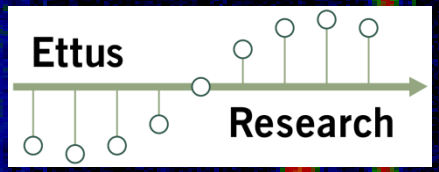
Notes and links in PDF comments on each slide

All Your RFz Are Belong to Me: Hacking the Wireless World with Software Defined Radio

Balint Seeber
balint@spench.net
@spenchdotnet

Applications Engineer
balint@ettus.com

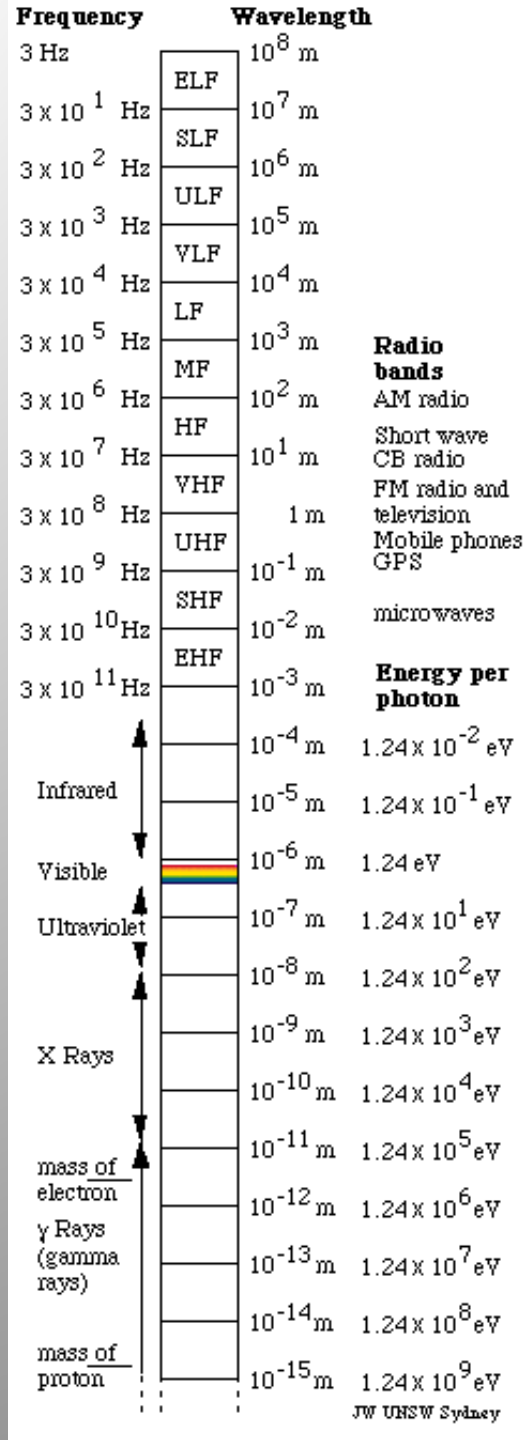


Overview

- RF 101
- The journey into Software Defined Radio
- Hospital pager systems
- Tracking planes
- Decoding satellite-downlink traffic
- Direction Finding

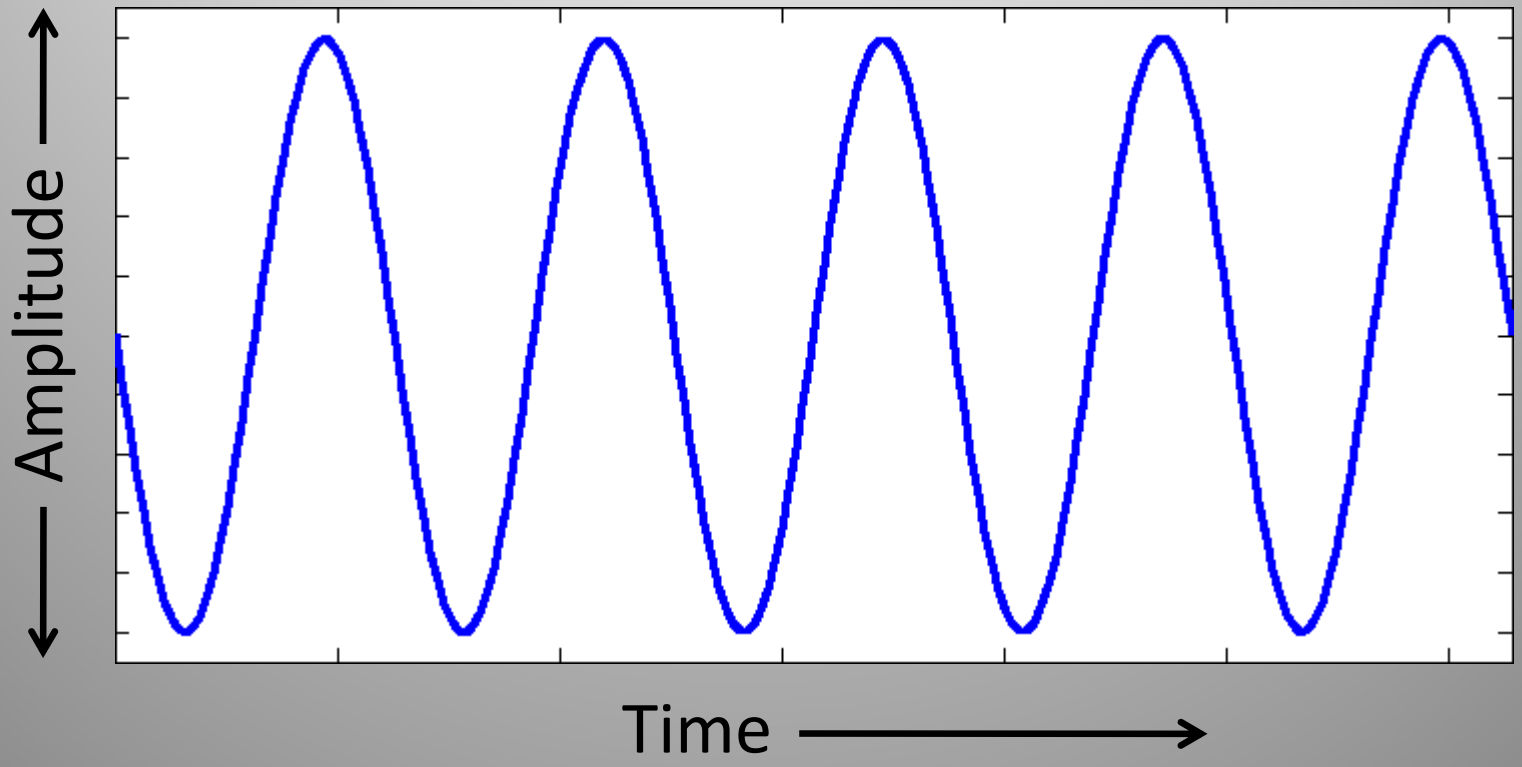
The Electromagnetic Spectrum

- Electromagnetism: one of four universal forces
- Radio wave exists due to energy being propagated at a particular frequency
- Can create and receive radio waves using electronics



Transmitting Data

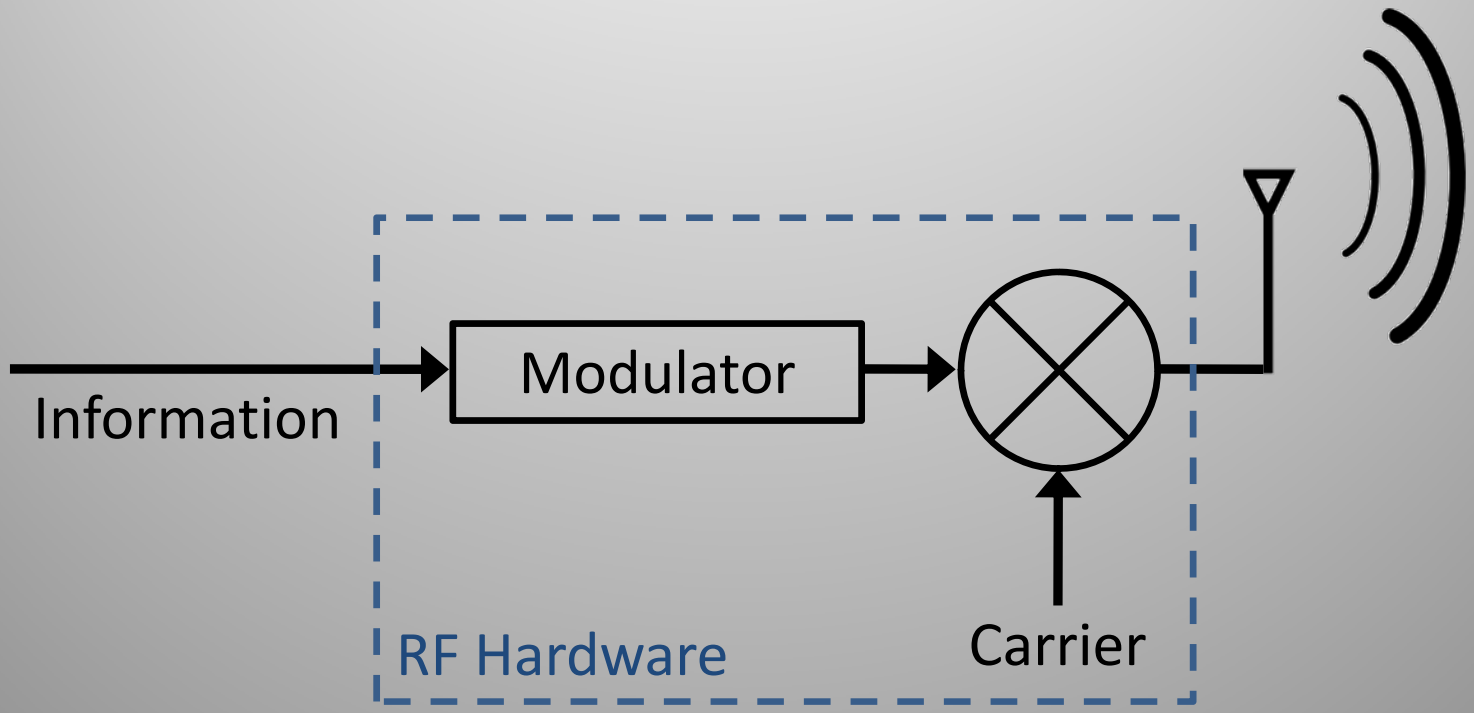
- Radio (carrier) wave must be modulated to convey information



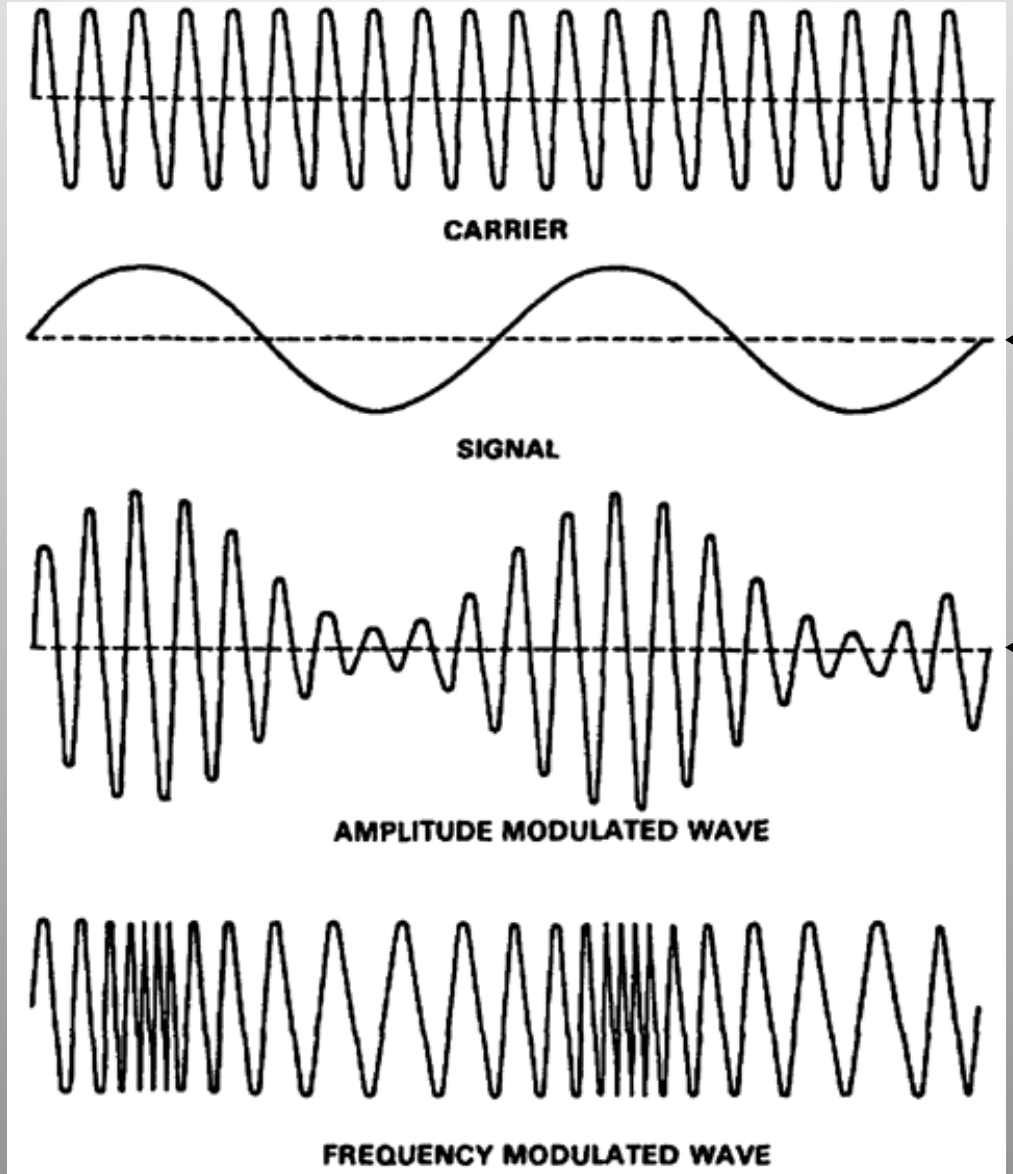
Transmitting Data

- 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

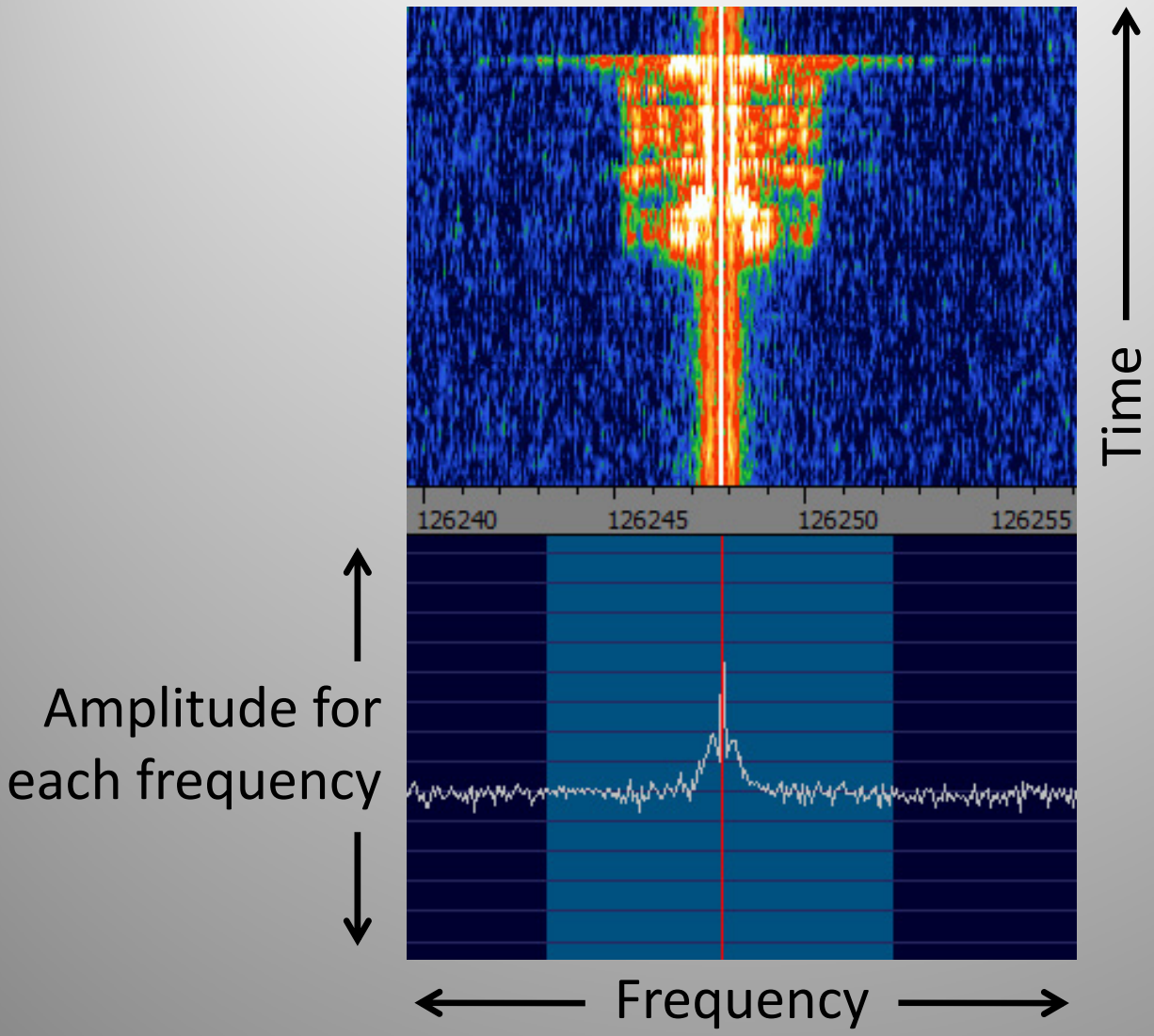


Analog or digital information

Constant amplitude

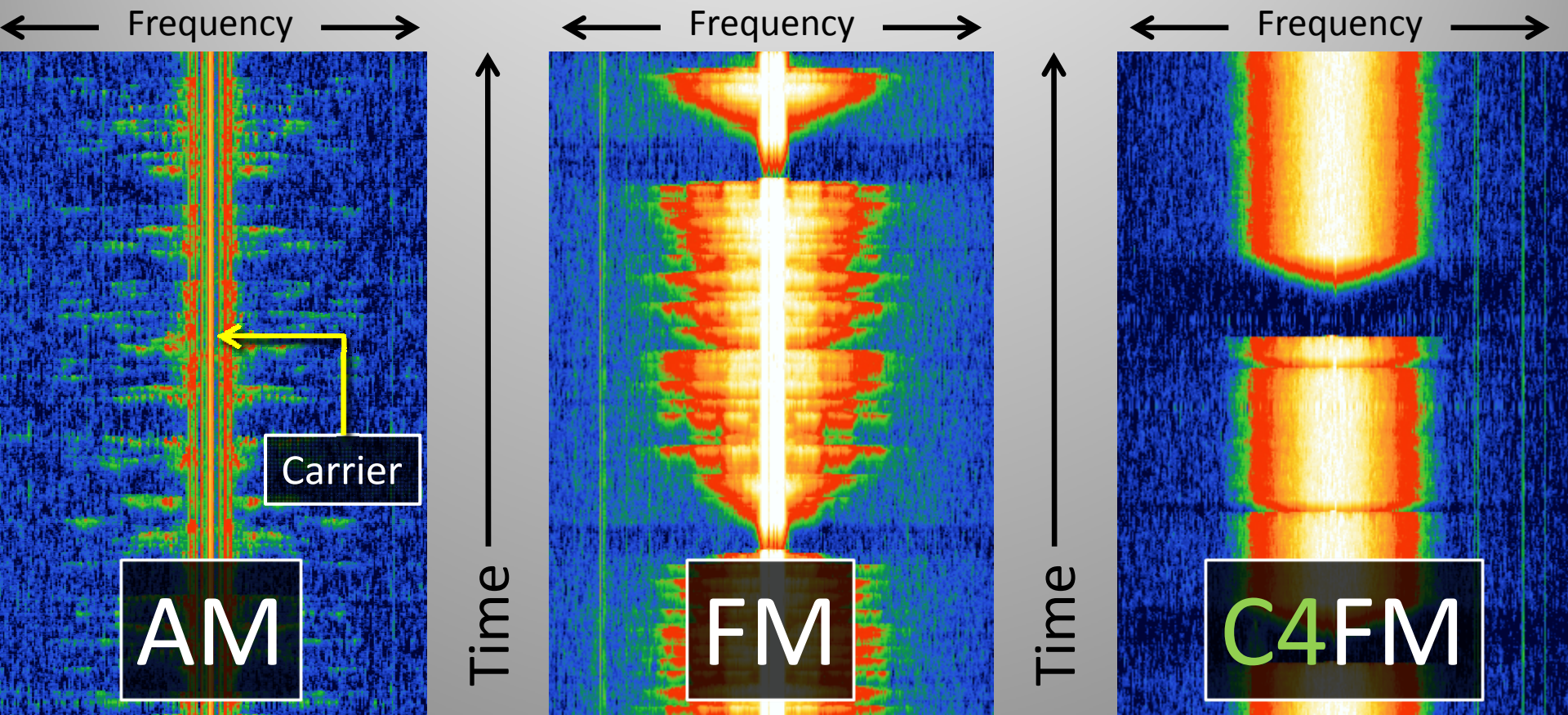
Constant frequency

In the Frequency Domain



Modulation

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

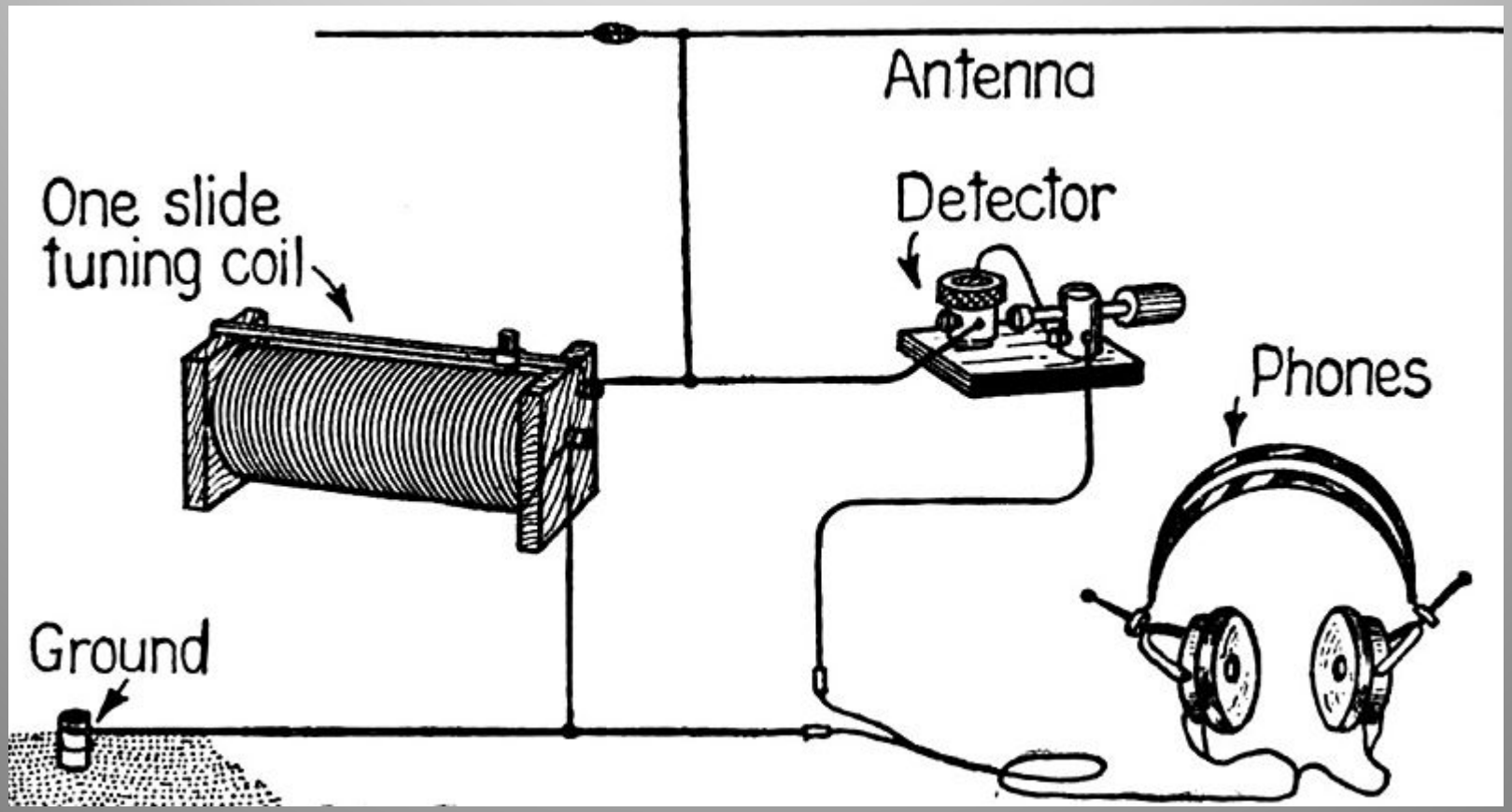


Hardware

- Crystal set receiver
  - Powerful AM transmissions

Hardware

- Crystal set receiver
  - Powerful AM transmissions

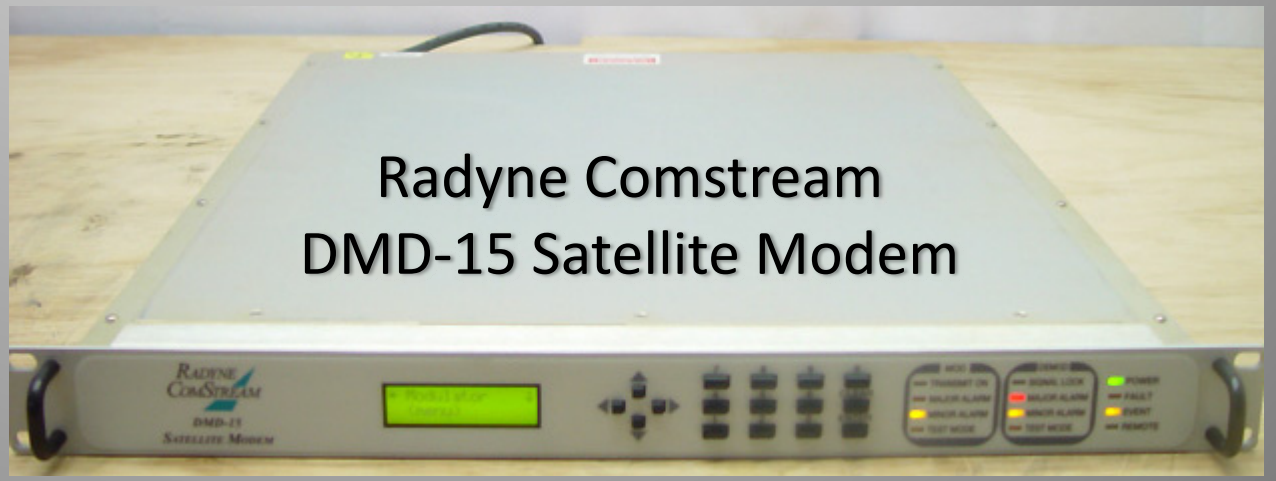


Hardware

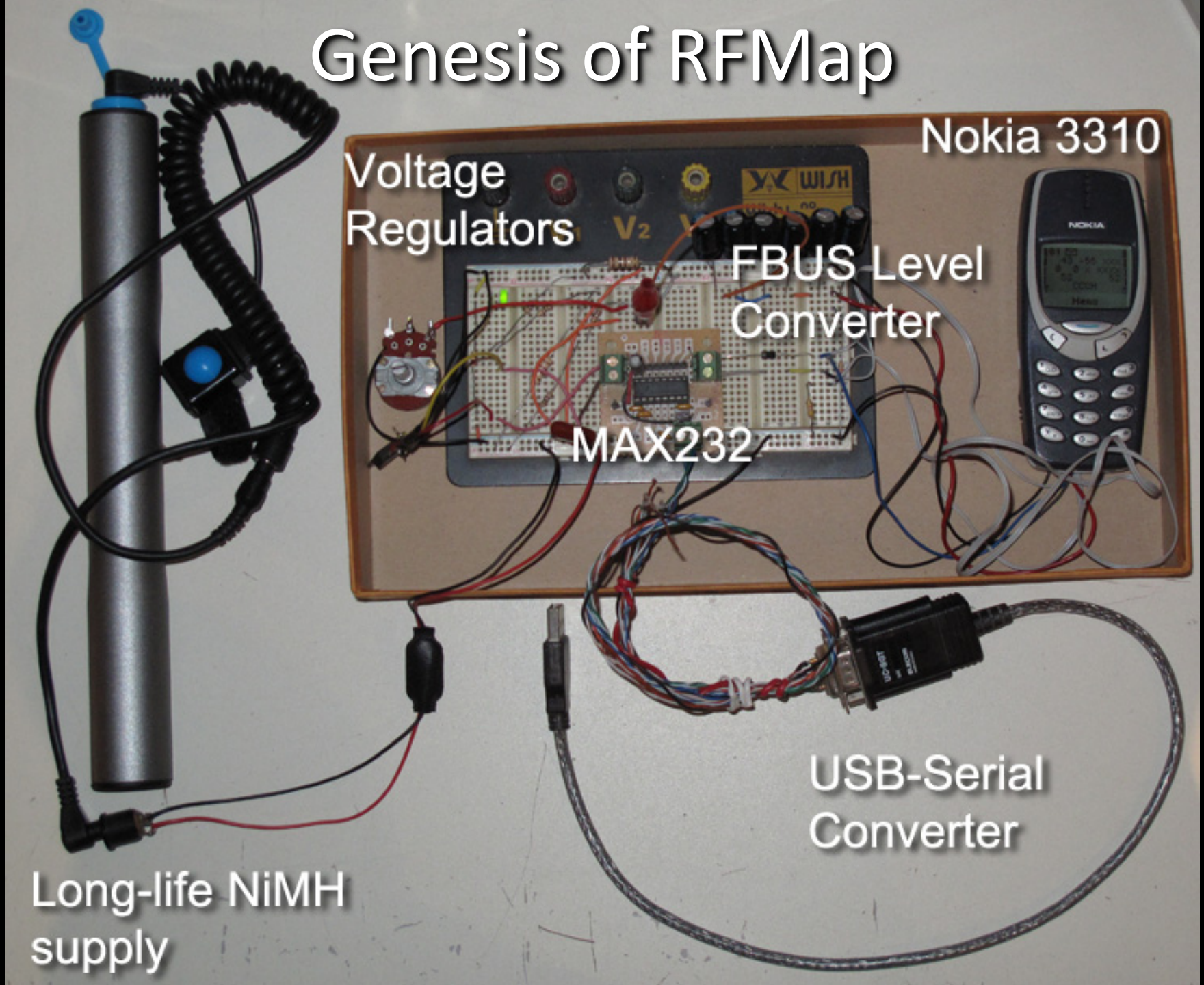
- Crystal set receiver
  - Powerful AM transmissions
- More advanced hardware to handle increasingly complex modulation schemes
  - FM, stereo FM, microwave, digital…

Modulation in Hardware

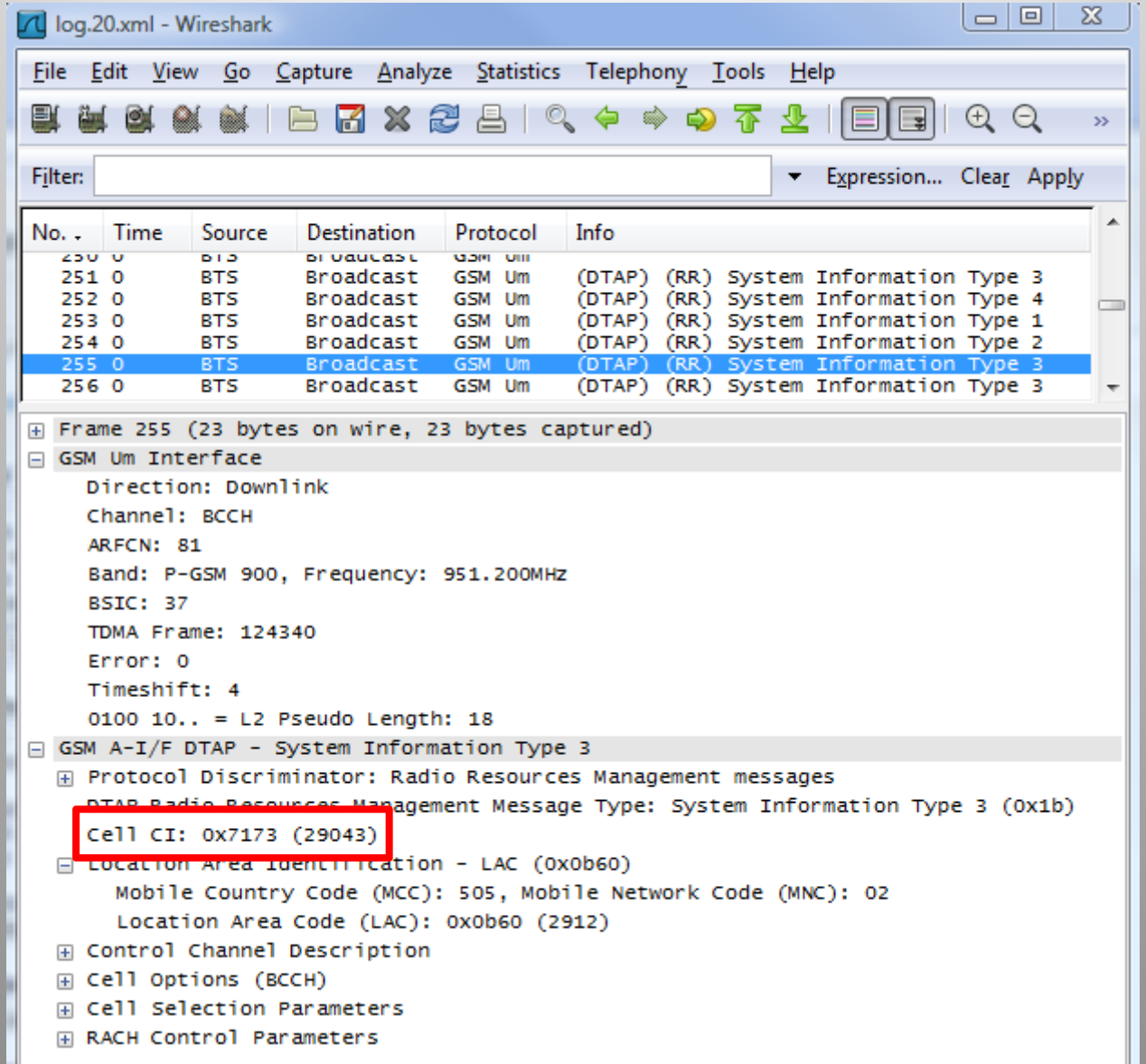
- **MO**dulation and **DE-M**odulation traditionally performed in hardware
- 'Black box' implementation
  - Not re-configurable
- Modern digital hardware allows more flexibility



The journey begins…

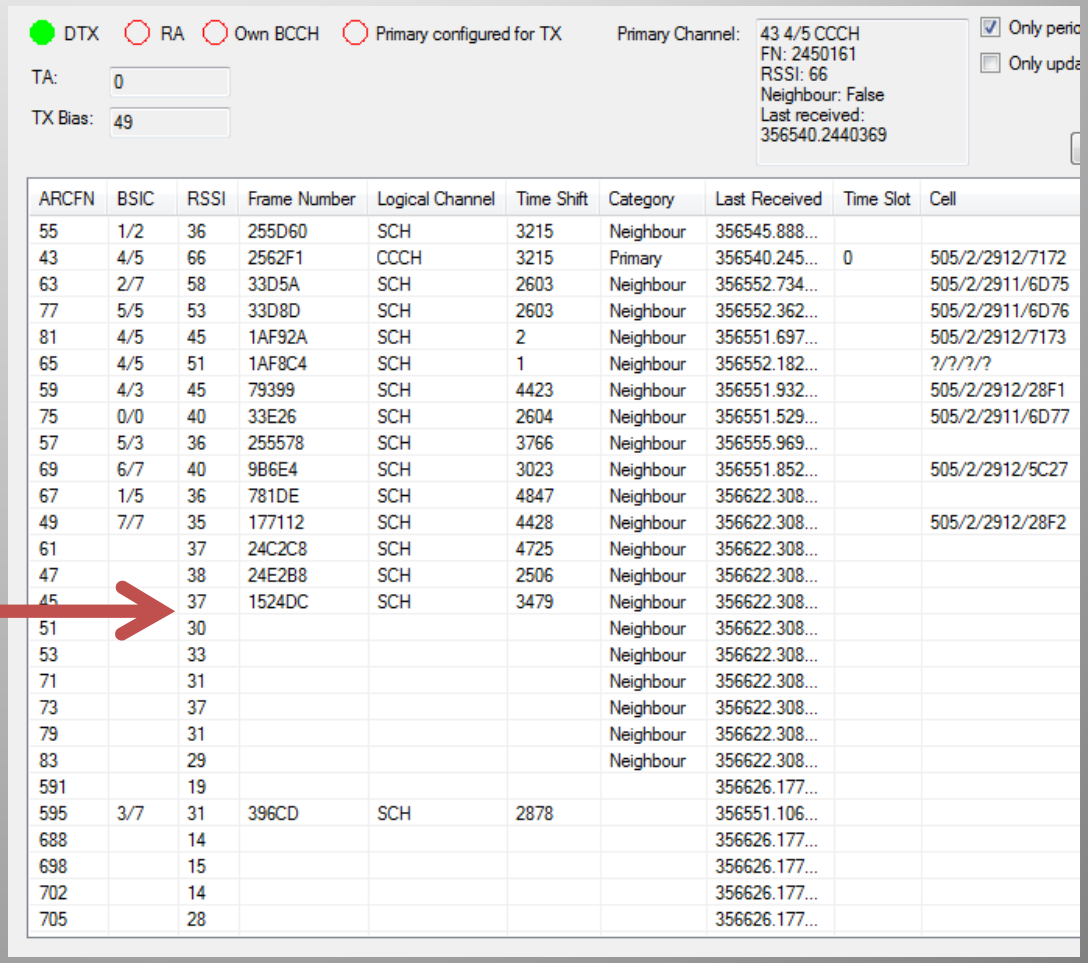

Genesis of RFMap
Nokia 3310
Voltage Regulators
FBUS Level Converter
MAX232
USB-Serial Converter
Long-life NiMH supply

GSM + Gammu + Wireshark



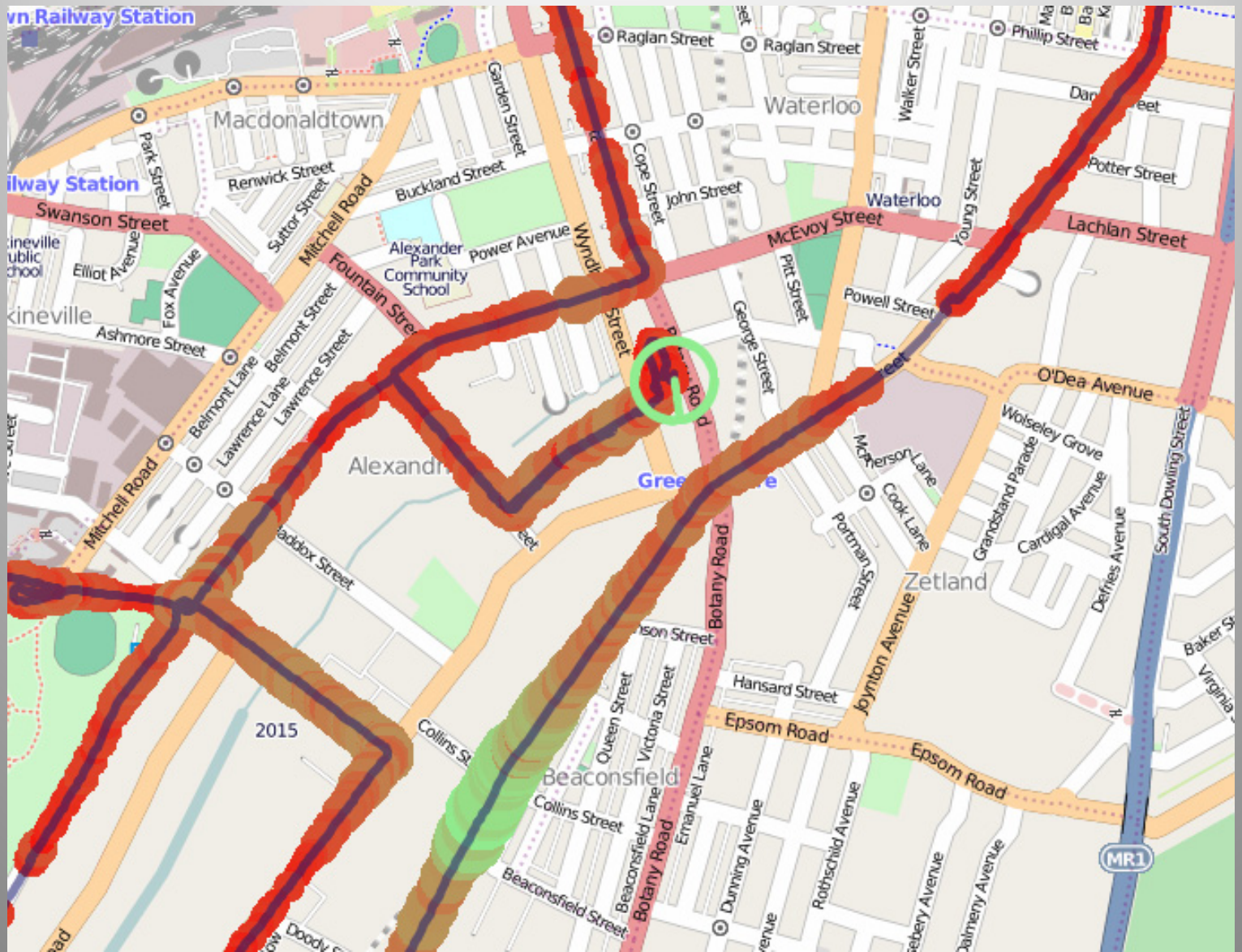
Field Test Mode

<1983> MDI:d2m/RSSI_RESULTS t=0afe nr=73: D 83:
00 00 b1 b1 00 65 ab a3 b1 a0 a0 a6 9d a1 80 a4 80 80 80 80 80 80 80 aa

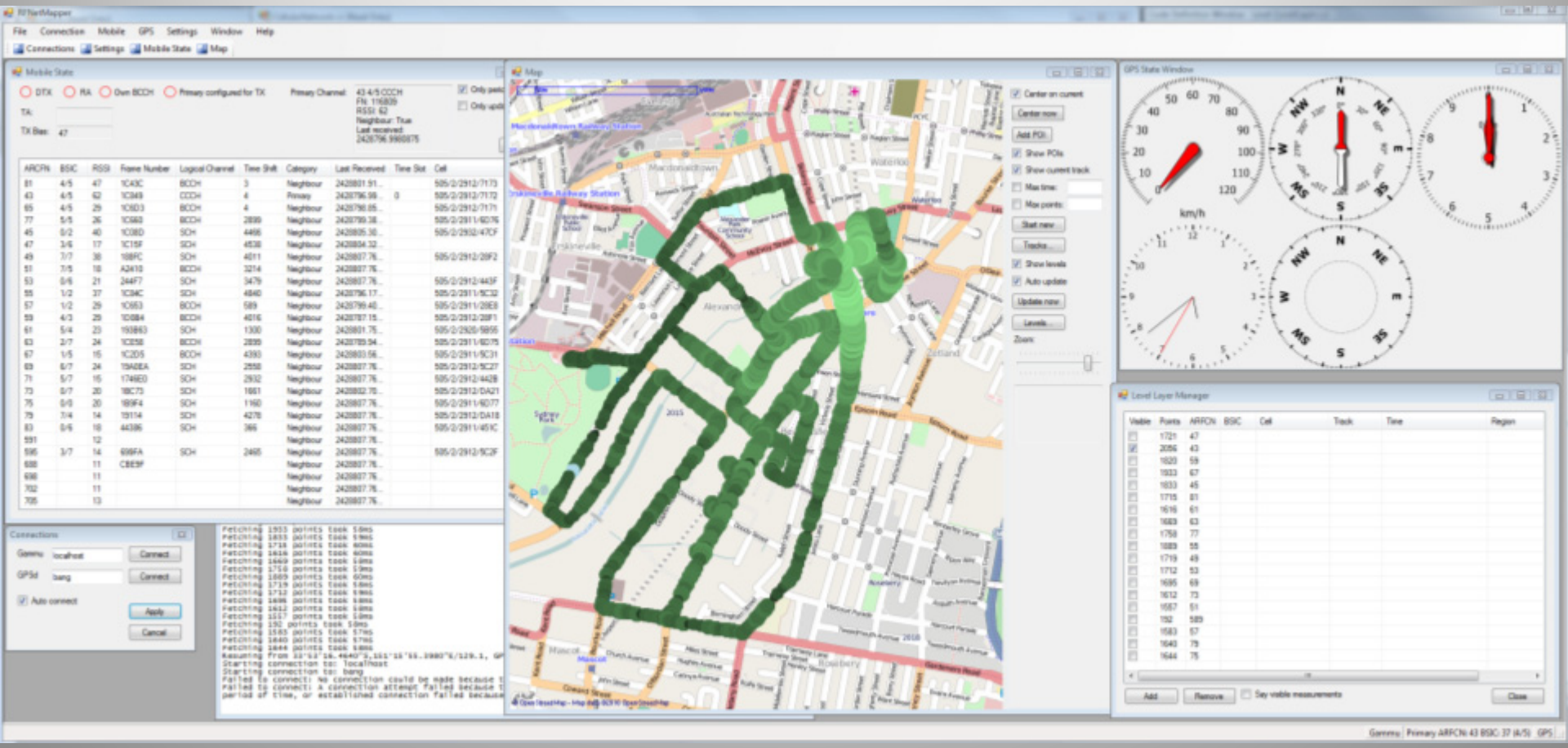


ARCFN	BSIC	RSSI	Frame Number	Logical Channel	Time Shift	Category	Last Received	Time Slot	Cell
55	1/2	36	255D60	SCH	3215	Neighbour	356545.888...		
43	4/5	66	2562F1	CCCH	3215	Primary	356540.245...	0	505/2/2912/7172
63	2/7	58	33D5A	SCH	2603	Neighbour	356552.734...		505/2/2911/6D75
77	5/5	53	33D8D	SCH	2603	Neighbour	356552.362...		505/2/2911/6D76
81	4/5	45	1AF92A	SCH	2	Neighbour	356551.697...		505/2/2912/7173
65	4/5	51	1AF8C4	SCH	1	Neighbour	356552.182...		?/?/?/?
59	4/3	45	79399	SCH	4423	Neighbour	356551.932...		505/2/2912/28F1
75	0/0	40	33E26	SCH	2604	Neighbour	356551.529...		505/2/2911/6D77
57	5/3	36	255578	SCH	3766	Neighbour	356555.969...		
69	6/7	40	9B6E4	SCH	3023	Neighbour	356551.852...		505/2/2912/5C27
67	1/5	36	781DE	SCH	4847	Neighbour	356622.308...		
49	7/7	35	177112	SCH	4428	Neighbour	356622.308...		505/2/2912/28F2
61		37	24C2C8	SCH	4725	Neighbour	356622.308...		
47		38	24E2B8	SCH	2506	Neighbour	356622.308...		
45		37	1524DC	SCH	3479	Neighbour	356622.308...		
51		30				Neighbour	356622.308...		
53		33				Neighbour	356622.308...		
71		31				Neighbour	356622.308...		
73		37				Neighbour	356622.308...		
79		31				Neighbour	356622.308...		
83		29				Neighbour	356622.308...		
591		19					356626.177...		
595	3/7	31	396CD	SCH	2878		356551.106...		
688		14					356626.177...		
698		15					356626.177...		
702		14					356626.177...		
705		28					356626.177...		

Geolocation with GSM



RFNetMapper



Determine accuracy by comparing to ground truth: where are the base stations?

ACMA RadCom Web Interface

acma.gov.au

Register of Radiocommunications Licences

Found **10526** sites within about a **200 kms** radius of: **Latitude: -34 17 47.782 Longitude: 150 56 20.778**.
Coordinate Projection: Australian Geodetic Datum 1966 [AGD66]
[List Nearby Sites] [New Site Search]

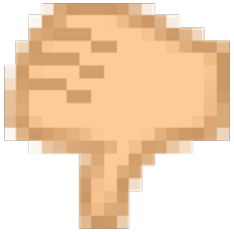
Pan 3 4 5 6 Zoom IN OUT

Site:
Approx distance:

Refine Search

Show Site names	☐				
Show ACMA mapgrid	☐				
Radius/Zoom	200 kms				
Latitude	D -34	M 17	S 47.782		
Longitude	D 150	M 56	S 20.778		
Go	[Use Degrees Decimal]				

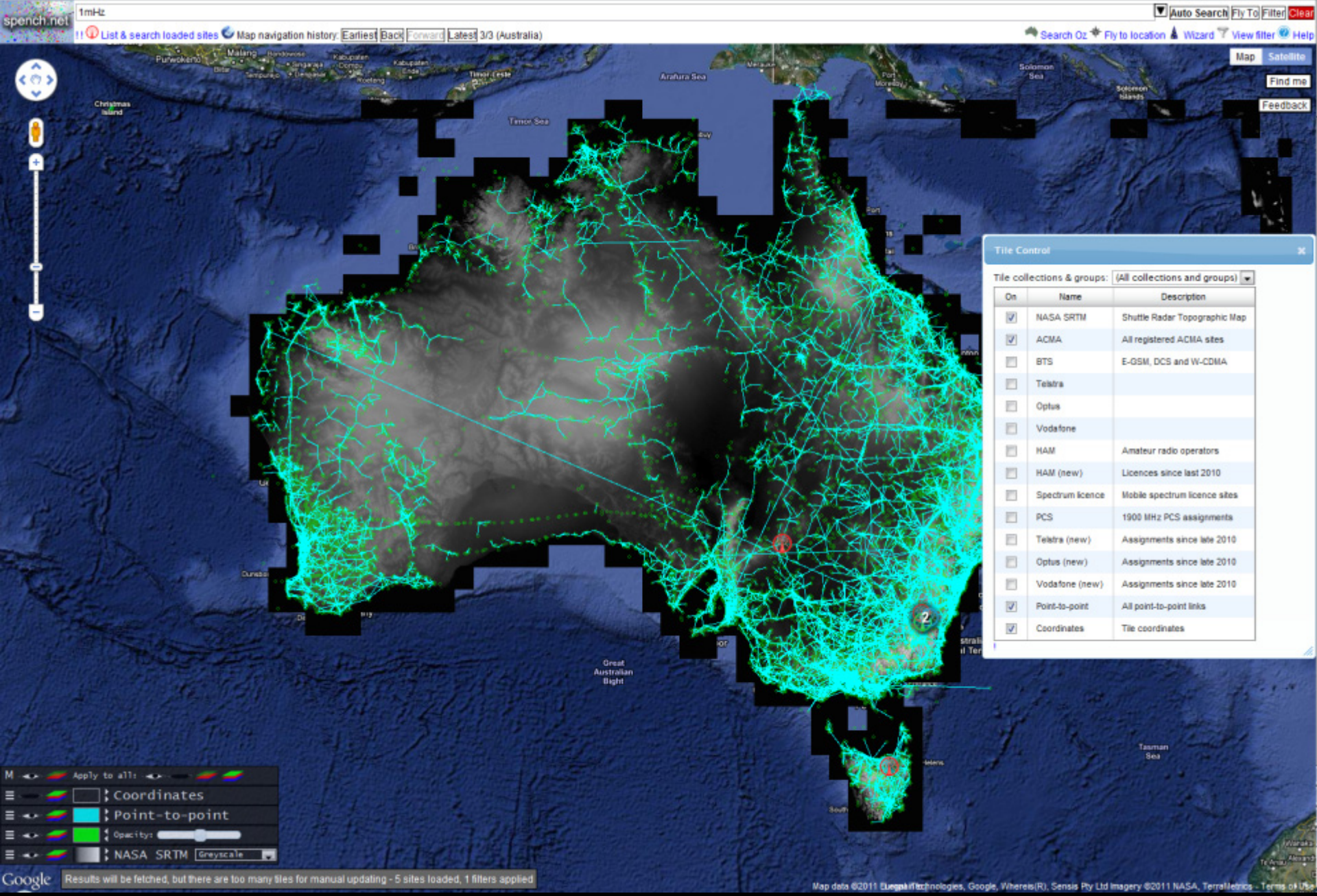
Parsing Error
tion: http://we
Number 9, Col



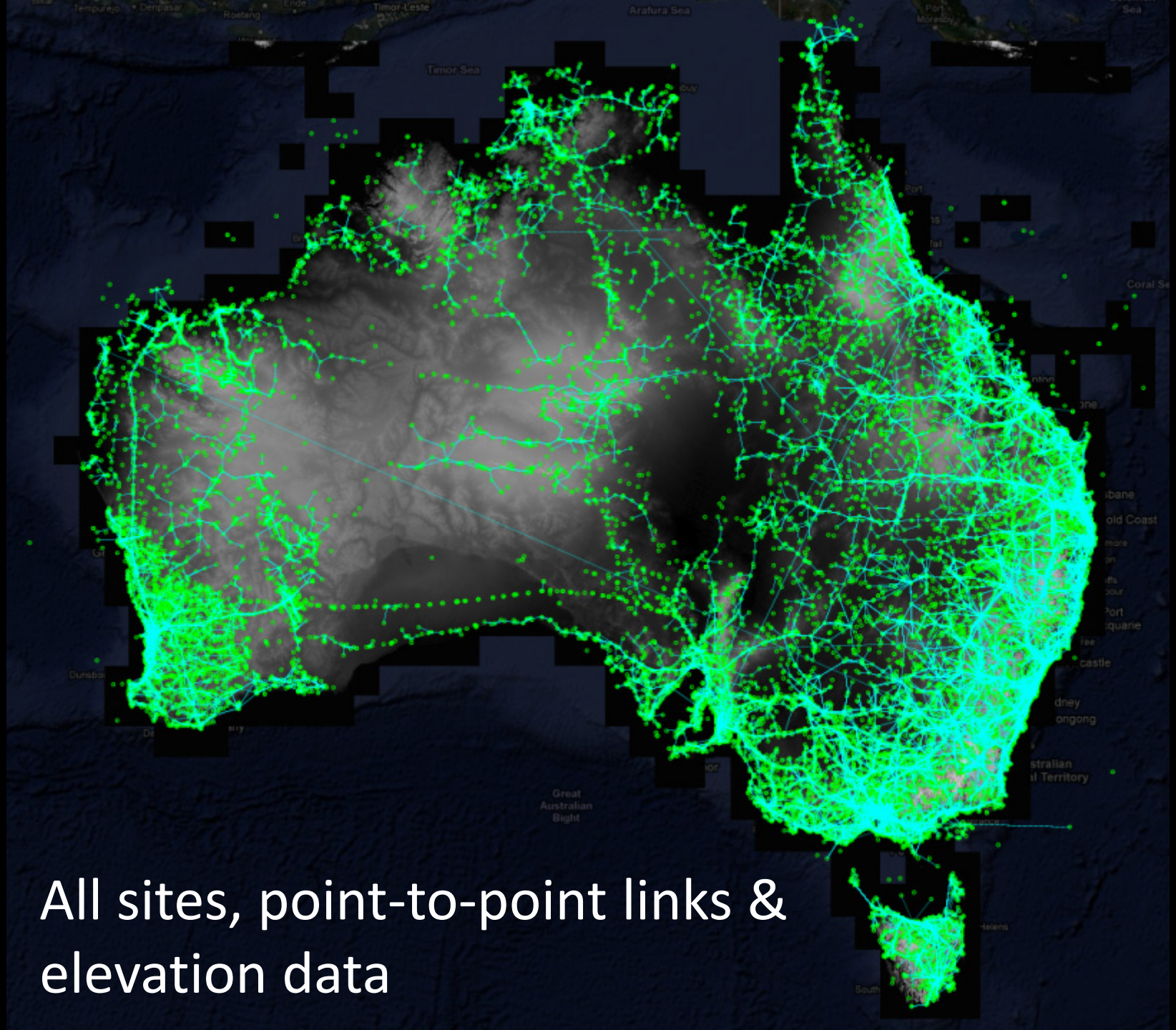
Site proximity usage notes;

- Map display accuracy within 10 metres.
- Distances shown are approximations only (they are not latitude compensated).
- To view images correclty, browser's must be able to accept both Javascript and compressed SVG content.
- You can **download** the SVG viewer Ver 3.0 from Adobe to view site search results.
- If you do not wish to install the SVG viewer, the List Nearby Sites link will display the results in table format.
- Use right mouse button for additional SVG pan and zoom functions.
- GMDA 1M 2001 and MAPDATA-2.5M data © Commonwealth of Australia (AUSLIG) 2001.

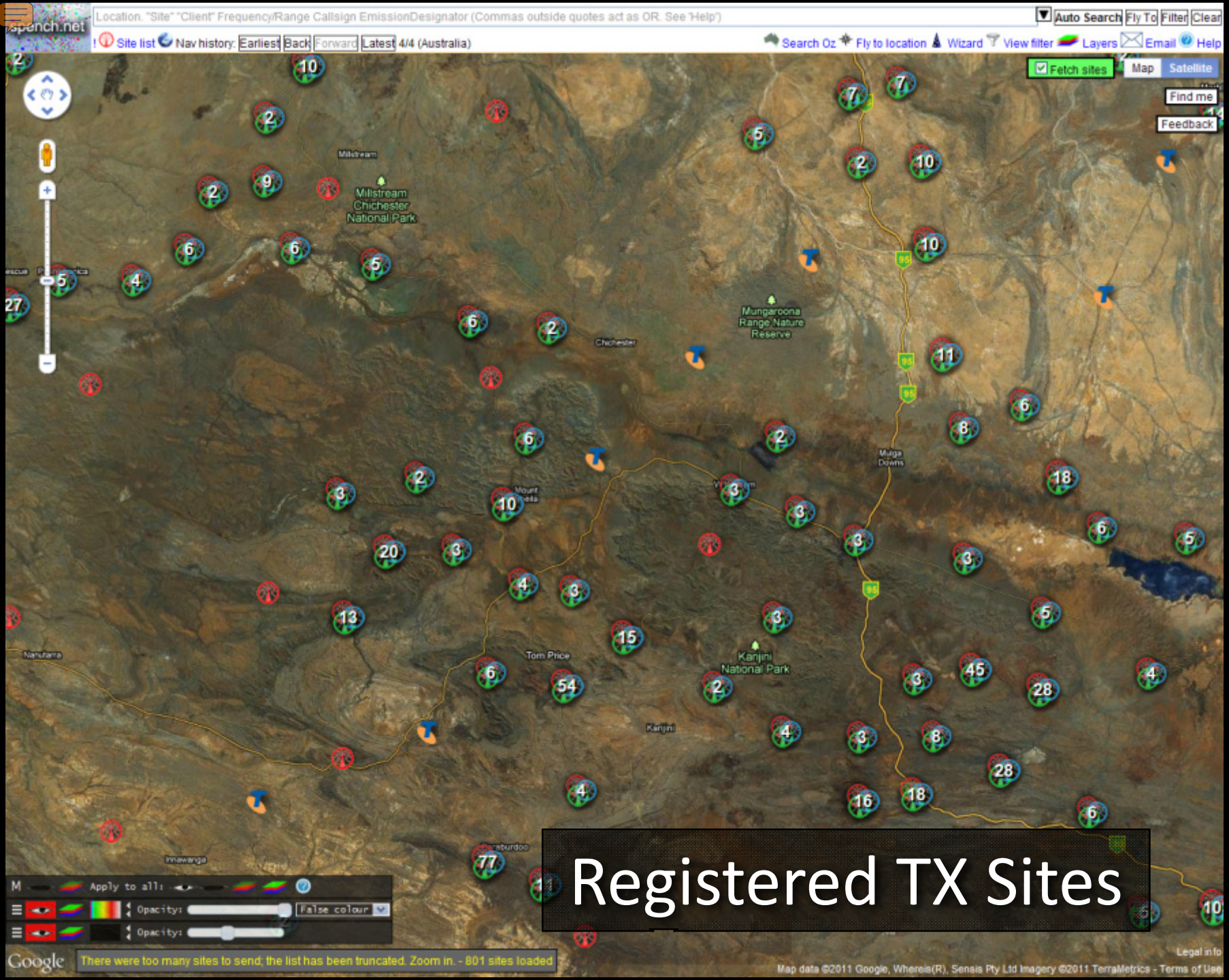
Enter RFMap…



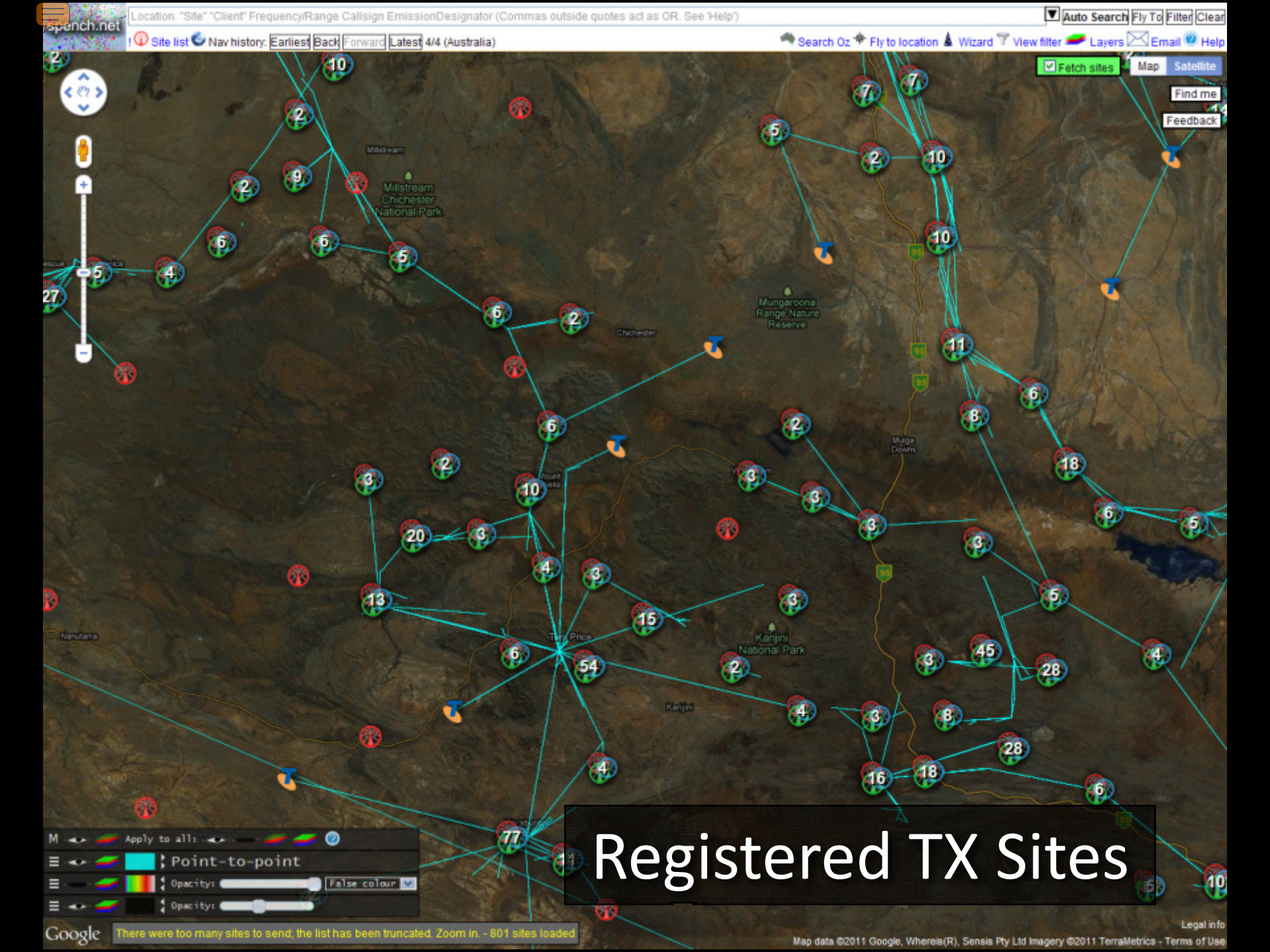
The RFMap web interface



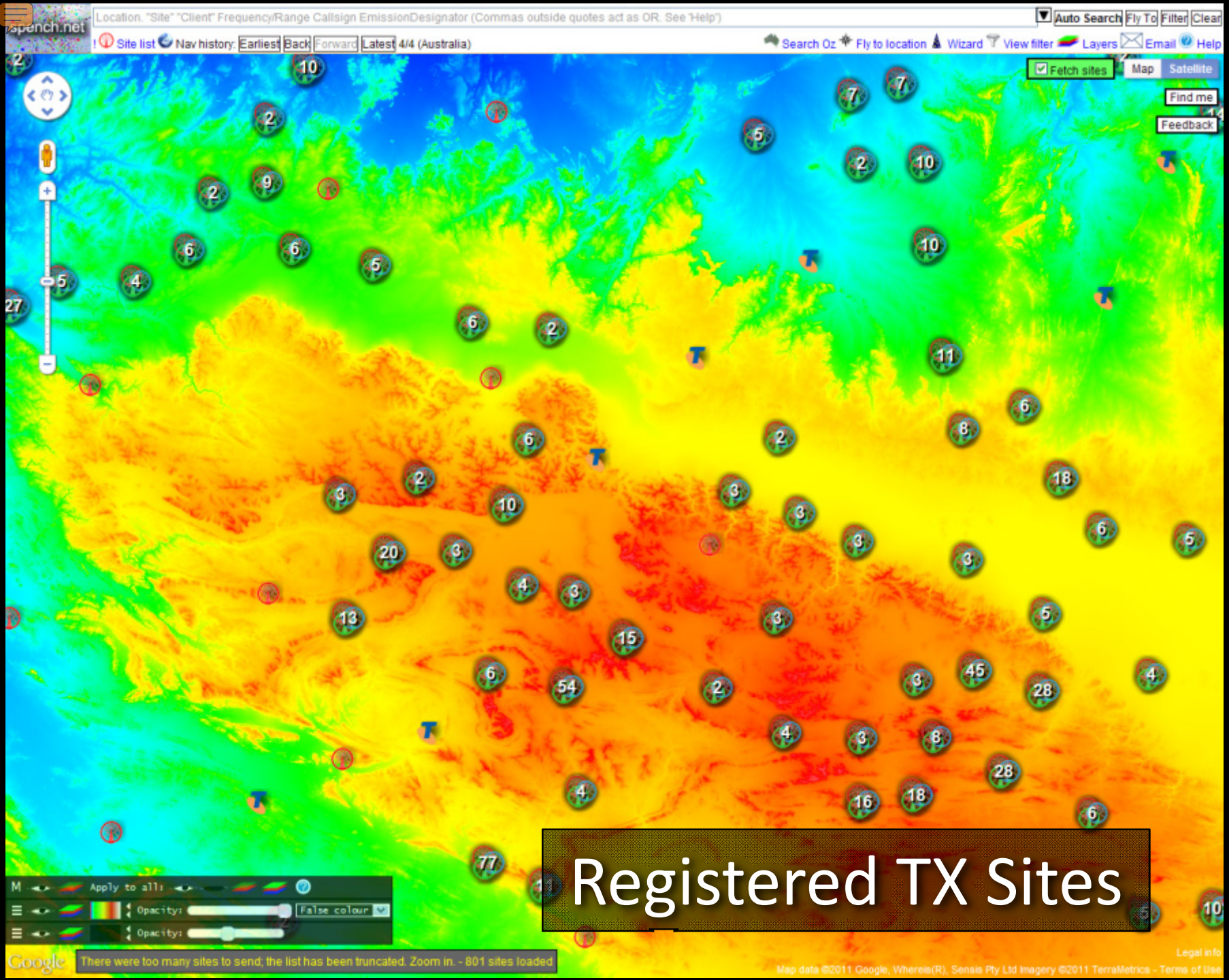
All sites, point-to-point links & elevation data

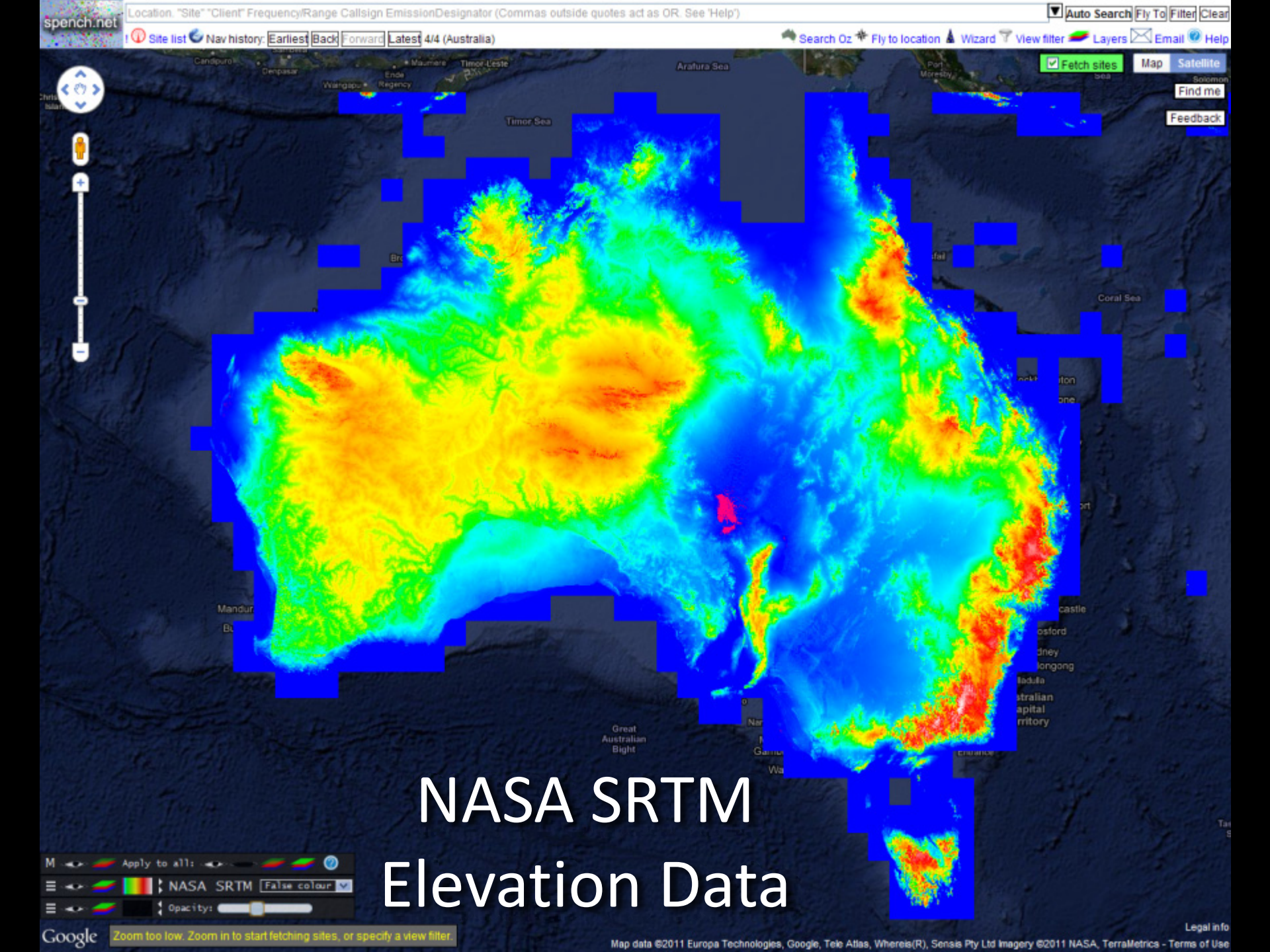


Registered TX Sites

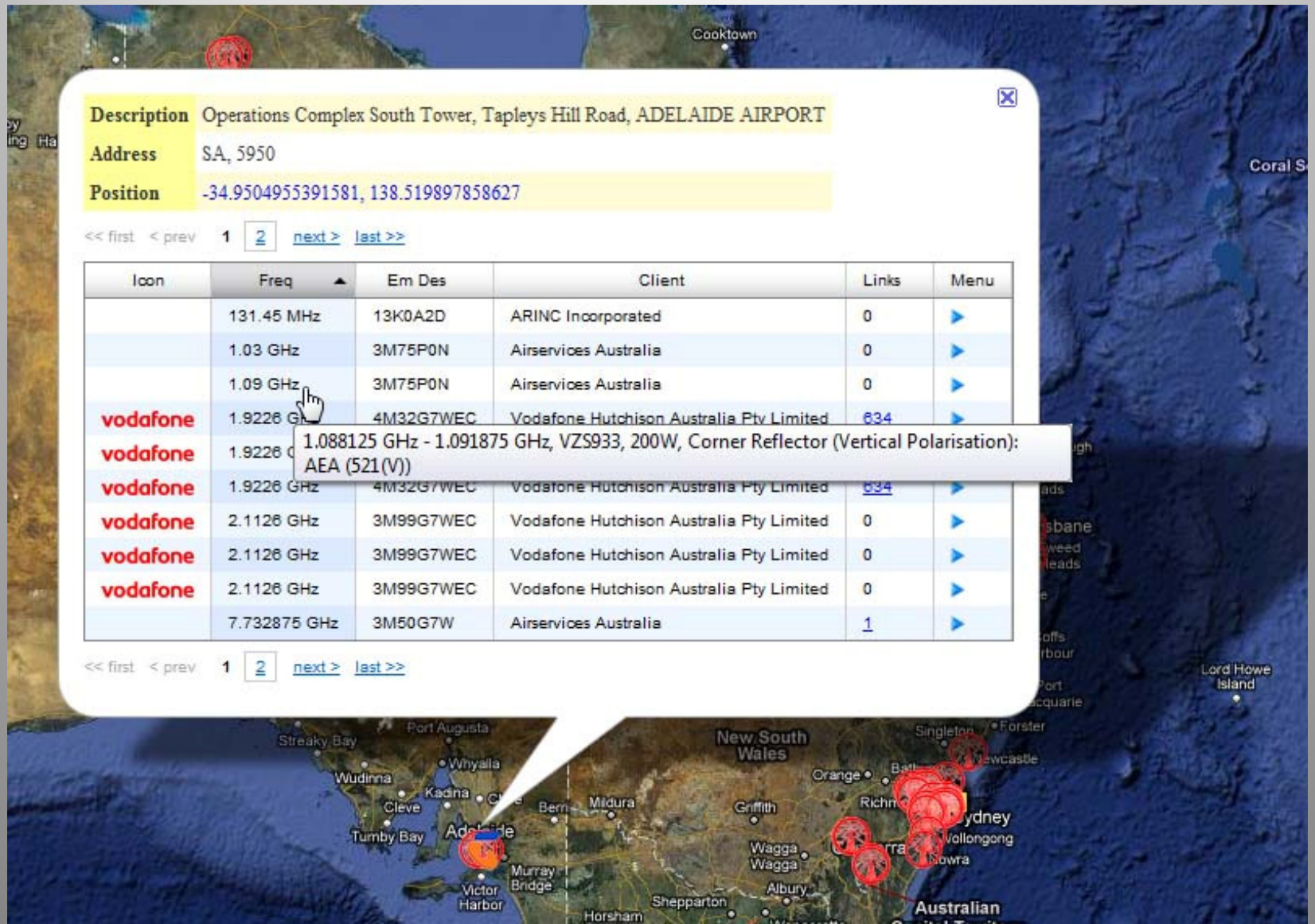


Registered TX Sites

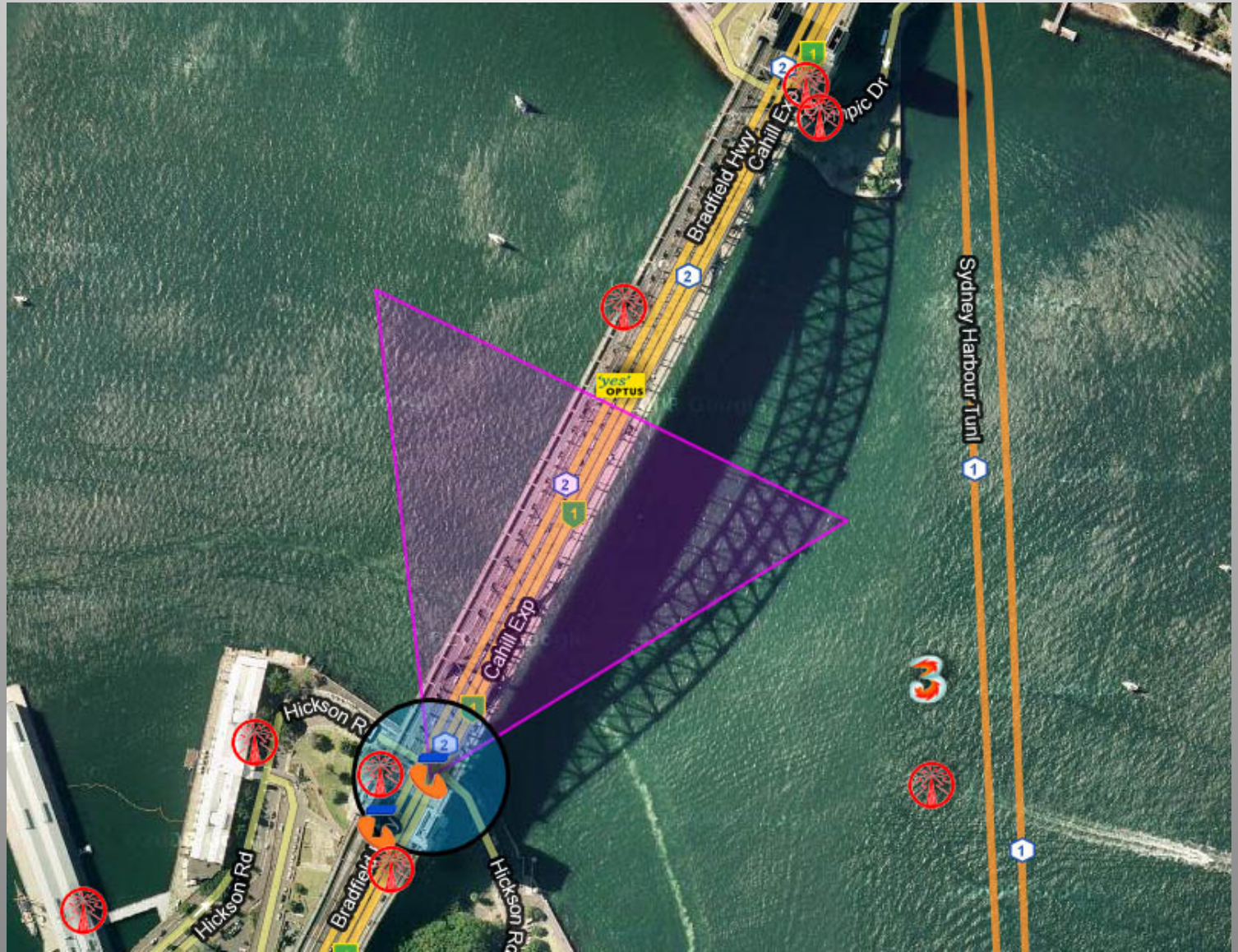

Location, "Site" "Client" Frequency/Range Callsign EmissionDesignator (Commas outside quotes act as OR. See 'Help')
Auto Search
Fly To
Filter
Clear
Site list
Nav history:
Earliest
Back
Forward
Latest
4/4 (Australia)
Search Oz
Fly to location
Wizard
View filter
Layers
Email
Help
Fetch sites
Map
Satellite
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
Legal info
Map data ©2011 Google, Whereis(R), Sensis Pty Ltd Imagery ©2011 TerraMetrics - Terms of Use
Registered TX Sites

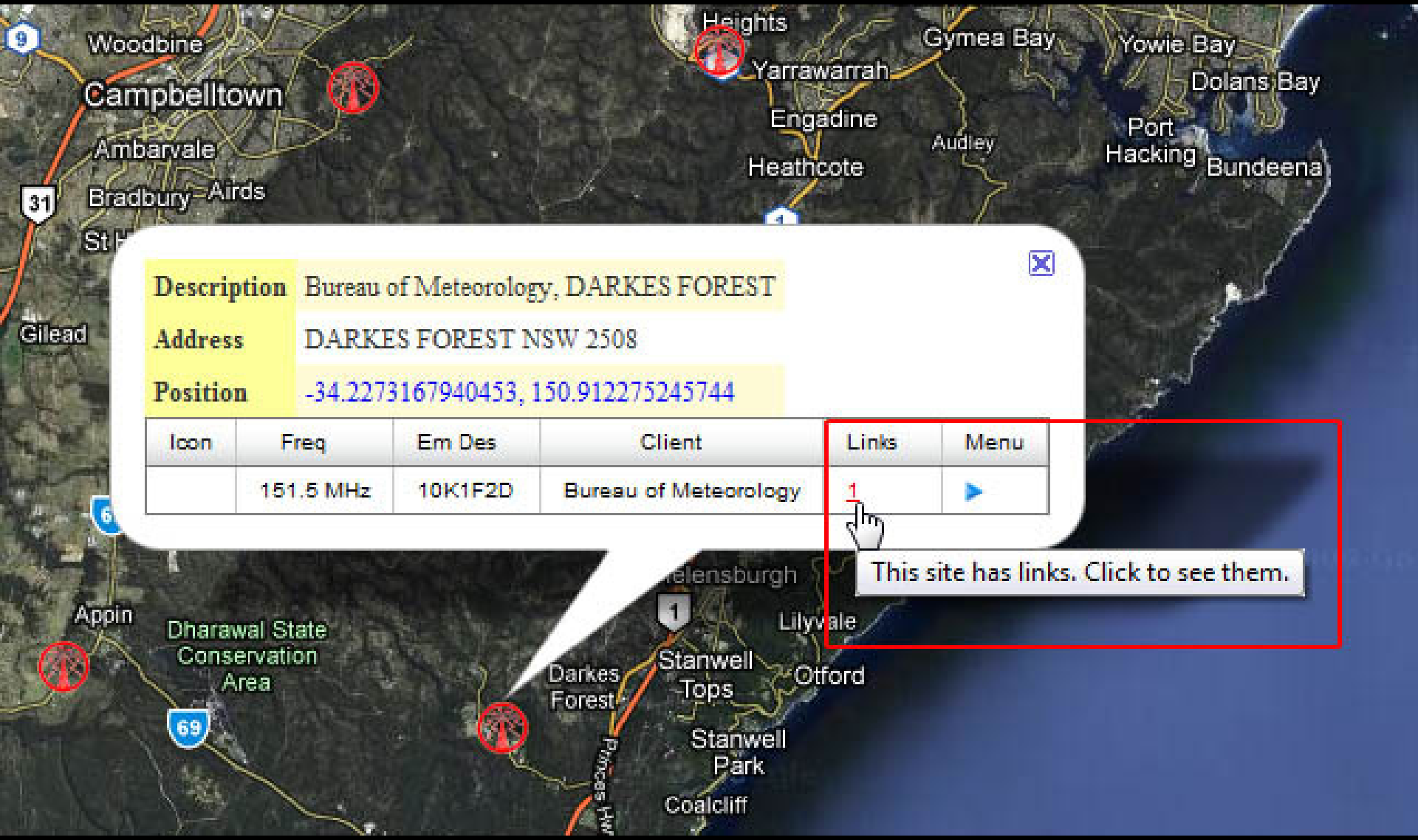

spench.net
Location. "Site" "Client" Frequency/Range Callsign EmissionDesignator (Commas outside quotes act as OR. See 'Help')
Auto Search
Fly To
Filter
Clear
Site list
Nav history:
Earliest
Back
Forward
Latest
4/4 (Australia)
Search Oz
Fly to location
Wizard
View filter
Layers
Email
Help
Fetch sites
Map
Satellite
Find me
Feedback
Timor Sea
Arafura Sea
Coral Sea
Great Australian Bight
NASA SRTM
Elevation Data
Apply to all:
NASA SRTM
False colour
Opacity:
Google
Zoom too low. Zoom in to start fetching sites, or specify a view filter.
Legal info
Map data ©2011 Europa Technologies, Google, Tele Atlas, Whereis(R), Sensis Pty Ltd Imagery ©2011 NASA, TerraMetrics - Terms of Use

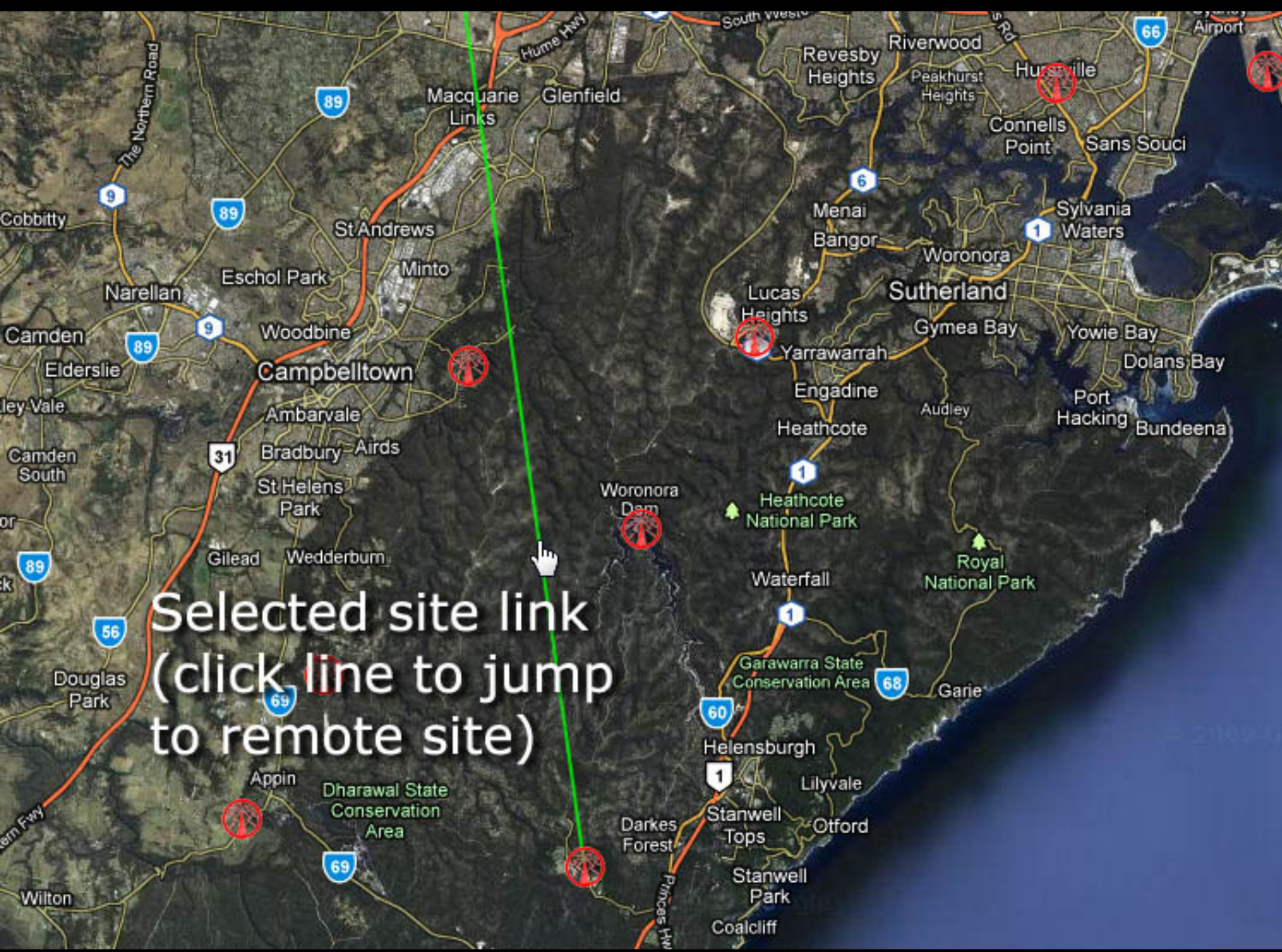
Site details: frequency assignments

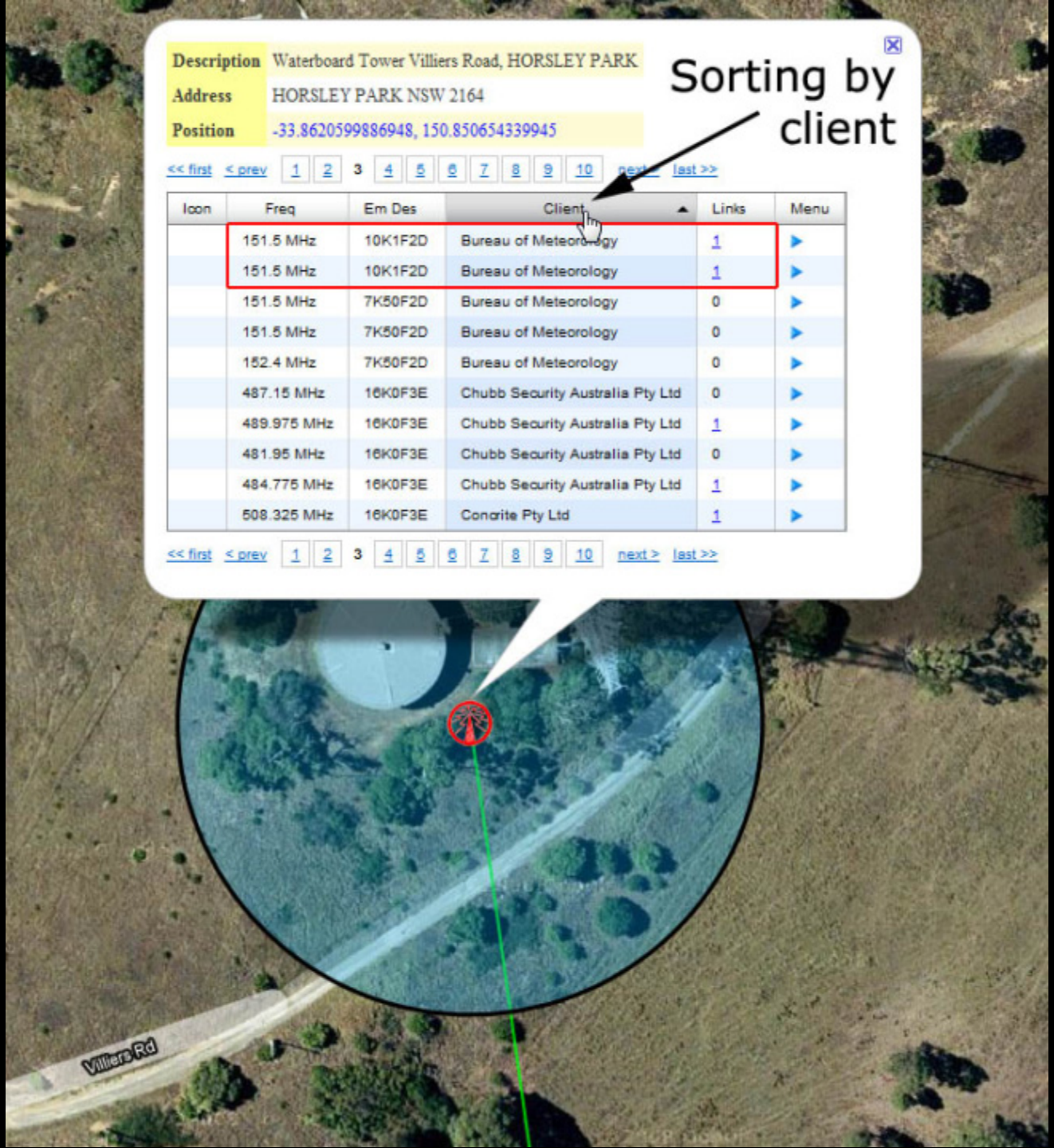


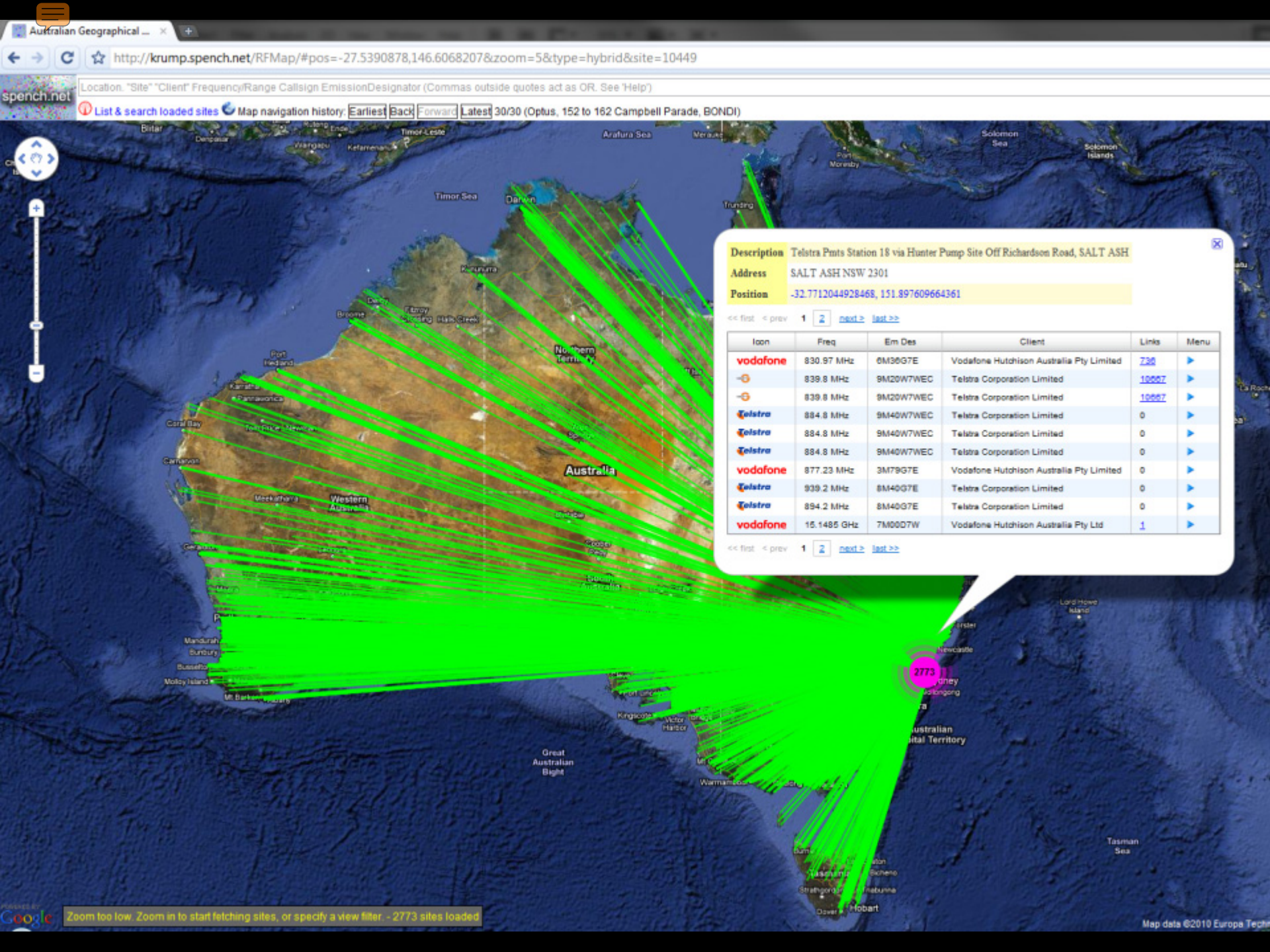
Antenna radiation pattern*

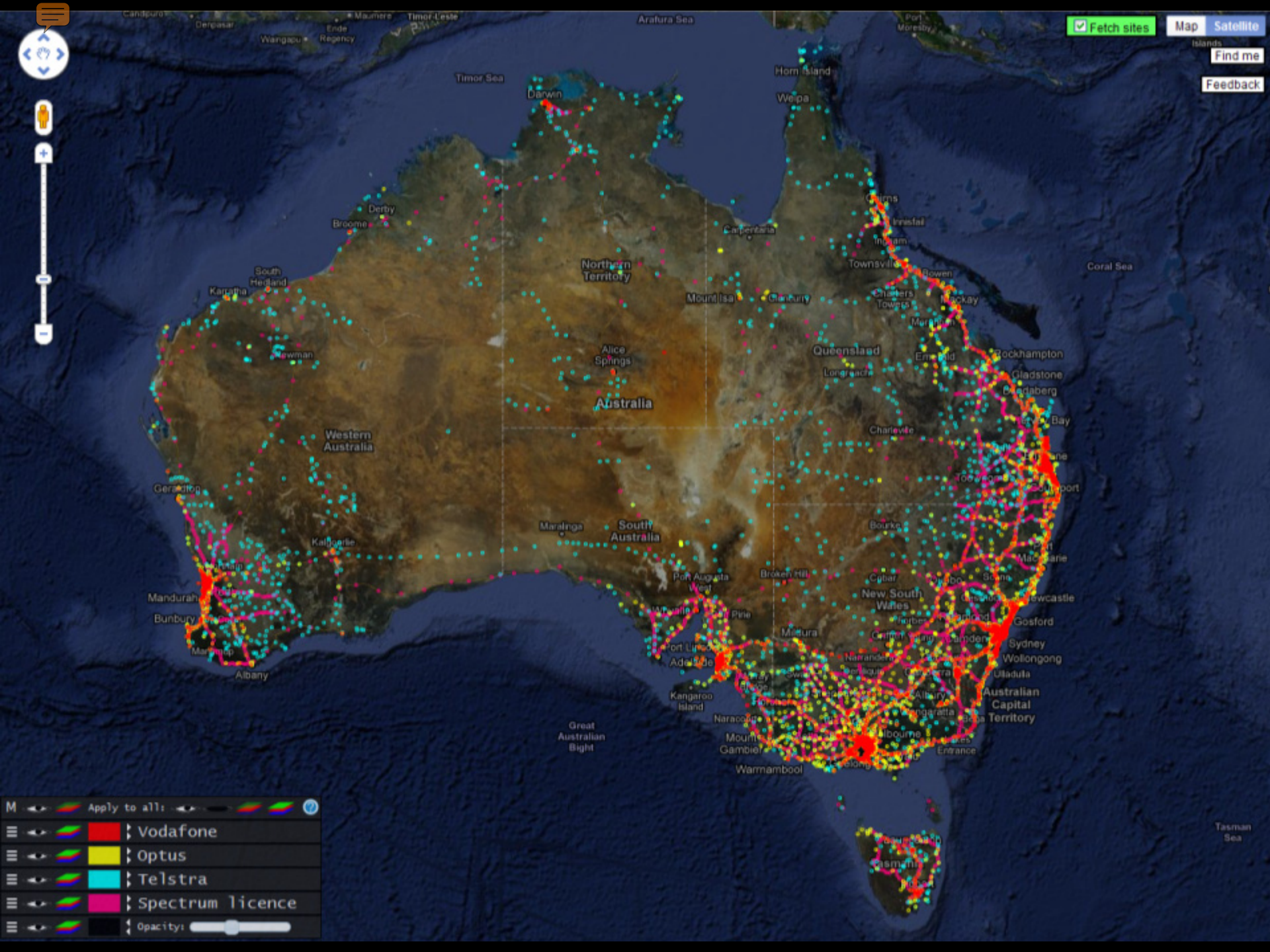


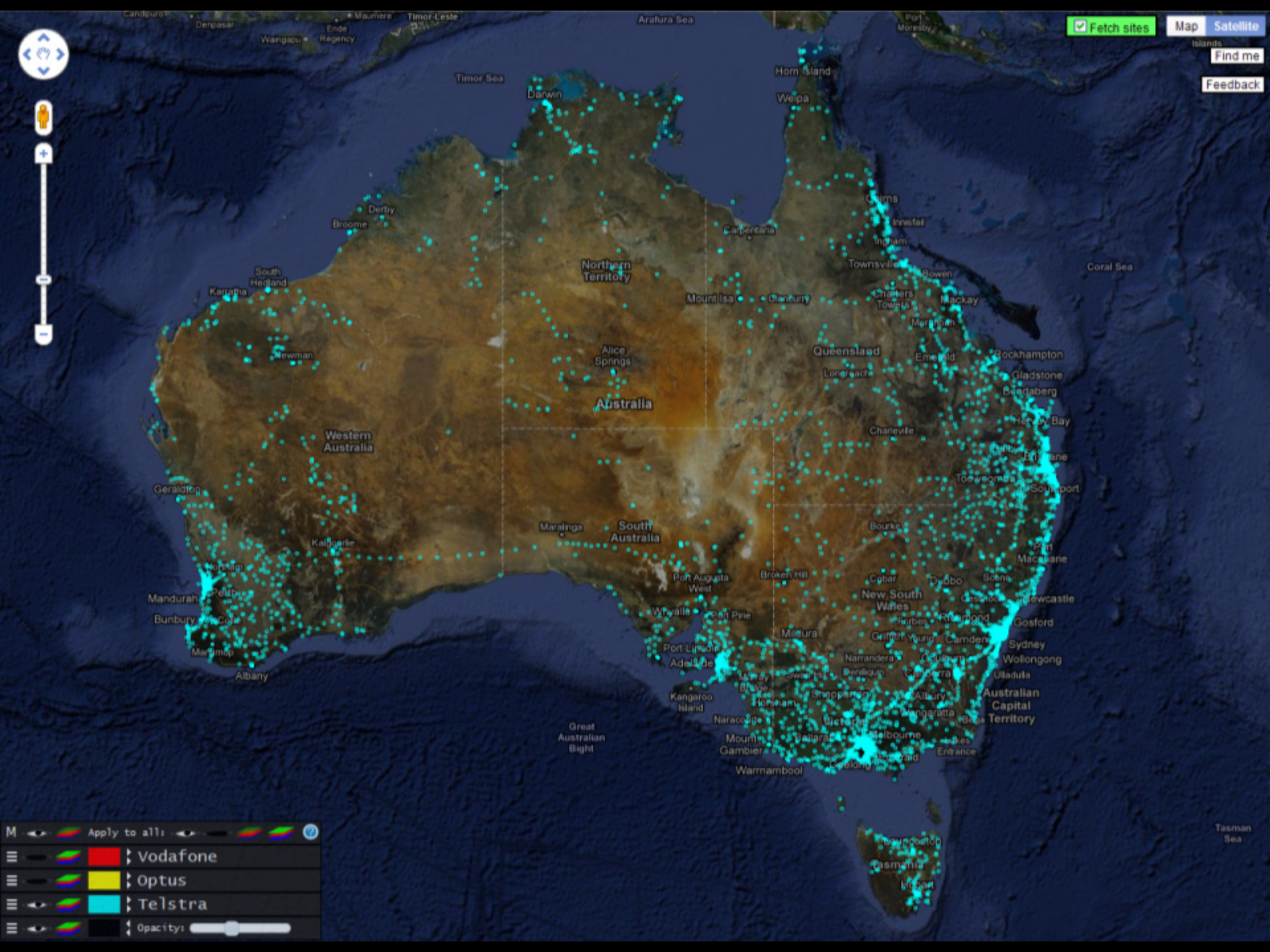

Heights
Gymea Bay
Yowie Bay
Yarrawarrah
Dolans Bay
Campbelltown
Engadine
Port Hacking
Ambarvale
Audley
Bundeena
Heathcote
Bradbury
Airds
Description
Bureau of Meteorology, DARKES FOREST
Address
DARKES FOREST NSW 2508
Position
-34.2273167940453, 150.912275245744
Icon
Freq
Em Des
Client
Links
Menu
151.5 MHz
10K1F2D
Bureau of Meteorology
1
This site has links. Click to see them.
Gilead
Appin
Dharawal State Conservation Area
Darkes Forest
Stanwell Tops
Otford
Lilyvale
Stanwell Park
Coalcliff

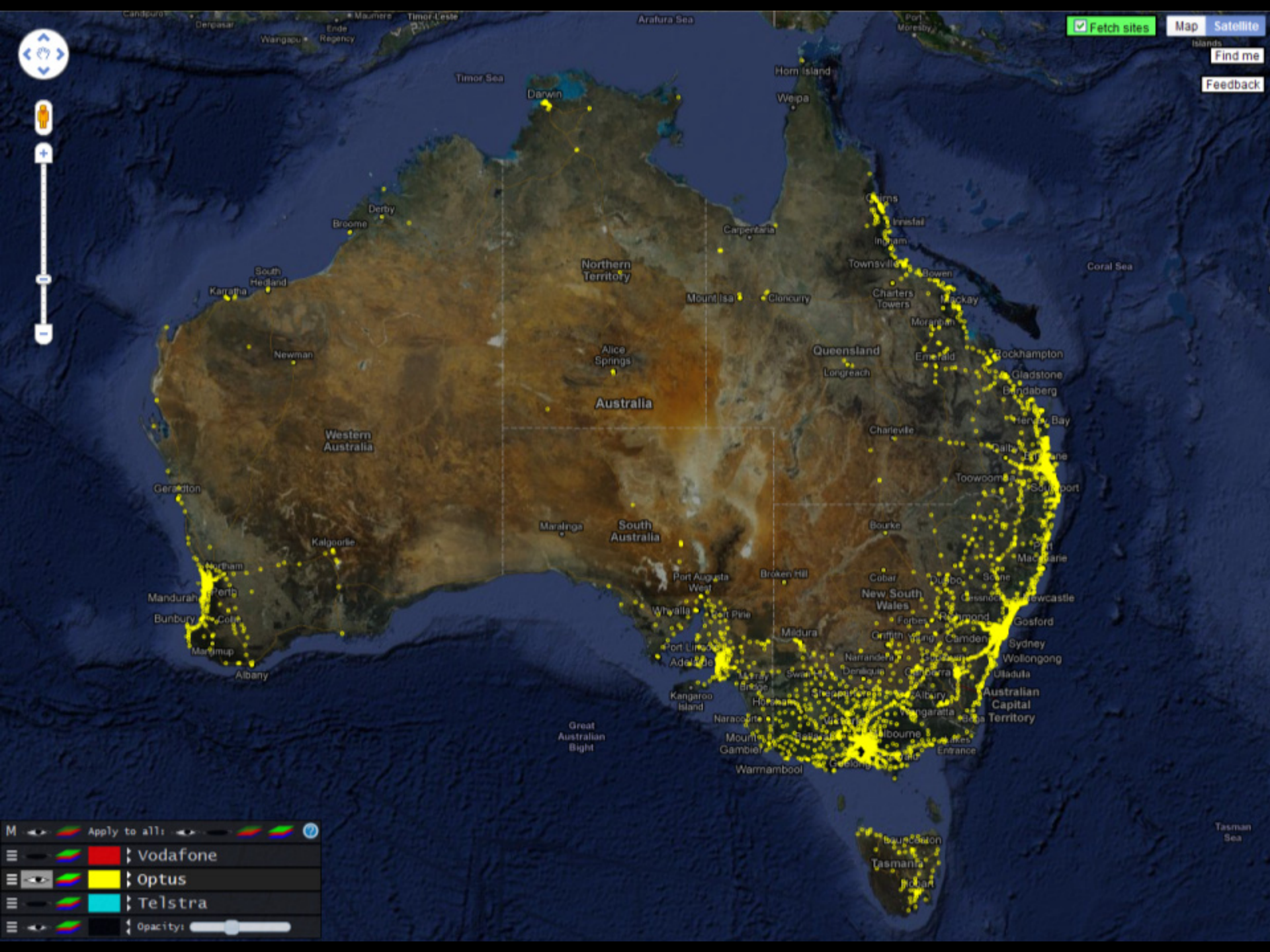

Selected site link
(click line to jump
to rembte site)
Macquarie Links
Glenfield
Revesby Heights
Riverwood
Peakhurst Heights
Connells Point
Sans Souci
Menai
Bangor
Sylvania Waters
Woronora
Sutherland
Lucas Heights
Gymea Bay
Yowie Bay
Dolans Bay
Yarrawarrah
Engadine
Heathcote
Audley
Port Hacking
Bundeena
Heathcote National Park
Royal National Park
Waterfall
Garawarra State Conservation Area
Garie
Helensburgh
Lilyvale
Stanwell Tops
Otford
Darkes Forest
Stanwell Park
Coalcliff
Cobbitty
Narellan
Camden
Elderslie
Eschol Park
St Andrews
Minto
Woodbine
Campbelltown
Ambarvale
Bradbury
Airds
St Helens Park
Gilead
Wedderburn
Camden South
Douglas Park
Appin
Dharawal State Conservation Area
Wilton
Woronora Dam
Hume Hwy
The Northern Road

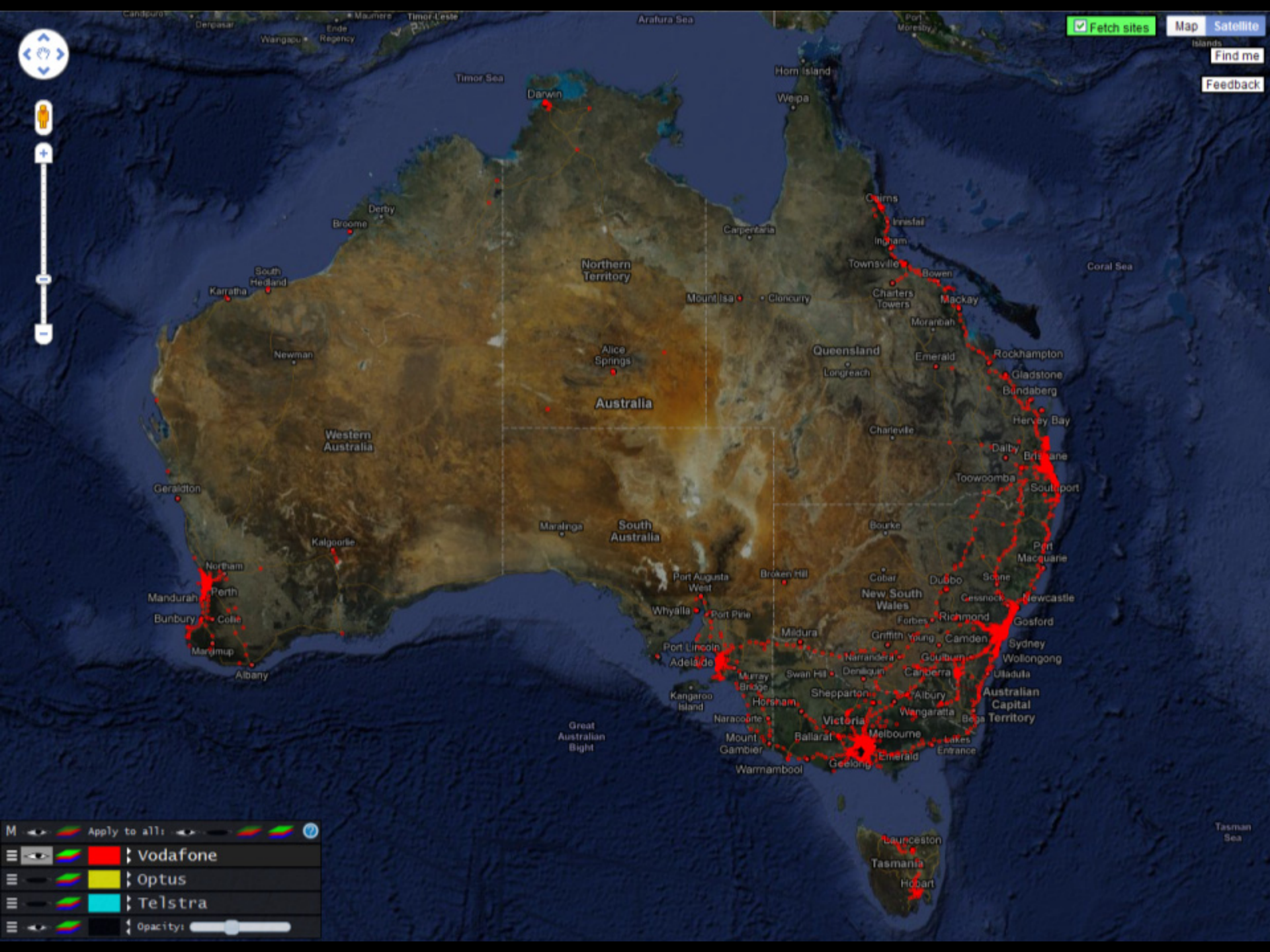

Description Waterboard Tower Villiers Road, HORSLEY PARK
Address HORSLEY PARK NSW 2164
Position -33.8620599886948, 150.850654339945
Sorting by client
<< first < prev 1 2 3 4 5 6 7 8 9 10 next > last >>
Icon | Freq | Em Des | Client | Links | Menu
151.5 MHz | 10K1F2D | Bureau of Meteorology | 1
151.5 MHz | 10K1F2D | Bureau of Meteorology | 1
151.5 MHz | 7K50F2D | Bureau of Meteorology | 0
151.5 MHz | 7K50F2D | Bureau of Meteorology | 0
152.4 MHz | 7K50F2D | Bureau of Meteorology | 0
487.15 MHz | 16K0F3E | Chubb Security Australia Pty Ltd | 0
489.975 MHz | 16K0F3E | Chubb Security Australia Pty Ltd | 1
481.95 MHz | 16K0F3E | Chubb Security Australia Pty Ltd | 0
484.775 MHz | 16K0F3E | Chubb Security Australia Pty Ltd | 1
508.325 MHz | 16K0F3E | Concrite Pty Ltd | 1
<< first < prev 1 2 3 4 5 6 7 8 9 10 next > last >>
Villiers Rd

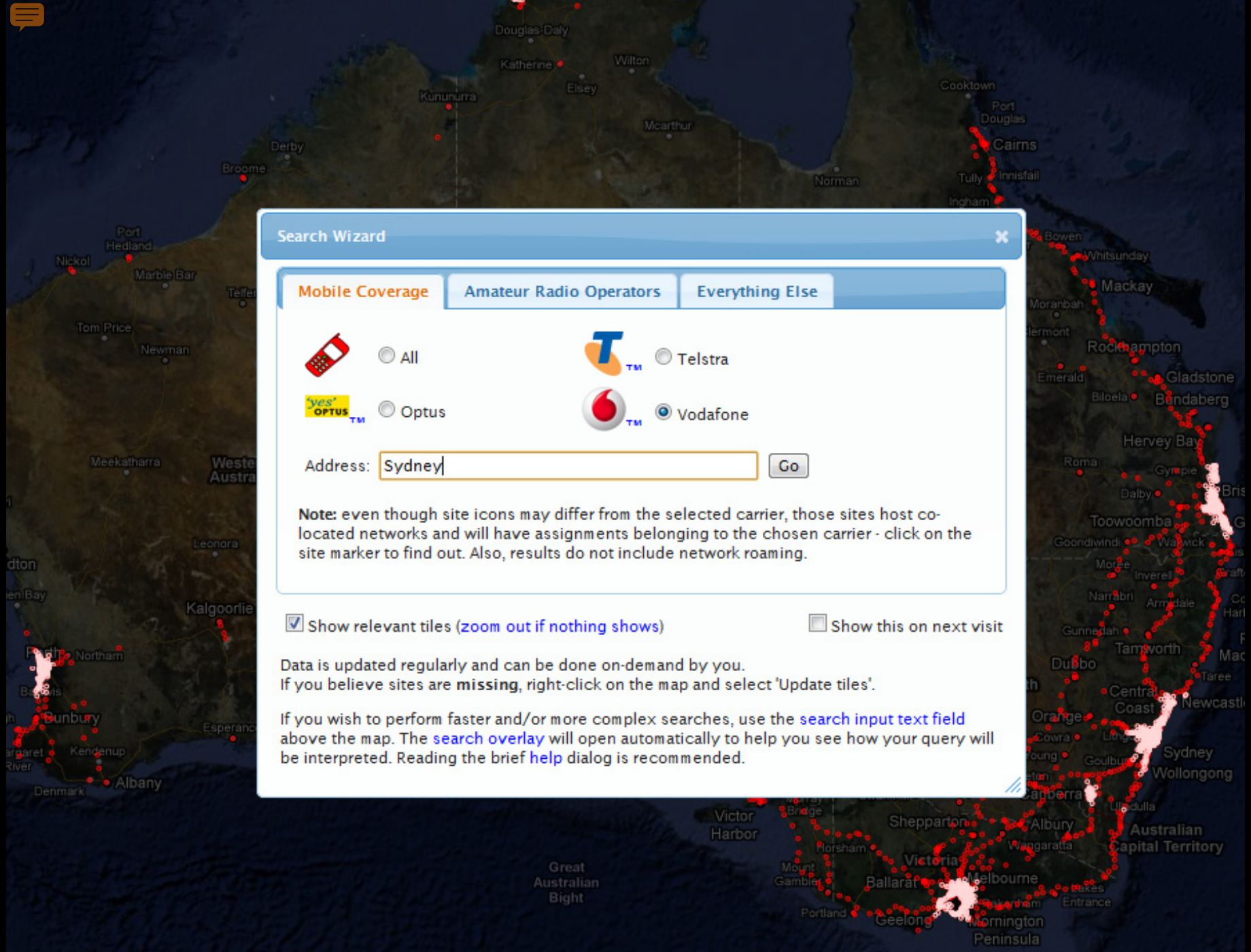

Australian Geographical ...
http://krump.spench.net/RFMap/#pos=-27.5390878,146.6068207&zoom=5&type=hybrid&site=10449
spench.net
Location, "Site" "Client" Frequency/Range Callsign EmissionDesignator (Commas outside quotes act as OR. See 'Help')
List & search loaded sites
Map navigation history: Earliest Back Forward Latest 30/30 (Optus, 152 to 162 Campbell Parade, BONDI)
Description Telstra Pmts Station 18 via Hunter Pump Site Off Richardson Road, SALT ASH
Address SALT ASH NSW 2301
Position -32.7712044928468, 151.897609664361
<< first < prev 1 2 next > last >>
Icon Freq Em Des Client Links Menu
vodafone 830.97 MHz 6M36G7E Vodafone Hutchison Australia Pty Limited 736
839.8 MHz 9M20W7WEC Telstra Corporation Limited 10667
839.8 MHz 9M20W7WEC Telstra Corporation Limited 10667
884.8 MHz 9M40W7WEC Telstra Corporation Limited 0
884.8 MHz 9M40W7WEC Telstra Corporation Limited 0
884.8 MHz 9M40W7WEC Telstra Corporation Limited 0
vodafone 877.23 MHz 3M79G7E Vodafone Hutchison Australia Pty Limited 0
939.2 MHz 8M40G7E Telstra Corporation Limited 0
894.2 MHz 8M40G7E Telstra Corporation Limited 0
vodafone 15.1485 GHz 7M00D7W Vodafone Hutchison Australia Pty Ltd 1
<< first < prev 1 2 next > last >>
Australia
Timor Sea
Arafura Sea
Great Australian Bight
Tasman Sea
2773
Zoom too low. Zoom in to start fetching sites, or specify a view filter. - 2773 sites loaded
Map data ©2010 Europa Tech

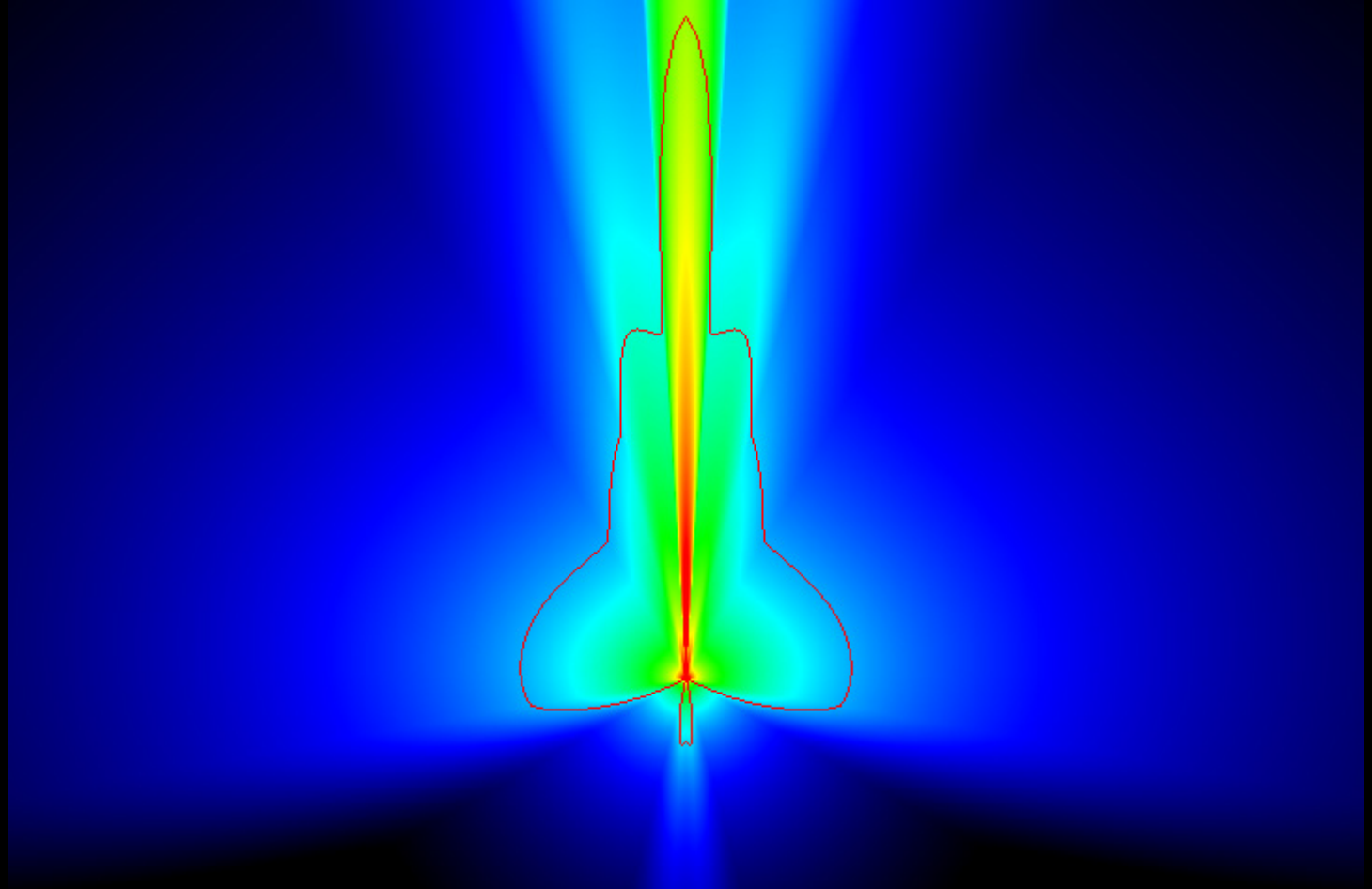

Fetch sites
Map
Satellite
Find me
Feedback
Apply to all:
Vodafone
Optus
Telstra
Spectrum licence
Opacity:
Australia
Northern Territory
Queensland
Western Australia
South Australia
New South Wales
Australian Capital Territory
Darwin
Perth
Adelaide
Sydney
Melbourne
Brisbane
Coral Sea
Tasman Sea
Great Australian Bight
Timor Sea
Arafura Sea


Fetch sites
Map
Satellite
Find me
Feedback
Apply to all:
Vodafone
Optus
Telstra
Opacity:
Darwin
Alice Springs
Perth
Adelaide
Brisbane
Sydney
Melbourne
Canberra
Hobart
Northern Territory
Western Australia
South Australia
Queensland
New South Wales
Australian Capital Territory
Tasmania
Coral Sea
Tasman Sea
Great Australian Bight
Timor Sea
Arafura Sea


Fetch sites
Map
Satellite
Find me
Feedback
Australia
Northern Territory
Western Australia
South Australia
Queensland
New South Wales
Australian Capital Territory
Tasmania
Coral Sea
Timor Sea
Arafura Sea
Great Australian Bight
Tasman Sea
Darwin
Alice Springs
Perth
Adelaide
Brisbane
Sydney
Melbourne
Canberra
Apply to all:
Vodafone
Optus
Telstra
Opacity:

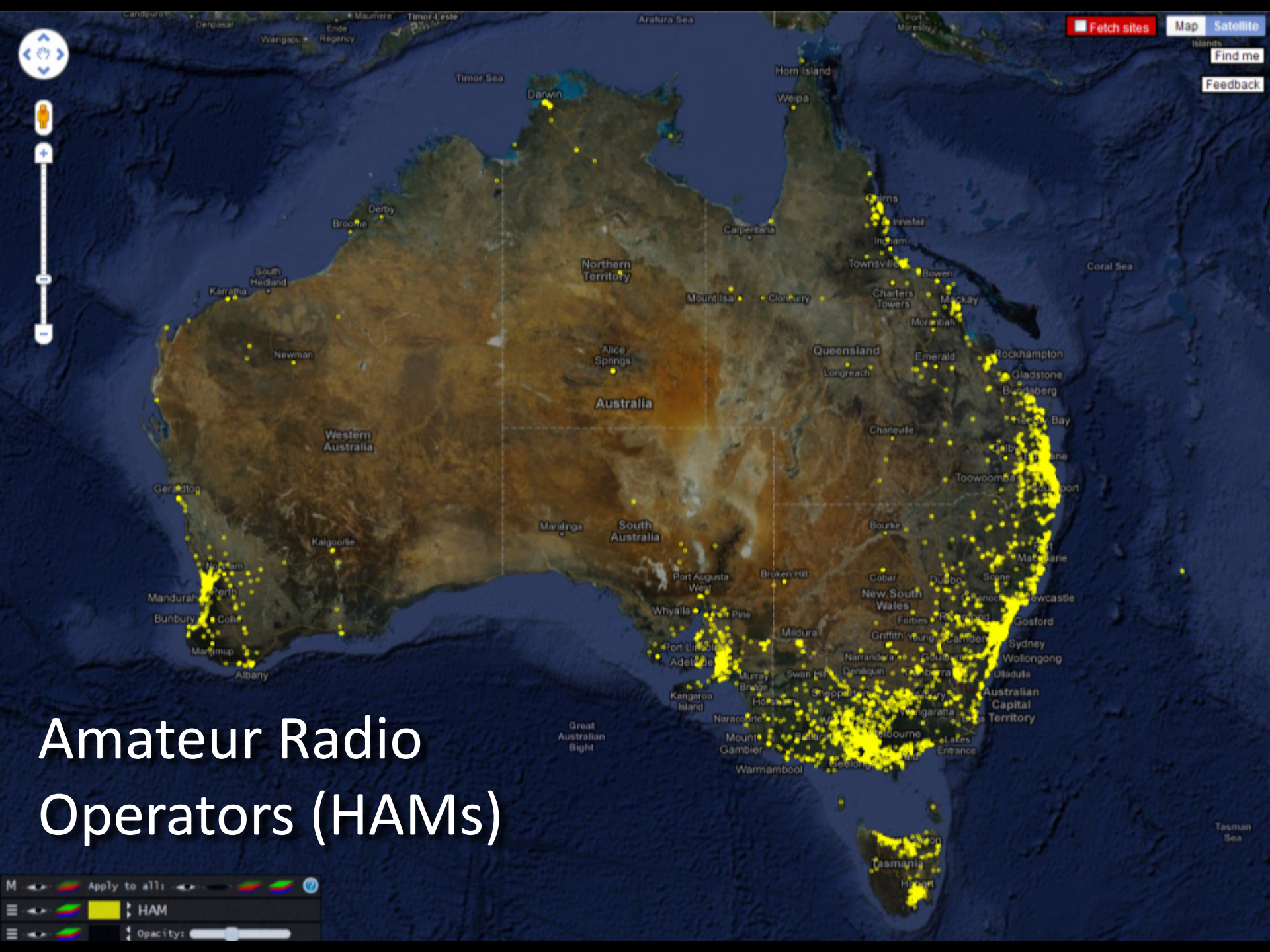

Fetch sites
Map
Satellite
Find me
Feedback
Apply to all:
Vodafone
Optus
Telstra
Opacity:
Australia
Northern Territory
Western Australia
South Australia
Queensland
New South Wales
Victoria
Australian Capital Territory
Tasmania
Darwin
Perth
Adelaide
Brisbane
Sydney
Melbourne
Canberra
Coral Sea
Tasman Sea
Great Australian Bight
Timor Sea
Arafura Sea


Search Wizard
Mobile Coverage
Amateur Radio Operators
Everything Else
All
Telstra
Optus
Vodafone
Address: Sydney
Go
Note: even though site icons may differ from the selected carrier, those sites host co-located networks and will have assignments belonging to the chosen carrier - click on the site marker to find out. Also, results do not include network roaming.
Show relevant tiles (zoom out if nothing shows)
Show this on next visit
Data is updated regularly and can be done on-demand by you.
If you believe sites are missing, right-click on the map and select 'Update tiles'.
If you wish to perform faster and/or more complex searches, use the search input text field above the map. The search overlay will open automatically to help you see how your query will be interpreted. Reading the brief help dialog is recommended.

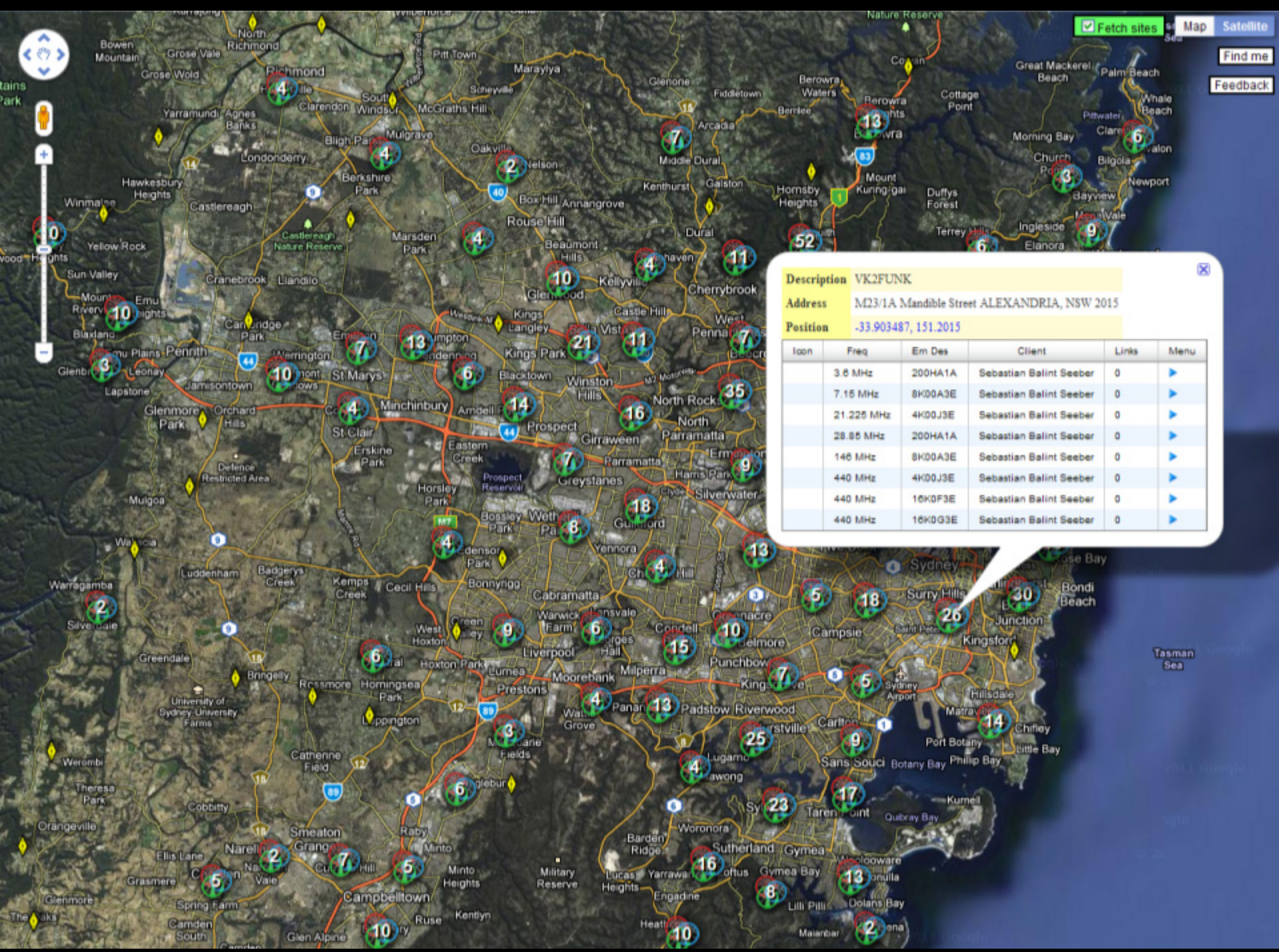


Antenna
Radiation
Envelope

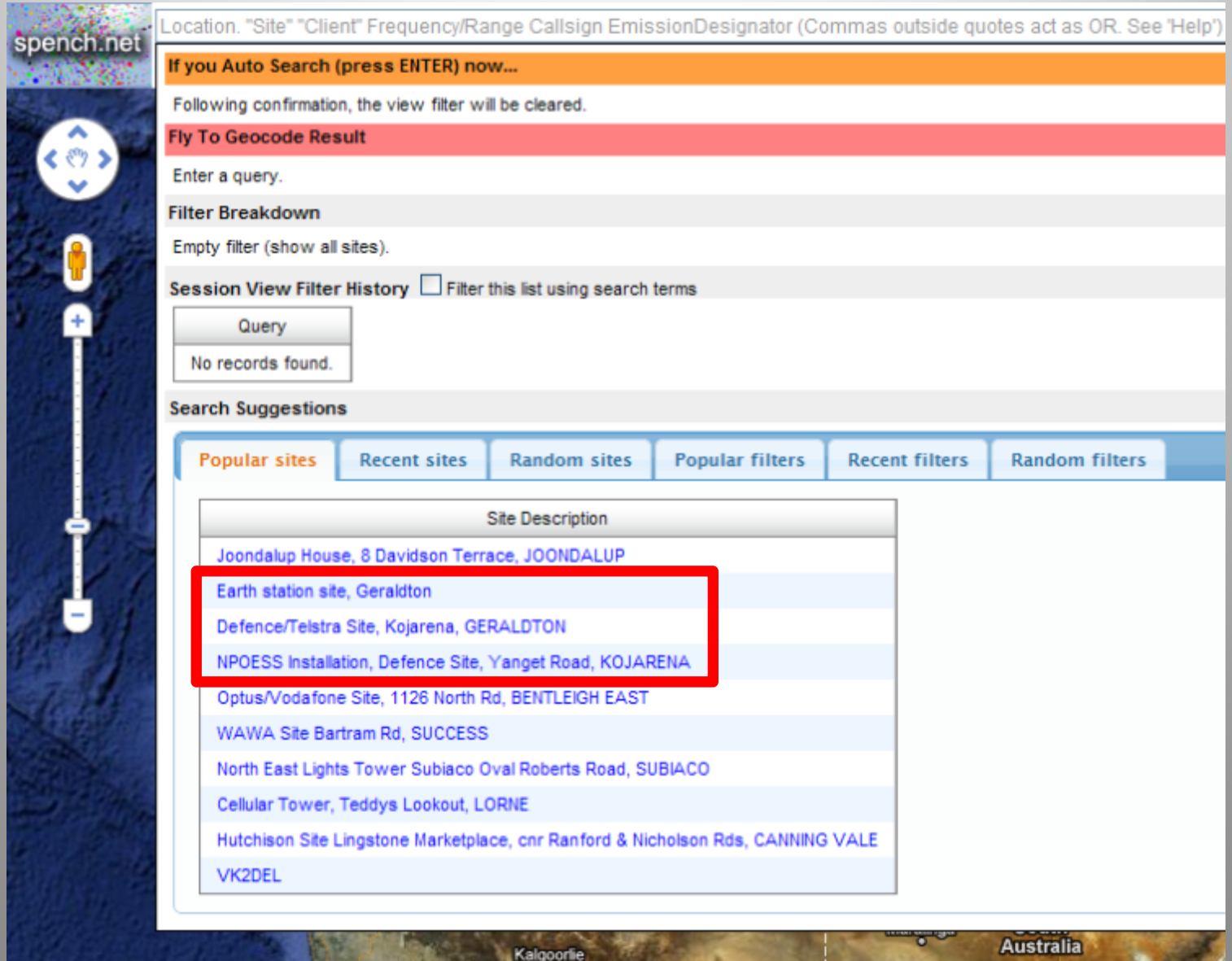
Radiation Heatmap



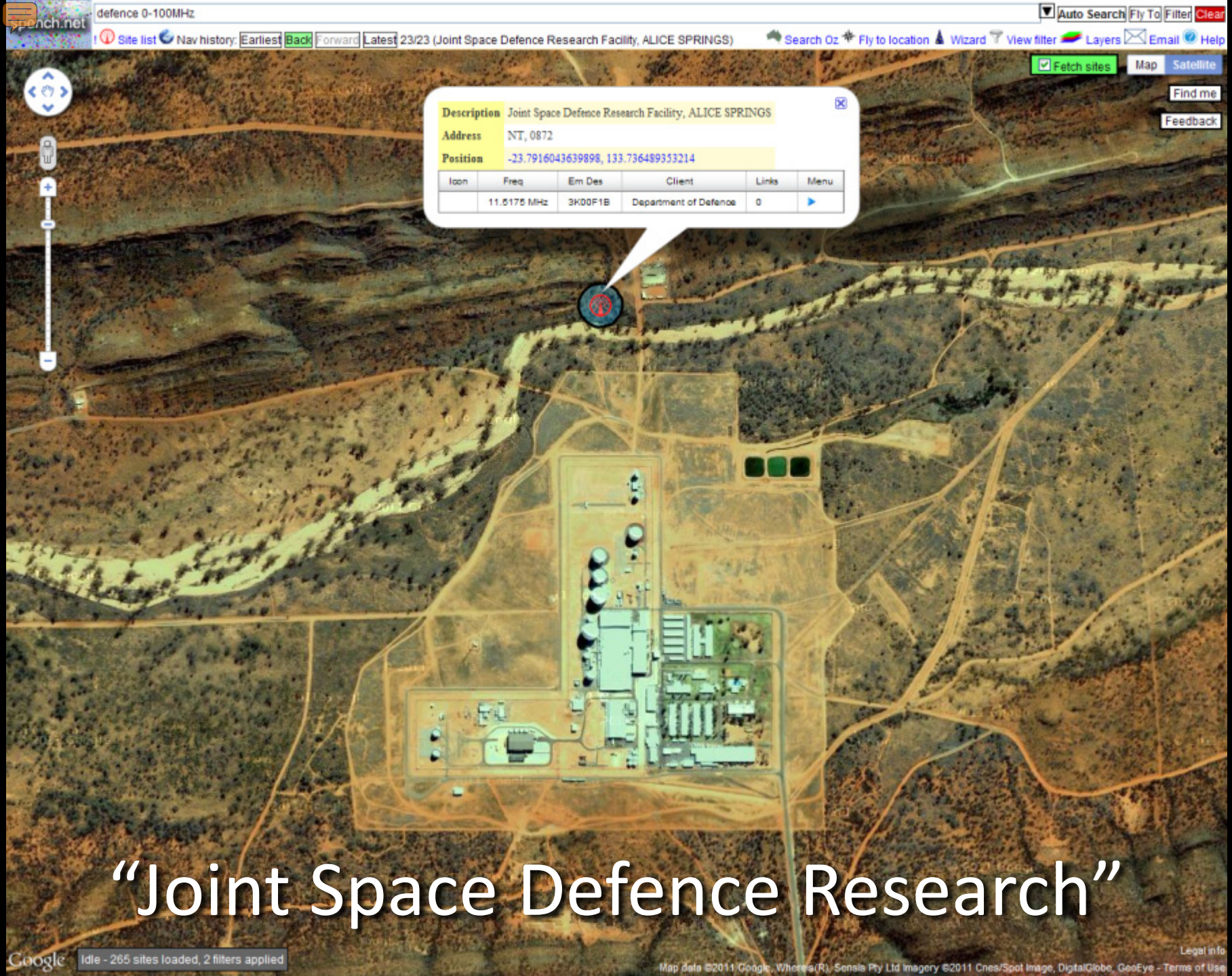
Amateur Radio Operators (HAMs)


Fetch sites
Map
Satellite
Find me
Feedback
Description VK2FUNK
Address M23/1A Mandible Street ALEXANDRIA, NSW 2015
Position -33.903487, 151.2015
Icon | Freq | Em Des | Client | Links | Menu
3.6 MHz | 200HA1A | Sebastian Balint Seeber | 0
7.15 MHz | 8K00A3E | Sebastian Balint Seeber | 0
21.225 MHz | 4K00J3E | Sebastian Balint Seeber | 0
28.85 MHz | 200HA1A | Sebastian Balint Seeber | 0
146 MHz | 8K00A3E | Sebastian Balint Seeber | 0
440 MHz | 4K00J3E | Sebastian Balint Seeber | 0
440 MHz | 16K0F3E | Sebastian Balint Seeber | 0
440 MHz | 16K0G3E | Sebastian Balint Seeber | 0

Most popular 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
8/8 (Earth station site, Geraldton)
Search Oz
Fly to location
Wizard
View filter
Layers
Email
Help
Fetch sites
Map
Satellite
Find me
Feedback
Defence & ECHELON
Google
Idle - 6 sites loaded
Legal info
Imagery ©2011 DigitalGlobe, GeoEye - Terms of Use



“Joint Space Defence Research”

Upset ADIRU of QF68/71/72 & JQ7 ?

Side note


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:

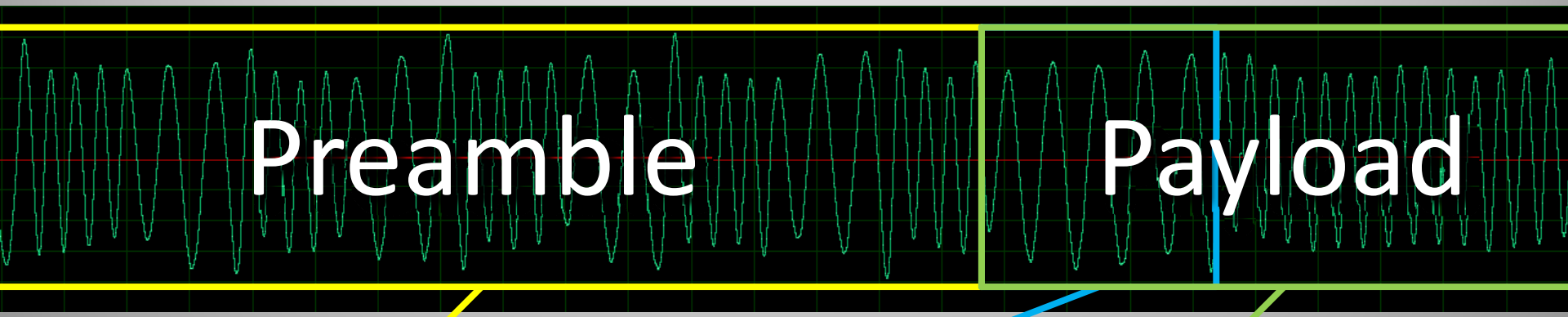
correlates with increased daytime activity.

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

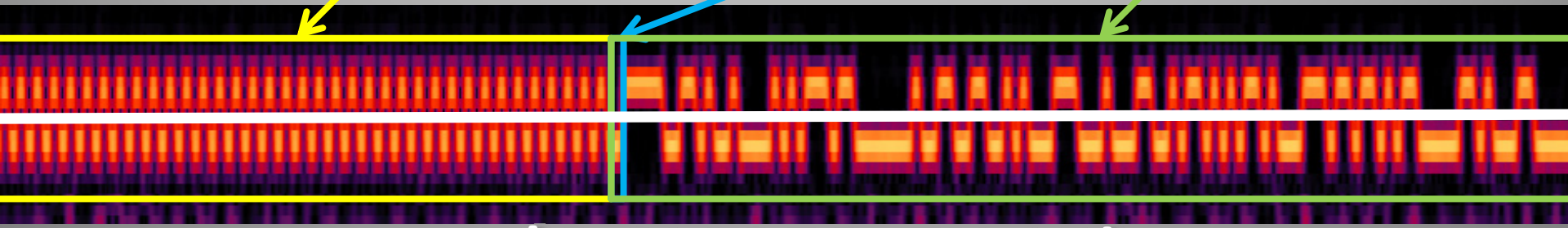
Step One: Look at the signal

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

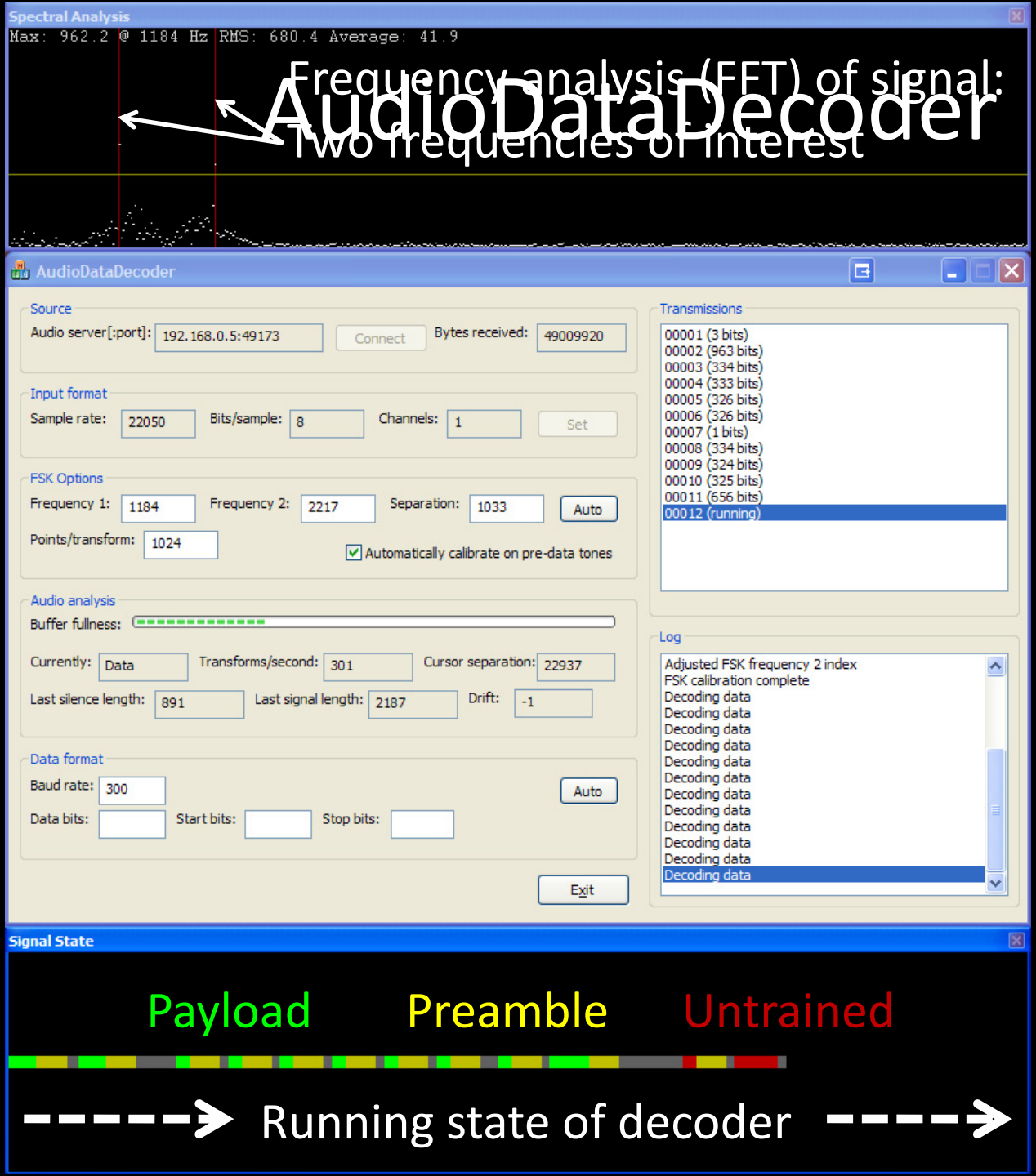
Signal in the time domain (voltage vs. time):



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



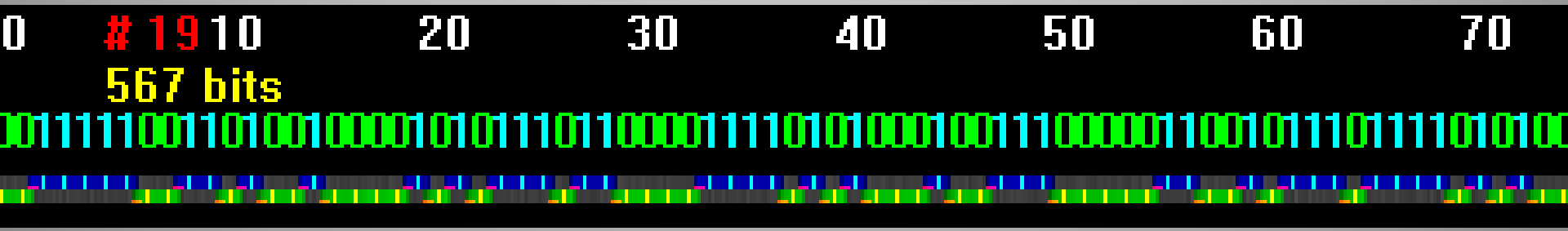
IT’S SLICER TIME!


Spectral Analysis
Max: 962.2 @ 1184 Hz RMS: 680.4 Average: 41.9
Frequency analysis (FFT) of signal:
Two frequencies of interest
AudioDataDecoder
AudioDataDecoder
Source
Audio server[:port]:
192.168.0.5:49173
Connect
Bytes received:
49009920
Input format
Sample rate:
22050
Bits/sample:
8
Channels:
1
Set
FSK Options
Frequency 1:
1184
Frequency 2:
2217
Separation:
1033
Auto
Points/transform:
1024
Automatically calibrate on pre-data tones
Audio analysis
Buffer fullness:
Currently:
Data
Transforms/second:
301
Cursor separation:
22937
Last silence length:
891
Last signal length:
2187
Drift:
-1
Data format
Baud rate:
300
Auto
Data bits:
Start bits:
Stop bits:
Exit
Transmissions
00001 (3 bits)
00002 (963 bits)
00003 (334 bits)
00004 (333 bits)
00005 (326 bits)
00006 (326 bits)
00007 (1 bits)
00008 (334 bits)
00009 (324 bits)
00010 (325 bits)
00011 (656 bits)
00012 (running)
Log
Adjusted FSK frequency 2 index
FSK calibration complete
Decoding data
Decoding data
Decoding data
Decoding data
Decoding data
Decoding data
Decoding data
Decoding data
Decoding data
Decoding data
Decoding data
Decoding data
Decoding data
Signal State
Payload
Preamble
Untrained
Running state of decoder

Step Two: FFT of 2FSK → Bitstream

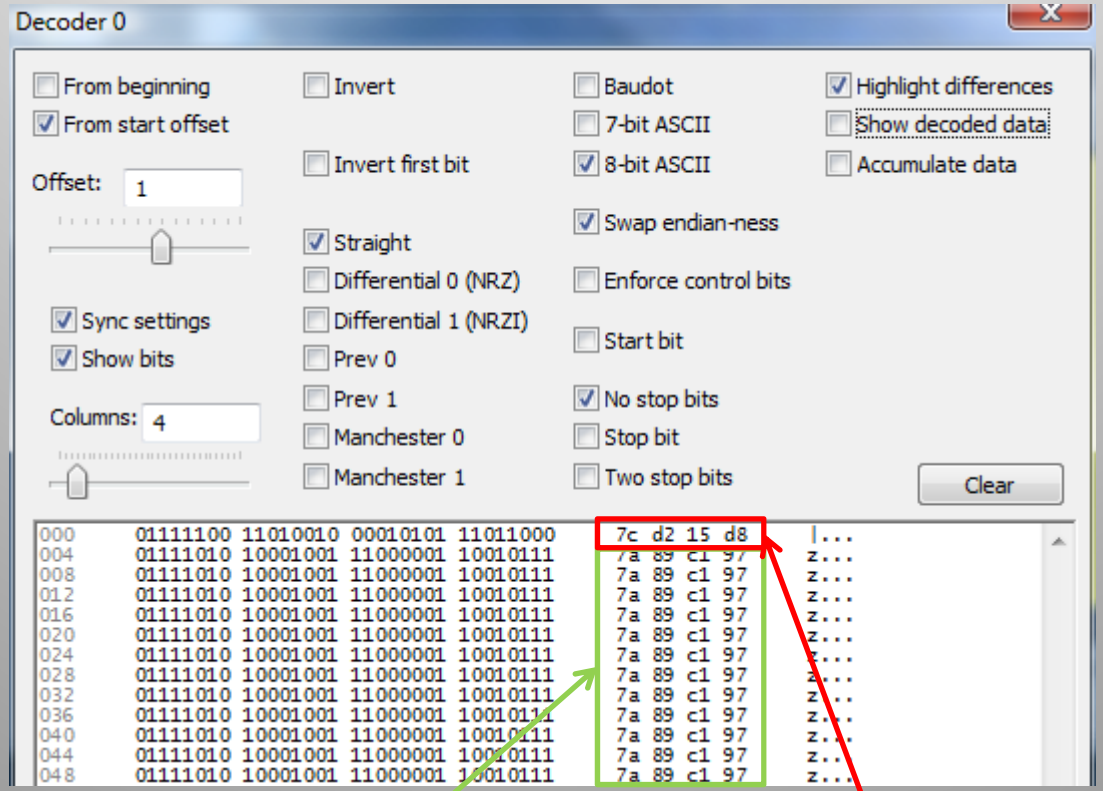
- Lock on two frequencies (**F**requency **S**hift **K**eying)
- Sample intensity of each at regular interval (baud rate)
- Pick which is the strongest:

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 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:

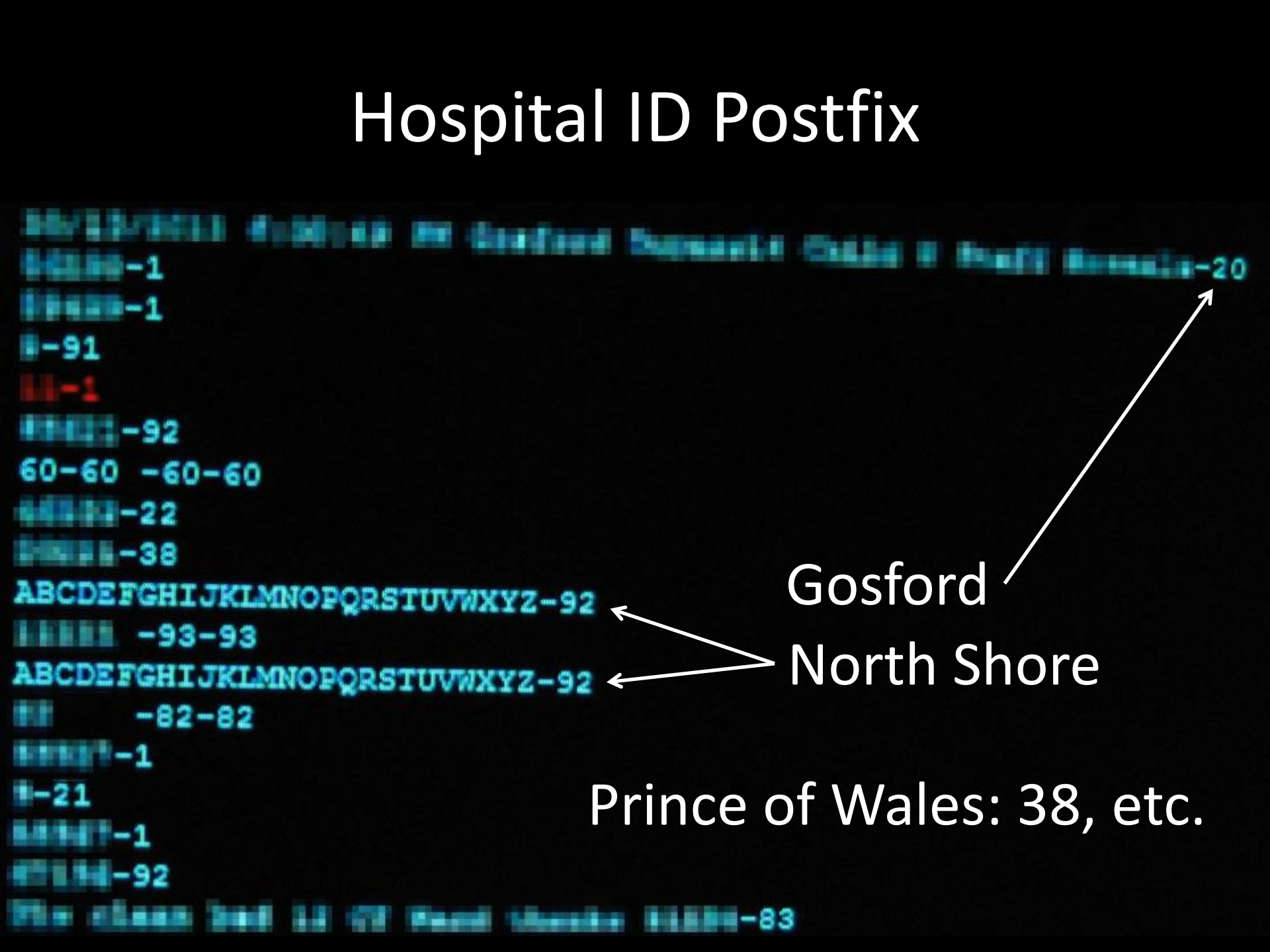
  Non-standard FSK ignored by decoders


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

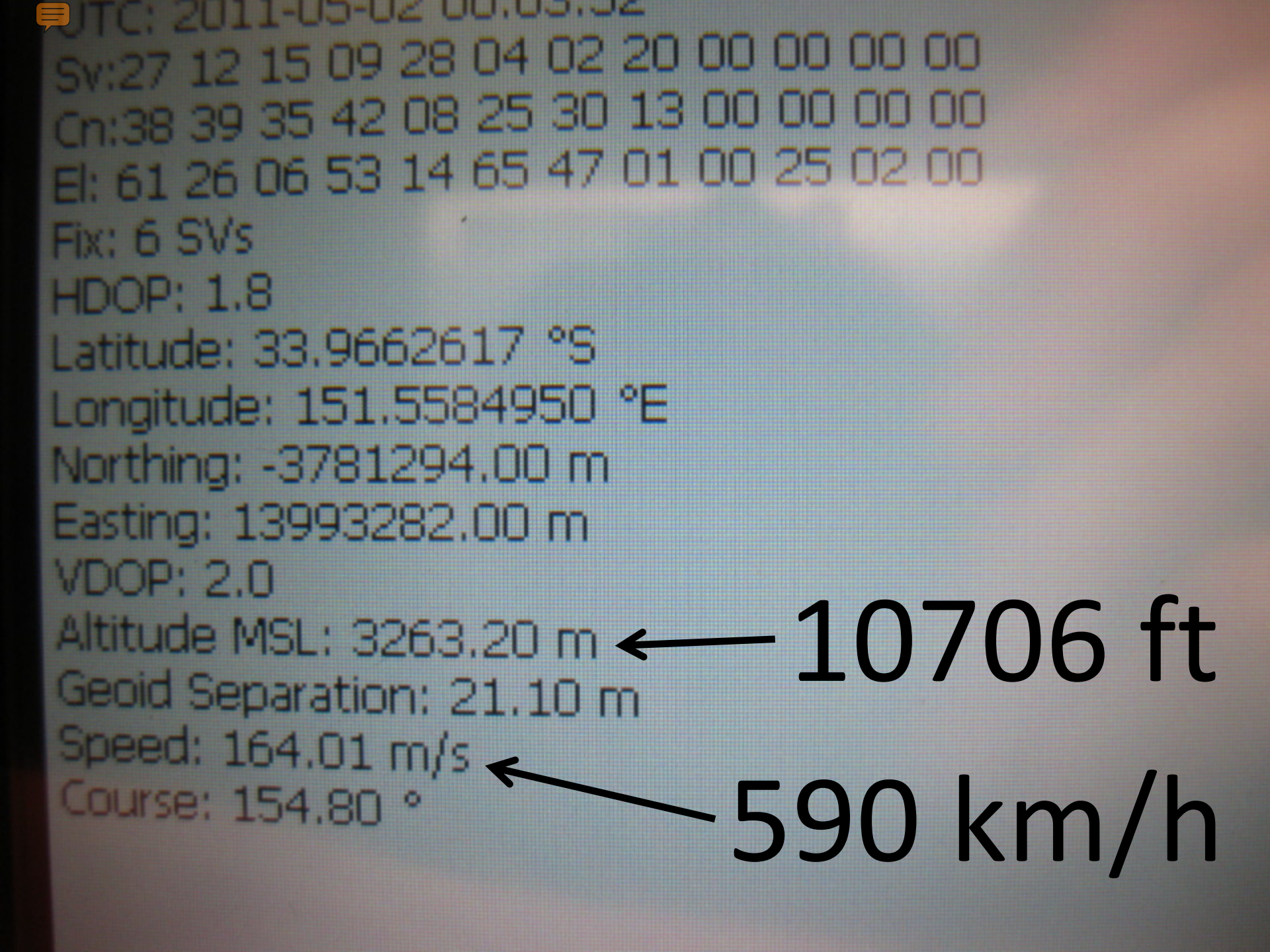
Hospital ID Postfix



Sensitive Information

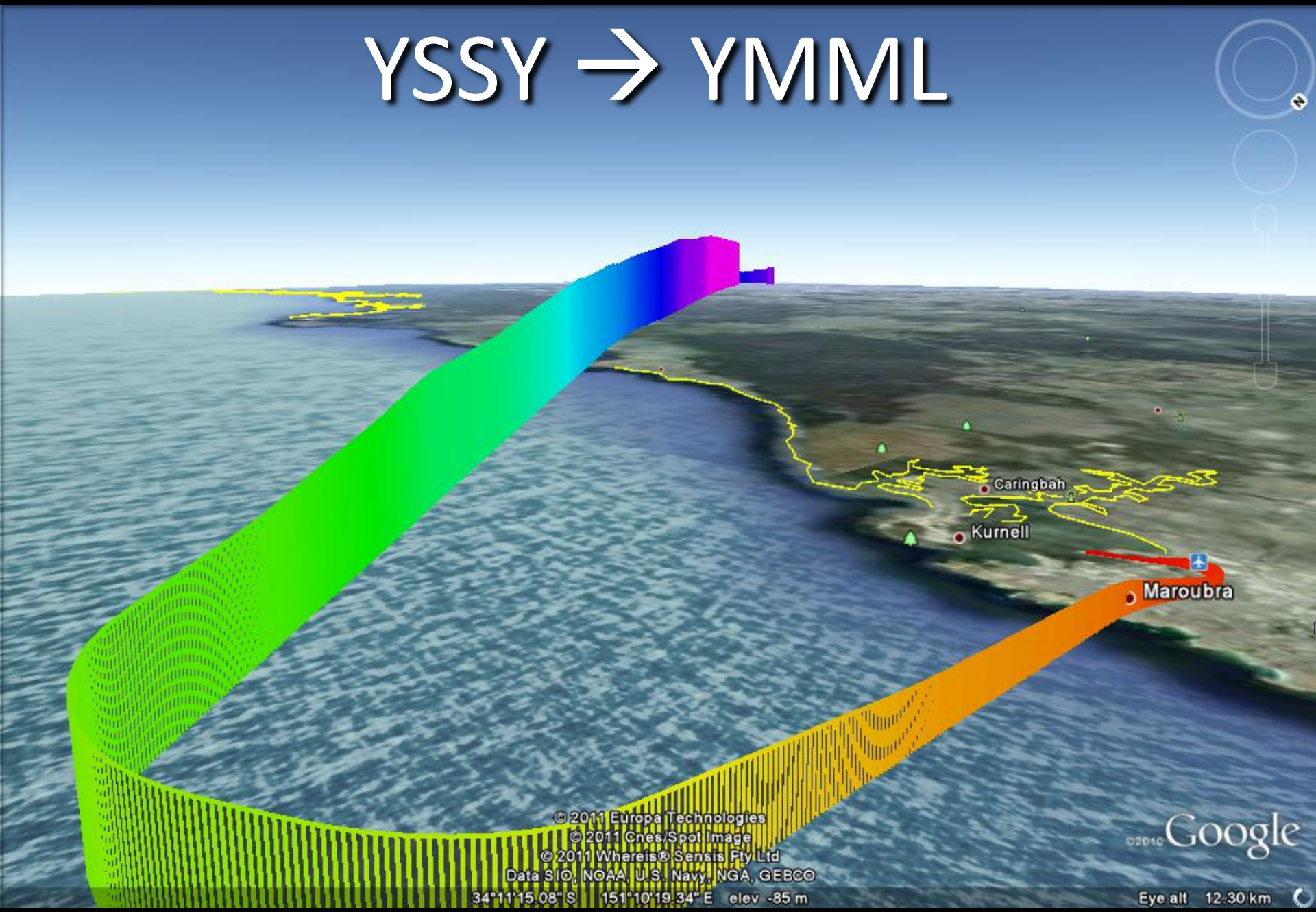
AviationMapper

Image by Oscar De Lellis


UTC: 2011-05-02 00:03:32
Sv:27 12 15 09 28 04 02 20 00 00 00 00
Cn:38 39 35 42 08 25 30 13 00 00 00 00
El: 61 26 06 53 14 65 47 01 00 25 02 00
Fix: 6 SVs
HDOP: 1.8
Latitude: 33.9662617 °S
Longitude: 151.5584950 °E
Northing: -3781294.00 m
Easting: 13993282.00 m
VDOP: 2.0
Altitude MSL: 3263.20 m
Geoid Separation: 21.10 m
Speed: 164.01 m/s
Course: 154.80 °
10706 ft
590 km/h


YSSY → YMML
New South Wales
Sydney
Canberra
Wollongong
Victoria
Melbourne
French Island
Montague Island
Raymond Island
Snake Island
Norman Island
Anser Island
Rodondo Island
Gabo Island
Hogan Island
Curtis Island
Erith Island
Deal Island
Craggy Island
122 km
© 2011 Whereis® Sensis Pty Ltd
© 2011 Europa Technologies
© 2011 Cnes/Spot Image
Data SIO, NOAA, U.S. Navy, NGA, GEBCO
lat -36.473525° lon 148.276967° elev 1056 m
©2010 Google
Eye alt 559.39 km

YSSY → YMML


Caringbah
Kurnell
Maroubra
© 2011 Europa Technologies
© 2011 Cnes/Spot Image
© 2011 Whereis® Sensis Pty Ltd
Data SIO, NOAA, U.S. Navy, NGA, GEBCO
34°11'15.08" S 151°10'19.34" E elev -85 m
©2010 Google
Eye alt 12.30 km


9:13 am
Satellite
Excellent
Accuracy
21 ft
Stopped Time
2m 16s
Moving Time
22m 40s
Moving Avg
244.4 Mph
Avg Speed
222.2 Mph
Distance to End

Time Travelled
24m 56s
Current Speed
481.1 Mph
Elevation
30700 ft
Heading
125°
Bearing

11:19 am
United State
Time to Next

Accuracy
26 ft
Conroe
Houston
© 2012 Cnes/Spot Image
Image © 2012 TerraMetrics
© 2012 Google
© 2012 INEGI
Google
lat 30.210870° lon -96.043489° elev 82 m
Eye alt 71.37 km

ATCRBS, PSP & SSR

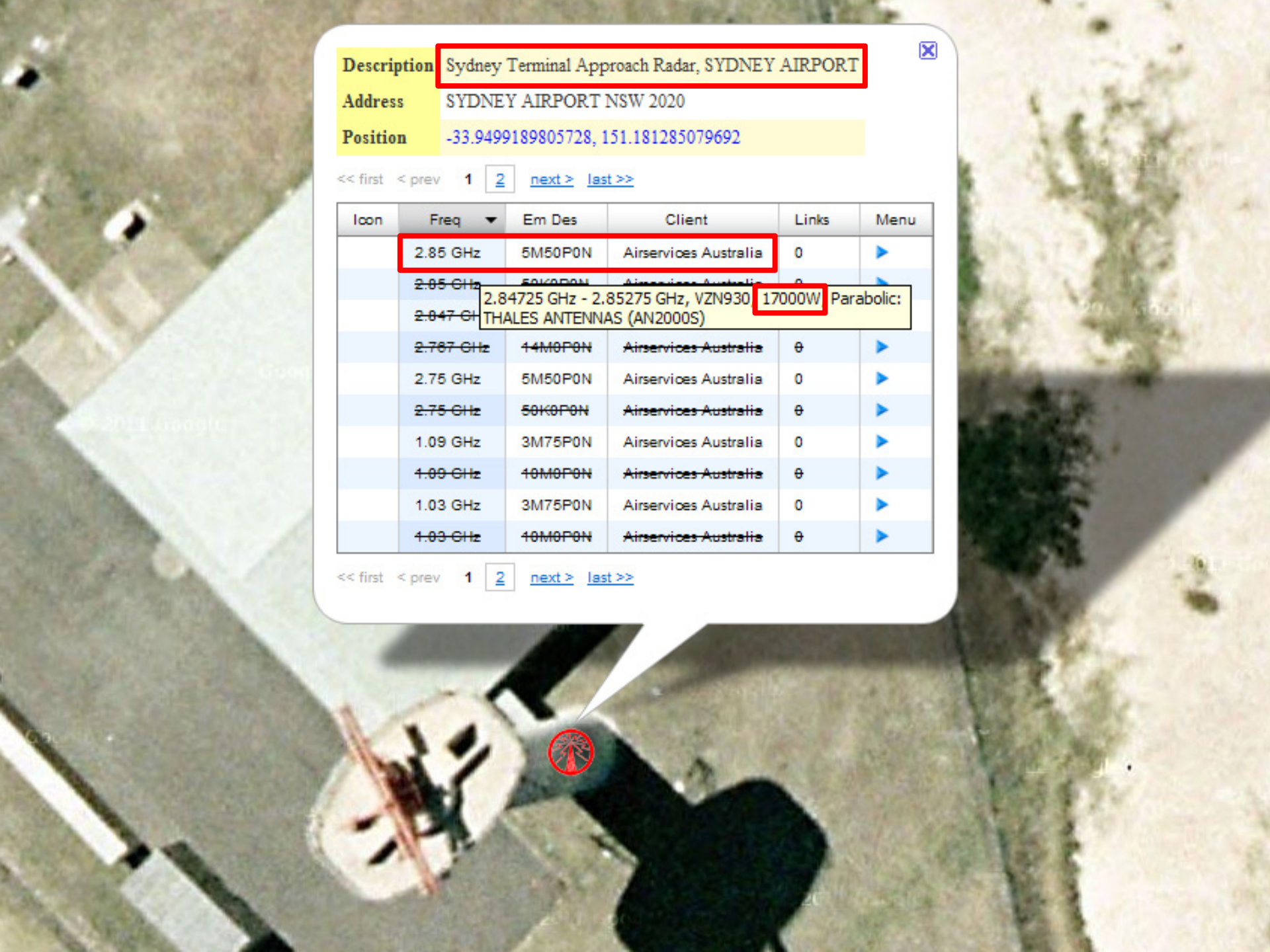
- **A**ir **T**raffic **C**ontrol **R**adar **B**eacon **S**ystem
  - **P**rimary **S**urveillance **R**adar
  - **S**econdary **S**urveillance **R**adar

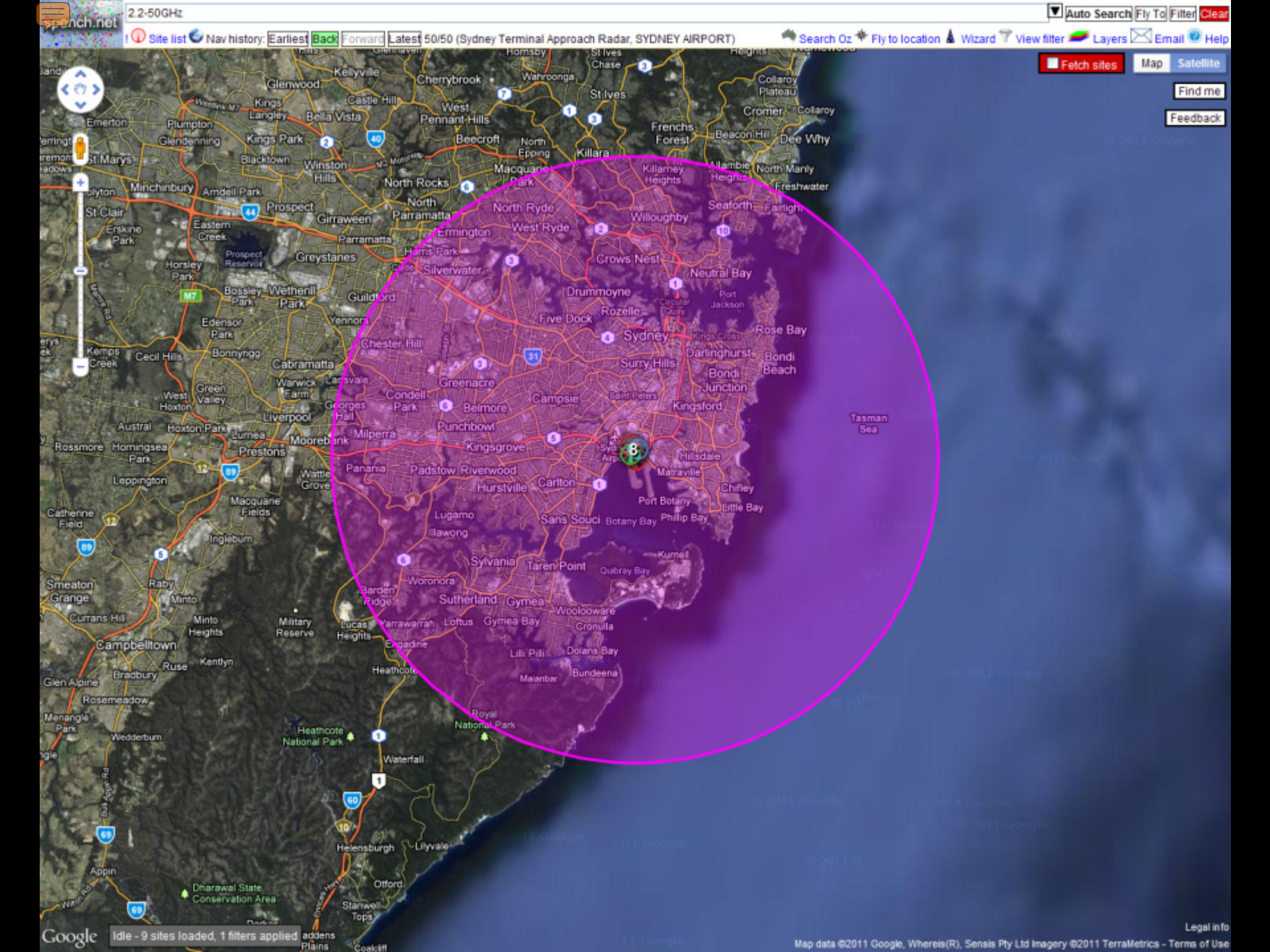
Primary:
- Traditional RADAR
- 'Paints skins' and listens for return
- Identifies and tracks primary targets, while ignoring 'ground clutter'
- Range limited by RADAR equation ($\frac{1}{d^4}$)

ATCRBS, PSP & 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

The Modes

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

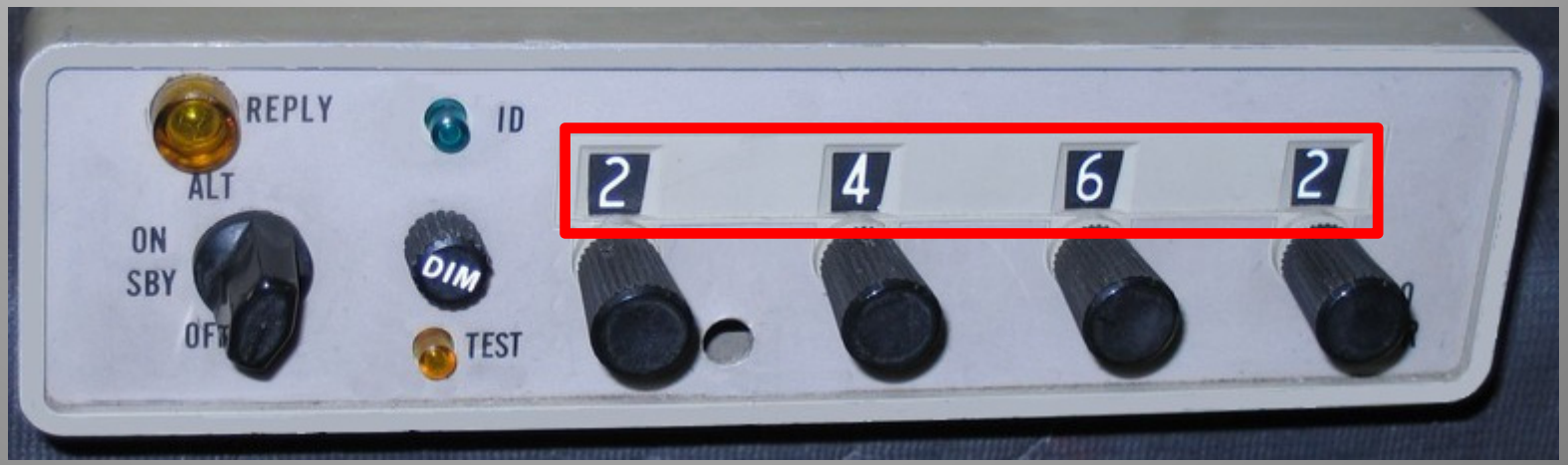
SSR

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

The Modes

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

SSR



Position

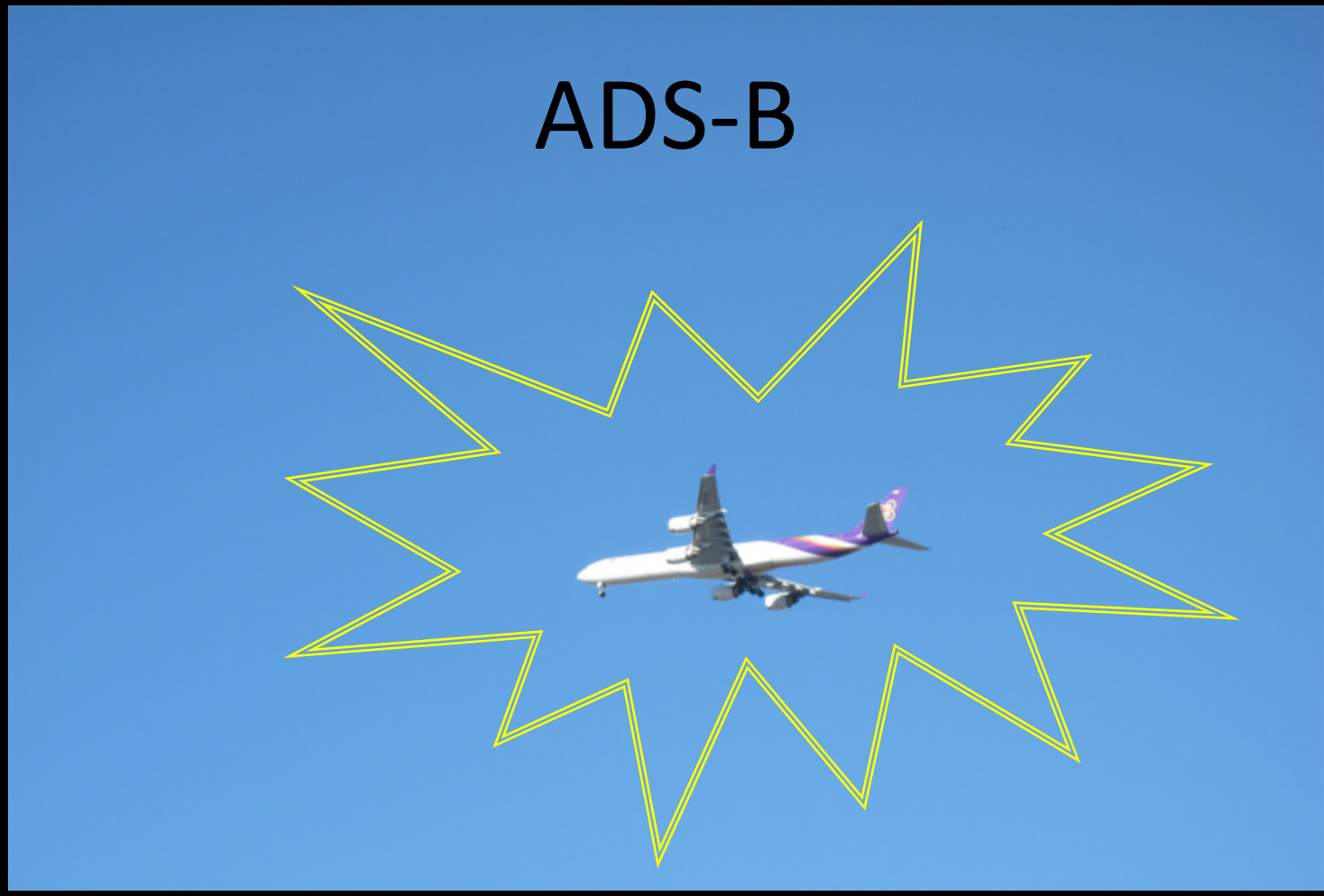
Heading

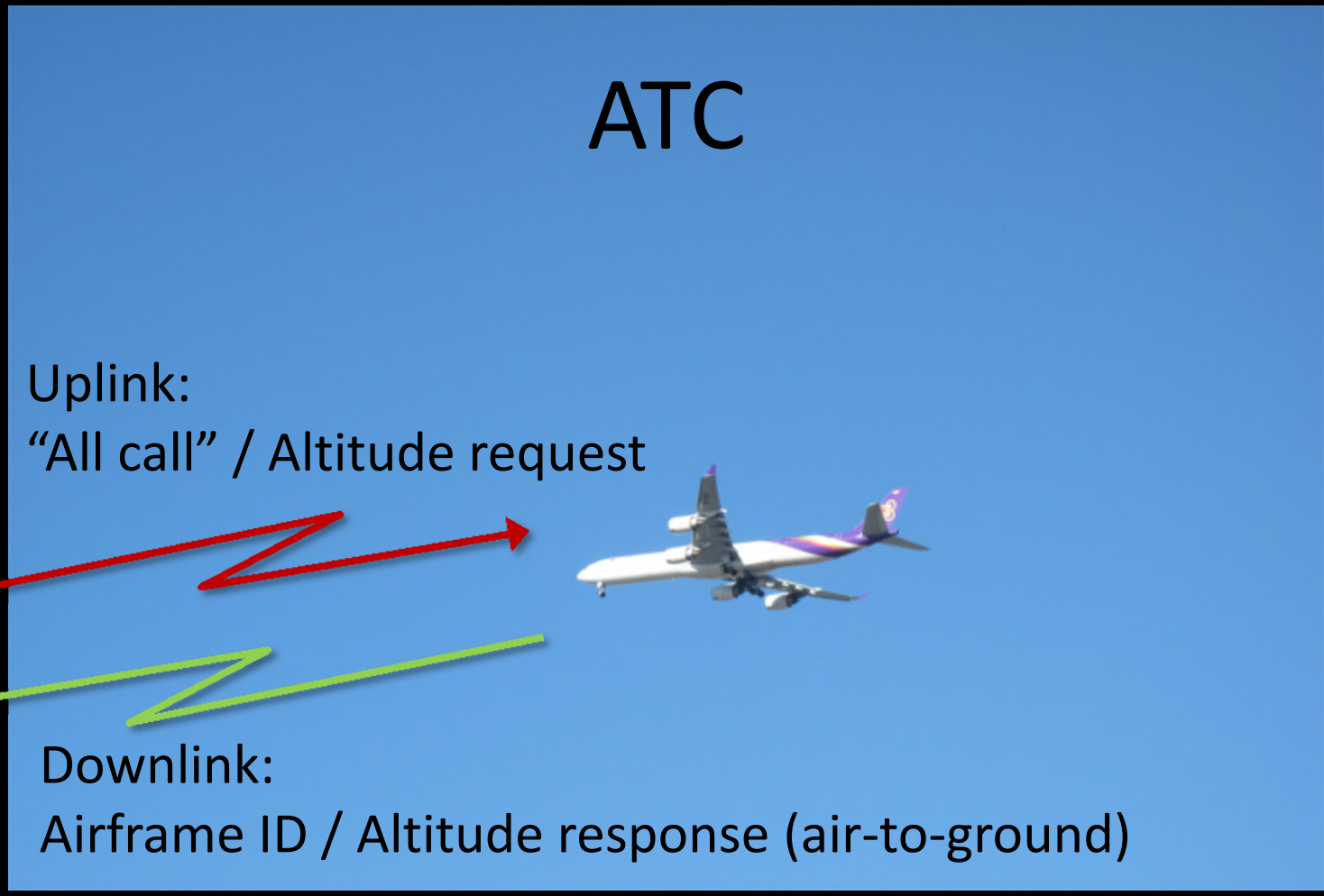
Altitude

Vertical rate

Flight ID

Squawk code





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

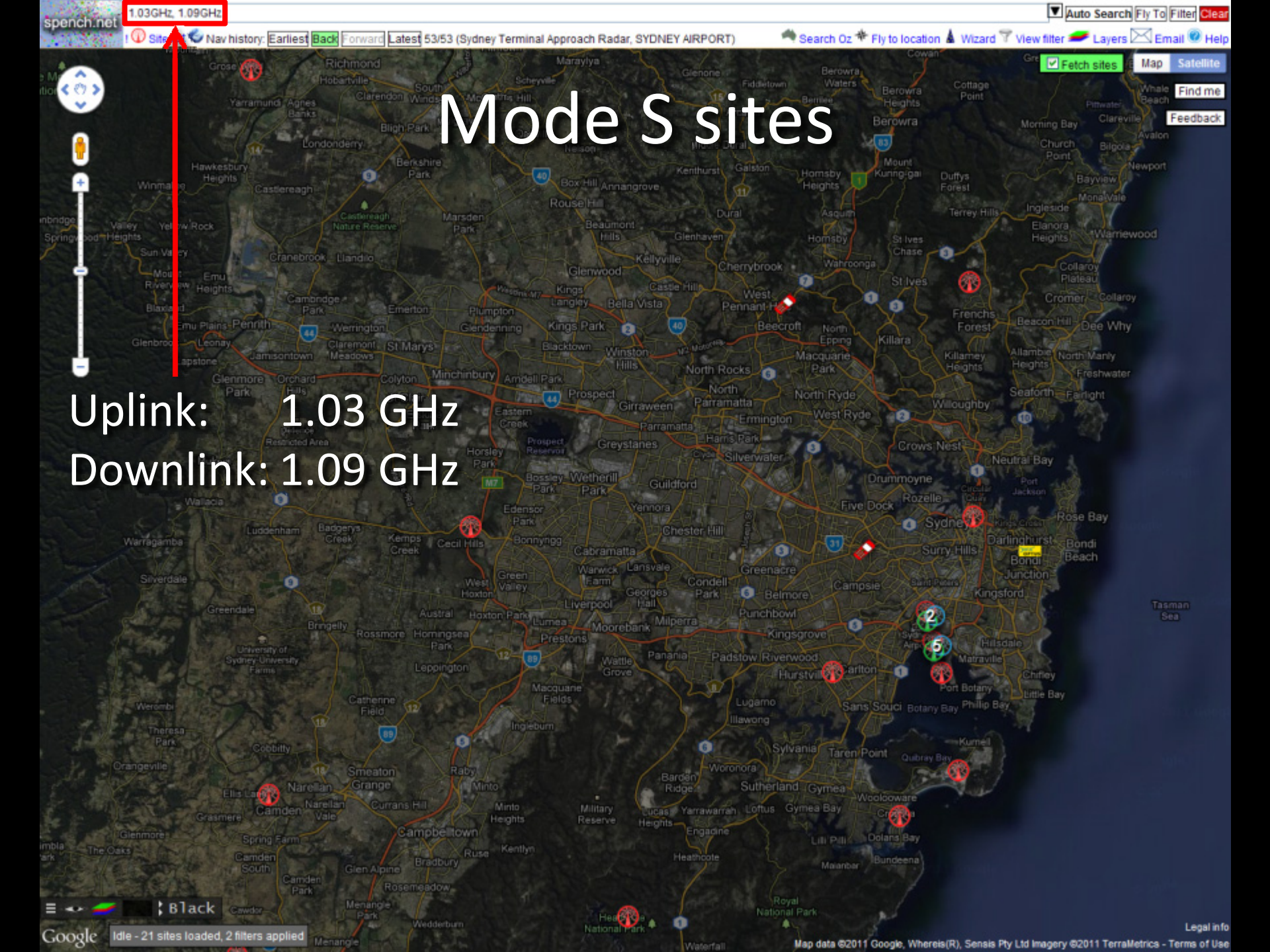
ACAS/TCAS

"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

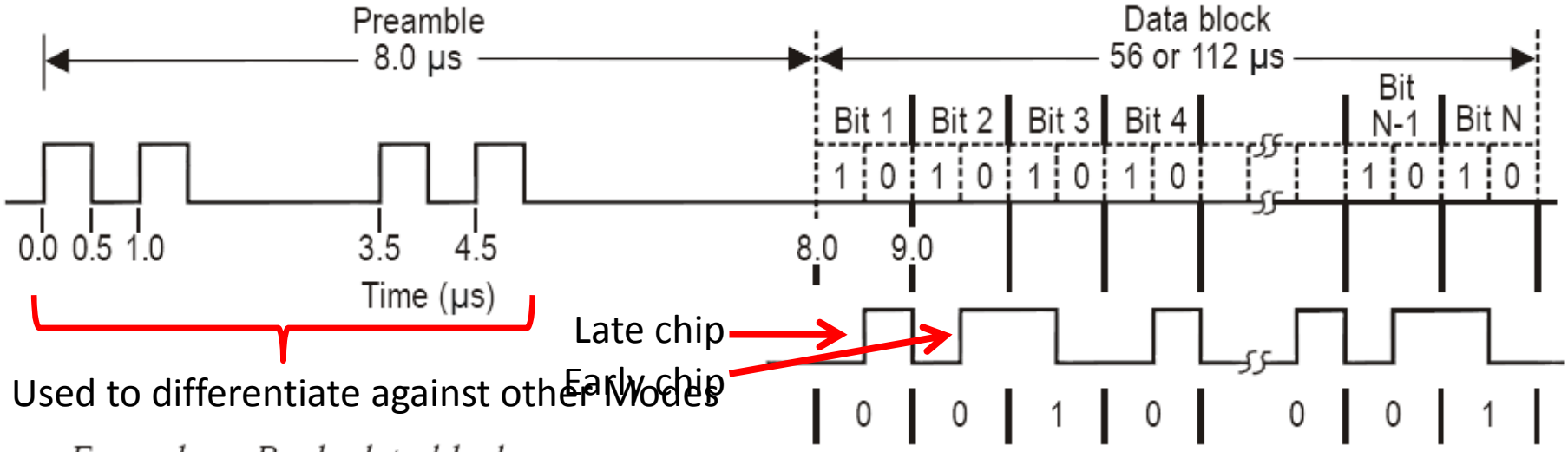
Mode S sites

Uplink: 1.03 GHz

Downlink: 1.09 GHz

Response Encoding

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



Used to differentiate against other Modes

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

Pulse Position Modulation (AM)

Pulse Position Modulation

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

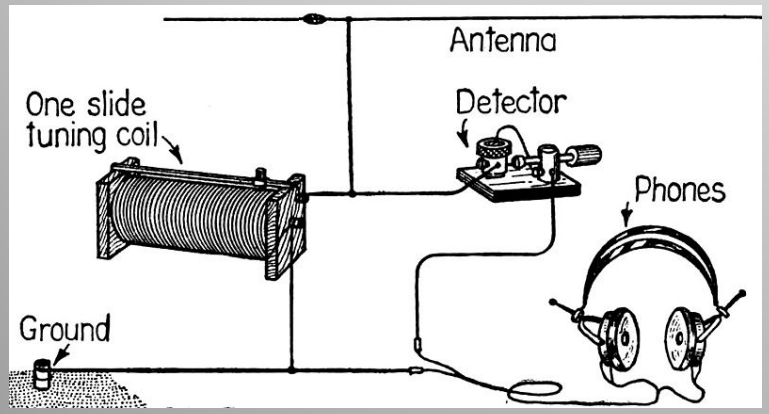
Enter **S**oftware **D**efined **R**adio…

SDR: Digitise the baseband

- Hardware is sophisticated, but purpose is simple: capture a chunk of the RF spectrum and stream it to your computer
- Computer is responsible for doing something useful with baseband data
- Instead of designing RF hardware, write it in software!
- Increased complexity/bandwidth requires more CPU power (pretty cheap)

Software **D**efined **R**adio

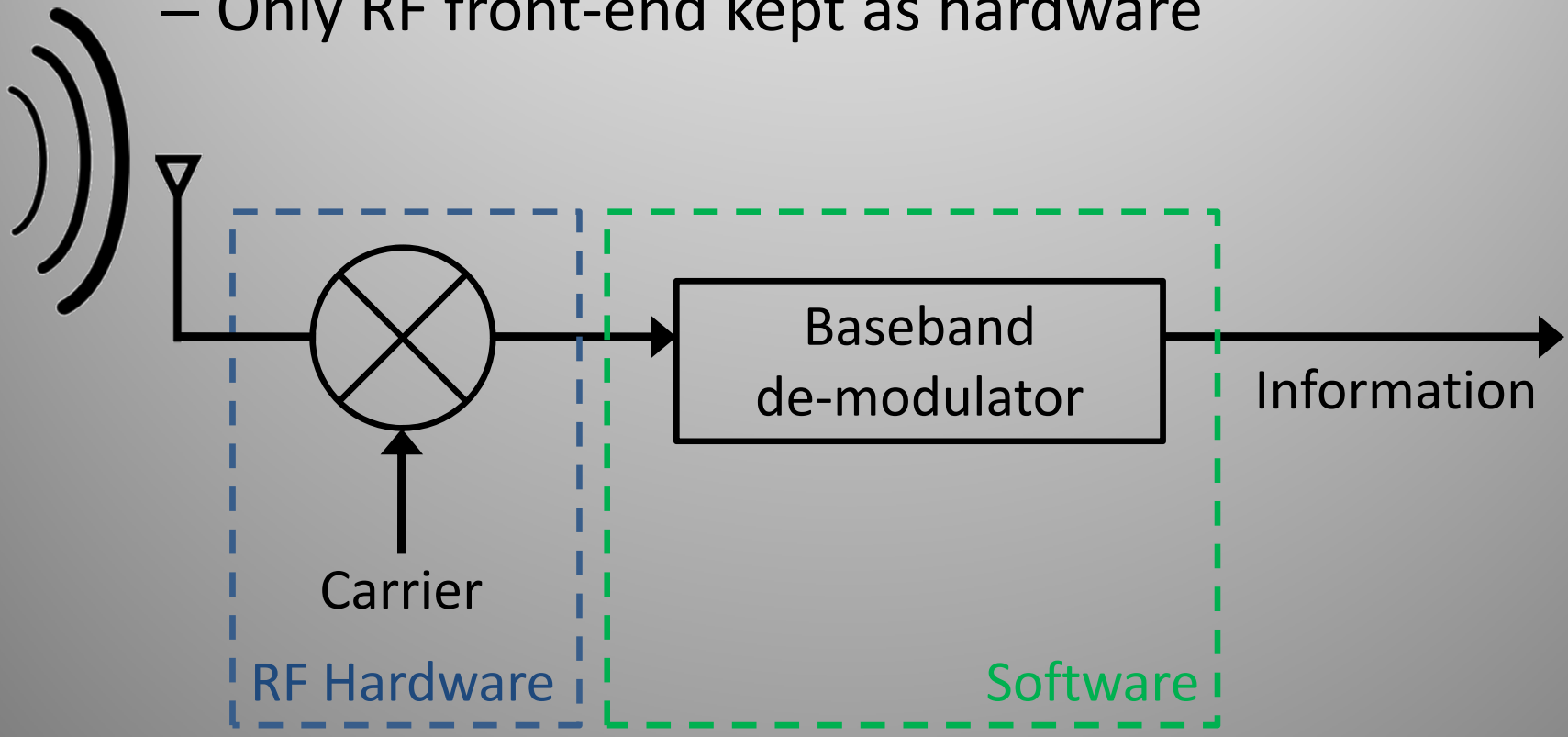
- Hardware → software representation
  - Completely re-configurable
  - Only RF front-end kept as hardware



$$\rightarrow \sqrt{I^2 + Q^2}$$

Software **D**efined **R**adio

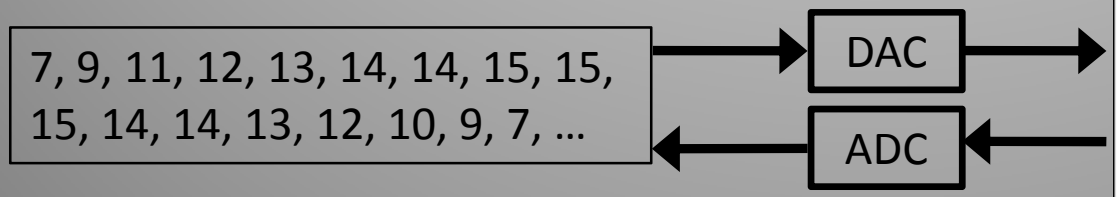
- Hardware → software representation
  - Completely re-configurable
  - Only RF front-end kept as hardware

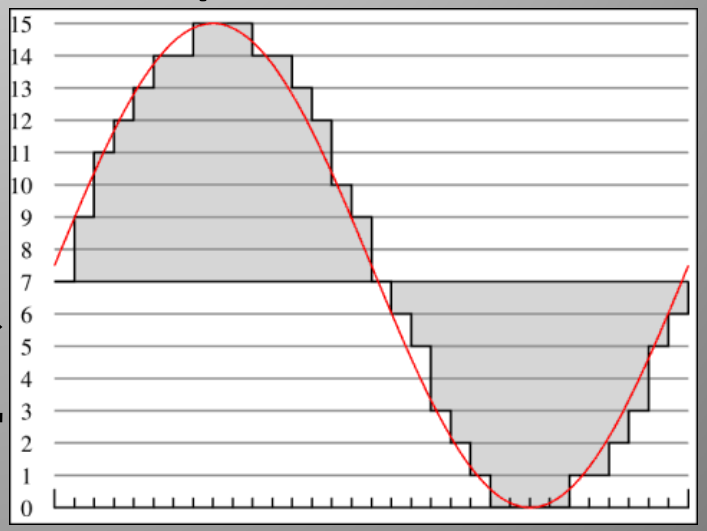


Software **D**efined **R**adio

- Hardware → software representation
  - Completely re-configurable
  - Only RF front-end kept as hardware

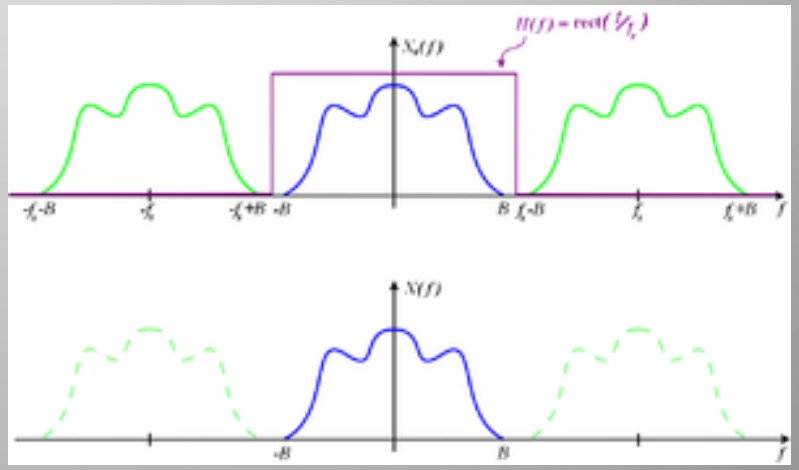
- Continuous process → discrete & quantised
  - Digital sampling produces voltage levels





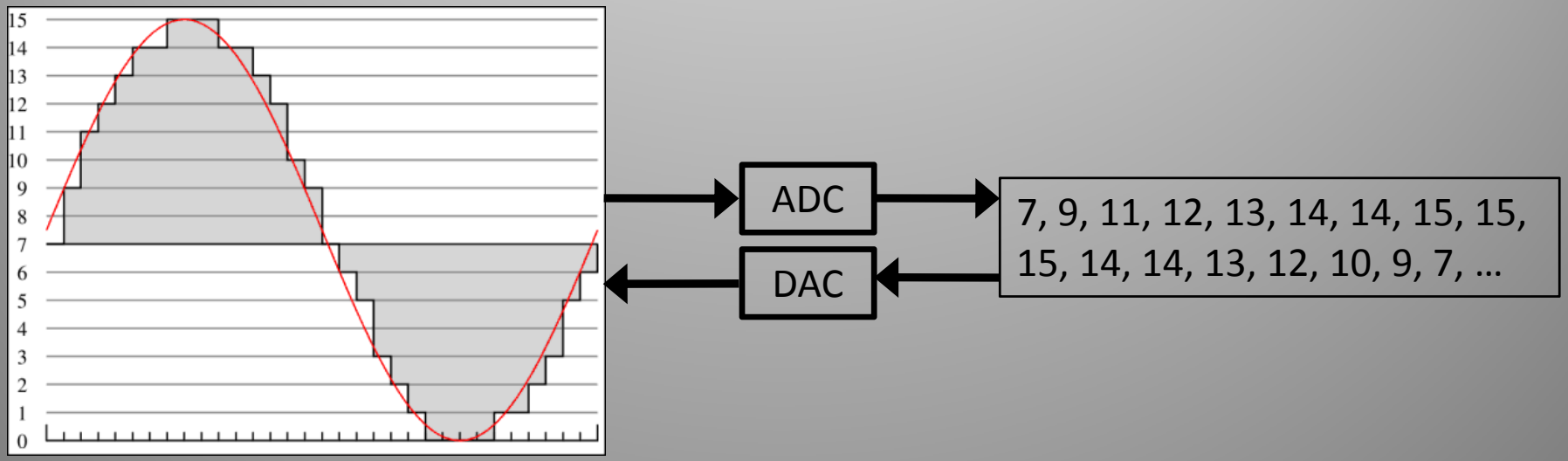
Sampling

- Nyquist-Shannon Sampling Theorem:
  - "Sample at twice the highest required frequency"
  - Avoid aliasing of signal



Sampling

- Nyquist-Shannon Sampling Theorem:
  - "Sample at twice the highest required frequency"
  - Avoid aliasing of signal
- **A**nalog-to-**D**igital **C**onverter (RX)
- **D**igital-to-**A**nalog **C**onverter (TX)



Sampling

- Nyquist-Shannon Sampling Theorem:
  - "Sample at twice the highest required frequency"
  - Avoid aliasing of signal
- **A**nalog-to-**D**igital **C**onverter (RX)
- **D**igital-to-**A**nalog **C**onverter (TX)
- ADC/DAC rate determines bandwidth*

Reception

- RF front-end down-converts signal to baseband
  - Zero IF receiver
- Sample & quantise baseband signal
- Simple approach would be to sample voltage level (amplitude)
  - Sound card

Real vs. Analytic Signals

- Real signal:
  - Amplitude for each sample
  - One ‘real’ number
- Analytic signal:
  - Amplitude and phase
  - ‘Real’ and ‘imaginary’ components (negative frequency)
  - Encode more information

Quadrature Modulation

- Analytic signals can be sampled by having two ADCs
- Baseband must first be separated into quadrature components (real and imaginary parts)
- Mix baseband with:
  - In-phase local oscillator (I channel)
  - Quadrature-phase LO (Q channel)

Sample Rate

- Analytic signal has two components
  - I & Q samples per sample time
- Negative frequency
  - Double the bandwidth
- Re-apply Shannon's sampling theorem:
  - Sampling rate directly determines bandwidth
- Produce a stream of complex stream (I/Q samples pairs) at sample rate

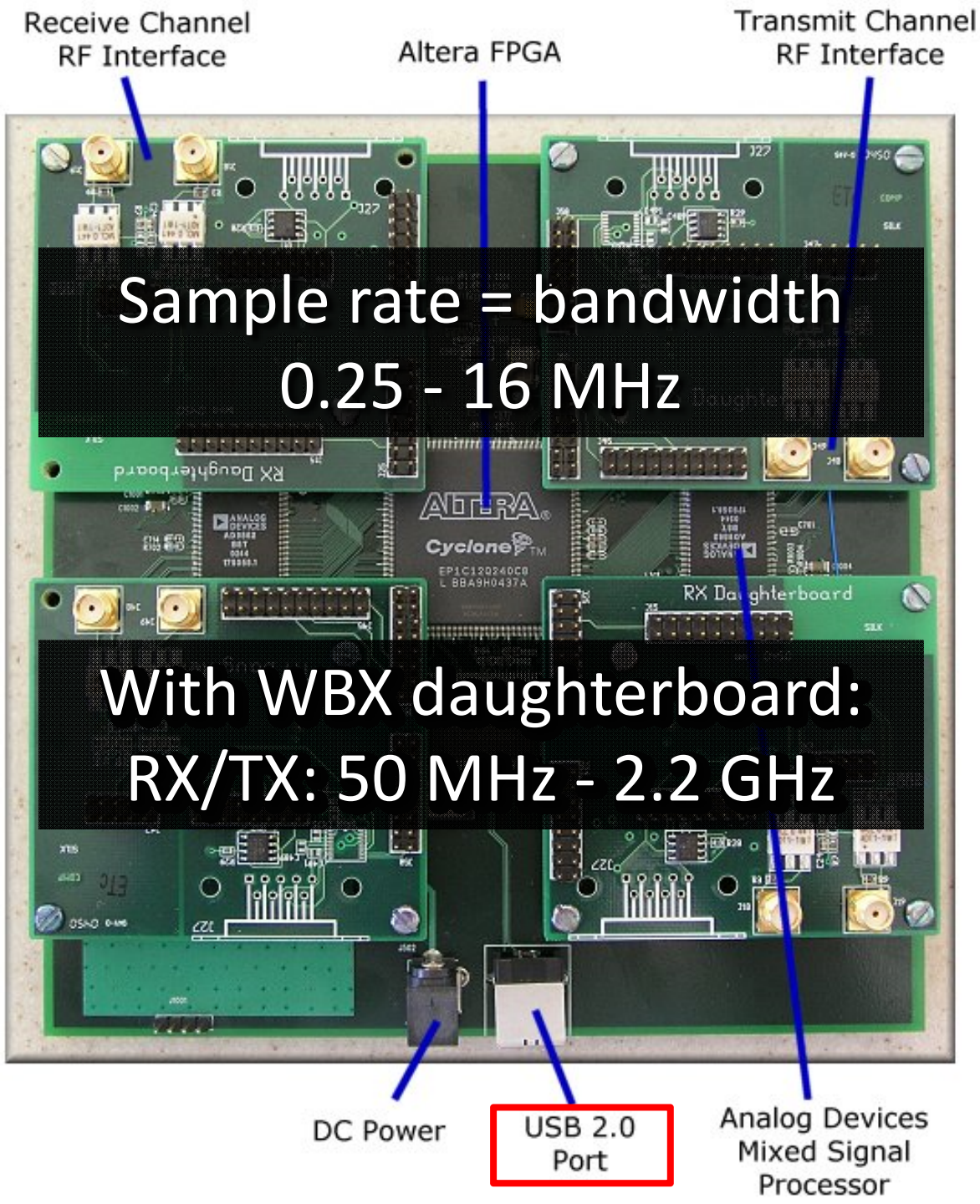
SDR (De-)modulation

- Complex stream passed through mathematical functions and state machines

The

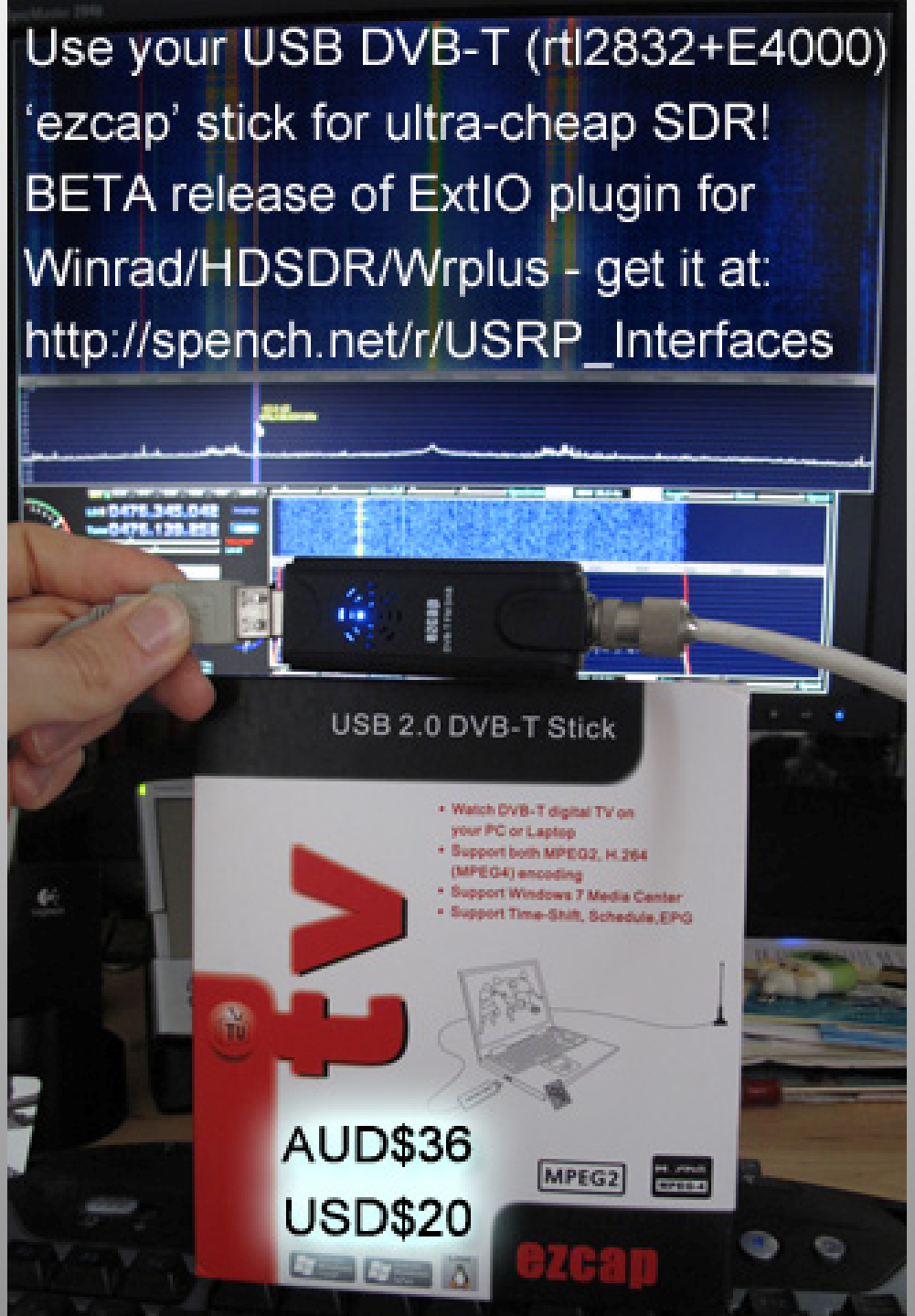
Universal
Software
Radio
Peripheral

(USRP 1)




ALTERA
Cyclone
CLOCK
CLOCK
BOSCH

The FUNcube Dongle


Use your USB DVB-T (rtl2832+E4000) 'ezcap' stick for ultra-cheap SDR!
BETA release of ExtIO plugin for Winrad/HDSDR/Wrplus - get it at:
http://spench.net/r/USRP_Interfaces
USB 2.0 DVB-T Stick
• Watch DVB-T digital TV on your PC or Laptop
• Support both MPEG2, H.264 (MPEG4) encoding
• Support Windows 7 Media Center
• Support Time-Shift, Schedule,EPG
AUD$36
USD$20
MPEG2
ezcap

Host Software

- Receive/transmit baseband samples
  - Analyse & display
  - (De-)modulate
  - Encode/decode (extract information)

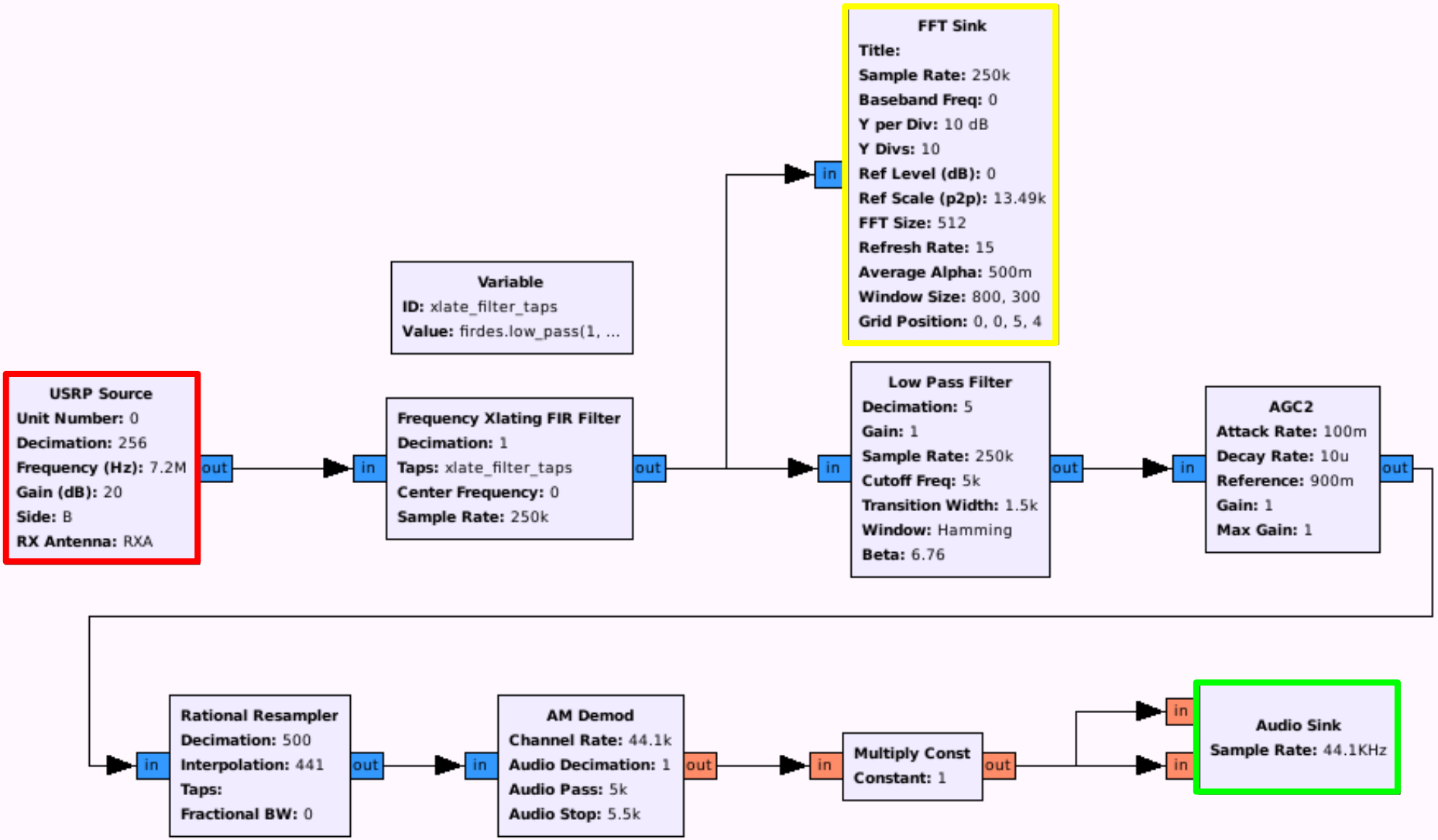
- Well-known platforms/programs:
  - LabVIEW
  - MATLAB Simulink

  Open source? **No.**

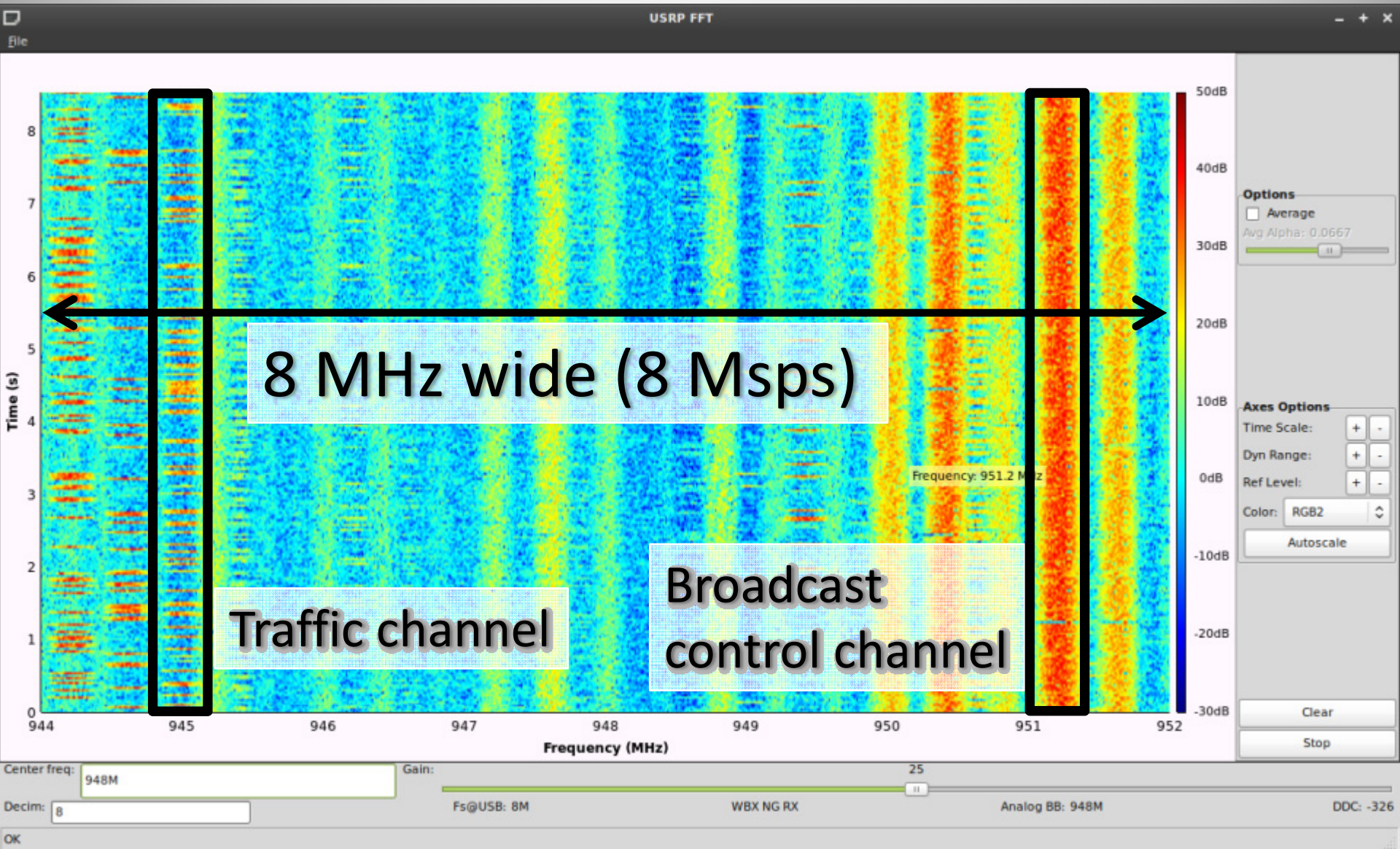
GNU **R**adio

- Open source signal processing toolkit
- Data flow paradigm
  - Signals flow from sources to sinks
- Intermediary blocks operate on signals
  - Sources & sinks: USRP, sound card, file, network
  - Visualisation: FFT, waterfall, scope
  - Signal types: complex, float, integers
  - Filters: traditional building blocks used in analog and digital RF hardware
- Completely extensible (Python: high level, C++: grunt)

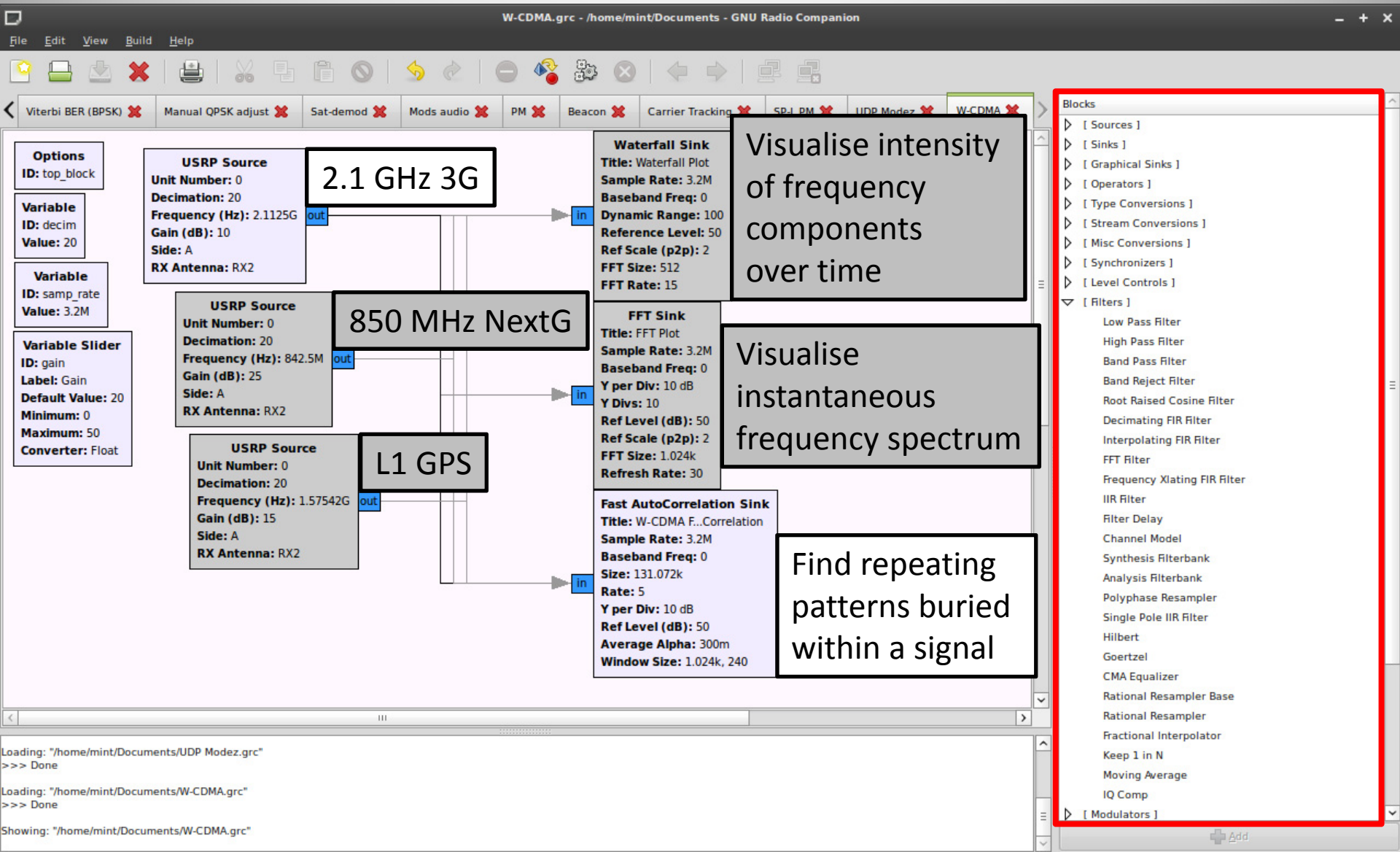
GNU Radio Companion



2G GSM Waterfall

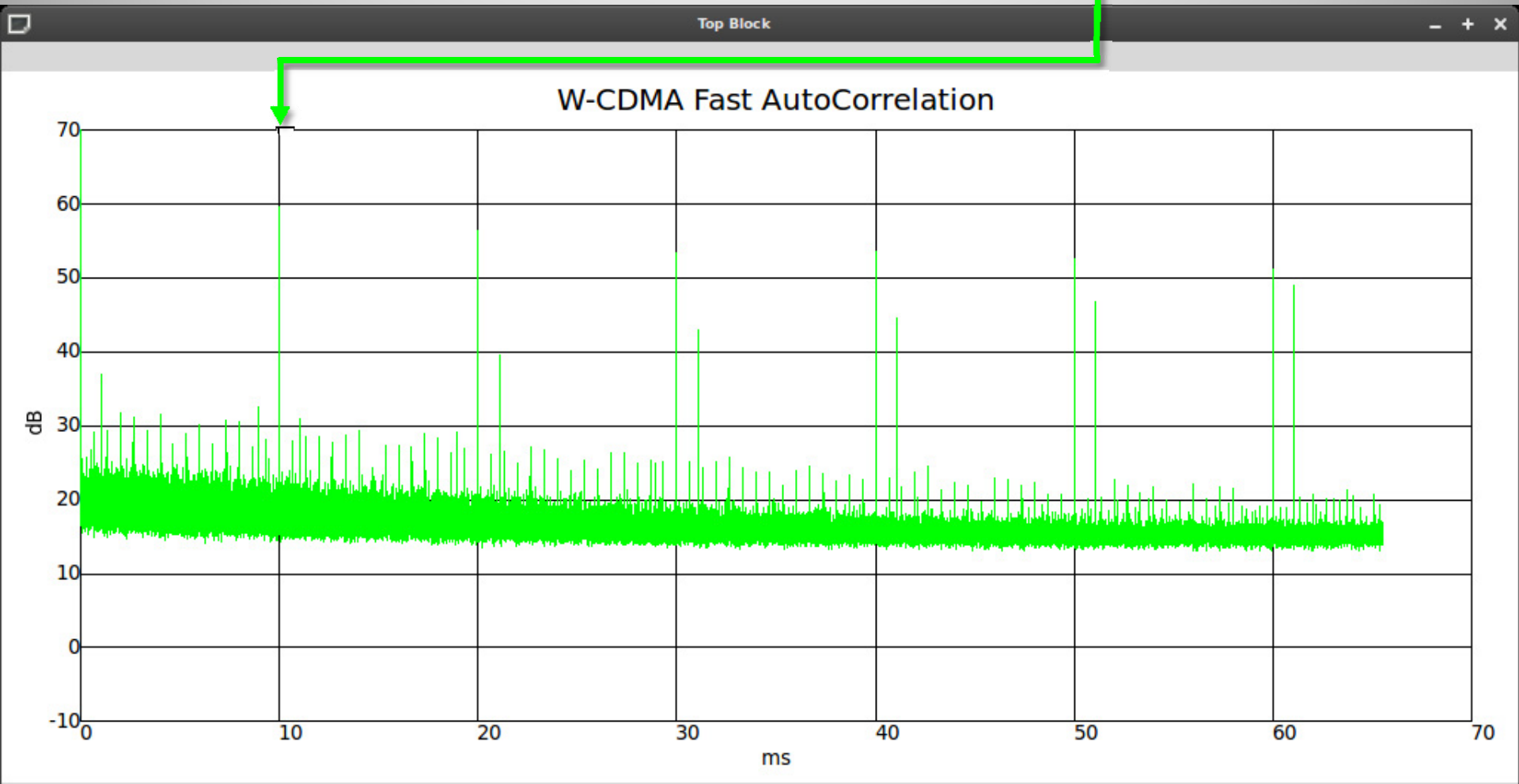


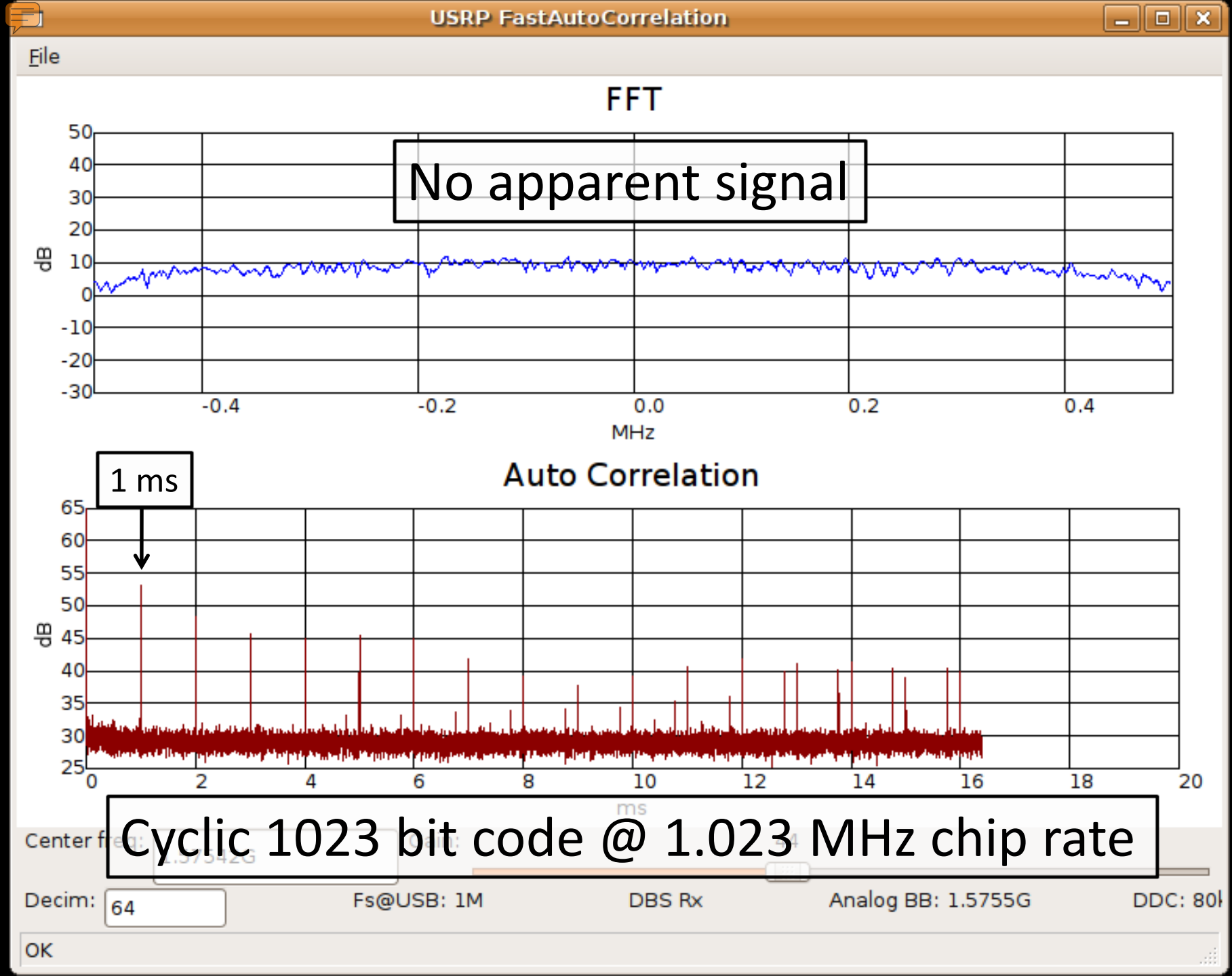
CDMA Detection with GRC

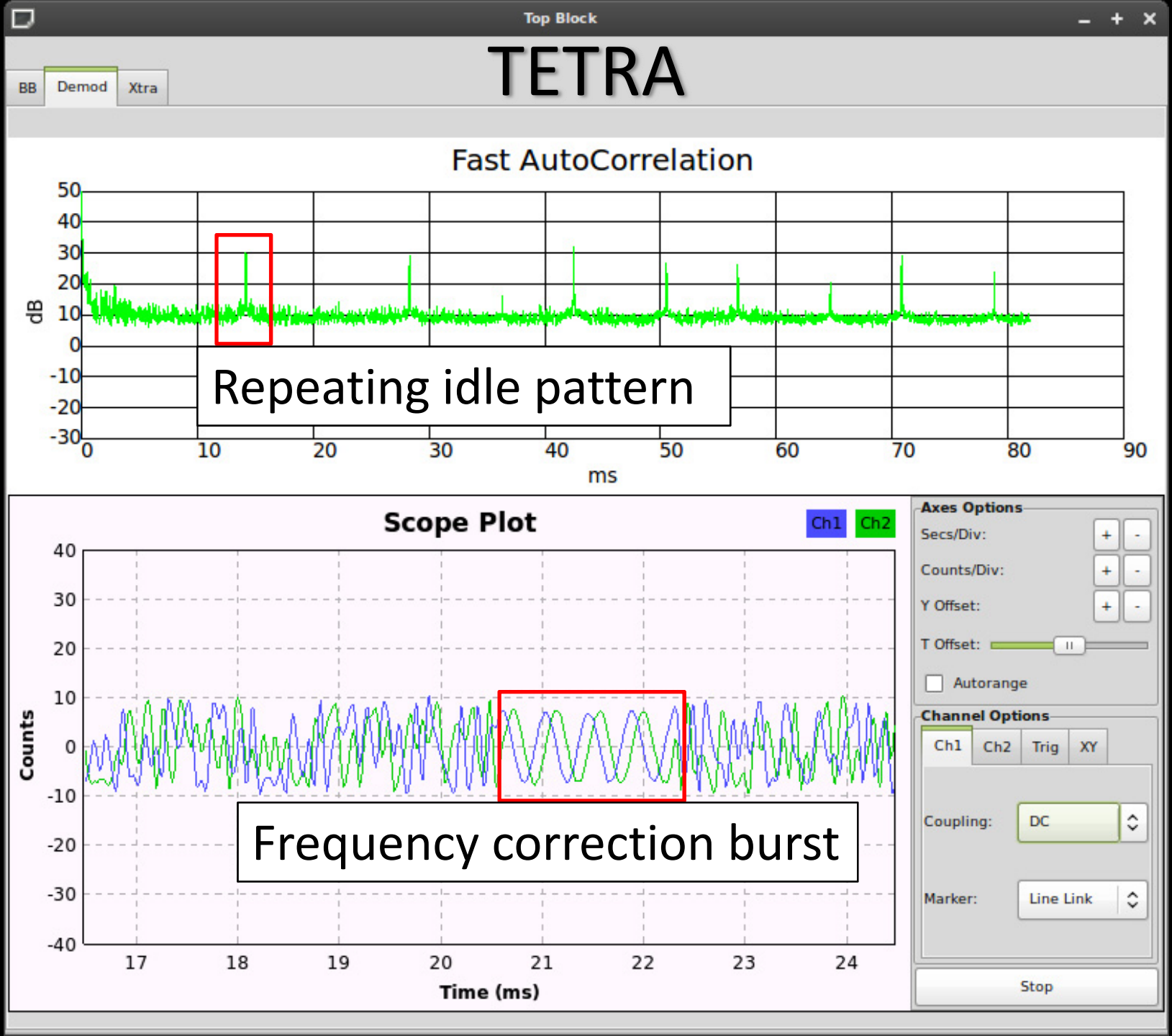


3G W-CDMA

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

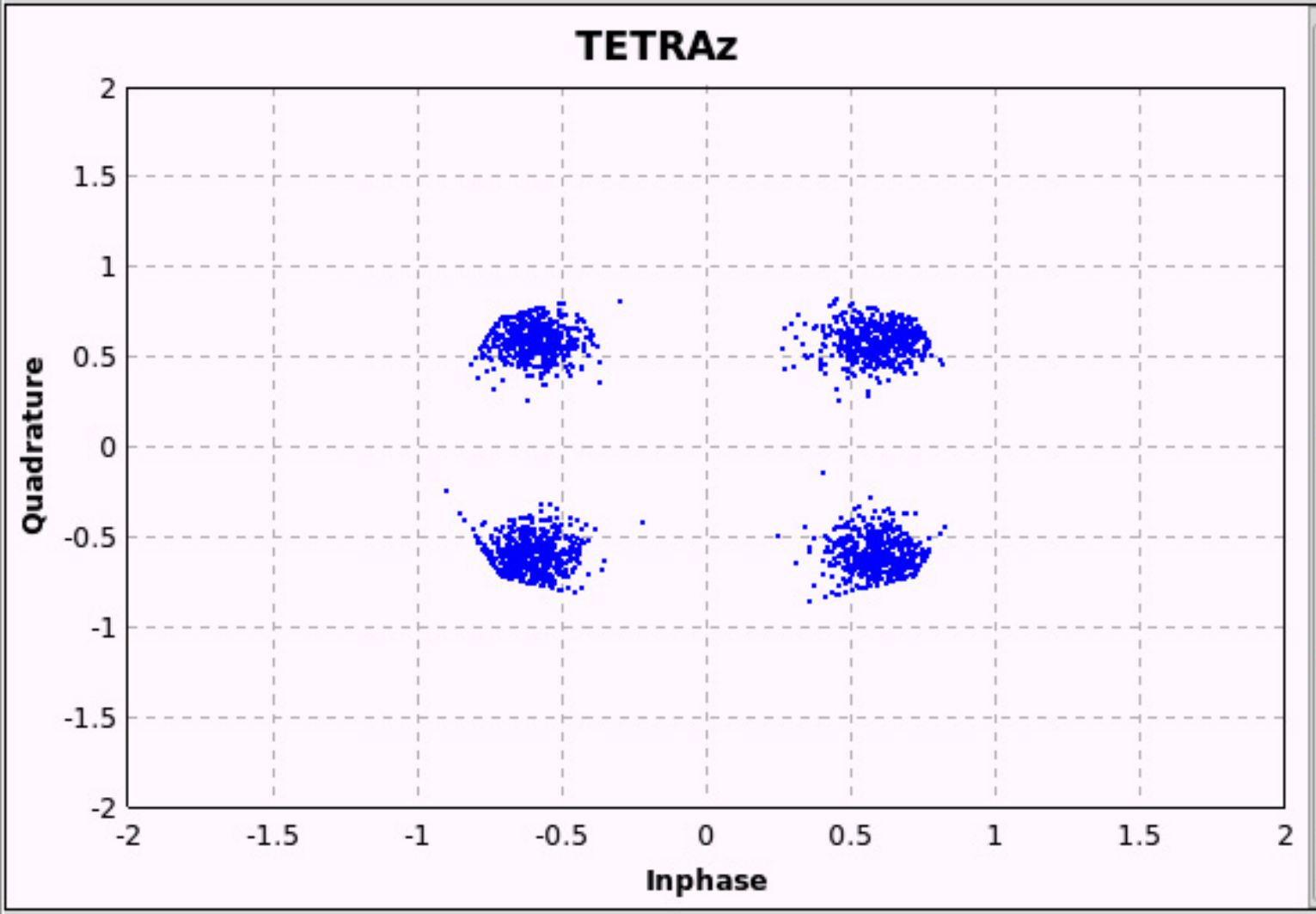



USRP FastAutoCorrelation
File
FFT
No apparent signal
50
40
30
20
10
0
-10
-20
-30
dB
-0.4
-0.2
0.0
0.2
0.4
MHz
1 ms
Auto Correlation
65
60
55
50
45
40
35
30
25
dB
0
2
4
6
8
10
12
14
16
18
20
ms
Cyclic 1023 bit code @ 1.023 MHz chip rate
Center freq:
Decim:
64
Fs@USB: 1M
DBS Rx
Analog BB: 1.5755G
DDC: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


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

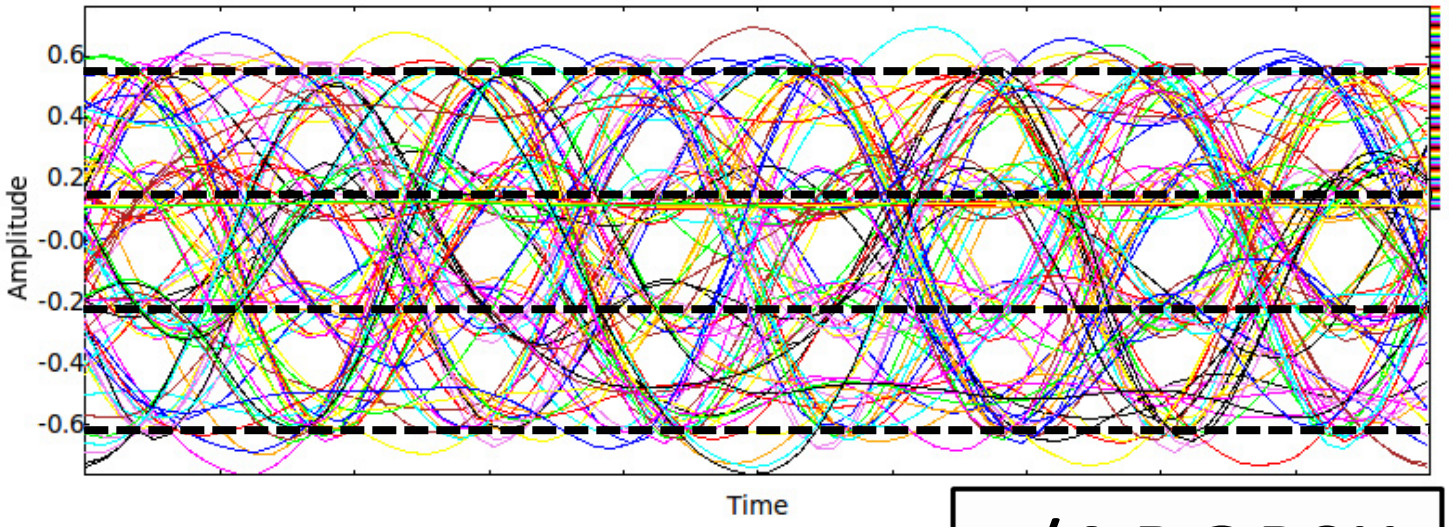
Symbol rate (coarse): 0

Symbol rate: 18000

Samples per symbol: 80

Num plots: 100

Data Scope



π/4 DQPSK

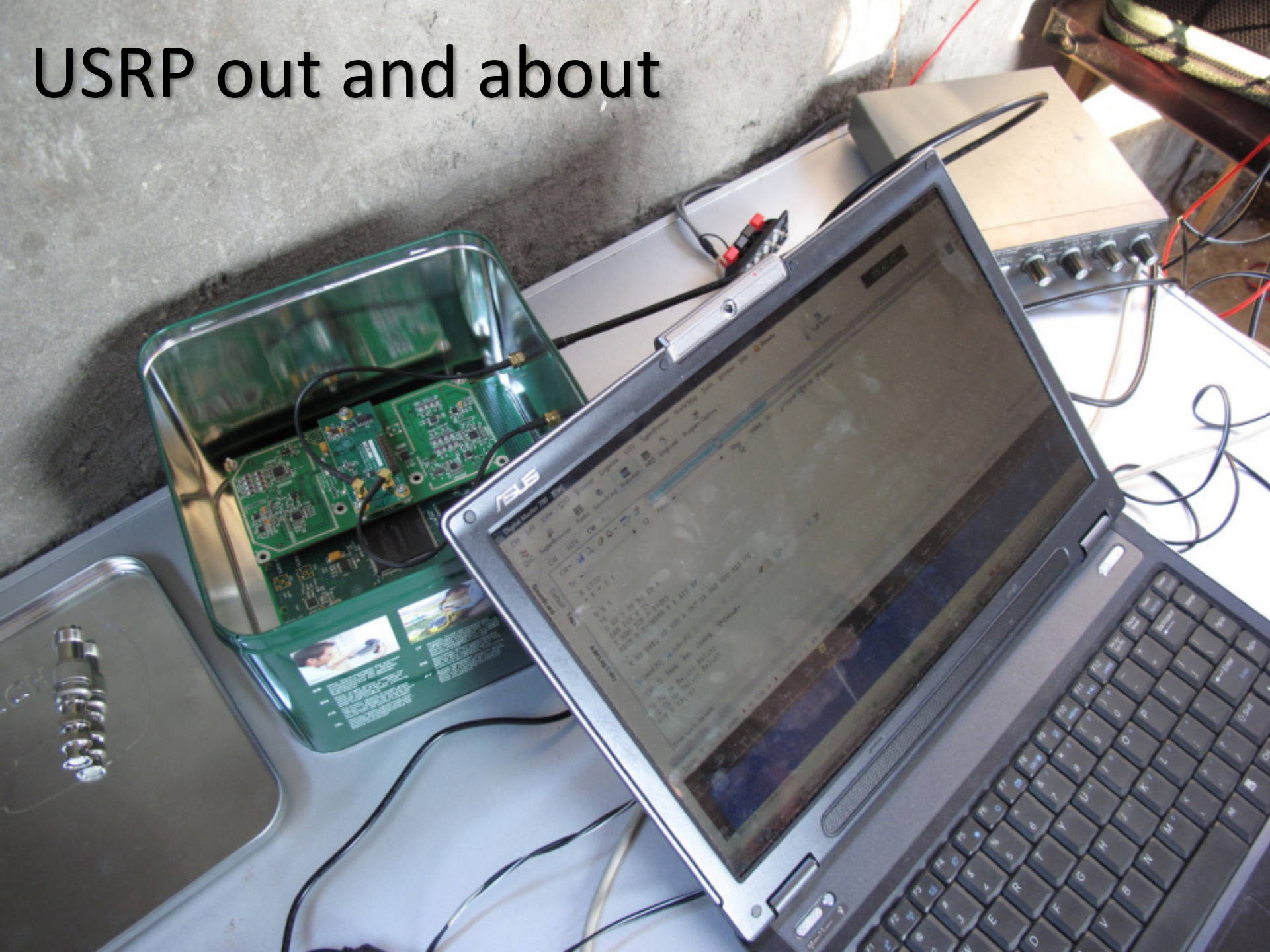
Fine Offset: 0

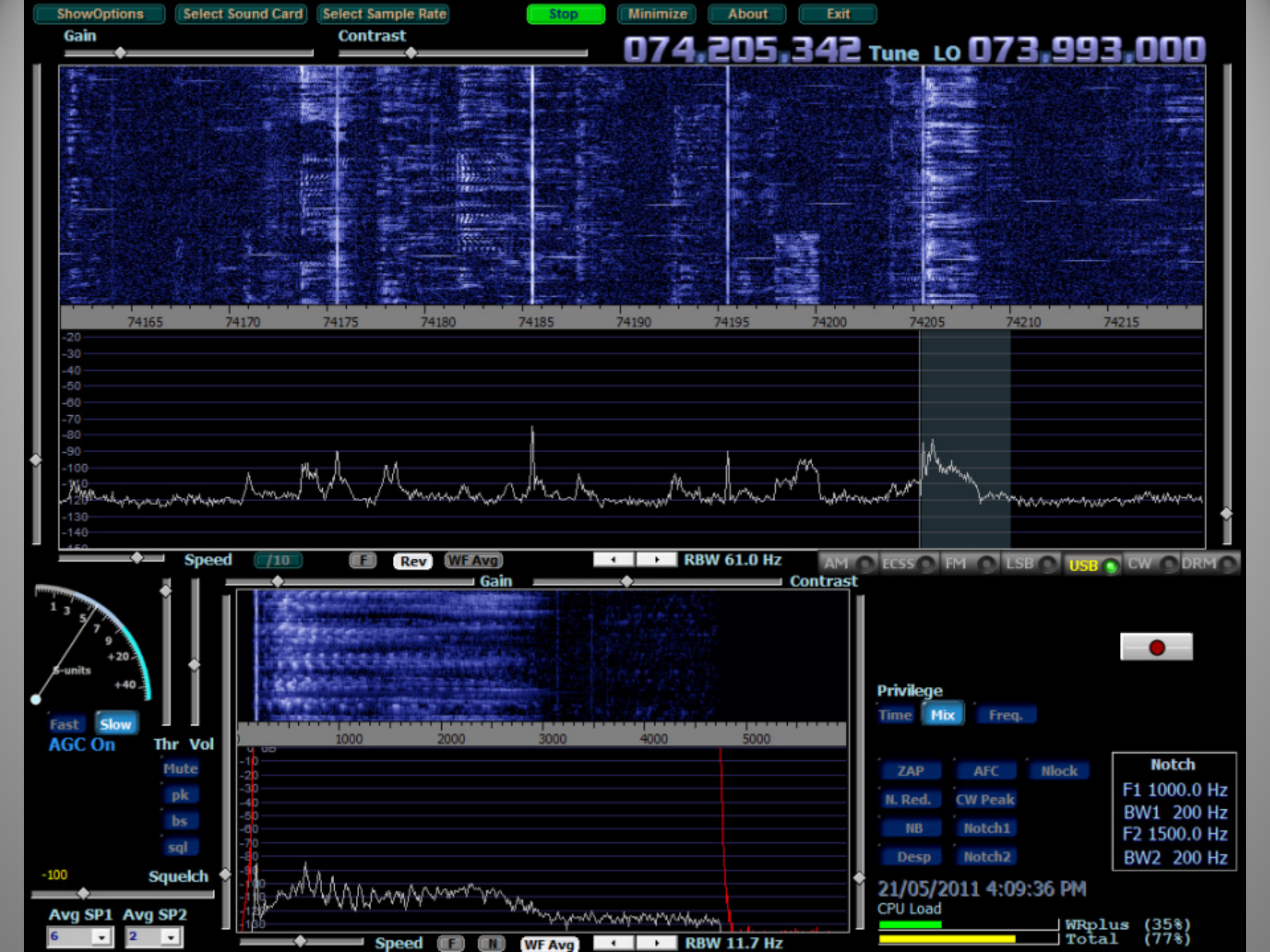
Coarse offset: 0

Xlate Offset: 117.708k

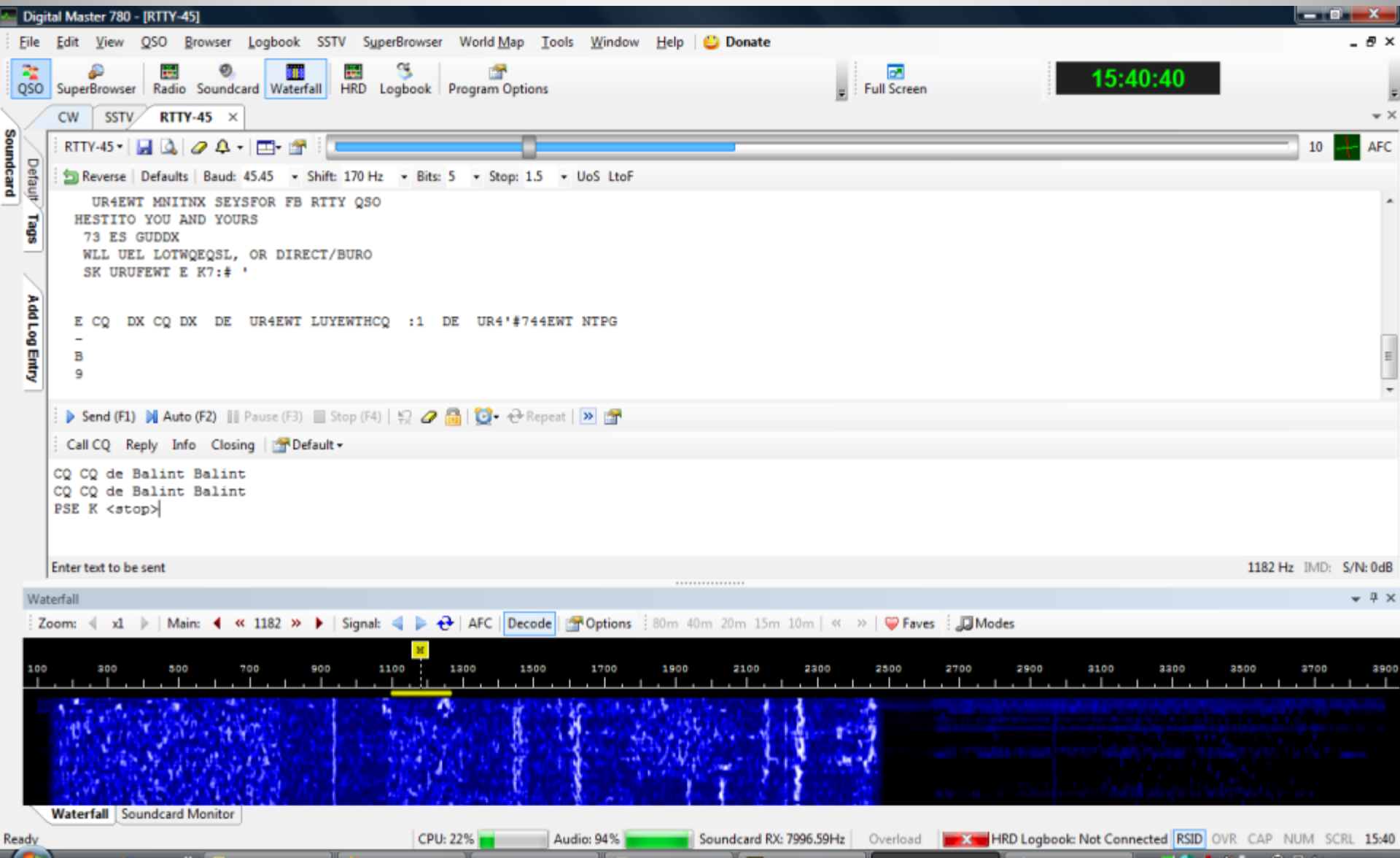
Xlate BW: 34.4375k

USRP out and about

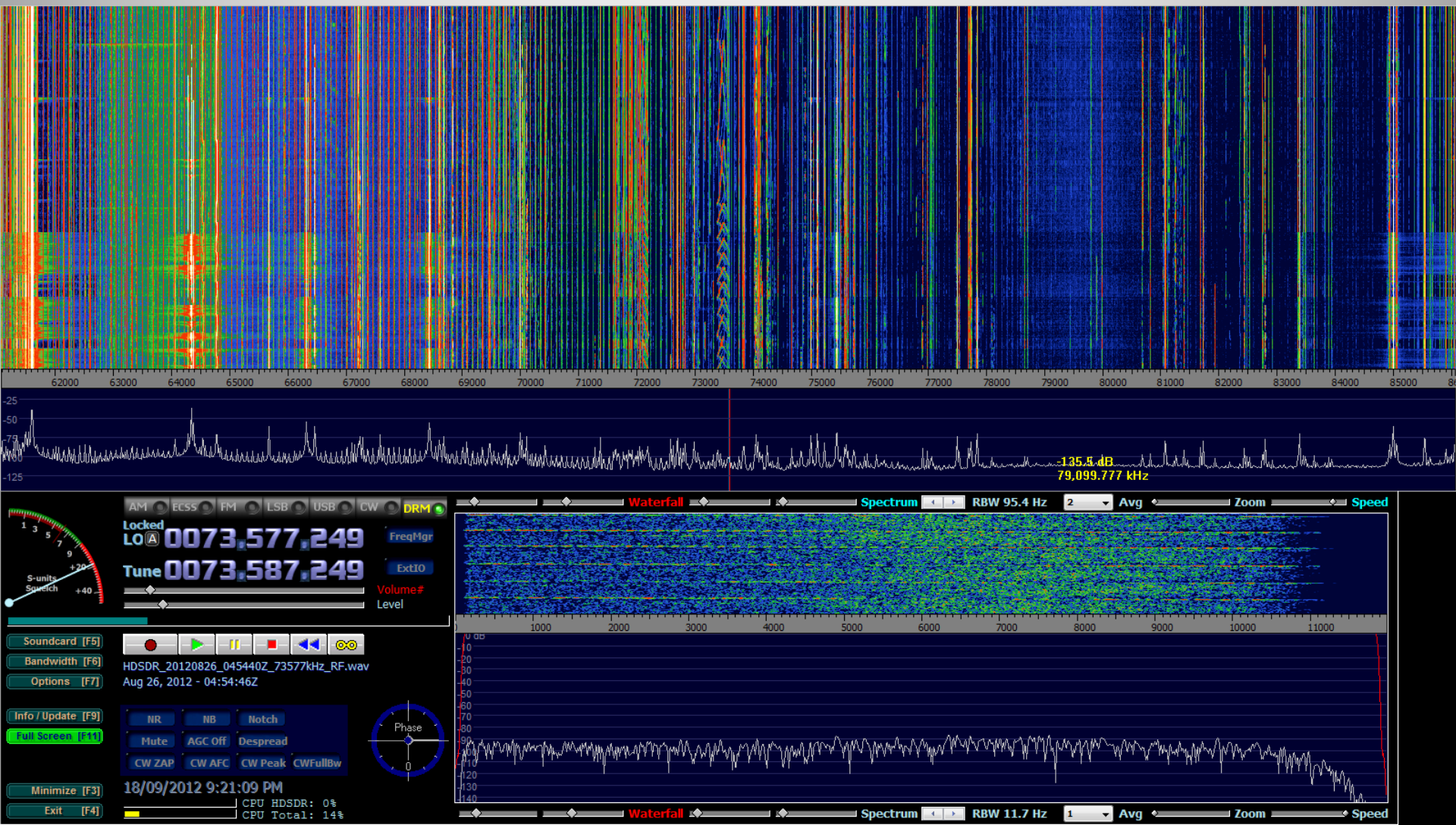



ShowOptions
Select Sound Card
Select Sample Rate
Stop
Minimize
About
Exit
Gain
Contrast
074.205.342 Tune LO 073.993.000
74165
74170
74175
74180
74185
74190
74195
74200
74205
74210
74215
-20
-30
-40
-50
-60
-70
-80
-90
-100
-110
-120
-130
-140
Speed
/10
F
Rev
WF Avg
RBW 61.0 Hz
AM
ECSS
FM
LSB
USB
CW
DRM
Gain
Contrast
1
3
5
7
9
+20
+40
S-units
Fast
Slow
AGC On
Thr
Vol
Mute
pk
bs
sql
-100
Squelch
Avg SP1
Avg SP2
6
2
1000
2000
3000
4000
5000
Speed
F
N
WF Avg
RBW 11.7 Hz
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
21/05/2011 4:09:36 PM
CPU Load
WRplus (35%)
Total (77%)

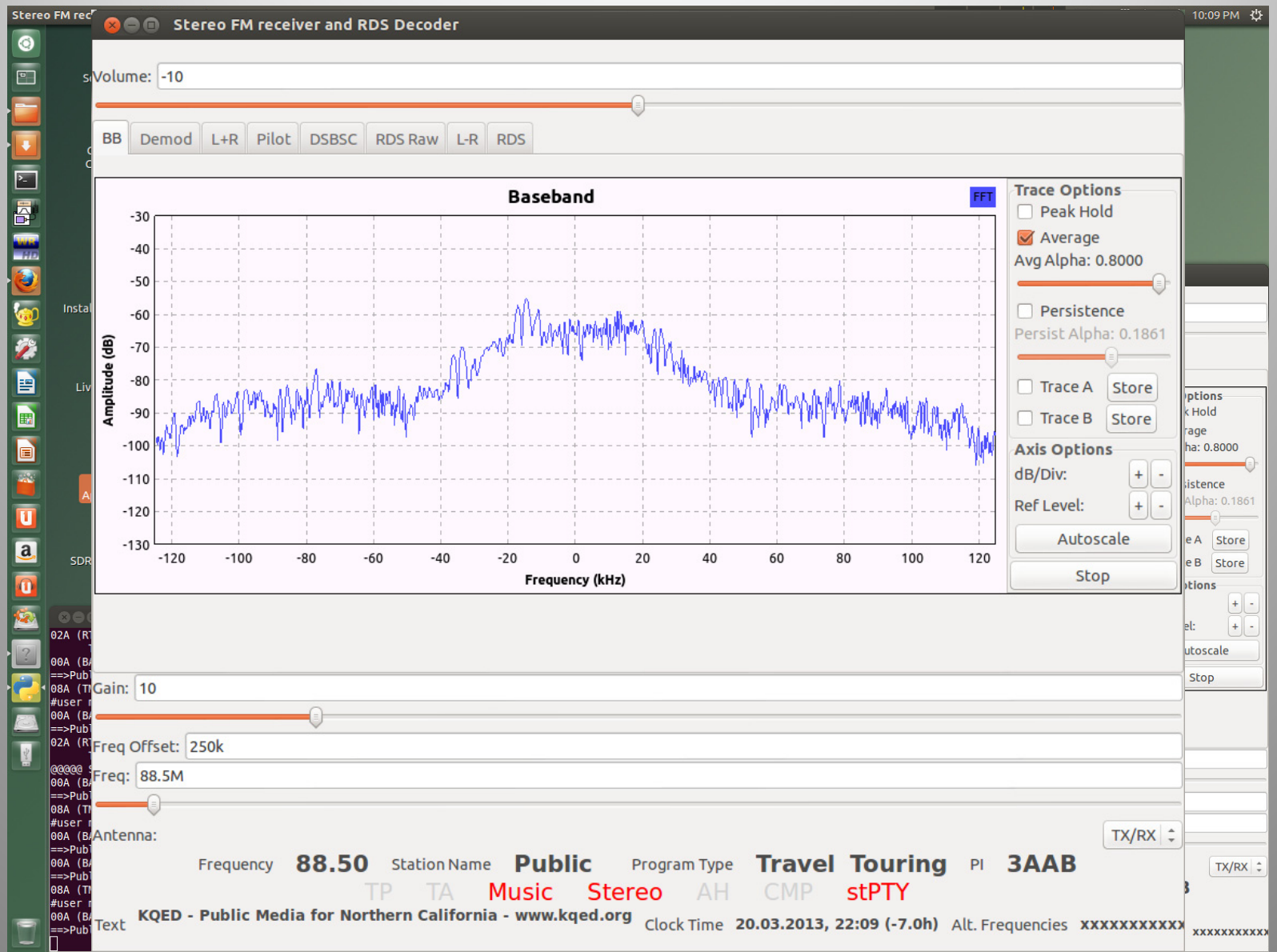
Amateur Digital Modes



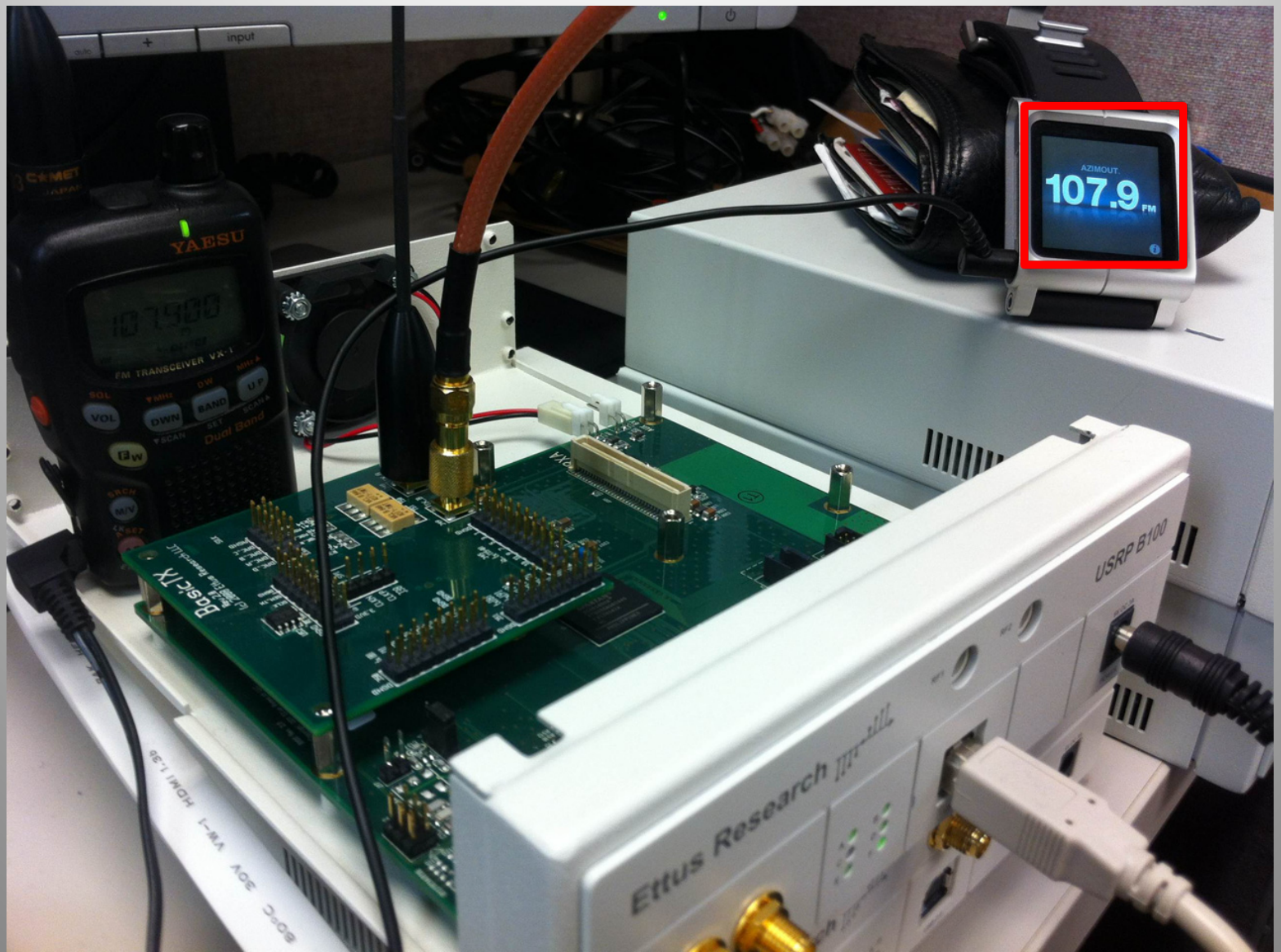
The Entire HAM Band



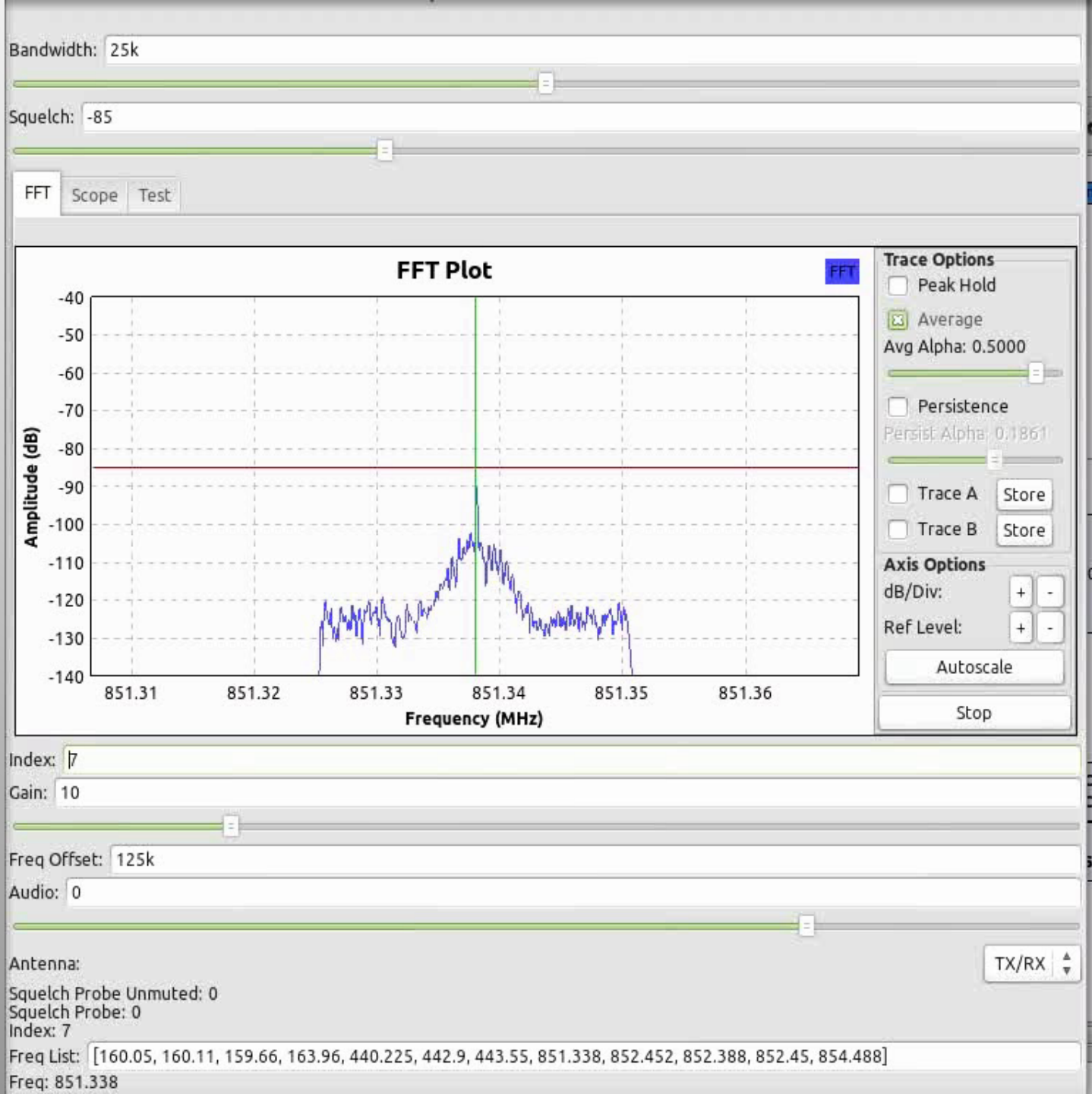
Stereo FM with RDS: Receiver



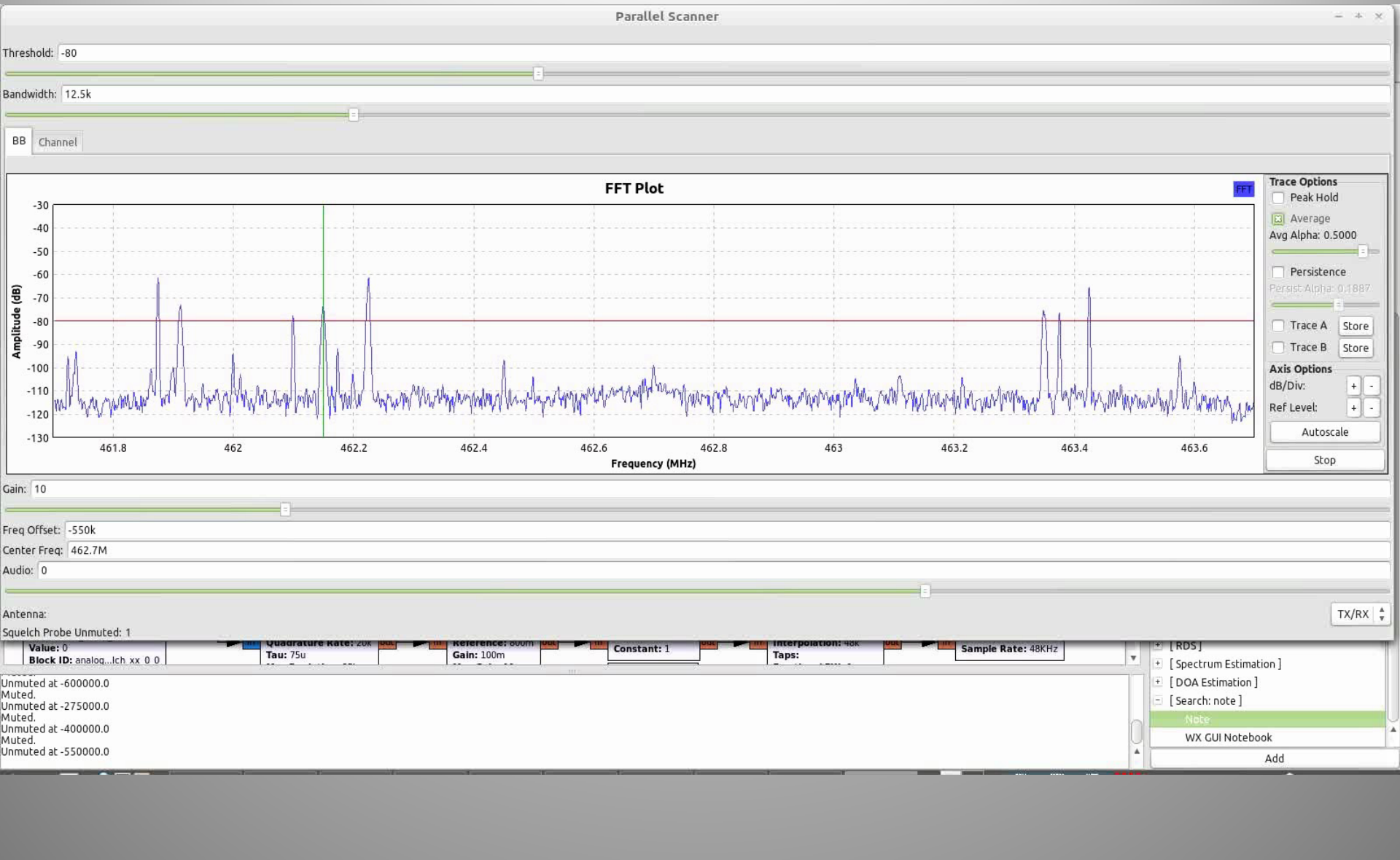
Stereo FM with RDS: Transmitter



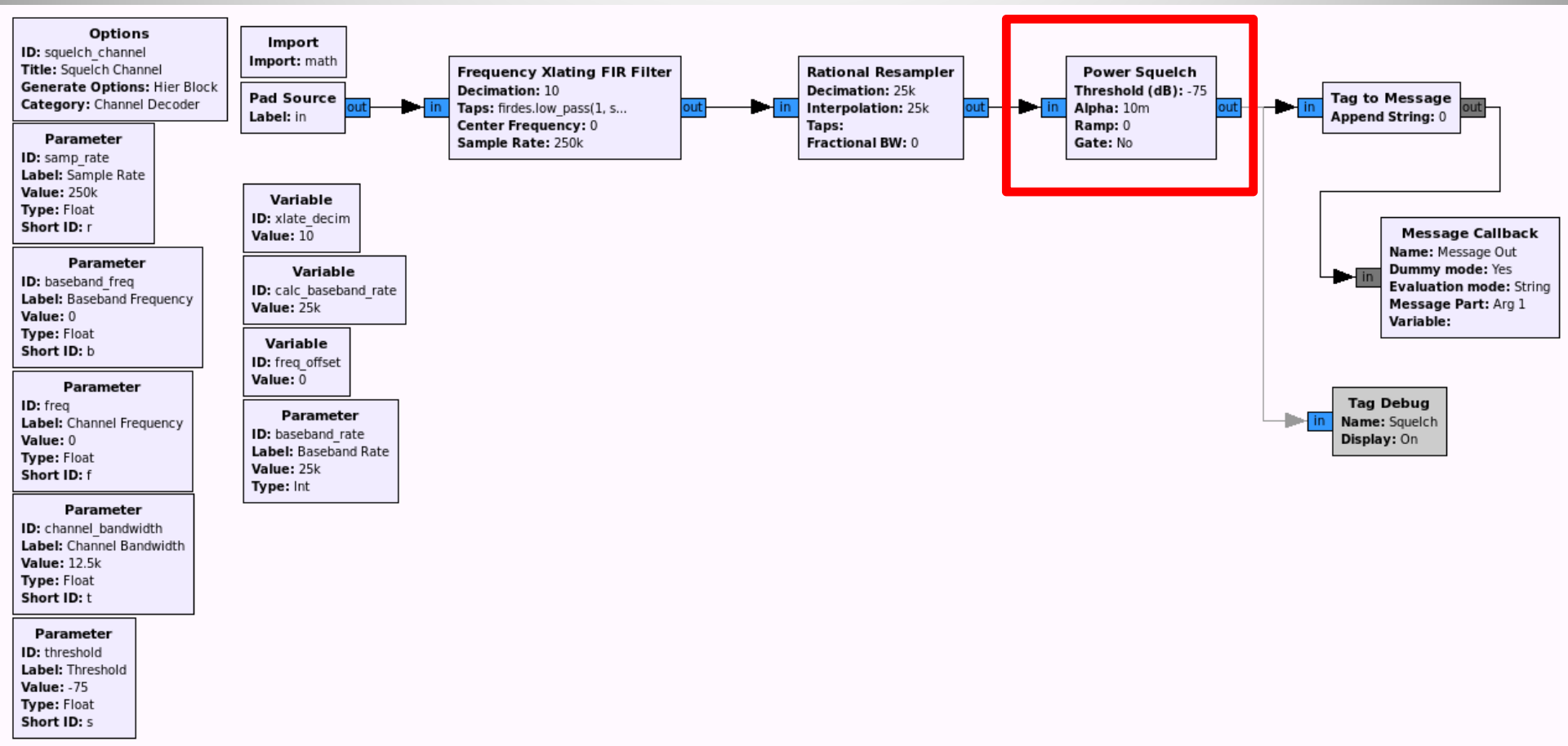
Sequential Scanning



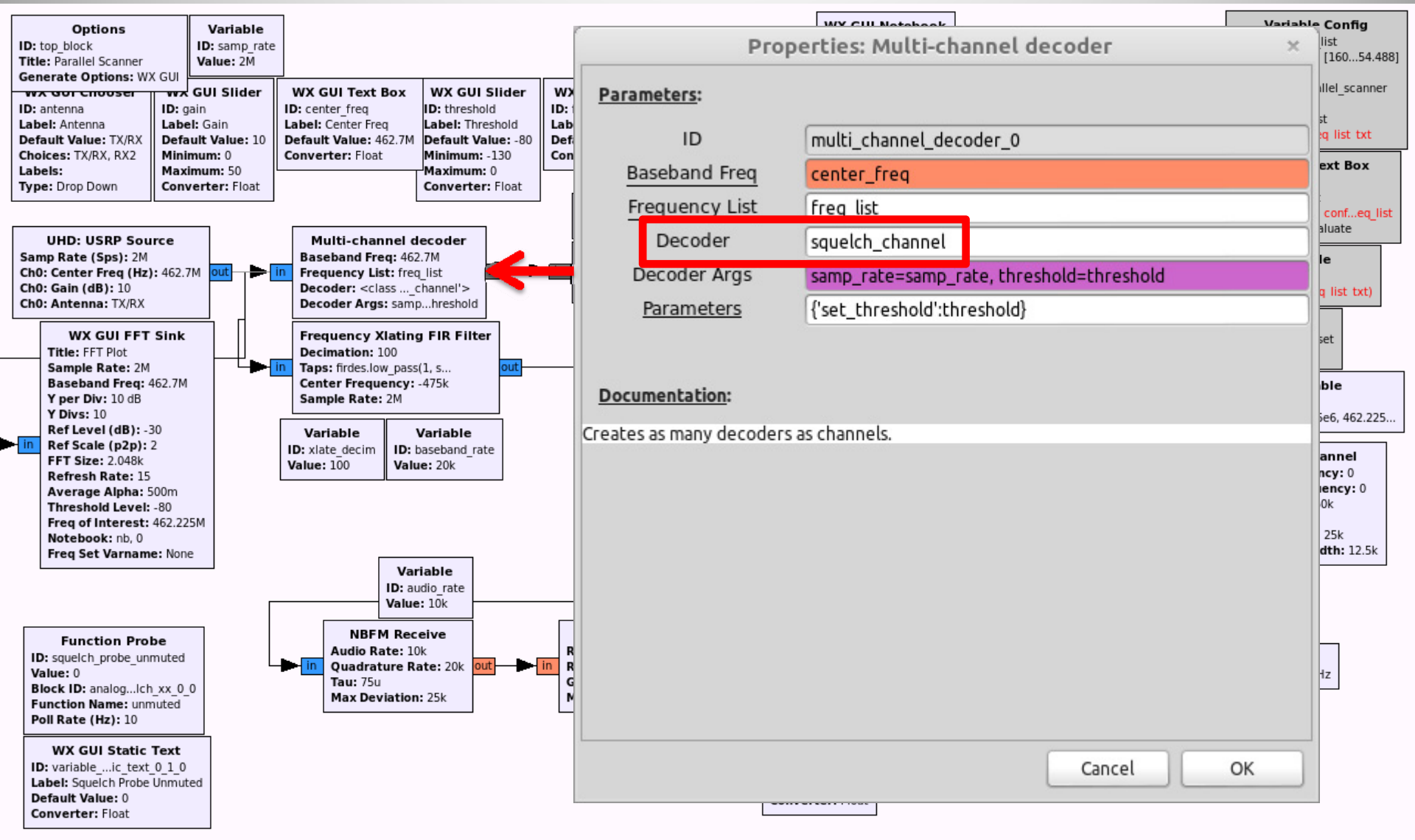
Parallel Decoding



Parallel Decoding: 1

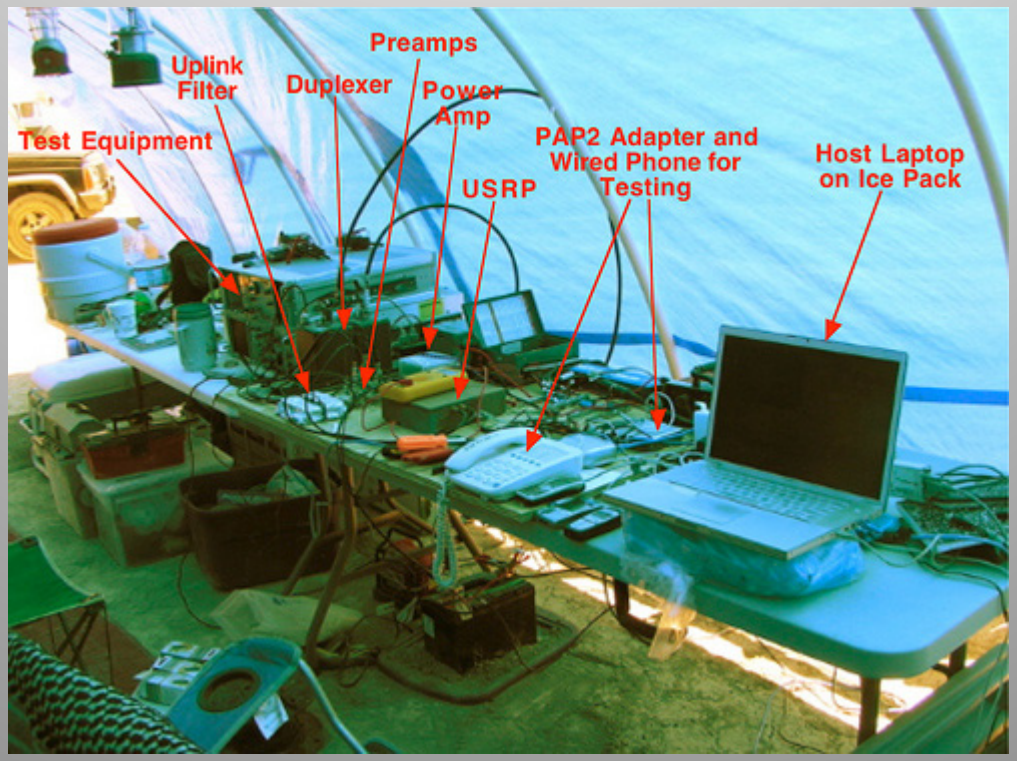


Parallel Decoding: N



OpenBTS

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



802.11agp decoding

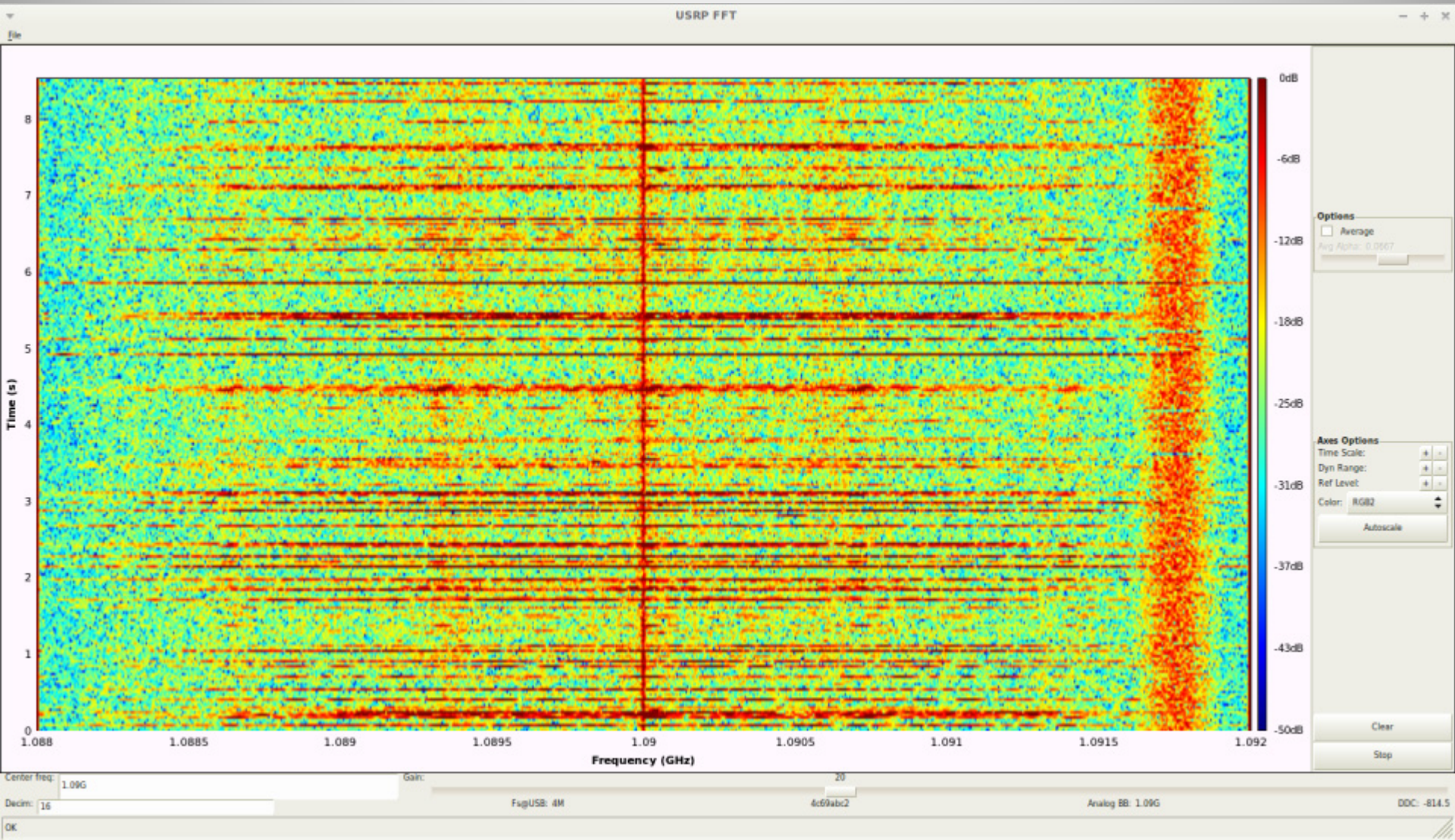
- 10/20 MHz OFDM
- gr-ieee-802-11
- BPSK & QPSK

Other Applications of SDR

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

- Much more…

Mode S Waterfall



Frank's Fantastically Fabulous

radiorausch

recreational! raw! rutabagas! riveting! random! rdlap! ridiculous! redundant!

radio related rambling

Four Level FSK & Motorola RD-LAP: Perhaps you have an interest in some of the following topics:

- Technical characteristics of Motorola's RD-LAP wireless data transmission protocol (same protocol as used on DataTAC networks).
- A real world example of TCM (Trellis Coded Modulation). For a nice introduction to TCM please see tutorial 23b at complextoreal.
- MDTs (Mobile Data Terminals) / MDCs (Mobile Data Computers), especially as related to public safety and police use in the greater Huntsville, Alabama area.
- The FBI's NCIC database system
- Security aspects of such systems vis a vis the scanner radio enthusiast
- A delightfully stimulating application of the Ettus Research USRP and the GNURadio based SDR

Illustration 1: Sample Mode S Transponder Squawk received on 1090 MHz with 3.2MHz sample rate.

Equipment used:

All from Ettus Research (http://www.ettus.com/custom.html):

- USRP With DBSRX 800 MHz – 2.4 GHz Daughterboard
- LP0926 Log Periodic Antenna

The sampling rate was selected at 3.2MHz (USRP decimation 20) to avoid DBSRX or computer generated frequency spurs that appear at ±2 MHz relative to 1090 MHz. Aviation transpond selected bandwidth is thus sufficient to catch each individual pulse.

MODE S Data Example:

The data from the illustration above is sliced at a level of about 250 A.U. and then processed into a stream of 0.5 µS pulses. After the 8 µS Mode S header we have a stream of data bits en for a '0' bit; the data bit rate is 1 megabit / second. With received data highlighted in yellow the above example becomes:

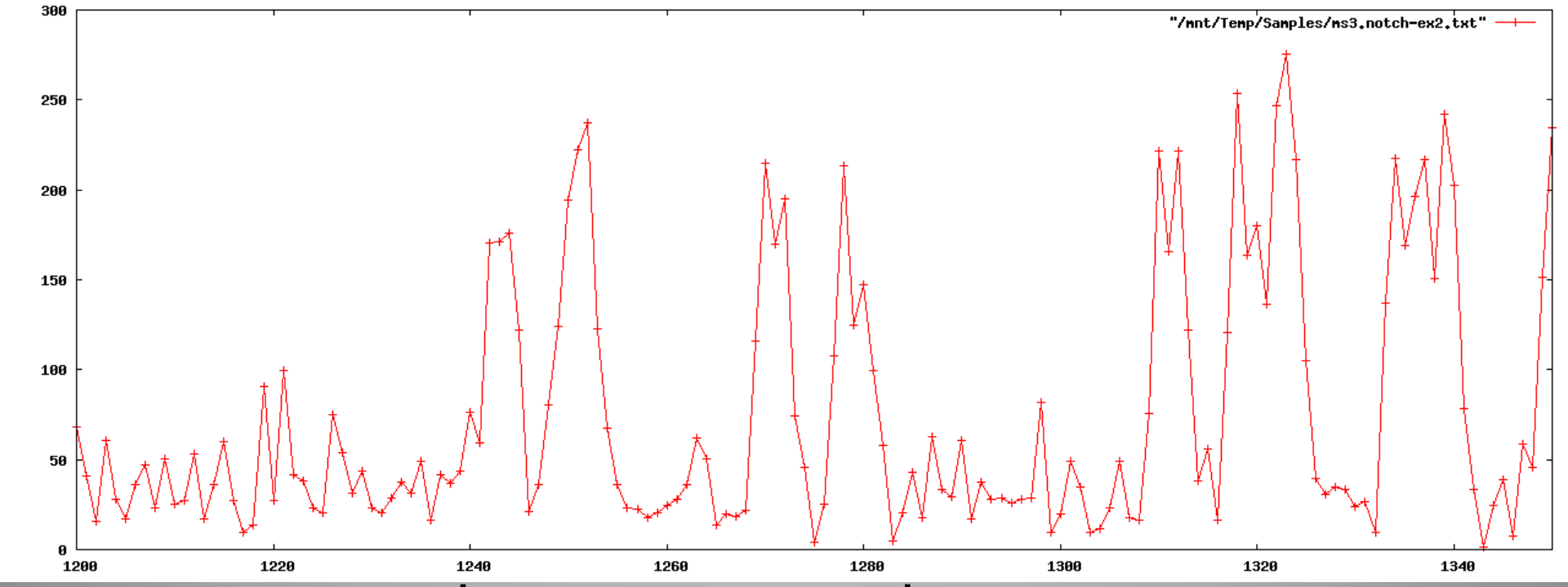
1010000101000000	MODE S Header: Pulses at 0, 1, 3.5, and 4.5 µS
0110011010 0 1 0 1 1	Format Number: DF = 11; (ALL CALL REPLY)
100110 1 0 1	Capability
10011001011001101010011010011010011001010110101001 1 0 1 0 0 1 0 1 1 1 0 1 1 0 1 1 0 1 0 0 1 1 1 0	MODE S Address: Hex A5DB4E (or 51355516 octal)
10101010011001101010101001101010011001010101010101 1 1 1 1 0 1 0 1 1 1 1 1 0 1 1 1 0 1 0 0 0 0 0 0	Parity

Downlink format (DF) 11 does not include altitude information. However, just with the MODE S address we may go to web pages such as http://www.airframes.org/ and learn more abou number N477CA, type, owner, et cetera.

Receivable 1090 MHz Traffic:

MODE C	Traditional aircraft squawk codes
MODE S	Traditional aircraft squawk codes

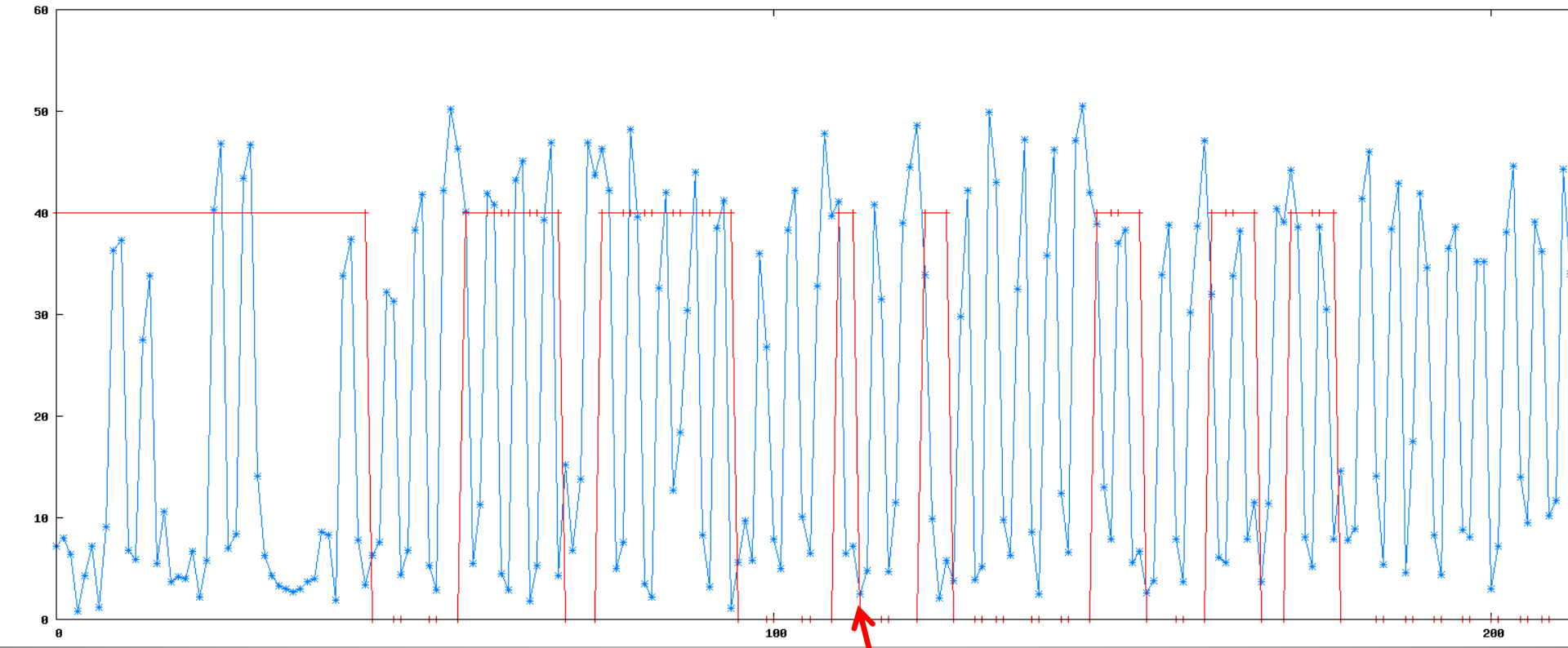
Time Domain



Preamble

Frame →

Time Domain



Preamble

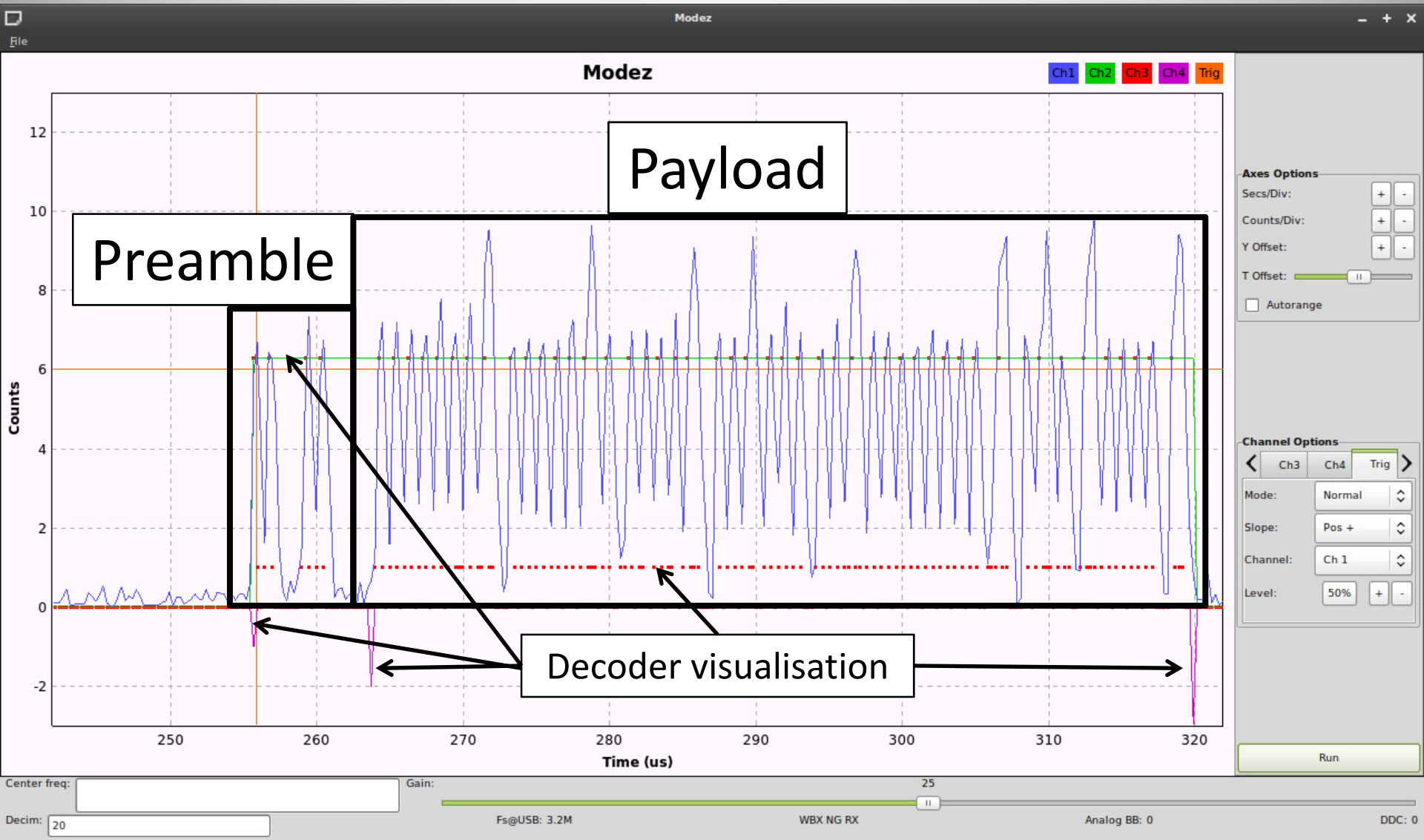
Frame ⟶

Data bits from early/late chips

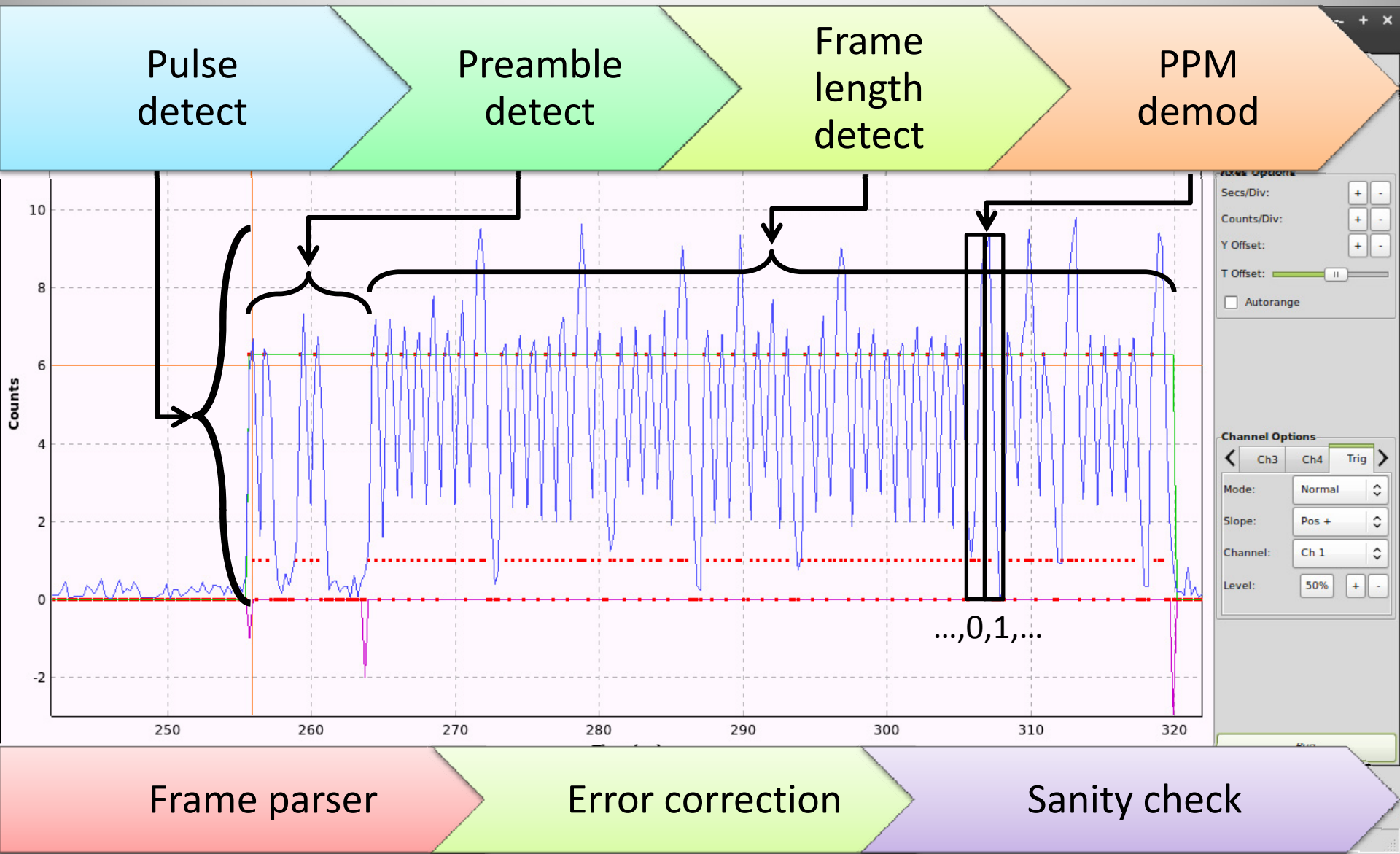
Starting Points

- gr-air by Eric Cottrell
  - Separates processing into several different GR blocks which detect/decode:
    1. Pulses
    2. Mode S preamble
    3. Frame length
    4. PPM chips/bits
- gr-air-modes by Nick Foster
  - Less complex (fewer steps) → better performance
  - Less overhead by using PMTs instead of passing state structs as ‘samples’ through GR runtime

Mode S Response: AM signal



Mode S Decoder Structure

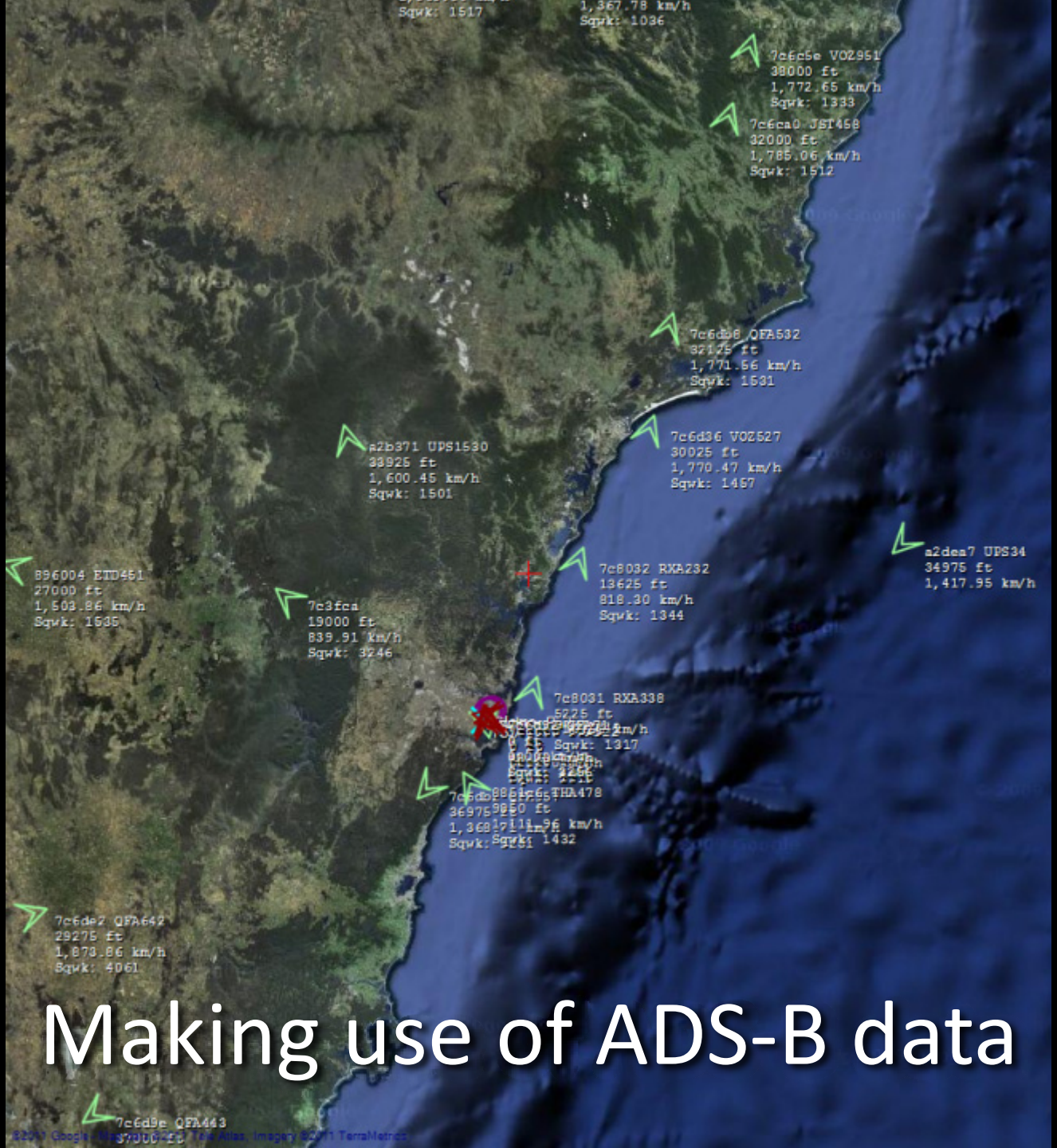


Mode S Frame Types

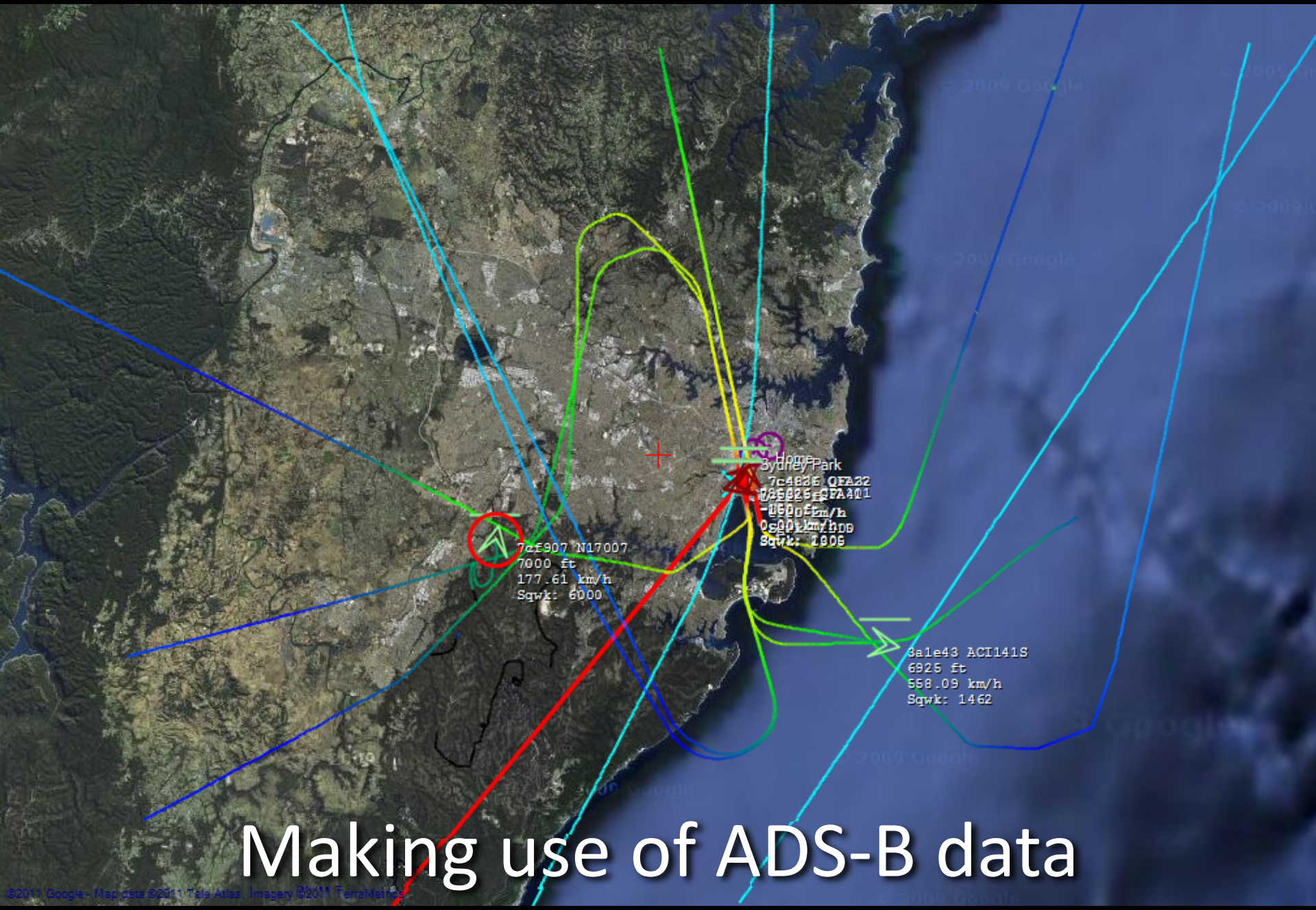
- Several **D**ownlink **F**ormats (DF)
  - Short/long frames (56/112 bits)
- Contains **A**irframe **A**ddress (AA)
  - 24-bit transponder address allocated by ICAO
- Appended CRC
  - ‘Normal’ mode (syndrome = 0)
  - Address overlaid mode (syndrome = AA)
- DF 11: All call, 5/20: Identity (squawk code),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

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

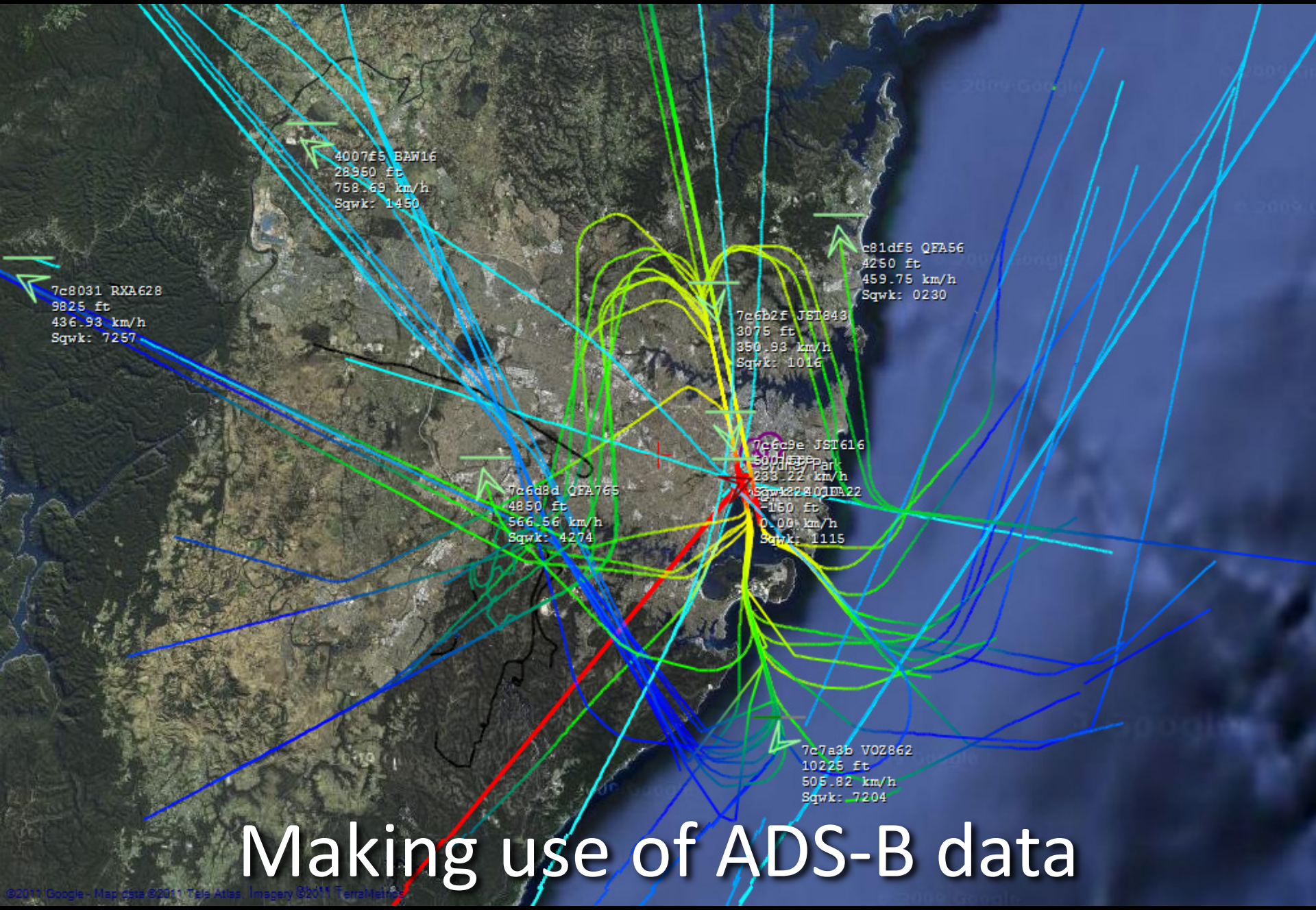
- Several ES types (DF 17):
  - Standard: position, altitude, heading, vertical rate, flight ID, transponder code
  - System information
  - Aircraft capabilities/status (e.g. autopilot enabled)
  - Aircraft intent
  - Traffic information
  - TCAS resolution advisories (“Pull up!”)



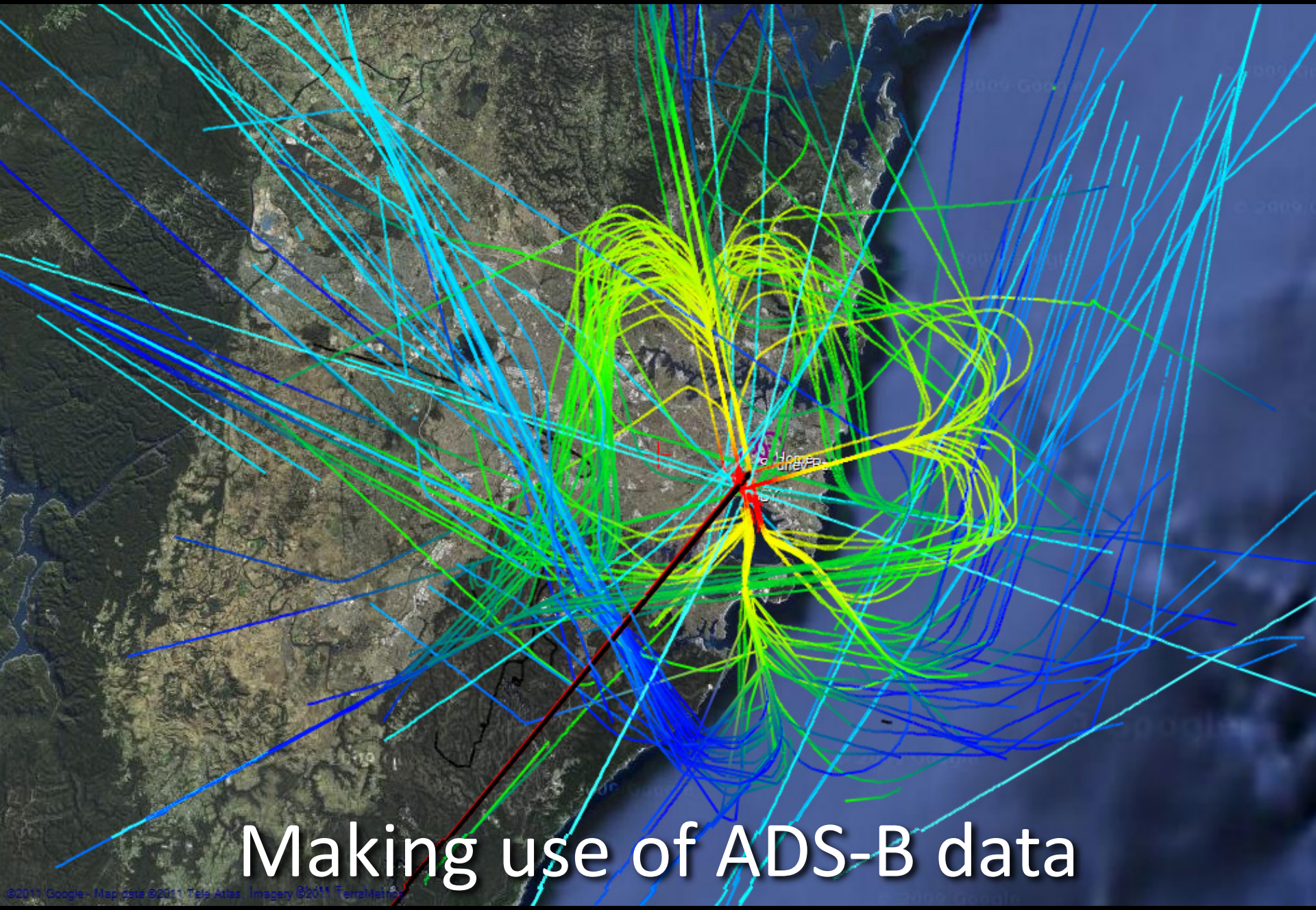
Making use of ADS-B data



Making use of ADS-B data



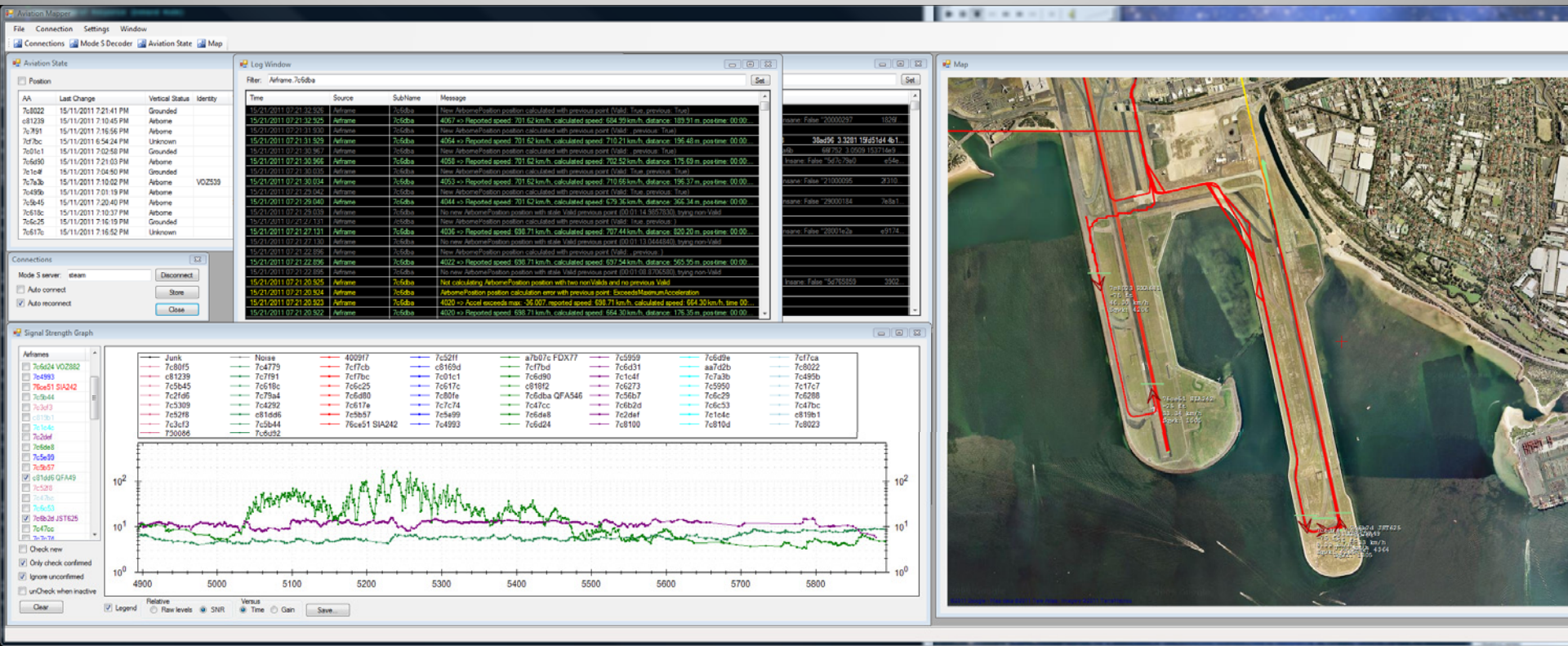
Making use of ADS-B data

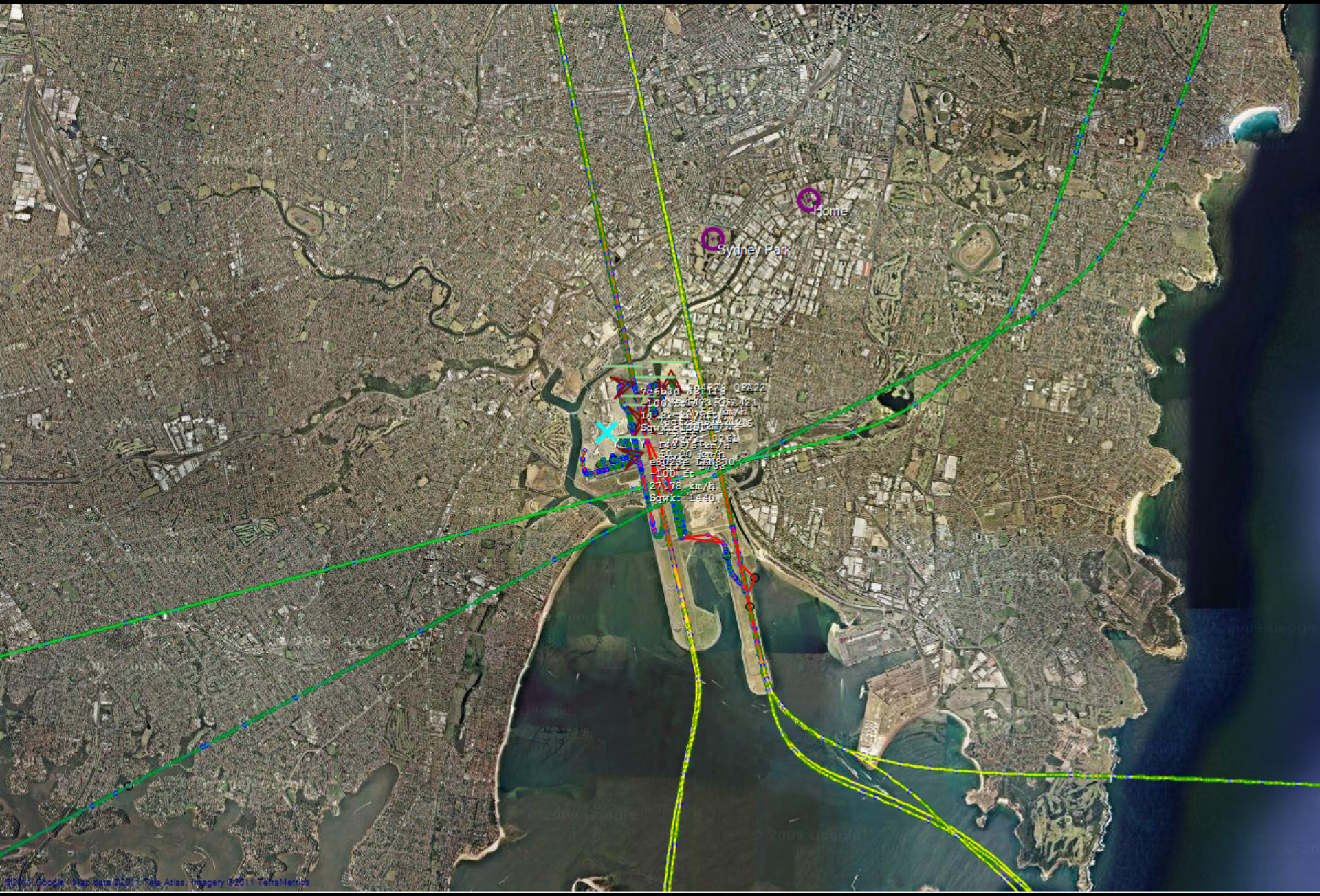


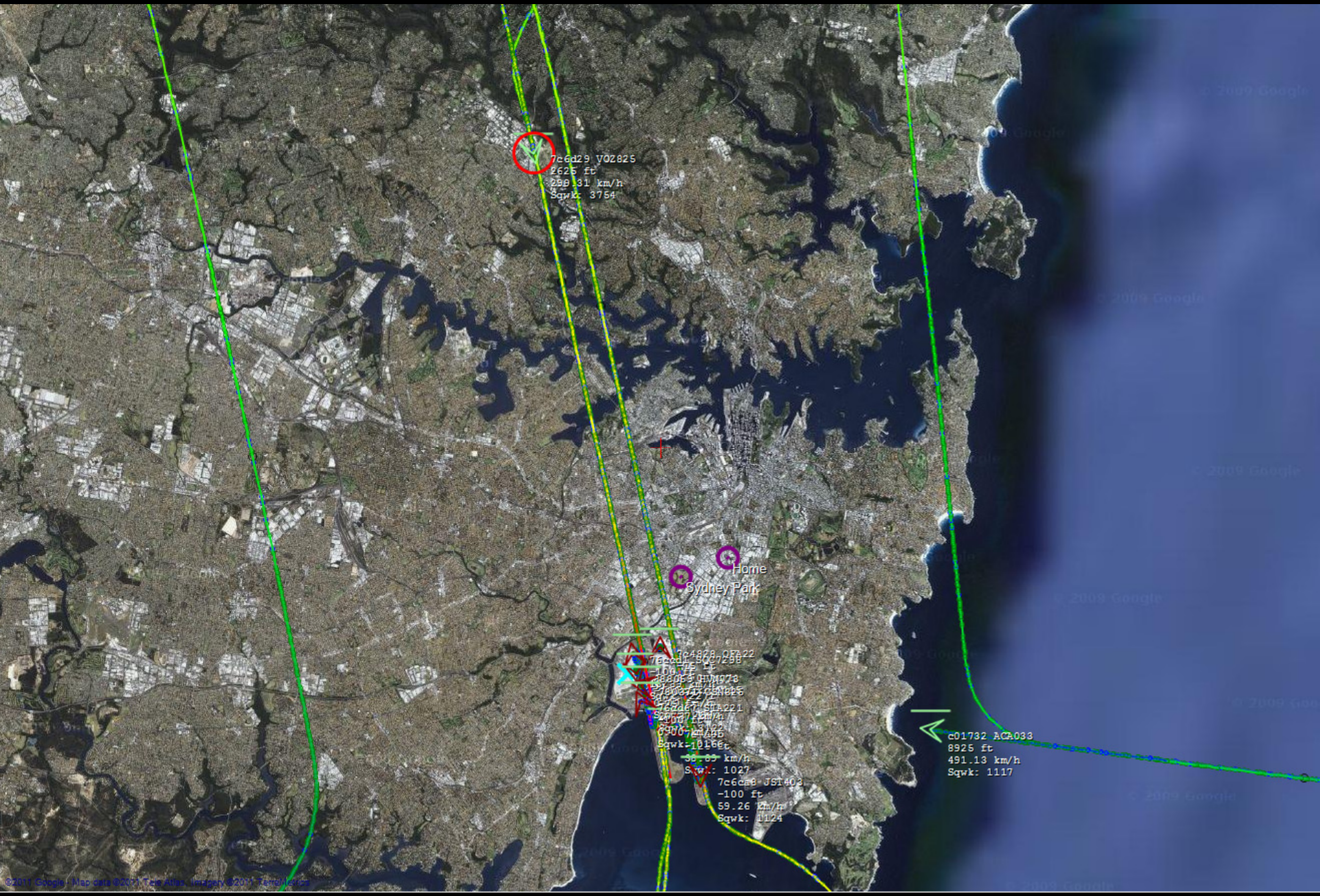
Making use of ADS-B data

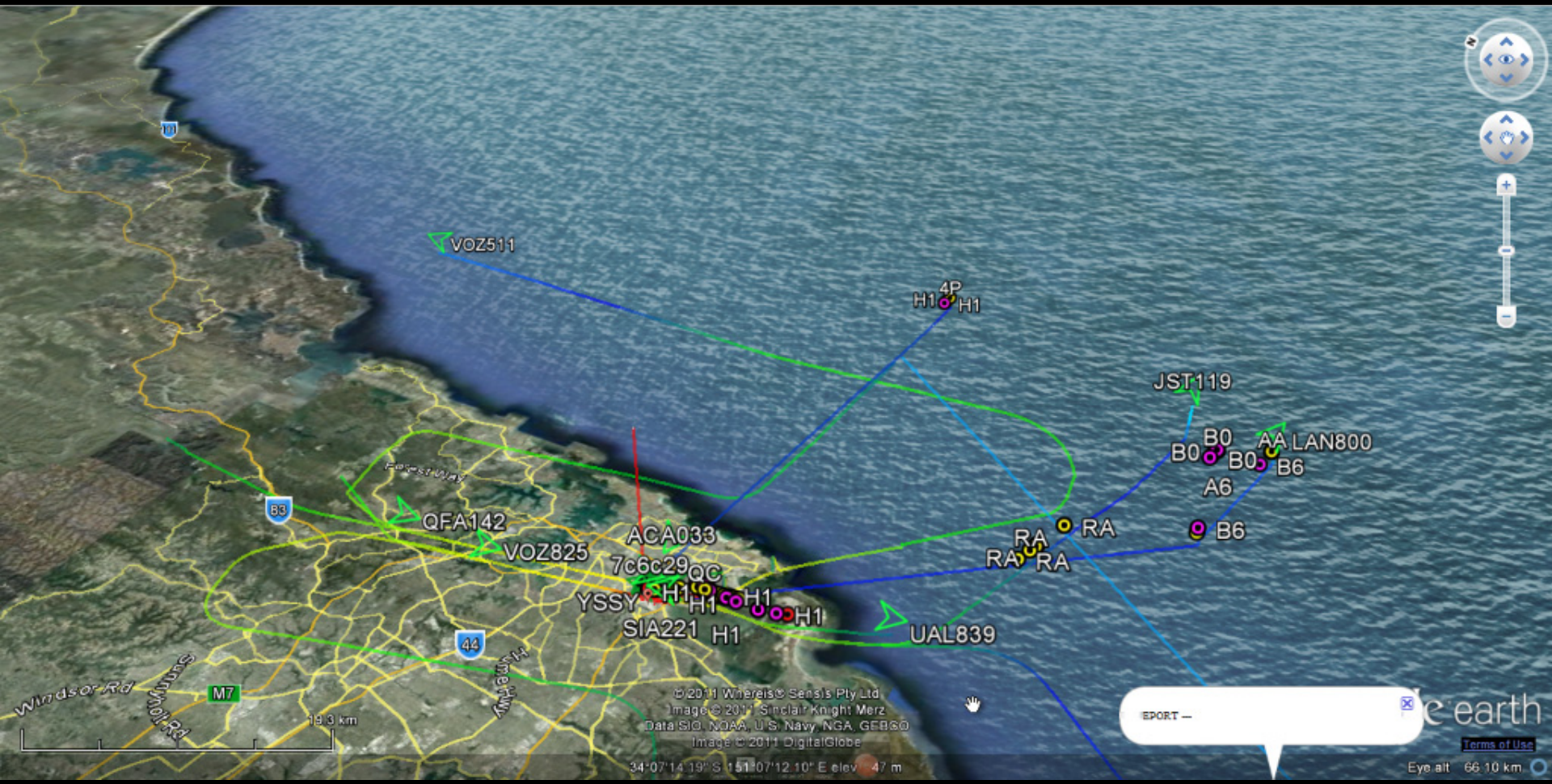
AviationMapper

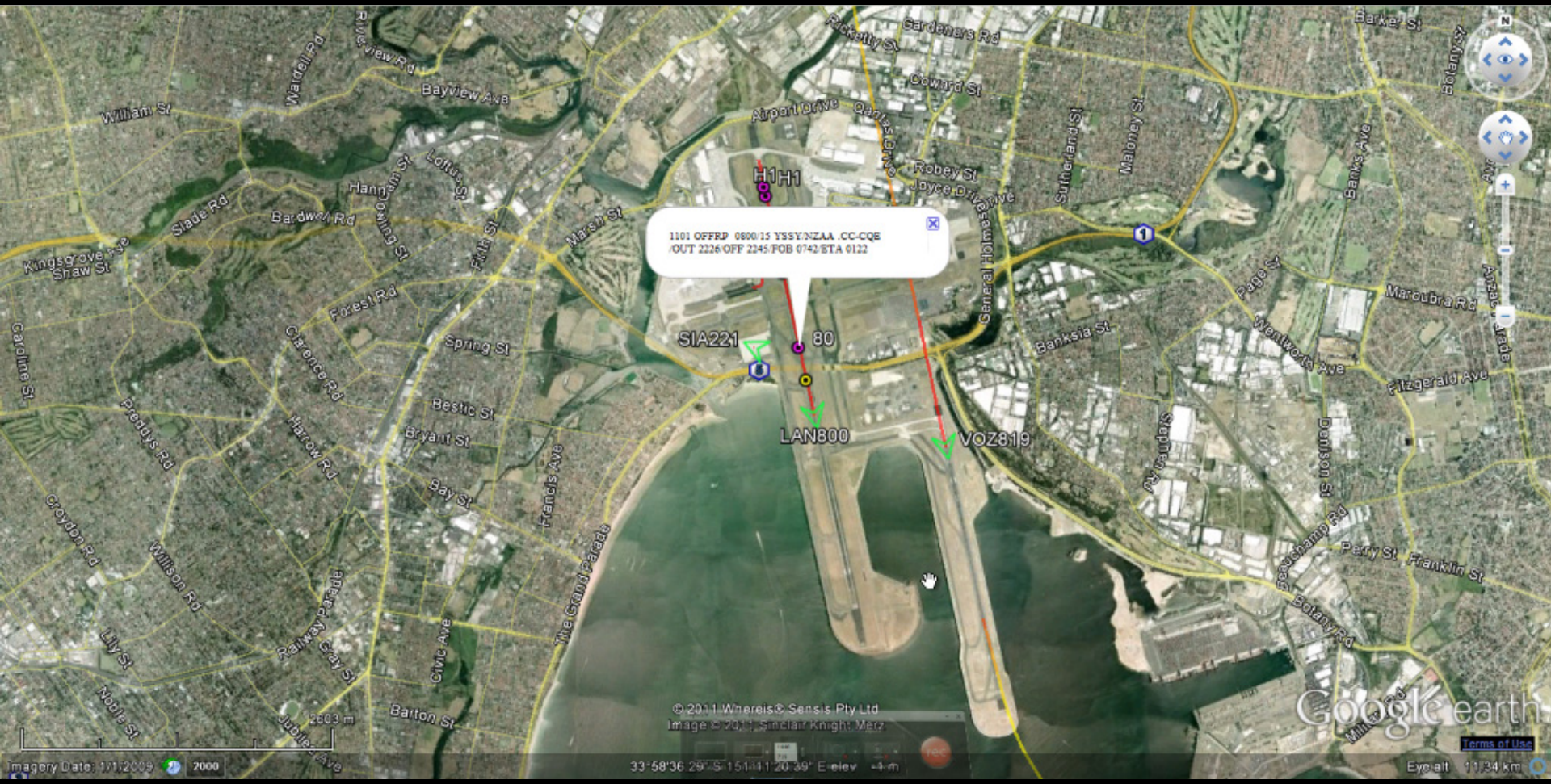
- Connects to Mode S decoder server
- Tracks & plots airframes, collects statistics
- Provides state server for web streaming

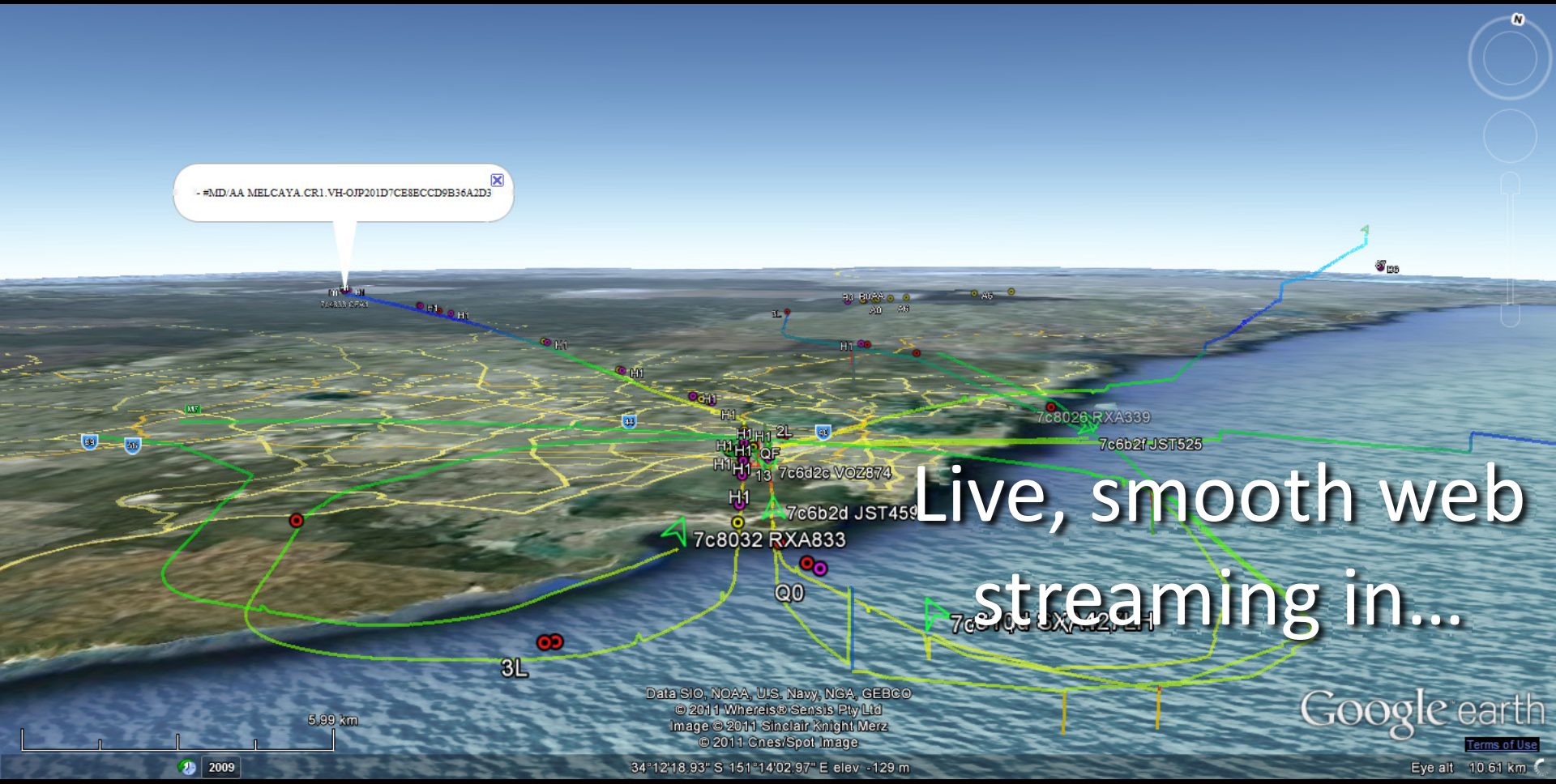



Home
Sydney Park
©2011 Google - Map data ©2011 Tele Atlas, Imagery ©2011 TerraMetrics


7c6d29 VOZ825
2625 ft
298.31 km/h
Sqwk: 3754
Home
Sydney Park
c01732 ACA033
8925 ft
491.13 km/h
Sqwk: 1117
7c6ca8 JST403
-100 ft
59.26 km/h
Sqwk: 1124
Sqwk: 1027
©2011 Google - Map data ©2011 Tele Atlas, Imagery ©2011 TerraMetrics


VOZ511
4P
H1
H1
JST119
B0
B0
AA
LAN800
B0
B6
A6
B6
RA
RA
RA
RA
QFA142
VOZ825
ACA033
7c6c29
QC
YSSY
H1
H1
H1
H1
SIA221
H1
UAL839
B3
44
M7
Windsor Rd
Pennant Hills Rd
Hills Hwy
19.3 km
© 2011 Whereis® Sensis Pty Ltd
Image © 2011 Sinclair Knight Merz
Data SIO, NOAA, U.S. Navy, NGA, GEBCO
Image © 2011 DigitalGlobe
34°07'14.19" S 151°07'12.10" E elev 47 m
EPORT —
earth
Terms of Use
Eye alt 66.10 km


1101 OFFRD 0800/15 YSSY/NZAA .CC-CQE
/OUT 2226/OFF 2245/FOB 0742/ETA 0122
H1H1
SIA221
80
LAN800
VOZ819
Qantas Drive
Joyce Drive
Robey St
Sutherland St
Maloney St
Banks Ave
Botany Rd
Gardeners Rd
Airport Drive
Bayview Ave
Waidell Rd
William St
Slade Rd
Bardwell Rd
Hannam St
Loftus St
Forest Rd
Spring St
Marsh St
Kingsgrove Ave
Shaw St
Caroline St
Clarence Rd
Peadys Rd
Harrow Rd
Bestic St
Bryant St
Bay St
Francis Ave
The Grand Parade
Croydon Rd
Willison Rd
Railway Parade
Gray St
Civic Ave
Lily St
Noble St
Jubilee Ave
Barton St
General Holmes Dr
Page St
Wentworth Ave
Banksia St
Maroubra Rd
Fitzgerald Ave
Anzac Pde
Denison St
Beauchamp Rd
Perry St
Franklin St
Botany Rd
Barker St
Botany St
2803 m
imagery Date: 1/1/2009
2000
Google earth
Terms of Use


- #MD/AA MELCAYA.CR1.VH-OJP201D7CE8ECCD9B36A2D3
7c8026 RXA339
7c6b2f JST525
7c6d2c VOZ874
7c6b2d JST459
7c8032 RXA833
Q0
3L
Live, smooth web streaming in...
Data SIO, NOAA, U.S. Navy, NGA, GEBCO
© 2011 Whereis® Sensis Pty Ltd
Image © 2011 Sinclair Knight Merz
© 2011 Cnes/Spot Image
5.99 km
2009
34°12'18.93" S 151°14'02.97" E elev -129 m
Google earth
Terms of Use
Eye alt 10.61 km


Modez Mk I
EXIDE

Modez Mk IIpoint5

Modez Mk III


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


7c6c32 TGW343
35000 ft
803.38 km/h
Sqwk: 1041
7cf85c REGL1
38800 ft
851.12 km/h
Sqwk: 1425
7c6dd8 QFA922
18875 ft
740.69 km/h
Sqwk: 1432
7c7a3b VOZ321
38000 ft
835.71 km/h
Sqwk: 1355
76ccd0 SQC7290
36000 ft
936.74 km/h
Sqwk: 0151
7c80fb
7700 ft
516.56 km/h
Sqwk: 4002
Sqwk: 0106
497.62 km/h
Sqwk: 3740
7c6d31 VOZ411
23850 ft
910.08 km/h
Sqwk: 3726
89611b UAE418
27200 ft
933.50 km/h
Sqwk: 1545
7c6c92 JST747
31850 ft
852.10 km/h
Sqwk: 4265
©2011 Google - Map data ©2011 Tele Atlas, Imagery ©2011 TerraMetrics

Aviation State

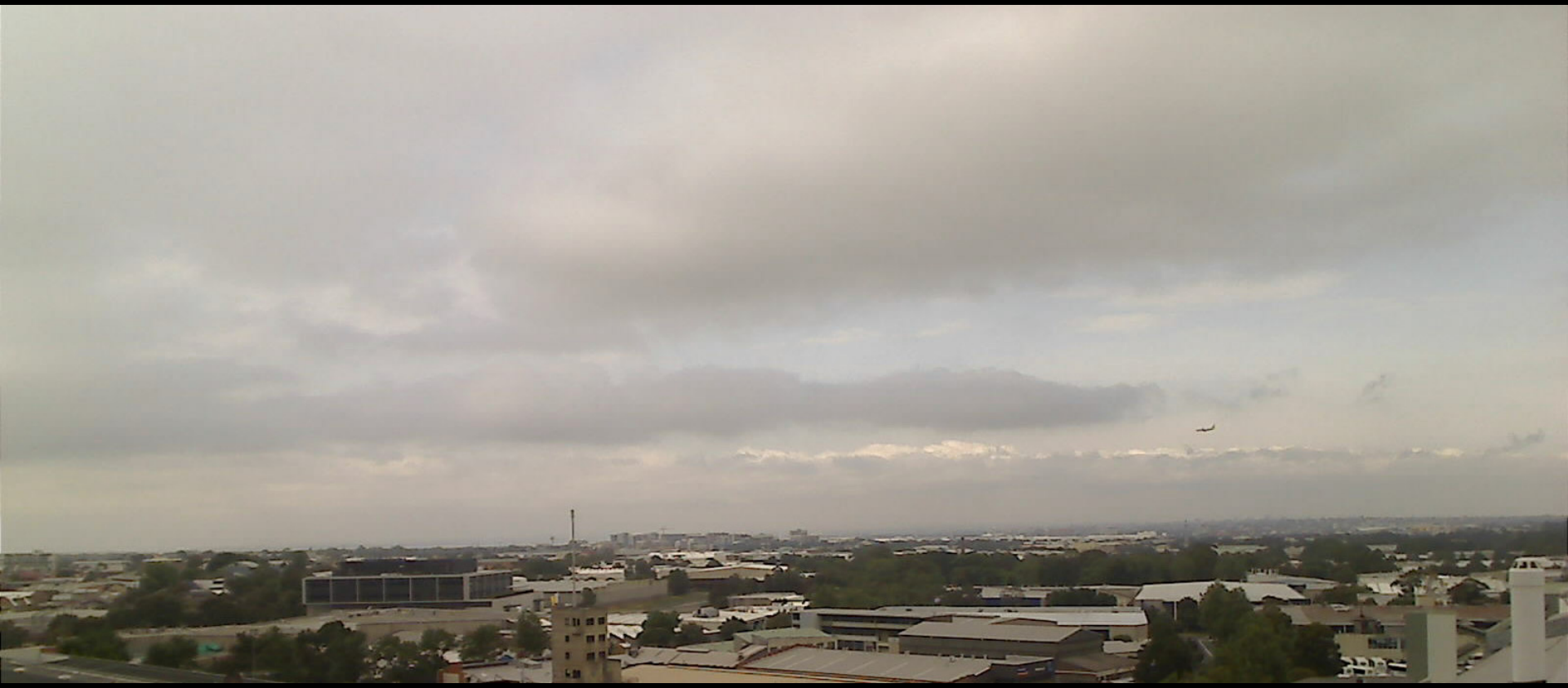
Position

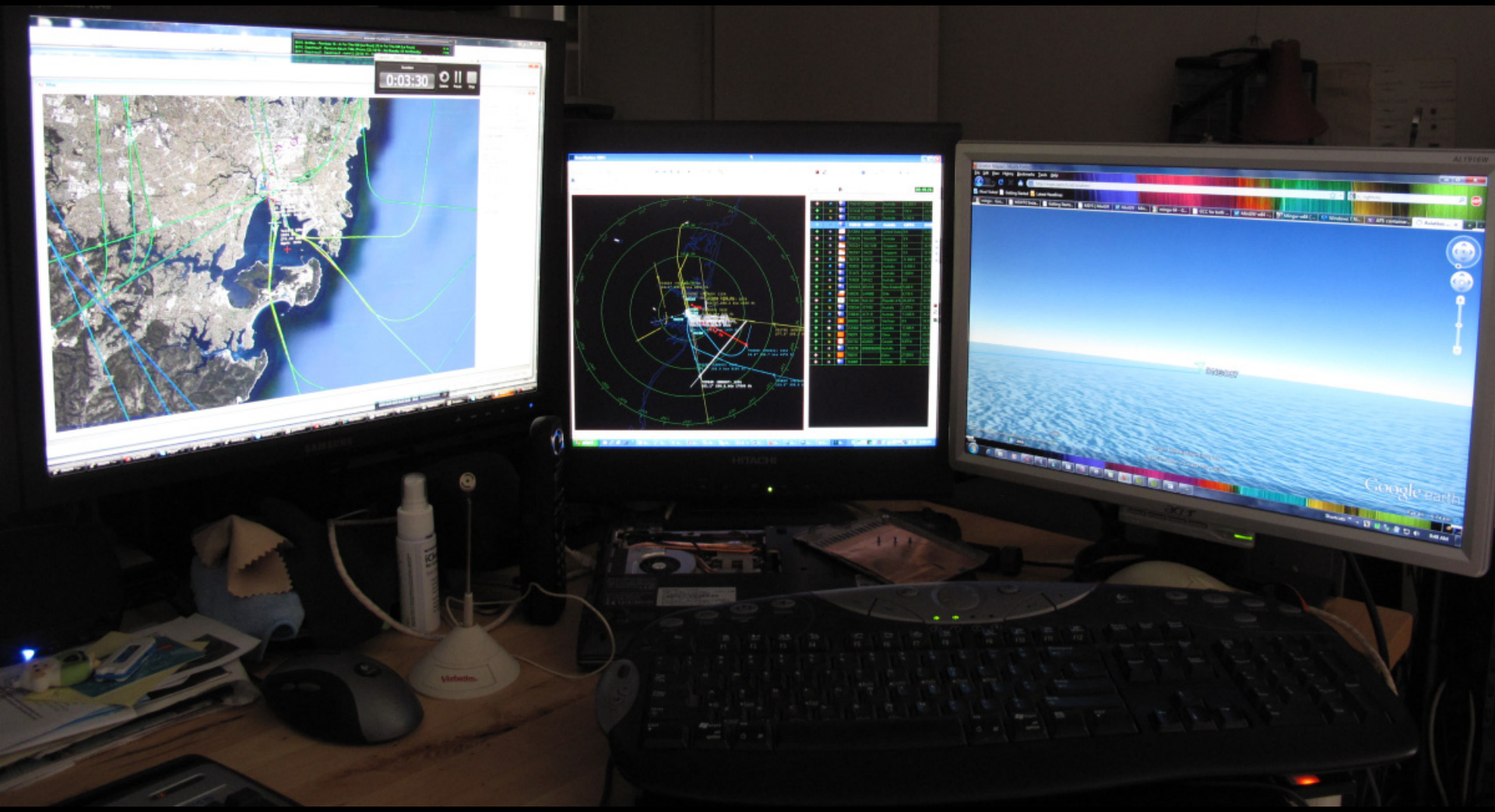
AA	Last Change	Vertical Status	Identity	Transponder	Altitude	Rate	Position	Speed	Heading	Distance
7c6289	16/11/2011 2:55:53 PM	Airborne			725					
7c6a7e	16/11/2011 1:29:35 PM	Airborne								
7c5310	16/11/2011 2:54:13 PM	Grounded		4253	-150					
7cf7cb	16/11/2011 2:49:52 PM	Grounded		7722						
780236	16/11/2011 2:56:58 PM	Grounded	CPA101	2000	-150	0	33°56'14.7095"S,151°10'08.5533"E	0.00 kts	253.1250°	4.81 km
7c80f5	16/11/2011 2:41:54 PM	Grounded			-125					4.60 km
7c52fa	16/11/2011 2:24:15 PM	Grounded			-125					
7c6d2b	16/11/2011 2:25:52 PM	Grounded		4361	-125					63.82 km
7cf8f3	16/11/2011 2:55:53 PM	Airborne	PLUTO07	2501	31000					
8a02b7	16/11/2011 1:37:10 PM	Airborne		1354		2432		362.40 kts	288.3350°	87.73 km
76cd64	16/11/2011 2:43:08 PM	Grounded	SIA231	2221	-125	0		0.00 kts	295.3125°	5.15 km
7c6d80	16/11/2011 2:40:56 PM	Airborne		7212	24375					
7cf7be	16/11/2011 2:50:46 PM	Unknown			29000					
7c6d96	16/11/2011 2:56:28 PM	Grounded				0		0.00 kts	98.4375°	
7c81d2	16/11/2011 2:52:15 PM	Airborne		3646	30075					
7c7a38	16/11/2011 1:36:33 PM	Grounded		3760	-175	0	33°56'18.9551"S,151°10'57.7963"E	13.50 kts	348.7500°	4.26 km
7c6d37	16/11/2011 2:43:32 PM	Airborne			13125					54.98 km
7c6d2c	16/11/2011 2:53:49 PM	Airborne	VOZ1421	1372	27800	1280	33°29'19.1607"S,150°44'38.2874"E	416.43 kts	345.9638°	62.59 km
7c6c5b	16/11/2011 2:45:53 PM	Airborne			22925					50.02 km
7c6c9e	16/11/2011 2:55:18 PM	Airborne			32500	1984		426.43 kts	233.7751°	70.44 km
3a1e43	16/11/2011 2:56:00 PM	Airborne	ACI141S	1462	125	2176	33°57'12.3486"S,151°10'40.1397"E	152.78 kts	169.0578°	5.95 km

AA	Last Change	Vertical Status	Identity	Transponder	Altitude	Rate
a74647	28/05/2011 8:27:51 AM	Airborne				
a9b40d	28/05/2011 8:27:37 AM	Airborne		1717	11875	
a78dd7	28/05/2011 8:27:15 AM	Airborne				
a59b5e	28/05/2011 8:28:23 AM	Airborne			15100	
acdde3	28/05/2011 8:28:21 AM	Airborne			6825	
a733b4	28/05/2011 8:27:55 AM	Airborne			1800	
a2e28f	28/05/2011 8:28:18 AM	Airborne			32000	
a096cd	28/05/2011 8:28:22 AM	Airborne		3725	11600	
a83951	28/05/2011 8:28:22 AM	Airborne			2125	
ab4151	28/05/2011 8:28:19 AM	Airborne			3875	
a1b1bc	28/05/2011 8:27:58 AM	Airborne			19575	
ac7f4e	28/05/2011 8:28:13 AM	Airborne			65800	
ab4c15	28/05/2011 8:28:22 AM	Airborne	2246		13825	3712
aae233	28/05/2011 8:28:22 AM	Airborne			10300	
a22426	28/05/2011 8:28:21 AM	Airborne	SCOTSUXX		9775	-128
acae9a	28/05/2011 8:28:06 AM	Airborne			9800	
ab473a	28/05/2011 8:28:15 AM	Airborne			6775	
ad0119	28/05/2011 8:28:18 AM	Airborne			18225	
a72b6b	28/05/2011 8:28:22 AM	Airborne			18825	
100000	28/05/2011 8:27:37 AM	Airborne				
a699a6	28/05/2011 8:27:32 AM	Airborne				
a1a2e0	28/05/2011 8:27:59 AM	Airborne			3800	
a3ca18	28/05/2011 8:28:20 AM	Airborne			17050	
a6dd66	28/05/2011 8:28:23 AM	Airborne			2000	
3c7202	28/05/2011 8:27:59 AM	Airborne	BER7393		6525	2432

Next Level Modez

intel
Centrino
nVIDIA



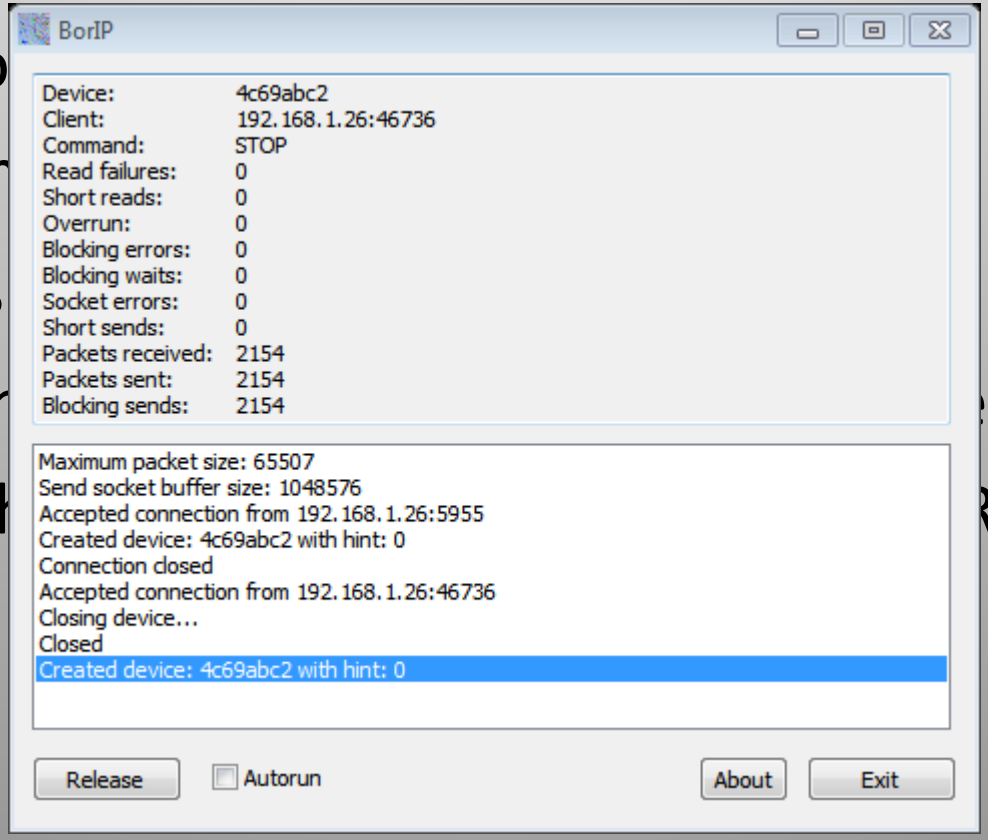

0:03:30
Google earth

BorIP

- Allows USRP 1 and computer to be separated by LAN
  - Control radio via TCP
  - Stream baseband via UDP
- Seamless drop-in for GR
  - If it can't find a local device, try remote
  - Everything just works (USRP Source, GR, etc)

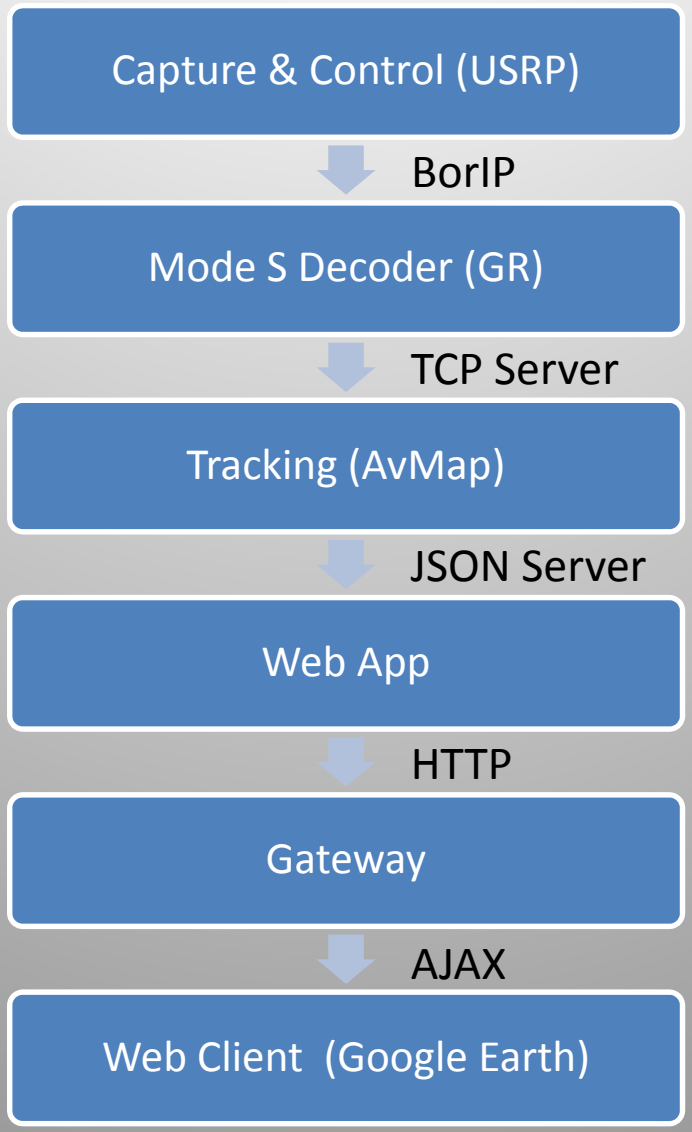
BorIP

- Allows USRP 1 and computer to be separated by LAN
  - Contro
  - Stream
- Seamles
  - If it car
  - Everyth



, etc)

Antenna to Google Earth

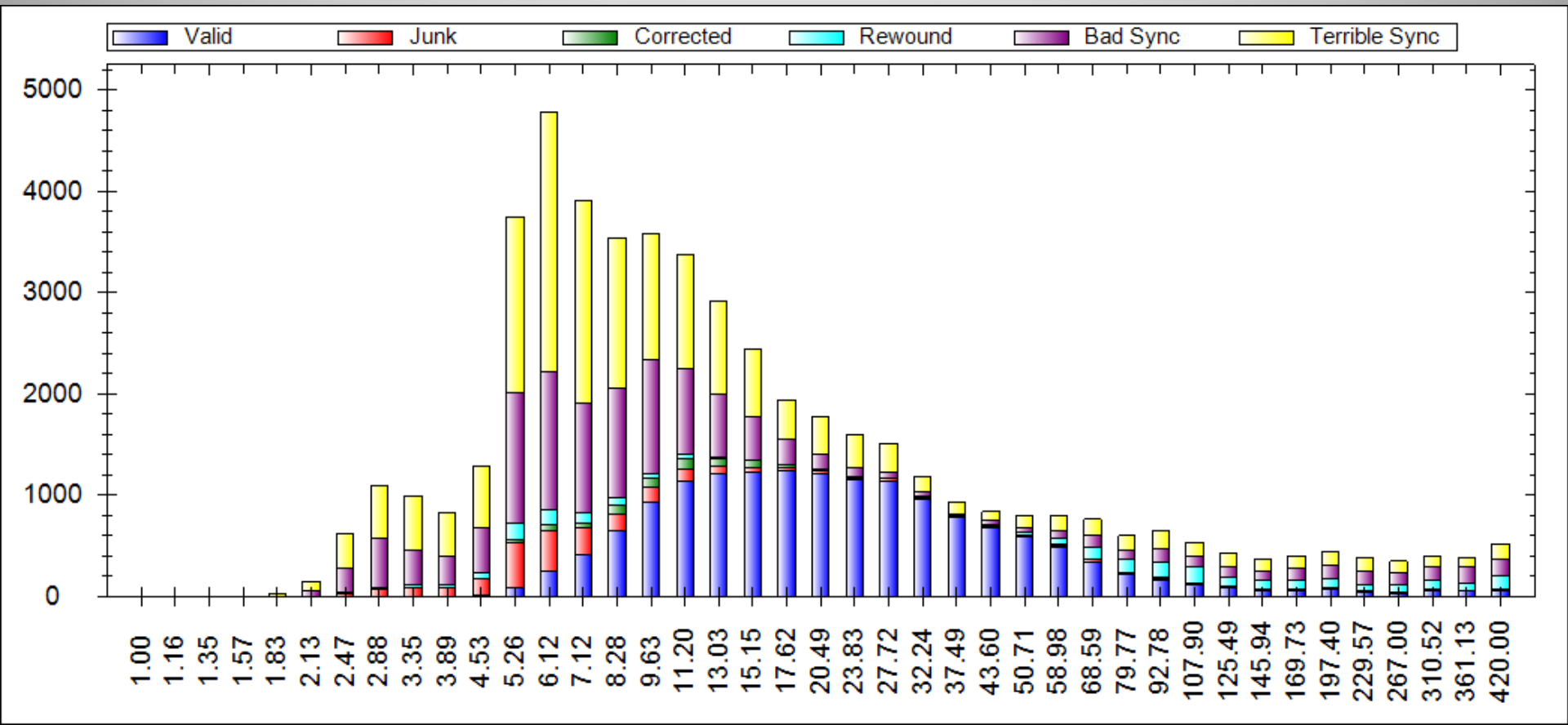


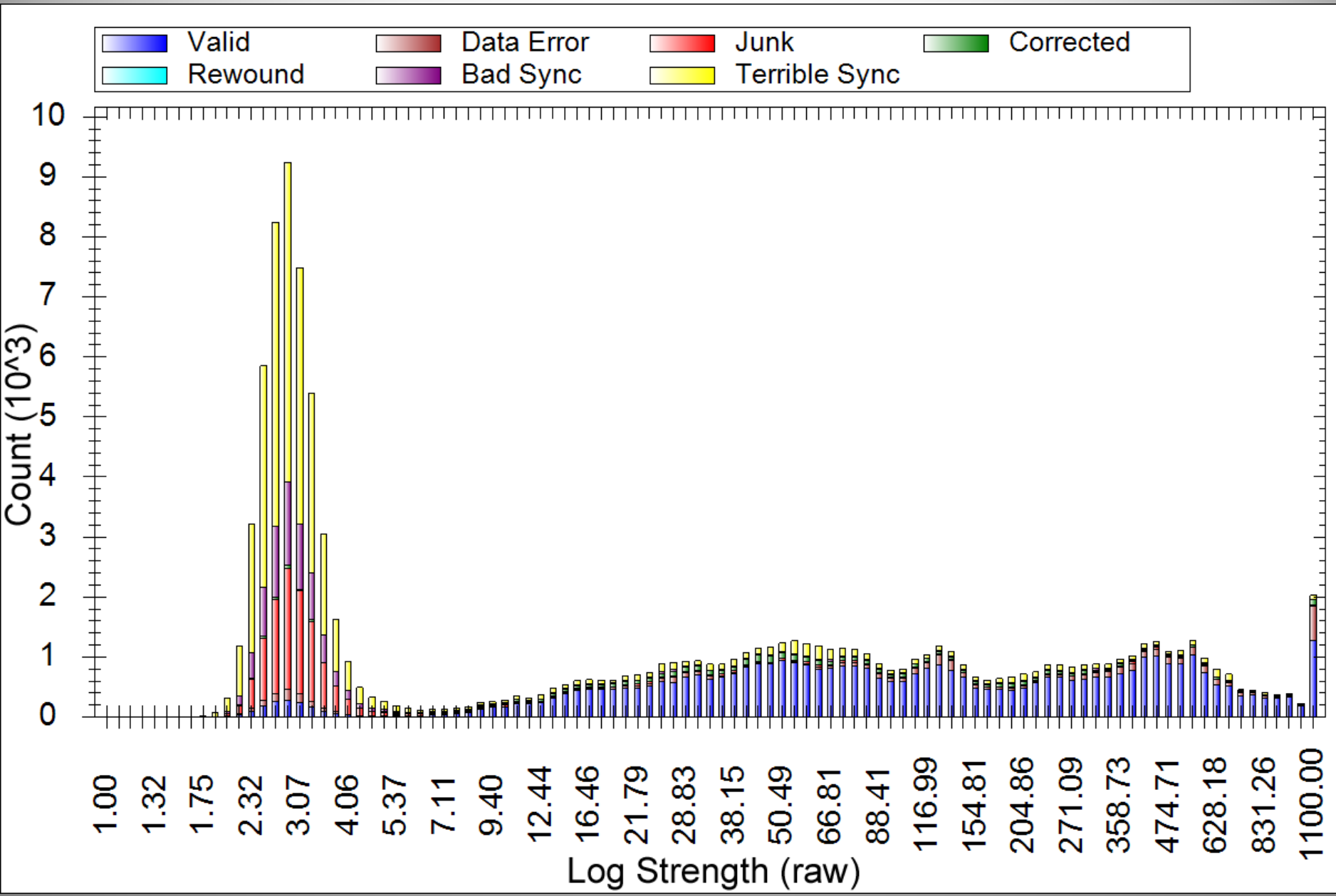
Modez Evolution

- Goal is to increase SNR
  - Increase gain: tuned antenna
  - Drop noise floor: front-end filter (GSM is nearby) & optimal sample rate to avoid artifacts (spurs)

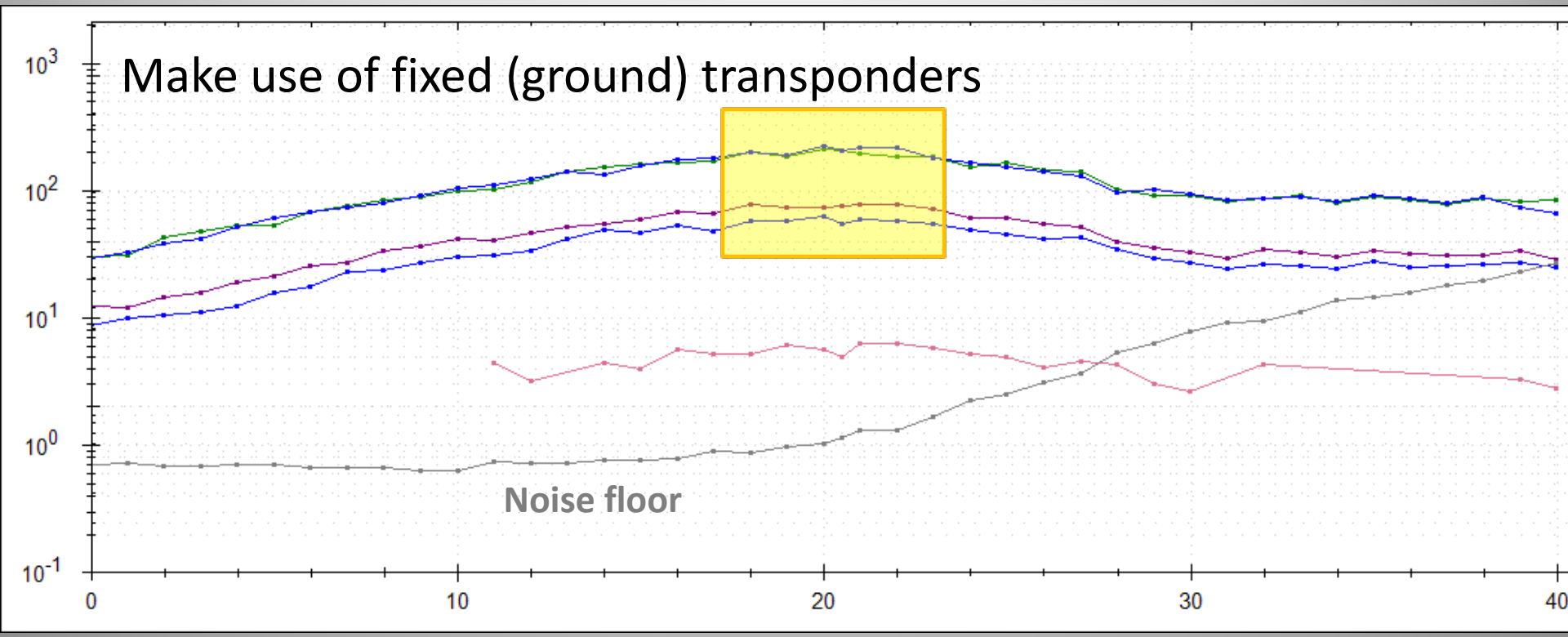
Signal Strength Distribution

- Evaluate how well decoder is doing



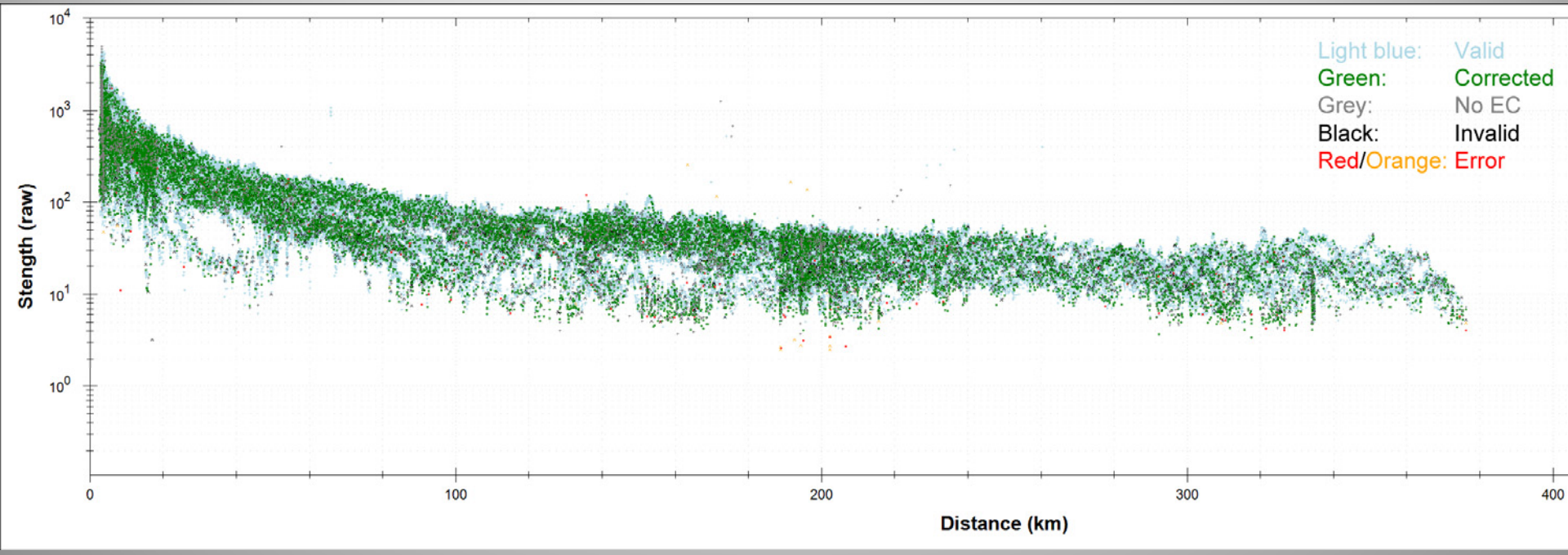

Valid
Data Error
Junk
Corrected
Rewound
Bad Sync
Terrible Sync
Count (10^3)
0
1
2
3
4
5
6
7
8
9
10
1.00
1.32
1.75
2.32
3.07
4.06
5.37
7.11
9.40
12.44
16.46
21.79
28.83
38.15
50.49
66.81
88.41
116.99
154.81
204.86
271.09
358.73
474.71
628.18
831.26
1100.00
Log Strength (raw)

SNR vs. Gain

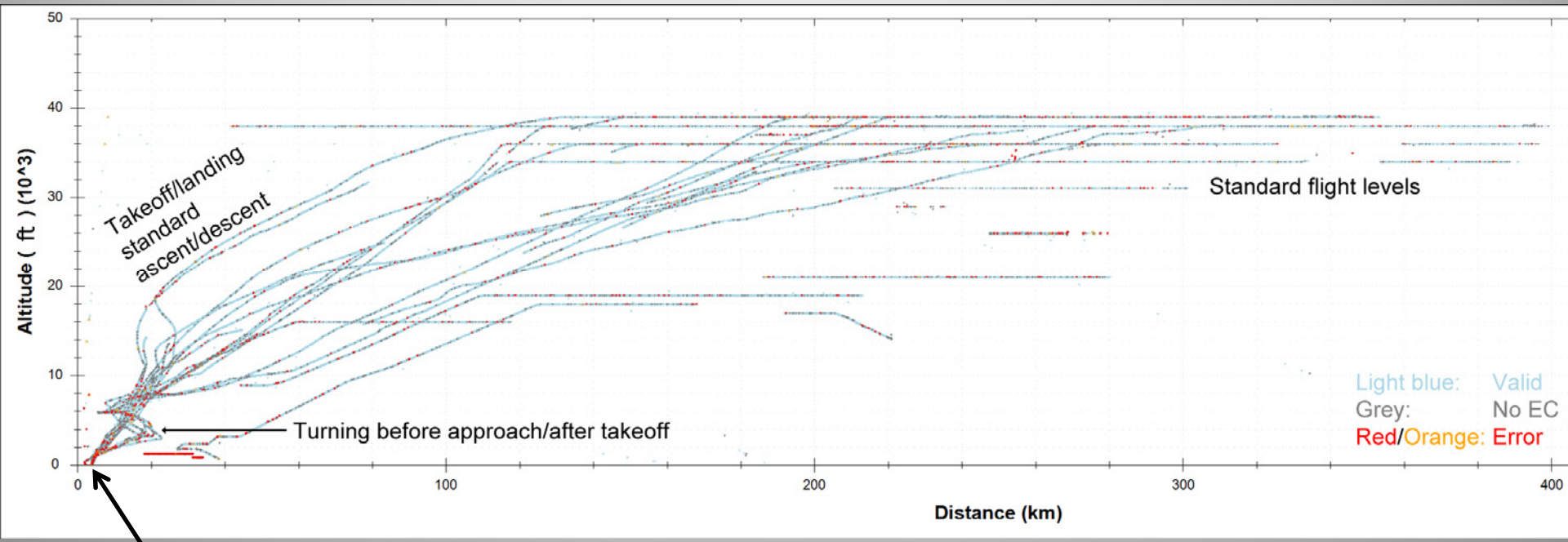


Change USRP/WBX gain

Strength vs. Distance

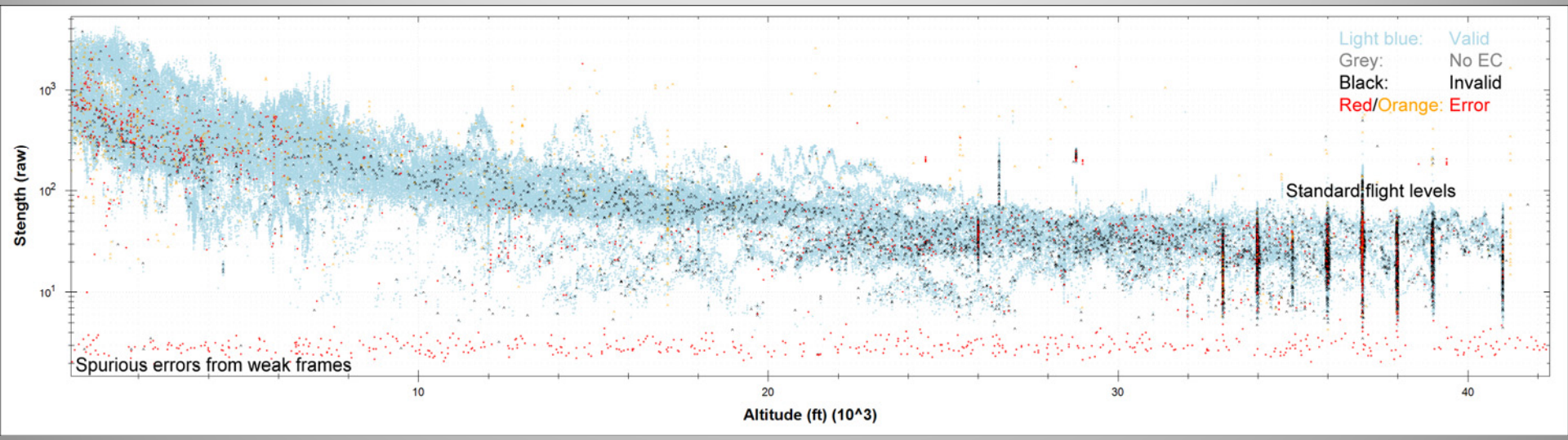


Altitude vs. Distance



Helps to live close to the airport

Strength vs. Altitude




- #MD/AA MELCAYA.CR1.VH-OJP201D7CE8ECCD9B36A2D3
7c8026 RXA339
7c6b2f JST525
7c6d2c VOZ874
7c6b2d JST459
7c8032 RXA833
7c810d SXA427LH
Q0
3L
2L
QF
13
H1
5.99 km
Data SIO, NOAA, U.S. Navy, NGA, GEBCO
© 2011 Whereis® Sensis Pty Ltd
Image © 2011 Sinclair Knight Merz
© 2011 Cnes/Spot Image
2009
34°12'18.93" S 151°14'02.97" E elev -129 m
Google earth
Terms of Use
Eye alt 10.61 km

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
```

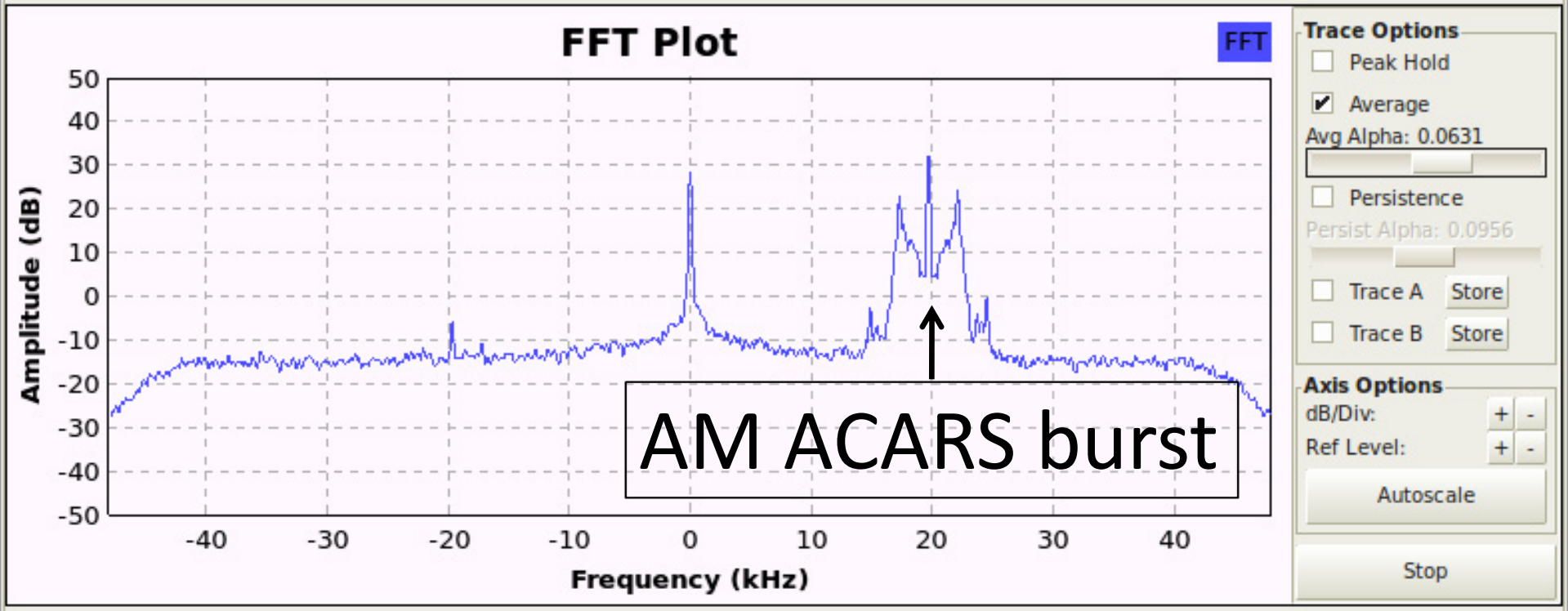
Acars Gui

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

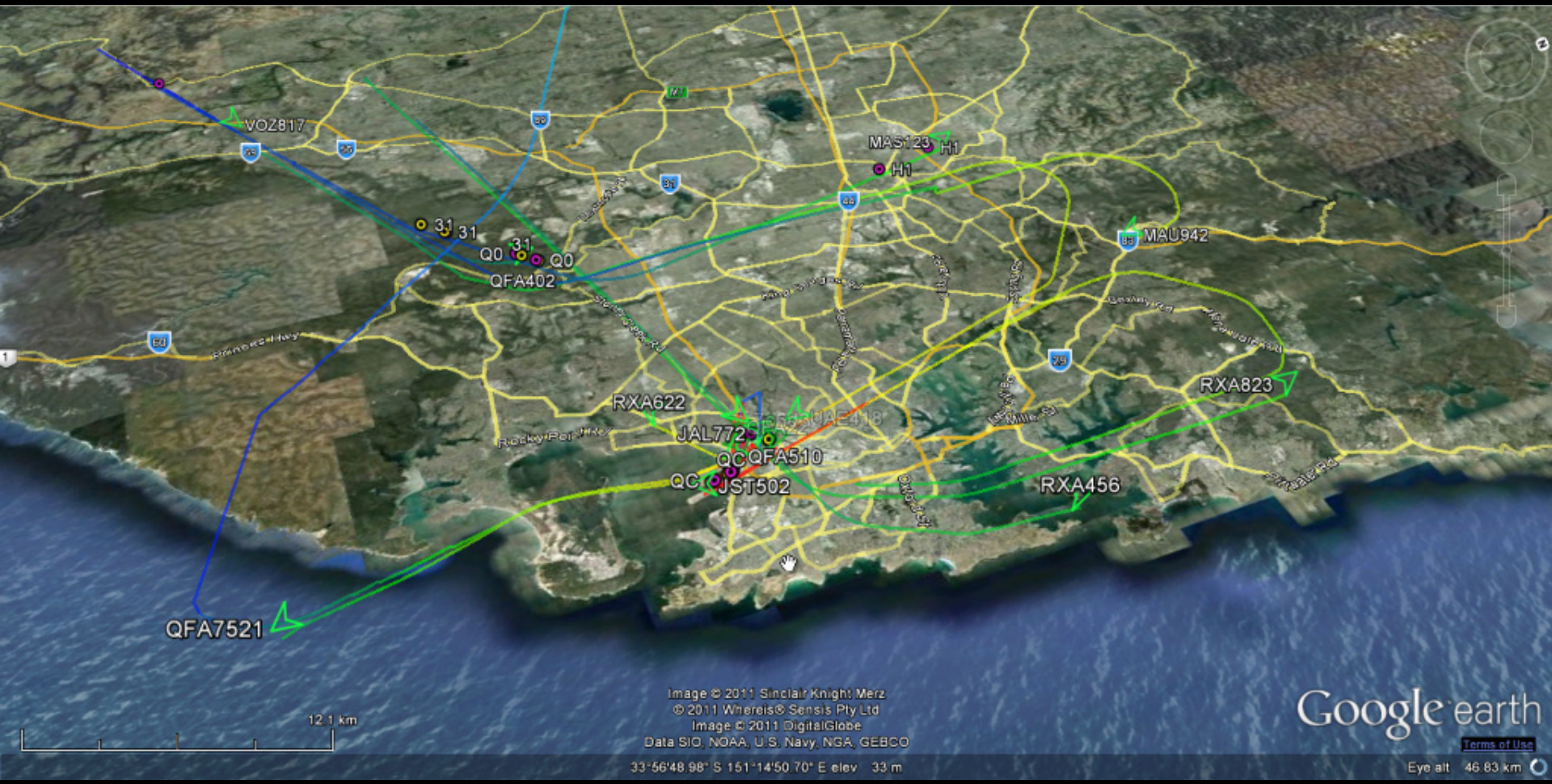
dB/Div: + -

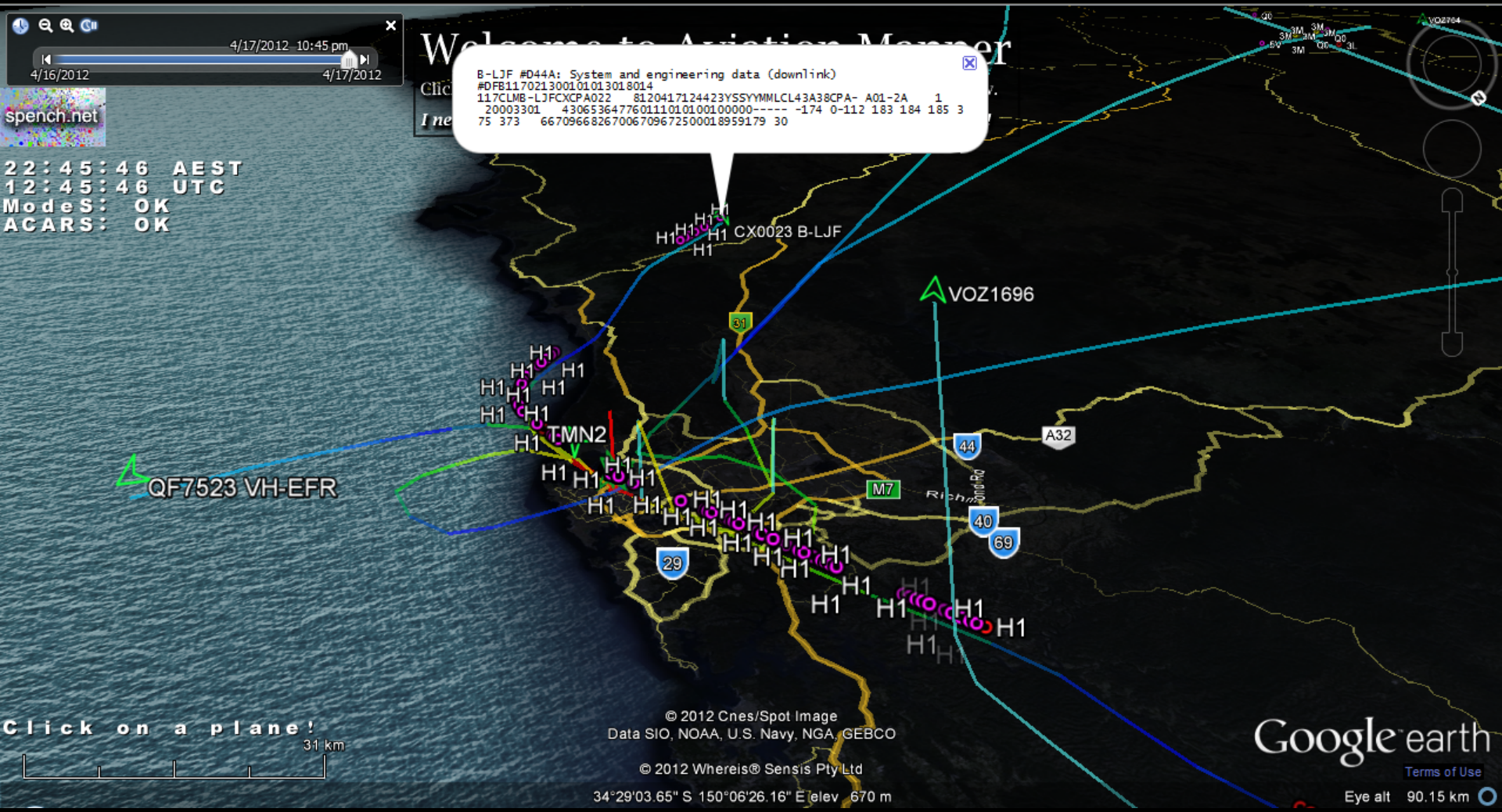
Ref Level: + -

Autoscale

Stop

am_bw: 5k


VOZ817
MAS123
H1
H1
31
31
31
Q0
Q0
QFA402
MAU942
RXA622
RXA823
JAL772
QC
QFA510
QC
JST502
RXA456
QFA7521
Image © 2011 Sinclair Knight Merz
© 2011 Whereis® Sensis Pty Ltd
Image © 2011 DigitalGlobe
Data SIO, NOAA, U.S. Navy, NGA, GEBCO
33°56'48.98" S 151°14'50.70" E elev 33 m
12.1 km
Google earth
Terms of Use
Eye alt 46.83 km


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

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;
```

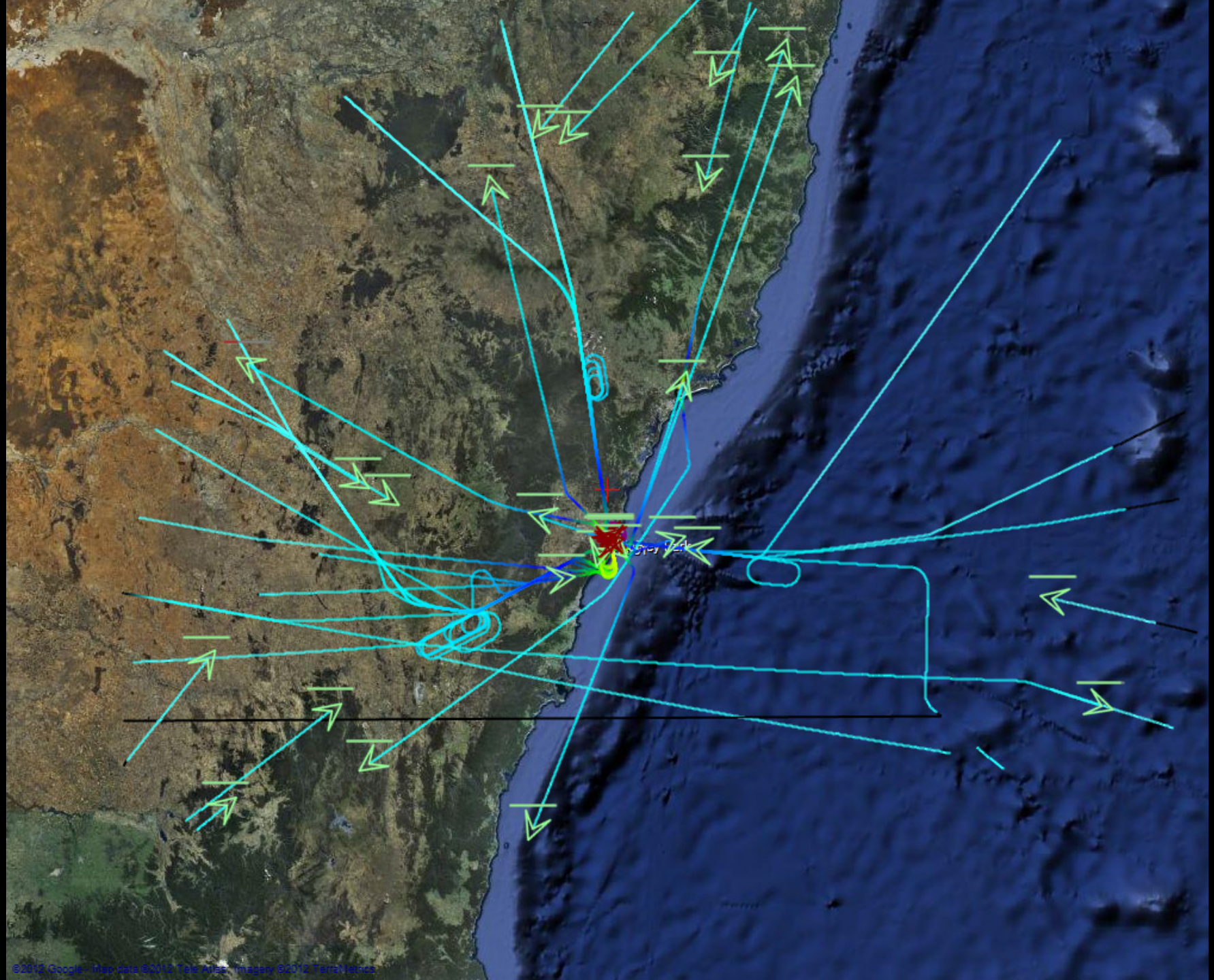
Examples

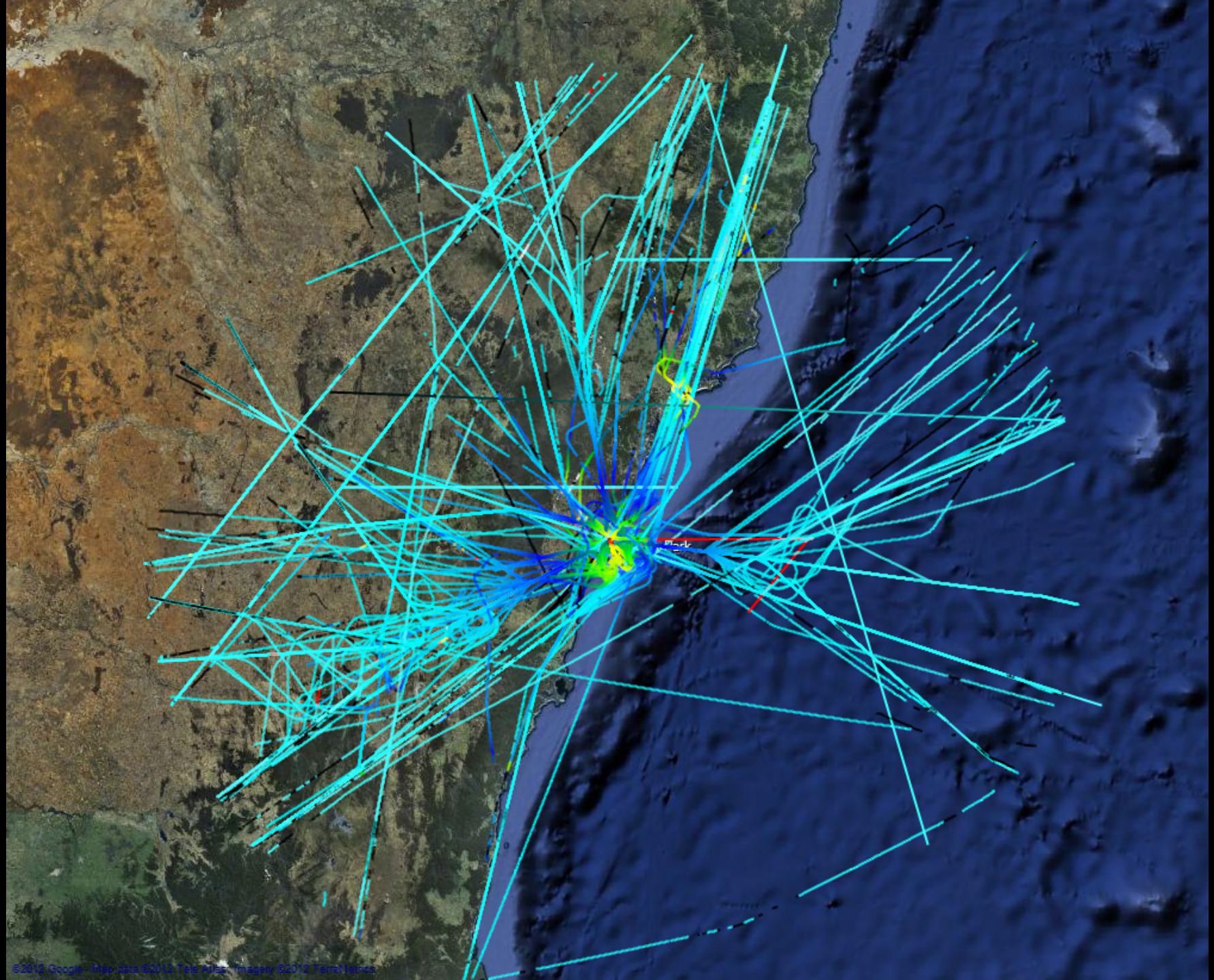
```
Time:       2011-11-16 09:49:06.844000
Station:    Home
Frequency:  131.45 MHz
Mode:       2 (either)
Address:    VN-A375
Ack:        NAK
Label:      H1: System and engineering data (downlink)
Block:      5
Message #:  C12B
Flight ID:  VN0773
#CFB383141VSC    1,,,,,,,LAV 61,HARD,202806;344137WXR2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

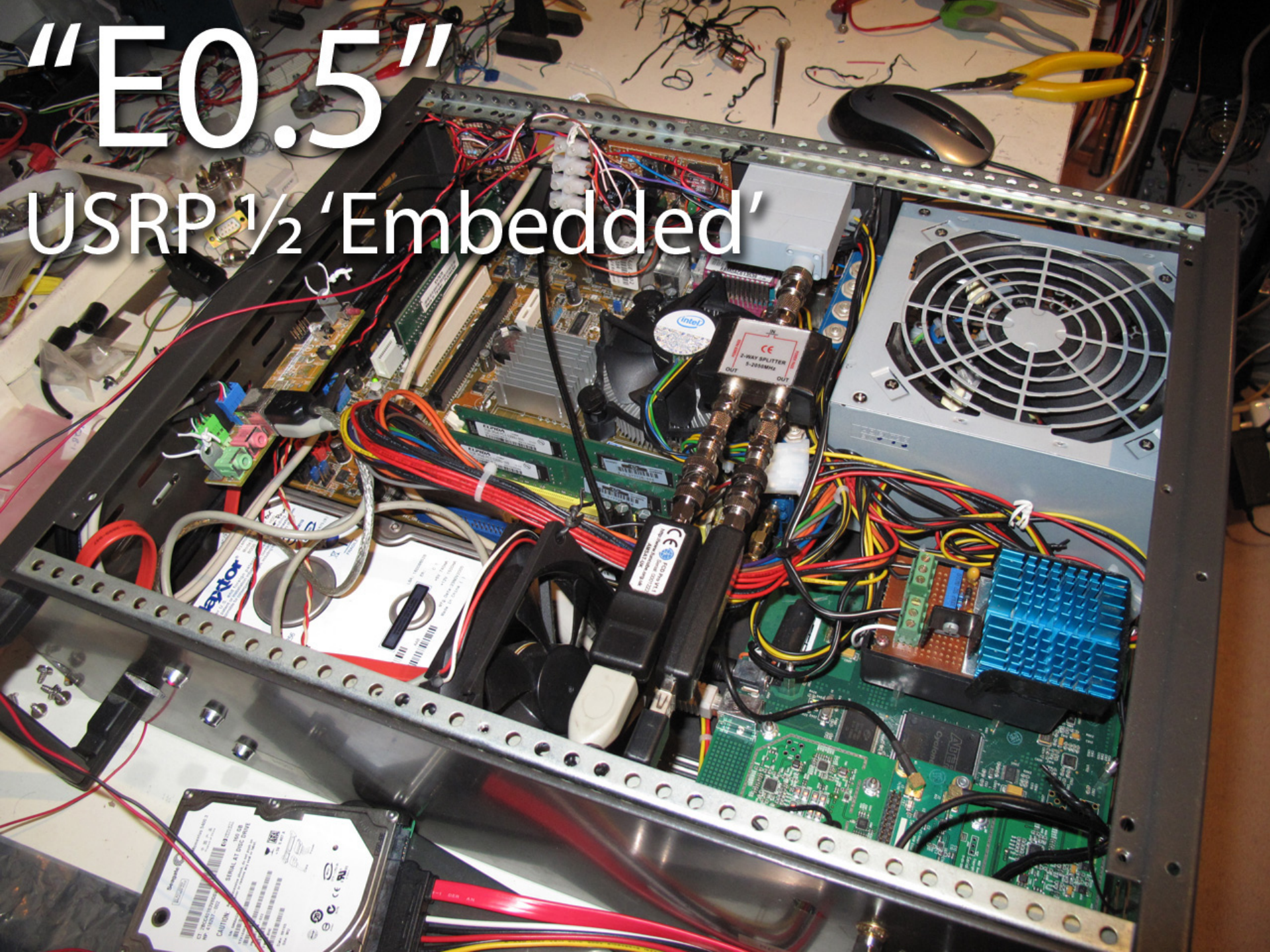

Welcome to Aviation Mapper
Click here for info, feedback and to share – if you like this, let me know.
I need to find a new receiver site near the airport ASAP - please help!
4/13/2012
2012
2012
spench.net
Mitchell Hwy
Barrier Hwy
ModeS: OK
ACARS: OK
BANDA
CORKY
BULGA
LV-ZRA #C71C: System and engineering 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

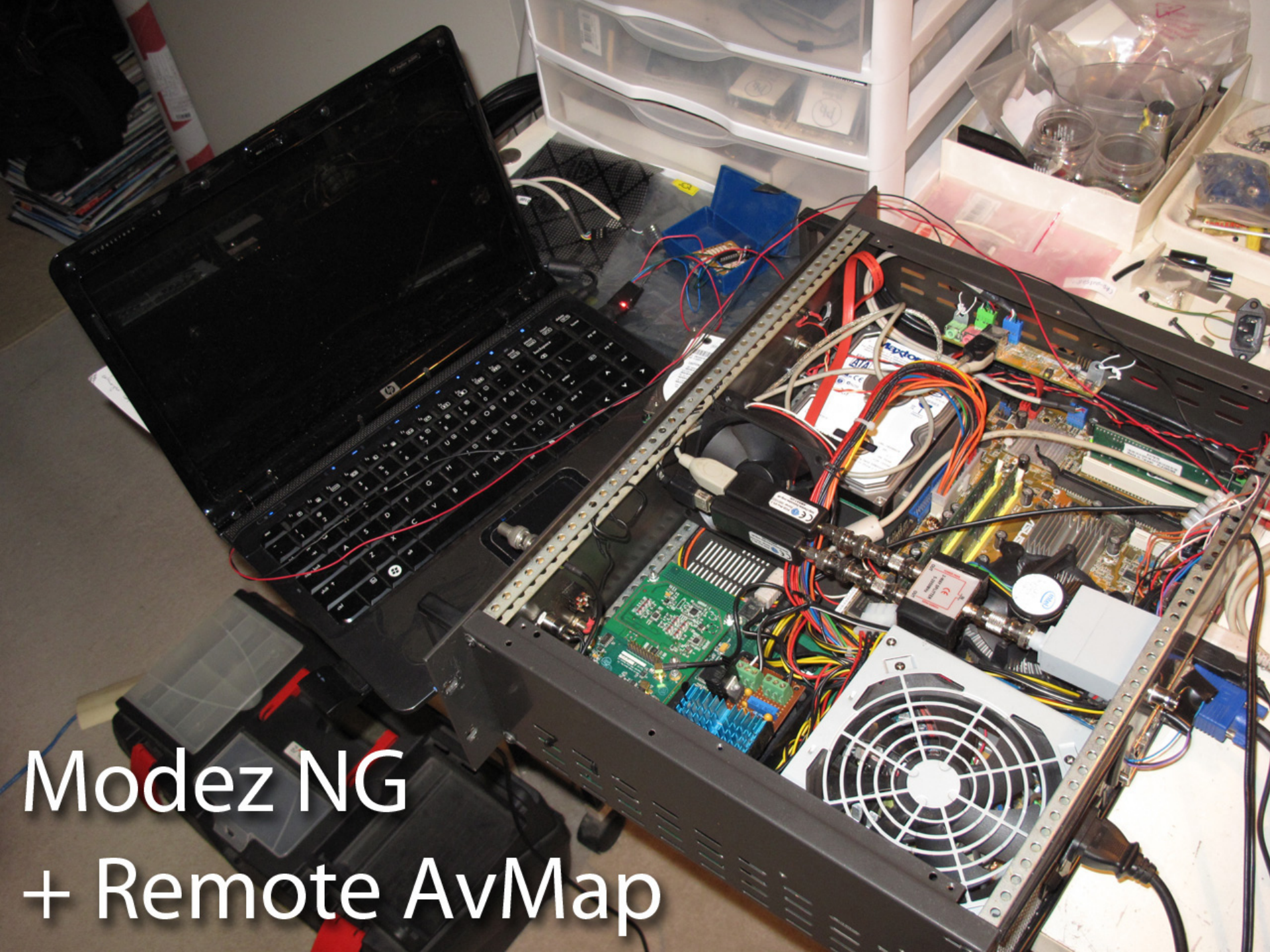

4/15/2012 9:45 pm
4/14/2012
4/15/2012
spench.net
21:02:32 AEST
11:02:32 UTC
ModeS: Terminated
ACARS: OK
Welcome to Aviation Mapper
Click here for info, feedback and to share - if you like this, let me know.
I need to find a new receiver site near the airport ASAP - please help!
http://maps.spench.net/aviation/
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


4/27/2012 5:06 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
15:46:23 AEST
05:46:23 UTC
ModeS: OK
ACARS: OK
Auto Balloons
Trails
Trails need more CPU
QF0012 VH-OJM
Click on a plane!
164 ft
© 2012 Whereis® Sensis Pty Ltd
Image © 2012 Sinclair Knight Merz
Google earth
Terms of Use
Imagery Date: 1/1/2009
2000
33°56'03.95" S 151°10'05.37" E elev 25 ft
Eye alt 760 ft


©2012 Google - Map data ©2012 Tele Atlas - Imagery ©2012 TerraMetrics


©2012 Google - Map data ©2012 Tele Atlas - Imagery ©2012 TerraMetrics


"E0.5"
USRP ½ 'Embedded'


Modez NG
+ Remote AvMap

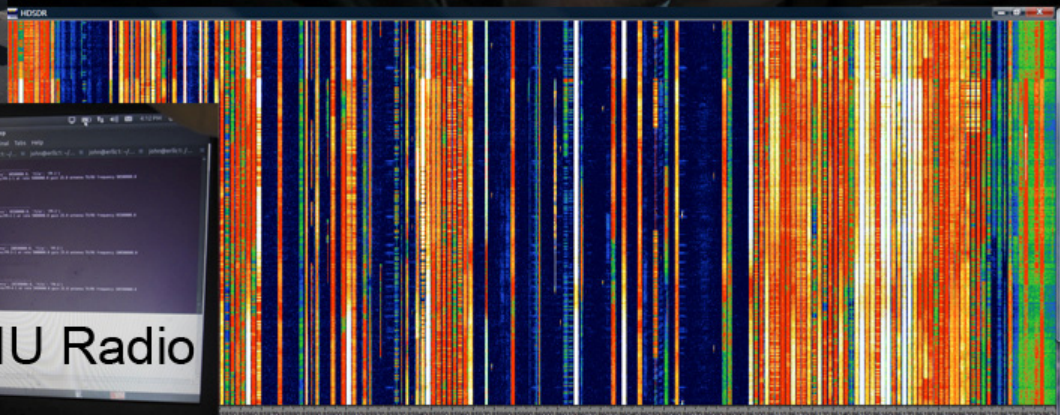

Modez NG
AvMap's view:

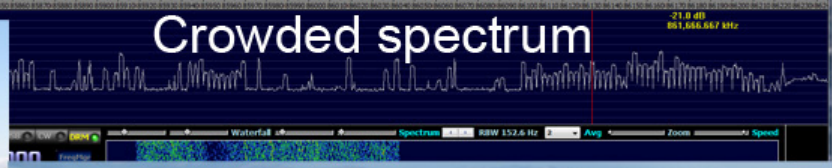

a835d1 VRD1757
30600 ft
795.21 km/h
a47557 AAL73
34000 ft
779.22 km/h
Sqwk: 5676
NoiseBridge
Sqwk: 3641
Ettus
ab856c VRD958
31575 ft
848.60 km/h
©2012 Microsoft Corporation, ©2012 NAVTEQ, ©2012 Image courtesy of NASA


89611c UAE226
675 ft
366.10 km/h
Sqwk: 3645
aaa244
-25 ft
25.00 km/h
a16c50 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

Taking SDR to the skies: Capturing the Bay Area's radio spectrum from the air

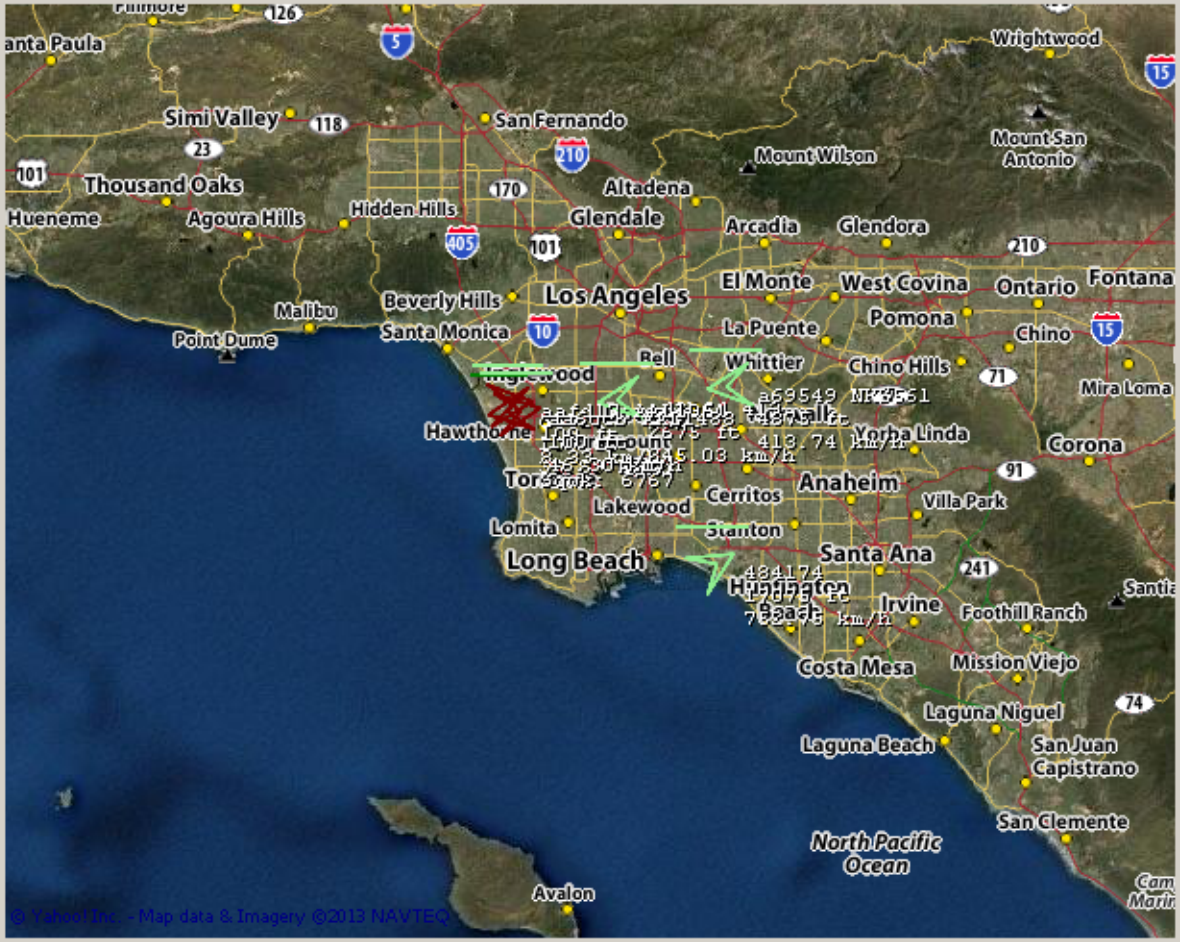
(All your RFz are belong to us)





Last Change	Vertical Sta...	Identity	Transponder	Altitude	Rate	Position	Speed	Heading	Distance
6/04/2013 2:21:45 PM	Airborne	CPA882	3322	700	-704	33°57'19.9292"N,118°22'05.1619"W	131.97 kts	263.0365°	509.42 km
6/04/2013 2:23:10 PM	Airborne								
6/04/2013 2:24:09 PM	Airborne		1320	1225					
6/04/2013 2:17:18 PM	Airborne								
6/04/2013 2:24:03 PM	Airborne		4626						
6/04/2013 2:21:16 PM	Airborne			7950					
PM	Airborne		6704	2875					
PM	Airborne			22450					
PM	Airborne			32000					515.86 km
PM	Unknown	TEST1234							
PM	Airborne			12075	2048	33°45'26.5320"N,118°06'35.9204"W	406.45 kts	58.8912°	541.63 km

Map



Centre
Cull
IFR
User
VFR
Continuous
Airframe Info
Messages

Yahoo Hybrid

View information:

Map zoom: 9
Map centre:
33.8658544540718
-118.289794921875

Mouse:
33.3603556667537
-119.056091308594

Click:
33.6717827836443
-118.361206054688

Save Image...

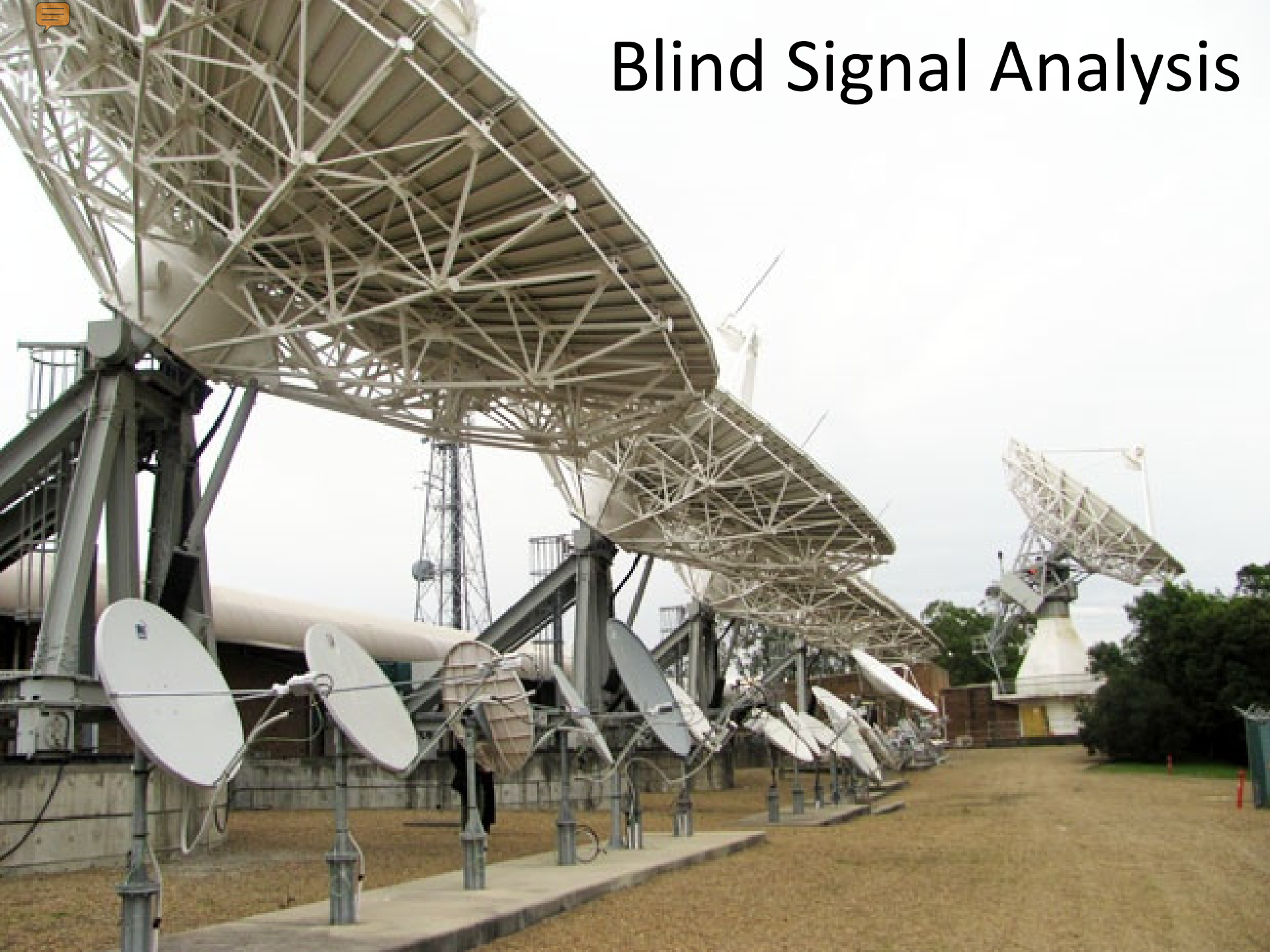
Decoder | 130/251 | Aviation State | 24/48 | Load | 89.8% | Request Cache | #0 0.0/s (Hit 0.0%) | Time | 2:24:09 PM


HFDL
PC-HFDL
X
X
UP0009
CES514
CES233
China
CCA150
CCA410
CCA451
3U8548
CSC865
CCA450
3U8931
5655
CSN309
Taipei
Nepal
IGO257
Kathmandu
Bhutan
3U8869
Taiwan
CI0931
Hong Kong
Macau
IGO212
Bangladesh
IGO245
IGO348
UP0021
IGO318
IGO041
India
Hà Nội
Myanmar (Burma)
SLK972
Laos
Naypyidaw
Philippines
Manila
Vientiane
IGO266
IGO377
6E0275
Paracel Islands
OMA811
6E0339
Thailand
IGO276
Vietnam
IGO436
VJC838
Bangkok
Cambodia
Phnom Penh
US Dept of State Geographer
© 2012 Google
© 2012 Tele Atlas
© 2012 Mapabc.com
lat 26.040498° lon 98.494735° elev 3003 m
Google
Eye alt 4407.20 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

Blind Signal Analysis



Recap

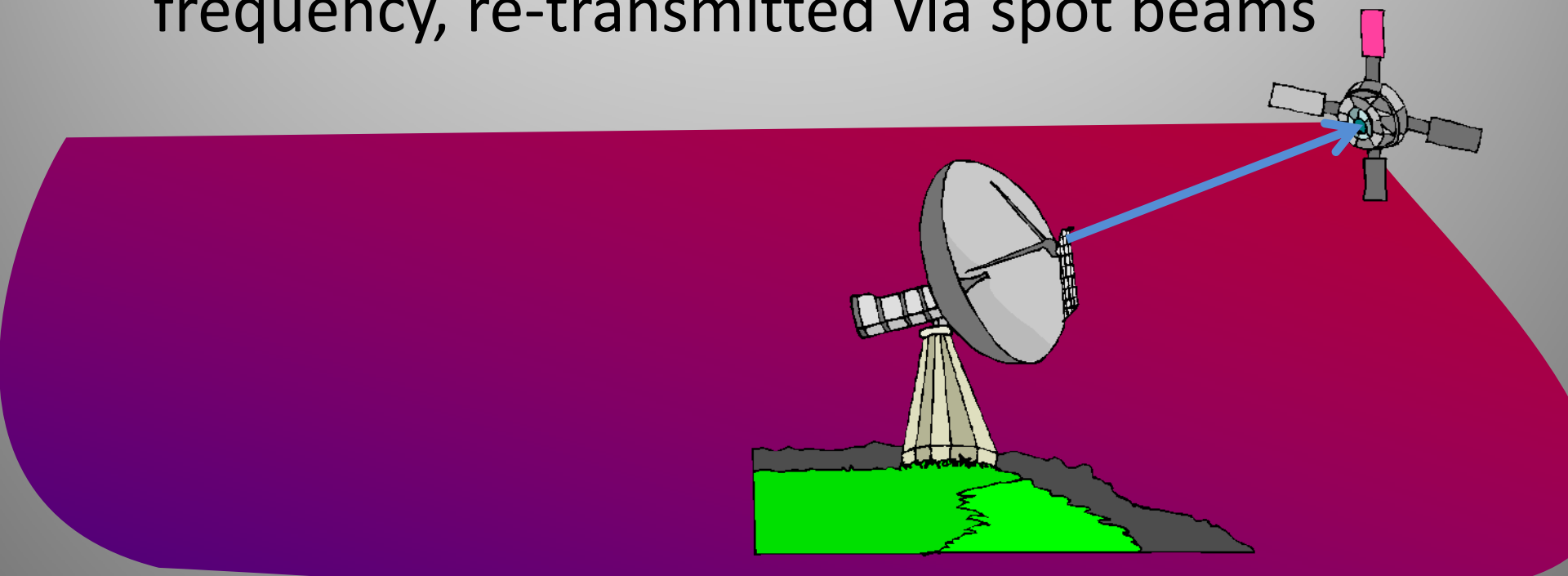
- Lots of different types of satellites
- Variables:
  - Purpose: comms, weather, MIL, amateur
  - Payload: transponders, cameras/sensors
  - Orbit: **L**ow **E**arth **O**rbit, geostationary (geosync)
  - Frequencies: uplink, downlink, beacon, command
- Two categories:
  - **Intelligent**: communication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

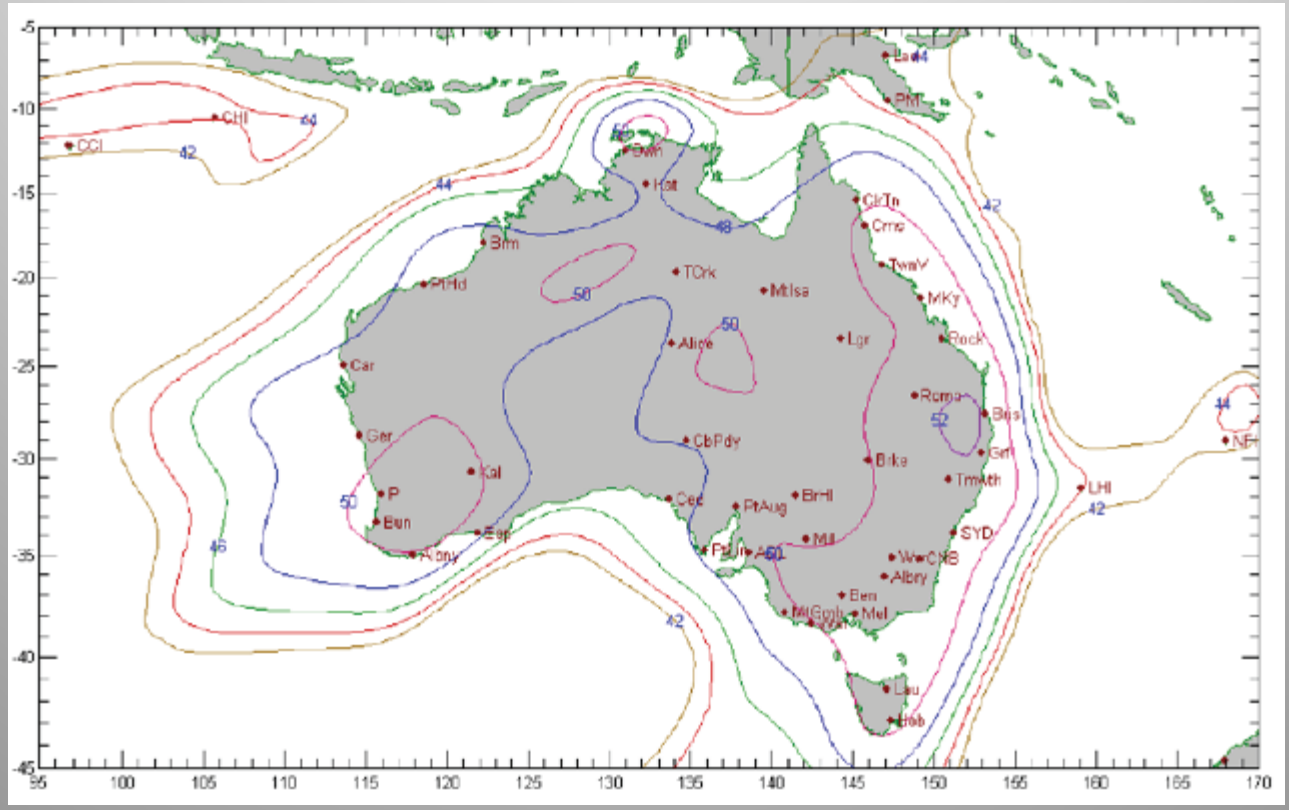
TT&C and UPC

- **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

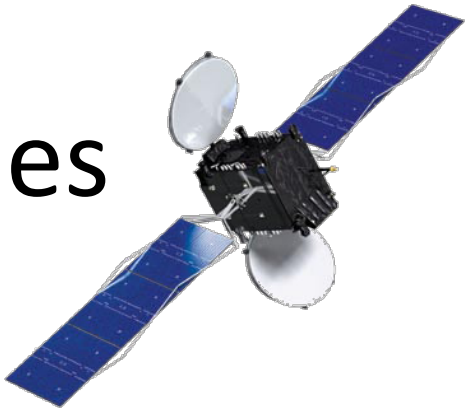
- 24 Ku band transponders
  - Multiplexed spot beams service Aus and NZ
  - Uplink: 14.0 - 14.5 GHz
  - Downlink: 12.25 - 12.75 GHz
  - Bandwidth: 54 MHz
- Mainly TV (wideband DVB-S)
  - ABC, SBS, Se7en, Nin9, SkyNZ
- Some other (narrowband) things…

FNA Beam Coverage

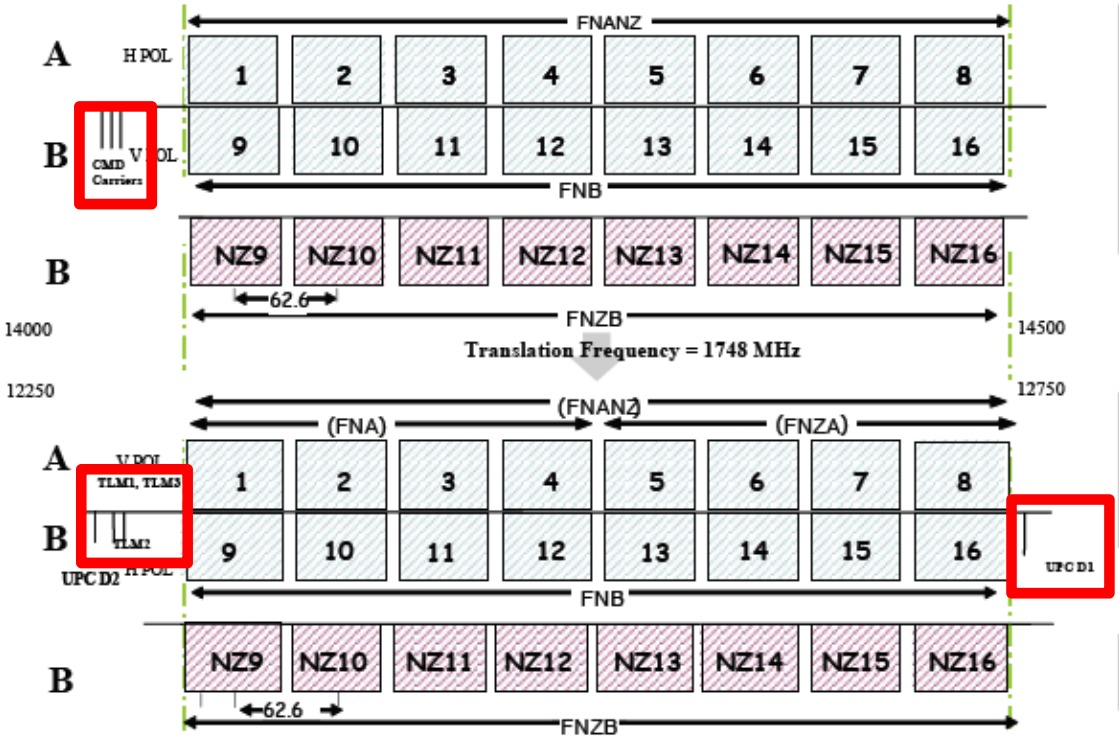


Effective **I**sotropic **R**adiated **P**ower (EIRP)

D1 Channel Frequencies



Uplink



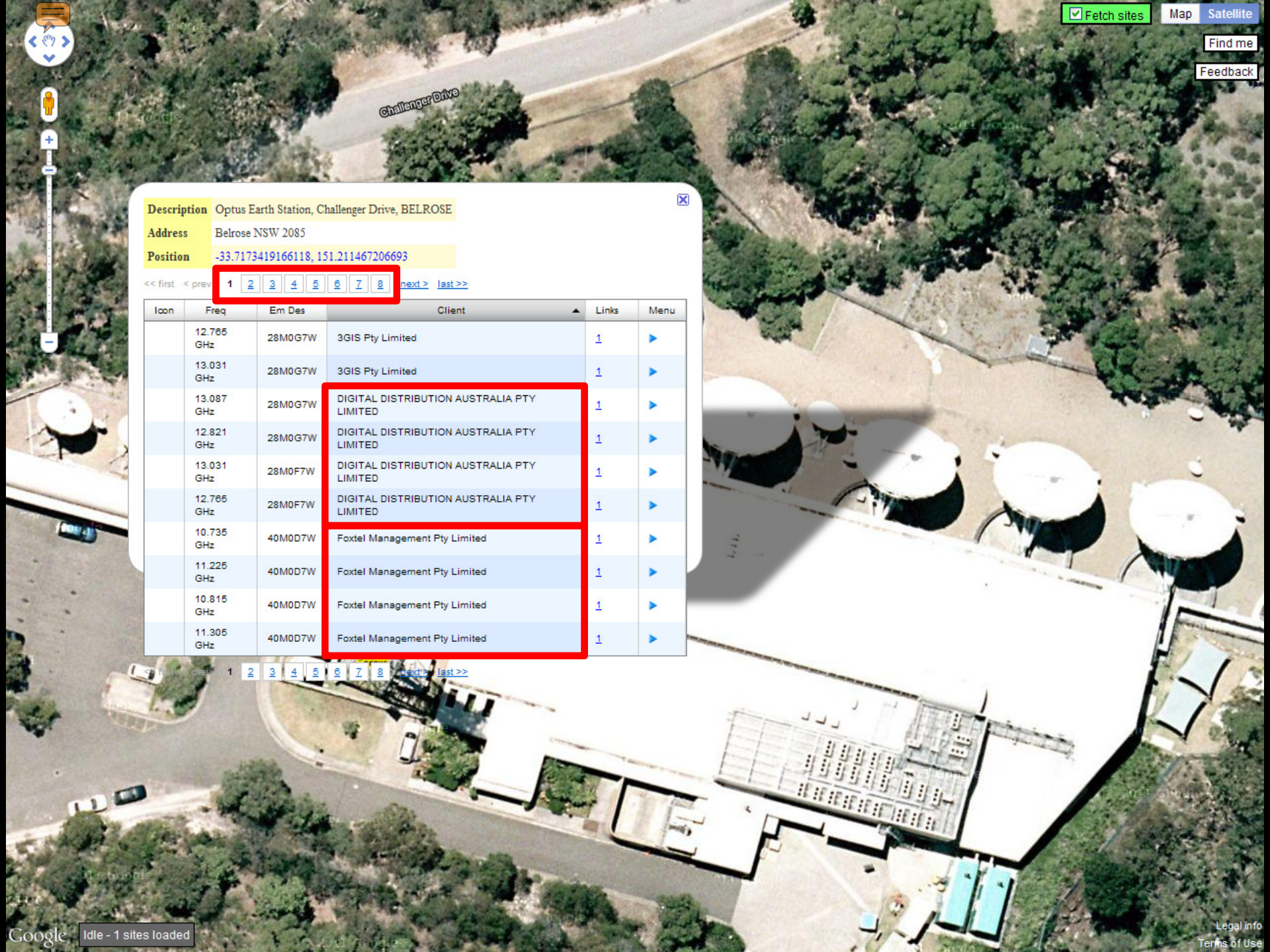
FSS Australia Centre Frequencies (MHz)		
Channel	Uplink	Downlink
1	14029.90	12281.90
2	14092.50	12344.50
3	14155.10	12407.10
4	14217.70	12469.70
5	14280.30	12532.30
6	14342.90	12594.90
7	14405.50	12657.50
8	14468.10	12720.10
9	14029.90	12281.90
10	14092.50	12344.50
11	14155.10	12407.10
12	14217.70	12469.70
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

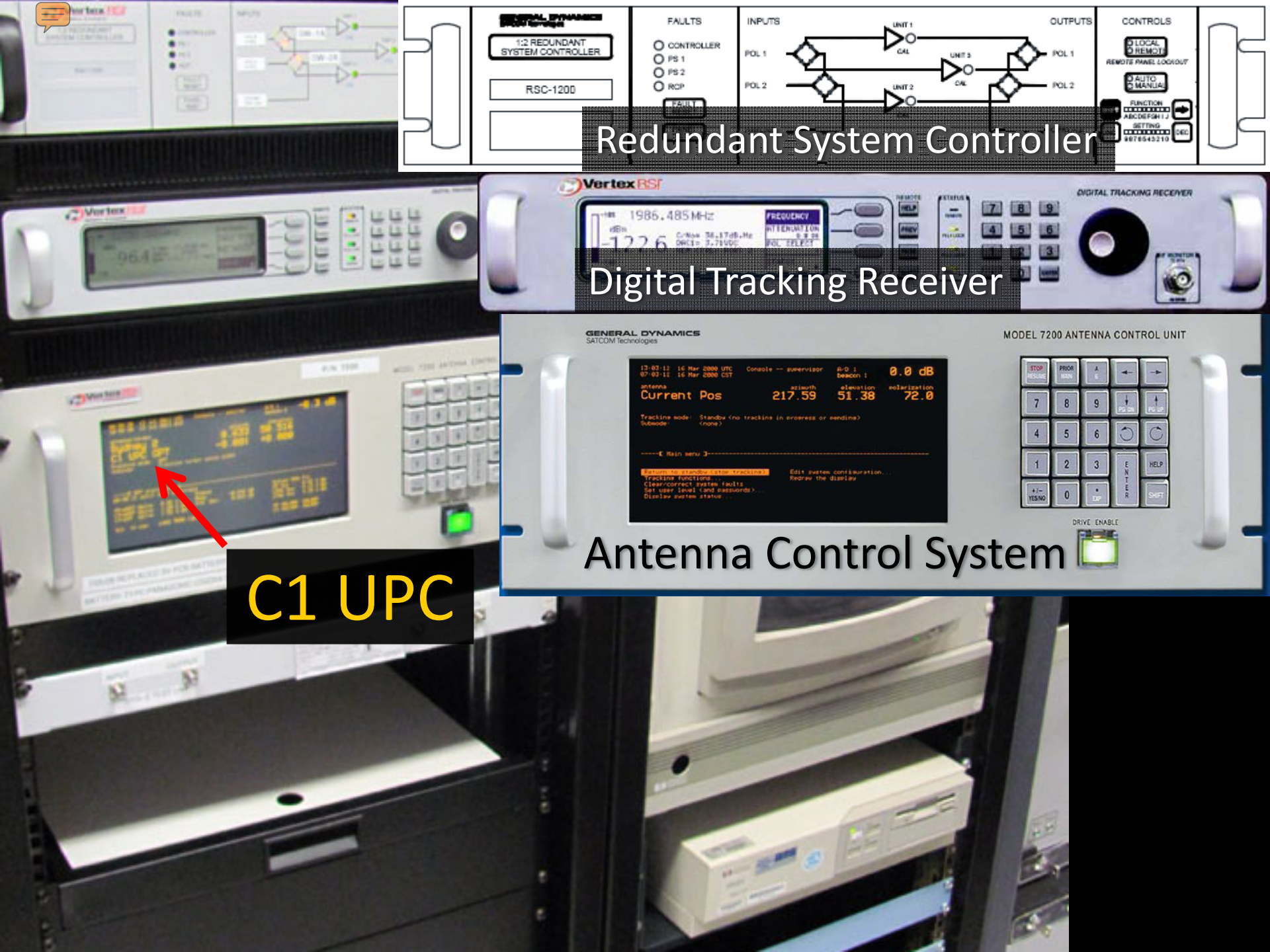
Downlink

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

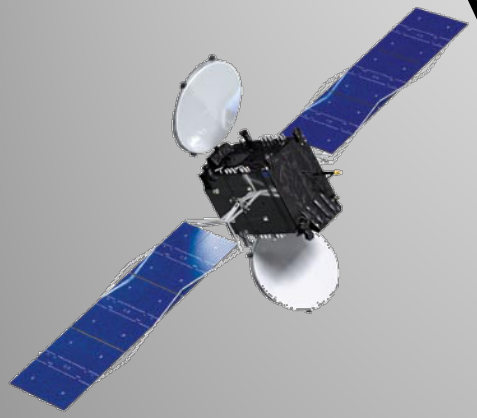
Radyne Comstream Satellite Modem DMD-15

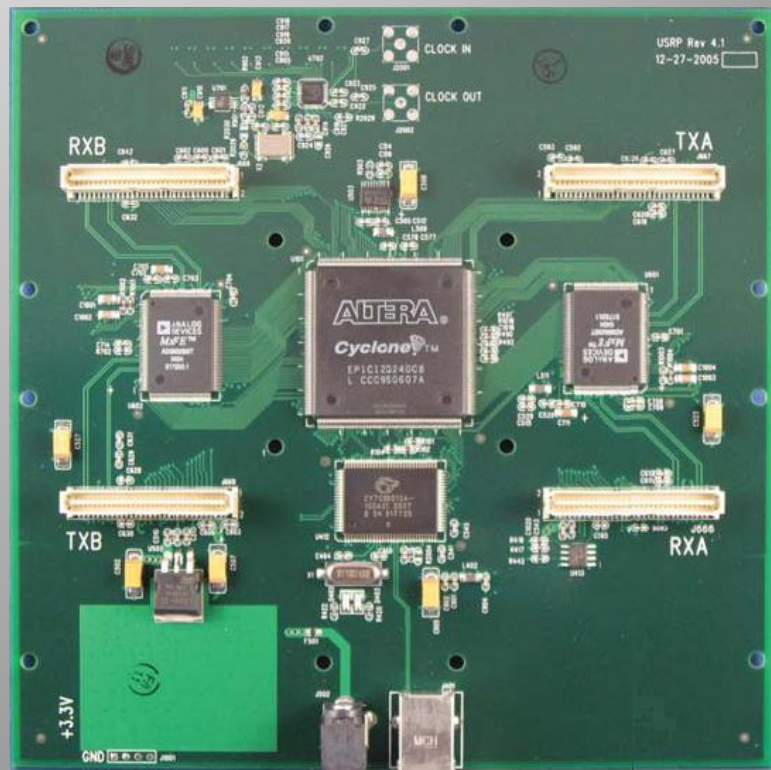

1:2 REDUNDANT SYSTEM CONTROLLER
RSC-1200
FAULTS
CONTROLLER
PS 1
PS 2
RCP
INPUTS
OUTPUTS
CONTROLS
Redundant System Controller
Vertex RSI
DIGITAL TRACKING RECEIVER
Digital Tracking Receiver
GENERAL DYNAMICS
SATCOM Technologies
MODEL 7200 ANTENNA CONTROL UNIT
Current Pos
217.59
51.38
72.0
Antenna Control 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

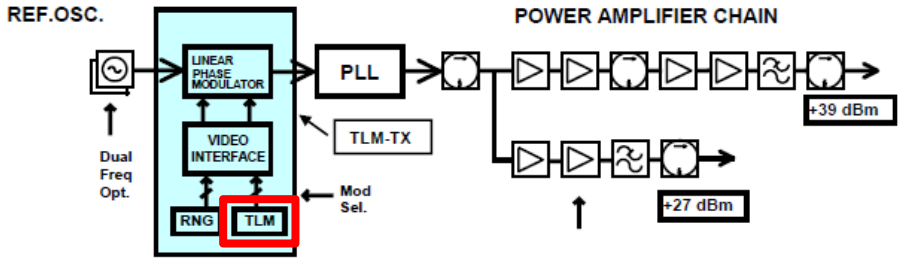
- AMC 14 - AMC 15 - AMC 16
- BSAT 2 A - BSAT 2 B
- BSAT 2 C
- BSAT3A
- ECHOSTAR 10
- ECHOSTAR 7
- GE 2A (NIMIQ2)
- HORIZON 2
- JCSAT 10
- JCSAT 11
- JCSAT 9
- NEWSKIES 6
- NEWSKIES 7
- OPTUS D1
- OPTUS D2
- Panamsat 11
- RAINBOW
- Thor2

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



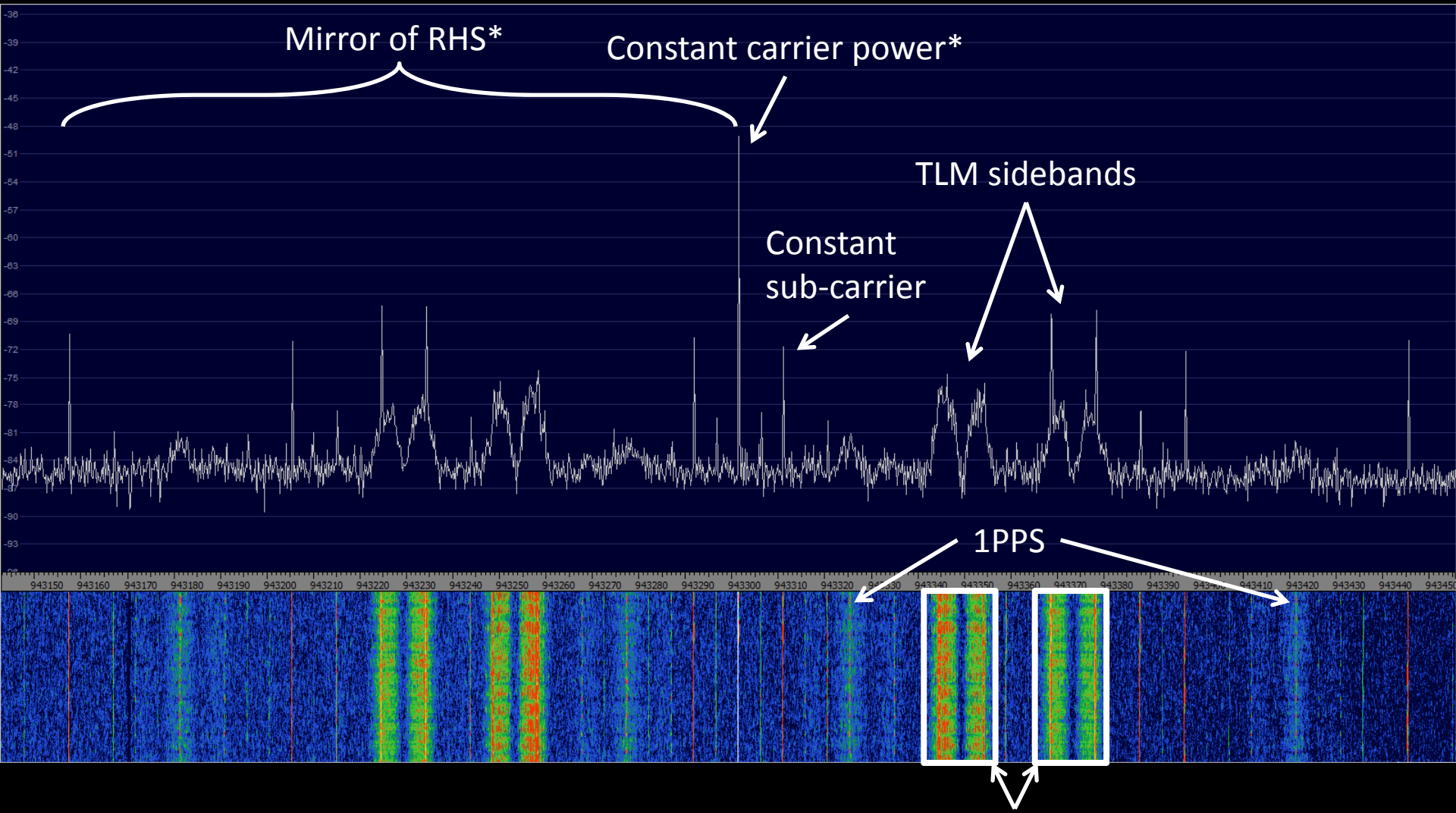
Main Performances

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

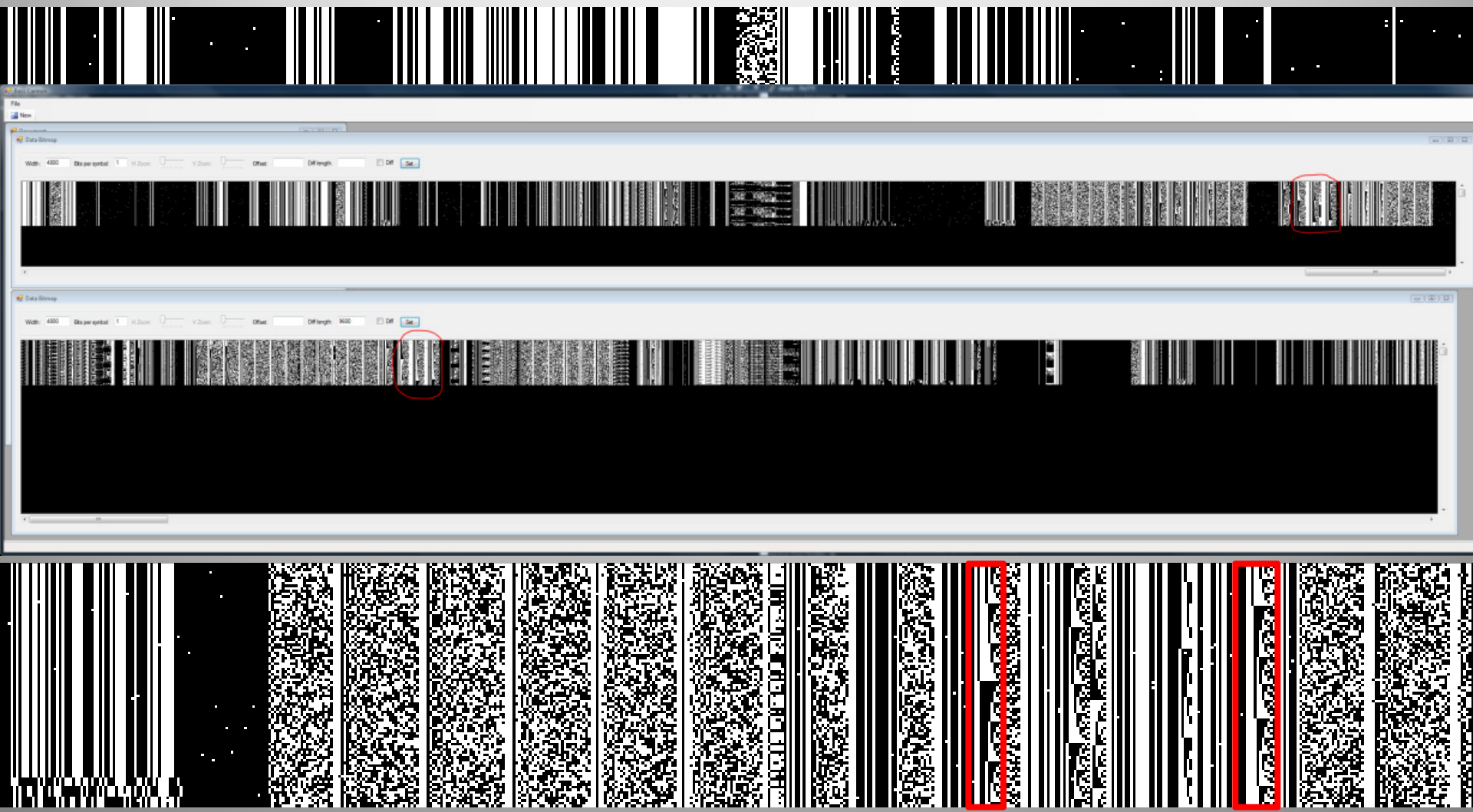
DC Power Consumption	High power mode Low power mode	<55W <18W (Dual Power Opt)
Mass Properties	< 2 kg	
Outline Dimensions	250 x 130 x 80 mm	

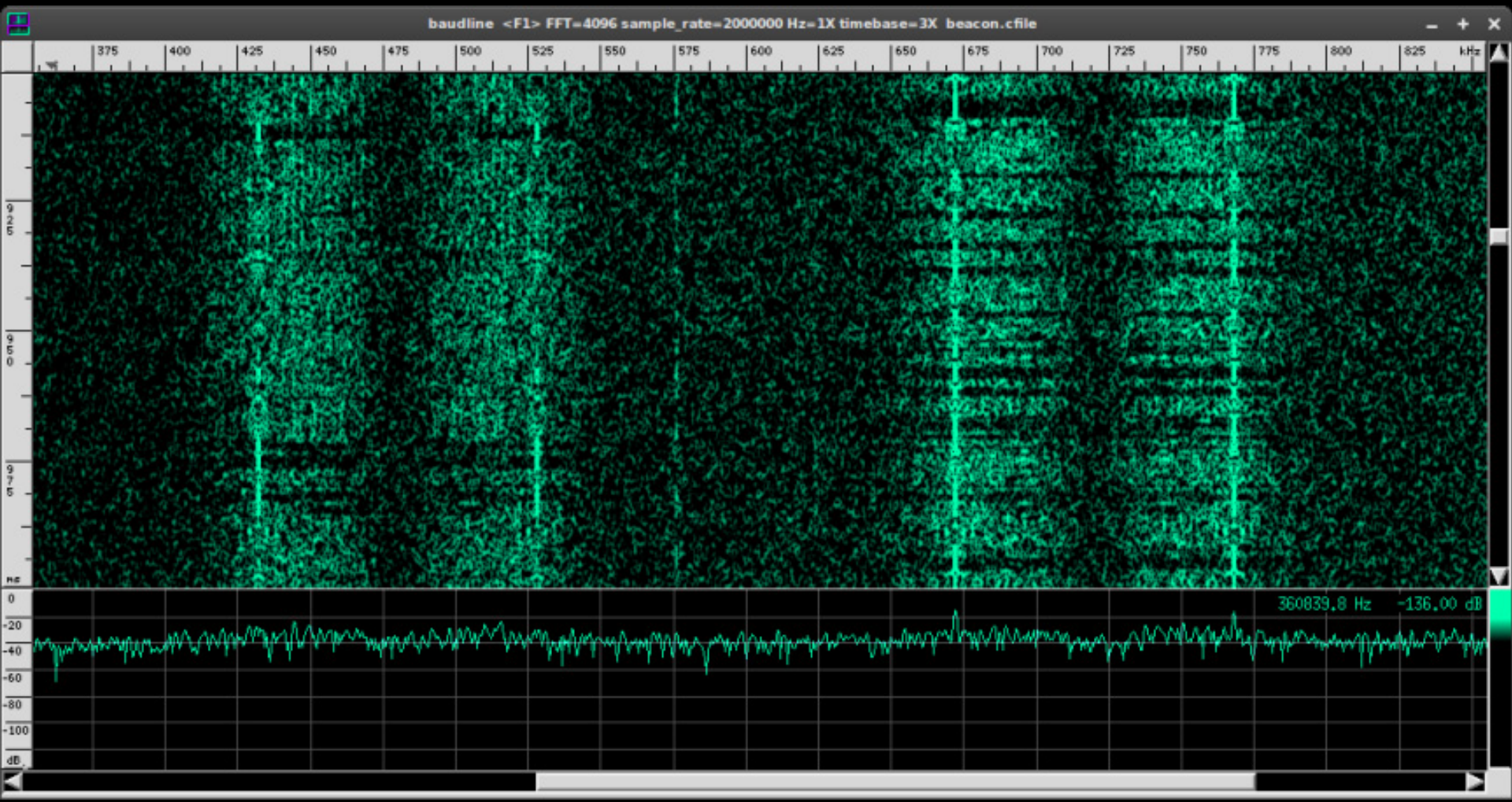
D1 TLM1: 12243.25 MHz



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

Visualisation




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

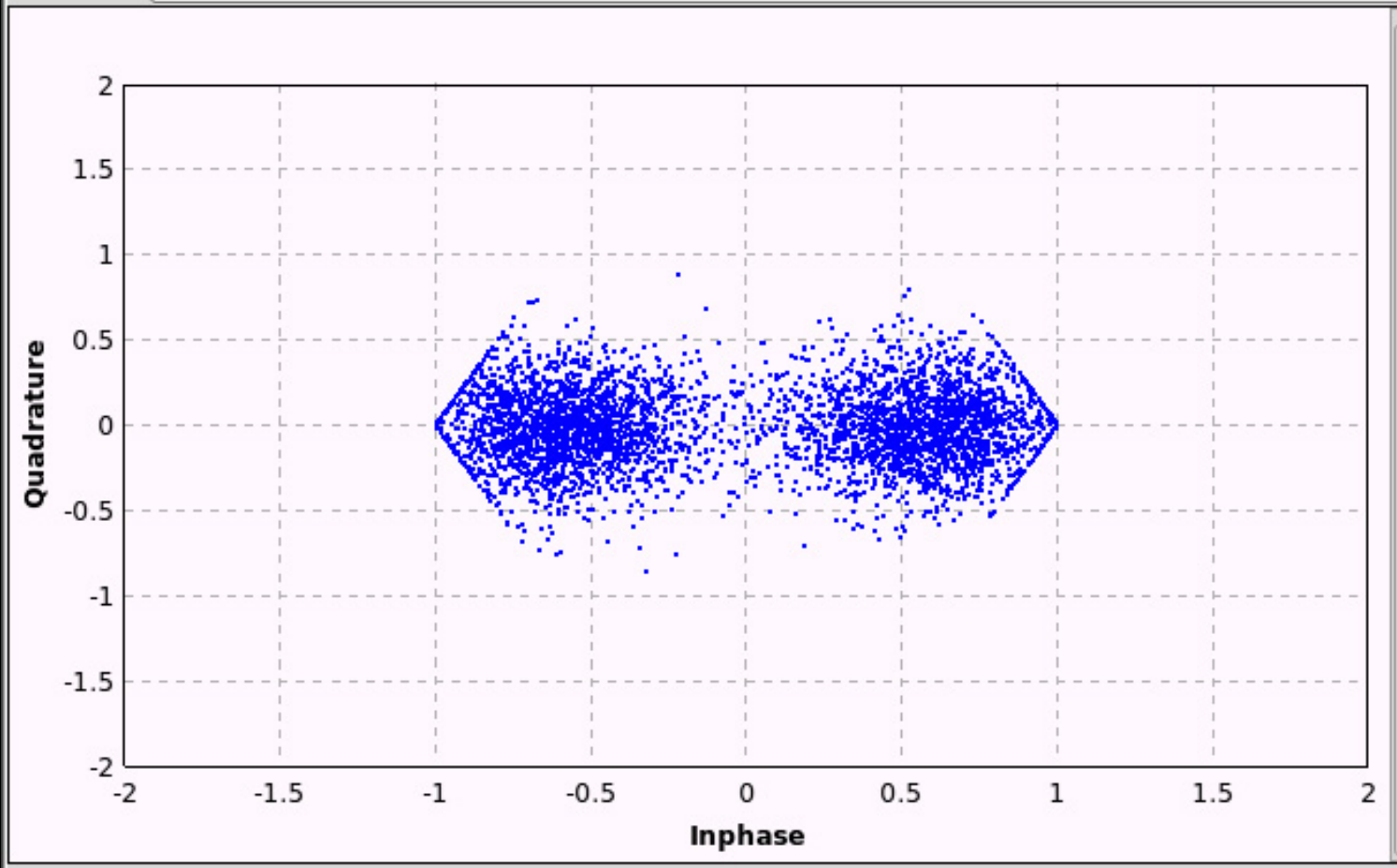
Top Block

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

Symbol rate (fine): 0

sym_rate_coarse: 0

Symbol rate: 9600



Options

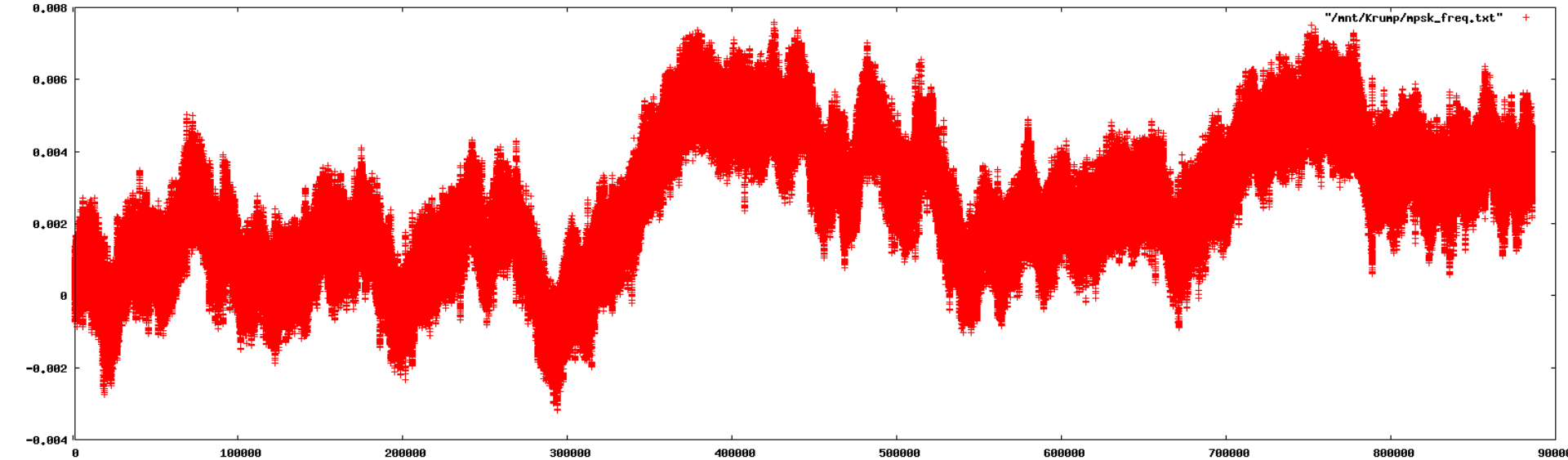
Alpha: 5m

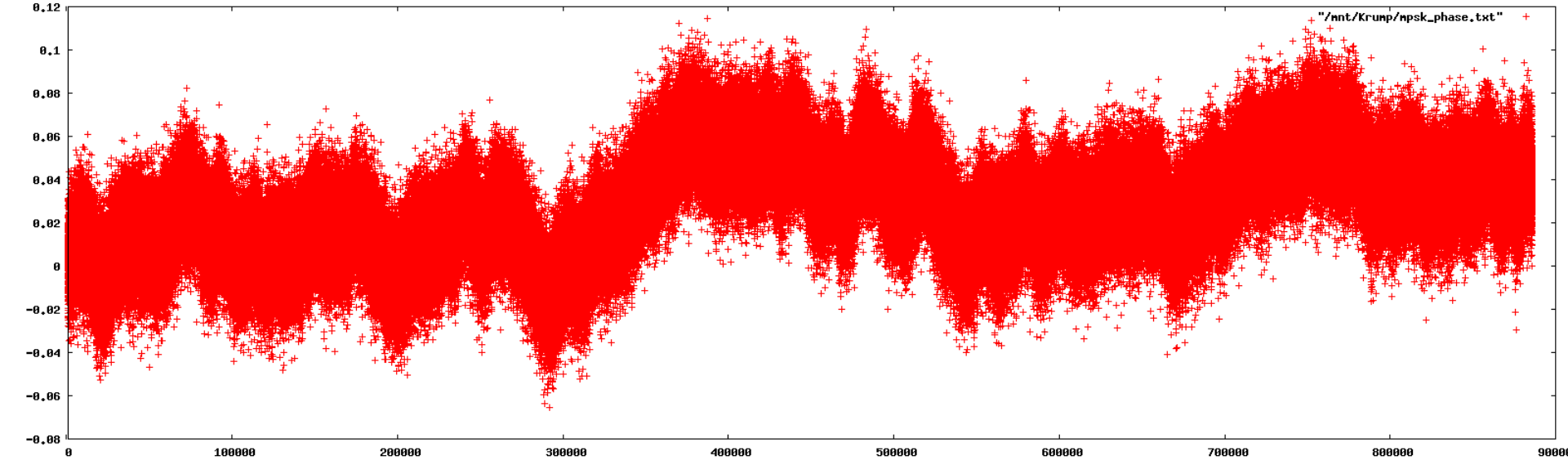
Gain Mu: 5m

Marker: Dot Medium

Run

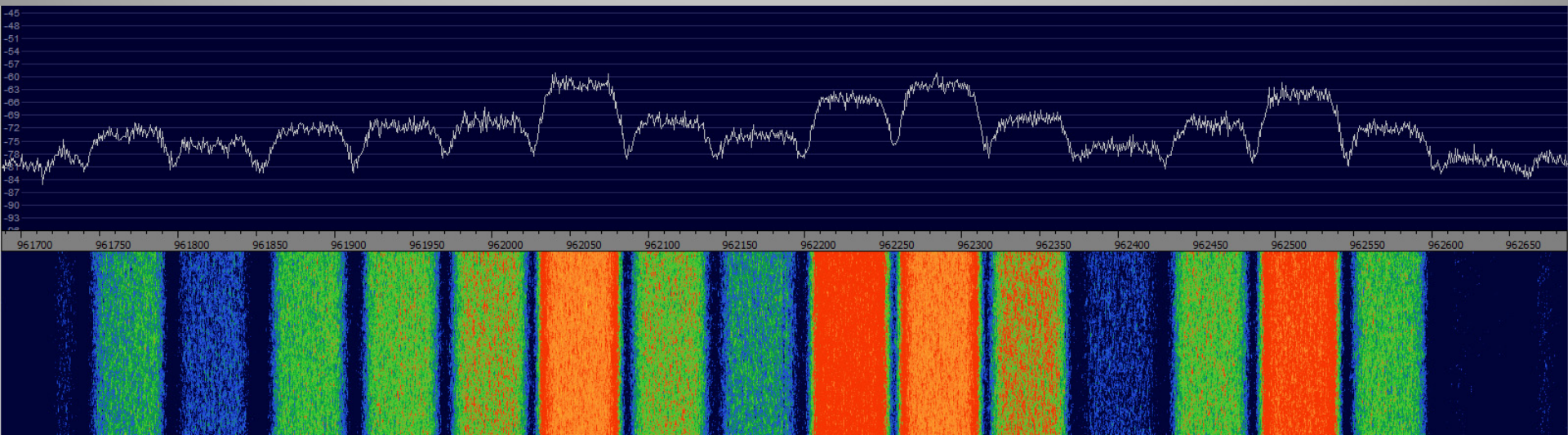
PSK Debug Output





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

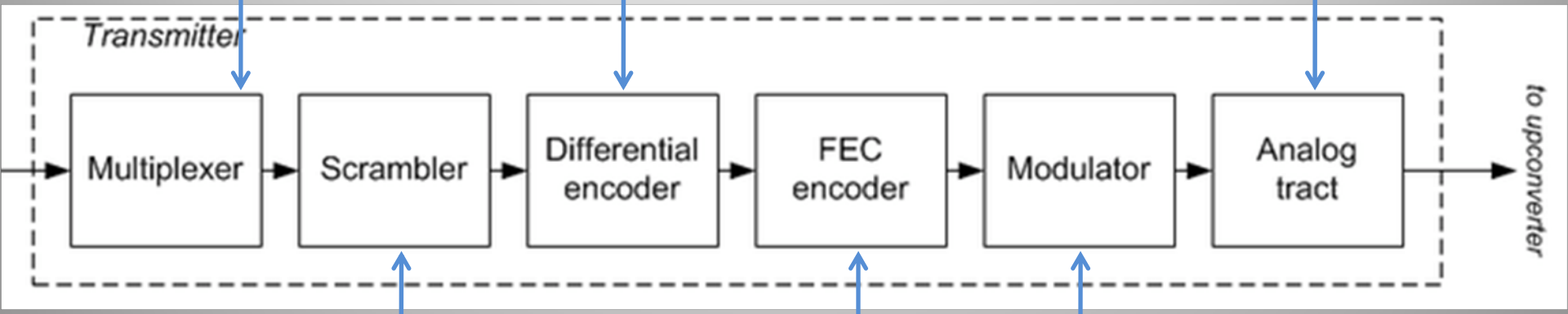


Modulation: pick your parameters

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)

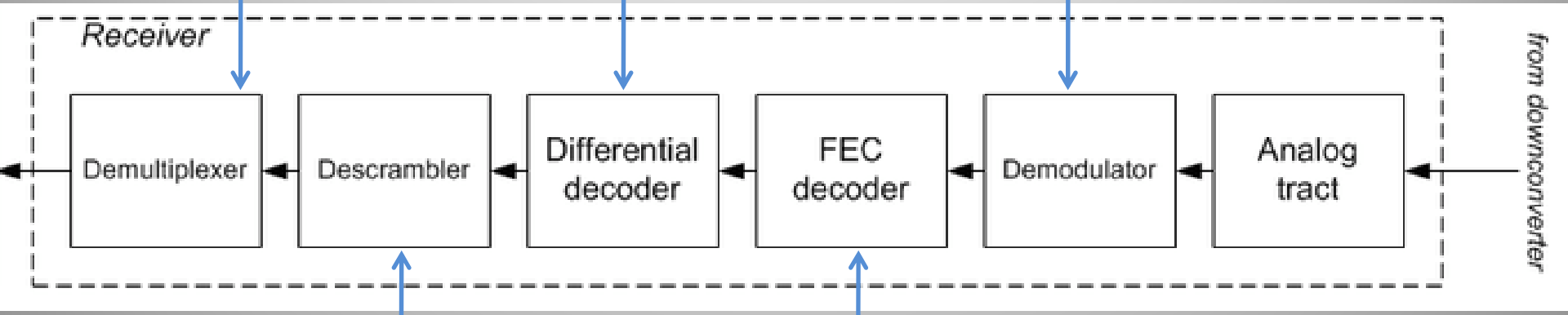
Protect integrity of data (corruption from noise on channel)

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?

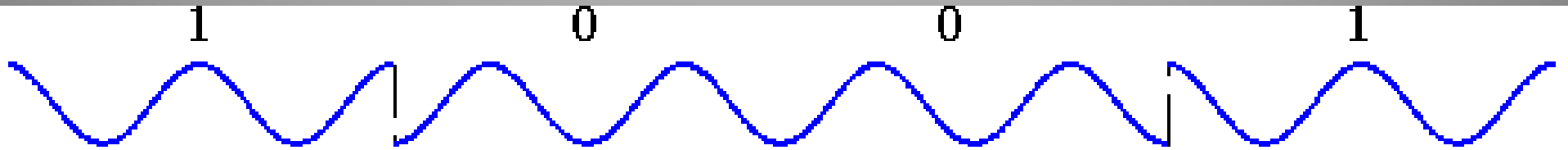
Which FEC(s) is used?
Is it a concatenated code?
What is the code rate?
What is the block size?
How is it synchronised?

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!

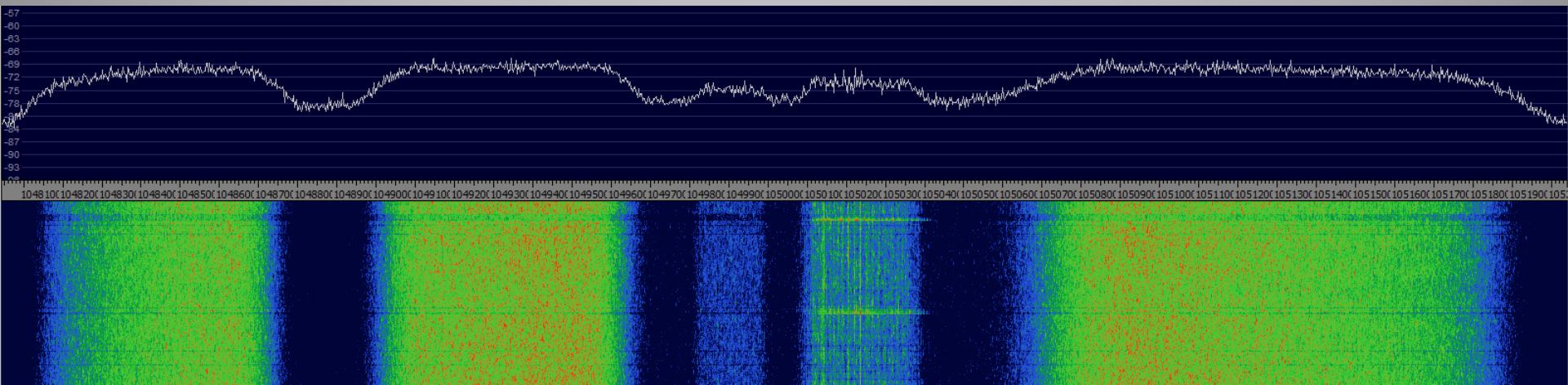
Aside: PSK, Symbols & Bits

- 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…

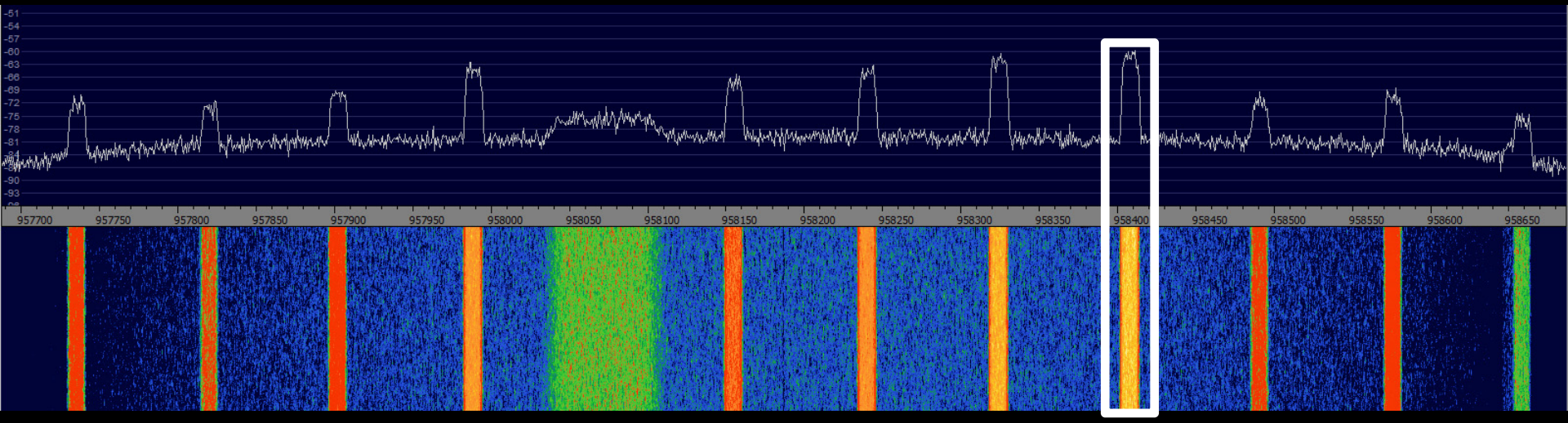


Determining modulation & rate

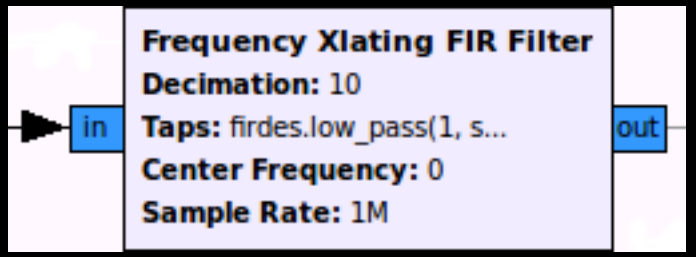
- Assuming PSK, easy to determine:
  - Modulation order: multiply the signal by itself
  - Symbol rate: multiply the signal by a lagged version of itself (cyclostationary analysis)
- Only a few GR blocks required do this



Let’s try one…

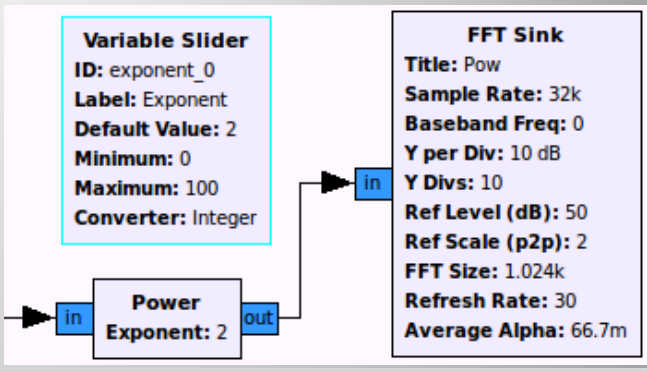


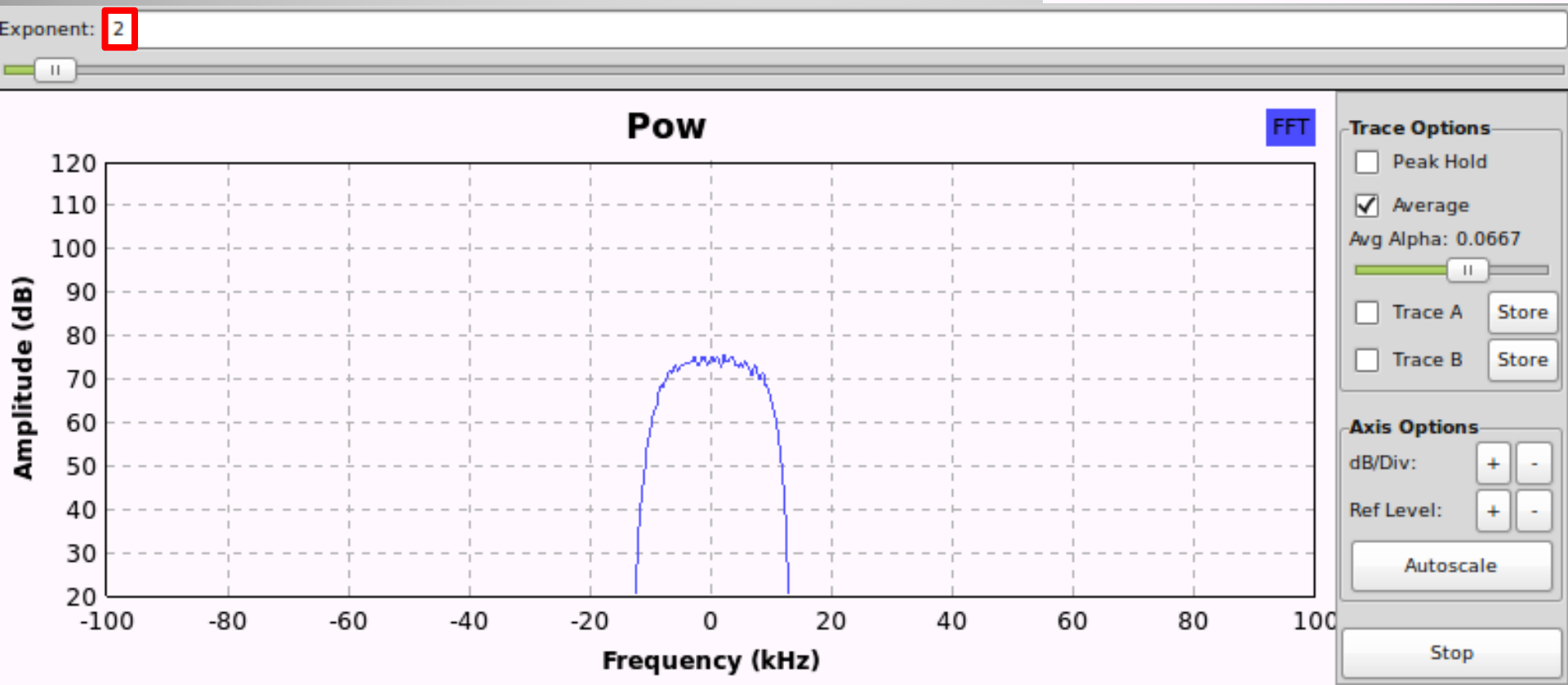
- Feed entire baseband spectrum into GR
- Perform ‘channel selection’ to isolate stream of interest (create new baseband centred on stream)



Determine PSK order

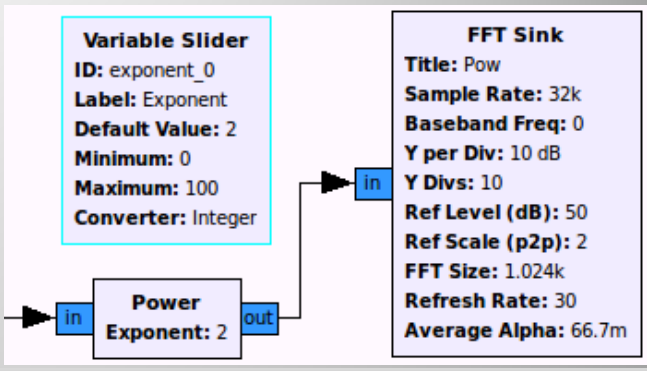
- Start at 2 and go up
- Stop when spike appears

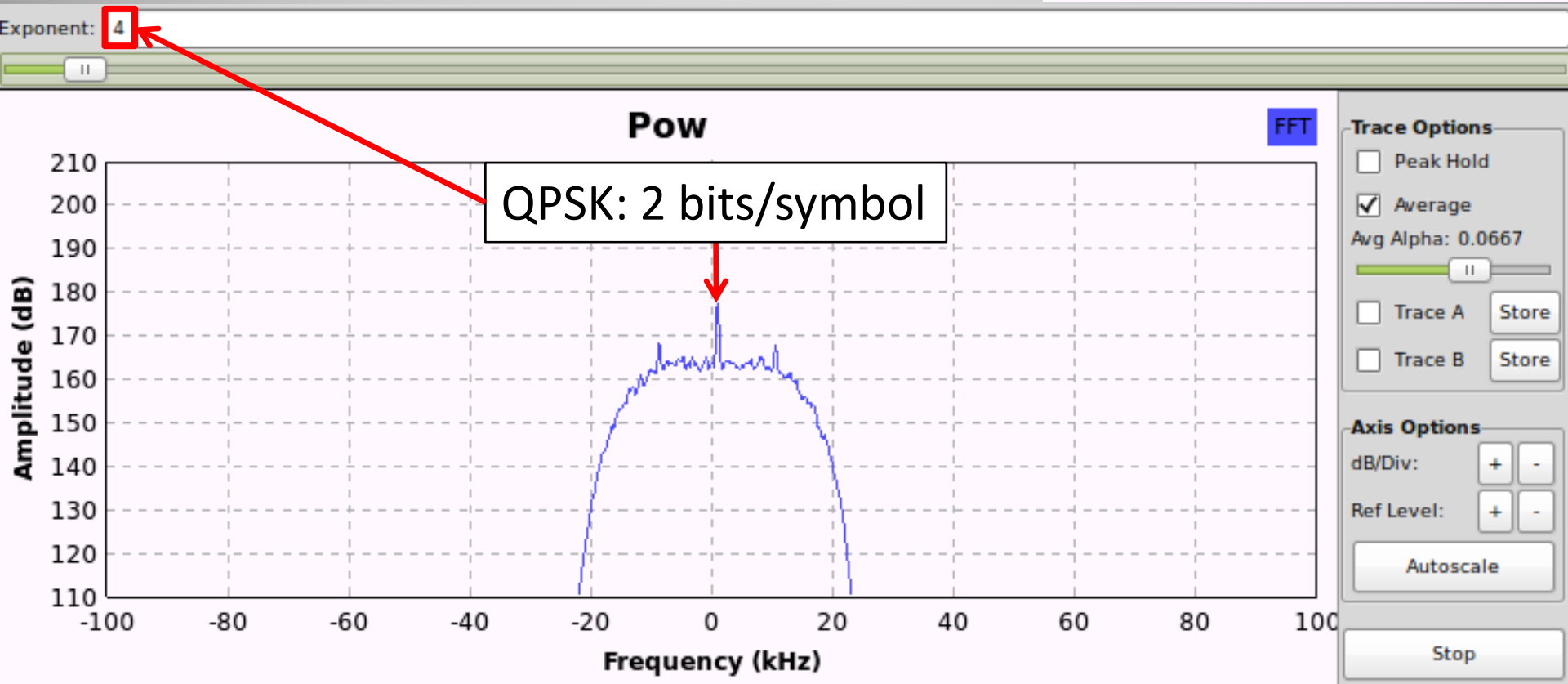




Determine PSK order

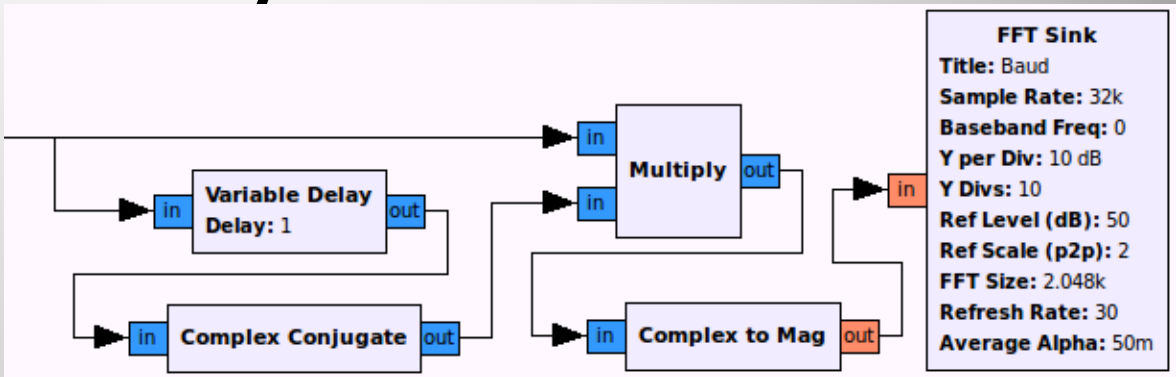
- Start at 2 and go up
- Stop when spike appears



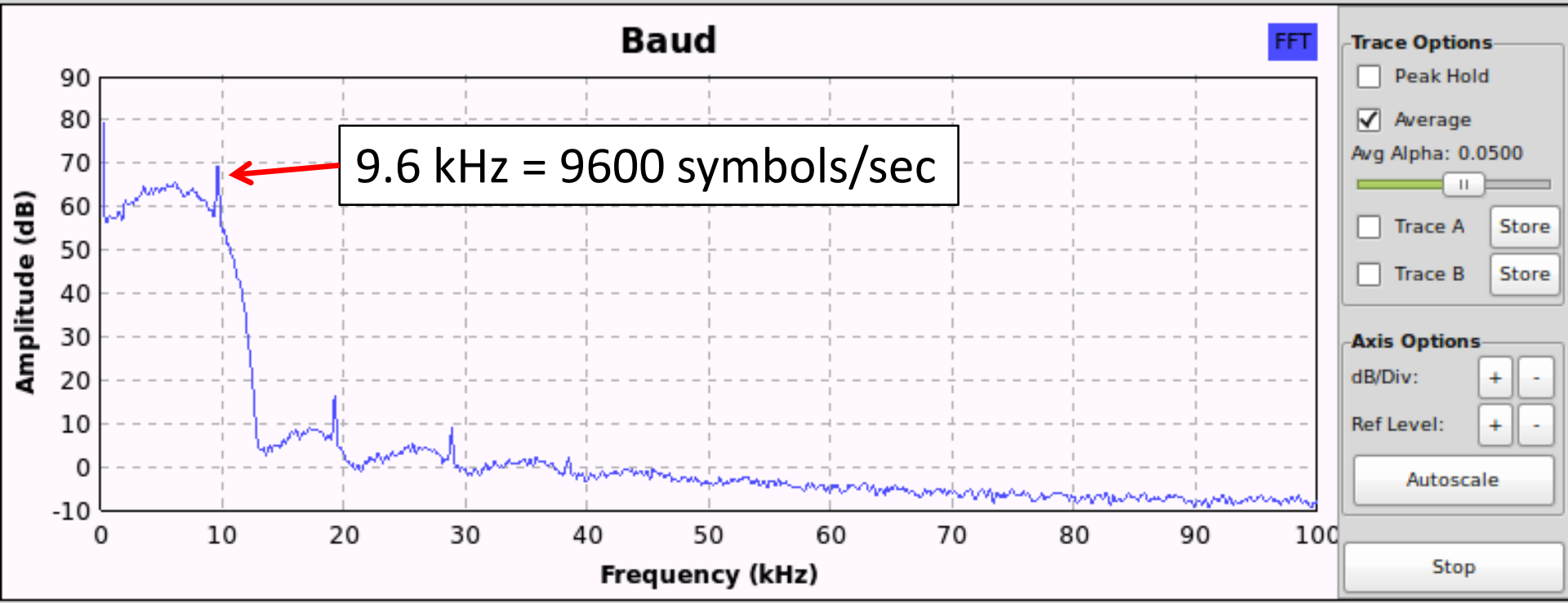


Determine Symbol Rate

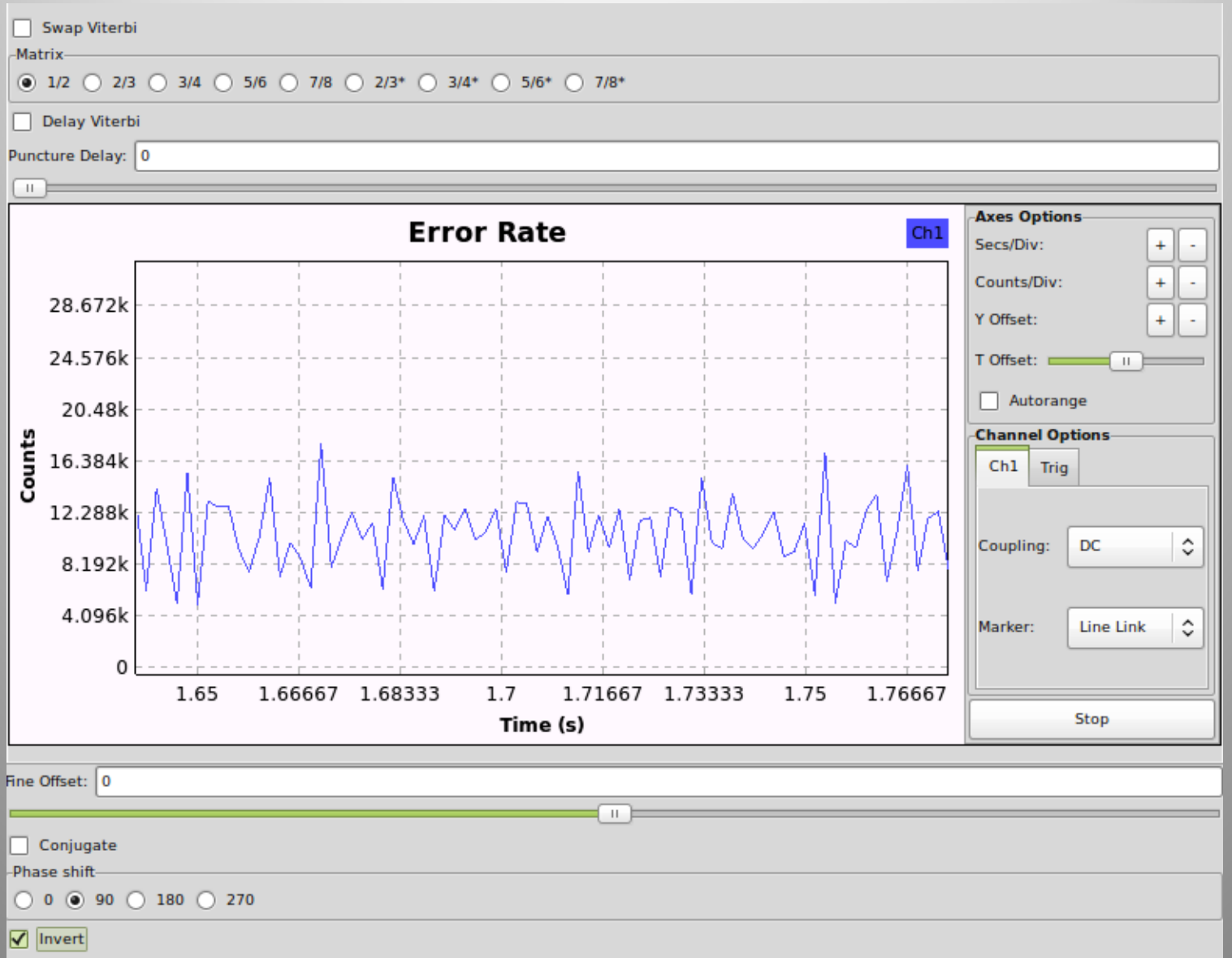
- Find first peak



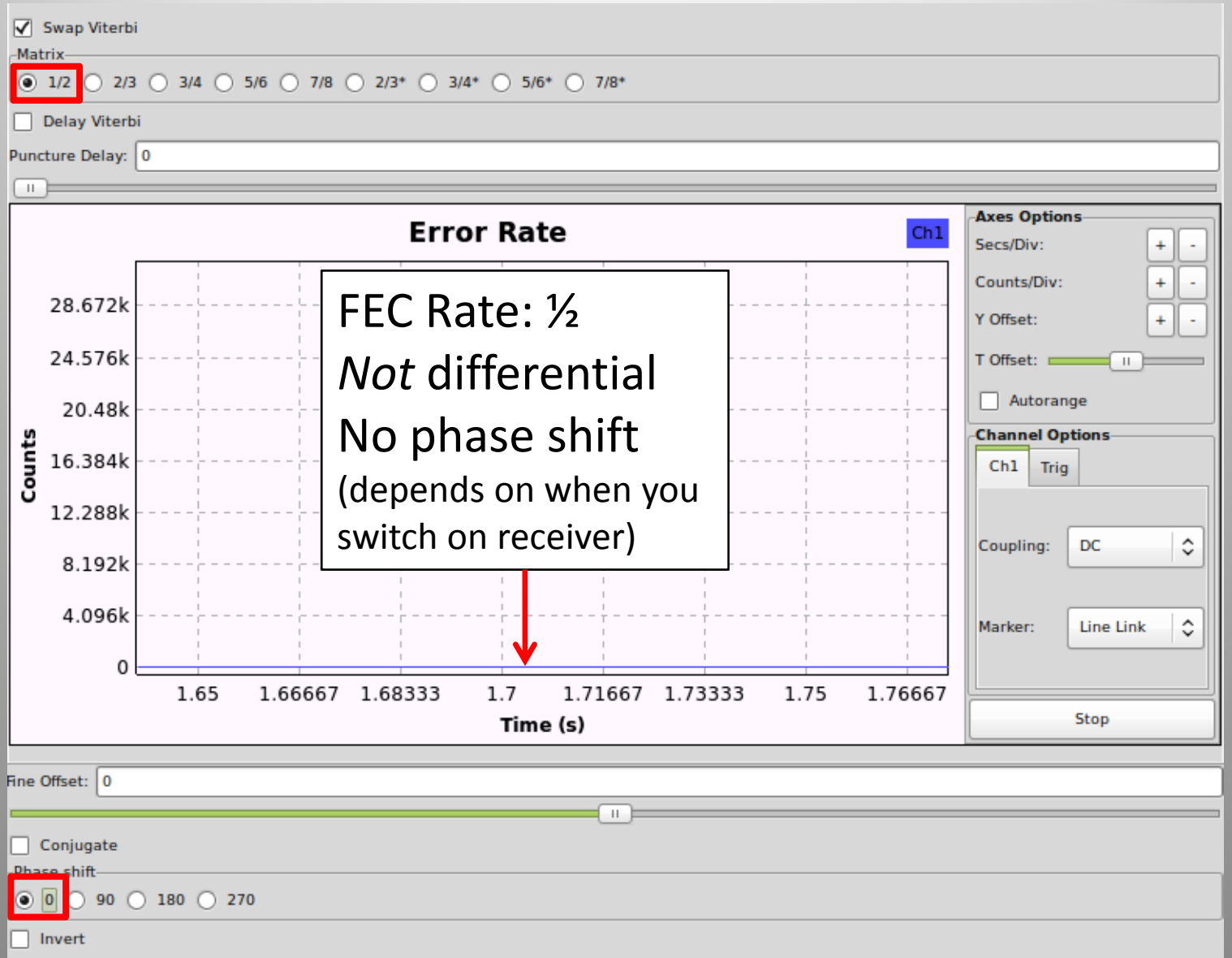
Nominal samples per symbol: 2

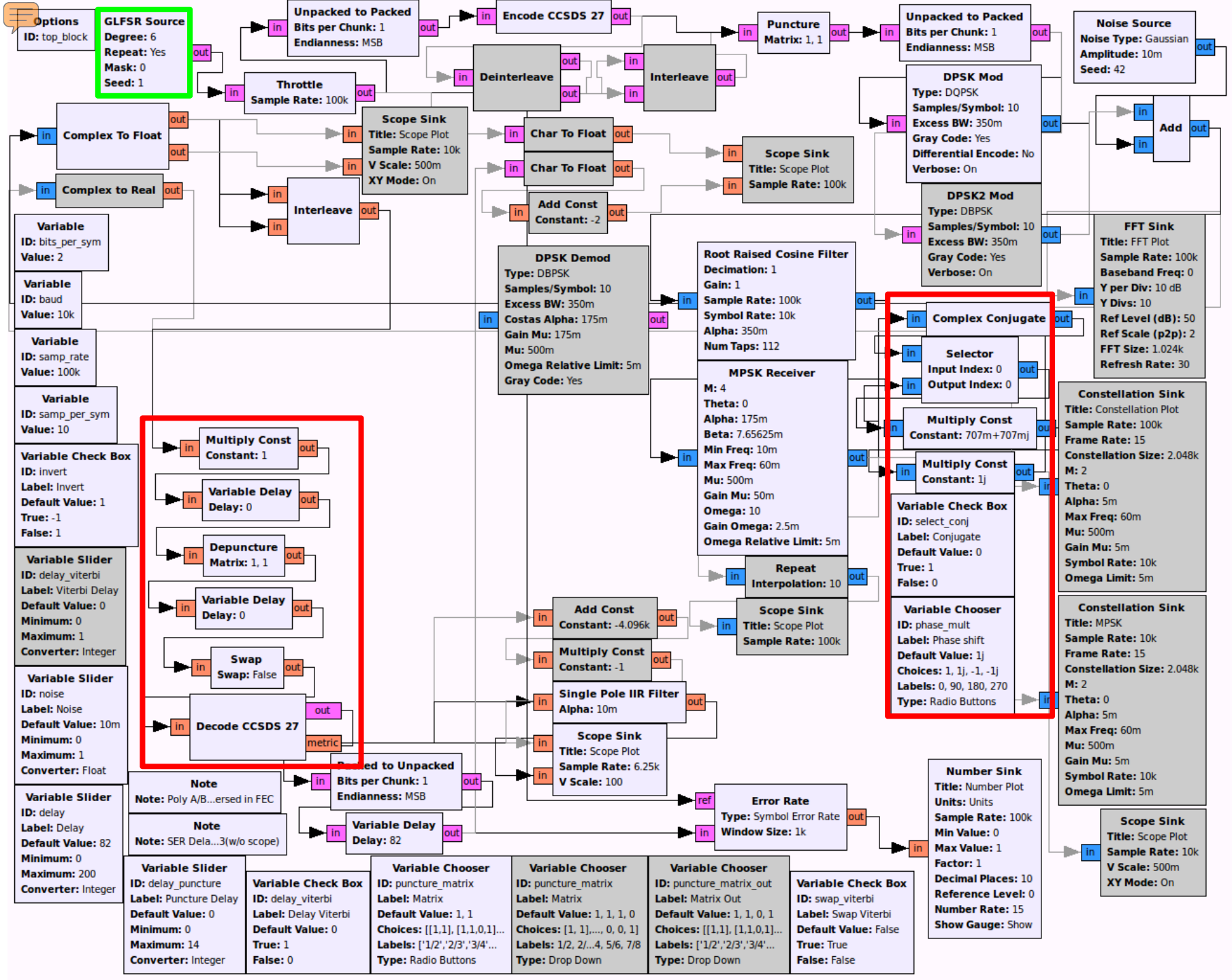


Try synchronisation & FEC

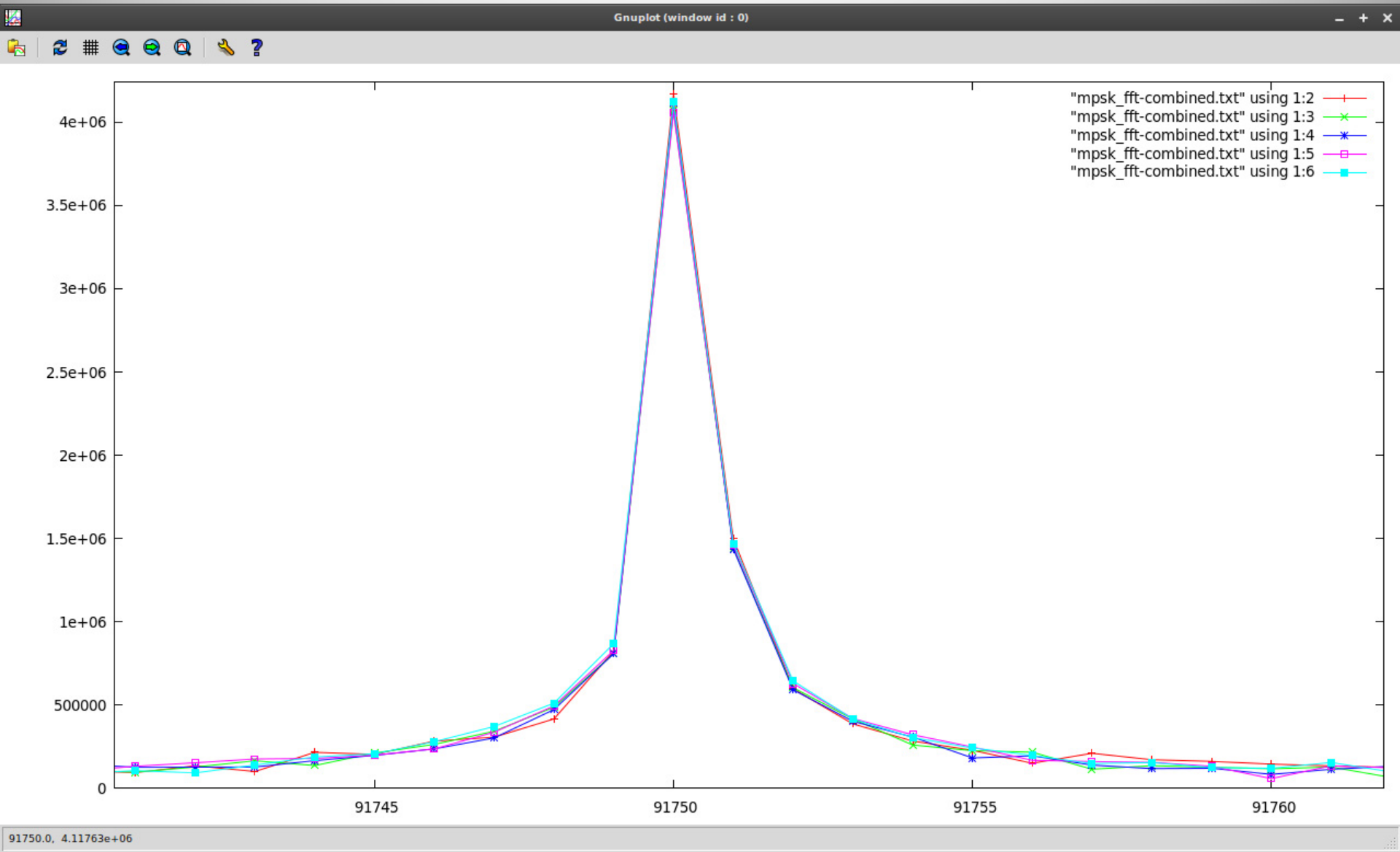


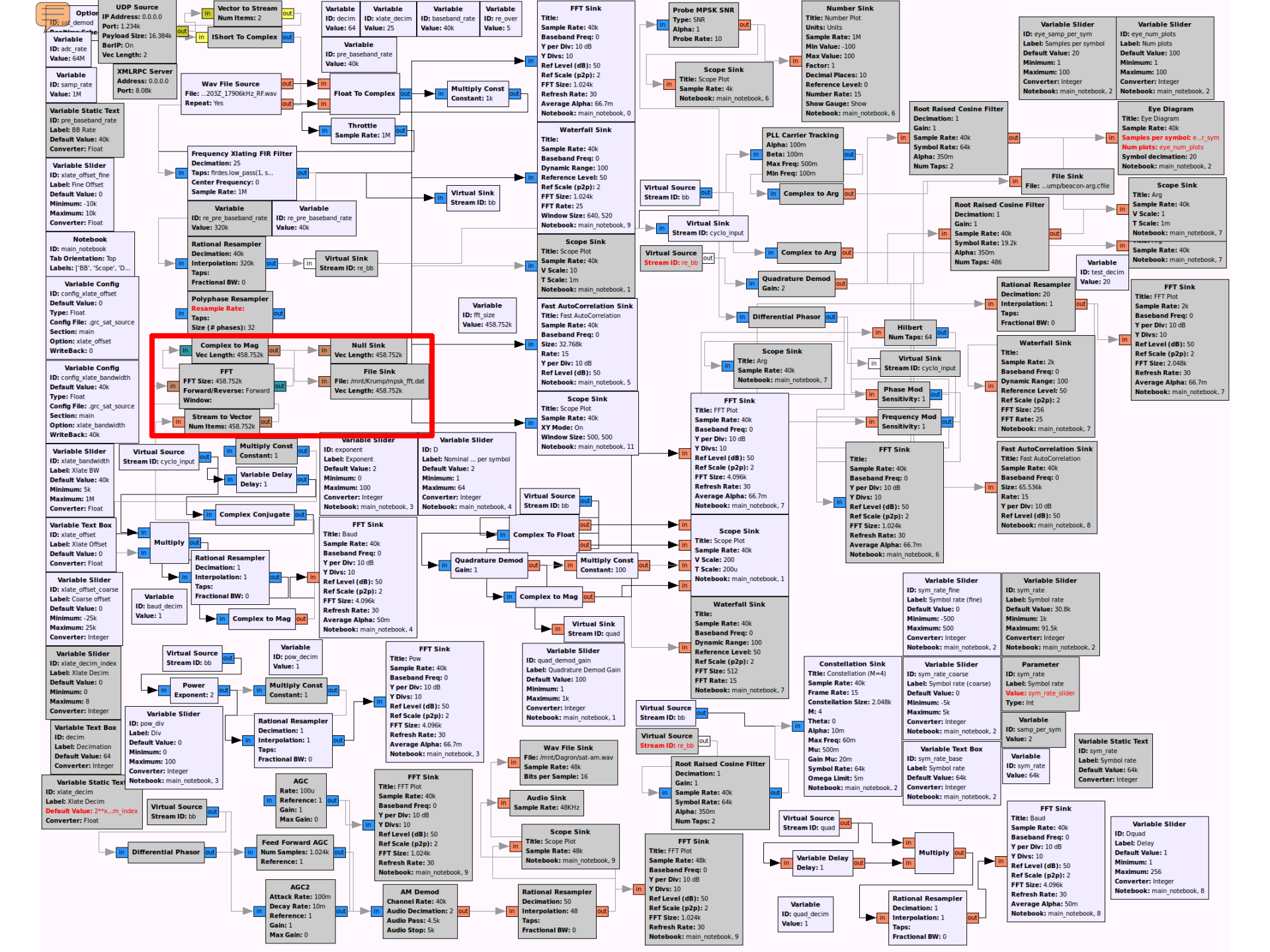
Try synchronisation & FEC

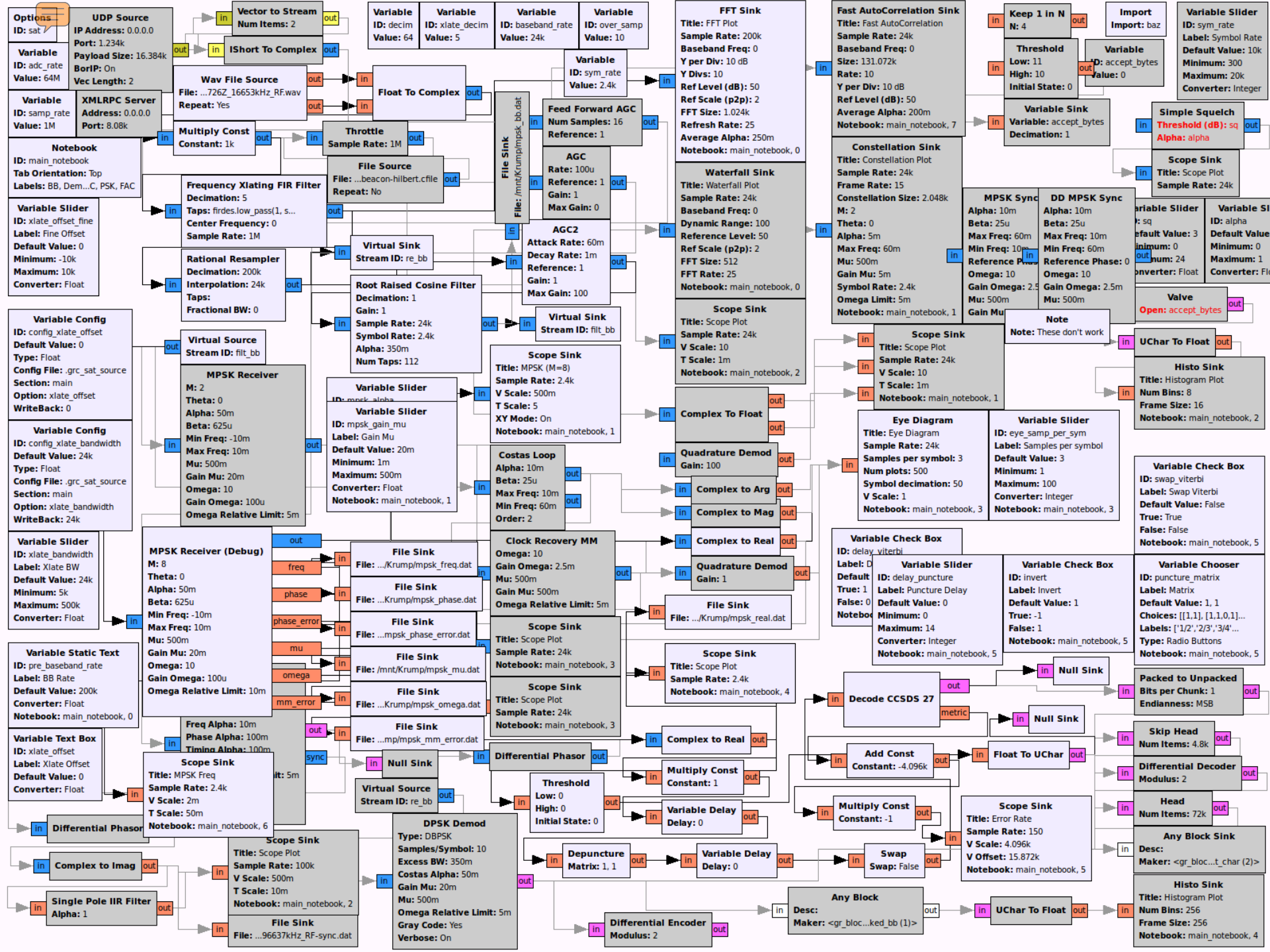


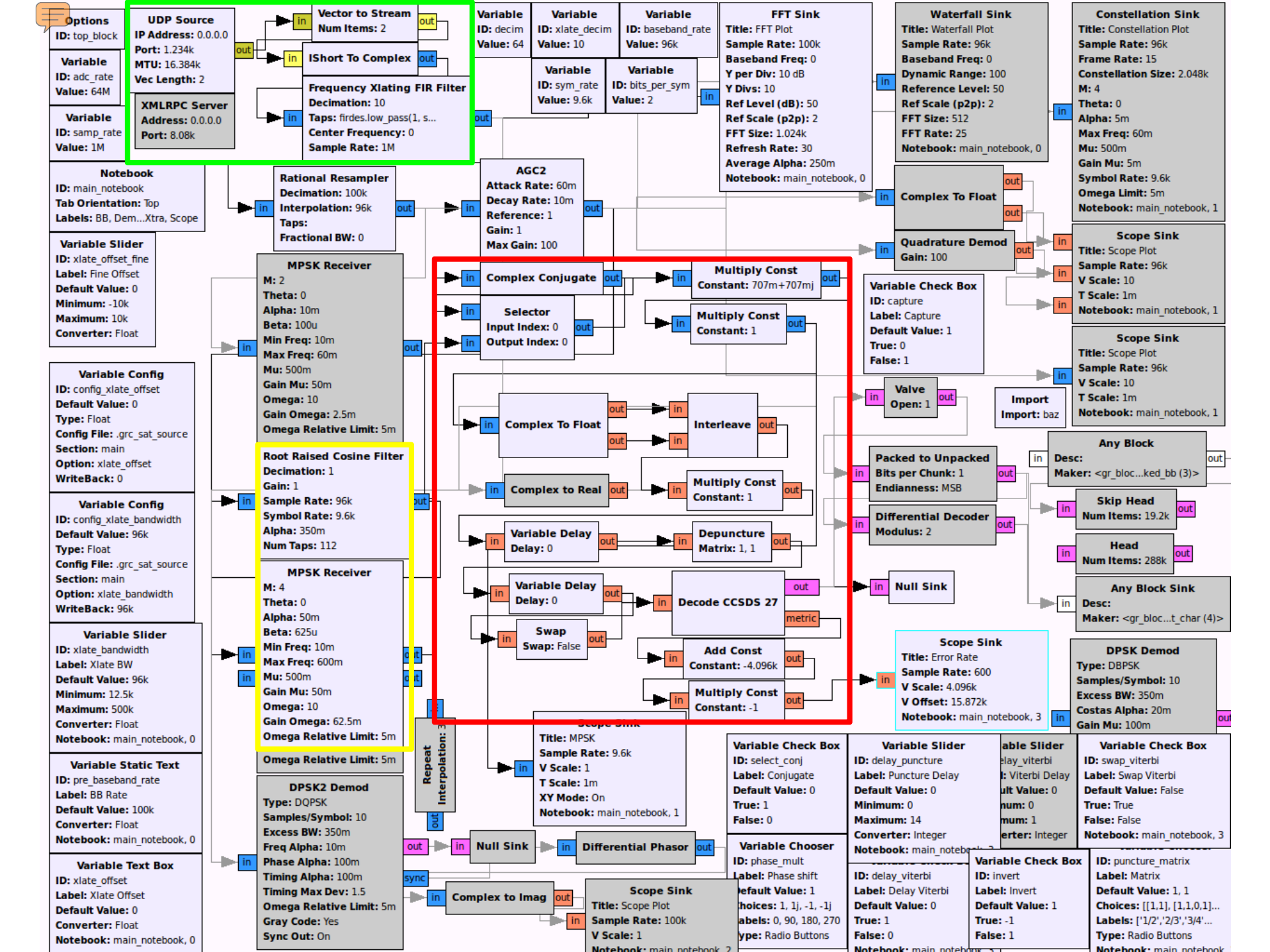

Options
ID: top_block
GLFSR Source
Degree: 6
Repeat: Yes
Mask: 0
Seed: 1
Unpacked to Packed
Bits per Chunk: 1
Endianness: MSB
Encode CCSDS 27
Puncture
Matrix: 1, 1
Unpacked to Packed
Bits per Chunk: 1
Endianness: MSB
Noise Source
Noise Type: Gaussian
Amplitude: 10m
Seed: 42
Throttle
Sample Rate: 100k
Deinterleave
Interleave
DPSK Mod
Type: DQPSK
Samples/Symbol: 10
Excess BW: 350m
Gray Code: Yes
Differential Encode: No
Verbose: On
Add
Complex To Float
Complex to Real
Scope Sink
Title: Scope Plot
Sample Rate: 10k
V Scale: 500m
XY Mode: On
Char To Float
Char To Float
Add Const
Constant: -2
Interleave
Scope Sink
Title: Scope Plot
Sample Rate: 100k
DPSK2 Mod
Type: DBPSK
Samples/Symbol: 10
Excess BW: 350m
Gray Code: Yes
Verbose: On
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
Variable
ID: bits_per_sym
Value: 2
Variable
ID: baud
Value: 10k
Variable
ID: samp_rate
Value: 100k
Variable
ID: samp_per_sym
Value: 10
DPSK Demod
Type: DBPSK
Samples/Symbol: 10
Excess BW: 350m
Costas Alpha: 175m
Gain Mu: 175m
Mu: 500m
Omega Relative Limit: 5m
Gray Code: Yes
Root Raised Cosine Filter
Decimation: 1
Gain: 1
Sample Rate: 100k
Symbol Rate: 10k
Alpha: 350m
Num Taps: 112
MPSK Receiver
M: 4
Theta: 0
Alpha: 175m
Beta: 7.65625m
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: 1j
Variable Check Box
ID: select_conj
Label: Conjugate
Default Value: 0
True: 1
False: 0
Variable Chooser
ID: phase_mult
Label: Phase shift
Default Value: 1j
Choices: 1, 1j, -1, -1j
Labels: 0, 90, 180, 270
Type: Radio Buttons
Constellation Sink
Title: Constellation Plot
Sample Rate: 100k
Frame Rate: 15
Constellation Size: 2.048k
M: 2
Theta: 0
Alpha: 5m
Max Freq: 60m
Mu: 500m
Gain Mu: 5m
Symbol Rate: 10k
Omega Limit: 5m
Constellation Sink
Title: MPSK
Sample Rate: 10k
Frame Rate: 15
Constellation Size: 2.048k
M: 2
Theta: 0
Alpha: 5m
Max Freq: 60m
Mu: 500m
Gain Mu: 5m
Symbol Rate: 10k
Omega Limit: 5m
Multiply Const
Constant: 1
Variable Delay
Delay: 0
Depuncture
Matrix: 1, 1
Variable Delay
Delay: 0
Swap
Swap: False
Decode CCSDS 27
out
metric
Repeat
Interpolation: 10
Scope Sink
Title: Scope Plot
Sample Rate: 100k
Add Const
Constant: -4.096k
Multiply Const
Constant: -1
Single Pole IIR Filter
Alpha: 10m
Scope Sink
Title: Scope Plot
Sample Rate: 6.25k
V Scale: 100
Variable Check Box
ID: invert
Label: Invert
Default Value: 1
True: -1
False: 1
Variable Slider
ID: delay_viterbi
Label: Viterbi Delay
Default Value: 0
Minimum: 0
Maximum: 1
Converter: Integer
Variable Slider
ID: noise
Label: Noise
Default Value: 10m
Minimum: 0
Maximum: 1
Converter: Float
Variable Slider
ID: delay
Label: Delay
Default Value: 82
Minimum: 0
Maximum: 200
Converter: Integer
Note
Note: Poly A/B...ersed in FEC
Note
Note: SER Dela...3(w/o scope)
Bits per Chunk: 1
Endianness: MSB
Variable Delay
Delay: 82
Error Rate
Type: Symbol Error Rate
Window Size: 1k
Number Sink
Title: Number Plot
Units: Units
Sample Rate: 100k
Min Value: 0
Max Value: 1
Factor: 1
Decimal Places: 10
Reference Level: 0
Number Rate: 15
Show Gauge: Show
Scope Sink
Title: Scope Plot
Sample Rate: 10k
V Scale: 500m
XY Mode: On
Variable Slider
ID: delay_puncture
Label: Puncture Delay
Default Value: 0
Minimum: 0
Maximum: 14
Converter: Integer
Variable Check Box
ID: delay_viterbi
Label: Delay Viterbi
Default Value: 0
True: 1
False: 0
Variable Chooser
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
Variable Chooser
ID: puncture_matrix
Label: Matrix
Default Value: 1, 1, 1, 0
Choices: [1, 1],...., 0, 0, 1]
Labels: 1/2, 2/...4, 5/6, 7/8
Type: Drop Down
Variable Chooser
ID: puncture_matrix_out
Label: Matrix Out
Default Value: 1, 1, 0, 1
Choices: [[1,1], [1,1,0,1]...
Labels: ['1/2','2/3','3/4'...
Type: Drop Down
Variable Check Box
ID: swap_viterbi
Label: Swap Viterbi
Default Value: False
True: True
False: False

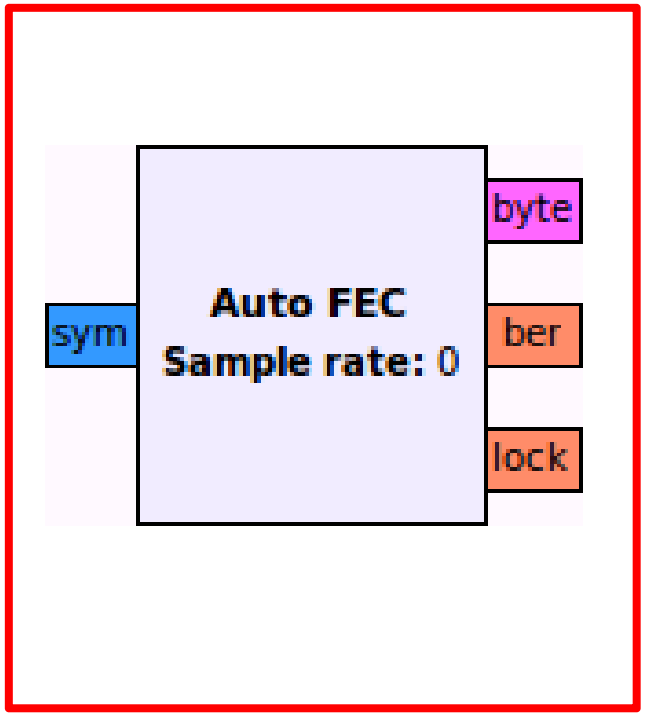
Find Precise Symbol Rate




UDP Source
IP Address: 0.0.0.0
Port: 1.234k
Payload Size: 16.384k
BorIP: On
Vec Length: 2
Vector to Stream
Num Items: 2
IShort To Complex
XMLRPC Server
Address: 0.0.0.0
Port: 8.08k
Variable
ID: adc_rate
Value: 64M
Variable
ID: samp_rate
Value: 1M
Variable Static Text
ID: pre_baseband_rate
Label: BB Rate
Default Value: 40k
Converter: Float
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', 'Scope', 'D...
Variable Config
ID: config_xlate_offset
Default Value: 0
Type: Float
Config File: .grc_sat_source
Section: main
Option: xlate_offset
WriteBack: 0
Variable Config
ID: config_xlate_bandwidth
Default Value: 40k
Type: Float
Config File: .grc_sat_source
Section: main
Option: xlate_bandwidth
WriteBack: 40k
Variable Slider
ID: xlate_bandwidth
Label: Xlate BW
Default Value: 40k
Minimum: 5k
Maximum: 1M
Converter: Float
Variable Text Box
ID: xlate_offset
Label: Xlate Offset
Default Value: 0
Converter: Float
Variable Slider
ID: xlate_offset_coarse
Label: Coarse offset
Default Value: 0
Minimum: -25k
Maximum: 25k
Converter: Integer
Variable Slider
ID: xlate_decim_index
Label: Xlate Decim
Default Value: 0
Minimum: 0
Maximum: 8
Converter: Integer
Variable Text Box
ID: decim
Label: Decimation
Default Value: 64
Converter: Integer
Variable Static Text
ID: xlate_decim
Label: Xlate Decim
Default Value: 2**x...m_index
Converter: Float
Wav File Source
File: ...203Z_17906kHz_RF.wav
Repeat: Yes
Throttle
Sample Rate: 1M
Float To Complex
Multiply Const
Constant: 1k
Variable
ID: decim
Value: 64
Variable
ID: xlate_decim
Value: 25
Variable
ID: baseband_rate
Value: 40k
Variable
ID: re_over
Value: 5
Variable
ID: pre_baseband_rate
Value: 40k
Frequency Xlating FIR Filter
Decimation: 25
Taps: firdes.low_pass(1, s...
Center Frequency: 0
Sample Rate: 1M
Variable
ID: re_pre_baseband_rate
Value: 320k
Variable
ID: re_pre_baseband_rate
Value: 40k
Rational Resampler
Decimation: 40k
Interpolation: 320k
Taps:
Fractional BW: 0
Virtual Sink
Stream ID: re_bb
Polyphase Resampler
Resample Rate:
Taps:
Size (# phases): 32
Complex to Mag
Vec Length: 458.752k
FFT
FFT Size: 458.752k
Forward/Reverse: Forward
Window:
Stream to Vector
Num Items: 458.752k
Null Sink
Vec Length: 458.752k
File Sink
File: /mnt/Krump/mpsk_fft.dat
Vec Length: 458.752k
Variable
ID: fft_size
Value: 458.752k
Virtual Source
Stream ID: cyclo_input
Multiply Const
Constant: 1
Variable Delay
Delay: 1
Complex Conjugate
Multiply
Rational Resampler
Decimation: 1
Interpolation: 1
Taps:
Fractional BW: 0
Variable
ID: baud_decim
Value: 1
Complex to Mag
Variable Slider
ID: exponent
Label: Exponent
Default Value: 2
Minimum: 0
Maximum: 100
Converter: Integer
Notebook: main_notebook, 3
Variable Slider
ID: D
Label: Nominal ... per symbol
Default Value: 2
Minimum: 1
Maximum: 64
Converter: Integer
Notebook: main_notebook, 4
Virtual Source
Stream ID: bb
Complex To Float
Quadrature Demod
Gain: 1
Multiply Const
Constant: 100
Complex to Mag
Virtual Sink
Stream ID: quad
Variable
ID: pow_decim
Value: 1
Virtual Source
Stream ID: bb
Power
Exponent: 2
Multiply Const
Constant: 1
Variable Slider
ID: pow_div
Label: Div
Default Value: 0
Minimum: 0
Maximum: 100
Converter: Integer
Notebook: main_notebook, 3
Rational Resampler
Decimation: 1
Interpolation: 1
Taps:
Fractional BW: 0
Virtual Source
Stream ID: bb
Differential Phasor
AGC
Rate: 100u
Reference: 1
Gain: 1
Max Gain: 0
Feed Forward AGC
Num Samples: 1.024k
Reference: 1
AGC2
Attack Rate: 100m
Decay Rate: 10m
Reference: 1
Gain: 1
Max Gain: 0
AM Demod
Channel Rate: 40k
Audio Decimation: 2
Audio Pass: 4.5k
Audio Stop: 5k
Rational Resampler
Decimation: 50
Interpolation: 48
Taps:
Fractional BW: 0
Wav File Sink
File: /mnt/Dagron/sat-am.wav
Sample Rate: 48k
Bits per Sample: 16
Audio Sink
Sample Rate: 48KHz
Scope Sink
Title: Scope Plot
Sample Rate: 48k
Notebook: main_notebook, 9
FFT Sink
Title: FFT Plot
Sample Rate: 48k
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
Notebook: main_notebook, 9
FFT Sink
Title:
Sample Rate: 40k
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: 66.7m
Notebook: main_notebook, 0
Waterfall Sink
Title:
Sample Rate: 40k
Baseband Freq: 0
Dynamic Range: 100
Reference Level: 50
Ref Scale (p2p): 2
FFT Size: 1.024k
FFT Rate: 25
Window Size: 640, 520
Notebook: main_notebook, 9
Scope Sink
Title: Scope Plot
Sample Rate: 40k
V Scale: 10
T Scale: 1m
Notebook: main_notebook, 1
Fast AutoCorrelation Sink
Title: Fast AutoCorrelation
Sample Rate: 40k
Baseband Freq: 0
Size: 32.768k
Rate: 15
Y per Div: 10 dB
Ref Level (dB): 50
Notebook: main_notebook, 5
Scope Sink
Title: Scope Plot
Sample Rate: 40k
XY Mode: On
Window Size: 500, 500
Notebook: main_notebook, 11
FFT Sink
Title: Baud
Sample Rate: 40k
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: 50m
Notebook: main_notebook, 4
FFT Sink
Title: Pow
Sample Rate: 40k
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: 66.7m
Notebook: main_notebook, 3
Variable Slider
ID: quad_demod_gain
Label: Quadrature Demod Gain
Default Value: 100
Minimum: 1
Maximum: 1k
Converter: Integer
Notebook: main_notebook, 1
Probe MPSK SNR
Type: SNR
Alpha: 1
Probe Rate: 10
Scope Sink
Title: Scope Plot
Sample Rate: 4k
Notebook: main_notebook, 6
Number Sink
Title: Number Plot
Units: Units
Sample Rate: 1M
Min Value: -100
Max Value: 100
Factor: 1
Decimal Places: 10
Reference Level: 0
Number Rate: 15
Show Gauge: Show
Notebook: main_notebook, 6
Virtual Source
Stream ID: bb
Virtual Sink
Stream ID: cyclo_input
Virtual Source
Stream ID: re_bb
Complex to Arg
Quadrature Demod
Gain: 2
Differential Phasor
PLL Carrier Tracking
Alpha: 100m
Beta: 100m
Max Freq: 500m
Min Freq: 100m
Root Raised Cosine Filter
Decimation: 1
Gain: 1
Sample Rate: 40k
Symbol Rate: 64k
Alpha: 350m
Num Taps: 2
Root Raised Cosine Filter
Decimation: 1
Gain: 1
Sample Rate: 40k
Symbol Rate: 19.2k
Alpha: 350m
Num Taps: 486
File Sink
File: ...ump/beacon-arg.cfile
Variable
ID: test_decim
Value: 20
Rational Resampler
Decimation: 20
Interpolation: 1
Taps:
Fractional BW: 0
Hilbert
Num Taps: 64
Phase Mod
Sensitivity: 1
Frequency Mod
Sensitivity: 1
Scope Sink
Title: Arg
Sample Rate: 40k
Notebook: main_notebook, 7
Virtual Sink
Stream ID: cyclo_input
Waterfall Sink
Title:
Sample Rate: 2k
Baseband Freq: 0
Dynamic Range: 100
Reference Level: 50
Ref Scale (p2p): 2
FFT Size: 256
FFT Rate: 25
Notebook: main_notebook, 7
FFT Sink
Title:
Sample Rate: 40k
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: 66.7m
Notebook: main_notebook, 7
Scope Sink
Title: Scope Plot
Sample Rate: 40k
V Scale: 200
T Scale: 200u
Notebook: main_notebook, 1
Scope Sink
Title: Scope Plot
Sample Rate: 40k
V Scale: 10
T Scale: 1m
Notebook: main_notebook, 6
Waterfall Sink
Title:
Sample Rate: 40k
Baseband Freq: 0
Dynamic Range: 100
Reference Level: 50
Ref Scale (p2p): 2
FFT Size: 512
FFT Rate: 15
Notebook: main_notebook, 7
Virtual Source
Stream ID: bb
Virtual Source
Stream ID: re_bb
Root Raised Cosine Filter
Decimation: 1
Gain: 1
Sample Rate: 40k
Symbol Rate: 64k
Alpha: 350m
Num Taps: 2
Constellation Sink
Title: Constellation (M=4)
Sample Rate: 40k
Frame Rate: 15
Constellation Size: 2.048k
M: 4
Theta: 0
Alpha: 10m
Max Freq: 60m
Mu: 500m
Gain Mu: 20m
Symbol Rate: 64k
Omega Limit: 5m
Notebook: main_notebook, 2
Virtual Source
Stream ID: quad
Variable Delay
Delay: 1
Variable
ID: quad_decim
Value: 1
Multiply
Rational Resampler
Decimation: 1
Interpolation: 1
Taps:
Fractional BW: 0
Variable Slider
ID: eye_samp_per_sym
Label: Samples per symbol
Default Value: 20
Minimum: 1
Maximum: 100
Converter: Integer
Notebook: main_notebook, 2
Variable Slider
ID: eye_num_plots
Label: Num plots
Default Value: 100
Minimum: 1
Maximum: 100
Converter: Integer
Notebook: main_notebook, 2
Eye Diagram
Title: Eye Diagram
Sample Rate: 40k
Samples per symbol: e...r_sym
Num plots: eye_num_plots
Symbol decimation: 20
Notebook: main_notebook, 2
Scope Sink
Title: Arg
Sample Rate: 40k
V Scale: 1
T Scale: 1m
Notebook: main_notebook, 7
Sample Rate: 40k
Notebook: main_notebook, 7
FFT Sink
Title: FFT Plot
Sample Rate: 2k
Baseband Freq: 0
Y per Div: 10 dB
Y Divs: 10
Ref Level (dB): 50
Ref Scale (p2p): 2
FFT Size: 2.048k
Refresh Rate: 30
Average Alpha: 66.7m
Notebook: main_notebook, 7
Fast AutoCorrelation Sink
Title: Fast AutoCorrelation
Sample Rate: 40k
Baseband Freq: 0
Size: 65.536k
Rate: 15
Y per Div: 10 dB
Ref Level (dB): 50
Notebook: main_notebook, 8
Variable Slider
ID: sym_rate_fine
Label: Symbol rate (fine)
Default Value: 0
Minimum: -500
Maximum: 500
Converter: Integer
Notebook: main_notebook, 2
Variable Slider
ID: sym_rate
Label: Symbol rate
Default Value: 30.8k
Minimum: 1k
Maximum: 91.5k
Converter: Integer
Notebook: main_notebook, 2
Variable Slider
ID: sym_rate_coarse
Label: Symbol rate (coarse)
Default Value: 0
Minimum: -5k
Maximum: 5k
Converter: Integer
Notebook: main_notebook, 2
Parameter
ID: sym_rate
Label: Symbol rate
Value: sym_rate_slider
Type: Int
Variable Text Box
ID: sym_rate_base
Label: Symbol rate
Default Value: 64k
Converter: Integer
Notebook: main_notebook, 2
Variable
ID: samp_per_sym
Value: 2
Variable
ID: sym_rate
Value: 64k
Variable Static Text
ID: sym_rate
Label: Symbol rate
Default Value: 64k
Converter: Integer
FFT Sink
Title: Baud
Sample Rate: 40k
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: 50m
Notebook: main_notebook, 8
Variable Slider
ID: Dquad
Label: Delay
Default Value: 1
Minimum: 1
Maximum: 256
Converter: Integer
Notebook: main_notebook, 8


Options
ID: sat
UDP Source
IP Address: 0.0.0.0
Port: 1.234k
Payload Size: 16.384k
BorIP: On
Vec Length: 2
Variable
ID: adc_rate
Value: 64M
Variable
ID: samp_rate
Value: 1M
XMLRPC Server
Address: 0.0.0.0
Port: 8.08k
Notebook
ID: main_notebook
Tab Orientation: Top
Labels: BB, Dem...C, PSK, FAC
Variable Slider
ID: xlate_offset_fine
Label: Fine Offset
Default Value: 0
Minimum: -10k
Maximum: 10k
Converter: Float
Variable Config
ID: config_xlate_offset
Default Value: 0
Type: Float
Config File: .grc_sat_source
Section: main
Option: xlate_offset
WriteBack: 0
Variable Config
ID: config_xlate_bandwidth
Default Value: 24k
Type: Float
Config File: .grc_sat_source
Section: main
Option: xlate_bandwidth
WriteBack: 24k
Variable Slider
ID: xlate_bandwidth
Label: Xlate BW
Default Value: 24k
Minimum: 5k
Maximum: 500k
Converter: Float
Variable Static Text
ID: pre_baseband_rate
Label: BB Rate
Default Value: 200k
Converter: Float
Notebook: main_notebook, 0
Variable Text Box
ID: xlate_offset
Label: Xlate Offset
Default Value: 0
Converter: Float
Vector to Stream
Num Items: 2
IShort To Complex
Wav File Source
File: ...726Z_16653kHz_RF.wav
Repeat: Yes
Multiply Const
Constant: 1k
Float To Complex
Throttle
Sample Rate: 1M
File Source
File: ...beacon-hilbert.cfile
Repeat: No
Frequency Xlating FIR Filter
Decimation: 5
Taps: firdes.low_pass(1, s...
Center Frequency: 0
Sample Rate: 1M
Rational Resampler
Decimation: 200k
Interpolation: 24k
Taps:
Fractional BW: 0
Virtual Source
Stream ID: filt_bb
MPSK Receiver
M: 2
Theta: 0
Alpha: 50m
Beta: 625u
Min Freq: -10m
Max Freq: 10m
Mu: 500m
Gain Mu: 20m
Omega: 10
Gain Omega: 100u
Omega Relative Limit: 5m
MPSK Receiver (Debug)
M: 8
Theta: 0
Alpha: 50m
Beta: 625u
Min Freq: -10m
Max Freq: 10m
Mu: 500m
Gain Mu: 20m
Omega: 10
Gain Omega: 100u
Omega Relative Limit: 10m
out
freq
phase
phase_error
mu
omega
mm_error
sync
Freq Alpha: 10m
Phase Alpha: 100m
Timing Alpha: 100m
Scope Sink
Title: MPSK Freq
Sample Rate: 2.4k
V Scale: 2m
T Scale: 50m
Notebook: main_notebook, 6
Differential Phasor
Complex to Imag
Single Pole IIR Filter
Alpha: 1
Scope Sink
Title: Scope Plot
Sample Rate: 100k
V Scale: 500m
T Scale: 10m
Notebook: main_notebook, 2
File Sink
File: ...96637kHz_RF-sync.dat
Variable
ID: decim
Value: 64
Variable
ID: xlate_decim
Value: 5
Variable
ID: baseband_rate
Value: 24k
Variable
ID: over_samp
Value: 10
Variable
ID: sym_rate
Value: 2.4k
File Sink
File: /mnt/Krumpf/mpsk_bb.dat
Feed Forward AGC
Num Samples: 16
Reference: 1
AGC
Rate: 100u
Reference: 1
Gain: 1
Max Gain: 0
AGC2
Attack Rate: 60m
Decay Rate: 1m
Reference: 1
Gain: 1
Max Gain: 100
Virtual Sink
Stream ID: re_bb
Root Raised Cosine Filter
Decimation: 1
Gain: 1
Sample Rate: 24k
Symbol Rate: 2.4k
Alpha: 350m
Num Taps: 112
Virtual Sink
Stream ID: filt_bb
Variable Slider
ID: mpsk_alpha
Variable Slider
ID: mpsk_gain_mu
Label: Gain Mu
Default Value: 20m
Minimum: 1m
Maximum: 500m
Converter: Float
Notebook: main_notebook, 1
Scope Sink
Title: MPSK (M=8)
Sample Rate: 2.4k
V Scale: 500m
T Scale: 5
XY Mode: On
Notebook: main_notebook, 1
Costas Loop
Alpha: 10m
Beta: 25u
Max Freq: 10m
Min Freq: 60m
Order: 2
Clock Recovery MM
Omega: 10
Gain Omega: 2.5m
Mu: 500m
Gain Mu: 500m
Omega Relative Limit: 5m
Scope Sink
Title: Scope Plot
Sample Rate: 24k
Notebook: main_notebook, 3
Scope Sink
Title: Scope Plot
Sample Rate: 24k
Notebook: main_notebook, 3
Scope Sink
Title: Scope Plot
Sample Rate: 2.4k
Notebook: main_notebook, 4
File Sink
File: .../Krumpf/mpsk_freq.dat
File Sink
File: ...Krumpf/mpsk_phase.dat
File Sink
File: ...mpsk_phase_error.dat
File Sink
File: /mnt/Krumpf/mpsk_mu.dat
File Sink
File: ...Krumpf/mpsk_omega.dat
File Sink
File: ...mp/mpsk_mm_error.dat
Null Sink
Virtual Source
Stream ID: re_bb
Differential Phasor
Threshold
Low: 0
High: 0
Initial State: 0
DPSK Demod
Type: DBPSK
Samples/Symbol: 10
Excess BW: 350m
Costas Alpha: 50m
Gain Mu: 20m
Mu: 500m
Omega Relative Limit: 5m
Gray Code: Yes
Verbose: On
Depuncture
Matrix: 1, 1
Variable Delay
Delay: 0
Swap
Swap: False
Differential Encoder
Modulus: 2
Any Block
Desc:
Maker: <gr_bloc...ked_bb (1)>
FFT Sink
Title: FFT Plot
Sample Rate: 200k
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: 25
Average Alpha: 250m
Notebook: main_notebook, 0
Waterfall Sink
Title: Waterfall Plot
Sample Rate: 24k
Baseband Freq: 0
Dynamic Range: 100
Reference Level: 50
Ref Scale (p2p): 2
FFT Size: 512
FFT Rate: 25
Notebook: main_notebook, 0
Scope Sink
Title: Scope Plot
Sample Rate: 24k
V Scale: 10
T Scale: 1m
Notebook: main_notebook, 2
Complex To Float
Quadrature Demod
Gain: 100
Complex to Arg
Complex to Mag
Complex to Real
Quadrature Demod
Gain: 1
File Sink
File: .../Krumpf/mpsk_real.dat
Complex to Real
Multiply Const
Constant: 1
Variable Delay
Delay: 0
Fast AutoCorrelation Sink
Title: Fast AutoCorrelation
Sample Rate: 24k
Baseband Freq: 0
Size: 131.072k
Rate: 10
Y per Div: 10 dB
Ref Level (dB): 50
Ref Scale (p2p): 2
Average Alpha: 200m
Notebook: main_notebook, 7
Constellation Sink
Title: Constellation Plot
Sample Rate: 24k
Frame Rate: 15
Constellation Size: 2.048k
M: 2
Theta: 0
Alpha: 5m
Max Freq: 60m
Mu: 500m
Gain Mu: 5m
Symbol Rate: 2.4k
Omega Limit: 5m
Notebook: main_notebook, 1
Scope Sink
Title: Scope Plot
Sample Rate: 24k
V Scale: 10
T Scale: 1m
Notebook: main_notebook, 1
Eye Diagram
Title: Eye Diagram
Sample Rate: 24k
Samples per symbol: 3
Num plots: 500
Symbol decimation: 50
V Scale: 1
Notebook: main_notebook, 3
Variable Slider
ID: eye_samp_per_sym
Label: Samples per symbol
Default Value: 3
Minimum: 1
Maximum: 100
Converter: Integer
Notebook: main_notebook, 3
Variable Check Box
ID: delay_viterbi
Variable Slider
ID: delay_puncture
Label: Puncture Delay
Default Value: 0
Minimum: 0
Maximum: 14
Converter: Integer
Notebook: main_notebook, 5
Variable Check Box
ID: invert
Label: Invert
Default Value: 1
True: -1
False: 1
Notebook: main_notebook, 5
Decode CCSDS 27
Add Const
Constant: -4.096k
Multiply Const
Constant: -1
Null Sink
Null Sink
Float To UChar
Scope Sink
Title: Error Rate
Sample Rate: 150
V Scale: 4.096k
V Offset: 15.872k
Notebook: main_notebook, 5
Keep 1 in N
N: 4
Threshold
Low: 11
High: 10
Initial State: 0
Variable
ID: accept_bytes
Value: 0
Variable Sink
Variable: accept_bytes
Decimation: 1
Import
Import: baz
Variable Slider
ID: sym_rate
Label: Symbol Rate
Default Value: 10k
Minimum: 300
Maximum: 20k
Converter: Integer
Simple Squelch
Threshold (dB): sq
Alpha: alpha
Scope Sink
Title: Scope Plot
Sample Rate: 24k
MPSK Sync
Alpha: 10m
Beta: 25u
Max Freq: 60m
Min Freq: 10m
Omega: 10
Gain Omega: 2.5
Mu: 500m
DD MPSK Sync
Alpha: 10m
Beta: 25u
Max Freq: 10m
Min Freq: 60m
Reference Phase: 0
Omega: 10
Gain Omega: 2.5m
Mu: 500m
Valve
Open: accept_bytes
Note
Note: These don't work
UChar To Float
Histo Sink
Title: Histogram Plot
Num Bins: 8
Frame Size: 16
Notebook: main_notebook, 2
Variable Check Box
ID: swap_viterbi
Label: Swap Viterbi
Default Value: False
True: True
False: False
Notebook: main_notebook, 5
Variable Chooser
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, 5
Packed to Unpacked
Bits per Chunk: 1
Endianness: MSB
Skip Head
Num Items: 4.8k
Differential Decoder
Modulus: 2
Head
Num Items: 72k
Any Block Sink
Desc:
Maker: <gr_bloc...t_char (2)>
Histo Sink
Title: Histogram Plot
Num Bins: 256
Frame Size: 256
Notebook: main_notebook, 4


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

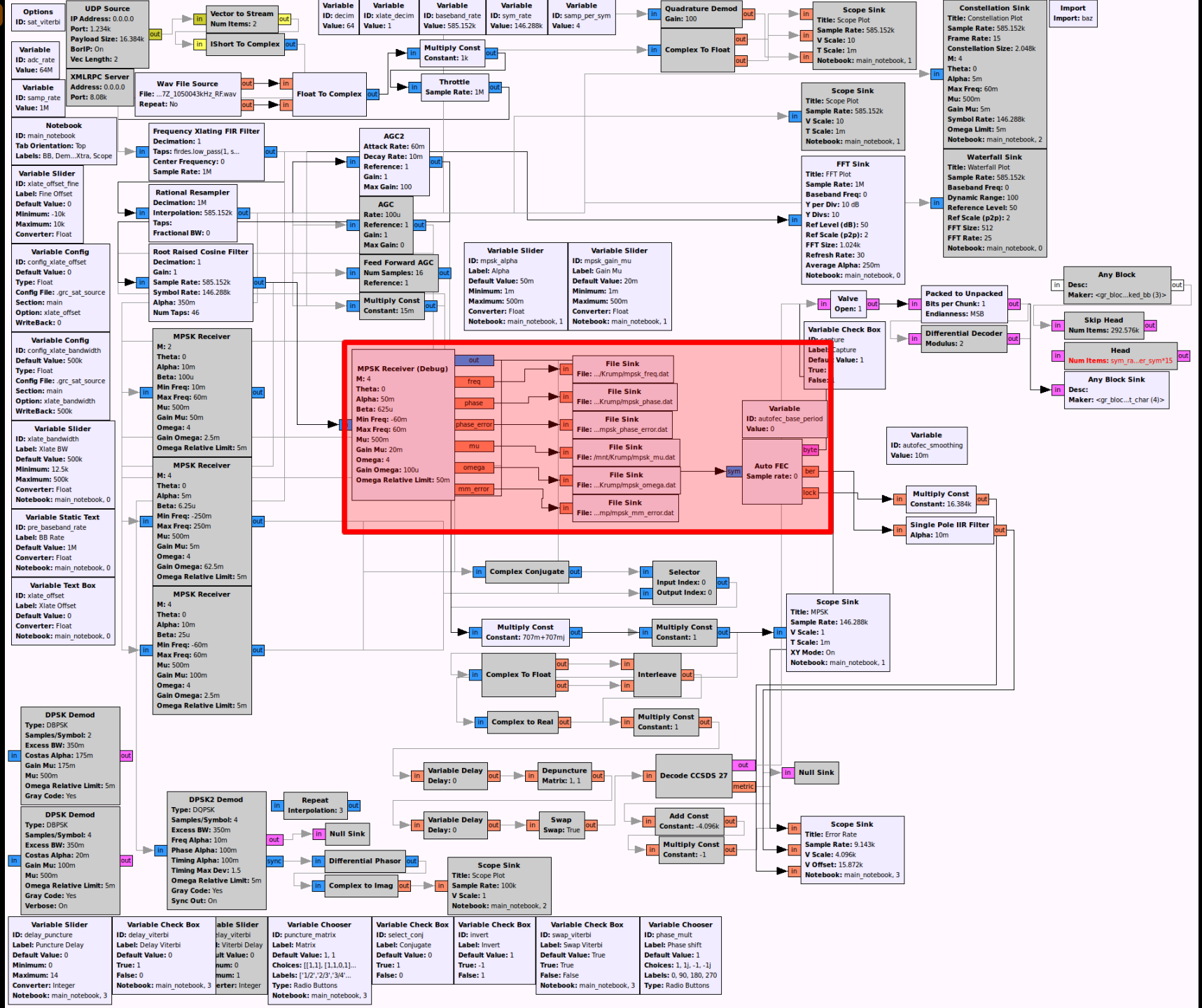

Auto FEC
Sample rate: 0
sym
byte
ber
lock

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
```

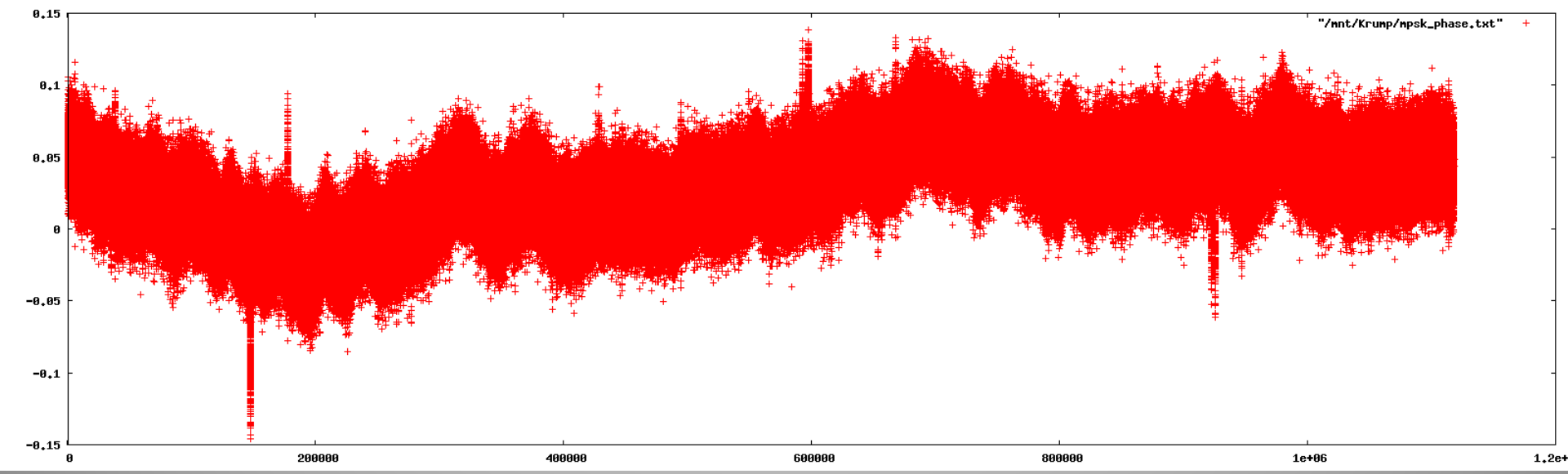

Options
ID: sat_viterbi
UDP Source
IP Address: 0.0.0.0
Port: 1.234k
Payload Size: 16.384k
BorIP: On
Vec Length: 2
Vector to Stream
Num Items: 2
IShort To Complex
Variable
ID: adc_rate
Value: 64M
XMLRPC Server
Address: 0.0.0.0
Port: 8.08k
Variable
ID: samp_rate
Value: 1M
Wav File Source
File: ...7Z_1050043kHz_RF.wav
Repeat: No
Float To Complex
Variable
ID: decim
Value: 64
Variable
ID: xlate_decim
Value: 1
Variable
ID: baseband_rate
Value: 585.152k
Variable
ID: sym_rate
Value: 146.288k
Variable
ID: samp_per_sym
Value: 4
Multiply Const
Constant: 1k
Throttle
Sample Rate: 1M
Quadrature Demod
Gain: 100
Complex To Float
Scope Sink
Title: Scope Plot
Sample Rate: 585.152k
V Scale: 10
T Scale: 1m
Notebook: main_notebook, 1
Constellation Sink
Title: Constellation Plot
Sample Rate: 585.152k
Frame Rate: 15
Constellation Size: 2.048k
M: 4
Theta: 0
Alpha: 5m
Max Freq: 60m
Mu: 500m
Gain Mu: 5m
Symbol Rate: 146.288k
Omega Limit: 5m
Notebook: main_notebook, 2
Import
Import: baz
Scope Sink
Title: Scope Plot
Sample Rate: 585.152k
V Scale: 10
T Scale: 1m
Notebook: main_notebook, 1
Waterfall Sink
Title: Waterfall Plot
Sample Rate: 585.152k
Baseband Freq: 0
Dynamic Range: 100
Reference Level: 50
Ref Scale (p2p): 2
FFT Size: 512
FFT Rate: 25
Notebook: main_notebook, 0
FFT Sink
Title: FFT Plot
Sample Rate: 1M
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
Notebook
ID: main_notebook
Tab Orientation: Top
Labels: BB, Dem...Xtra, Scope
Frequency Xlating FIR Filter
Decimation: 1
Taps: firdes.low_pass(1, s...
Center Frequency: 0
Sample Rate: 1M
AGC2
Attack Rate: 60m
Decay Rate: 10m
Reference: 1
Gain: 1
Max Gain: 100
Variable Slider
ID: xlate_offset_fine
Label: Fine Offset
Default Value: 0
Minimum: -10k
Maximum: 10k
Converter: Float
Rational Resampler
Decimation: 1M
Interpolation: 585.152k
Taps:
Fractional BW: 0
AGC
Rate: 100u
Reference: 1
Gain: 1
Max Gain: 0
Variable Slider
ID: mpsk_alpha
Label: Alpha
Default Value: 50m
Minimum: 1m
Maximum: 500m
Converter: Float
Notebook: main_notebook, 1
Variable Slider
ID: mpsk_gain_mu
Label: Gain Mu
Default Value: 20m
Minimum: 1m
Maximum: 500m
Converter: Float
Notebook: main_notebook, 1
Variable Config
ID: config_xlate_offset
Default Value: 0
Type: Float
Config File: .grc_sat_source
Section: main
Option: xlate_offset
WriteBack: 0
Root Raised Cosine Filter
Decimation: 1
Gain: 1
Sample Rate: 585.152k
Symbol Rate: 146.288k
Alpha: 350m
Num Taps: 46
Feed Forward AGC
Num Samples: 16
Reference: 1
Multiply Const
Constant: 15m
Valve
Open: 1
Packed to Unpacked
Bits per Chunk: 1
Endianness: MSB
Differential Decoder
Modulus: 2
Variable Check Box
ID: capture
Label: Capture
Default Value: 1
True:
False:
Any Block
Desc:
Maker: <gr_bloc...ked_bb (3)>
Skip Head
Num Items: 292.576k
Head
Num Items: sym_ra...er_sym*15
Any Block Sink
Desc:
Maker: <gr_bloc...t_char (4)>
Variable Config
ID: config_xlate_bandwidth
Default Value: 500k
Type: Float
Config File: .grc_sat_source
Section: main
Option: xlate_bandwidth
WriteBack: 500k
MPSK Receiver
M: 2
Theta: 0
Alpha: 10m
Beta: 100u
Min Freq: 10m
Max Freq: 60m
Mu: 500m
Gain Mu: 50m
Omega: 4
Gain Omega: 2.5m
Omega Relative Limit: 5m
MPSK Receiver (Debug)
M: 4
Theta: 0
Alpha: 50m
Beta: 625u
Min Freq: -60m
Max Freq: 60m
Mu: 500m
Gain Mu: 20m
Omega: 4
Gain Omega: 100u
Omega Relative Limit: 50m
out
freq
phase
phase_error
mu
omega
mm_error
File Sink
File: .../Krump/mpsk_freq.dat
File Sink
File: ...Krump/mpsk_phase.dat
File Sink
File: ...mpsk_phase_error.dat
File Sink
File: /mnt/Krump/mpsk_mu.dat
File Sink
File: ...Krump/mpsk_omega.dat
File Sink
File: ...mp/mpsk_mm_error.dat
Variable
ID: autofec_base_period
Value: 0
Auto FEC
Sample rate: 0
sym
byte
ber
lock
Variable
ID: autofec_smoothing
Value: 10m
Variable Slider
ID: xlate_bandwidth
Label: Xlate BW
Default Value: 500k
Minimum: 12.5k
Maximum: 500k
Converter: Float
Notebook: main_notebook, 0
MPSK Receiver
M: 4
Theta: 0
Alpha: 5m
Beta: 6.25u
Min Freq: -250m
Max Freq: 250m
Mu: 500m
Gain Mu: 5m
Omega: 4
Gain Omega: 62.5m
Omega Relative Limit: 5m
Multiply Const
Constant: 16.384k
Single Pole IIR Filter
Alpha: 10m
Variable Static Text
ID: pre_baseband_rate
Label: BB Rate
Default Value: 1M
Converter: Float
Notebook: main_notebook, 0
MPSK Receiver
M: 4
Theta: 0
Alpha: 10m
Beta: 25u
Min Freq: -60m
Max Freq: 60m
Mu: 500m
Gain Mu: 100m
Omega: 4
Gain Omega: 2.5m
Omega Relative Limit: 5m
Complex Conjugate
Selector
Input Index: 0
Output Index: 0
Variable Text Box
ID: xlate_offset
Label: Xlate Offset
Default Value: 0
Converter: Float
Notebook: main_notebook, 0
Multiply Const
Constant: 707m+707mj
Multiply Const
Constant: 1
Scope Sink
Title: MPSK
Sample Rate: 146.288k
V Scale: 1
T Scale: 1m
XY Mode: On
Notebook: main_notebook, 1
Complex To Float
Interleave
Complex to Real
Multiply Const
Constant: 1
DPSK Demod
Type: DBPSK
Samples/Symbol: 2
Excess BW: 350m
Costas Alpha: 175m
Gain Mu: 175m
Mu: 500m
Omega Relative Limit: 5m
Gray Code: Yes
Variable Delay
Delay: 0
Depuncture
Matrix: 1, 1
Decode CCSDS 27
Null Sink
DPSK Demod
Type: DBPSK
Samples/Symbol: 4
Excess BW: 350m
Costas Alpha: 20m
Gain Mu: 100m
Mu: 500m
Omega Relative Limit: 5m
Gray Code: Yes
Verbose: On
DPSK2 Demod
Type: DQPSK
Samples/Symbol: 4
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
Repeat
Interpolation: 3
Null Sink
Differential Phasor
Complex to Imag
Variable Delay
Delay: 0
Swap
Swap: True
Add Const
Constant: -4.096k
Multiply Const
Constant: -1
Scope Sink
Title: Error Rate
Sample Rate: 9.143k
V Scale: 4.096k
V Offset: 15.872k
Notebook: main_notebook, 3
Scope Sink
Title: Scope Plot
Sample Rate: 100k
V Scale: 1
Notebook: main_notebook, 2
Variable Slider
ID: delay_puncture
Label: Puncture Delay
Default Value: 0
Minimum: 0
Maximum: 14
Converter: Integer
Notebook: main_notebook, 3
Variable Check Box
ID: delay_viterbi
Label: Delay Viterbi
Default Value: 0
True: 1
False: 0
Notebook: main_notebook, 3
Variable Chooser
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, 3
Variable Check Box
ID: select_conj
Label: Conjugate
Default Value: 0
True: 1
False: 0
Variable Check Box
ID: invert
Label: Invert
Default Value: 1
True: -1
False: 1
Variable Check Box
ID: swap_viterbi
Label: Swap Viterbi
Default Value: True
True: True
False: False
Notebook: main_notebook, 3
Variable Chooser
ID: phase_mult
Label: Phase shift
Default Value: 1
Choices: 1, 1j, -1, -1j
Labels: 0, 90, 180, 270
Type: Radio Buttons

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

QPSK Phase Debug

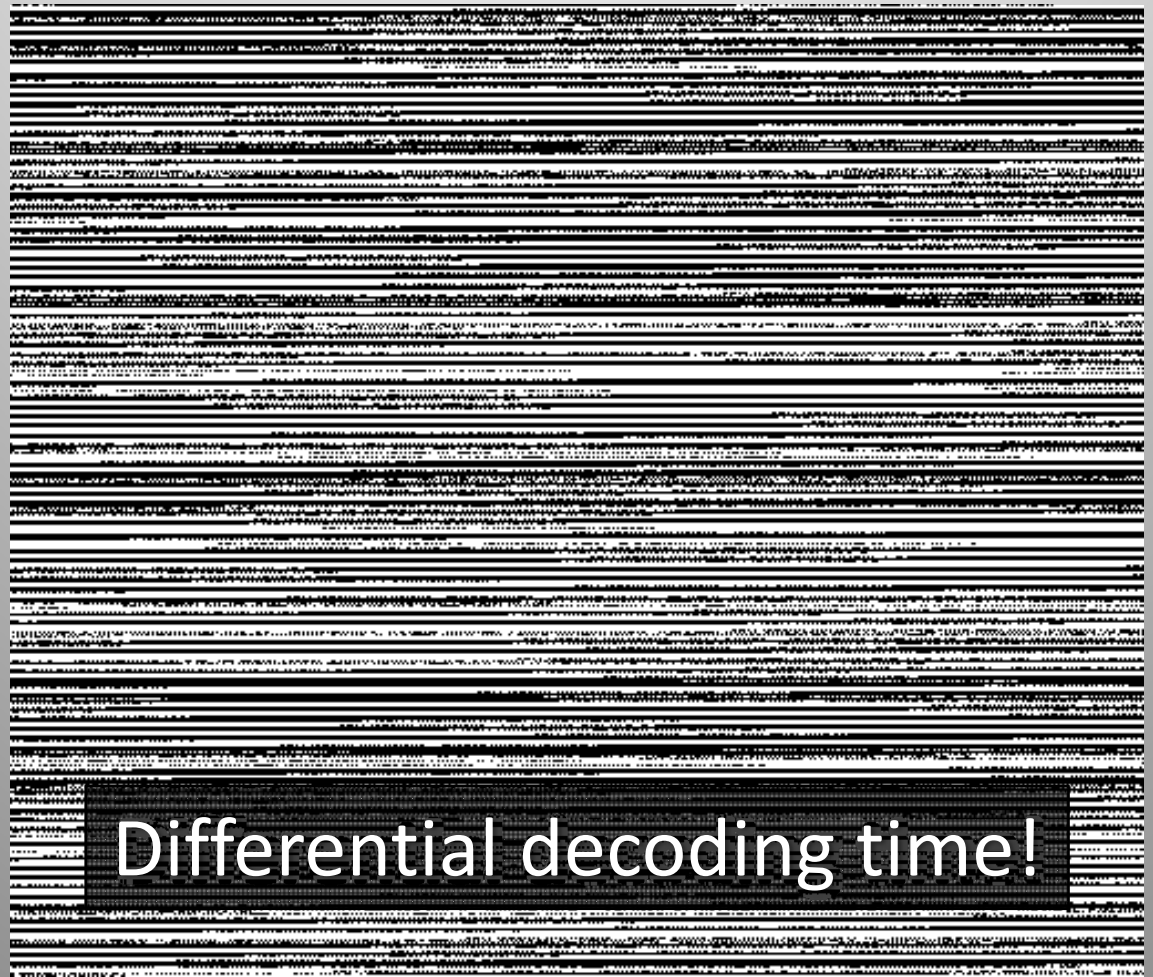


Visualisation

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

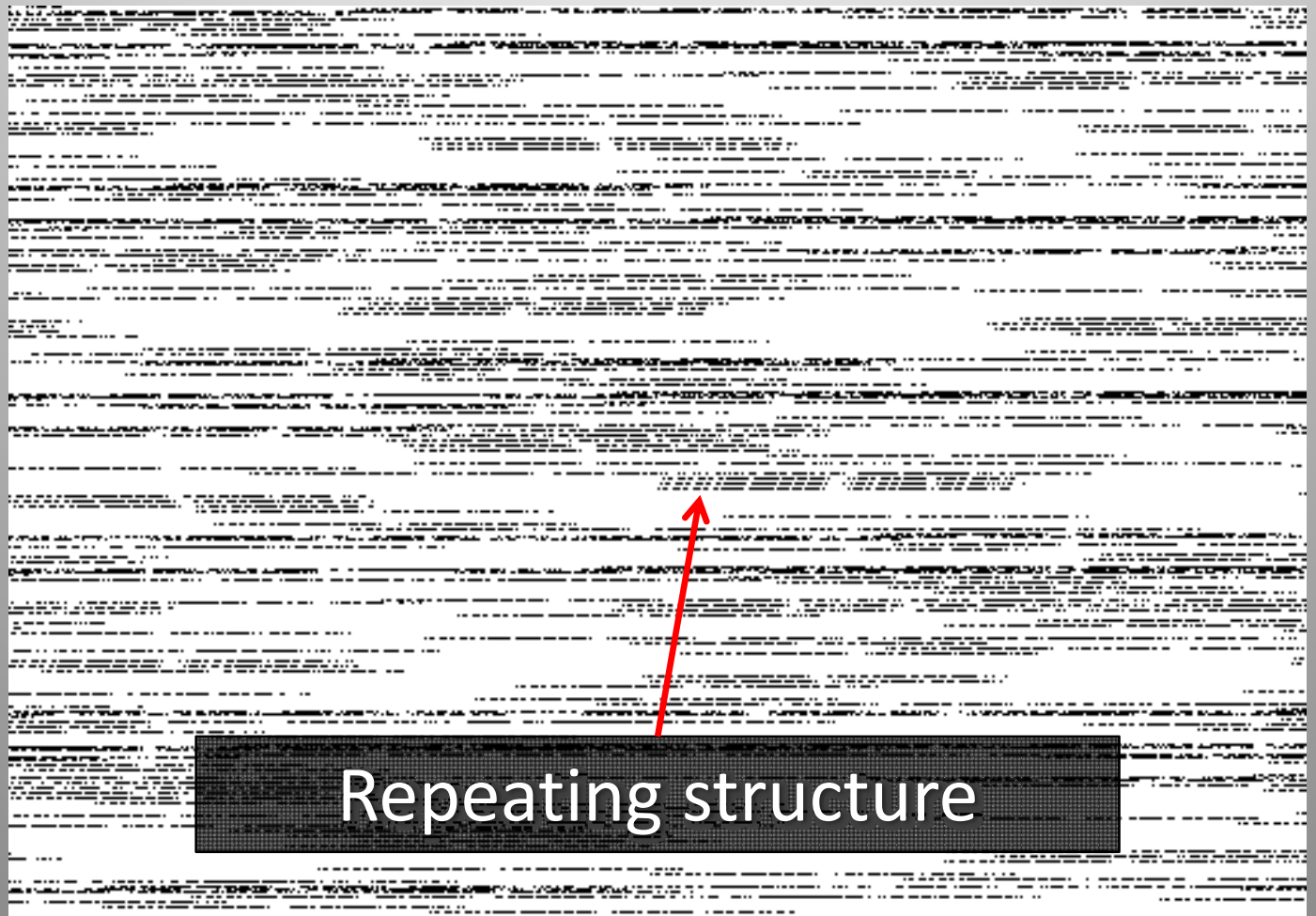
De-scrambled

- 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]: 00000001100100011101001100001100001010000000 (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]: 00000001100010011101001100001100001010000000 (430cb9180)
42 bits #0000-0004[+0002, /0000]: 00000011000001100001000101111010101011111111 (3f55e8860c0)

41 bits #0002-0002[+0000, /0000]: 00000001000011001001110000100111110000000000 (3e4393080)
41 bits #0003-0003[+0000, /0000]: 00000001000101001001110000001111111000000000 (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]: 00000010000111010000000011110101110000001 (81b780b840)
40 bits #0000-0003[+0001, /0000]: 00000011000100111010011000011000001000000 (21865c8c0)
40 bits #0001-0004[+0000, /0000]: 00000001000011101000000010001011101111111 (fdd1017080)
40 bits #0001-0004[+0000, /0000]: 00000001000011101000000011111011011000000 (36f017080)
40 bits #0001-0005[+0000, /0000]: 00000001000011101000000010100000010101111 (f505017080)
40 bits #0006-0006[+0000, /0000]: 00000001000001000010000001011111110000000 (1fa042080)

39 bits #0002-0002[+0000, /0000]: 11111010010111001111010000100011000000 (c42f3a5f)
39 bits #0002-0002[+0000, /0000]: 00100000011111110100101110000101111111 (7f43a5fc04)
39 bits #0002-0002[+0000, /0000]: 00000001010101010010001101000111000001 (41e2c4aa80)
39 bits #0002-0002[+0000, /0000]: 01110100101110011010000001000110000010 (2062059d2e)
39 bits #0002-0002[+0000, /0000]: 01111101001011100111010000100011000000 (1885e74be)
39 bits #0002-0002[+0000, /0000]: 01011010010111000110000000100011000000 (c4063a5a)
39 bits #0000-0003[+0001, /0000]: 00000010001010010011100000011111000000 (1f81c9440)
39 bits #0000-0004[+0001, /0000]: 00000010000111010000000100010111011111 (7ee880b
39 bits #0000-0004[+0001, /0000]: 00000010000111010000000111101101100000 (1b780b8
39 bits #0000-0005[+0002, /0000]: 00000010000111010000000101000001010111 (7a8280b
39 bits #0000-0006[+0004, /0000]: 00000010000010000100000010111111110000 (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)
```

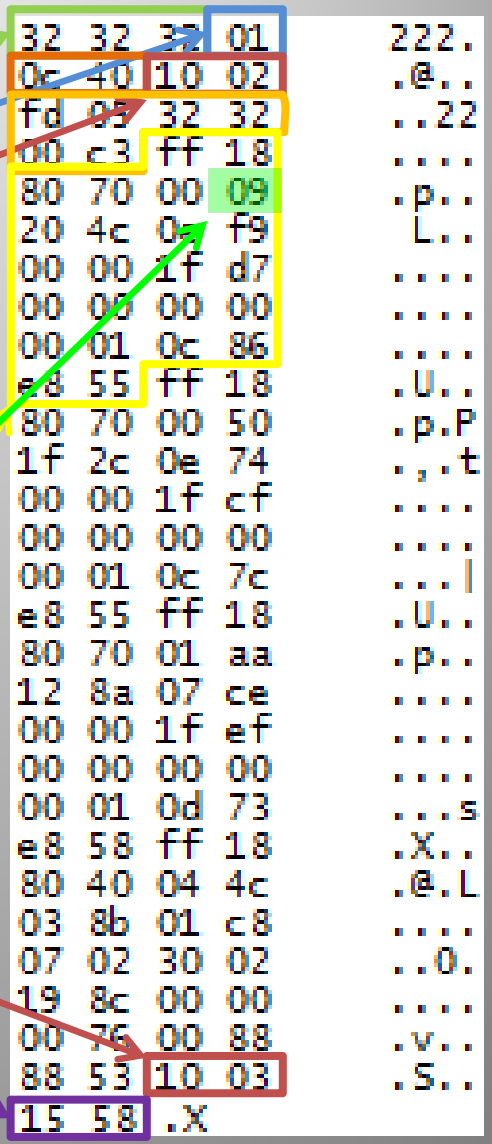
- Search for repeating strings of bits
- Try to find frame header
- Clue: sudden increase in # of occurrences

```
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)
```

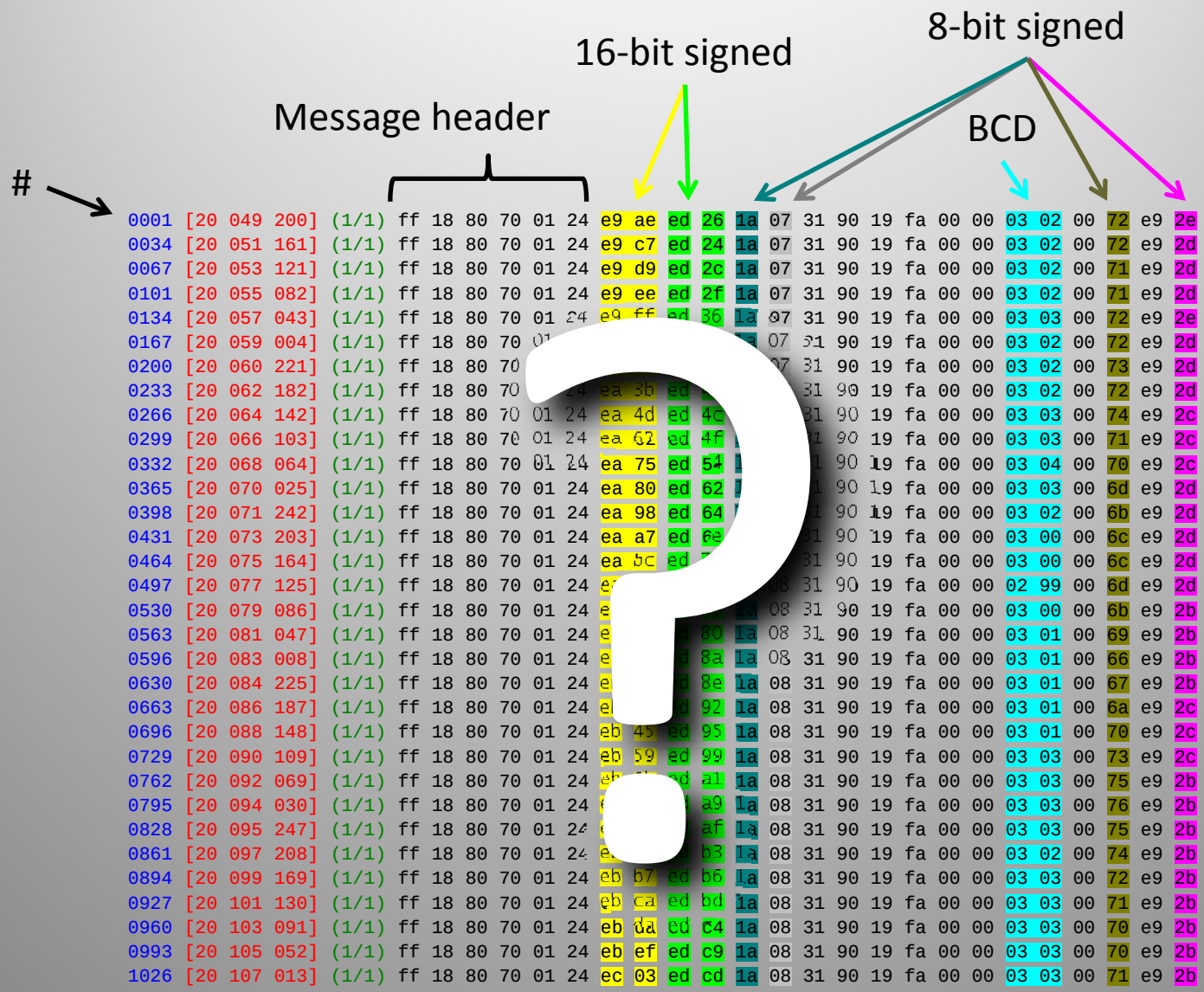
Preceding 1s are just part of ‘idle’ stream when no data is being sent

Frame analysis

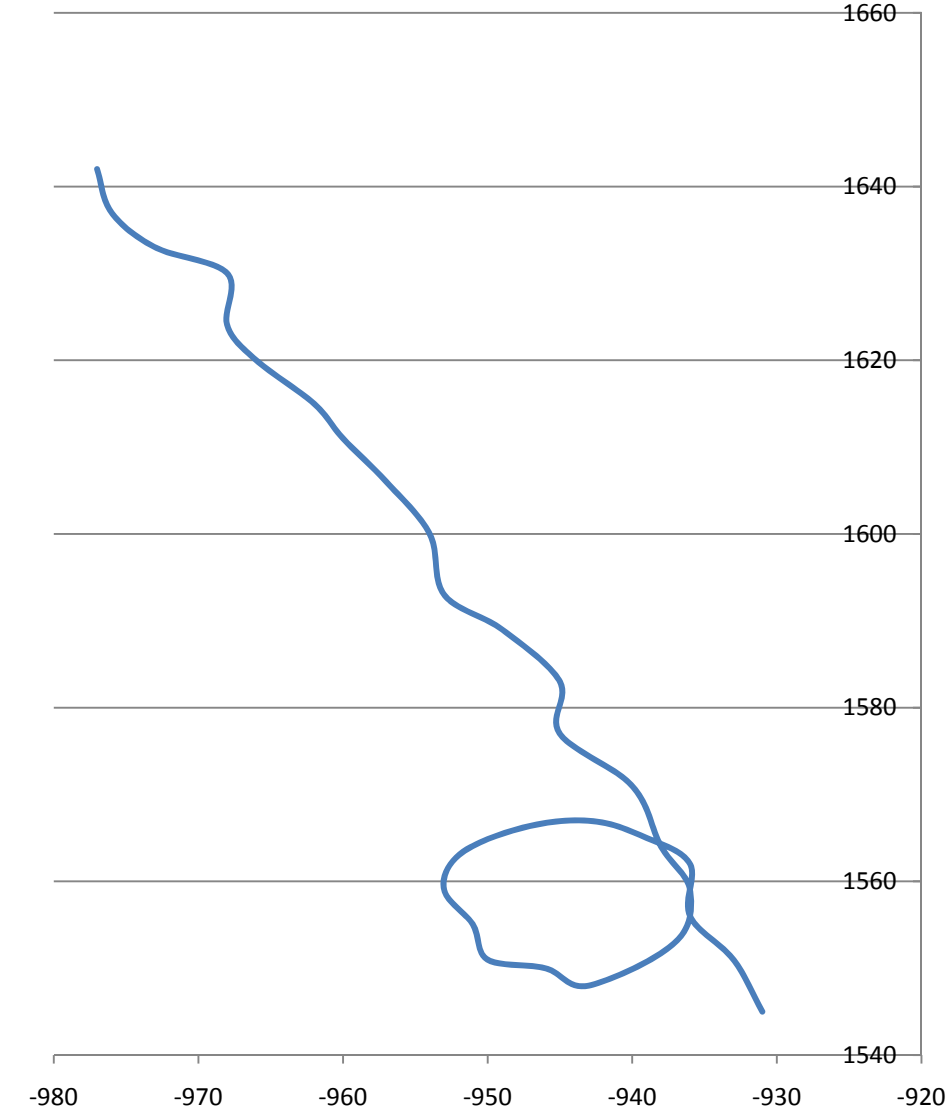
- Header
  - SYN SYN SYN (EBCDIC)
- Character-oriented encoding:
  - SOH
  - STX
  - ETX
  - CRC (CCITT-16)
- Numbers of fixed-length messages
  - Each contains an ID

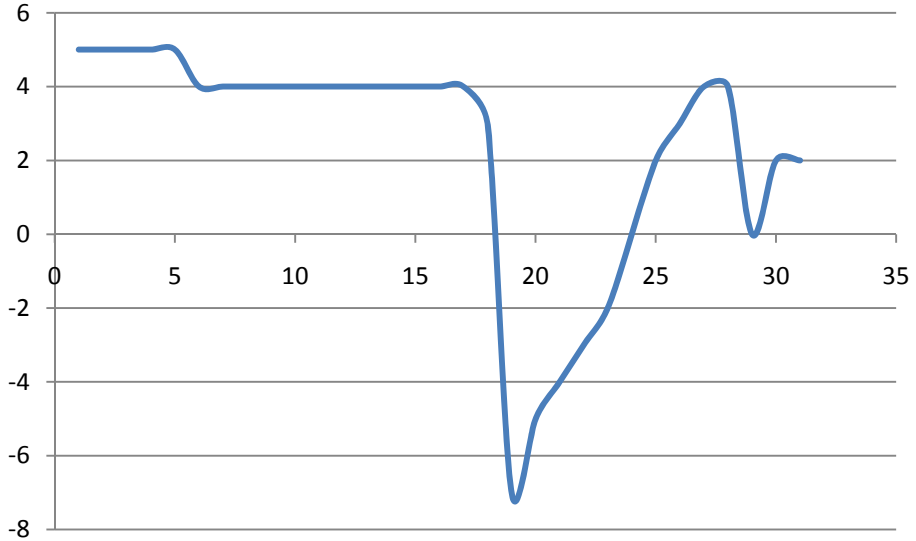


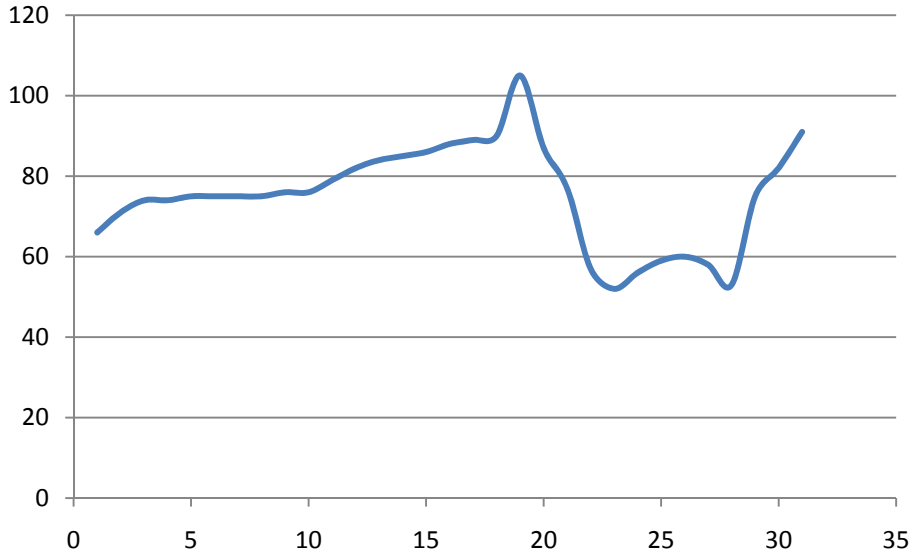
Un-pack & find patterns



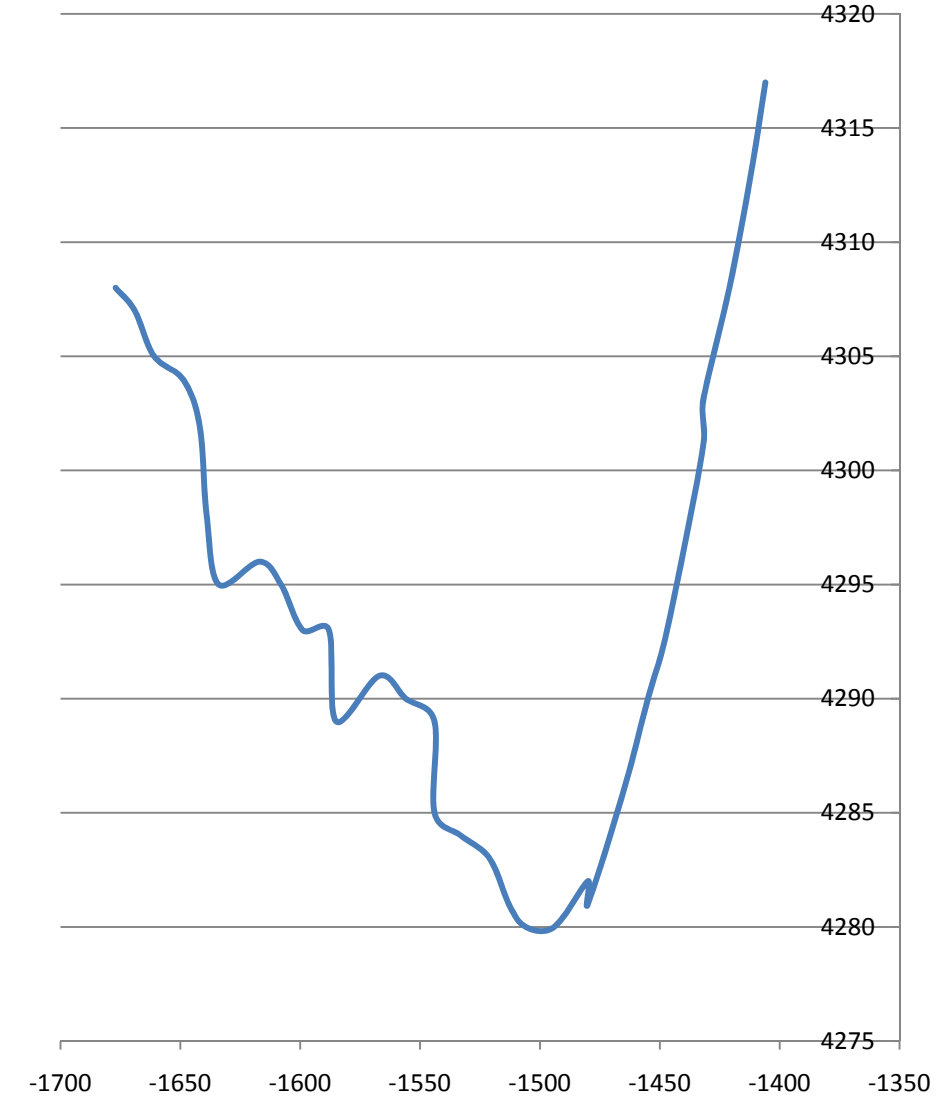
Graphing the Data

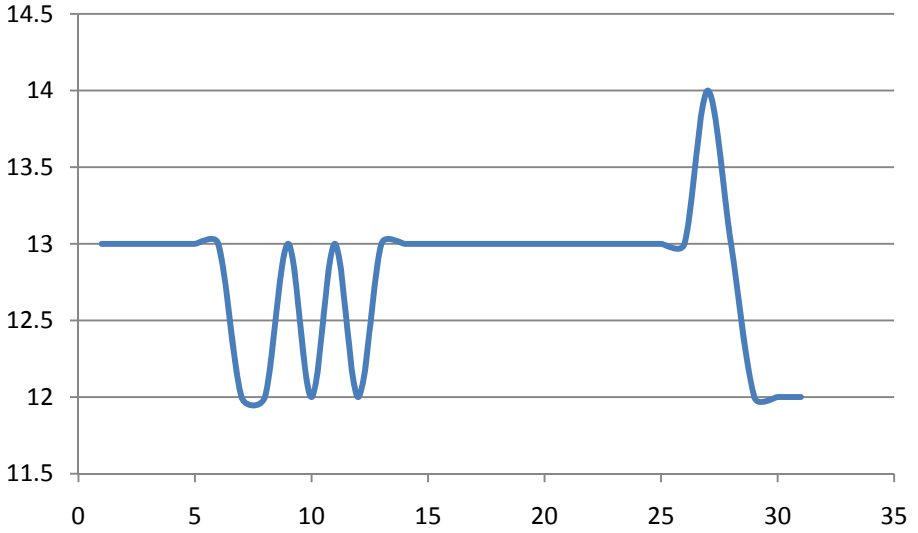


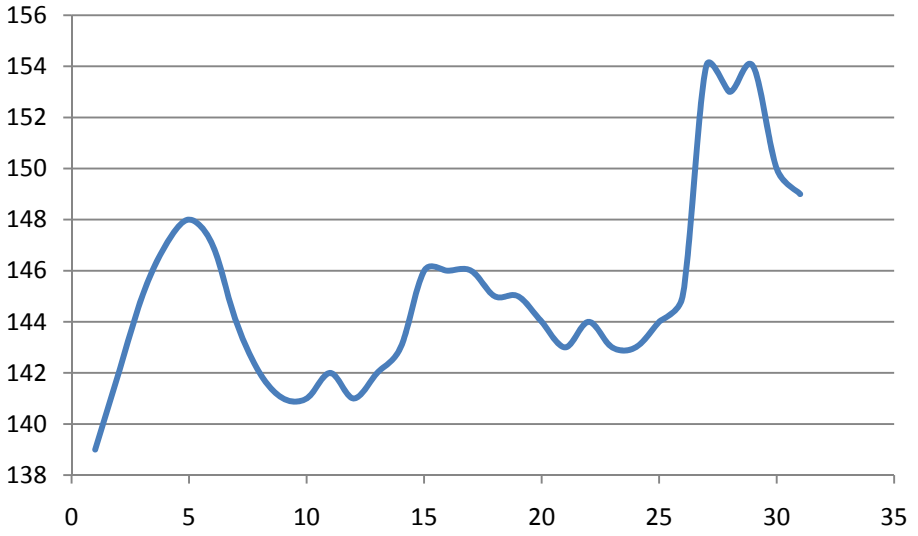


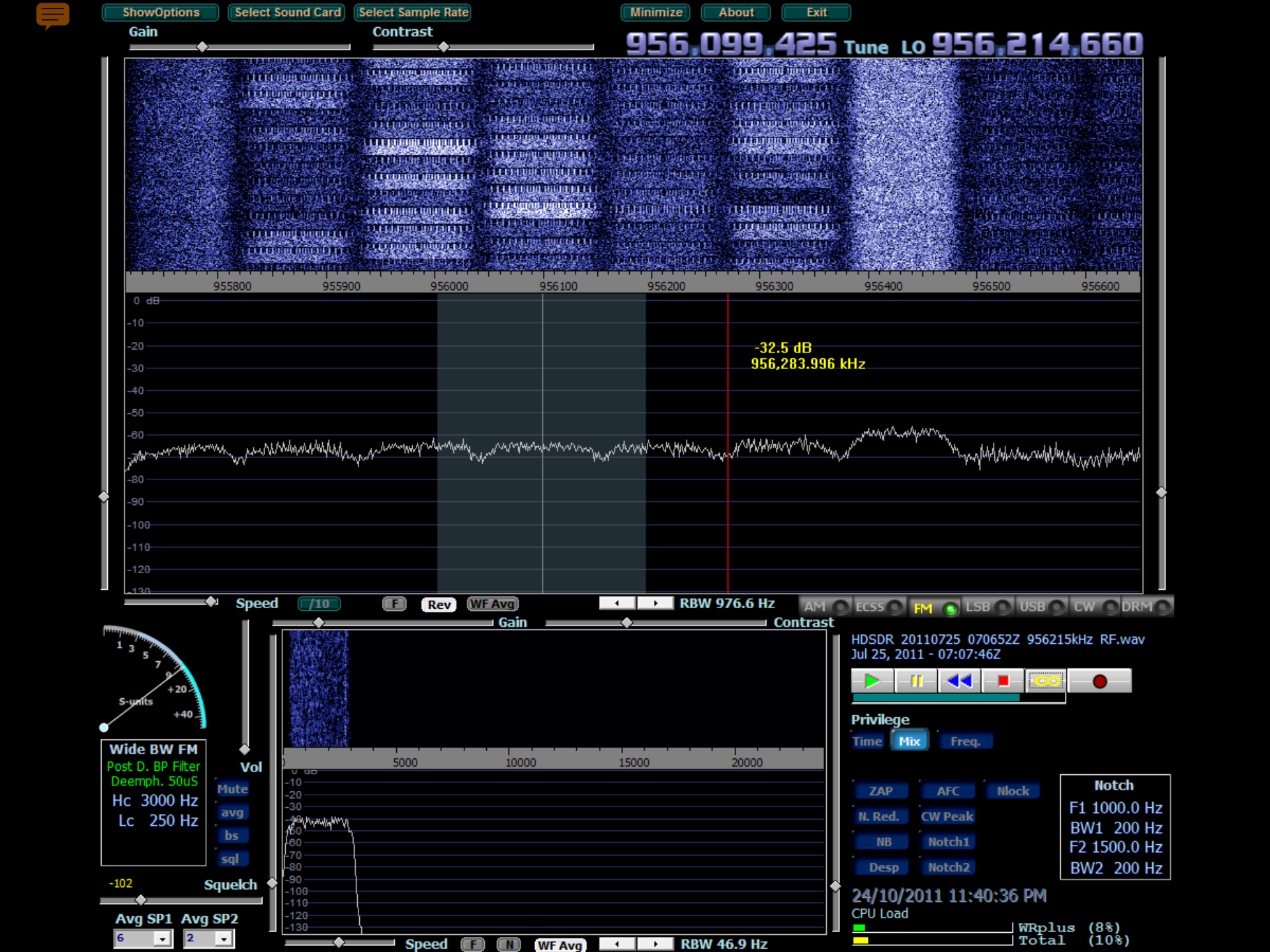


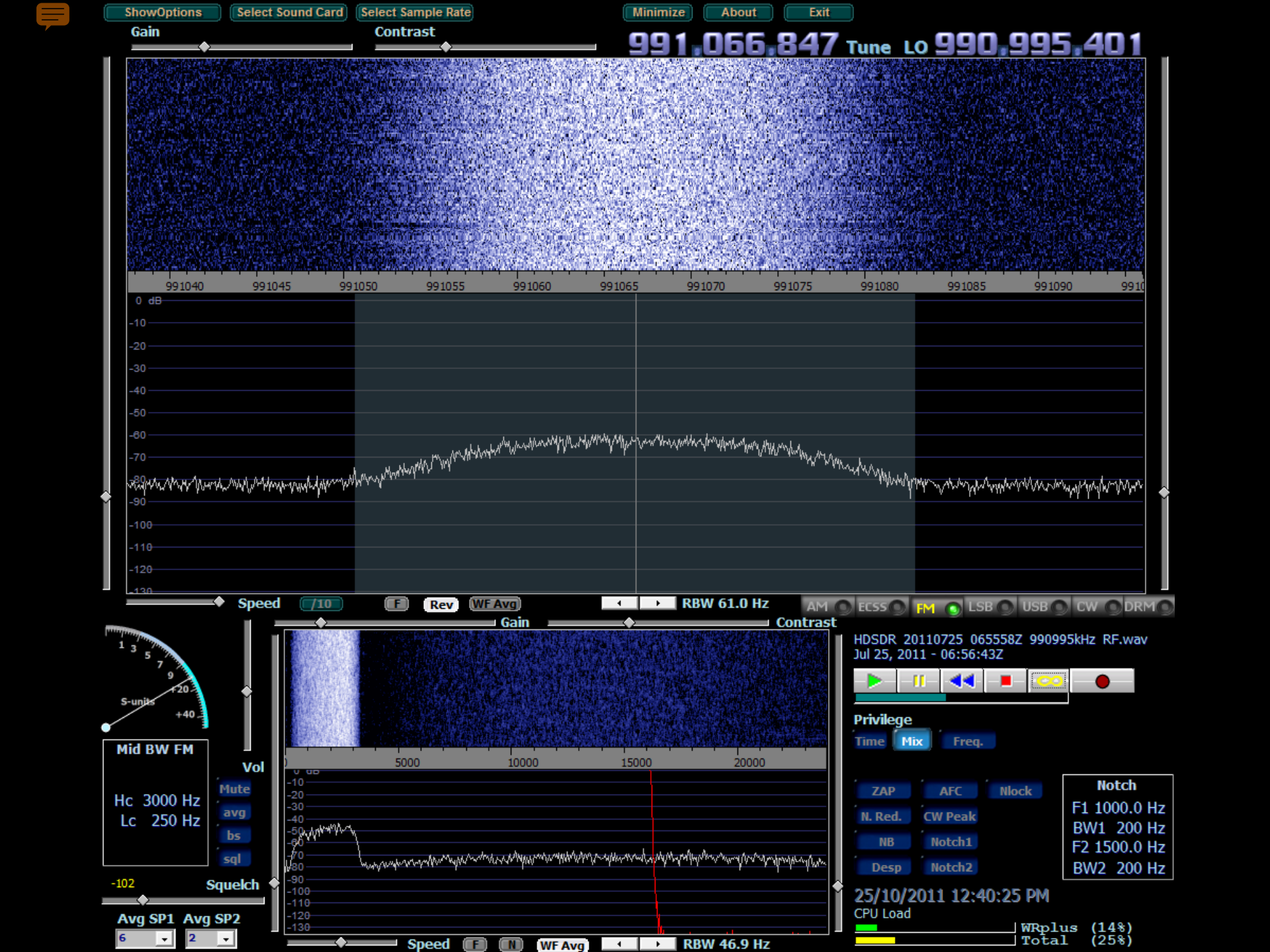
Graphing the Data



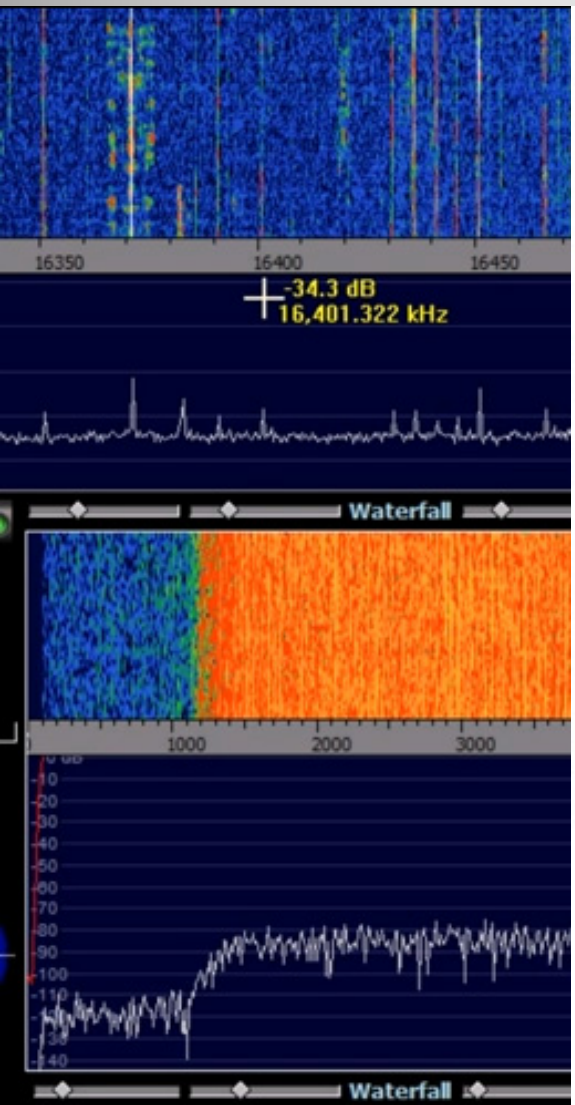





ShowOptions
Select Sound Card
Select Sample Rate
Minimize
About
Exit
Gain
Contrast
956.099.425 Tune LO 956.214.660
955800
955900
956000
956100
956200
956300
956400
956500
956600
0 dB
-10
-20
-30
-40
-50
-60
-70
-80
-90
-100
-110
-120
-130
-32.5 dB
956,283.996 kHz
Speed
/10
F
Rev
WF Avg
RBW 976.6 Hz
AM
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

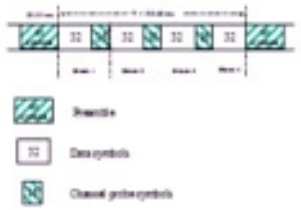
The modulation technique used in this mode consists of phase shift keying (8-PSK) of a single tone sub-carrier of 1800 Hz. The modulation speed (symbol rate) is always 2400 Bd.

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...**:

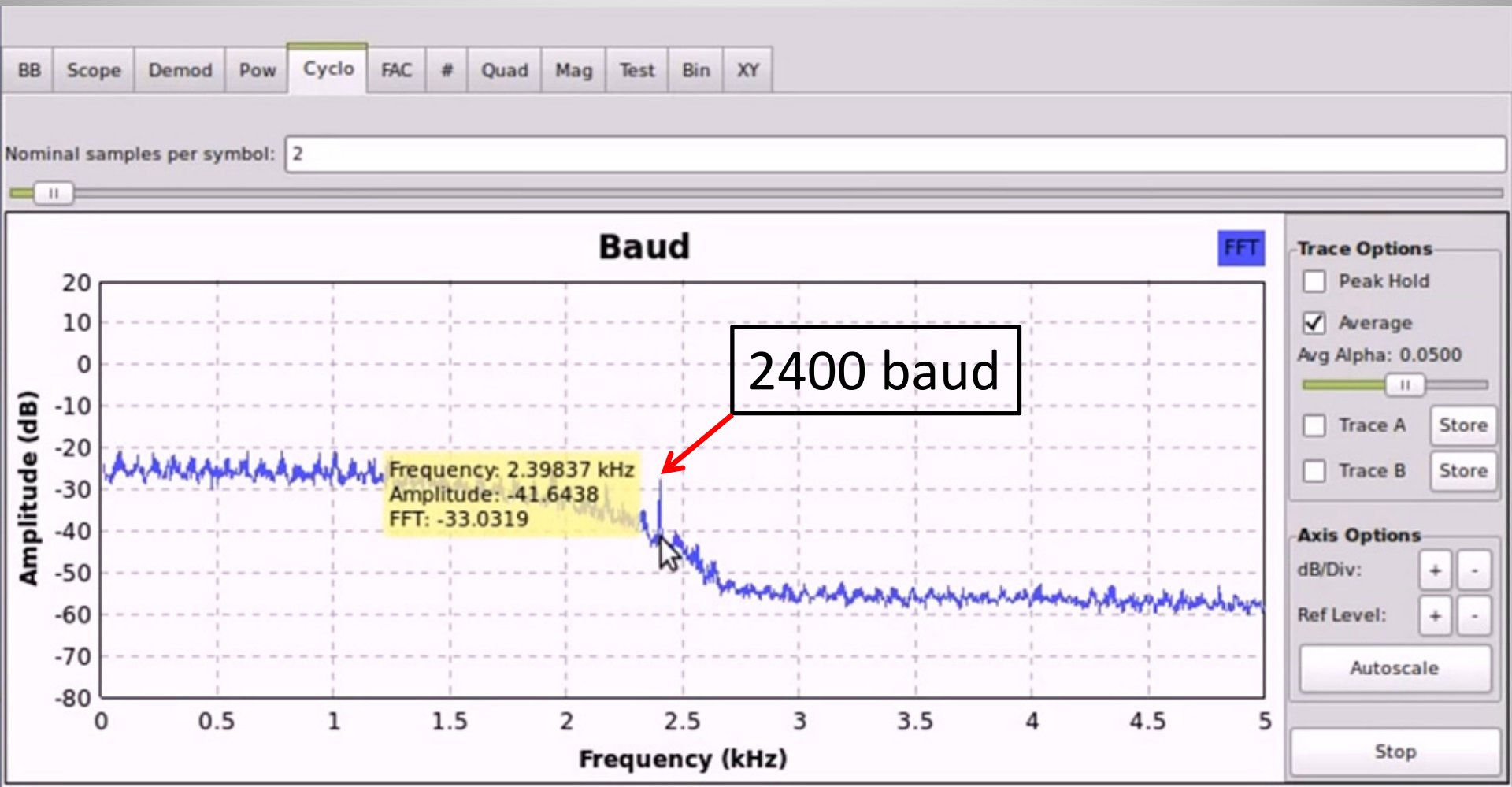
Baud Rate	User data rate (bps)	User data rate (bps)	FEC coding rate	Interleaver	No. of unknown 8-phase symbols (User Data)	No. of known 8-phase symbols (Channel Probe)
2400	2400	3 (8-PSK)	2 / 3	SHORT or LONG	32	16
2400	1200	2 (QPSK)	1 / 2	SHORT or LONG	32	16
2400	600	1 (BPSK)	1 / 2	SHORT or LONG	32	16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

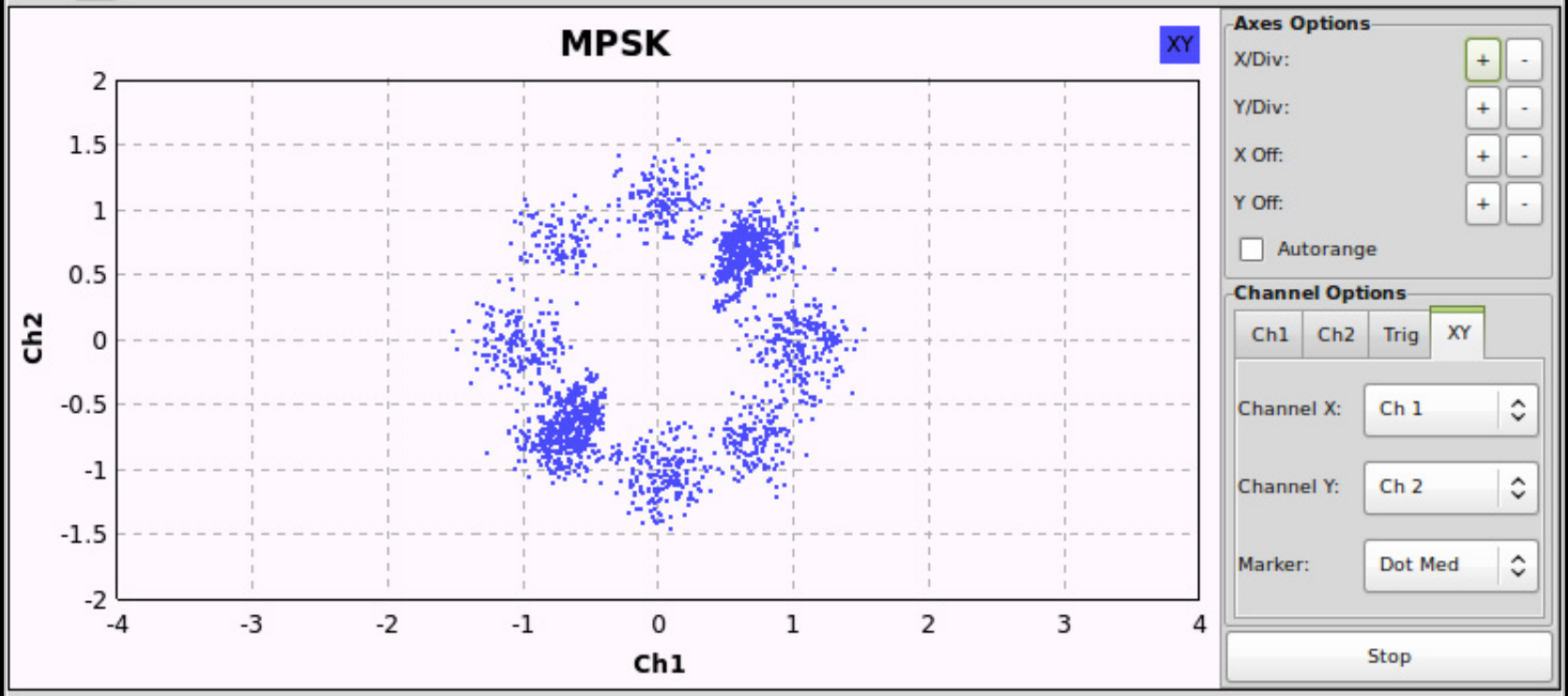
Xlate Offset: -306.325k

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

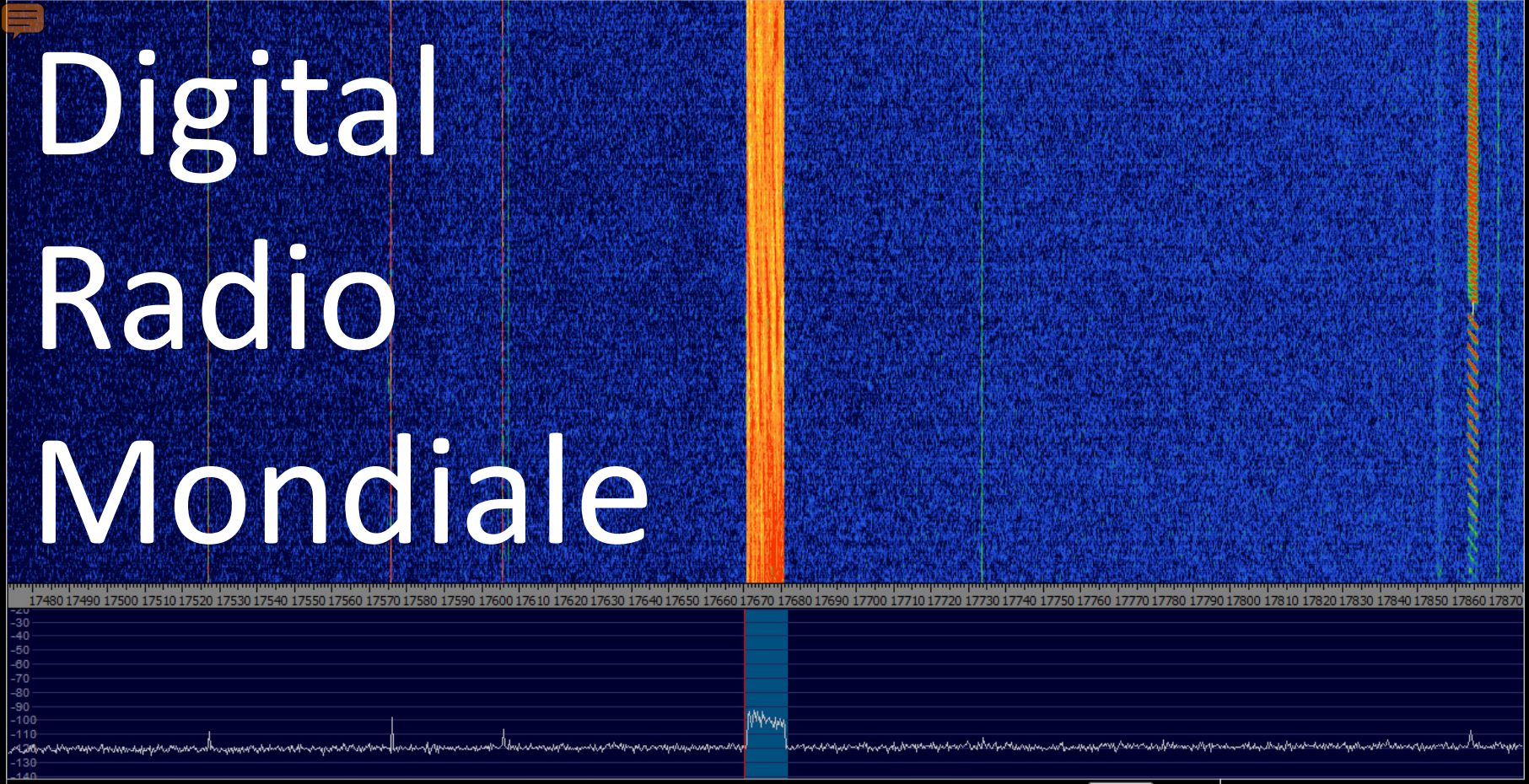
Stop

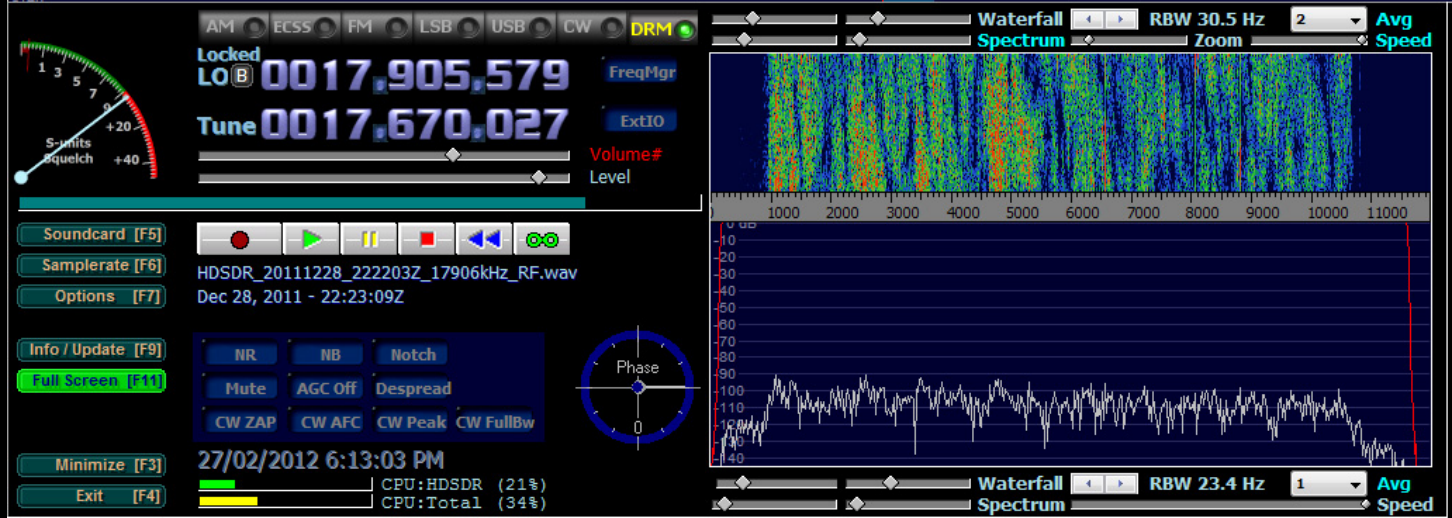
Fine Offset: 0

Xlate Offset: -306.325k

Xlate BW: 5k

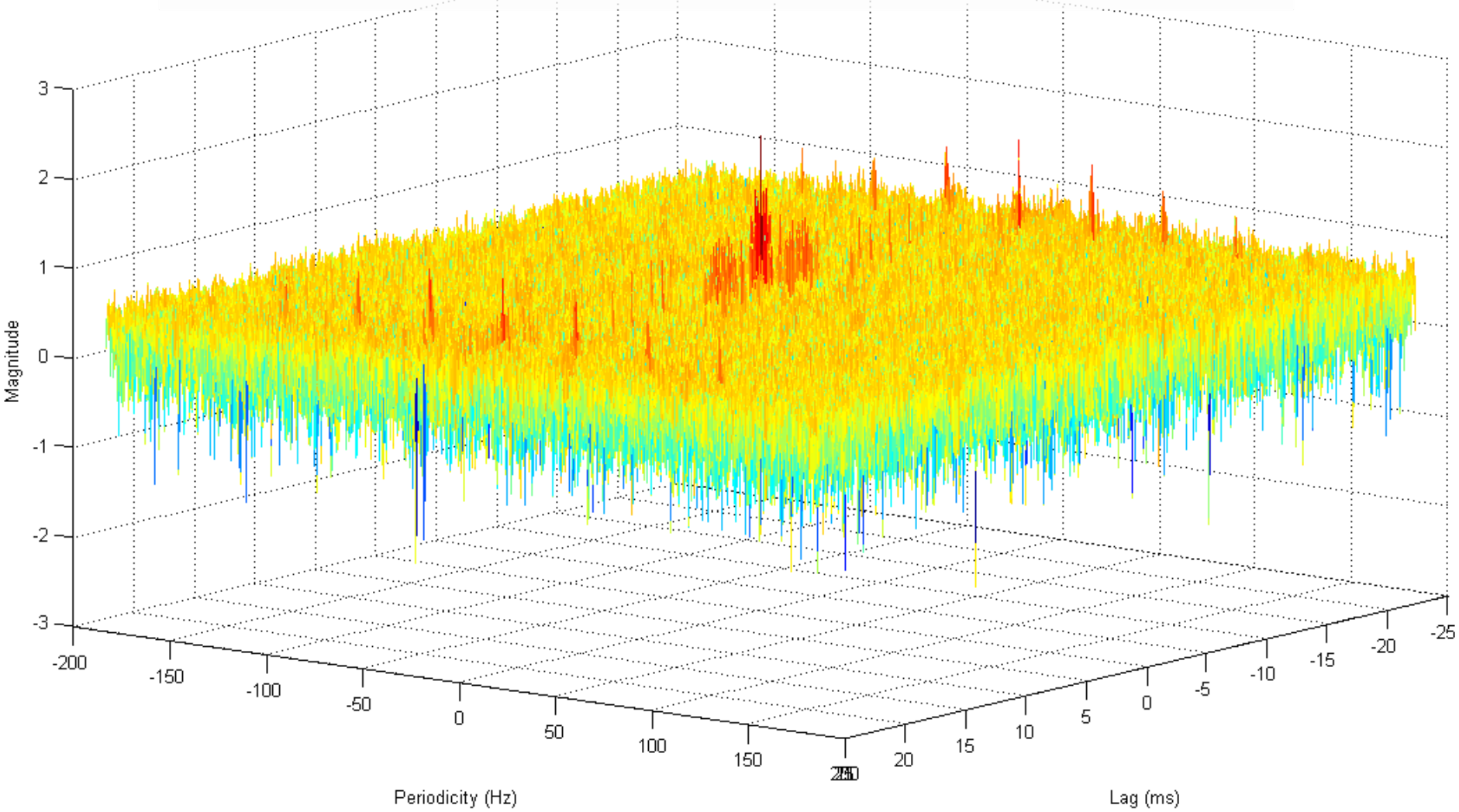
Digital Radio Mondiale



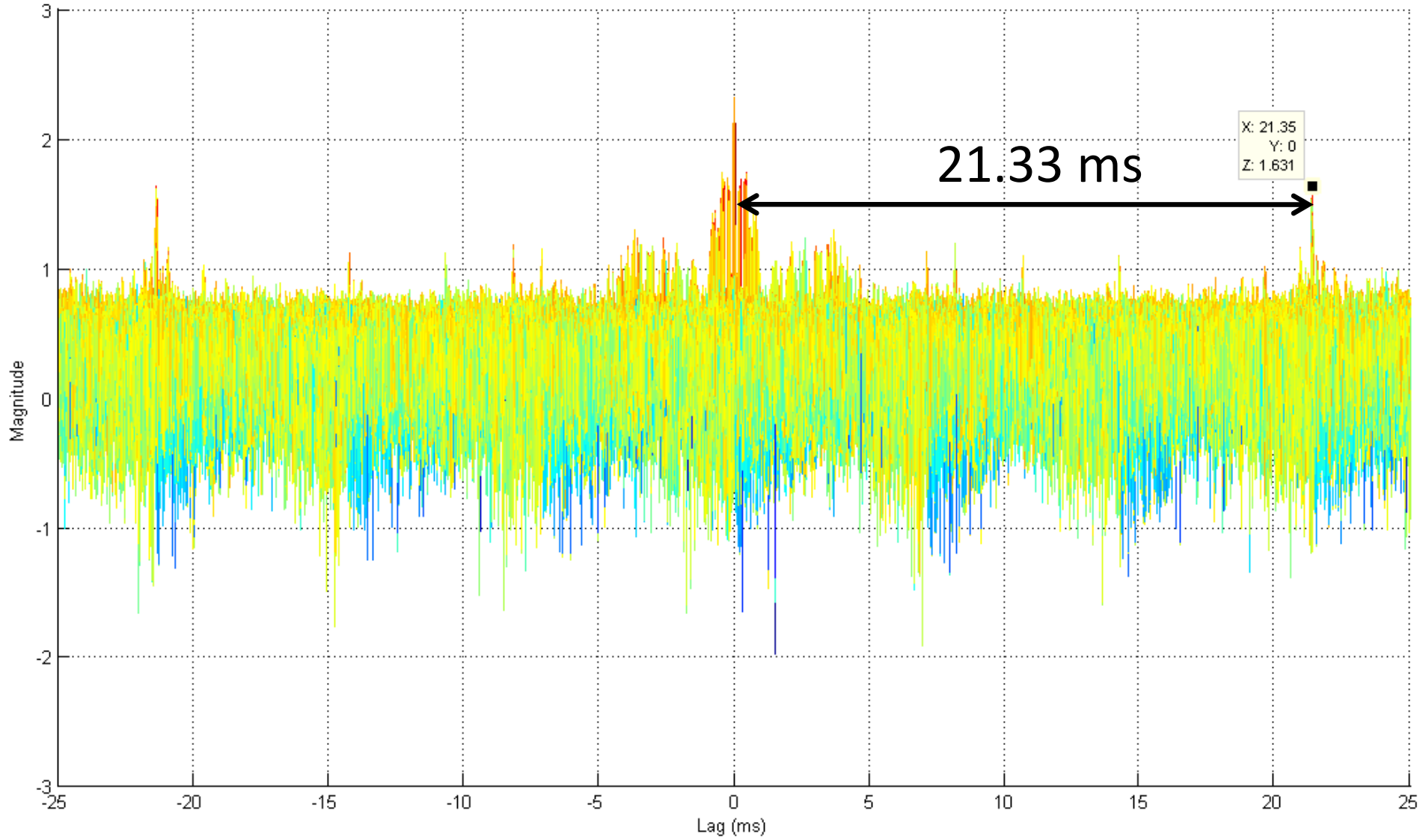


Cyclic Autocorrelation Function

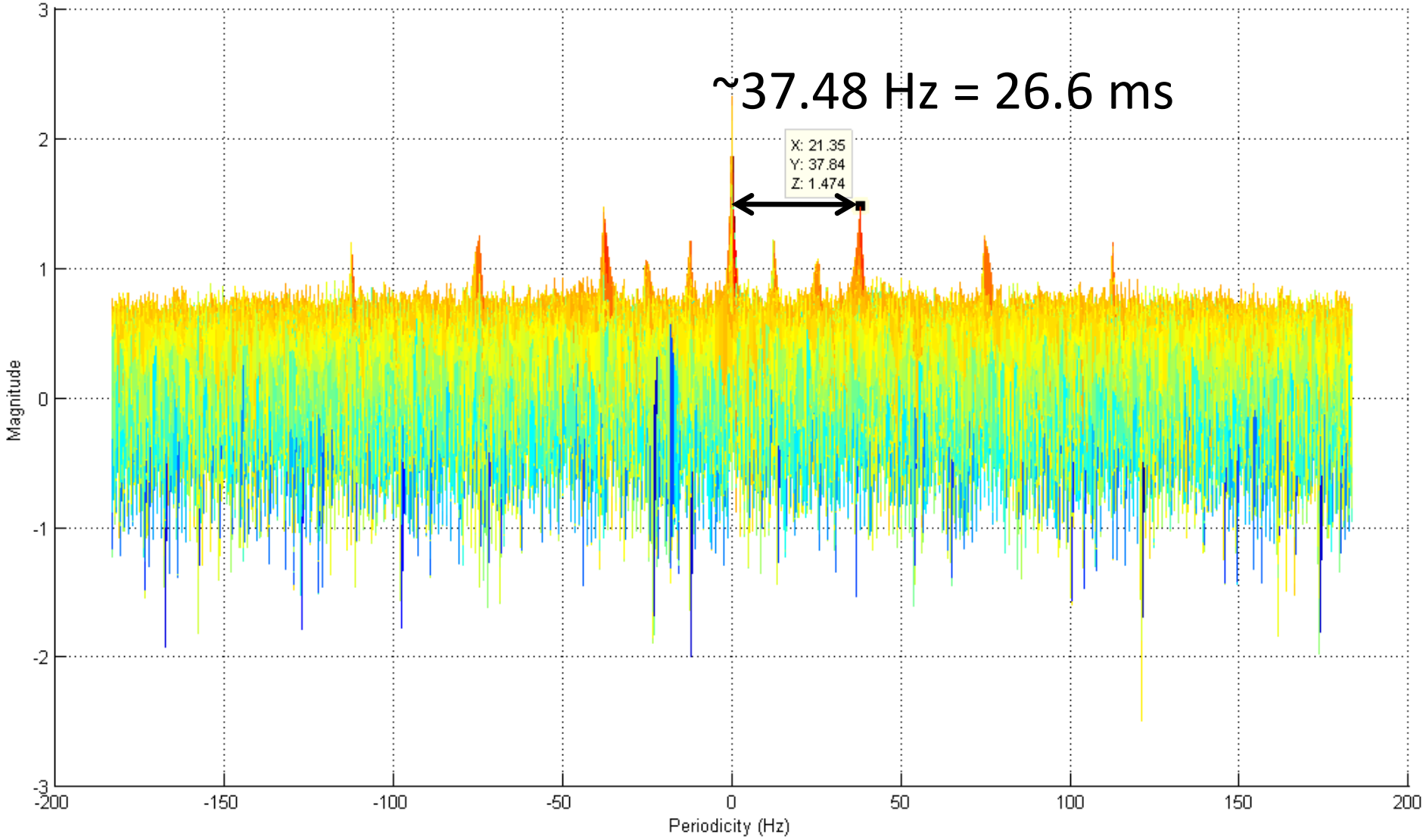
Han, Sohn & Moung,"A Blind OFDM Detection and Identification Method Based on Cyclostationarity for Cognitive Radio Application"



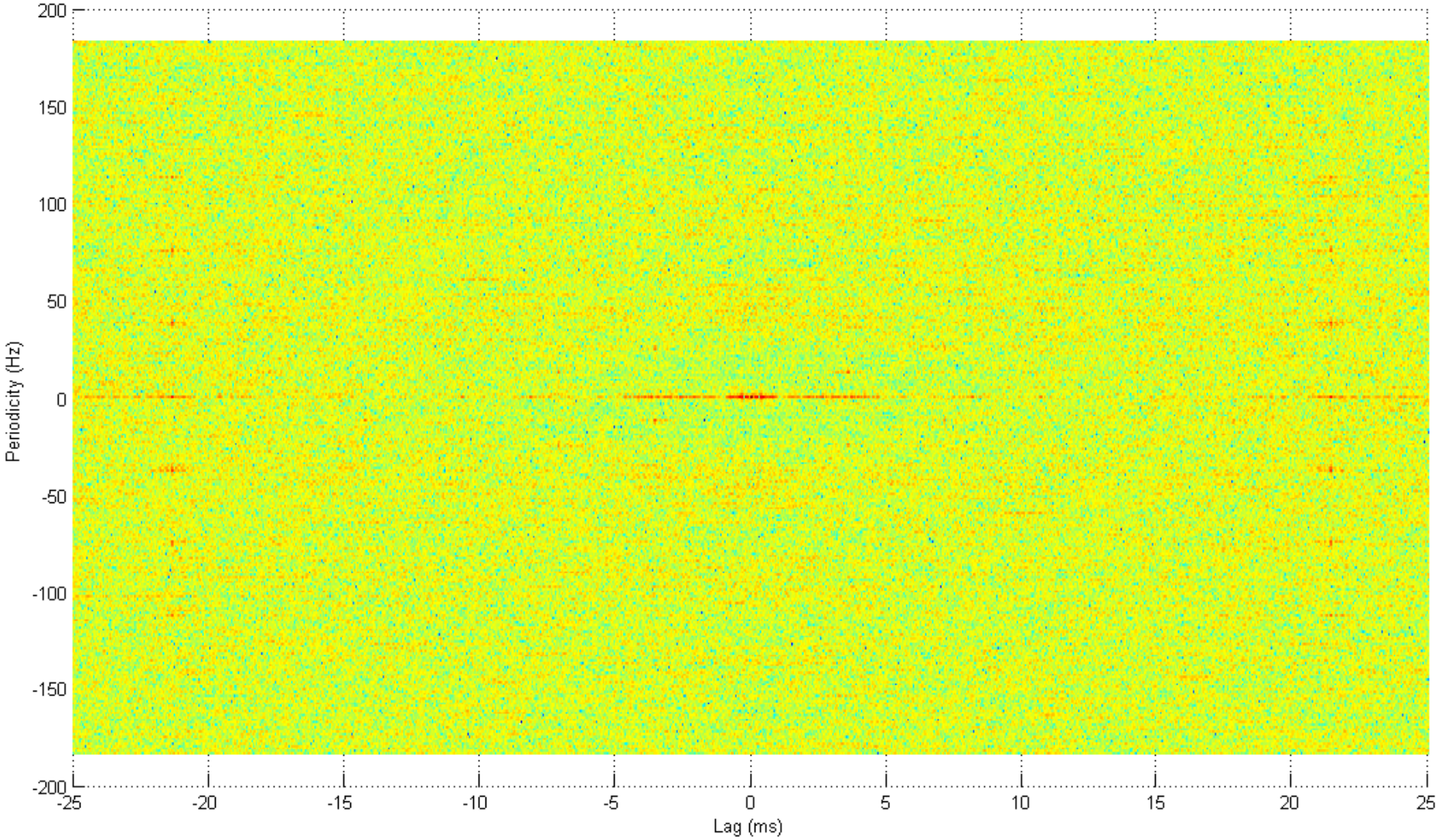
Un-guarded Symbol Time



Total Symbol Duration



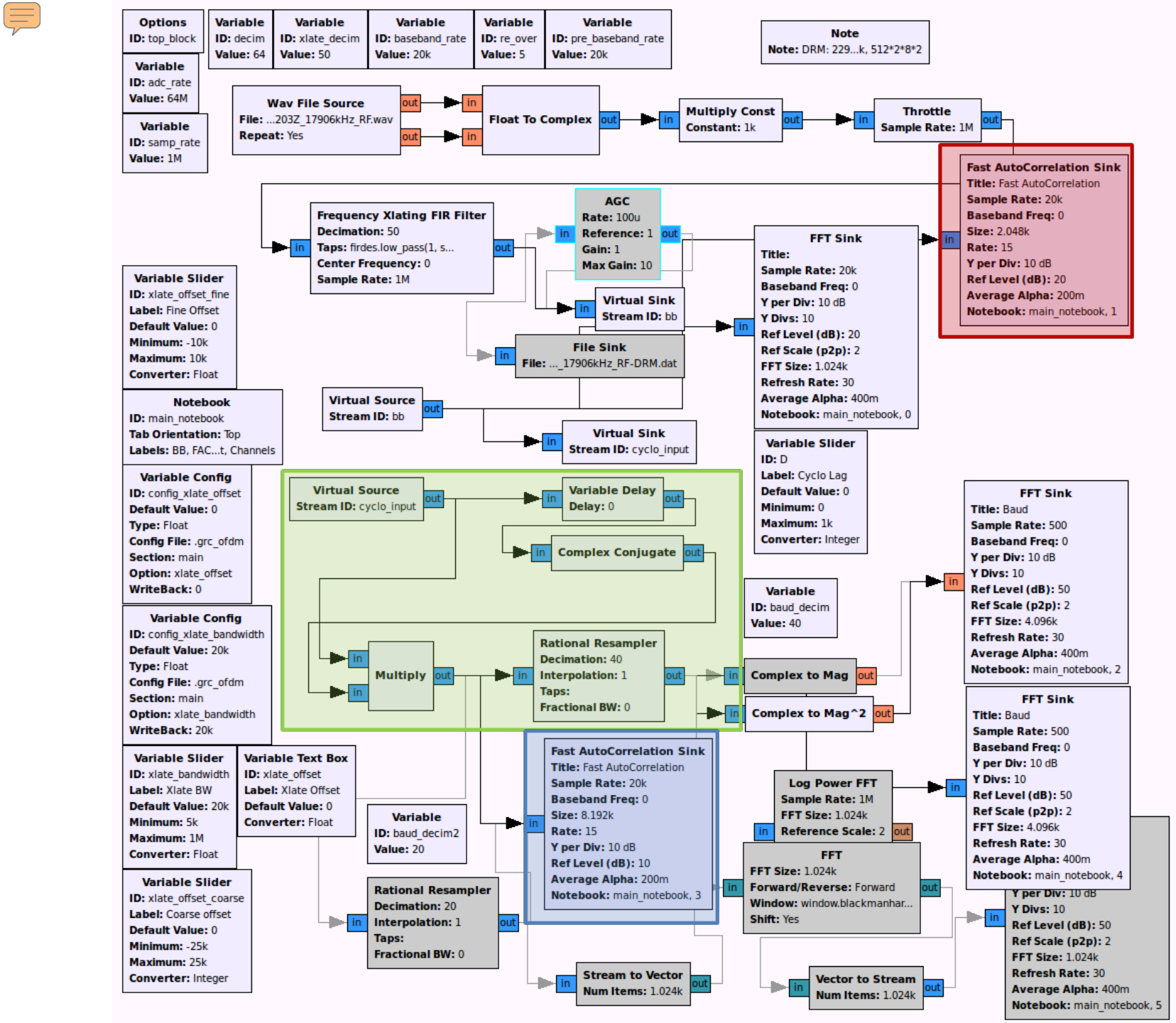
Top-down DRM Symmetry

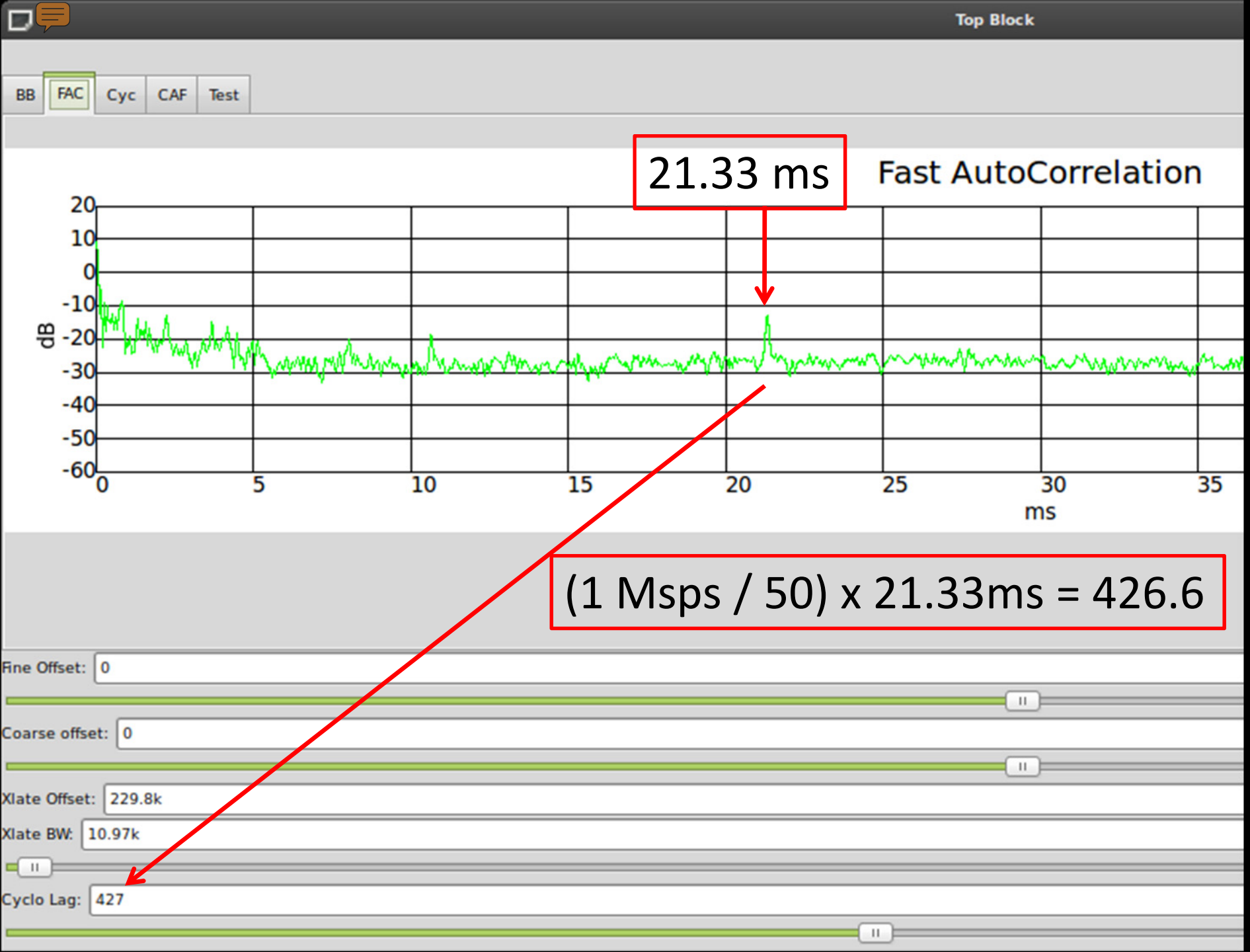


DRM Class B

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

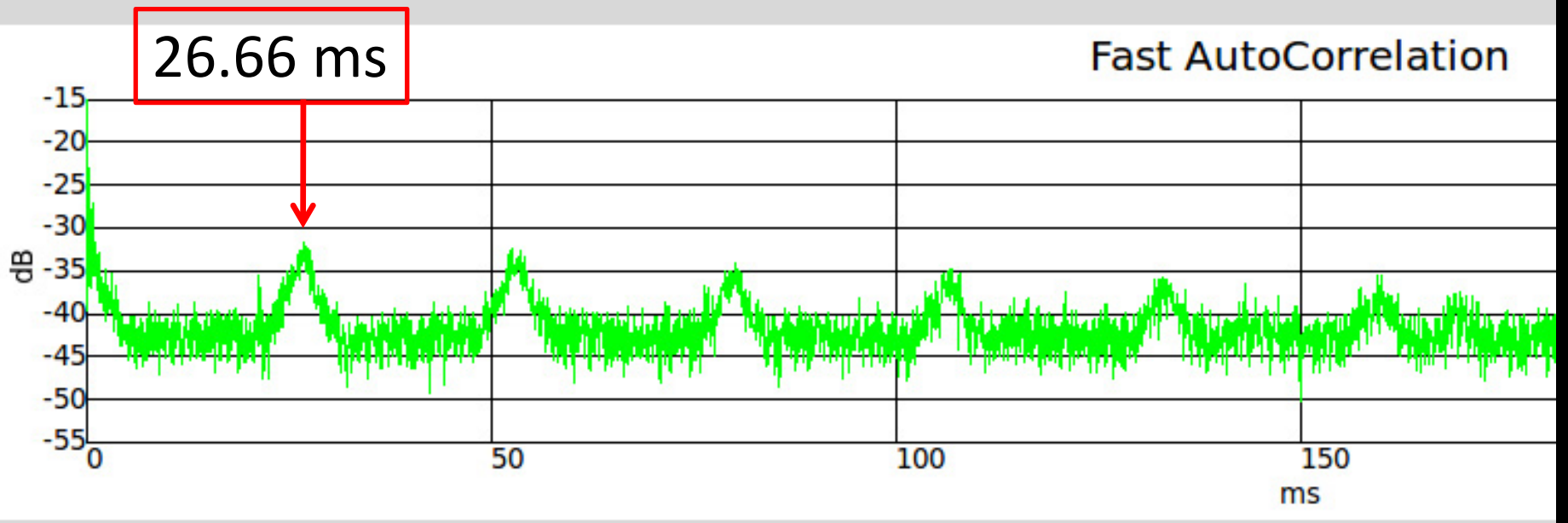
1 / (21.33 ms)


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



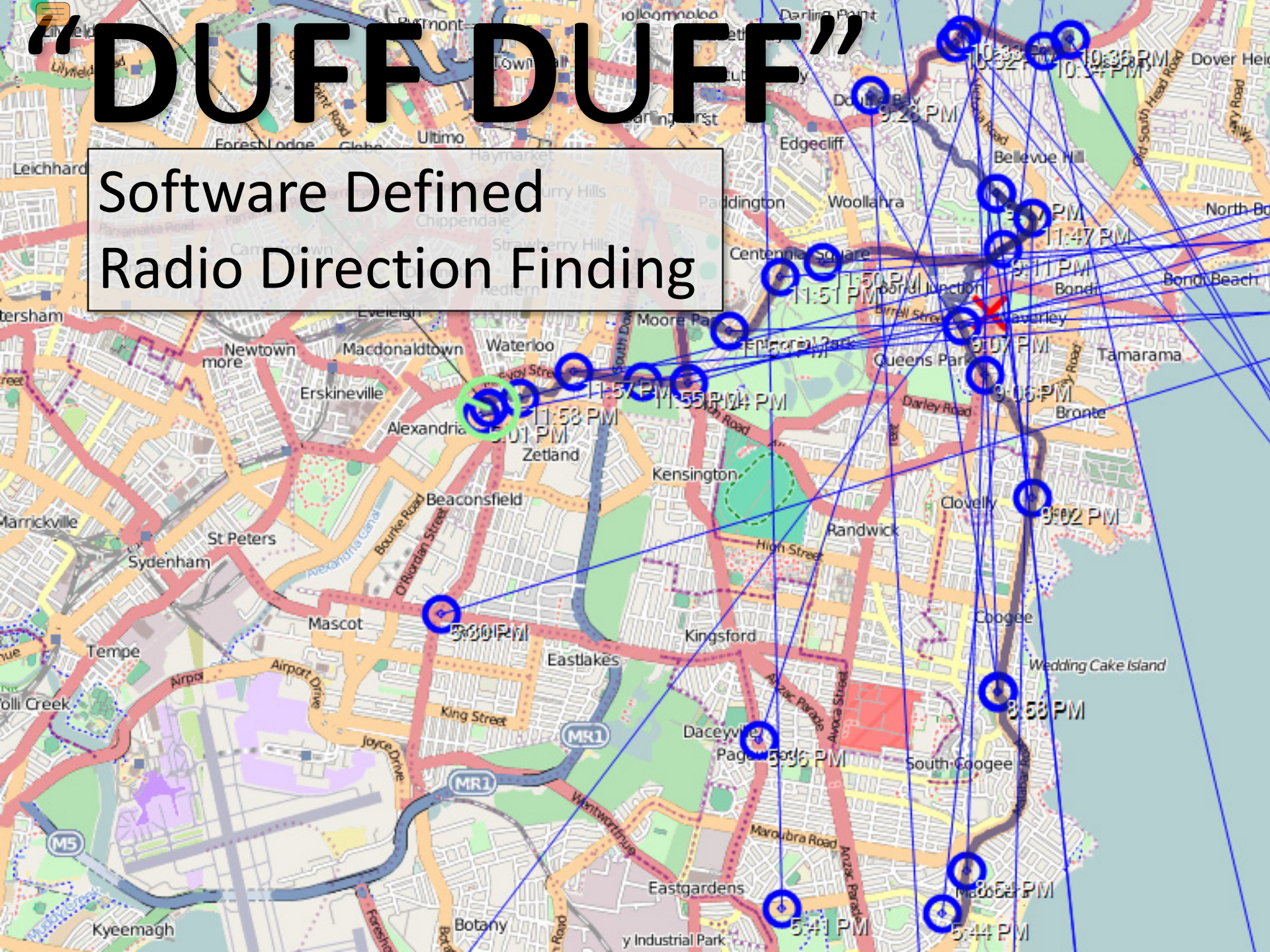
Fine Offset: 0

Coarse offset: 0

Xlate Offset: 229.8k

Xlate BW: 10.97k

Cyclo Lag: 427


“DUFF DUFF”
Software Defined
Radio Direction Finding

DF Usage

- Radio navigation
  - Predecessor to RADAR
- SIGINT
- Emergency aid
  - Avalanche rescue
- Wildlife tracking
- Reconnaissance
  - Trajectory tracking
- Sport?!

History

- WW I & II
  - Y-stations along the British coastline
  - Find bearing to U-boats in Atlantic
  - ‘U-Adcock’ system
    - Four 10m high vertical aerials around hut →
    - DF goniometer (angle measurement) & radio

DF for HF

- HF: 3-30 MHz
  - long wavelengths → large distances
- HF/DF = “HUFF DUFF!”
- Used for SIGINT
- Large installations: AN/FLR-9 array near Augsburg, Germany →

Amateur RDF

- ‘Fox hunts’
- Competitor on ‘2-meter band’ ARDF course

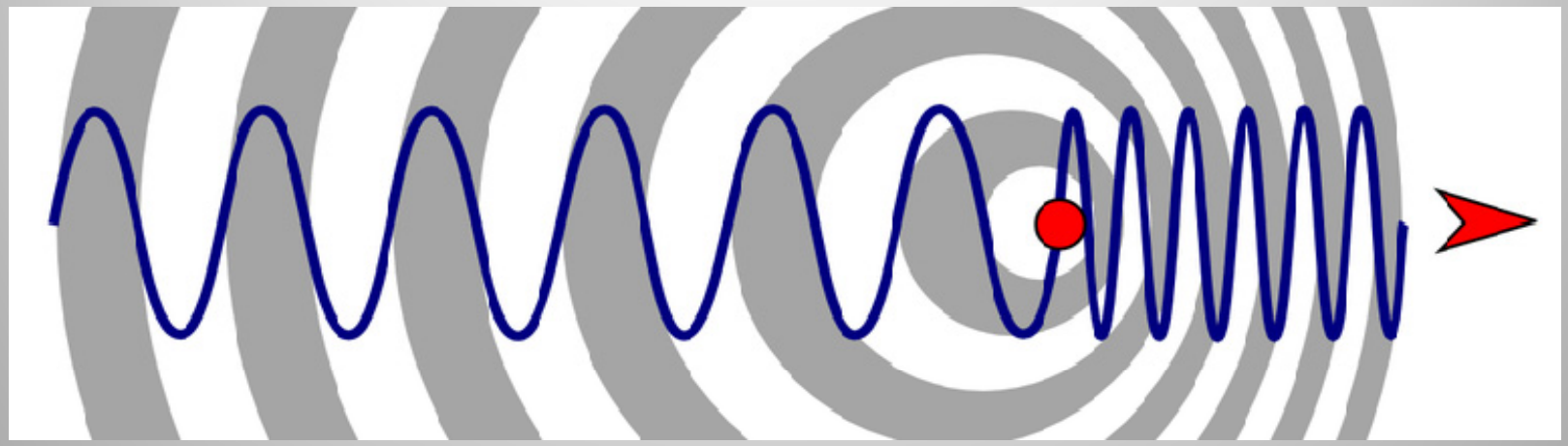
(Pseudo-) Doppler DF

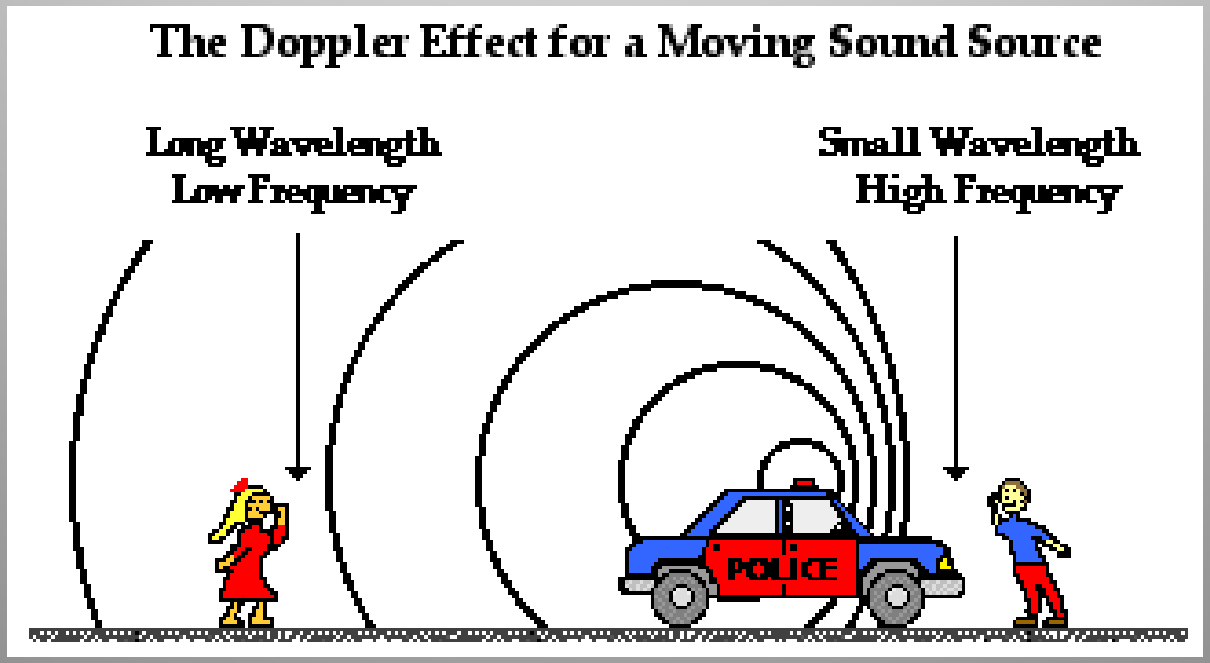
- Exploit Doppler shifting of radio waves caused by motion of an antenna

- Measure the shift in detected signal

  →Determine direction of transmission

Recap: Doppler Effect





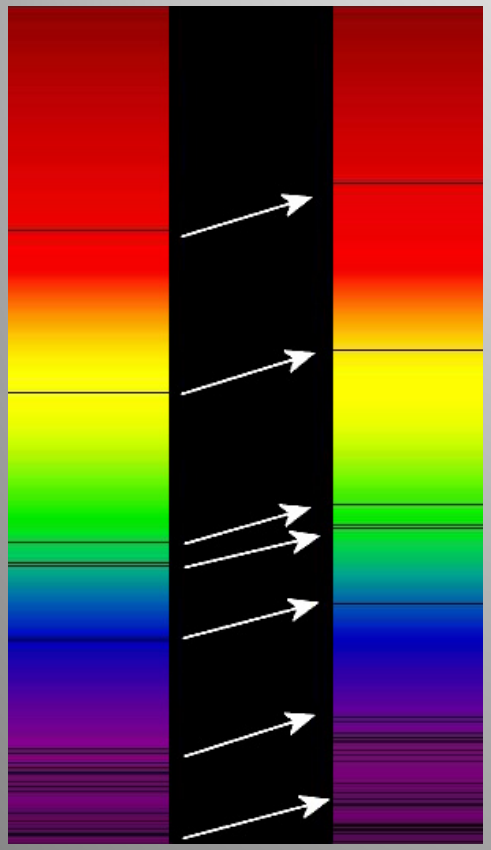
Aside: Siren Misconception

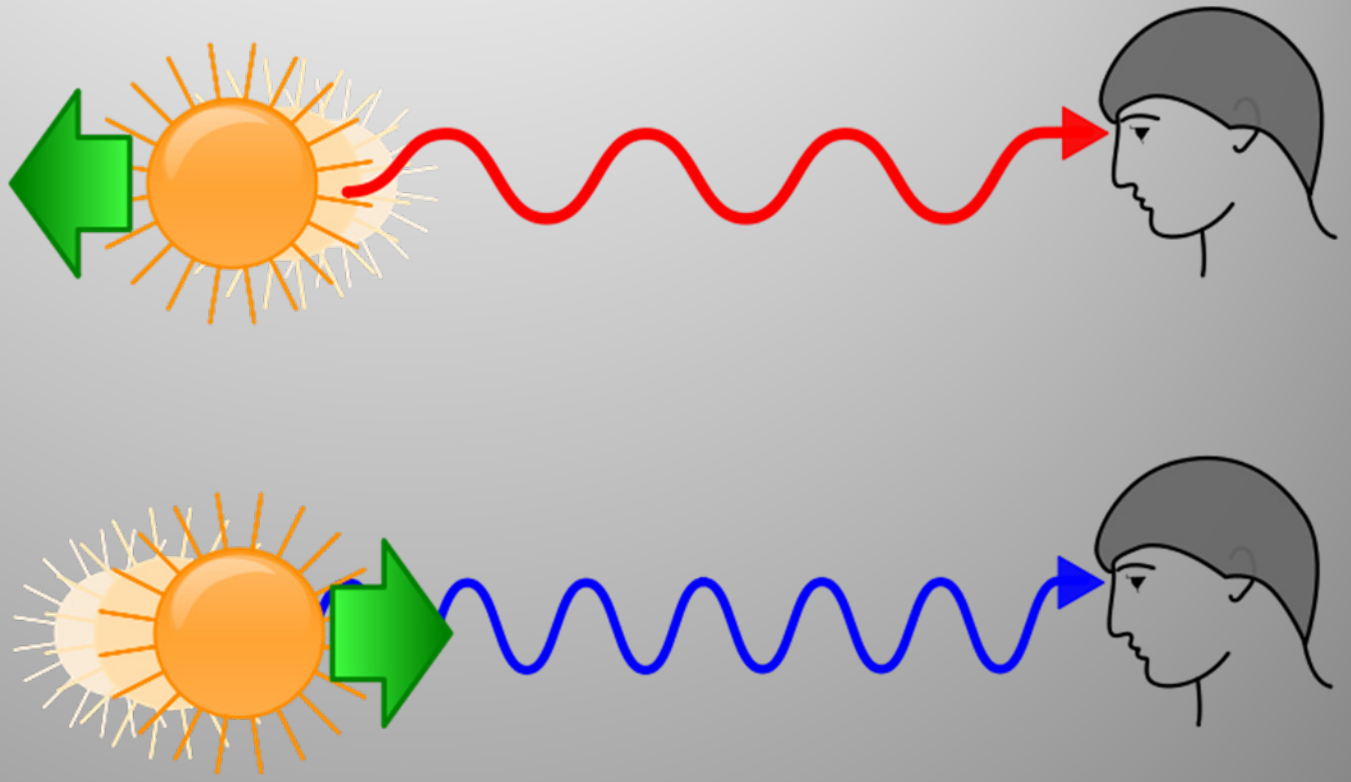
"…the **observed** frequency **increases** as the object approaches an observer and then **decreases** only as the object passes the observer."

"…**Higher sound pressure levels** make for a small decrease in **perceived pitch** in low frequency sounds, and for a small increase in perceived pitch for high frequency sounds."

A Swan

Cosmological Redshift

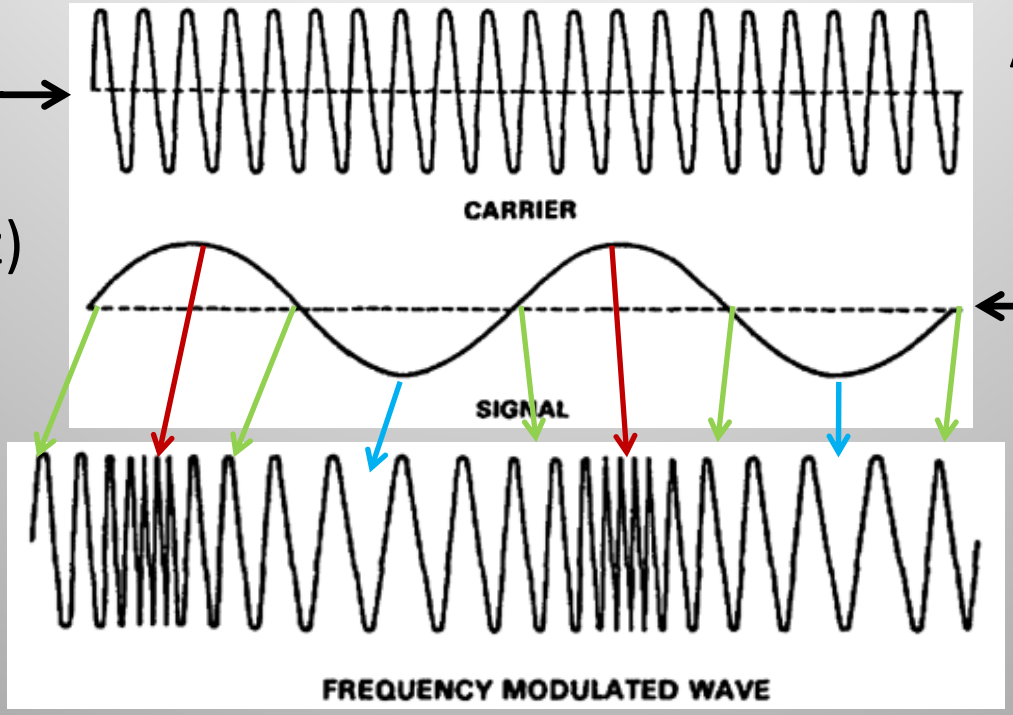




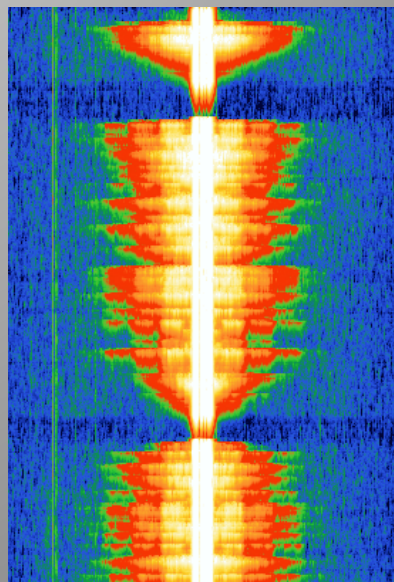
Expansion of space, not motion of radiating object!

Frequency Modulation 101

'Main' transmission frequency (e.g. 105.7 MHz)

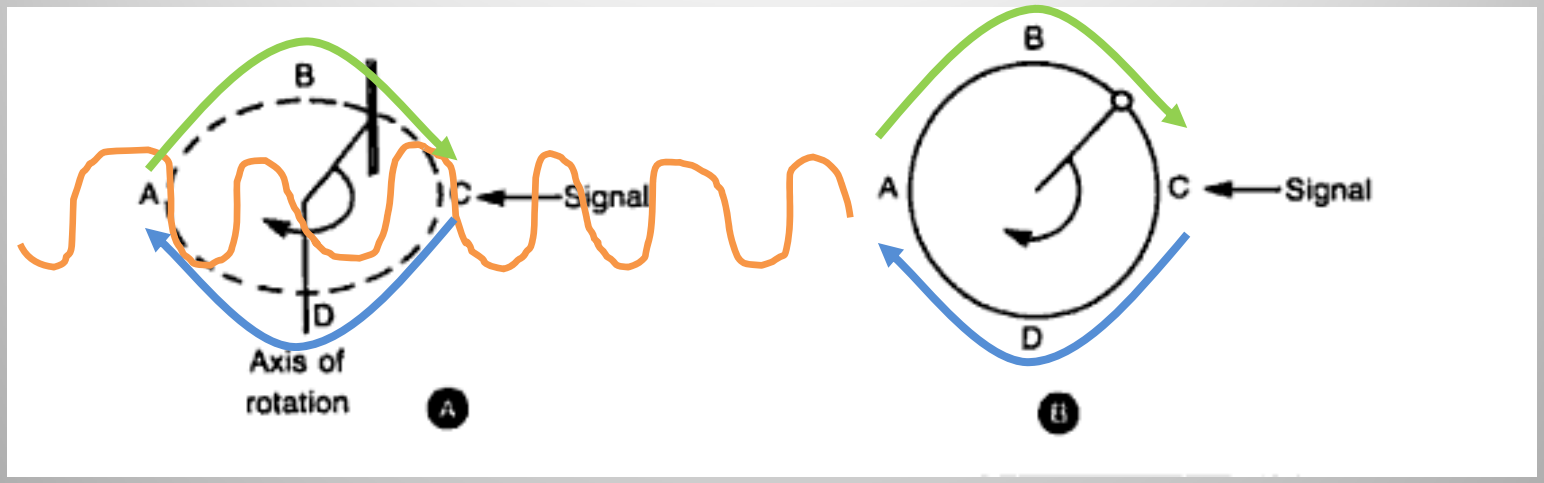


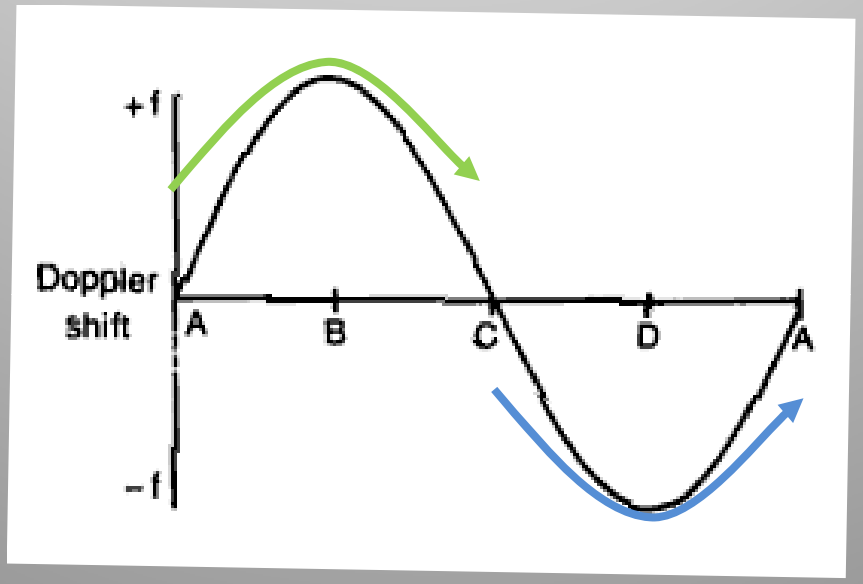
Analog or digital Information to be transmitted



Frequency modulation changes the carrier's frequency
→ Moves the carrier slightly left/right of its original position on frequency plot

Physically Rotated Antenna



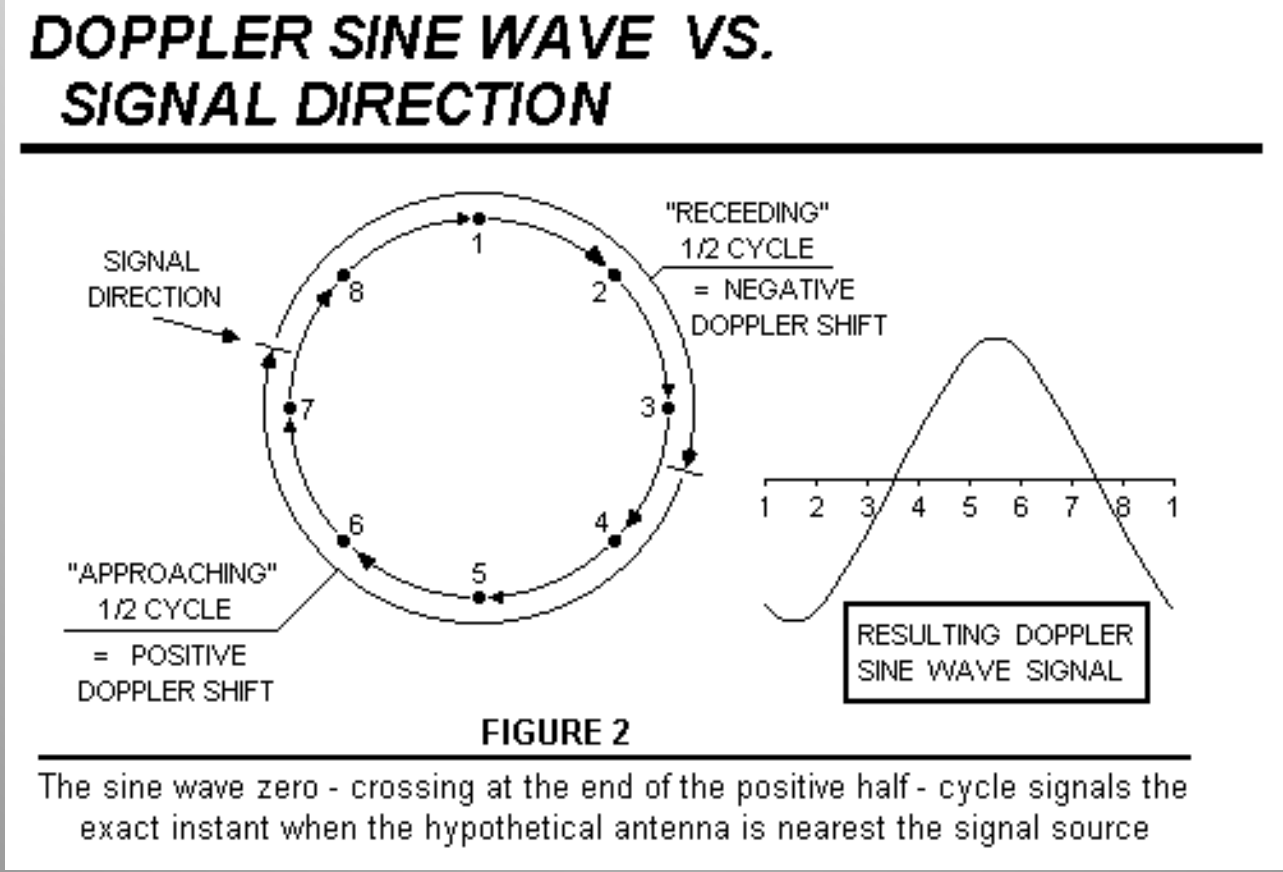


Joseph Moell, "Transmitter Hunting: Radio Direction Finding Simplified", 1987 (McGraw-Hill)

Doppler Shift

- Doppler shift of received signal used to calculate angle of transmitter
- Easy with an FM radio!
- Frequency Modulation:
  - Shifts the centre (carrier) frequency about based on the original modulating signal
  - Doppler shift just moves it around some more
- FM receiver detects Doppler as an extra tone!

Extra tone: sine wave



http://silcom.com/~pelican2/PicoDopp/ABOUT_DOPP.html

Mechanical Rotation Rate

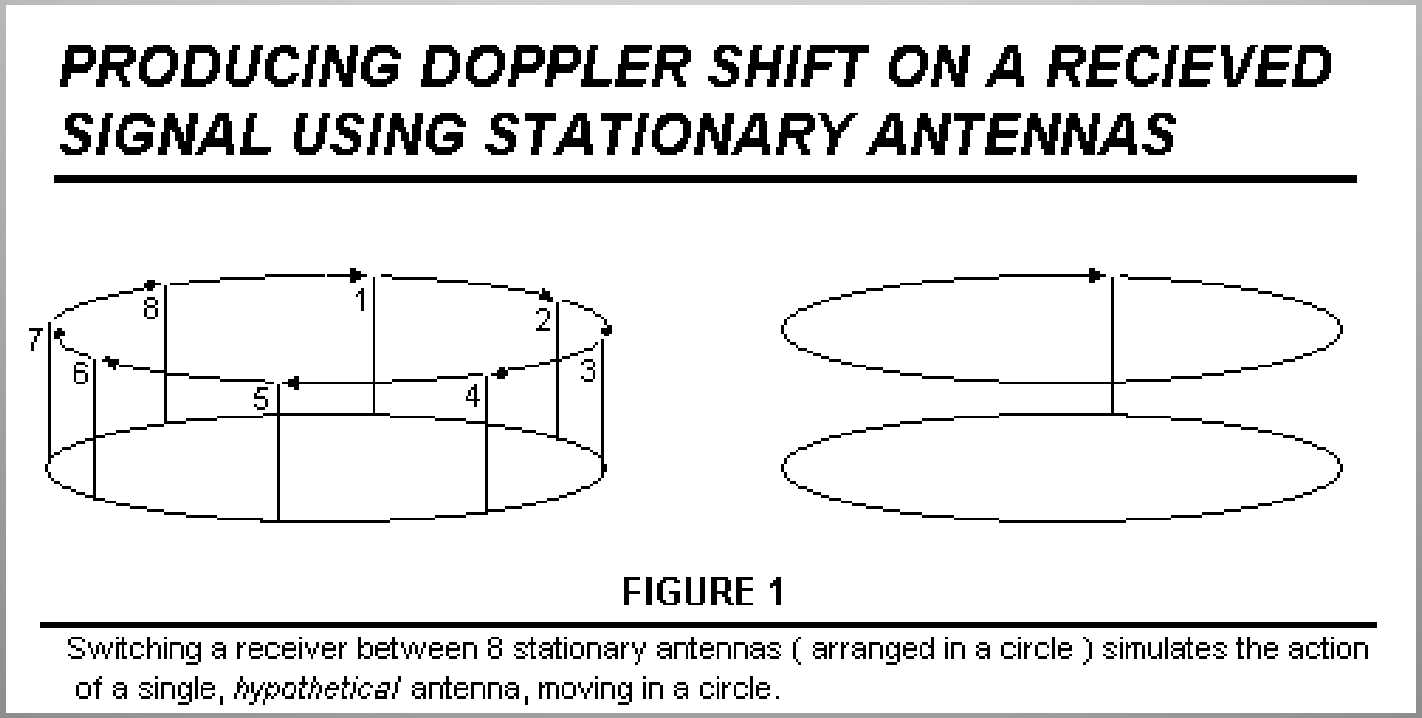
- Doppler equation relates:
  - Doppler shift
  - Radius of antenna
  - Angular velocity (rotation rate)
  - Frequency of signal
- For a small antenna setup tuned to 2m wavelength (~150 MHz), requires:

38600 RPM

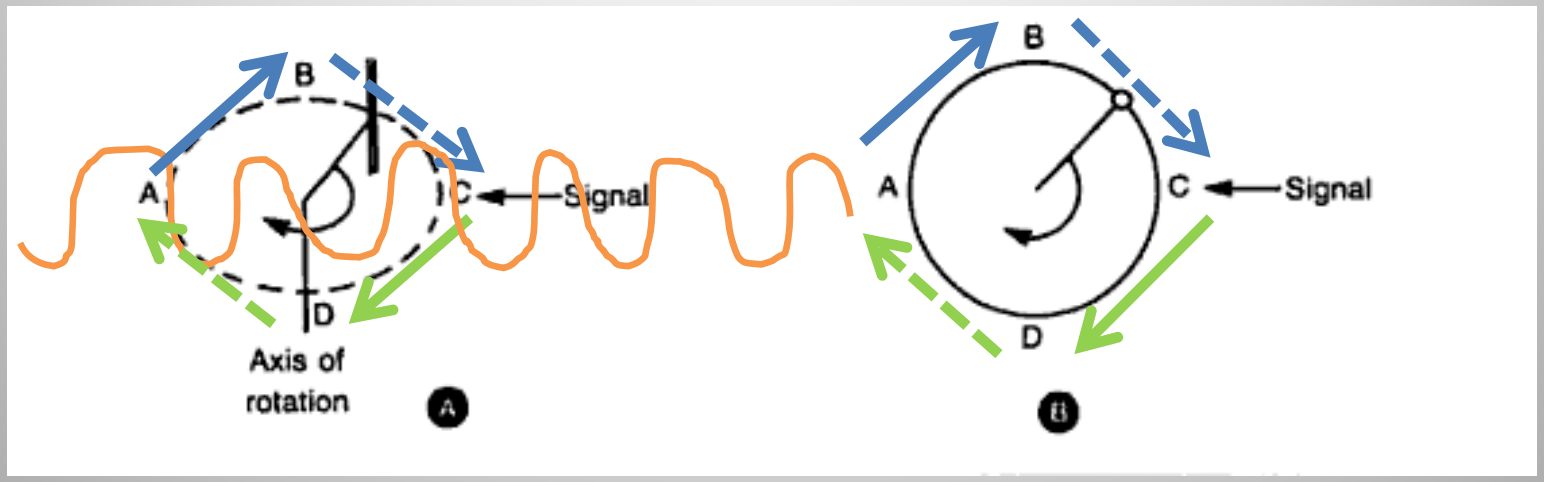
~643 rot/sec

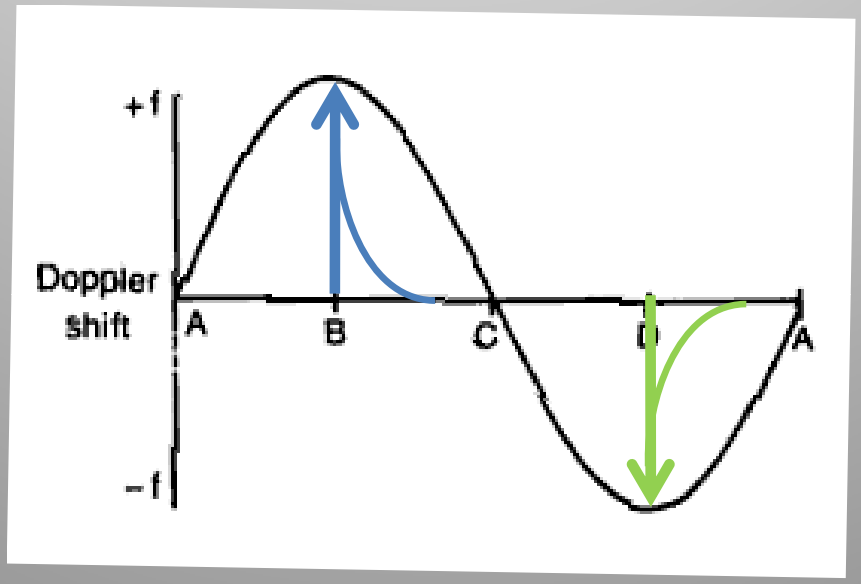
Pseudo-Doppler

- Array of **fixed** antennas
- Switch **electronically** between them
  - 'Simulate' physical rotation



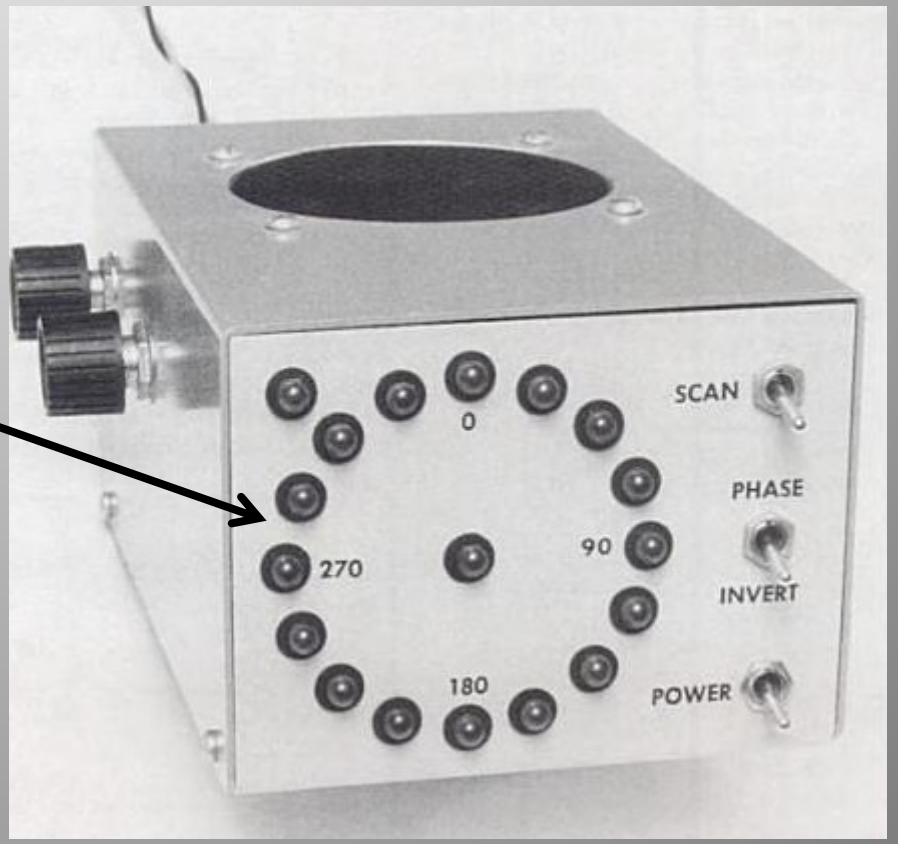
Electronically Rotated Antenna





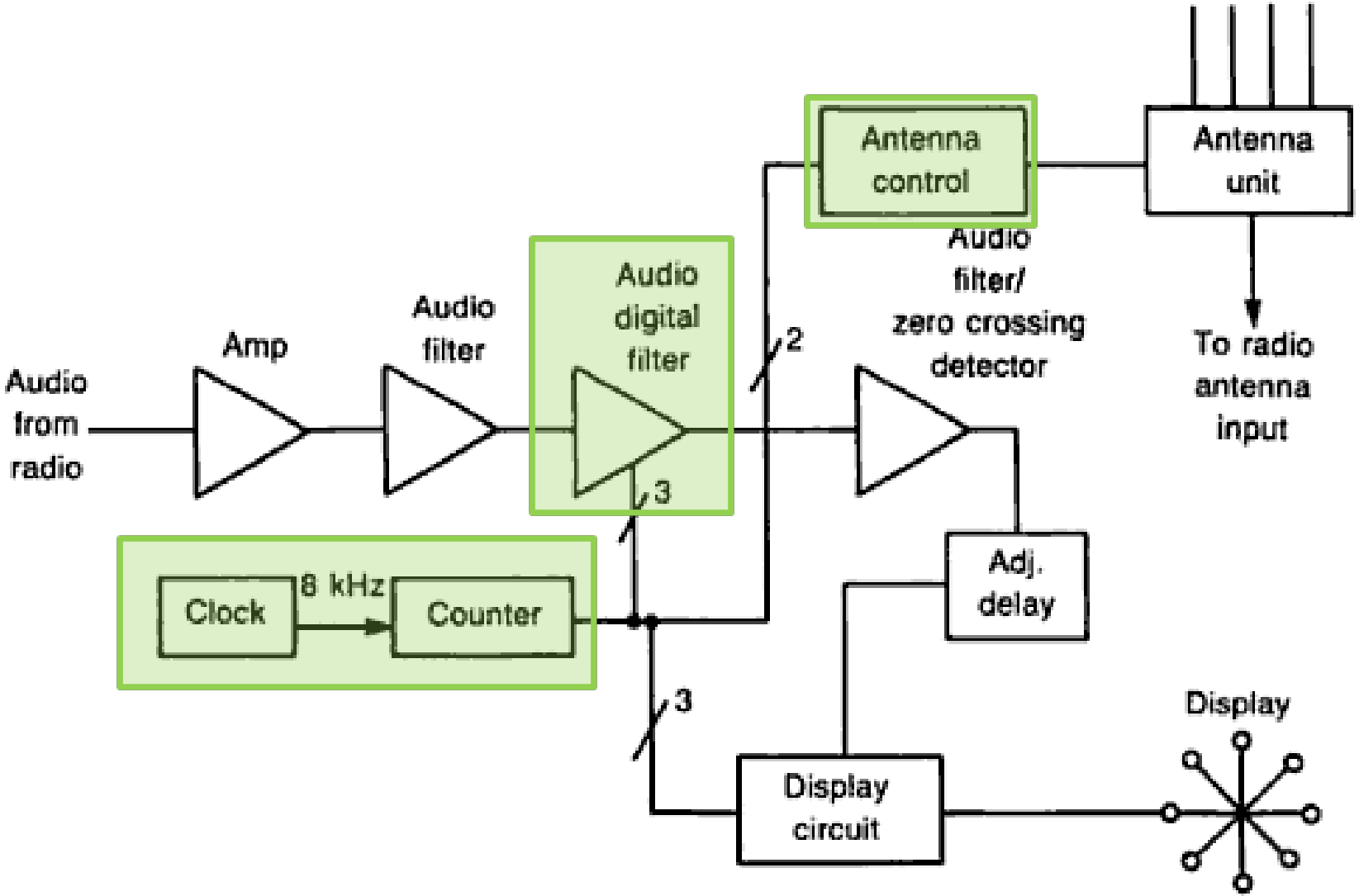
Home-made RDF

- ‘Roanoke Doppler’
- Four antennas
- Control box
- Plug in **any standard FM radio**
- LEDs indicate direction

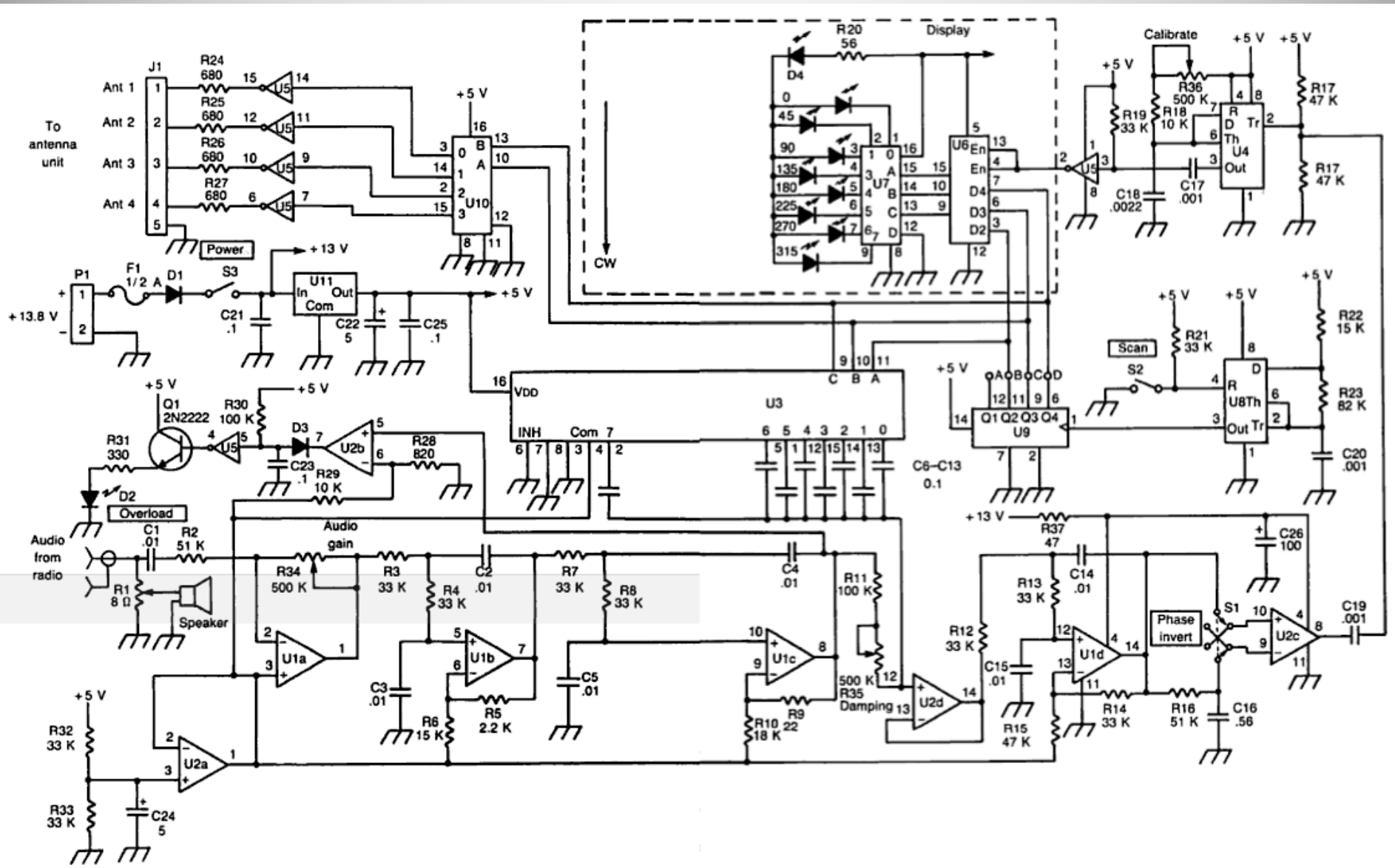


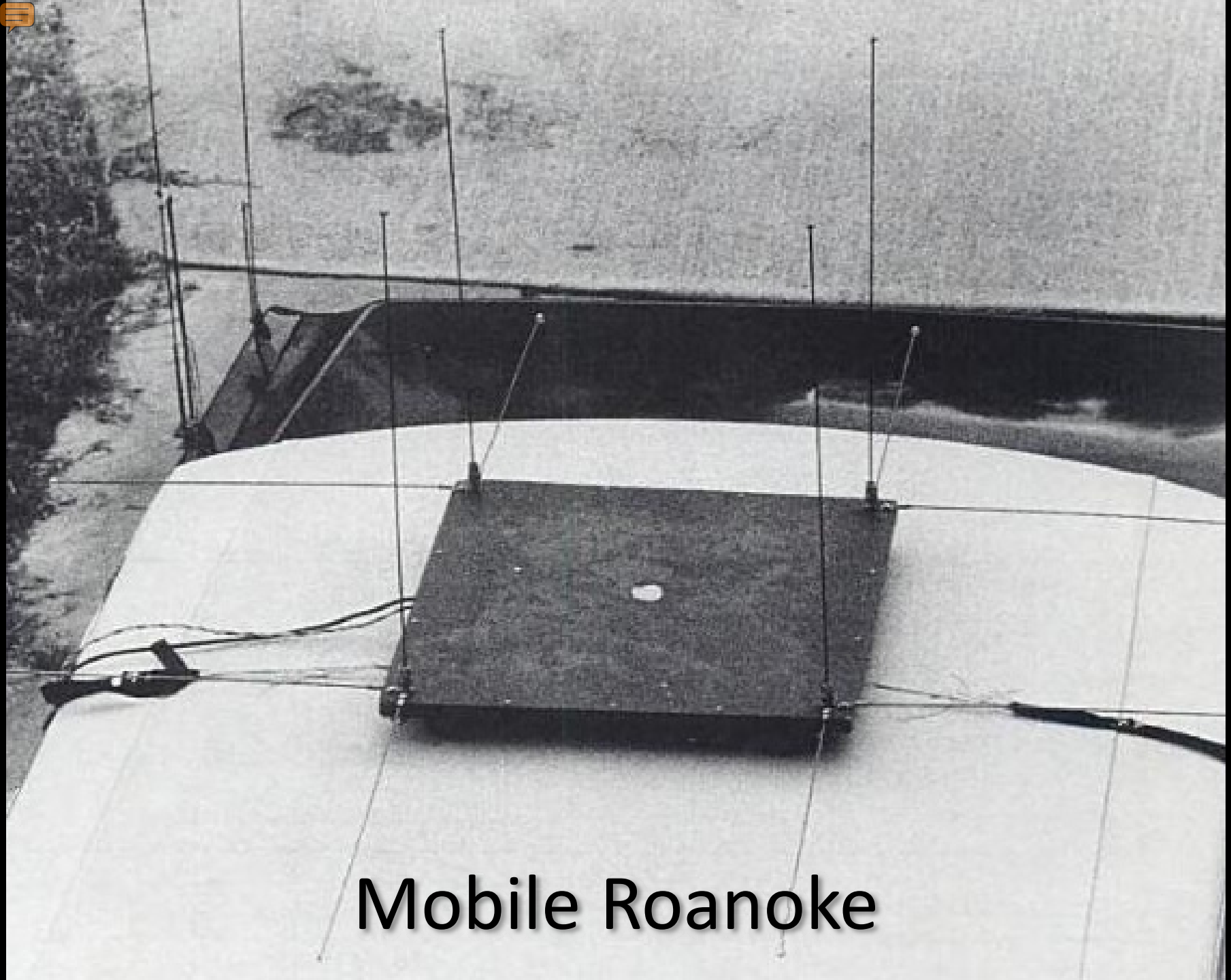
Joseph Moell,
“Transmitter Hunting:
Radio Direction Finding Simplified”,
1987 (McGraw-Hill)

Block Diagram

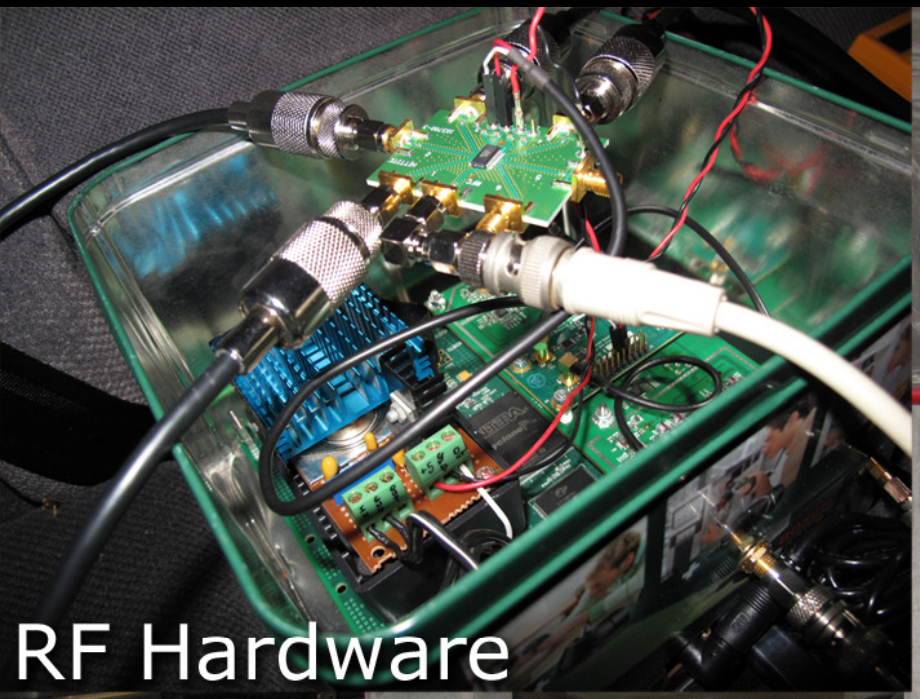


Circuit Diagram




Mobile Roanoke

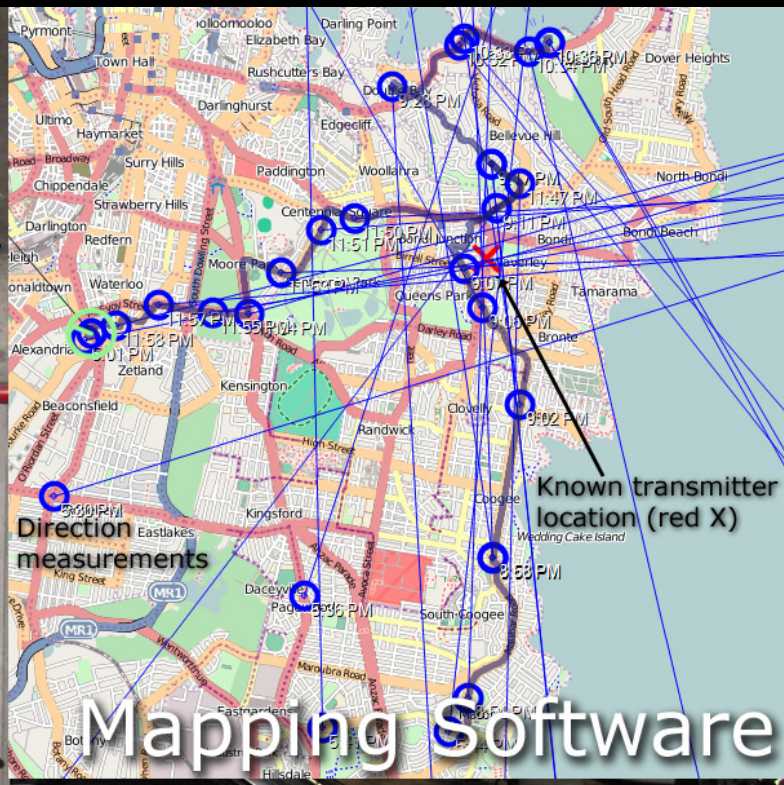
Time to go colour...



RF Hardware

Software-Defined Radio

Direction Finding



Mapping Software

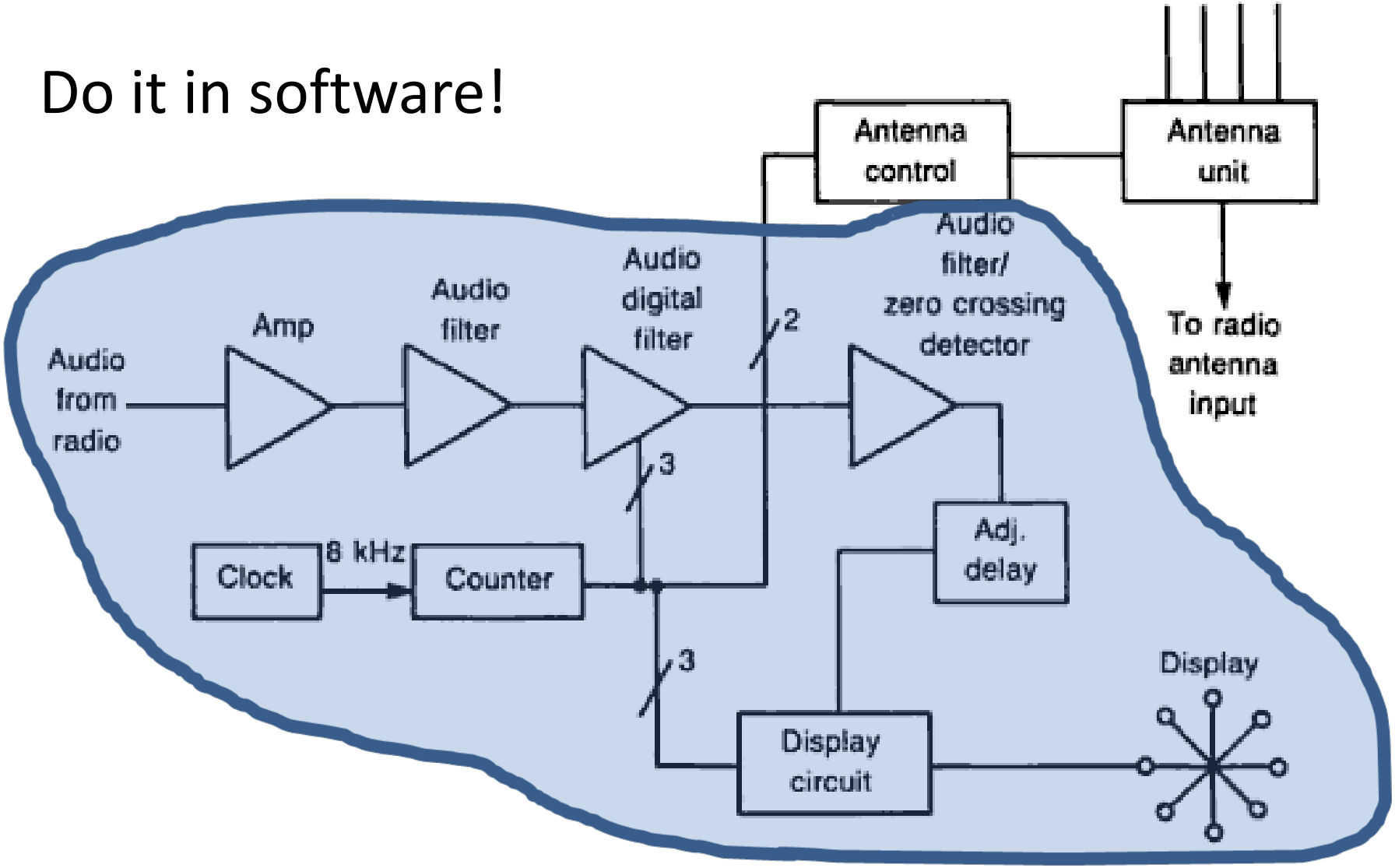
Antenna Array

The DUF-Mobile

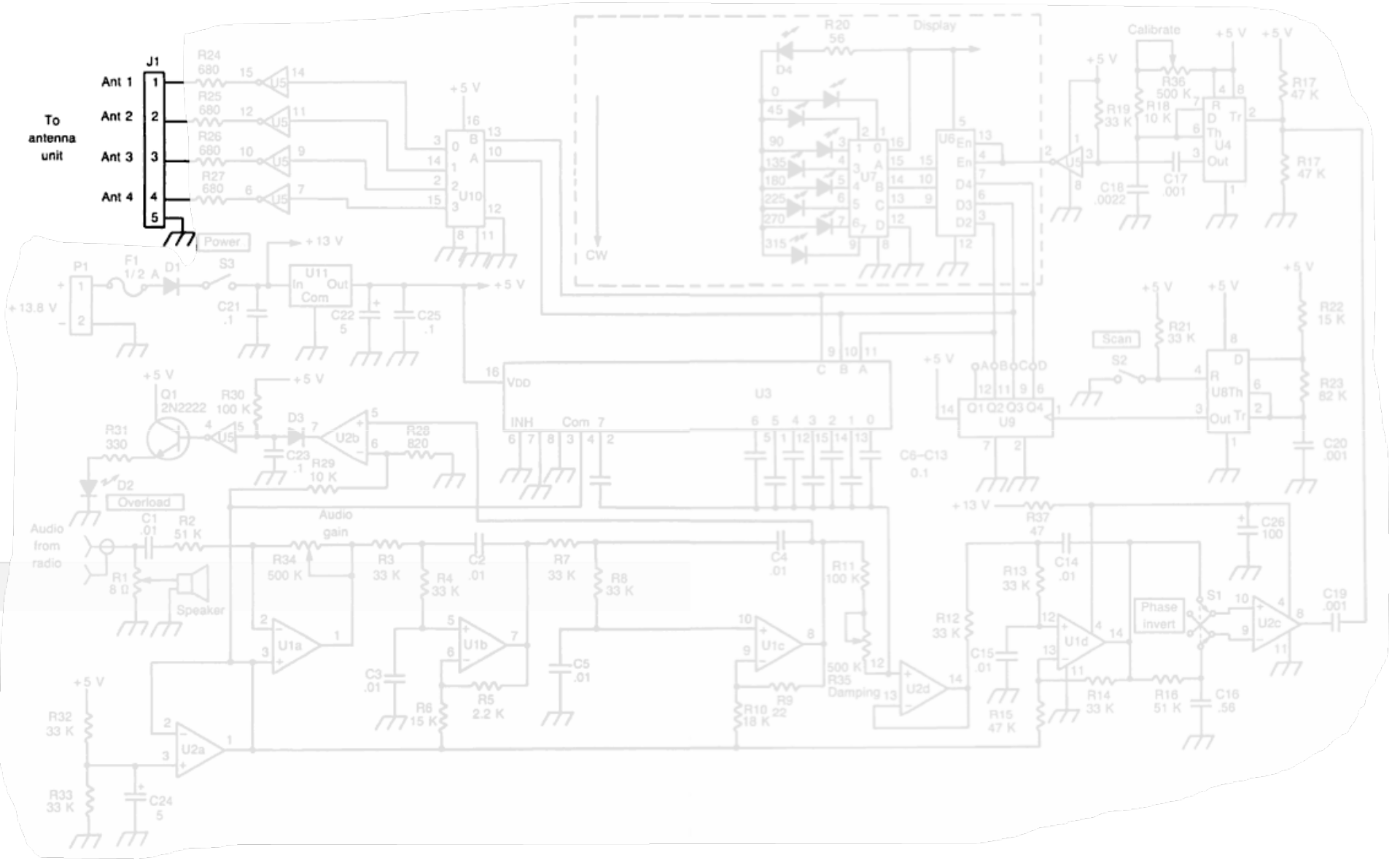
Balint Seeber
http://spench.net/

Software Defined RDF

Do it in software!

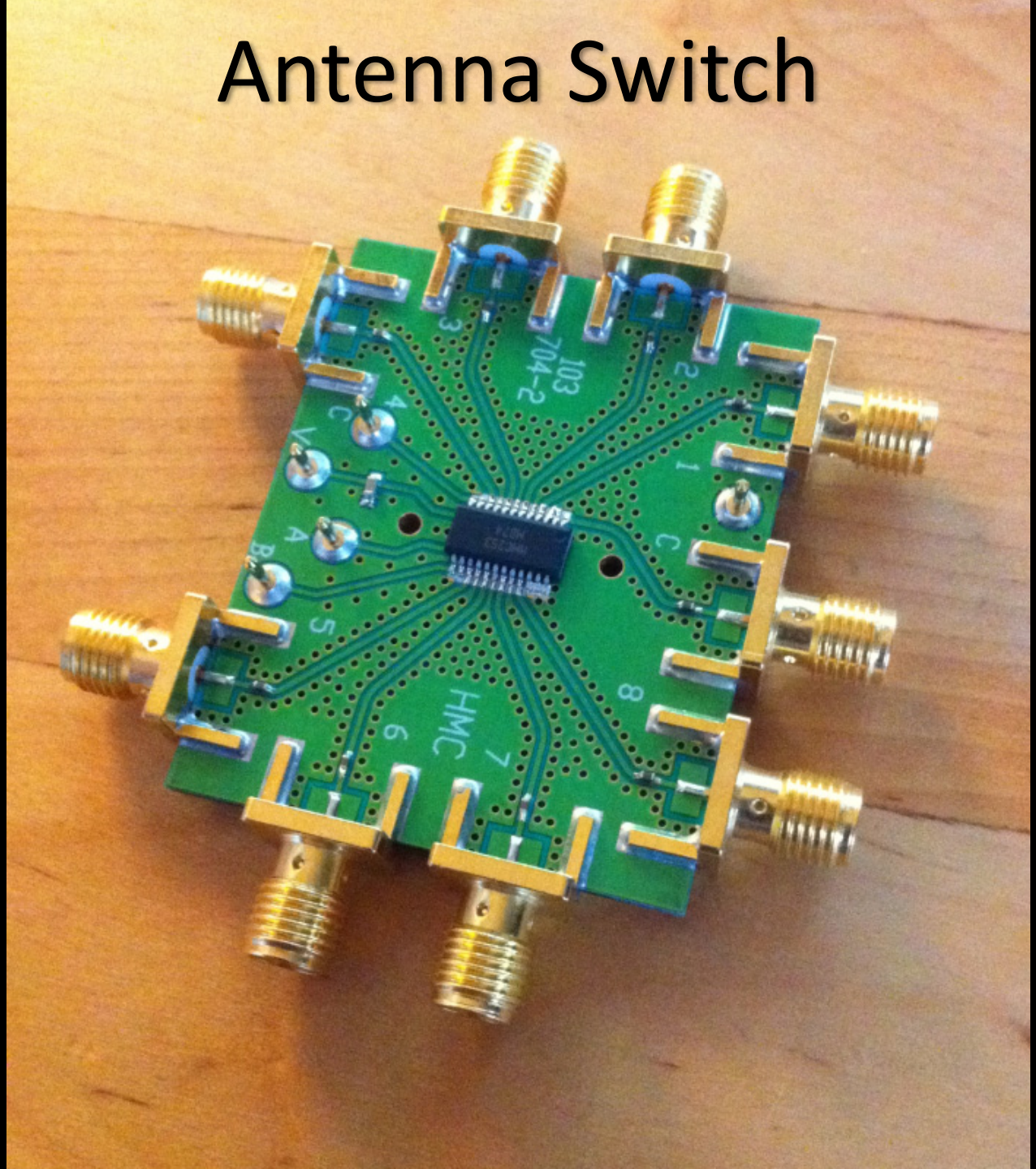


Software Defined RDF



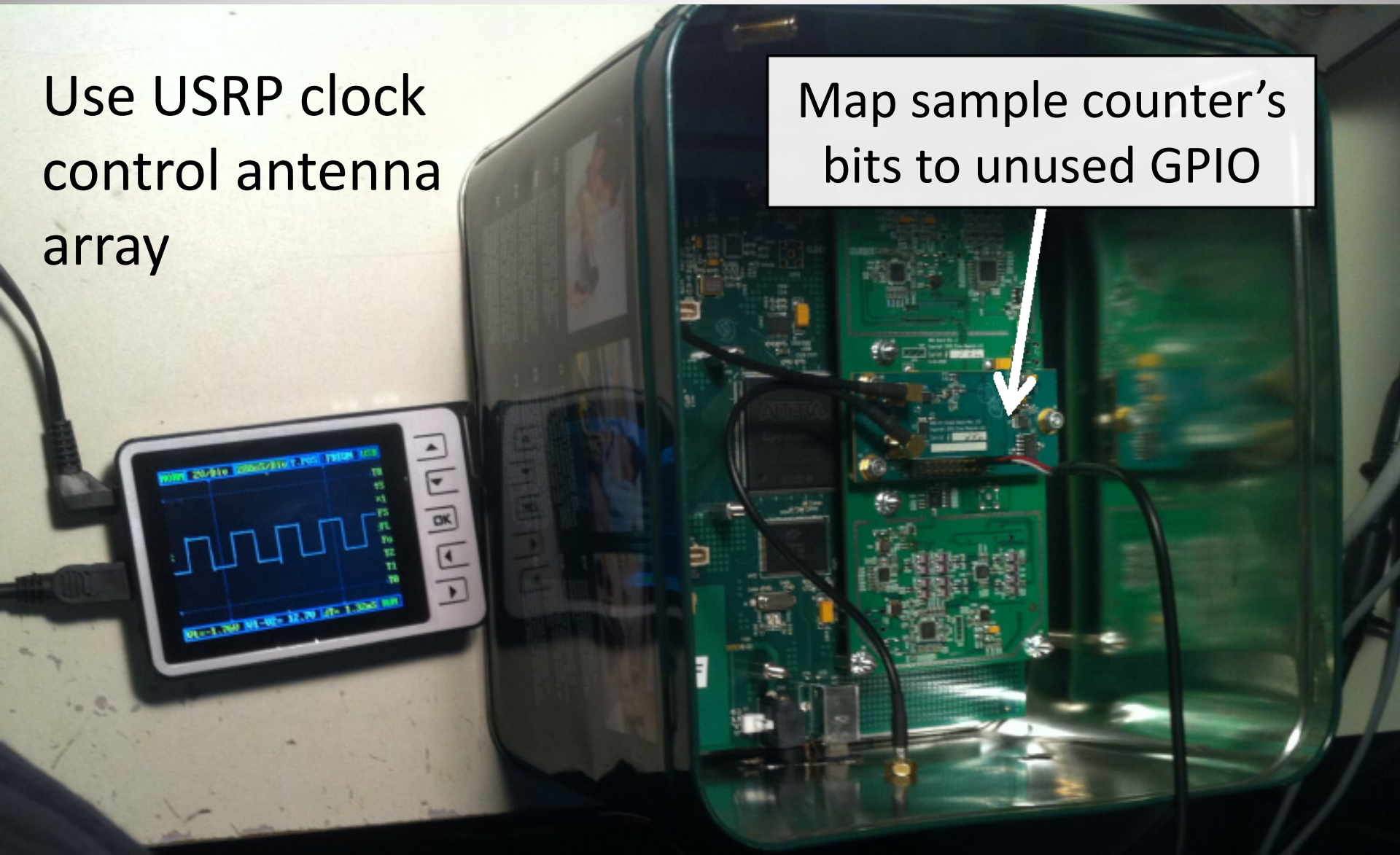

Antenna
Array

Antenna Switch



FPGA Modification

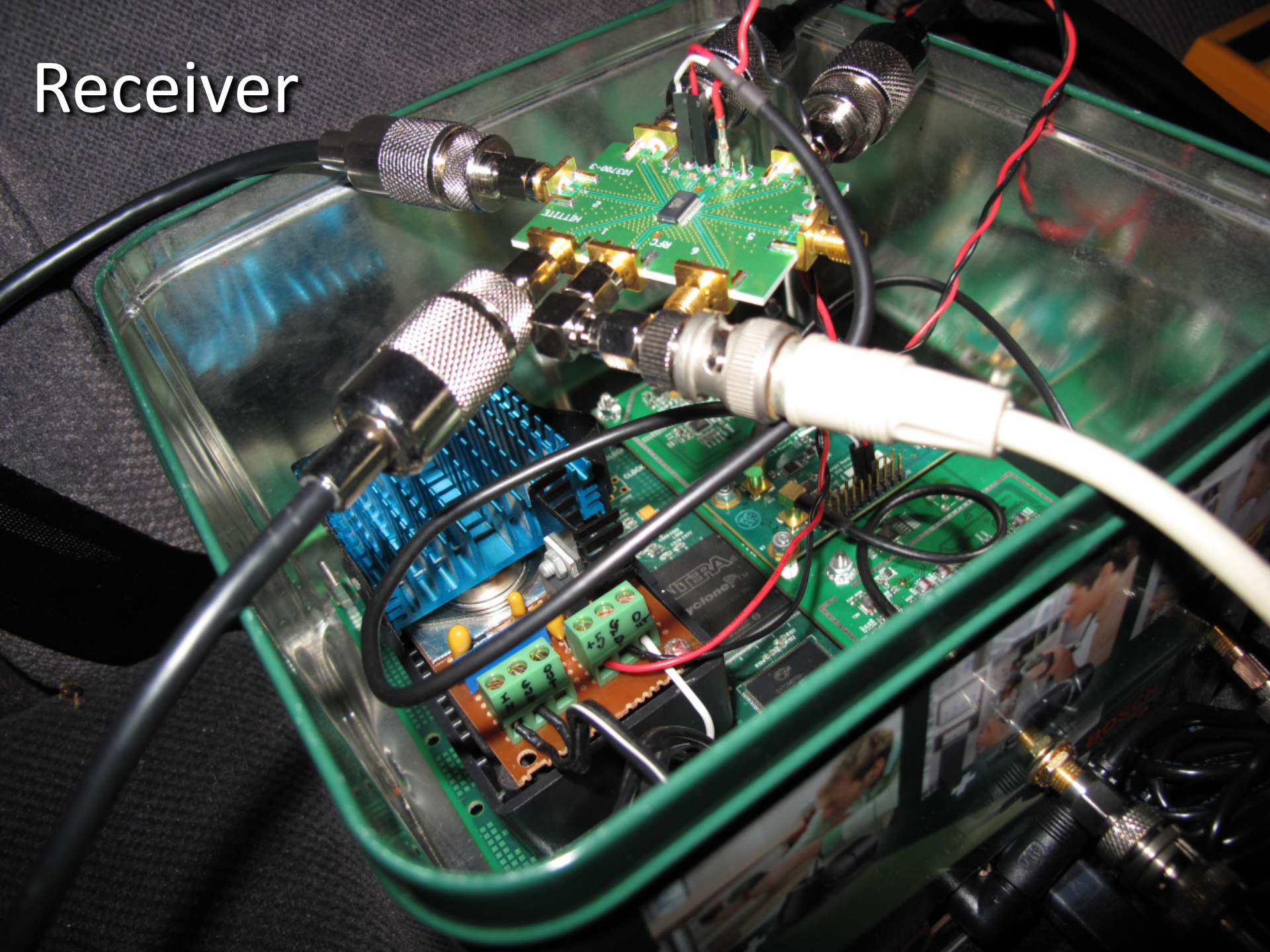
Use USRP clock control antenna array



Modification Bonuses

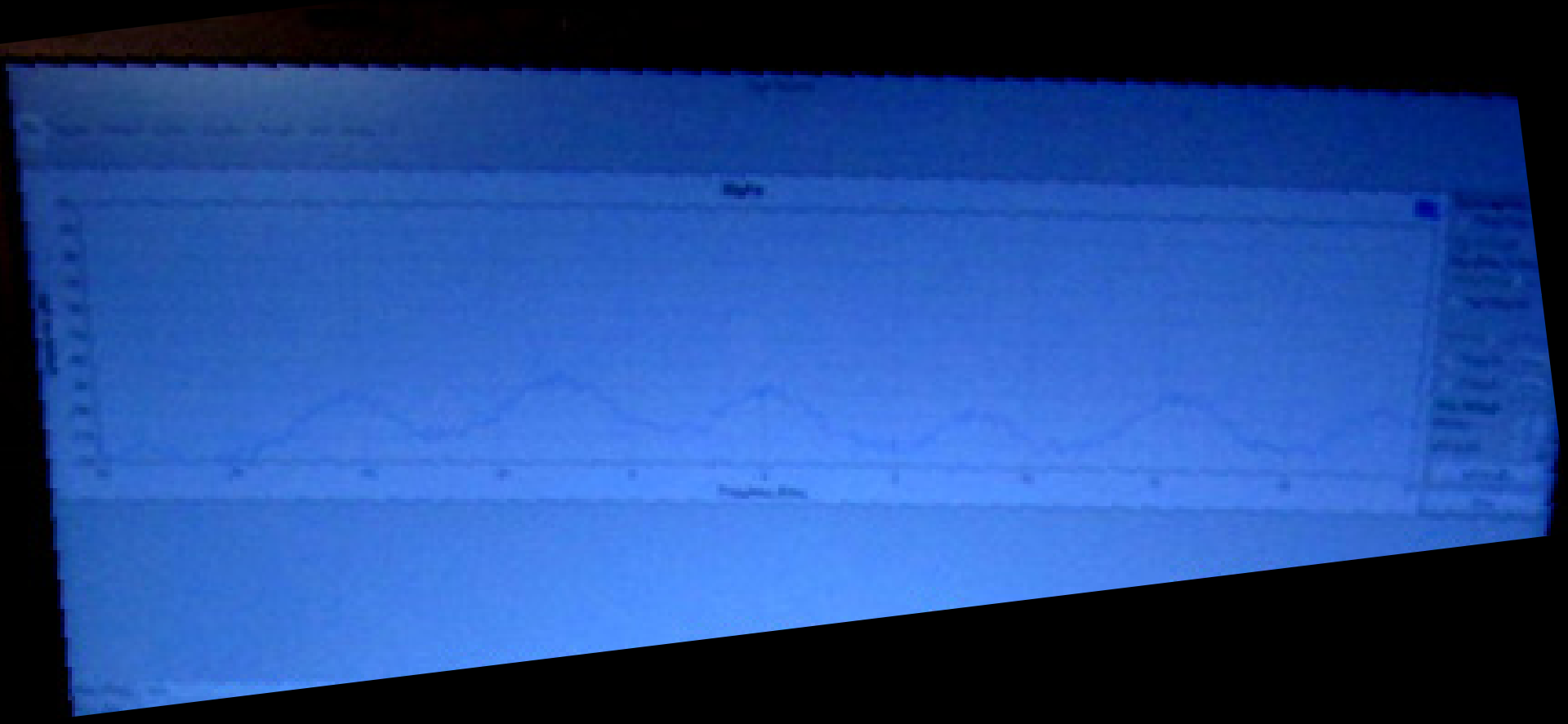
- Using FPGA clock ensures antenna switching is in lockstep with samples arriving at host
  - Same clock domain → host-side 'just works'
  - Use host-generated sine wave as reference
- FPGA's sample counter begins at zero for each stream start
  - Calibrate array orientation just once

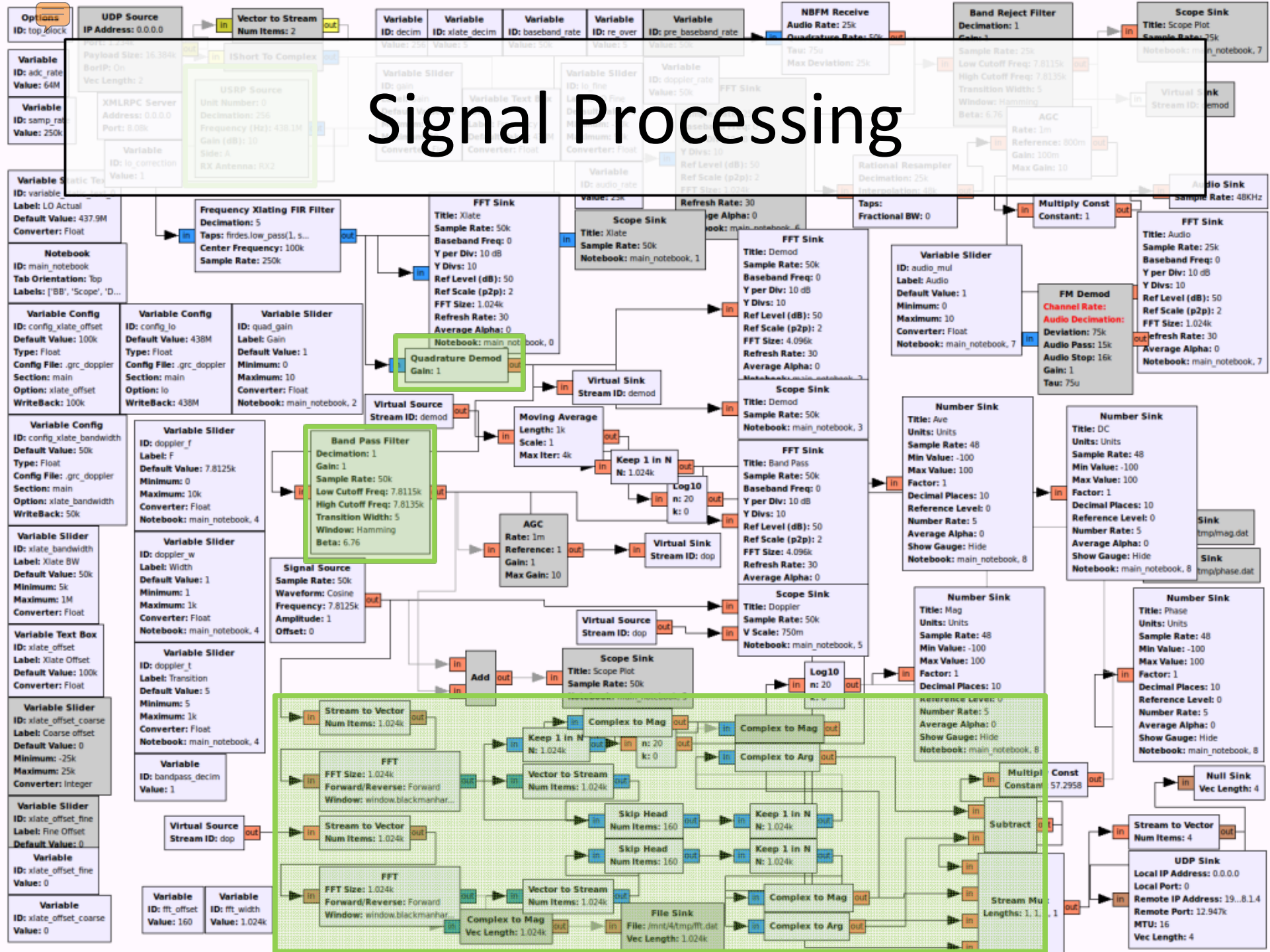
Receiver

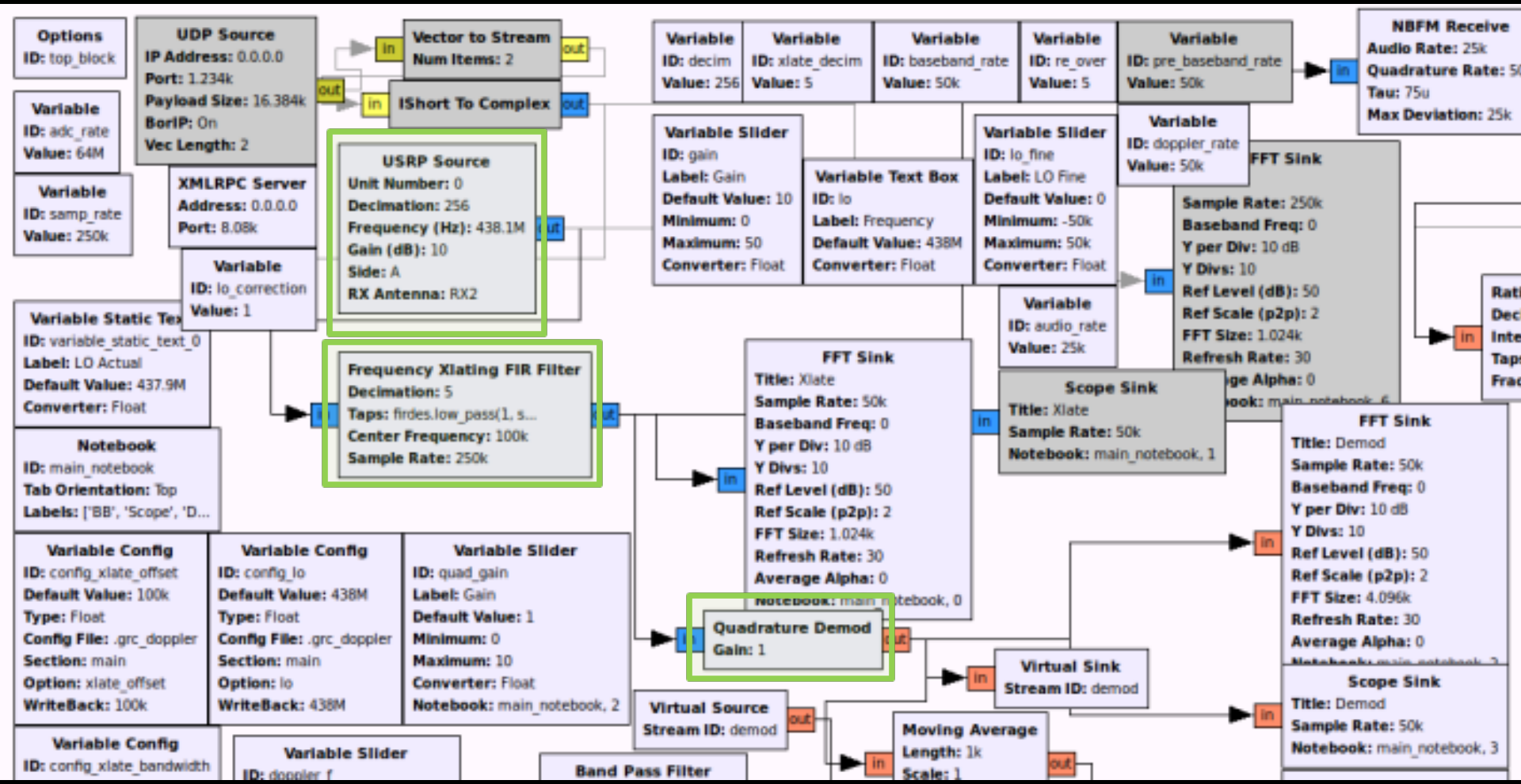



Processing & Display

Switching affecting spectrum




Signal Processing
Options
ID: top_block
UDP Source
IP Address: 0.0.0.0
Vector to Stream
Num Items: 2
Variable
ID: decim
Variable
ID: xlate_decim
Variable
ID: baseband_rate
Variable
ID: re_over
Variable
ID: pre_baseband_rate
NBFM Receive
Audio Rate: 25k
Band Reject Filter
Decimation: 1
Scope Sink
Title: Scope Plot
Variable
ID: adc_rate
Value: 64M
Variable
ID: samp_rate
Value: 250k
Frequency Xlating FIR Filter
Decimation: 5
Taps: firdes.low_pass(1, s...
Center Frequency: 100k
Sample Rate: 250k
FFT Sink
Title: Xlate
Sample Rate: 50k
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: 0
Scope Sink
Title: Xlate
Sample Rate: 50k
Baseband Freq: 0
Notebook: main_notebook, 1
Multiply Const
Constant: 1
Audio Sink
Sample Rate: 48KHz
Variable
ID: variable_static_text_0
Label: LO Actual
Default Value: 437.9M
Converter: Float
Notebook
ID: main_notebook
Tab Orientation: Top
Labels: ['BB', 'Scope', 'D...
Variable Config
ID: config_xlate_offset
Default Value: 100k
Type: Float
Config File: .grc_doppler
Section: main
Option: xlate_offset
WriteBack: 100k
Variable Config
ID: config_lo
Default Value: 438M
Type: Float
Config File: .grc_doppler
Section: main
Option: lo
WriteBack: 438M
Variable Slider
ID: quad_gain
Label: Gain
Default Value: 1
Minimum: 0
Maximum: 10
Converter: Float
Notebook: main_notebook, 2
Quadrature Demod
Gain: 1
Virtual Sink
Stream ID: demod
Virtual Source
Stream ID: demod
Moving Average
Length: 1k
Scale: 1
Max Iter: 4k
Keep 1 in N
N: 1.024k
Log10
n: 20
k: 0
FFT Sink
Title: Demod
Sample Rate: 50k
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: 0
Scope Sink
Title: Demod
Sample Rate: 50k
Notebook: main_notebook, 3
Variable Slider
ID: audio_mul
Label: Audio
Default Value: 1
Minimum: 0
Maximum: 10
Converter: Float
Notebook: main_notebook, 7
FM Demod
Channel Rate:
Audio Decimation:
Deviation: 75k
Audio Pass: 15k
Audio Stop: 16k
Gain: 1
Tau: 75u
FFT Sink
Title: Audio
Sample Rate: 25k
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: 0
Notebook: main_notebook, 7
Variable Config
ID: config_xlate_bandwidth
Default Value: 50k
Type: Float
Config File: .grc_doppler
Section: main
Option: xlate_bandwidth
WriteBack: 50k
Variable Slider
ID: doppler_f
Label: F
Default Value: 7.8125k
Minimum: 0
Maximum: 10k
Converter: Float
Notebook: main_notebook, 4
Band Pass Filter
Decimation: 1
Gain: 1
Sample Rate: 50k
Low Cutoff Freq: 7.8115k
High Cutoff Freq: 7.8135k
Transition Width: 5
Window: Hamming
Beta: 6.76
AGC
Rate: 1m
Reference: 1
Gain: 1
Max Gain: 10
Virtual Sink
Stream ID: dop
Signal Source
Sample Rate: 50k
Waveform: Cosine
Frequency: 7.8125k
Amplitude: 1
Offset: 0
Virtual Source
Stream ID: dop
FFT Sink
Title: Band Pass
Sample Rate: 50k
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: 0
Scope Sink
Title: Doppler
Sample Rate: 50k
V Scale: 750m
Notebook: main_notebook, 5
Number Sink
Title: Ave
Units: Units
Sample Rate: 48
Min Value: -100
Max Value: 100
Factor: 1
Decimal Places: 10
Reference Level: 0
Number Rate: 5
Average Alpha: 0
Show Gauge: Hide
Notebook: main_notebook, 8
Number Sink
Title: DC
Units: Units
Sample Rate: 48
Min Value: -100
Max Value: 100
Factor: 1
Decimal Places: 10
Reference Level: 0
Number Rate: 5
Average Alpha: 0
Show Gauge: Hide
Notebook: main_notebook, 8
Variable Slider
ID: doppler_w
Label: Width
Default Value: 1
Minimum: 1
Maximum: 1k
Converter: Float
Notebook: main_notebook, 4
Variable Slider
ID: xlate_bandwidth
Label: Xlate BW
Default Value: 50k
Minimum: 5k
Maximum: 1M
Converter: Float
Variable Slider
ID: doppler_t
Label: Transition
Default Value: 5
Minimum: 5
Maximum: 1k
Converter: Float
Notebook: main_notebook, 4
Variable Text Box
ID: xlate_offset
Label: Xlate Offset
Default Value: 100k
Converter: Float
Add
Scope Sink
Title: Scope Plot
Sample Rate: 50k
Log10
n: 20
Number Sink
Title: Mag
Units: Units
Sample Rate: 48
Min Value: -100
Max Value: 100
Factor: 1
Decimal Places: 10
Number Rate: 5
Average Alpha: 0
Show Gauge: Hide
Notebook: main_notebook, 8
Number Sink
Title: Phase
Units: Units
Sample Rate: 48
Min Value: -100
Max Value: 100
Factor: 1
Decimal Places: 10
Reference Level: 0
Number Rate: 5
Average Alpha: 0
Show Gauge: Hide
Notebook: main_notebook, 8
Variable Slider
ID: xlate_offset_coarse
Label: Coarse offset
Default Value: 0
Minimum: -25k
Maximum: 25k
Converter: Integer
Variable
ID: bandpass_decim
Value: 1
Stream to Vector
Num Items: 1.024k
Complex to Mag
Keep 1 in N
N: 1.024k
Complex to Mag
Complex to Arg
FFT
FFT Size: 1.024k
Forward/Reverse: Forward
Window: window.blackmanhar...
Vector to Stream
Num Items: 1.024k
Const
Null Sink
Vec Length: 4
Variable Slider
ID: xlate_offset_fine
Label: Fine Offset
Default Value: 0
Virtual Source
Stream ID: dop
Stream to Vector
Num Items: 1.024k
Skip Head
Num Items: 160
Keep 1 in N
N: 1.024k
Subtract
Stream to Vector
Num Items: 4
Variable
ID: xlate_offset_fine
Value: 0
Skip Head
Num Items: 160
Keep 1 in N
N: 1.024k
FFT
FFT Size: 1.024k
Forward/Reverse: Forward
Window: window.blackmanhar...
Vector to Stream
Num Items: 1.024k
Complex to Mag
Complex to Arg
UDP Sink
Local IP Address: 0.0.0.0
Local Port: 0
Remote IP Address: 19...8.1.4
Remote Port: 12.947k
MTU: 16
Vec Length: 4
Variable
ID: xlate_offset_coarse
Value: 0
Variable
ID: fft_offset
Value: 160
Variable
ID: fft_width
Value: 1.024k
Complex to Mag
Vec Length: 1.024k
File Sink
File: /mnt/4/tmp/fft.dat
Vec Length: 1.024k


Options
ID: top_block
UDP Source
IP Address: 0.0.0.0
Port: 1.234k
Payload Size: 16.384k
BorIP: On
Vec Length: 2
Vector to Stream
Num Items: 2
IShort To Complex
Variable
ID: adc_rate
Value: 64M
Variable
ID: samp_rate
Value: 250k
XMLRPC Server
Address: 0.0.0.0
Port: 8.08k
USRP Source
Unit Number: 0
Decimation: 256
Frequency (Hz): 438.1M
Gain (dB): 10
Side: A
RX Antenna: RX2
Variable
ID: lo_correction
Value: 1
Variable Static Tex
ID: variable_static_text_0
Label: LO Actual
Default Value: 437.9M
Converter: Float
Frequency Xlating FIR Filter
Decimation: 5
Taps: firdes.low_pass(1, s...
Center Frequency: 100k
Sample Rate: 250k
Notebook
ID: main_notebook
Tab Orientation: Top
Labels: ['BB', 'Scope', 'D...
Variable Config
ID: config_xlate_offset
Default Value: 100k
Type: Float
Config File: .grc_doppler
Section: main
Option: xlate_offset
WriteBack: 100k
Variable Config
ID: config_lo
Default Value: 438M
Type: Float
Config File: .grc_doppler
Section: main
Option: lo
WriteBack: 438M
Variable Slider
ID: quad_gain
Label: Gain
Default Value: 1
Minimum: 0
Maximum: 10
Converter: Float
Notebook: main_notebook, 2
Variable Config
ID: config_xlate_bandwidth
Variable Slider
ID: doppler_f
Band Pass Filter
Variable
ID: decim
Value: 256
Variable
ID: xlate_decim
Value: 5
Variable
ID: baseband_rate
Value: 50k
Variable
ID: re_over
Value: 5
Variable
ID: pre_baseband_rate
Value: 50k
NBFM Receive
Audio Rate: 25k
Quadrature Rate: 5
Tau: 75u
Max Deviation: 25k
Variable Slider
ID: gain
Label: Gain
Default Value: 10
Minimum: 0
Maximum: 50
Converter: Float
Variable Text Box
ID: lo
Label: Frequency
Default Value: 438M
Converter: Float
Variable Slider
ID: lo_fine
Label: LO Fine
Default Value: 0
Minimum: -50k
Maximum: 50k
Converter: Float
Variable
ID: doppler_rate
Value: 50k
FFT Sink
Sample Rate: 250k
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
Variable
ID: audio_rate
Value: 25k
FFT Sink
Title: Xlate
Sample Rate: 50k
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: 0
Scope Sink
Title: Xlate
Sample Rate: 50k
Notebook: main_notebook, 1
Quadrature Demod
Gain: 1
FFT Sink
Title: Demod
Sample Rate: 50k
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: 0
Virtual Sink
Stream ID: demod
Virtual Source
Stream ID: demod
Moving Average
Length: 1k
Scale: 1
Scope Sink
Title: Demod
Sample Rate: 50k
Notebook: main_notebook, 3

Tricks

- Only need to know:
  1. Sample rate (FPGA clock / decimation)
  2. Which bit of sample counter is MSB of switch

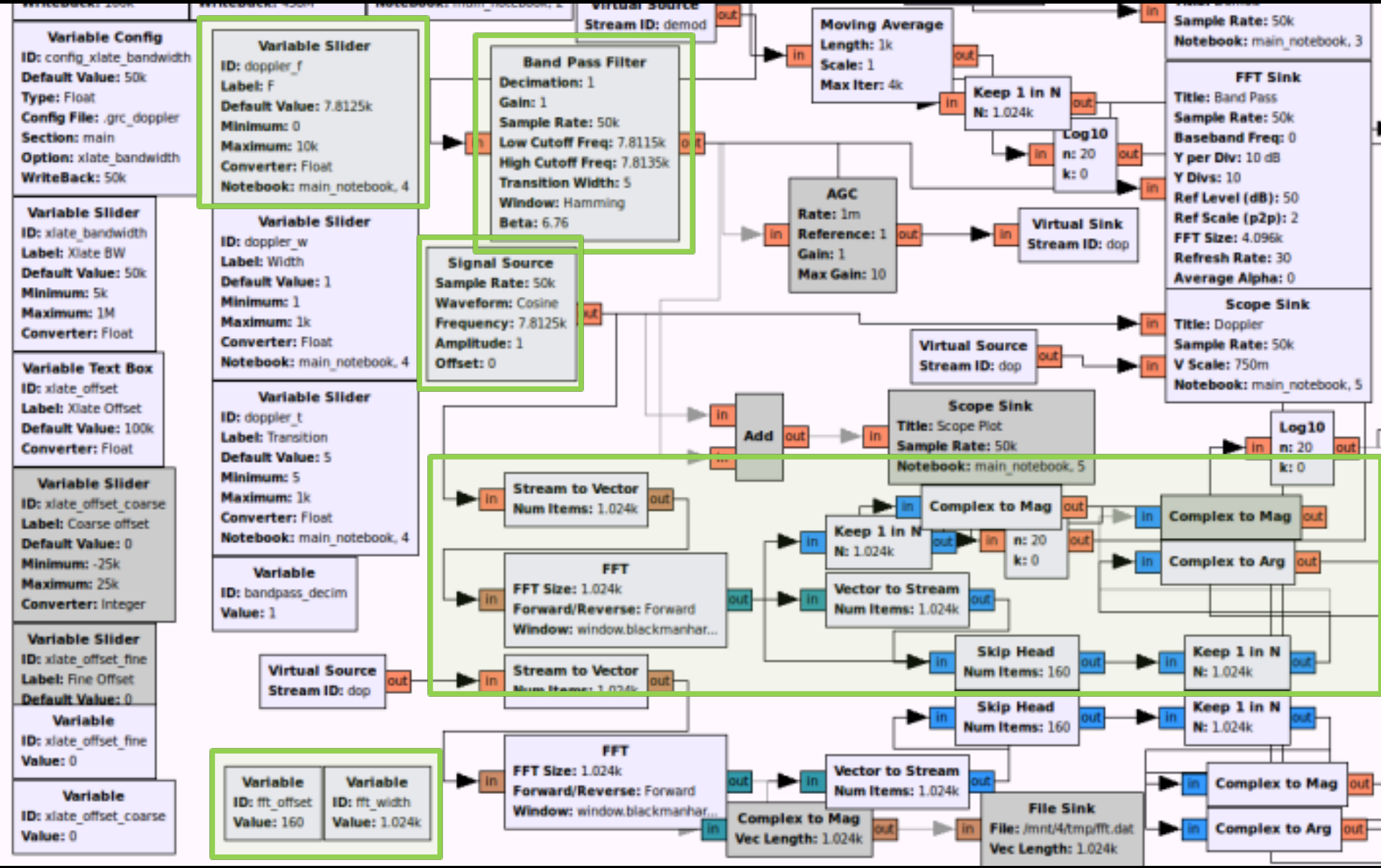
(64 MHz / 256) = **250 ksps**

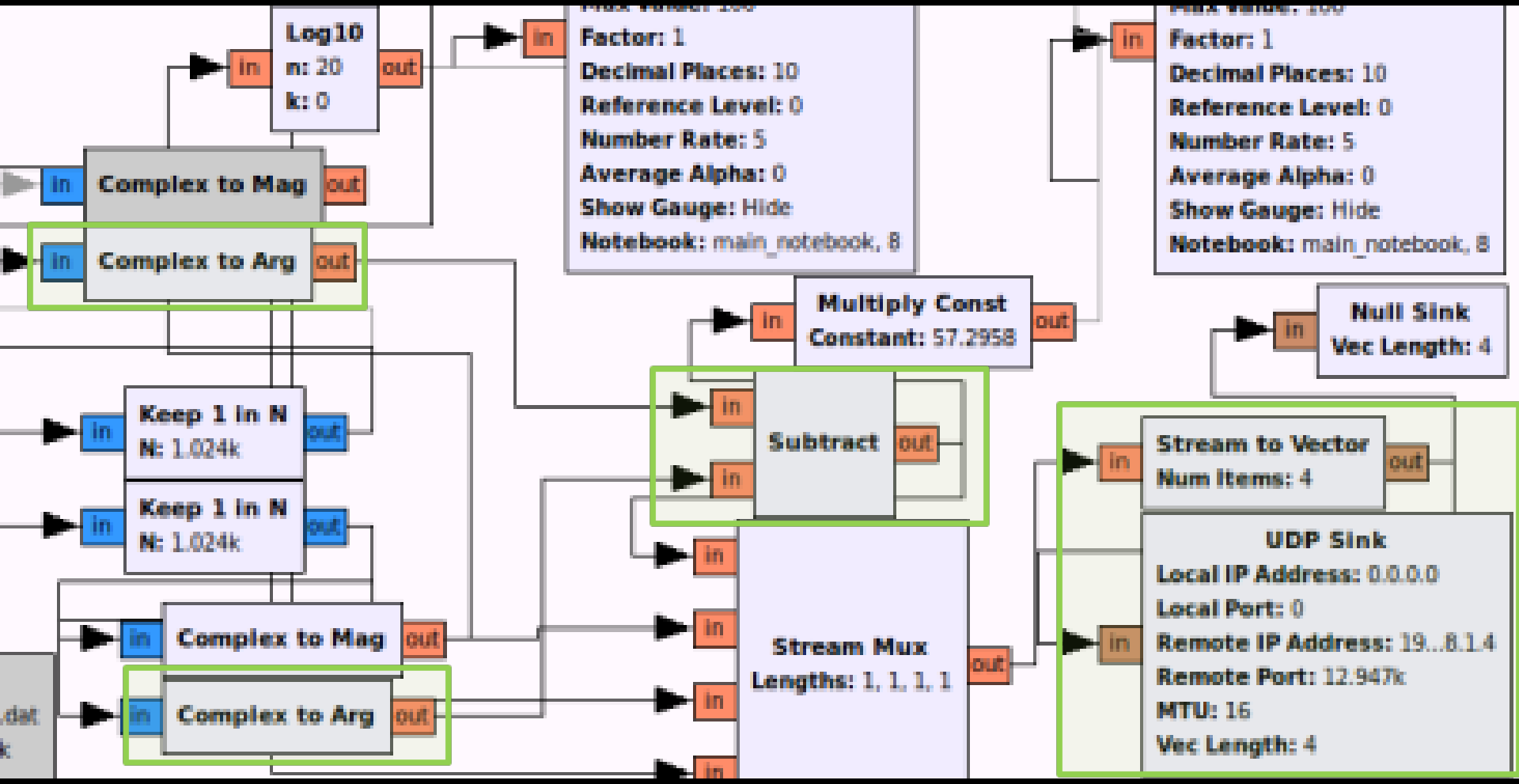
31st and **32nd** bits used

→ 250k / 32 = 7.8125 kHz tone

For Xlate **decim 5** & **1024 FFT bins**, tone sits in:

((250 ksps / 5) / 1024) * 7812.5 = **160 exactly**


Variable Config
ID: config_xlate_bandwidth
Default Value: 50k
Type: Float
Config File: .grc_doppler
Section: main
Option: xlate_bandwidth
WriteBack: 50k
Variable Slider
ID: xlate_bandwidth
Label: Xlate BW
Default Value: 50k
Minimum: 5k
Maximum: 1M
Converter: Float
Variable Text Box
ID: xlate_offset
Label: Xlate Offset
Default Value: 100k
Converter: Float
Variable Slider
ID: xlate_offset_coarse
Label: Coarse offset
Default Value: 0
Minimum: -25k
Maximum: 25k
Converter: Integer
Variable Slider
ID: xlate_offset_fine
Label: Fine Offset
Default Value: 0
Variable
ID: xlate_offset_fine
Value: 0
Variable
ID: xlate_offset_coarse
Value: 0
Variable Slider
ID: doppler_f
Label: F
Default Value: 7.8125k
Minimum: 0
Maximum: 10k
Converter: Float
Notebook: main_notebook, 4
Variable Slider
ID: doppler_w
Label: Width
Default Value: 1
Minimum: 1
Maximum: 1k
Converter: Float
Notebook: main_notebook, 4
Variable Slider
ID: doppler_t
Label: Transition
Default Value: 5
Minimum: 5
Maximum: 1k
Converter: Float
Notebook: main_notebook, 4
Variable
ID: bandpass_decim
Value: 1
Variable
ID: fft_offset
Value: 160
Variable
ID: fft_width
Value: 1.024k
Band Pass Filter
Decimation: 1
Gain: 1
Sample Rate: 50k
Low Cutoff Freq: 7.8115k
High Cutoff Freq: 7.8135k
Transition Width: 5
Window: Hamming
Beta: 6.76
Signal Source
Sample Rate: 50k
Waveform: Cosine
Frequency: 7.8125k
Amplitude: 1
Offset: 0
Virtual Source
Stream ID: demod
Moving Average
Length: 1k
Scale: 1
Max Iter: 4k
Keep 1 in N
N: 1.024k
Log10
n: 20
k: 0
AGC
Rate: 1m
Reference: 1
Gain: 1
Max Gain: 10
Virtual Sink
Stream ID: dop
Virtual Source
Stream ID: dop
Add
Scope Sink
Title: Scope Plot
Sample Rate: 50k
Notebook: main_notebook, 5
FFT Sink
Title: Band Pass
Sample Rate: 50k
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: 0
Notebook: main_notebook, 3
Scope Sink
Title: Doppler
Sample Rate: 50k
V Scale: 750m
Notebook: main_notebook, 5
Stream to Vector
Num Items: 1.024k
FFT
FFT Size: 1.024k
Forward/Reverse: Forward
Window: window.blackmanhar...
Complex to Mag
Complex to Arg
Vector to Stream
Num Items: 1.024k
Skip Head
Num Items: 160
Complex to Mag
Vec Length: 1.024k
File Sink
File: /mnt/4/tmp/fft.dat
Vec Length: 1.024k


Log10
n: 20
k: 0
in
out
Complex to Mag
Complex to Arg
Keep 1 in N
N: 1.024k
Keep 1 in N
N: 1.024k
Complex to Mag
Complex to Arg
Factor: 1
Decimal Places: 10
Reference Level: 0
Number Rate: 5
Average Alpha: 0
Show Gauge: Hide
Notebook: main_notebook, 8
Multiply Const
Constant: 57.2958
Subtract
Stream Mux
Lengths: 1, 1, 1, 1
Factor: 1
Decimal Places: 10
Reference Level: 0
Number Rate: 5
Average Alpha: 0
Show Gauge: Hide
Notebook: main_notebook, 8
Null Sink
Vec Length: 4
Stream to Vector
Num Items: 4
UDP Sink
Local IP Address: 0.0.0.0
Local Port: 0
Remote IP Address: 19...8.1.4
Remote Port: 12.947k
MTU: 16
Vec Length: 4

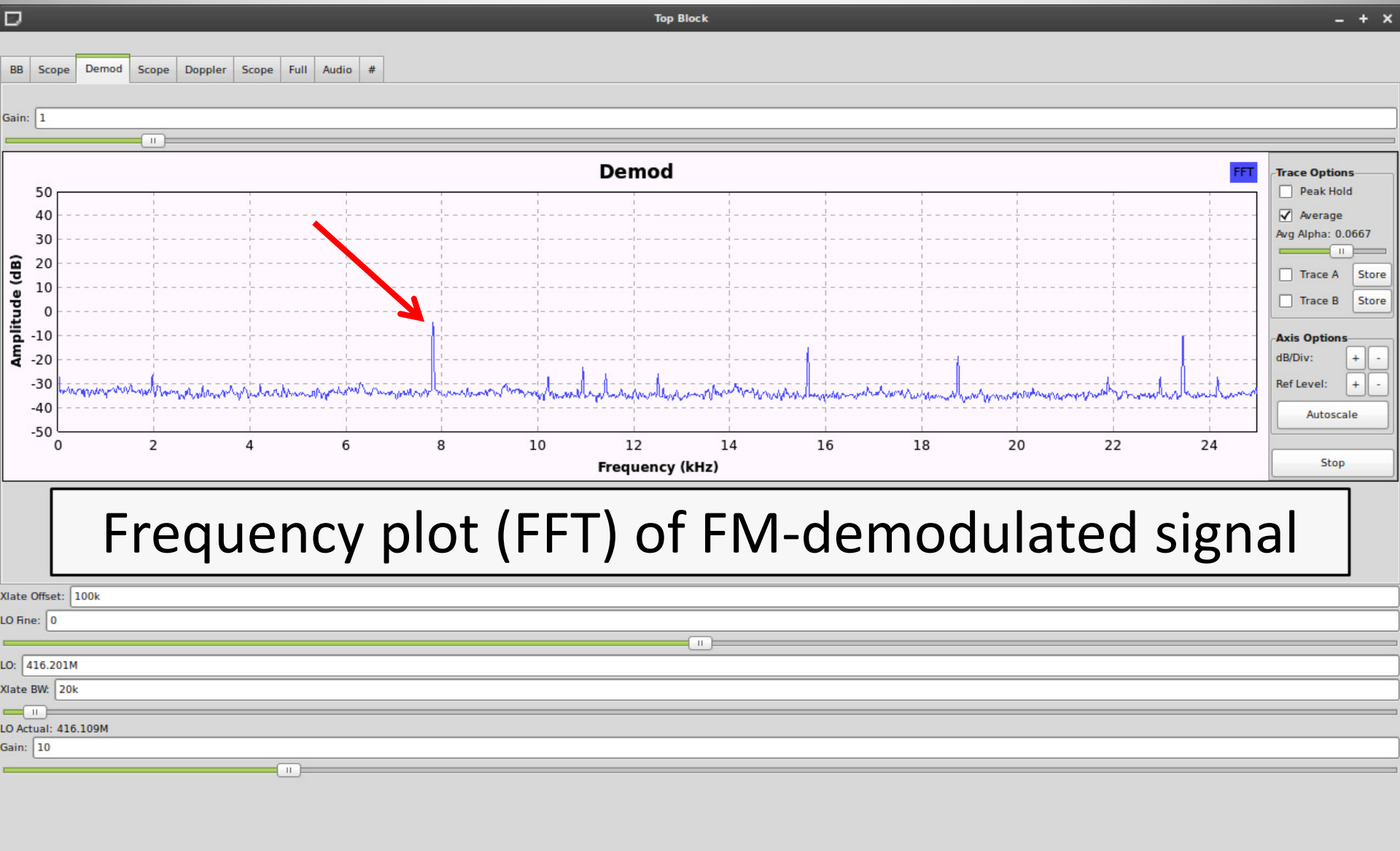
Magic of SDR

FM (quadrature) demodulation:

→ Multiply current signal sample by complex conjugate of previous one and find the argument (angle)

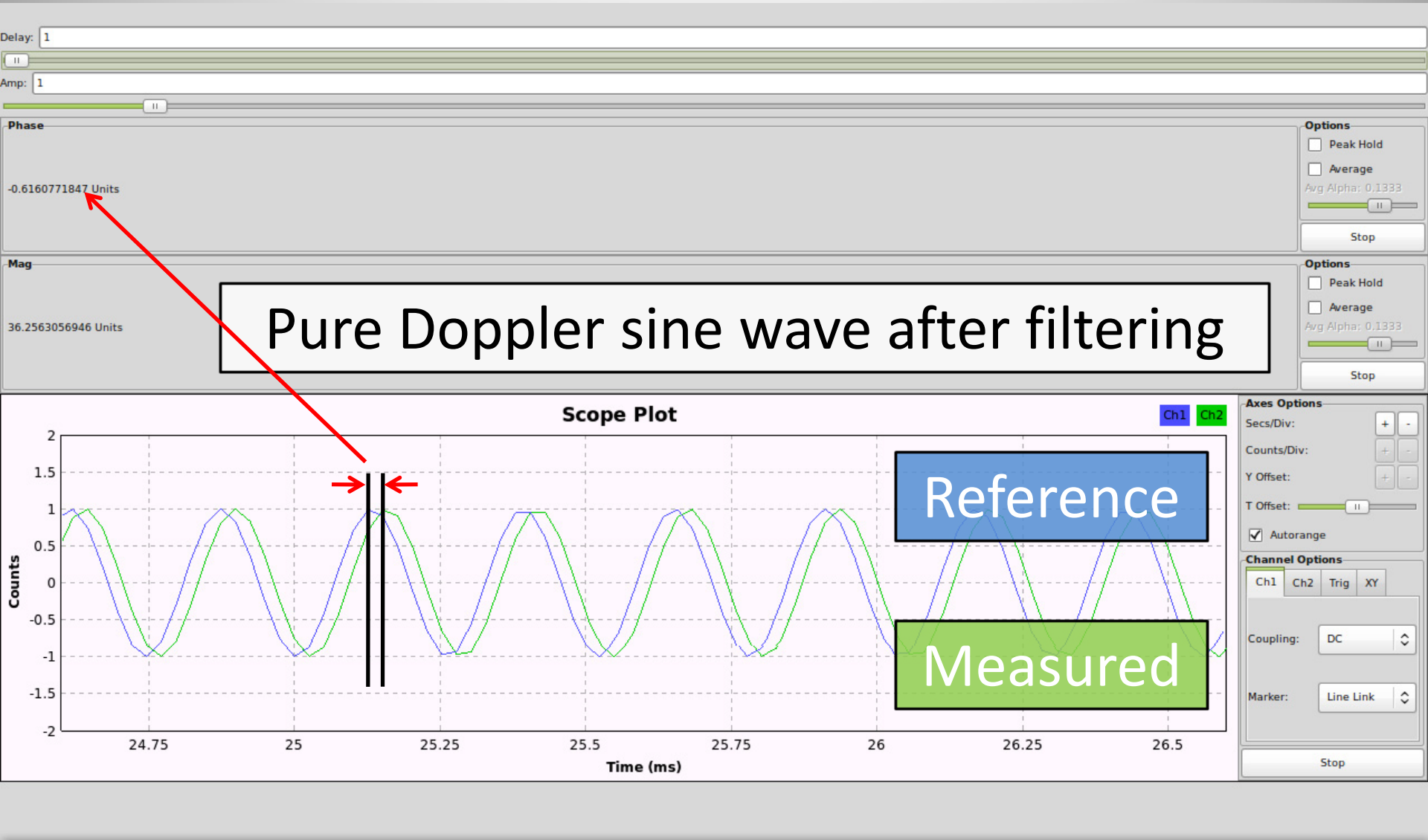
```
 for (int i = 0; i < noutput_items; i++) {
    gr_complex product = in[i] * conj(in[i-1]);
    out[i] = d_gain * arg (product);
}
```

Doppler sine wave



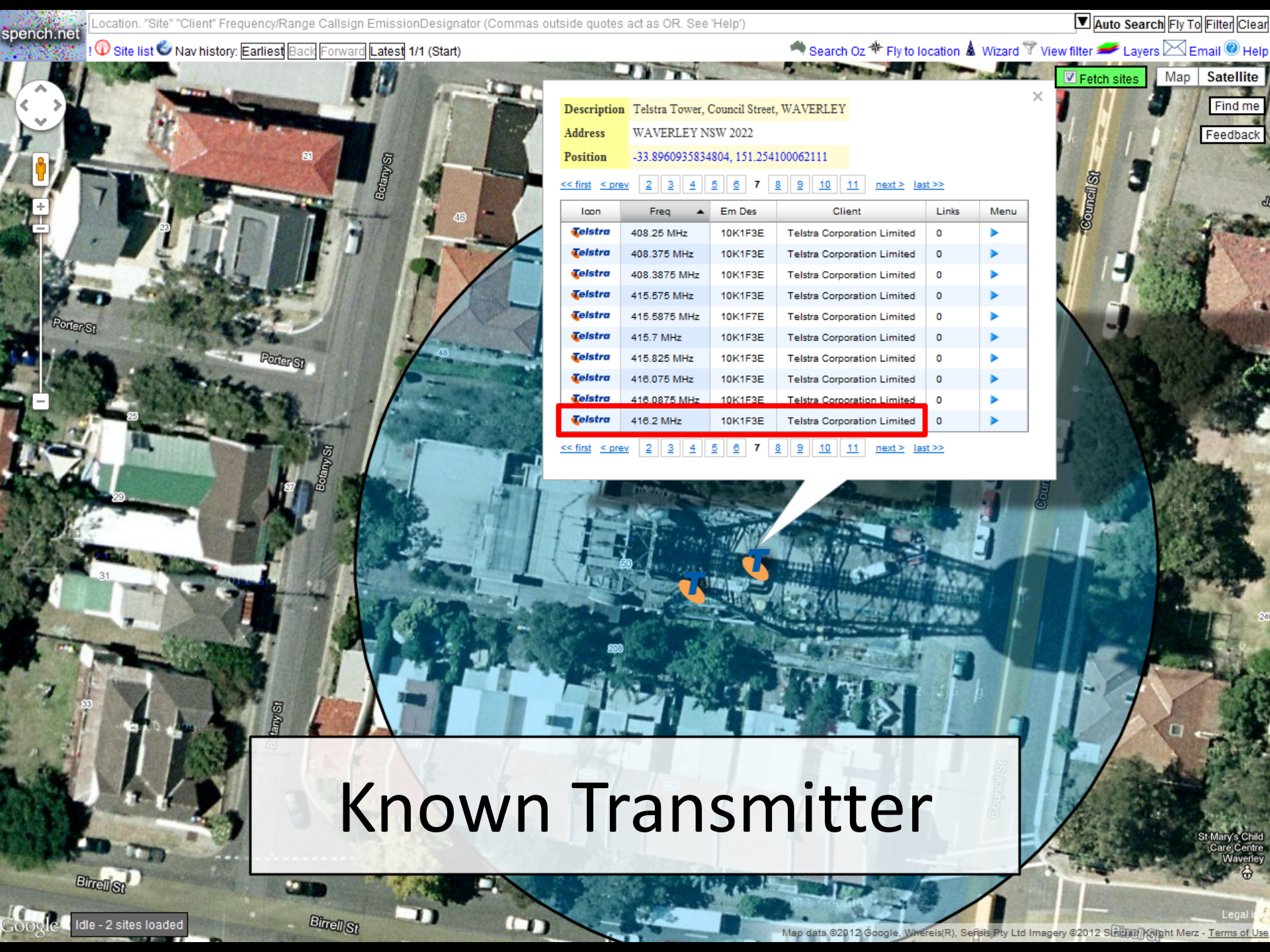
Frequency plot (FFT) of FM-demodulated signal

Doppler sine wave



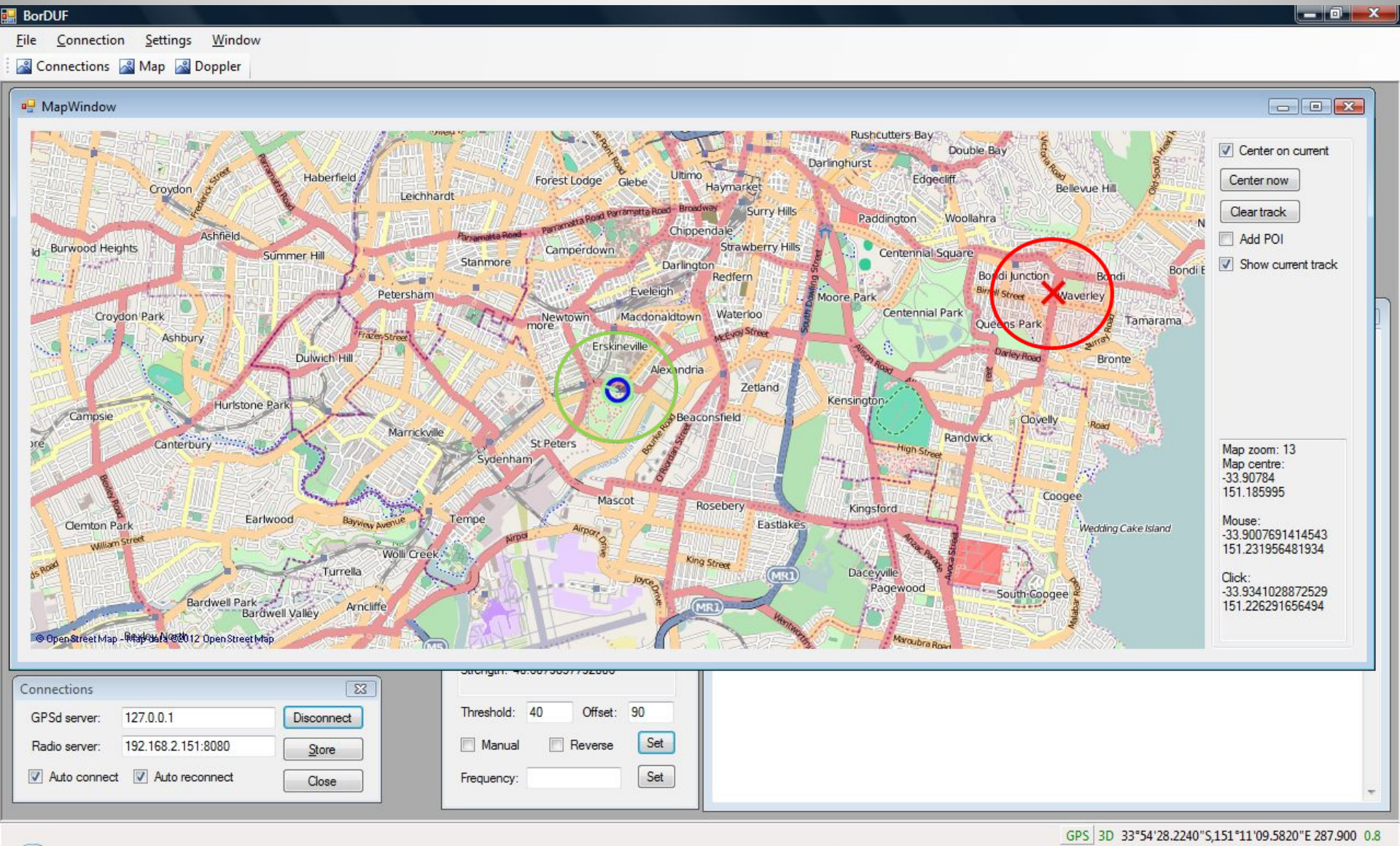

Find a target


Telstra Tower on Council St

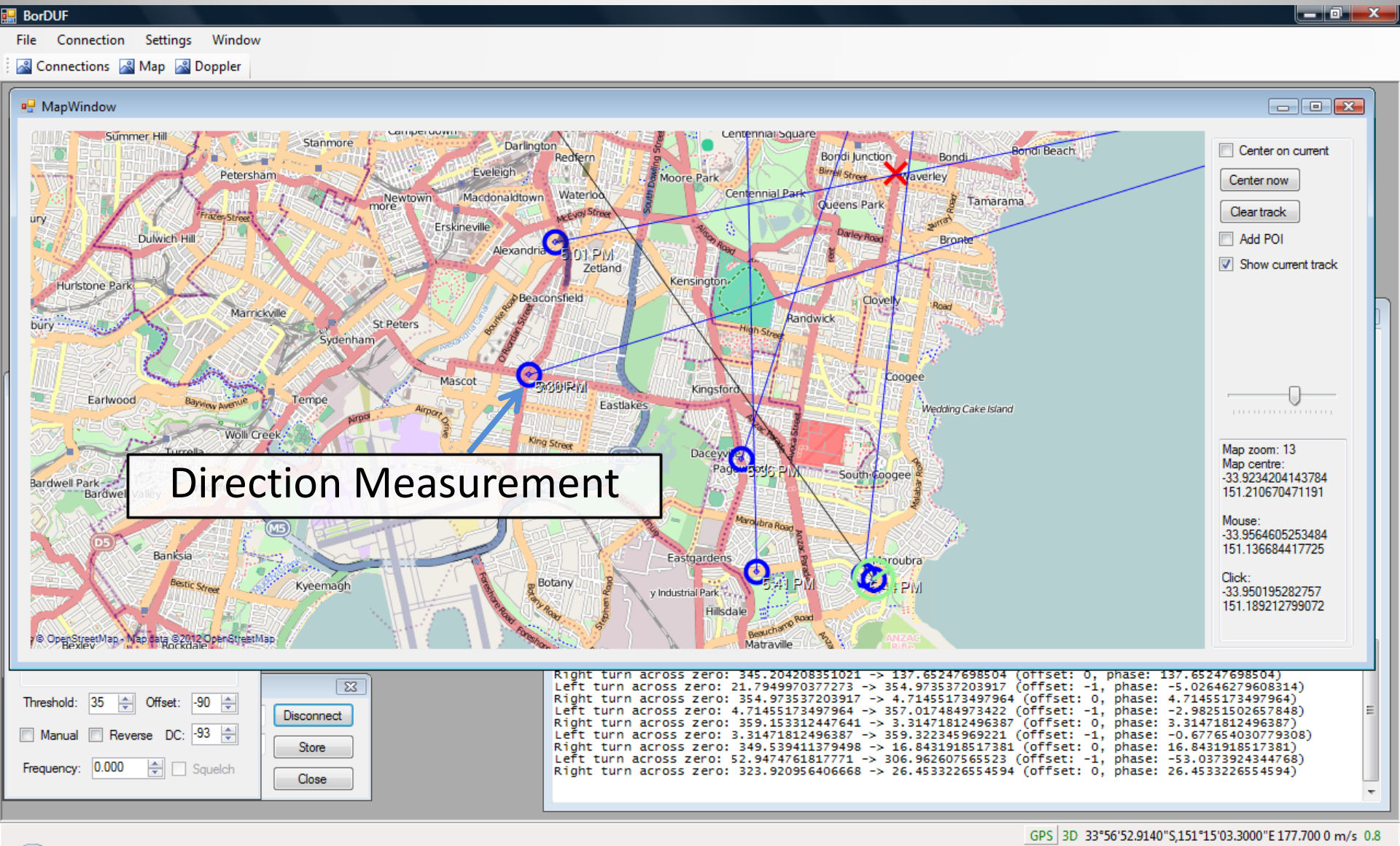


Known Transmitter

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

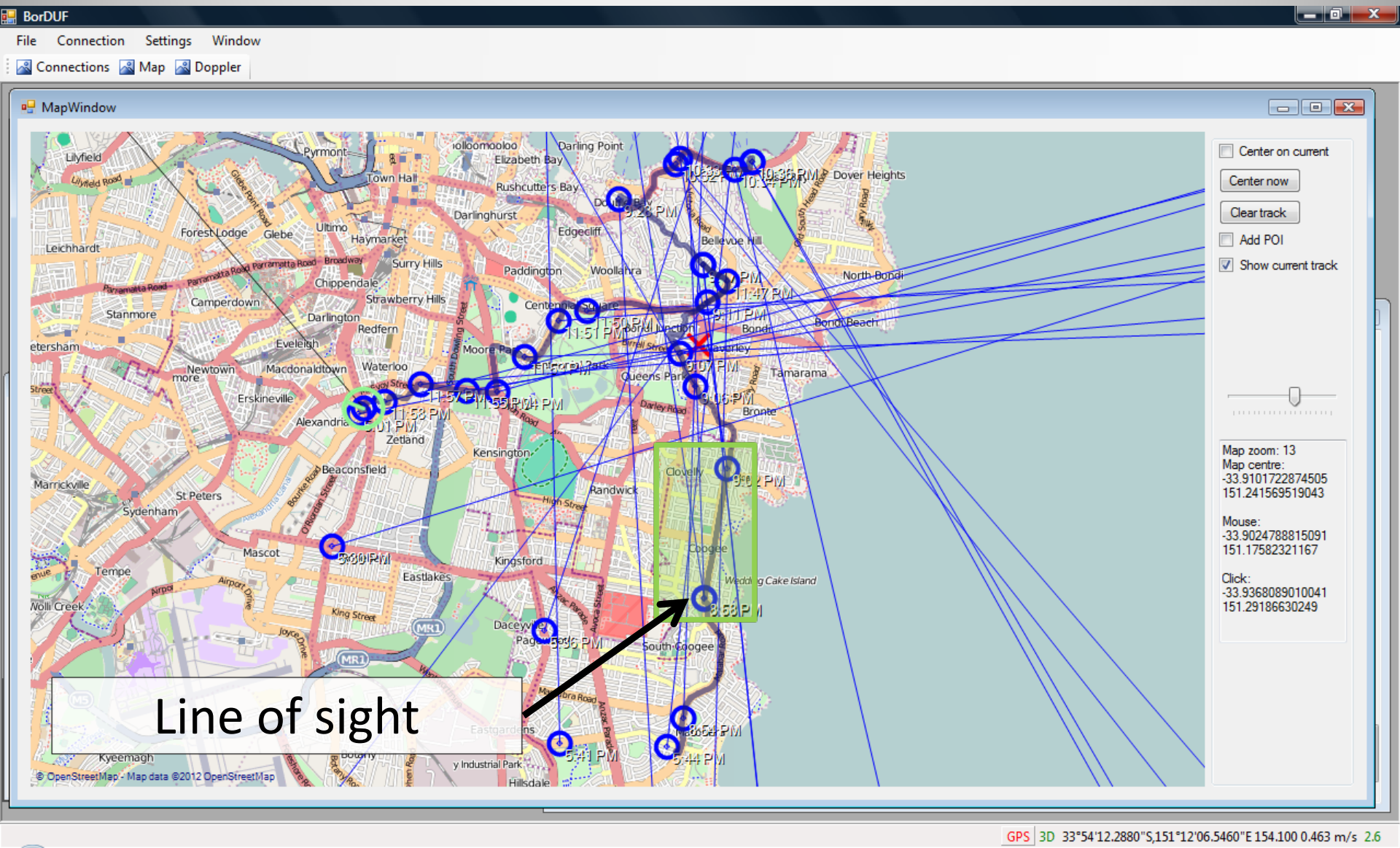
Drive


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

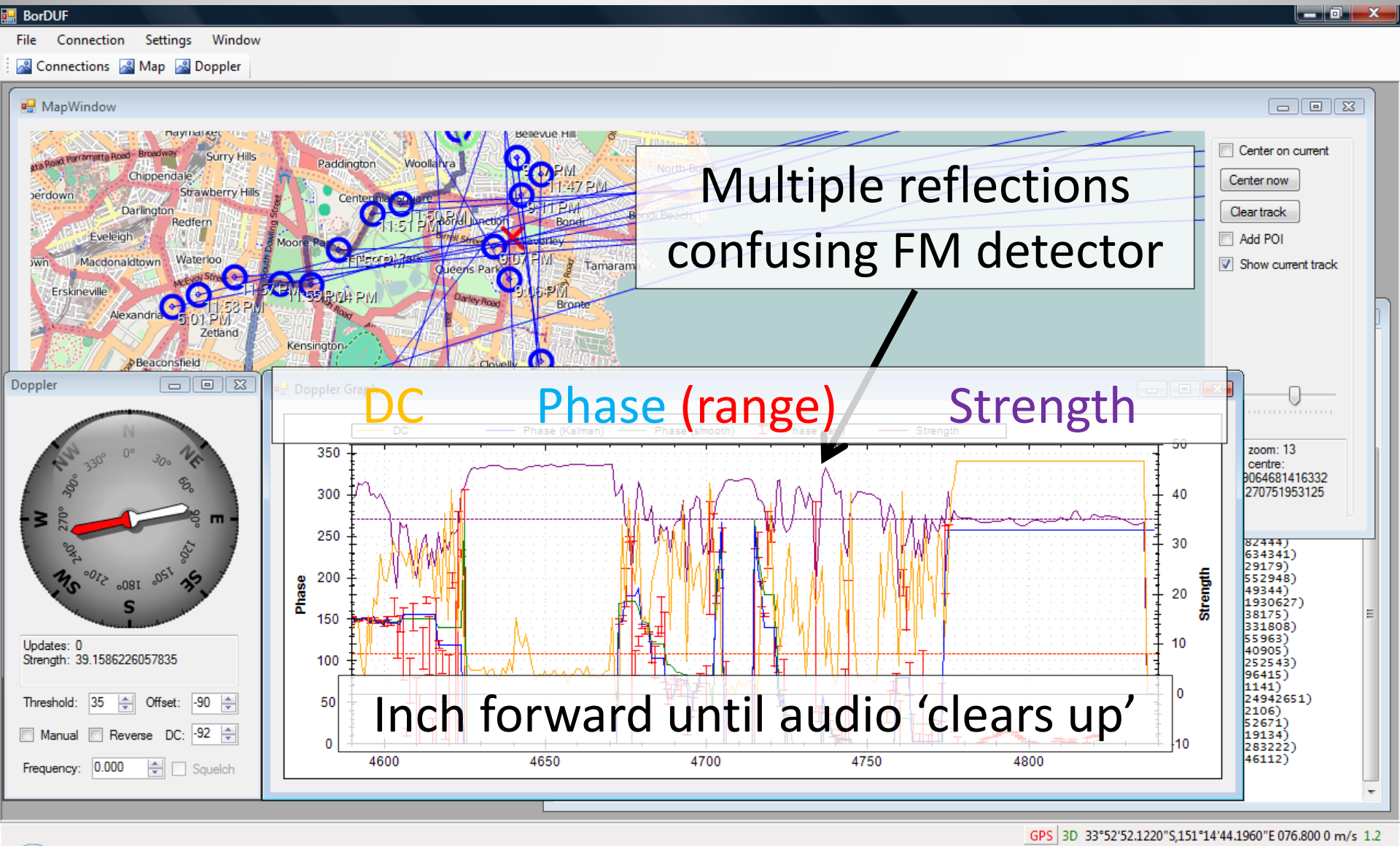
Complications

- Line-Of-Sight
  - Beware of reflections
    - Descending into ‘valley’…
  - Reflections in urban areas
  - Multiple wavefronts will ‘confuse’ FM detector
    - Doppler

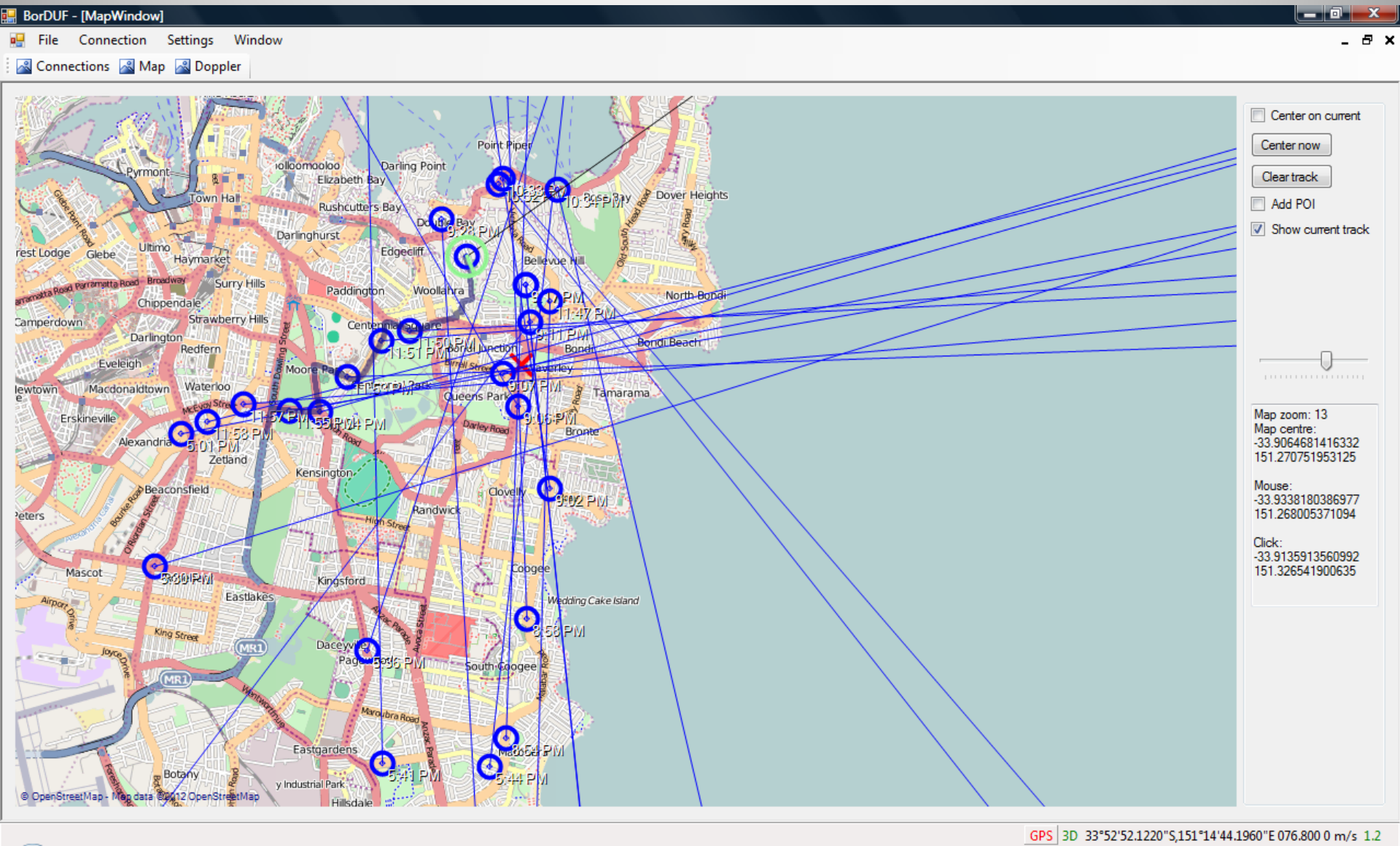
Complications: Coogee



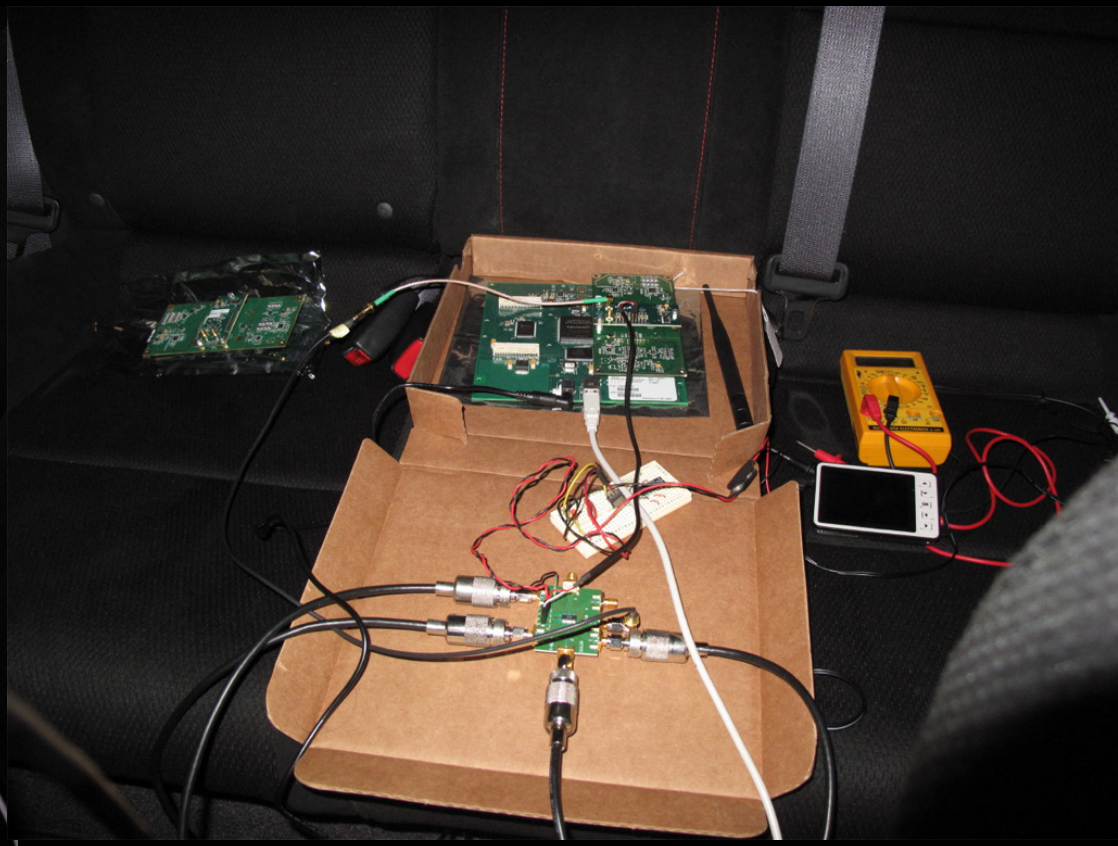
Listen: Multipath



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

Closer to (my new) home

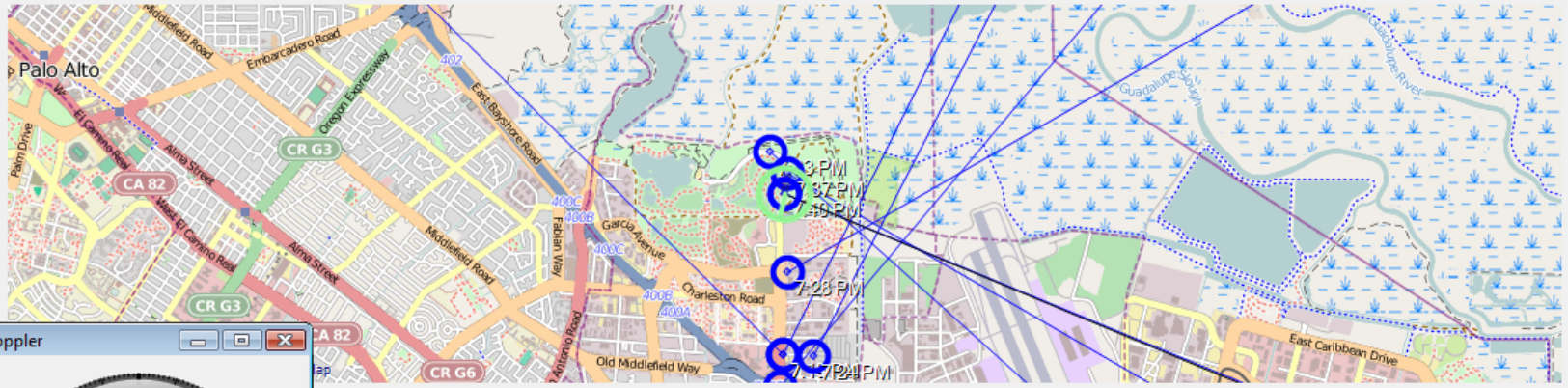


BorDUF

File Connection Settings Window

Connections Map Doppler

MapWindow



Center on current

Center now

Clear track

Add POI

Show current track

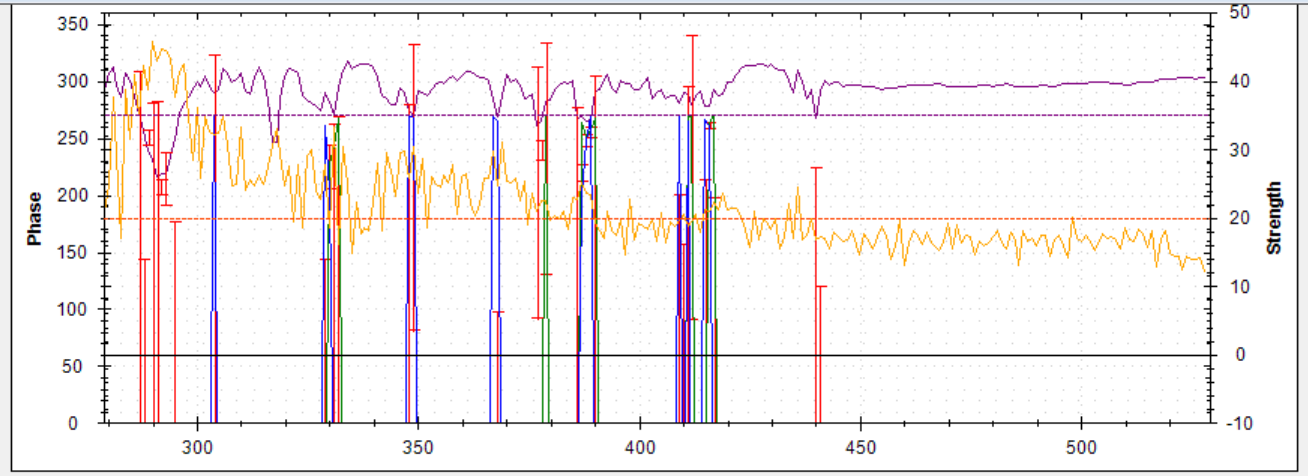
Doppler

Updates: 43
Strength: 40.4121494123098

Threshold: 35 Offset: -90

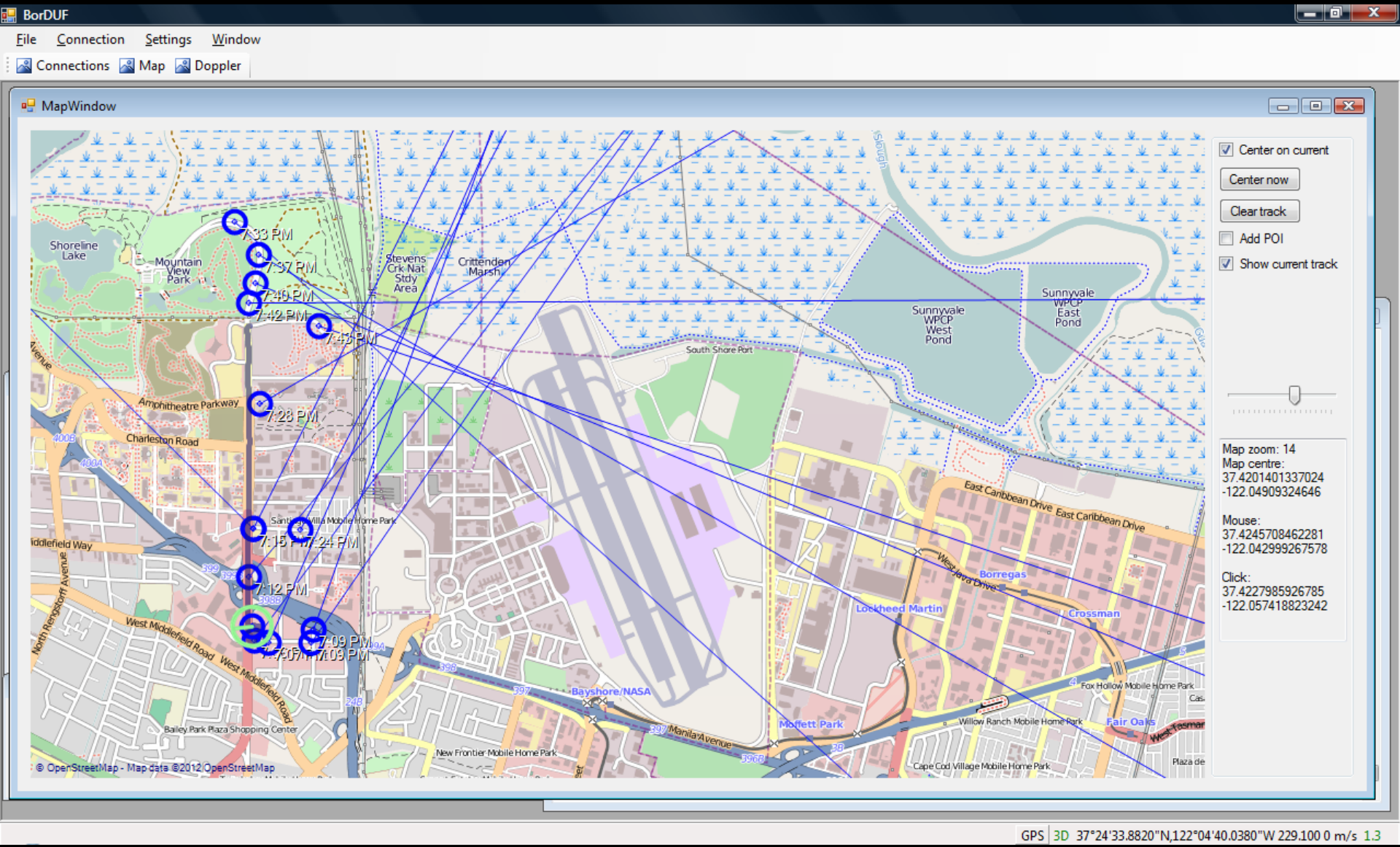
Manual Reverse DC: -80

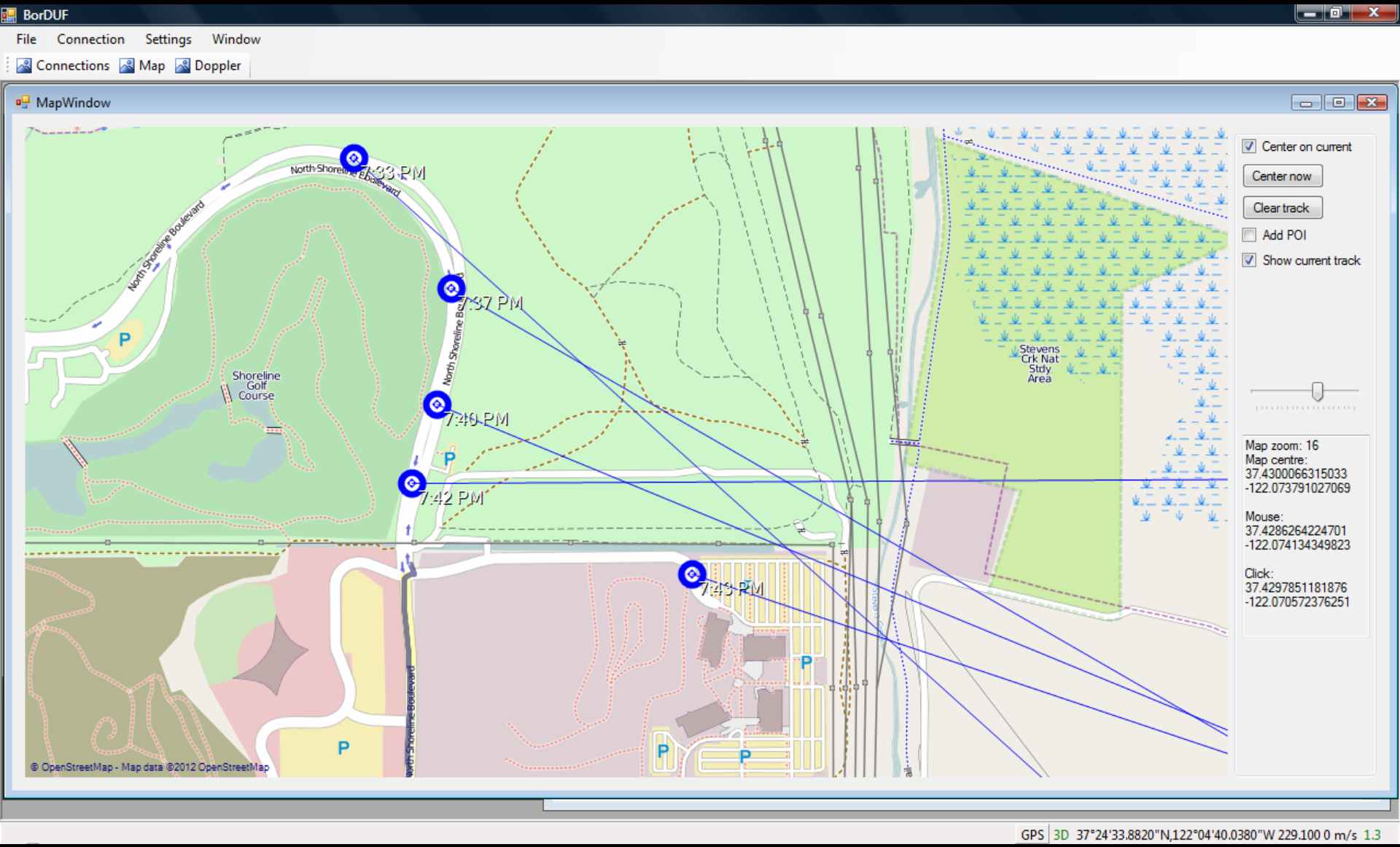
Frequency: 0.000 Squelch

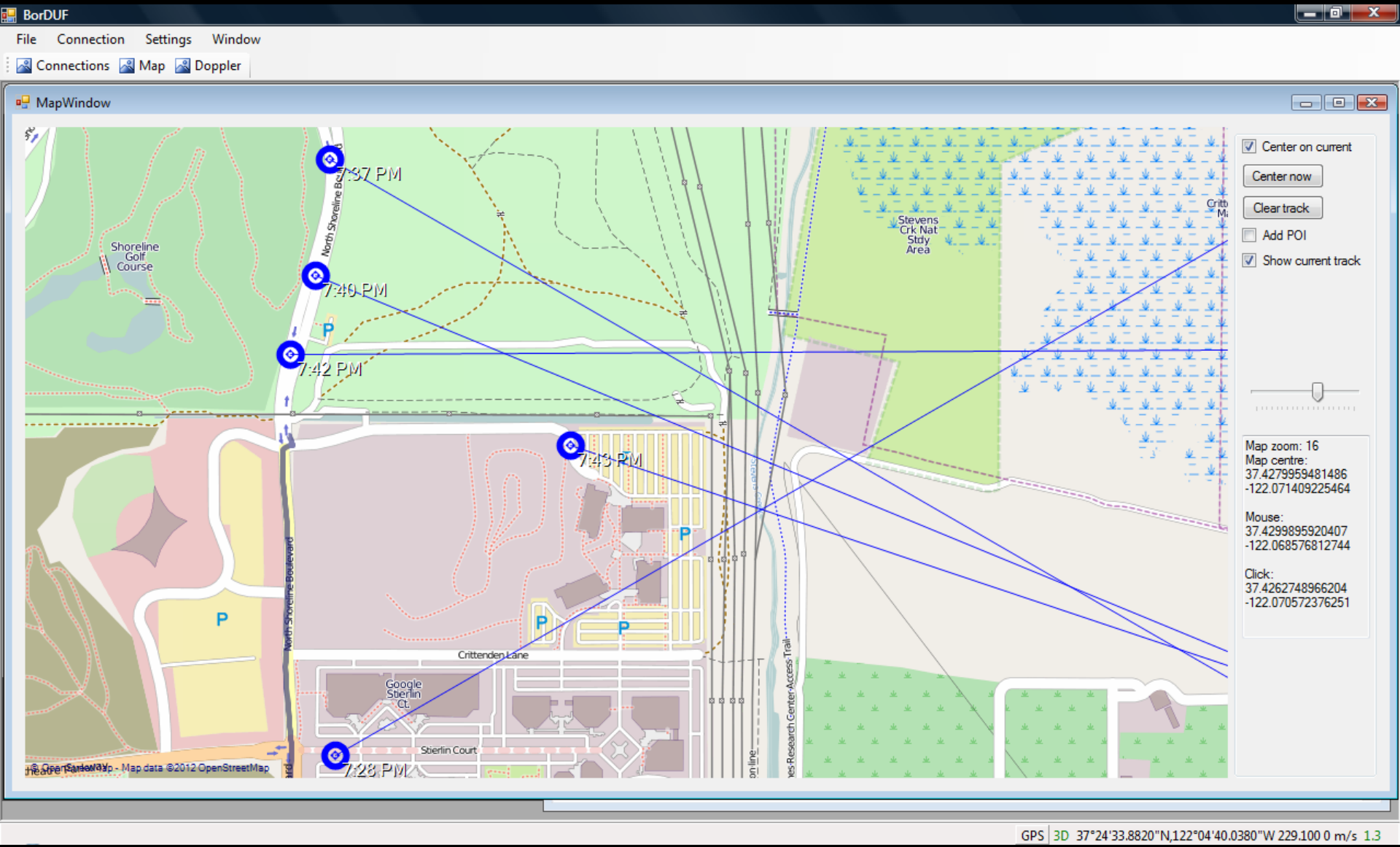


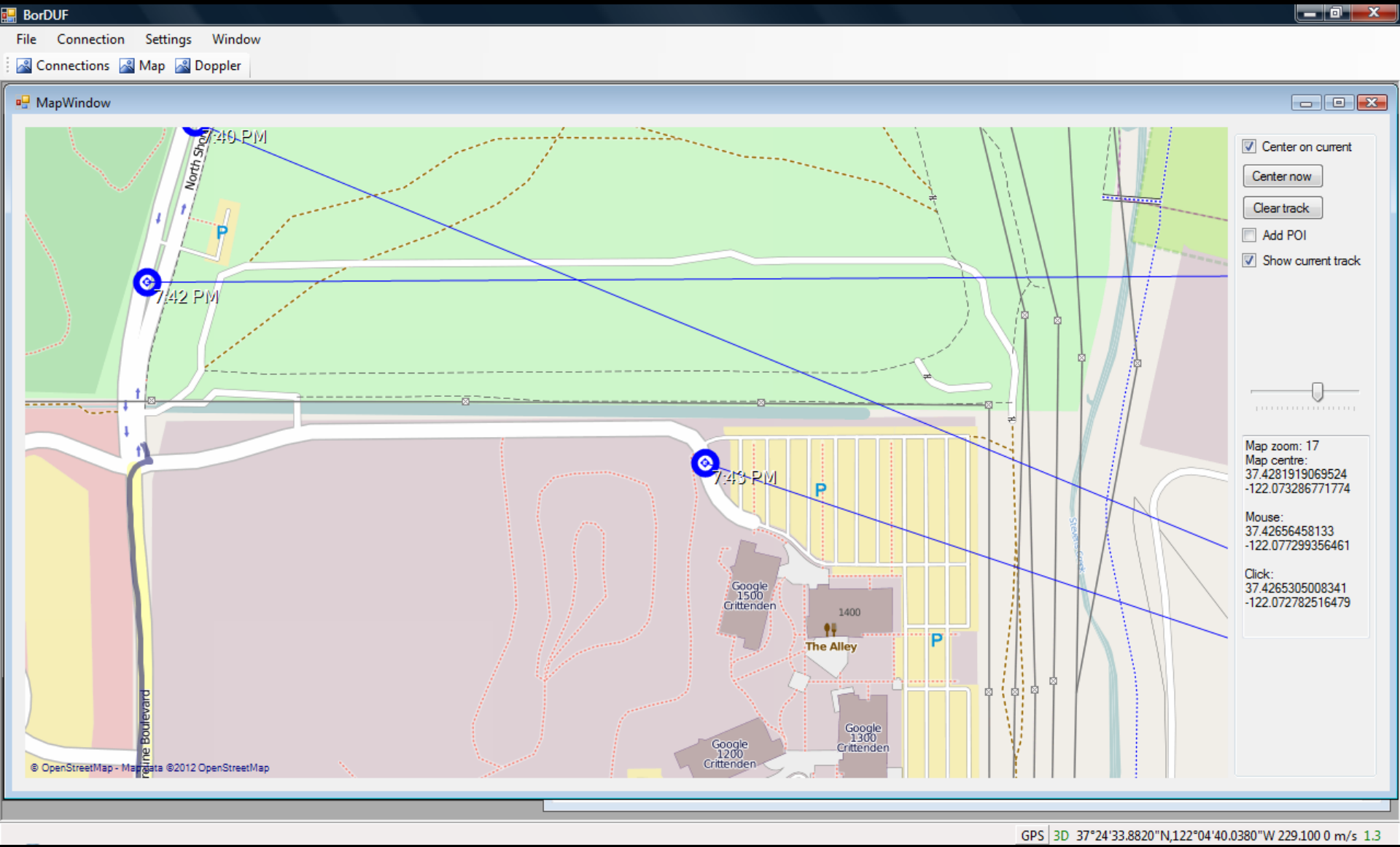
2659342)
59)
78497395)
259419)
839766286)
893056)
096886375)
540519)
7677959504)
670448)
5722486)
2116244659)
2228148)
086838732202)
6525021)
1750909972)
70712956)
27751085)
6156612)
5107070131)

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

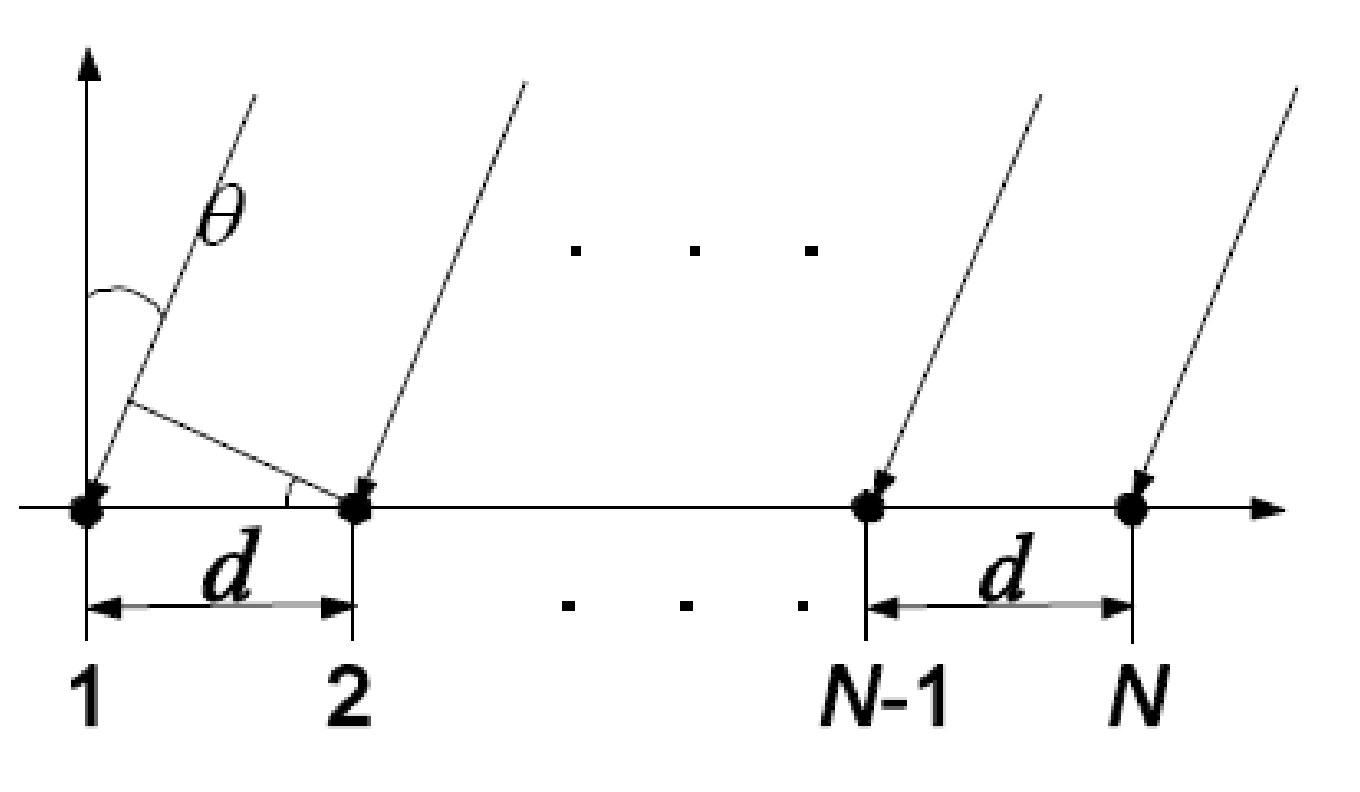

BorDUF
File
Connection
Settings
Window
Connections
Map
Doppler
MapWindow
7:37 PM
7:40 PM
7:42 PM
7:43 PM
7:28 PM
Shoreline Golf Course
North Shoreline Boulevard
Stevens Crk Nat Stdy Area
Crittenden Lane
Google Stierlin Ct
Stierlin Court
Center on current
Center now
Clear track
Add POI
Show current track
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

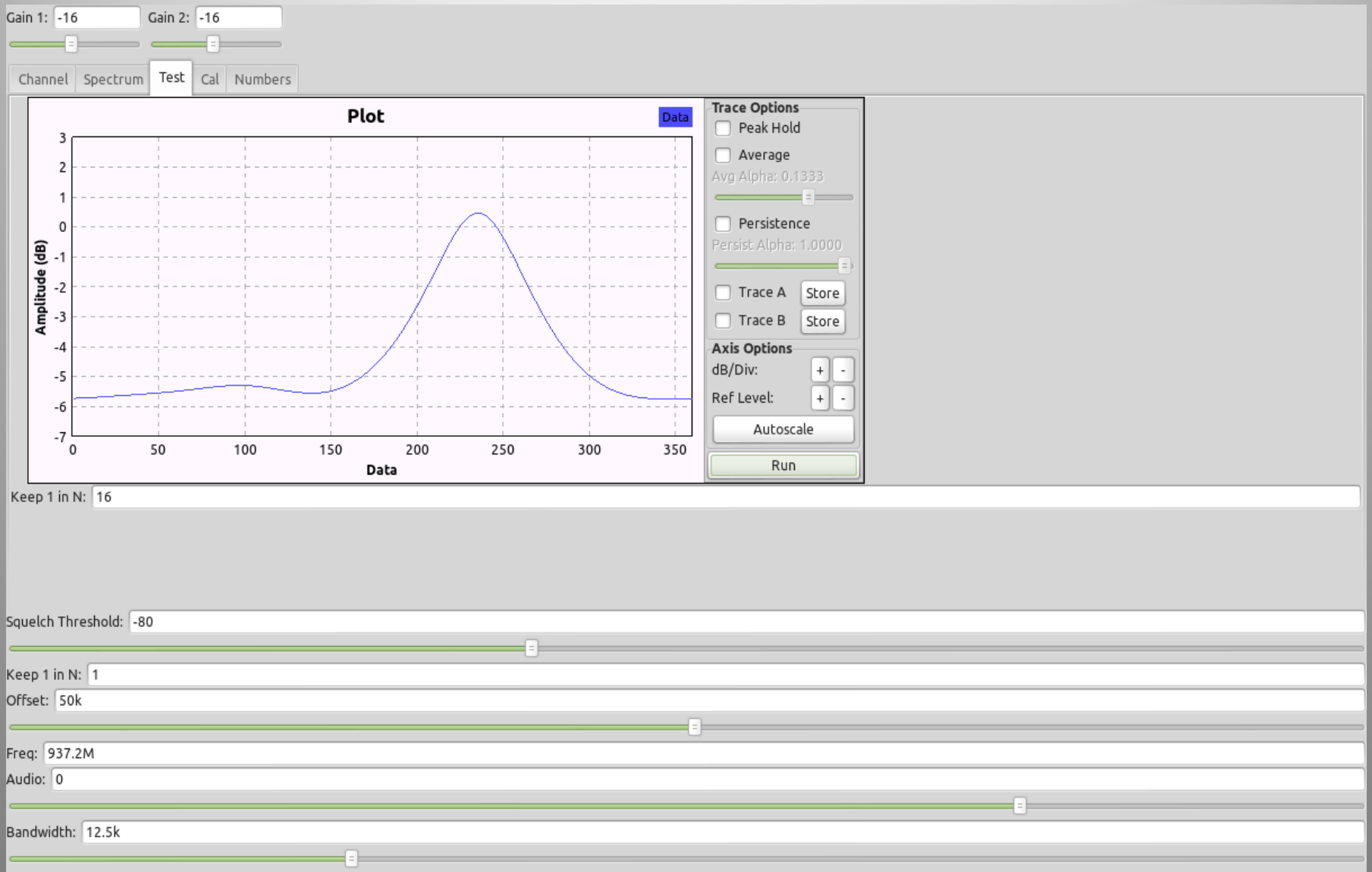
Method 2: Super-resolution algorithms

- Simultaneously receive multiple streams
  - One stream per antenna → antenna array
- Apply a mathematical model
  - Linear (far-field) wavefront approaching antenna array
  - Model/calibrate for antenna response
- MUSIC: **MU**ltiple **SI**gnal **C**lassification
  - Sample signal at each antenna (assuming sinusoids)
  - Maths (sample correlation matrix, eigenvector decomposition, orthogonal signal/noise subspaces)
  - Search through array response to find peak → DOA

Wavefront impinging on antenna array



Find maximal array response

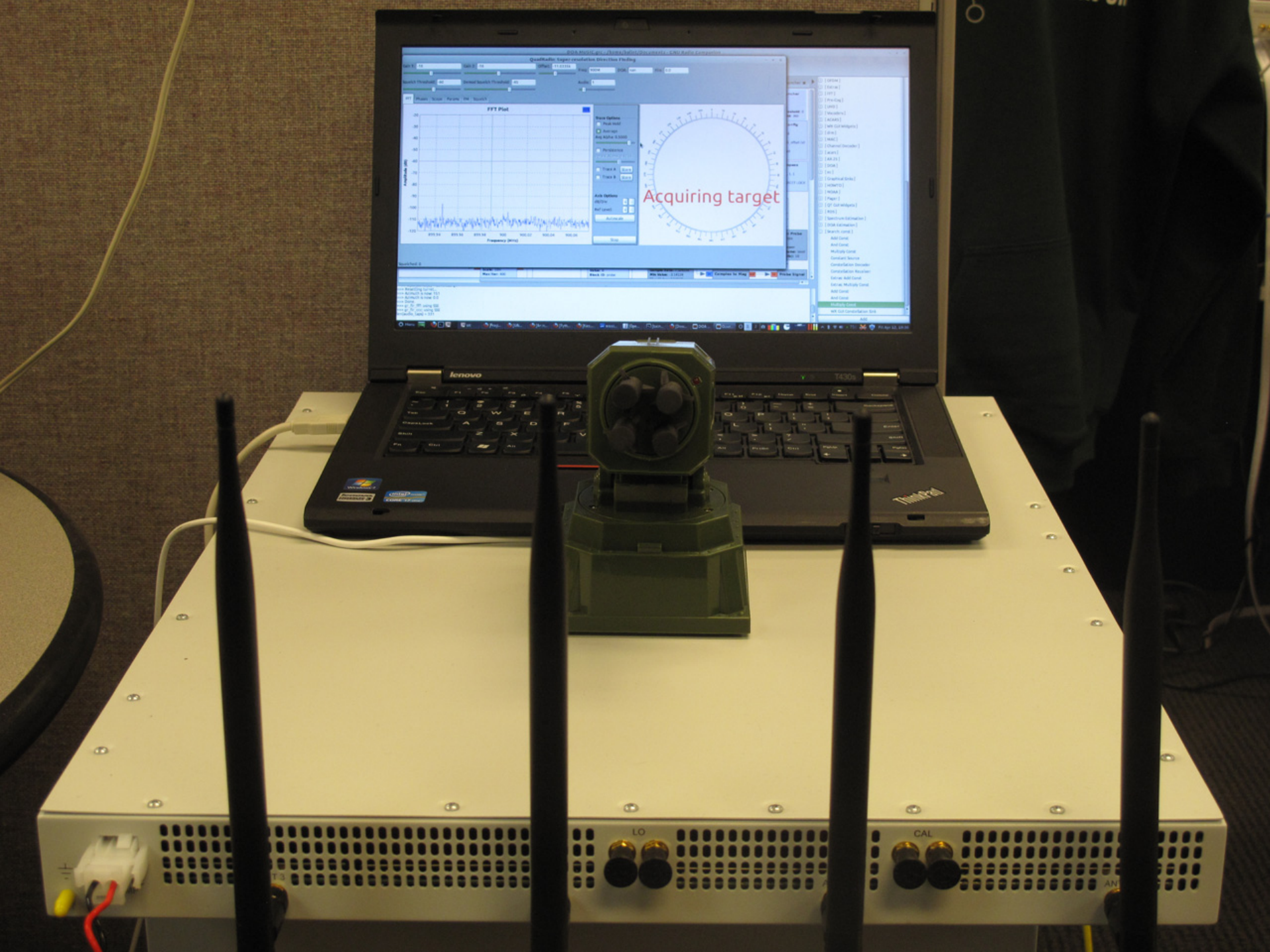


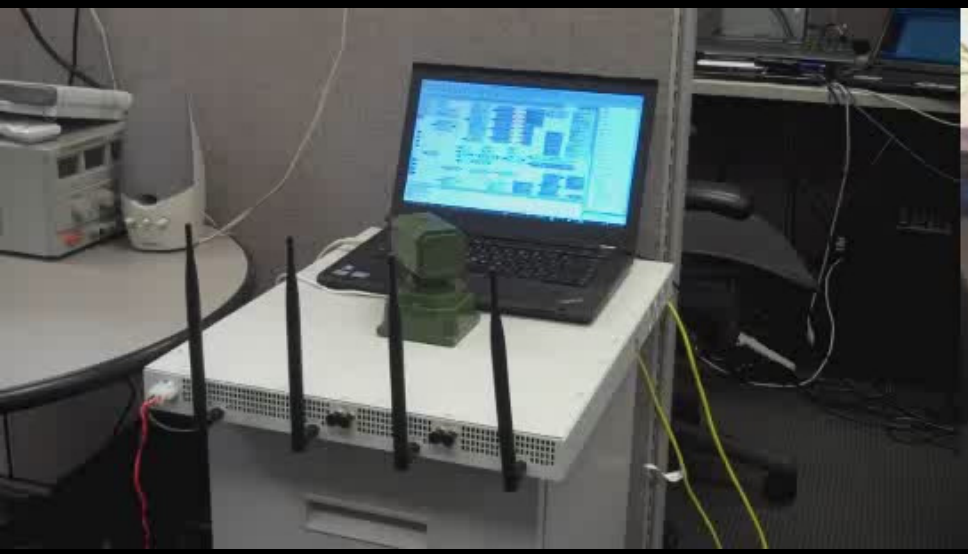
Advantages

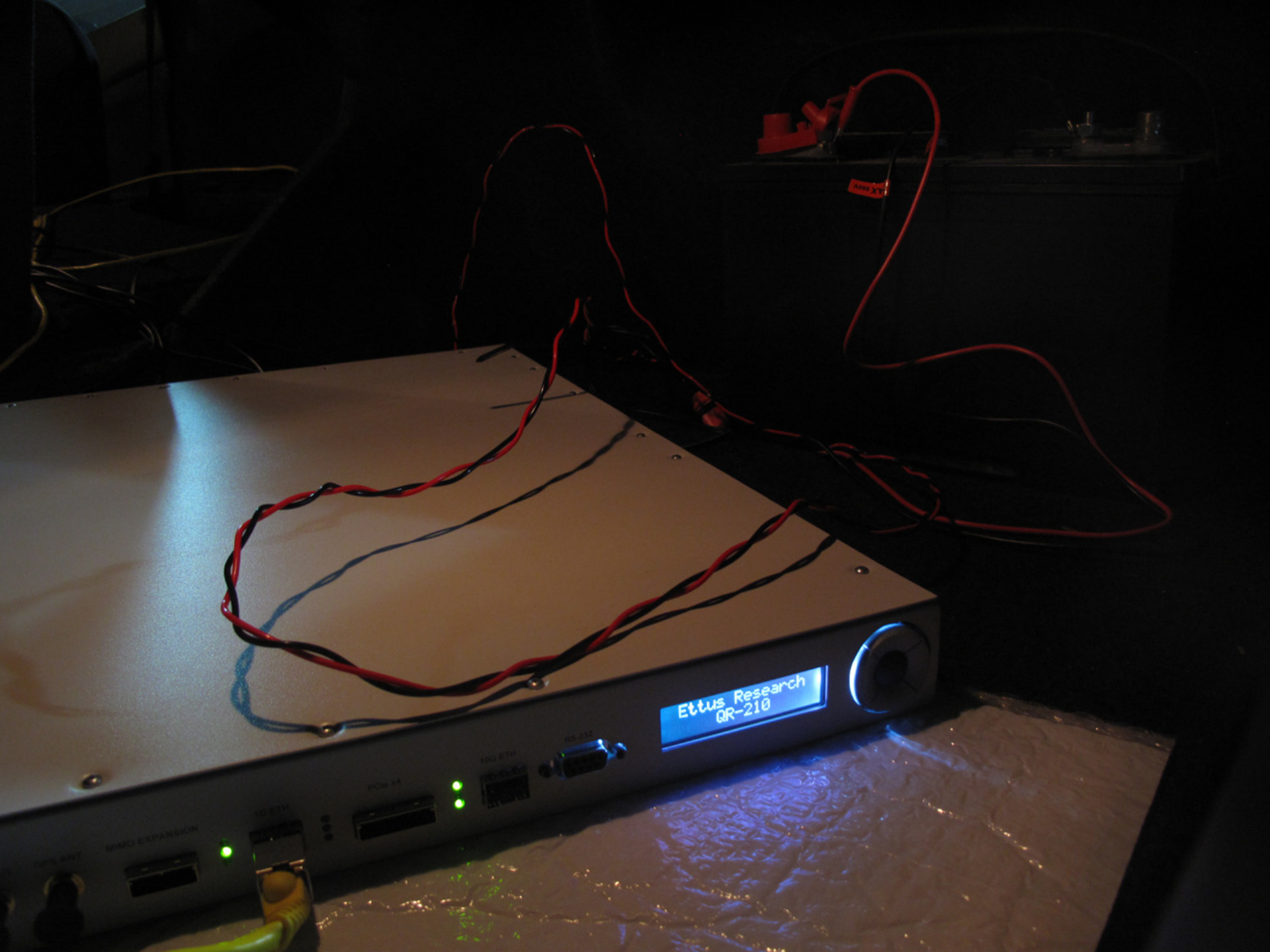
- Much higher resolution
  - Assuming model is correct & system is calibrated
- Detect & process multiple signals of interest simultaneously!

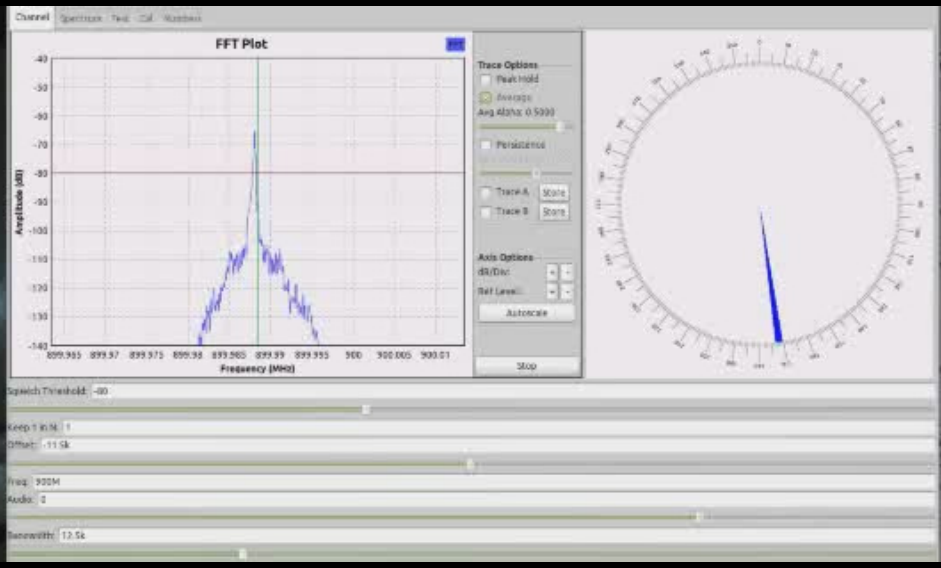
- However…

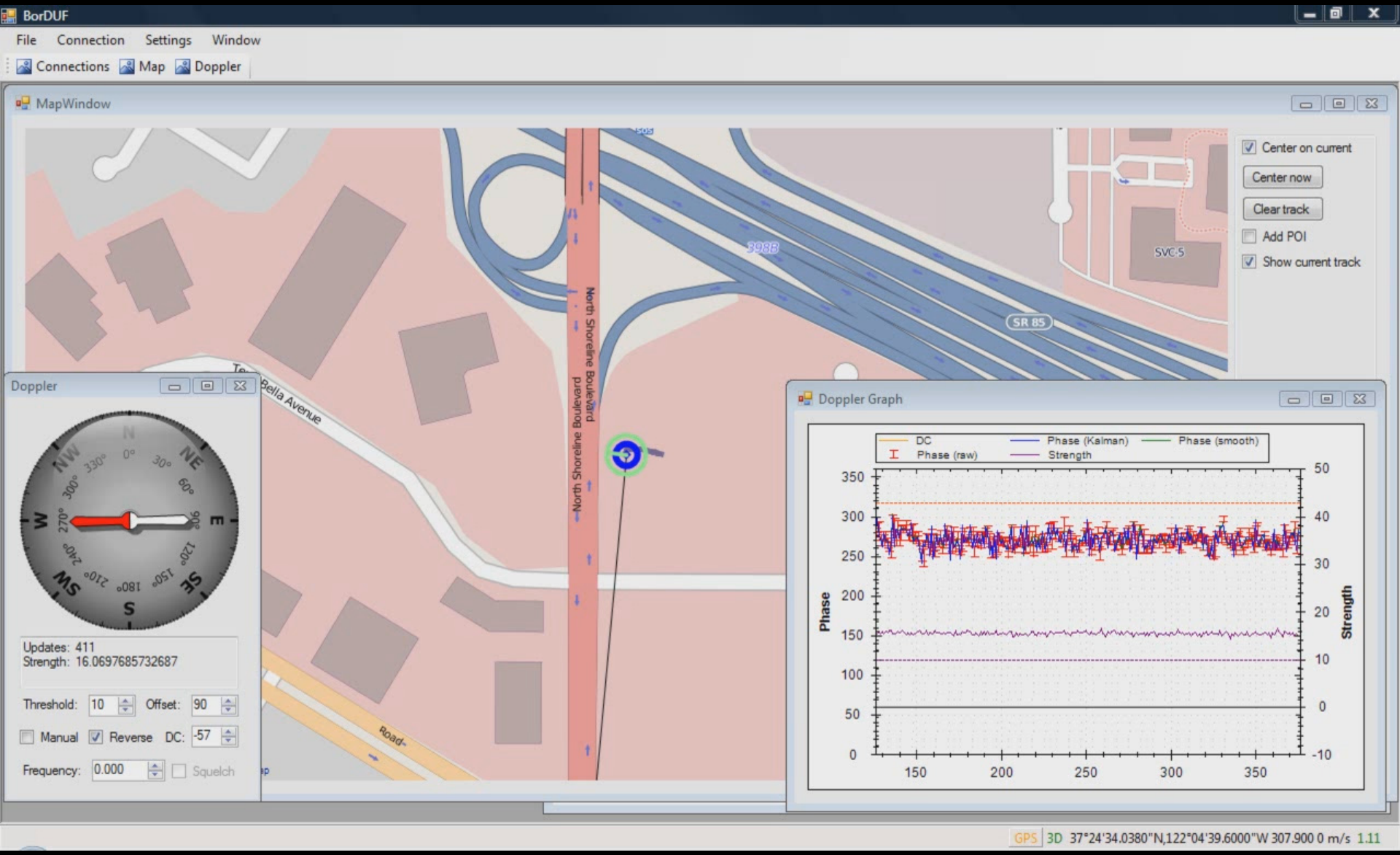
  you need more (coherent) radios.

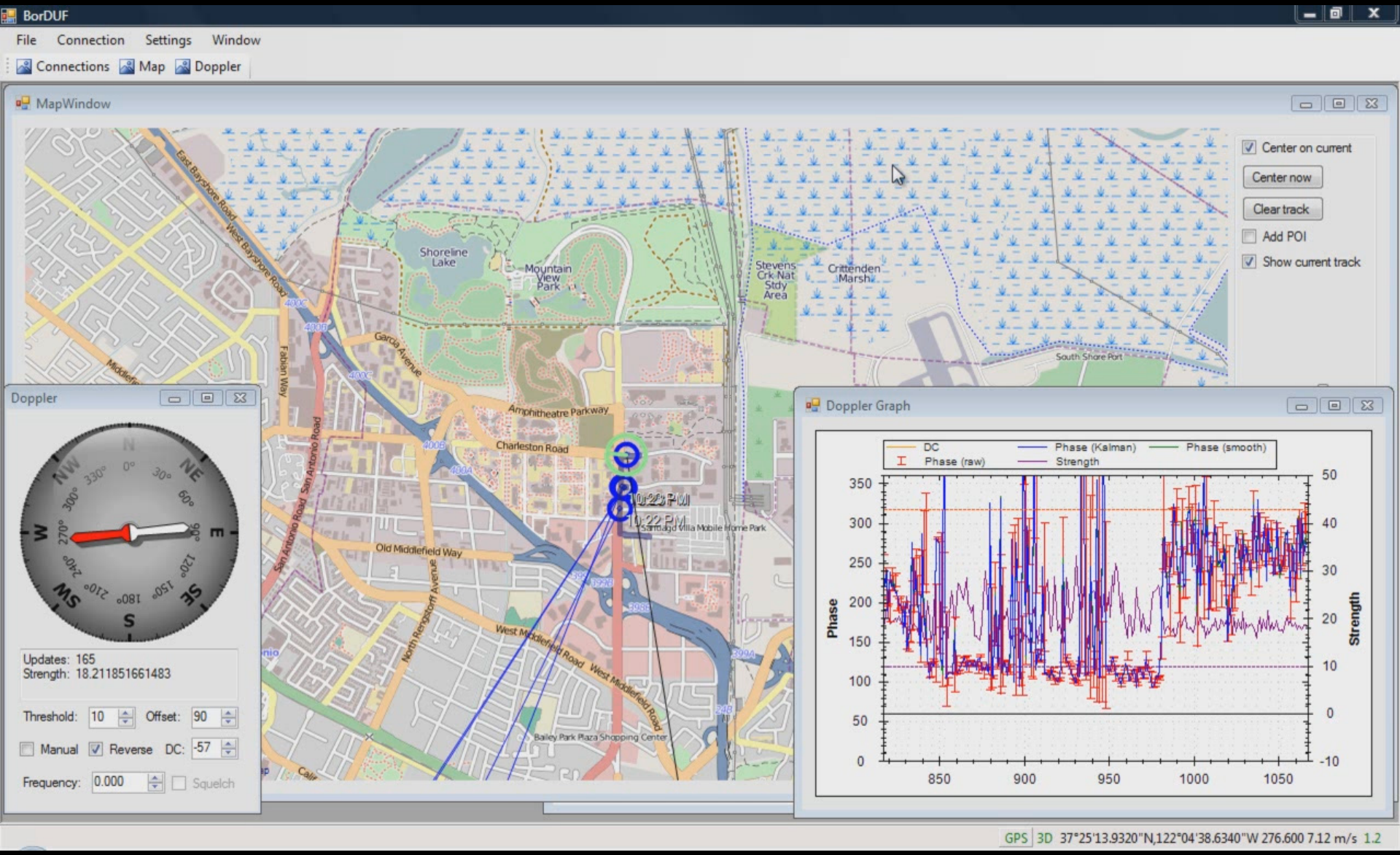

FFT Plot
Acquiring target
lenovo
ThinkPad
LO
CAL



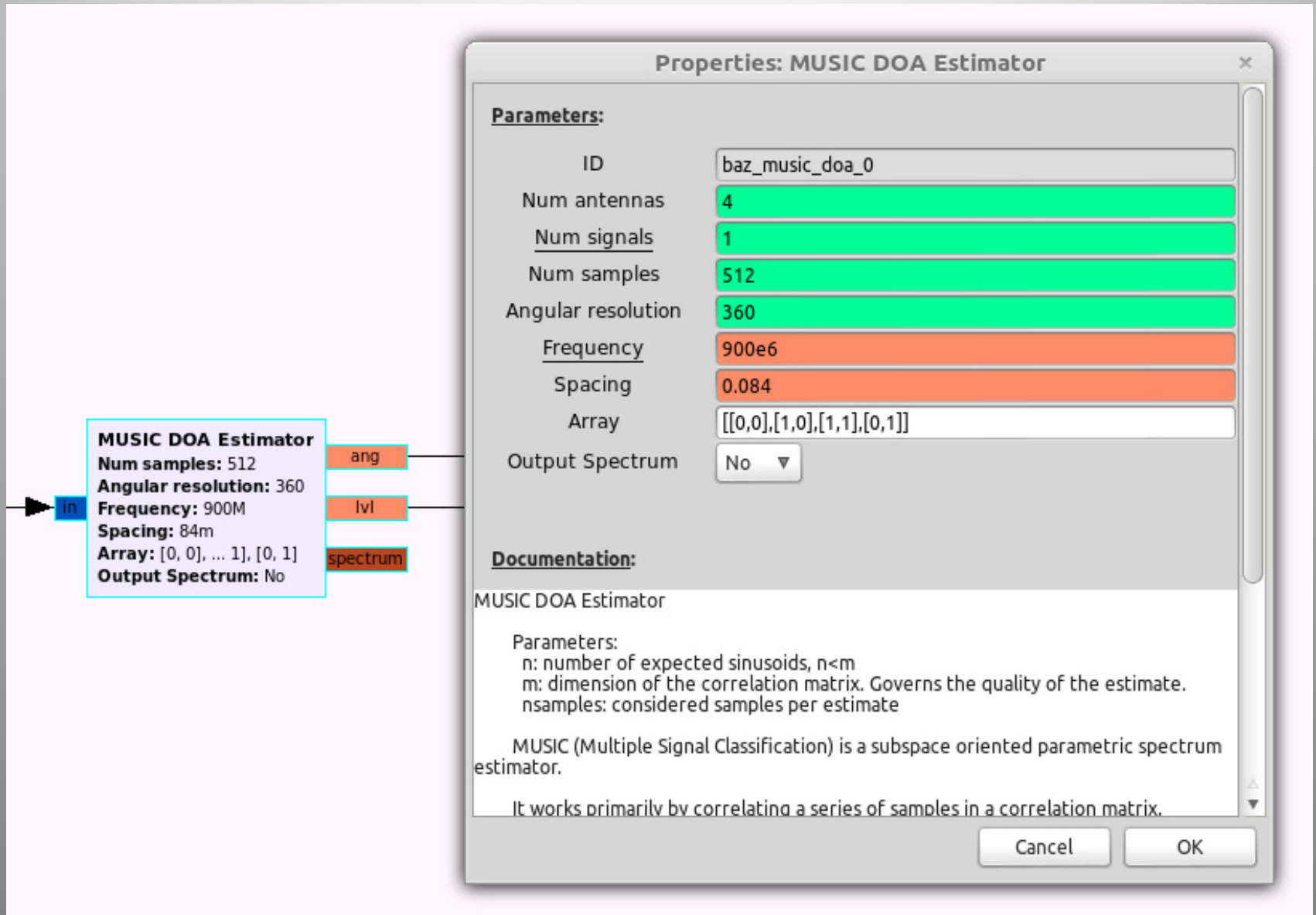

Ettus Research
QR-210


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

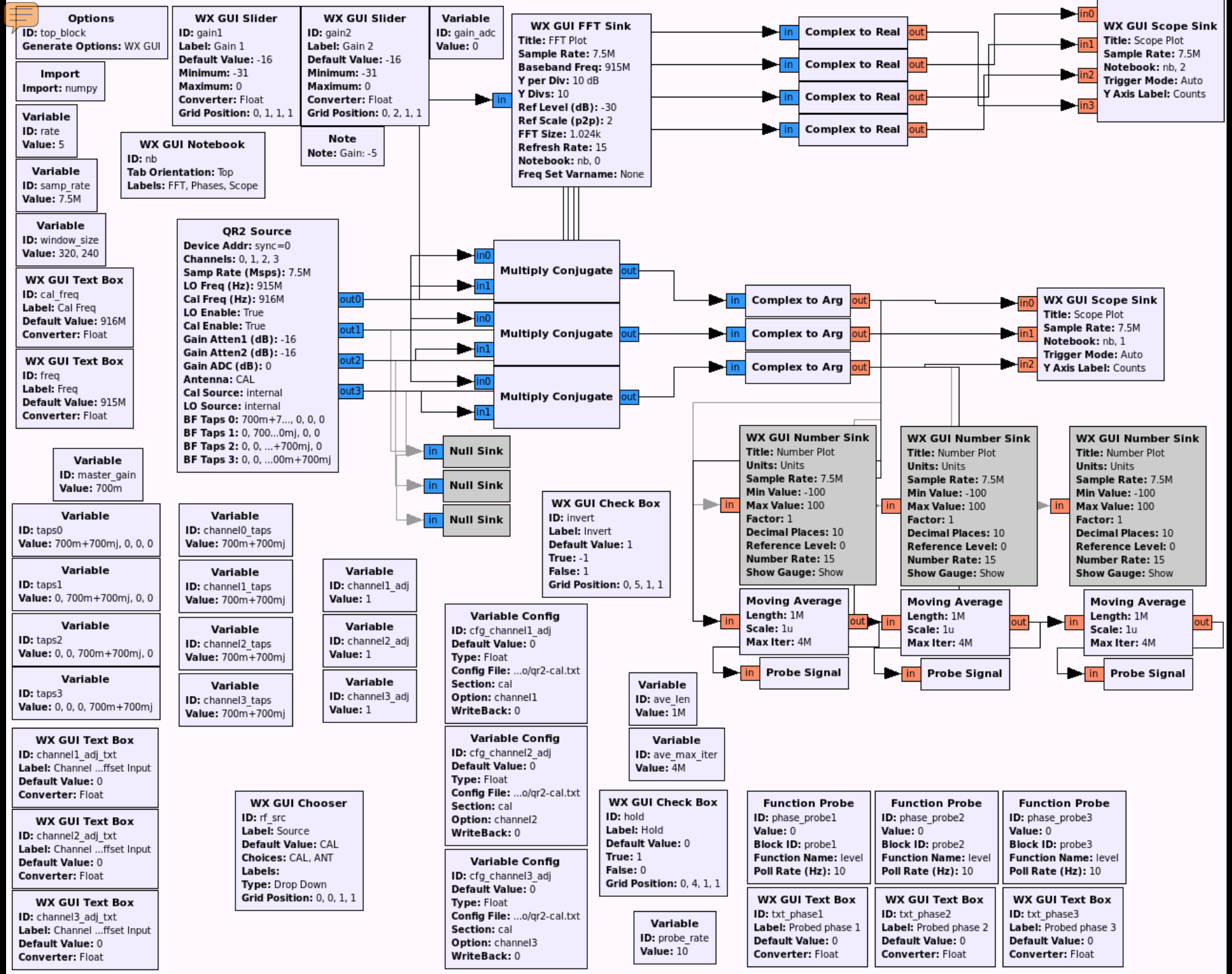

BorDUF
File
Connection
Settings
Window
Connections
Map
Doppler
MapWindow
Center on current
Center now
Clear track
Add POI
Show current track
Shoreline Lake
Mountain View Park
Stevens Crk Nat Stdy Area
Crittenden Marsh
South Shore Port
East Bayshore Road
West Bayshore Road
Fabian Way
Garcia Avenue
Amphitheatre 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



Calibration

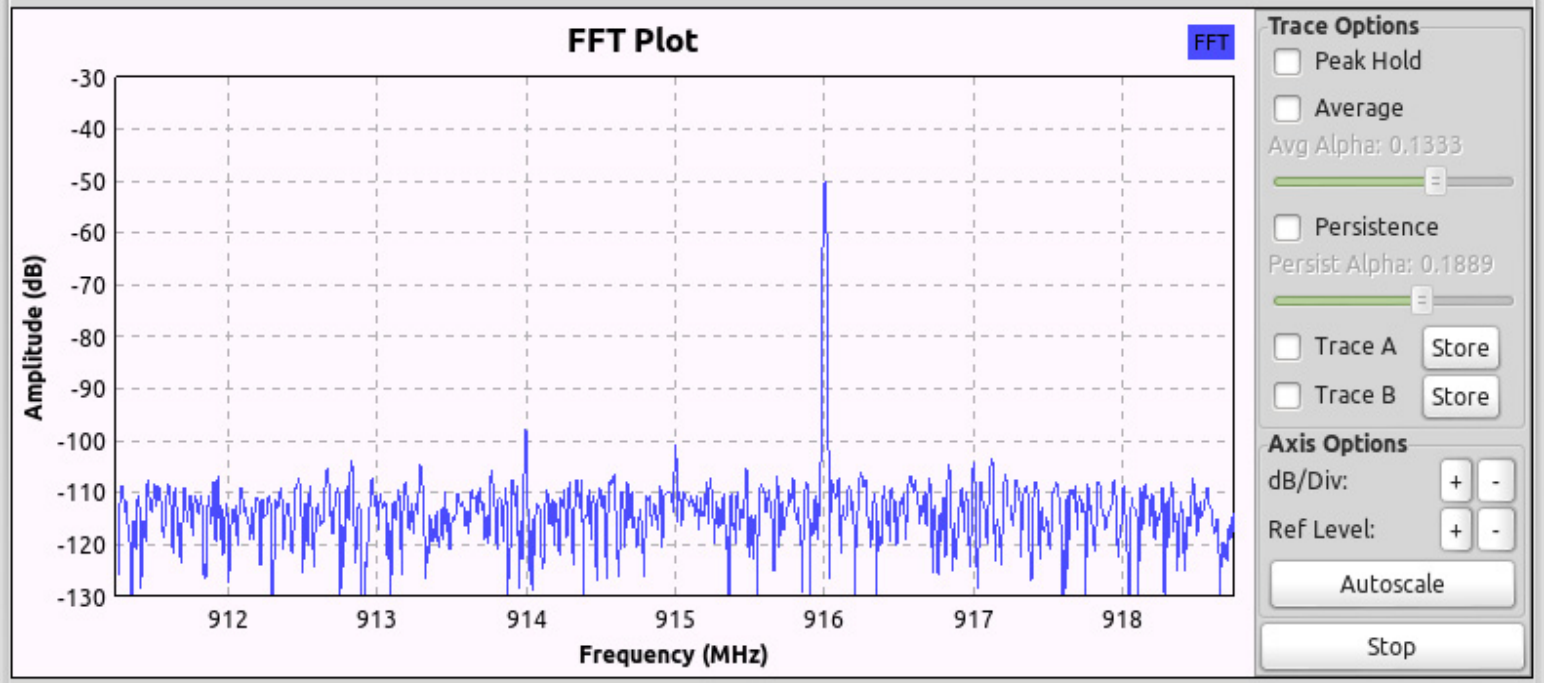
- Use shared Local Oscillator
- Inject shared tone in each channel
- Calculate per-channel phase differences
  - w. r. t. reference channel
- Apply corrections
- Periodically re-calibrate


Options
ID: top_block
Generate Options: WX GUI
Import
Import: numpy
Variable
ID: rate
Value: 5
Variable
ID: samp_rate
Value: 7.5M
Variable
ID: window_size
Value: 320, 240
WX GUI Text Box
ID: cal_freq
Label: Cal Freq
Default Value: 916M
Converter: Float
WX GUI Text Box
ID: freq
Label: Freq
Default Value: 915M
Converter: Float
WX GUI Slider
ID: gain1
Label: Gain 1
Default Value: -16
Minimum: -31
Maximum: 0
Converter: Float
Grid Position: 0, 1, 1, 1
WX GUI Slider
ID: gain2
Label: Gain 2
Default Value: -16
Minimum: -31
Maximum: 0
Converter: Float
Grid Position: 0, 2, 1, 1
Variable
ID: gain_adc
Value: 0
Note
Note: Gain: -5
WX GUI Notebook
ID: nb
Tab Orientation: Top
Labels: FFT, Phases, Scope
WX GUI FFT Sink
Title: FFT Plot
Sample Rate: 7.5M
Baseband Freq: 915M
Y per Div: 10 dB
Y Divs: 10
Ref Level (dB): -30
Ref Scale (p2p): 2
FFT Size: 1.024k
Refresh Rate: 15
Notebook: nb, 0
Freq Set Varname: None
Complex to Real
Complex to Real
Complex to Real
Complex to Real
WX GUI Scope Sink
Title: Scope Plot
Sample Rate: 7.5M
Notebook: nb, 2
Trigger Mode: Auto
Y Axis Label: Counts
QR2 Source
Device Addr: sync=0
Channels: 0, 1, 2, 3
Samp Rate (Msps): 7.5M
LO Freq (Hz): 915M
Cal Freq (Hz): 916M
LO Enable: True
Cal Enable: True
Gain Atten1 (dB): -16
Gain Atten2 (dB): -16
Gain ADC (dB): 0
Antenna: CAL
Cal Source: internal
LO Source: internal
BF Taps 0: 700m+7..., 0, 0, 0
BF Taps 1: 0, 700...0mj, 0, 0
BF Taps 2: 0, 0, ...+700mj, 0
BF Taps 3: 0, 0, ...00m+700mj
Multiply Conjugate
Multiply Conjugate
Multiply Conjugate
Complex to Arg
Complex to Arg
Complex to Arg
WX GUI Scope Sink
Title: Scope Plot
Sample Rate: 7.5M
Notebook: nb, 1
Trigger Mode: Auto
Y Axis Label: Counts
Null Sink
Null Sink
Null Sink
Variable
ID: master_gain
Value: 700m
Variable
ID: taps0
Value: 700m+700mj, 0, 0, 0
Variable
ID: taps1
Value: 0, 700m+700mj, 0, 0
Variable
ID: taps2
Value: 0, 0, 700m+700mj, 0
Variable
ID: taps3
Value: 0, 0, 0, 700m+700mj
Variable
ID: channel0_taps
Value: 700m+700mj
Variable
ID: channel1_taps
Value: 700m+700mj
Variable
ID: channel2_taps
Value: 700m+700mj
Variable
ID: channel3_taps
Value: 700m+700mj
Variable
ID: channel1_adj
Value: 1
Variable
ID: channel2_adj
Value: 1
Variable
ID: channel3_adj
Value: 1
WX GUI Check Box
ID: invert
Label: Invert
Default Value: 1
True: -1
False: 1
Grid Position: 0, 5, 1, 1
WX GUI Number Sink
Title: Number Plot
Units: Units
Sample Rate: 7.5M
Min Value: -100
Max Value: 100
Factor: 1
Decimal Places: 10
Reference Level: 0
Number Rate: 15
Show Gauge: Show
WX GUI Number Sink
Title: Number Plot
Units: Units
Sample Rate: 7.5M
Min Value: -100
Max Value: 100
Factor: 1
Decimal Places: 10
Reference Level: 0
Number Rate: 15
Show Gauge: Show
WX GUI Number Sink
Title: Number Plot
Units: Units
Sample Rate: 7.5M
Min Value: -100
Max Value: 100
Factor: 1
Decimal Places: 10
Reference Level: 0
Number Rate: 15
Show Gauge: Show
Moving Average
Length: 1M
Scale: 1u
Max Iter: 4M
Moving Average
Length: 1M
Scale: 1u
Max Iter: 4M
Moving Average
Length: 1M
Scale: 1u
Max Iter: 4M
Probe Signal
Probe Signal
Probe Signal
Variable Config
ID: cfg_channel1_adj
Default Value: 0
Type: Float
Config File: ...o/qr2-cal.txt
Section: cal
Option: channel1
WriteBack: 0
Variable Config
ID: cfg_channel2_adj
Default Value: 0
Type: Float
Config File: ...o/qr2-cal.txt
Section: cal
Option: channel2
WriteBack: 0
Variable Config
ID: cfg_channel3_adj
Default Value: 0
Type: Float
Config File: ...o/qr2-cal.txt
Section: cal
Option: channel3
WriteBack: 0
Variable
ID: ave_len
Value: 1M
Variable
ID: ave_max_iter
Value: 4M
WX GUI Check Box
ID: hold
Label: Hold
Default Value: 0
True: 1
False: 0
Grid Position: 0, 4, 1, 1
Variable
ID: probe_rate
Value: 10
Function Probe
ID: phase_probe1
Value: 0
Block ID: probe1
Function Name: level
Poll Rate (Hz): 10
Function Probe
ID: phase_probe2
Value: 0
Block ID: probe2
Function Name: level
Poll Rate (Hz): 10
Function Probe
ID: phase_probe3
Value: 0
Block ID: probe3
Function Name: level
Poll Rate (Hz): 10
WX GUI Text Box
ID: txt_phase1
Label: Probed phase 1
Default Value: 0
Converter: Float
WX GUI Text Box
ID: txt_phase2
Label: Probed phase 2
Default Value: 0
Converter: Float
WX GUI Text Box
ID: txt_phase3
Label: Probed phase 3
Default Value: 0
Converter: Float
WX GUI Text Box
ID: channel1_adj_txt
Label: Channel ...ffset Input
Default Value: 0
Converter: Float
WX GUI Text Box
ID: channel2_adj_txt
Label: Channel ...ffset Input
Default Value: 0
Converter: Float
WX GUI Text Box
ID: channel3_adj_txt
Label: Channel ...ffset Input
Default Value: 0
Converter: Float
WX GUI Chooser
ID: rf_src
Label: Source
Default Value: CAL
Choices: CAL, ANT
Labels:
Type: Drop Down
Grid Position: 0, 0, 1, 1

Top Block

Source: CAL | Gain 1: -16 | Gain 2: -16 | Hold | Invert

FFT | Phases | Scope



Trace Options
- Peak Hold
- Average
- Avg Alpha: 0.1333
- Persistence
- Persist Alpha: 0.1889
- Trace A | Store
- Trace B | Store

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

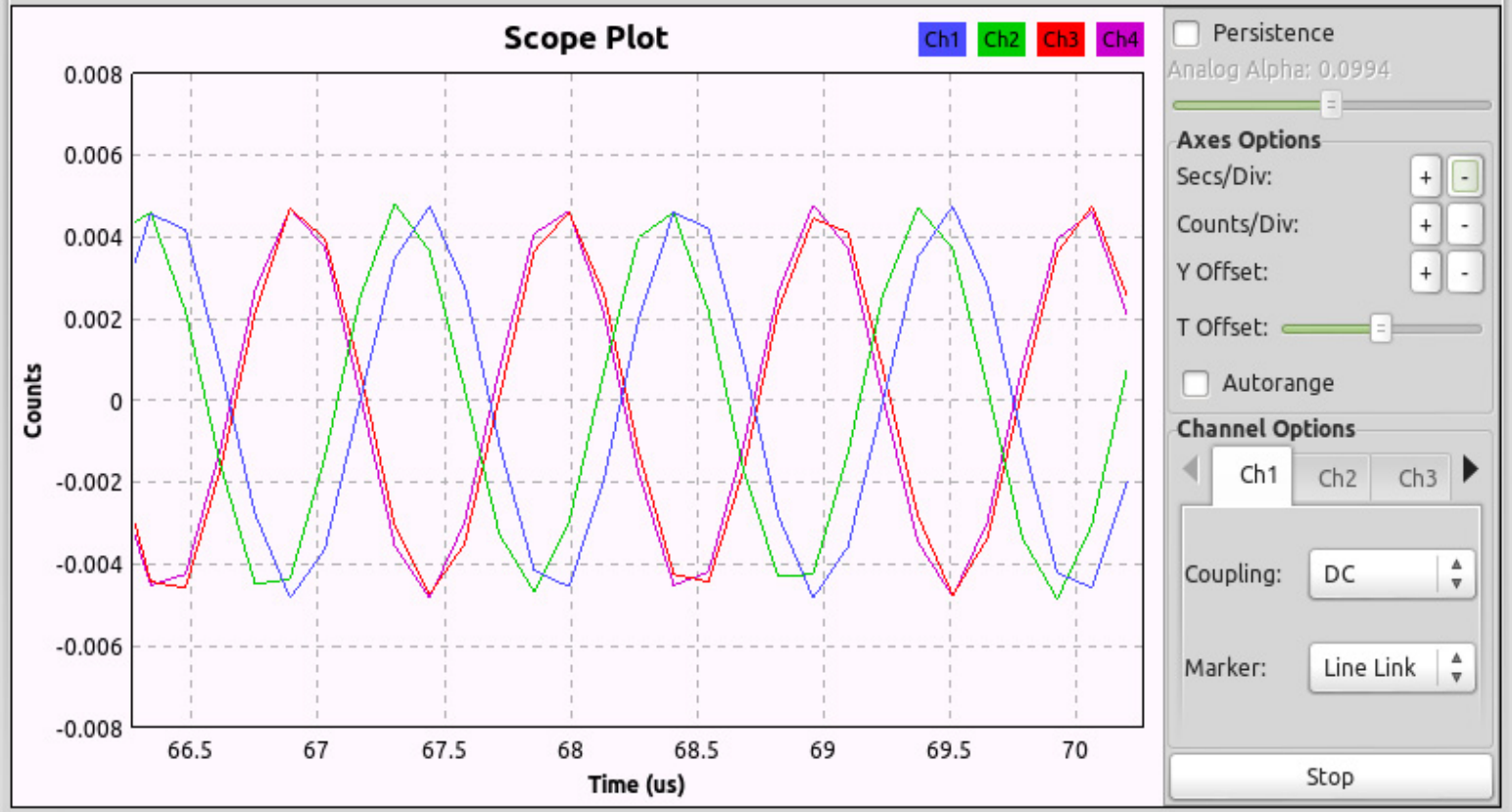
Stop

Freq:	915M
Cal Freq:	916M
Probed phase 3:	-57.5379m
Probed phase 2:	-344.164m
Probed phase 1:	2.26746m
Channel 3 Phase Offset Input:	181.716m
Channel 2 Phase Offset Input:	386.061m
Channel 1 Phase Offset Input:	594.121m

Top Block

Source: CAL Gain 1: -16 Gain 2: -16 Hold Invert

FFT | Phases | Scope



Persistence
Analog Alpha: 0.0994

Axes Options
Secs/Div: + -
Counts/Div: + -
Y Offset: + -
T Offset:
Autorange

Channel Options
Ch1 | Ch2 | Ch3
Coupling: DC
Marker: Line Link

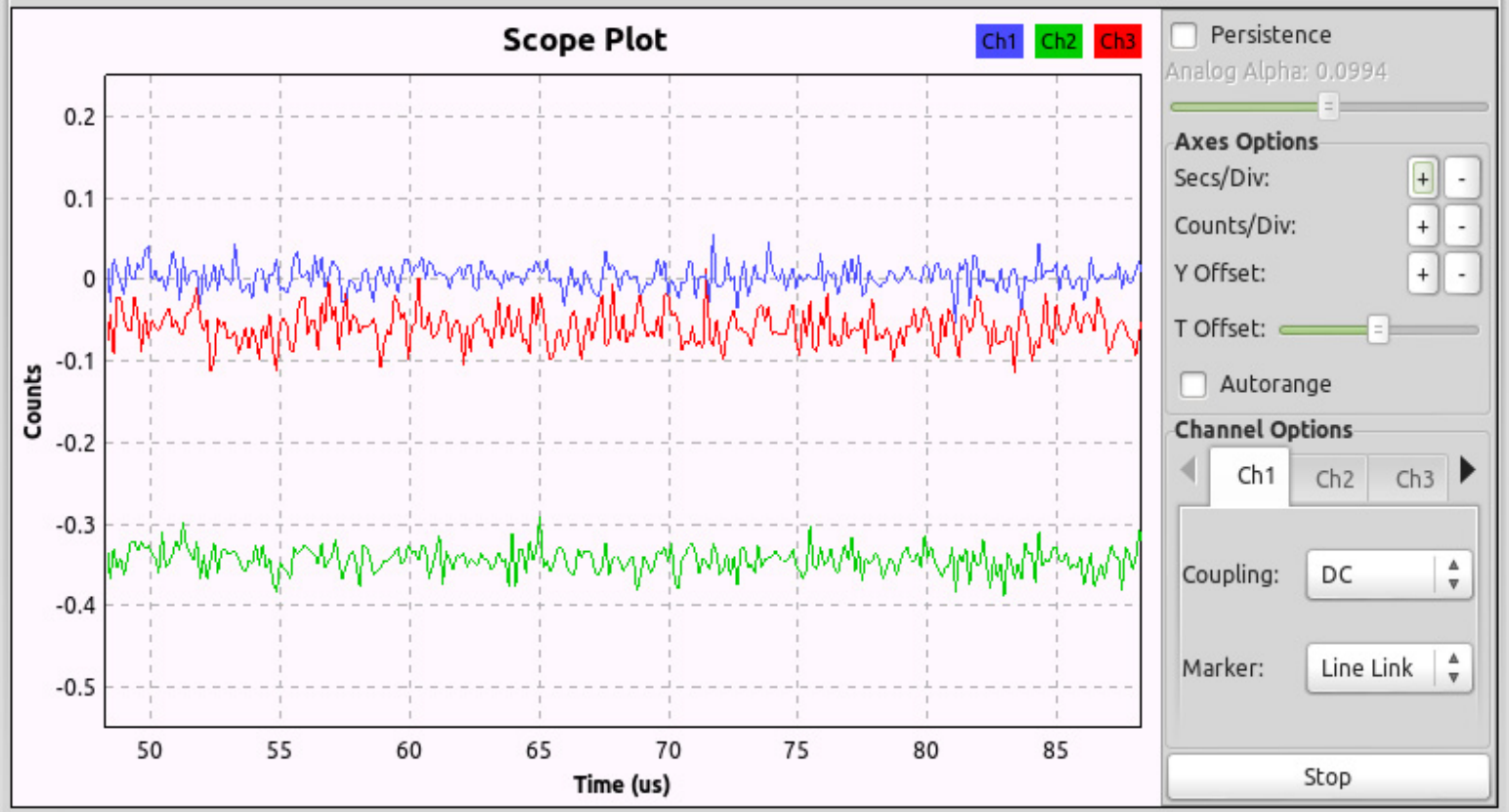
Stop

Freq: 915M
Cal Freq: 916M
Probed phase 3: -57.6652m
Probed phase 2: -344.528m
Probed phase 1: 2.28574m
Channel 3 Phase Offset Input: 0
Channel 2 Phase Offset Input: 0
Channel 1 Phase Offset Input: 0

Top Block

Source: CAL Gain 1: -16 Gain 2: -16 Hold Invert

FFT | Phases | Scope



Persistence
Analog Alpha: 0.0994

Axes Options
Secs/Div: + -
Counts/Div: + -
Y Offset: + -
T Offset:
Autorange

Channel Options
Ch1 | Ch2 | Ch3
Coupling: DC
Marker: Line Link

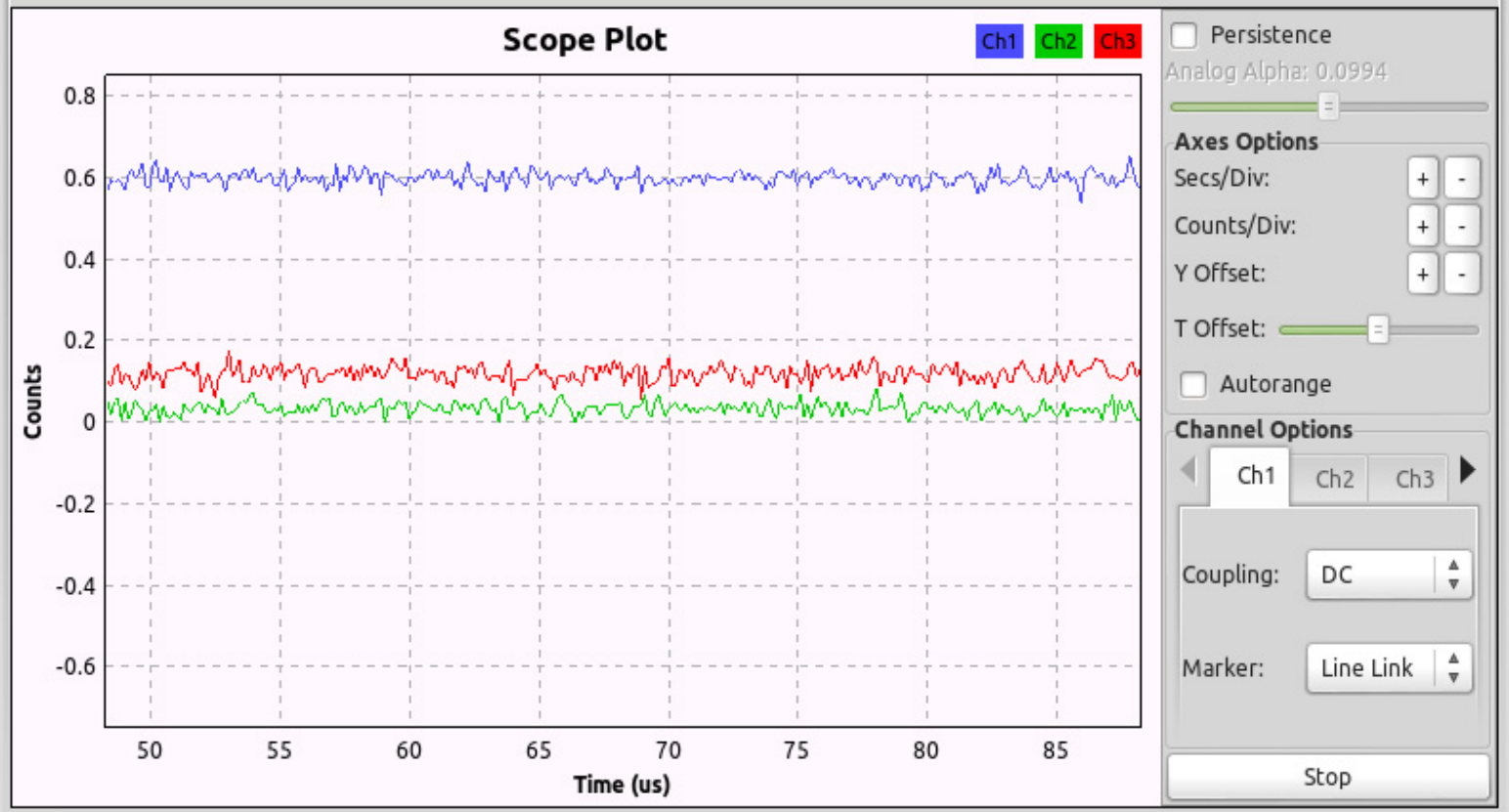
Stop

Freq: 915M
Cal Freq: 916M
Probed phase 3: -57.5955m
Probed phase 2: -344.187m
Probed phase 1: 2.29332m
Channel 3 Phase Offset Input: 181.716m
Channel 2 Phase Offset Input: 386.061m
Channel 1 Phase Offset Input: 594.121m

Top Block

Source: CAL Gain 1: -16 Gain 2: -16 Hold Invert

FFT | Phases | Scope



Persistence
Analog Alpha: 0.0994

Axes Options
Secs/Div: + -
Counts/Div: + -
Y Offset: + -
T Offset:
Autorange

Channel Options
Ch1 | Ch2 | Ch3
Coupling: DC
Marker: Line Link

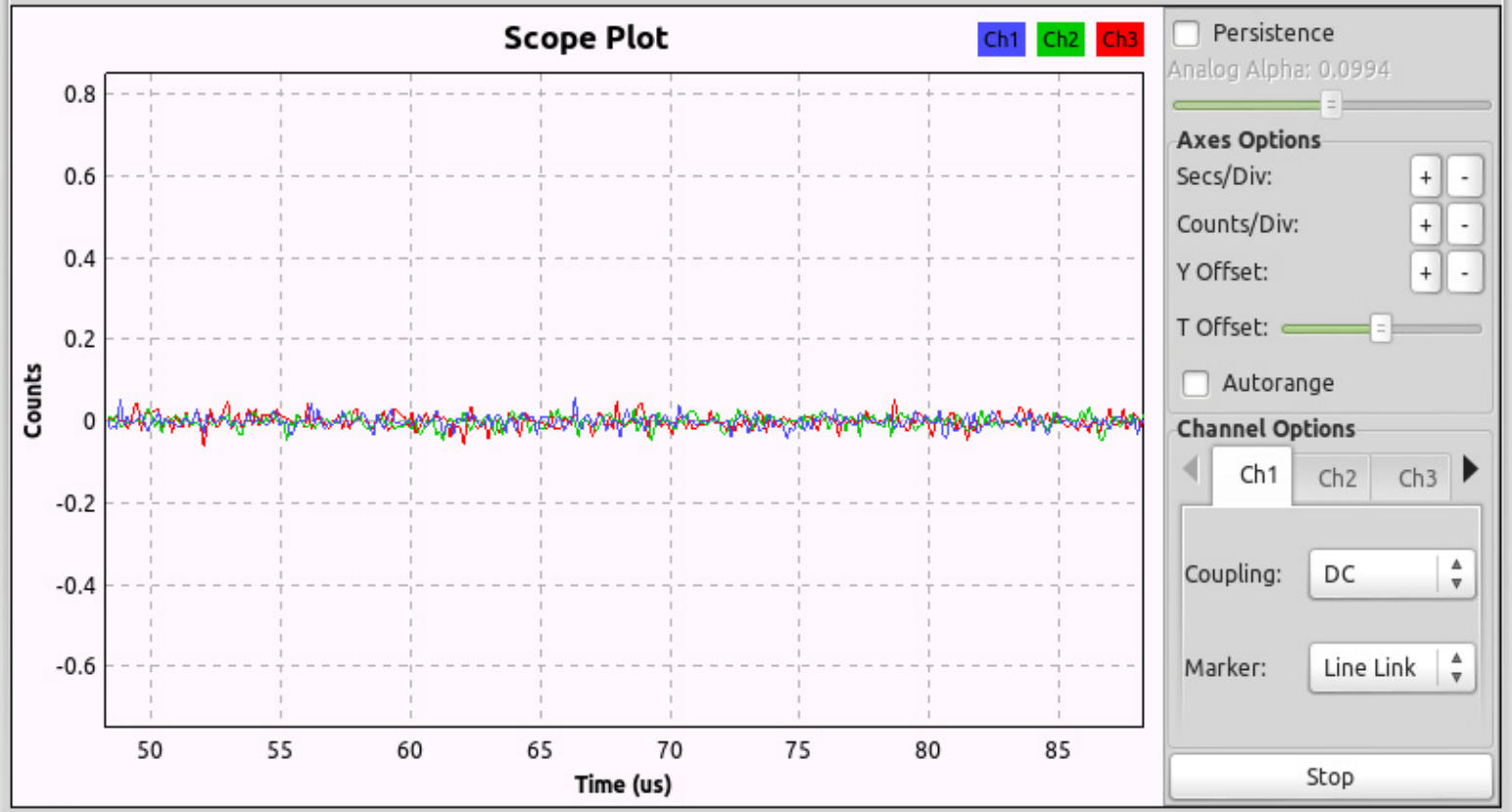
Stop

Freq: 915M
Cal Freq: 916M
Probed phase 3: 119.943m
Probed phase 2: 34.8406m
Probed phase 1: 597.494m
Channel 3 Phase Offset Input: 119.943m
Channel 2 Phase Offset Input: 34.8406m
Channel 1 Phase Offset Input: 597.494m

Top Block

Source: CAL Gain 1: -16 Gain 2: -16 Hold Invert

FFT | Phases | Scope



Persistence
Analog Alpha: 0.0994

Axes Options
Secs/Div: + -
Counts/Div: + -
Y Offset: + -
T Offset:
Autorange

Channel Options
Ch1 | Ch2 | Ch3
Coupling: DC
Marker: Line Link

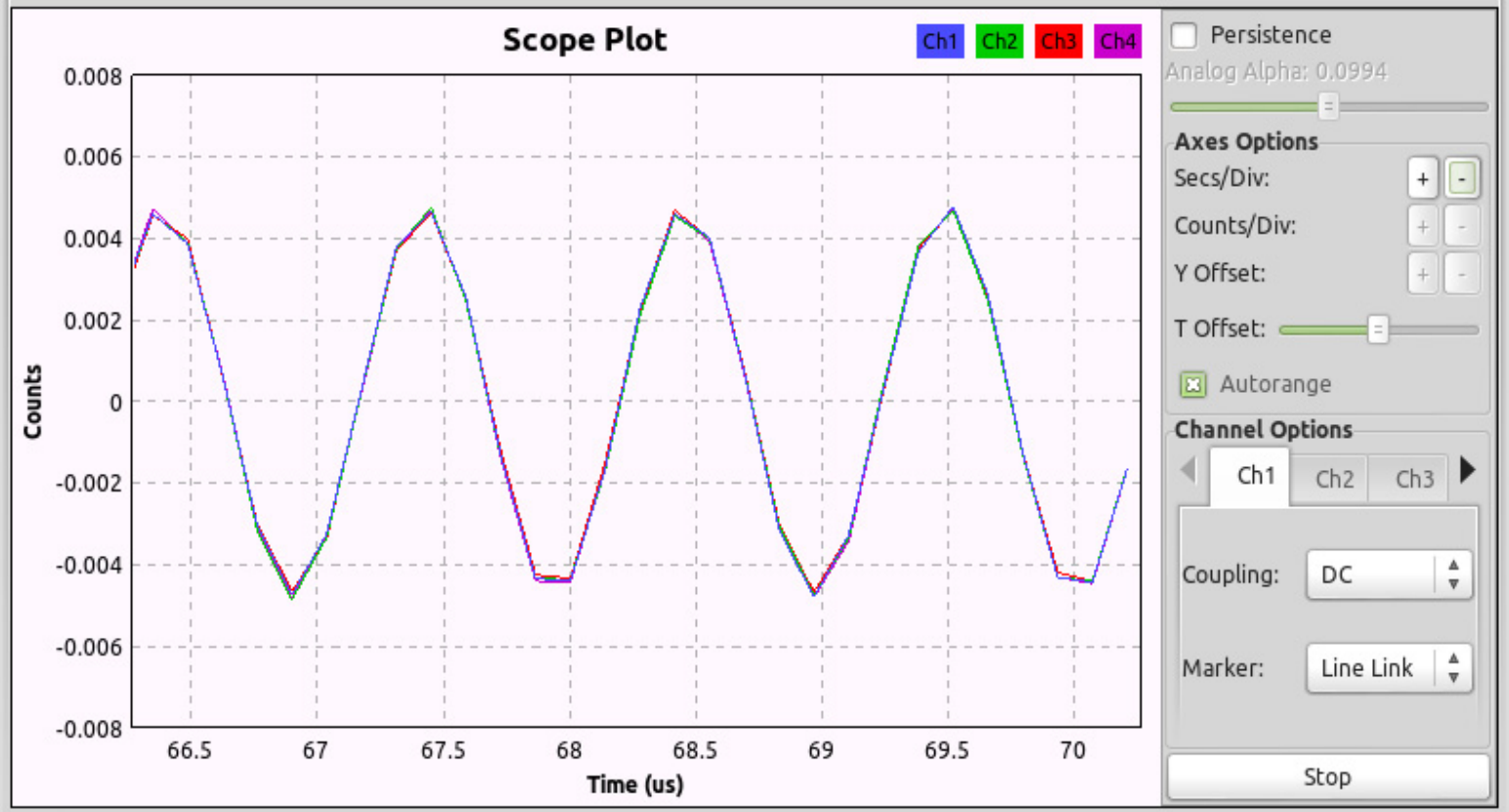
Stop

Freq: 915M
Cal Freq: 916M
Probed phase 3: 119.943m
Probed phase 2: 34.8406m
Probed phase 1: 597.494m
Channel 3 Phase Offset Input: 119.943m
Channel 2 Phase Offset Input: 34.8406m
Channel 1 Phase Offset Input: 597.494m

Top Block

Source: CAL | Gain 1: -16 | Gain 2: -16 | Hold | Invert

FFT | Phases | Scope



Persistence

Analog Alpha: 0.0994

Axes Options

Secs/Div: + -

Counts/Div: + -

Y Offset: + -

T Offset:

Autorange

Channel Options

Ch1 | Ch2 | Ch3

Coupling: DC

Marker: Line Link

Stop

Freq: 915M

Cal Freq: 916M

Probed phase 3: 1.78844m

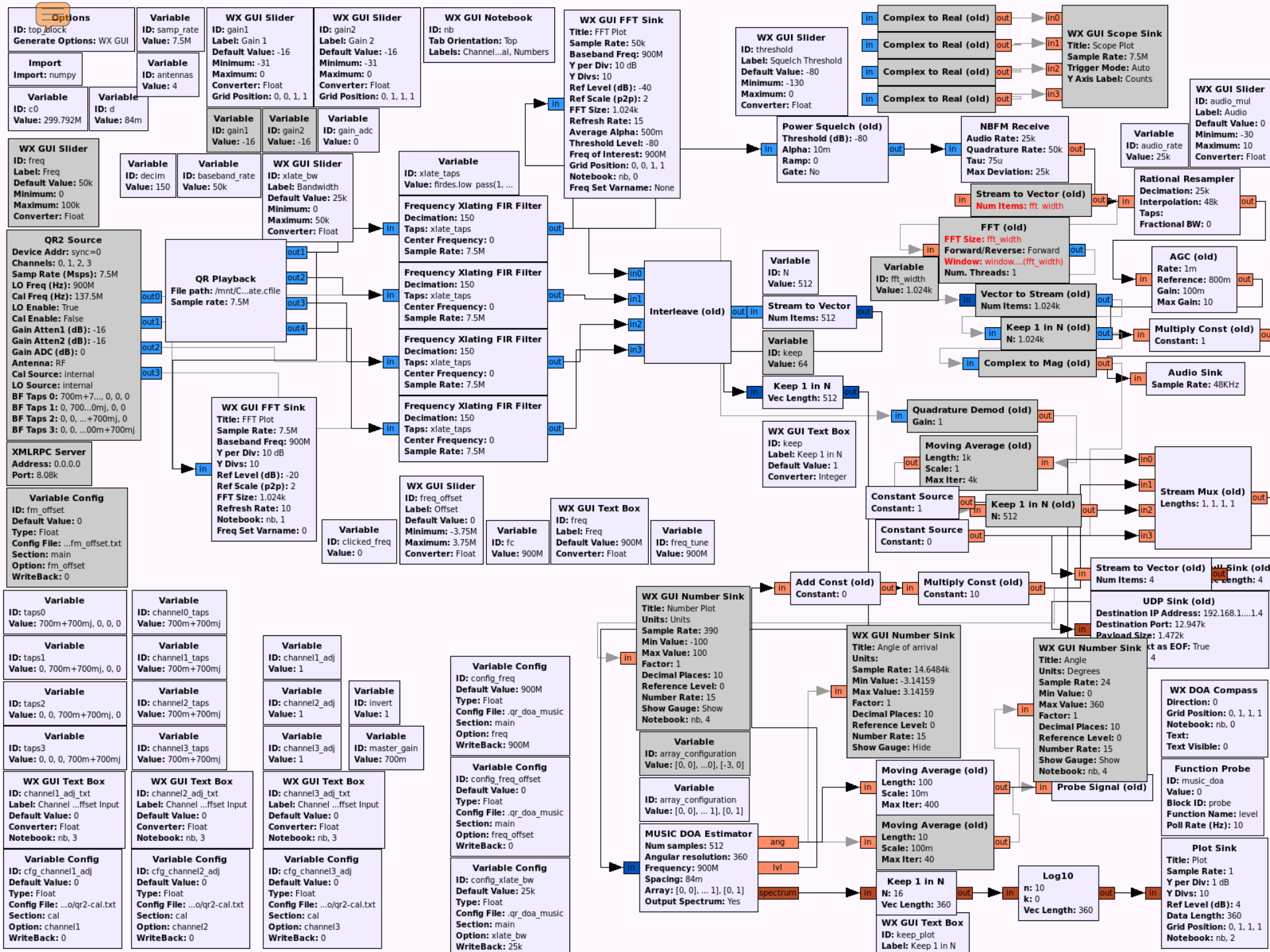
Probed phase 2: -170.943u

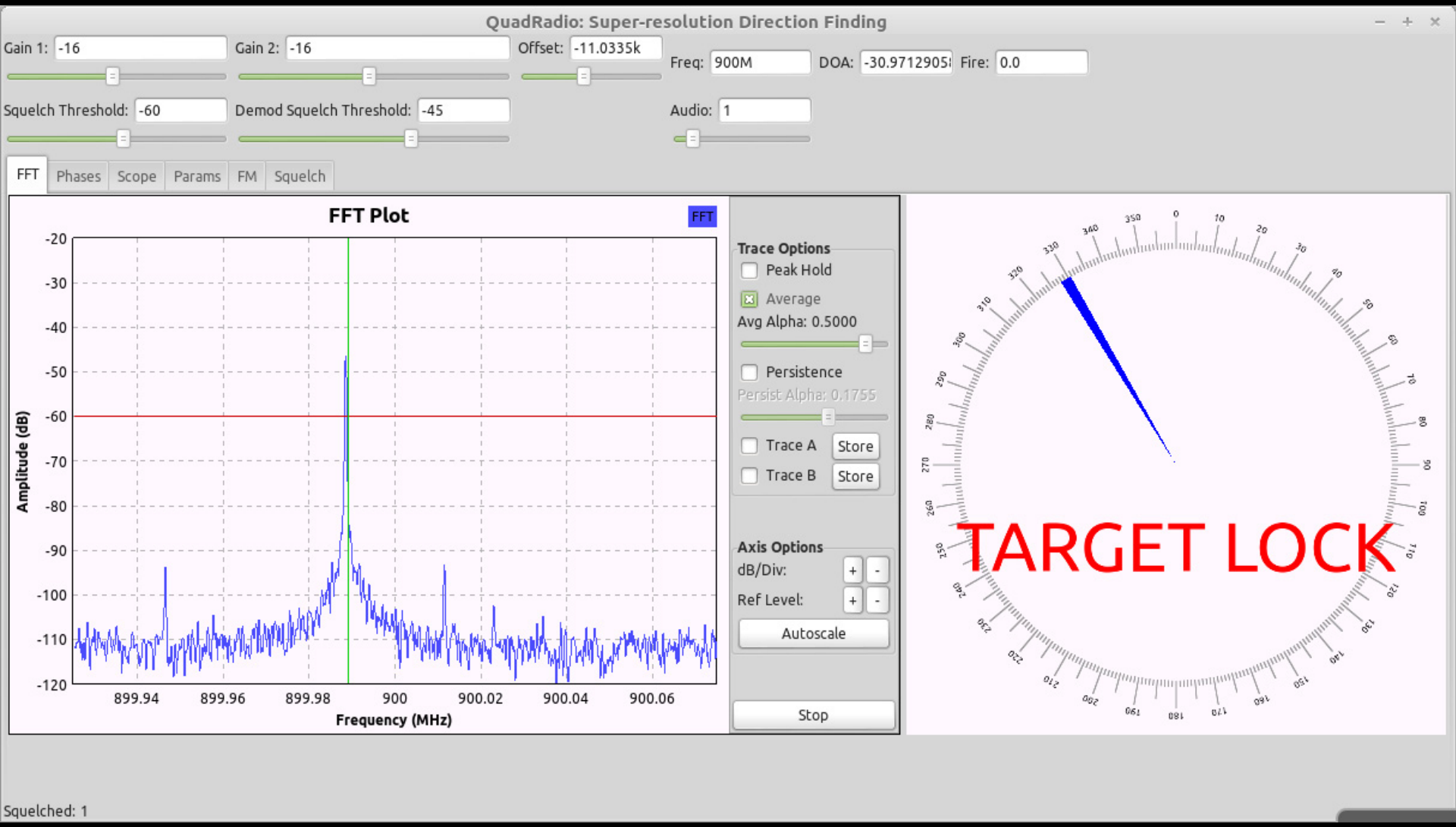
Probed phase 1: -37.9453u

Channel 3 Phase Offset Input: 123.942m

Channel 2 Phase Offset Input: 34.8406m

Channel 1 Phase Offset Input: 597.494m


Options
ID: top_block
Generate Options: WX GUI
Variable
ID: samp_rate
Value: 7.5M
WX GUI Slider
ID: gain1
Label: Gain 1
Default Value: -16
Minimum: -31
Maximum: 0
Converter: Float
Grid Position: 0, 0, 1, 1
WX GUI Slider
ID: gain2
Label: Gain 2
Default Value: -16
Minimum: -31
Maximum: 0
Converter: Float
Grid Position: 0, 1, 1, 1
WX GUI Notebook
ID: nb
Tab Orientation: Top
Labels: Channel...al, Numbers
WX GUI FFT Sink
Title: FFT Plot
Sample Rate: 50k
Baseband Freq: 900M
Y per Div: 10 dB
Y Divs: 10
Ref Level (dB): -40
Ref Scale (p2p): 2
FFT Size: 1.024k
Refresh Rate: 15
Average Alpha: 500m
Threshold Level: -80
Freq of Interest: 900M
Grid Position: 0, 0, 1, 1
Notebook: nb, 0
Freq Set Varname: None
WX GUI Slider
ID: threshold
Label: Squelch Threshold
Default Value: -80
Minimum: -130
Maximum: 0
Converter: Float
Complex to Real (old)
Complex to Real (old)
Complex to Real (old)
Complex to Real (old)
WX GUI Scope Sink
Title: Scope Plot
Sample Rate: 7.5M
Trigger Mode: Auto
Y Axis Label: Counts
WX GUI Slider
ID: audio_mul
Label: Audio
Default Value: 0
Minimum: -30
Maximum: 10
Converter: Float
Import
Import: numpy
Variable
ID: antennas
Value: 4
Variable
ID: c0
Value: 299.792M
Variable
ID: d
Value: 84m
Variable
ID: gain1
Value: -16
Variable
ID: gain2
Value: -16
Variable
ID: gain_adc
Value: 0
Power Squelch (old)
Threshold (dB): -80
Alpha: 10m
Ramp: 0
Gate: No
NBFM Receive
Audio Rate: 25k
Quadrature Rate: 50k
Tau: 75u
Max Deviation: 25k
Variable
ID: audio_rate
Value: 25k
WX GUI Slider
ID: freq
Label: Freq
Default Value: 50k
Minimum: 0
Maximum: 100k
Converter: Float
Variable
ID: decim
Value: 150
Variable
ID: baseband_rate
Value: 50k
WX GUI Slider
ID: xlate_bw
Label: Bandwidth
Default Value: 25k
Minimum: 0
Maximum: 50k
Converter: Float
Variable
ID: xlate_taps
Value: firdes.low_pass(1, ...
Stream to Vector (old)
Num Items: fft_width
Rational Resampler
Decimation: 25k
Interpolation: 48k
Taps:
Fractional BW: 0
QR2 Source
Device Addr: sync=0
Channels: 0, 1, 2, 3
Samp Rate (Msps): 7.5M
LO Freq (Hz): 900M
Cal Freq (Hz): 137.5M
LO Enable: True
Cal Enable: False
Gain Atten1 (dB): -16
Gain Atten2 (dB): -16
Gain ADC (dB): 0
Antenna: RF
Cal Source: internal
LO Source: internal
BF Taps 0: 700m+7..., 0, 0, 0
BF Taps 1: 0, 700...0mj, 0, 0
BF Taps 2: 0, 0, ...+700mj, 0
BF Taps 3: 0, 0, ...00m+700mj
QR Playback
File path: /mnt/C...ate.cfile
Sample rate: 7.5M
Frequency Xlating FIR Filter
Decimation: 150
Taps: xlate_taps
Center Frequency: 0
Sample Rate: 7.5M
Frequency Xlating FIR Filter
Decimation: 150
Taps: xlate_taps
Center Frequency: 0
Sample Rate: 7.5M
Frequency Xlating FIR Filter
Decimation: 150
Taps: xlate_taps
Center Frequency: 0
Sample Rate: 7.5M
Frequency Xlating FIR Filter
Decimation: 150
Taps: xlate_taps
Center Frequency: 0
Sample Rate: 7.5M
Interleave (old)
FFT (old)
FFT Size: fft_width
Forward/Reverse: Forward
Window: window....(fft_width)
Num. Threads: 1
Variable
ID: fft_width
Value: 1.024k
AGC (old)
Rate: 1m
Reference: 800m
Gain: 100m
Max Gain: 10
Variable
ID: N
Value: 512
Stream to Vector
Num Items: 512
Vector to Stream (old)
Num Items: 1.024k
Keep 1 in N (old)
N: 1.024k
Multiply Const (old)
Constant: 1
Variable
ID: keep
Value: 64
Keep 1 in N
Vec Length: 512
Complex to Mag (old)
Audio Sink
Sample Rate: 48KHz
WX GUI FFT Sink
Title: FFT Plot
Sample Rate: 7.5M
Baseband Freq: 900M
Y per Div: 10 dB
Y Divs: 10
Ref Level (dB): -20
Ref Scale (p2p): 2
FFT Size: 1.024k
Refresh Rate: 10
Notebook: nb, 1
Freq Set Varname: 0
Quadrature Demod (old)
Gain: 1
WX GUI Text Box
ID: keep
Label: Keep 1 in N
Default Value: 1
Converter: Integer
Moving Average (old)
Length: 1k
Scale: 1
Max Iter: 4k
Stream Mux (old)
Lengths: 1, 1, 1, 1
Constant Source
Constant: 1
Keep 1 in N (old)
N: 512
Constant Source
Constant: 0
XMLRPC Server
Address: 0.0.0.0
Port: 8.08k
Variable Config
ID: fm_offset
Default Value: 0
Type: Float
Config File: ...fm_offset.txt
Section: main
Option: fm_offset
WriteBack: 0
Variable
ID: clicked_freq
Value: 0
WX GUI Slider
ID: freq_offset
Label: Offset
Default Value: 0
Minimum: -3.75M
Maximum: 3.75M
Converter: Float
Variable
ID: fc
Value: 900M
WX GUI Text Box
ID: freq
Label: Freq
Default Value: 900M
Converter: Float
Variable
ID: freq_tune
Value: 900M
Stream to Vector (old)
Num Items: 4
UDP Sink (old)
Destination IP Address: 192.168.1....1.4
Destination Port: 12.947k
Payload Size: 1.472k
Send as EOF: True
Add Const (old)
Constant: 0
Multiply Const (old)
Constant: 10
WX GUI Number Sink
Title: Number Plot
Units: Units
Sample Rate: 390
Min Value: -100
Max Value: 100
Factor: 1
Decimal Places: 10
Reference Level: 0
Number Rate: 15
Show Gauge: Show
Notebook: nb, 4
WX GUI Number Sink
Title: Angle of arrival
Units:
Sample Rate: 14.6484k
Min Value: -3.14159
Max Value: 3.14159
Factor: 1
Decimal Places: 10
Reference Level: 0
Number Rate: 15
Show Gauge: Hide
WX GUI Number Sink
Title: Angle
Units: Degrees
Sample Rate: 24
Min Value: 0
Max Value: 360
Factor: 1
Decimal Places: 10
Reference Level: 0
Number Rate: 15
Show Gauge: Show
Notebook: nb, 4
WX DOA Compass
Direction: 0
Grid Position: 0, 1, 1, 1
Notebook: nb, 0
Text:
Text Visible: 0
Variable
ID: array_configuration
Value: [0, 0], ...0], [-3, 0]
Variable
ID: array_configuration
Value: [0, 0], ... 1], [0, 1]
Moving Average (old)
Length: 100
Scale: 10m
Max Iter: 400
Moving Average (old)
Length: 10
Scale: 100m
Max Iter: 40
Probe Signal (old)
Function Probe
ID: music_doa
Value: 0
Block ID: probe
Function Name: level
Poll Rate (Hz): 10
MUSIC DOA Estimator
Num samples: 512
Angular resolution: 360
Frequency: 900M
Spacing: 84m
Array: [0, 0], ... 1], [0, 1]
Output Spectrum: Yes
ang
lvl
spectrum
Keep 1 in N
N: 16
Vec Length: 360
Log10
n: 10
k: 0
Vec Length: 360
Plot Sink
Title: Plot
Sample Rate: 1
Y per Div: 1 dB
Y Divs: 10
Ref Level (dB): 4
Data Length: 360
Grid Position: 0, 1, 1, 1
Notebook: nb, 2
WX GUI Text Box
ID: keep_plot
Label: Keep 1 in N
Variable
ID: taps0
Value: 700m+700mj, 0, 0, 0
Variable
ID: taps1
Value: 0, 700m+700mj, 0, 0
Variable
ID: taps2
Value: 0, 0, 700m+700mj, 0
Variable
ID: taps3
Value: 0, 0, 0, 700m+700mj
Variable
ID: channel0_taps
Value: 700m+700mj
Variable
ID: channel1_taps
Value: 700m+700mj
Variable
ID: channel2_taps
Value: 700m+700mj
Variable
ID: channel3_taps
Value: 700m+700mj
Variable
ID: channel1_adj
Value: 1
Variable
ID: channel2_adj
Value: 1
Variable
ID: channel3_adj
Value: 1
Variable
ID: invert
Value: 1
Variable
ID: master_gain
Value: 700m
WX GUI Text Box
ID: channel1_adj_txt
Label: Channel ...ffset Input
Default Value: 0
Converter: Float
Notebook: nb, 3
WX GUI Text Box
ID: channel2_adj_txt
Label: Channel ...ffset Input
Default Value: 0
Converter: Float
Notebook: nb, 3
WX GUI Text Box
ID: channel3_adj_txt
Label: Channel ...ffset Input
Default Value: 0
Converter: Float
Notebook: nb, 3
Variable Config
ID: cfg_channel1_adj
Default Value: 0
Type: Float
Config File: ...o/qr2-cal.txt
Section: cal
Option: channel1
WriteBack: 0
Variable Config
ID: cfg_channel2_adj
Default Value: 0
Type: Float
Config File: ...o/qr2-cal.txt
Section: cal
Option: channel2
WriteBack: 0
Variable Config
ID: cfg_channel3_adj
Default Value: 0
Type: Float
Config File: ...o/qr2-cal.txt
Section: cal
Option: channel3
WriteBack: 0
Variable Config
ID: config_freq
Default Value: 900M
Type: Float
Config File: .qr_doa_music
Section: main
Option: freq
WriteBack: 900M
Variable Config
ID: config_freq_offset
Default Value: 0
Type: Float
Config File: .qr_doa_music
Section: main
Option: freq_offset
WriteBack: 0
Variable Config
ID: config_xlate_bw
Default Value: 25k
Type: Float
Config File: .qr_doa_music
Section: main
Option: xlate_bw
WriteBack: 25k


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

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

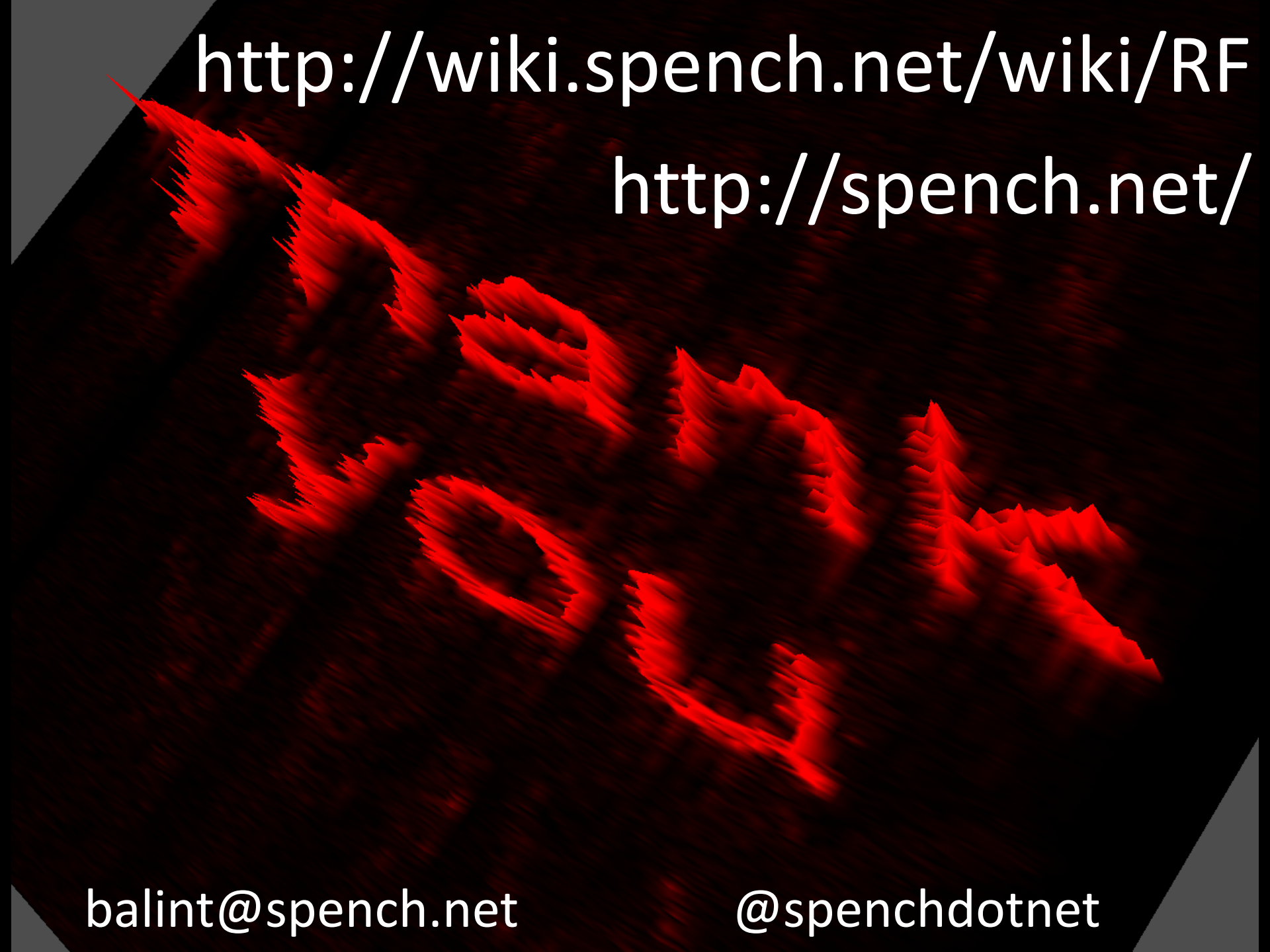
- Uplink power is generally kept at the minimum level to save money
- Depends on the weather:
  - Clear sky: a few W
  - Heavy rain: a few kW
- Turn yours up to (theirs + 1)

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.


Remember: be legal and be….
SAFE
BOSCH
BOSCH

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

http://spench.net/



balint@spench.net

@spenchdotnet