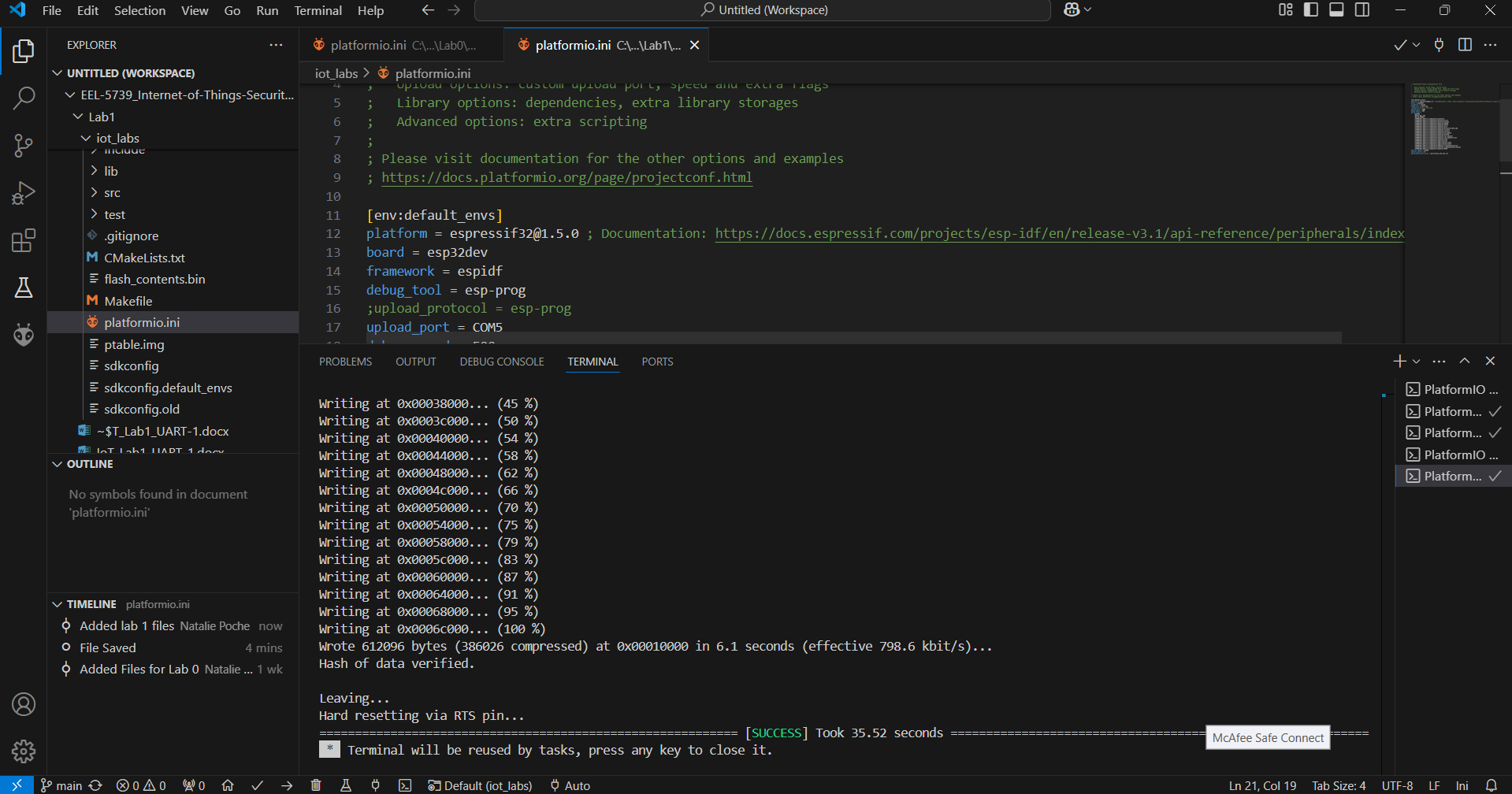
# Lab 1: Attacking a UART Console

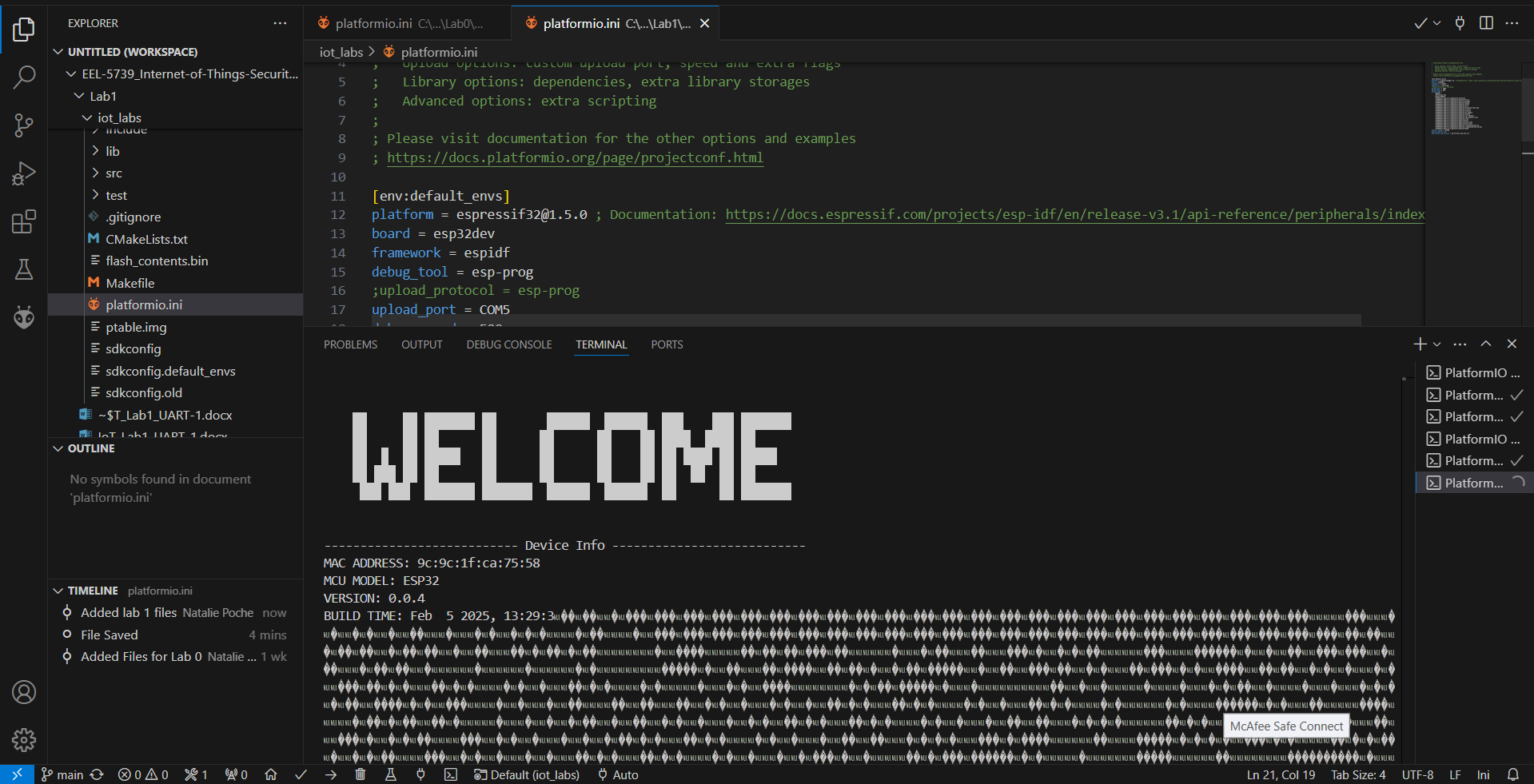
## Uploading the Code (10 Pts):

1. Download the code for Lab 1 from Canvas under files.
2. Extract the code and open it through PlatformIO.
3. Flash the board with the new code.



## Determining Connection Parameters (30 Pts):

1. Make sure the serial monitor is closed. Every time you run the code you must hit the enable(EN) button on the ESP32 board for each attempt to connect.



1. Try to open a serial console connected to the board, does the serial port look properly configured? Why or why not?



The serial port does not look properly configured because it is not human-readable.

– Python script opens a connection to the terminal, you know if you can translate to human language, otherwise it will be nonsense – pressing the button is to reset the board. Screenshots help complete the lab to get partial credit if you get it wrong

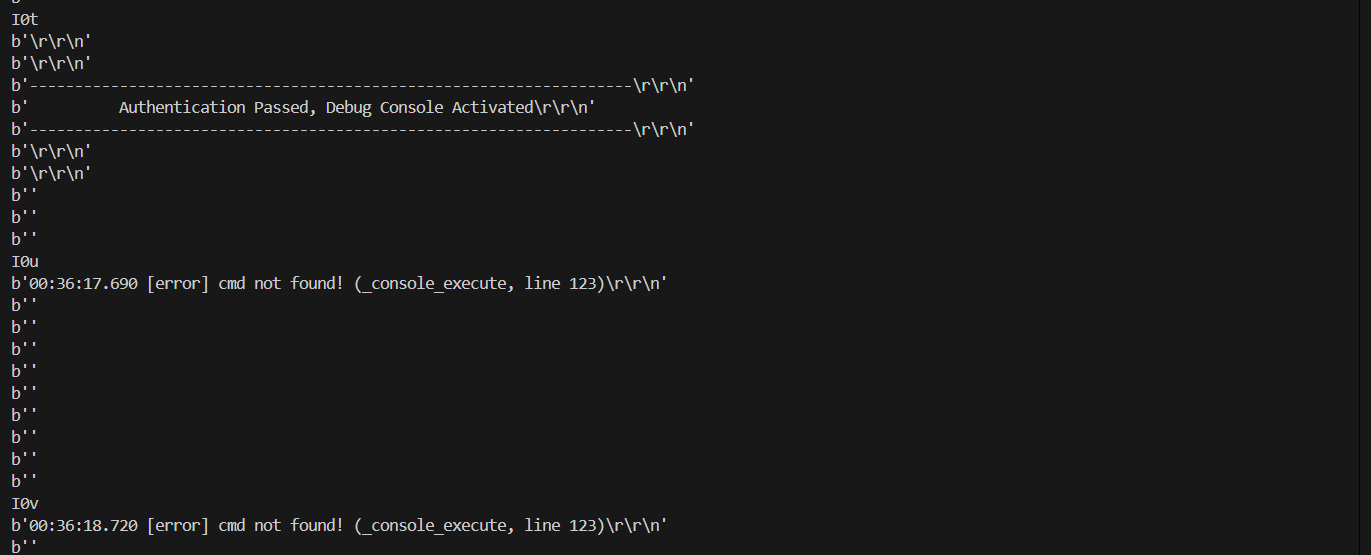
1. What is the proper baud rate and parity of the port? (Hint: use the script we made in class)

Baud rate 9600 and parity odd

## Using the Serial Console (40 Pts):

1. What is the password to the evaluated access level? To simplify and shorten this attack, you can assume you know the following: It is 3 characters. The first character is an uppercase letter (A-Z), the second the numbers (0-9), and the third a lowercase letter (a-z). (Hint: modify the script we made in class) – Perform brute force attack (trying every single possible combination)

I0t



1. Using elevated access, recover the sensitive Wi-Fi information from the device and list it here.

DummyPass



## Closing Thoughts (20 Pts):

1. Describe a method to brute force a password of *n* characters, in which each character can be any valid ASCII character. **You do NOT need to code this in Python.**

A method to brute force a password of n characters in which each character would be a valid ASCII character

1. Describe a method to brute force a password of *unknown* length. **You do NOT need to code this in Python.**

A method to brute force a password of unknown length would be

1. Describe one method in which the UART connection could be better secured.

A method a UART connection could be better secured would be.