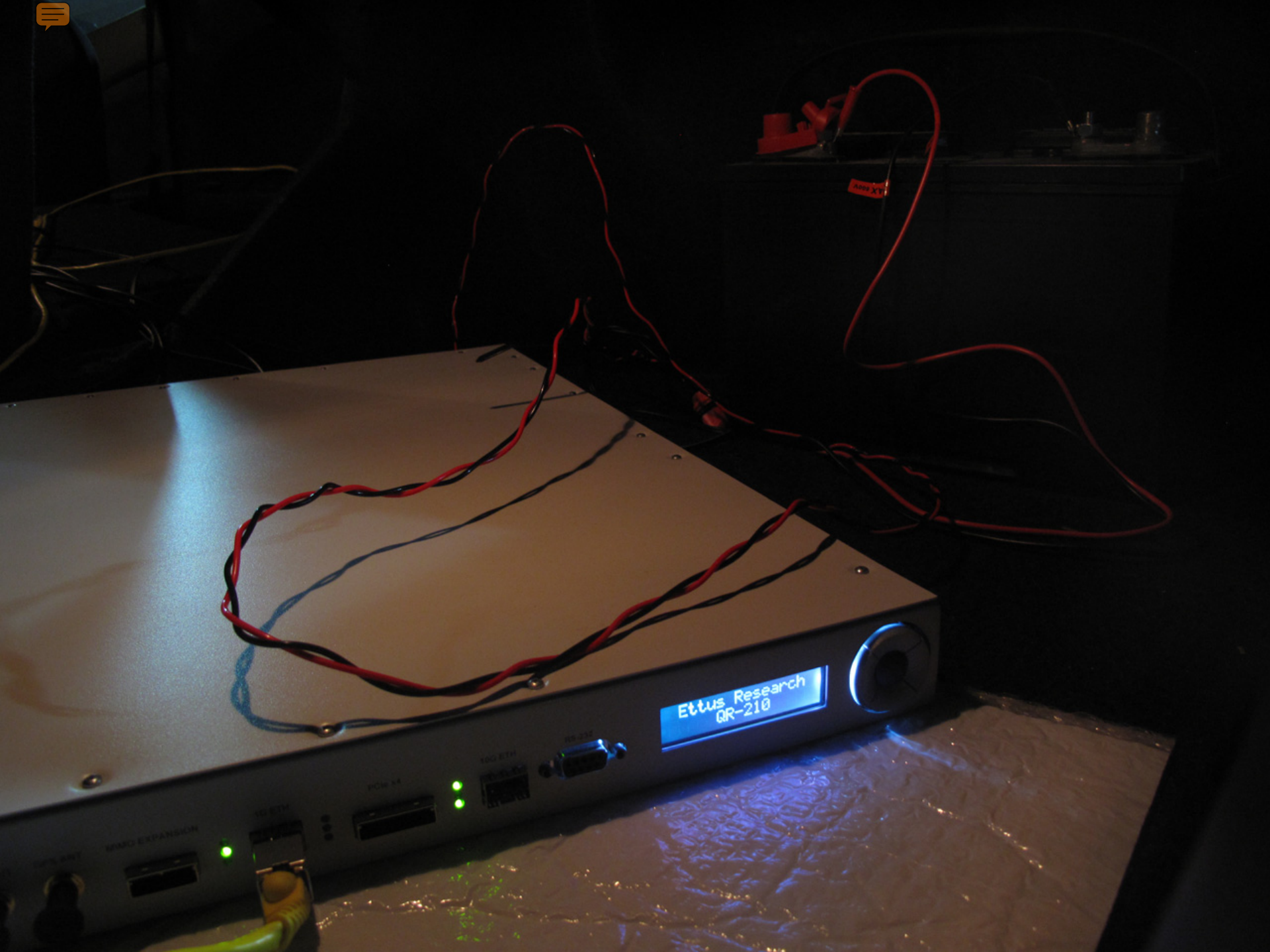

BorDUF
File
Connection
Settings
Window
Connections
Map
Doppler
MapWindow
7:37 PM
7:40 PM
7:42 PM
7:43 PM
7:28 PM
Shoreline Golf Course
North Shoreline Boulevard
Stevens Crk Nat Stdy Area
Crittenden Lane
Google Stierlin Ct
Stierlin Court
Center on current
Center now
Clear track
Add POI
Show current track
Map zoom: 16
Map centre:
37.4279959481486
-122.071409225464
Mouse:
37.4299895920407
-122.068576812744
Click:
37.4262748966204
-122.070572376251
© OpenStreetMap - Map data ©2012 OpenStreetMap
GPS
3D
37°24'33.8820"N,122°04'40.0380"W 229.100 0 m/s 1.3

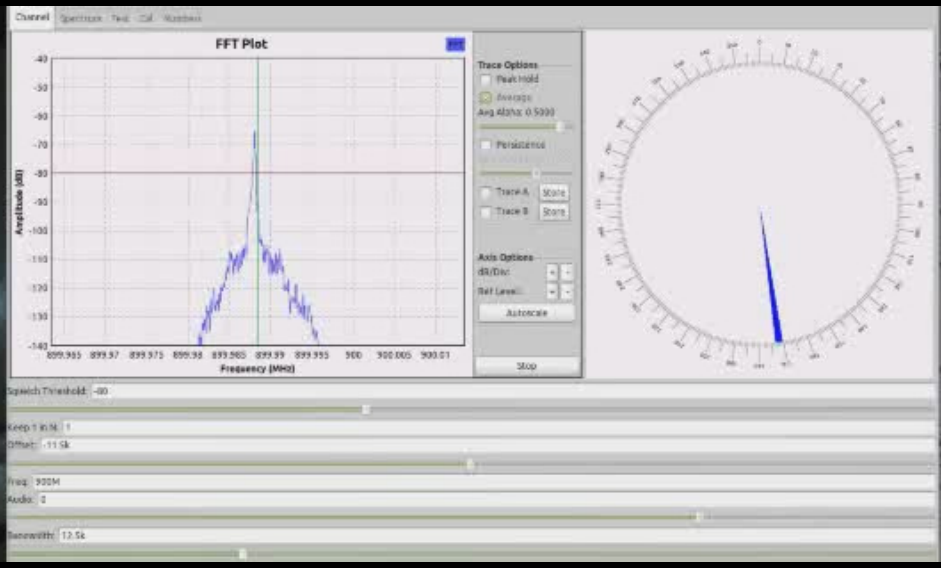

BorDUF
File
Connection
Settings
Window
Connections
Map
Doppler
MapWindow
7:40 PM
7:42 PM
7:43 PM
North Shore
P
Google
1500
Crittenden
1400
The Alley
Google
1300
Crittenden
Google
1200
Crittenden
Center on current
Center now
Clear track
Add POI
Show current track
Map zoom: 17
Map centre:
37.4281919069524
-122.073286771774
Mouse:
37.4265658133
-122.077299356461
Click:
37.4265305008341
-122.072782516479
© OpenStreetMap - Map data ©2012 OpenStreetMap
GPS
3D
37°24'33.8820"N,122°04'40.0380"W 229.100 0 m/s 1.3

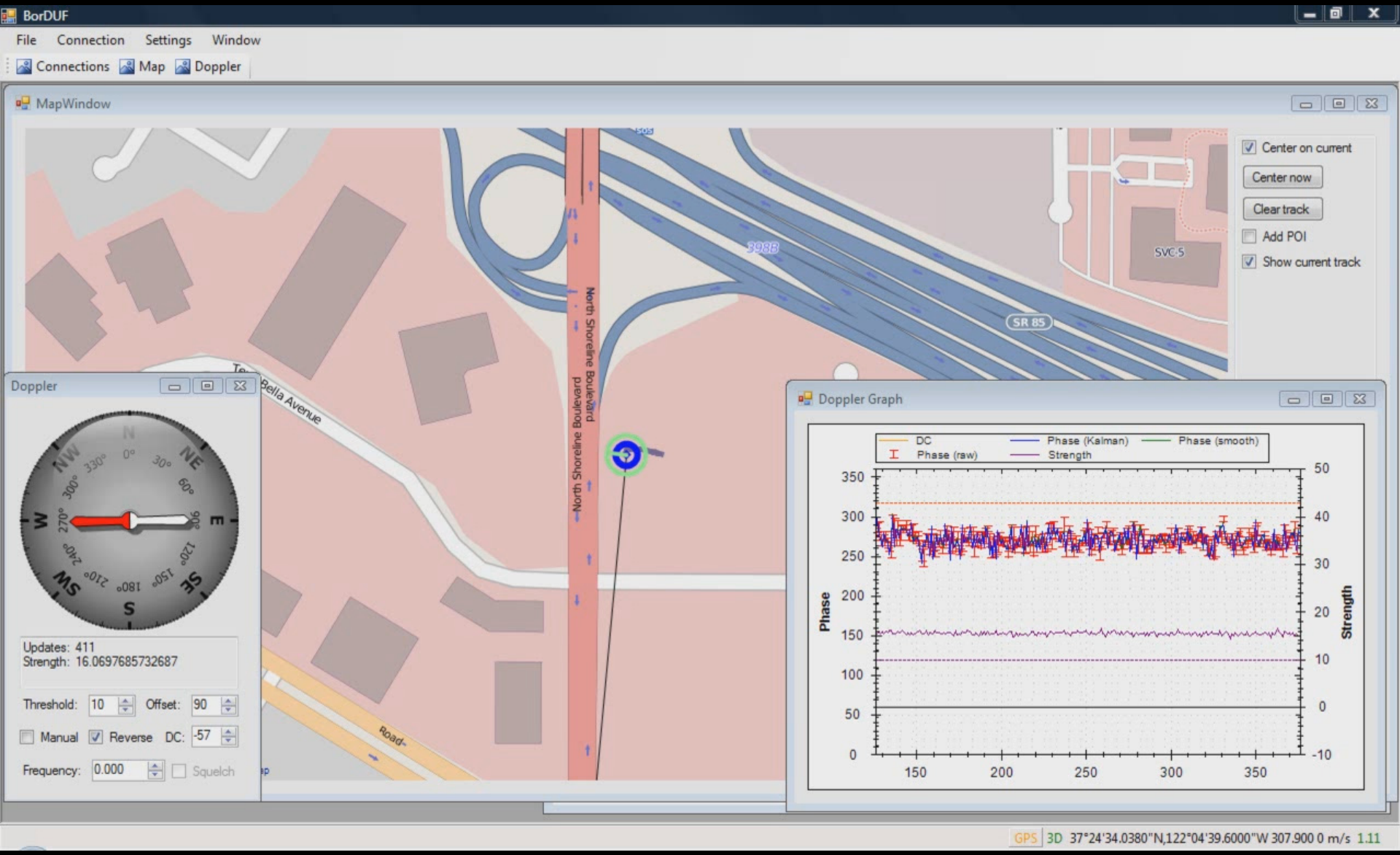

FFT Plot
Acquiring target
lenovo
ThinkPad
LO
CAL

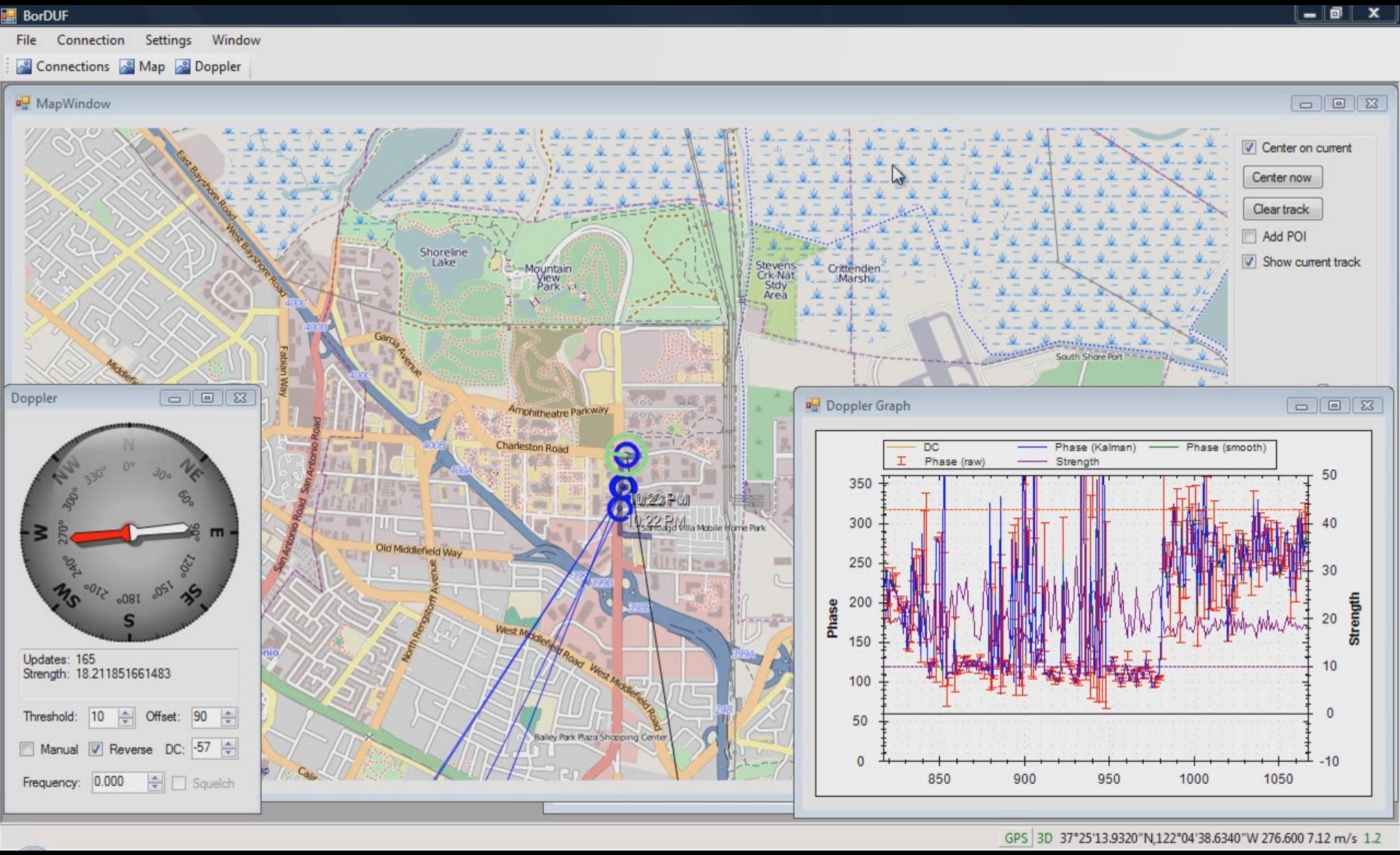

QuadRadio: Super-resolution Direction Finding
Gain 1: -16
Gain 2: -16
Offset: -11.0335k
Freq: 900M
DOA: -30.9712905
Fire: 0.0
Squelch Threshold: -60
Demod Squelch Threshold: -45
Audio: 1
FFT
Phases
Scope
Params
FM
Squelch
FFT Plot
FFT
Amplitude (dB)
-20
-30
-40
-50
-60
-70
-80
-90
-100
-110
-120
899.94
899.96
899.98
900
900.02
900.04
900.06
Frequency (MHz)
Trace Options
Peak Hold
Average
Avg Alpha: 0.5000
Persistence
Persist Alpha: 0.1755
Trace A
Store
Trace B
Store
Axis Options
dB/Div:
Ref Level:
Autoscale
Stop
TARGET LOCK
Squelched: 1



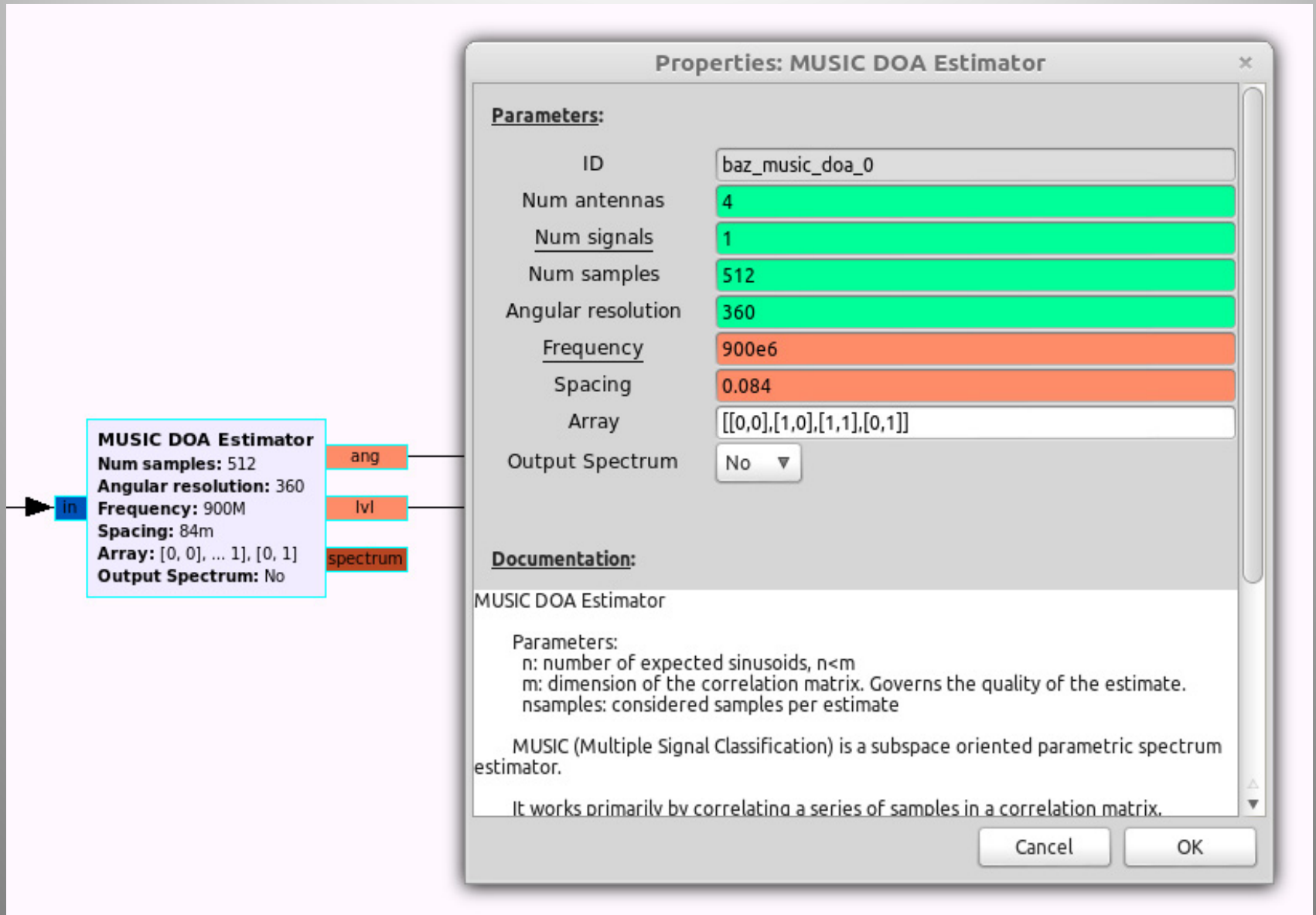

Ettus Research
QR-210


Channel
FFT Plot
Trace Options
Peak Hold
Average
Persistence
Trace A
Trace B
Store
Axis Options
dB/Div
Ref Level
Autoscale
Stop
Amplitude (dB)
Frequency (MHz)
Squelch Threshold
Keep 1 in N
Offset
Freq
Audio
Bandwidth


BorDUF
File
Connection
Settings
Window
Connections
Map
Doppler
MapWindow
Center on current
Center now
Clear track
Add POI
Show current track
SR 85
North Shoreline Boulevard
Bella Avenue
Doppler
Updates: 411
Strength: 16.0697685732687
Threshold: 10
Offset: 90
Manual
Reverse
DC: -57
Frequency: 0.000
Squelch
Doppler Graph
DC
Phase (raw)
Phase (Kalman)
Strength
Phase (smooth)
Phase
Strength
GPS 3D 37°24'34.0380"N,122°04'39.6000"W 307.900 0 m/s 1.11


BorDUF
File
Connection
Settings
Window
Connections
Map
Doppler
MapWindow
Center on current
Center now
Clear track
Add POI
Show current track
Shoreline Lake
Mountain View Park
Stevens Crk Nat Stdy Area
Crittenden Marsh
South Shore Port
East Bayshore Road
West Bayshore Road
Fabian Way
Garcia Avenue
Amphitheatre Parkway
Charleston Road
San Antonio Road
Old Middlefield Way
North Rengstorff Avenue
West Middlefield Road
Bailey Park Plaza Shopping Center
Doppler
Updates: 165
Strength: 18.211851661483
Threshold: 10
Offset: 90
Manual
Reverse
DC: -57
Frequency: 0.000
Squelch
Doppler Graph
DC
Phase (raw)
Phase (Kalman)
Strength
Phase (smooth)
Phase
Strength
GPS 3D 37°25'13.9320"N,122°04'38.6340"W 276.600 7.12 m/s 1.2

GNU Radio MUSIC DOA block




23

Police Checklist

- Car's rego paper
- Amateur Radio licence
- Antenna structural redundancy
- Dress code
- Clean-shaven
- Hide Motorola XTS radios
- Avoid turning around and trying to desperately disconnect antennas

Gedanken: TX

DO NOT TRY THIS AT…

WHEREVER!

Gedanken: Pagers

- Don’t like a doctor/nurse?
  - Send them on many a wild goose chase
- Is your arch-nemesis in hospital?
  - Tell them to remove the *other* ********
- Need to distract security?
  - Issue an ‘automated’ alert

Gedanken: Mode S

- Want to reach cruising altitude a little quicker?
  - Put a ‘plane’ heading towards you (at a slightly lower altitude)
- Think the pilot made the wrong choice in deciding to land?
  - Put a ‘plane’ on the runway
- Want to display a message on everyone’s radar screen?
  - Spell one using ‘aircraft marker’ art

Gedanken: ACARS

- Don’t want to fly on a particular aircraft?
  - Send a severe fault report
- Was the flight a little bumpy?
  - Send an engine performance report to RR with large vibration values
- Need to message the cockpit privately?
  - Address the message to cockpit printer #1

Gedanken: Satellite

- Uplink power is generally kept at the minimum level to save money
- Depends on the weather:
  - Clear sky: a few W
  - Heavy rain: a few kW
- Turn yours up to (theirs + 1)
- "a malfunctioning UPC system can interfere with

Customers may use uplink power control systems (UPC) to compensate for uplink rain attenuation. Since a malfunctioning UPC system can interfere with other services and even damage a satellite TWTA, UPC systems must be approved by Optus before use and are strictly limited in the amount of uplink compensation permitted. Details of the amount of UPC permitted under various operating conditions may be obtained from Optus.

Gedanken: Satellite

- Uplink power is generally kept at the minimum level to save money
- Depends on the weather:
  - Clear sky: a few W
  - Heavy rain: a few kW
- Turn yours up to (theirs + 1)
- "…a malfunctioning UPC system can interfere with other services and even damage a satellite Travelling Wave Tube Amplifier…"

Customers may use uplink power control systems (UPC) to compensate for uplink rain attenuation. Since a malfunctioning UPC system can interfere with other services and even damage a satellite TWTA, UPC systems must be approved by Optus before use and are strictly limited in the amount of uplink compensation permitted. Details of the amount of UPC permitted under various operating conditions may be obtained from Optus.

Gedanken: FasTrak

- Don’t want to pay the toll?
  - Masquerade as anyone else
    - Collect IDs by standing on an overpass
- Want traffic management (511) to think there’s an auto-stampede?
  - Respond with lots of different valid IDs
- Keep tabs on someone?
  - Look out for their tag ID


Remember: be legal and be….
SAFE
BOSCH
BOSCH


http://wiki.spench.net/wiki/RF
http://spench.net/
GitHub: balint256
balint@spench.net
balint@ettus.com
@spenchdotnet