(30 pts) CS3843 Computer Organization Exam #2 Name/abc123:_____
(30 pts) Part 1 - BONUS

Short Answer (24 pts)

1. (6 pts) Given the memory shown below and esp = 0x18FC20. What is value of eax after executing a "pop eax" instruction? What is esp after executing the pop instruction? Given that ecx = 0x000000FE, show where it goes (underneath the correct values) on the stack when a "push ecx" is now executed.

```
0018FC1C   FE 22 B0 CA  EF BE CE D1  12 58 22 F0  3A 81 BB 6E

           ___________  ___________  ___________  ___________ ← show ecx on 1 of these


eax = ____________________     esp = ____________________
```

2. (18 pts) Inside func0 after setting up the standard stack frame, ebp = 0x15D10, esp=0x15D04, that [ebp+0x08] = 0x51CF3, [ebp+12] = 0x401305, [ebp-8] = 0x1000.

```
CODE A:                  vs.        CODE B:                  .
mov ebx, [ebp - 8]                  lea ebx, [ebp - 8]
push ebx                            push ebx
mov ecx, [ebp + 0x0C]               mov ecx, [ebp + 0x0C]
push ecx                            push ecx
call func1                          call func1

__________                          __________  ← (2 pts) Show instruction that goes here
```

   a. (10 pts) Complete the stack for Code A. Show only any differences on the Code B stack. If you do not know a value, then write the description. Yep, 1 point per correct answer.

Stack	CODE A:		CODE B:
0x15CF4			← Show in code A, the ebp value
0x15CF8			
0x15CFC			
0x15D00			
0x15D04			
0x15D08			
0x15D0C			
0x15D10	Prior ebp = ???		
0x15D14	Return Address func0		
0x15D18			
0x15D1C			

b. (6 pts) Inside func1, assume that the following instruction is executed: "mov [ebp+12],0xABCD1234." Describe the difference between what happens in Code A vs. what happens in Code B.

Reading Code (6 pts)

3. (6 pts) **Carefully** examine the following assembly instructions, and answer the subsequent questions.

```
400020 mov eax, [ebp + 0x0C]     ; value here = 0x00000082
400023 mov cl,  [ebp + 0x08]     ; value here = 0x80
400026 cmp cl, al
400028 jb  label1          ; label1 is at address 40003C, jb <jmp below> is unsigned
...
Label1:
40003C sub cl, al          ; cl = cl - al
40003E jl label2           ; jae <jmp less> is signed
...
Label2:                    ; note these addresses are less than those above
400010 neg cl
```

a. (1 pt) Given the current values, is the jb taken? (YES, NO)

b. (1 pt) Assuming al and cl remain unchanged at address 40003C, is the jl taken? (YES, NO)

c. (2 pts) What is the decimal value of cl after executing the sub instruction at 0x40003C? Show both the signed and unsigned values.

d. (2 pts) What is the value of cl after executing the NEG instruction at address 400010?