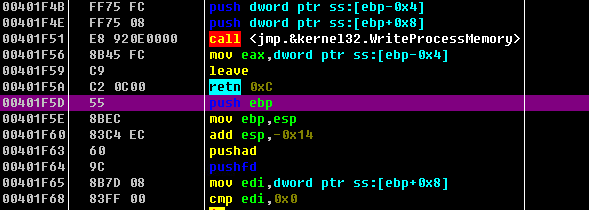
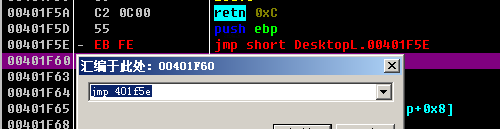
在附加进程 之前要确保所有相关的 进程全部杀掉，因为程序本身具有互斥体的检测：

直接调试DesktopLayer.exe,跳到401f5d的位置（这块应该是像chrome注入的地方）



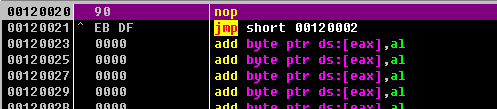
之后再下一句处修改汇编指令为： jmp 401f5E(意思就是让他不断地跳到自己的地方，创建一个死循环) 修改之前记得把之前的汇编指令复制一下，下边还会用



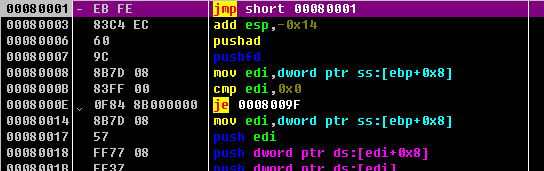
修改这个位置的汇编指令

修改完之后，F9，把程序跑起来，之后再打开一个OD，按F1附加进程，选择Chrome进程

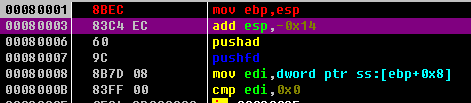
附加之后进来是这样的（这个好像不确定，每次都是不一样的）



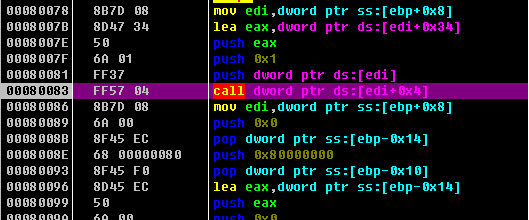
之后，f9跑起来之后，需要手动暂停下来（因为我们之前设置了死循环，所以可以停下来），到了这，可以看到这个就是我们创建的死循环，之后再这个地方把汇编指令修改回来，（修改成原来的汇编指令：mov ebp esp）



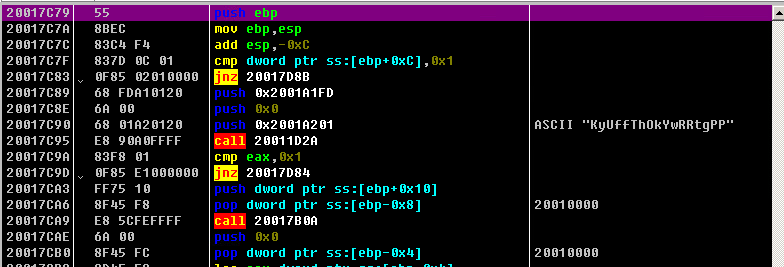
修改之后：



接着f4运行到这：（就在修改汇编指令下边的10来行）



F7进去之后就可以接着分析了：



和IDA的地址对不上是因为，加了基址（通过OD的地址找IDA的地址的话，需要减去10010000）