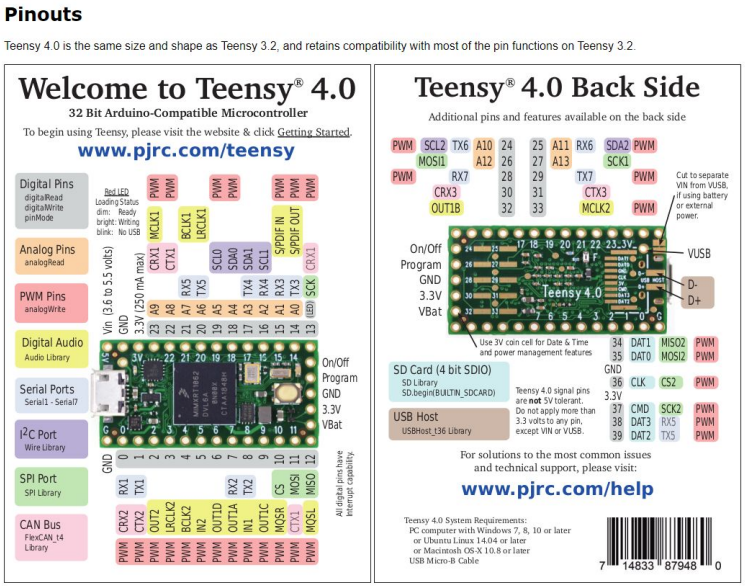
Nicolas Barraclough
11/22/2020
CS373 - Defense Against the Dark Arts

Lab 4 - Hardware Hacking

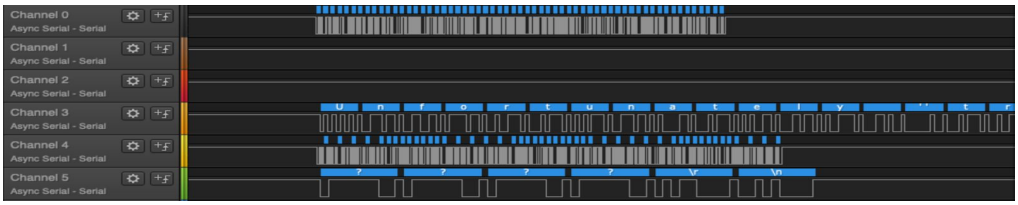
Set up for this lab took about 3 hours. Installing necessary software and setting up the hardware took longer than anticipated and longer than expected given the setup instructions.
I'm going to paste the pinout here so that I have easier availability. "Remaining pins" in my document will refer to all pins excluding the ground pins.



So to begin, I hooked up my ground wires and the MOSI. Then hooked up all remaining wires into consecutive ports starting with 1. Right off the bat, I received a signal on channel 0 in pin 1 and when I set the Async Serial Analyzer to channel 0, I got the message: "This is not the message you're looking for. <WAVES HANDS>\r\n"

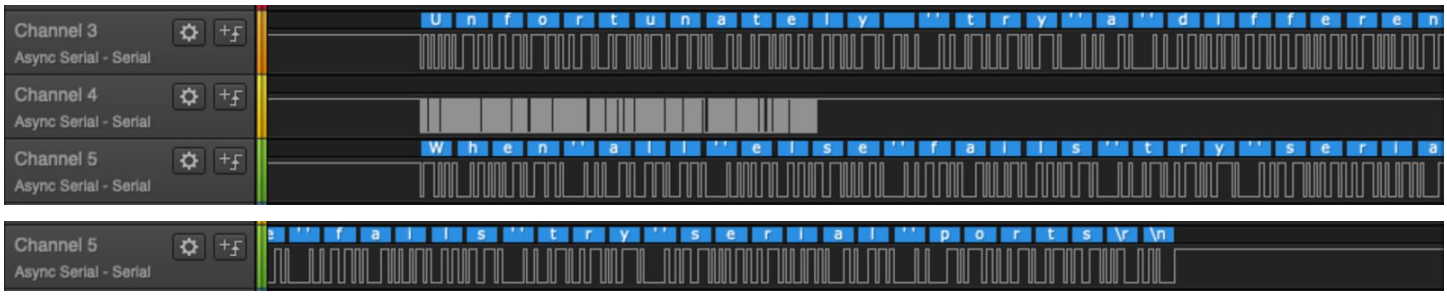
Message 1 obtained, although it was very misleading (lol).

Fumbling around with resetting my pins, I saw on Slack that we should use the serial ports, so with my remaining wires, I led them all to random serial ports to see what I could see. I got a pretty strange output this time… With the same message 1 in channel 0, and another that read "Unfortunately, try a different pin\r\n"



There are 2 unidentifiable signals in channels 4 and 5. Channel 4's signal reads a bunch of values with 'errors' on them. Channel 5's signal is just four '?'s and then '\r\n'. That is likely not a secret message. So I guess I have found one more message.
Message 2: Unfortunately, try a different pin\r\n

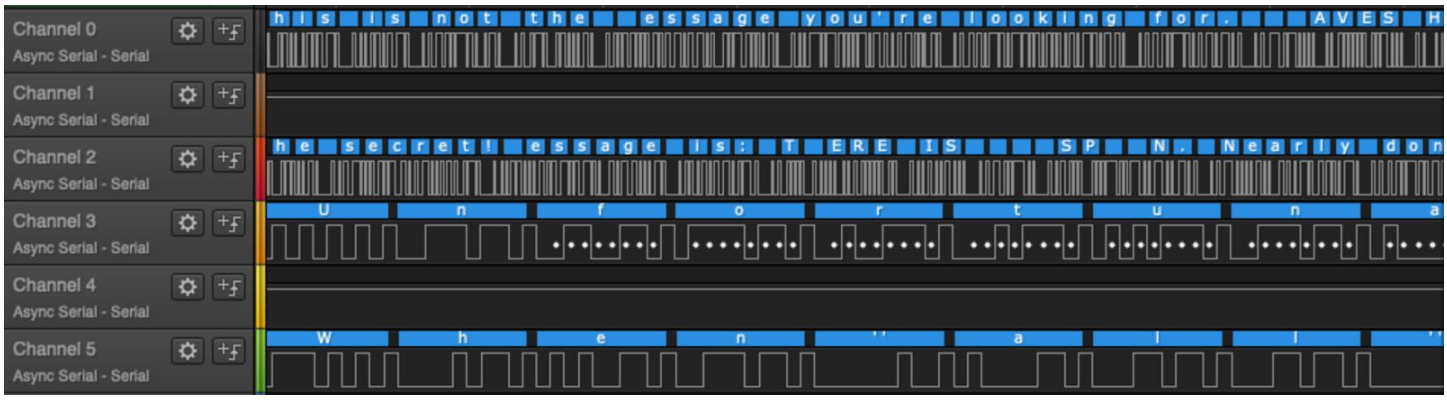
Randomly selecting my remaining pins I am running the program until I find a signal that can be decoded. I keep getting the same original message in channel 0 which contains my message 1 and I kept the same pin in channel 3 leading to pin 8 so message 2 stayed there as well. Channel 5 leads to pin 14 which is now giving me a message, “When all else fails try serial ports\r\n”.



Message 3: When all else fails try serial ports\r\n

Finding the next message was very tricky. I switched pins until I found a signal. I used autobaud and got a signal that decoded into a bunch of ‘!’ with a bit rate of 62500. I thought that this might be a message and so I adjusted the bit rate by 500 up and down until a message began to form. This worked! The exclamation marks turned into ascii text at a bit rate of 60500. The message read “The secret message is: THERE IS NO SPOON. Nearly done with CS373!\r\n”

Here is a screen capture with the beginning of all four messages. Some messages had a different bit rate than others, so they are more spread out than the others.



For the first 3 messages, I found their signals by sliding through the recording until I saw the signal bounce. I was able to decode them with ‘autobaud’ set. For the last message, autobaud did not find the right bit rate in order to decode the message so I had to play around with the bit rate until the message became clear. There was a single framing error in the last message but it didn’t affect the transcription, it still showed the corresponding character.