

Lab 1

1.) Exchanging with direct addressing

```
DOSBox 0.74-3, Cpu speed: 3000 cycles, Frameskip 0, Program: DEBUG x
```



```
-a 100
0859:0100 mov al,[0200]
0859:0103 mov bl,[0201]
0859:0107 mov [0200],bl
0859:010B mov [0201],al
0859:010E
-g 100
AX=0000 BX=0000 CX=0000 DX=0000 SP=FFFF BP=0000 SI=0000 DI=0000
DS=0859 ES=0859 SS=0859 CS=0859 IP=0100 NU UP EI NG NZ NA PE NC
0859:0100 A00002 MDU AL,[0200] DS:0200=00
```

Exchanging with register relative addressing

```

DOSBox 0.74-3, Cpu speed: 3000 cycles, Frameskip 0, Program: DEBUGX x
-
-a 100
0059:0100 mov bp, 200
0059:0103 mov al, 0fbpl
0059:0106 mov bl, 10fbpl
0059:0109 mov 0fbpl, bl
0059:010C mov 10fbpl, al
0059:010F
-g 100
AX=0000 BX=0000 CX=0000 DX=0000 SP=FFFE BP=0000 SI=0000 DI=0000
DS=0059 ES=0059 SS=0059 CS=0059 IP=0100 NV UP EI NG NZ NA PE NC
0059:0100 BD0002 MOV BP,0200

```

Exchanging with Base-Indexed addressing

```
DOSBox 0.74-3, Cpu speed: 3000 cycles, Frameskip 0, Program: DEBUG x
-
-a 100
0059:0100 mov bp, 200
0059:0103 mov si, 0
0059:0106 mov al, [bp+si]
0059:0108 mov bl, [bp+si+10]
0059:010B mov [bp+si], bl
0059:010D mov [bp+si+10], al
0059:0110
-g 100
AX=0000 BX=0000 CX=0000 DX=0000 SP=FFFE BP=0000 SI=0000 DI=0000
DS=0059 ES=0059 SS=0059 CS=0059 IP=0100 NV UP EI NG NZ NA PE NC
0059:0100 BD0002          MOV     BP,0200
```

Using E command to add data

```
DOSBox 0.74-3, Cpu speed: 3000 cycles, Frameskip 0, Program: DEBUGX x
```

```
-  
-  
-  
-  
-  
-  
-  
-  
-  
-  
-  
-  
-  
-  
-  
-e DS:200  
0059:0200 00.42 00.  
-e DS:210  
0059:0210 00.43 00.  
-
```

Tracing the program

```

DOSBox 0.74-3, Cpu speed: 3000 cycles, Frameskip 0, Program: DEBUGX x
-
-
-
-
-t
AX=0043 BX=0000 CX=0000 DX=0000 SP=FFFE BP=0000 SI=0000 DI=0000
DS=0059 ES=0059 SS=0059 CS=0059 IP=0103 NU UP EI NG NZ NA PE NC
0059:0103 8A1E1002 MOV BL,[0210] DS:0210=42
-t
AX=0043 BX=0042 CX=0000 DX=0000 SP=FFFE BP=0000 SI=0000 DI=0000
DS=0059 ES=0059 SS=0059 CS=0059 IP=0107 NU UP EI NG NZ NA PE NC
0059:0107 881E0002 MOV [0200],BL DS:0200=43
-t
AX=0043 BX=0042 CX=0000 DX=0000 SP=FFFE BP=0000 SI=0000 DI=0000
DS=0059 ES=0059 SS=0059 CS=0059 IP=010B NU UP EI NG NZ NA PE NC
0059:010B A21002 MOV [0210],AL DS:0210=42
-t
AX=0043 BX=0042 CX=0000 DX=0000 SP=FFFE BP=0000 SI=0000 DI=0000
DS=0059 ES=0059 SS=0059 CS=0059 IP=010E NU UP EI NG NZ NA PE NC
0059:010E 0000 ADD [BX+SI],AL DS:0042=00
-

```

Before and after the swap:

```
DOSBox 0.74-3, Cpu speed: 3000 cycles, Frameskip 0, Program: DEBUG x
0059:0300 43 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 C.....
0059:0210 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 B.....
0059:0220 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0059:0230 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0059:0240 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0059:0250 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0059:0360 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0059:0270 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

-i 200
0059:0300 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 B.....
0059:0210 43 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 C.....
0059:0220 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0059:0230 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0059:0240 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0059:0250 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0059:0360 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0059:0270 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

Exchanging 16 bit values:

```
DOSBox 0.74-3, Cpu speed:   3000 cycles, Frameskip 0, Program: DEBUGX x
```

```
-  
-  
-  
-  
-  
-  
-  
-  
-  
-  
-  
-  
  
-a 100  
0859:0100 mov ax,[200]  
0859:0103 mov bx,[210]  
0859:0107 mov [200],bx  
0859:010B mov [210],ax  
0859:010E
```

Executing for 16 bits

```

DOSBox 0.74-3, Cpu speed: 3000 cycles, Frameskip 0, Program: DEBUGX x
-
-
-
-
-r ip 100
-t
AX=3412 BX=0042 CX=0000 DX=0000 SP=FFFE BP=0000 SI=0000 DI=0000
DS=0859 ES=0859 SS=0859 CS=0859 IP=0103 00 UP EI NG NZ NA PO NC
0859:0103 8B1E0002      MOV     BX,[0210]                      DS:0210=7856
-t
AX=3412 BX=7856 CX=0000 DX=0000 SP=FFFE BP=0000 SI=0000 DI=0000
DS=0859 ES=0859 SS=0859 CS=0859 IP=0107 00 UP EI NG NZ NA PO NC
0859:0107 891E0002      MOV     [0200],BX                      DS:0200=3412
-t
AX=3412 BX=7856 CX=0000 DX=0000 SP=FFFE BP=0000 SI=0000 DI=0000
DS=0859 ES=0859 SS=0859 CS=0859 IP=010B 00 UP EI NG NZ NA PO NC
0859:010B A31002      MOV     [0210],AX                      DS:0210=7856
-t
AX=3412 BX=7856 CX=0000 DX=0000 SP=FFFE BP=0000 SI=0000 DI=0000
DS=0859 ES=0859 SS=0859 CS=0859 IP=010E 00 UP EI NG NZ NA PO NC
0859:010E 0000      ADD     [BX+SI],AL                      DS:7856=00

```

Values before and after

```
DOSBox 0.74-3, Cpu speed: 3000 cycles, Frameskip 0, Program: DEBUGX x
DOSBox 0.74-3, Cpu speed: 3000 cycles, Frameskip 0, Program: DEBUGX x

-d 200
0059:0200 12 34 00 00 00 00 00 00-00 00 00 00 00 00 00 .4.....
0059:0210 56 78 00 00 00 00 00 00-00 00 00 00 00 00 00 Ux.....
0059:0220 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
0059:0230 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
0059:0240 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
0059:0250 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
0059:0260 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
0059:0270 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....

-d 200
0059:0200 56 78 00 00 00 00 00 00-00 00 00 00 00 00 00 Ux.....
0059:0210 12 34 00 00 00 00 00 00-00 00 00 00 00 00 00 .4.....
0059:0220 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
0059:0230 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
0059:0240 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
0059:0250 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
0059:0260 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
0059:0270 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
```

Exchanging 32 bit values

```
DOSBox 0.74-3, Cpu speed:   3000 cycles, Frameskip 0, Program: DEBUGX x
```

```
-  
-  
-  
-  
-  
-  
-  
-  
-  
-  
-  
-  
-  
-  
-  
  
-a 100  
0059:0100 mov eax,[200]  
0059:0104 mov ebx,[210]  
0059:0108 mov [200],ebx  
0059:010E mov [210],eax  
0059:0112  
-
```

Executing for 32 bits

```

DOSBox 0.74-3, Cpu speed: 3000 cycles, Frameskip 0, Program: DEBUGX x
-
-
-
-
-
-
-r ip 100
-t
AX=3412 BX=7856 CX=0000 DX=0000 SP=FFFE BP=0000 SI=0000 DI=0000
DS=0859 ES=0859 SS=0859 CS=0859 IP=0104 00 UP EI NG NZ NA PO NC
0859:0104 668B1E0002 MDU EBX,[0220] DS:0220=00000000
-t
AX=3412 BX=0000 CX=0000 DX=0000 SP=FFFE BP=0000 SI=0000 DI=0000
DS=0859 ES=0859 SS=0859 CS=0859 IP=0109 00 UP EI NG NZ NA PO NC
0859:0109 66891E0002 MDU [0200],EBX DS:0200=78563412
-t
AX=3412 BX=0000 CX=0000 DX=0000 SP=FFFE BP=0000 SI=0000 DI=0000
DS=0859 ES=0859 SS=0859 CS=0859 IP=010E 00 UP EI NG NZ NA PO NC
0859:010E 66A32002 MDU [0220],EAX DS:0220=00000000
-t
AX=3412 BX=0000 CX=0000 DX=0000 SP=FFFE BP=0000 SI=0000 DI=0000
DS=0859 ES=0859 SS=0859 CS=0859 IP=0112 00 UP EI NG NZ NA PO NC
0859:0112 0000 ADD [BX+SI],AL DS:0000=CD

```

Values before and after:

[illegible]

Checking and verifying

```
DOSBox 0.74-3, Cpu speed: 3000 cycles, Frameskip 0, Program: DEBUG x
-
-
-
-
-
-r ip 100
-u 100
0000:0100 66A10002      MOV     EAX,[0200]
0000:0104 668B1E1002      MOV     EBX,[0210]
0000:0109 66891E0002      MOV     [0200],EBX
0000:010E 66A31002      MOV     [0210],EAX
0000:0112 00F0          ADD     AL,DH
0000:0114 60          PUSHa
0000:0115 1000          ADC     [BX+SI],AL
0000:0117 F0801100      LOCK   ADC     BYTE PTR [BX+DI],00
0000:011B F0          LOCK   (unused)
0000:011C 60          PUSHa
0000:011D 1000          ADC     [BX+SI],AL
0000:011F F0          LOCK   (unused)
-g 112
AX=3412 BX=6587 CX=0003 DX=001D SP=A0C7 BP=B197 SI=0003 DI=0955
DS=0859 ES=0026 SS=0859 CS=0000 IP=0112 NV UP EI NG NZ AC PO CY
0000:0112 00F0          ADD     AL,DH
-
```

Values before and after

DOSBox 0.74-3, Cpu speed: 3000 cycles, Frameskip 0, Program: DEBUG x	DOSBox 0.74-3, Cpu speed: 3000 cycles, Frameskip 0, Program: DEBUG x
-d 200	-d 200
0859:0200 12 34 56 78 00 00 00-00 00 00 00 00 00 00 .4Ux.....	0859:0200 07 65 43 21 00 00 00-00 00 00 00 00 00 00 .eC!.....
0859:0210 87 65 43 21 00 00 00-00 00 00 00 00 00 00 .eC!.....	0859:0210 12 34 56 78 00 00 00-00 00 00 00 00 00 00 .4Ux.....
0859:0220 00 00 00 00 00 00 00-00 00 00 00 00 00 00	0859:0220 00 00 00 00 00 00 00-00 00 00 00 00 00 00
0859:0230 00 00 00 00 00 00 00-00 00 00 00 00 00 00	0859:0230 00 00 00 00 00 00 00-00 00 00 00 00 00 00
0859:0240 00 00 00 00 00 00 00-00 00 00 00 00 00 00	0859:0240 00 00 00 00 00 00 00-00 00 00 00 00 00 00
0859:0250 00 00 00 00 00 00 00-00 00 00 00 00 00 00	0859:0250 00 00 00 00 00 00 00-00 00 00 00 00 00 00
0859:0260 00 00 00 00 00 00 00-00 00 00 00 00 00 00	0859:0260 00 00 00 00 00 00 00-00 00 00 00 00 00 00
0859:0270 00 00 00 00 00 00 00-00 00 00 00 00 00 00	0859:0270 00 00 00 00 00 00 00-00 00 00 00 00 00 00

```

DOSBox 0.74-3, Cpu speed: 3000 cycles, Frameskip 0, Program: DEBUGX x
-
-
-
-
-
-
-
-
-
-
-N c:\new.txt
-L 100
-s 100 L 50 "virus"
0859:0119
-d 100
0859:0100 54 68 69 73 20 69 73 20-64 65 66 69 6E 69 74 65 This is definite
0859:0110 6C 79 20 4E 4F 54 20 61-20 76 69 72 75 73 21 21 ly NOT a virus!!
0859:0120 21 0A 00 00 00 00 00 00-00 00 00 00 00 00 00 00 !.....
0859:0130 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 .....
0859:0140 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 .....
0859:0150 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 .....
0859:0160 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 .....
0859:0170 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 .....
-
-

```

```

DOSBox 0.74-3, Cpu speed: 3000 cycles, Frameskip 0, Program: DEBUGX
-
-e DS:200
0859:0200 12.12 34.34 00.
-a 100
0859:0100 mov ax, [200]
0859:0103 mov bx, [200]
0859:0107 mov cx, [200]
0859:010B mov dx, [200]
0859:010F mov si, [200]
^ Error
0859:010F mov si, [200]
0859:0113 mov di, [200]
0859:0117
-M c:\newfile.com
-r bx 0
-r cx 100
-w 100
Writing 0100 bytes
-
DOSBox 0.74-3, Cpu speed: 3000 cycles, Frameskip 0, Program: DEBUGX
-w 100
Writing 0100 bytes
-q
C:\MSM611\BIN>debugx c:\NEWFILE.COM
-l 100
-d 100
0863:0100 A1 00 02 8B 1E 00 02 8B-0E 00 02 8B 16 00 02 8B .....>
0863:0110 36 00 02 8B 3F 00 02 00-00 00 00 00 00 00 00 00 .....
0863:0120 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 .....
0863:0130 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 .....
0863:0140 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 .....
0863:0150 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 .....
0863:0160 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 .....
0863:0170 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 .....
0863:0180 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 .....
0863:0190 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 .....
0863:01A0 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 .....
0863:01B0 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 .....
0863:01C0 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 .....
0863:01D0 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 .....
0863:01E0 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 .....
0863:01F0 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 .....

```


DOSBox 0.74-3, Cpu speed: 3000 cycles, Frameskip 0, Program: DEBUGX x

```

- F 200 L 100 "this is staored in equivalent ascii format"
- d 200
0059:0200 74 68 69 73 20 69 73 20-73 74 61 6F 72 65 64 20 this is staored
0059:0210 69 6E 20 65 71 75 69 76-61 6C 65 6E 74 20 61 73 in equivalent as
0059:0220 63 69 69 20 66 6F 72 6D-61 74 74 68 69 73 20 69 cii formatthis i
0059:0230 73 20 73 74 61 6F 72 65-64 20 69 6E 20 65 71 75 s staored in equ
0059:0240 69 76 61 6C 65 6E 74 20-61 73 63 69 69 20 66 6F ivalent ascii fo
0059:0250 72 6D 61 74 74 68 69 73-20 69 73 20 73 74 61 6F rmatthis is stao
0059:0260 72 65 64 20 69 6E 20 65-71 75 69 76 61 6C 65 6E red in equivalen
0059:0270 74 20 61 73 63 69 69 20-66 6F 72 6D 61 74 74 68 t ascii formatth

```

Annotations:

- Memory Location: Points to the address 0059:0200.
- No. of bytes: Points to the value 100.
- Data to store: Points to the string "this is staored in equivalent ascii format".
- Data stored in equivalent ascii format: Points to the repeated string in the memory dump.

It also keeps repeating the message till the byte limit is reached.