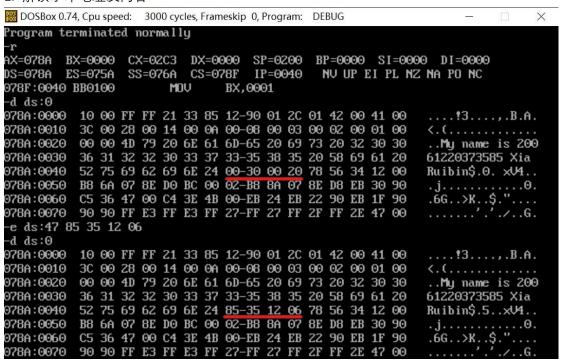
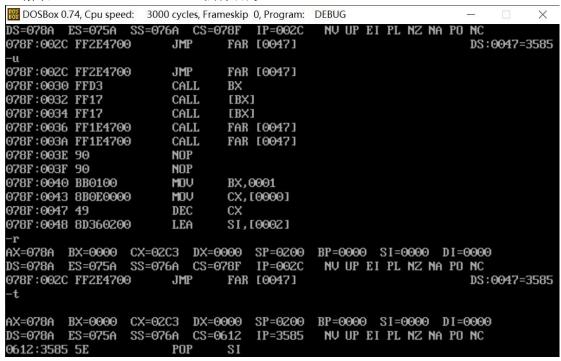
1. 解读水印地址及内容



将原先 ADD1 中的 20003000 改为了班号学号(太长了,截取部分)06123585

2. 解读 JMP DWORD PTR ADD1 执行后的 CS:IP



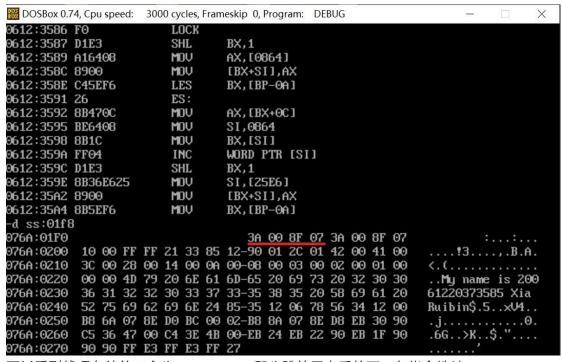
其实单步执行的话应该用 p,不过这里用 t 效果都一样,就不再改了 CS:IP 变为了 0612:3585,也就是 JMP 指令的转移目标地址(位于 ADD1 中)。

3. 解读 CALL DWORD PTR ADD1 执行后栈顶数据区的地址及内容

```
DOSBox 0.74, Cpu speed: 3000 cycles, Frameskip 0, Program: DEBUG
                                                                              X
IP 002C
:36
AX=078A BX=0000 CX=02C3 DX=0000 SP=01FC BP=0000 SI=0000 DI=0000
DS=078A ES=075A SS=076A CS=078F IP=0036
                                              NU UP EI PL NZ NA PO NC
078F:0036 FF1E4700
                                FAR [0047]
                                                                    DS:0047=3585
                        CALL
-u
078F:0036 FF1E4700
                        CALL
                                FAR [0047]
078F:003A FF1E4700
                                FAR [0047]
                        CALL
078F:003E 90
                        NOP
078F:003F 90
                        NNP
078F:0040 BB0100
                        MOV
                                BX,0001
                        MOV
078F:0043 8B0E0000
                                CX,[0000]
078F:0047 49
                        DEC
                                CX
078F:0048 8D360200
                                $1,000021
                        LEA
078F:004C 8B04
                        MOV
                                AX,[SI]
078F:004E 3B4402
                        CMP
                                AX.[SI+02]
                                005B
078F:0051 7308
                        JNB
078F:0053 874402
                        XCHG
                                AX,[SI+02]
AX=078A BX=0000 CX=02C3 DX=0000 SP=01F8 BP=0000 SI=0000 DI=0000
DS=078A ES=075A SS=076A CS=0612
                                    IP=3585
                                             NU UP EI PL NZ NA PO NC
0612:3585 5E
                        POP
                               SI
```

(发现用 p 和用 t 一样, 应该是跳转地址是乱填的缘故)

CS:IP 变为了 0612:3585. 同样是 CALL 段间间接调用的跳转目标地址。



可以看到栈顶存储的双字为 078f:003a, 即为跳转回来后的下一条指令地址 (第二行开始往下的内容, 和 DS:0000 的内容一模一样, 不是很清楚原理)