实验四 PE壳设计与验证

实验目的：

1. 验证PE文件结构构建
2. 验证PE文件壳的基本原理

实验内容：

1. 实现简单的跳转壳，在PE文件中添加新节，在新节其中加入跳转至原入口的指令，实现对原程序的启动。

(1).首先了解增加一个节，需要修改哪些内容

(1).FileHeader.NumberOfSections 节表数量（偏移 6 字节）0x0006

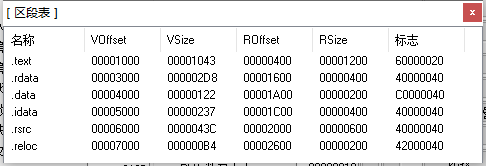
(2).OptionalHeaders.SizeOfHeaders PE头的大小(因为增加了一个新的 IMAGE\_SECION\_HEADER)（偏移 20 字节）0x00E0

(3).OptionalHeaders.SizeOfImage 加载入内存后的PE映像大小（偏移 56 字节）0x000070B4

(4).构造新的 IMAGE\_SECTION\_HEADER

(5).在节表的末尾添加新的内容

(2).添加前（共 6 节）：



(3). 节表的每个结构（28H字节）包含了该节的具体信息，结构如下：



编辑新的节

Name: 2E 74 65 73 74 00 00 00

virtualSize 00 01 00 00（随便，差不多大就可以）

VA: 00 80 00 00（前一节为 00 70 00 00）

SizeOfRawData: 00 02 00 00

PointerToRawData: 00 28 00 00（前一节开始 0x00003600，大小0x00000200）

PointerToRelactions 00 00 00 00 （置0即可）

PointerToLineNumber 00 00 00 00 （置0即可）

numberOfRelocation 00 00 （置0即可）

numberOfLinenumber 00 00 （置0即可）

character: 20 00 00 60 节的属性 可读取，可执行 ，代码。

重要：

原oep: 05 10 00 00

新oep: 00 80 00 00

1. 实现PE文件加密壳，对原程序代码节内容异或运算，在原程序中加入新节实现对原代码节内容解密并启动运行。