电脑报 总策划

黑客通缉令

谁动了我的电脑

华师傅资讯 ◆ 编著

查一知百
从蛛丝马迹查看谁动过我的电脑

知己知彼
了解黑客要对你干什么

层层设障
打造系统铜墙铁壁

坚壁清野
让破门而入者一无所获

软硬兼施
从硬件入手锁定你的电脑

有备无患
从系统灾难中神奇地恢复数据

精彩光盘
卡巴斯基反病毒软件
金山木马专杀工具
各类数据备份修复工具荟萃

山东电子音像出版社出版

黑客通缉令

谁动了我的电脑

编著 华师傅资讯

山东电子音像出版社出版

目录 CONTENTS

第1章

蛛丝马迹——
三招两式看谁动过我的电脑

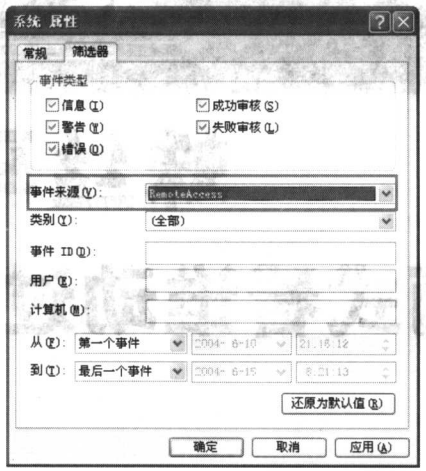
1.1 看看在我的系统上干了什么

仿照我们大脑的记忆功能，微软也为它的视窗操作系统设计了记忆功能，从启动登录记录，到程序运行记录应有尽有。要查看系统的变动情况，我们总有足够的蛛丝马迹可循，如同案发现场总会留下痕迹，只要你细细搜寻就一定会发现。

1.1.1 用 Windows 事件查看器看使用记录

1．查看上网时间

在 Windows XP 中，通过“事件查看器”可以查看我们过去的上网时间。方法为：打开“控制面板”，双击“管理工具”，然后打开“事件查看器”。在左侧的窗口中选择“系统”选项，单击鼠标右键，在弹出的快捷菜单中选择“属性”，在“系统属性”窗口中选择“筛选器”选项卡，在“事件来源”中选择“RemoteAccess”，如下图：



查看上网时间

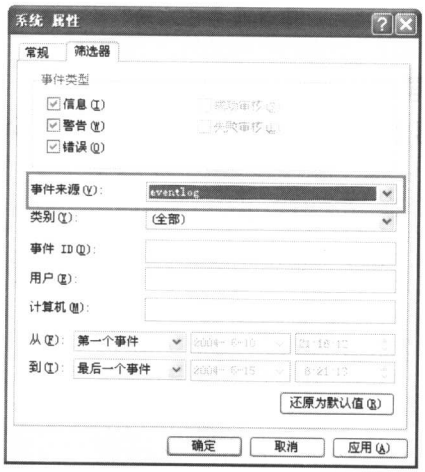
单击“确定”，回到“事件查看器”主窗口，在右边的窗口中就会显示出上网的开始时间和结束时间，相邻的两个时间中较早的就是你开始上网的时间，较晚的则是下线的时间。

2．查看计算机开关机记录

在Windows XP中，我们可以通过“事件查看器”的事件日志服务查看计算机的开、关机时间。因为事件日志服务会随计算机一起启动和关闭，并在事件日志中留下记录。

在这里有必要介绍两个ID号：6006和6005。在事件查看器里ID号为6006的事件表示事件日志服务已停止，如果你没有在当天的事件查看器中发现这个ID号为6006的事件，那么就表示计算机没有正常关机，可能是因为系统原因或者直接按下了计算机电源键，没有执行正常的关机操作造成的。当你启动系统的时候，事件查看器的事件日志服务就会启动，这就是ID号为6005的事件。

通过这两个ID号保存的信息，我们可以轻松查看计算机开、关机记录。方法为：打开“控制面板”，双击“管理工具”，然后打开“事件查看器”，在左边的窗口中选择“系统”选项。单击鼠标右键，在弹出的快捷菜单中选择“属性”，在打开的“系统属性”窗口中选择“筛选器”选项卡，在“事件来源”列表中选择“eventlog”选项，如下图：



查看计算机开关机记录

继续设定其他条件后，单击“确定”，即可看到需要的事件记录了。双击某条记录，如果描述信息为“事件服务已启动”，那就代表计算机开机或重新启动的时间，如果描述信息是“事件服务已停止”，即代表计算机的关机时间，如下图：