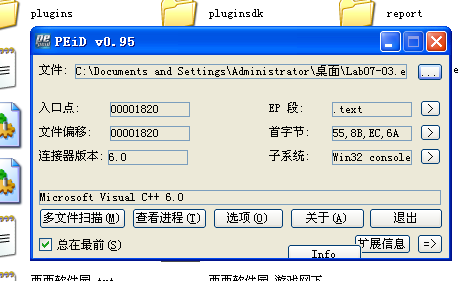
### 作业二

1. 发现一些复制文件的API，可能会无限复制自身

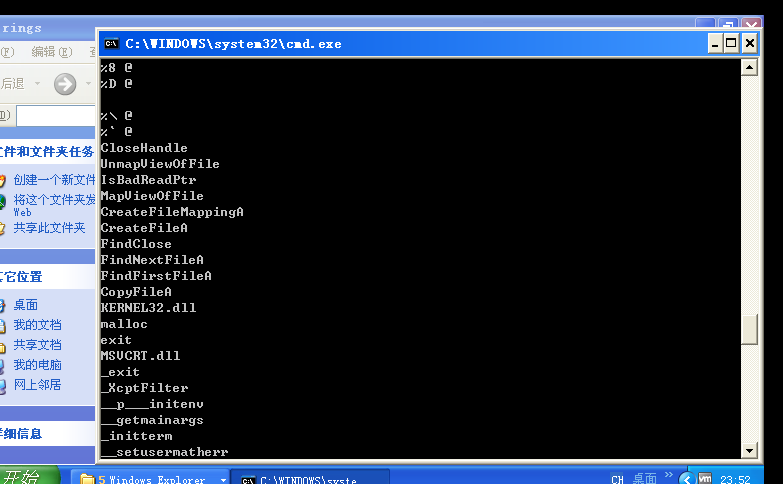
另外发现一些网络操作，可能会接受远程的控制或者下载远程服务器上的木马。

二、

1.使用PEiD扫描是否加壳，由图中可见，并没有加壳



1. 使用strings.exe进行扫描

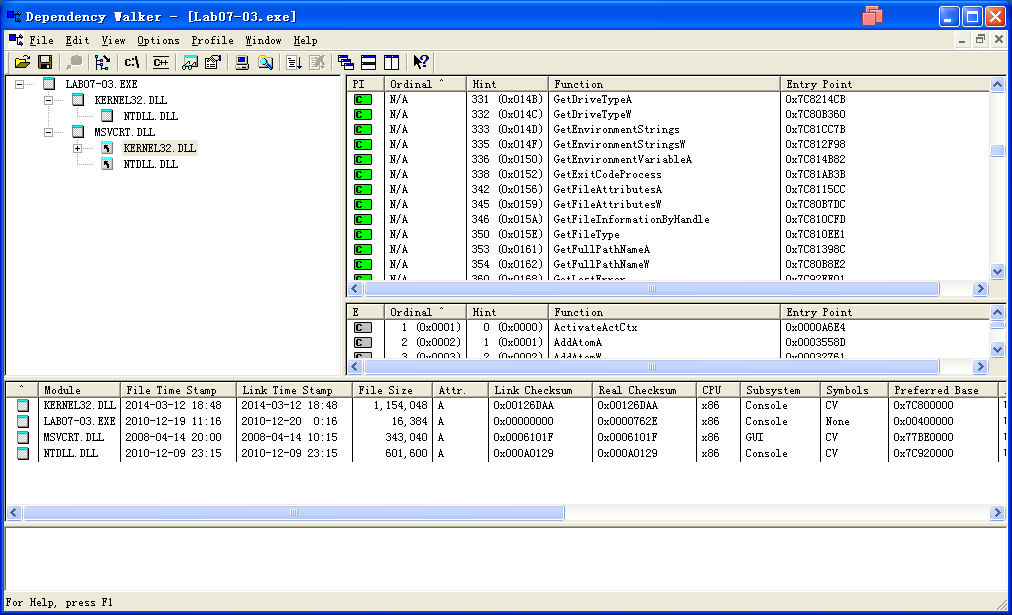


这是Lab07-03.exe扫描出来的结果，发现一些文件操作，认为它可能会不断复制自己



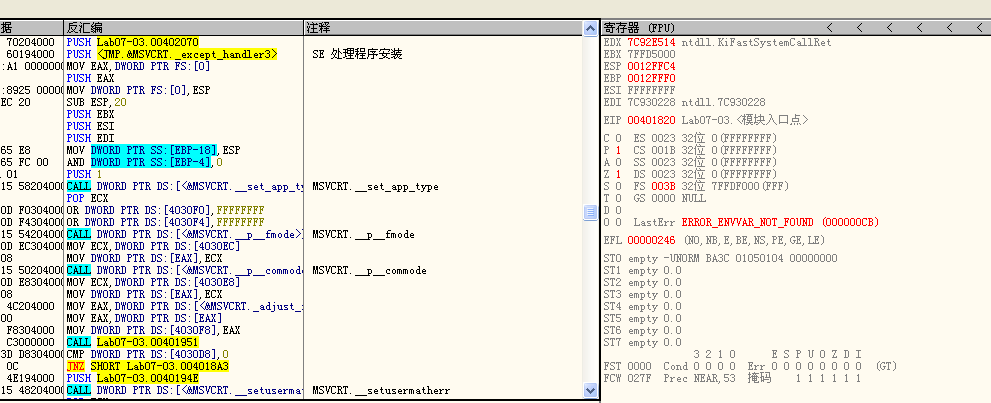
于是接着扫描Lab07-03.dll,在里面发现了创建进程和访问网络的API，同时找到了一个类似于ip地址的数字。可能是从指定的ip下载木马运行它，也可能是接受指定ip的命令，执行破坏程序。

1. 使用Dependency Walker扫描，似乎也只能发现那些文件操作的函数，并没有找到网络和注册表的操作函数。



bpx (MessageBoxA)

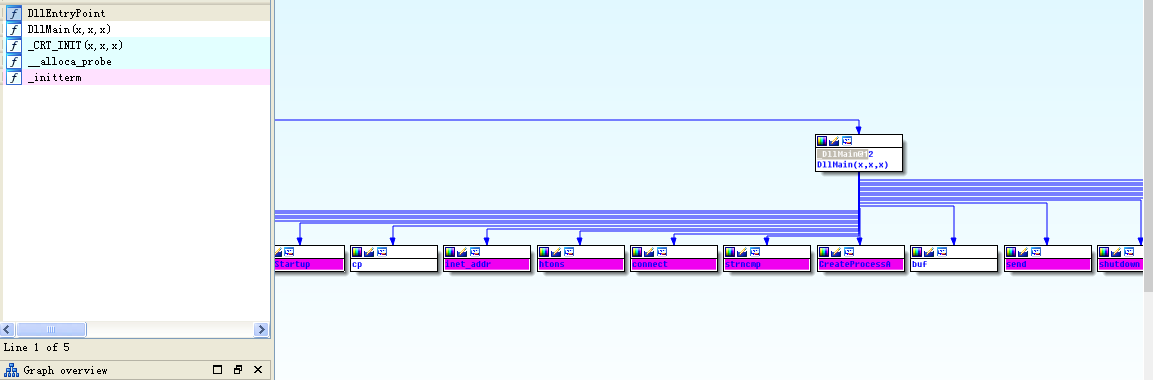
1. 用OllyDbg调试



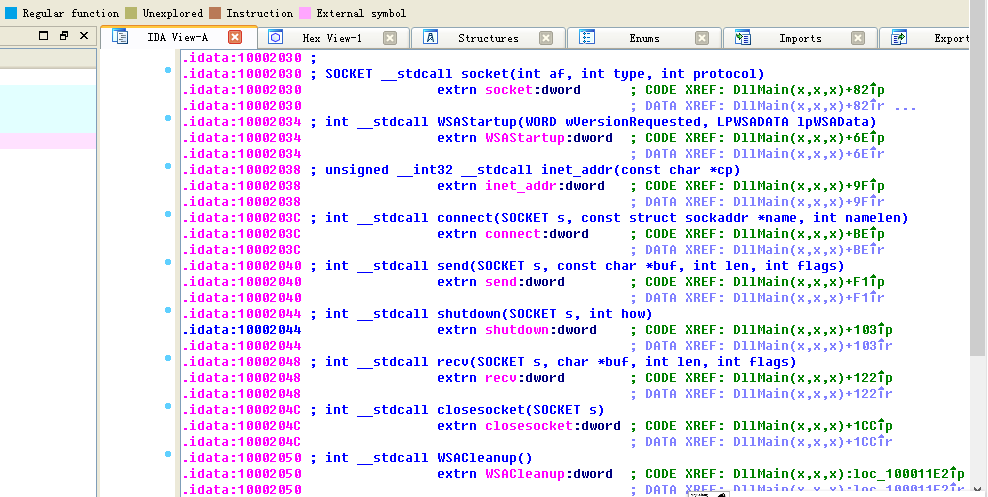
它竟然因为环境变量没有找到退出了

5 Ada

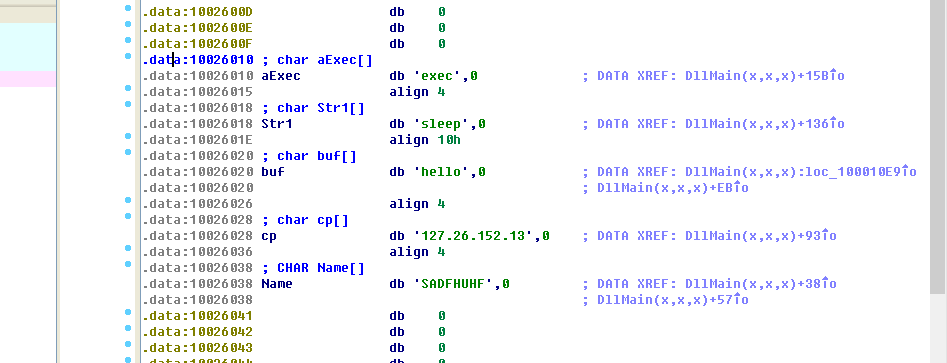
在庞大的函数中，似乎只见到了网络相关的函数



仔细查找了一下，并且双击，直接定位到代码的位置。



发现了socket操作函数



以及ip地址

三、总结

1. 调试有的时候需要看运气，有的时候病毒没加壳那就省不少功夫，有的时候随意使用了一个小工具可能会有大发现。而且我这里这个病毒出异常退出了，而我因为能力不济也不知道该如何配置环境让它成功运行起来，实在是耽误事。

2. 经验十分重要，虽然书上推荐了许许多多的工具，但是初学者真的会错过很多有用的工具，也因此错过了很多软件的细节。十分可惜。

3.这是个及其需要耐心的细致活，那么多汇编代码，容易懵逼，需要调试人员付出极大的时间和精力才能调试好的。

4.社区十分重要，我在吾爱破解论坛上学到了许多调试的技巧。