(150 pts) CS3843 Computer Organization Exam #2 Name/abc123:_____
(70 pts) Part 2

Stack (30 pts)

1. (10 pts) Complete the stack frame given the following assembly code when **`eip starts at 0x401A45 and ends at 0x4019B4`**. Make sure to fill in the stack addresses that are not already complete and any other blank spaces.

   Given: **`esp = 0x12F00, ebp = 0x12F04 when eip = 0x401A45`**

```
Func0:
00401A45 8B 55 0C              mov     edx, [ebp+0Ch]
00401A48 52                    push    edx
00401A49 8B 45 08              mov     eax, [ebp+8]
00401A4C 50                    push    eax
00401A4D E8 4E FF FF FF        call    Func1
00401A52 83 C4 10              add     esp, 8

Func1:
004019A0 55                    push    ebp
004019A1 8B EC                 mov     ebp, esp
004019A3 83 EC 08              sub     esp, 8
004019A6 C7 45 F8 00 00 00 00  mov     [ebp-8], 0
004019AD C7 45 FC 00 00 00 00  mov     [ebp-4], 123Fh
004019B4
```

Address	Value	Description
0x12F00	**00 00 00 00**	Local variable in Func0
0x12F04	**80 2F 01 00**	Previous ebp
	D3 12 40 00	Return Address of function calling Func0
	F2 82 C1 0F	
	48 F0 18 00	
	?? ?? ?? ??	Unknown

2. (4 pts) What is the address of Func1? _____

3. (4 pts) Show how the assembler calculated the offset for the call to Func1. You do not have to do the math.

4. (4 pts) Why do we add 8 to esp at address 0x401A52? _____

5. (4 pts) Why do we subtract 8 at address 0x4019A3? _____

6. (4 pts) What is the value of ebp when eip = 0x4019B4? _____

Reading Assembly (40 pts)

7. (20 pts) Intelligently comment each line of code.

```
00401A68 B9 0B 00 00 00   mov ecx, 0Bh           ; _____________________________

00401A6D BE 84 D3 40 00   mov esi, offset ConstantData; _____________________________

00401A72 8D 7D CC         lea edi, [ebp-34h]     ; _____________________________

00401A75 F3 A5            rep movsd   ; _____________________________

00401A77 66 A5            movsw       ; _____________________________
```

8. (4 pts) What does the code above do?

9. (2 pts) How many times will it repeat? _____

10. (2 pts) How many bytes are copied? _____

11. (2 pts) In what type of memory is ConstantData stored? _____

12. (10 pts) Consider the code below: (I cut out some pieces for brevity) Comment each of the groups of code above the blank line. Looking for 1 – 3 sentence descriptions, so include as much detail as you can. No need to comment each line, don't care, want to know what the code does collectively.

```
StartOfLoop:
004019B6 8B 45 F8        mov     eax, [ebp-8]
004019B9 83 C0 01        add     eax, 1
004019BC 89 45 F8        mov     [ebp-8], eax
```

; (1 pt) _____

```
004019BF 8B 4D F8              mov     ecx, [ebp-8]
004019C2 3B 4D 0C              cmp     ecx, [ebp+0Ch]
004019C5 7D 36                 jge     EXIT
```

; (3 pts) _____

```
004019CD 0F BE 02              movsx   eax, byte ptr [edx]
004019D6 0F BE 11              movsx   edx, byte ptr [ecx]
004019D9 33 C2                 xor     eax, edx
004019E1 88 01                 mov     [ecx], al
```

; (3 pts) _____

```
004019EC 8B 45 FC              mov     eax, [ebp-4]
004019EF 3B 45 14              cmp     eax, [ebp+14h]
004019F2 75 07                 jnz     0x4019FB
004019F4 C7 45 FC 00 00 00 00  mov [ebp-4], 0
```

; (3 pts) _____

```
004019FB EB B9                 jmp     StartOfLoop
```

; (0 pts) _jumps to beginning of loop_