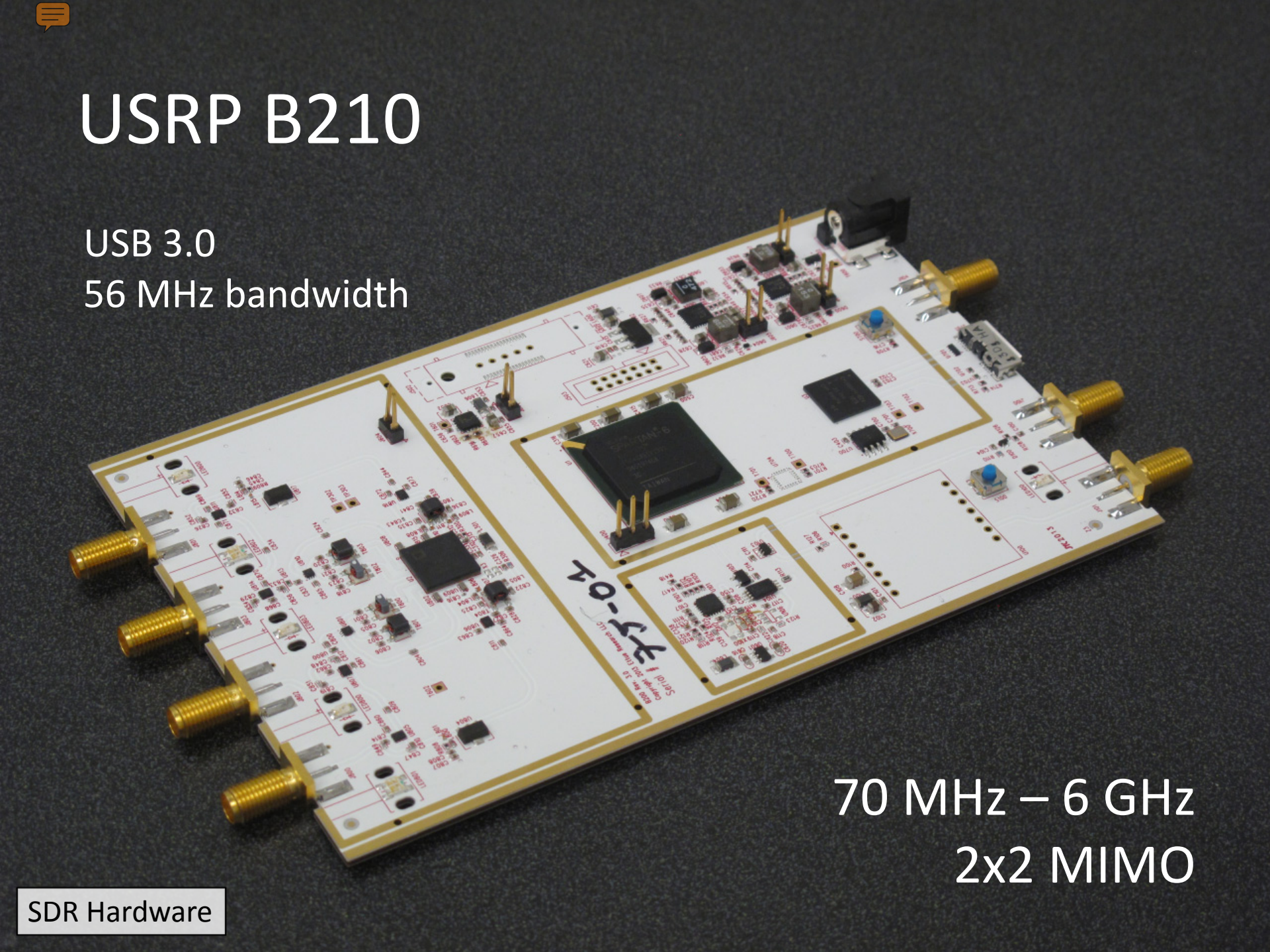
Preview:

Hacking the Wireless World with Software Defined Radio – 2.0

Balint Seeber
Applications Specialist & SDR Evangelist
balint@ettus.com
balint@spench.net @spenchdotnet

USRP B210



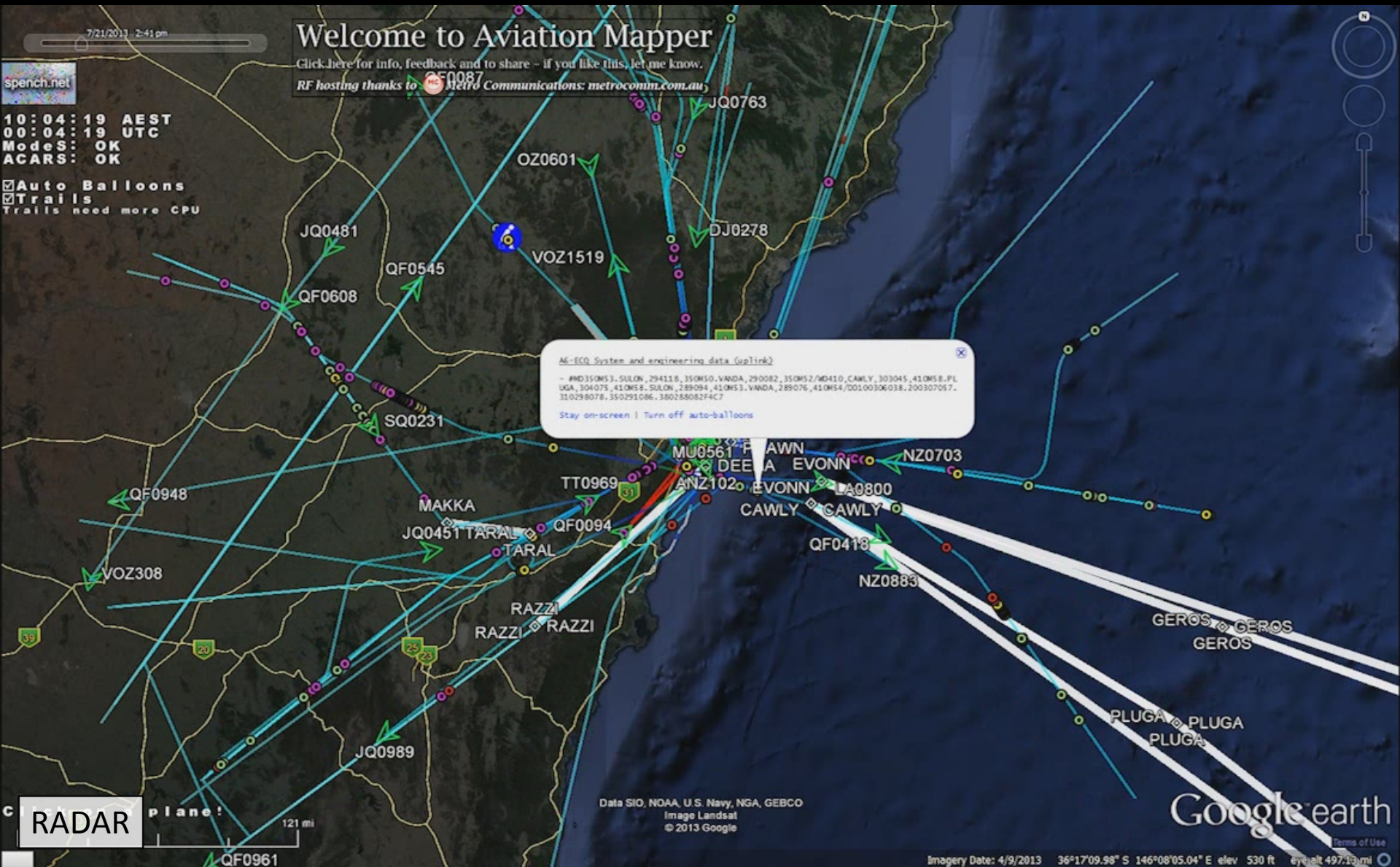
USB 3.0
56 MHz bandwidth

70 MHz – 6 GHz
2x2 MIMO

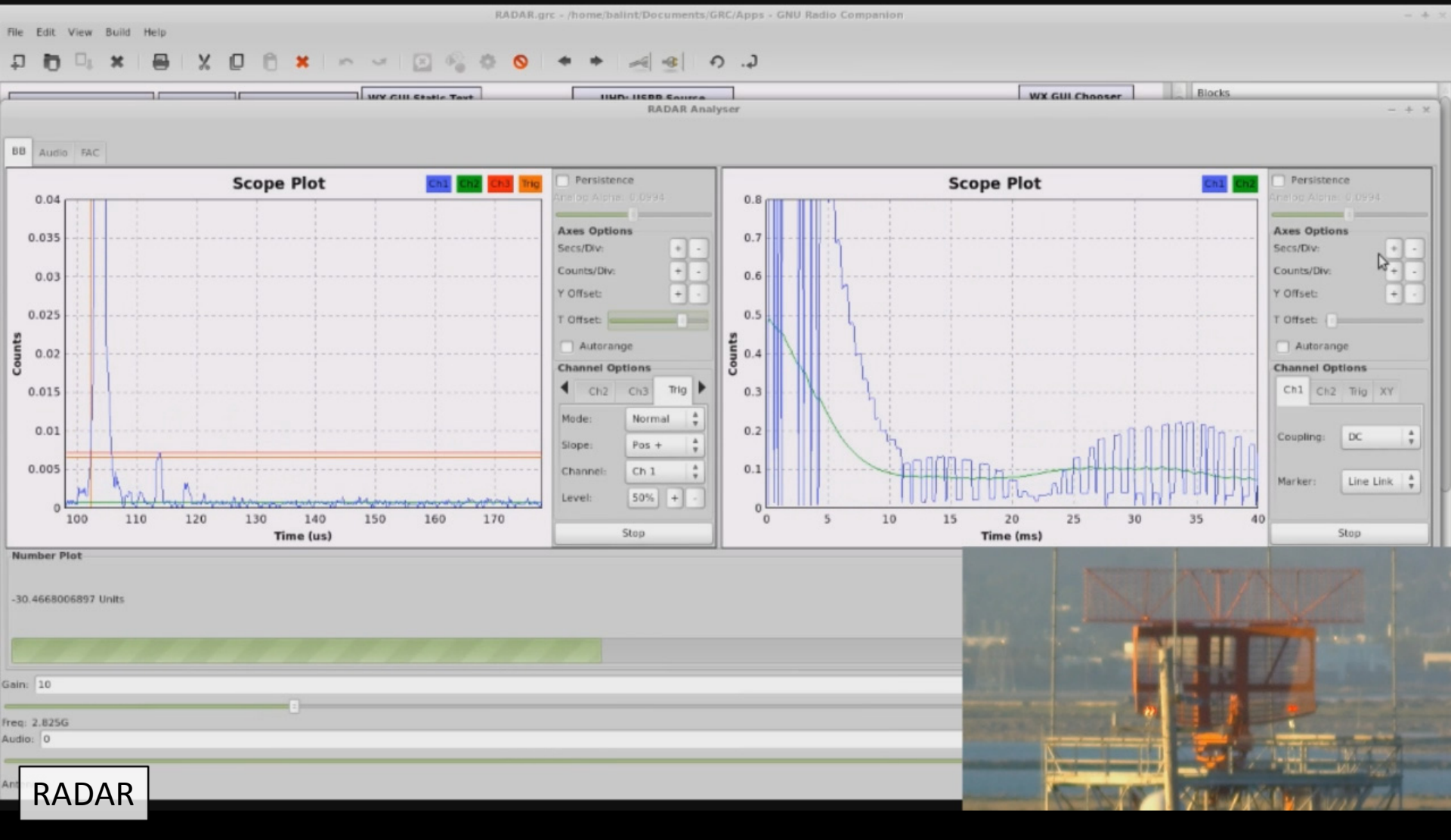
SDR Hardware

Aviation RADAR

Secondary Surveillance: ADS-B/Mode S



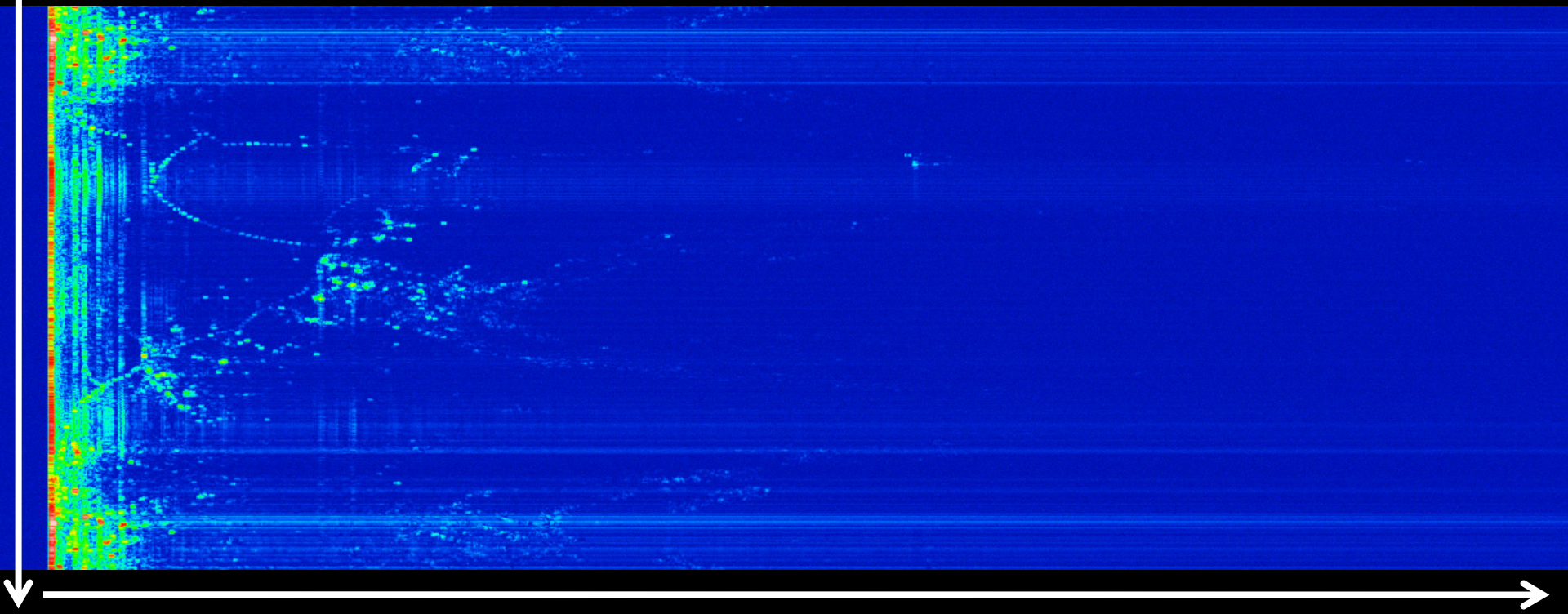
Primary Surveillance RADAR



RADAR

Raw RADAR Return Plot

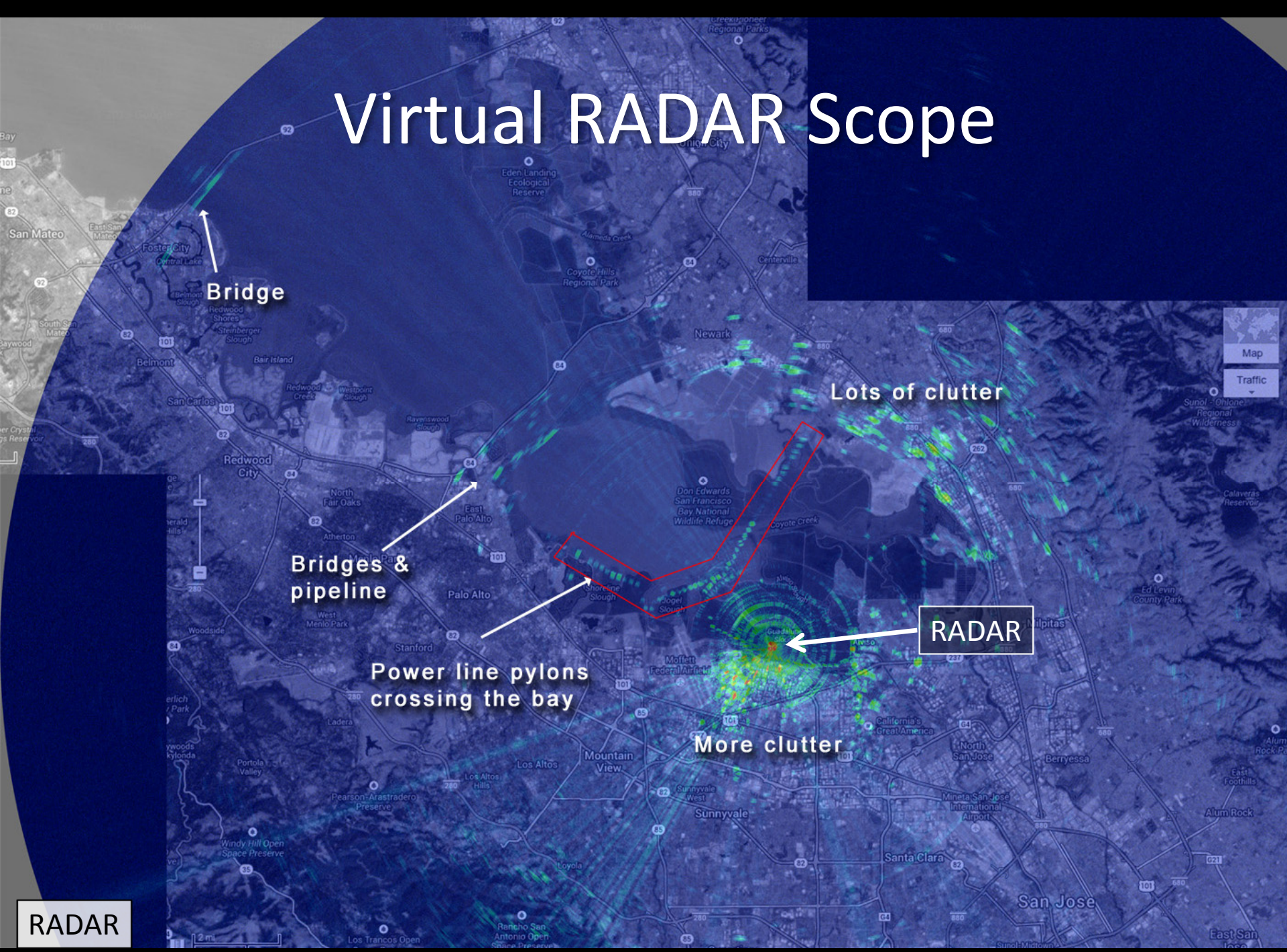
Each scanline is synchronised to an emitted pulse



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

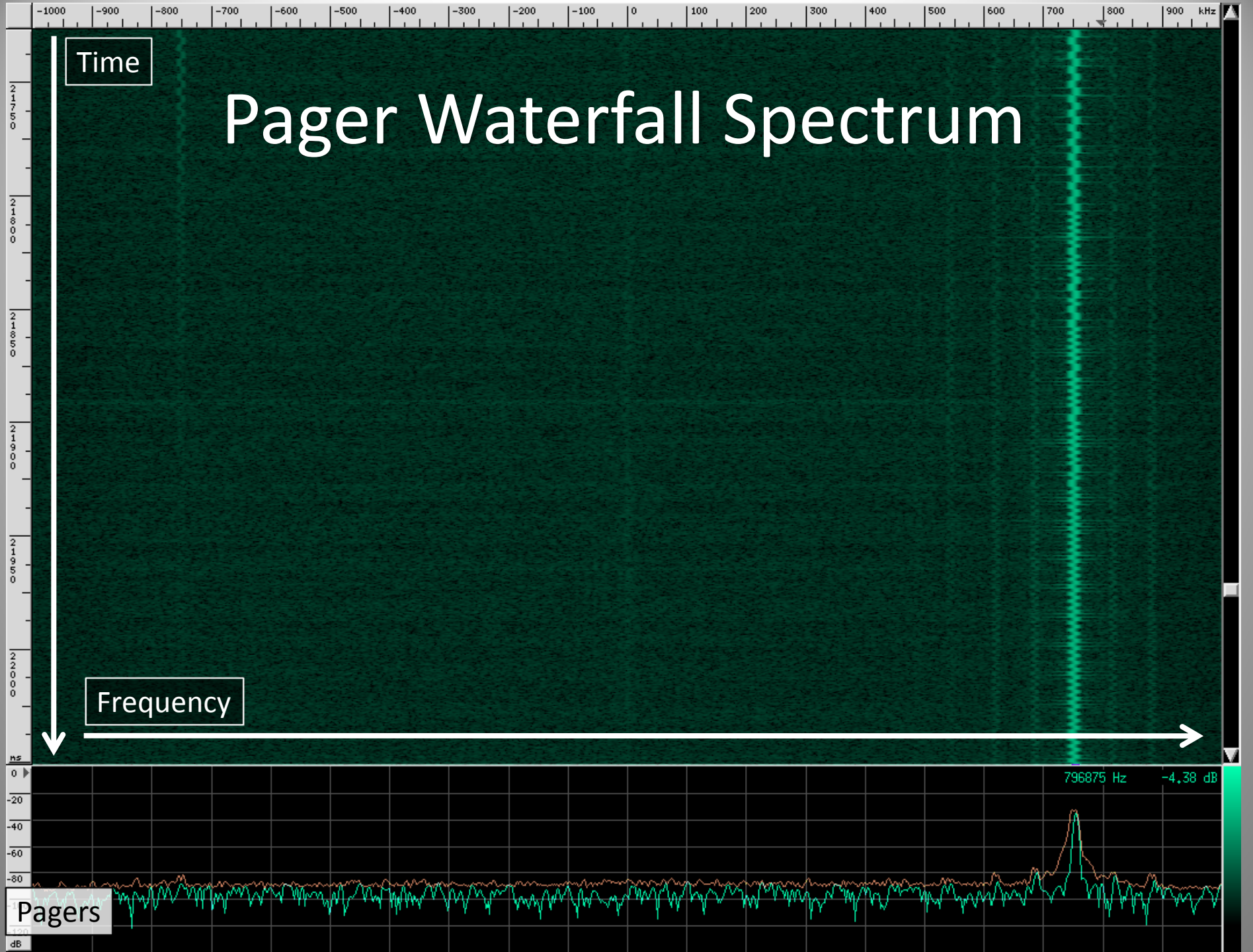
RADAR

Virtual RADAR Scope

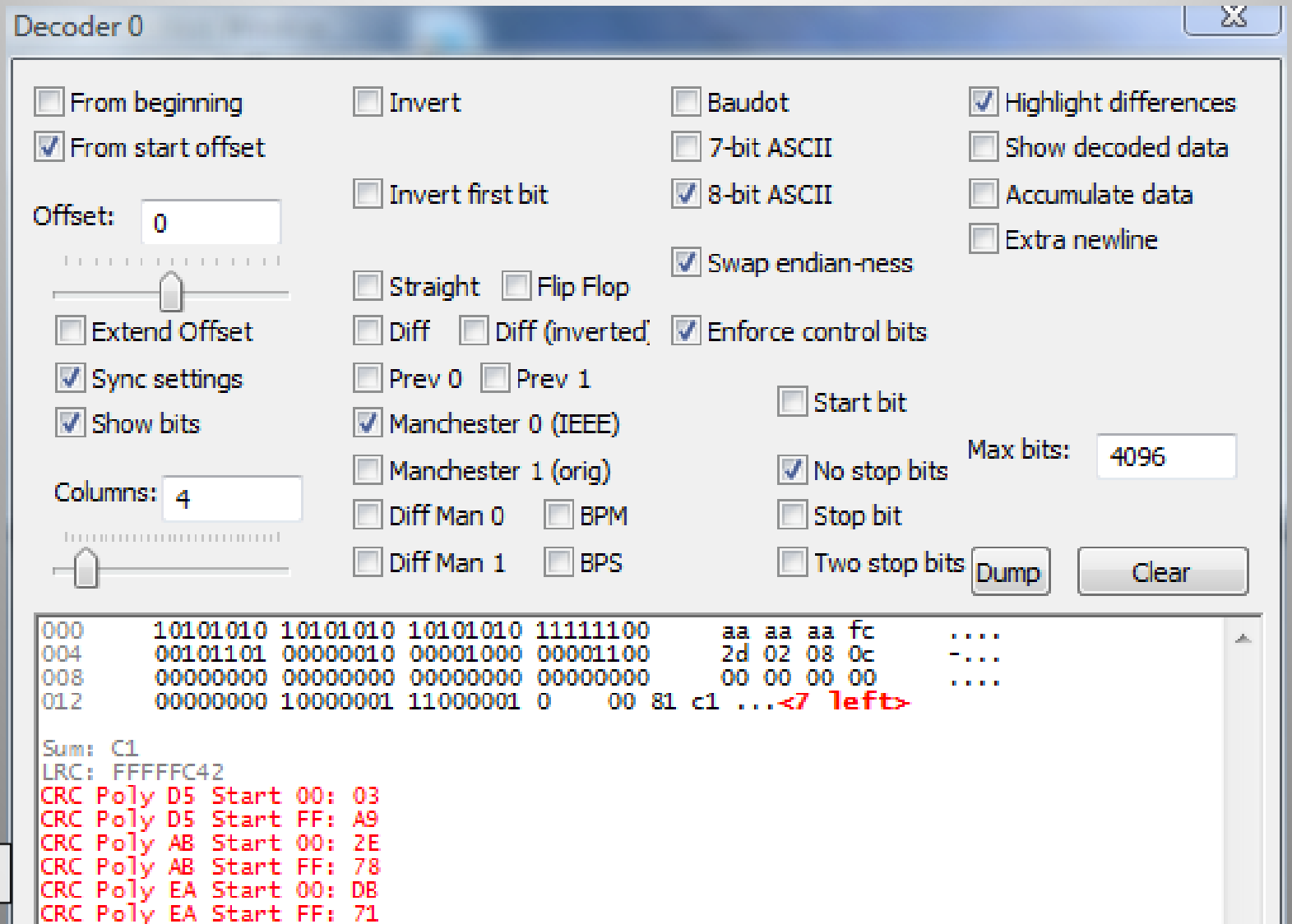


Restaurant Pagers

Pagers

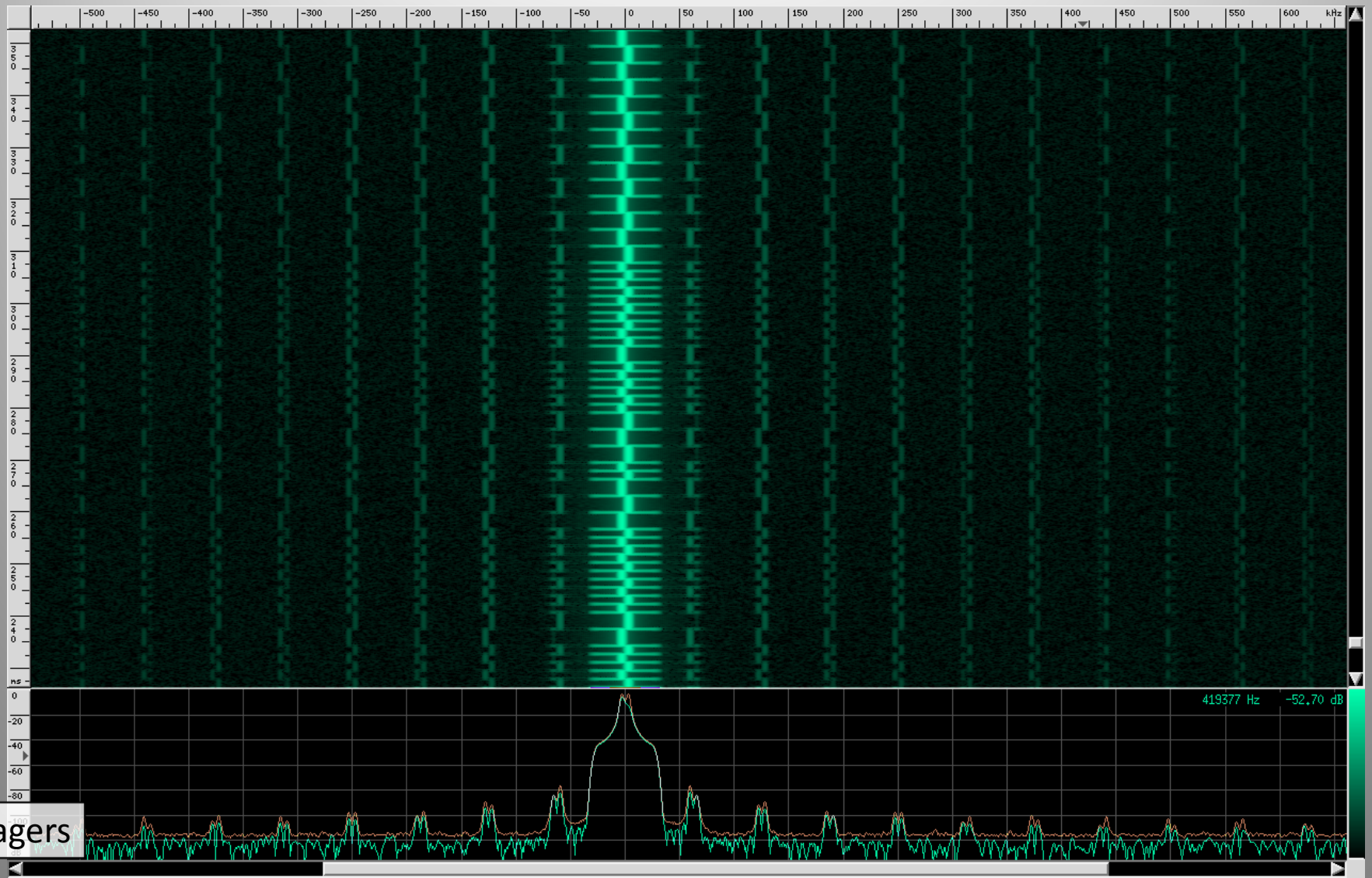

Time
Pager Waterfall Spectrum
Frequency
796875 Hz
-4.38 dB
Pagers

Making sense of raw bits



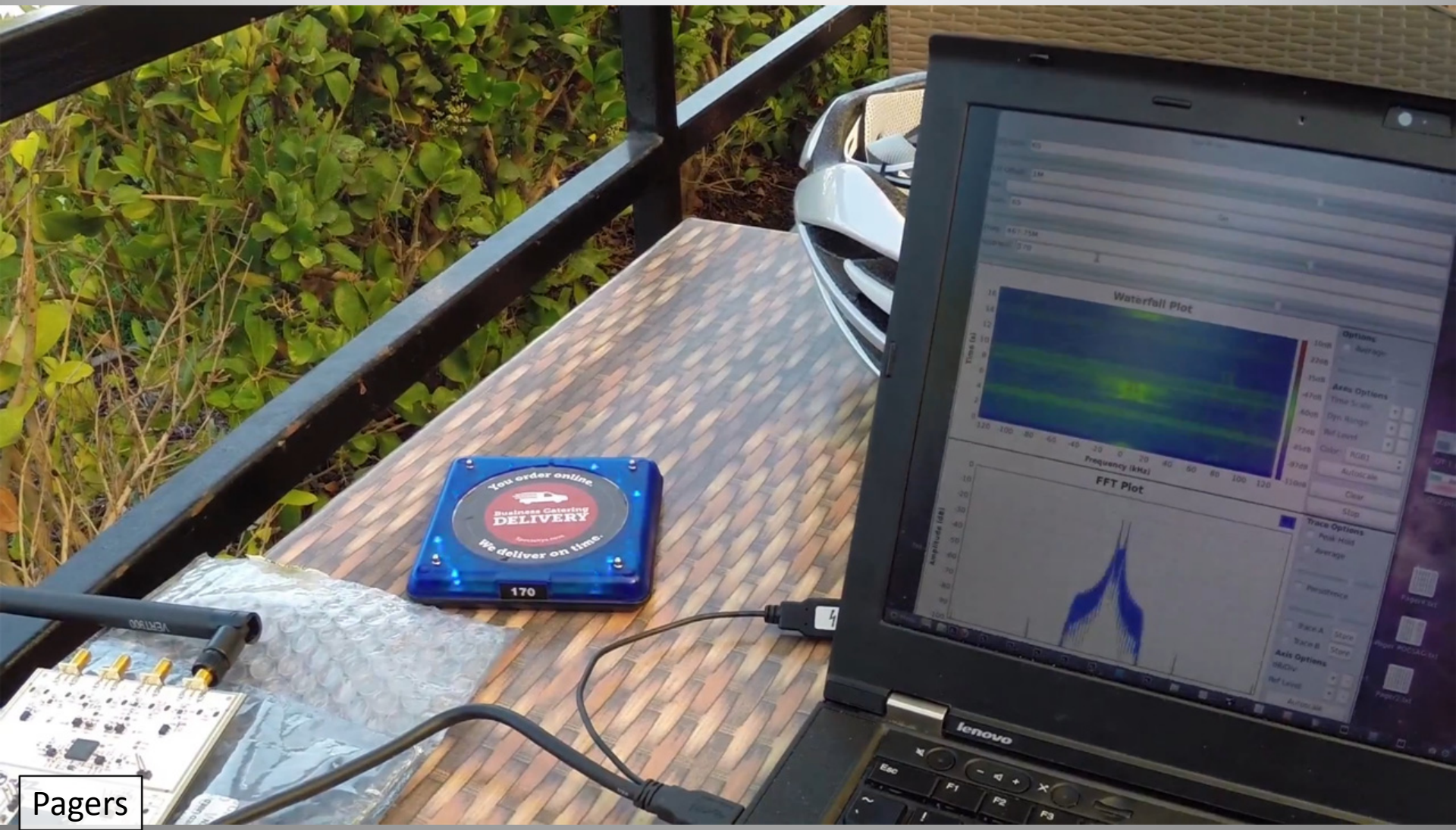
Pagers

Modulator Output



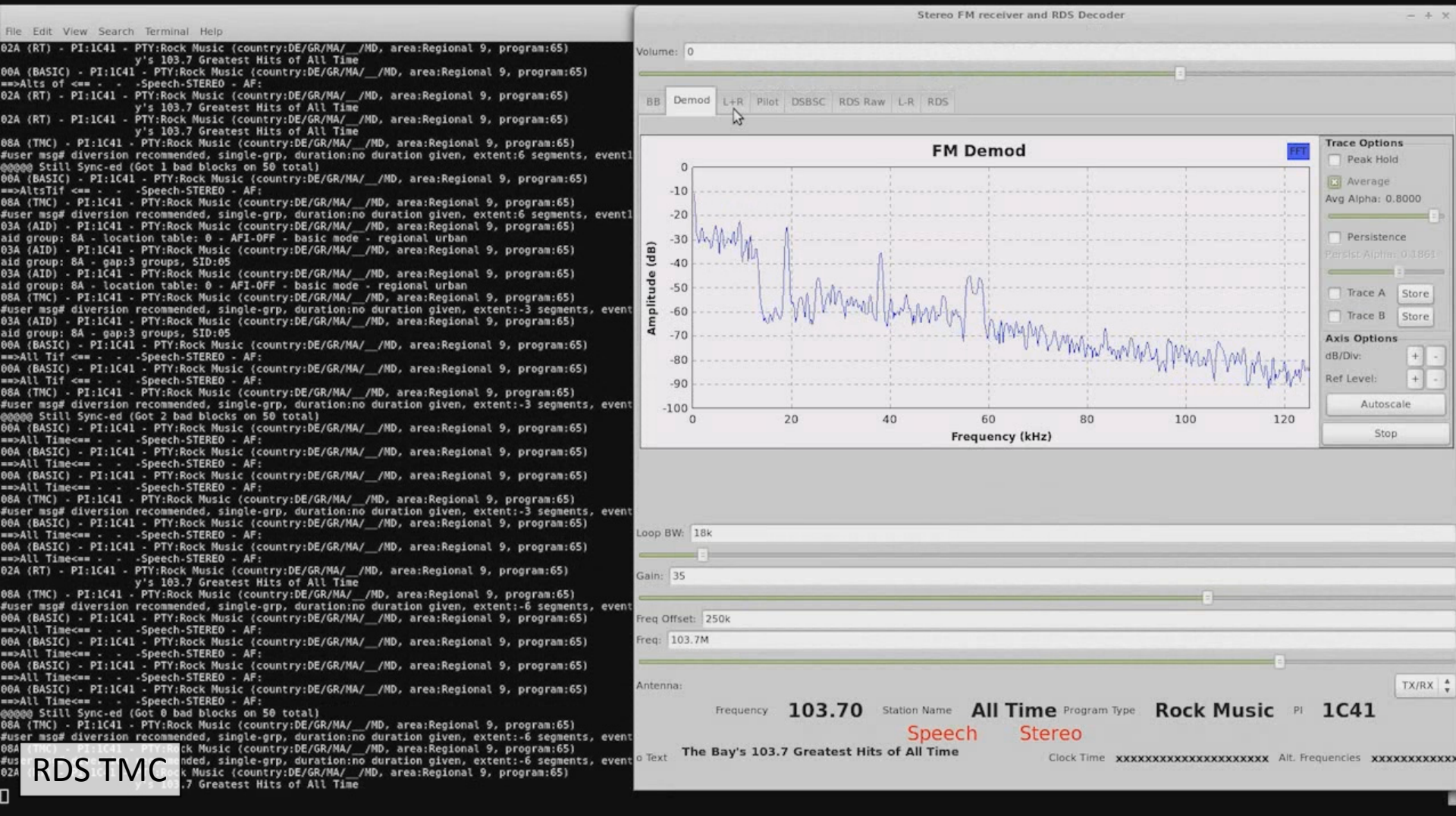
Pagers

Pager Spoofing



Pagers

RDS Traffic Message Channel



RDS TMC

Compare Against Trusted Source

RDS TMC

Brute Force Search

```
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
```

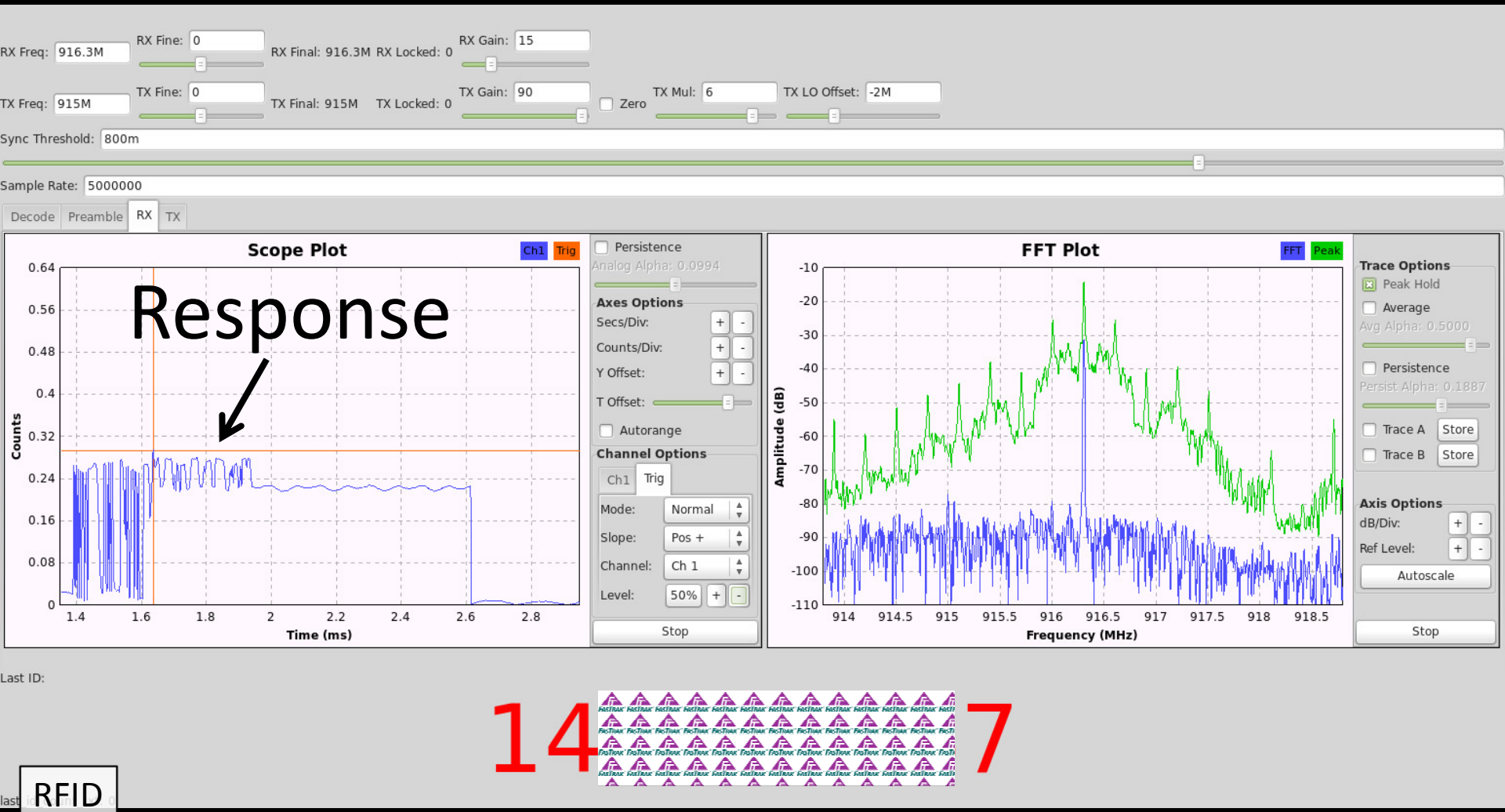
```
Encryption ID   2 has       2 possible keys
Encryption ID   3 has      15 possible keys
Encryption ID   4 has       5 possible keys
Encryption ID   5 has       4 possible keys
Encryption ID   6 has       3 possible keys
Encryption ID   7 has       5 possible keys
Encryption ID   8 has       7 possible keys
Encryption ID   9 has       2 possible keys
Encryption ID  10 has      34 possible keys
Encryption ID  11 has       1 possible keys
[redacted]
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
[redacted]
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
[redacted]
Encryption ID  30 has       2 possible keys
Encryption ID  31 has       4 possible keys
```

RDS TMC

Reading a FasTrak Toll Tag

RFID

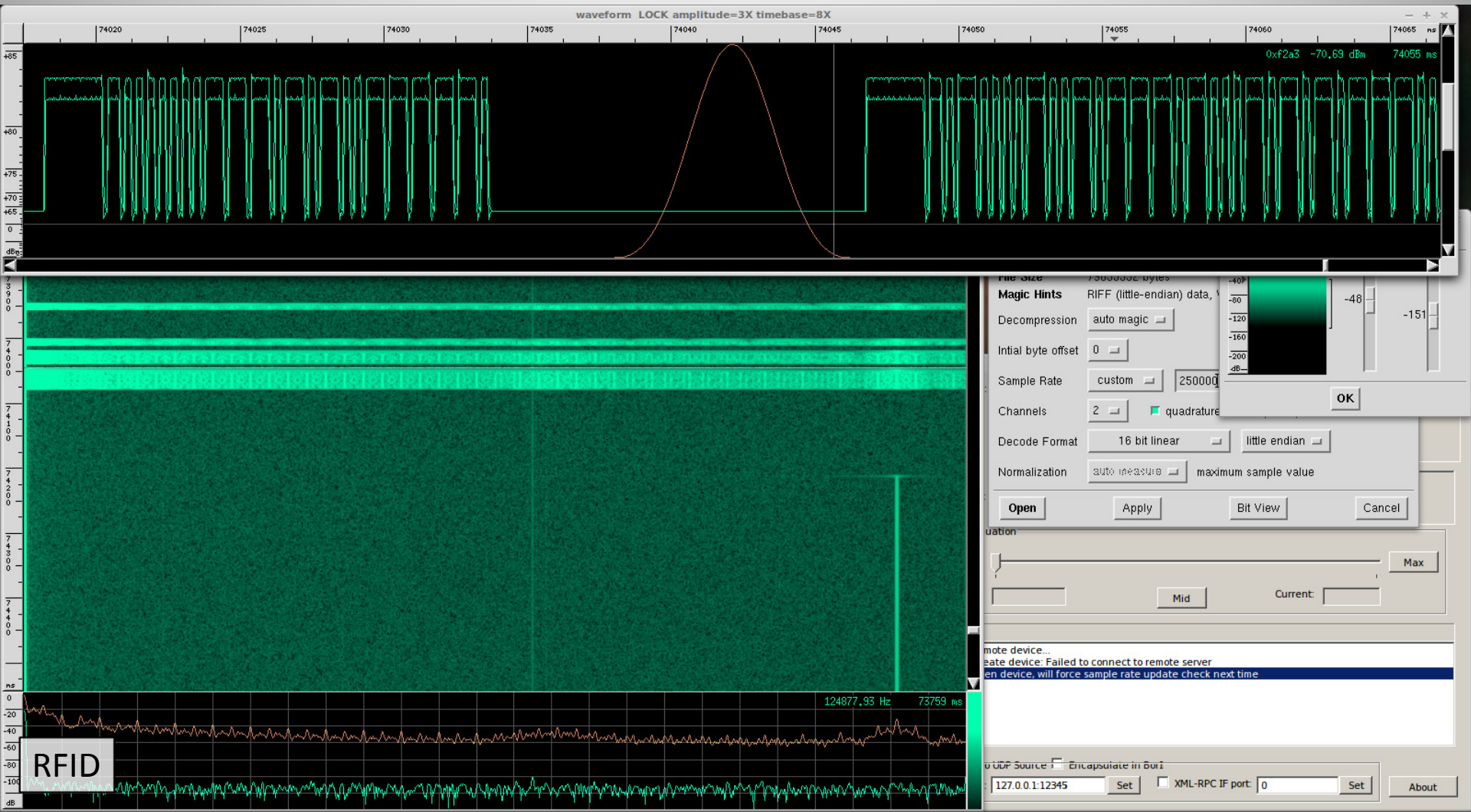
Received Signal



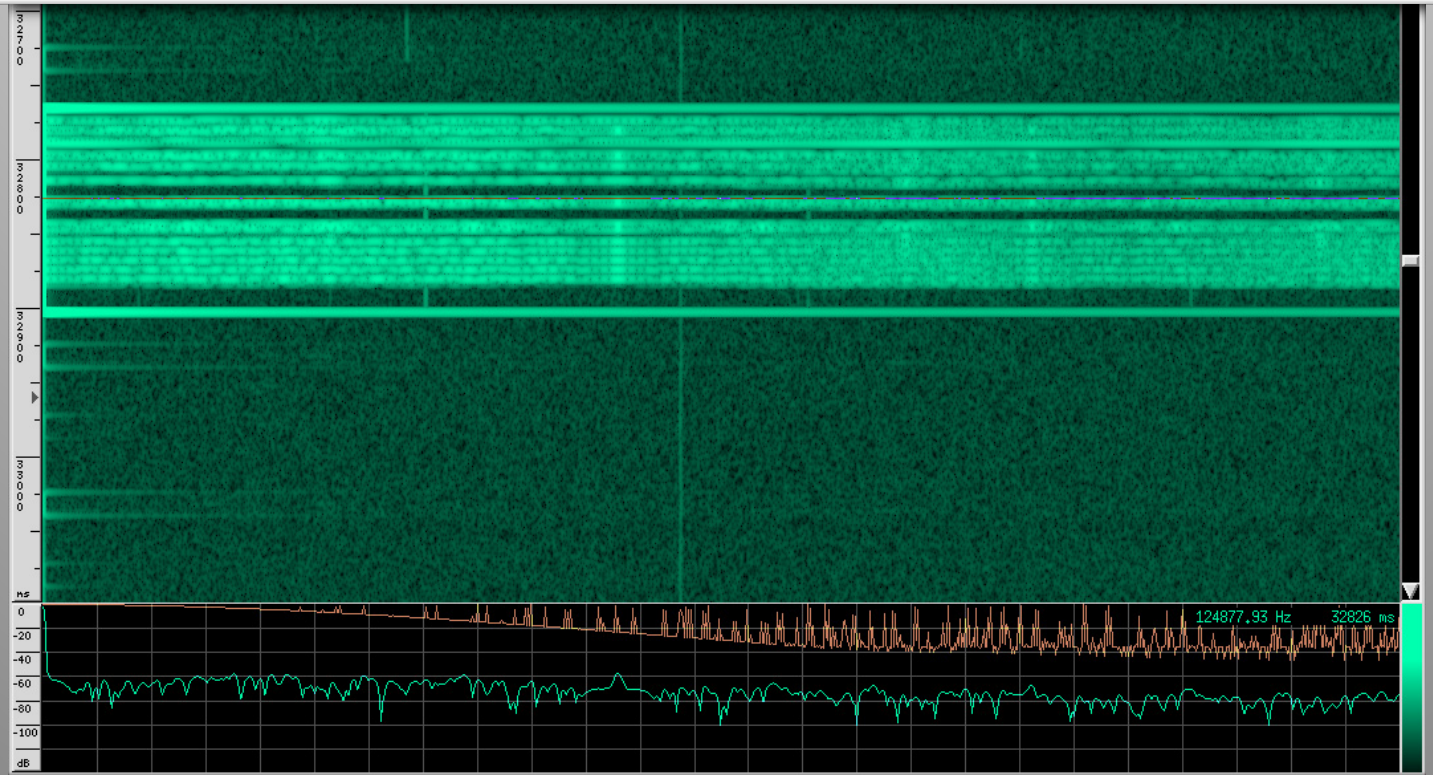
Reading a Tag Outside

RFID

Toyota Prius Keyless Entry Auth



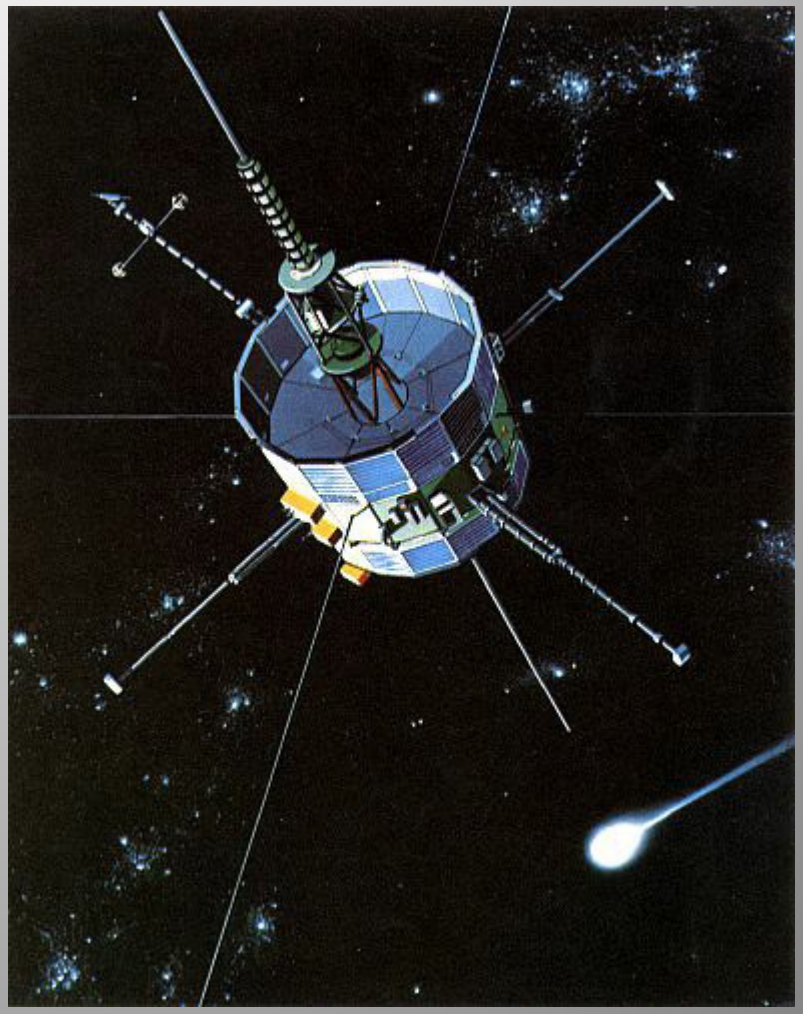
Building Security Badge Auth



RFID

ISEE-3 Reboot Project

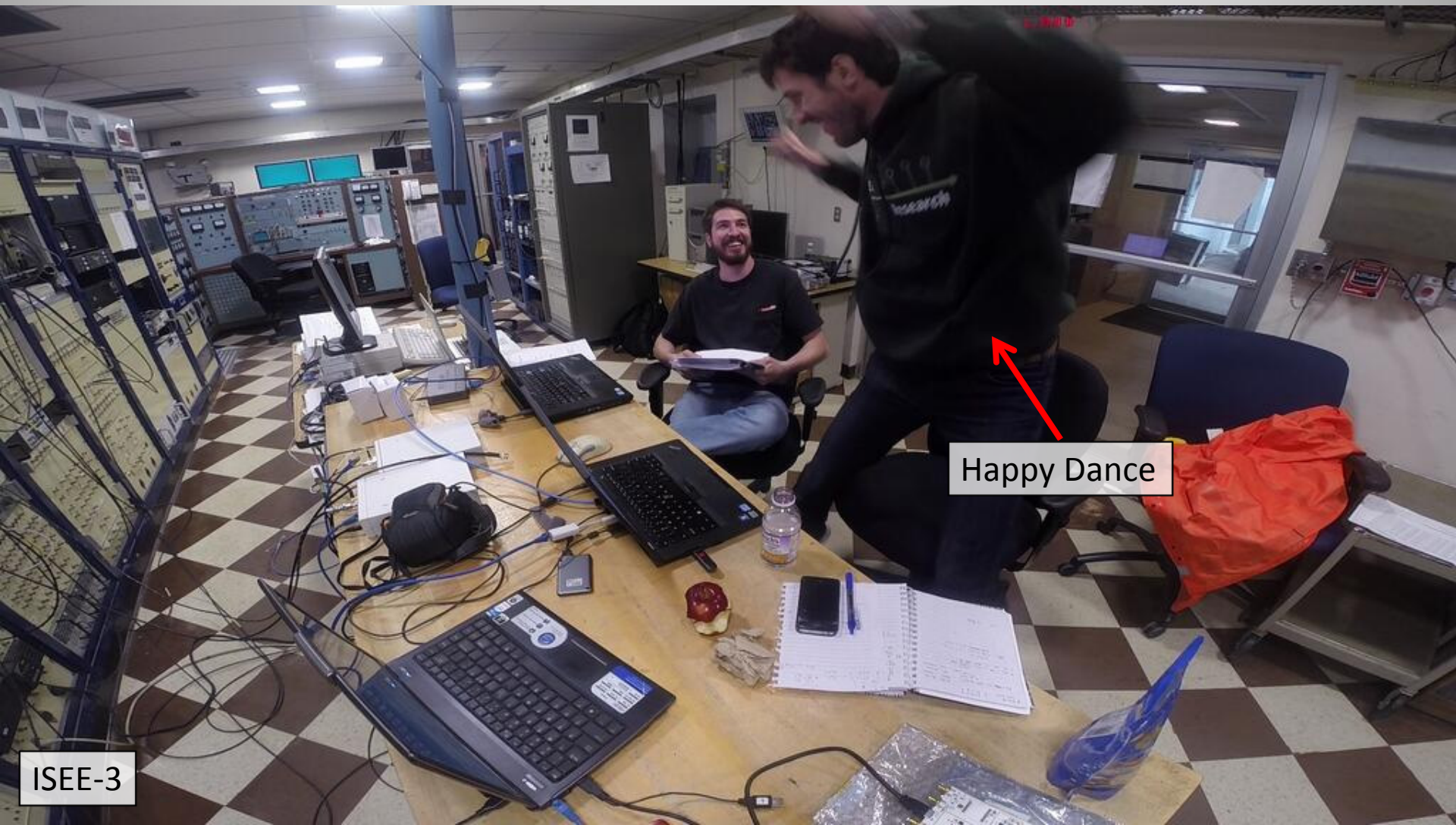
- **I**nternational **S**un/**E**arth **E**xplorer 3
- Launched: August 12, 1978
- Heliocentric Orbit
- Study interaction between solar wind and Earth's magnetic field



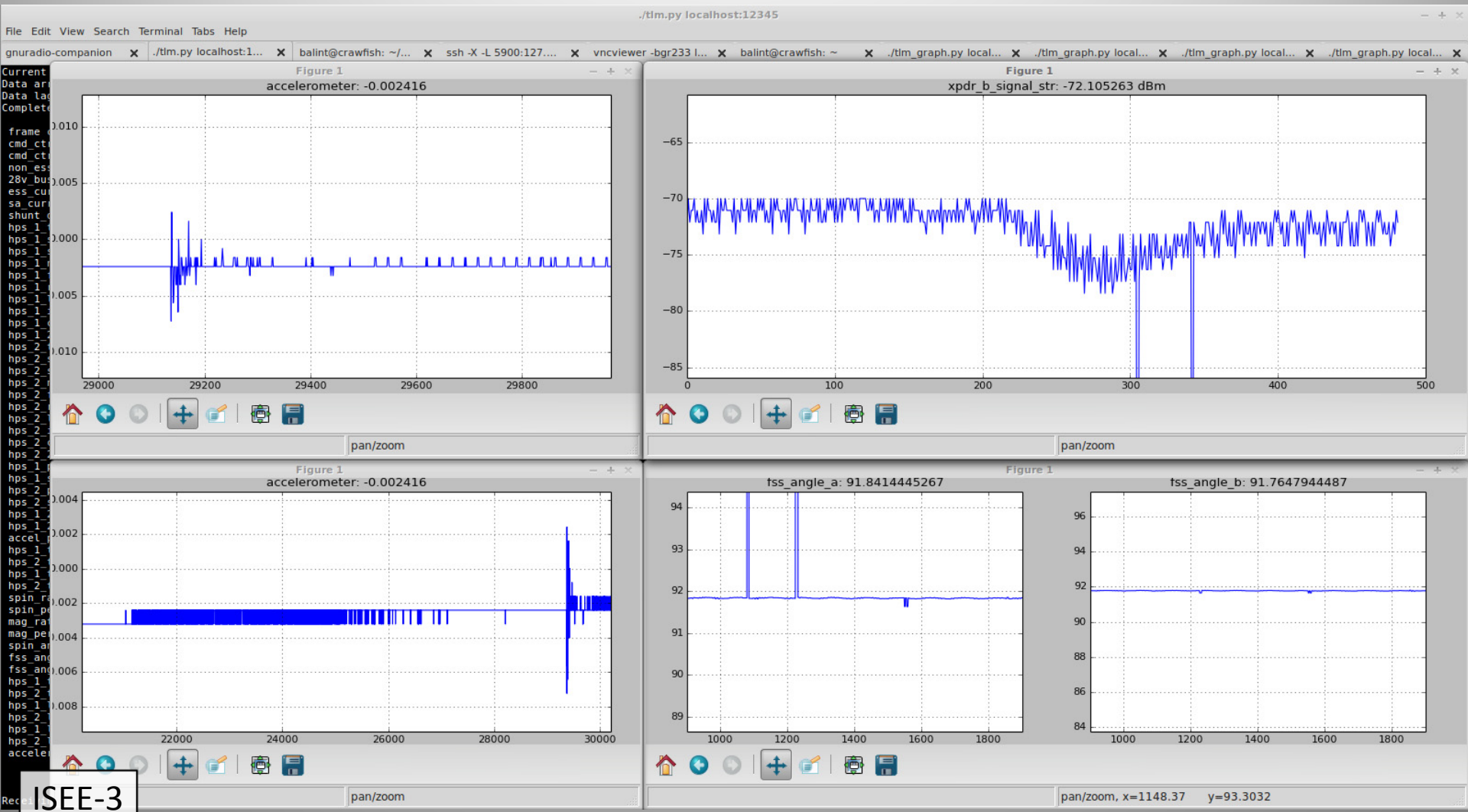
ISEE-3


ISEE-3

Moment of First Contact



Telemetry During Thruster Firing



ISEE-3


http://wiki.spench.net/wiki/RF
http://spench.net/
GitHub: balint256
balint@spench.net
balint@ettus.com
@spenchdotnet