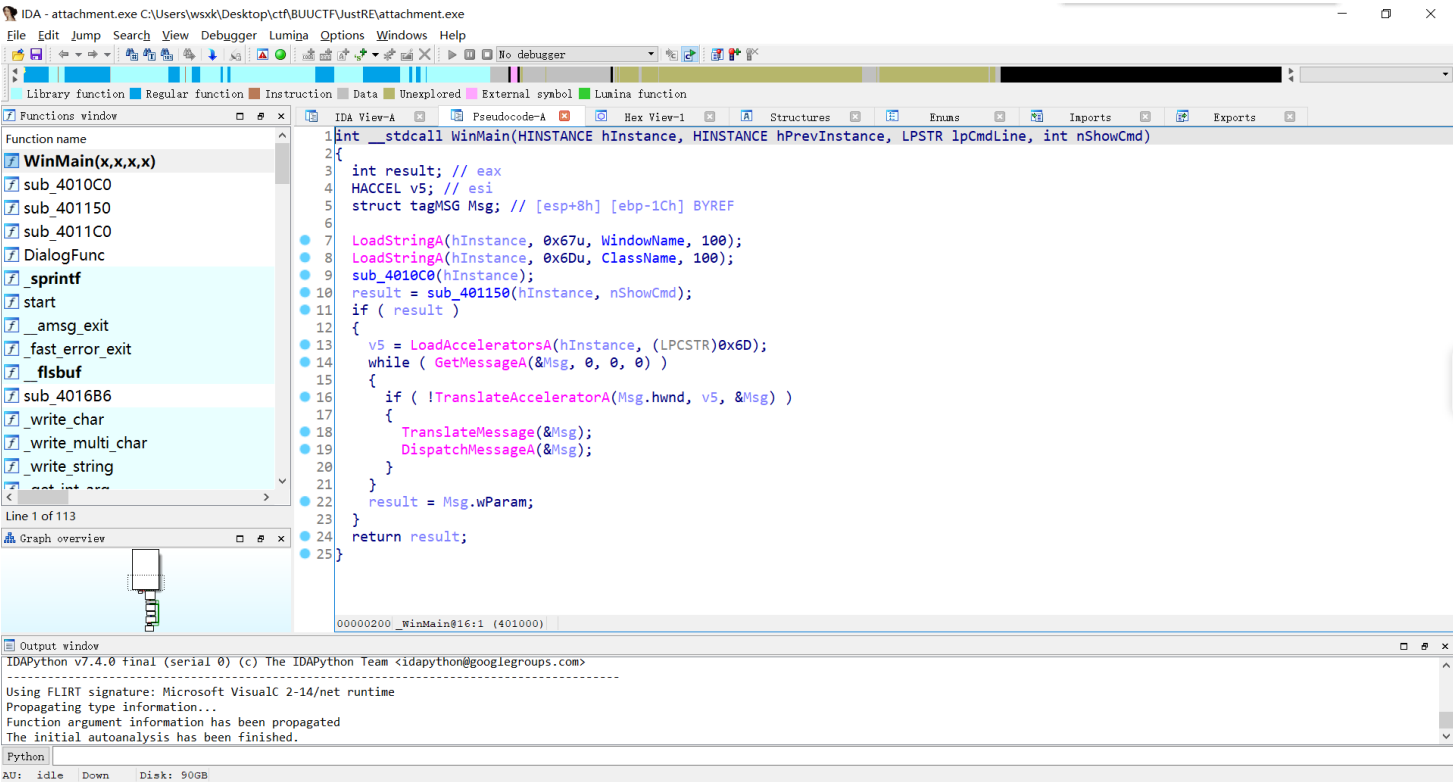


这是一道mfc逆向题

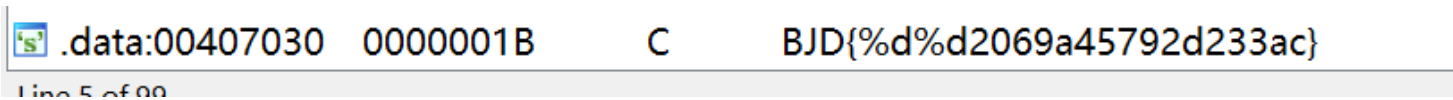
先拖入ida中查看



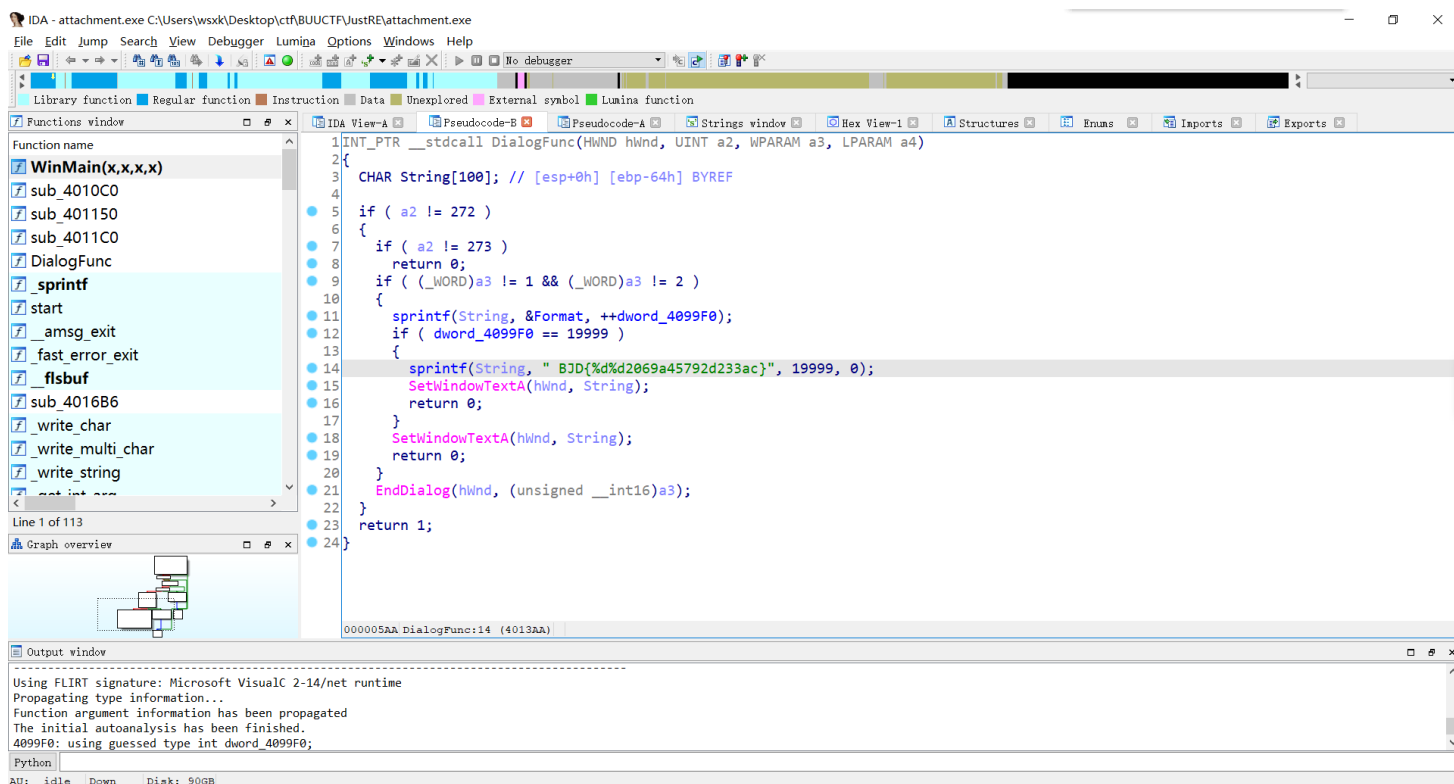
显然是找不到任何东西的

这里我们的首要目标是找到核心代码段在哪里：

方法一 直接查看字符串



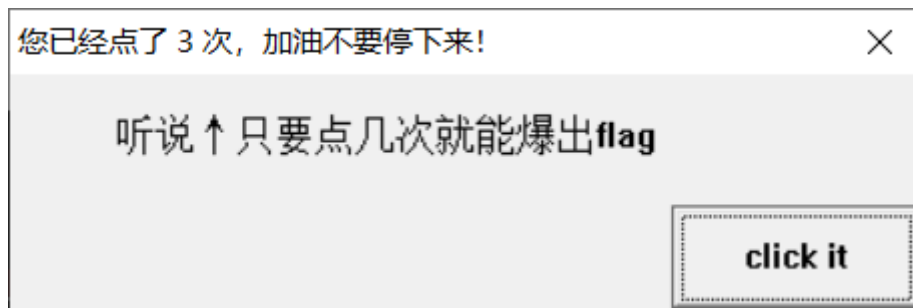
交叉引用找到目标



其实已经得到了flag

方法二 CE找变化的内存

在运行程序时，有一个计数器

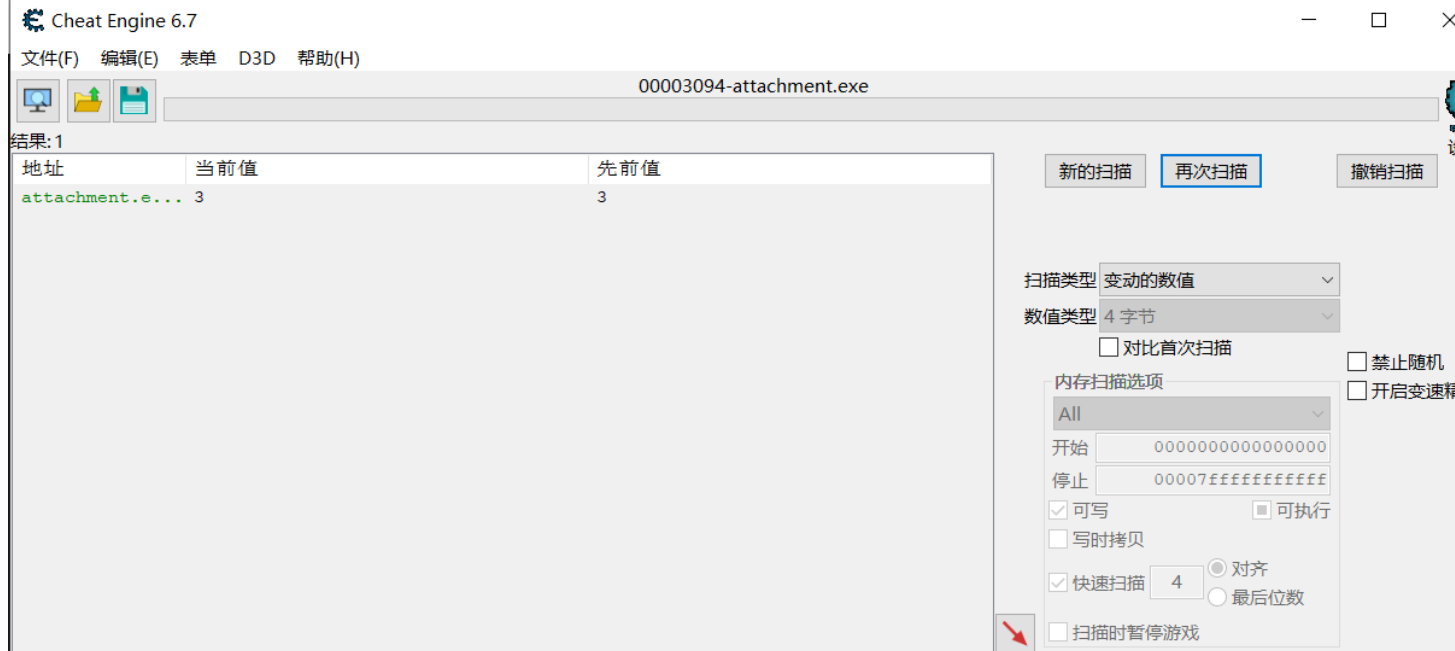


可以CE扫变动的值，找到该地址

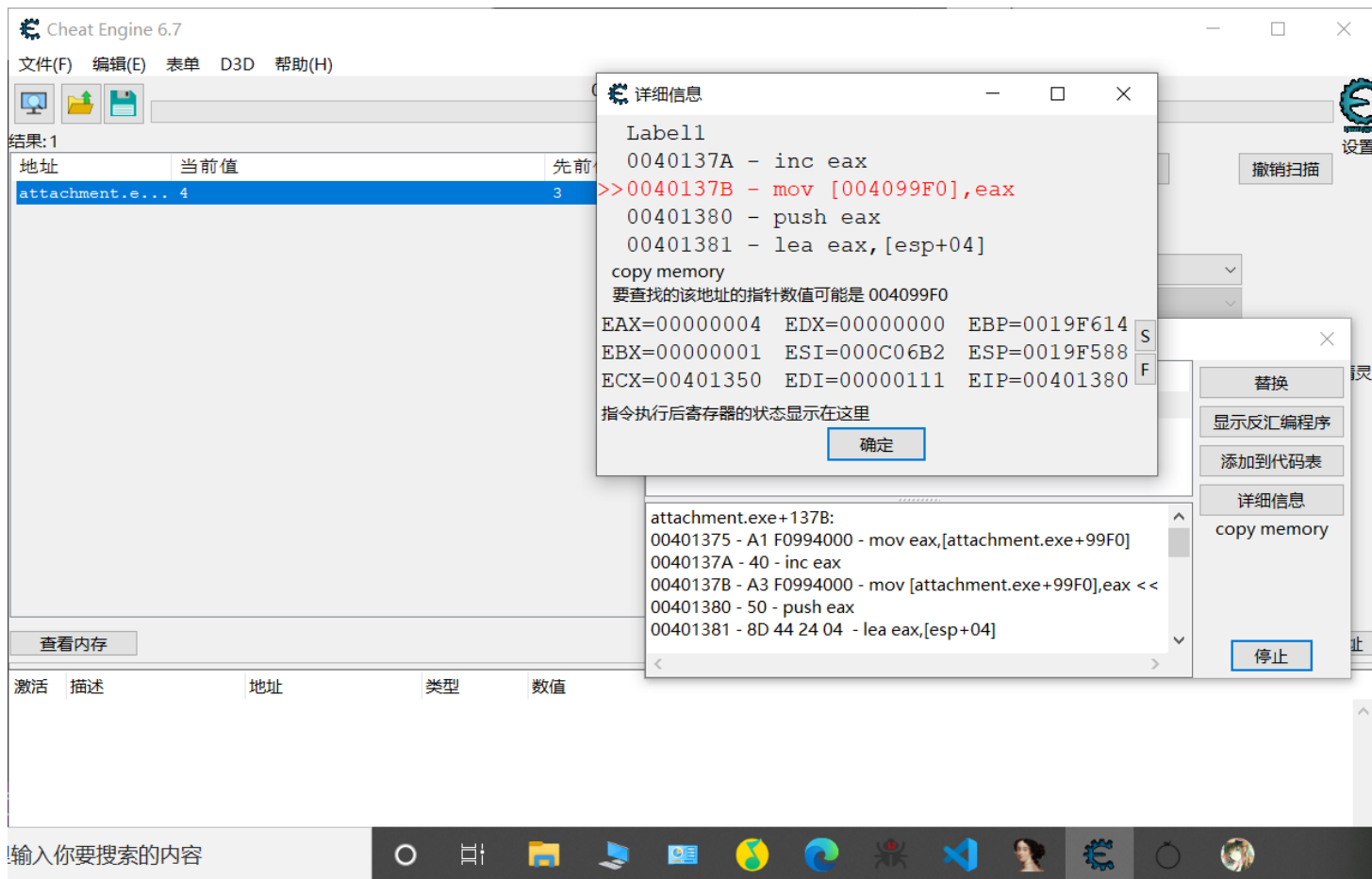
已经点了 3 次，加油不要停下来！

发在哪里：

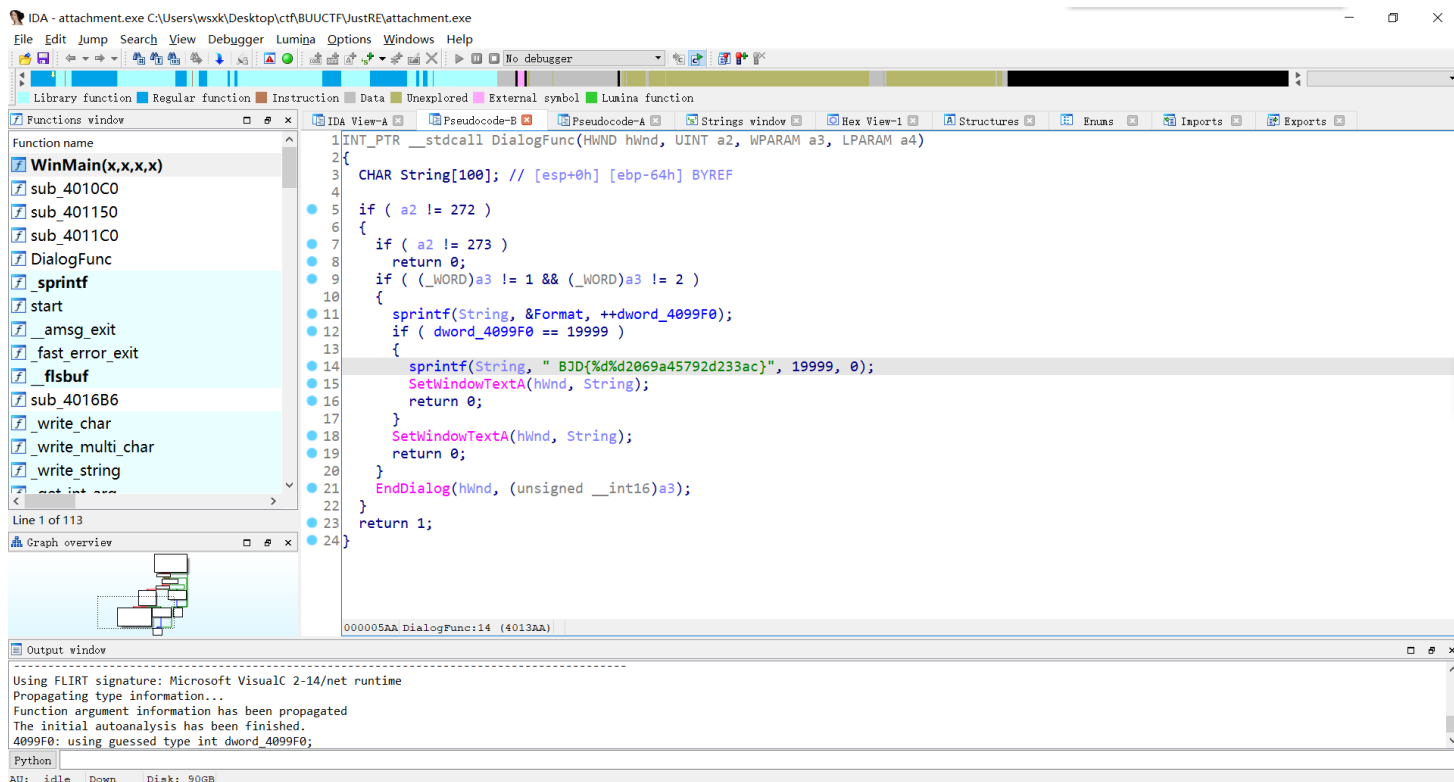
```
sub_4010C0  
sub_401150  
sub_4011C0  
DialogFunc  
_sprintf  
start  
_amsg_exit  
fast_error_exit  
if ( a2 != 272 )  
{  
    if ( a2 != 275 )  
        return 0;  
    if ( (_WORD)a3 != 1 && (  
        sprintf(string, $forma  
        if ( dword_4099F0 == 3  
    )  
}
```



找到是哪一行代码修改了它



可以发现是0x40137b的地址修改了它
在ida中搜索0x40137b,也能找到



一样得到flag

其实也可以动态调试，问题不是很大

flag{1999902069a45792d233ac}