Tu Lam

CS 373 (Defense Against the Dark Arts)

Dr. Bram Lewis

November 17th, 2021

Lab #4 (Hardware Hacking)

This time in lab No.4, focus on using the ***Teensy 4.0*** board that we bought back in the beginning of the term. In this lab, we will use the pin that is located ***Teensy 4.0*** to see what it can tell us and how we are hacking the hardware. Beside that, we will identify what type of pins are located on the ***Teensy 4.0*** as well.

At the start, the lab provided us an instruction on downloading the ***Teensy Loader application*** to help load our code (which is in a hex file) into the ***Teensy board*** and control it functionality. In the setup, we were able to mess around with the application of ***Arduino*** to show how a code from there can implement into the Teensy board. Below is an image of what the Teensy Loader application looks like and an image of what the ***Teensy 4.0*** looks like. Beside that, we were instructed to download the ***Logic software*** to pick up the wave form from what the hex file that we were given in lab produce when run on the Teensy board. In this lab, we are also a ***Logic Analyzer*** to determine the pin of the Teensy and see what result it will produce from the board as well. Also, in the figure below, we will be showing off the Logic Analyzer as well.

Figure #1: *The Teensy Loader application display on the Windows*

Figure #2: *The Teensy 4.0*

Figure #3: *The Logic Analyzer component*

First part of the lab, I downloaded the ***Logic Software*** that was require for the lab and install on my machine. Also, in the lab, they said that "There are a lot of pins on a Teensy. I'd recommend identifying them". From there, I was able to find a website called PJRC that would have a good manual on how the pins are layout and what do they represent. Below will be two figures, one is showing the manual, while the other one shows the Logic software when it first started after the installation.

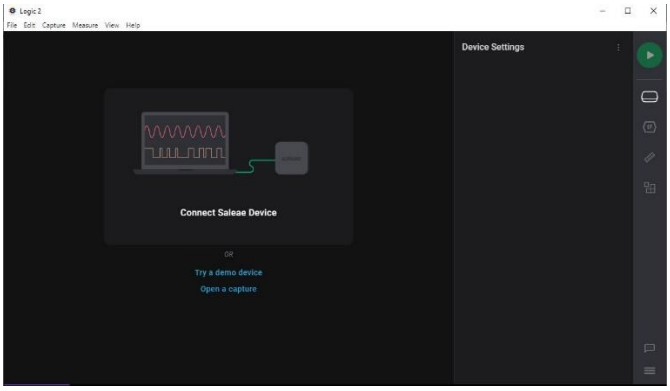

Figure #4: *The application of Logic Software*

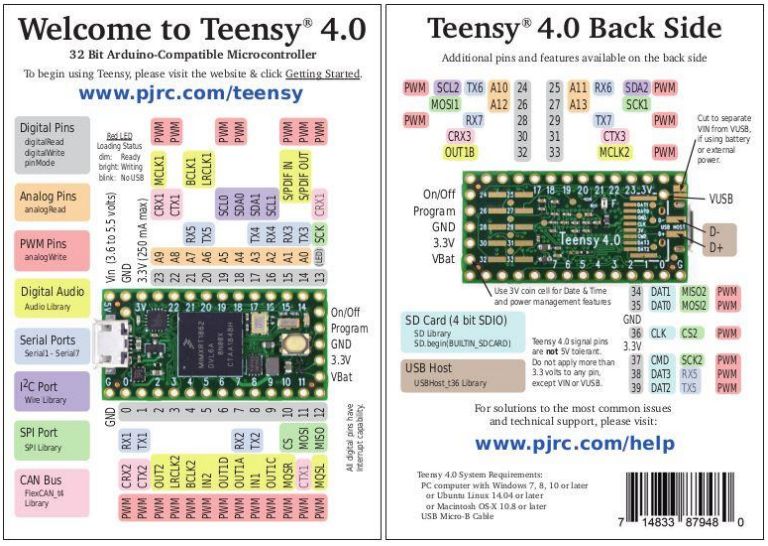

Figure #5: *The manual of Teensy 4.0 pins based on the PJRC website*

Next, I then watch the video that was provided on the lab on how to use the ***Logic Analyzer*** and how it connects with the ***Teensy*** board to be identify. When I connect the Logic Analyzer to the computer, the Logic software application automatically detected and show the pin color of what needs to be connected to the ***Logic Analyzer***. Below is a figure showing the color to connect them to the Logic Analyzer. Beside that, I see extra wires in the color of black and white and I think they are representing the GND port on the analyzer, but I could be wrong on that. Then I connect the remaining end onto the Teensy board on the first ***8 pins*** that matches the color on the ***Logic Analyzer***.

Figure #6: *Showing the color which port is connected on which string*

From there, I loaded up the program onto the ***Teensy Loader application*** with the hex file that was given to us. Then I started to record the signal, and once I finish the recording, one of the channels display some signal data, and the only channel that display this is ***channel 1***. A picture of the signal will be shown below for reference of what I got for running it the first time. From there, it was great that the Logic software is capturing something from the hex file that was given, and this is from the first try connecting it to the first 8 pins that is on the first set of pins on the Teensy 4.0.

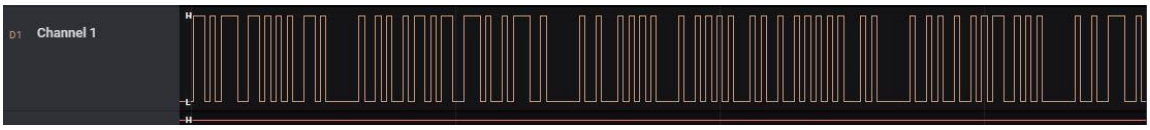

Figure #7: *A signal form in microseconds showing what was transmitted in channel 1*

Next, using the Analyzer tab, I chose the setting of ***Async Serial*** to decode my data in ***Channel 1*** and see what data it provides for me. From what I see, the data are all random jumble of hex numbers and random non-characters symbol that was displaying in channel 1. Below is an image showing what I was talking about when analyzing it. I believe the decoder show one of the randomness codes that the lab was talking about.

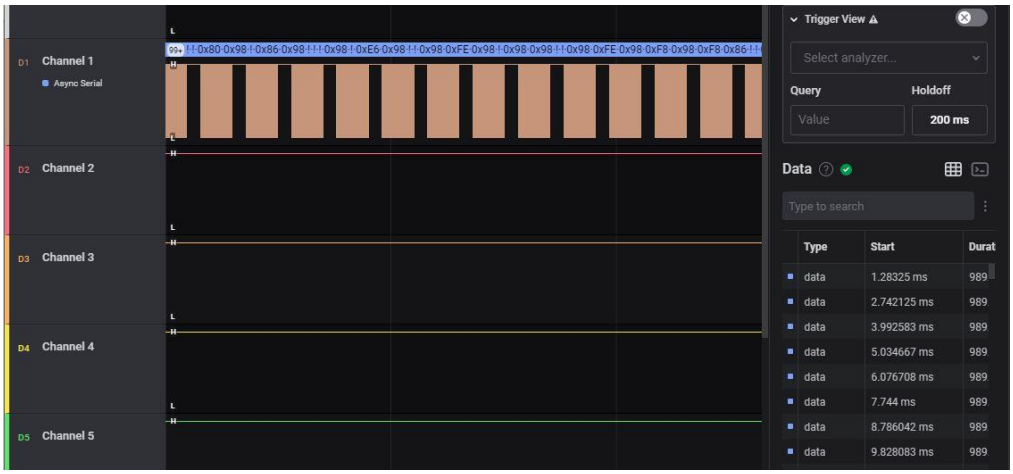

Figure #8: *Showing the decode of the message based on Channel 1*

The set of first pin was from **pin 0-7** and only channel 1 produces a signal. Then I set the next 8 pins as it said in the lab "*You may not find everything with only 8 channels. You might need to run the capture multiple times with different pins connected*.". The next set of pins I tried out was pin ranging from ***7-14*** and see what that will give us. I then recorded another capture to see what it can produce. I still only got channel 1 to produce a signal after inputting ***pin 7-14***. And using the analyzer setting from above, the code produces out a bunch of randomness code as well. A figure below will show it, and the randomness in code.

Figure #9: *Channel 1 data after changing a set of pins from 7-14 on Teensy 4.0*

Then, as I was browsing the setting around the Analyzer section in the Logic software, I notice that there is an option to produce an ASCII character instead of hex, and I retry with this option, and I got a message from one of the pins ranging from 7-14. An image below will show it and the data I got was that "*Unfortunately, try different pin*" as a message.

Figure #10: *The message after converting the hex to ASCII for pin 7-14*

Moving forward to the next set of 8 pins, I try pins ranging from ***12-19***, and this time I got couple channels to produce rather than just one channel. This time I got ***channel 1, 2, and 5*** to produce, but the message was just random garbage message that did not mean anything. Below is a figure showing the result of it.

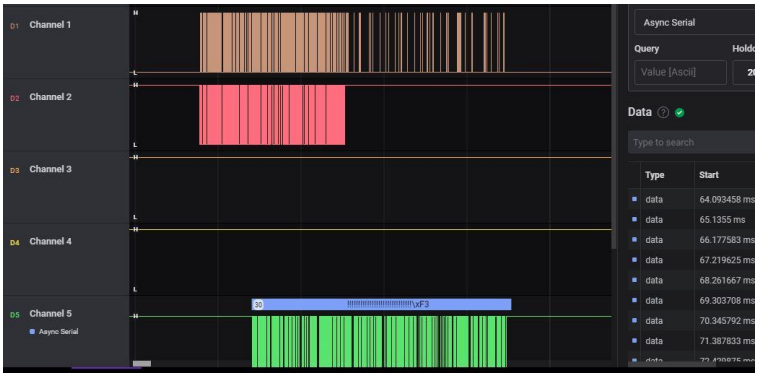

Figure #11: *The other channels appear as switching to pins 12-19*

Then, I noticed that channel 1 produce a message at pin 8 on the board and then I try and tested and found that pin ***14*** produces the next message. Below is an image of what it said about this pin location. With this message in mind, I went back to PJRC website and look at the manual, I found that the serial port was listed on the front of the manual, and I plug in that method to try it out. From there, I couldn't find any message display on my end and start my search over again.

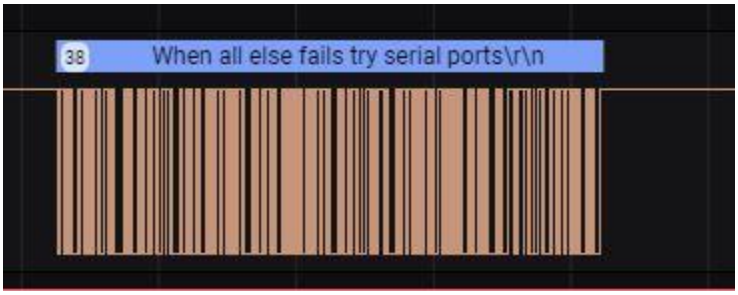

Figure #12: *The next message in pin 14 from channel 1*

With no luck insight, I decided to mess around with it and try to put the Teensy board onto the cardboard that it came with (the black piece of foam). With that, I see that the LED starts showing up around pin 13 where it usually didn't show up once before. With that in mind, I started playing around with the wire orientation and found there are hole on the side of the wire part where you plug in the bar into the wire. With messing it around, I found that the signal was also can be send via this way as well. From the message I got in channel 0, I was able to find the message after decoding the string a little bit and the message I got was "The secret message is: THERE IS NO SPOON. Nearly done with CS373!". And that wrap up what was the hidden message that the hex file was hidden. Below is an image of the message I got from decoding at channel 0.

Figure #13: *The image of channel 0 produce the hidden message*

Overall, this lab let us look at the hardware Teensy 4.0 and see if we could hack it by discovering the hidden message that was left inside a hex file. Through trial and error, we were thinking inside the box, but there was a scenario where we must think outside of the box for the hidden message to appear. It is a fun lab and a clever way for us to use our brain to decode the message and explore new tools such as ***Teensy application, Arduino, and Logic software***.

Reference(s):

1. Company, P. J. R. C. (2010). Teensy® 4.0 Development Board. PJRC. Retrieved November 18, 2021, from https://www.pjrc.com/store/teensy40.html.
2. Electronics, S. F. (2010). Teensy 4.0. DEV-15583 - SparkFun Electronics. Retrieved November 18, 2021, from https://www.sparkfun.com/products/15583.