### 基础知识

upx官网：<https://github.com/upx/upx>

常用命令：

upx -1 test.exe //最快压缩

upx -9 test.exe //更高的压缩率

upx --best test.exe //最大限度压缩

upx -k test.exe //保留备份文件

upx -t test.exe //查看是否为upx压缩

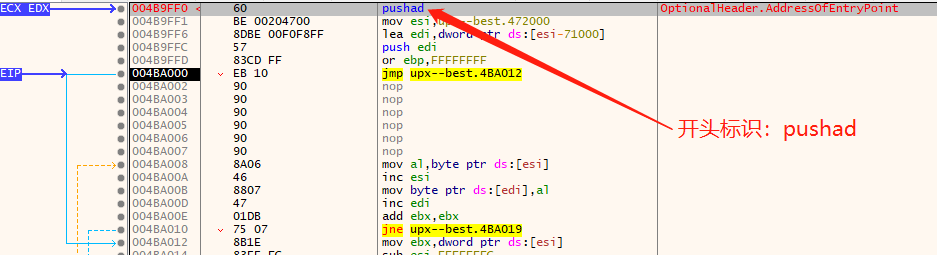
upx -l test.exe //查看upx压缩文件的详细信息

### 脱壳

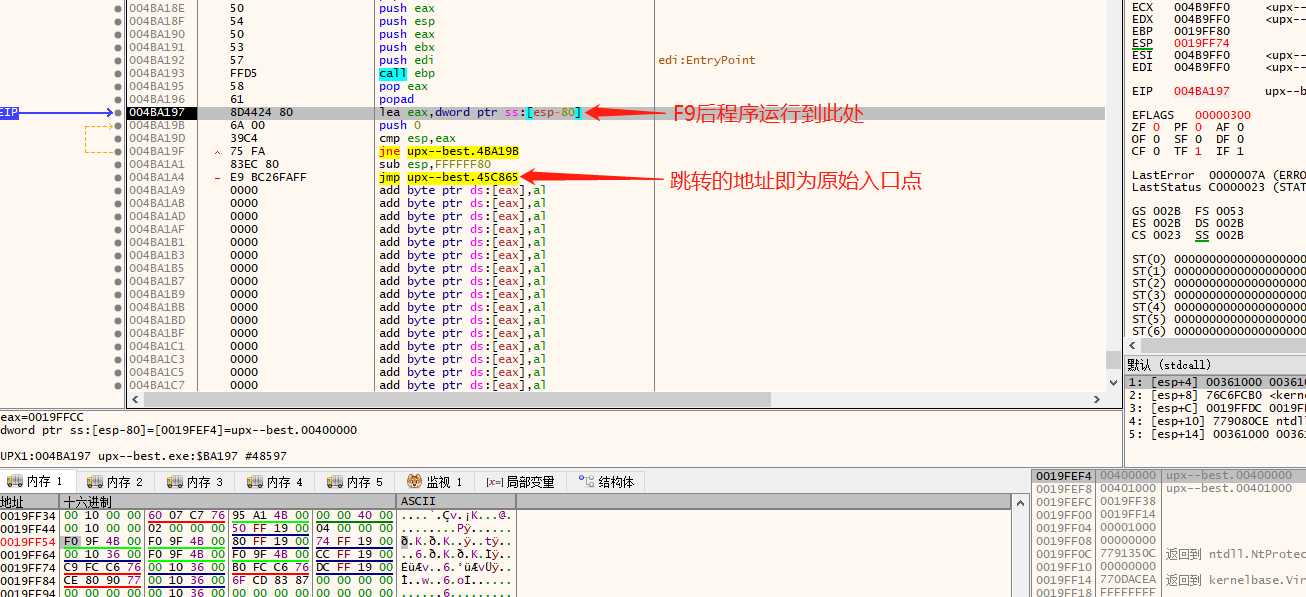
自动脱壳：

upx -d test.exe //去掉upx壳

手动脱壳（ESP定律）：



1. 将test.exe拖入x64dbg，单步F8，观察到只有ESP和EIP发生变化
2. 选中ESP，选择“在内存窗口中转到”
3. 在内存窗口中选中相应的数据，下硬件访问断点，大小为DWORD
4. F9运行程序，删除硬件断点



5、修复导入表，使用X64DBG的scylla插件修复失败，改用OD+ImportREC,打开ImportREC,载入调试的进程，填写OEP、RVA、大小；其中OEP要填写偏移地址（记得减去ImageBase）

6、寻找RVA：OD中，右键-查找-所有模块间的调用，双击程序本身的任意一个函数（不要是系统函数），右键-跟随；右键-数据窗口中跟随-内存地址；右键-长型-地址，找到IAT的开始和结束位置，得到RVA和大小，然后修正转储

### 番外

OEP的特征

vc6.0的OEP处的第一个API调用是GetVersion

VS2013是GetSystemTimeAsFileTime

Delphi是GetModuleHandleA

### 原理

1. UPX压缩后的两个区段，其中UPX0是一个空的区段，是原程序用来保存代码的地方；UPX1是保存被压缩后的程序数据的地方；通过对UPX1的处理，解码出原程序代码放到UPX0中去
2. 进行call和jmp的重定位
3. 调用LoadLibrary和GetProcAddress来进行API重定位







