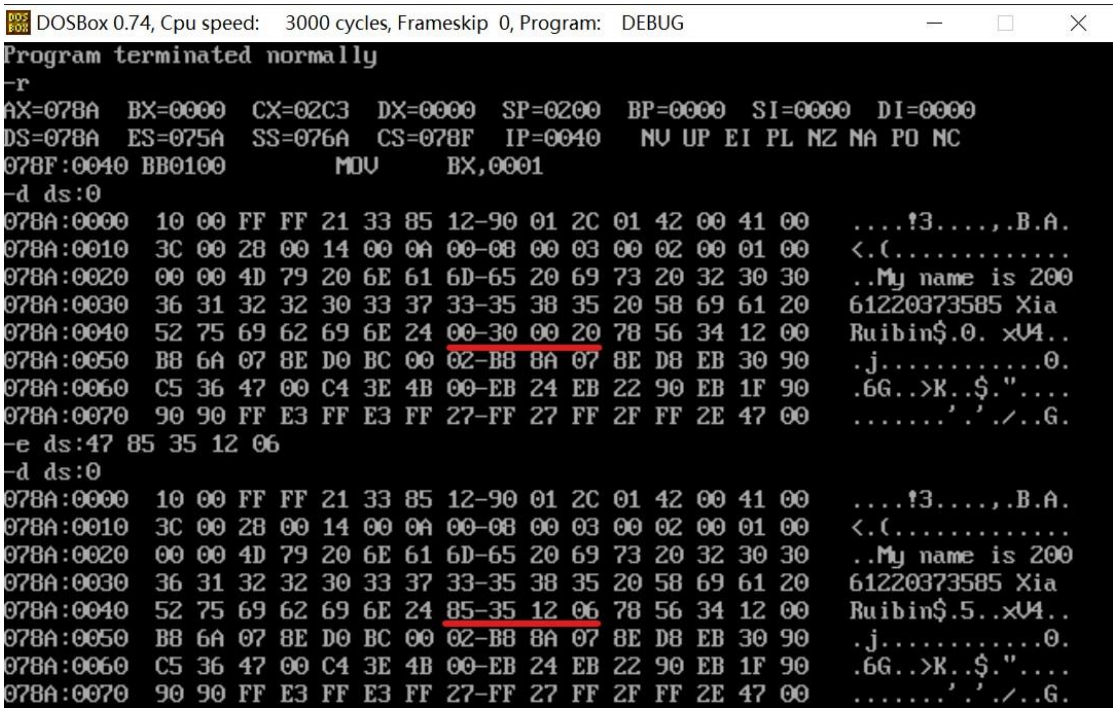
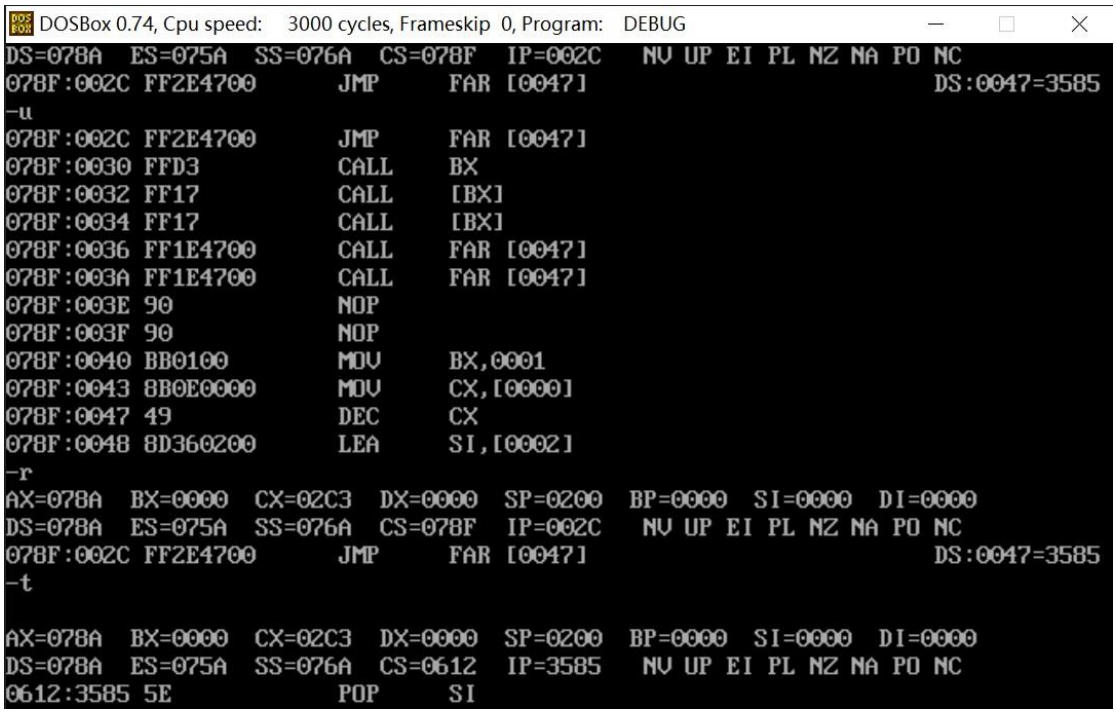
20373585 夏瑞斌 200612

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

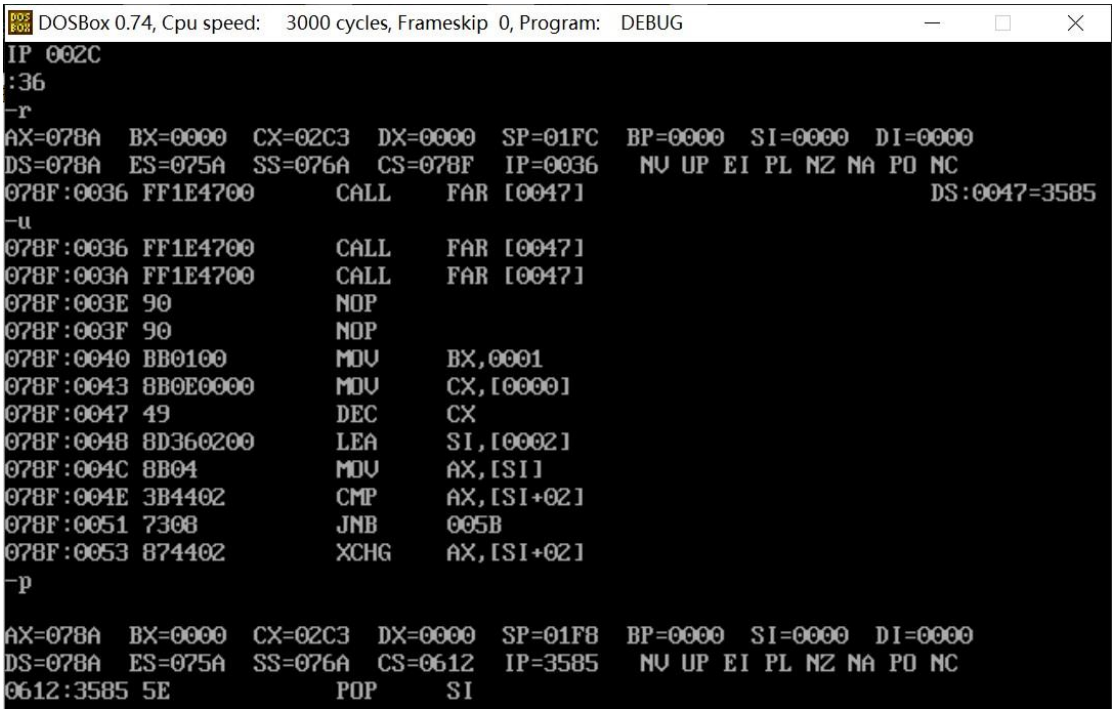
2. 解读 JMP DWORD PTR ADD1 执行后的 CS:IP



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

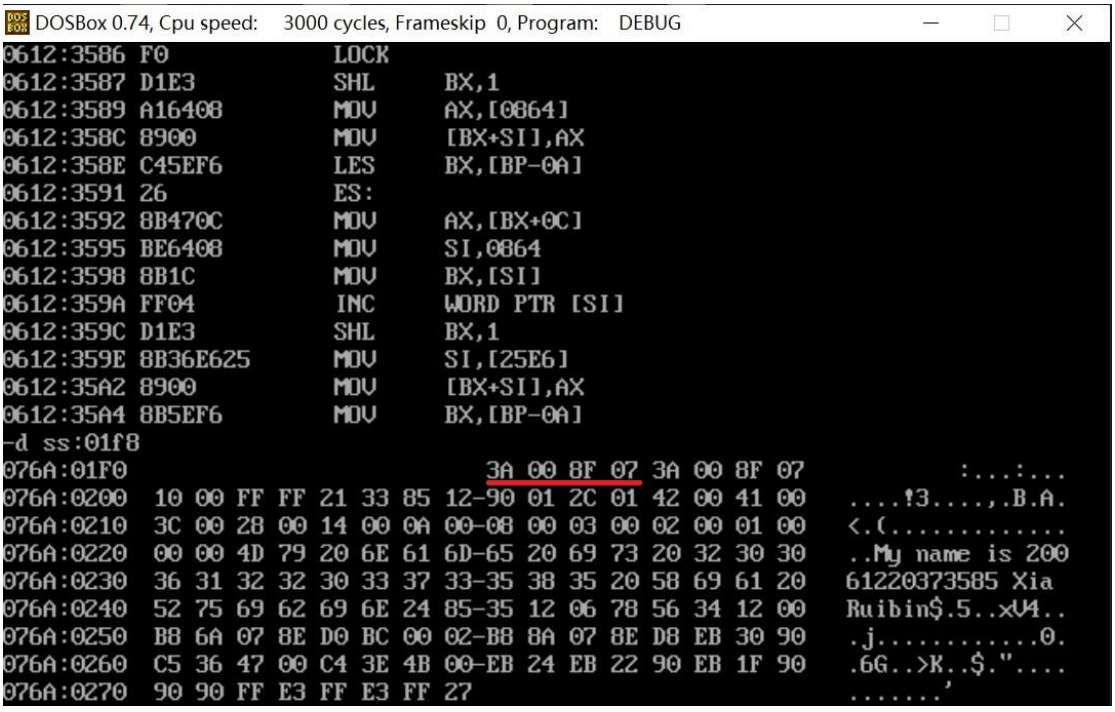
CS:IP 变为了 0612:3585，也就是 JMP 指令的转移目标地址（位于 ADD1 中）。

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



（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）