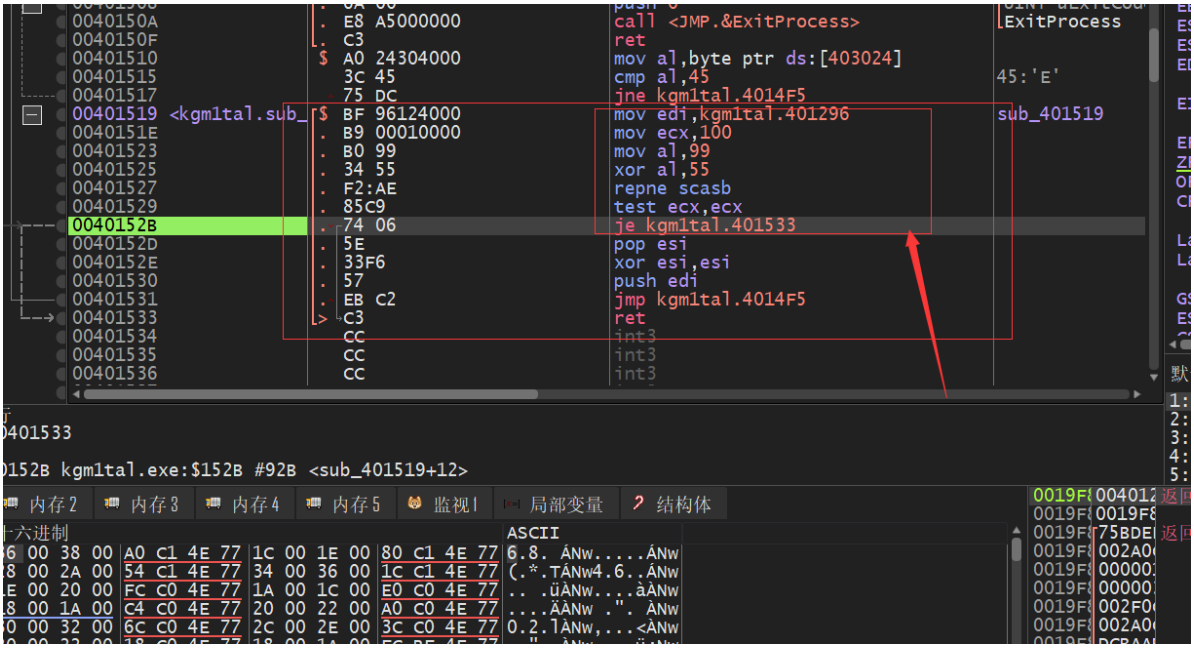
记录一种简单的反调试手段（调试随手笔记）

1.先上图



2.解析

```
mov edi,kgm1tal.401296     ;将401296这个函数地址给edi
mov ecx,100                ;设置循环次数
mov al,99
xor al,55                  ;al=cc 即int 3断点
repne scasb                ;循环比较al与byte ptr [edi] ,直到相等或者ecx==0
test ecx,ecx               ;对ecx判断是否为0，不为0存在cc断点，可直接退出
je kgm1tal.401533
```

3.总结

一种自校验的手段，检测一定函数区域内是否被下软件断点。