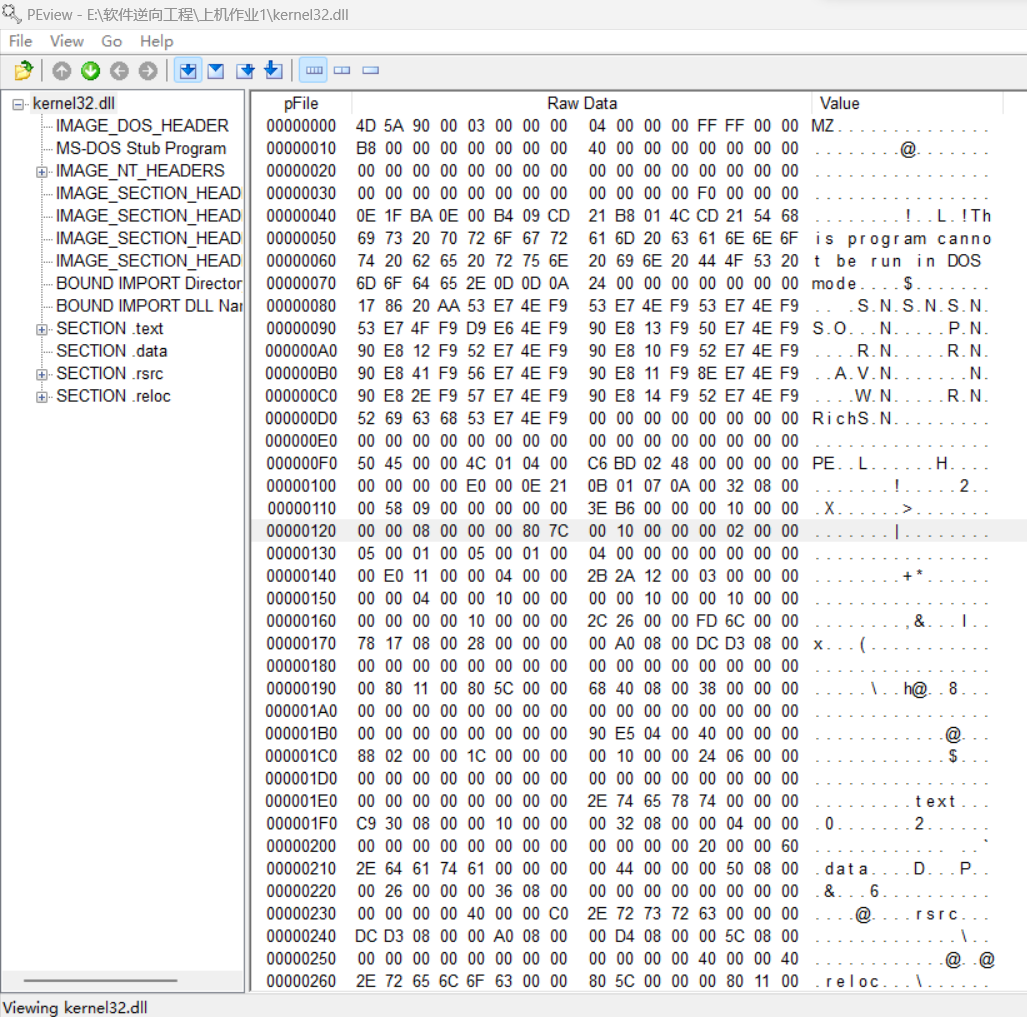
## 软件逆向工程 上机作业1：分析 kernel32.dll

使用PEviews与OllyDbg分析Kernel32.dll

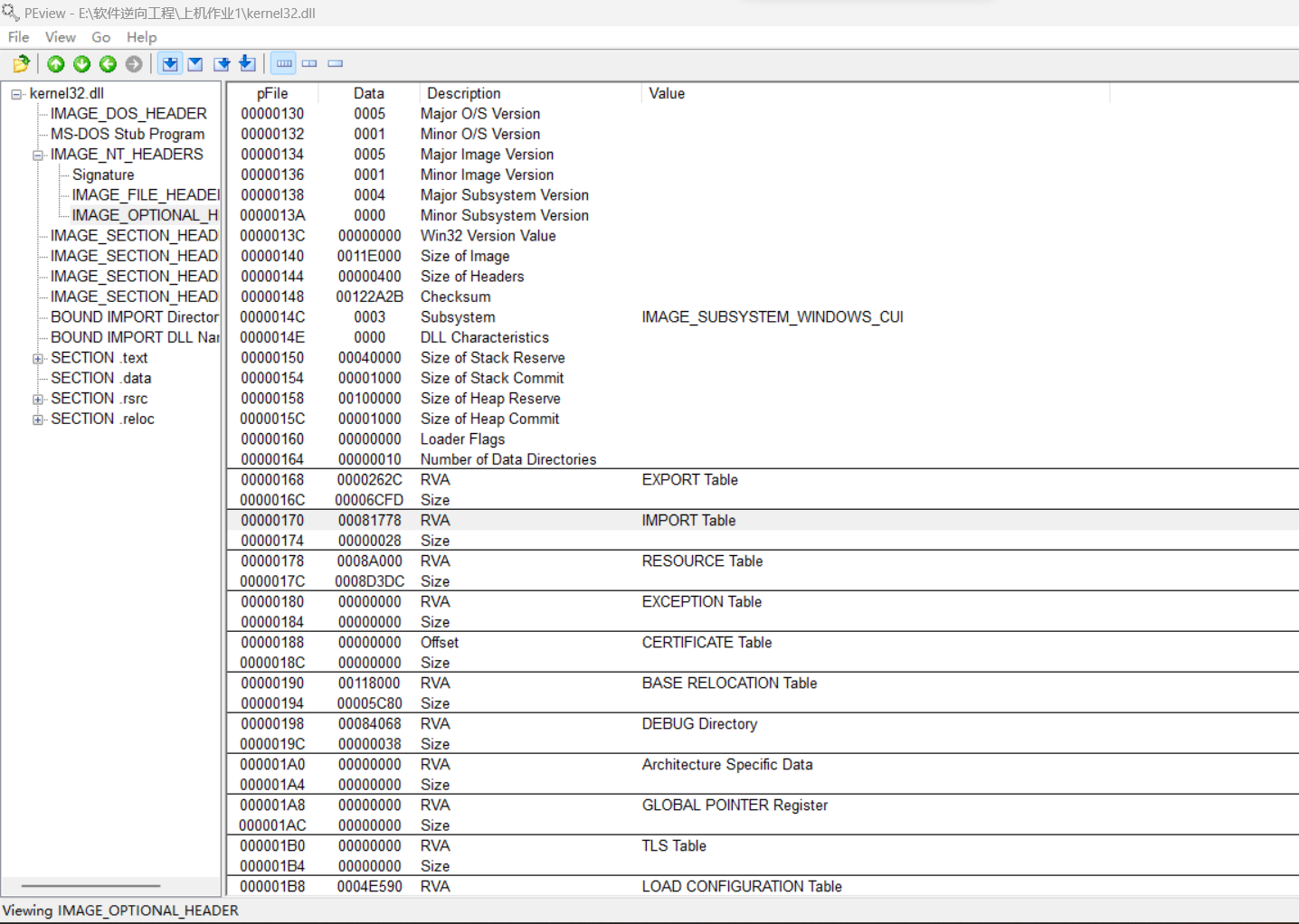
首先准备好PEviews与OllyDbg

使用PEviews打开Kernel32.dll

注意文件格式为.dll



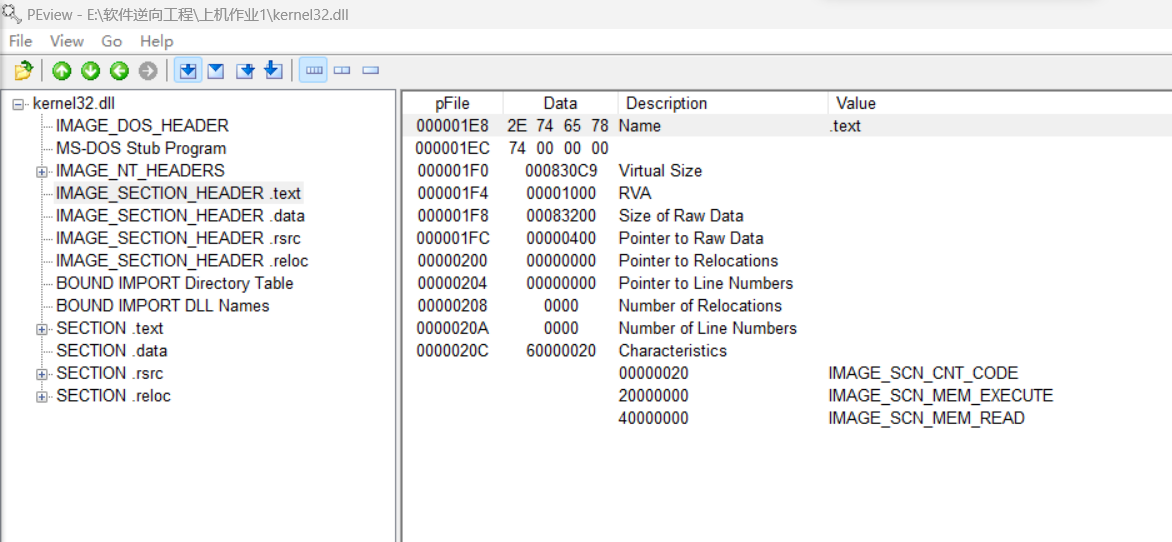
查看 IMPORT Table 的 RVA



查看路径为NT\_HEADERS->OPTIONAL\_HEADERS->IMPORT Table

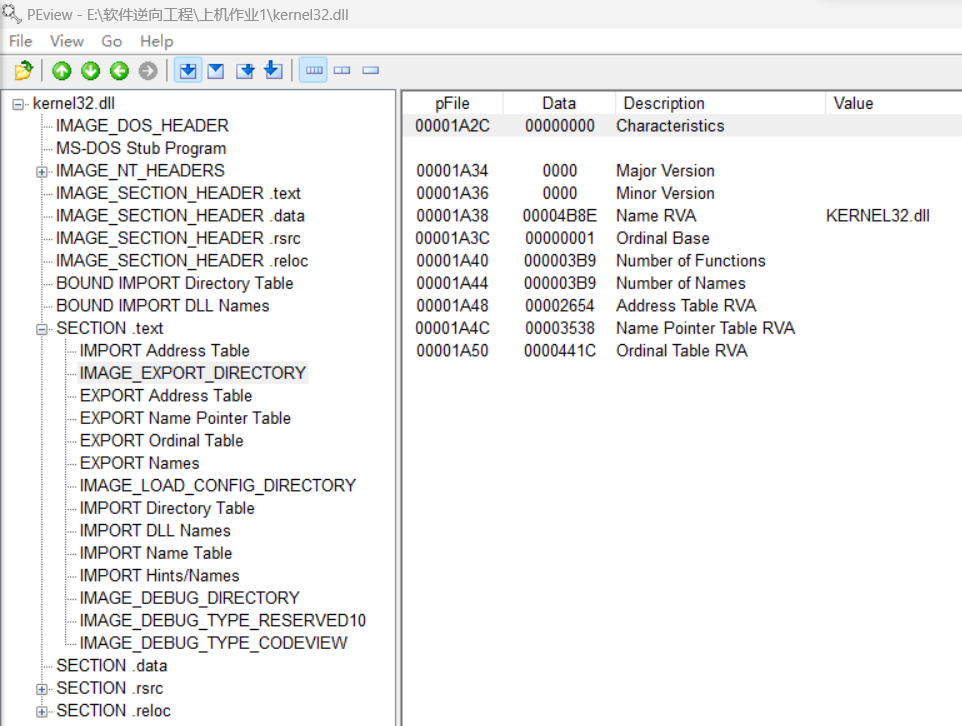
可以看到，IMAGE\_IMPORT\_DESCRIPTOR数组的起始 RVA为：262C

查看RVA(section.txt)与RAW(section.txt)



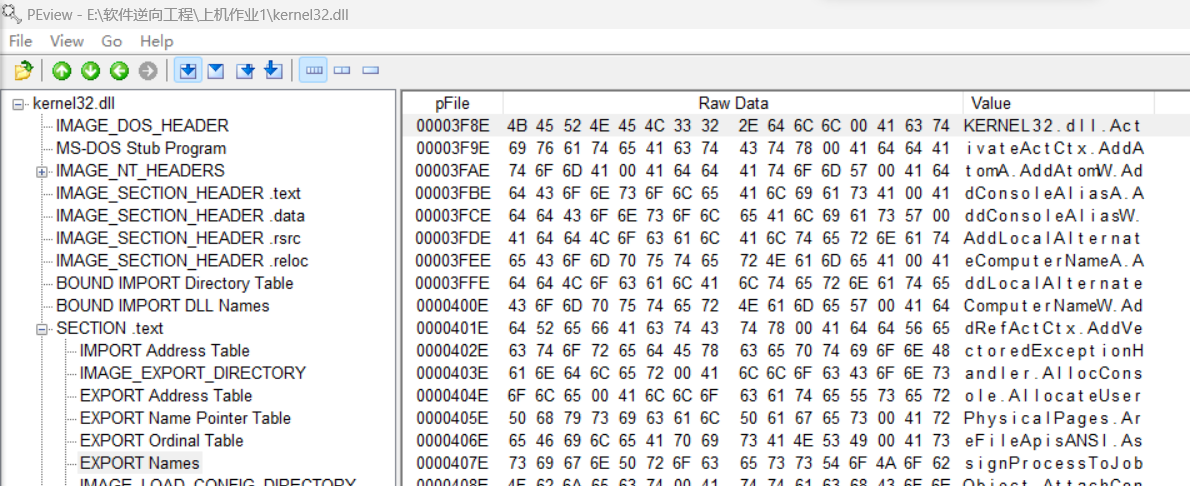
其RVA(section.txt) = 1000，RAW(section.txt) = 400。  
首个IMAGE\_IMPORT\_DESCRIPTOR 结构的 RAW 为：  
RAW = 262C-1000+400=1A2C

观察IMPORT\_Directory\_Table的1A2C位置

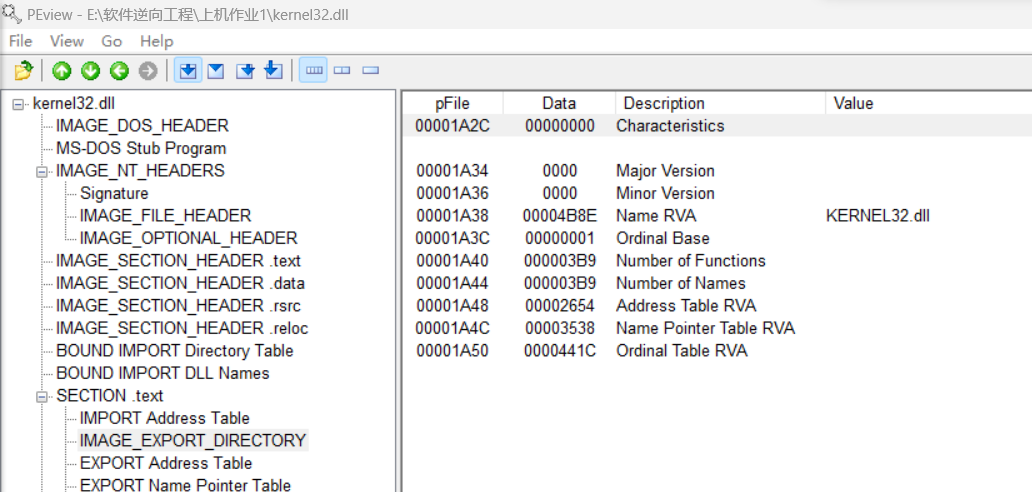


可以知道DLL名称“KERNEL32.dll”所在RAW=4B8E-1000+400=3F8E

观察EXPORT Names的3F8E位置就在第一行的位置

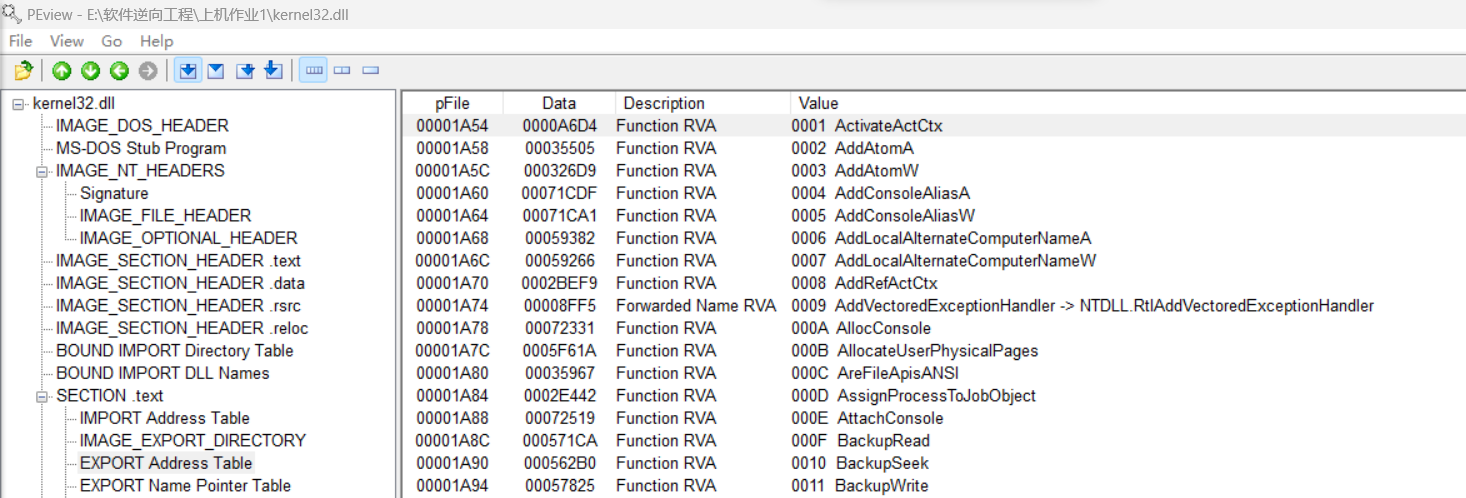


观察Address Table RVA的值为2654

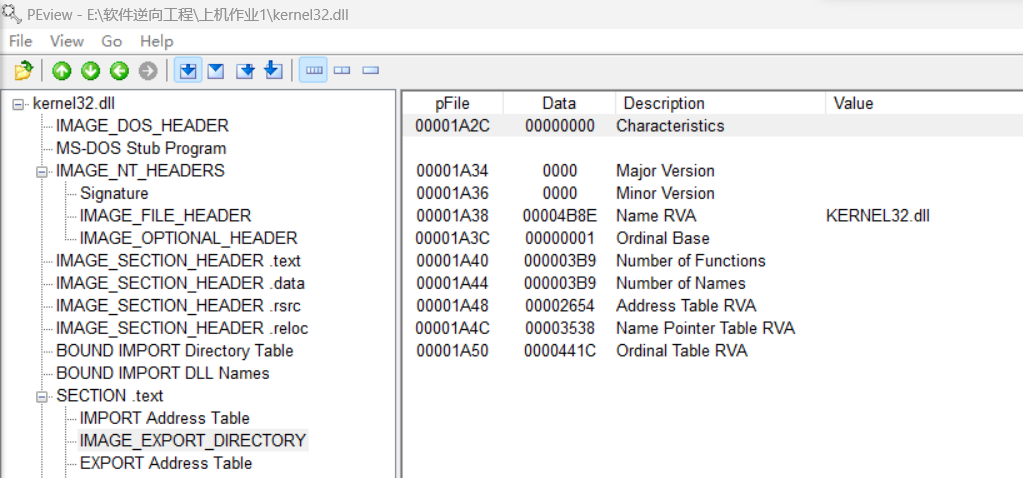


所以可以知道Address Table RVA所在RAW=2654-1000+400=1A54

观察1A54位置在第一行

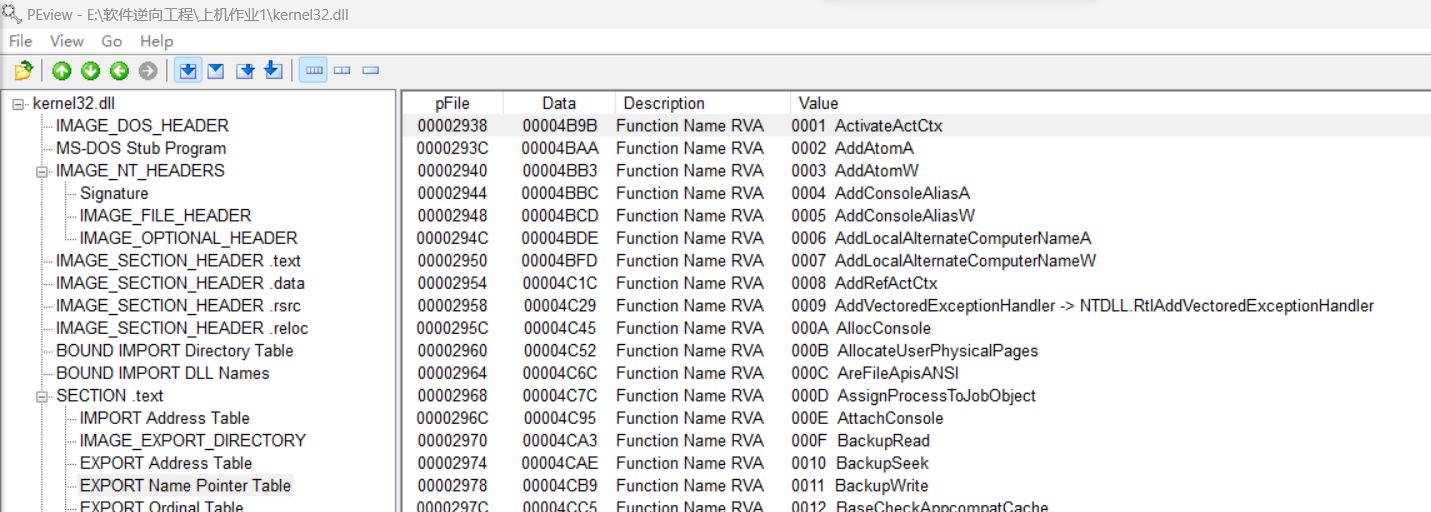


观察Name Pointer Table RVA为3538

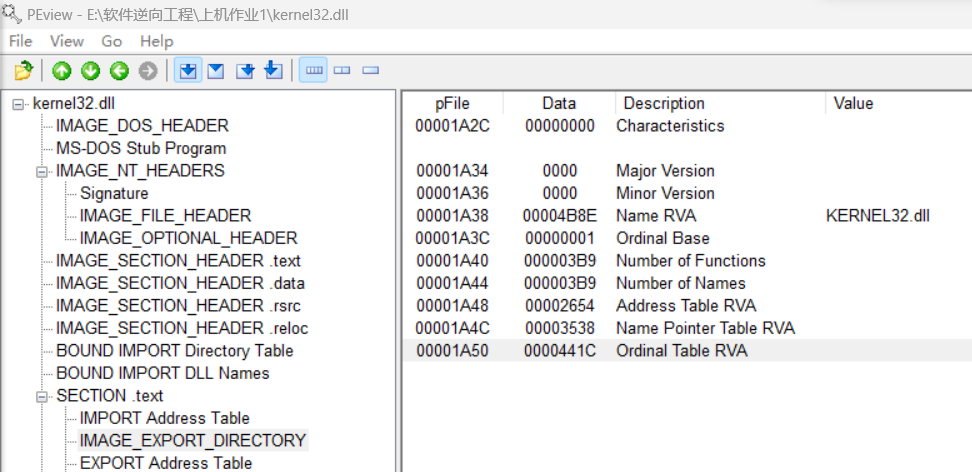


可以知道Name Pointer Table RVA所在RAW=3538-1000+400=2938

观察2938位置在第一行

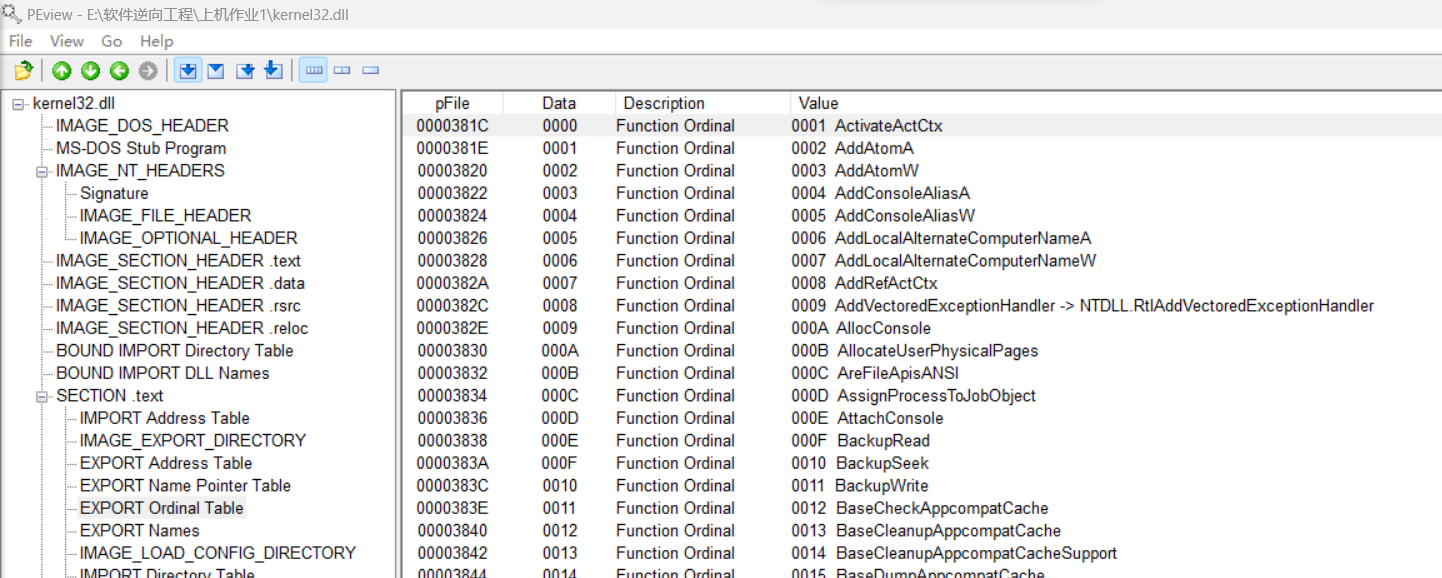


观察Ordinal Table RVA为441C



可以知道Ordinal Table所在RAW=441C-1000+400=381C

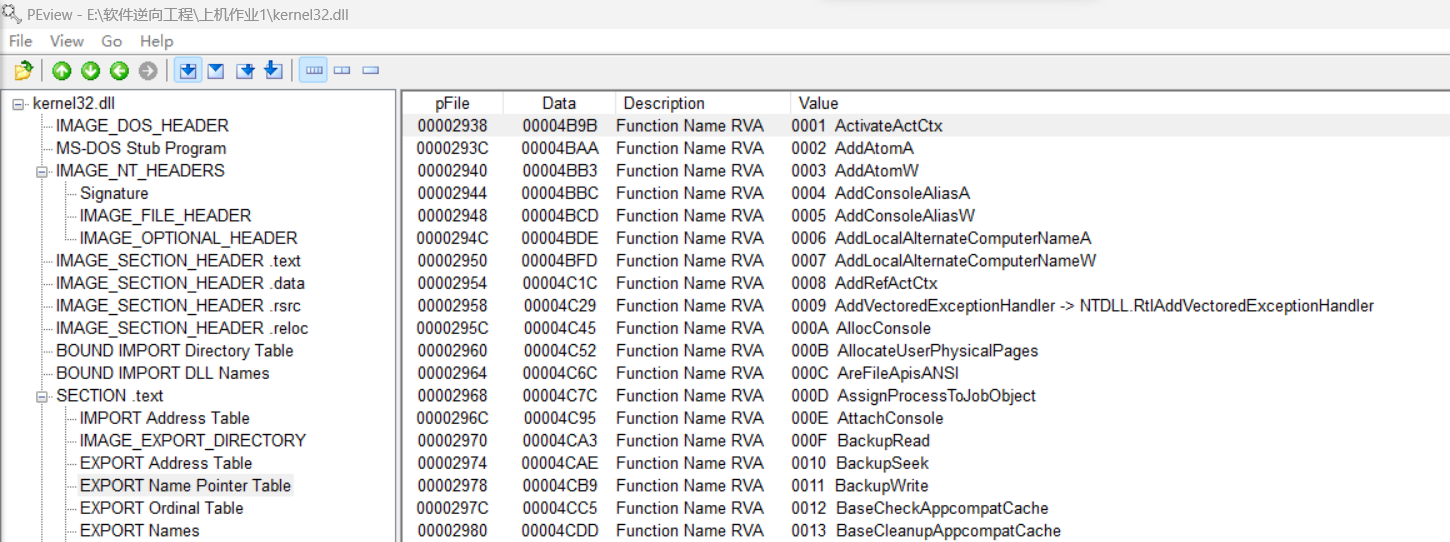
观察381C在第一行



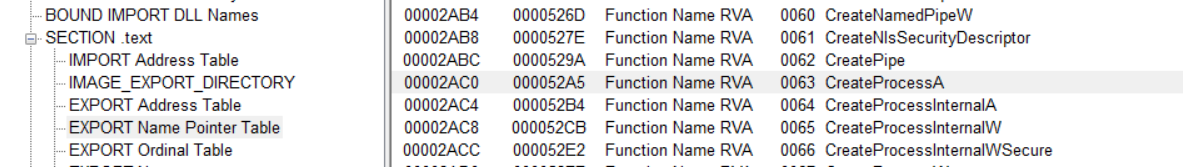
分析CreateProcessA

首先依据查询到的Name Pointer Table RVA，

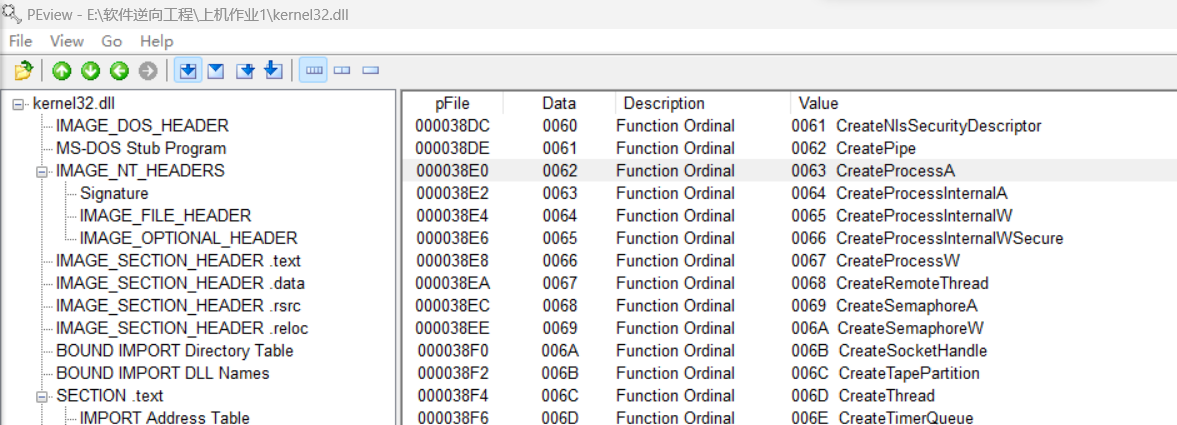
可以知道所在RAW=3538-1000+400=2938



查询到CreateProcessA的地址为2AC0



在RAW偏移量为381C的序数数组找到38E0（381C+0062\*2=38E0）项



可以知道1A54+0062\*4=1BDC

因此RAW偏移量为1A54位置的函数入口地址数组中保存有1BDC

