计算机安全与维护

第二章 Windows系统进阶使用

温故（1/2）

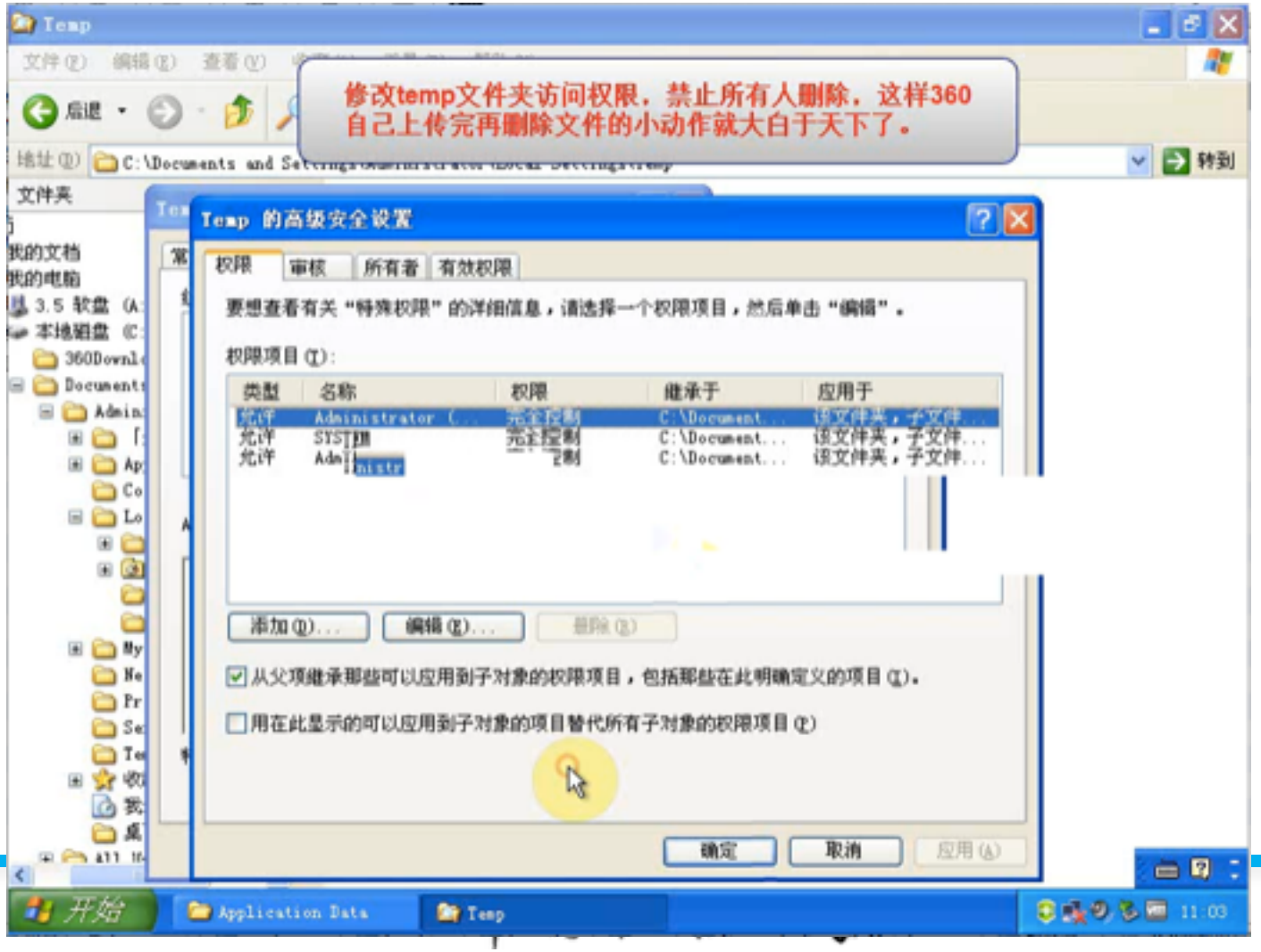
- 简单描述Windows系统的访问控制如何实现
  - —限制某个文件只能被特定用户打开
  - —限制某个文件夹只能被指定的几个特定用户打开
  - —Windows的权限机制只可以作用于文件和文件夹吗？
- 简单描述可执行程序和进程、线程之间的关系
- 简单描述内核态和用户态的区别？

温故（2/2）

- 使用虚拟机软件对我们的实验有何意义和作用
  —概念：主机系统、宾客系统、客机增强件
- 使用VirtualBox进行信息安全类实验如何保证实验安全?

历史热点案例点评

- 如何客观公正看待这个“隐私窃取”事件?



知新

- NTFS文件系统的一些有意思的特性
- 纯净Windows系统上常见的
  - —系统文件
  - —注册表项
  - —进程项
  - —网络端口
  - —服务
- 深入理解Windows系统原理的常用辅助工具

本章内容提要

- NTFS文件系统
- 常见系统文件
- 常见注册表项
- 常见进程项
- 常见网络端口
- 常见服务
- Sysinternals工具集功能介绍

- 上一章对windows的各种文件系统做了一个简单的介绍，这一部分重点对其中的NTFS文件格式进行详细介绍。
- NTFS是Windows NT及其以后系统例如Windows XP和Windows 7的标准文件系统。
- NTFS有五个正式发布的版本，最新的V3.1版本来自于Windows XP，并且被应用于之后的Windows Vista和Windows 7。

NTFS文件格式的特性

- 可恢复性

—为了解决“可靠的数据存储和数据访问”需求，NTFS在“原子性事务”概念的基础上提供了文件系统恢复功能。

—“原子性事务”的基本原则是一个事务的独立磁盘操作必须按原子方式来执行，如果系统失败中断了该事务，已完成的部分必须被撤销或者回滚。好像该事务从未发生过。

—对于关键的文件系统信息，NTFS使用额外的存储区，如果磁盘上的一个扇区坏了，NTFS仍然可以访问该卷的关键文件系统数据。

- 安全性

—NTFS的安全性来源于Windows的对象模型。文件和目录都是被保护的对象，可以避免遭受未授权用户的访问。

—文件对象的安全描述符被作为该文件的一部分存储在磁盘上，在打开文件对象之前，安全系统检验进程的权限，通过安全描述符和用户口令结合确保访问的安全性。

- 数据冗余和容错能力

—为了保证数据不会因为电源断电或者灾难性的磁盘错误而遭受损害。为用户文件的完全恢复提供保证，其保护是通过数据冗余机制来提供的。

—文件的数据冗余机制是通过Windows的分层驱动程序模型来实现的。该模型支持容错磁盘，当把数据写到磁盘上时，NTFS与卷管理器通信，将数据复制到另一个磁盘上，作为冗余的拷贝，称为RAID 1。如果磁盘上的数据丢失或不可访问了，驱动程序可以通过异或操作来重构磁盘的内容。

NTFS的高级特性

- 多数据流
  - —在NTFS中，与每个文件相关联的信息，都被实现为一个文件属性。每个属性是由一个流构成。这样就很容易为一个文件加入更多的属性。而NTFS文件或者文件目录可以包含多个数据流。
  - —数据流的名称通过在文件后再加上一个冒号“：”来指定。比如：myfile.dat：stream2
- 基于UNICODE的名称
  - —NTFS完全支持UNICODE，使用UNICODE字符来存储文件，目录和卷的名称。

NTFS的高级特性

- 通用的索引设施
  - —NTFS的总体结构是高度结构化的，从而允许对磁盘卷上的文件属性进行索引。这一特性使得文件系统可以高效的定位到符合某种准则的文件。
  - —NTFS的特性用到了通用的索引机制。
- 动态的坏簇重新映射
  - —对于磁盘中的坏簇，Windows的容错驱动程序将会动态的获得此扇区的好的拷贝，之后发送警告，该扇区已坏。
  - —NTFS分配一个新的簇替换坏掉的簇，拷贝数据到新簇，对坏的簇做标记，不再使用。

- 硬链接和交接

—硬链接使得多个路径指向同一个文件（不支持目录）

—除了硬链接，NTFS还支持交接的重定向机制。交接也称为符号链接（symbol link），交接机制只能链接到本地卷的目录中，不能链接远程目录。

—交接机制建立在一种称为重解析点的NTFS机制的基础上。

硬链接、软链接和快捷方式——文件

特性	硬链接	软链接	快捷方式
是否需要管理员权限	否	是	否
操作方式	*mklink /H Link Target*	*mklink Link Target*	通过鼠标右键创建“快捷方式”
创建限制-1	*Target*只支持文件	*Target*可以是文件，也可以是目录*(/D)*	无
是否占用额外空间	否	否	受目标文件绝对路径长度影响，固定大小
创建限制-2	链接和目标必须位于同一个本地分区内	链接和目标必须位于同一个物理主机上	无
重命名目标文件	不受影响	无法找到	不受影响
移除目标文件	不受影响	无法找到	无法找到
移除目标文件*A*后添加同名文件*A*	不受影响	不受影响	无法找到
修改链接文件	和目标文件保持同步	和目标文件保持同步	快捷方式文件大小固定
文件图标	同目标文件图标	目标文件图标增加了快捷方式箭头	目标文件图标增加了快捷方式箭头

refs: http://msdn.microsoft.com/zh-cn/library/windows/desktop/aa365006(v=vs.85).aspx

为目录创建目录符号链接、联接和快捷方式

- 创建目录符号链接：mklink /D Link Target
  - 需要管理员权限
- 创建联接：mklink /J Link Target
- 创建快捷方式：鼠标右键目标文件-创建快捷方式

- 压缩文件和稀疏文件

—NTFS支持文件数据的压缩功能，应用程序可以直接利用这一特性。

—第二种压缩类型稀疏文件，当文件被标记为稀疏的，NTFS并不为文件中被应用程序指定为空的部分分配磁盘卷空间。当应用程序从一个稀疏文件的空区域中读取数据的时候，NTFS返回以0填充的缓冲区。

- 变化日志

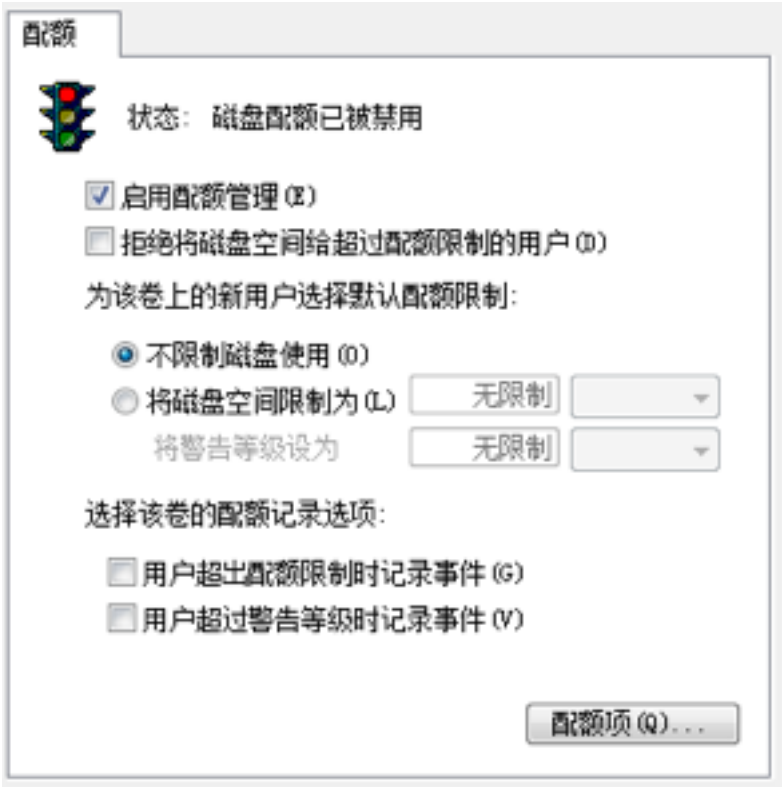
—许多类型的应用程序需要监视卷中的文件和目录的变化，NTFS把相关的文件和目录变化信息记录到变化日志

—这种方式减少对系统性能的影响，同时不必使监控的程序一直运行。

—变化日志文件通常要足够大，保证应用程序有机会毫无遗漏的处理这些变化。

- 针对每个用户的卷配额

—系统管理员通常需要跟踪或限制用户在共享的存储卷上的磁盘空间使用量。NTFS包含了配额管理支持，允许为每个用户指定相应的配额限制。



NTFS的高级特性

- 链接跟踪
  - —外壳快捷方式允许用户把一些文件放在外壳名字空间中，这些文件实际上又链接到文件系统名字空间中的其他文件上。
  - —NTFS包含了一个称为分布式链接-跟踪的服务应用程序的支持，当链接的目标移动时，它会维护这些链接的完整性。
- 加密
  - —NTFS包含一个称为加密文件系统（EFS）的设施，用户可以利用该设施来加密敏感数据，若是有权查看文件数据的用户账号，文件数据自动解密。

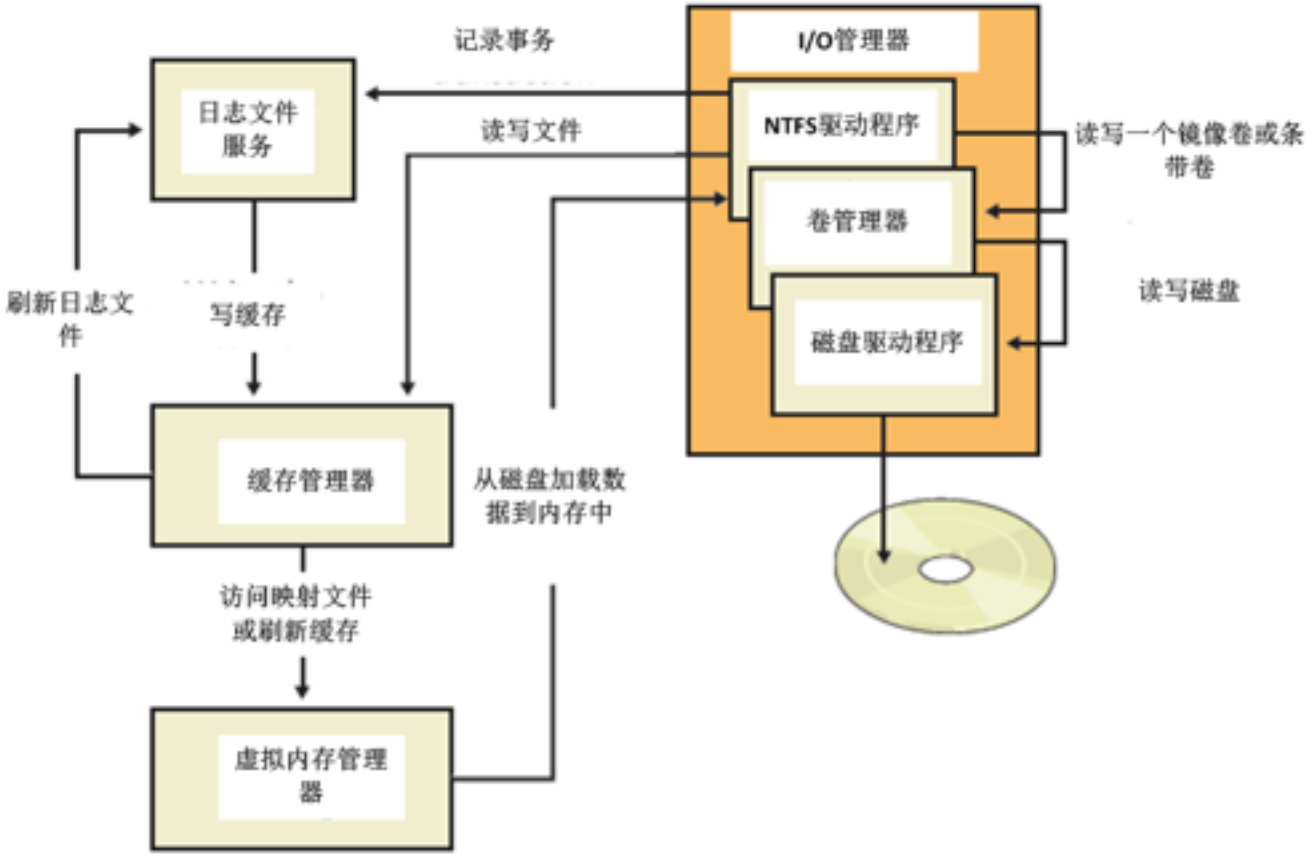
NTFS的高级特性

- POSIX支持
  - —Windwos早期的要求之一是完全支持POSIX 1003.1标准，比如大小写敏感，硬链接等。
- 碎片整理
  - —Windows包含了一个碎片整理API，支持第三方开发磁盘碎片整理工具。
  - —Windows内置了一个碎片整理工具，使用Disk Defragmenter工具（Dfg.msc）可以访问到。
  - —在windows xp中，NTFS的碎片整理支持被重写了。功能的唯一限制是，页面文件和NTFS日志文件不能整理碎片。

- 只读支持
  - —Windows xp以前，NTFS文件系统驱动程序挂载的卷必须位于可写介质上，可以重置事务型日志文件。
  - —Windows xp以后的NTFS驱动程序可以挂载只读介质上的卷，对于具有只读的基本文件系统映像的嵌入式系统来说，这一功能是必要的。

NTFS文件系统驱动程序

- NTFS及其相关组件

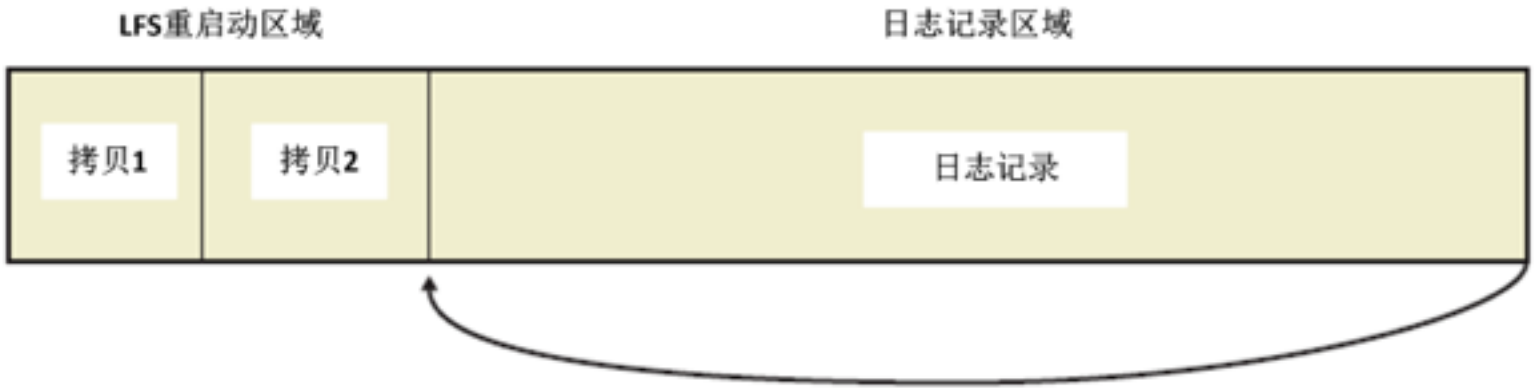


- 日志文件服务（LFS）

—它提供了相应的服务来维护关于磁盘写操作的日志。万一系统失败的话，LFS写得日志文件可被用来恢复一个NTFS格式的卷。

—NTFS传递给LFS一个指针，指向一个已打开的文件对象，指定要访问的日志文件。LFS要么初始化一个新的日志文件，要么调用windows的缓存管理器通过缓存访问已有的日志文件。

- 日志文件服务（LFS）
  - —LFS将日志文件分为两个区域：重启动区域和一个“无限”日志记录区域。
  - —LFS使用逻辑序列号（LSN）来表示这些被写到日志文件中的记录。NTFS使用64位来表达LSN。

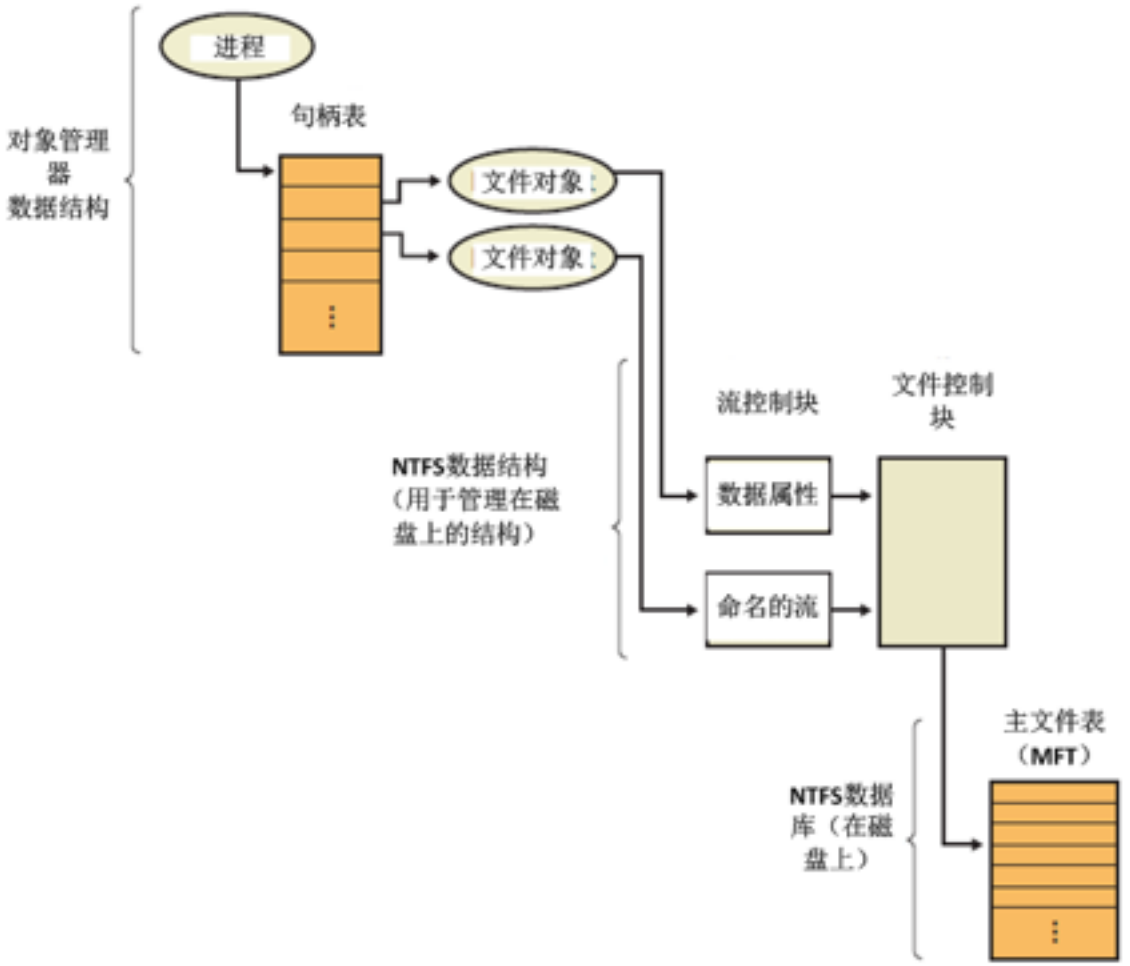


- 缓存管理器
  - —为NTFS和其他的文件系统驱动程序提供了系统范围的缓存服务。
  - —缓存管理器提供了专门的文件系统接口访问windows内存管理器，从磁盘获取文件内容，将缓存的内容刷新到磁盘上。

NTFS数据结构

—文件对象指向文件属性对应的流控制块（SCB）。

—SCB指向一个公共的数据结构，称为文件控制块(FCB)，指向该文件的主文件表（MFT）中的记录。

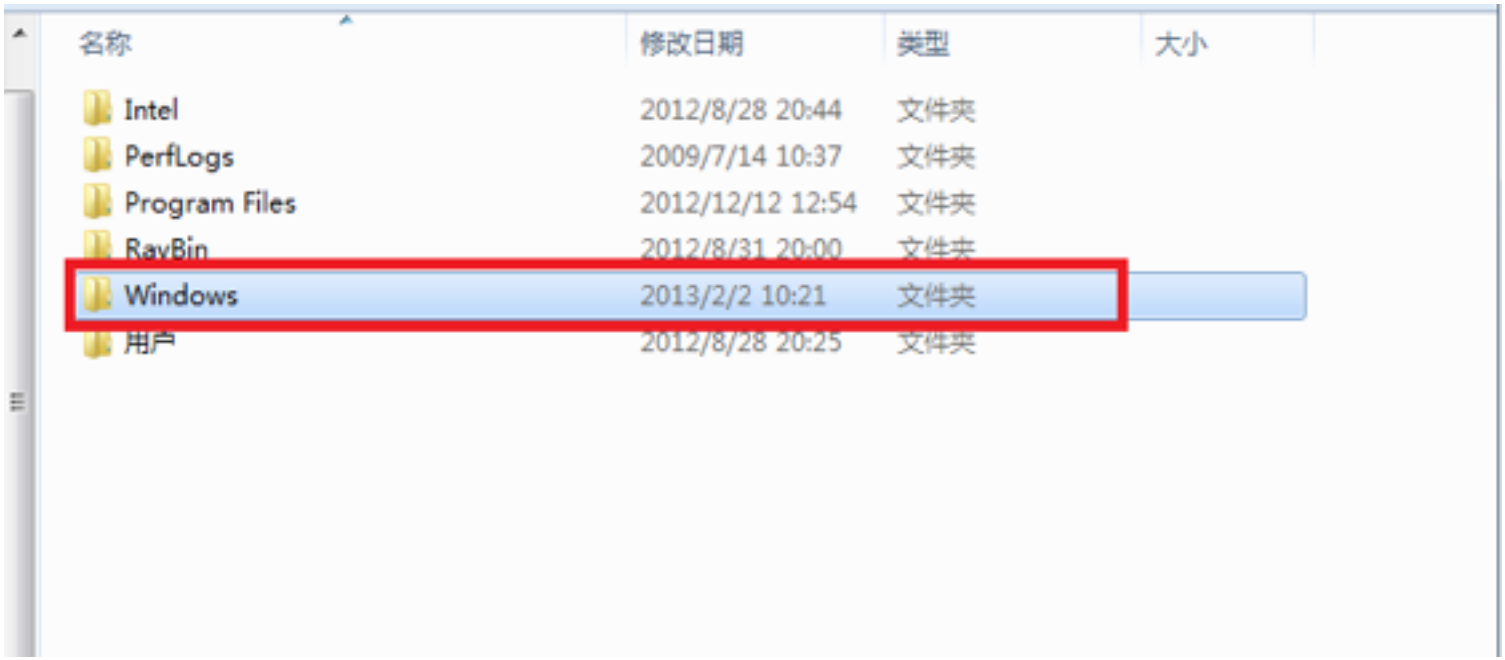


本章内容提要

- NTFS文件系统
- 常见系统文件
- 常见注册表项
- 常见进程项
- 常见网络端口
- 常见服务
- Sysinternals工具集功能介绍

常见系统文件

- 一般来讲，系统一般都位于操作系统所在的分区的Windows文件中



常见系统文件

- System32文件夹用来存放Windows的系统文件和硬件驱动程序
- System文件夹用来存放系统虚拟设备文件

常见系统文件

- CALC.EXE - 计算器应用程序
- REGEDIT.EXE - 注册编辑器
- NOTEPAD.EXE-记事本程序
- CMD.EXE-控制台程序
- MSPAINT.EXE-绘图板程序
- MSCONFIG.EXE-系统配置实用程序

常见系统文件

- ADVAPI32.DLL - 高级Win32应用程序接口
- EXPLORER.EXE - "资源管理器"应用程序
- EXTRACT.EXE - 解压缩工具
- CHKDSK.EXE - DOS磁盘检查工具
- CONTROL.EXE - "控制面板"应用程序

常见系统文件

- HAL.DLL-硬件抽象层
  - —HAL是可加载的内核模式模块，它为Windows系统所运行的硬件平台提供低级接口，隐藏硬件相关的细节
- NTOSKRNL.EXE-Windows系统的内核
  - —在硬件抽象层之上，提供系统的基本机制和硬件支持
  - —可在用户模式下调用导出函数，并通过Ntdll导出

常见系统文件

- NTDLL.DLL-用于子系统DLL
  - —系统服务分发存根，调用Windows执行体系统服务
  - —内部支持函数，供子系统DLL以及其他的原生映像文件使用
- Win32k.sys-内核模式设备驱动程序
  - —窗口管理器，控制窗口显示，屏幕输出，采集来自键盘鼠标和其他设备的输入，同时负责将用户的消息传递给应用程序
  - —图形设备接口，针对图形输出设备的函数库

常见系统文件

- KERNEL32.DLL-子系统DLL
  - —内核级文件，它控制着系统的内存管理、数据的输入输出操作和中断处理
- GDI32.DLL-子系统DLL
  - —gdi32.dll是Windows GDI图形用户界面相关程序，包含的函数用来绘制图像和显示文字
- USER32.DLL-子系统DLL
  - —Windows用户界面相关应用程序接口，用于包括Windows处理，基本用户界面等特性，如创建窗口和发送消息

本章内容提要

- NTFS文件系统
- 常见系统文件
- 常见注册表项
- 常见进程项
- 常见网络端口
- 常见服务
- Sysinternals工具集功能介绍

常见的注册表项(启动项)

- 系统启动时加载相关的注册表项（win7）
  - —HKLM\System\CurrentControlSet\Control\Terminal Server\Wds\rdpwd\StartupPrograms
  - —HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit
  - —HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\VmApplet
  - —HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell
  - —HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell
  - —HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
  - —HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components
  - —HKLM\Software\Microsoft\Windows NT\CurrentVersion\Windows\IconServiceLib
  - —HKCU\Software\Microsoft\Windows\CurrentVersion\Run

常见的注册表项(文件关联)

- txt文件默认的打开方式
  —HKEY_CLASSES_ROOT\txtfile\shell\open\command\
- txt文件关联
  —HKEY_CLASSES_ROOT\.txt\
- exe文件默认的打开方式
  —HKEY_CLASSES_ROOT\exefile\shell\open\command\
- exe文件关联
  —HKEY_CLASSES_ROOT\.exe\

常见的注册表项(系统配置)

- 应用程序劫持项（恶意程序利用该键实现自动运行）
  —HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution
- IE浏览器启动时自动加载对象
  —HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper

常见的注册表项(系统配置)

- 系统启动时加载Native程序，启动早于所有的windows子系统进程
  - —HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\BootExecute
- 修改该值会造成任务管理器无法启动
  - —HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\windows\currentVersion\policies\system\DisableTaskMgr
  - —HKEY_CURRENT_USER\SOFTWARE\Microsoft\windows\currentVersion\policies\system\DisableTaskMgr

常见的注册表项(系统配置)

- 保存驱动程序加载顺序的列表（恶意程序修改其值，使相关驱动更早被加载，躲避安全软件的检测）

  —HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\ServiceGroupOrder\List

- 记录windows安全模式的相关信息，删除该项，用户无法登陆安全模式

  —HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot

常见的注册表项(系统配置)

- 恶意程序利用该键值在CMD运行前启动其他应用程序

  —HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\AutoRun

- 在该项下增加程序文件名，使explorer.exe无法运行被指定的程序

  —HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\DisAllowRun\

常见的注册表项(IE配置)

- 该项在IE用户界面添加工具栏按钮，运行脚本并加载相应的组件（恶意程序利用它达到运行代码的目的）
  - —HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\Extension
  - —HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Extension

常见的注册表项(IE配置)

- IE无法确认用户输入的地址所使用的协议时，就会根据这个键值指定的组件来解析地址（恶意程序利用这个键值实现自动启动）
  - —HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\URLSearchHooks
  - —HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\URLSearchHooks

常见的注册表项(IE配置)

- 指向IE的主页（恶意程序会改写此项，使浏览器显示访问恶意或者用户不期望的页面）
  - —HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\Main\Start Page
  - —HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\Start Page

常见的注册表项(杂项)

- Windows NT 4.0以上版本系统使用KnowDll注册表项来搜索并加载动态库（恶意程序通过修改使系统加载恶意程序的动态库并实现自动运行）
  - —HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\knownDlls
- TCP/IP数据库路径，TCP/IP设置保存在该目录下
  - —HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\DataBasePath

本章内容提要

- NTFS文件系统
- 常见系统文件
- 常见注册表项
- 常见进程项
- 常见网络端口
- 常见服务
- Sysinternals工具集功能介绍

查看进程的两种方法


```
C:\Users\satiago>tasklist

映像名称                       PID 会话名              会话#       内存使用
========================= ======== ================ =========== ============
System Idle Process              0 Services                   0         24 K
System                           4 Services                   0      2,388 K
smss.exe                       308 Services                   0        200 K
csrss.exe                      496 Services                   0      2,364 K
wininit.exe                    548 Services                   0        388 K
csrss.exe                      556 Console                    1     25,764 K
winlogon.exe                   604 Console                    1      1,740 K
services.exe                   648 Services                   0      3,972 K
lsass.exe                      664 Services                   0      4,272 K
lsm.exe                        672 Services                   0      1,292 K
svchost.exe                    776 Services                   0      3,180 K
nvvsvc.exe                     844 Services                   0      1,880 K
nvSCPAPISvr.exe                868 Services                   0      1,344 K
svchost.exe                    916 Services                   0      4,016 K
svchost.exe                   1028 Services                   0      9,288 K
svchost.exe                   1060 Services                   0     80,120 K
svchost.exe                   1104 Services                   0     24,188 K
svchost.exe                   1296 Services                   0      5,388 K
svchost.exe                   1476 Services                   0      9,348 K
sched.exe                     1688 Services                   0      1,396 K
svchost.exe                   1740 Services                   0      9,072 K
AlipaySecSvc.exe              1876 Services                   0      3,328 K
avguard.exe                   1928 Services                   0        724 K
AppleMobileDeviceService.     1948 Services                   0        964 K
mDNSResponder.exe             1980 Services                   0      1,968 K
```

常见进程项（系统进程）

- System进程
  - —进程名称：windows内存处理系统进程
  - —描述：windows页面内存管理进程，拥有0级优先。
- alg进程
  - —进程名称：应用层网关服务
  - —描述：这是一个应用层网关服务，用于网络共享。
- csrss进程
  - —进程名称：客户端服务子系统
  - —描述：用以控制windows图形相关子系统

常见进程项（系统进程）

- System Idle Process进程
  - —进程名称：windows空闲进程
  - —描述：表示CPU的空闲率
- Lsass进程
  - —进程名称：本地安全权限服务
  - —描述：本地安全权限服务控制windows安全机制
- Services进程
  - —进程名称：windows服务控制
  - —描述：管理windows服务

常见进程项（系统进程）

- Smss进程
  - —进程名称：会话管理子系统
  - —描述：该进程为会话管理子系统用以初始化系统变量，调用win32子程序在登录过程中运行。
- Spoolsv进程
  - —进程名称：打印机服务
  - —描述：用于使打印机就绪

常见进程项（系统进程）

- Svchost进程
  - —进程名称：主机服务程序
  - —描述：标准的动态链接库主机处理服务
- Winlogon进程
  - —进程名称：windows登陆进程
  - —描述：windows用户的登陆程序
- Taskmgr进程
  - —进程名称：windows任务管理器
  - —描述：执行windows的任务

常见进程项（系统进程）

- Explorer进程
  - —进程名称：windows资源管理器
  - —描述：管理windows图形壳，包括开始菜单，任务栏，桌面和文件管理

本章内容提要

- NTFS文件系统
- 常见系统文件
- 常见注册表项
- 常见进程项
- 常见网络端口
- 常见服务
- Sysinternals工具集功能介绍

常见网络端口

- 查看网络端口的指令

```
Microsoft Windows [版本 6.1.7600]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Users\satiago netstat -an

活动连接

  协议  本地地址          外部地址        状态
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:912            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1025           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1026           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1027           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1029           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1031           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:7712           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:11862          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:12048          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:17500          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:34383          0.0.0.0:0              LISTENING
  TCP    10.109.39.226:139      0.0.0.0:0              LISTENING
  TCP    10.109.39.226:1148     219.230.87.50:18600    LAST_ACK
  TCP    10.109.39.226:3725     61.54.7.55:80          CLOSE_WAIT
```

常见网络端口

- 21端口
  - —端口说明：21端口主要用于FTP(文件传输协议)服务，实现两台计算机之间文件的上传与下载。另外，还有20端口号用于FTP数据传输的默认端口号。
  - —操作建议：FTP由于可以匿名登录，常被黑客和木马利用，不架设FTP服务器时，建议关闭21端口。
- 23端口
  - —端口说明：23端口主要用于Telnet（远程登录）服务，允许用户使用命令行进行相应的操作。
  - —操作建议：利用Telnet服务，黑客可以扫描系统的服务和类型，也是木马的常用端口。

常见网络端口

- 25端口

  —端口说明：该端口用于SMTP服务器开放，用于发送邮件。

  —操作建议：木马通过这个端口监视计算机正在运行的所有的窗口和模块，无SMTP服务时建议关闭。

- 53端口

  —端口说明：该端口为DNS（域名服务器）开放，主用用于域名解析。

  —操作建议：黑客利用该端口获取web服务器的IP地址，不提供服务时建议关闭。

常见网络端口

- 69端口
  - —端口说明：该端口为TFTP（次要文件传输协议）服务开放，类似于简单的FTP。
  - —操作建议：黑客可以利用TFTP的错误配置从系统获取任何文件，建议关闭。
- 80端口
  - —端口说明：该端口为HTTP(超文本传输协议)开放，用于在www传输协议。
  - —操作建议：有些木马程序会通过该端口攻击计算机，但上网时，必须开启。

常见网络端口

- 110端口
  - —端口说明：该端口是为POP3(邮件协议)开放的，主要用于接收邮件。
  - —操作建议：该端口的服务漏洞可以被木马利用来窃取用户名，密码。无服务是建议关闭。
- 135端口
  - —端口说明：该端口用于RPC(远程过程调用)协议并提供DCOM(分布式组件对象模型)服务。
  - —操作建议：为了避免“冲击波”病毒的攻击，建议关闭。

- 143端口

  —端口说明：该端口为IMAP(Internet消息访问协议)开放，用于邮件的接收，是目前的主流协议。

  —操作说明：该端口服务存在缓冲区漏洞，泄露用户名和密码，无服务是建议关闭。

- 161端口

  —端口说明：该端口为SNMP(简单网络管理协议)开放，用于管理TCP\IP网络中的协议。

  —操作建议：黑客用该端口获取网络中的设备信息和对设备的控制，建议关闭。

- 443端口
  - —端口说明：该端口用于HTTPS(提供加密和安全传输)服务，保证信息的安全性。
  - —操作建议：HTTPS服务通过SSL来保证安全性，SSL的漏洞可能被利用，建议开启，及时安装SSL补丁。
- 1080端口
  - —端口说明：该端口是Socks代理服务使用的端口。
  - —操作建议：一些蠕虫病毒会监听1080端口，建议无服务时关闭。

- 4000端口

—端口说明：该端口用于QQ工具的客户端，服务端是8000端口，这两种端口属于UDP协议。

—操作建议：该端口的服务存在漏洞，蠕虫病毒可以伪造数据写入硬盘，一般为了使用QQ聊天，建议开启。

更多知名端口对应服务关系表

- *nix系统上的/etc/services文件

```
72 ftp-data          20/udp     # File Transfer [Default Data]
73 ftp-data          20/tcp     # File Transfer [Default Data]
74 ftp               21/udp     # File Transfer [Control]
75 ftp               21/tcp     # File Transfer [Control]
76 #                            Jon Postel <postel@isi.edu>
77 ssh               22/udp     # SSH Remote Login Protocol
78 ssh               22/tcp     # SSH Remote Login Protocol
79 #                            Tatu Ylonen <ylo@cs.hut.fi>
80 telnet            23/udp     # Telnet
81 telnet            23/tcp     # Telnet
```

```
408 netbios-ns       137/udp     # NETBIOS Name Service
409 netbios-ns       137/tcp     # NETBIOS Name Service
410 netbios-dgm      138/udp     # NETBIOS Datagram Service
411 netbios-dgm      138/tcp     # NETBIOS Datagram Service
412 netbios-ssn      139/udp     # NETBIOS Session Service
413 netbios-ssn      139/tcp     # NETBIOS Session Service
```

本章内容提要

- NTFS文件系统
- 常见系统文件
- 常见注册表项
- 常见进程项
- 常见网络端口
- 常见服务
- Sysinternals工具集功能介绍

Windows服务初印象

- 可长时间运行的进程
- 可实现开机自启动

名称	描述	状态	启动类型	登录为
Routing and Remote Access	在局域网以及广域网环境中为企业提供路由服务。		已禁用	本地系统
Secondary Logon	启用替换凭据下的启用进程。如果此服务被终止，此类型登录访问将不可用。如果此服务被禁用，任何...	已启动	自动	本地系统
Security Accounts Manager	存储本地用户帐户的安全信息。	已启动	自动	本地系统
Security Center	监视系统安全设置和配置。	已启动	自动	本地系统
Server	支持此计算机通过网络的文件、打印、和命名管道共享。如果服务停止，这些功能不可用。如果服务被...	已启动	自动	本地系统
Shell Hardware Detection	为自动播放硬件事件提供通知。		已禁用	本地系统
Smart Card	管理此计算机对智能卡的取读访问。如果此服务被终止，此计算机将无法取读智能卡。如果此服务被禁...	已启动	自动	本地服务
SSDP Discovery Service	启动您家庭网络上的 UPnP 设备的发现。	已启动	手动	本地服务
System Event Notification	跟踪系统事件，如登录 Windows，网络以及电源事件等。将这些事件通知给 COM+ 事件系统 “订阅者(s...	已启动	自动	本地系统
System Restore Service	执行系统还原功能。 要停止服务，请从“我的电脑”的属性中的系统还原选项卡关闭系统还原	已启动	自动	本地系统
Task Scheduler	使用户能在此计算机上配置和制定自动任务的日程。如果此服务被终止，这些任务将无法在日程时间里...	已启动	自动	本地系统
TCP/IP NetBIOS Helper	允许对“TCP/IP 上 NetBIOS (NetBT)”服务以及 NetBIOS 名称解析的支持。	已启动	自动	本地服务
Telephony	提供 TAPI 的支持，以便程序控制本地计算机，服务器以及 LAN 上的电话设备和基于 IP 的语音连接。	已启动	手动	本地系统
Telnet	允许远程用户登录到此计算机并运行程序，并支持多种 TCP/IP Telnet 客户，包括基于 UNIX 和 Windo...		已禁用	本地系统
Terminal Services	允许多位用户连接并控制一台机器，并且在远程计算机上显示桌面和应用程序。这是远程桌面(包括管理...	已启动	手动	本地系统
Themes	为用户提供使用主题管理的经验。	已启动	自动	本地系统
Uninterruptible Power Supply	管理连接到计算机的不间断电源(UPS)。		手动	本地服务
Universal Plug and Play Device Host	为主持通用即插即用设备提供支持。		手动	本地服务
VirtualBox Guest Additions Service	Manages VM runtime information, time synchronization, remote sysprep execution and miscella...	已启动	自动	本地系统
Volume Shadow Copy	管理并执行用于备份和其它目的的卷影复制。如果此服务被终止，备份将没有卷影复制，并且备份会失...		手动	本地系统
WebClient	使基于 Windows 的程序能创建、访问和修改基于 Internet 的文件。如果此服务被终止，将会失去这些...	已启动	自动	本地服务
Windows Audio	管理基于 Windows 的程序的音频设备。如果此服务被终止，音频设备及其音效将不能正常工作。如果此...	已启动	自动	本地系统
Windows Firewall/Internet Connection Sharing (ICS)	为家庭和小型办公网络提供网络地址转换、寻址、名称解析和/或入侵保护服务。	已启动	自动	本地系统
Windows Image Acquisition (WIA)	为扫描仪和照相机提供图像捕获。		手动	本地系统

本章内容提要

- NTFS文件系统
- 常见系统文件
- 常见注册表项
- 常见进程项
- 常见网络端口
- 常见服务
- Sysinternals工具集功能介绍

Sysinternals工具分类

- 文件和磁盘工具
- 网络工具
- 进程安全
- 安全工具
- 系统信息工具
- 杂项工具

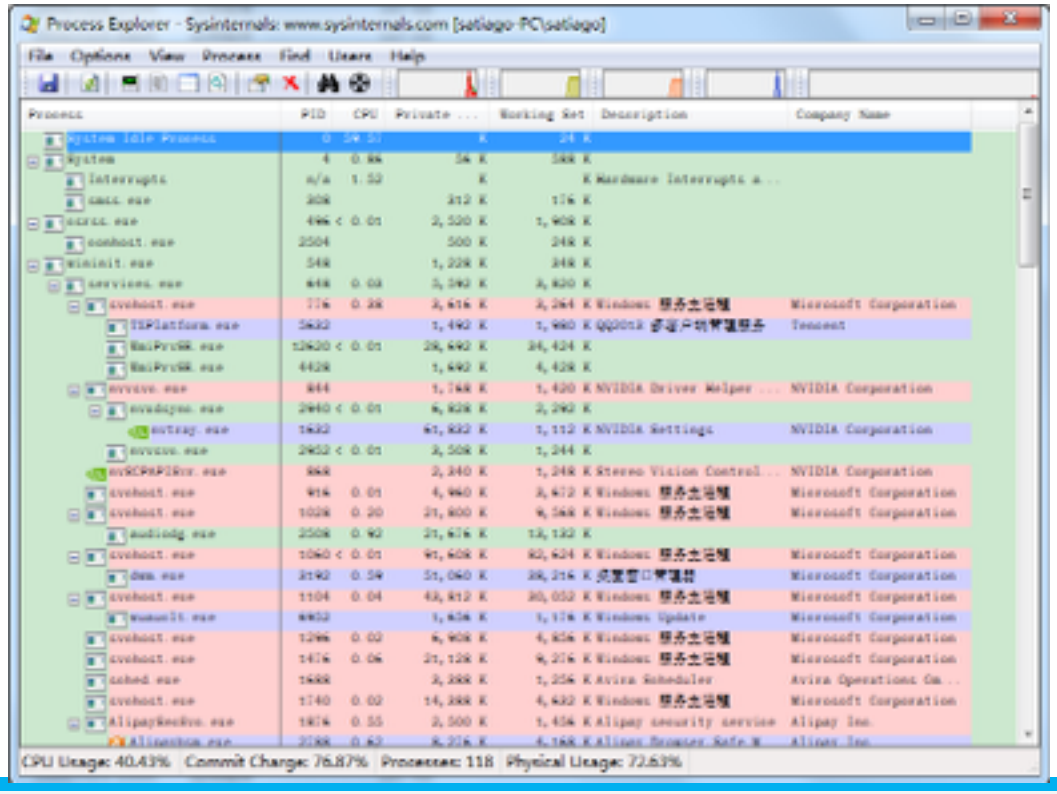
下载链接：http://technet.microsoft.com/en-us/sysinternals/bb545027

Sysinternals工具的TOP10

- Process Explorer
- AutoRuns
- Process Monitor （已更名为ProcMon）
- PsTools
- PageDefrag
- RootkitRevealer
- TcpView
- BgInfo
- BlueScreen
- Desktops

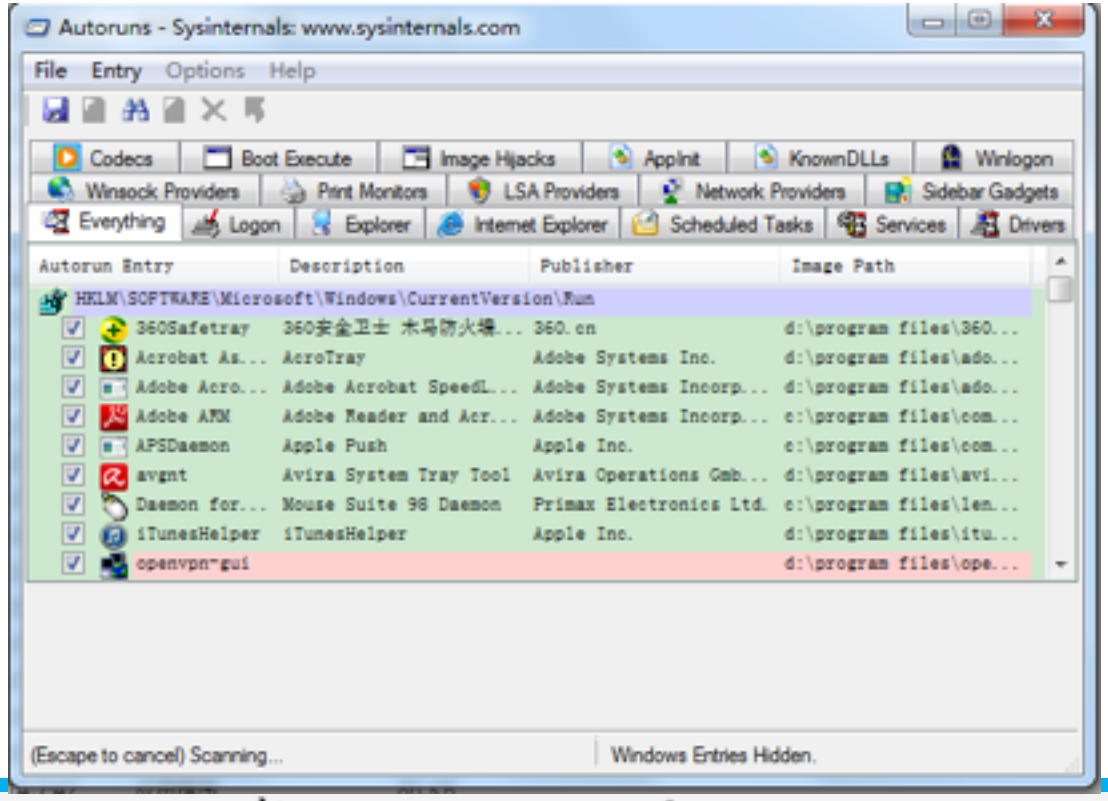
Process Explorer

- 找出进程打开了哪些文件、注册表项和其他对象以及已加载哪些 DLL 等信息。甚至可以显示每个进程的所有者。



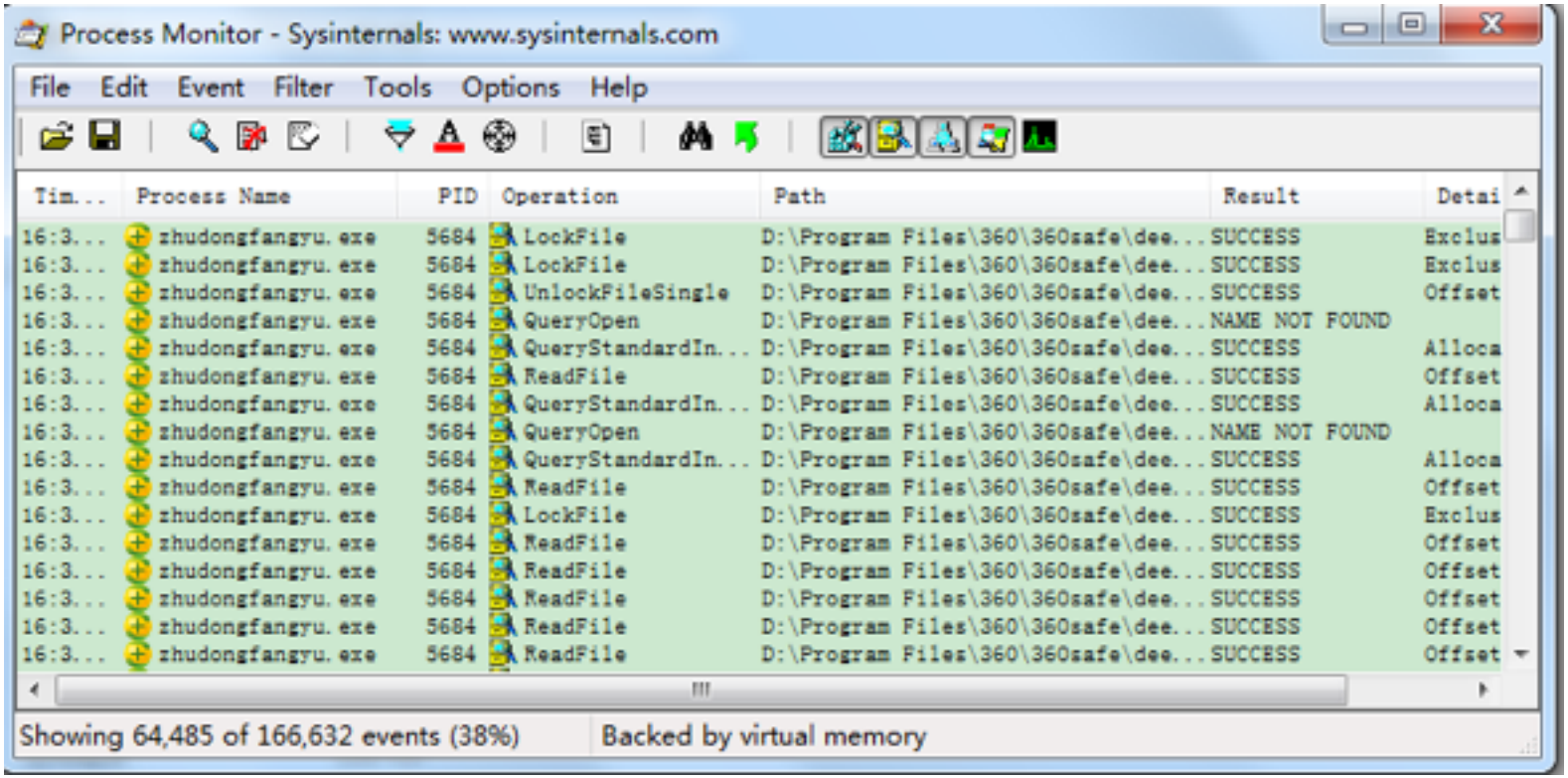
AutoRuns

- 查看哪些程序被配置为在系统启动和您登录时自动启动。Autoruns 还能够完整列出应用程序可以配置自动启动设置的注册表和文件位置。



Process Monitor

- 实时监视文件系统、注册表、进程、线程和DLL 活动。



PsTools

- PsTools 套件包括一些命令行程序，可列出本地或远程计算机上运行的进程、远程运行进程、重新启动计算机、转储事件日志，以及执行其他任务。
  - —PsExec在远程系统上执行进程。
  - —PsFile查看远程打开的文件。
  - —PsGetSid显示计算机或用户的 SID。
  - —PsInfo获取有关系统的信息。
  - —PsKill终止本地或远程进程。
  - —PsList显示有关进程和线程的信息。

PsTools

—PsLoggedOn显示登录到某个系统的用户。

—PsLogList转储事件日志记录。

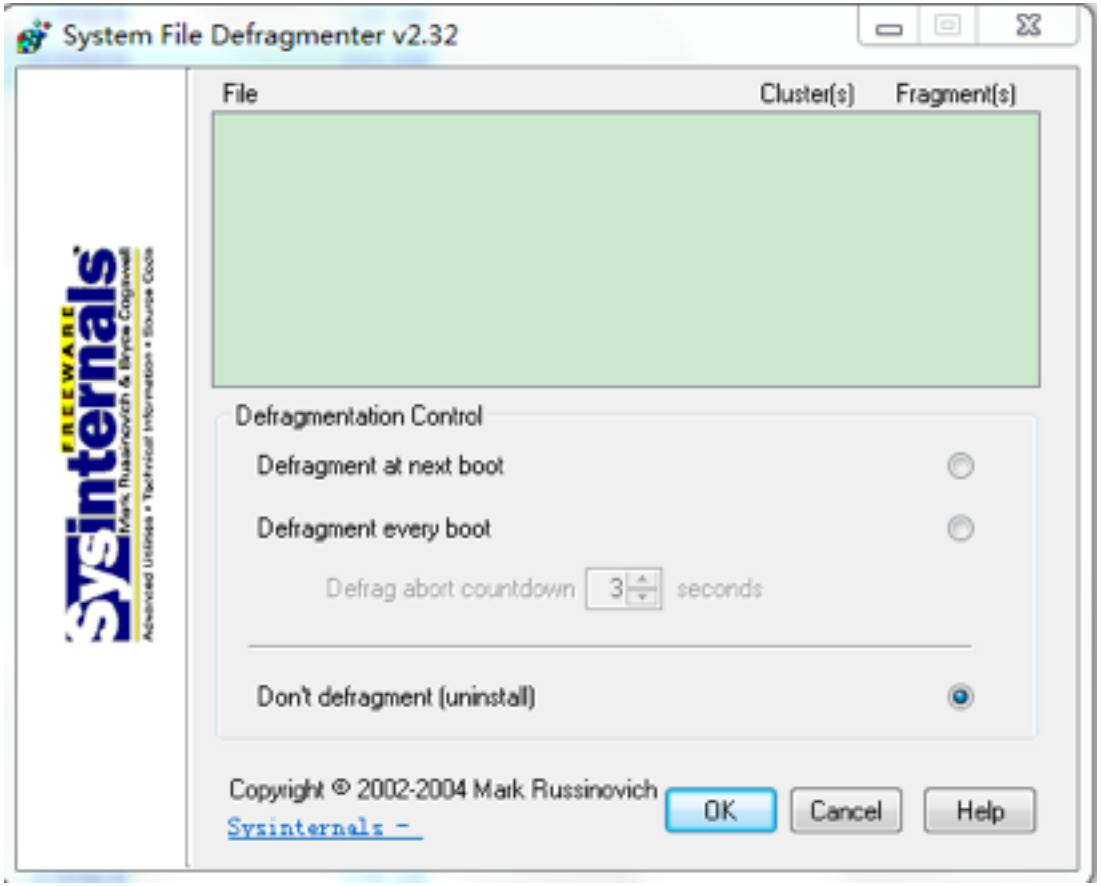
—PsPasswd更改帐户密码。

—PsService查看和控制服务。

—PsShutdown关闭并重新启动（可选）计算机。

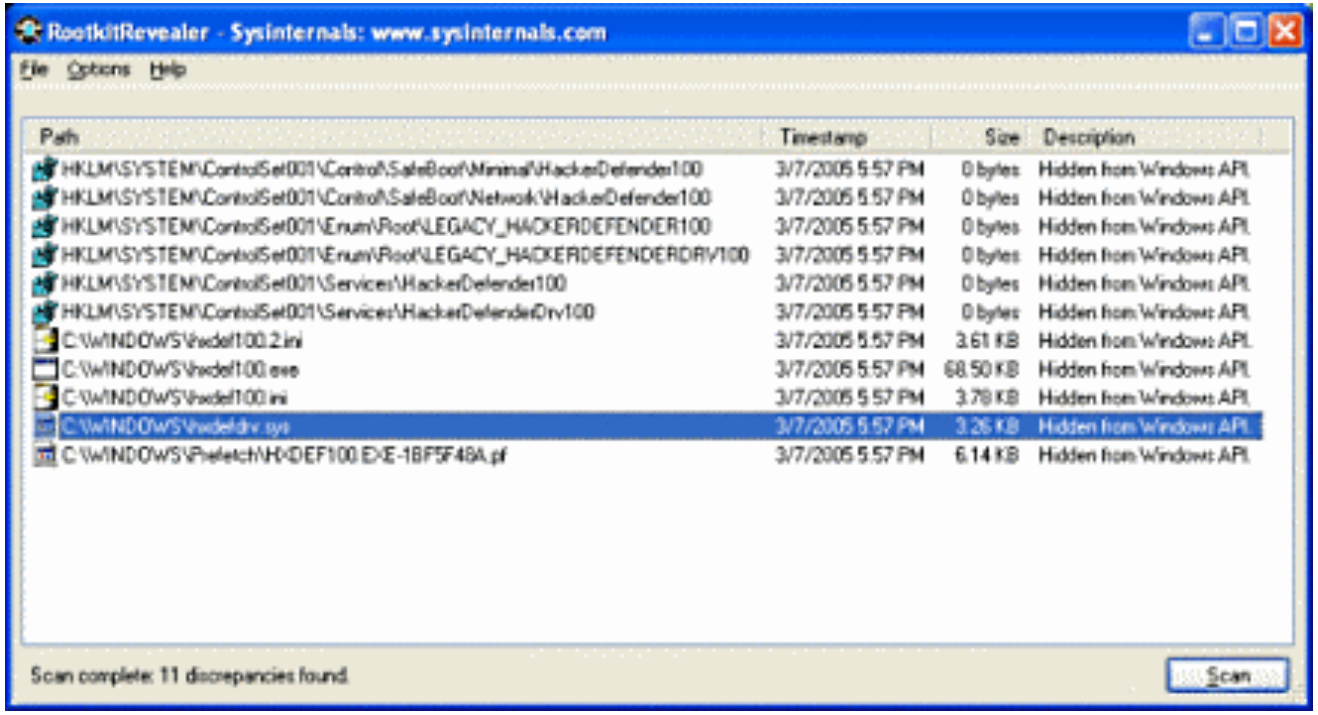
—PsSuspend挂起和继续进程。

- 对您的分页文件和注册表配置单元进行碎片整理。



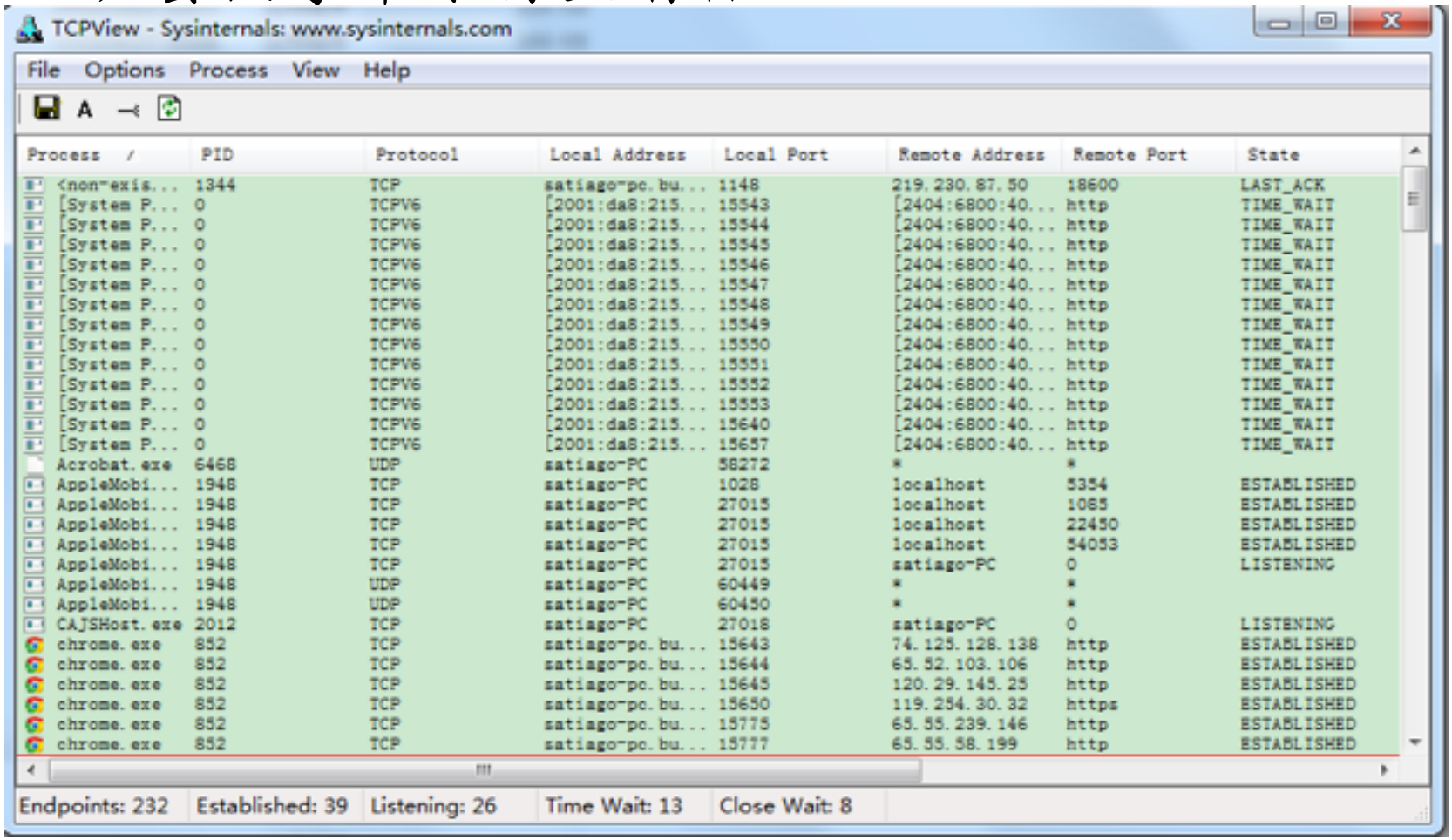
RootkitRevealer

- 扫描系统以找出基于 Rootkit 的恶意软件。



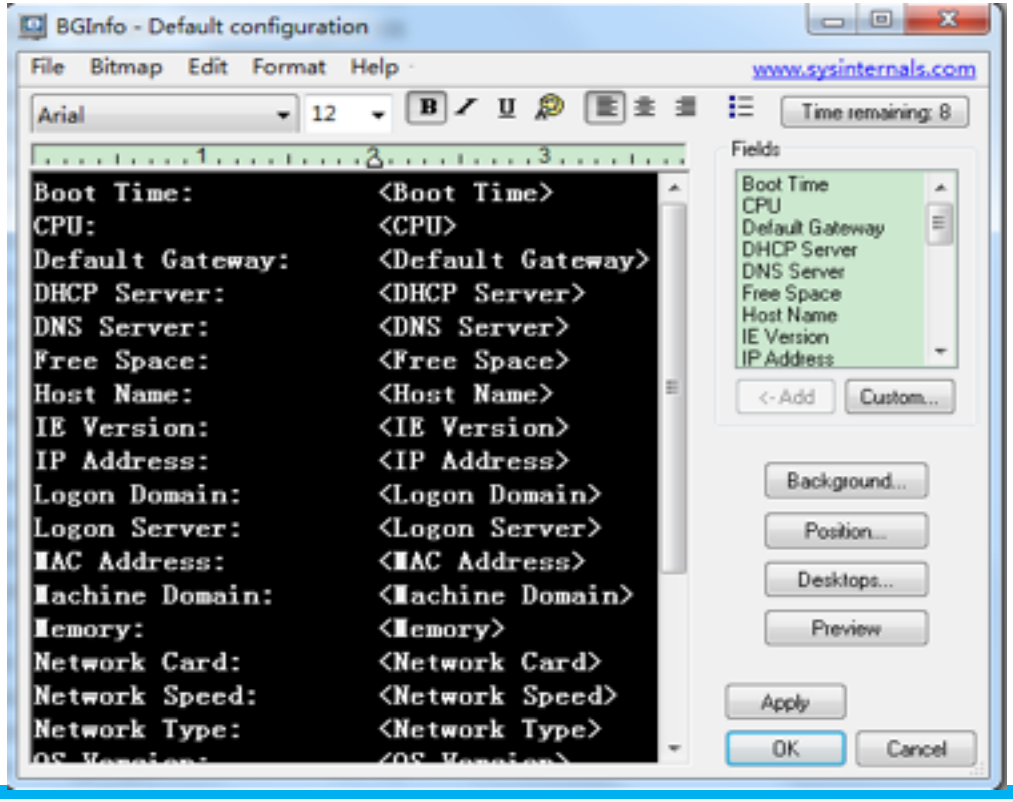
TcpView

- 活动套接字命令行查看器。



BgInfo

- 此完全可配置程序会自动生成桌面背景，其中包含有关系统的 IP 地址、计算机名称、网络适配器及更多内容的重要信息。

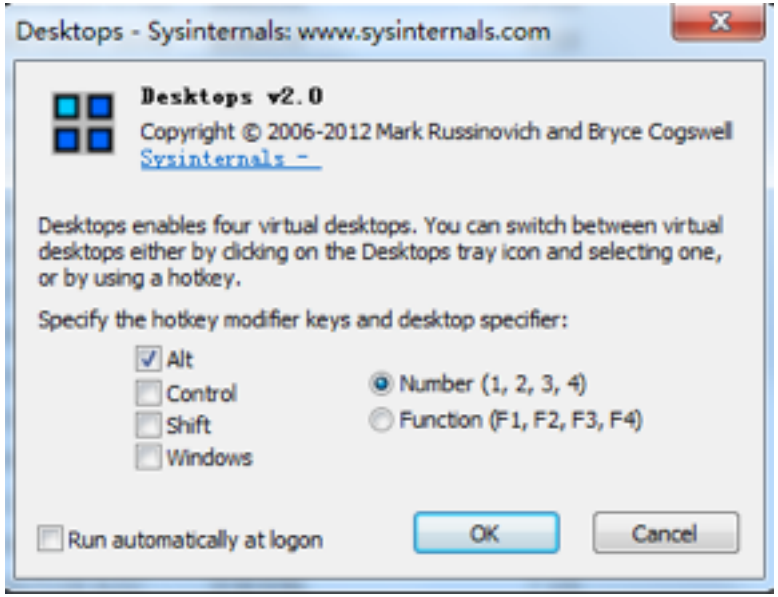


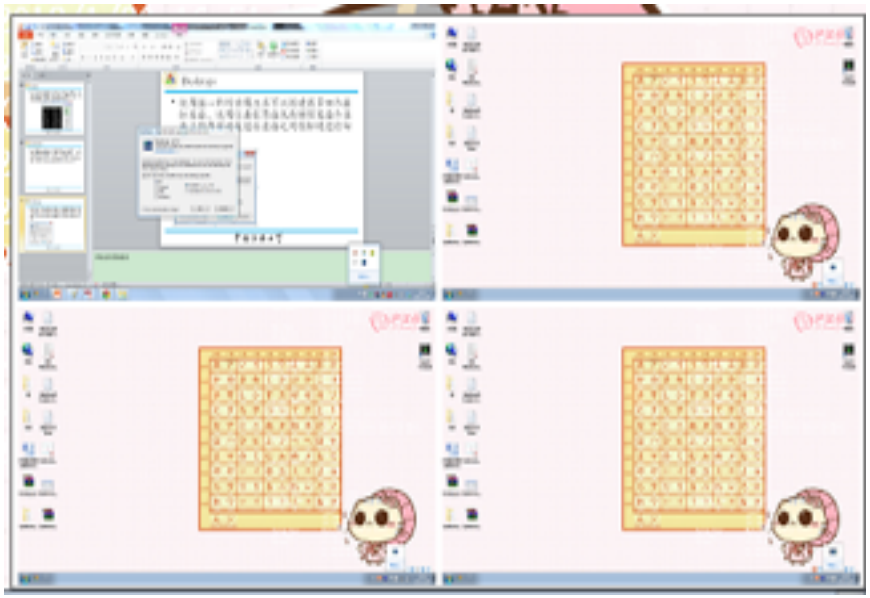
BlueScreen（屏幕保护程序）

- 此屏幕保护程序不仅精确模拟“蓝屏”，而且也模拟重新启动（完成 CHKDSK），并可在 Windows NT 4、Windows 2000、Windows XP、Server 2003 和 Windows 9x 上工作。

Desktops

- 使用这一新的实用工具可以创建最多四个虚拟桌面，使用任务栏界面或热键预览每个桌面上的内容并在这些桌面之间轻松地进行切换。





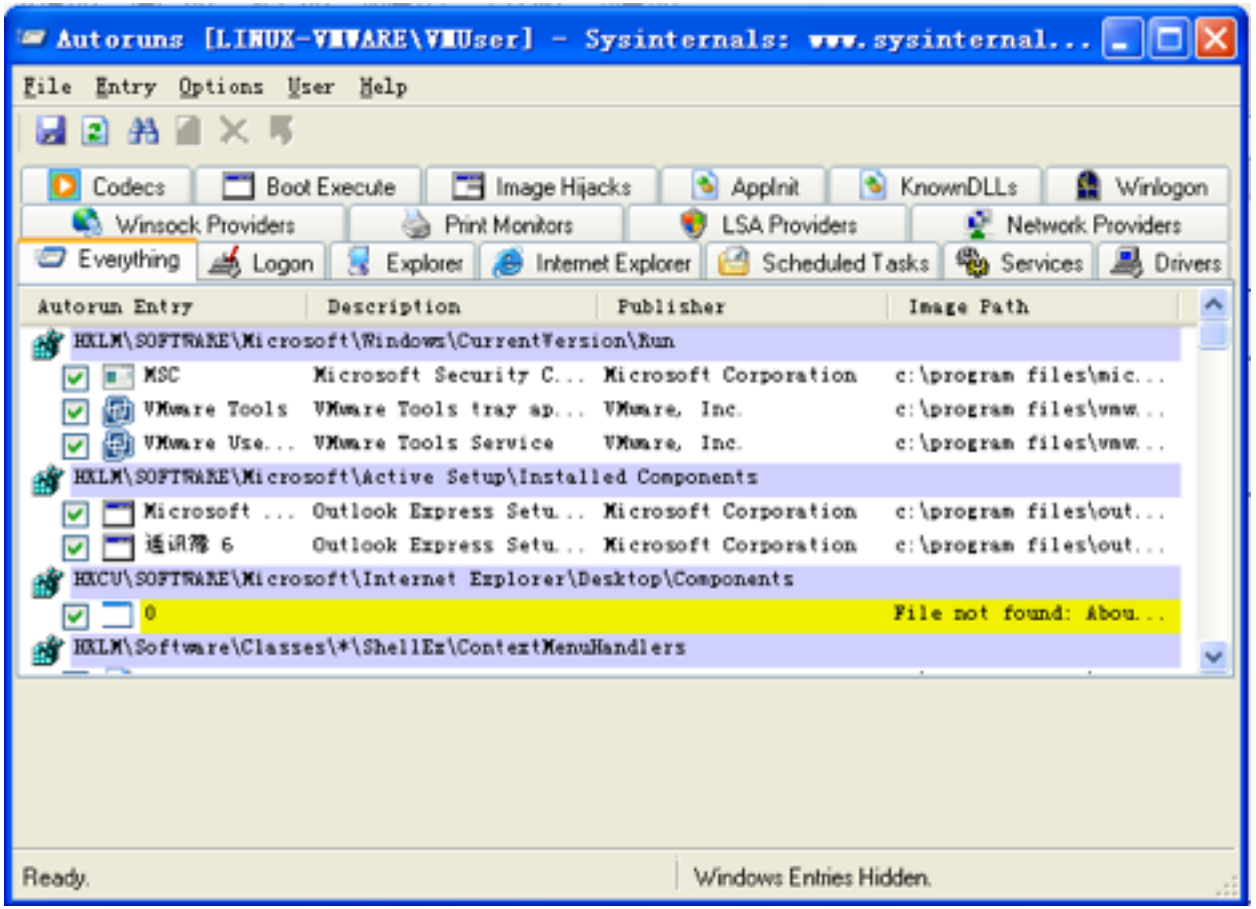
深入Windows内部技术细节的相关工具

TABLE 1-3 Tools for Viewing Windows Internals

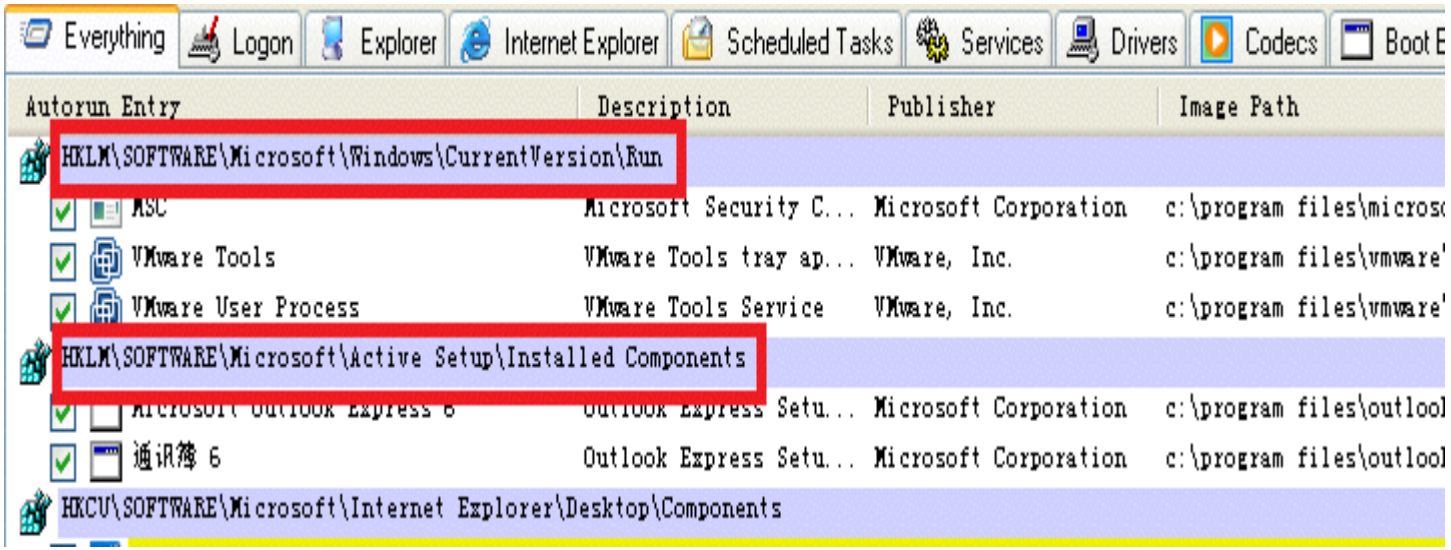
Tool	Image Name	Origin
Startup Programs Viewer	AUTORUNS	Sysinternals
Access Check	ACCESSCHK	Sysinternals
Dependency Walker	DEPENDS	*www.dependencywalker.com*
Global Flags	GFLAGS	Debugging tools
Handle Viewer	HANDLE	Sysinternals
Kernel debuggers	WINDBG, KD	Debugging tools, Windows SDK
Object Viewer	WINOBJ	Sysinternals
Performance Monitor	PERFMON.MSC	Windows built-in tool
Pool Monitor	POOLMON	Windows Driver Kit
Process Explorer	PROCEXP	Sysinternals
Process Monitor	PROCMON	Sysinternals
Task (Process) List	TLIST	Debugging tools
Task Manager	TASKMGR	Windows built-in tool

课内实验

- 实验一 sysinternals工具使用--Autoruns

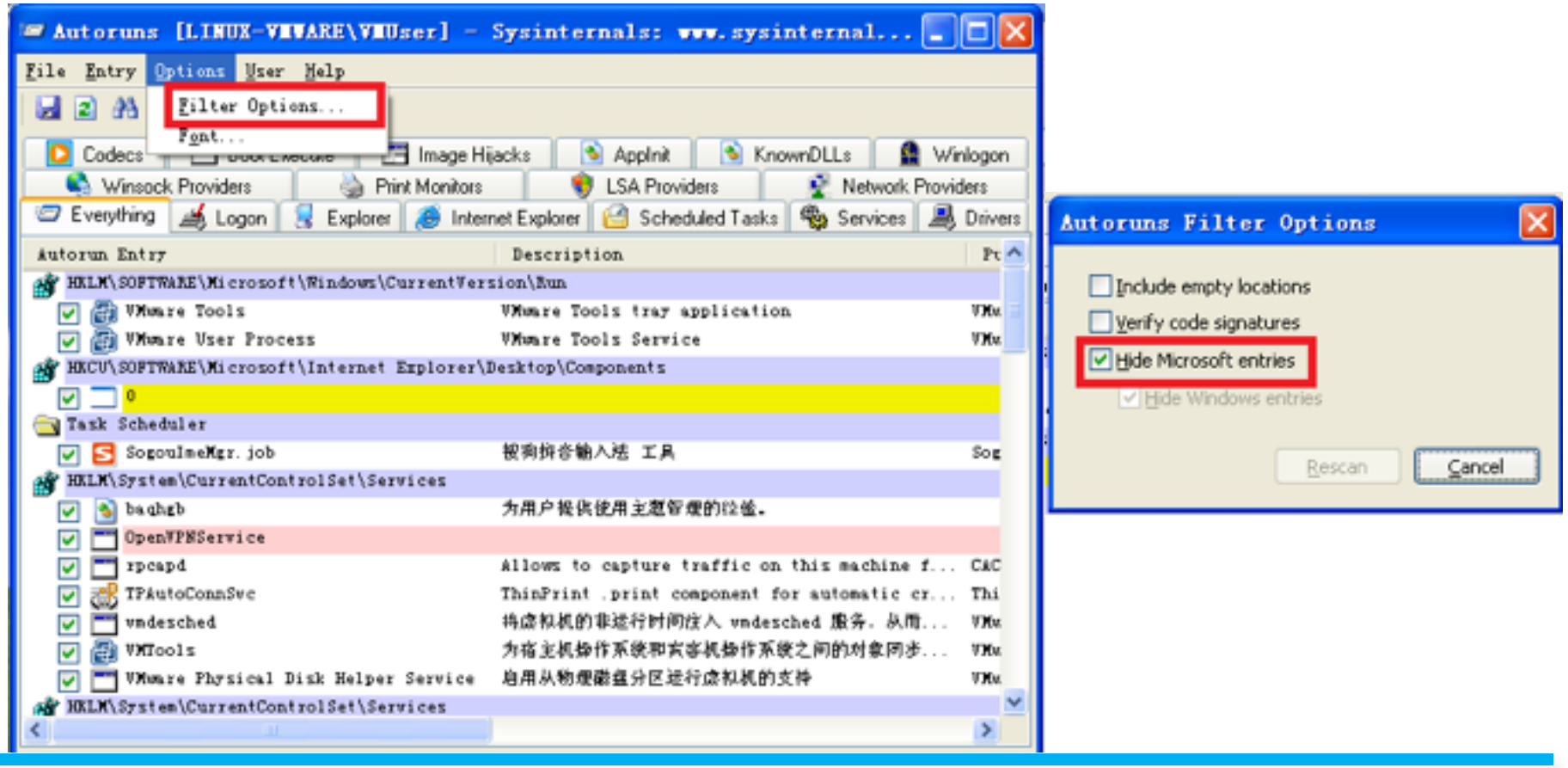


- 该工具可以查看对应的注册表项的自启动项，还可以分类参看，方便和注册表的比对



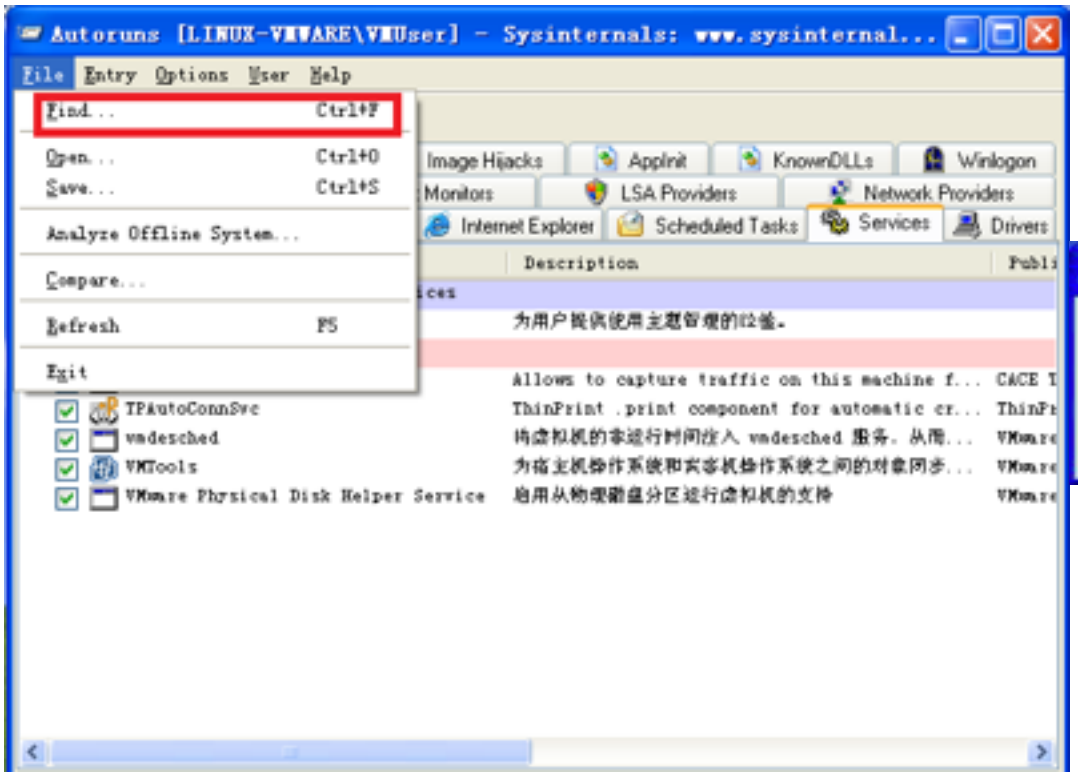
课内实验

- 查看不明自启动项，排除微软自己的自启动项，方便查看



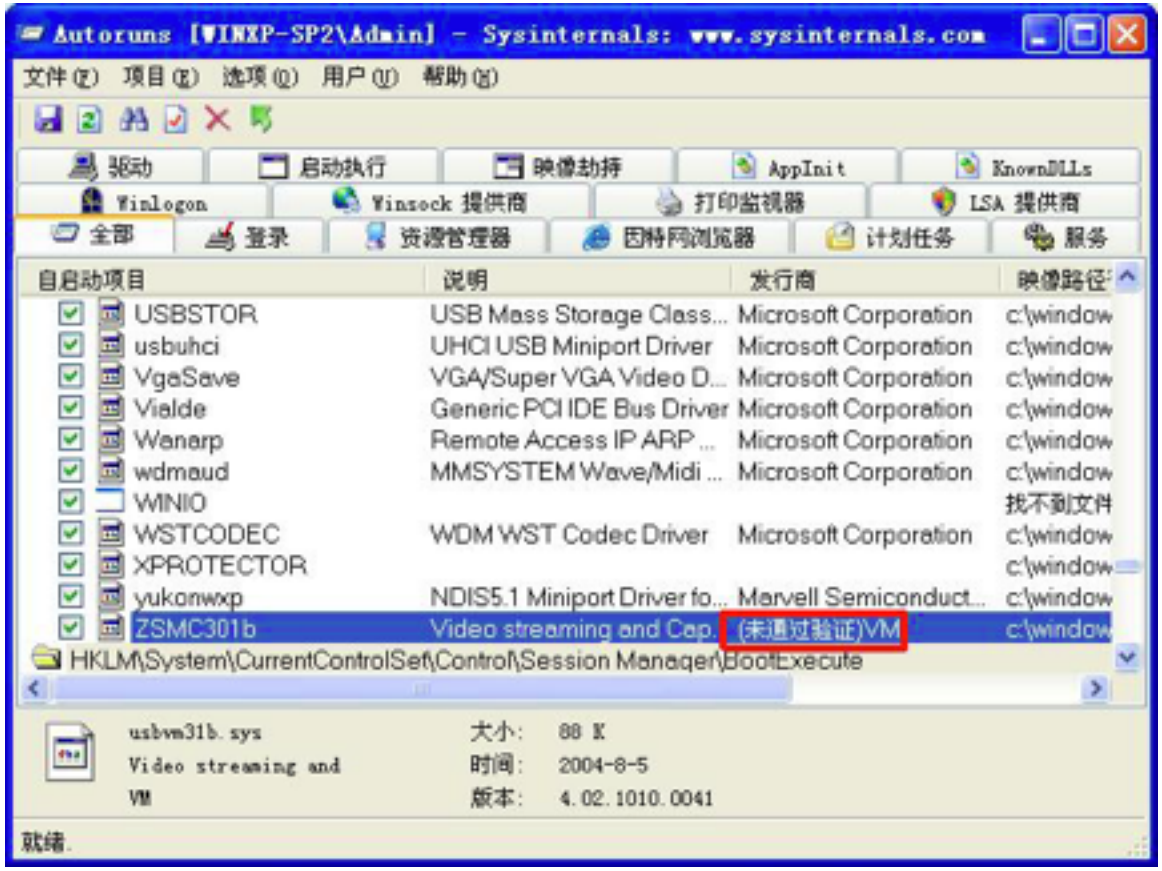
课内实验

- 查找可疑的自启动程序（这里USBVM31B.sys为摄像头驱动程序，作为可疑程序）



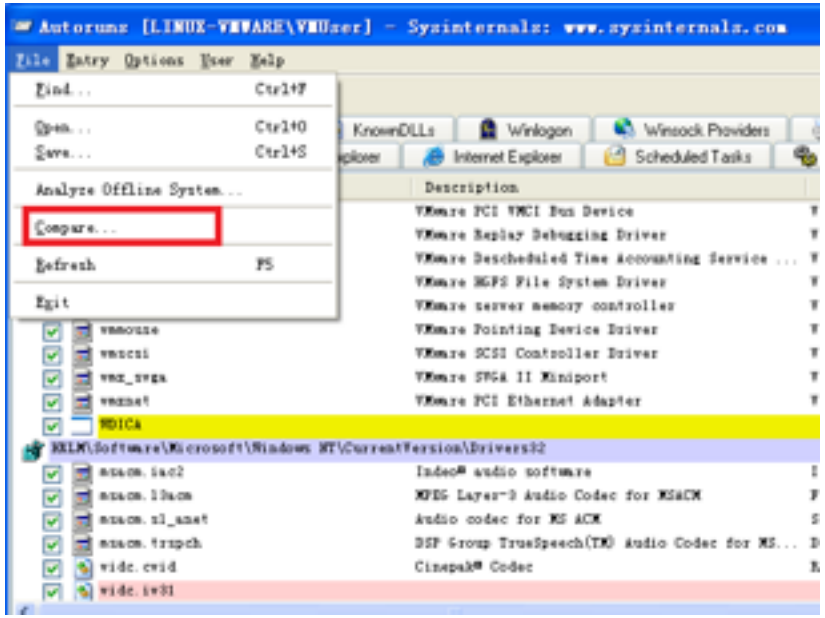
课内实验

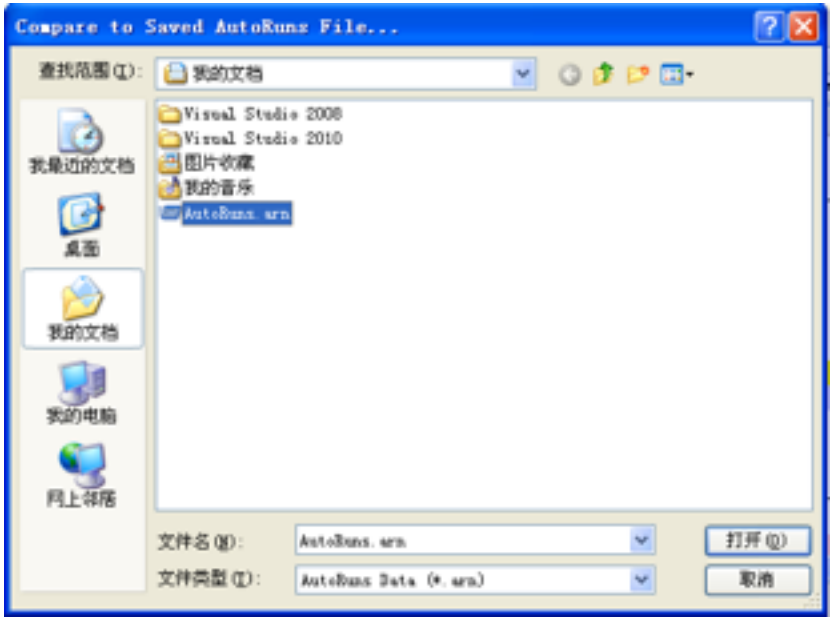
- 该驱动程序未通过验证，右键“删除”



课内实验

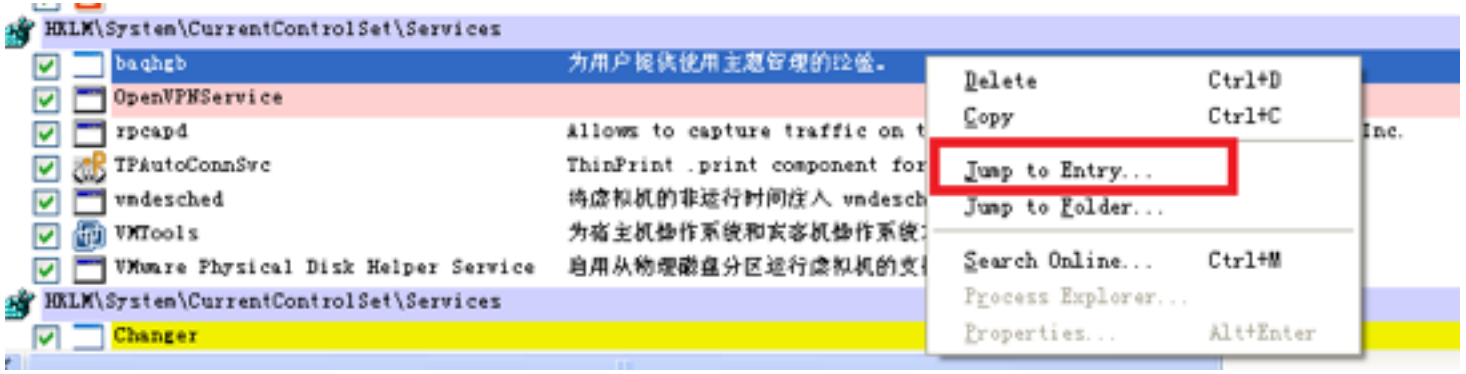
- 文件比较，选择之前保存的日志文件，查看启动项的变化

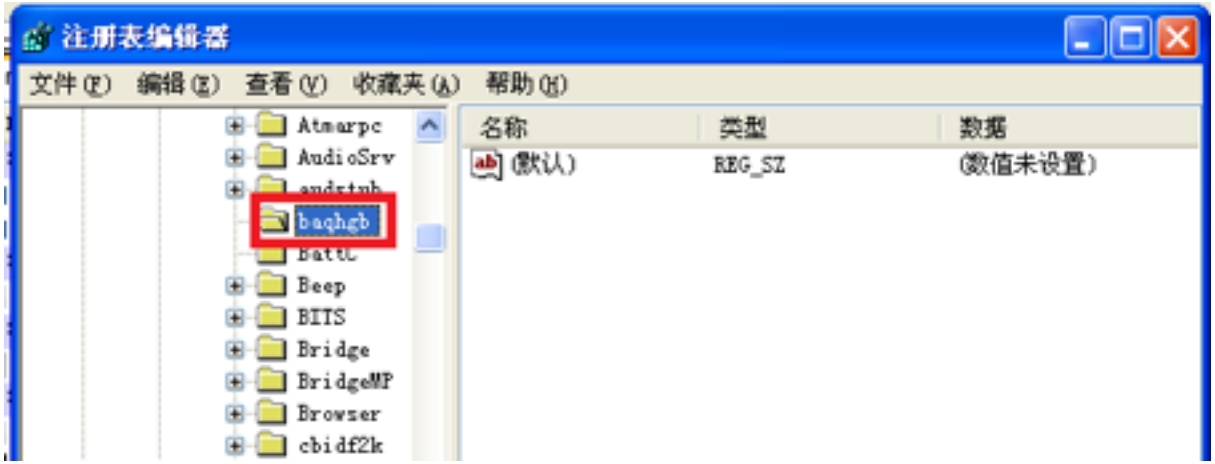




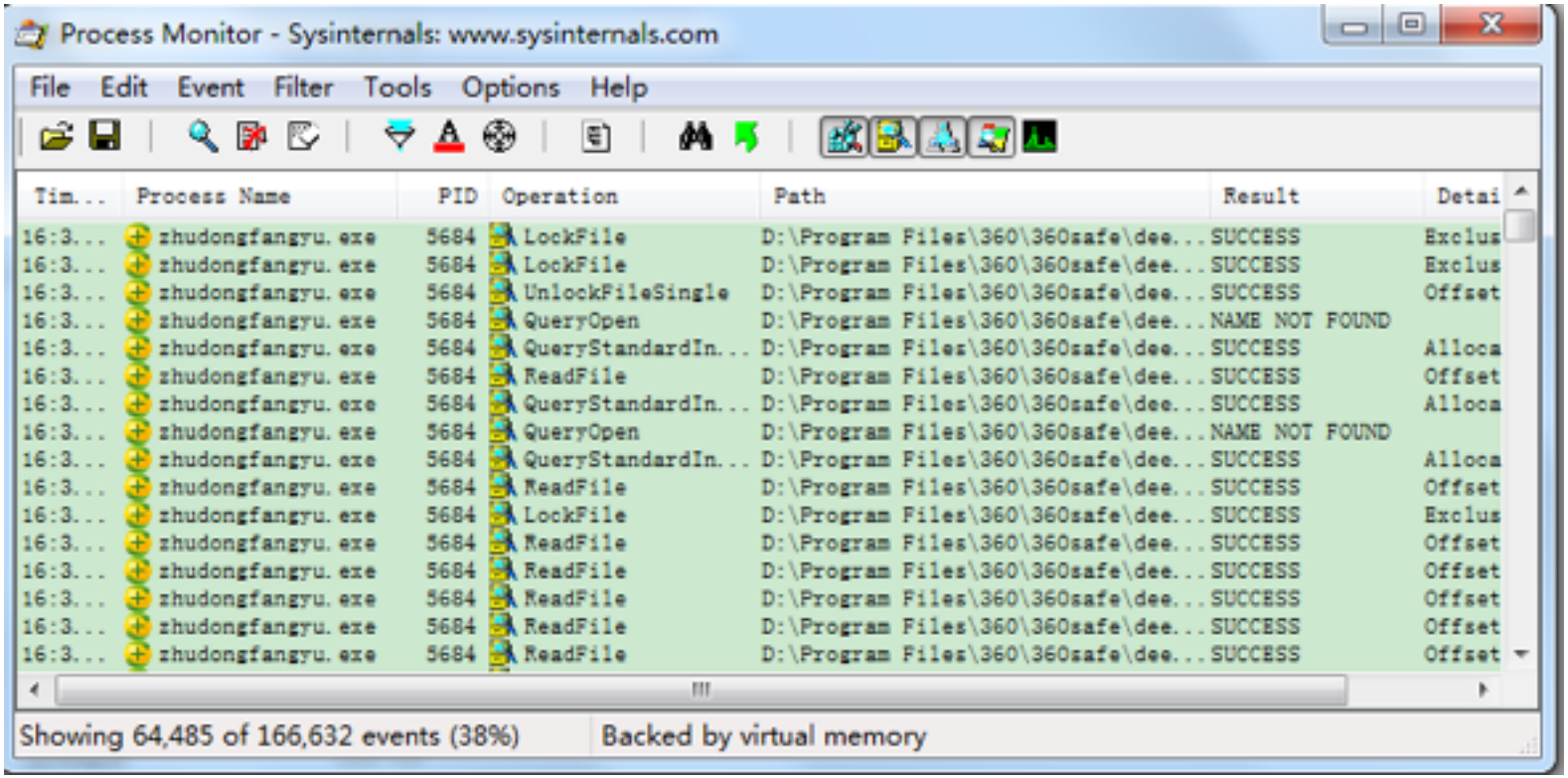
课内实验

- 通过跳转到功能查看注册表项





- 实验二 sysinternals工具使用—Process Monitor

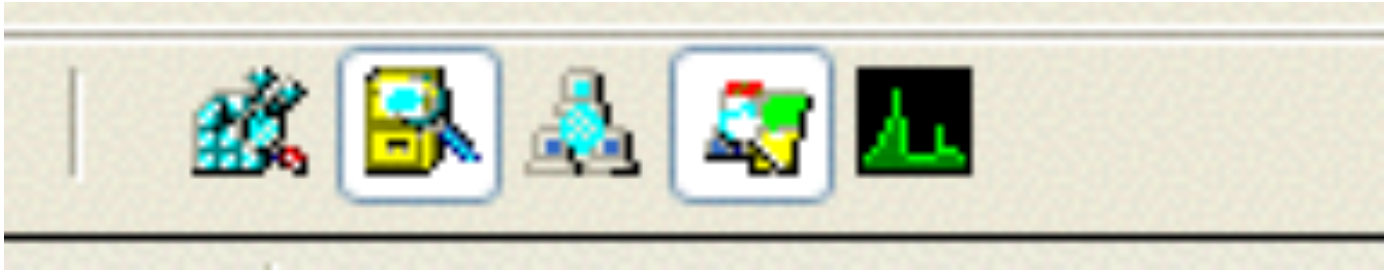



查看进程的注册表活动


查看进程和线程活动

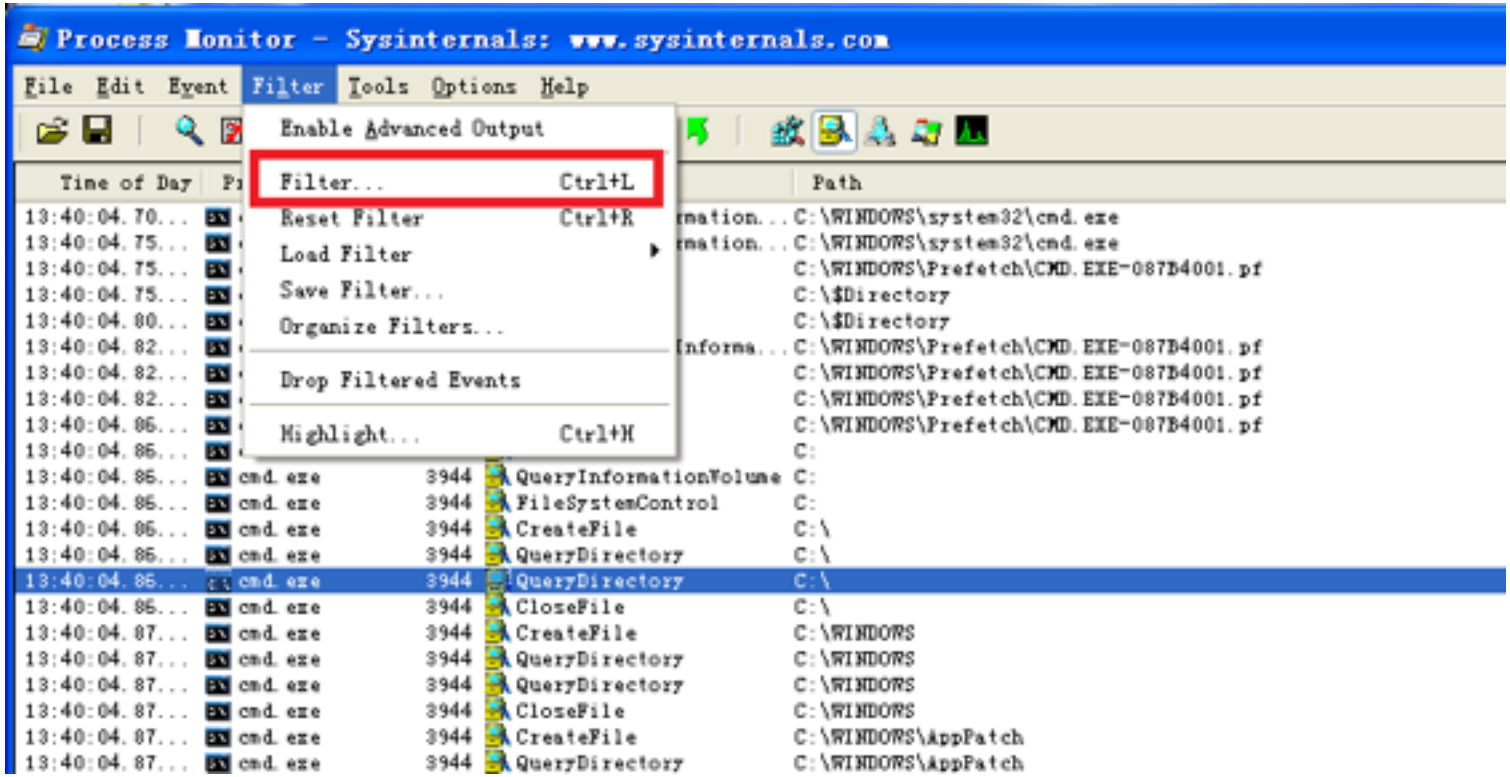

查看进程的网络活动


查看进程的文件活动

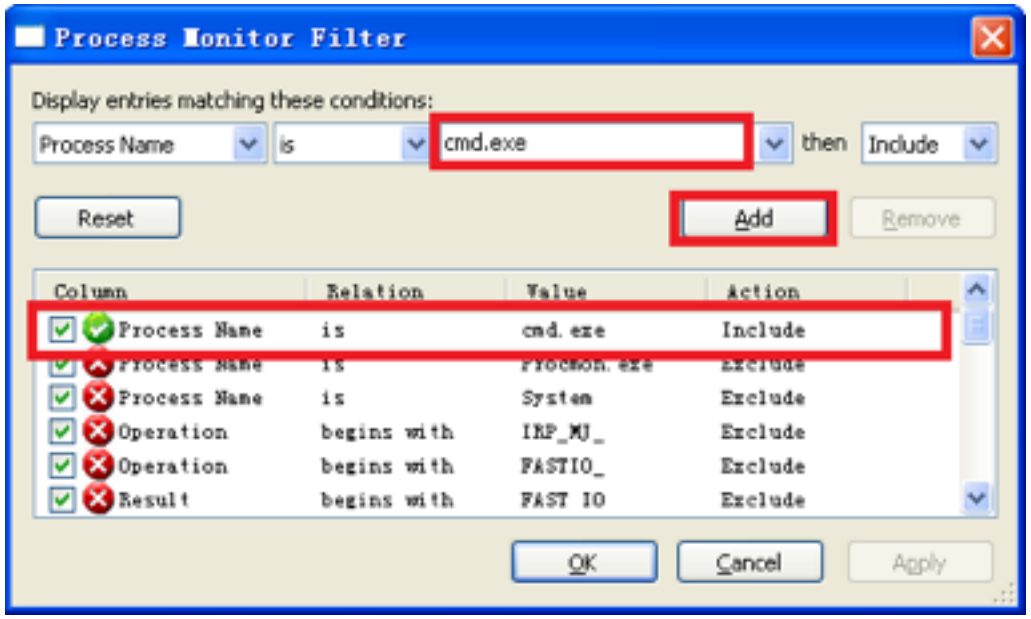


课内实验

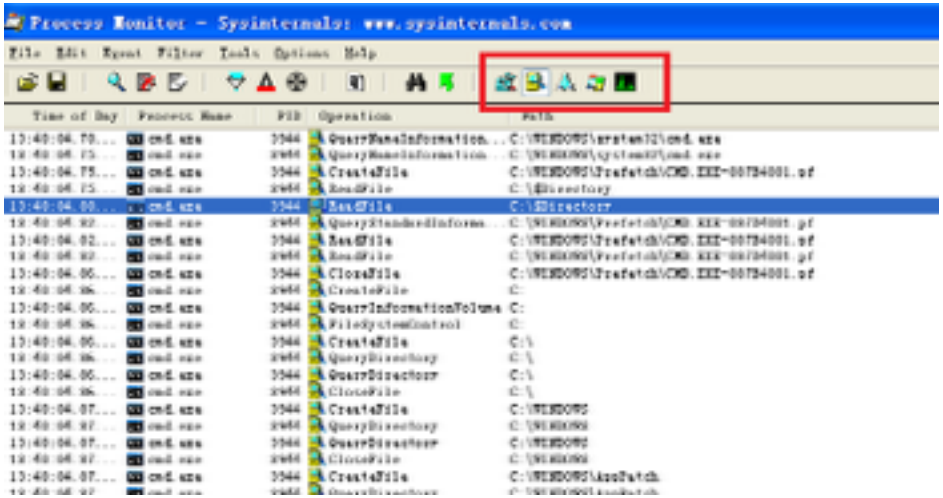
- Cmd.exe进程作为实验目标，通过过滤器只设置查看该进程

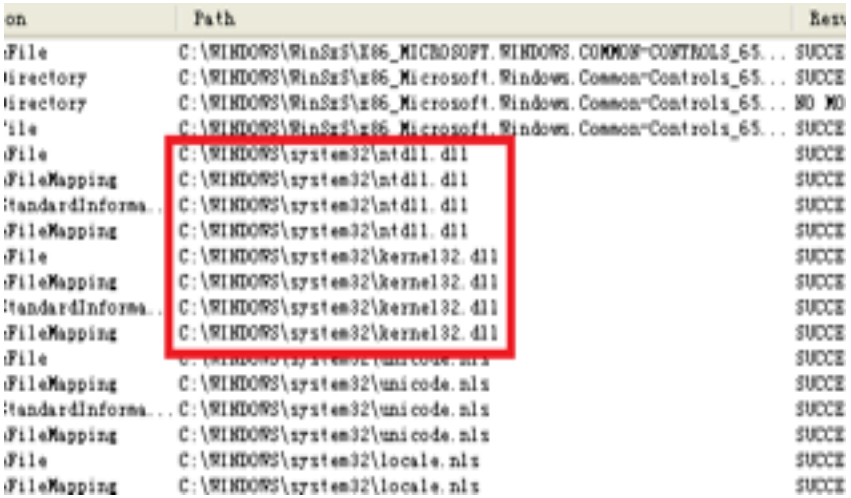


- 在过滤器中添加过滤条件，进程名为cmd.exe,点击“add”包含到过滤条件中



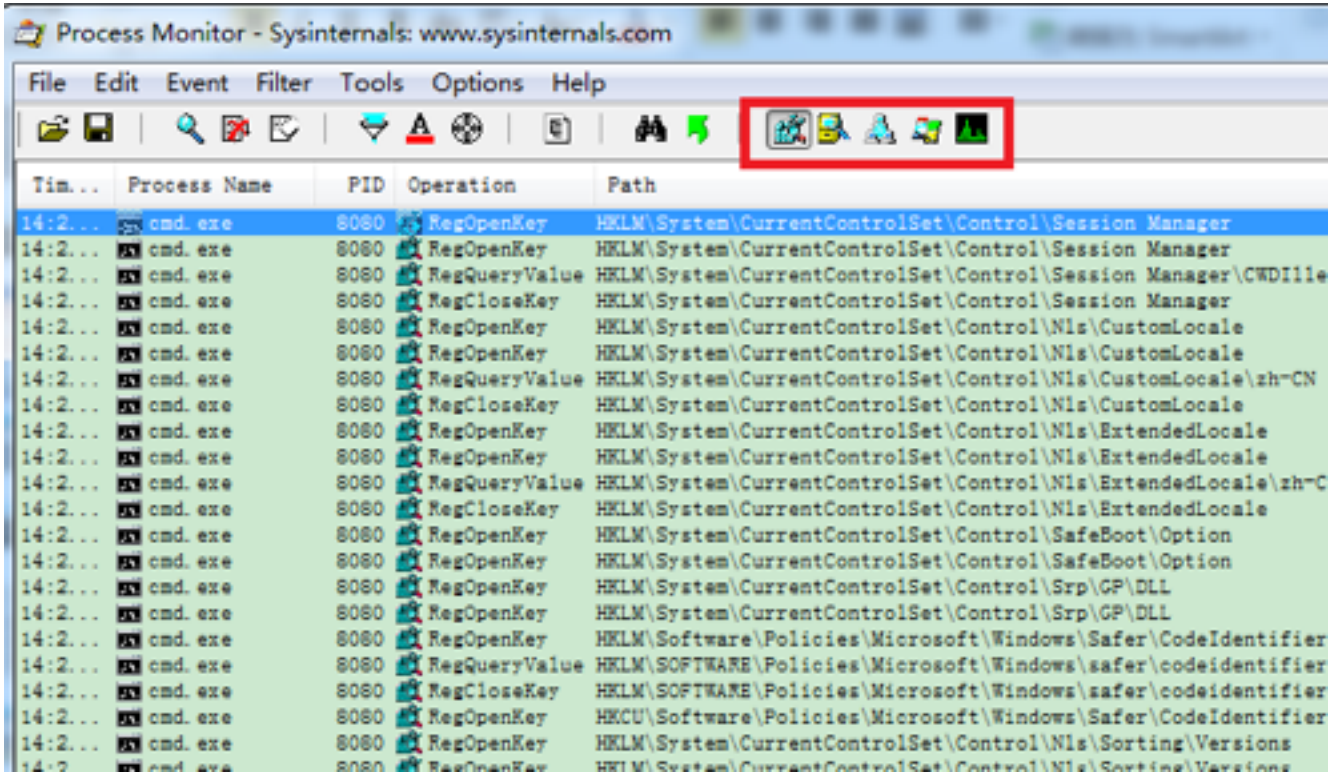
- 查看的筛选条件设置为只查看文件活动，可以看到该进程调用的库文件或其他调用的文件



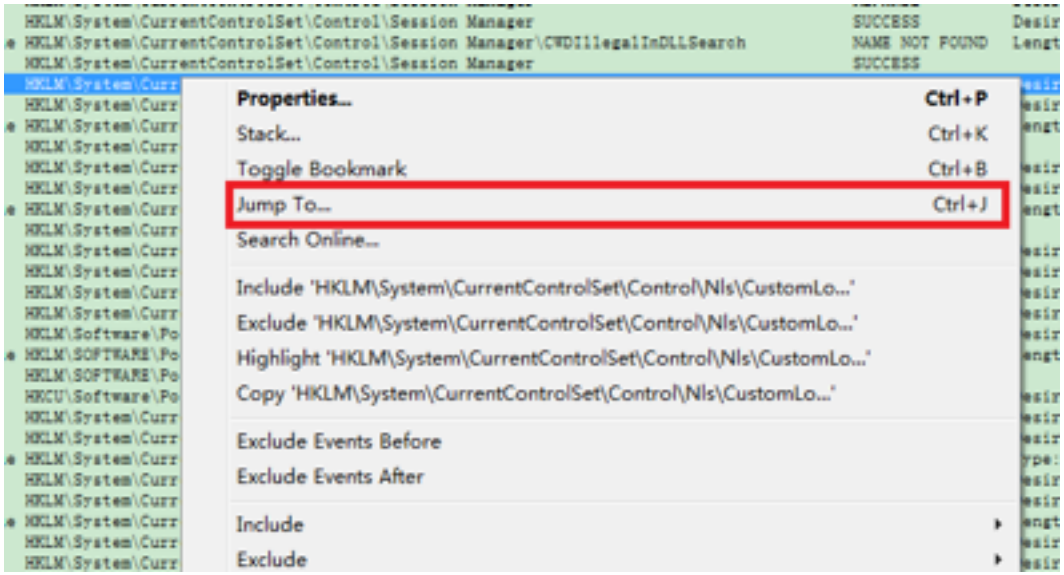


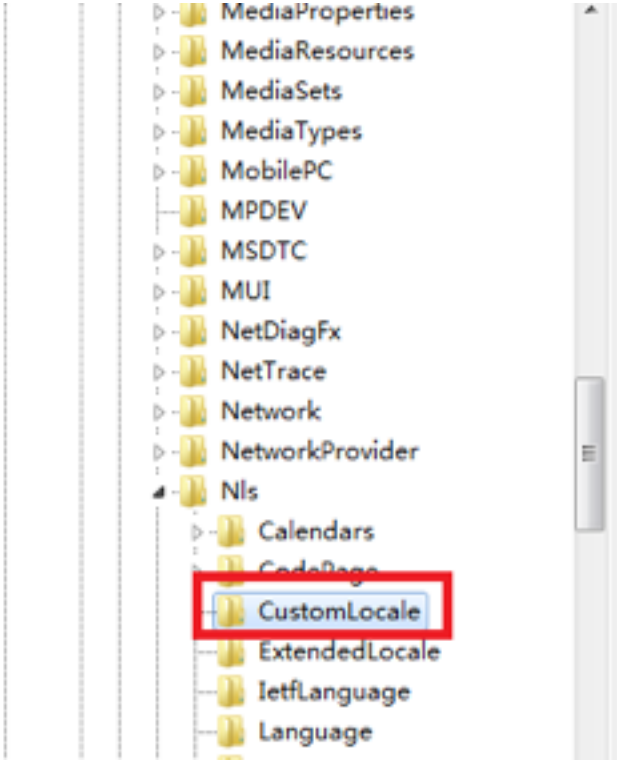
课内实验

- 修改筛选条件为查看注册表活动

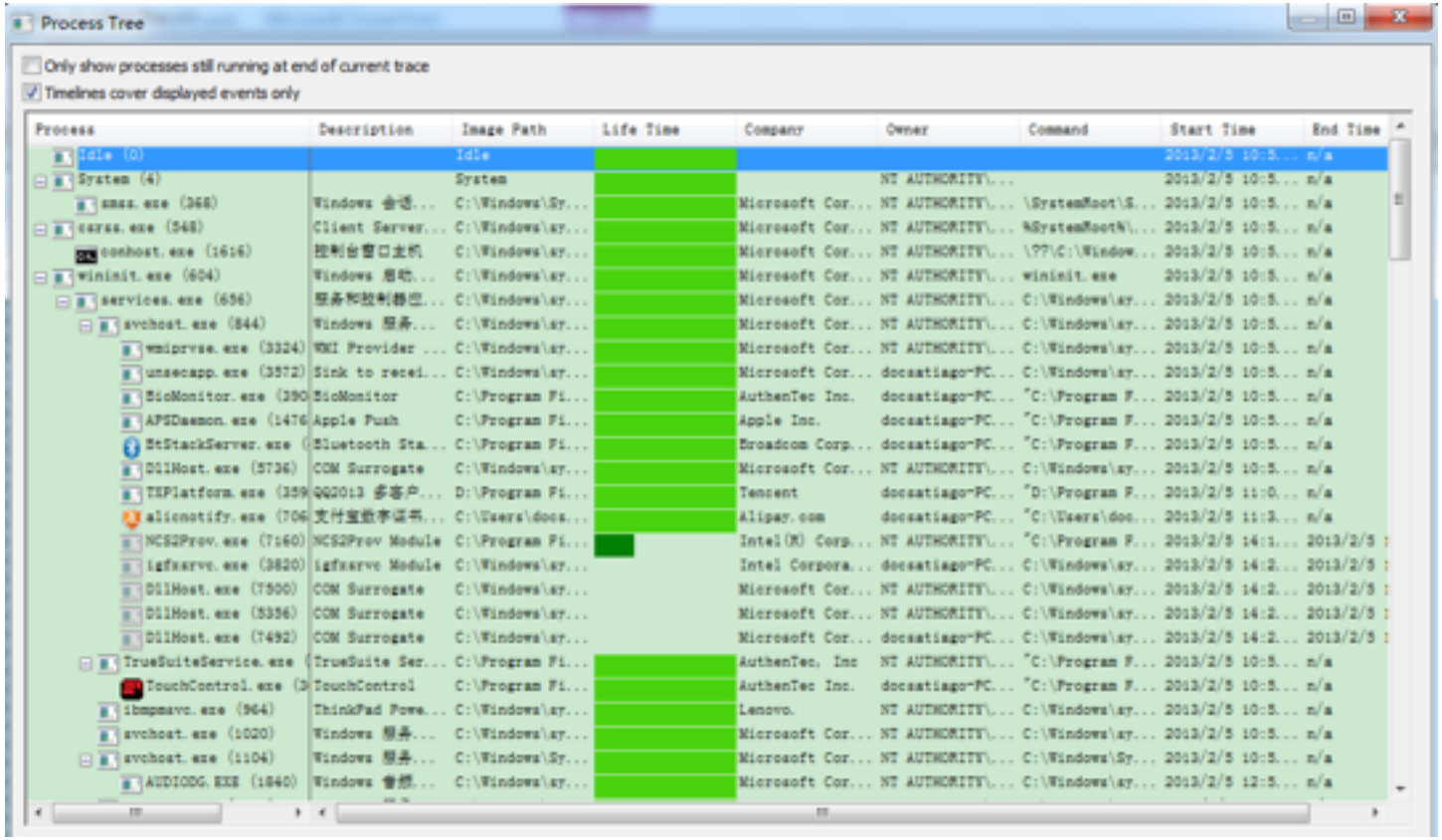


- 选择相应的注册表项，可以直接跳转到编辑器





- Process Tree 查看进程和子进程



课后实验

- 使用ProcMon研究记事本程序从打开到编辑文字到最后保存文件到文件系统，整个过程的内部执行流程和细节
  - —执行了哪些文件系统访问操作?
  - —是否有注册表访问操作?
  - —是否有网络访问行为?
  - —如果是第三方文本编辑软件呢?
    - 会有网络访问行为吗？为什么要联网？联网干了些什么?

课后实验

- 实验准备：
  - 在桌面上新建一个目录：dir
  - 创建dir的目录符号链接dir1
  - 创建dir的目录联接dir2
- 实验问题：
  - 如果仅移动dir到其他目录，dir1和dir2还能访问到dir吗？
  - 如果同时移动dir、dir1和dir2到一个新的目录下，dir1和dir2还能访问到dir吗？
  - Windows 7上有哪些目录分别用到了目录符号链接技术和目录联接技术？举例说明