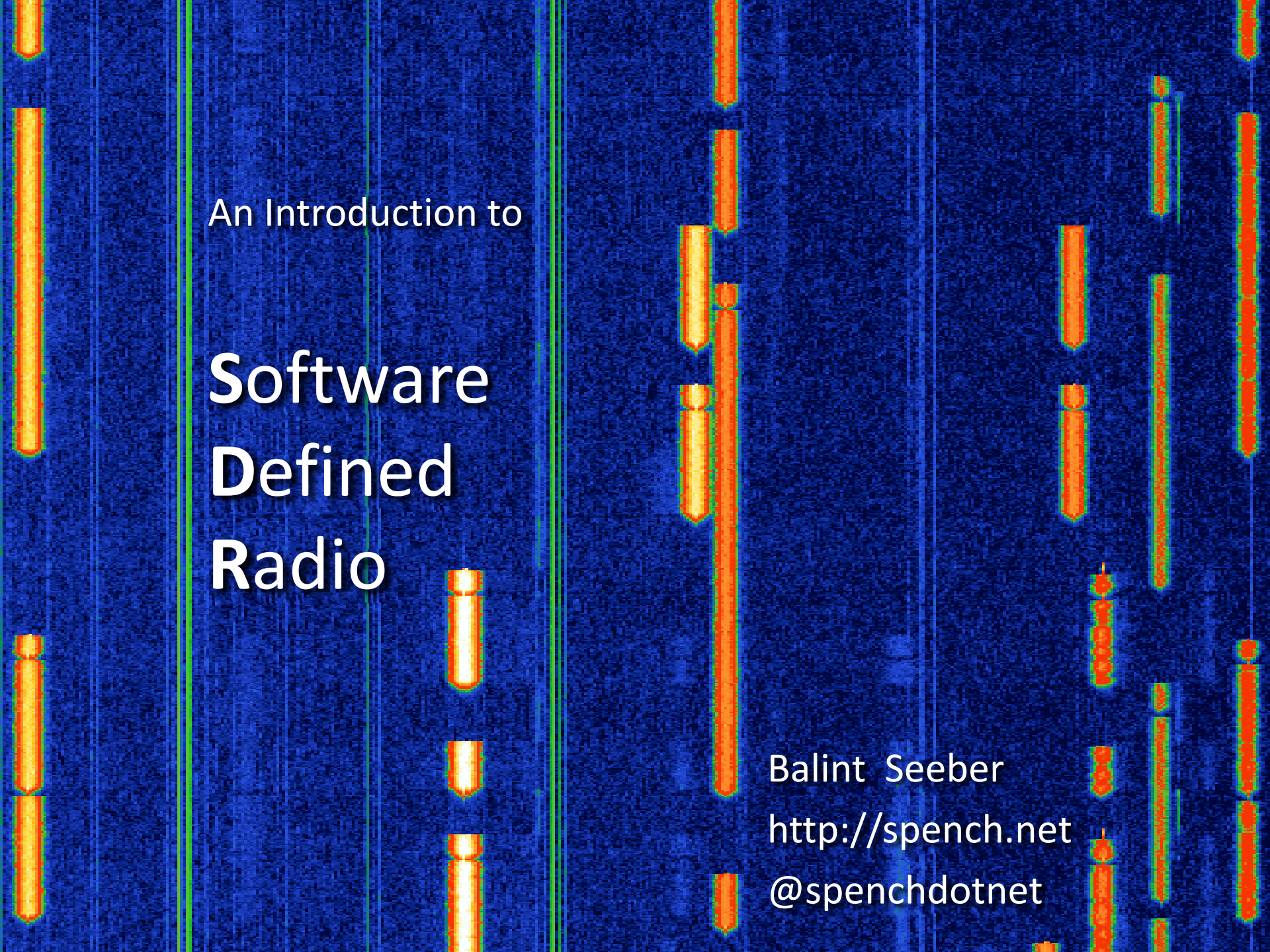
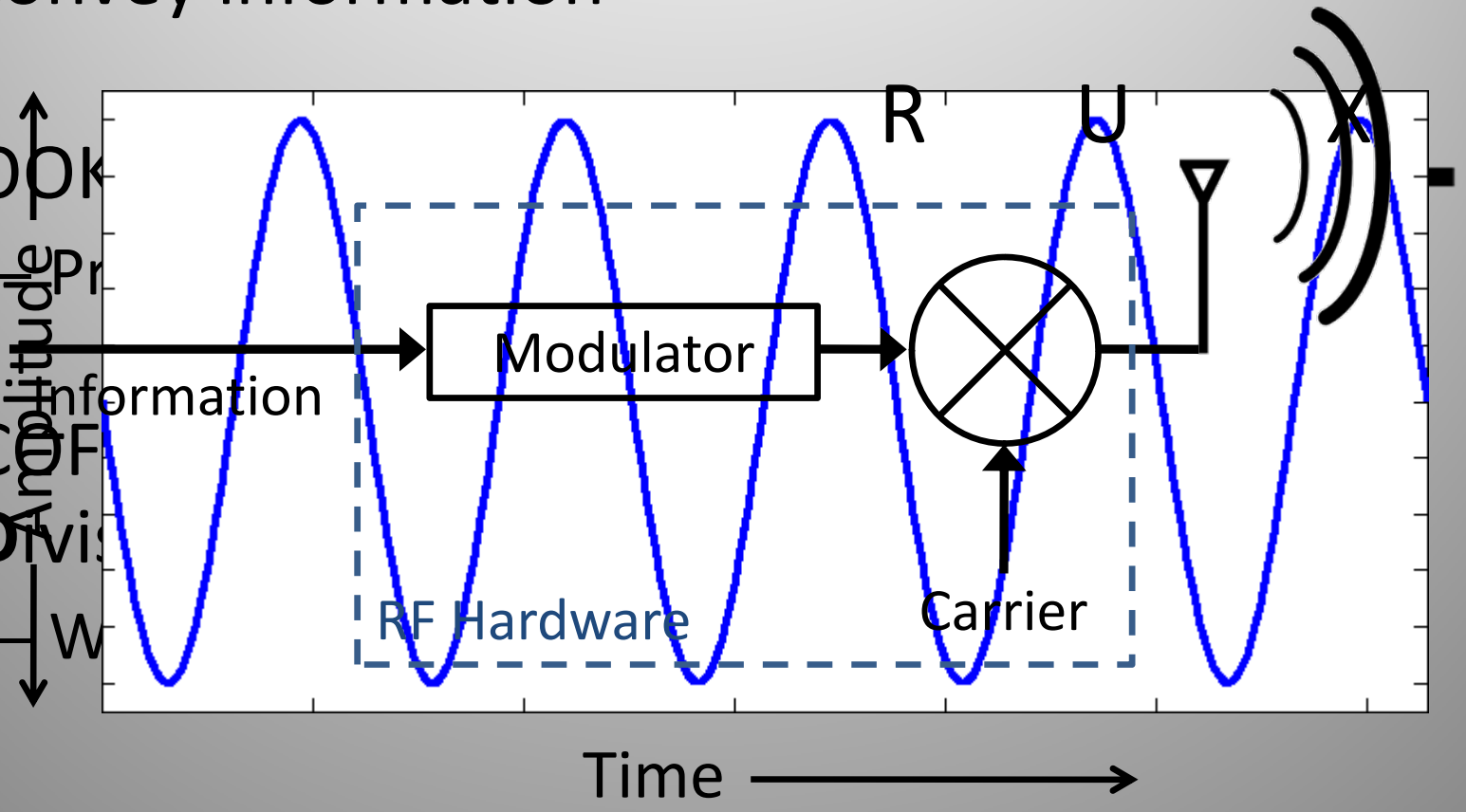

An Introduction to
Software
Defined
Radio
Balint Seeber
http://spench.net
@spenchdotnet

Overview

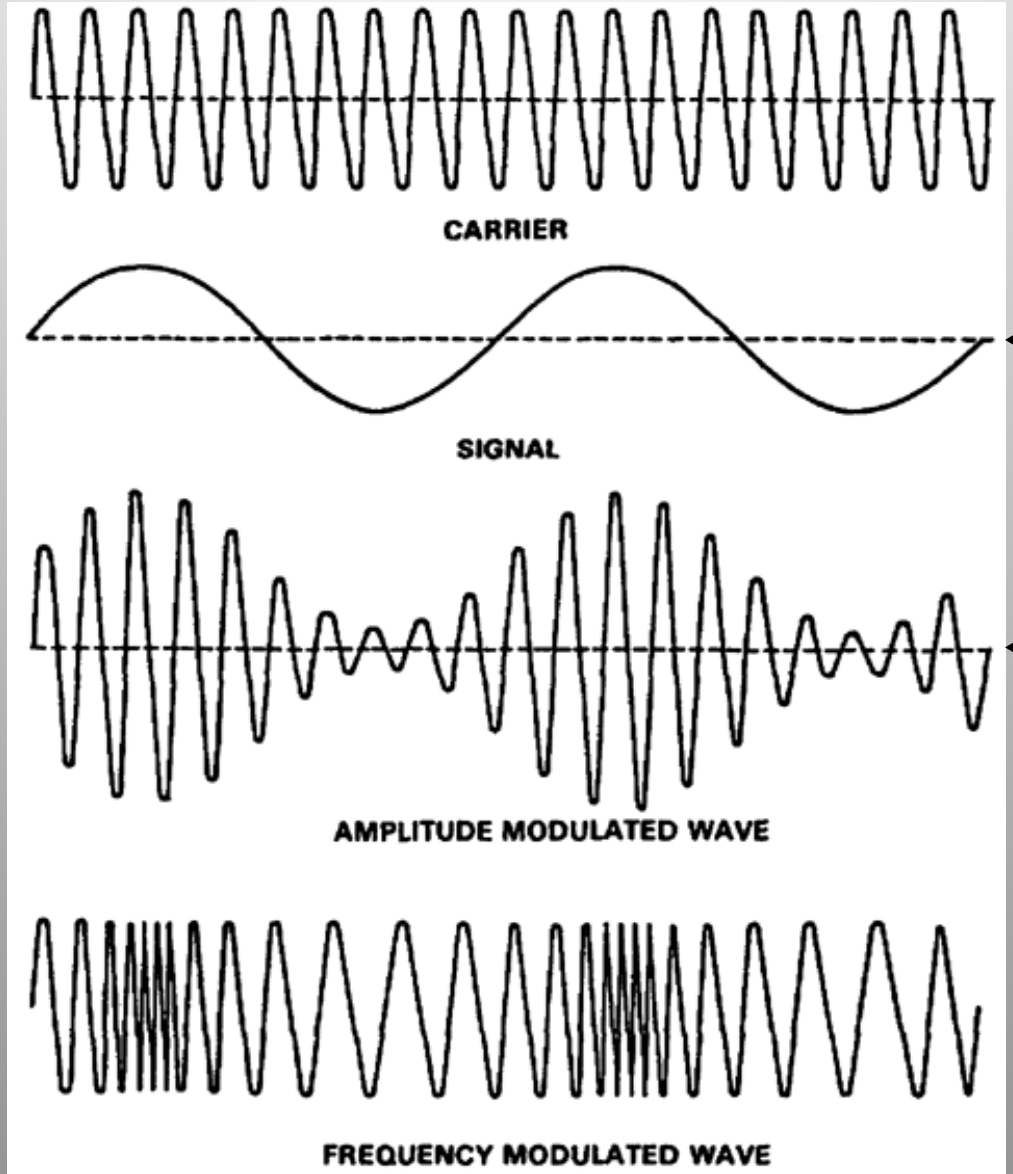
- RF 101
- Hardware → Software
- SDR Platforms
- Applications & Examples

Transmitting Data

- Radio (carrier) wave must be modulated to convey information
- OOK
- Pr
- CDF
- Divi
- W



AM & FM: In the Time Domain

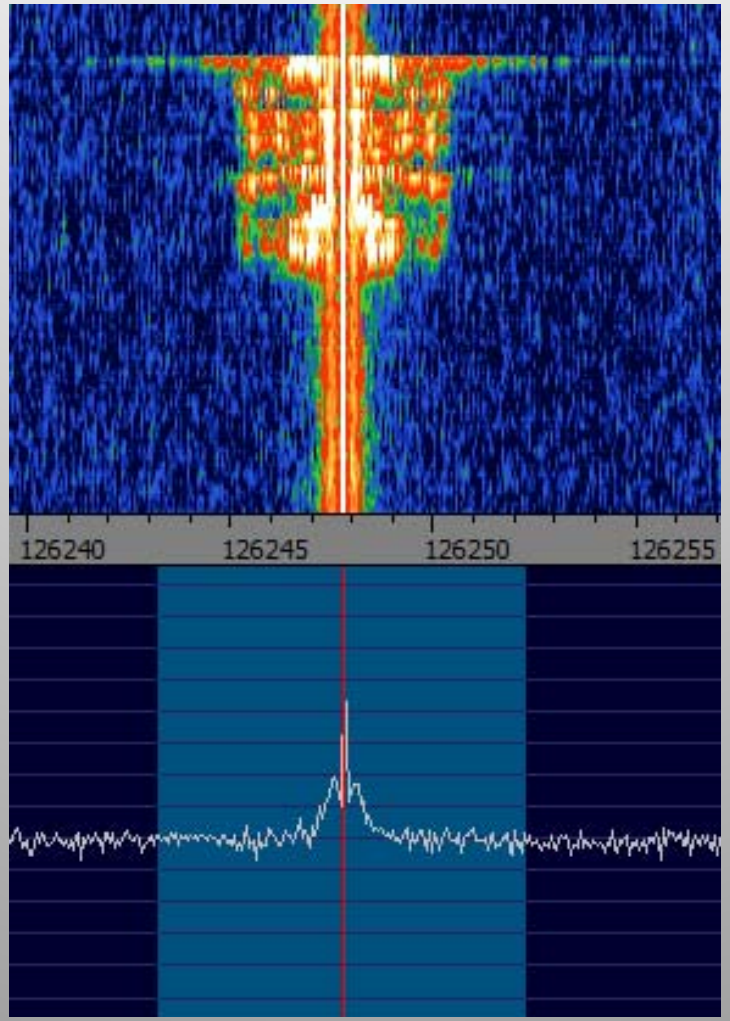


Analog or digital information

Constant amplitude

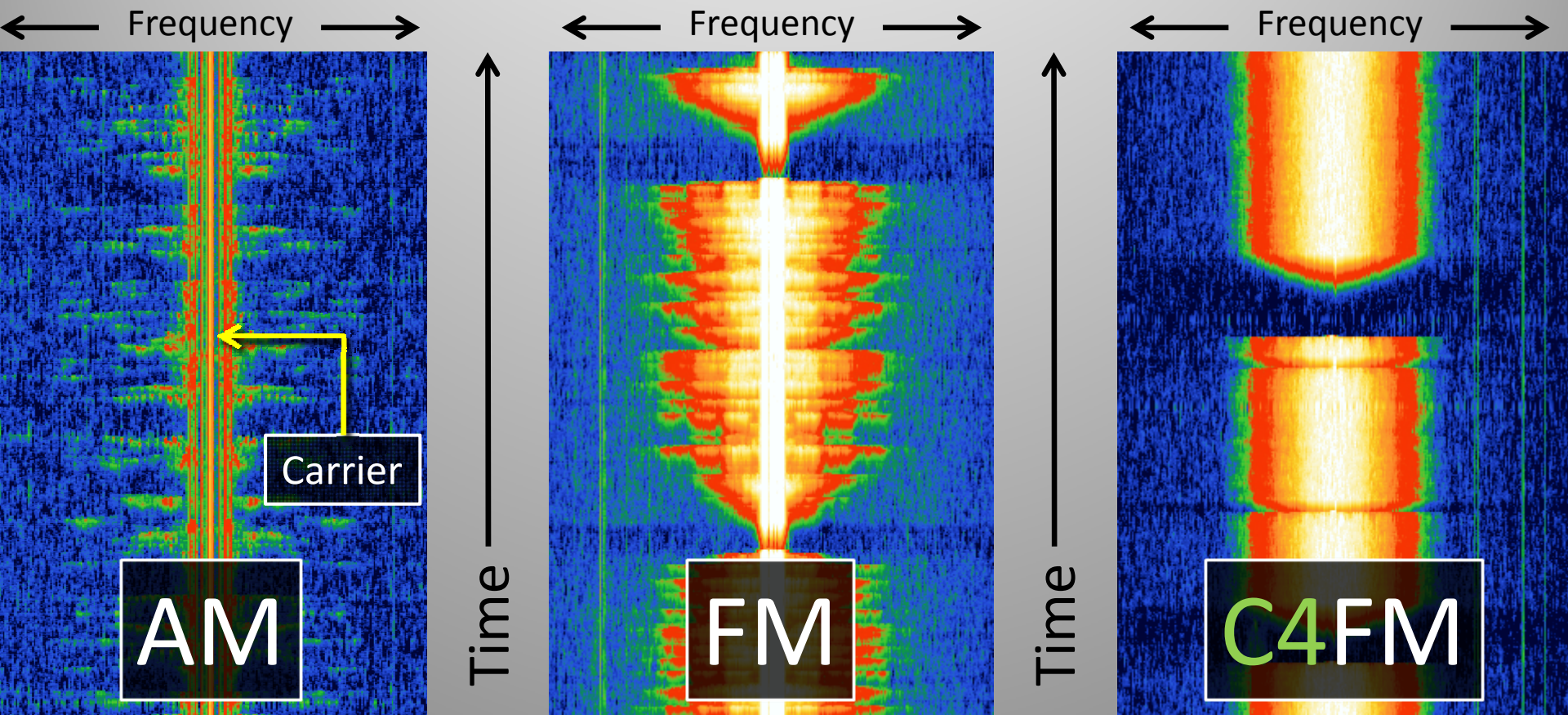
Constant frequency

In the Frequency Domain



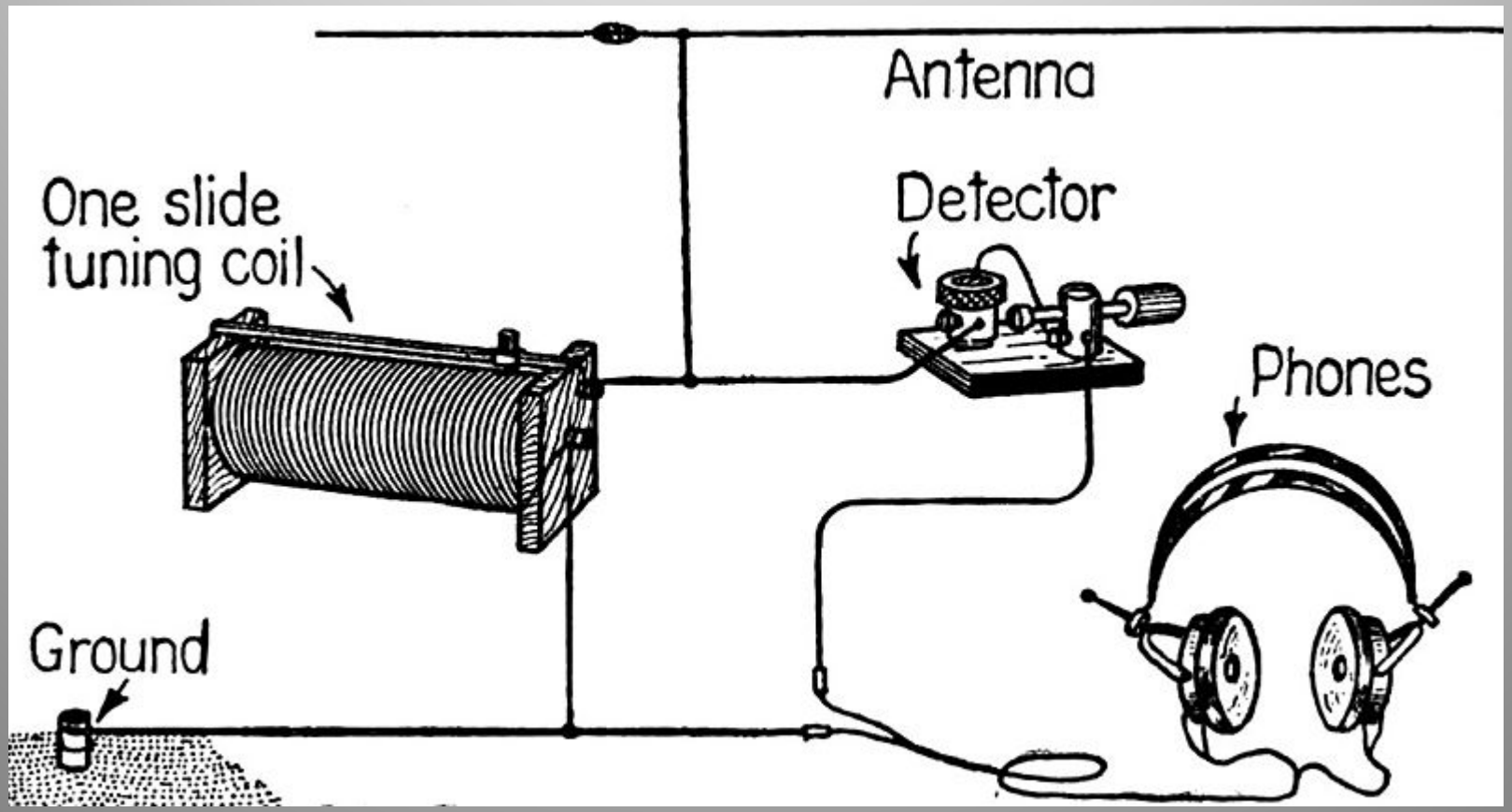
Modulation

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



Hardware

- Crystal set receiver
  - Powerful AM transmissions
-

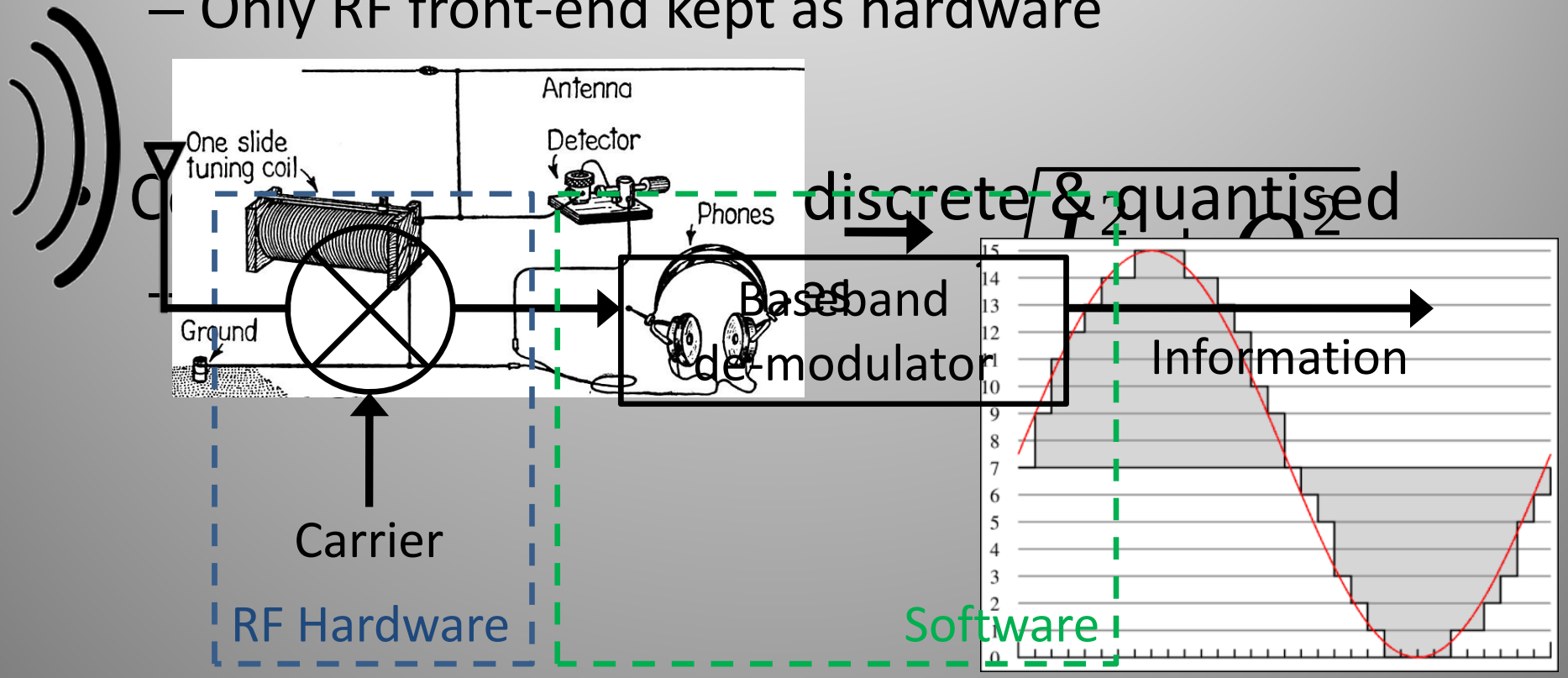


Modulation in Hardware

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

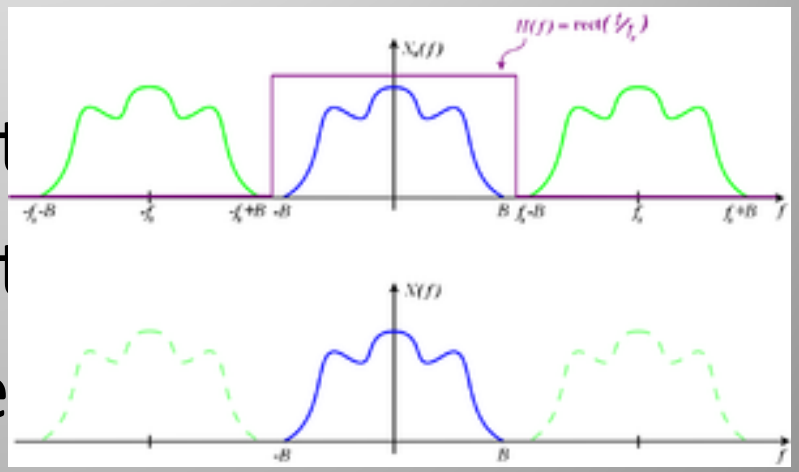
Software Defined Radio

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

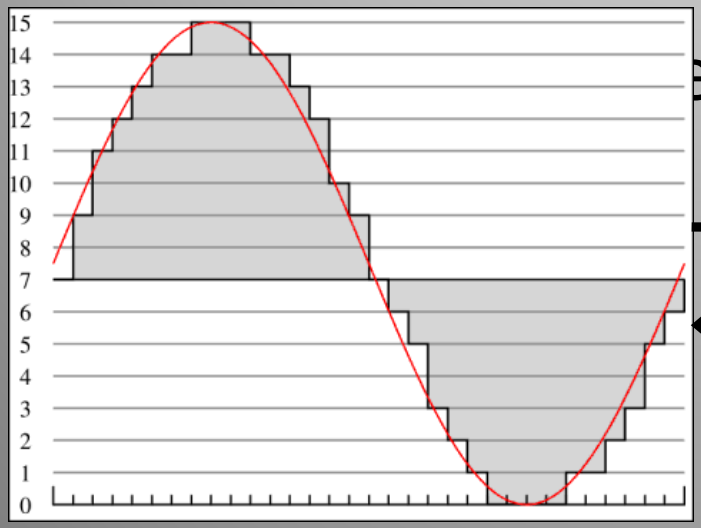


Sampling

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



etermine



ADC

DAC

7, 9, 11, 12, 13, 14, 14, 15, 15,
15, 14, 14, 13, 12, 10, 9, 7, …

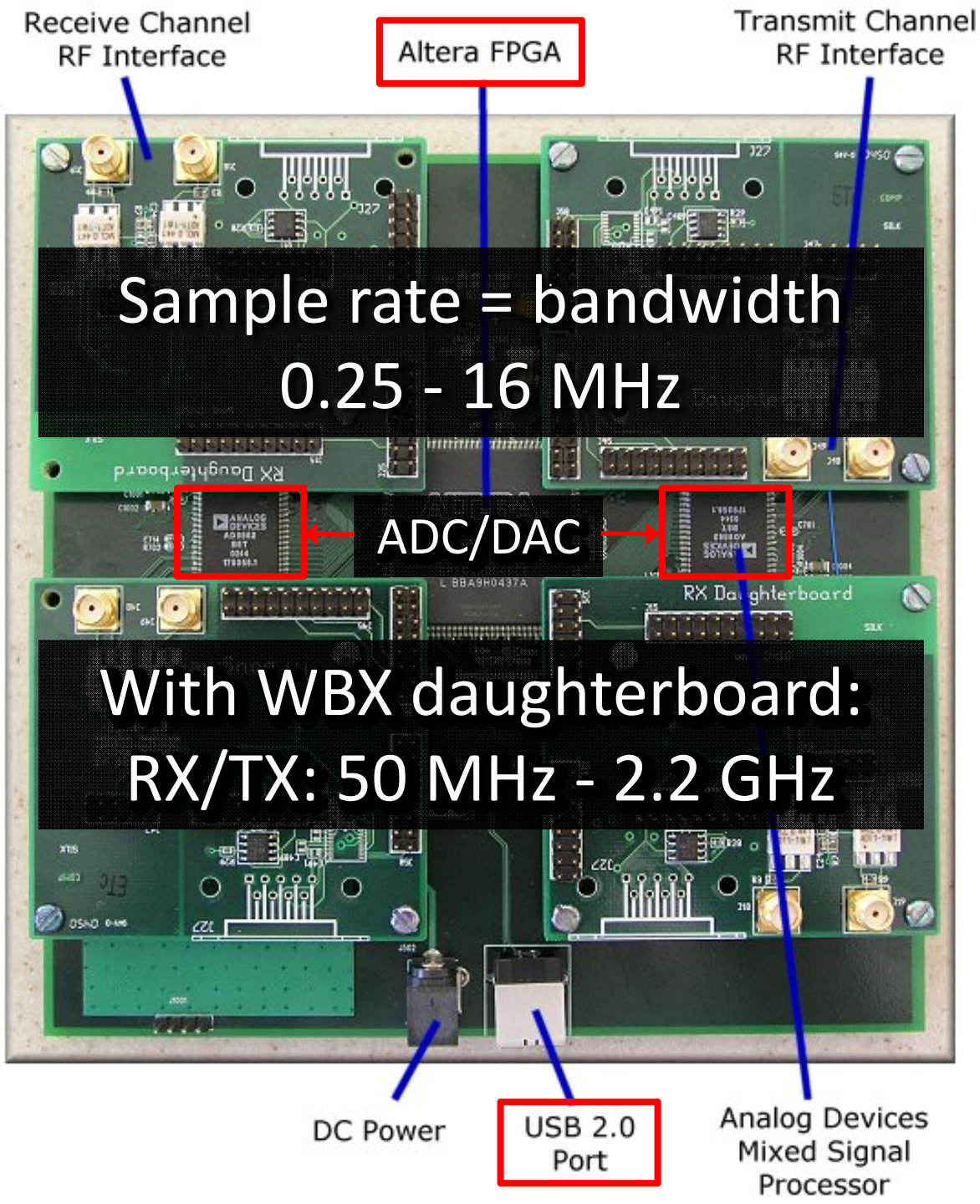
COTS SDRs

Open source? **No.**

The

Universal
Software
Radio
Peripheral

(USRP 1)



The FUNcube Dongle

Host Software

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

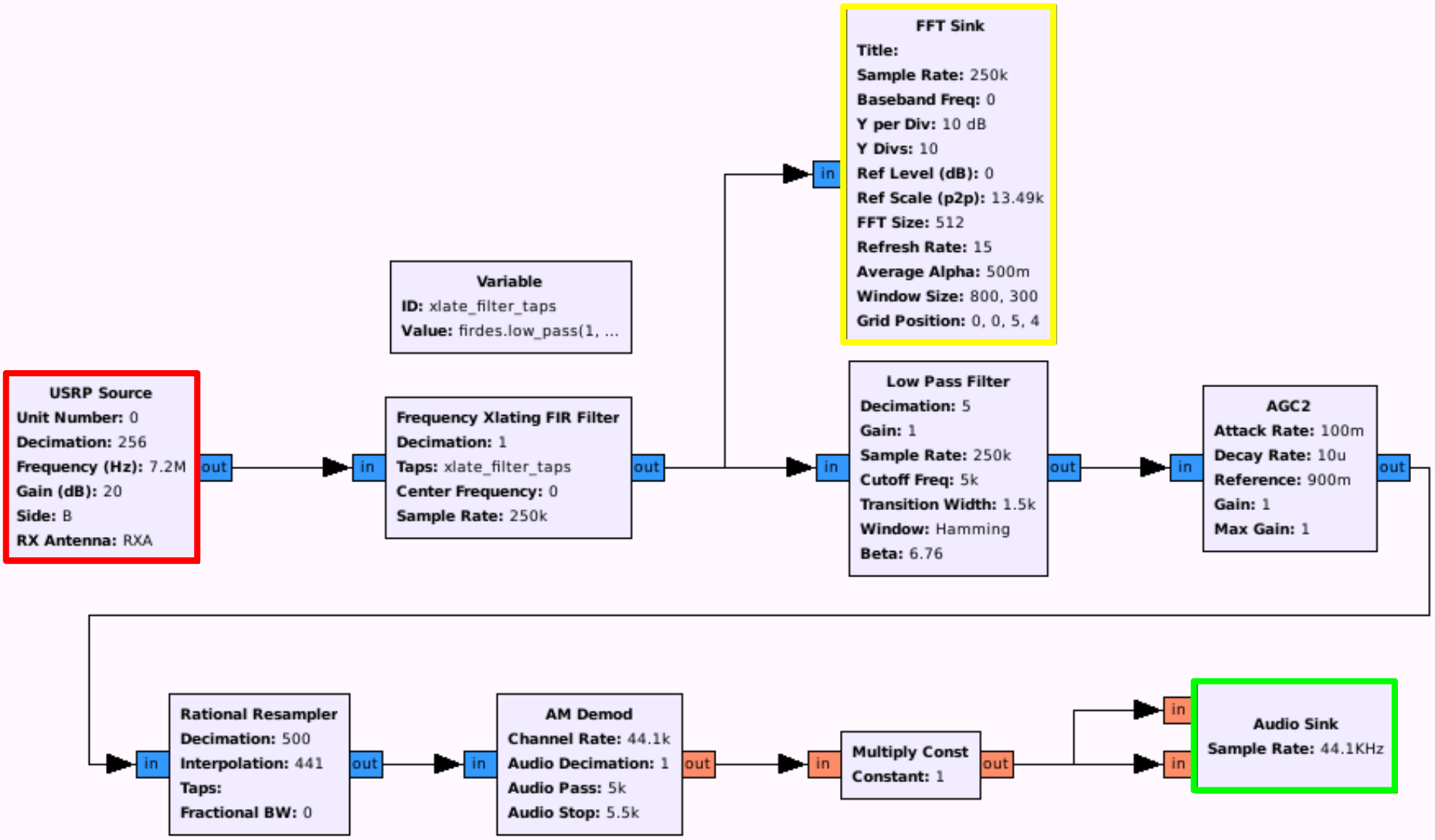
- Well-known platforms/programs:
  - LabVIEW
  - MATLAB Simulink

  Open source? **No.**

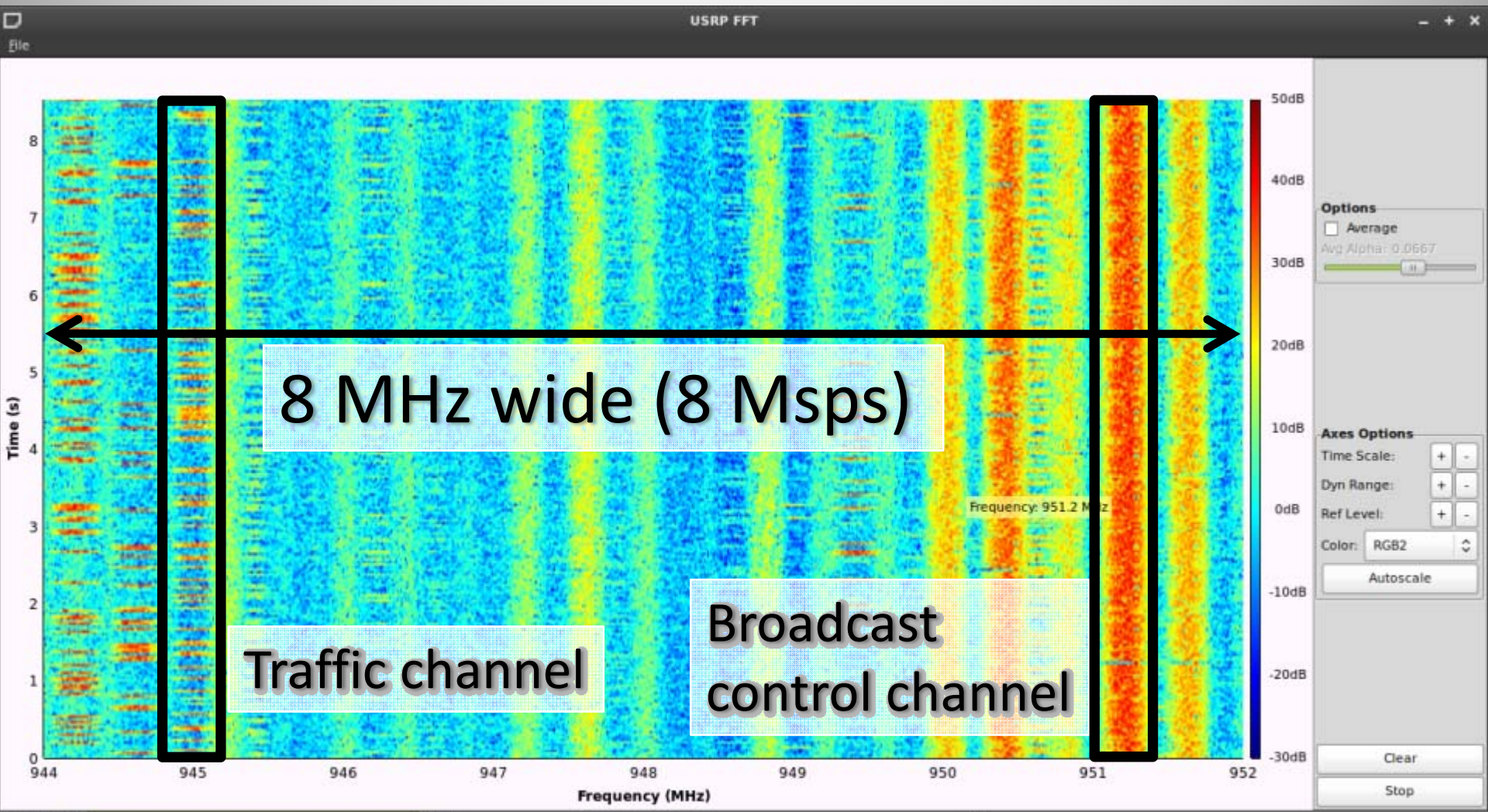
GNU **R**adio

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

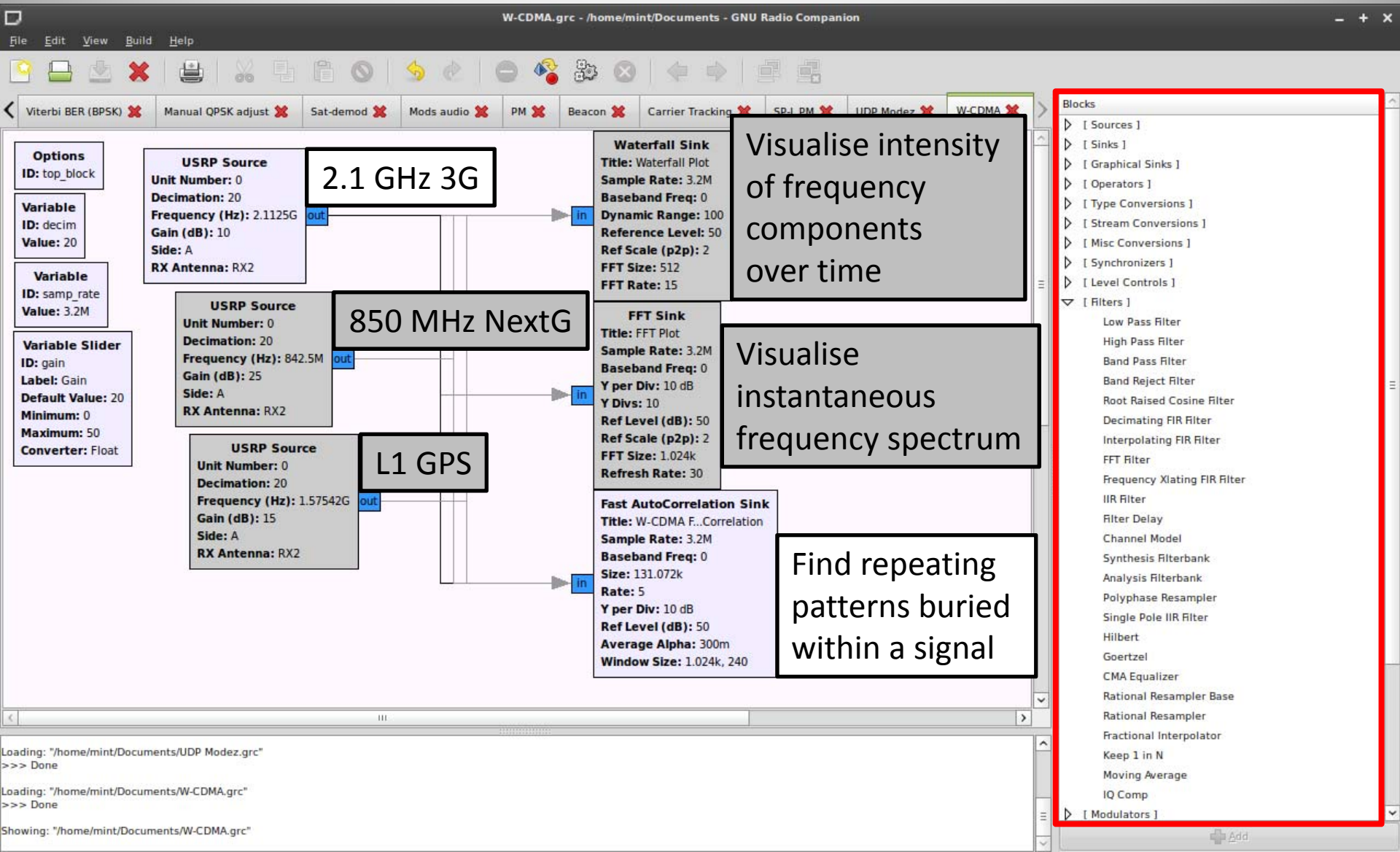
GNU Radio Companion



2G GSM Waterfall

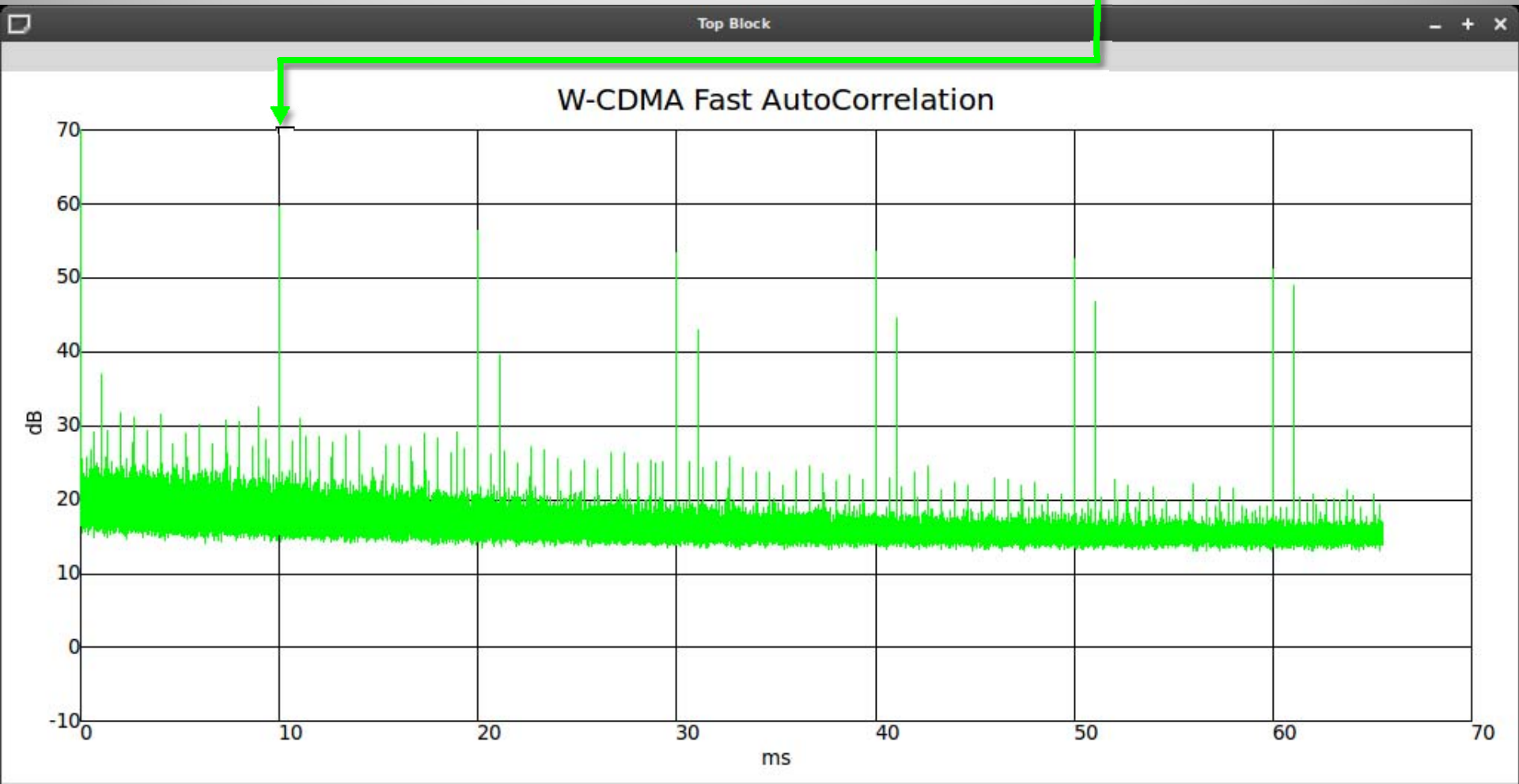


CDMA Detection with GRC

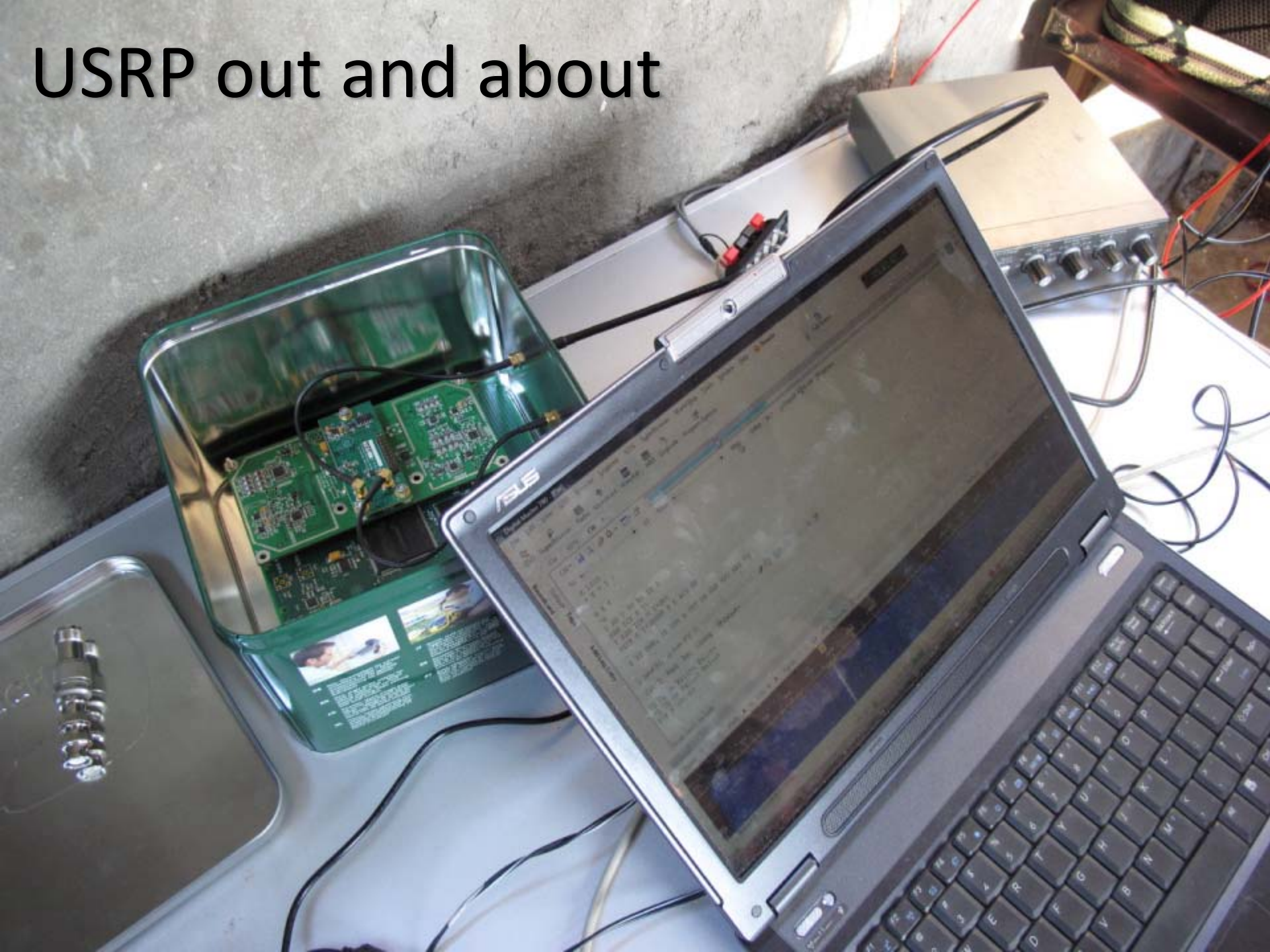


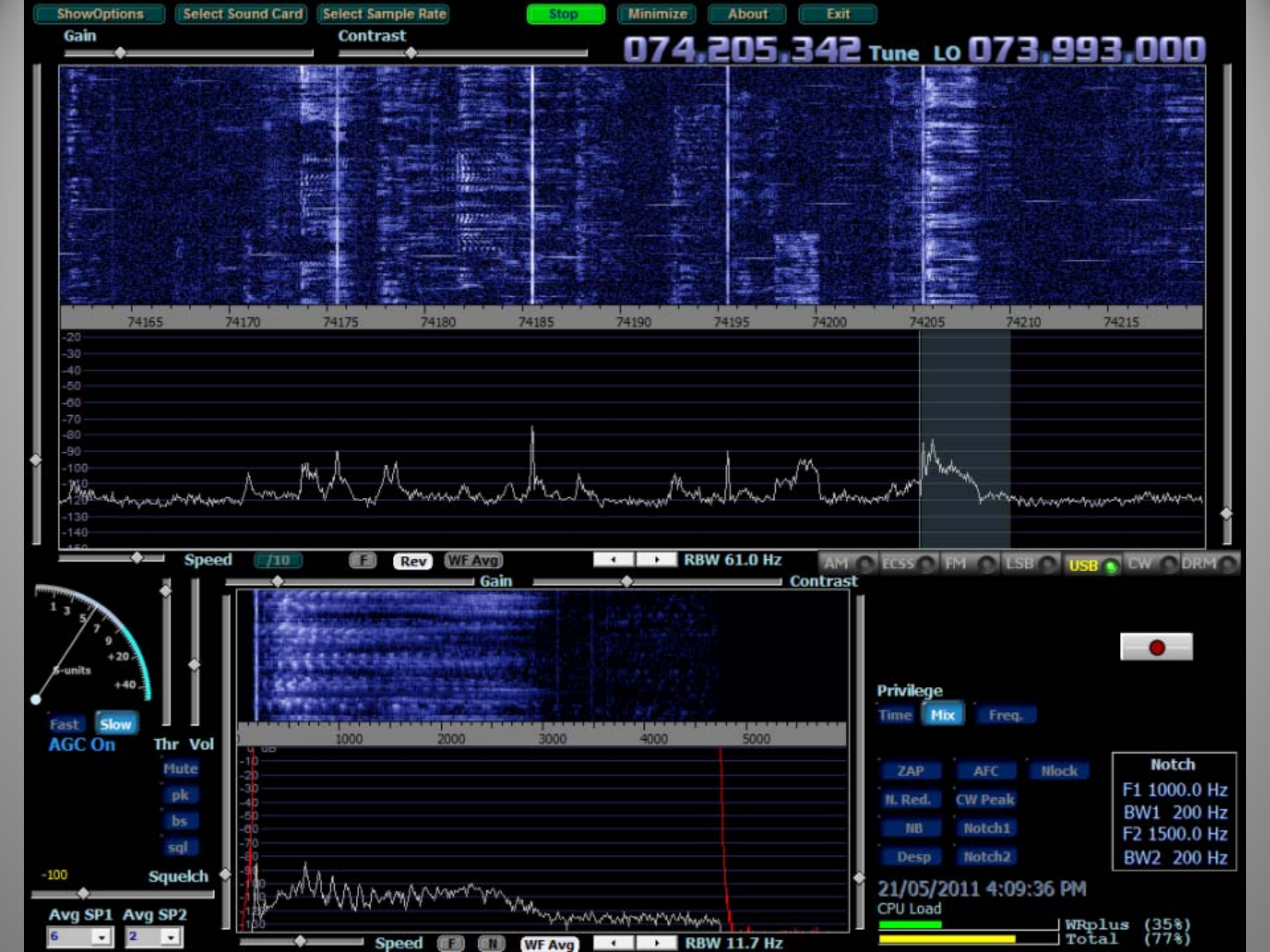
3G W-CDMA

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



USRP out and about




ShowOptions
Select Sound Card
Select Sample Rate
Stop
Minimize
About
Exit
Gain
Contrast
074.205.342 Tune LO 073,993,000
74165
74170
74175
74180
74185
74190
74195
74200
74205
74210
74215
-20
-30
-40
-50
-60
-70
-80
-90
-100
-110
-120
-130
-140
Speed
10
F
Rev
WF Avg
RBW 61.0 Hz
AM
ECSS
FM
LSB
USB
CW
DRM
Gain
Contrast
1
3
5
7
9
+20
+40
S-units
Fast
Slow
AGC On
Thr
Vol
Mute
pk
bs
sql
-100
Squelch
Avg SP1
Avg SP2
6
2
1000
2000
3000
4000
5000
Speed
F
N
WF Avg
RBW 11.7 Hz
Privilege
Time
Mix
Freq.
ZAP
AFC
Nlock
N. Red.
CW Peak
NB
Notch1
Desp
Notch2
Notch
F1 1000.0 Hz
BW1 200 Hz
F2 1500.0 Hz
BW2 200 Hz
21/05/2011 4:09:36 PM
CPU Load
WRplus (35%)
Total (77%)

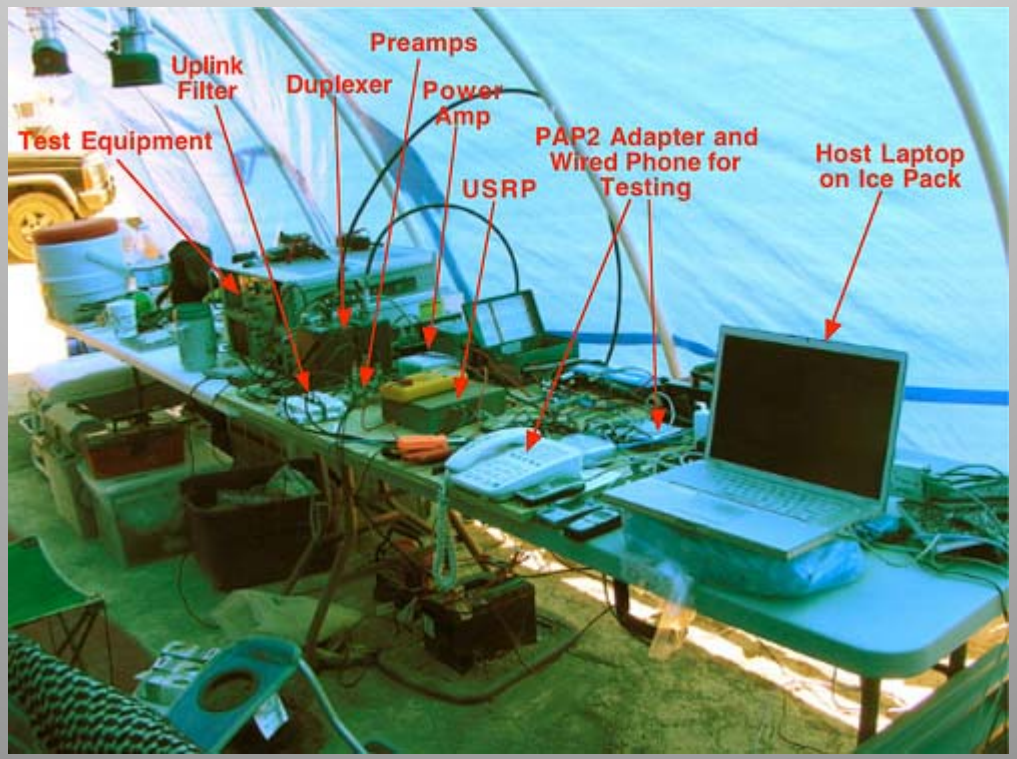
Applications of SDR

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

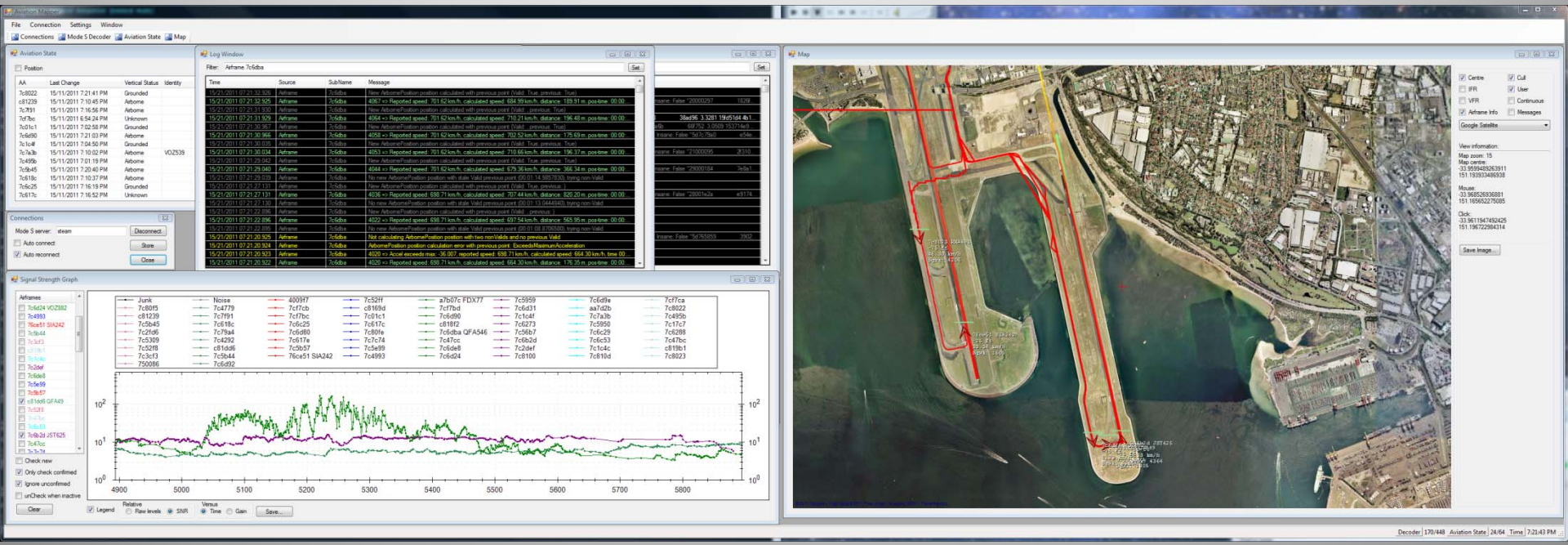
- Much more…

OpenBTS

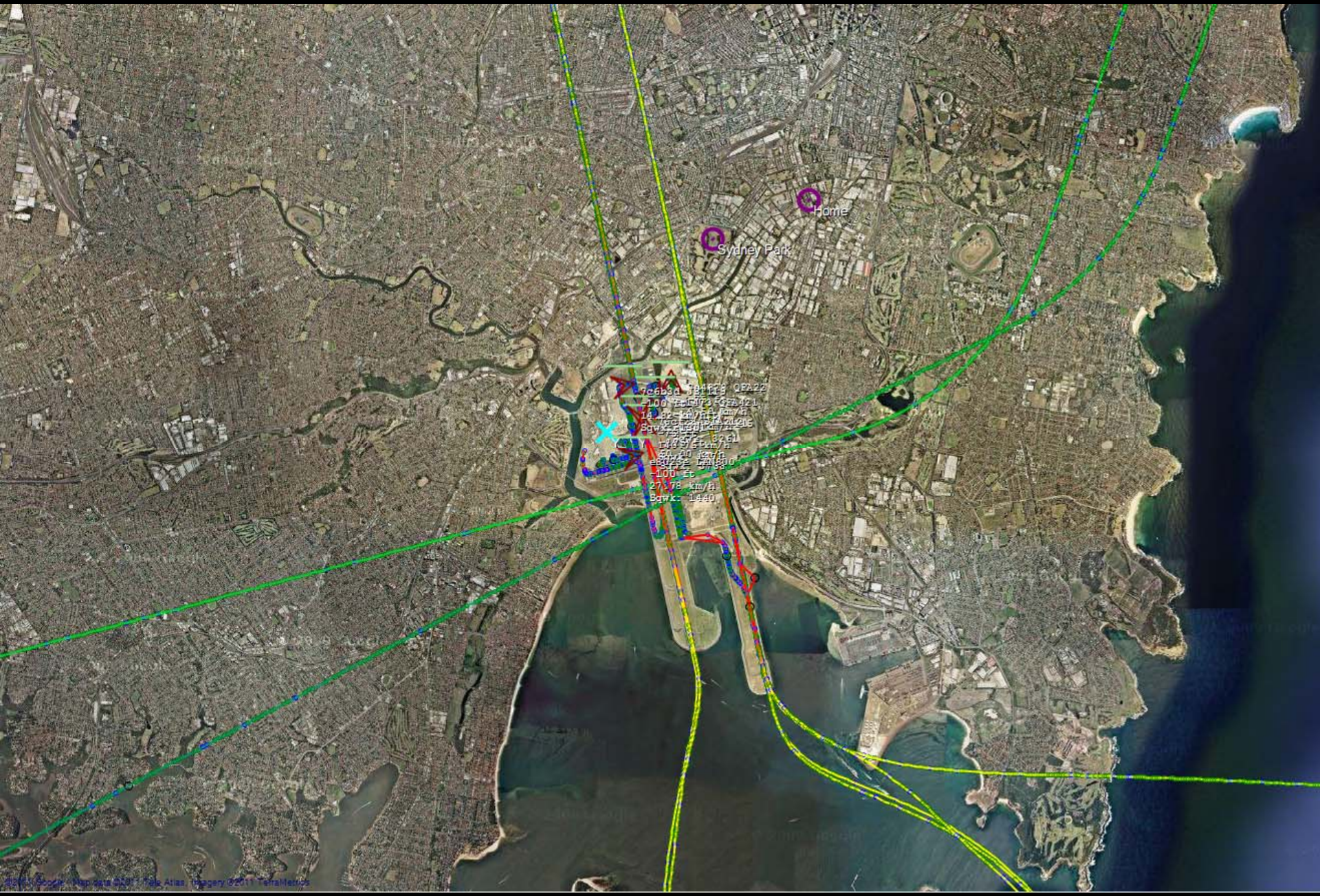
- Open-source 2G GSM stack
  - Asterix softswitch (PBX)
  - VoIP backhaul

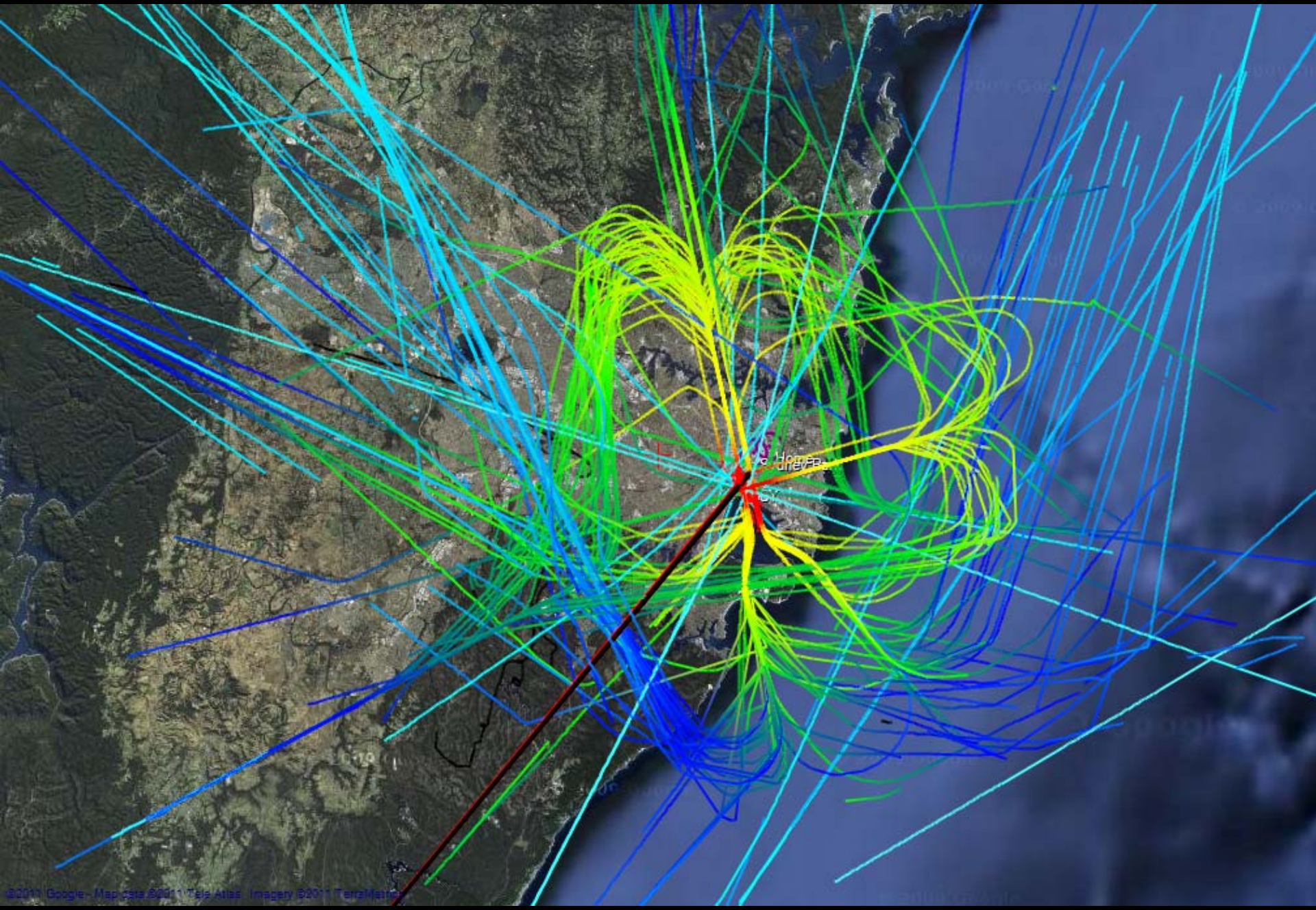


Tracking Aircraft: “Modez”

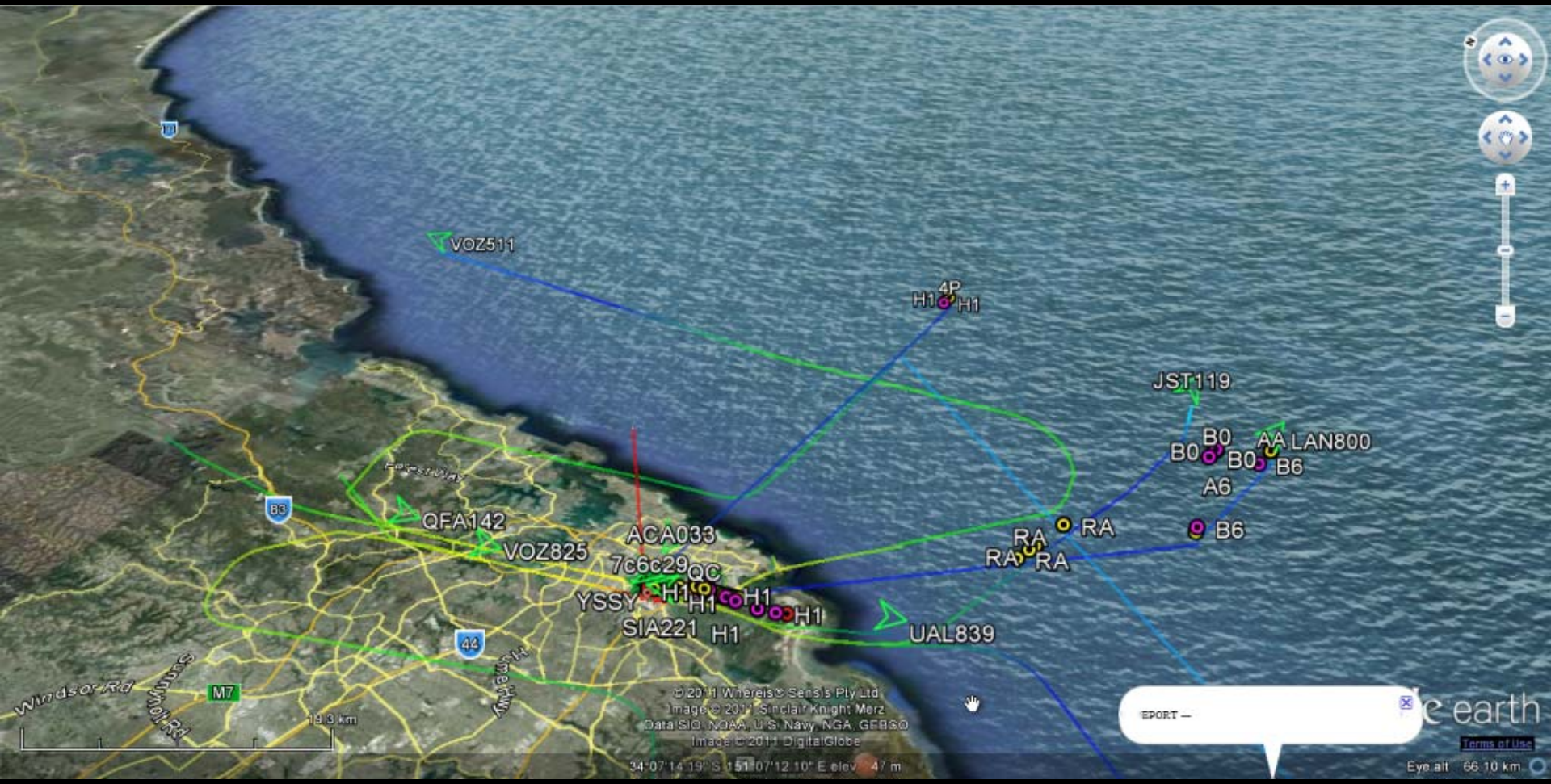


AviationMapper


Home
Sydney Park


©2011 Google - Map data ©2011 Tele Atlas Imagery ©2011 TerraMetrics


- #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

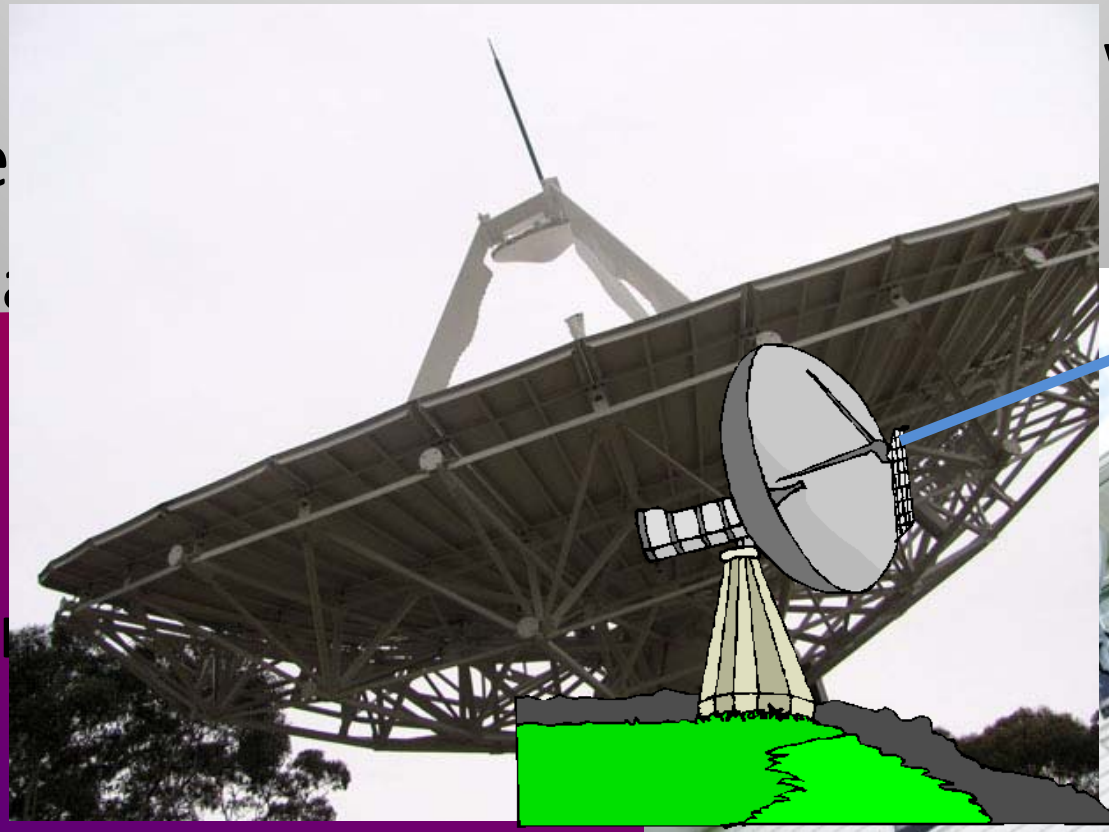

VOZ511
4P
H1
H1
JST119
B0
B0
B0
AA
LAN800
B6
A6
B6
RA
RA
RA
RA
QFA142
VOZ825
ACA033
7c6c29
QC
YSSY
H1
H1
H1
H1
SIA221
H1
UAL839
B3
44
M7
Windsor Rd
Pennant Hills Rd
Hills Hwy
19.3 km
© 2011 Whereis® Sensis Pty Ltd
Image © 2011 Sinclair Knight Merz
Data SIO, NOAA, U.S. Navy, NGA, GEBCO
Image © 2011 DigitalGlobe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

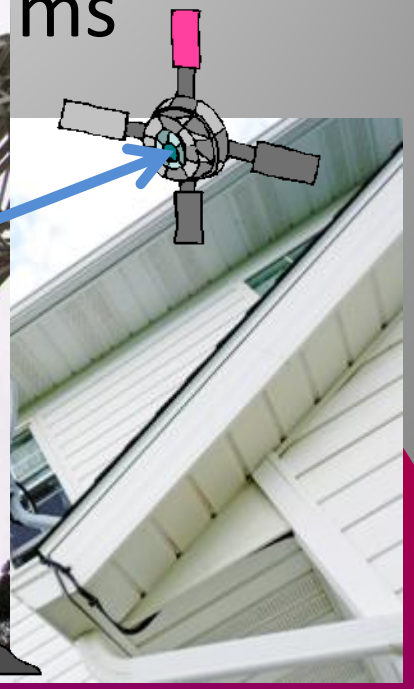
Satellite **Com**munications

- 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

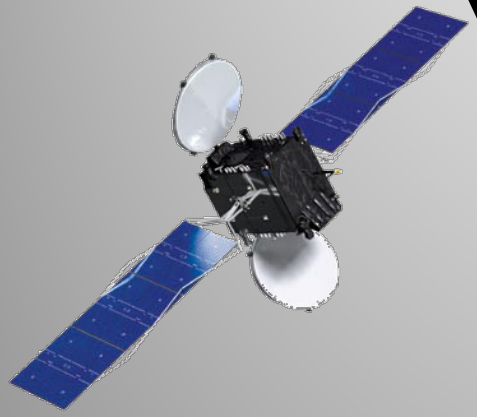




What you need

Dish + LNB + power injector + USRP + GNU Radio

(set-top box with LNB-thru)

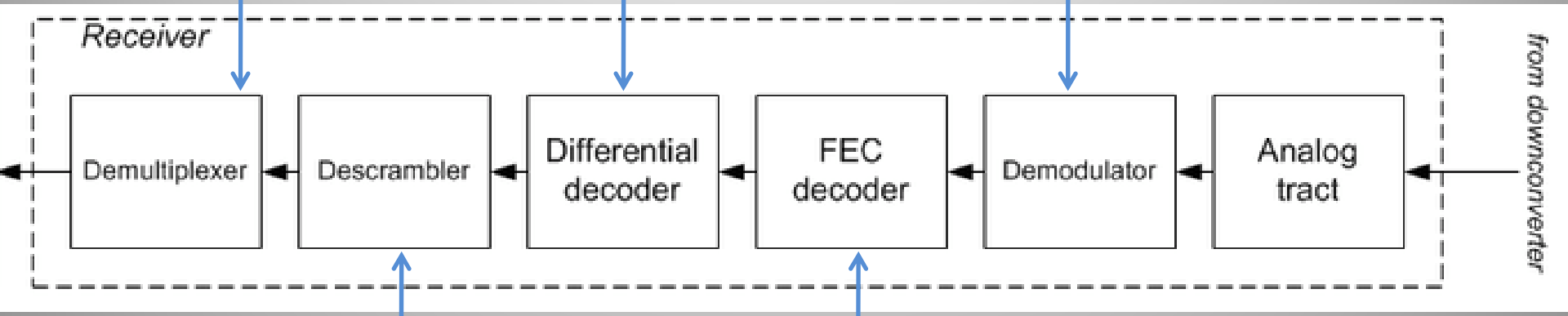


Demodulation: easy when you know

Are there multiple streams?
How are they multiplexed?

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

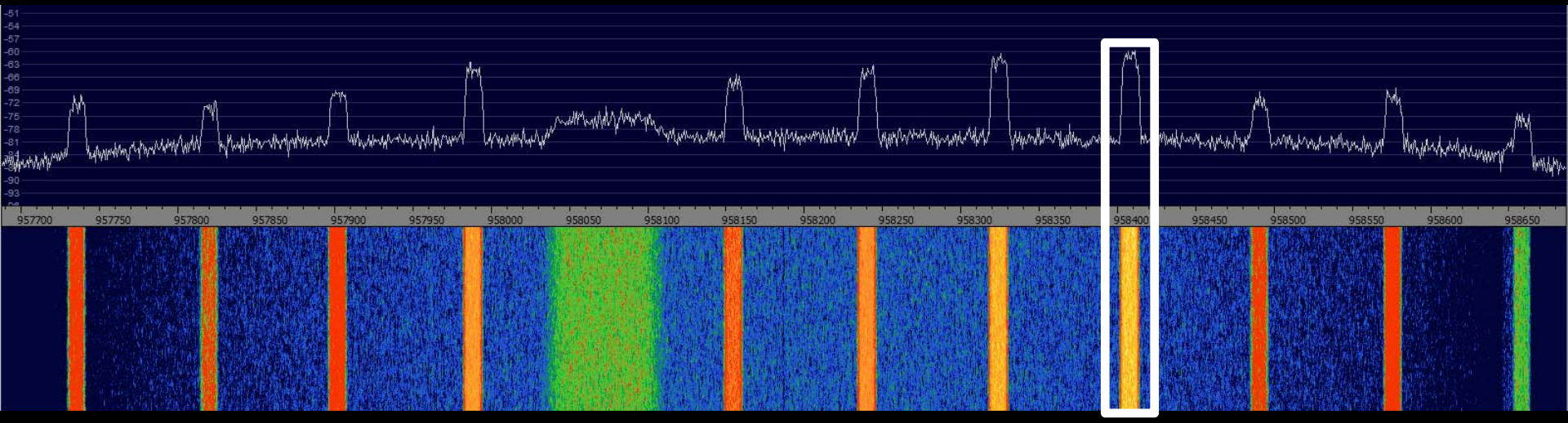
What is the modulation?
Symbol rate? Require coherence?
What is the phase difference?
Need to conjugate complex plane?



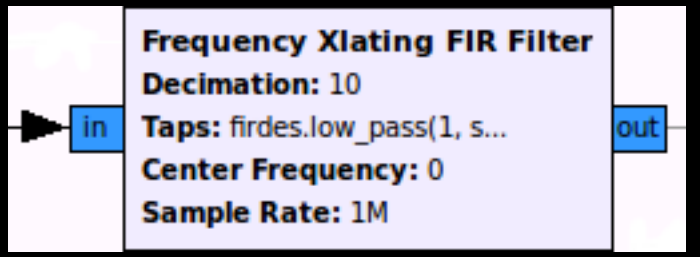
Possible to determine if it is scrambled
(calculate stats), but what is the scrambler?
Is it additive or multiplicative?
How is it synchronised?

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

Let’s try one…

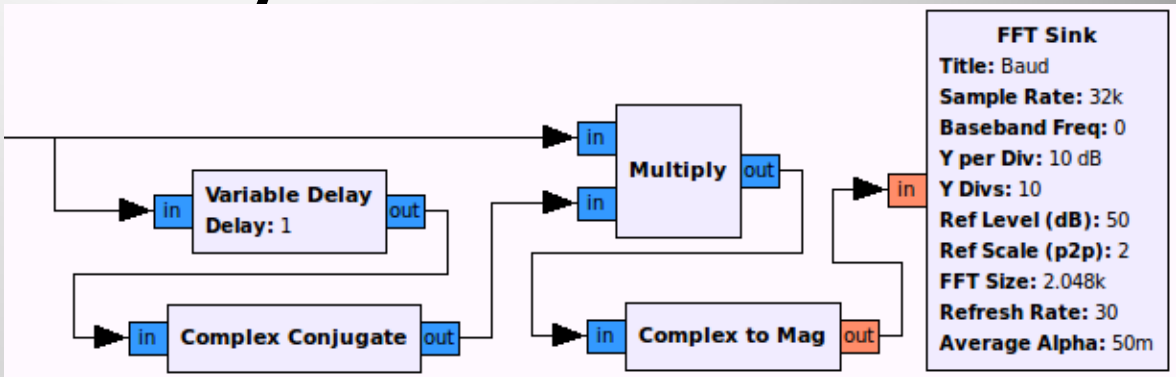


- Feed entire baseband spectrum into GR
- Perform ‘channel selection’ to isolate stream of interest (create new baseband centred on stream)

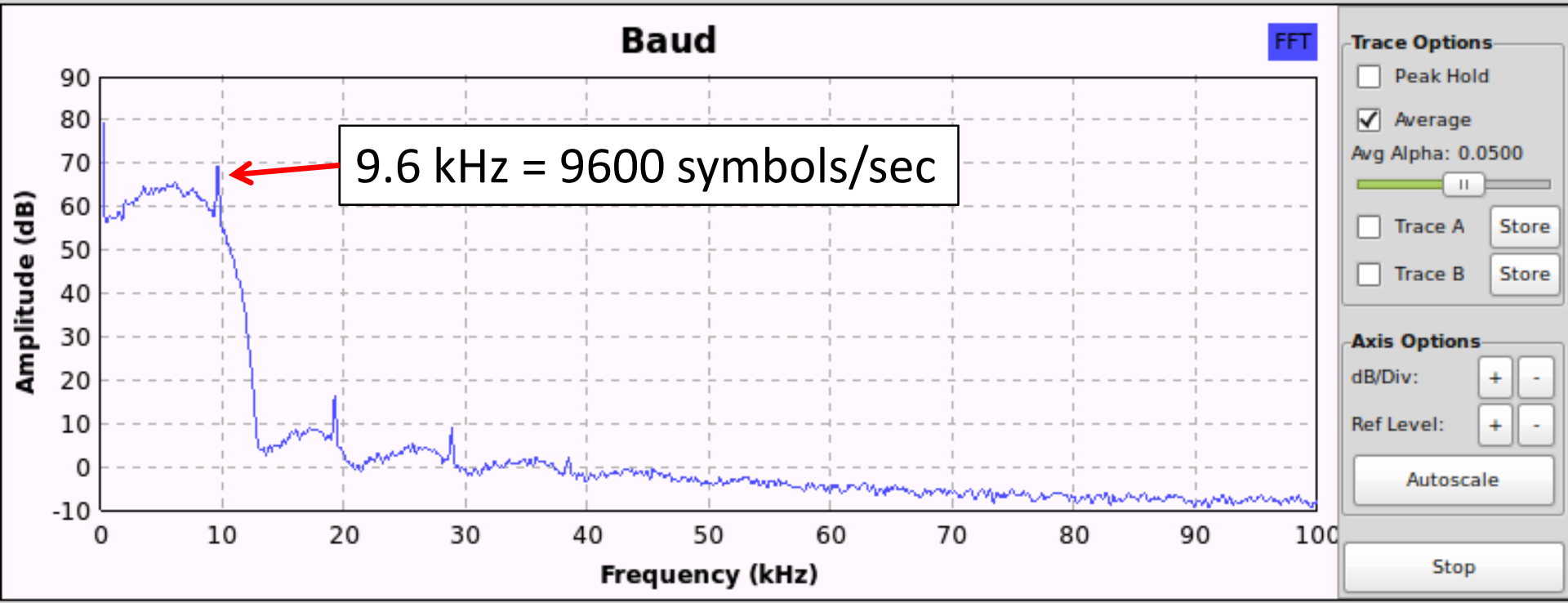


Determine Symbol Rate

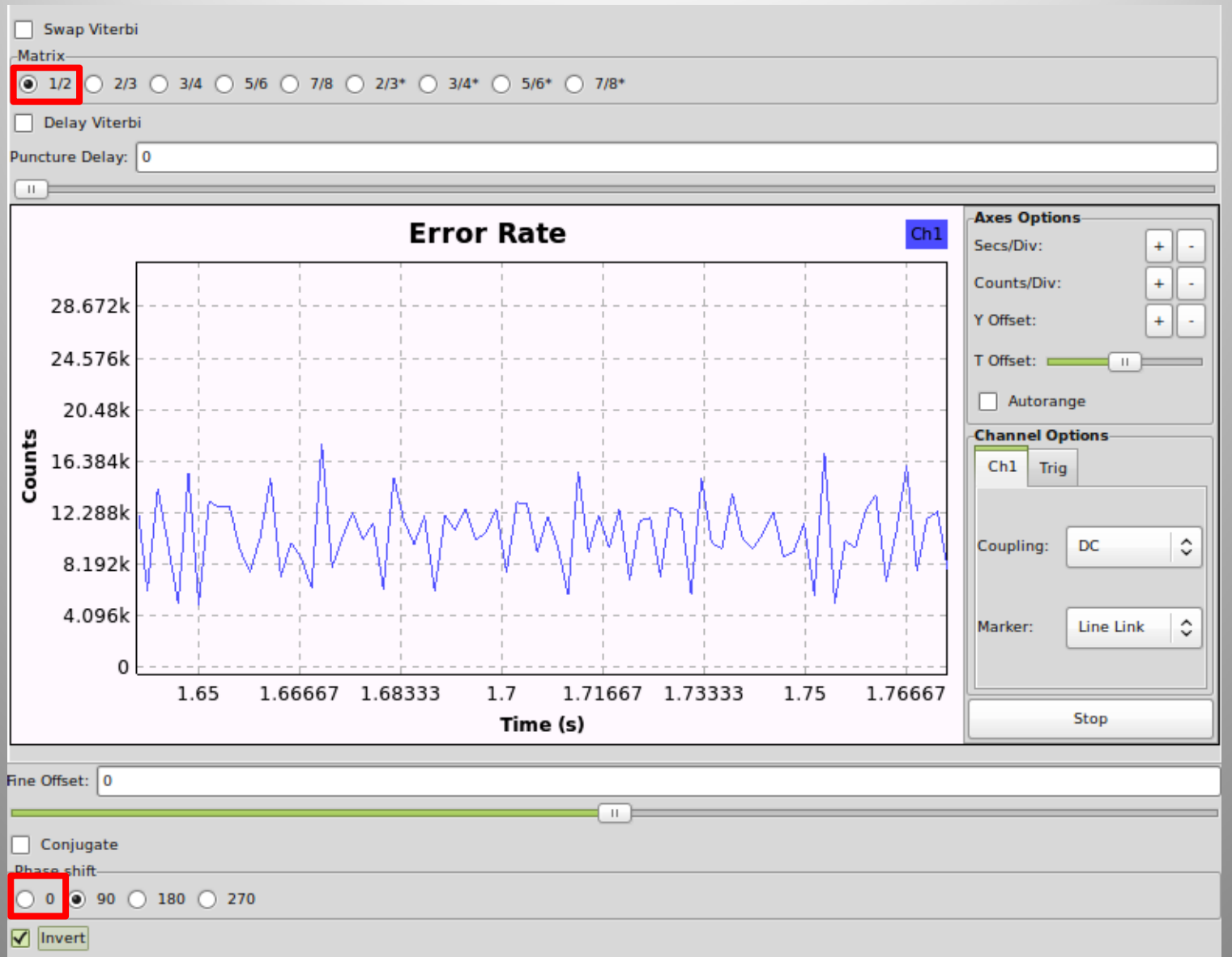
- Find first peak

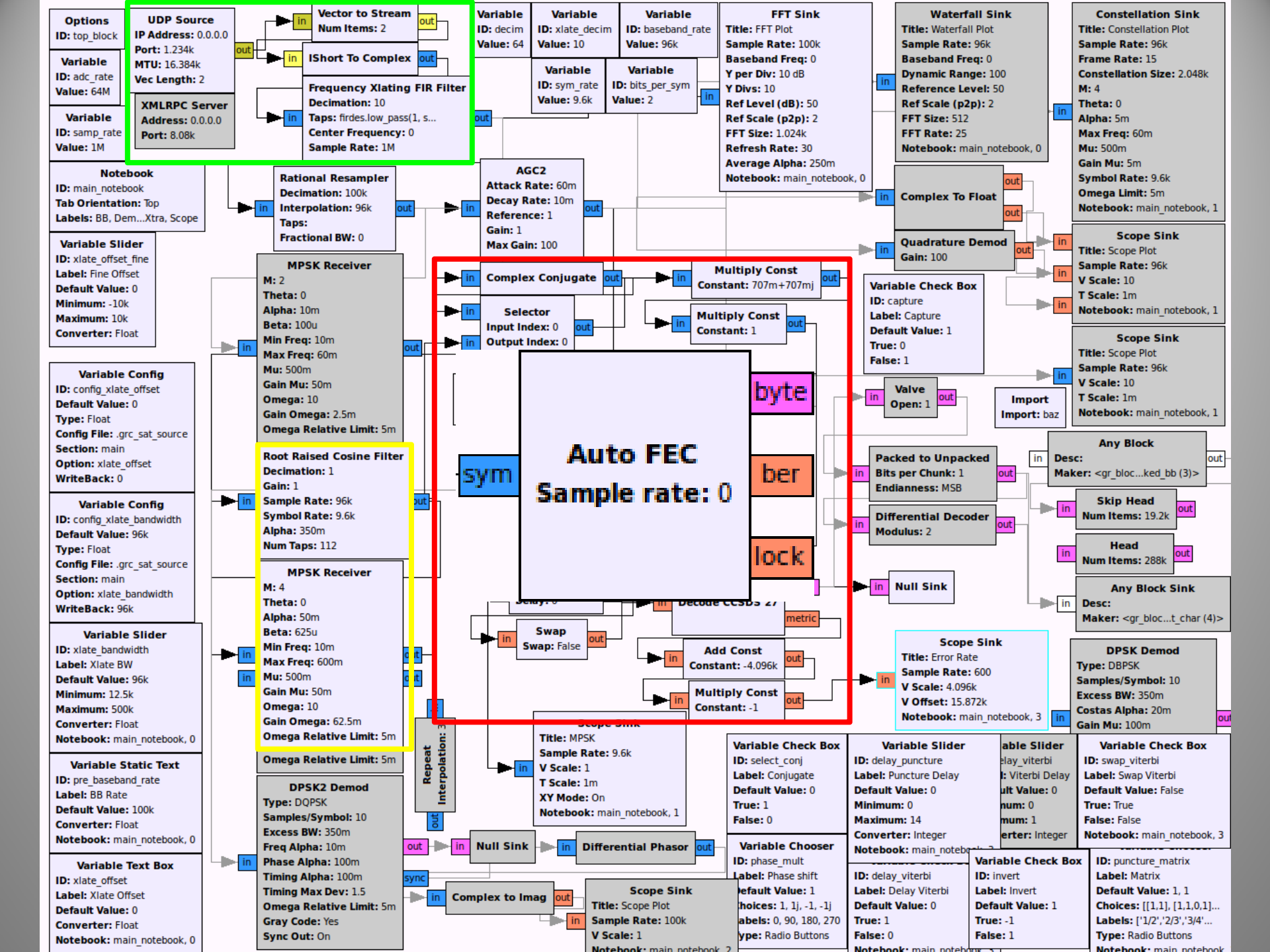


Nominal samples per symbol: 2



Try synchronisation & FEC



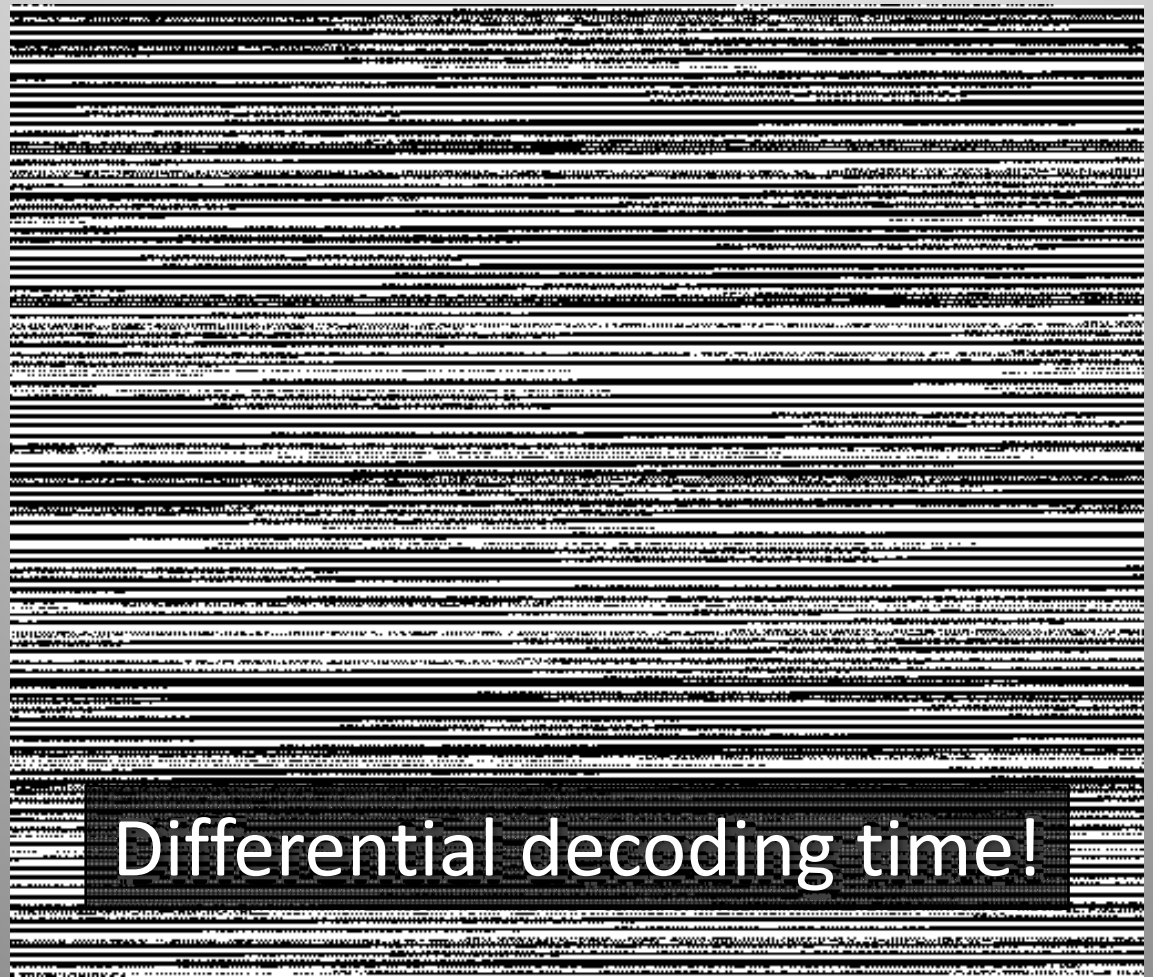

Options
ID: top_block
Variable
ID: adc_rate
Value: 64M
Variable
ID: samp_rate
Value: 1M
UDP Source
IP Address: 0.0.0.0
Port: 1.234k
MTU: 16.384k
Vec Length: 2
XMLRPC Server
Address: 0.0.0.0
Port: 8.08k
Vector to Stream
Num Items: 2
IShort To Complex
Frequency Xlating FIR Filter
Decimation: 10
Taps: firdes.low_pass(1, s...
Center Frequency: 0
Sample Rate: 1M
Variable
ID: decim
Value: 64
Variable
ID: xlate_decim
Value: 10
Variable
ID: baseband_rate
Value: 96k
Variable
ID: sym_rate
Value: 9.6k
Variable
ID: bits_per_sym
Value: 2
FFT Sink
Title: FFT Plot
Sample Rate: 100k
Baseband Freq: 0
Y per Div: 10 dB
Y Divs: 10
Ref Level (dB): 50
Ref Scale (p2p): 2
FFT Size: 1.024k
Refresh Rate: 30
Average Alpha: 250m
Notebook: main_notebook, 0
Waterfall Sink
Title: Waterfall Plot
Sample Rate: 96k
Baseband Freq: 0
Dynamic Range: 100
Reference Level: 50
Ref Scale (p2p): 2
FFT Size: 512
FFT Rate: 25
Notebook: main_notebook, 0
Constellation Sink
Title: Constellation Plot
Sample Rate: 96k
Frame Rate: 15
Constellation Size: 2.048k
M: 4
Theta: 0
Alpha: 5m
Max Freq: 60m
Mu: 500m
Gain Mu: 5m
Symbol Rate: 9.6k
Omega Limit: 5m
Notebook: main_notebook, 1
Notebook
ID: main_notebook
Tab Orientation: Top
Labels: BB, Dem...Xtra, Scope
Rational Resampler
Decimation: 100k
Interpolation: 96k
Taps:
Fractional BW: 0
AGC2
Attack Rate: 60m
Decay Rate: 10m
Reference: 1
Gain: 1
Max Gain: 100
Complex To Float
Quadrature Demod
Gain: 100
Scope Sink
Title: Scope Plot
Sample Rate: 96k
V Scale: 10
T Scale: 1m
Notebook: main_notebook, 1
Variable Slider
ID: xlate_offset_fine
Label: Fine Offset
Default Value: 0
Minimum: -10k
Maximum: 10k
Converter: Float
MPSK Receiver
M: 2
Theta: 0
Alpha: 10m
Beta: 100u
Min Freq: 10m
Max Freq: 60m
Mu: 500m
Gain Mu: 50m
Omega: 10
Gain Omega: 2.5m
Omega Relative Limit: 5m
Complex Conjugate
Selector
Input Index: 0
Output Index: 0
Multiply Const
Constant: 707m+707mj
Multiply Const
Constant: 1
Variable Check Box
ID: capture
Label: Capture
Default Value: 1
True: 0
False: 1
Valve
Open: 1
Import
Import: baz
Variable Config
ID: config_xlate_offset
Default Value: 0
Type: Float
Config File: .grc_sat_source
Section: main
Option: xlate_offset
WriteBack: 0
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
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

Visualisation

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

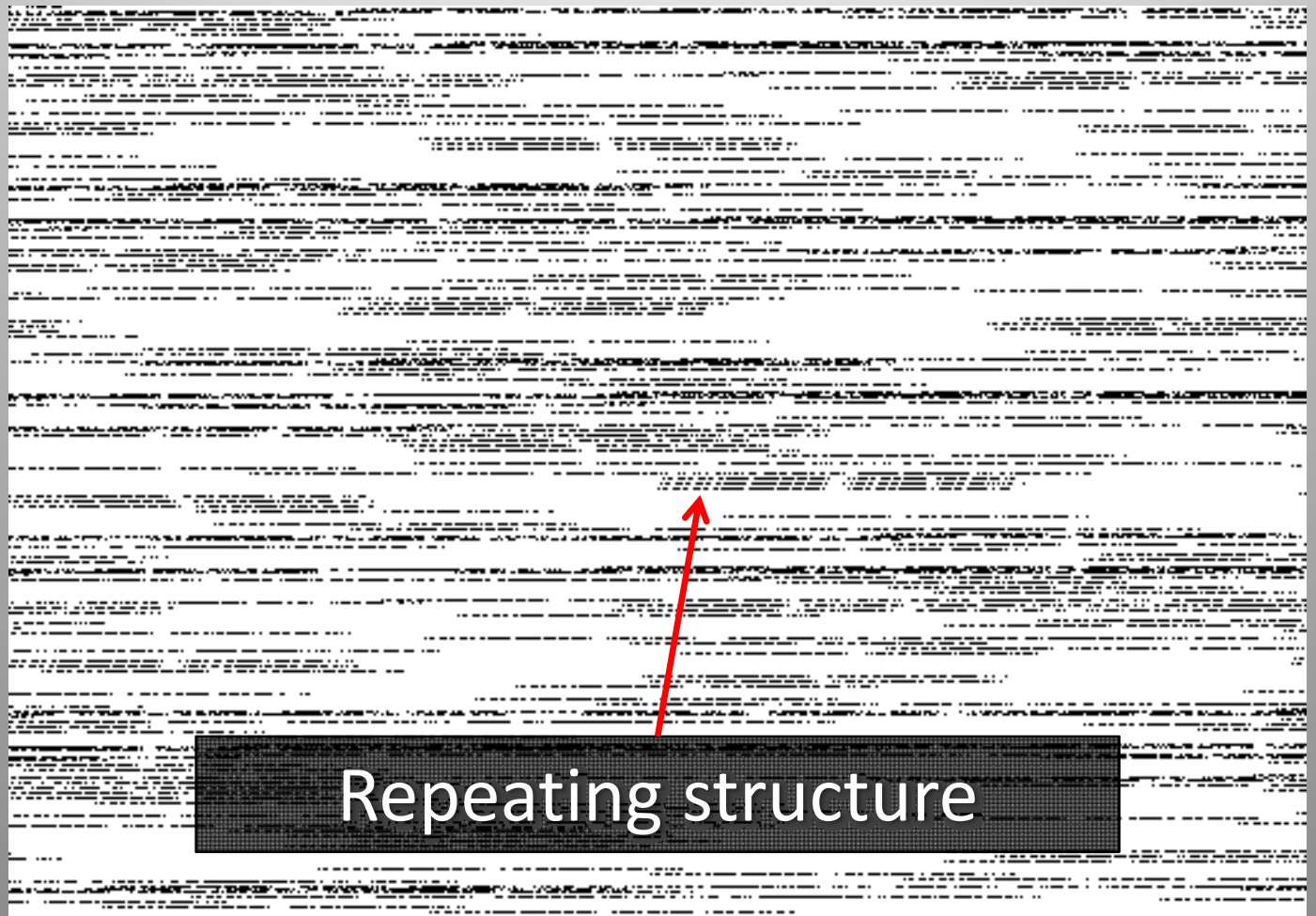
De-scrambled

- 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

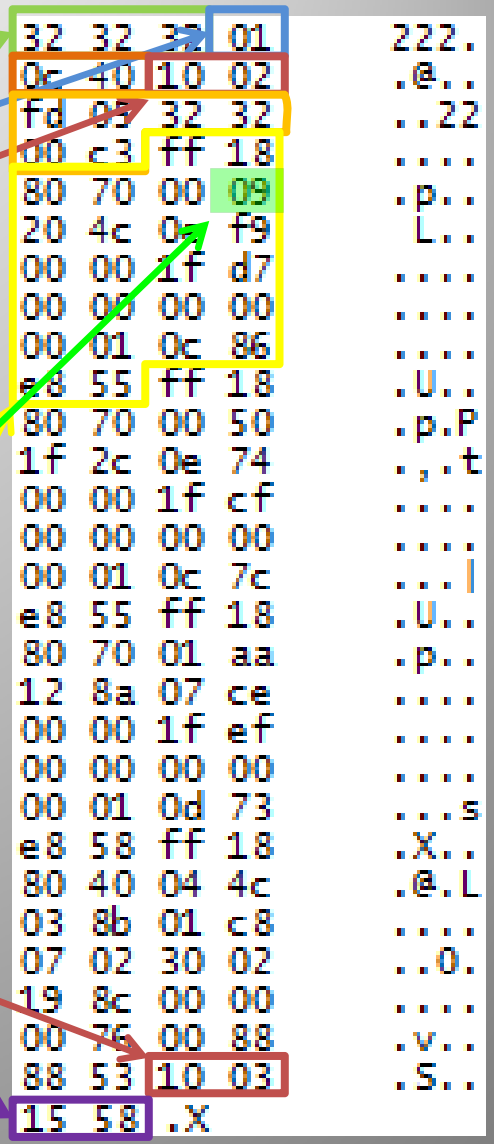
```
38 bits #0000-0006[+0004, /0000]: 00000010000010000100000010111111000000 (fd021040)
38 bits #0000-0172[+0166, /0000]: 111111010011000100110001001100100000000 (4c8c8cbf)

37 bits #0002-0002[+0000, /0000]: 11101100000001110101101100000001000000 (40dae037)
37 bits #0002-0002[+0000, /0000]: 10110100101111011010000001000110000000 (6205bd2d)
```

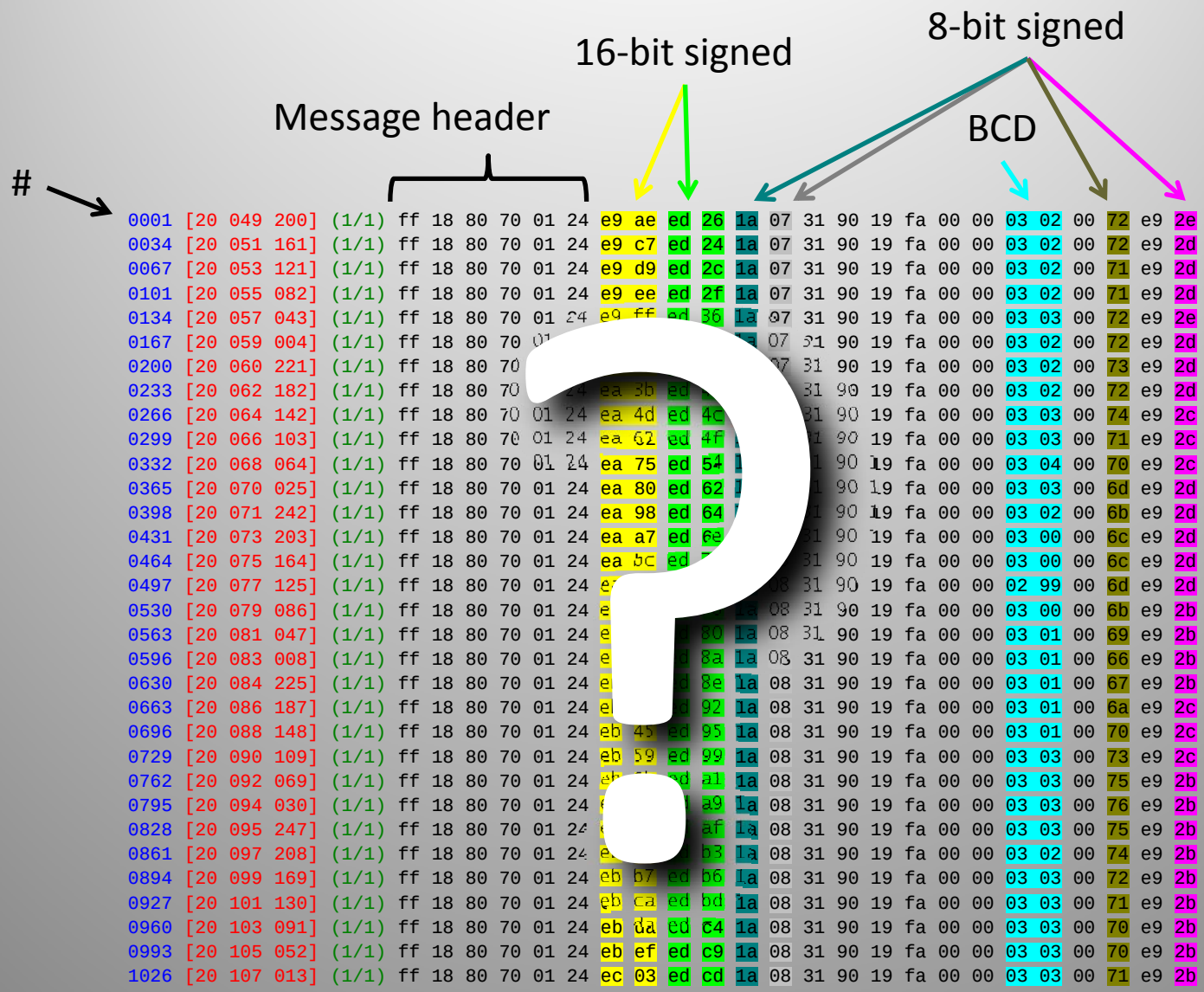
Preceding 1s are just part of ‘idle’ stream when no data is being sent

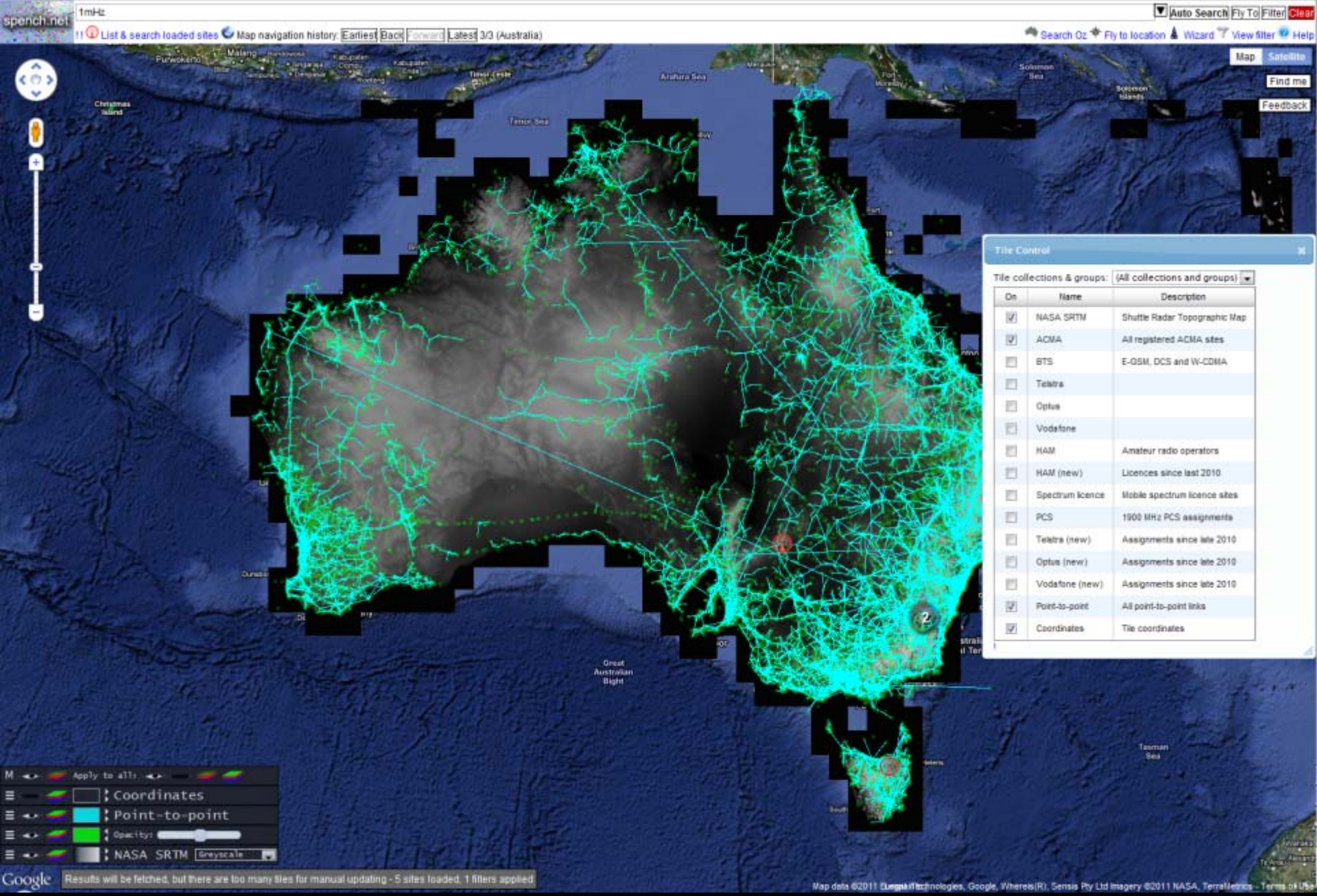
Frame analysis

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

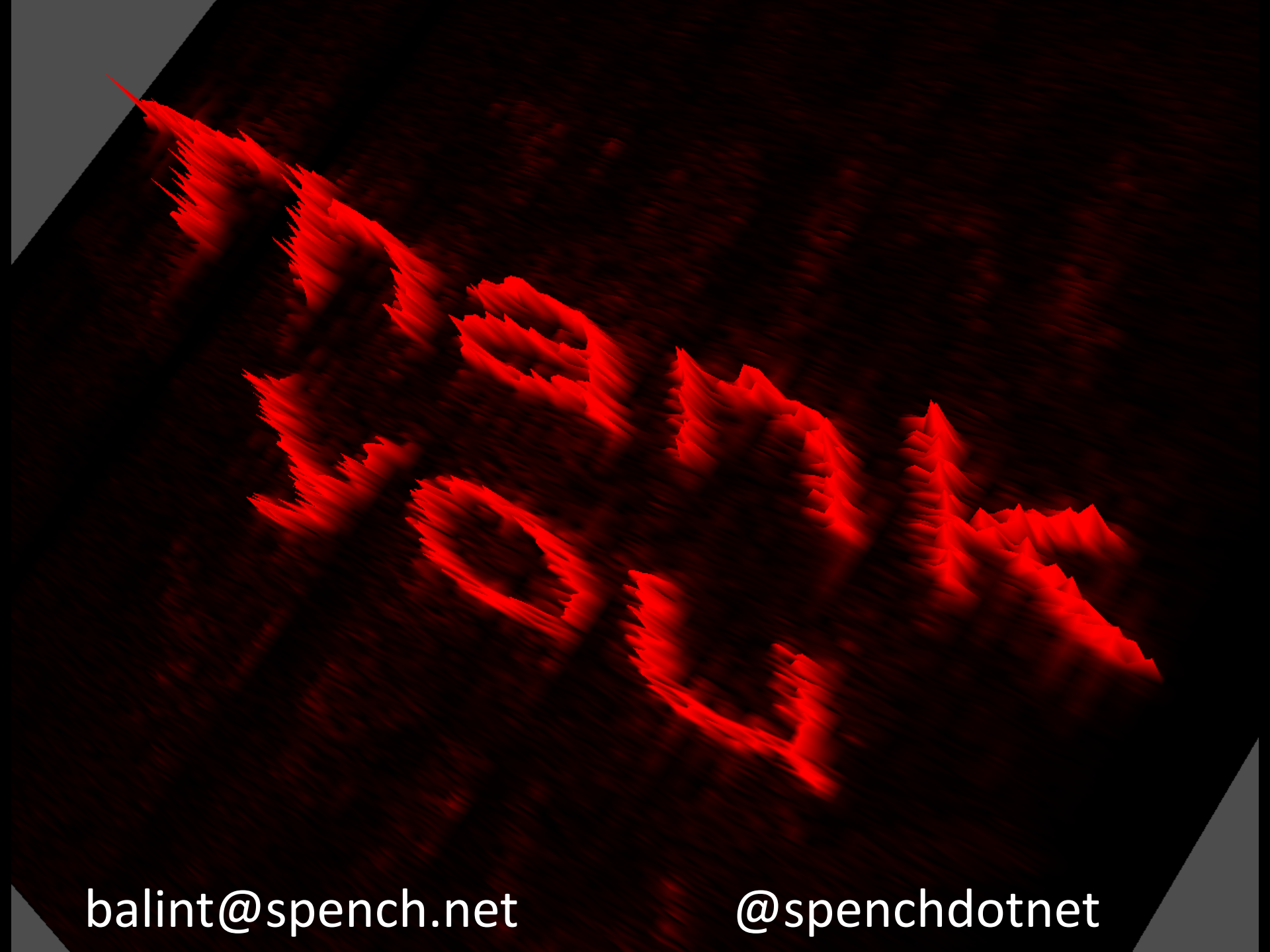


Un-pack & find patterns





The RFMap web interface



balint@spench.net @spenchdotnet