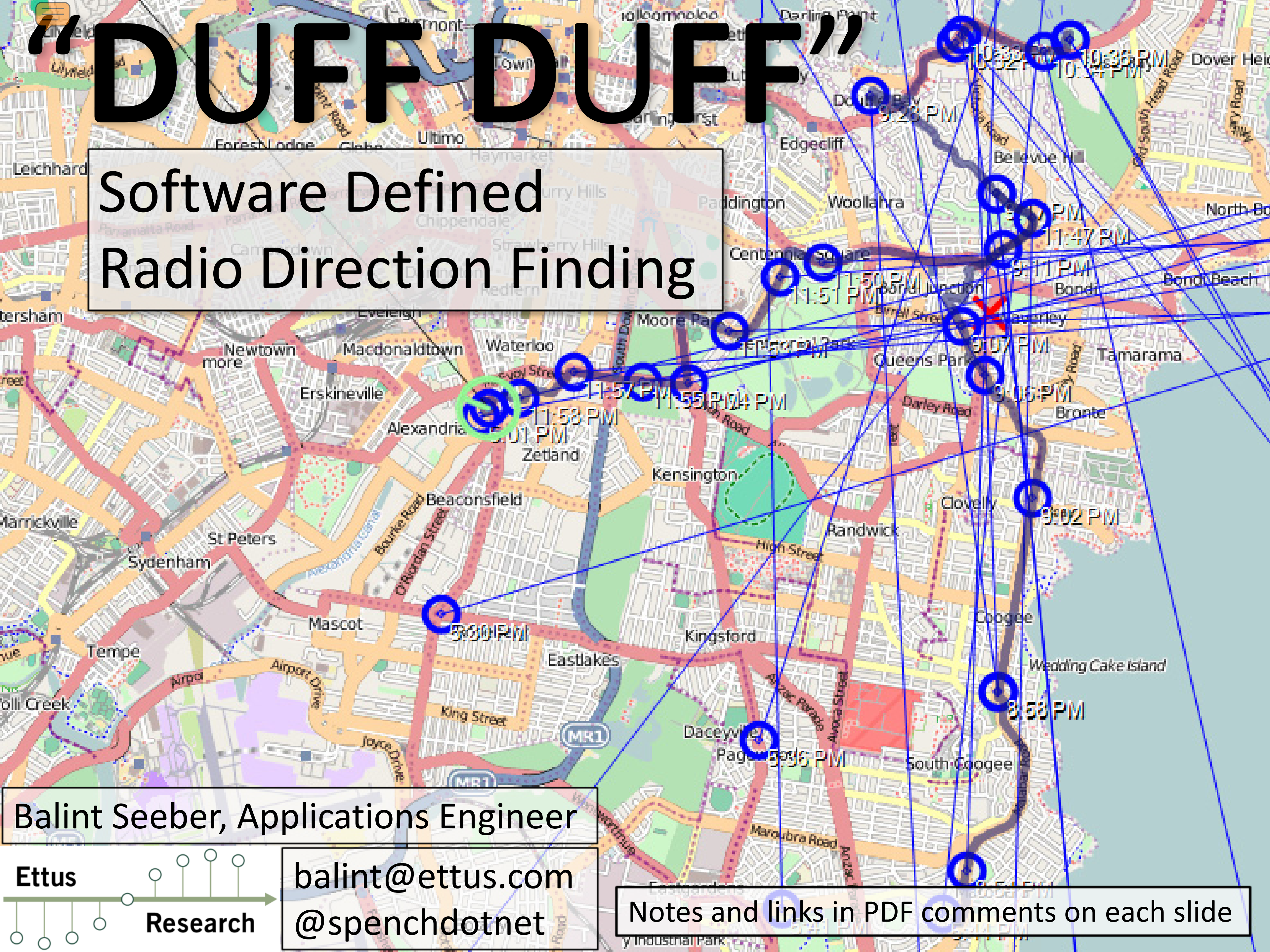
"DUFF DUFF"

Software Defined Radio Direction Finding



Balint Seeber, Applications Engineer

Ettus Research

balint@ettus.com
@spenchdotnet

Notes and links in PDF comments on each slide

DF Usage

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

Rotatable
loop antenna

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

Highly-directional Yagi antenna

Crazy-serious German HAM

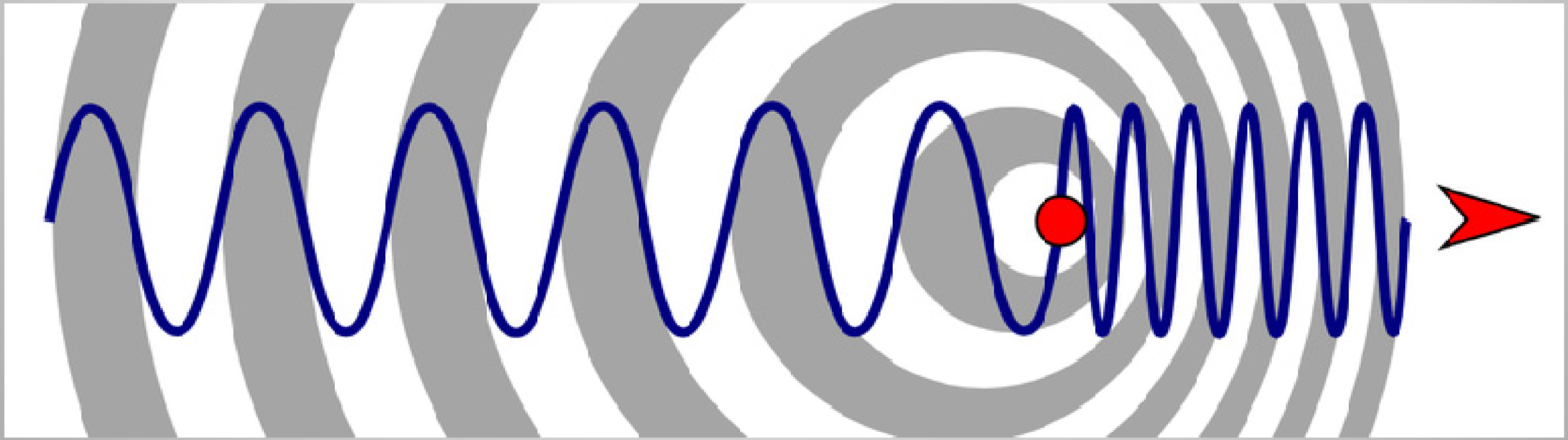
(Pseudo-) Doppler DF

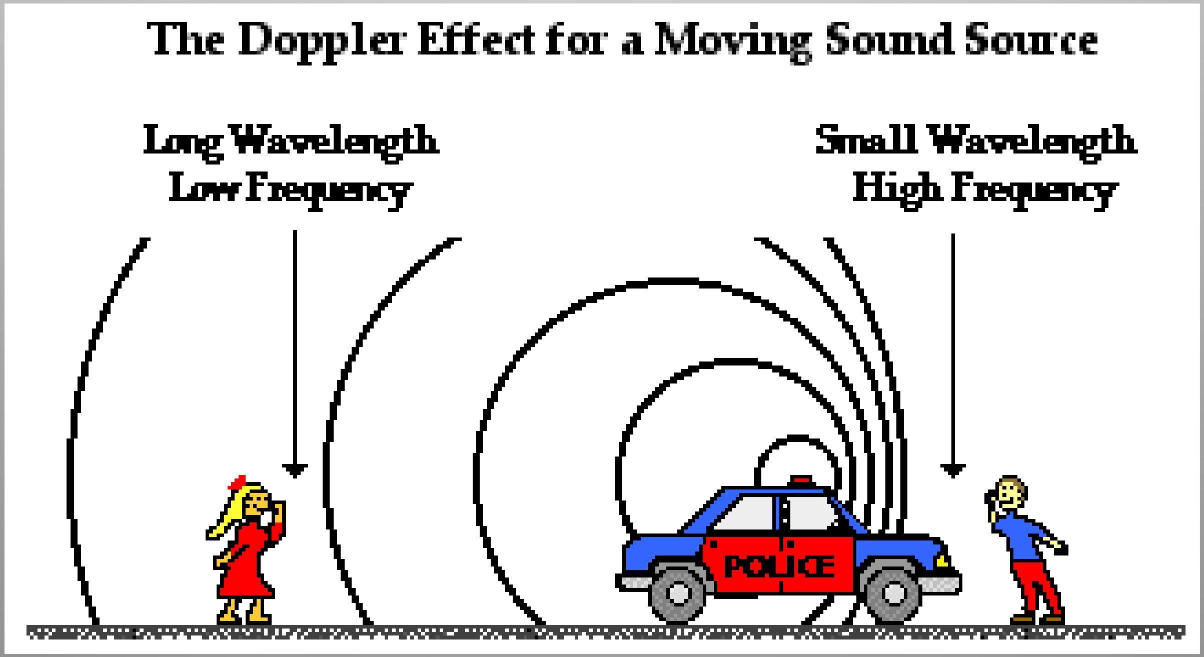
- Exploit Doppler shifting of radio waves caused by motion of an antenna

- Measure the shift in detected signal

  → Determine direction of transmission

Recap: Doppler Effect



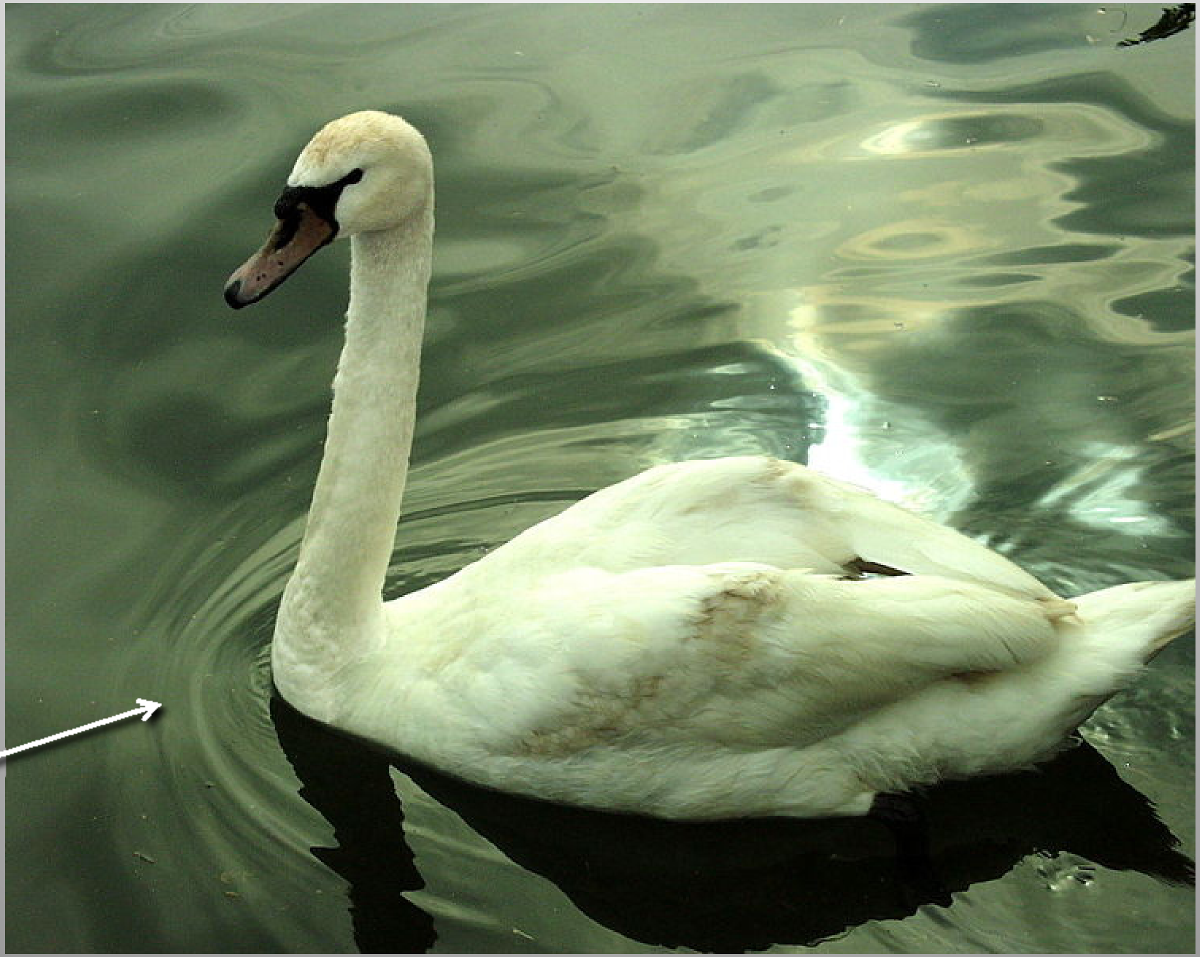


Aside: Siren Misconception

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

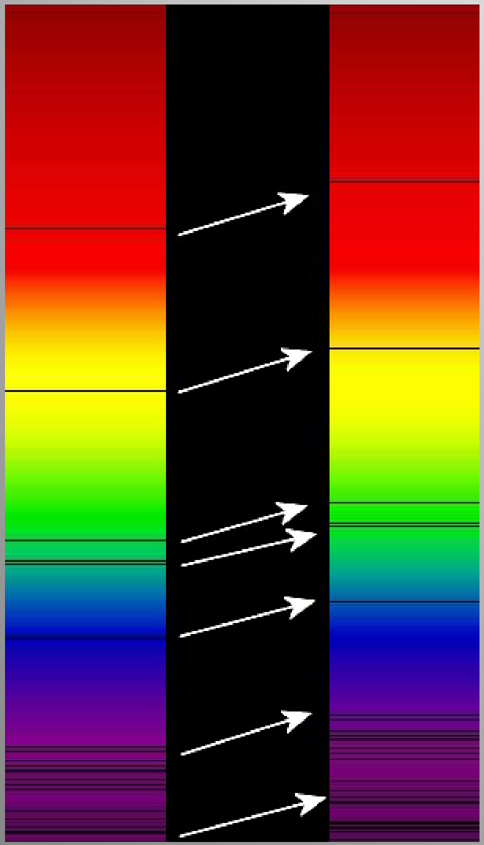
"…**Higher sound pressure levels** make for a small decrease in **perceived pitch** in low frequency sounds, and for a small increase in perceived pitch for high frequency sounds."

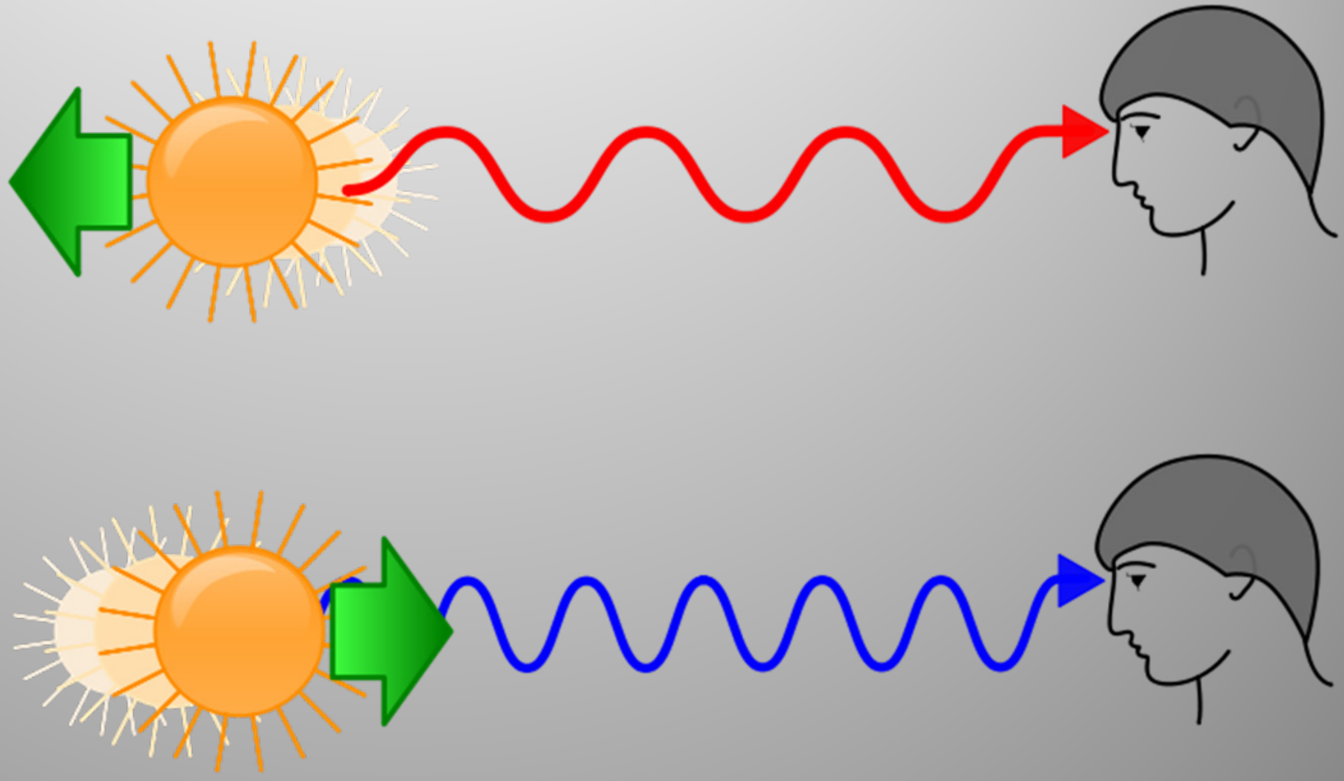
A Swan



Doppler
Effect

Cosmological Redshift

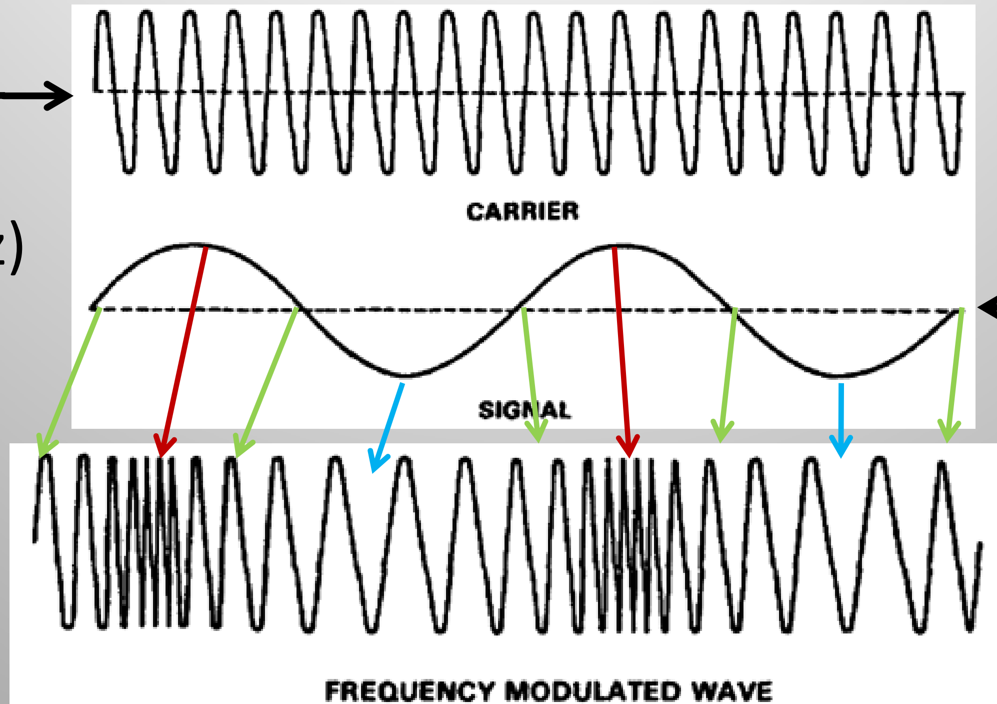




Expansion of space, not motion of radiating object!

Frequency Modulation 101

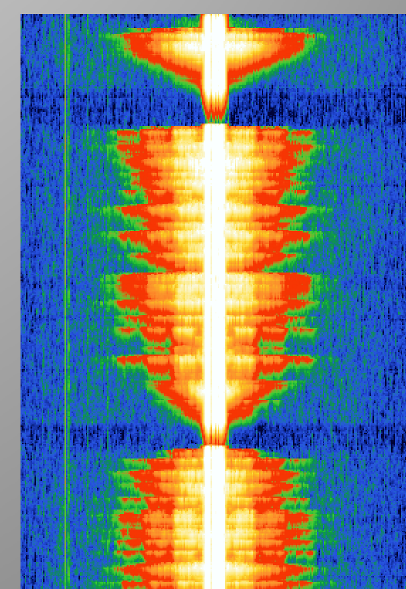
‘Main’ transmission frequency (e.g. 105.7 MHz)



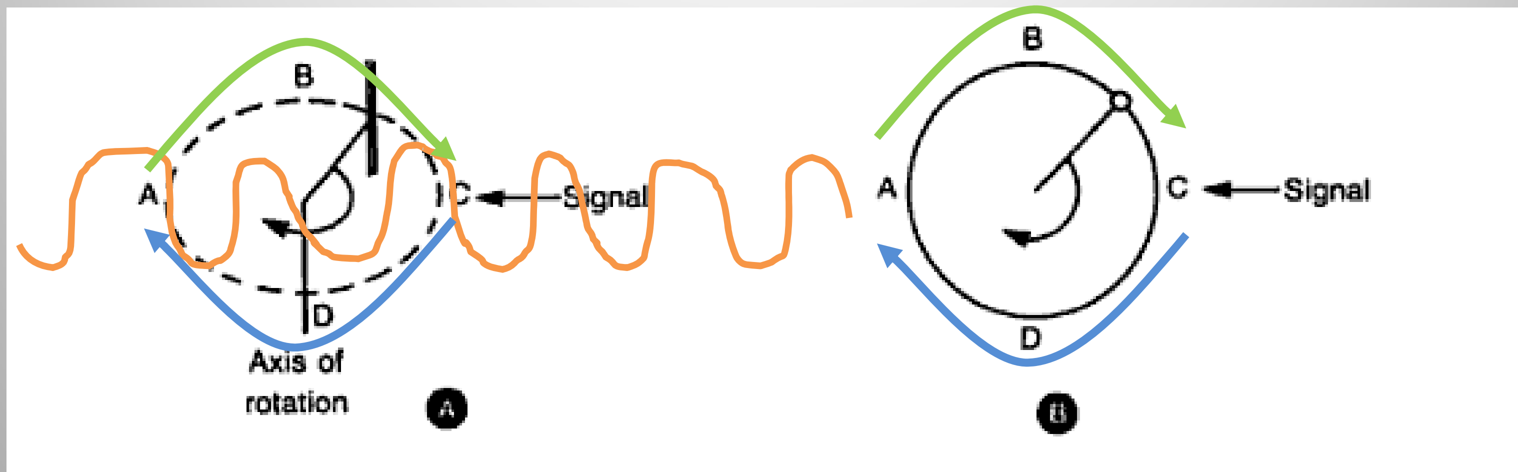
Analog or digital Information to be transmitted

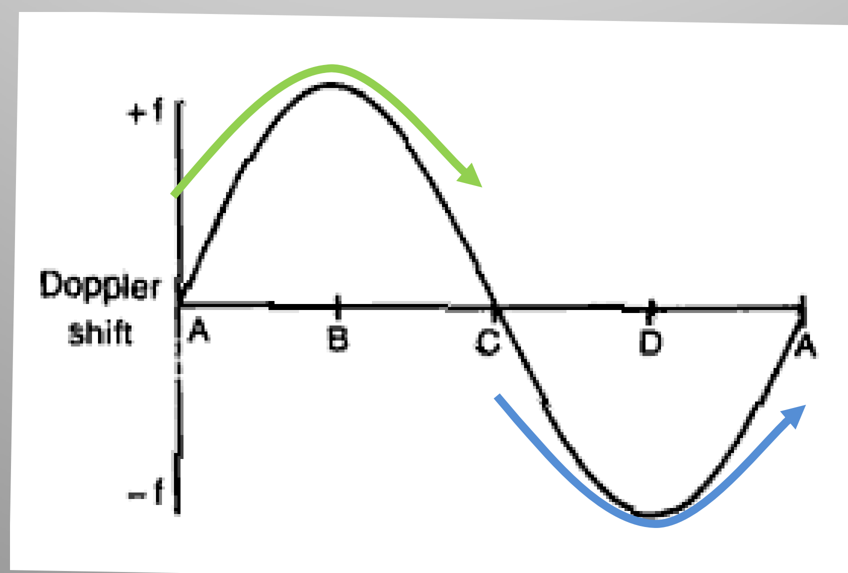
Frequency modulation changes the carrier’s frequency

→ Moves the carrier slightly left/right of its original position on frequency plot



Physically Rotated Antenna



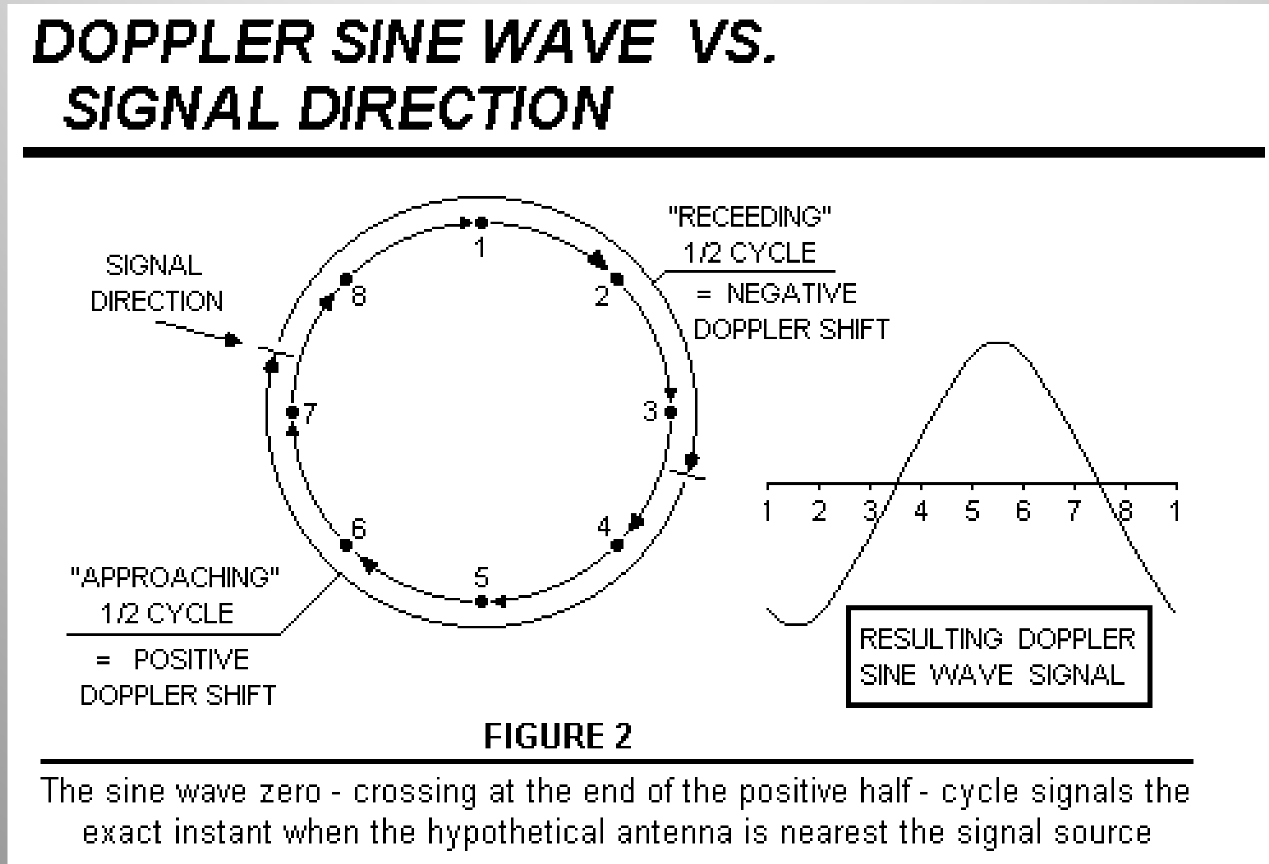


Joseph Moell, “Transmitter Hunting: Radio Direction Finding Simplified”, 1987 (McGraw-Hill)

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

PRODUCING DOPPLER SHIFT ON A RECIEVED SIGNAL USING STATIONARY ANTENNAS

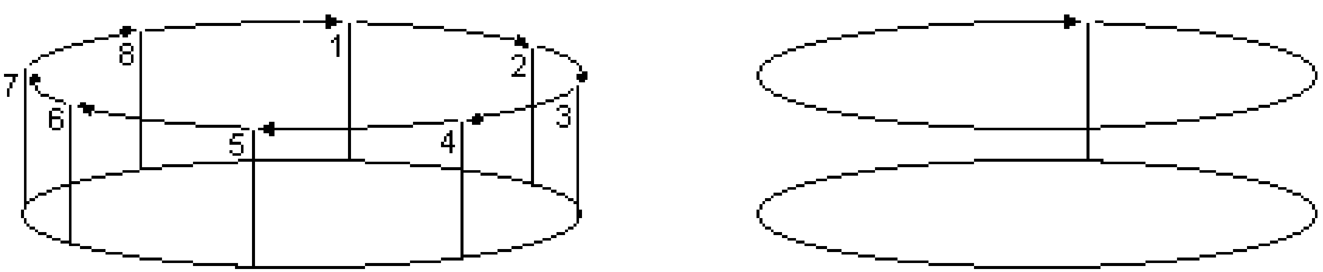
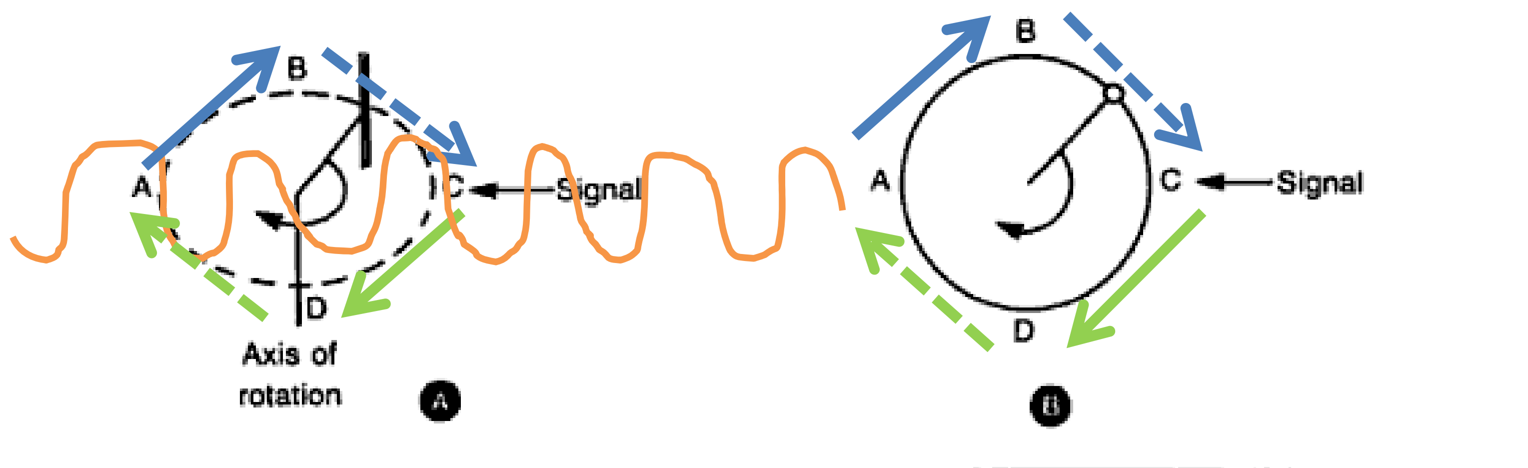
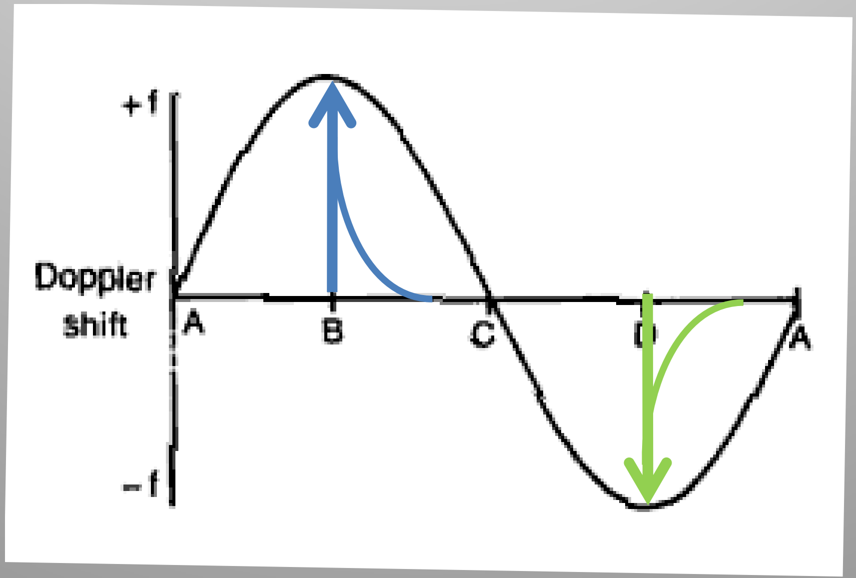


FIGURE 1

Switching a receiver between 8 stationary antennas (arranged in a circle) simulates the action of a single, *hypothetical* antenna, moving in a circle.

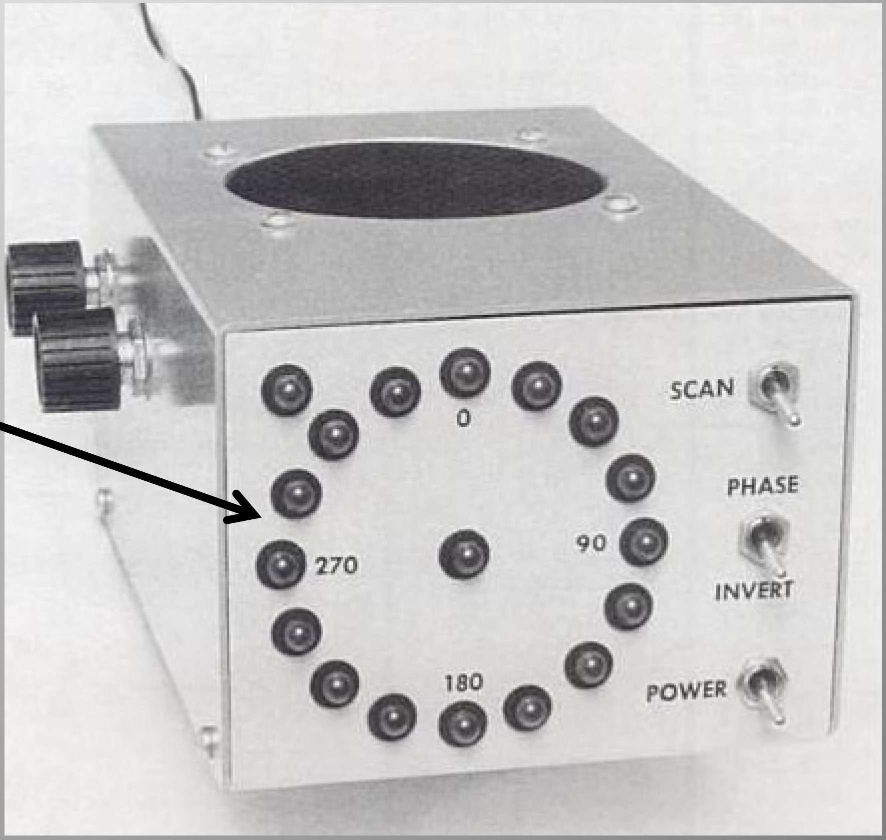
Electronically Rotated Antenna





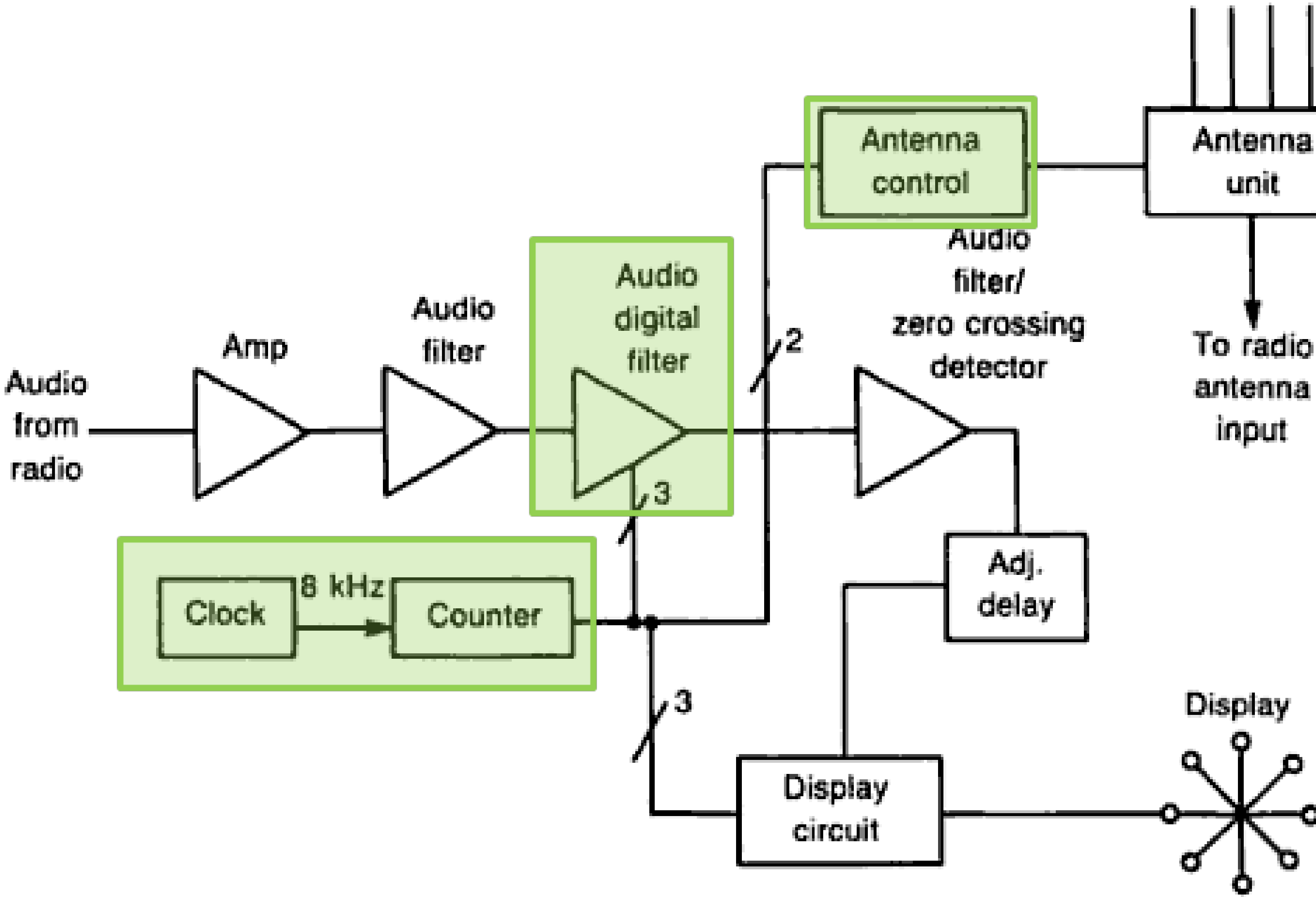
Home-made RDF

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

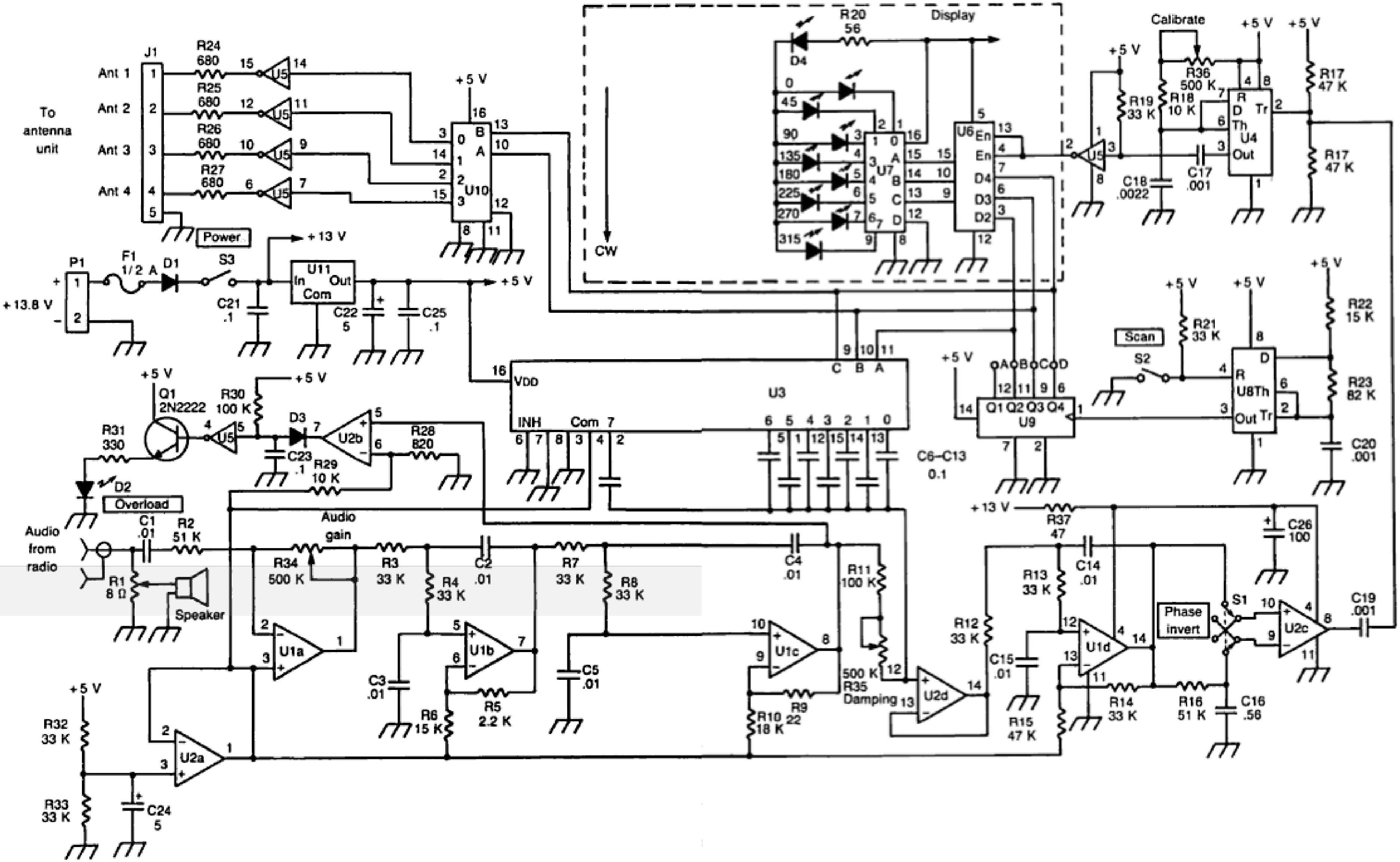


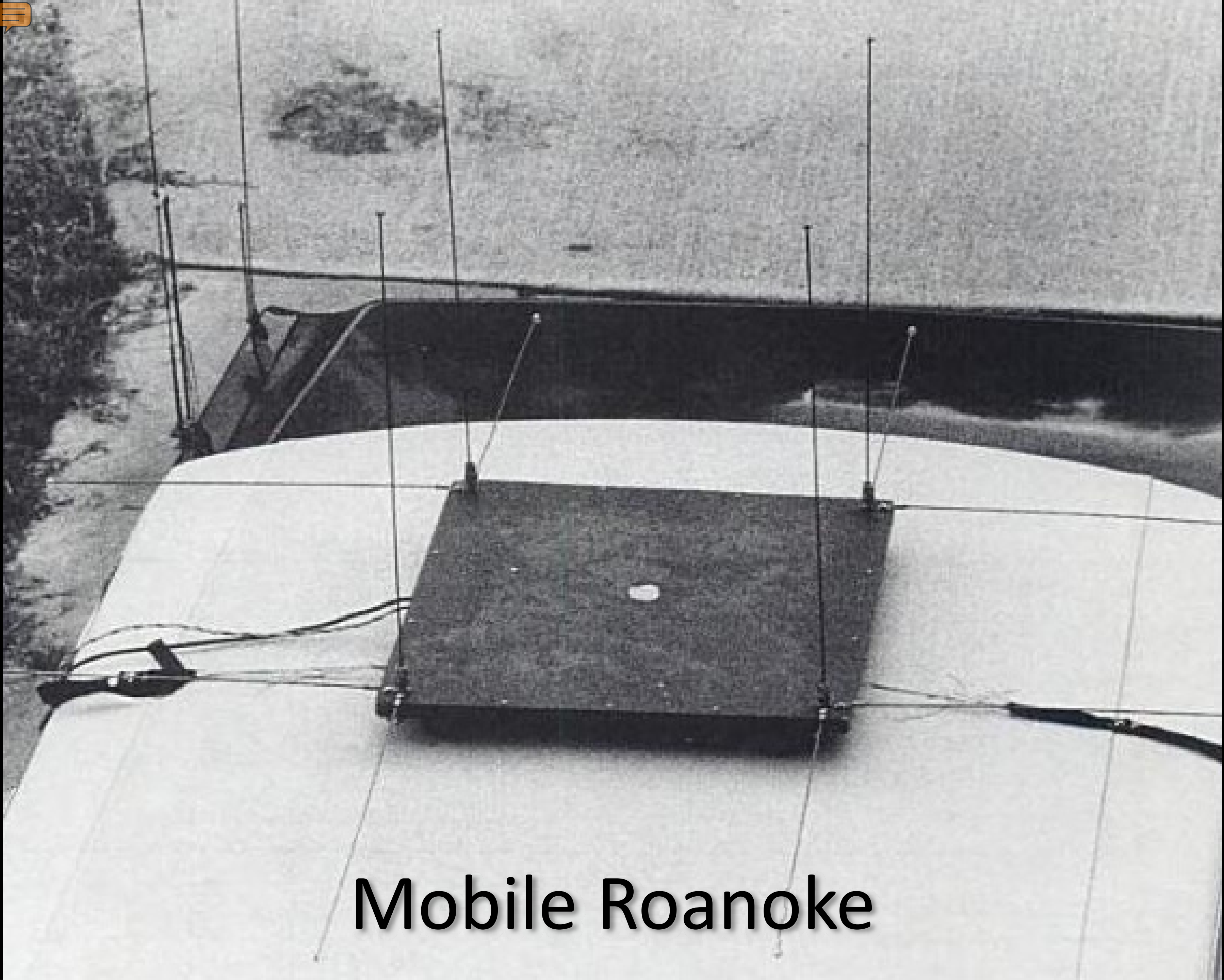
Joseph Moell,
“Transmitter Hunting:
Radio Direction Finding Simplified”,
1987 (McGraw-Hill)

Block Diagram



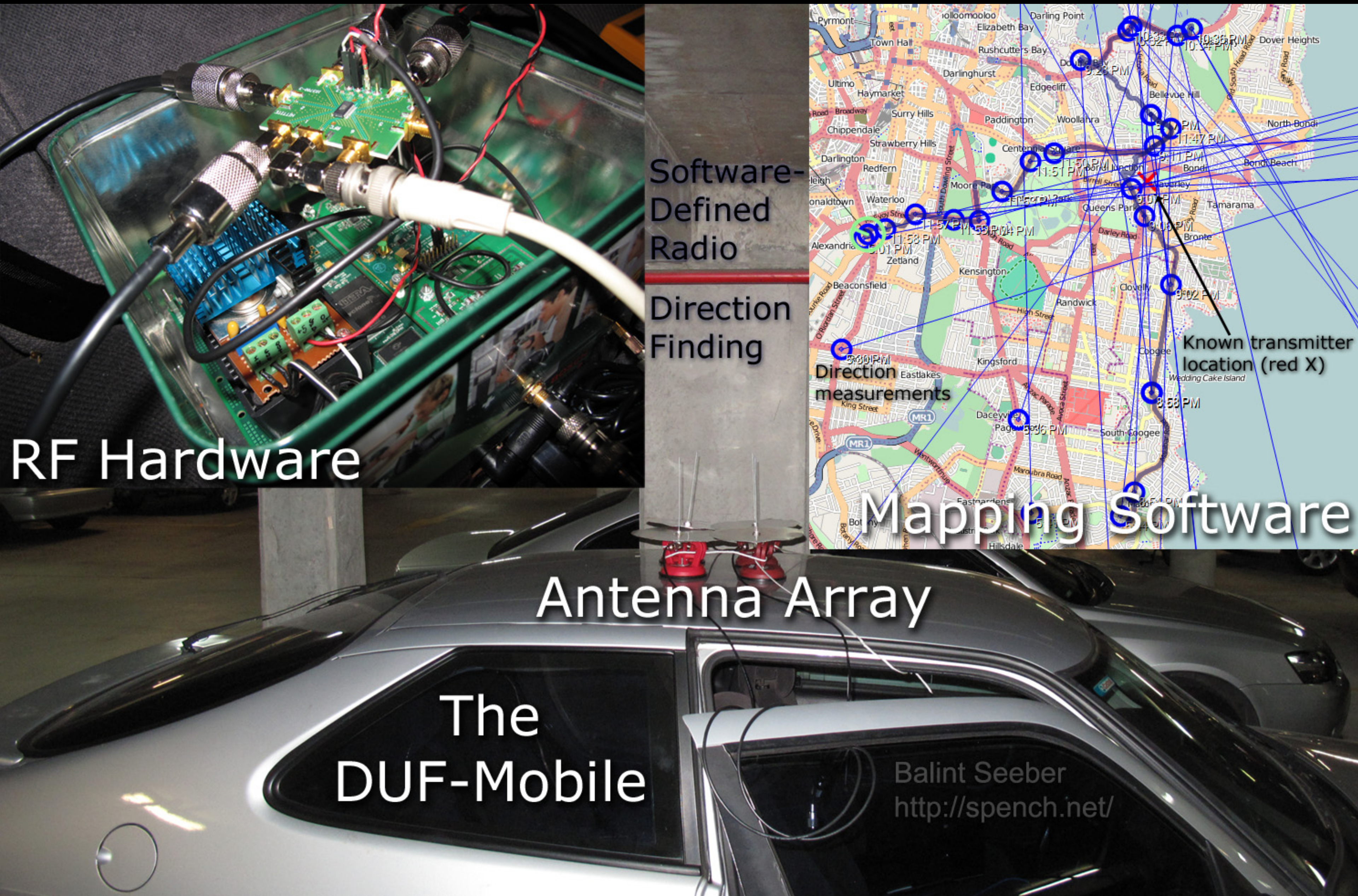
Circuit Diagram





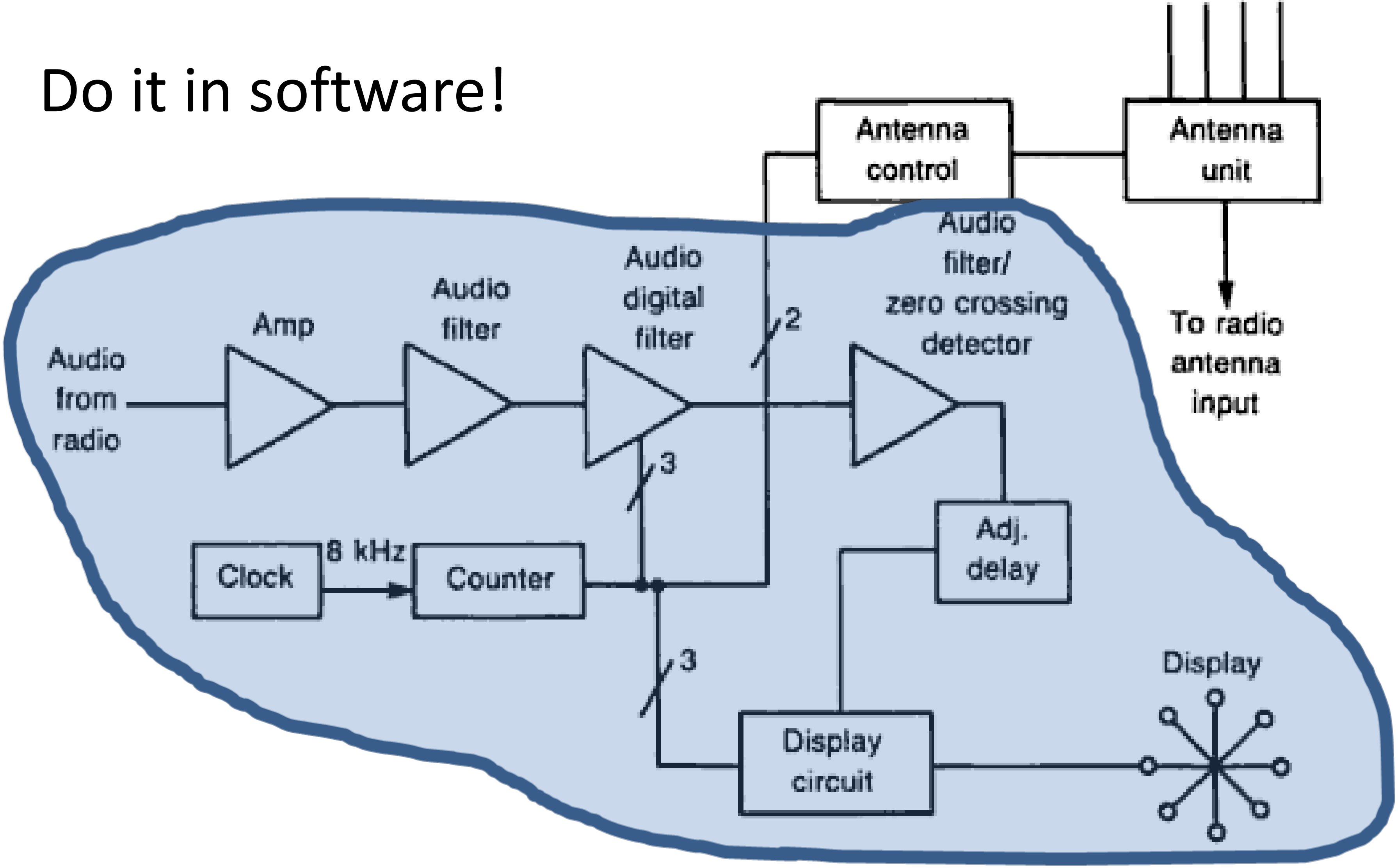
Mobile Roanoke

Time to go colour…

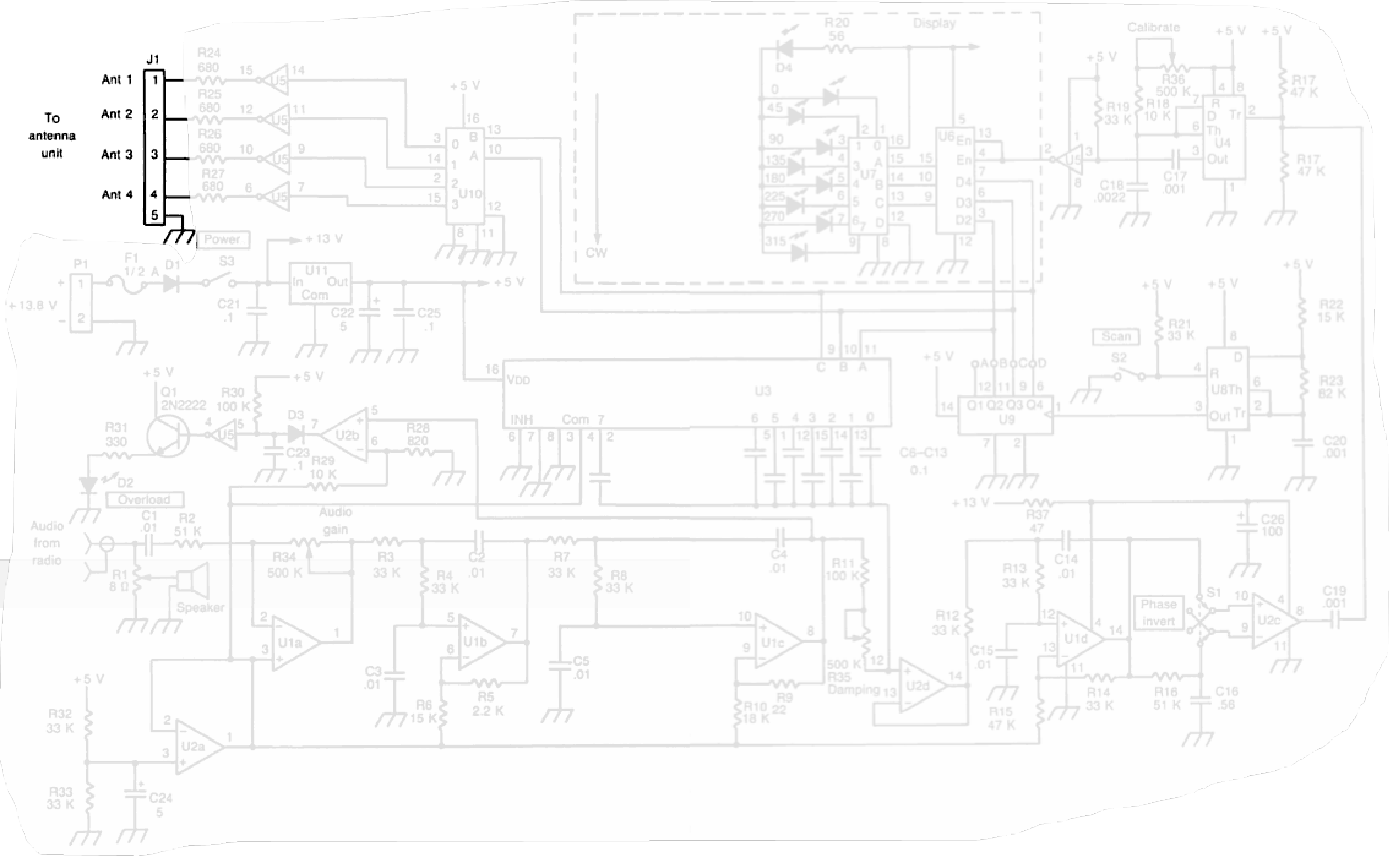


Software Defined RDF

Do it in software!

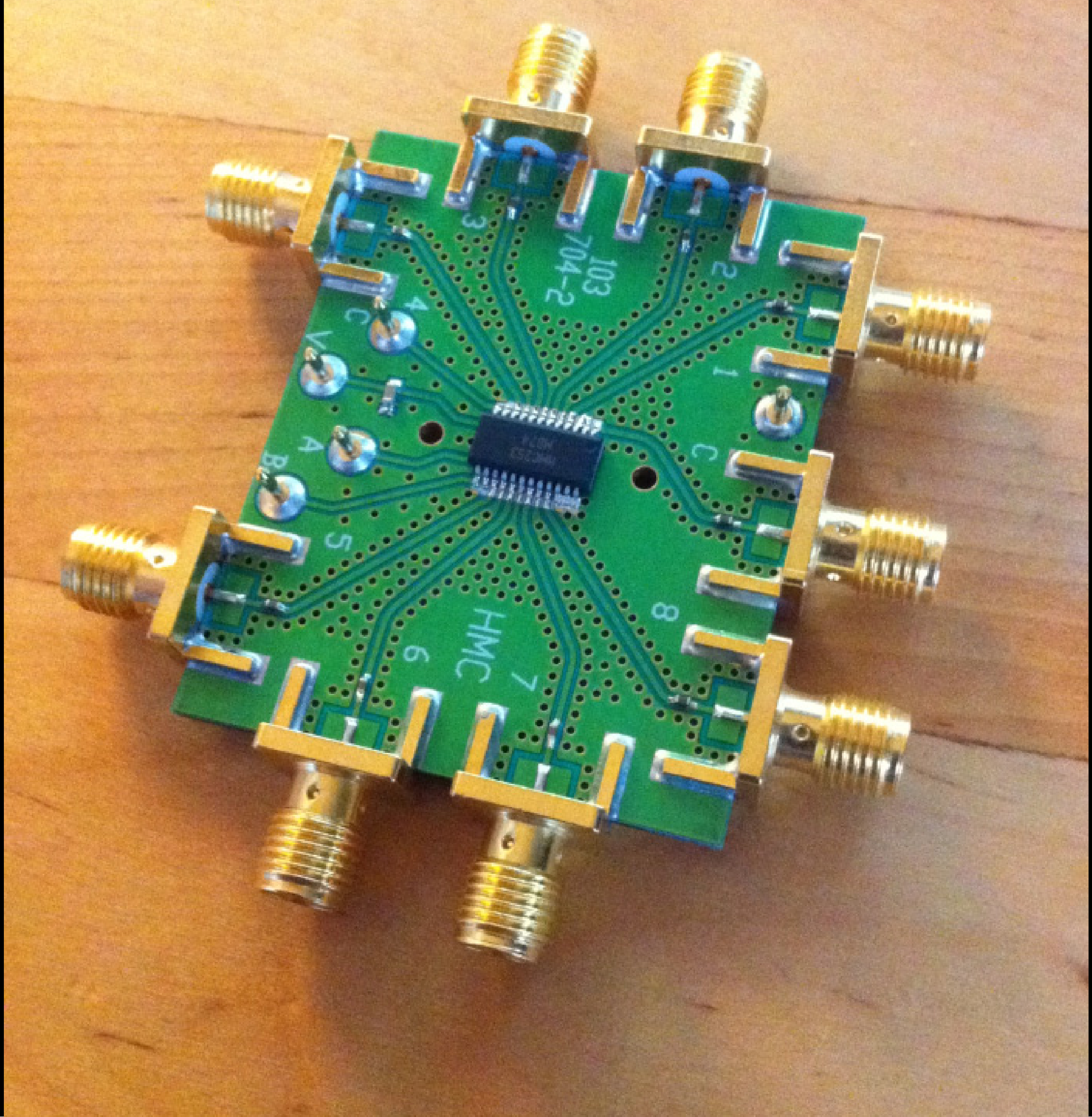


Software Defined RDF

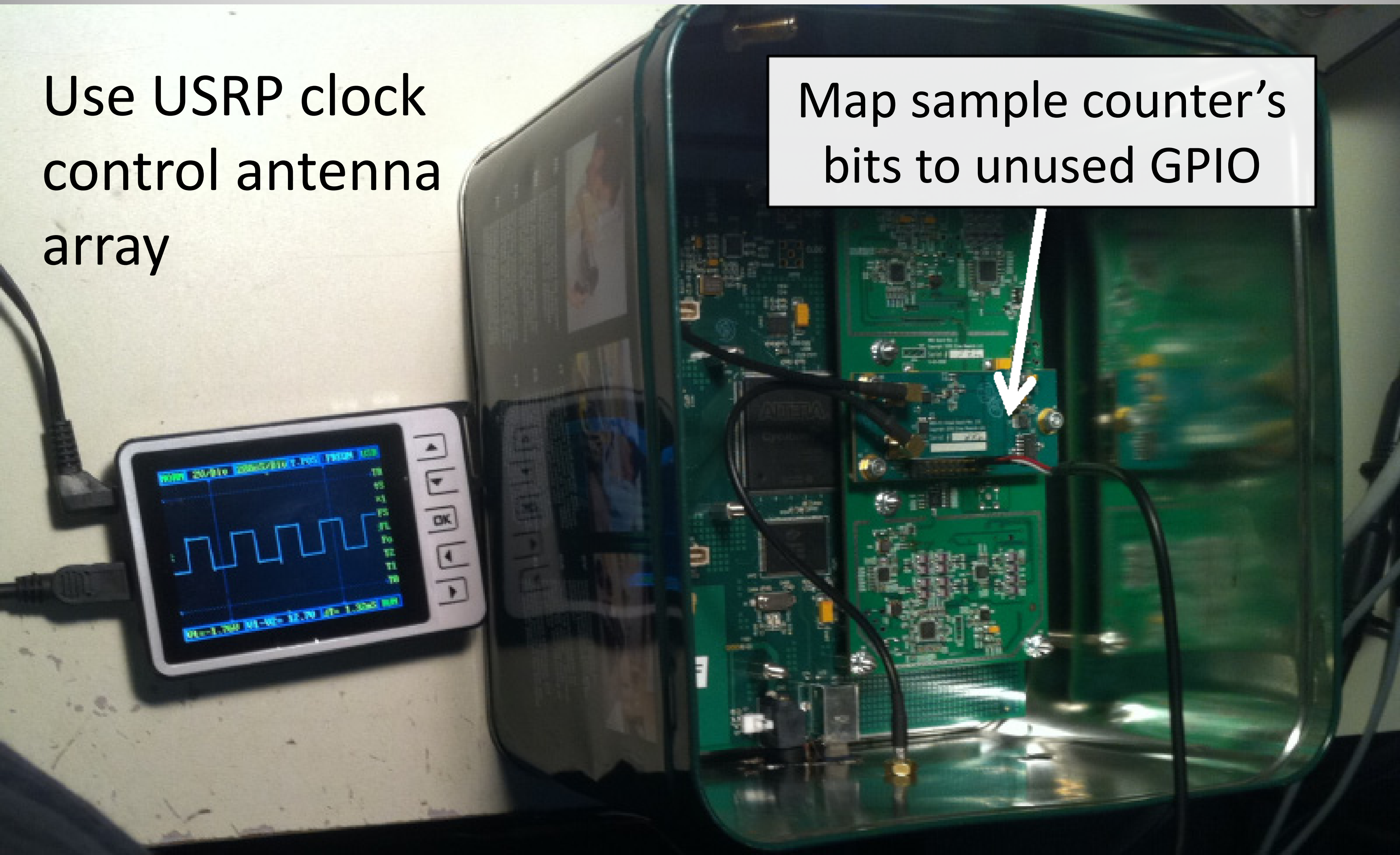



Antenna
Array

Antenna Switch



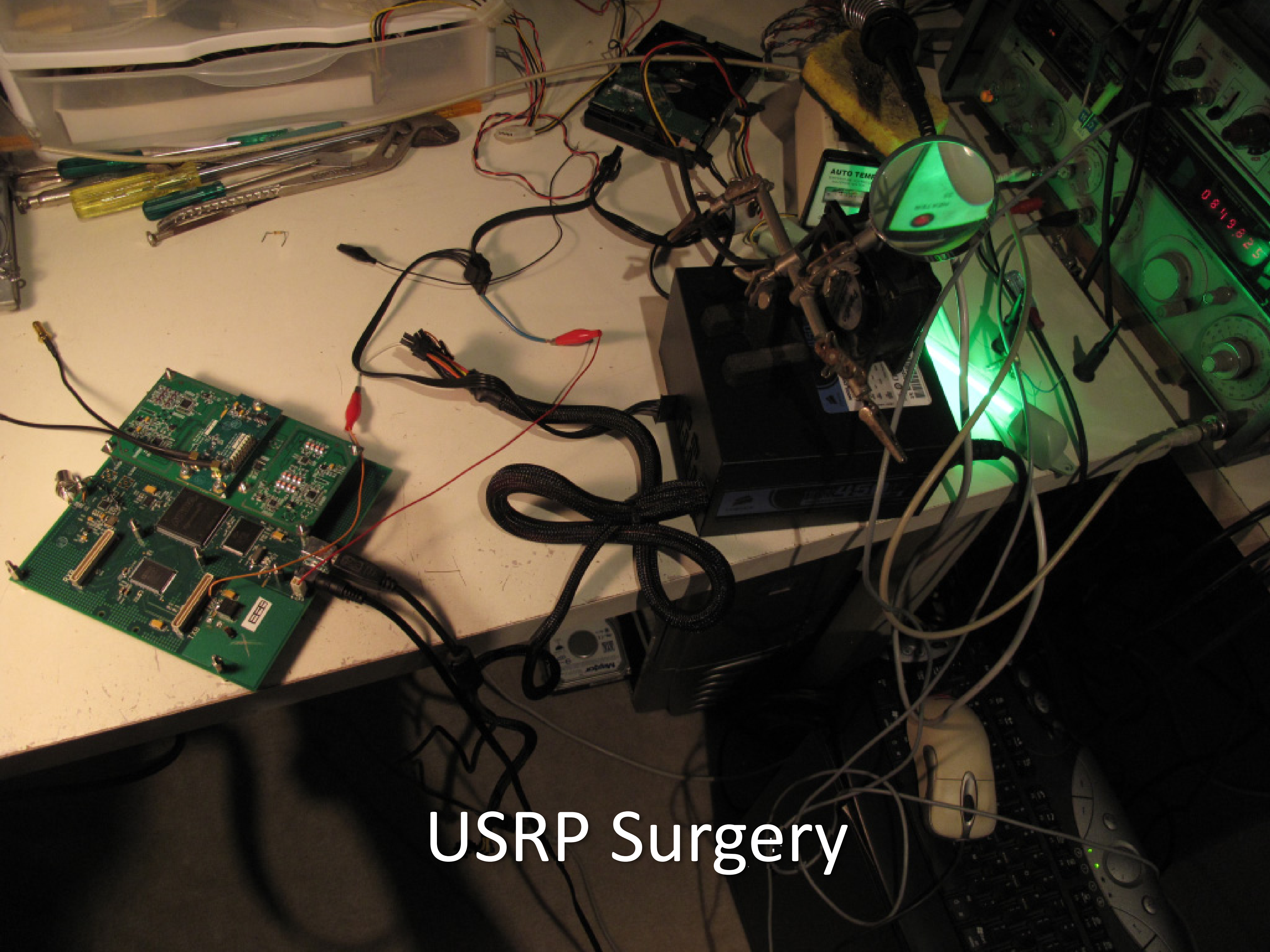
FPGA Modification



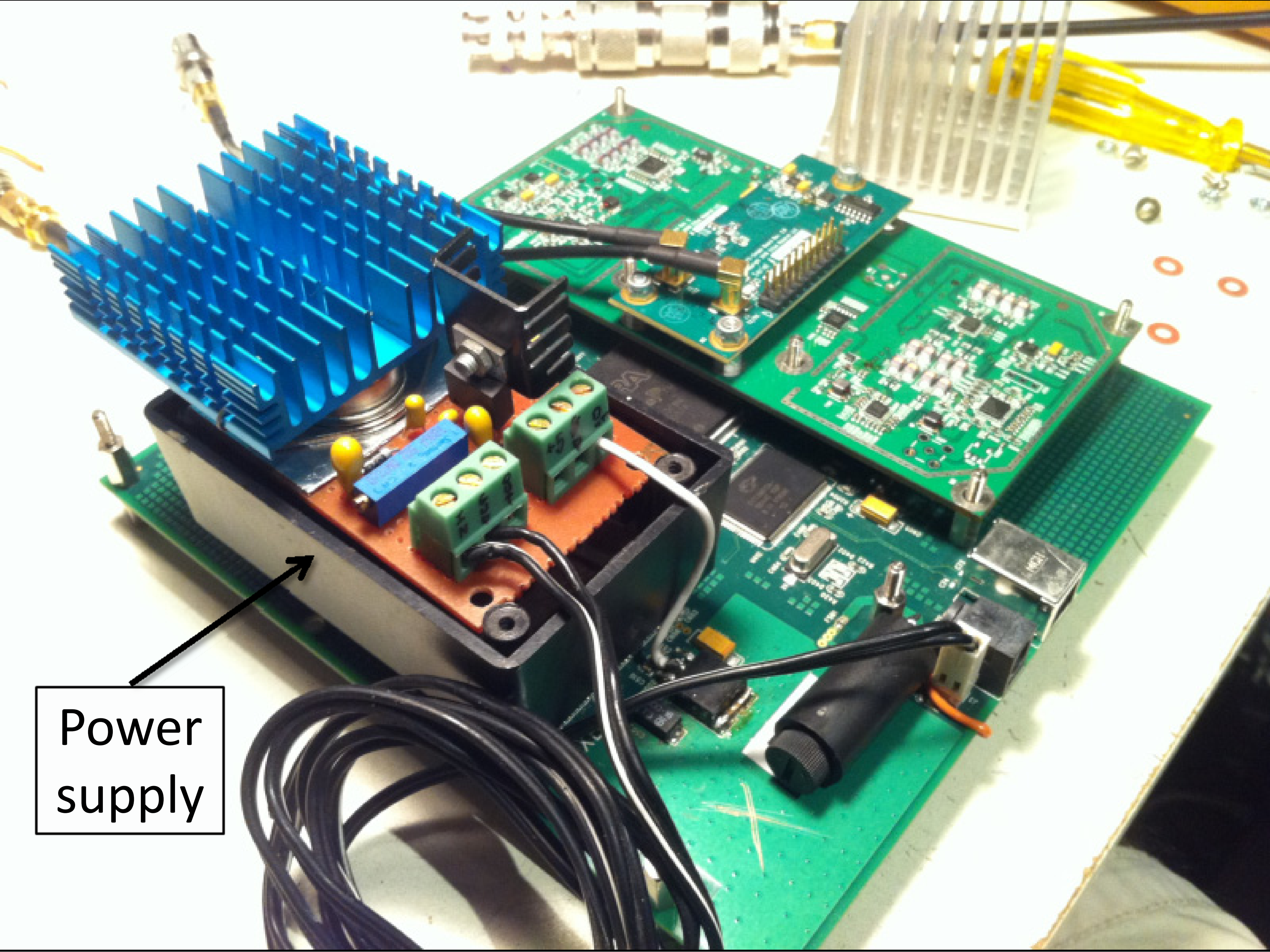
Modification Bonuses

- 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

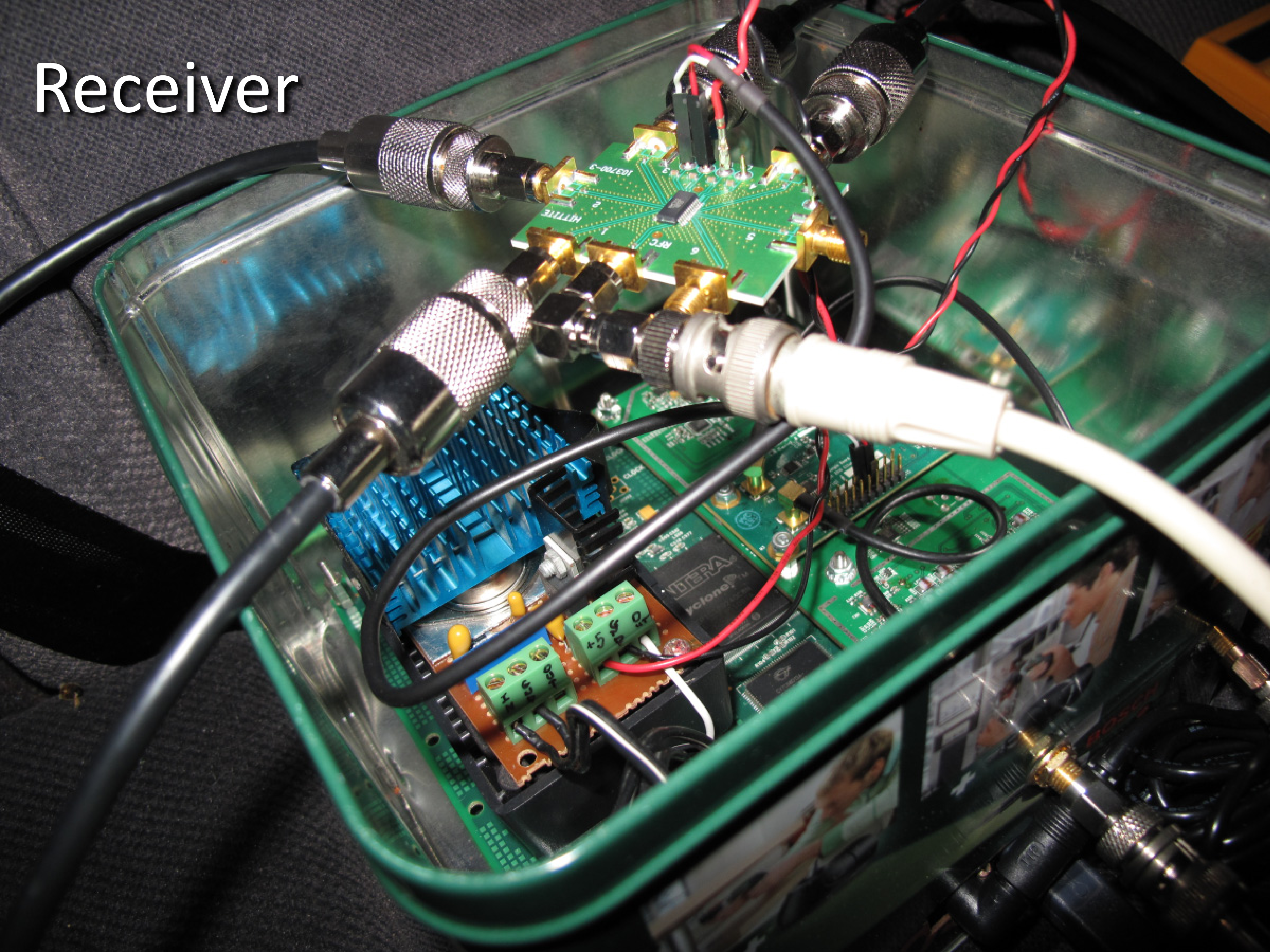

Power supply
BOOM!
TXB



USRP Surgery

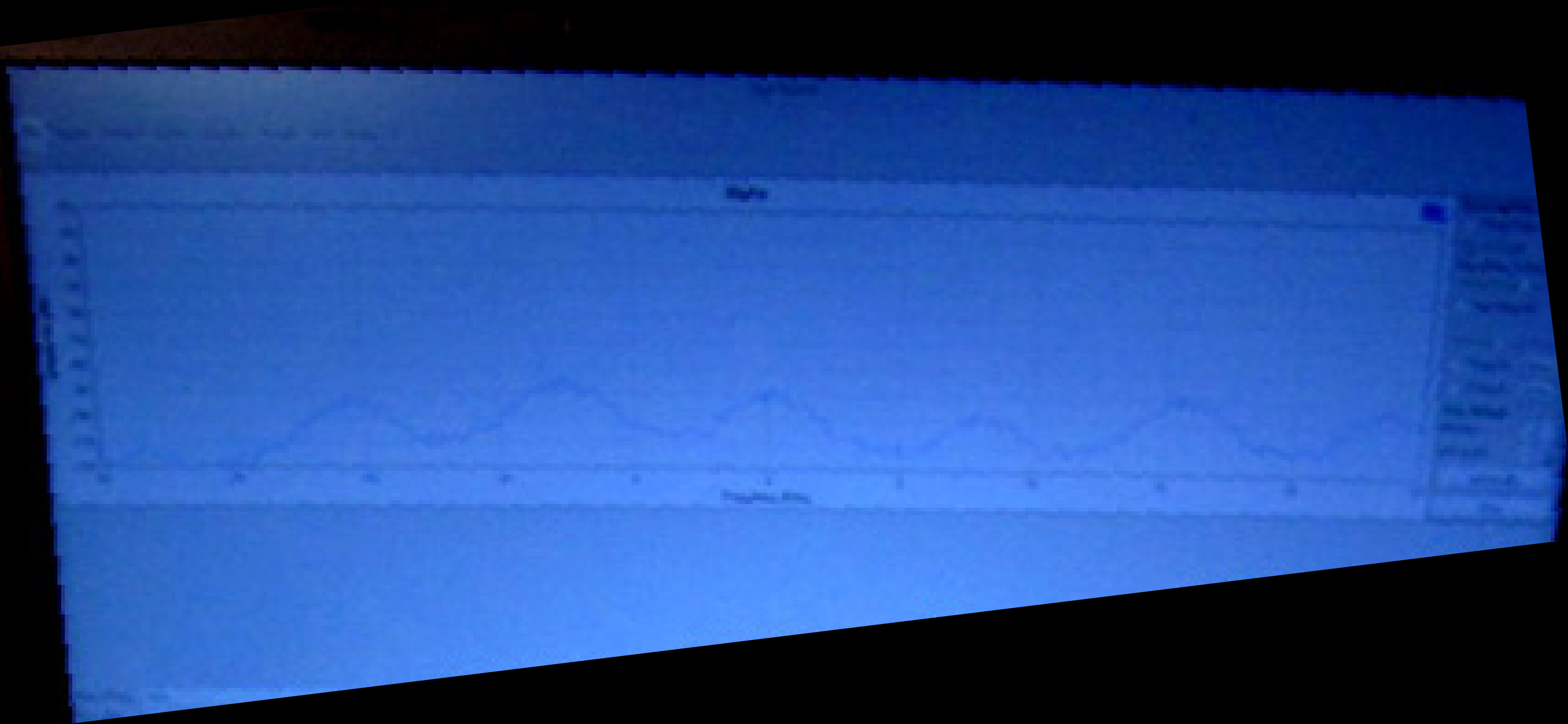

Power
supply

Receiver

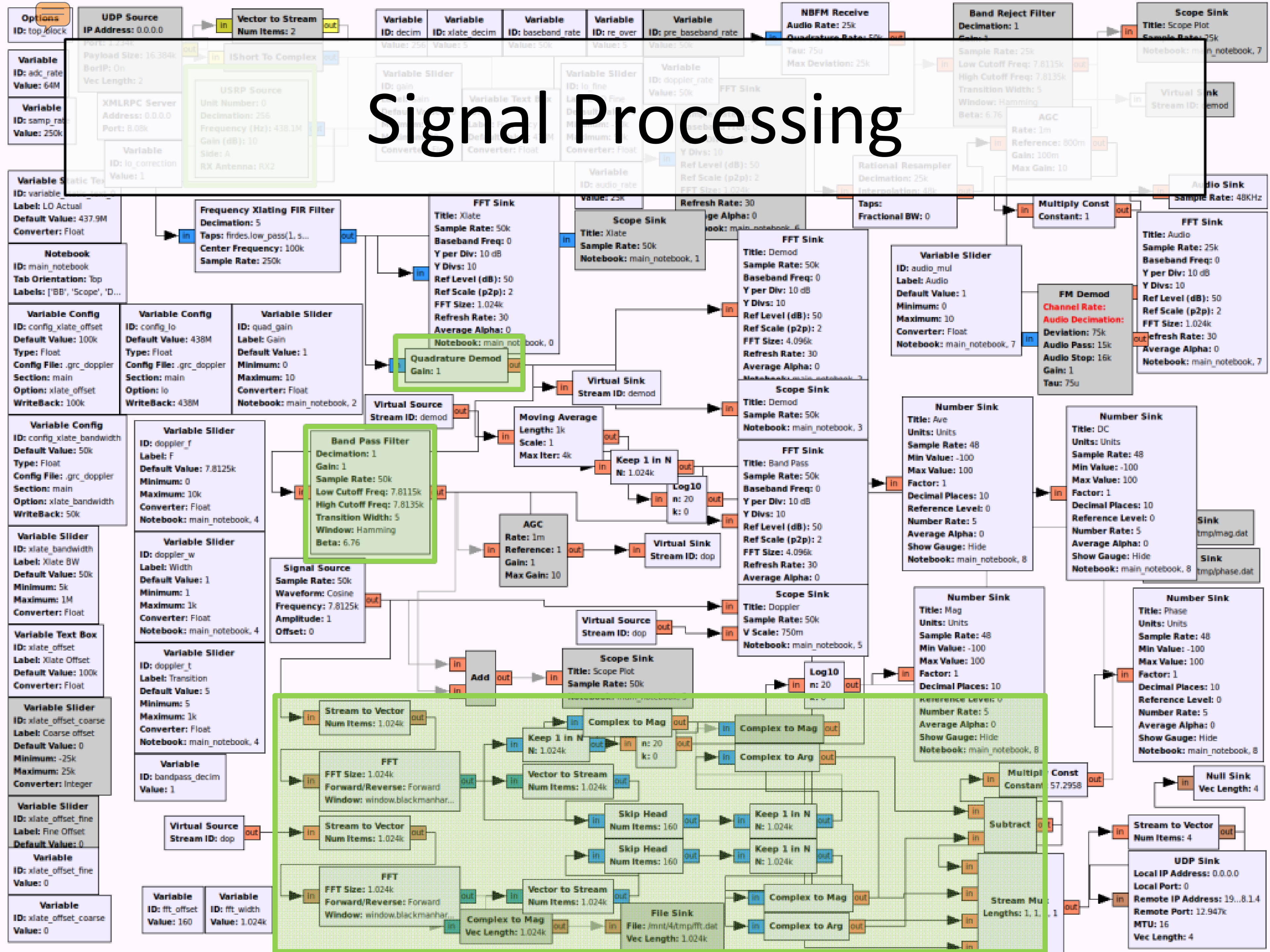


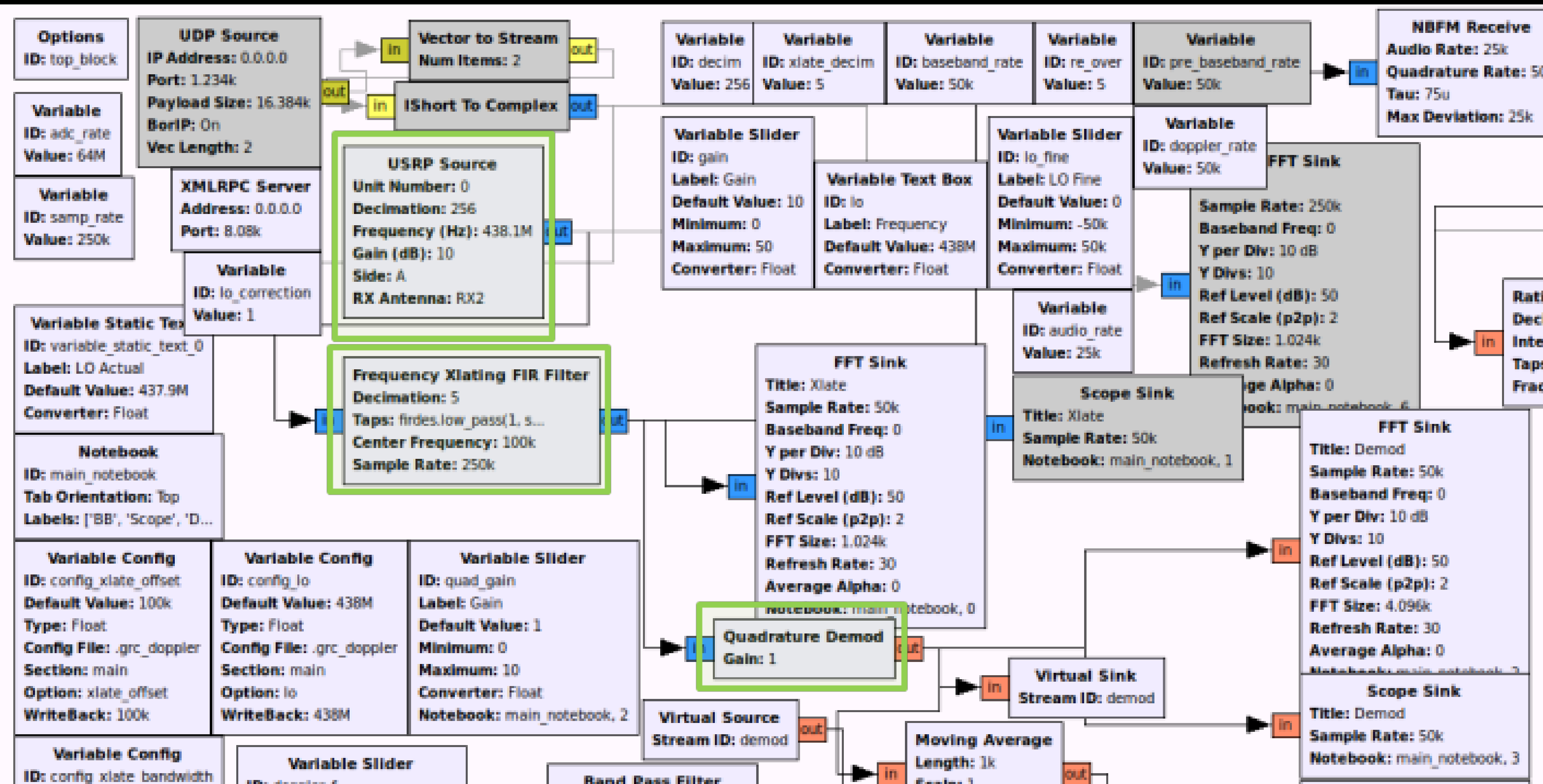
Processing & Display

Switching affecting spectrum



Signal Processing





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
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
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
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
Quadrature Demod
Gain: 1
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

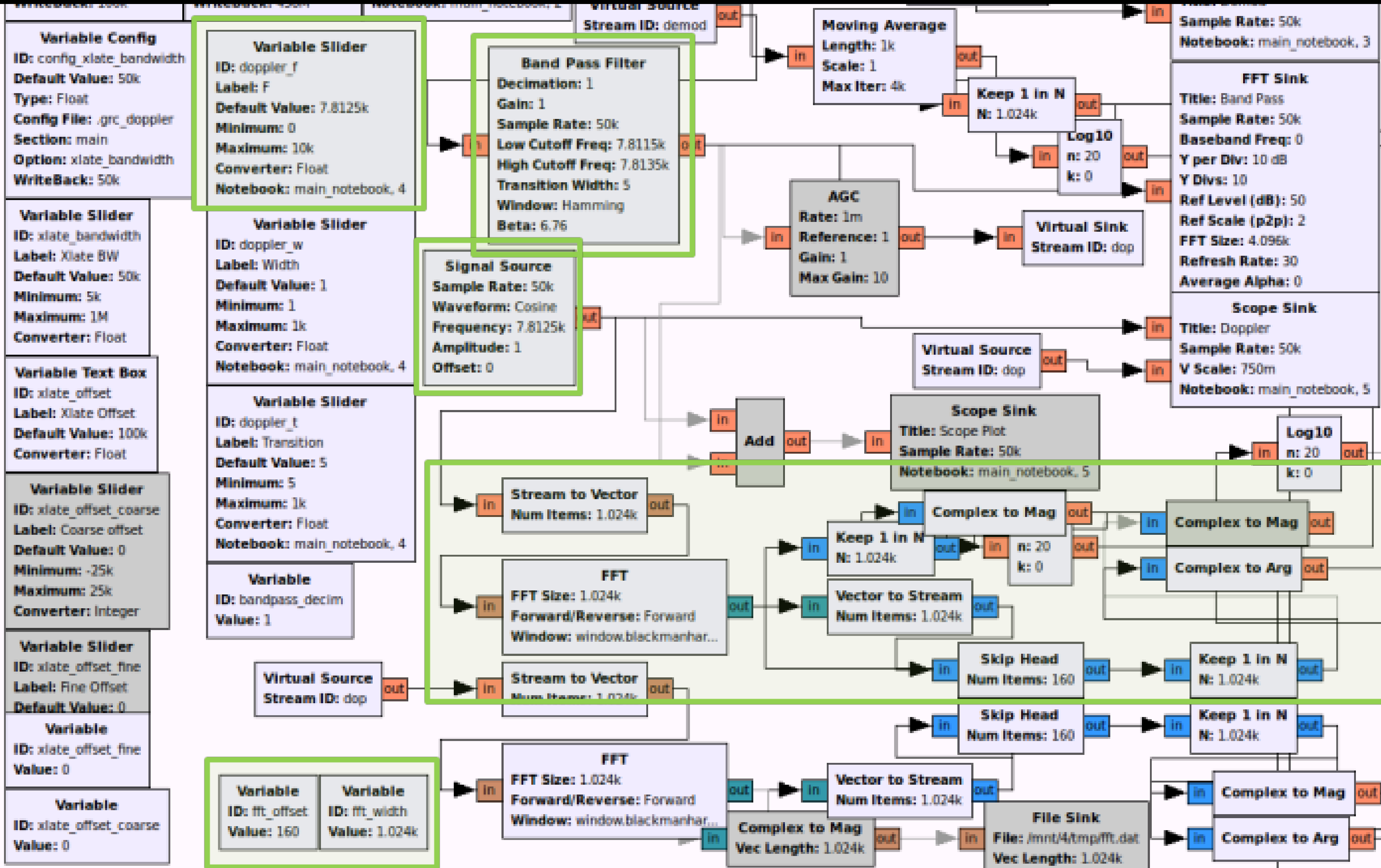
(64 MHz / 256) = **250 ksps**

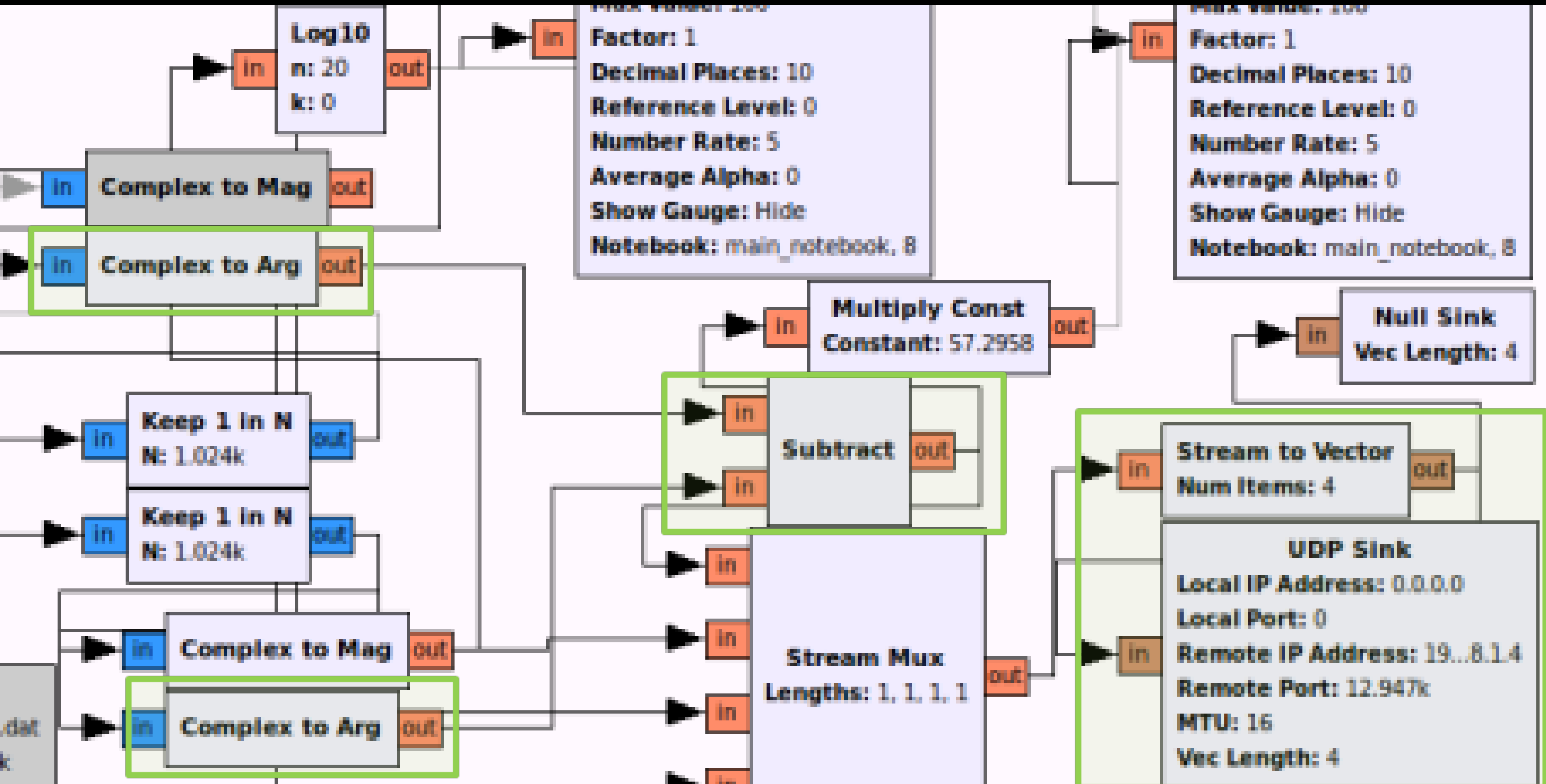
31st and **32nd** bits used

→ 250k / 32 = 7.8125 kHz tone

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

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


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



Log10
n: 20
k: 0
Factor: 1
Decimal Places: 10
Reference Level: 0
Number Rate: 5
Average Alpha: 0
Show Gauge: Hide
Notebook: main_notebook, 8
Factor: 1
Decimal Places: 10
Reference Level: 0
Number Rate: 5
Average Alpha: 0
Show Gauge: Hide
Notebook: main_notebook, 8
Complex to Mag
Complex to Arg
Multiply Const
Constant: 57.2958
Null Sink
Vec Length: 4
Keep 1 in N
N: 1.024k
Keep 1 in N
N: 1.024k
Subtract
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
Stream Mux
Lengths: 1, 1, 1, 1
Complex to Mag
Complex to Arg

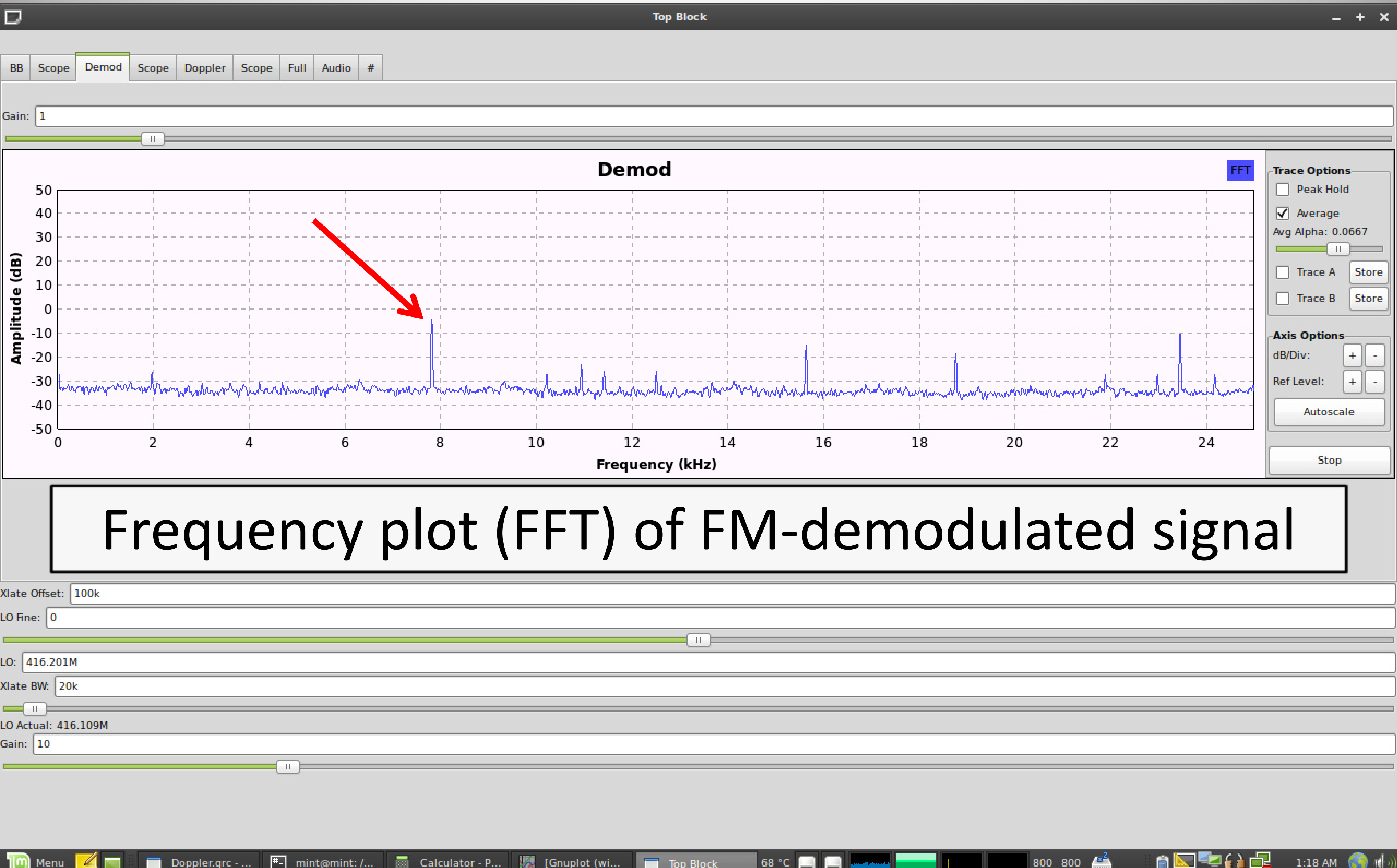
Magic of SDR

FM (quadrature) demodulation:

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

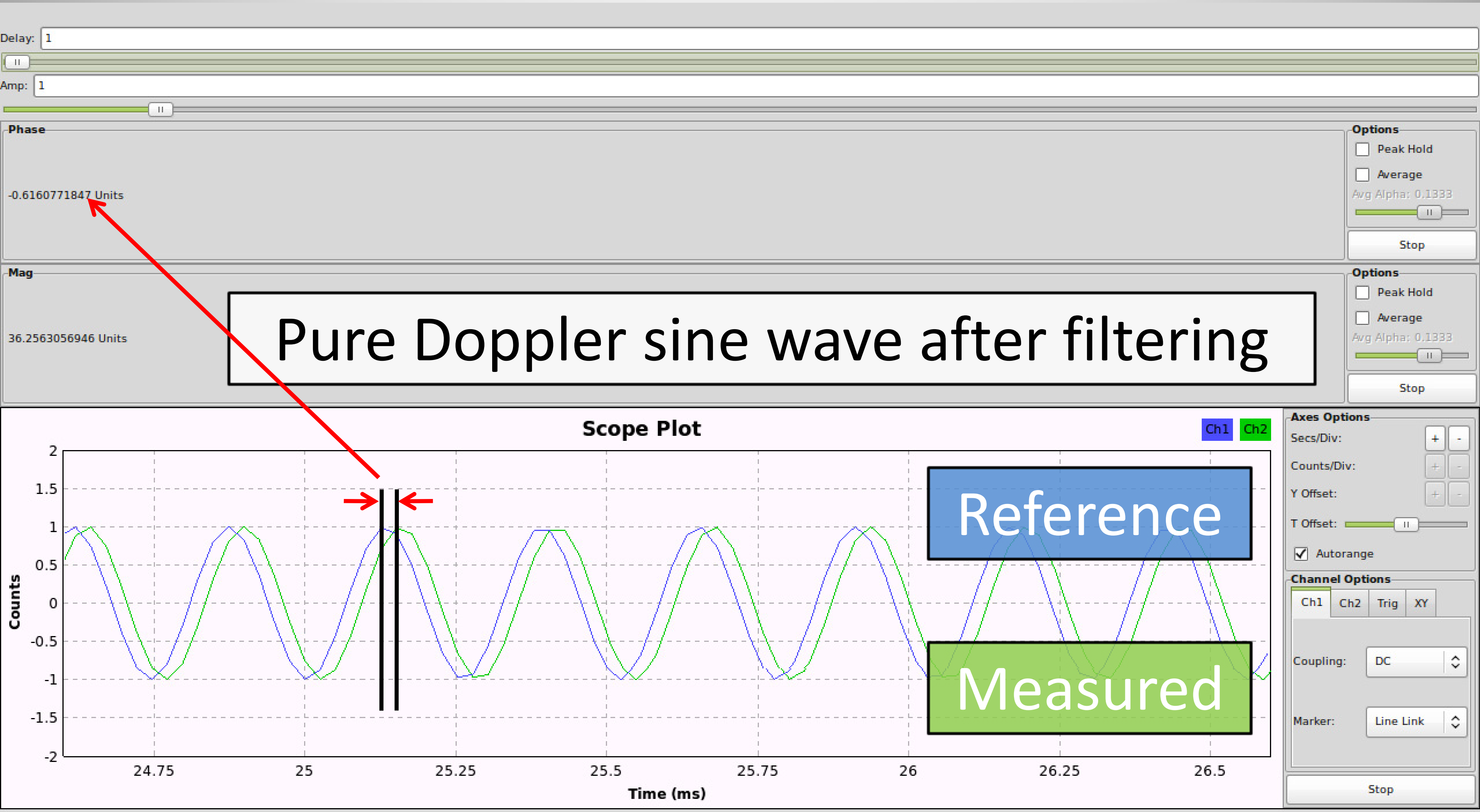
```
 for (int i = 0; i < noutput_items; i++) {
    gr_complex product = in[i] * conj(in[i-1]);
    out[i] = d_gain * arg (product);
}
```

Doppler sine wave



Frequency plot (FFT) of FM-demodulated signal

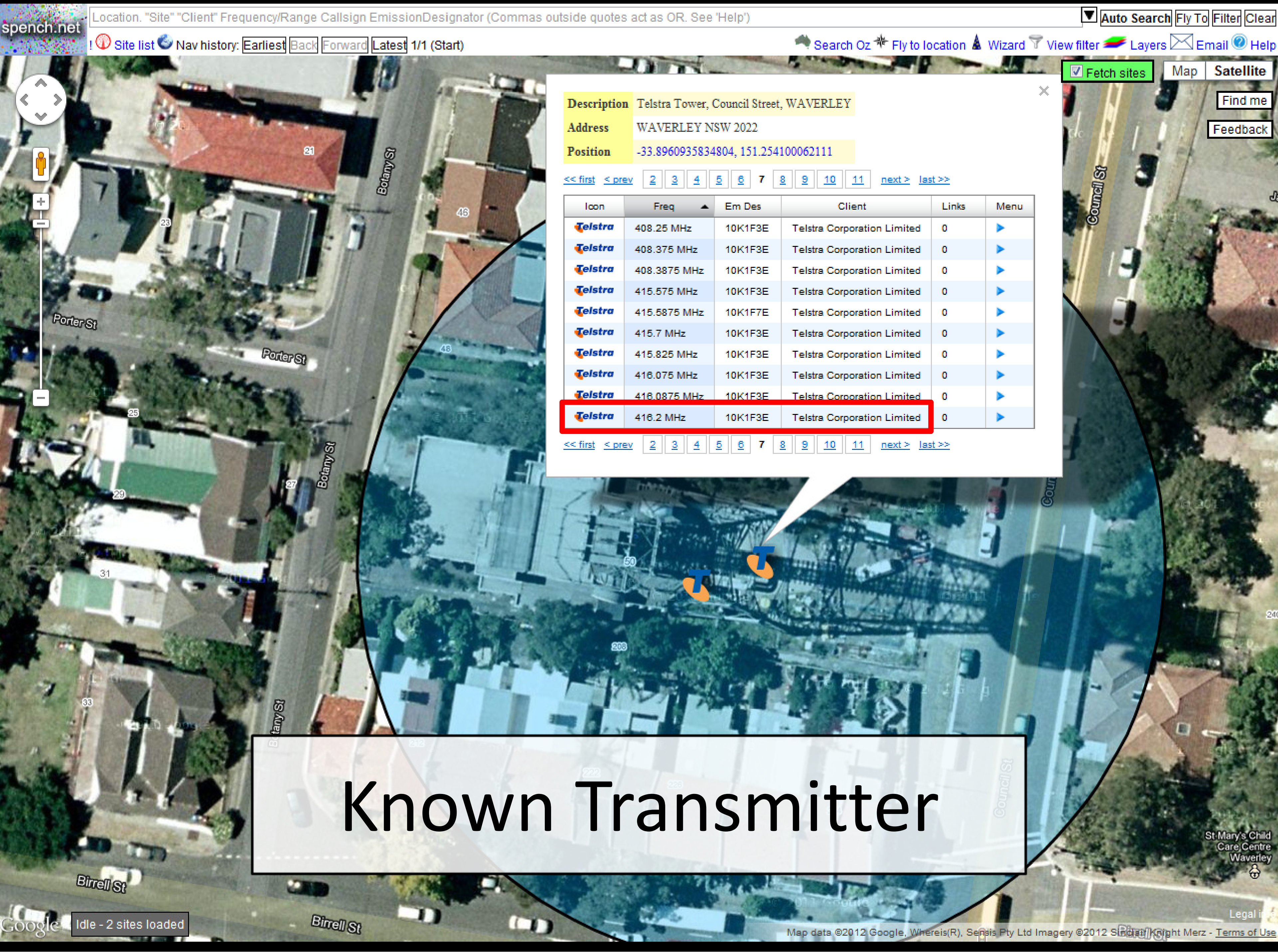
Doppler sine wave




Find a target

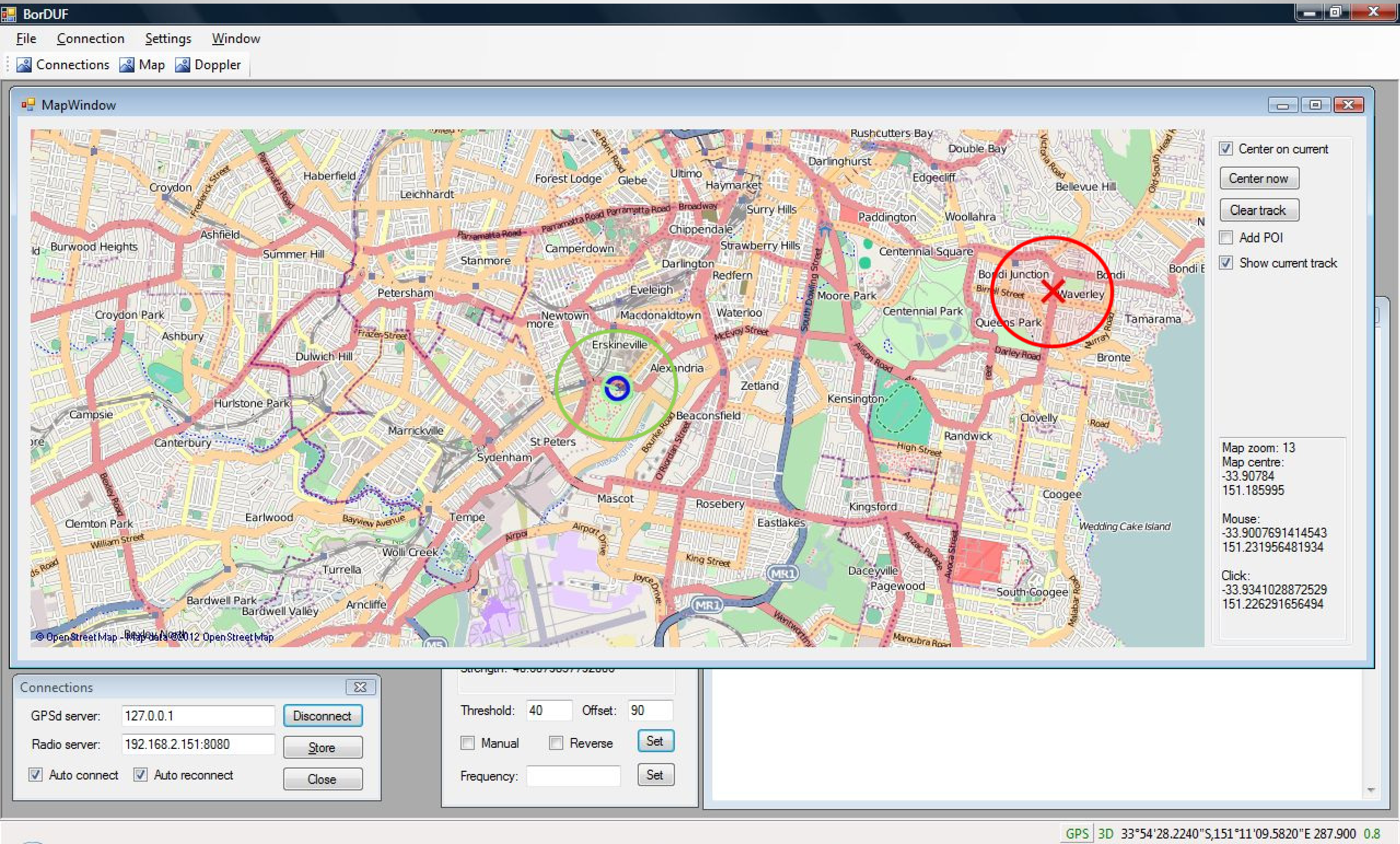

Telstra Tower on Council St

Known Transmitter



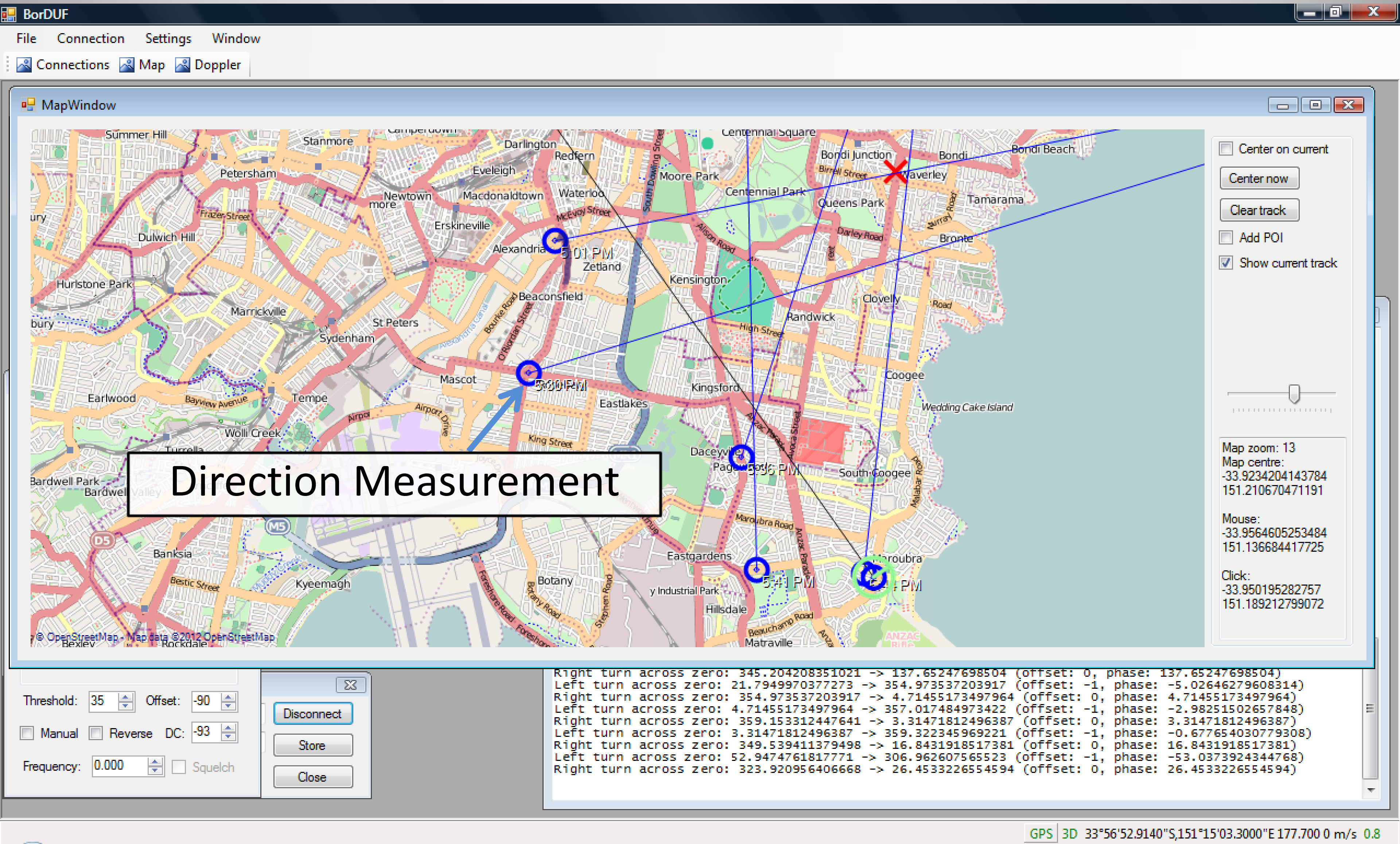
Icon	Freq	Em Des	Client	Links	Menu
Telstra	408.25 MHz	10K1F3E	Telstra Corporation Limited	0	▶
Telstra	408.375 MHz	10K1F3E	Telstra Corporation Limited	0	▶
Telstra	408.3875 MHz	10K1F3E	Telstra Corporation Limited	0	▶
Telstra	415.575 MHz	10K1F3E	Telstra Corporation Limited	0	▶
Telstra	415.5875 MHz	10K1F7E	Telstra Corporation Limited	0	▶
Telstra	415.7 MHz	10K1F3E	Telstra Corporation Limited	0	▶
Telstra	415.825 MHz	10K1F3E	Telstra Corporation Limited	0	▶
Telstra	416.075 MHz	10K1F3E	Telstra Corporation Limited	0	▶
Telstra	416.0875 MHz	10K1F3E	Telstra Corporation Limited	0	▶
Telstra	416.2 MHz	10K1F3E	Telstra Corporation Limited	0	▶

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
© OpenStreetMap - Map data ©2012 OpenStreetMap
Croydon
Haberfield
Leichhardt
Forest Lodge
Glebe
Ultimo
Haymarket
Darlinghurst
Double Bay
Edgecliff
Bellevue Hill
Surry Hills
Paddington
Woollahra
Ashfield
Burwood Heights
Summer Hill
Chippendale
Camperdown
Stanmore
Strawberry Hills
Centennial Square
Darlington
Redfern
Bondi Junction
Bondi
Waverley
Petersham
Eveleigh
Moore Park
Centennial Park
Queens Park
Tamarama
Croydon Park
Ashbury
Newtown
Macdonaldtown
Waterloo
Dulwich Hill
Erskineville
Alexandria
Zetland
Bronte
Kensington
Campsie
Hurlstone Park
Beaconsfield
Clovelly
Canterbury
Marrickville
St Peters
Randwick
Sydenham
Mascot
Rosebery
Kingsford
Coogee
Clemton Park
Earlwood
Tempe
Eastlakes
Wedding Cake Island
Wolli Creek
Turrella
Daceyville
Pagewood
South Coogee
Bardwell Park
Bardwell Valley
Arncliffe
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

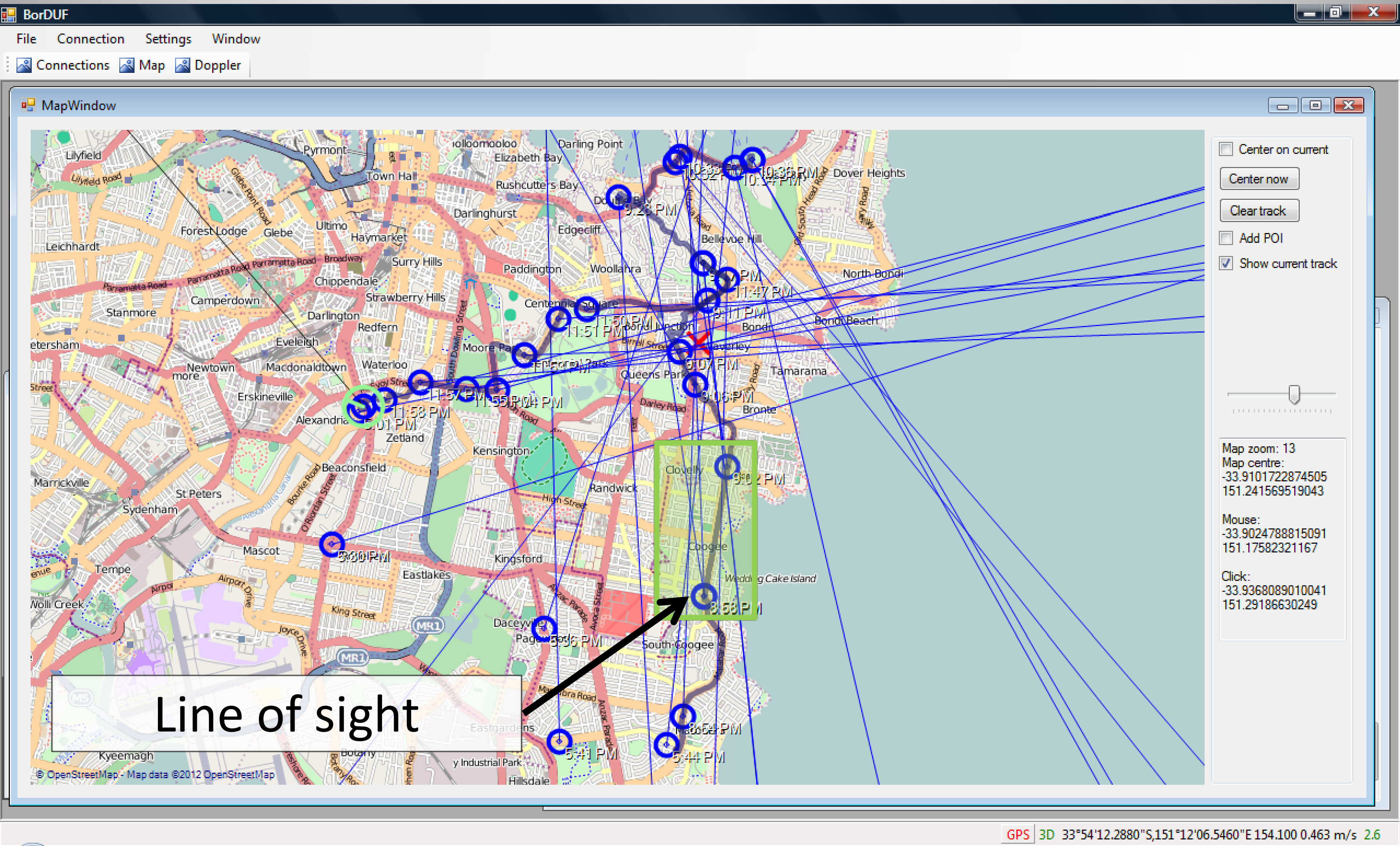
Drive


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
© OpenStreetMap - Map data ©2012 OpenStreetMap
Threshold:
35
Offset:
-90
Manual
Reverse
DC:
-93
Frequency:
0.000
Squelch
Disconnect
Store
Close
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

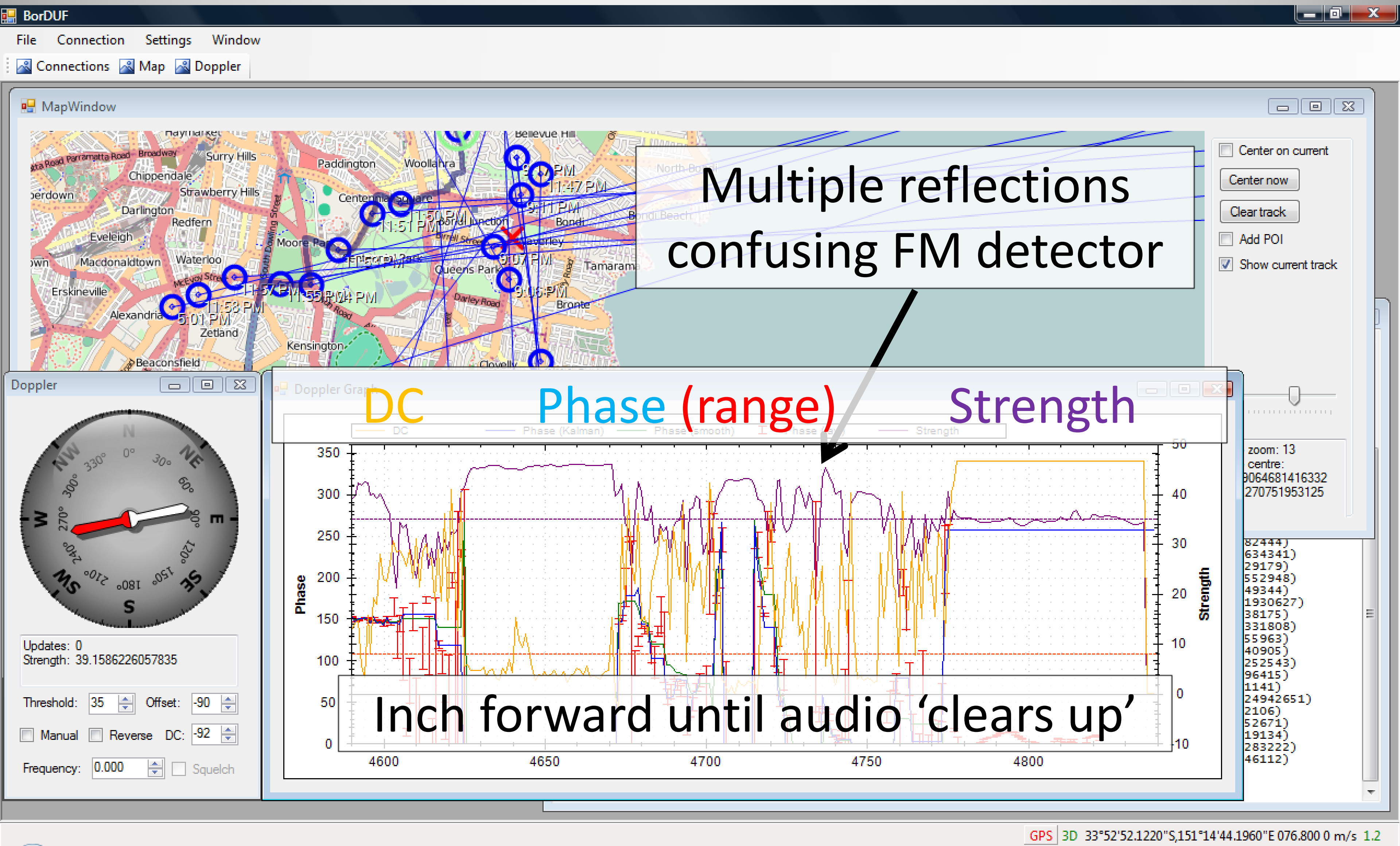
Complications

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

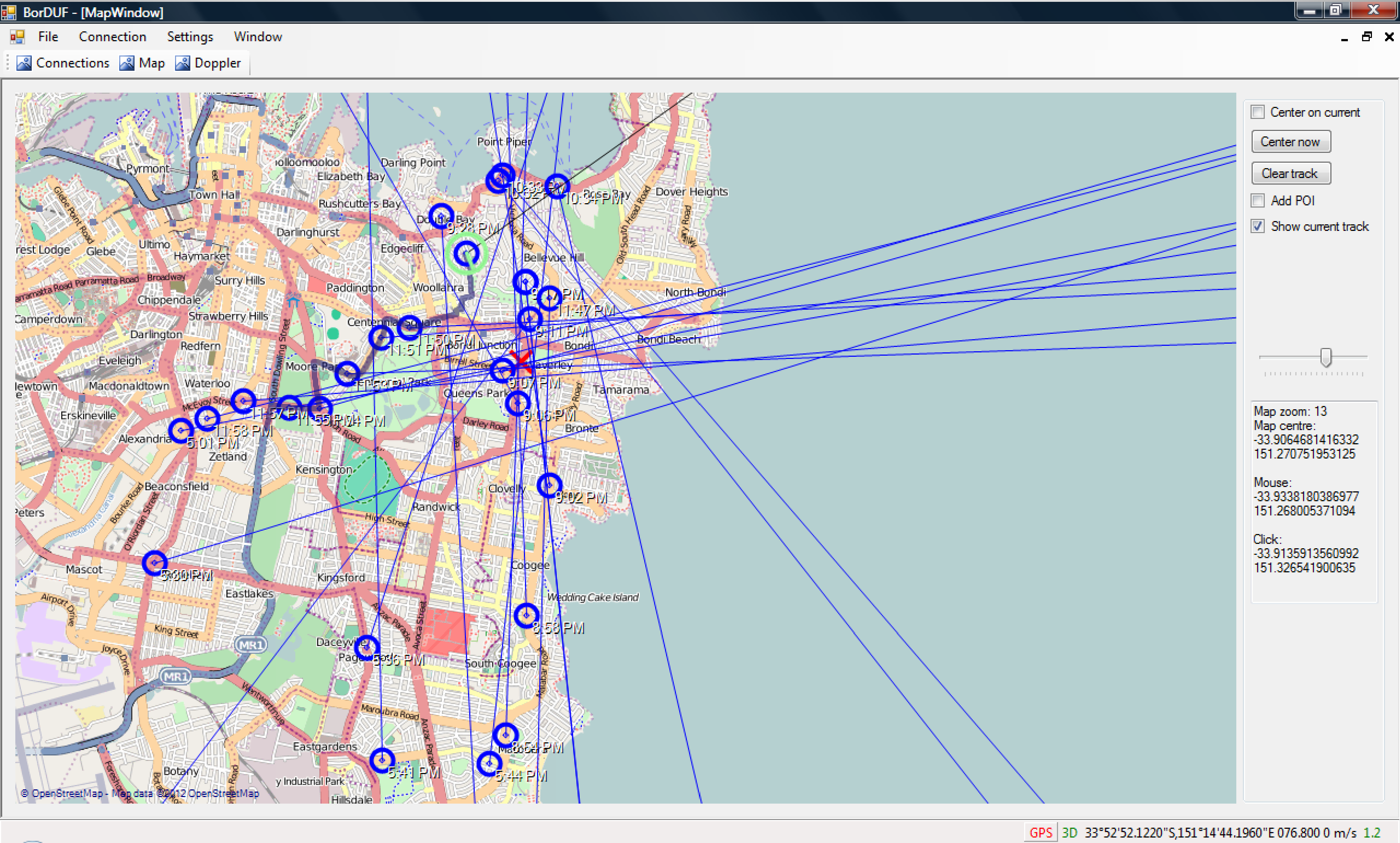
Complications: Coogee



Listen: Multipath

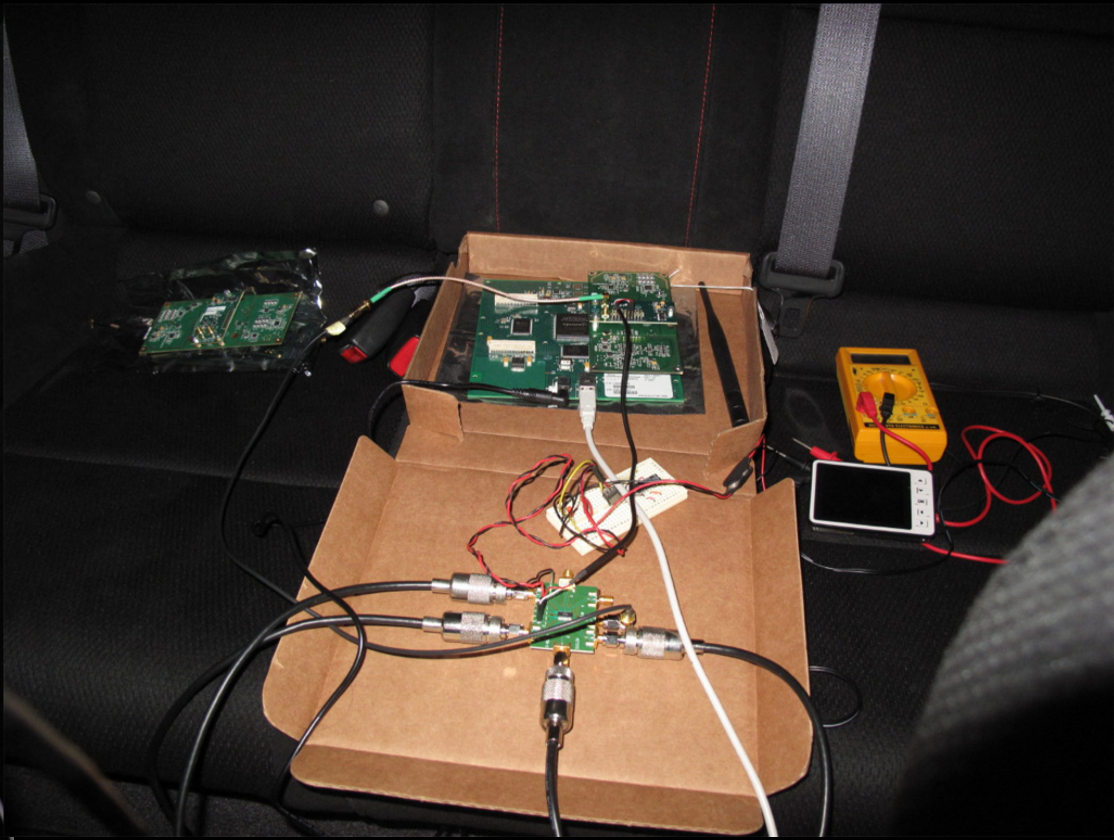


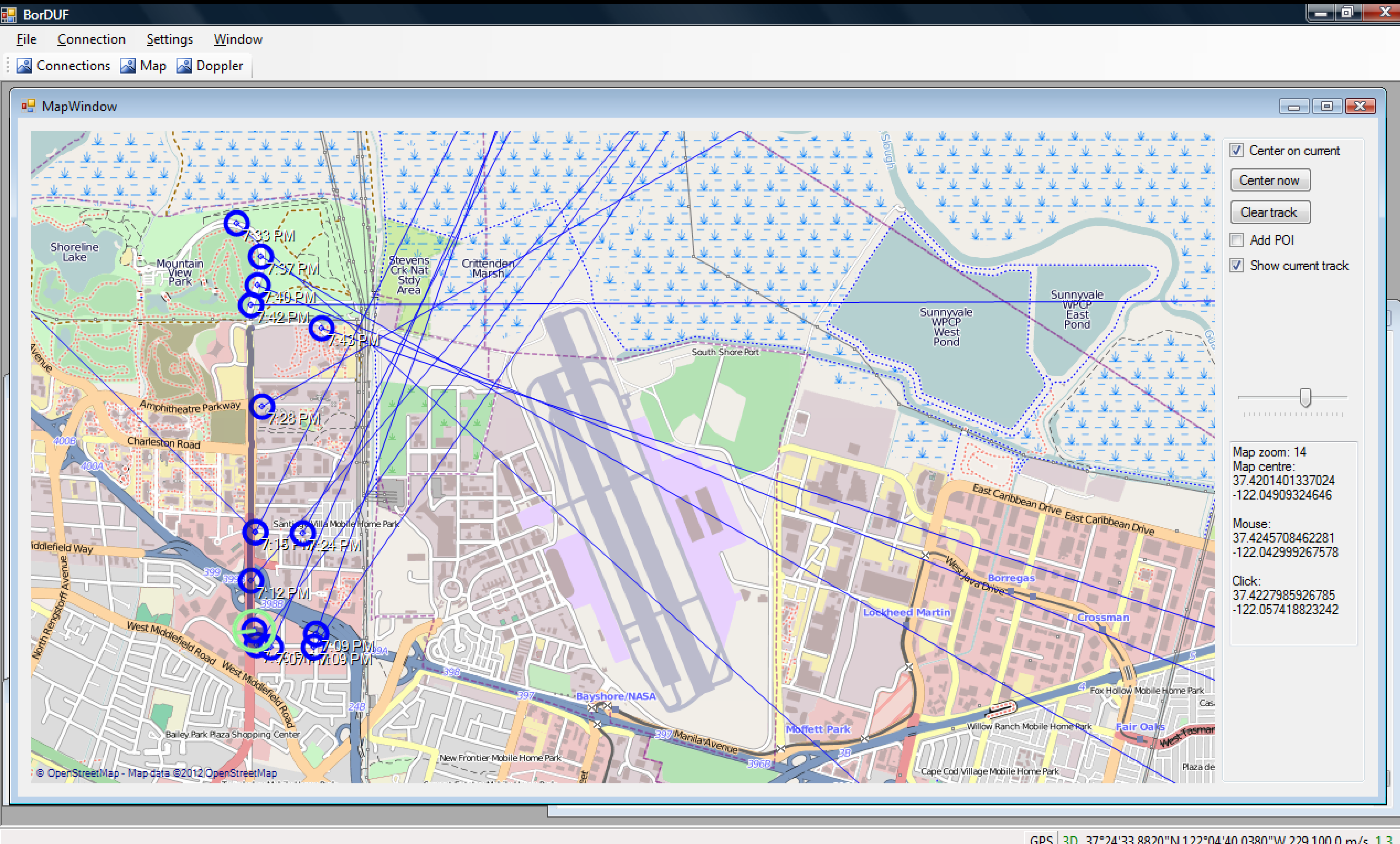
Done



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
GPS
3D
33°52'52.1220"S,151°14'44.1960"E 076.800 0 m/s 1.2
© OpenStreetMap - Map data ©2012 OpenStreetMap

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
Map zoom: 14
Map centre:
37.4201401337024
-122.04909324646
Mouse:
37.4245708462281
-122.042999267578
Click:
37.4227985926785
-122.057418823242
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
Middlefield Way
West Middlefield Road
North Rengstorff Avenue
East Caribbean Drive
West Java Drive
Borregas
Lockheed Martin
Crossman
Bayshore/NASA
Manila Avenue
Moffett Park
Fair Oaks
Fox Hollow Mobile Home Park
Willow Ranch Mobile Home Park
Cape Cod Village Mobile Home Park
New Frontier Mobile Home Park
Bailey Park Plaza Shopping Center
Santiago Villa Mobile Home Park
7:33 PM
7:37 PM
7:40 PM
7:42 PM
7:45 PM
7:28 PM
7:15 PM
7:24 PM
7:12 PM
7:09 PM
© OpenStreetMap - Map data ©2012 OpenStreetMap
GPS 3D 37°24'33.8820"N,122°04'40.0380"W 229.100 0 m/s 1.3

"HonDF"

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

Videos:

- [SDRDF talk given at Ruxmon Sydney]
- [DF phase calculation in GNU Radio flowgraph]

balint@ettus.com

spench.net

@spenchdotnet