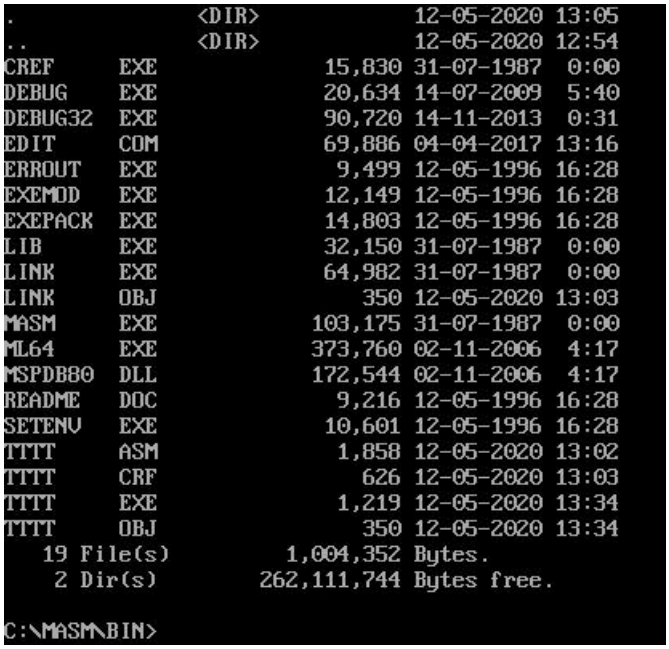
X86 汇编程序设计第一次实验作业

1. 建立 DOSBox 环境，至少包含 edit, masm, link, debug。建立好后，dir BIN 目录下的文件，截屏。命名：”MASM 编程环境截屏.JPG”



2. 用 EDIT 修改样例程序 TTTT.asm，在 Name 后将“Zhang Wuji”修改为“XXXX YYYY”。XXXX 是你的班号学号，YYYY 是你的姓名的全拼音；汇编、连接，运行，截取完整汇编、连接、运行及显示结果的屏幕，命名为:“TTTT 汇编连接及运行.JPG”。

3. 在 DEBUG 下，跟踪执行 TTTT.exe

(1) 在 DEBUG 下，修改要排序的表，合适位置放入字“XXYY”（水印），XX 为小班号，YY 为学号；

(2) 在 DEBUG 下，修改 JBE 为 JAE，将程序由升序排序改为降序排序。

(3) 单步执行，先执行至排序前，找到数据区，显示数据段，截屏；再执行至排序结束，找到数据区，显示数据段，截屏；将两个截屏文件放入 Word 文件，解读“水印”在排序前后数据段内的地址，标示出来。此 Word 文件命名为：“TTTT 降序排序前后水印位置”文档，并转换为 PDF 文件，提交“TTTT 降序排序前后水印位置.PDF”。

答：

首先，利用-e 修改内存，将 DS:0010 处的字修改为 3157H。

（我的完整学号是 17373157，在此处截取最后四位 3157）

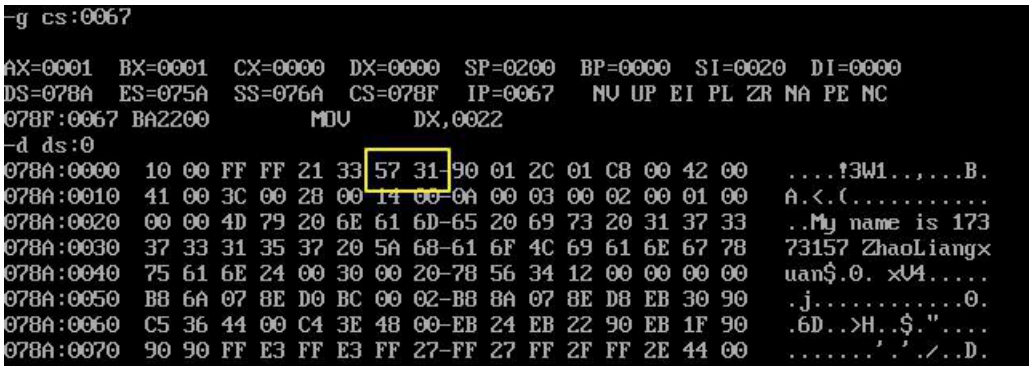
```
-d ds:0
078A:0000  10 00 C8 00 2C 01 90 01-0A 00 14 00 00 00 01 00   ....,...........
078A:0010  08 00 41 00 28 00 42 00-21 33 3C 00 FF FF 02 00   ..A.(.B.!3<.....
078A:0020  03 00 4D 79 20 6E 61 6D-65 20 69 73 20 31 37 33   ..My name is 173
078A:0030  37 33 31 35 37 20 5A 68-61 6F 4C 69 61 6E 67 78   73157 ZhaoLiangx
078A:0040  75 61 6E 24 00 30 00 20-78 56 34 12 00 00 00 00   uan$.0. xV4.....
078A:0050  B8 6A 07 8E D0 BC 00 02-B8 8A 07 8E D8 EB 30 90   .j............0.
078A:0060  C5 36 44 00 C4 3E 48 00-EB 24 EB 22 90 EB 1F 90   .6D..>H..$."....
078A:0070  90 90 FF E3 FF E3 FF 27-FF 27 FF 2F FF 2E 44 00   .......'.'./..D.
-e ds:0010
078A:0010  08.57   00.31   41.

-d ds:0
078A:0000  10 00 C8 00 2C 01 90 01-0A 00 14 00 00 00 01 00   ....,...........
078A:0010  57 31 41 00 28 00 42 00-21 33 3C 00 FF FF 02 00   W1A.(.B.!3<.....
078A:0020  03 00 4D 79 20 6E 61 6D-65 20 69 73 20 31 37 33   ..My name is 173
078A:0030  37 33 31 35 37 20 5A 68-61 6F 4C 69 61 6E 67 78   73157 ZhaoLiangx
078A:0040  75 61 6E 24 00 30 00 20-78 56 34 12 00 00 00 00   uan$.0. xV4.....
078A:0050  B8 6A 07 8E D0 BC 00 02-B8 8A 07 8E D8 EB 30 90   .j............0.
078A:0060  C5 36 44 00 C4 3E 48 00-EB 24 EB 22 90 EB 1F 90   .6D..>H..$."....
078A:0070  90 90 FF E3 FF E3 FF 27-FF 27 FF 2F FF 2E 44 00   .......'.'./..D.
```

然后，利用-a 修改指令，将 CS:0051 处的 JBE 修改为 JAE(JNB)。

```
-a cs:0051
078F:0051 jae 005b
078F:0053
-u cs:004e
078F:004E 3B4402        CMP     AX,[SI+02]
078F:0051 7308          JNB     005B
078F:0053 874402        XCHG    AX,[SI+02]
078F:0056 8904          MOV     [SI],AX
078F:0058 BB0000        MOV     BX,0000
078F:005B 83C602        ADD     SI,+02
078F:005E E2EC          LOOP    004C
078F:0060 83FB01        CMP     BX,+01
078F:0063 7402          JZ      0067
078F:0065 EBD9          JMP     0040
078F:0067 BA2200        MOV     DX,0022
078F:006A B409          MOV     AH,09
078F:006C CD21          INT     21
```

最后，利用-g 跳转到降序冒泡排序结束处，再利用-d 查看内存。发现水印 3157H 被挪动到了 DS:0006 处。



4. （选做题）

(1) 在 DEBUG 下，将 ADD1 修改为长度为 32 位的“班号学号”双字水印，如 11223434h(根据你的班号学号改)，显示数据区，指出 ADD1 地址及内容。

(2) 改 CS：IP 至 JMP DWORD PTR ADD1，截取单步执行此命令后的屏幕，在后面的文档中解读 CS：IP 的值及含义。

(3) 改 CS：IP 至 CALL DWORD PTR ADD1，截取单步执行此命令后的屏幕，显示堆栈段的栈顶处， 截取堆栈栈顶数据区屏幕，在后面的文档中解读栈顶值及含义。

(4) 在 WORD 下粘贴上述三个截屏文件，分别解读截屏中的“水印”地址及内容；解读 JMP DWORD PTR ADD1 执行后的 CS:IP 值；解读 CALL DWORD PTR ADD1 执行后栈顶数据区的地址及内容（SS:[SP]处的双字）、含义,CS:IP 值。存成 Word 文档，并转换为 PDF 文件，提交“段间转移及调用指令解读.PDF”。

答：

第一步，将 ADD1 修改为双字水印 17373157H。利用-d 查到 ADD1 的地址为 DS:0044，将原本的值 20003000H，修改为 17373157H。

```
-d ds:0
078A:0000  10 00 C8 00 2C 01 90 01-0A 00 14 00 00 00 01 00   ....,...........
078A:0010  08 00 41 00 28 00 42 00-21 33 3C 00 FF FF 02 00   ..A.(.B.!3<.....
078A:0020  03 00 4D 79 20 6E 61 6D-65 20 69 73 20 31 37 33   ..My name is 173
078A:0030  37 33 31 35 37 20 5A 68-61 6F 4C 69 61 6E 67 78   73157 ZhaoLiangx
078A:0040  75 61 6E 24 00 30 00 20-78 56 34 12 00 00 00 00   uan$.0. xV4.....
078A:0050  B8 6A 07 8E D0 BC 00 02-B8 8A 07 8E D8 EB 30 90   .j............0.
078A:0060  C5 36 44 00 C4 3E 48 00-EB 24 EB 22 90 EB 1F 90   .6D..>H..$."....
078A:0070  90 90 FF E3 FF E3 FF 27-FF 27 FF 2F FF 2E 44 00   .......'.'./..D.
-e ds:0044
078A:0044  00.57   30.31   00.37   20.17

-d ds:0
078A:0000  10 00 C8 00 2C 01 90 01-0A 00 14 00 00 00 01 00   ....,...........
078A:0010  08 00 41 00 28 00 42 00-21 33 3C 00 FF FF 02 00   ..A.(.B.!3<.....
078A:0020  03 00 4D 79 20 6E 61 6D-65 20 69 73 20 31 37 33   ..My name is 173
078A:0030  37 33 31 35 37 20 5A 68-61 6F 4C 69 61 6E 67 78   73157 ZhaoLiangx
078A:0040  75 61 6E 24 57 31 37 17-78 56 34 12 00 00 00 00   uan$W17.xV4.....
078A:0050  B8 6A 07 8E D0 BC 00 02-B8 8A 07 8E D8 EB 30 90   .j............0.
078A:0060  C5 36 44 00 C4 3E 48 00-EB 24 EB 22 90 EB 1F 90   .6D..>H..$."....
078A:0070  90 90 FF E3 FF E3 FF 27-FF 27 FF 2F FF 2E 44 00   .......'.'./..D.
-_ ;_
```

第二步，利用-r 移动至 JMP DWORD PTR ADD1 指令处，利用-t 单步执行，发现 CS:IP 变为 1737:3157，正是 ADD1 的值，ADD1 的高字成为 CS，低字成为 IP。这是 JMP 中的段间间接转移。

```
-u
078F:0020 90            NOP
078F:0021 90            NOP
078F:0022 FFE3          JMP     BX
078F:0024 FFE3          JMP     BX
078F:0026 FF27          JMP     [BX]
078F:0028 FF27          JMP     [BX]
078F:002A FF2F          JMP     FAR [BX]
078F:002C FF2E4400      JMP     FAR [0044]
078F:0030 FFD3          CALL    BX
078F:0032 FF17          CALL    [BX]
078F:0034 FF17          CALL    [BX]
078F:0036 FF1E4400      CALL    FAR [0044]
078F:003A FF1E4400      CALL    FAR [0044]
078F:003E 90            NOP
078F:003F 90            NOP
-r ip
IP 000D
:002c
-t

AX=078A  BX=0000  CX=02C3  DX=0000  SP=0200  BP=0000  SI=0000  DI=0000
DS=078A  ES=075A  SS=076A  CS=1737  IP=3157   NV UP EI PL NZ NA PO NC
1737:3157 0A00          OR      AL,[BX+SI]                   DS:0000=10
-_ ;
```

第三步，利用-r 修改 CS 和 IP 移动至 CALL DWORD PTR ADD1 指令处，利用-t 单步执行，发现 CS:IP 变为 1737:3157，对 CS:IP 的分析与第二步相同。这是 CALL 的段间间接调用。

```
078F:0034 FF17          CALL    [BX]
078F:0036 FF1E4400      CALL    FAR [0044]
078F:003A FF1E4400      CALL    FAR [0044]
078F:003E 90            NOP
078F:003F 90            NOP
-r ip
IP 000D
:002c
-t

AX=078A  BX=0000  CX=02C3  DX=0000  SP=0200  BP=0000  SI=0000  DI=0000
DS=078A  ES=075A  SS=076A  CS=1737  IP=3157   NV UP EI PL NZ NA PO NC
1737:3157 0A00          OR      AL,[BX+SI]                      DS:0000=10
-r cs
CS 1737
:078f
-r ip
IP 3157
:0036
-t

AX=078A  BX=0000  CX=02C3  DX=0000  SP=01FC  BP=0000  SI=0000  DI=0000
DS=078A  ES=075A  SS=076A  CS=1737  IP=3157   NV UP EI PL NZ NA PO NC
1737:3157 0A00          OR      AL,[BX+SI]                      DS:0000=10
```

由于是 CALL 指令，故会对堆栈进行操作。利用-d 指令查看堆栈中的数据（我最开始尝试使用-d ss:sp 和-d ss:[sp]，报了 Error，这是因为 sp 不能用于间接寻址，将 sp 替换为其实际的值 01FC 后就对了）。在 SS:01FC（即栈顶）处存储了一个双字 078F003AH，这个双字代表着返回地址，即下一条指令 CALL ADD1 所处的位置，其中高字 078F 为返回地址段值（下一条指令的 CS 值），低字 003A 为返回地址偏移值（下一条指令的 IP 值）。

```
AX=078A  BX=0000  CX=02C3  DX=0000  SP=01FC  BP=0000  SI=0000  DI=0000
DS=078A  ES=075A  SS=076A  CS=1737  IP=3157   NV UP EI PL NZ NA PO NC
1737:3157 0A00          OR      AL,[BX+SI]                      DS:0000=10
-d ss:sp
      ^ Error
-d ss:[sp]
      ^ Error
-d ss:01fc
076A:01F0                                       3A 00 8F 07              :...
076A:0200  10 00 C8 00 2C 01 90 01-0A 00 14 00 00 00 01 00   ....,...........
076A:0210  08 00 41 00 28 00 42 00-21 33 3C 00 FF FF 02 00   ..A.(.B.!3<.....
076A:0220  03 00 4D 79 20 6E 61 6D-65 20 69 73 20 31 37 33   ..My name is 173
076A:0230  37 33 31 35 37 20 5A 68-61 6F 4C 69 61 6E 67 78   73157 ZhaoLiangx
076A:0240  75 61 6E 24 57 31 37 17-78 56 34 12 00 00 00 00   uan$W17.xV4.....
076A:0250  B8 6A 07 8E D0 BC 00 02-B8 8A 07 8E D8 EB 30 90   .j............0.
076A:0260  C5 36 44 00 C4 3E 48 00-EB 24 EB 22 90 EB 1F 90   .6D..>H..$."....
076A:0270  90 90 FF E3 FF E3 FF 27-FF 27 FF 2F               .......'.'./
```