《汇编语言》王爽 P88 实验3

原创

酱油瓶被人注册了 于 2018-03-07 14:38:26 发布 5009 收藏 16

分类专栏： 汇编 文章标签： 汇编 王爽 实验3

本文链接：https://blog.csdn.net/qq_25175067/article/details/79470838

《汇编语言》王爽 P88 实验3

Mac系统配置这些蛮麻烦的：

下载个DOSBOX，再下载debug，在DOSBOX中把debug挂到C盘去吧

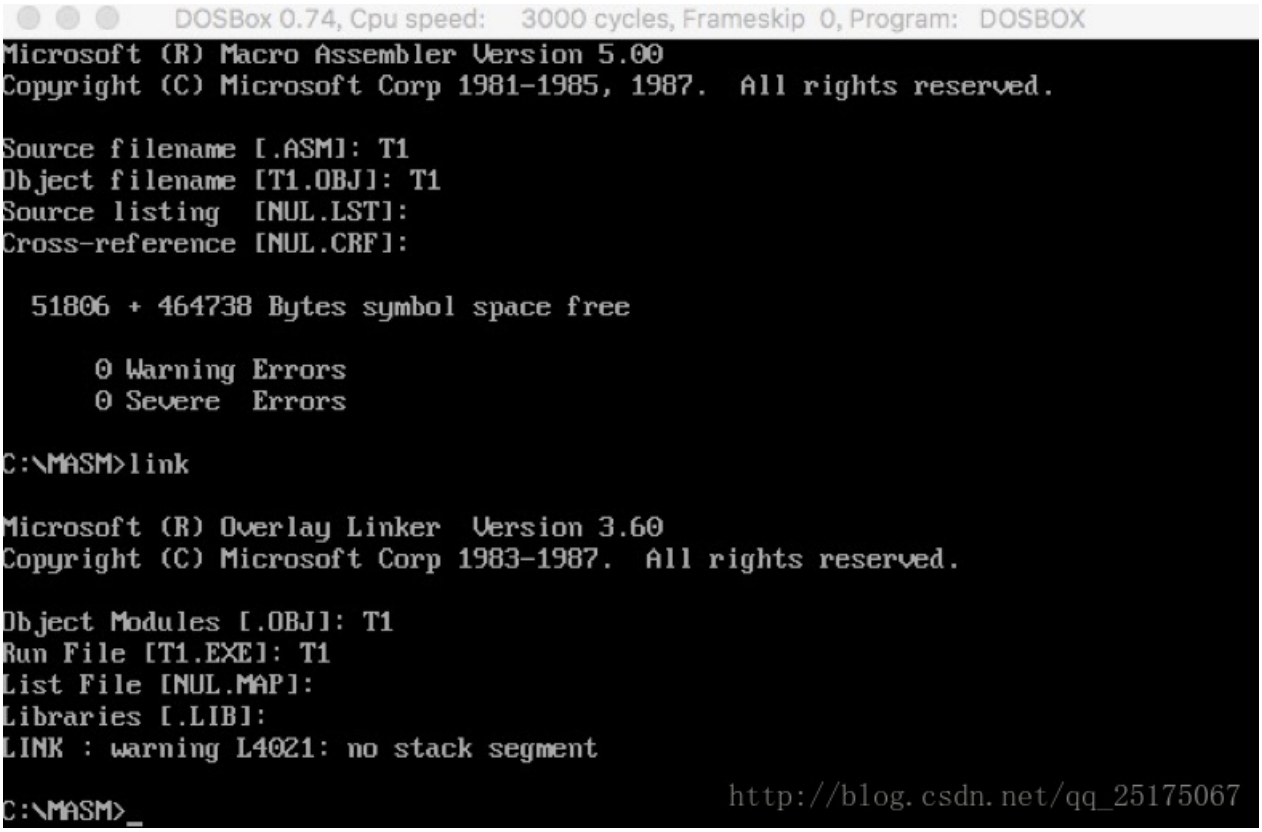
比如我想把air下面的debug文件挂成C盘，就括号中这条命令：

（mount c /Users/air/debug），当然你也可以放其他位置，取其他的名字，只要后面的目录对就可以；

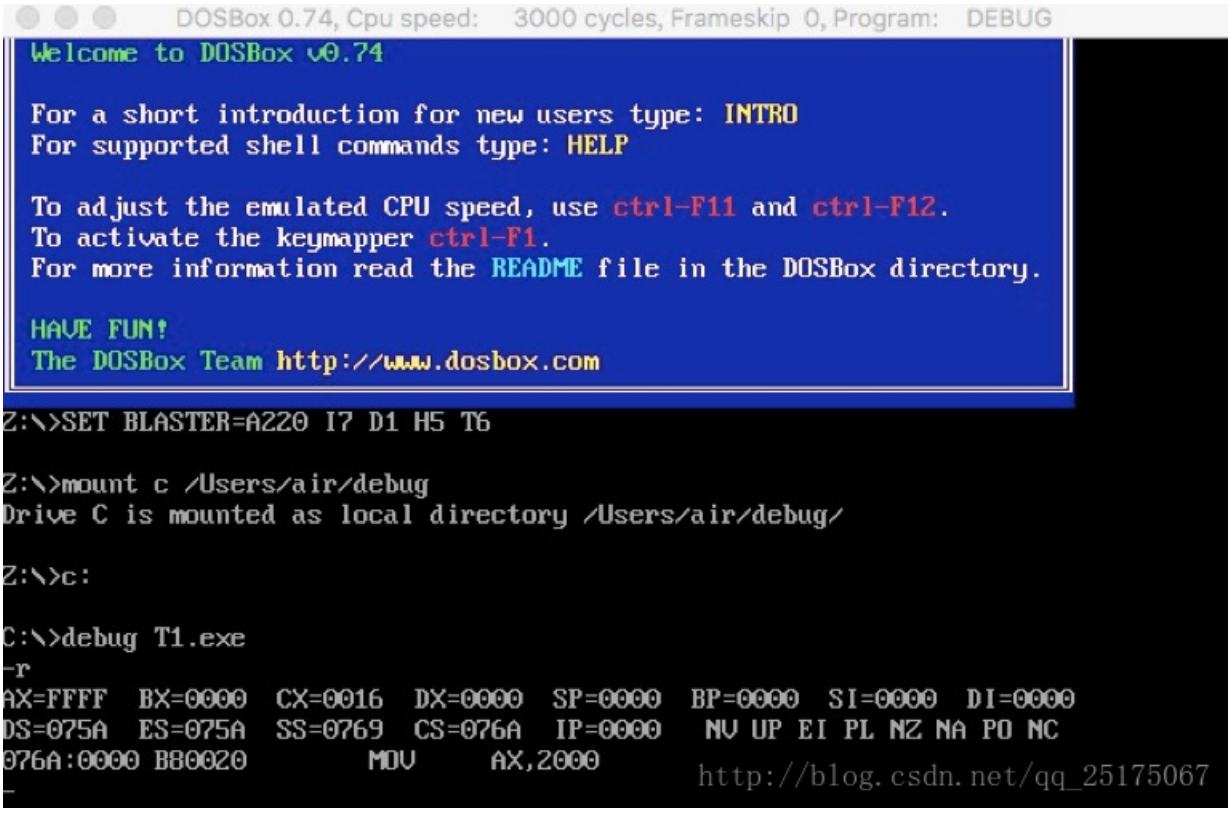
下载edit.exe 和masm都放到debug这个文件中去吧，这样执行起来也方便

1）生成t1,exe （注：数字后面一定要加h, 我一开始很蠢的把）

```
assume cs : codeseg
codeseg segment
    mov ax, 2000H
    mov ss, ax
    mov sp, 0
    add sp, 4
    pop ax
    pop bx
    push ax
    push bx
    pop ax
    pop bx
    mov ax,4c00H
    int 21h
codeseg ends
end
```



2）debug执行T1.exe之后：



可以看出 DS = 075A; CS=076A，两个段地址相差10H，是因为PSP的256个字节的原因；

疑惑：DS和CS的不同，有什么用嘛？

CX=0016是T1的字节长度，16H个字节；

从mov ax,2000到int 21的每个指令的字节长度为：3，2，3，3，1，1，1，1，1，1，3，2，sum之后是22个字节，写成16进制就是16H (16*1+6=22).

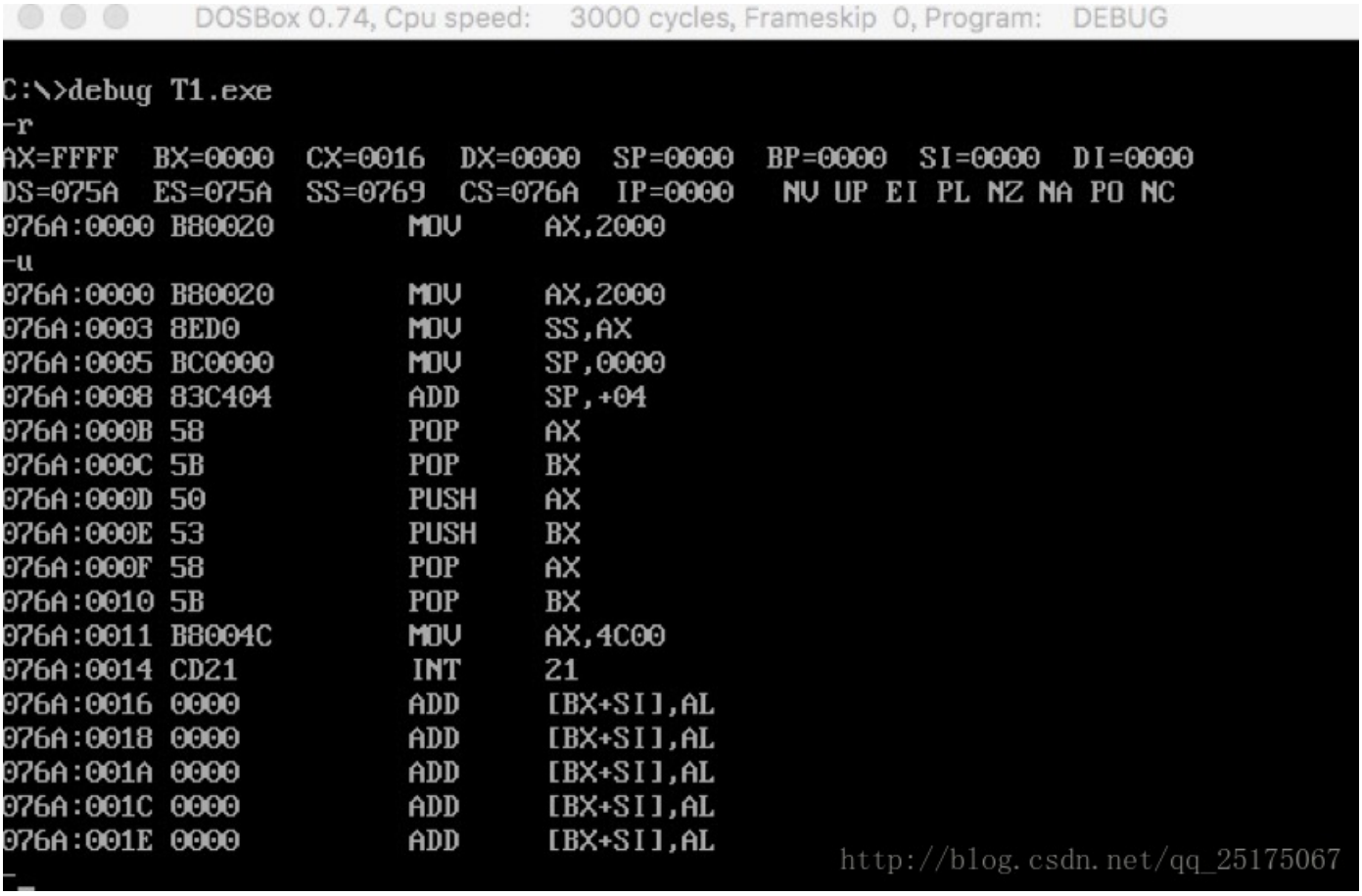
以下为执行mov ax, 2000H

mov ss, ax

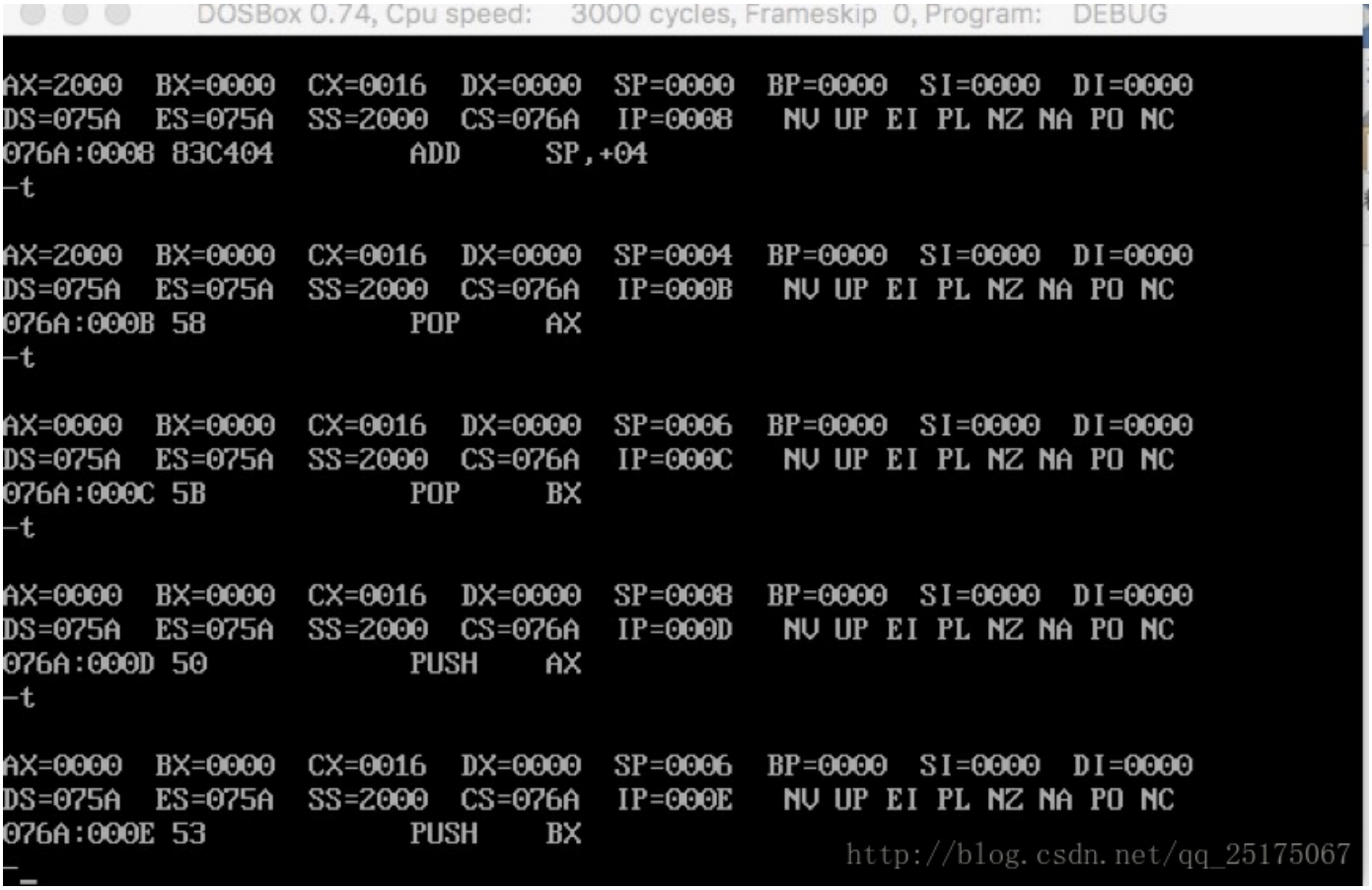
mov sp, 0

add sp, 4

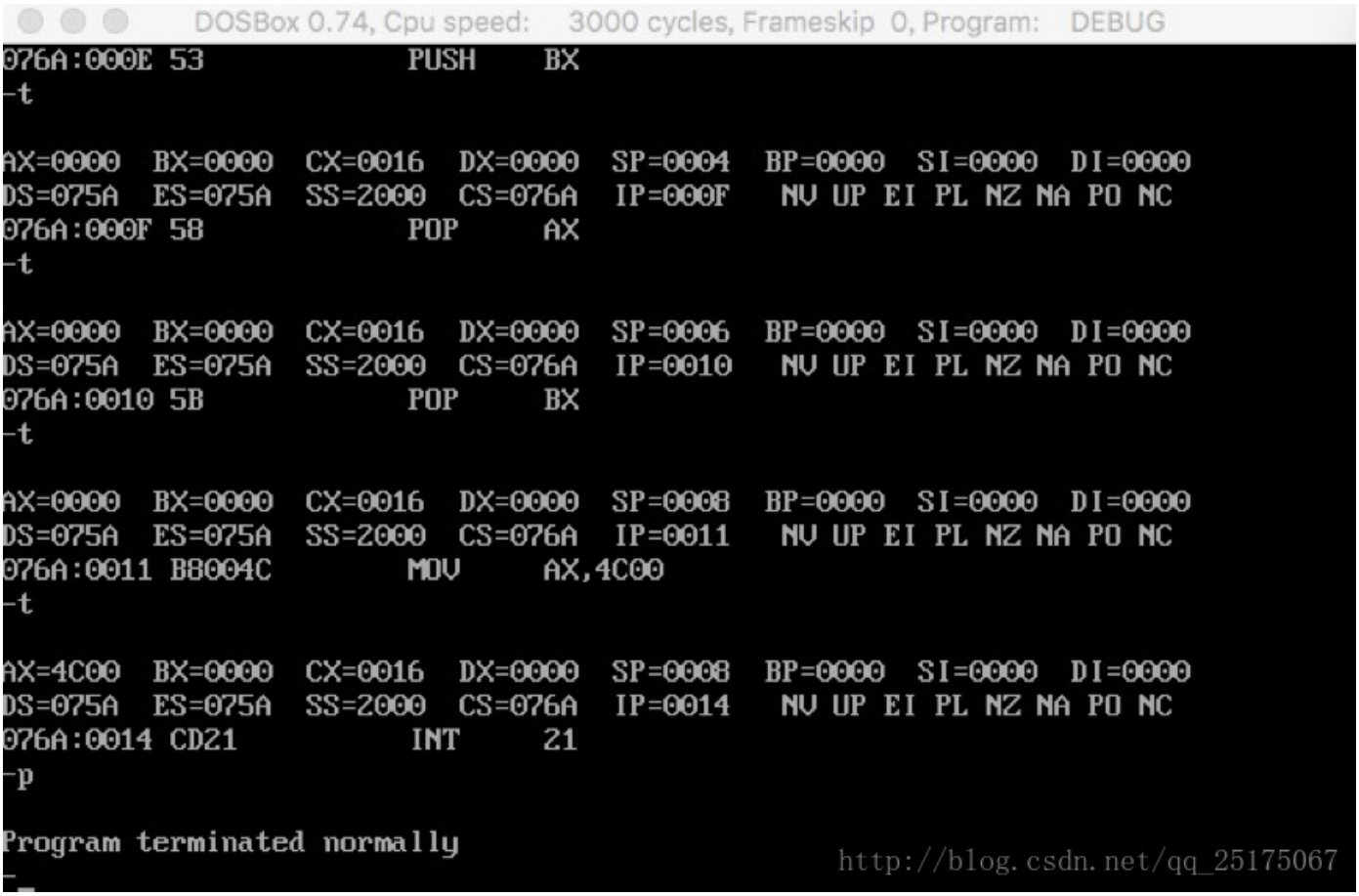
很容易看出来 mov ss, ax 和 mov sp, 0000同时执行了



以下为执行pop ax
pop bx
push ax
push bx
很容易看出来 每次pop之后 SP+2; 每次push之后，SP-2, 初始为SP=0004
pop ax, 把栈顶内容存入寄存器ax，所以ax从2000编程0000， SP=0006
pop bx, 把栈顶内容存入寄存器bx，SP=0008
push ax, 把寄存器ax内容压入栈顶， SP=0006
猜测一下：push bx, 把寄存器bx内容压入栈顶， SP=0004



以下为执行pop ax
pop bx
mov ax,4c00H
int 21h
最后program terminated normally, 一切正常。



3）PSP的头两个字节是CD20，用debug加载t1.exe，查看PSP的内容

也就是说要查看内存075A:0的内容嘛；

使用命令： -d ds:0 , 答案bingo!