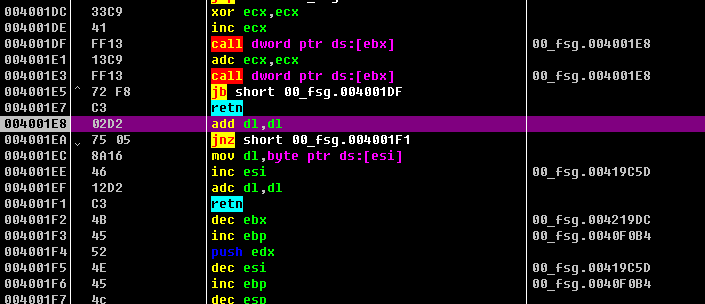
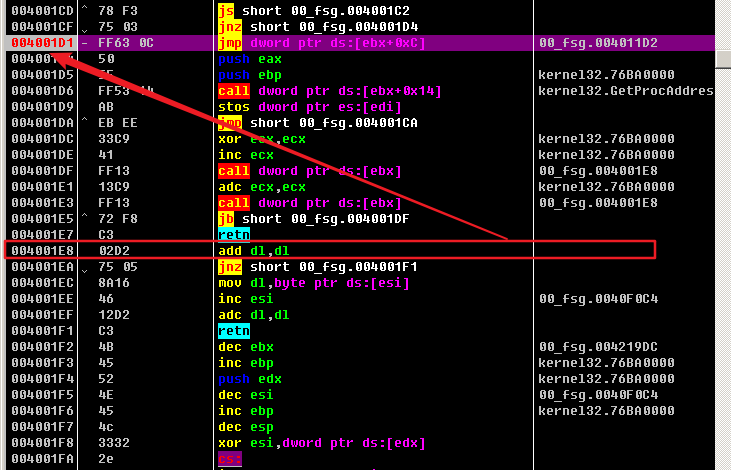


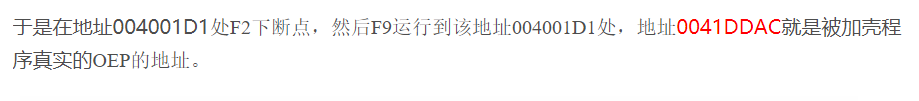
shift+f9

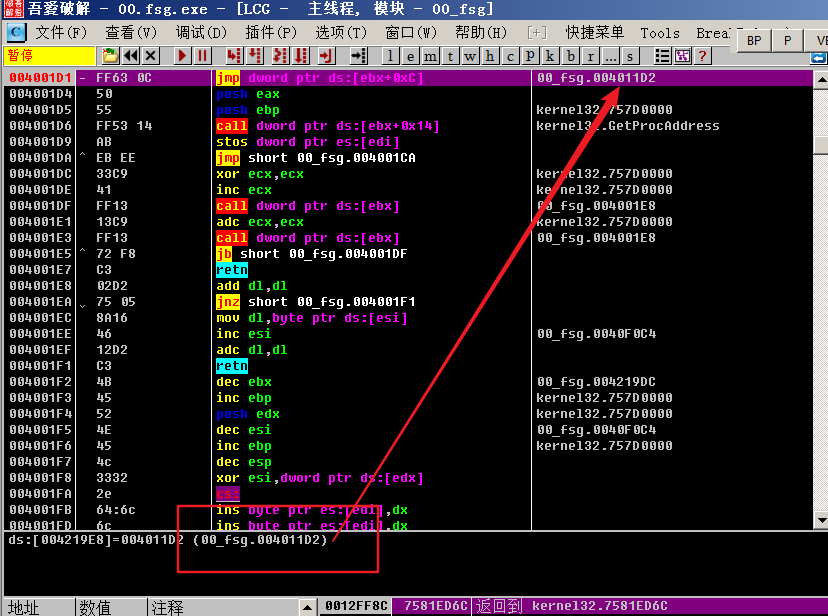


向上找jmp，下断点，重新加载程序，f9直接运行到断点处

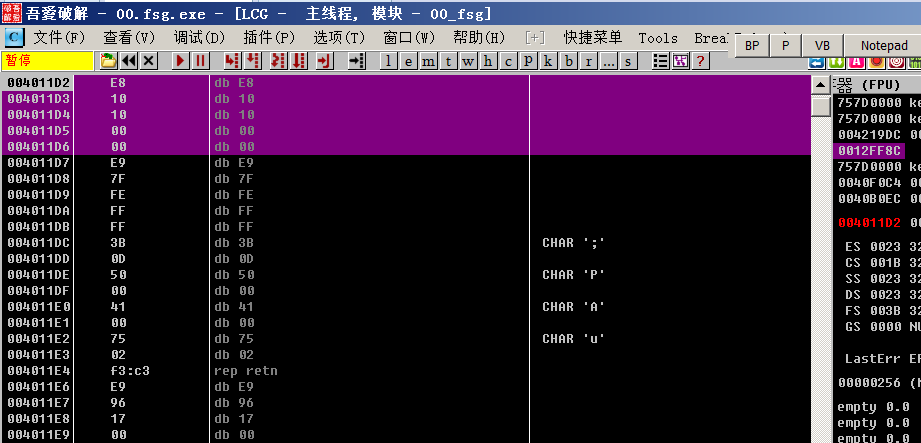


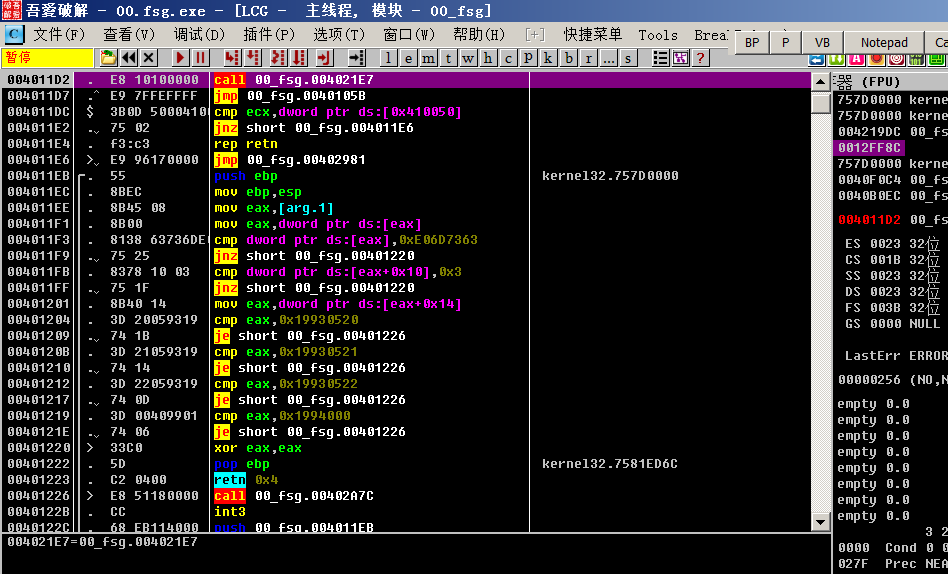
enter进入来到jmp



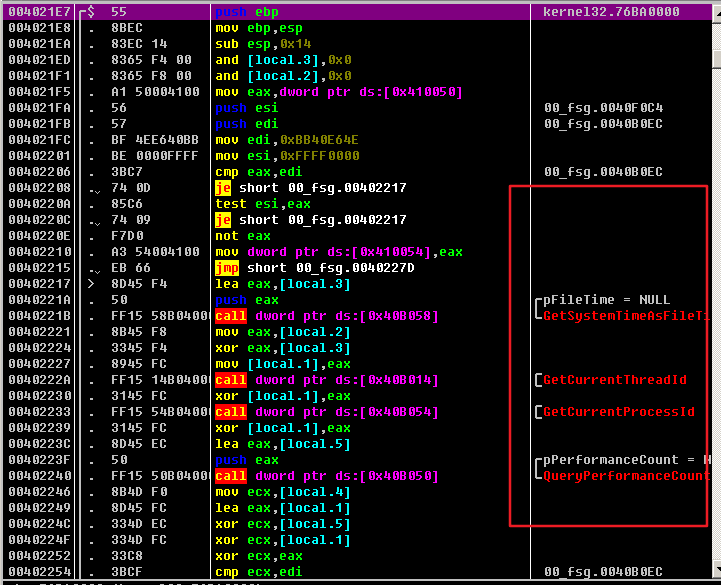


F7进入，选中未正确显示的，右键分析代码

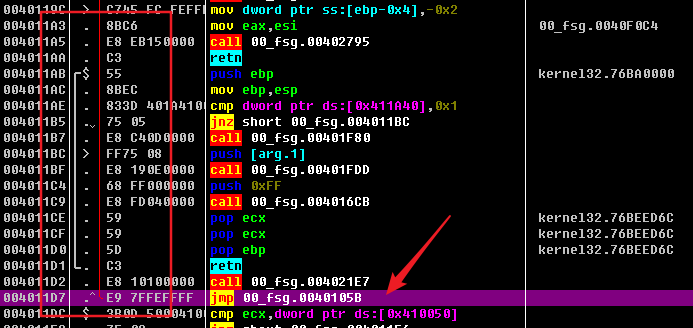




再次进入发现此call确实为入口

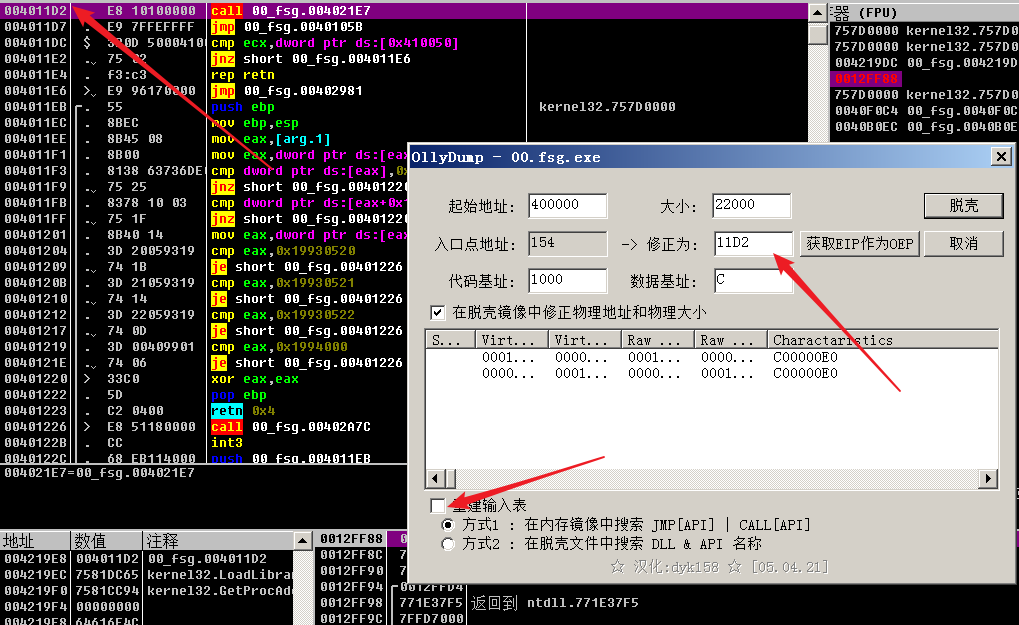


退回来，往下看jmp为大跳，确实是入口点

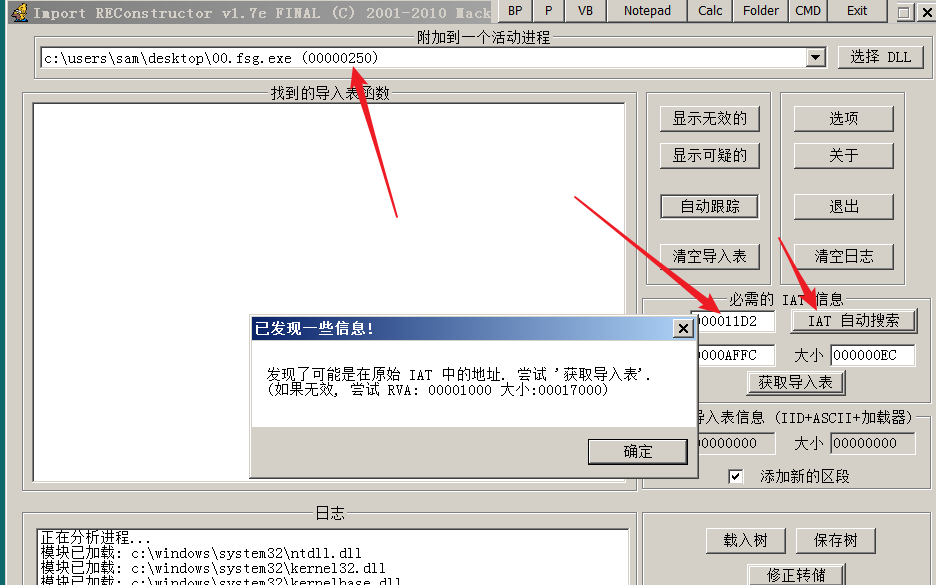




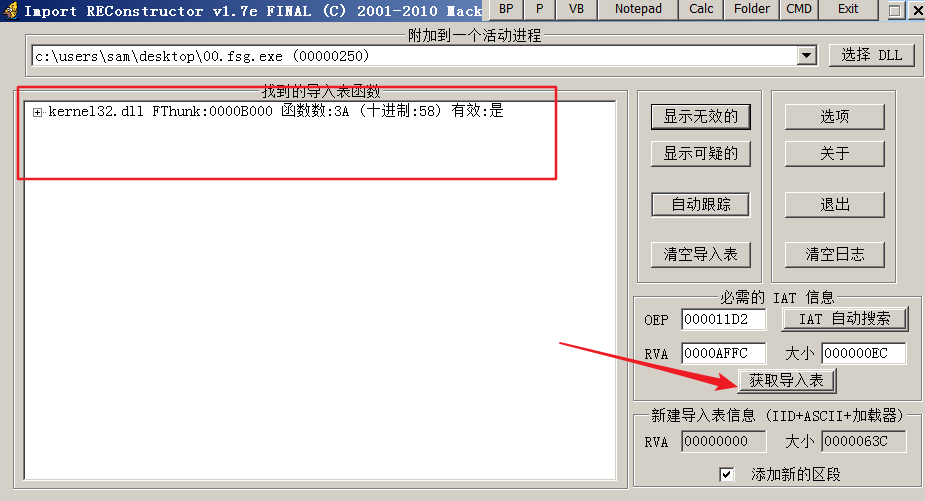
在call处右键脱壳——4011d2



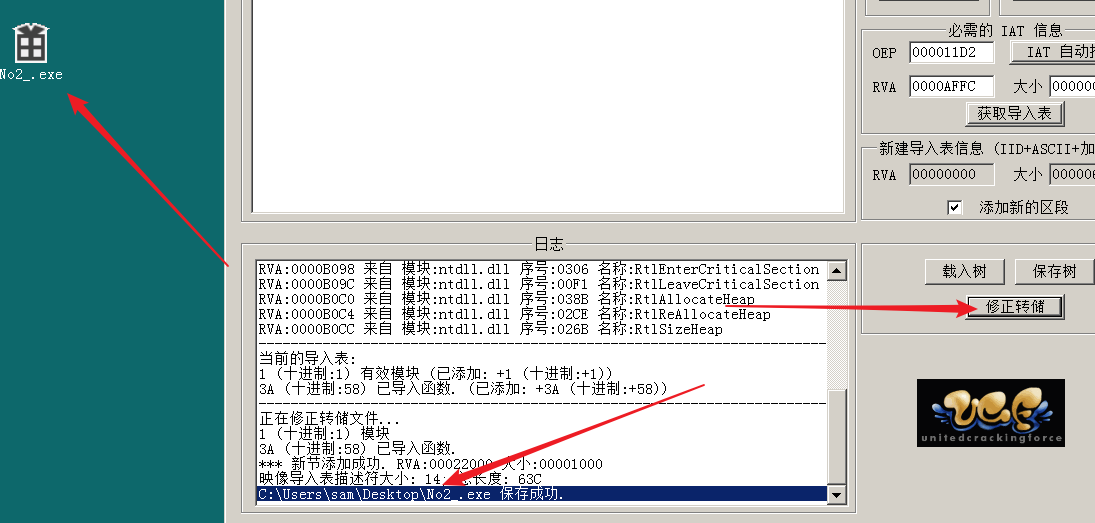
recImport修复重定位表地址



获取导入表，发现只有一个，应该不正常

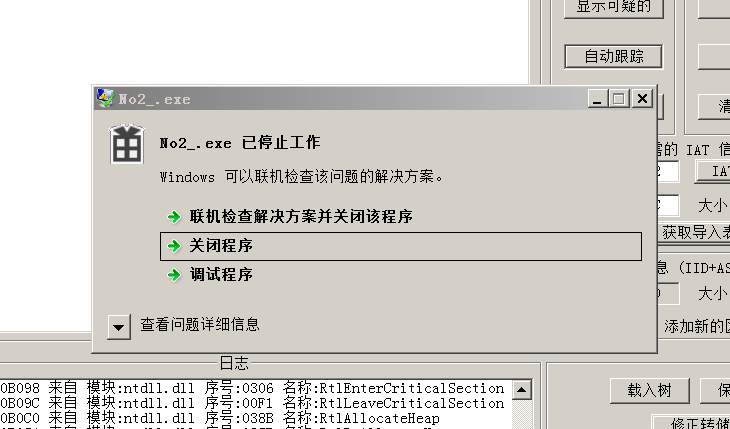


修正转储一下



运行发现确实不正确

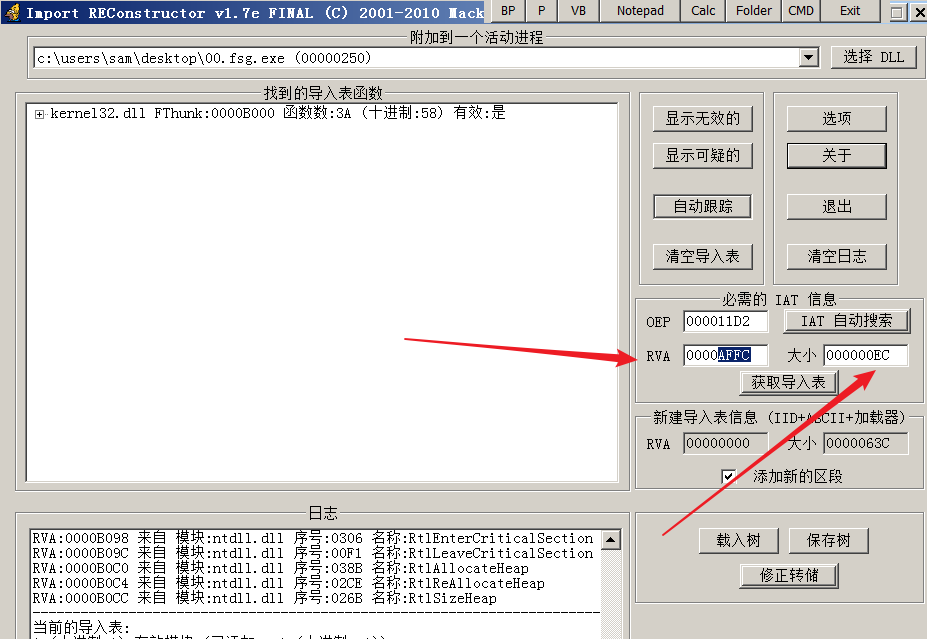




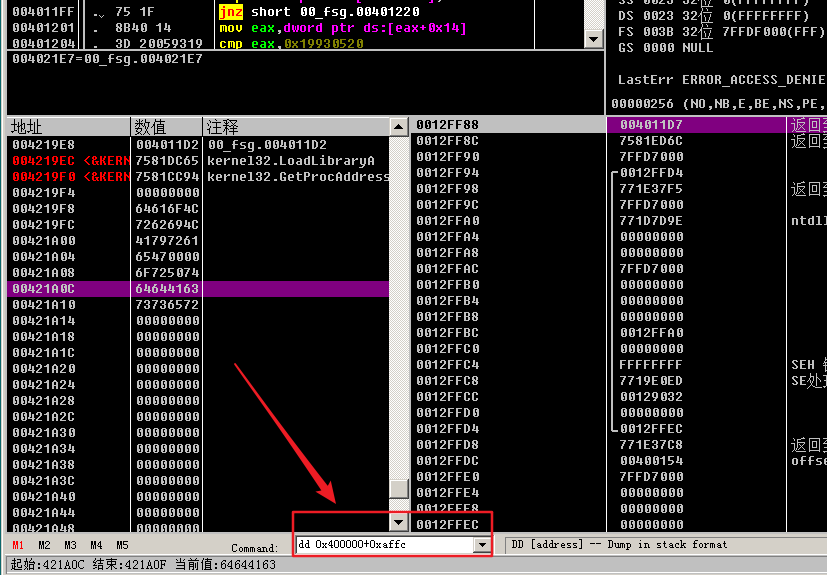
手动修复IAT表的方式：

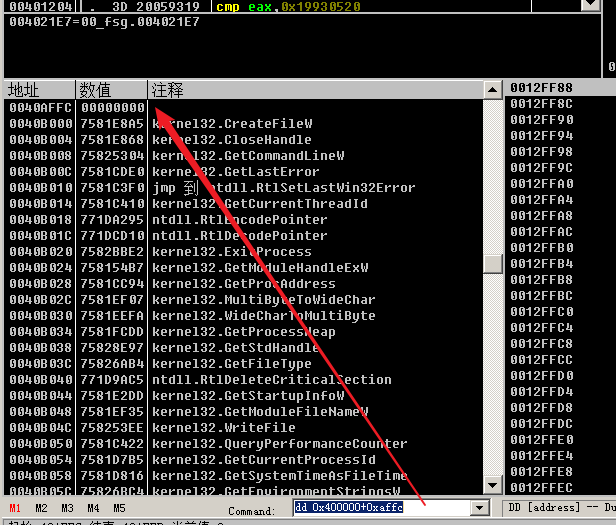
遗憾啦，RECImport工具没用使用好，通过OD查看内存数据发现，RECImport工具对Dump后的程序的IAT的修复不完全。

在RECImport工具中，IAT自动搜索到的程序的导入表的函数不完全。如图，函数导入表的起始RVA地址是0000AFFC，函数导入表的结束RVA地址是0000AFFC +EC=0000B0E8也就导入表函数的个数是0xEC，但是经过OD的观察发现，这两个参数有误。

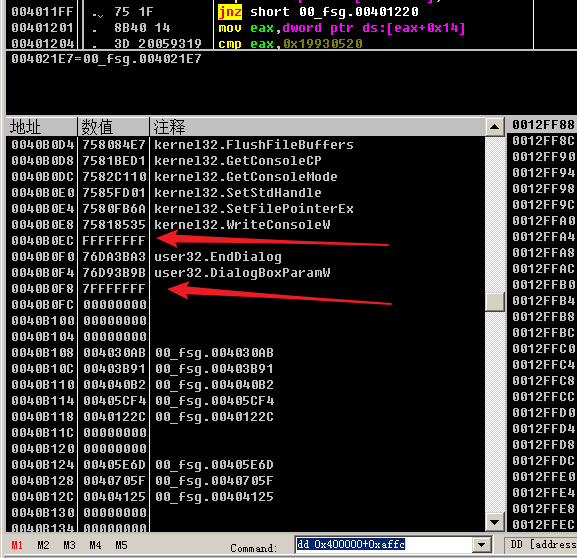


回到OD中，输入地址，回车来到此地址处



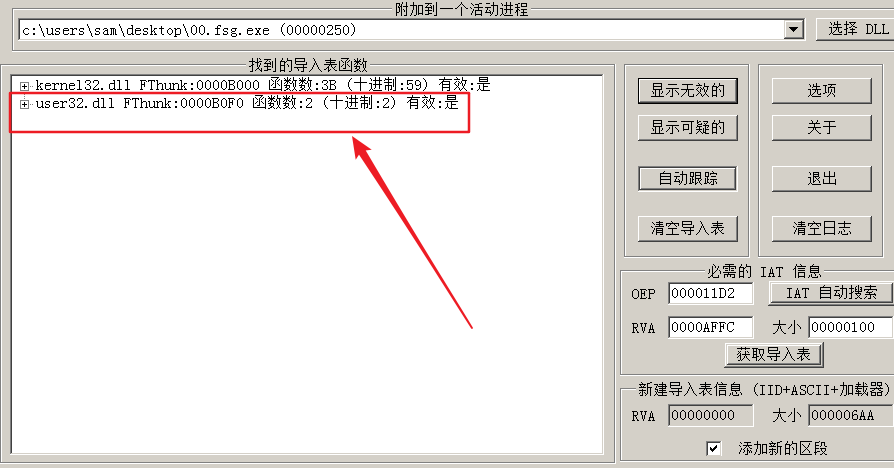


如下两处为异常，修改为0

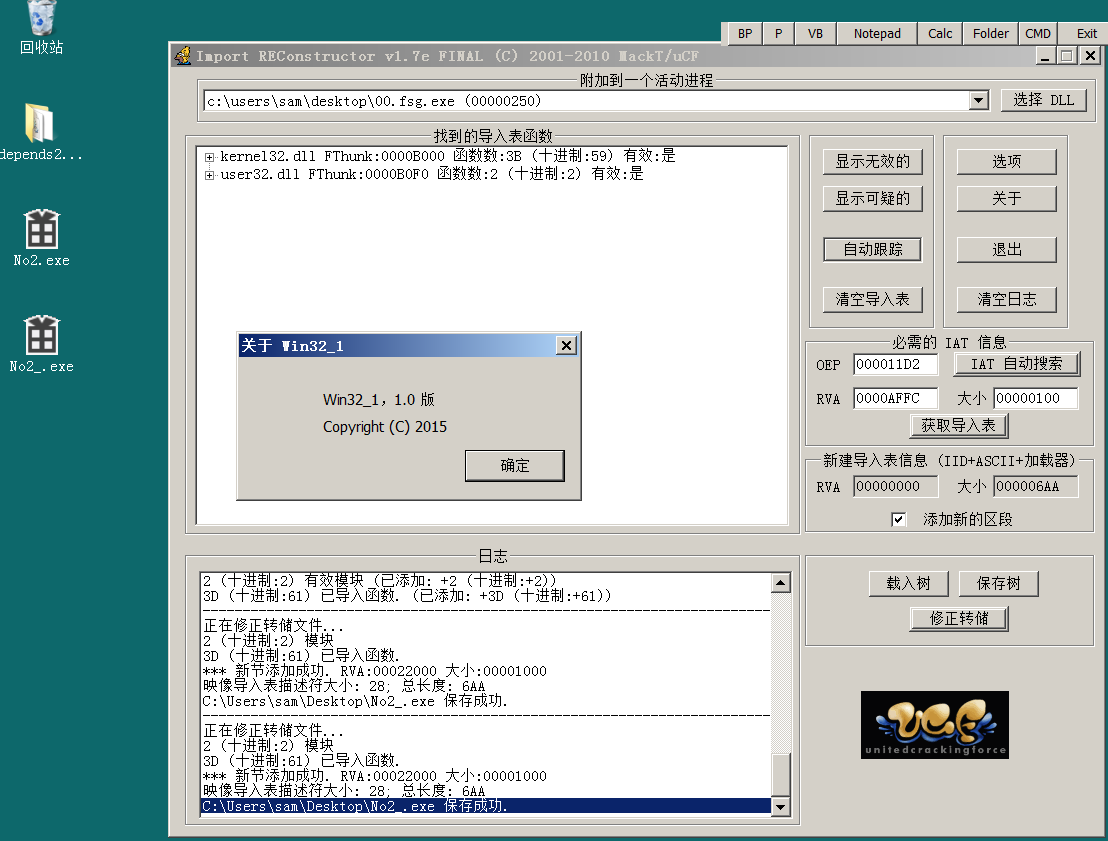




重新打开RecImport 导入fsg.exe，进行上一步操作，出现了新导入表，正常



修正转储，运行成功



<https://blog.csdn.net/qq1084283172/article/details/46817103>