CS 373: Defense Against the Dark Arts
Alex Young
8/7/2021
Lab 4 - Hardware Hacking

Lab Write-up

In this lab I used the logic software with a logic analyzer to decode waveforms loaded into the Teensy chip by the given hex file.

I found the setup for this lab was interesting, especially when I was ensuring that the teesy chip worked as expected. Here I loaded in a blink .iso file into the arduino->teensy and was able to program the teensy chip to do different things.

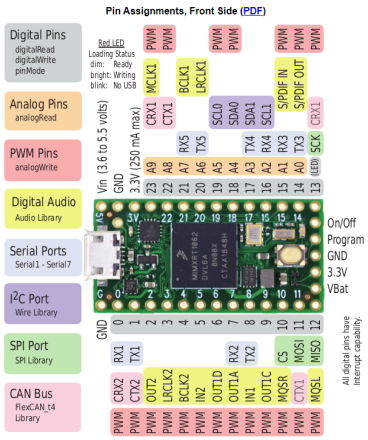
To start the lab I loaded in the hex file into the teensy. From here I knew that I needed to connect the leads from the logic analyzer to the pins on the Teensy. After I did this I loaded up the logic software to decode the waveforms.

Due to there being 24 different pins and only 8 channels, I started the lab by testing every pin to see if there was a waveform in the analyzer. Here are my results:

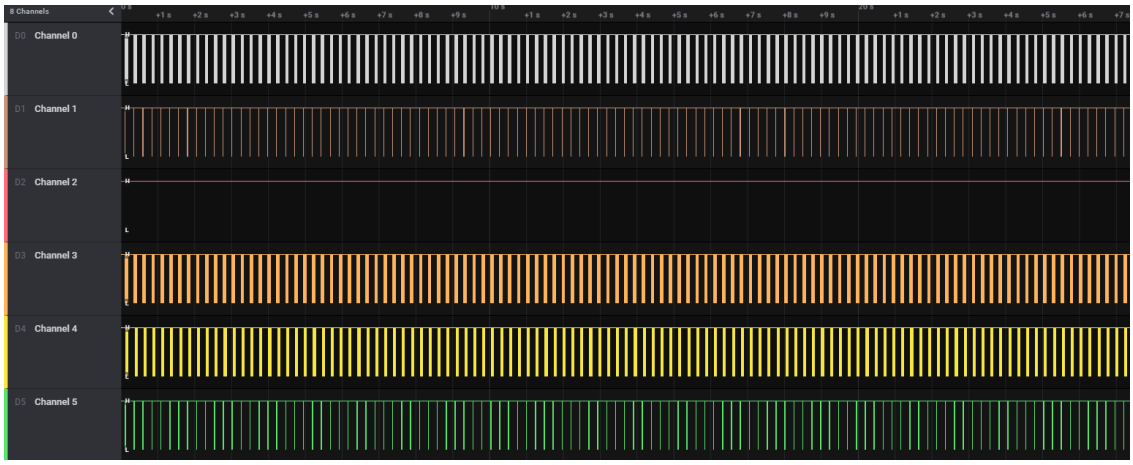
Pins with output waveforms:
1
8
14
17
20

I used the following pinout to match with these digital pins:
https://www.pjrc.com/teensy/pinout.html

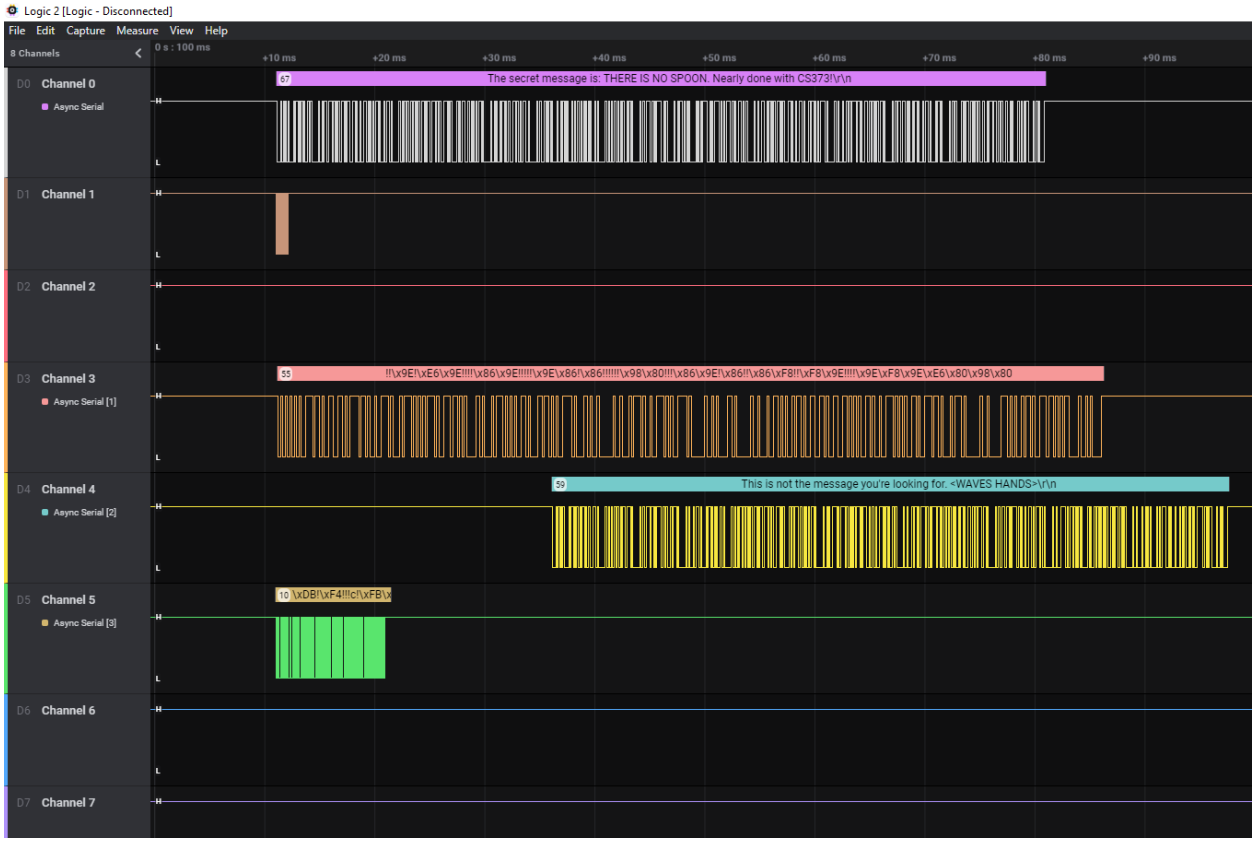
Teensy 4.0 Pins



The next step was combining all 5 waveforms and capturing them in a 10 second period. The output can be seen below:

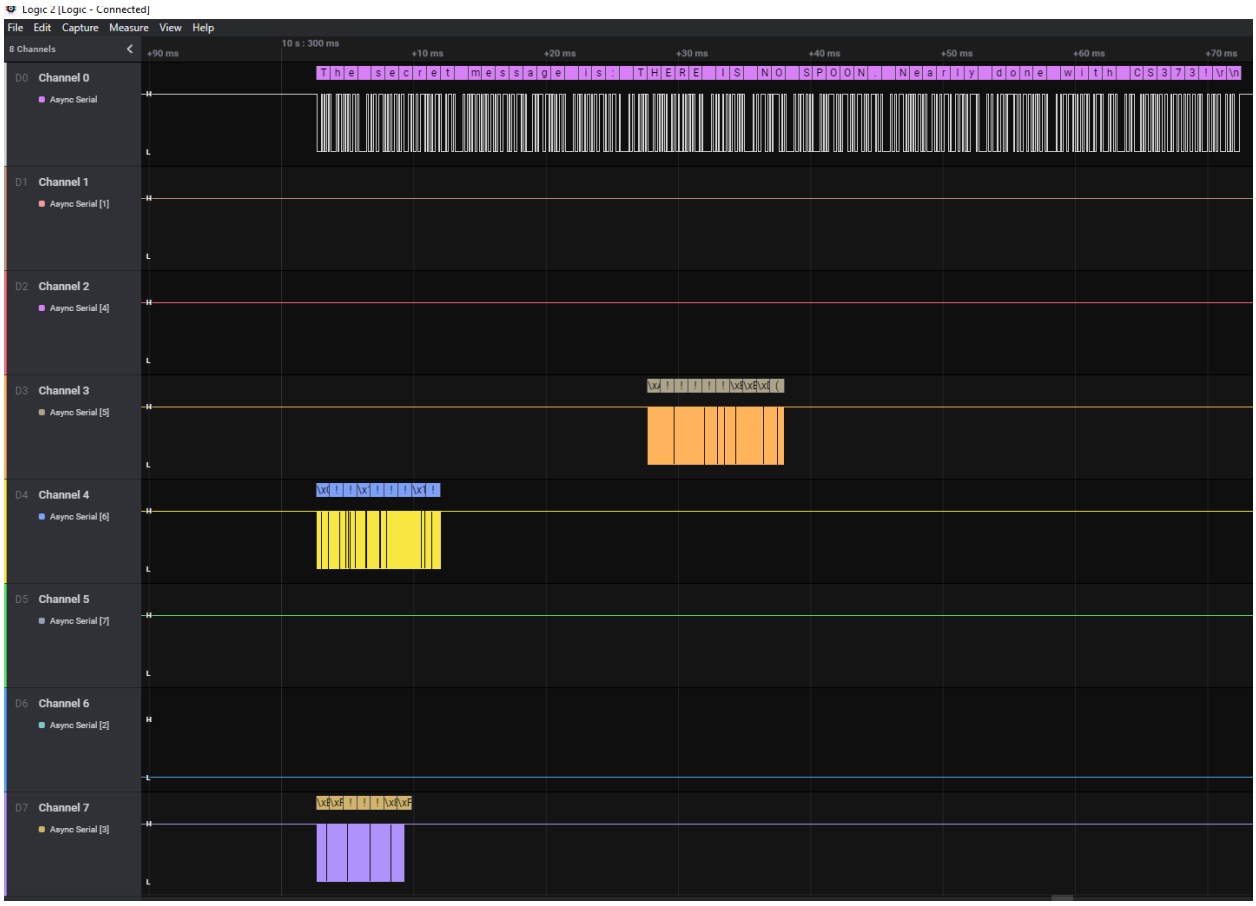


Once I got the output I saved the capture and attempted to decode it using the built in analyzers, including the SPI, I2C and Async Serial. Only Async Serial seemed to give a readable output, and when I changed the output to ASCII from hex, I found the secret message.



There are two decipherable messages here:
“This is not the message you’re looking for. <WAVES HANDS>\r\n”
“The secret message is: THERE IS NO SPOON. Nearly done with CS373!\r\n”

From here I was not certain I found all the messages due to the undecipherable channel 3 with frame errors, so I tried reading in the waveforms a few more times to check that there weren't any errors when I was reading in from the Teensy, but every time I got similar results to below:



Once again it shows that "The secret message is: THERE IS NO SPOON. Nearly done with CS373!\r\n" and the other channels don't seem to have any decipherable messages with such small output waveforms.

So here I concluded that this is the correct final message. I found the lab interesting because of the use of the logic software to help automatically decode the hex file. I wonder how this sort of hardware analysis is helpful in hacking or cybersecurity.