实验七　软件的动态分析和破解

1.实验目的

通过对简单软件的动态分析和破解，了解静态、动态分析软件的基本功能和使用方法；了解动态分析软件破解程序基本方法；　加强对软件保护知识的认识。

2. 实验原理

本实验提供了一种破解程序的简单方法。针对不同的软件保护方法，会有很多更复杂的分析方法，而这些都必须在熟悉OllyDbg使用的情况下才能实现。在实验过程中还要重点熟悉OllyDbg功能和使用。建议该实验课时为2个学时。

3.实验环境

安装 Windows 7 的操作系统。

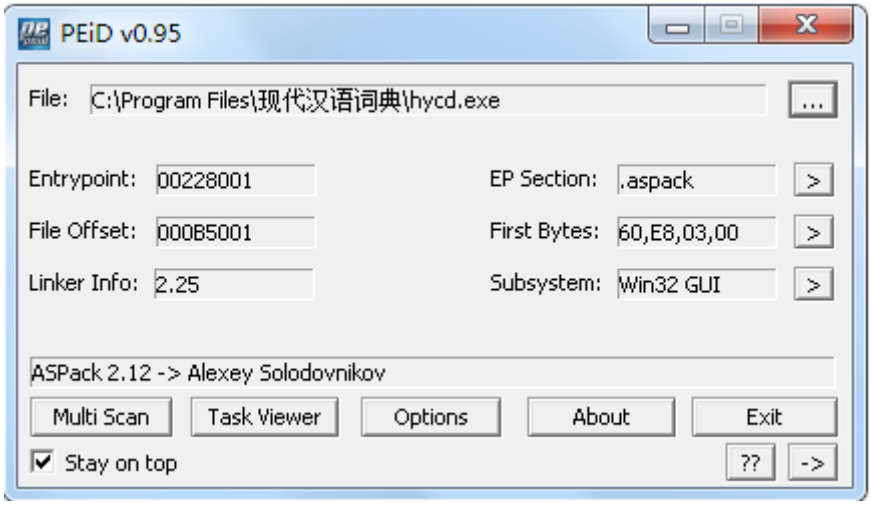
4.实验内容和步骤

任务一 现代汉语词典软件的破解

步骤1：从服务器上下载并安装现代汉语词典软件；下载破解软件常用的软件工具，包括PEiD、AspackDie、OllyDBG等。现代汉语词典注册页面如图A.47所示。

图A.47现代汉语词典注册信息

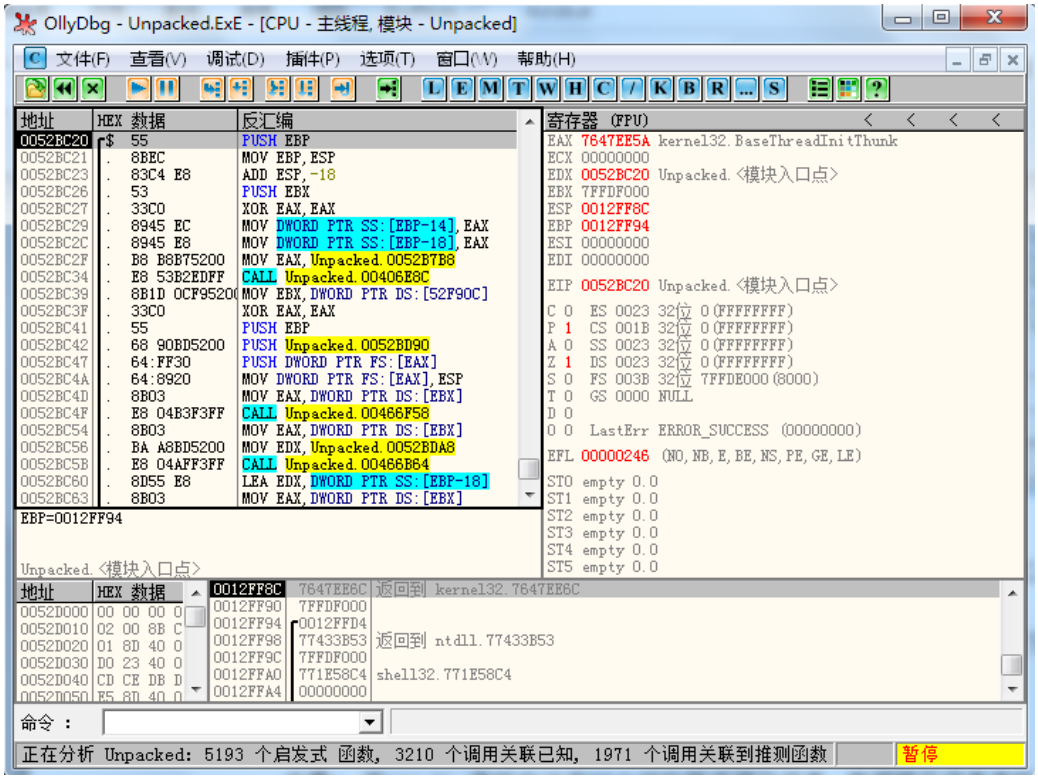
步骤2：用工具软件PEid查找该软件的壳以及编程语言、入口等信息。然后进行脱壳处理。



图A. 48查看软件的相关信息

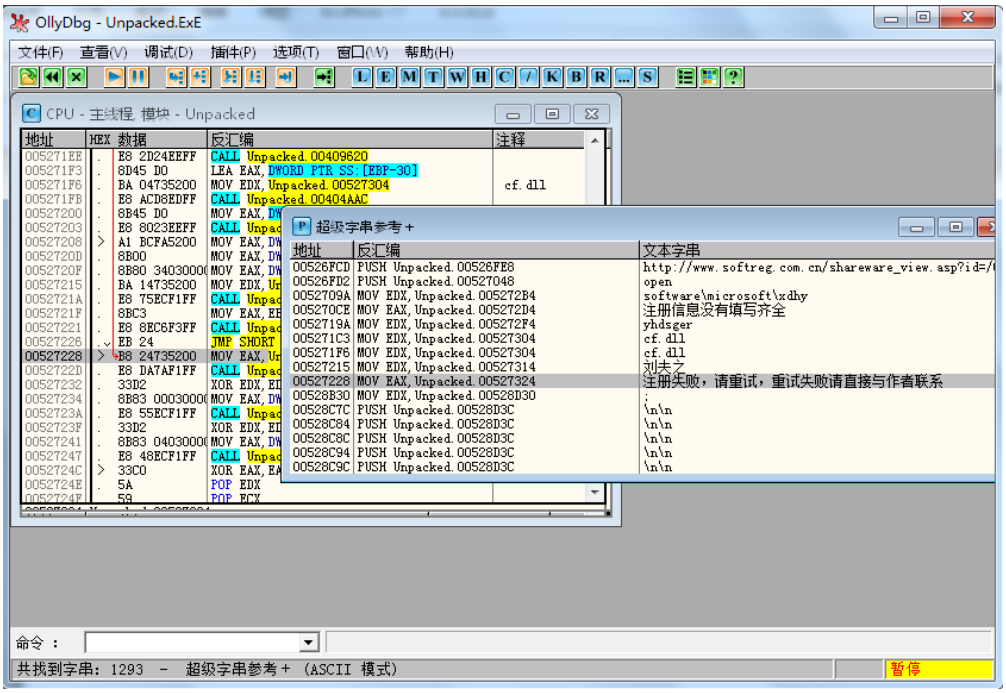
从中可以看出该软件用ASPack2. 12进行了加壳，所以要找到对应的脱壳工具进行脱壳处理。这里可以采用ASPackDie对该软件进行脱壳。

步骤3： 执行OllyDbg.exe文件，在OllyDbg窗口上选择“文件（File）”|“打开（Open）”，装载上步已经脱壳完成的主程序进行调试。



图A.49 用Ollydbg载入已经脱壳后的主程序

步骤4：在OllyDbg中的超级字串参考信息里面，查找在注册时出现的错误提示信息，根据提示信息查找关键Call和关键跳转指令的位置。



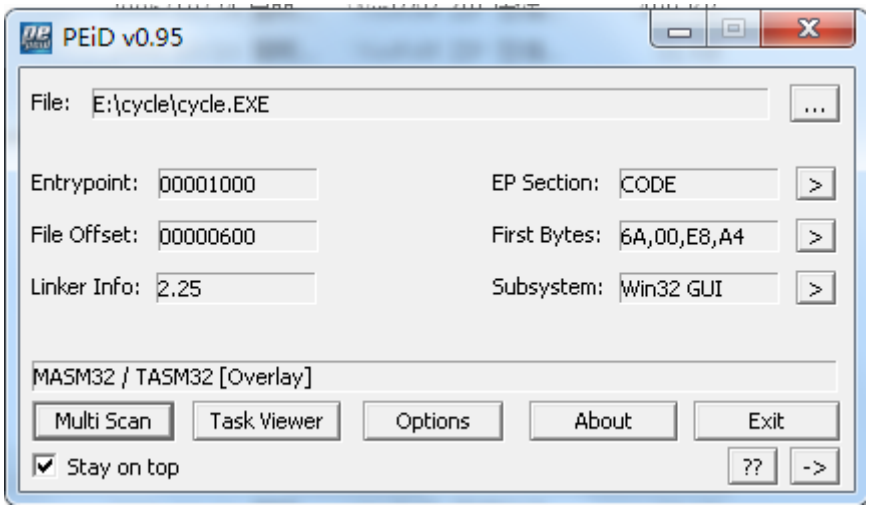
图A.50 查找关键Call位置

步骤5：单步执行查找内存中保存的注册码等信息。或对程序的指令代码进行修改；或用Keymaker制作注册机。

任务二 普通注册软件的破解

步骤1：从服务器上下载破解专用小软件Cycle，

步骤2：利用工具软件安查找软件的相关信息，具体如图所示。



图A.51 Cycle软件信息

步骤3：用OllyDbg导入需要调试的Cycle进行单步跟踪调试，找到对应的注册码信息，对软件进行跟踪和破解。

实验说明：

本实验重点在于了解对软件的静态分析和动态分析方法，通过静态分析能够了解软件的壳以及编译系统的概貌，能够为软件的动态分析提供参考。软件的动态分析要求学生能够掌握对简单软件调试、跟踪的一般方法，从而提高对自己设计软件的保护能力和水平。

5.实验报告要求

要求对任务一按照步骤要求对现代汉语词典分别采用查找注册码和修改二进制代码两种方式对软件进行破解，并对每个步骤进行解释和截图；对任务二，要求通过查找资料的方式，找到对该小软件进行破解的注册码或进行破解，每步要有对应的截图，并要有详细的说明。