

COAL Lab 04

Name: Sufiyaan Usmani

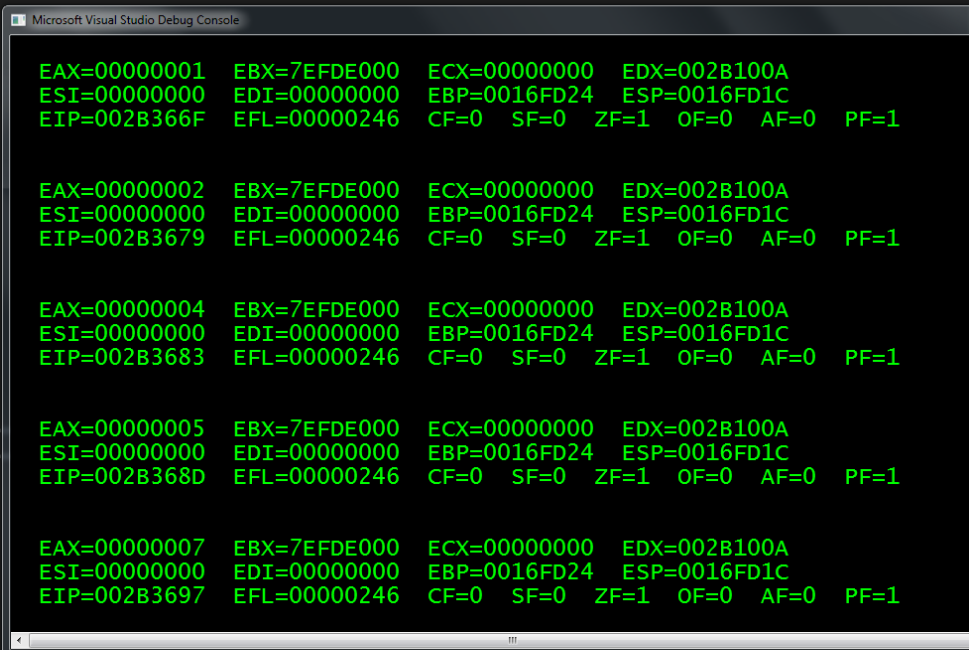
Roll No: 21K-3195

Section: BCS-3J

Instructor: Sir Kashan Hussain

Task 1:

```
1 ; Sufiyaan Usmani
2 ; 21K-3195
3 ; BCS-3J
4 ; Task 1
5
6 INCLUDE Irvine32.inc
7
8 .data
9     arr DWORD 7, 4, 1, 5, 2
10
11 .code
12     main PROC
13         mov eax, 0
14         mov eax, arr[8]
15         call DumpRegs
16
17         mov eax, arr[16]
18         call DumpRegs
19
20         mov eax, arr[4]
21         call DumpRegs
22
23         mov eax, arr[12]
24         call DumpRegs
25
26         mov eax, arr[0]
27         call DumpRegs
28         exit
29     main ENDP
30 END main
```

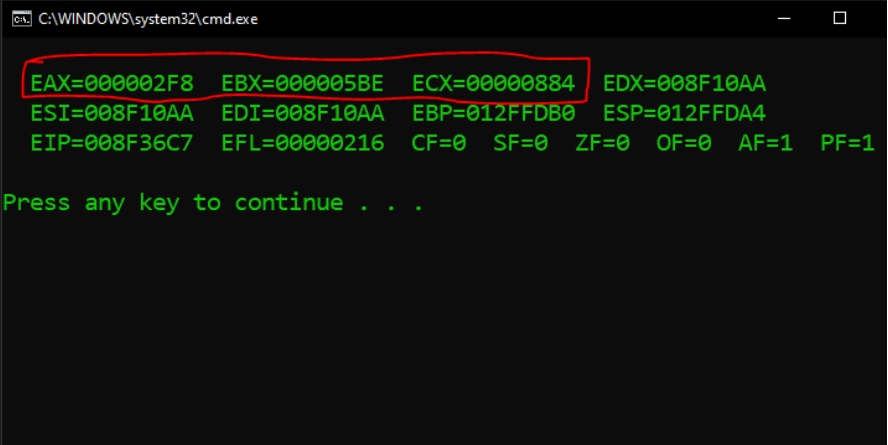


The screenshot shows the Microsoft Visual Studio Debug Console with the following register values at five different points in the program execution:

Point	EAX	EBX	ECX	EDX	ESI	EDI	EBP	ESP	EIP	EFL	CF	SF	ZF	OF	AF	PF
1	00000001	7EFDE000	00000000	002B100A	00000000	00000000	0016FD24	0016FD1C	002B366F	00000246	0	0	1	0	0	1
2	00000002	7EFDE000	00000000	002B100A	00000000	00000000	0016FD24	0016FD1C	002B3679	00000246	0	0	1	0	0	1
3	00000004	7EFDE000	00000000	002B100A	00000000	00000000	0016FD24	0016FD1C	002B3683	00000246	0	0	1	0	0	1
4	00000005	7EFDE000	00000000	002B100A	00000000	00000000	0016FD24	0016FD1C	002B368D	00000246	0	0	1	0	0	1
5	00000007	7EFDE000	00000000	002B100A	00000000	00000000	0016FD24	0016FD1C	002B3697	00000246	0	0	1	0	0	1

Task 2:

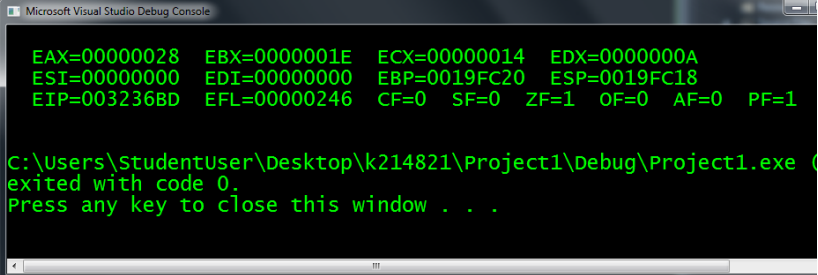
```
1 ; Sufiyaan Usmani
2 ; 21K-3195
3 ; BCS-3J
4 ; Task 2
5
6 INCLUDE Irvine32.inc
7
8 .data
9     arrayB BYTE 10, 20, 30
10    arrayW WORD 150, 250, 350
11    arrayD DWORD 600, 1200, 1800
12    sum1 DWORD 0
13    sum2 DWORD 0
14    sum3 DWORD 0
15
16 .code
17     main PROC
18         movzx eax, arrayB[0]
19         movzx ebx, arrayW[0]
20         add eax, ebx
21         add eax, arrayD[0]
22         mov sum1, eax
23
24         movzx eax, arrayB[1]
25         movzx ebx, arrayW[2]
26         add eax, ebx
27         add eax, arrayD[4]
28         mov sum2, eax
29
30         movzx eax, arrayB[2]
31         movzx ebx, arrayW[4]
32         add eax, ebx
33         add eax, arrayD[8]
34         mov sum3, eax
35
36         mov eax, sum1
37         mov ebx, sum2
38         mov ecx, sum3
39         call DumpRegs
40         exit
41     main ENDP
42     END main
```



Task 3:

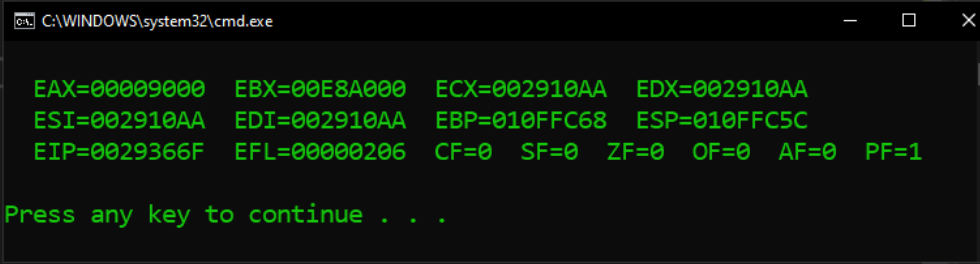
This task was done in class

```
1 ; Sufiyaan Usmani
2 ; 21K-3195
3 ; BCS-3J
4 ; Task 3
5
6 INCLUDE Irvine32.inc
7
8 .data
9     array1 BYTE 10, 20, 30, 40
10    array2 BYTE 4 DUP(?)
11
12 .code
13     main PROC
14         mov eax, 0
15         mov al, array1[3]
16         mov array2[0], al ; array2: 40
17
18         mov al, array1[2]
19         mov array2[1], al ; array2: 40, 30
20
21         mov al, array1[1]
22         mov array2[2], al ; array2: 40, 30, 20
23
24         mov al, array1[0]
25         mov array2[3], al ; array2: 40, 30, 20, 10
26
27         ; printing values of array2
28         mov eax, 0
29         mov ebx, 0
30         mov ecx, 0
31         mov edx, 0
32
33         mov al, [array2]
34         mov bl, [array2 + 1]
35         mov cl, [array2 + 2]
36         mov dl, [array2 + 3]
37         call DumpRegs
38         exit
39     main ENDP
40     END main
```



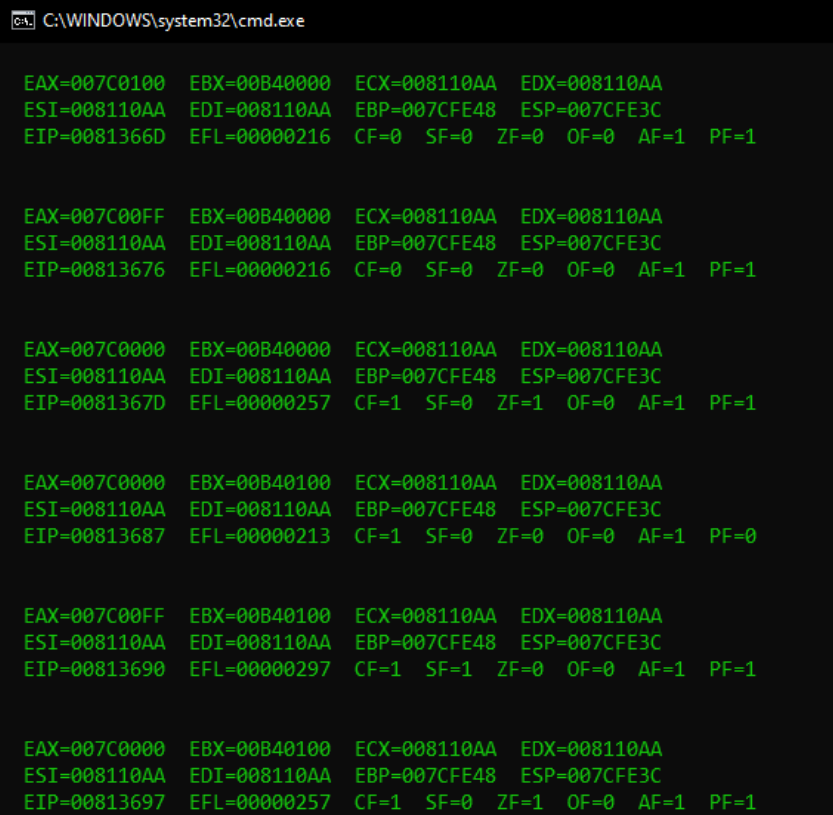
Question from lab manual

```
1 ; Sufiyaan Usmani
2 ; 21K-3195
3 ; BCS-3J
4 ; Task 3
5
6 INCLUDE Irvine32.inc
7
8 .data
9     val1 SDWORD 8000h
10
11 .code
12     main PROC
13         mov eax, val1
14         add eax, 1000h
15         call DumpRegs
16         exit
17     main ENDP
18     END main
```



Task 4:

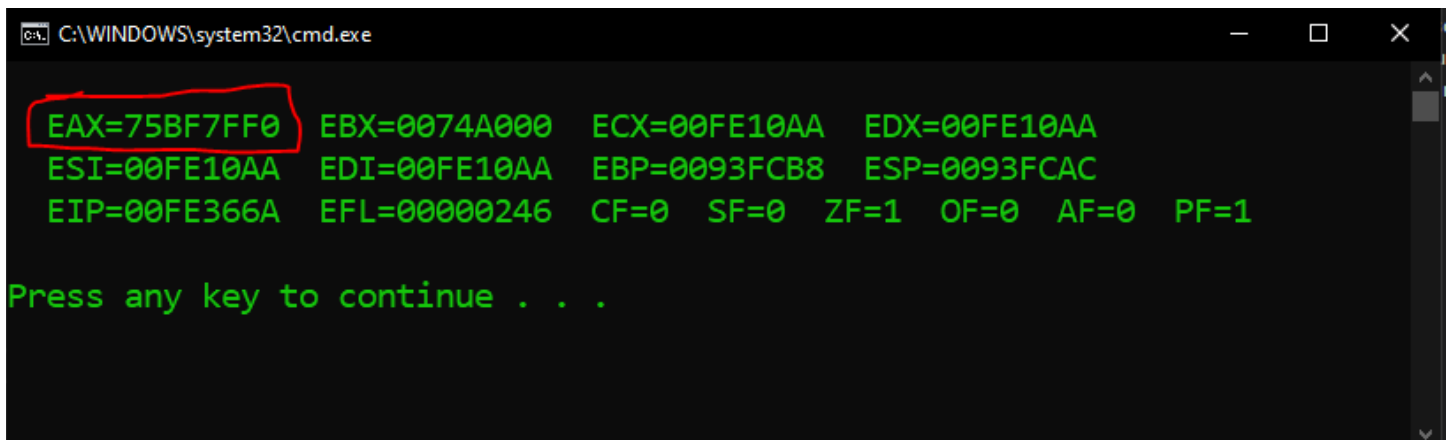
```
1 ; Sufiyaan Usmani
2 ; 21K-3195
3 ; BCS-3J
4 ; Task 4
5
6 INCLUDE Irvine32.inc
7
8 .code
9     main PROC
10         mov ax, 0FFh
11         add ax, 1
12         call DumpRegs
13         sub ax, 1
14         call DumpRegs
15         add al, 1
16         call DumpRegs
17         mov bh, 6Ch
18         add bh, 95h
19         call DumpRegs
20         mov al, 2
21         sub al, 3
22         call DumpRegs
23         inc al
24         call DumpRegs
25         exit
26     main ENDP
27     END main
28
```



Task 5:

```
1 ; Sufiyaan Usmani
2 ; 21K-3195
3 ; BCS-3J
4 ; Task 5
5
6 INCLUDE Irvine32.inc
7
8 .code
9     main PROC
10         mov ax, 7FF0h
11         add al, 10h
12         add ah, 1
13         add ax, 2
14         call DumpRegs
15         exit
16     main ENDP
17 END main
```

(a)



C:\WINDOWS\system32\cmd.exe

```
EAX=75BF7FF0 EBX=0074A000 ECX=00FE10AA EDX=00FE10AA
ESI=00FE10AA EDI=00FE10AA EBP=0093FCB8 ESP=0093FCAC
EIP=00FE366A EFL=00000246 CF=0 SF=0 ZF=1 OF=0 AF=0 PF=1

Press any key to continue . . .
```

(b)

```
C:\WINDOWS\system32\cmd.exe

EAX=75BF7F00  EBX=00CC0000  ECX=00F510AA  EDX=00F510AA
ESI=00F510AA  EDI=00F510AA  EBP=00BBFC50  ESP=00BBFC44
EIP=00F5366C  EFL=00000247  CF=1  SF=0  ZF=1  OF=0  AF=0  PF=1

Press any key to continue . . .
```

(c)

```
C:\WINDOWS\system32\cmd.exe

EAX=75BF8000  EBX=00414000  ECX=00C110AA  EDX=00C110AA
ESI=00C110AA  EDI=00C110AA  EBP=006FFAE0  ESP=006FFAD4
EIP=00C1366F  EFL=00000A92  CF=0  SF=1  ZF=0  OF=1  AF=1  PF=0

Press any key to continue . . .
```

(d)

```
C:\WINDOWS\system32\cmd.exe

EAX=75BF8002  EBX=0038D000  ECX=001110AA  EDX=001110AA
ESI=001110AA  EDI=001110AA  EBP=004FF7AC  ESP=004FF7A0
EIP=00113673  EFL=00000282  CF=0  SF=1  ZF=0  OF=0  AF=0  PF=0

Press any key to continue . . .
```