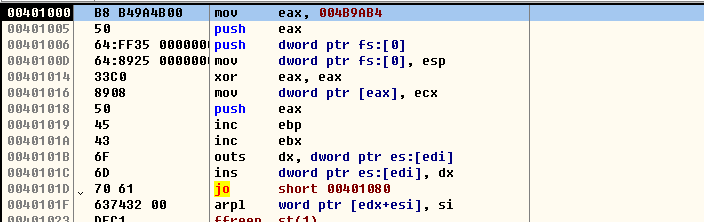
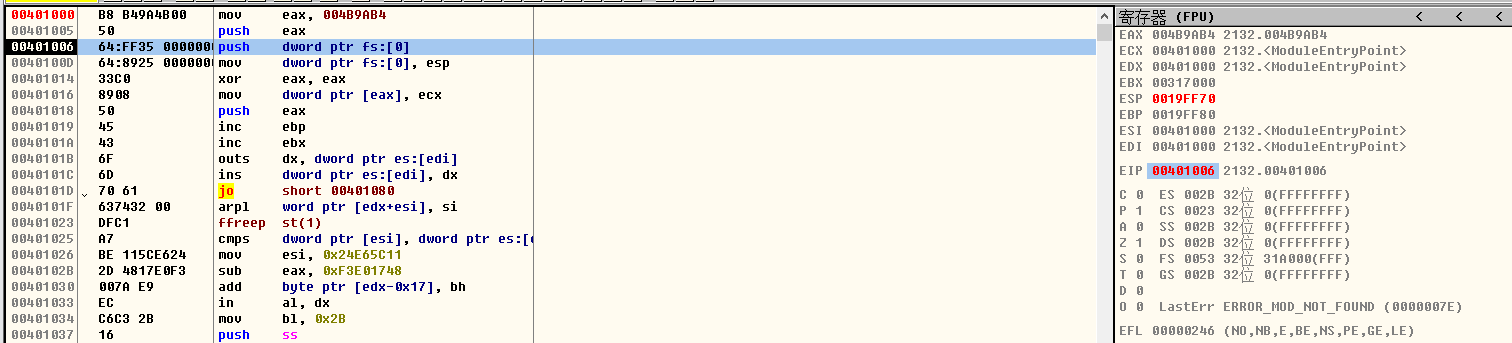
官网：<https://bitsum.com/pecompact.htm>

脱壳流程：

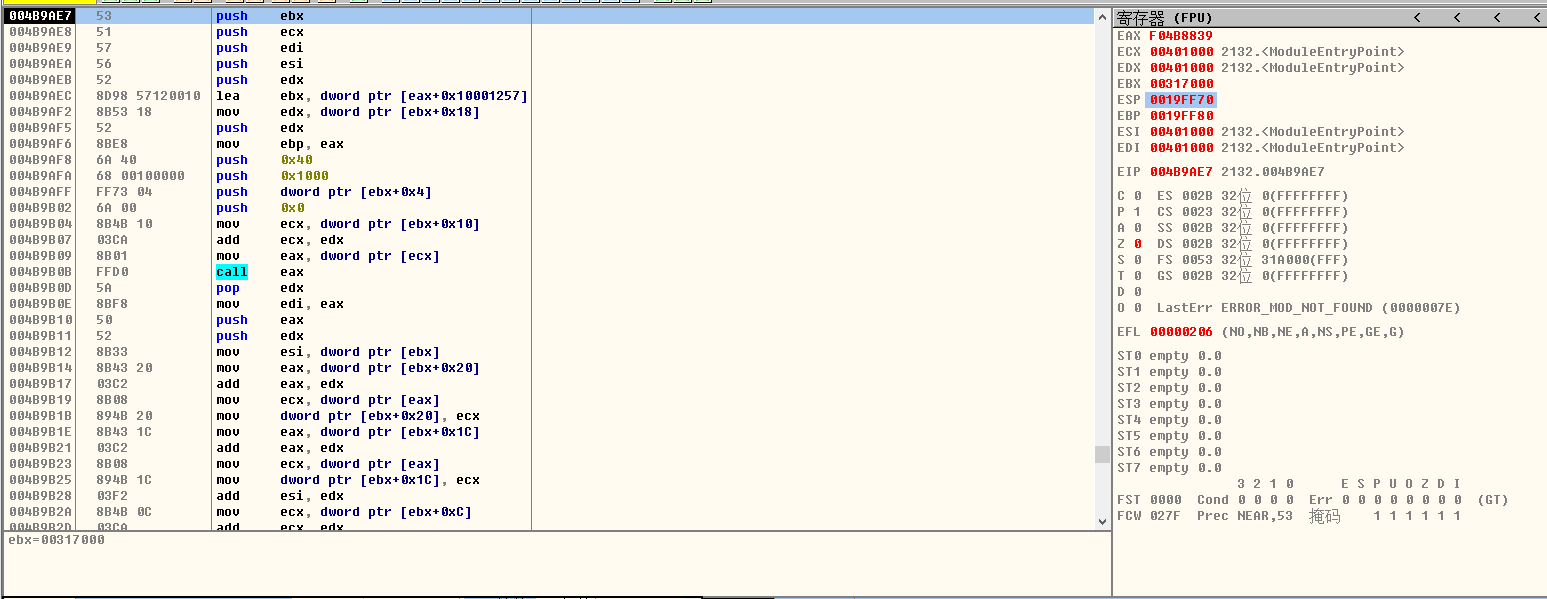
开头特征



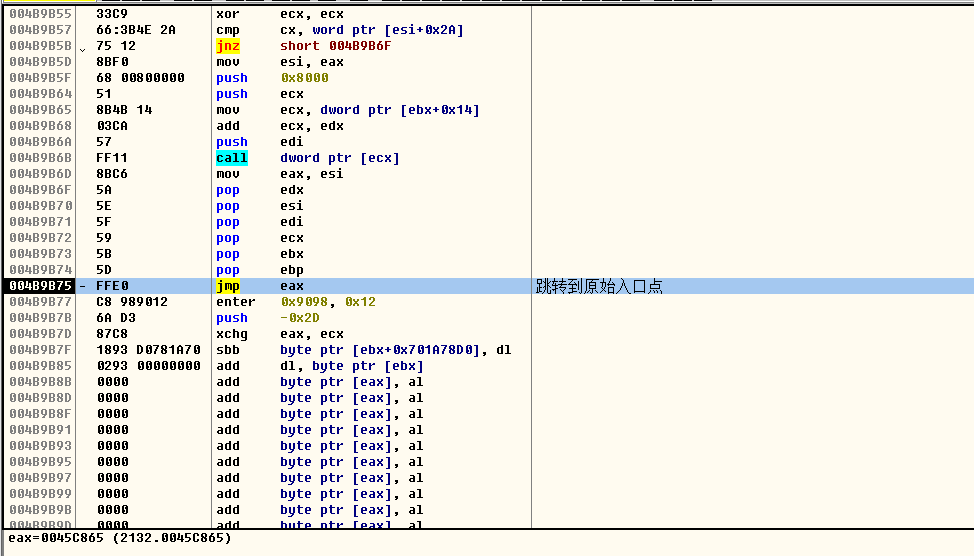
两次F8，然后ESP定律



运行程序，4次F9，观察当前模块是在ntdll中还是主模块中



向下寻找到如下特征（不远处）



之后修复导入表即可