Hacking the Wireless World with Software Defined Radio – 2.0+

Balint Seeber, Director of Vulnerability Research

balint@bastille.io
balint@spench.net
@spenchdotnet

Bastille

Overview

- Drones & FPV
- Vehicular Keyless Entry
- Multi-path

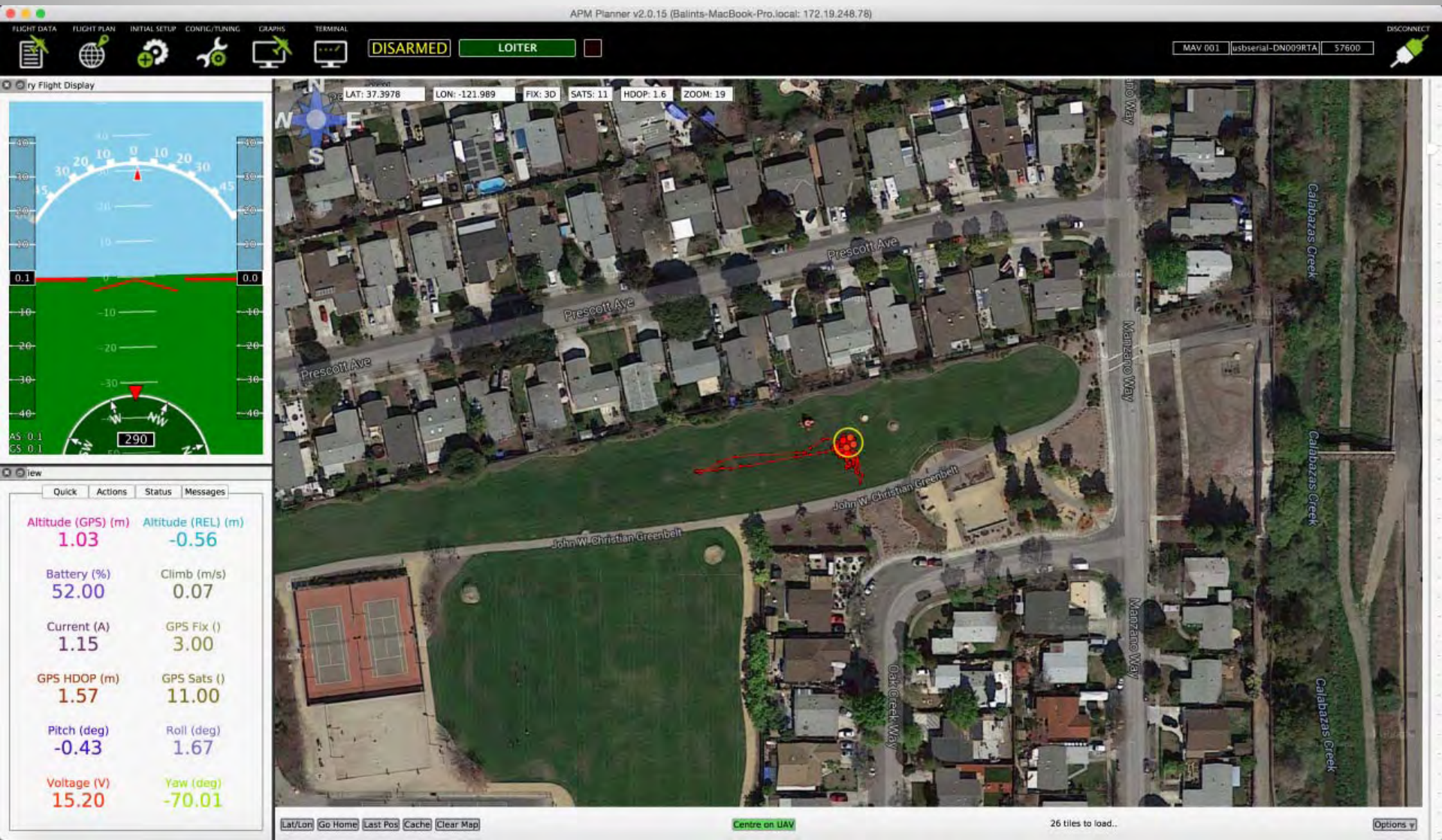
Drones & FPV

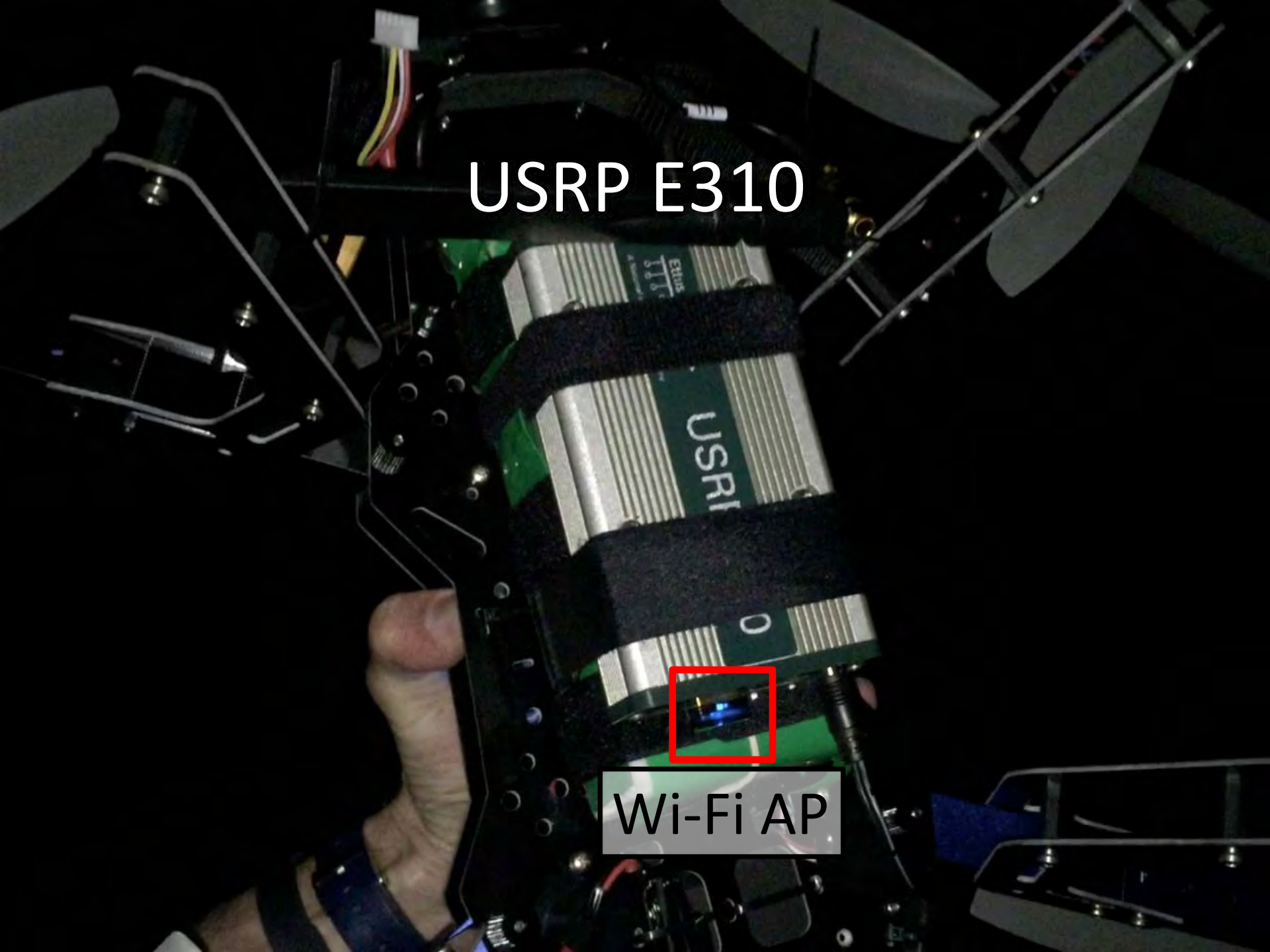

Berkeley Drone meetup


Sniffing RF uplink &
downlink with B210


3DR X8+

Live Telemetry

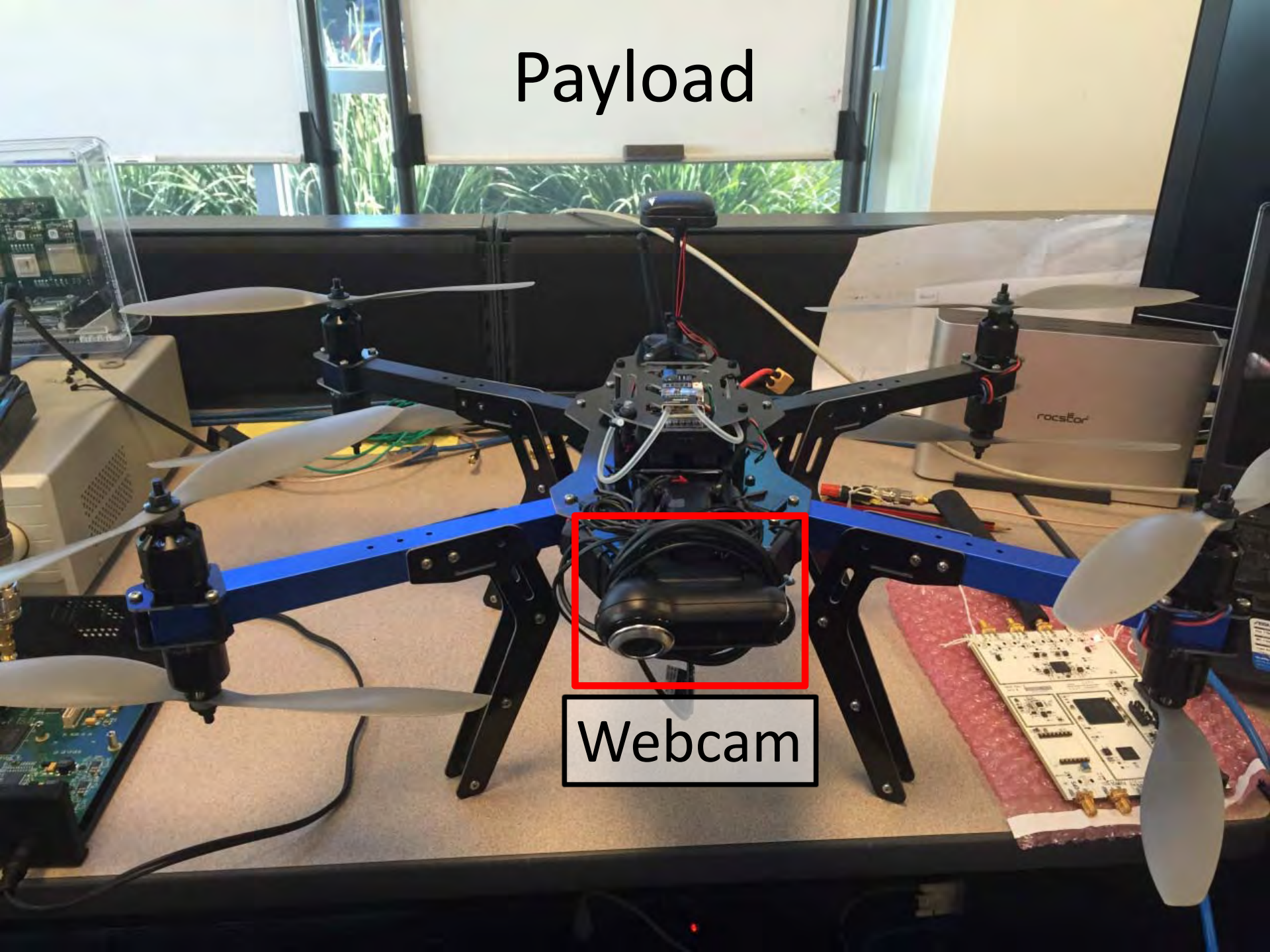


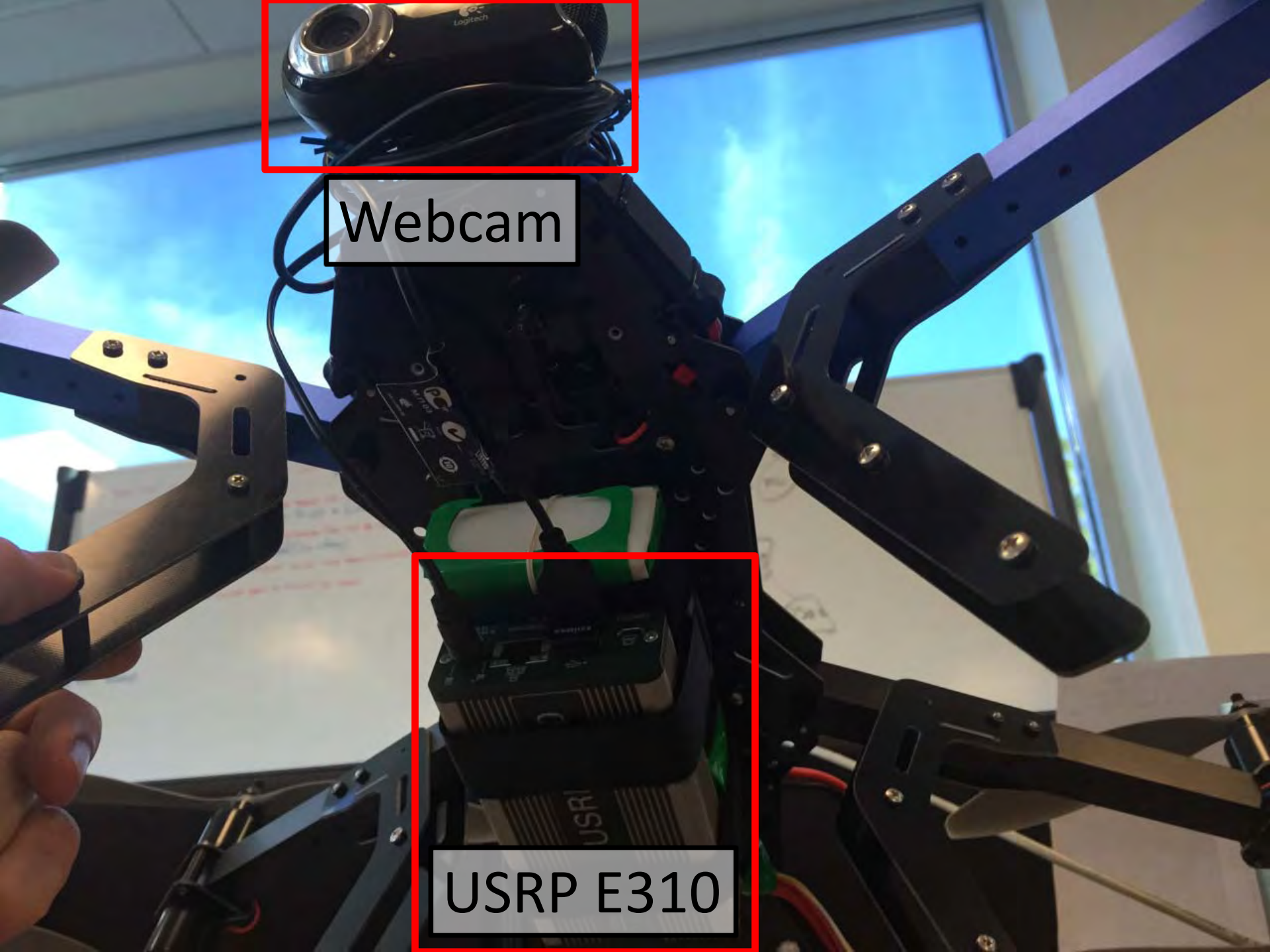

USRP E310
Wi-Fi AP

FPV

Frequency Management: Don't Wreck Your Neighbor's Drone

By Tyler Winegarner March 3rd, 2015 3:12 pm Category Electronics, Robotics


Payload
Webcam


Webcam
USRP E310

System Components

Transmitter

- Image acquisition
- Packetisation & framing
- Modulation

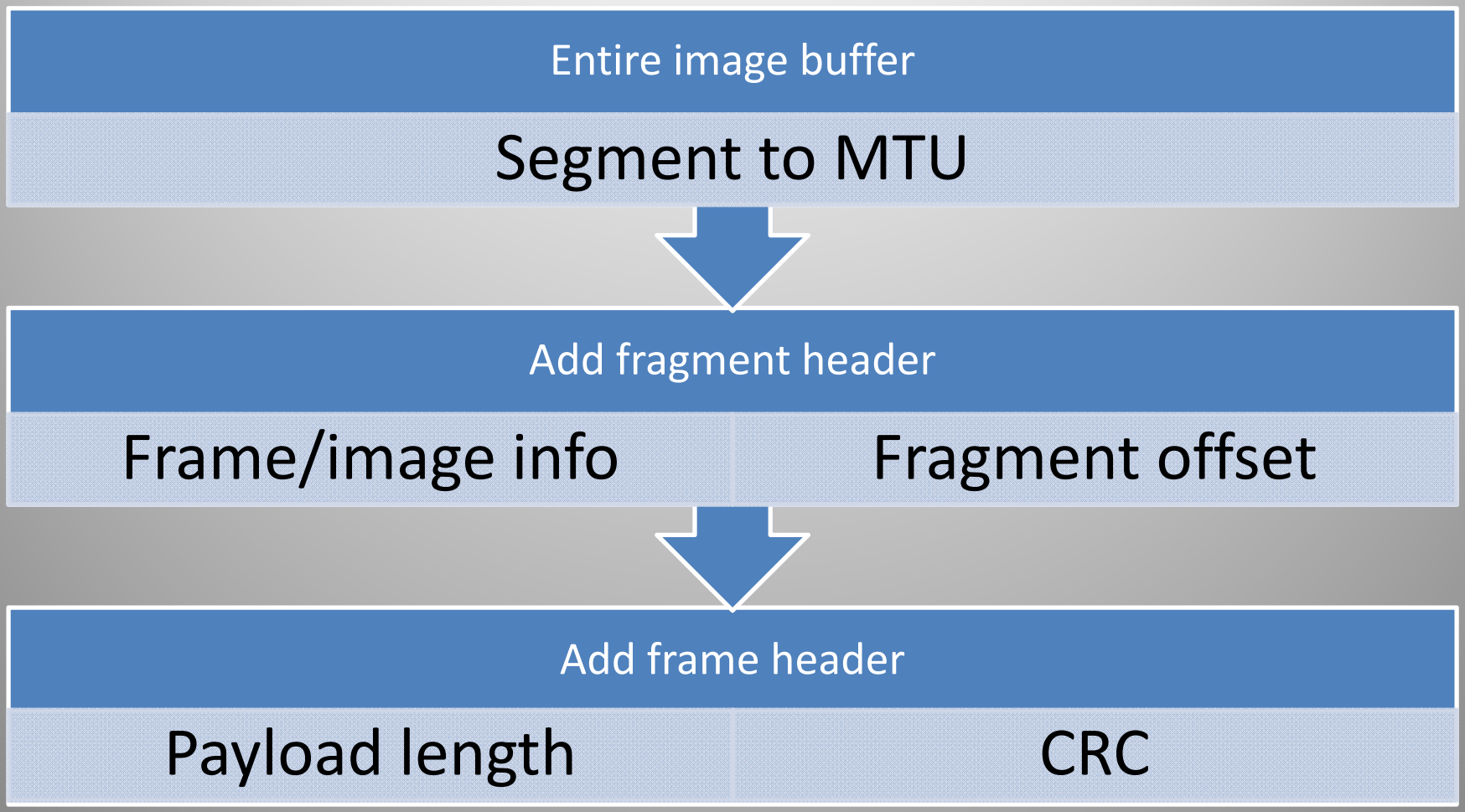
Receiver

- Demodulation
- Deframing
- Image display

Image Acquisition

- v4l: Video for Linux
- Webcam
  - Raw
  - MJPEG: Motion JPEG
  - (H264 on C920)
- Python: python-v4l2capture
- Get image buffer

Packetisation & Framing



Frame structure

Packet

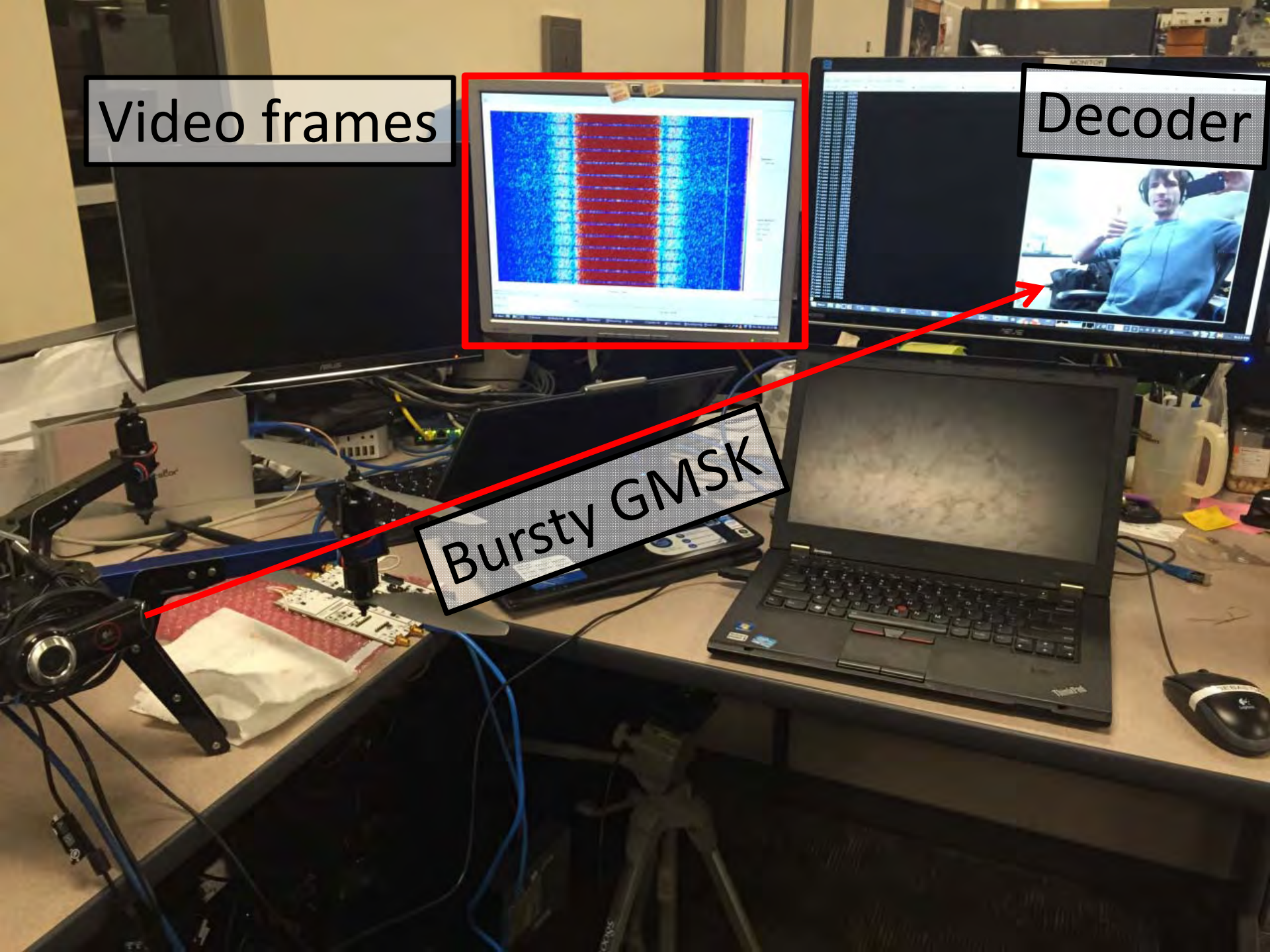
- Preamble
- Access code
- Length
- Whitener index
- CRC

Image fragment

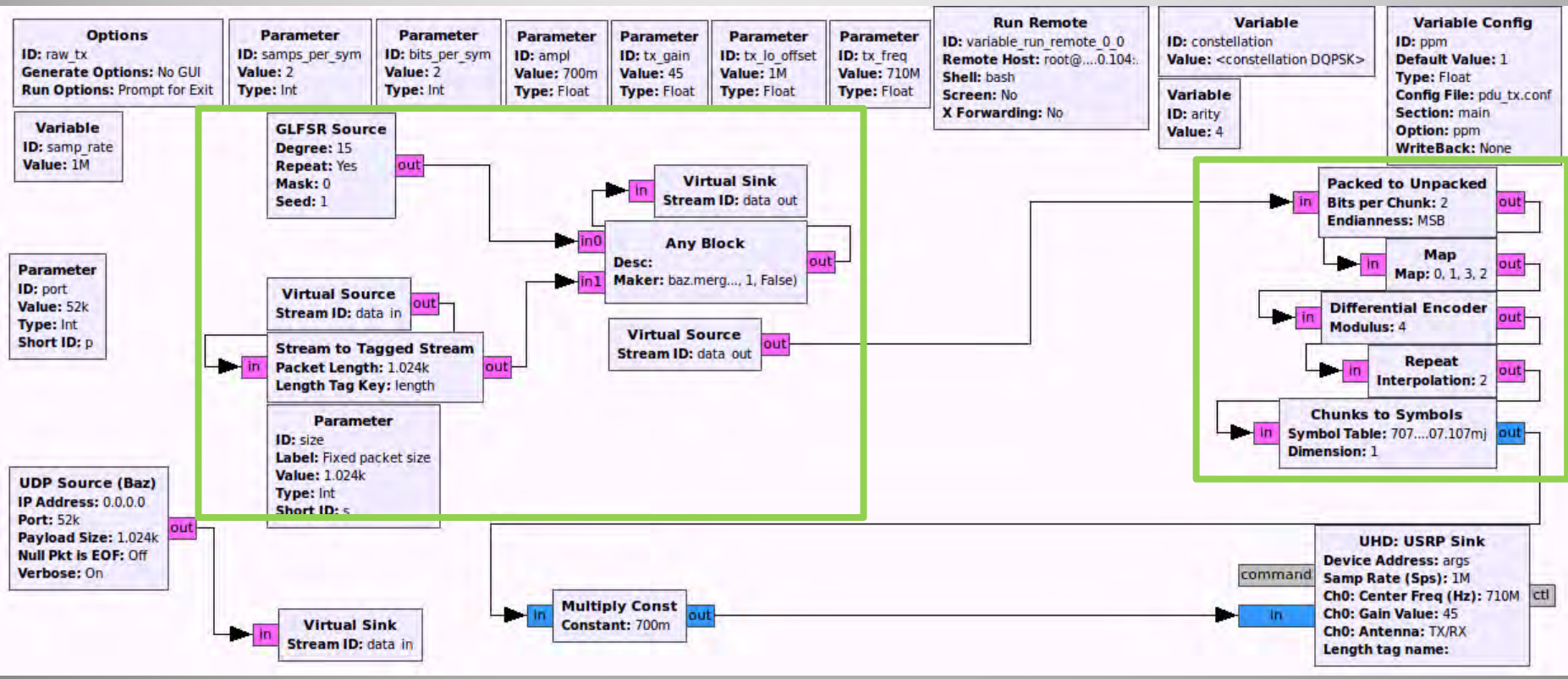
- FOURCC
- Resolution
- Sequence #
- Total frame size
- Fragment length
- Offset

Payload

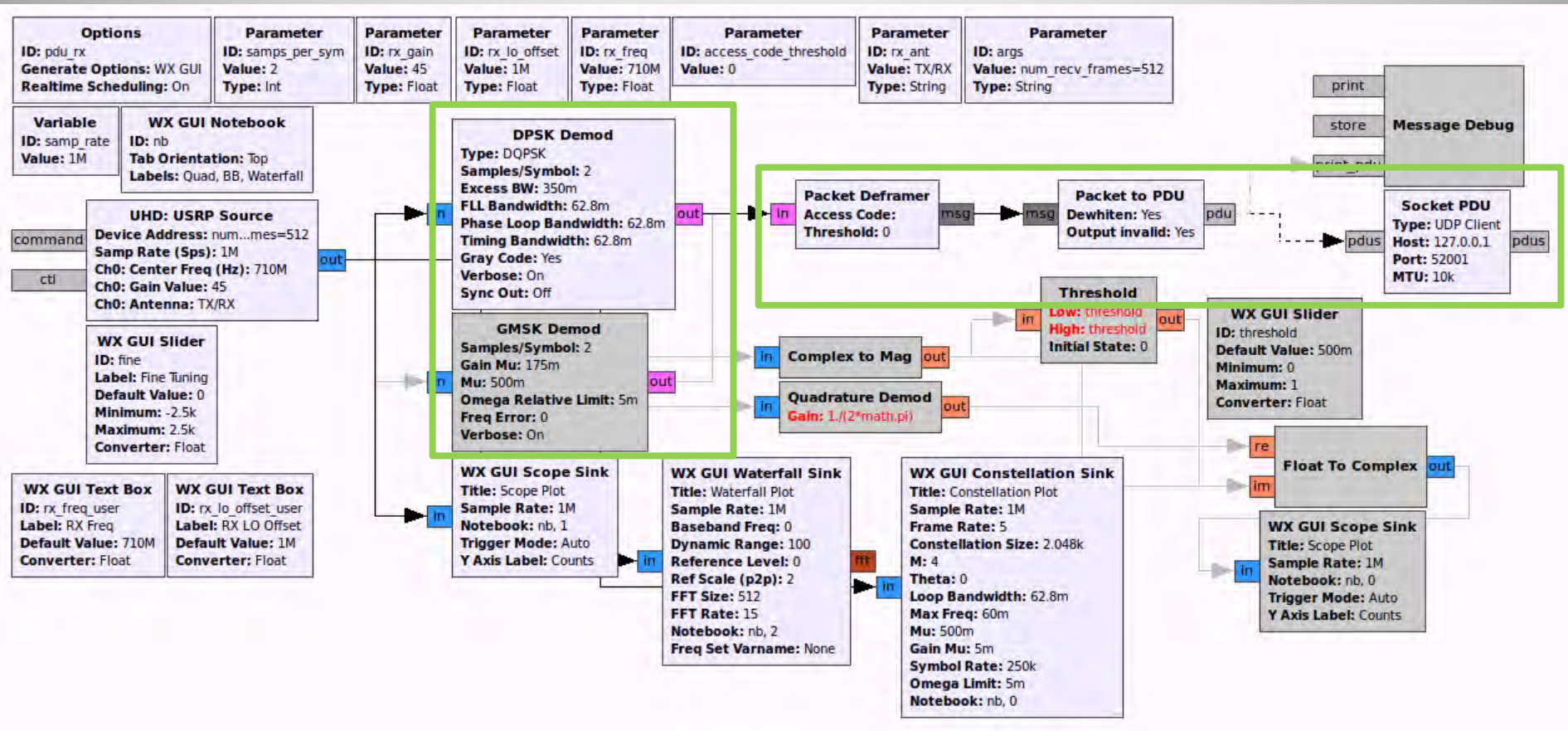
- Image fragment


Video frames
Decoder
Bursty GMSK

TX Flowgraph



RX Flowgraph

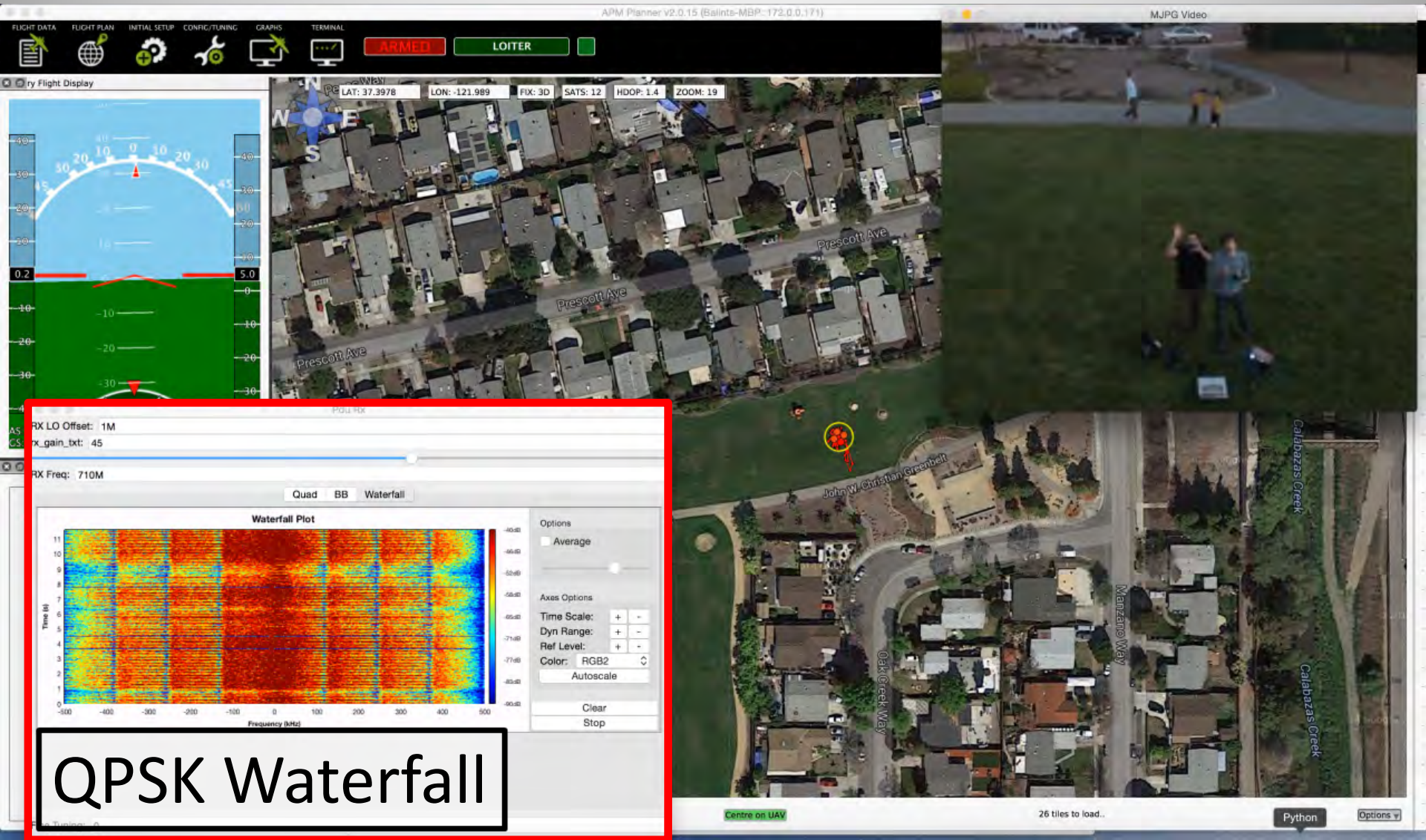


First Outdoor Test

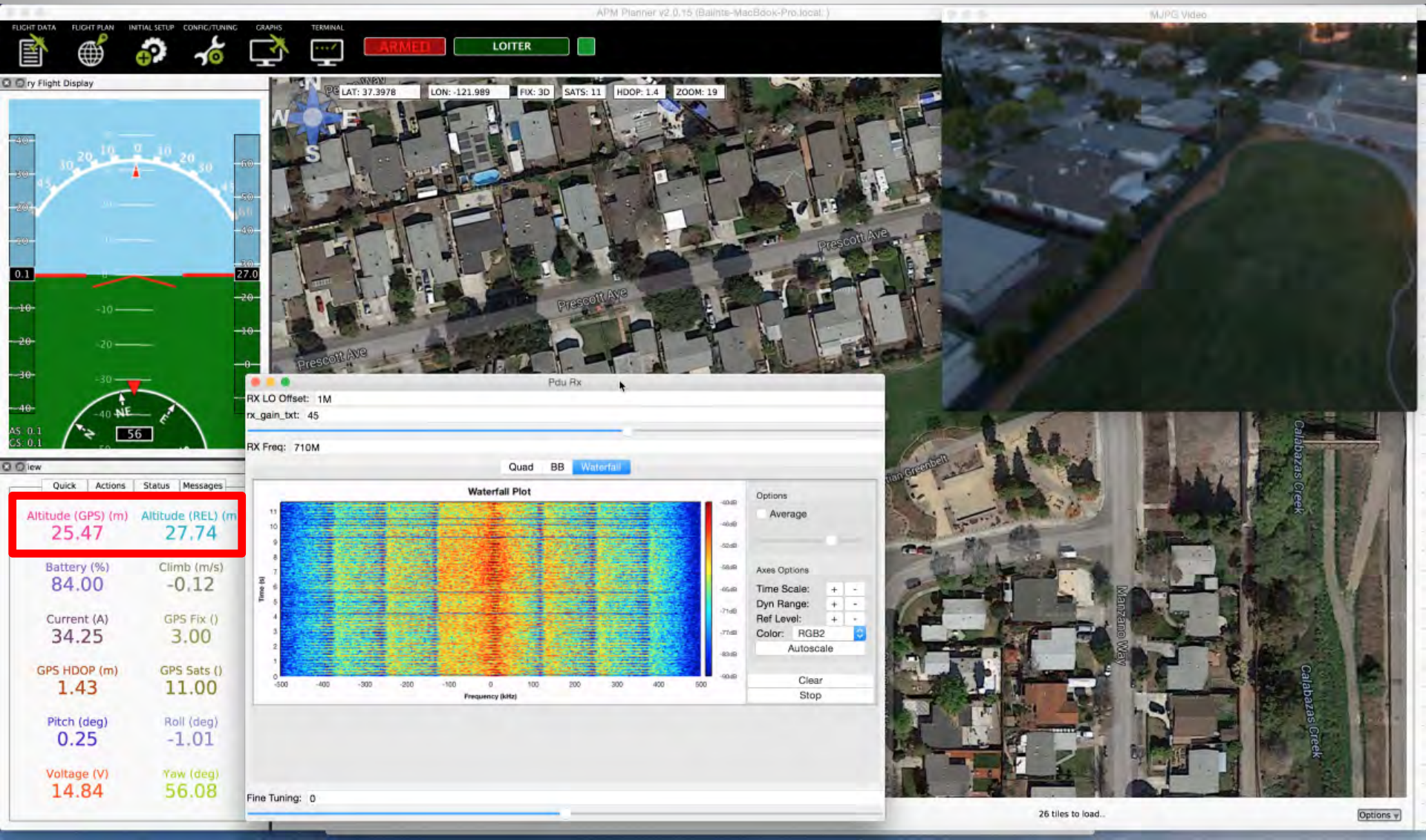
First Outdoor Test

Frame Packet Parser

Wave to the Drone!



View from Above

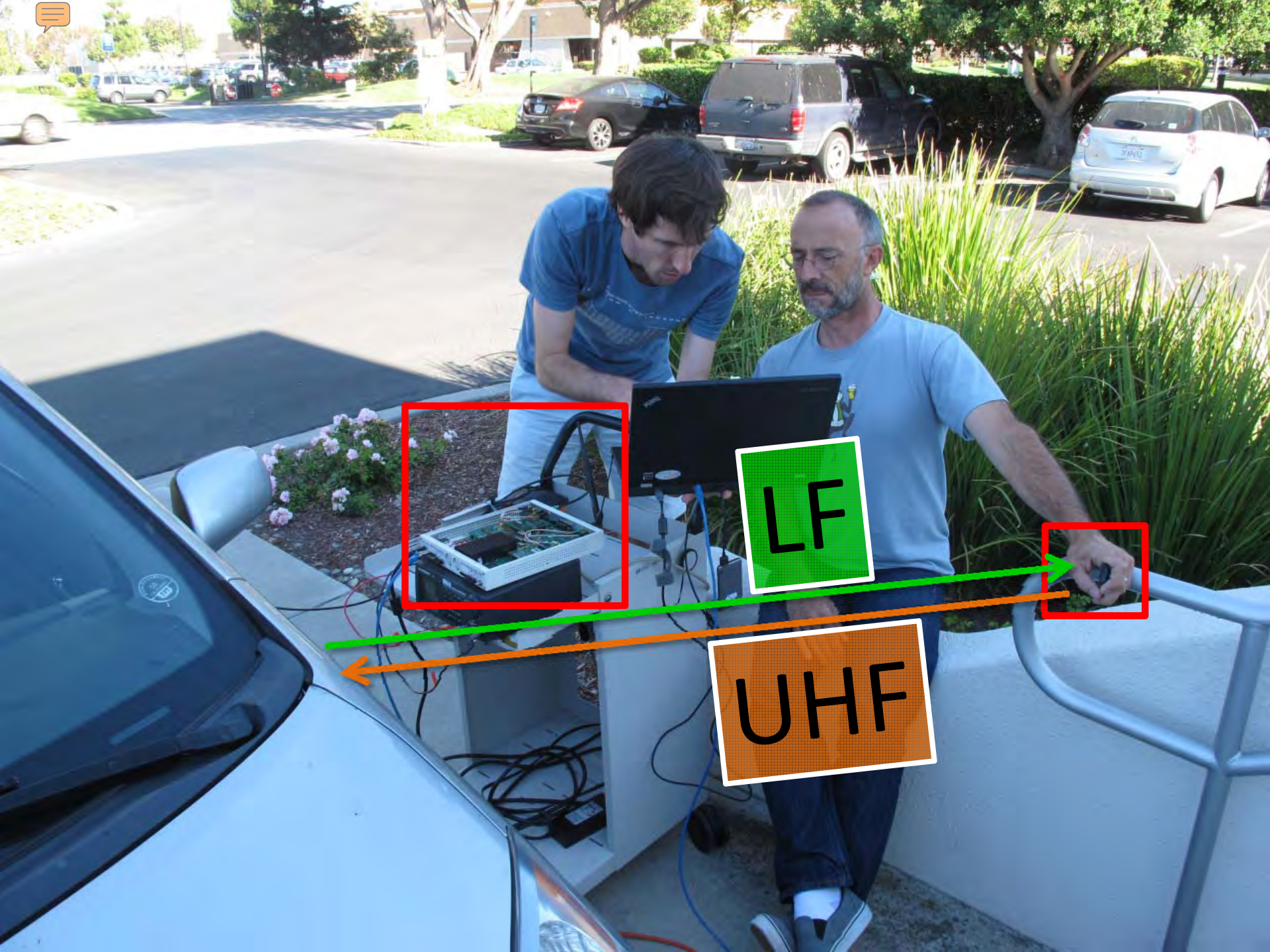


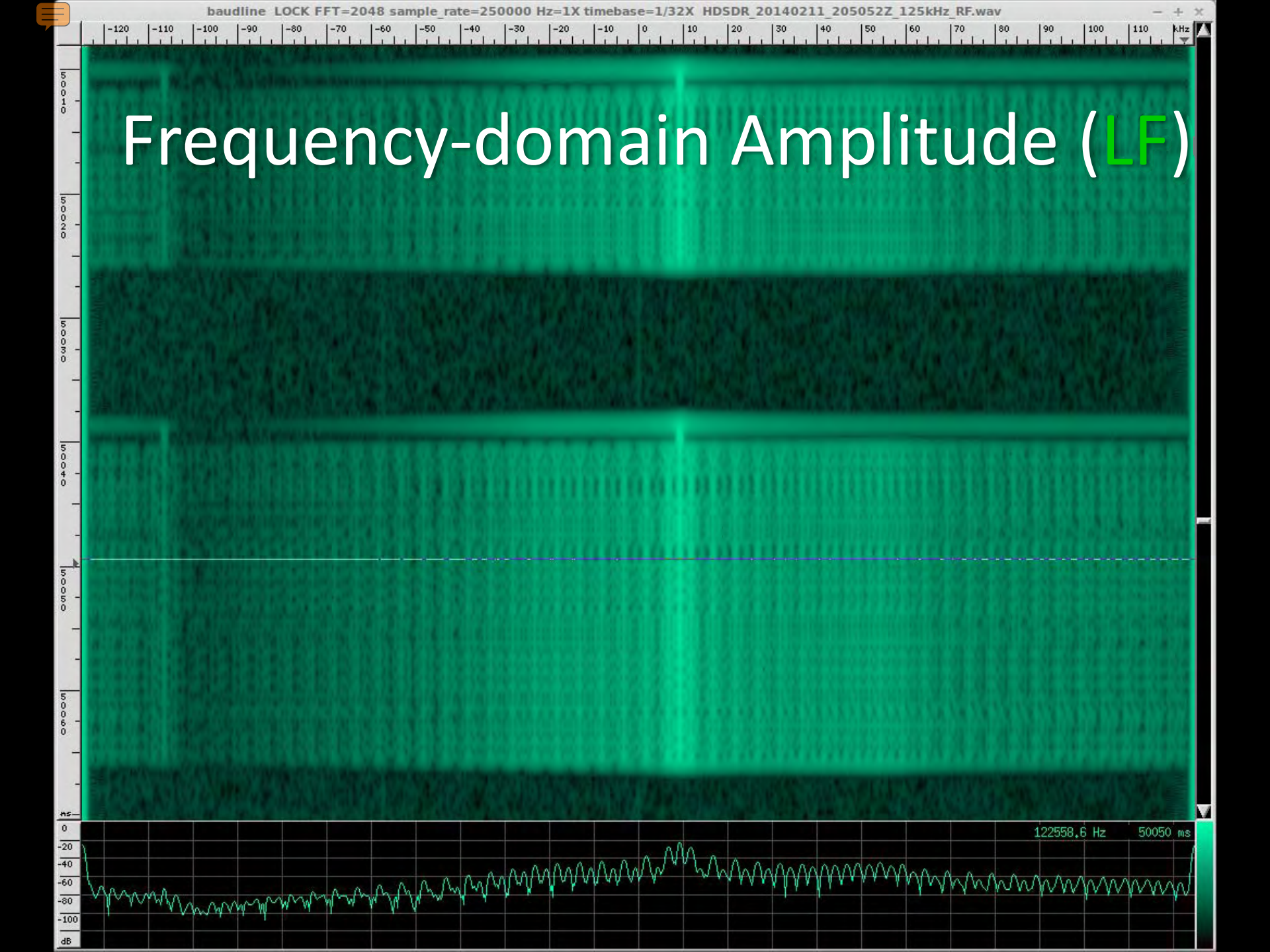

MJPG Video

View from Above

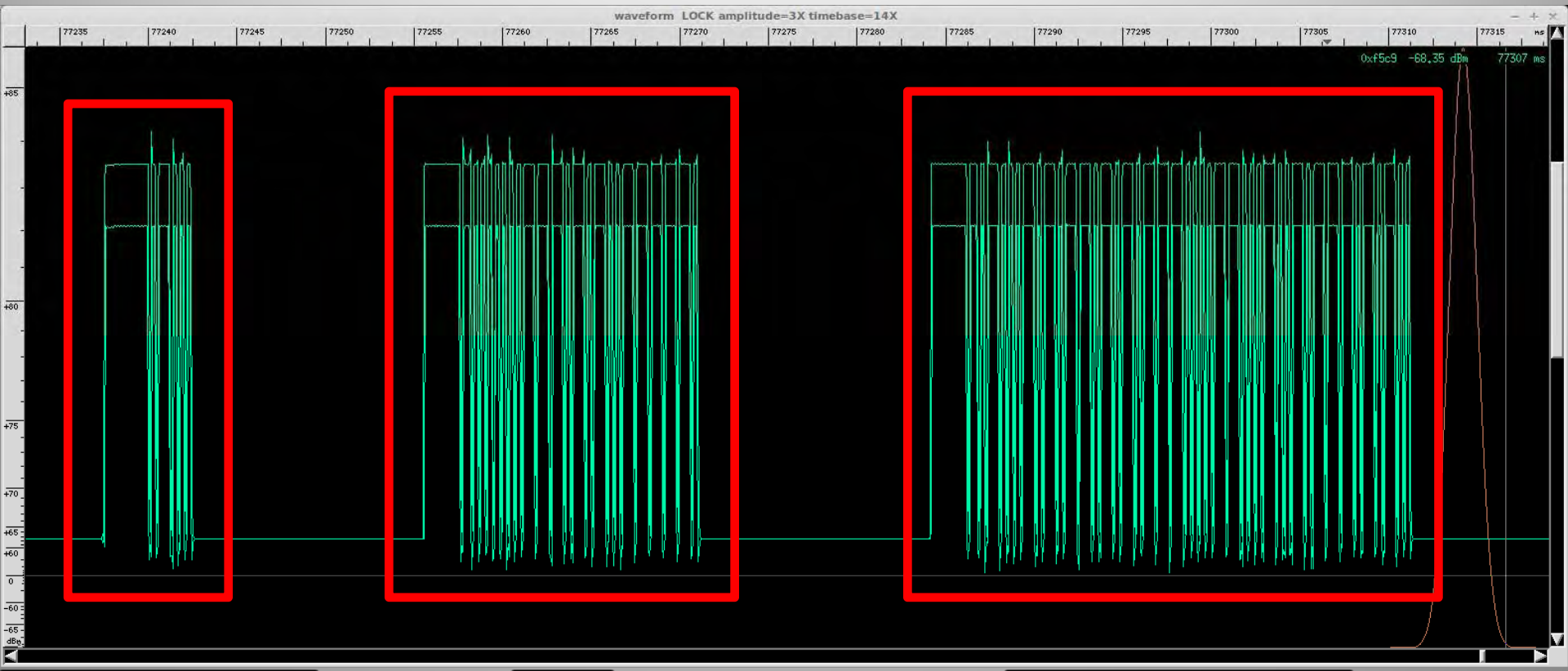
View from Above

Vehicular Keyless Entry

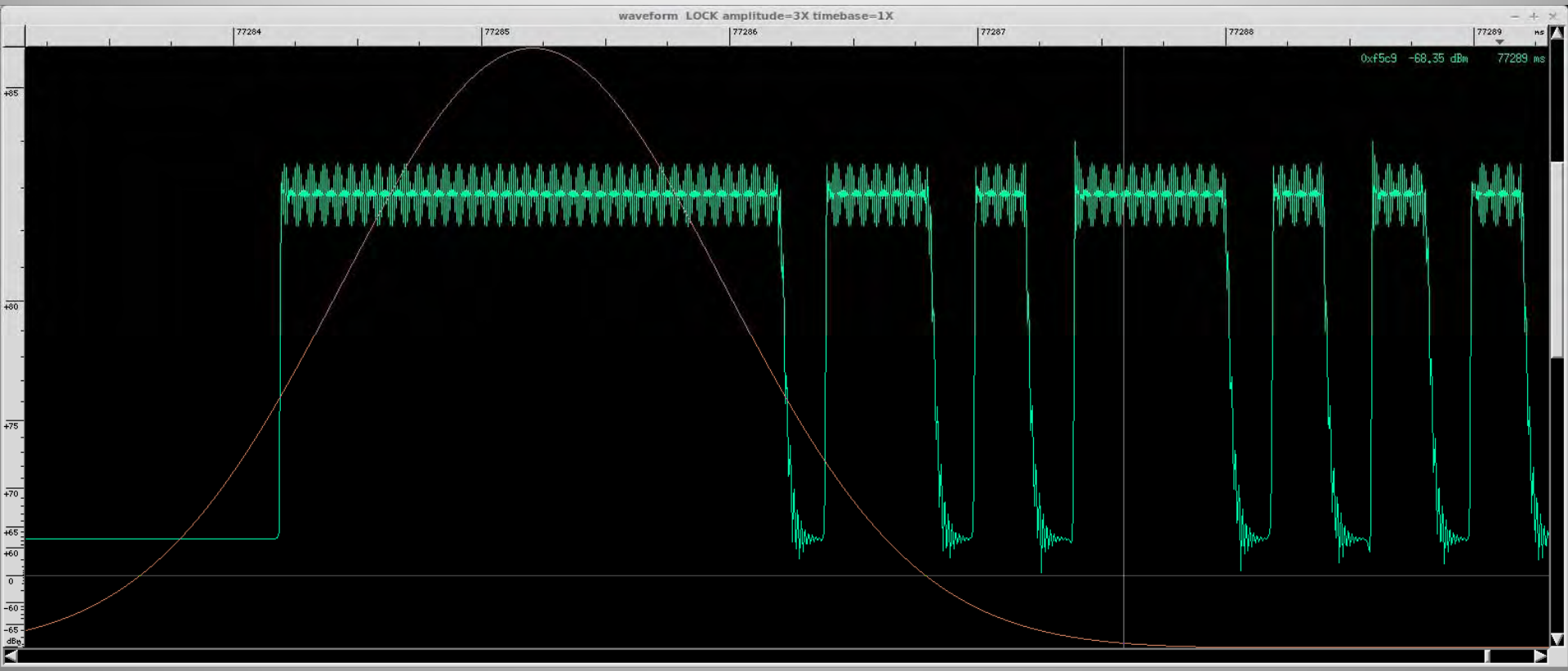

LF
UHF


baudline LOCK FFT=2048 sample_rate=250000 Hz=1X timebase=1/32X HDSDR_20140211_205052Z_125kHz_RF.wav
Frequency-domain Amplitude (LF)
122558.6 Hz
50050 ms

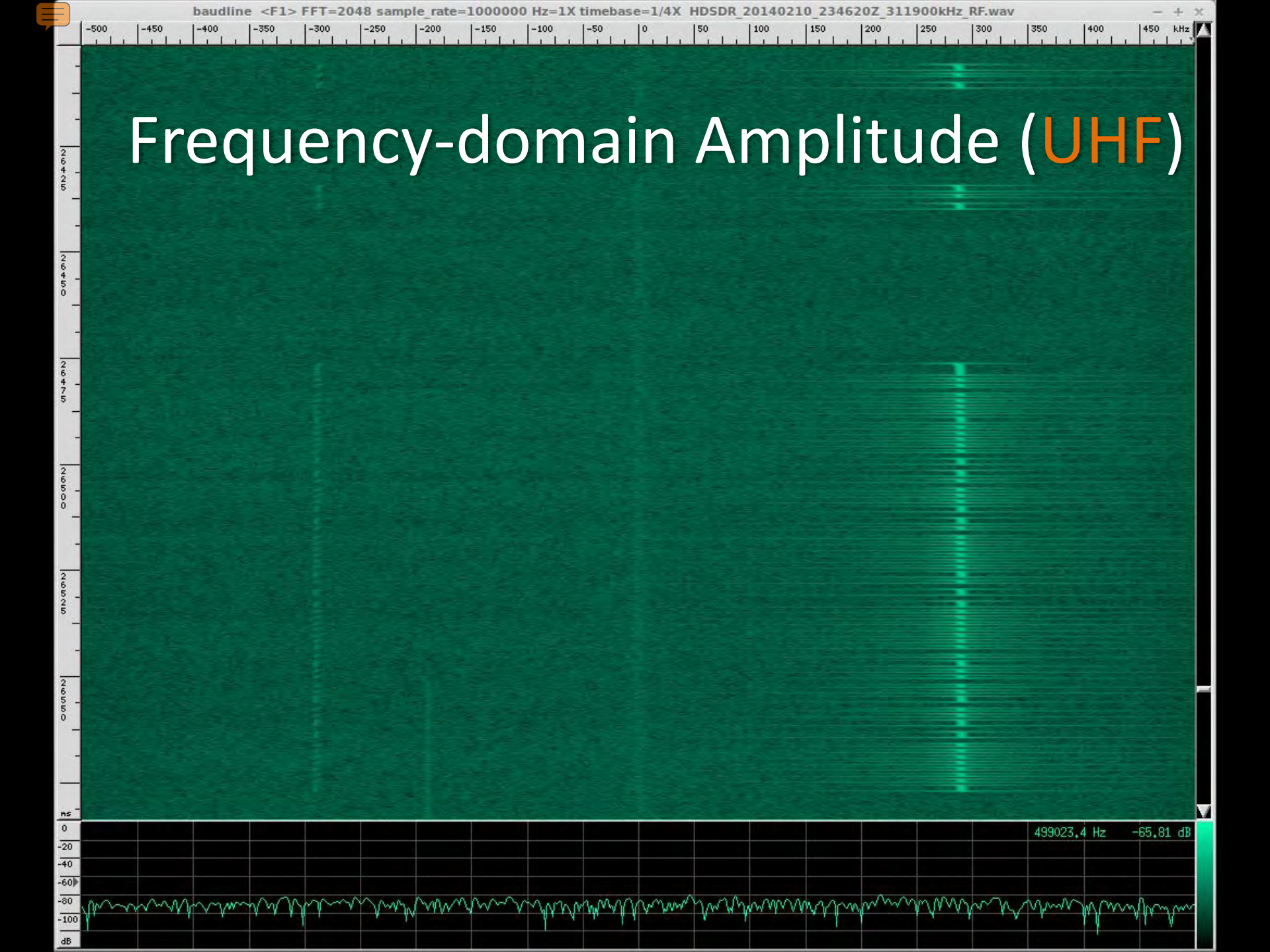
Time-domain Amplitude (LF)



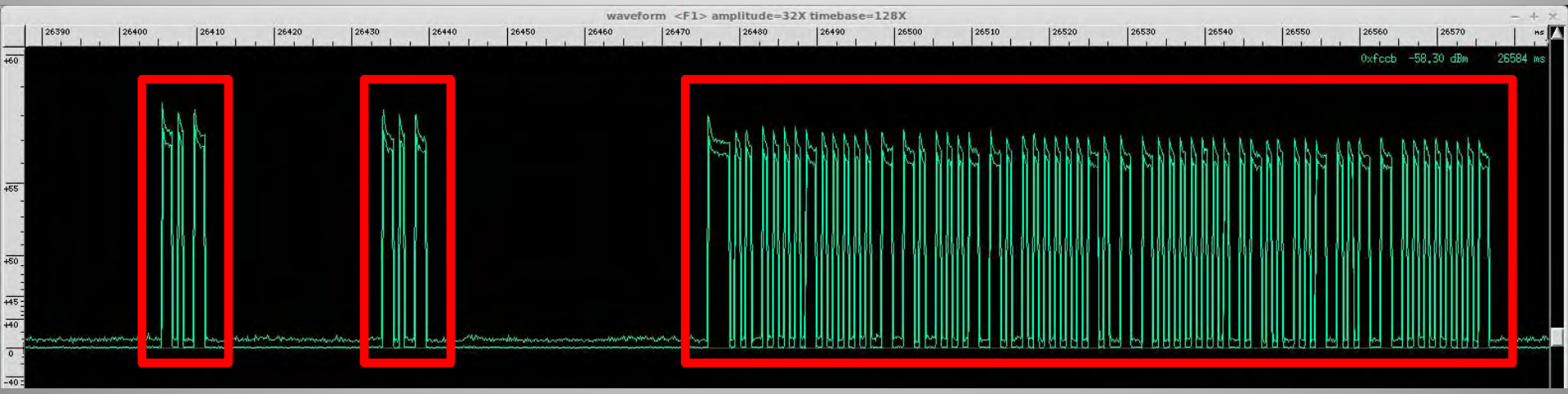
Time-domain Amplitude (LF)



Wake-up


baudline <F1> FFT=2048 sample_rate=1000000 Hz=1X timebase=1/4X HDSDR_20140210_234620Z_311900kHz_RF.wav
-500 -450 -400 -350 -300 -250 -200 -150 -100 -50 0 50 100 150 200 250 300 350 400 450 kHz
Frequency-domain Amplitude (UHF)
499023.4 Hz -65.81 dB
0 -20 -40 -60 -80 -100 dB

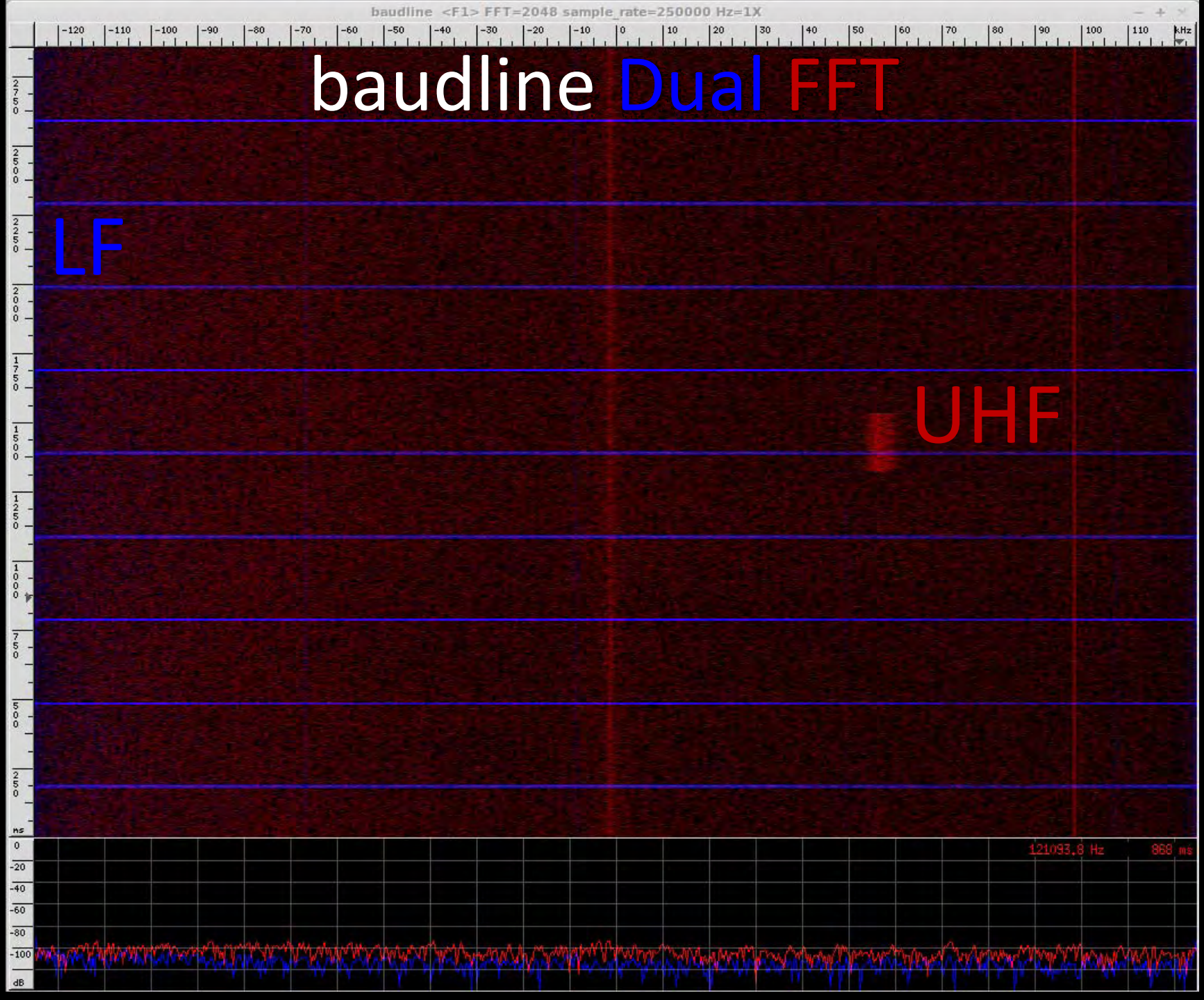
Time-domain Amplitude (UHF)



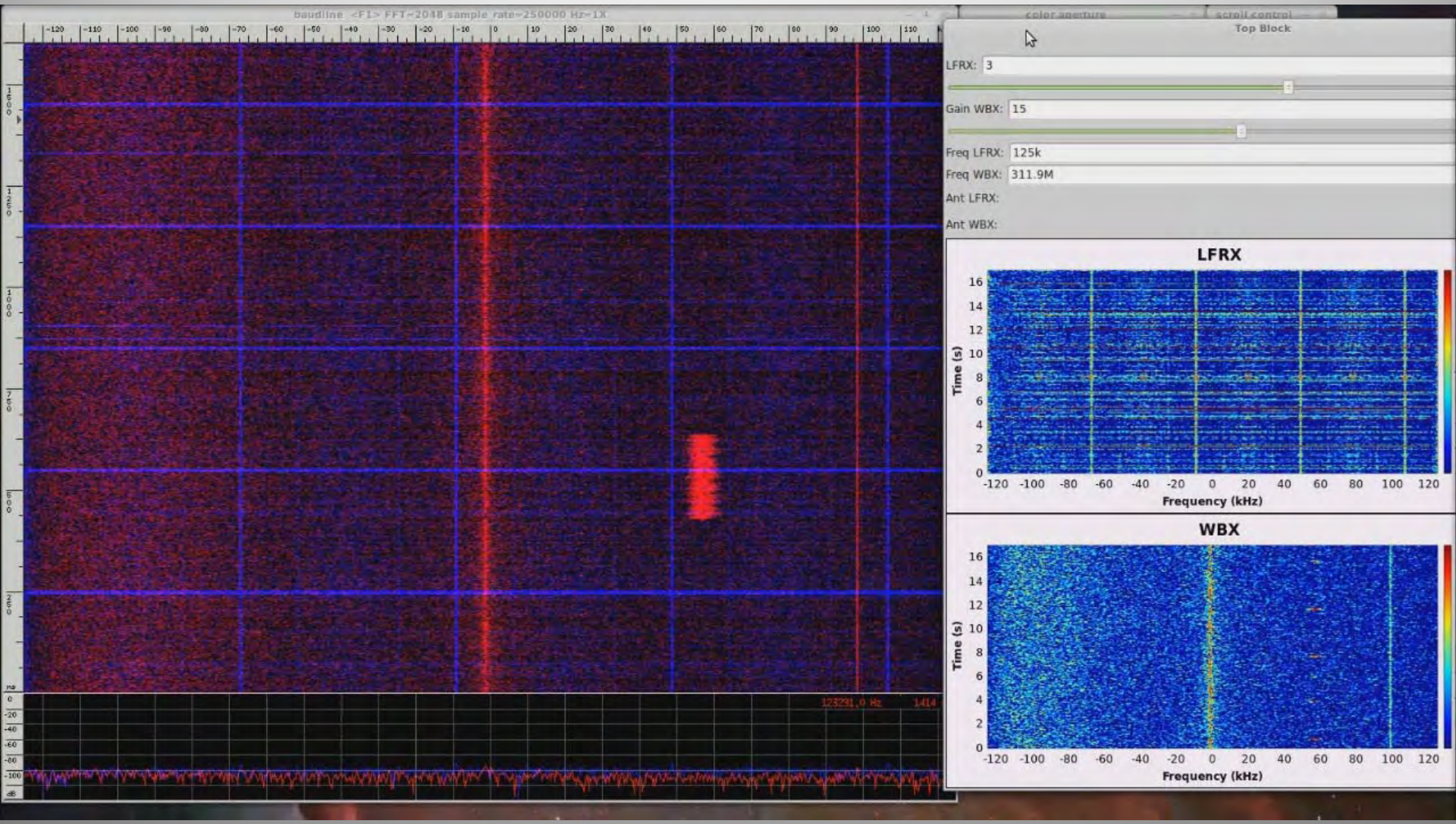
ACK

ACK

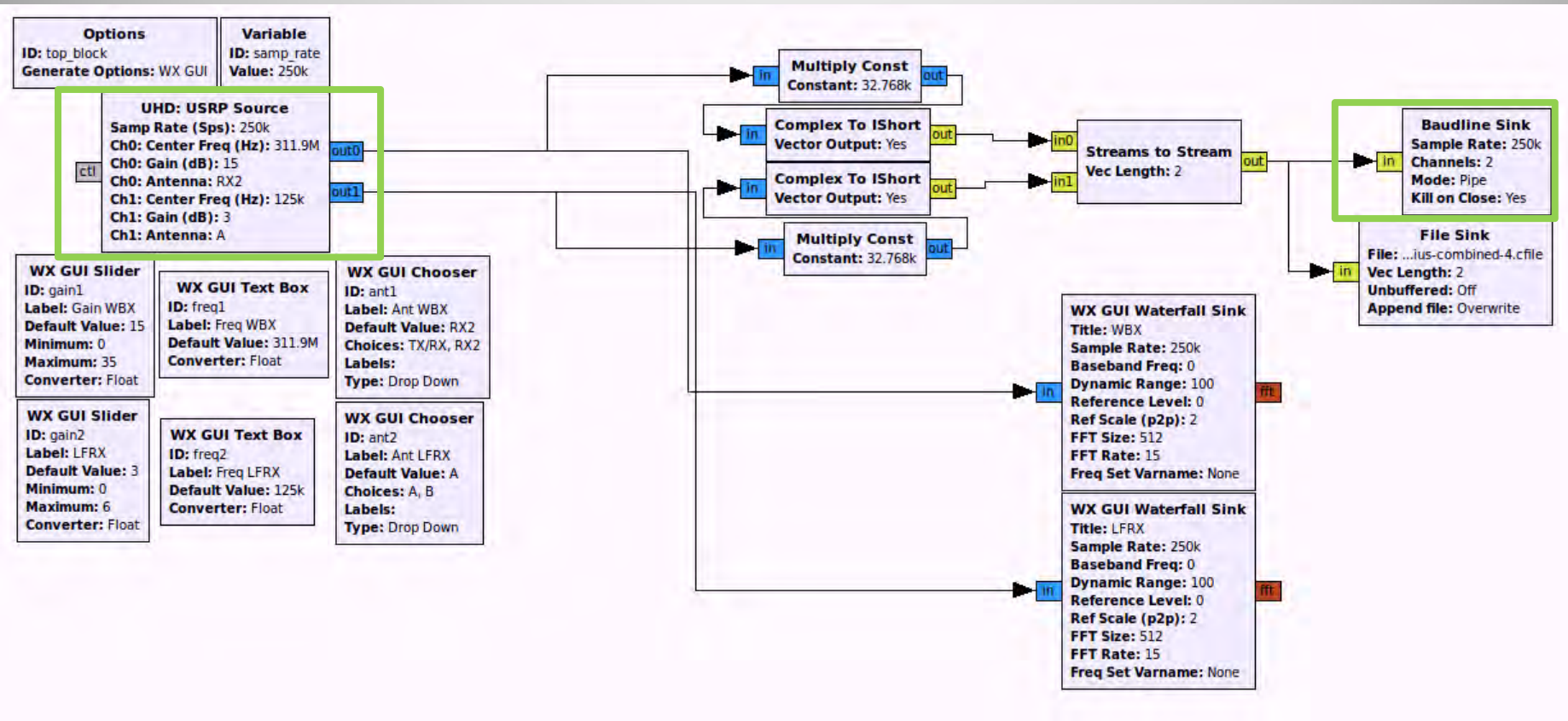
Response


baudline <F1> FFT=2048 sample_rate=250000 Hz=1X
baudline Dual FFT
LF
UHF
121093.8 Hz
868 ms

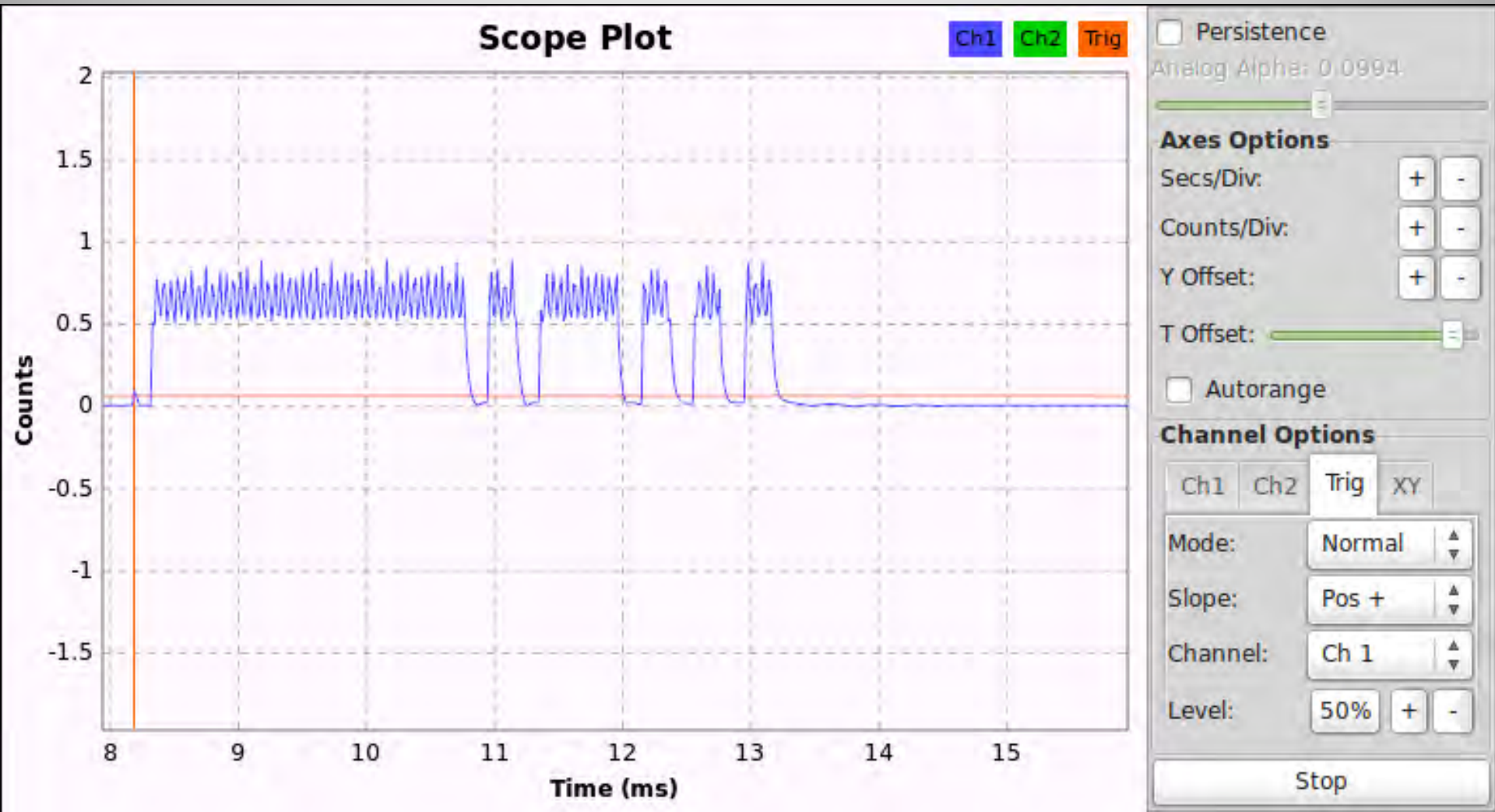
Dual Channel FFT



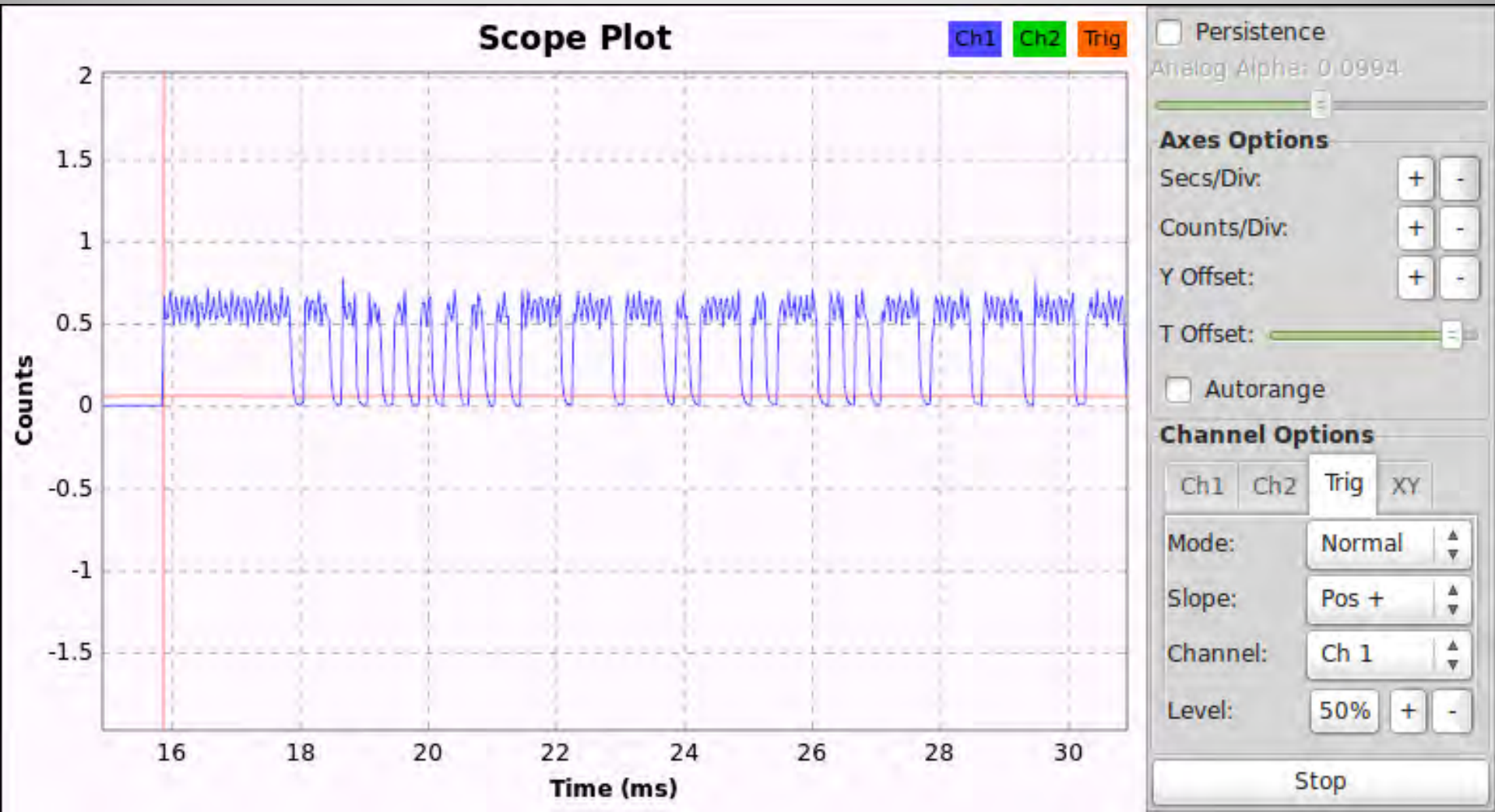
GNU Radio + baudline



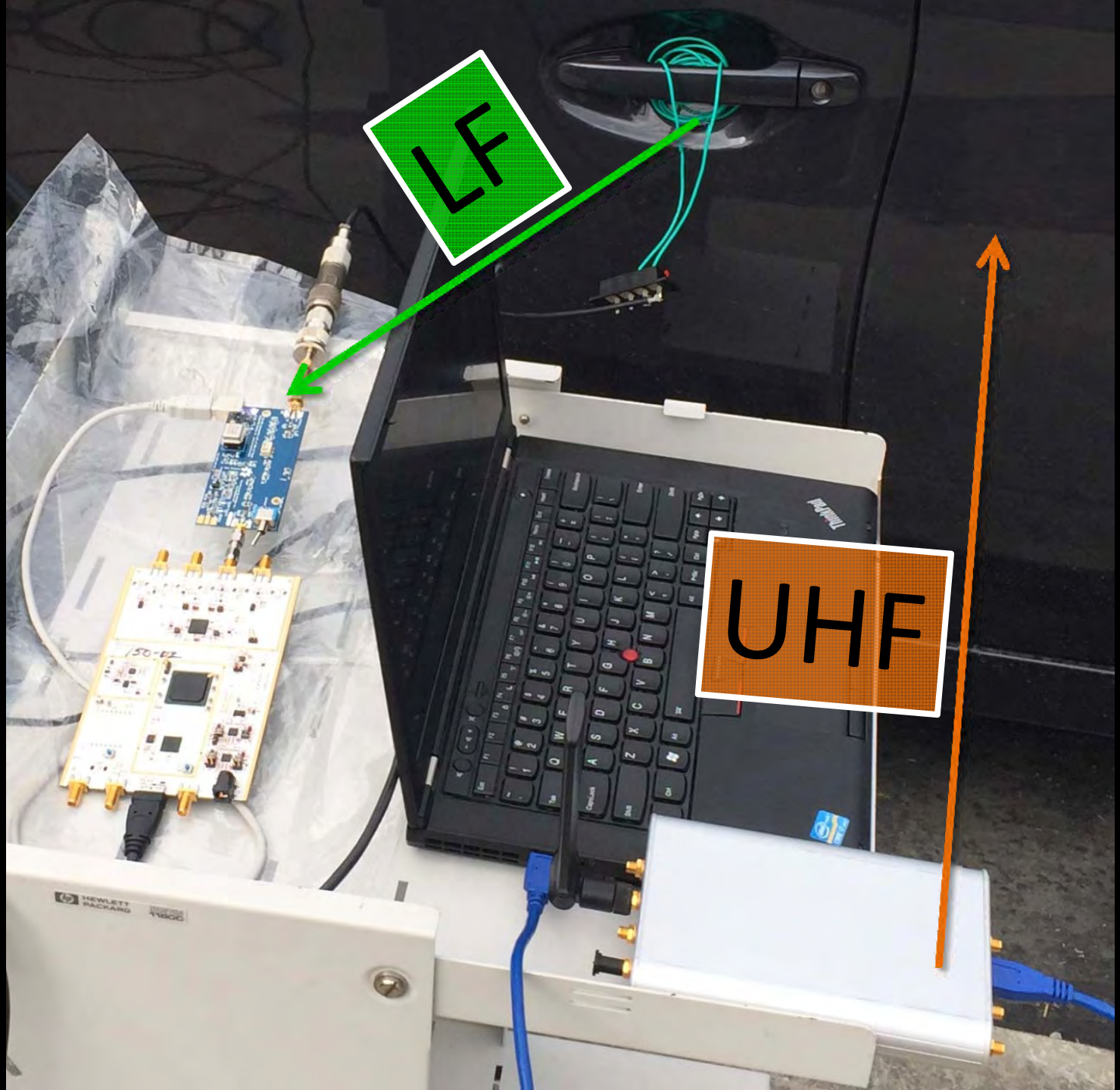
Wake-up

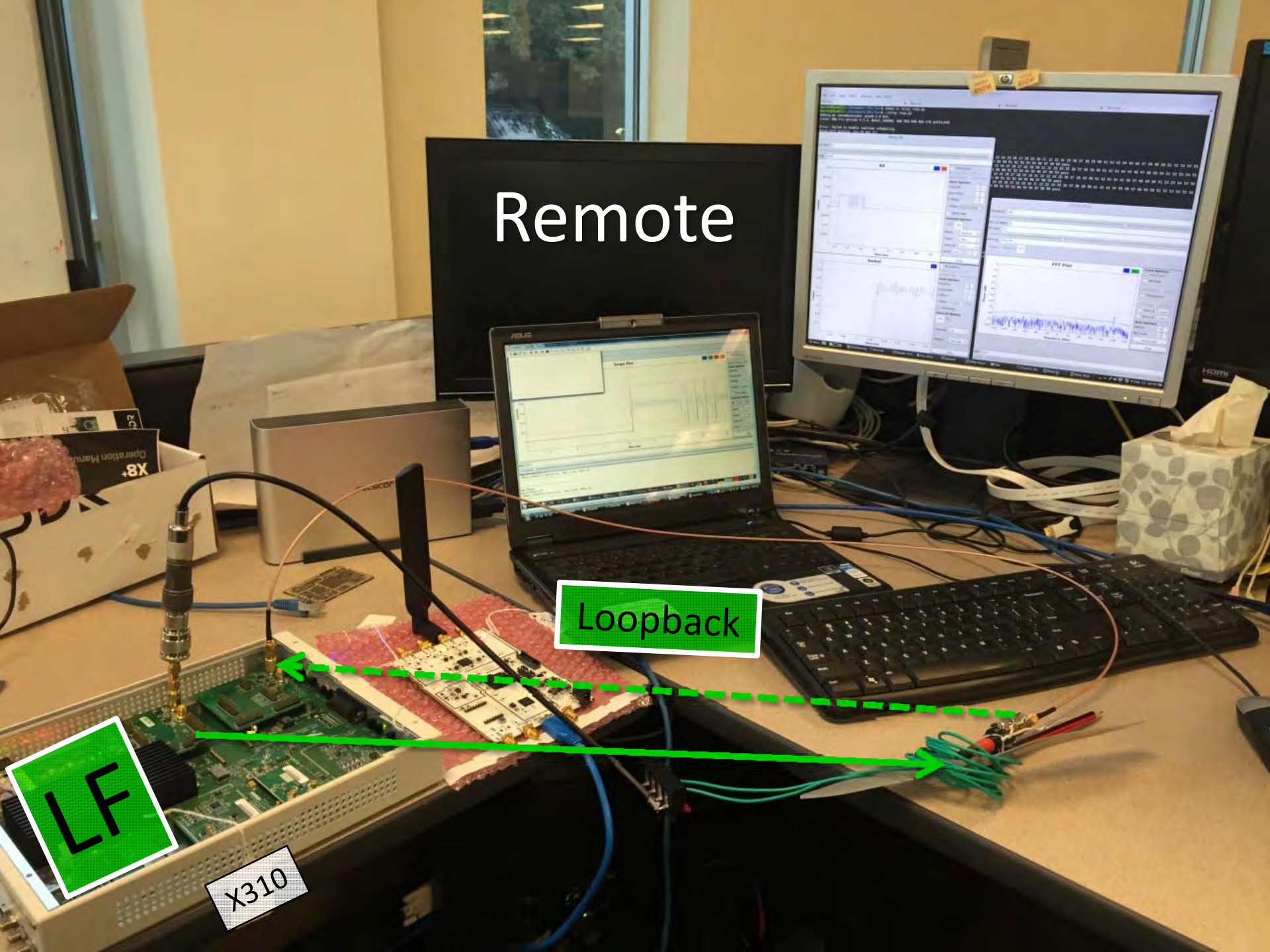

Scope Plot
Ch1
Ch2
Trig
2
1.5
1
0.5
0
-0.5
-1
-1.5
Counts
8
9
10
11
12
13
14
15
Time (ms)
Persistence
Analog Alpha: 0.0994
Axes Options
Secs/Div:
Counts/Div:
Y Offset:
T Offset:
Autorange
Channel Options
Ch1
Ch2
Trig
XY
Mode:
Normal
Slope:
Pos +
Channel:
Ch 1
Level:
50%
Stop

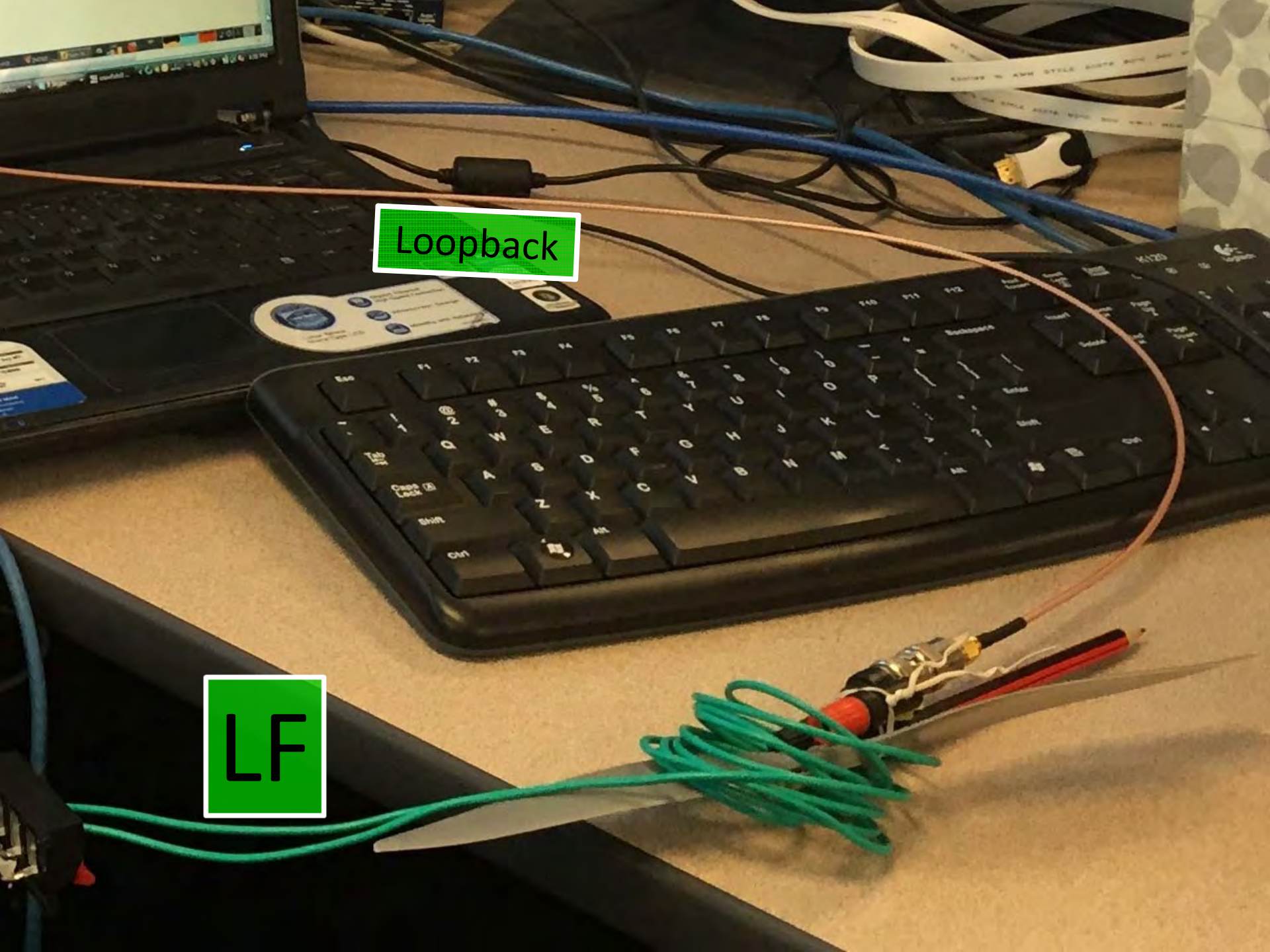
Challenge

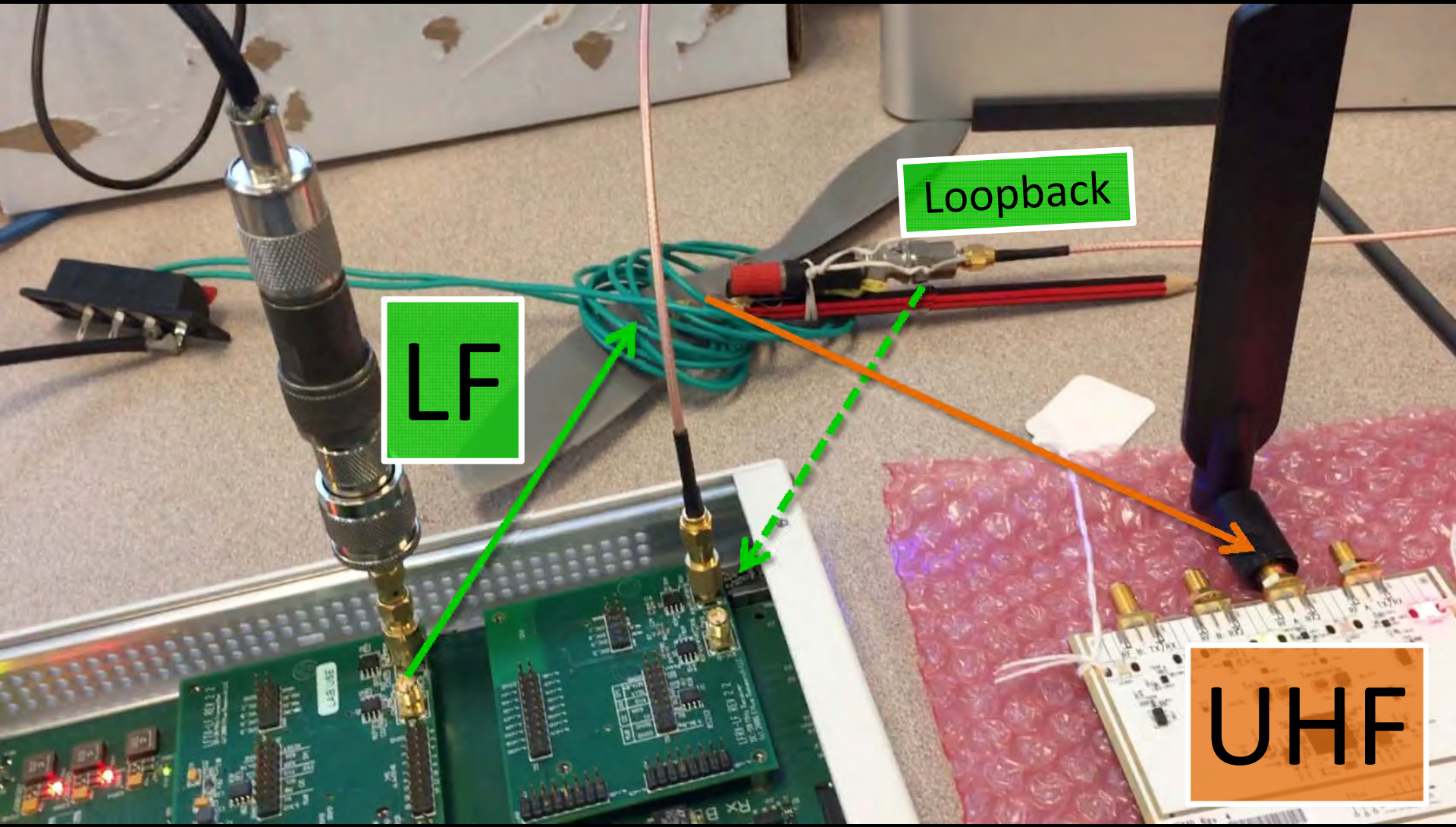

Scope Plot
Ch1
Ch2
Trig
2
1.5
1
0.5
0
-0.5
-1
-1.5
Counts
16
18
20
22
24
26
28
30
Time (ms)
Persistence
Analog Alpha: 0.0994
Axes Options
Secs/Div:
Counts/Div:
Y Offset:
T Offset:
Autorange
Channel Options
Ch1
Ch2
Trig
XY
Mode:
Normal
Slope:
Pos +
Channel:
Ch 1
Level:
50%
Stop

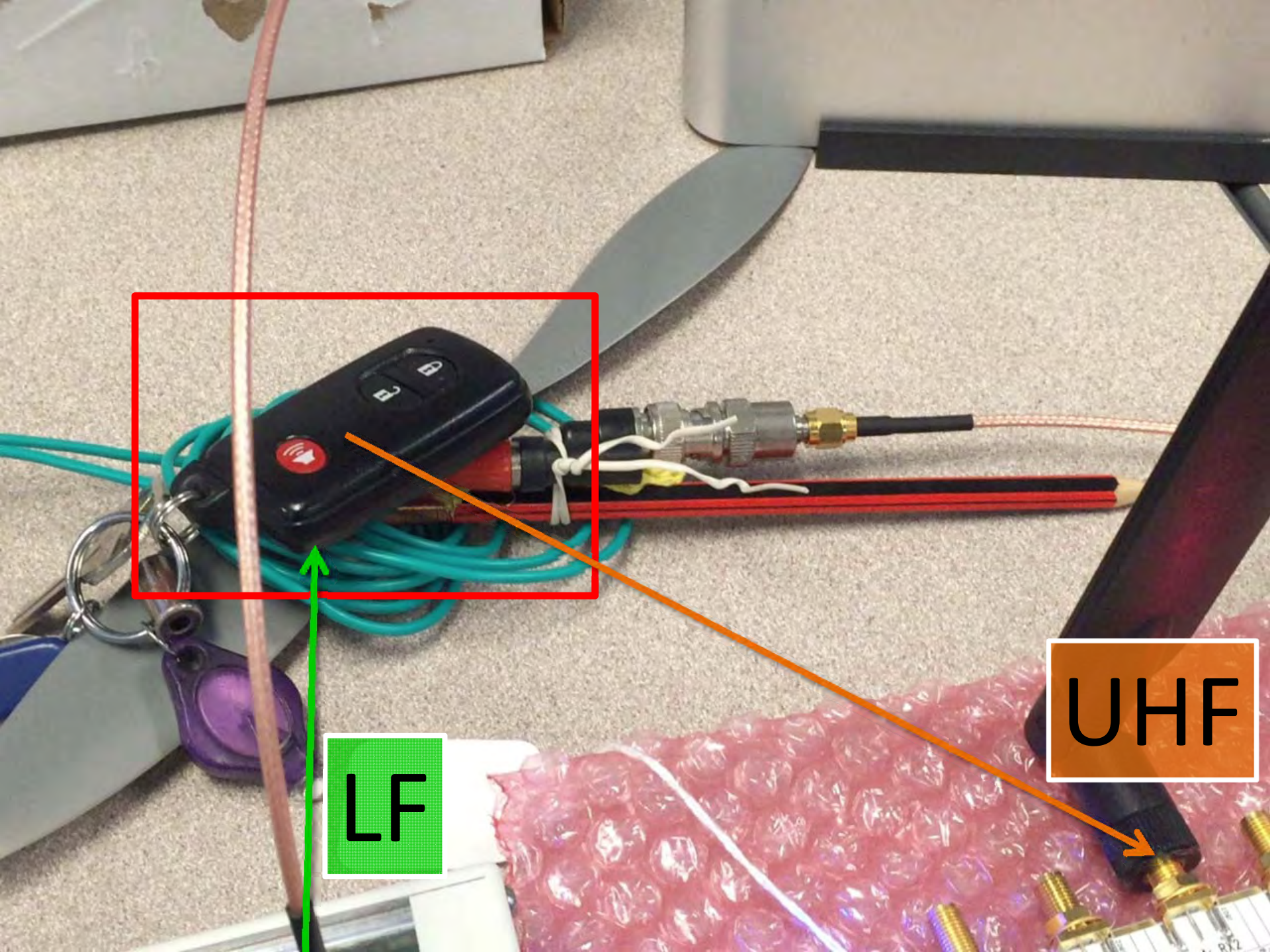

Vehicle
HYBRID


LF
UHF

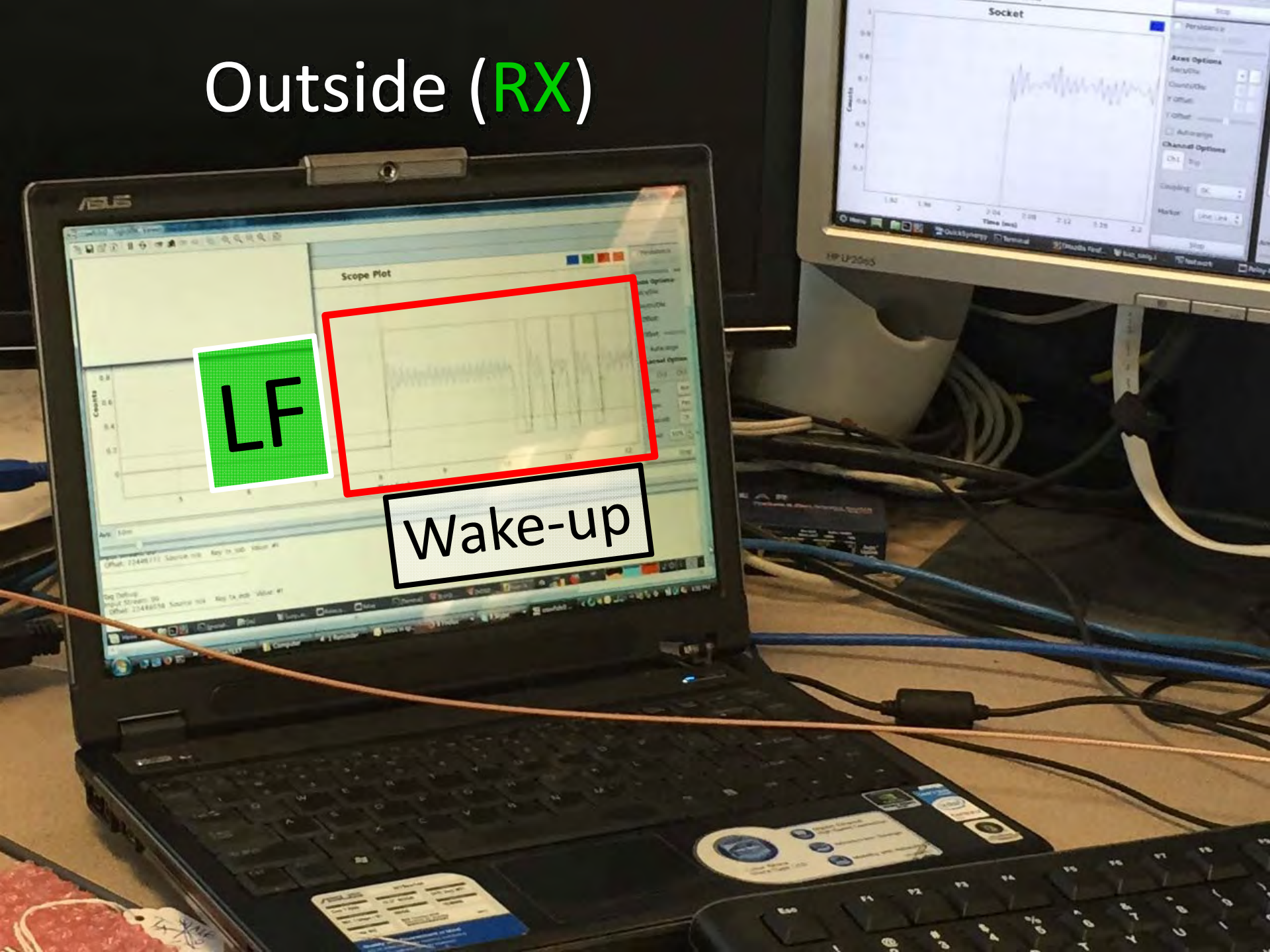

Remote
Loopback
LF
X310


Loopback
LF

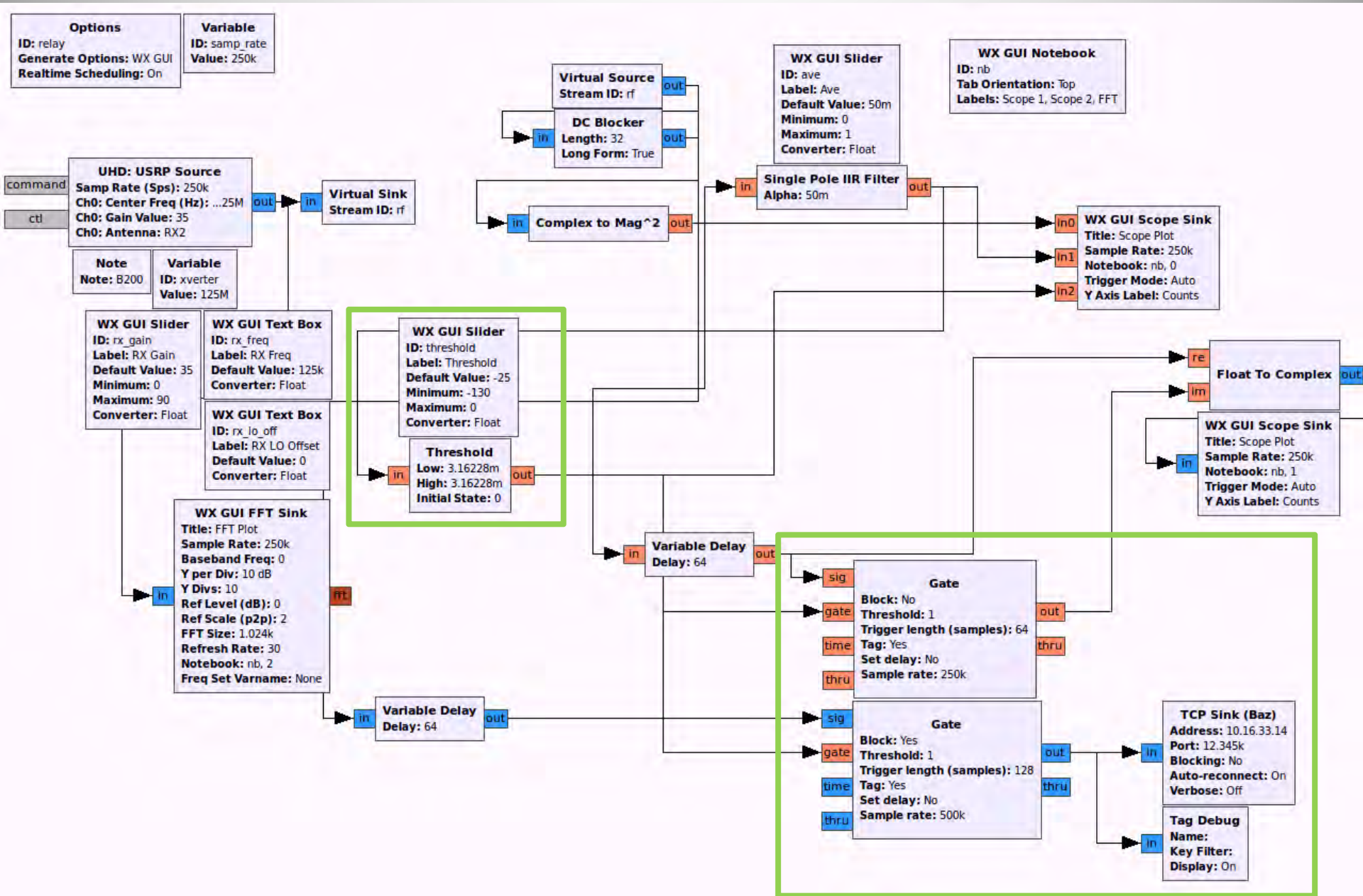

Loopback
LF
UHF


LF
UHF

Outside (RX)

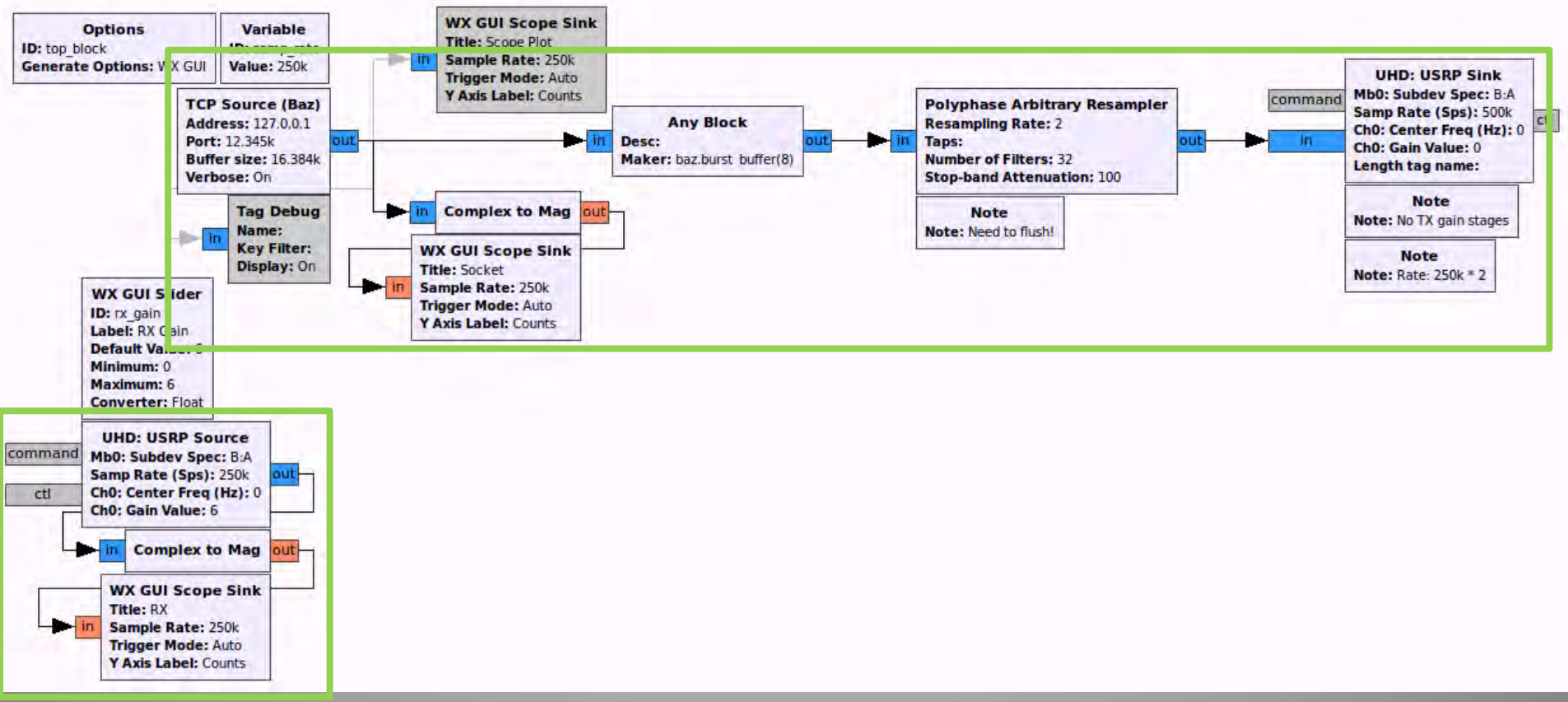


LF Relay (RX Outside)

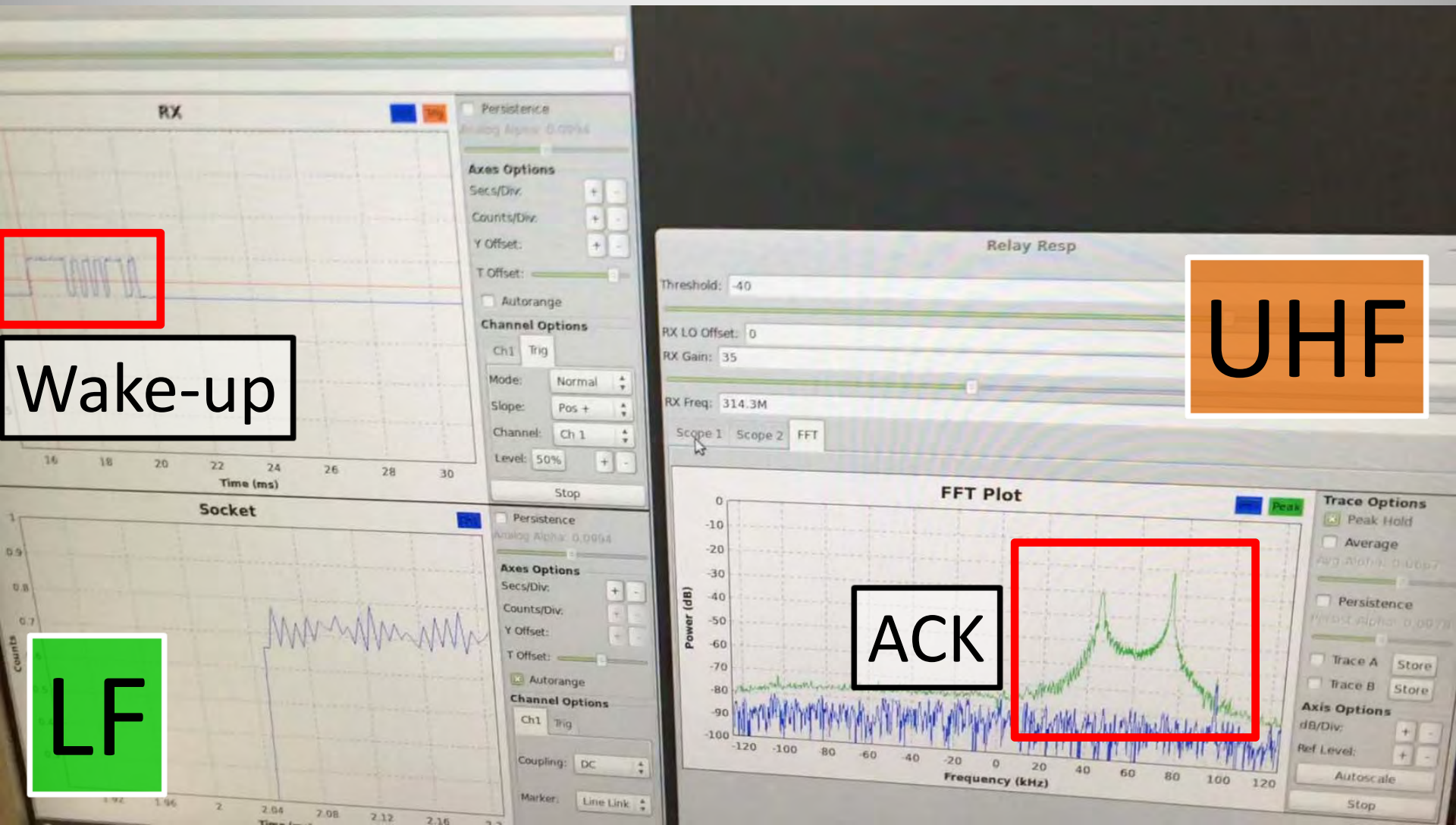



Inside (TX → RX)
RX
Socket
FFT Plot
LF
UHF

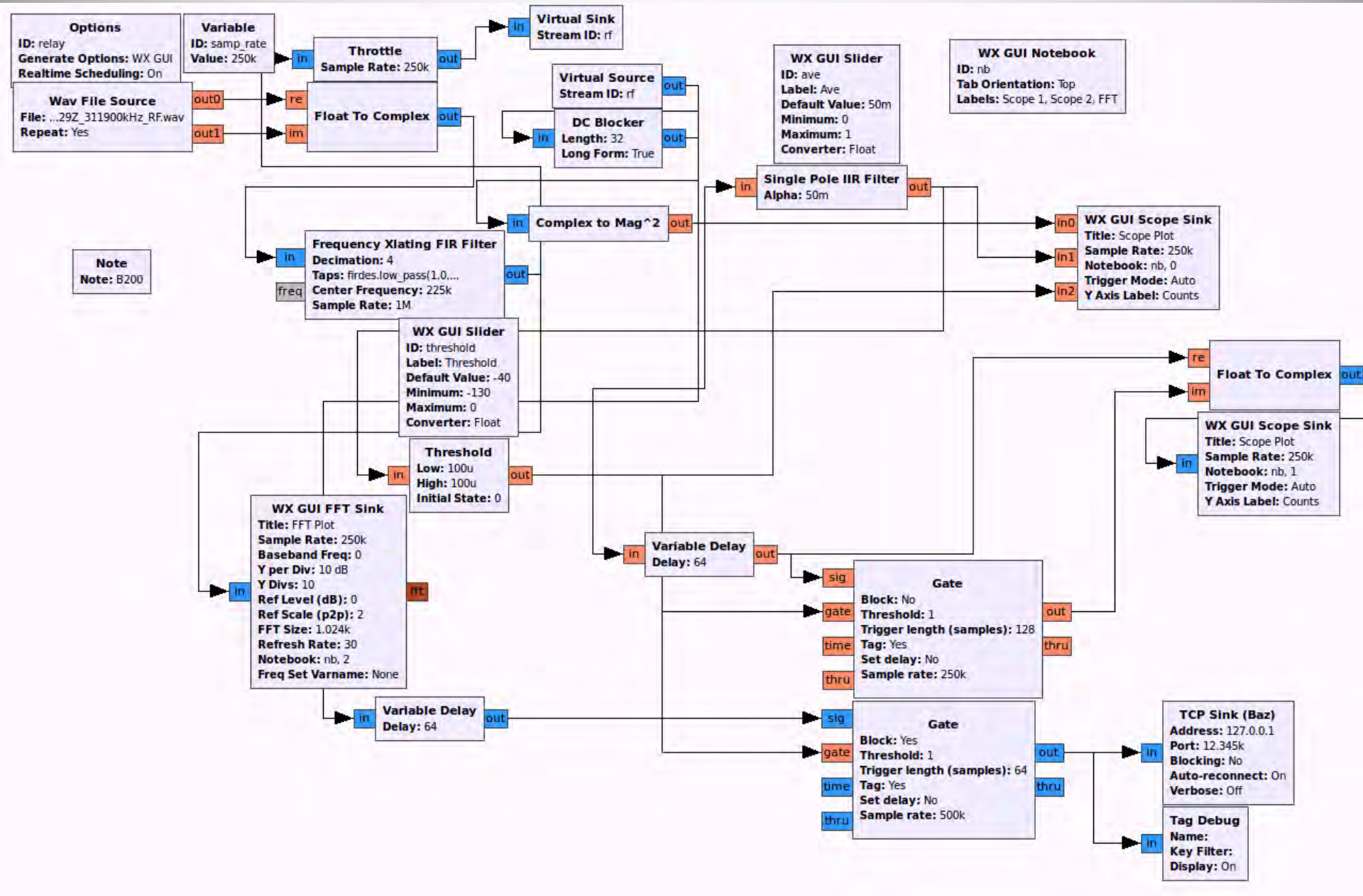
LF Relay (TX Inside)



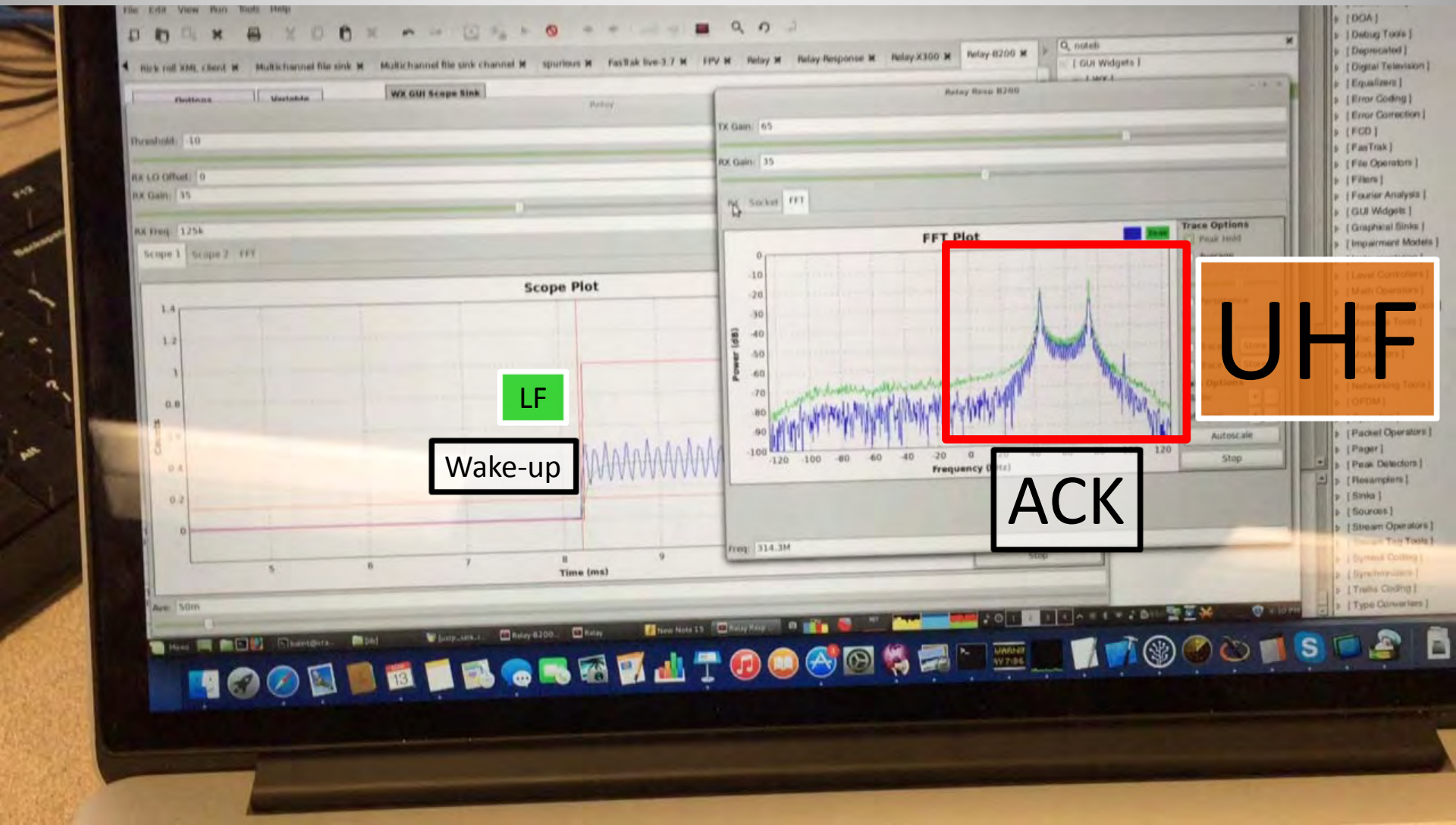
Inside (TX → RX)


RX
Persistence
Axes Options
Secs/Div:
Counts/Div:
Y Offset:
T Offset:
Autorange
Channel Options
Ch1
Trig
Mode:
Normal
Slope:
Pos +
Channel:
Ch 1
Level:
50%
Stop
Time (ms)
Wake-up
Socket
Persistence
Axes Options
Secs/Div:
Counts/Div:
Y Offset:
T Offset:
Autorange
Channel Options
Ch1
Trig
Coupling:
DC
Marker:
Line Link
Counts
LF
Relay Resp
Threshold:
-40
RX LO Offset:
0
RX Gain:
35
RX Freq:
314.3M
Scope 1
Scope 2
FFT
UHF
FFT Plot
Peak
Power (dB)
Frequency (kHz)
ACK
Trace Options
Peak Hold
Average
Persistence
Trace A
Store
Trace B
Store
Axis Options
dB/Div:
Ref Level:
Autoscale
Stop

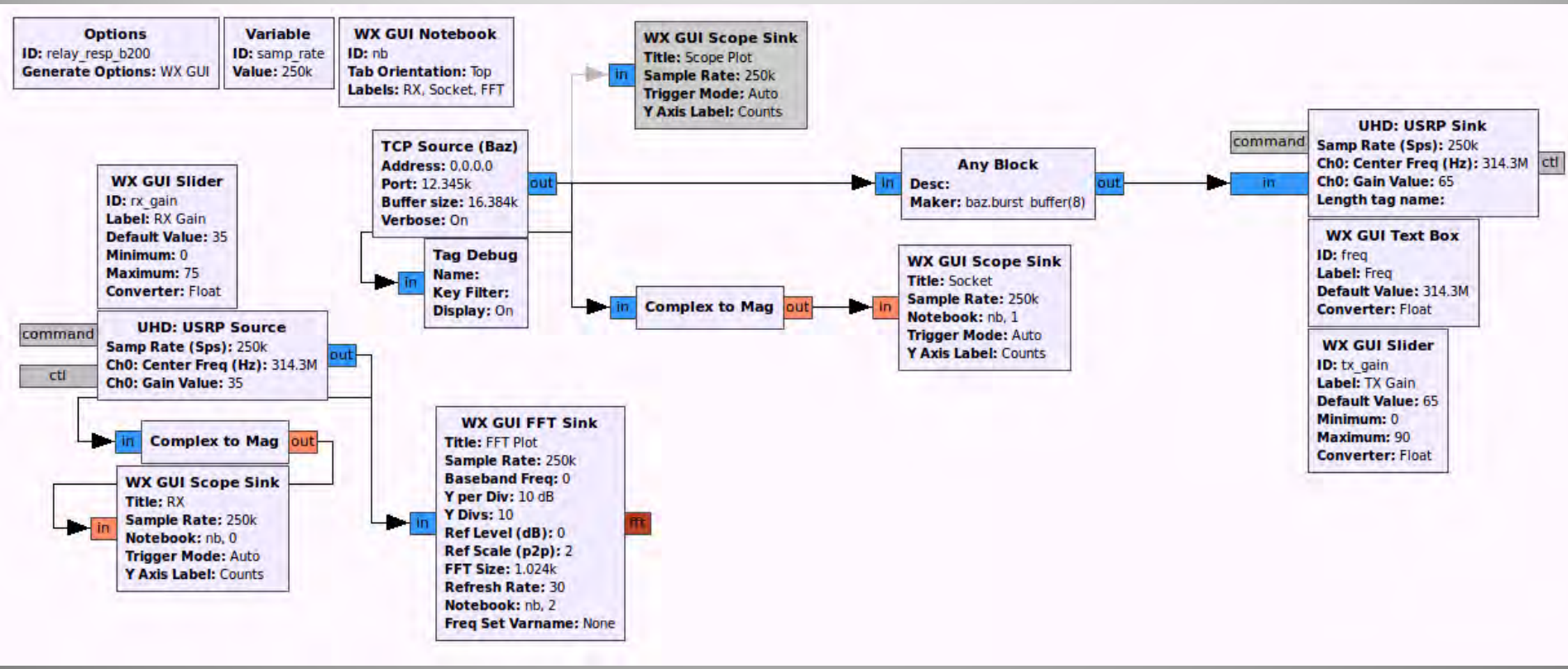
UHF Relay (RX Inside)



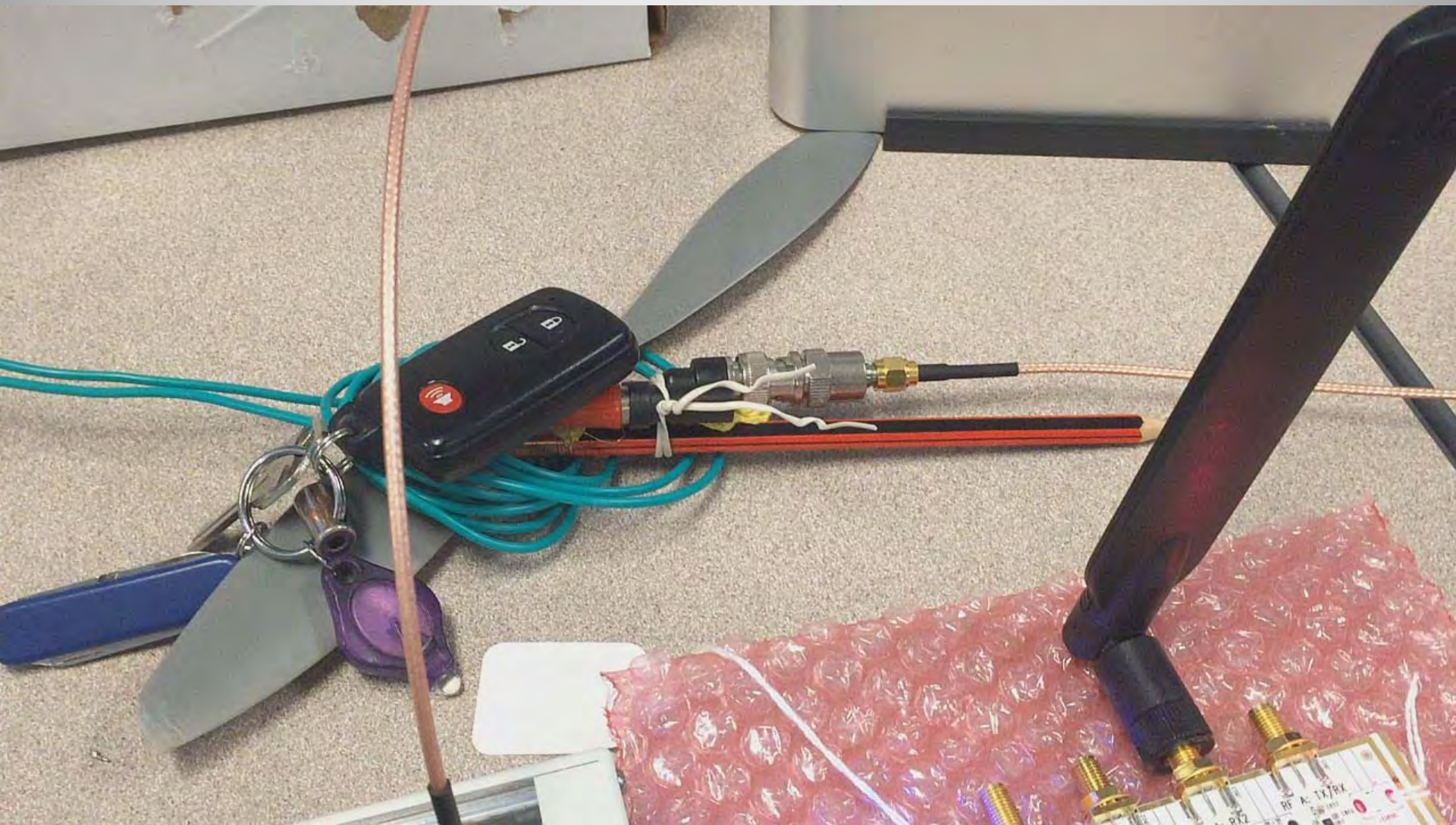
Outside (TX)

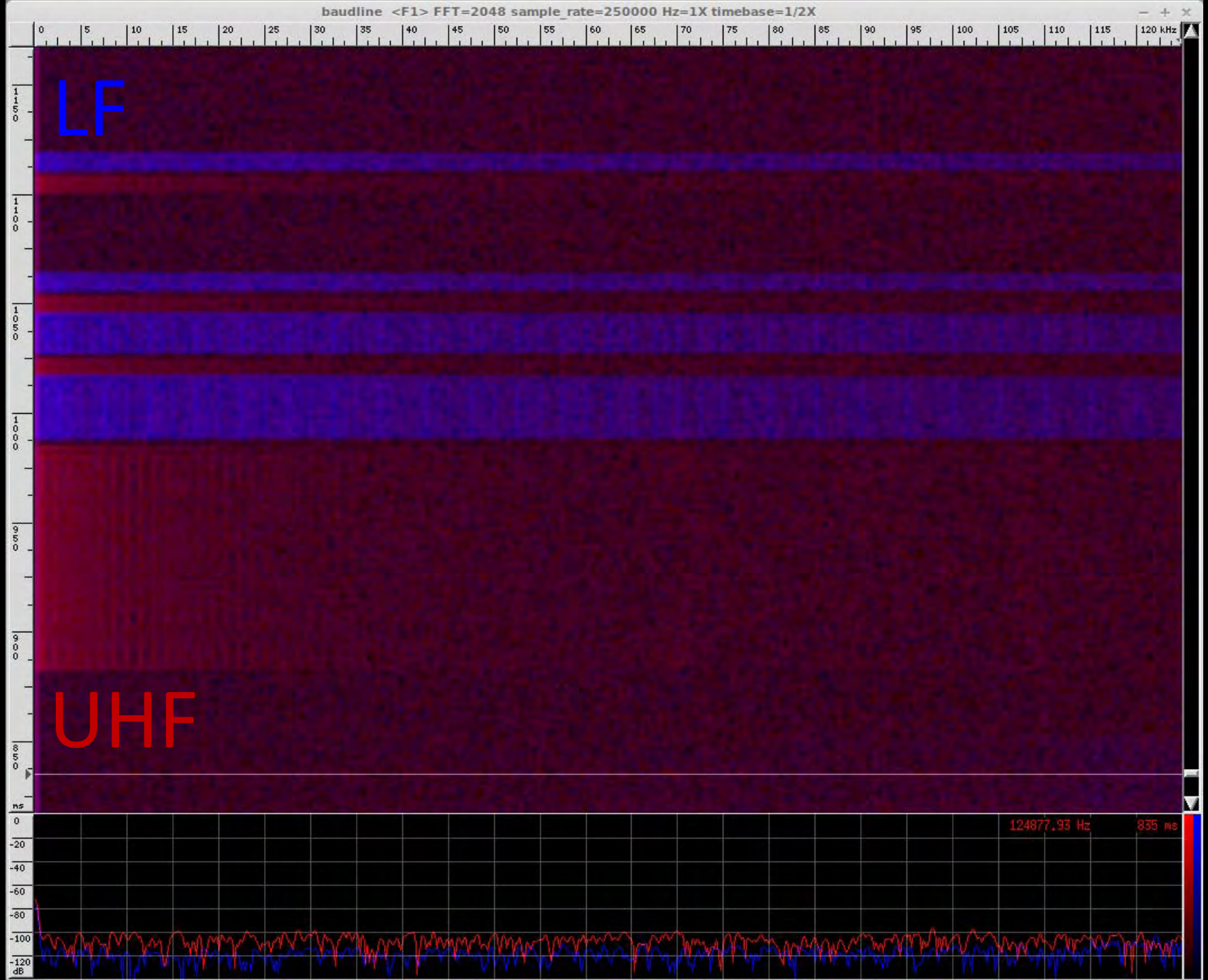


UHF Relay (TX Outside)

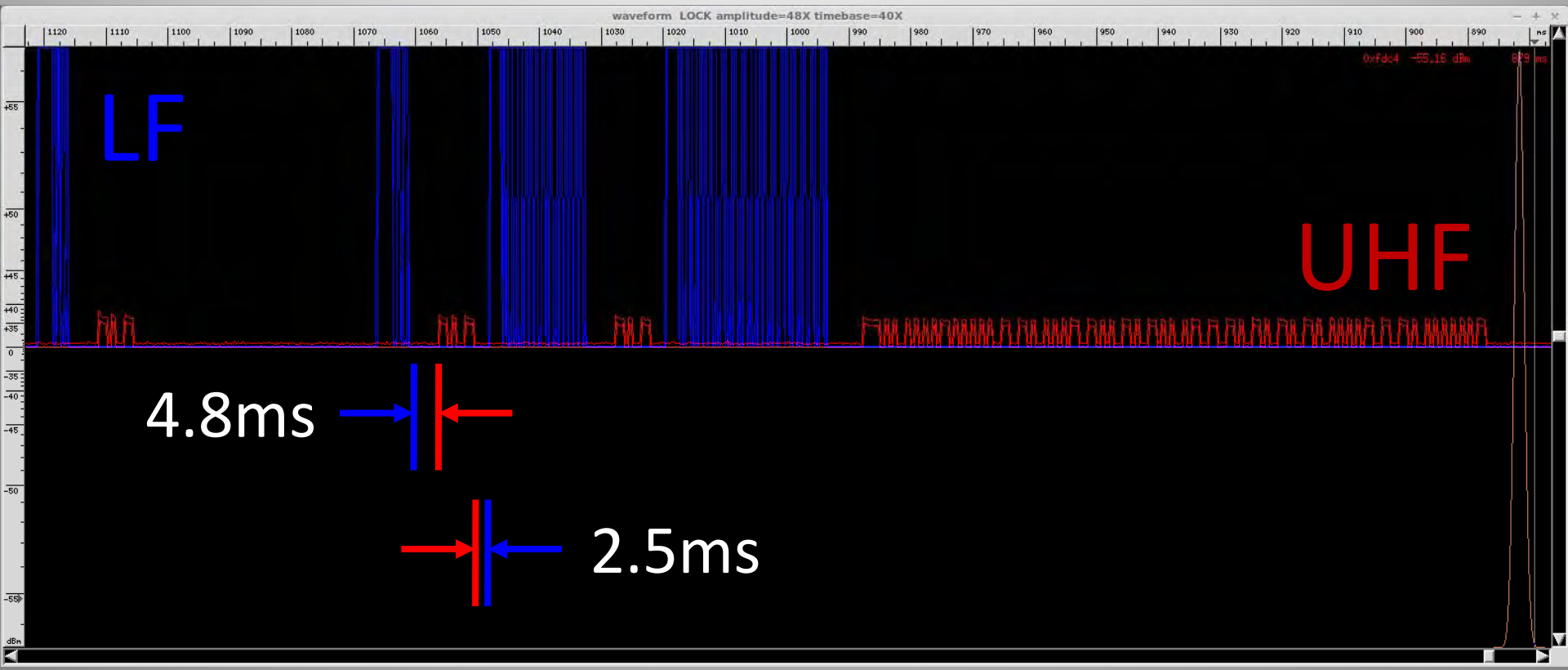


Test



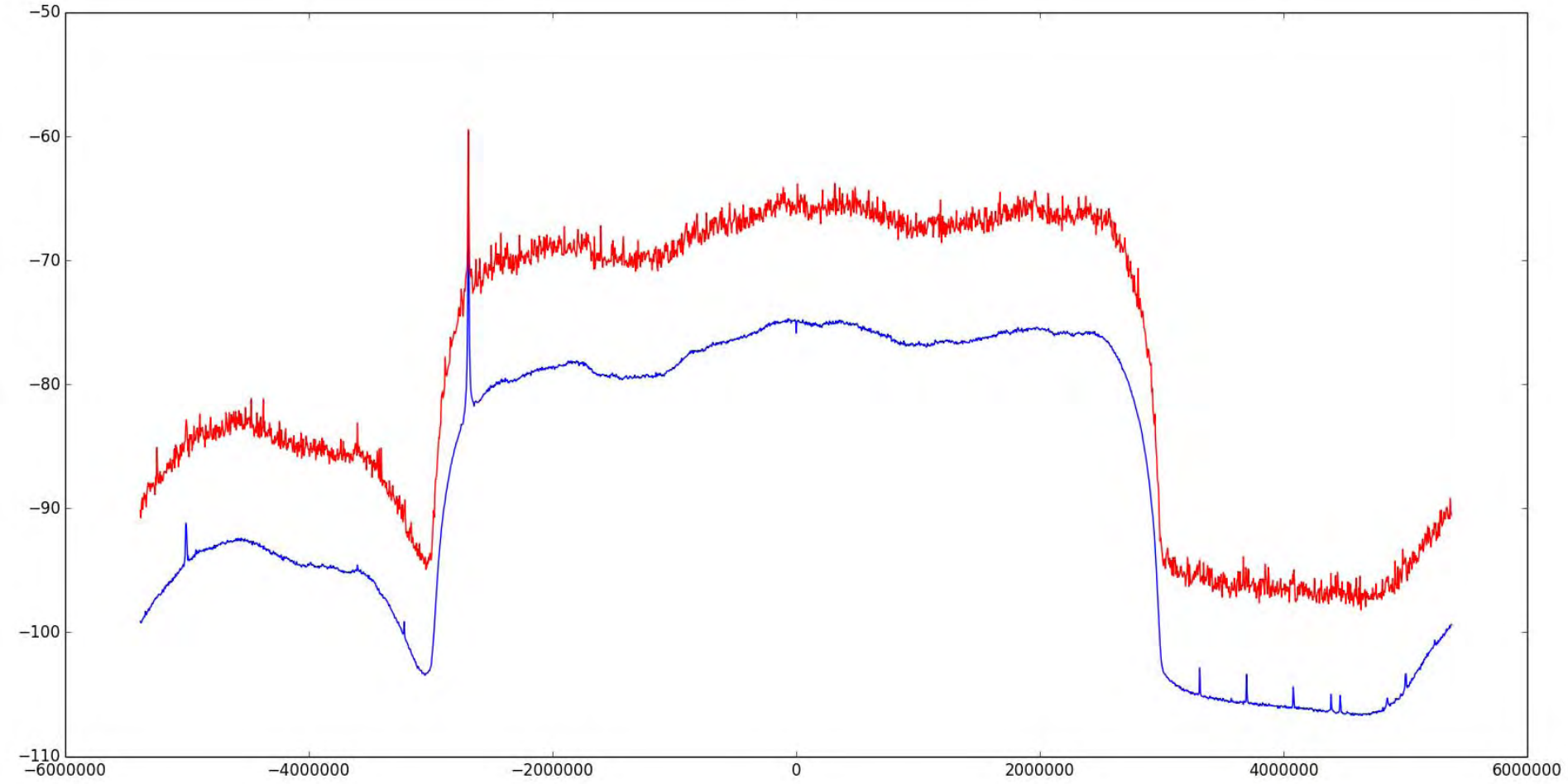

baudline <F1> FFT=2048 sample_rate=250000 Hz=1X timebase=1/2X
0
5
10
15
20
25
30
35
40
45
50
55
60
65
70
75
80
85
90
95
100
105
110
115
120 kHz
LF
UHF
1150
1100
1050
1000
950
900
850
ms
0
-20
-40
-60
-80
-100
-120
dB
124877.93 Hz
835 ms

Latency!

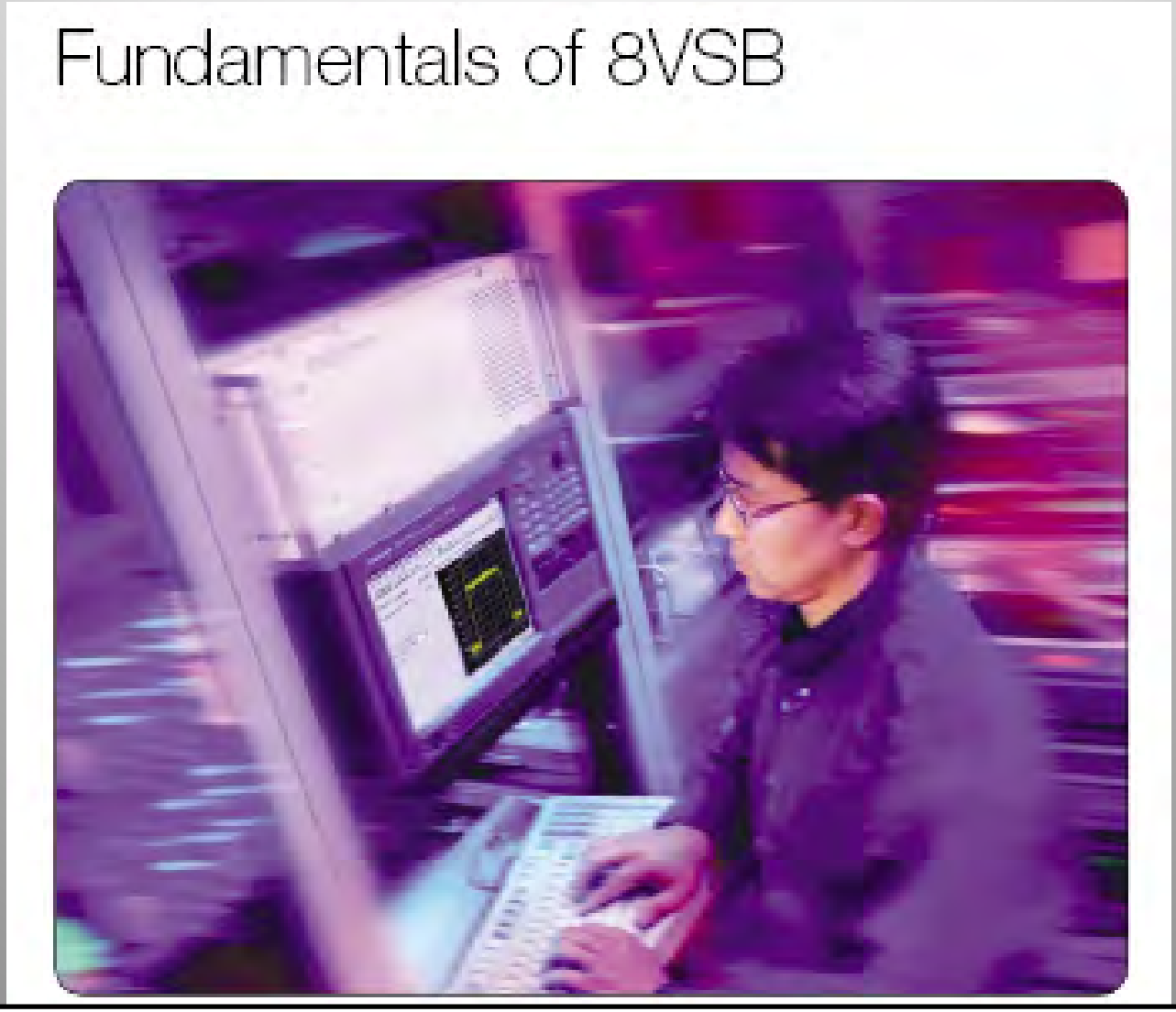


Multipath

ATSC

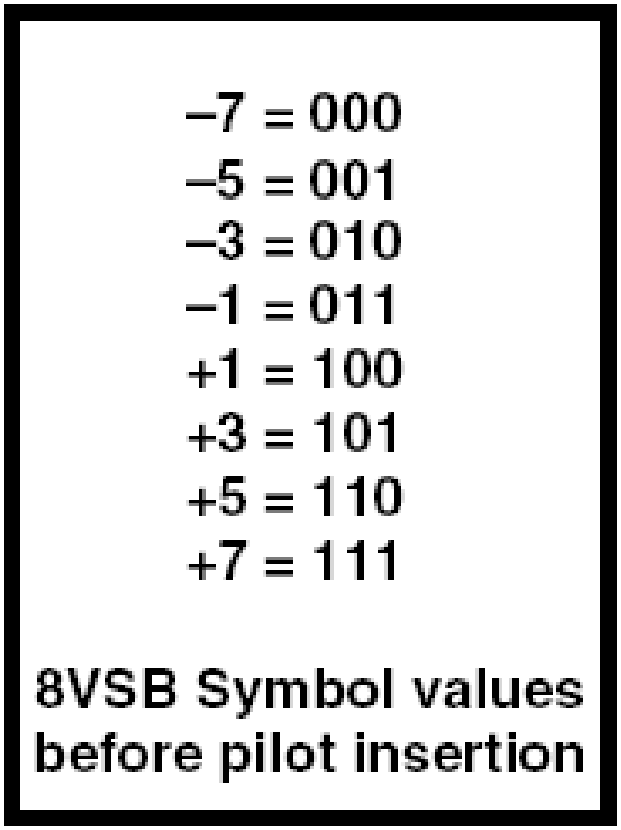

−50
−60
−70
−80
−90
−100
−110
−6000000
−4000000
−2000000
0
2000000
4000000
6000000

8VSB



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

8VSB



Calculation of Symbol Rate:

Sr (MHz) = 4.5 / 286 x 684 = 10.76 MHz

Frequency of a Data Segment:

f_{seq} = Sr / 832 = 12.94 x 10^3 data segments/s

Data Frame Rate:

$f_{frame} = f_{seg}$ / 620 = 20.66 frames/s

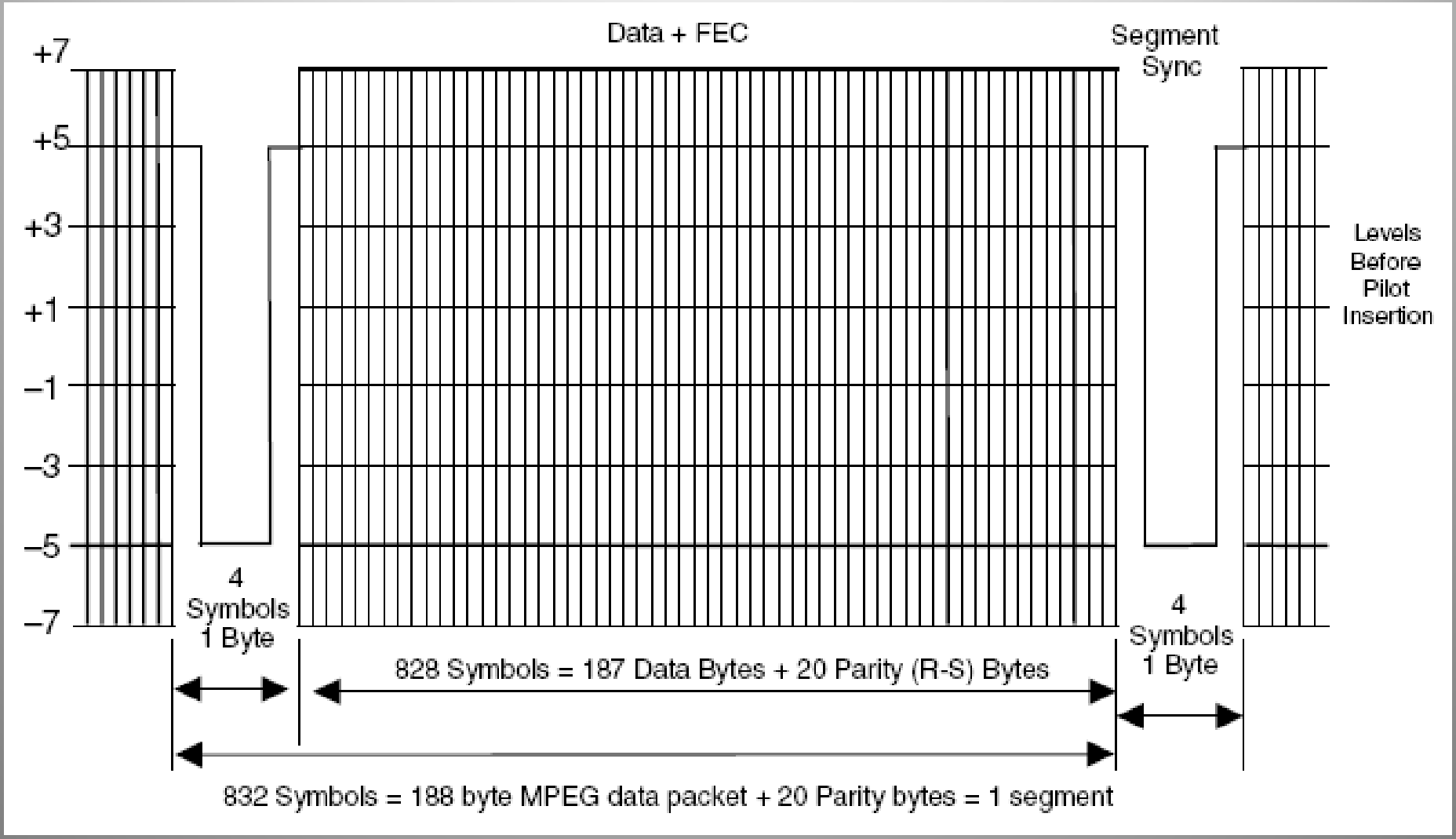
Total Number of Bits:

187 data + 20 RS = 207 byte packet = 1656 bits

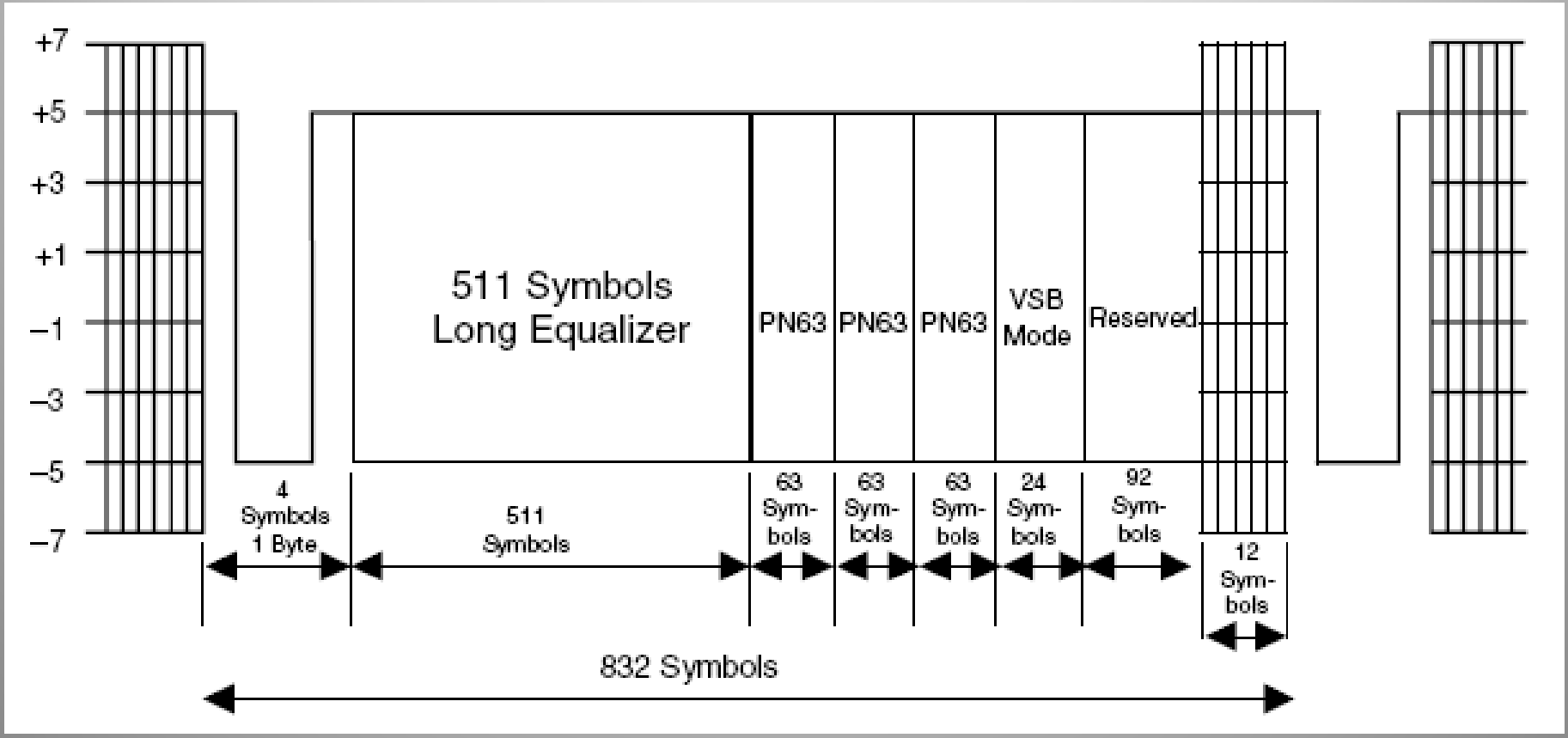
Trellis coding requires:

3 / 2 x 1656 bits = 2484 bits

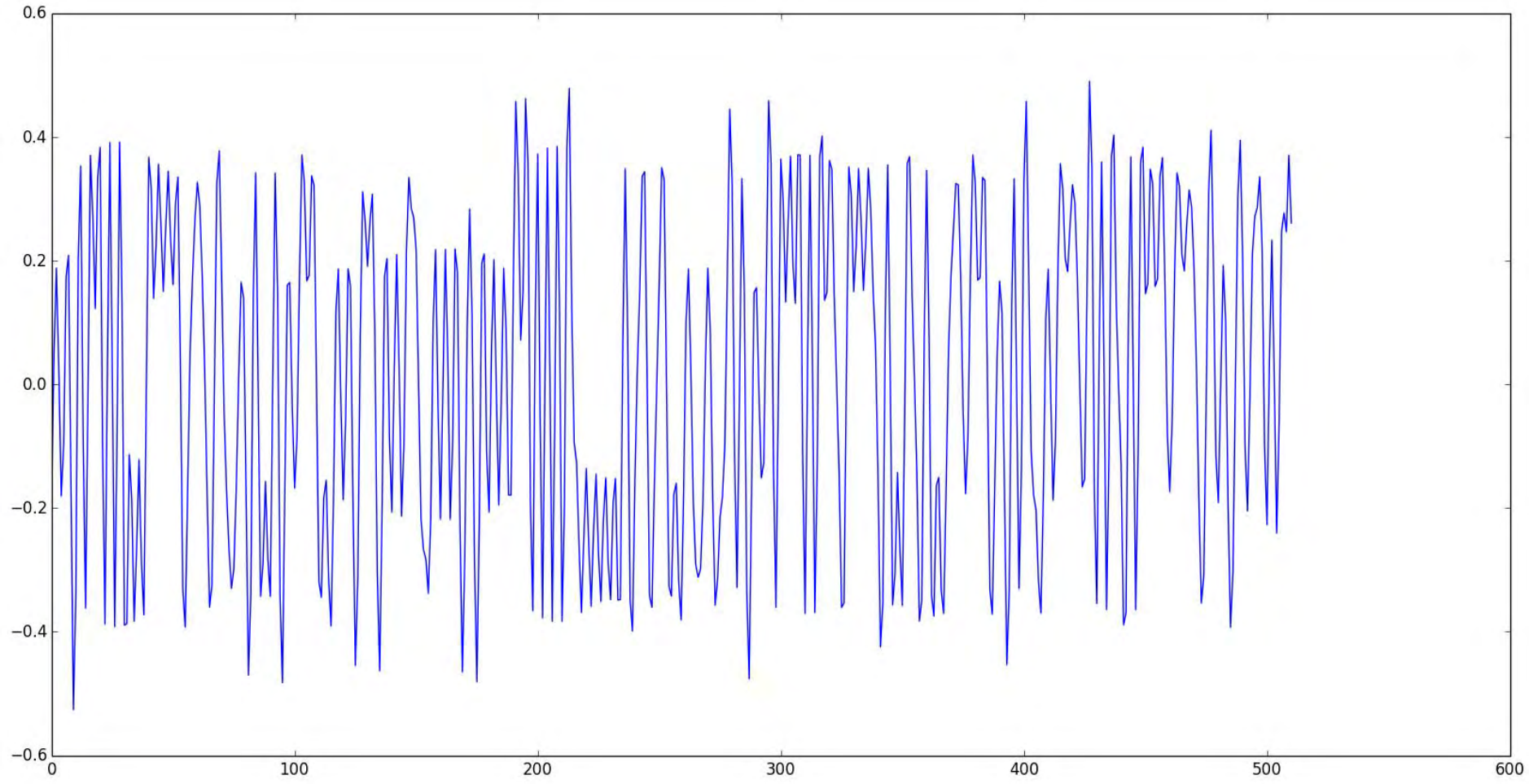
Synchronisation

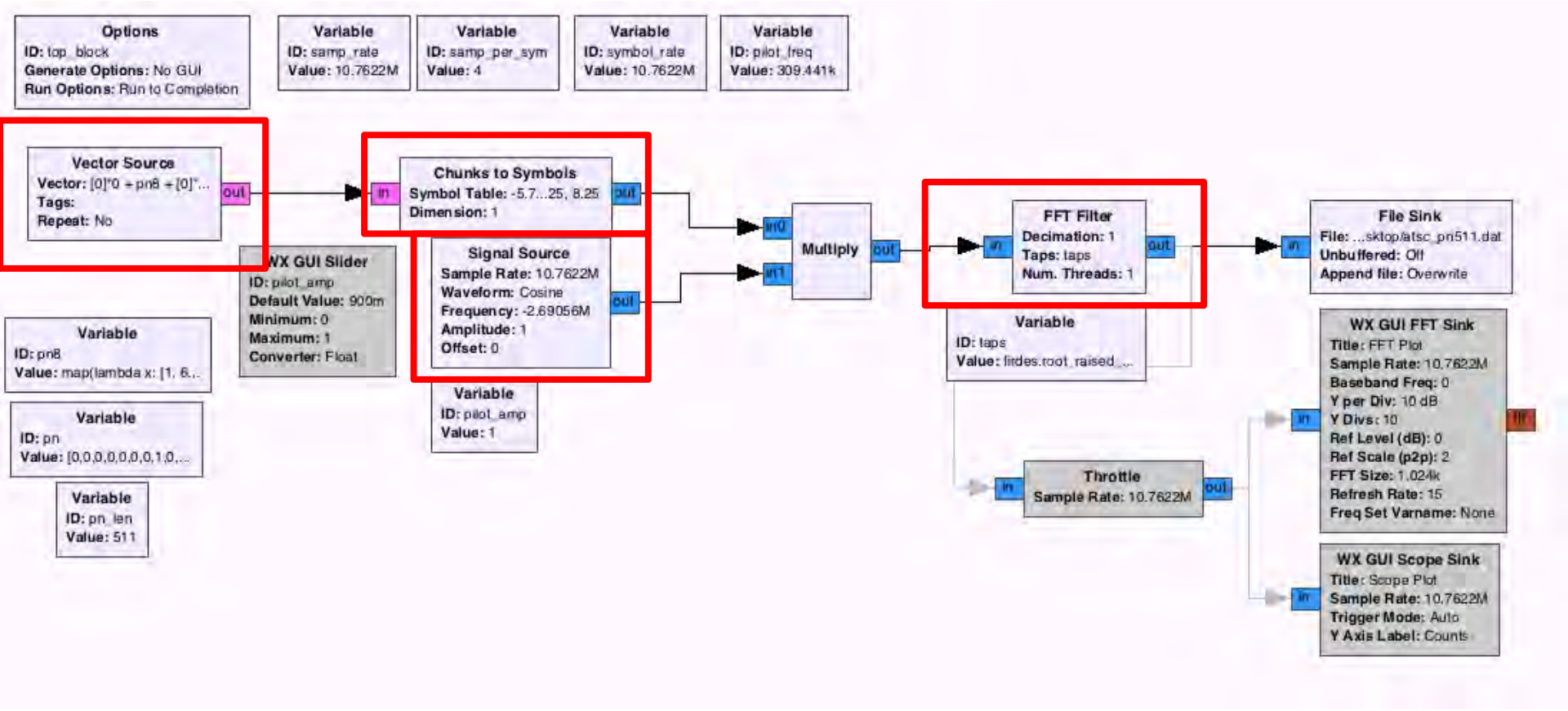


Synchronisation

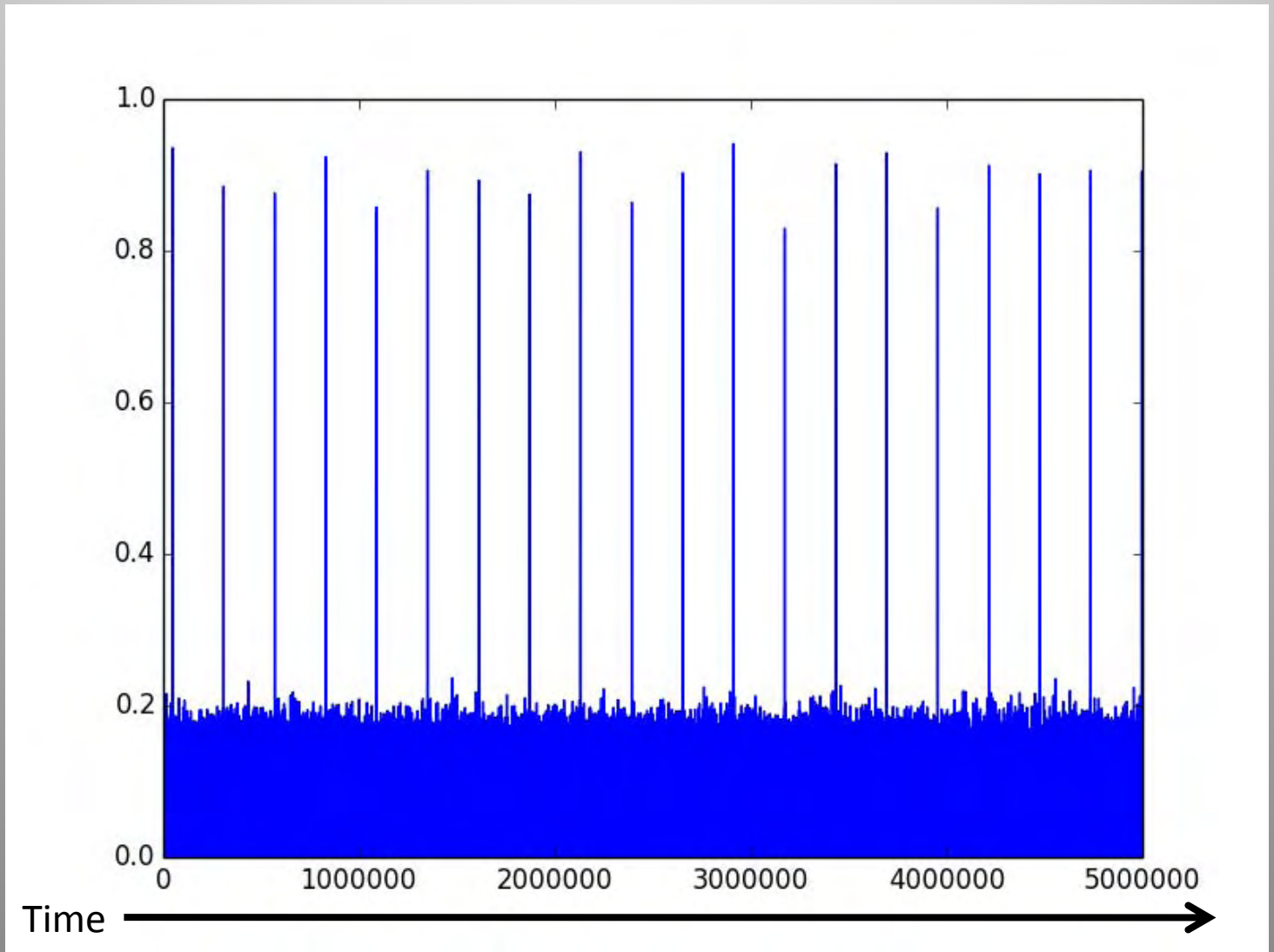


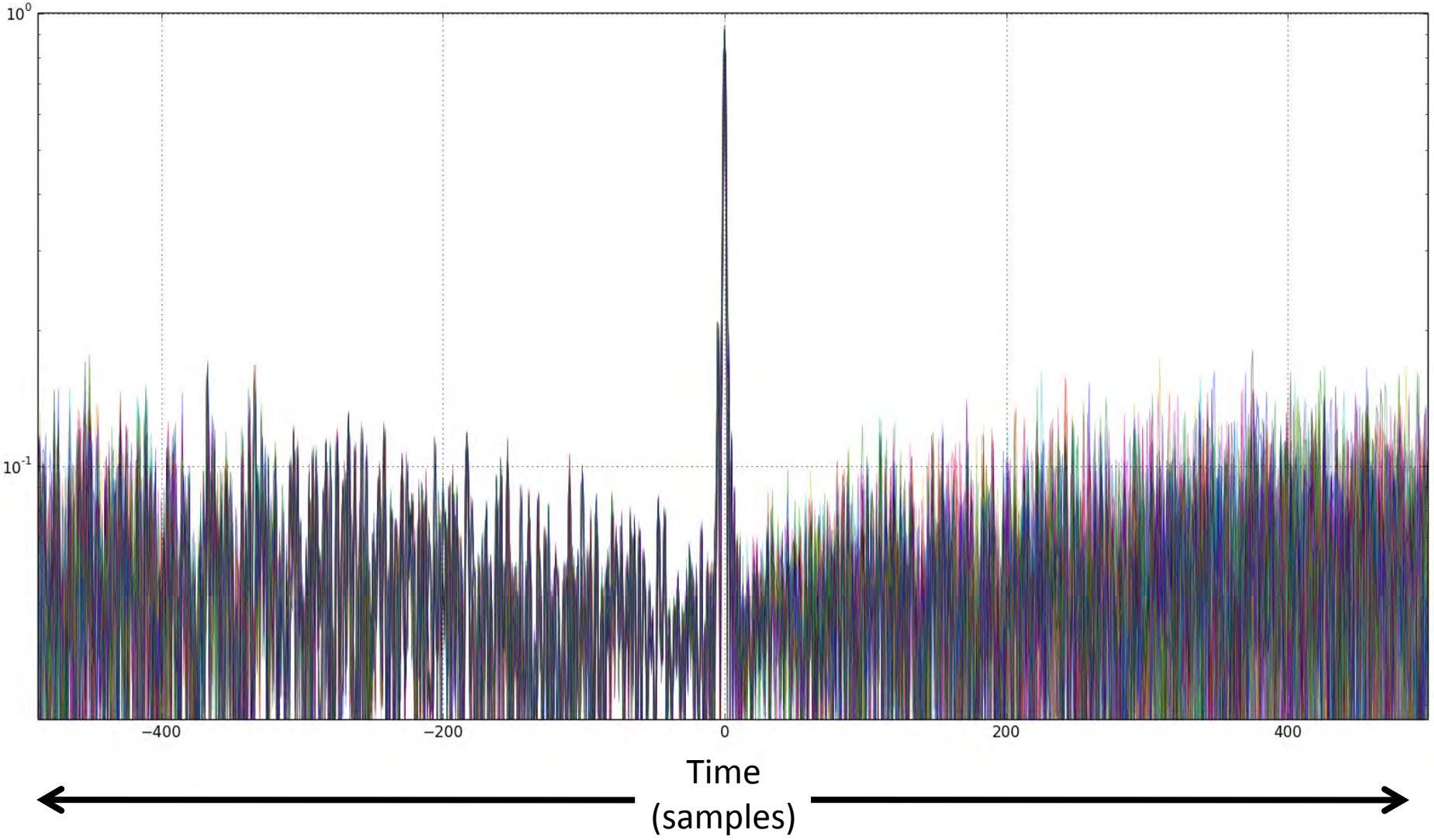
PN511

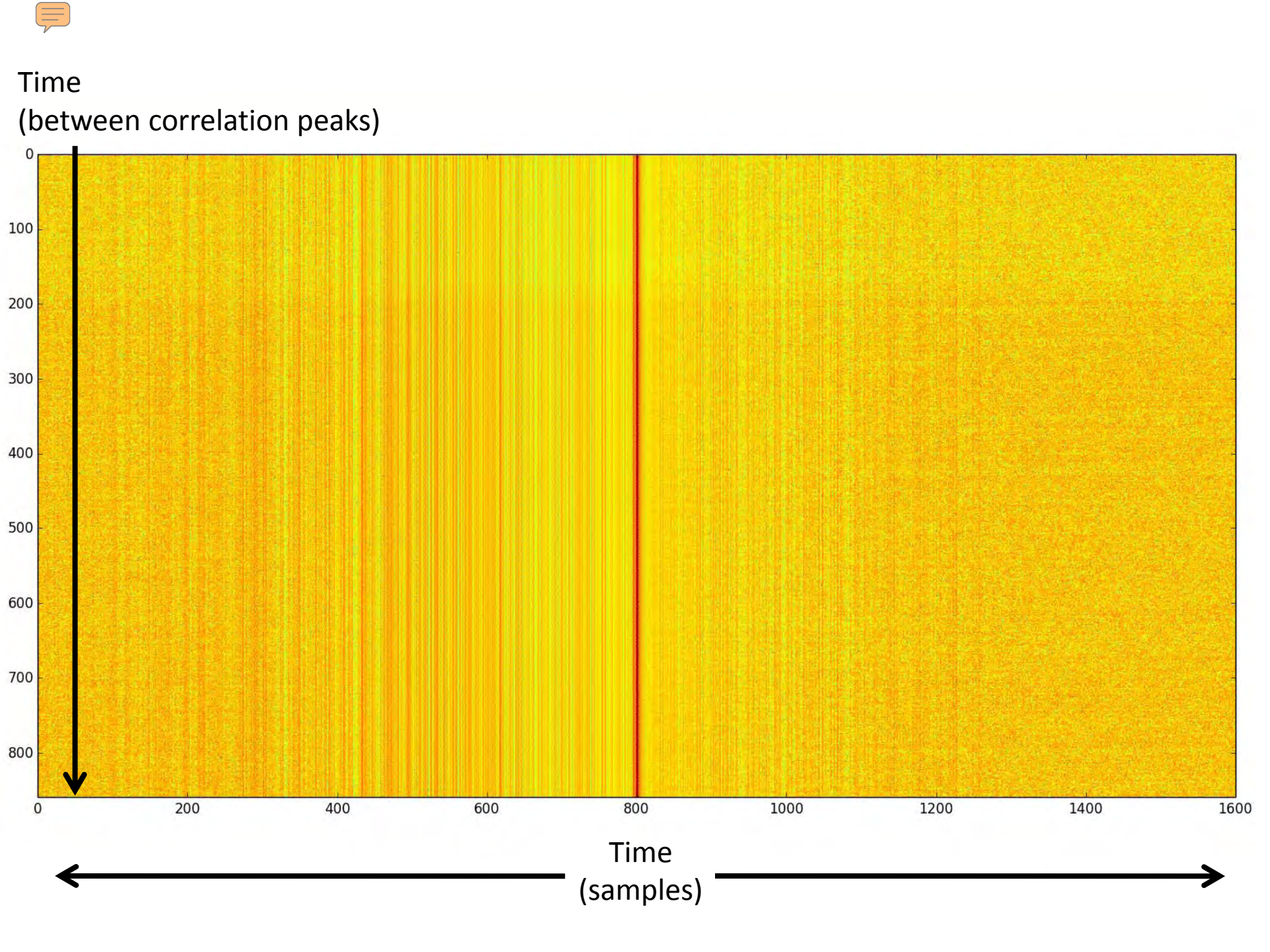



Options
ID: top_block
Generate Options: No GUI
Run Options: Run to Completion
Variable
ID: samp_rate
Value: 10.7622M
Variable
ID: samp_per_sym
Value: 4
Variable
ID: symbol_rate
Value: 10.7622M
Variable
ID: pilot_freq
Value: 309.441k
Vector Source
Vector: [0]*0 + pn8 + [0]*...
Tags:
Repeat: No
out
Chunks to Symbols
Symbol Table: -5.7...25, 8.25
Dimension: 1
in
out
WX GUI Slider
ID: pilot_amp
Default Value: 900m
Minimum: 0
Maximum: 1
Converter: Float
Signal Source
Sample Rate: 10.7622M
Waveform: Cosine
Frequency: -2.69056M
Amplitude: 1
Offset: 0
Variable
ID: pilot_amp
Value: 1
Multiply
in0
in1
out
FFT Filter
Decimation: 1
Taps: taps
Num. Threads: 1
Variable
ID: taps
Value: firdes.root_raised_...
Throttle
Sample Rate: 10.7622M
File Sink
File: ...sktop/atsc_pn511.dat
Unbuffered: Off
Append file: Overwrite
WX GUI FFT Sink
Title: FFT Plot
Sample Rate: 10.7622M
Baseband Freq: 0
Y per Div: 10 dB
Y Divs: 10
Ref Level (dB): 0
Ref Scale (p2p): 2
FFT Size: 1.024k
Refresh Rate: 15
Freq Set Varname: None
WX GUI Scope Sink
Title: Scope Plot
Sample Rate: 10.7622M
Trigger Mode: Auto
Y Axis Label: Counts
Variable
ID: pn8
Value: map(lambda x: [1, 6,..
Variable
ID: pn
Value: [0,0,0,0,0,0,0,1,0,...
Variable
ID: pn_len
Value: 511

Correlation Peaks




10^0
10^{-1}
−400
−200
0
200
400
Time
(samples)

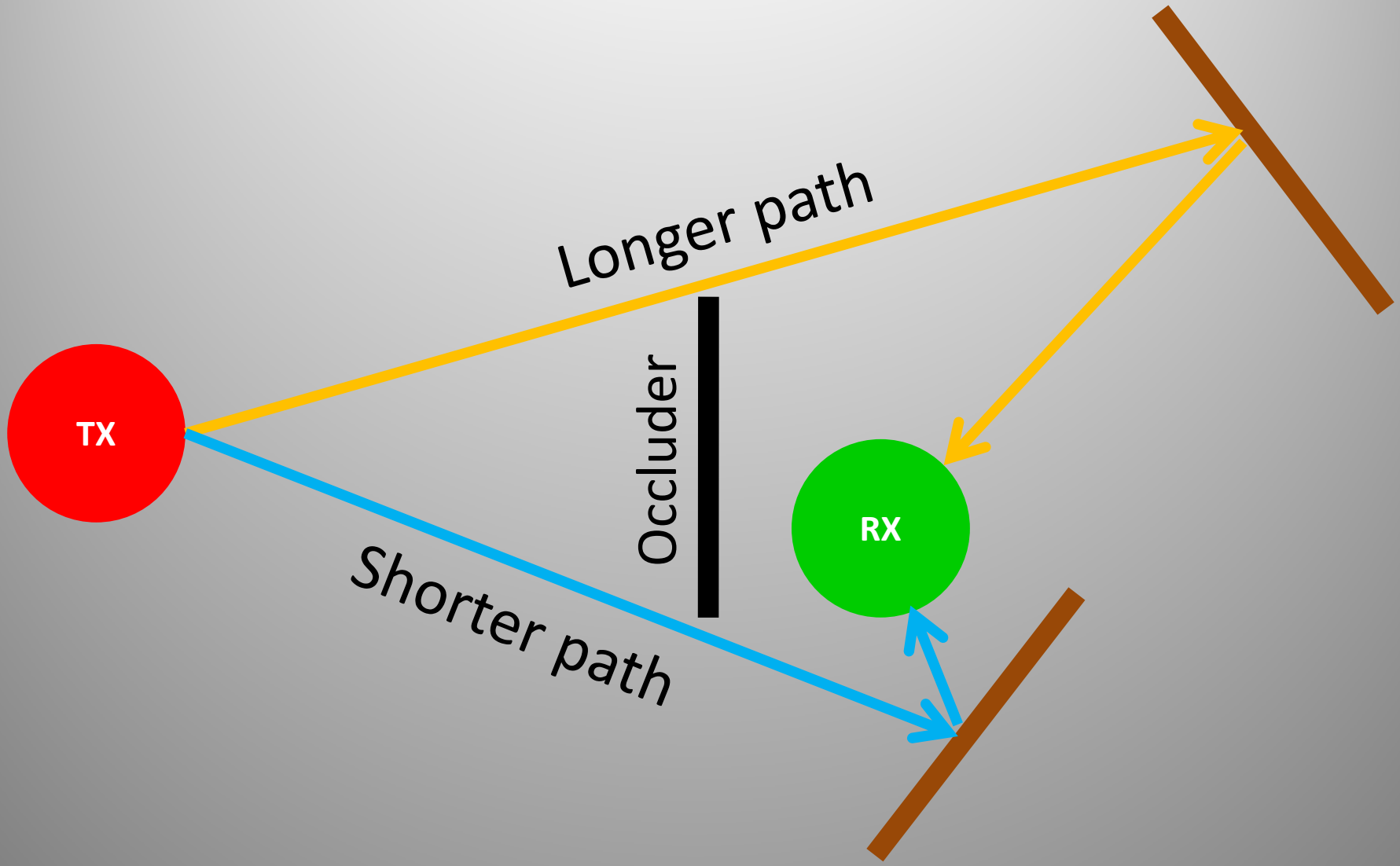

Time
(between correlation peaks)
0
100
200
300
400
500
600
700
800
0
200
400
600
800
1000
1200
1400
1600
Time
(samples)

Direct Path

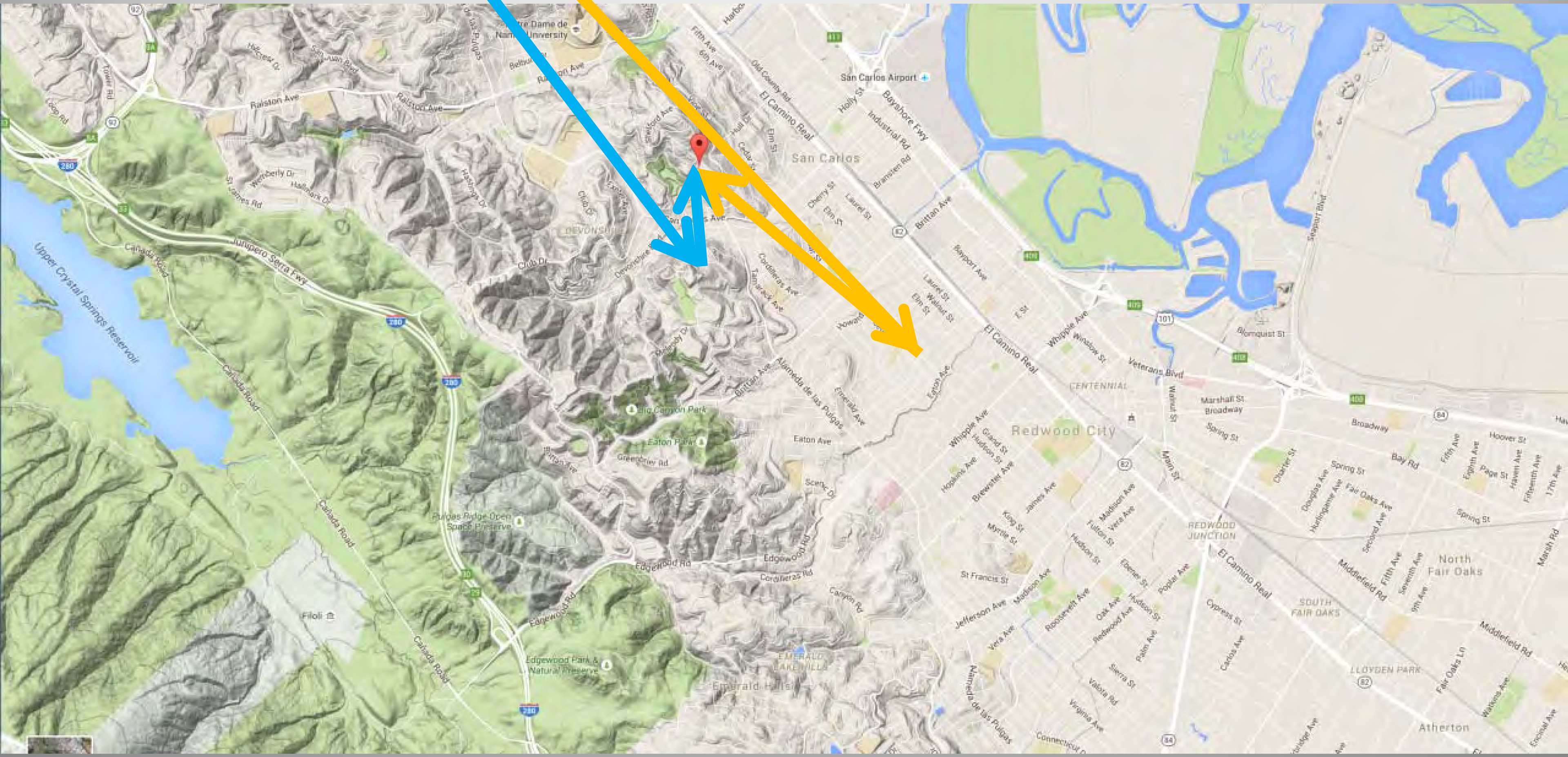
Longer path

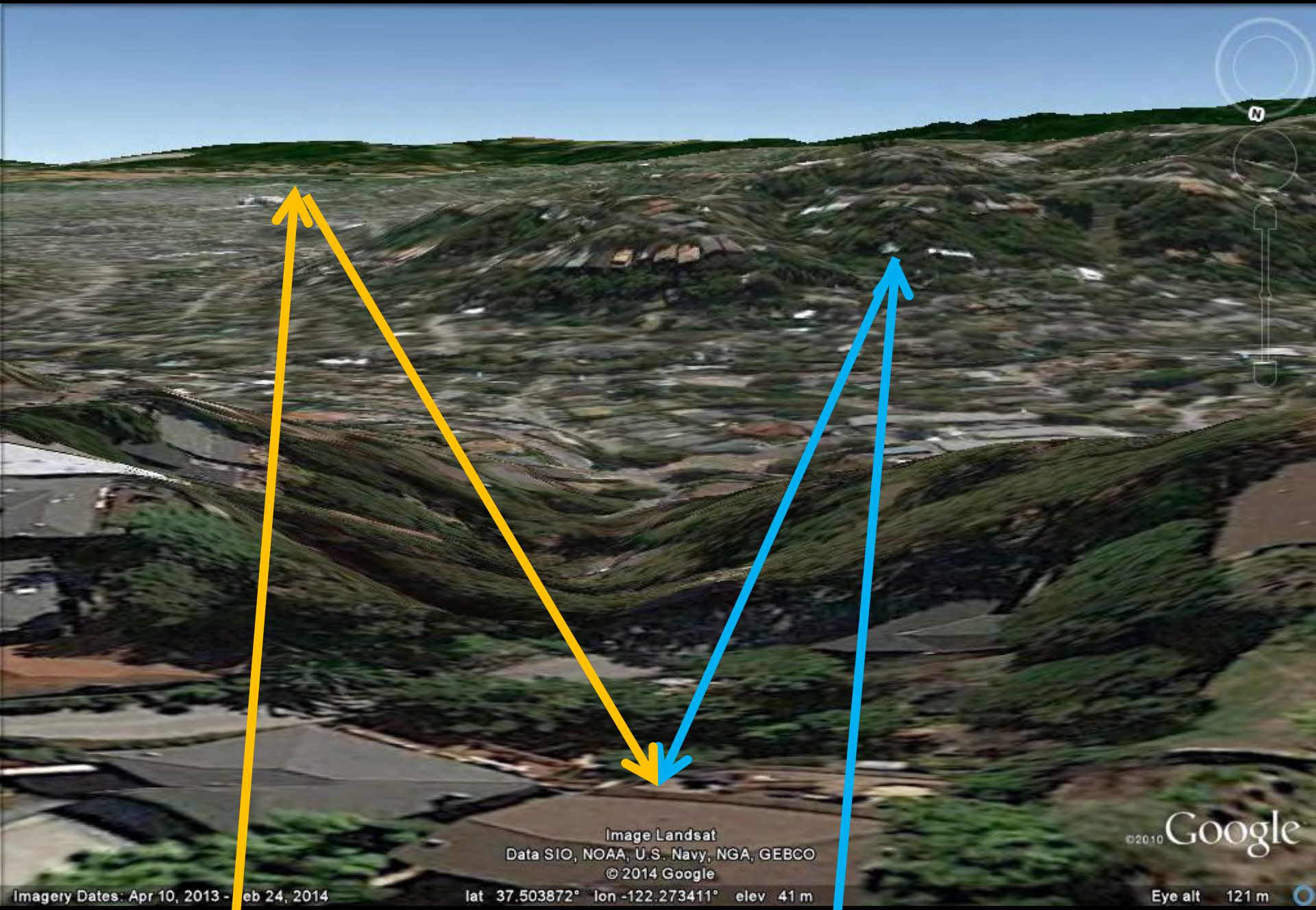
No reflection

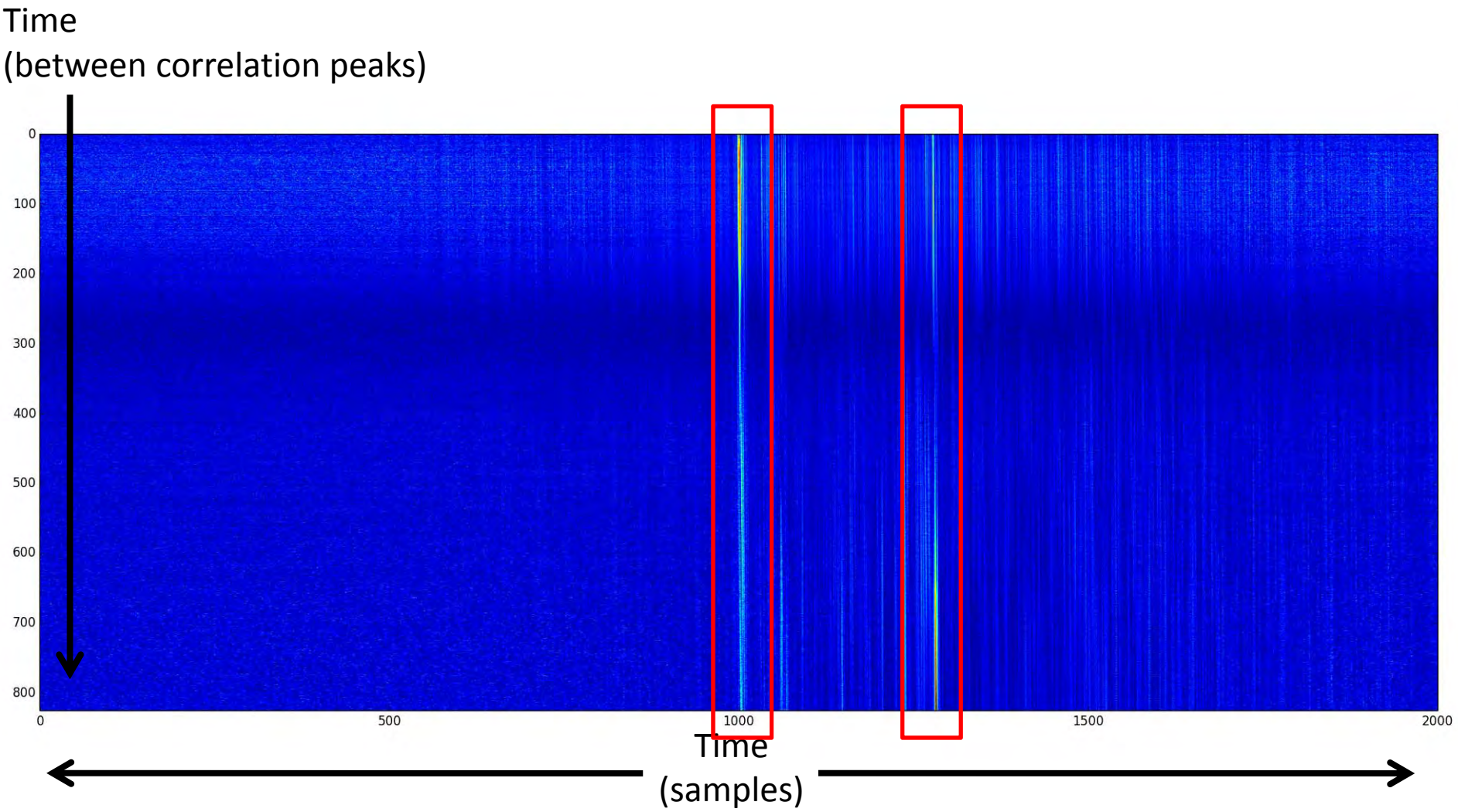
Multipath

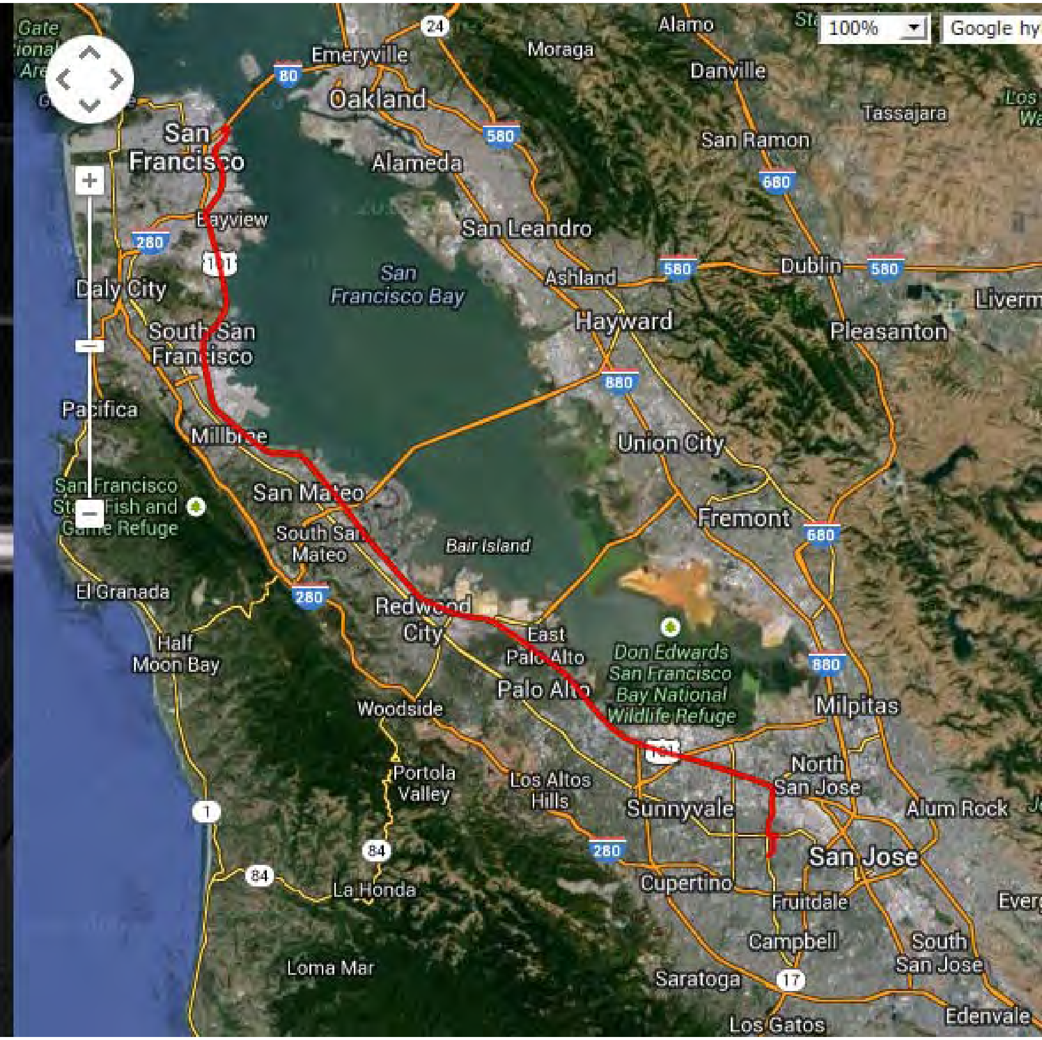


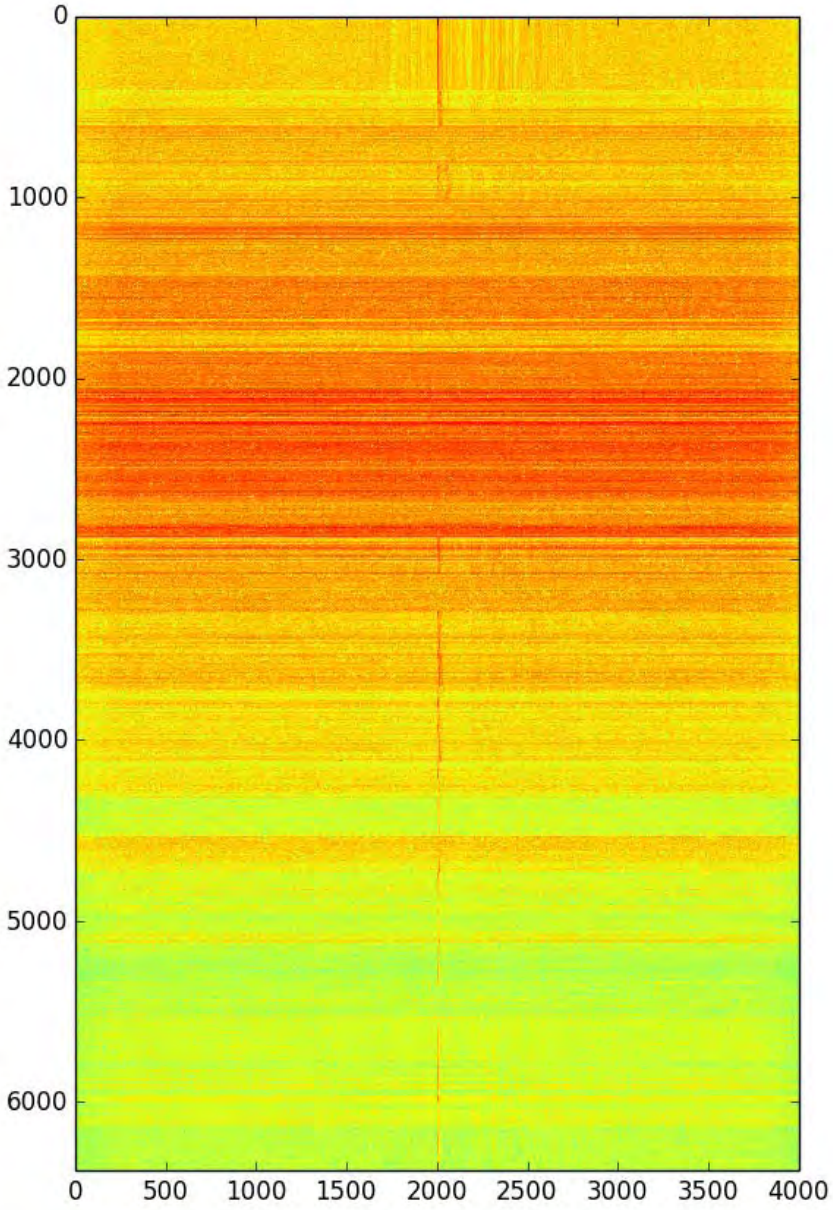
Map

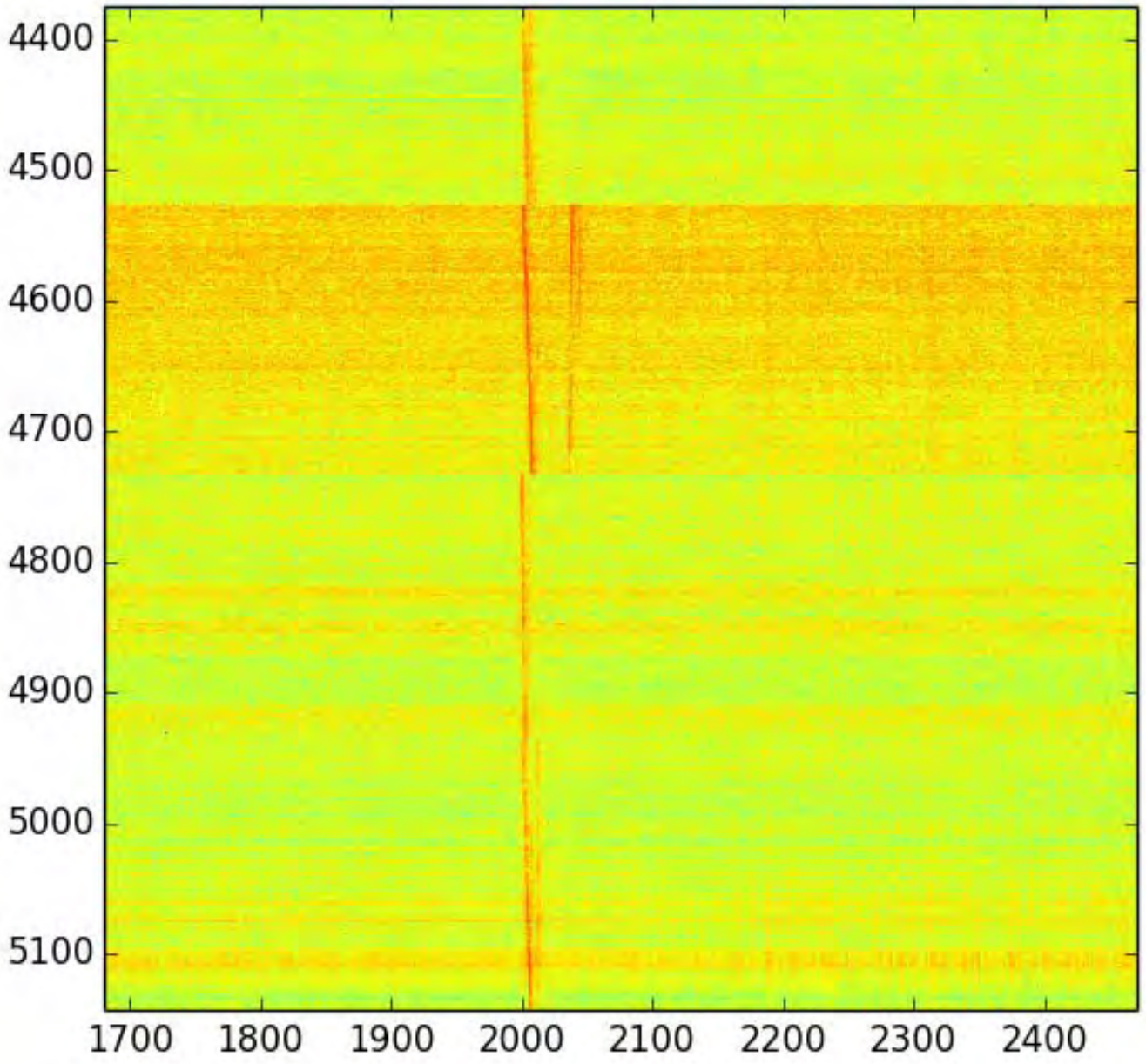

San Carlos
Redwood City
San Carlos Airport
Upper Crystal Springs Reservoir
Junipero Serra Fwy
El Camino Real
Bayshore Fwy
Big Canyon Park
Eaton Park
Pulgas Ridge Open Space Preserve
Edgewood Park & Natural Preserve
Filoli
Emerald Hills
Redwood Junction
North Fair Oaks
Atherton
Centennial
Devonshire
South Fair Oaks
Lloyden Park
Notre Dame de Namur University
Ralston Ave
Alameda de las Pulgas
Edgewood Rd
Canada Road
Veterans Blvd
Broadway
Middlefield Rd


N
Image Landsat
Data SIO, NOAA, U.S. Navy, NGA, GEBCO
© 2014 Google
©2010 Google
Imagery Dates: Apr 10, 2013 - eb 24, 2014
lat 37.503872° lon -122.273411° elev 41 m
Eye alt 121 m

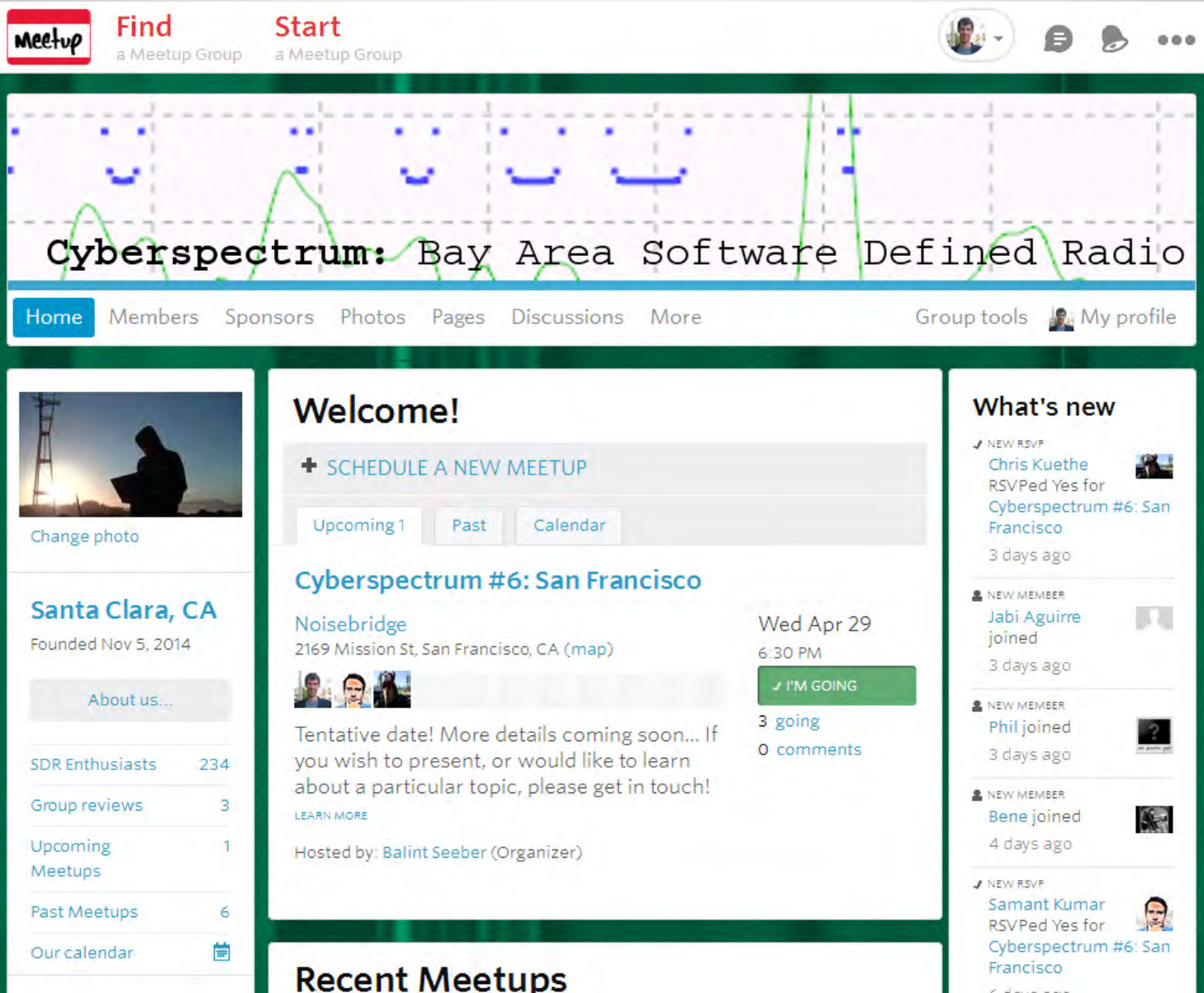

Time
(between correlation peaks)
0
100
200
300
400
500
600
700
800
0
500
1000
1500
2000
Time
(samples)


100%
Emeryville
Oakland
Alamo
Moraga
Danville
Tassajara
San Ramon
San Francisco
Alameda
Bayview
San Leandro
Ashland
Dublin
Daly City
San Francisco Bay
Hayward
Pleasanton
South San Francisco
Pacifica
Millbrae
Union City
San Mateo
South San Mateo
Bair Island
Fremont
El Granada
Redwood City
East Palo Alto
Half Moon Bay
Palo Alto
Don Edwards San Francisco Bay National Wildlife Refuge
Milpitas
Woodside
Portola Valley
Los Altos Hills
North San Jose
Sunnyvale
Alum Rock
San Jose
La Honda
Cupertino
Fruitdale
Campbell
South San Jose
Loma Mar
Saratoga
Los Gatos
Edenvale


0
1000
2000
3000
4000
5000
6000
0
500
1000
1500
2000
2500
3000
3500
4000


4400
4500
4600
4700
4800
4900
5000
5100
1700
1800
1900
2000
2100
2200
2300
2400

Cyberspectrum SDR Meetups




Cyberspectrum #10
Washington, D.C.
meetup.com/Cyberspectrum
VirginiaTech
Invent the Future
Ted and Karyn
Hume Center for National Security and Technology
Wednesday 26th


http://wiki.spench.net/wiki/RF
http://spench.net/
GitHub: balint256
balint@spench.net
balint@bastille.io
@spenchdotnet