RSAConference2017
San Francisco | February 13 – 17 | Moscone Center

POWER OF OPPORTUNITY

SESSION ID: HTA-F01

Decoding LoRa, a Wireless Network for the Internet of Things

Matt Knight
Senior Software Engineer, Security Research
Bastille Networks
@embeddedsec

Who Am I

- Matt Knight
  - matt@Bastille.net
  - @embeddedsec
- Software Engineer and Security Researcher
- BE & BA from Dartmouth
- Applied RF security research

Wireless Proliferation

- Cisco IBSG: **50 billion devices** by 2020
  - Fewer wires every year
- Wireshark wasn't always a thing
- 802.11 monitor mode wasn't always a thing
- Low-level access to interfaces is paramount for enabling comprehensive security research

Agenda

1. Introduce LoRa and LPWANs
2. Review technical radio concepts
3. Demodulate and decode the **LoRa PHY** with SDR
4. Introduce **gr-lora**

What's LoRa?

Wireless IoT Protocol

IoT == Embedded

Internet of Radios

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?

Cellular?

1. IT WORKS EVERYWHERE
2. EASY TO INSTALL

It’s Thirsty

It's Going Away*

*2G, THAT IS

Deprecation: A Developer's Conundrum

- AT&T turned off 2G GPRS on **January 1, 2017**
- Other major carriers have plans to follow

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

Replacing 2G

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

Void in Market

RSAConference2017

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**: **L**ow **P**ower **W**ide **A**rea **N**etwork
- **Like cellular**, but optimized for **IoT**/M2M
  - Network of basestations worldwide
  - Star network to endpoints, UL/DL traffic
  - Range in **miles**

Emerging Standards

LTE-M

NB-LTE

IEEE 802.11ah

EC-GSM

ZigBee3.0

Bastille.net

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

Aggressive Investment

- SIGFOX raised **€150MM** in November 2016
  - WSJ/FT: Possible US IPO soon
- Senet and Actility, LoRa backers, raised a combined **51MM**
- LoRa Alliance membership tripled in 2015

senet
the *sensible* network company

actility
Making Things Smart

SIGFOX
One network A billion dreams

Bastille.net

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

Optimized for IOT

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

Compromise as a Feature

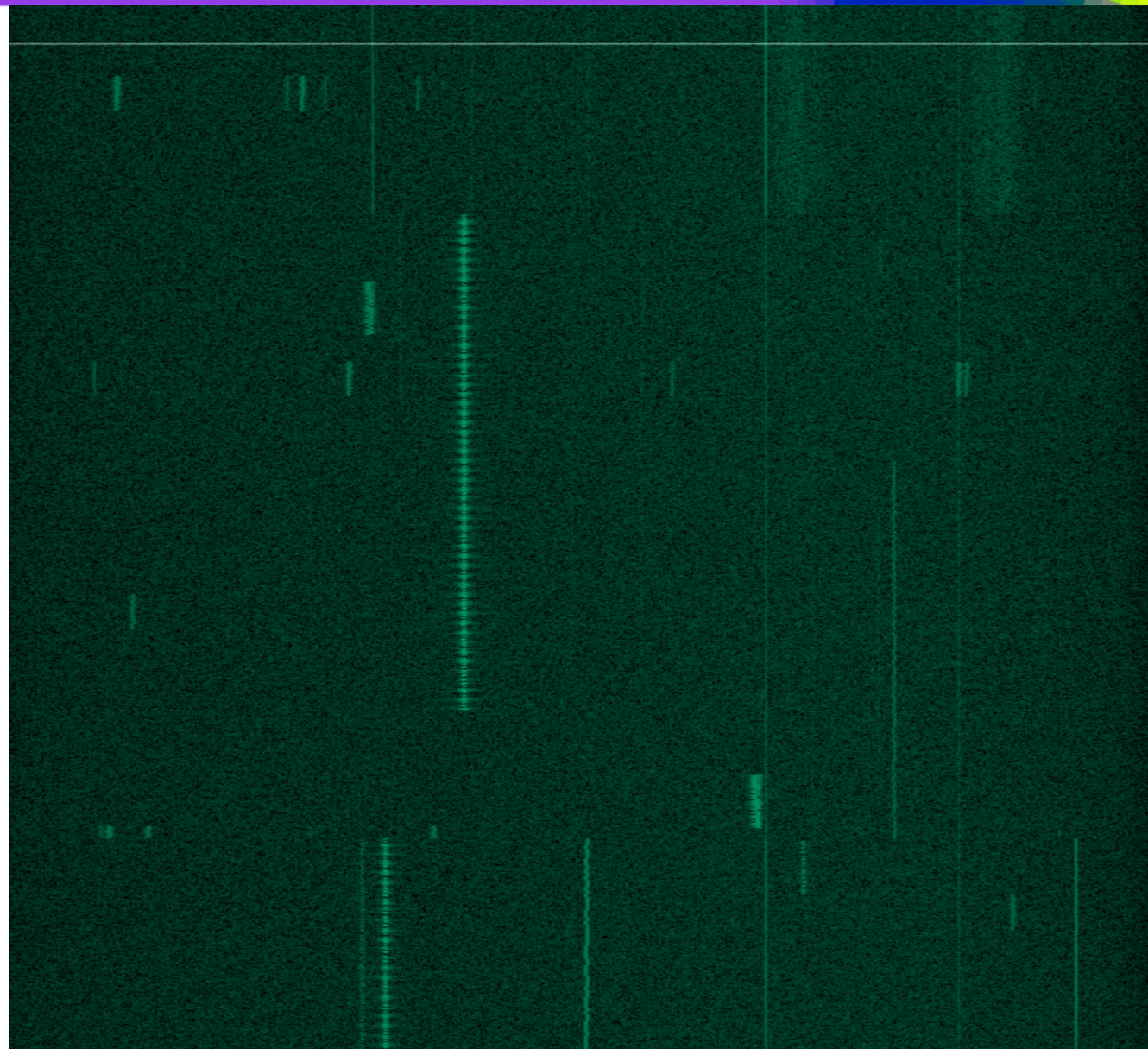
- Conservative **duty-cycling** and listening
- Very **sparse** datagrams
- Highly **rate-limited**

Compromise as a Feature

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

Licensure, or Lack Thereof

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



Licensure, or Lack Thereof

- Compare this with cellular
  - Regulatory authorities auction cellular spectrum licenses for billions
  - Restricts infrastructure to biggest telcos
- Right: opening bid list for FCC TV whitespace reverse auction

DMA[1]	Call Sign	Move Off-Air	Move to Low VHF	Move to High VHF
New York, NY	WABC-TV	603,628,380	351,5	NA
New York, NY	WCBS-TV	900,000,000		
New York, NY	WDVB-CD	424,772,100	318,5	169,908,840
New York, NY	WEBR-CD	376,508,700	282,381,52	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	229,530,520

Bastille.net

LoRaWAN Network Providers

- Senet
  - Commercial network
- The Things Network
  - Crowdsourced
- LoRaHAM
  - Travis Goodspeed & neighbors
- **No licensed spectrum required…!!**

Bastille.net

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

Nomenclature

- LoRa vs. LoRaWAN
  - **LoRa**: PHY layer
  - **LoRaWAN**: MAC, NWK, and APP built on LoRa

RSAConference2017

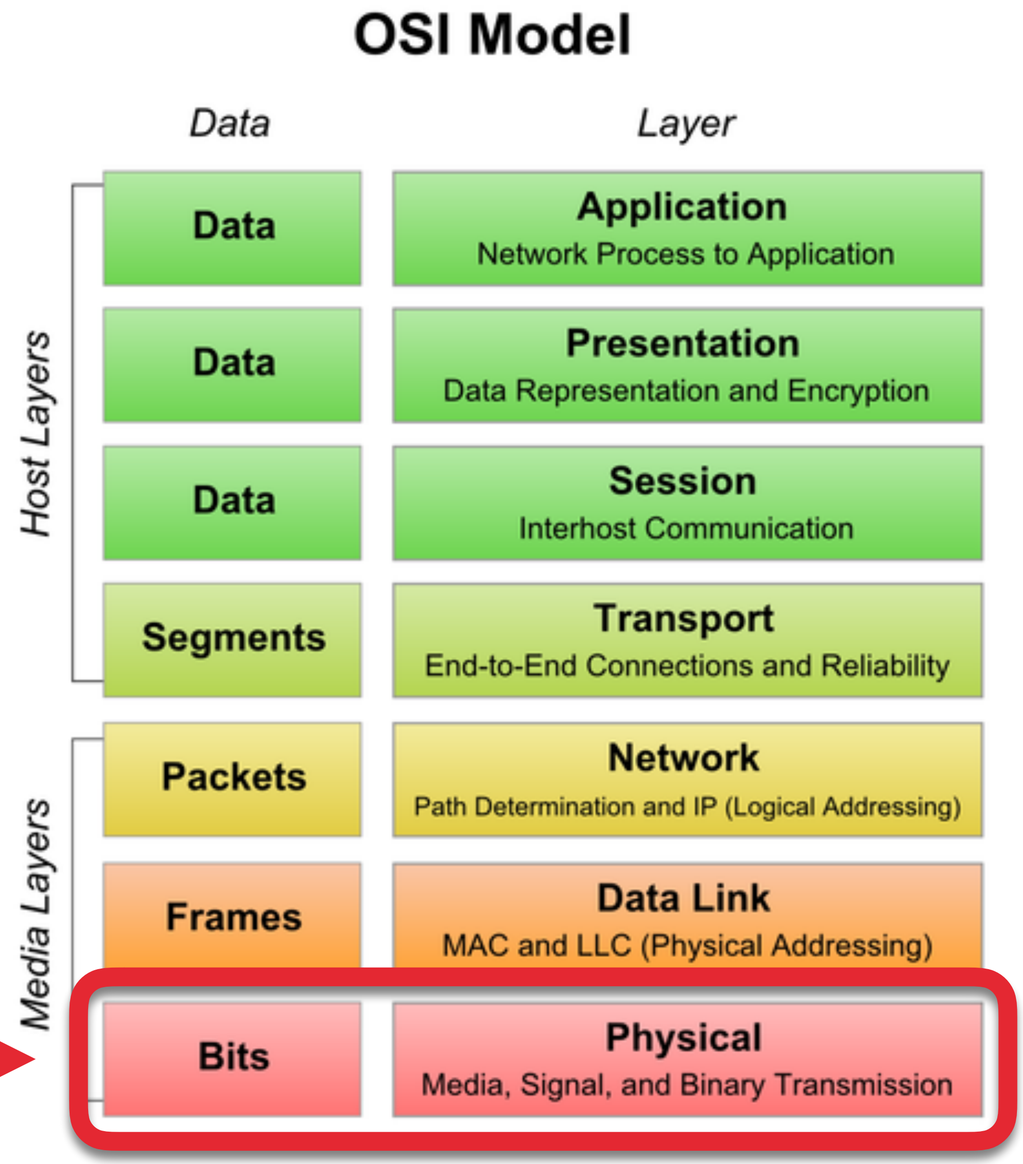
OFFENSIVELY

~~Obscenely~~ Short

Radio Crash Course

PHY Layer

- Lowest layer in communication stack
- In wired protocols: voltage, timing, and wiring defining 1s and 0s
- In wireless: patterns of energy being sent over **RF medium**

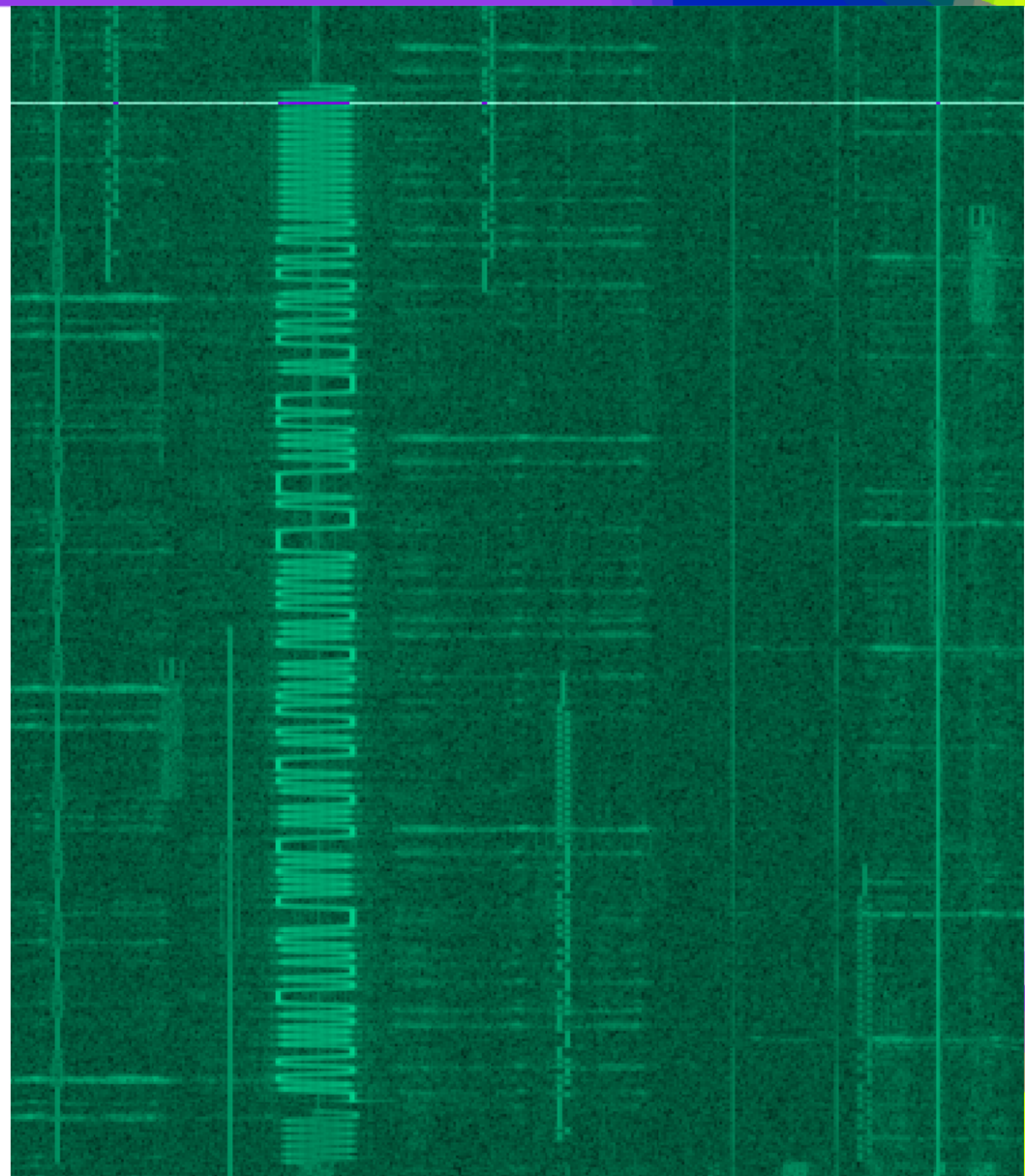


Bastille.net

http://www.tech-faq.com/wp-content/uploads/2009/01/osimodel.png

What is RF?

- “[RF] is one of the four fundamental forces of the universe!”
  - Tom Rondeau, DARPA PM and former GNU Radio lead
- “Radio Frequency”
- Electromagnetic waves
- **Energy**



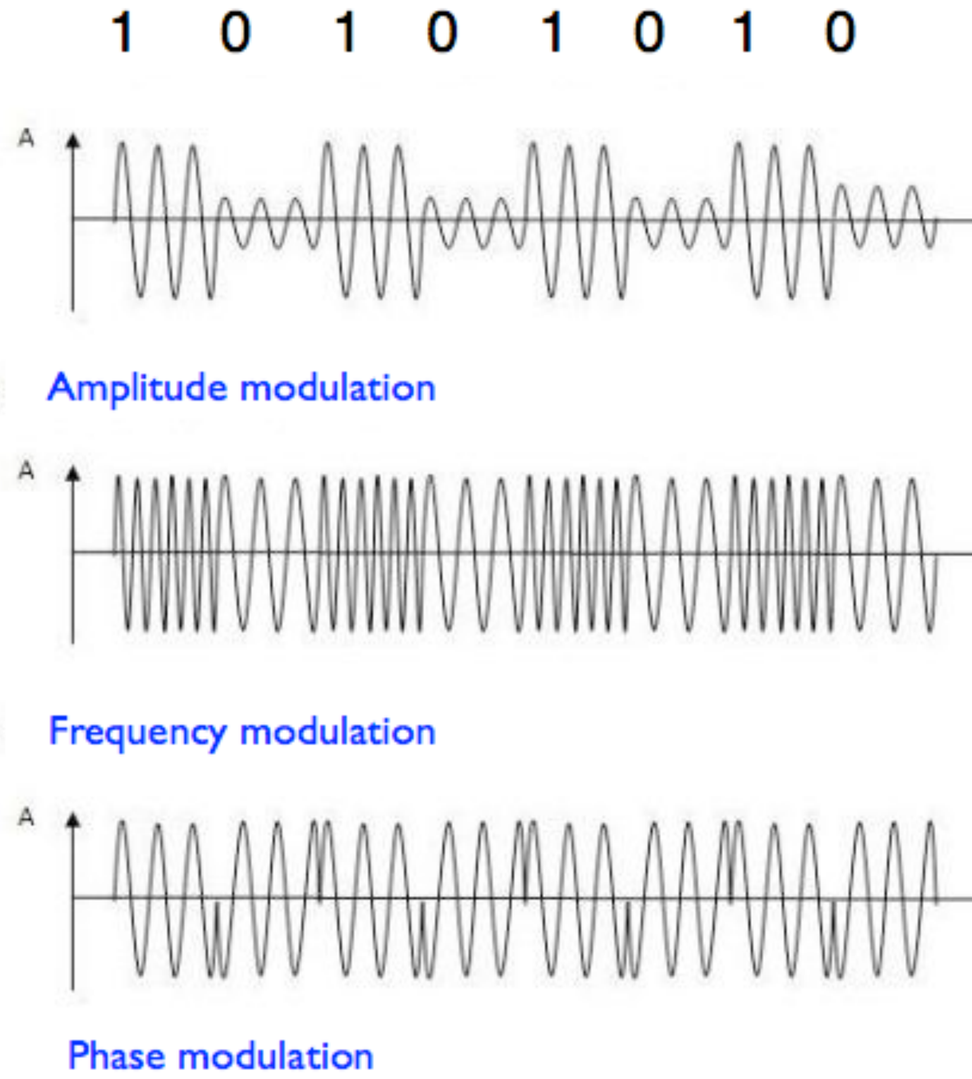
Bastille.net

Manipulating RF

- Done with a radio
- Hardware defined
  - RF and protocol **in silicon**
- **Software Defined Radio** (**SDR**)
  - Flexible silicon handles RF
  - Protocol-specific components implemented **in software** (CPU or FPGA)

PHY Components

- Modulation
  - How digital values are mapped to RF energy
- RF parameters that can be modulated:
  - Amplitude
  - Frequency
  - Phase
  - some combination of the above



Bastille.net

http://xenon.colorado.edu/spotlight/kb/gps_basics/modulations.001.png

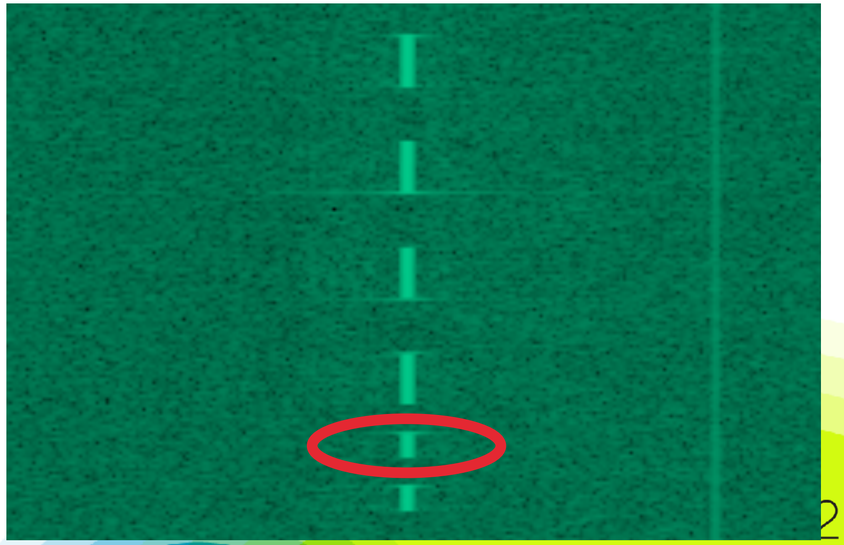
Modulation

- Modulators can modulate analog or digital information
- Digital modulation
  - **Symbols**: discrete RF energy state representing some quantity of information

Symbols Illustrated

- Top: FSK
- Bottom: OOK/ASK

- Compare with analog modulation
  - Analog = infinite precision
  - Digital = finite number of possible symbols, defined by modulation

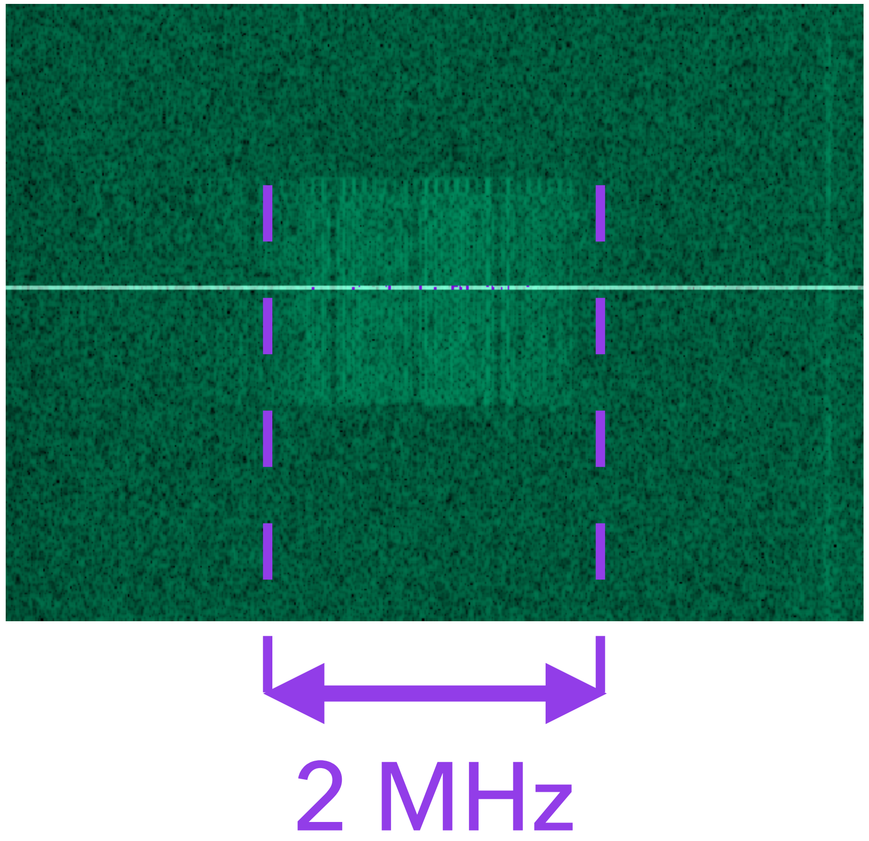


Bastille.net

http://3.bp.blogspot.com/-w66qwKucSJI/UgWKKmPUP2I/AAAAAAAADYA/B9NMGYzqJVk/s1600/Screenshot-2013-08-03-04-41-52.png

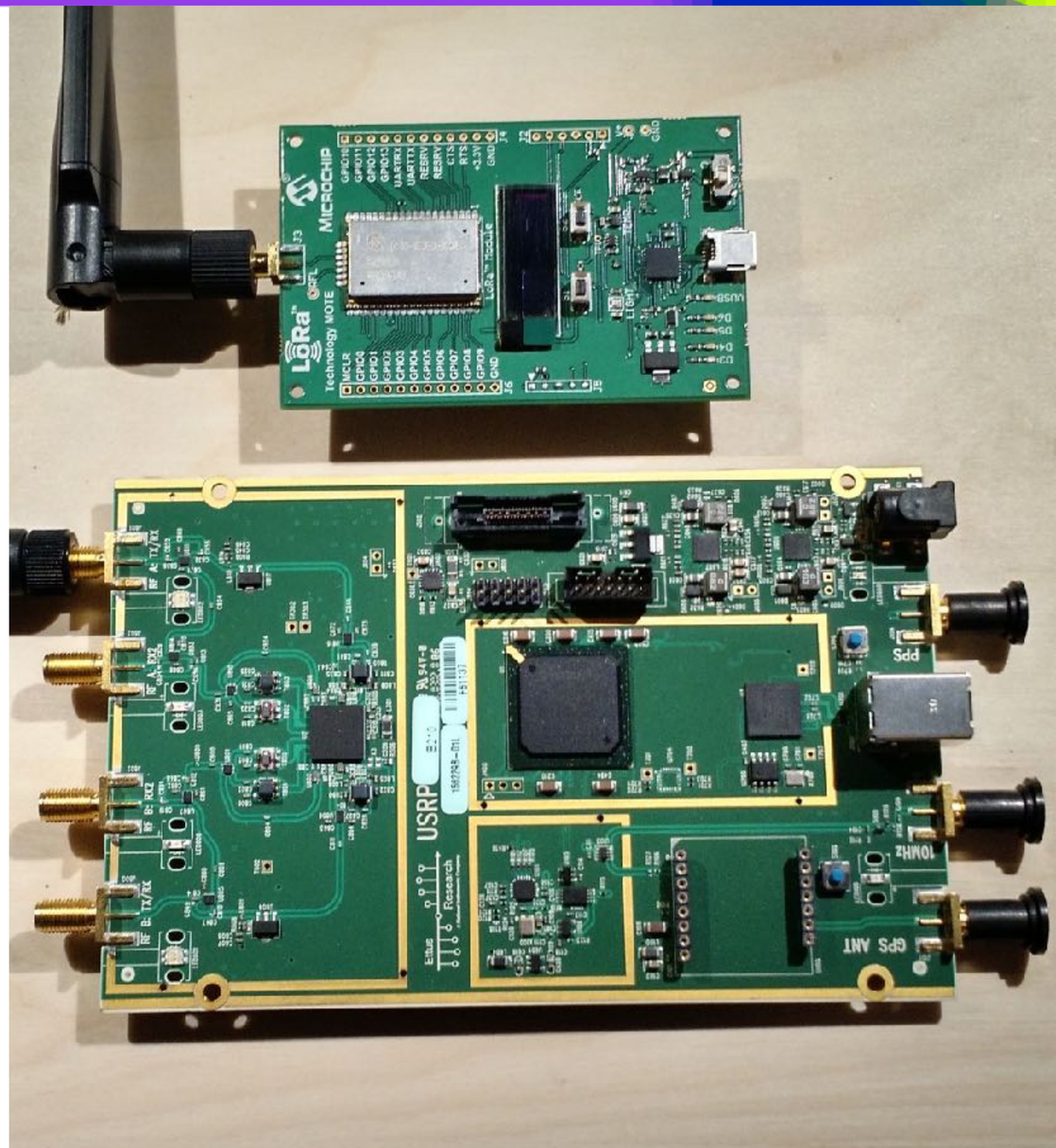
More Complicated IoT PHYs

- Spread spectrum
  - Data bits are encoded at a higher rate and occupy more spectrum
  - **Resilient** to RF noise
- Example: 802.15.4



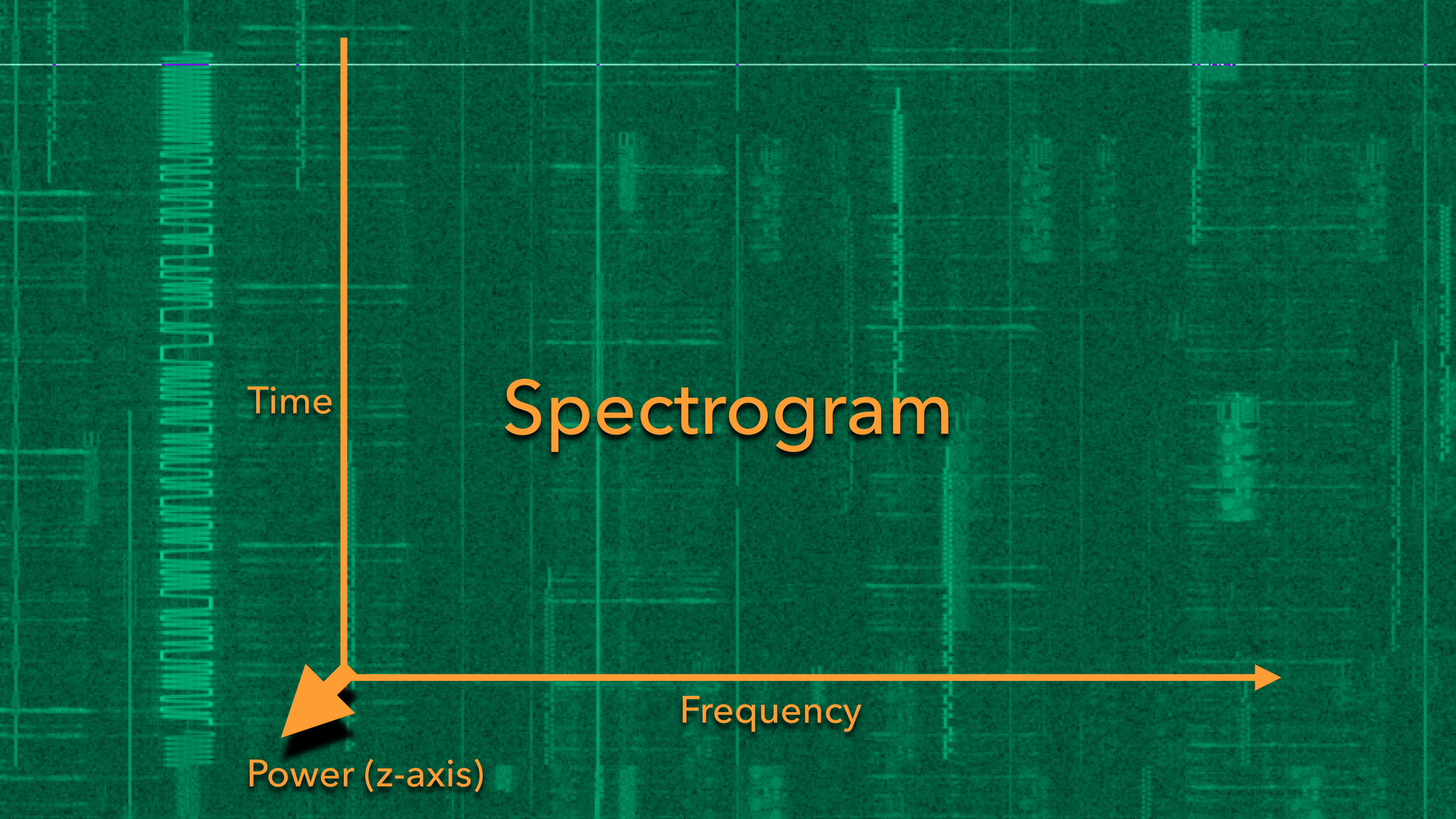
Tools Used in this Talk

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



Last thing… FFT

- Fast Fourier Transform
- Decomposes a signal into its **component frequencies**
  - Any periodic signal can be modeled as the sum of harmonic sine waves
  - FFT figures out which frequencies are present
- Allows analysis and visualization of frequency domain


Spectrogram
Time
Frequency
Power (z-axis)

RSAConference2017

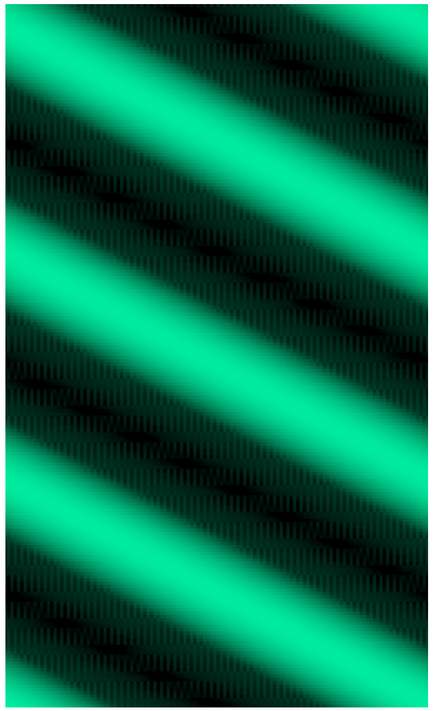
LoRa

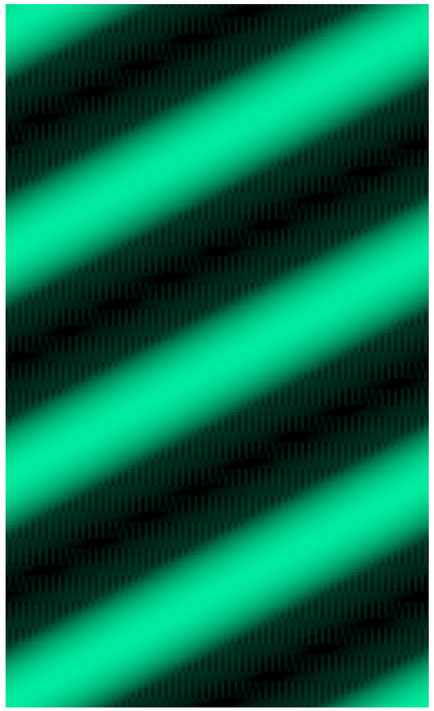
Technical Details

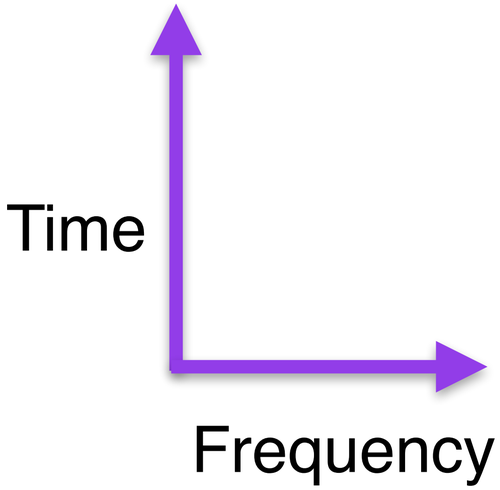
LoRa's Proprietary PHY

- 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
  - Increasing frequency
- Downchirp
  - Decreasing frequency

CSS Advantages

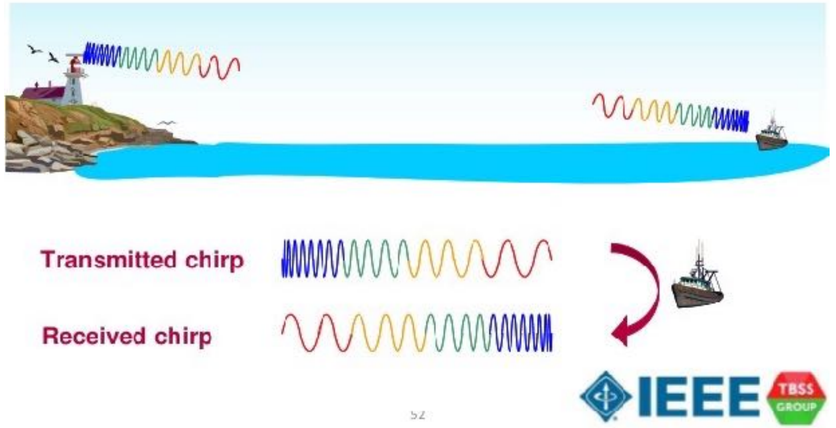
- Great link budget
  - **Resilience** to interference
  - Performance at **low power**
- Resistant to:
  - Multi-path (urban applications)
  - Doppler effect (mobile applications)

Interesting set of pros… where else are chirps used?

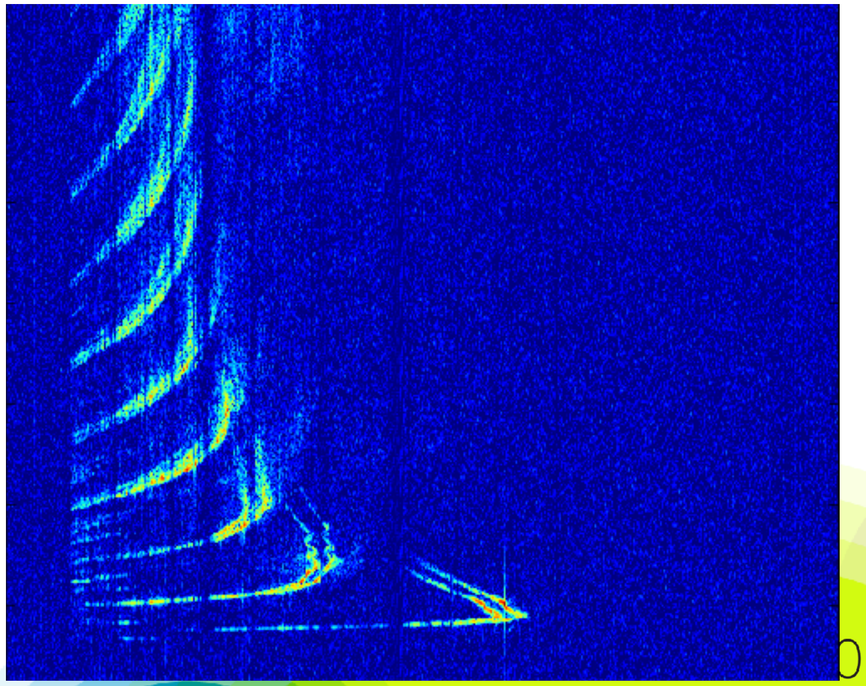
RADAR

Chirps in RADAR

- Military and marine radars
  - Wideband and pulse compression



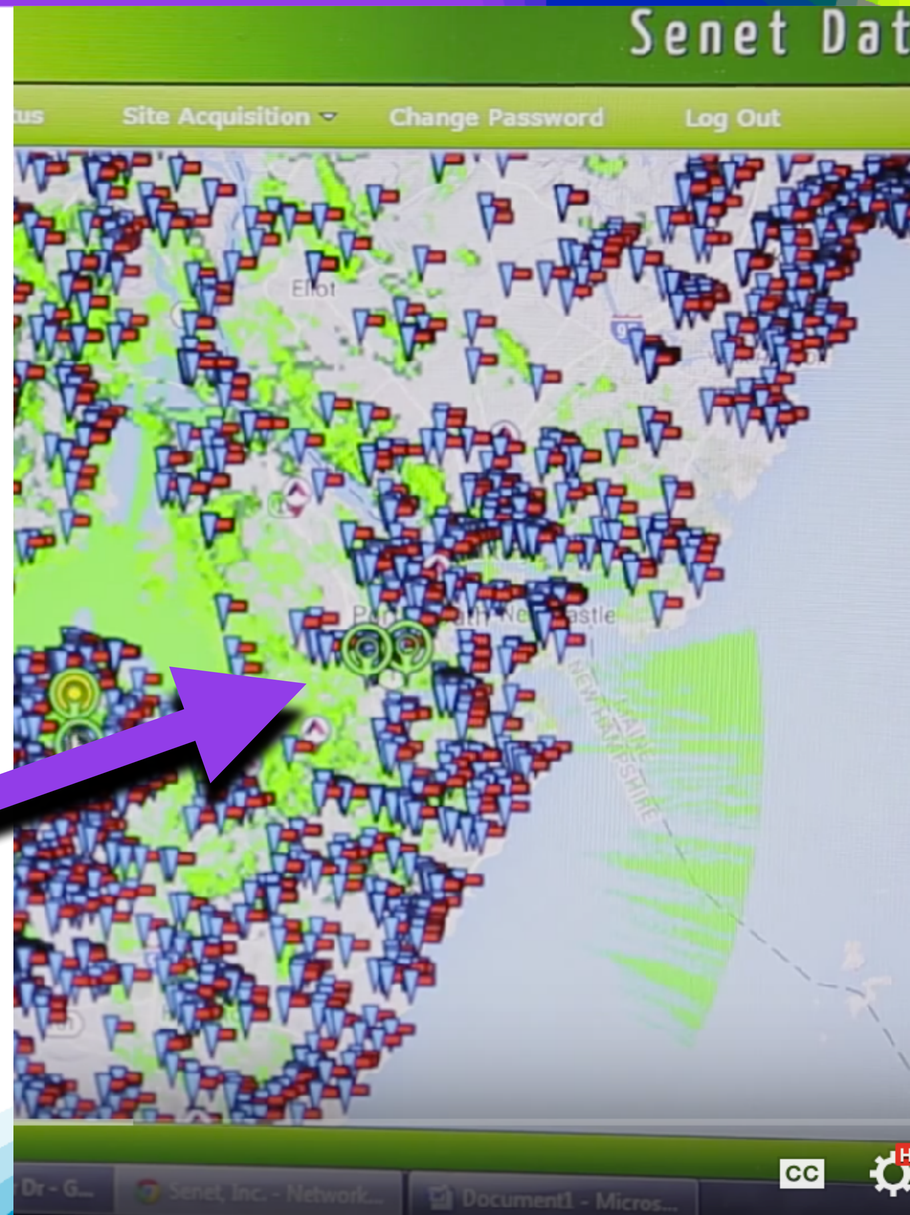
- Open source GNU Chirp Sounder
  - Ionospheric radars
  - Space weather



Seeking LoRa

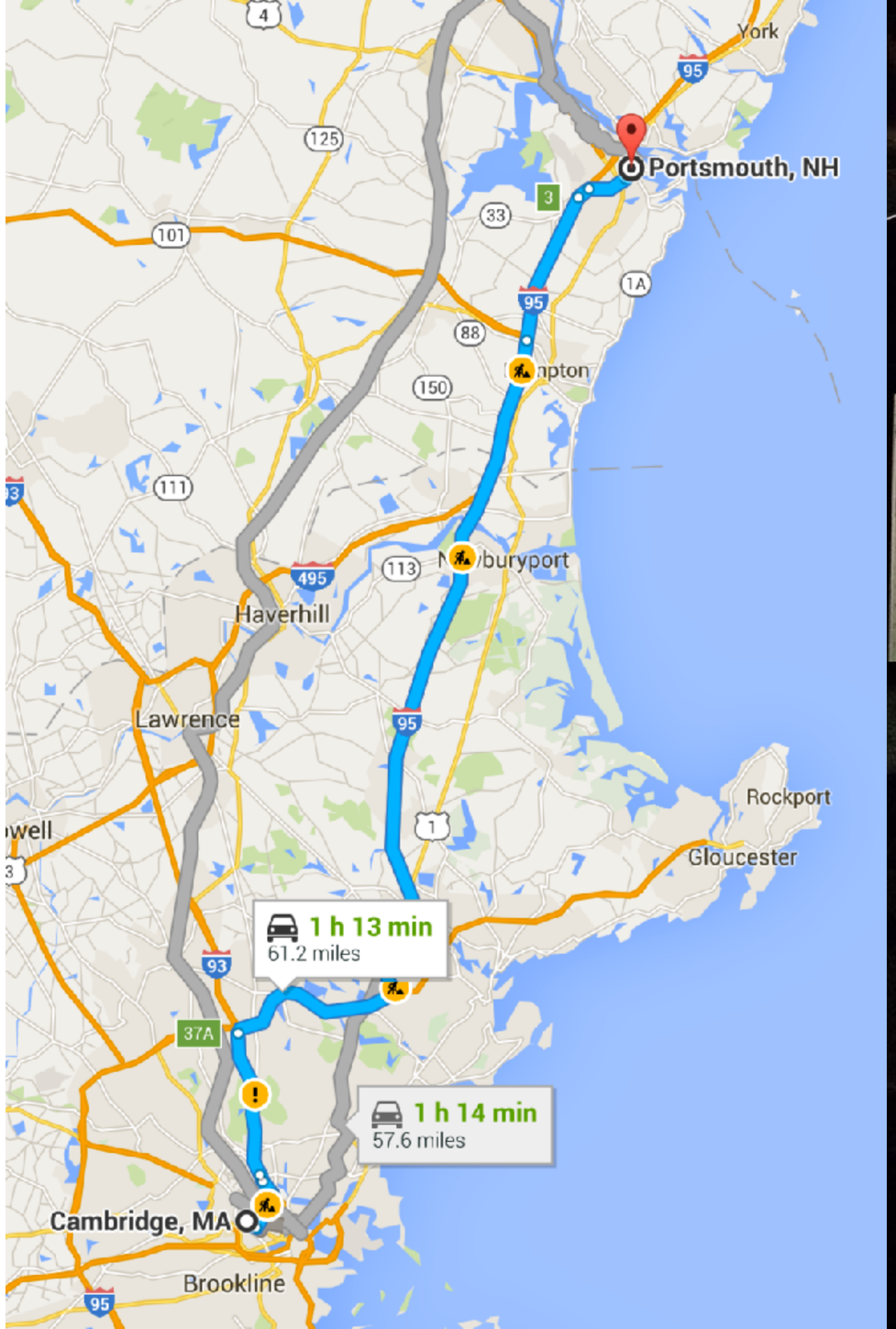
- December 2015: No LoRa sightings in major US cities
- I encountered **Senet** at a Meetup event in Cambridge, MA
- While watching one of their marketing videos…

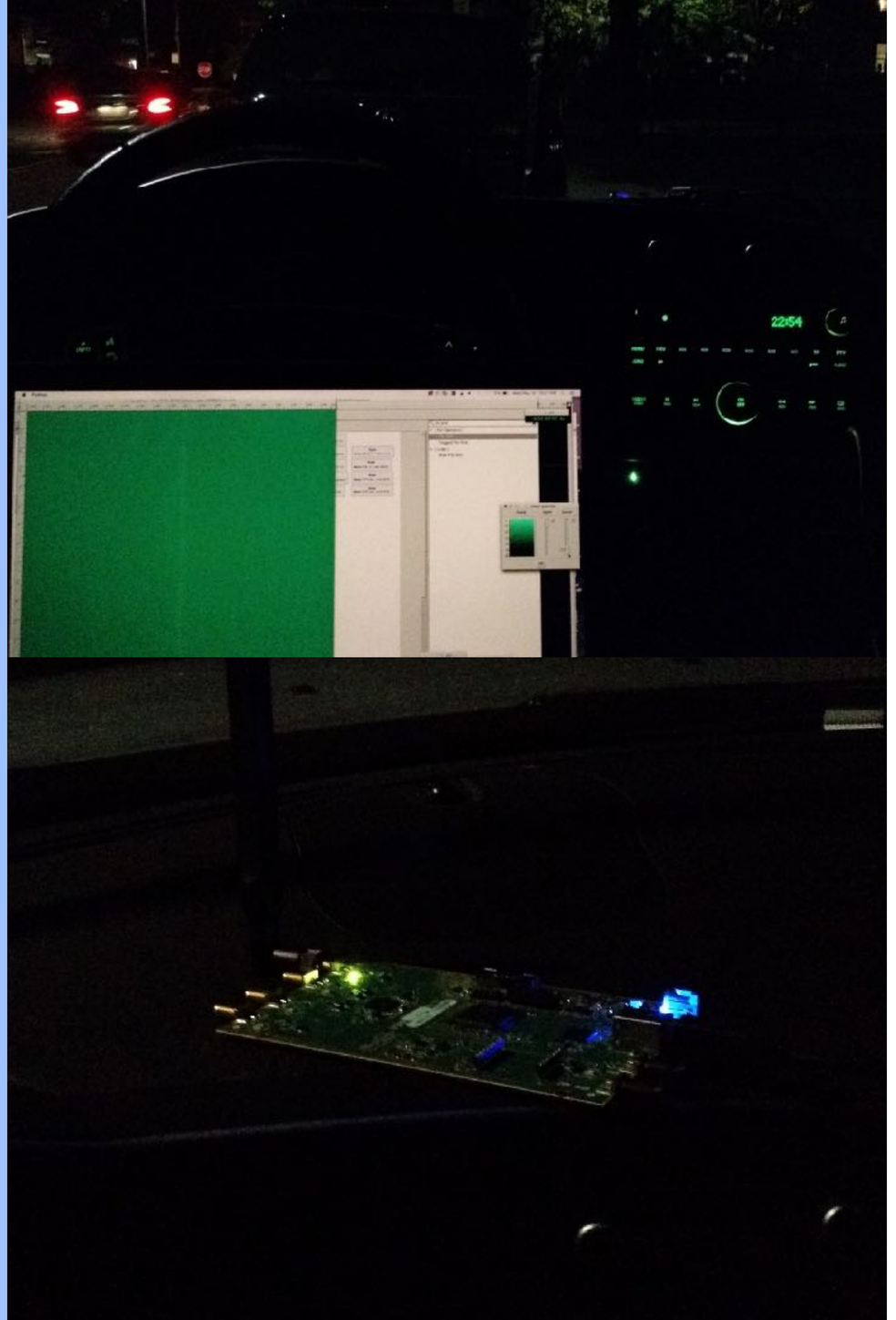
Portsmouth, NH!

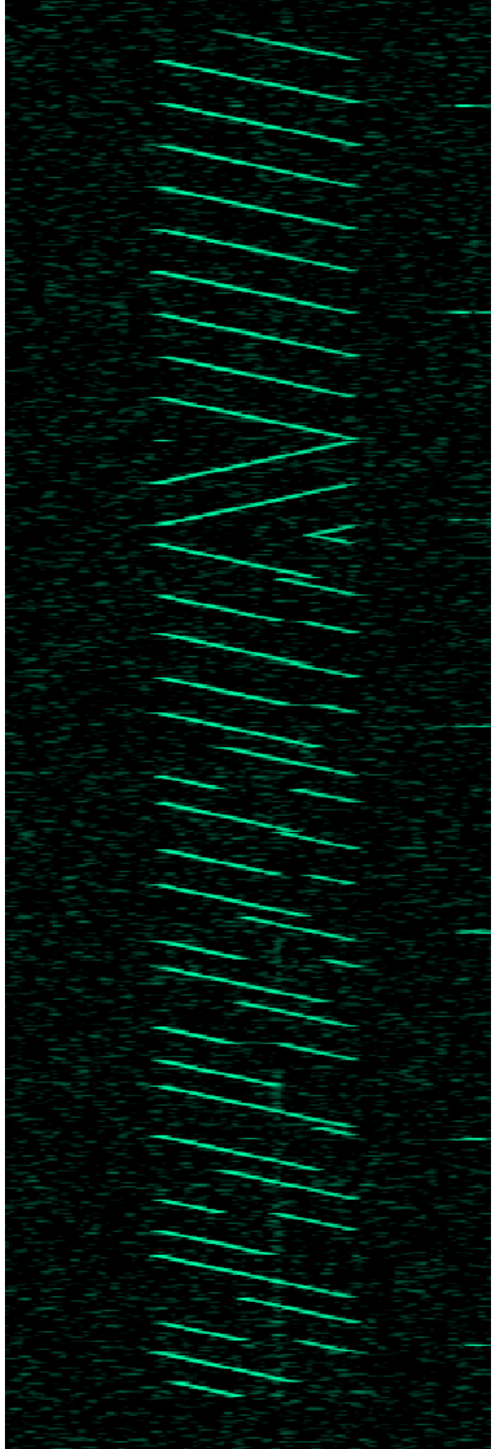


Bastille.net

ROAD TRIP

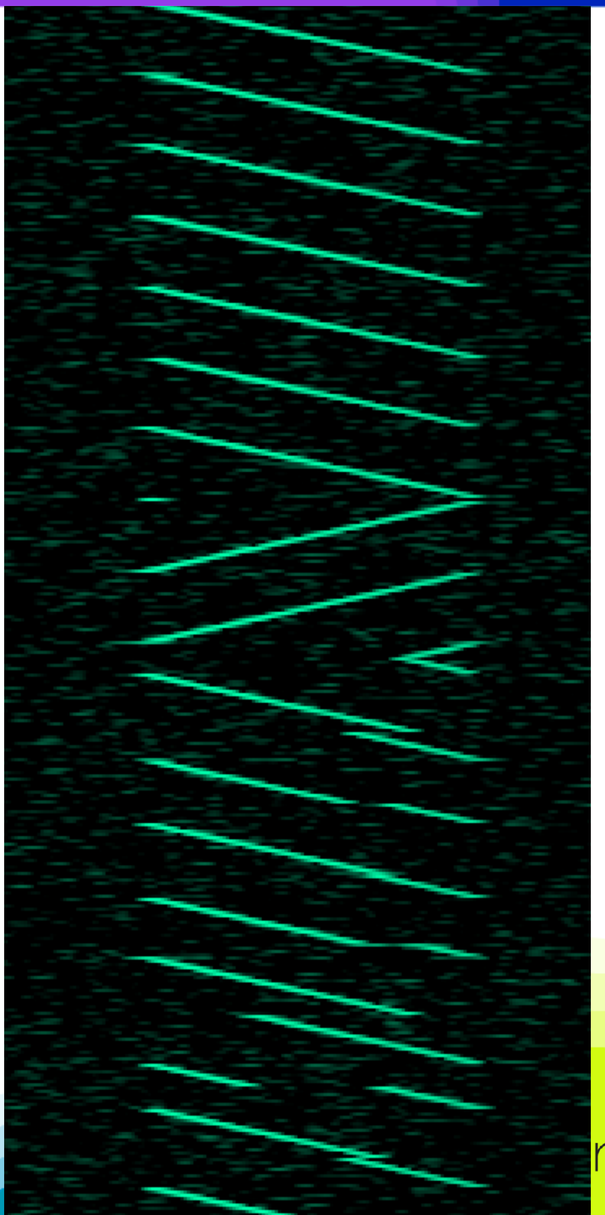

York
Portsmouth, NH
Haverhill
Lawrence
Rockport
Gloucester
1 h 13 min
61.2 miles
1 h 14 min
57.6 miles
Cambridge, MA
Brookline





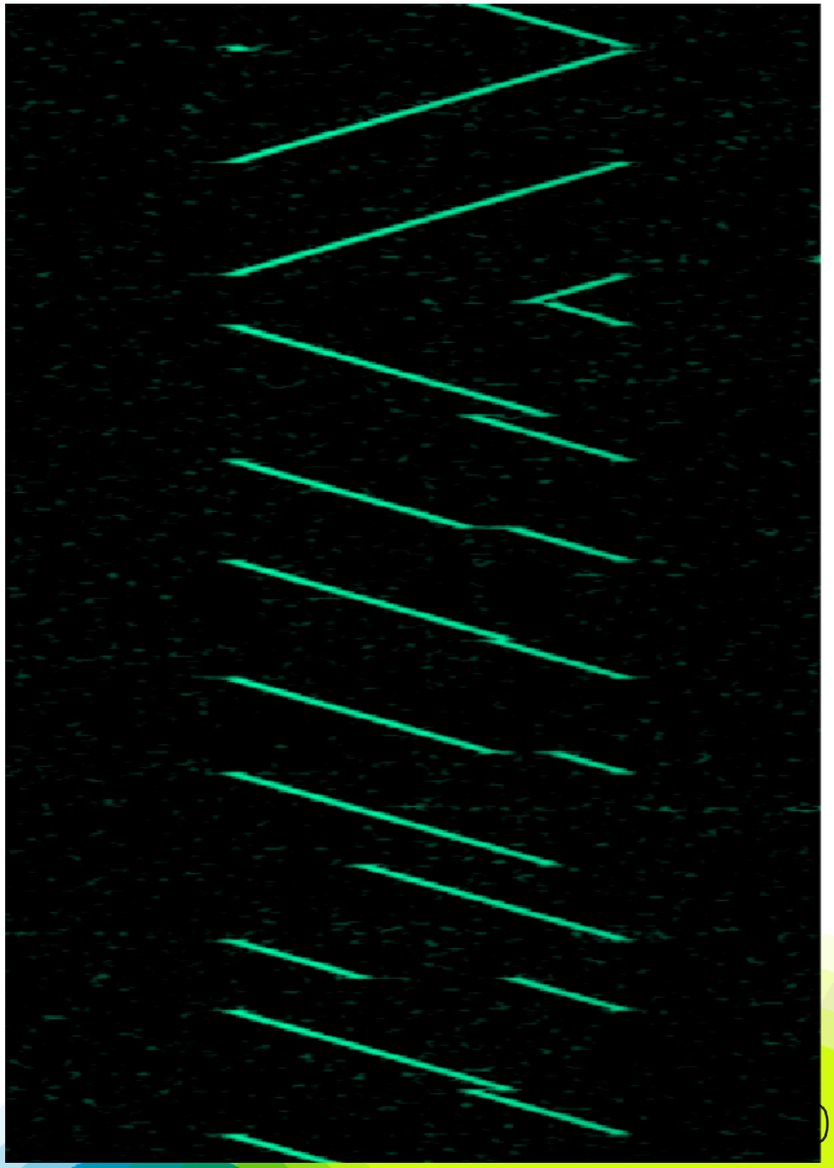
Examining the Lora PHY Frame

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



PHY Data Unit Structure

- Chirp frequency is static
- Chirp “jumps” throughout band
- **Instantaneous frequency changes** are result of data being modulated onto the chirps
  - Chirp **“phase”**



Bastille.net

RSAConference2017

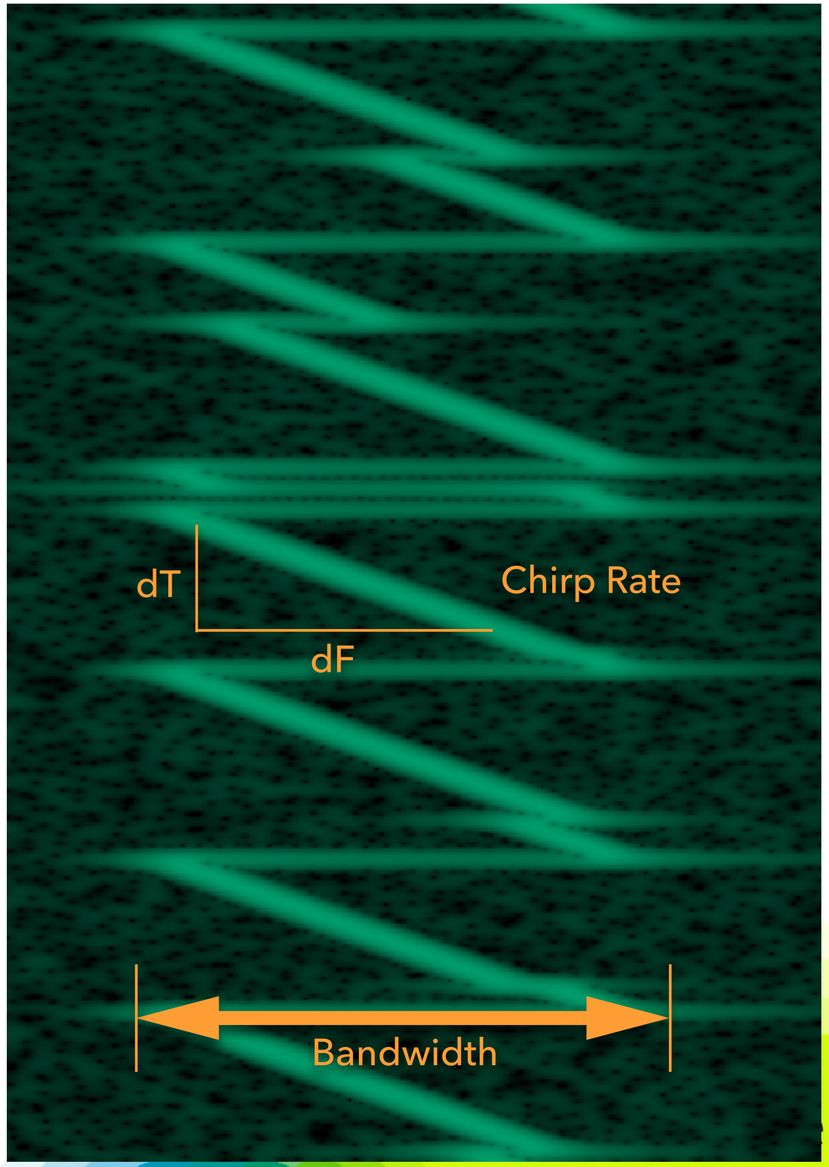
Demodulating LoRa

Before we get started… OSINT

- Technical documentation
  - Semtech European **patent application** 13154071.8
  - LoRa Alliance LoRaWAN spec (**MAC/NWK only**, not a PHY spec)
  - Semtech **app notes** AN1200.18 and AN1200.22
- Prior art
  - Partial implementation in open source rtl-sdrangelove
  - Observations at https://revspace.nl/DecodingLora

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

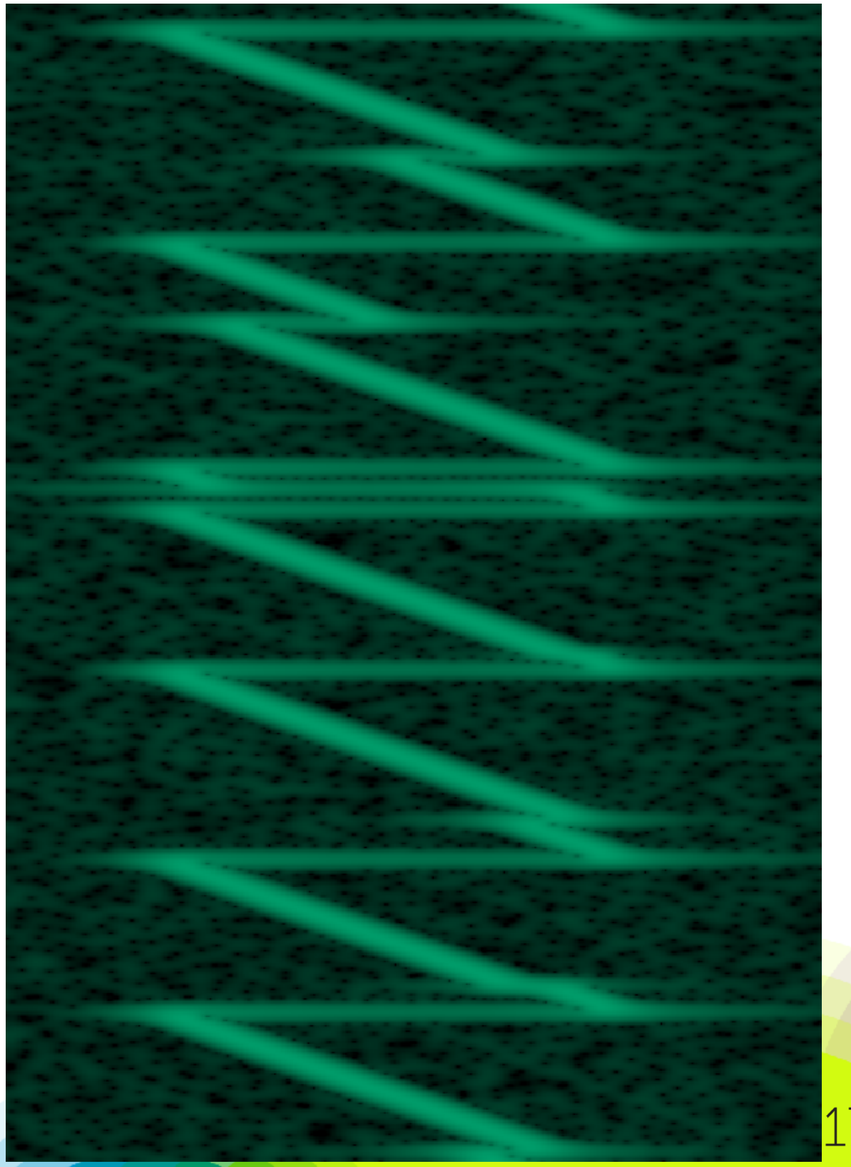


Some numbers…

- **Bandwidth**: width of spectrum occupied by chirp → US: 125, 250, 500 kHz
- **Spreading factor**: number of bits encoded per symbol (RF state, remember?) → US: [7-12] bits per symbol
- **Chirp rate**: first derivative of chirp frequency → bandwidth/(2**spreading_factor)

So what's a **symbol**?

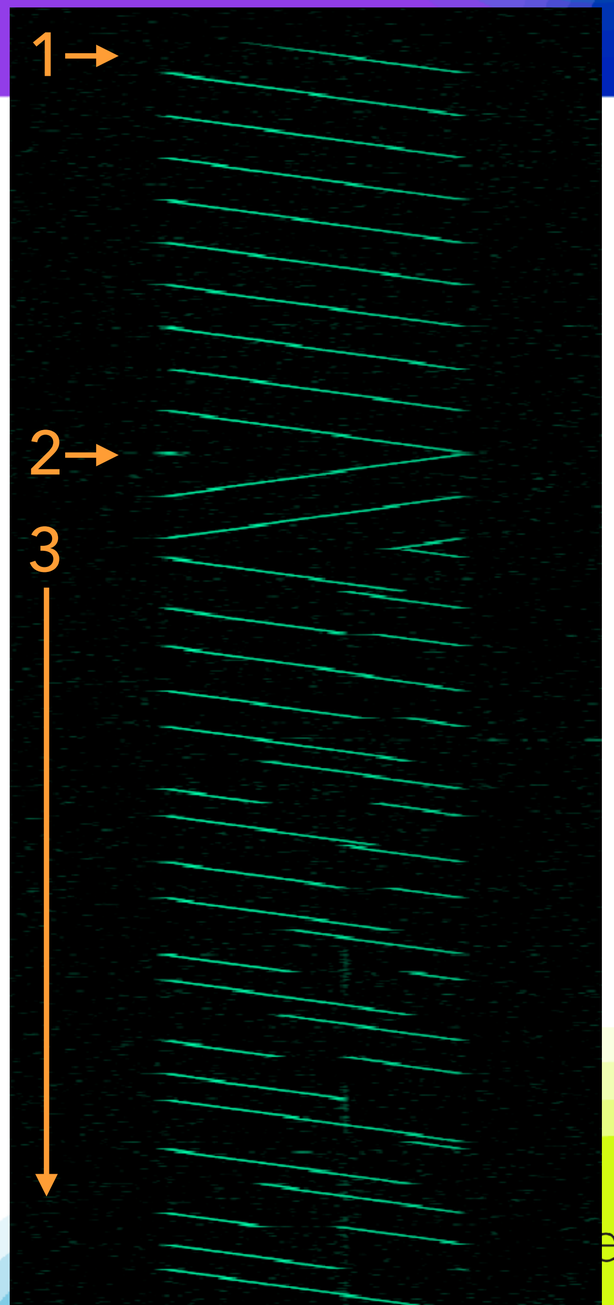
- Instantaneous change in frequency
- **FM modulated chirps**



Demodulating the PHY

- Identify the beginning of a frame
- Find the beginning of the PHY data unit
- Extract data from instantaneous frequency transitions

- **How?** We need to **quantify** the frequency transitions



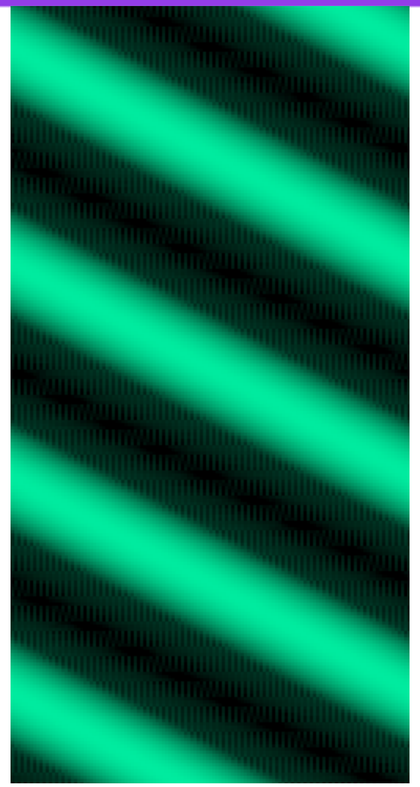
Bastille.net

MATH

$$f_0 * f_1 = f_0 + f_1$$

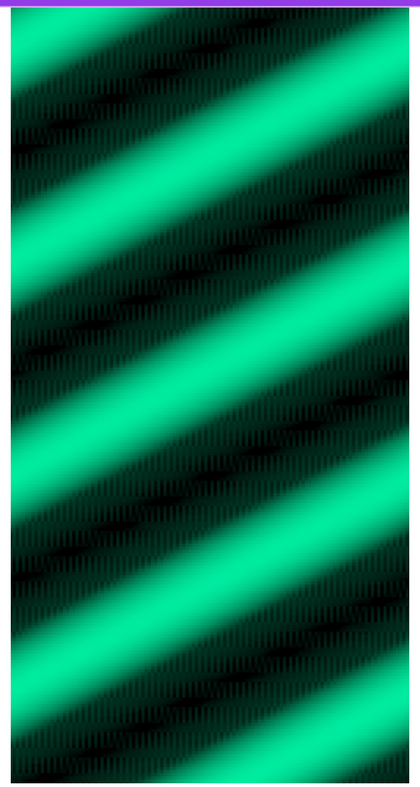
$$f_0 * -f_0 = 0$$

(complex conjugate)



Upchirp

*

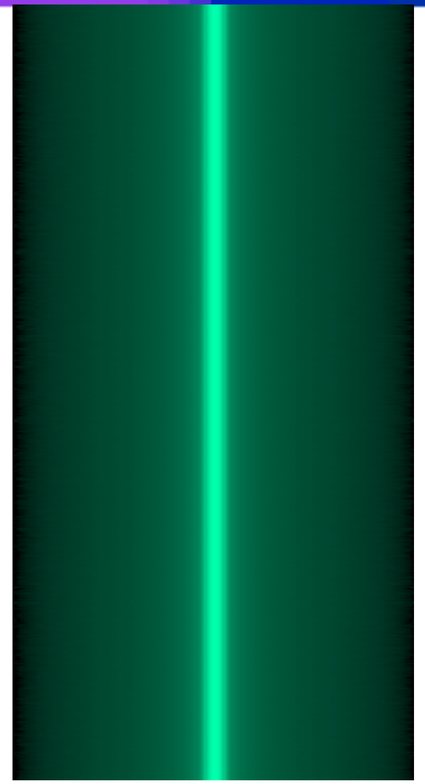


Downchirp

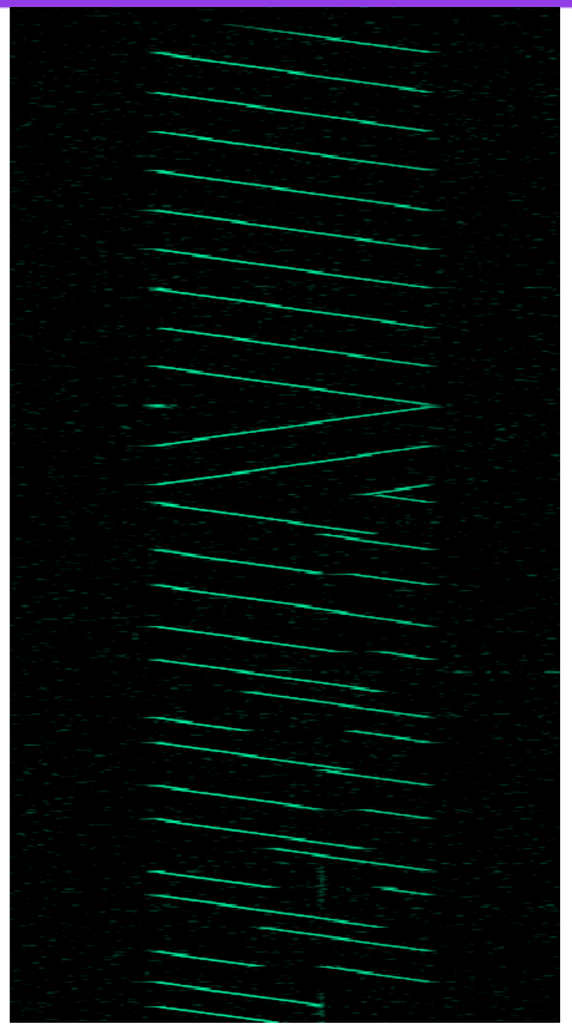
=

Why not necessarily DC?

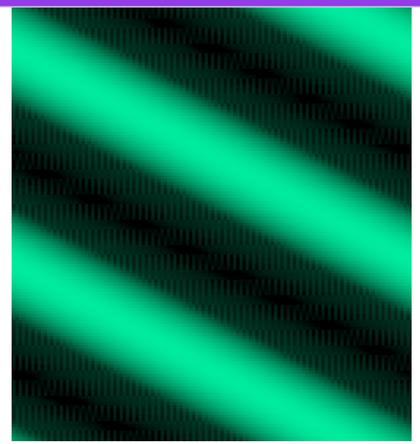
Chirp phase!



Constant Frequency



*

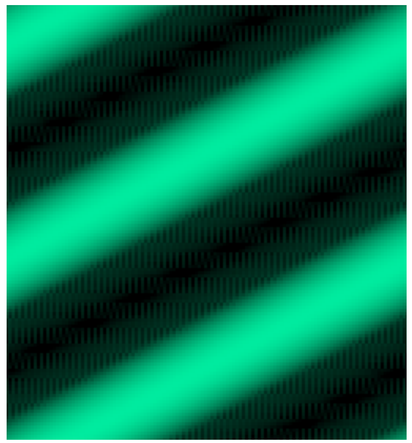


Upchirp

=

??

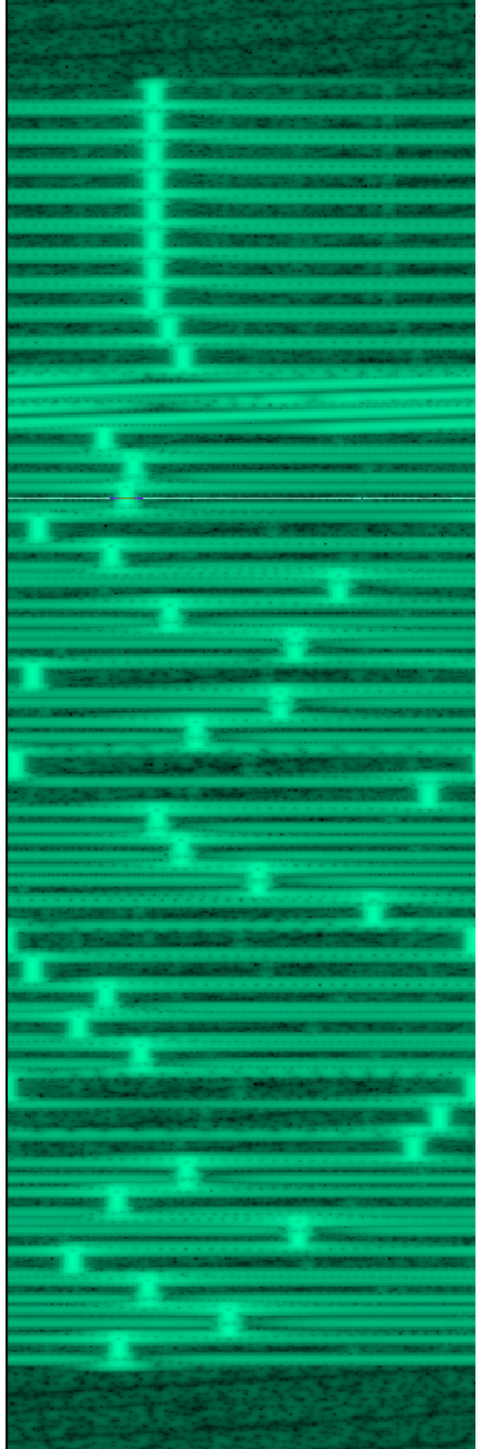
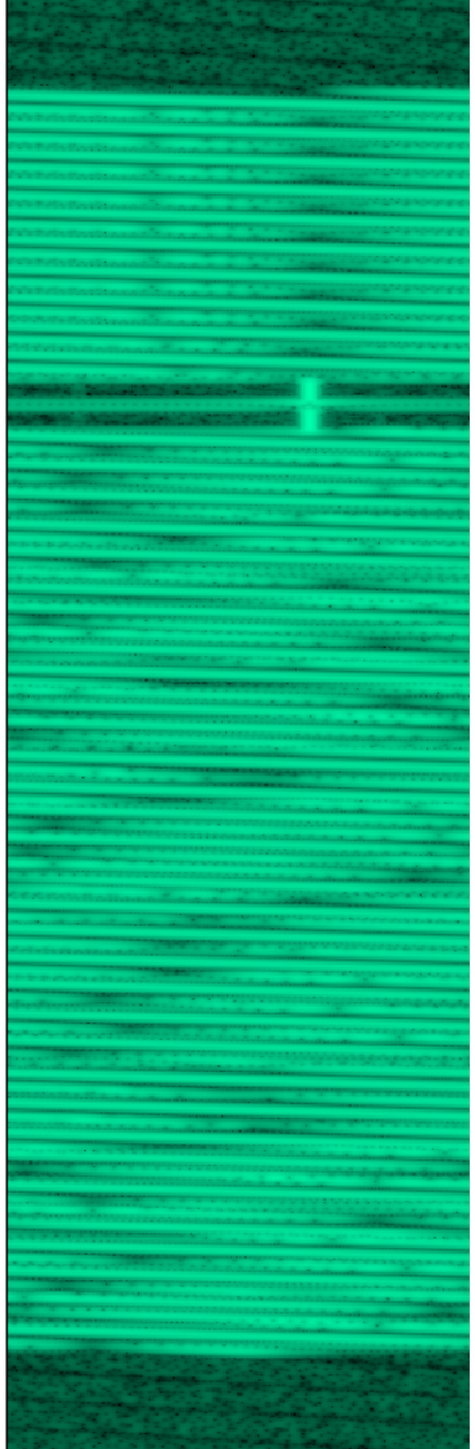
*



Downchirp

=

??

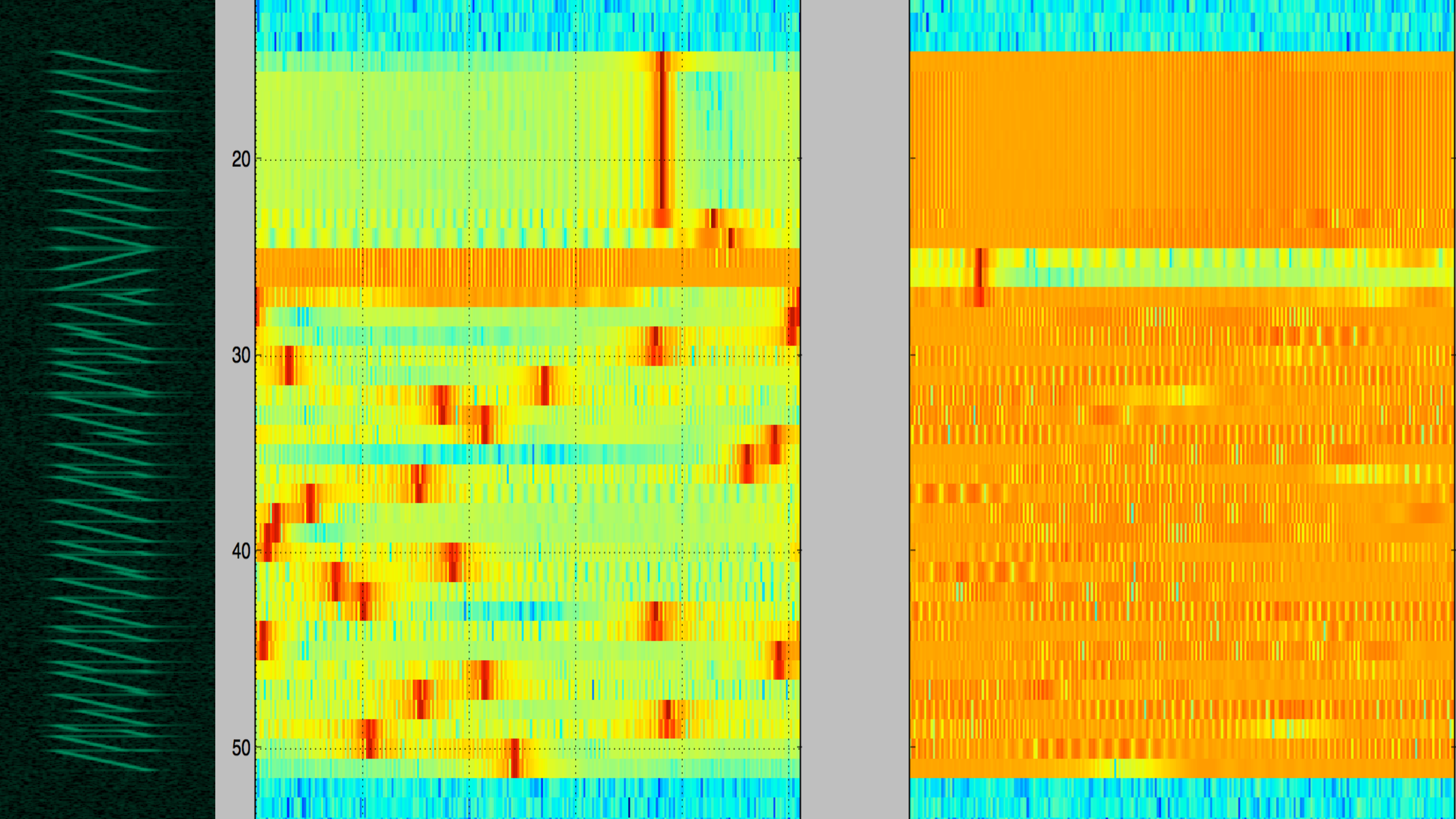
Remember Symbols?

- Symbol: RF **state** representing some quantity of information
- LoRa spreading factor: **number of bits** encoded into each symbol

- How many **possible symbols** are there?
  - **2**spreading_factor** !!

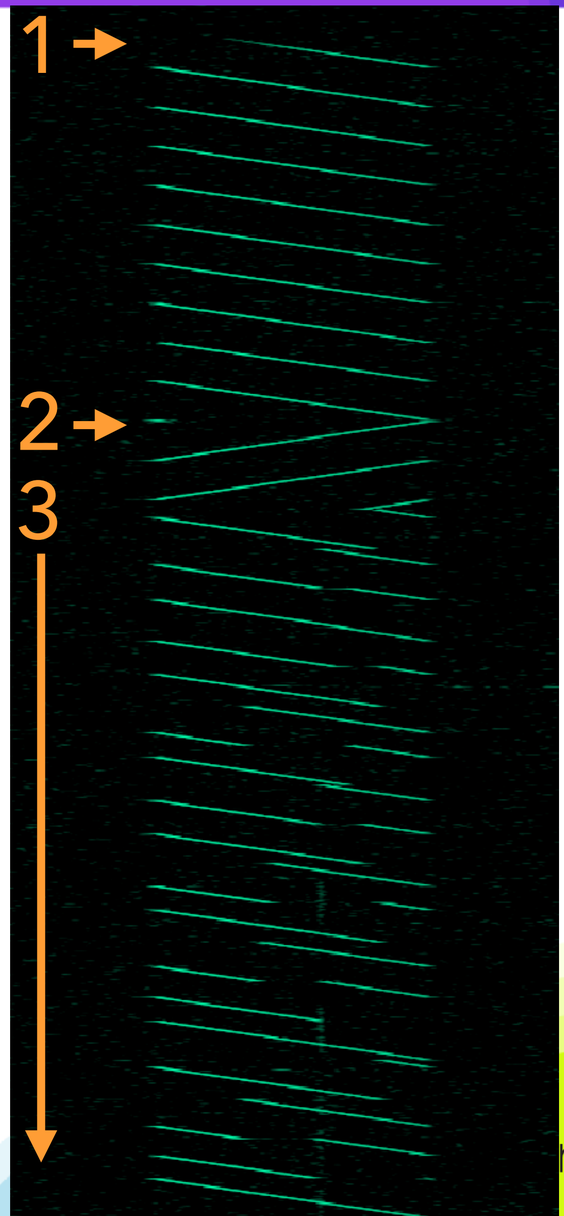
Extracting Symbols

- 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!**


20
30
40
50

Demodulation Summary

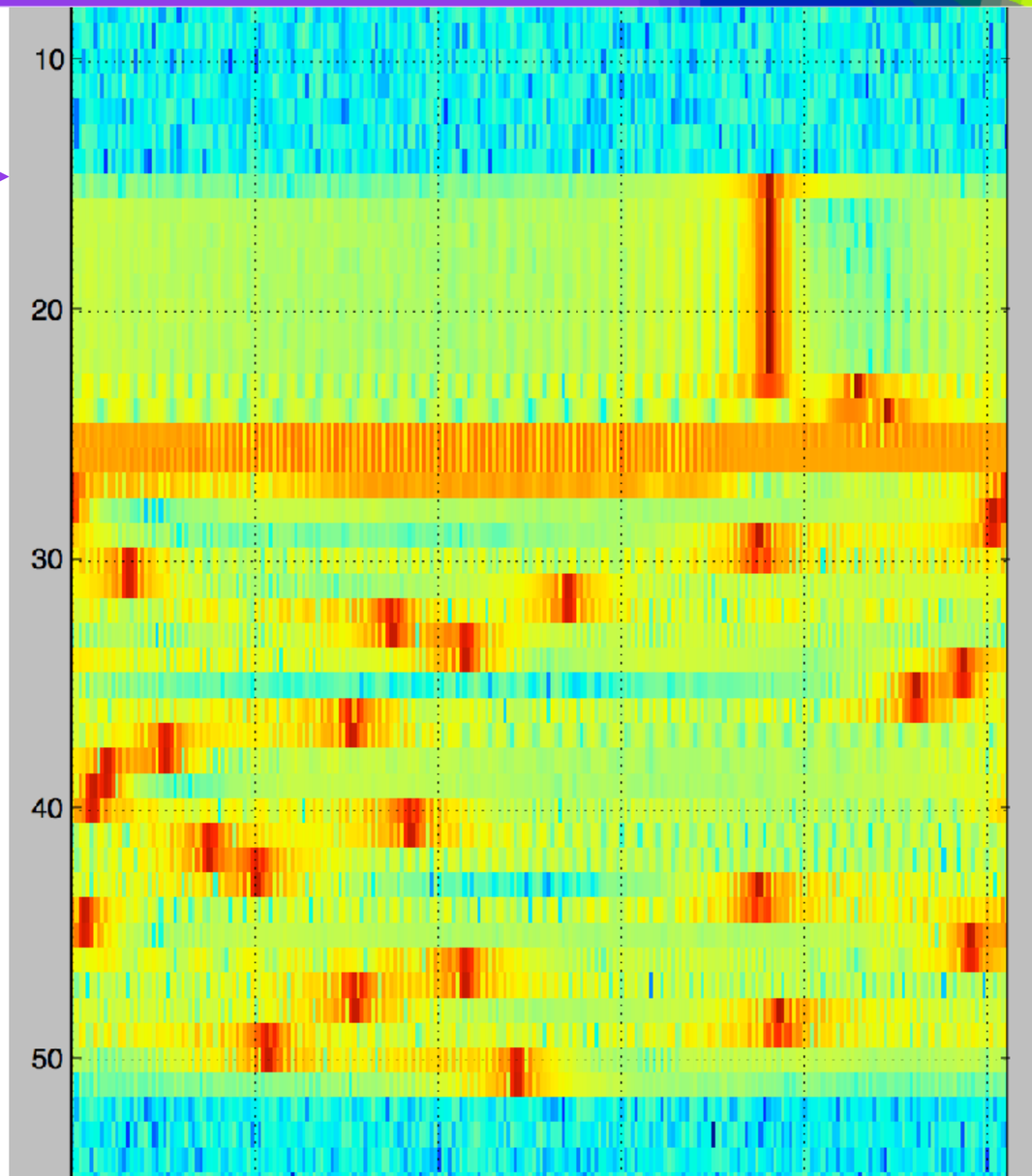
1. Identify the beginning of a **frame**
2. Find the beginning of the **PHY data unit**
3. Extract data from **instantaneous frequency transitions**



Demodulation Summary (1/3)

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**

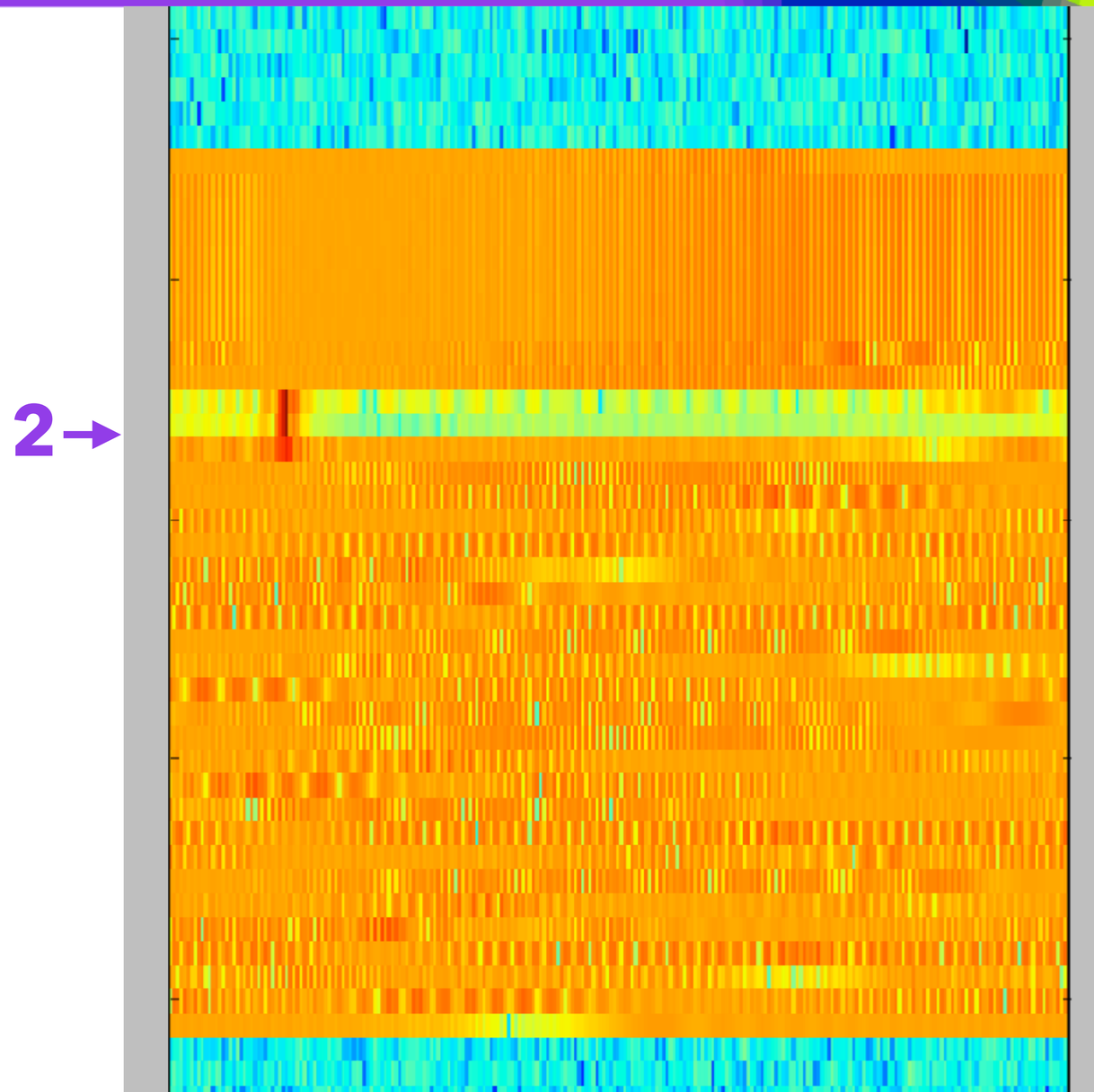


Bastille.net

Demodulation Summary (2/3)

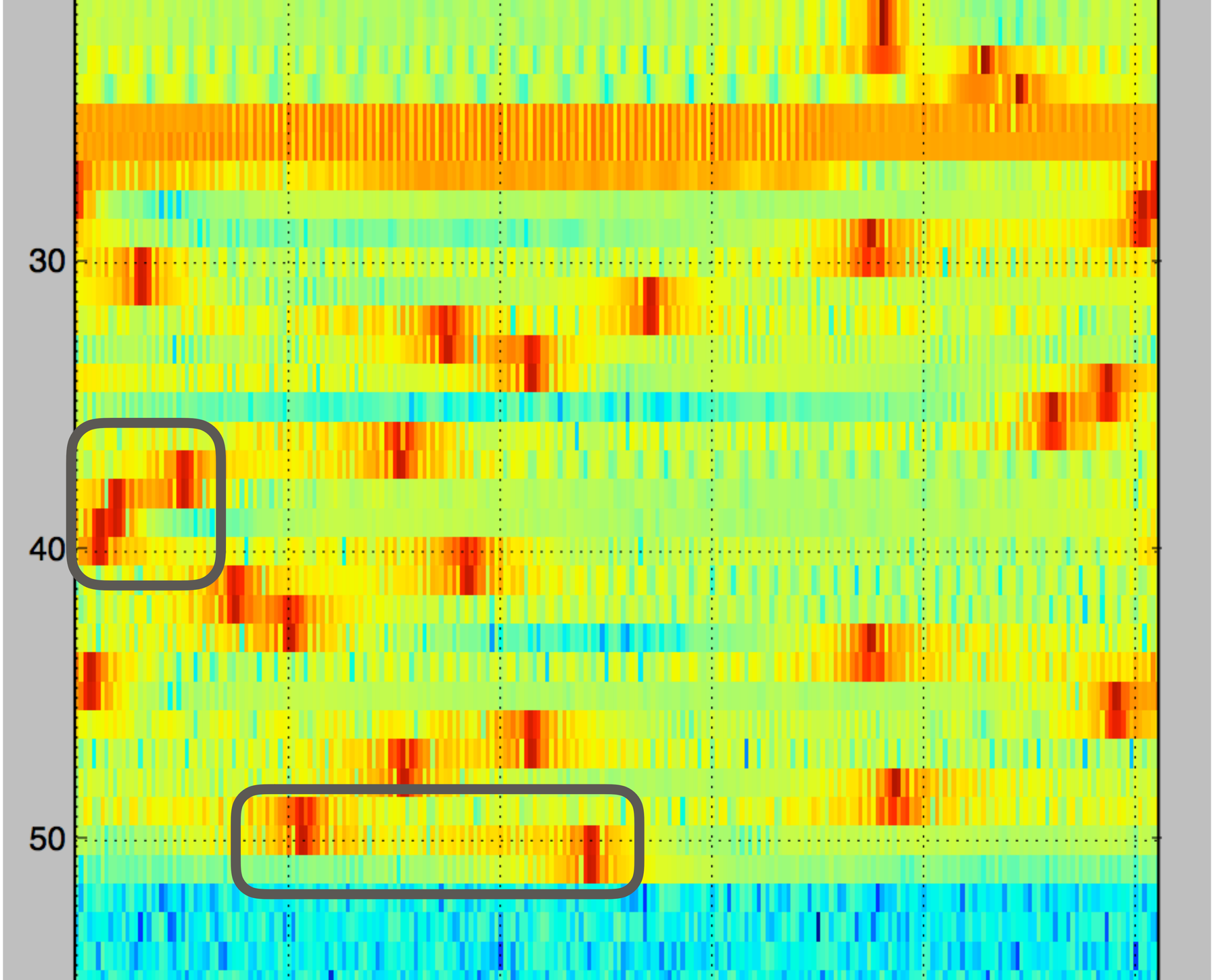
2. Find the beginning of the PHY data unit

- Repeat same process looking for SFD down-chirps
- Down-chirp is complex conjugate of the up-chirp
- PHY data unit begins 2.25 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!**

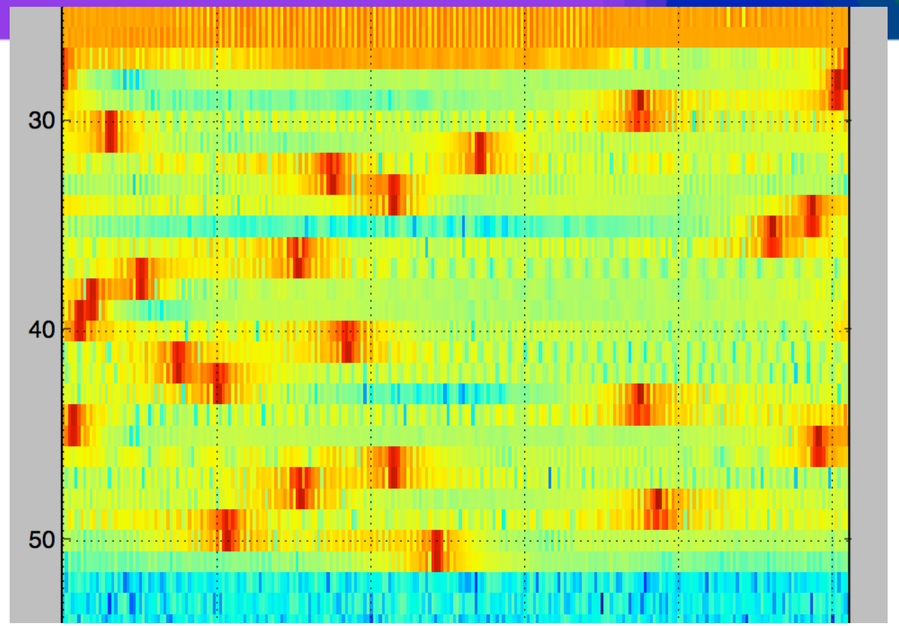

30
40
50

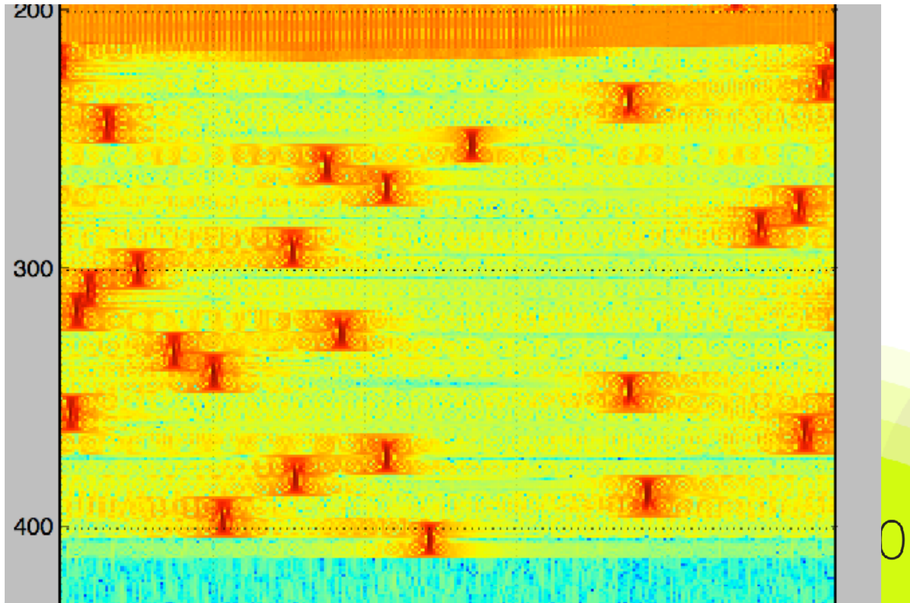
SFD Sync Solution

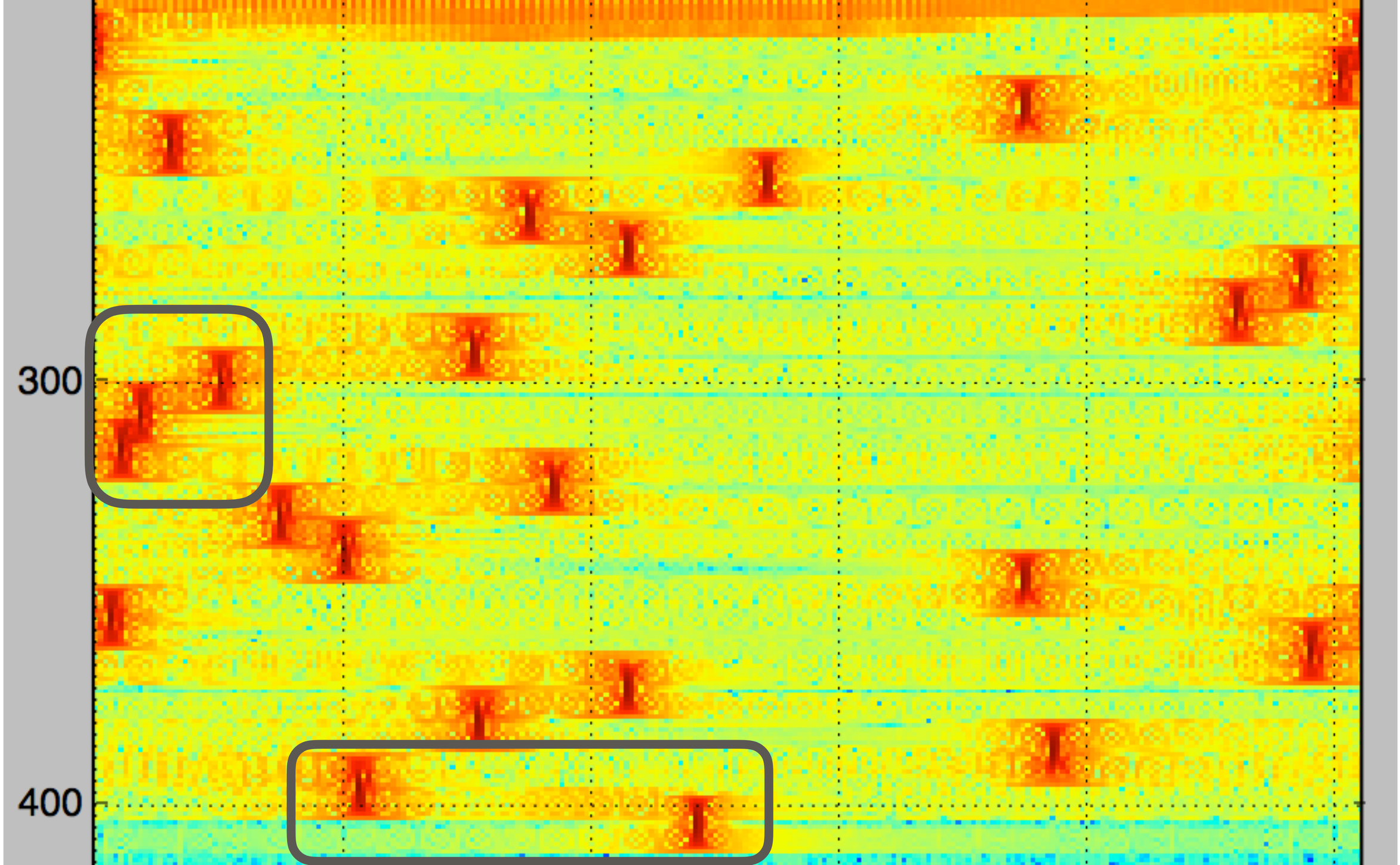
- Increase FFT time-based precision once preamble is found
- **Overlapping FFT** sample buffers!

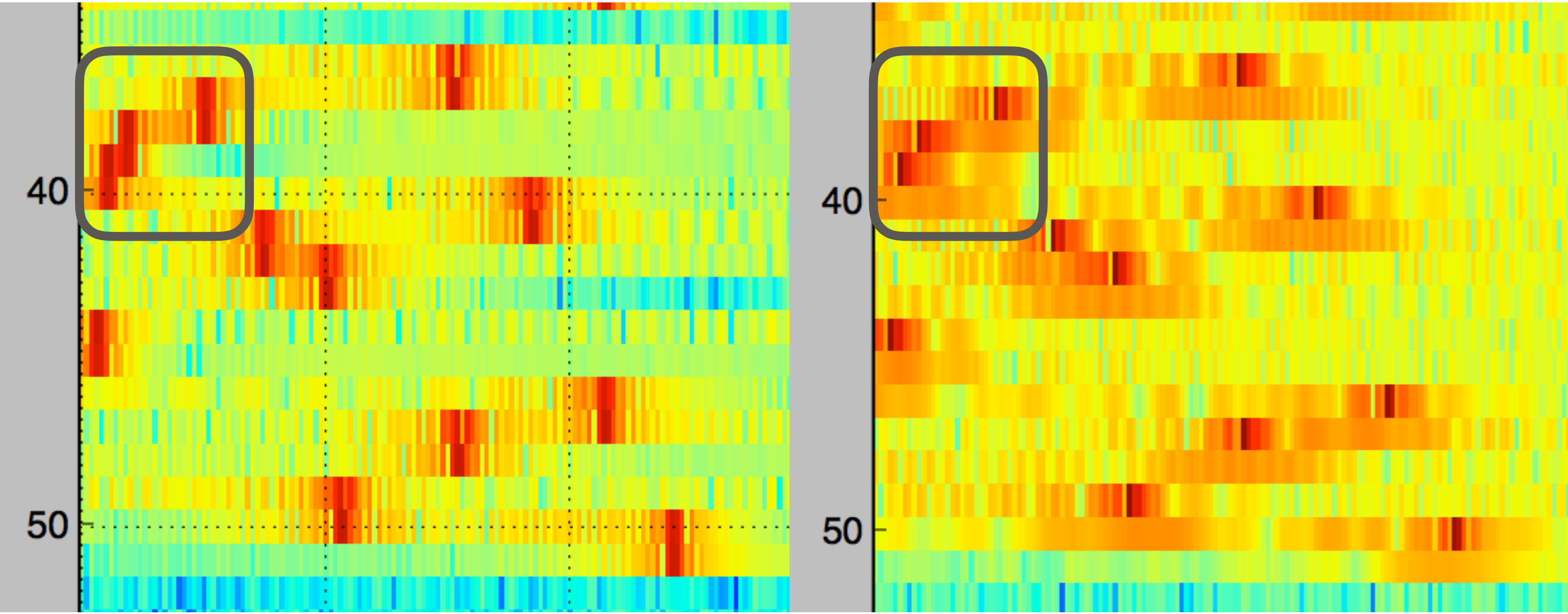
Overlapping FFTs

- Use overlapping FFTs to **synchronize** to first sample in the first SFD symbol



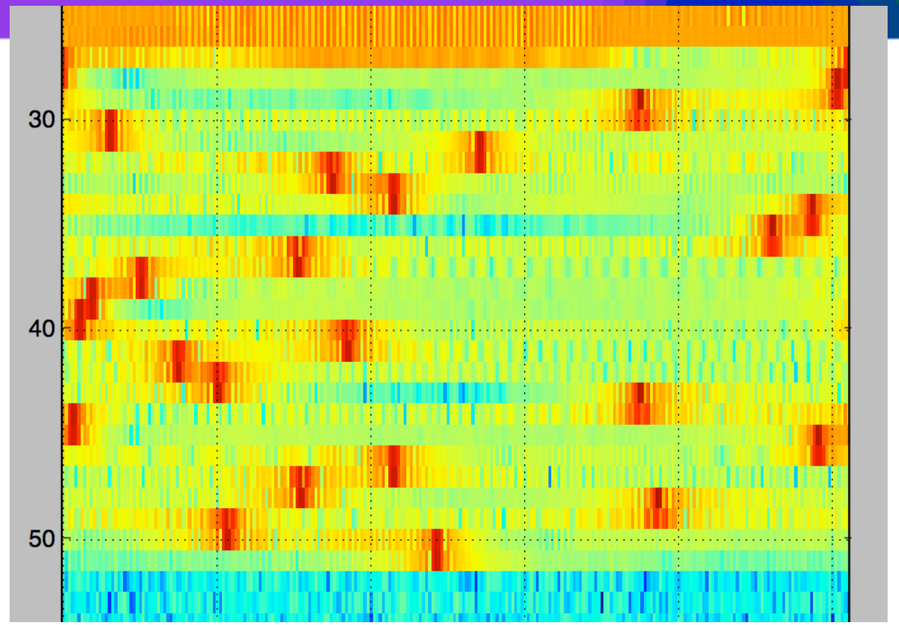



300
400

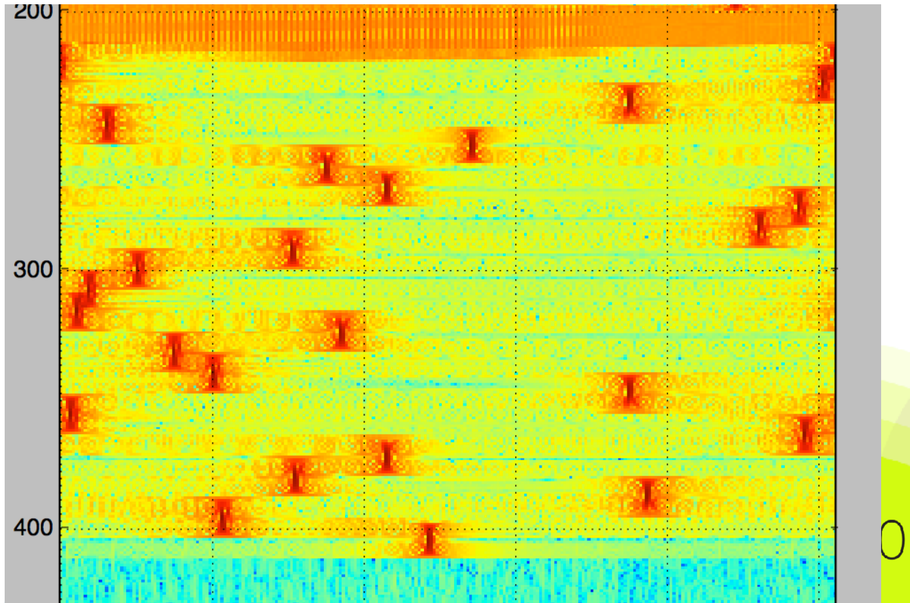

40
50
40
50

Overlapping FFTs

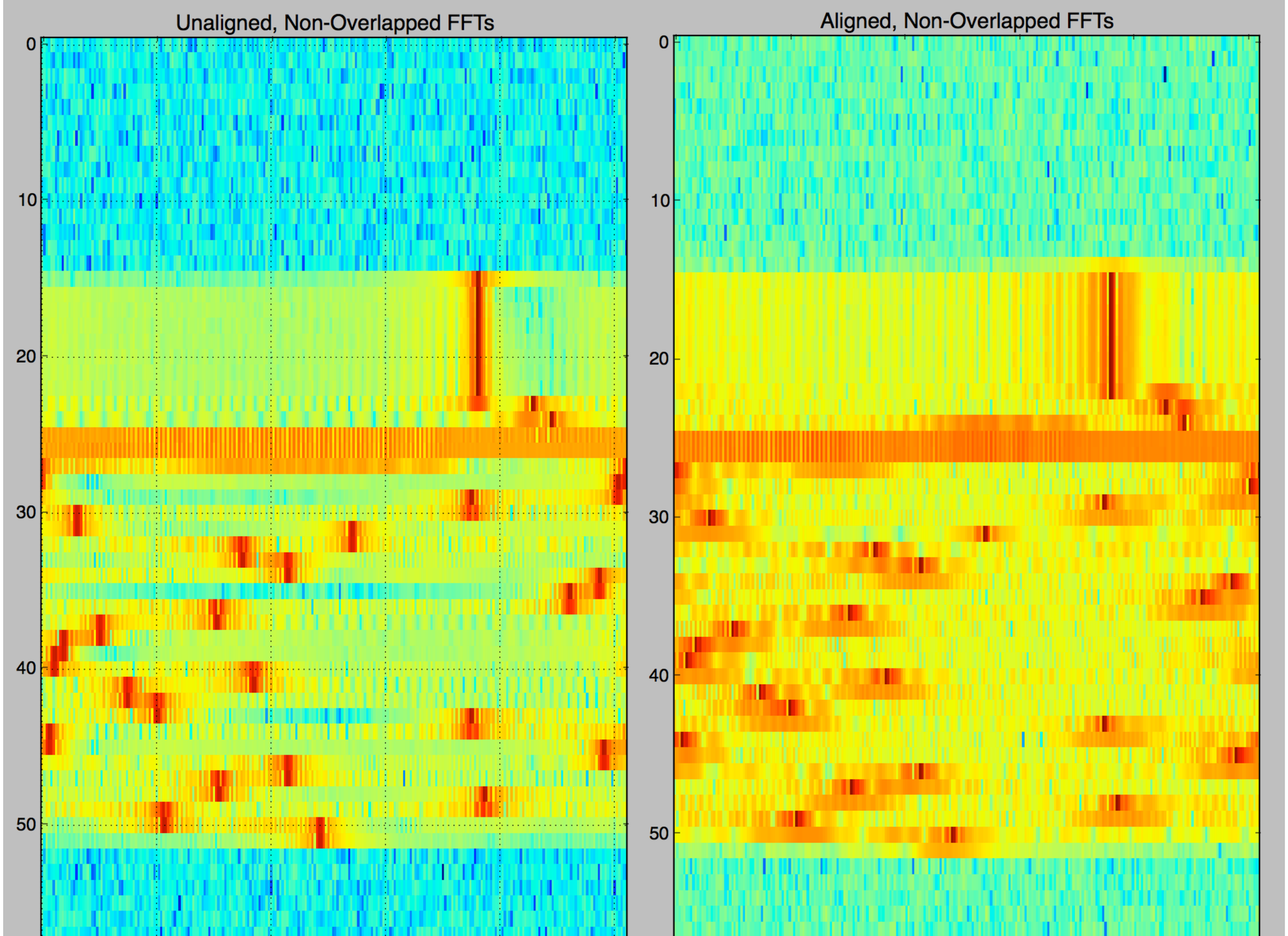
- Use overlapping FFTs to **synchronize** to first sample in the first SFD symbol



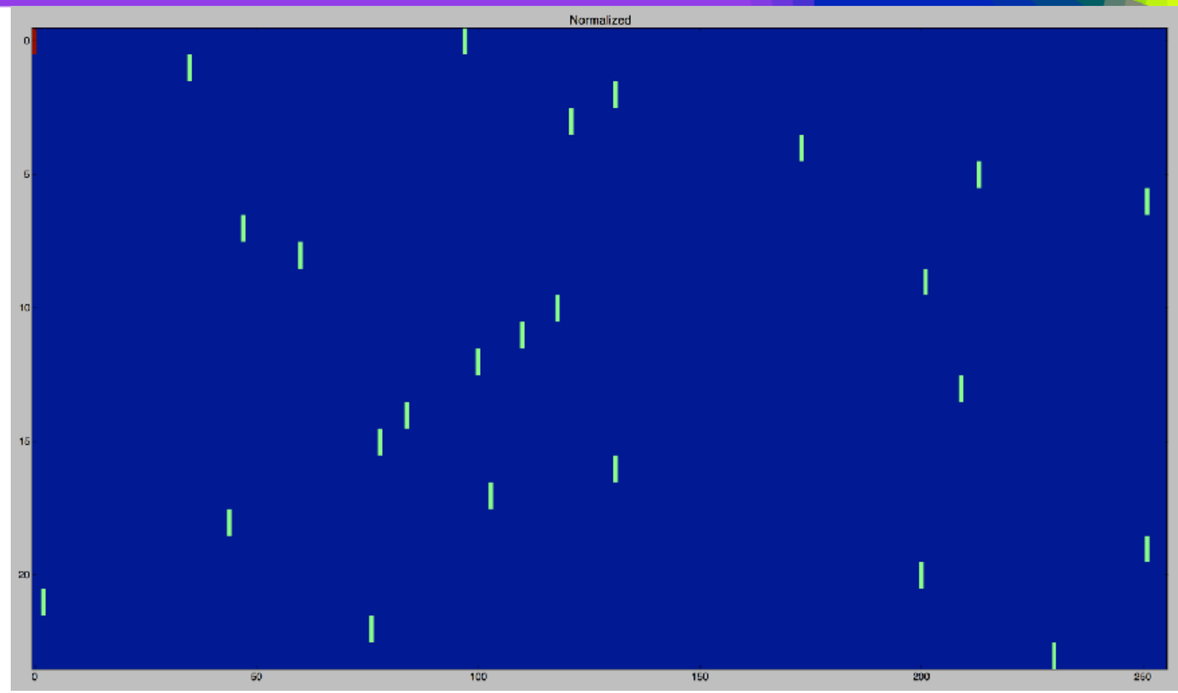
- Re-compute with non-overlapping FFTs to get your data!



Bastille.net


Unaligned, Non-Overlapped FFTs
Aligned, Non-Overlapped FFTs
0
10
20
30
40
50

Demodulation Summary (3/3)



3. Extract data from chirp frequency transitions

- Use described FFT method
- **Normalize** data about the value of the preamble (always value 0)

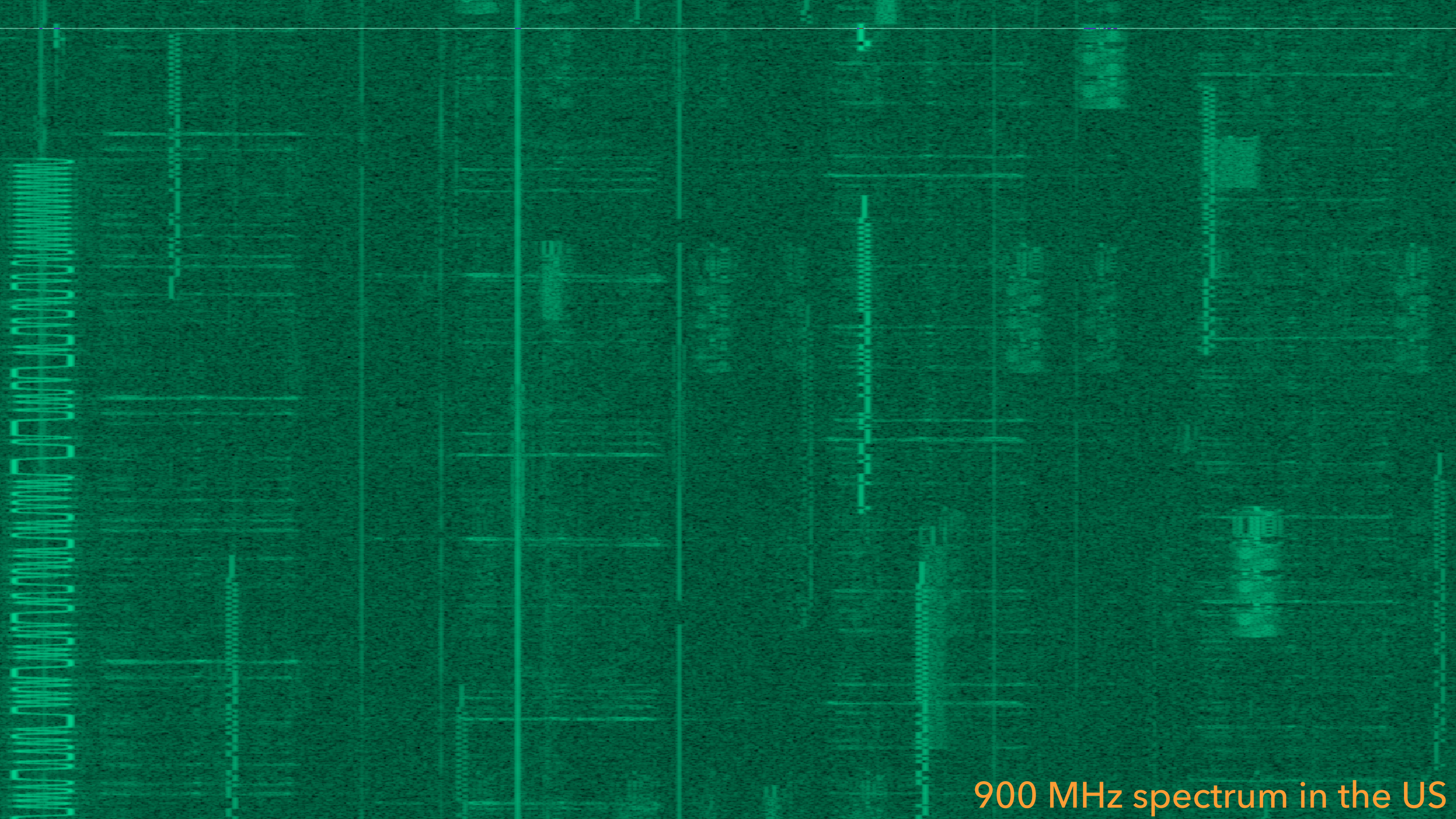
We’re done, right?

lol!

why not?

Data Encoding

- Symbols represent encoded data
  - What?
- Data is **transformed** before it is transmitted
  - Why?
- Encoding increases **OTA resiliency**


900 MHz spectrum in the US

RF is a brutal environment

- All systems see **interference** from weather, geomagnetic activity, etc.
- Some systems have protected/reserved frequencies
- LoRa is ISM — TONS OF CHATTER
  - RF contention/collision is guaranteed

- **Encoding** scrambles and replicates data within frame

Closed Source

What kind of encoding?

- 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!

Cracking the Decoder

- Decoding stages:

1. Symbol “gray indexing” → Gray Coding
2. Data whitening → PRNG algorithm in app note
3. Interleaving → Interleaver algorithm in patent
4. Forward Error Correction → Standard Hamming(N,4) algorithm

Easy Enough?

lol!

Why not?

Documentation Lies!

Red Herrings

- Decoding stages:

	Documentation:
1. Symbol “gray indexing”	European patent
2. Data whitening	Data sheet
3. Interleaving	European patent
4. Forward Error Correction	European patent, data sheets

Cracking the Interleaver

- 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

https://media.ccc.de/v/33c3-7945-decoding_the_lora_phy

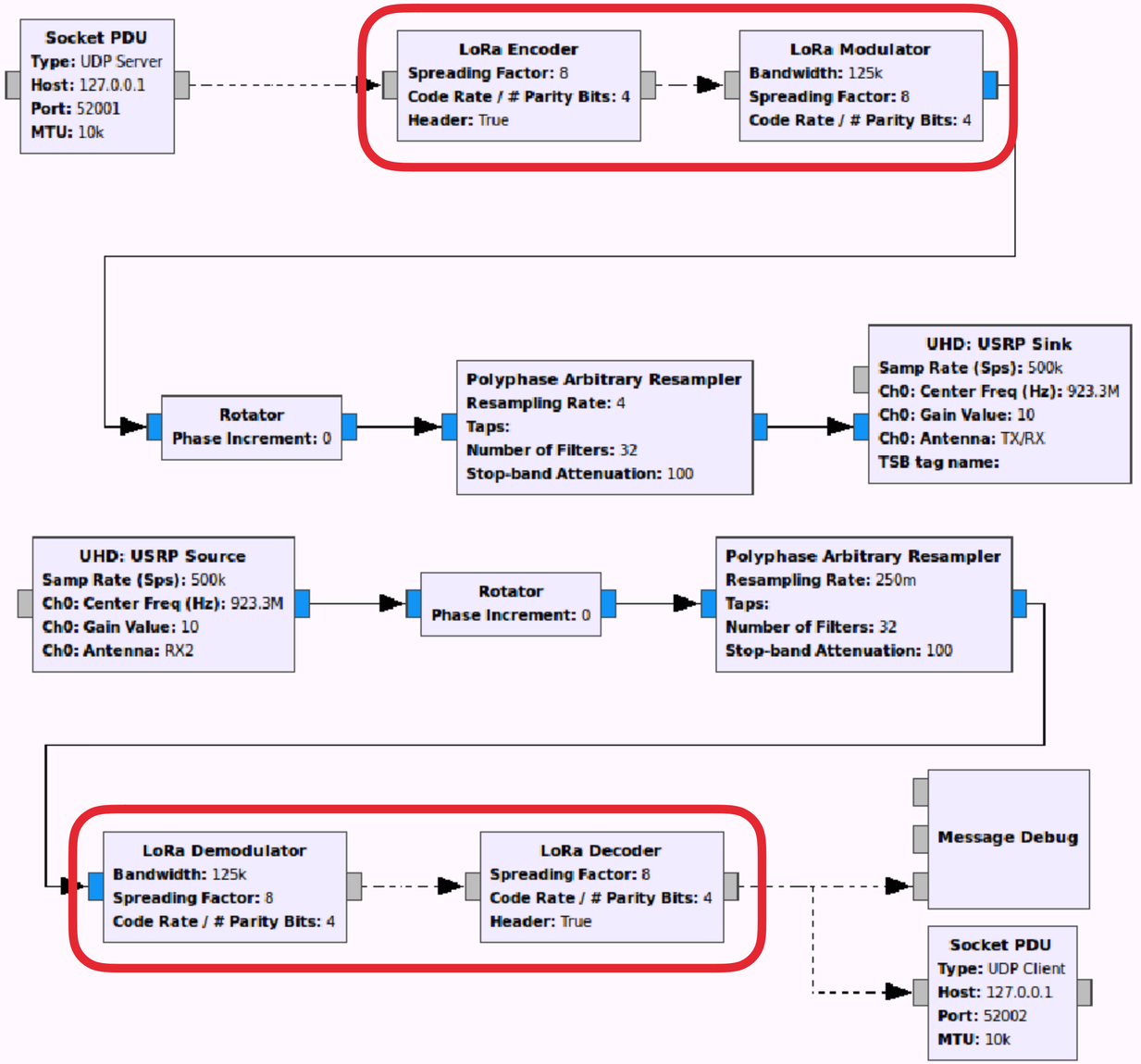
PoC||GTFO 0x13, 33c3 Presentation

RSAConference2017

Introducing *gr-lora*

gr-lora

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



Bastille.net

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 [illegible] Rebecca Shapiro, Sergey Bratus, Travis Goodspeed, Ryan Speers
  - Evading IDS // network monitors by fingerprinting receiver PHYs and crafting packets for **selective evasion**

PHYS MATTER

GNU Radio // POTHOS Prior Art

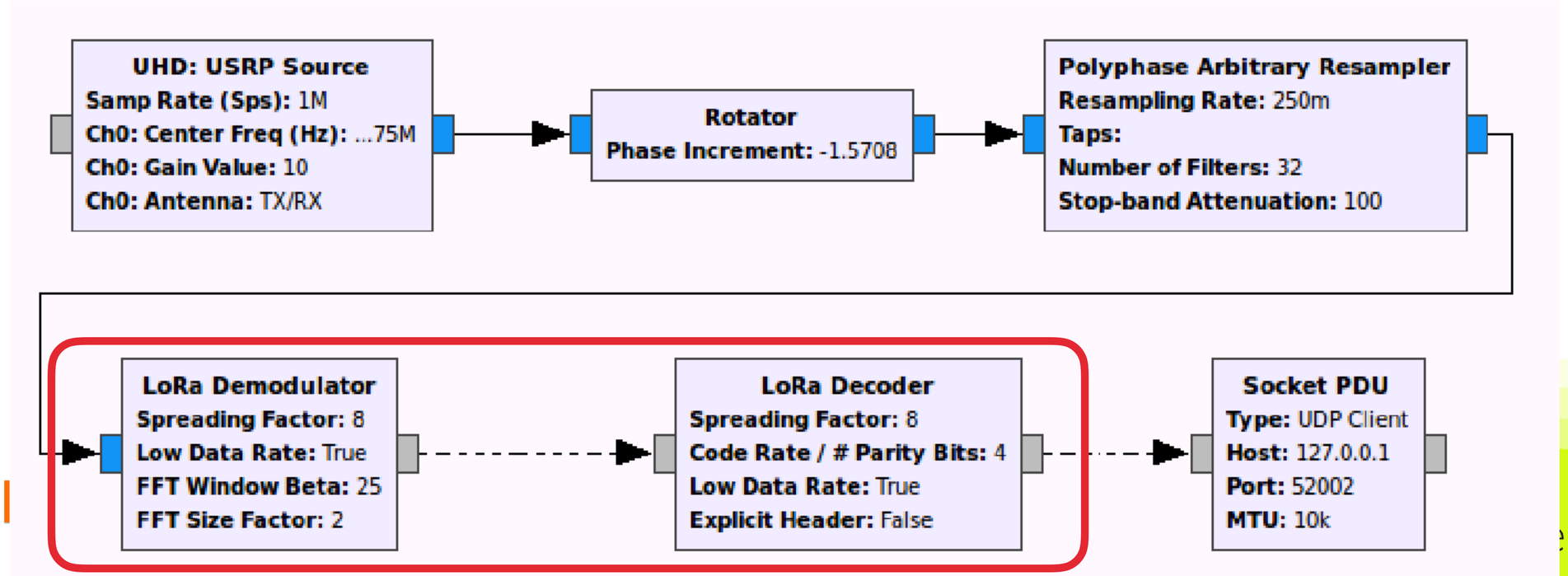
- Josh Blum's LoRa-SDR for POTHOS
  - Implements a LoRa-like modulation
  - Encoding/decoding is incomplete — follows reference documents, which differ drastically from reality
- rpp0's gr-lora

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

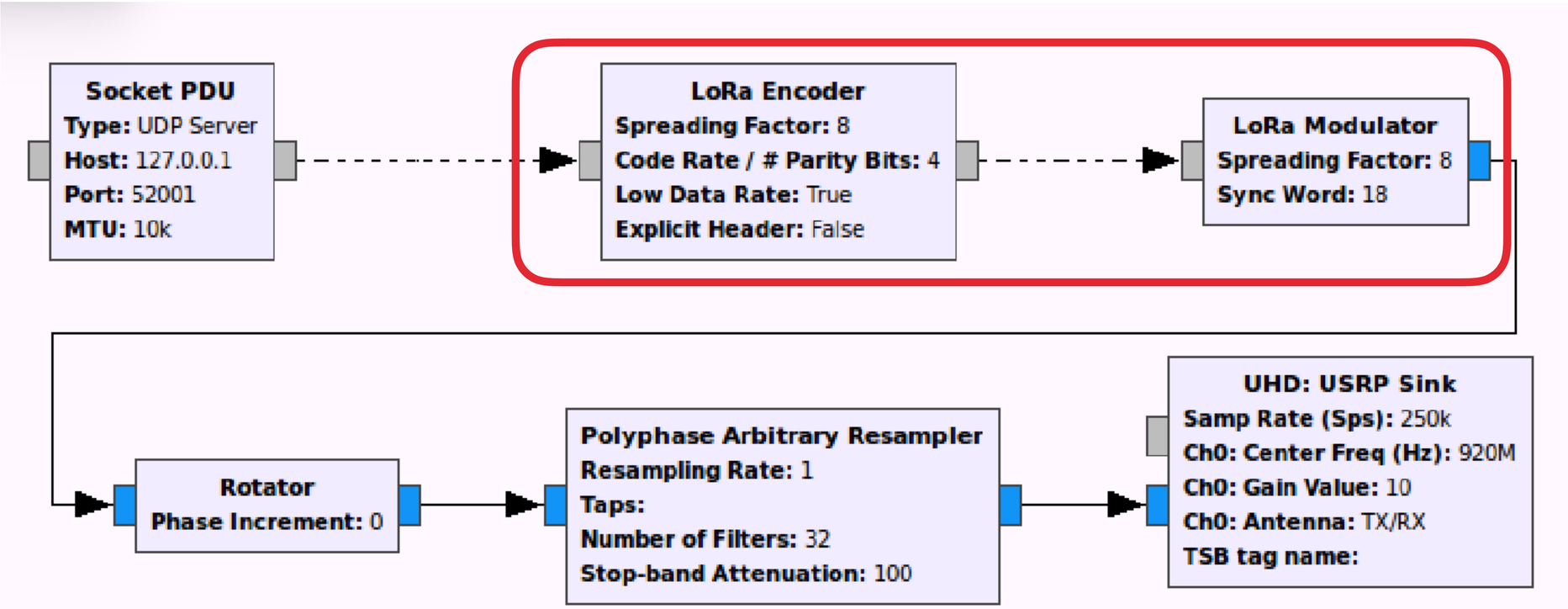
Demodulator // Decoder

- Implements the decoding algorithm we just outlined
  - Dechirping, stacked FFTs, etc.



Modulator // Encoder

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



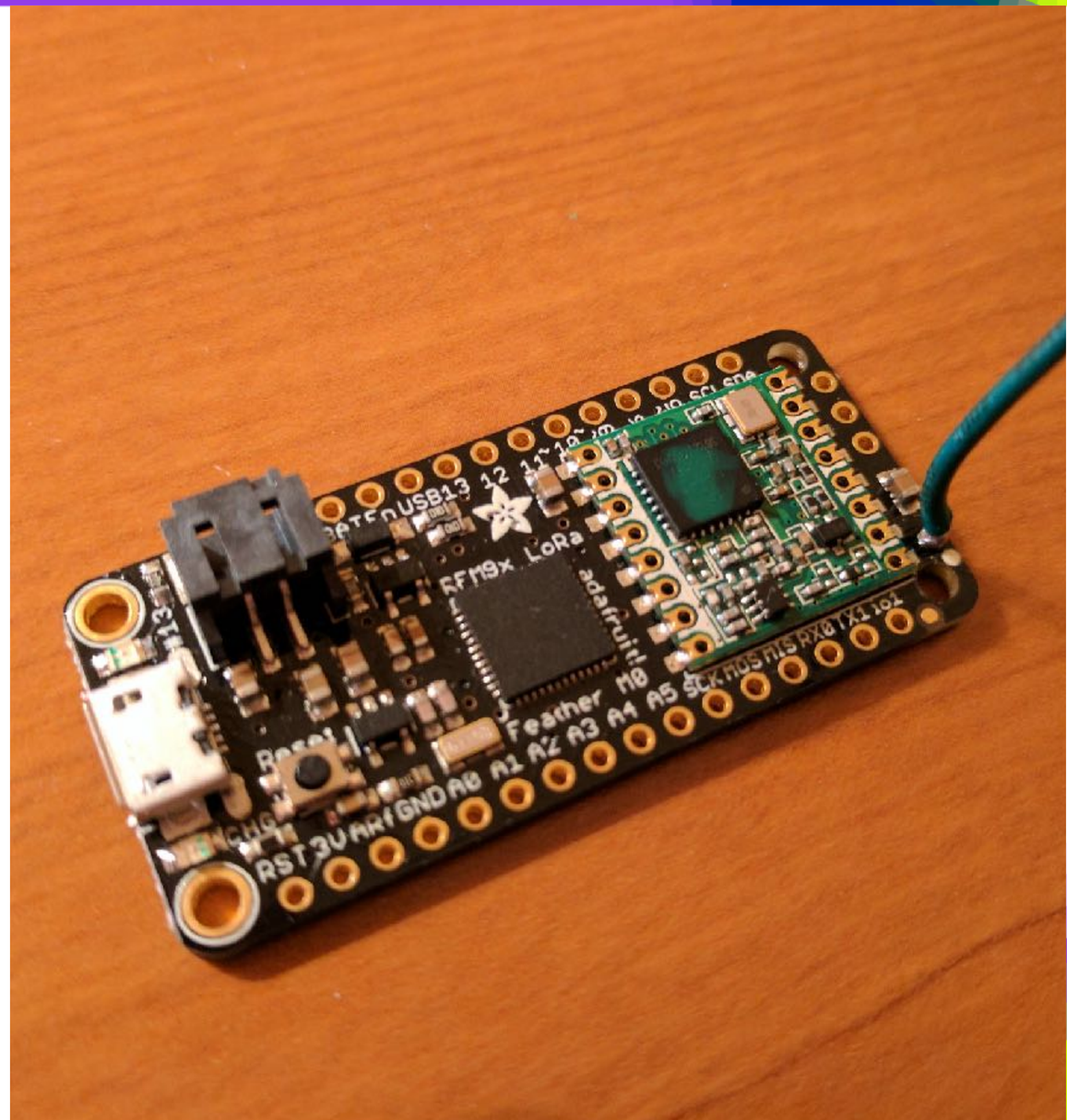
gr-lora source

github.com/BastilleResearch/gr-lora

Demo Time!

Demo Scenario

- Let’s sniff some traffic!
- Transmitter
  - Adafruit Feather M0 w/ hardware-defined LoRa module
- Receiver
  - gr-lora
  - fed by Ettus USRP B210



Bastille.net

RSAConference2017

Conclusions

So What?

- Current-gen IT infrastructure secures WiFi and Ethernet
- Wireless IoT/M2M networks represent **unchecked threat frontier**
  - **Cellular** (rogue devices // rogue cell towers // BYOD // data exfil)
  - **Bluetooth** (rogue devices // Bluetooth tethering // data exfil)
  - **Proprietary Wireless** (**Mousejack**: vulnerable mice and keyboards)
  - **LoRa** (data exfiltration // subversive asset tracking)

What can **YOU** do?

As an IT Professional, how can you secure your org against wireless threats?

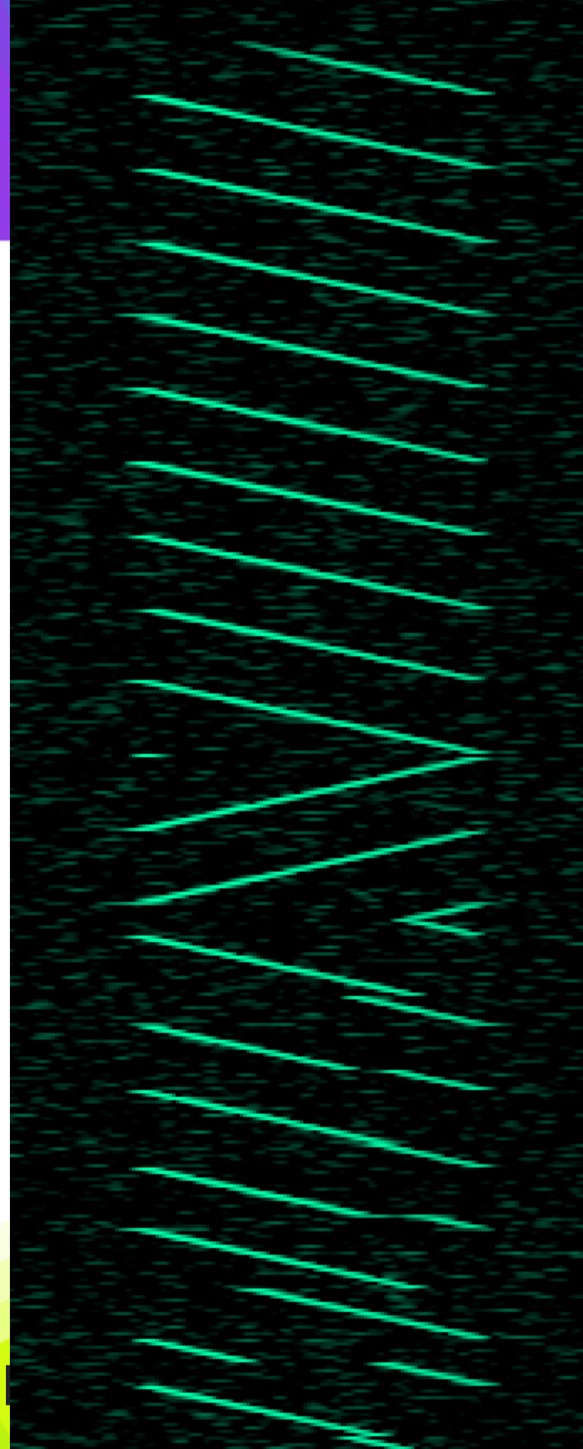
Awareness + Visibility = Empowerment

Now What?

- Next week you should:
  - Assess your org's exposure to IoT devices (including cellular/BYOD)
- In the first three months following this presentation you should:
  - Define an IoT security policy for your organization
- Within six months you should:
  - Add a **security capability** that empowers you to monitor cellular, IoT, and other wireless devices within your organization
  - **Take action** against IoT-based threats!

To Conclude

- LPWANs have momentum and are proliferating
- RF stacks are becoming more diverse
  - Wireless is not just WiFi anymore
- Shown how hackers go from obscure RF —> bits
- Added a new tool to the RF security researcher's arsenal



Bastille.net

Acknowledgements

- Balint Seeber, Bastille Threat Research Team
- Josh Blum, hexameron, and Bertrik Sikken, open source contributors
- Thomas Telkamp and Chuck Swiger, IQ donors

- RSA Conference for hosting!

matt@Bastille.net
@embeddedsec

Thanks!

matt@Bastille.net
@embeddedsec

Questions?