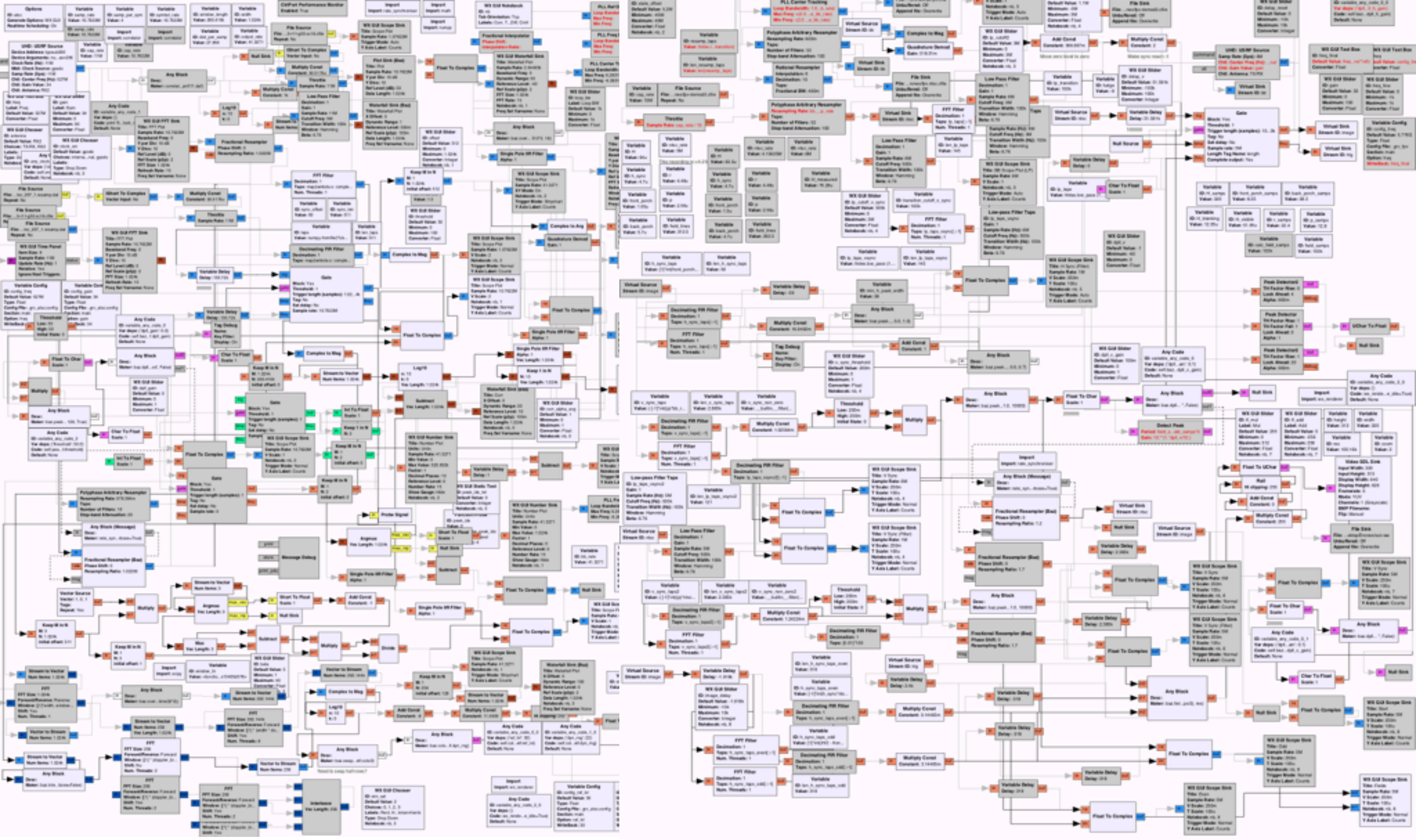
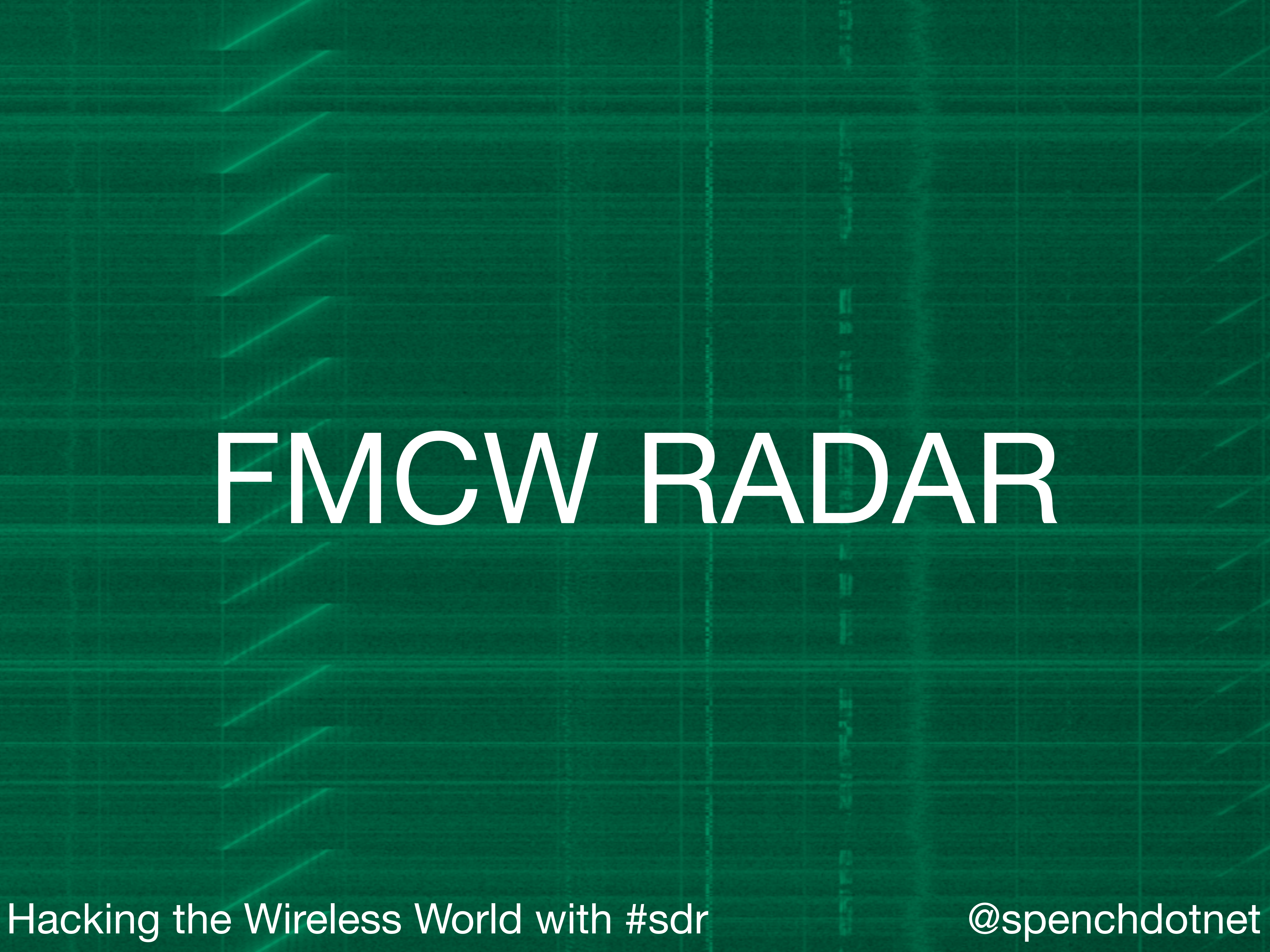


Hacking the Wireless World: Software Defined Radio Exploits

Balint Seeber
Director of Vulnerability Research
Bastille

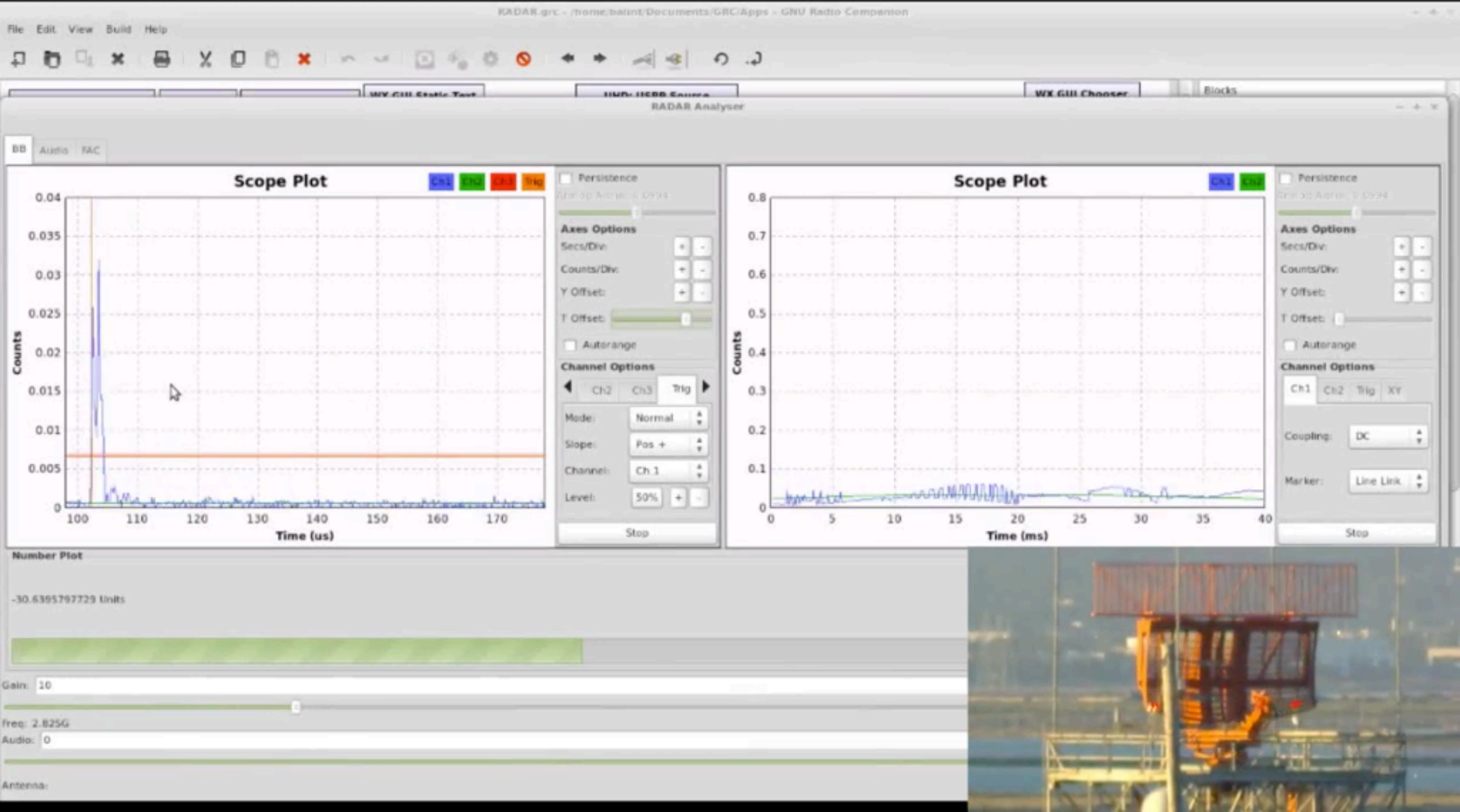
Overview

- FMCW & Passive RADAR
- FPV Decoding



FMCW RADAR

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

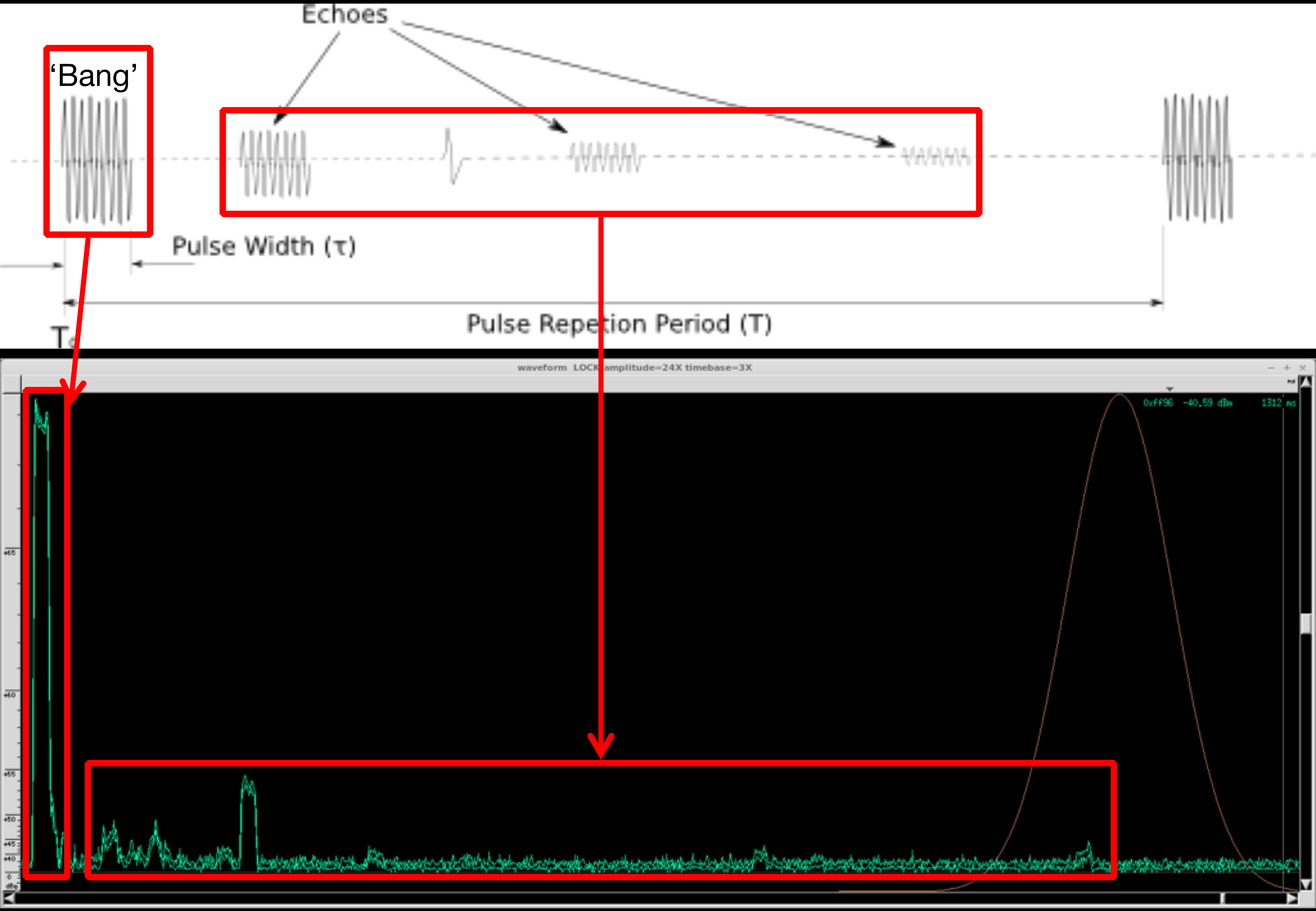


Mode: Normal
Slope: Pos +
Channel: Ch 1
Level: 50%

Coupling: DC
Marker: Line Link

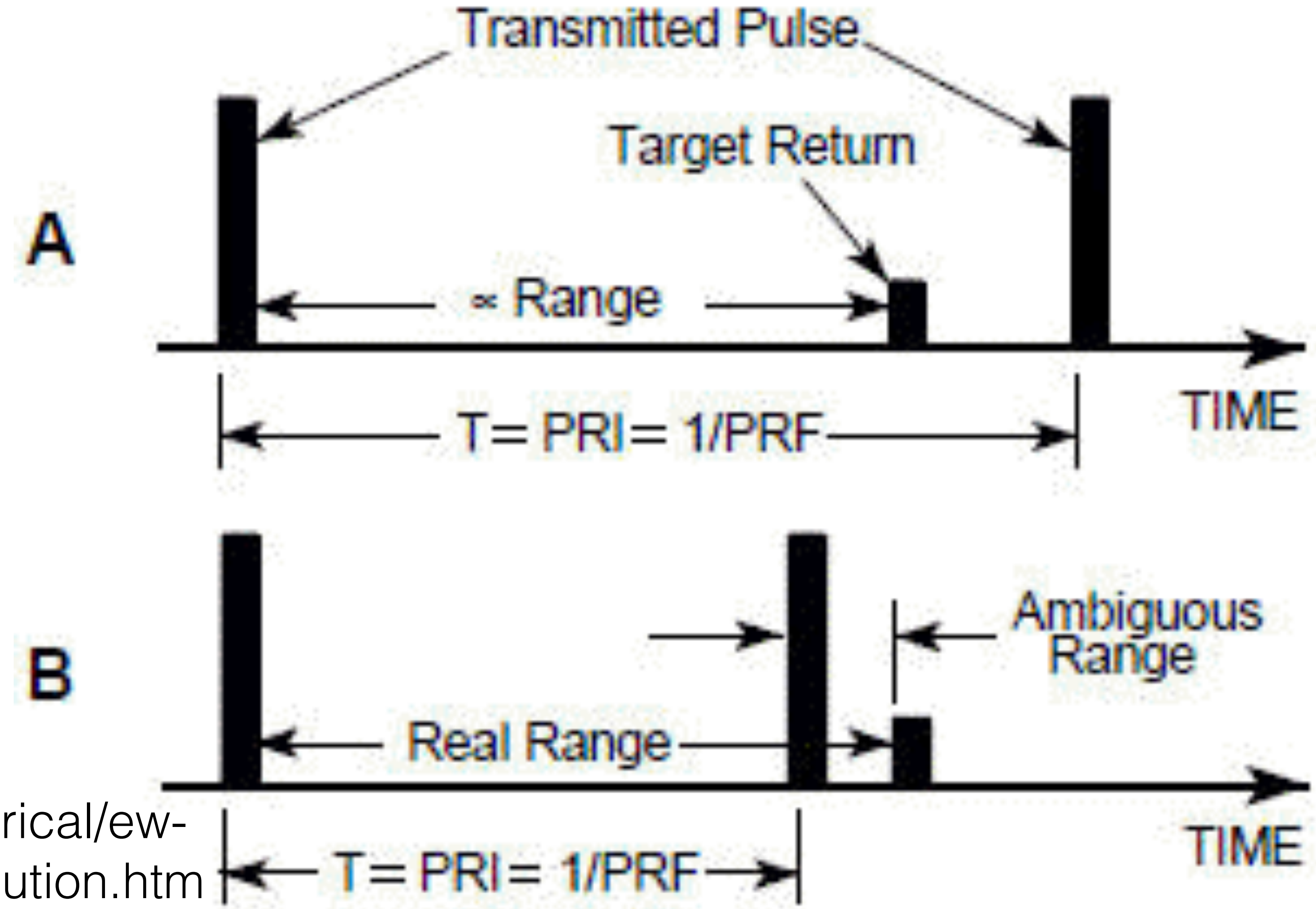
-30.6395797729 Units

Gain: 10
Freq: 2.825G
Audio: 0
Antenna:


'Bang'
Echoes
Pulse Width (τ)
Pulse Repetion Period (T)
T
waveform LOCK amplitude=24X timebase=3X
0xff96 -40.59 dBm
1312 ms
+65
+60
+55
+50
+45
+40
0
dBs

RADAR Range

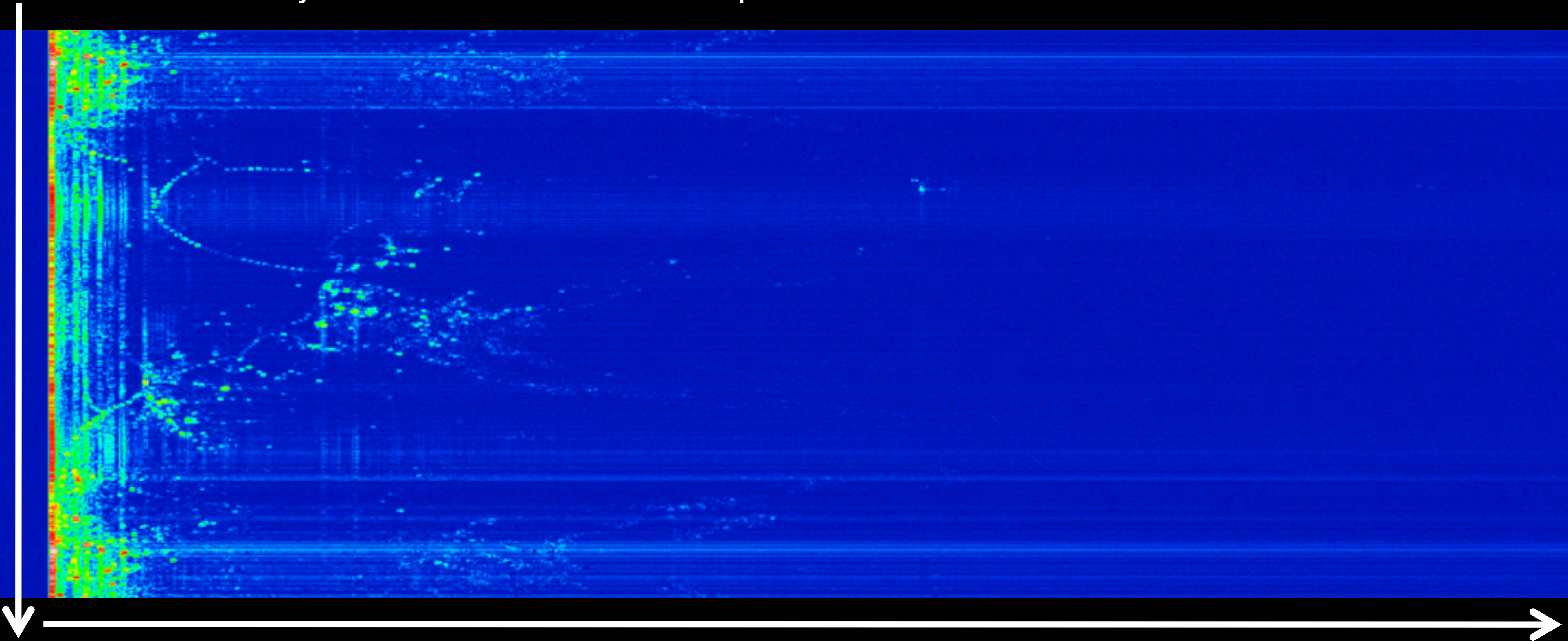
- PRF / PRI: **P**ulse **R**epetition **F**requency / **I**nterval
- Pulse of width TX'd at PRF, switch to RX during idle
- Time delay = RTT
- Range = RTT x c / 2
- **A**: Unambiguous
- **B**: Ambiguous



http://www.rfcafe.com/references/electrical/ew-radar-handbook/propagation-time-resolution.htm

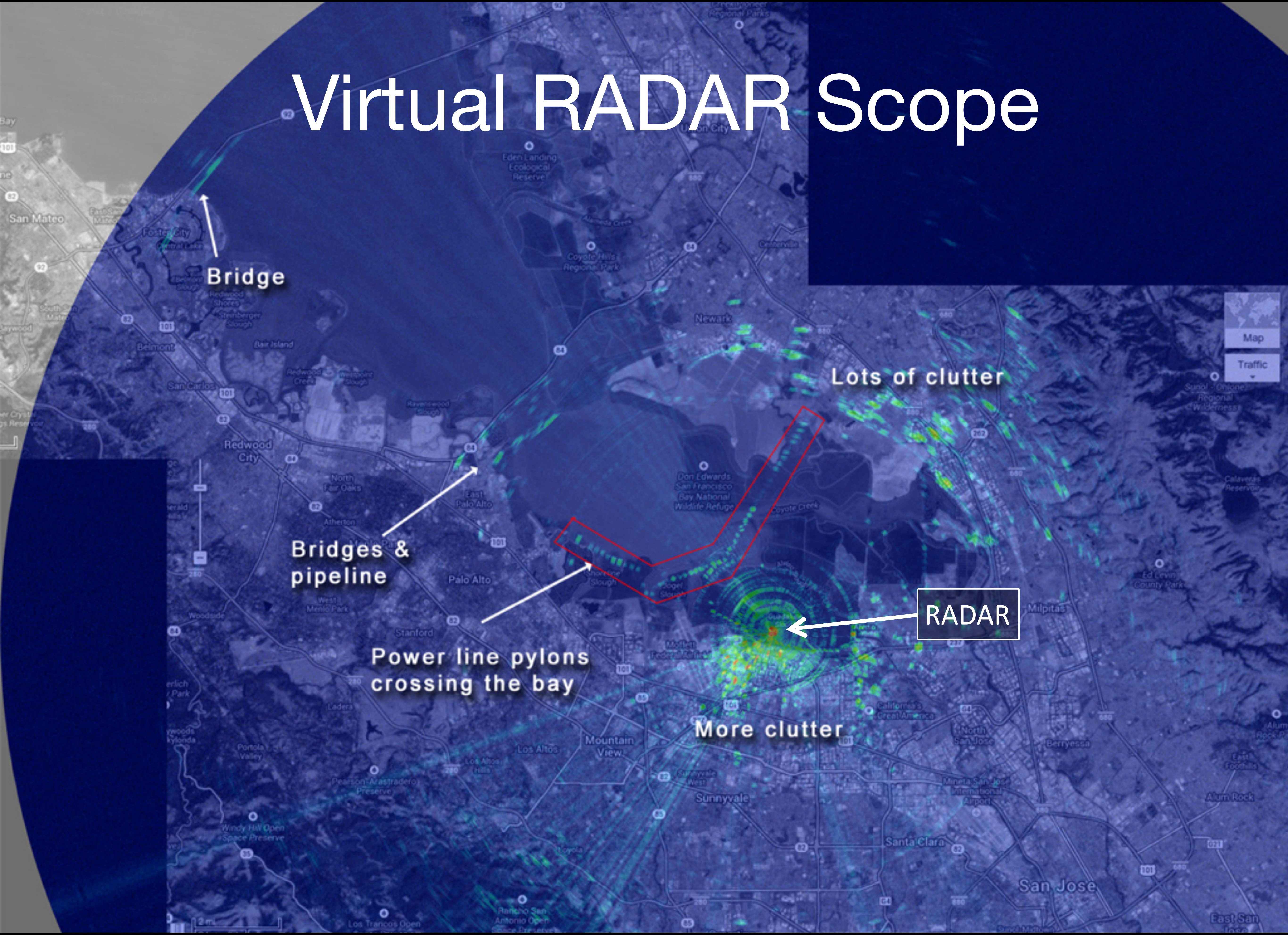
Raw RADAR Return Plot

Each scanline is synchronised to an emitted pulse



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

Virtual RADAR Scope



Bridge

Bridges & pipeline

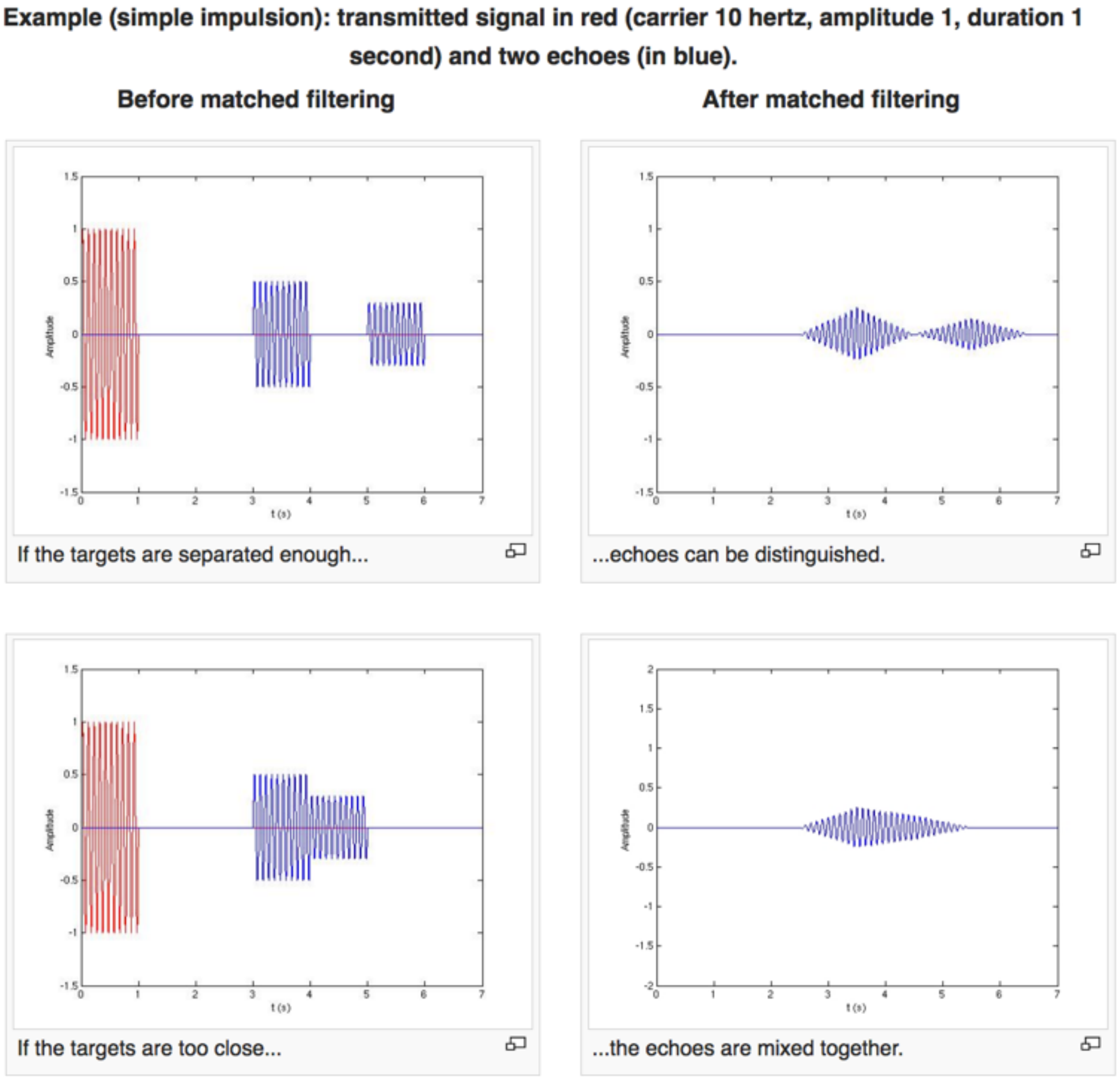
Power line pylons crossing the bay

Lots of clutter

RADAR

More clutter

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



Example (simple impulsion): transmitted signal in red (carrier 10 hertz, amplitude 1, duration 1 second) and two echoes (in blue).

Before matched filtering

After matched filtering

If the targets are separated enough...

...echoes can be distinguished.

If the targets are too close...

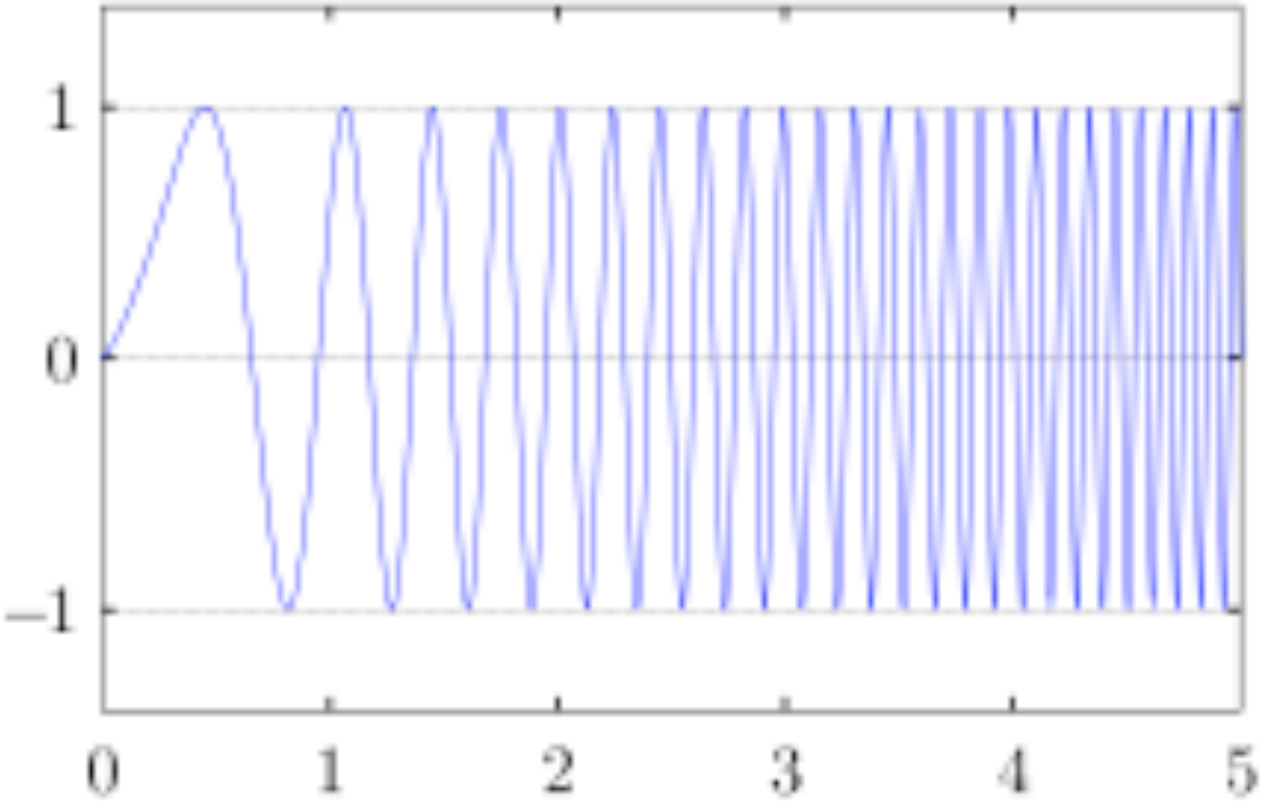
...the echoes are mixed together.

FMCW

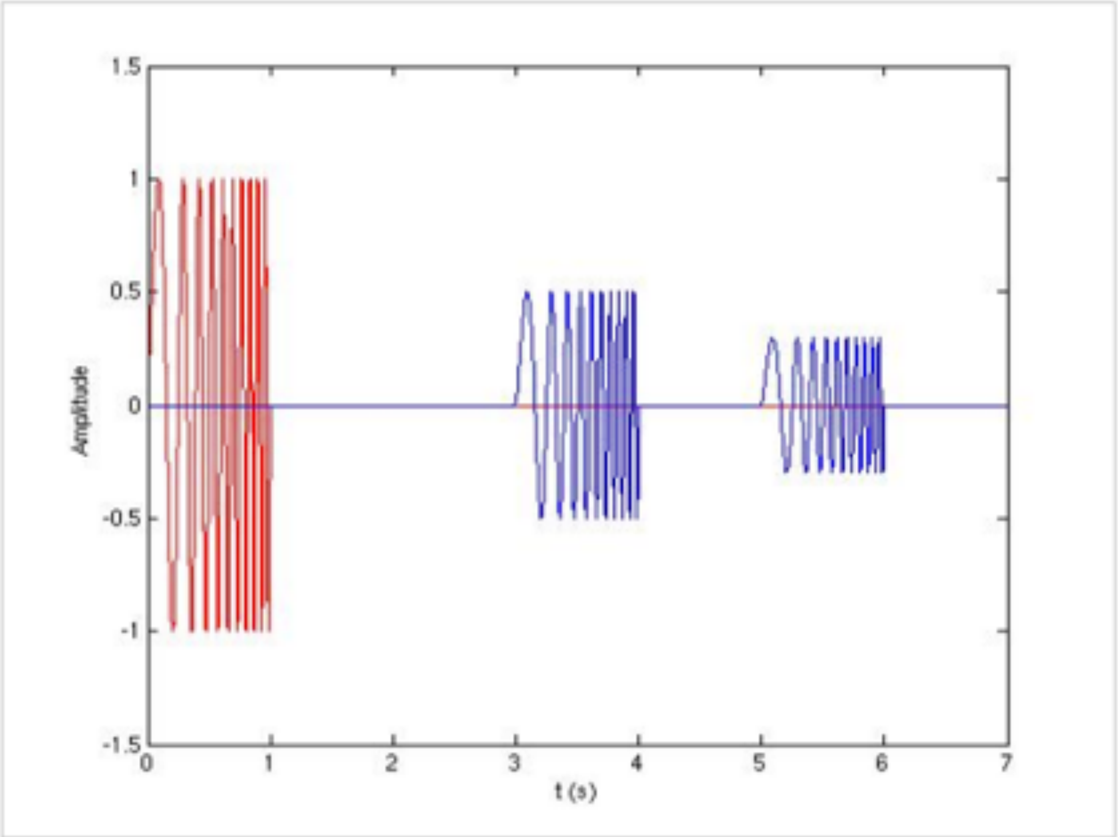
- Transmit a ‘chirp’ (strong self-correlation)

- Can be full TX duty cycle

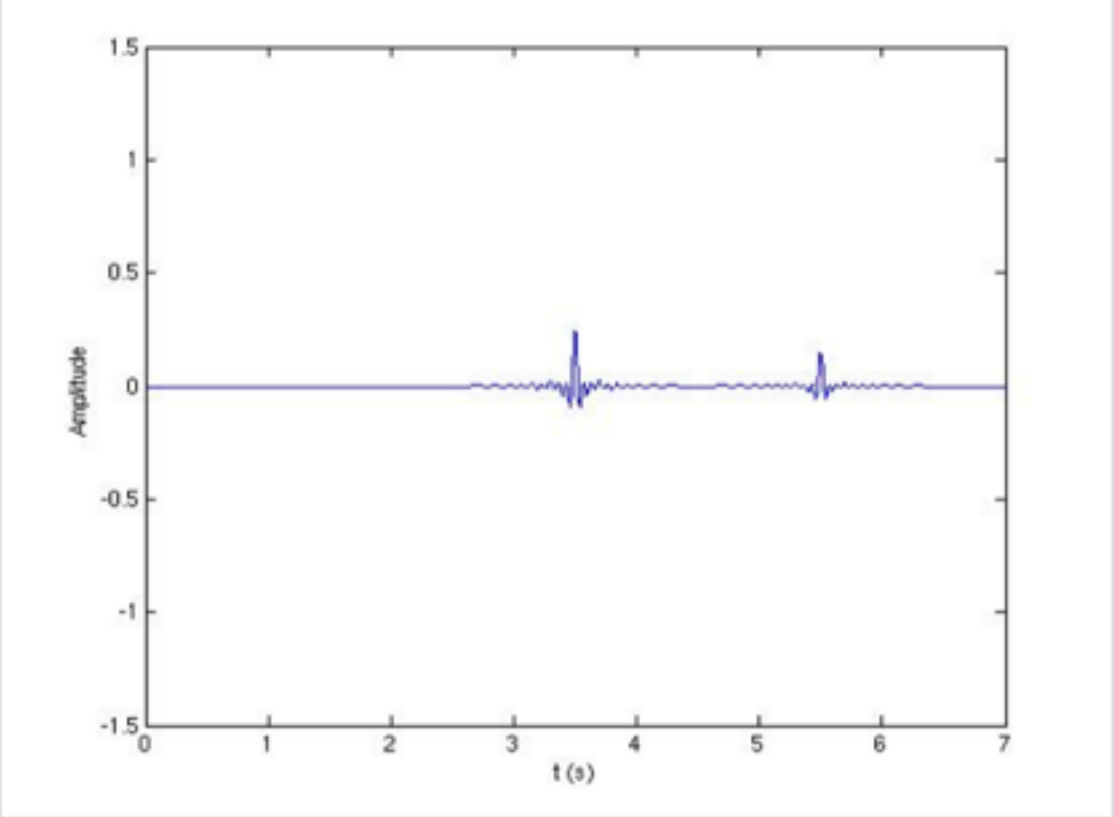
- Think about chirp as a matched filter (not a VCO)
  Filtered result is range information
  like normal CW pulsed echos



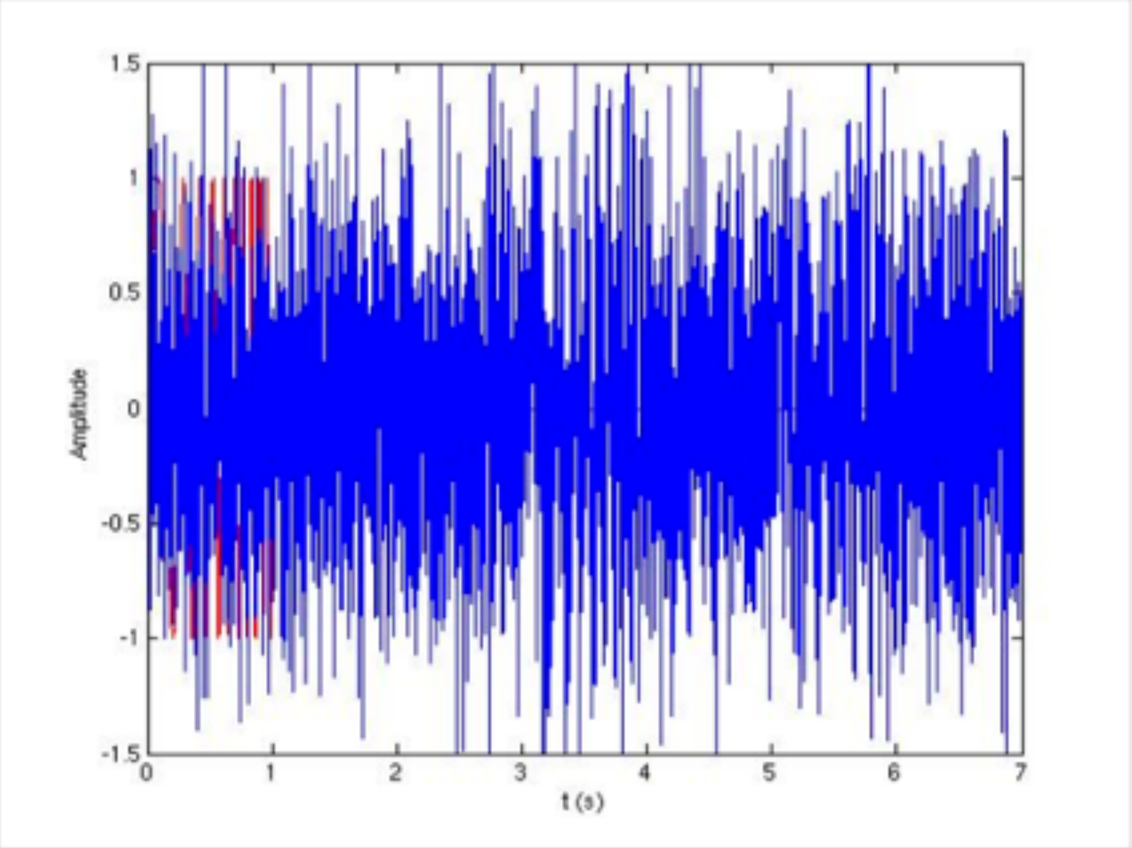
https://en.wikipedia.org/wiki/Pulse_compression



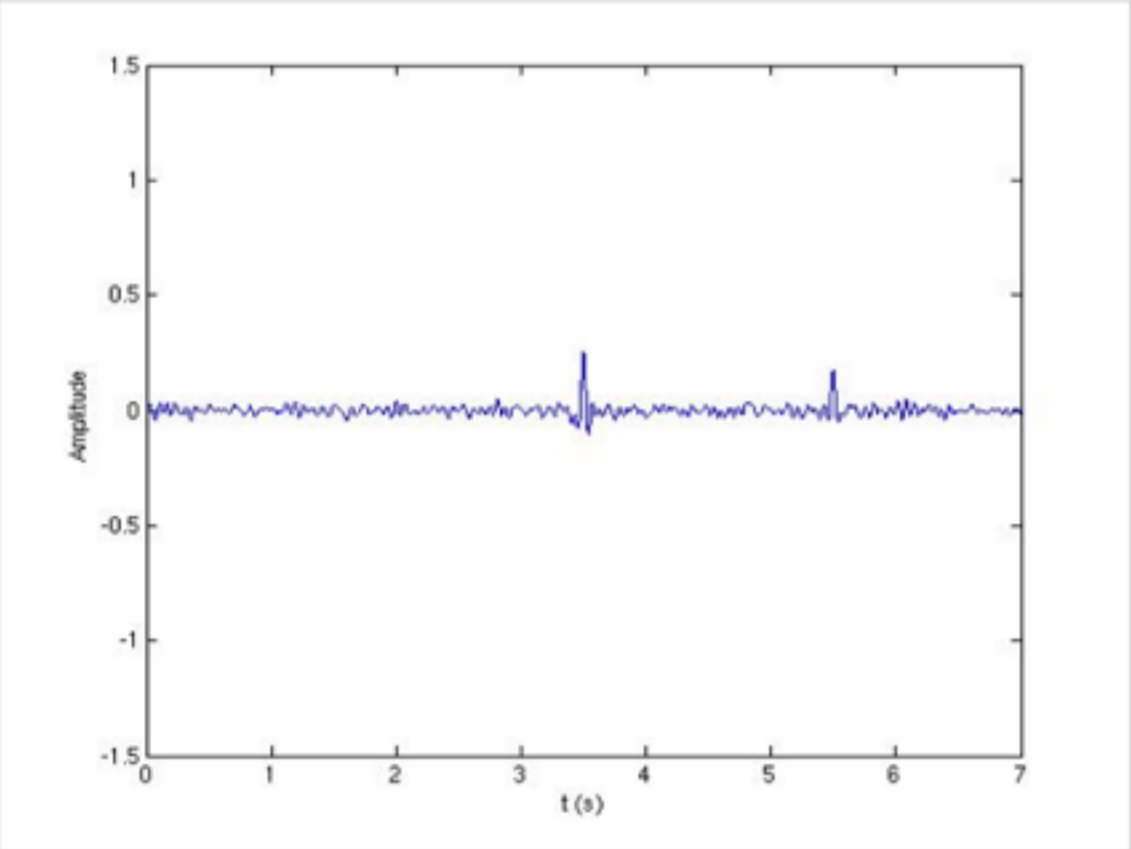
Before matched filtering



After matched filtering: the echoes are shorter in time.

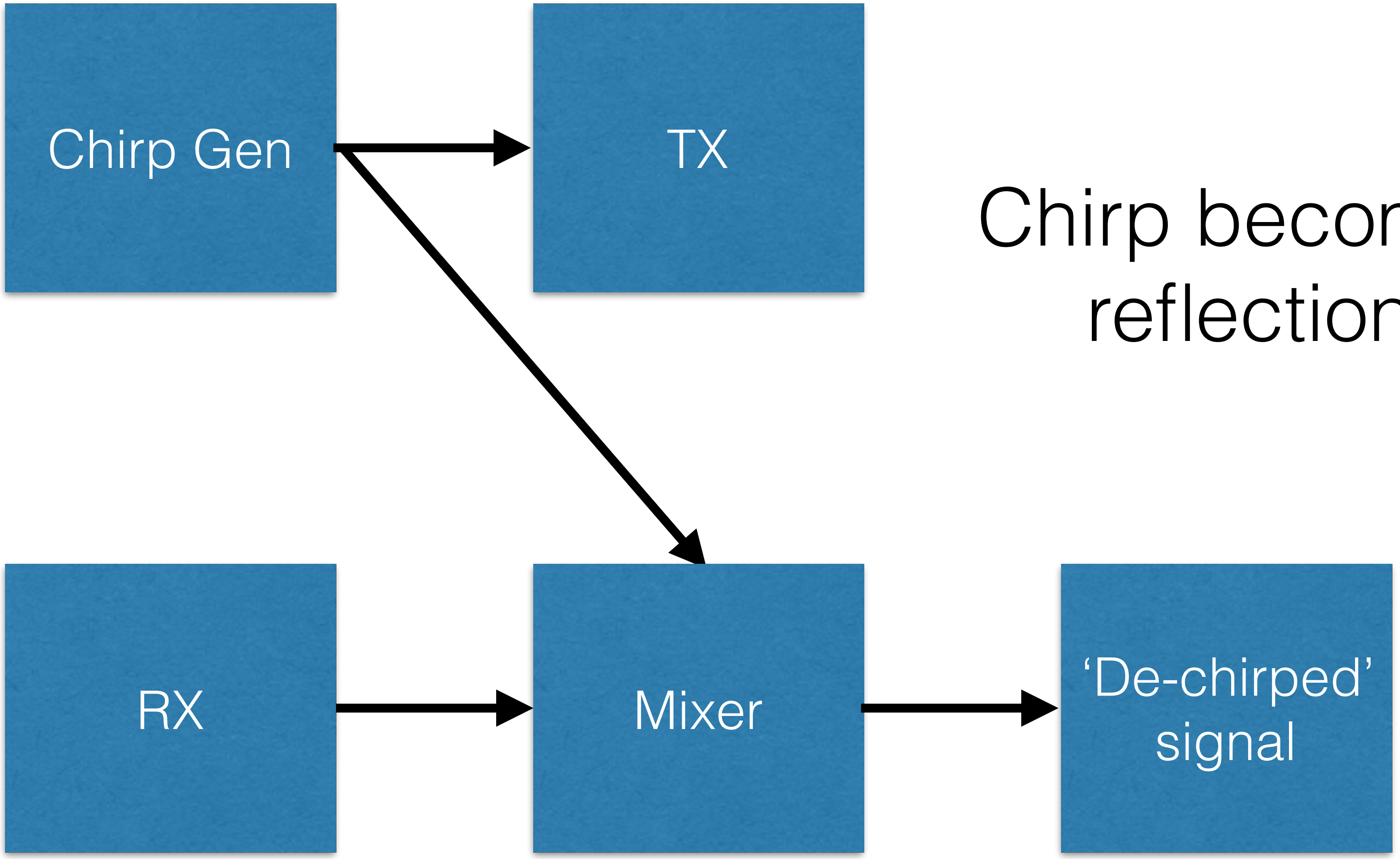


Before matched filtering: the signal is hidden in noise



After matched filtering: echoes become visible.

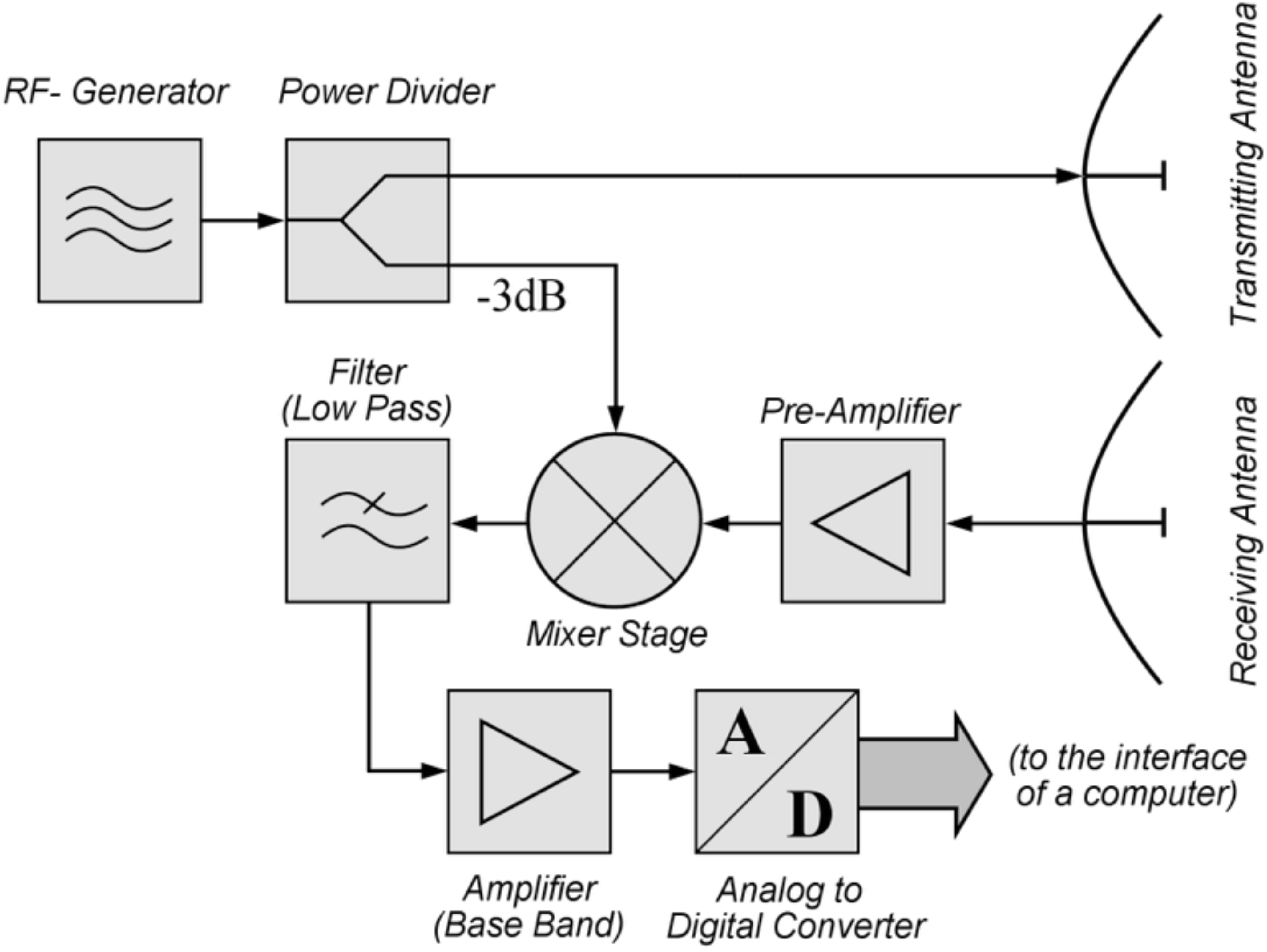
Signal Flow (Continuous / Full Duty Cycle)



Chirp becomes constant tone,
reflections higher tones!

In RF plumbing: can remove locally RX'd TX signal,
only hear echoes (make better use of ADC dynamic range)

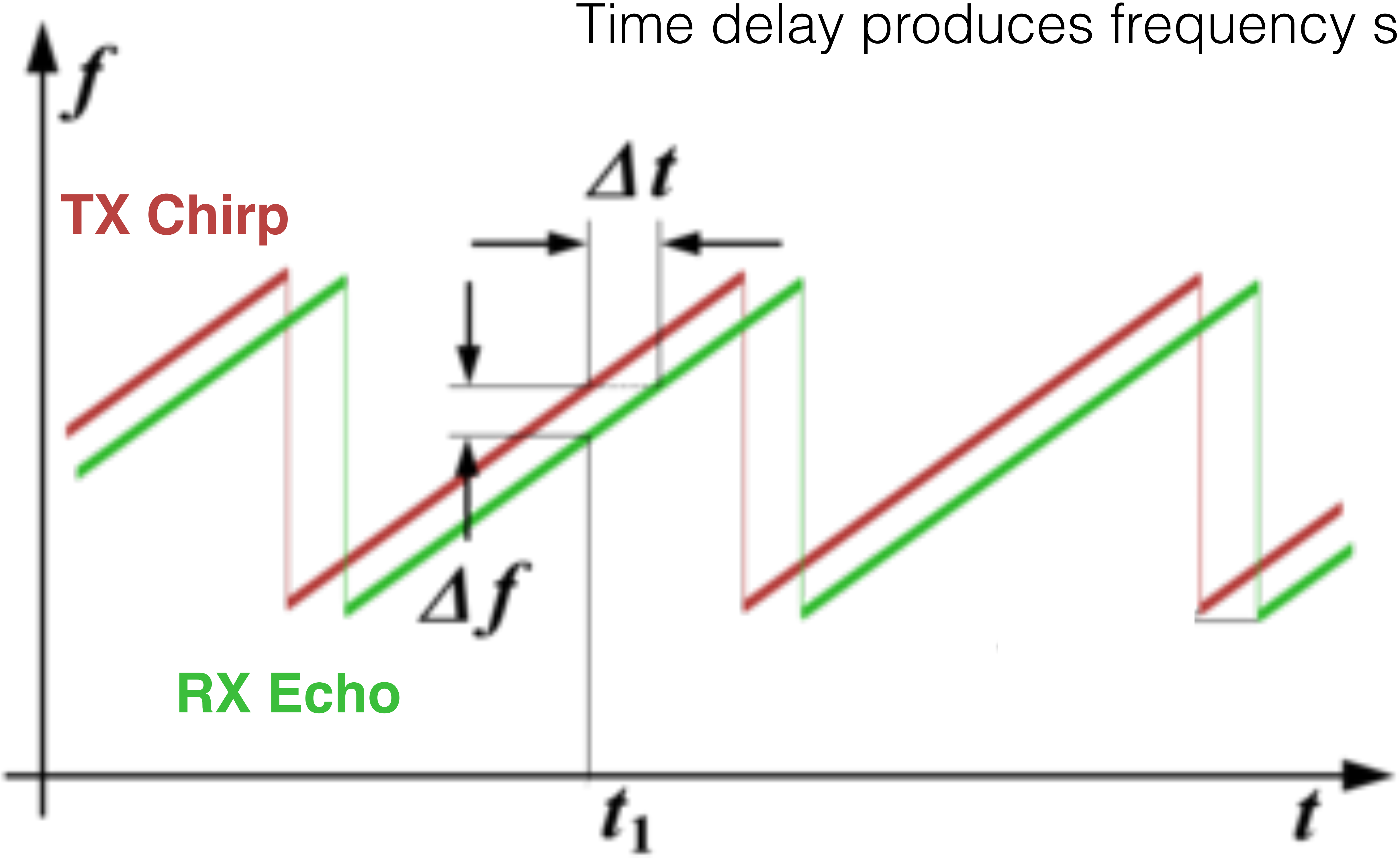
Signal Flow (Continuous / Full Duty Cycle)



https://en.wikipedia.org/wiki/Continuous-wave_radar

FMCW in the Frequency Domain

Time delay produces frequency shift!

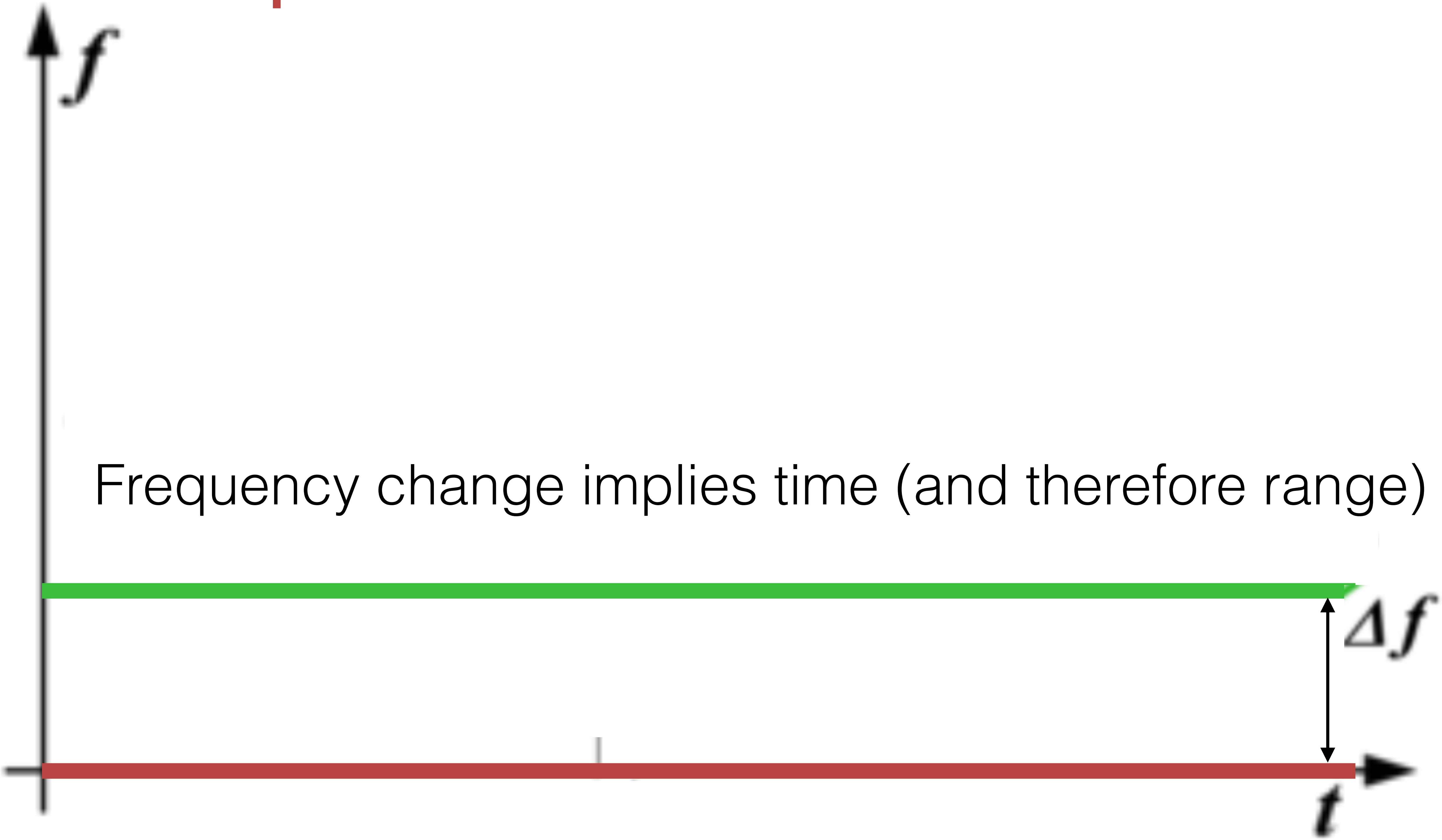


TX Chirp

RX Echo

FMCW in the Frequency Domain (De-chirped)

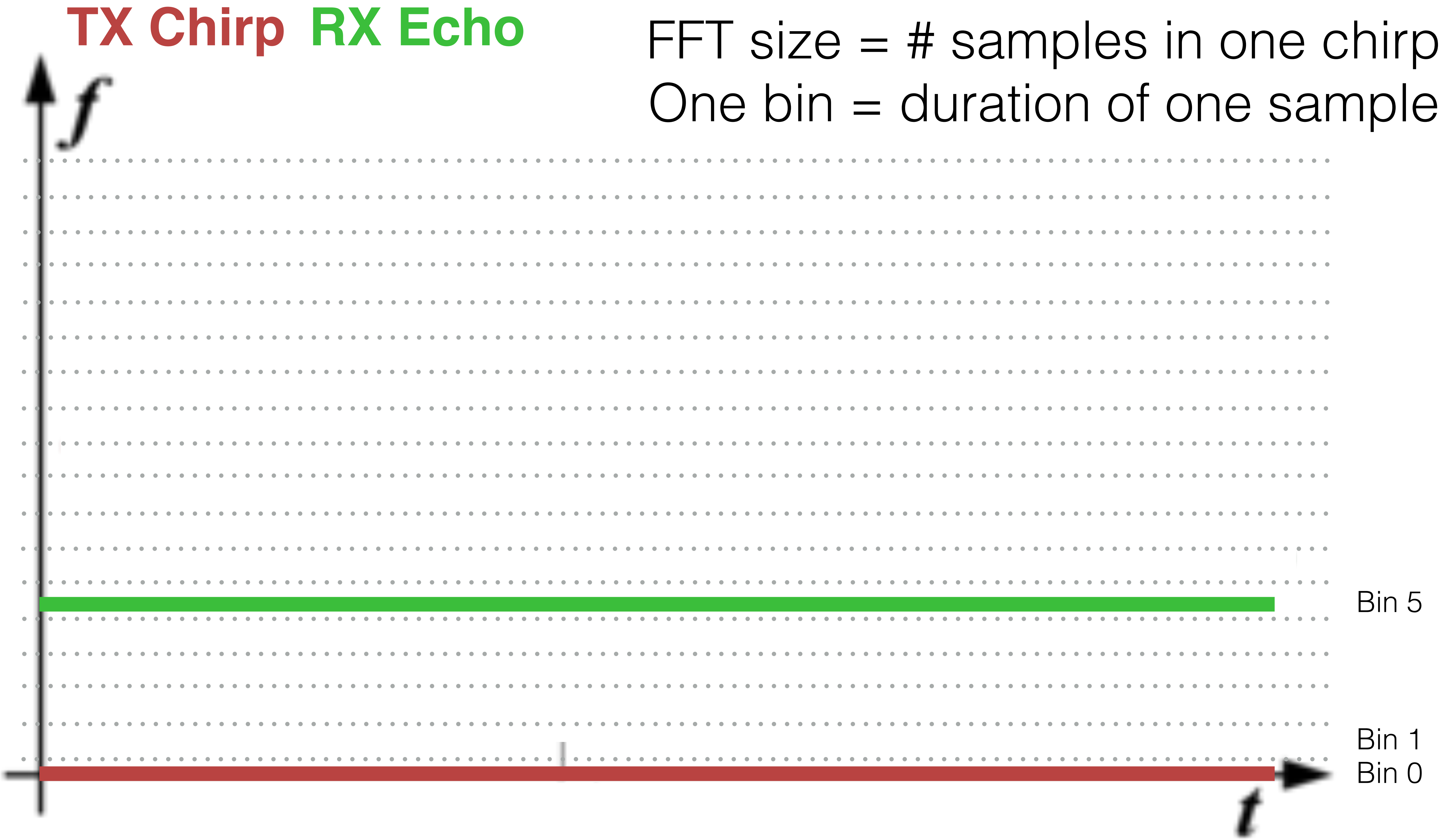
TX Chirp **RX Echo**



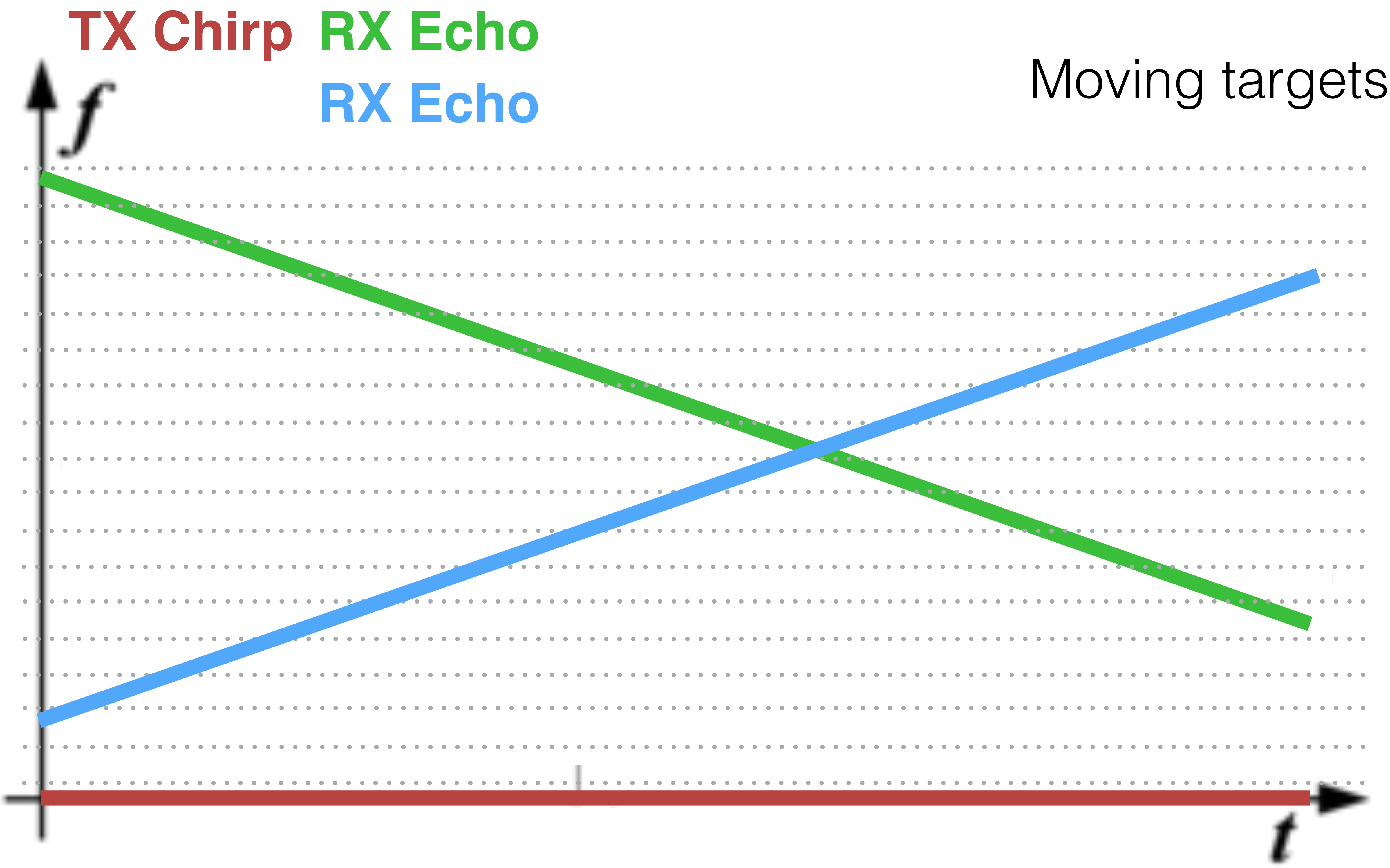
Frequency change implies time (and therefore range)

FMCW in the Frequency Domain (De-chirped, **FFT**)

FFT size = # samples in one chirp
One bin = duration of one sample



FMCW in the Frequency Domain (De-chirped, **FFT**)



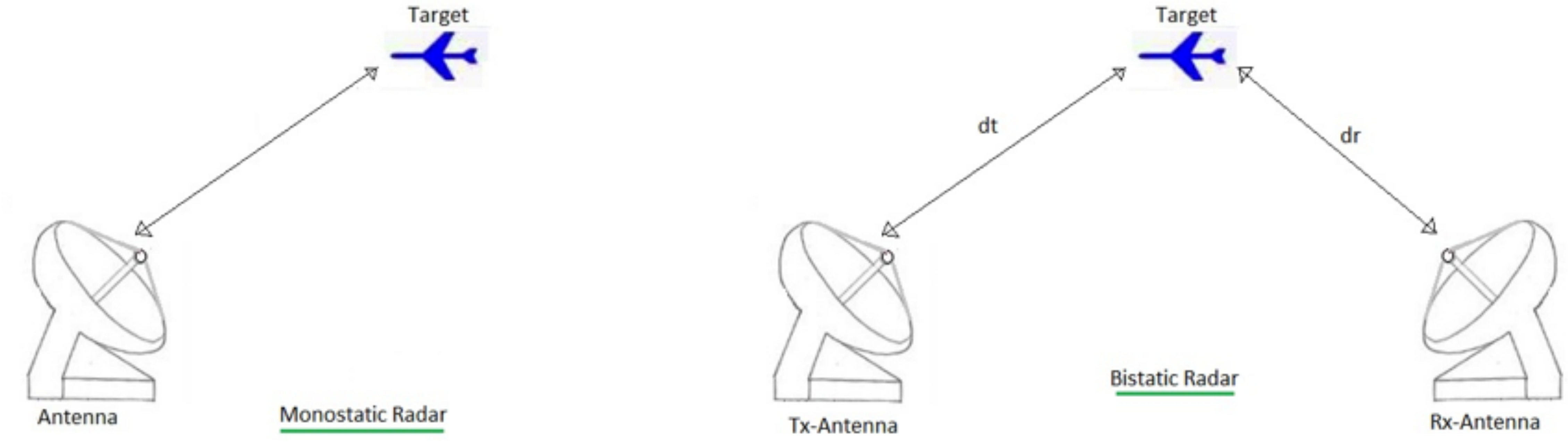
Moving targets

Many Variables

- Sample Rate: sets sample duration, limits range resolution

- Chirp length: sets PRF, limits unambiguous range

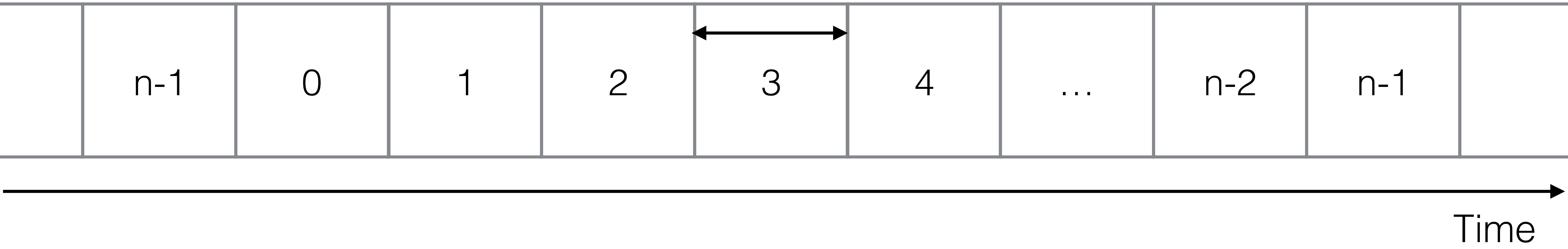
- TX/RX geometry: monostatic/bistatic, sets path (signal propagation/time model)



http://www.rfwireless-world.com/Terminology/Monostatic-radar-vs-Bistatic-radar.html

Many Variables

- RF: speed of light (fast)
- Time of one sample: large distance
- Increased sample rate: better range resolution



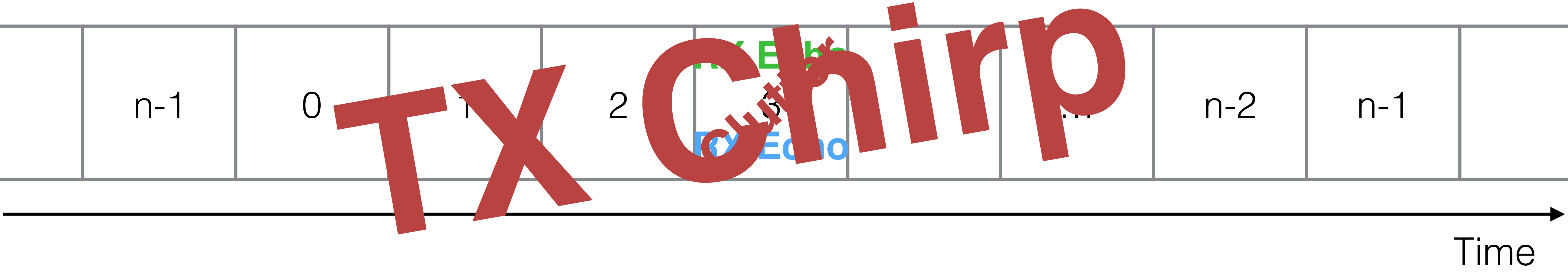
	n-1	0	1	2	3	4	…	n-2	n-1	

Time

N range (FFT) bins (each one sample duration)
Energy in each: reflected energy at that (RTT) time

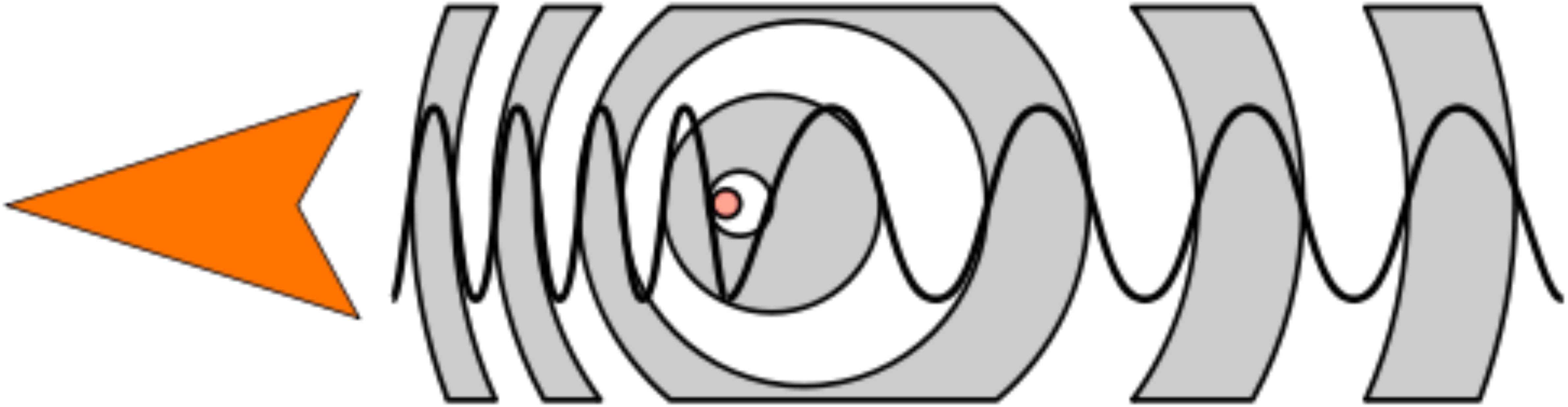
Hidden Returns

- Multiple targets end up in same range bin
- Target echo is too weak, swamped by local TX/clutter
- Any other information we can use to disambiguate?



Doppler Effect

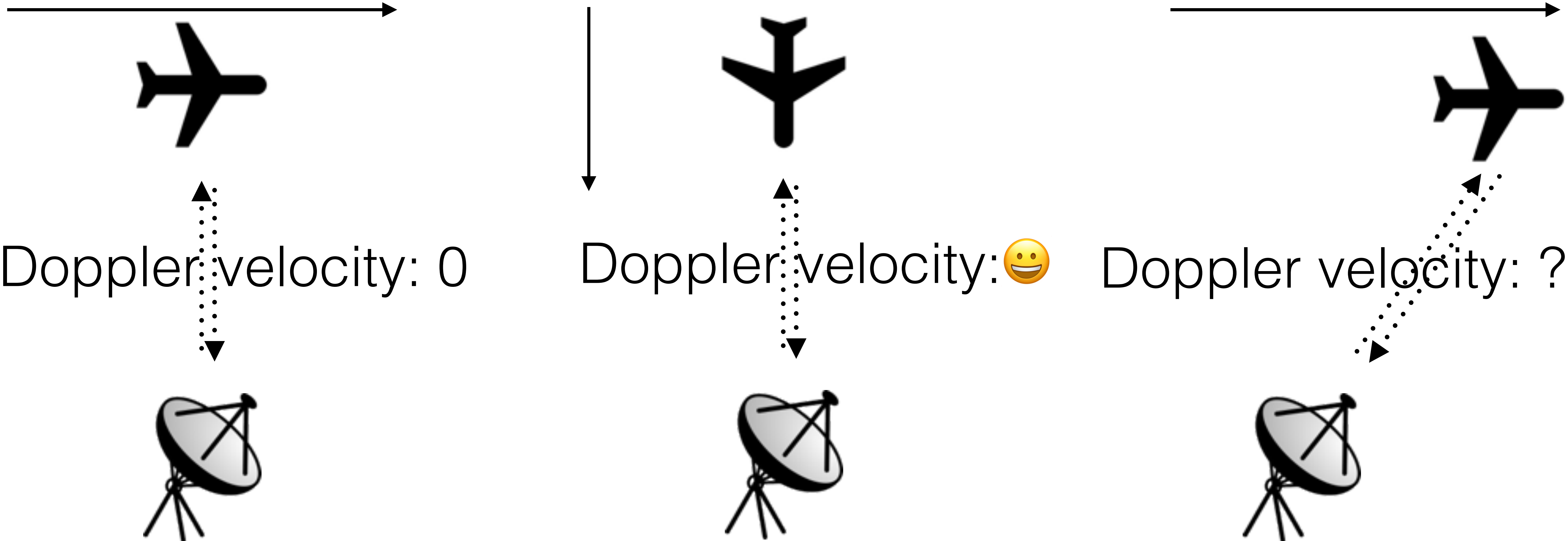
- Moving target will cause slight shift in received frequency
- Think about wavefront being received after reflection off target: **phase change due to motion**



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

Doppler Processing

- Collect multiple return periods (requires *Integration Time)*
- FFT across each range bin
- Velocity information for targets (w.r.t. RADAR system!)

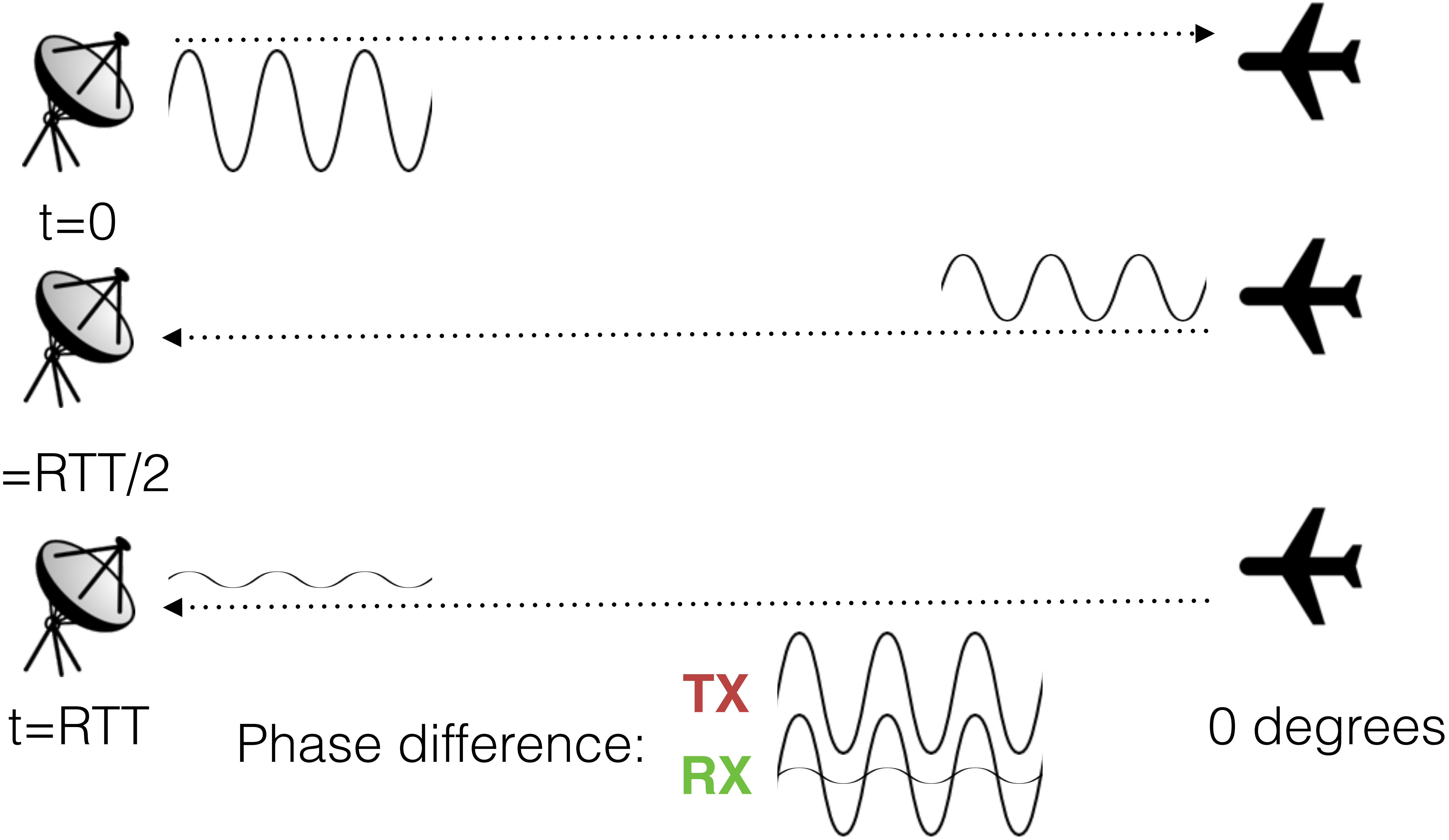


Doppler velocity: 0

Doppler velocity:😀

Doppler velocity: ?

Doppler Processing



t=0

t=RTT/2

t=RTT

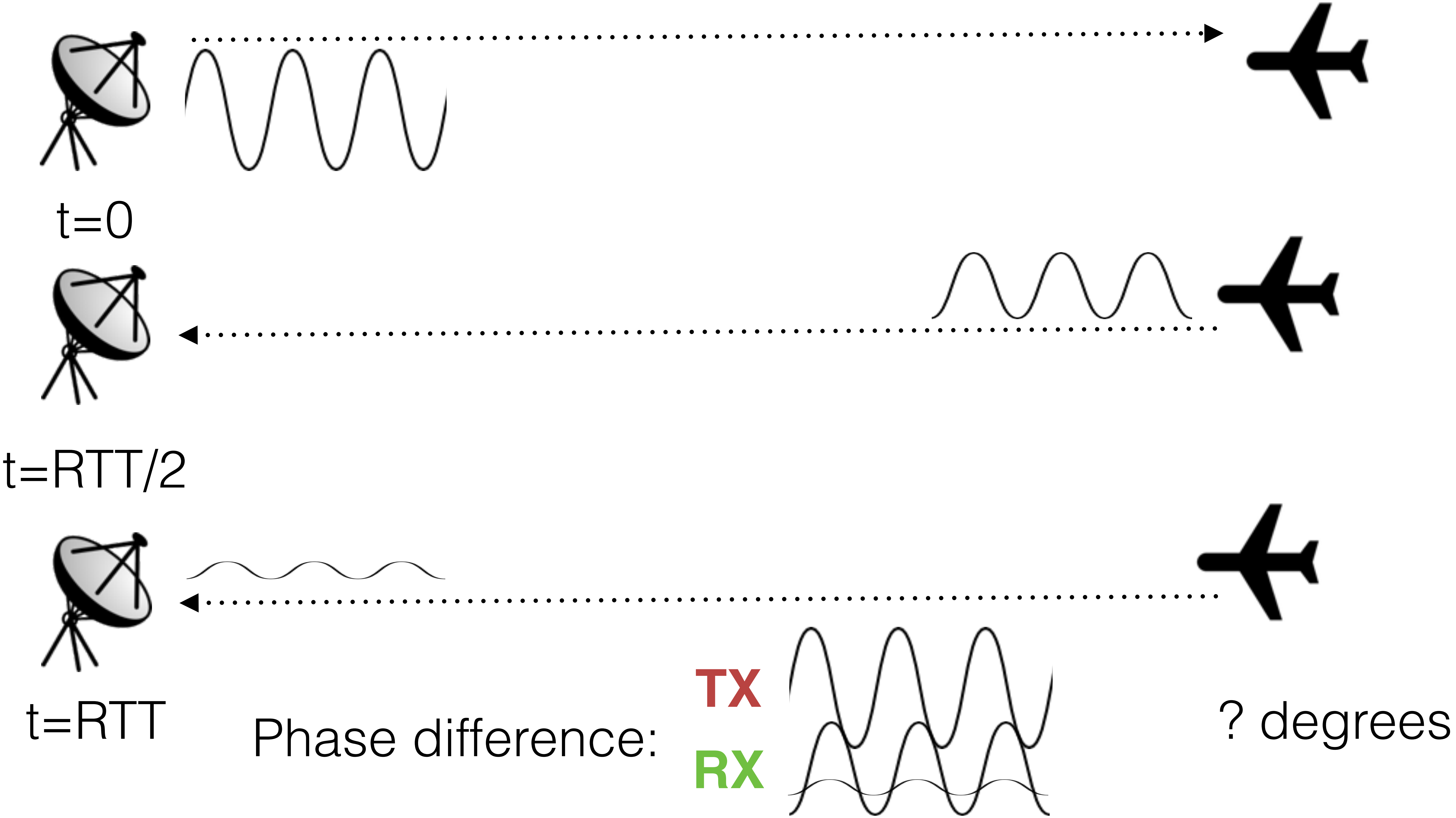
Phase difference:

TX

RX

0 degrees

Doppler Processing



t=0

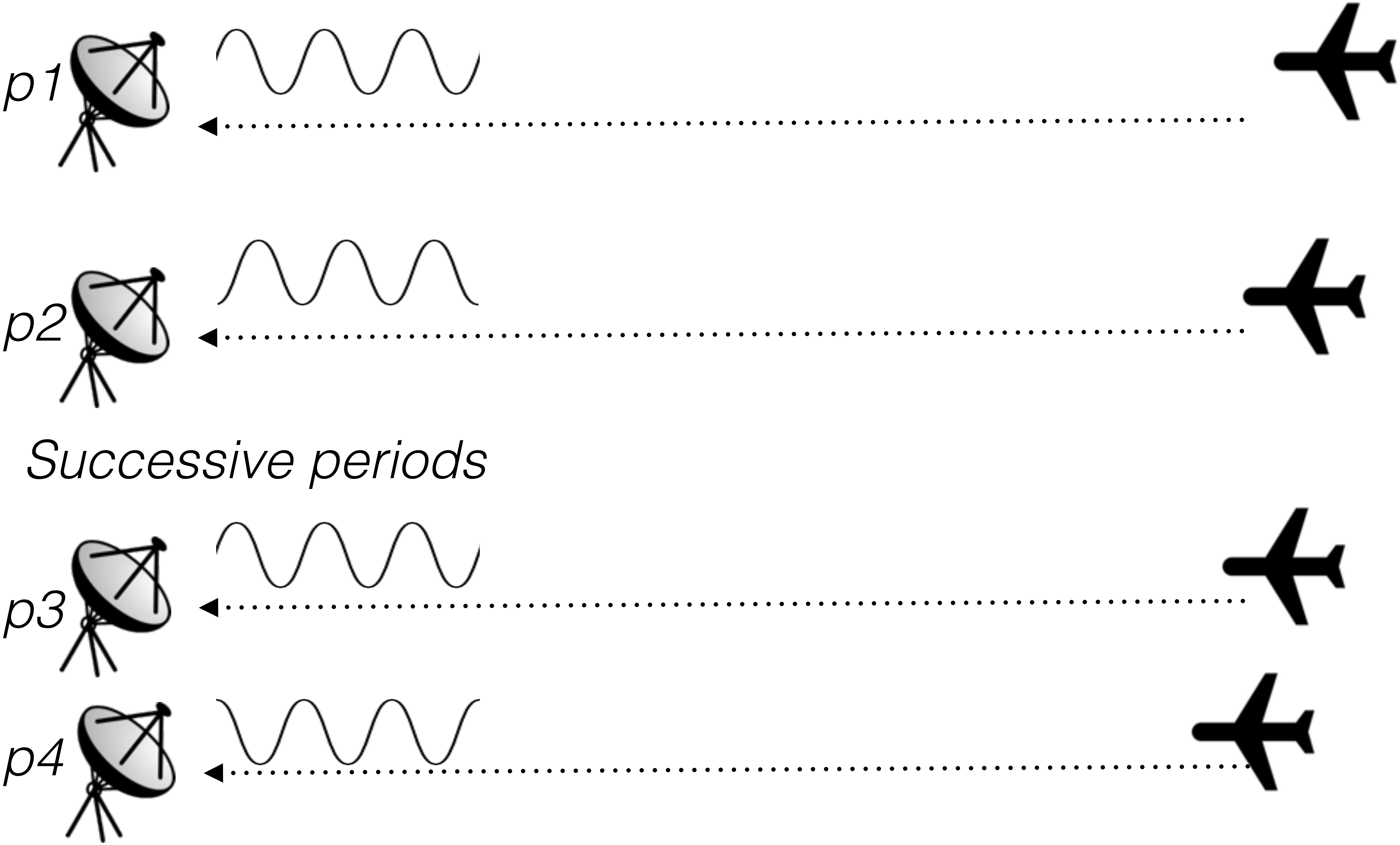
t=RTT/2

t=RTT

Phase difference: TX RX

? degrees

Doppler Processing (Integration Period)



p1

p2

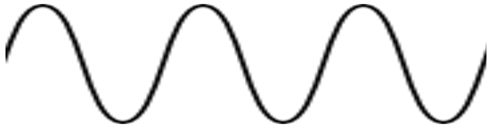
Successive periods

p3

p4

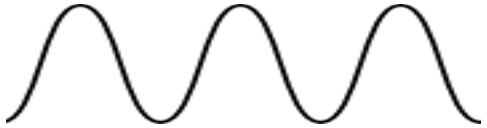
Doppler Processing (Integration Period)

p1



Changing phase over integration period

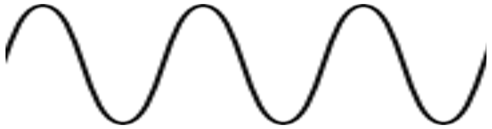
p2

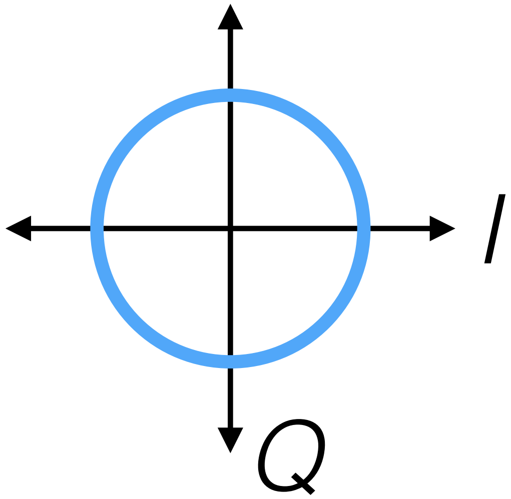


Get phase information from each FFT bin for each range transform

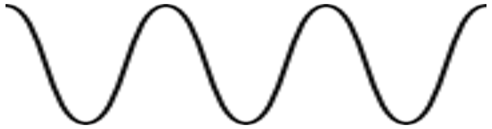
Successive periods

p3





p4

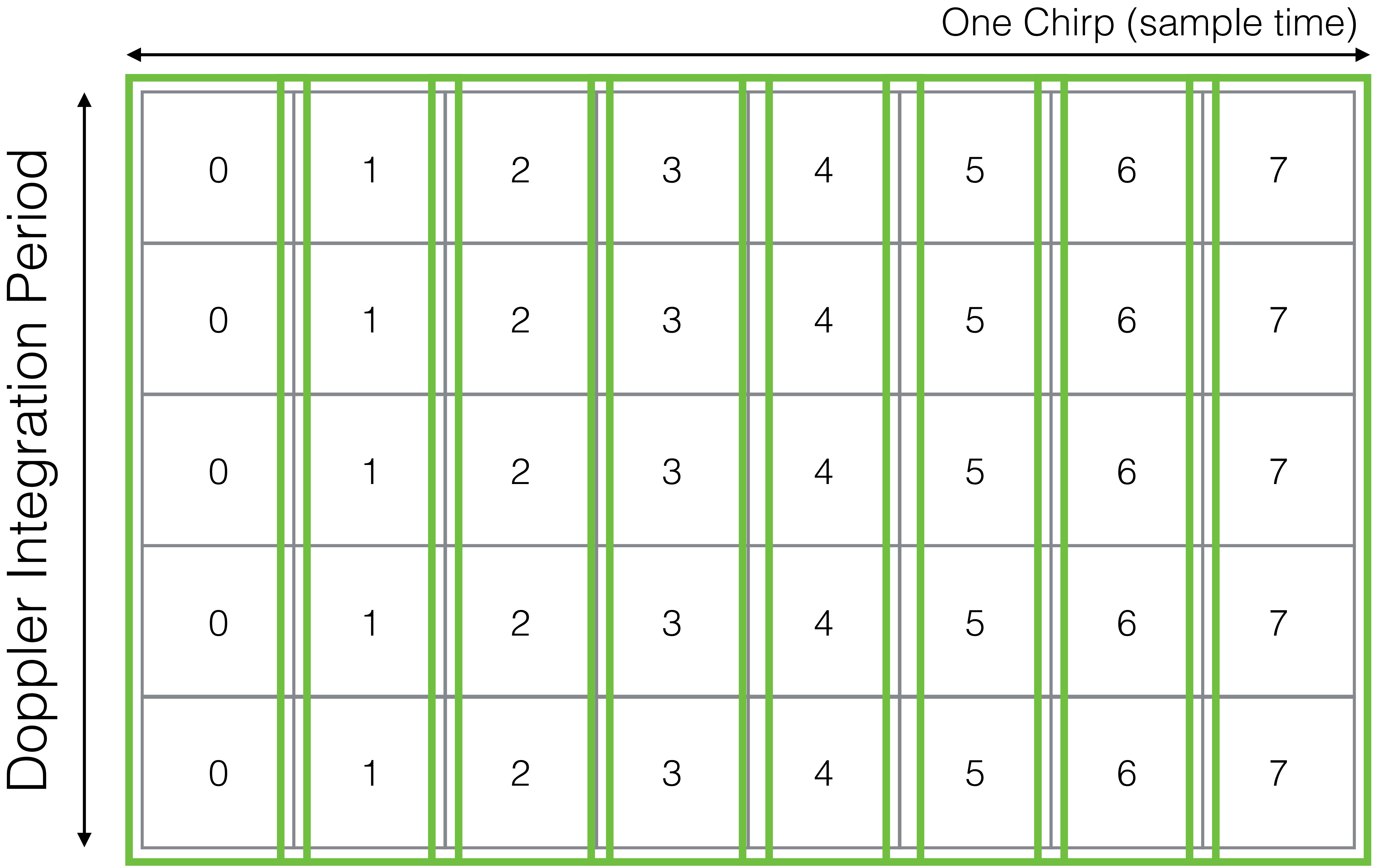


Changing phase over time = ?

Doppler Processing

Row: range (FFT) bins

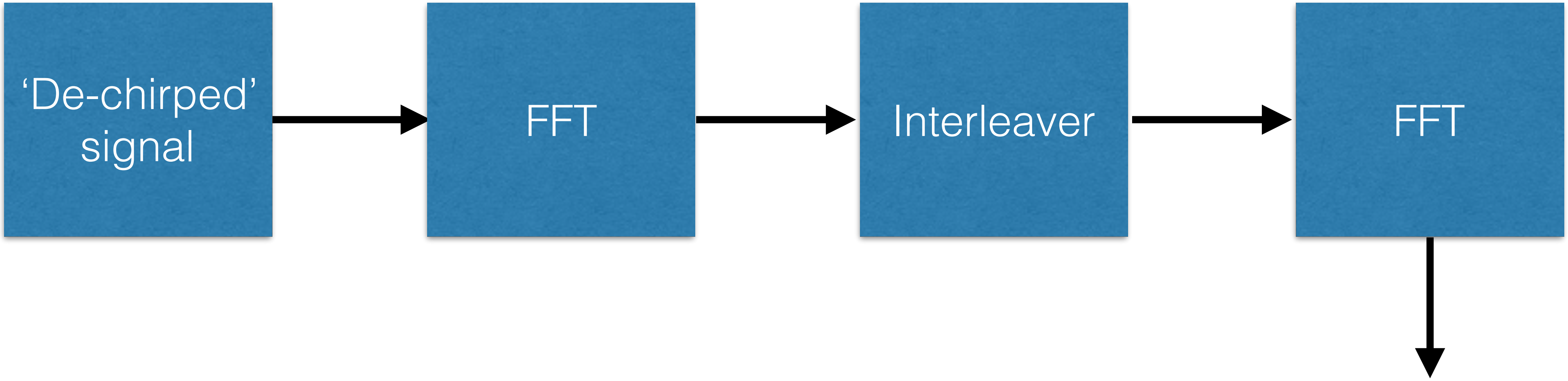
Column: same range bin over integration period



0	1	2	3	4	5	6	7
0	1	2	3	4	5	6	7
0	1	2	3	4	5	6	7
0	1	2	3	4	5	6	7
0	1	2	3	4	5	6	7

Doppler Processing

- Fill in rows, read out columns
- Interleaver! (read out more frequently for faster updates)



‘De-chirped’ signal

FFT

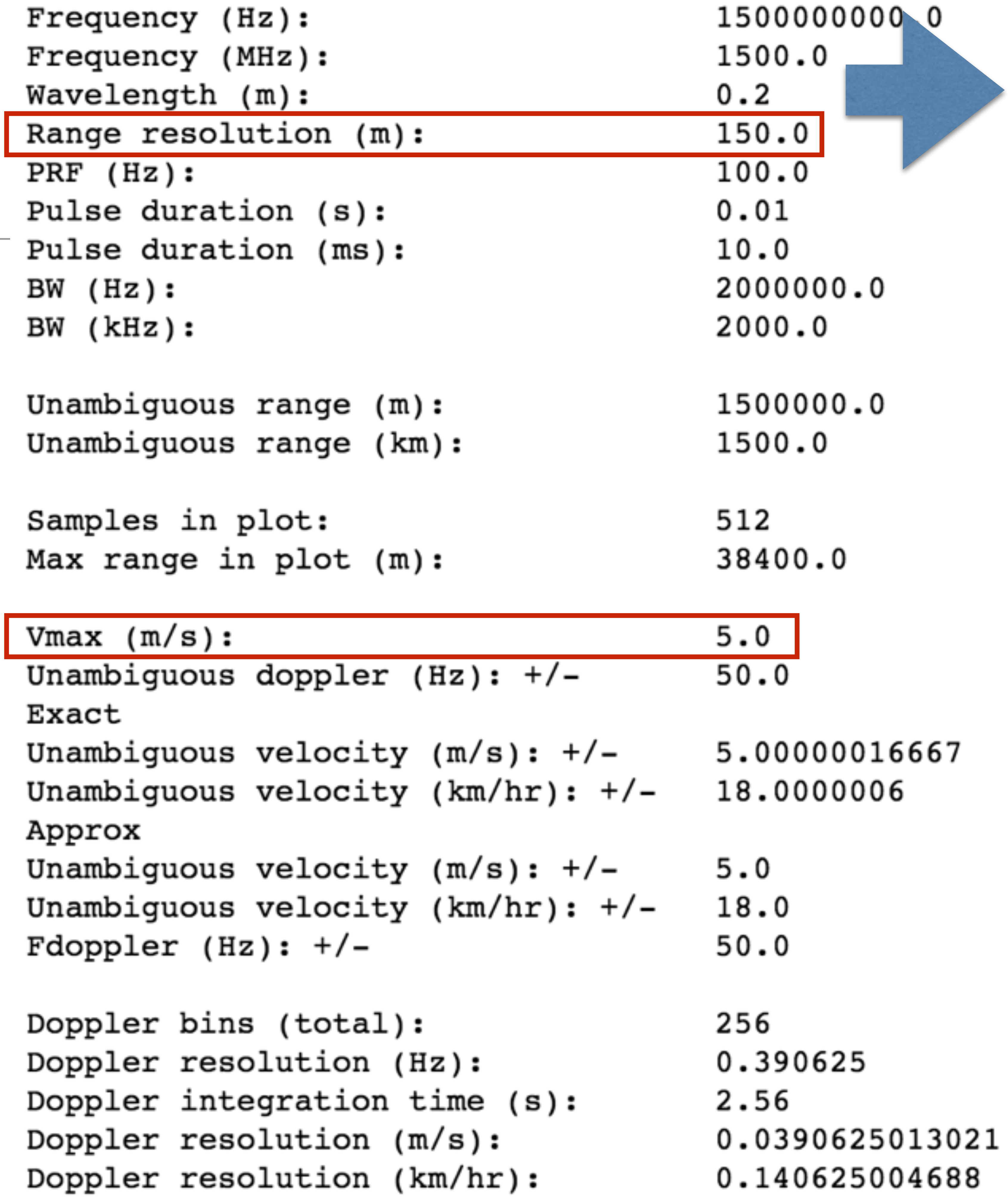
Interleaver

FFT

Magnitude: velocity for a given doppler velocity, for a given range (display as image!)

Speed of Light

- Range resolution too low

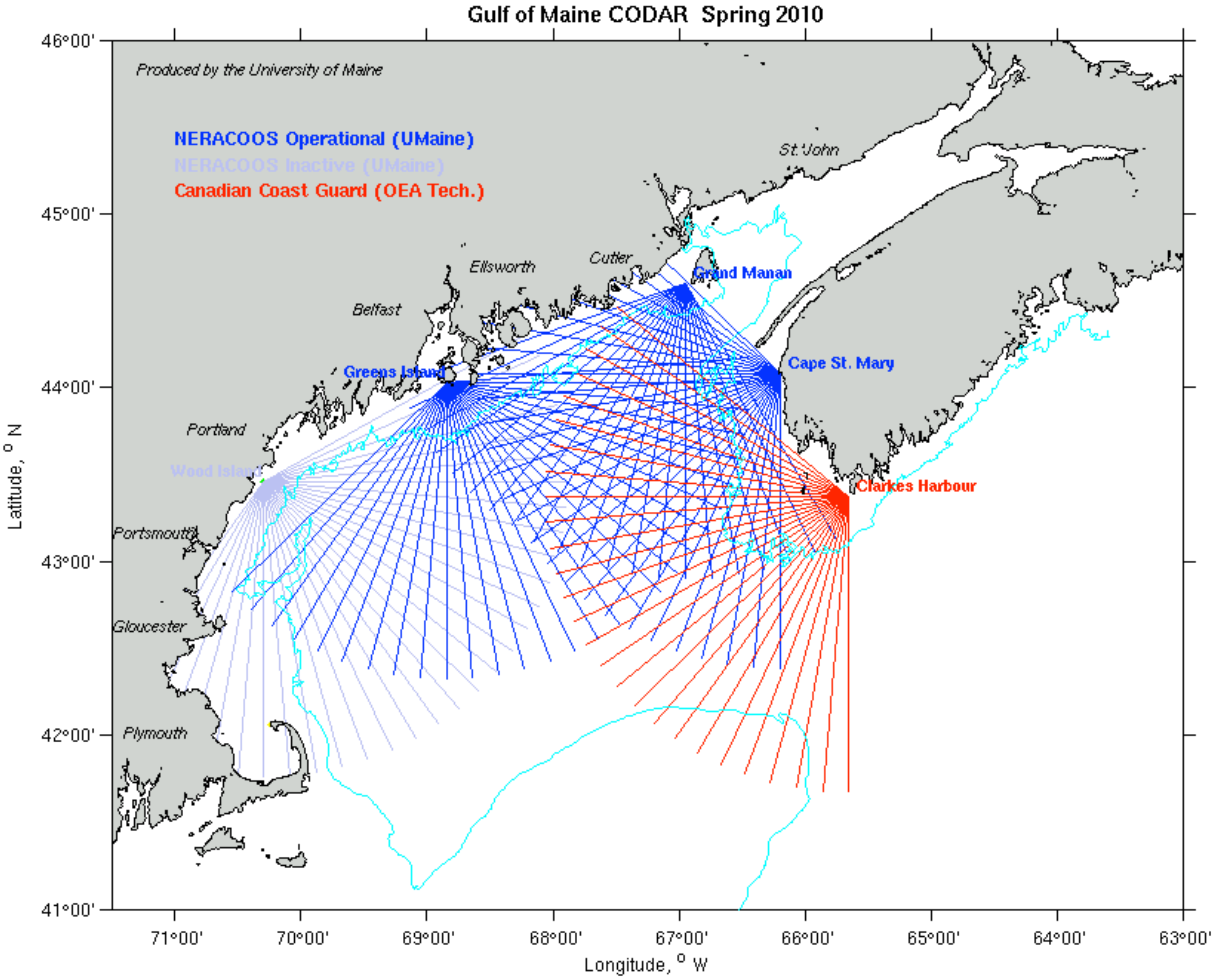


```
Frequency (Hz):                     1500000000.0
Frequency (MHz):                    1500.0
Wavelength (m):                     0.2
Range resolution (m):               150.0
PRF (Hz):                           100.0
Pulse duration (s):                 0.01
Pulse duration (ms):                10.0
BW (Hz):                            2000000.0
BW (kHz):                           2000.0

Unambiguous range (m):              1500000.0
Unambiguous range (km):             1500.0

Samples in plot:                    512
Max range in plot (m):              38400.0

Vmax (m/s):                         5.0
Unambiguous doppler (Hz): +/-       50.0
Exact
Unambiguous velocity (m/s): +/-     5.00000016667
Unambiguous velocity (km/hr): +/-   18.0000006
Approx
Unambiguous velocity (m/s): +/-     5.0
Unambiguous velocity (km/hr): +/-   18.0
Fdoppler (Hz): +/-                  50.0

Doppler bins (total):               256
Doppler resolution (Hz):            0.390625
Doppler integration time (s):       2.56
Doppler resolution (m/s):           0.0390625013021
Doppler resolution (km/hr):         0.140625004688
```

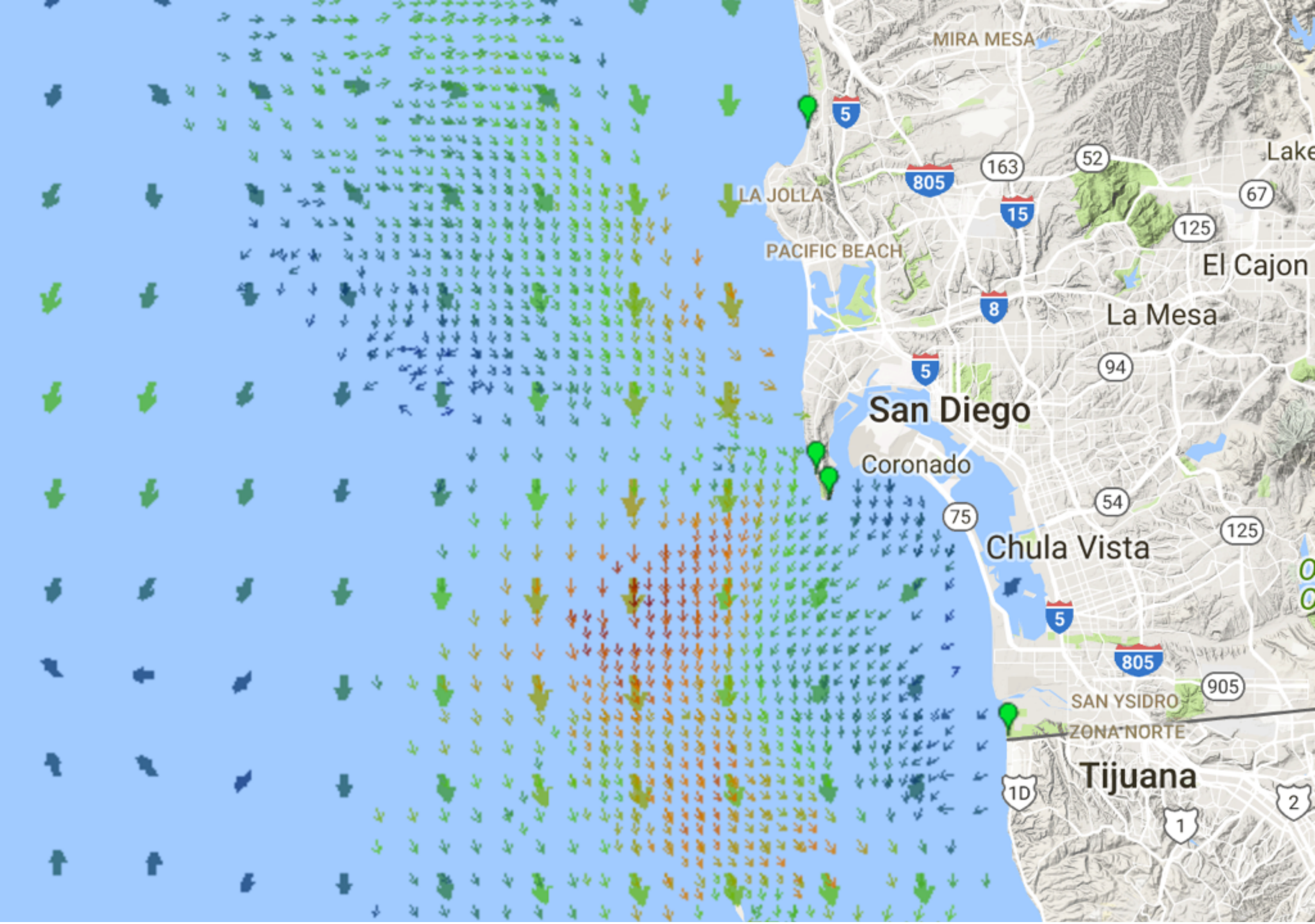
CODAR

- Mapping ocean currents with HF RADAR

http://www.codar.com/



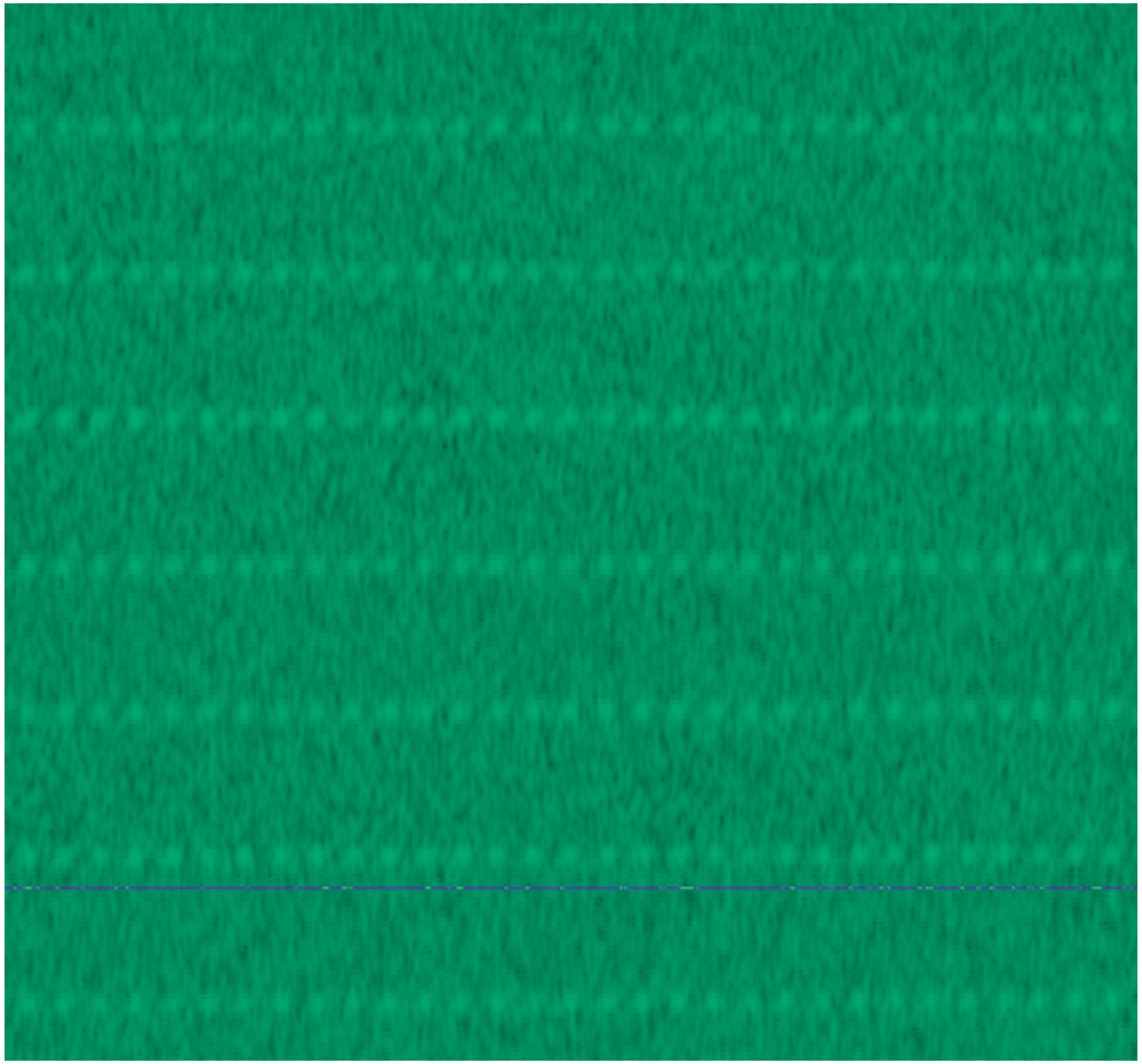
http://gyre.umeoce.maine.edu/gomoos/codar/

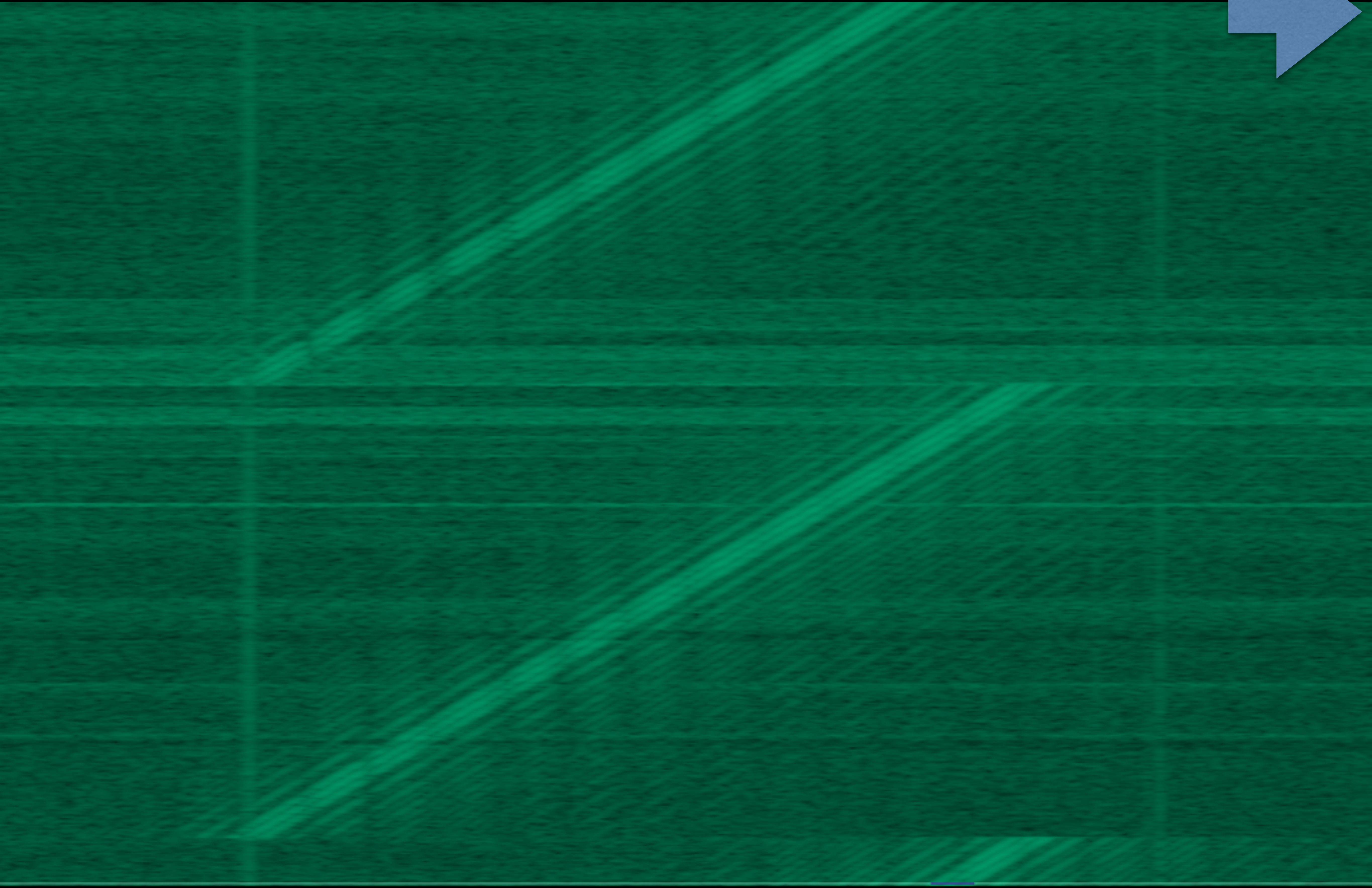


http://cordc.ucsd.edu/projects/mapping/maps/

Mixing (Nulling) or Gating (Switching)

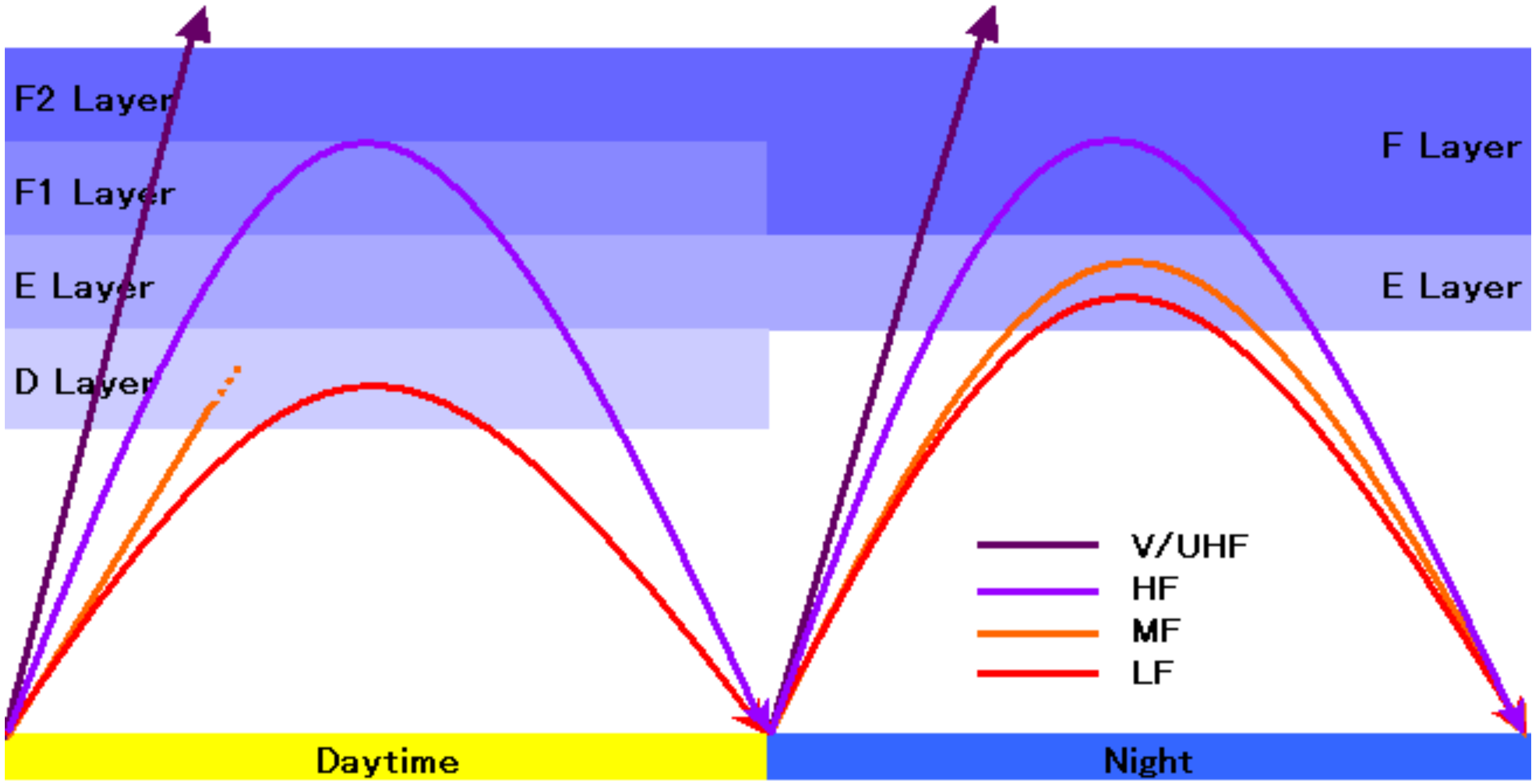
- TX & RX same site (monostatic)
- Remove TX signal at receiver before digitising (avoid saturation)
- Discontinuous TX (gating TX signal)
- Gating produces AM sidebands in frequency domain





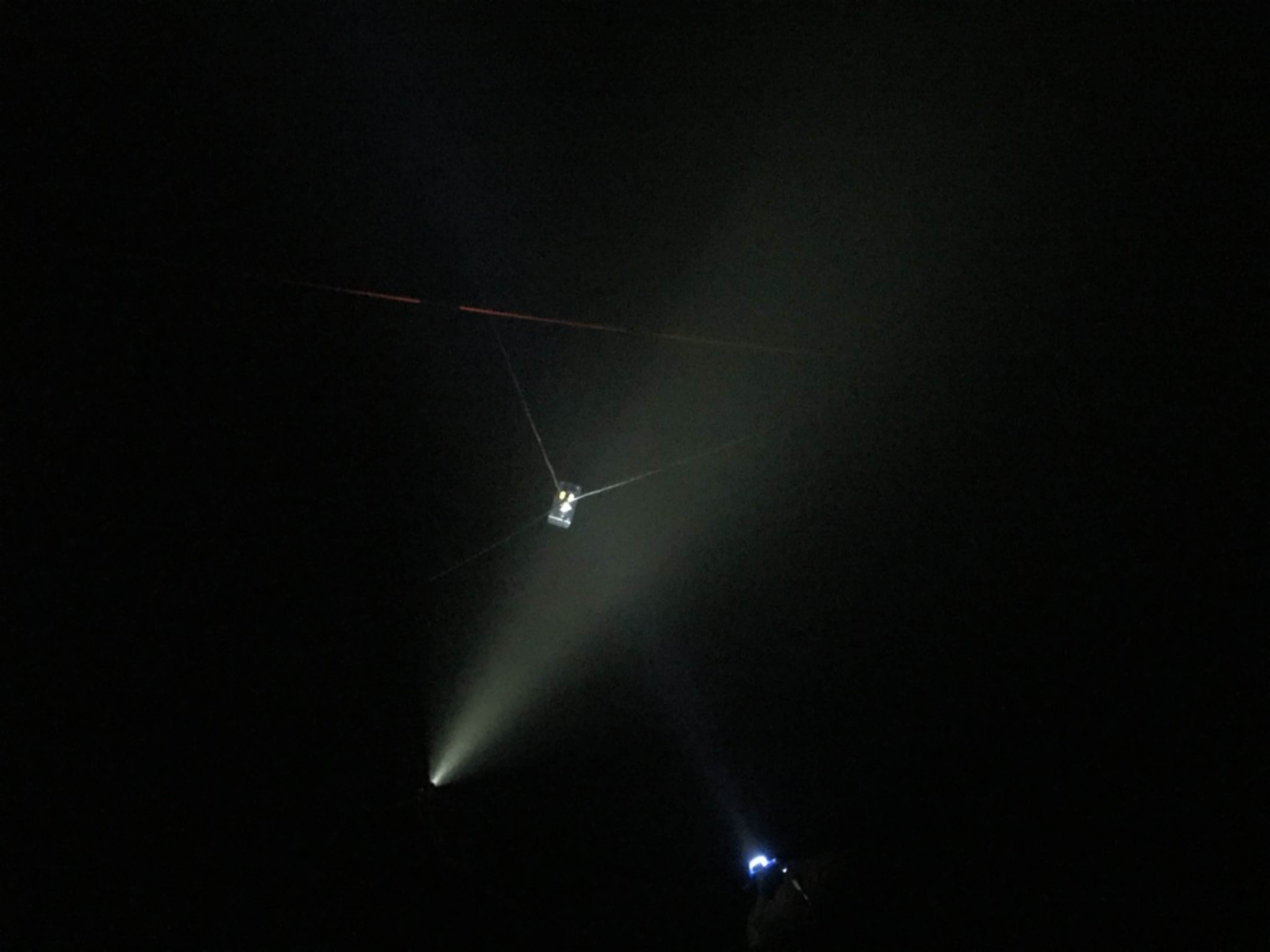
Ionosphere

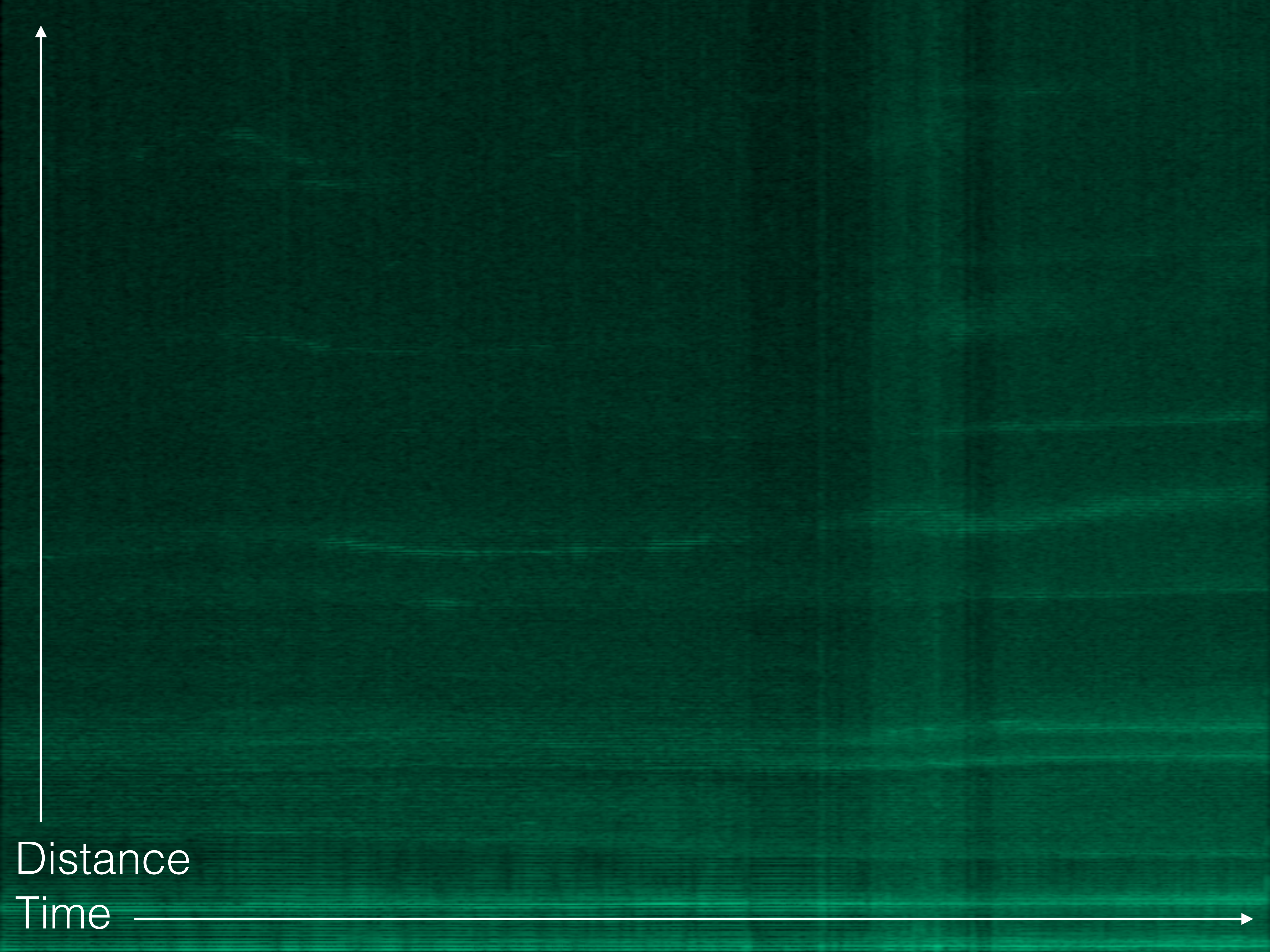
- Will reflect CODAR waveform!
- Can image ionosphere

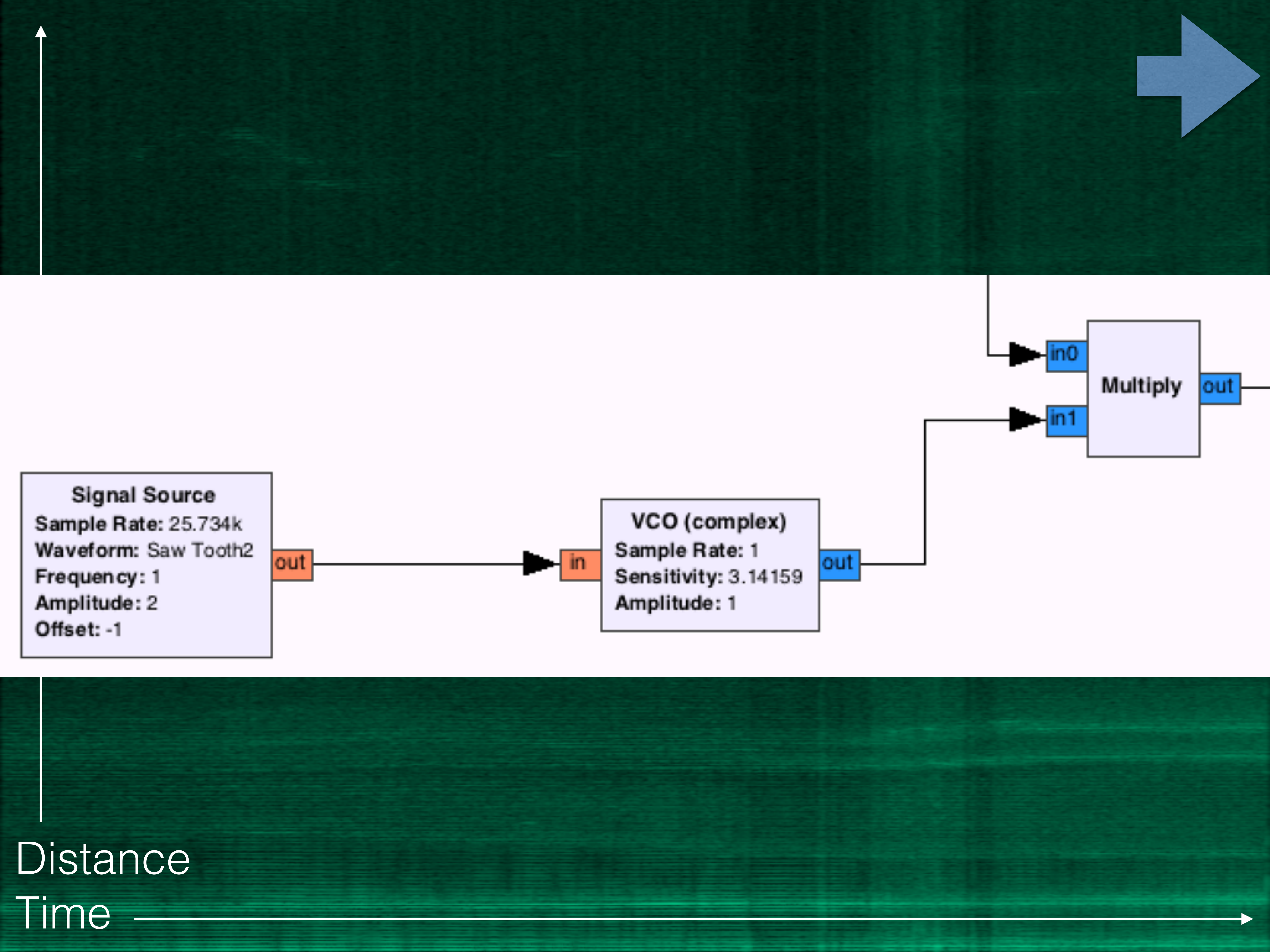


Ionospheric reflection
(under normal condition)

TRAVEL MAT



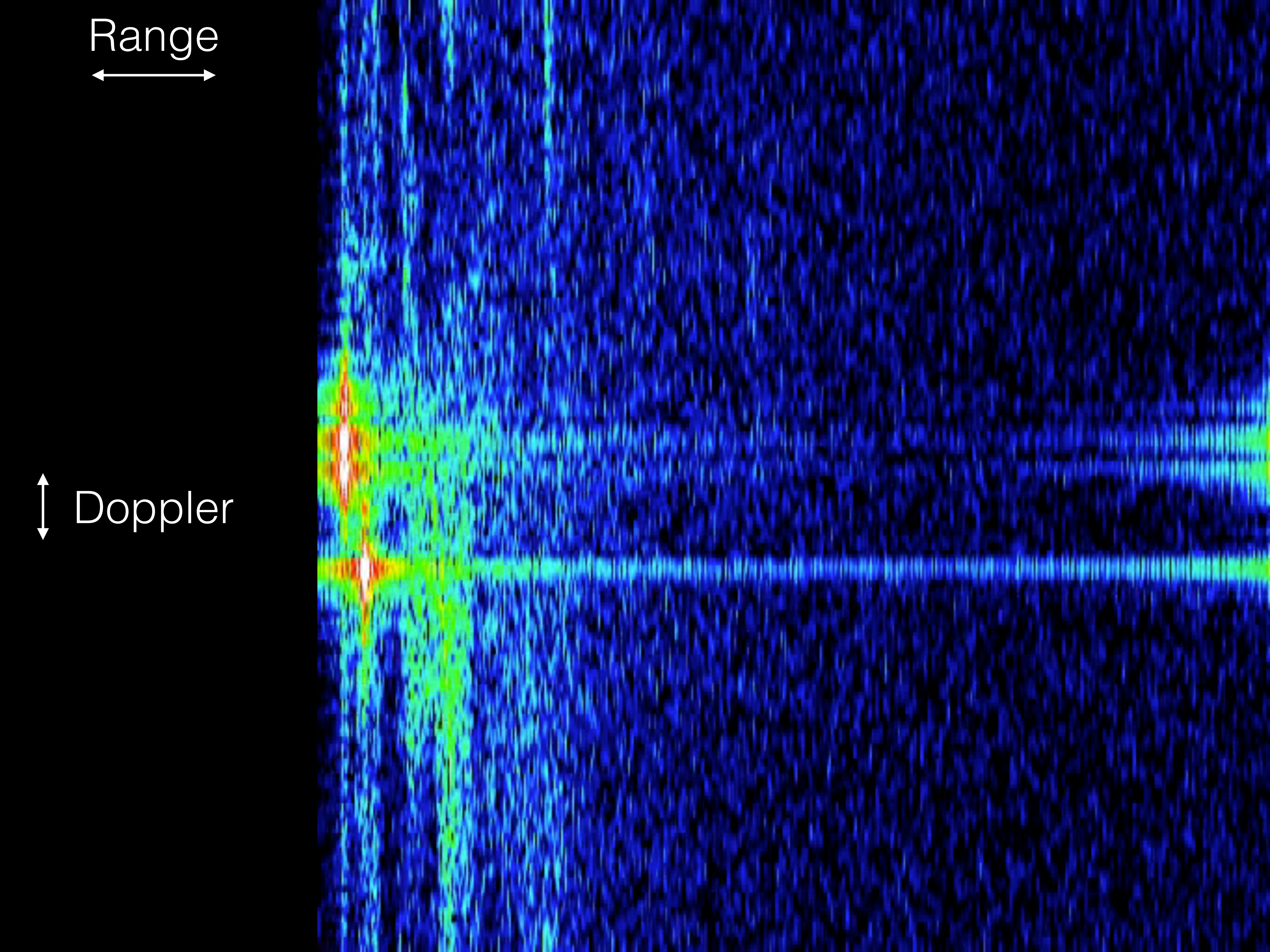

Distance
Time



Signal Source
Sample Rate: 25.734k
Waveform: Saw Tooth2
Frequency: 1
Amplitude: 2
Offset: -1

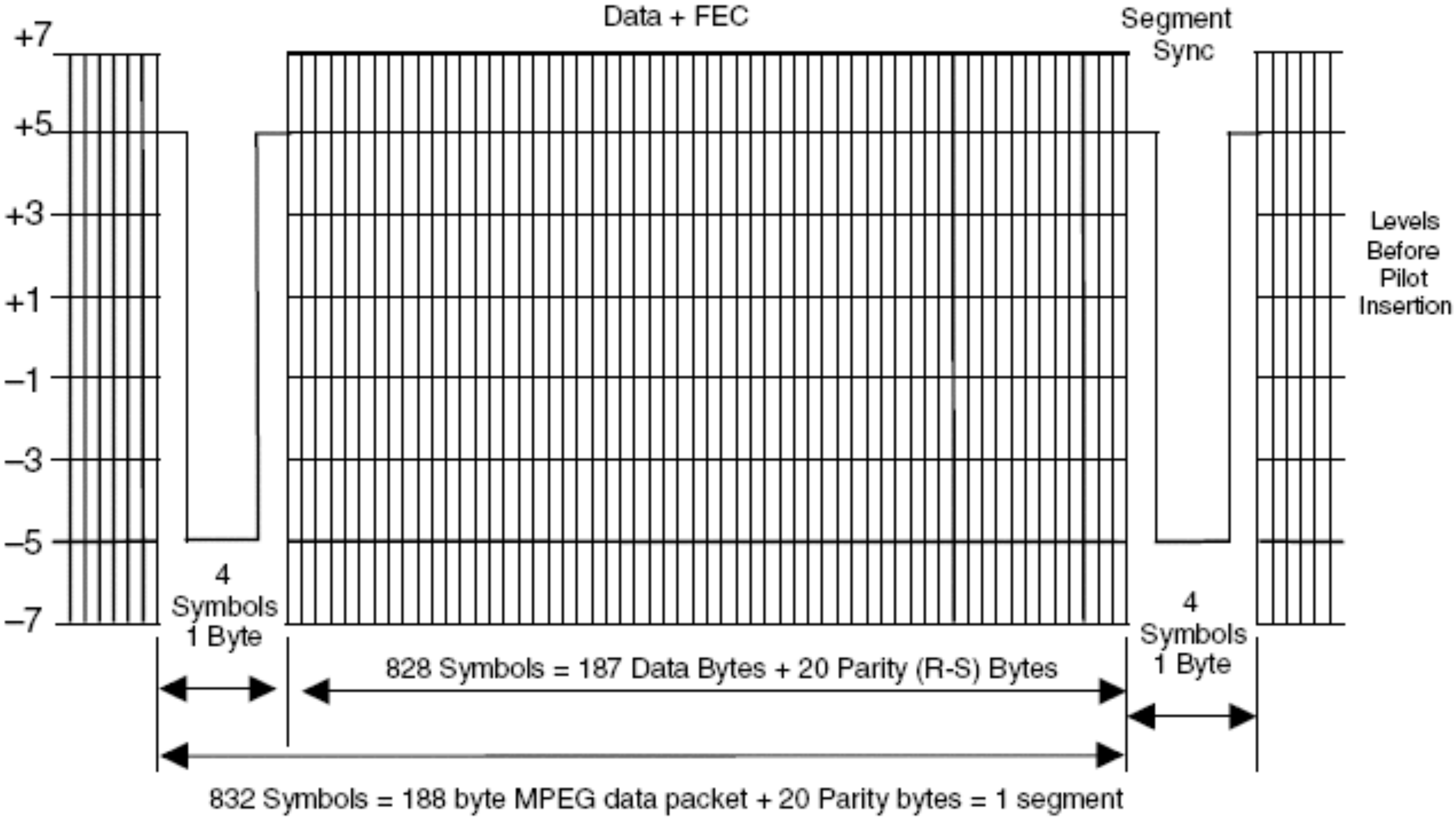
VCO (complex)
Sample Rate: 1
Sensitivity: 3.14159
Amplitude: 1

Multiply

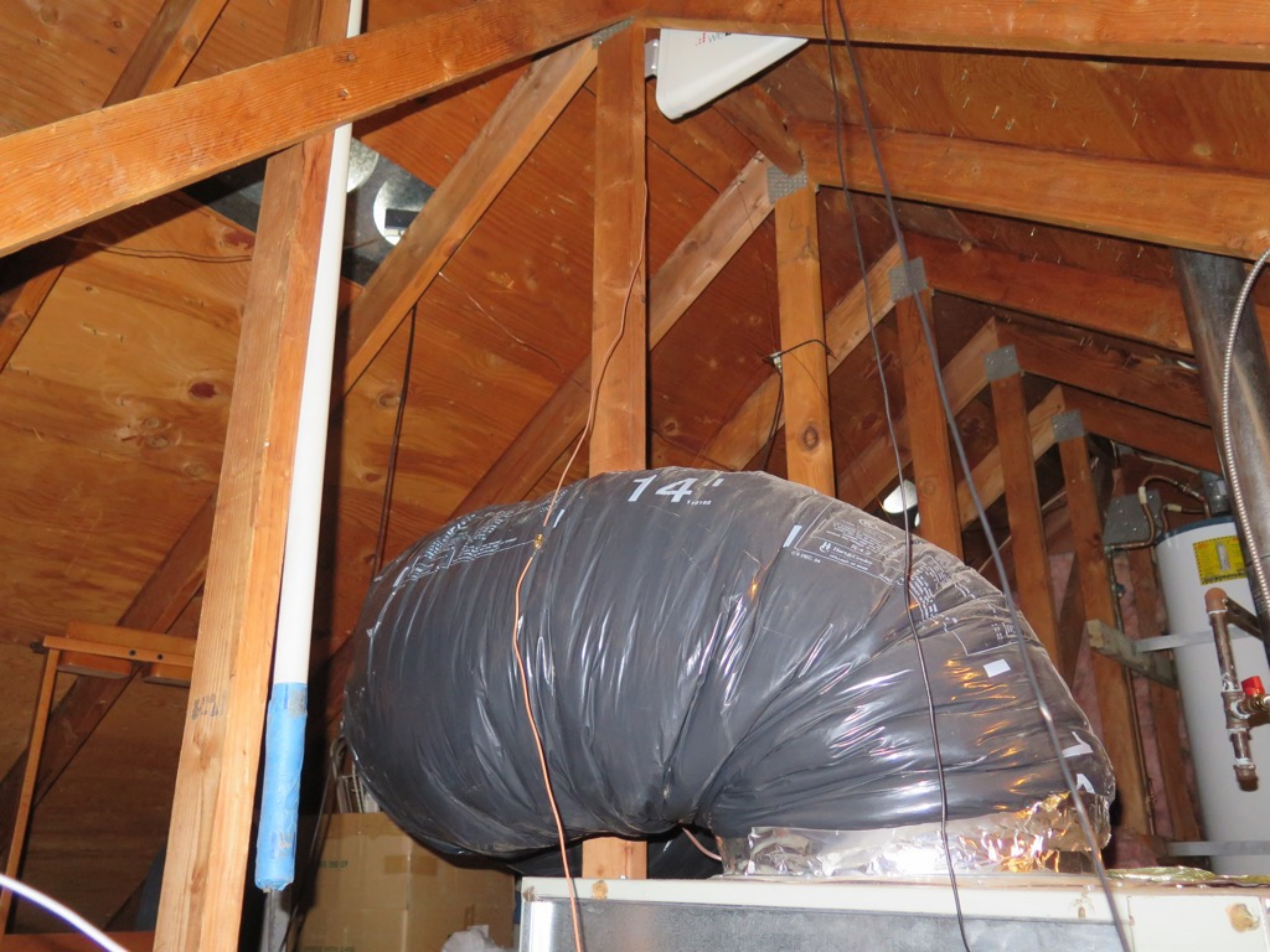

Range
Doppler

ATSC Live Passive RADAR

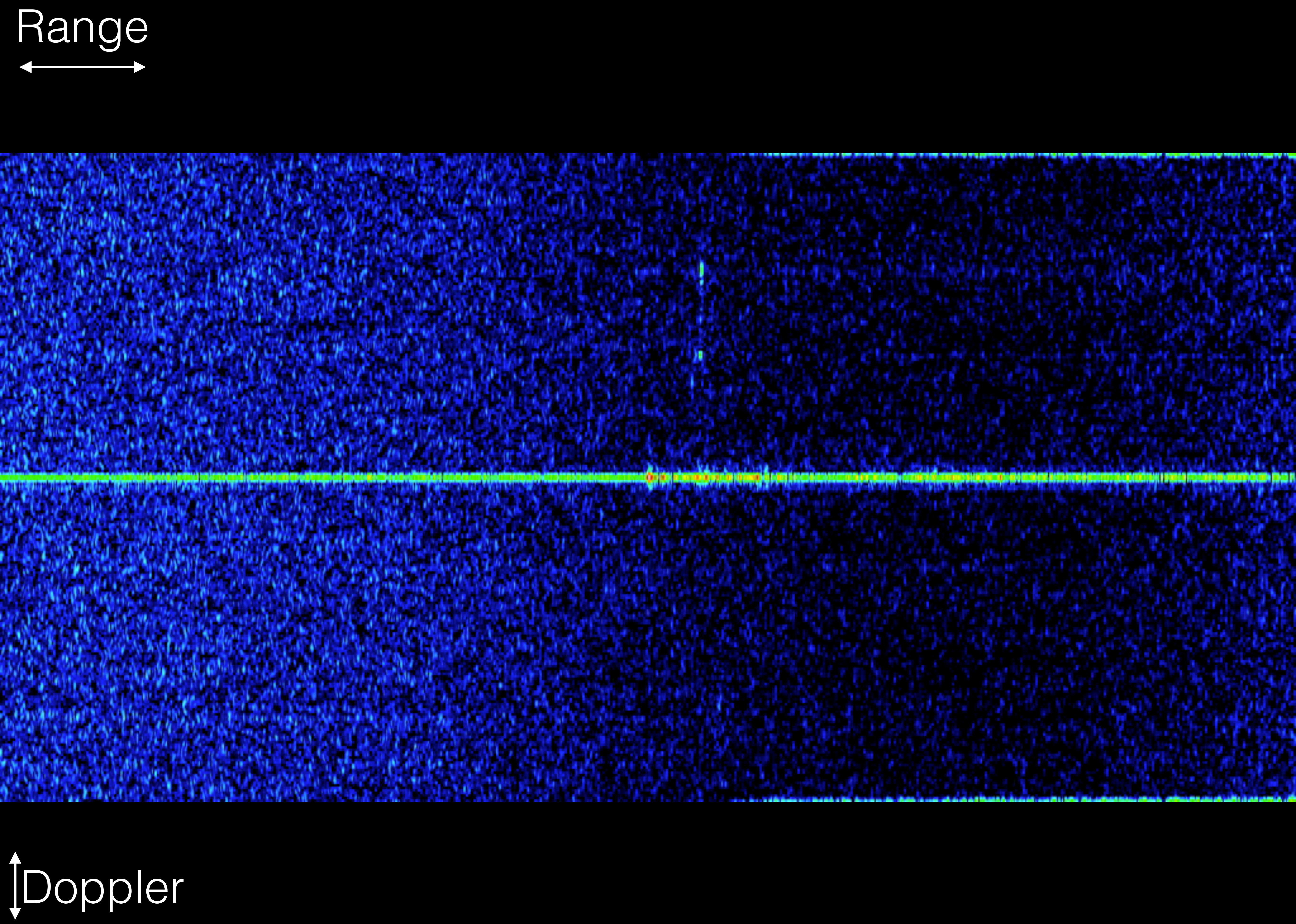
- Use known 511 PN synchronisation sequence
- ~41 Hz
- ~28 m
- +/- ~5 m/s

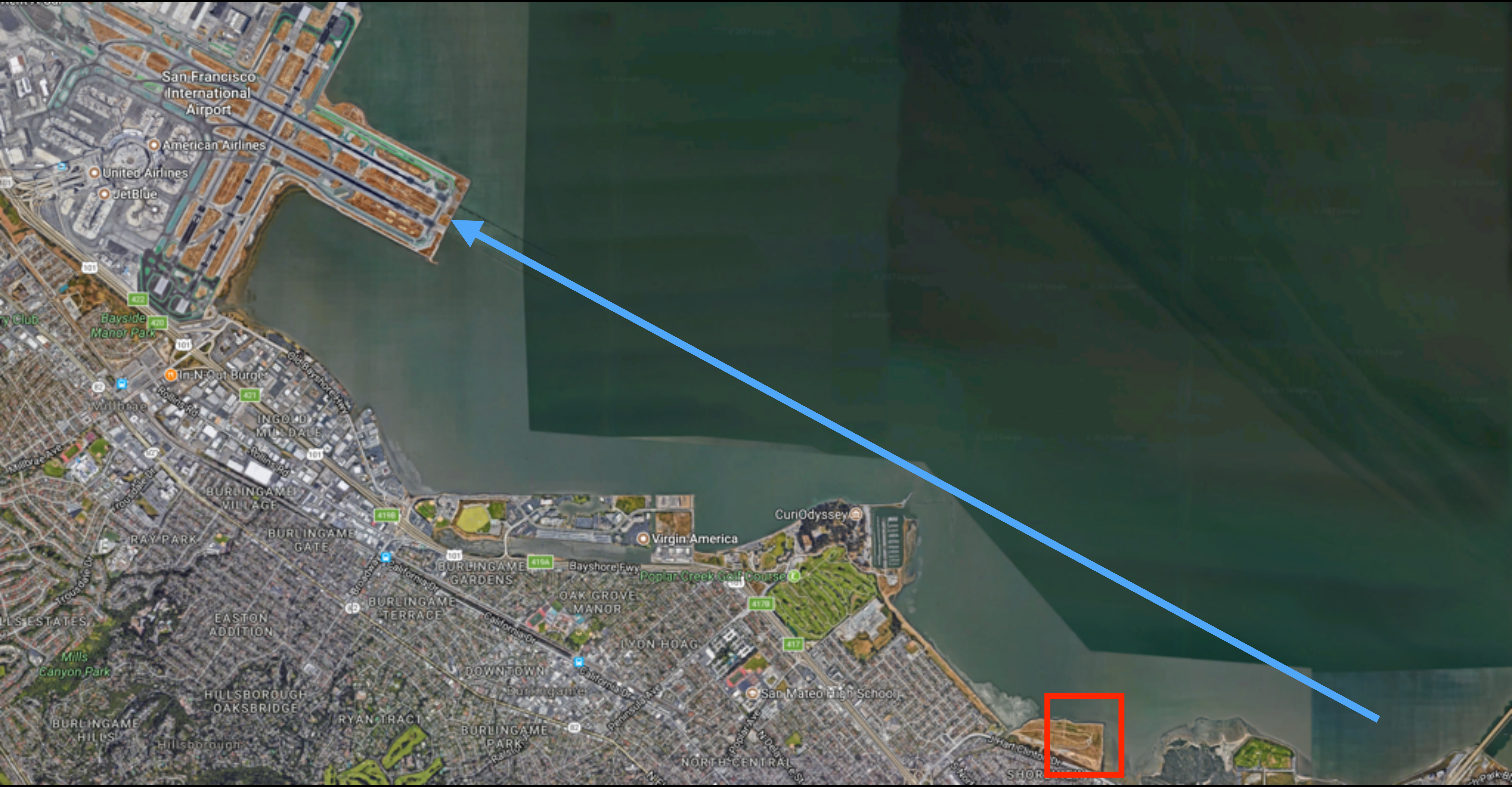

Data + FEC
Segment Sync
+7
+5
+3
+1
–1
–3
–5
–7
Levels Before Pilot Insertion
4 Symbols 1 Byte
828 Symbols = 187 Data Bytes + 20 Parity (R-S) Bytes
4 Symbols 1 Byte
832 Symbols = 188 byte MPEG data packet + 20 Parity bytes = 1 segment

http://www.tek.com/document/primer/fundamentals-8vsb

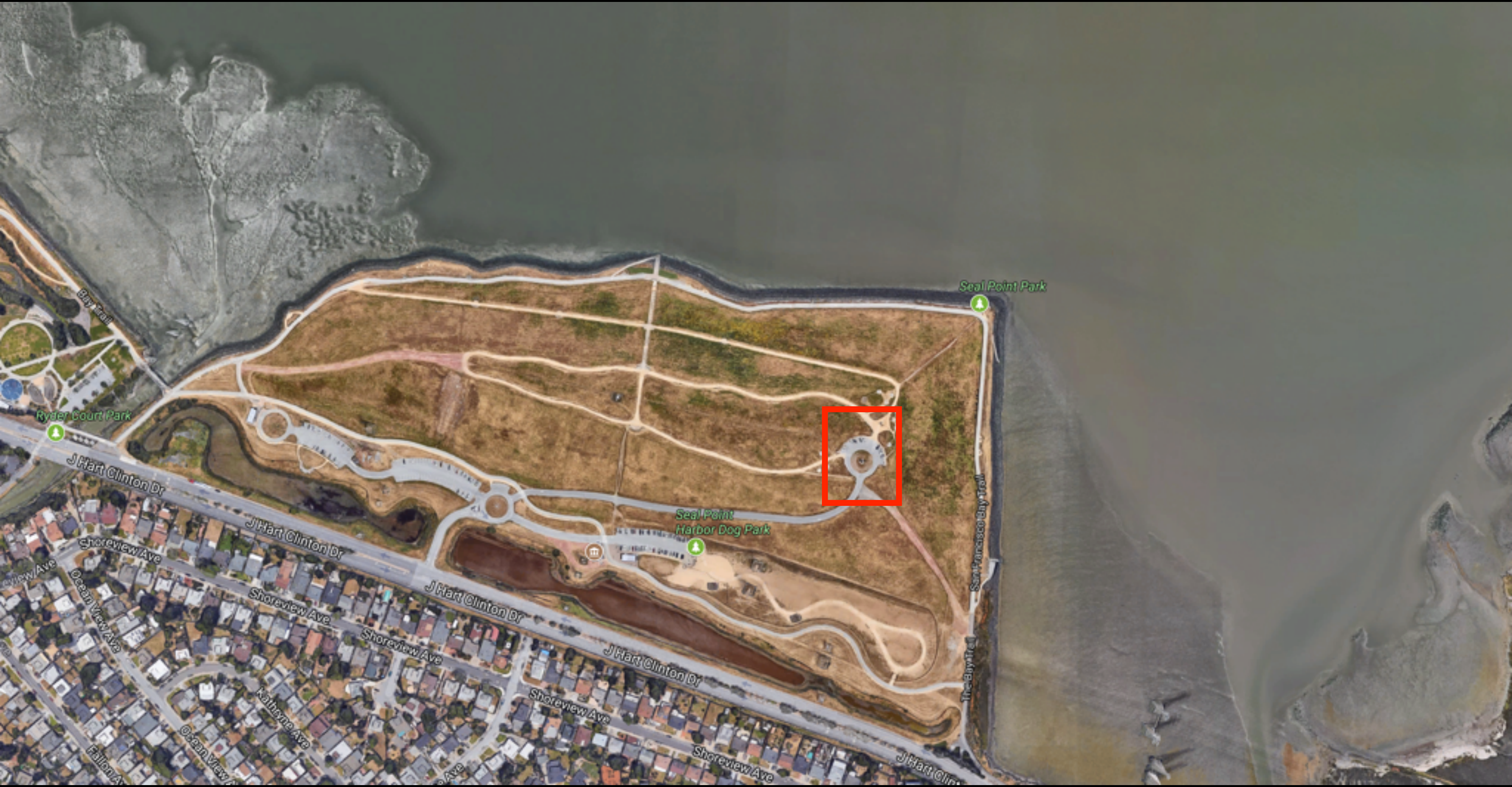

14"

2200

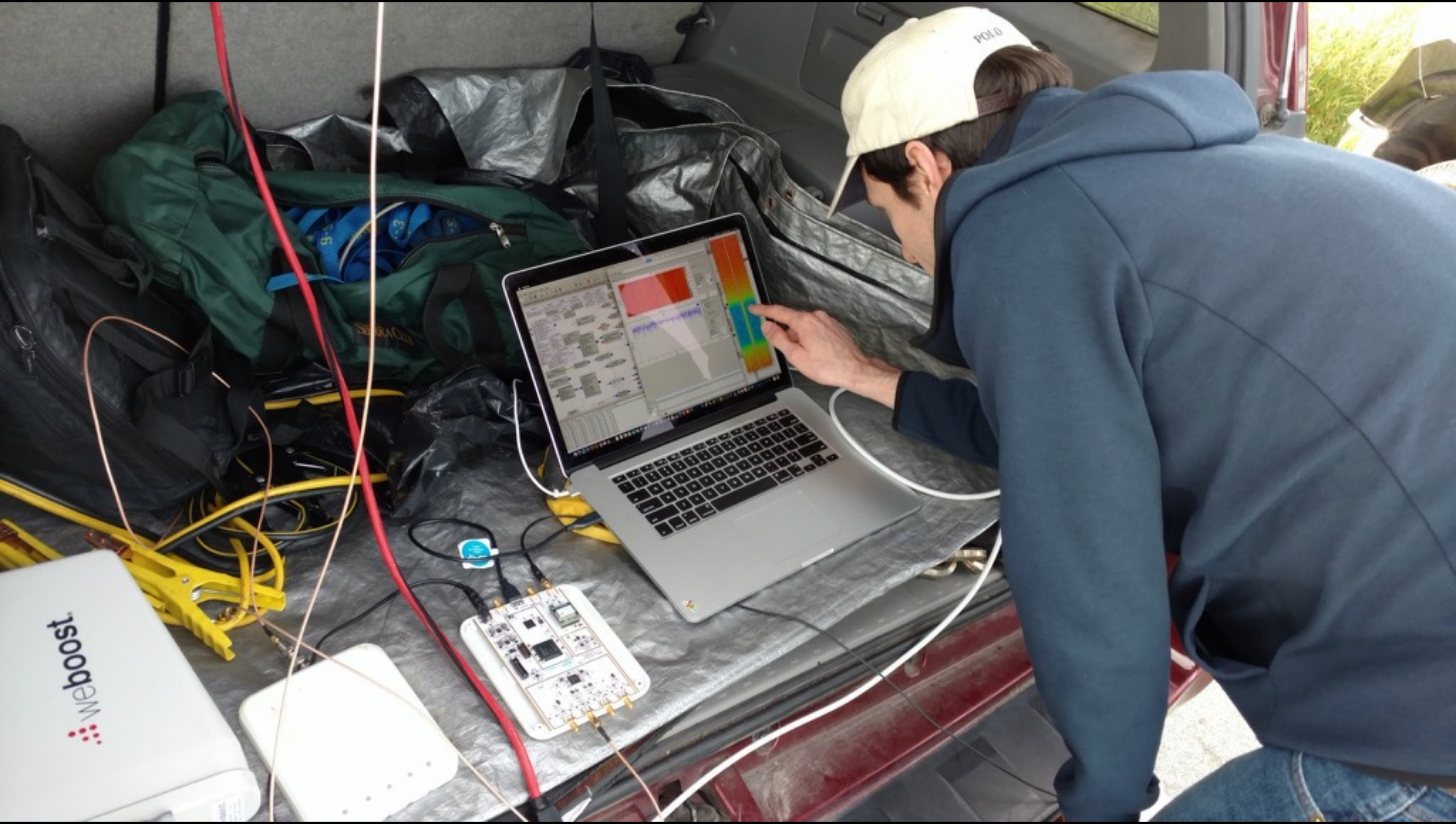

Range
Doppler



San Francisco International Airport
American Airlines
United Airlines
JetBlue
Bayside Manor Park
In-N-Out Burger
Millbrae
INGOLD MILLSDALE
BURLINGAME VILLAGE
RAY PARK
BURLINGAME GATE
CuriOdyssey
Virgin America
Bayshore Fwy
BURLINGAME GARDENS
Poplar Creek Golf Course
BURLINGAME TERRACE
OAK GROVE MANOR
EASTON ADDITION
LYON HOAG
DOWNTOWN
Burlingame
San Mateo High School
Mills Canyon Park
HILLSBOROUGH OAKSBRIDGE
RYAN TRACT
BURLINGAME HILLS
Hillsborough
BURLINGAME PARK
NORTH CENTRAL
J Hart Clinton Dr
SHORE
101
422
420
421
419B
419A
417B
417

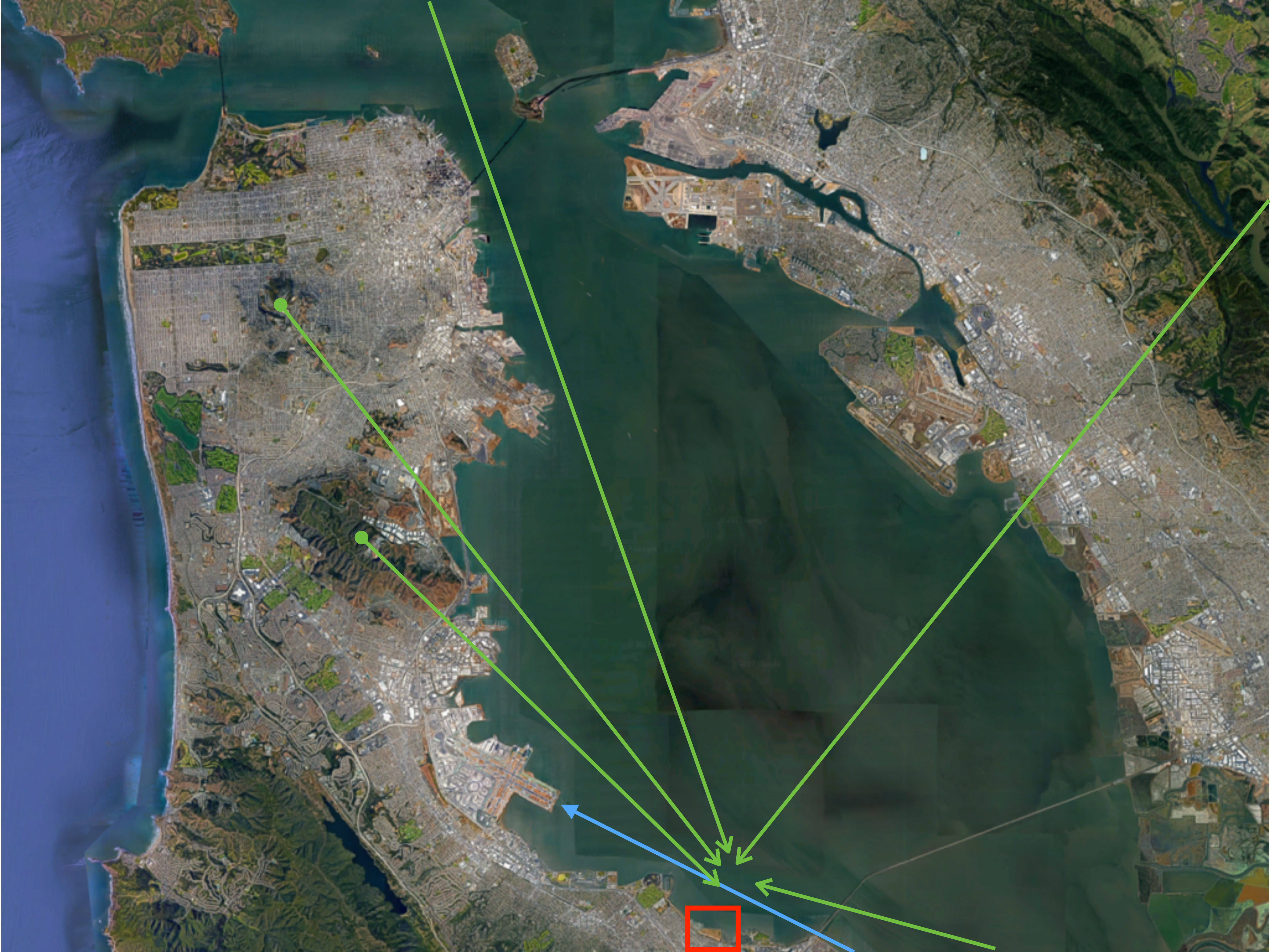

Seal Point Park
Bay Trail
Ryder Court Park
J Hart Clinton Dr
J Hart Clinton Dr
J Hart Clinton Dr
J Hart Clinton Dr
J Hart Clinton
Seal Point Harbor Dog Park
San Francisco Bay Trail
The Bay Trail
Shoreview Ave
Shoreview Ave
Shoreview Ave
Shoreview Ave
Shoreview Ave
Ocean View Ave
Ocean View Ave
Kathryne Ave
Fallon Ave

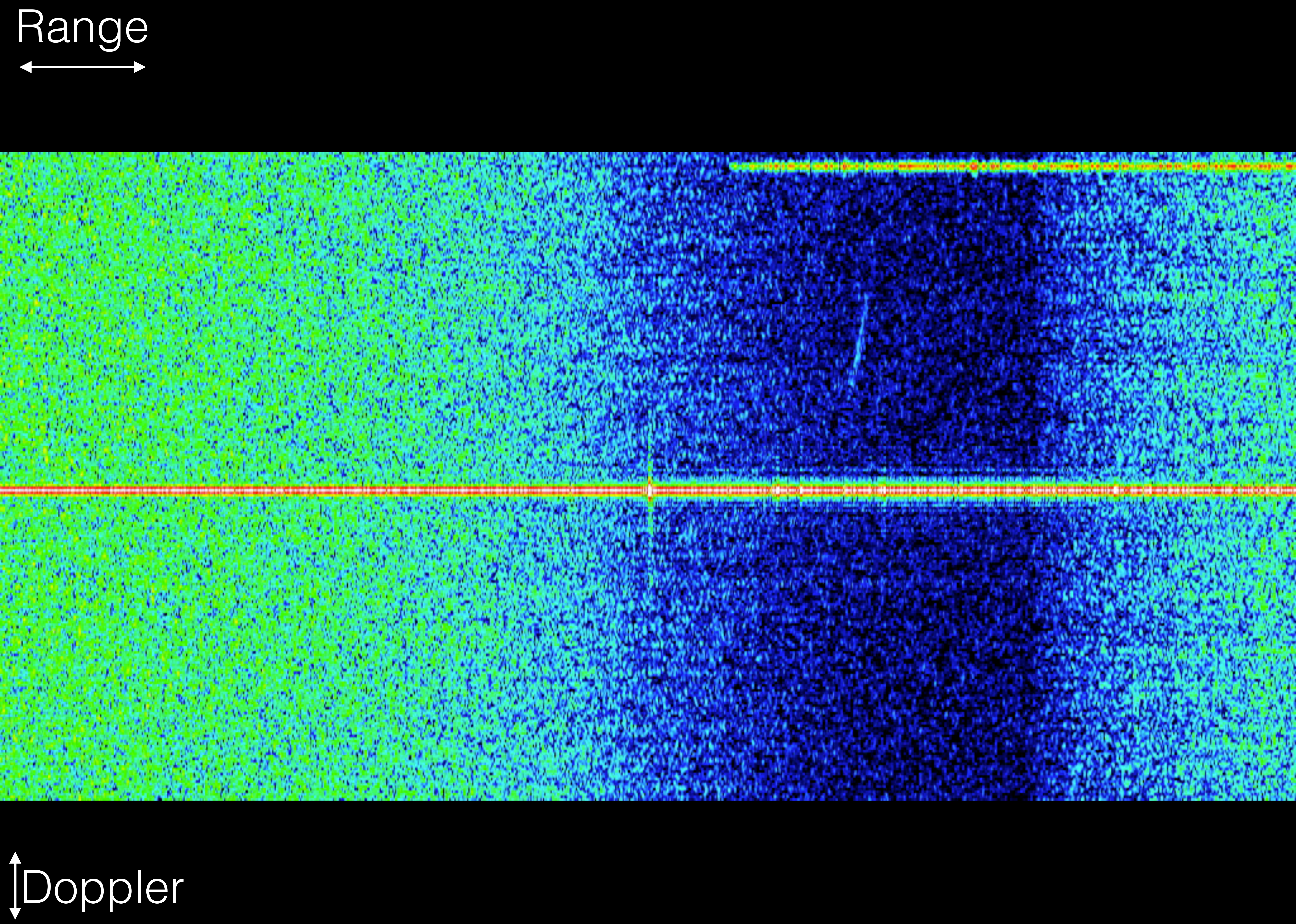
SLOW
Google

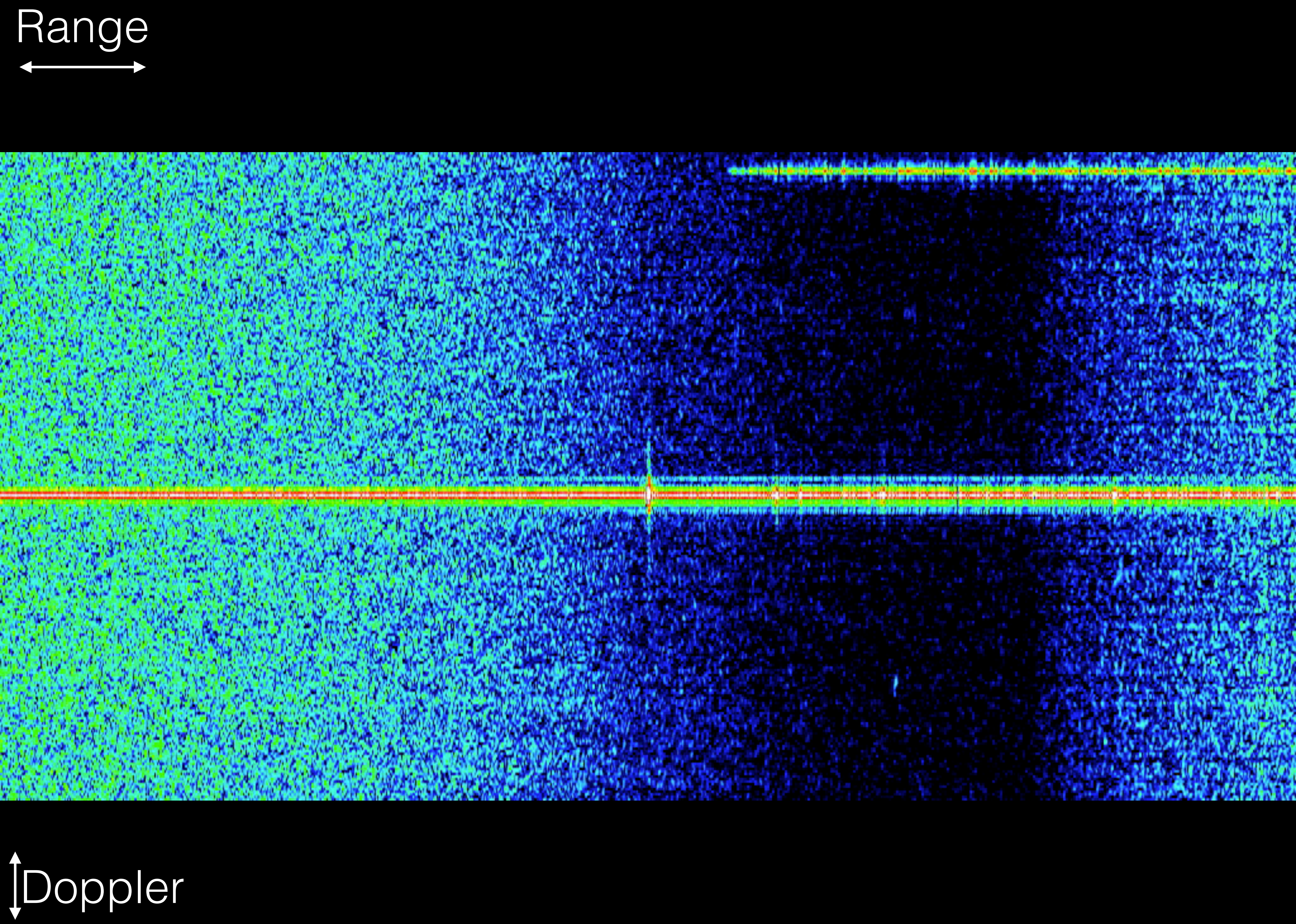

POLO
weboost

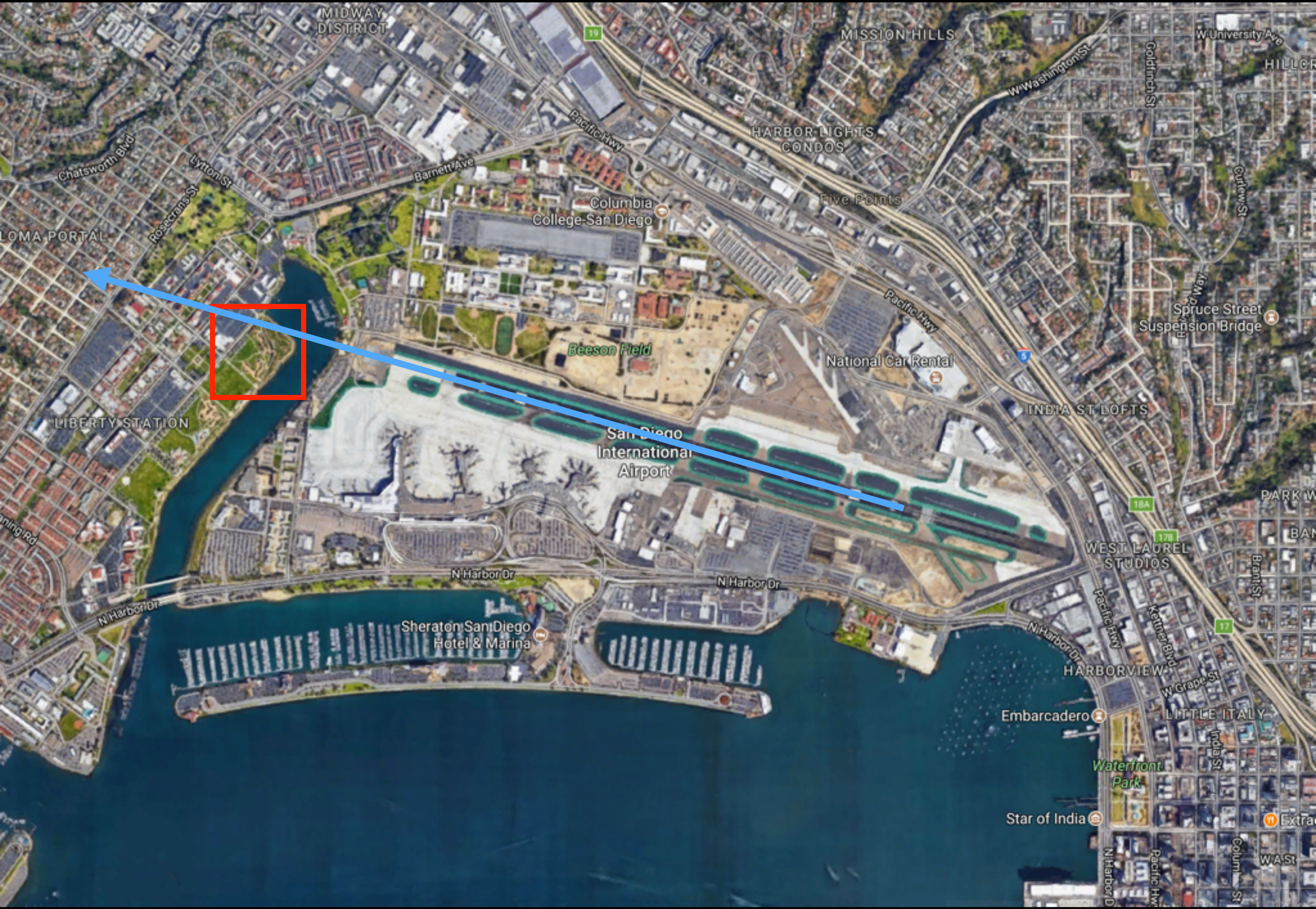
Bistatic Geometry

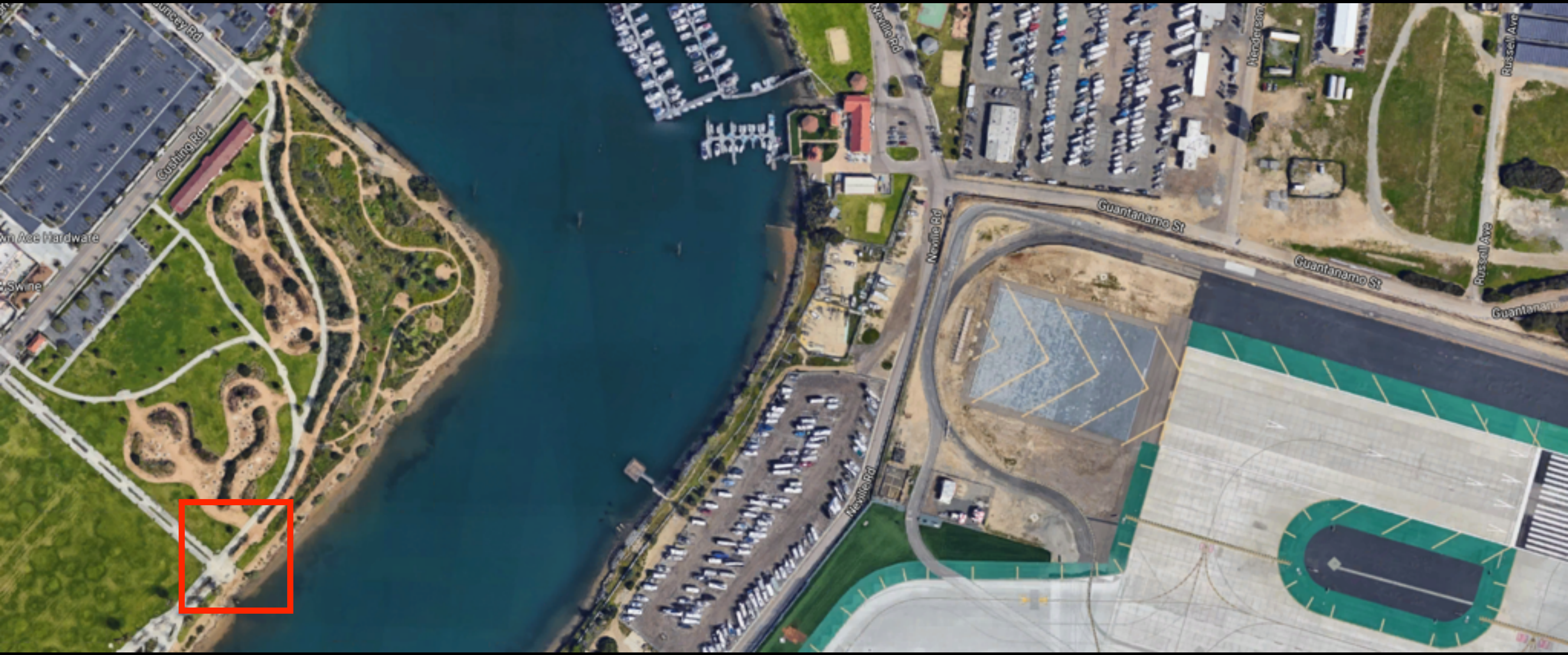
- Range is path from transmitter to object + reflection to receiver
- Important to remind yourself: *not monostatic*
- Factors:
  - Position of transmitter
  - Position of receiver
  - RCS of target (consider surfaces)

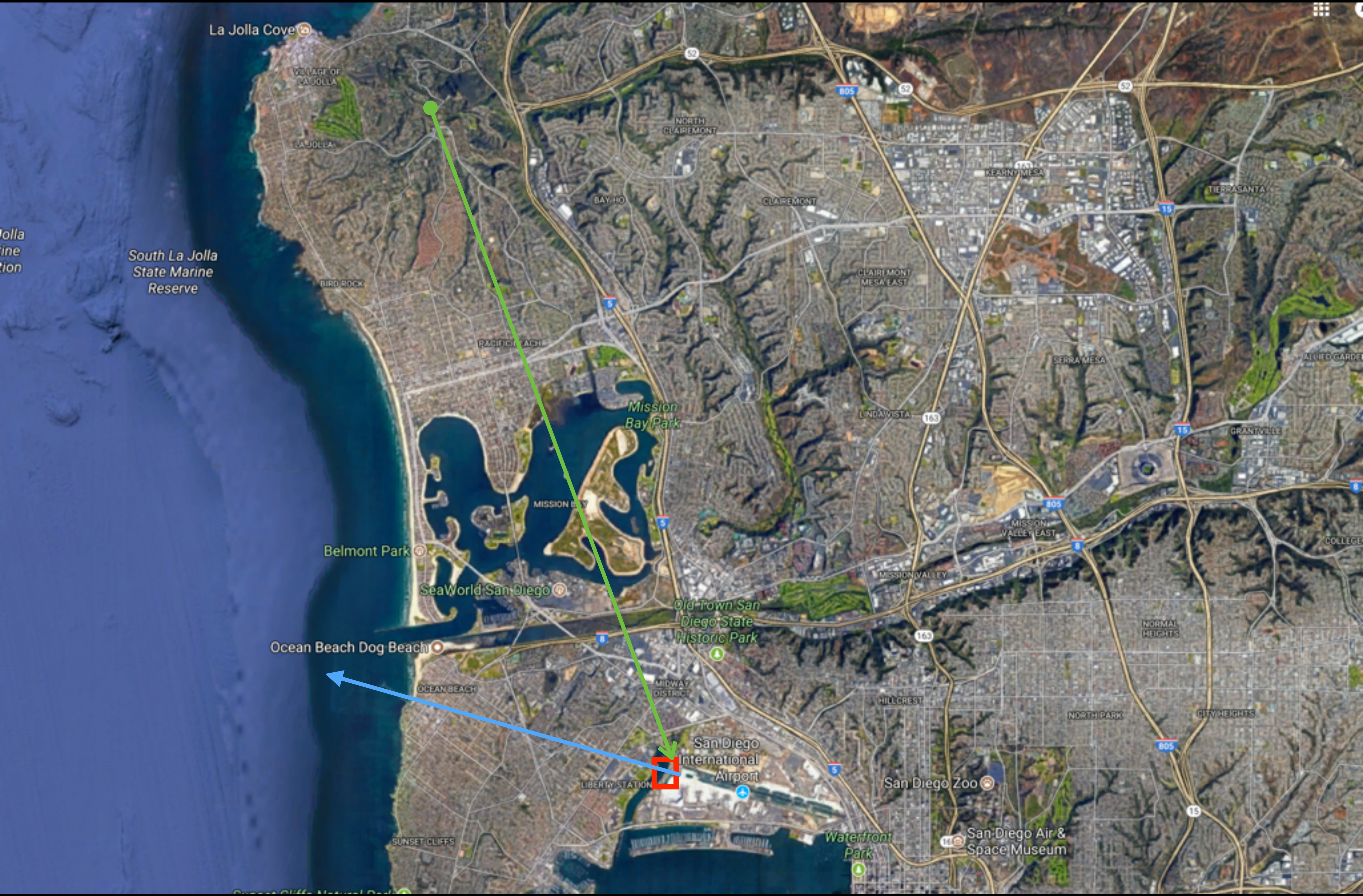


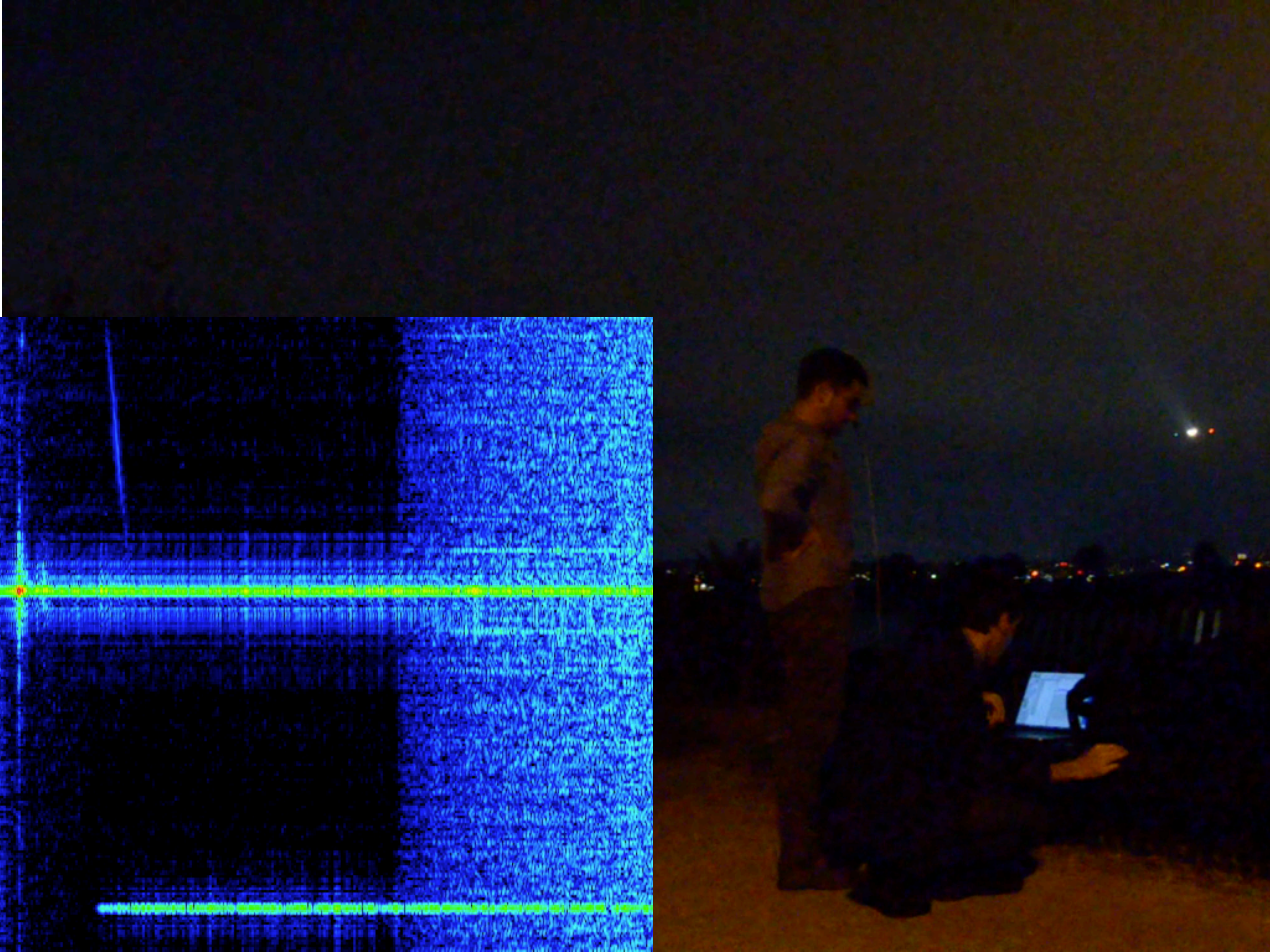

Range
Doppler

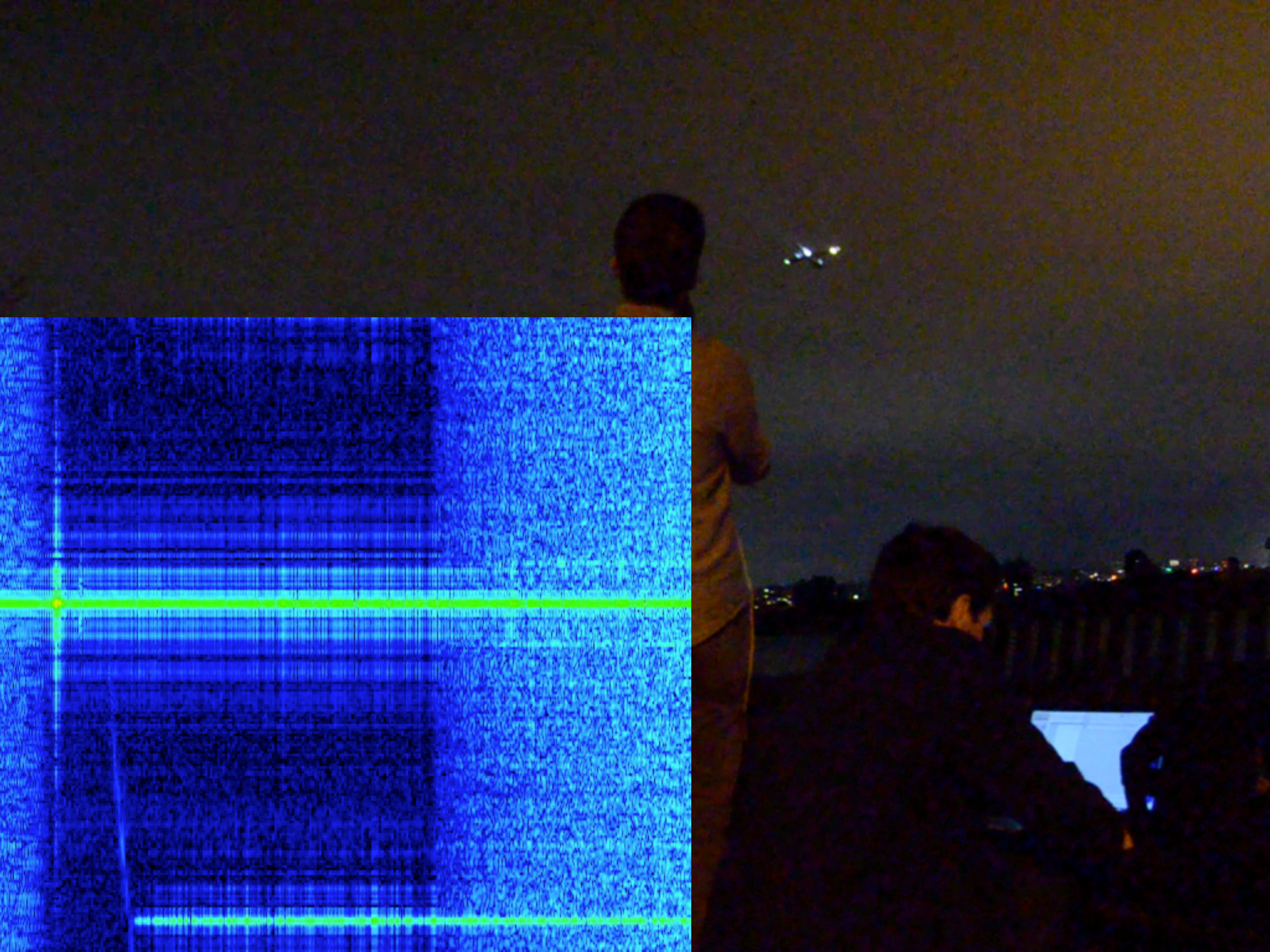

Range
Doppler

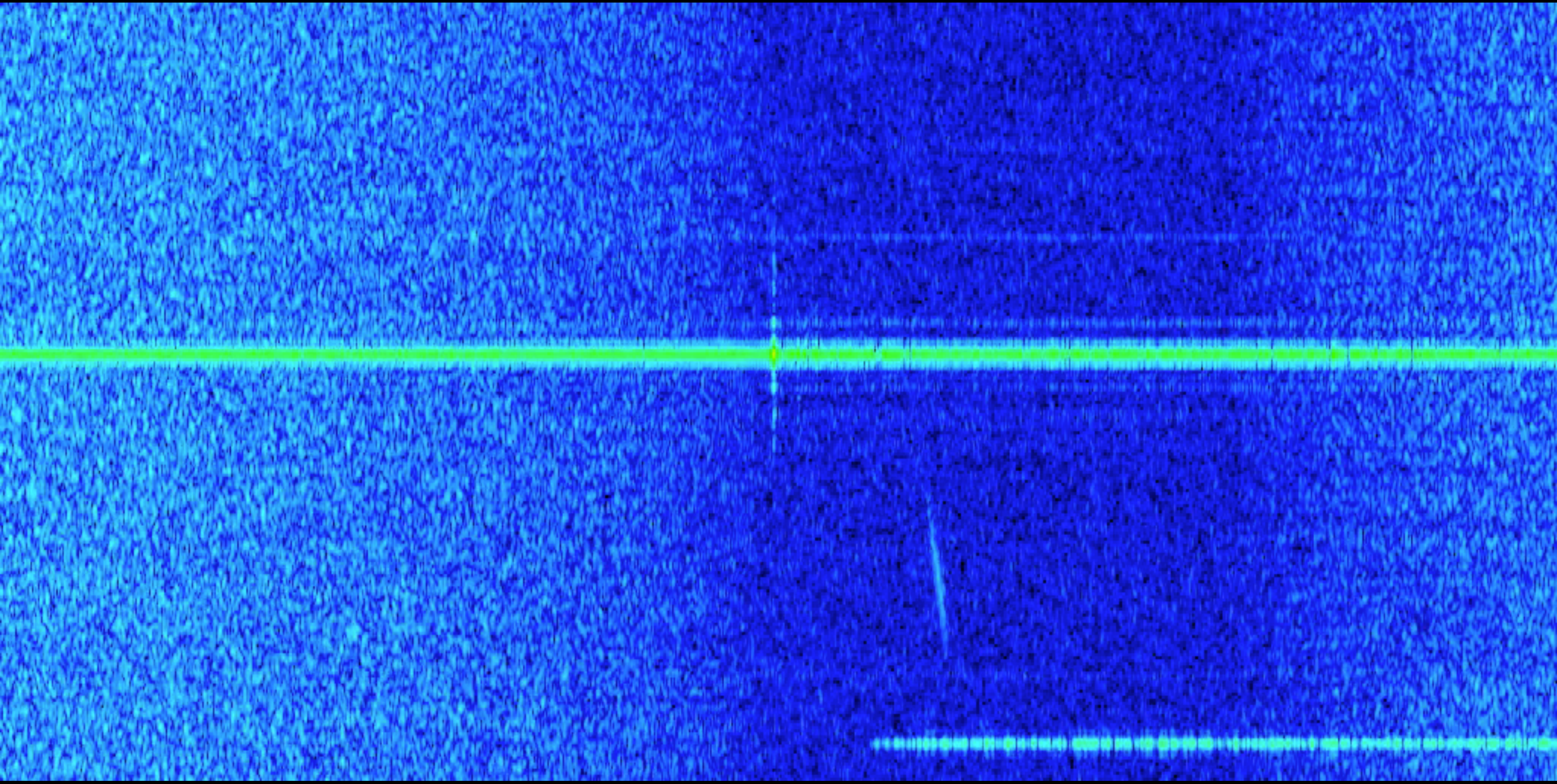

MIDWAY DISTRICT
MISSION HILLS
W University Ave
HILLCR
19
W Washington St
Goldfinch St
HARBOR LIGHTS CONDOS
Pacific Hwy
Barnett Ave
Chatsworth Blvd
Lytton St
Rosecrans St
Columbia College San Diego
Five Points
Curlew St
LOMA PORTAL
Reynard Way
Spruce Street Suspension Bridge
Pacific Hwy
Beeson Field
National Car Rental
5
INDIA ST LOFTS
LIBERTY STATION
San Diego International Airport
PARK W
18A
BAN
ning Rd
17B
WEST LAUREL STUDIOS
Brant St
N Harbor Dr
N Harbor Dr
N Harbor Dr
Pacific Hwy
Kettner Blvd
17
Sheraton San Diego Hotel & Marina
N Harbor Dr
HARBORVIEW
W Grape St
Embarcadero
LITTLE ITALY
India St
Waterfront Park
Star of India
Extra
N Harbor Dr
Pacific Hwy
Columbia St
W A St


uncey Rd
Cushing Rd
wn Ace Hardware
Swine
Neville Rd
Neville Rd
Neville Rd
Henderson
Guantanamo St
Guantanamo St
Guantanam
Russell Ave
Russell Ave


La Jolla Cove
Village of La Jolla
La Jolla
South La Jolla State Marine Reserve
Bird Rock
Pacific Beach
North Clairemont
Bay Ho
Clairemont
Clairemont Mesa East
Kearny Mesa
Tierrasanta
Serra Mesa
Allied Garde
Linda Vista
Grantville
Mission Bay Park
Mission Bay
Mission Valley East
Mission Valley
College
Belmont Park
SeaWorld San Diego
Old Town San Diego State Historic Park
Ocean Beach Dog Beach
Ocean Beach
Midway District
Normal Heights
Hillcrest
North Park
City Heights
San Diego International Airport
Liberty Station
San Diego Zoo
Waterfront Park
San Diego Air & Space Museum
Sunset Cliffs
Sunset Cliffs Natural Park
52
805
5
163
15
8





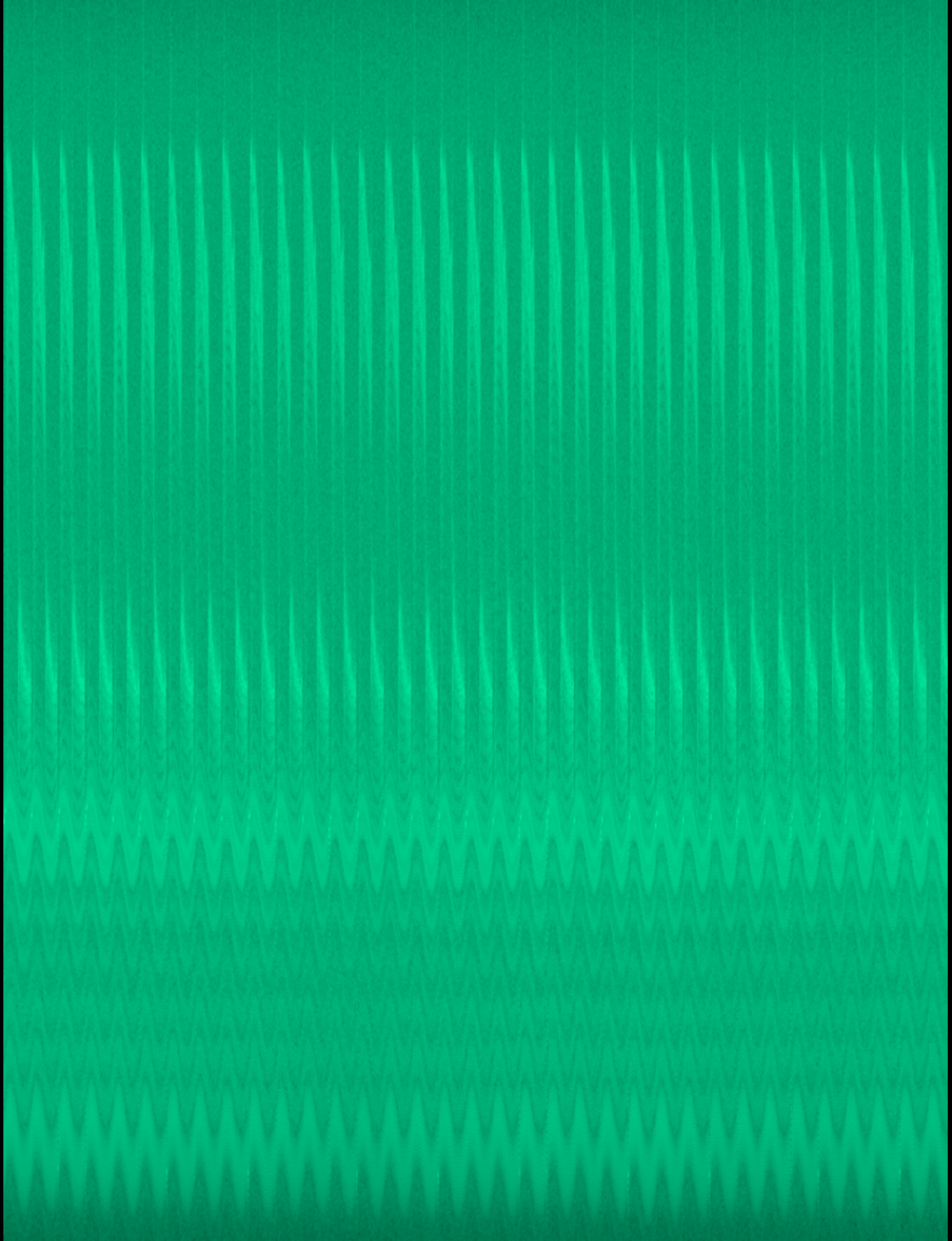


FPV

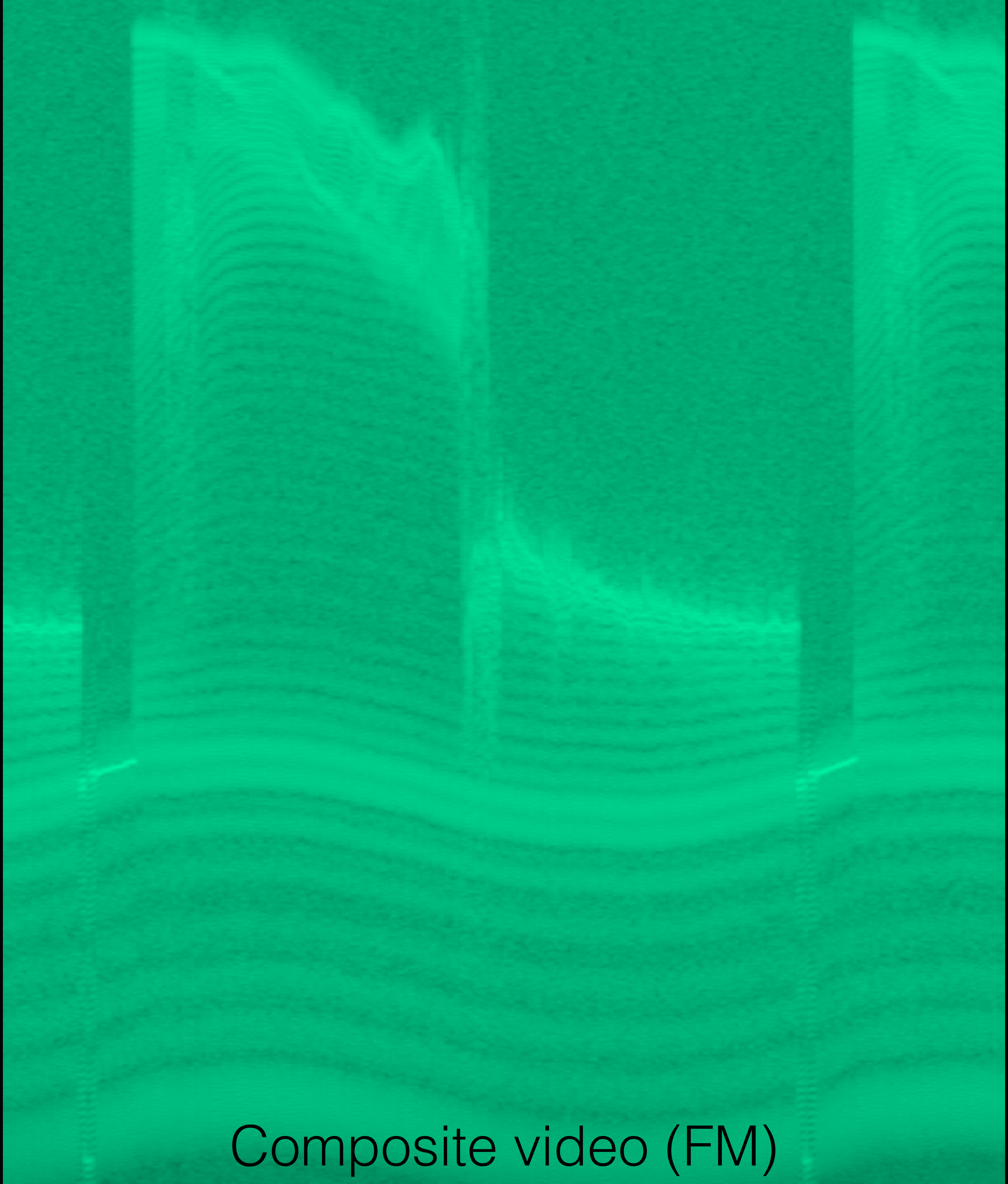
First Person View

- Analog video = low latency (no encoder/decoder delay)
- 5.8 GHz band

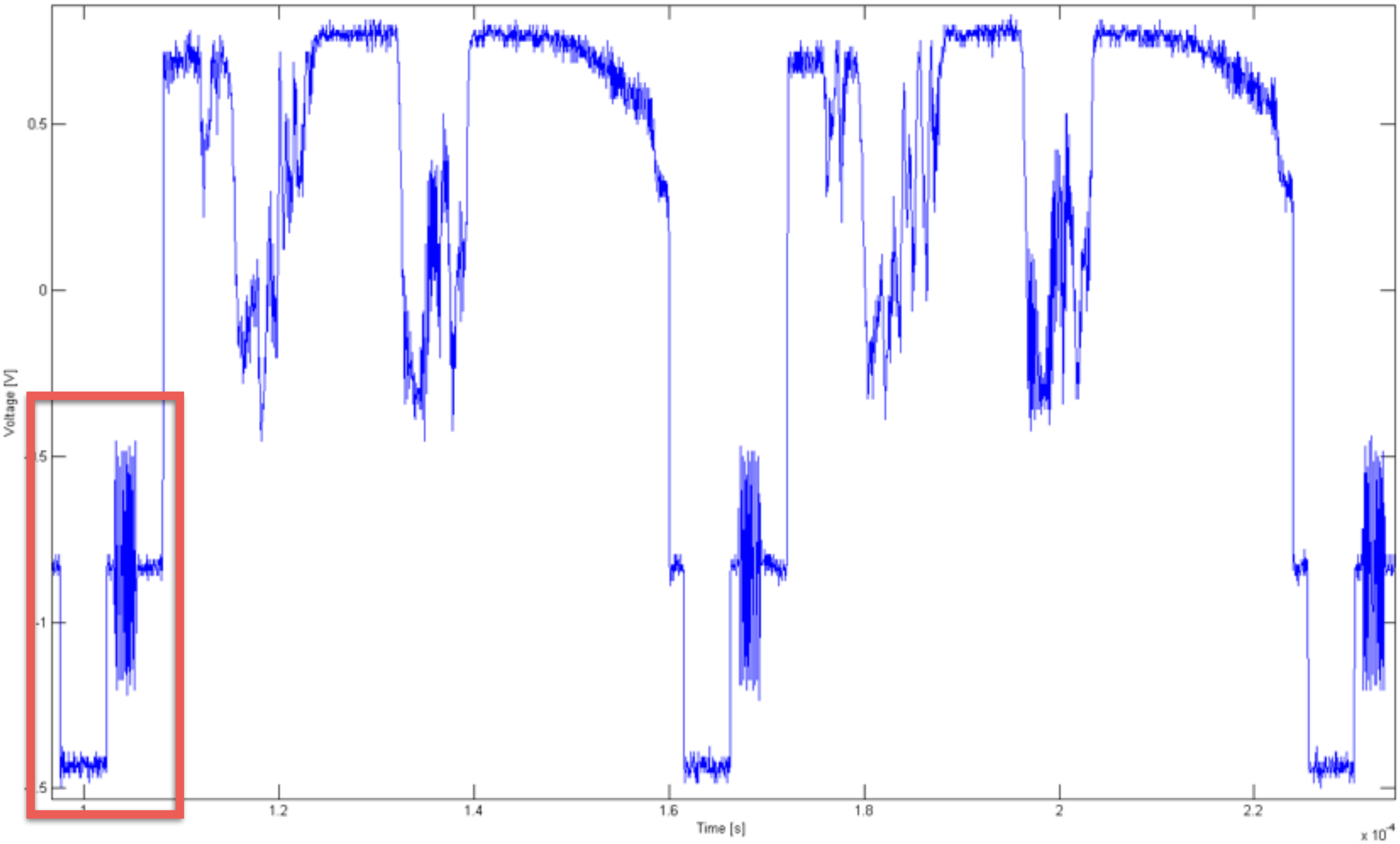
dronepedia.xyz



(Rotated)

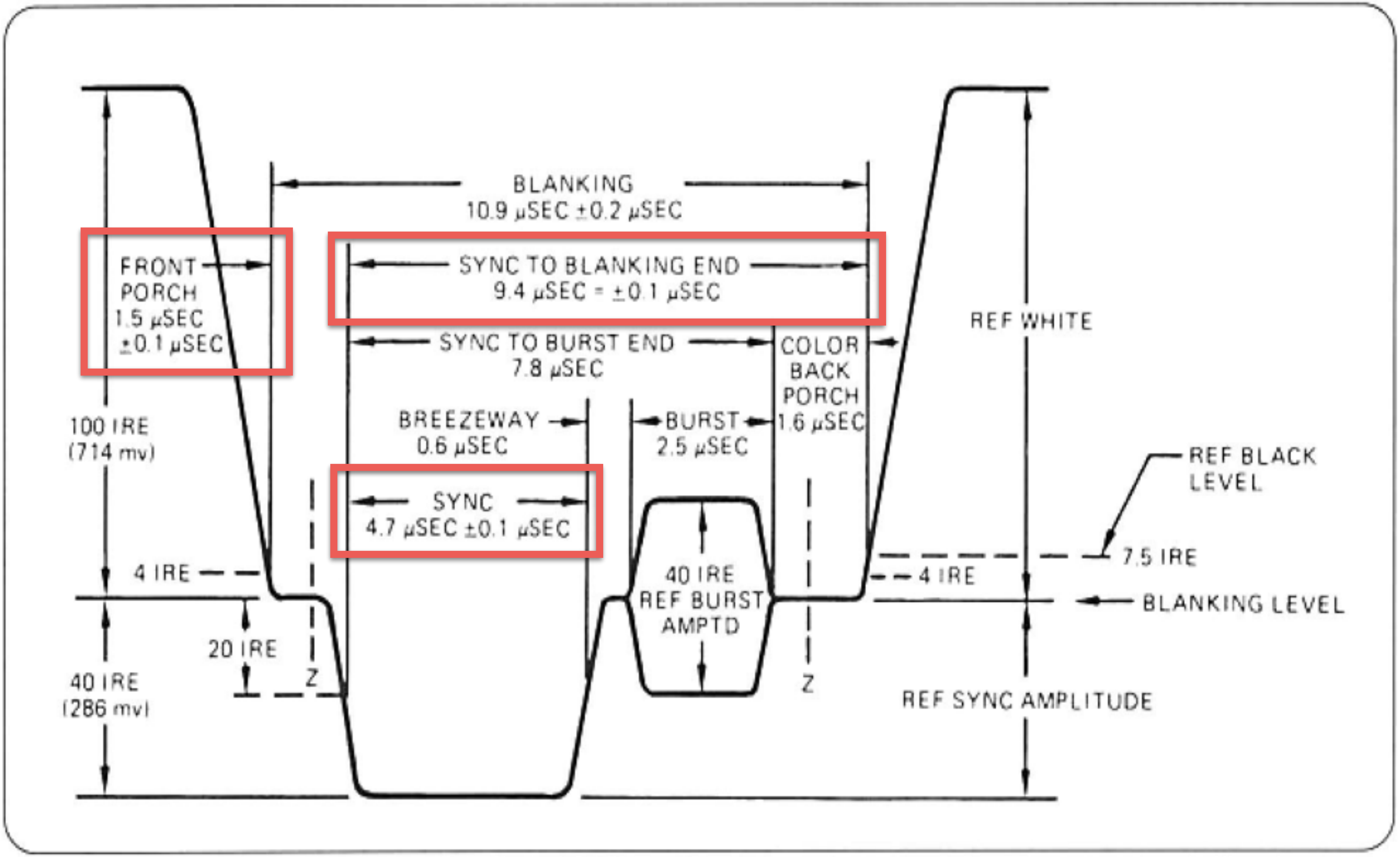


Composite video (FM)



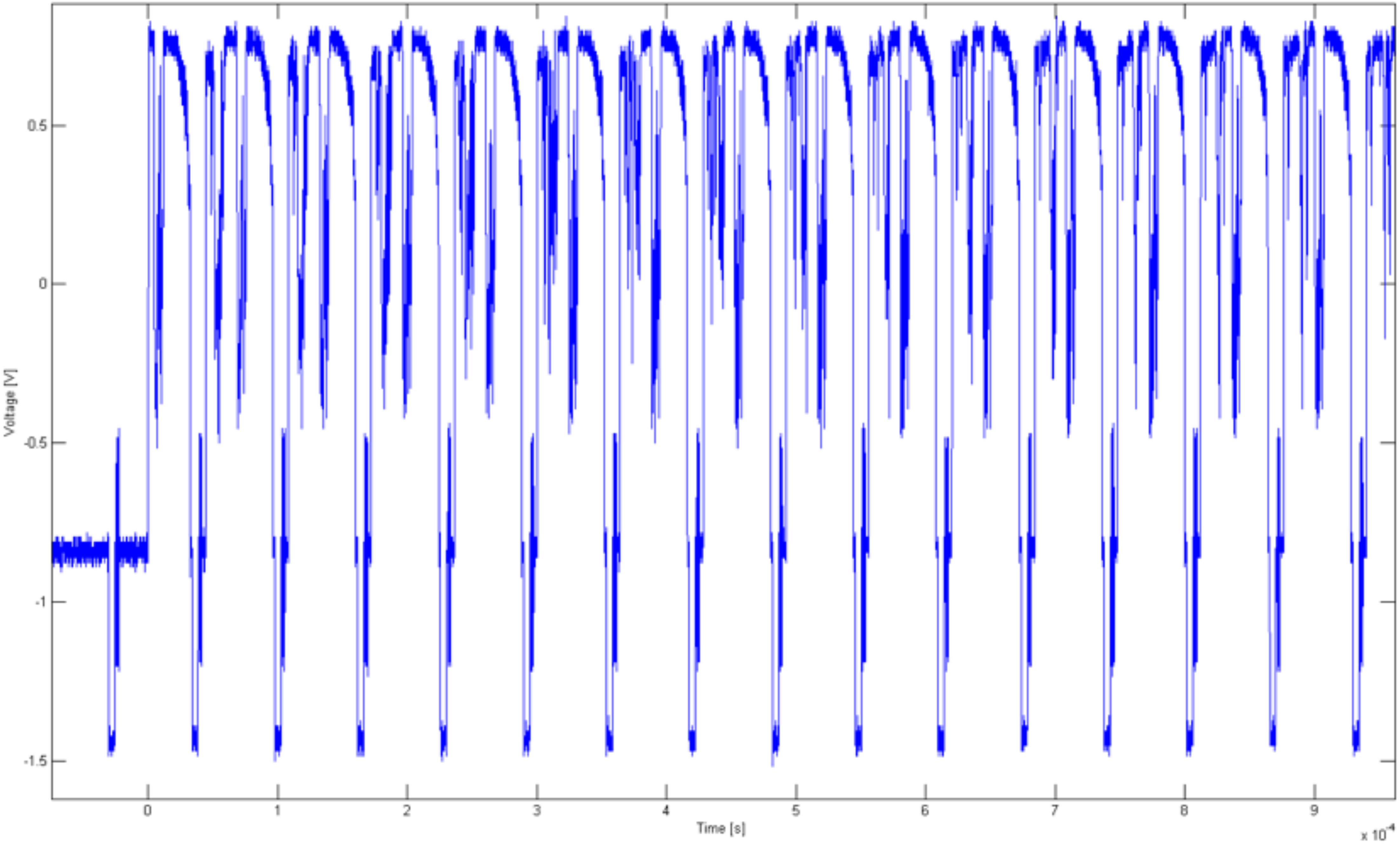
H Sync

Wikipedia

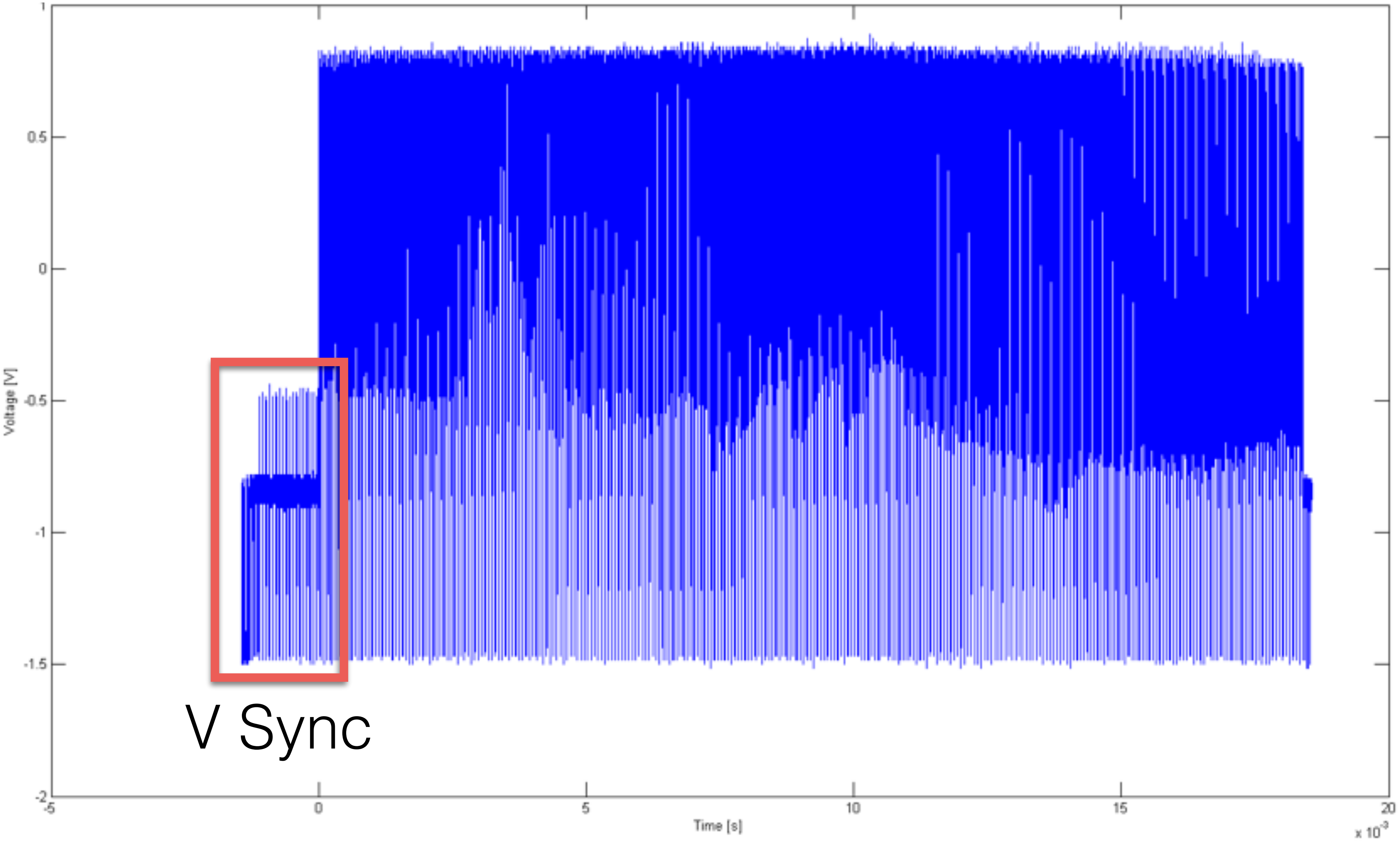


1H = 63.5us

http://www.oocities.org/yehcheang/Composite_horizontal_blanking.htm



Voltage [V]
0.5
0
-0.5
-1
-1.5
0
1
2
3
4
5
6
7
8
9
Time [s]
x 10^-4



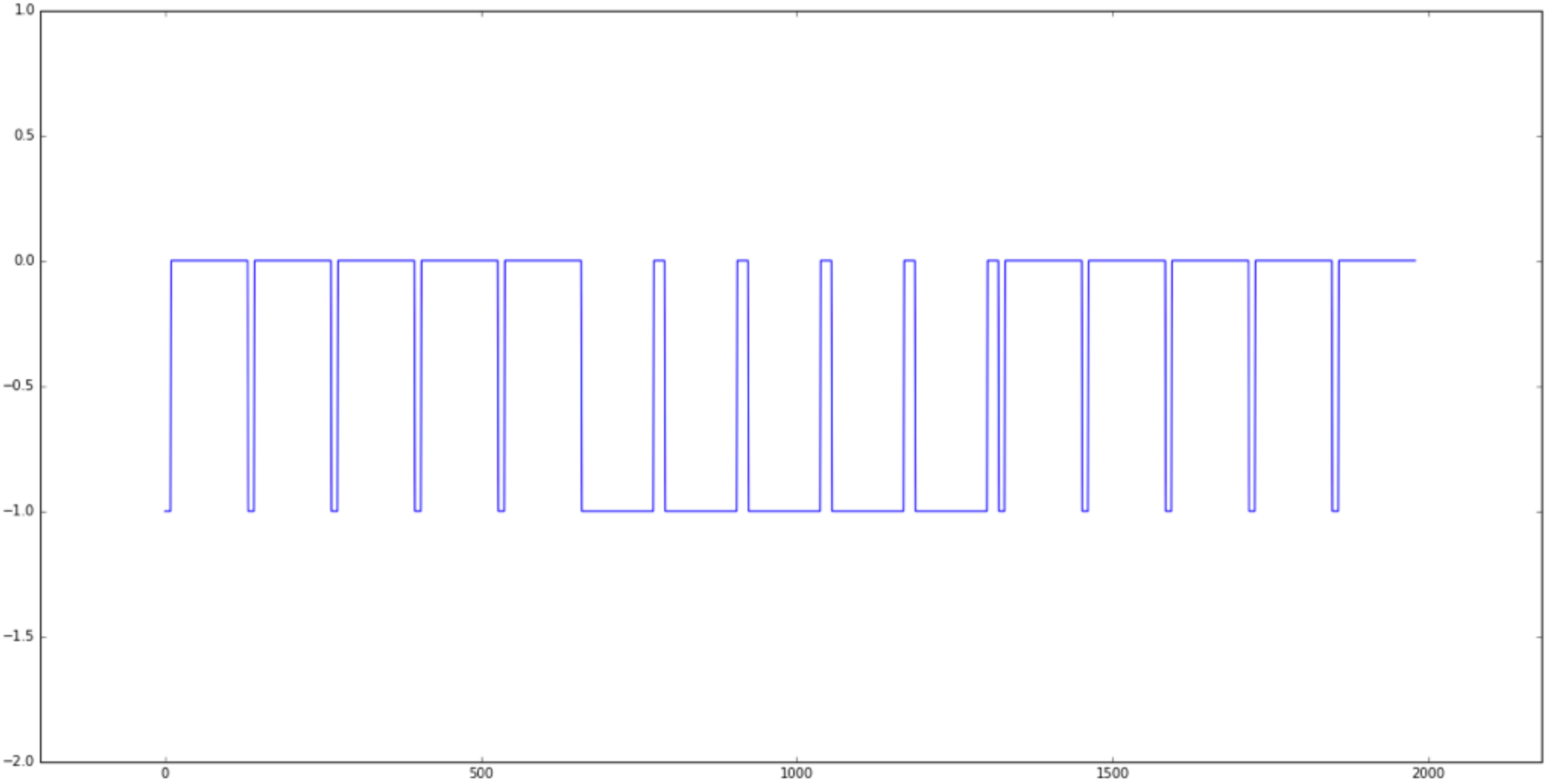
V Sync

Simple Decoder

- Black & white (luminance only)
- Matched filter for vertical sync
- Read out fixed number of samples for raster
- Adapt resampler to match expected vertical sync rate
- Handle interlacing (even/odd fields)

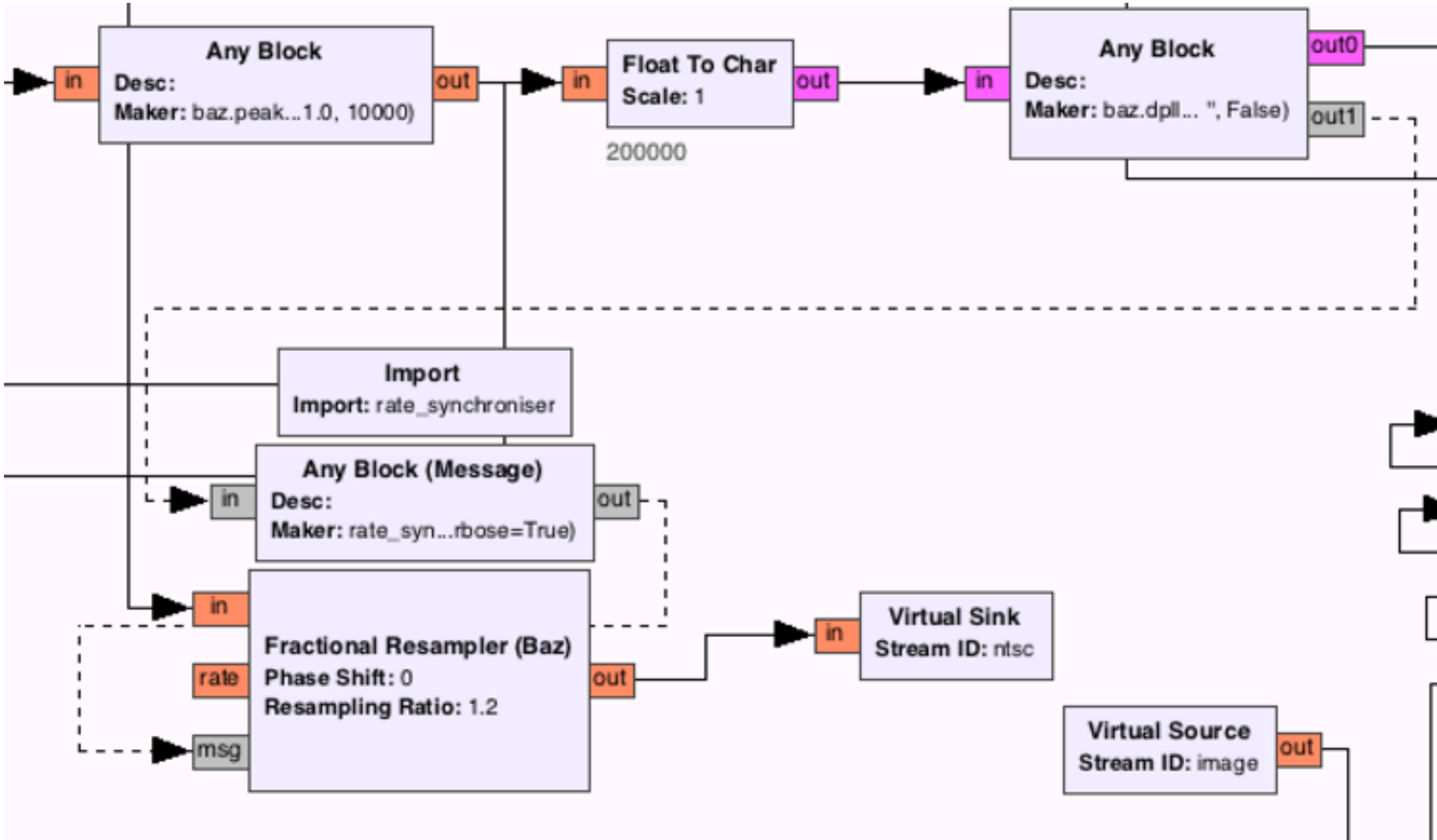
Vertical Sync Matched Filter

- Determine even/odd field immediately after V Sync



Rate matching

- V Sync filter output fed to peak detector
- DPLL locks to pulses
- Rate Synchroniser uses DPLL period & target rate



Any Block
Desc:
Maker: baz.peak...1.0, 10000)

Float To Char
Scale: 1

200000

Any Block
Desc:
Maker: baz.dpll... '', False)

Import
Import: rate_synchroniser

Any Block (Message)
Desc:
Maker: rate_syn...rbose=True)

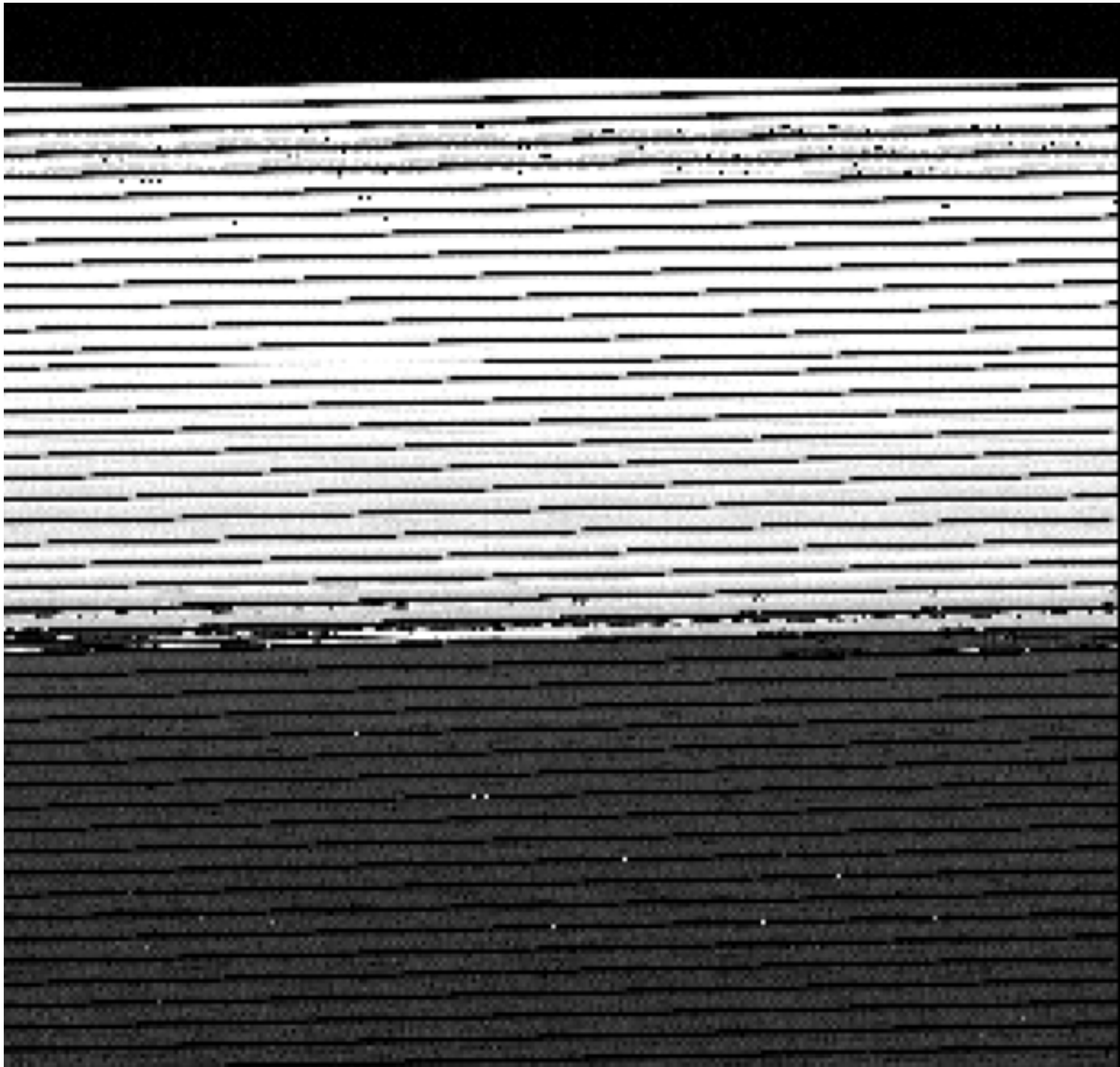
Fractional Resampler (Baz)
Phase Shift: 0
Resampling Ratio: 1.2

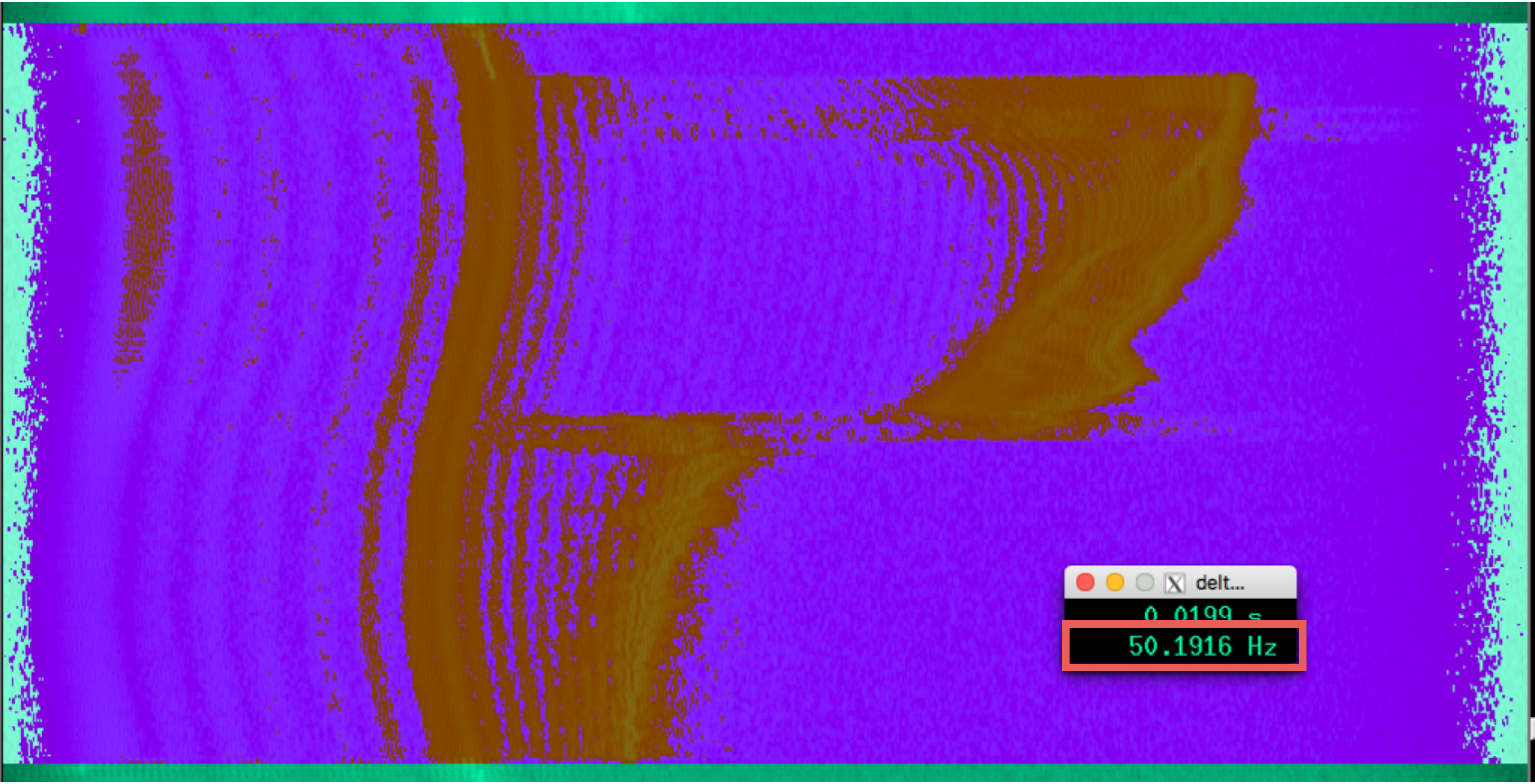
Virtual Sink
Stream ID: ntsc

Virtual Source
Stream ID: image

Not Quite…

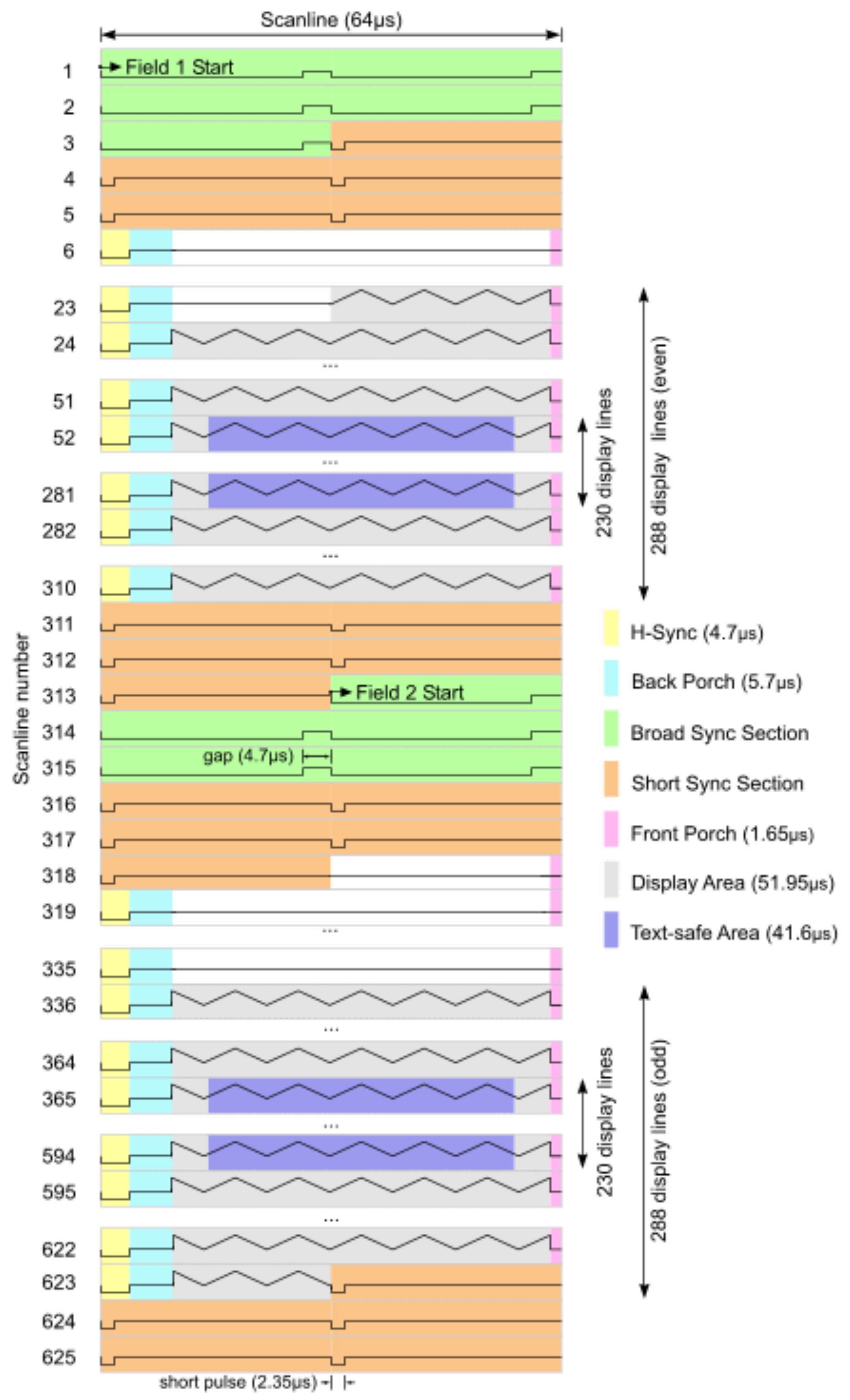
- Wouldn’t lock



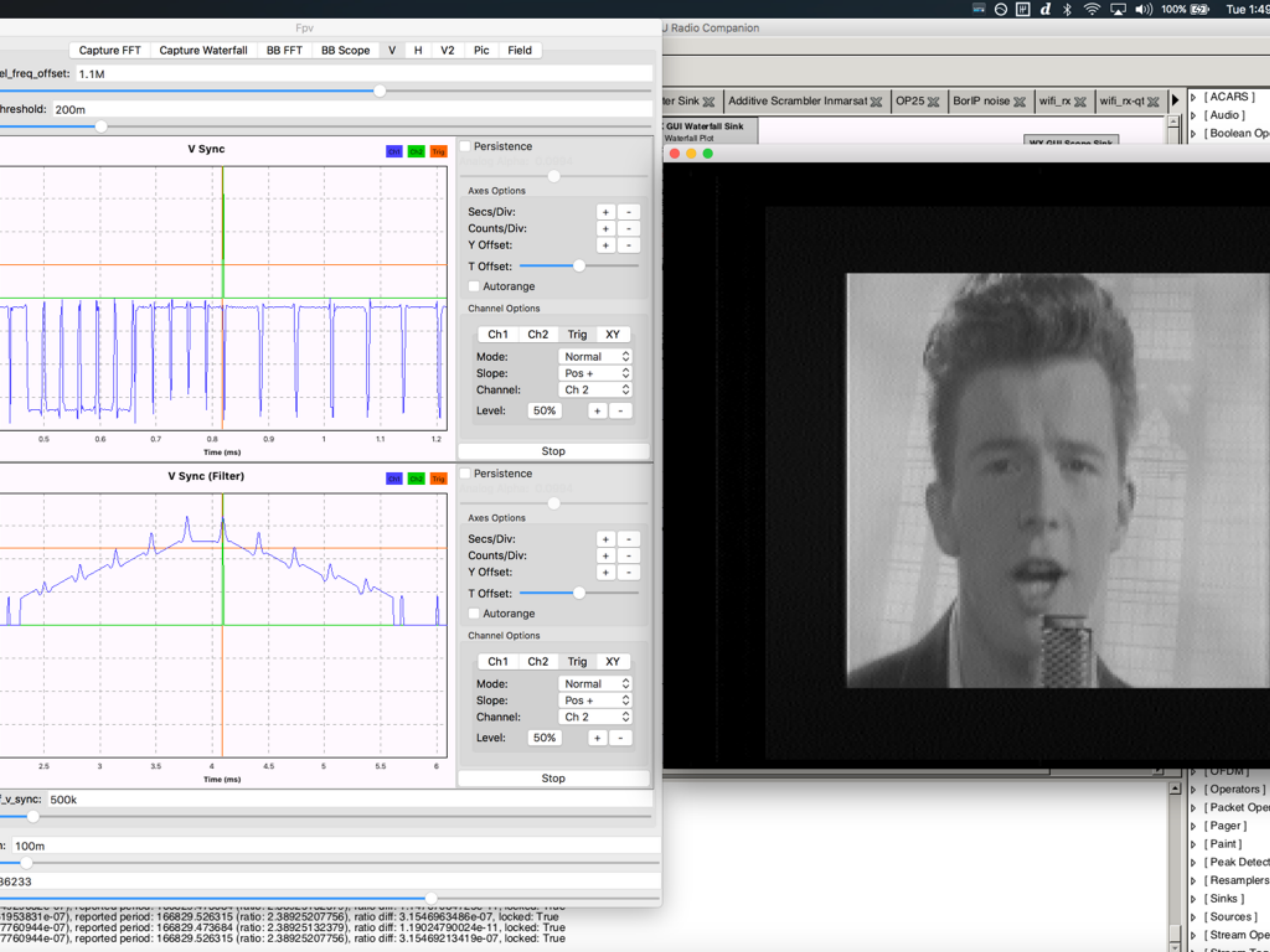


```
0.0199 s
50.1916 Hz
```

It’s not NTSC, it’s PAL!



//www.batsocks.co.uk/readme/video_timing.htm



el_freq_offset: 1.1M

hreshold: 200m

Mode: Normal
Slope: Pos +
Channel: Ch 2
Level: 50%

Mode: Normal
Slope: Pos +
Channel: Ch 2
Level: 50%

f_v_sync: 500k

n: 100m

36233

```
1953831e-07), reported period: 166829.526315 (ratio: 2.38925207756), ratio diff: 3.1546963486e-07, locked: True
7760944e-07), reported period: 166829.473684 (ratio: 2.38925132379), ratio diff: 1.19024790024e-11, locked: True
7760944e-07), reported period: 166829.526315 (ratio: 2.38925207756), ratio diff: 3.15469213419e-07, locked: True
```

Thank you!

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

@spenchdotnet

balint@bastille.net

GitHub: balint256

GitHub: BastilleResearch

Bastille