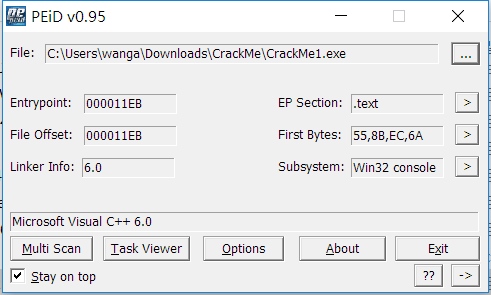
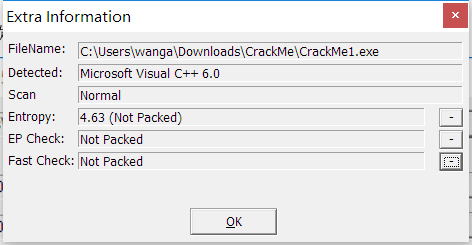
证明自己吧 WriteUp

1、首先使用PEid软件打开可执行文件，进行查壳：





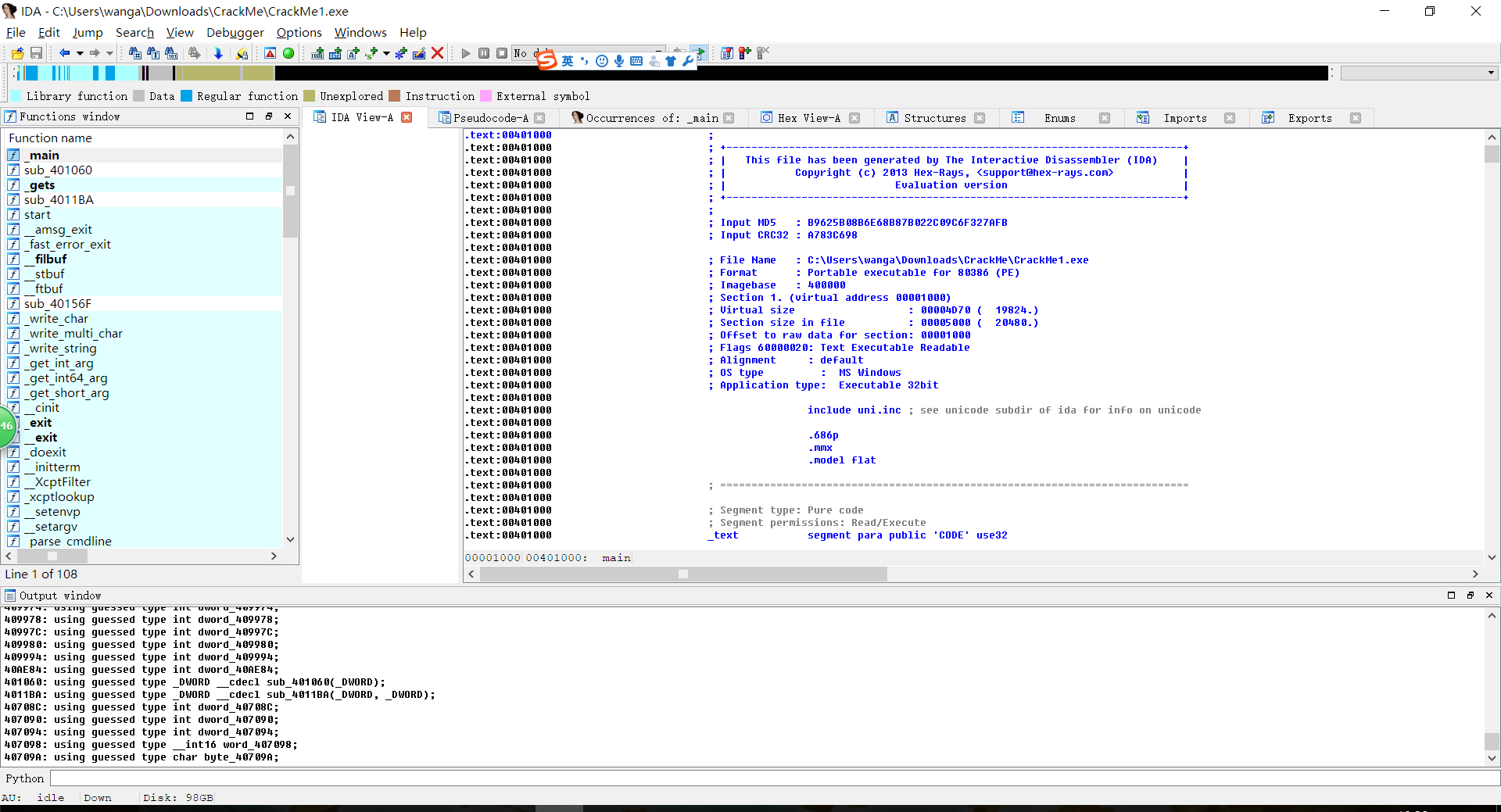
上述not packed说明未加壳，可以直接反编译。

PS：

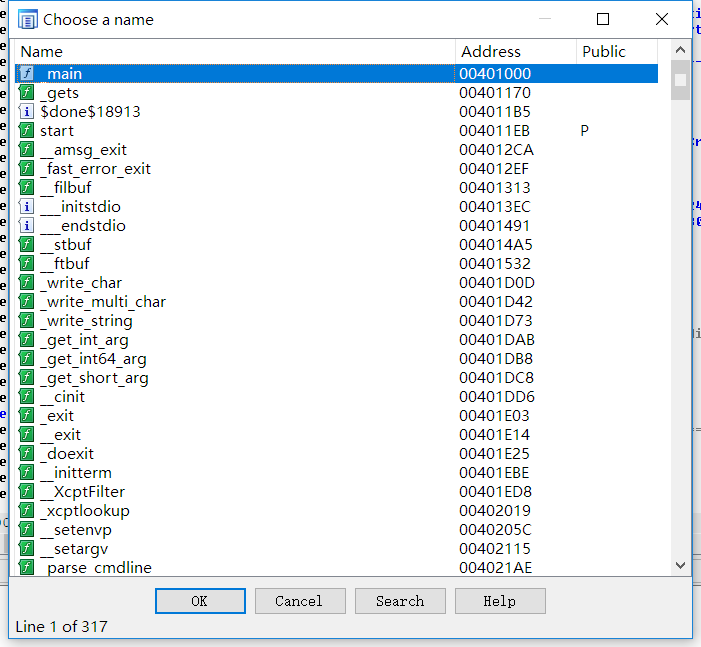
带壳程序应该是指一些加壳的应用程序。一般的病毒就是这样做免杀的。加壳的全称是可执行程序资源压缩，是保护文件的常用手段。加壳过的程序可以直接运行,但是不能查看源代码.要经过脱壳才可以查看源代码。加壳其实是利用特殊的算法，对EXE、DLL文件里的资源进行压缩。类似WINZIP的效果，只不过这个压缩之后的文件，可以独立运行，解压过程完全隐蔽，都在内存中完成。

所以之前有的程序无法反编译可能是由于已经加壳，只有解壳后才能反编译。

2、用IDA反编译：



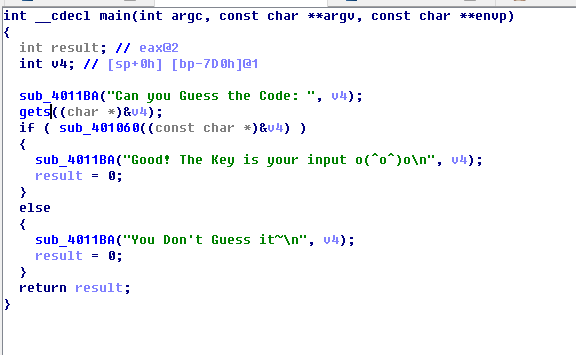
按住CTRL+L查找相关标签：



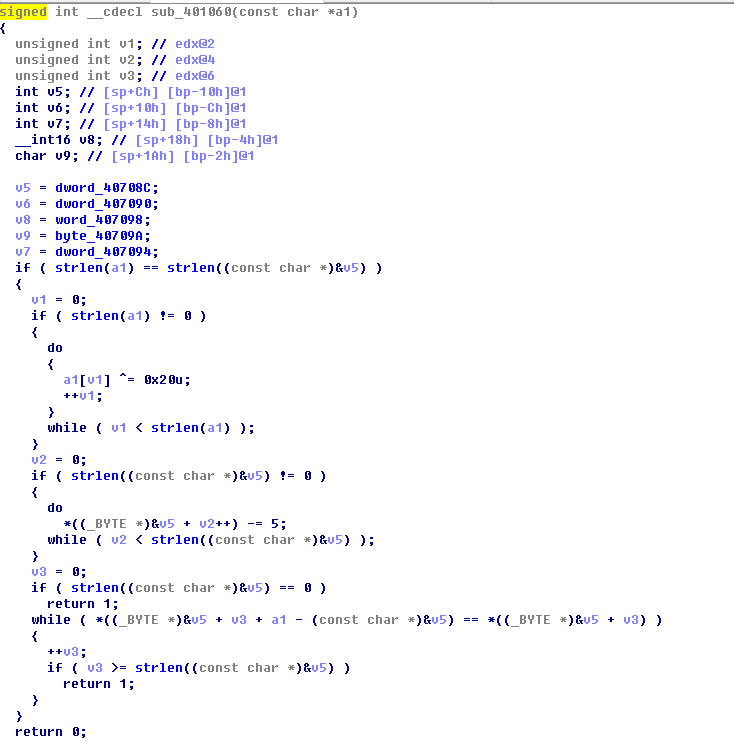
猜测\_main为main函数，点击\_main标签进入相关代码：



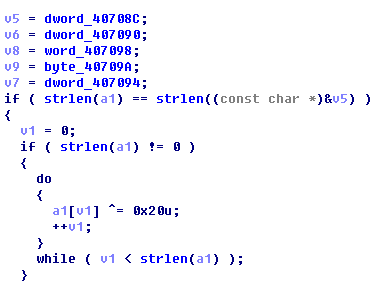
F5生成C代码：



可以看出sub\_401060为判断code是否正确的函数，点击sub\_401060进入相关代码：



第一段代码：

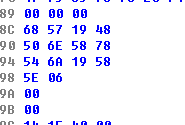


看到我们传进来的字符串叫做a1，假如a1的长度等于v5的长度，则开始逐个元素做异或运算，和20异或。

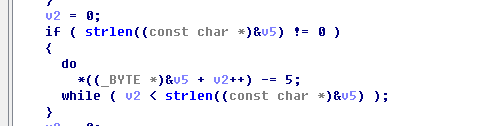
点击dword\_40708C进入定义区，发现后续有一个db伪指令定义的0。



猜测这是一个结尾是’\0’的字符串，并可以看出字符串为：68571948 506e5878 546a1958 5e06H。

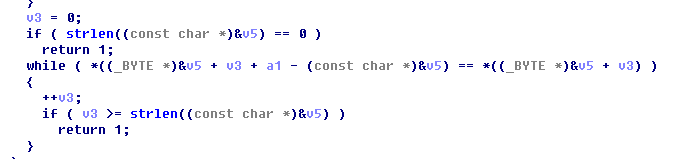


第二段代码：



v5中的每个字节中存储的值-5。

第三段代码：



故意混淆代码，实际作用仍然为：\*（v3+a1）。

此段代码是比较如果当前的v5字符串和a1相同，说明a1为正确值。

3、仔细分析：

a) 输入字符串，对每个字节异或0x20u；

b) 待比较字符串每个字节值减5；

c) 此时如果输入串和待比较字符串相同，则输入串正确。

贴出解密代码：

