HW 3 Part 1

Justin Wen jhw89

1. The cmp eax ebx was changed to cmp eax eax so it was always true. This exe was saved in CRACKMESOLUTION.exe. I found the location following the steps in the slides.
2. First I put in my name, Justin into the program. After looking through the ollydbg and the IDA program at the same time I traced 2 locations where there were XOR calls to a constant value. From this I inferred that the program probably compared some value from the name to get the serial value. The two values I saw were 0x5678 and 0x1234 in hexadecimal. Following the code I assumed they were both used on the same value, which I assumed to be some function of the Name field. From there I tried combinations of getting the value of my name and getting the XOR value after both constants. I tried hex values as is, case insensitive upper, case insensitive lower, then decimal values as is and finally got the proper value and case insensitive upper for decimal values. The value for my name, “Justin”, came out to be 17809. It worked for any other value I tried as well.