HOMEWORK 4 SOLUTIONS

QUESTIONS 4–10: ANALYSIS OF MEMORY ACCESSES

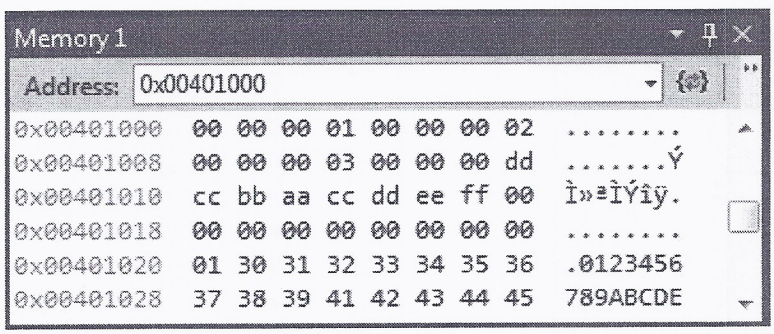
4.
```
main PROC        ; Display the last element of arr1
     mov esi, arr1      ESI = 1
     mov ecx, LENGTHOF arr1   ECX = 3
     call lastElement
     call WriteHex
     exit
main ENDP

lastElement PROC          1 + 3*4          - 4     = 9
     mov eax, DWORD PTR [esi + ecx*SIZEOF SDWORD - SIZEOF SDWORD]
     ret
lastElement ENDP
```

a. If `start` = 00401000h, what value is passed in ESI to the `lastElement` procedure? 1 (00000001h)

b. Consider the memory operand for the `mov` instruction in the `lastElement` procedure. If `start` = 00401000h, what memory address does it access? 00000009h

c. The following image shows the 48 bytes of the memory, beginning at 00401000h. `start` = 00401000h, what four bytes comprise the DWORD value that is copied into EAX? Circle them. If the memory address that is accessed is not shown, write "Not shown."



Not shown

d. For every program, the expected output is 00000003—the last value in the `arr1` array.. What will the *actual* output be? Or will the program crash due to an invalid memory access?

Crash

5.

```
main PROC        ; Display the last element of arr1
     mov esi, OFFSET arr1
     mov ecx, LENGTHOF arr1
     call lastElement
     call WriteHex
     exit
main ENDP

lastElement PROC
     mov eax, DWORD PTR [esi + ecx*SIZEOF SDWORD]
     ret
lastElement ENDP
```

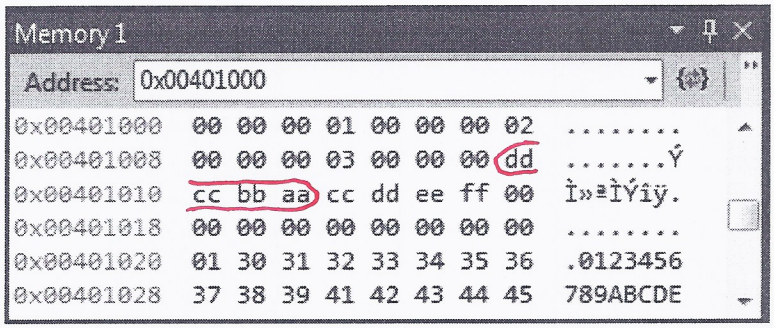
ESI = 00401003h
ECX = 3

4010036 + 3*4 = 40100Fh

a. If `start` = 00401000h, what value is passed in ESI to the `lastElement` procedure? 00401003h

b. Consider the memory operand for the `mov` instruction in the `lastElement` procedure. If `start` = 00401000h, what memory address does it access? 0040100Fh

c. The following image shows the 48 bytes of the memory, beginning at 00401000h. `start` = 00401000h, what four bytes comprise the DWORD value that is copied into EAX? Circle them. If the memory address that is accessed is not shown, write "Not shown."



d. For every program, the expected output is 00000003—the last value in the `arr1` array.. What will the *actual* output be? Or will the program crash due to an invalid memory access?

AABBCCDD

7.

```
main PROC        ; Display the last element of arr1
     mov esi, OFFSET arr1
     mov ecx, LENGTHOF arr1
     call lastElement
     call WriteHex
     exit
main ENDP

lastElement PROC
     mov eax, DWORD PTR [esi + ecx - SIZEOF SDWORD]
     ret
lastElement ENDP
```

401003h

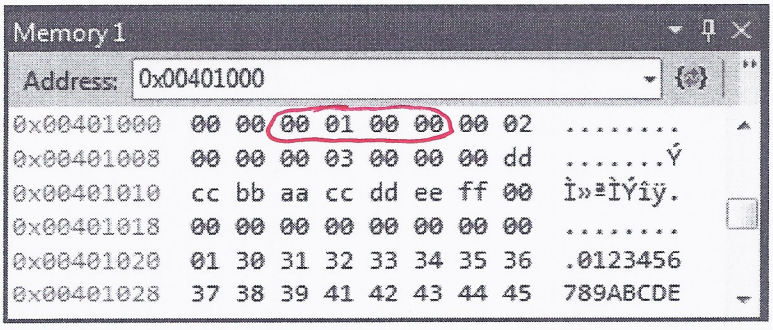
3

401003h + 3 − 4 = 401002h

a. If `start` = 00401000h, what value is passed in ESI to the `lastElement` procedure? 00401003h

b. Consider the memory operand for the `mov` instruction in the `lastElement` procedure. If `start` = 00401000h, what memory address does it access? 00401002h

c. The following image shows the 48 bytes of the memory, beginning at 00401000h. `start` = 00401000h, what four bytes comprise the DWORD value that is copied into EAX? Circle them. If the memory address that is accessed is not shown, write "Not shown."



d. For every program, the expected output is 00000003—the last value in the `arr1` array.. What will the *actual* output be? Or will the program crash due to an invalid memory access?

00000100h

9.
```
main PROC        ; Display the last element of arr1
     mov esi, OFFSET arr1
     mov ecx, LENGTHOF arr1
     call lastElement
     call WriteHex
     exit
main ENDP

lastElement PROC
     mov eax, DWORD PTR [esi + ecx*SIZEOF SDWORD - 2*SIZEOF SDWORD]
     ret
lastElement ENDP
```

00401003h

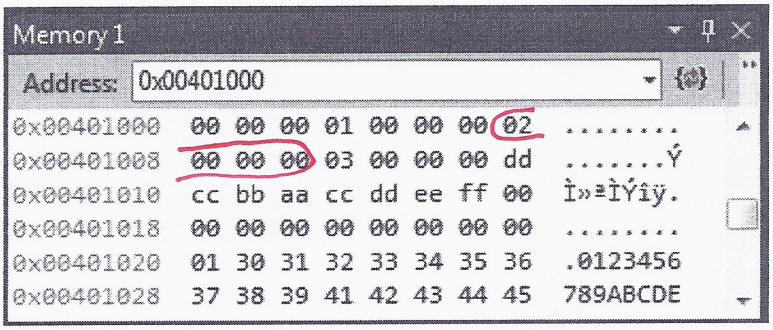
3

4010037h + 3*4 − 8 = 4010074h

a. If `start` = 00401000h, what value is passed in ESI to the `lastElement` procedure?

b. Consider the memory operand for the `mov` instruction in the `lastElement` procedure. If `start` = 00401000h, what memory address does it access?

c. The following image shows the 48 bytes of the memory, beginning at 00401000h. `start` = 00401000h, what four bytes comprise the DWORD value that is copied into EAX? Circle them. If the memory address that is accessed is not shown, write "Not shown."



d. For every program, the expected output is 00000003—the last value in the `arr1` array.. What will the *actual* output be? Or will the program crash due to an invalid memory access?

00000002

10.
```
main PROC        ; Display the last element of arr1
     mov esi, OFFSET arr1
     mov ecx, LENGTHOF arr1
     call lastElement
     call WriteHex
     exit
main ENDP

lastElement PROC
     mov eax, DWORD PTR [ecx + esi*SIZEOF SDWORD - SIZEOF SDWORD]
     ret
lastElement ENDP
```

00401003h

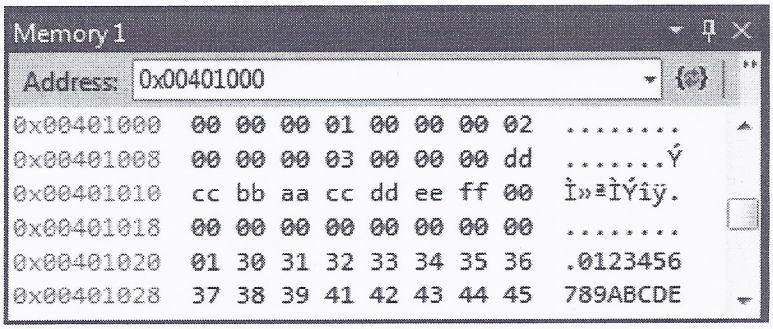
3

3 + 401003h * 4 - 4 = 0100400Bh

a. If `start` = 00401000h, what value is passed in ESI to the `lastElement` procedure? 00401003h

b. Consider the memory operand for the `mov` instruction in the `lastElement` procedure. If `start` = 00401000h, what memory address does it access? 0100400Bh

c. The following image shows the 48 bytes of the memory, beginning at 00401000h. `start` = 00401000h, what four bytes comprise the DWORD value that is copied into EAX? Circle them. If the memory address that is accessed is not shown, write "Not shown."



Not shown

d. For every program, the expected output is 00000003—the last value in the `arr1` array.. What will the *actual* output be? Or will the program crash due to an invalid memory access?

Crash