实验一

1. virustotal扫描

见 截图 目录，

**VirusTotal1.png ：**显示的社区内的人对它的看法，，认为是安全的4人但是认为不安全的有13人。底下还有一些人对其的评论。

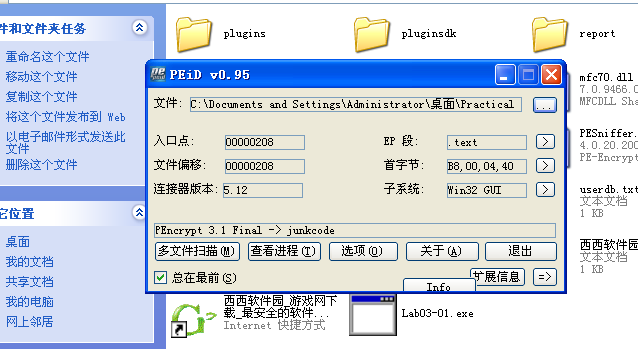
**VirusTotal2.png ：**跟它有关的一些文件，这里指的是压缩文件。

**VirusTotal3.png ：**这里记录了这个文件的分析结果，包括MD5，文件类型等甚至该程序包含的程序，数据段等详细信息。

**VirusTotal4.png ：**65个杀毒引擎中有62个认为这个文件是病毒，并给出了它们的命名。

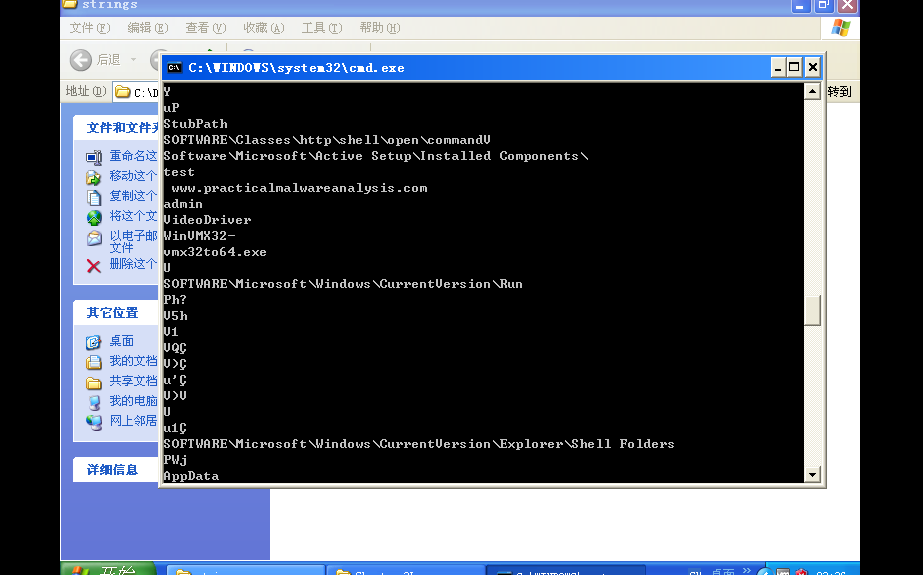
（2）

1.第一步首先使用PEiD分析是否加壳

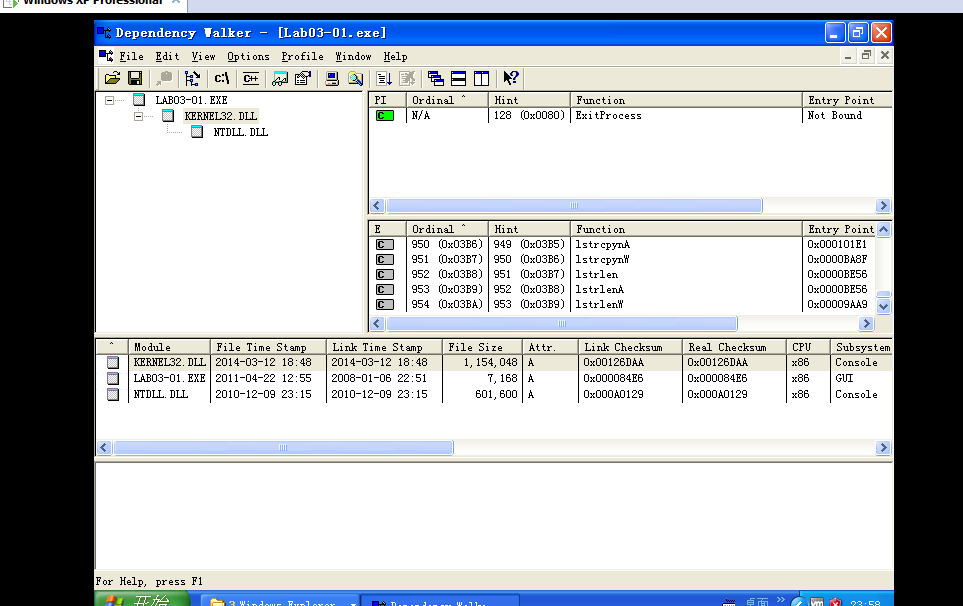


由PEiD分析可知，他是PEncrypt 3.1 Final -> junkcode**加壳的**

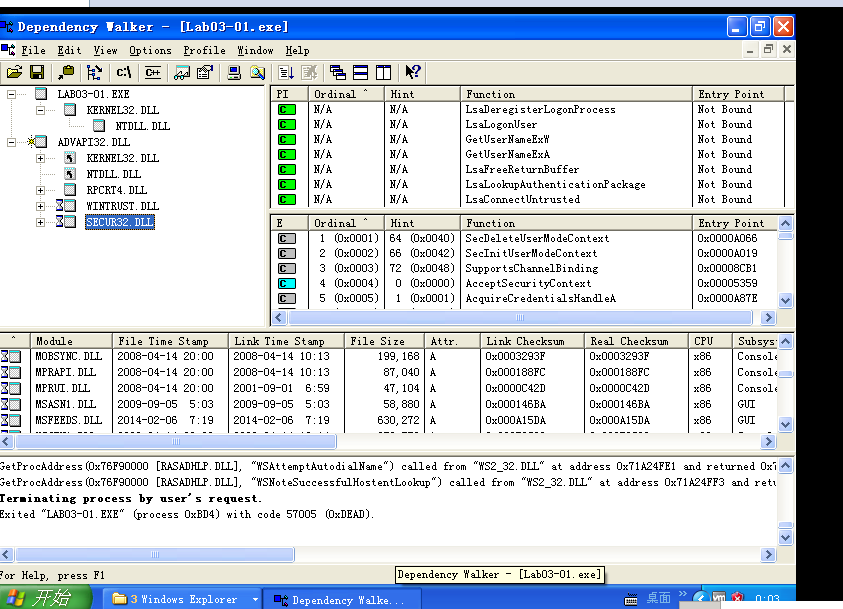
**2.第二步，用strings分析字符串**



**但是由于它加壳过了，因此得到的信息不多，尝试用一些通用的脱壳工具对它进行脱壳，但是都失败了。**

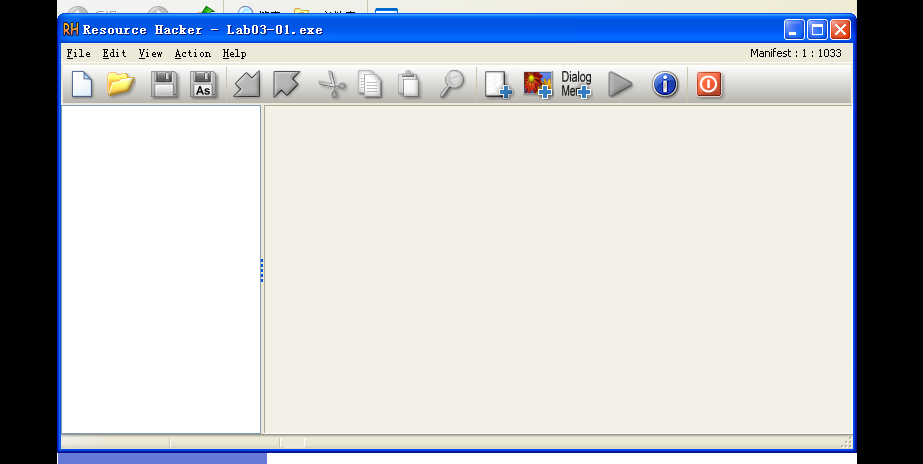
**3.不知道加壳后的程序能否被检测出一些函数，我们先尝试使用Dependency Walker打开它，**

**发现它只有一个叫ExitProgress的导入函数，然后再将其动态运行后发现，它其实调用了好多函数，**

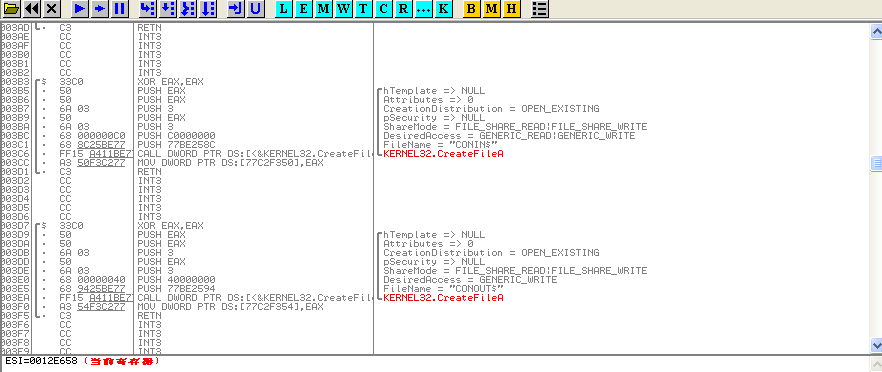


**尝试分析它调用的一些API，但是实在是太多太复杂，看到一些操作进程和窗口的api，应该是用来获取别的程序，还有一些图片加密的API**

**4.加壳过后的程序似乎也看不到资源节**



**5，用OllyDbg进行调试，发现其中有许多文件操作和硬盘读取**



**还在其中找到了创建文件和setbuf的函数，怀疑是进行无限复制的。**

**6. 一些工具介绍**

**PE Explorer**

PE Explorer是一个强大的程序资源编辑工具，可以直接查看、修改软件的资源，包括菜单、对话框、字符串表等；另外，还具备有 W32DASM 软件的反编译能力和 PEditor 软件的PE文件头编辑功能；该软件支持插件，你可以通过增加插件加强该软件的功能，原公司在该工具中捆绑了一个UPX插件，可以解开用UPX 0.8－UPX 3.01版本加壳的软件。

**Unpacksdk**

UnpackSDK是PCHunter作者很久前开发的!通过自写一些脱壳函数,来脱一些变异壳,，挺方便的!

**qunpack21**

一款强劲的脱壳工具