**Lab 03 – Beacon Scavenger Hunt**

## Instructions

* 1. a

## Questions

### Locate a beacon that’s hiding its SSID. What is the SSID length?

* + The BSSID 02:18:4A:14:AB:FF is hiding its SSID and has a length of 4.

A screenshot of a computer

Description automatically generated

### Locate two beacons that are operating on a channel other than 1, 6 or 11

* + CHP (E6:95:6E:4A:87:D6) and Vlads\_Place (E4:95:6E:4A:87:D6) are both operating on channel 2

A screenshot of a computer

Description automatically generated

### The timestamps for the official DSU networks are all very consistent, find a non-DSU beacon containing a timestamp that is significantly different

* + 02:18:4A:14:AB:FF has an unusual uptime value of 131d 11:52:25, which is significantly different from the uptime values of the other networks.

A screen shot of a computer

Description automatically generated

### Many AP’s do not beacon any regulatory domain information, but one does. Can you find it?

* + There were a couple of AP’s that contained regulatory domain information in the capture. Two examples were “CHP” (E6:95:6E:4A:87:D6) and “Vlads\_Place” (E4:95:6E:4A:87:D6) that displayed the Country Code “RU”

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

### Create two screenshots, one with the best, one with the worst signal strength you can find

* + The strongest Signal is “Vlads\_Place” (E4:95:6E:4A:87:D6) with a signal strength of -9 dBm.

A screenshot of a computer

Description automatically generated

* + The weakest signal is “eduroam” (18:64:72:E8:E0:63) with a signal strength of -52 dBm.

A screenshot of a computer

Description automatically generated

### Find a network that does not have the Privacy flag set

* + “Guest” (18:64:72:E8:E0:61) does not have the Privacy flag set

A screenshot of a computer

Description automatically generated

### Display a list of all of the unique ESSID’s you can detect in a given area

* + CubeFarm, AAA\_Mobile, eduroam (AAA), AAAGaming, Guest, GoTrojans (AAA), Vlads\_Place, CHP, and two hidden

A screen shot of a computer

Description automatically generated

### Display a list of all of the unique BSSID’s you can detect in a given area

* + 00:00:00:00:00:00, 78:8A:20:08:CC:DF, 7E:8A:20:08:CC:DF, 18:64:72:E8:E0:63, 18:64:72:E8:E0:62, 18:64:72:E8:E0:61, 18:64:72:E8:E0:60, 02:18:4A:14:AB:FF, E4:95:6E:4A:87:D6, and E6:95:6E:4A:87:D6

A screen shot of a screen

Description automatically generated

### Many beacons contain “vendor specific” information, you can see this in Wireshark if you look at a beacon frame. What is this for?

* + Vendor-specific information in beacon frames contains additional data that is specific to a particular manufacturer or vendor. This can include information such as the product model/serial number, firmware version, hardware capabilities, and other proprietary features. This enables vendors to differentiate their products and provide specific functionality based on their unique specifications.

### Researchy question! 802.11ax, marketed to the muggles as WiFi 6, is pretty neat. It’s introduced a lot of new features, they’re really only useful in dense environments. Advice: don’t bother upgrading to AX in order to improve your home’s wifi performance. To that end, one of the neat features that are introduced is the notion of “spatial reuse”. We achieve this through coloring (basic service set coloring or more broadly as a network color code). No crayons needed. What is this?

* + x

# 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
   1. GNU Radio is typically happiest on Linux
   2. 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.
   1. You’re welcome to investigate demodulating it manually as well
   2. 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**

*A diagram of a computer

Description automatically generated*

#### *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.

#### *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 () to input rate (). 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)* |  |  |
| Decimation Factor *(input rate)* |  |  |
| Resampling Factor |  |  |

#### *Audio Sink*

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

A screenshot of a computer

Description automatically generated

### **Part 1 Questions**

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

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

1. 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)

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

### **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

A screen shot of a graph

Description automatically generated

### **Configure Settings and Record**

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

A screenshot of a computer

Description automatically generated

### **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.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

### **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.

A screenshot of a computer

Description automatically generated

### **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.

A diagram of data frames

Description automatically generated

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

|  |  |
| --- | --- |
|  | *Preamble* |
|  | *Header/Control Flags* |
|  | *Data Frames* |

**Convert to Hex**

Lastly, I copied these values into the Binary to Hex editor at [Tools a Day](https://toolsaday.com/number-tools/binary-to-hex) to find their hexadecimal equivalent.

A number and text on a white background

Description automatically generated

## 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:  
A blue and grey striped background

Description automatically generated

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

A screenshot of a computer screen

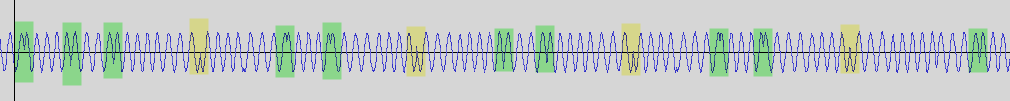
Description automatically generated

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.

A screenshot of a computer

Description automatically generated

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).