

Windows 平台下的监控取证技术

作者：泉哥

主页：<http://riusksk.blogbus.com>

前言

监控取证技术大多被国家政府公安部门采用的技术，主要用于针对计算机犯罪而进行取证，以此确保人民信息安全。当然对于我们一般的平民，掌握一定的取证技术也可以很好采取反监控技术，以防止我们的个人隐私泄露，造成不必要的损失。但监控取证技术的范围很广，本专题主要针对 windows 平台下的监控取证技术进行简要分析，希望大家能有所得。

一.NTFS 属性

NTFS (New Technology File System)是 [Windows](#) NT 操作环境和 Windows NT 高级[服务器](#)网络操作系统环境的[文件系统](#).NTFS 的目标是提供：可靠性，通过可恢复能力(事件跟踪)和热定位的容错特征实现；增加功能性的一个平台；对 [POSIX](#) 需求的支持；消除 [FAT](#) 和 [HPFS](#) 文件系统限制。NTFS 提供长文件名、数据保护和恢复，并通过[目录](#)和[文件](#)许可实现安全性。NTFS 支持大[硬盘](#)和在多个硬盘上存储文件(称为跨越分区)。例如，一个大公司的数据库可能大得必须跨越不同的硬盘。NTFS 提供内置安全性特征，它控制文件的隶属关系和访问。从 [DOS](#) 或其他[操作系统](#)上不能直接访问 NTFS 分区上的文件。如果要在 DOS 下读写 NTFS 分区文件的话可以借助第三方软件；现如今，[Linux](#) 系统上已可以使用 [NTFS-3G](#) 进行对 NTFS 分区的完美读写，不必担心数据丢失。这是 Windows NT 安全性系统的一部分，但是，只有在使用 NTFS 时才是这样。

说白了，NTFS 就是一种文件系统，而非文件格式，FAT16，FAT32 均是如此。你查看一下磁盘的属性就可查看是何种文件系统了，如图

1:



图 1

在 NTFS 文件系统中，文件亦是按簇进行分配的，文件通过主文件表 MFT（Master File Table）来确定其在磁盘上的存储位置、大小、属性等信息。每个文件都有一个文件记录（File Record）数据结构，其中第一个记录就是 MFT 自己本身。MFT 结构如图 2，3 所示：

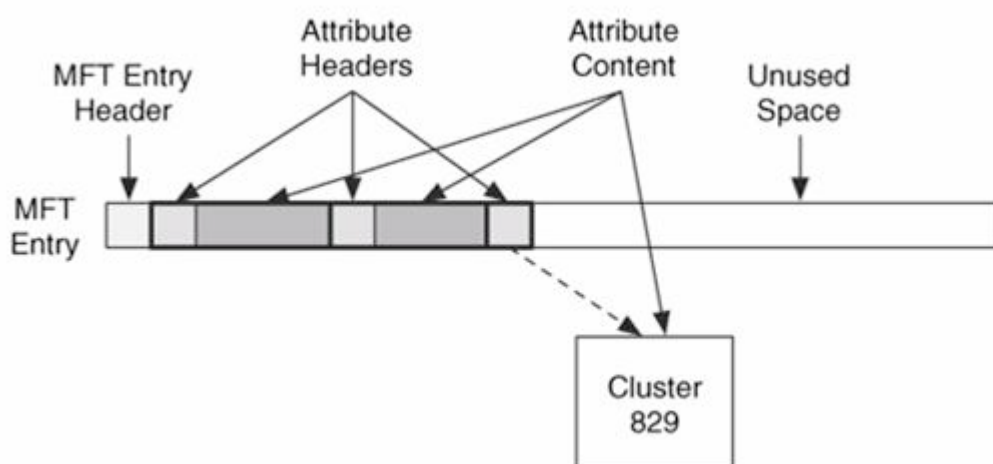


图 2

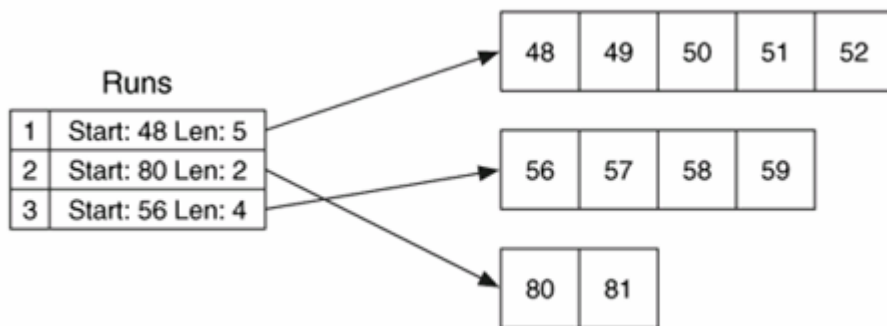


图 3

关于 MFT 更详细的资料可参考《NTFS 中的 \$MFT 详解》一文：

http://hi.baidu.com/sc_wolf/blog/item/e3f6d35cb063b345faf2c05b.html

下面是 FILE Record 的结构：

Offset	Size	Description
0x00	4	Magic number 'FILE' //标志，一定是“FILE”
0x04	2	Offset to the update sequence //更新序列 US 的偏移
0x06	2	Size in words of Update Sequence Number & Array (S) //更新序列号 USN 的大小与数组，包括第一个字节
0x08	8	\$LogFile Sequence Number (LSN) // 日志文件序列号 LSN
0x10	2	Sequence number //序列号 (SN)
0x12	2	Hard link count //硬连接数
0x14	2	Offset to Update Sequence Array // 第一个属性的偏移地址
0x16	2	Flags //标志，1 表示记录正在使用，2 表示该记录为目录
0x18	4	Real size of the FILE record //记录头和属性的总长度，即文件记录的实际长度
0x1C	4	Allocated size of the FILE record //总共分配给记录的长度
0x20	8	File reference to the base FILE record //基本文件记录中的文件索引号
0x28	2	Next Attribute Id //下一属性 ID
0x2A	2	Align to 4 byte boundary //XP 中使用，边界

0x2C 4 Number of this MFT Record //XP 中使用，本文件记录号

2 Update Sequence Number (a) //更新序列号，大小为 2B，是为了保证该扇区是否正确，以扇区的最后

两个字节与该值比较，如果一样，则说明该扇区是正确的，否则就是有问题。

2S-2 Update Sequence Array (a) //更新序列数组，大小一般为 $2 \times 2B = 4B$ ，如果该扇区正确，在解析的时候，

则将该数组中的两个 2B 大小的数字依次复制到该 File Record 所在的两个扇区的最后两个字节。

在日志文件 \$LogFile 中包含所有文件系统操作日志，删除文件会在 \$LogFile 中留有记录，因此找到一些不在磁盘上的文件是完全有可能的，在 \$LogFile 上还可以找到一些被系统调用过的文件。在 NTFS 中包含四个时间戳：创建时间，最后访问时间，最后写入时间以及最后修改时间，因此能过它我们可以查看我们的秘密文件是否被复制，查看等操作。刚好这里在网上找到一篇关于 NTFS 分区格式化数据恢复的文件，有兴趣的可以看下：

NTFS 分区格式化后用 WINHEX 手工提取数据：<http://blog.intohard.com/html/44/t-46244.html>

二. 注册文件

注册文件 *.reg 文件是一种注册表脚本文件，通过它将数据导入注册表中，以此来操作注册表，因此在该文件中包含有各类软件、硬件、用户的相关信息及设置。在注册表包含有一组主键或根键（HKEY）、键（key）、子键(subkey)、键值(value)，通过它可以进行数据备份。在 win98 中，注册文件命名为 user.dat 与 system.dat；在 windows millennium edition 中则为 classes.dat, user.dat 和 system.dat；而在 2000\xp 及 vista 中是在 C:\windows\system32\config 文件。通过查看备份的数据可以获得一些已删除文件或程序的相关信息，对于取证有一定的帮助。另外能过注册表还可以用于确定用户进行了哪些操作，比如攻击者经常要运行一些指令，而且经常是通过启动->运行.....然后输入需要运行的程序名，接着启动程序或指令。而在 windows 中就记录了大部分注册表中当前用户通过该方式执行的最近 26 条指令，只需查看 HKCU、Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU 这里举个实例，先用启动->运行->输入 regedit，然后查看以上键值，结果如图 4 所示：

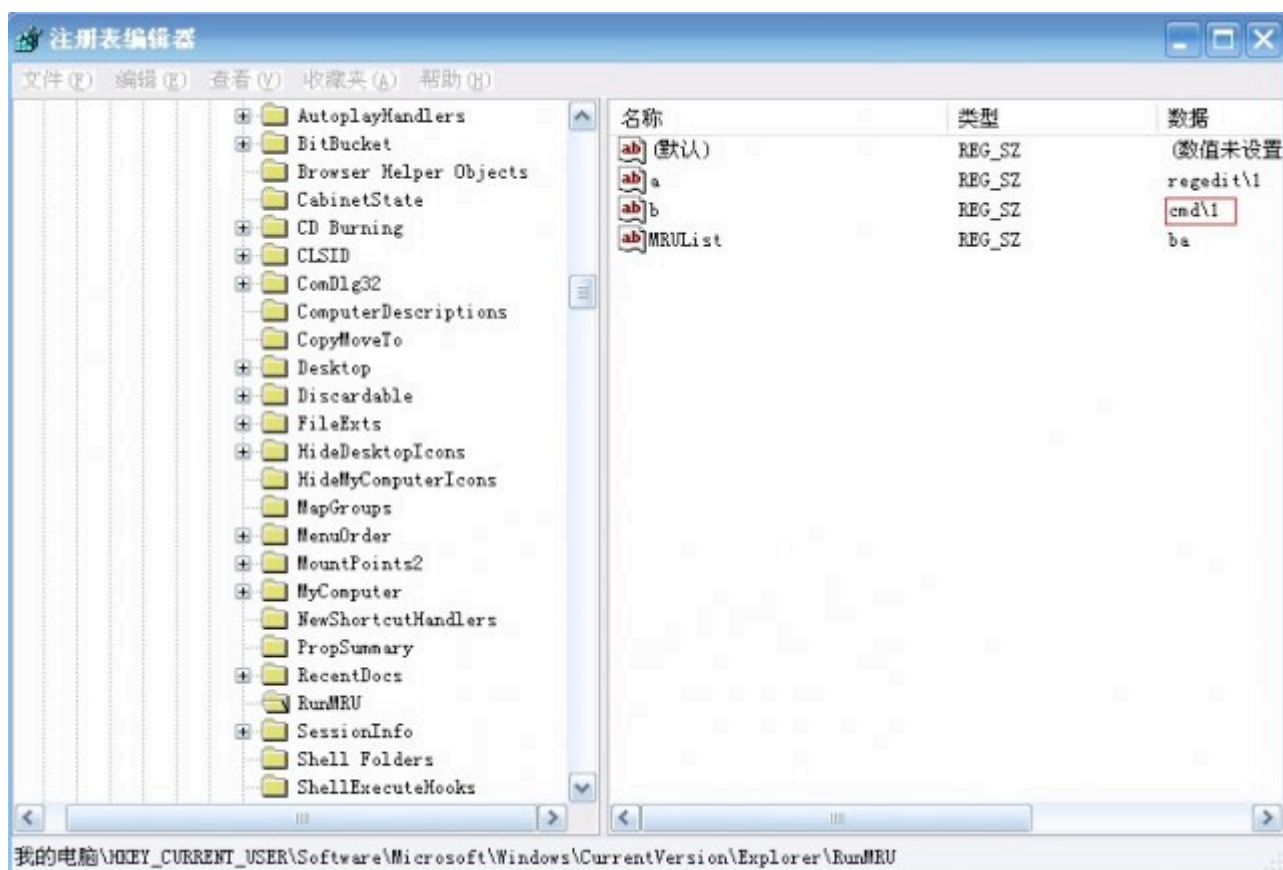


图 4

另外还有一个地方可以用来查看当前用户最近打开的文件名：HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs 如图 5 所示：

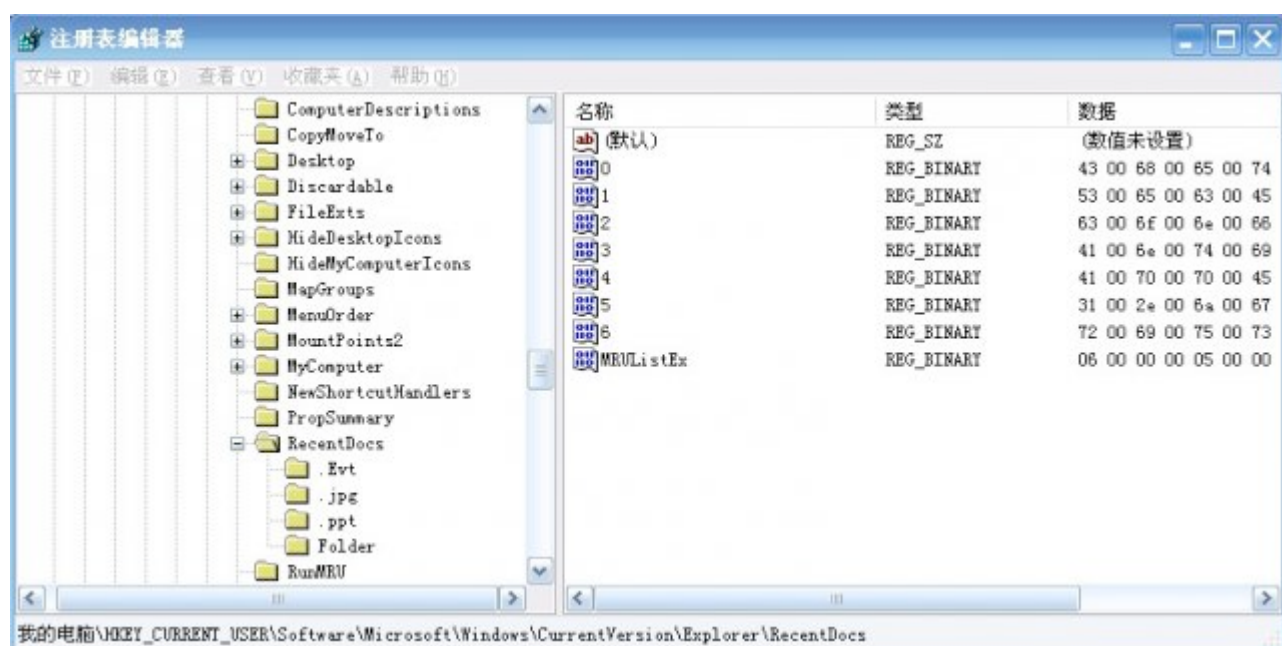


图 5

除此之外，还有 `hkcu\software\microsoft\internet explorer\typedurls` 可以查看所有 IE 中 URL，

`hkcu\software\realvnc\vncviewer4\mru` 可以查看黑客进入到的系统的历史记录。在《[mining digital evidence in microsoft windows](#)》一文中提到注册表中包含下列事件：

system and user-specific settings

UserAssist

MuiCache

MRU Lists

ProgramsCache

StreamMRU

Shellbags Usbstor

IE passwords

and many more!

- 三. 预读取文件 **prefetch file (*.pf)**

MS 在 WinXP 以后的操作系统中加入了预读取文件的功能，用于提高系统启动，程序加载及文件读取的速度。通过缓存正在被使用的程序，可以帮助系统分配用户可能即将访问的系统资源，以此来提高访问速度。预读取文件保存在 `c:\windows\Prefetch` 目录中，每个应用程序都会在 `Prefetch` 目录中留下相应的预读取文件，预读取文件描述了应用程序或系统启动时各个模块的装载顺序，其命名方式是以应用程序的可执行文件名为基础，加上一个“-”和描述执行文件完整路径的十六进制值，再加上文件扩展名 **PF** 构成的，例如 `opera.exe-0065A2A1.pf`。不过，windows XP 启动的预读取文件总是同一个名称，即 `NTOSBOOT-B00DFAAD.PF`，其中包含着启动

时载入文件的记录。预读取文件的功能可能过修改注册表 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\PrefetchParameters 来设置，如图 6 所示：

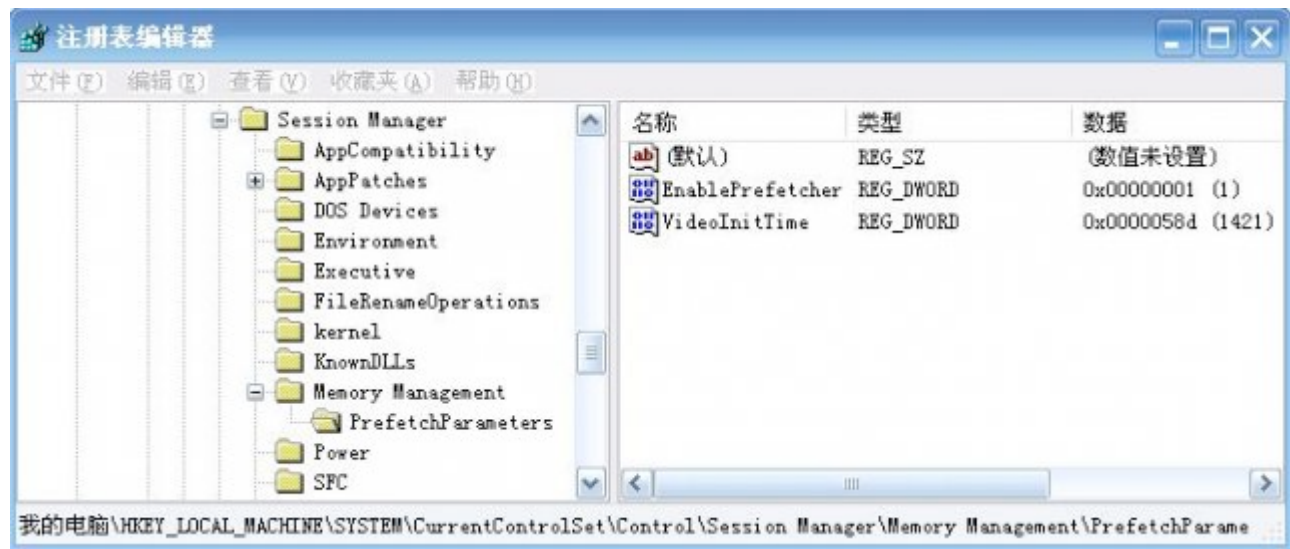


图 6

可修改 EnablePrefetcher 的“DWORD”值为：

- “0”——取消预读取功能；
- “1”——系统将只预读取应用程序；
- “2”——系统将只预读取 Windows 系统文件，此为 Windows XP/Server 2003 的默认设置；
- “3”——系统将预读取 Windows 系统文件和应用程序。

预读取文件的分析可借助 WFA（windows file analyzer）来进行，如图 7 所示：

Windows File Analyzer - [PA - Prefetch]							
File Windows Help							
PA - Prefetch							
Prefetch Analysis							
Directory: C:\WINDOWS\Prefetch							
Volume serial: 345F-A906							
Volume label:							
lication	Created	Written	Last Accessed	Embedded Date	Runs	File Path Hash	MD5
TUANESEX.EXE-070A6954.pf	2009-1-28 11:49:40	2009-1-26 9:26:54	2009-1-28 11:49:40	2009-1-26 9:26:42	1	70A6954	487455B04937DA356F4
NLOGON.EXE-32C57D49.pf	2009-1-28 11:49:40	2009-1-28 9:05:04	2009-1-28 11:49:40	2009-1-28 9:04:52	37	32C57D49	5F458C52ADA277C4F4C
WINDOW清理助手.EXE-39E246E...	2009-1-28 11:49:40	2009-1-26 14:00:32	2009-1-28 11:49:40	2009-1-26 14:00:29	1	39E246ED	0E7359FA36311C66B25
IRAR.EXE-39C6DAD9.pf	2009-1-28 11:49:40	2009-1-28 11:20:28	2009-1-28 11:49:40	2009-1-28 11:20:21	23	39C6DAD9	4130DE3C25C06717EF3
LOGINPROXY.EXE-1781D844.pf	2009-1-28 11:49:40	2009-1-28 11:39:48	2009-1-28 11:49:40	2009-1-28 11:39:36	31	1781D844	73D6A300997EC62E77E
IIADAP.EXE-2DF425B2.pf	2009-1-28 11:49:40	2009-1-28 9:09:26	2009-1-28 11:49:40	2009-1-28 9:09:15	34	2DF425B2	B3A42C74ACDA15A7A1
IIPRVSE.EXE-28F301A9.pf	2009-1-28 11:49:40	2009-1-28 11:20:30	2009-1-28 11:49:40	2009-1-28 11:20:19	74	28F301A9	F11DF0027949135E9F8
AUCLT.EXE-399A8E72.pf	2009-1-28 11:49:40	2009-1-28 9:06:16	2009-1-28 11:49:40	2009-1-28 9:06:02	36	399A8E72	1FFC5B1289B814B2896
反恐精英V1.5 硬盘版_CCTVGA...	2009-1-28 11:49:38	2009-1-26 8:30:40	2009-1-28 11:49:38	2009-1-26 8:30:29	1	1085FA23	6A6BC20C0E4E34C36D
11.EXE-11C8F411.pf	2009-1-28 11:49:40	2009-1-27 2:58:02	2009-1-28 11:49:40	2009-1-27 2:57:57	16	11C8F411	85EEE1E18812702E4AC
快打.EXE-05A32CAB.pf	2009-1-28 11:49:40	2009-1-26 9:25:16	2009-1-28 11:49:40	2009-1-26 9:25:15	4	5A32CAB	B6F091899DA3DFC5BD
兵团.EXE-2AA2CE3B.pf	2009-1-28 11:49:40	2009-1-28 11:27:02	2009-1-28 11:49:40	2009-1-28 11:26:56	28	2AA2CE3B	04A7585C78B9B0B55D0
泡泡.SCR-03CA1111.pf	2009-1-28 11:49:40	2009-1-28 11:38:02	2009-1-28 11:49:40	2009-1-28 11:37:51	2	3CA1111	9BC872407A7B047E715
files found							

图 7

通过上图可知，*.pf 文件中包含程序的最新访问时间，嵌入数据的时间，运行次数及文件路径 hash 值等信息。

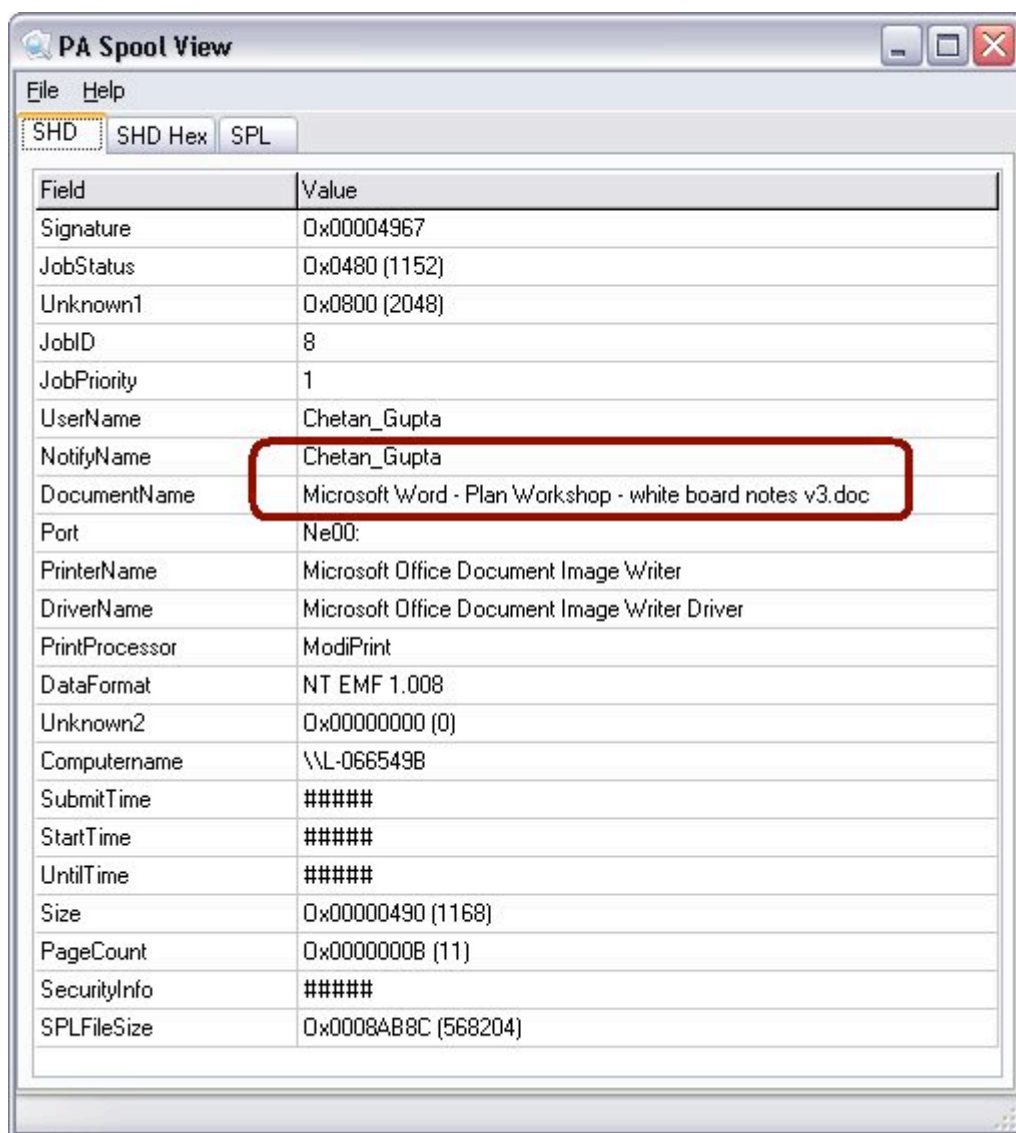
• 四. 后台打印文件(print spooler file)

在打印作业完成之后，会在 C:\Winnt\System32\Spool\Printers 目录中留下几个 SPL 和 SHD 文件。

SPL 文件是实际的后台打印（打印作业）文件。

SHD 文件提供有关的打印机打印作业已发送与其打印作业一起提供的信息。 一个 SHD 文件是"影子"文件跟踪的哪些逻辑打印机（同一号码） xxxxx.spl 文件转到。 它还包含队列，发送该的打印机和其他信息的文件在用户中的文件的顺序。 除非逻辑打印机设置否则状态，通常会删除这些文件。

可以通过 Splview.exe（<http://undocprint.printassociates.com>）来查看这类文件的元数据，如图 8 所示：



PA Spool View

File Help

SHD SHD Hex SPL

Field	Value
Signature	0x00004967
JobStatus	0x0480 (1152)
Unknown1	0x0800 (2048)
JobID	8
JobPriority	1
UserName	Chetan_Gupta
NotifyName	Chetan_Gupta
DocumentName	Microsoft Word - Plan Workshop - white board notes v3.doc
Port	Ne00:
PrinterName	Microsoft Office Document Image Writer
DriverName	Microsoft Office Document Image Writer Driver
PrintProcessor	ModiPrint
DataFormat	NT EMF 1.008
Unknown2	0x00000000 (0)
Computername	\\L-066549B
SubmitTime	#####
StartTime	#####
UntilTime	#####
Size	0x00000490 (1168)
PageCount	0x0000000B (11)
SecurityInfo	#####
SPLFileSize	0x0008AB8C (568204)

图 8

也可通过 EMF Spool viewer (<http://www.codeproject.com/dotnet/EMFSpoolViewer/EMFSpoolViewer.zip>) 来查看实际的后台打印工作，如图 9 所示：

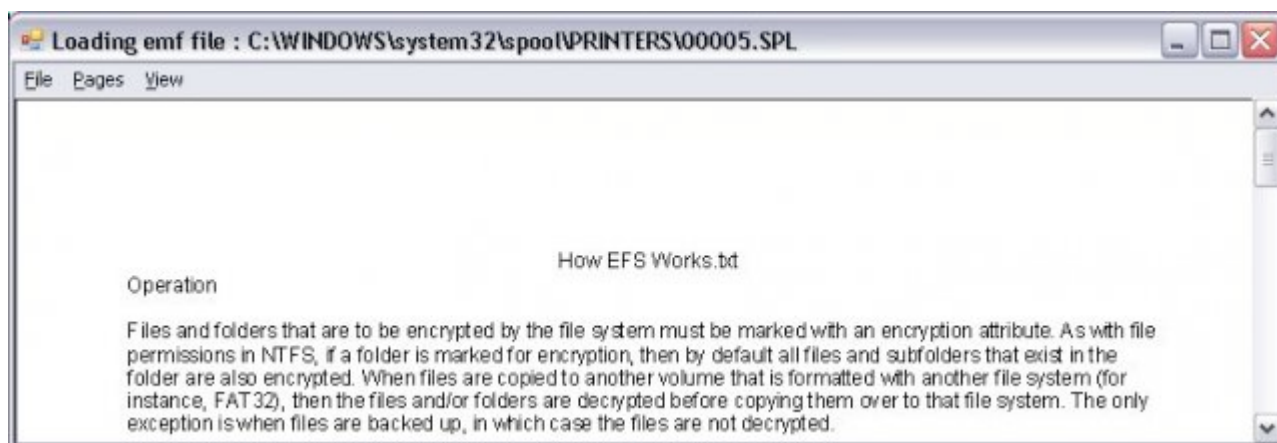


图 9

• 五. info2 文件

info2 文件中记录着每个被删除后放入回收站的文件的相应信息,比如驱动器指示器 **dirve designator** ,原删除文件的完整文件名,文件大小,存放的位置(路径)以及文件被移到回收站的时间。当一文件被移动到回收站时,该文件被重命名为:

D%DriveLetter%_%IndexNumber%_%FileExtension%.

D%DriveLetter%:

“D”代表 Drive, %DriveLetter%为文件放置的磁盘,第一磁盘均有其自己的 Recycler 目录以及 info2 文件。

%IndexNumber%:

每一被放入回收站的文件或文件夹均会被分配一索引号,用来标记删除次序,索引号越大,说明越晚删除。但当回收站清空或系统重启时,索引号将会从新开始分配。

%FileExtension%:

原始文件的扩展名。当一文件夹被删除时,它将没有扩展名。

例如:

一个文件名为 hacker.txt 被删除而放入回收站后，该文件将会被重命名为 Dc2.txt，文件入口可在 C:\Recycler\%SID%\INFO2 文件中找到。

关于 INFO2 文件结构可参考下图(来源: www.cybersecurityinstitute.biz):

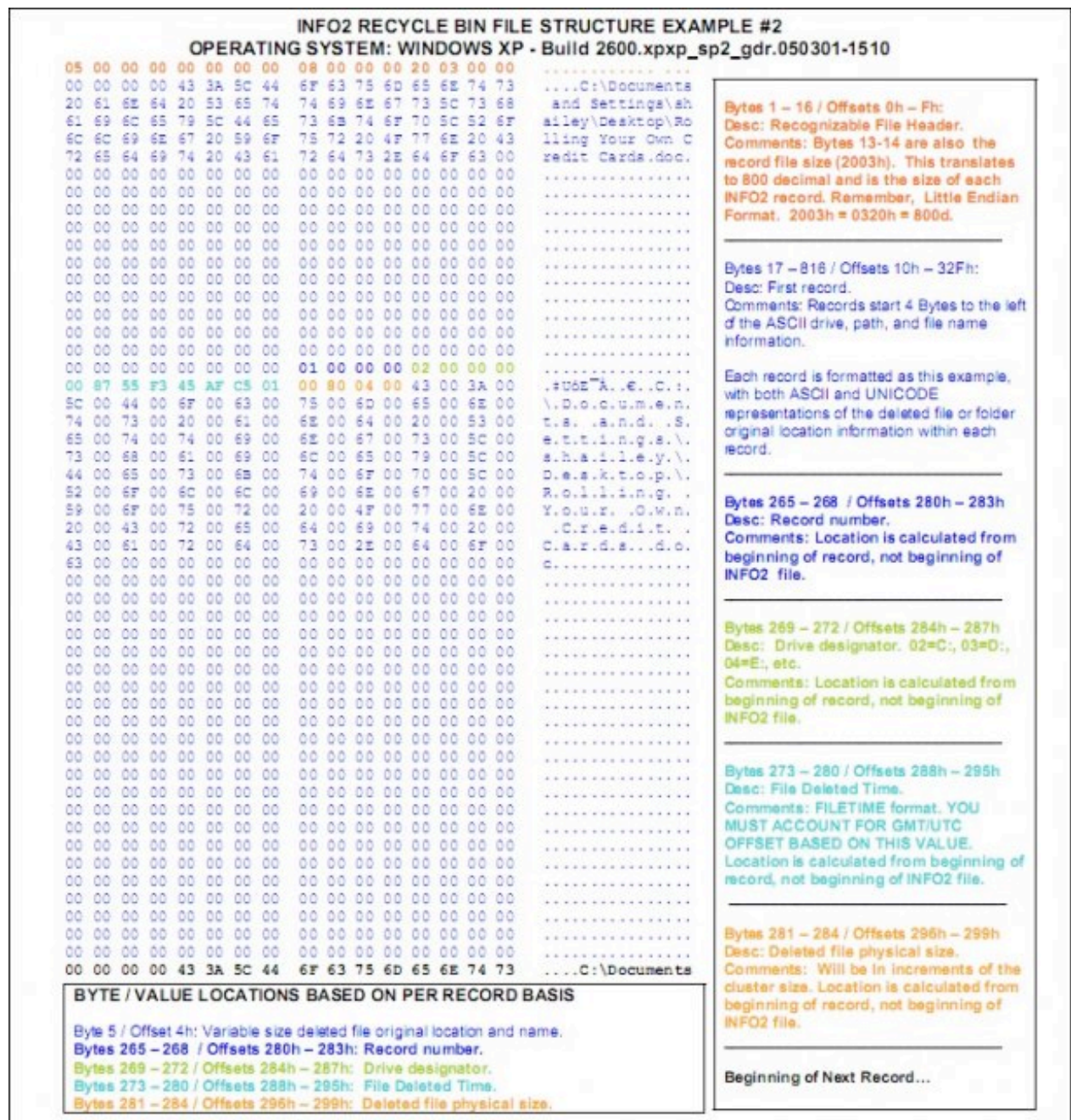


图 10

六. thumbs.db 文件

thumbs.db 文件是用于缓存文件中的缩略图，以提高图片的读取速度，它保存在每个包含图片的目录中，里面保存了这个目录下所有图像文件的缩略图(格式为 jpeg)，相当于一个缩略图数据库，当以缩略图查看图片时，就会生成一个 Thumbs.db 文件。OLE（Object Linking and Embedding：对象连接与嵌入，是在一个文件或一个程序中能够包含多种不同数据格式的数据内容而产生的）就在 thumbs.db 文件中嵌入当前数据。在一些情况下，当图片从目录中被删除后，图片仍然保存在 thumbs.db 缓存中，因此该文件也存在一定的安全风险。下面引用百度百科上的一个例子：

比如当你上传电脑的数码[相片](#)，在查看时，删除了其中的一张“SSA2501”，再将其后的“SSA2502”改成了“SSA2501”，看，“SSA2502”的照片立刻换成了“SSA2501”的照片，不只是名字换了，照片也变了。如果再将“SSA2503”的名字重命名成“SSA2502”，奇迹发生了，原来的“SSA2502”照片又回来了，“SSA2503”的照片不见了！

在 Windows XP/2003 中，用户可以通过以下操作来关闭它，如图 11 所示：

- 1 .打开工具栏——文件夹选项
- 2 .点击查看
- 3 .打勾，不缓存缩略图
- 4 .确定

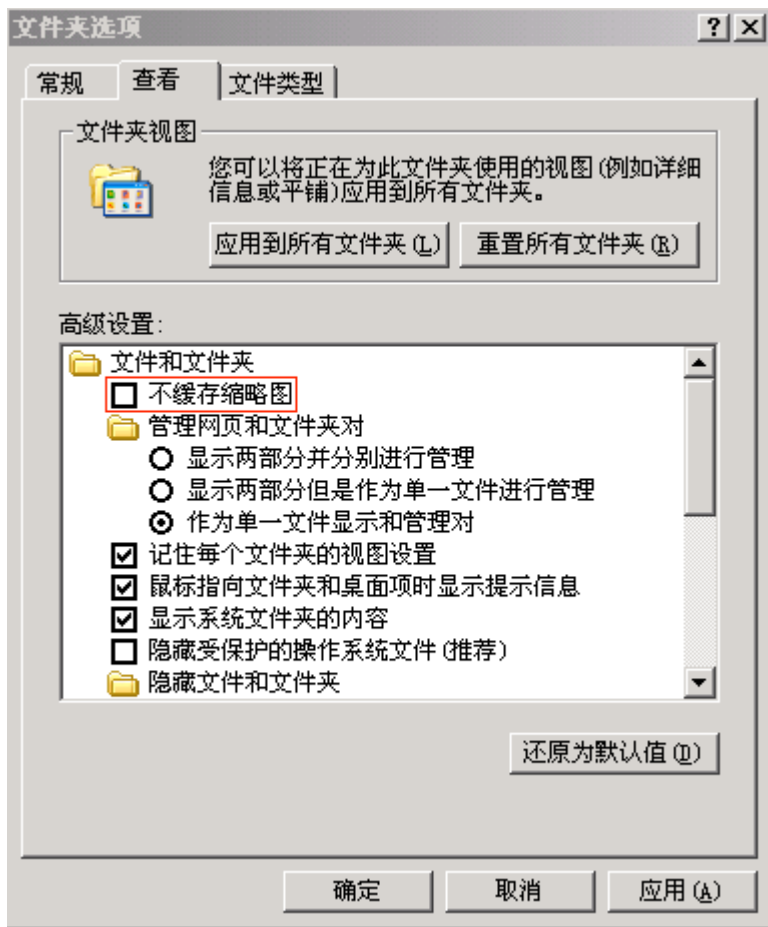


图 11

但在 windows vista 中,微软取消了 thumbs.db 文件, 而是使用把缩略图数据库" thumbcache_xxxx.db "文件集中保存于
\\Users\\[user name]\\AppData\\Local\\Microsoft\\Windows\\Explorer 该目录中。

如果你想查看 thumbs.db 文件中缓存的图片, 那么可以借助 windows file analyzer 来查看, 如图 12 所示:

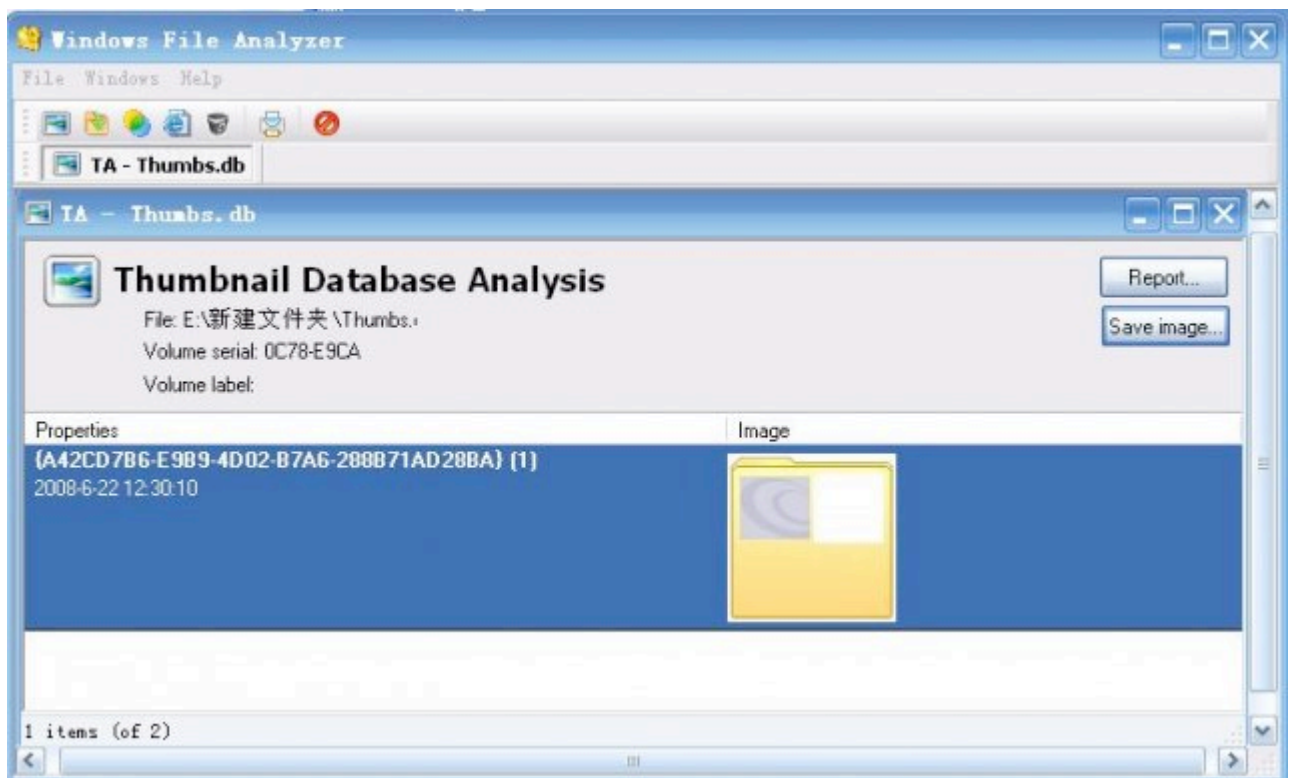


图 12

接下来直接点“save image”保存图片即可。也可采用司法分析软件 FTK 进行查看，如图 13 所示：

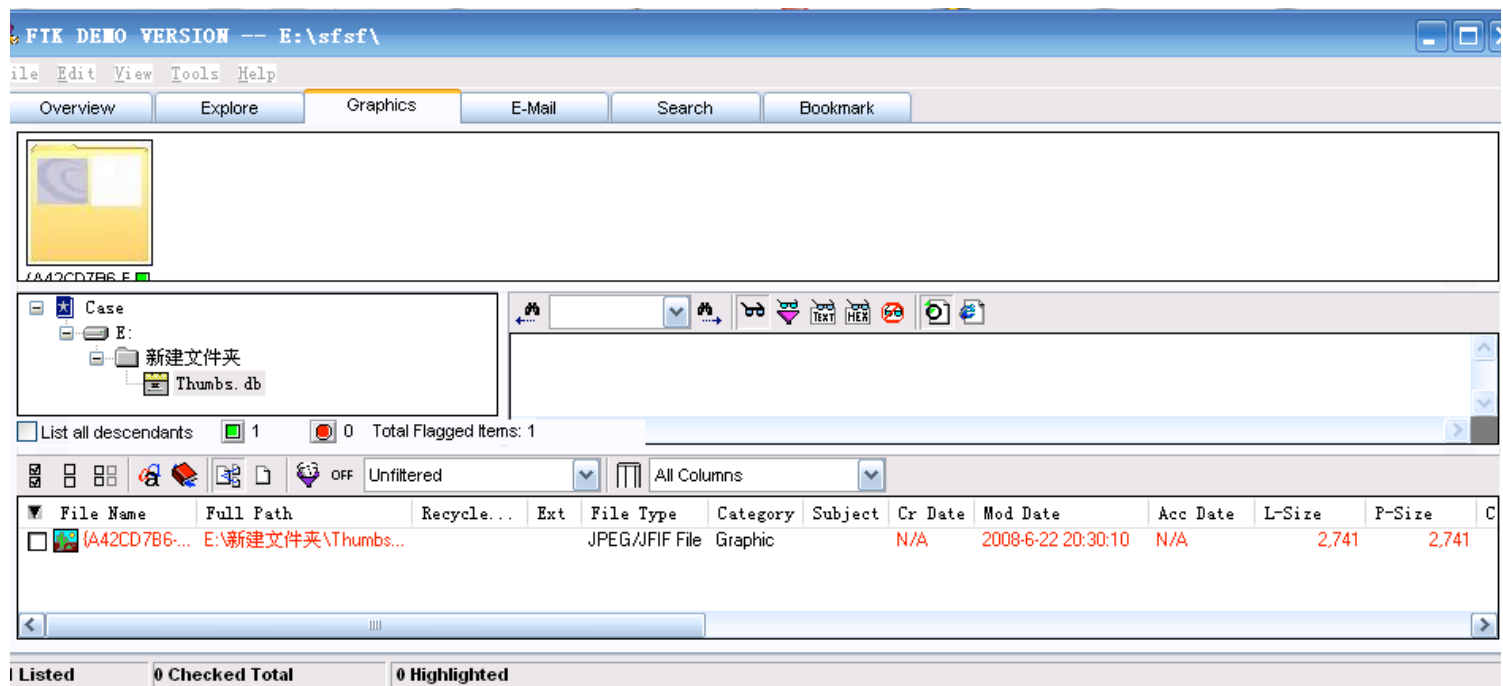


图 13

• 七. 日志文件 (*.evt)

windows 系统中的日志文件提供了系统中发生的重要事件，再结合注册表数据可用于追踪之前发生的系统事件，它主要有三种形式：应用程序，系统，安全性，通过打开开始菜单>运行,输入 Eventvwr.msc 或打开开始>控制面板>管理工具>事件查看器即可查看相关的日志文件，如图 14 所示：

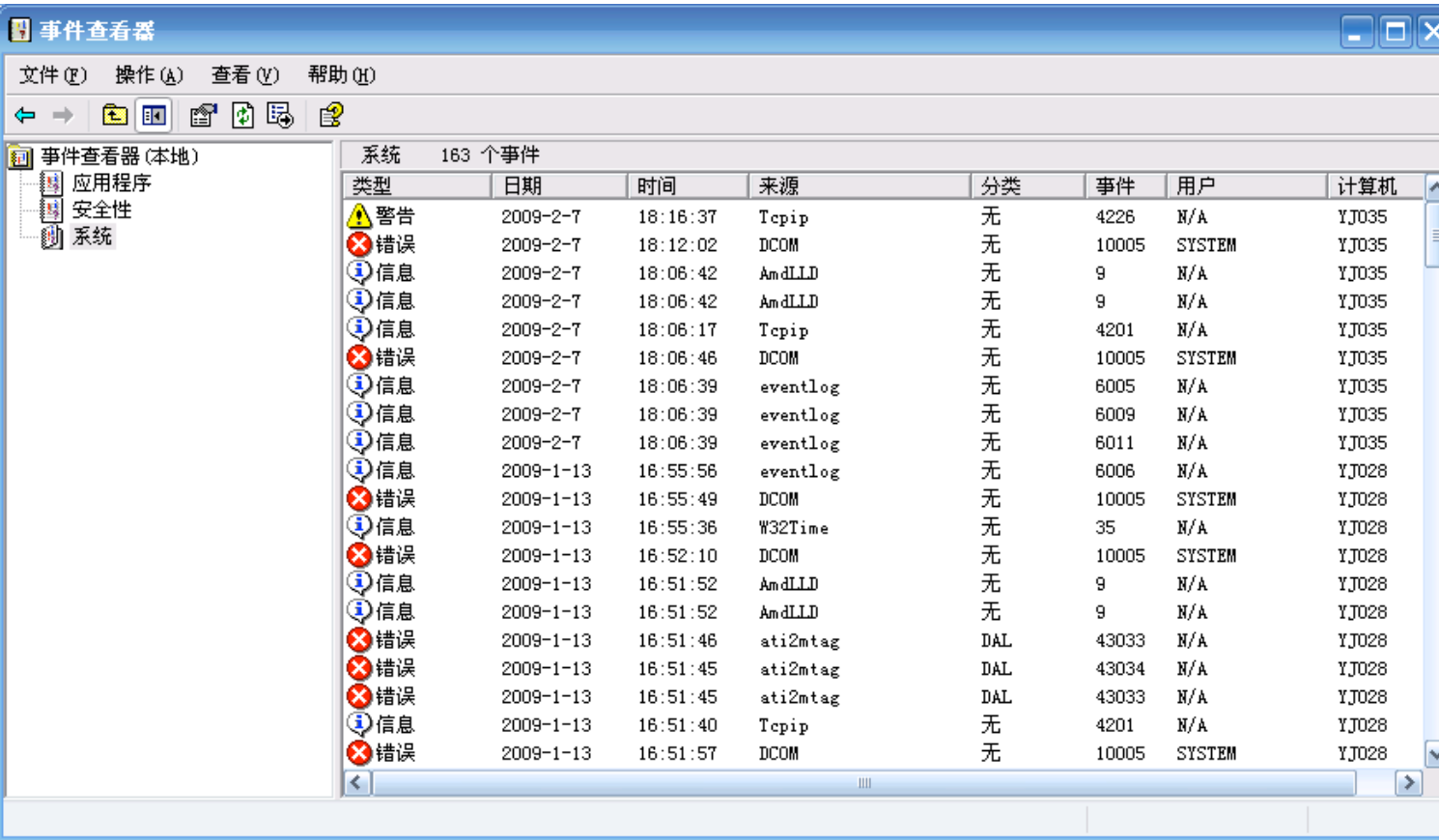


图 14

本文我是在网吧写，开始里面作了限制，不能打开运行，因此写了一个内容为 cmd.exe 的批处理文件 1.bat，打开运行进入 dos 后，输入 Eventvwr.msc 亦可打开事件查看器。

通过查看日志文件，我们可以知晓：

- 1.失败的登陆尝试，
- 2.成功的权限提升尝试，

- 3.更改系统时间,
- 4.突破登陆时间限制,
- 5.登陆/退出时间,
- 6.成功/失败的对象访问。

默认情况下，windows 的安全设置是不支持日志文件，另外，可惜的是，日志文件只记录 Netbios Name，而不记录 IP 地址。

• 八. 网络历史文件

网络浏览器将用户浏览过的站点及图片，还有 cookie 文件等保存在硬盘上，对于调查用户的网站浏览行为提供帮助，如图 1 所示：

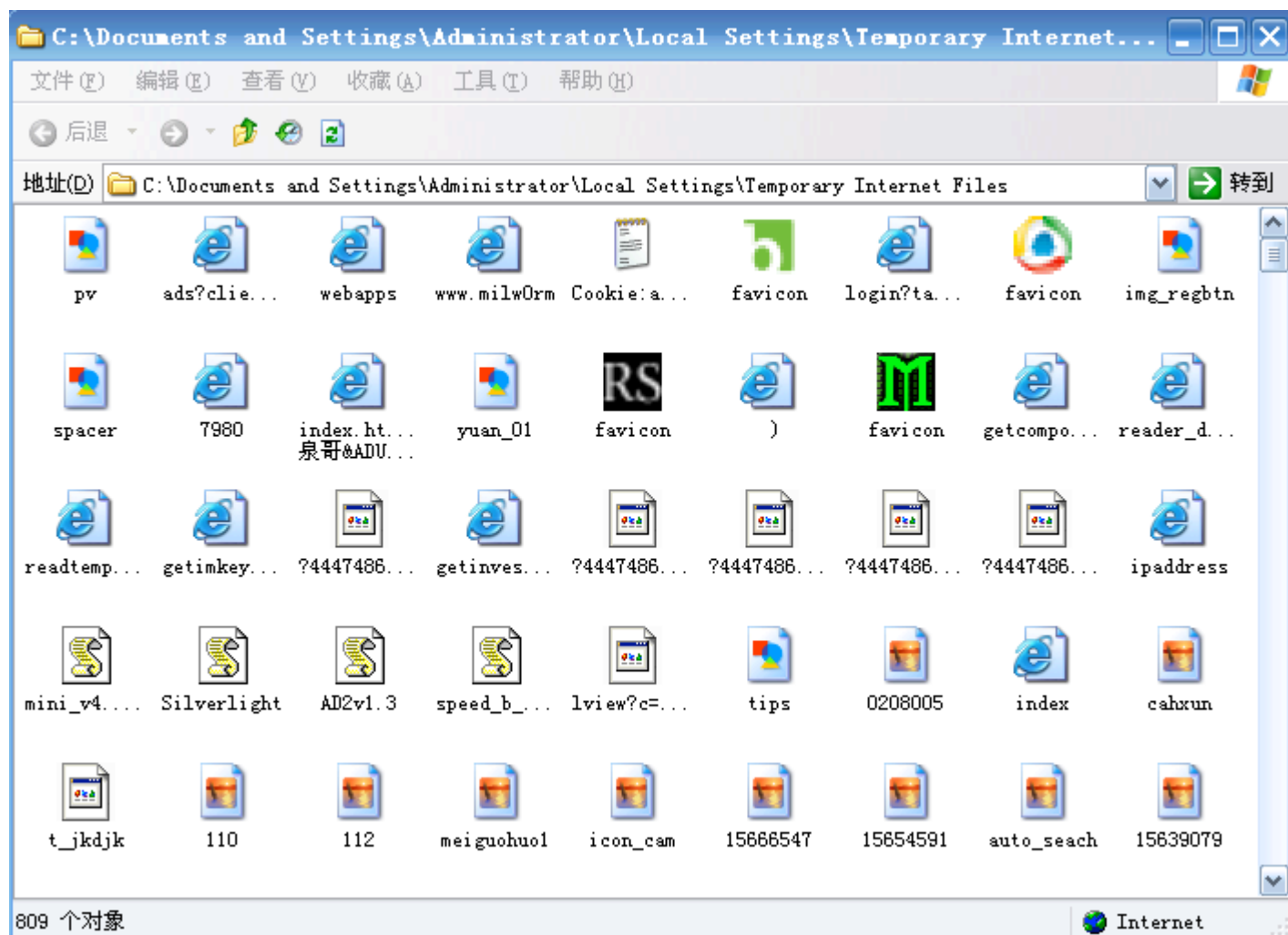


图 15

图 15 是 IE 浏览器保存在硬盘上的历史文件，不同的浏览器保存的历史文件路径不一样，但腾讯 TT 浏览器与 IE 是共用历史文件的，因此路径也是一样。我们也可以通过一些阅读工具来读取这些网络历史文件，比如：Encase,NetAnalysis,WebHistorian。通过 IE 的历史文件我们就可以获得用户浏览过的站点，cookie 以及相关的临时文件。如果我们能够窃取 cookie 文件，我们就可以获得用户的登陆权限了。

• 九. 快捷方式文件(*.lnk)

快捷方式文件(*.lnk)用于链接到目标文件的一种文件,目标文件可为应用程序,目录,文档或者数据文件,在 link 文件中包含有目标文件的各种属性:

- * 目标文件的完整路径

- * 目标文件或者目录所在的卷标(volume label)和卷序列号(volume serial number),这些将有利于将文件连接到一唯一的卷(volume)

- * 文件大小(bytes)

- * 目标文件的 MAC 时间戳

- * 媒体类型(如图 1)

- * 工作目录

- * MAC 地址

- * 远程共享文件名

Media Type	描述
all	Used for all media type devices 可用在所有媒介设备上
aural	Used for speech and sound synthesizers[发音]
braille	Used for braille tactile feedback devices[触觉]
embossed	Used for paged braille printers[盲人专用打印机]
handheld	Used for small or handheld devices[移动]
print	Used for printers[普通打印]
projection	Used for projected presentations, like slides[幻灯片]
screen	Used for computer screens[屏幕]
tty	Used for media using a fixed-pitch character grid, like teletypes and terminals[电报]
tv	Used for television-type devices[电视]

图 16

快捷方式文件的整体结构如图 17 所示：

文件头
Shell item ID list段
文件位置信息段
描述字符段
相对路径段
工作目录段
命令行段
图标文件段
附加信息段

底色为的是可选项

图 17

关于该文件更为详细的资料可参考此文(**Windows 快捷方式文件格式解**

析):<http://www.vckbase.com/document/viewdoc/?id=1411>

link 文件可在未分配的集群(clusters)与交换(swap)内存空间找到。

我们也可借助相关工具来读取 link 文件所包含的信息,比如 Encase link parser EnScript 和 Windows File Analyzer,如图 18 所示:

Windows File Analyzer - [SA - 桌面]

File Windows Help

SA - 桌面

Shortcut Analysis

Directory: C:\Documents and Settings\3320\桌面
Volume serial: 7854-EFB8
Volume label: WINXP

Report...

me	Linked path	Created	Written	Last Accessed	Size [B]	Vol Type	Vol Serial	Vol Name	NetBIOS	MAC Address
ndows Me...	C:\Program Files\Windows Media Player\wmplayer.exe	2008-6-23 7:51:43	2006-11-2 15:06:20	2008-11-28 16:00:00	63488	Fixed	7854 - EFB8	WINXP		00:00:77:00:00:00
mxthon.lnk	D:\Program Files\Maxthon\Maxthon.exe	2007-10-13 1:32:14	2007-10-13 1:32:14	2008-11-28 17:12:43	2224128	Fixed	4C91 - 671F	软件安装	pc-200811...	00:19:DB:86:4F:51
里旺旺(淘...	D:\Program Files\Alisoft\WangWang\WangWang.exe	2008-9-4 10:42:34	2008-5-7 7:19:56	2008-11-28 17:06:16	6363072	Fixed	4C91 - 671F	软件安装	pc-200811...	00:19:DB:86:4F:51
Goo.lnk	D:\Program Files\KuGou\KuGou2008\KuGoo.exe	2008-9-23 7:22:21	2008-9-28 8:33:40	2008-11-28 17:14:01	3465216	Fixed	4C91 - 671F	软件安装	pc-200811...	00:19:DB:86:4F:51
内通.lnk	D:\Program Files\xiaonei\xtalk.exe	2008-8-25 5:58:08	2008-8-25 5:58:08	2008-11-29 0:39:54	4246672	Fixed	4C91 - 671F	软件安装	pc-200811...	00:19:DB:86:4F:51
讯QQ2008...	D:\Program Files\Tencent\qq\CaiHong.exe	2008-10-9 7:05:04	2008-10-9 7:05:04	2008-11-29 5:51:42	57344	Fixed	4C91 - 671F	软件安装	pc-200811...	00:19:DB:86:4F:51
登陆器.lnk	D:\Program Files\Tencent\qq\登陆器.exe	2008-10-20 9:19:28	2008-10-20 9:19:28	2008-11-29 5:51:44	168448	Fixed	4C91 - 671F	软件安装	pc-200811...	00:19:DB:86:4F:51
讯QQ.lnk	D:\Program Files\QQ\QQ.exe	2008-11-28 16:39:14	2008-6-6 12:37:18	2008-11-29 8:35:23	2037144	Fixed	4C91 - 671F	软件安装	pc-200811...	00:19:DB:86:4F:51
星卡卡上...	C:\Program Files\Rising\AntiSpyware\vas.exe	2008-12-8 10:19:10	2008-12-8 10:18:46	2008-12-8 16:00:00	39024	Fixed	7854 - EFB8	WINXP	00:00:77:00:00:00	
的文档.lnk	D:\My Documents	2008-8-30 4:06:20	2008-12-9 13:18:47	2008-12-9 13:19:31	0	Fixed	4C91 - 671F	软件安装	pc-200811...	00:19:DB:86:4F:51
zngj.exe.lnk	D:\软件\qyzngj.exe	2008-6-22 15:06:24	2005-10-30 23:48:28	2009-2-14 15:32:21	106496	Fixed	4C91 - 671F	软件安装	pc-200811...	00:19:DB:86:4F:51

es found

图 18

• 十. 系统还原点(System Restore Point)

系统还原是 Windows 操作系统默认的一个功能，它用来帮助你恢复你的电脑到预设的状态，同时不会丢失你的数据文件,可通过“开始-程序-附件-系统工具-系统还原”来建立系统还原点,如果你选择系统还原，你就可以看到最新的系统还原点了。

关于系统还原更多的资料可参考下面两篇文章：

《windows vista 系统还原专题》：<http://tech.ddvip.com/2007-05/117852074823533.html>

《windows xp Professional 系统恢复浅谈》：

<http://www.microsoft.com/china/community/program/originalarticles/techdoc/WinxpSys.msp>

rp.log 文件是存储在还原点(Restore Point)目录的日志文件，设置系统还原点后，就会生成该文件。通过 rp.log 文件，我们可以获得以下信息：

- * 还原点类型 (APPLICATION_INSTALL , CANCELLED_OPERATION)
- * 还原点创建事件的名称 (i.e, 应用程序或设备驱动程序安装/卸载等)
- * 通过 64-bit FILETIME object 可取得还原点的创建时间

CHANGE.LOG.x 文件 (x 为一数字) 是系统还原所用的一个记录文件是系统更改日志，通过它我们可以获得以下信息：

- * 当系统记录发生更改时，原始文件名会连同一序列号及其它信息 (比如：记录更改类型：文件删除，属性更改或内容更改等) 存入 change.log 文件中
- * 有时整个文件可能被保存 (Axxxxxx.ext 格式)

通过还原点，我们可以获得以下信息：

- * 应用程序的安装或卸载
- * 系统时间更改
- * 删除/卸载的应用程序的碎片
- * 被删除的文件的碎片
- * 曾被访问过的文件迹象

• 十一. P2P 软件调查取证

P2P (point to point) 即点对点的意思, 当一台主机从其它服务器下载文件时, 它作为客户端; 当其它主机从它机上下载文件时, 它就作为服务端, 像 BT,eMule,PPLive 等均为 P2P 软件, 本文主要以 BT 为例来讲解 P2P 软件的调查取证, 其它 P2P 软件的取证可以此为参考。P2P 软件调查取证的主要目的是为了查找不良信息或危害言论的传染源, 以及时切断传染源, 防止其继续传播并追究相关人员的法律责任。

BT 的运行原理

我们需要先从 WEB 服务器上下载种子文件*.torrent, 该文件中包含 tracker 服务端地址列表以及下载文件的哈希值, 通过种子文件中的服务端地址, 我们就可以向其发送以下载文件名哈希值为参数的 HTTP get 请求, 服务端再查找种子列表, 提供各下载服务器地址给我们, 我们就可以从这些服务器上下载文件片段了。

种子文件格式:

BT 种子文件使用了一种叫 bencoding 的编码方法来保存数据。

bencoding 现有四种类型的数据: srings(字符串), integers(整数), lists(列表), dictionaries(字典)

整个文件为一个字典结构, 包含如下关键字:

announce:tracker 服务器的 URL(字符串)

announce-list(可选):备用 tracker 服务器列表(列表)

creation date(可选):种子创建的时间, Unix 标准时间格式, 从 1970 1 月 1 日 00:00:00 到创建时间的秒数(整数)

comment(可选):备注(字符串)

created by(可选):创建人或创建程序的信息(字符串)

info:一个字典结构, 包含文件的主要信息, 为分二种情况: 单文件结构或多文件结构

单文件结构如下:

length:文件长度, 单位字节(整数)

md5sum(可选): 长 32 个字符的文件的 MD5 校验和, BT 不使用这个值, 只是为了兼容一些程序所保留!(字符串)

name:文件名(字符串)

piece length:每个块的大小，单位字节(整数)

pieces:每个块的 20 个字节的 SHA1 Hash 的值(二进制格式)

多文件结构如下:

files:一个字典结构

length:文件长度，单位字节(整数)

md5sum(可选):同单文件结构中相同

path:文件的路径和名字，是一个列表结构，如\test\test.txt 列表为 l4:test8test.txte

name:最上层的目录名字(字符串)

piece length:同单文件结构中相同

pieces:同单文件结构中相同

关于种子文件格式更为详细的内容可参考此文: BT 种子文件格式 <http://dev.csdn.net/article/25/25292.shtm>

实例:

用记事本打开一个.torrent 可以看来类似如下内容



图 19

通过上面可以很容易地读懂了，这里不在多说。

我们这里用迅雷打开.torrent 文件看看，如下图:

文件名称	文件大小	进度
<input checked="" type="checkbox"/> 五笔打字员\wbdzy69.exe	30.76MB	未启动
<input type="checkbox"/> 五笔打字员\说明_Readme.html	2.50KB	未启动
<input checked="" type="checkbox"/> wnwb_71_x29.exe	5.57MB	未启动

图 20

Tracker 服务器:

http://scubt.wjl.cn:8080/announce

图 21

这跟上面的.torrent 文件显示的内容是一样的。

种子文件调查取证

先下载可疑的种子文件，并从其中获取服务端地址及下载的文件名，再通过查看服务器日志来确定上传种子文件的主机 IP。虽然这不一定能够找到传染源，但至少能够通过关掉相关服务器来及时控制传播，以免造成更大的危害。

十二. 数据恢复

在监控取证中经常要利用到数据恢复技术，因为公安部门在对犯罪分子进行电脑上信息搜集时，相关的犯罪资料常常是被犯罪分子删除的，因此需要进行数据恢复以提取重要的犯罪信息。关于数据恢复技术的书籍，在国内当首推由戴士剑与涂彦辉合著的《数据恢复技术》一书：

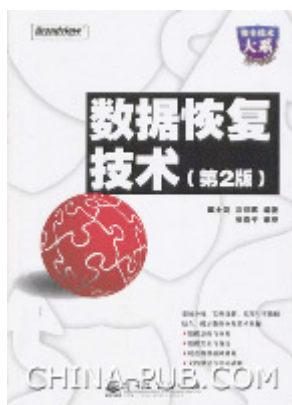


图 22

该书里面从基础讲起，很适合这方面的初学者，有兴趣的朋友可以去看下，本文主要是讲针对文件彻底删除或磁盘格式化后的数据恢复，主要使用 EasyRecovery 和 Finaldata 两个工具。

我们先在 E: / 盘上建个恢复测试.doc 文件，里面就写“恢复测试”四字，然后 shift+delete 彻底删除：

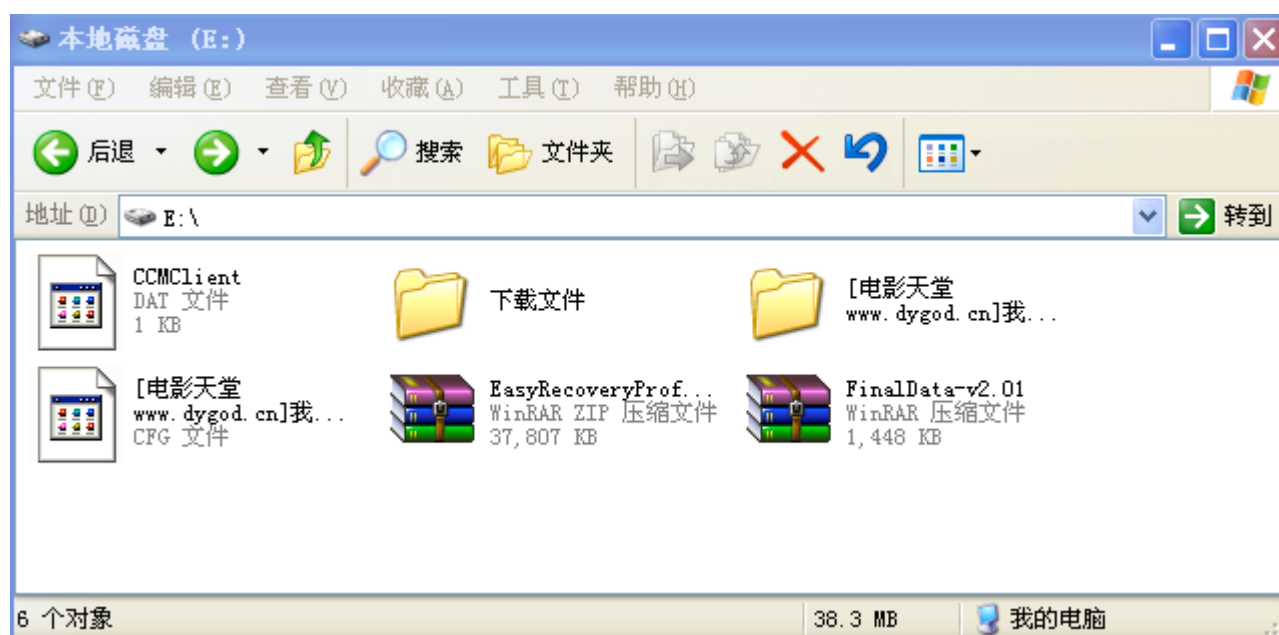


图 23

接着我们用 EasyRecovery 来恢复,选择 Data Recovery->FormantRecovery,跳出提示框，点 OK:

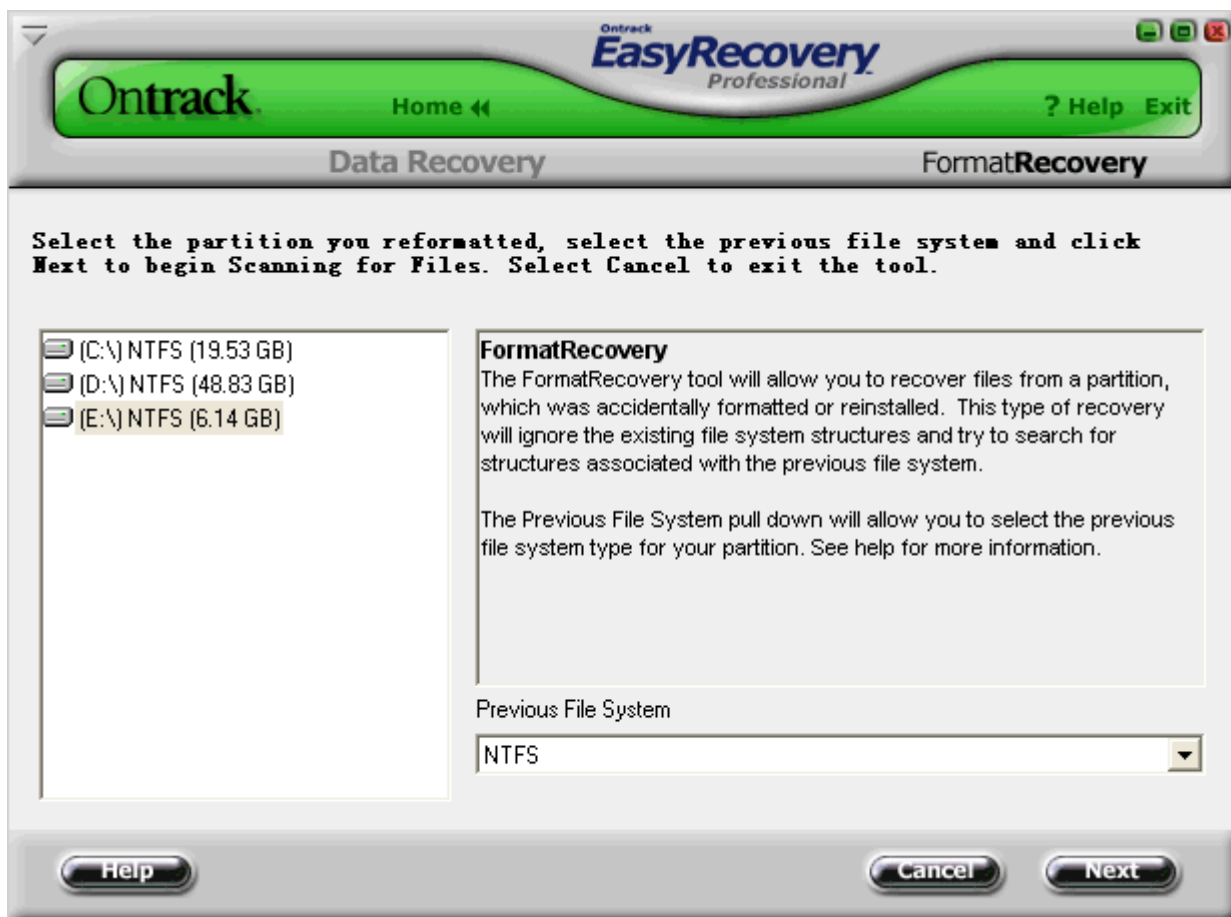


图 24

选择 E: \盘—>next,然后它就开始扫描系统了:

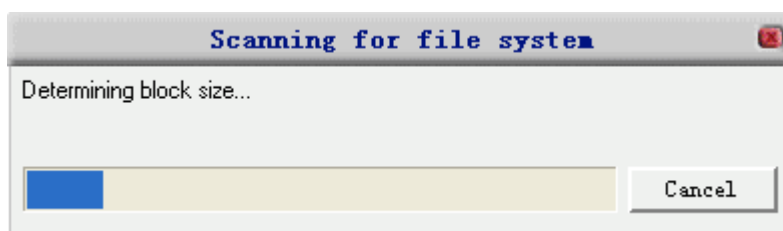


图 25

接着扫描文件, 给出包含删除的文件, 点击 view file 就可查看已删除的文件:

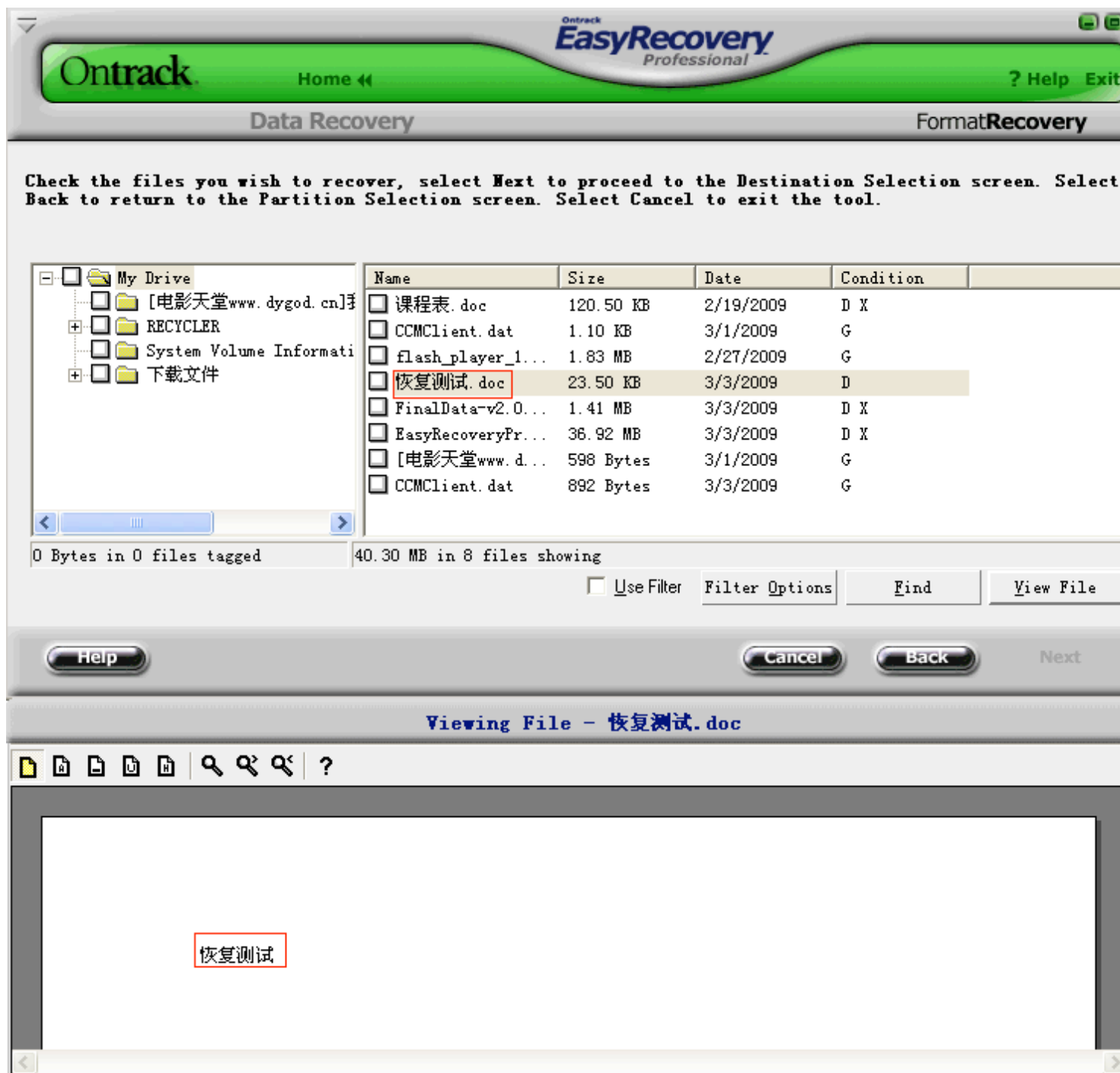


图 26

另外我们也可以用 FinalData 来对已删除的文件进行恢复，因操作简单，这里不再叙述，结果如图 27：

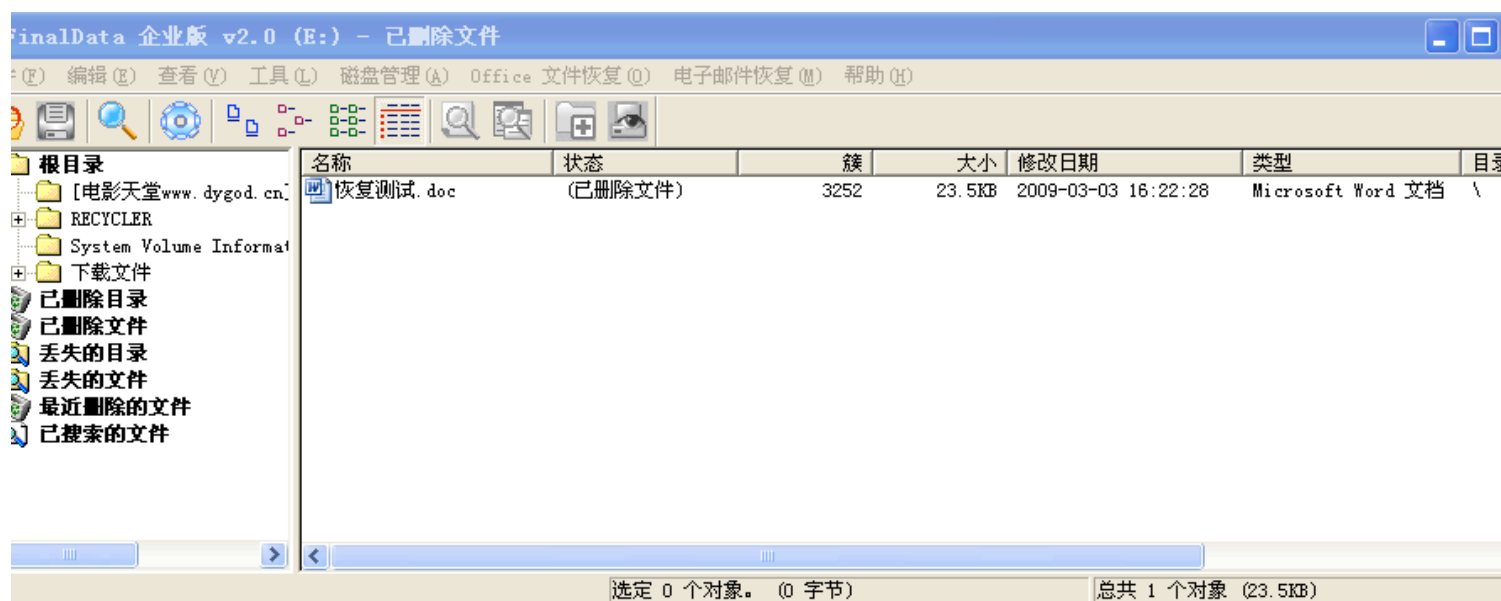


图 27

后记

关于 windows 平台下的监控取证技术到此就告一段落了，但这方面的技术远远不止这些，这里只是希望能起到一个抛砖引玉的作用，如果读者对监控取证技术感兴趣，可以到网上多搜索这方面的内容。