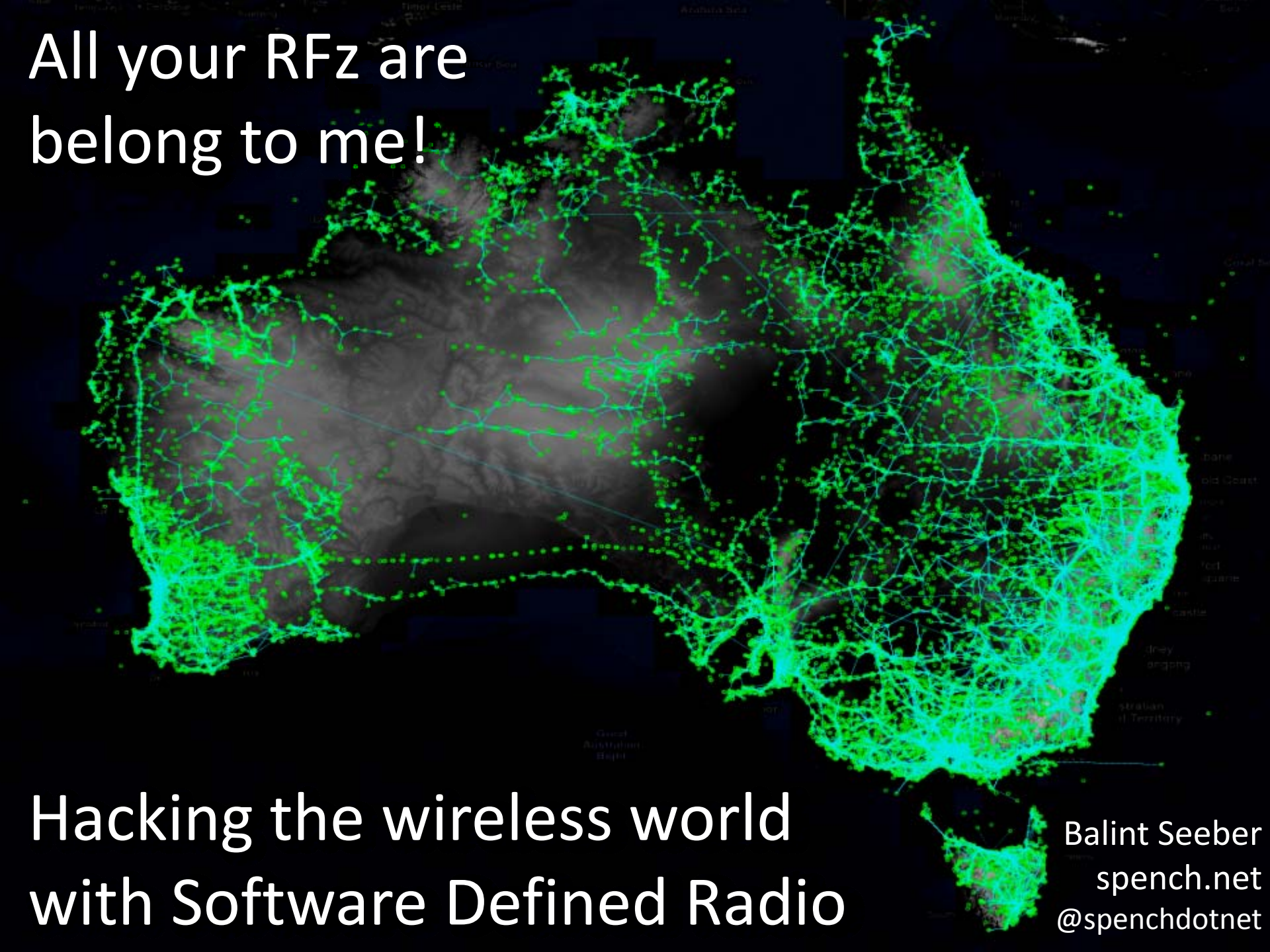


Hacking the wireless world with Software Defined Radio

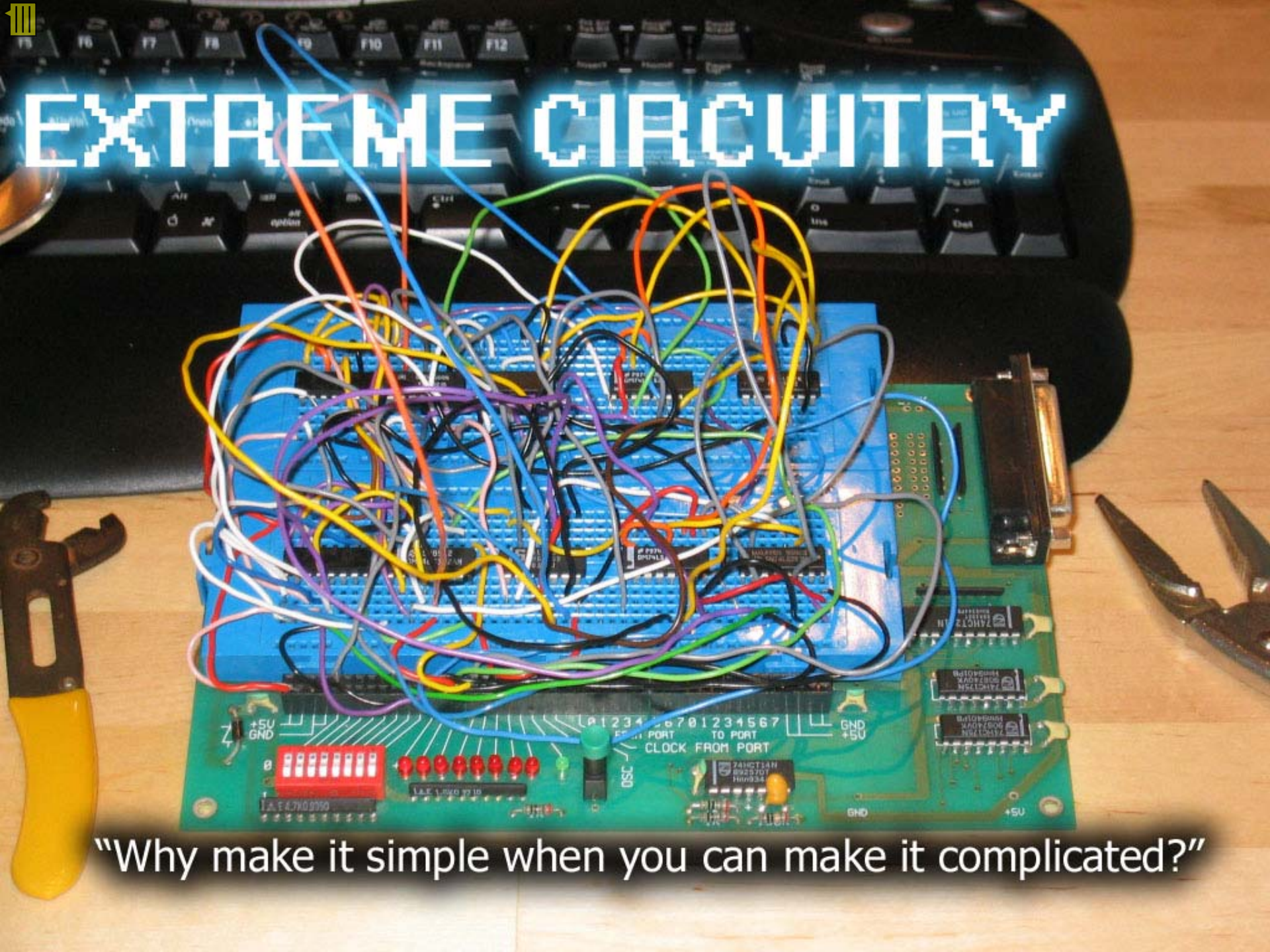
Balint Seeber
spench.net
@spenchdotnet

Overview

- Introduction
- The Australian Geographical RadioFrequency Map
  (as a research tool)
- Security through obscurity in hospital pager systems
- Tracking planes in your local airspace:
  combined Mode S transponder and ACARS receiver
- Decoding satellite-downlink traffic

About me

EXTREME CIRCUITRY

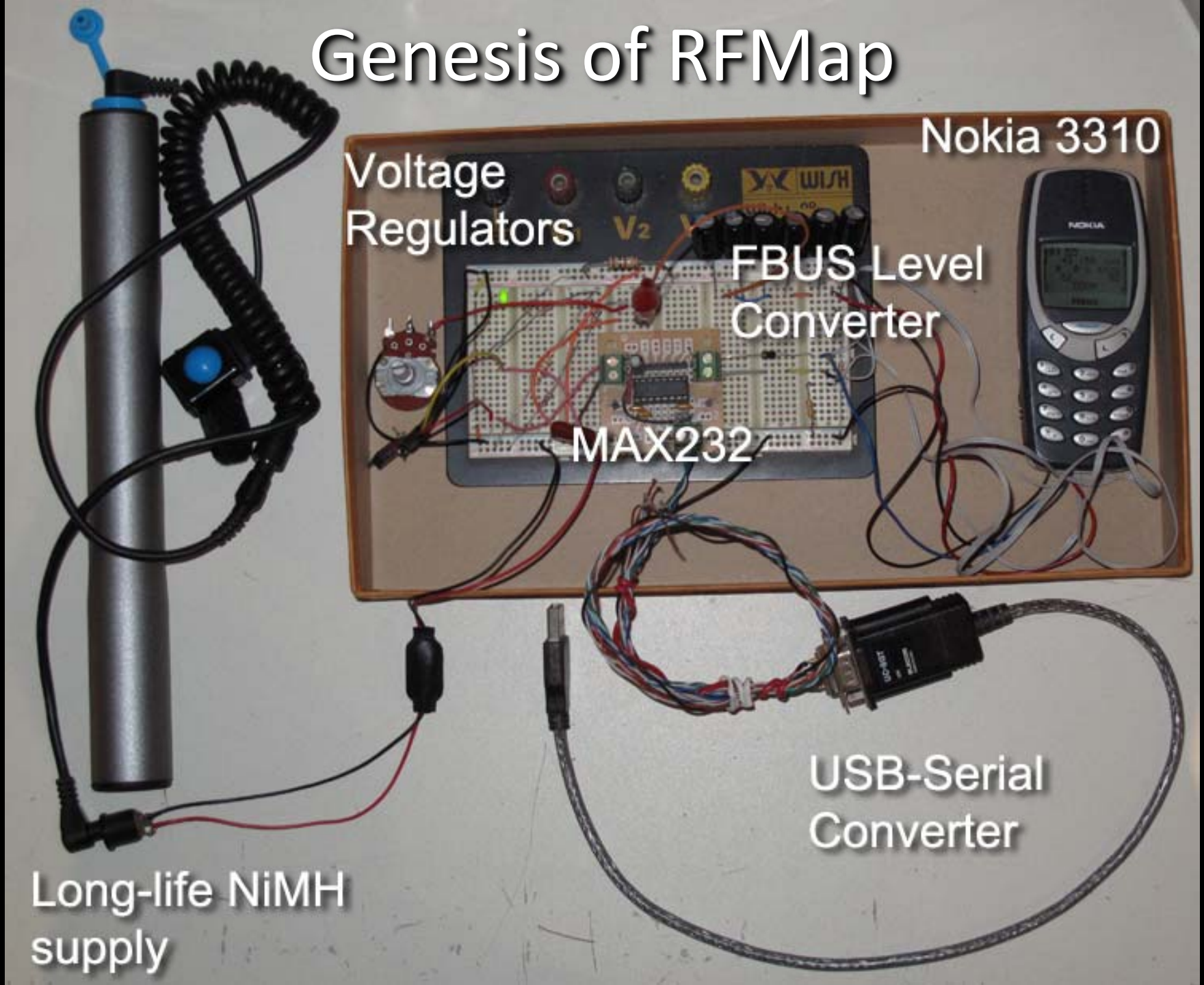


"Why make it simple when you can make it complicated?"

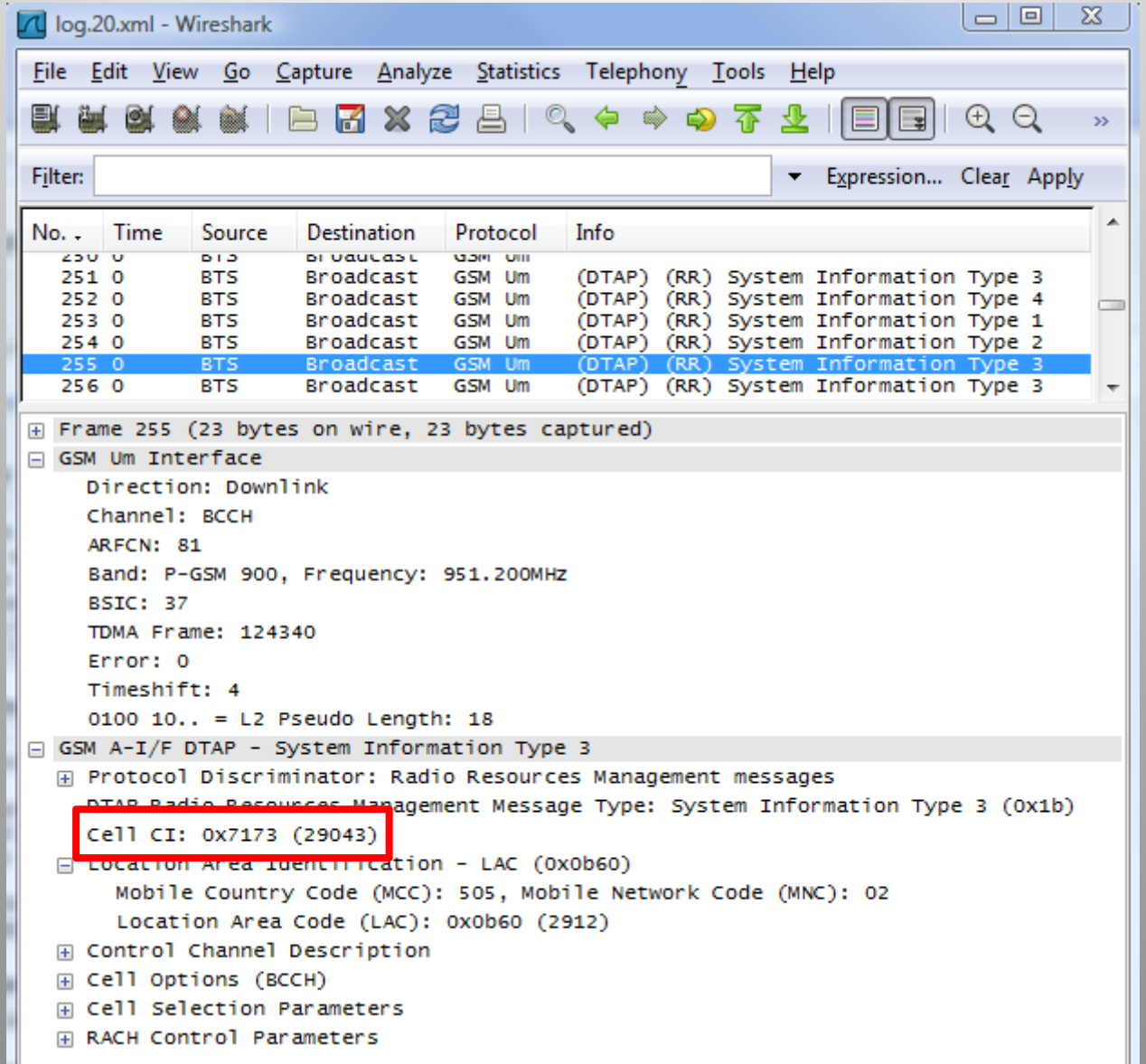
The Australian Geographical RadioFrequency Map

"RFMap"

Genesis of RFMap

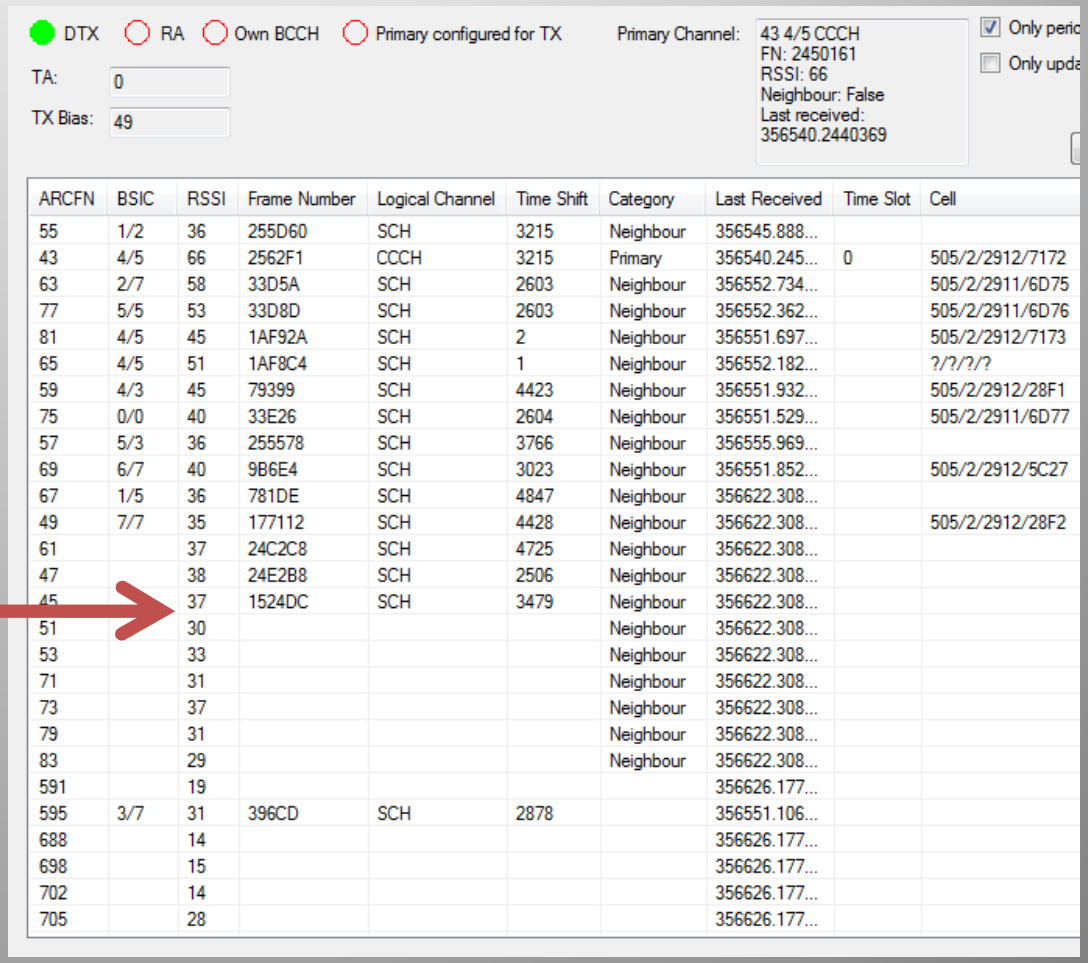


GSM + Gammu + Wireshark



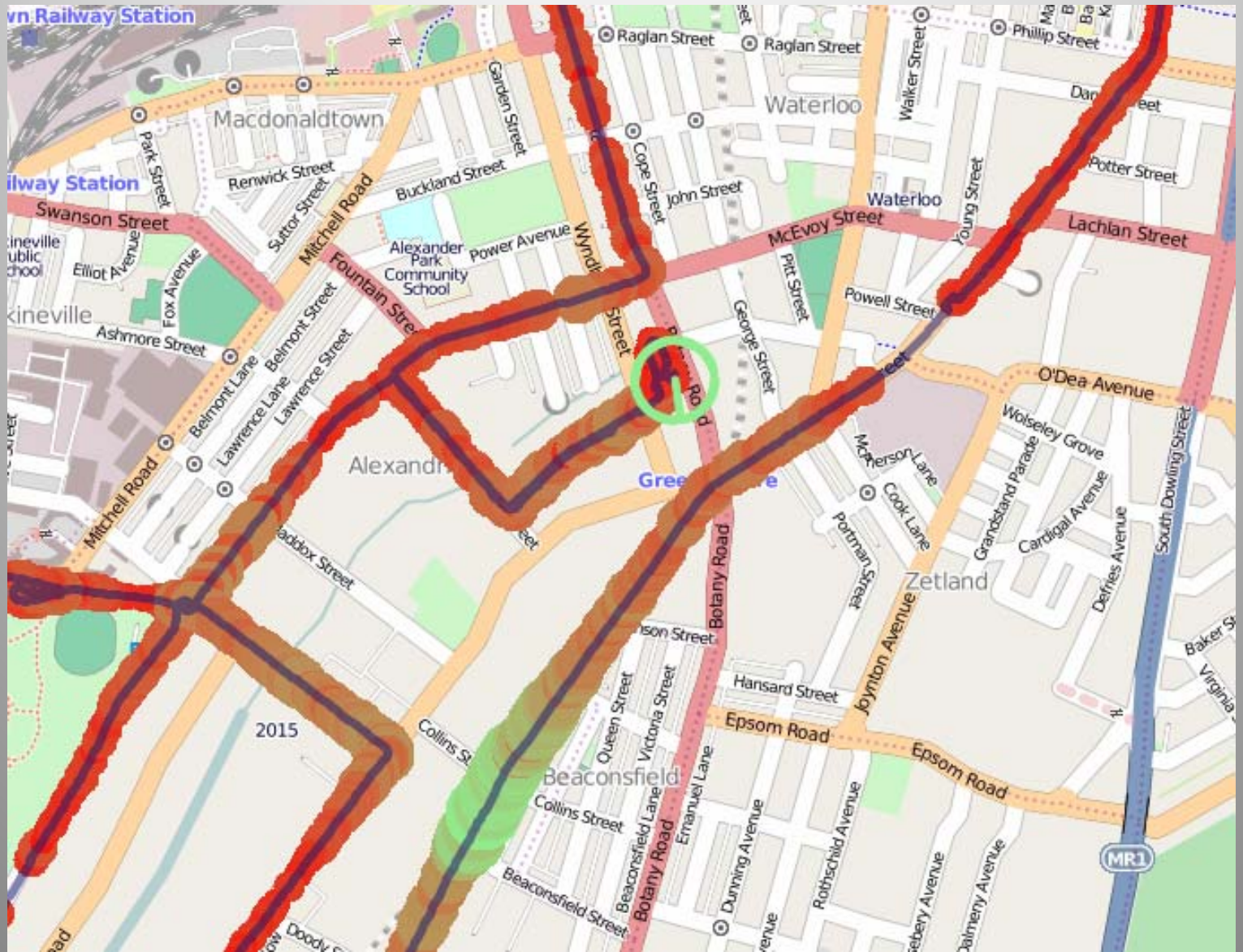
Field Test Mode

<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

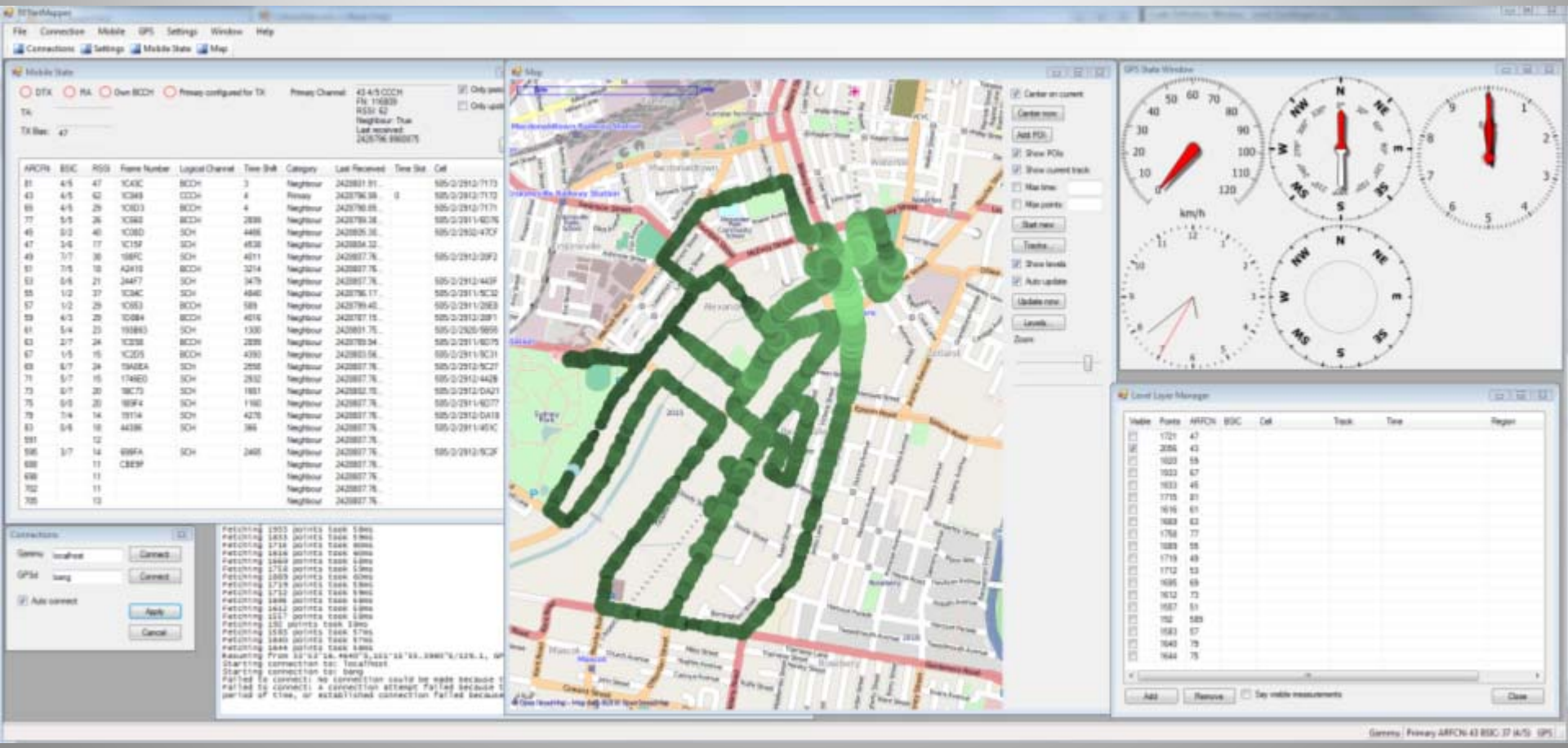


ARCFN	BSIC	RSSI	Frame Number	Logical Channel	Time Shift	Category	Last Received	Time Slot	Cell
55	1/2	36	255D60	SCH	3215	Neighbour	356545.888...		
43	4/5	66	2562F1	CCCH	3215	Primary	356540.245...	0	505/2/2912/7172
63	2/7	58	33D5A	SCH	2603	Neighbour	356552.734...		505/2/2911/6D75
77	5/5	53	33D8D	SCH	2603	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

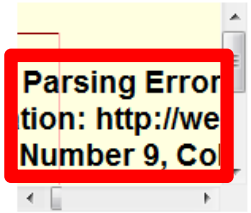
Found **10526** sites within about a **200 kms** radius of: **Latitude: -34 17 47.782 Longitude: 150 56 20.778.**
Coordinate Projection: Australian Geodetic Datum 1966 [AGD66]
[List Nearby Sites] [New Site Search]

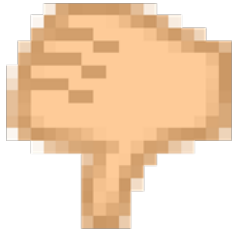
Pan 3 4 5 6 Zoom IN OUT

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]				

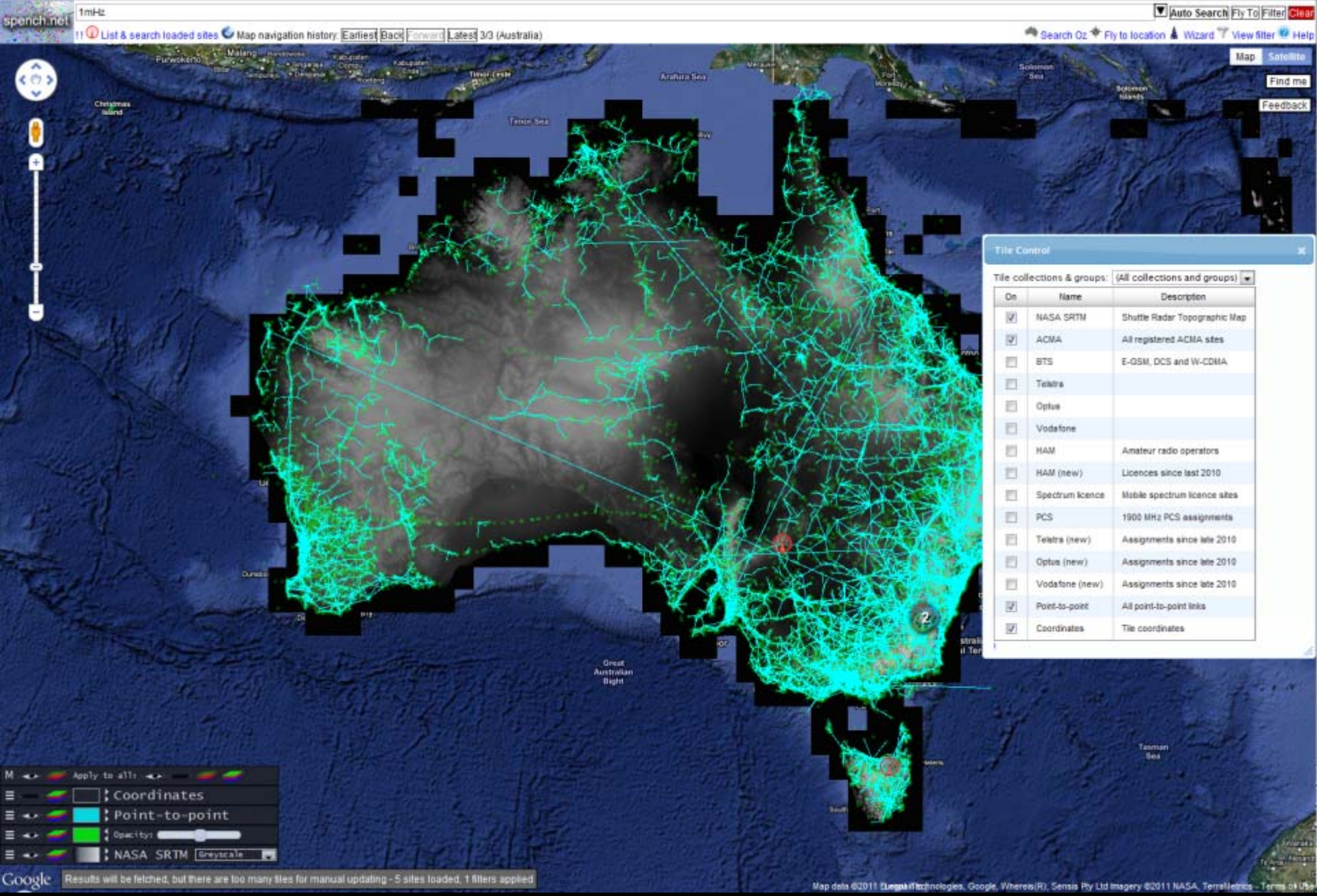




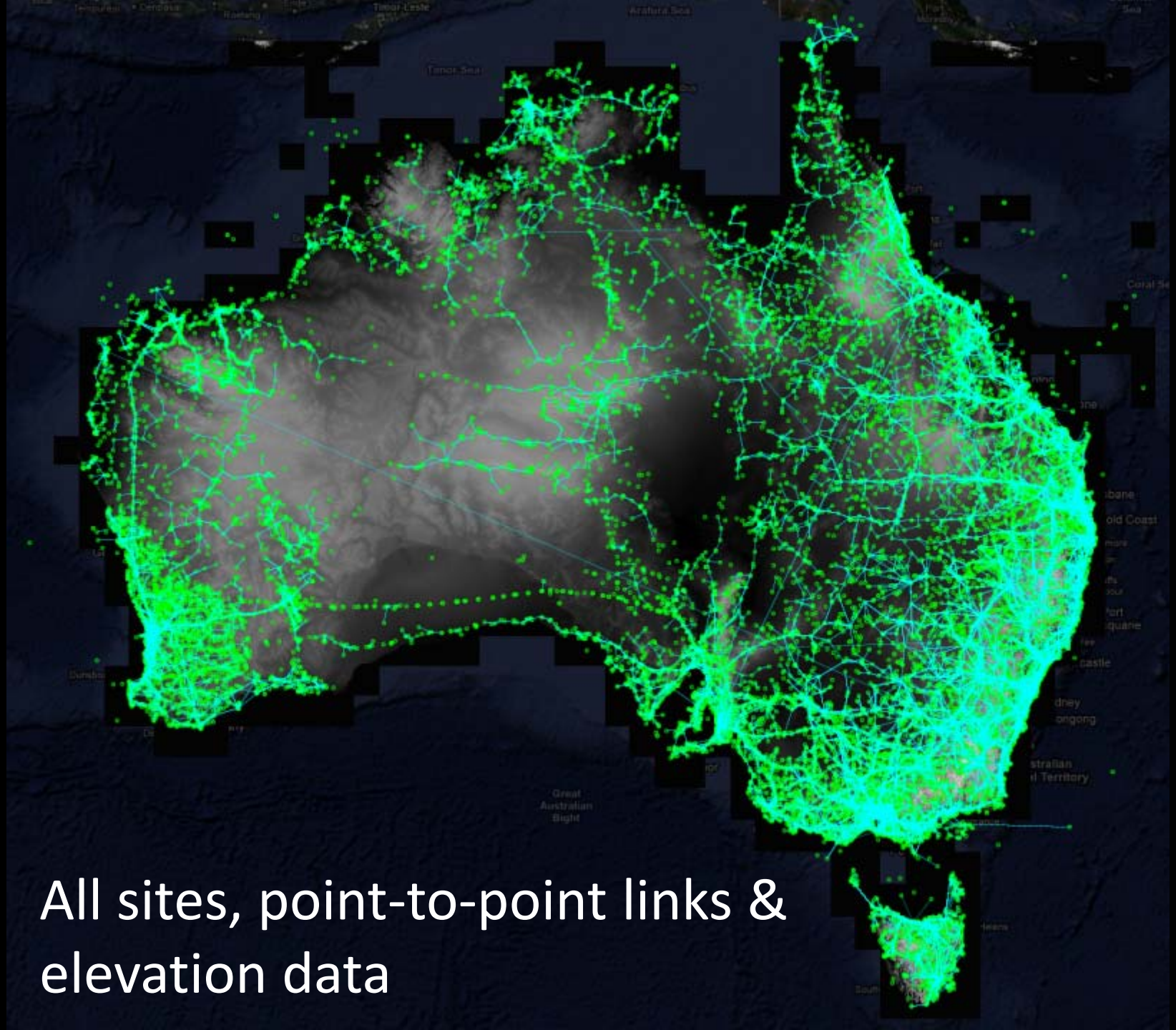
Site proximity usage notes;

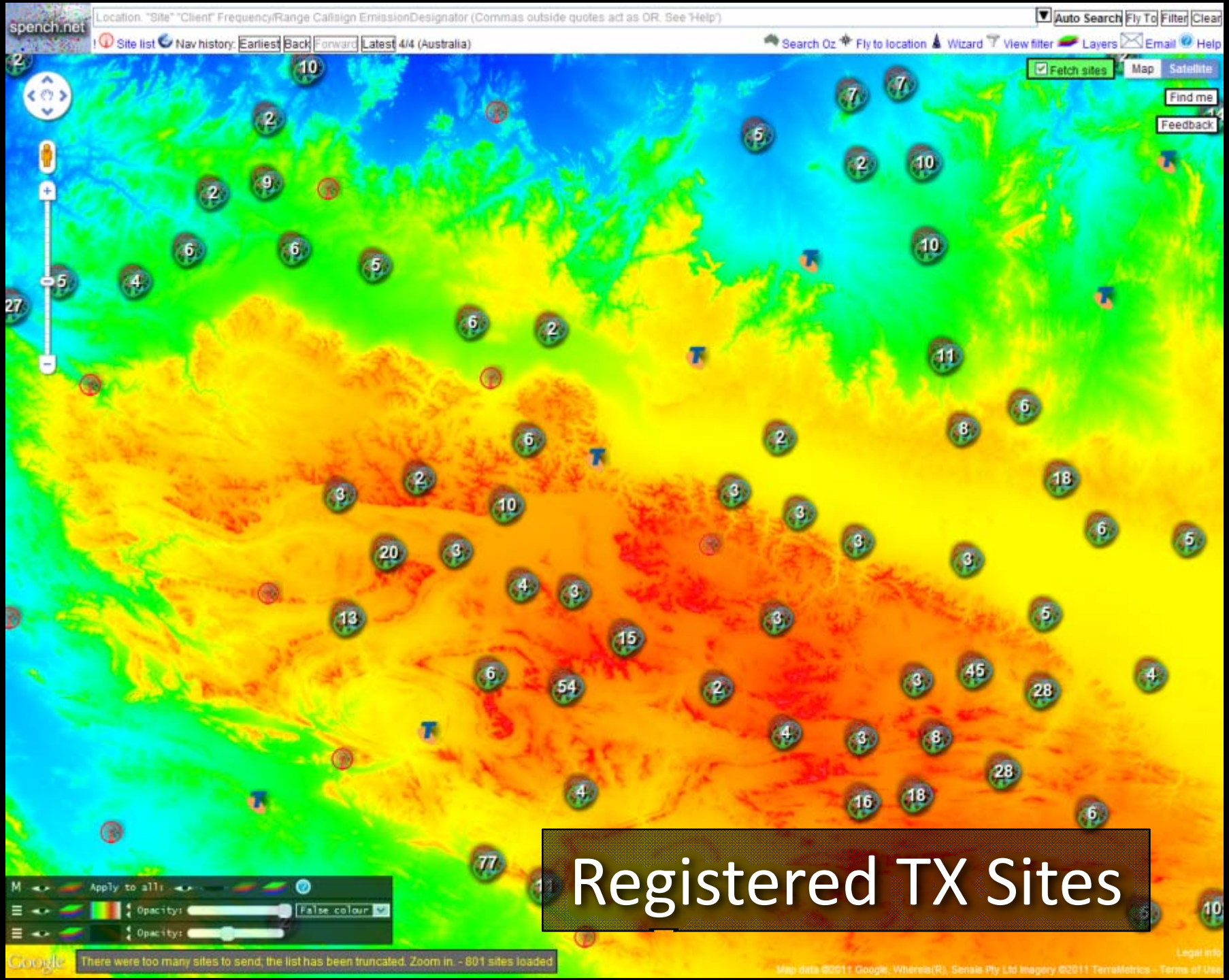
- Map display accuracy within 10 metres.
- Distances shown are approximations only (they are not latitude compensated).
- To view images correclty, browser's must be able to accept both Javascript and compressed SVG content.
- You can **download** the SVG viewer Ver 3.0 from Adobe to view site search 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.

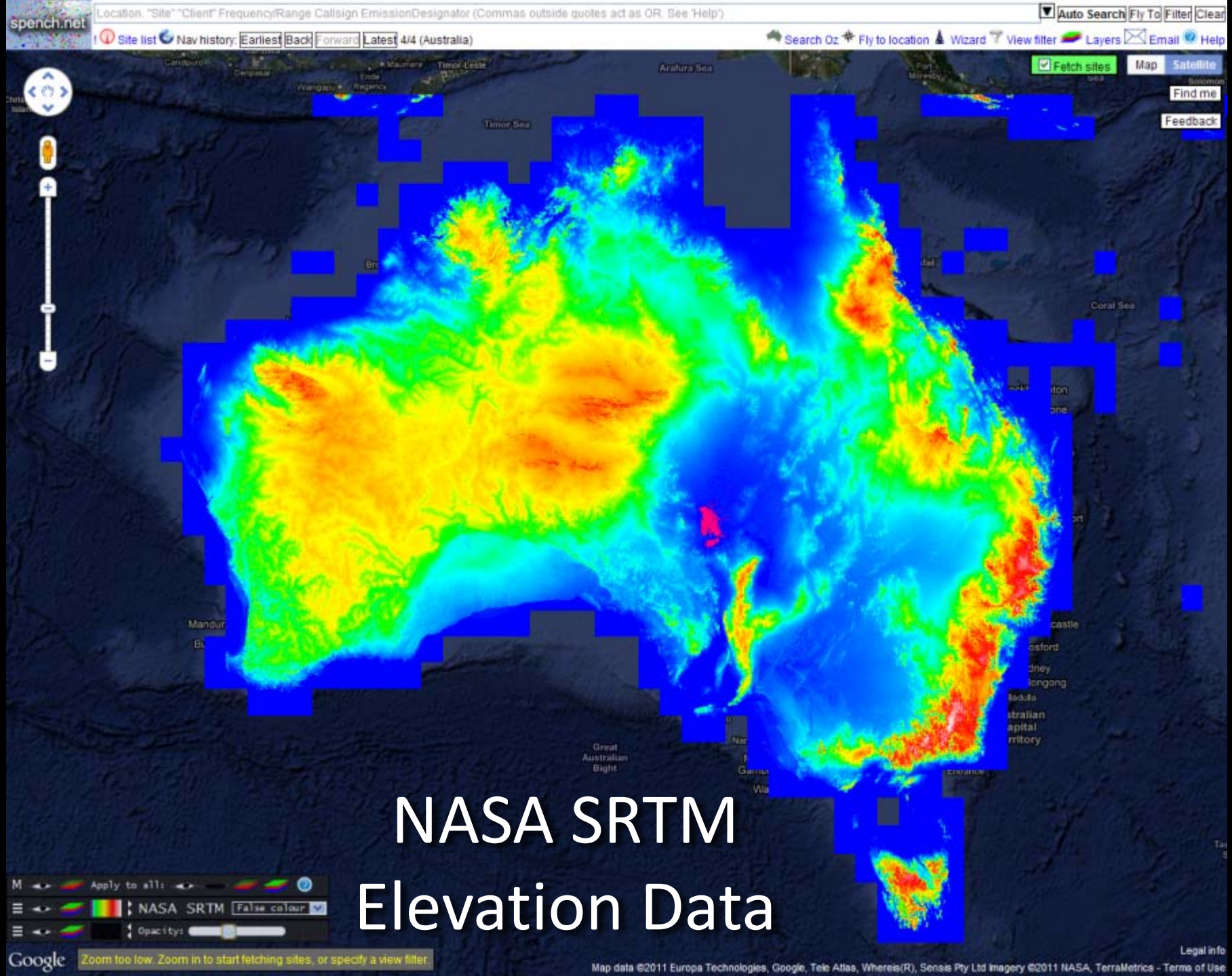
Enter RFMap…



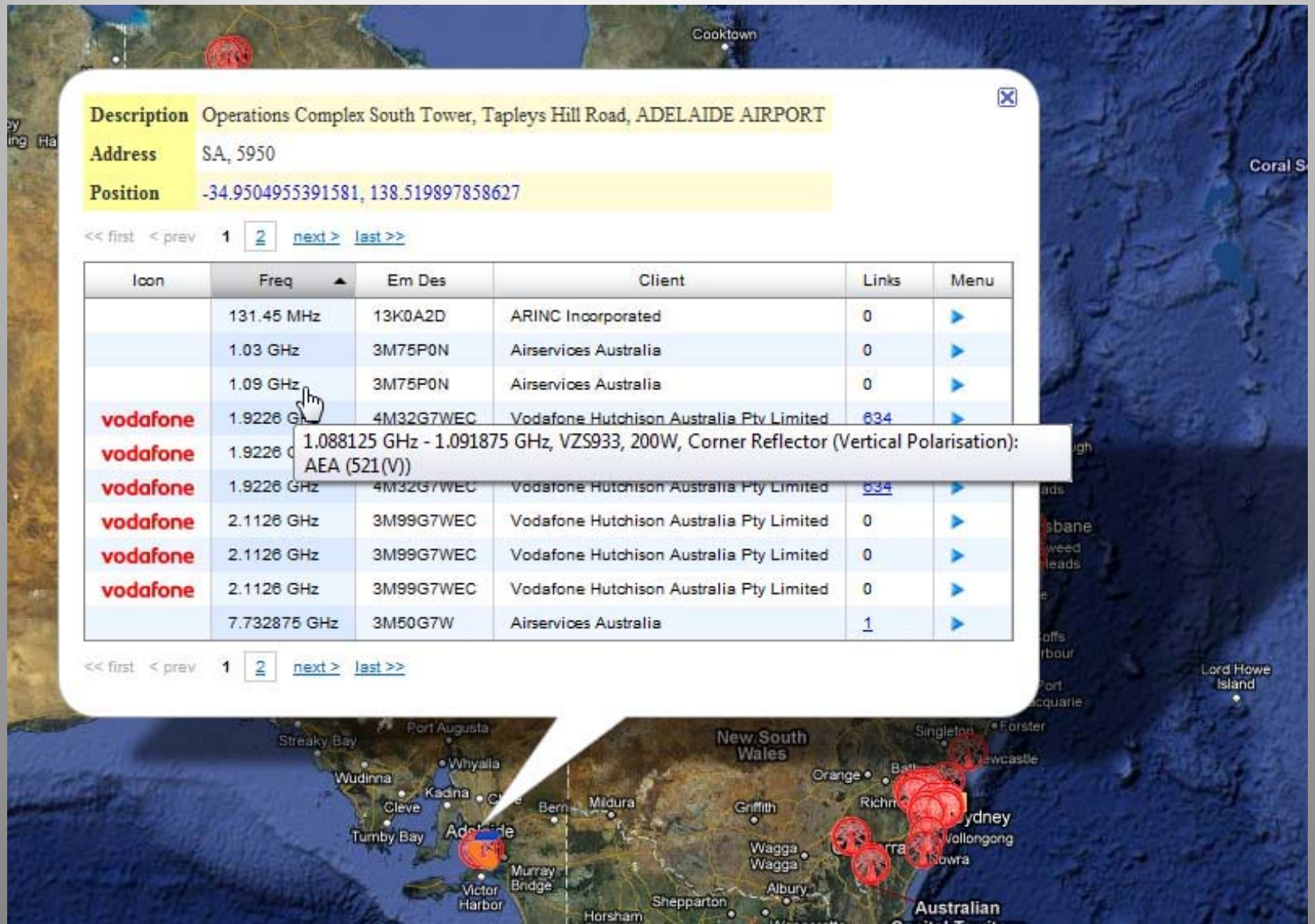
The RFMap web interface


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

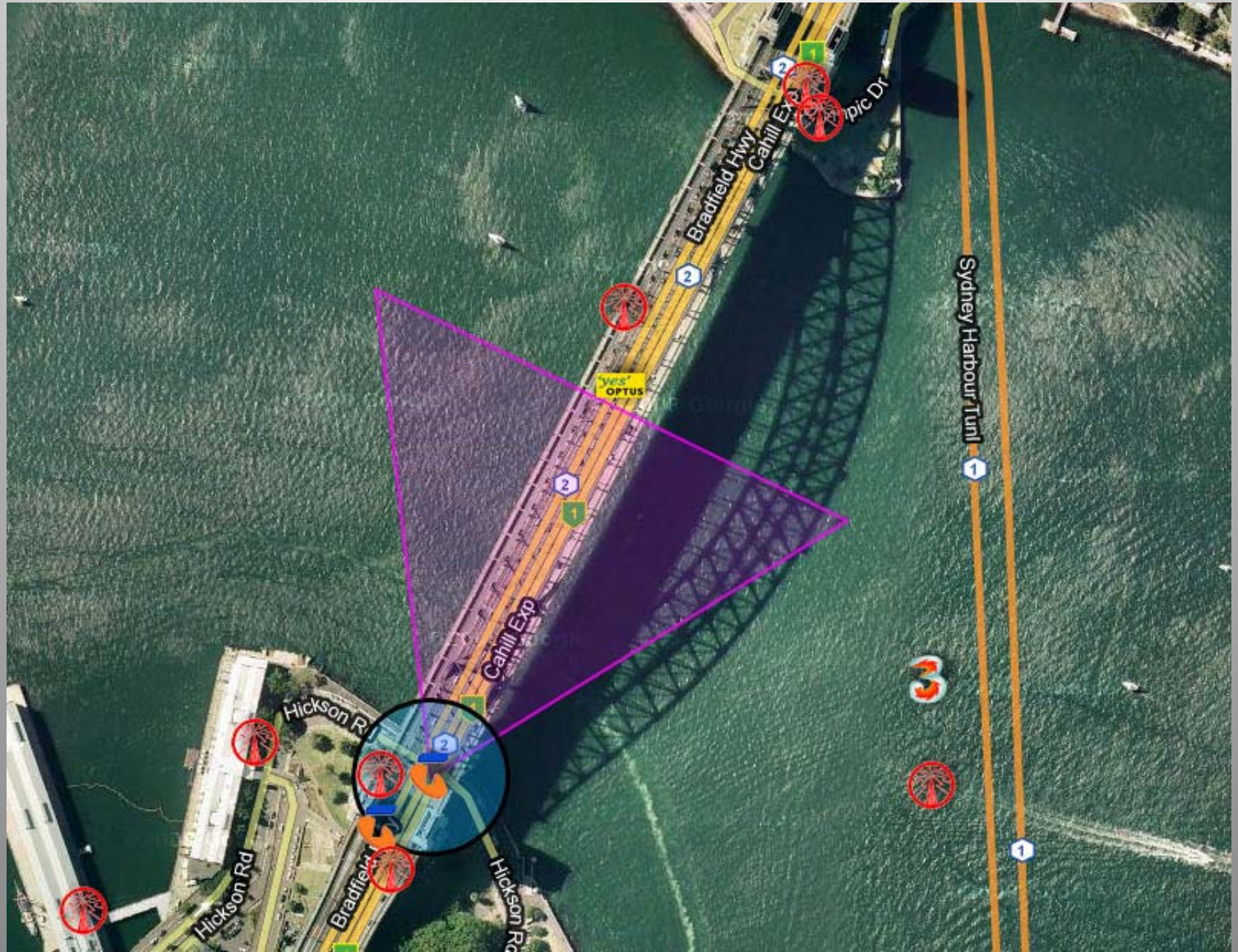

spench.net
Location: "Site" "Client" Frequency/Range Callsign EmissionDesignator (Commas outside quotes act as OR. See 'Help')
Auto Search
Fly To
Filter
Clear
Site list
Nav history:
Earliest
Back
Forward
Latest
4/4 (Australia)
Search Oz
Fly to location
Wizard
View filter
Layers
Email
Help
Fetch sites
Map
Satellite
Find me
Feedback
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
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

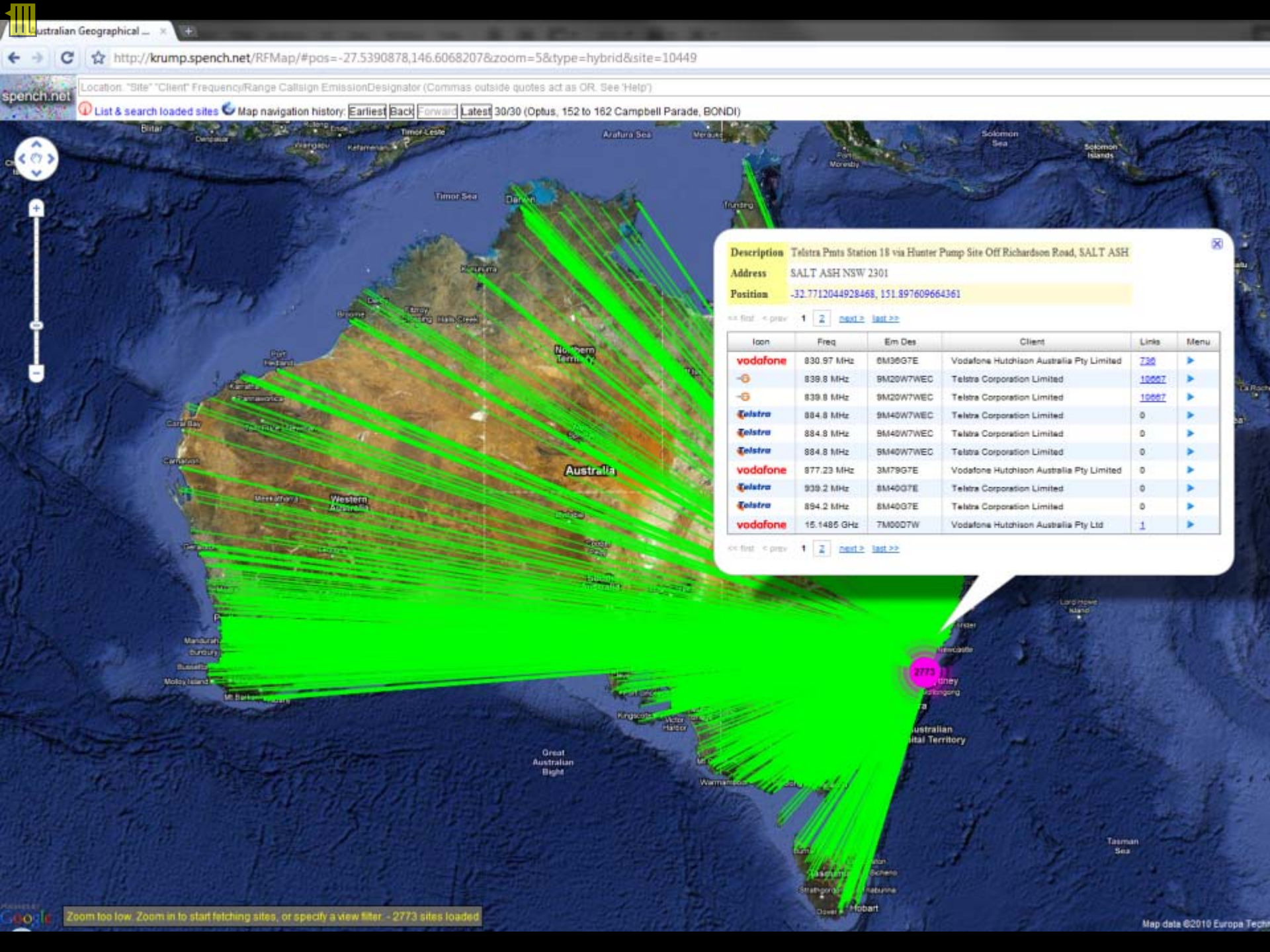
Site details: frequency assignments

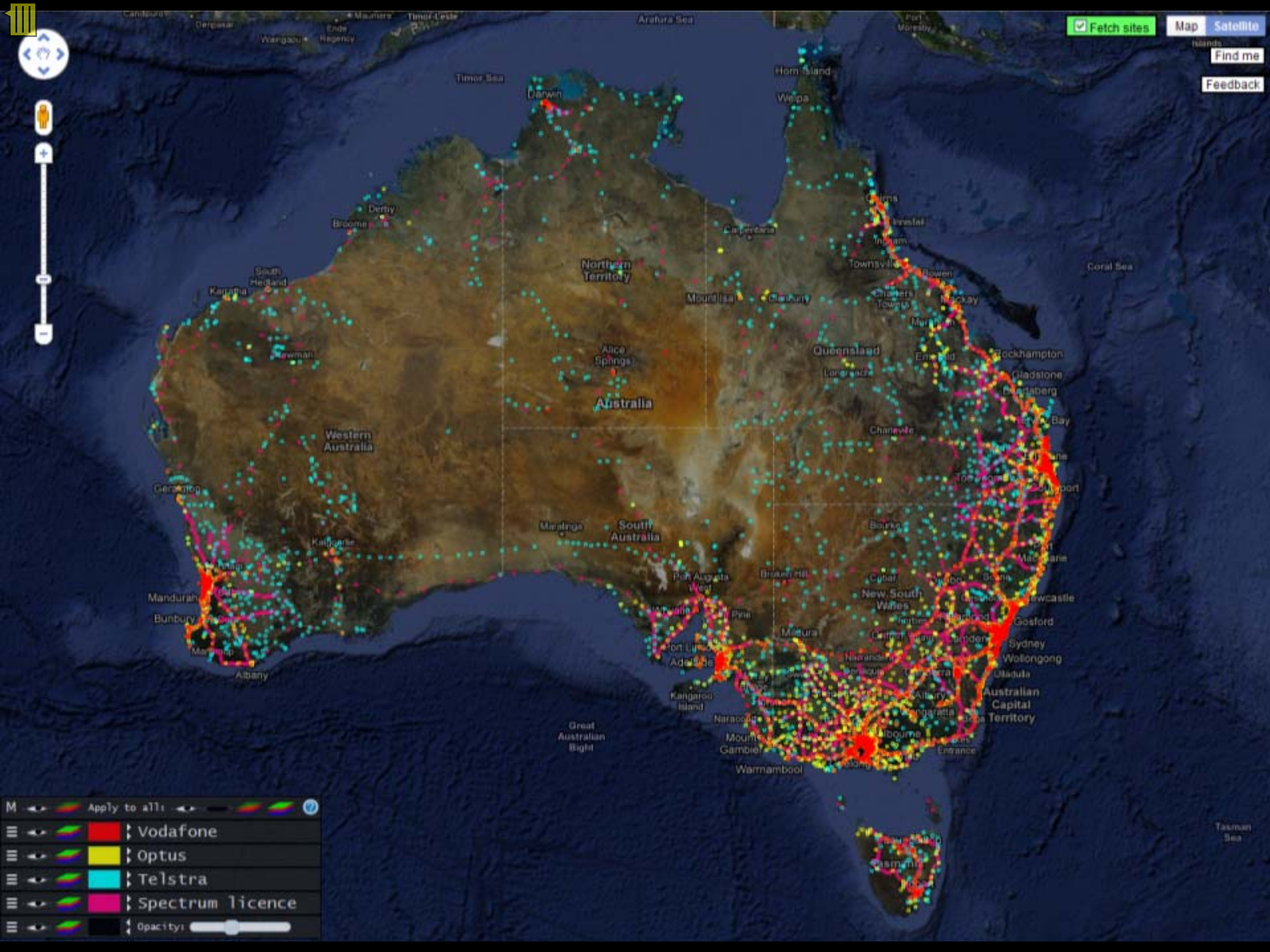


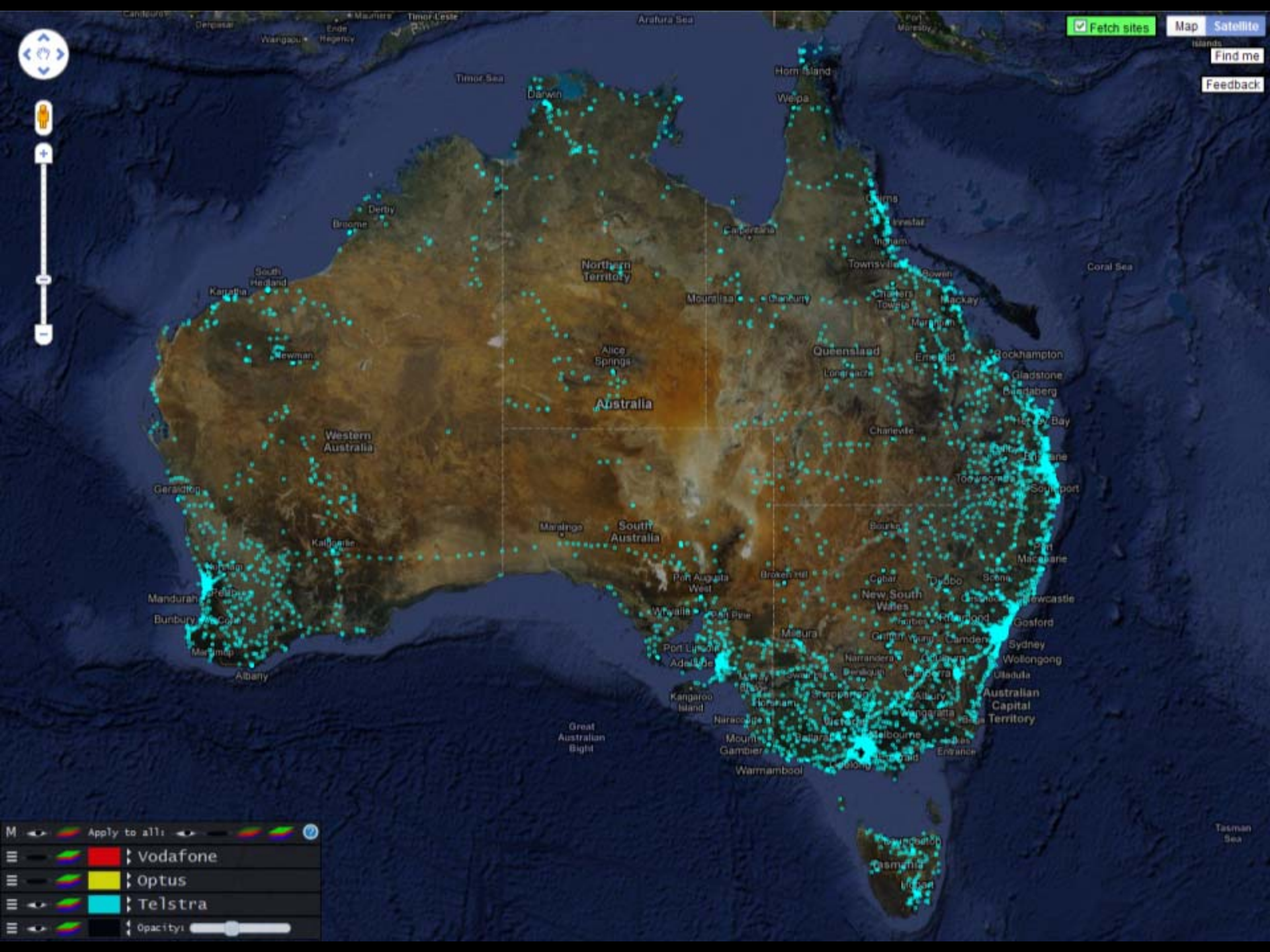
Antenna radiation pattern*

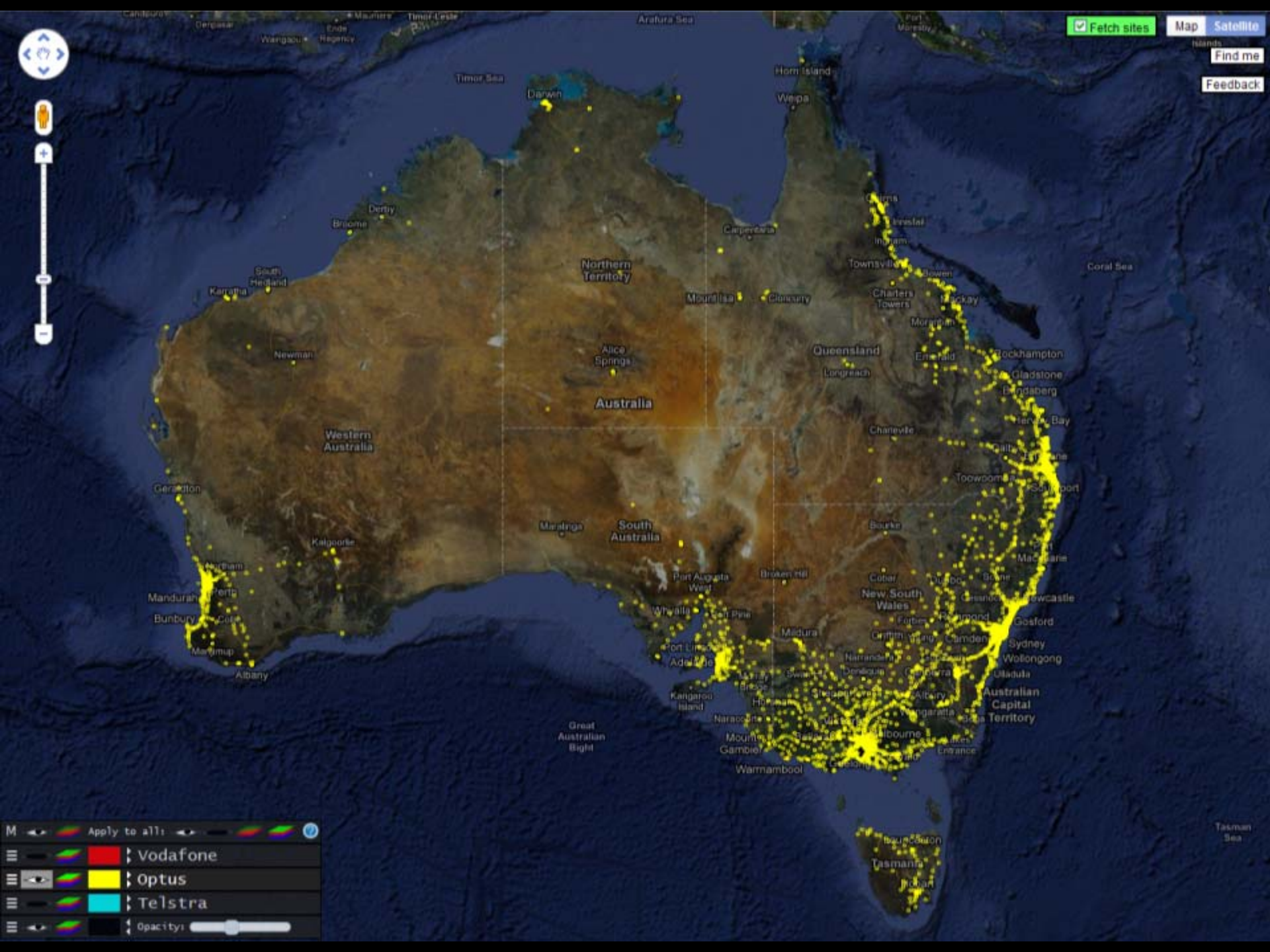


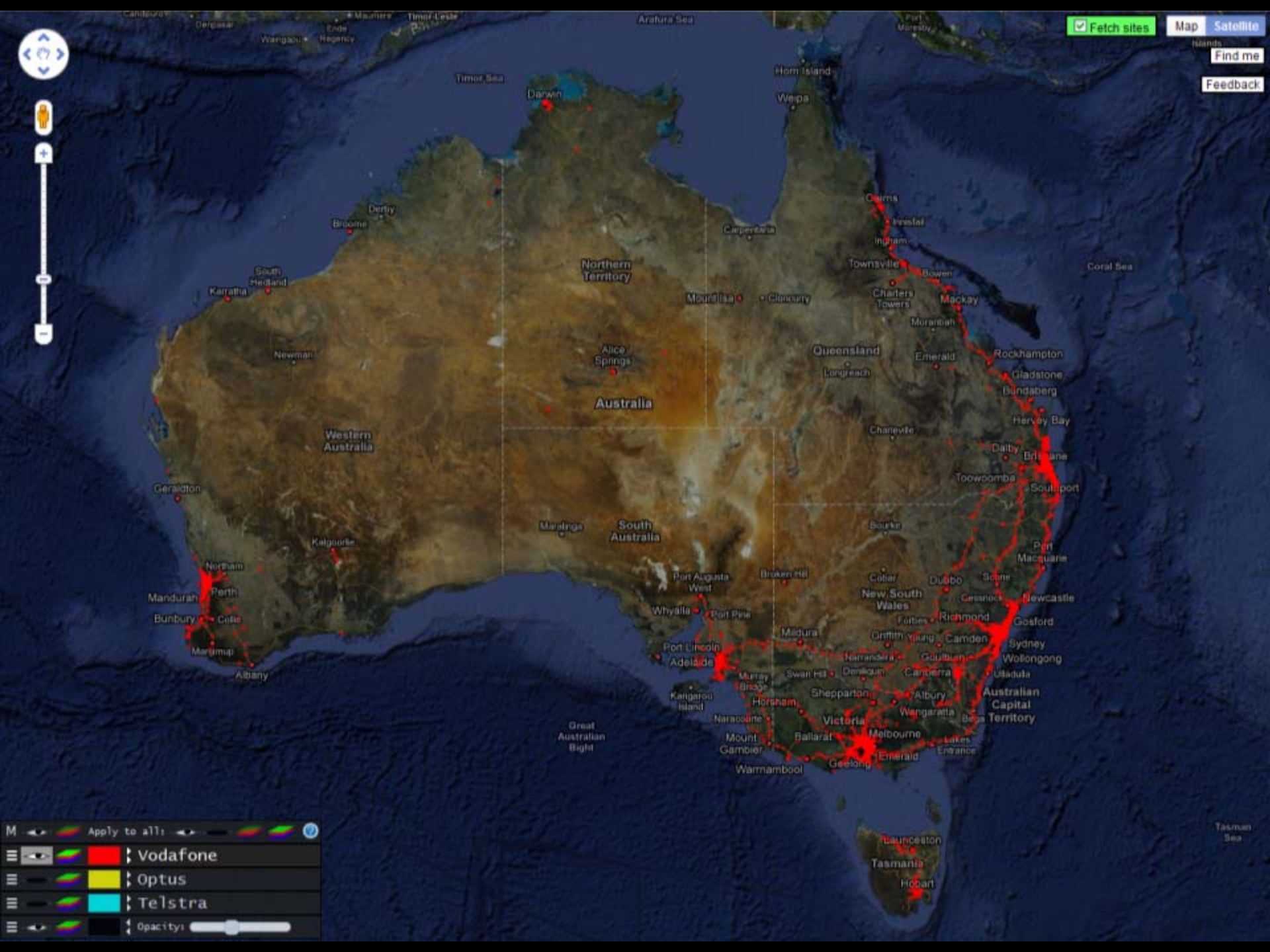

Description Waterboard Tower Villiers Road, HORSLEY PARK
Address HORSLEY PARK NSW 2164
Position -33.8620599886948, 150.850654339945
Sorting by client
<< first < prev 1 2 3 4 5 6 7 8 9 10 next > last >>
Icon | Freq | Em Des | Client | Links | Menu
151.5 MHz | 10K1F2D | Bureau of Meteorology | 1
151.5 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
Cobbitty
Narellan
Camden
Elderslie
Camden South
Douglas Park
Wilton
Sans Souci
Dolans Bay
Bundeena
Airport

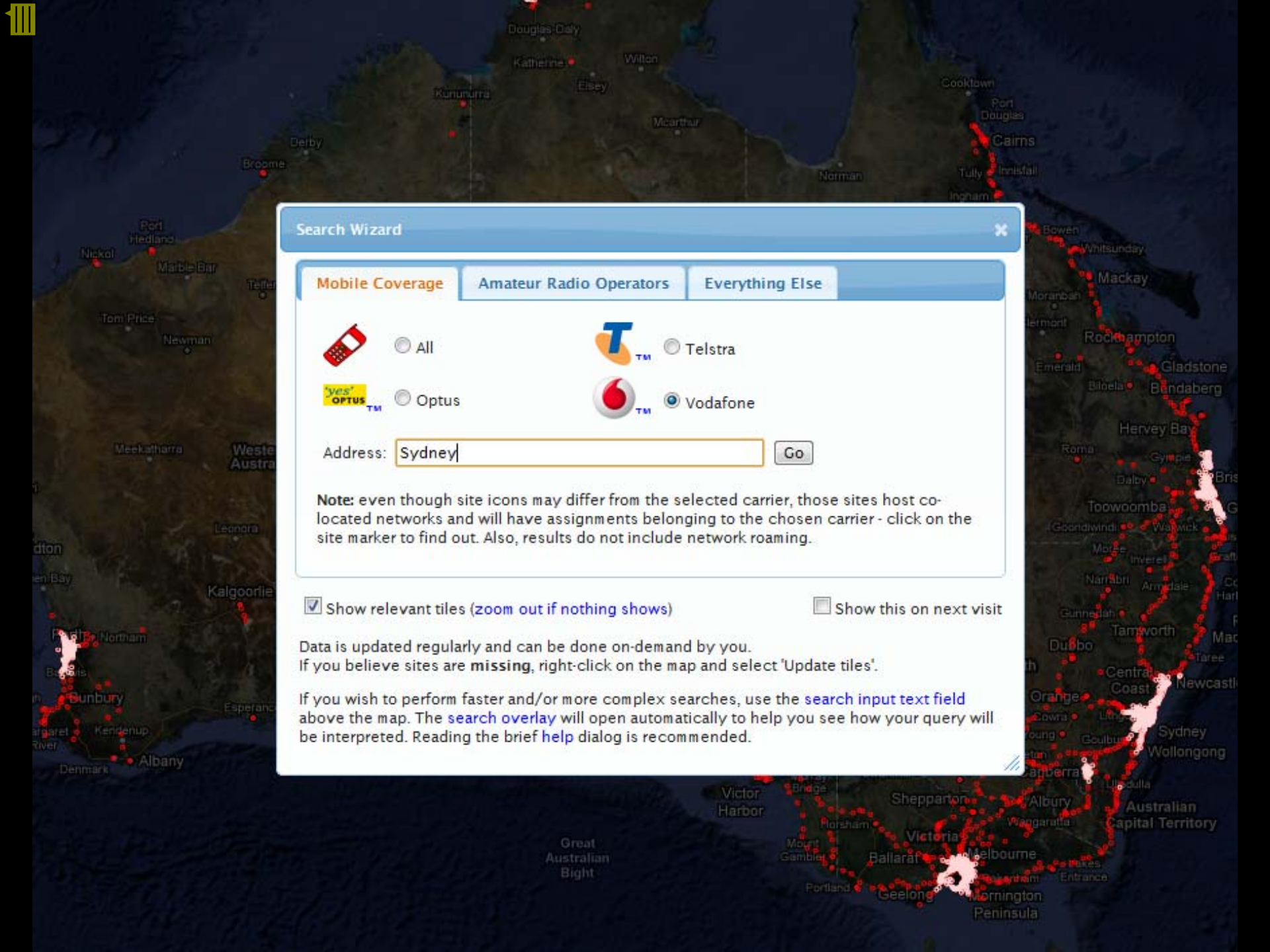

Australian Geographical ...
http://krump.spench.net/RFMap/#pos=-27.5390878,146.6068207&zoom=5&type=hybrid&site=10449
spench.net
Location: "Site" "Client" Frequency/Range Callsign EmissionDesignator (Commas outside quotes act as OR. See 'Help')
List & search loaded sites
Map navigation history: Earliest 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
Telstra | 839.8 MHz | 9M20W7WEC | Telstra Corporation Limited | 10667
Telstra | 839.8 MHz | 9M20W7WEC | Telstra Corporation Limited | 10667
Telstra | 884.8 MHz | 9M40W7WEC | Telstra Corporation Limited | 0
Telstra | 884.8 MHz | 9M40W7WEC | Telstra Corporation Limited | 0
Telstra | 884.8 MHz | 9M40W7WEC | Telstra Corporation Limited | 0
vodafone | 877.23 MHz | 3M79G7E | Vodafone Hutchison Australia Pty Limited | 0
Telstra | 939.2 MHz | 8M40G7E | Telstra Corporation Limited | 0
Telstra | 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
Hobart
2773
Zoom too low. Zoom in to start fetching sites, or specify a view filter. - 2773 sites loaded
Map data ©2010 Europa Tech

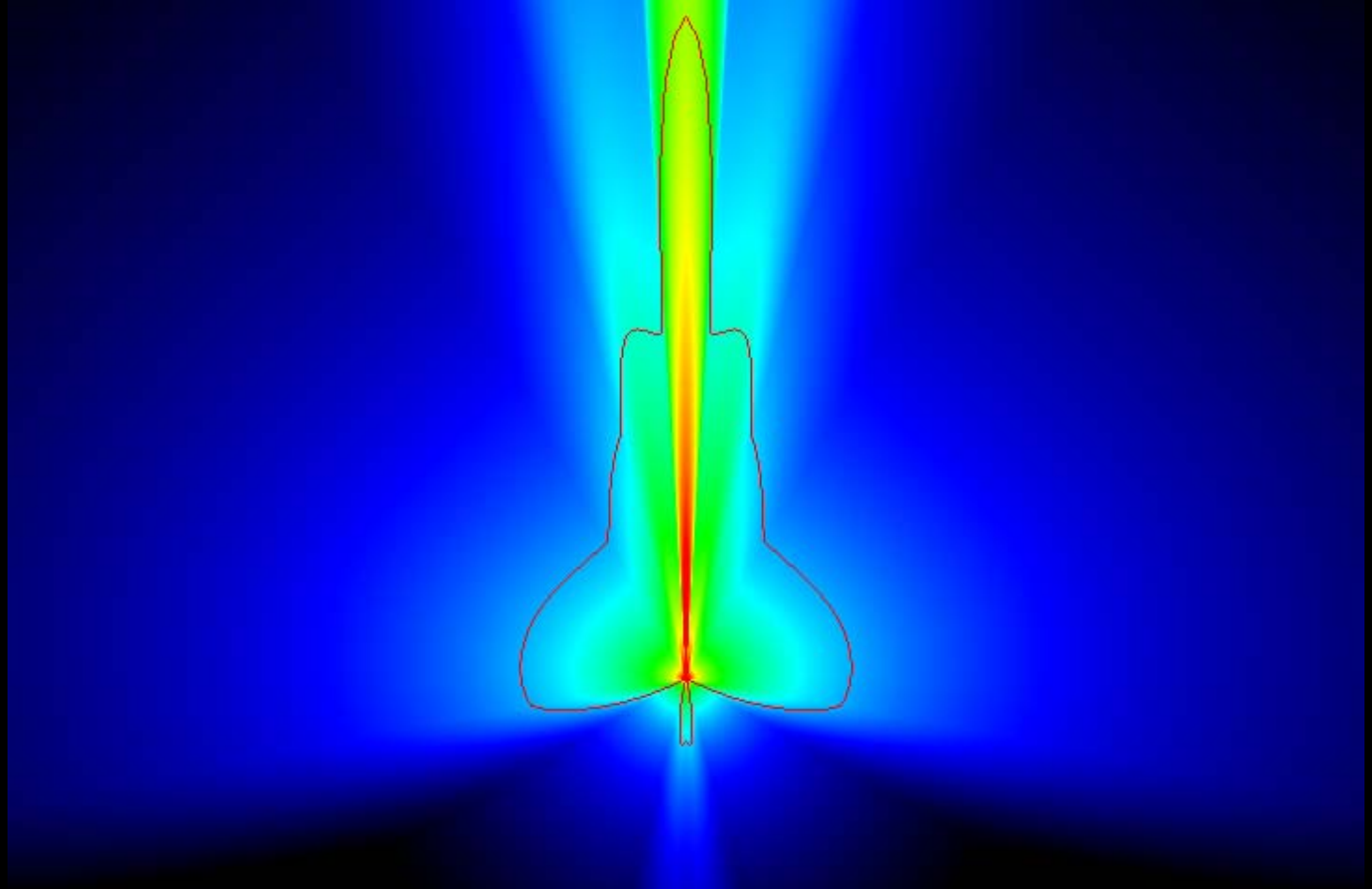

Fetch sites
Map
Satellite
Find me
Feedback
Vodafone
Optus
Telstra
Spectrum licence
Apply to all:
Opacity:
Australia
Northern Territory
Western Australia
South Australia
Queensland
New South Wales
Australian Capital Territory
Darwin
Perth
Adelaide
Brisbane
Sydney
Melbourne
Coral Sea
Tasman Sea
Great Australian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


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

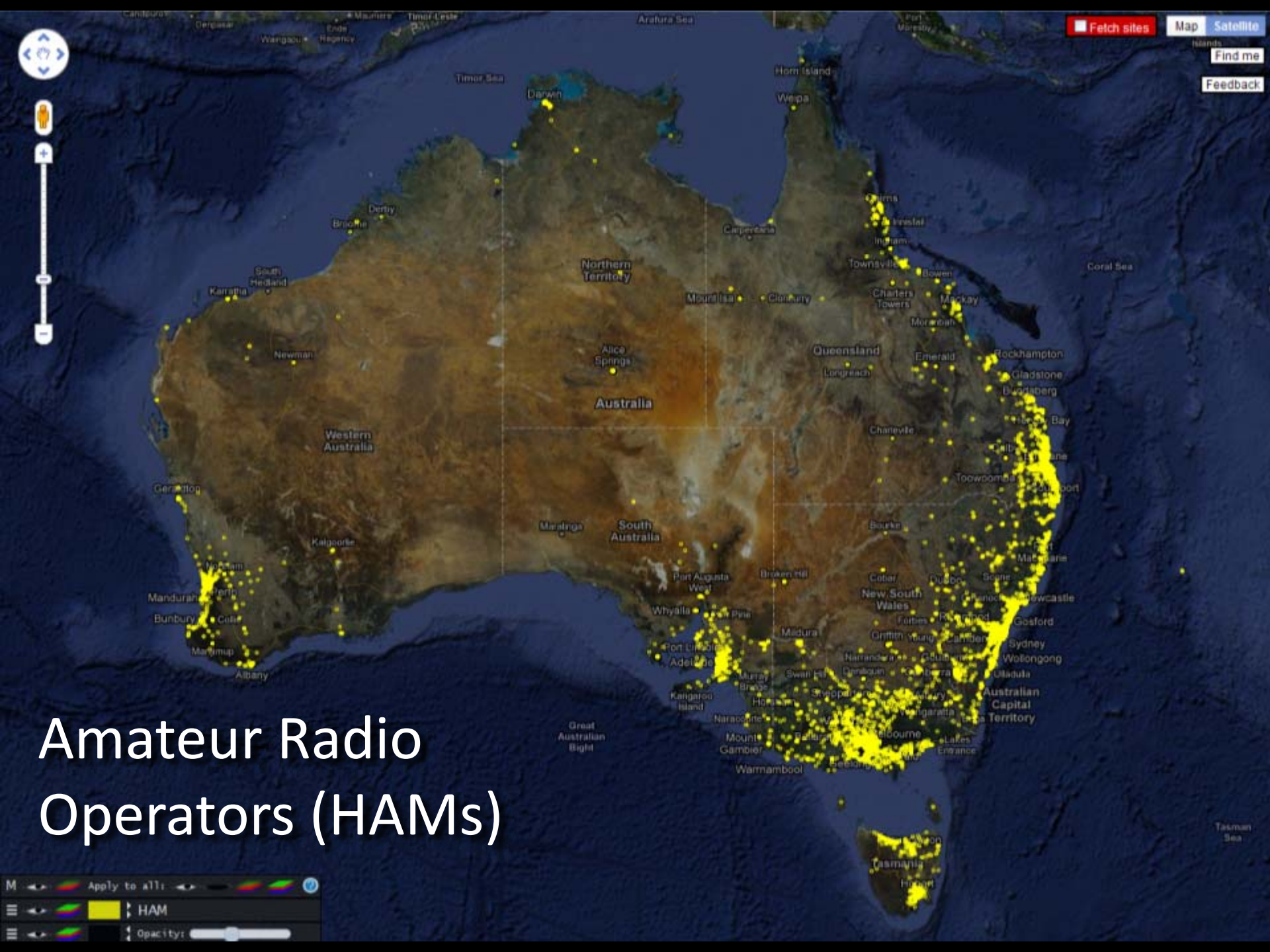

Fetch sites
Map
Satellite
Find me
Feedback
Arafura Sea
Timor Sea
Darwin
Horn Island
Weipa
Cairns
Townsville
Coral Sea
Broome
Derby
Carpentaria
Northern Territory
Mount Isa
Charters Towers
Mackay
Queensland
Rockhampton
Gladstone
Bundaberg
Hervey Bay
Emerald
Longreach
Alice Springs
Australia
Western Australia
Newman
Geraldton
Kalgoorlie
Perth
Mandurah
Bunbury
Albany
Meekatharra
South Australia
Port Augusta
Whyalla
Port Pirie
Broken Hill
Bourke
Dubbo
New South Wales
Newcastle
Gosford
Sydney
Wollongong
Canberra
Australian Capital Territory
Albury
Shepparton
Horsham
Victoria
Melbourne
Ballarat
Mount Gambier
Warrnambool
Geelong
Great Australian Bight
Kangaroo Island
Port Lincoln
Adelaide
Mildura
Griffith
Narrandera
Tasmania
Launceston
Hobart
Tasman Sea
M
Apply to all:
Vodafone
Optus
Telstra
Opacity:


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.

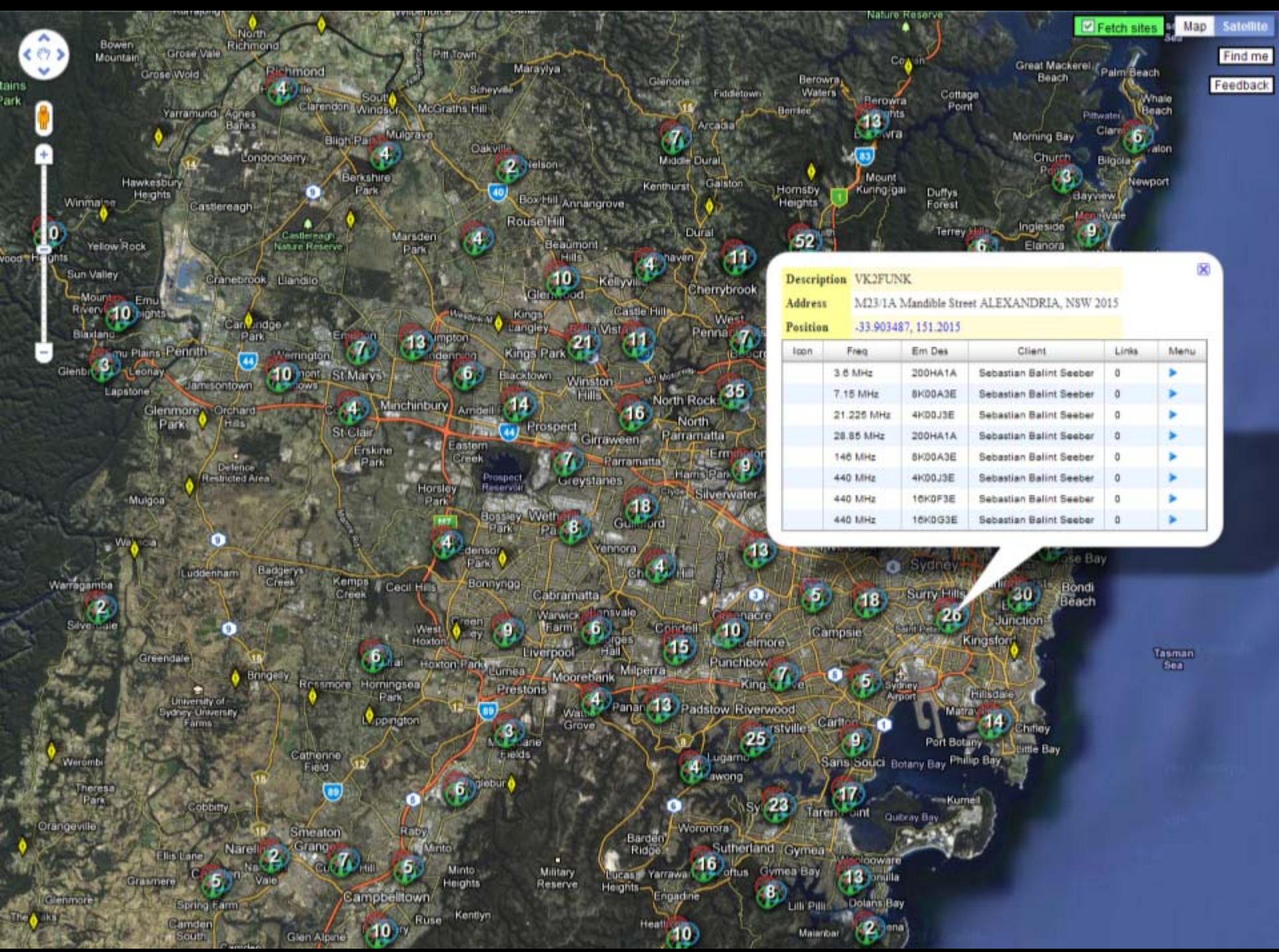


Antenna
Radiation
Envelope

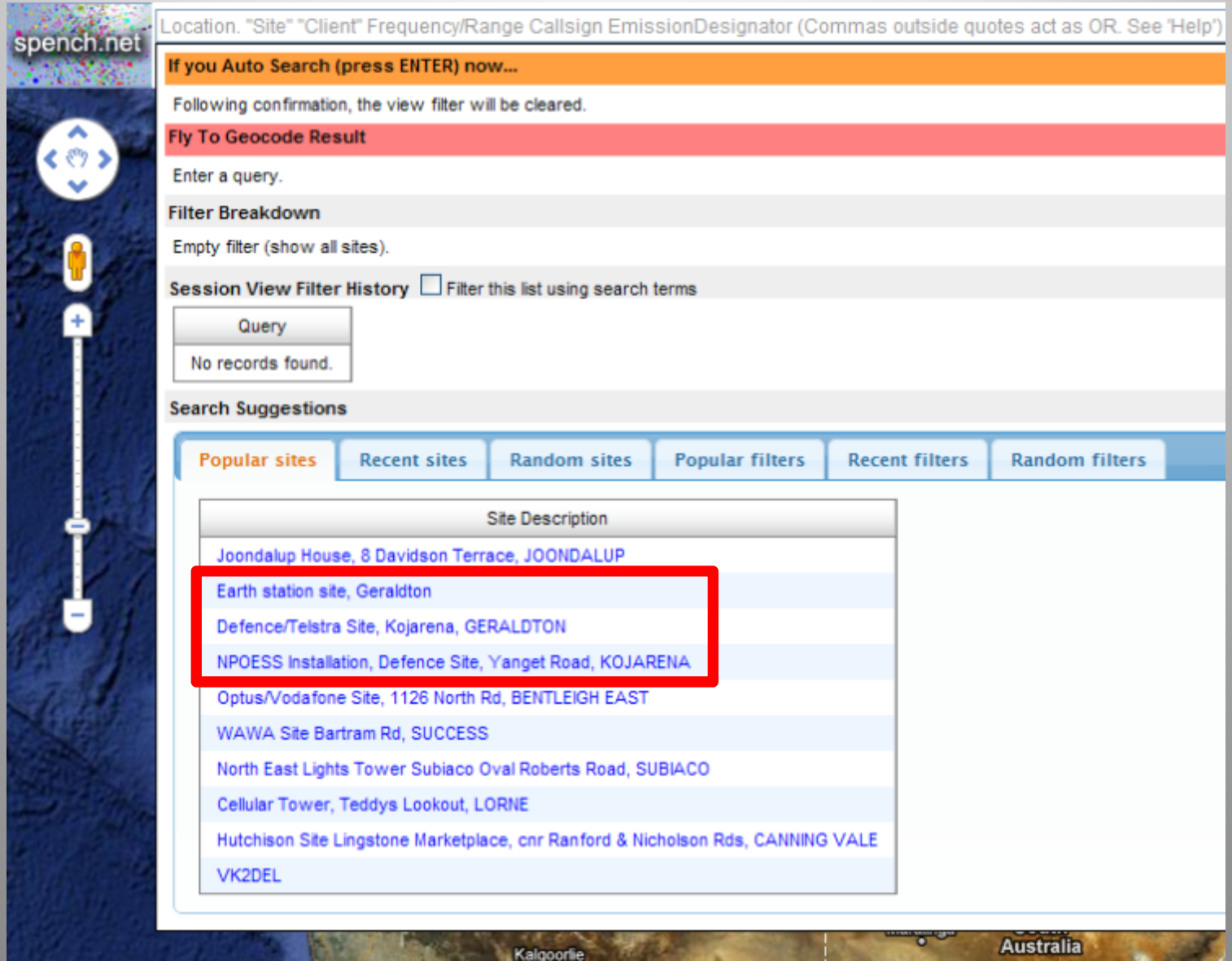
Radiation Heatmap



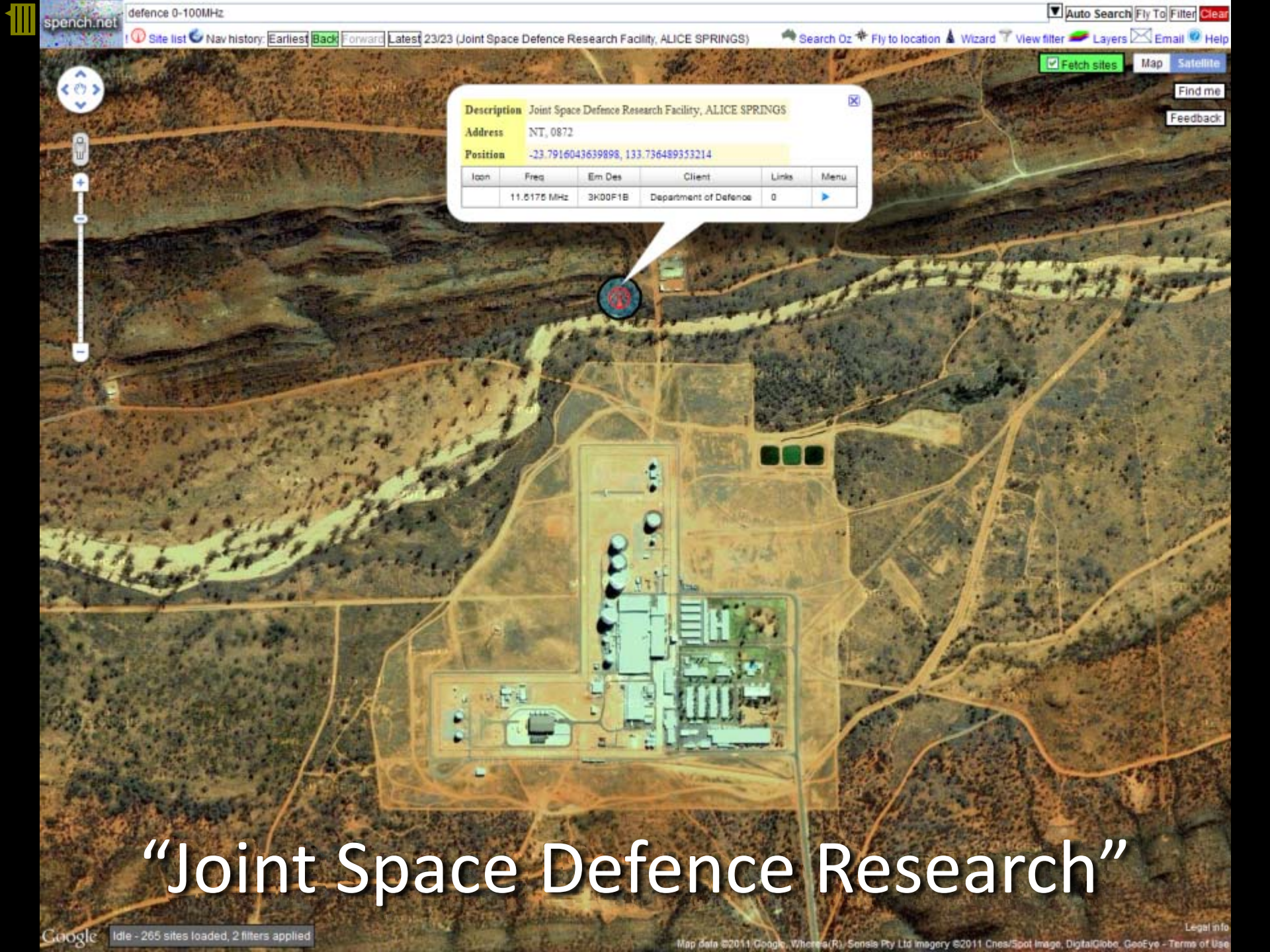
Amateur Radio Operators (HAMs)


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

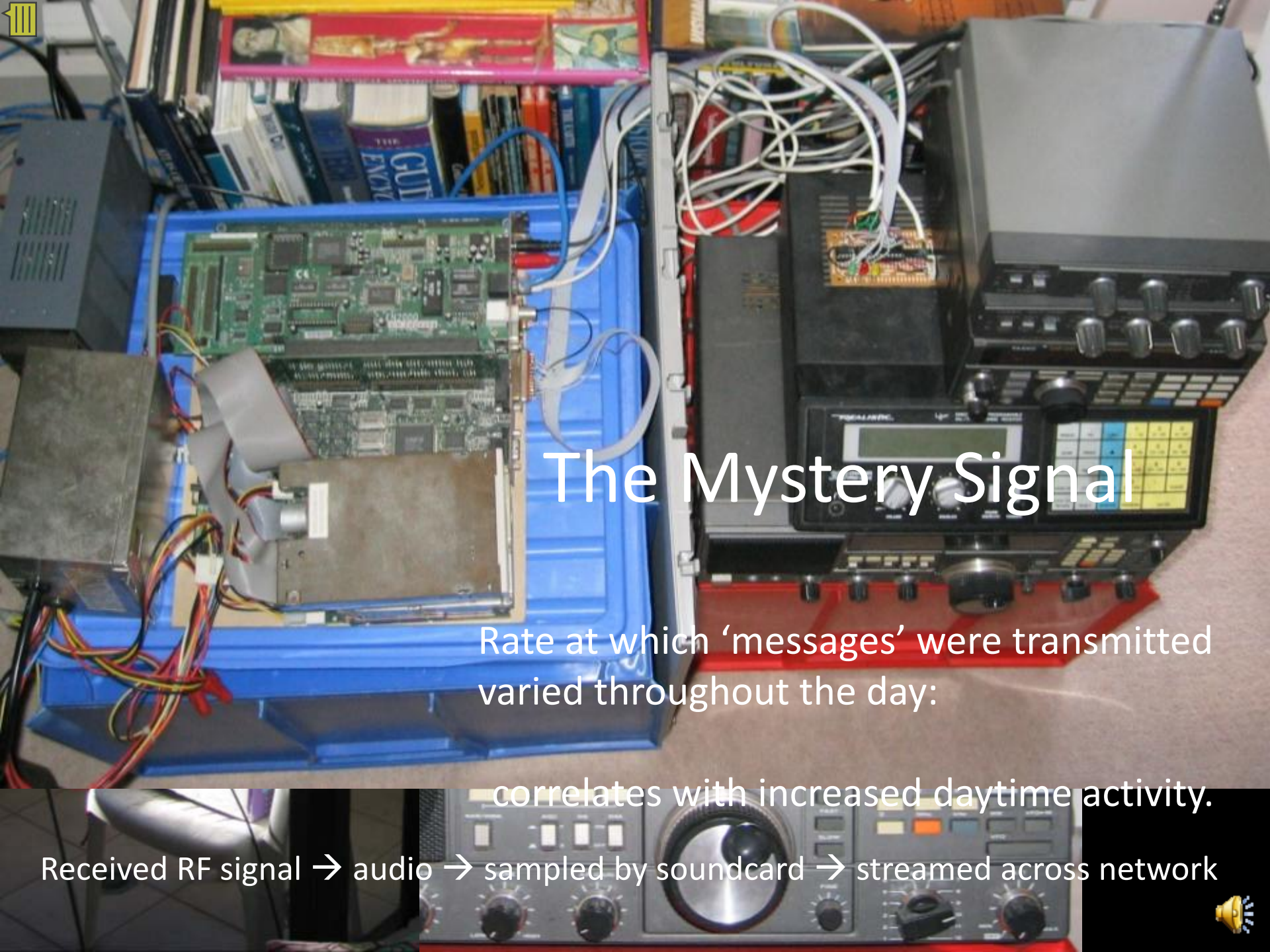



spench.net
Location, "Site" "Client" Frequency/Range Callsign EmissionDesignator (Commas outside quotes act as OR. See 'Help')
Auto Search
Fly To
Filter
Clear
Site list
Nav history:
Earliest
Back
Forward
Latest
8/8 (Earth station site, Geraldton)
Search Oz
Fly to location
Wizard
View filter
Layers
Email
Help
Fetch sites
Map
Satellite
Find me
Feedback
Defence & ECHELON
Google
Idle - 6 sites loaded
Legal info
Imagery ©2011 DigitalGlobe, GeoEye - Terms of Use


spench.net
defence 0-100MHz
Auto Search
Fly To
Filter
Clear
Site list
Nav history:
Earliest
Back
Forward
Latest
23/23 (Joint Space Defence Research Facility, ALICE SPRINGS)
Search Oz
Fly to location
Wizard
View filter
Layers
Email
Help
Fetch sites
Map
Satellite
Find me
Feedback
Description
Joint Space Defence Research Facility, ALICE SPRINGS
Address
NT, 0872
Position
-23.7916043639898, 133.736489353214
Icon
Freq
Em Des
Client
Links
Menu
11.6175 MHz
3K00F1B
Department of Defence
0
"Joint Space Defence Research"
Google
Idle - 265 sites loaded, 2 filters applied
Legal info
Map data ©2011 Google, Whereis(R), Sensis Pty Ltd Imagery ©2011 Cnes/Spot Image, DigitalGlobe, GeoEye - Terms of Use

Upset ADIRU of QF68/71/72 & JQ7 ?

Side note



The Mystery Signal

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

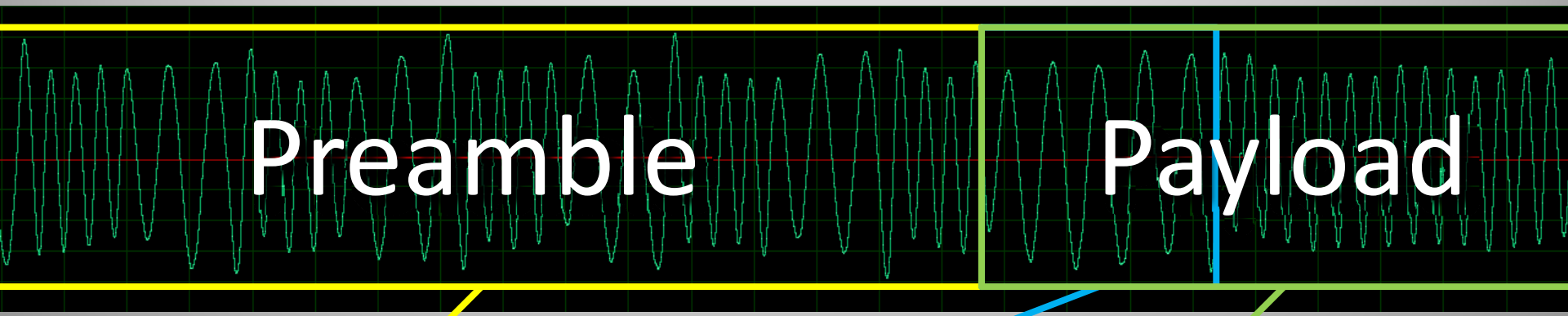
correlates with increased daytime activity.

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

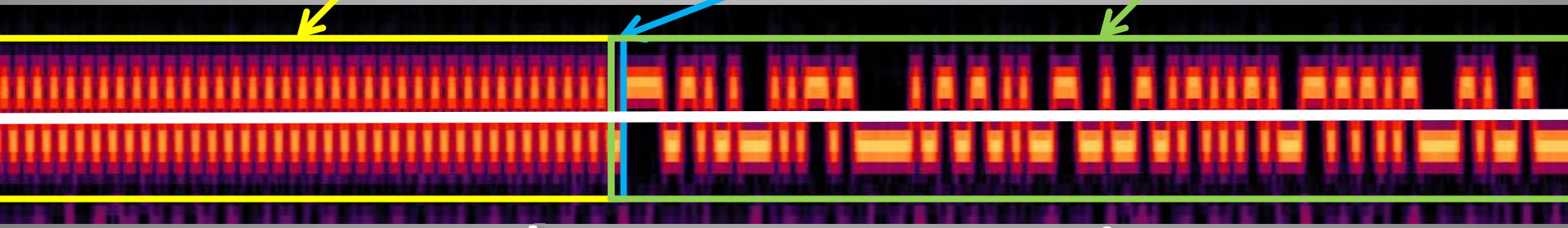
Step One: Look at the signal

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

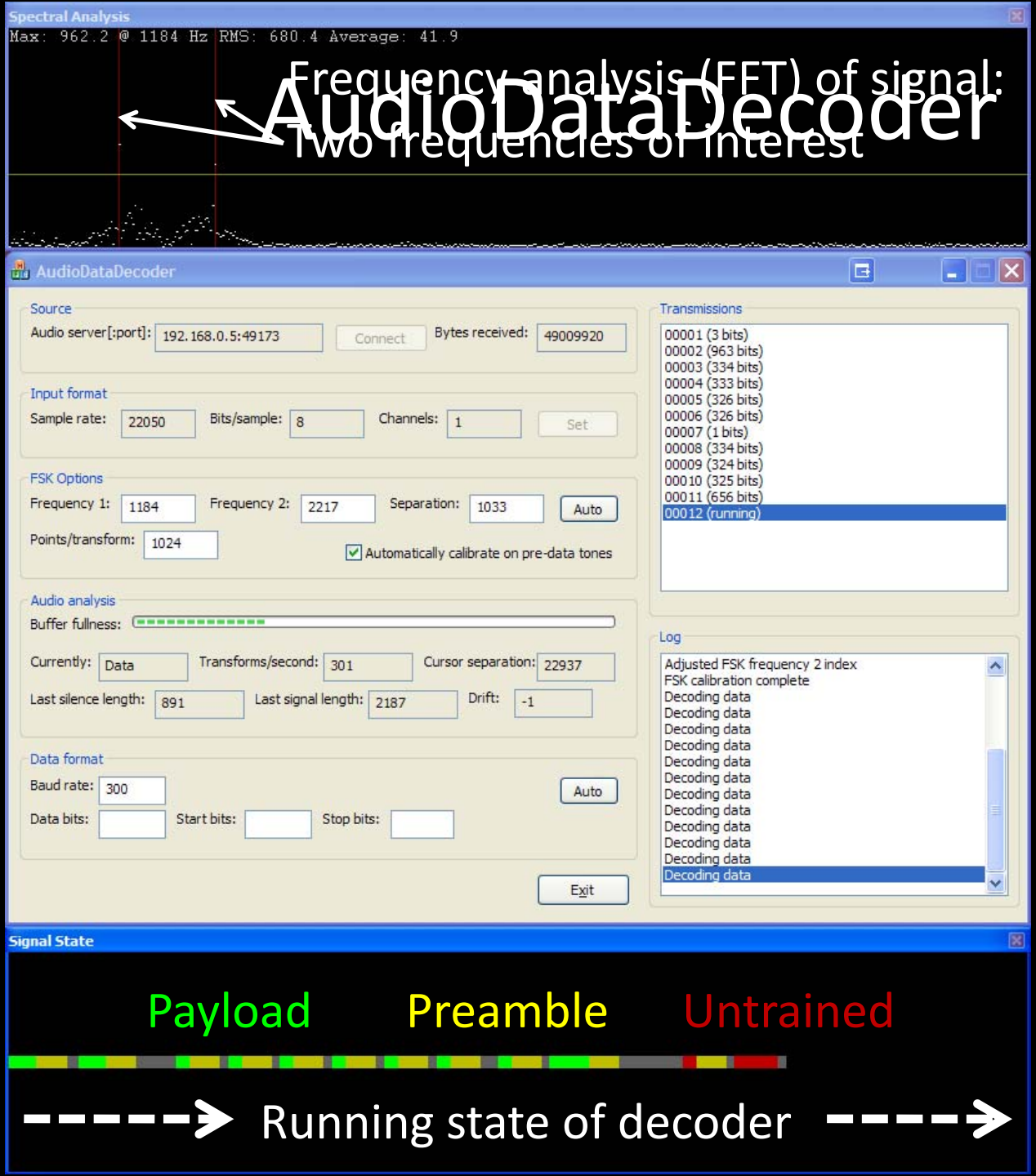
Signal in the time domain (voltage vs. time):



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



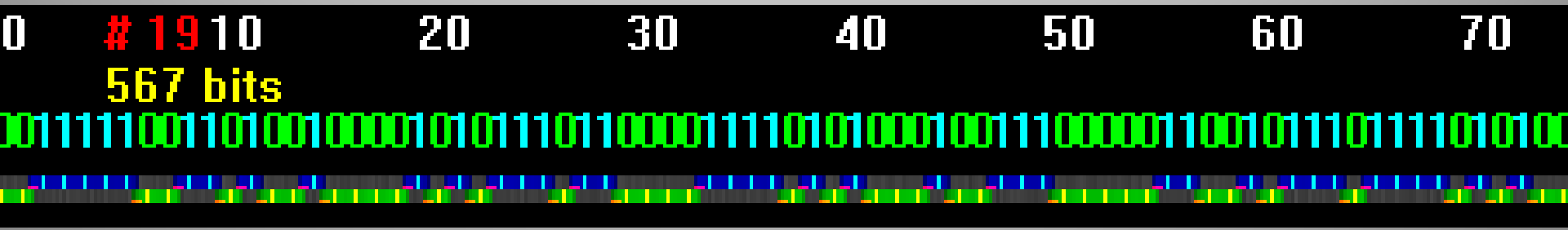
IT’S SLICER TIME!


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
Signal State
Payload
Preamble
Untrained
Running state of decoder

Step Two: FFT of 2FSK → Bitstream

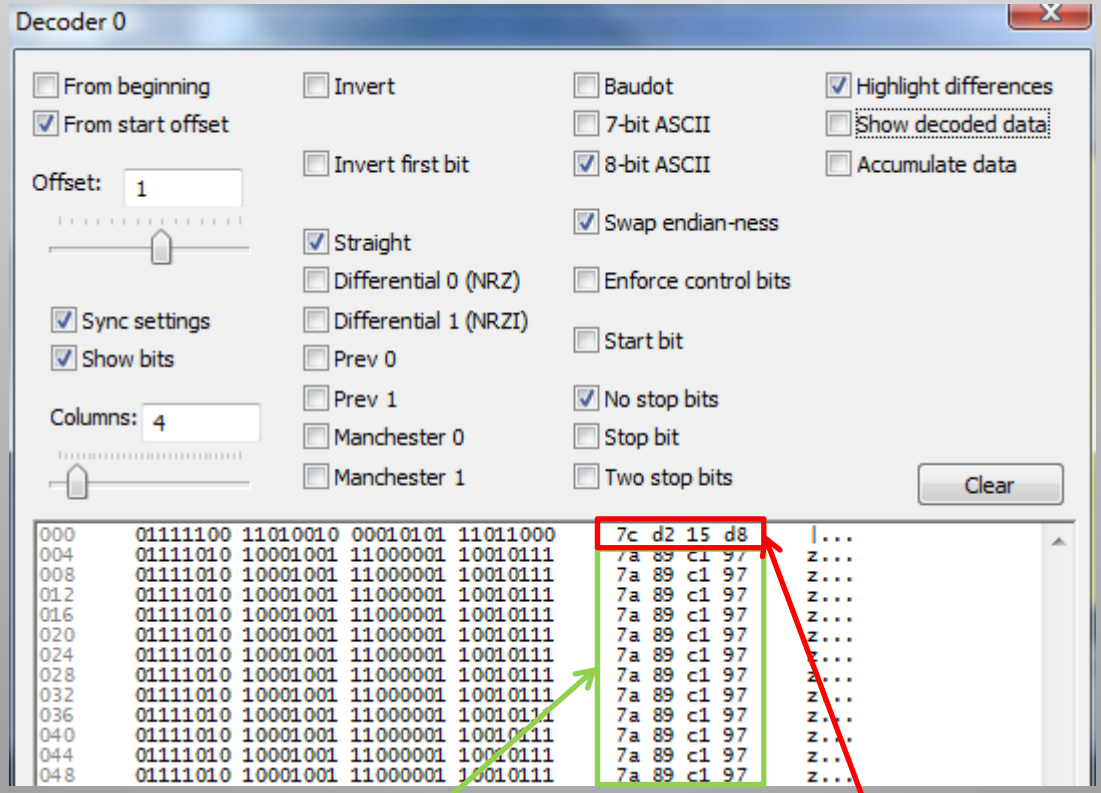
- Lock on two frequencies (**F**requency **S**hift **K**eying)
- Sample intensity of each at regular interval (baud rate)
- Pick which is the strongest:

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:

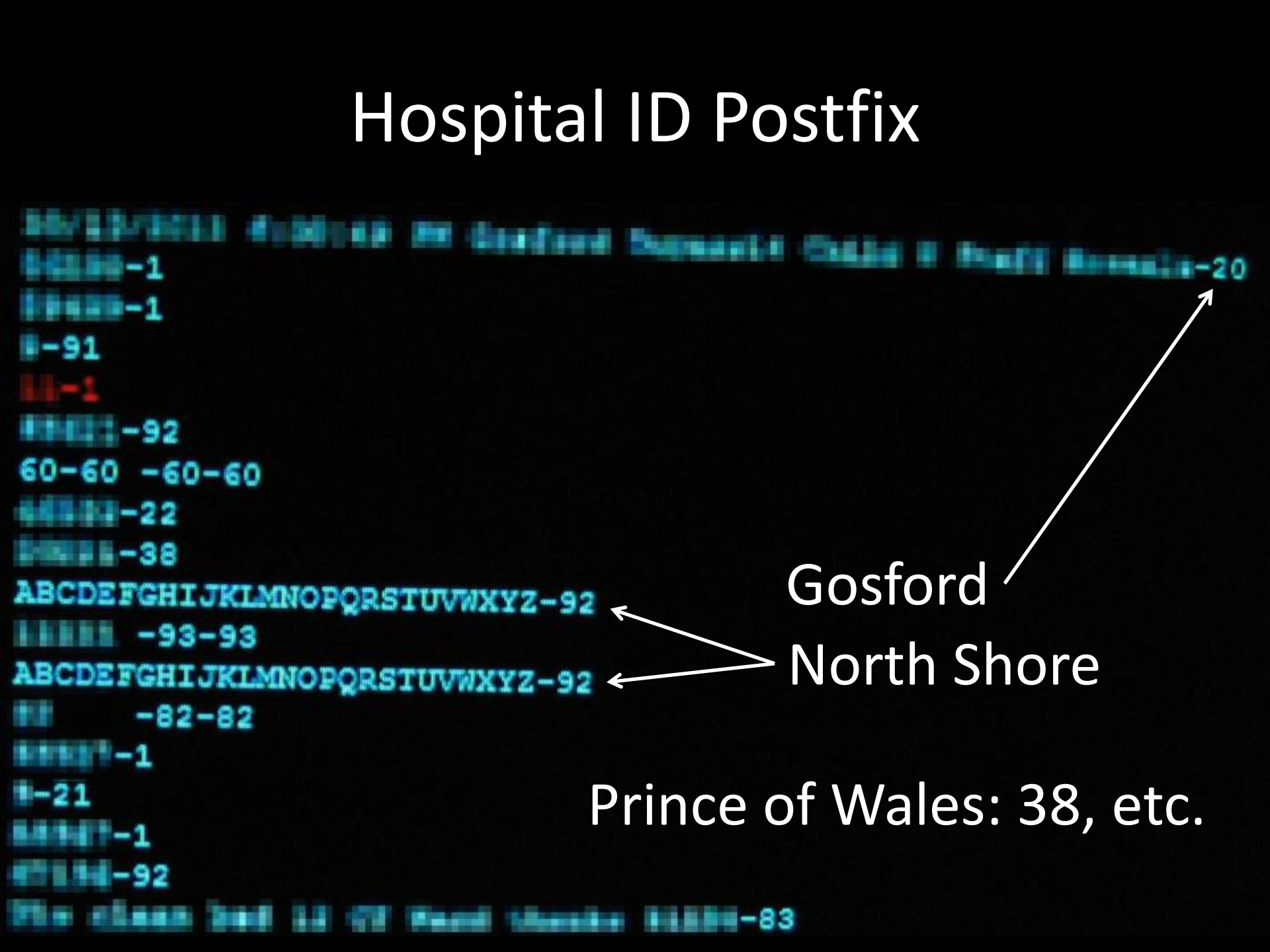
  Non-standard FSK ignored by decoders


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 >>
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


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

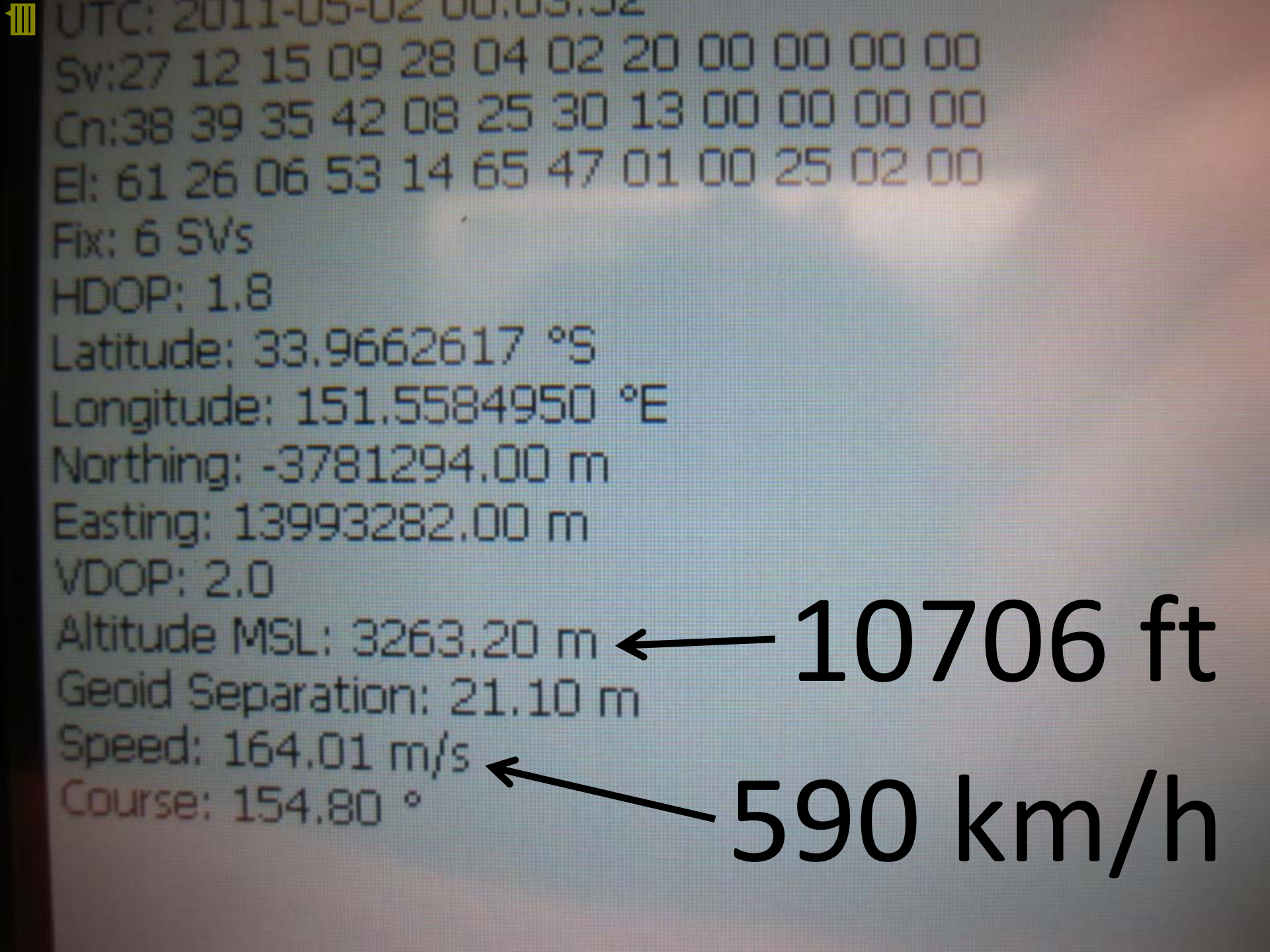
Hospital ID Postfix

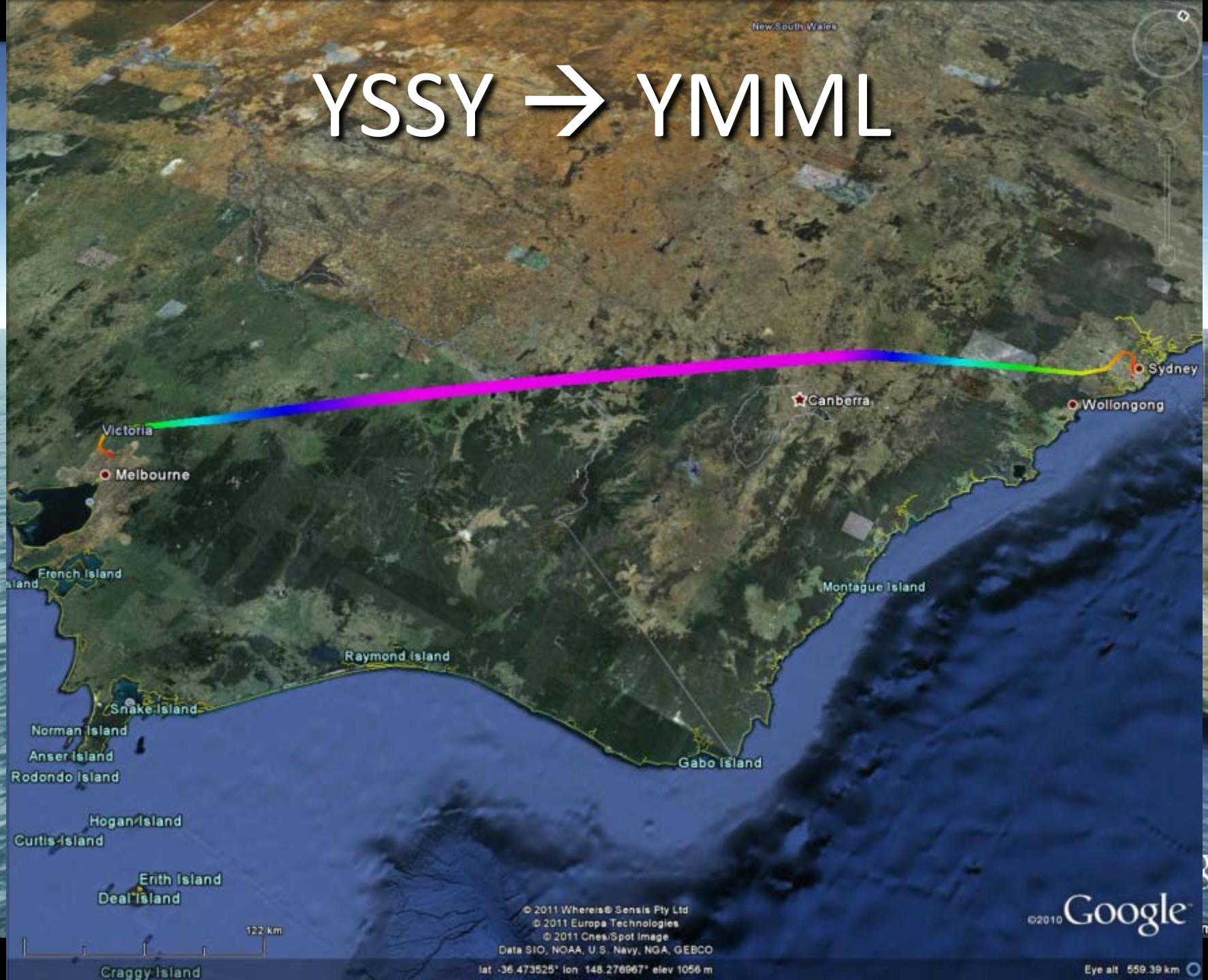


Sensitive Information

Mode S & ACARS

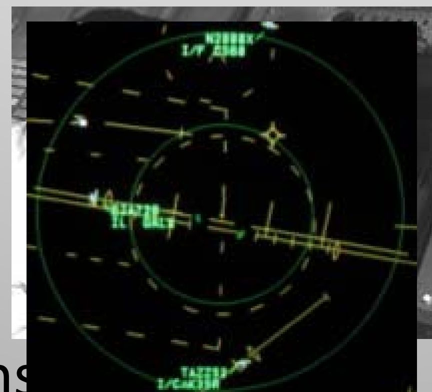
“Modez”

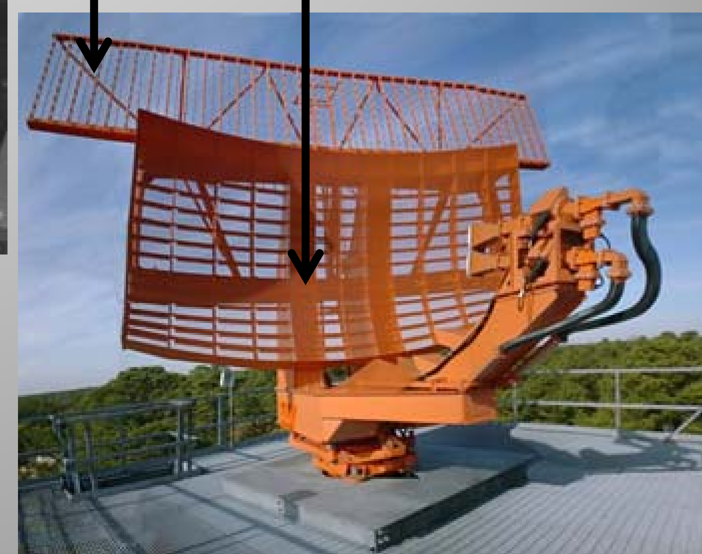

UTC: 2011-05-02 00:03:32
Sv:27 12 15 09 28 04 02 20 00 00 00 00
Cn:38 39 35 42 08 25 30 13 00 00 00 00
El: 61 26 06 53 14 65 47 01 00 25 02 00
Fix: 6 SVs
HDOP: 1.8
Latitude: 33.9662617 °S
Longitude: 151.5584950 °E
Northing: -3781294.00 m
Easting: 13993282.00 m
VDOP: 2.0
Altitude MSL: 3263.20 m
Geoid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

ATCRBS, PSP & SSR

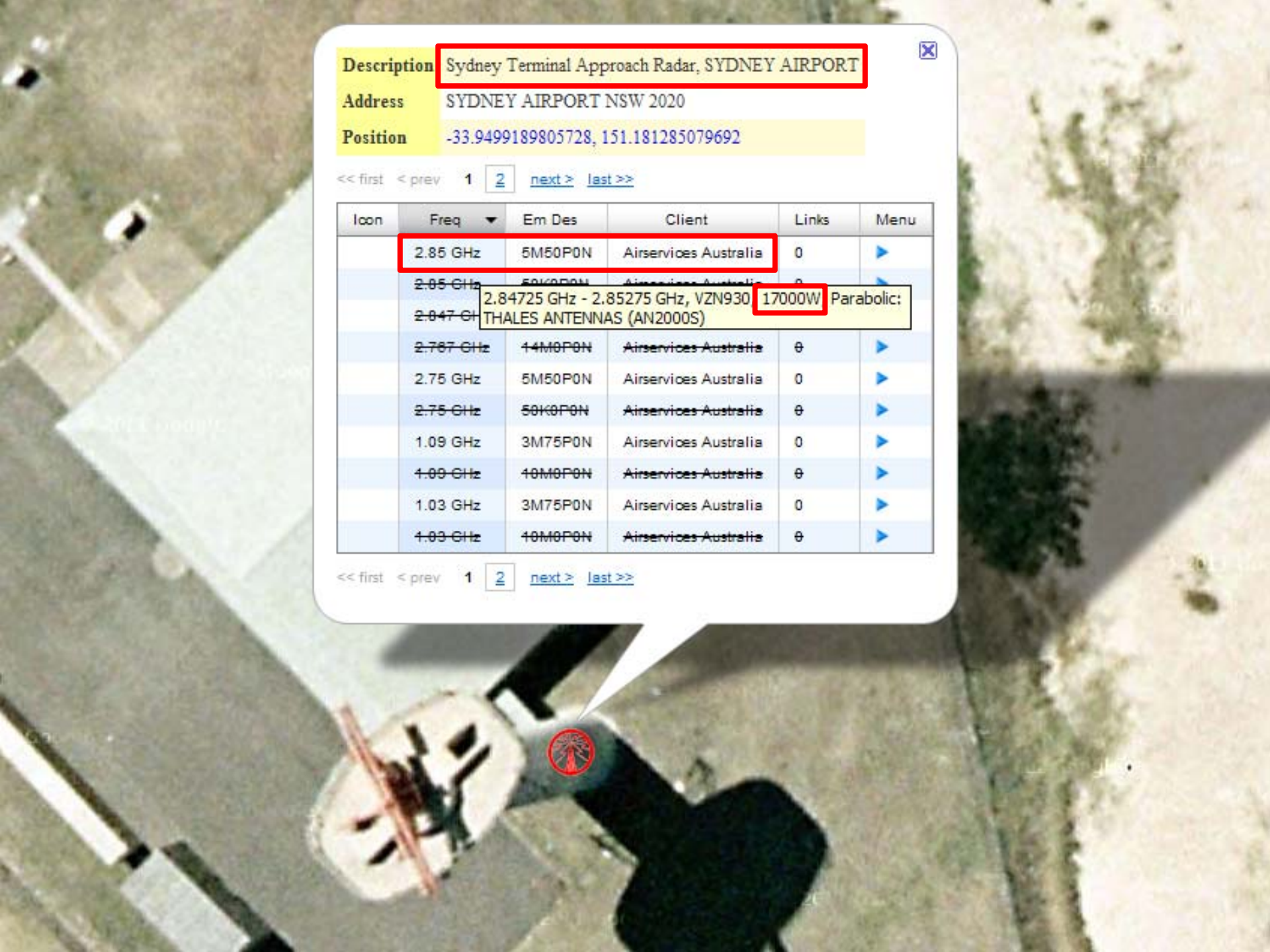
- **A**ir **T**raffic **C**ontrol **R**adar **B**eacon **S**ystem
  - **P**rimary **S**urveillance **R**adar
  - **S**econdary **S**urveillance **R**adar

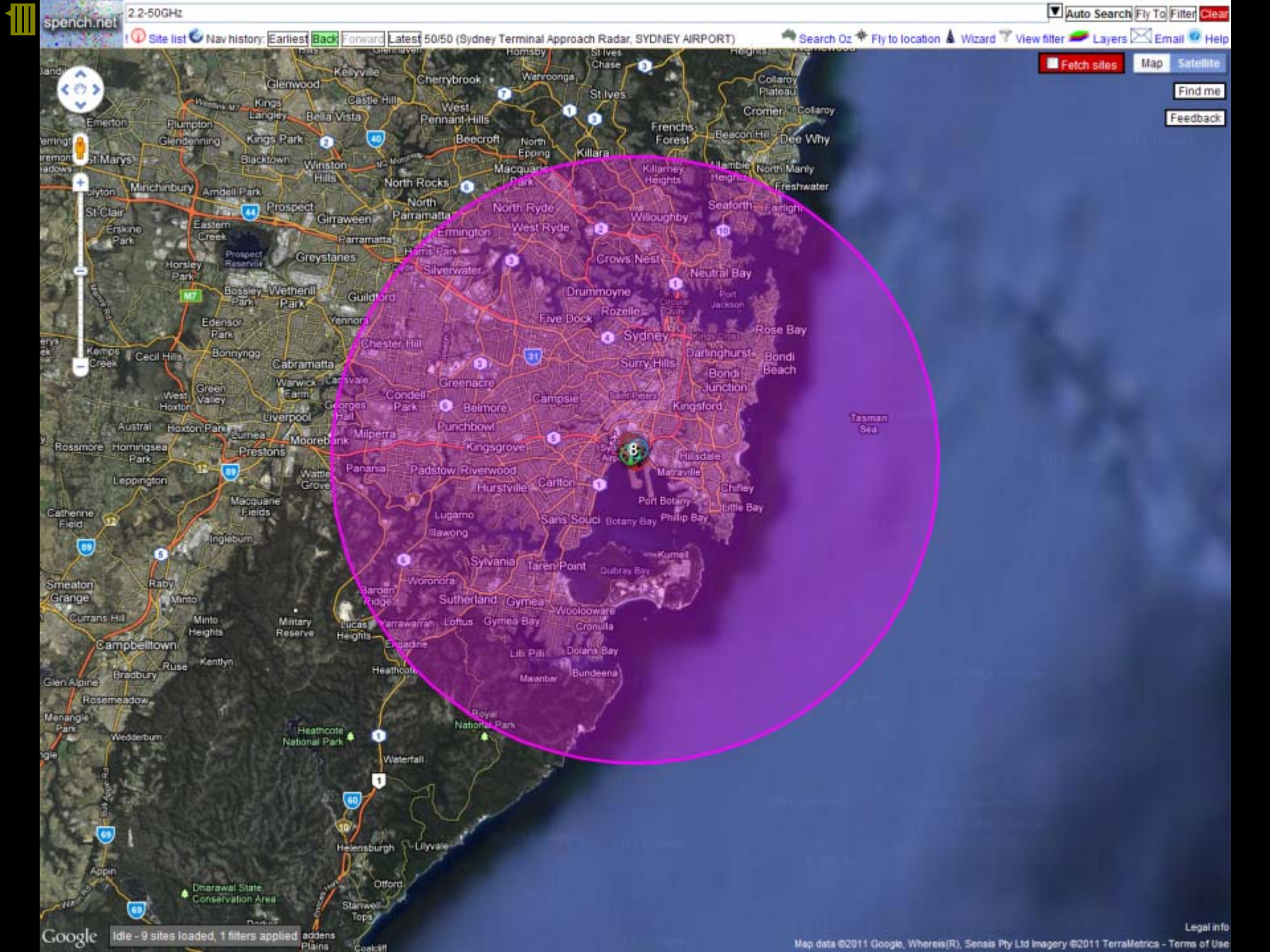




Primary:
- Traditional RADAR
- 'Paints skin' and listens
- Identifies and tracks primary targets, while ignoring 'ground clutter'
- Range limited by RADAR equation ($\frac{1}{d^4}$)

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 >>


spench.net
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
Cronulla
Sutherland
Hurstville
Kogarah
Rockdale
Botany Bay
Port Botany
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, Wheresis(R), Sensis Pty Ltd Imagery ©2011 TerraMetrics - Terms of Use

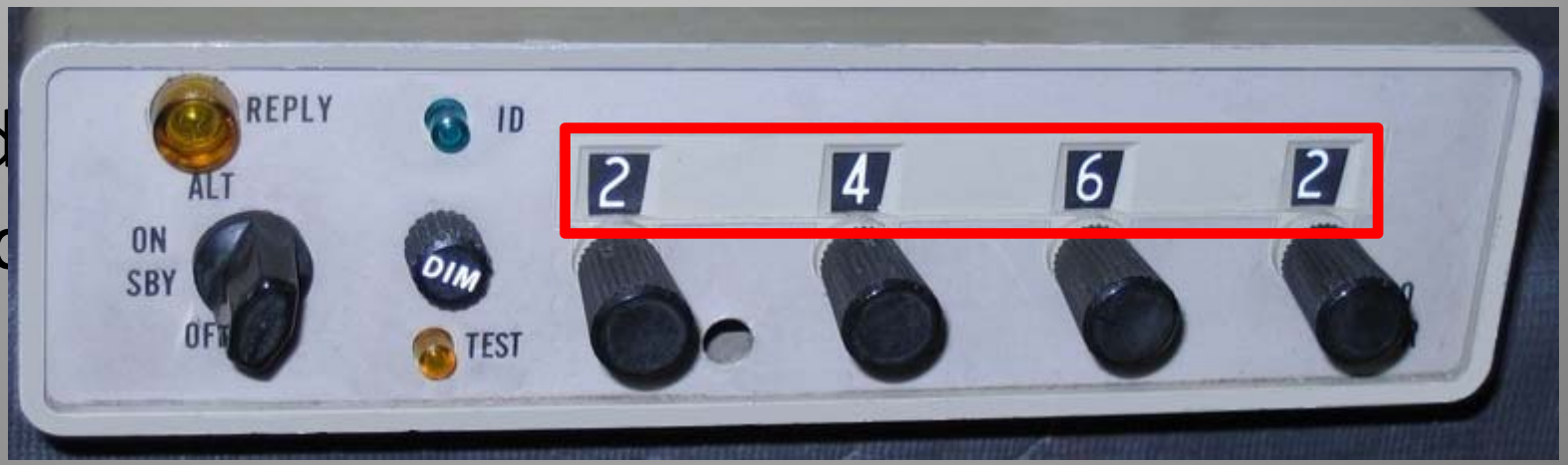
The Modes

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

SSR

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

- Mod
radic



Position

Heading

Altitude

Vertical rate

Flight ID

Squawk code

ATC

Uplink:
“All call” / Altitude request

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

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

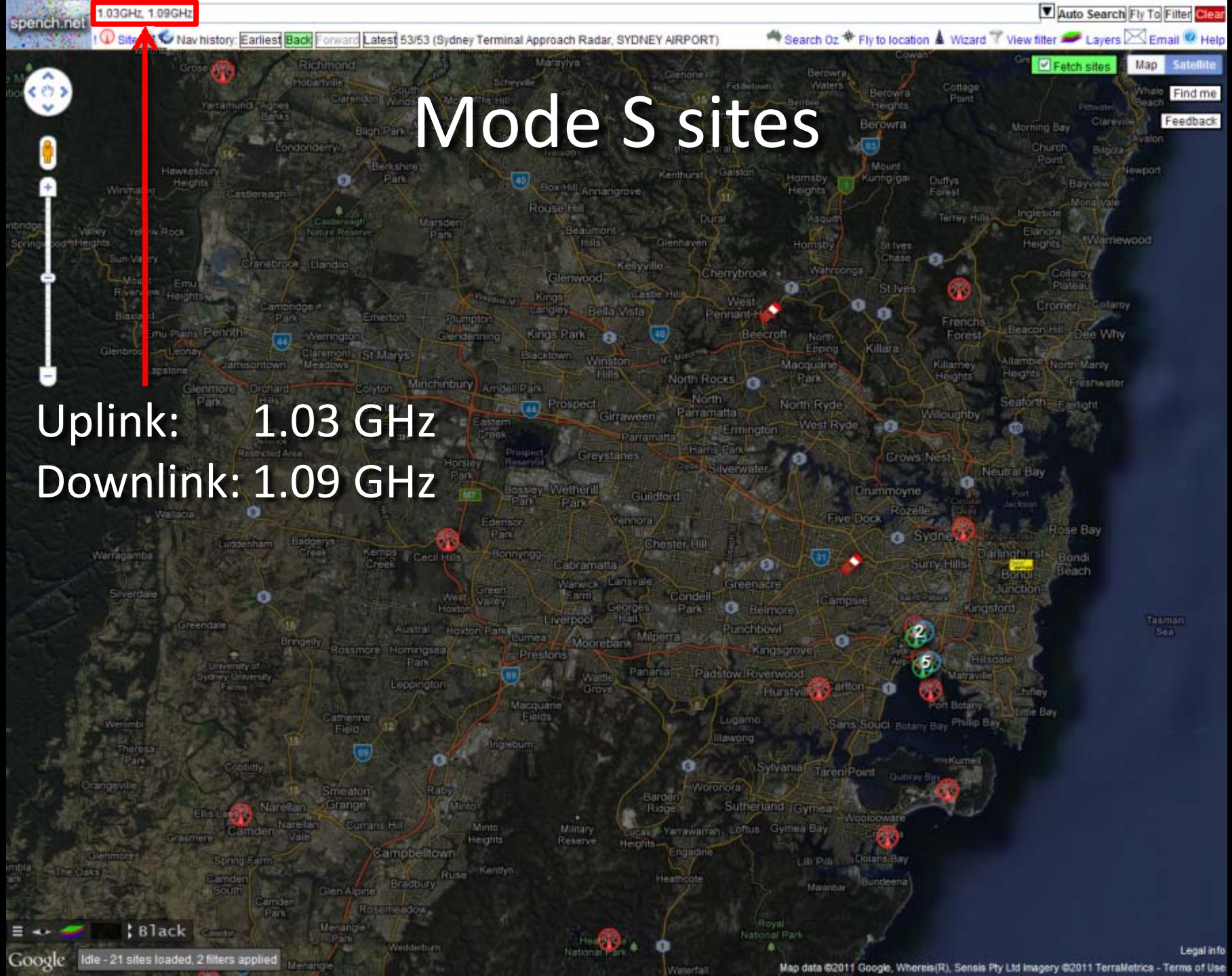
ACAS/TCAS

"PULL UP"

"TRAFFIC"

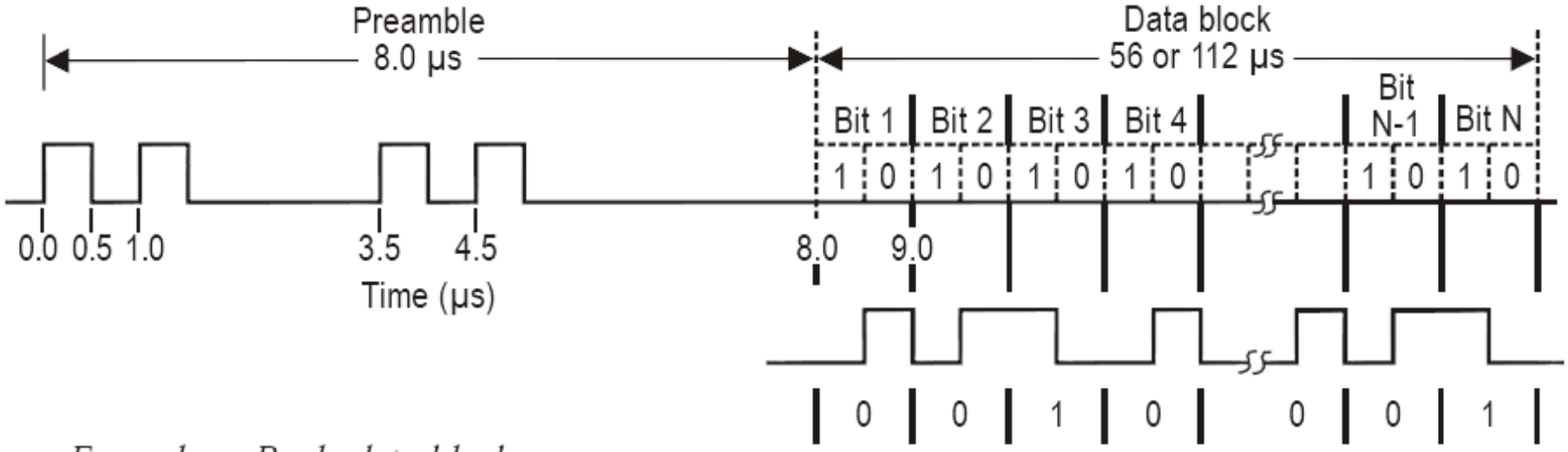
Altitude request

Altitude response (air-to-air)


spench.net
1.03GHz, 1.09GHz
Auto Search
Fly To
Filter
Clear
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

Response Encoding

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



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

Pulse Position Modulation

- 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…

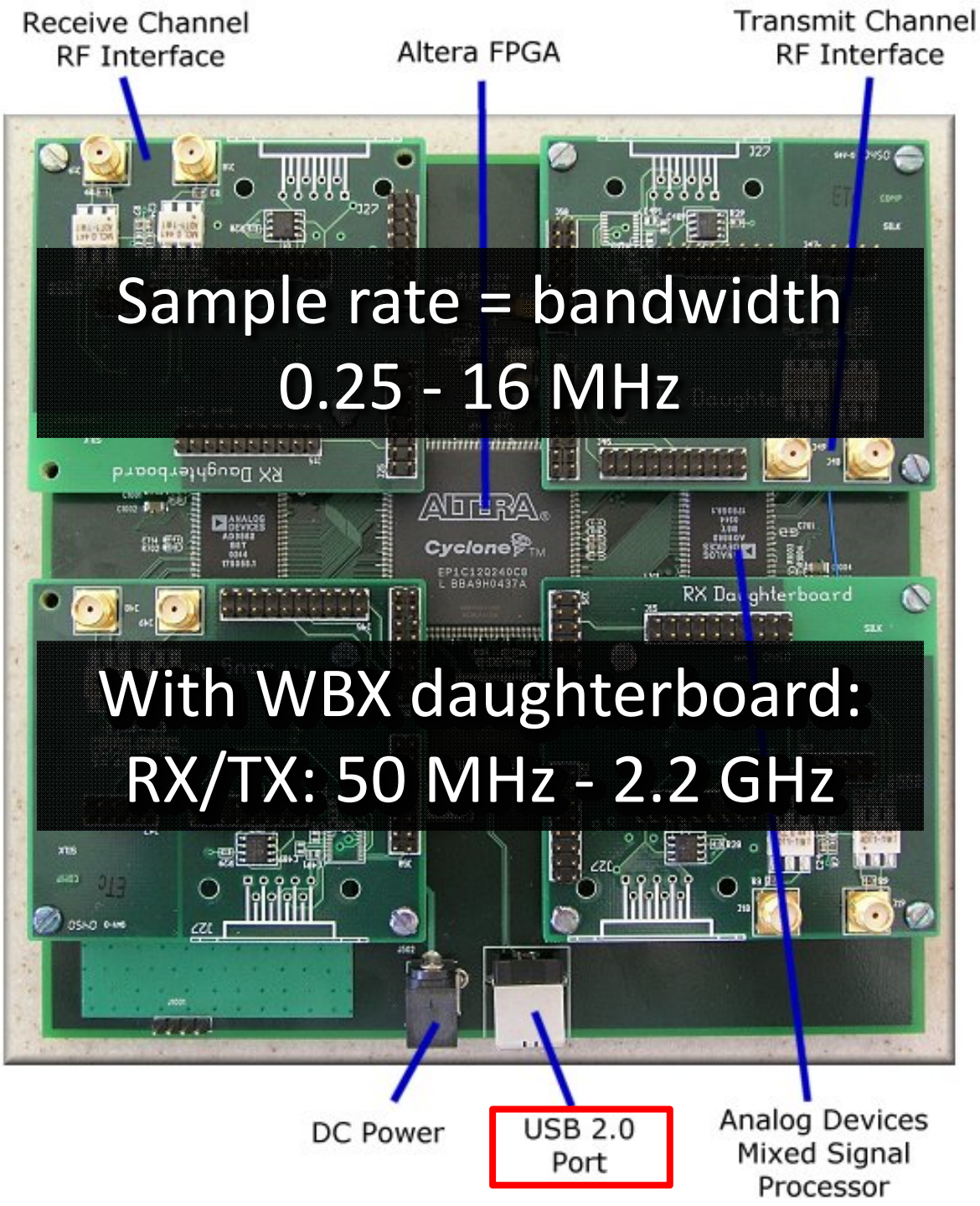
SDR: Digitise the baseband

- 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)

The

Universal
Software
Radio
Peripheral

(USRP 1)

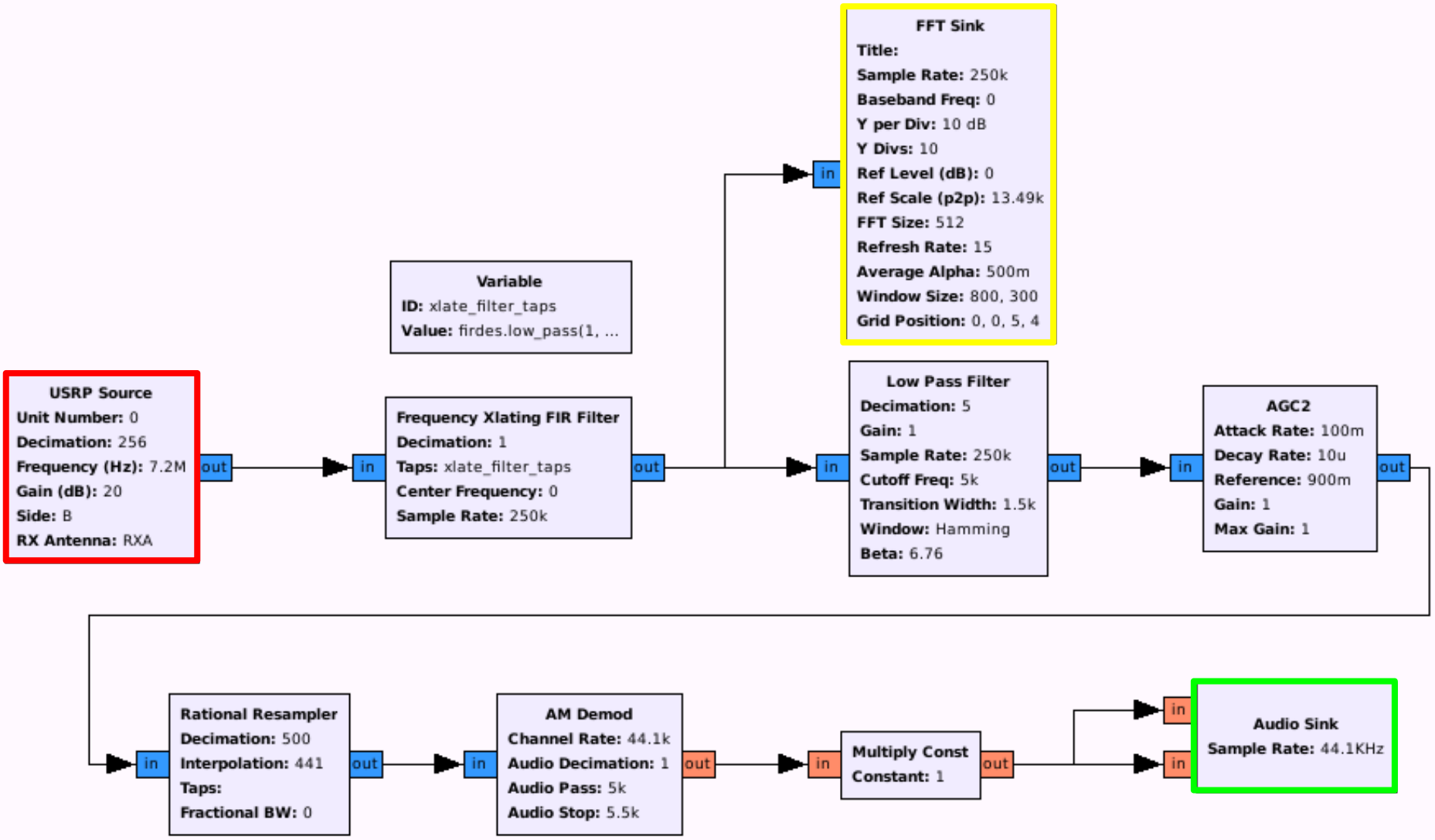


The FUNcube Dongle

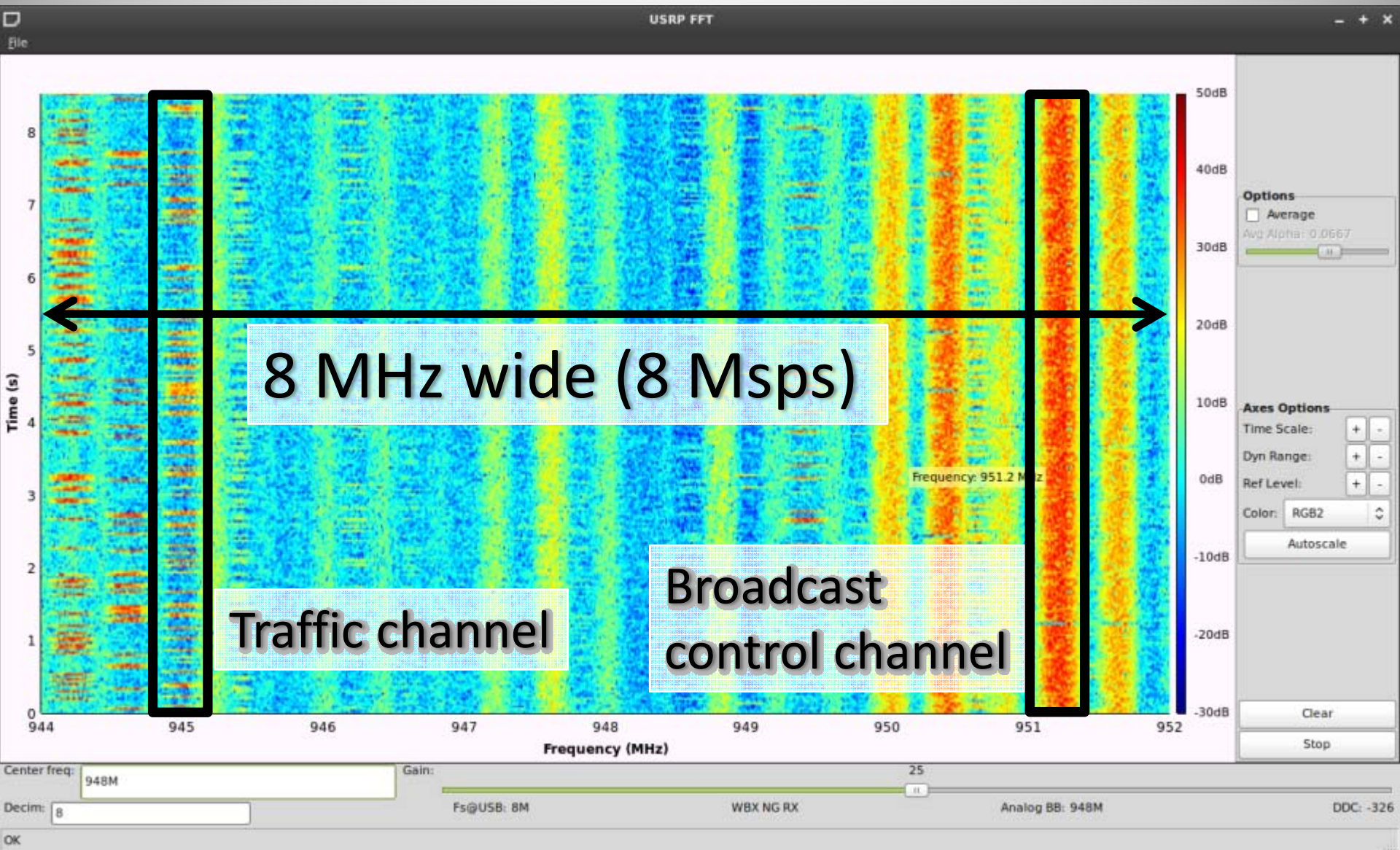
GNU **R**adio

- 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)

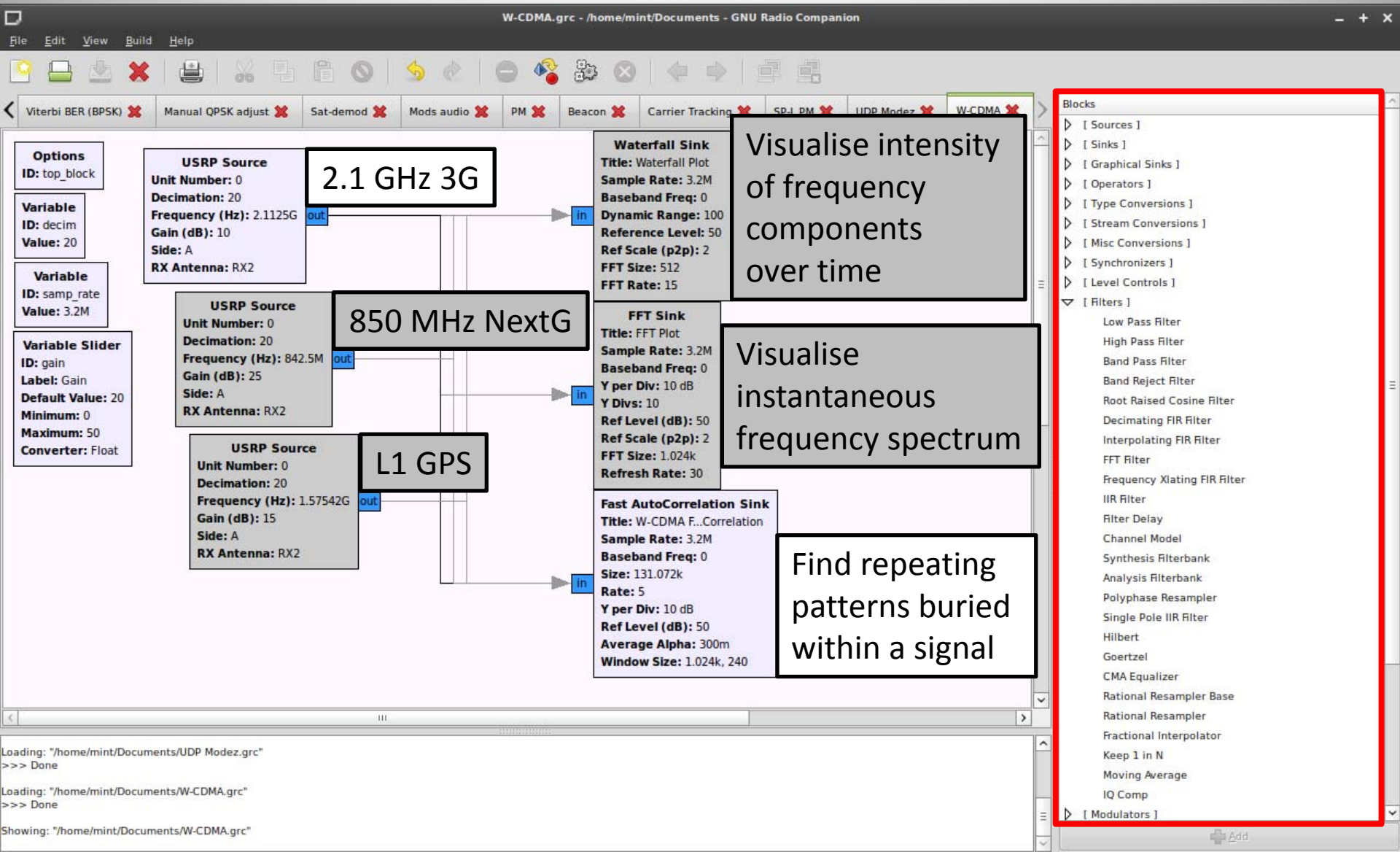
GNU Radio Companion



2G GSM Waterfall

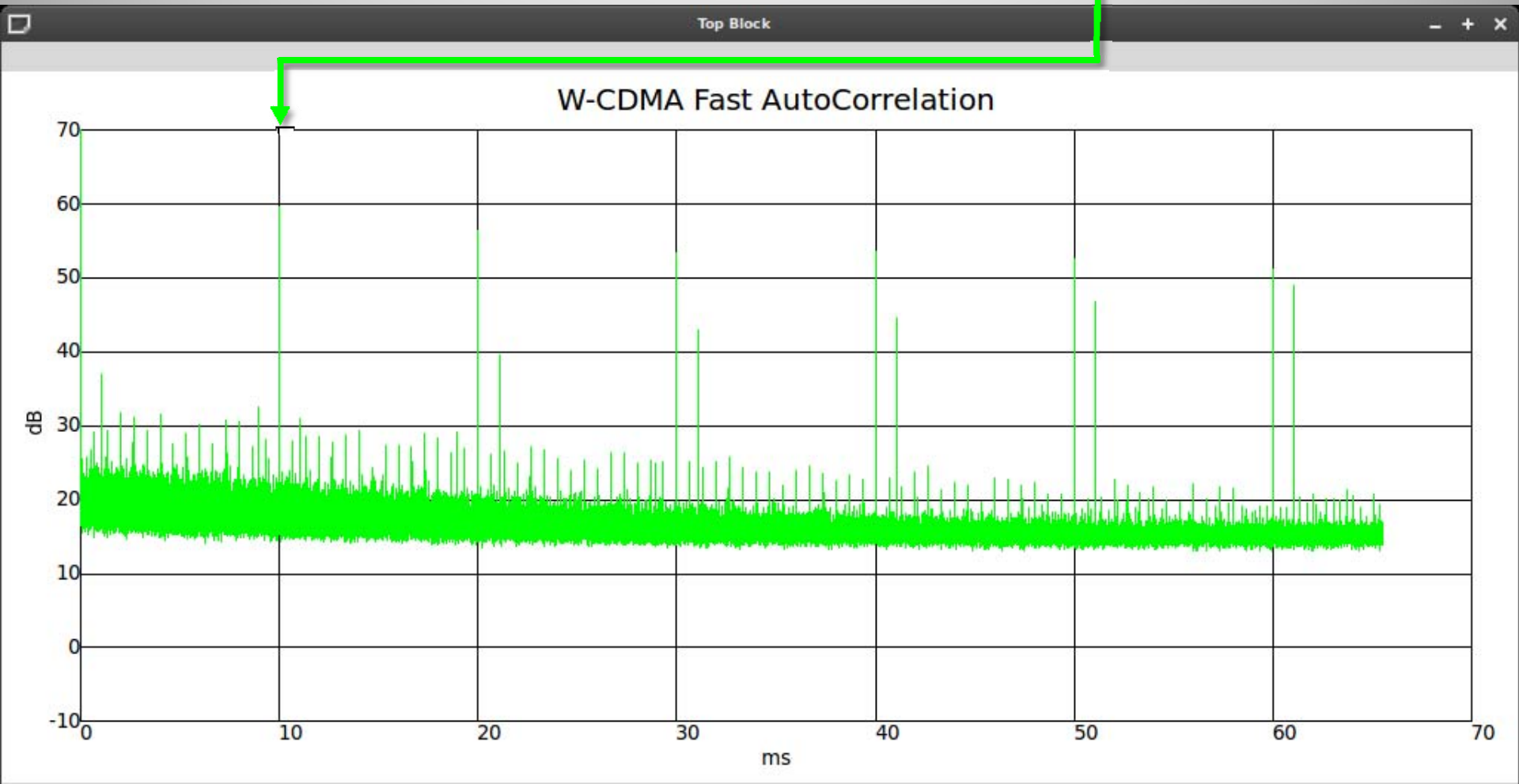


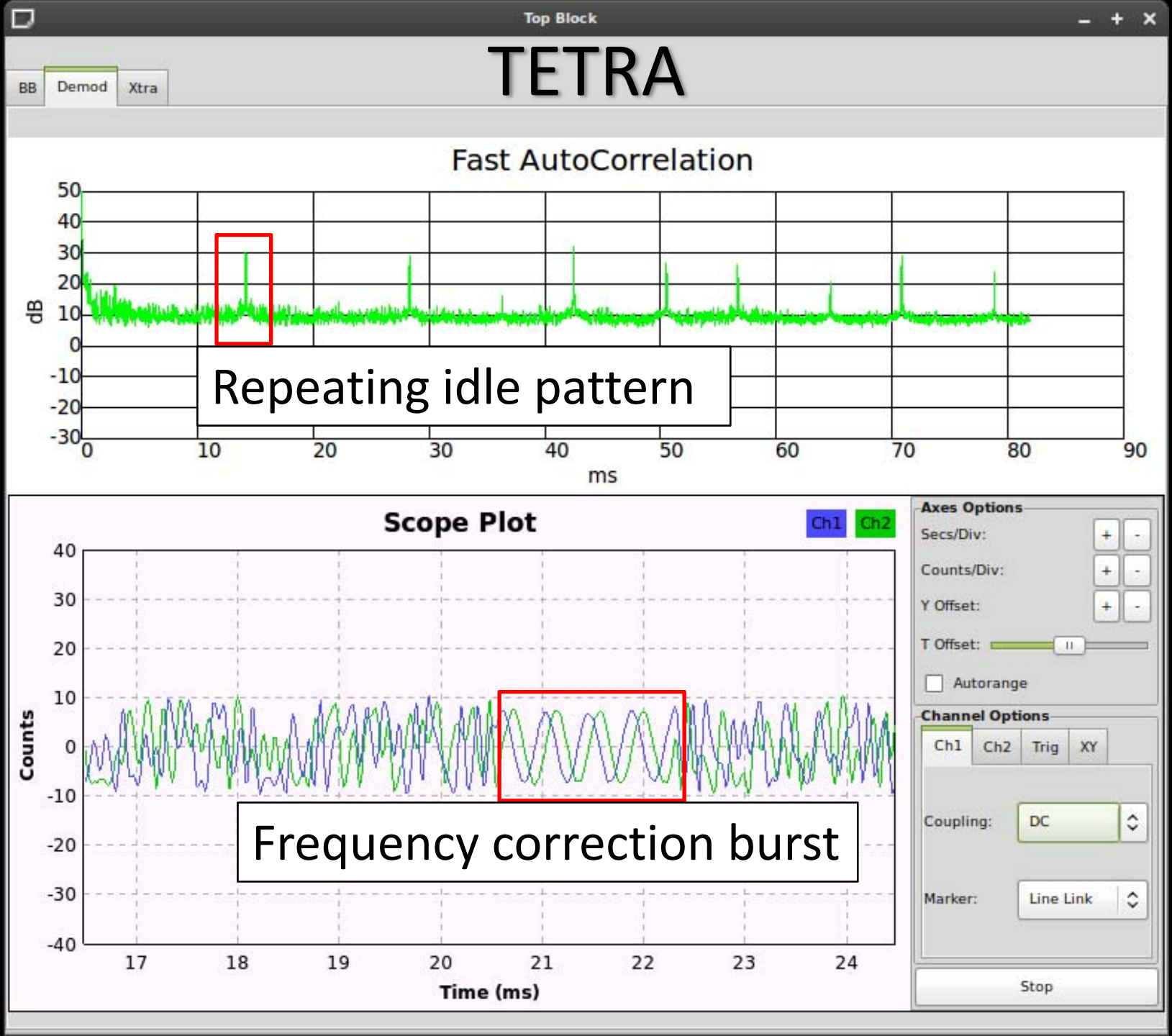
CDMA Detection with GRC



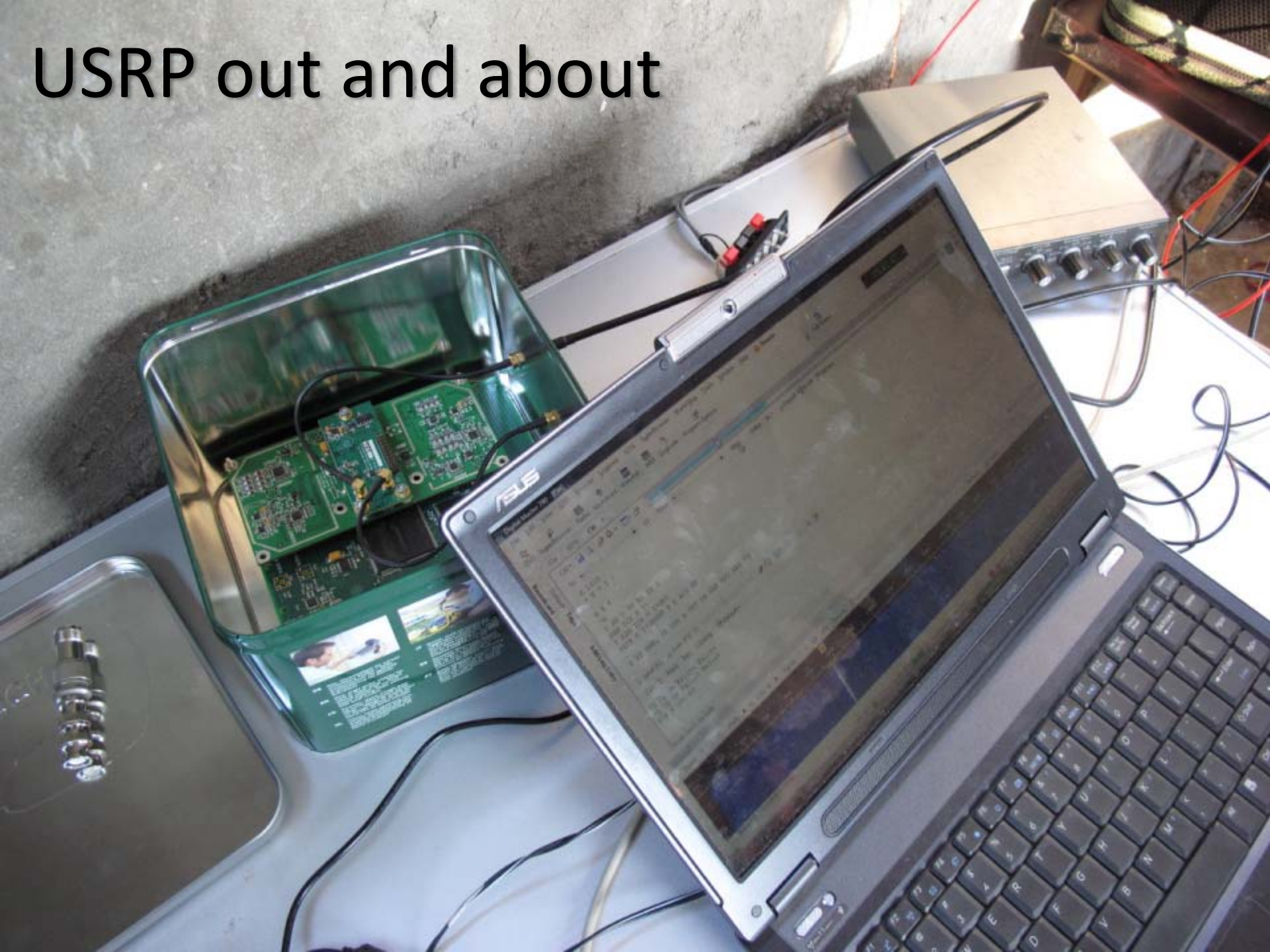
3G W-CDMA

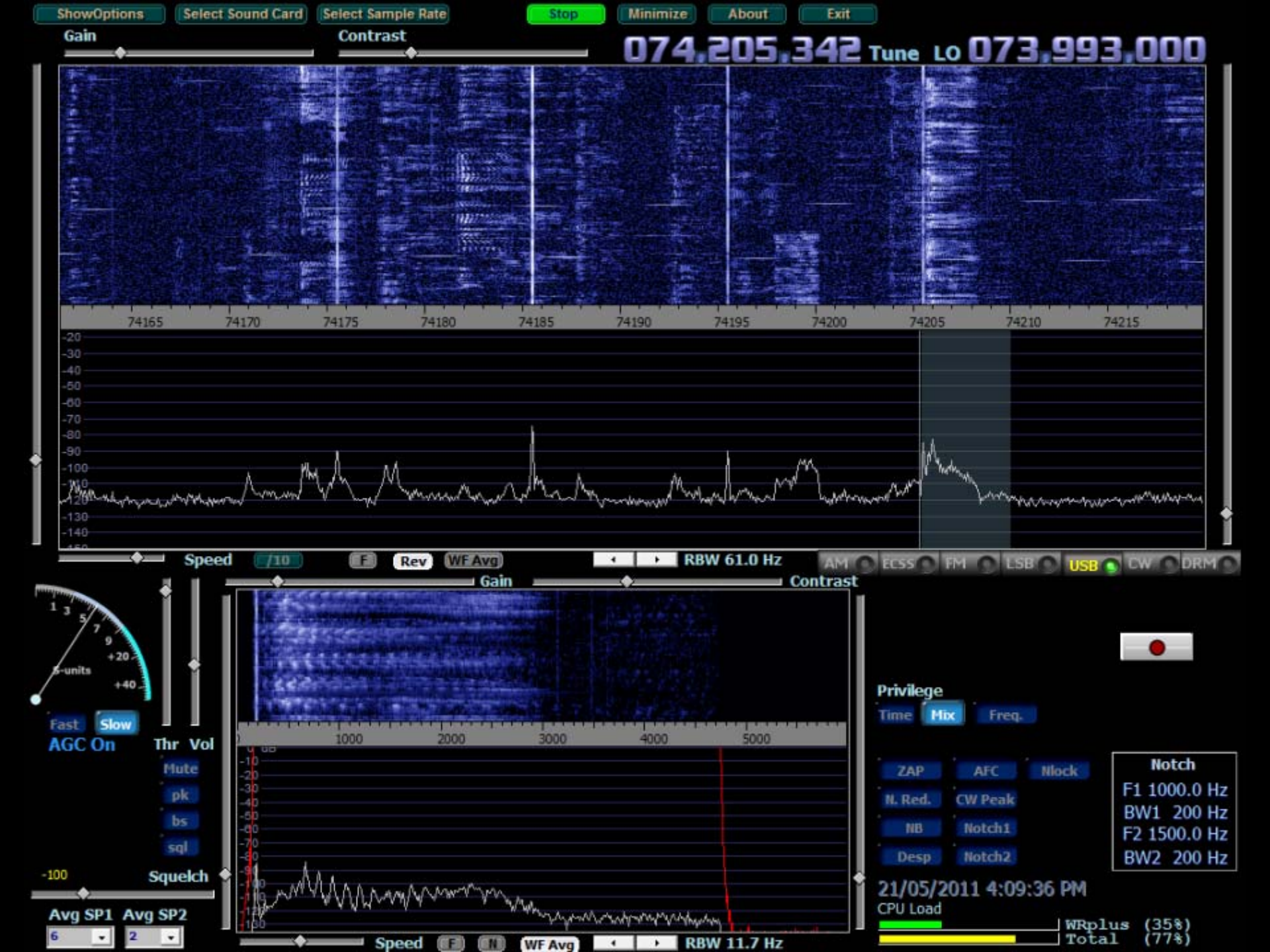
Signature of UMTS: repeating data in CPICH at 10 ms intervals

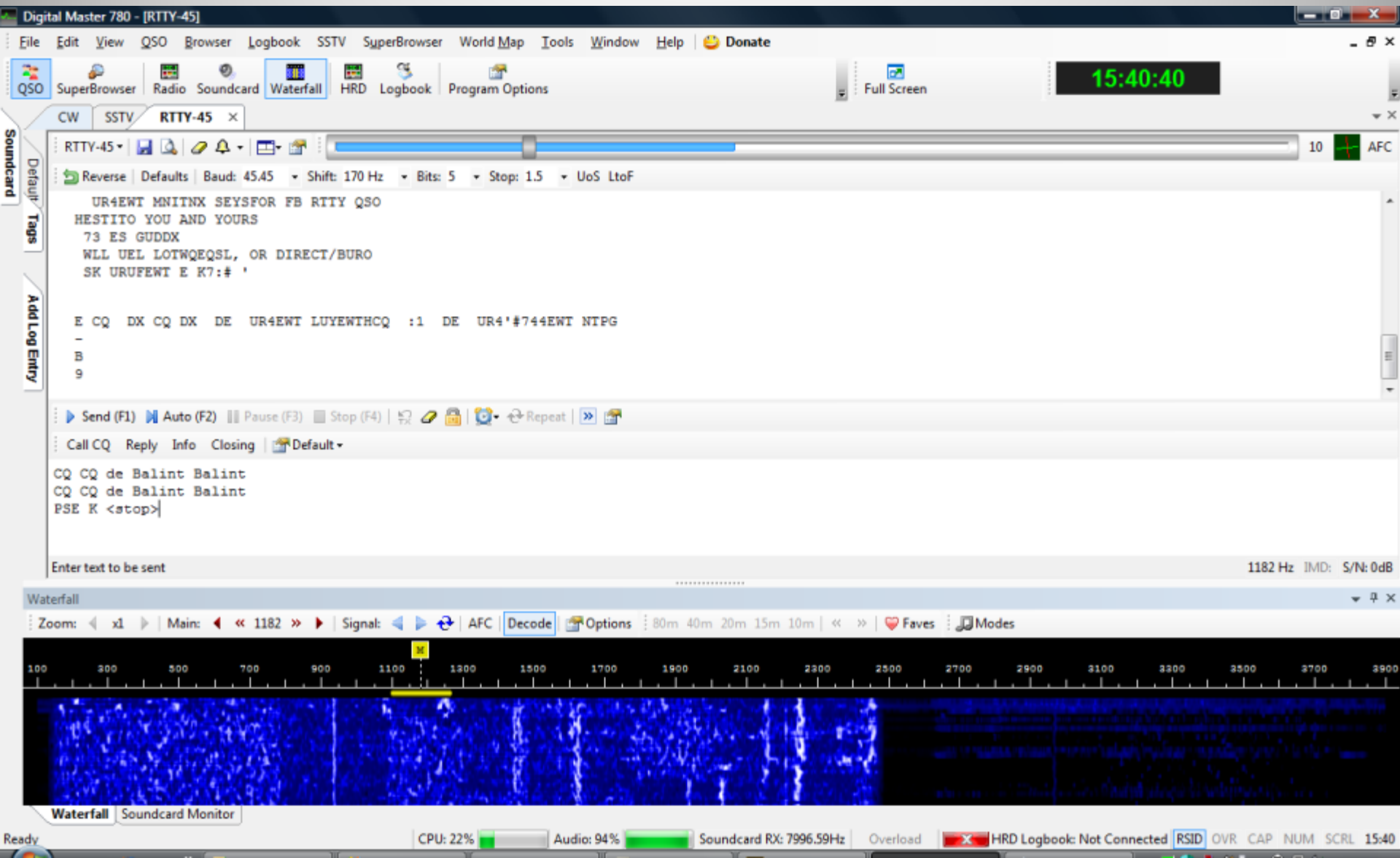



Top Block
TETRA
BB
Demod
Xtra
Fast AutoCorrelation
dB
ms
Repeating idle pattern
Scope Plot
Ch1
Ch2
Counts
Time (ms)
Frequency correction burst
Axes Options
Secs/Div:
Counts/Div:
Y Offset:
T Offset:
Autorange
Channel Options
Ch1
Ch2
Trig
XY
Coupling:
DC
Marker:
Line Link
Stop

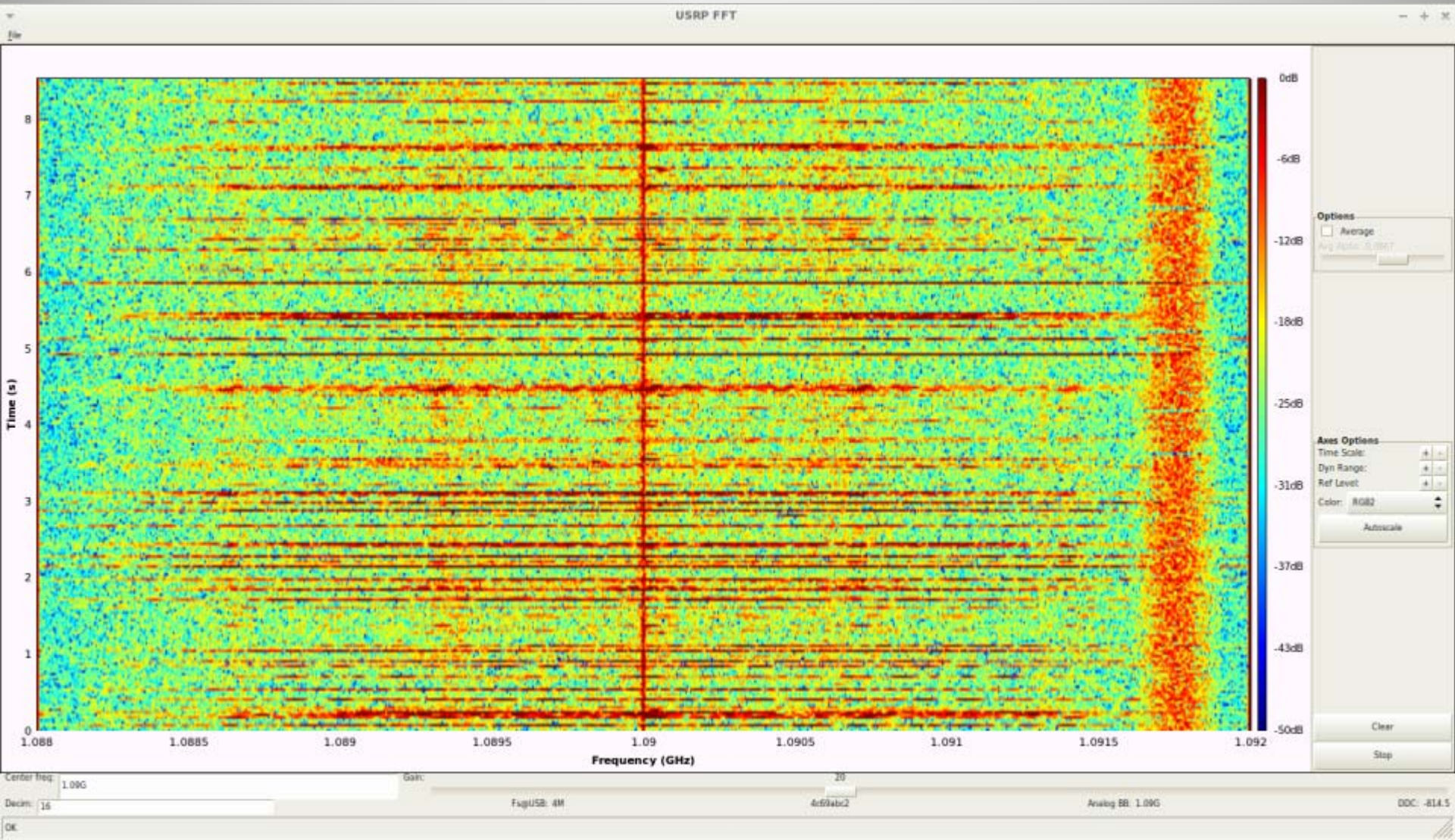
USRP out and about



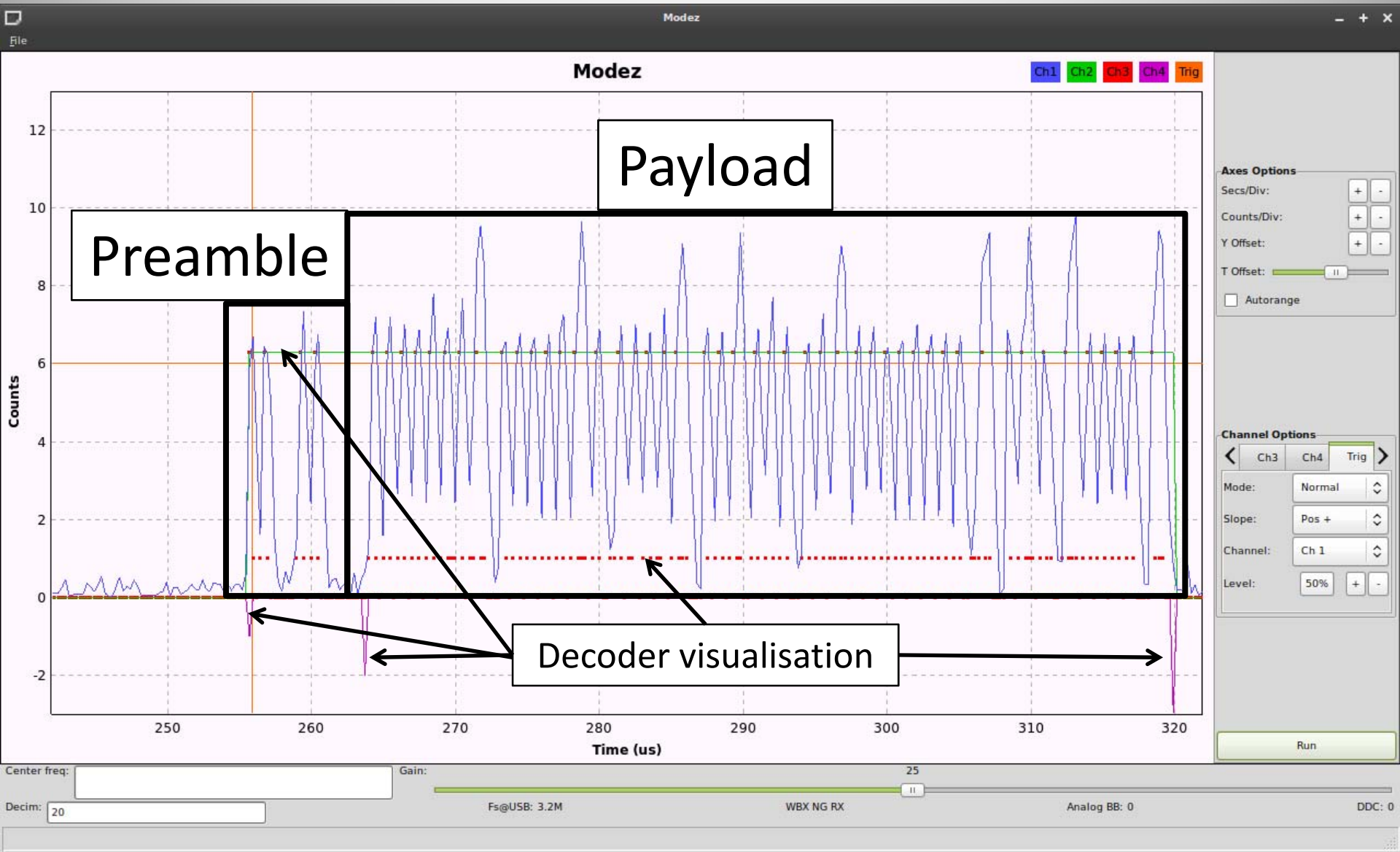

ShowOptions
Select Sound Card
Select Sample Rate
Stop
Minimize
About
Exit
Gain
Contrast
074,205,342 Tune LO 073,993,000
74165
74170
74175
74180
74185
74190
74195
74200
74205
74210
74215
-20
-30
-40
-50
-60
-70
-80
-90
-100
-110
-120
-130
-140
Speed
/10
F
Rev
WF Avg
RBW 61.0 Hz
AM
ECSS
FM
LSB
USB
CW
DRM
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
-10
-20
-30
-40
-50
-60
-70
-80
-90
-100
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%)


Digital Master 780 - [RTTY-45]
File Edit View QSO Browser Logbook SSTV SuperBrowser World Map Tools Window Help Donate
QSO SuperBrowser Radio Soundcard Waterfall HRD Logbook Program Options
Full Screen
15:40:40
CW SSTV RTTY-45
RTTY-45
10
AFC
Reverse Defaults Baud: 45.45 Shift: 170 Hz Bits: 5 Stop: 1.5 UoS LtoF
UR4EWT MNITNX SEYSFOR FB RTTY QSO
HESTITO YOU AND YOURS
73 ES GUDDX
WLL UEL LOTWQEQSL, OR DIRECT/BURO
SK URUFEWT E K7:# '
E CQ DX CQ DX DE UR4EWT LUYEWTHCQ :1 DE UR4'#744EWT NTPG
Send (F1) Auto (F2) Pause (F3) Stop (F4) Repeat
Call CQ Reply Info Closing Default
CQ CQ de Balint Balint
CQ CQ de Balint Balint
PSE K <stop>
Enter text to be sent
1182 Hz IMD: S/N: 0dB
Waterfall
Zoom: x1 Main: 1182 Signal: AFC Decode Options 80m 40m 20m 15m 10m Faves Modes
100 300 500 700 900 1100 1300 1500 1700 1900 2100 2300 2500 2700 2900 3100 3300 3500 3700 3900
Waterfall Soundcard Monitor
Ready
CPU: 22% Audio: 94% Soundcard RX: 7996.59Hz Overload HRD Logbook: Not Connected RSID OVR CAP NUM SCRL 15:40

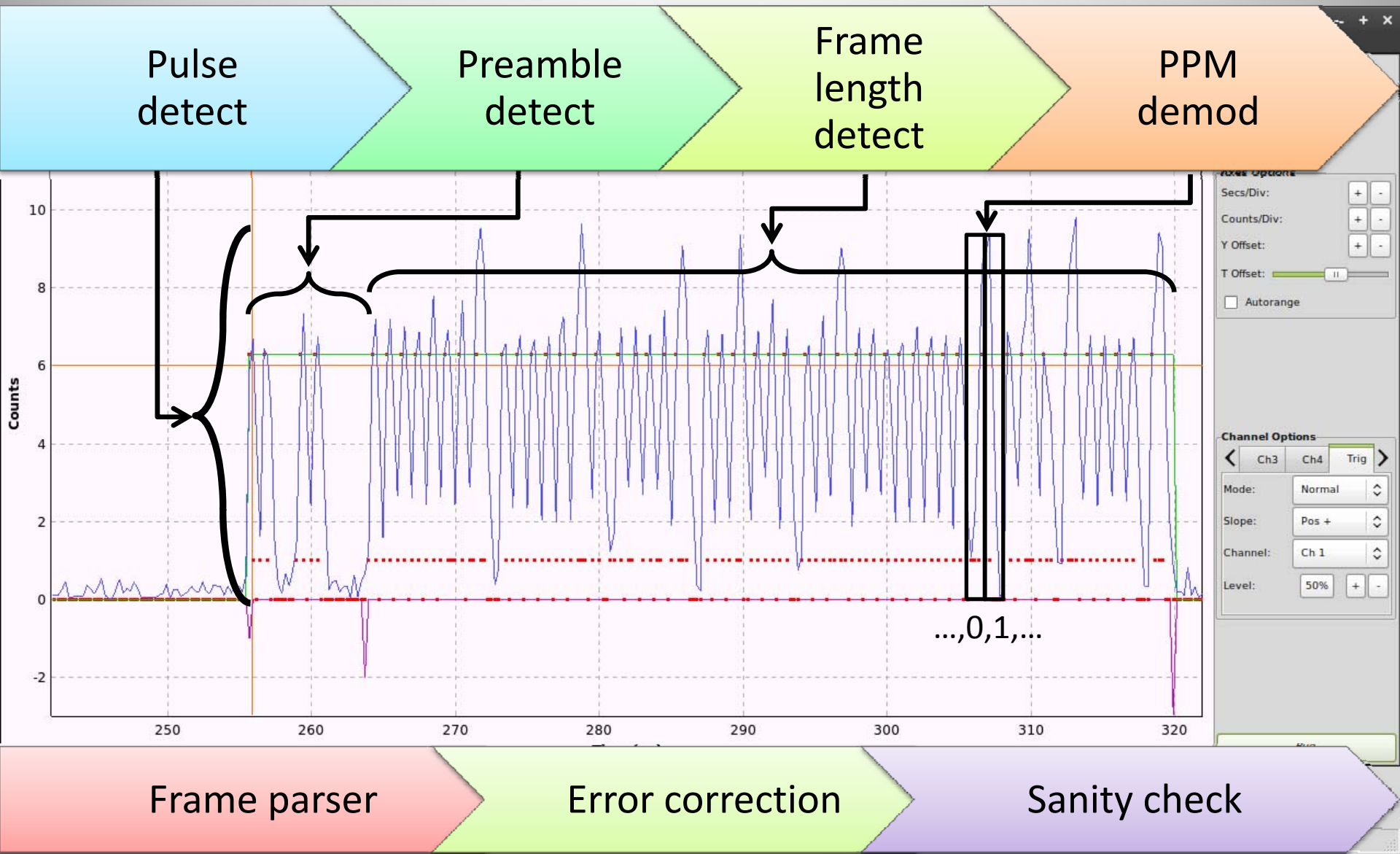
Mode S Waterfall



Mode S Response: AM signal



Mode S Decoder Structure

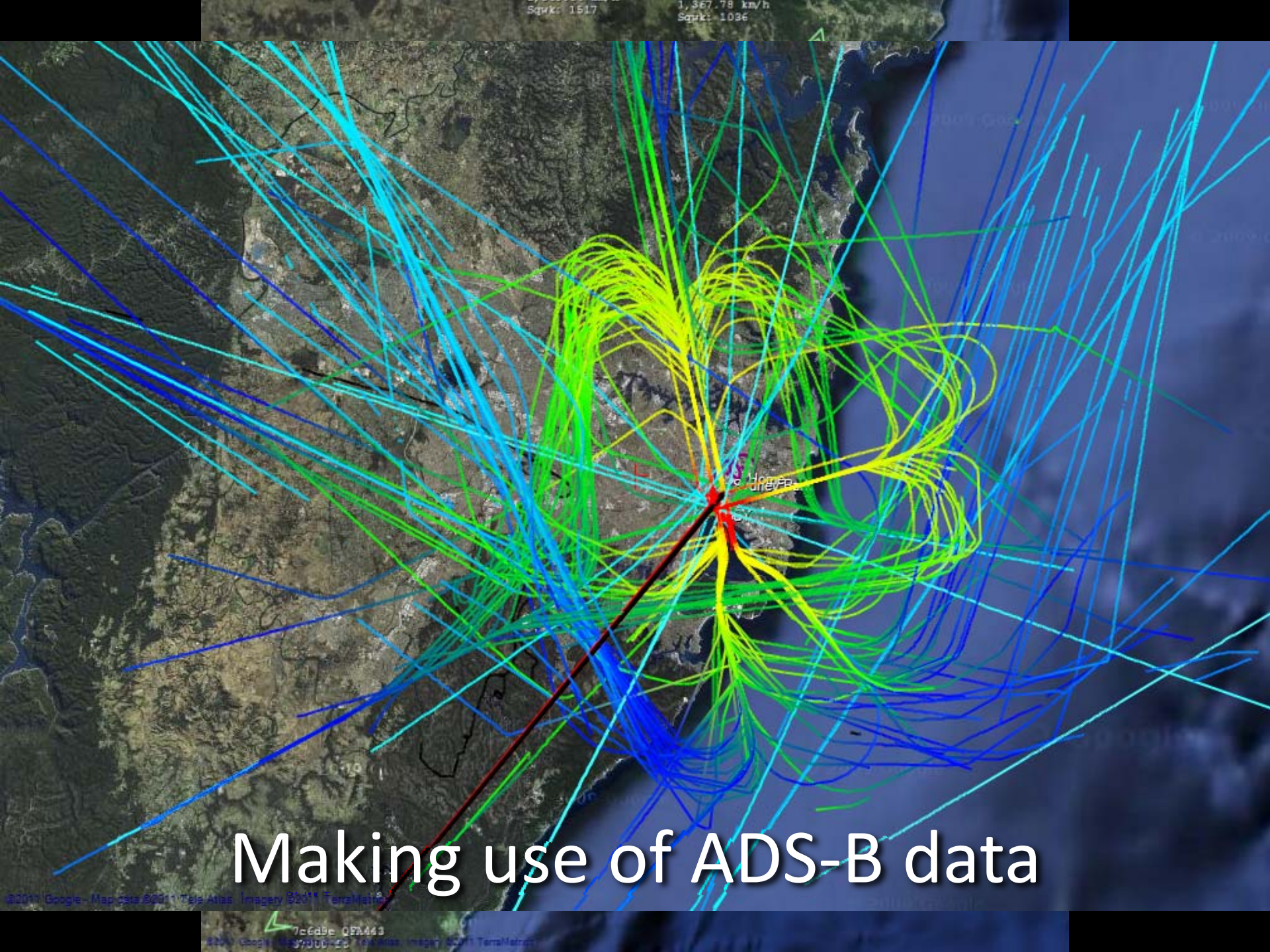


ADS-B: **E**xtended **S**quitter

- Several ES types:
  - 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!”)

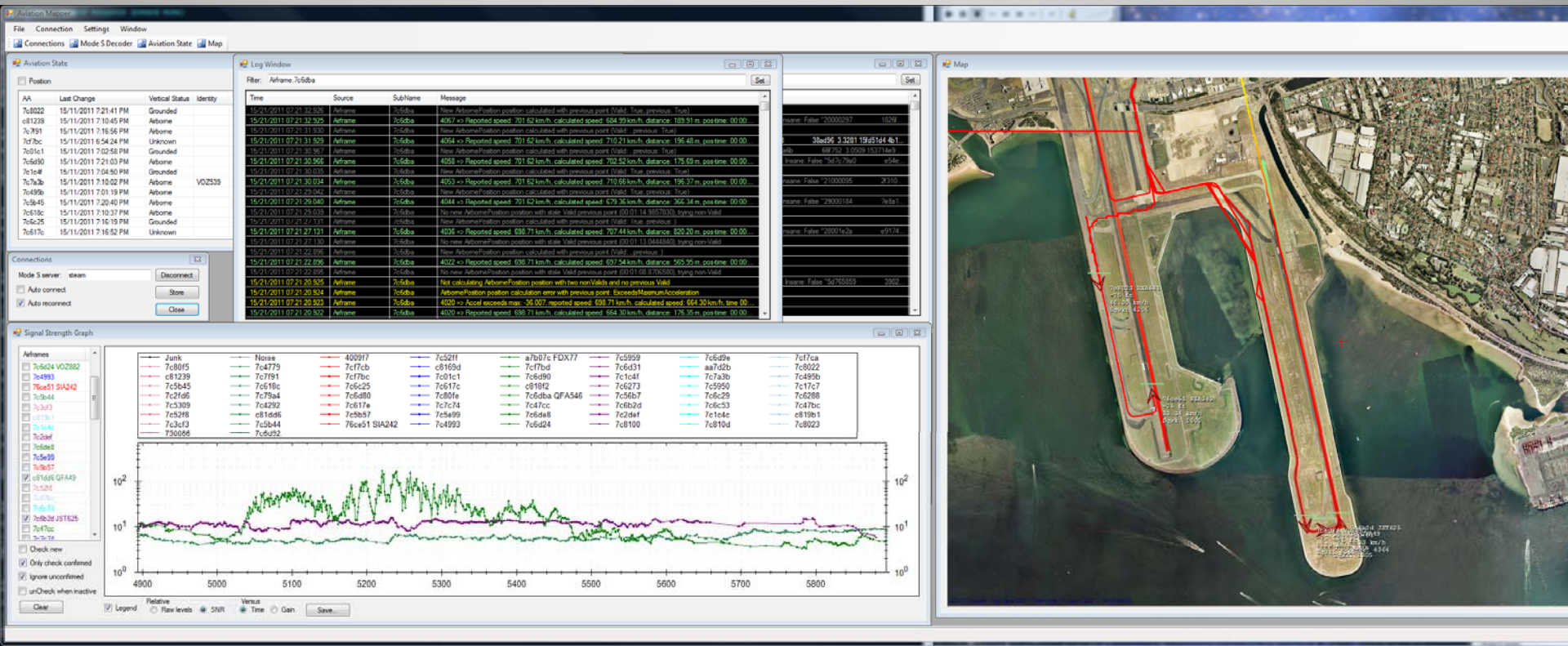
“Carl… get the diagnostics.”

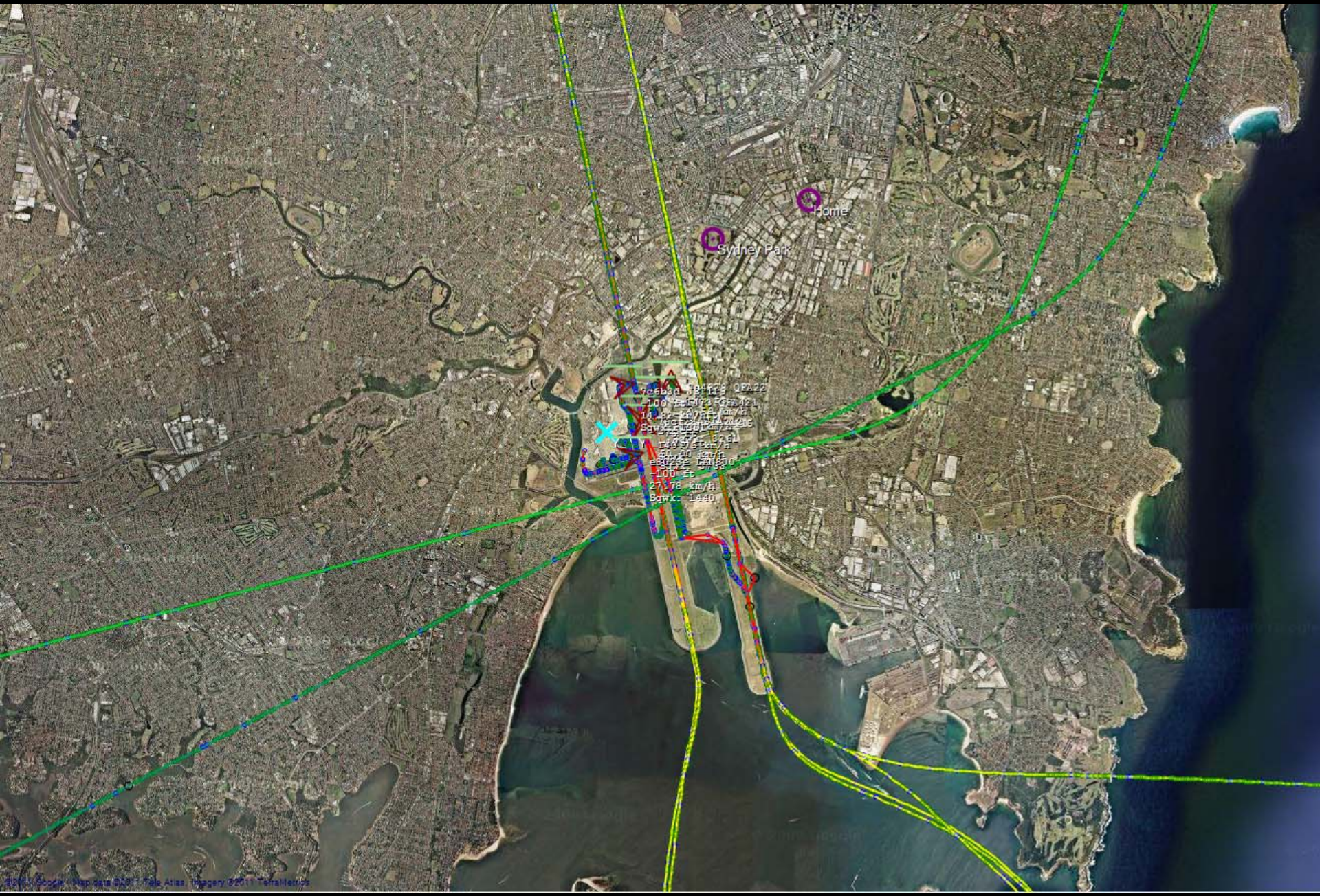
“Carl, you got your little black book?”

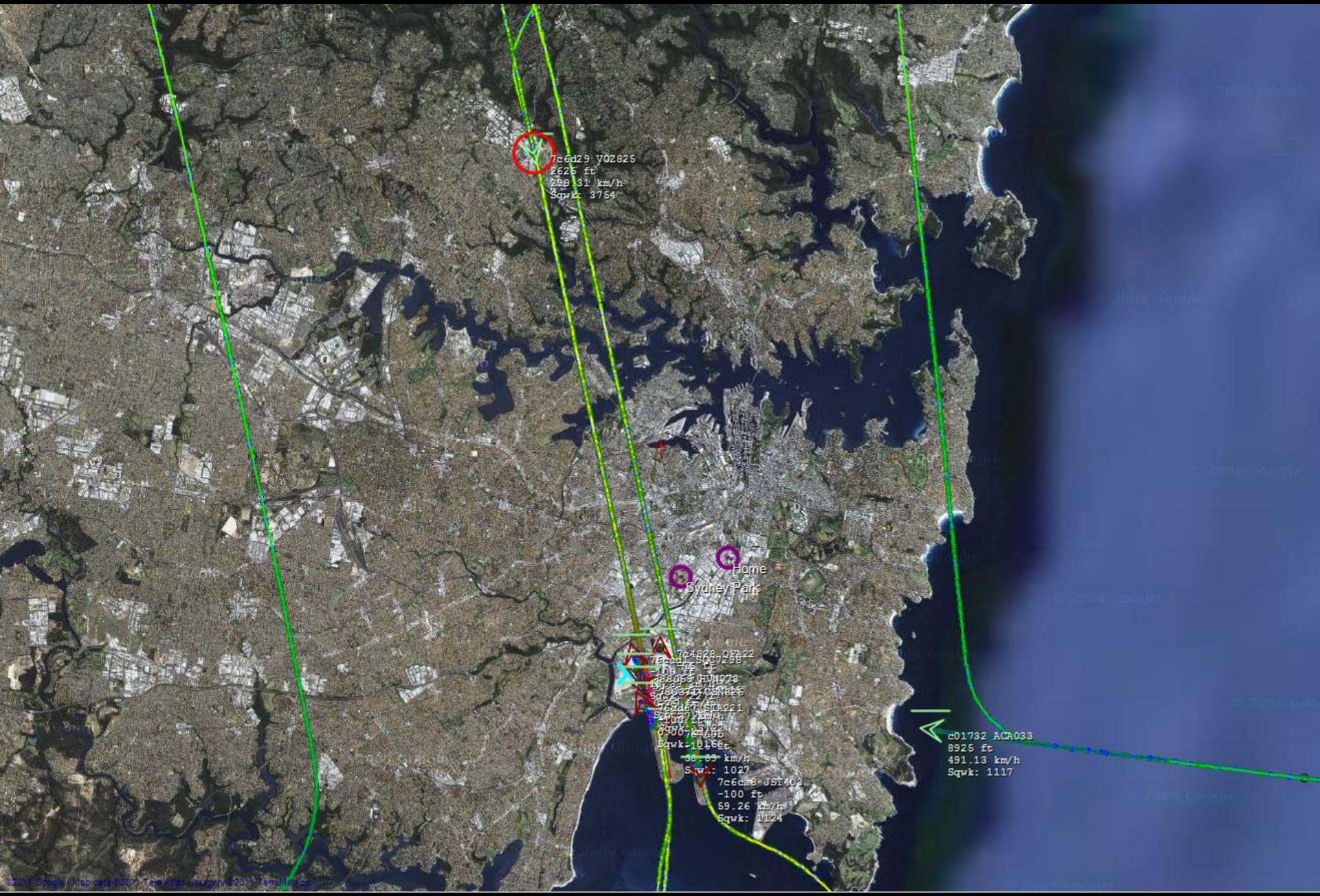

Making use of ADS-B data

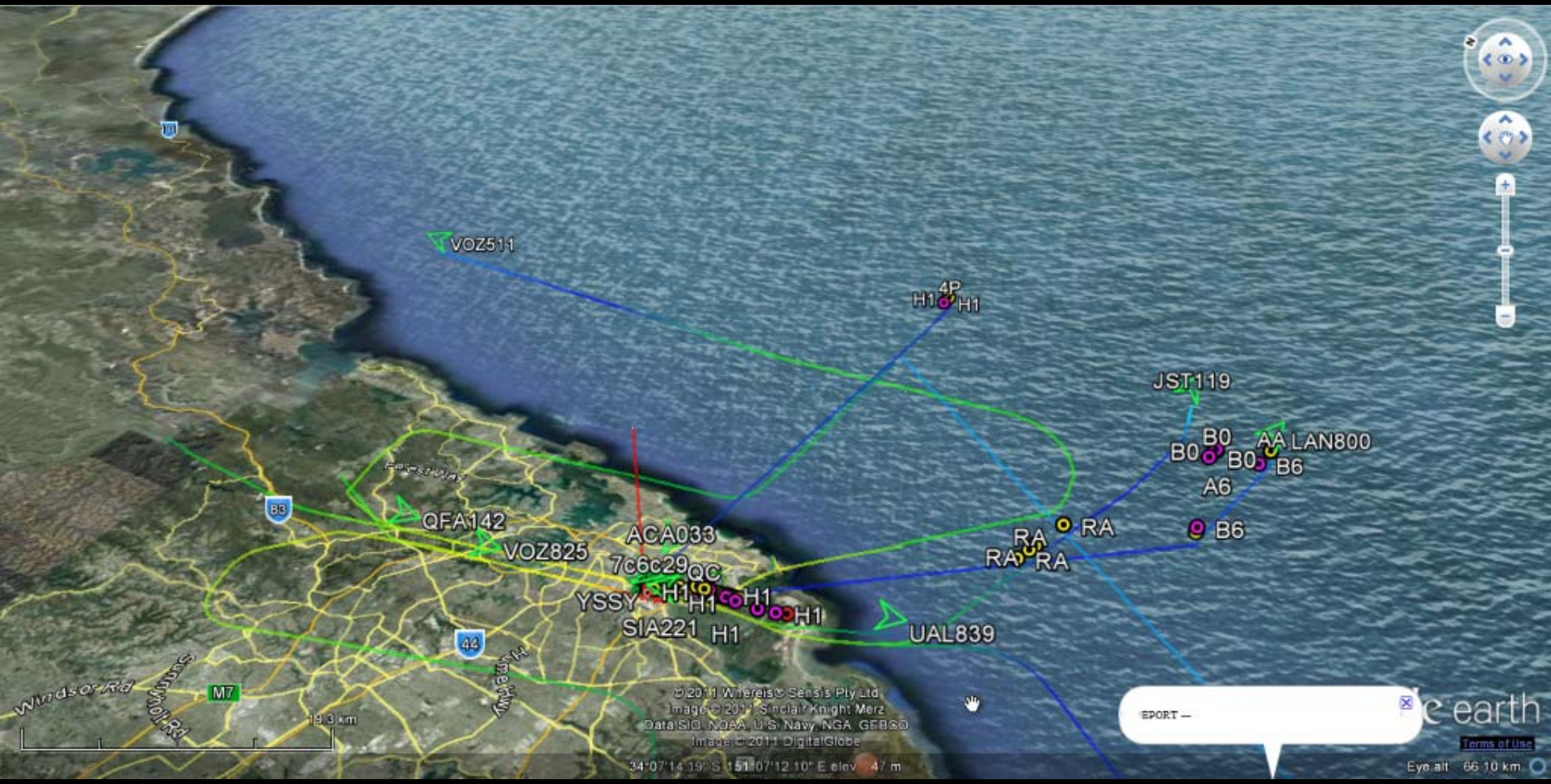
AviationMapper

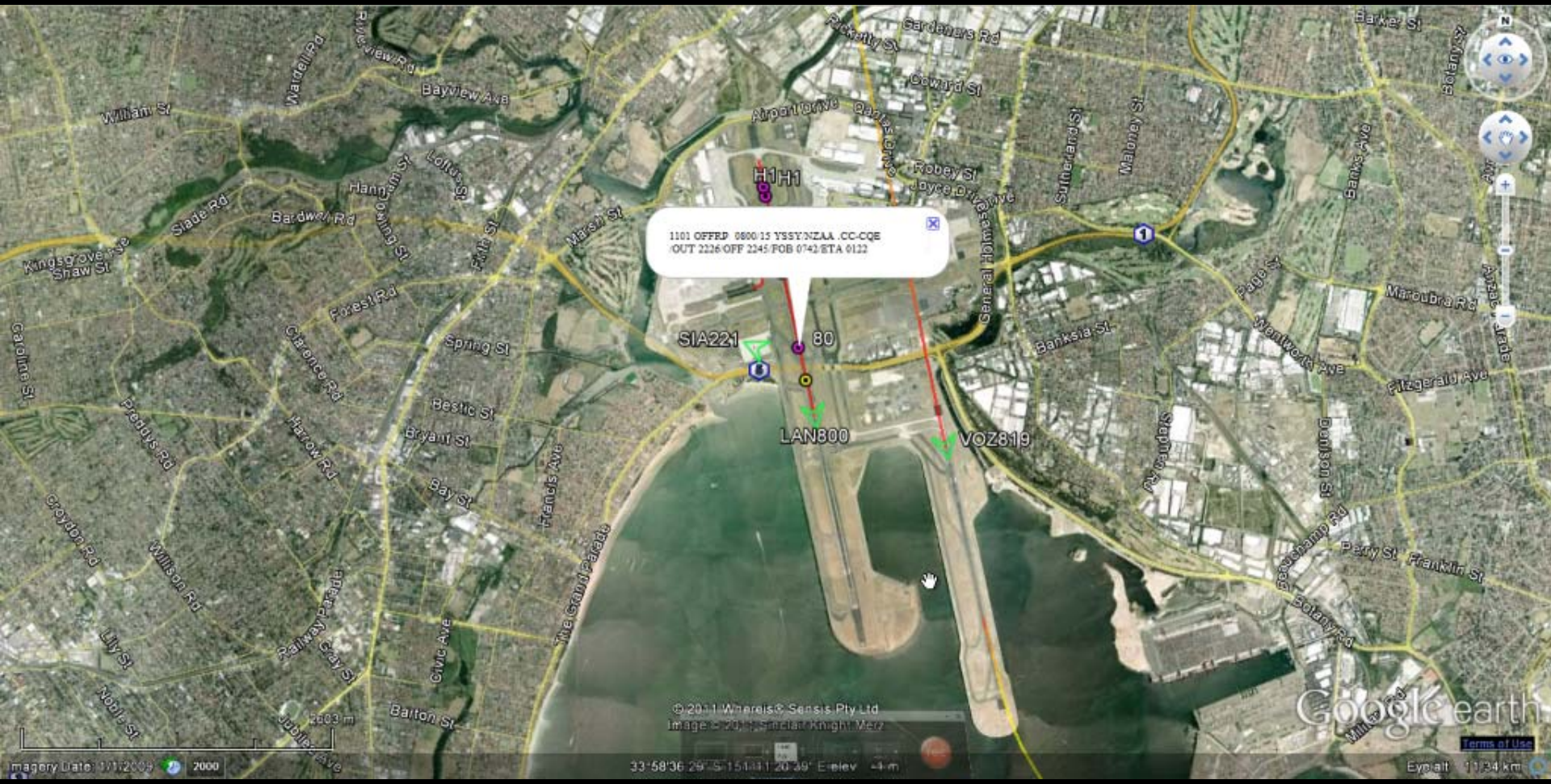
- Connects to Mode S decoder server
- Tracks & plots airframes, collects statistics
- Provides state server for web streaming

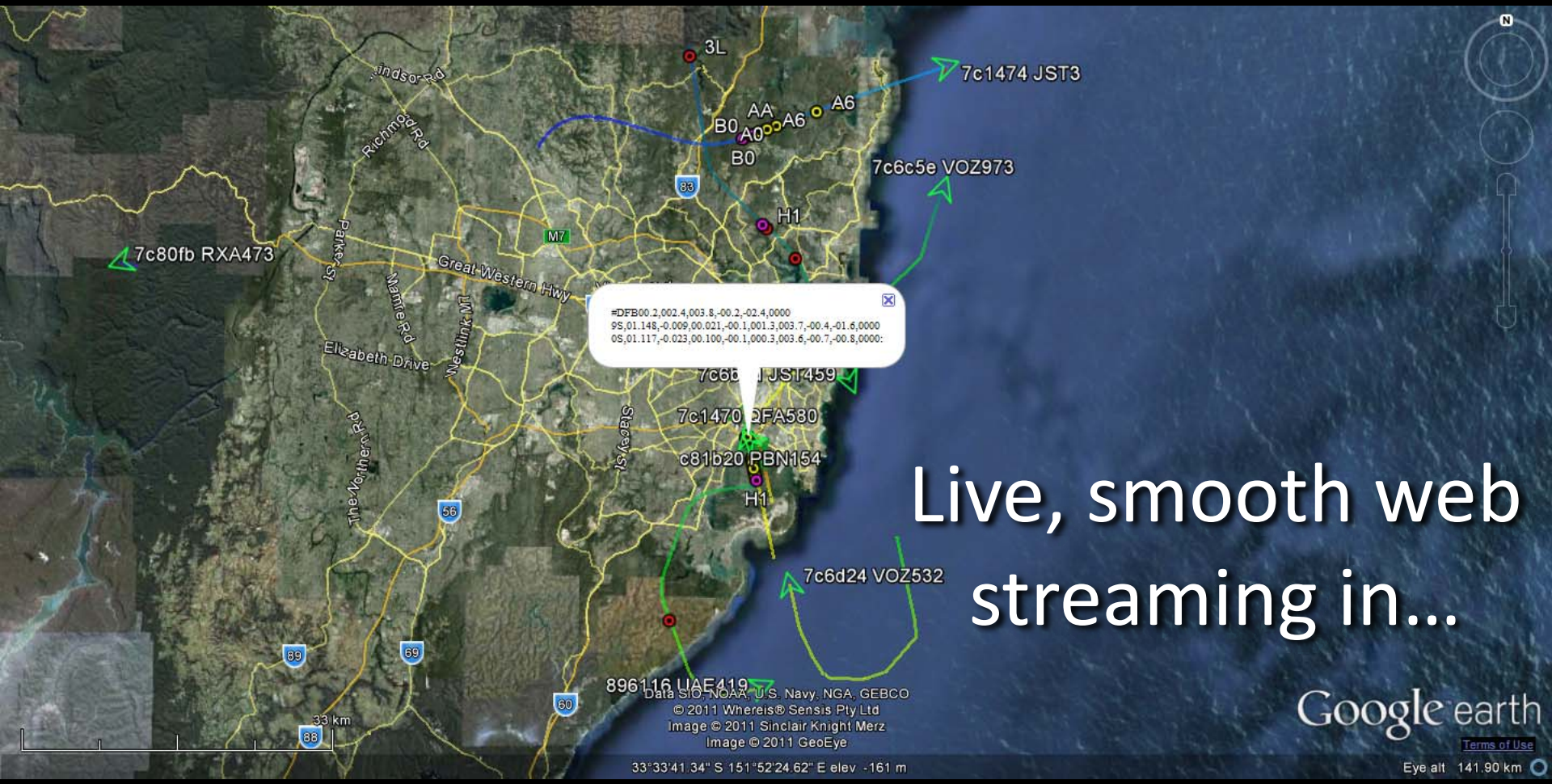



Home
Sydney Park


7c6d29 VOZ825
2625 ft
298.31 km/h
Sqwk: 3754
Home
Sydney Park
c01732 ACA033
8925 ft
491.13 km/h
Sqwk: 1117
7c6da8 JST403
-100 ft
59.26 km/h
Sqwk: 1124


VOZ511
4P
H1
H1
JST119
B0
B0
B0
AA
LAN800
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
Google earth


3L
7c1474 JST3
A6
AA
A6
B0
A0
B0
7c6c5e VOZ973
H1
7c80fb RXA473
Great Western Hwy
#DFB00.2,002.4,003.8,-00.2,-02.4,0000
9S,01.148,-0.009,00.021,-00.1,001.3,003.7,-00.4,-01.6,0000
0S,01.117,-0.023,00.100,-00.1,000.3,003.6,-00.7,-00.8,0000:
Elizabeth Drive
7c1470 QFA580
c81b20 PBN154
H1
7c6d24 VOZ532
896116 UAE419
Live, smooth web streaming in…
Data SIO, NOAA, U.S. Navy, NGA, GEBCO
© 2011 Whereis® Sensis Pty Ltd
Image © 2011 Sinclair Knight Merz
Image © 2011 GeoEye
33°33'41.34" S 151°52'24.62" E elev -161 m
Google earth
Terms of Use
Eye alt 141.90 km

Modez History

Re: ADS-B

by citabria Mon Dec 28, 20

Geoff,

Just out of interest there has
for someone with the right co

http://sites.google.com/si

Cheers,
Matt

Modez Mk IIpoint5

Science experiment

in progress until 10pm -

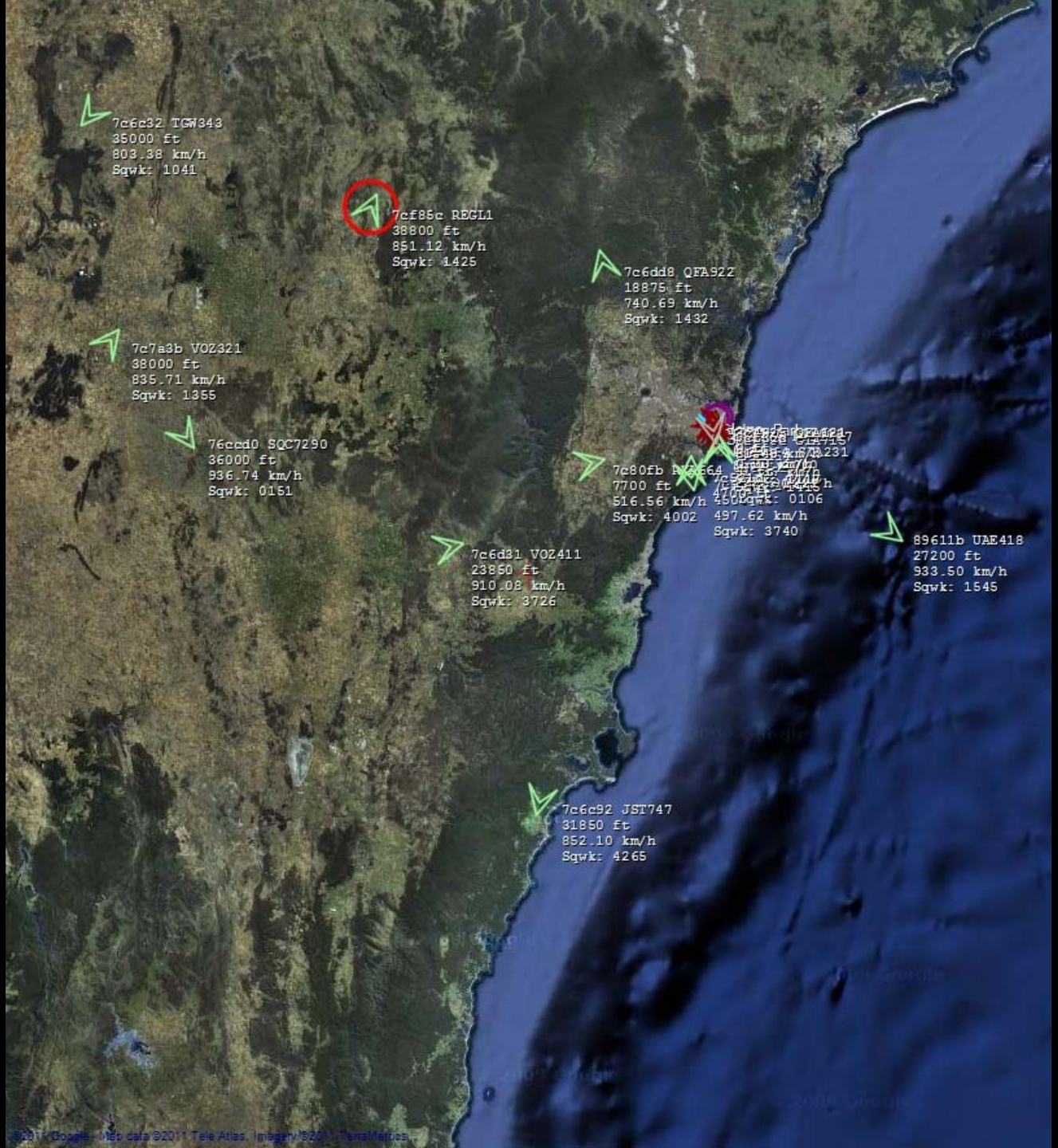
please do not touch.

Any questions, please call

[redacted]

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
89611b UAE418
27200 ft
933.50 km/h
Sqwk: 1545
7c6d31 VOZ411
23850 ft
910.08 km/h
Sqwk: 3726
7c6c92 JST747
31850 ft
852.10 km/h
Sqwk: 4265

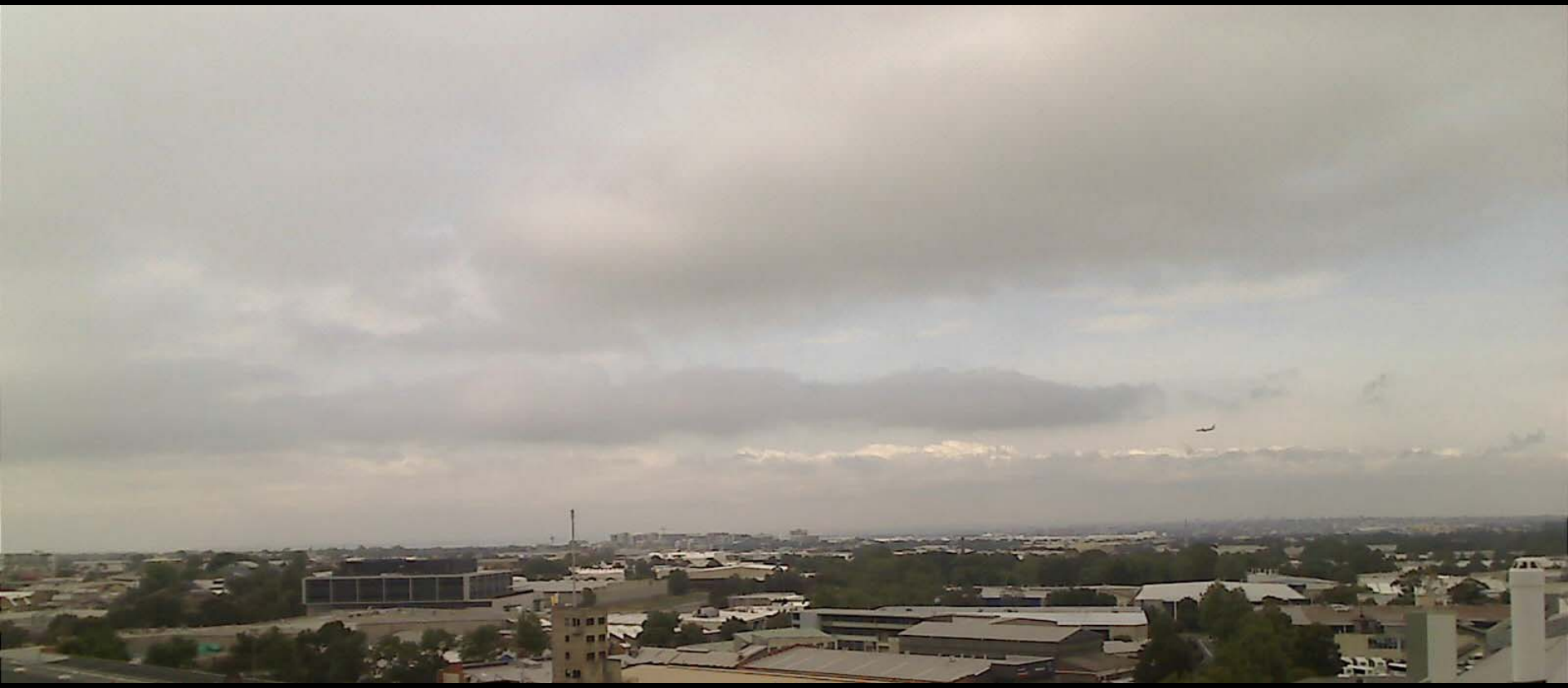
Aviation State

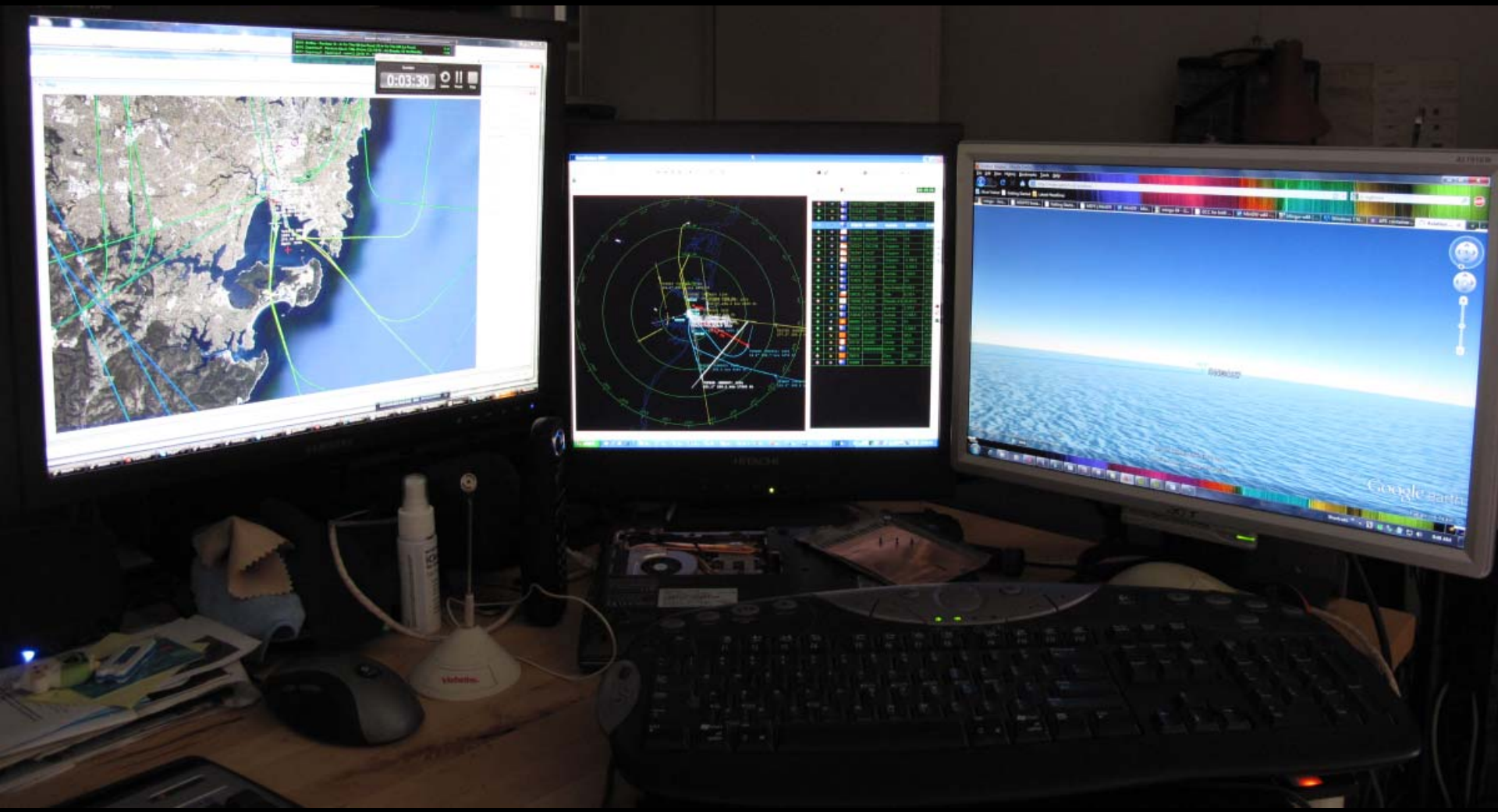
Position

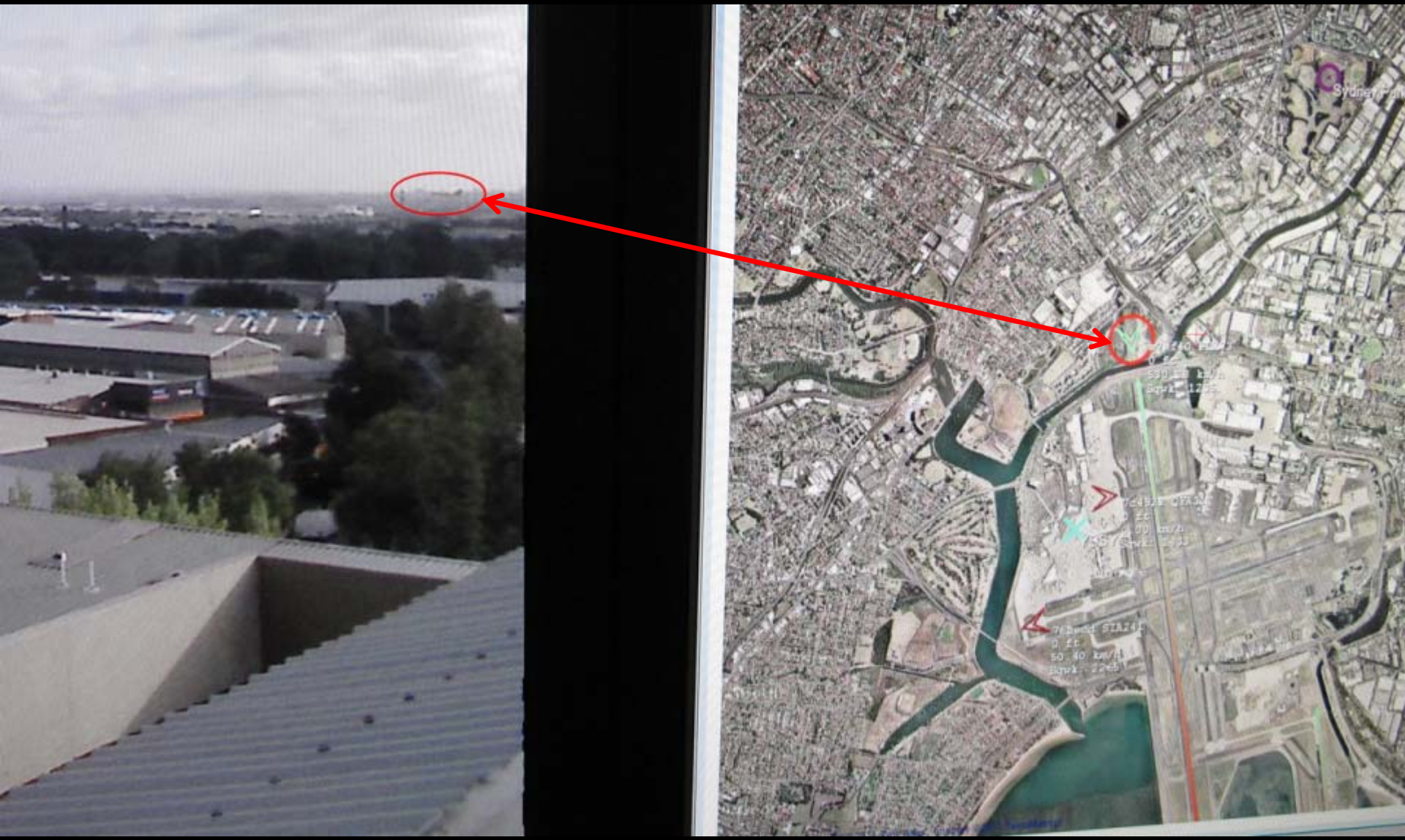
AA	Last Change	Vertical Status	Identity	Transponder	Altitude	Rate	Position	Speed	Heading	Distance
7c6289	16/11/2011 2:55:53 PM	Airborne			725					
7c6a7e	16/11/2011 1:29:35 PM	Airborne								
7c5310	16/11/2011 2:54:13 PM	Grounded		4253	-150					
7cf7cb	16/11/2011 2:49:52 PM	Grounded		7722						
780236	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

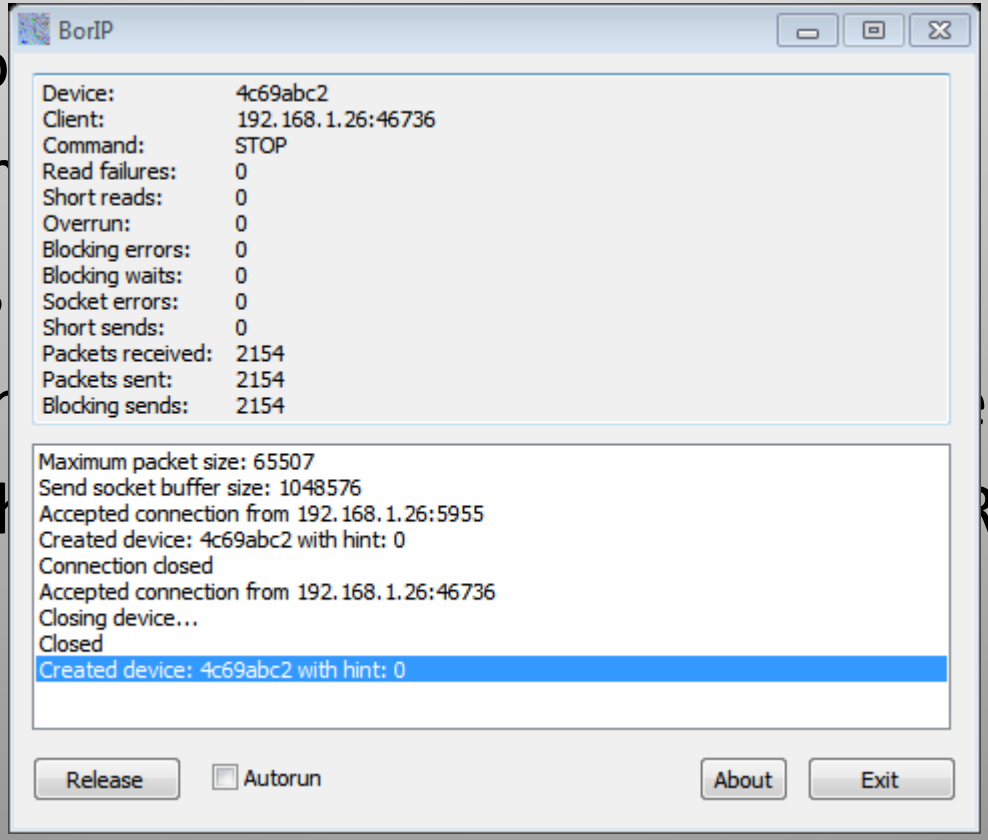



0:03:30



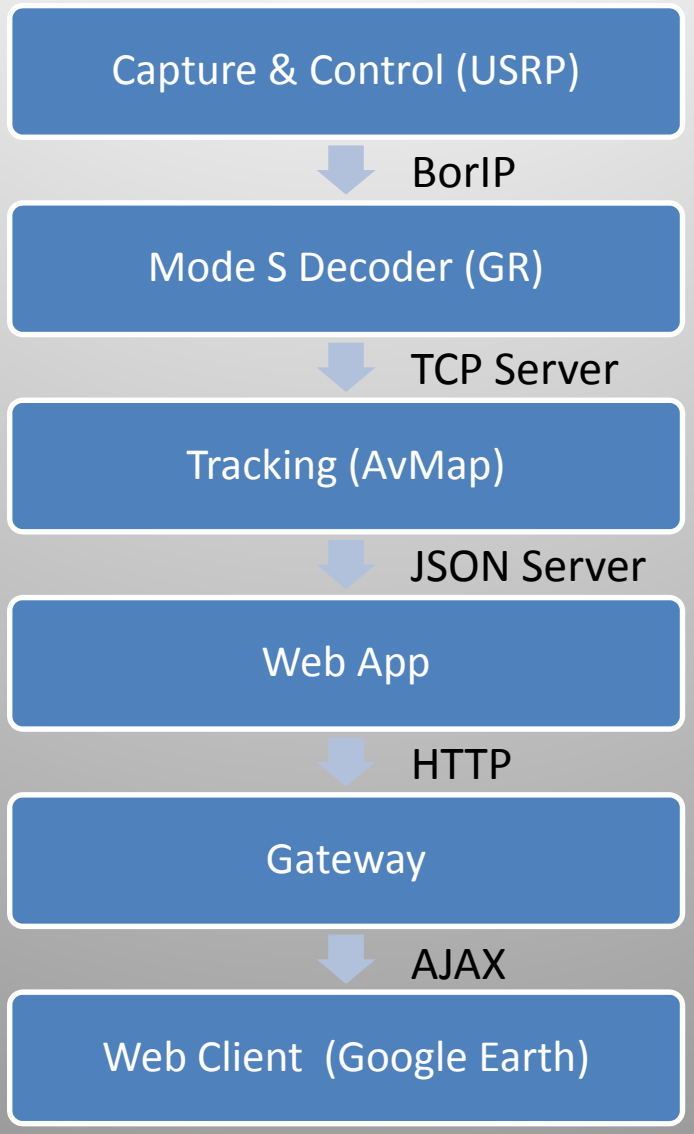
BorIP

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



, etc)

Antenna to Google Earth

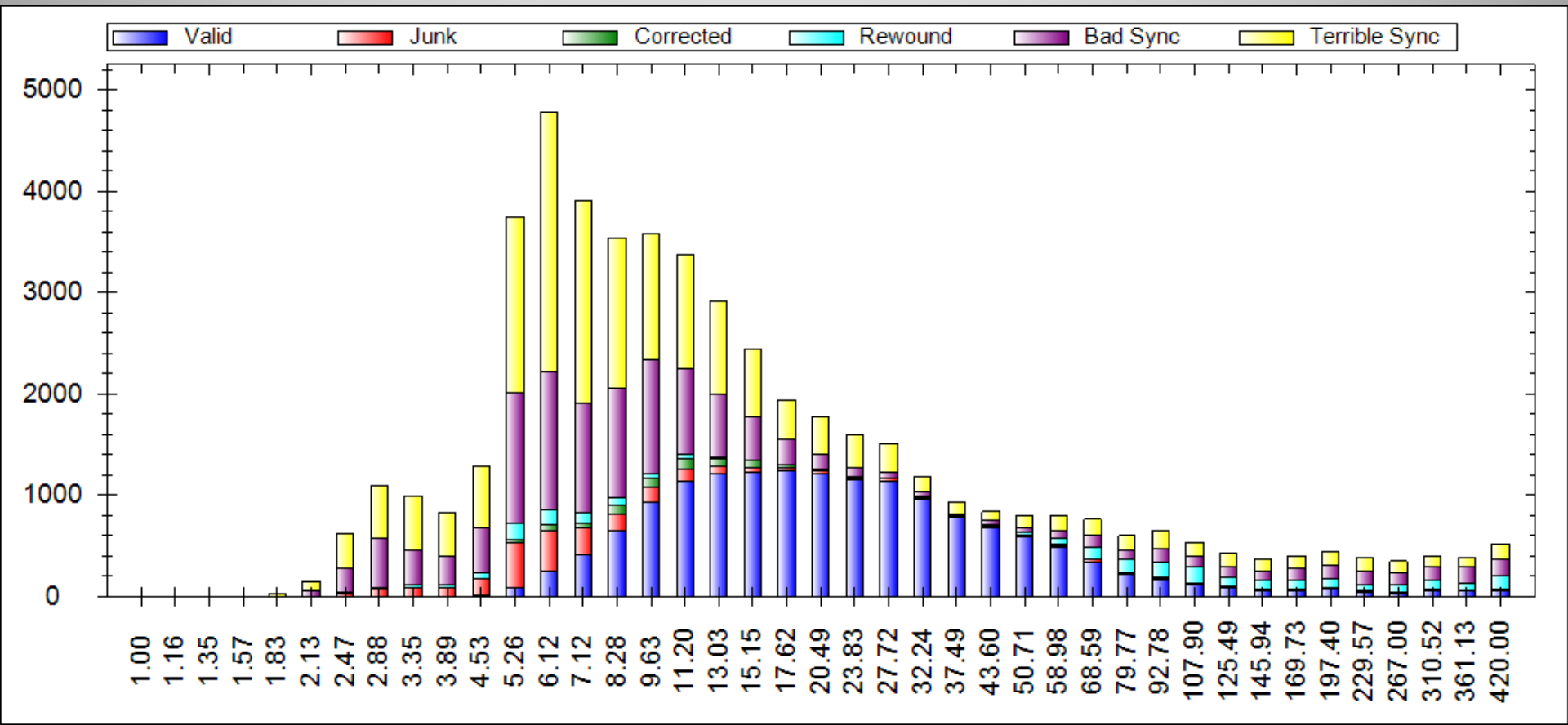


Modez Evolution

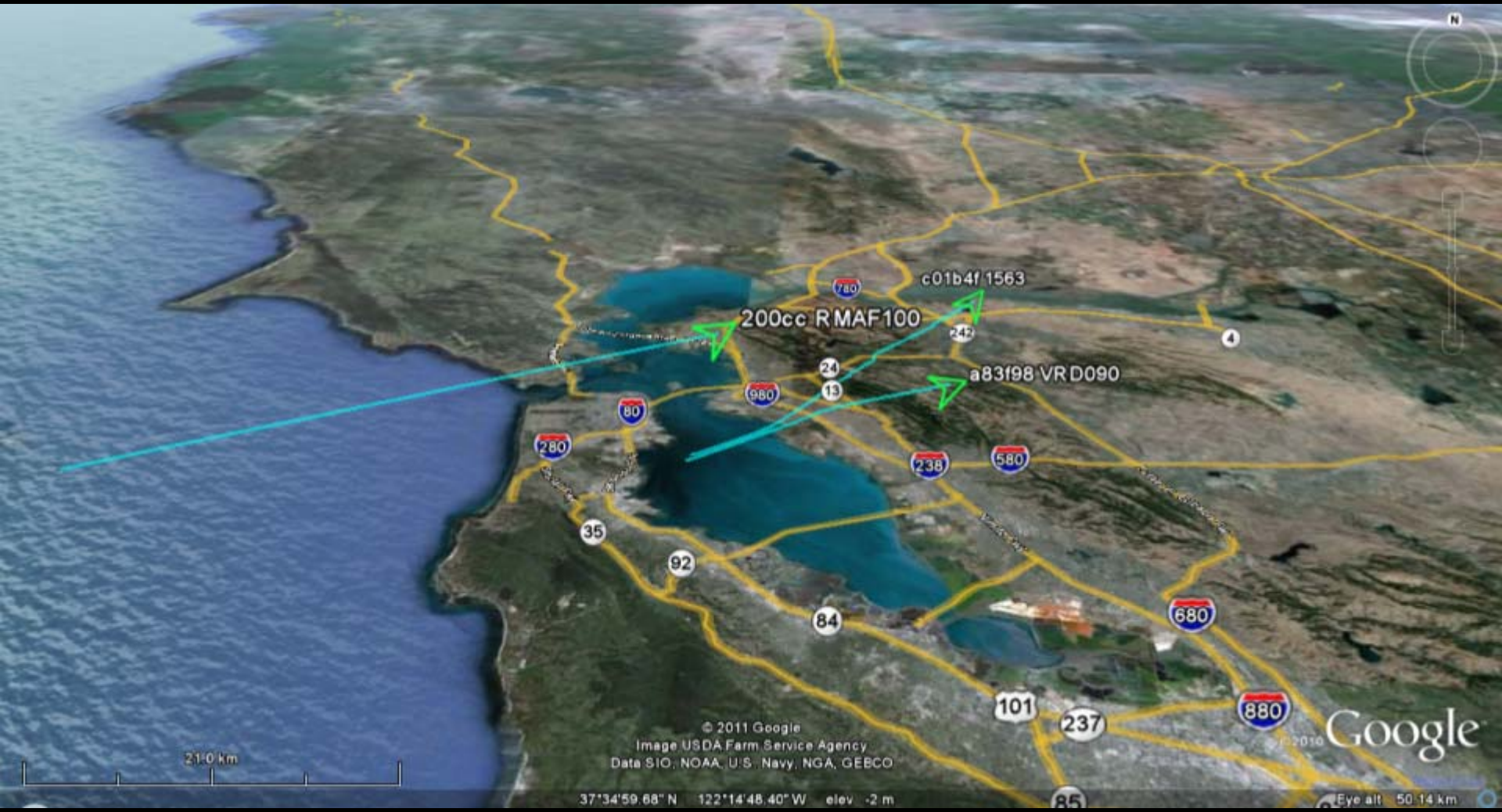
- Goal is to increase SNR
  - Best option is to drop the noise floor: filter, and/or choose optimal sample rate to avoid artifacts

Signal Strength Distribution

- Evaluate how well decoder is doing




4004e1 BAW228
34000 ft
791.37 km/h
Sqwk: 4
4ca5c7 EIN10X
17050 ft
698.06 km/h
Sqwk: 4
a77c11 COA54
9850 ft
627.04 km/h
Sqwk: 4
e8404c 2K0700
1550 ft
327.24 km/h
Sqwk: 4
40073e BAW183
0 ft
269.02 km/h
Sqwk: 4
40040f BAW114
0 ft
299.57 km/h
Sqwk: 4
3c4a81 DLH405
3800 ft
555.75 km/h
Sqwk: 4


c01b4f 1563
200cc R MAF100
a83f98 VR D090
780
242
4
24
13
980
80
280
238
580
35
92
84
680
101
237
880
N
© 2011 Google
Image USDA Farm Service Agency
Data SIO, NOAA, U.S. Navy, NGA, GEBCO
21.0 km
37°34'59.68" N 122°14'48.40" W elev -2 m
Eye alt 50.14 km
Google


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

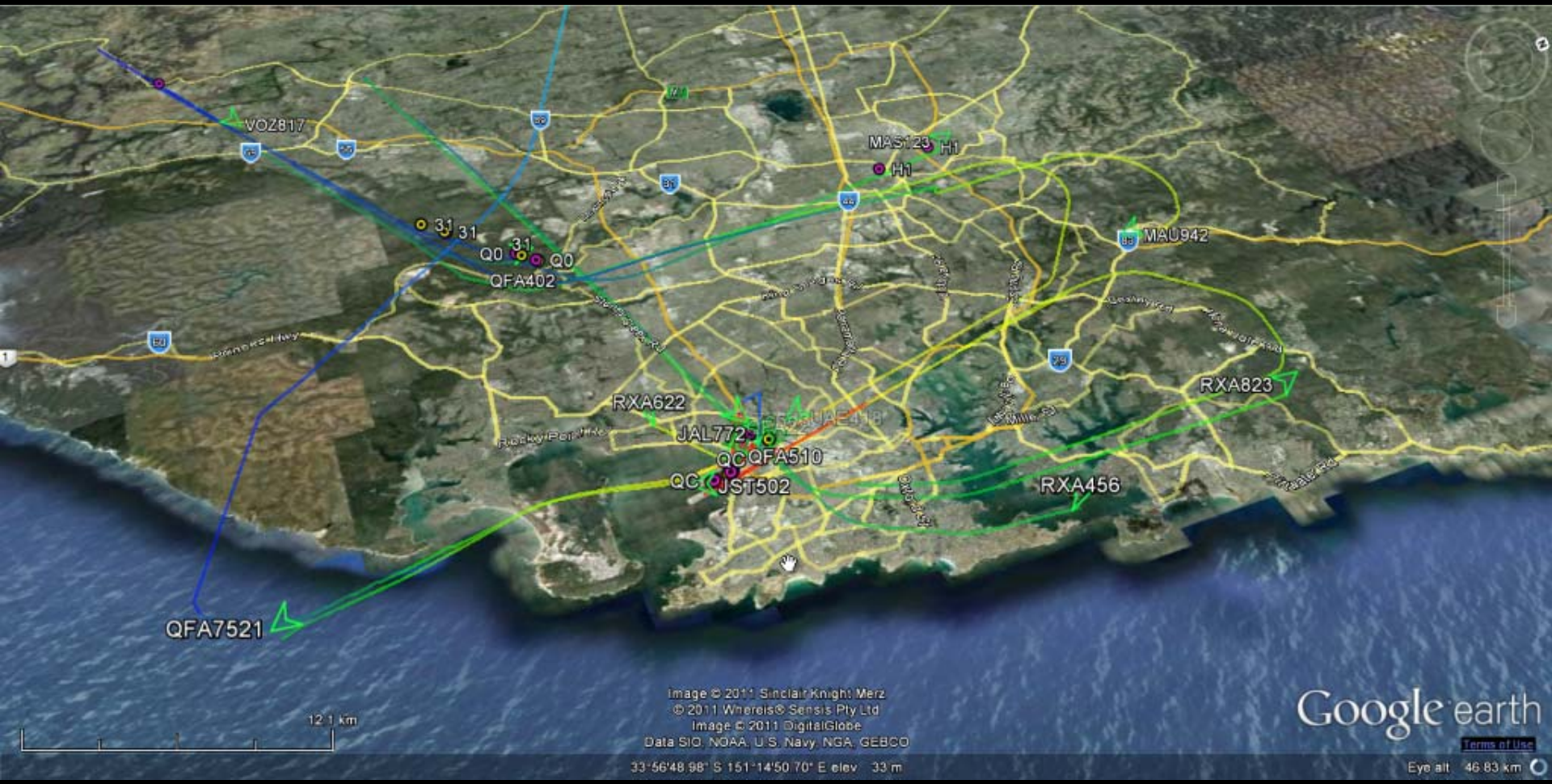
ACARS

- **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

- Two SDRs listening to primary & secondary frequency
- 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
```


VOZ817
MAS123
H1
H1
31
31
31
Q0
Q0
QFA402
MAU942
RXA622
RXA823
JAL772
QC
QFA510
QC
JST502
RXA456
QFA7521
12.1 km
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
Google earth
Terms of Use
Eye alt 46.83 km

Examples

Time: 2001-11-11 16:09:49.073000
Station: Home
Frequency: 131.55 MHz
Mode: 2 (uplink, LCN: 19)
Address: 9M-MPO
Ack: NAK
Label: H1 System Acknowledge (downlink)
Block: W
Message #: S12B
Flight ID: VNO373

TOILET CC1-INOP

LAV 61,HARD

LAV 37,HARD,140505;237346CIDS1 1,,,,,,,DEU A
(200RH2),HARD,140505;383141VSC 1,,,,,,,LAV 53,HARD,174906;


Section of Front Spar

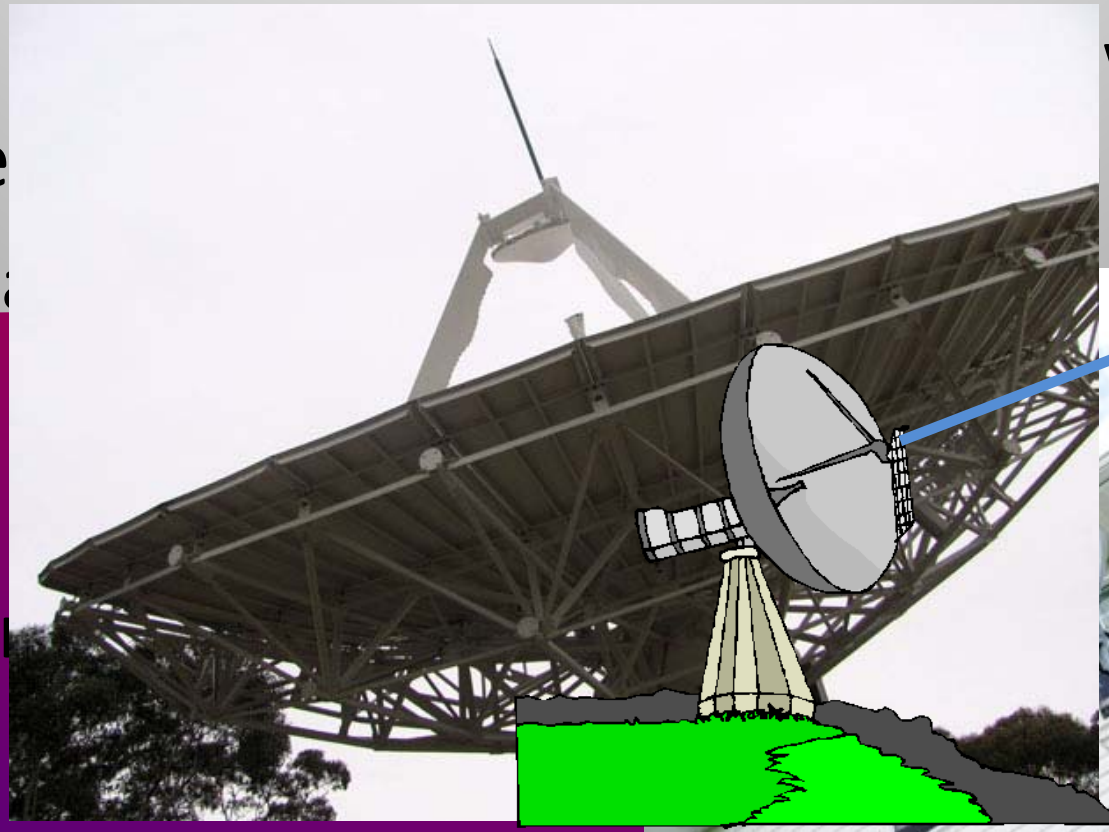
Decoding satellite downlinks

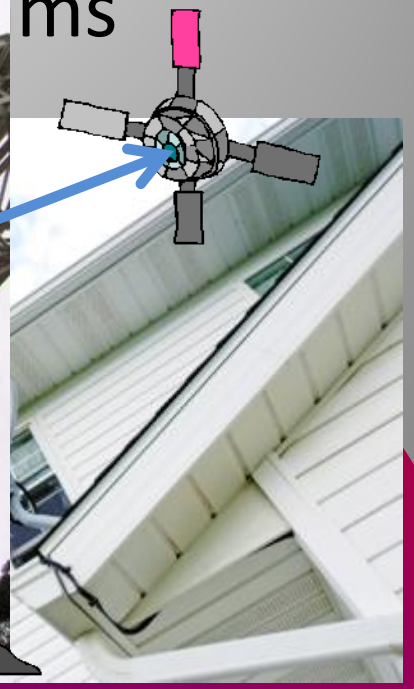
Recap

- 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
- Linear wnlink freque ms
- Cover a
- Linear anythi





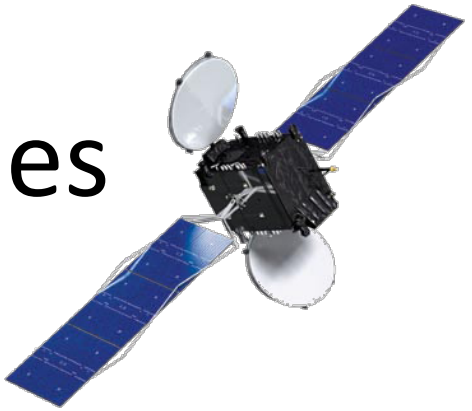
TT&C and UPC

- **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 $$$)

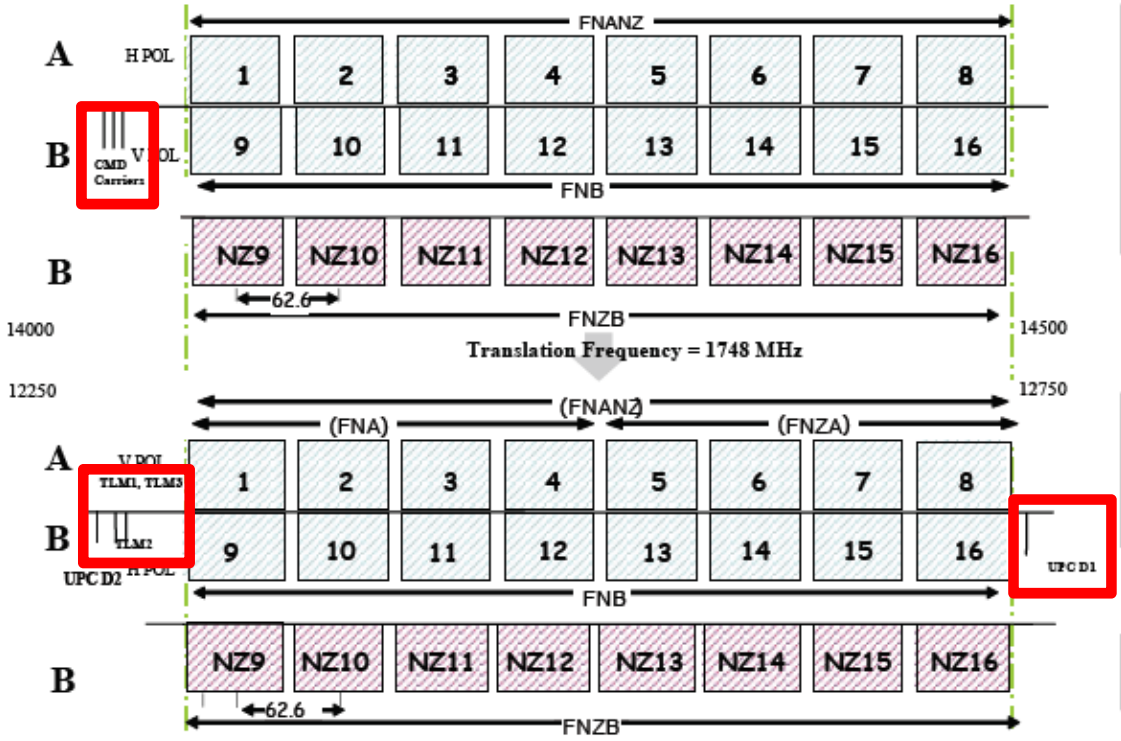
Optus D1

- 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…

D1 Channel Frequencies



Uplink



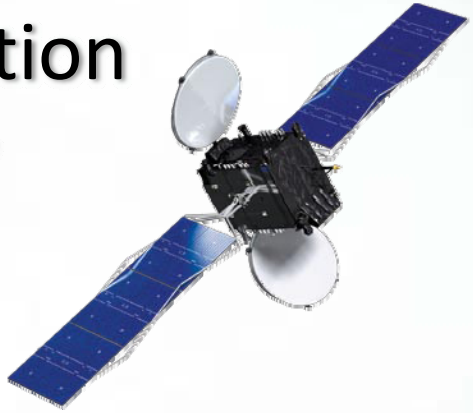
FSS Australia Centre Frequencies (MHz)		
Channel	Uplink	Downlink
1	14029.90	12281.90
2	14092.50	12344.50
3	14155.10	12407.10
4	14217.70	12469.70
5	14280.30	12532.30
6	14342.90	12594.90
7	14405.50	12657.50
8	14468.10	12720.10
9	14029.90	12281.90
10	14092.50	12344.50
11	14155.10	12407.10
12	14217.70	12469.70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

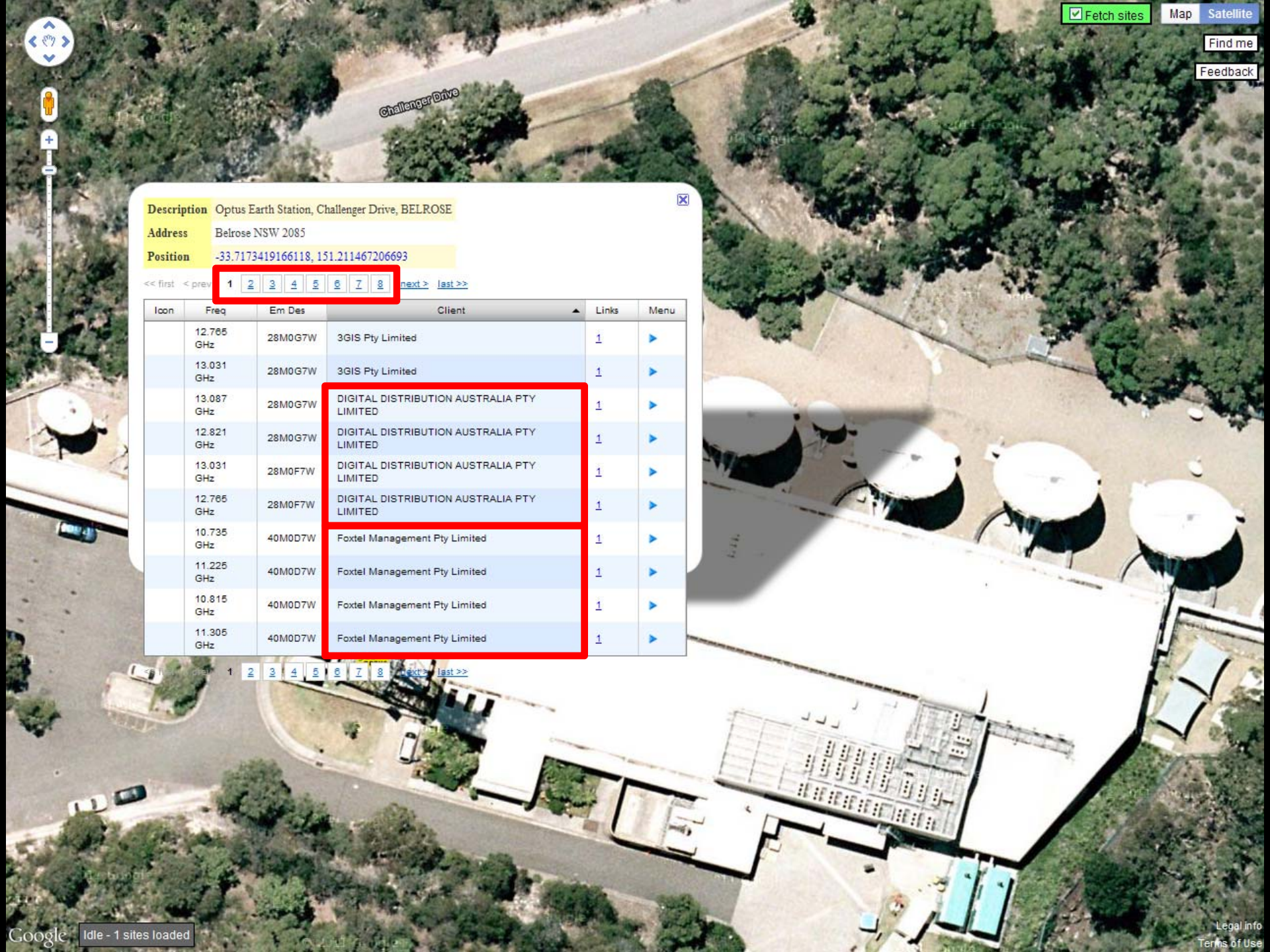
FSS NZ Centre Frequencies (MHz)		
Channel	Uplink	Downlink
NZ9	14029.90	12281.90
NZ10	14092.50	12344.50
NZ11	14155.10	12407.10
NZ12	14217.70	12469.70
NZ13	14280.30	12532.30
NZ14	14342.90	12594.90
NZ15	14405.50	12657.50
NZ16	14468.10	12720.10

D1

Downlink

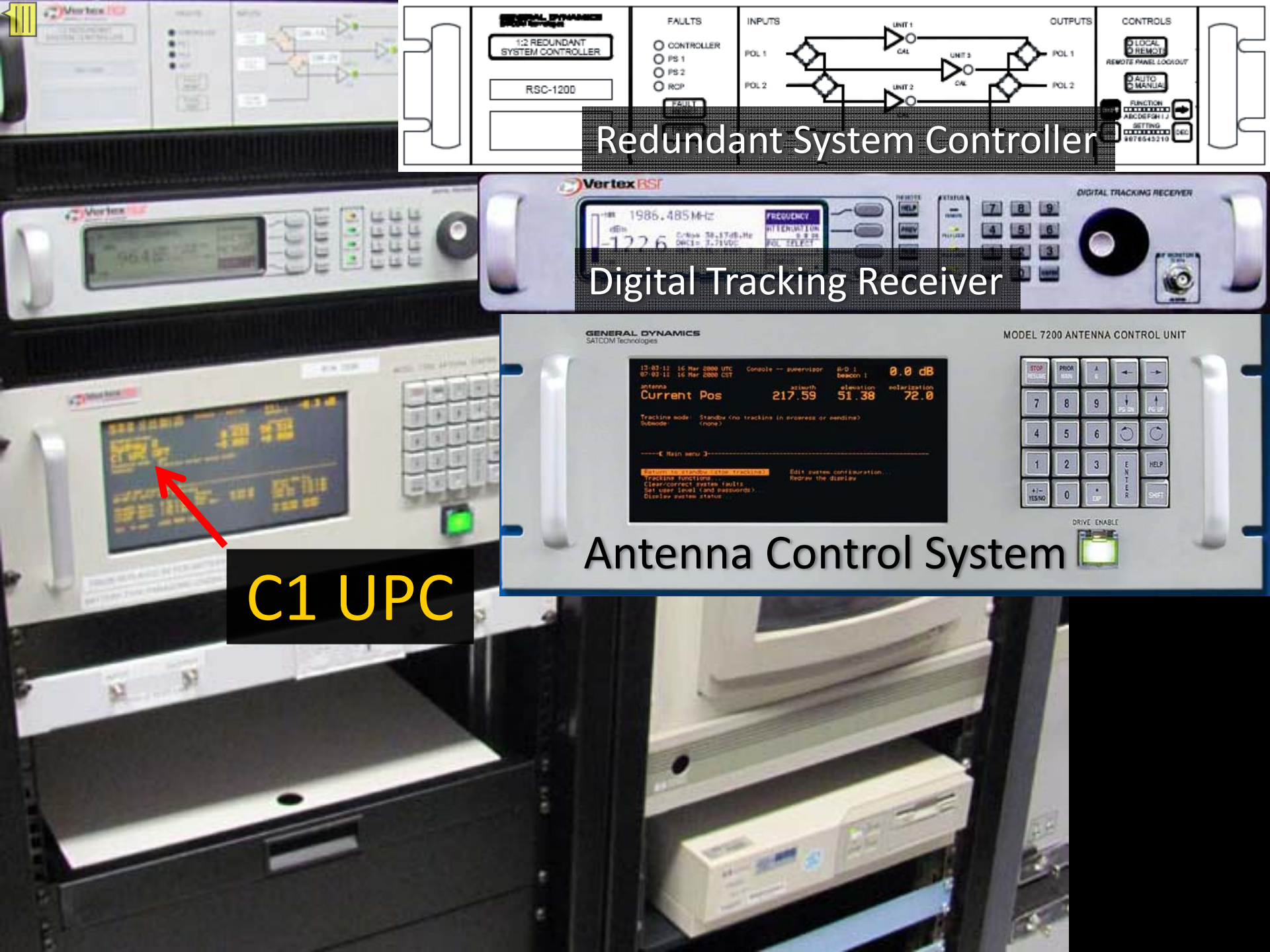
Optus Earth Station
Belrose, Sydney




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

Spot the satellite modem

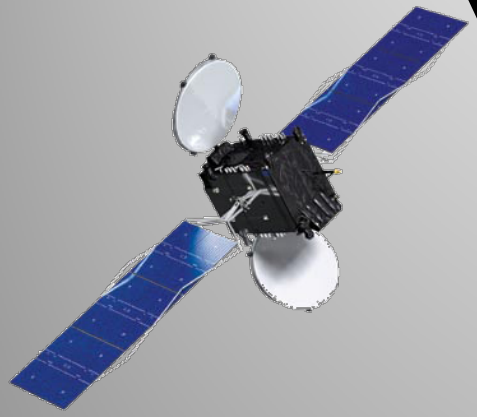
Radyne Comstream
Satellite Modem
DMD-15


1:2 REDUNDANT SYSTEM CONTROLLER
RSC-1200
FAULTS
CONTROLLER
PS 1
PS 2
RCP
INPUTS
OUTPUTS
POL 1
POL 2
UNIT 1
UNIT 2
UNIT 3
CAL
CONTROLS
LOCAL
REMOTE
REMOTE PANEL LOCKOUT
AUTO
MANUAL
Redundant System Controller
Vertex RSI
DIGITAL TRACKING RECEIVER
1986.485 MHz
FREQUENCY
ATTENUATION
POL SELECT
Digital Tracking Receiver
GENERAL DYNAMICS
SATCOM Technologies
MODEL 7200 ANTENNA CONTROL UNIT
0.0 dB
Current Pos
azimuth
elevation
polarization
217.59
51.38
72.0
DRIVE ENABLE
Antenna Control System
C1 UPC

What you need

Dish + LNB + power injector + USRP + GNU Radio

(set-top box with LNB-thru)



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

Subtract 11.3 GHz from downlink frequency: 950 - 1450 MHz

Ku Band High Power TM Transmitters

Applications

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

Main features

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

Technologies

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

Background

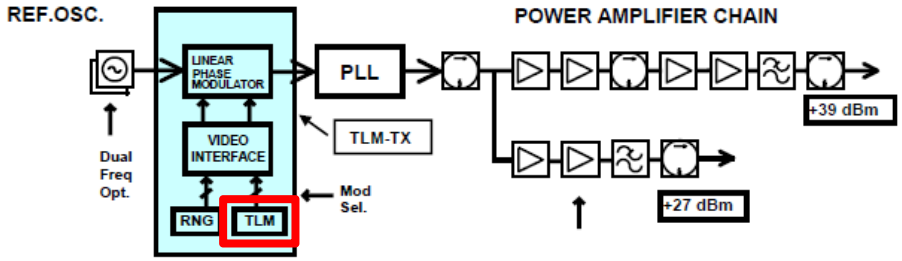
- AMC 14 - AMC 15 - AMC 16
- BSAT 2 A - BSAT 2 B
- BSAT 2 C
- BSAT3A
- ECHOSTAR 10
- ECHOSTAR 7
- GE 2A (NIMIQ2)
- HORIZON 2
- JCSAT 10
- JCSAT 11
- JCSAT 9
- NEWSKIES 6
- NEWSKIES 7
- OPTUS D1
- OPTUS D2
- Panamsat 11
- RAINBOW
- Thor2

Technical Description

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

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

Ku Band High Power Telemetry Transmitter Block Diagram



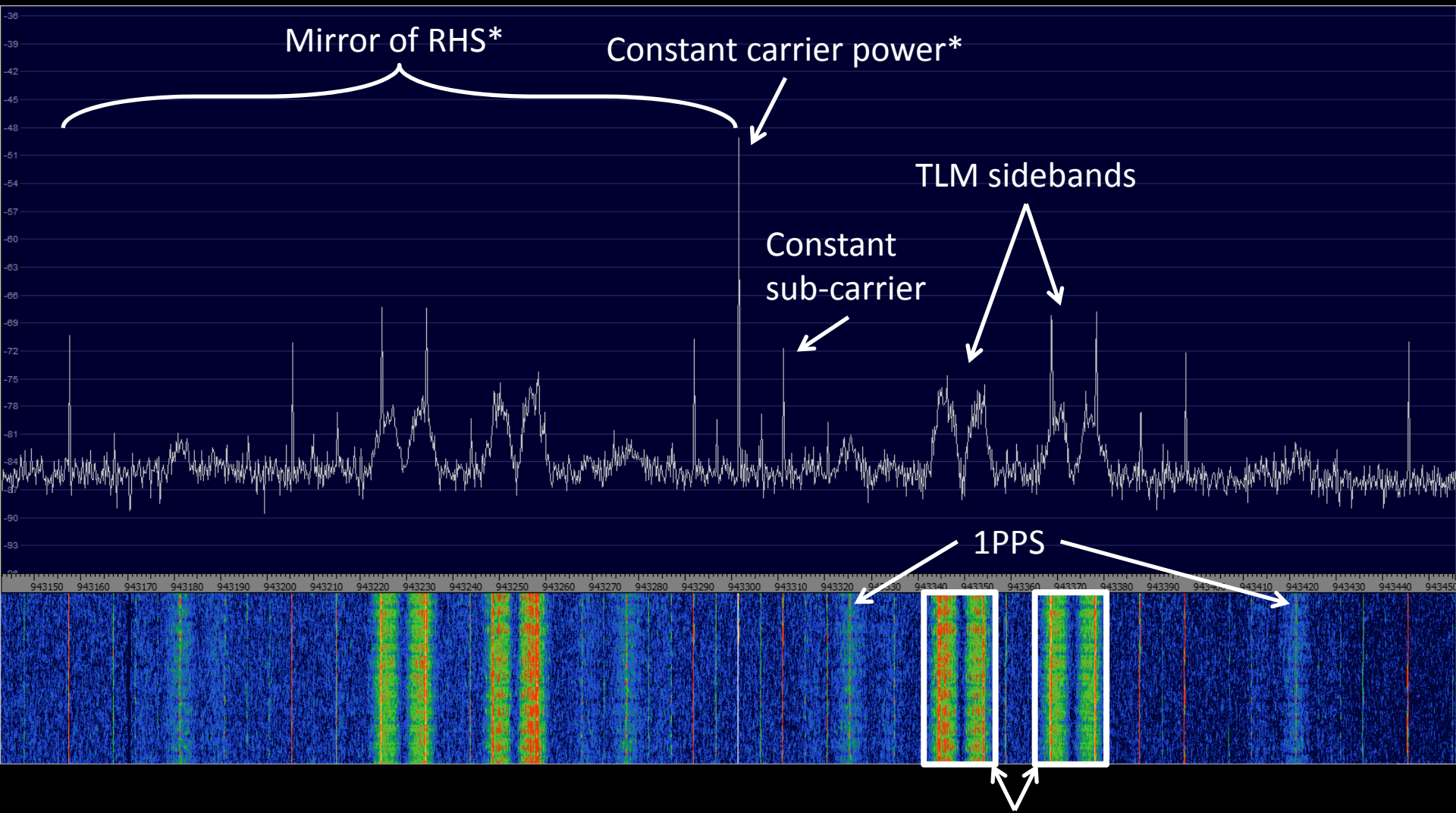
Main Performances

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

Mass, Dimensions and Consumption

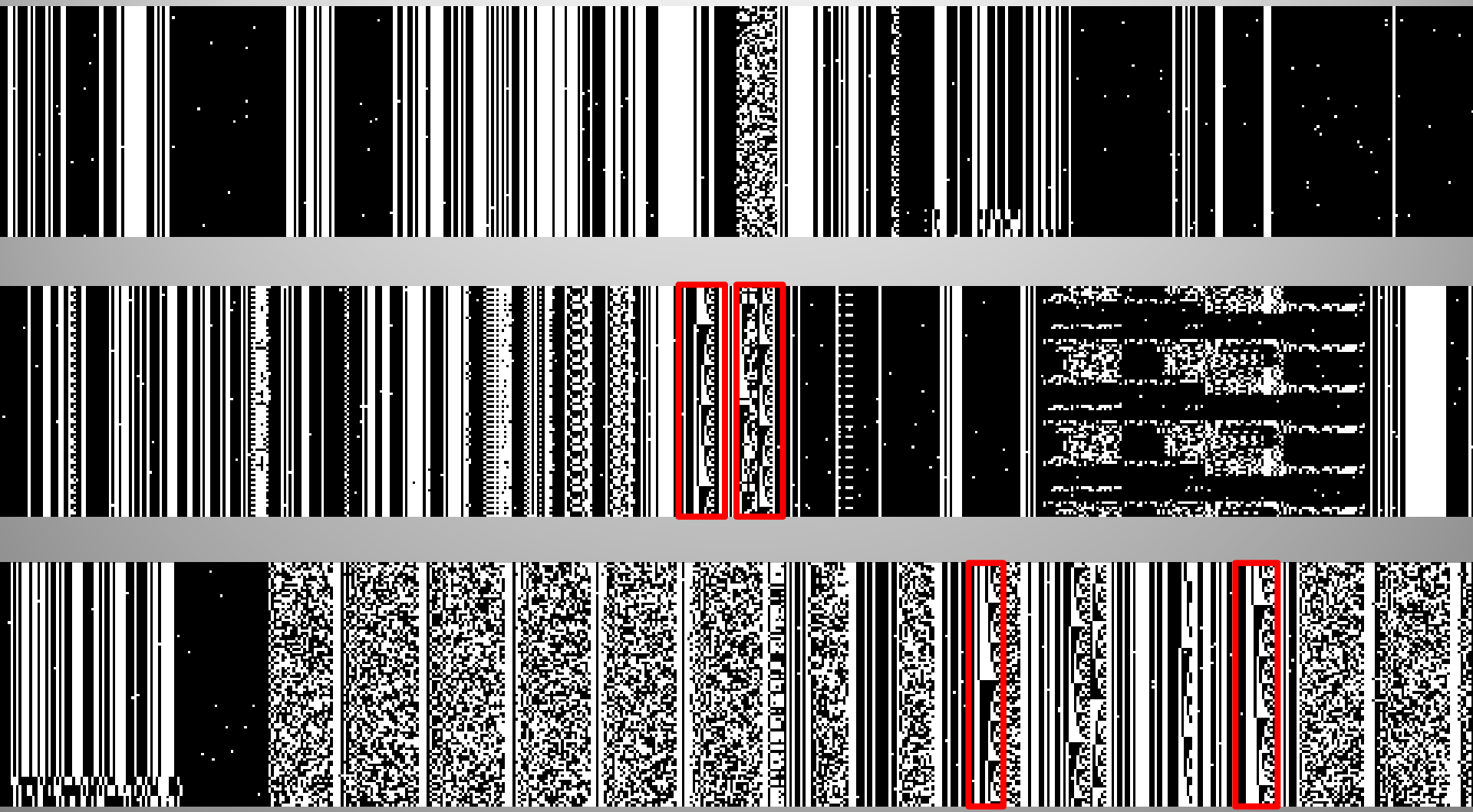
DC Power Consumption	High power mode Low power mode	<55W <18W (Dual Power Opt)
Mass Properties	< 2 kg	
Outline Dimensions	250 x 130 x 80 mm	

D1 TLM1: 12243.25 MHz



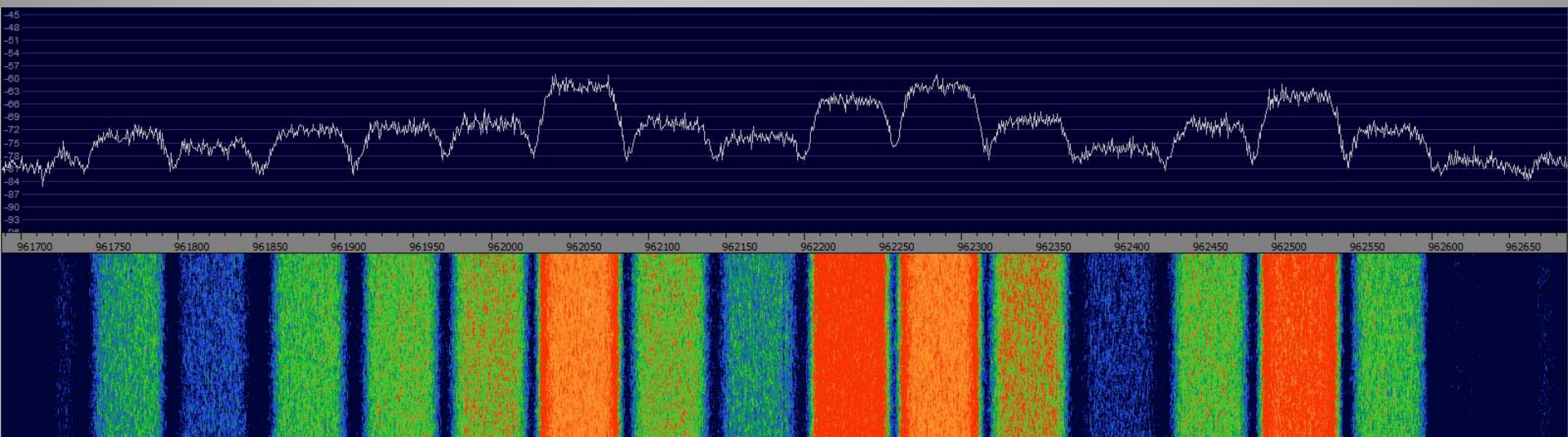
Beacon with **P**hase **M**odulation* (PM): 1PPS and two telemetry streams (sidebands)

Visualisation

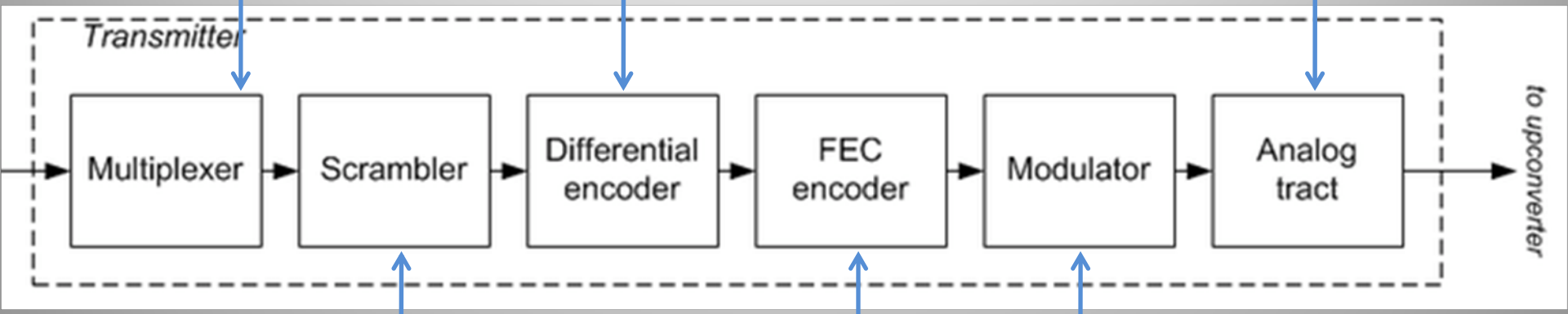


Data Streams

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



Modulation: pick your parameters

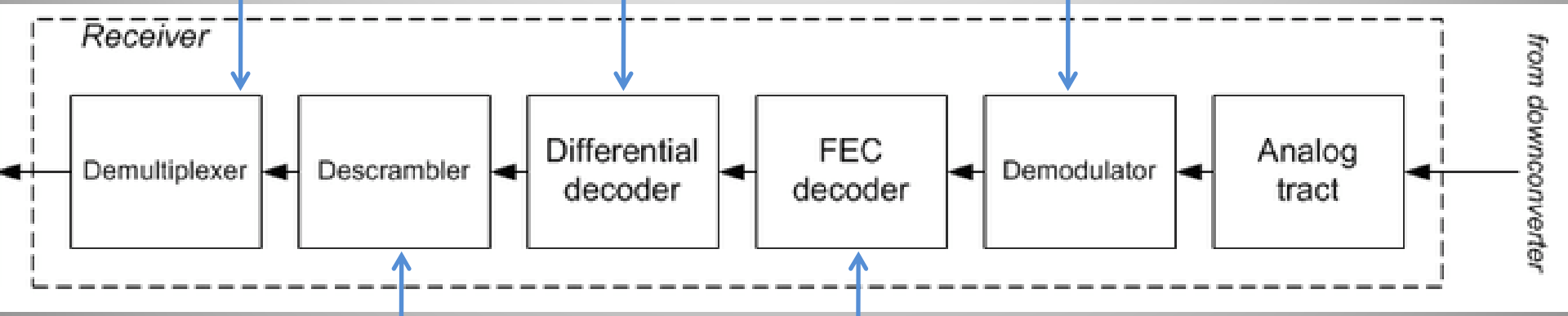


Demodulation: easy when you know

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?

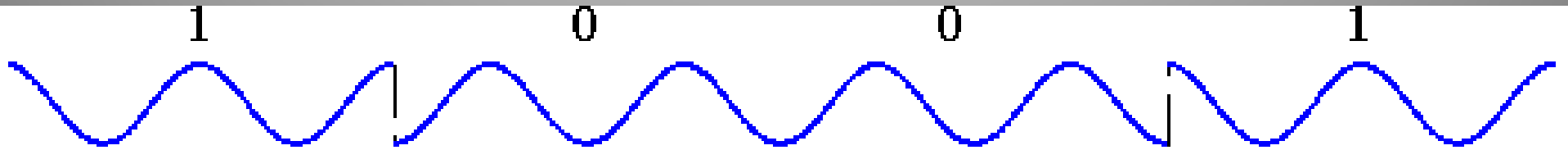
Which FEC(s) is used?
Is it a concatenated code?
What is the code rate?
What is the block size?
How is it synchronised?

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!

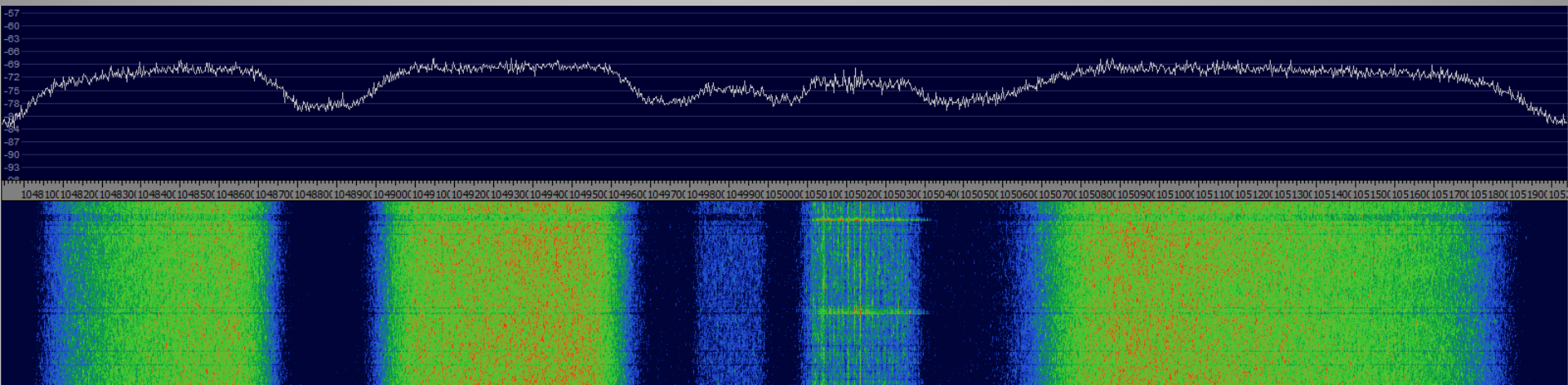
Aside: PSK, Symbols & Bits

- 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…

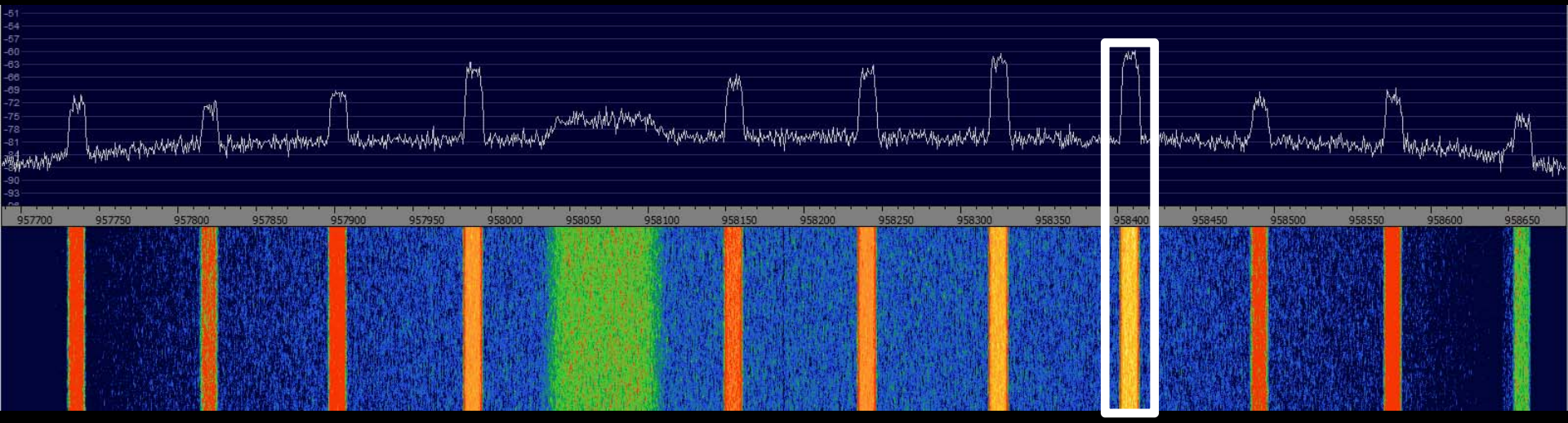


Determining modulation & rate

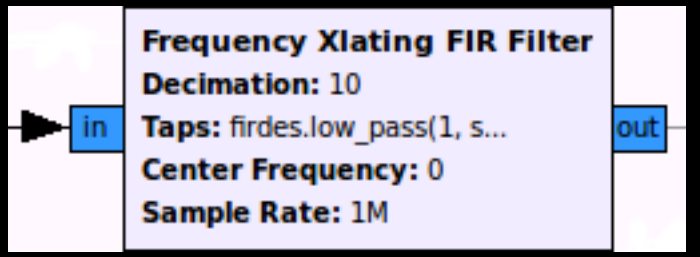
- Assuming PSK, easy to determine:
  - Modulation order: multiply the signal by itself
  - Symbol rate: multiply the signal by a lagged version of itself (cyclostationary analysis)
- Only a few GR blocks required do this



Let’s try one…

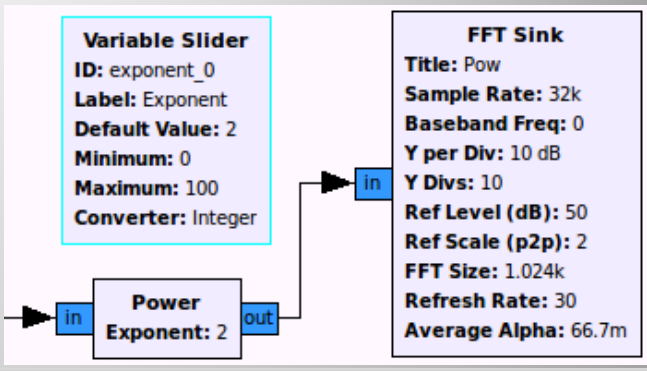


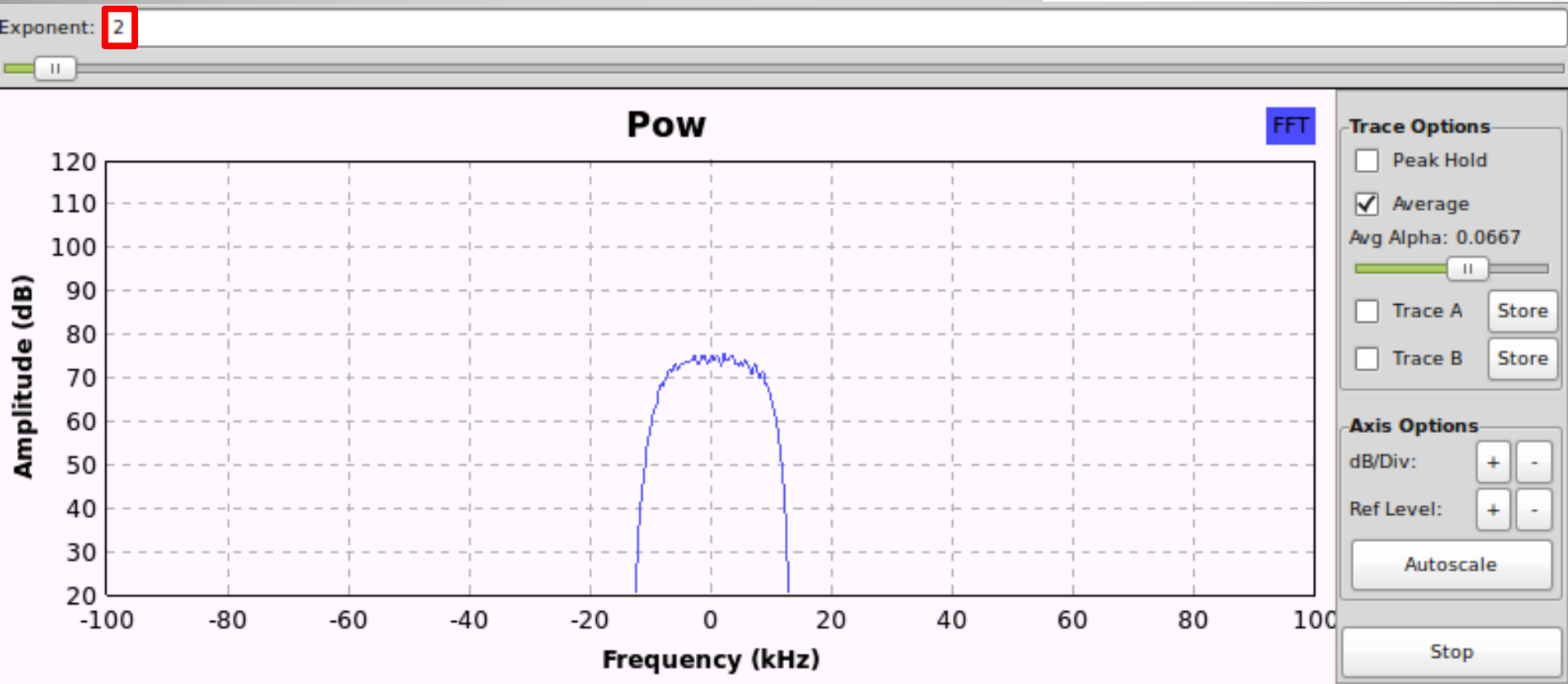
- Feed entire baseband spectrum into GR
- Perform ‘channel selection’ to isolate stream of interest (create new baseband centred on stream)



Determine PSK order

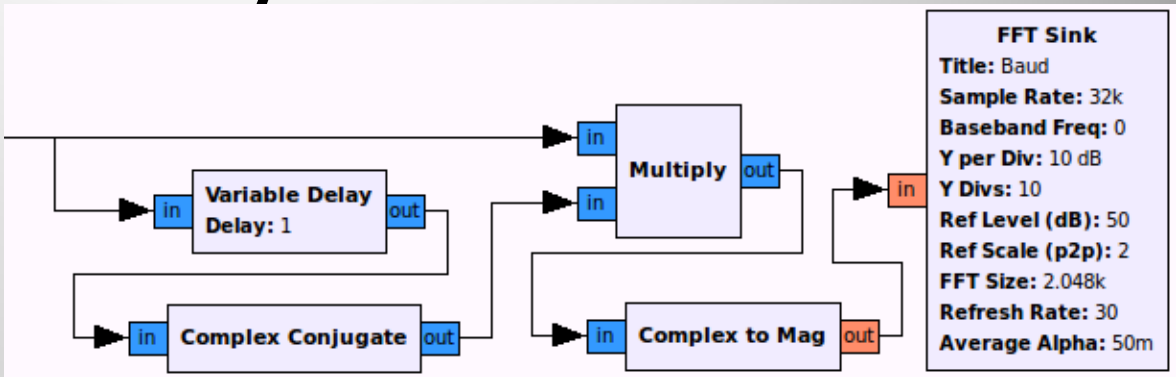
- Start at 2 and go up
- Stop when spike appears



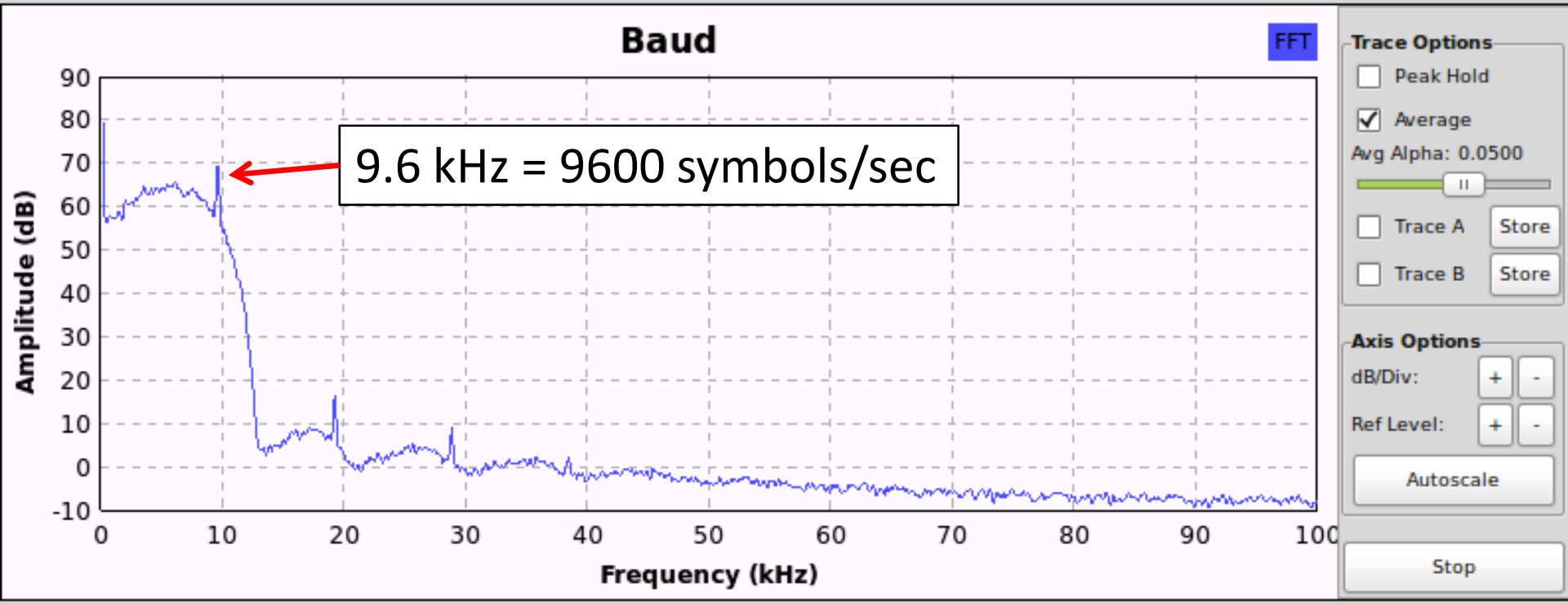


Determine Symbol Rate

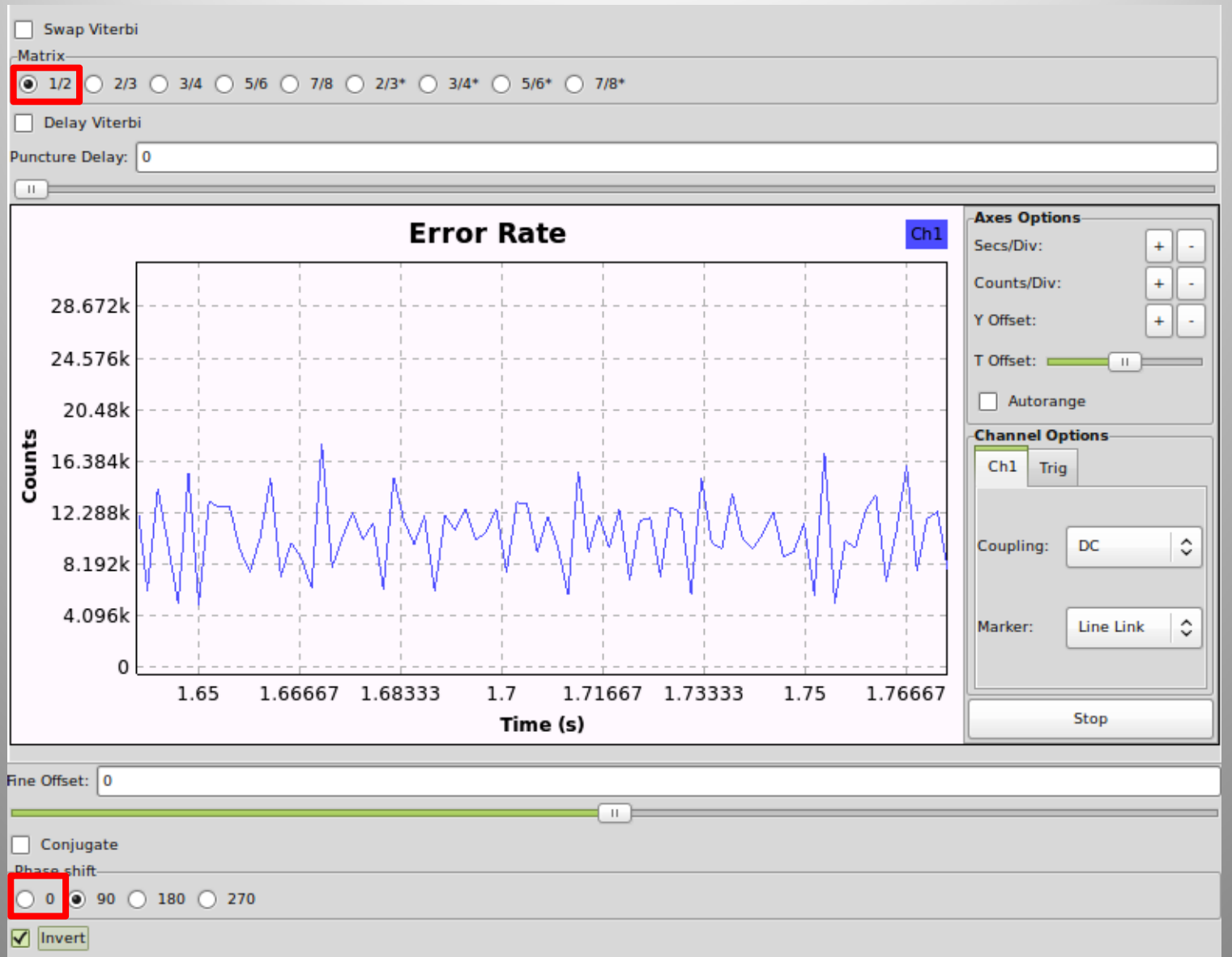
- Find first peak

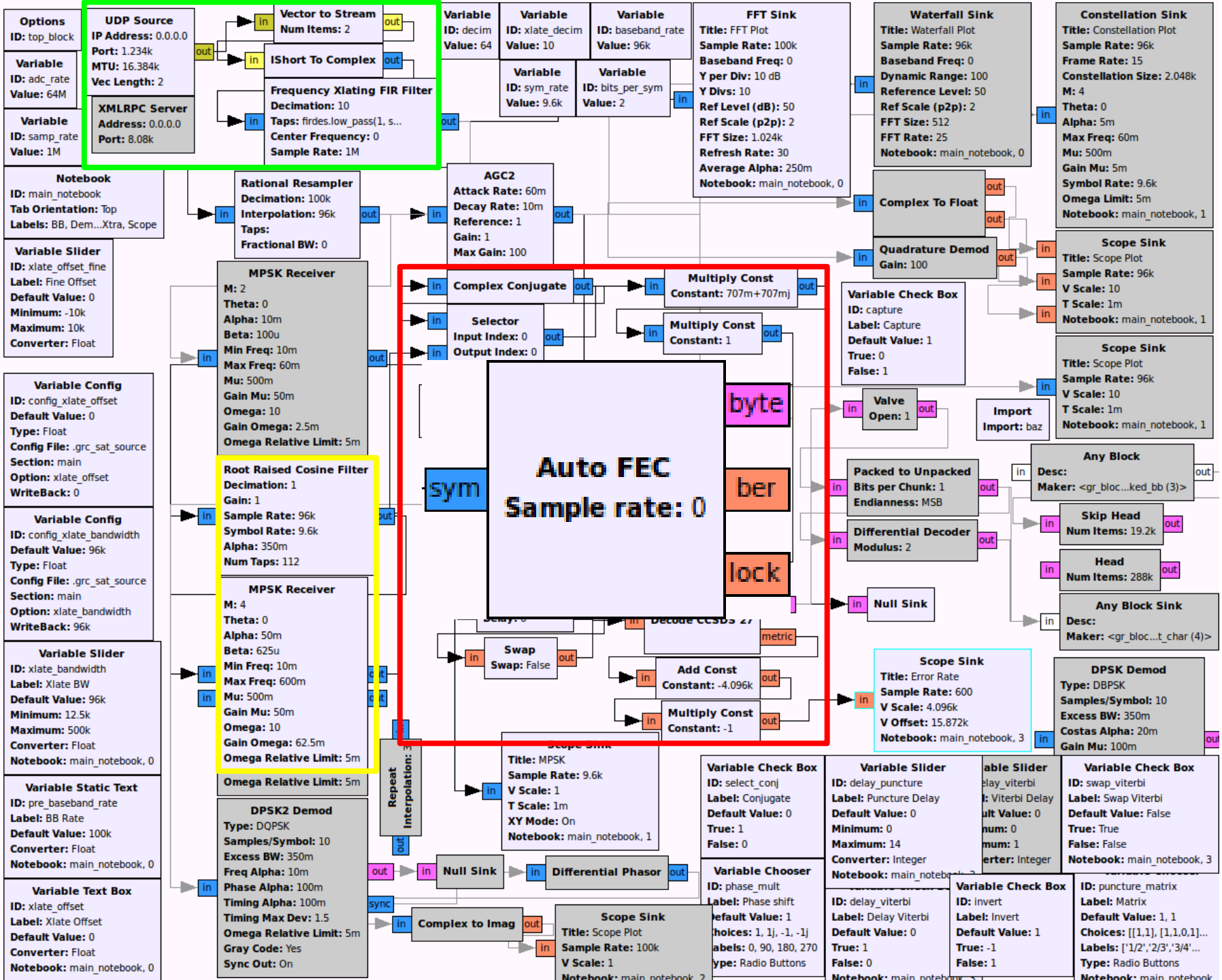


Nominal samples per symbol: 2



Try synchronisation & FEC




Options
ID: top_block
UDP Source
IP Address: 0.0.0.0
Port: 1.234k
MTU: 16.384k
Vec Length: 2
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
XMLRPC Server
Address: 0.0.0.0
Port: 8.08k
Variable
ID: adc_rate
Value: 64M
Variable
ID: samp_rate
Value: 1M
Notebook
ID: main_notebook
Tab Orientation: Top
Labels: BB, Dem...Xtra, Scope
Variable Slider
ID: xlate_offset_fine
Label: Fine Offset
Default Value: 0
Minimum: -10k
Maximum: 10k
Converter: Float
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
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
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
Root Raised Cosine Filter
Decimation: 1
Gain: 1
Sample Rate: 96k
Symbol Rate: 9.6k
Alpha: 350m
Num Taps: 112
byte
sym
Auto FEC
Sample rate: 0
ber
lock
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)>
Null Sink
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
Swap
Swap: False
Add Const
Constant: -4.096k
Multiply Const
Constant: -1
metric
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 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
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
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

Demodulated & error-corrected

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

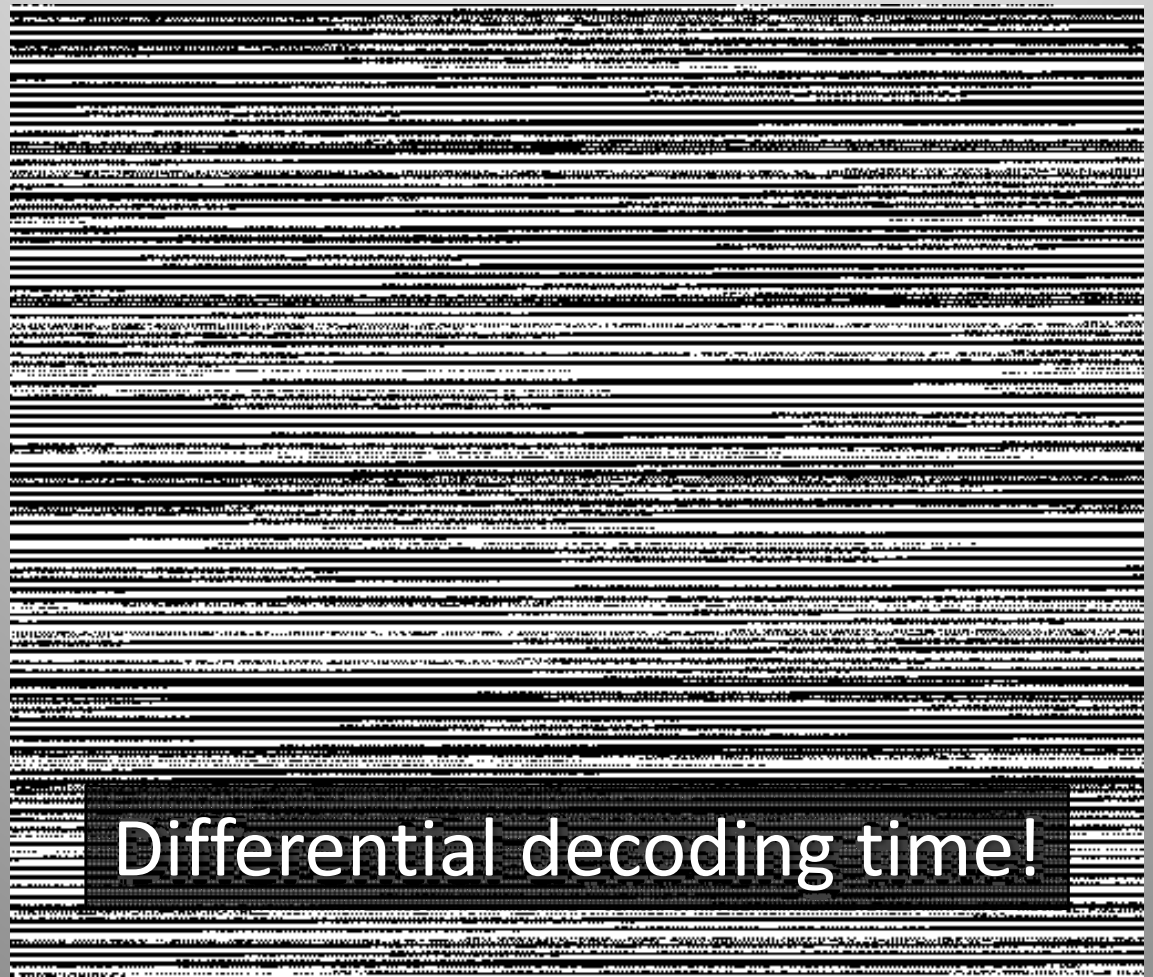
- Visualise data: look for additional clues
  - Differential encoding
  - Scrambling
  - Structure

Visualisation

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

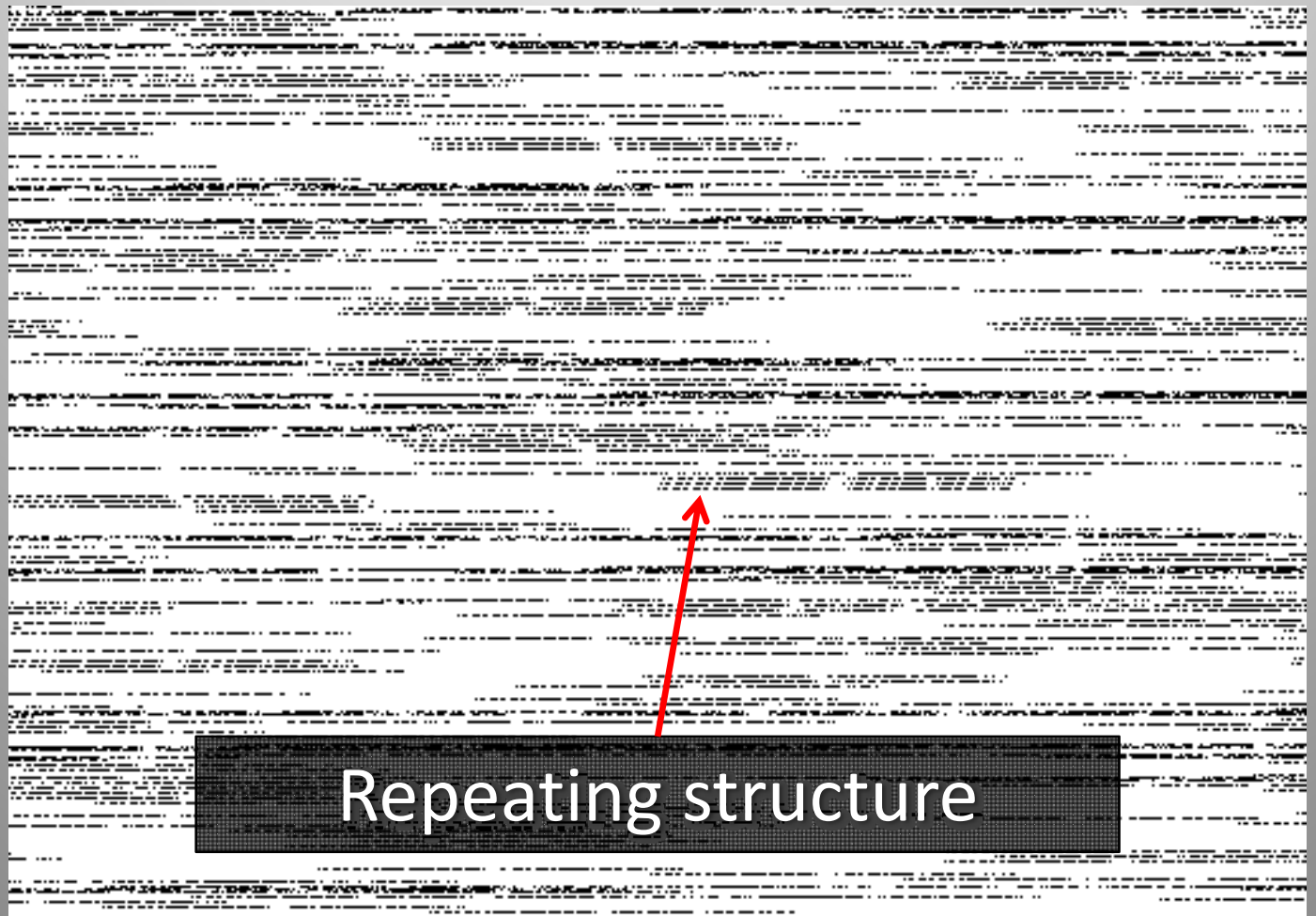
De-scrambled

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



Diff. decoded & de-scrambled

- Structured, asynchronous packets of data!



Pattern Search

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

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

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

41 bits #0002-0002[+0000, /0000]: 00000001000011001001110000100111110000000000 (3e4393080)
41 bits #0003-0003[+0000, /0000]: 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]: 00100000011111111010010111000010111111 (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]: 10110100101111011010000001000110000000 (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)
```

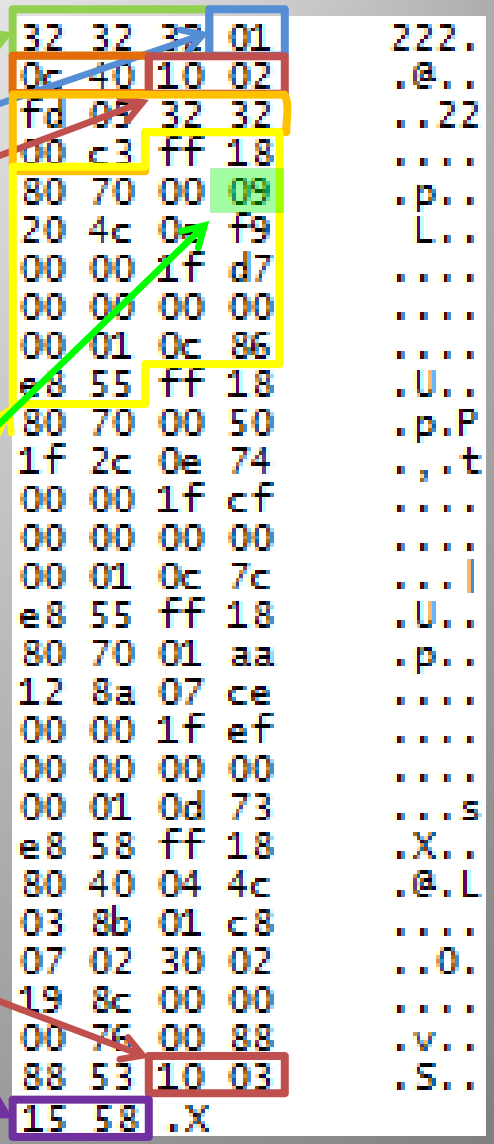
- Search for repeating strings of bits
- Try to find frame header
- Clue: sudden increase in # of occurrences

```
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]: 10110100101111011010000001000110000000 (6205bd2d)
```

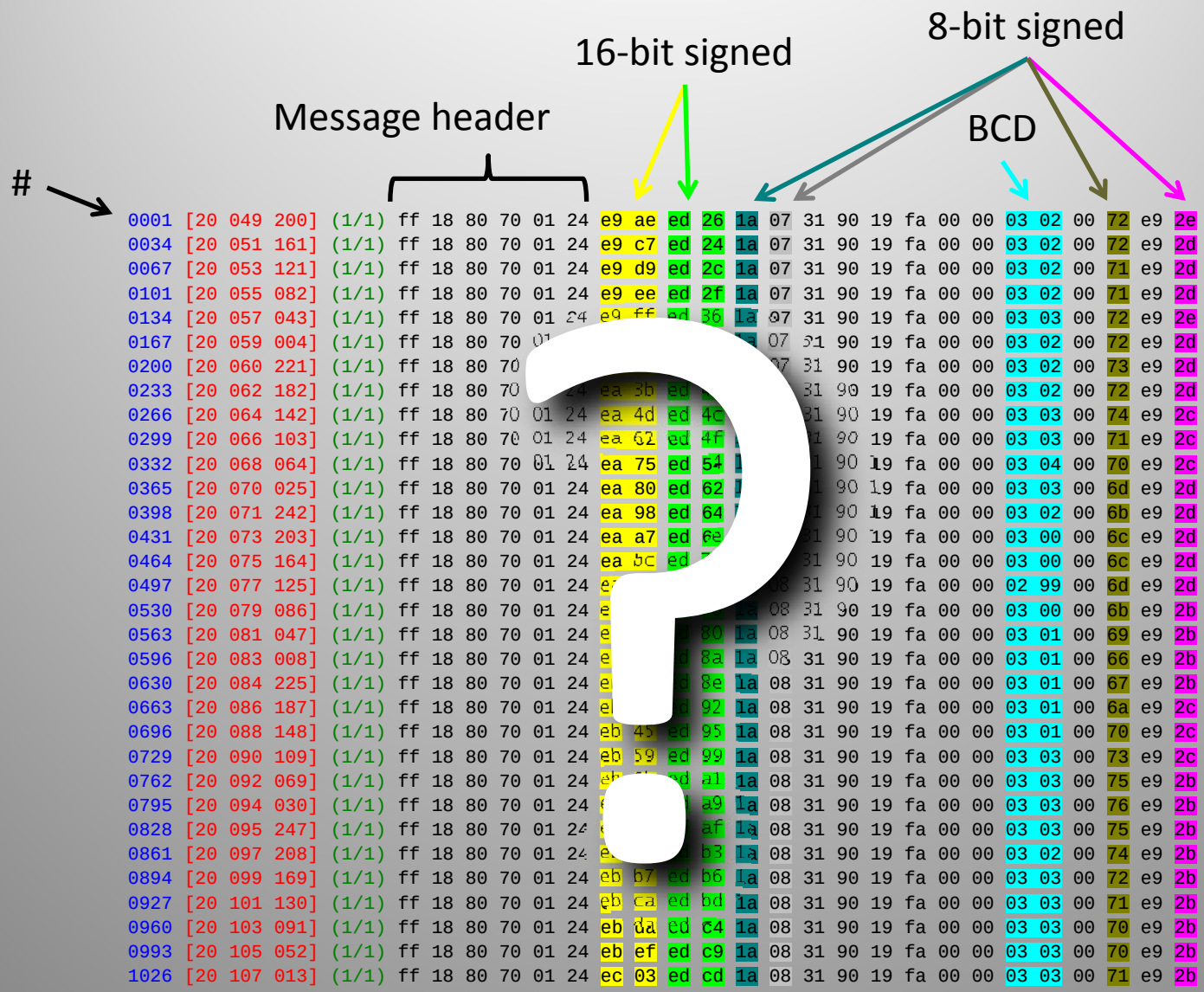
Preceding 1s are just part of ‘idle’ stream when no data is being sent

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



Gedanken: TX

DO NOT TRY THIS AT…

WHEREVER!

Gedanken: Pagers

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

Gedanken: Mode S

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

Gedanken: ACARS

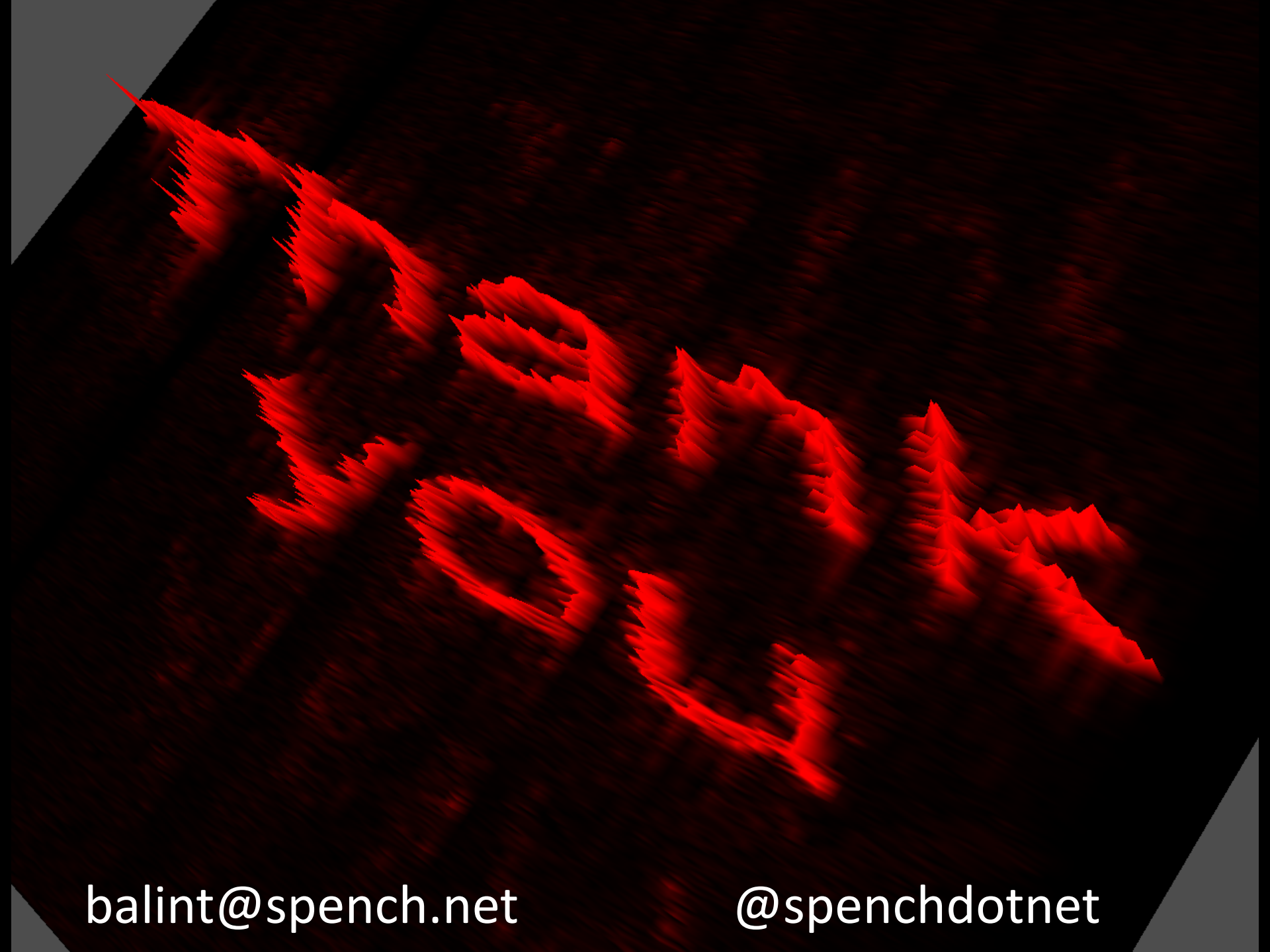
- Don’t want to fly on a particular aircraft?
  - Send a severe fault report
- Was the flight a little bumpy?
  - Send an engine performance report to RR with large vibration values
- Need to message the cockpit privately?
  - Address the message to cockpit printer #1

Gedanken: Satellite

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

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

Remember: be legal and be….


balint@spench.net
@spenchdotnet