

Preview:

Hacking the Wireless World with Software Defined Radio – 2.0

Balint Seeber

Applications Specialist & SDR Evangelist

balint@ettus.com

balint@spenchnet

@spenchnet

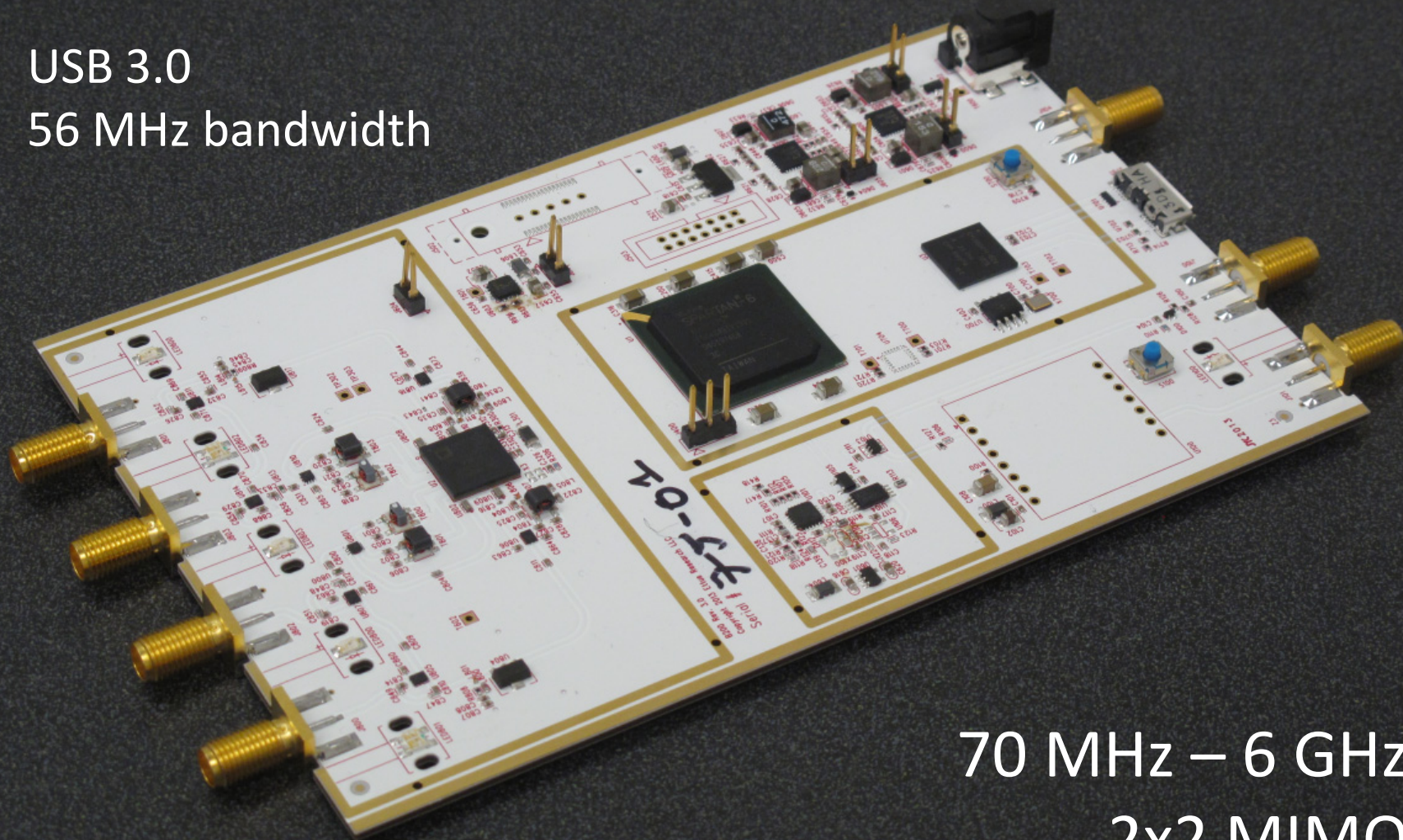




USRP B210

USB 3.0

56 MHz bandwidth



70 MHz – 6 GHz

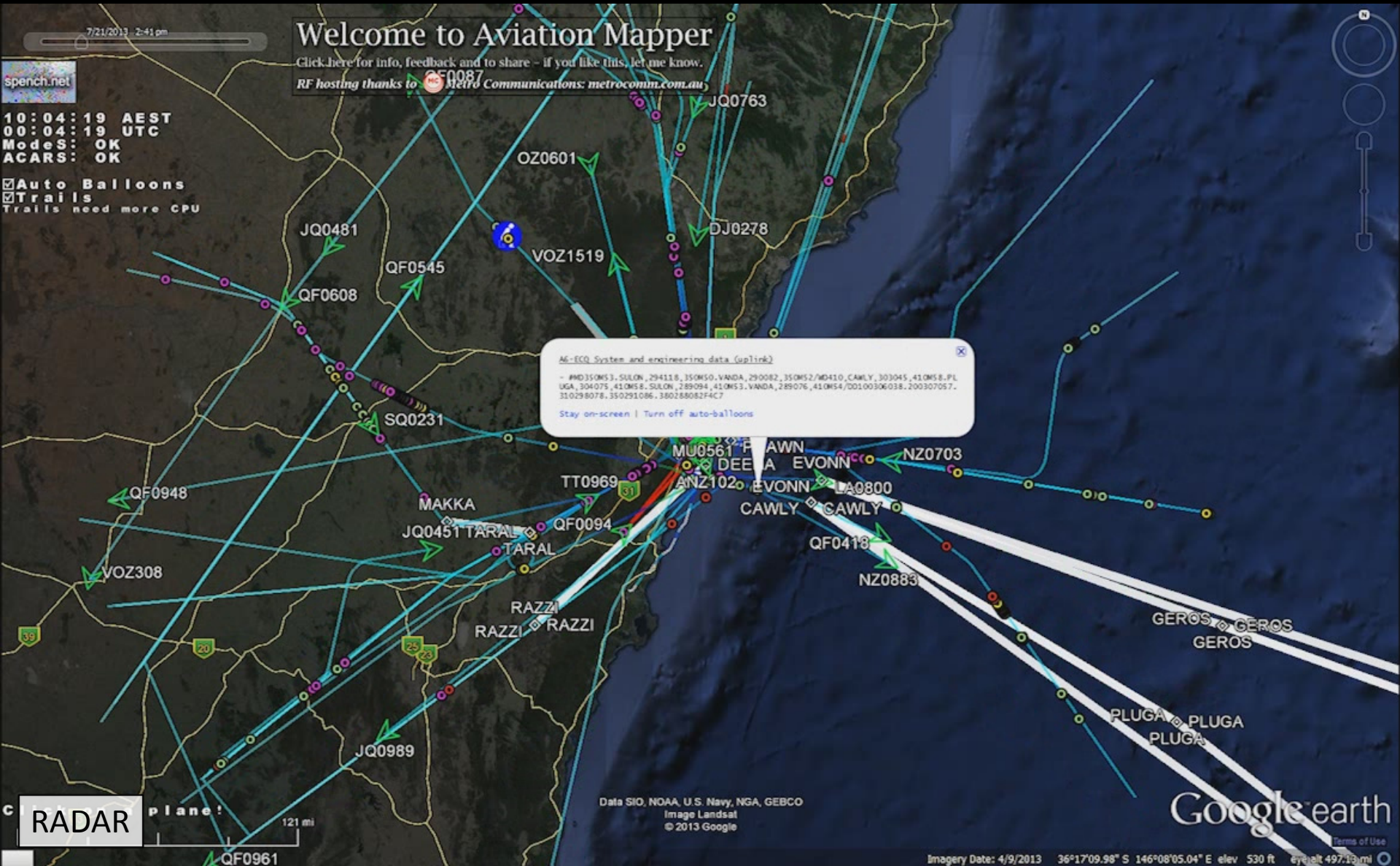
2x2 MIMO

Aviation RADAR



RADAR

Secondary Surveillance: ADS-B/Mode S



Primary Surveillance RADAR

The screenshot displays the GNU Radio Companion interface for a RADAR project. The main window is titled "RADAR.grc - /home/balint/Documents/GRC/Apps - GNU Radio Companion". The interface includes a menu bar (File, Edit, View, Build, Help) and a toolbar with various icons for file operations and signal processing.

Two "Scope Plot" windows are visible, both showing "Counts" on the y-axis and "Time" on the x-axis. The left plot shows a signal over a time range of 100 to 170 microseconds (us), with a y-axis from 0 to 0.04. The right plot shows a signal over a time range of 0 to 40 milliseconds (ms), with a y-axis from 0 to 0.8. Both plots show a sharp initial peak followed by a decay and then a series of smaller oscillations.

Below the plots, there are control panels for "Axes Options" and "Channel Options". The "Axes Options" panel includes settings for Persistence, Analog Alpha, Secs/Div, Counts/Div, Y Offset, and T Offset. The "Channel Options" panel includes settings for Mode, Slope, Channel, and Level. A "Stop" button is located at the bottom of each control panel.

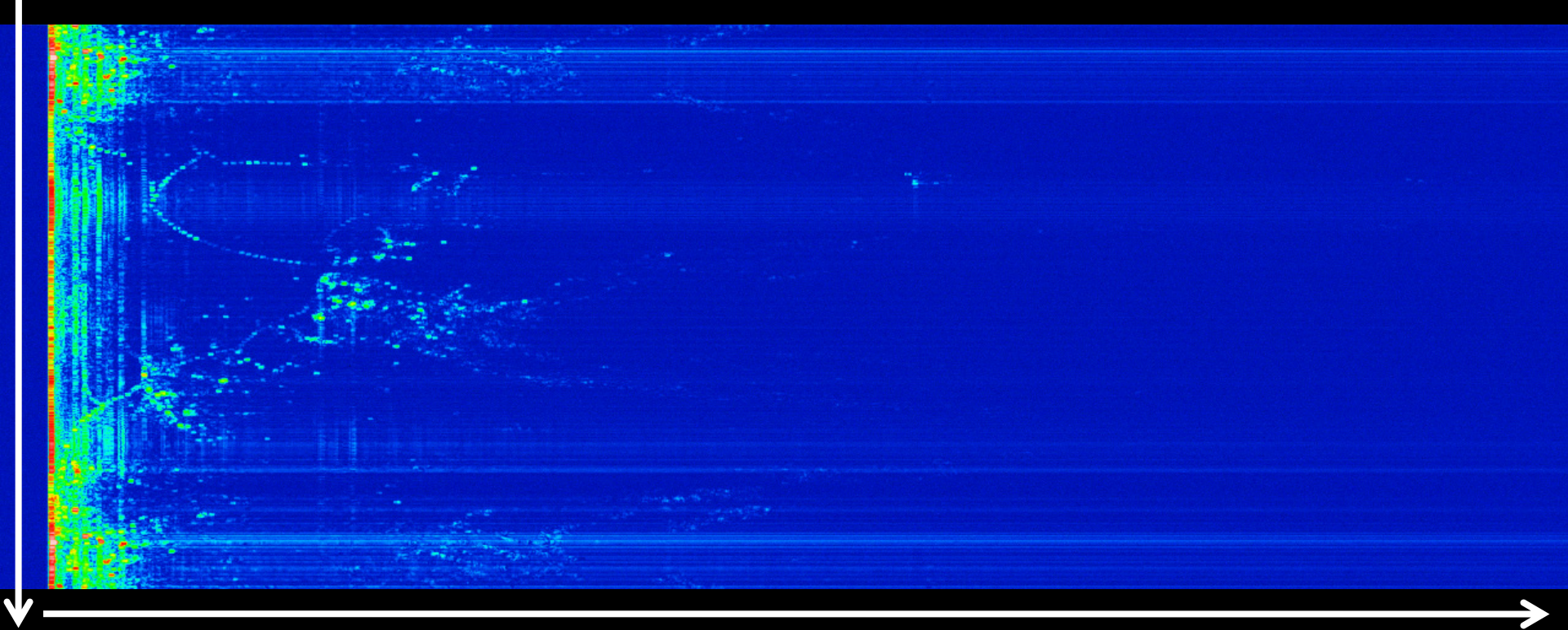
At the bottom left, there is a "Number Plot" showing a value of -30.4668006897 Units. Below this, there are sliders for Gain (set to 10), Freq (set to 2.825G), and Audio (set to 0).

At the bottom right, there is a photograph of a radar antenna structure, likely a primary surveillance radar, mounted on a tower. The structure is illuminated with orange lights, and the background shows a body of water and a clear sky.

A white box with the word "RADAR" is overlaid on the bottom left corner of the image.

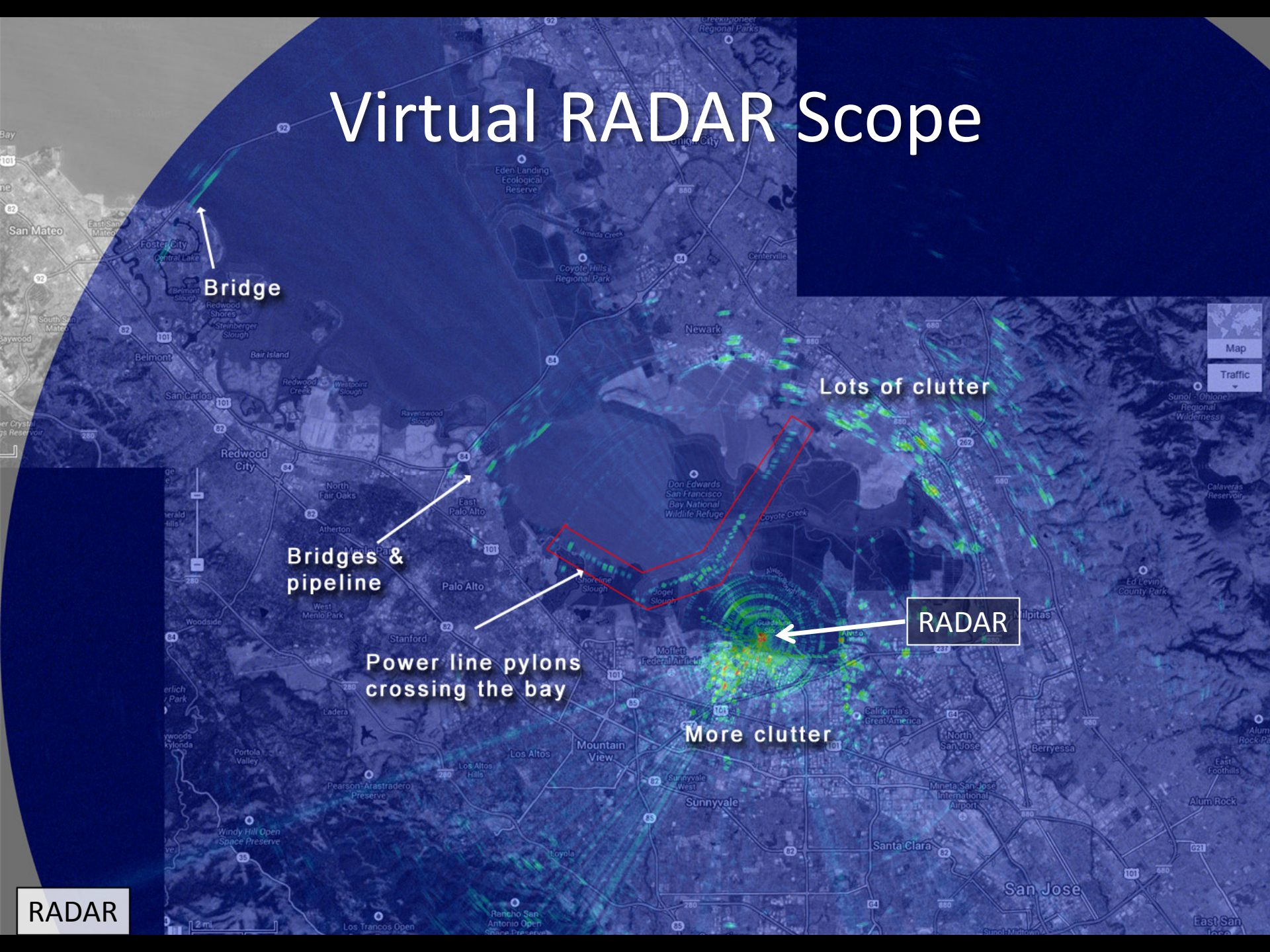
Raw RADAR Return Plot

Each scanline is synchronised to an emitted pulse



Scanline is amplitude of samples over time (also range of the return)

Virtual RADAR Scope



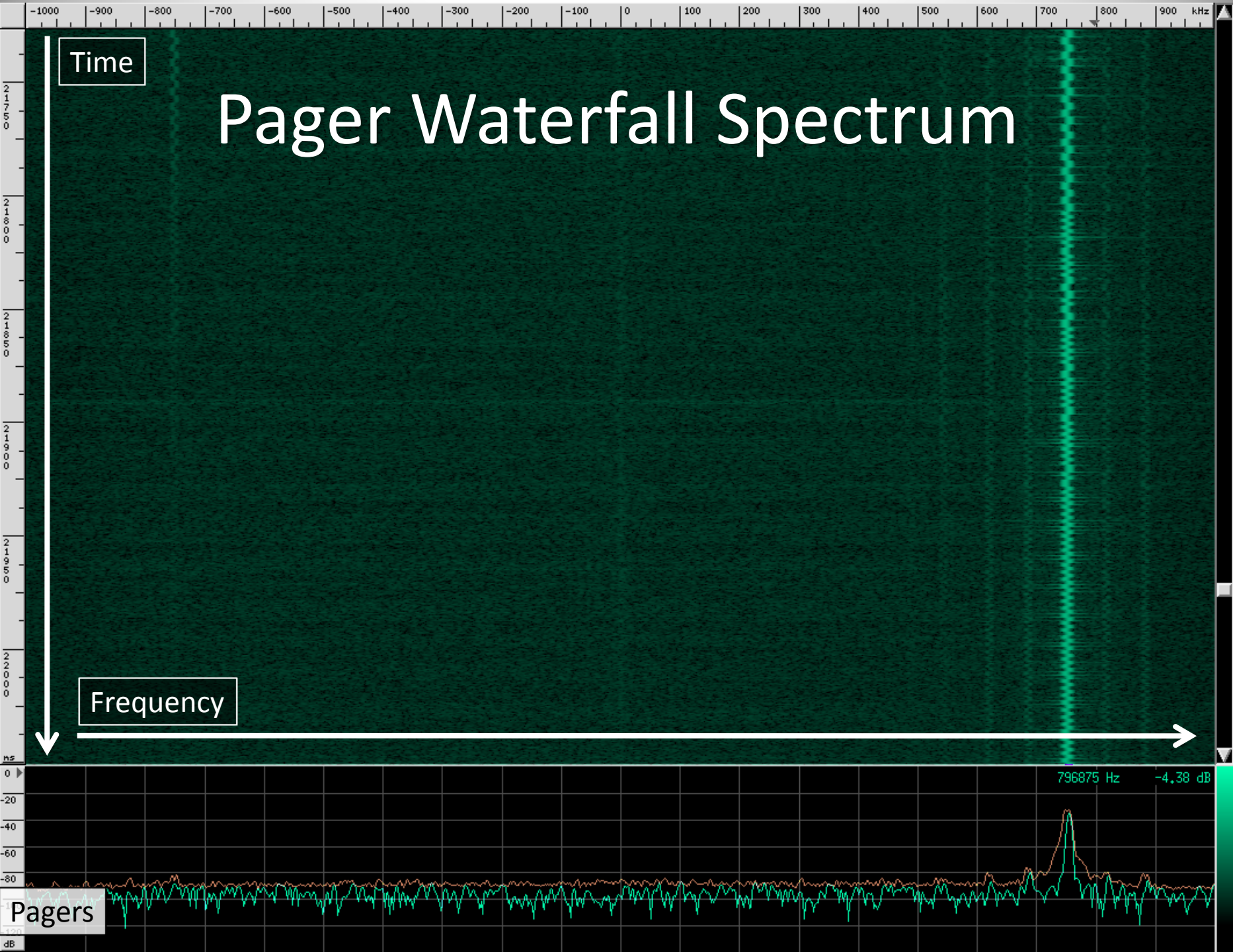
Restaurant Pagers



Pager Waterfall Spectrum

Time

Frequency



Pagers

796875 Hz -4.38 dB

Making sense of raw bits

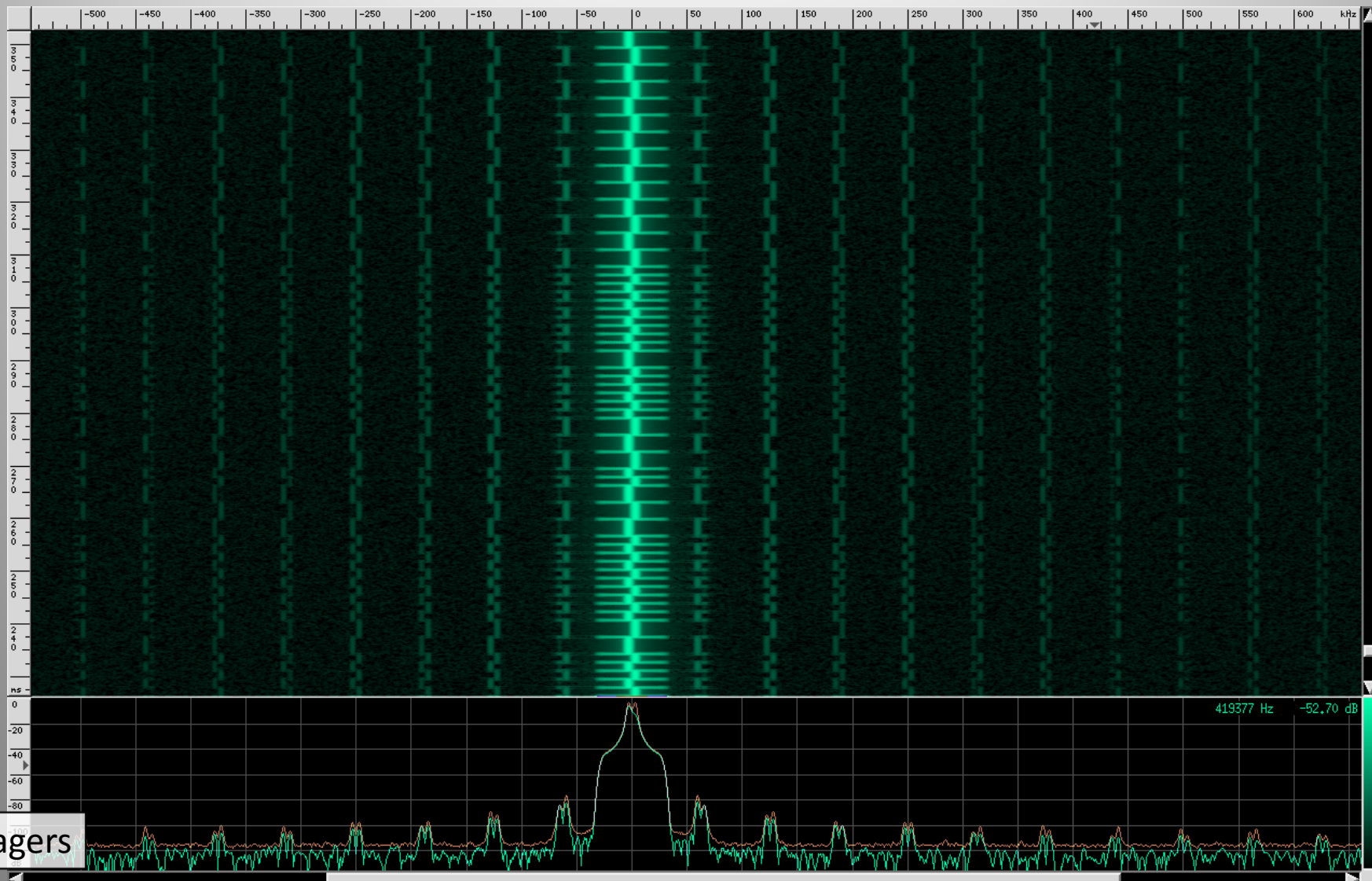
Decoder 0

From beginning Invert Baudot Highlight differences
 From start offset 7-bit ASCII Show decoded data
Offset: Invert first bit 8-bit ASCII Accumulate data
 Extend Offset Straight Flip Flop Swap endianness Extra newline
 Sync settings Diff Diff (inverted) Enforce control bits
 Show bits Prev 0 Prev 1 Start bit
 Manchester 0 (IEEE) Manchester 1 (orig) No stop bits Max bits:
 Diff Man 0 BPM Stop bit
 Diff Man 1 BPS Two stop bits

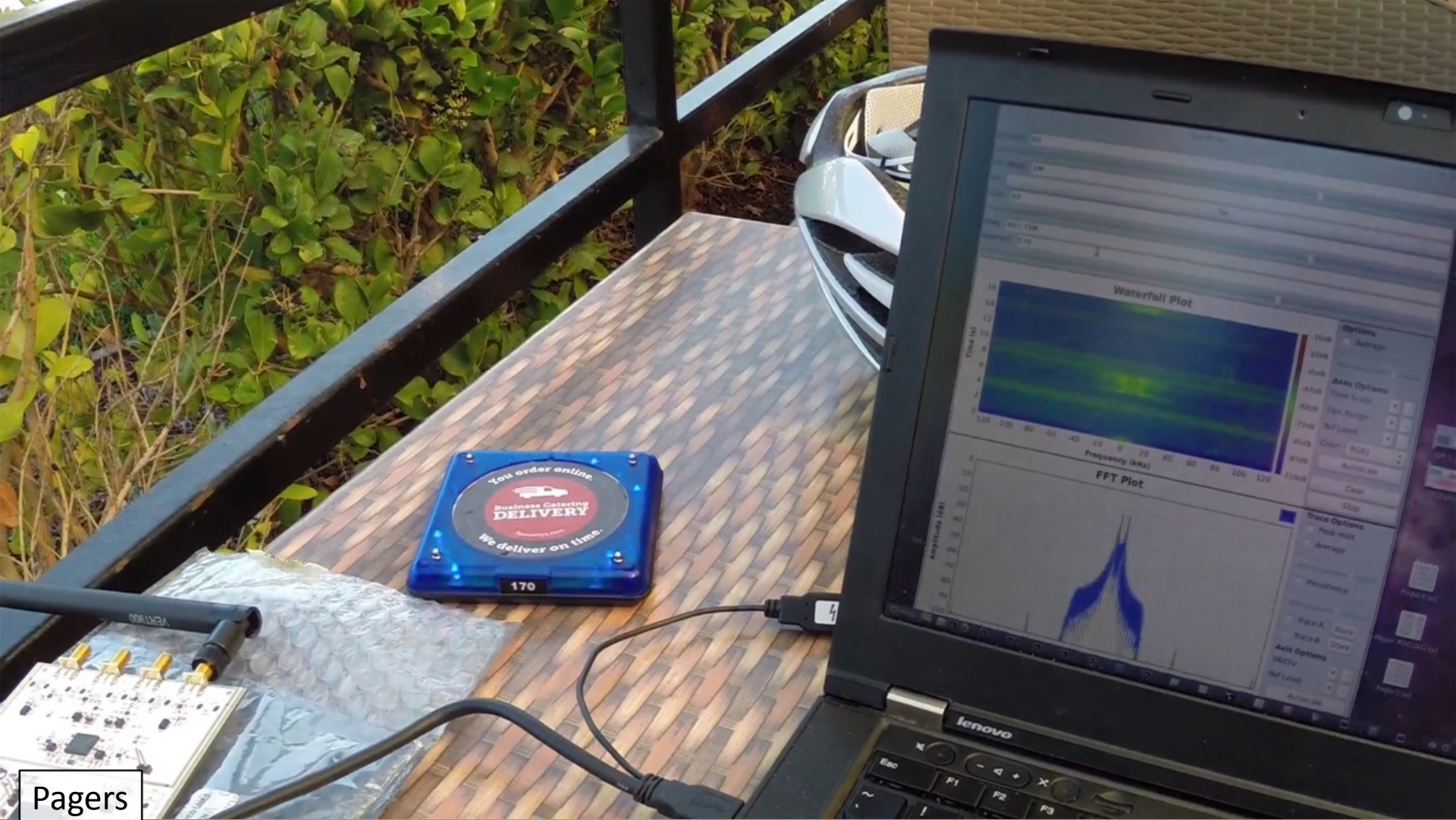
```
000 10101010 10101010 10101010 11111100 aa aa aa fc ....
004 00101101 00000010 00001000 00001100 2d 02 08 0c -...
008 00000000 00000000 00000000 00000000 00 00 00 00 ....
012 00000000 10000001 11000001 0 00 81 c1 ...<7 left>
```

Sum: C1
LRC: FFFFFC42
CRC Poly D5 Start 00: 03
CRC Poly D5 Start FF: A9
CRC Poly AB Start 00: 2E
CRC Poly AB Start FF: 78
CRC Poly EA Start 00: DB
CRC Poly EA Start FF: 71

Modulator Output



Pager Spoofing



Pagers

RDS Traffic Message Channel

```
File Edit View Search Terminal Help
02A (RT) - PI:1C41 - PTY:Rock Music (country:DE/GR/MA/_/MD, area:Regional 9, program:65)
y's 103.7 Greatest Hits of All Time
00A (BASIC) - PI:1C41 - PTY:Rock Music (country:DE/GR/MA/_/MD, area:Regional 9, program:65)
=>Alts of <== - -Speech-STEREO - AF:
02A (RT) - PI:1C41 - PTY:Rock Music (country:DE/GR/MA/_/MD, area:Regional 9, program:65)
y's 103.7 Greatest Hits of All Time
02A (RT) - PI:1C41 - PTY:Rock Music (country:DE/GR/MA/_/MD, area:Regional 9, program:65)
y's 103.7 Greatest Hits of All Time
08A (TMC) - PI:1C41 - PTY:Rock Music (country:DE/GR/MA/_/MD, area:Regional 9, program:65)
#user msg# diversion recommended, single-grp, duration:no duration given, extent:6 segments, event1
@@@@ Still Sync-ed (Got 1 bad blocks on 50 total)
00A (BASIC) - PI:1C41 - PTY:Rock Music (country:DE/GR/MA/_/MD, area:Regional 9, program:65)
=>AltsTif <== - -Speech-STEREO - AF:
08A (TMC) - PI:1C41 - PTY:Rock Music (country:DE/GR/MA/_/MD, area:Regional 9, program:65)
#user msg# diversion recommended, single-grp, duration:no duration given, extent:6 segments, event1
03A (AID) - PI:1C41 - PTY:Rock Music (country:DE/GR/MA/_/MD, area:Regional 9, program:65)
aid group: 8A - location table: 0 - AFI-OFF - basic mode - regional urban
03A (AID) - PI:1C41 - PTY:Rock Music (country:DE/GR/MA/_/MD, area:Regional 9, program:65)
aid group: 8A - gap:3 groups, SID:05
03A (AID) - PI:1C41 - PTY:Rock Music (country:DE/GR/MA/_/MD, area:Regional 9, program:65)
aid group: 8A - location table: 0 - AFI-OFF - basic mode - regional urban
08A (TMC) - PI:1C41 - PTY:Rock Music (country:DE/GR/MA/_/MD, area:Regional 9, program:65)
#user msg# diversion recommended, single-grp, duration:no duration given, extent:3 segments, event
03A (AID) - PI:1C41 - PTY:Rock Music (country:DE/GR/MA/_/MD, area:Regional 9, program:65)
aid group: 8A - gap:3 groups, SID:05
00A (BASIC) - PI:1C41 - PTY:Rock Music (country:DE/GR/MA/_/MD, area:Regional 9, program:65)
=>All Tif <== - -Speech-STEREO - AF:
00A (BASIC) - PI:1C41 - PTY:Rock Music (country:DE/GR/MA/_/MD, area:Regional 9, program:65)
=>All Tif <== - -Speech-STEREO - AF:
08A (TMC) - PI:1C41 - PTY:Rock Music (country:DE/GR/MA/_/MD, area:Regional 9, program:65)
#user msg# diversion recommended, single-grp, duration:no duration given, extent:3 segments, event
00A (BASIC) - PI:1C41 - PTY:Rock Music (country:DE/GR/MA/_/MD, area:Regional 9, program:65)
@@@@ Still Sync-ed (Got 2 bad blocks on 50 total)
00A (BASIC) - PI:1C41 - PTY:Rock Music (country:DE/GR/MA/_/MD, area:Regional 9, program:65)
=>All Time<== - -Speech-STEREO - AF:
00A (BASIC) - PI:1C41 - PTY:Rock Music (country:DE/GR/MA/_/MD, area:Regional 9, program:65)
=>All Time<== - -Speech-STEREO - AF:
00A (BASIC) - PI:1C41 - PTY:Rock Music (country:DE/GR/MA/_/MD, area:Regional 9, program:65)
=>All Time<== - -Speech-STEREO - AF:
08A (TMC) - PI:1C41 - PTY:Rock Music (country:DE/GR/MA/_/MD, area:Regional 9, program:65)
#user msg# diversion recommended, single-grp, duration:no duration given, extent:3 segments, event
00A (BASIC) - PI:1C41 - PTY:Rock Music (country:DE/GR/MA/_/MD, area:Regional 9, program:65)
=>All Time<== - -Speech-STEREO - AF:
00A (BASIC) - PI:1C41 - PTY:Rock Music (country:DE/GR/MA/_/MD, area:Regional 9, program:65)
=>All Time<== - -Speech-STEREO - AF:
00A (BASIC) - PI:1C41 - PTY:Rock Music (country:DE/GR/MA/_/MD, area:Regional 9, program:65)
=>All Time<== - -Speech-STEREO - AF:
00A (BASIC) - PI:1C41 - PTY:Rock Music (country:DE/GR/MA/_/MD, area:Regional 9, program:65)
=>All Time<== - -Speech-STEREO - AF:
00A (BASIC) - PI:1C41 - PTY:Rock Music (country:DE/GR/MA/_/MD, area:Regional 9, program:65)
=>All Time<== - -Speech-STEREO - AF:
@@@@ Still Sync-ed (Got 0 bad blocks on 50 total)
08A (TMC) - PI:1C41 - PTY:Rock Music (country:DE/GR/MA/_/MD, area:Regional 9, program:65)
#user msg# diversion recommended, single-grp, duration:no duration given, extent:6 segments, event
08A (TMC) - PI:1C41 - PTY:Rock Music (country:DE/GR/MA/_/MD, area:Regional 9, program:65)
#user msg# diversion recommended, single-grp, duration:no duration given, extent:6 segments, event
02A (RT) - PI:1C41 - PTY:Rock Music (country:DE/GR/MA/_/MD, area:Regional 9, program:65)
y's 103.7 Greatest Hits of All Time
```

Stereo FM receiver and RDS Decoder

Volume: 0

BB Demod L+R Pilot DSBSC RDS Raw L-R RDS

FM Demod

Trace Options
 Peak Hold
 Average
Avg Alpha: 0.8000
 Persistence
Persist Alpha: 0.185
 Trace A Store
 Trace B Store

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

Loop BW: 18k
Gain: 35
Freq Offset: 250k
Freq: 103.7M
Antenna: TX/RX

Frequency 103.70 Station Name All Time Program Type Rock Music PI 1C41
Speech Stereo
The Bay's 103.7 Greatest Hits of All Time
Clock Time xxxxxxxxxxxxxxxxxxxxxx Alt. Frequencies xxxxxxxxxxxxxx

RDS TMC

Compare Against Trusted Source



RDS TMC

Brute Force Search

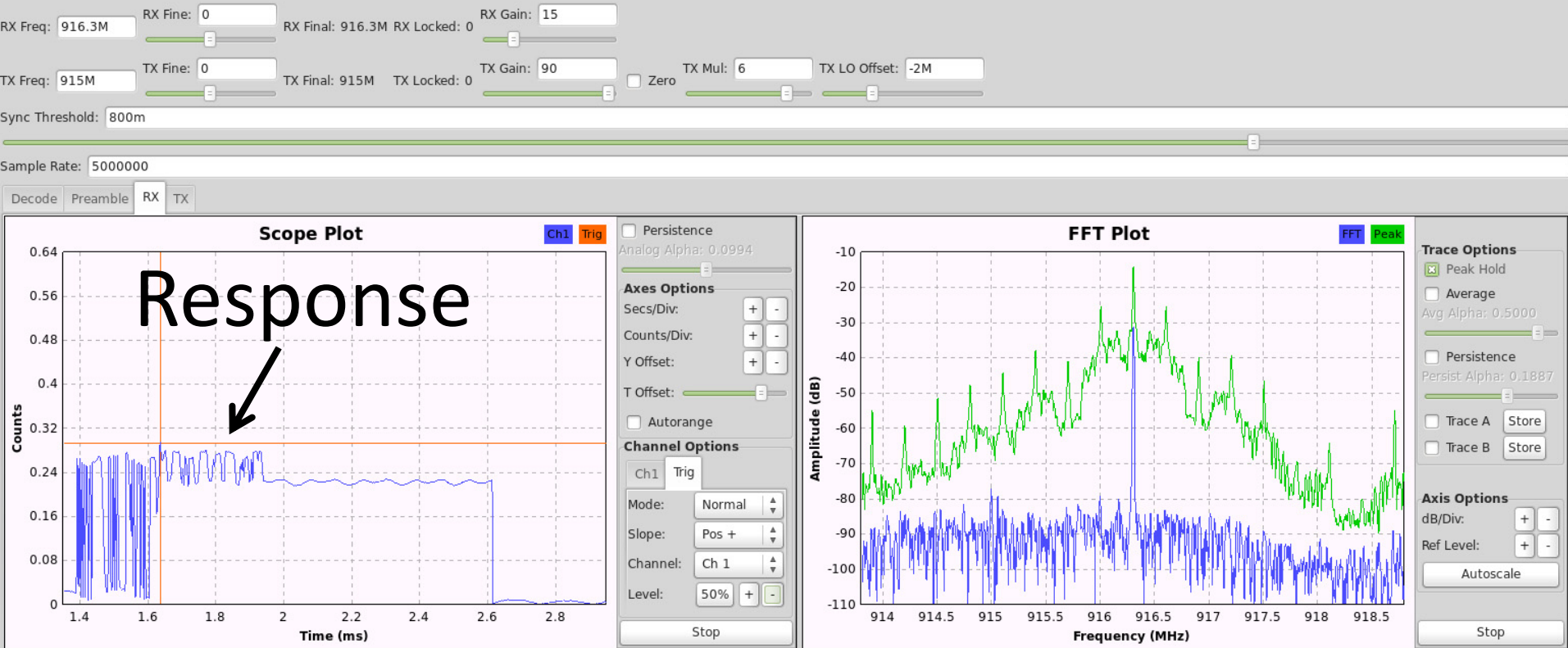
Location # 1 has	1 possible plain codes	Encryption ID 2 has	2 possible keys
4603 11fb		Encryption ID 3 has	15 possible keys
Location # 2 has	1 possible plain codes	Encryption ID 4 has	5 possible keys
4401 1131		Encryption ID 5 has	4 possible keys
Location # 3 has	1 possible plain codes	Encryption ID 6 has	3 possible keys
4172 104c		Encryption ID 7 has	5 possible keys
Location # 4 has	1 possible plain codes	Encryption ID 8 has	7 possible keys
5134 140e		Encryption ID 9 has	2 possible keys
Location # 5 has	1 possible plain codes	Encryption ID 10 has	34 possible keys
4193 1061		Encryption ID 11 has	1 possible keys
Location # 6 has	1 possible plain codes	Encryption ID 13 has	4 possible keys
4527 11af		Encryption ID 15 has	2 possible keys
Location # 7 has	1 possible plain codes	Encryption ID 17 has	2 possible keys
4329 10e9		Encryption ID 18 has	3 possible keys
Location # 8 has	1 possible plain codes	Encryption ID 20 has	3 possible keys
5611 15eb		Encryption ID 21 has	4 possible keys
Location # 9 has	1 possible plain codes	Encryption ID 22 has	6 possible keys
4538 11ba		Encryption ID 24 has	1 possible keys
Location # 10 has	1 possible plain codes	Encryption ID 25 has	3 possible keys
4303 10cf		Encryption ID 26 has	5 possible keys
Location # 11 has	1 possible plain codes	Encryption ID 27 has	3 possible keys
4223 107f		Encryption ID 28 has	1 possible keys
Location # 12 has	1 possible plain codes	Encryption ID 30 has	2 possible keys
4834 12e2		Encryption ID 31 has	4 possible keys

Reading a FasTrak Toll Tag



RFID

Received Signal



Last ID:

147

RFID

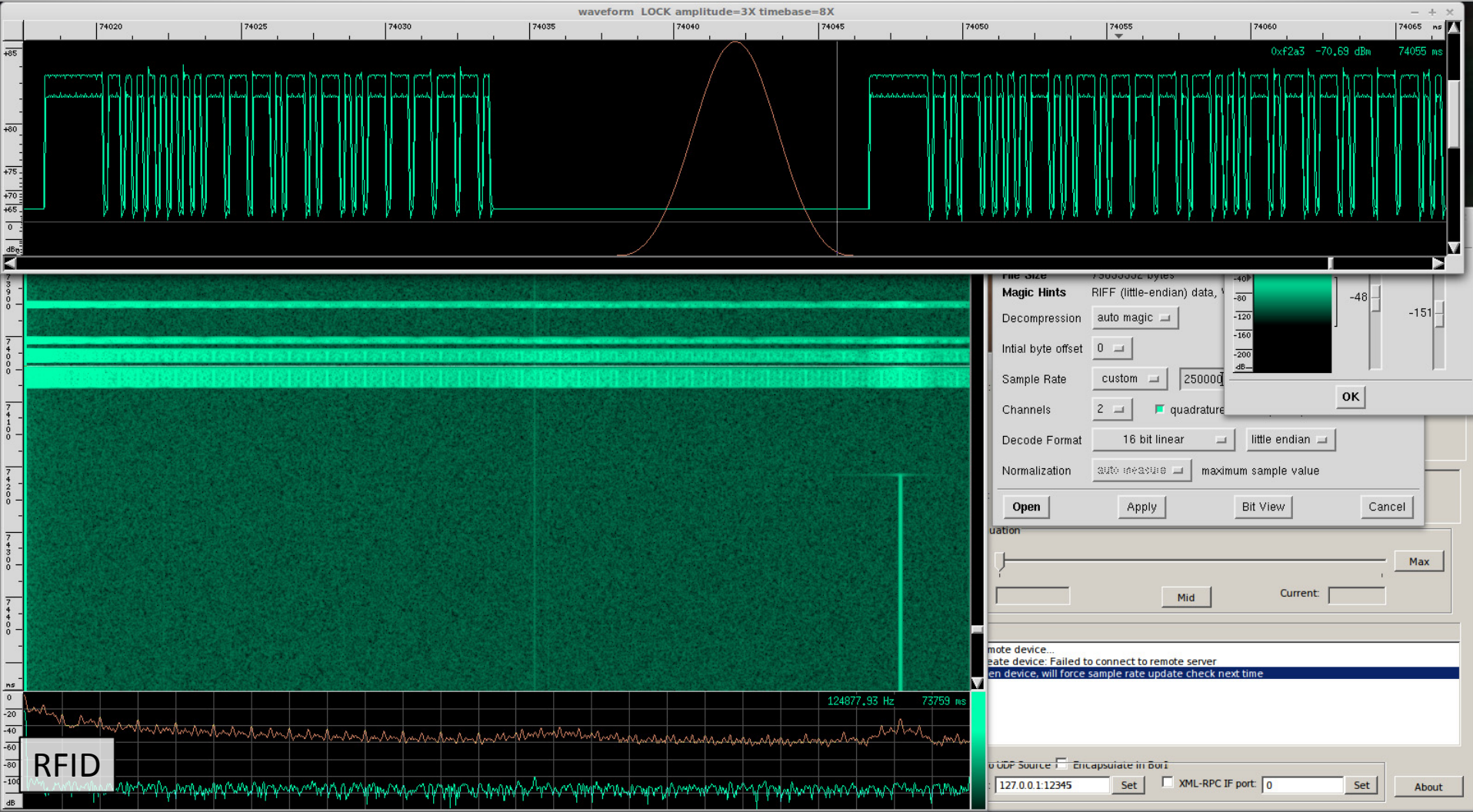
Reading a Tag Outside



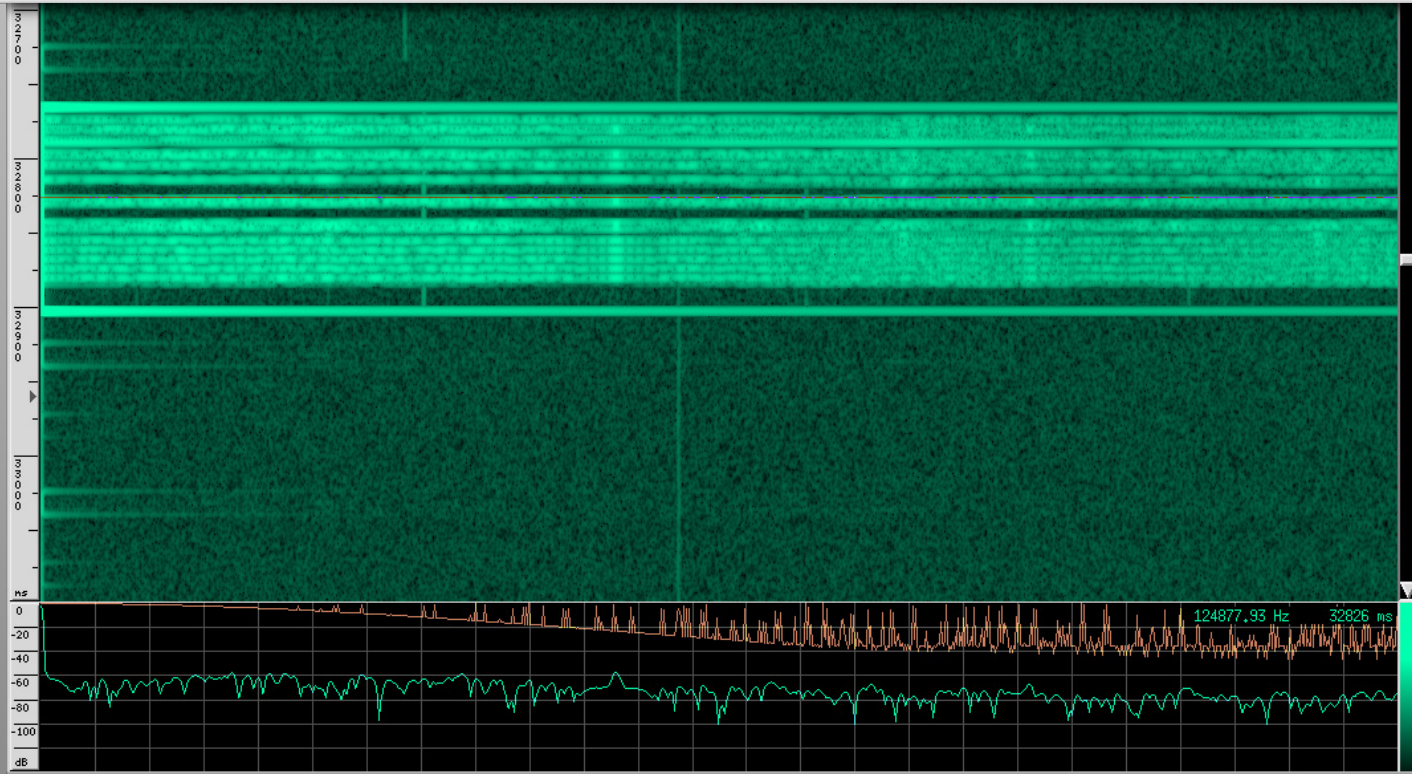
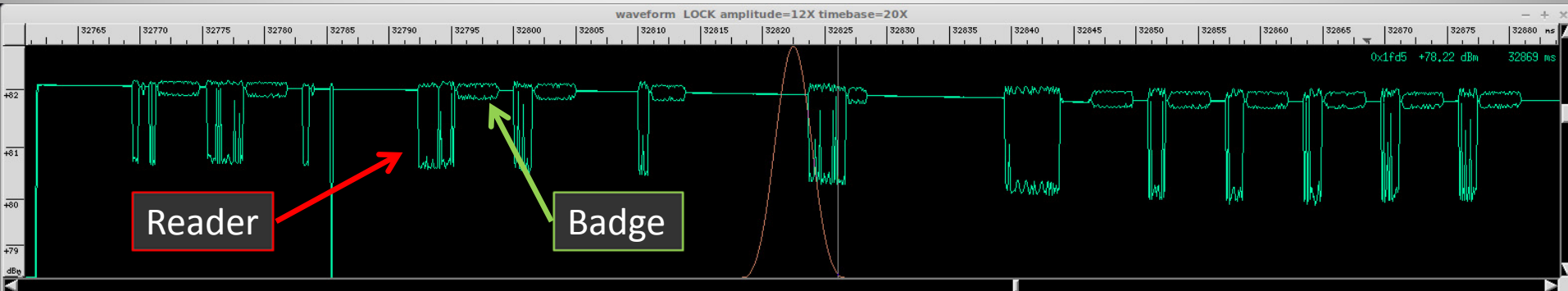


RFID

Toyota Prius Keyless Entry Auth

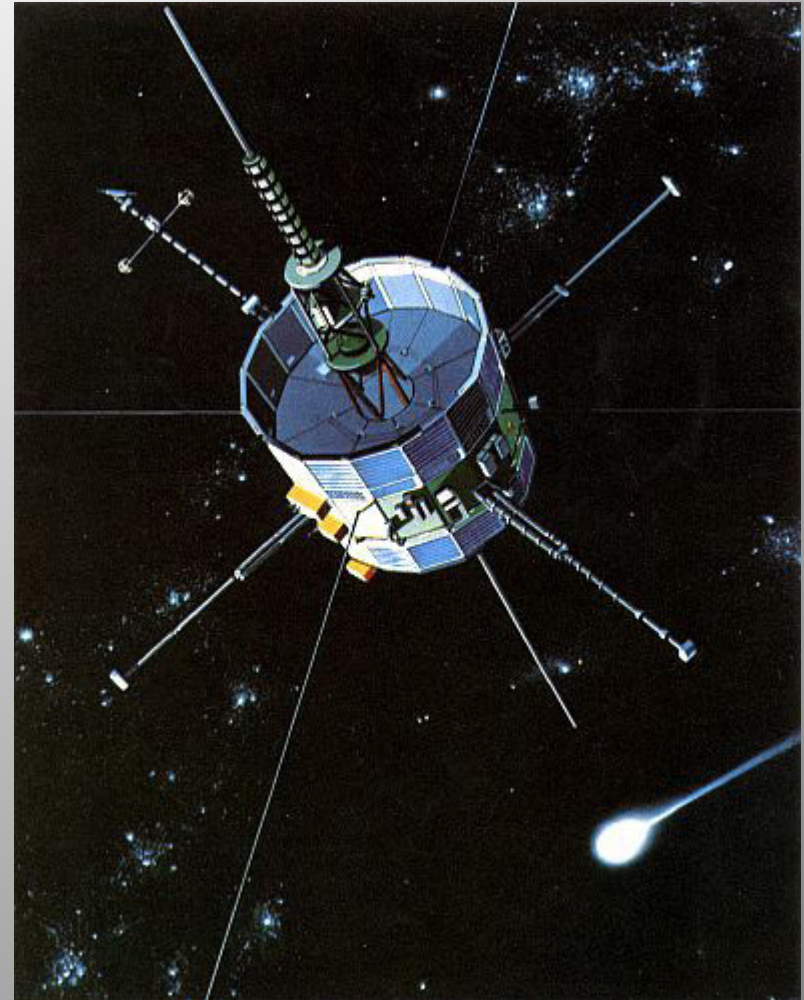


Building Security Badge Auth



ISEE-3 Reboot Project

- International Sun/Earth Explorer 3
- Launched: August 12, 1978
- Heliocentric Orbit
- Study interaction between solar wind and Earth's magnetic field





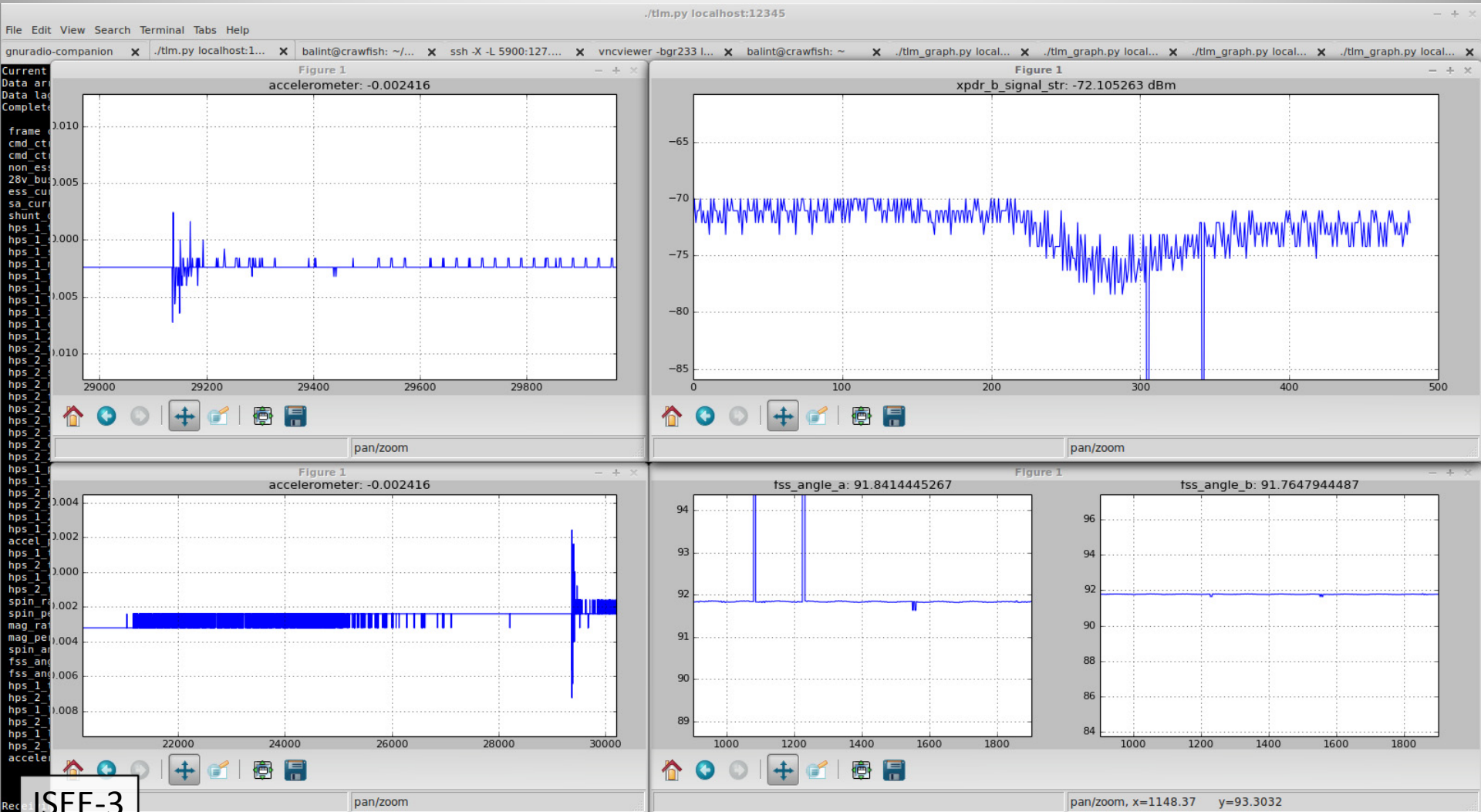
ISEE-3

Moment of First Contact



ISEE-3

Telemetry During Thruster Firing



ISEE-3



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

<http://spench.net/>

GitHub: balint256

balint@spench.net

balint@ettus.com

@spenchnet