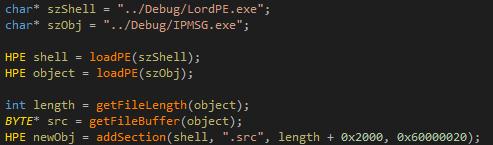
首先选择任意一个程序做为壳，再选择你想给哪个程序加壳

这里假设壳程序名称为shell, 你的程序为object

给shell程序新增一个节，大小为0x2000+lengh, length表示你的程序大小，这样我们得到一个新的加过节的filebuffer, 待会我们要把我们的object程序和我们的解壳代码加到这个节里，0x2000的意思就是我们为解壳代码预留的区域。

代码是下面这个样子：



拿到这个新的filebuffer的最后一个节的节表，根据节表往节里复制数据：

1. 从最后一个节的起始位置复制解壳的硬编码（这个在第二部分讨论，解壳硬编码小于0x2000字节，所以我就只预留了0x2000字节）

2. 修改这个filebuffer的入口点为这个节在内存中的偏移(RVA)。

3 从最后一个节偏移为0x2000的位置复制你的object的filebuffer, 你可以在这部分把你的filebuffer加密，为了方便学习，我没给filebuffer加密

4. 把这个新的加过节的filebuffer保存到本地。整个加壳过程完毕。

代码是下面这个样子：

