(150 pts) CS3843 Computer Organization Exam #2 Name/abc123:________________
(80 pts) Part 1

Fast Answer: (40 pts, 2 pts each)

1. Exactly how many bytes are in 1 KB of memory? ______

2. Given a 1 byte operand, what is the range of signed displacement values? ______

3. The stack is always aligned to a _____ byte boundary.

4. The following instruction reserves stack space for (**parameters, local variables, global variables, registers**).

   `sub esp, 0x20`

5. (4 pts) When a value is popped from the stack, the data is read (**before, after**) esp is (**incremented, decremented**).

6. Given the stack frame set up we have seen and discussed in class, mov eax, [ebp + 8] will move what into eax? (**parameter, local variable, global variable**)

7. Given that same stack frame set up, what will be in eax after executing this instruction:

   `mov eax, [ebp + 4]`? __________ Hint: It is NOT any of the selections above.

8. There are two instructions that efficiently set a register to zero. List one of them. ________

9. After executing either of those instructions, what is the value of the ZERO flag? ________

10. A “push edx” instruction uses which register implicitly? _______

11. Ecx is implicitly used by which type of instructions? ______

12. For what type of instructions are edi/esi used implicitly? _______

13. The “trap” flag is used to ______. Circle one (single-step, enable interrupts, set privilege level).

14. Given that cl = 0xA2, show the value of eax after this instruction: **`movsx eax,cl`**

15. Given that cl = 0xEC, show the value of eax after this instruction: **`movzx eax,cl`**

16. List the 3 types of memory partitions as discussed in class.

17. In which of the 3 types of memory are static variables stored?

18. There are two things the NOP instruction accomplishes while doing nothing, list one.

19. Given ecx = 0x0000007B, so cl=0x7B, what is the minimum value that when added, would set the OVERFLOW flag?

```
add cl, __________ ; minimum value to cause OF to be set
```

Short Answer (40 pts)

20. (4 pts) Given esp = 0x18F448, what is value of eax after executing a “pop eax” instruction? What is esp after executing the pop instruction?

```
0018FF44   B0 CA CC BE EF BE AD DE     eax = __________  esp = __________
```

21. (12 pts) Given that [ebp - 0x14] refers to a local variable named tmpD = 0xDE76A1 and ebp = 0x1288C.

```
CODE A:                          CODE B:              .
mov ecx, [ebp - 0x14]      vs.      lea ecx, [ebp – 0x14]
push ecx                            push ecx
call func1                          call func1
```

a. (4 pts) Briefly describe the difference between the CODE A instructions and the CODE B instructions.

b. (4 pts) For each one, show what ecx looks like on the stack.

Stack	CODE A:		CODE B:
0x12880			

c. (4 pts) Show the matching C function call for each.

22. (4 pts) What 2 operations are performed by a call instruction?

23. (4 pts) What 2 operations are performed by a ret instruction?

24. (14 pts) Examine the following assembly instructions, and answer the subsequent questions.

```
0020 mov eax, [ebp + 0x10] ; value here = 0x00000052
0023 mov ecx, [ebp + 0x08] ; value here = 0x0000009C
0026 cmp al, cl
0028 jg  label       ; label is at address 003C, jg is signed
002A nop
002B
...
003C label: sub al, cl
```

a. (3 pts) Inside a function, assuming that ebp is used for the stack frame, what is at the address ebp+0x10 with respect to a C function call?

b. (2 pts) Given a signed operation, al is (**greater than, less than, equal to**) cl?

c. (3 pts) What is the address from which the offset to the jg is calculated? __________

d. (3 pts) What is the value of the offset for the jg instruction? __________

e. (3 pts) What is the difference between the “cmp” instruction at address 26 and the “sub” instruction at address 3C?

f. (2 pts) Suppose ecx = 0x12345678 prior to executing the code above. What is the new value after executing the code at address 23.

ecx = 0x________________