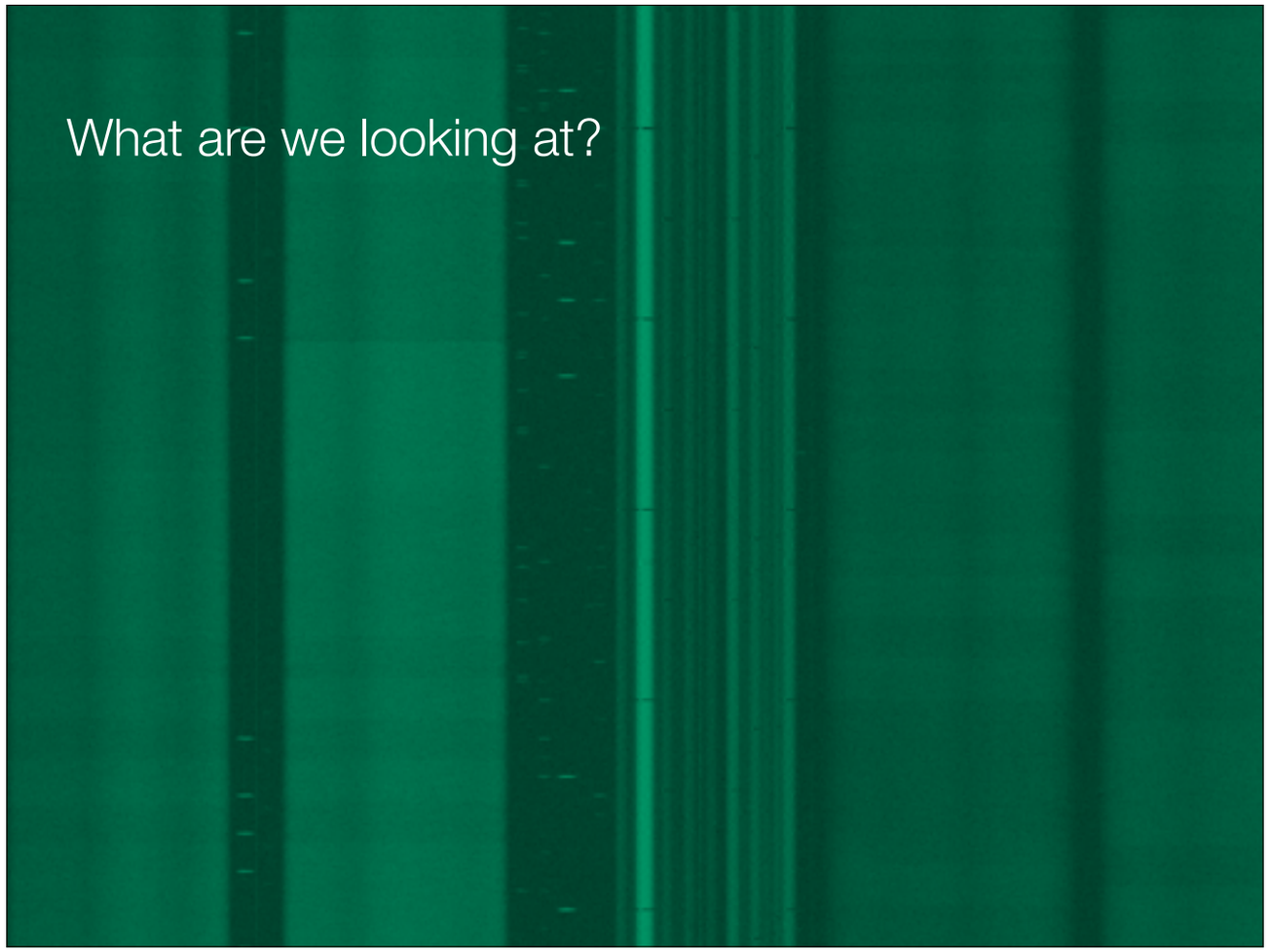
Hacking the Wireless World: Software Defined Radio Exploits

Balint Seeber
Director of Vulnerability Research
Bastille


Getting ready for some serious sampling
by the Adriatic Sea

What are we looking at?

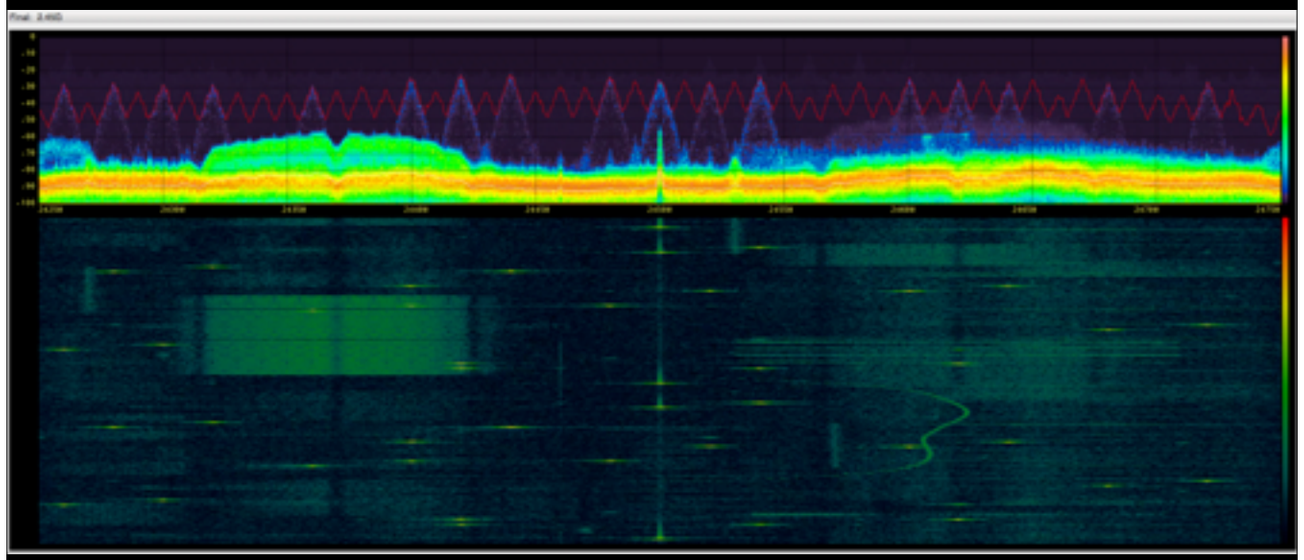


Overview

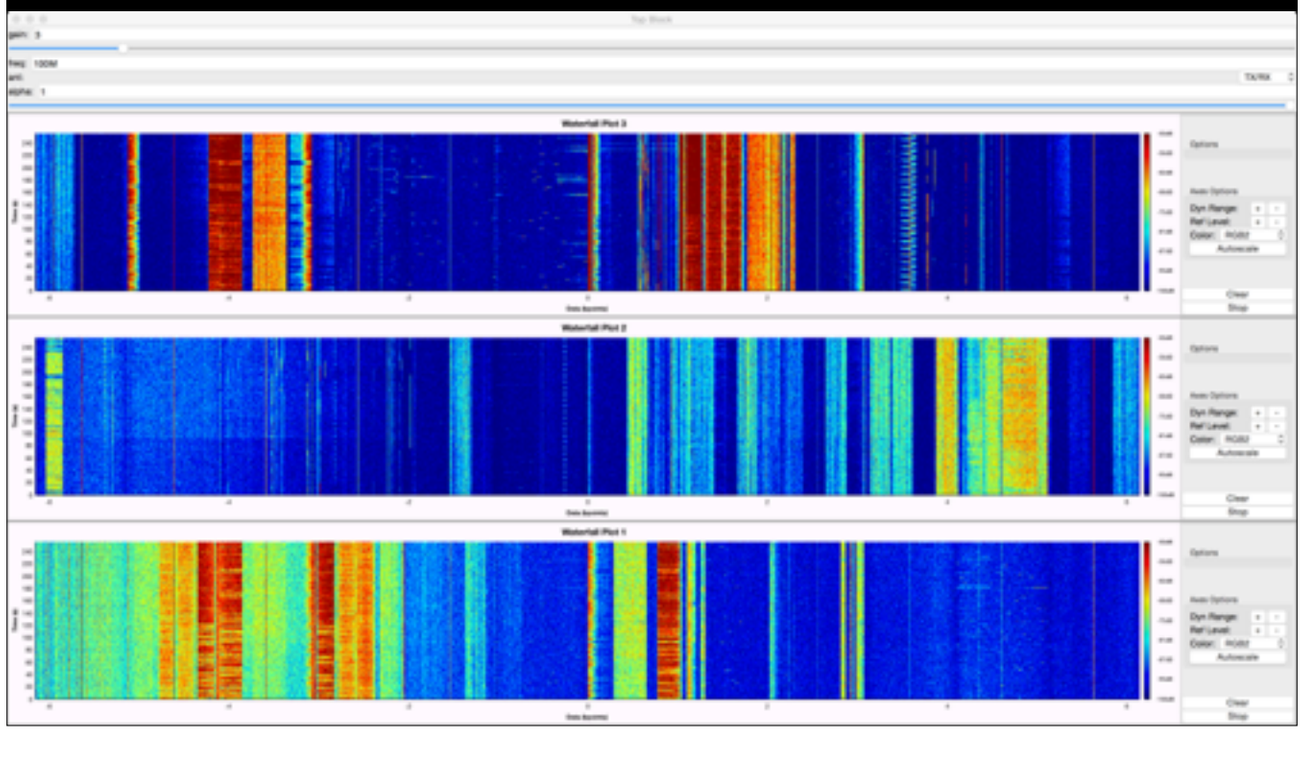
- The Radio Frequency Spectrum
- Aviation / INMARSAT Aero
- Drones / Airborne Surveillance
- Restaurant Pagers / Keyless Entry
- ISEE-3 Reboot Mission

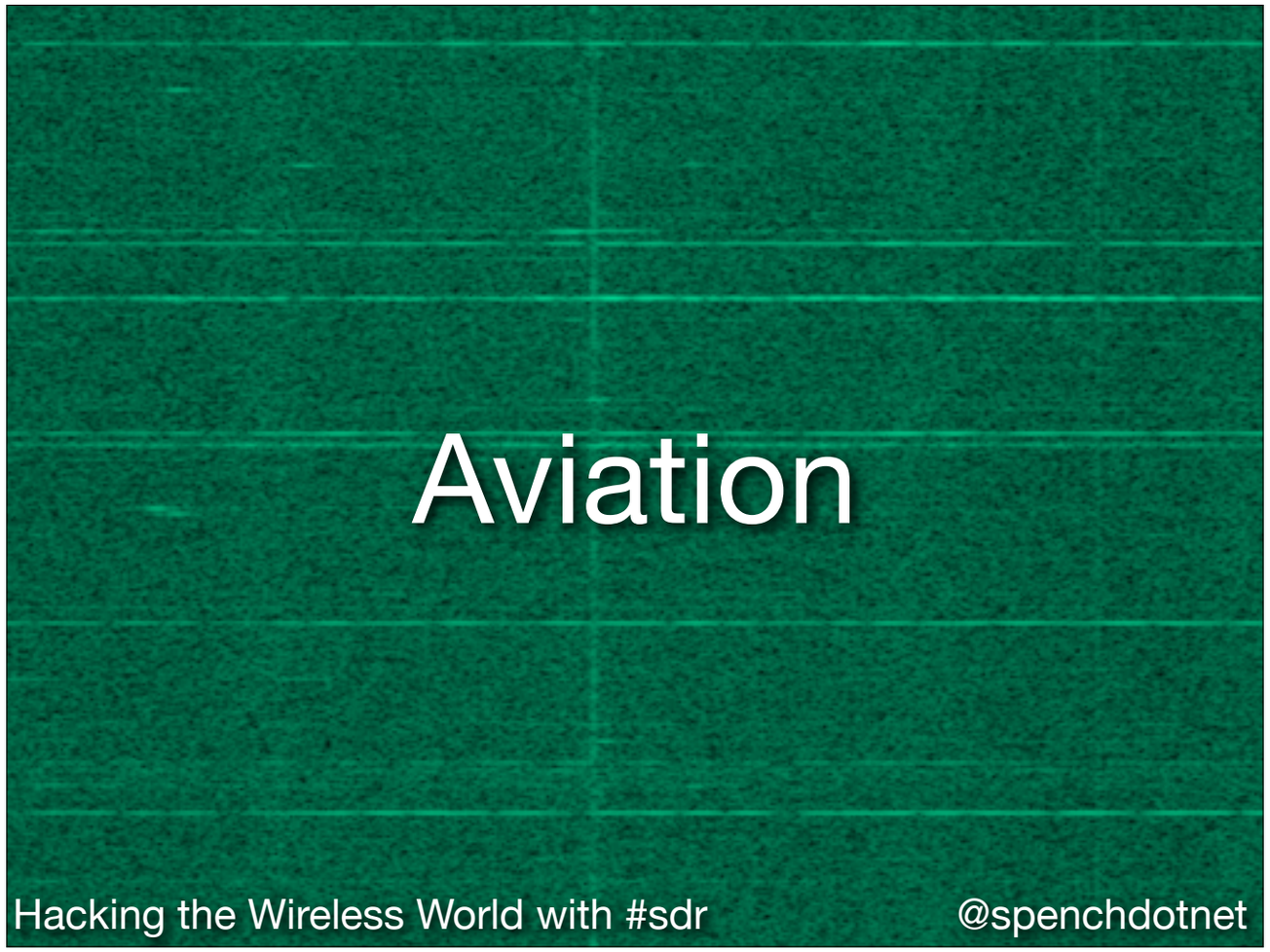
GNURadio
THE FREE & OPEN SOFTWARE RADIO ECOSYSTEM

2.4 GHz ISM Band Activity

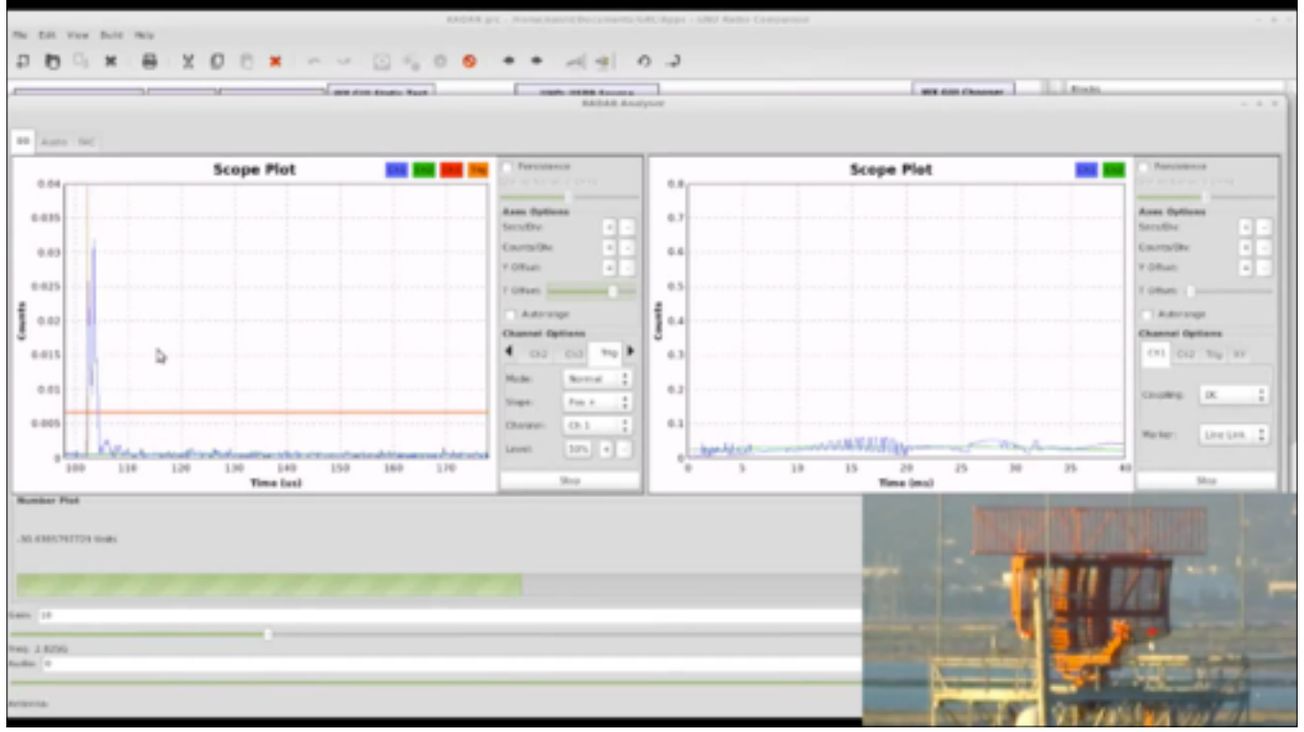


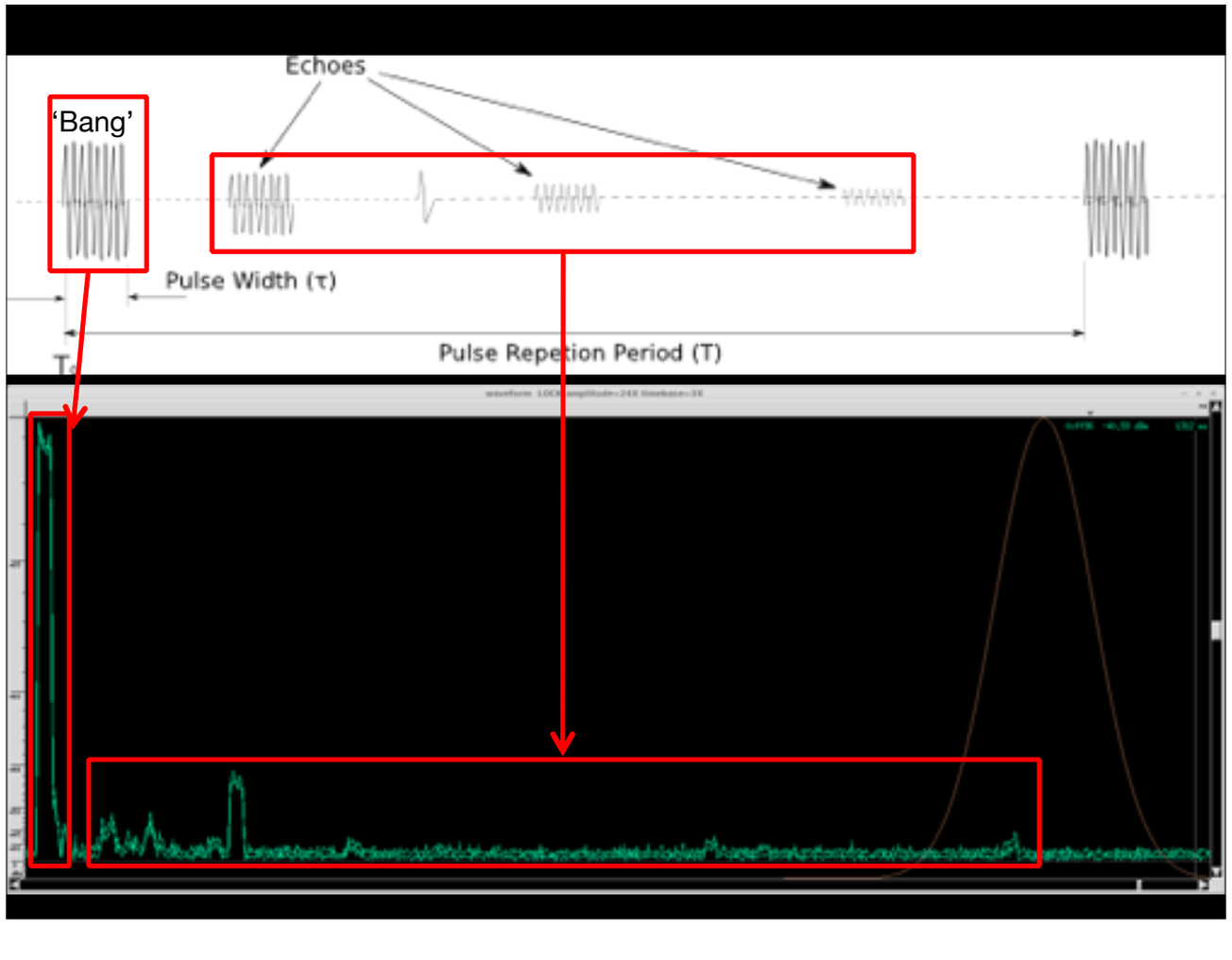
Wideband Activity: 50 MHz - 1.25 GHz




Aviation
Hacking the Wireless World with #sdr
@spenchdotnet

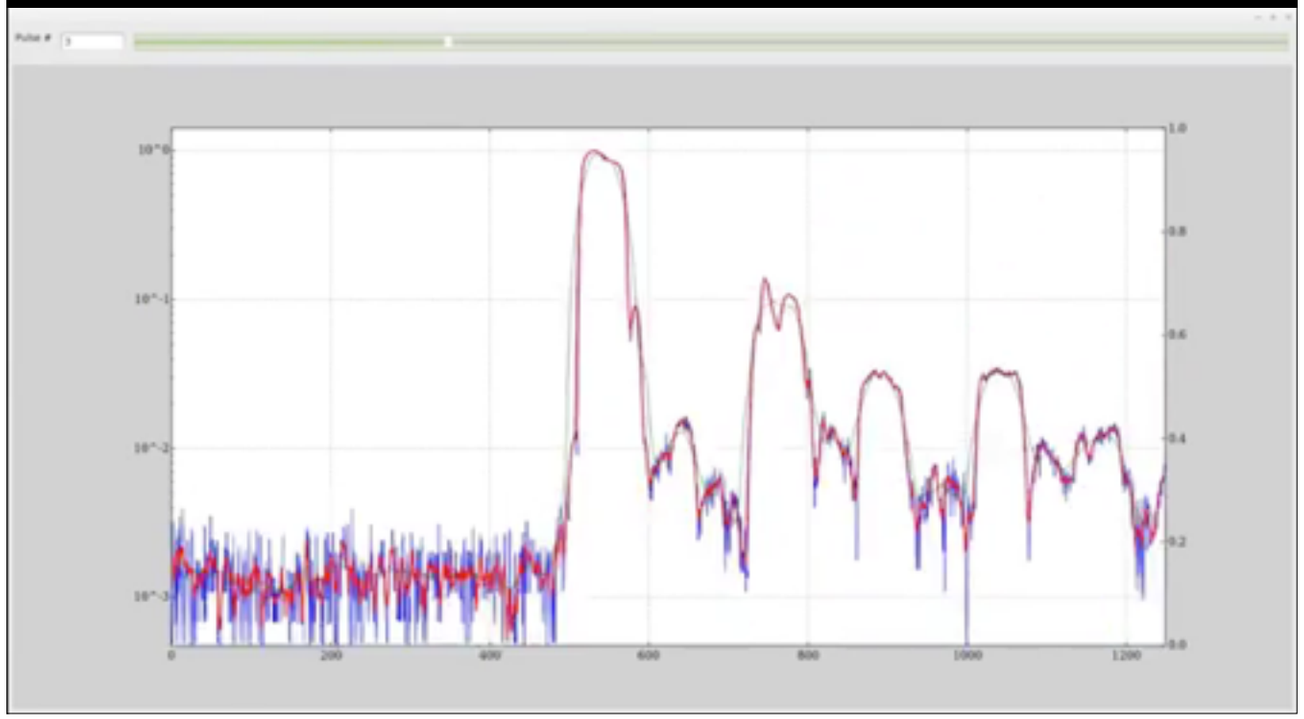
Primary **S**urveillance **R**ADAR (PSR)



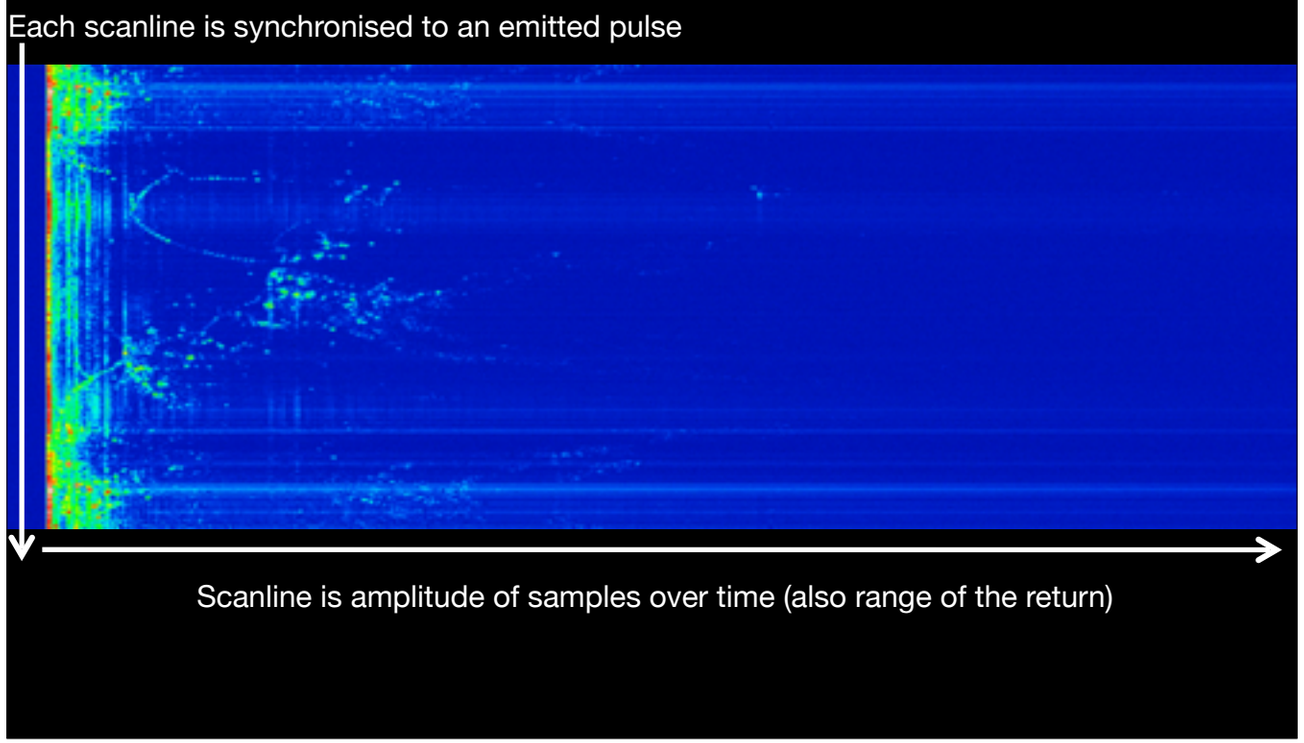


http://en.wikipedia.org/wiki/Radar_signal_characteristics

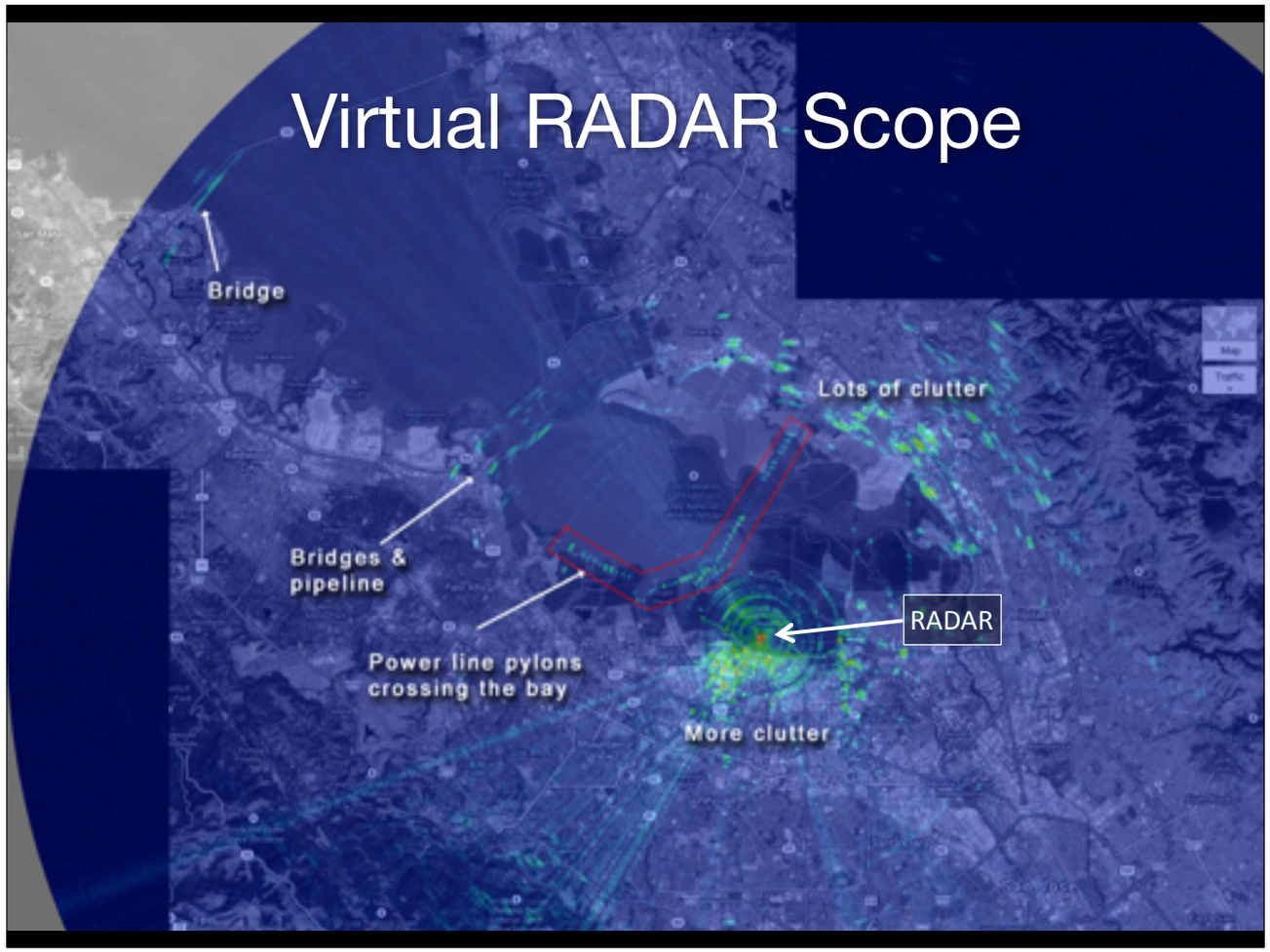
Animated Returns (Magnitude vs Time)



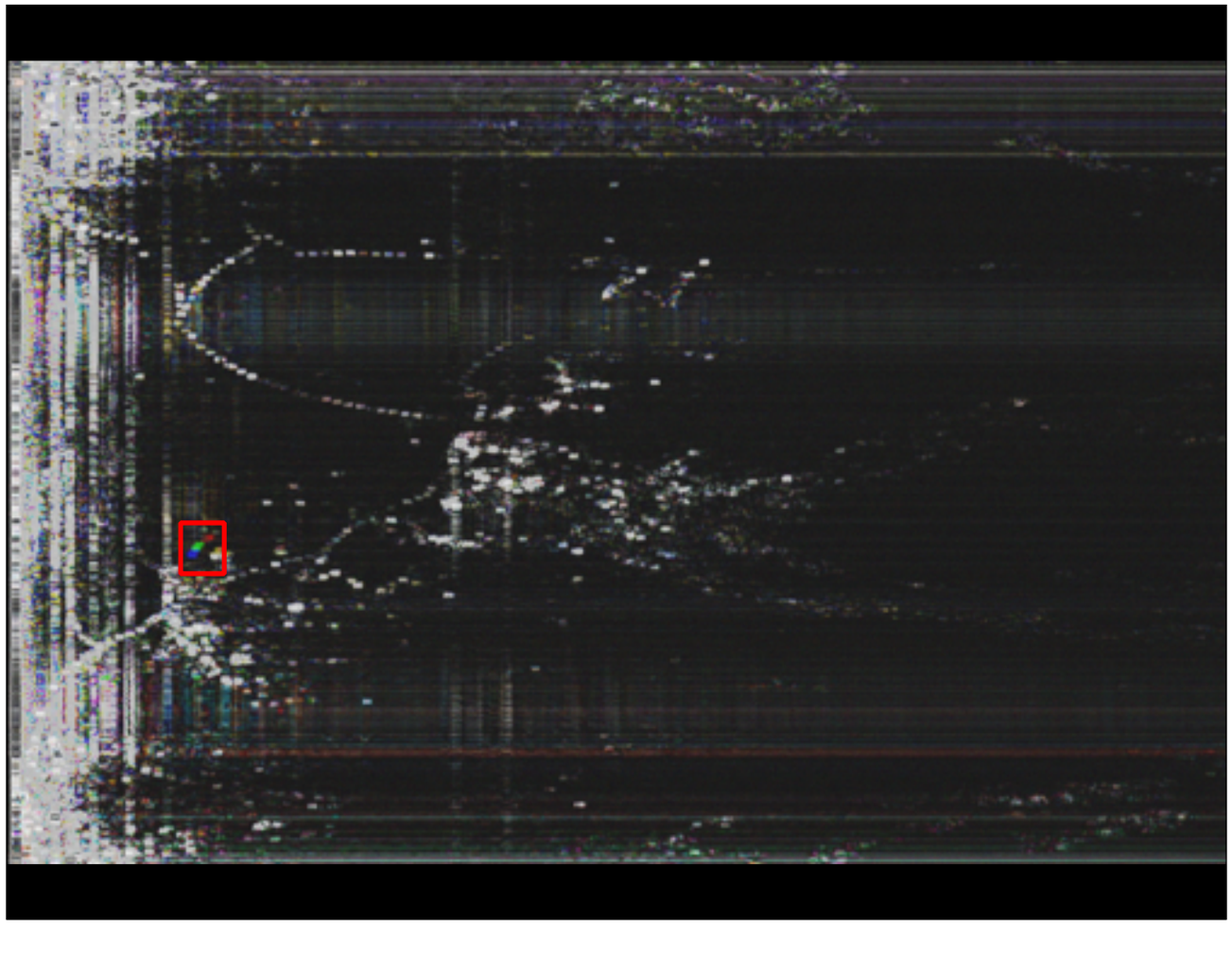
Raw RADAR Return Plot



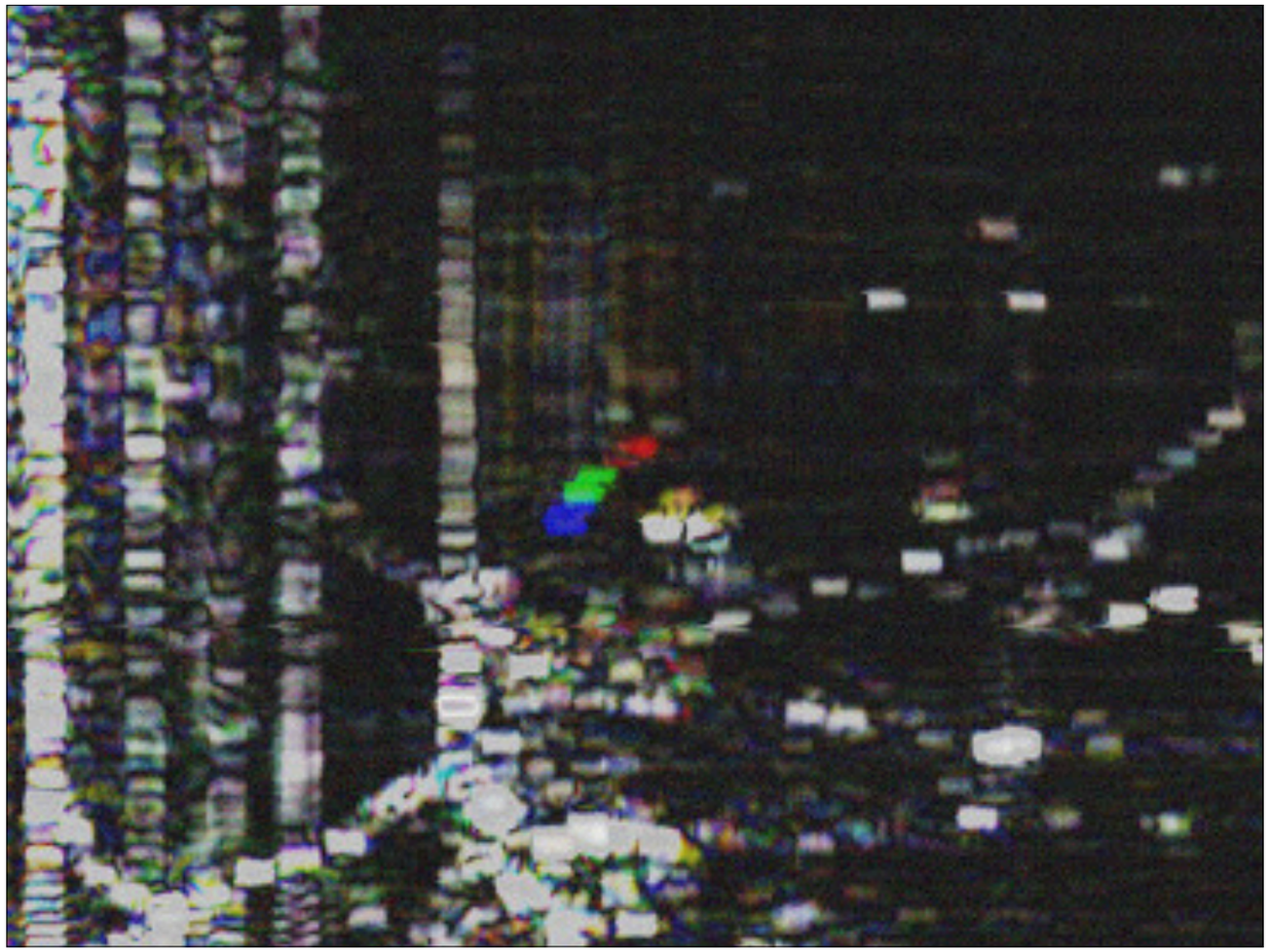
Taking each ‘frame’ (or pulse-triggered group of samples) from the last sequence, and stacking them vertically produces this raster plot of the sample magnitudes where each scanline is triggered by a pulse



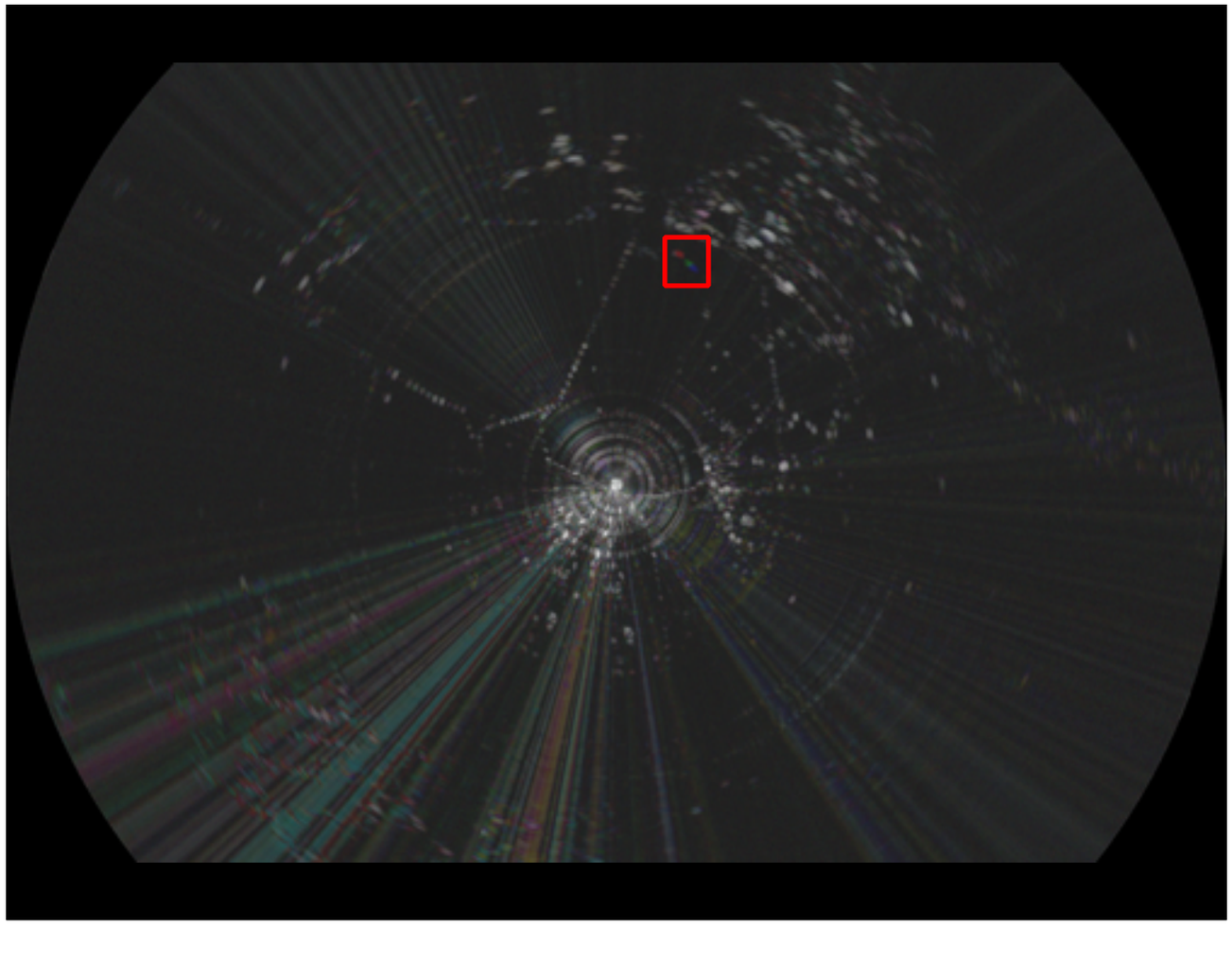
The raster plot can undergo a polar-coordinate transformation and be unwrapped onto the map (with the image centred on the RADAR's position). The 'interesting features' now line up with real physical features of the area.



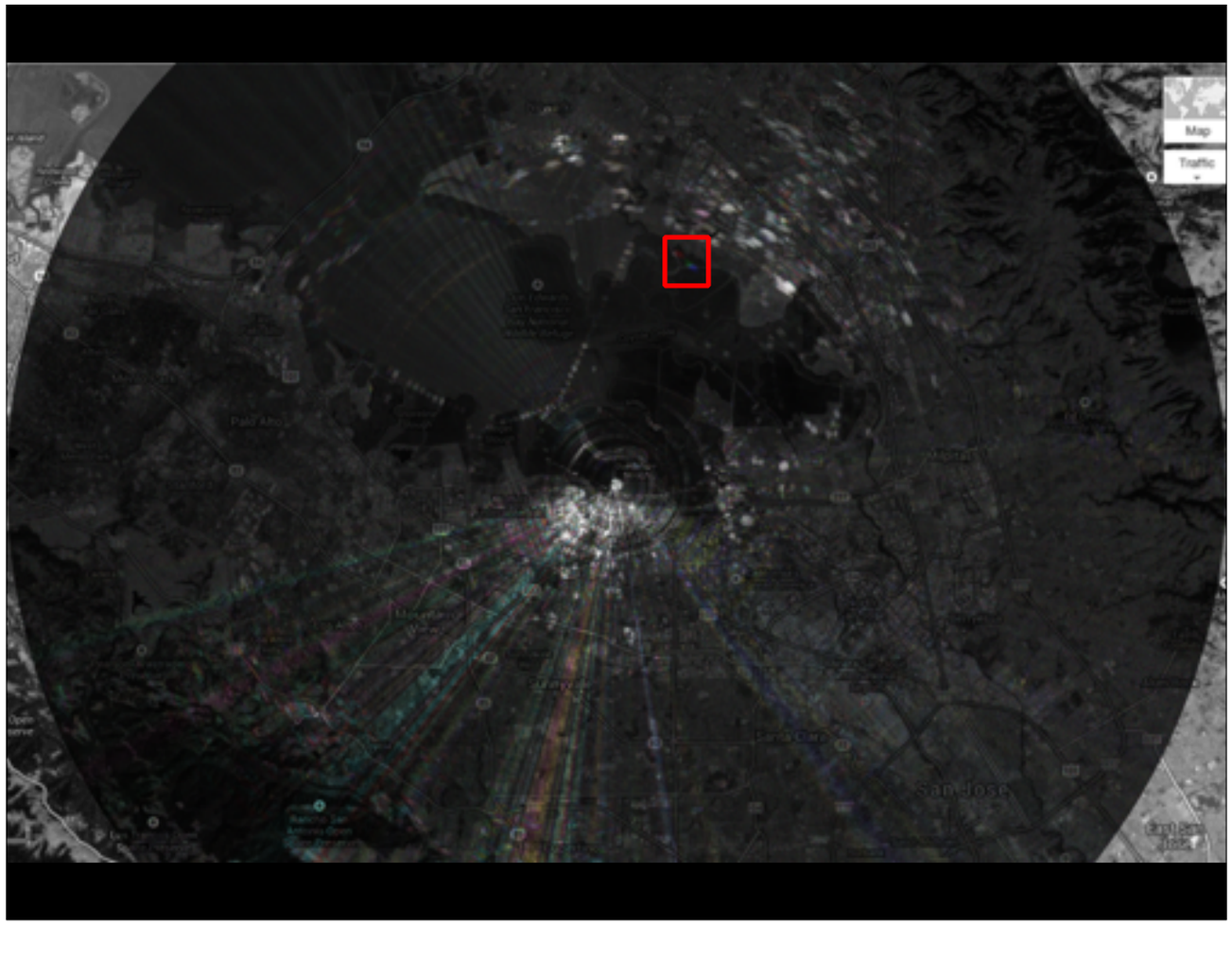
In this image, the R-G-B separation caused by moving target can be seen (each rotation will have that cluster of pixels move, so the pixels will no longer line up on top of each other in each colour channel)



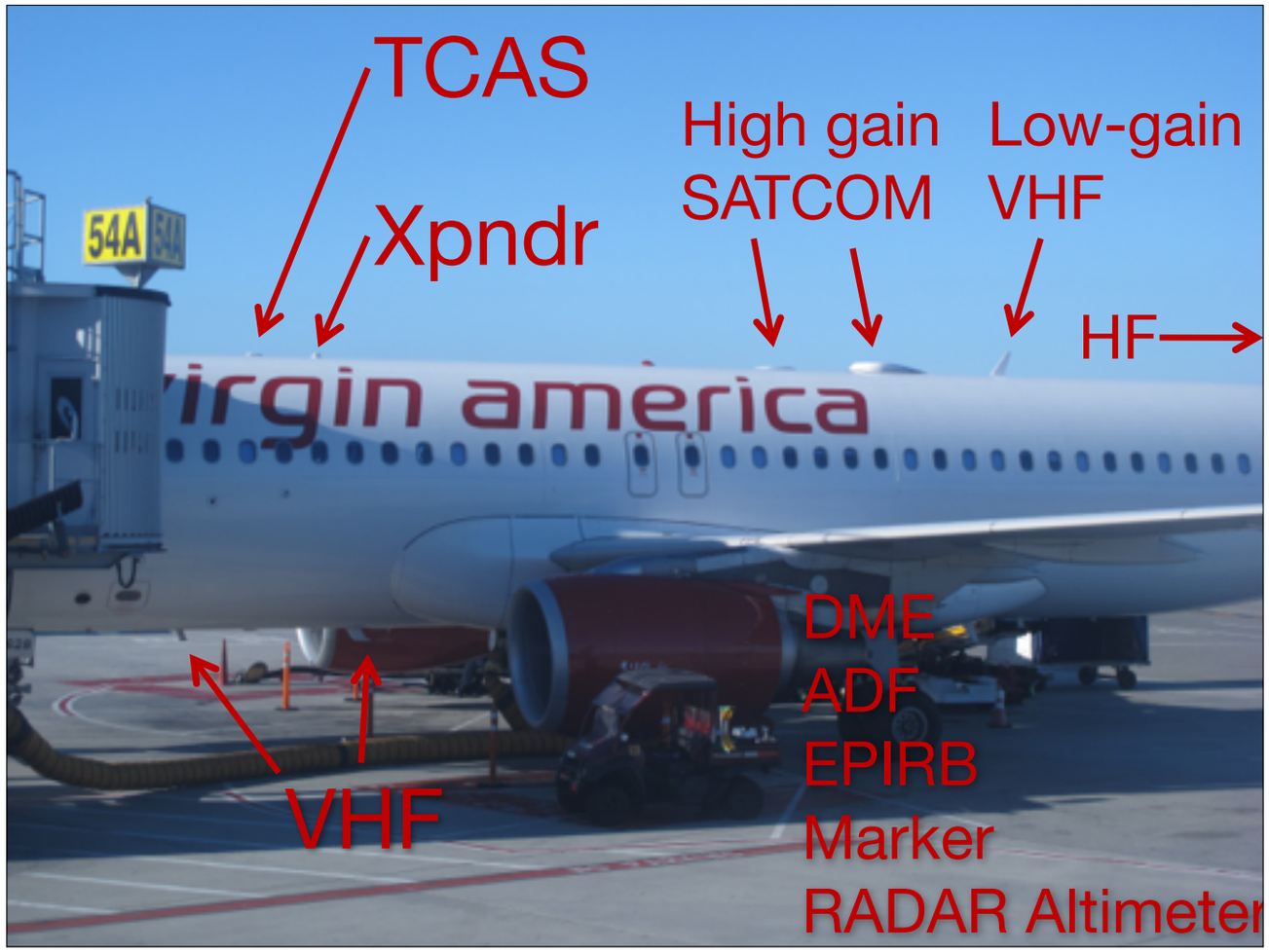
Close-up of moving target



Polar un-wrap of moving-target plot



Adding map underlay to moving-target plot



Some of the antenna positions are guesses!
HF in vertical stabilizer
Distance Measuring Equipment
Automatic Direction Finder
Emergency Position Indicating Radio Beacon

A Typical 747 has…

31 radios

- 2 x 400 W voice HF
- 3 x 25 W voice/data VHF
- 2 x 100 W 9GHz RADARs
- 2 x GPS, 1.5GHz 60 W voice/data SATCOM
- 2 x 75MHz marker beacons
- 3 x VHF LOC localiser
- 3 x UHF glide slope
- 2 x LF ADF automatic direction finder
- 2 x VOR VHF omni-directional range
- 2 x 1GHz 600 W transponders
- 2 x 1GHz 700 W DME distance measuring equipment
- 3 x 500mW 4.3GHz radar altimeters
- 3 x 406MHz EPIRB

Position

Heading

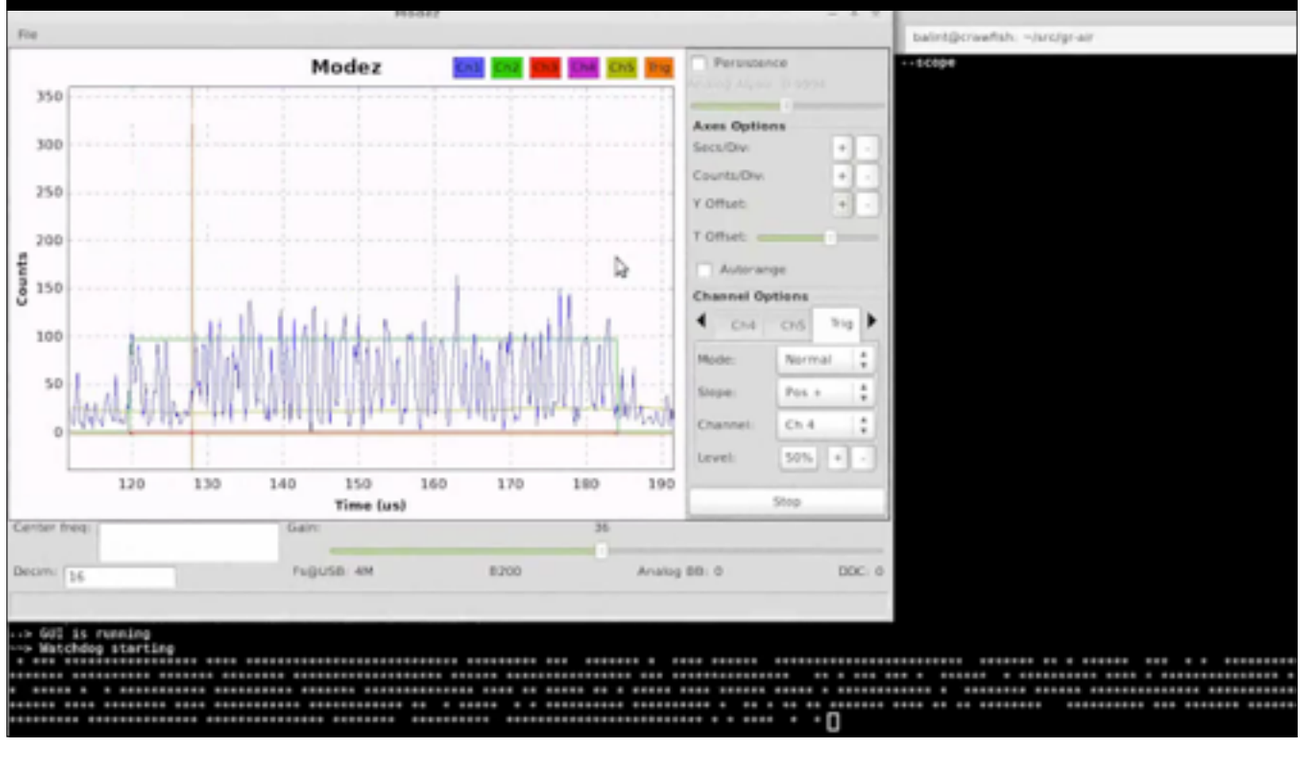
Altitude

Vertical rate

Flight ID

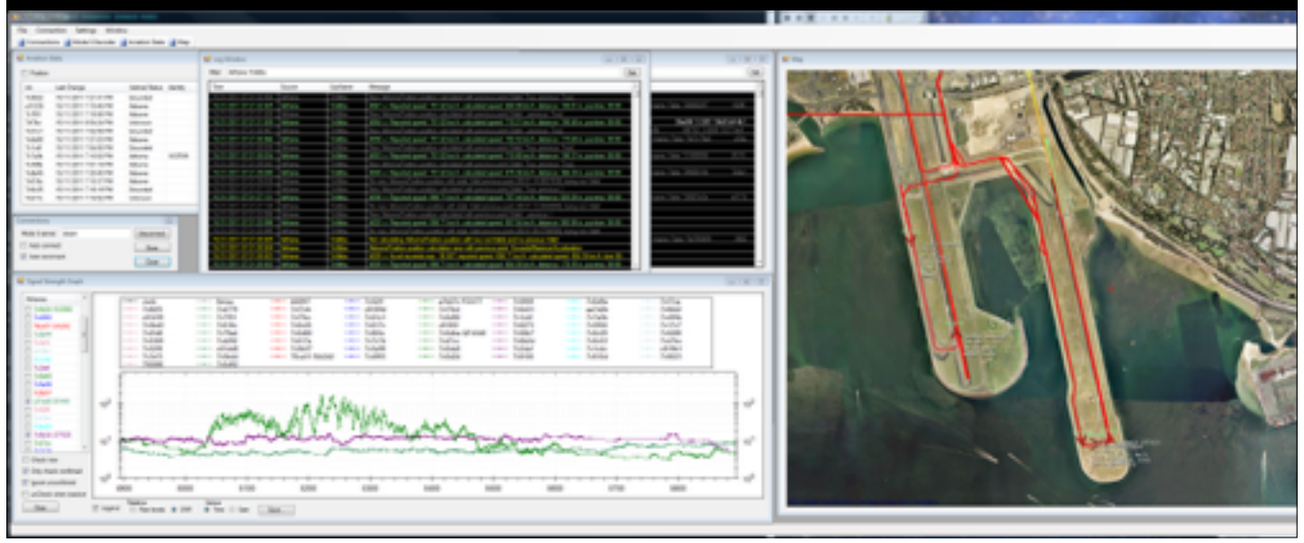
Squawk code

Mode S Decoder

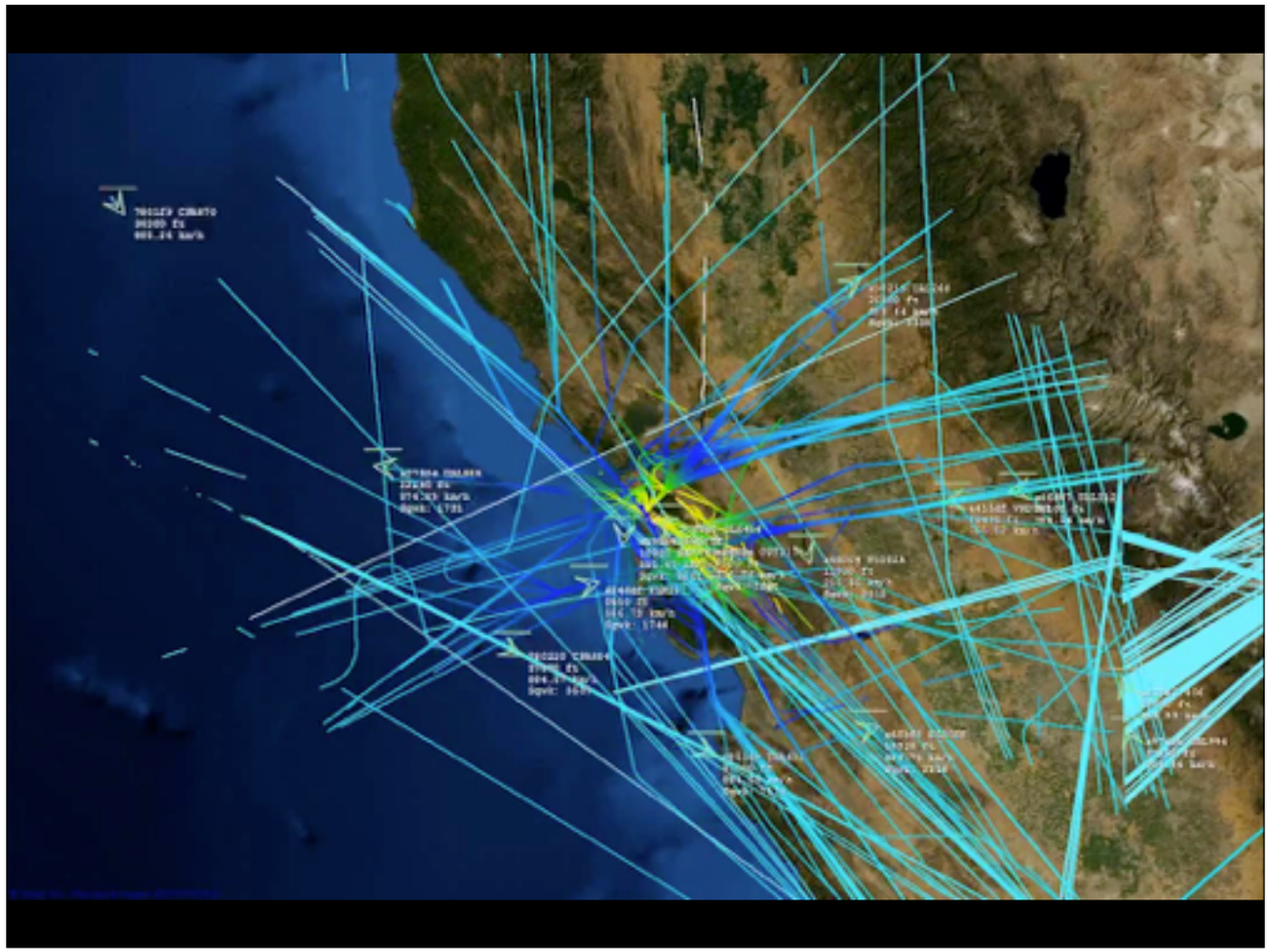


Aviation **Map**per

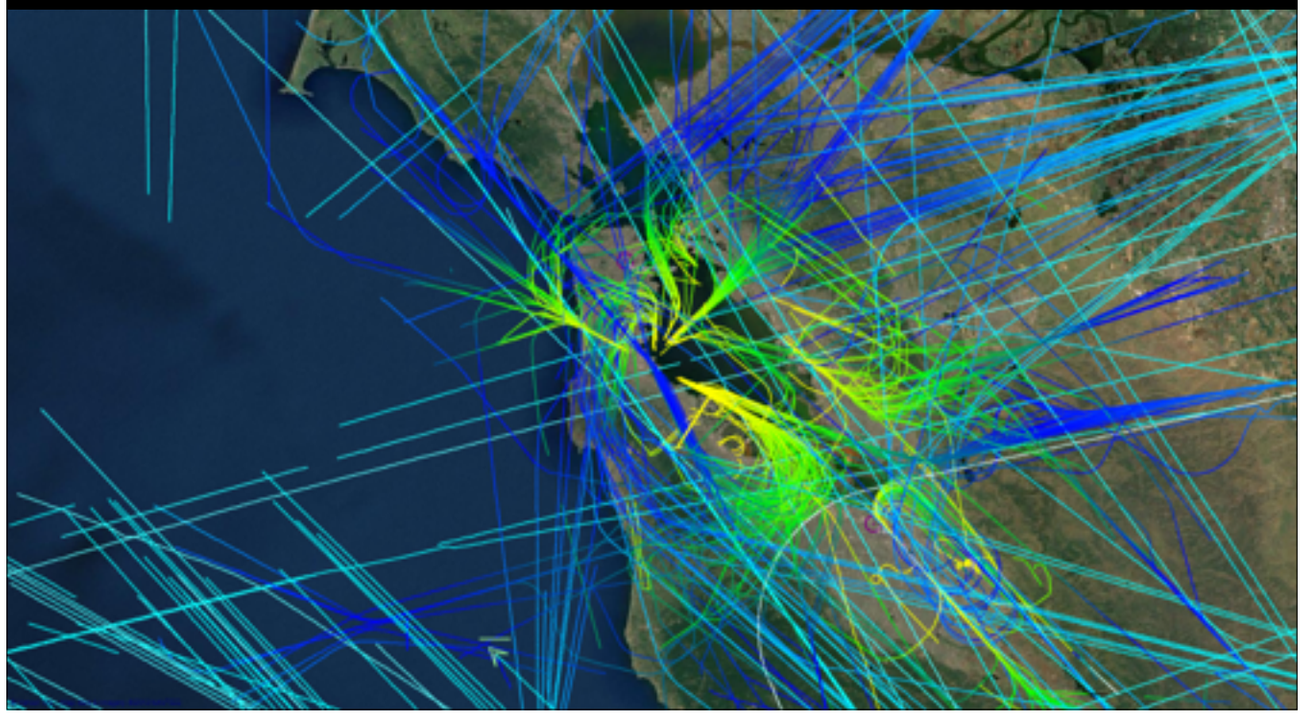
- Connects to Mode S decoder server
- Tracks & plots airframes, collects statistics
- Provides state server for web streaming



http://spench.net/drupal/research/mode-s



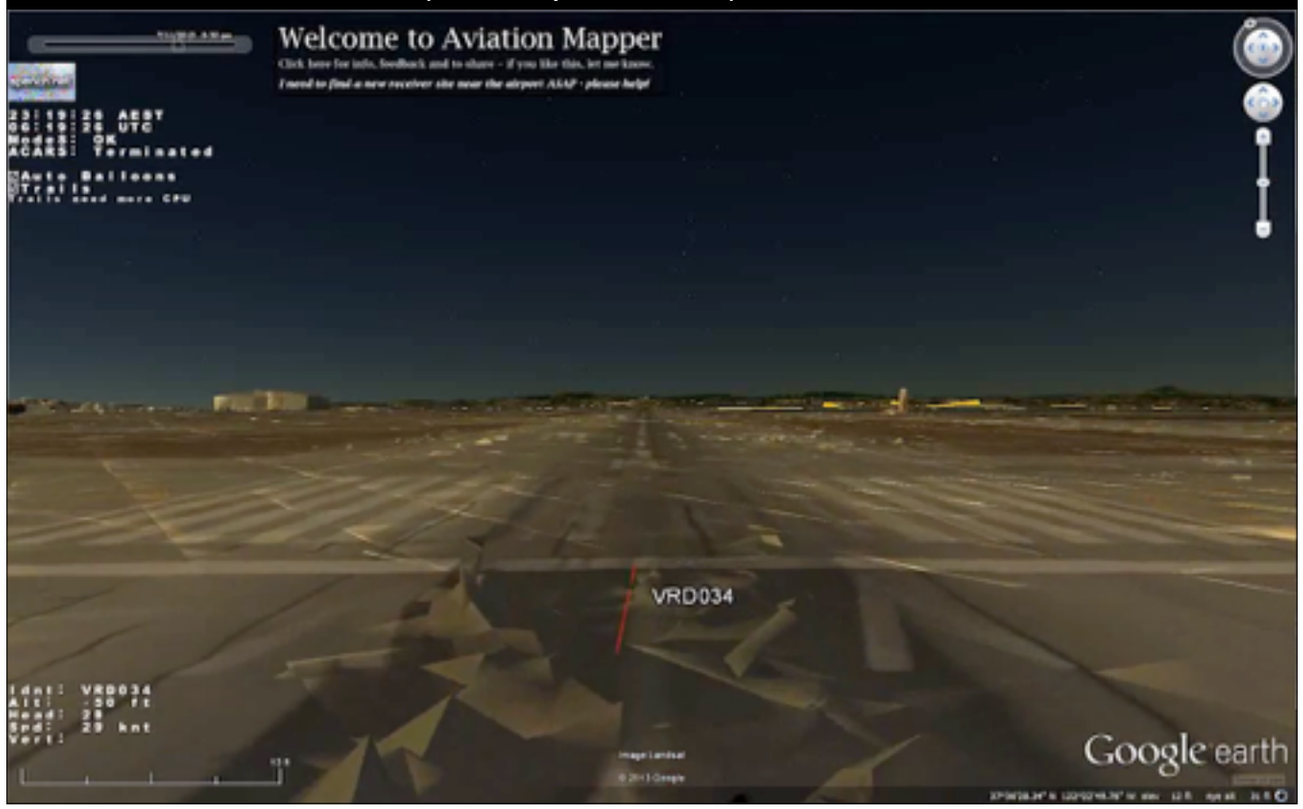
Aircraft Trails with Colour-coded Altitude



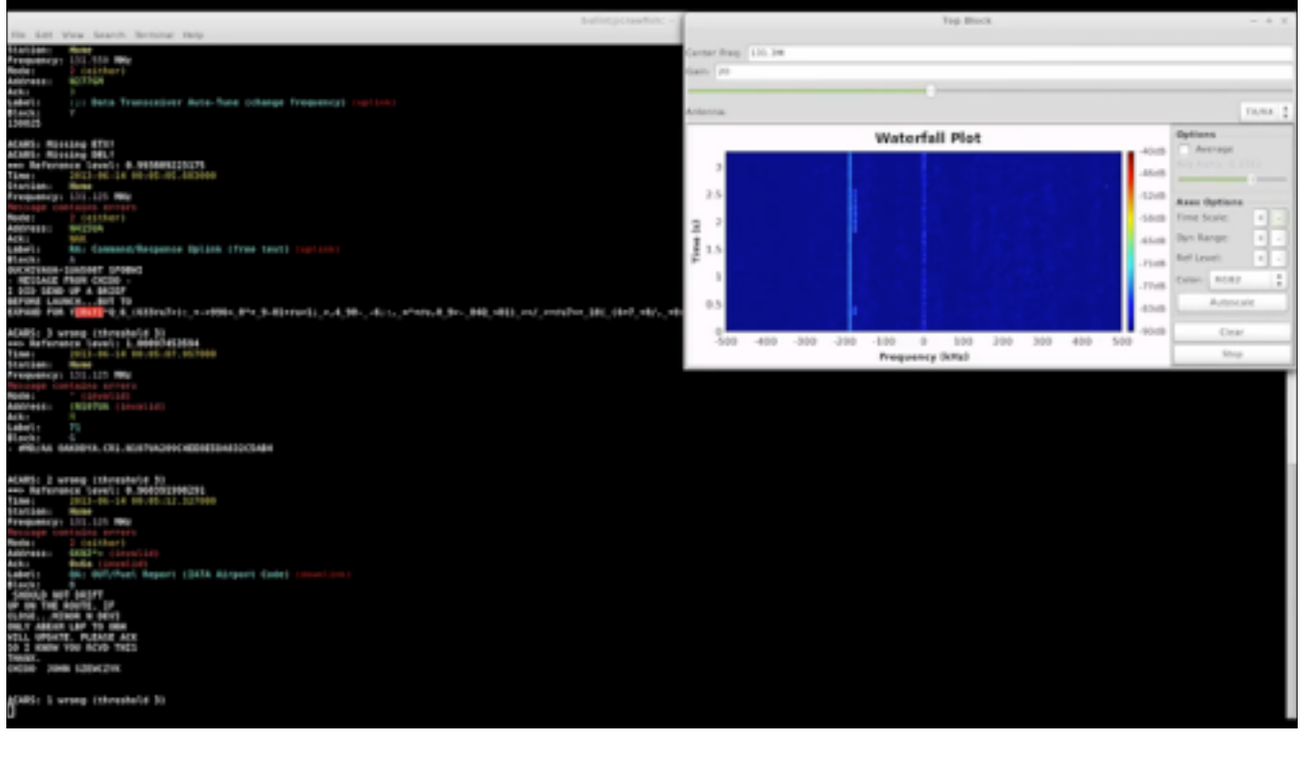
Bay Area.
Trails are altitude colour-coded.

Landing at SFO

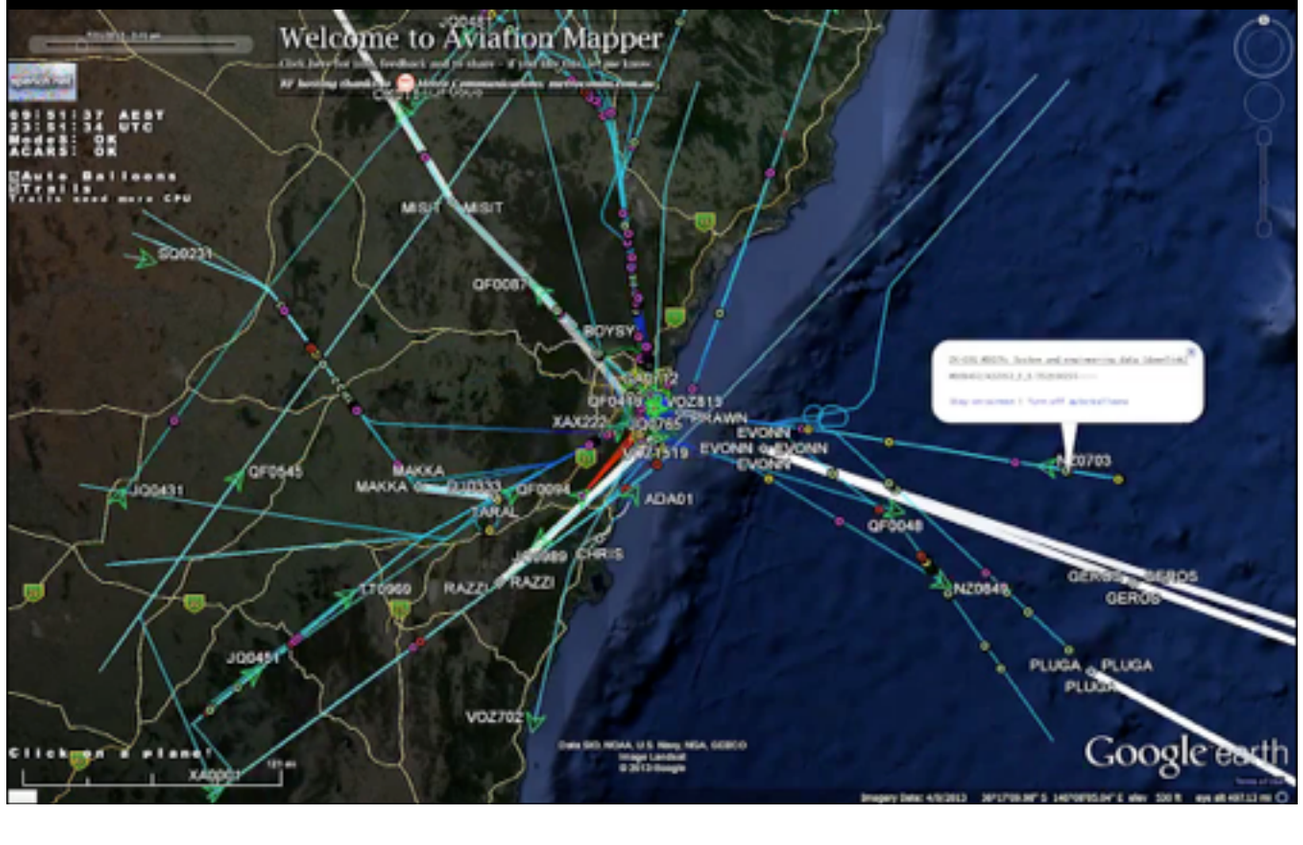
Takeoff at SFO (Cockpit View)



ACARS Decoder



Combined Mode S & ACARS

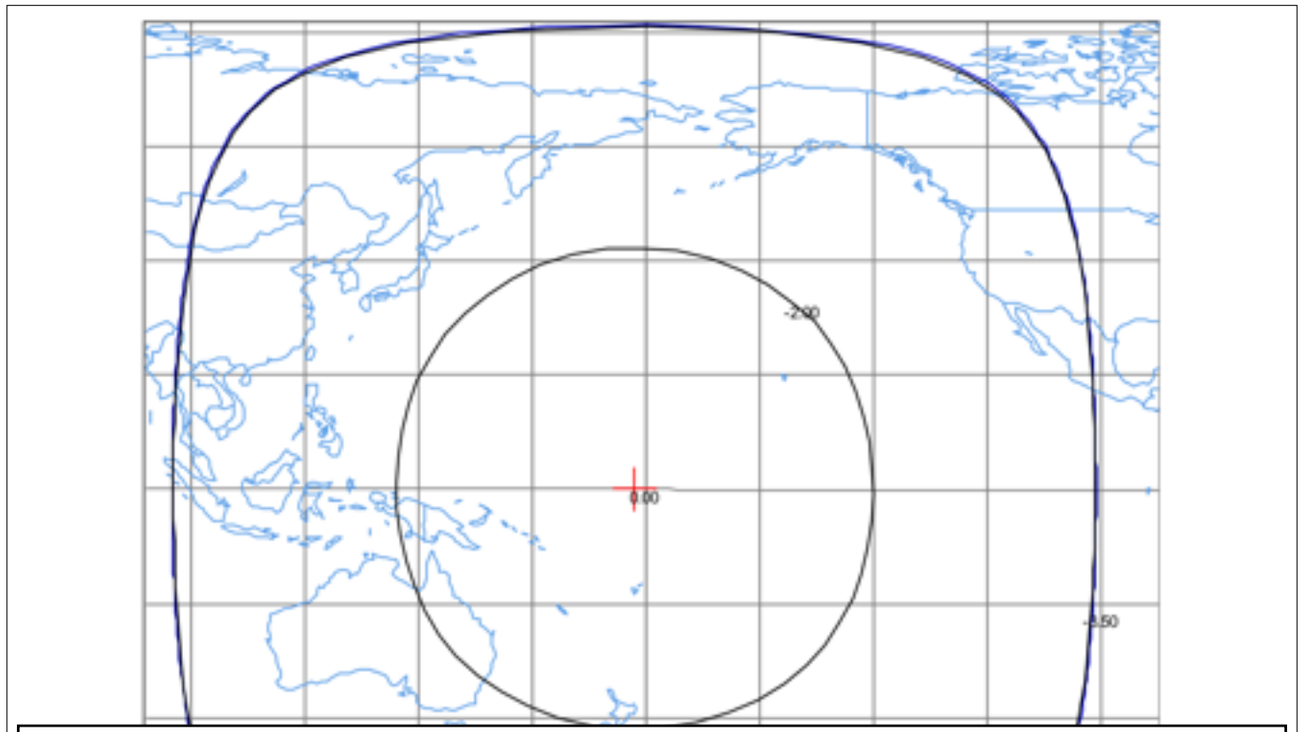


‘Engineering’ Status Messages over ACARS

Easter Egg

Waypoints Transmitted over ACARS

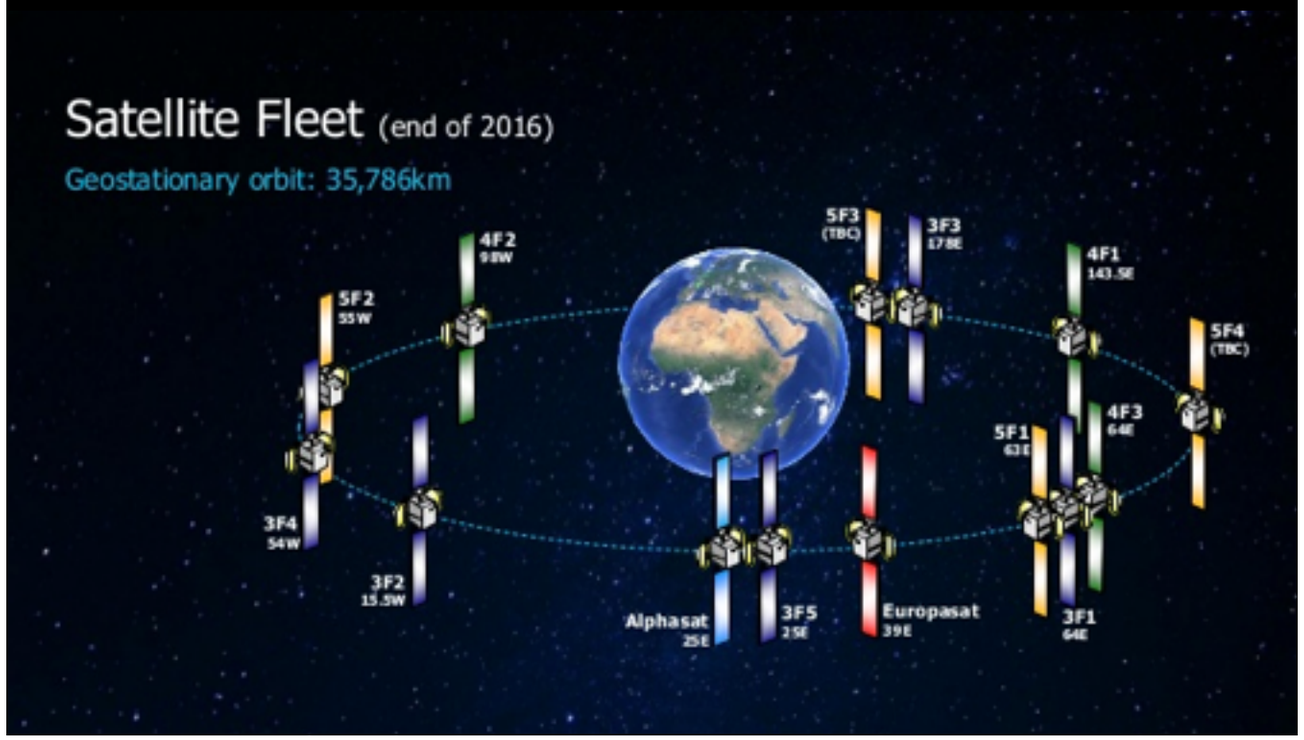
Long-haul flights into Asia

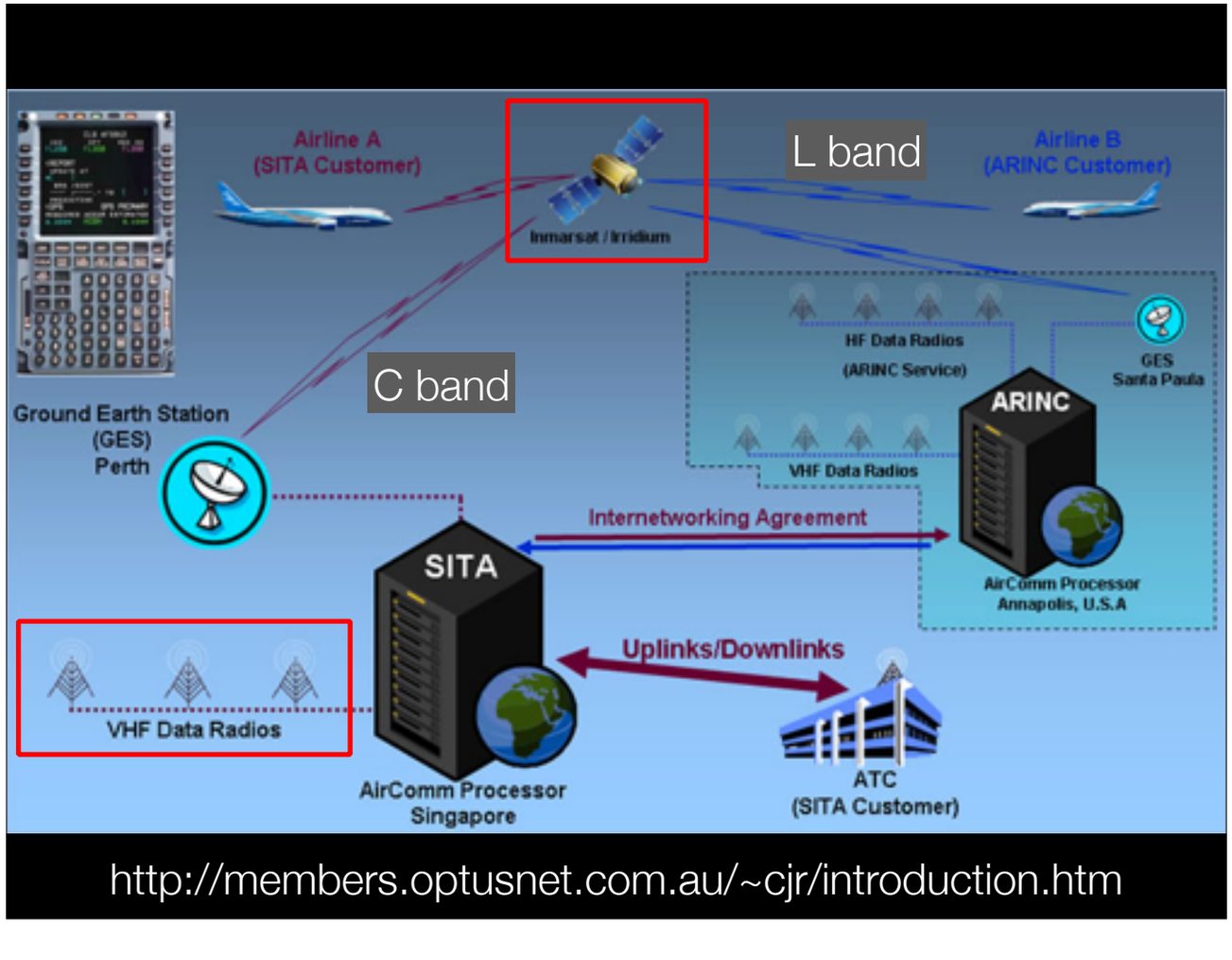


http://licensing.fcc.gov/cgi-bin/ws.exe/prod/ib/forms/attachment_menu.hts?id_app_num=68368&acct=263899&id_form_num=13&filing_key=-127644

INMARSAT-3

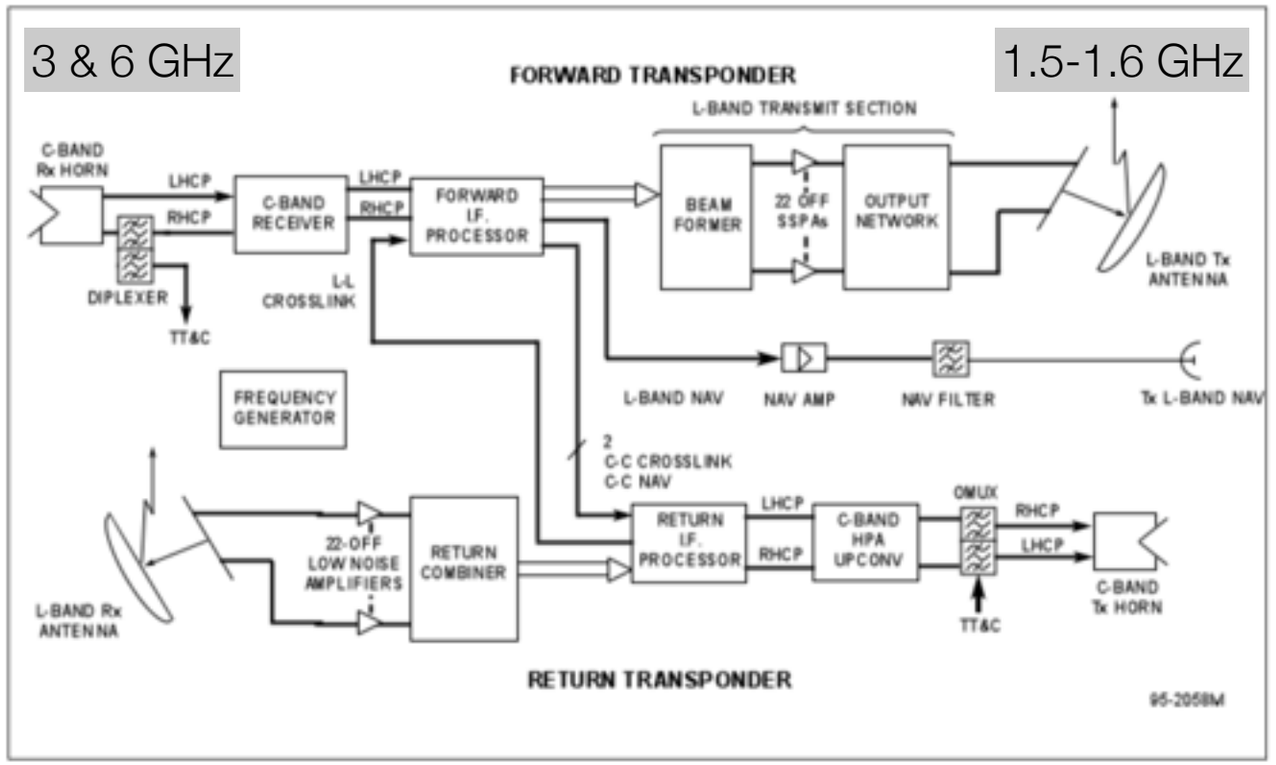
INMARSAT Geostationary Birds



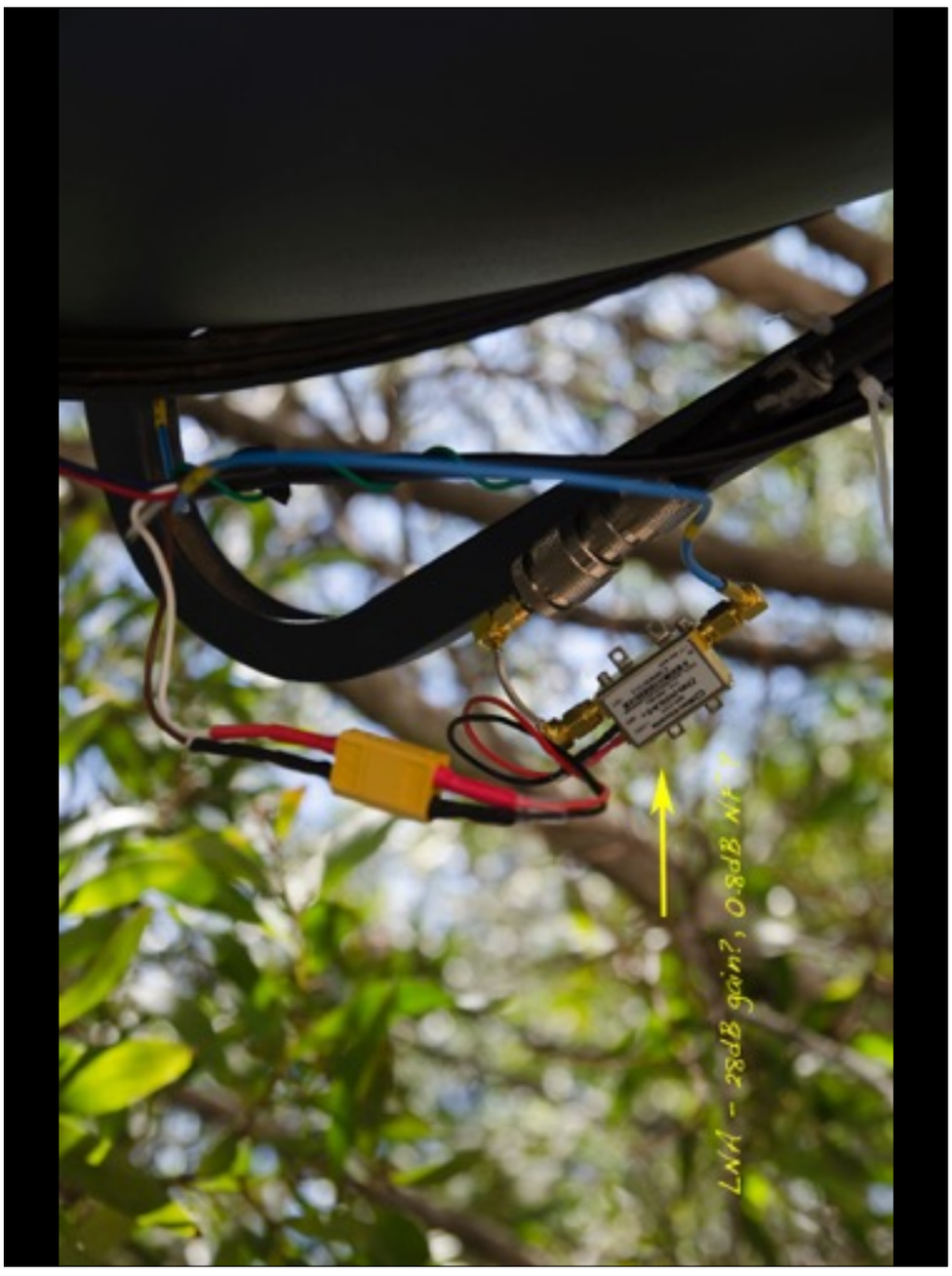


http://members.optusnet.com.au/~cjr/introduction.htm

INMARSAT ‘Bent Pipe’ Transponders



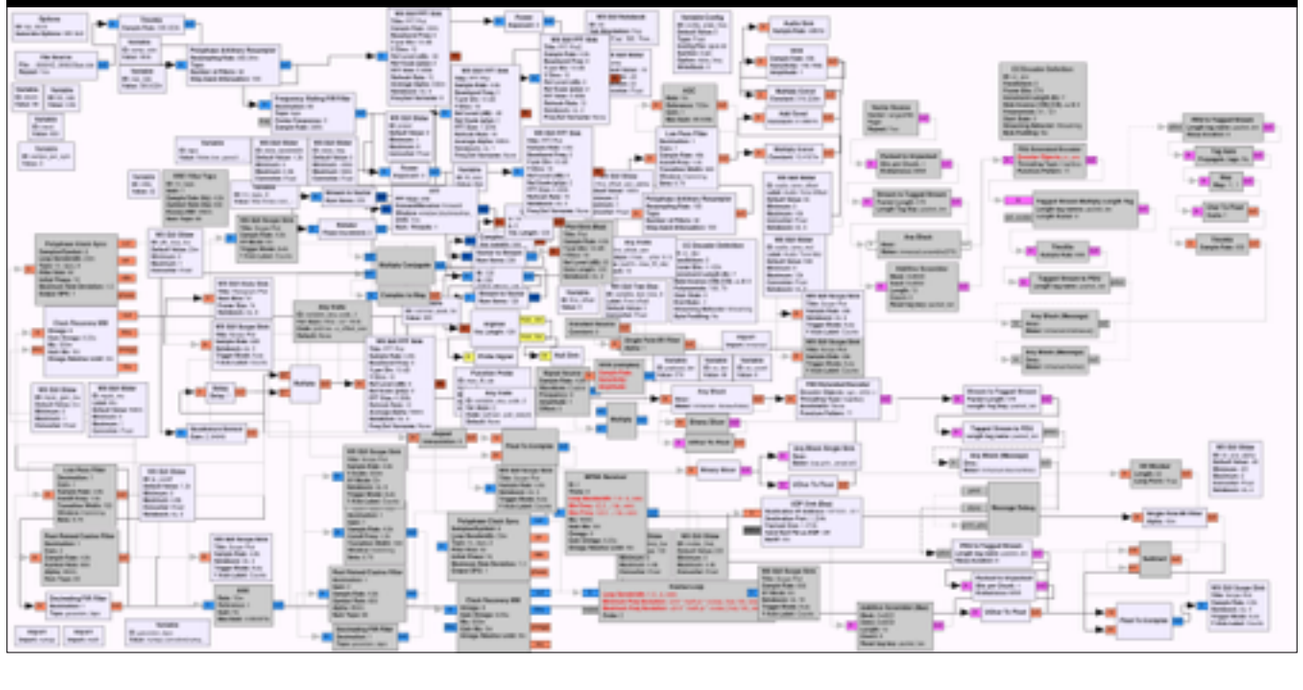

Bandpass Filter 1560MHz, 20MHz BW
LNA - Gain 41.8dB, NF 0.46dB
LH/CP Helical Feed

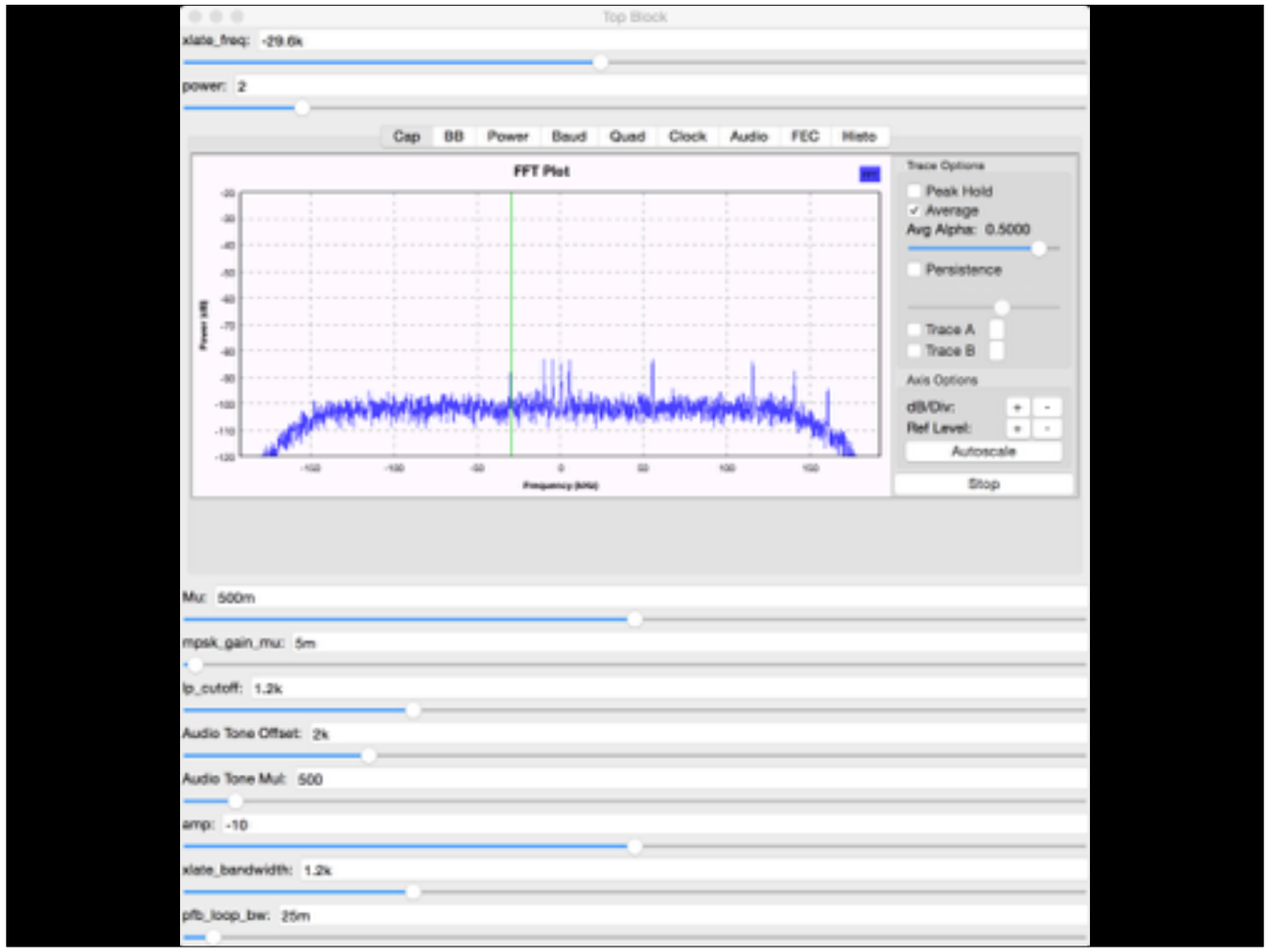

LNA - 28dB gain?, 0.8dB NF?

INMARSAT Aero

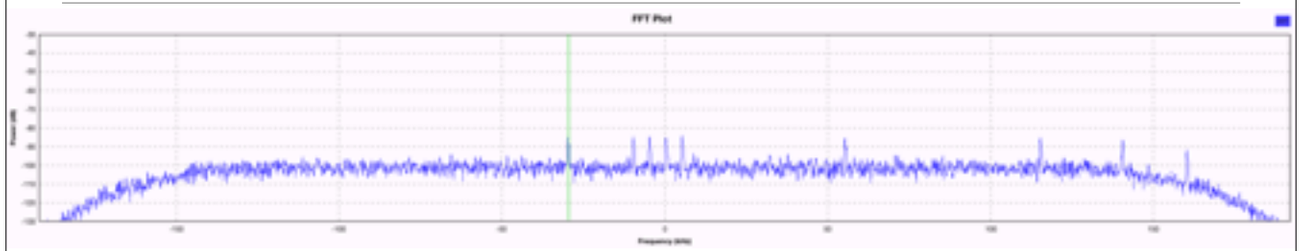
- **P Channel** - *coordination and timing begins here!*
  - Packet mode Time Division Multiplex (TDM)
  - Sent *to* aircraft, carries signalling & user data
- R Channel: random access signalling & user data, *from* aircraft
- T Channel: Reservation TDMA, *from* aircraft, for data transmission
- C Channel: Circuit-mode, *to & from* aircraft, carries voice and user data

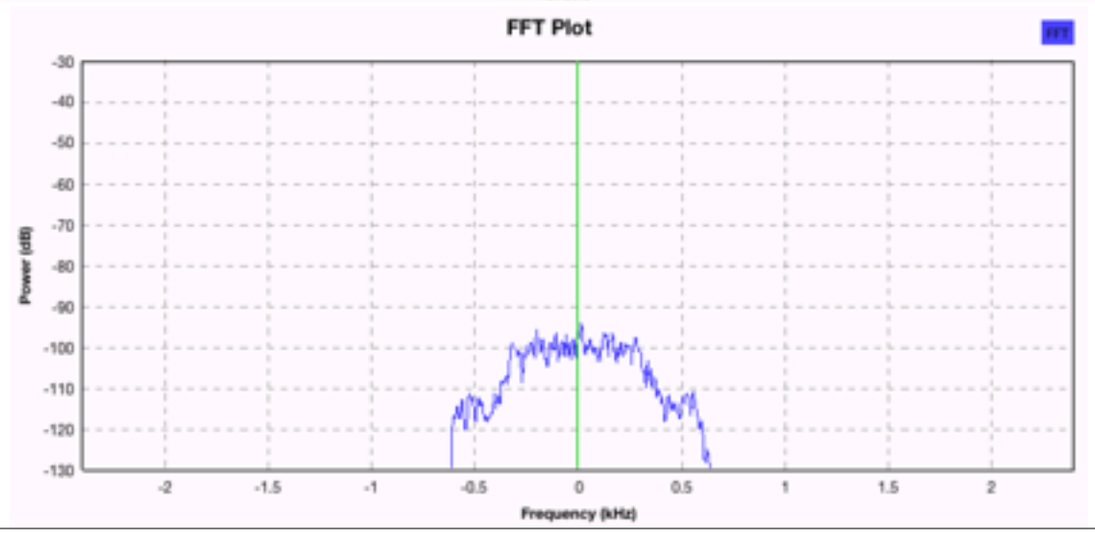
The P Channel Flowgraph so far…




Top Block
xlate_freq: -29.6k
power: 2
Cap
BB
Power
Baud
Quad
Clock
Audio
FEC
Histo
FFT Plot
Trace Options
Peak Hold
Average
Avg Alpha: 0.5000
Persistence
Trace A
Trace B
Axis Options
dB/Div:
Ref Level:
Autoscale
Stop
Mu: 500m
mpsk_gain_mu: 5m
lp_cutoff: 1.2k
Audio Tone Offset: 2k
Audio Tone Mul: 500
amp: -10
xlate_bandwidth: 1.2k
pfb_loop_bw: 25m

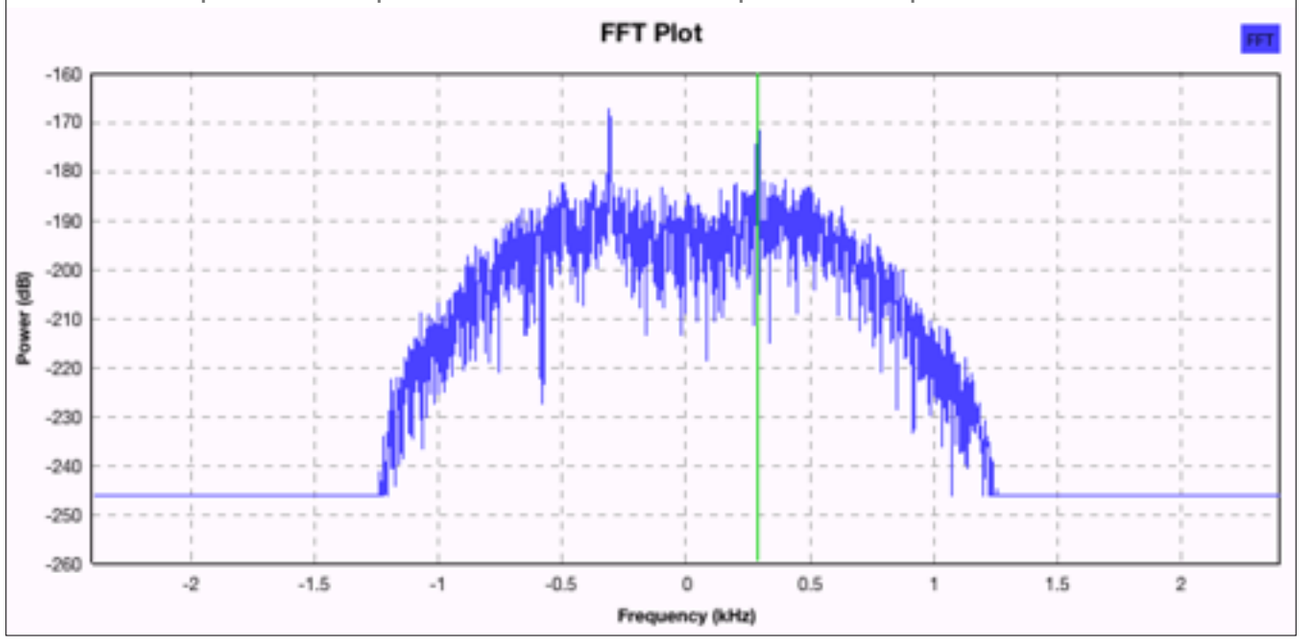
Channel Selection





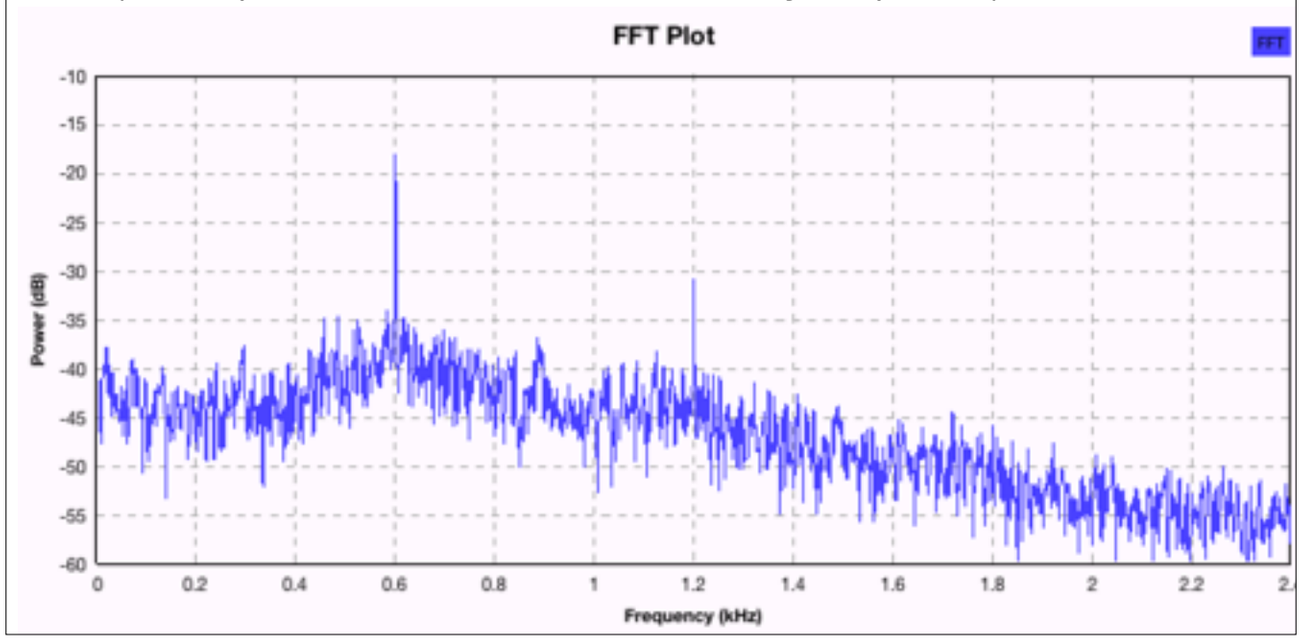
Modulation Type

- **G**aussian **M**inimum **S**hift **K**eying (GMSK): FFT of squared complex samples results in two peaks equidistant from 0



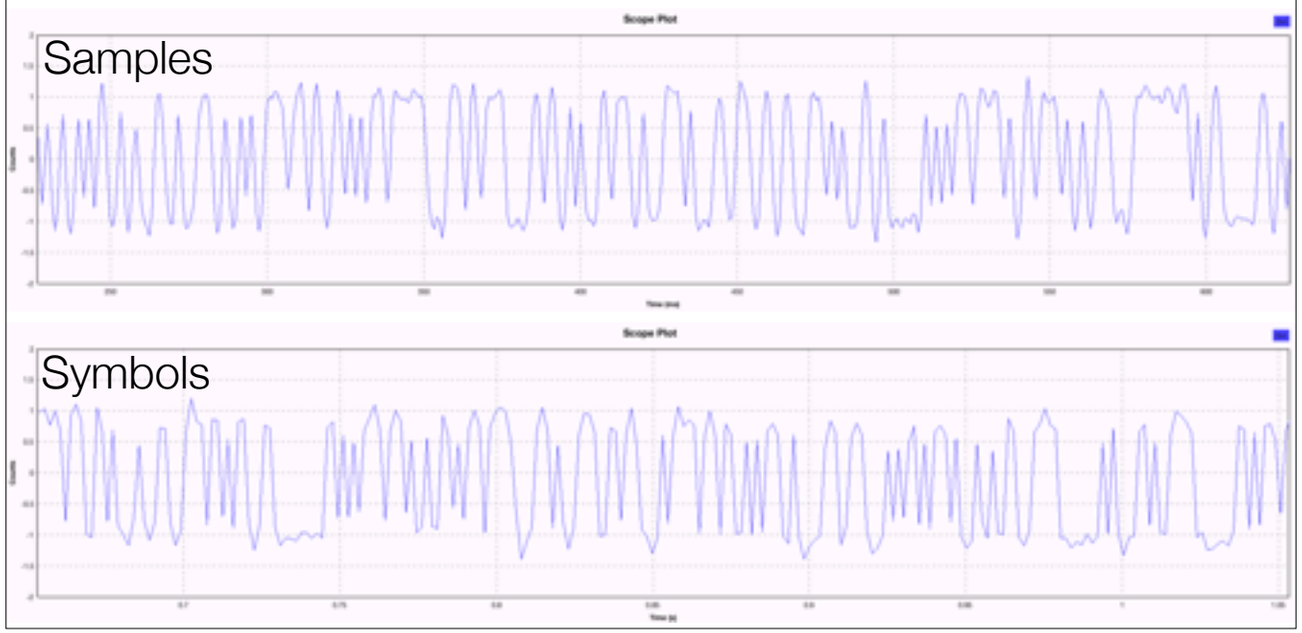
Symbol (Baud) Rate

- Cyclostationary Analysis: rate is first peak in plot (600 bps, also distance between cyclo peaks)



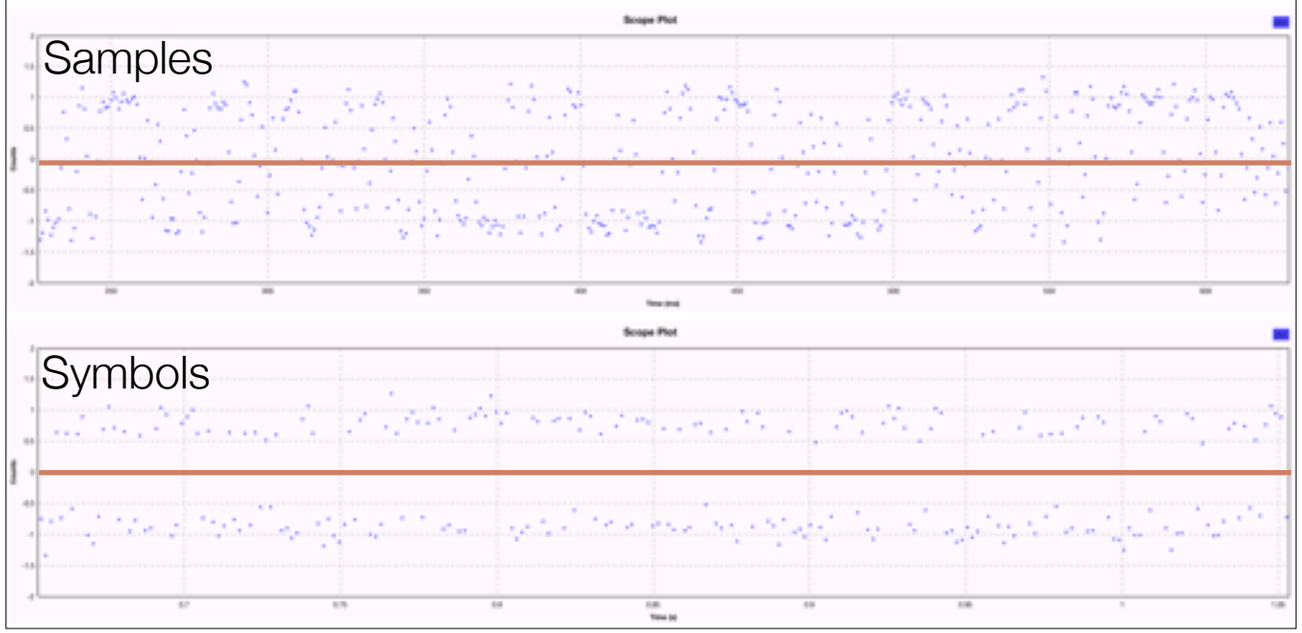
Clock Recovery

- Enough information to begin tracking symbols in channel (and output them to enable operation on bits)



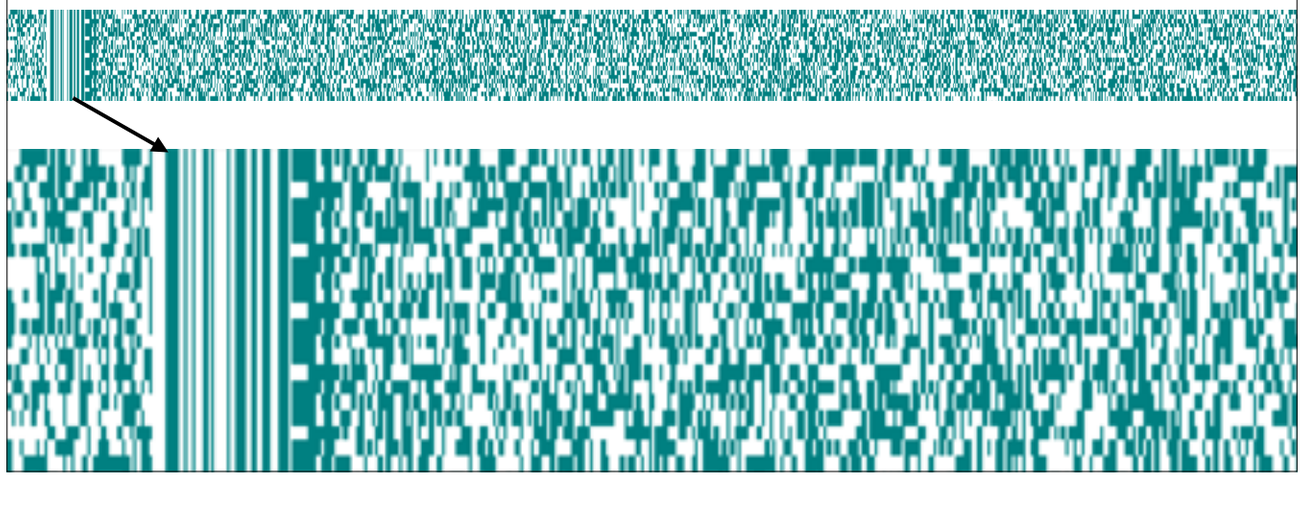
Clock Recovery Quality

- Increased separation between symbols about 0



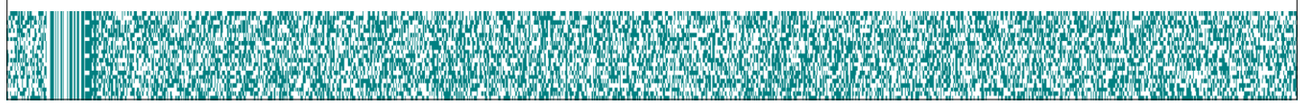
Frame Structure

- Search for repeating patterns in raster plot
  - 1200 bits wide (line up pattern vertically): unique word (sync), frame header, payload



Payload Encoding

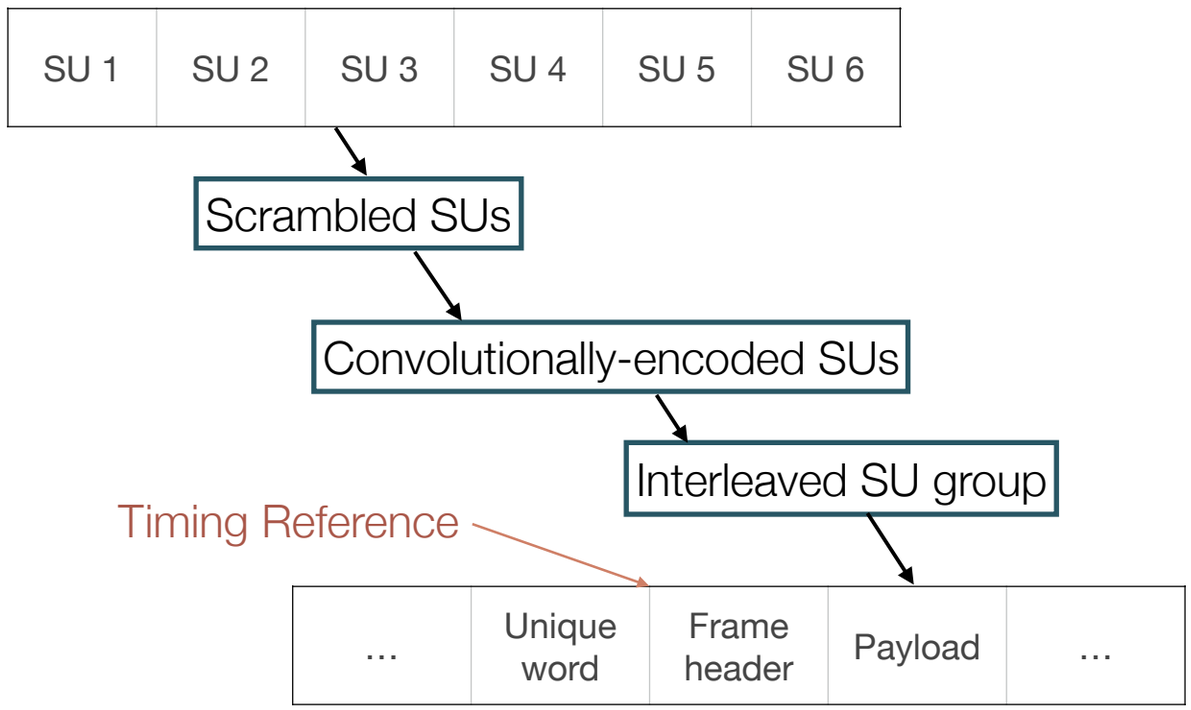
- Appears ‘random’
- Generally data has gone through:
    1. Interleaving (protects against burst errors)
    2. **F**orward **E**rror **C**orrection (data redundancy)
    3. Scrambling (energy dispersal & clock recovery)
- Complex process - difficult to test each step individually



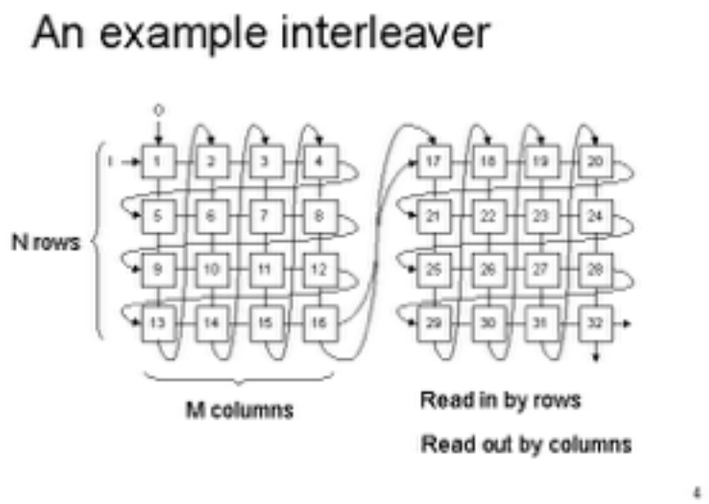
Payload Details

- RTFM
- Frame payload consists of multiple fixed-length Signal Units (number of SUs depends on data rate of channel, here 6 of 96 bits each)
- For transmission, the entire SU group is:
    1. scrambled
    2. 1/2-rate convolutionally encoded
    3. fed through an interleaver

Frame Details



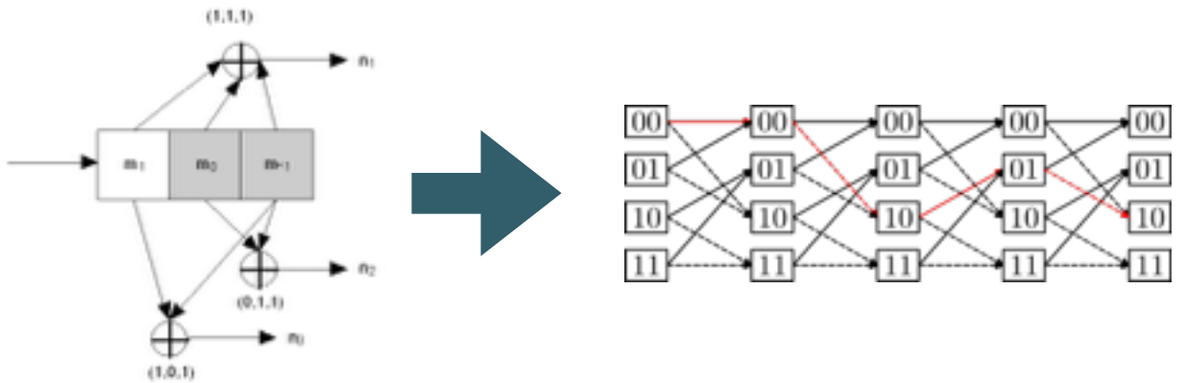
#1: De-interleaving



https://www.cl.cam.ac.uk/~jac22/otalks/rtpi/sld004.htm

#2: Convolutional (Viterbi) Decoding

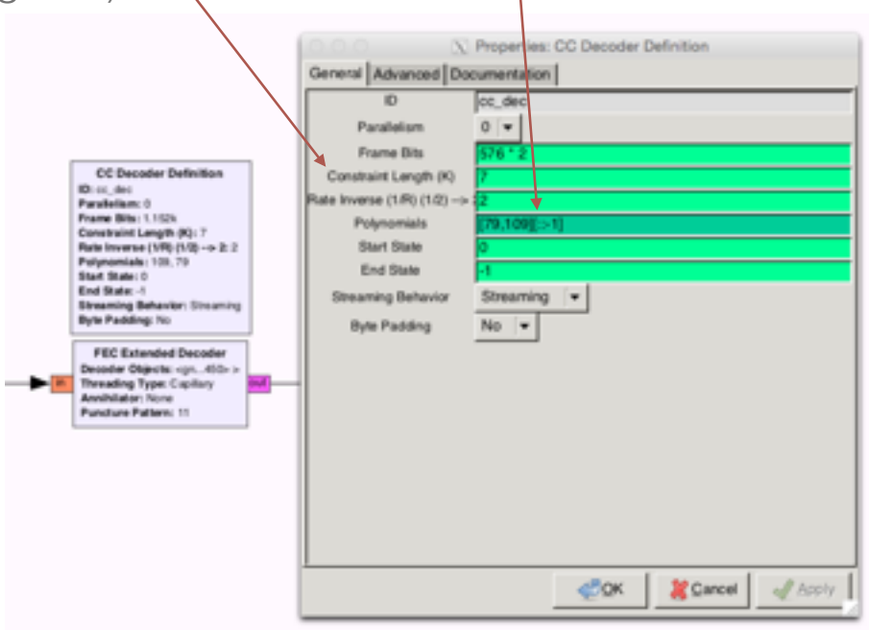
- A convolutional code adds additional bits to a stream so that a receiver can correct errors
- Given received error-prone symbols, a Viterbi decoder will output the bits that represent the most likely path through a trellis matching the convolutional code



https://en.wikipedia.org/wiki/Convolutional_code

#2: Viterbi Decoder

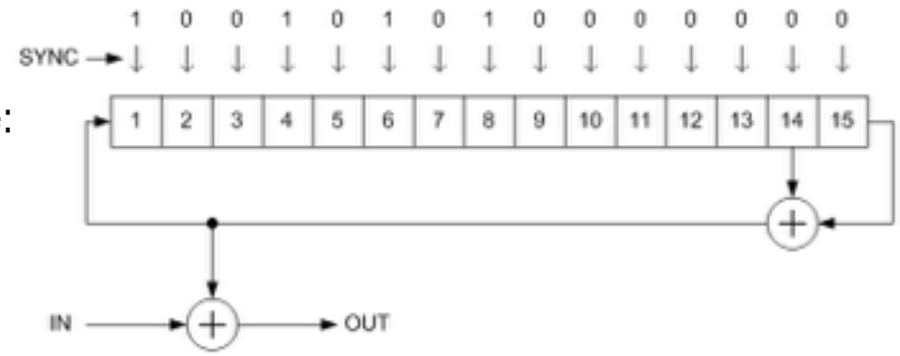
- The NASA Voyager K=7 convolutional code is popular, and used here (gr-fec)



#3: De-scrambling

- Implemented as a Linear Feedback Shift Register
- Reset (sync'd) at the beginning of a new frame

Example:



https://en.wikipedia.org/wiki/Scrambler

Validation

- Inspect raster plot of output to check if there is more structure:

- Compute CRC checksum to confirm correct decode: CRC-16-CCITT should yield **`f0b8`**

Decoding

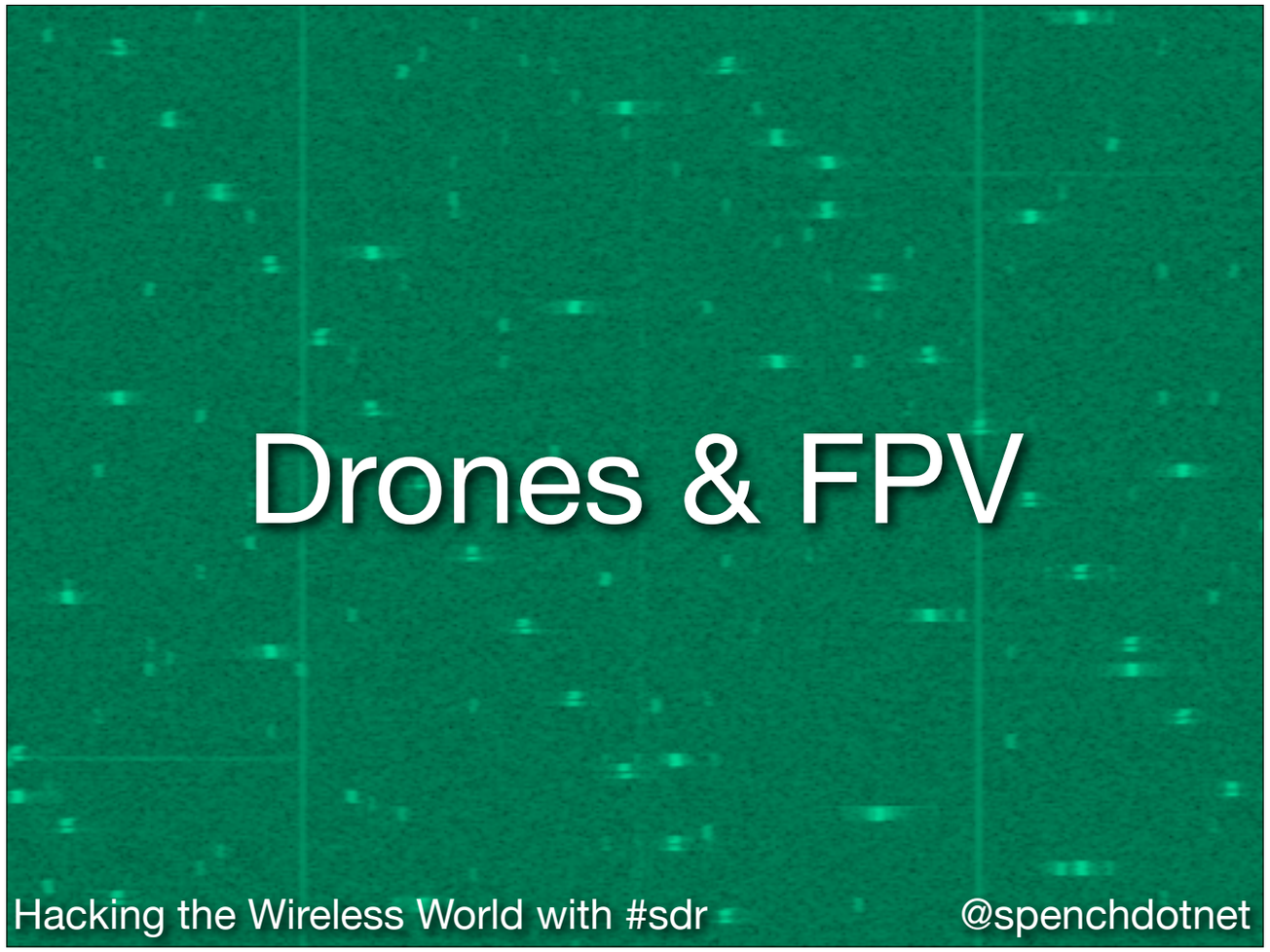
```
71780a5b82751e60ffff1c75 f0b8 ISU (User Data)
62ae146182748e0000000eee f0b8 ACK
d676d35420706167e5201a8 f0b8 User Data begins
d5762fae0d8a2fd33231cbfb f0b8
d4762f4ab0b031b52fc25cab f0b8
d376b0322f46b0342f4f8c67 f0b8
d2763131b5b0b00d8a2f437024 f0b8
d176c1c4c44954494fce4775 f0b8
d076c14c2049ce464f526db5 f0b8
11a9322582df000a84526d98 f0b8 Log on
40a9322582d831663856f222 f0b8 Channel control
c0d83781384a000000005331 f0b8
41a9322582d941063787551e f0b8 Channel control
c0d936c336b836c51101af14 f0b8
6271c274827d8e000000d259 f0b8 ACK
```

Decoding

```
cf76cdc154494fce2fae332f f0b8
ce760d8a2fc4b0324c2f7f34 f0b8
cd76ae2f542fae0d8a2f3719 f0b8
cc76c8b032b3b32fae2f10bd f0b8
cb764f31b6b0b02faec1be14 f0b8
ca76f2f2e97661ec20678197 f0b8
c97661f4e5206e756d624cd8 f0b8
c876e5f2ba0d8a2f4f31f556 f0b8
c776b6b0b02f5831b92f7d65 f0b8
c676450d8a2fd332b62f0091 f0b8
c5764f31b6b0b02fae0d2599 f0b8
c4768ac26167676167e576ea f0b8
c37620e3ec61e96d20e68b9d f0b8
c276eff220c8cbc720610933 f0b8
c176f2f2e97661ecba0db0a2 f0b8
c0768a2f9762917f0000f199 f0b8 User Data ends
```

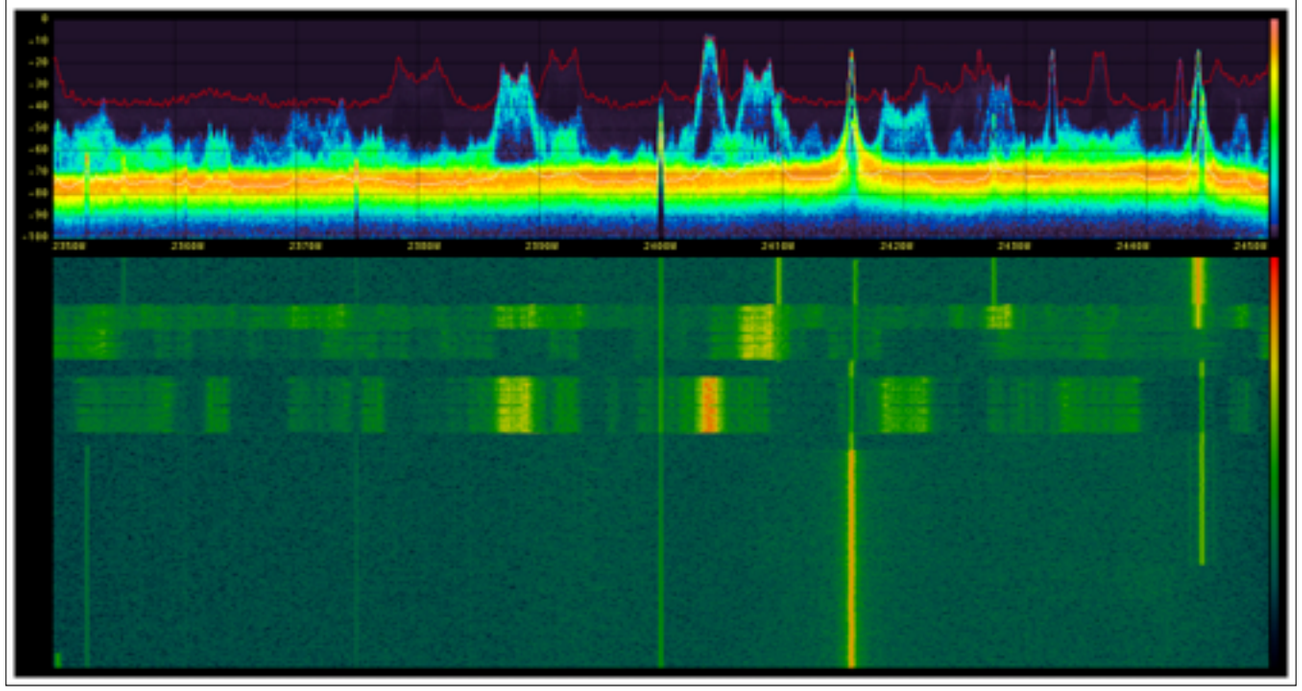
User Data: ACARS Message

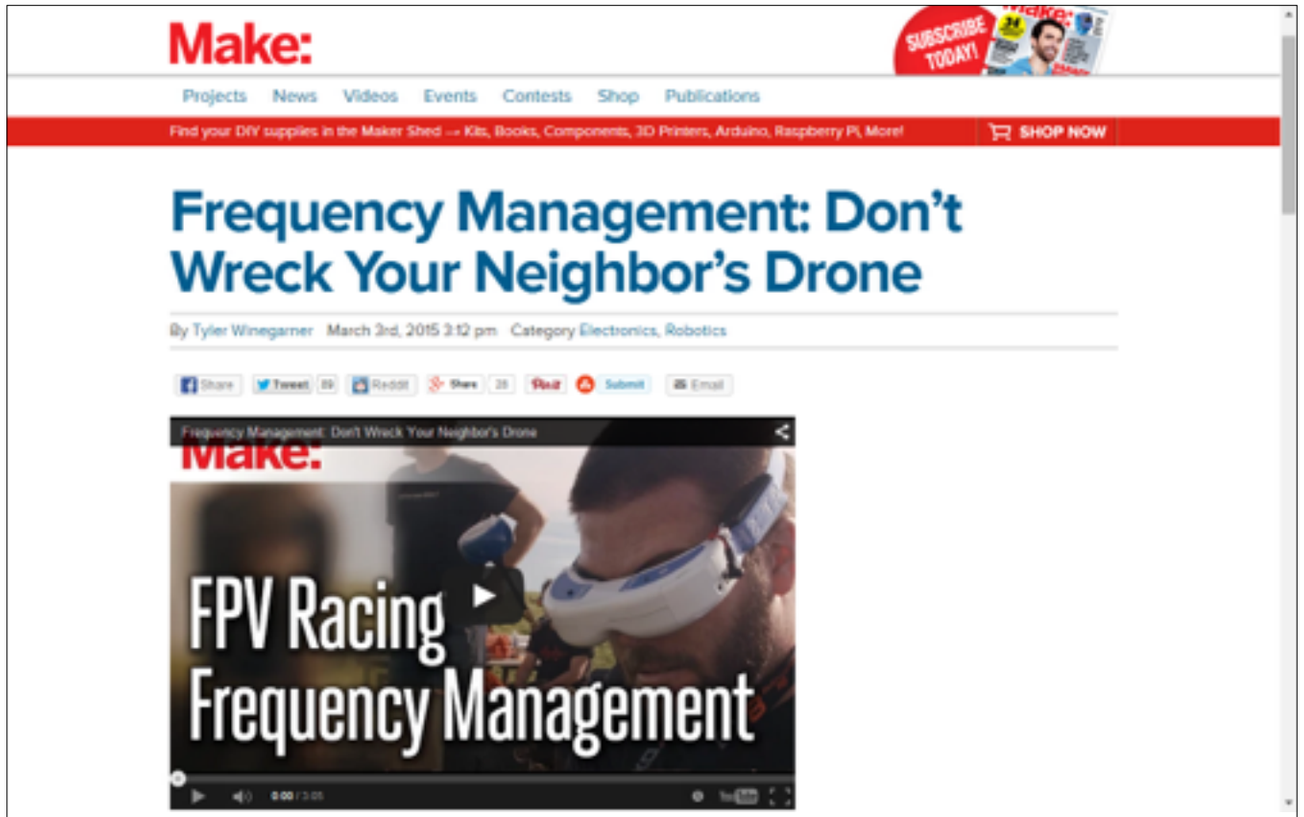

```
'\x7f\x7f\x012..B-KQK\x15H1F\x02-
#T1O1600/X26/E\r\n/S22/B02/O1600\r
\n/.Please arrive at the boarding gate at
least/.\r\n/O1500/X02/E/O1500\r\n/S23/B02/
X05/F04/O1500\r\nminutes\r\n/O1600/X12/
before departure./.\r\nLate passengers may
not be accepted for/.\r\ntravel. \x17Z
\x02\x7f'
```


Drones & FPV
Hacking the Wireless World with #sdr
@spenchdotnet


Sniffing RF uplink &
downlink with B210
Berkeley Drone meetup

2.4 GHz ISM Band Activity: Drone R/C





http://makezine.com/2015/03/03/frequency-management-dont-wreck-your-neighbors-drone/

Make:

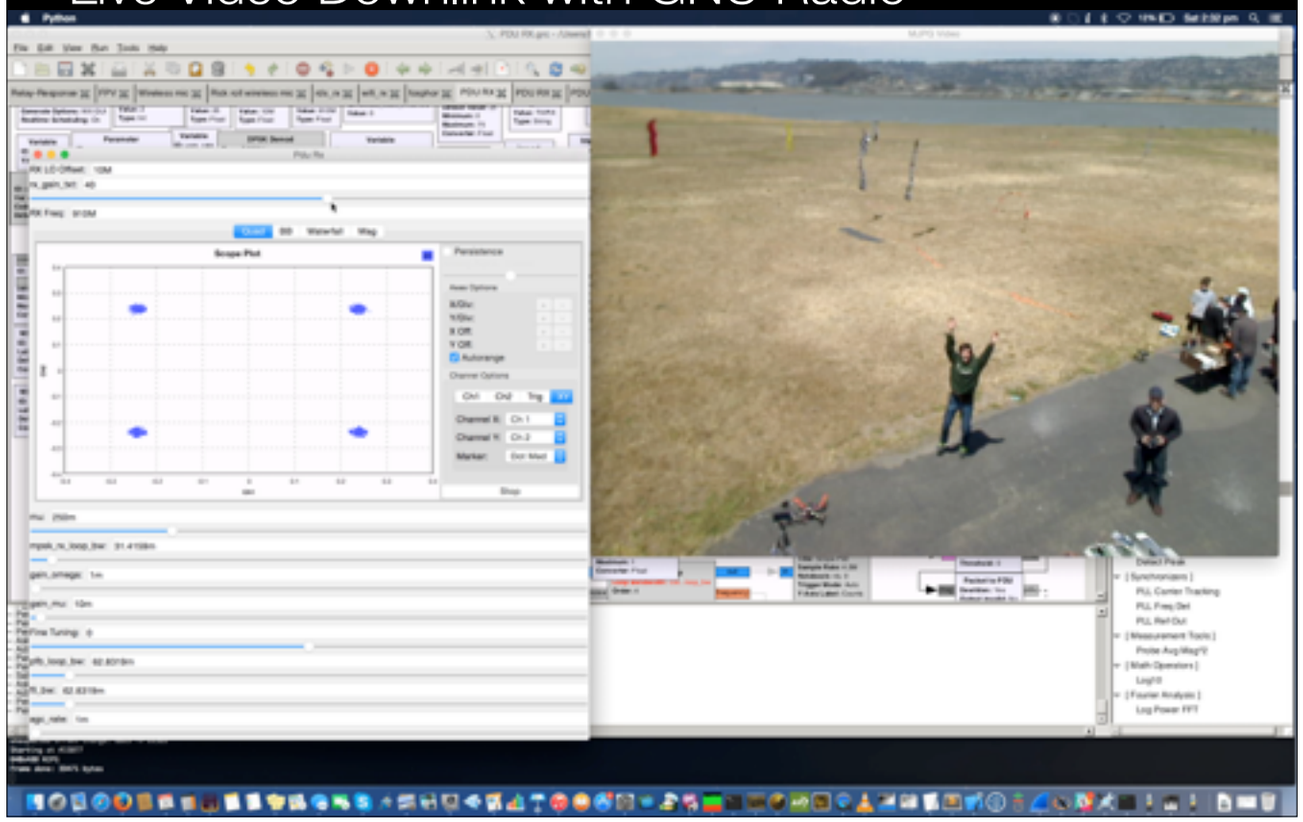
https://www.youtube.com/watch?v=oIn07J0iNDg

What are we looking at?

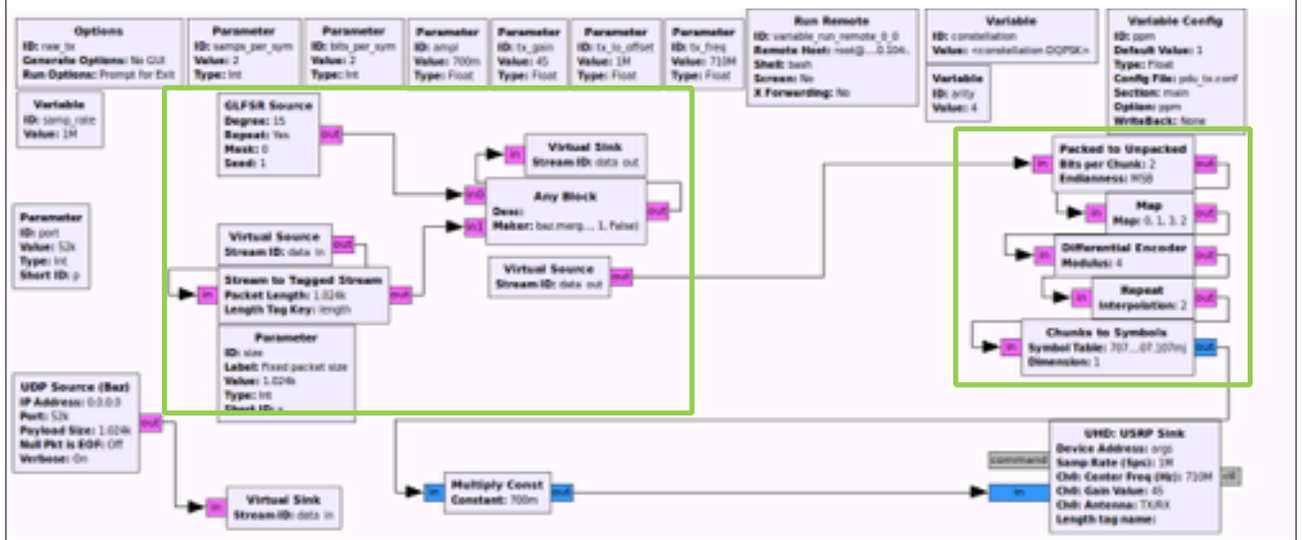
3D Robotics X8+


Webcam

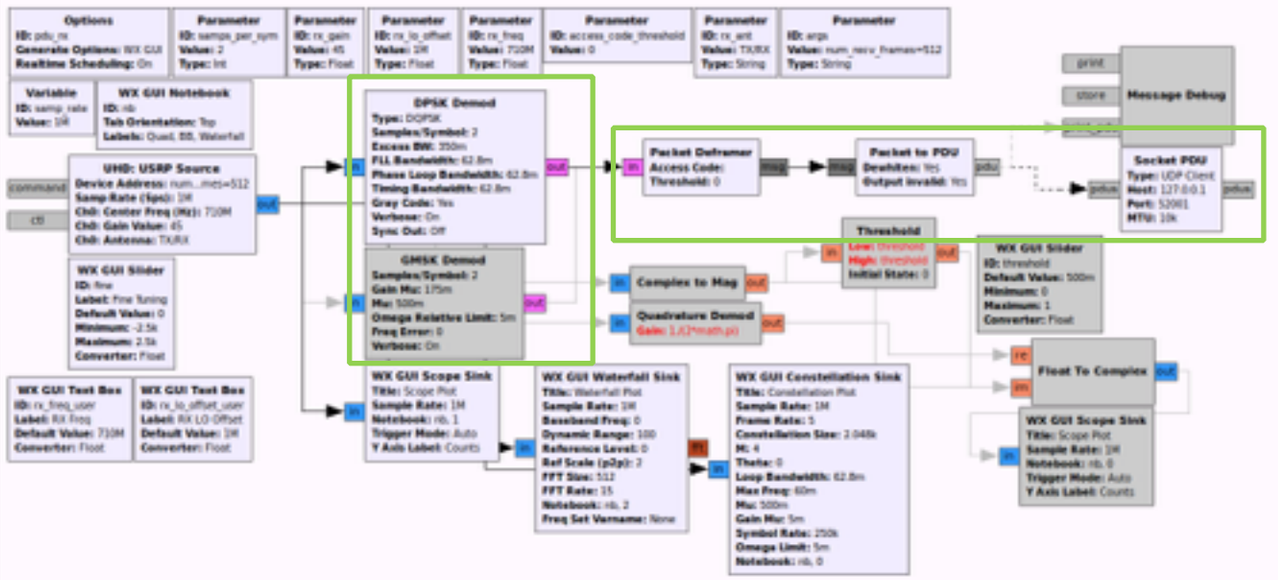
Live Video Downlink with GNU Radio

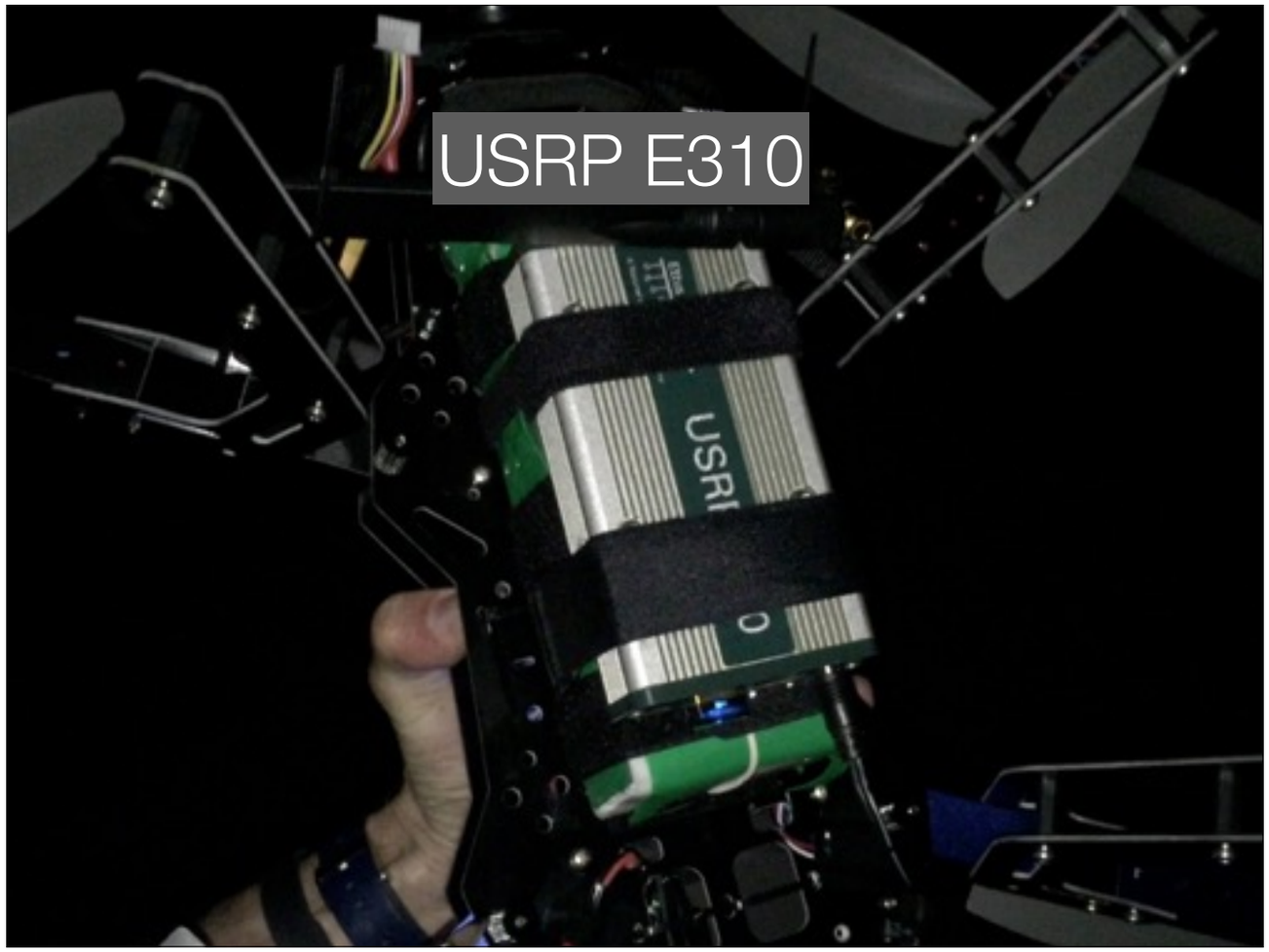


TX Flowgraph

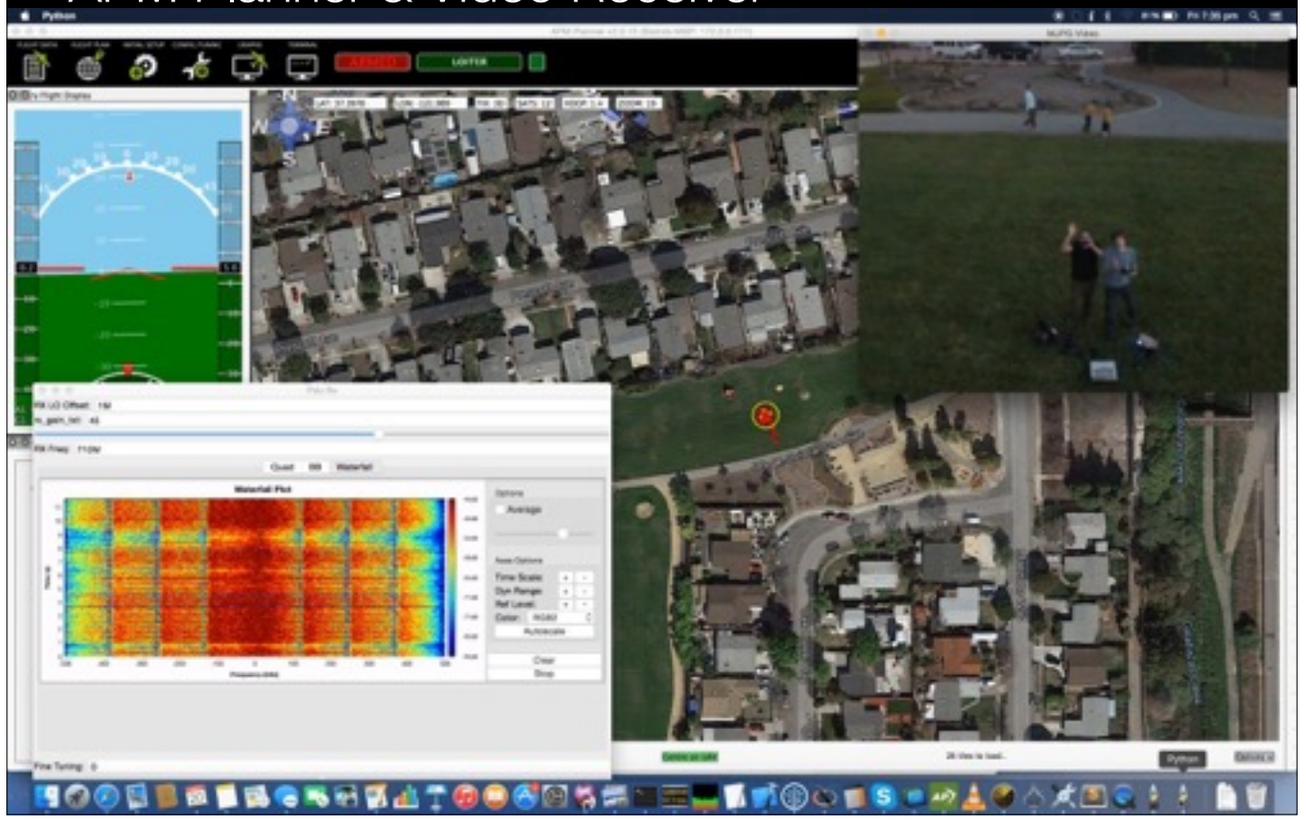


RX Flowgraph

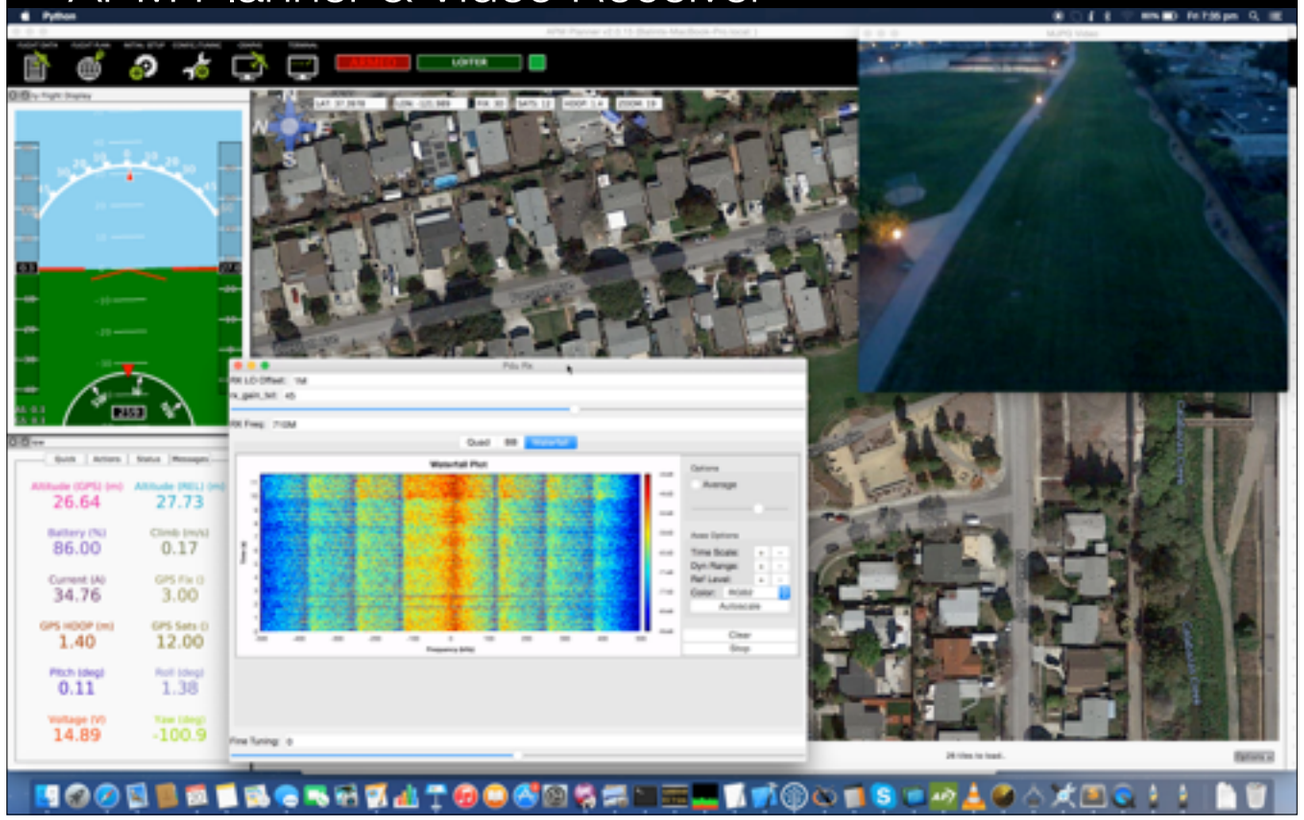



USRP E310
USRI
0

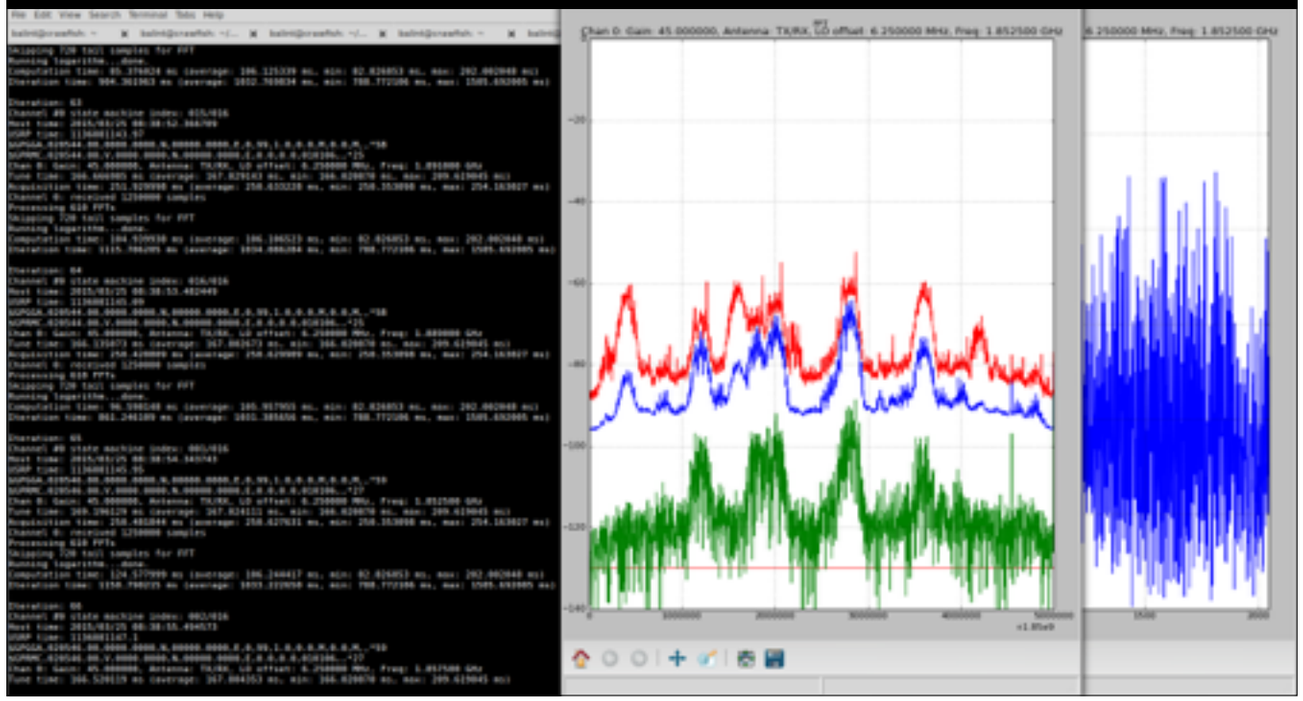
APM Planner & Video Receiver



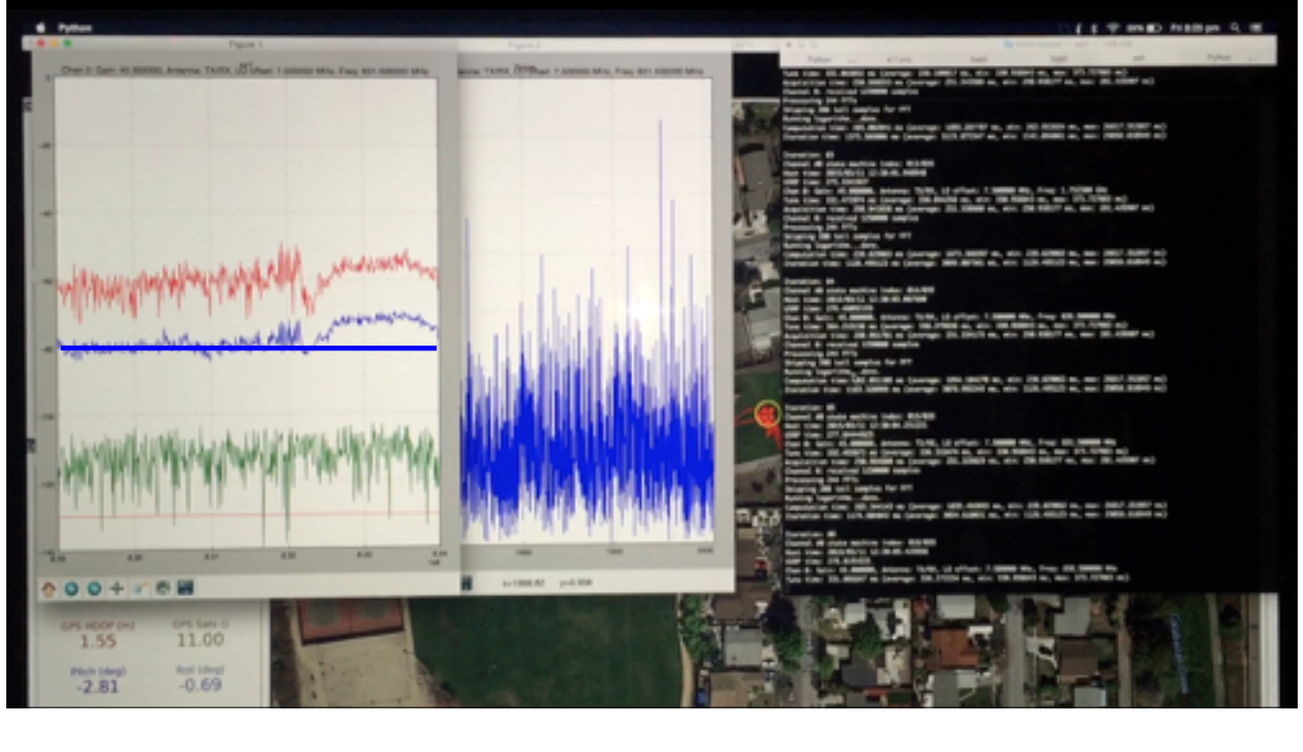
APM Planner & Video Receiver



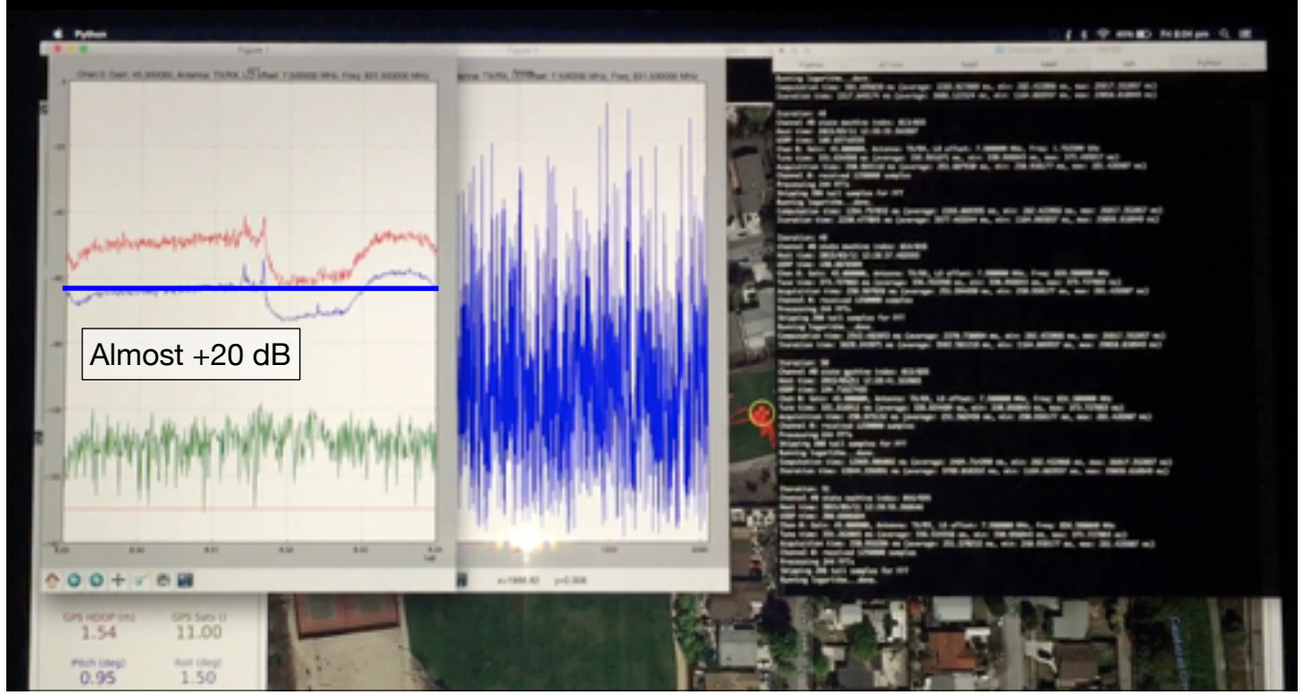
Spectrum Scanner



Ground-Level SNR



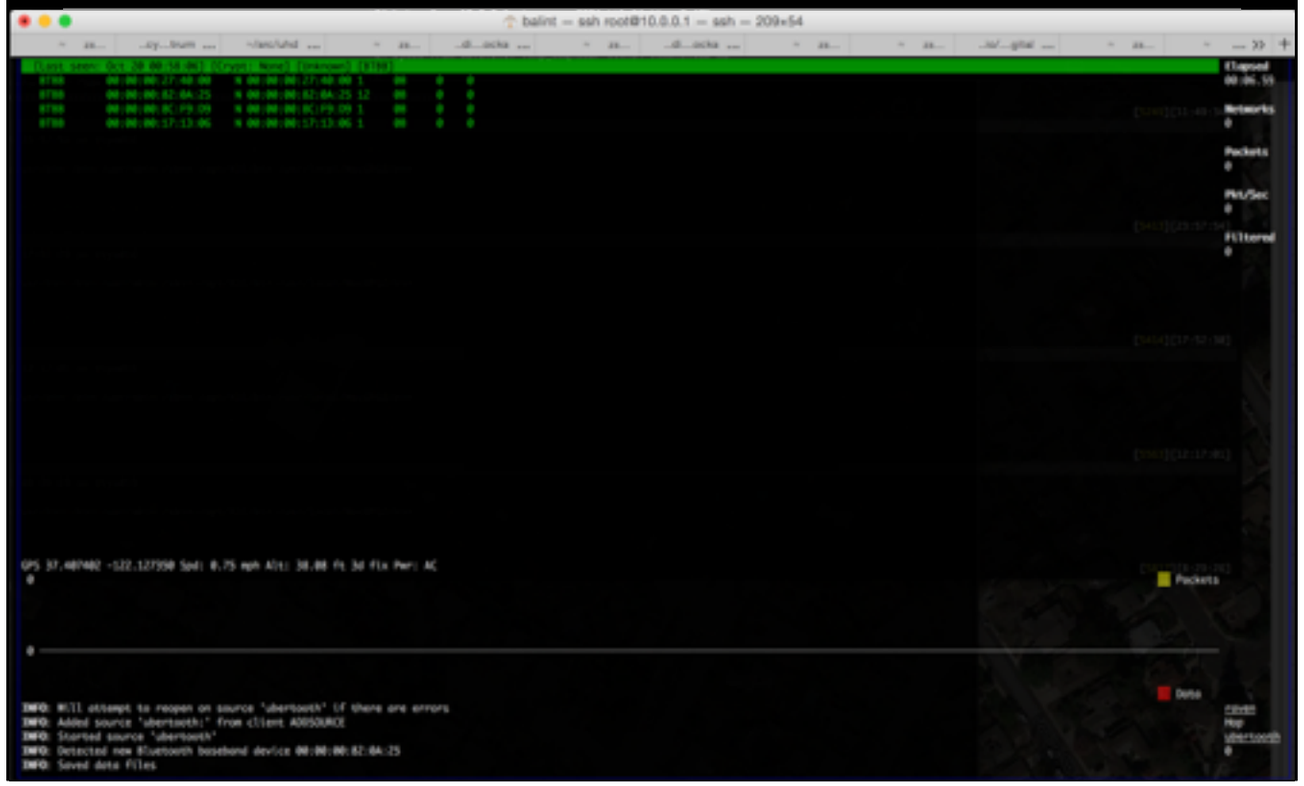
Airborne SNR



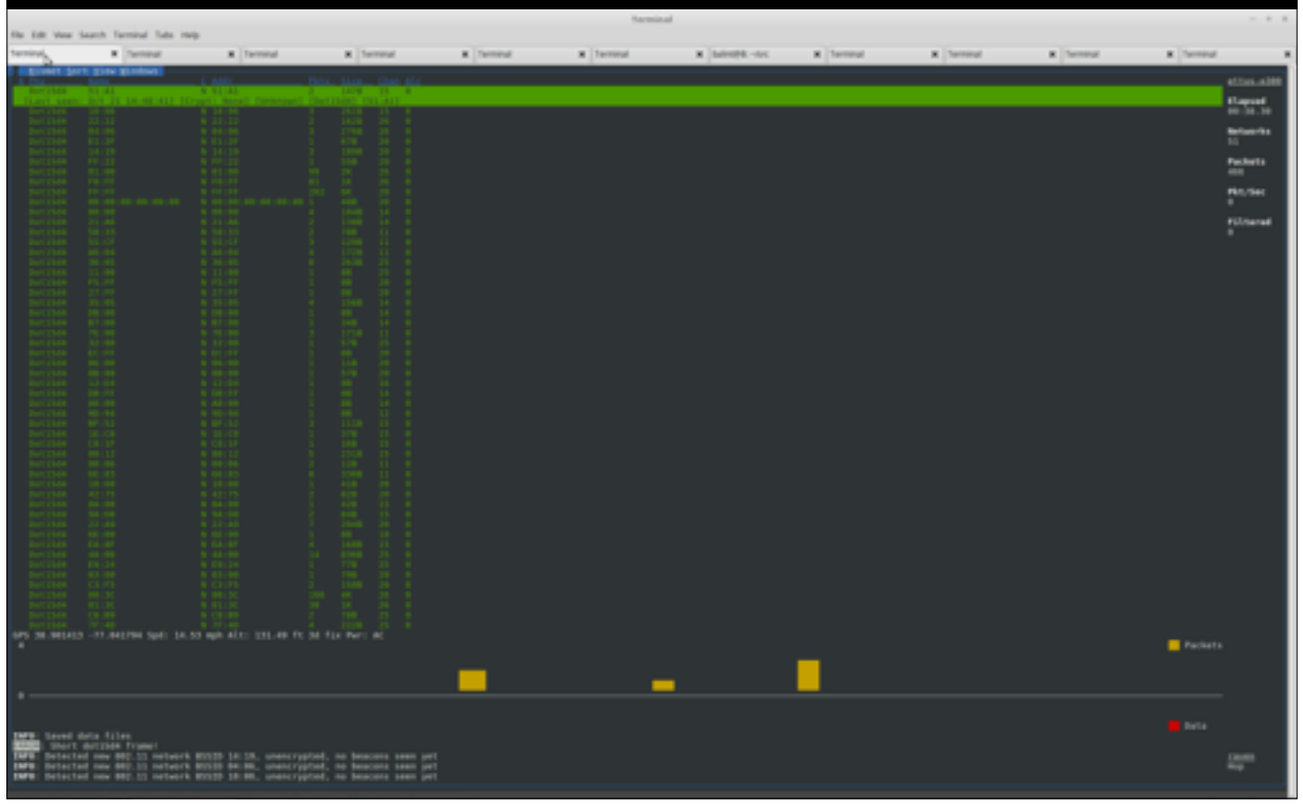

GSG Ubertooth dongle

Atmel RZRAVEN ZigBee dongle

Kismet with Ubertooth Plugin on E310

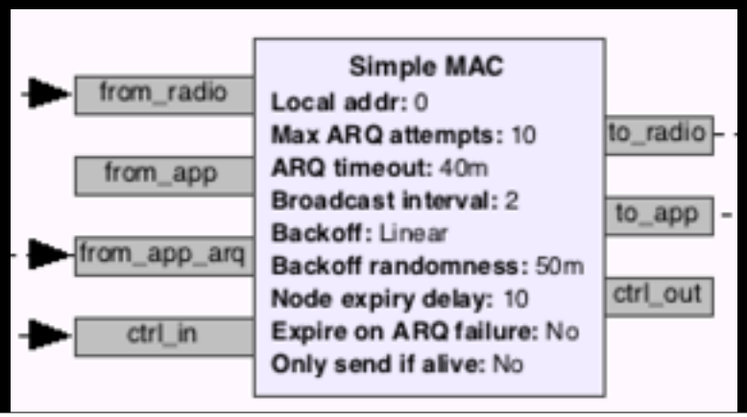


Kismet with ZigBee Plugin on E310



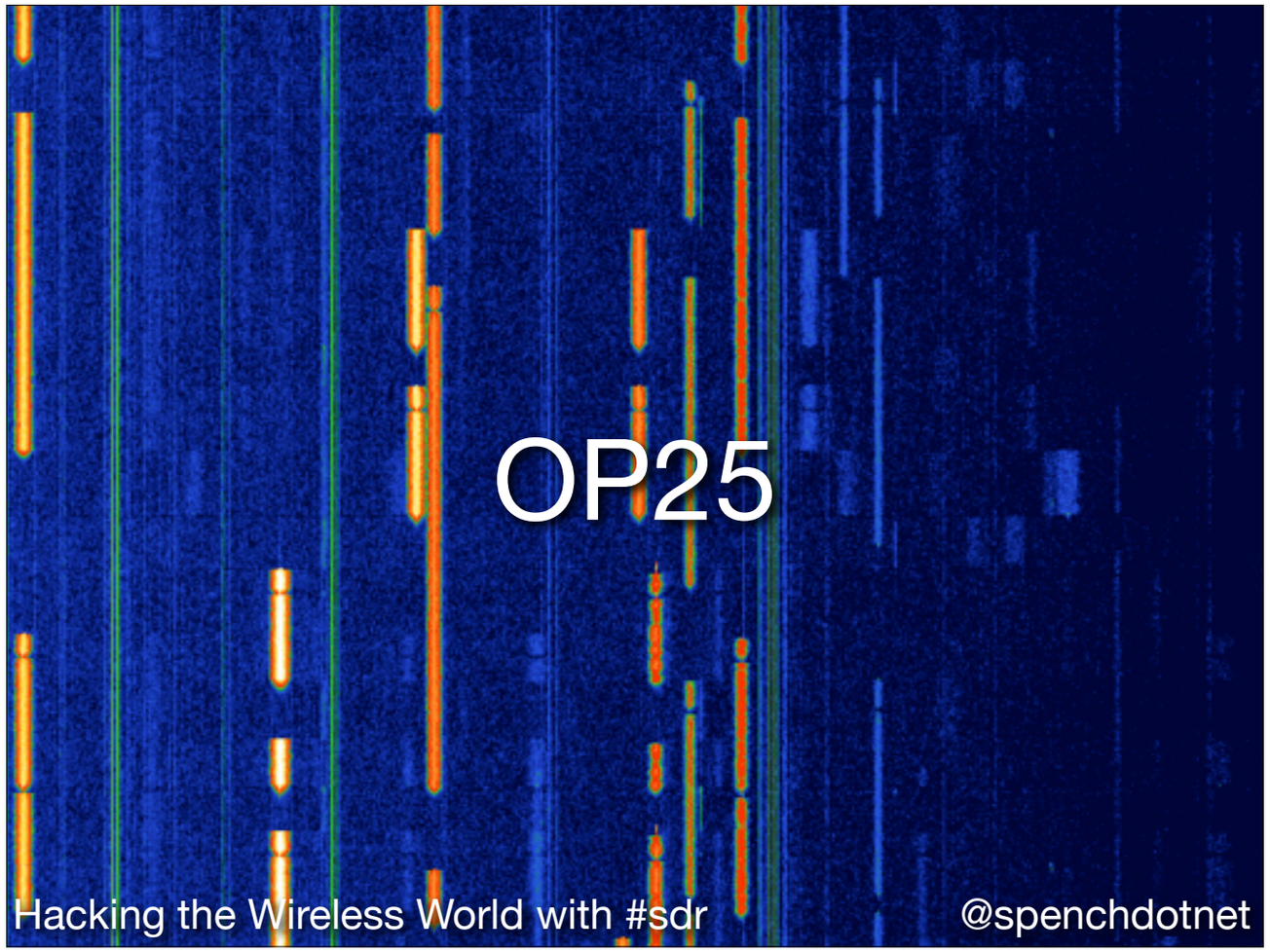
Backhaul

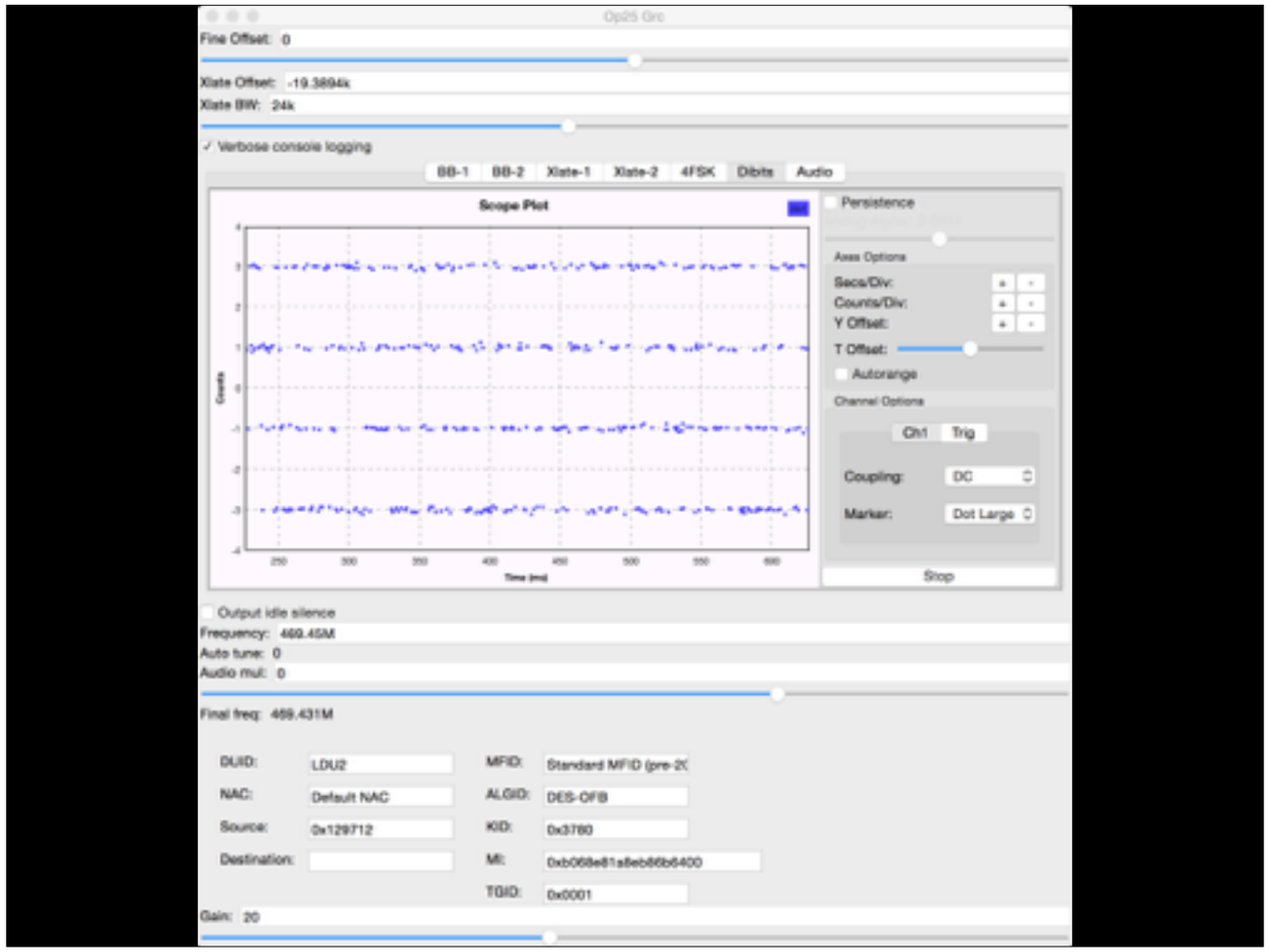
- None: Run unattended
- Wi-Fi: More 2.4 GHz ISM activity close to receiver & limited range
- Custom through SDR: greater range

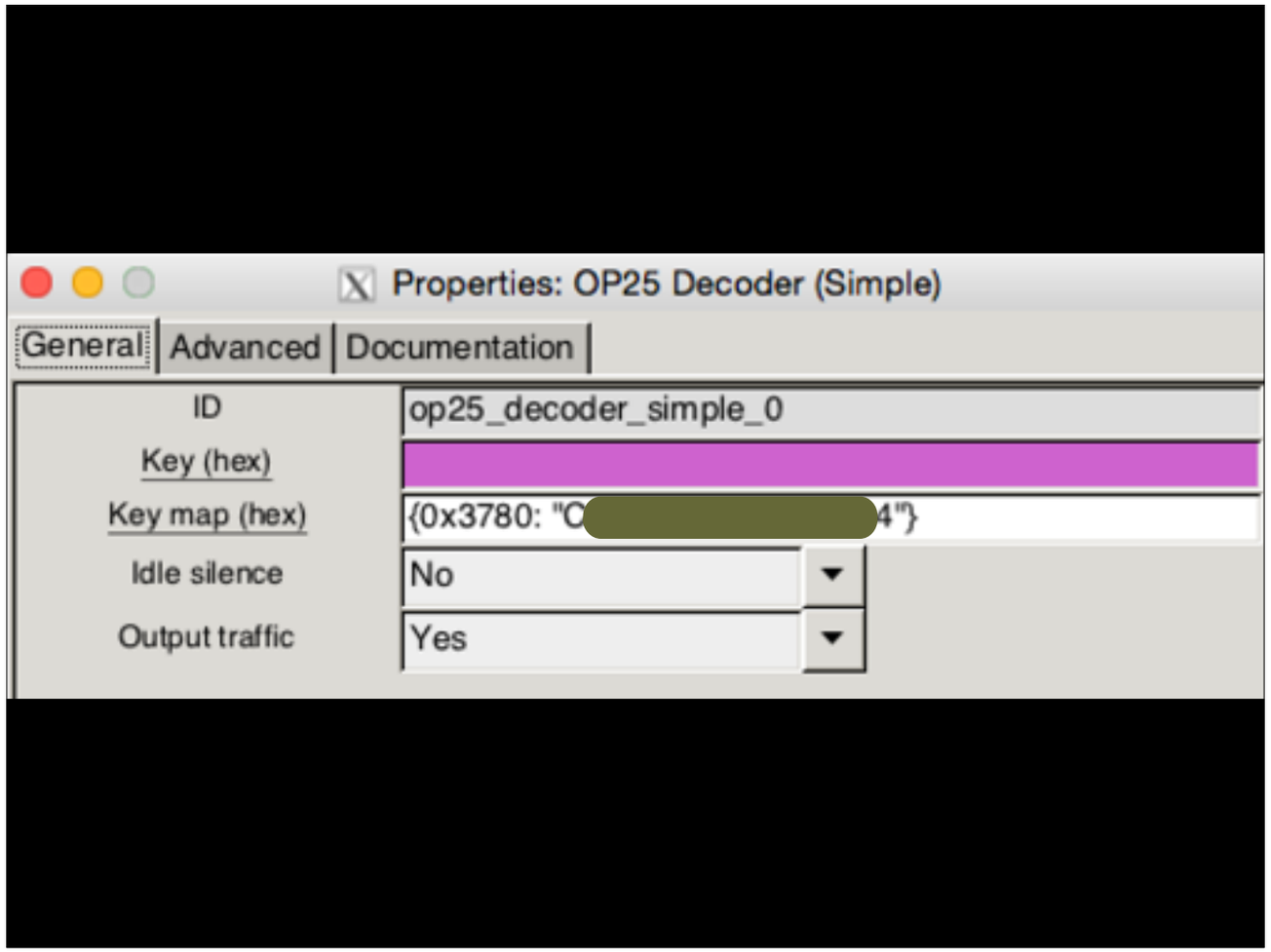


Airborne Platform

- Spectrum Monitoring & Recording
- Wi-Fi
- Bluetooth
- ZigBee
- Live Video
- Custom Backhaul


OP25
Hacking the Wireless World with #sdr
@spenchdotnet

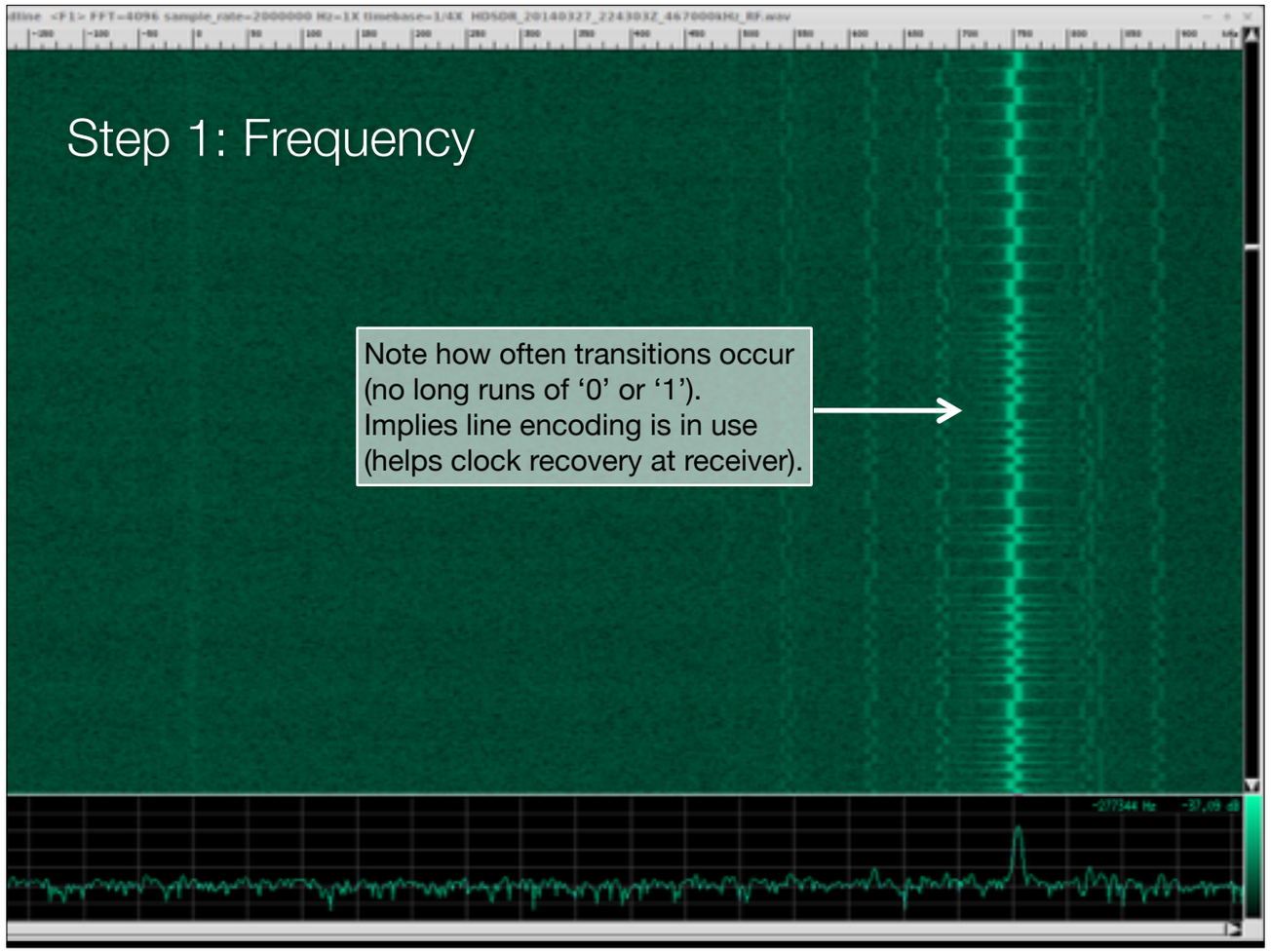

Op25 Gnc
Fine Offset: 0
Xlate Offset: -19.3894k
Xlate BW: 24k
✓ Verbose console logging
BB-1
BB-2
Xlate-1
Xlate-2
4FSK
Dibits
Audio
Scope Plot
Persistence
Axes Options
Secs/Div:
Counts/Div:
Y Offset:
T Offset:
Autorange
Channel Options
Ch1
Trig
Coupling:
DC
Marker:
Dot Large
Stop
Output idle silence
Frequency: 469.45M
Auto tune: 0
Audio mul: 0
Final freq: 469.431M
DUID:
LDU2
NAC:
Default NAC
Source:
0x129712
Destination:
MFID:
Standard MFID (pre-2(
ALGID:
DES-OFB
KID:
0x3780
MI:
0xb068e81a8eb86b6400
TGID:
0x0001
Gain: 20


Properties: OP25 Decoder (Simple)
General
Advanced
Documentation
ID
op25_decoder_simple_0
Key (hex)
Key map (hex)
{0x3780: "C
4"}
Idle silence
No
Output traffic
Yes

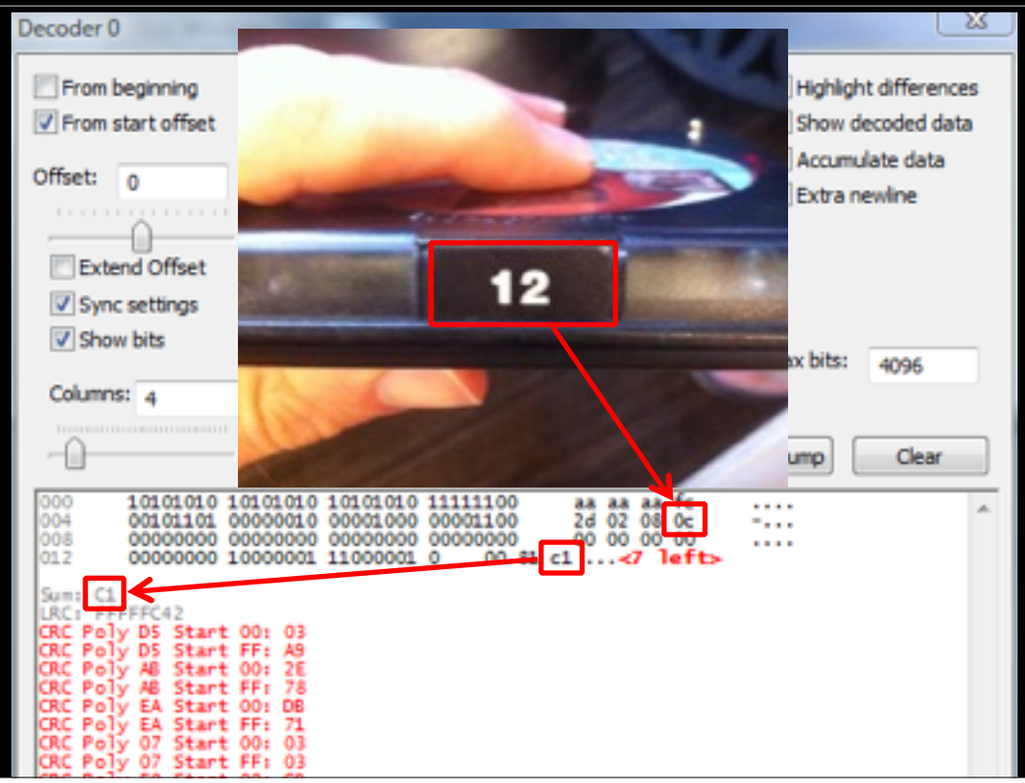
```
LDU2: LSDW: 0xf301, valid
LDU2: 0 hamming errors, valid
LDU2: 0874 0535 013F 082E 07FF 02E2 061E 0010
LDU2: 08F4 03DC 0605 08A3 07FF 06ED 0361 0064
LDU2: 0935 0248 05EE 06A9 07FF 0578 014F 00DE
LDU2: 0935 014D 0DE1 024F 07FF 0557 05B9 00DA
LDU2: 0975 0908 09EA 0FD6 07FF 04C5 00F2 004C
LDU2: 096D 090C 0A39 04ED 07FF 07BC 024F 0020
LDU2: 0966 0CD2 06D3 0018 0400 037F 0128 00D5
LDU2: 0924 0FC1 09DB 0550 07FF 057A 04FF 00AA
LDU2: 09DD 0179 0D81 0C1C 06DE 0197 04CE 0046
LDU2:   AlgID: 0x81, KID: 0x3780, MI: ceed5275a045652600
DES:    1704 bits used from 28 iterations

LDU1: LSDW: 0xf83e, valid
LDU1: 0 hamming errors, valid
LDU1: LCF: 0x00, MFID: 0x00
LDU1: Emergency: 0x00, Reserved: 0x4000, TGID: 0x0001, Source: 0x129712
LDU1: 0855 0F42 05F5 0534 0400 0130 0466 00E2
LDU1: 00A2 05B3 0BFB 06B9 0033 016C 062C 00F0
LDU1: 082F 05F2 0161 0011 0400 0309 04FA 0060
LDU1: 08ED 019A 0732 065C 07FF 04AE 04C2 00BF
LDU1: 08EC 0358 0777 02A4 07FF 0649 05F8 009D
LDU1: 08AC 016C 01FE 0ED0 07FF 073A 05C6 00BA
LDU1: 0874 05F0 01DD 0168 07FF 0426 057C 0031
LDU1: 0874 04F6 07DD 0736 07FF 0403 01E6 00F8
LDU1: 082C 05B4 009F 0AC2 07FF 0785 06A0 00CD
```

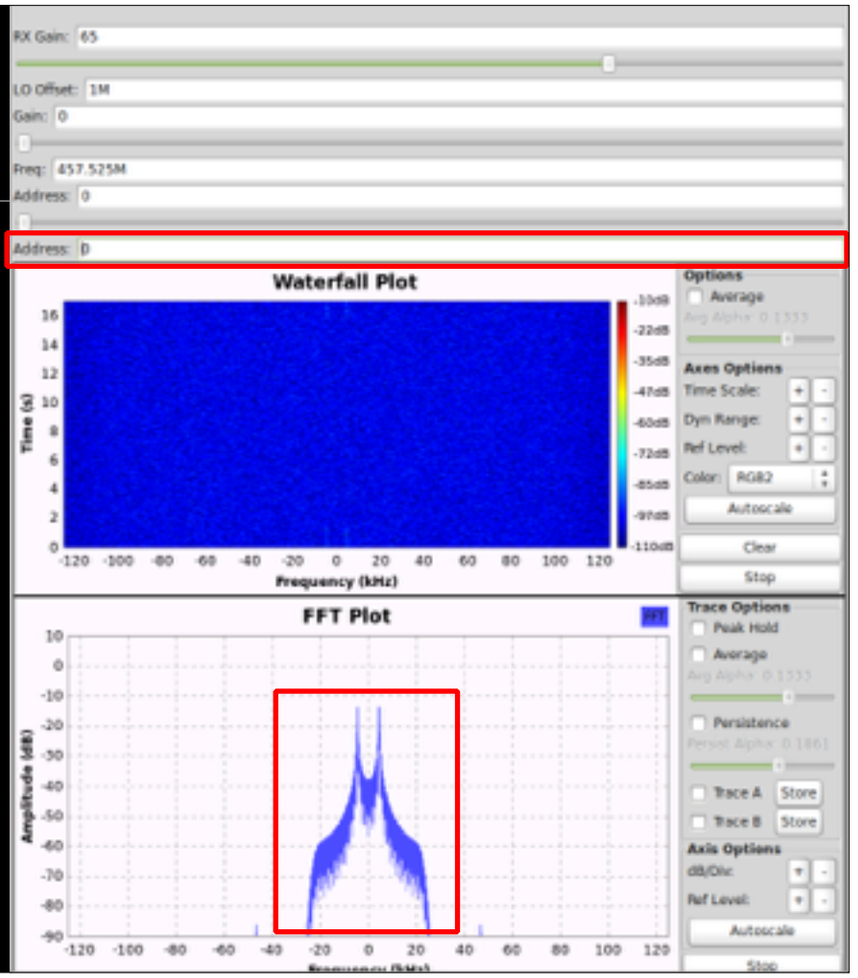

Restaurant Pagers
Hacking the Wireless World with #sdr
@spenchdotnet


Step 1: Frequency
Note how often transitions occur (no long runs of ‘0’ or ‘1’). Implies line encoding is in use (helps clock recovery at receiver).

Step 8: Finding the ID



Modulator


RX Gain: 65
LO Offset: 1M
Gain: 0
Freq: 457.525M
Address: 0
Address: 0
Waterfall Plot
Time (s)
Frequency (kHz)
Options
Average
Axes Options
Time Scale:
Dyn Range:
Ref Level:
Color: RGB2
Autoscale
Clear
Stop
FFT Plot
FFT
Amplitude (dB)
Trace Options
Peak Hold
Average
Persistence
Trace A
Trace B
Store
Axis Options
dB/Div:
Ref Level:
Autoscale
Stop

Demo

POCSAG Pager

- Other restaurant pager systems adopt a standard
- Decode with gr-pocsag
  - Modified to end frame decoding when squelch closes

ZigBee Pager

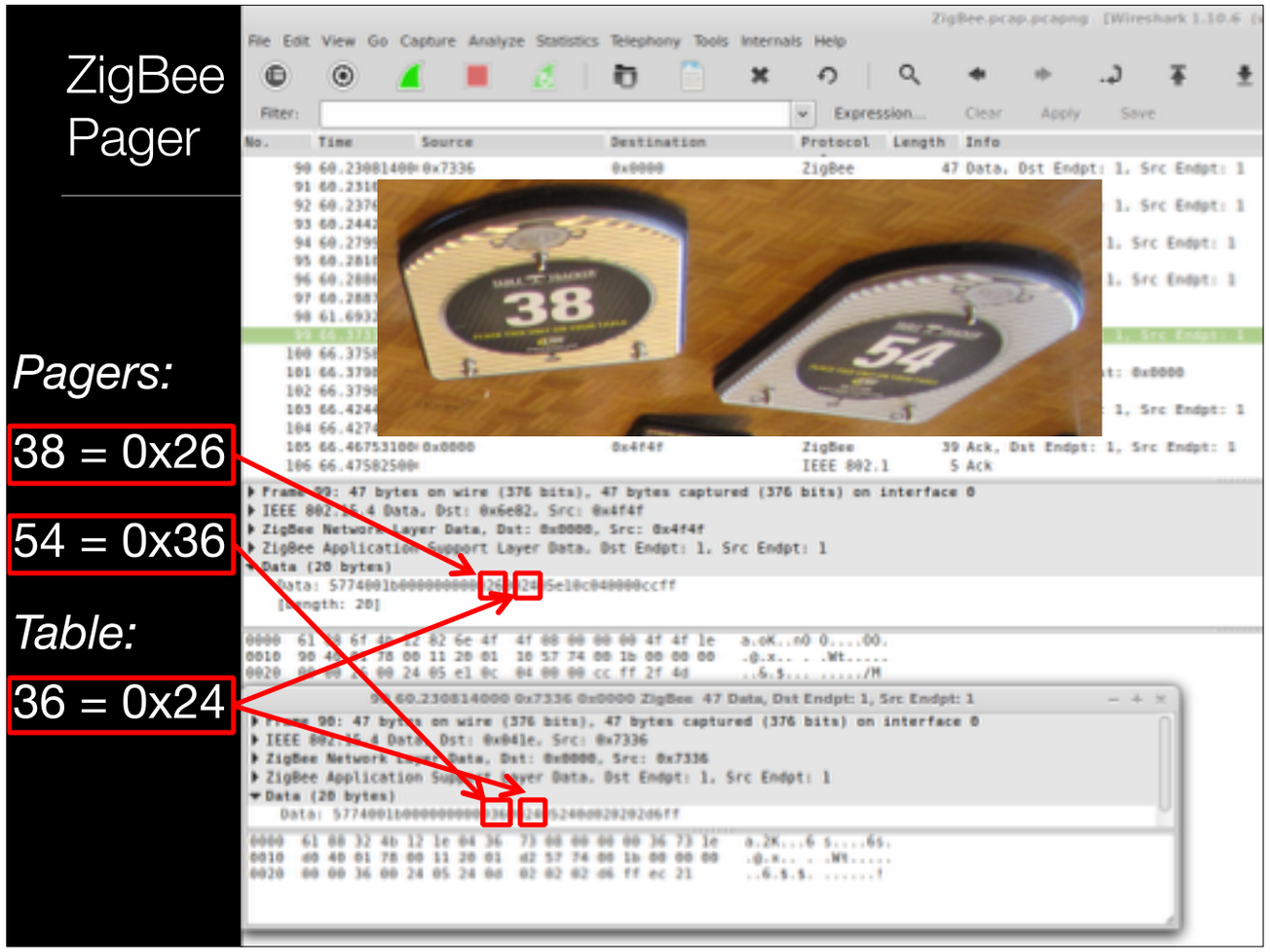
Pagers:

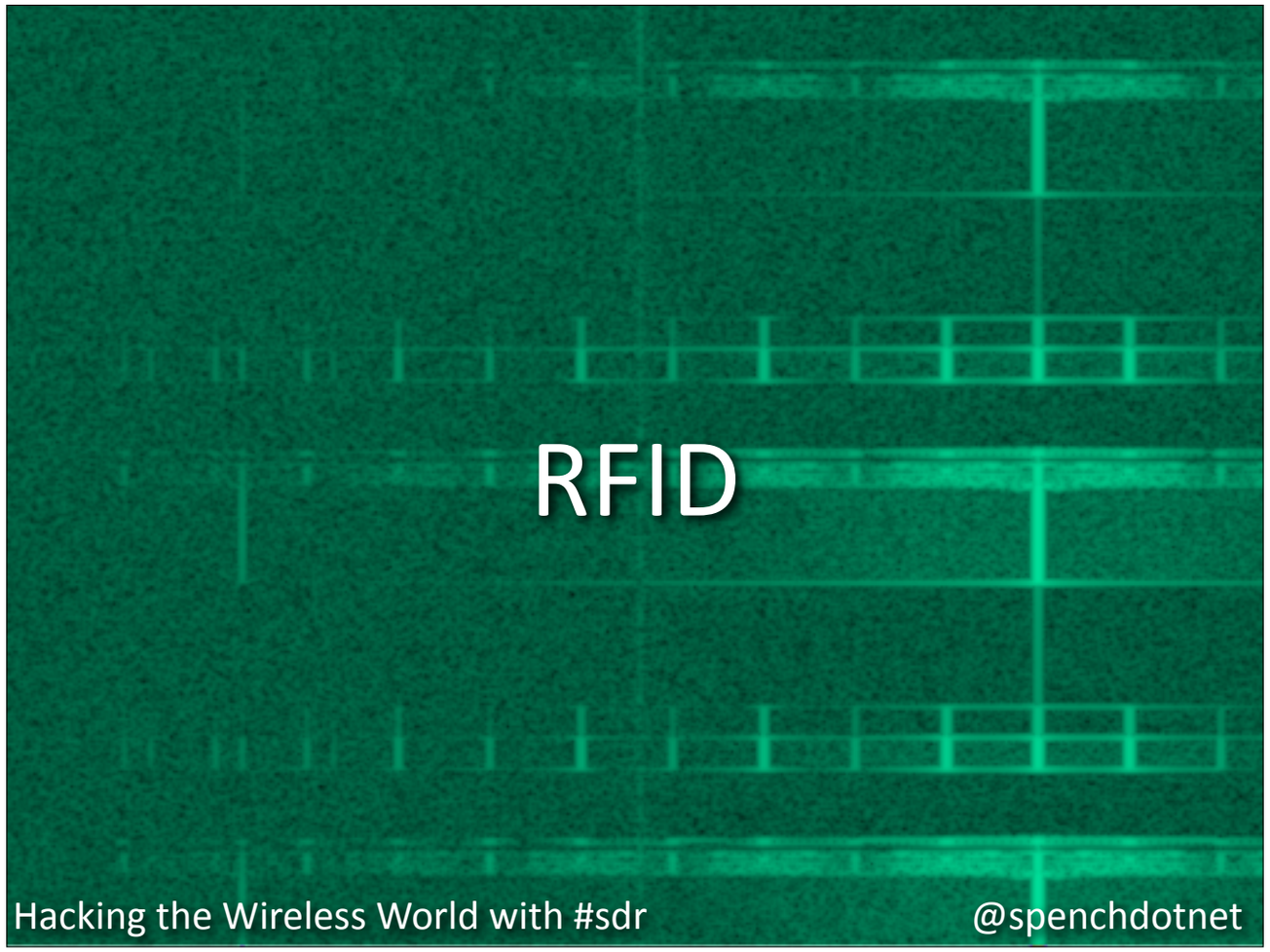
38 = 0x26

54 = 0x36

Table:

36 = 0x24



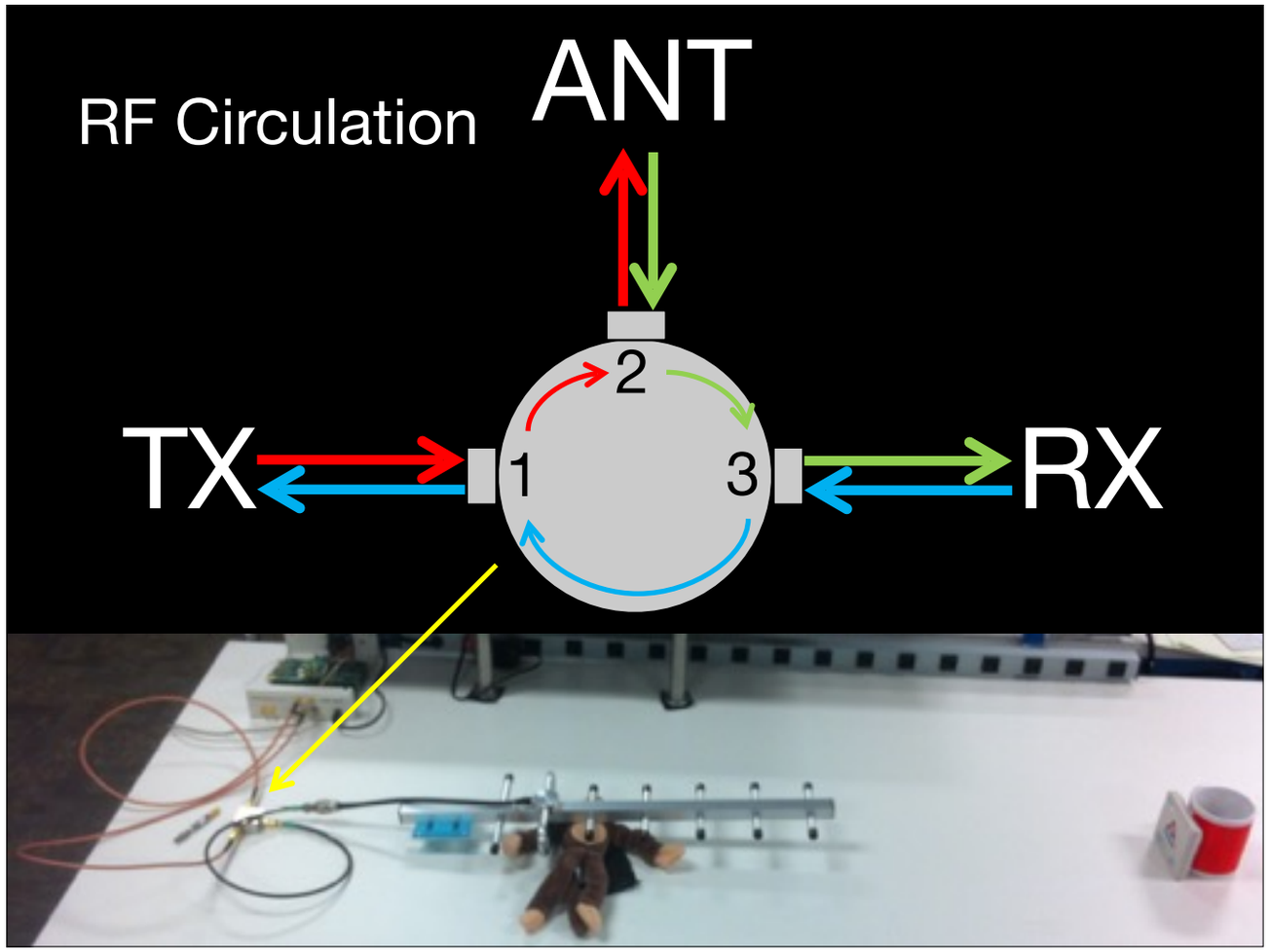


Waterfall of FasTrak interrogation

Yagi antennas pointed into each lane. This is not a toll point! This is traffic ‘monitoring’.

http://en.wikipedia.org/wiki/FasTrak

Drive-through toll implementation

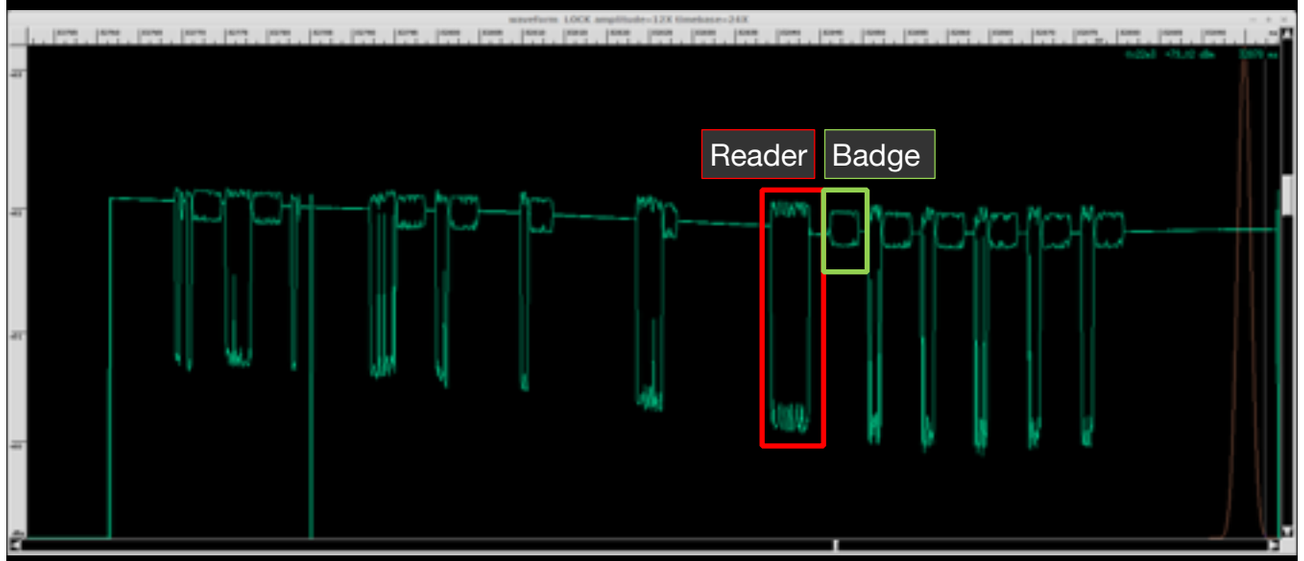


http://en.wikipedia.org/wiki/Circulator

Reading a Tag Outside

https://www.youtube.com/watch?v=tAkujpOP4XI&index=39&list=PLPmwwVknVIiVReNIEhQ-cBIE7gklFef8_

RFID Badges/Keys: Time-domain Amplitude

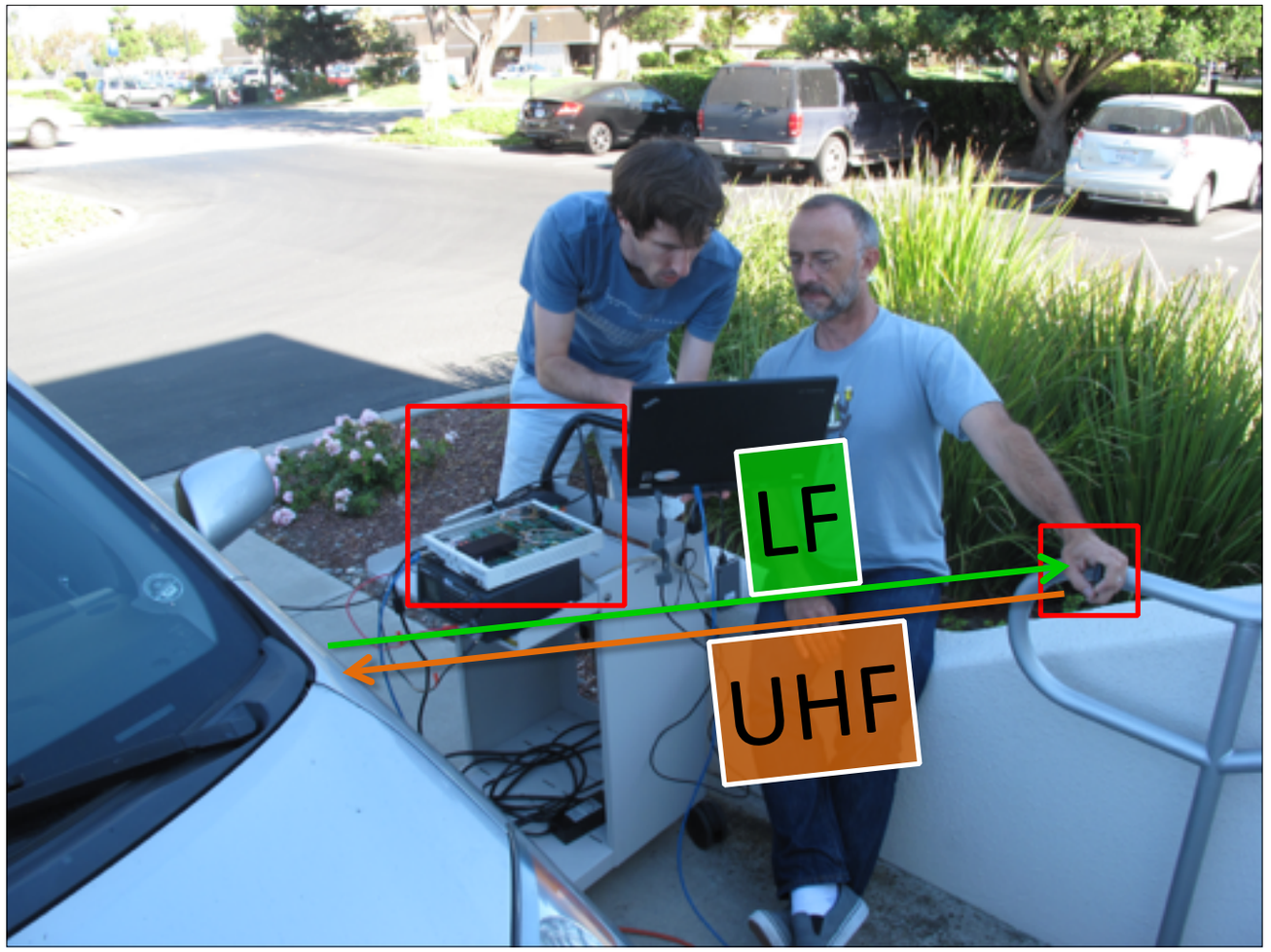


Vehicular Keyless Entry

Hacking the Wireless World with #sdr

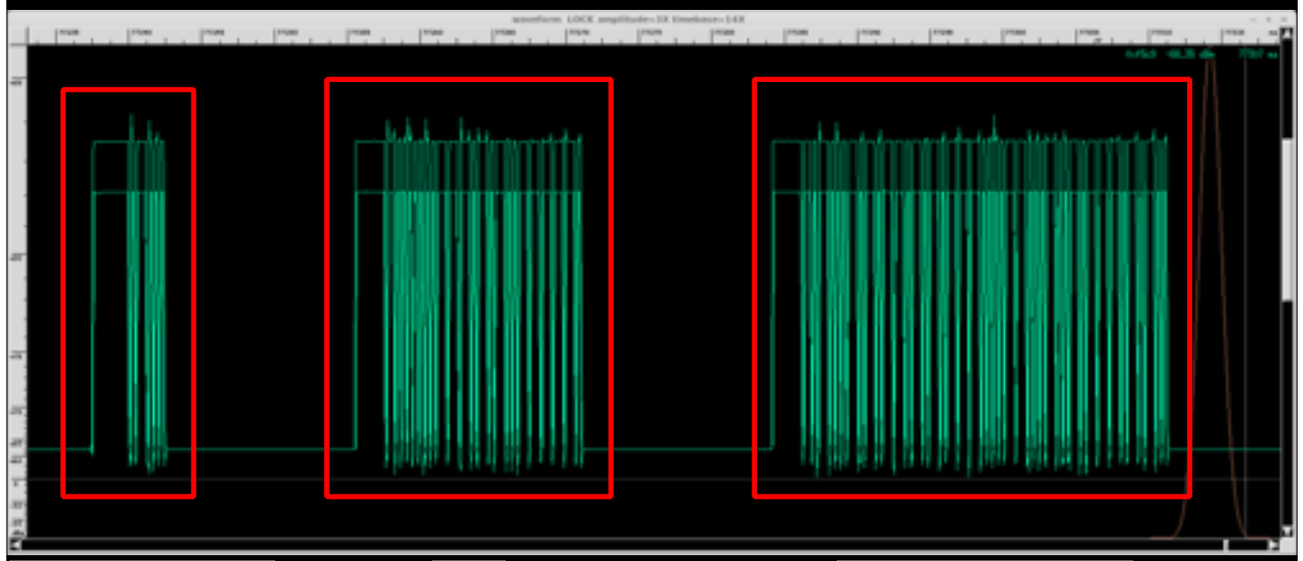
@spenchdotnet

Waterfall of FasTrak interrogation



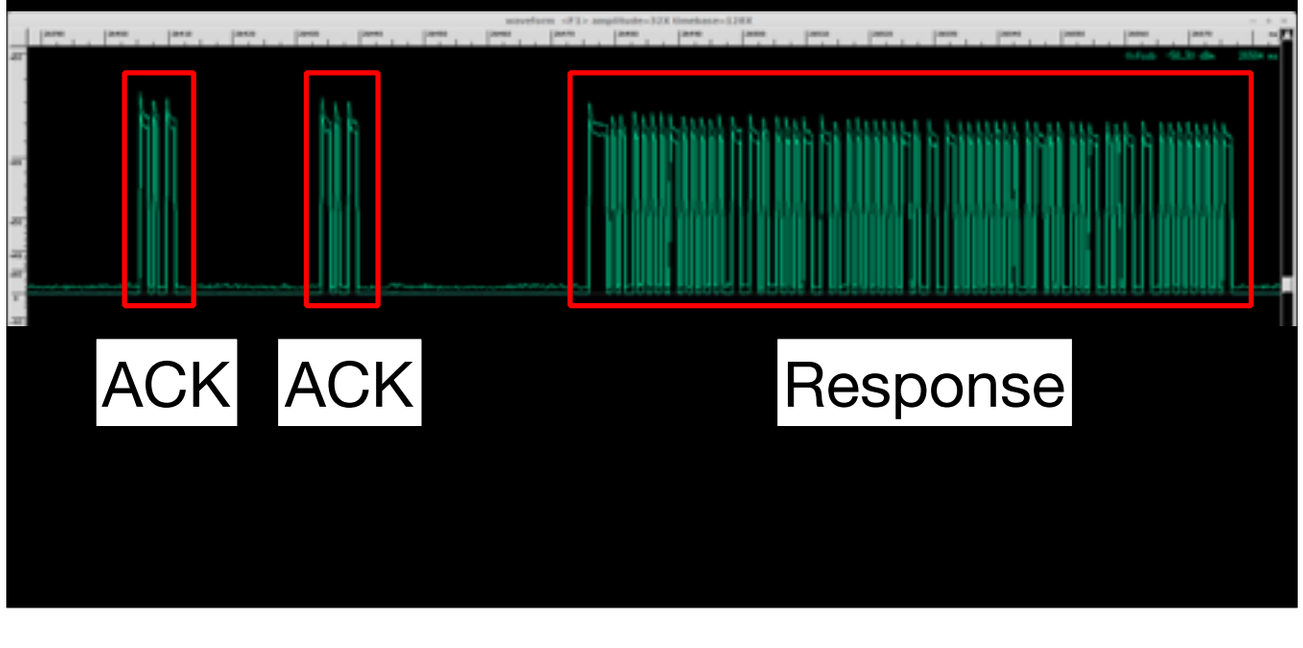
WBX is used to receive UHF transmission from remote control, which is triggered by LF challenge from car

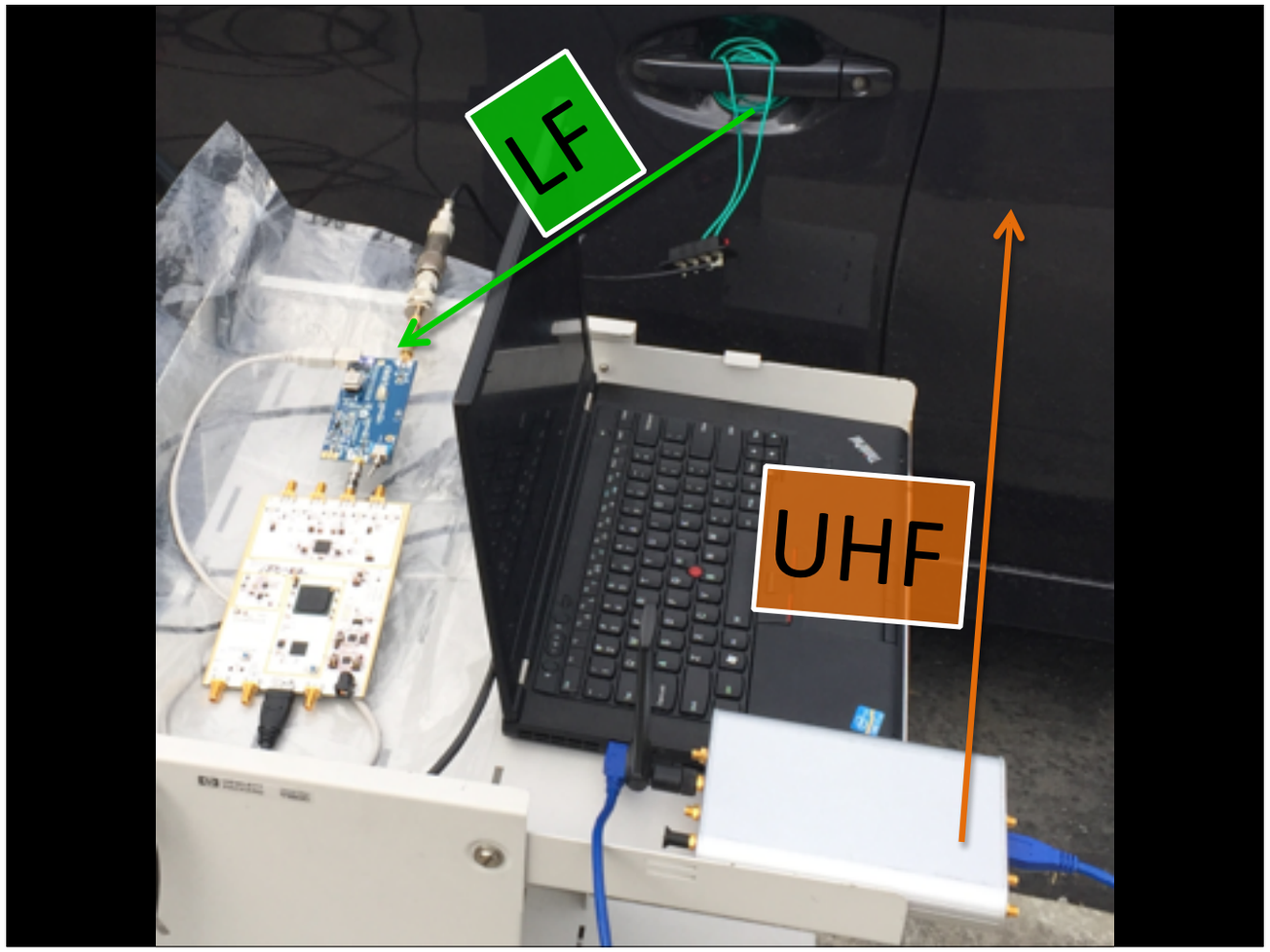
Time-domain Amplitude (LF)



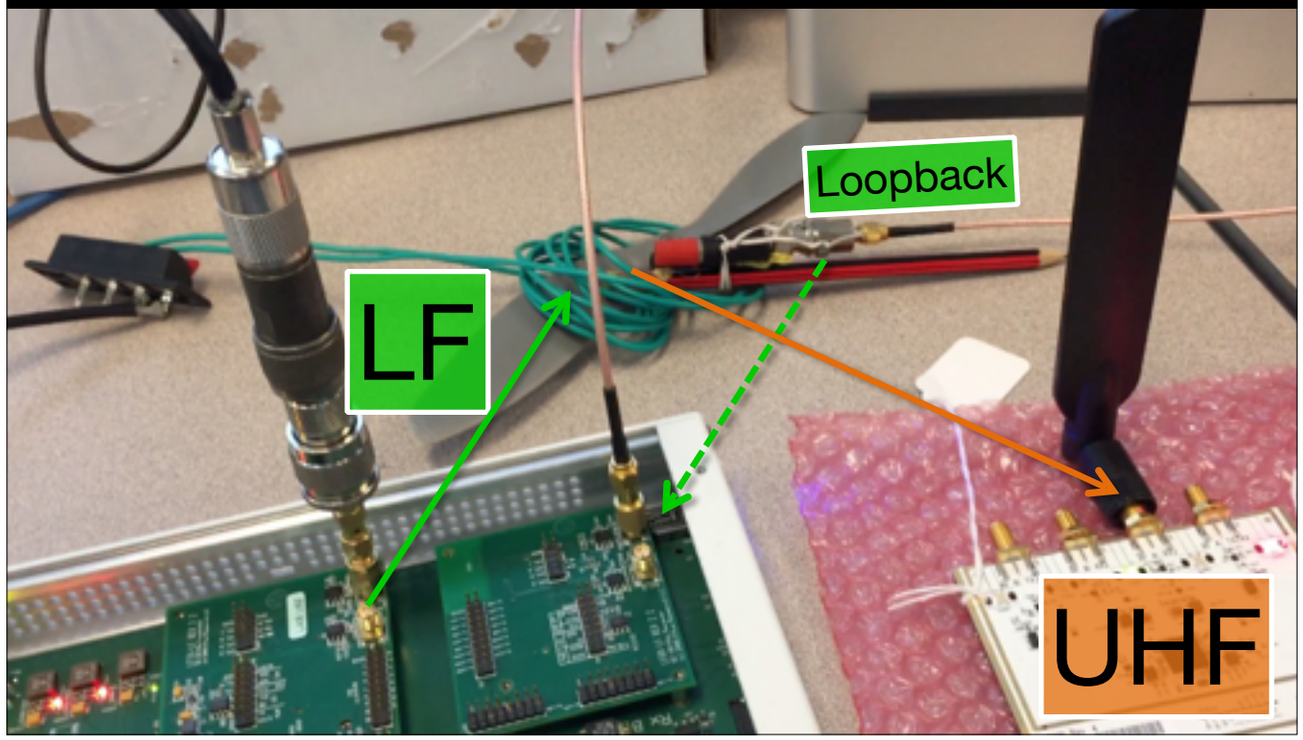
Challenge

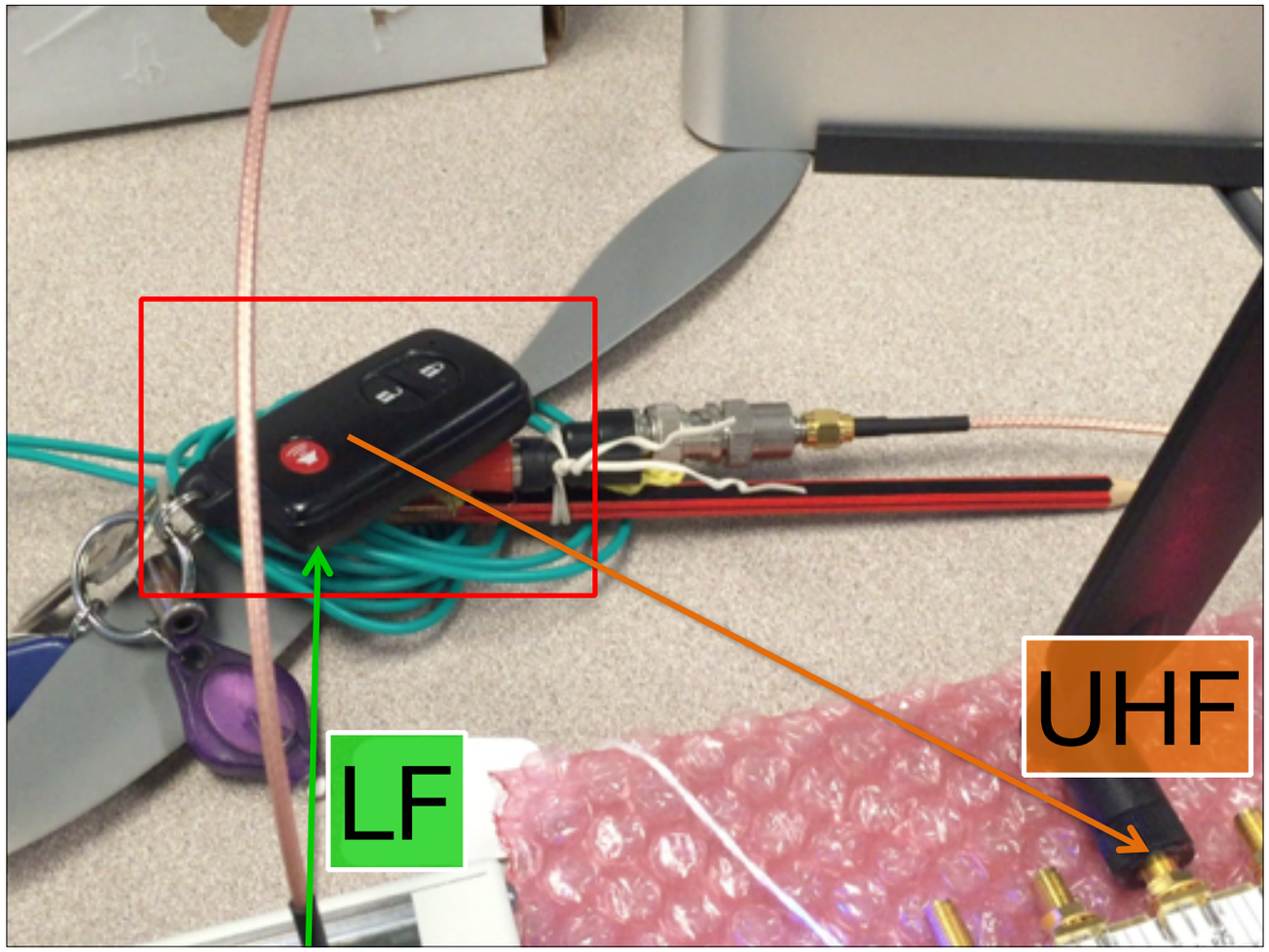
Time-domain Amplitude (UHF)

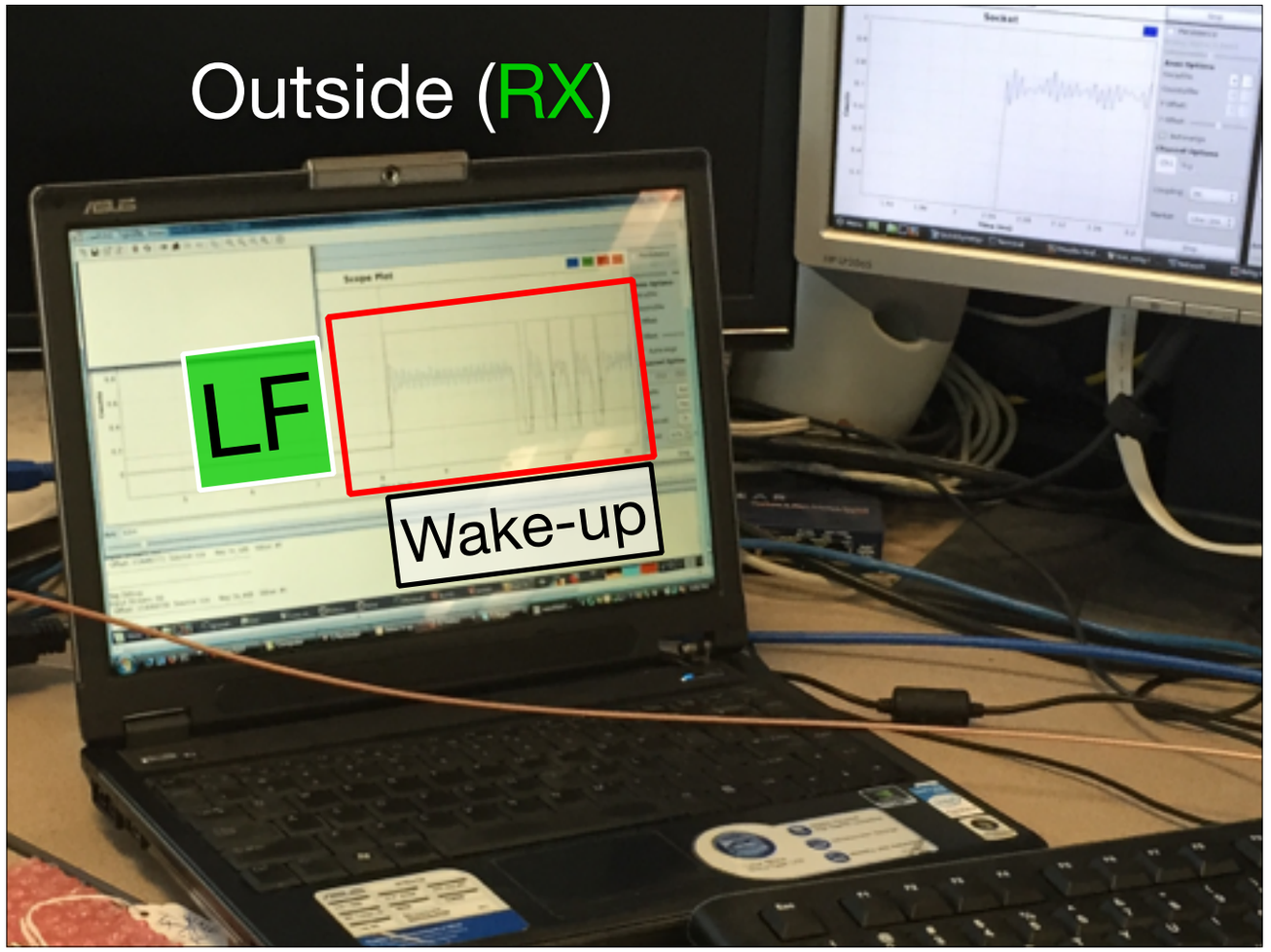



LF
UHF

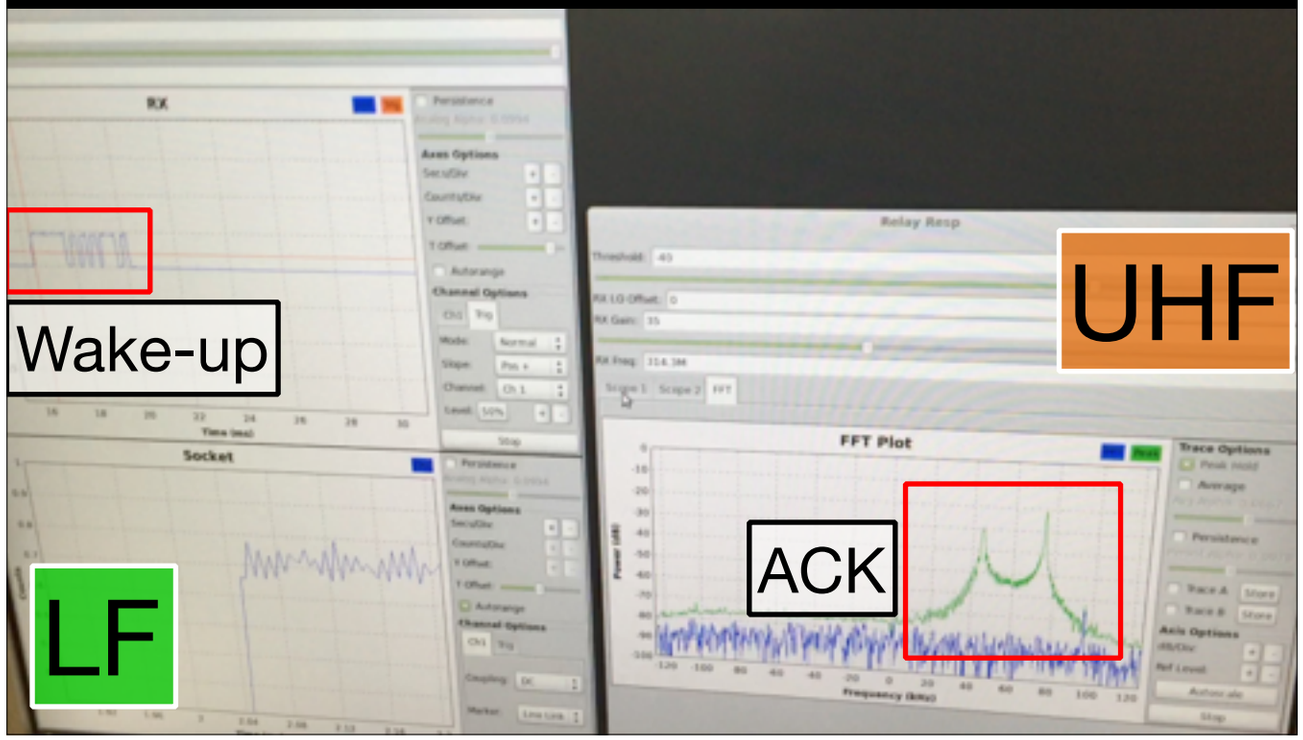
Remote Side



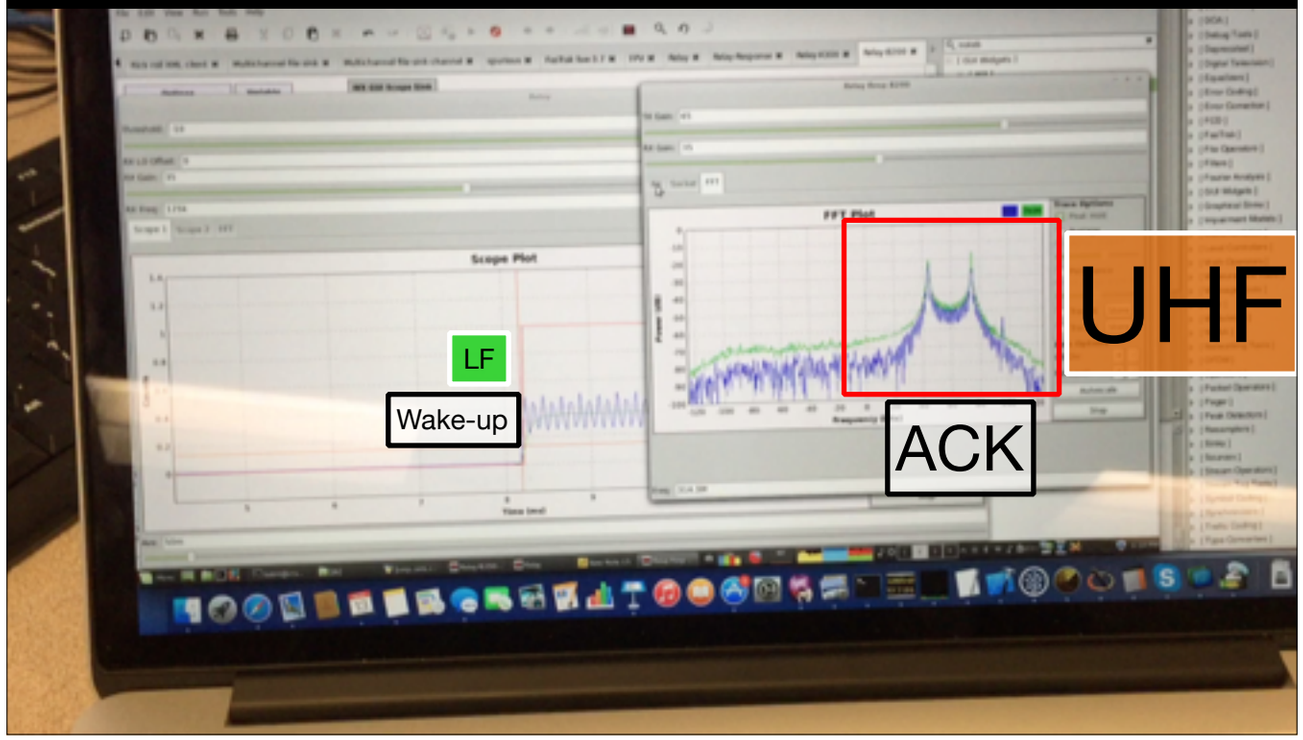

LF
UHF


Outside (RX)
LF
Wake-up

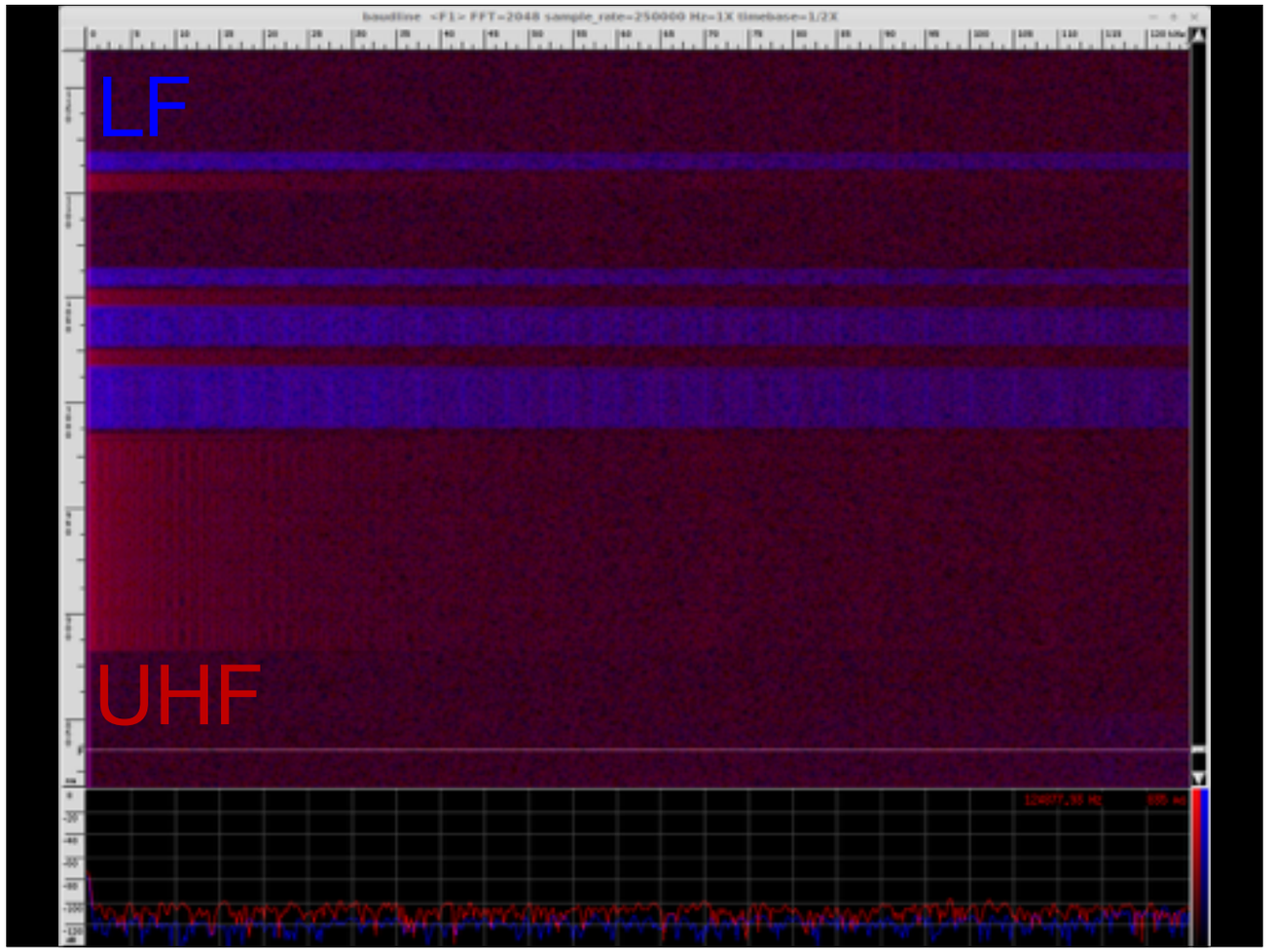
Inside (TX → RX)



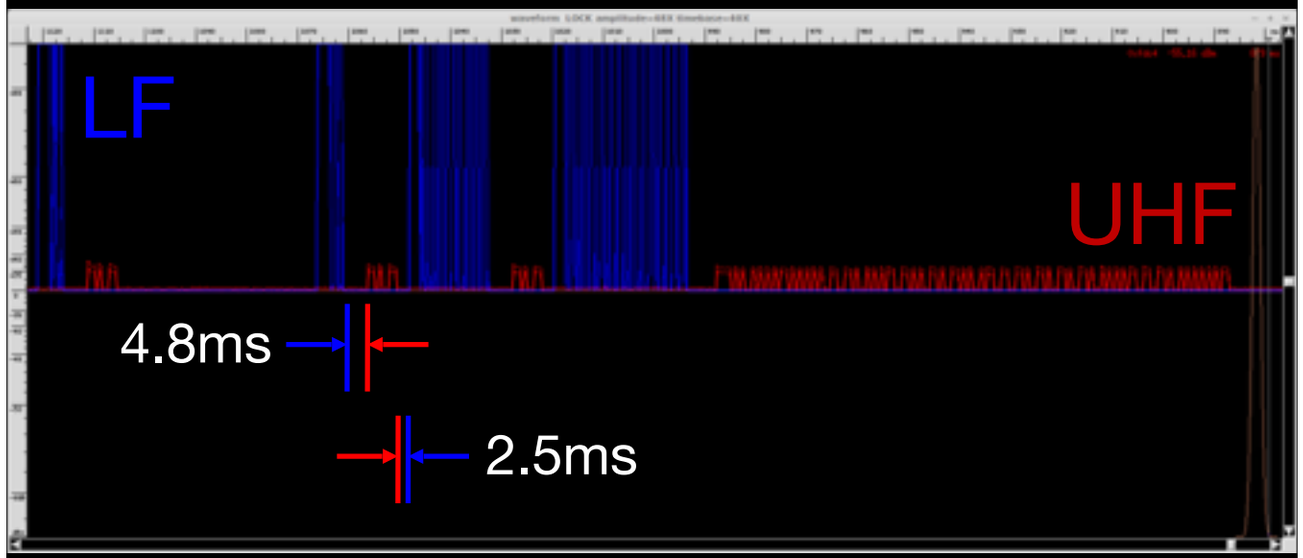
Outside (TX)



Test


LF
UHF

Latency!



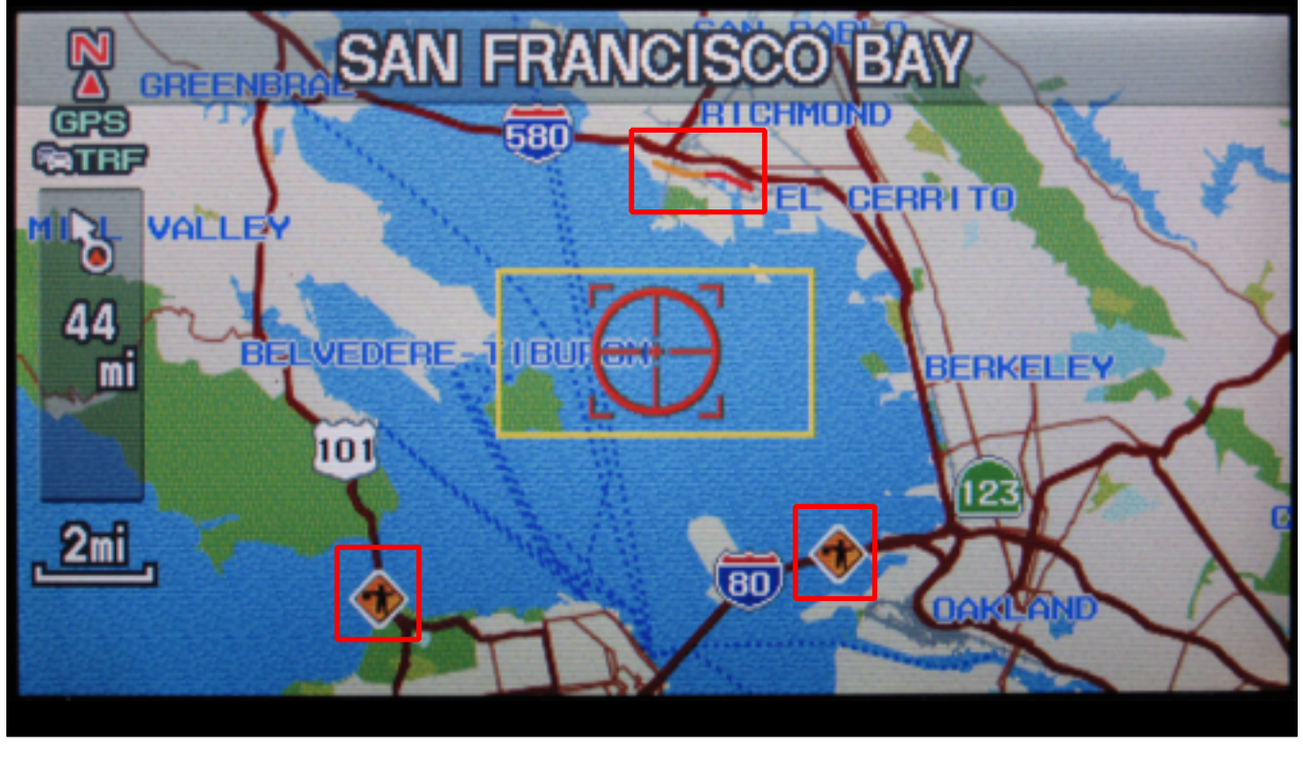
Other Applications

Stereo FM with RDS: Receiver

Radio **D**ata **S**ervice

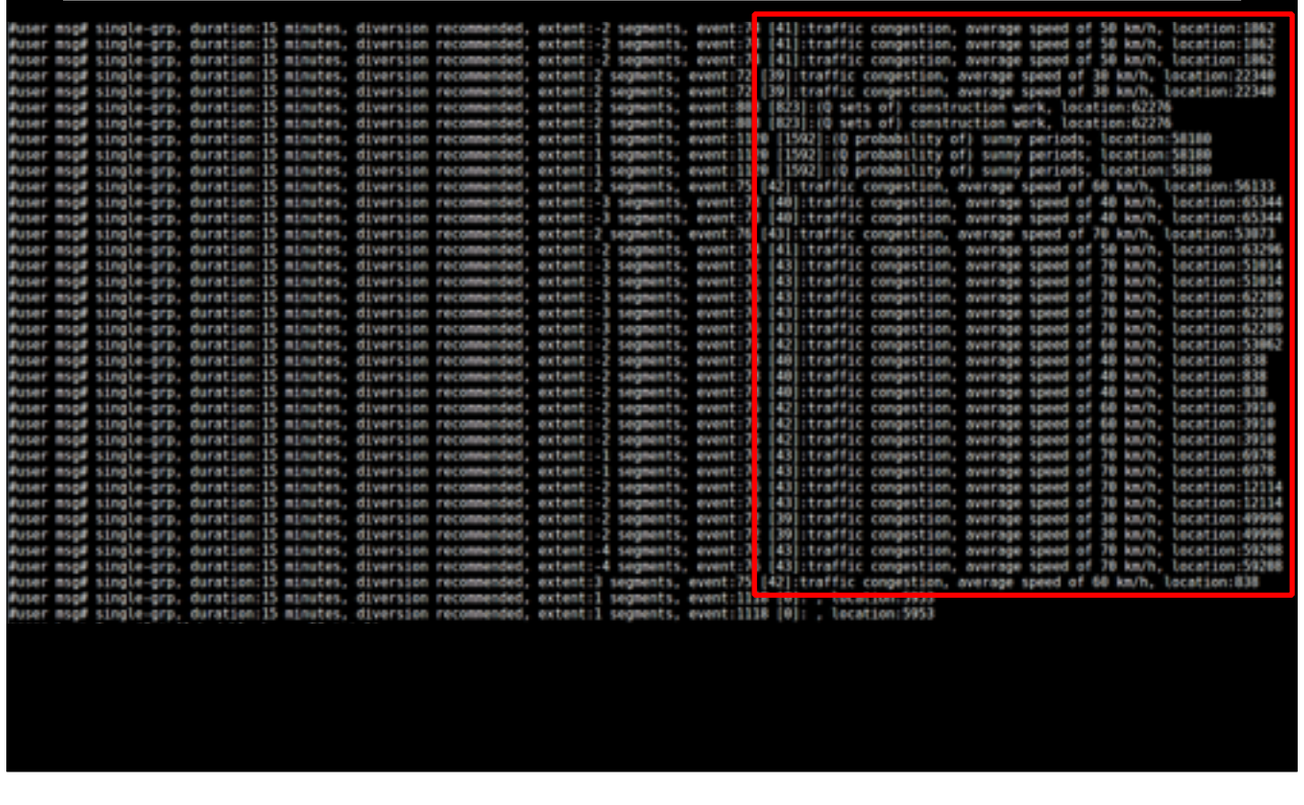
https://github.com/balint256/gr-rds

Traffic Message Channel



Happens to flow via Sirius terrestrial repeater. Blanked FM band and Sirius bands to find which.

Traffic Message Channel



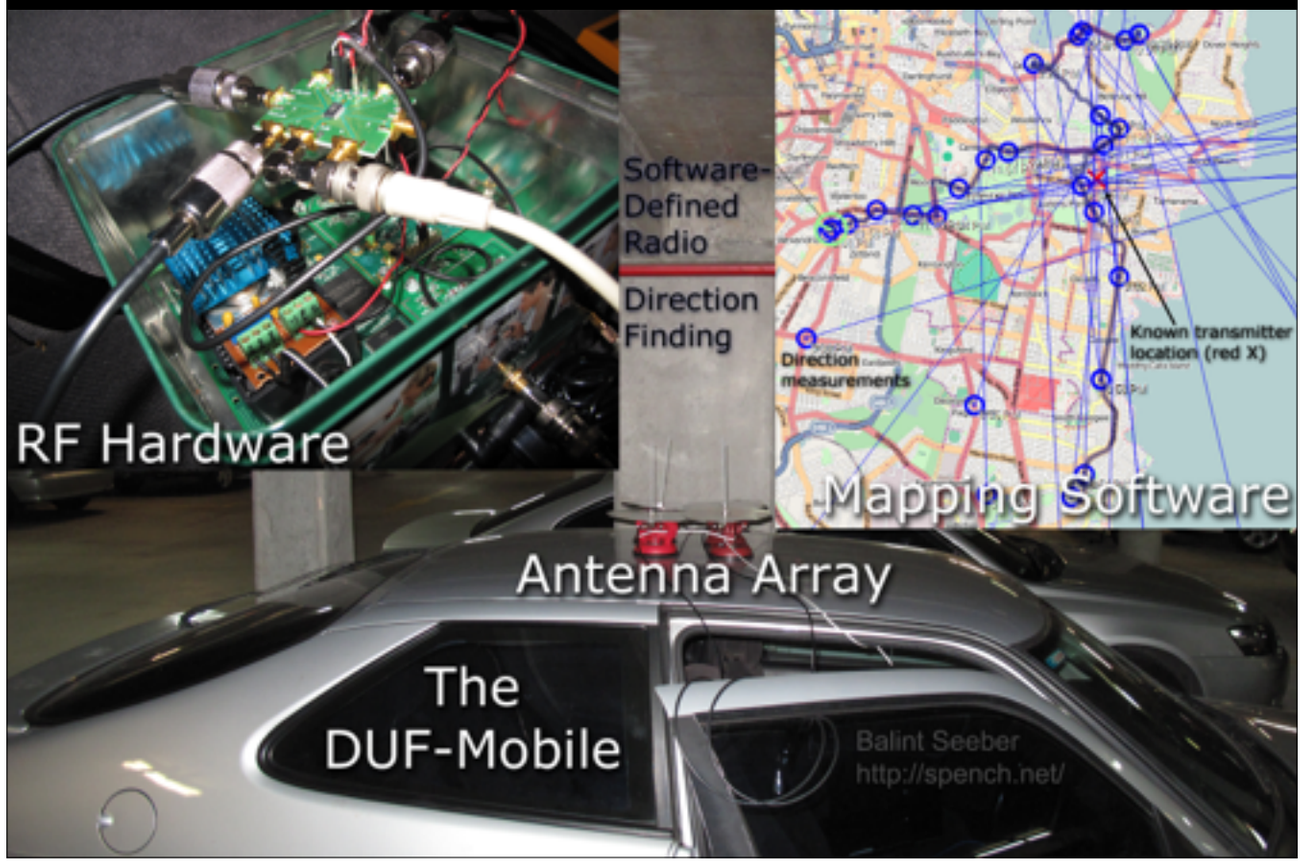
Results

```
Location #  1 has     1 possible plain codes
  4603  11fb
Location #  2 has     1 possible plain codes
  4401  1131
Location #  3 has     1 possible plain codes
  4172  104c
Location #  4 has     1 possible plain codes
  5134  140e
Location #  5 has     1 possible plain codes
  4193  1061
Location #  6 has     1 possible plain codes
  4527  11af
Location #  7 has     1 possible plain codes
  4329  10e9
Location #  8 has     1 possible plain codes
  5611  15eb
Location #  9 has     1 possible plain codes
  4538  11ba
Location # 10 has     1 possible plain codes
  4303  10cf
Location # 11 has     1 possible plain codes
  4223  107f
Location # 12 has     1 possible plain codes
  4834  12e2
```

```
Encryption ID   2 has      2 possible keys
Encryption ID   3 has     15 possible keys
Encryption ID   4 has      5 possible keys
Encryption ID   5 has      4 possible keys
Encryption ID   6 has      3 possible keys
Encryption ID   7 has      5 possible keys
Encryption ID   8 has      7 possible keys
Encryption ID   9 has      2 possible keys
Encryption ID  10 has     34 possible keys
Encryption ID  11 has      1 possible keys
[illegible]
Encryption ID  13 has      4 possible keys
Encryption ID  15 has      2 possible keys
Encryption ID  17 has      2 possible keys
Encryption ID  18 has      3 possible keys
Encryption ID  20 has      3 possible keys
Encryption ID  21 has      4 possible keys
Encryption ID  22 has      6 possible keys
Encryption ID  24 has      1 possible keys
[illegible]
Encryption ID  25 has      3 possible keys
Encryption ID  26 has      5 possible keys
Encryption ID  27 has      3 possible keys
Encryption ID  28 has      1 possible keys
[illegible]
Encryption ID  30 has      2 possible keys
Encryption ID  31 has      4 possible keys
```

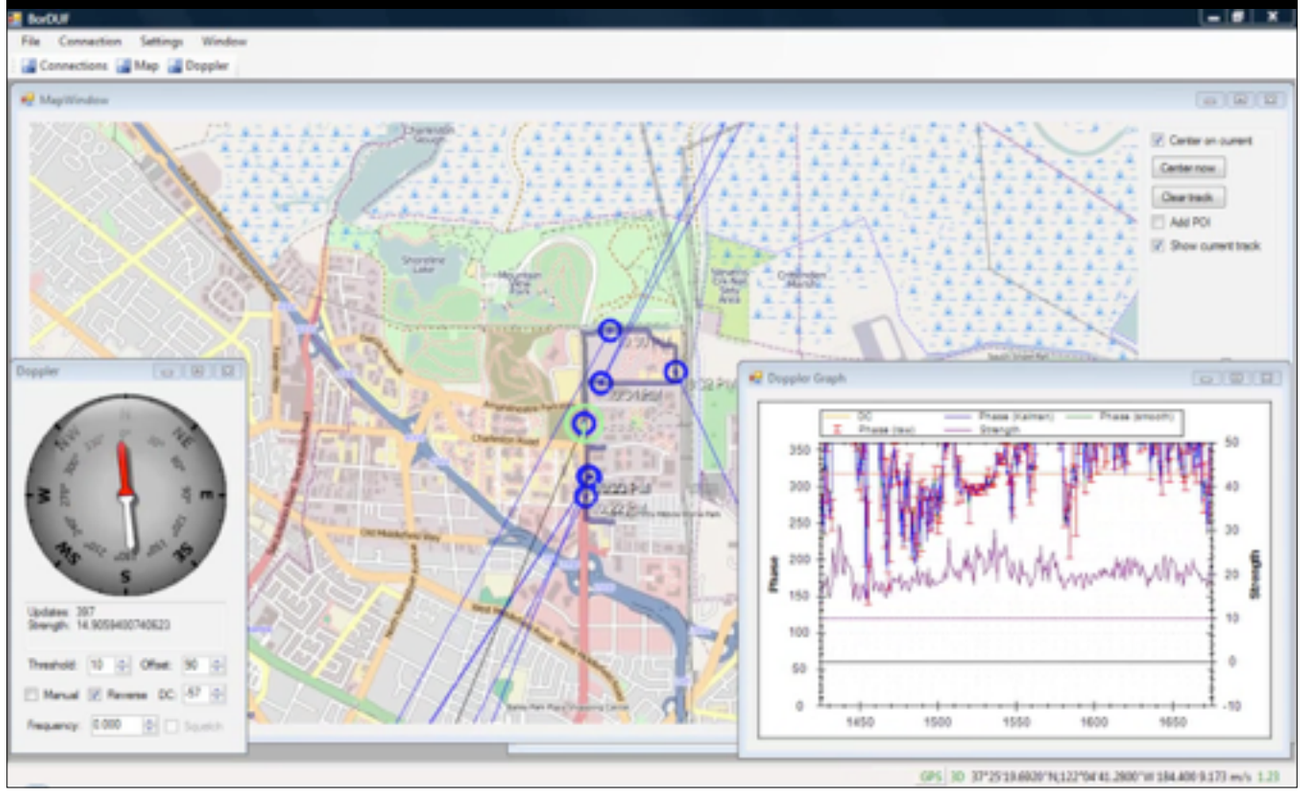

101.9MHz
ST
RDS
SDR-FM!!
11 33

SDR Direction Finding



http://wiki.spench.net/wiki/SDRDF

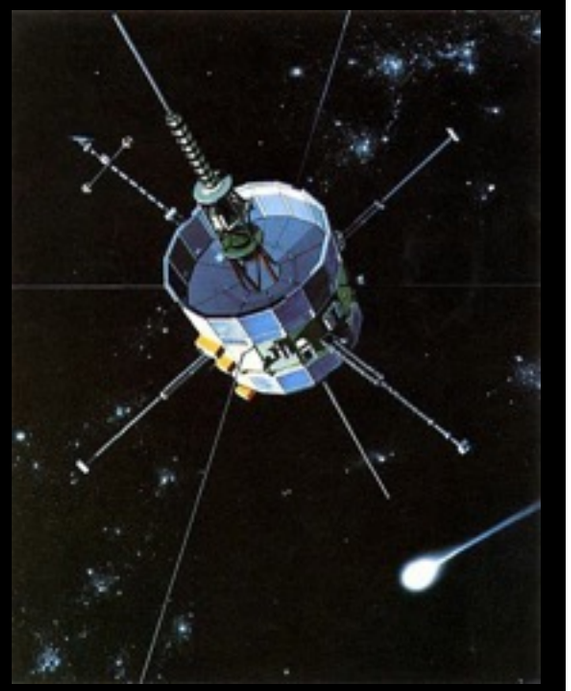
Radio Direction Finding & Mapping



Waterfall of ISEE-3 telemetry
For more detailed information, see the separate presentation: http://wiki.spench.net/wiki/Presentations#ISEE-3_Reboot_Project

ISEE-3

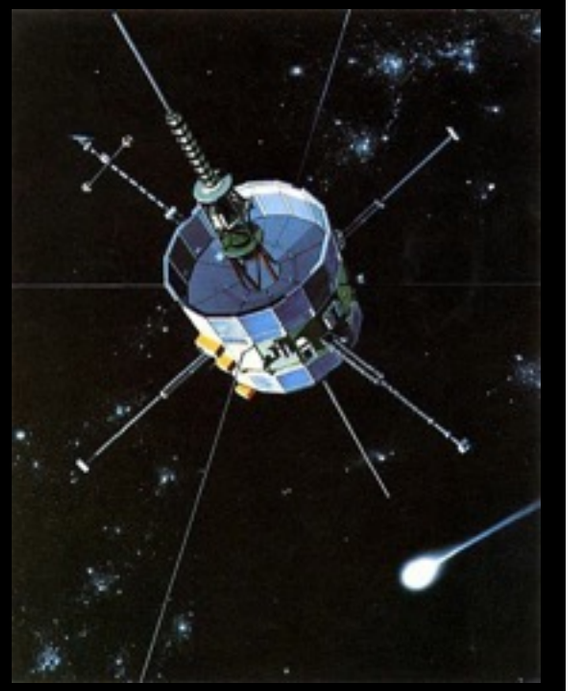
- **I**nternational **S**un/**E**arth **E**xplorer 3
- Launched: August 12, 1978
- Heliocentric Orbit
- Study interaction between solar wind and Earth's magnetic field



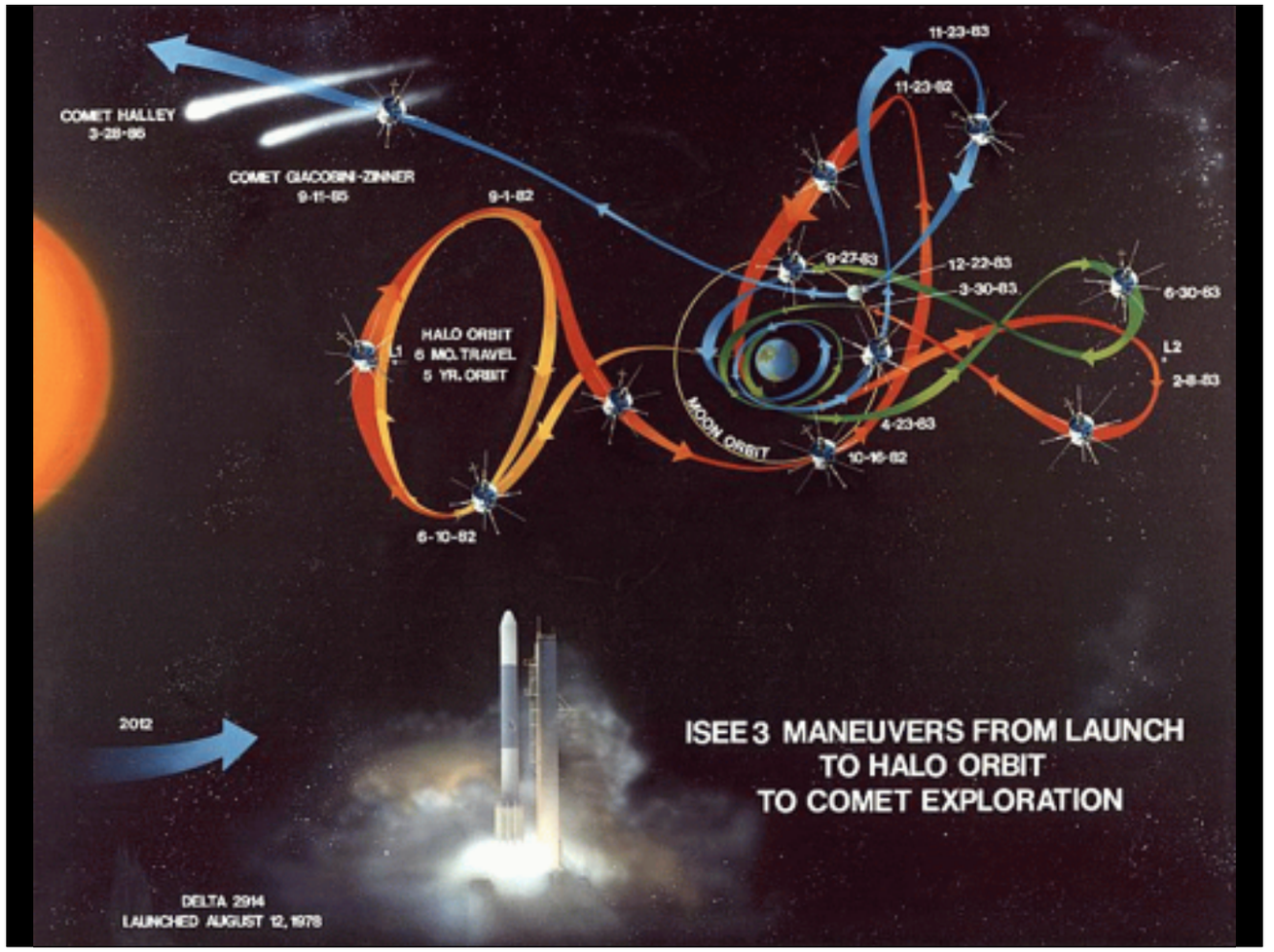
http://en.wikipedia.org/wiki/International_Cometary_Explorer

ISEE-3

- Renamed ICE: **I**nternational **C**ometary **E**xplorer
- First spacecraft in halo orbit at an Earth-Sun L1 (Lagrange point)
- First spacecraft to pass through tail of a comet (Giacobini-Zinner)

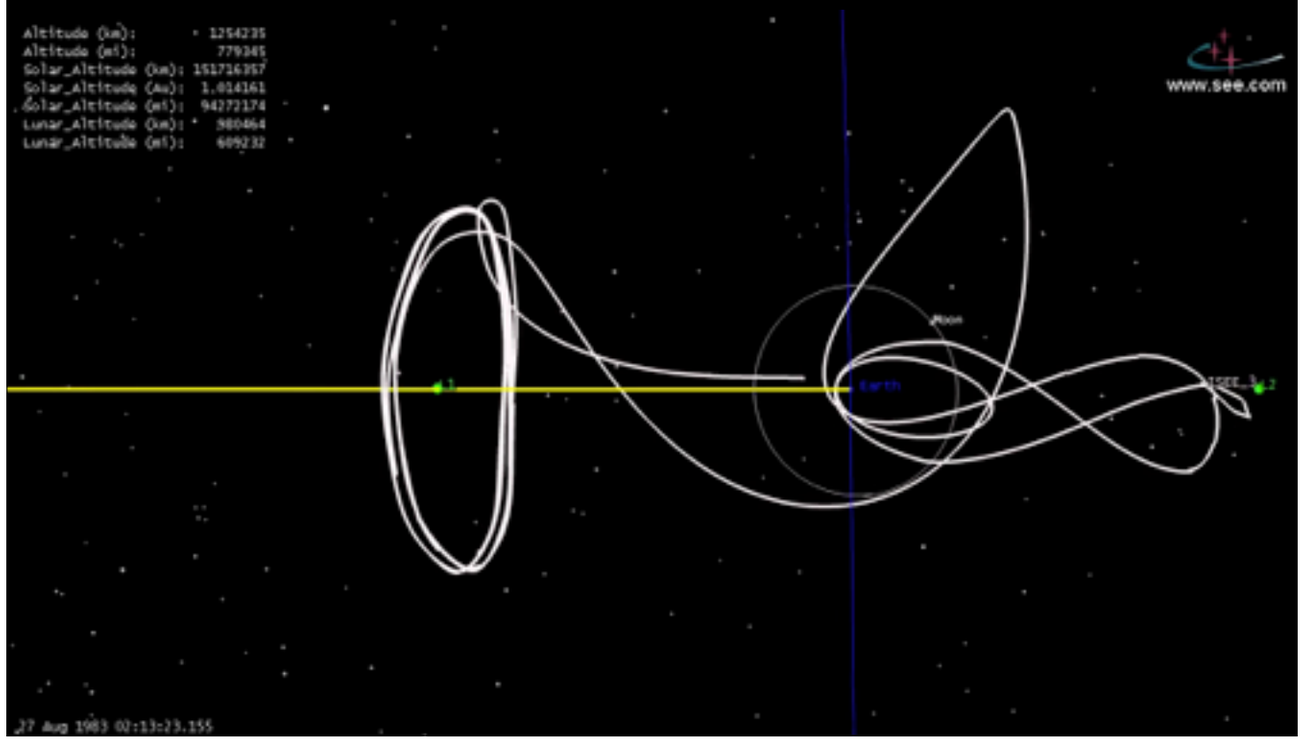


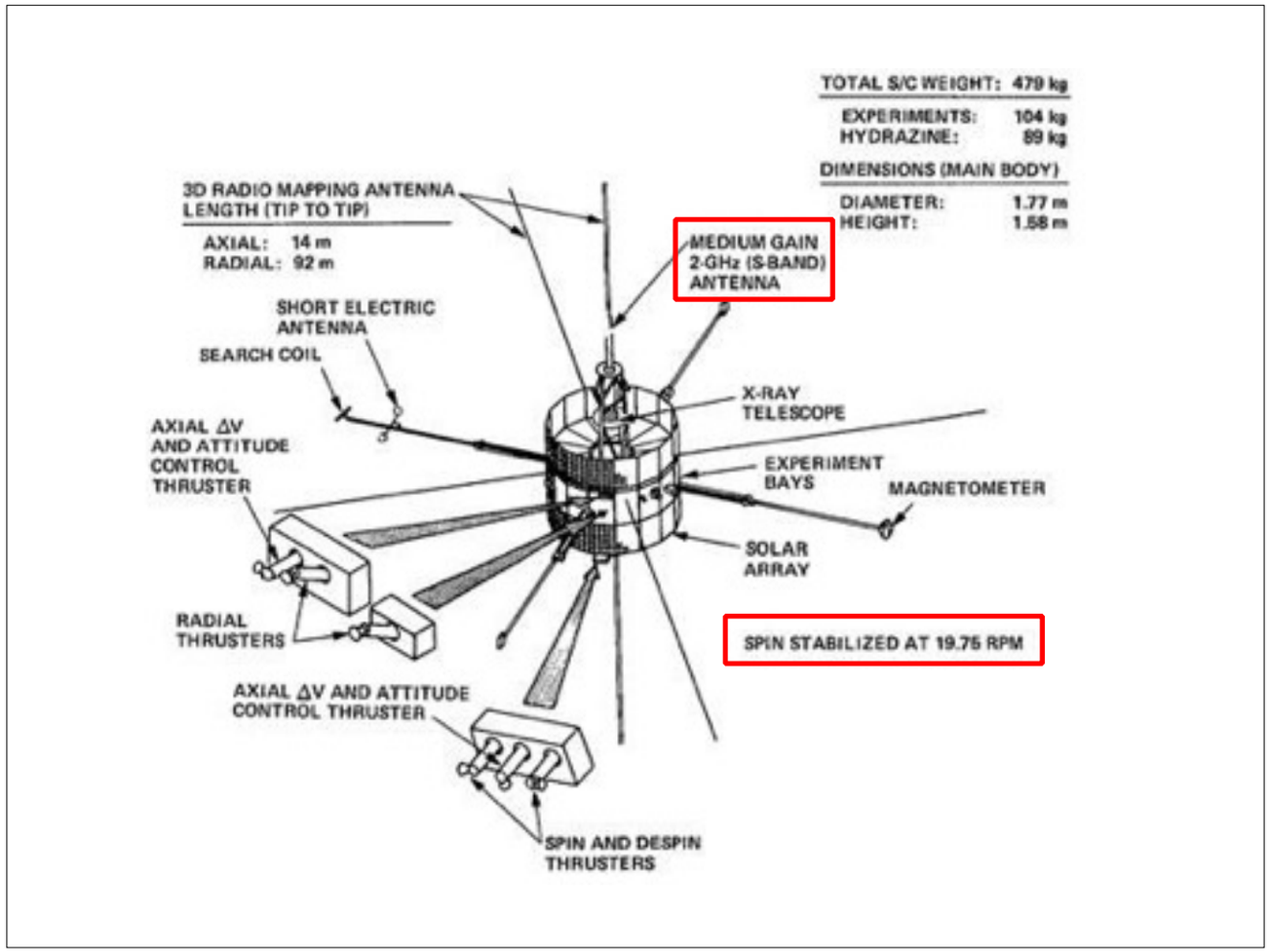
http://en.wikipedia.org/wiki/Lagrangian_point
http://en.wikipedia.org/wiki/21P/Giacobini-Zinner



http://denniswingo.wordpress.com/2014/05/15/isee-3-reboot-project-aiming-for-first-contact/

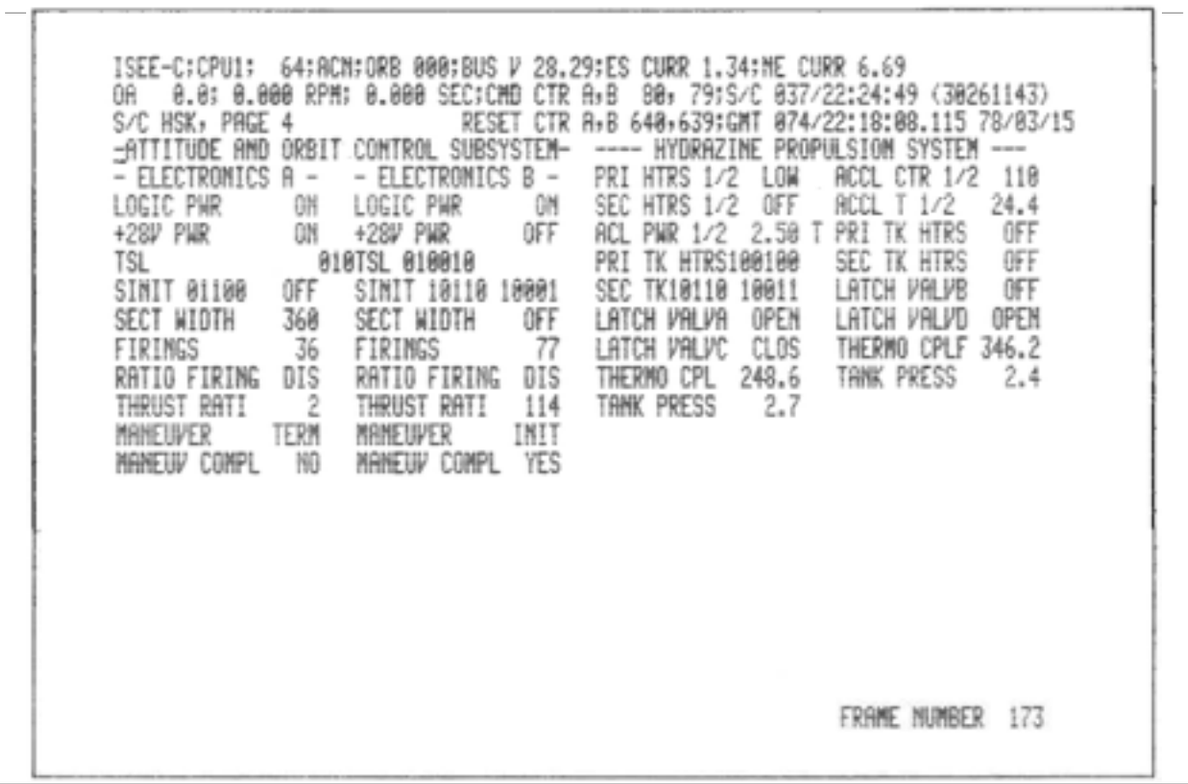
Slingshot Manoeuvre after Orbiting L1





http://denniswingo.wordpress.com/2014/05/04/isee-3-reboot-project-near-term-objectives/

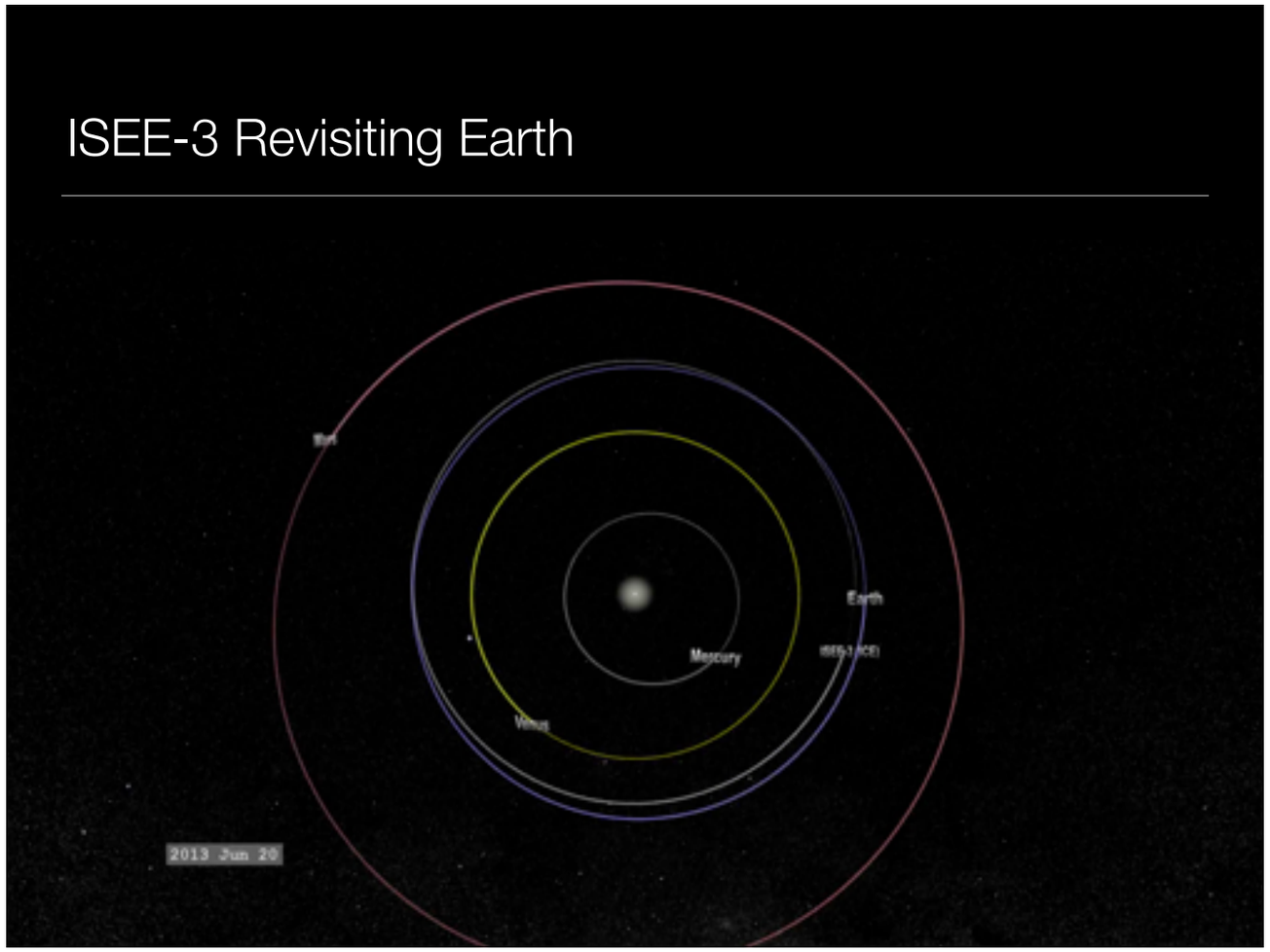
Old Telemetry Screen



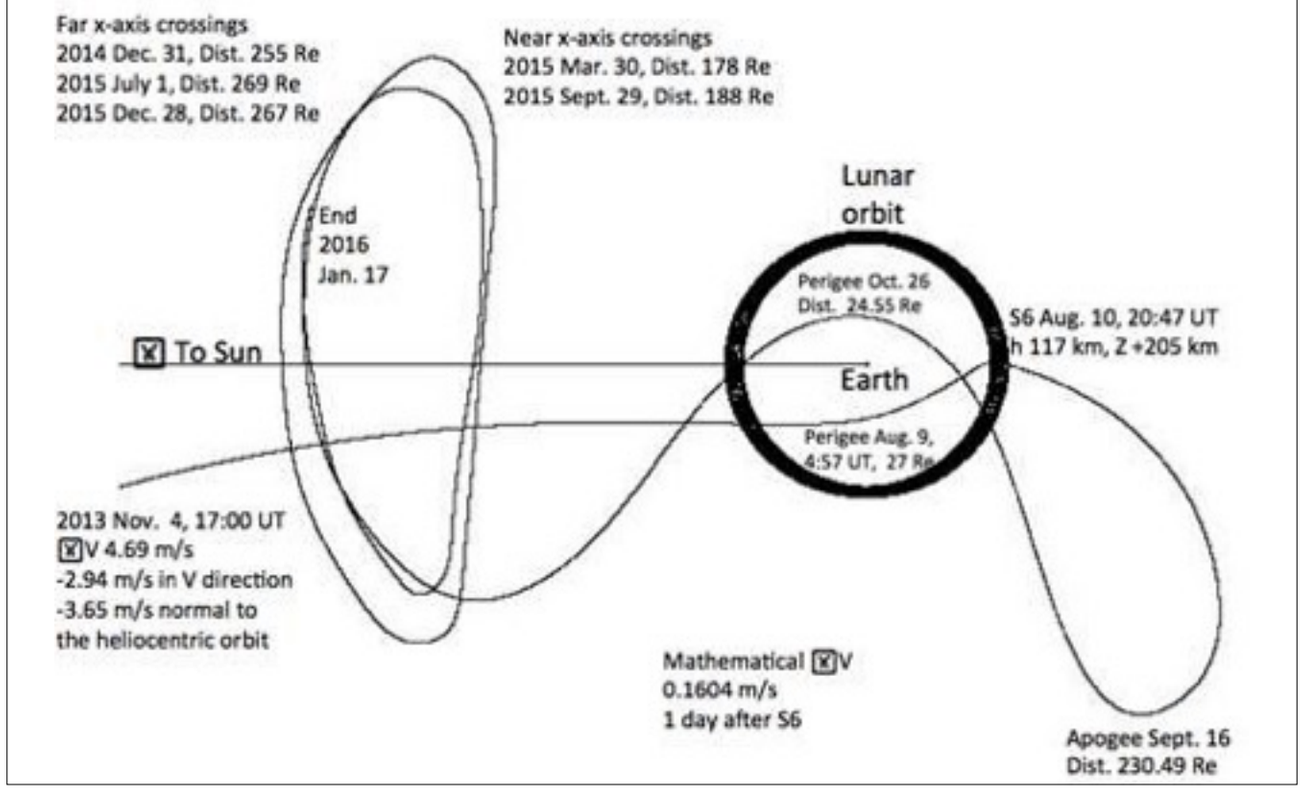
```
ISEE-C;CPU1;  64;ACN;ORB 000;BUS V 28.29;ES CURR 1.34;ME CURR 6.69
OA   0.0; 0.000 RPM; 0.000 SEC;CMD CTR A,B  00; 79;S/C 037/22:24:49 (30261143)
S/C HSK, PAGE 4              RESET CTR A,B 640,639;GMT 074/22:18:08.115 78/03/15
=ATTITUDE AND ORBIT CONTROL SUBSYSTEM-  ---- HYDRAZINE PROPULSION SYSTEM ---
- ELECTRONICS A -   - ELECTRONICS B -  PRI HTRS 1/2  LOW   ACCL CTR 1/2  110
LOGIC PWR     ON   LOGIC PWR     ON   SEC HTRS 1/2  OFF   ACCL T 1/2   24.4
+28V PWR      ON   +28V PWR     OFF   ACL PWR 1/2  2.58 T PRI TK HTRS   OFF
TSL             010TSL 010010        PRI TK HTRS100100   SEC TK HTRS   OFF
SINIT 01100   OFF  SINIT 10110 10001  SEC TK10110 10011   LATCH VALVB   OFF
SECT WIDTH    360  SECT WIDTH    OFF  LATCH VALVA  OPEN   LATCH VALVD  OPEN
FIRINGS        36  FIRINGS        77  LATCH VALVC  CLOS   THERMO CPLF 346.2
RATIO FIRING  DIS  RATIO FIRING  DIS  THERMO CPL  248.6   TANK PRESS    2.4
THRUST RATI     2  THRUST RATI   114  TANK PRESS    2.7
MANEUVER     TERM  MANEUVER     INIT
MANEUV COMPL   NO  MANEUV COMPL  YES


                                                    FRAME NUMBER  173
```

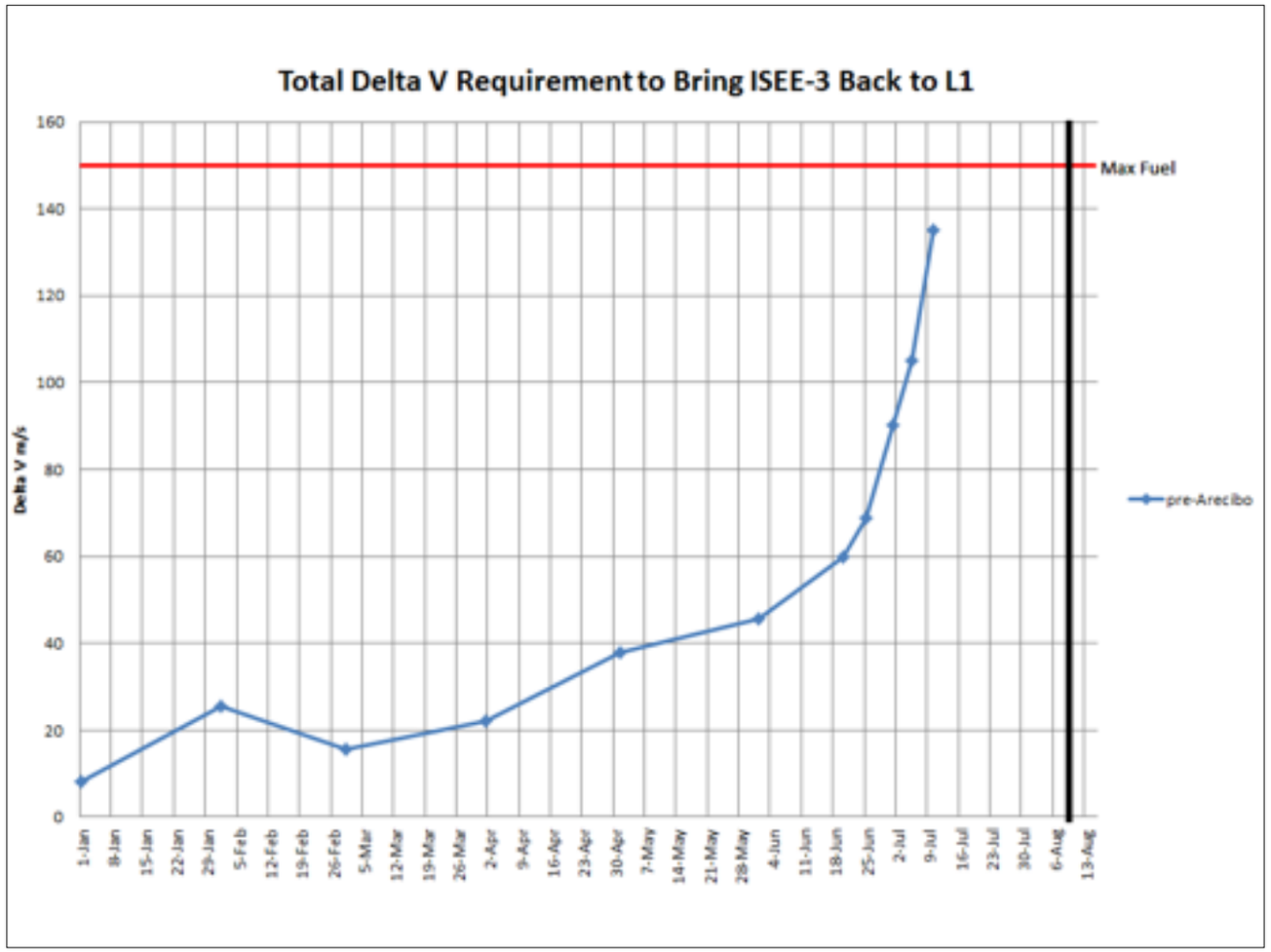
ISEE-3 Revisiting Earth



Success Case



http://denniswingo.wordpress.com/2014/05/01/isee-3-reboot-project-technical-update-and-discussion/



http://denniswingo.wordpress.com/2014/05/01/isee-3-reboot-project-technical-update-and-discussion/

Python Real-time Tracker

```
UTC  : 2014-05-28 07:50:06.234132
Local: 2014-05-28 03:50:06.234096 (-4.0)

Lines: 471/2881 (2410 left)

Speed (km/s) : -3.4829406
Speed (m/s)  : -3482.9406368
Speed (km/hr): -12538.5862925

Dist (AU) : 0.10369466811595
Dist (km) : 15512501.553089

Light time (one-way) : 51.744135 s
Light time (two-way) : 103.488271 s

R.A.:  7.7720059526
Decl: +21.4076608943
(adjusted for light time)

Downlink frequencies:

2.270400000 GHz: 2.270426377 GHz (+26.377449 kHz)
2.217500000 GHz: 2.217525763 GHz (+25.762858 kHz)
```

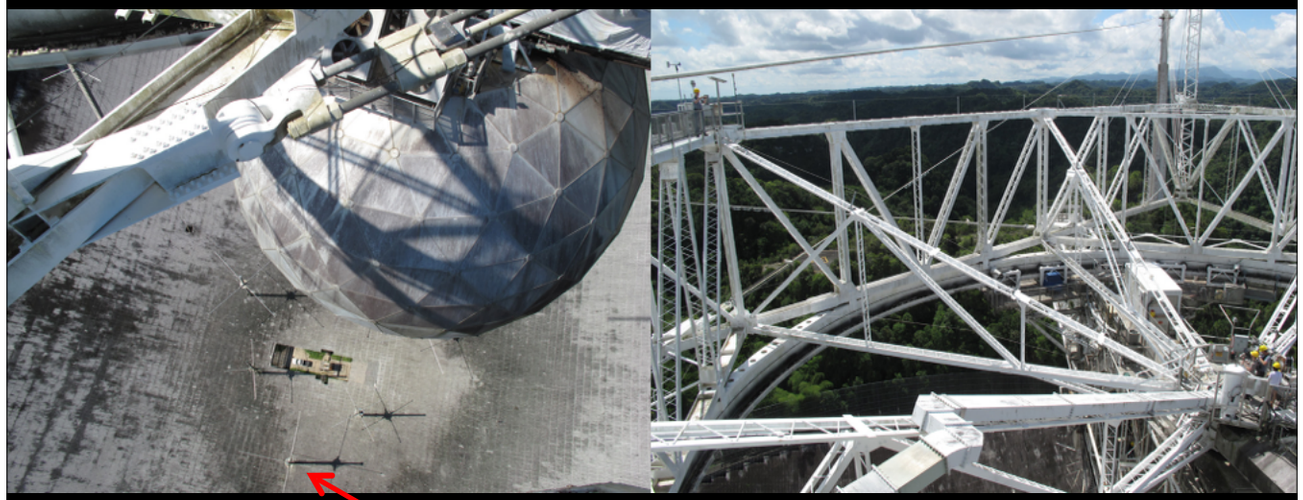
Note predicted Doppler shifts on downlink frequencies (relative to Arecibo, velocity of spacecraft, rotation & movement of the Earth)

http://en.wikipedia.org/wiki/Arecibo_Observatory
http://www.naic.edu/

Arecibo Radio Observatory

View from the 12m dish

View from Above



Heaters are not yet operational

Receiving Unmodulated Carrier

After Improving Pointing

- ~45 dB C/N
- Moving peak below due to Doppler shift

Much better SNR

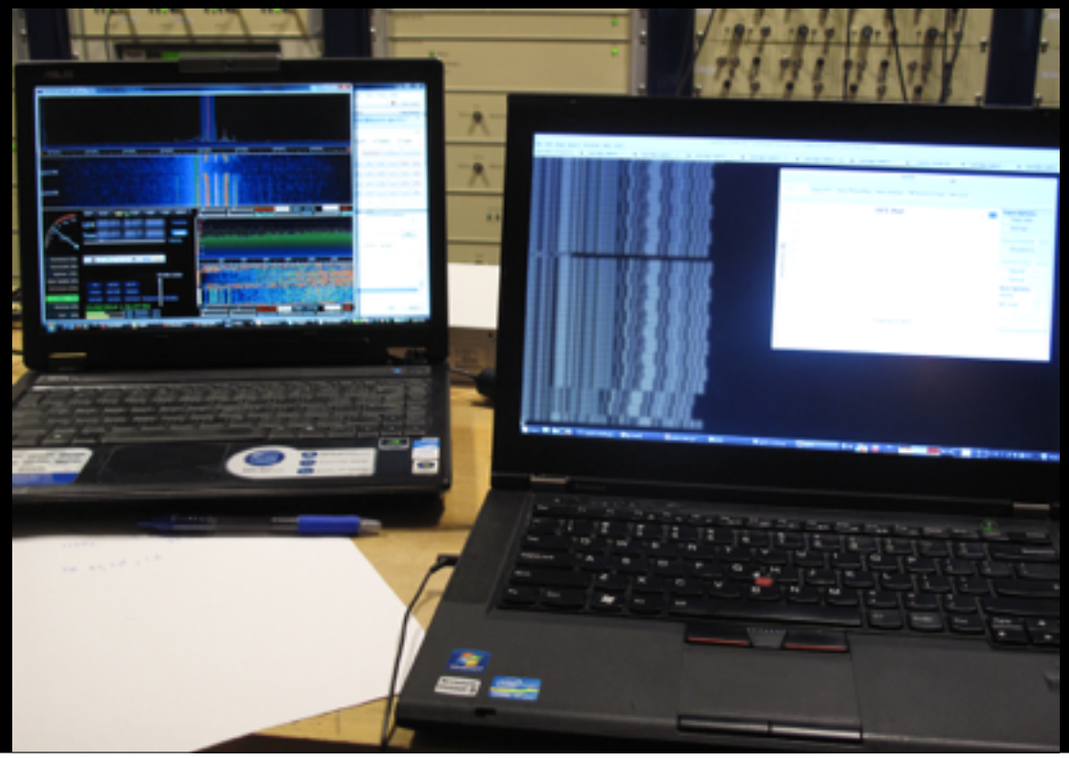
Preparing for Uplink

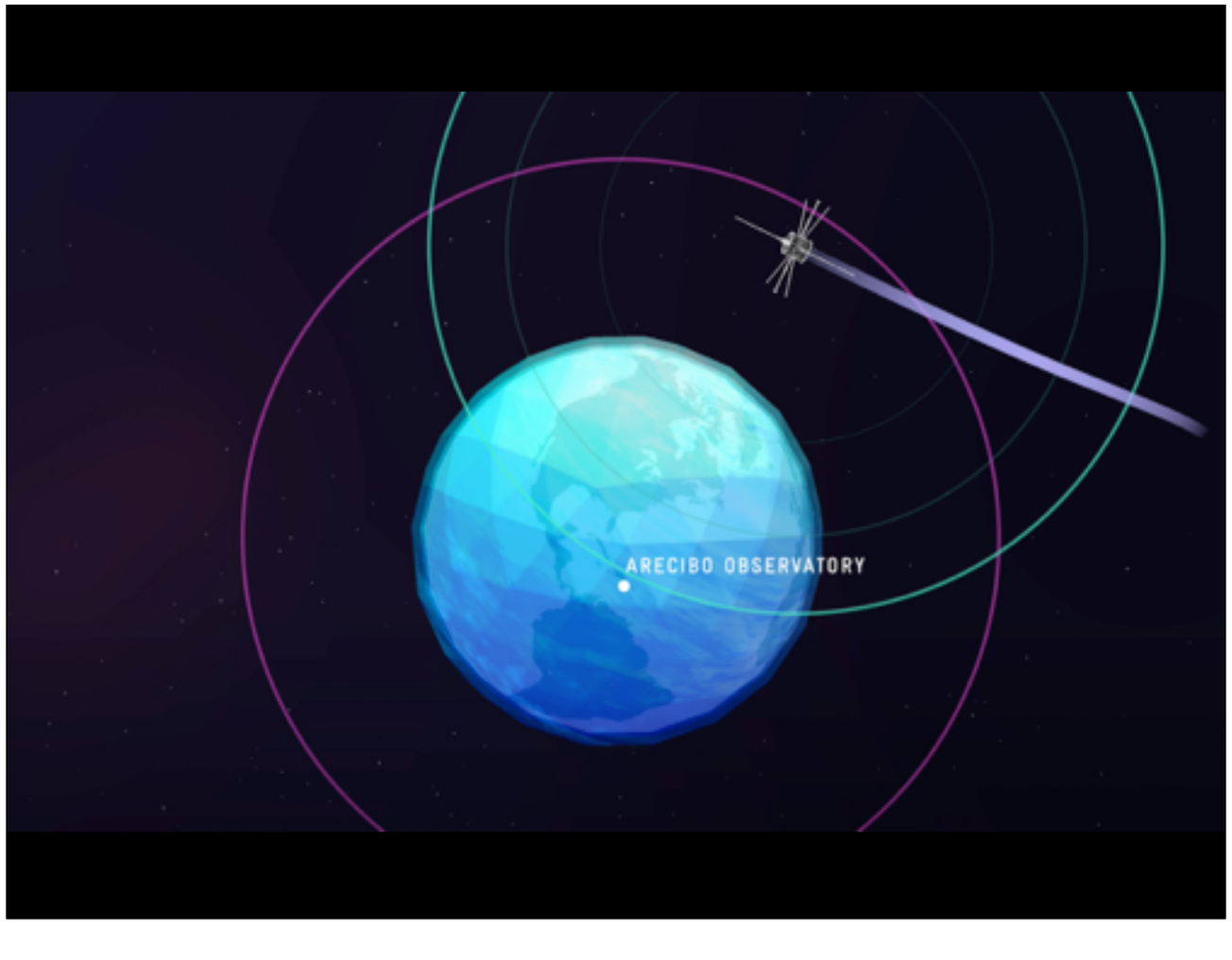
TX USRP installed in the ‘WAAP Room’

Fingers Crossed

The ‘away team’ with Dennis Wingo (L) and Austin Epps (M)

Transmission to Enable Telemetry

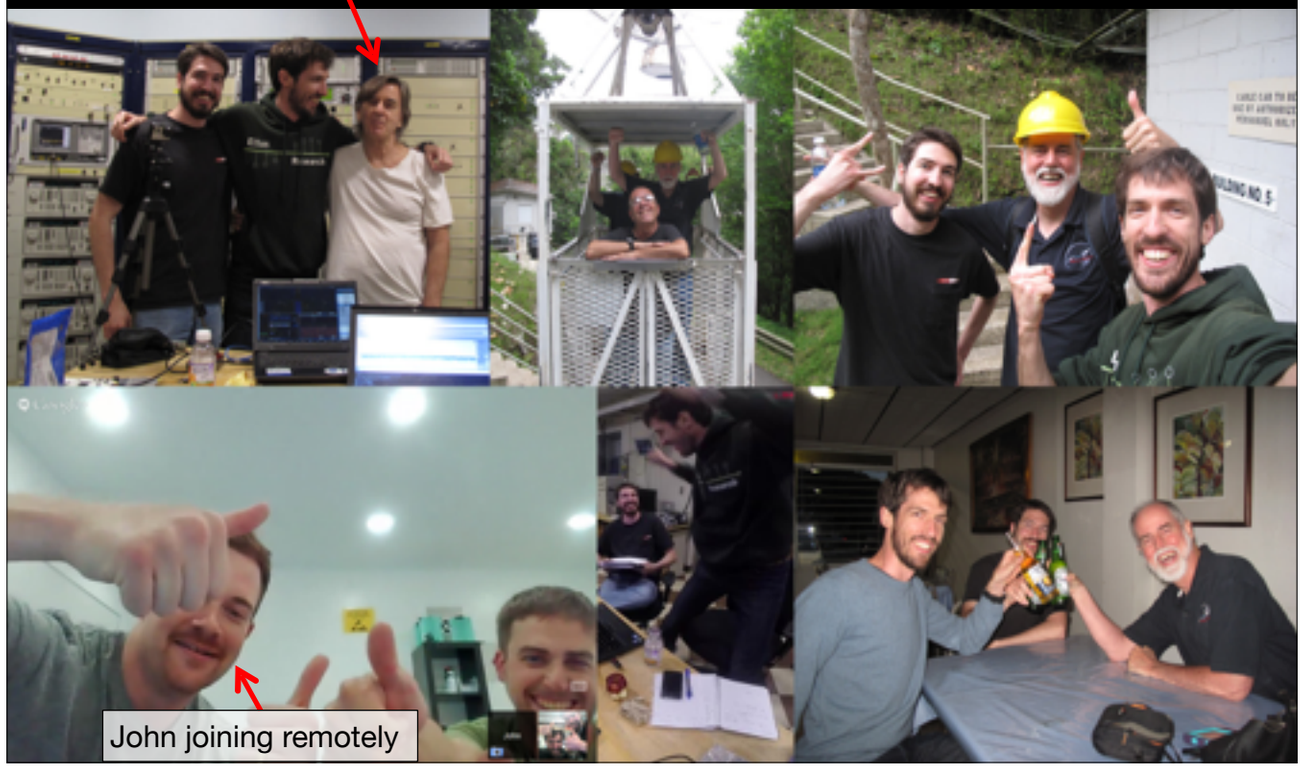



ARECIBO OBSERVATORY

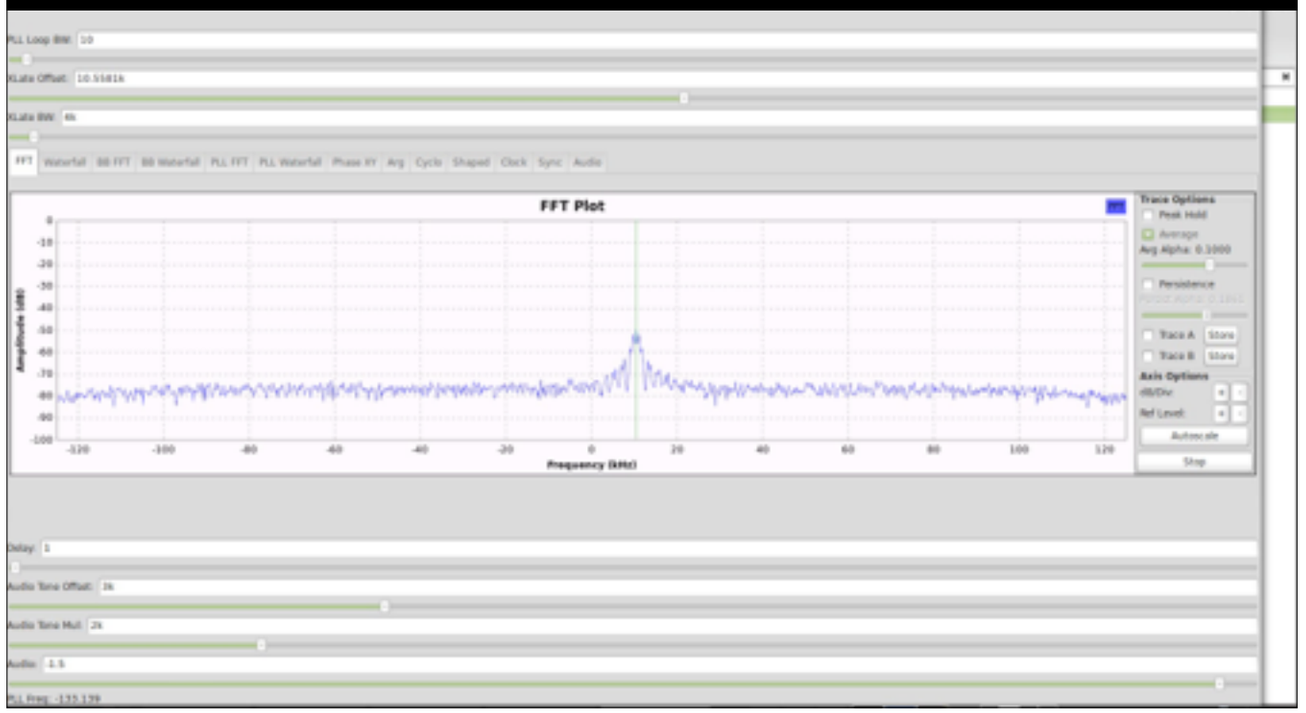
Round-trip Suspense

Live Sampled Baseband

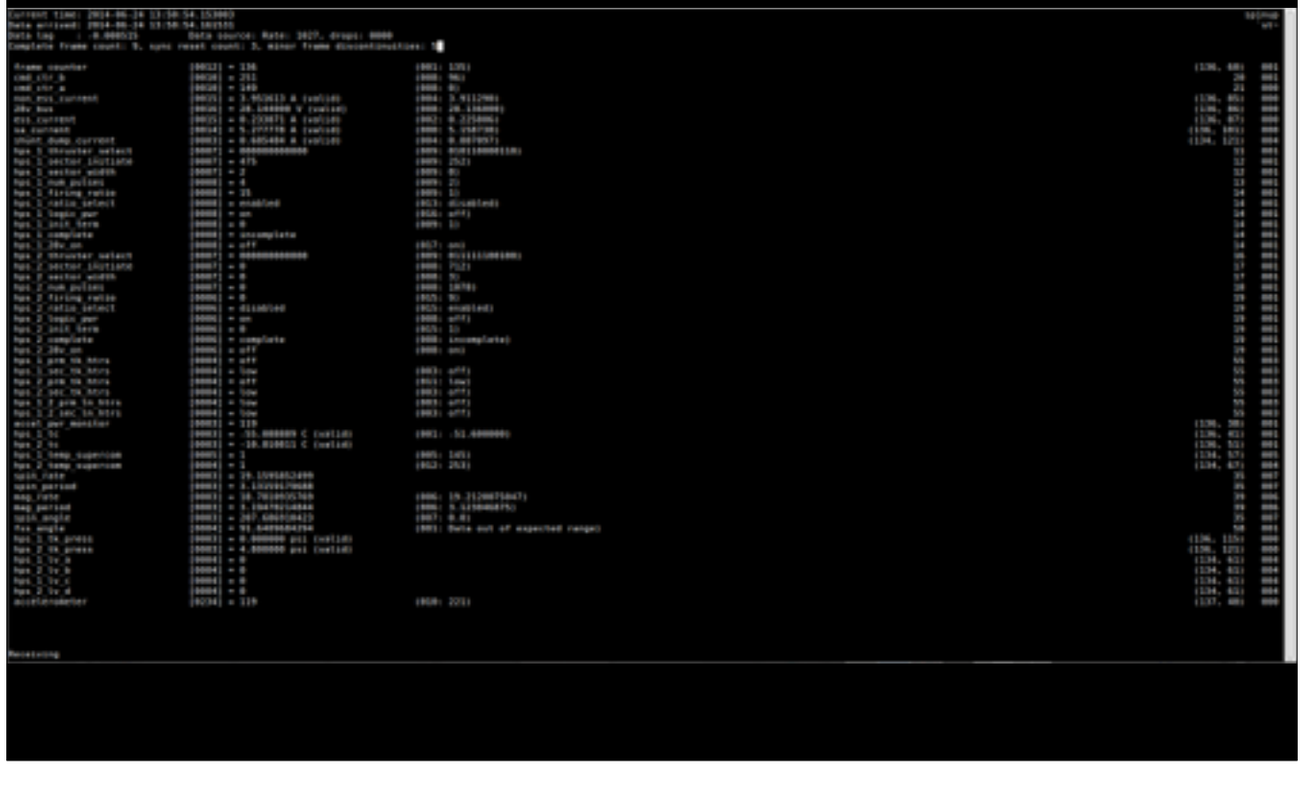
Celebration



Telemetry Demodulation & Decoding (512 bps)



Propulsion System

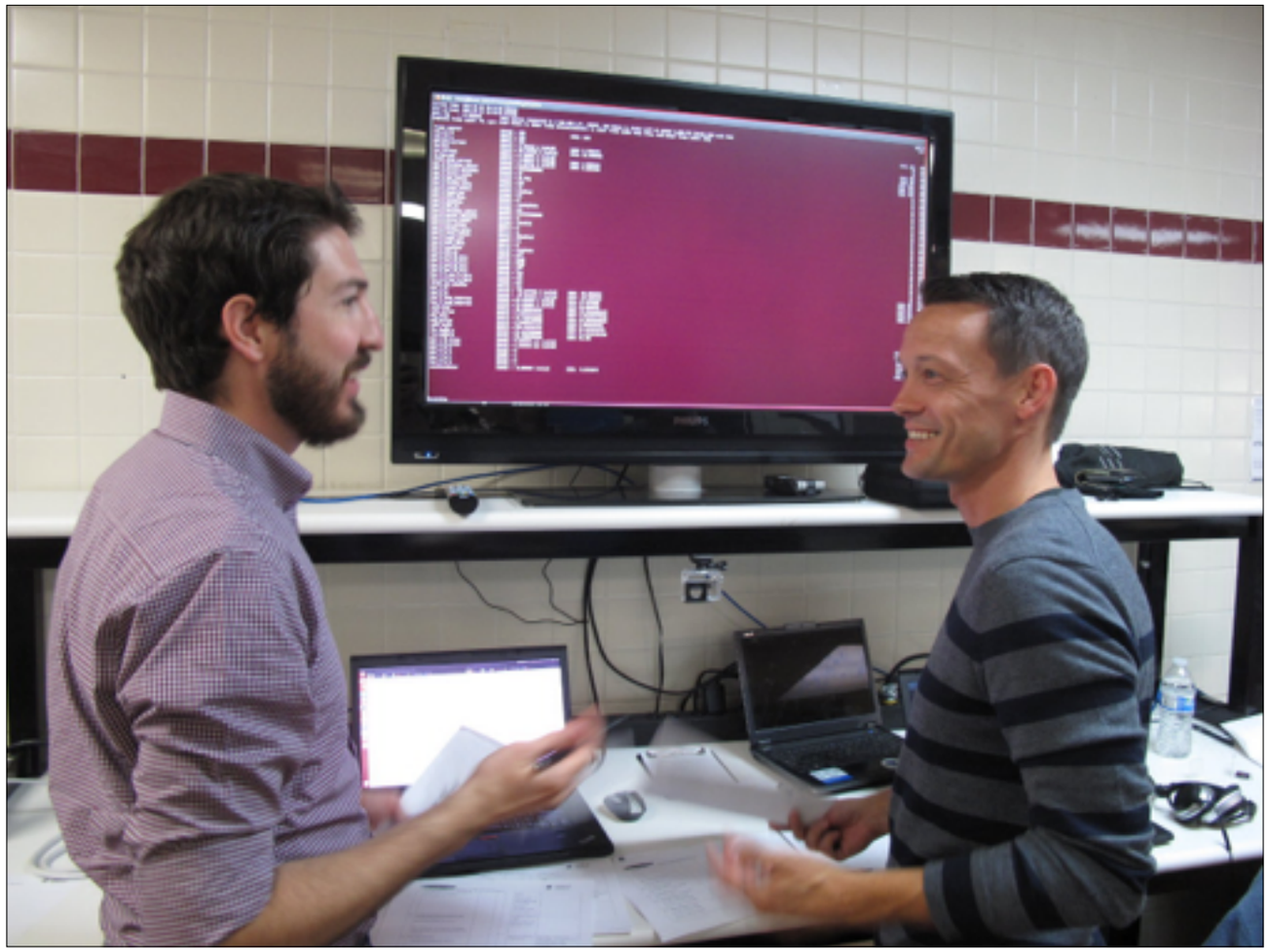


Output of ‘tlm’ from: https://github.com/balint256/ice/

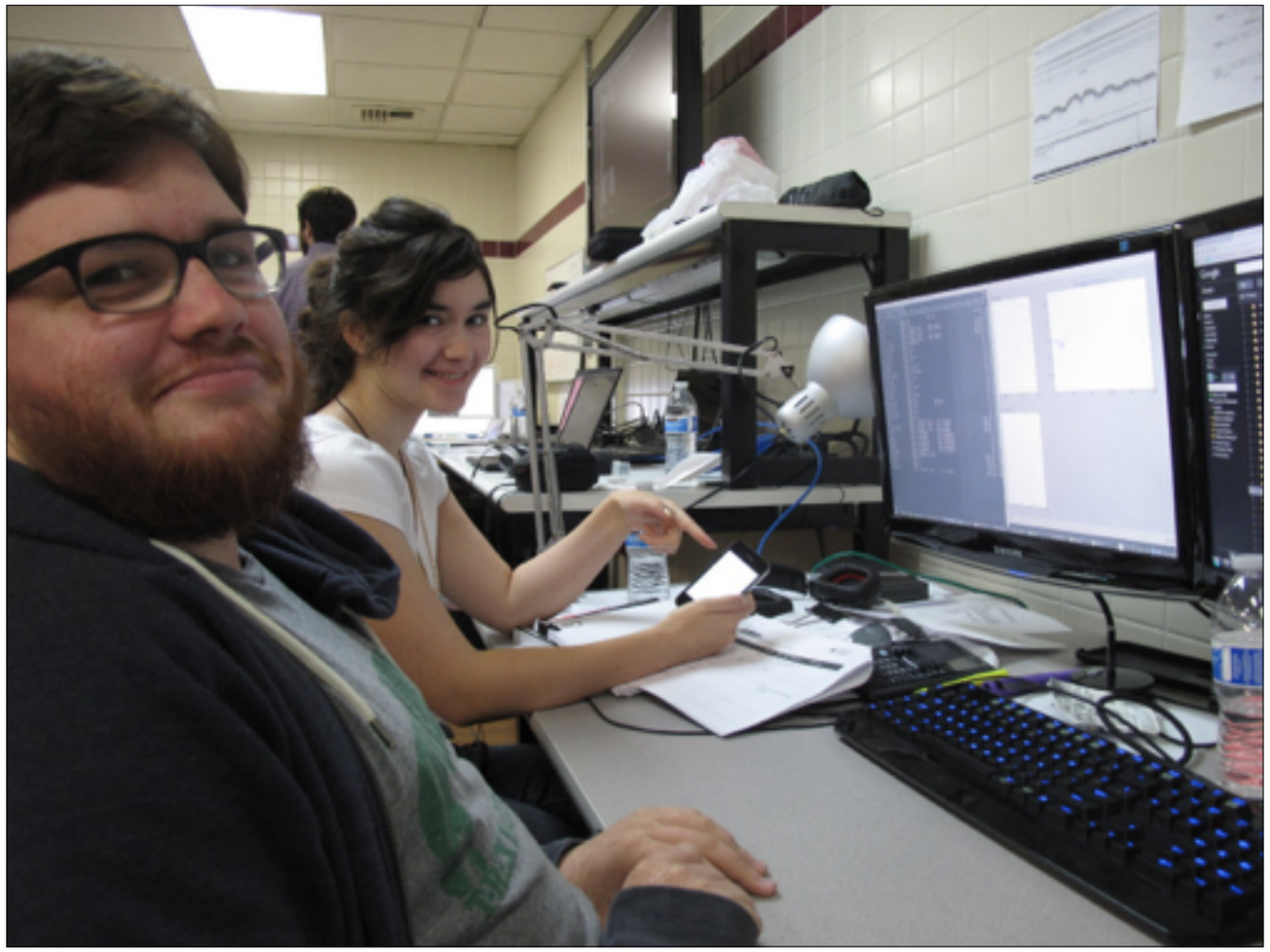
Live Telemetry from Bochum

- Many thanks to our friends at AMSAT-DL

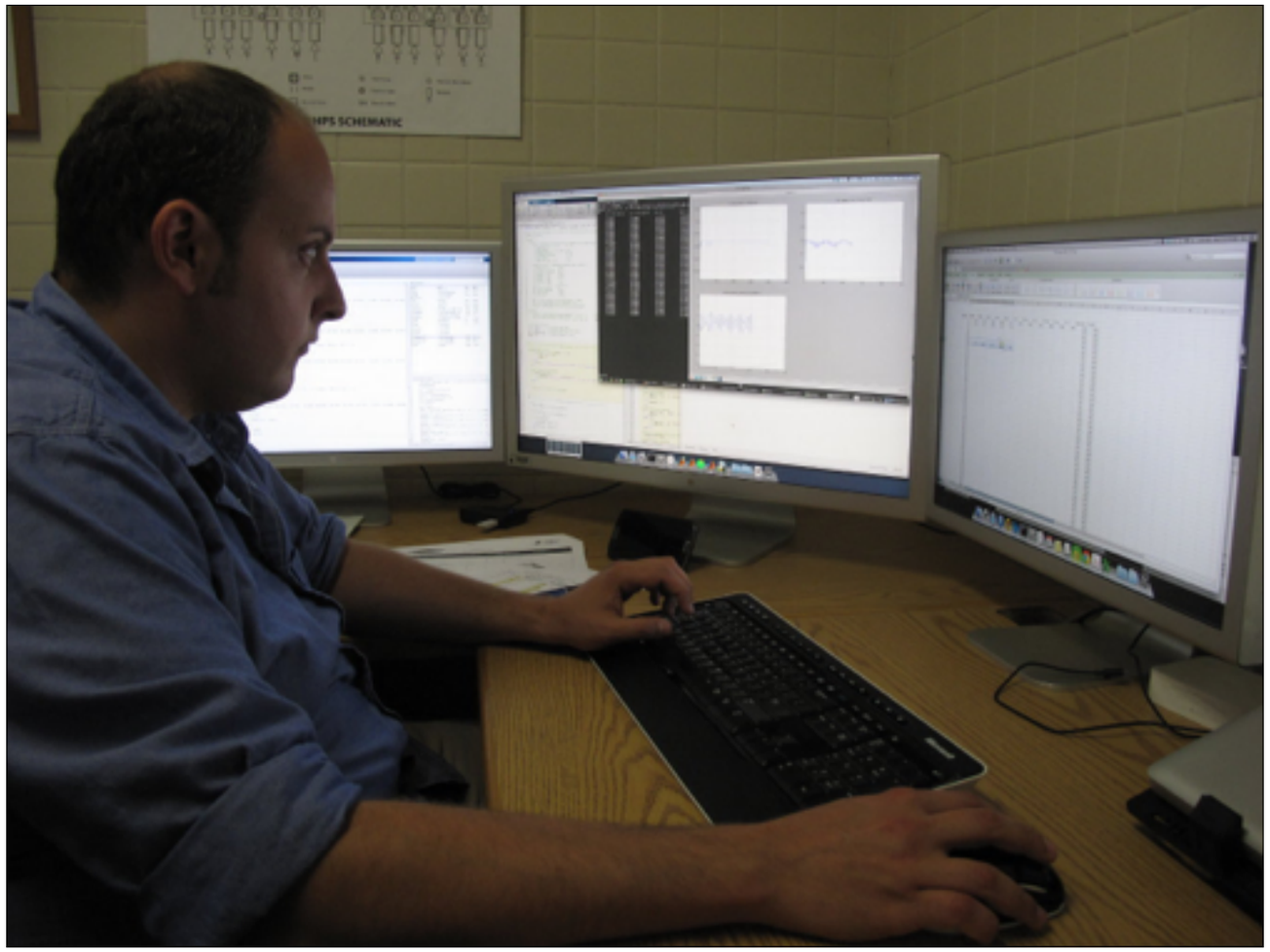
http://en.wikipedia.org/wiki/Bochum_Observatory
http://www.amsat.org/amsat-dl/adl-engl.html



Austin Epps, Cameron Woodman

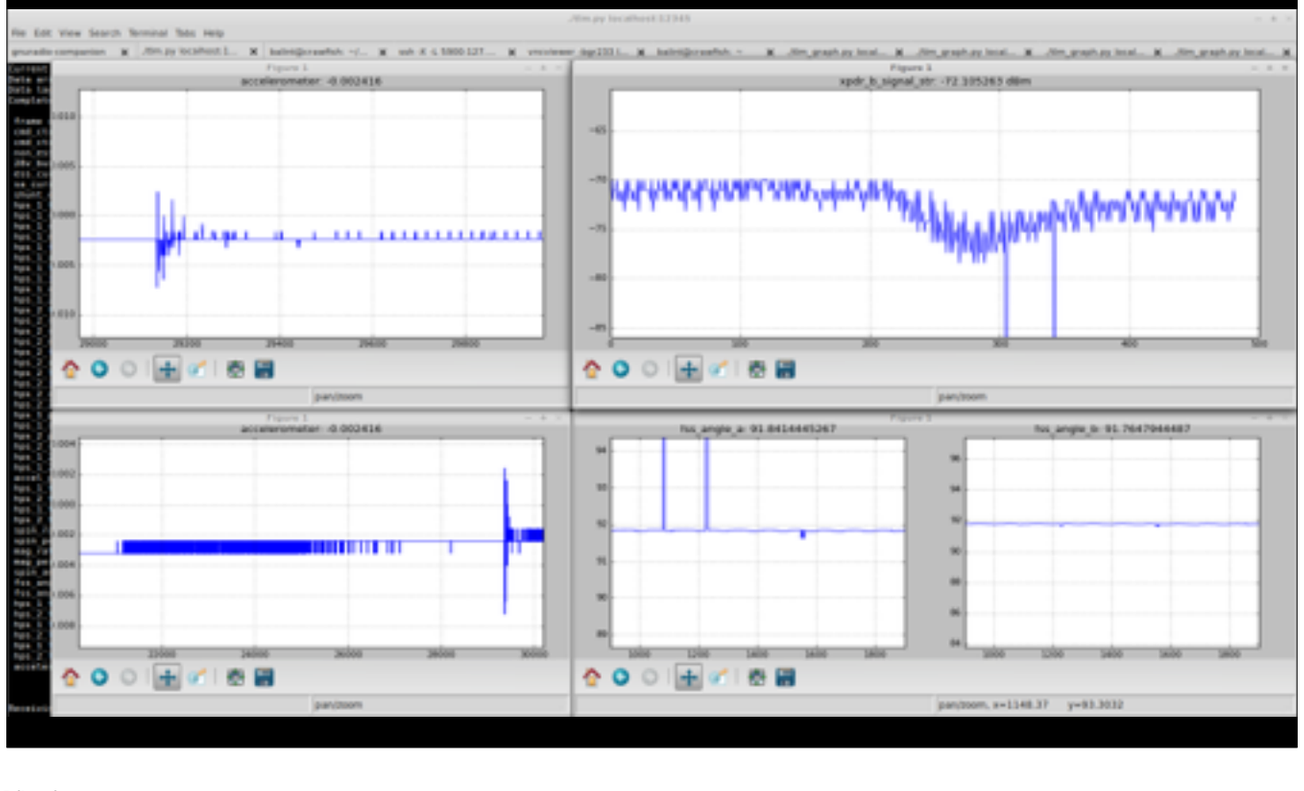


Jacob Gold, Casey Harper



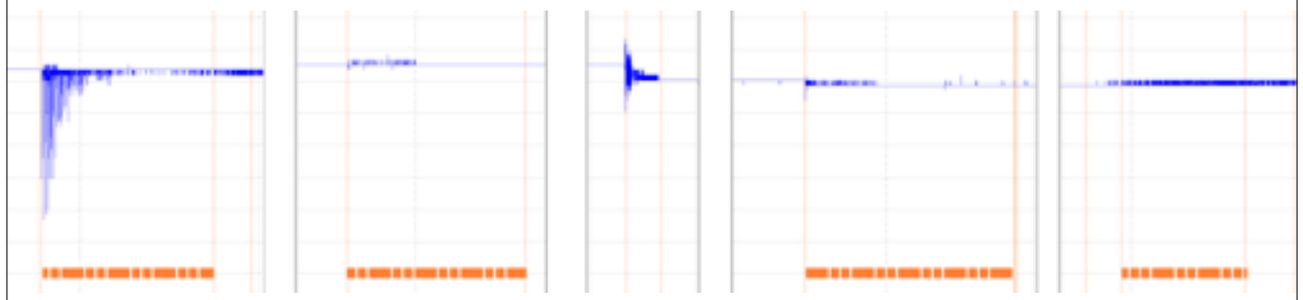
Marco Colleluori

Telemetry During Thruster Firing



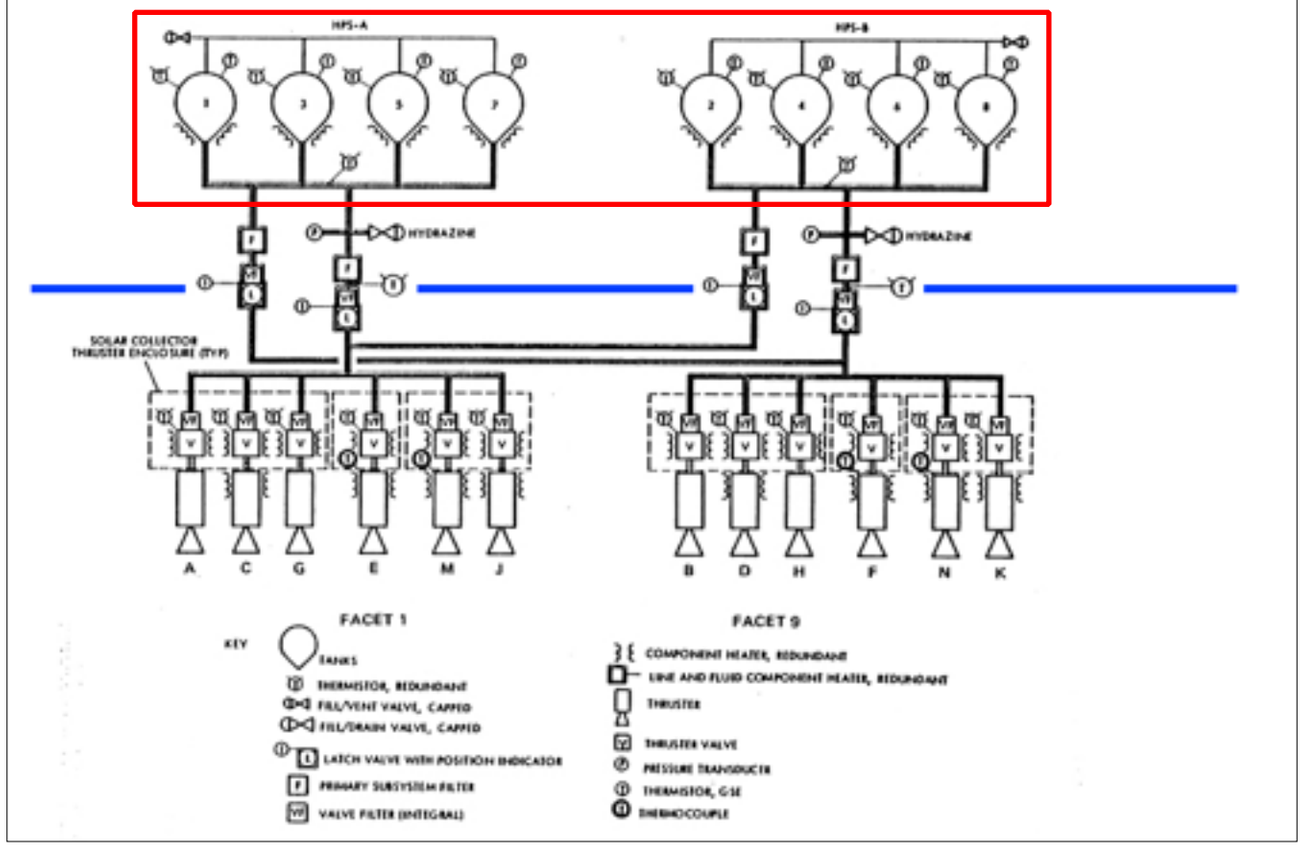
Graphed with ‘tlm_graph’ from: https://github.com/balint256/ice/

No Thrust



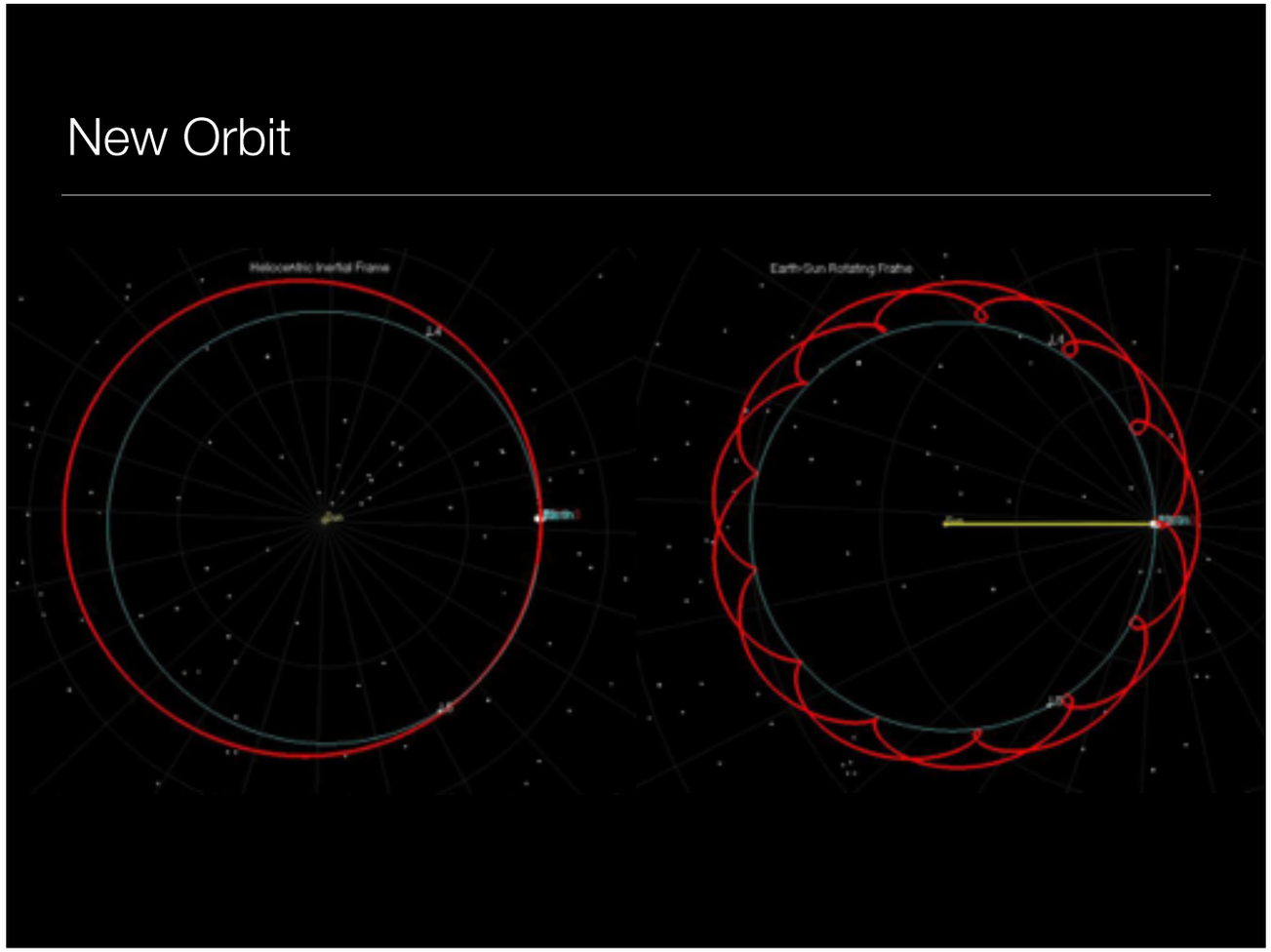
Each attempt would produce only one (or no) pulse on the real-time accelerometer data. Expectation was to see a large pulse for each firing of the selected thrusters.

Hydrazine Propulsion System

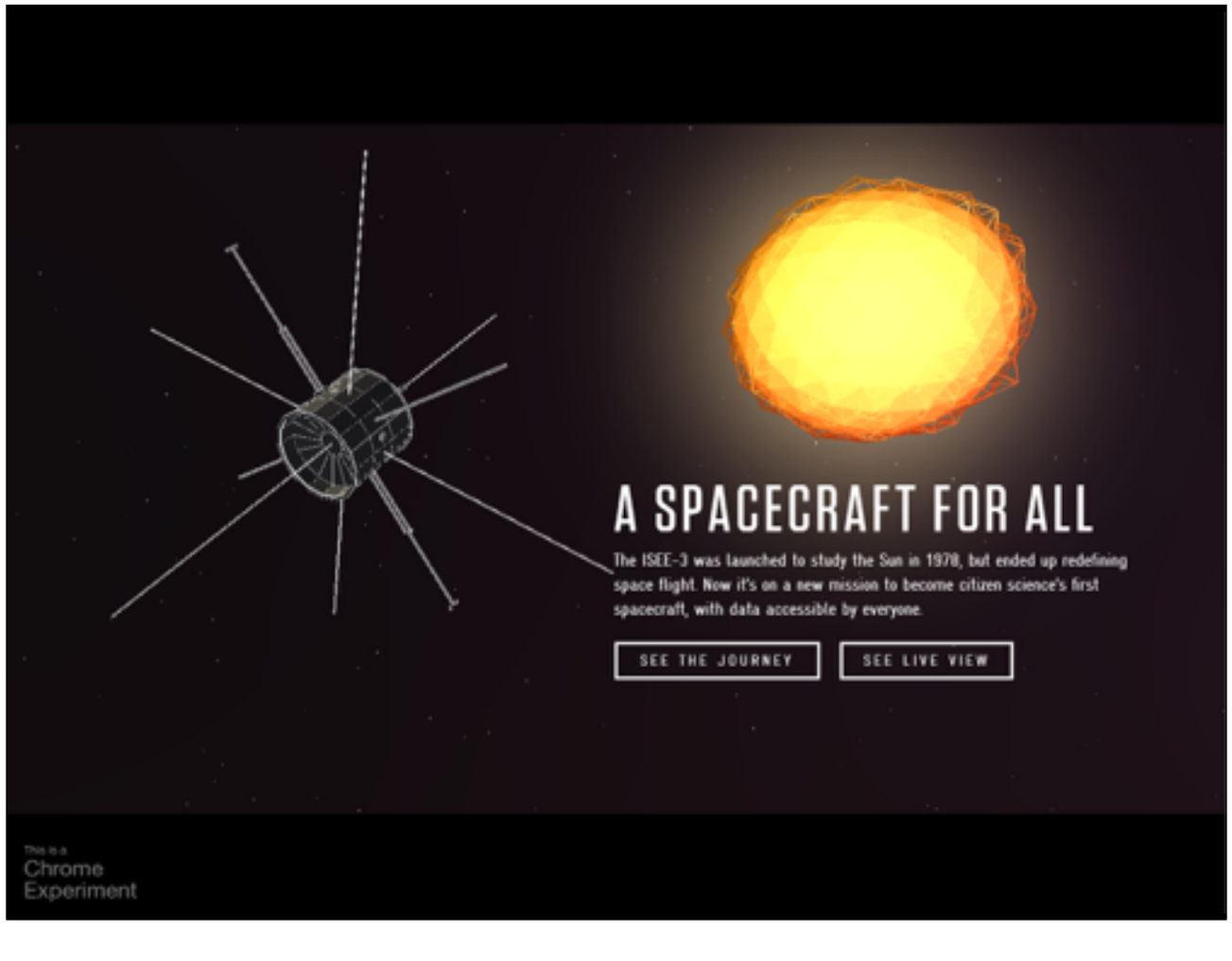


Nitrogen (pressurant) might have leaked out of both sets of tanks.

New Orbit

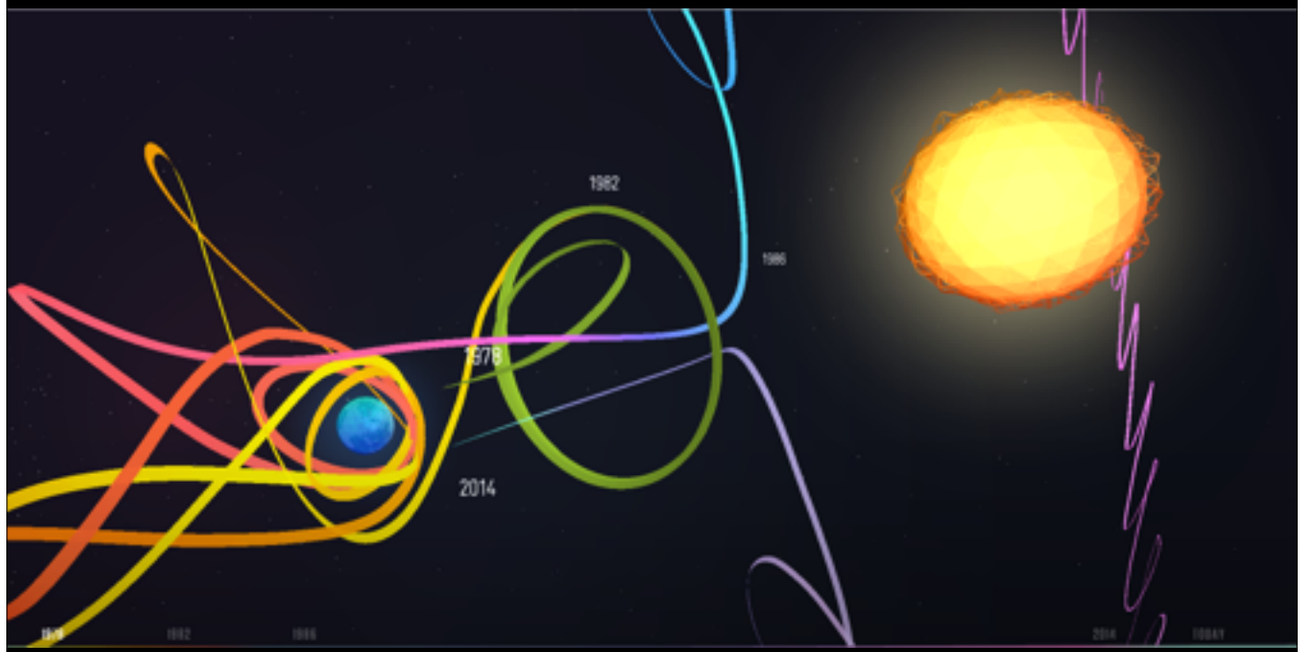


From Cameron Woodman:
“So with the failure to perform a trajectory maneuver before the lunar flyby, we passed the Moon at an altitude of 13,000 km instead of the 50 km we needed to bring the s/c back
Here is it’s new orbit and it’s now mostly outside Earth’s orbit
Brings new challenges, the spacecraft will be farther away from the sun than it was ever designed to be ~20% farther at it’s furthest point:
Less power generated by the solar arrays, it’s also going to be a lot colder.
It will come back again in 15 years.
After the failure of the propulsion system we quickly shifted gears, turned on the data from the science experiments and powered up some of the remaining experiments.”



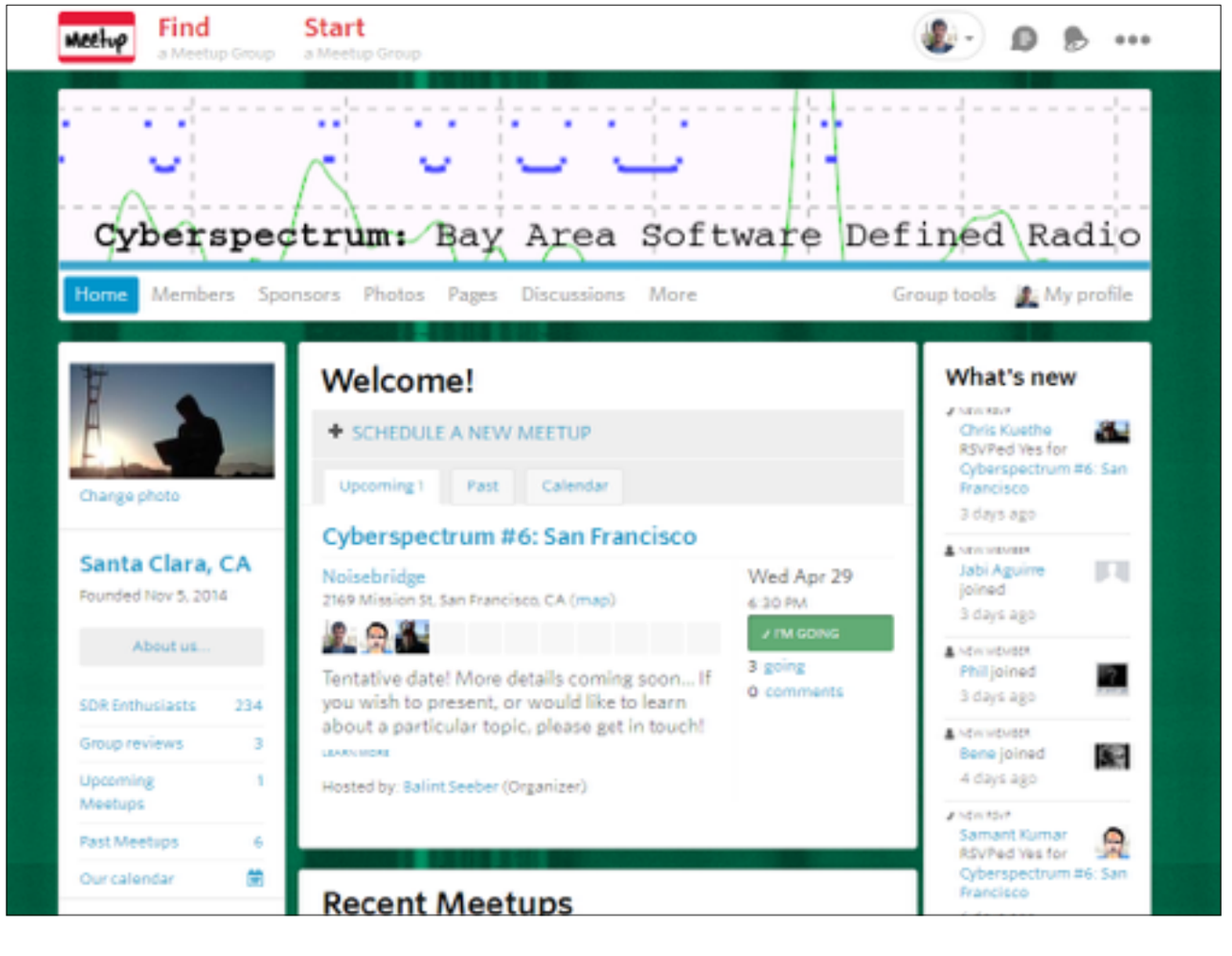
http://spacecraftforall.com/

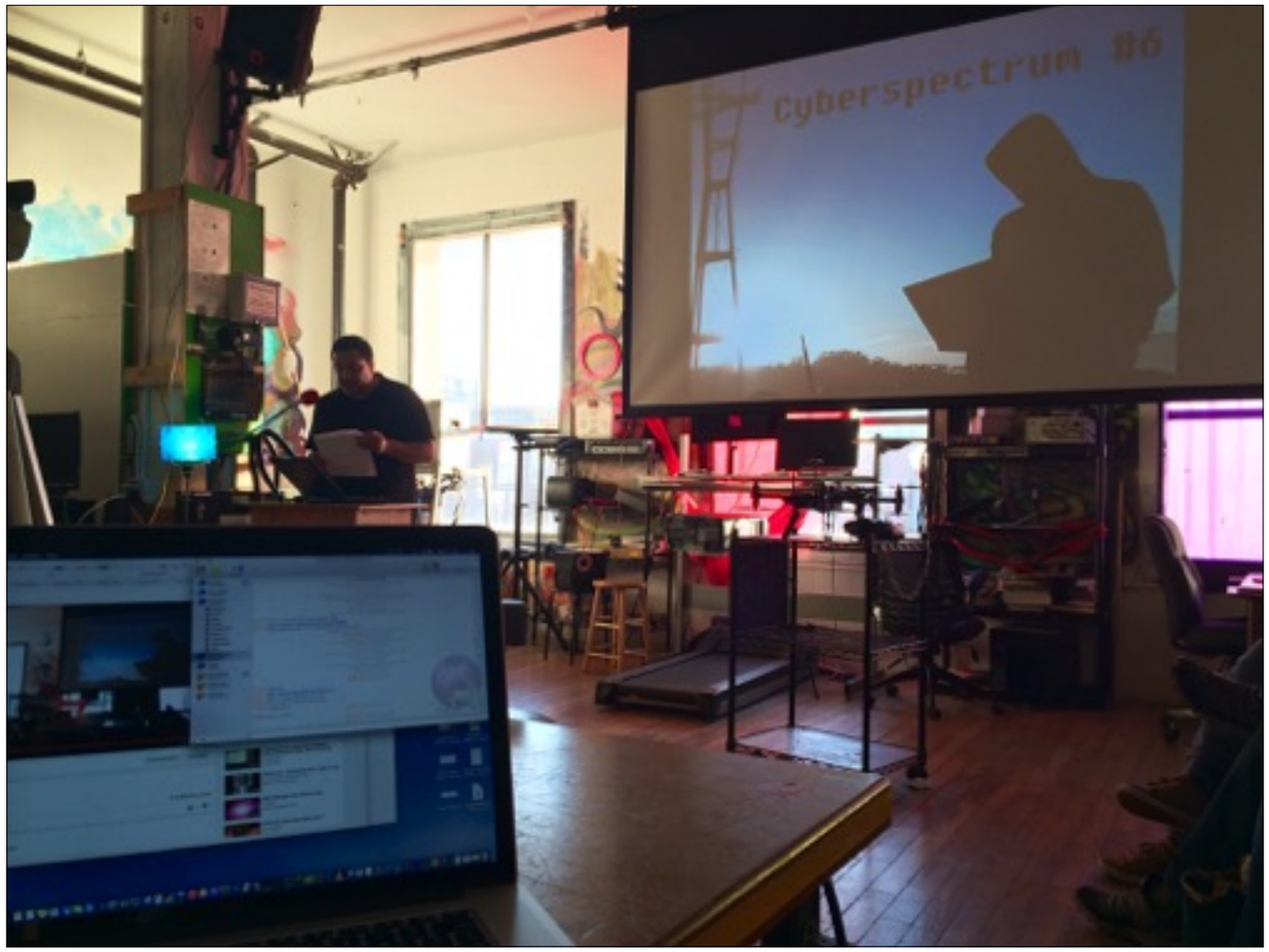
www.spacecraftforall.com

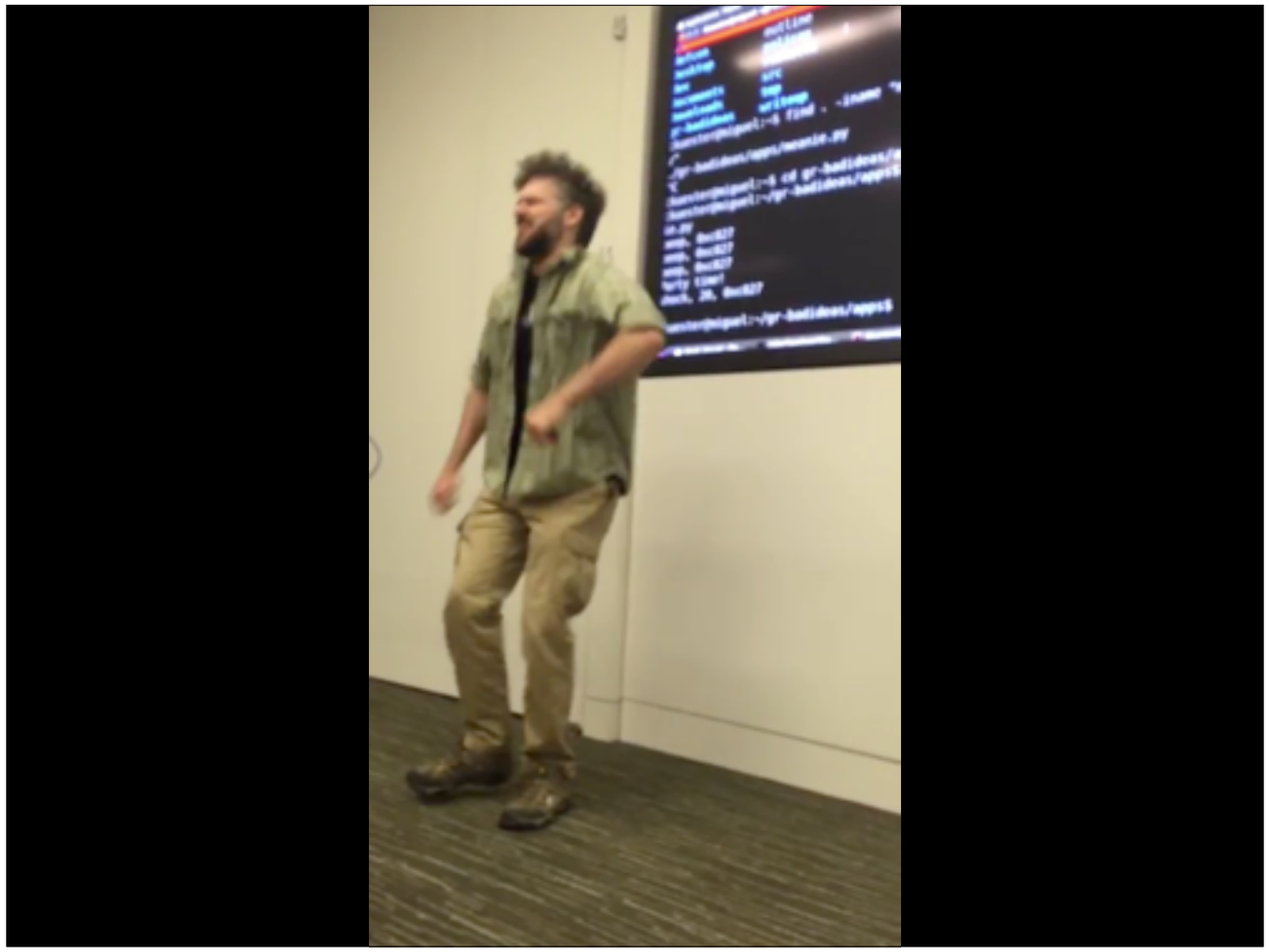


http://spacecraftforall.com/

The team outside McMoons


Find
a Meetup Group
Start
a Meetup Group
Cyberspectrum: Bay Area Software Defined Radio
Home
Members
Sponsors
Photos
Pages
Discussions
More
Group tools
My profile
Change photo
Santa Clara, CA
Founded Nov 5, 2014
About us...
SDR Enthusiasts 234
Group reviews 3
Upcoming Meetups 1
Past Meetups 6
Our calendar
Welcome!
SCHEDULE A NEW MEETUP
Upcoming 1
Past
Calendar
Cyberspectrum #6: San Francisco
Noisebridge
2169 Mission St, San Francisco, CA (map)
Wed Apr 29
6:30 PM
I'M GOING
3 going
0 comments
Tentative date! More details coming soon... If you wish to present, or would like to learn about a particular topic, please get in touch!
Hosted by: Balint Seeber (Organizer)
What's new
Chris Kuethe RSVPed Yes for Cyberspectrum #6: San Francisco
3 days ago
Jabi Aguirre joined
3 days ago
Phil joined
3 days ago
Bene joined
4 days ago
Samant Kumar RSVPed Yes for Cyberspectrum #6: San Francisco
Recent Meetups


Cyberspectrum 86



Thank you!

You can't protect what you can't see.

@spenchdotnet

balint@bastille.io

GitHub: balint256

Bastille