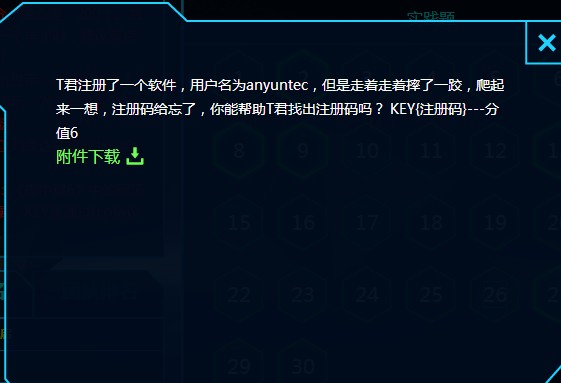
## 题目



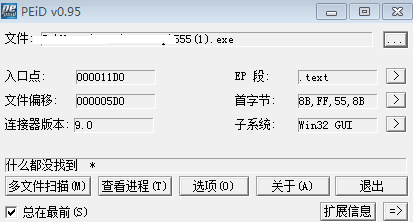
## 知识点

概念：消息机制与消息循环，加壳，导入表，8086CPU寄存器与标志寄存器；

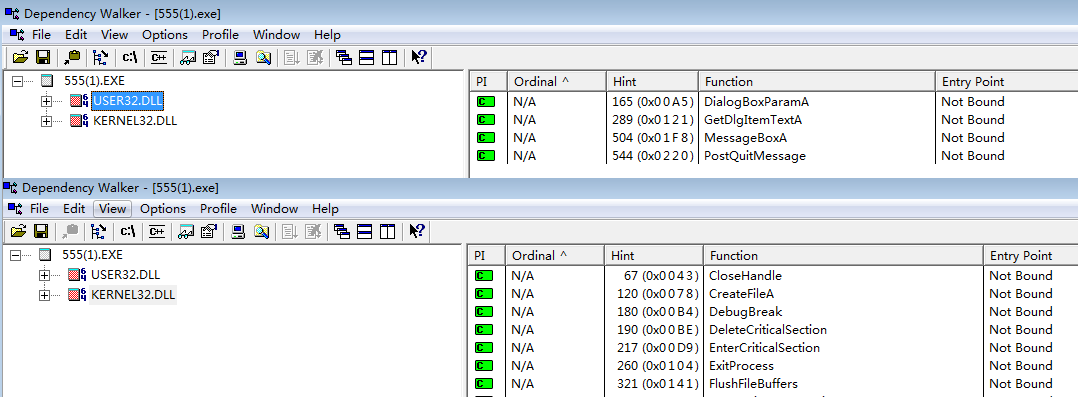
工具：PEiD, Dependency Walker, OllyDbg。

## 分析过程

首先使用PEiD查壳：

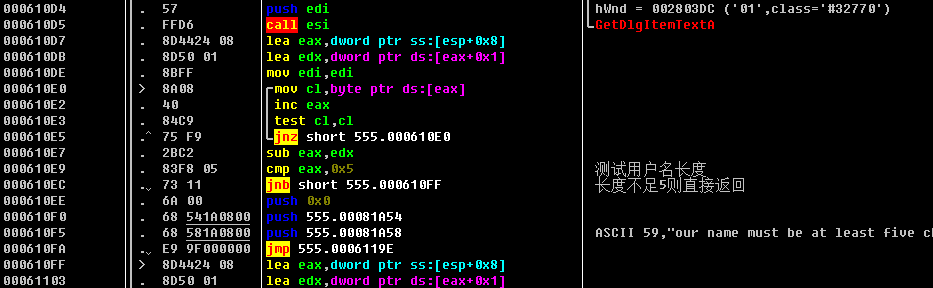


PEiD没有提供任何信息，可能没有加壳，可能加了PEiD无法识别的壳。进一步通过导入函数判断。使用Dependency Walker加载文件：



函数导入表提示了较多导入函数。一般地，加壳文件往往只有（且至少含有）LoadLibrary和GetProcAddress两个函数，这两个函数用于加载和使用其他函数功能，具体函数功能可查阅微软MSDN网站。

打开OllyDbg加载文件调试，在调用GetDlgItemA()处下断点，F2执行，根据题目输入用户名anyuntec，密码任意输入。



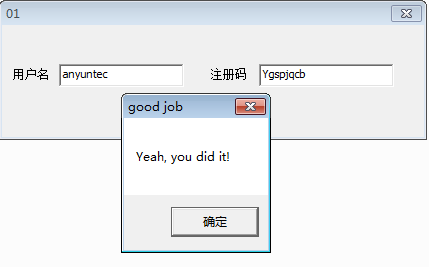
程序在获取用户名之后，首先检测用户名长度，若少于5个字符则直接弹窗报错。由于本题指定了长度为8的用户名anyuntec，故该检测可顺利通过。



接下来程序执行到用户名密码验证阶段。经分析可知，第i位密码的生成算法如下：

取用户名第i位的ASCII码，减去用户名长度，加i-1。

根据上述算法编写程序，得到与anyuntec对应的密码Ygspjqcb。



得到KEY{Ygspjqcb}。

密码计算程序Java代码：

public class MainActivity {

public static void main(String[] args)

{

String name="anyuntec";//指定待计算的用户名

for(int i=0;i<name.length();++i)

System.out.print((char)(name.charAt(i)-name.length()+i));

}

}