Searchlight: An Accurate, Sensitive, and Fast RF Energy Detection System

Richard Bell, Isamu Poy, Kyle Watson, Tianyi Hu, fred harris, and Dinesh Bharadia

30 October – 3 November 2023 // Boston, MA, USA

Motivation: Wireless Security Threats

5G
Wi Fi
Waveform A
Waveform B
Decibels
Frequency (Hz)
x 10^4

Video Recording

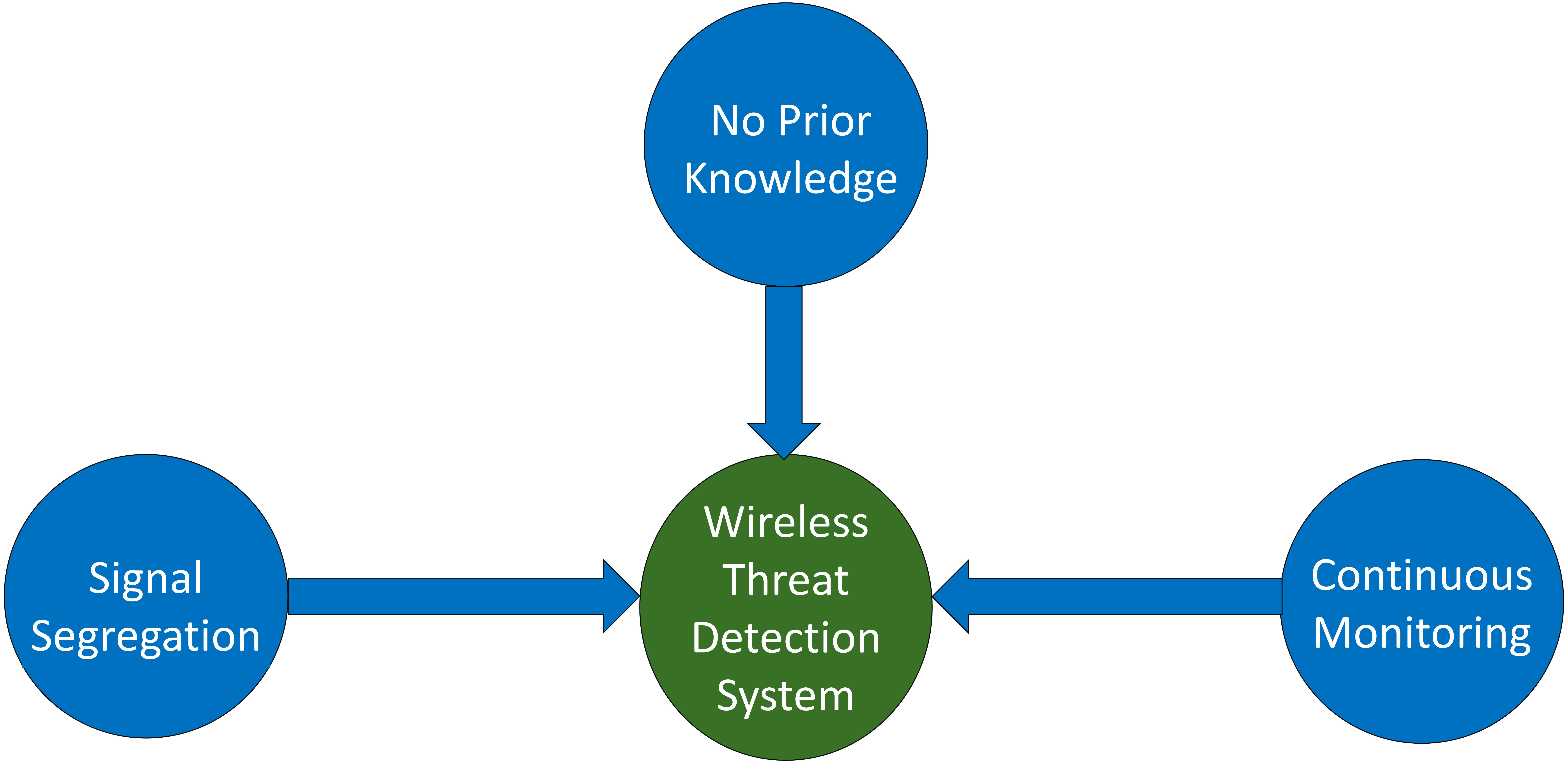
Audio Recording

Family finds hidden camera livestreaming from their Airbnb in Ireland

https://www.cnn.com/2019/04/05/europe/ireland-airbnb-hidden-camera-scli-intl

Concealed Devices

Three requirements of countermeasure systems


No Prior Knowledge

Signal Segregation

Wireless Threat Detection System

Continuous Monitoring

Consumer countermeasures are not sufficient

Entry Level

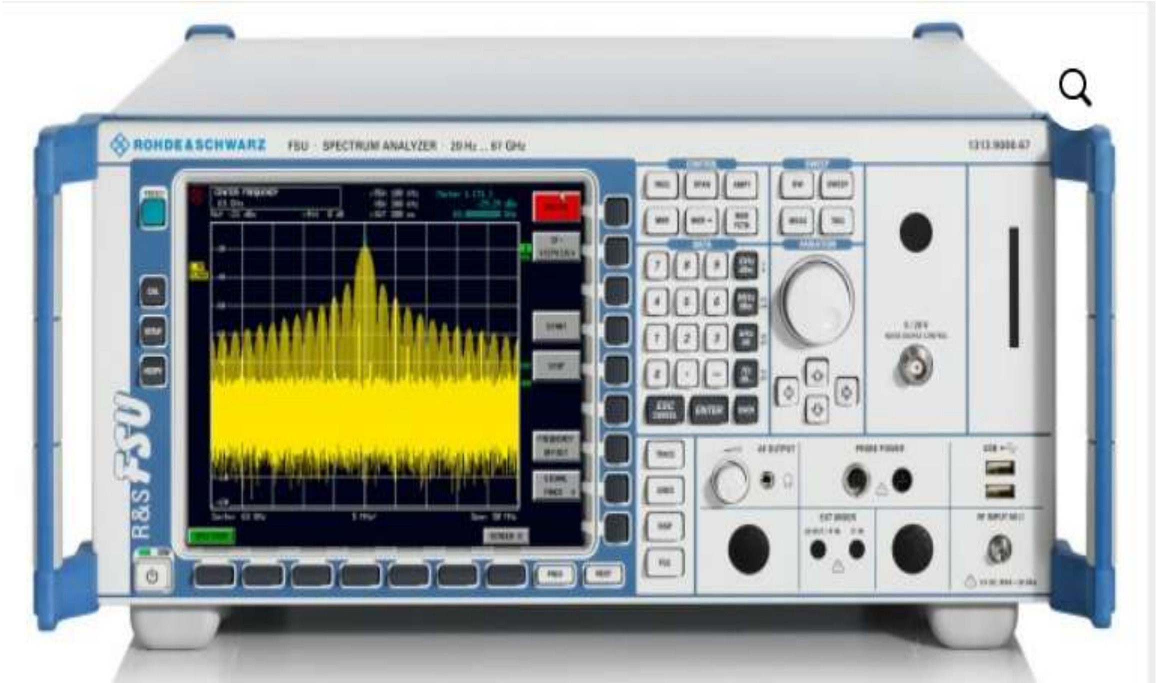
LM-8 Hidden Camera & Bug Detector
$150

T-9 Specialty Bug Detector
$199

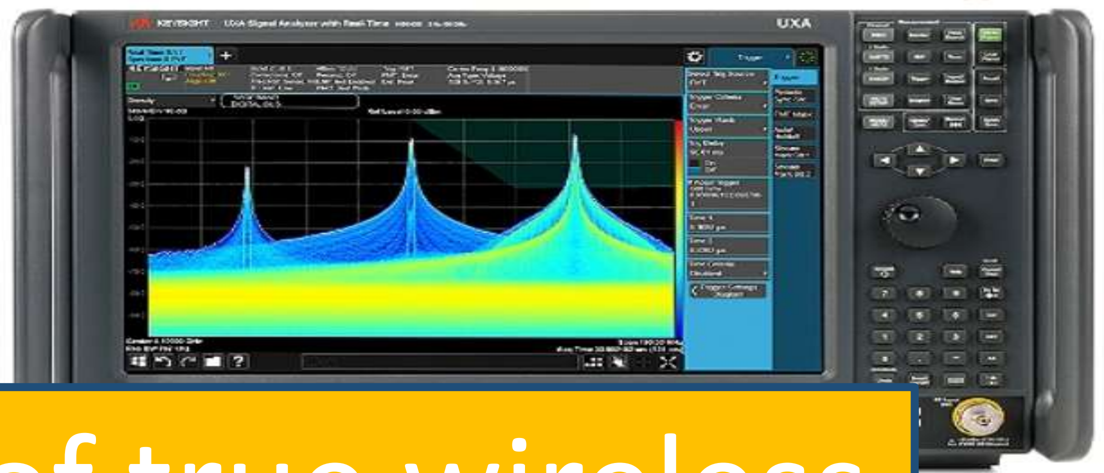
$40

Professional

Signal Hound SM200C
$16,890



Rohde & Schwarz FSU26



$118,435

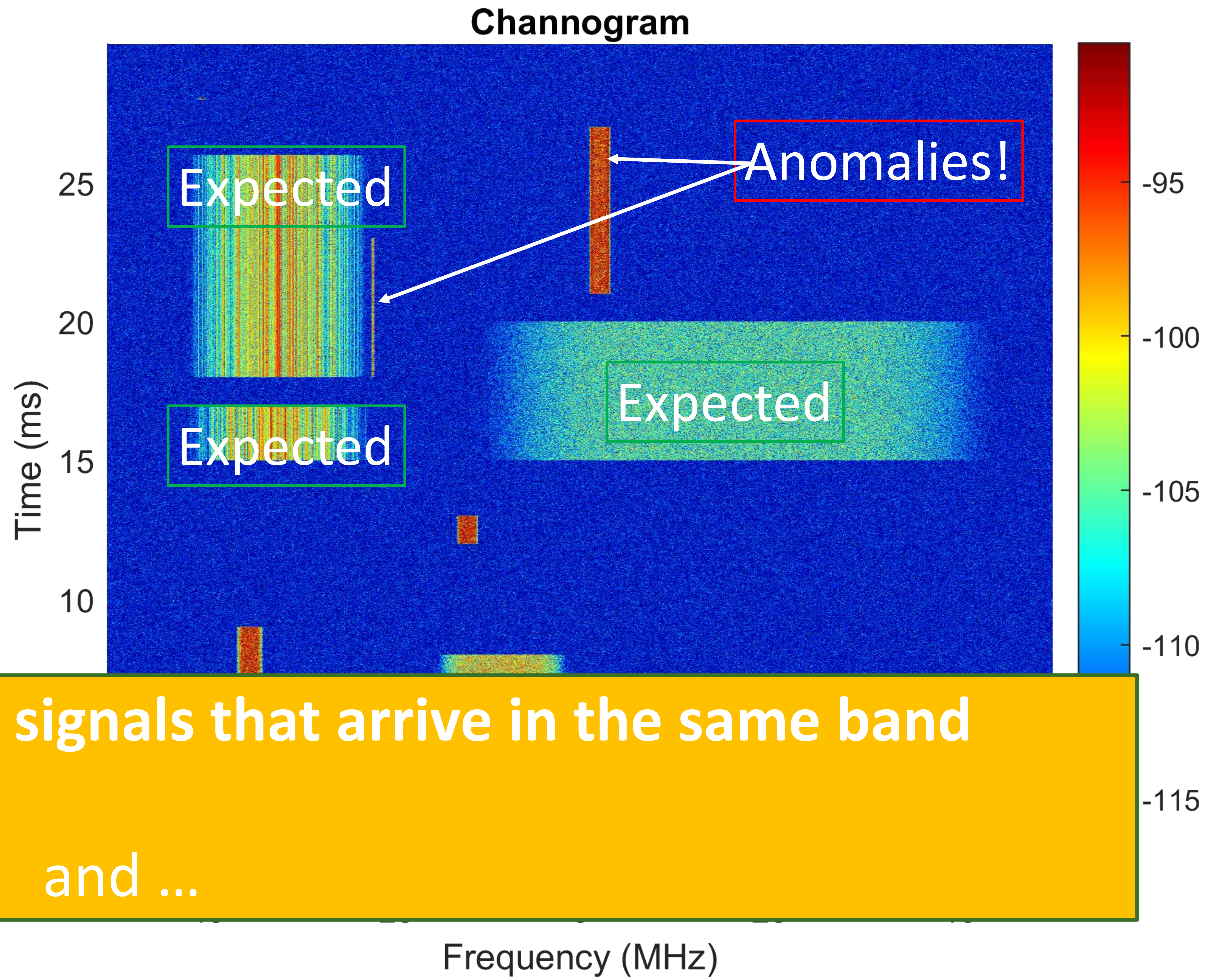
Consumer products lack the features required to alert users of true wireless threats as they occur

No signal segregation
No continuous monitoring

No signal segregation

Why does the system need to segregate signals?

- The receiver cannot control what signals it collects in band
  - If there are many, all of them will be combined into one time series



The system must segregate signals that arrive in the same band

and …

Why can't we assume prior knowledge?

- If you are doing something you shouldn't be, you won't do it in the open
  - Threats will hide and keep information secret

The system must segregate signals that arrive in the same band

The system should not require prior knowledge to perform well

and …

Why is continuous monitoring required?

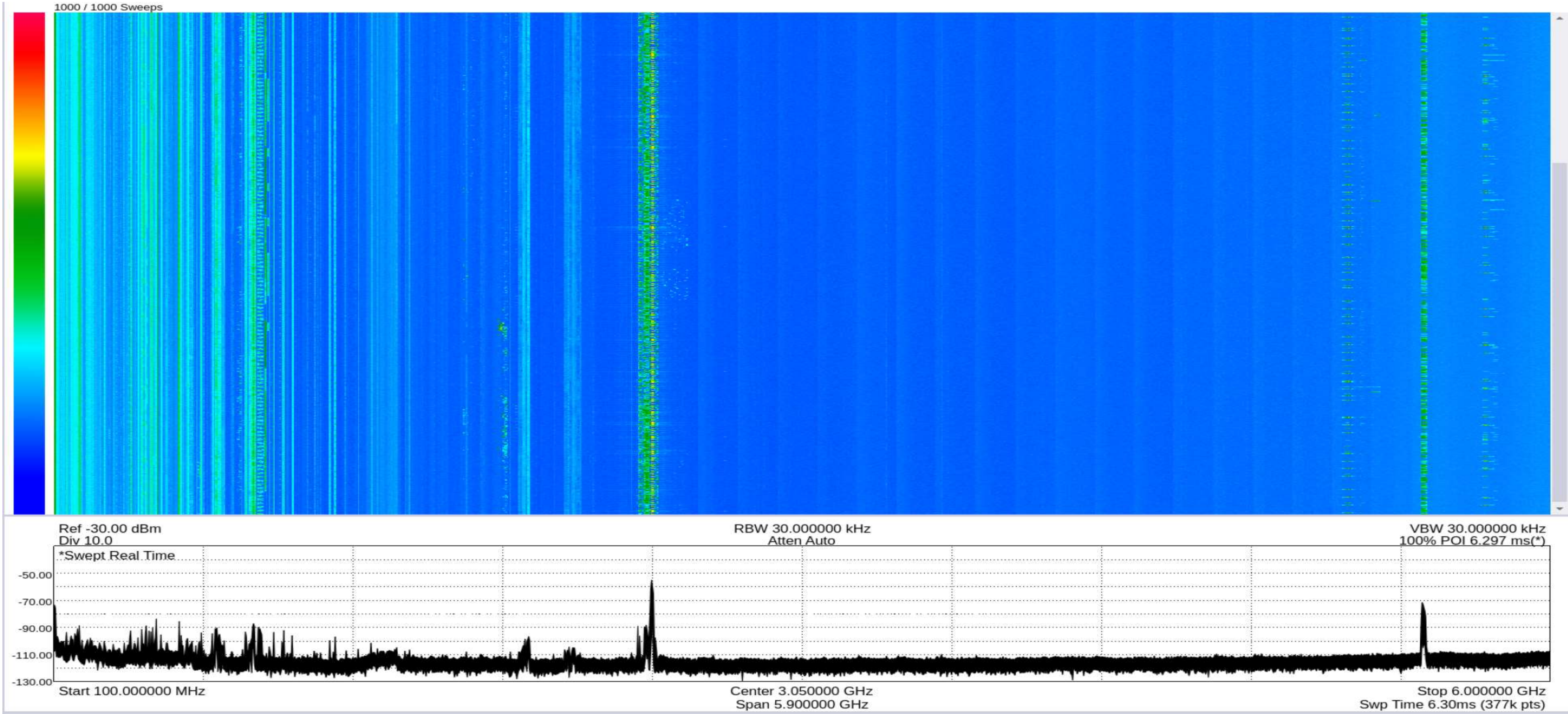
- Receivers support wide instantaneous bandwidth (IBW) to support coverage across 6+ GHz of spectrum
  - USRP N210 40 MHz IBW
  - USRP N320 200 MHz IBW
  - Signal Hound SM200C 160 MHz IBW
- Sample rate of 100 MHz corresponds to 400 MBps continuously needing to be processed
  - Multiple antennas/receivers multiplies this rate up accordingly

The system must segregate signals that arrive in the same band

The system should not require prior knowledge to perform well

The system must be efficient and support this kind of throughput!

Why is this problem hard


1000 / 1000 Sweeps

Ref -30.00 dBm
Div 10.0

RBW 30.000000 kHz
Atten Auto

VBW 30.000000 kHz
100% POI 6.297 ms(*)

*Swept Real Time

Start 100.000000 MHz

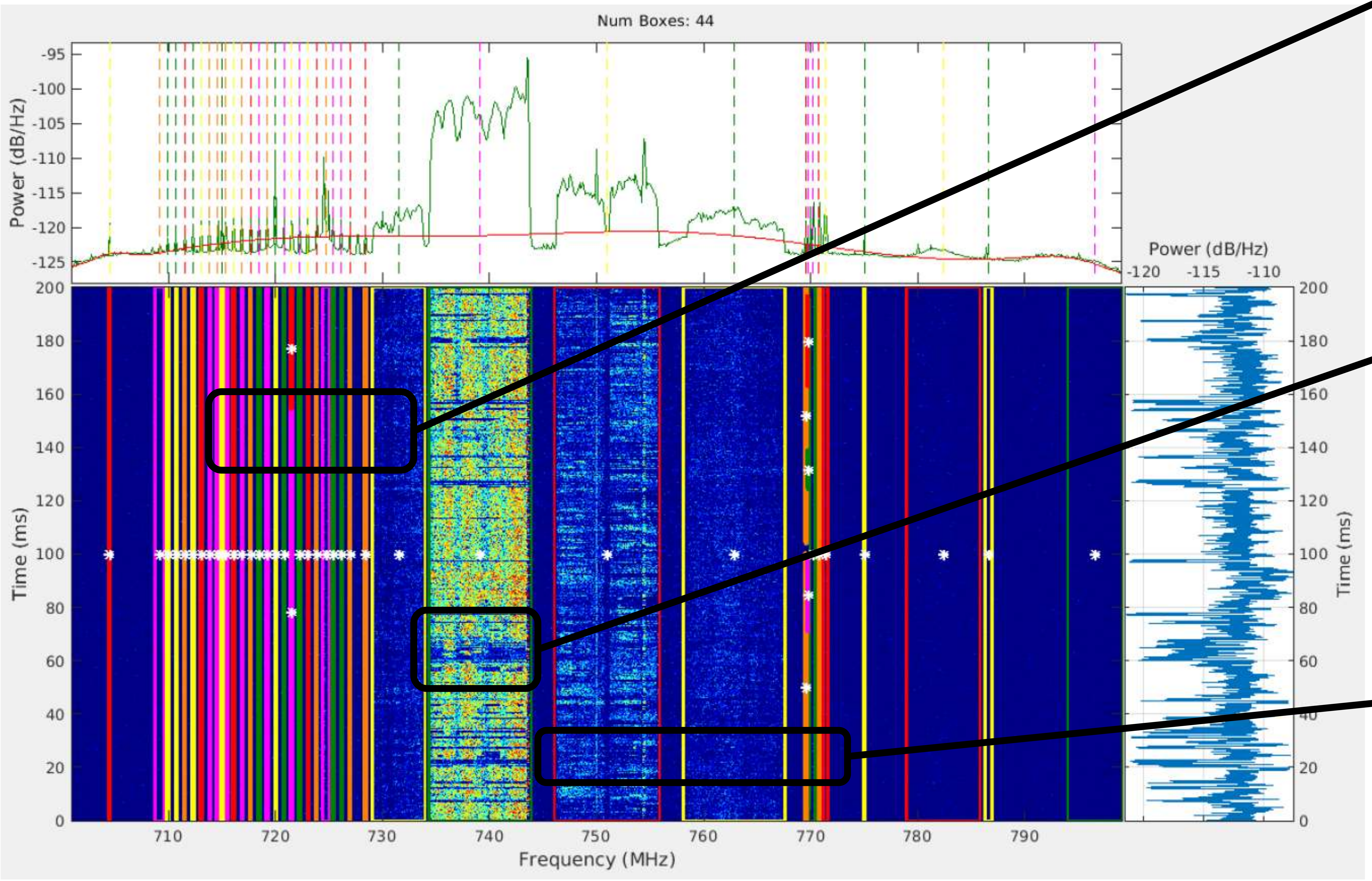
Center 3.050000 GHz
Span 5.900000 GHz

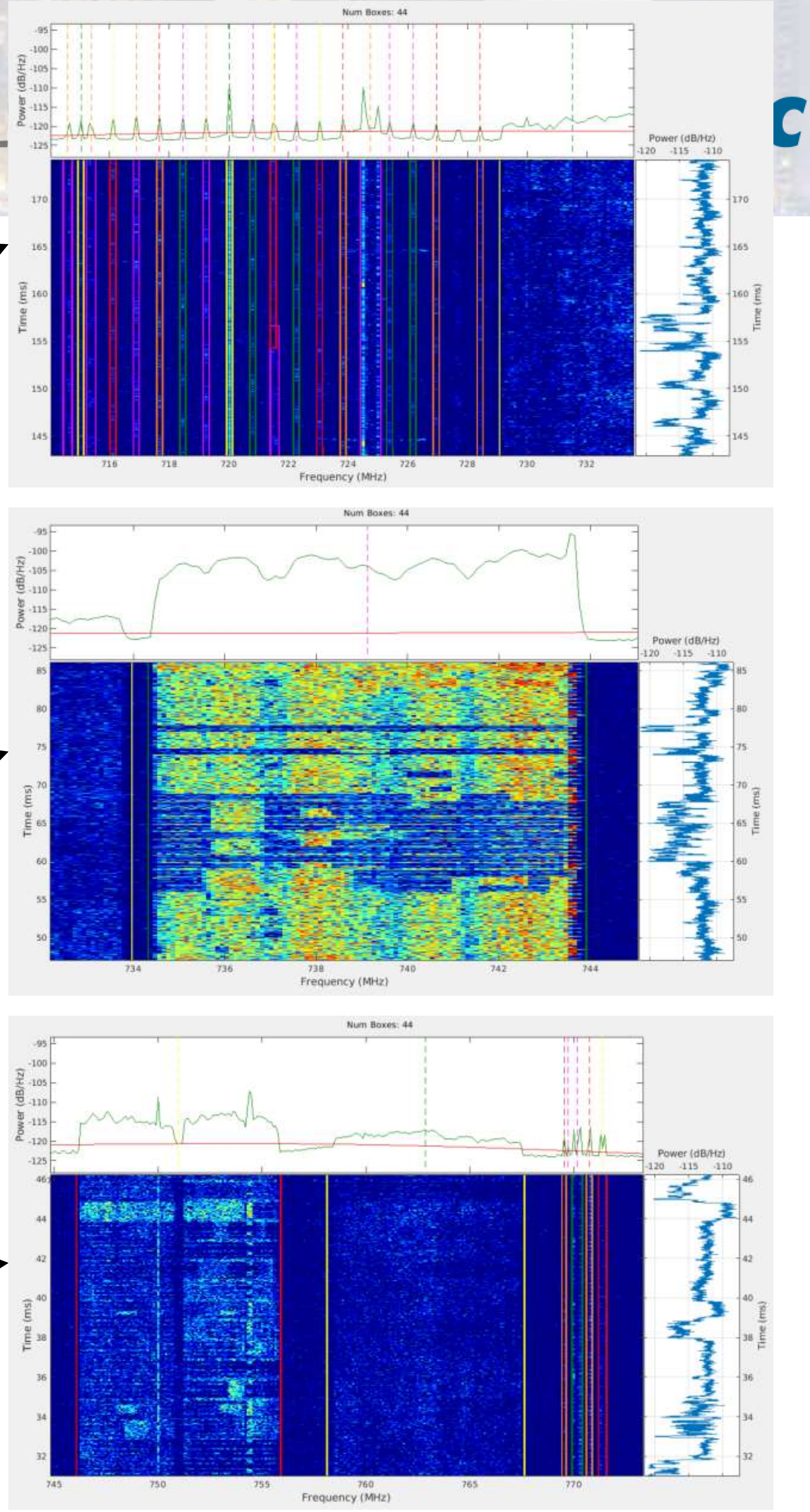
Stop 6.000000 GHz
Swp Time 6.30ms (377k pts)

Why is this problem hard?
Spectrum Example – 2.45 GHz

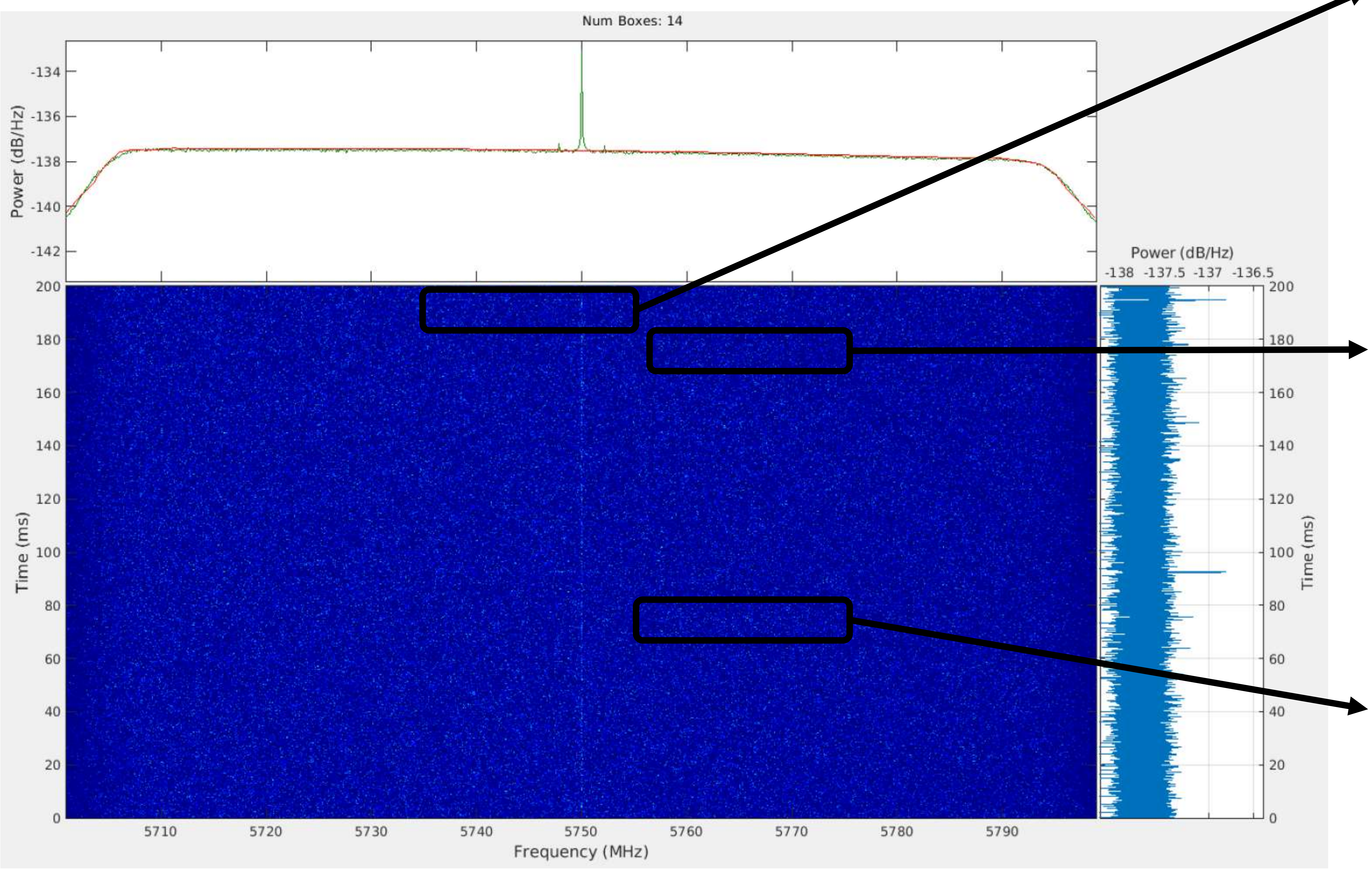
Num Boxes: 376
Power (dB/Hz)
-85
-90
-95
-100
-105
Power (dB/Hz)
-110
-90
Time (ms)
200
180
160
140
120
100
80
60
40
20
0
2410
2420
2430
2440
2450
2460
2470
2480
2490
Frequency (MHz)
Time (ms)
Num Boxes: 376
Frequency (MHz)
Num Boxes: 376
Frequency (MHz)
Num Boxes: 376
Frequency (MHz)

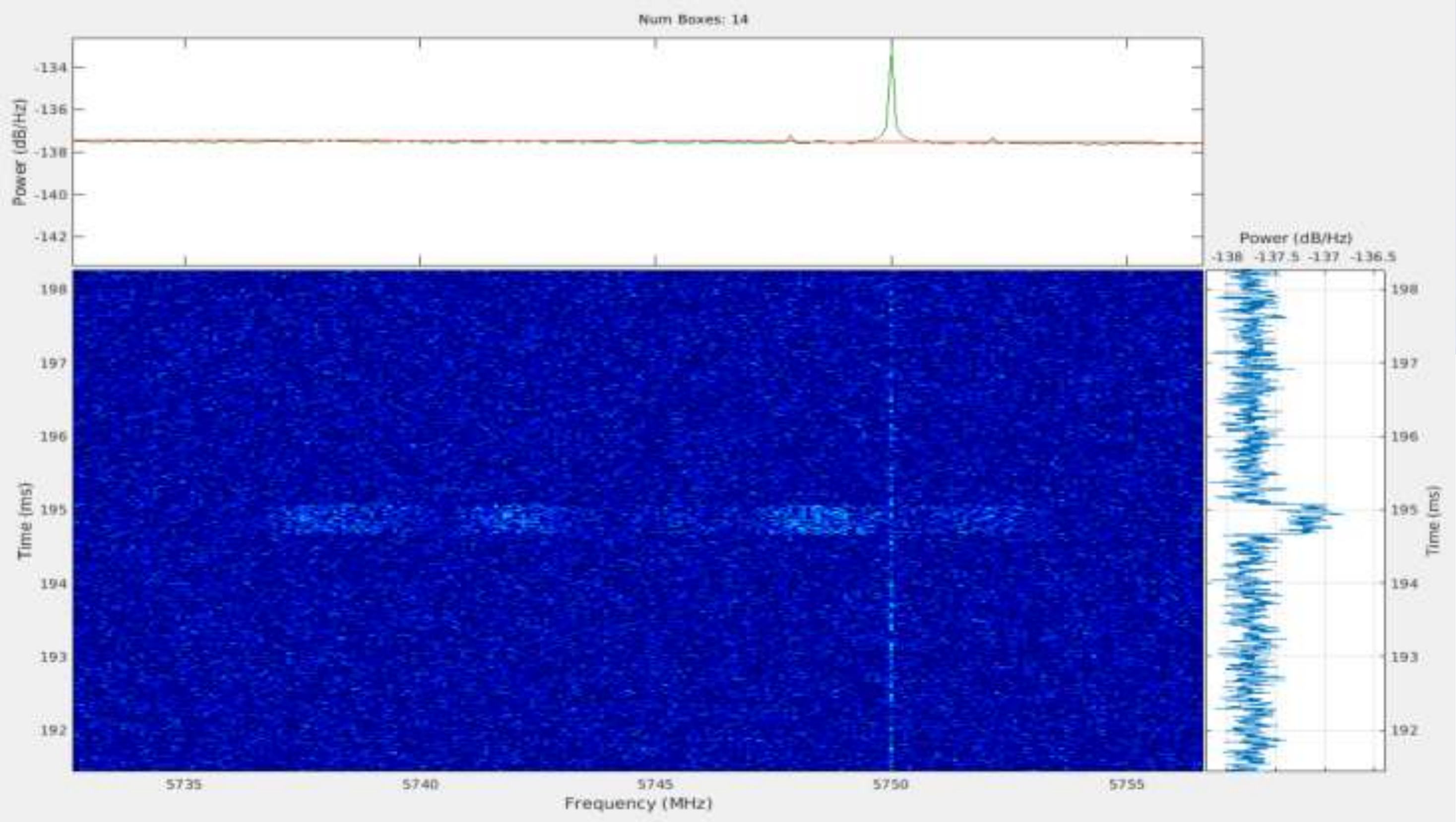
Why is this problem hard?
Spectrum Example – 750 MHz

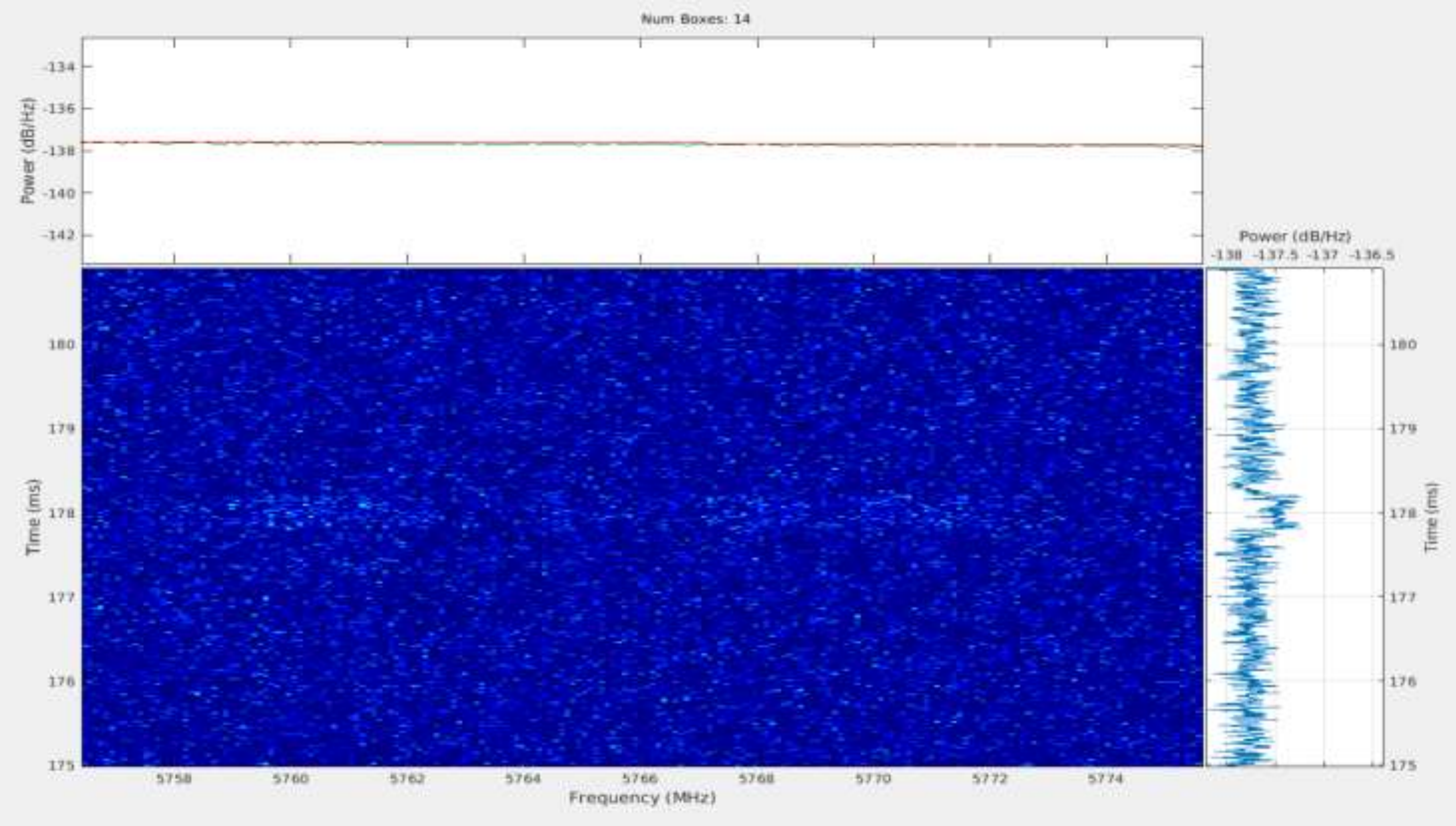


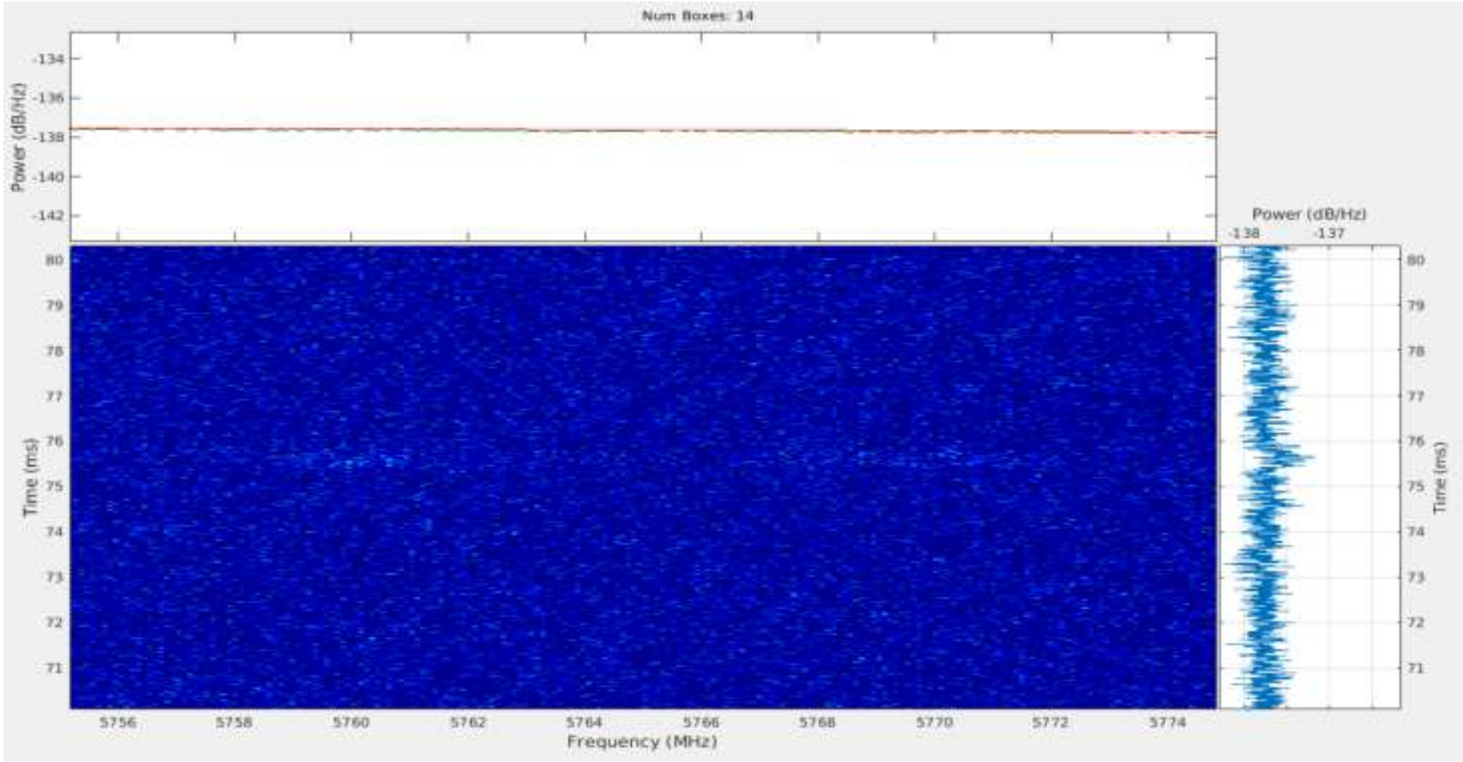


Why is this problem hard?
Spectrum Example – 5.75 GHz



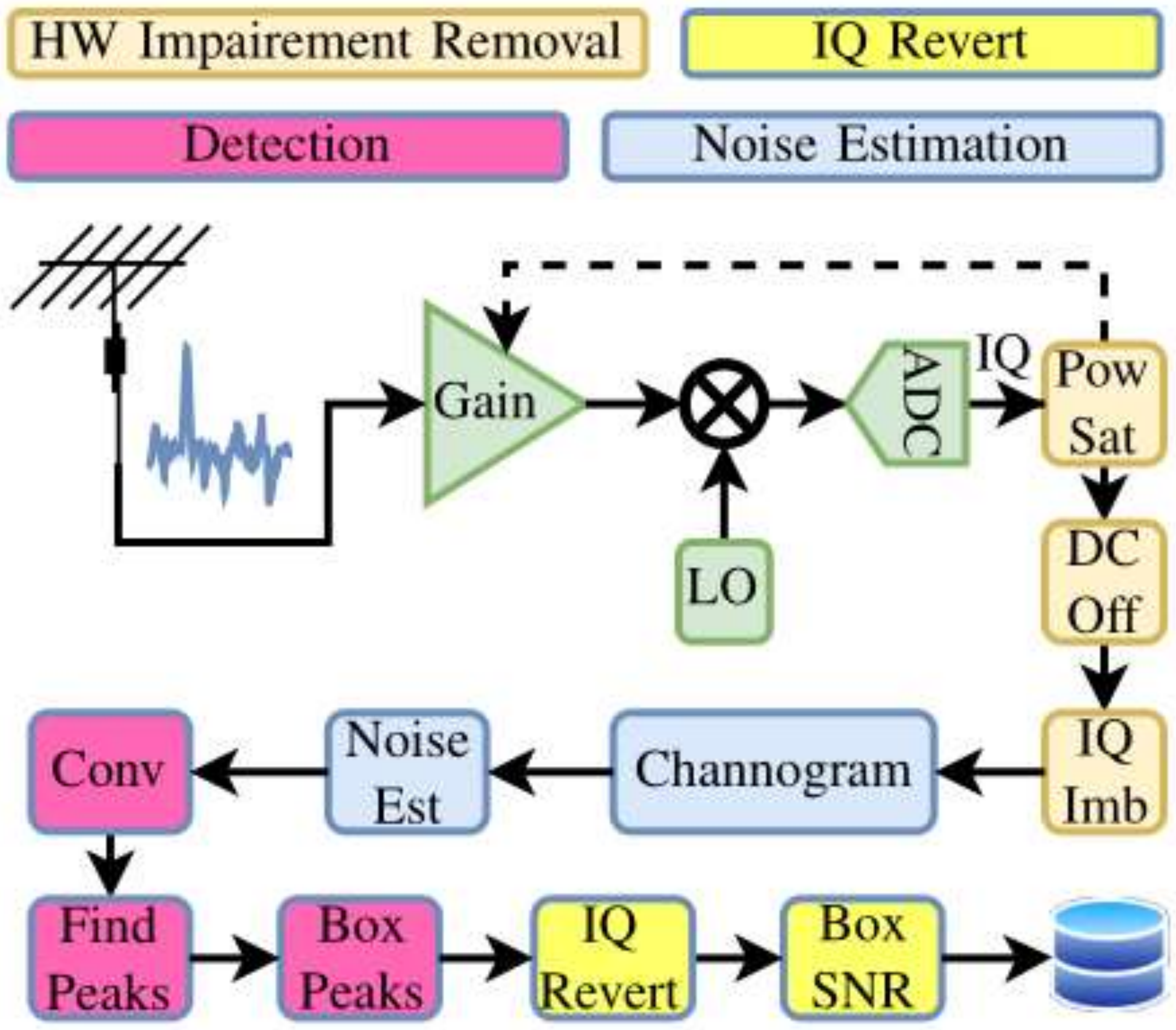






Our solution: Searchlight

- Detect signals as much as -18 dB below noise floor



HW Impairement Removal

IQ Revert

Detection

Noise Estimation

Gain

ADC

IQ

Pow Sat

LO

DC Off

IQ Imb

Channogram

Noise Est

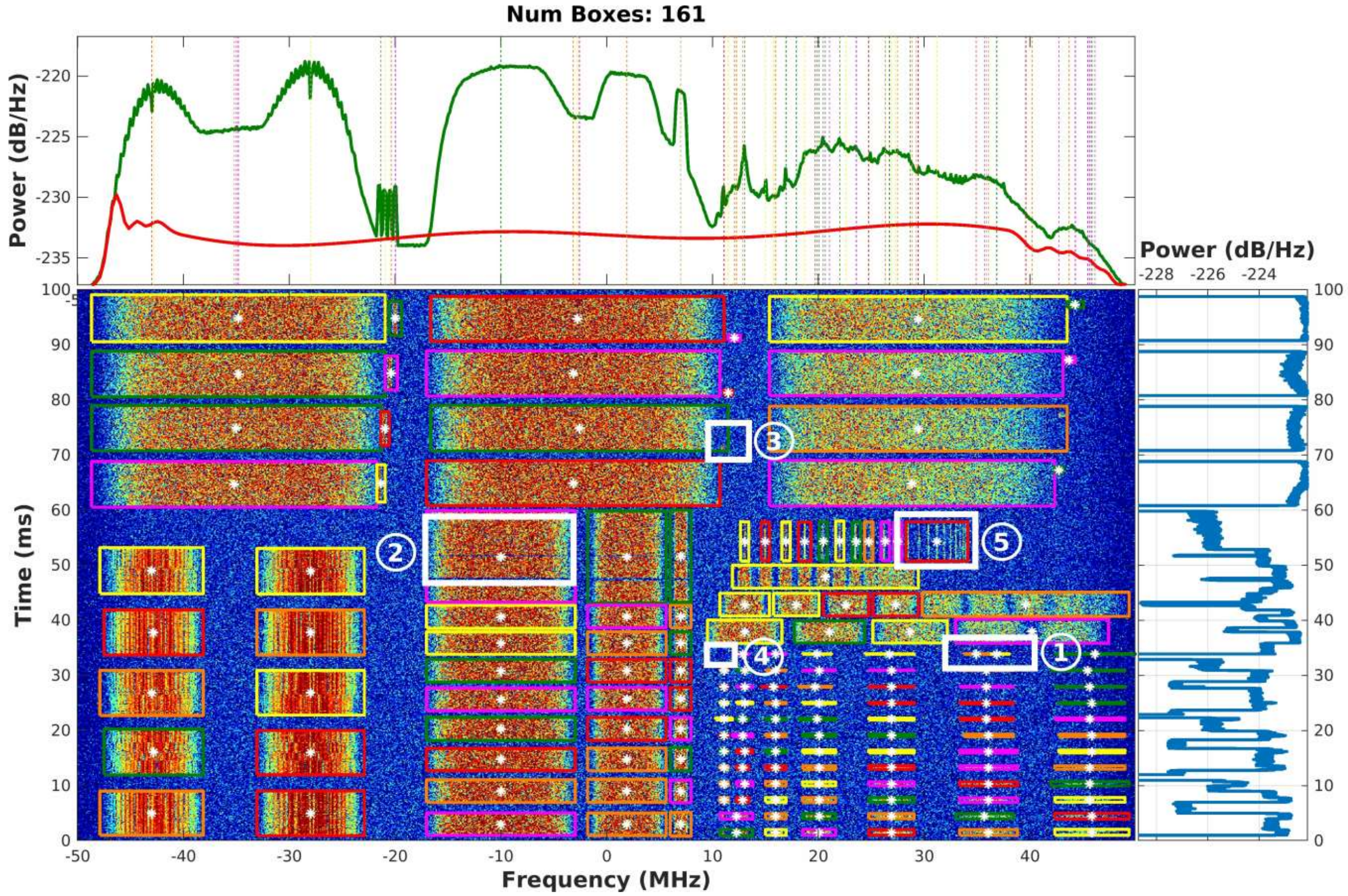
Conv

Find Peaks

Box Peaks

IQ Revert

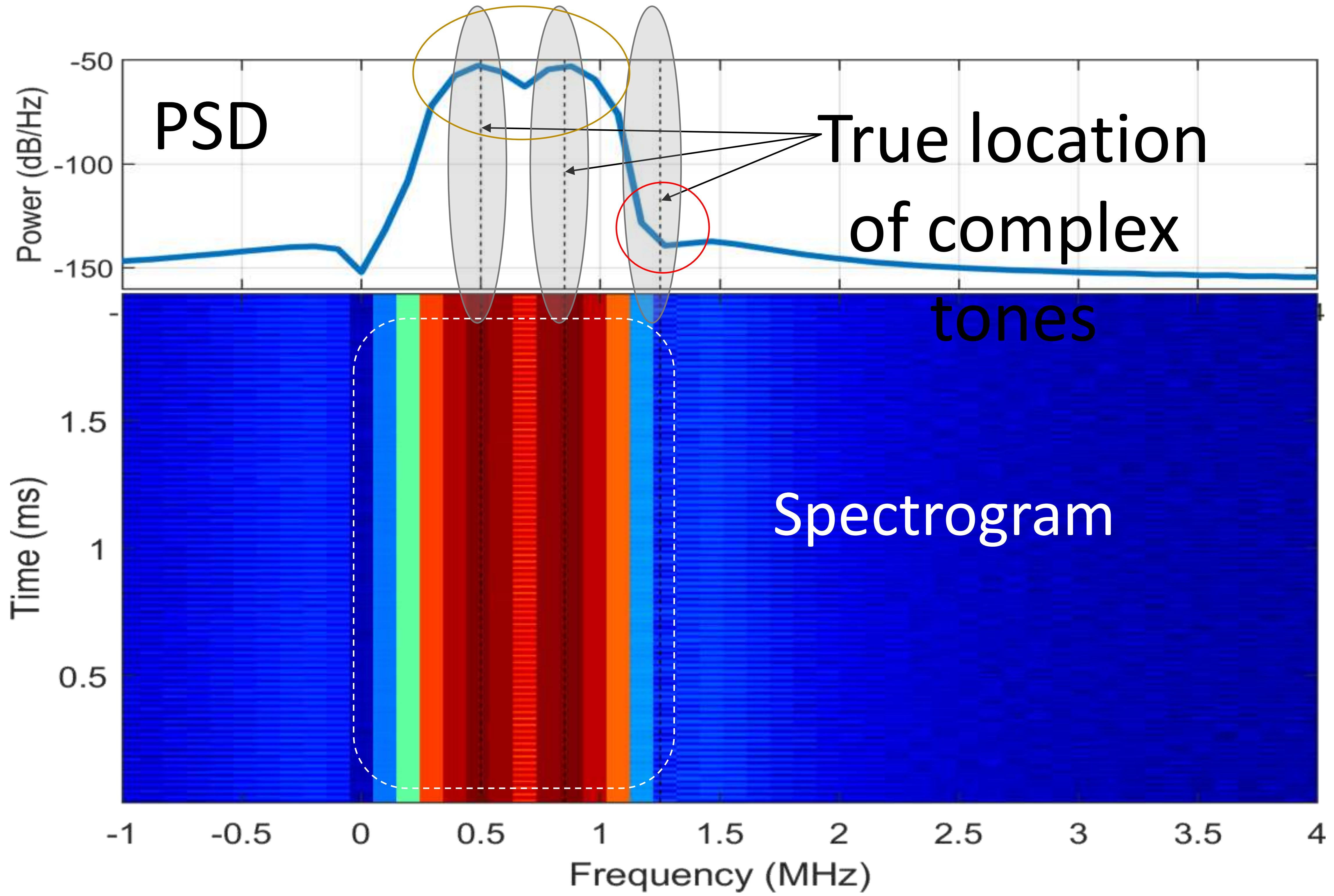
Box SNR



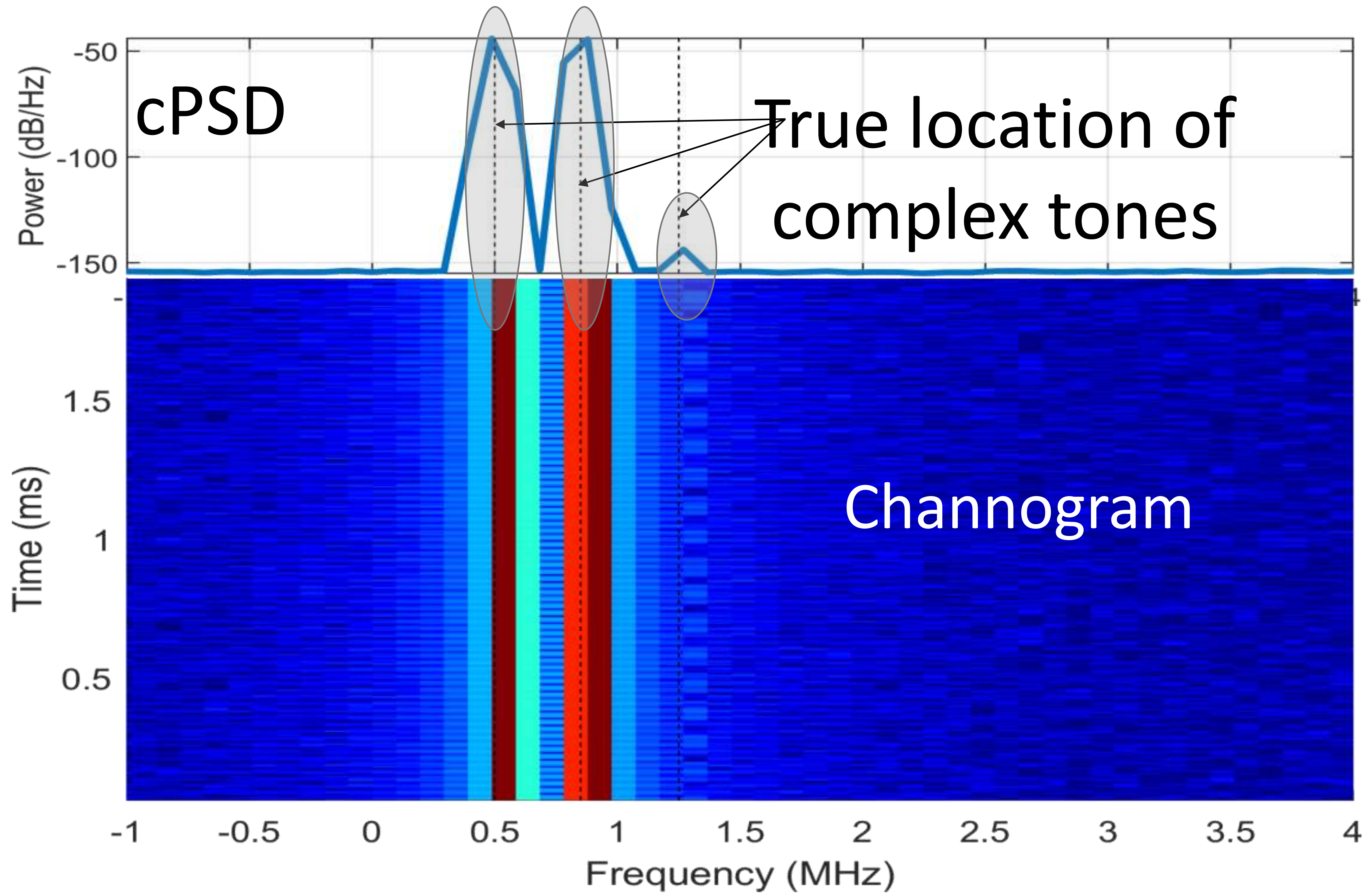
Num Boxes: 161

Searchlight
Super-resolution Channograms

- Three complex tones centered at 0.5 MHz, 0.85 MHz and 1.25 MHz are to be estimated
  - The first two tones are equal power while the third tone has 100 dB less power

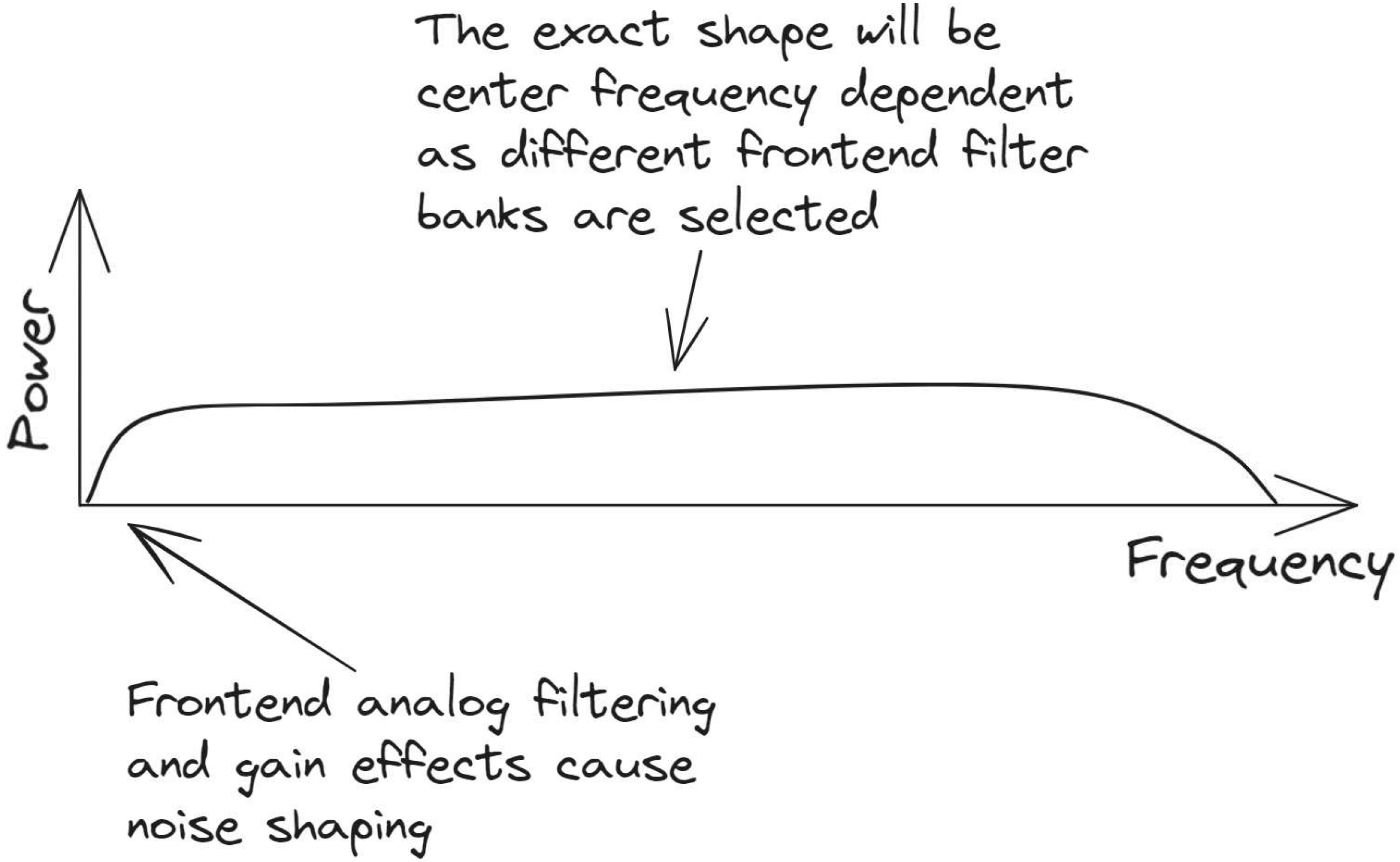


STFT Properties: 1024 Point Kaiser window with beta 10, 50% overlap, 1024 Point FFT



Channelizer Properties: 1024 Channels, 24576 Length Prototype Filter, Beta 5

Searchlight
Non-flat noise floor estimation



The exact shape will be center frequency dependent as different frontend filter banks are selected

Frontend analog filtering and gain effects cause noise shaping

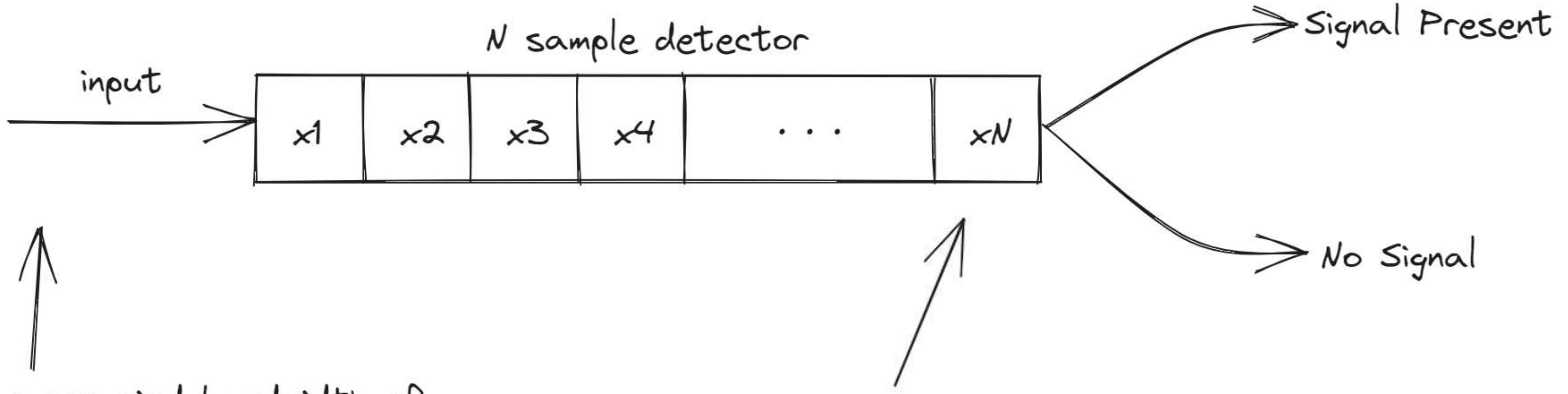
The Classic Detection Problem

Binary hypothesis test

H0 - all samples noise only

H1 - all samples signal plus noise

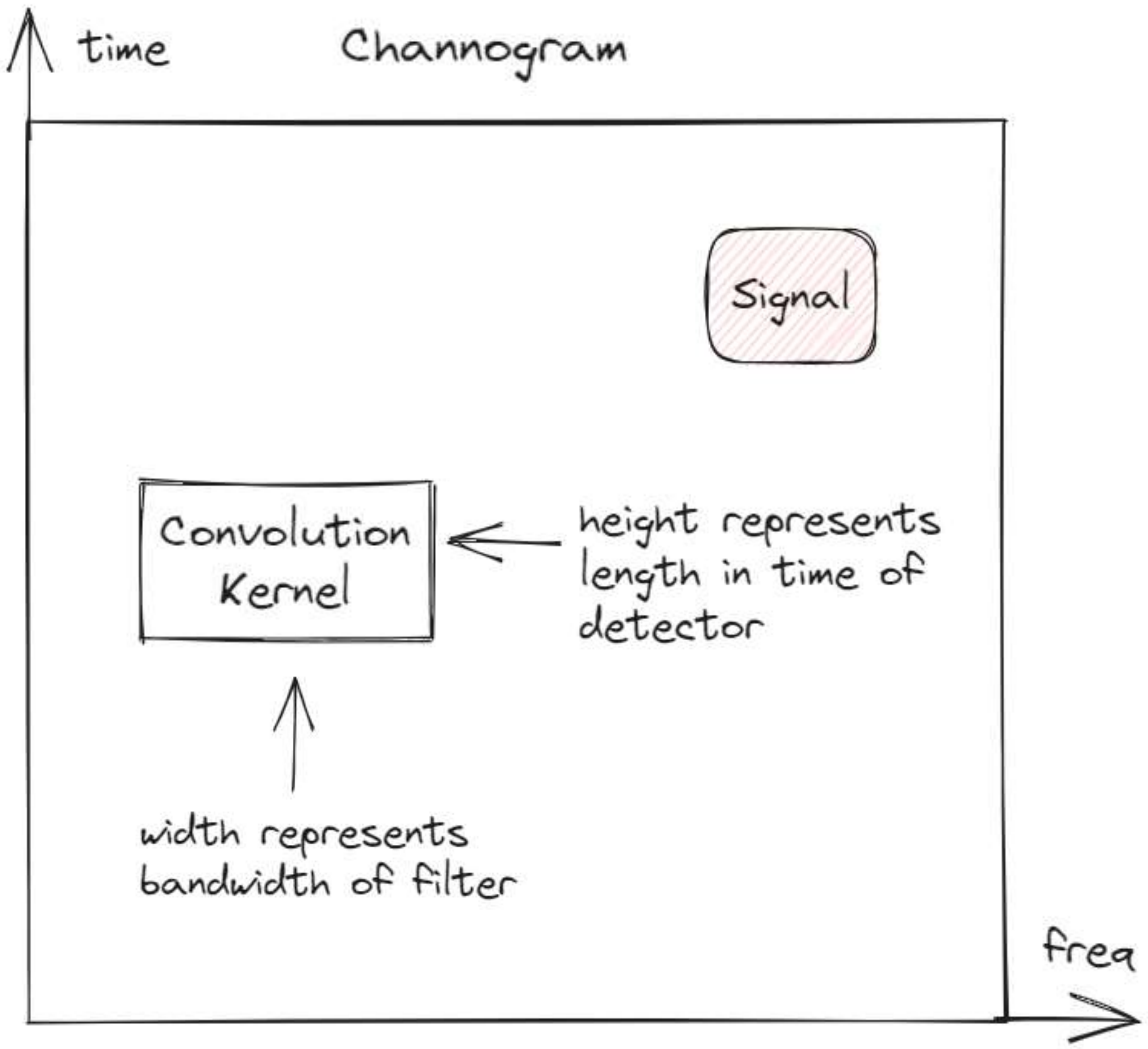
→ Generalized Likelihood Ratio Test (GLRT) → Energy Detector



What if the occupied bandwidth of the input is not equal to the sample rate?

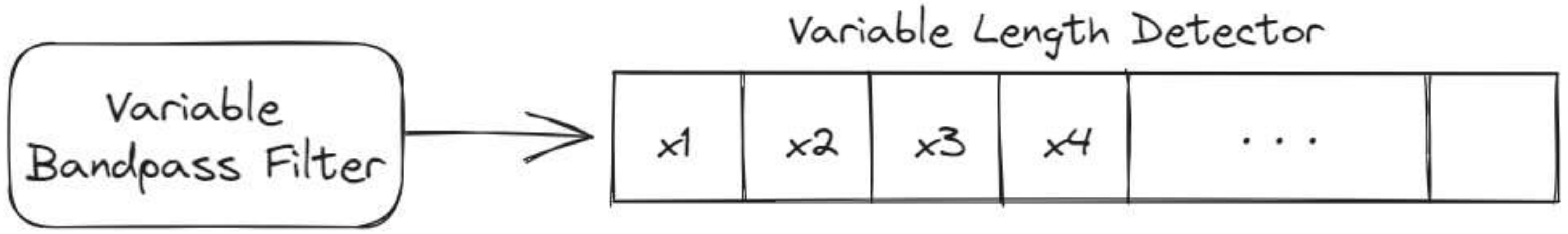
What if the signal length is unknown or variable?

Detection using 2D convolution

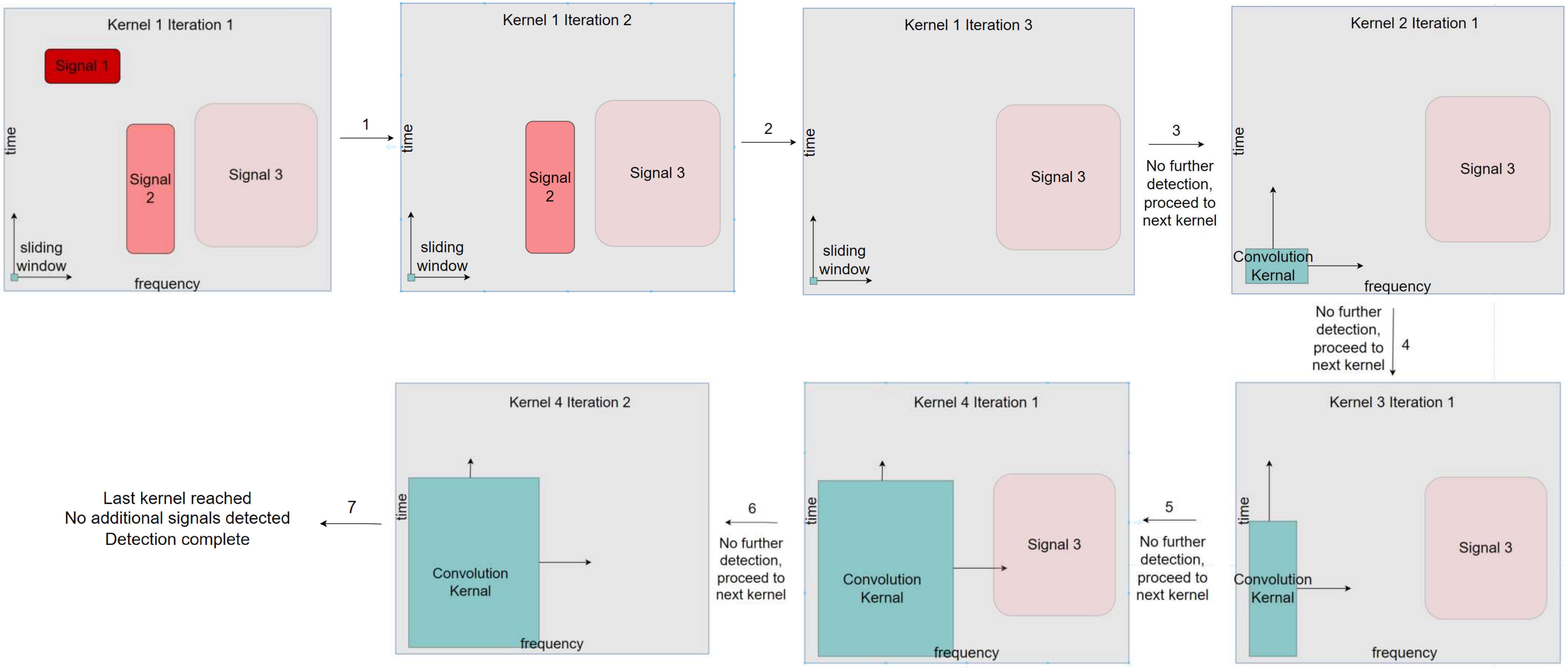

time
Channogram
Signal
Convolution Kernel
height represents length in time of detector
width represents bandwidth of filter
freq

Parseval's Theorem

$$\sum_{n=0}^{N-1} |x_n|^2 = \frac{1}{N} \sum_{k=0}^{N-1} |X_k|^2$$



Searchlight- Iterative detection and cancellation



Kernel 1 Iteration 1

Signal 1

Signal 2

Signal 3

time

sliding window

frequency

1

Kernel 1 Iteration 2

Signal 2

Signal 3

time

sliding window

2

Kernel 1 Iteration 3

Signal 3

time

sliding window

3

No further detection, proceed to next kernel

Kernel 2 Iteration 1

Signal 3

time

Convolution Kernal

frequency

No further detection, proceed to next kernel

4

Kernel 3 Iteration 1

time

Convolution Kernal

Signal 3

frequency

5

No further detection, proceed to next kernel

Kernel 4 Iteration 1

time

Convolution Kernal

Signal 3

frequency

6

No further detection, proceed to next kernel

Kernel 4 Iteration 2

time

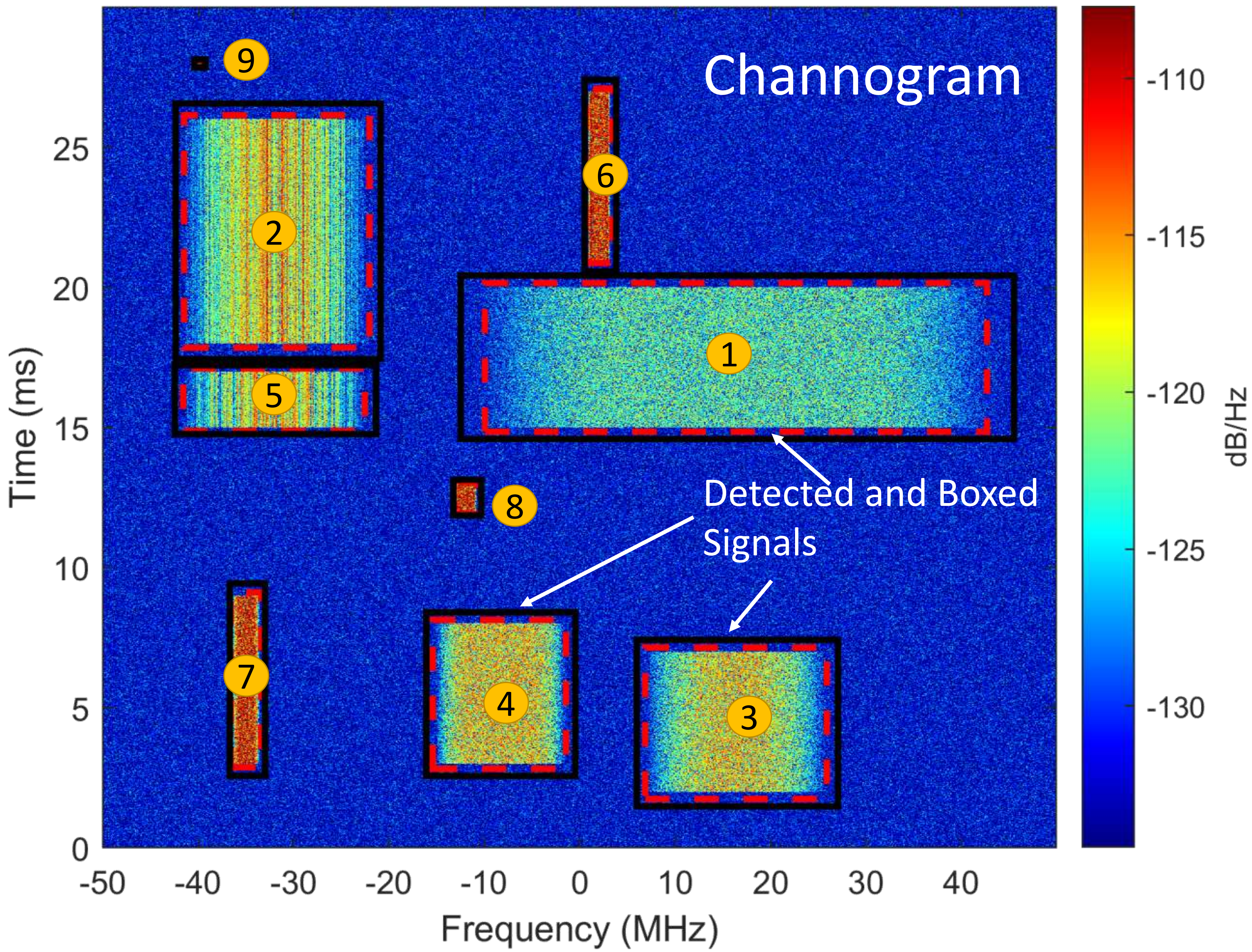
Convolution Kernal

frequency

7

Last kernel reached
No additional signals detected
Detection complete

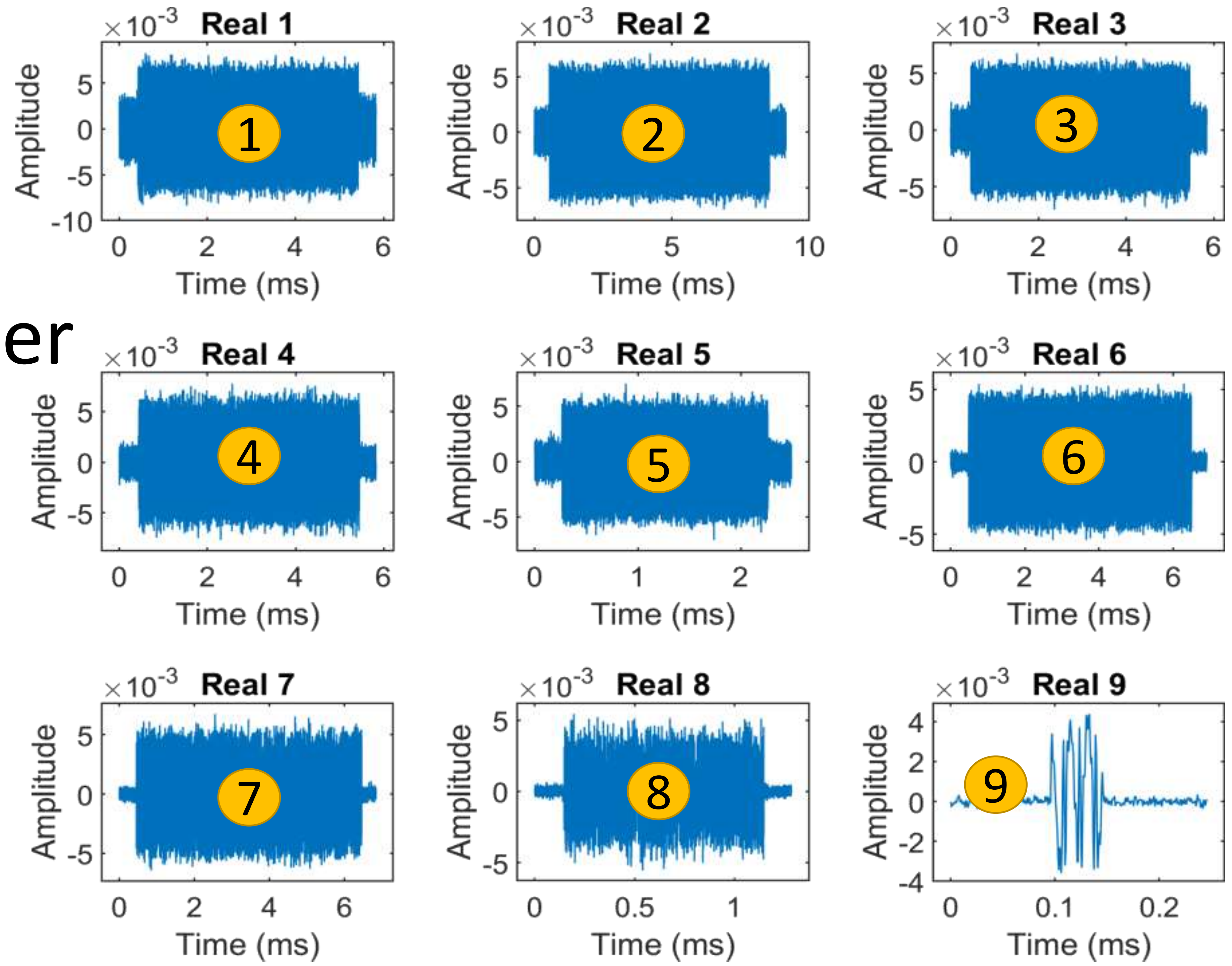
Searchlight - Signal segregation using a synthesis channelizer and the channogram



Channogram

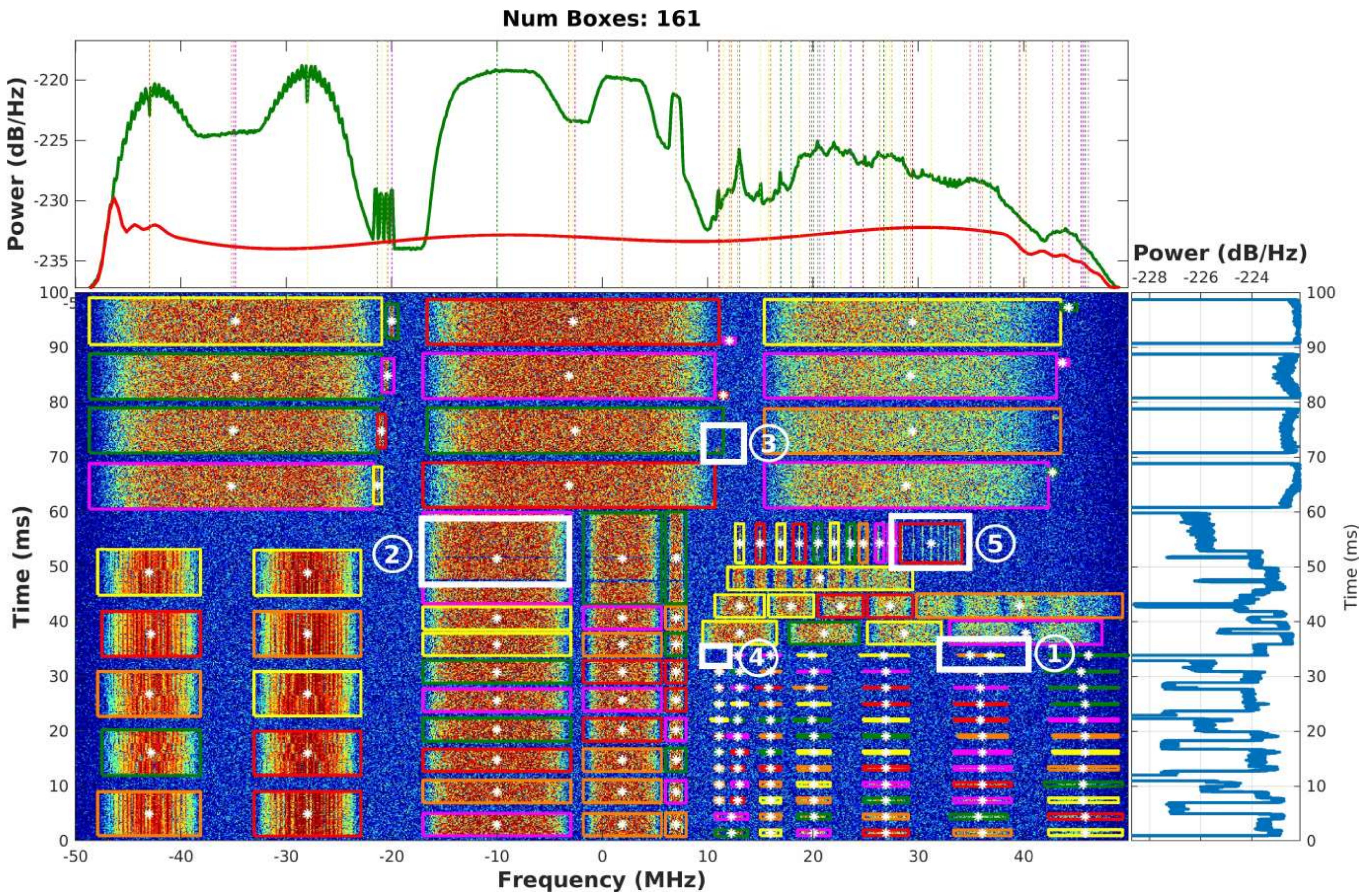
Detected and Boxed Signals

Synthesis Channelizer



Searchlight Performance

- Ground truth is difficult to manage for over-the-air (OTA) testing
  - We developed a tool called OTA Testbed that allows us to maintain ground truth association after transmitting and receiving synthetically generated data over-the-air
- Estimating SNR at the receiver is still a challenge, largely a manual calibration process, prone to error



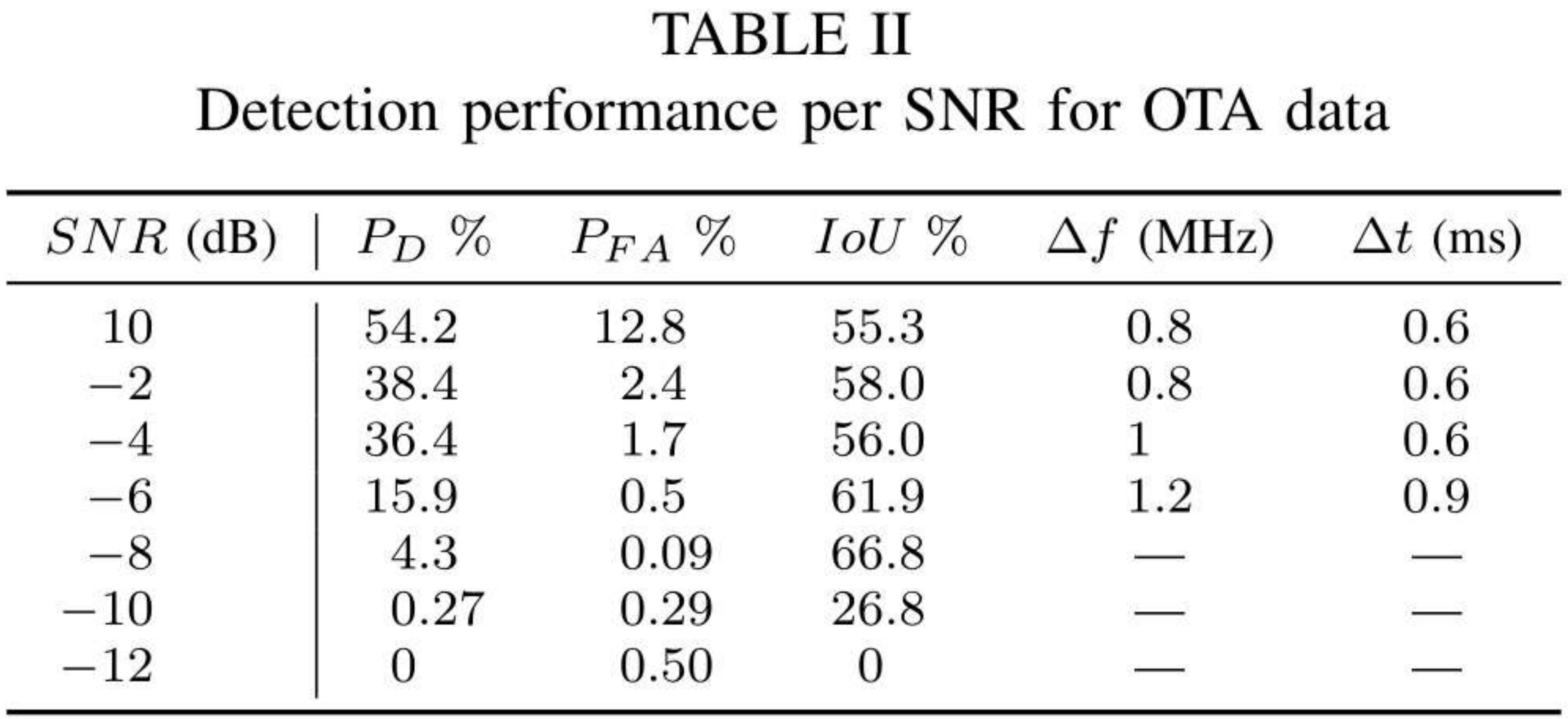


TABLE II
Detection performance per SNR for OTA data

SNR (dB)	P_D %	P_{FA} %	IoU %	Δf (MHz)	Δt (ms)
10	54.2	12.8	55.3	0.8	0.6
−2	38.4	2.4	58.0	0.8	0.6
−4	36.4	1.7	56.0	1	0.6
−6	15.9	0.5	61.9	1.2	0.9
−8	4.3	0.09	66.8	—	—
−10	0.27	0.29	26.8	—	—
−12	0	0.50	0	—	—

Searchlight Processing Speed

- If the average sample processing throughput is less than input sample rate, memory overflows will occur
  - If memory overflow occurs, it is equivalent to turning detection off for the overflowed samples, signals can be missed

- Instantaneous processing throughput can be lower than the input sample rate so long as it is short enough that the system can catch up before overflow occurs

- Searchlight supports an average throughput of 50 Msps when there are on average 6 or fewer signals per block of samples
  - Processing time in regions with hundreds of boxes like 2.4 GHz will get amortized over regions with no boxes, such as large swaths of 3 GHz – 5 GHz

Acknowledgement

IARPA

Home • Research • Office of Collection • SCISRS

SCISRS

SECURING COMPARTMENTED INFORMATION WITH SMART RADIO SYSTEMS

https://www.iarpa.gov/research-programs/scisrs

This research is based upon work supported in part by the Office of the Director of National Intelligence (ODNI), Intelligence Advanced Research Projects Activity (IARPA), via [2021-2106240007]. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of ODNI, IARPA, or the U.S. Government. The U.S. Government is authorized to reproduce and distribute reprints for governmental purposes notwithstanding any copyright annotation therein.

Searchlight

- Points of contact
  - Richard Bell: rcbell@ucsd.edu
  - Dinesh Bharadia: dineshb@ucsd.edu
  - fred harris: fjharris@ucsd.edu

- Questions and collaborations welcomed

- Thank you