LAB 02 - DECODING SIGNALS

## PART I: DEMODULATE AUDIO

analyze and demodulate provided FM RF data file

INSTRUCTIONS

1. Setup a system with GNU Radio and GNU Radio Companion or use the VM provided in D2L
   a. GNU Radio is typically happiest on Linux
   b. If you fell in love with BSD in 840, please consider breaking up
2. On your canvas, load the data file and demodulate it using the demodulate module.
   a. You're welcome to investigate demodulating it manually as well
   b. Many tutorials exist online for demodulating the signal of a Software Defined Radio. You can use those, just swap the file source for the RTL-SDR source (you may need to add a throttle with the signal rate too)

FINDINGS AND ANALYSIS

GRC Canvas
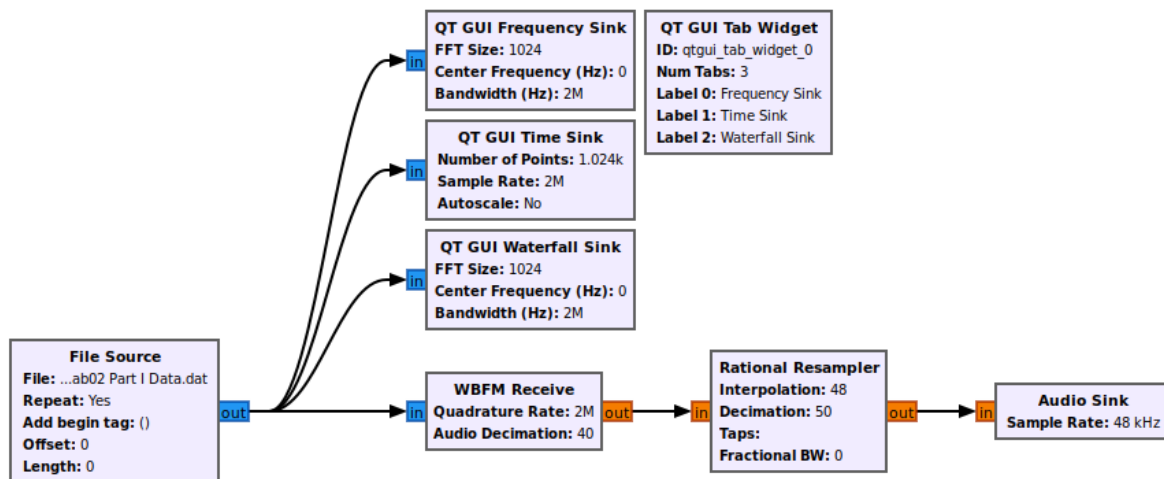
Demodulate FM (WBFM Receive)

To reduce the computational load and focus processing on the relevant information for audio playback, I selected an audio decimation rate of 40. Since the quadrature rate is 2M, I chose to decimate it by a factor of 40 to produce an audio sample rate of 50k.

$$\frac{2,000,000}{40} = 50,000$$

Resample (Rational Resampler)

Next, I selected the Rational Resampler to match the sample rate of the demodulated signal to the desired audio sample rate for playback (48kHz). I solved for the Resampling Factor by solving for the ratio of output rate (L) to input rate (M). Since the sample rate is currently 50kH due to demodulation and 48kH is the desired output, the Resampling Factor can be solved mathematically as follows:

Interpolation Factor (output rate)	L	$48k$
Decimation Factor (input rate)	M	$50k$
Resampling Factor	$\dfrac{L}{M}$	$\dfrac{48k}{50k} = \dfrac{48000}{50000} = \dfrac{48}{50}$

Audio Sink

Lastly, the Audio Sink was connected and set to the target 48kHz sample rate and the signal was played.
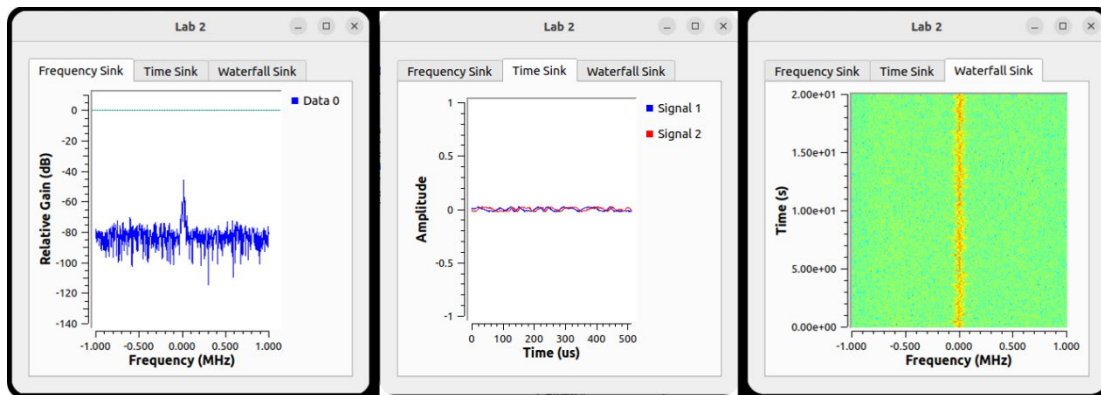
Part 1 Questions

Q1. Who is the sweepstakes open to which age groups?

The sweepstakes is open to South Dakota teens, age 14-19

Q2. There's a commercial with a big-wig CEO, who is it or what is he the CEO of?

The commercial features Jay Farner, CEO of Rocket Mortgage

PART II: DEMODULATE DIGITAL DATA

discover, analyze, and decode transmissions

INSTRUCTIONS

1. Use SDR# to connect to the radio from the first lab (sdr://138.247.12.20:5555)
2. Tune into ISM band where this mystery device is transmitting
3. Identify frequency of the device using the provided FCCID (M3N-A2C31243300)
4. Capture transmission from this mystery device
5. Open transmissions in Audacity (or another appropriate tool for waveform analysis)
6. Identify waveform
7. Decode digital data and convert to hexadecimal format

### FINDINGS AND ANALYSIS (TRANSMISSION 1)

Research Device using FCC ID

First, I looked up the device using its Federal Communications Commission Identification (FCC ID)

FCC ID Search:

FCC ID: M3N-A2C31243300   [Search]

Application: Automobile Entry/Security Transmitter

Equipment Class: DXX - Part 15 Low Power Communication Device Transmitter

Short Link: fcc.id/M3NA2C31243300

Sources: FCC.gov | FCC.report

Registered By: Continental Automotive Systems US Inc. - M3N (United States)
you@youremail.com   [Subscribe]

App #	Purpose	Date	Unique ID
1	Original Equipment	2012-04-17	xIS01m3yvOYkdHMixo7Qyw==

Operating Frequencies

Device operates within approved frequencies overlapping with the following cellular bands: CDMA 3,JTACS UP | GSM 900 E UP | GSM 900 P UP | GSM 900 R UP | LTE 8,900 GSM UP | UMTS CH 8 UP |

| Frequency Range	Rule Parts	Line Entry
902.375 MHz	15C	1
903.425 MHz	15C	2

Tune to Device

During my research, I found the device frequency is around 902-903mHz. When I looked around this area in SR#, I was able to locate the signal at 90.1.9375mHz


901.9375 MHz
-71.2 dBFS

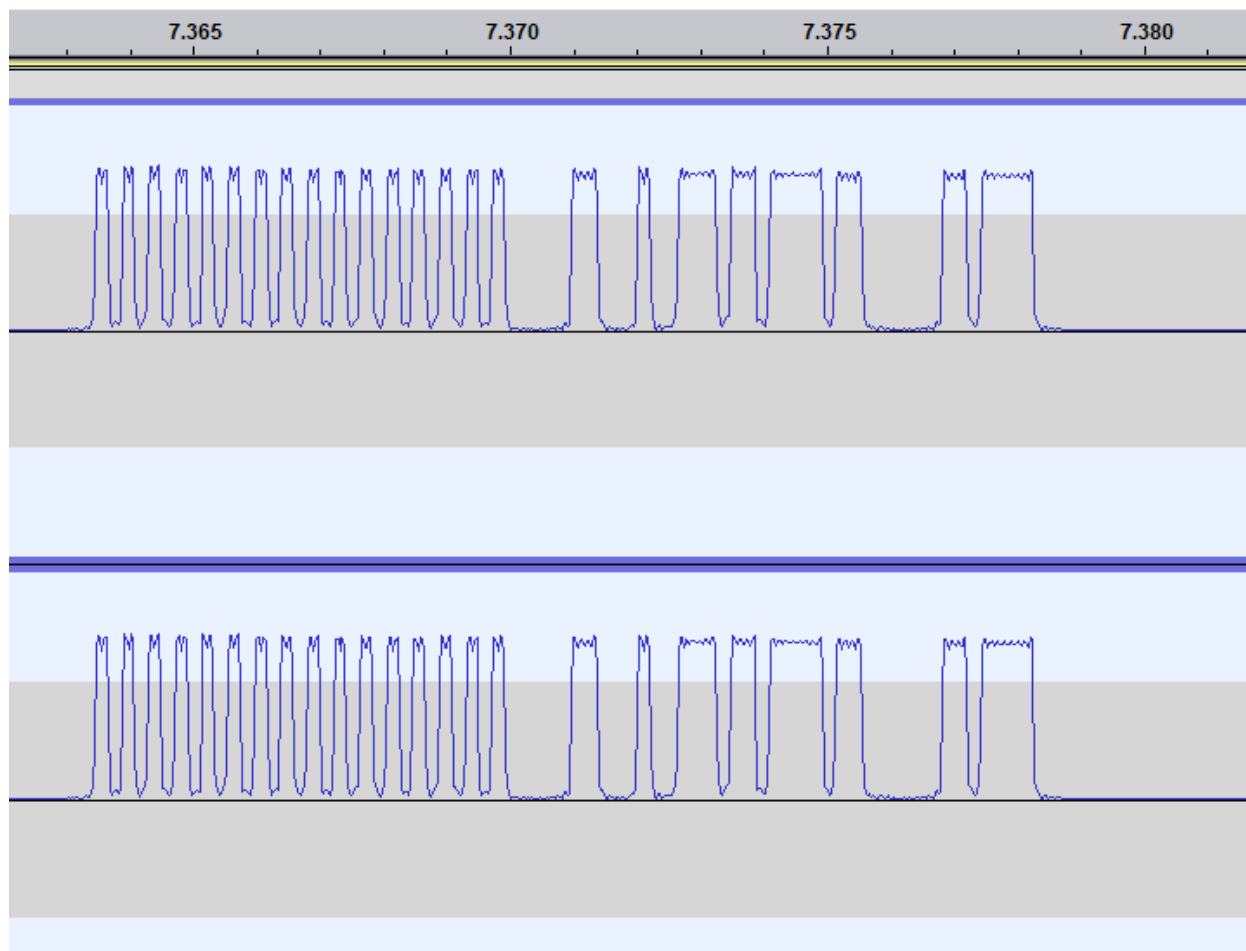902.000 M
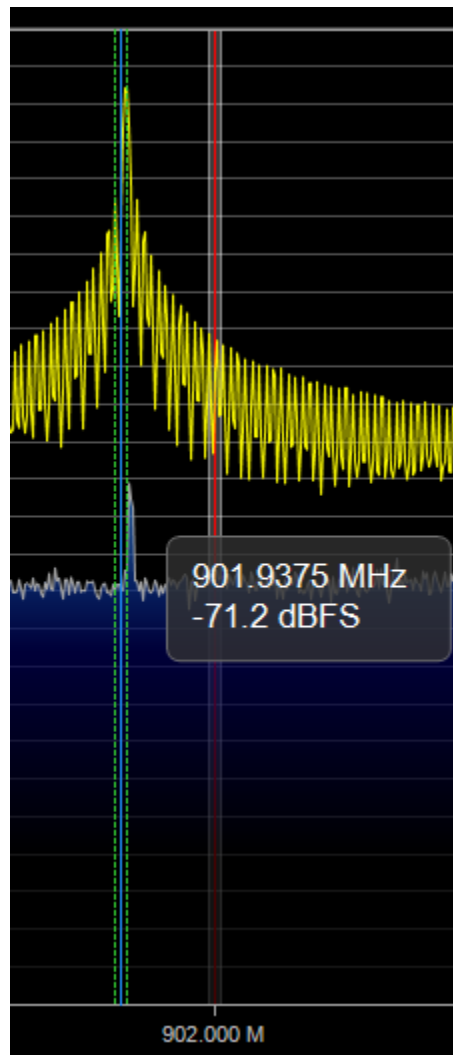
Configure Settings and Record

After setting bandwidth to 30k and modulation to AM, I was able to effectively capture and record the signal.
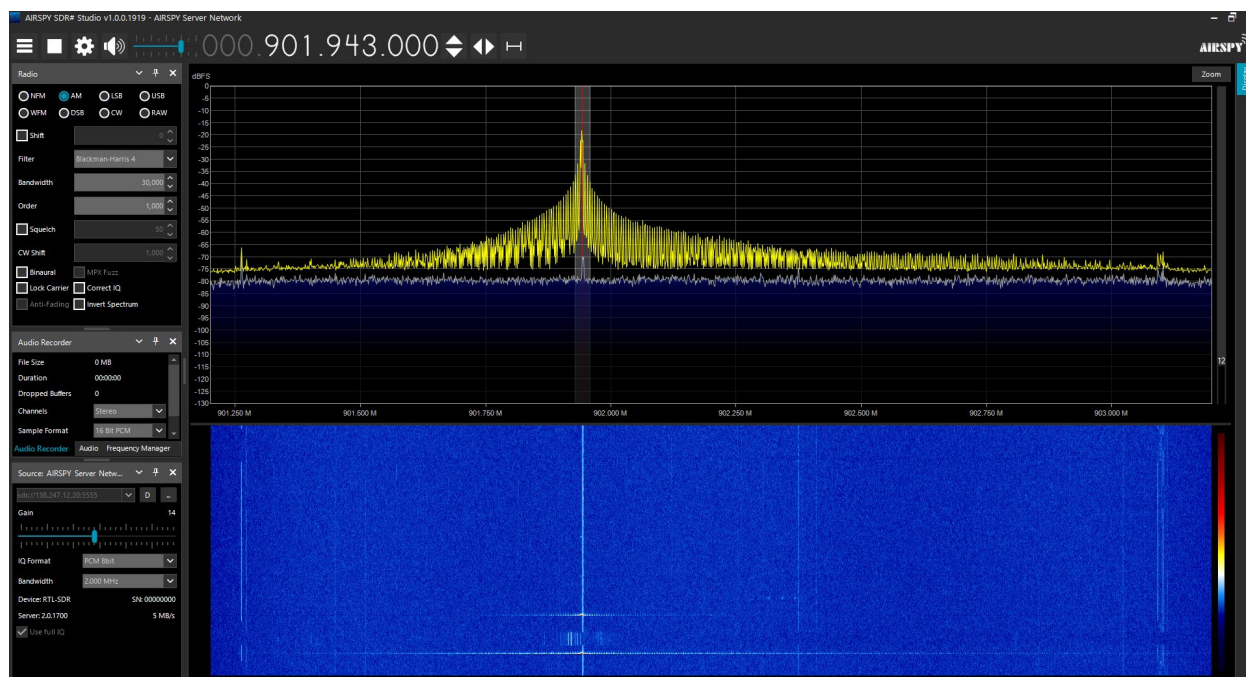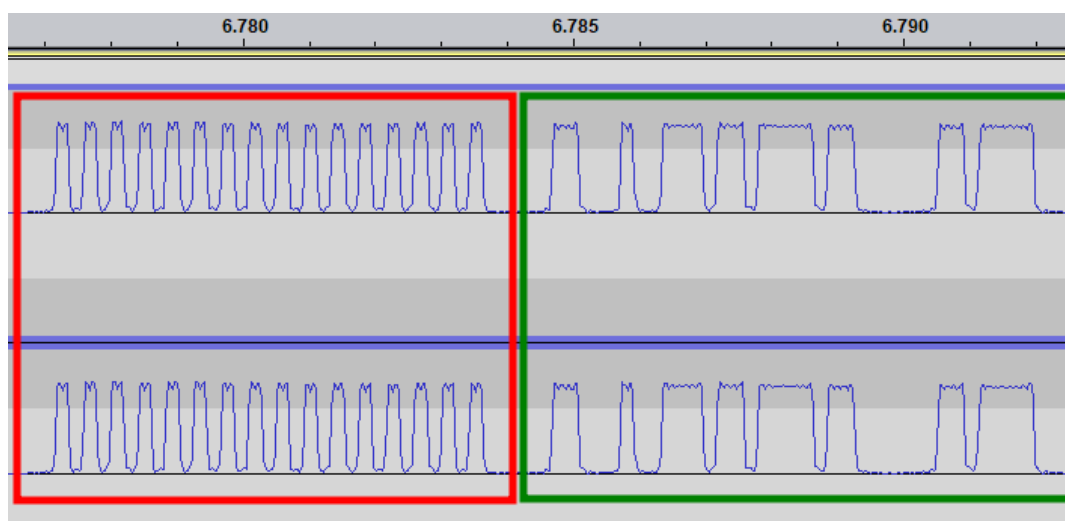

Open Recording in Audacity

As shown in the image below, the signal is repeating. Therefore, I decided to isolate the target signal and zoom in to get a better view of the amplitude modulation wavelength.
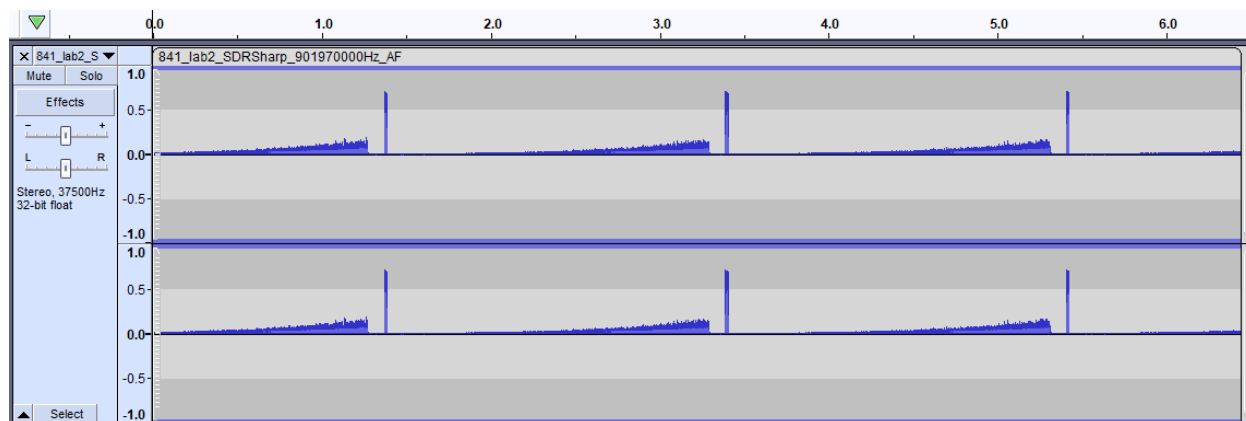
Analyze

As shown in the zoomed in view below, there are a series of consistent repeating patterns (shown in red), followed by different variations (shown in green). This is because the red section is the Preamble, which the transmitter uses to wake up a receiver. A Preamble has a distinctive pattern or structure that the receiver can quickly recognize. The section in green is comprised of the Data frames. These data frames contain the target information.

Decode

In order to decode this signal, it is important to understand that this modulation type is characterized by peaks representing '1's and valleys representing '0's. To ensure consistency while counting these, I uploaded the file into Universal Radio Hacker (URH) to decode the signal efficiently and effectively.

This capture contains the following binary sequence(s) (displayed in their corresponding sections):

1010 1010 1010 1010 1010 1010 1010 1010	*Preamble*
0000	*Header/Control Flags*
1100 0100 1110 1101 1110 1100 0000 1101 1110	*Data Frames*

Convert to Hex

Lastly, I copied these values into the Binary to Hex editor at Tools a Day to find their hexadecimal equivalent.

01010101010101010101010101010101010   ×   aaaaaaaa

0000   0

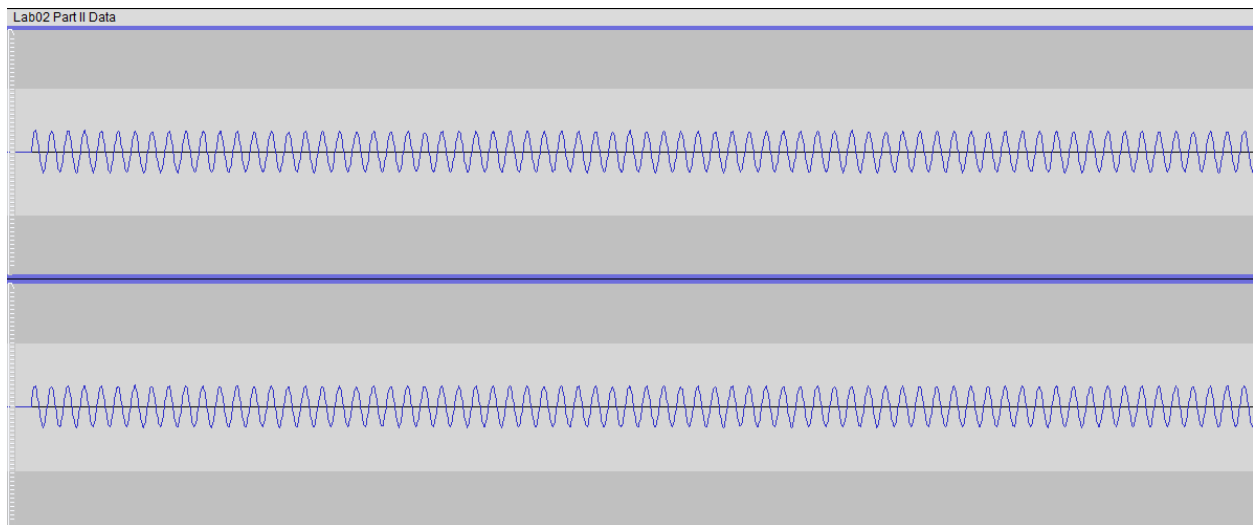11000100111011011110110000011011110   c4edec0de

## FINDINGS AND ANALYSIS (TRANSMISSION 1)

I struggled quite a bit with this one, as I am not quite sure how to proceed. When I input the raw data into Audacity, I saw the following block of signals:


Upon closer inspection, I can see there are some wavelength patterns.

The beginning of the signal is consistent with a Preamble as it has a distinctive and consistent pattern that a receiver could quickly recognize. This pattern continues for a significant length of time, as shown as a 'circular pattern' to the left of the line below.
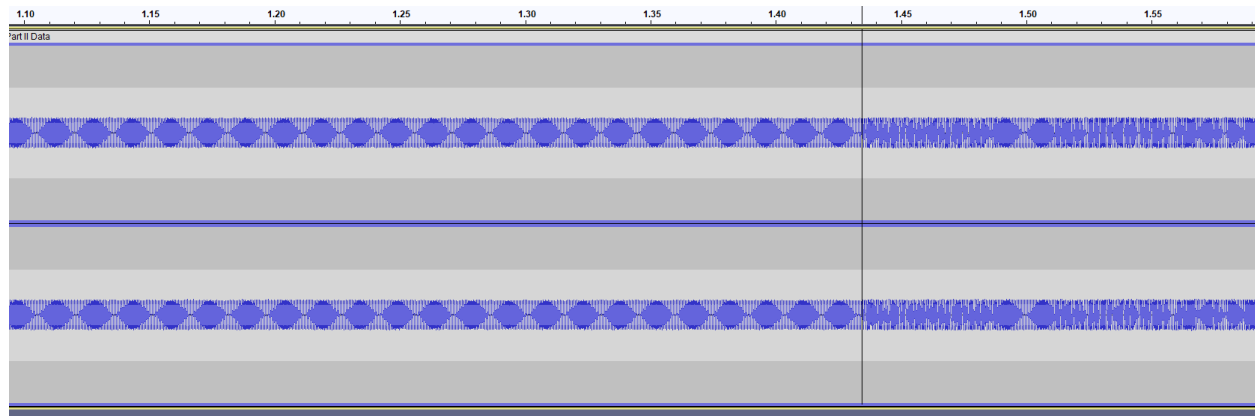
Around 16,000 steps into the signal, the pattern begins to change (as shown immediately to the right of the black line). If we zoom in on this area we can see that there are anomalies in the pattern.
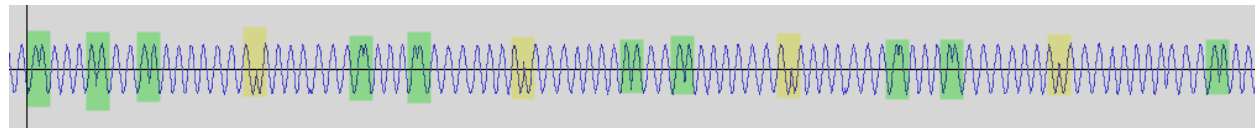
We can see that in some areas the wavelength does not complete its intended direction before returning. Green highlights areas where this happens above the median, and yellow highlights where this happens below the median. However, it is hard to determine if this is encoded data or simply normal signal variations. Similarly, it is hard to tell if some lines meet the set qualifications – For example, it is clear that the 4th and 5th green mark from the left are anomalies, but would the 2nd and 3rd meet the same criteria? They do not complete the normal pattern, but they do pass the median line. Also, there seems to be a broader pattern of "2 green, 1 yellow, repeat." As such, I cannot confidently decode this signal given I am unable to definitively determine which areas constitute a 0 or a 1. However, my guess is that the 0 and 1 either correspond to the side of the median they fall on (i.e green = 1 and yellow = 0) or it relates to the distance between the signals (which corresponds to either ≈100 or ≈200 samples).

Given these assumptions, I would guess that this segment is either 11101101101101 (0x3b6d) or 0011011011011 (0x6db).