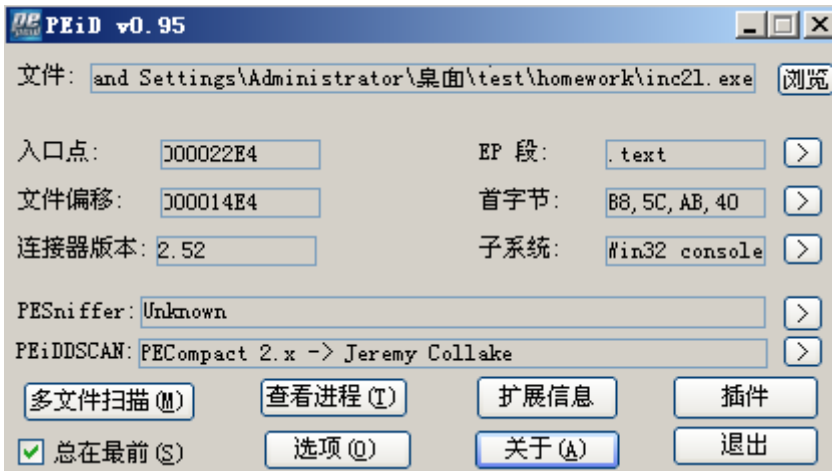
ESP定律脱壳

ESP定律的原理就是“**堆栈平衡**”原理。

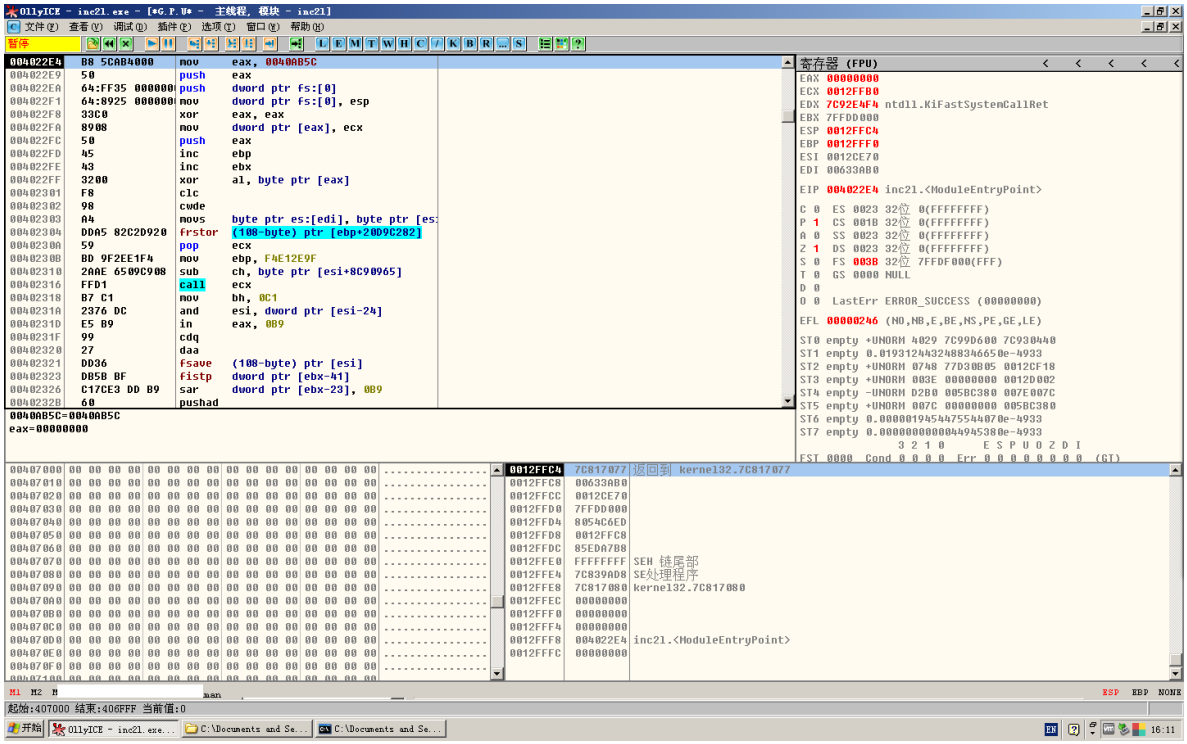
在无对抗性的压缩壳下，在壳对原始程序还原后，必定会对寄存器等环境进行还原。那么就可以利用压缩壳最开始对寄存器保存和最后跳入OEP时对寄存器还原这一特点定位OEP

以inc2l程序为例

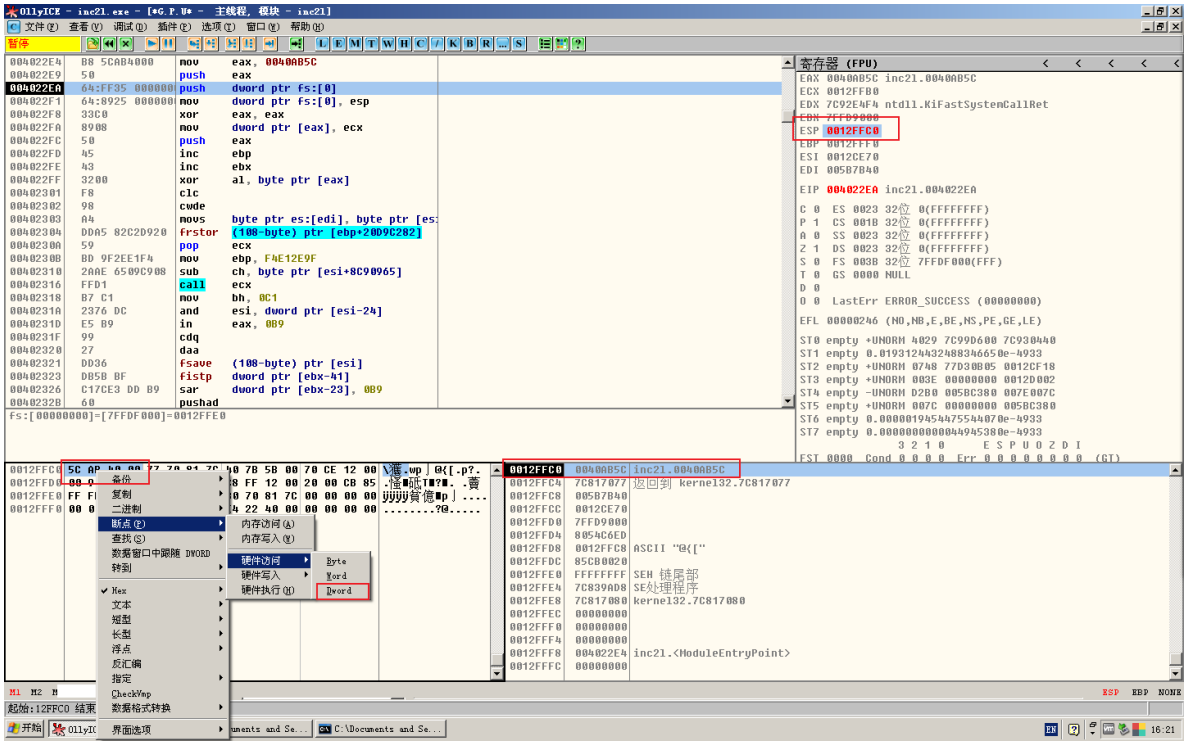
先用PEID查看下特征



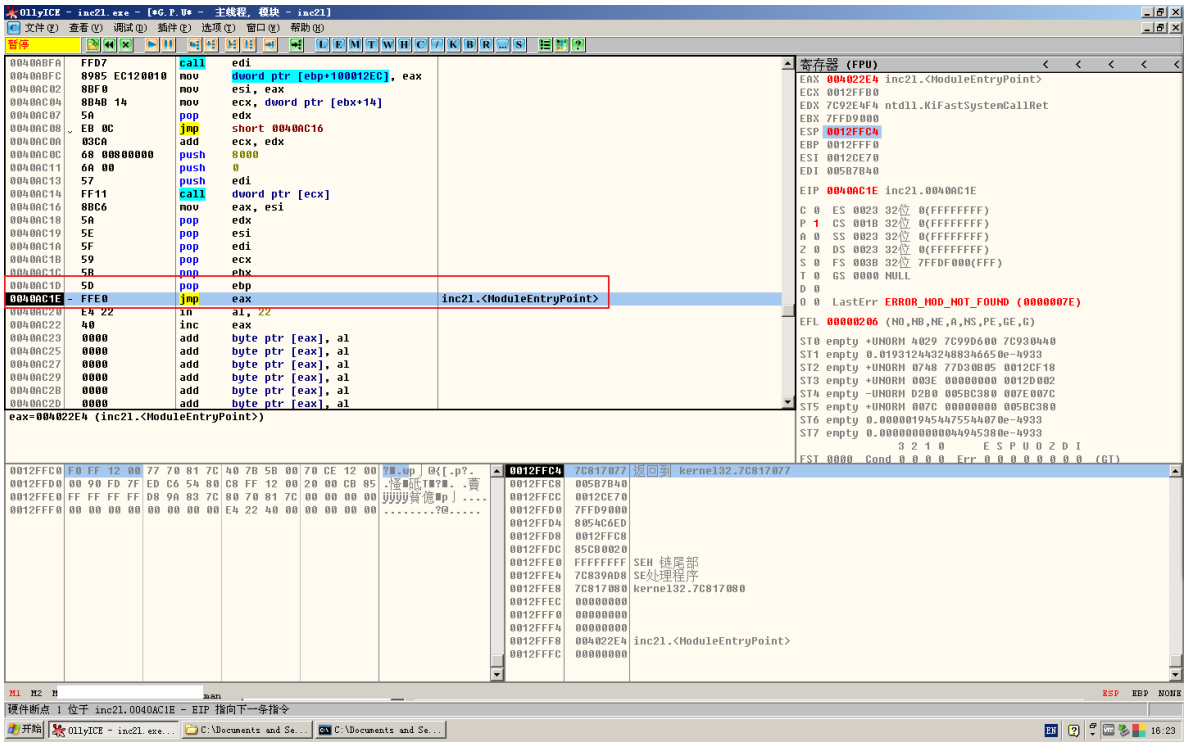
载入OD，入口点下方有个`push`



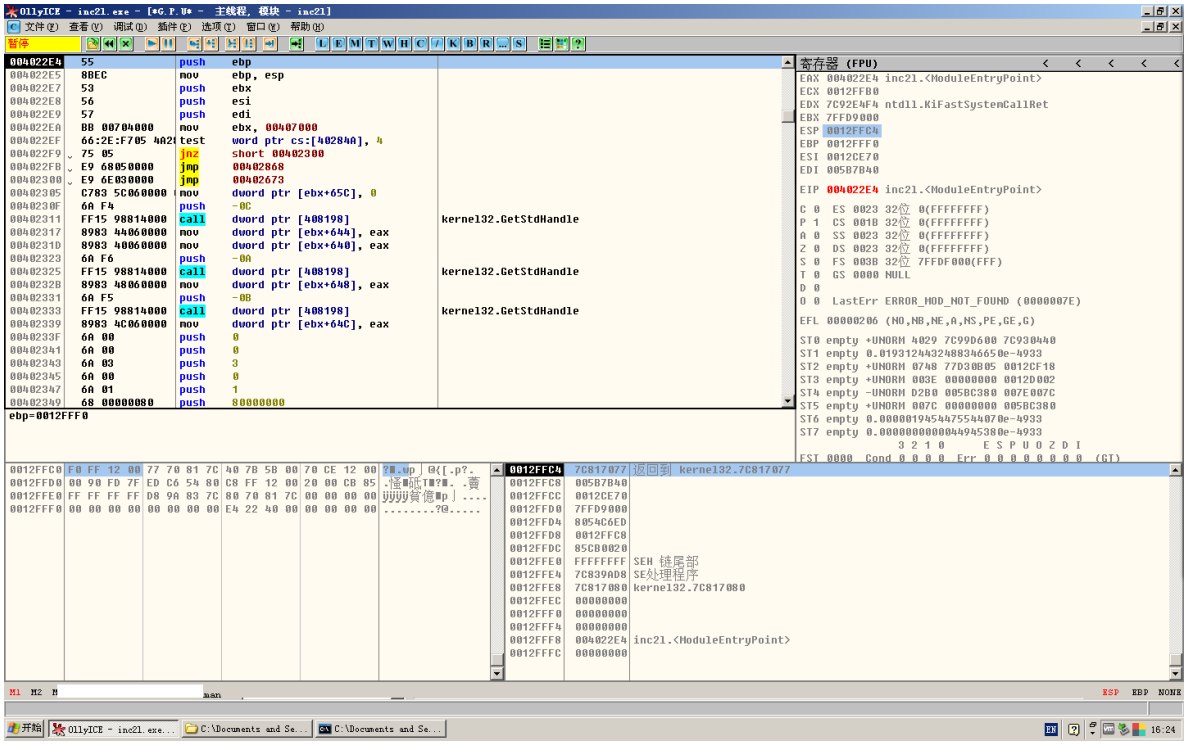
执行完`push`指令后在对ESP所指向的内存地址中的数据下硬件访问断点（内存访问也可，就是效率低）



然后F9运行持续跟踪并查看上下文中的指令，找到有大量的`pop`操作后有个大`jmp`

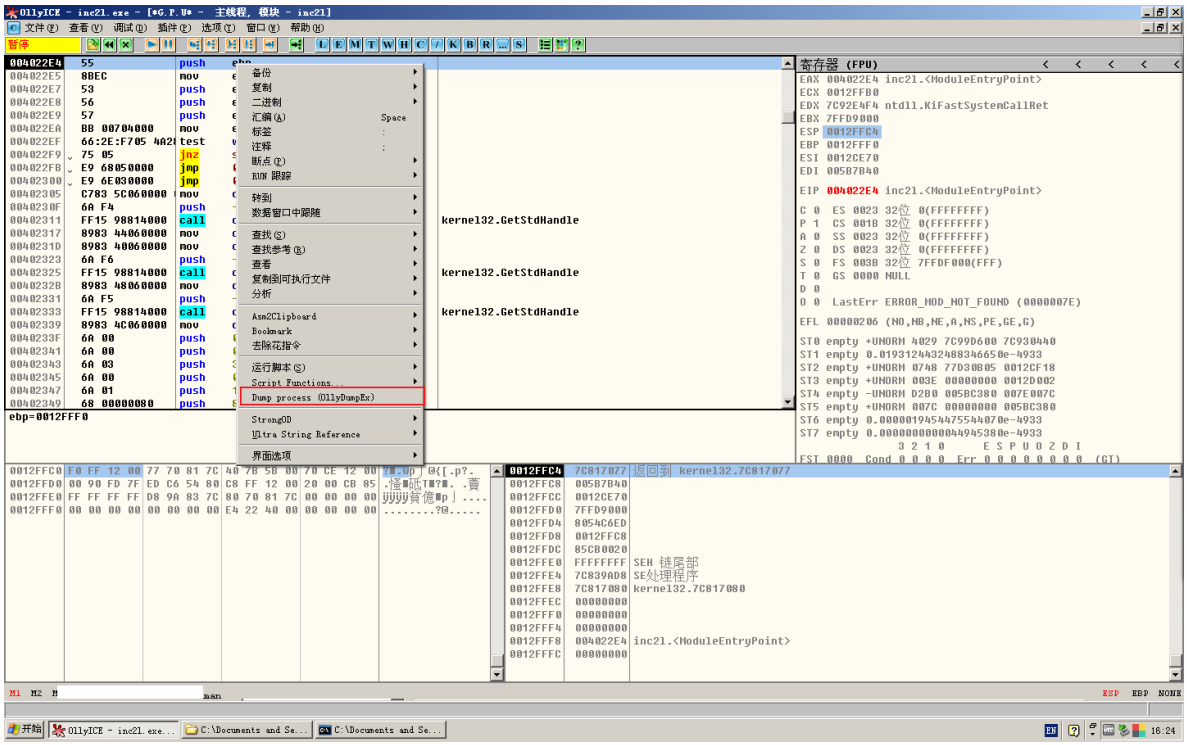


即找到了OEP

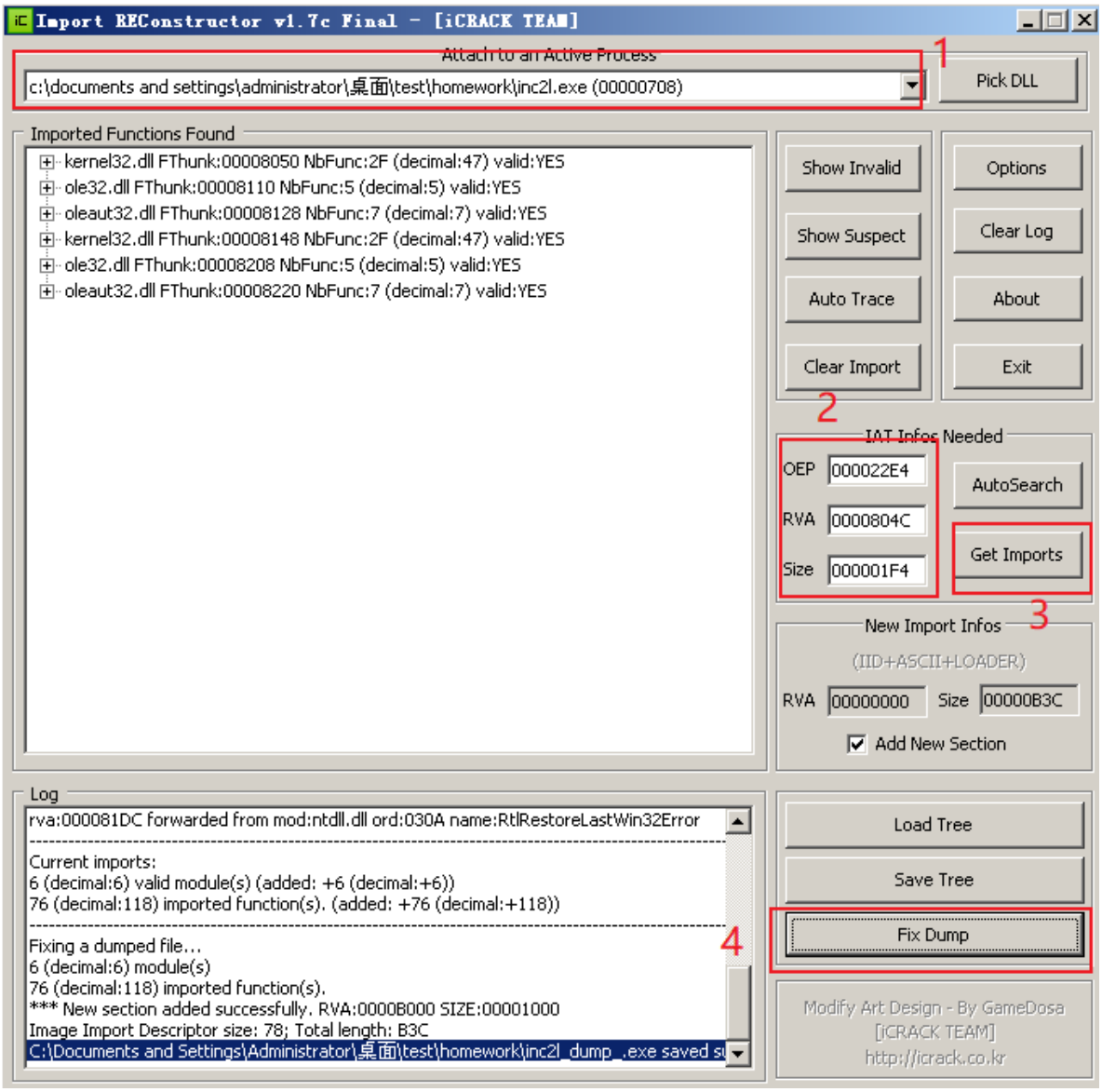


脱壳

使用OD的脱壳插件，一切选项默认



修复导入表，利用工具Import REC打开OD中正在调试的进程读取IAT（因为IAT是在程序加载的时候填写，所以必须要打开正在运行的程序才能获取到IAT的信息），然后修复到我们dump下来的程序中


Import REConstructor v1.7c Final - [iCRACK TEAM]
Attach to an Active Process
1
c:\documents and settings\administrator\桌面\test\homework\inc2l.exe (00000708)
Pick DLL
Imported Functions Found
kernel32.dll FThunk:00008050 NbFunc:2F (decimal:47) valid:YES
ole32.dll FThunk:00008110 NbFunc:5 (decimal:5) valid:YES
oleaut32.dll FThunk:00008128 NbFunc:7 (decimal:7) valid:YES
kernel32.dll FThunk:00008148 NbFunc:2F (decimal:47) valid:YES
ole32.dll FThunk:00008208 NbFunc:5 (decimal:5) valid:YES
oleaut32.dll FThunk:00008220 NbFunc:7 (decimal:7) valid:YES
Show Invalid
Options
Show Suspect
Clear Log
Auto Trace
About
Clear Import
Exit
2
IAT Infos Needed
OEP 000022E4
RVA 0000804C
Size 000001F4
AutoSearch
Get Imports
3
New Import Infos
(IID+ASCII+LOADER)
RVA 00000000
Size 00000B3C
Add New Section
Log
rva:000081DC forwarded from mod:ntdll.dll ord:030A name:RtlRestoreLastWin32Error
Current imports:
6 (decimal:6) valid module(s) (added: +6 (decimal:+6))
76 (decimal:118) imported function(s). (added: +76 (decimal:+118))
Fixing a dumped file...
6 (decimal:6) module(s)
76 (decimal:118) imported function(s).
*** New section added successfully. RVA:0000B000 SIZE:00001000
Image Import Descriptor size: 78; Total length: B3C
C:\Documents and Settings\Administrator\桌面\test\homework\inc2l_dump_.exe saved
4
Load Tree
Save Tree
Fix Dump
Modify Art Design - By GameDosa
[iCRACK TEAM]
http://icrack.co.kr