1. 修改ADD1

```
-e ds:003f
078A:003F  00.21
078A:0040  30.32   00.37   20.21

-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 32 31 33   ..My name is 213
078A:0030  37 33 32 32 31 20 44 65-6E 67 20 54 61 6F 24 21   73221 Deng Tao$!
078A:0040  32 37 21 78 56 34 12 00-00 00 00 00 00 00 00 00   27!xV4..........
078A:0050  B8 6A 07 8E D0 BC 00 02-B8 8A 07 8E D8 EB 30 90   .j............0.
078A:0060  C5 36 3F 00 C4 3E 43 00-EB 24 EB 22 90 EB 1F 90   .6?..>C..$."....
078A:0070  90 90 FF E3 FF E3 FF 27-FF 27 FF 2F FF 2E 3F 00   .......'.'./..?.
```

将ADD1修改为学号**21373221H**，ADD1的起始地址为**078A:003f**

2. 改CS：IP至JMP DWORD ADD1

使用u指令可以找到`JMP DWORD PTR ADD1`指令的位置为002C，使用**r IP 002C**修改IP寄存器的值，使用t单部执行

```
-r IP
IP 000D
:002C
-r
AX=078A  BX=0000  CX=02C3  DX=0000  SP=0200  BP=0000  SI=0000  DI=0000
DS=078A  ES=075A  SS=076A  CS=078F  IP=002C   NV UP EI PL NZ NA PO NC
078F:002C FF2E3F00      JMP     FAR [003F]                    DS:003F=3221
-t

AX=078A  BX=0000  CX=02C3  DX=0000  SP=0200  BP=0000  SI=0000  DI=0000
DS=078A  ES=075A  SS=076A  CS=2137  IP=3221   NV UP EI PL NZ NA PO NC
2137:3221 0000          ADD     [BX+SI],AL                    DS:0000=10
```

CS:IP为程序执行到的位置，修改其值可以指定下一条执行的汇编指令的位置，通过修改IP使程序直接执行指令`JMP DWORD PTR ADD1`此指令跳转到ADD1内存中存储的地址，即**21373221H**，于是在执行此指令后，CS:IP的值就变为了**2137:3221H**

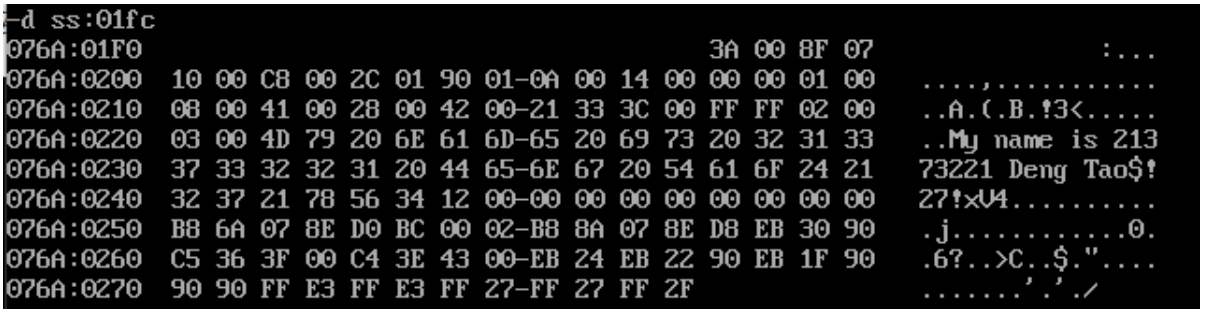
3. 改CS：IP至CALL DWORD ADD1

与上题步骤类似，运行的结果如下图：

```
-r CS
CS 2137
:078F
-r IP
IP 3221
:0036
-r
AX=078A  BX=0000  CX=02C3  DX=0000  SP=0200  BP=0000  SI=0000  DI=0000
DS=078A  ES=075A  SS=076A  CS=078F  IP=0036   NV UP EI PL NZ NA PO NC
078F:0036 FF1E3F00      CALL    FAR [003F]                    DS:003F=3221
-t

AX=078A  BX=0000  CX=02C3  DX=0000  SP=01FC  BP=0000  SI=0000  DI=0000
DS=078A  ES=075A  SS=076A  CS=2137  IP=3221   NV UP EI PL NZ NA PO NC
2137:3221 0000          ADD     [BX+SI],AL                    DS:0000=10
```

堆栈段的顶部地址可由SS和SP寄存器值相加得到，堆栈段的栈顶处数据区屏幕屏幕如下：



可以看到栈顶的一个双字为**078F003AH**，这个值记录了CALL指令结束之后需要返回的指令地址，即`CALL DWORD PTR ADD1`的下一条指令的地址，即指令`CALL ADD1`的地址