Form A

COMP 3350-002 / Fall 2014 / J. Overbey

– Exam 2 Bonus / Form A –

Name: Solutions **Score:** ____/____

For questions 1–2, consider the following data section.

```
.data
array WORD 1122h, 3344h, 5566h, 7788h
bytez BYTE 12h, 34h, 56h, -1
```

1. This .data section will be stored in memory as a sequence of 12 bytes. Write the values of these bytes, in *hexadecimal*, starting with the byte at the lowest memory address.

22 11 44 33 66 55 88 77 12 34 56 FF

2. Suppose the first byte of `array` is at address **00404000h**. What is the value of EAX after each of the following instruction sequences executes? Write your answers in *hexadecimal*. Do not have to write leading 0's

a. `movzx eax, array` ; EAX = 0000 1122

b. `movzx eax, WORD PTR [array + 1]` ; EAX = 0000 4411

c. `movzx eax, WORD PTR [array + 2]` ; EAX = 0000 3344

d. `mov eax, OFFSET array` ; EAX = 00404000

e. `lea eax, array` ; EAX = 00404000

f. `lea eax, [array + 2]` ; EAX = 00404002

g. `mov eax, LENGTHOF array` ; EAX = 4

h. `mov eax, SIZEOF array` ; EAX = 8

i. `movzx eax, BYTE PTR [array]` ; EAX = 00000022

j. `lea eax, bytez` ; EAX = 00404008

k. `lea eax, [bytez + 2]` ; EAX = 0040400A

l. `movzx eax, WORD PTR [bytez]` ; EAX = 00003412

m. `movzx eax, WORD PTR [bytez + 1]` ; EAX = 00005634

n. `mov eax, DWORD PTR [bytez]` ; EAX = FF563412

o. `movzx eax, WORD PTR [bytez + 2]` ; EAX = 0000FF56

3. Suppose your .data section contains

```
.data
array WORD 0FFEEh, DDCCh, 5566h, 7788h
```

and you want to display the values in the array in hexadecimal, one per line:

```
0000FFEE
0000DDCC
00005566
00007788
```

WORD PTR is optional (can be omitted since array is a WORD array)

2 could be SIZEOF WORD

Fill in the missing instruction.

```
        mov ecx, 0                          ; ECX will count up from 0
top:    movzx eax, [array+2*ecx]            ; Load the next array element into EAX
        call WriteHex                       ; Display that value...
        call Crlf                           ; ...followed by a newline
        inc ecx                             ; Increase ECX
        cmp ecx, LENGTHOF array             ; Are we done?
        jb top                              ; Jump back to show next element
```

WORD PTR

4. How to each of the following instructions affect the value of ESP?

a.	`push eax`	○ Adds 4 to ESP	● Subtracts 4 from ESP	○ ESP does not change
b.	`pop eax`	● Adds 4 to ESP	○ Subtracts 4 from ESP	○ ESP does not change
c.	`call eax`	○ Adds 4 to ESP	● Subtracts 4 from ESP	○ ESP does not change
d.	`ret 0`	● Adds 4 to ESP	○ Subtracts 4 from ESP	○ ESP does not change

5. Suppose a procedure:

- Receives two stack arguments.
- Has a prologue that issues `enter 0,0` and then pushes ESI.

a. The stack frame for this procedure consists of five 4-byte values (suppose they are stored in the memory addresses shown below). In a word or two, describe what is stored in each 4-byte entry of the stack frame.

0013FF6Ch	Argument 2	
0013FF68h	Argument 1	
0013FF64h	Return Address	
0013FF60h	Saved EBP	←EBP
0013FF5Ch	Saved ESI	←ESP

b. Suppose, after the stack frame is created, you want to load the first argument into EAX. The normal way to do this would be to use the instruction

```
mov eax, [ebp+8]
```

could have DWORD PTR

With the stack frame above, you could also use `mov eax, DWORD PTR [esp+12]`