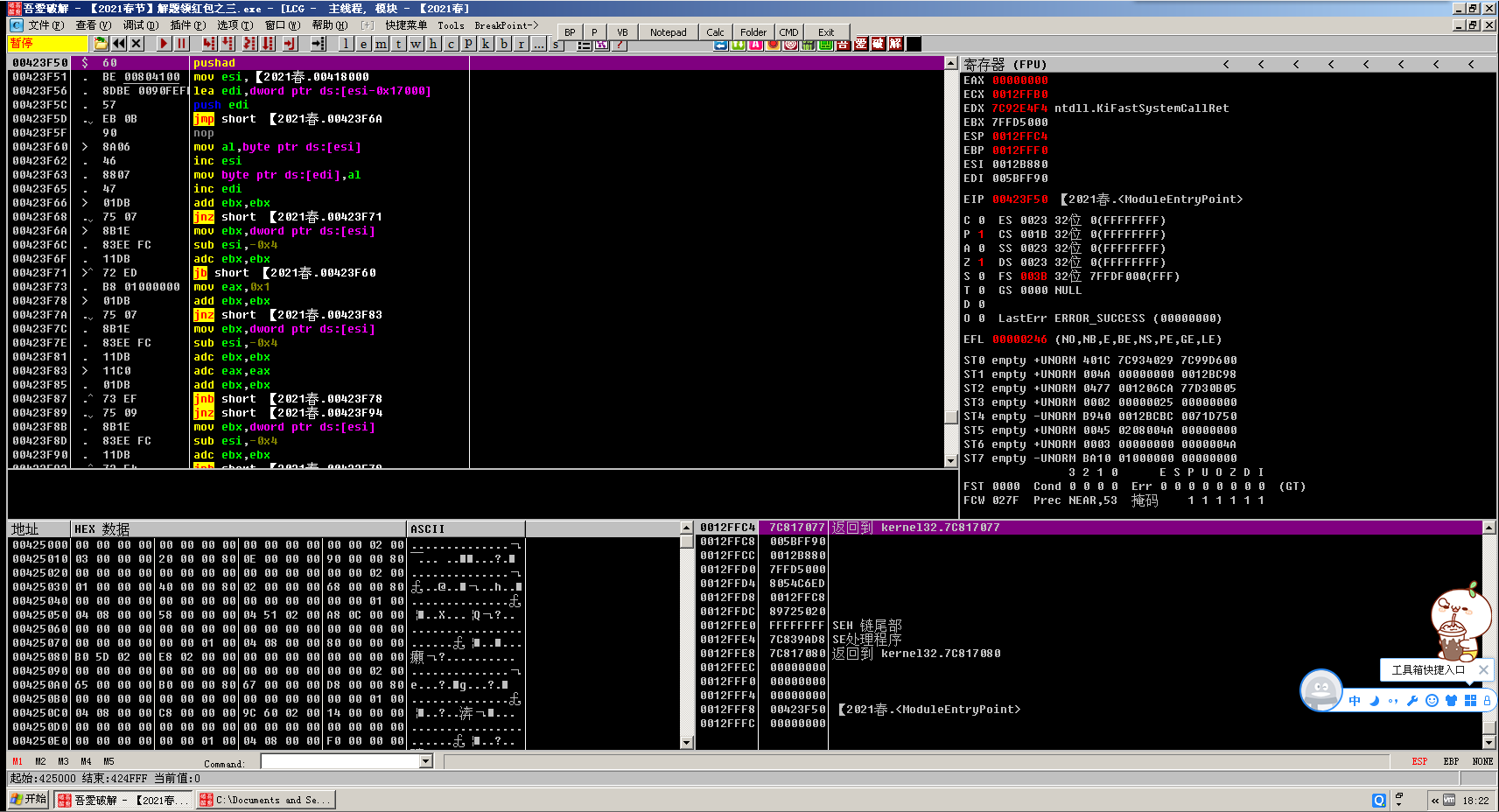
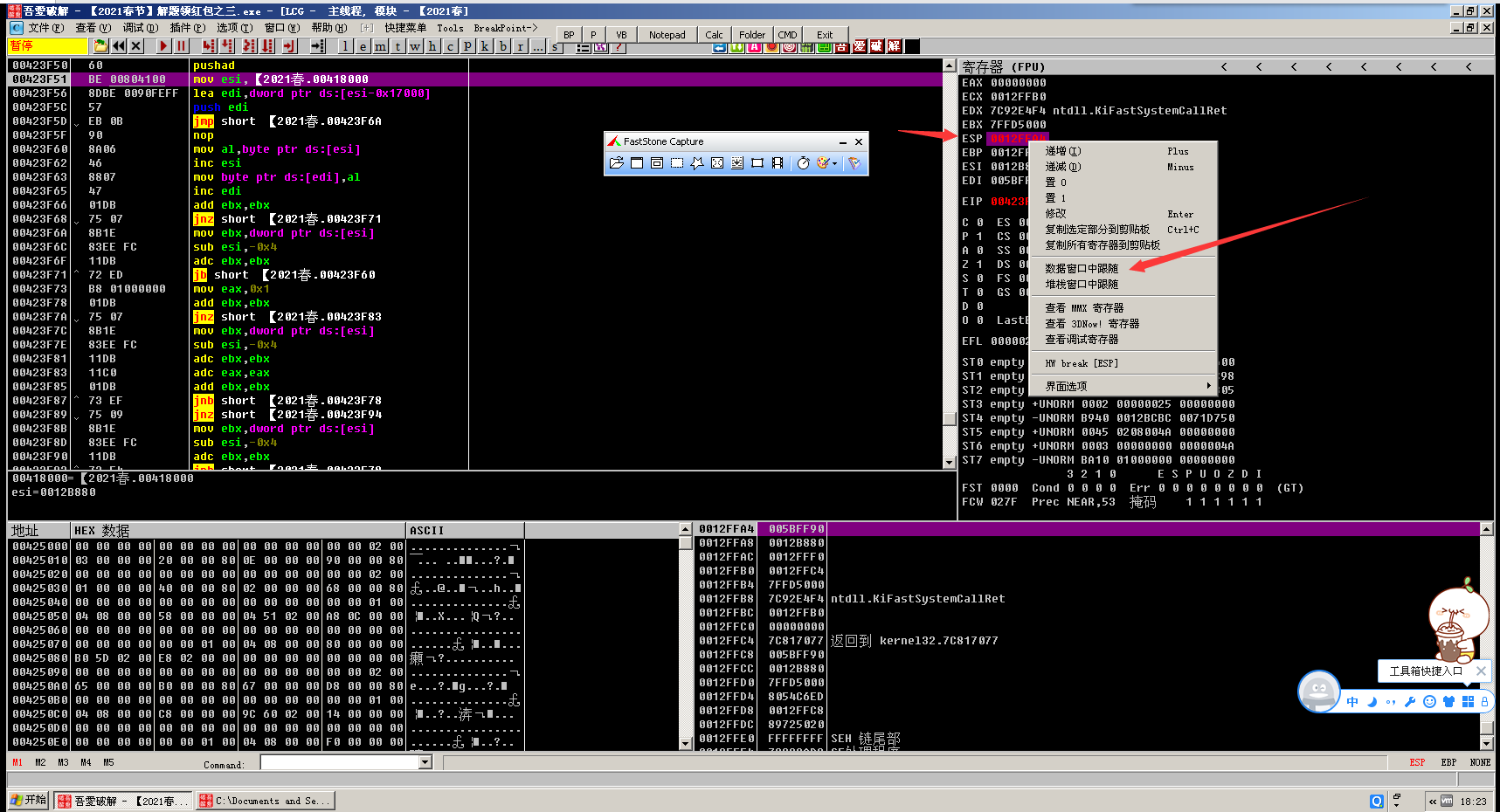
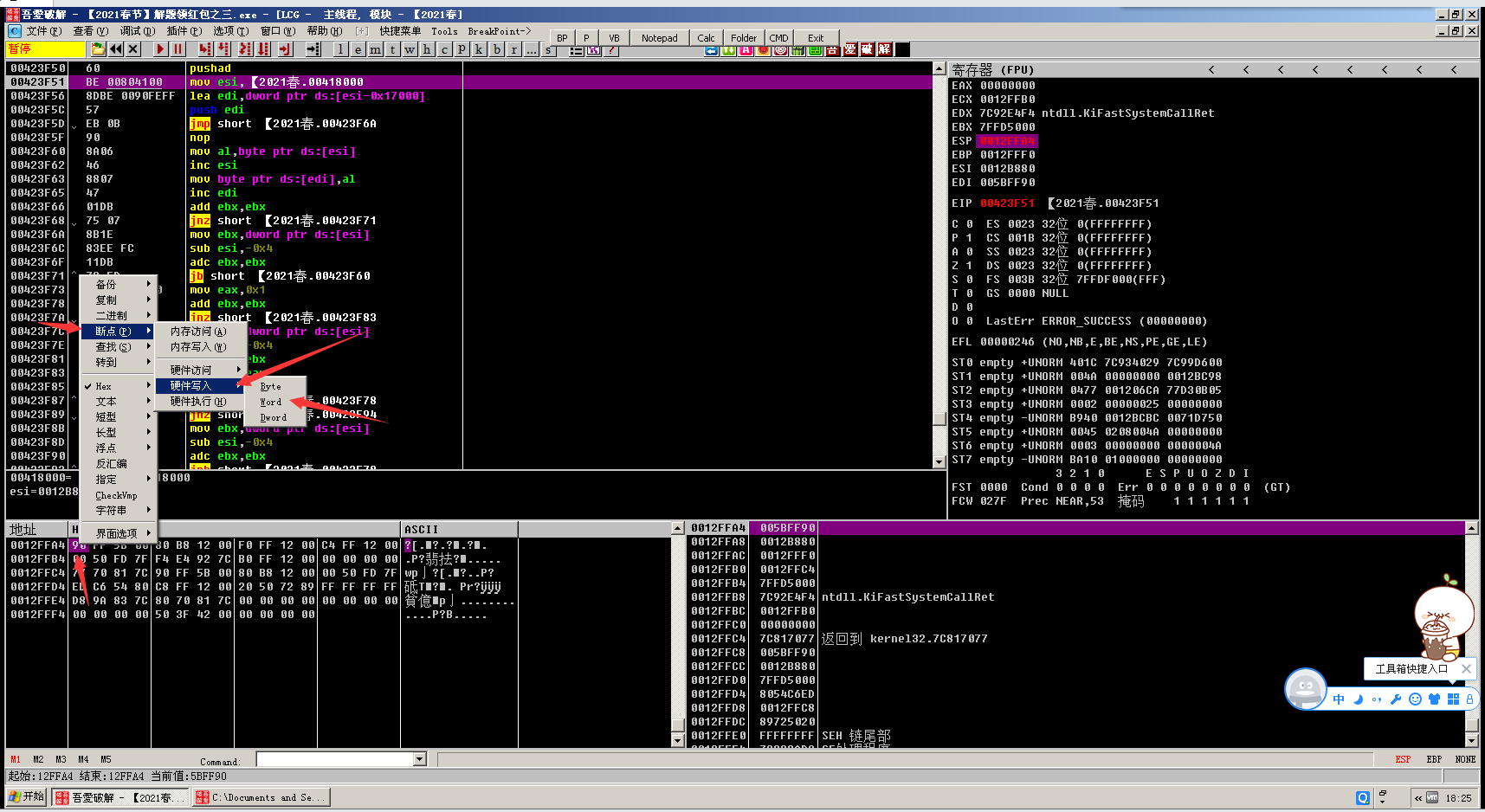
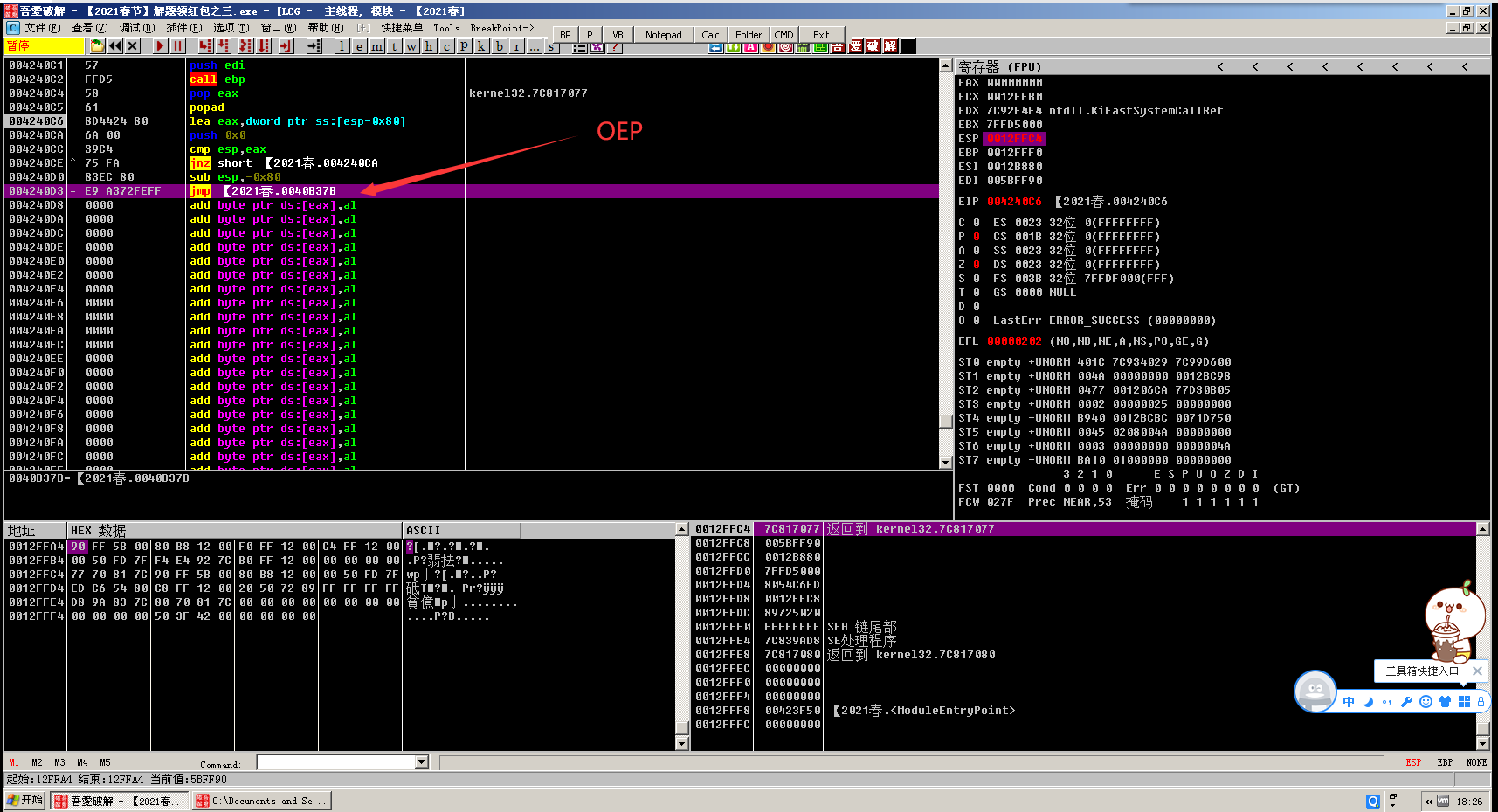
1.载入后看到压栈指令pushfd，使用esp定律，F8单步



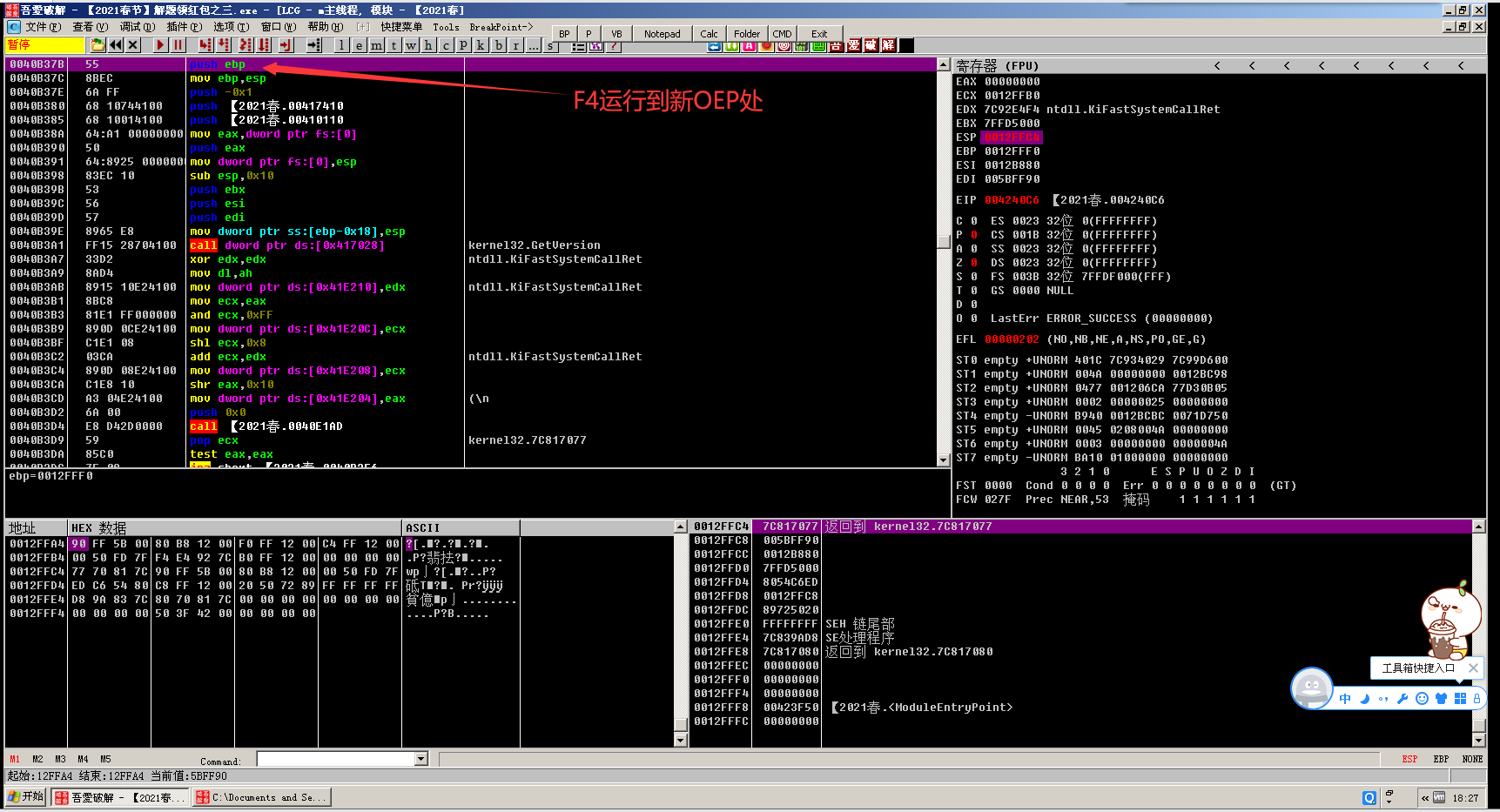
2.可以看到寄存器窗口ESP产生变化，选中后右键数据窗口跟随，在HEX数据窗口选中一行数据，设置硬件断点

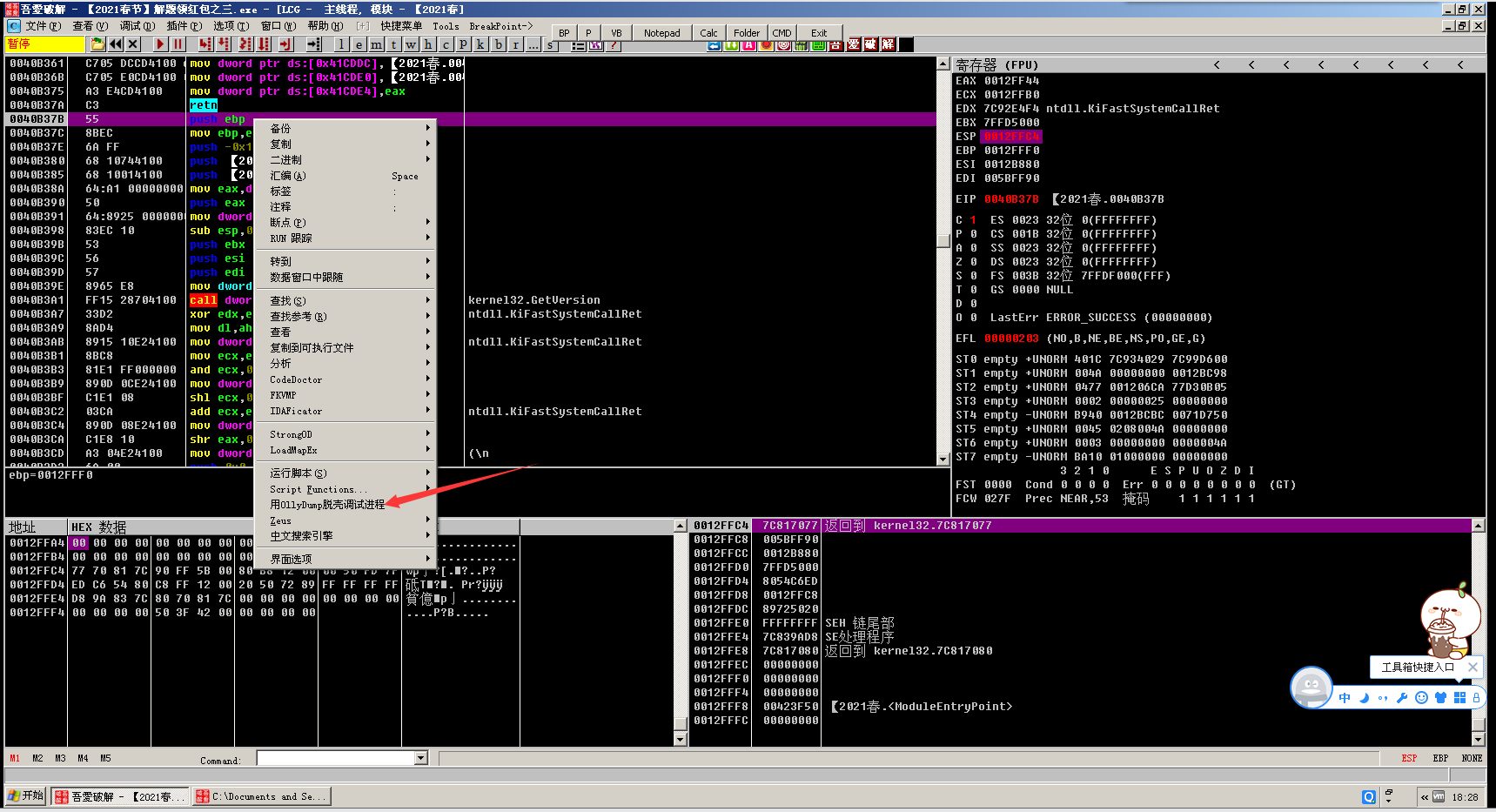


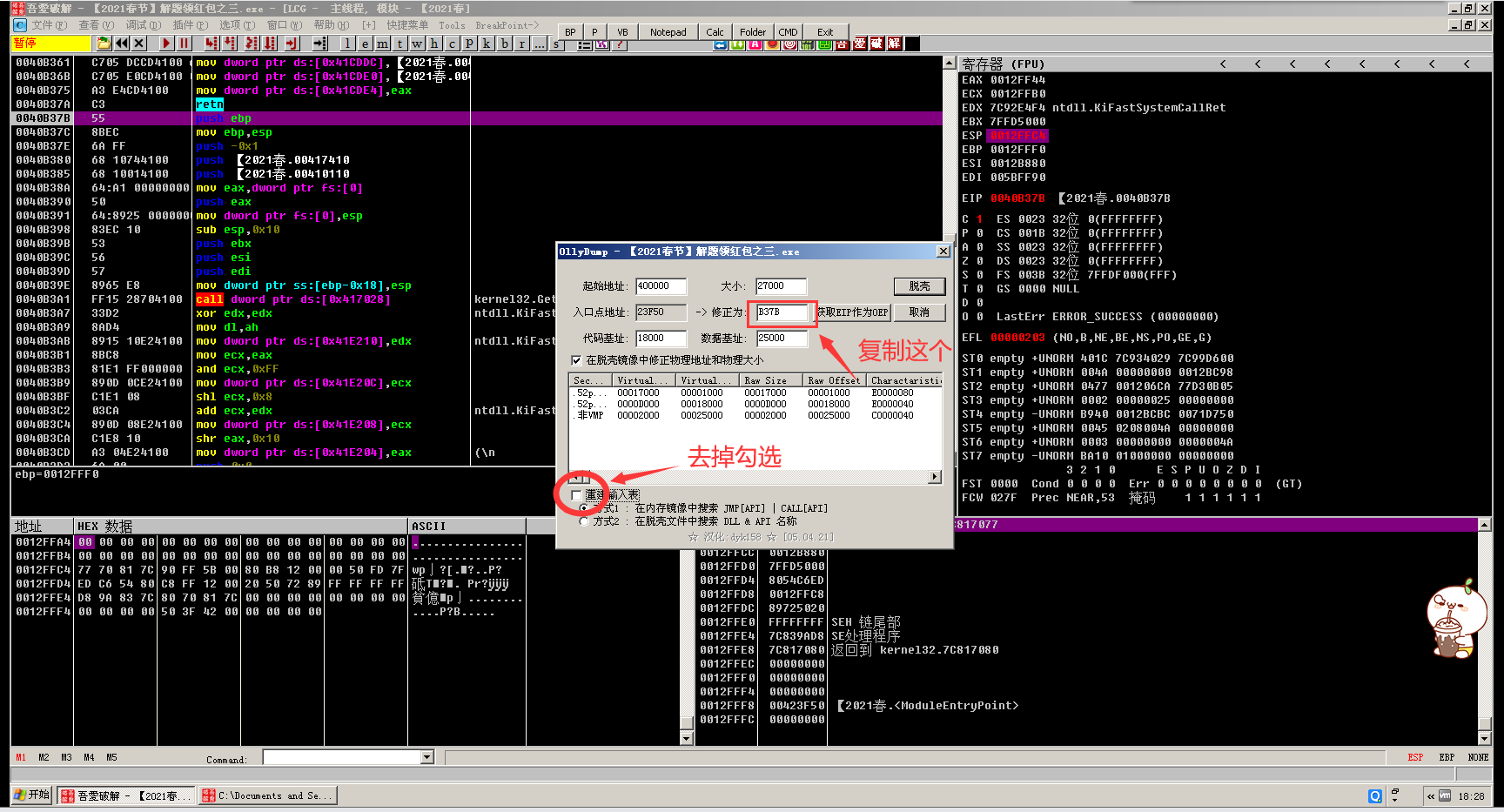




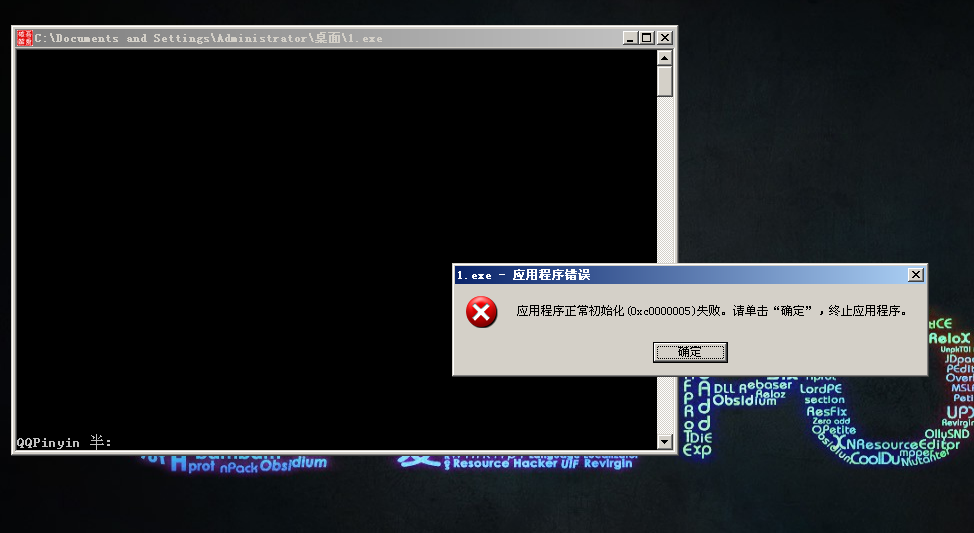
3. F4断点运行到新OEP，右键脱壳，记住红框处修正地址，不勾选重建输入表，确定导出到脱壳文件1.exe



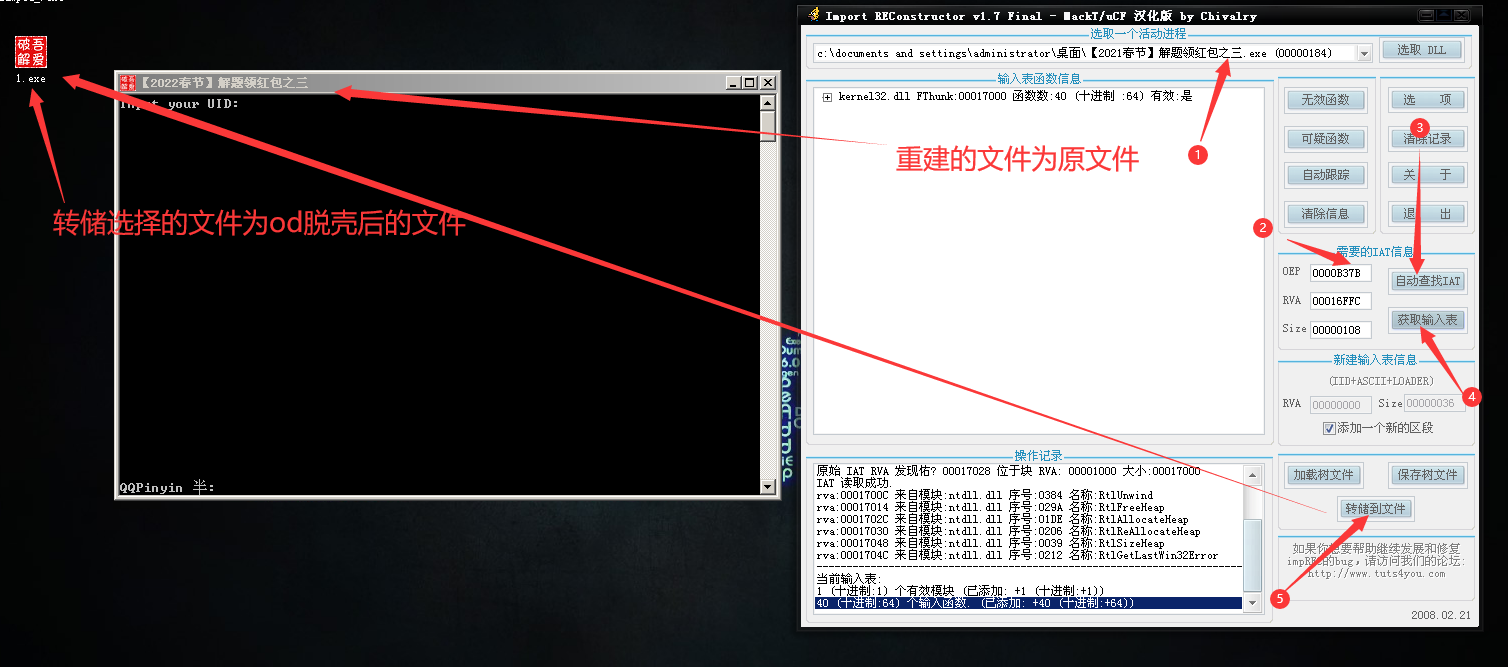




4. 运行原程序,使用importREC重建，选中未脱壳原程序进程，在OEP处输入刚刚记住的修正地址，记得加上00，然后IAT自动搜索 -- 获取导入表 -- 修正转储 –选择脱壳完的1.exe文件



无法运行,所以要修复输入表,使用importREC



5.运行修复后文件

