EECS 388: Embedded System

Homework: Reverse Engineering Total Points: 2

In this assignment, you will analyze a binary file build for Intel 8051 architecture using Keil software. Refer to the lecture slides and recording on how to obtain and use the tool.

The binary is generated from a program that maintains stable room temperatures in the hospital rooms of critical patients. The program collects temperature every 10 minutes from memory where a sensor writes the temperate data. The program calculates an average from six temperatures collected in an hour (in external memory) along with the current average (i.e., (sum of six temperatures + past average)/7). Finally, the average temperature is compared with the threshold, and based on the comparison, it sends a signal to the output port of the microcontroller. The target device for which the binary is generated is made by a vendor named "**Microchip**," and the model of the device is "**AT89C51**". The binary file is attached as a file "unknown" in the assignment.

Based on the program behavior through the disassembly window of Keil (as shown in the class), find out the following information from the binary:

1. What is the memory address of the "START" label? (0.1 point)
2. What is the initial return address of the first function call? (0.1 point)
3. How many times does the program collect the data from external memory (ROM)? (0.2 point)
4. What is the value in decimal of the last hour's temperature (before averaging)? (0.2 points)
5. What is the mean value in decimal of the temperature after averaging it? (0.2 point)
6. What is the threshold value in decimal? (0.2 point)
7. What temperature values in decimal did you observe in the external memory? Also, report their locations. (0.3 point)
8. Which output port of the microcontroller is used to send the signal (i.e., P1 or P0, or P2, etc)? (0.2 point)
9. Is there any signal sent based on the temperature data found in the memory? (0.2 point)
10. In the location "C:0x034D," we can observe that the program is jumping to the "START" label using the "JNZ" opcode. Let's say a rookie programmer used "ACALL" instead of the "JNZ" opcode. What could be the possible consequences if we use "ACALL" instead of "JNZ"? (0.3 point)

Submit your answer as typed using an MS Word file.