

根据PE文件结构标准，DOS头在执行过程中需要检查MZ签名和根据e\_lfanew字段定位NT头，因此无论中间的值如何奇怪，可以定位到NT头在地址00 00 00 10处。在upack打包程序中，upack通过修改中间字段使DOS头和NT头混合，e\_lfanew字段同时也作为IMAGE\_OPTIONAL\_HEADER中的magic值（0x10B=32位，所以upack只能用来打包32位程序）使用。

接下来说一下常见的关注点，但在本例中可能不涉及。

NT文件头的SizeOfOptionalHeader（可选头大小）定义了标准头结束和节区表开始的位置。当SizeOfOptionalHeader被修改时，程序能够正常执行（其实是有时候可以，可以参考我写的另外一篇Windows加载文件全流程文档），但对于很多分析器像调试器、文件解析工具、反汇编器等将造成影响。修改目的大部分是为了反调试，但也有一些版本的upack壳中在此处扩展字段来插入解码代码。

可选头的NumberOfRvaAndSizes（数据目录项数），通常值为16（0x10），修改后可能干扰工具解析文件，运行时不受影响，但对于工具来说就是分析数据目录项数的解析标杆，可能出现无意义值或者显示不全。在本例中没有被修改，但是我在未打包程序上测试的可修改后正常运行的最小值为0x06。当修改值小于16时，后面的条目将无法被读取，变成程序用不上的区域。

严格根据e\_lfanew + 4（签名） + 20（COFF头） + SizeofOptionalHeader计算节区头的起始位置，本例中计算得到10H + 4H + 14H + 148H = 170H，跳转至170地址处就是节区头。

