GNURADIO CONFERENCE 2016

MATT KNIGHT // BASTILLE NETWORKS

GR-LORA

INTRODUCTION

- Matt Knight
- Software Engineer and Threat Researcher @ Bastille
- BE & BA from Dartmouth
- Background in electrical engineering, embedded software, etc.

matt@Bastille.net
@embeddedsec

AGENDA

1. Introduce LPWANs
2. Discuss the LoRa PHY, as informed via SDR
3. Introduce gr-lora

WHAT'S LORA?

WIRELESS IOT PROTOCOL

IOT == EMBEDDED

802.15.4

(ZIGBEE)

802.11

BLUETOOTH

BLE

AND [. . .]

WHAT'S WRONG WITH [YOUR FAVORITE PROTOCOL]?

- Require local provisioning
- Some require gateways to connect out
- [802.11] Thirsty battery requirements
- What's ideal then?

HOW ABOUT CELLULAR?

1. IT WORKS EVERYWHERE
2. EASY TO INSTALL

IT'S THIRSTY

AND IT'S GOING AWAY*

*2G, THAT IS

DEPRECATION: A DEVELOPER'S CONUNDRUM

- AT&T to sunset 2G on January 1, 2017
- Other major carriers to follow

- 2G advantages: ubiquitous, battery-conscious, somewhat inexpensive
  - Exactly what IoT devices require

REPLACING 2G

- 3G
  - More expensive
  - Harder power requirements
- LTE-M/NB-LTE Release 13
  - IoT focused cellular protocols
  - Not ready by the sunset date, which means…

VOID IN MARKET

INTRODUCING

LORA

http://www.gsm-modem.de/M2M/wp-content/uploads/2015/10/LWPAN-versus-LTE.png

HISTORY

- LPWAN developed by Semtech
- PHY patented in June 2014
- LoRaWAN MAC/NWK stack released in January 2015
- Supported by LoRa Alliance

http://actility.thingpark.com/thingpark-store/87-thickbox_leoelec/thingpark-cloud-application-partner-kit-lora-sensors.jpg

LPWAN

- LPWAN: Low Power Wide Area Network
- Like cellular, but optimized for IoT/M2M
- Network of basestations worldwide
- Star network to endpoints, UL/DL traffic
- Range in miles

EMERGING STANDARDS

SIGFOX
One network A billion dreams

nwave

LoRa™

LTE-M

NB-LTE

INGENU

WEIGHTLESS

IEEE 802.11ah

DASH7™ ALLIANCE

EC-GSM

ZigBee3.0

Bluetooth® 4.0

http://www.itwissen.info/bilder/lpwan-konzepte-fuer-das-internet-of-things-iot.png

AGGRESSIVE INVESTMENT

- SIGFOX raised 115MM last year
  - WSJ: Possible US IPO soon
- Senet and Actility, LoRa backers, raised a combined 51MM
- LoRa alliance membership tripled last year

http://img.scoop.it/pkne9jh9_fl-PFplrbFgL4XXXL4j3HpexhjNOf_P3YmryPKwJ94QGRtDb3Sbc6KY
https://pbs.twimg.com/profile_images/615790171116601345/Q1PU_OuW.png

NETWORKS OPTIMIZED FOR IOT

- Battery-conscious
  - SIGFOX advertises 10 years on 1 AA battery
- Long range
  - LoRa advertises up to 13.6 miles

HOW!?

- Compare this with…
  - 2G: typically 1-2 miles, max 22 miles, a few days
  - 802.15.4: 10-100 meters, months-years
  - WiFi: 30 meters, a few days

COMPROMISES

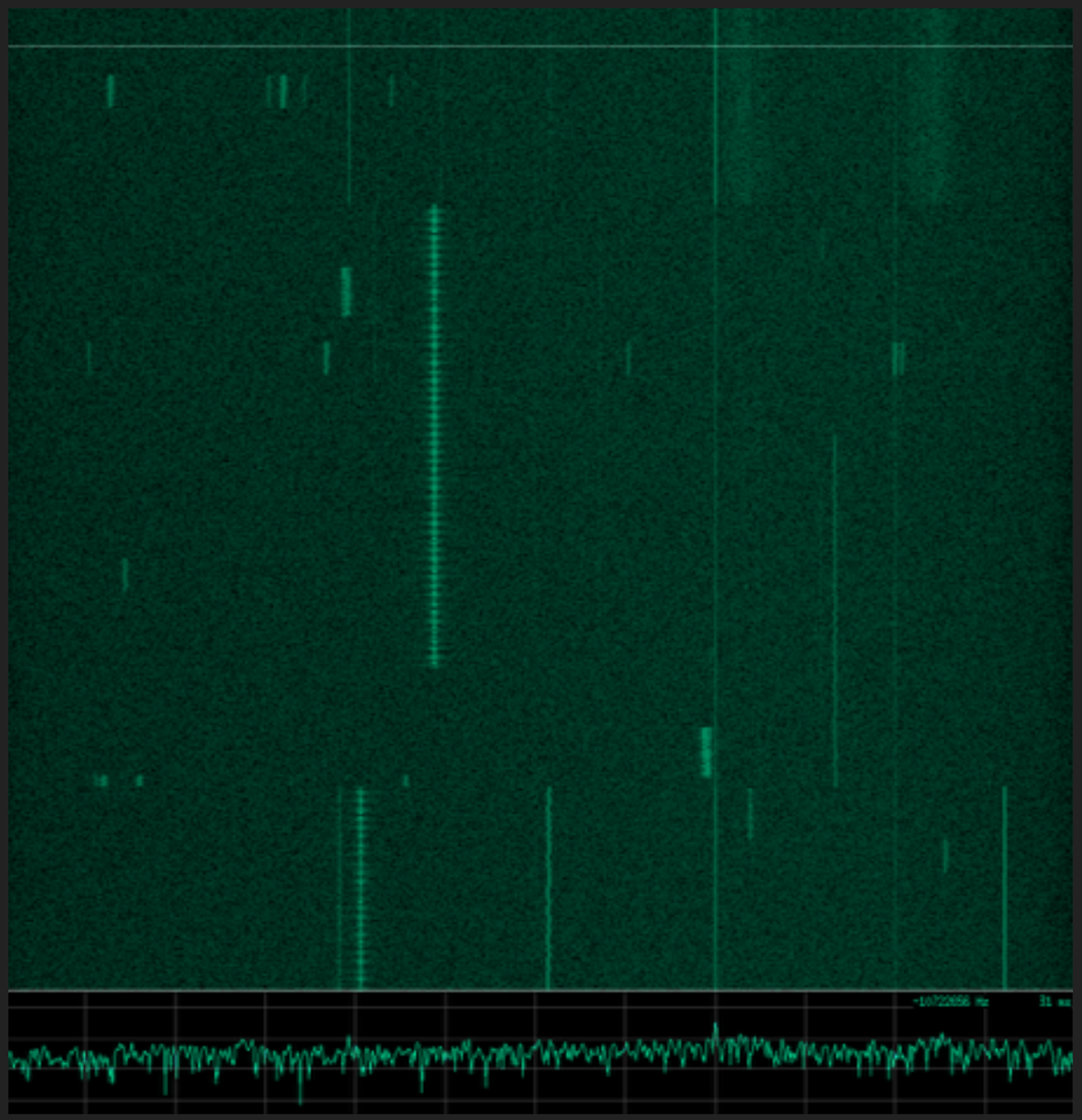
EMBRACING COMPROMISE

- Conservative duty-cycling and listening
- Very sparse datagrams
- Highly rate-limited

EMBRACING COMPROMISE

- Examples
  - SIGFOX limits devices to 140 12-byte datagrams per day
  - Weightless-N is uplink-only
  - LoRa Class A devices can only receive downlink momentarily after uplinking

LICENSURE, OR LACK THEREOF



- LoRa uses 900 MHz ISM
  - US: 902-928 MHz
  - EU: 868 MHz
- No special license required

LICENSURE, OR LACK THEREOF

DMA[1]	Call Sign	Move Off-Air	Move to Low VHF	Move to High VHF
New York, NY	WABC-TV	[illegible]	351,539,055	NA
New York, NY	WCBS-TV	900,000,000	675,000,000	360,000,000
New York, NY	WDVB-CD	[illegible]	318,579,075	169,908,840
New York, NY	WEBR-CD	376,508,700	282,381,525	150,603,480
New York, NY	WEDW	448,103,700	336,077,775	179,241,480
New York, NY	WEPT-CD	129,438,900	97,079,175	51,775,560
New York, NY	WFTY-DT	438,170,400	328,627,800	175,268,160
New York, NY	WFUT-DT	788,135,400	591,101,550	315,254,160
New York, NY	WJLP	206,954,325	NA	NA
New York, NY	WLIW	672,446,700	504,335,025	268,978,680
New York, NY	WLNY-TV	483,707,700	362,780,775	193,483,080
New York, NY	WMBC-TV	805,447,800	604,085,850	322,179,120
New York, NY	WMBQ-CD	445,109,400	333,832,050	178,043,760
New York, NY	WMUN-CD	364,589,100	273,441,825	145,835,640
New York, NY	WNBC	869,160,600	651,870,450	347,664,240
New York, NY	WNET	443,269,260	258,573,735	NA
New York, NY	WNJB	475,608,780	277,438,455	NA
New York, NY	WNJN	775,742,400	581,806,800	310,296,960
New York, NY	WNJU	819,342,000	614,506,500	327,736,800
New York, NY	WNYE-TV	770,259,600	577,694,700	308,103,840
New York, NY	WNYJ-TV	625,505,400	469,129,050	250,202,160
New York, NY	WNYW	824,922,000	618,691,500	329,968,800
New York, NY	WPIX	435,535,920	254,062,620	NA
New York, NY	WPXN-TV	745,848,900	559,386,675	298,339,560
New York, NY	WRNN-TV	846,911,700	635,183,775	338,764,680
New York, NY	WTBY-TV	683,951,400	512,963,550	273,580,560
New York, NY	WVVH-CD	31,156,200	23,367,150	12,462,480
New York, NY	WWOR-TV	810,039,600	607,529,700	324,015,840
New York, NY	WXTV-DT	832,842,000	624,631,500	333,136,800
New York, NY	WZME	483,669,000	362,751,750	193,467,600
Los Angeles, CA	KABC-TV	305,469,360	178,190,460	NA
Los Angeles, CA	KAZA-TV	557,458,200	418,093,650	222,983,280
Los Angeles, CA	KBEH	617,519,700	463,139,775	247,007,880
Los Angeles, CA	KCAL-TV	299,840,400	174,906,900	NA
Los Angeles, CA	KCBS-TV	544,991,400	408,743,550	217,996,560
Los Angeles, CA	KCET	492,480,900	369,360,675	196,992,360
Los Angeles, CA	KCOP-TV	333,967,860	194,814,585	NA
Los Angeles, CA	KDOC-TV	539,584,200	404,688,150	215,833,680
Los Angeles, CA	KFTR-DT	573,801,300	430,350,975	229,520,520
Los Angeles, CA	KHTV-CD	457,959,600	343,469,700	183,183,840

- Compare this with cellular
  - FCC auctions cellular spectrum licenses for billions
  - Restricts building infrastructure to biggest telcos
- Left: opening bid list for FCC TV whitespace reverse auction

LORAWAN NETWORK PROVIDERS

- Senet
  - Commercial network
- The Things Network
  - Crowdsourced

- No licensed spectrum required…!!

http://img.scoop.it/pkne9jh9_fl-PFplrbFgL4XXXL4j3HpexhjNOf_P3YmryPKwJ94QGRtDb3Sbc6KY
http://thenextweb.com/insider/2015/08/19/the-things-network-wants-to-make-every-city-smart-starting-with-amsterdam/#gref

RADICALLY DIFFERENT

TECHNICAL DETAILS

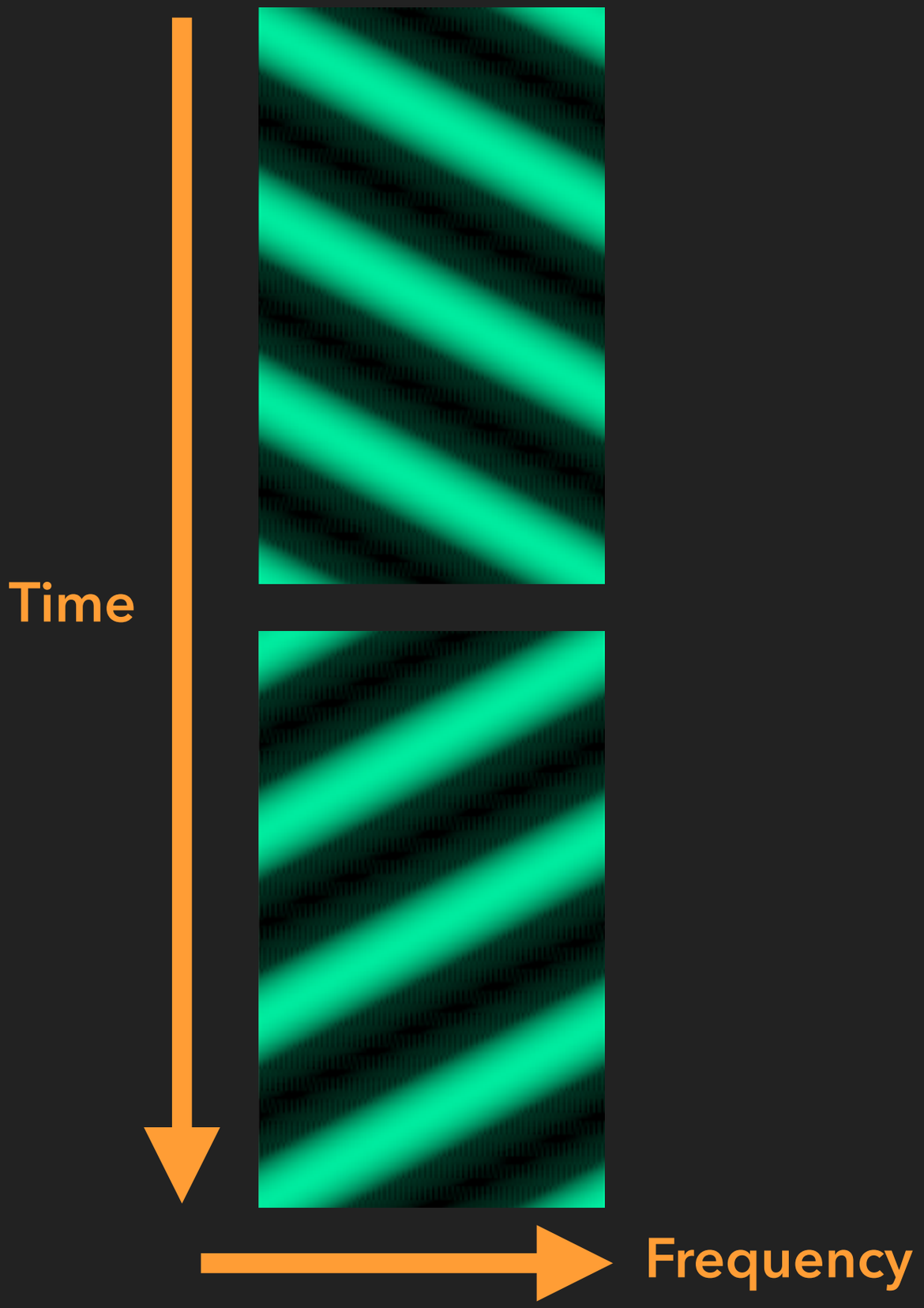
LORA

LORA'S PROPRIETARY PHY

- Modulation: Chirp Spread Spectrum (CSS)
- What's a chirp?
  - A signal of continuously increasing or decreasing frequency
  - i.e. a "sweeped tone"

CSS CHIRPS

- **Upchirp** (top)
  - Increasing frequency
- **Downchirp** (bottom)
  - Decreasing frequency



CSS ADVANTAGES

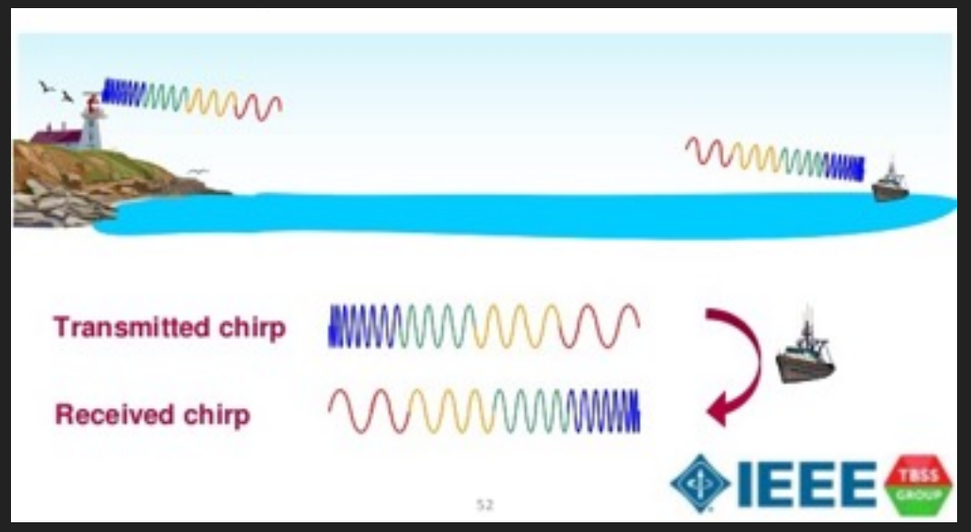
- Great link budget
  - Resilience to interference
  - Performance at low power
- Resistance to multi-path effects
- Resistance to Doppler effect (mobile applications)

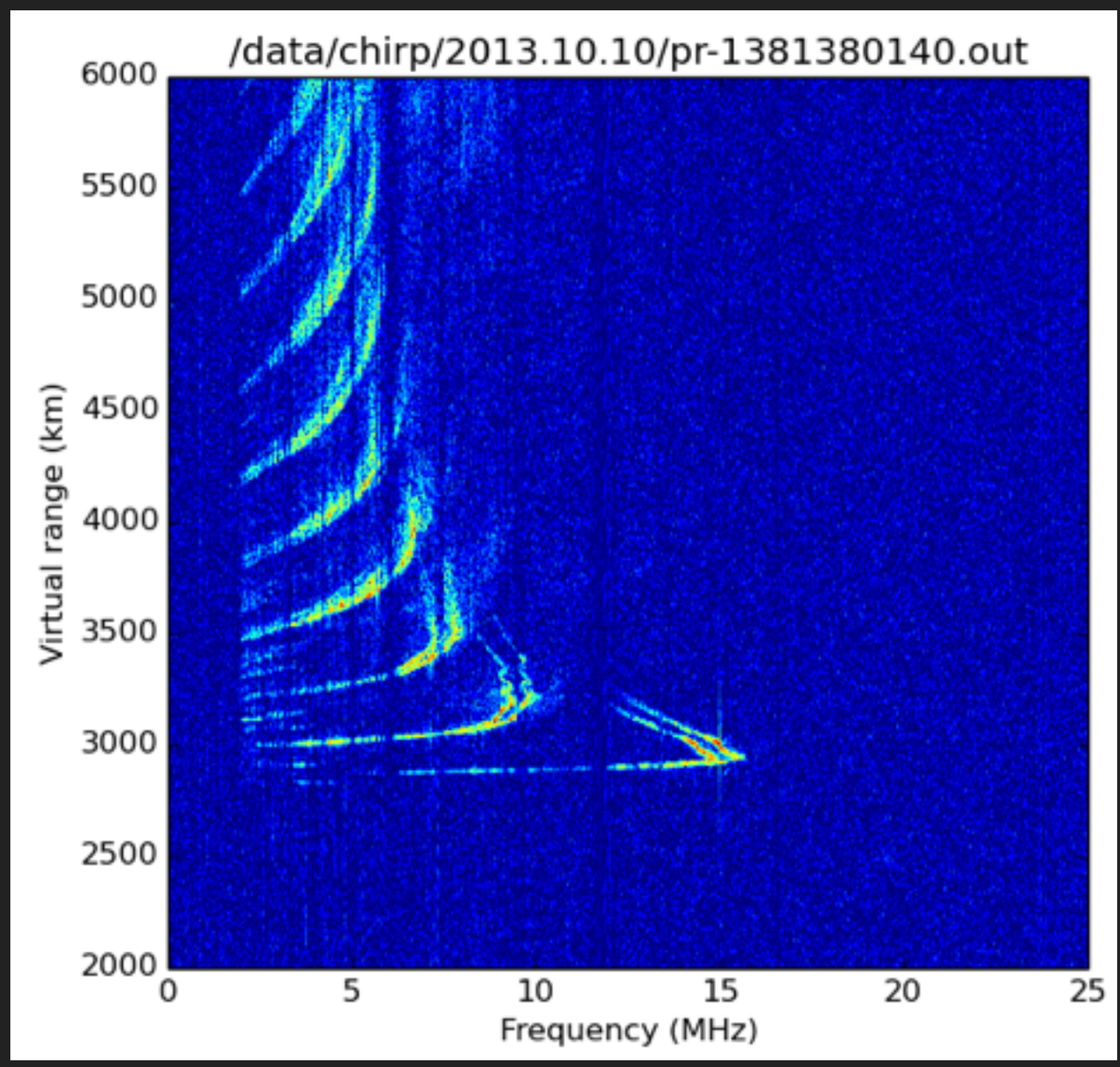
- Interesting set of pros… where else are chirps used?

RADAR

CHIRPS IN RADAR

- Various military and marine radars
  - Wideband and pulse compression
- Open source GNU Chirp Sounder
  - Ionospheric radars
  - Space weather





LORA STANDARD

- LoRa PHY is proprietary – the standard has not been published
- Still, LoRa looks awesome…
- What is one to do?

DECODING LORA

- Presented at:

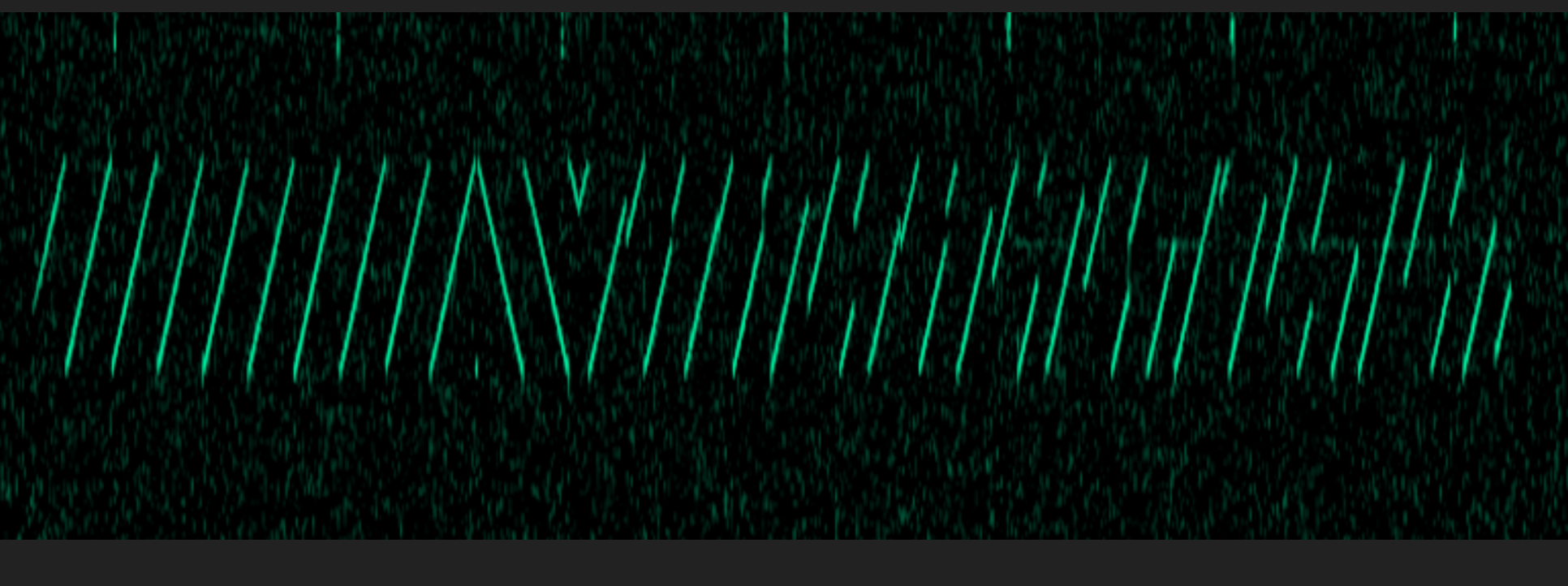
JAILBREAK BREWING COMPANY

SECURITY SUMMIT

- Slides: github.com/matt-knight/research
- Technical papers: GRCon16 Proceedings and PoC||GTFO

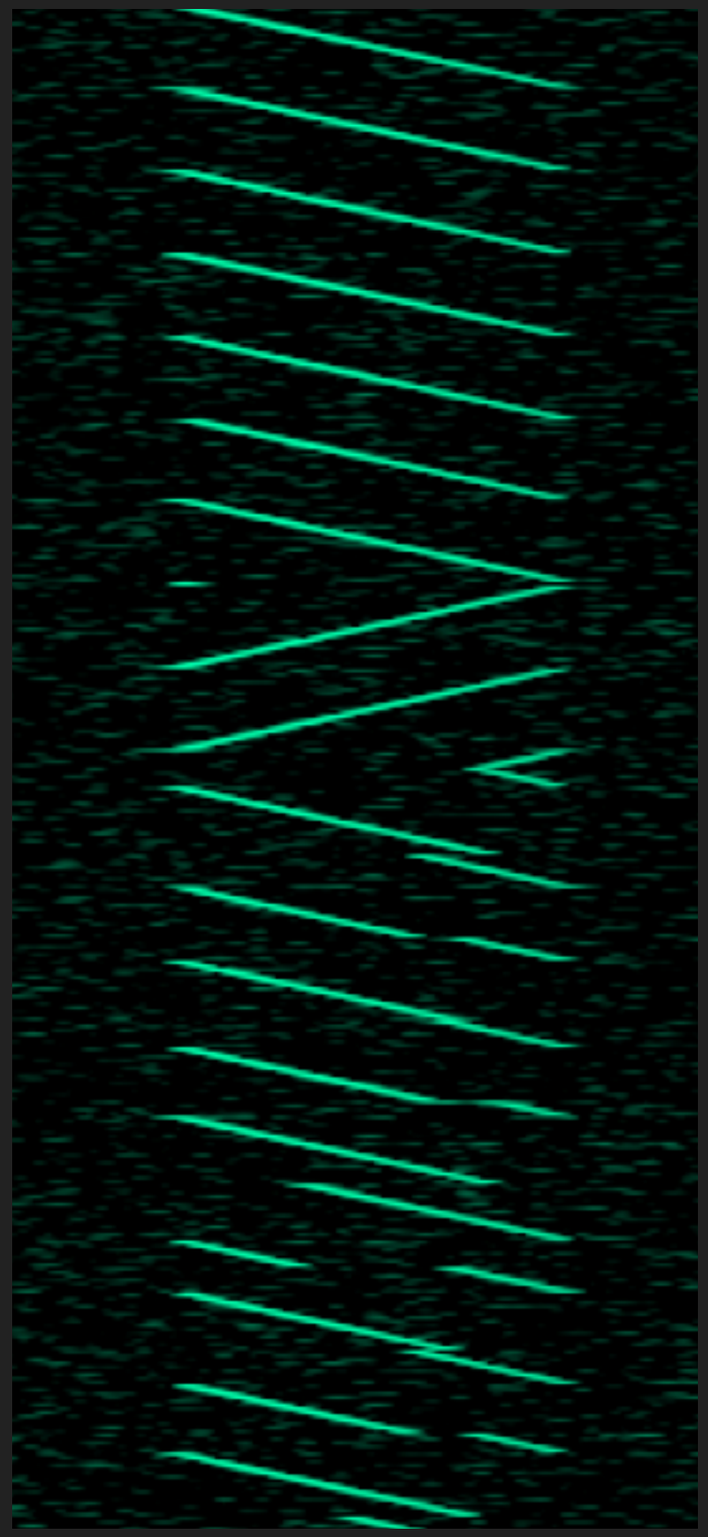
TOOLS USED

- Transmitter: Microchip LoRa RN2903 Module
  - Contains hardware-defined Semtech LoRa radio
- Receiver: Ettus B210
  - Software-defined radio
  - Python, GNURadio, and Baudline to process



EXAMINING THE LORA PHY FRAME

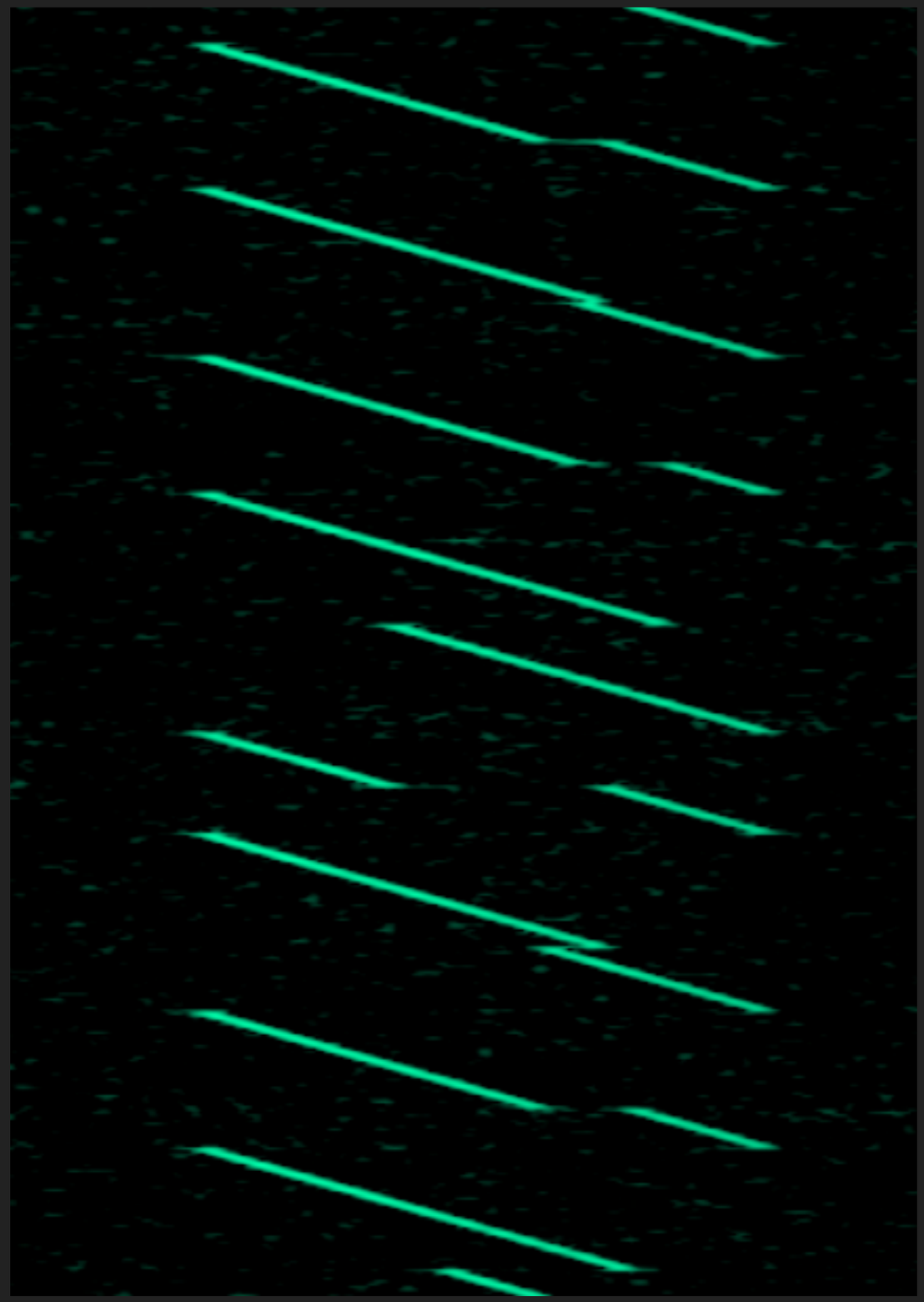
- Repeated upchirps
  - Preamble/Training Sequence
- Two downchirps
  - Start of frame delimiter (SFD)
- Choppy upchirps of varying length
  - Data!



PHY DATA UNIT STRUCTURE

- Chirp rate is static
- Chirp “jumps” throughout band

- Instantaneous frequency changes are result of data being modulated onto the chirps
  - Frequency modulated chirps



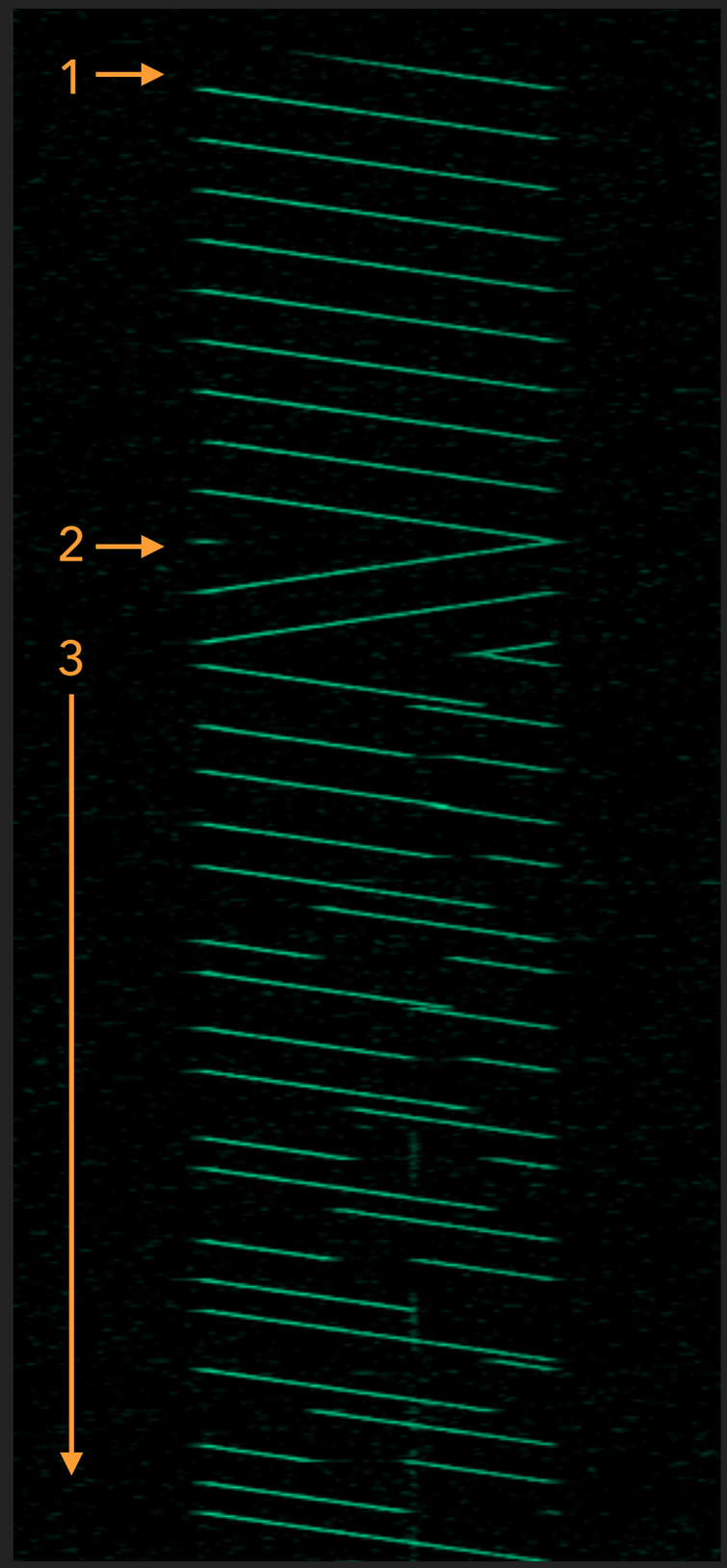
DEMODULATING

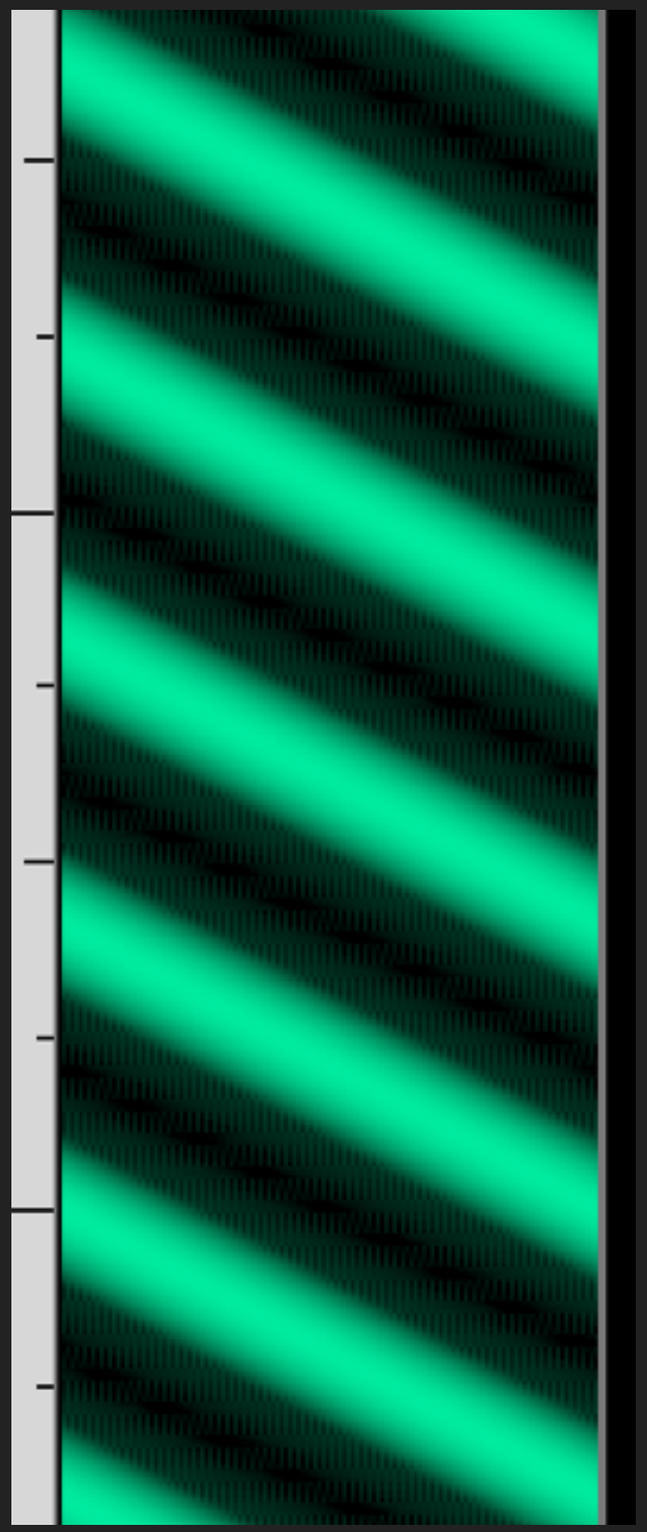
LORA

DEMODULATING THE PHY

1. Identify the beginning of a frame
2. Find the beginning of the PHY data unit
3. Extract data from instantaneous frequency transitions

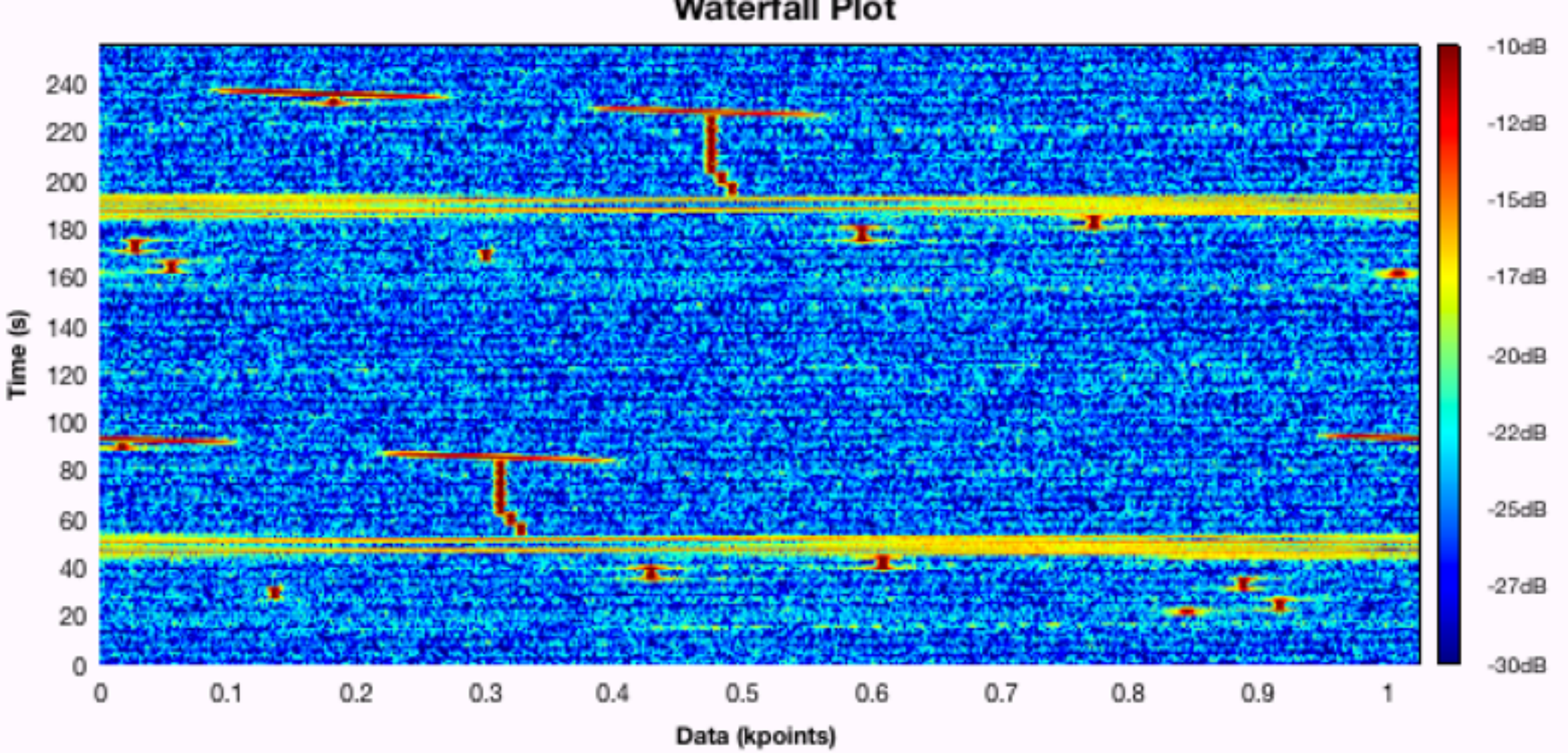
- How? We need to quantify the frequency transitions





TRANSFORMING THE SIGNAL

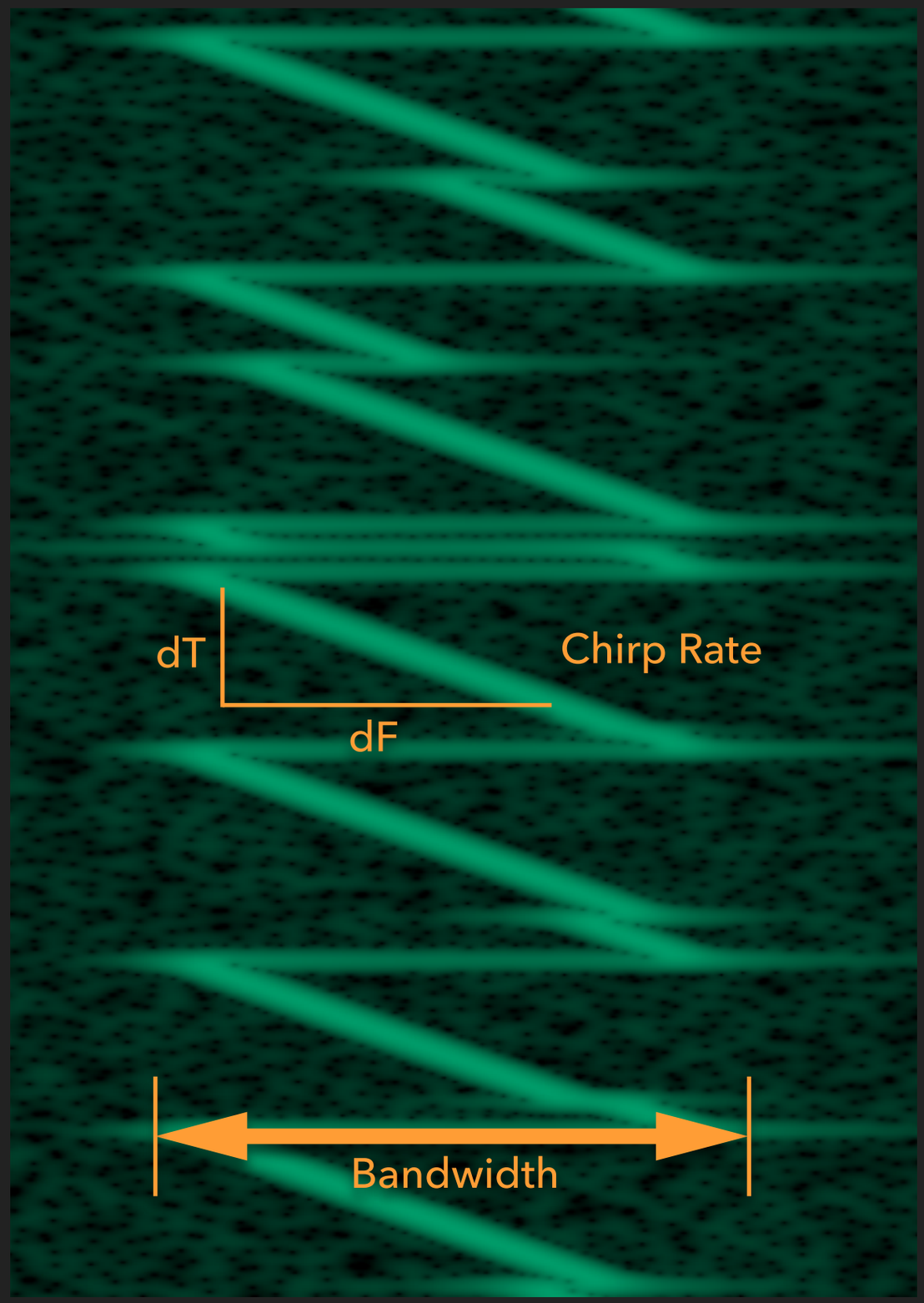
- De-chirping the signal makes analysis easier
- Generate local upchirp and downchirp at the appropriate chirp rate
- Multiply each against the signal and something interesting happens...



Waterfall Plot
Time (s)
240
220
200
180
160
140
120
100
80
60
40
20
0
0
0.1
0.2
0.3
0.4
0.5
0.6
0.7
0.8
0.9
1
-10dB
-12dB
-15dB
-17dB
-20dB
-22dB
-25dB
-27dB
-30dB
Options
Axes Options
Dyn Range:
+
-
Ref Level:
+
-
Color:
RGB2
Autoscale
Clear

SOME DEFINITIONS...

- Bandwidth: width of spectrum occupied by chirp
- Spreading factor: number of bits encoded per symbol (RF state, remember?)
- Chirp rate: first derivative of chirp frequency



SOME DEFINITIONS…

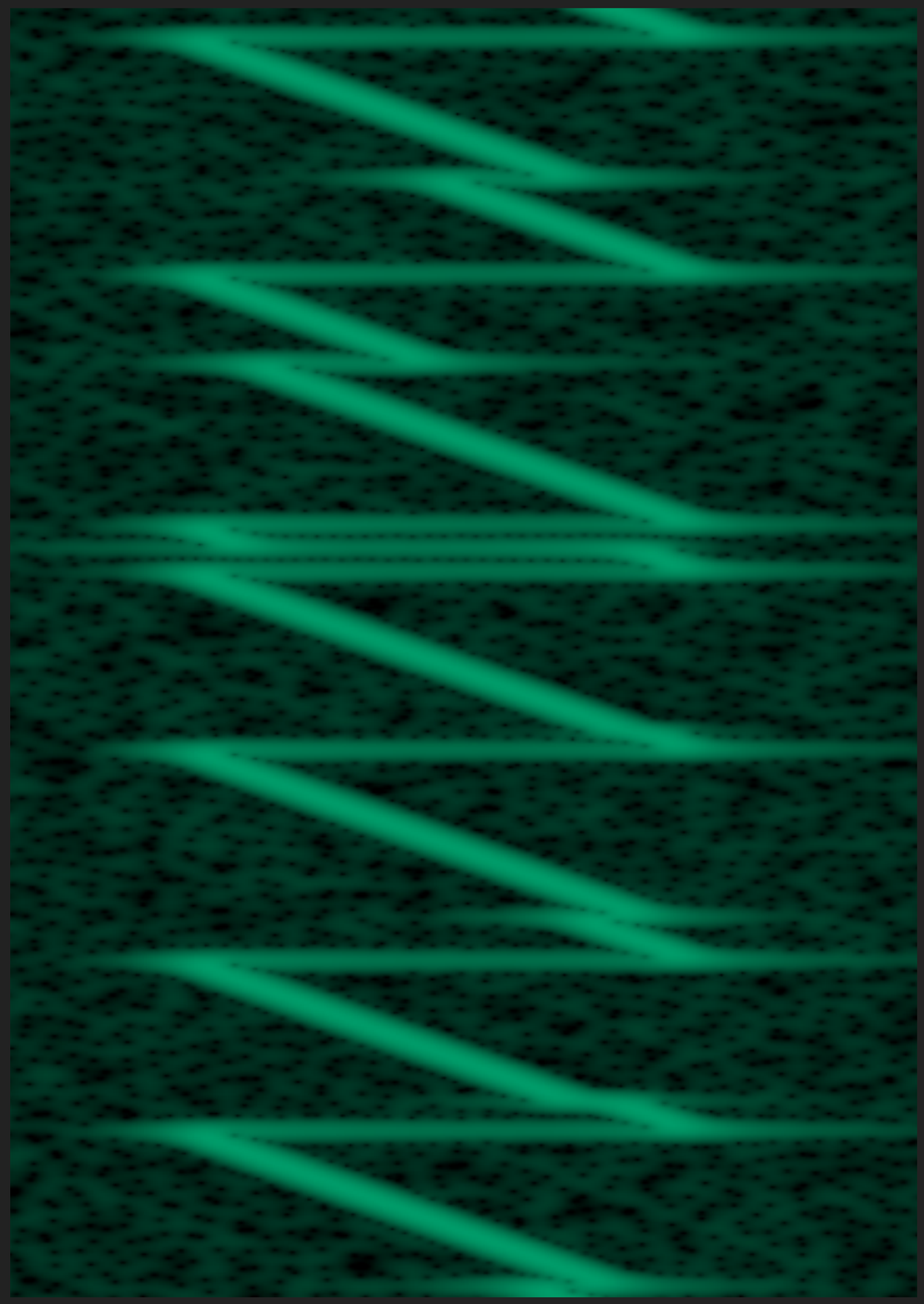
- Bandwidth: width of spectrum occupied by chirp
- Spreading factor: number of bits encoded per symbol (RF state, remember?)
- Chirp rate: first derivative of chirp frequency

SOME NUMBERS…

- US: 125kHz, 250kHz, 500kHz
- US: [7-12] bits per symbol
- bandwidth/(2**spreading_factor)

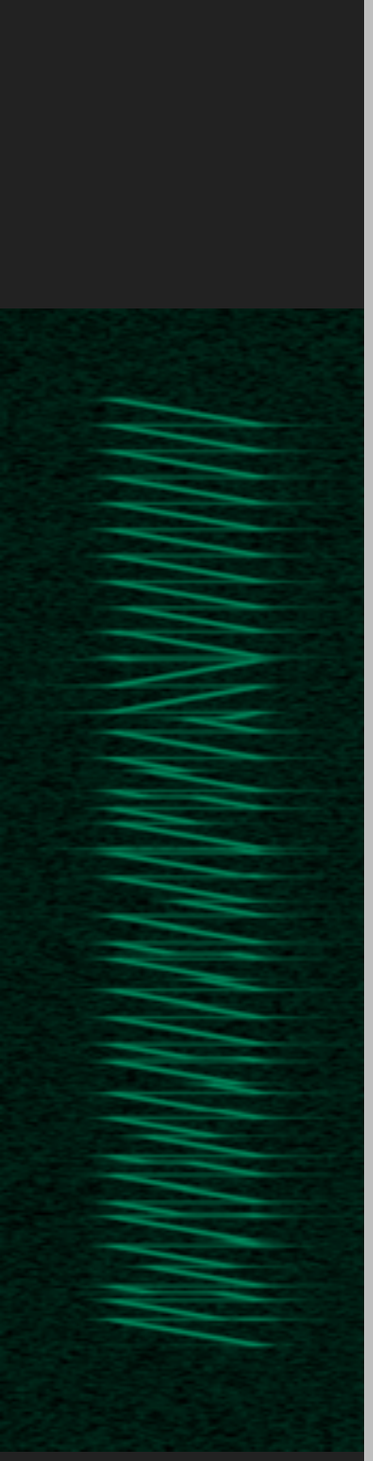
SO WHAT'S A SYMBOL?

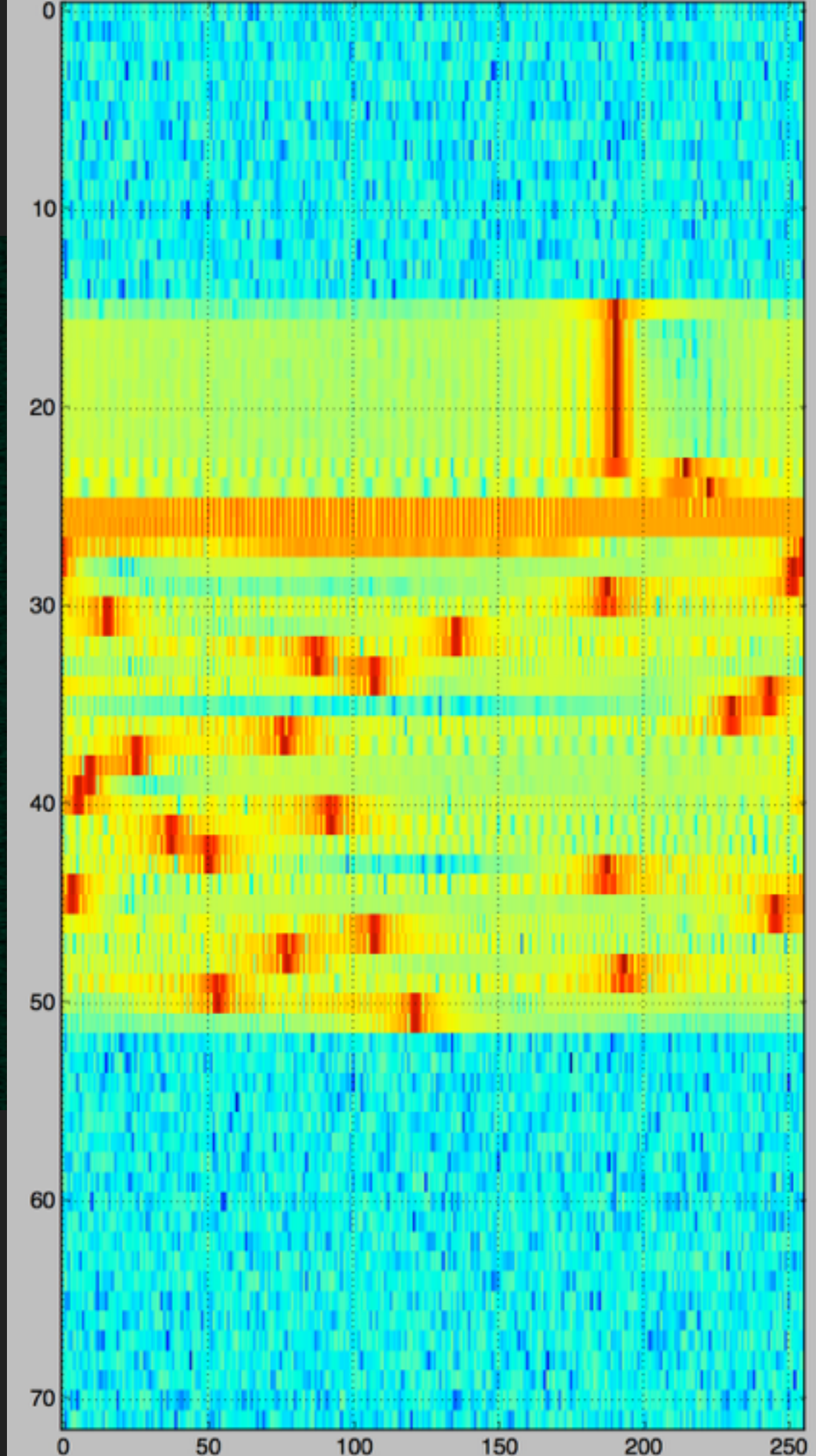
- Instantaneous change in frequency
  - FM modulated chirps
- LoRa spreading factor: number of bits encoded into each symbol
- How many possible symbols are there?
  - 2**spreading_factor

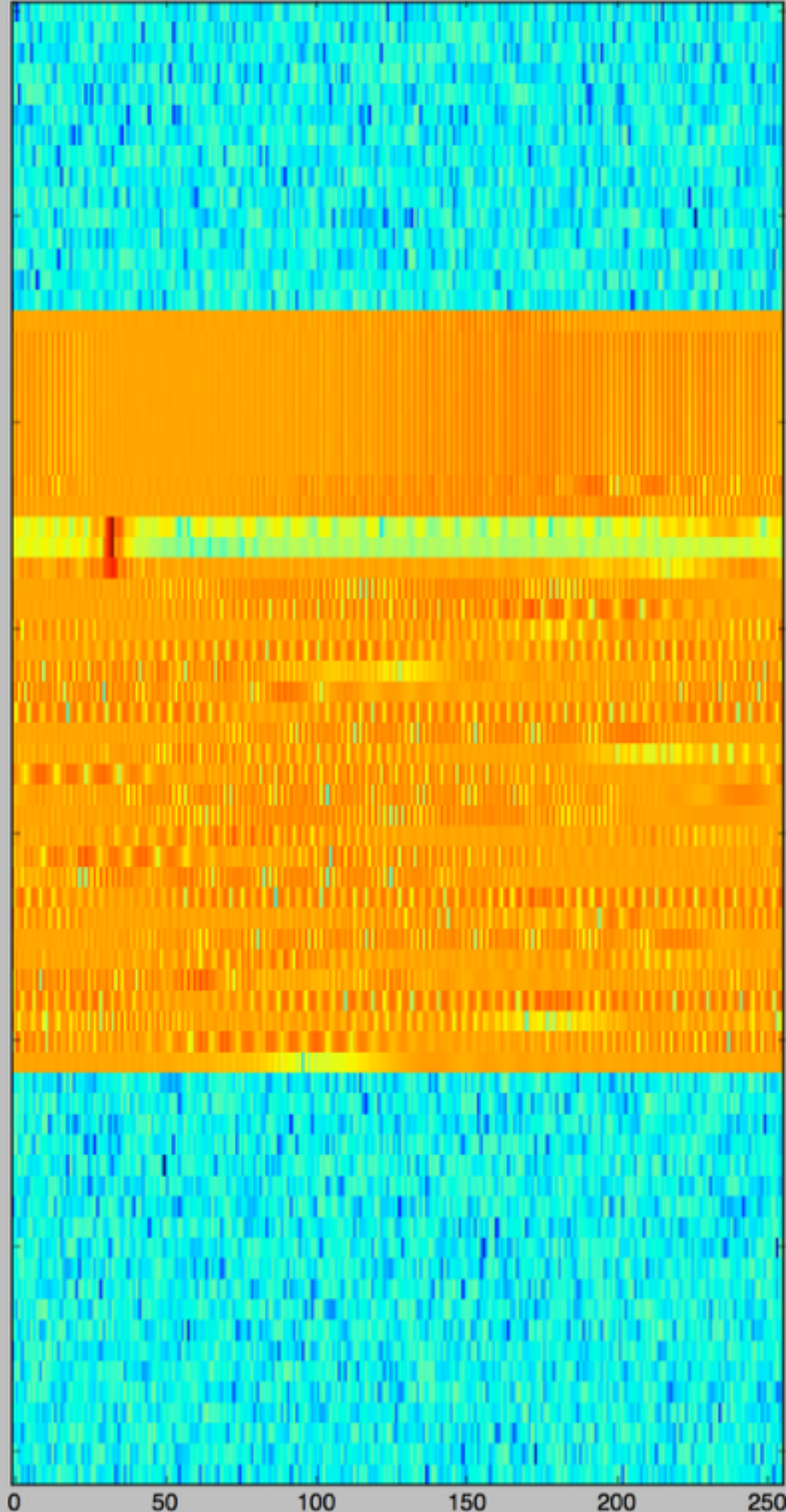


EXTRACTING SYMBOLS

- Channelize and resample signal to chirp bandwidth
- De-chirp with locally generated signal
- Take FFT of de-chirped signals, where length of FFT is equal to the number of possible symbols
- Most powerful component in each FFT is the symbol!




0
10
20
30
40
50
60
70
0
50
100
150
200
250


0
50
100
150
200
250

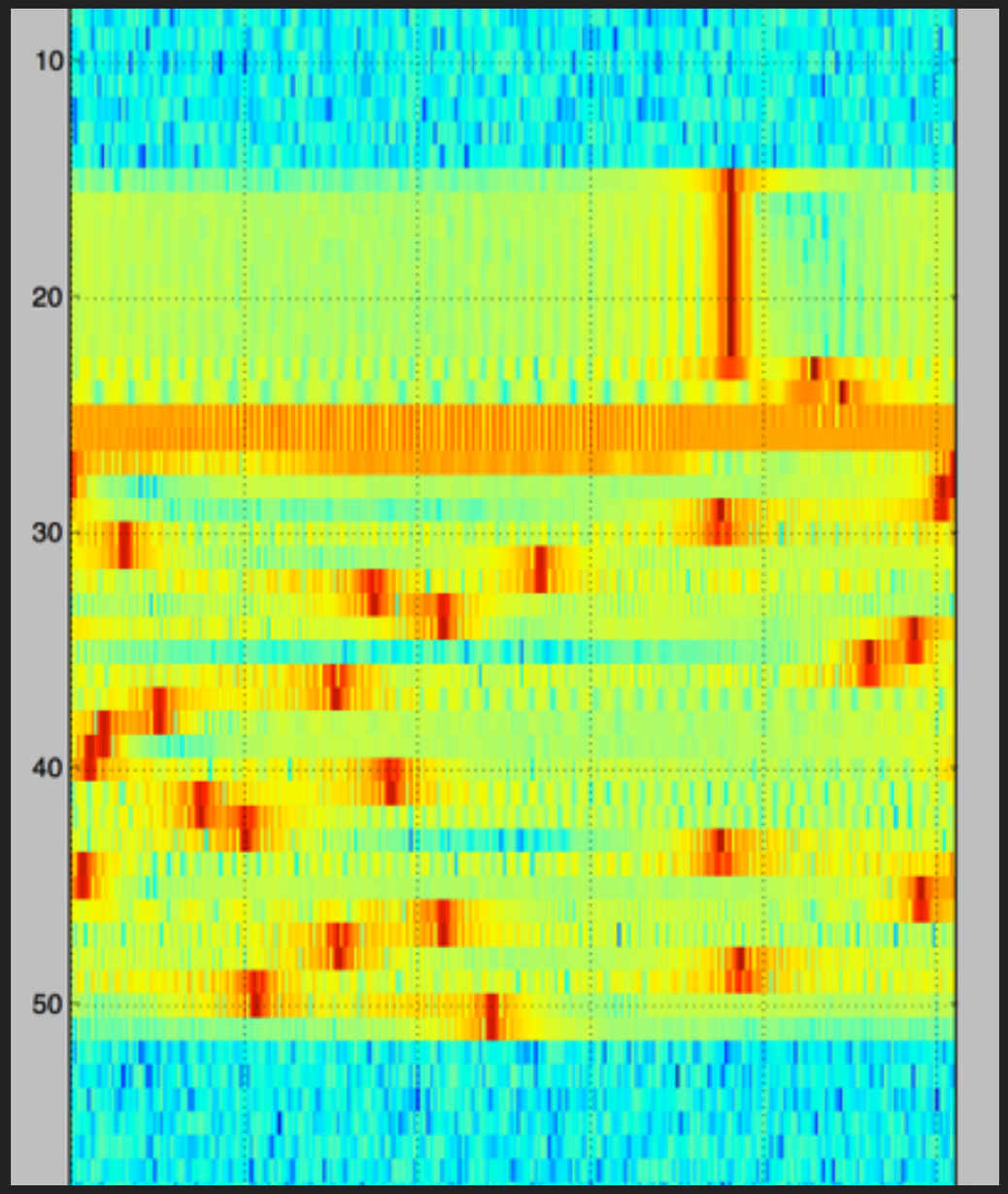
DEMODULATION SUMMARY

1. Identify the beginning of a packet

   - Preamble signified by continuous up-chirp

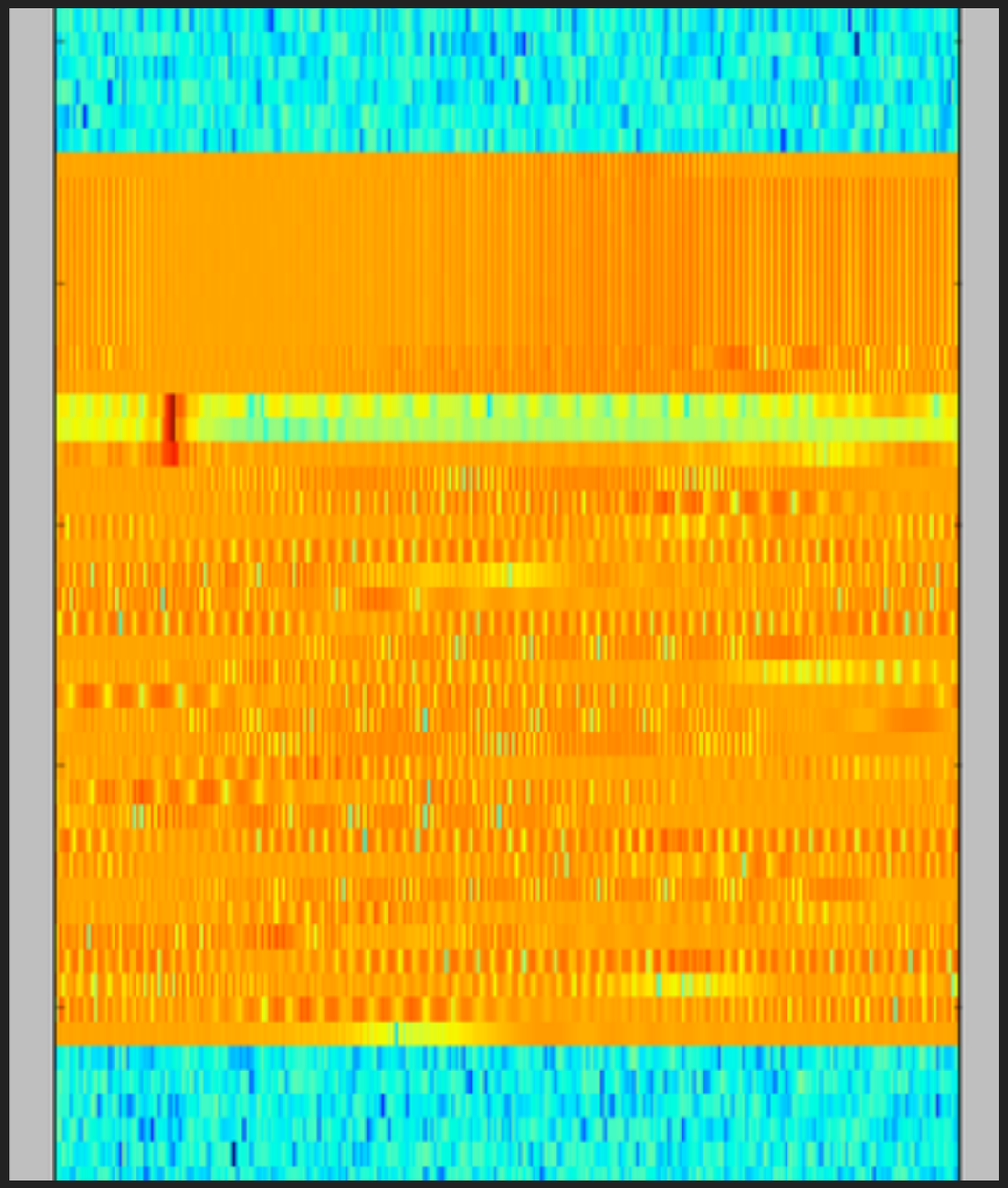
   - == same symbol being transmitted over and over

   - Look for some number of consecutive FFTs with maximum power in the same bin



DEMODULATION SUMMARY

2. Find the beginning of the PHY data unit
   - Repeat same process looking for SFD down-chirps
   - Down-chirp is complex conjugate of the up-chirp
   - PHY data unit begins 2 symbols after the SFD



BUT WAIT!

- Accurately finding SFD is essential for receiver synchronization
- Bad sync can spread symbol energy between adjacent FFTs
  - == incorrect data!

30

40

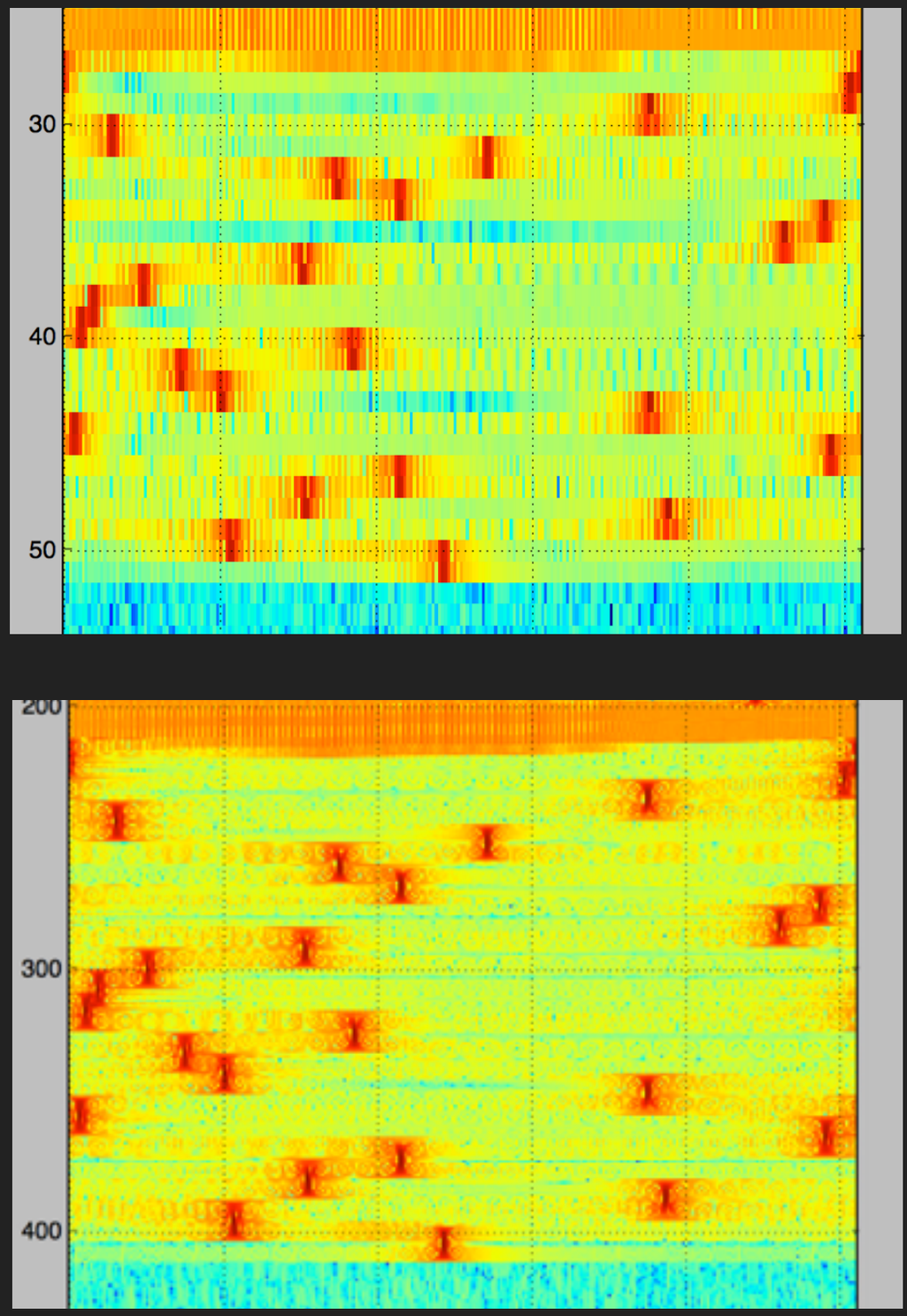
50

SFD SYNC SOLUTION

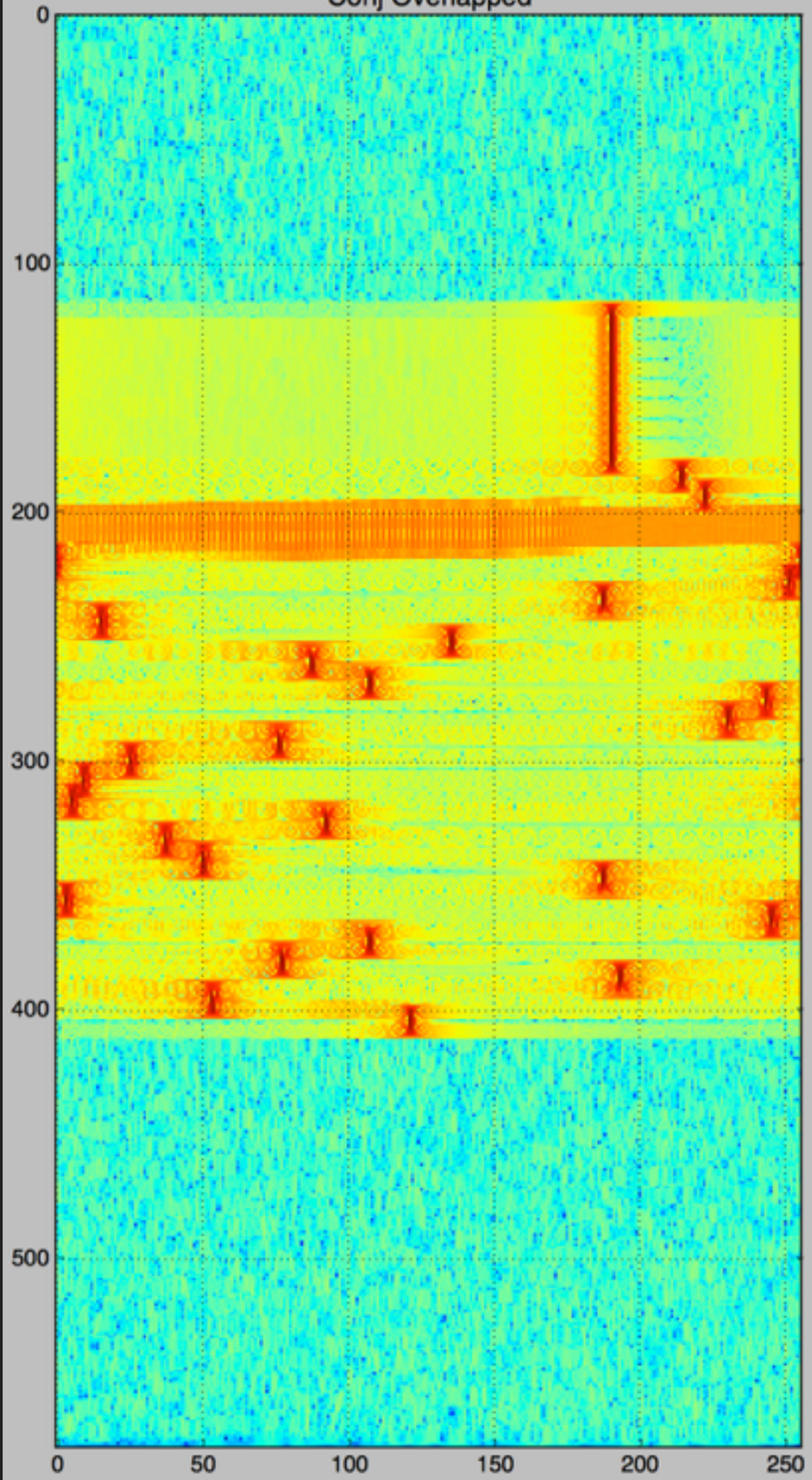
- Increase FFT time-based precision once preamble is found
- Overlapping FFT sample buffers!

OVERLAPPING FFTS

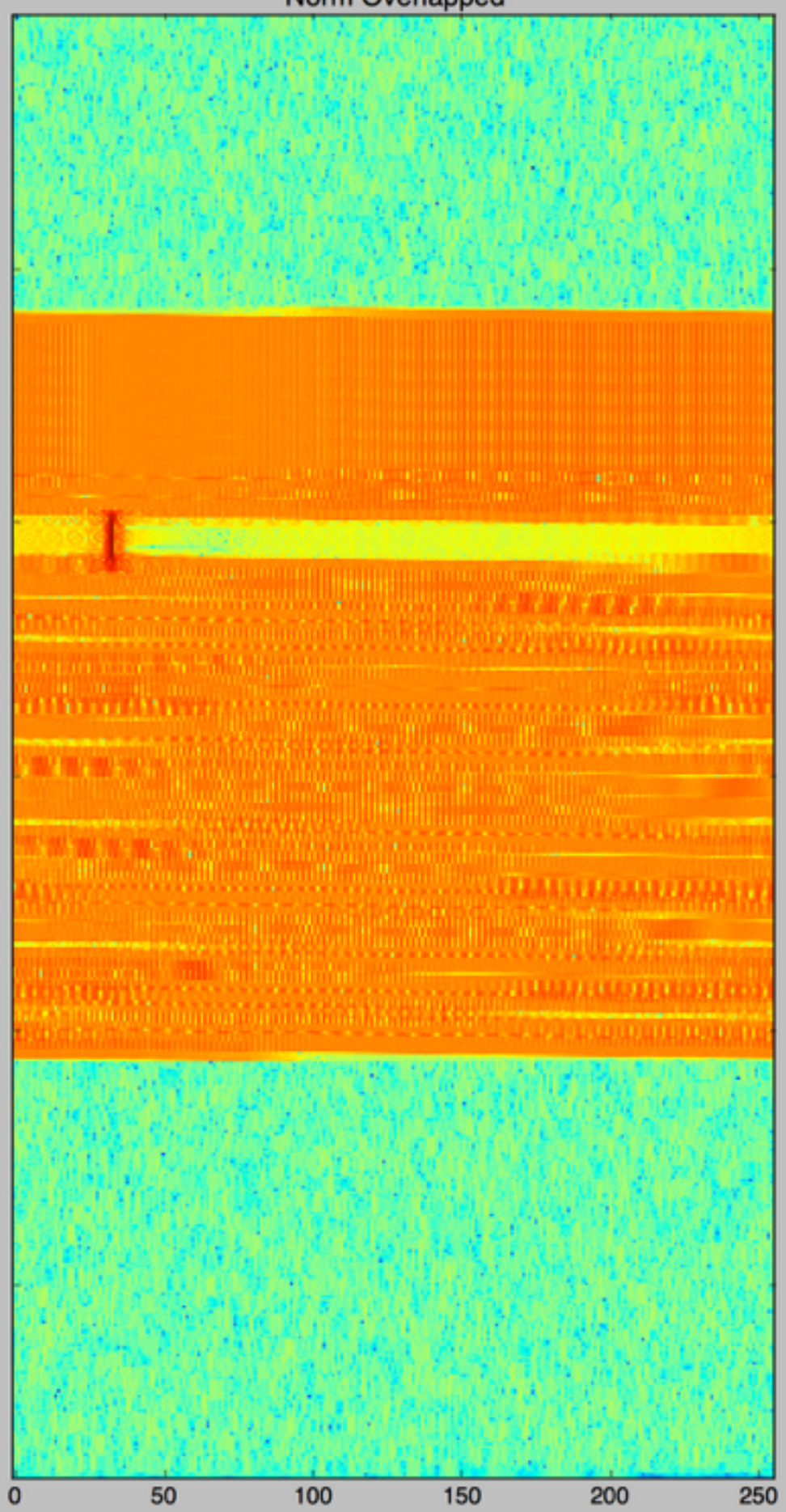
- Top: non-overlapping FFT
  - Each sample processed exactly once
  - [i*fft_len:(i+1)*fft_len-1]
- Bottom: overlapping FFT
  - Samples shifted across multiple FFTs
  - [i*(fft_len/n_overlaps]:(i+1)*(fft_len/n_overlaps)-1]

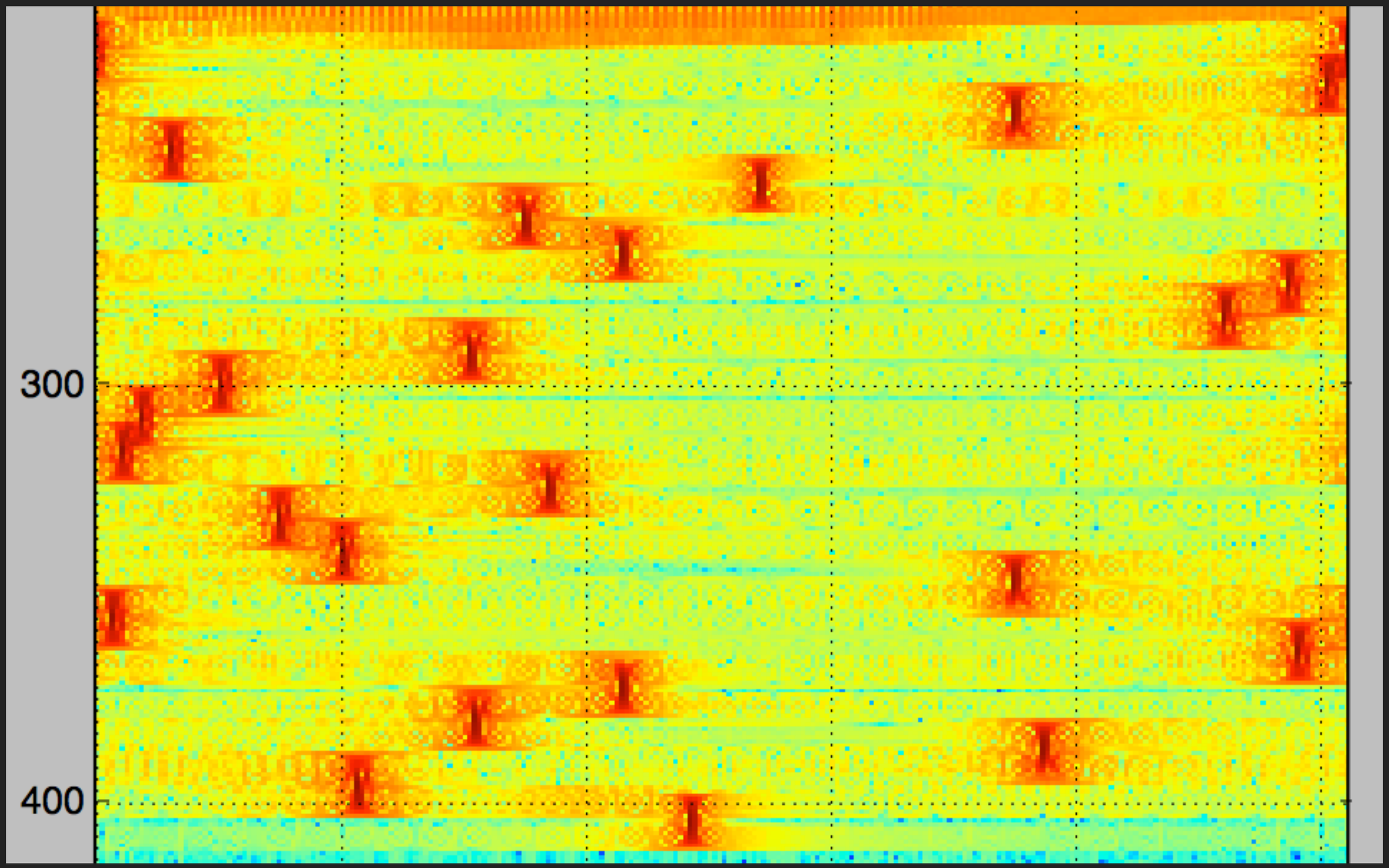


Conj Overlapped



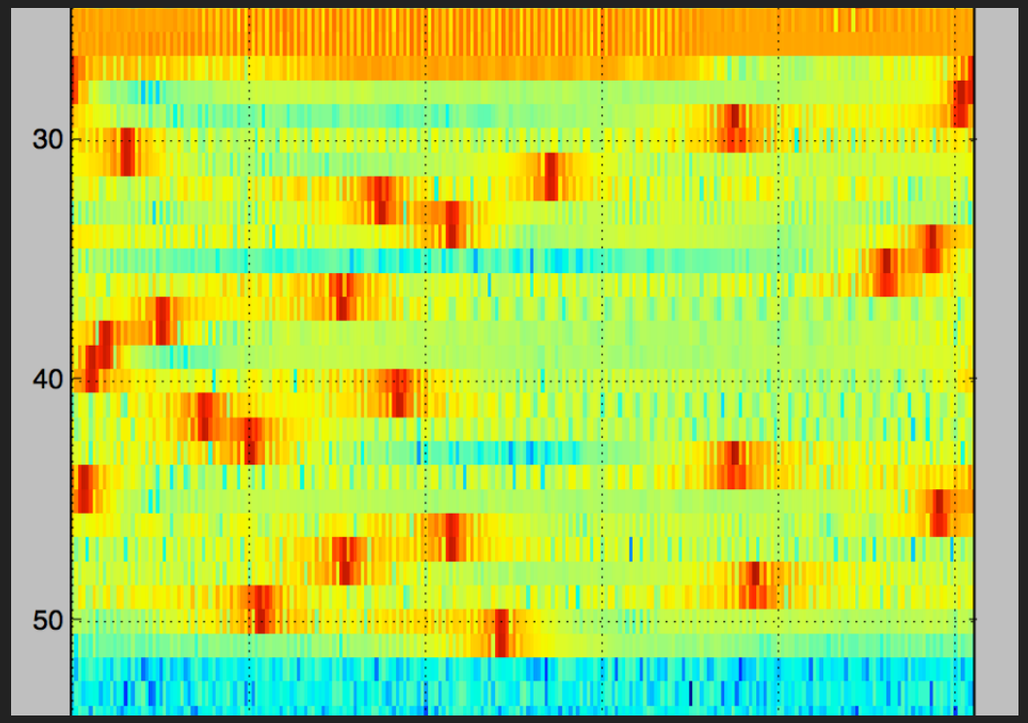
Norm Overlapped

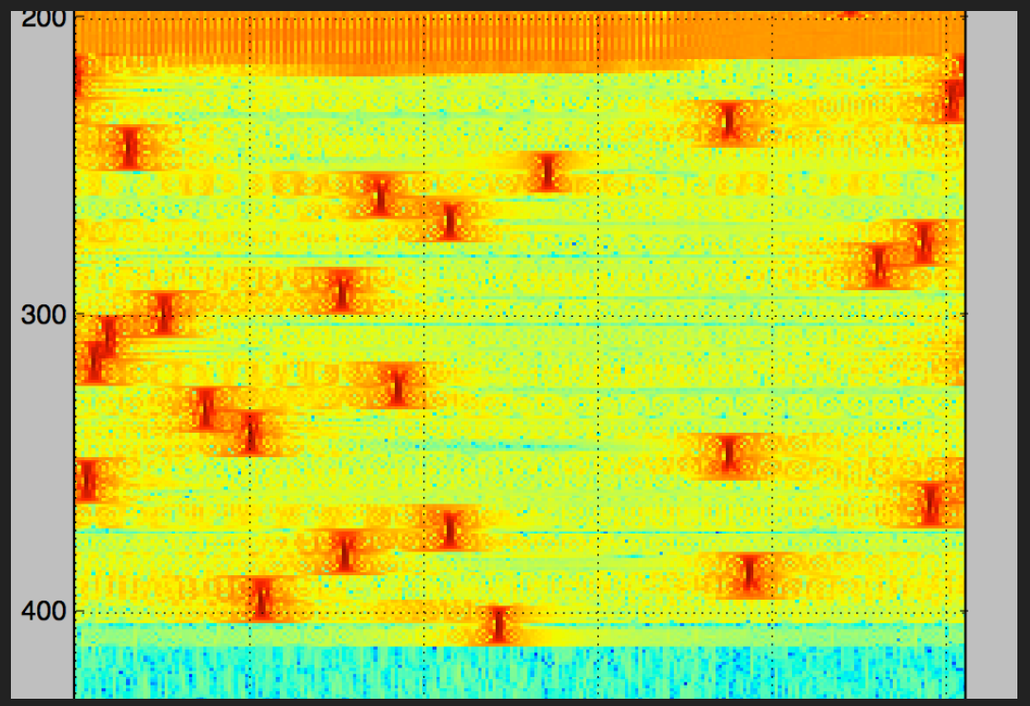


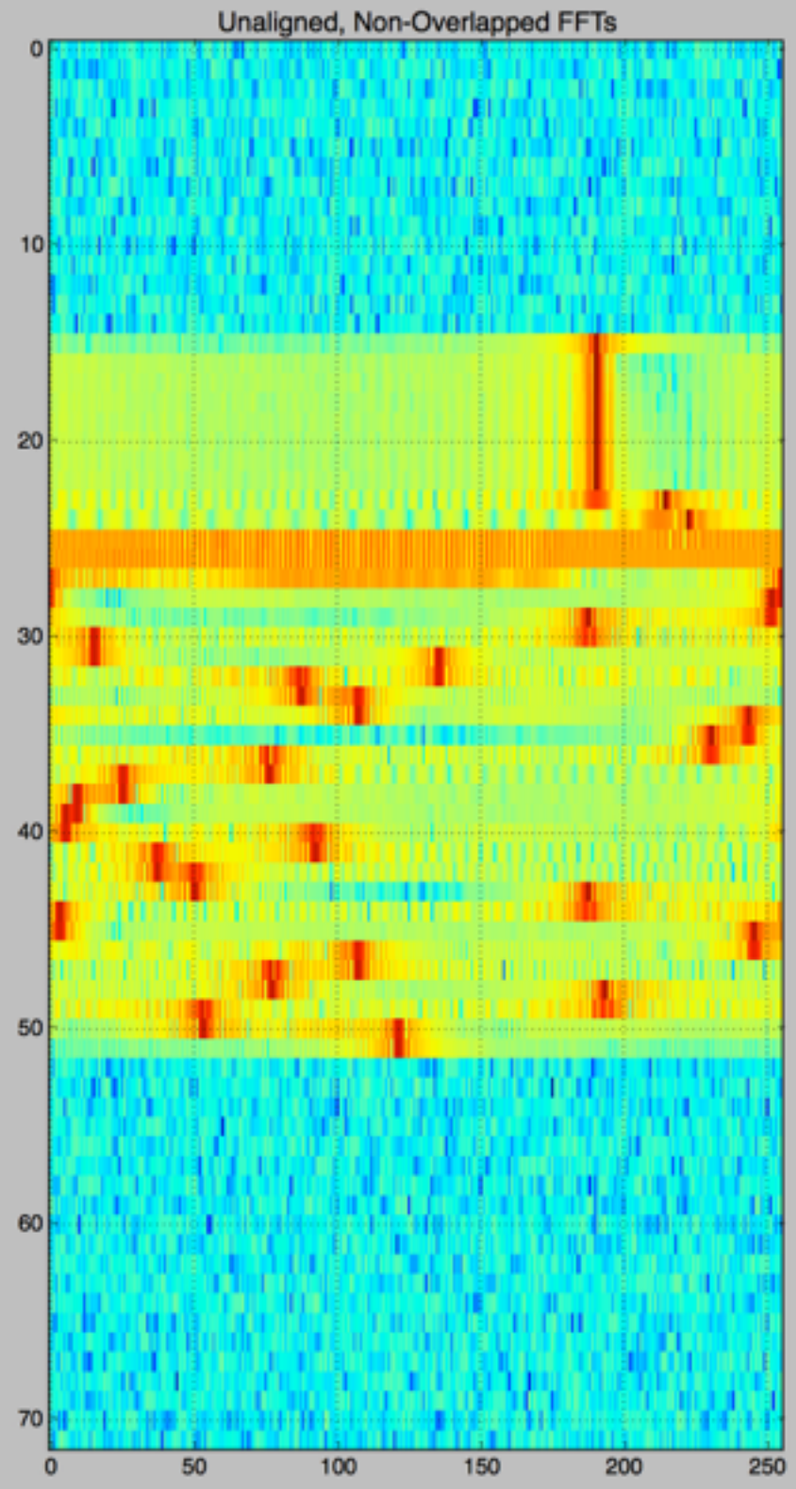

300
400

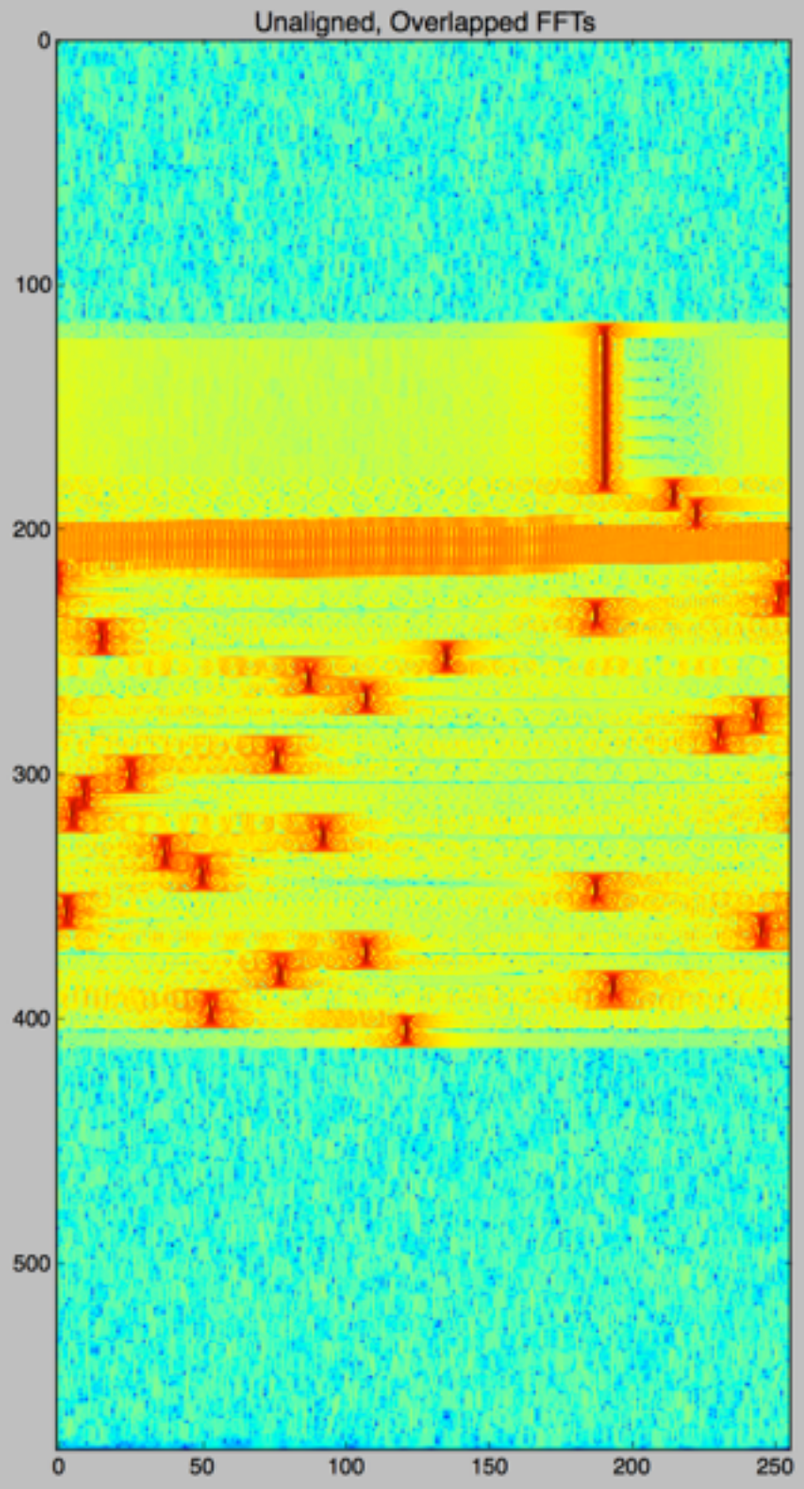
OVERLAPPING FFTS

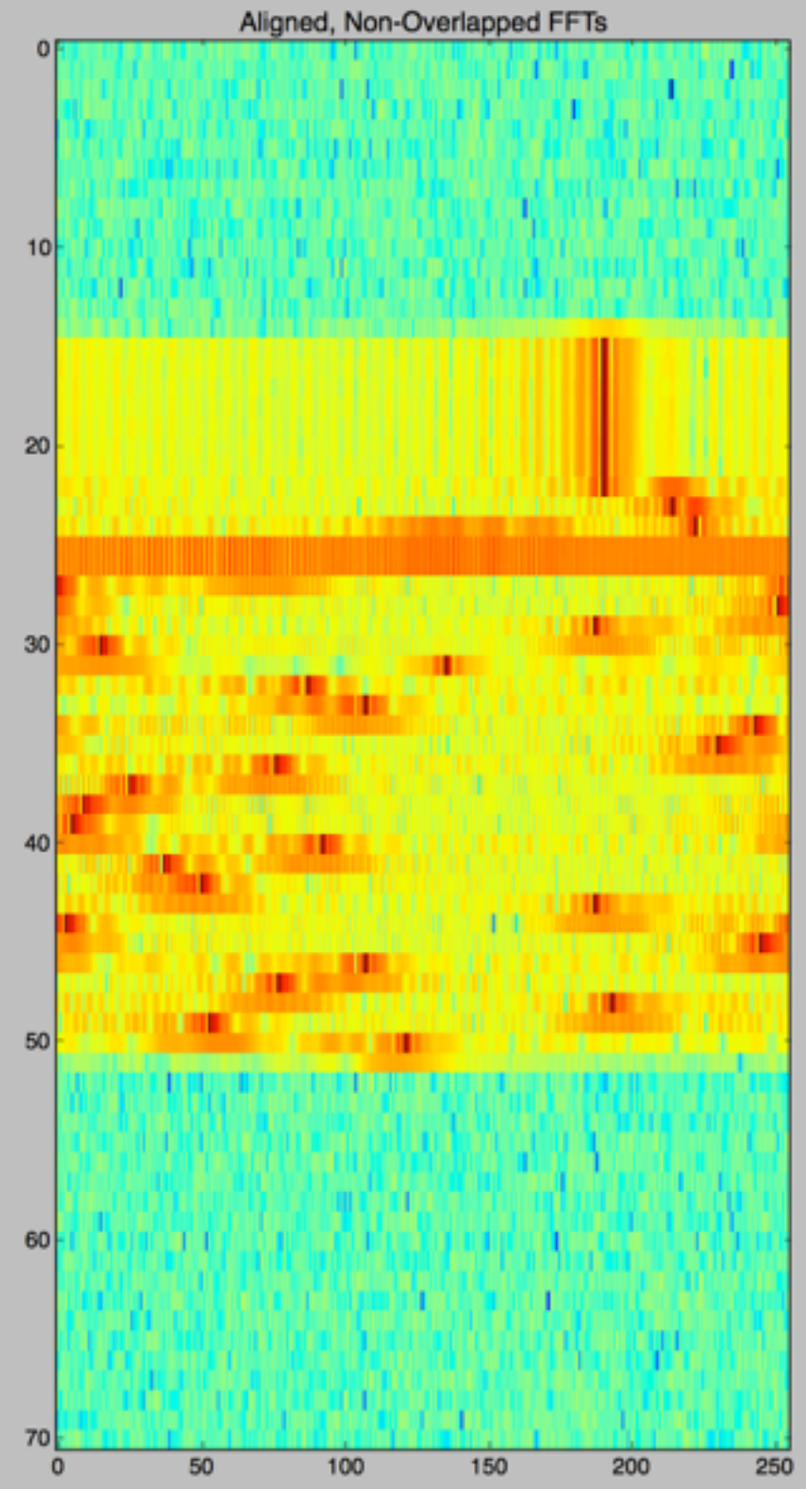
- Use overlapping FFTs to synchronize to first sample in the first SFD symbol
- Re-compute with non-overlapping FFTs to get your data!

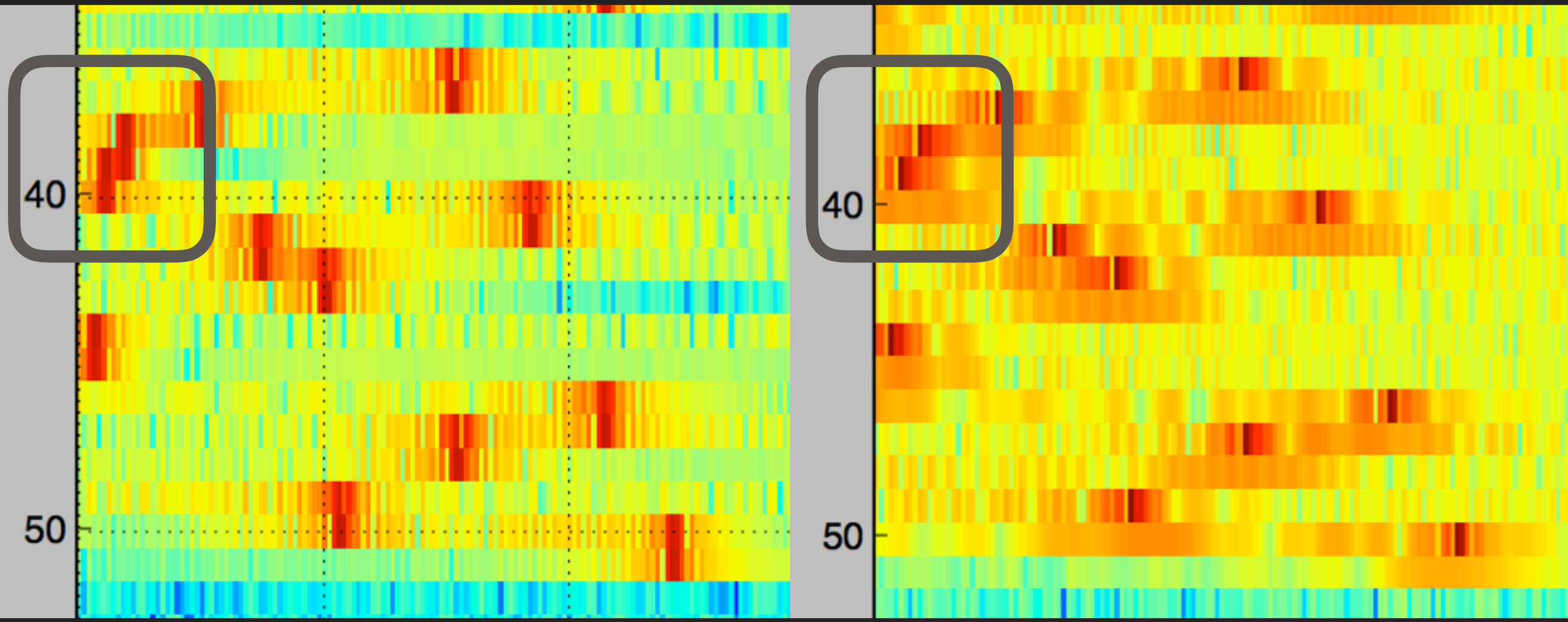


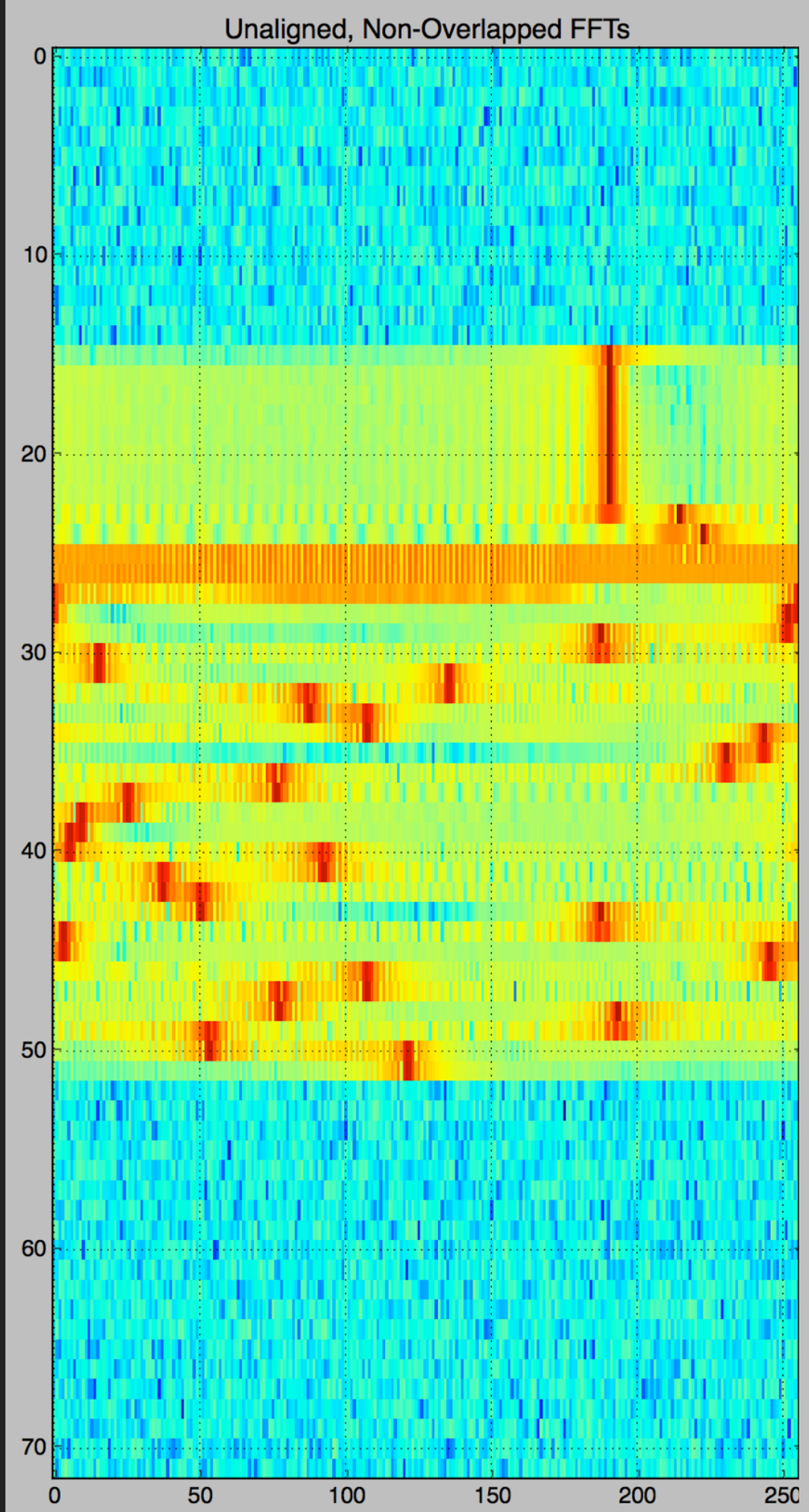


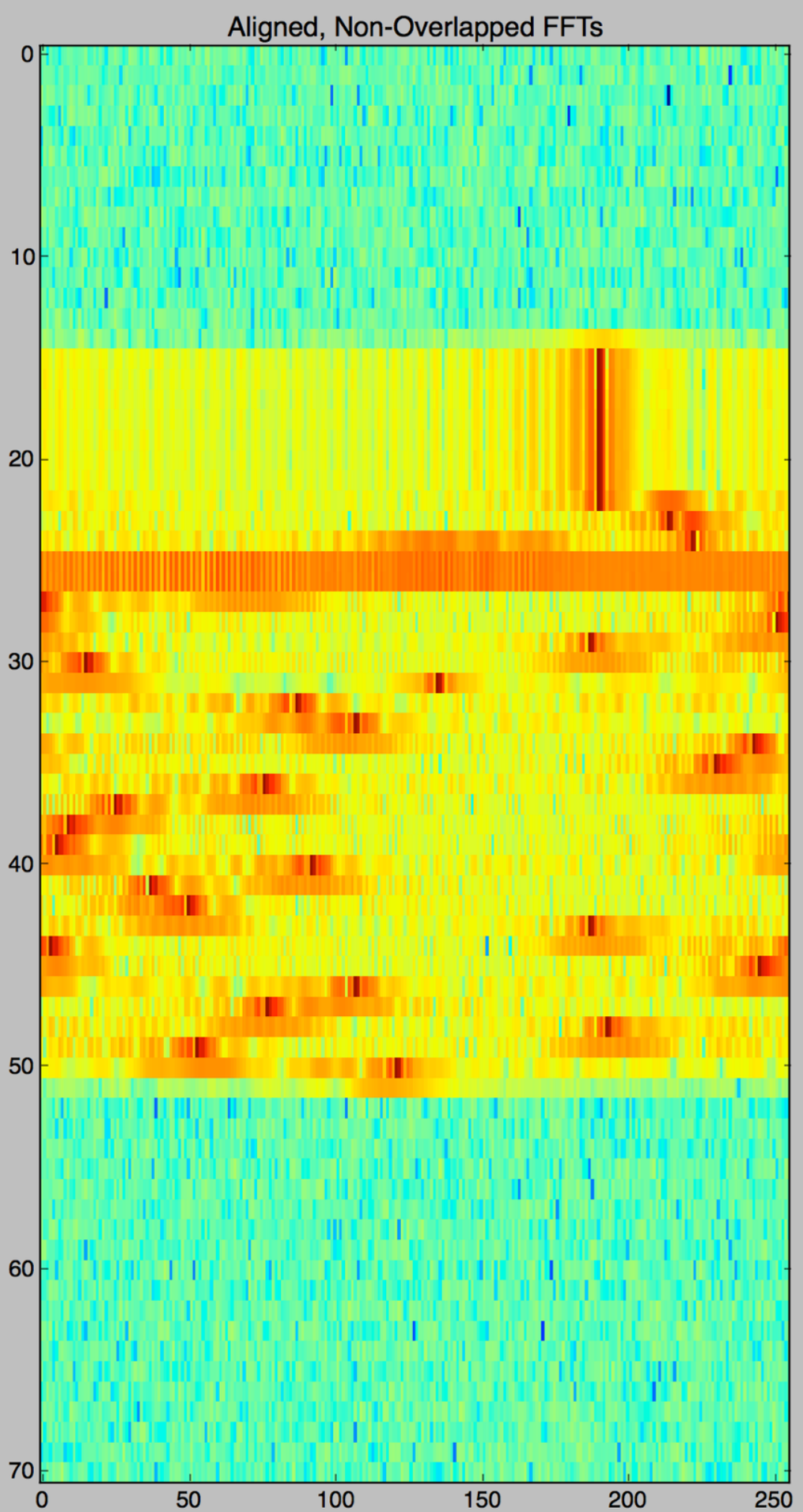

Unaligned, Non-Overlapped FFTs
0
10
20
30
40
50
60
70
0
50
100
150
200
250


Unaligned, Overlapped FFTs
0
100
200
300
400
500
0
50
100
150
200
250

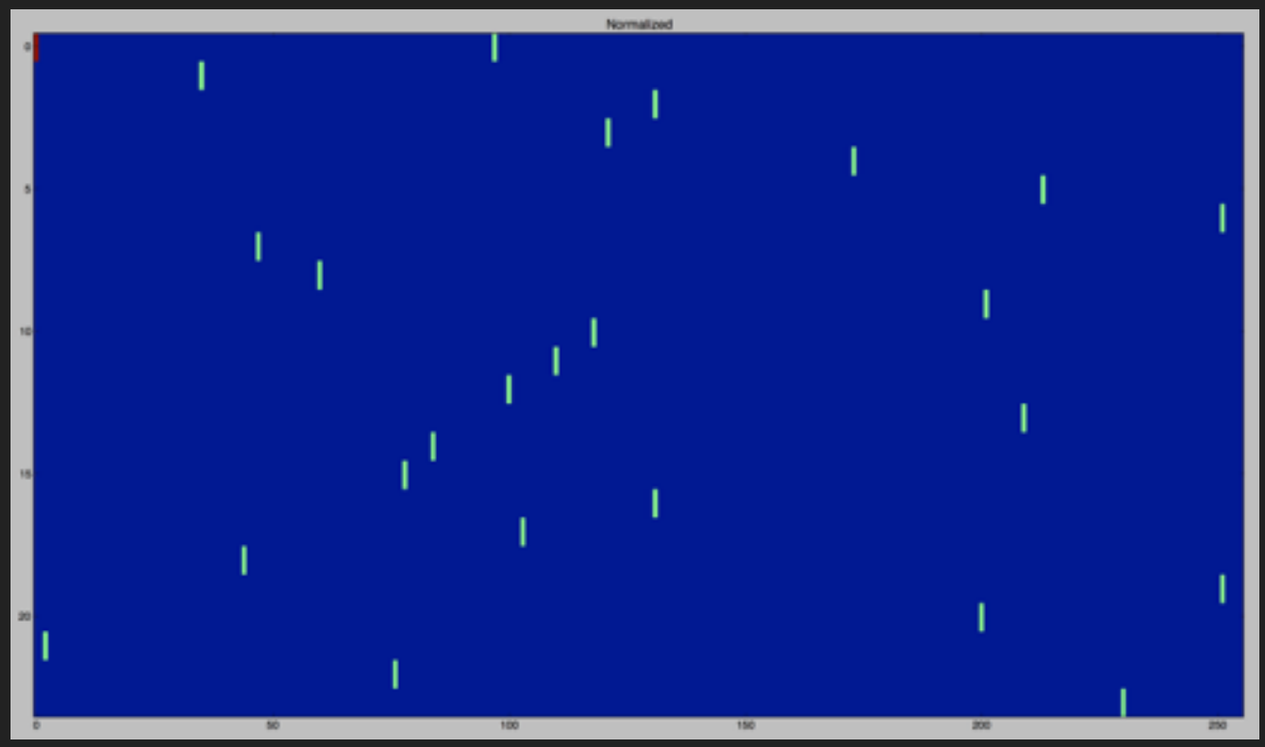

Aligned, Non-Overlapped FFTs
0
10
20
30
40
50
60
70
0
50
100
150
200
250


40
50
40
50


Unaligned, Non-Overlapped FFTs
0
10
20
30
40
50
60
70
0
50
100
150
200
250


Aligned, Non-Overlapped FFTs
0
10
20
30
40
50
60
70
0
50
100
150
200
250

DEMODULATION SUMMARY



3. Extract data from chirp phase transitions
   - Use described FFT method
   - Normalize data about the value of the preamble (always value 0)

WHAT ABOUT ENCODING?

CLOSED SOURCE

ENCODING DETAILS

- Semtech European patent application clues:
  1. Symbol “gray indexing” — Adds error tolerance
  2. Data whitening — Induces randomness
  3. Interleaving — Scrambles bits within frame
  4. Forward Error Correction — Adds correcting parity bits
- 4 distinct operations to reverse!

EASY ENOUGH?

NOPE

Why not?

DOCUMENTATION LIES

RED HERRINGS

- Decoding stages:
  1. Symbol “gray indexing”
  2. Data whitening
  3. Interleaving
  4. Forward Error Correction

Documentation:

- European patent LIE
- Datasheet LIE
- European patent SUPER LIE
- European patent, data sheets …actually ok

CRACKING THE DECODER

- Decoding stages:

1. Symbol “gray indexing”	CONTROLLED
2. Data whitening	CONTROLLED
3. Interleaving	?????
4. Forward Error Correction	…pretty confident

Only 1 experimental variable!

THIS WAS HARD

See my previous material for details

github.com/matt-knight/research

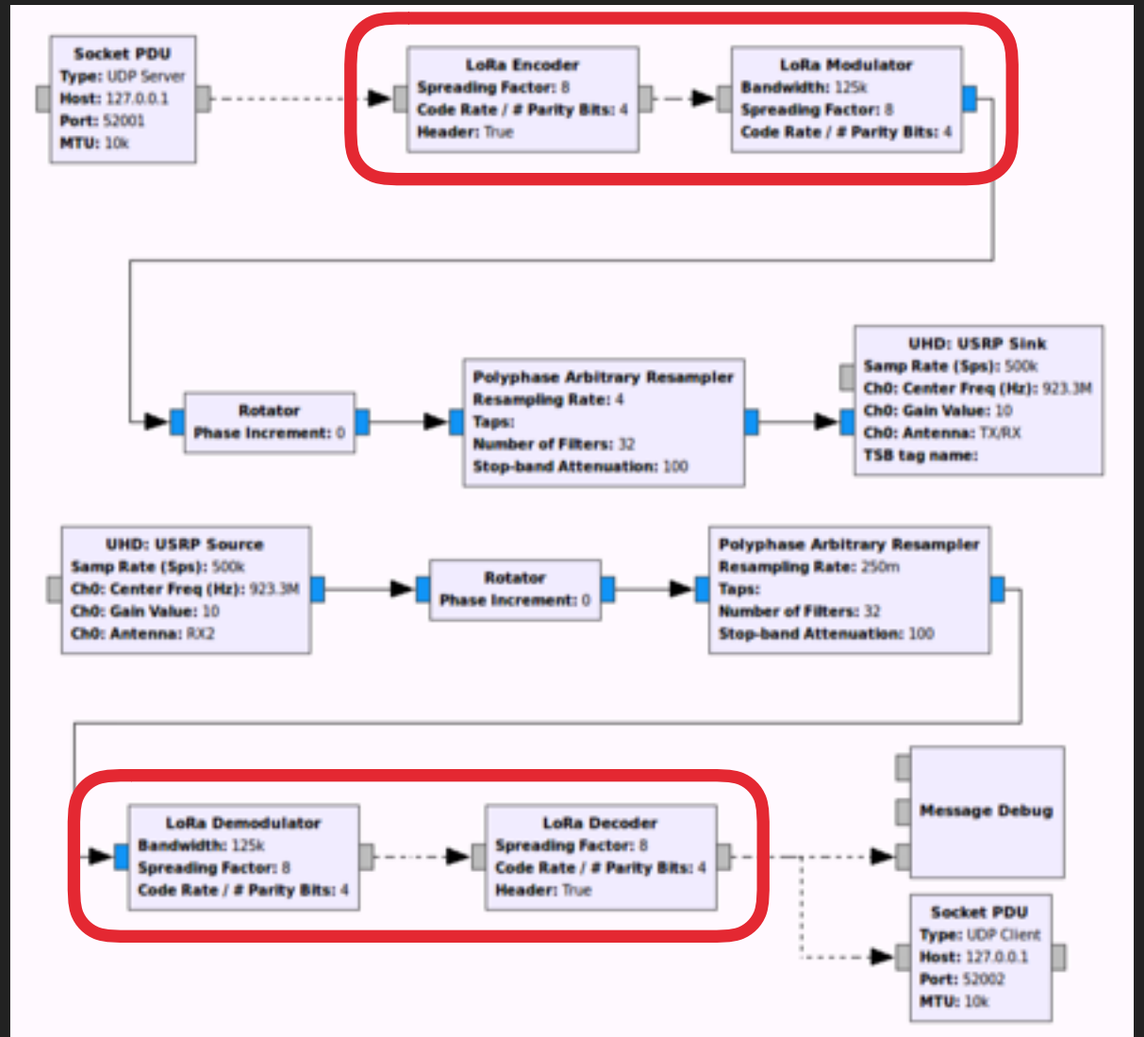
PoC||GTFO, GRCon16 Proceedings

INTRODUCING

GR-LORA

GR-LORA

- OOT GNU Radio module
- Open-source implementation of the PHY



MOTIVATION

- Existing interfaces to LoRa are at Layer 2 and above
  - IC interfaces and data sheets
  - LoRaMAC // LoRaWAN standards
- PHY layer security can’t be taken for granted

802.15.4 PHY LAYER EXPLOITS

- Packet-in-packet – Travis Goodspeed, Sergey Bratus, Ricky Melgares, Rebecca Shapiro, Ryan Speers
  - Layer 7->1 compromise
- WIDS evasion – Ira Ray Jenkins, Rebecca Shapiro, Sergey Bratus, Travis Goodspeed, Ryan Speers
  - Evading IDS // network monitors by fingerprinting receiver PHYs and crafting packets for selective evasion

802.15.4 PHY LAYER EXPLOITS

- Packet-in-packet – Travis Goodspeed, [illegible]erge[illegible] Br[illegible]us, R[illegible]ky Melgares, Rebecca Shapiro, [illegible]van [illegible]eer
  - Layer 7->1 c[illegible]romi[illegible]
- [illegible]VDD[illegible]e[illegible]asio[illegible] – Ira Ray Jenkins, Rebecca Shapiro, Sergey Bratu[illegible] Travis Goodspeed, Ryan Speers
  - Evading IDS // network monitors by fingerprinting receiver PHYs and crafting packets for selective evasion

PHYS MATTER

GNURADIO/POTHOS PRIOR ART

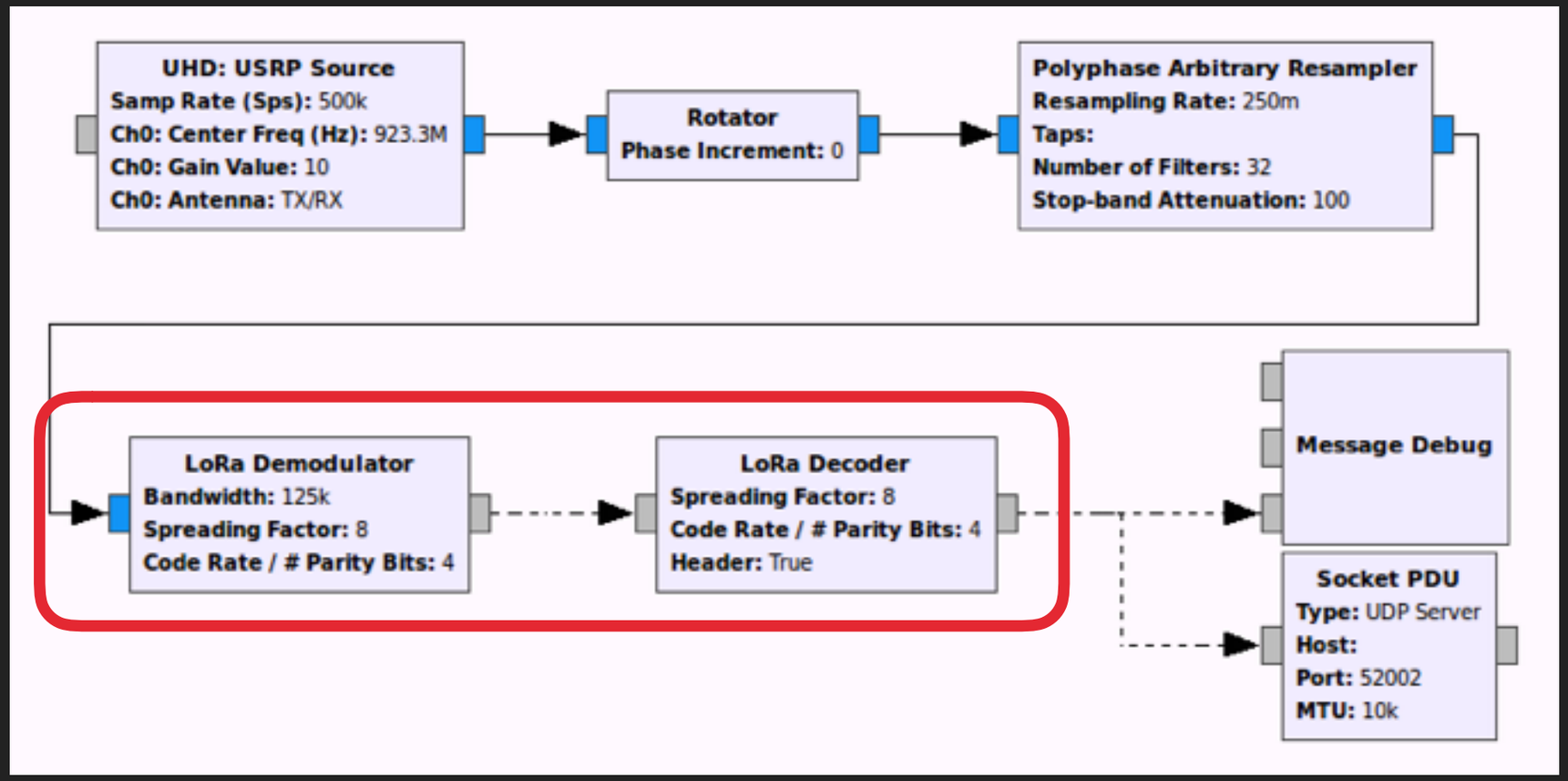
- Josh Blum's LoRa-SDR for POTHOS
  - Implements a LoRa-like modulation
    - Encoding/decoding is incorrect – follows reference documents, which differ drastically from reality
- rpp0's gr-lora
  - Python-based receiver for sf7 coderate 4/8
  - I couldn't get it to work

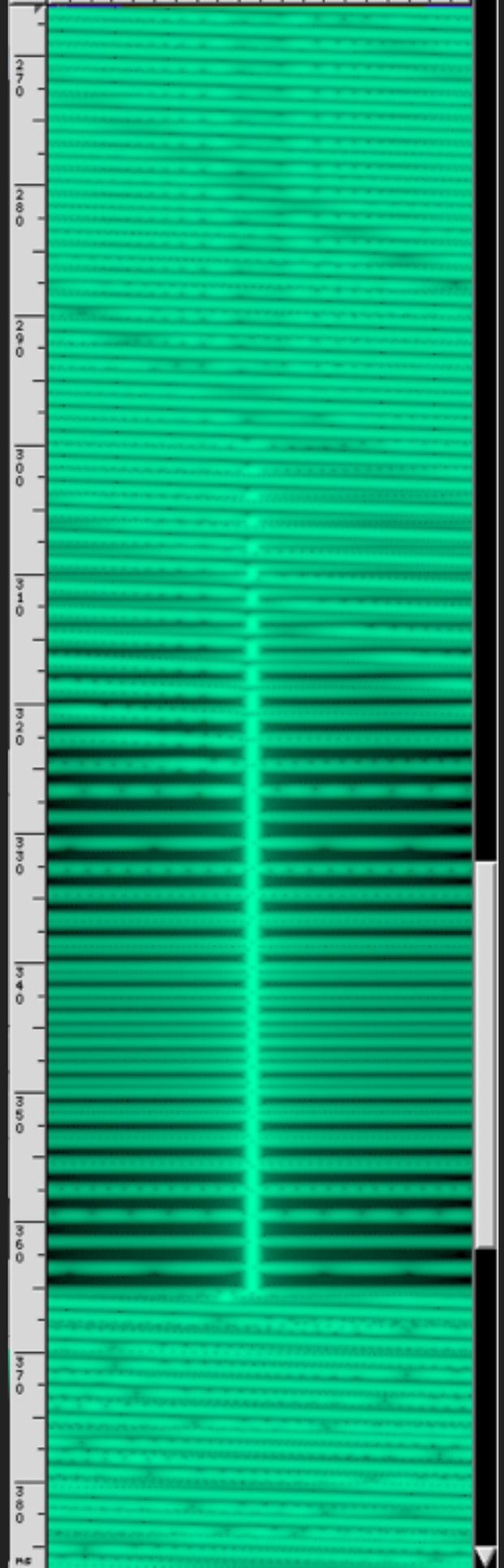
GR-LORA ARCHITECTURE

- Modulation and encoding stages are modeled as separate blocks
  - Allows for modularity and experimentation
- Asynchronous PDU interface between blocks
  - Super simple socket interface

DEMODULATOR // DECODER

- Implements algorithm gleaned from my Jailbreak Security Summit/DEFCON 24 research github.com/matt-knight/research
  - Dechirping, stacked FFTs, etc.



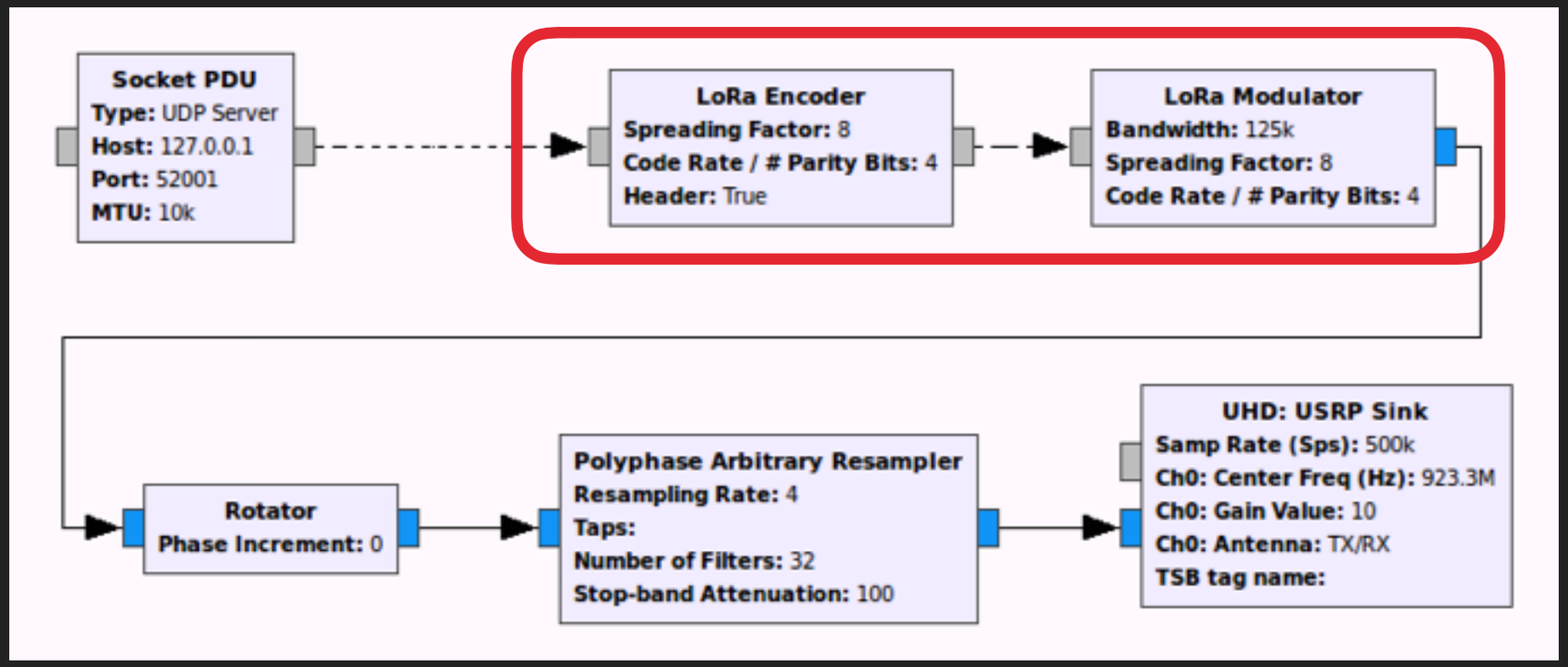


<– SFD samples shifting into FFT buffer

<– SFD sync found!

MODULATOR // ENCODER

- Modulator uses a pre-calculated c32 chirp LUT and a phase accumulator
  - More efficient than FM or IFFT



GR-LORA SOURCE

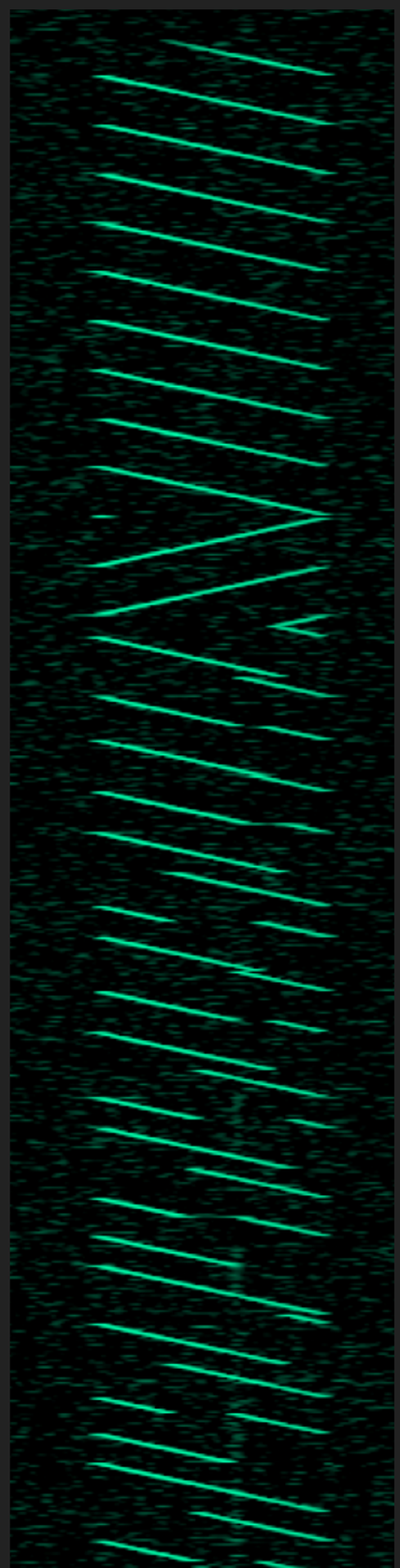
- github.com/BastilleResearch/gr-lora

GR-LORA TODOS

- Additional spreading factors and code rates
- Improve whitening sequence accuracy
  - PHY header support
  - PHY CRC support
- Alternate demod strategies, sync improvements
- Clock recovery, if necessary
- Implement upper layers (LoRaWAN)

TO CONCLUDE

- LPWANs have momentum and are proliferating
- RF stacks are becoming more diverse
  - Wireless is no longer just WiFi
- Shown how to go from obscure RF –> bits
- Added a new tool to the RF researcher's arsenal



ACKNOWLEDGEMENTS

- Balint Seeber, Bastille Threat Research Team
- Josh Blum, hexameron, and Bertrik Sikken, open source contributors
- GNU Radio Conference for hosting
- GNU Radio community for everything over the years

THANKS

matt@Bastille.net
@embeddedsec

QUESTIONS?

matt@Bastille.net
@embeddedsec