Windows操作系统取证实训

电子数据主要存储在计算机中,Windows 目前是在普通用户的计算机上使用最广泛的 操作系统,占据了中国绝大多数个人计算机用户的操作系统市场,因此针对 Windows 系统 的电子数据取证始终是电子取证研究方向的主流。基于 Windows 系统的计算机中可能包 含着与犯罪事件相关的重要数据。这些数据隐藏在计算机的深处,如用户身份、犯罪记录、 不良数据等信息。本章通过相关的实验,读者能够掌握 Windows 操作系统中重要数据的存 放位置和主要的取证方法。

3.1 易失性数据提取

3.1.1 预备知识:易失性数据

一般来说,从计算机证据的时态性分类,可将计算机证据分为两种:持久性数据和易失 性数据。持久性数据是储存在本地硬盘上的数据,当计算机关闭时会保存下来。易失性数 据是当电脑断电或关闭时,会丢失的数据。传统的取证调查方法是在存储介质上进行事后 检查,即将可疑的计算机接上电源以后再进行数字证据的搜索与获取。但是,随着硬盘加密 技术,反取证工具与技术的不断发展,以及内存容量的不断扩展,传统的事后取证方法会导 致丢失包含在易失性数据中的有价值的证据,而这些数据对于确定计算机犯罪活动往往是 十分重要的。易失性数据驻留在注册表的缓存和随机访问内存(RAM)中,对易失性数据的 调查称为"实时取证"。

易失性数据主要包含:

(1) 描述计算机基本配置信息的系统概要文件。如:计算机操作系统的版本、型号、安装时间、系统目录、系统注册用户、物理内存、安装的硬件及其配置和安装的应用软件等。

(2) 网络连接状况及路由信息。

(3) 当前系统的日期、时间等记录。

(4) 计算机从上一次启动到现在一共运行的时间,用于确定收集的易失性数据是否具 有一定的价值。

(5)当前系统运行的进程列表,可能会发现一些恶意进程、未授权的软件及已终止的合法进程。

(6) 登录用户最近的活动记录。

(7) 启动文件和剪贴板中的数据等。

在涉网案件的现场勘验过程中,应该首先处理会很快消失的电子数据,即易失性数据。

3.1.2 实验目的与条件

1. 实验目的

通过本实验,读者在了解了电子数据取证的基本流程及规范的基础上,熟悉计算机中易失性 数据的种类,掌握使用常用软件工具,进行涉网案件现场易失性数据提取的常用方法和注意点。

2. 实验条件

本实验所需要的软硬件清单如表 3-1 所示。

序 号	设备	数量	参数
1	取证工作站	1台	Windows XP 以上
2	工具 U 盘(内含一些软件)	1 个	包含绿色版工具
3	屏幕录像机(oCam).exe	1 个	绿色版
4	MD5. exe	1 个	绿色版
5	clipbrd. exe	1 个	绿色版
6	6 DumpIt. exe 1个		绿色版
7	systeminfo. exe	1 个	绿色版

表 3-1 易失性数据提取实验清单

3.1.3 实验过程

在取证过程中,首先要准备一个专用的取证工具 U 盘,如 E 盘,里面包含常用的取证工具,如 cmd. exe、MD5Checker. exe、systeminfo. exe、DumpIt. exe 等。然后按下面的方法进行数据的收集,最后将所有数据都保存到工具 U 盘中。

步骤 1: 将手表或手机时间界面置于计算机前方,对照计算机右下角时间信息进行拍照,完成计算机时间信息提取。

步骤 2: 插入 U 盘,运行 U 盘中的绿色版屏幕录像软件,打开软件设置,将后续快照、录像文件保存路径修改为该 U 盘,如图 3-1 所示。

國設置	
录制 声音 屏幕捕获 动图	保存路径: E:\ ×H+台. <prefix>_<yyyy_mm_dd_hh_nn_ss_z< th=""></yyyy_mm_dd_hh_nn_ss_z<></prefix>
快捷键 效果 保存 时间限制 水印 摄像头 性能 语言	开始编号在:1
重置(В)	截图(Alt + A) 确定(Q) 关闭(C)

图 3-1 修改生成文件的保存路径

步骤 3: 单击录制按钮对后续电脑操作进行全程录像和截屏保存。

注意:操作过程中不能在硬盘上进行写入或修改操作,不得将生成、提取的数据存储在 原始存储媒介中,不得在目标系统中安装新的应用程序。

步骤 4: 在 U 盘中新建文件夹,分别存放内存提取文件、屏幕信息提取文件、硬盘及操 作系统信息文件、正在运行有密码保护的文件、录屏及摄像文件等,如图 3-2 所示。

Service + Handle + KINGSTON (H:) +	A DEC DEC		* ++ HER KINGSTON (H:)
2件(F) 编辑(E) 查看(V) 工具(T) 帮助(H)			
组织 · 劉打开 共享 · 封梁 新建文	件夹		🖬 • 🗖 😡
WPS网合 Pr存提取文 Pr存提取文 F F G 安命2256編視頭 そ 使	1959年 1959日 1989日 1989日 1987日 日 1987 1987 1987 1987 1987 1987 1987 1987	没有预测。	
 文档(E) 可移动磁盘(G) × KINGSTON (H) 研惑 新建文件夹 修改日際: 2020/8/31 16:17 文件夫 			

图 3-2 在 U 盘中新建文件夹

步骤 5: 打开 U 盘中的内存提取工具,将获取的内存保存在 U 盘相应文件夹中,如图 3-3 所示。

C AccessData FTK Imager 3.1.1.8		-			- 0	×
Elie View Mode Help		1111				
	CISIDE	1 M 1 2 .				
Evidence Tree ×	File List	1 1	louis d l		1. 闪仔数据提取	×
	Name	Size Type	Date Mod			-
		Memory Progress				
		Destination: Just th 71	10 Y (1) marching man			
		Status: Dumping	RAM: 0 bytes/0 bytes [0%]	i		
			rear a plant a plan fa st			
Custom Content Sources ×						1
Evidence:File System[Path]File Options			Cancel			
· ·						- 11
New Edit Bernove Remove All Greate Imag						
Properties Hex Value I Custom Co	J					*
For User Guide, press F1	Statement in the second				NUM	-
🐮 🕲 🔛 9. # 🕓) 网址	微信 📄 Win 🧕	ocam RTKL.	=: 2) ā 8	*e Gr □ * ♥ ▲ ■ 16:2 2020/8	3/31

图 3-3 获取计算机运行内存

步骤 6: 查看硬盘分区状况、文件显示属性、网络连接信息等,并进行录屏和截屏,保存 在 U 盘相应文件夹中,部分如图 3-4、图 3-5 所示。



图 3-4 获取硬盘分区状况



图 3-5 获取网络连接状态信息

步骤 7:用录像和截图软件进行屏幕信息提取,提取打开的文件信息,并保存在 U 盘相 应文件夹中,如图 3-6 所示。

步骤 8:运行 U 盘中的粘贴板查看器,提取粘贴板信息,并保存在 U 盘相应文件夹中, 如图 3-7 所示。

步骤 9: 提取浏览器、网页相关信息,并保存在 U 盘相应文件夹中。

步骤 10:对正在运行的有密码保护的数据,如微信、QQ、邮箱、网银、支付宝等,进行相关备份文件提取,并将其保存到 U 盘相应文件夹中,如图 3-8 所示。

步骤 11: 将录屏文件、摄像录屏文件保存在 U 盘相应文件夹中,如图 3-9 所示。

68



图 3-6 提取打开的文件信息

R• 🖻 177	刻梁 新建文件	*			a .	
		四 的影響直看過 - (的影)	M)			×
WPS阿盘	Ē		2金(S) 查看(V) 窗口(W) 楷 同篇	Ø(H)		. # X
3 ML	enpora	2006.08.08	20153214118	2015.11.30	2020.11.29	14
副 爱奇艺热频视频 	1	3952093304 2006.08.08 3701404127	20153214008	2015.11.30	2020.11.29	· -
5. 图片		2006.08.08	20153214026	2015.11.30	2020.11.29	1
5.文档 4.音乐		2006.08.08 3951701727	20153214027	2015.11.30	2020.11.29	1
111000		2006.08.08	20153214028	2015.11.30	2020.11.29	1
▶ 系统 (C:) ▶ 软件 (D:)		2006.08.08 3451919909	20153214029	2015.11.30	2020.11.29	1
⇒ 文档(E)		×1				.j ∴ 5
。可移动磁盘 (G:)		剪點板				
KINGSTON (H:)						
PRIS .						
	STREE SAAF LAIF S	0.00 0/06/300 303				

图 3-7 提取粘贴板信息

2 9	Q ### + 文件传	输助手	≉ - Ø ×
adudder, 191		4. 有	密码保护的数据提取
0	文件 备份与恢复	-	×
LES REFERS		F	
-	TAT/ 备份聊天记录至电脑	恢复聊天记录至手机	
64.9 939 <u>1</u>	Ancie Ancie		
	5 152A	新建40文件	
	*12天葉 約時130万. 昨天 日本10次10000- 丸		发送(5)
3 Ø M	9.* 🚫 929 🛗 Wind 🕅 ocam 👘	59°C 5 4	- CHE & S & M (12:10

图 3-8 提取微信备份文件

(F) Man(c) 単位(V) 版・ ②打开・	工具(T) 帮助(F 打印 触梁	0 新建文件夹		5. 录屏	及摄像文件保存
L WPS网盘	2020 09	日本日本日本日本日本日本日本日本日本日本日本日本日本日本日本日本日本日本日本			268)
■ 愛奇艺热攝視鏡 ● 視頭 ● 園片 ● 文档 ● 音乐	01_12_38_ 48_795				00:00:17 1.3MB / 61.5GB
[计算机 ■ 系统 (C:) ■ 软件 (D:) ■ 文档 (E:) ■ CAN(CN) (G)					
CANON (G:) KINGSTON (H:) EOS_DIGITAL (t)					

图 3-9 保存录屏及摄像文件

步骤 12:使用 U 盘中的 MD5 工具,对录屏文件及所有提取的电子数据进行哈希值计算,记录文件类型、用户名、密码、路径来源及哈希值,如图 3-10 所示。

8) 开	a I	插入 页	面布局 2	at star	市岡 祝!	日 开发工机	a and a second	MICTOSOTTE	15.5	_			_		8 - 0
12 私	***	宋体	z u -)(· 11		• = _ [*	- ジョ助 使 送合井	换行 后周中 - [**现 明- ** •	11 -21	第二日 条件格式 表 表格	日 単元楷 記・样式・	6. ң	上子数	据固定	日 (今40 重秋) (市石) - 浅祥
剪天	极压		3	字体	19	对	东方式	9	数字	6	样子	c	单元的		1911	ł
-	A9	-	• (XYL	摄像机录用	文件				-	_					
Z	A	in the	В	C	D	E	F	G	н	1	3	K	L	M	N	0
1	文件类	222	用户名	密码	来源路径	哈希值						_	_			
2	求屏文	て件		_	-	File: H:\操	作录屏文件	\录制_20	20_09_01_1	2_38_4	18_795.mp4	-	-			
3				-	_	Size: 3270	58 bytes	11 12.24								
4						Modified:	2020年9月1	日,12:38	3:54		-		-			
5					-	MDS: A40	348D9FBED	16E0B/3	3/09/2004	JUZE TO ALCO	111053		-		-	
		_		-	-	SHA1: 930	SC/AEA000	23450/04	6/82E1041	/84104	111962					
		-		-		CRC32: FU	503320			-					-	
2	18 /0 is	136	2-0-14		-	File: H-\#	作品国文件	「「「「「「」」	TO AL MTS	-		-	-			
0	264,884.07	1.7	(XIII)			Size: 1253	376 hutec	1202 804-310.07	- Citrating	-	_		-		-	-
1				-		Modified:	2015年5月2	7H 6-08-	12	-	_					
2						MD5: 4C4	A1D046069	D546FAF	088CAAF13	0887		-				-
3					-	SHA1: 53	35DECCF8E	65603010	C106F1B3C	843486	07EE82	-				
4						CRC32: E	5019549	1		1		-				
5										-						
6																
7																
8																
9																
4		Shee	t1 Sheet	2 Sheet3	0			· · · · · ·	a fan hij e					_		
X															341.4	日志甘
	6	T)	9 A	* Æ	B102	0.22	Win	i •	am 🔠	Micr	Y Hash	5:	5 -6 cr 5	* 9	4.87.4	12:00

图 3-10 哈希值计算

注意:易失性数据提取完成后,对于保存数据信息的专用存储介质和现场录像等,进行 唯一性编号并封存。

3.1.4 实验小结

传统的在计算机犯罪中所使用的取证流程大多数为关闭涉案计算机后,使用即插即用 设备按字节流完全复制计算机的磁盘数据建立磁盘镜像,然后在实验室中对镜像数据进行 事后分析。然而,随着计算机硬件水平的不断发展,大容量的内存广泛被使用,同时各种加

密与反取证技术的出现,导致在这样传统的取证过程中损失了大量有价值的信息。

计算机的易失性数据中可能包含关于犯罪行为的关键性信息,如用来加密信息所使用 的密码,系统在犯罪行为发生过程中的状态,使用反取证工具的痕迹以及一些调查者在分析 硬盘数据过程中容易忽略的至关重要的恶意软件或系统级后门程序等相关信息。所以近年 来针对计算机易失性数据的取证分析工作越来越受到司法界和计算机安全专家的重视。

传统上一般将获取易失性数据的方法分为两类:一类基于硬件设备实现;另一类基于 软件方法实现。硬件设备获取内存镜像被业界广泛认为具有更高的安全性和可靠性,而软 件运行时必然会导致内存中部分数据发生变化,可能会影响到获得的内存镜像的完整性。 虽然相较而言,硬件获取方式比软件更可靠,但由于软件方式使用方便、成本低,故仍然被广 泛使用。本实验考虑通用性和实践操作性,选用软件方式为例进行易失性数据提取。

在实验的过程中,要注意强调操作的规范性,如录屏、哈希校验等,否则即使提取到相关 重要涉案数据,也会面临证据失效的风险。

3.2 内存的获取与分析

3.2.1 预备知识:内存取证、DumpIt工具、Volatility工具

1. 内存取证

网络攻击内存化和网络犯罪隐遁化,使得部分关键数字证据只存在于物理内存或暂存 于页面交换文件中,这使得传统的基于文件系统的计算机取证不能有效应对。内存取证作 为传统文件系统取证的重要补充,是计算机取证科学的重要组成部分,通过全面获取内存数 据、详尽分析内存数据,并在此基础上提取与网络攻击或网络犯罪相关的数字证据。近年 来,内存取证已赢得相关领域的持续关注,获得了长足的发展与广泛应用,在网络应急响应 和网络犯罪调查中发挥着不可替代的作用。

内存取证(有时称为内存分析)是指对计算机内存转储中易失性数据进行的一种分析。 信息安全专业人员可以通过内存取证,来调查和识别那些不会在硬盘驱动器数据中留下痕 迹的攻击或恶意行为。通过内存取证,安全专业人员可以了解运行时的各种系统活动,例如 开放的网络连接或最近执行的命令和进程等。程序在计算机上运行之前,首先需要被加载 到内存中,这使得内存取证变得非常重要——这意味着所有被创建、检查或删除的程序或数 据都将被保存到 RAM 中。其中包括图像、所有 Web 浏览活动、加密密钥、网络连接或注入 的代码片段。在许多情况下,某些证据只能在 RAM 中找到,例如在崩溃期间存在的开放网 络连接。由于攻击者可以开发只驻留在内存中而不在硬盘落地的恶意软件,从而使标准的 计算机取证方法几乎看不到该恶意软件,这使得内存取证变得愈发重要。

内存取证研究的首要问题是如何完整地获取内存数据。目前,获取物理内存数据的方法很多,一般利用操作系统的相关机制和特性,通过不同方法获取物理内存数据。这些方法可概括为两大类:基于硬件的内存获取和基于软件的内存获取。在获取了内存数据之后,就需要对其进行深度分析,解析、重建出内存数据中所蕴含的网络攻击和网络犯罪证据信息。传统的内存数据分析主要采用字符串搜索方法,通过搜索内存中用户名、口令、IP 地址等文本字符串,获取部分取证辅助信息。尽管该方法操作简单、使用方便,能够提取部分内存信息,但却不能有效分析与网络攻击和网络犯罪相关的进程、注册表、解密密钥、网络连

接、可执行文件、系统状态等信息。为了全面地进行内存数据分析,需依据操作系统内核数据结构和相关机制去解析与重建内存数据所蕴含的信息,进而提取相关网络攻击和网络犯罪证据。目前的内存分析内容大致可以分为6种:①进程信息分析;②注册表信息分析; ③密钥恢复分析;④网络连接分析;⑤可执行文件分析;⑥系统状态信息分析。

内存取证作为计算机取证科学的一个重要分支,在预防网络攻击、调查网络犯罪等方面 有重要且不可替代的作用和应用前景,已成为信息安全研究者所关注的热点研究领域。

2. DumpIt 工具

不同的操作系统需要用到不同的物理内存获取工具,此外在获取物理内存数据时还需 尽量减少对原有内存数据的覆盖,最大程度提取出内存数据。MoonSols DumpIt 是一款同 时支持 Windows32dd 和 Windows64dd 的内存副本获取工具。用户只需双击 DumpIt. exe 即可执行程序,在提示问题后面输入 y,等待几分钟时间即可在当前目录下生成主机物理内 存的副本,该副本文件是以*.raw 为后缀的镜像文件。raw 是未经处理的意思,使用该工 具对物理内存进行复制是逐位进行深度复制,即按原样进行复制,这样可以避免丢失一些重 要数据。

3. Volatility 工具

在最初研究内存取证的阶段使用的工具的主要功能是打开二进制(十六进制)文件,查 看具体地址及内容,比如 WinHex 工具。WinHex 可以打开内存 dump 文件并查看相应的 地址和内容,一般采用字符串搜索的方式。除此之外微软公司还提供了用于 Windows 操作 系统的 debug 工具(Microsoft Debugging Tools for Windows)。Windows debug 工具是一 个包含了一系列功能的工具集,其中某些小工具能十分简便地帮助进行取证工作,比如打开 Windows 崩溃的 dump 文件。

2008年,内存取证领域有了一定的发展并出现了一个集合了其他各种内存取证工具的 取证框架工具 Volatility。Volatility 是一款基于 GNU 协议的开源框架,使用 Python 语言 编写而成,可以分析内存中的各种数据。Volatility 各项功能都是由插件实现的,各地的取 证研究者可以根据自己的需要开发 Volatility 的插件来拓展其功能。Volatility 支持对 32 位或 64 位 Windows、Linux、macOS、安卓操作系统的 RAM(随机存储器)数据进行提取与 分析。

Volatility 是以命令提示符方式使用的,所以同 DOS 下面的命令一样,Volatility 的开 发人员也同样为我们提供了使用该工具的帮助命令。即通过-h 或-help 选项可以显示该工 具的帮助列表信息。该命令显示了可用的命令选项(Options)以及支持当前操作系统版本 的插件命令(Supported Plugins Command)。

例如-f FILENAME 选项的功能是说明打开一个镜像文件所使用的文件名,这个命令 选项几乎在所有命令中都会用到。

Volatility 的命令格式如下:

volatility -f <文件名> - - profile = <配置文件> <插件> [插件参数]

Volatility 常用插件如下:

① imageinfo:显示目标镜像的摘要信息;

② pslist:列举出系统进程,但它不能检测到隐藏或者解链的进程,psscan可以;

③ psscan: 可以找到先前已终止(不活动)的进程以及被 rootkit 隐藏或解链的进程;

④ pstree: 以树的形式查看进程列表;

⑤ mendump: 提取出指定进程;

⑥ filescan: 扫描所有的文件列表;

⑦ hashdump: 查看当前操作系统中的 password hash,例如 Windows 的 SAM 文件

内容;

⑧ svcscan: 扫描 Windows 的服务;

⑨ connscan: 查看网络连接。

3.2.2 实验目的与条件

1. 实验目的

通过本实验,读者可以掌握以下内容:

(1) 了解内存的基本概念和内存中常见的有价值的数据;

(2) 掌握物理内存的获取方法;

(3) 掌握使用 Volatility 工具进行内存分析的方法。

2. 实验条件

本实验所需要的软硬件清单如表 3-2 所示。

表 3-2 内存取证实验清单

序号	设 备	数 量	参数
1	取证工作站	1台	Windows XP 以上
2	DumpIt 软件	1 个	无
3	Volatility 软件	1个	绿色版

3.2.3 实验过程

步骤 1:双击 DumpIt. exe 可执行程序,在提示问题后面输入 y(如图 3-11 所示),等待 几分钟时间即可在当前目录下生成主机物理内存的副本,该文件是以*.raw 为后缀的镜像 文件。

G:\mem\DumpIt.exe	
DumpIt - v1.3.2.20110401 Copyright (c) 2007 - 2011 Copyright (c) 2010 - 2011	- One click memory memory dumper , Matthieu Suiche <http: www.msuiche.net=""> , MoonSols <http: www.moonsols.com=""></http:></http:>
Address space size: Free space size:	10460594176 bytes (9976 Mb) 1431141588992 bytes (1364842 Mb)
<pre>* Destination = \??\G:\</pre>	mem\DESKTOP-APSMTEM-20161127-051232.raw
> Are you sure you wa + Processing	nt to continue? [y/n] y

图 3-11 内存获取

注意:此步骤一般在 3.1 节现场勘验易失性数据提取环节完成。

步骤 2: 将步骤 1 中获取的内存镜像文件与 Volatility 工具放于同一级目录下。打开 cmd 命令行工具,进入该级目录下。

步骤 3: 使用 imageinfo 命令查看正在分析的内存样本的摘要信息,命令格式如下:

```
volatility - f victor_PC_memdump.dmp imageinfo
```

该命令可以显示主机所使用的操作系统版本、服务包以及硬件结构(32 位或 64 位)、页 目录表的起始地址和获取该内存镜像的时间等基本信息。该命令的输出结果如图 3-12 所示。

D:\work\电子取证\内存取证>volatility -f victor_PC_memdump.dmp imageinfo
Volatility Foundation Volatility Framework 2.6
INFO : volatility.debug : Determining profile based on KDBG search
Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win2008R2SP1x64_2400
0, Win2008R2SP1x64_23418, Win2008R2SP1x64, Win7SP1x64_24000, Win7SP1x64_23418
AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
AS Layer2 : FileAddressSpace (D:\work\电子取证\内存取证\victor_PC_memdump
. dmp)
PAE type : No PAE
DTB : 0x187000L
KDBG : 0xf80003ffc0a0L
Number of Processors : 2
Image Type (Service Pack) : 1
KPCR for CPU 0 : 0xfffff80003ffdd00L
KPCR for CPU 1 : 0xfffff880009ef000L
KUSER_SHARED_DATA : 0xfffff7800000000L
Image date and time : 2018-11-02 10:31:12 UTC+0000
Image local date and time : 2018-11-02 18:31:12 +0800

图 3-12 imageinfo 命令

Win7SP1x64 表明操作系统版本为 Windows 7、服务包为 SP1、硬件结构是 x64(即 64 位)。 其他信息和取证关系不大。

步骤 4: 使用 pslist 命令和 psscan 命令查看进程信息,查看是否有明显可疑的进程在运行。

注意: pslist 命令不能检测到内存中的隐藏进程以及由于系统受攻击导致未在链表中 出现的进程信息,但 psscan 命令能够解决这个问题。

所以,本实验使用 psscan 命令查看内存进程信息,其运行结果如图 3-13 所示。由于该 命令输出结果较多,我们通过> psscan.txt 将其输出结果重定向到 psscan.txt 文件中。

D:\work\电子取证\内存取证>volati can.txt Volatility Foundation Volatility	lity -f victor_PC_memdump. 7 Framework 2.6	.dmpprofile=W	in7SP1x64 psscan ≻pss
psscan.txt	2019/11/26 15:49	文本文档	11 KB

psscan.txt	2019/11/26 15:49	又本又档	11 KB
victor_PC_memdump.dmp	2018/11/2 18:43	DMP 文件	2,097,152 KB
Volatility.exe	2018/6/6 9:39	应用程序	17,771 KB
volatility_2.6_win64_standalone.zip	2019/11/26 14:20	WinRAR ZIP 压缩文件	15,201 KB
图 内存取证工具Volatility_Framework.doc	2015/9/9 20:04	DOC 文档	978 KB

图 3-13 psscan 命令

步骤 5:使用 dlllist 命令显示一个进程装载的动态链接库的信息,使用-p PID 选项过滤输出结果,比如想要查看 PID 为 5204 的 firefox.exe 进程在运行过程中加载了哪些动态链接库,就可以通过在 dlllist 后面加上选项-p 5204,即可显示其详细信息,显示列表主要包括加载的动态链接库文件的基地址、文件大小以及文件所在路径,如图 3-14 所示。

步骤 6: 使用 netscan 命令来列出所有进程连接的网络,如图 3-15 所示。

步骤 7:使用 hivelist 命令定位与硬盘上对应的注册表文件在内存中的虚拟地址和物理地址。hivelist 命令运行结果如图 3-16 所示。

D:\work\电子取证\内存取证>volatility -f victor_PC_memdump.dmp --profile=Win7SP1x64 dlllist -p 5204 Volatility Foundation Volatility Framework 2.6

firefox.exe pid: 5204 Command line: "C:\Program Files (x86)\Mozilla Firefox\firefox.exe" -contentproc --channel="50 24.24.1484987846\1709745999" -childID 5 -isForBrowser -prefsHandle 3904 -prefMapHandle 3336 -p refsLen 7748 -prefMapSize 190024 -schedulerPrefs 0001, 2 -parentBuildID 20181030165643 -greomni "C:\Program Files (x86)\Mozilla Firefox\omni.ja" -appomni "C:\Program Files (x86)\Mozilla Fir efox\browser\omni.ja" -appdir "C:\Program Files (x86)\Mozilla Firefox\browser" - 5024 "\\.\pip e\gecko-crash-server-pipe.5024" 7776 tab

Base	Size	LoadCount	LoadTime			Path
0x0000000000120000	0x72000	0xffff	1970-01-01	00:00:00	UTC+0000	C:\Pro
gram Files (x86)\Mozilla	Firefox\firefox.exe					
0x0000000077ad0000	0x1a9000	Oxffff	1970-01-01	00:00:00	UTC+0000	C:\Win
dows\SYSTEM32\ntdl1.dl1						
0+000000074960000	0*2£000	0-2	2018-11-02	10.97.46	UTC+0000	C.\Win

图 3-14 dlllist 命令

D:\work\电子	「取证\内存取证>volatility -f victor PC me	emdump.dmpprofile=Win7S	P1x64 netscan		
Volatility	Foundation Volatility Framework 2.6				
Offset(P)	Proto Local Address	Foreign Address	State	Pid	Owner
Created					
0x7d4001e0	UDPv4 0. 0. 0: 1900	*:*		1680	PKit.exe
2018-11-02	10:29:49 UTC+0000				
0x7d404240	UDPv4 0. 0. 0. 0:50745	*:*		3232	BaofengPlatfor
2018-11-02	10:29:49 UTC+0000				
0x7d406bb0	UDPv4 127. 0. 0. 1:49340	*:*		1364	svchost.exe
2018-11-02	10:24:58 UTC+0000				
0x7d40f670	UDPv4 127. 0. 0. 1:58194	*:*		4940	BFPush. exe
2018-11-02	10:29:59 UTC+0000				
0x7d421ec0	UDPv4 0. 0. 0. 0: 5005	*:*		3880	wmpnetwk.exe
2018-11-02	10:24:58 UTC+0000				
0x7d424910	UDPv4 0. 0. 0: 5004	*:*		3880	wmpnetwk.exe
2018-11-02	10:24:58 UIC+0000				
0x7d4292a0	UDPv4 0. 0. 0. 0:63714	*:*		3232	BaofengPlatfor
2018-11-02	10:29:56 U1C+0000	30.0 AP		0000	
0x7d456a90	UDPV4 0. 0. 0: 5004	*:*		3880	wmpnetwk.exe
2018-11-02	10:24:58 U1C+0000	4.4		2000	man a tarda a sea
0X70406890	10-04-59 UTC:0000	*:*		3860	wmpnetwk.exe
2018-11-02	10:24:58 UIC+0000	4.4		1964	anabaat ana
2012-11-02	10.24.52 UTC+0000	9 • (P)		1304	svenost. exe
0x7d475010	UDPv4 0.0.0.15585	***		3204	OvPlayer ere

图 3-15 netscant 命令

Volatility Foundat: Virtual	on Volatility Frame Physical	Name
0xffffff8a006433410	0x000000001ee81410	\??\C:\System Volume Information\Syscache.hve
0xfffff8a00000d010	0x00000002c317010	[no name]
0xfffff8a000024010	0x00000002c274010	\REGISTRY\MACHINE\SYSTEM
0xfffff8a000054010	0x00000002c264010	\REGISTRY\MACHINE\HARDWARE
0xfffff8a000110010	0x000000029f1d010	\SystemRoot\System32\Config\SECURITY
0xfffff8a000300010	0x00000001e644010	\SystemRoot\System32\Config\SAM
0xfffff8a0008df410	0x000000021c63410	\Device\HarddiskVolume1\Boot\BCD
0xfffff8a000a55010	0x00000002a597010	\SystemRoot\System32\Config\SOFTWARE
0xfffff8a001252010	0x00000002865b010	\??\C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT
0xfffff8a0012ea010	0x000000022725010	\??\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT
0xfffff8a0019d3010	0x00000001436d010	\??\C:\Users\victor\ntuser.dat
0xffffff8a001ad5010	0x0000000096aa010	\??\C:\Users\victor\AppData\Local\Microsoft\Windows\UsrC
lass. dat		
0xfffff8a0063bb010	0x0000000029a63010	\SystemRoot\System32\Config\DEFAULT

图 3-16 hivelist 命令

从运行结果可以发现,SECURITY 注册表文件在内存中的虚拟地址是 0xffff8a000110010, SYSTEM 注册表文件在内存中的虚拟地址是 0xfffff8a000024010,这两个值我们稍后马上 会用到。

步骤 8:使用 lsadump 命令读取注册表中与本地授权相关的数据。使用该命令的时

候,需要把步骤 7 中得到的 SYSTEM 注册表的虚拟地址作为-y 选项的参数,SECURITY 注册表文件的虚拟地址作为-s 选项的参数,lsa 命令及其运行结果如图 3-17、图 3-18 所示。

D:\work\电子取证\内存取证>volatility -f victor_PC_memdump.dmp --profile=Win7SP1x64 lsadump -y 0xffff8a000024010 -s 0xfffff8a000110010 >lsadump.txt Volatility Foundation Volatility Framework 2.6

图 3-17 lsa 命令

🚺 lsadump.txt	- id	潘木															
文件(2) 编辑(2)	相式()	1) 通	唐 W) 朝日	助的												
0x0000010	65	00	5f	00	64	00	32	00	44	00	45	00	00	00			e d. 2. D. E
_SC_Dnscach	e																
_SC_LmHosts																	
RasDialPara	ms!!	S-1-	-5-3	21-1	1071	808	153	3-2	995	0220	67-	180	167	453	1-5	00#0	
0x00000000	34	00	36	00	30	00	34	00	39	00	36	00	31	00	00	00	4.6.0.4.9.6.1
0x00000010	31	00	36	00	30	00	30	00	00	00	37	00	00	00	00	00	1. 6. 0. 0 7
0x00000020	00	00	41	00	64	00	6d	00	69	00	6e	00	69	00	73	00	A. d. m. i. n. i. s.
0x00000030	74	00	72	00	61	00	74	00	6f	00	72	00	00	00	69	00	t. r. a. t. o. r i.
0x00000040	74	00	31	00	39	00	38	00	39	00	31	00	30	00	30	00	t. 1. 9. 8. 9. 1. 0. 0.
0x00000050	34	00	00	00	00	0.0	30	0.0	0.0	0.0	31	0.0	38	00	32	0.0	1 0 1 8 7
0x00000060	37	00	33	00	33	00	37	00	35	00	00	00	31	00	36	00	73375 16
0x00000070	30	00	30	0.0	0.0	00	36	0.0	31	0.0	00	0.0	00	00	00	00	0 0 6 1
0x00000080	b0	00	0.9	00	21	00	39	0.0	43	00	20	00	51	00	20	00	190 0
0x000000000	32	00	30	00	31	00	35	0.0	33	00	34	00	30	00	35	00	2 0 1 5 3 4 0 5
0x000000000	22	00	20	00	21	00	20	00	20	00	40	00	62	00	71	00	2.0.1.0.0.0.0.0
0x000000000	75	00	70	00	74	00	00	00	00	00	40	00	21	00	00	00	2. 3. 1. 0. 3. 0. C. q.
0x00000000	21	00	20	00	20	00	20	00	26	00	20	00	51	00	21	00	u. p. t
02000000000	31	00	39	00	20	00	28	00	30	00	39	00	00	00	51	00	1. 9. 0. 8. 5. 9 1.
000000000000000000000000000000000000000	36	00	50	00	50	00	00	00	30	00	31	00	00	00	00	00	6. 0. 0 6. 1

图 3-18 lsa 命令运行结果

从部分运行结果可以看见两条有用信息:第一处下画线的地方显示的是本地主机 Administrator用户的密码: it19891004(这也确实是电脑的开机密码);第二处下画线的地 方显示的 15340529109@cqupt 正好是登录 NetKeeper 连接互联网所使用的账号名称。当 然,这只是部分与 lsa 相关的账户和密码信息,更多的信息还有待进一步挖掘。

步骤 9: 获取 SAM 表中所有的用户,输出结果如图 3-19 所示。

命令格式如下: volatility -f victor_PC_memdump.dmp --profile=Win7SP1x64 printkey -K "SAM\Domains\Account\Users\Names"



图 3-19 获取用户列表

步骤 10:使用 hashdump 命令获取注册表中用户密码的哈希值,具体运行结果如图 3-20 所示,下一步可使用哈希密码破解工具尝试破解密码。

命令格式如下: hashdump -y (system 的 virtual 地址) -s (sam 的 virtual 地址) 步骤 11: 使用 filescan 命令获取当前所有的文件列表,如图 3-21 所示。

<pre>b:\work\电子取证\内存取证>volatility -f victor_PC_memdump.dmpprofile=Win7SP1x64 hashdump -y 0xfffff8a000024010 -s 0xf fff8a000300010 'olatility Foundation Volatility Framework 2.6 dministrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0::: buest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0::: rictor:1001:aad3b435b51404eeaad3b435b51404ee:ec042512edb5cc251bc9904d2e55fa25::: iomeGroupUser\$:1002:aad3b435b51404eeaad3b435b51404ee:ec042512edb5cc251bc9904d2e55fa25::: iily:1003:aad3b435b51404eeaad3b435b51404ee:ec042512edb5cc251bc9904d2e55fa25::: simon:1004:aad3b435b51404eeaad3b435b51404ee:ec042512edb5cc251bc9904d2e55fa25:::</pre>							
				图 3-20 用户密码哈希值			
D:\work\电子取证\内 Volatility Foundati Offset(P)	存取证> on Vola #Ptr	volatil tility #Hnd	lity -f Framewo Access	victor_PC_memdump.dmp — profile=Win7SP1x64 filescan rk 2.6 Name			
0x000000007d400b30	3	0	RW-rwd	\Device\HarddiskVolume3\\$Directory			
0x00000007d402240	2	ĩ	R-rwd	\Device\HarddiskVolume4\			
0x00000007d4048d0	5	0	R-r-d	\Device\HarddiskVolume3\Windows\SysW0W64\msvbym60.dll			
0x000000007d4093c0	2	0	RW-rwd	\Device\HarddiskVolume3\\$Directory			
0x00000007d409f20	17	1	R-r-d	\Device\HarddiskVolume3\Windows\System32\zh-CN\WinSATAPI.dll.mui			
0x000000007d40ade0	6	0	R-rwd	\Device\HarddiskVolume3\Windows\Fonts\malgun.ttf			
0x000000007d40b650	1	1	R-r-d	\Device\HarddiskVolume3\Windows\SysWOW64\zh-CN\kernel32.dll.mui			
0x000000007d40c970	19	0	RW-rwd	\Device\HarddiskVolume3\\$Directory			
0x00000007d40ddd0	1	1	R-r-d	\Device\HarddiskVolume3\Windows\SysWOW64\zh-CN\kernel32.dll.mui			
0x00000007d40f370	11	0	R-r-d	\Device\HarddiskVolume3\Program Files (x86)\Baofeng\StormPlayer\diag.dll			
0x000000007d4113c0	2	0	RW-rwd	\Device\HarddiskVolume3\\$Directory			
0x000000007d411630	1	1	R-r-	\Device\HarddiskVolume3\Windows\Registration\R0000000006.clb			
0x000000007d411c80	17	1	RW-rw-	\Device\HarddiskVolume3\Windows\ServiceProfiles\NetworkService\AppData\Local\Mic			
rosoft\Windows\Temp	orary In	nternet	Files	Content. IE5\index. dat			
0x000000007d413ae0	16	0	R-r-	\Device\HarddiskVolume3\Windows\inf\acpi.PNF			
0x000000007d418a70	17	1	RW-rw-	\levice\HarddiskVolume3\Windows\ServiceProfiles\NetworkService\AnnData\Local\Mic			

图 3-21 文件列表

3.2.4 实验小结

内存取证作为计算机取证科学的一个重要分支,在网络攻击、网络犯罪调查等方面有重 要且不可替代的作用和应用前景,已成为信息安全研究者所关注的热点研究领域。本实验 旨在让读者掌握基本的内存数据获取与分析方法。除了掌握常见的 Volatility 命令外,更 重要的是具备一定的侦查思维,读者可多选取几个内存样本进行分析,尤其是开源的问题样 本,分析的方式和思路参照但不局限于本实验。

3.3 注册表分析取证

3.3.1 预备知识: 注册表

1. 注册表基础知识

注册表是 Windows 系统存储关于计算机配置信息的中央数据库,在系统中起着核心作 用,存放有计算机硬件和软件的配置信息、应用软件和文档文件的关联关系以及各种网络状态信息和其他数据,可以说计算机上所有针对硬件、软件、网络的操作都是源于注册表的。 同时它也是一个信息丰富的证据库,所以对电子数据取证非常重要。电子数据取证中,很多 证据都是直接来源于注册表的,例如用户账号、访问记录、软件的运行历史等都是取证工作 中非常重要的信息。因此,正确提取注册表中的有效数据将对取证工作大有帮助。

早期的注册表是以 ini 为扩展名的文本文件的配置文件,从 Windows 95 操作系统开始,才逐渐形成了注册表,Windows NT 是第一个从系统级别广泛使用注册表的操作系统,并在其后的操作系统中继续沿用至今。

要了解注册表,首先打开注册表编辑器,用户可以通过"Win+R"键打开命令提示界面, 输入 regedit 进入注册表编辑器,如图 3-22、图 3-23 所示。

@ 运行	×
Windows 将根据你所能 文件夹、文档或 Intern	俞入的名称,为你打开相应的程序、 et 资源。
+TIT(O)	

图 3-22 运行窗口打开注册表编辑器

注册表编辑器		×
文件(F) 编辑(E) 查看(V) 收藏夹(A) 帮助(H)		
十算机\HKEY_CLASSES_ROOT		
 ◆● 计算机 > HKEY_CLASSES_ROOT > ■ HKEY_CURRENT_USER > ■ HKEY_LOCAL_MACHINE > ■ HKEY_USERS > ■ HKEY_CURRENT_CONFIG 	名称 •••••(默认)	

图 3-23 注册表编辑器

在注册表编辑器左侧窗格的定位区域,每一个文件夹表示注册表中的项,项又包括子项 和值项,项和子项的关系就像目录可以包含子目录一样。值项也称为键值,类似硬盘上的树 状目录的末端文件,项和子项可以包括一个和多个值项。值项由名称、数据类型和数值三部 分组成,其格式为:"名称:类型:数据"。

预定义项,是代表注册表中的主要部分的项,是指在注册表中以 HKEY 作为前缀的文件夹,位于注册表树状结构的最顶层。预定义项类似于硬盘上的根目录,Windows 2000/XP 及以上的注册表编辑器中有五大预定义项,分别为:

① HKEY_CLASSES_ROOT。

包含了启动应用程序所需的全部信息,包括文件扩展关联信息及 OLE 数据库,存储在 这里的信息可确保使用 Windows 资源管理器打开文件时能打开正确的程序。

② HKEY_USERS。

包含了计算机上的所有以活动方式加载的用户信息(如用户在该系统中设置的口令、标 识等)和默认配置文件,默认配置文件决定了没有人登录时,计算机如何响应。

③ HKEY_LOCAL_MACHINE。

包含了本地计算机的配置信息(用于任何用户),如软件、硬件及安全。

④ HKEY_CURRENT_USER。

包含了当前登录用户的配置信息。用户的文件夹、屏幕颜色和"控制面板"设置都存储 在这里。

5 HKEY_CURRENT_CONFIG.

在启动过程中动态创建,包含系统启动时的硬件相关的配置信息。

配置单元是作为文件出现在系统注册表的一部分,位于 HKEY_LOCAL_MACHINE 和 HKEY_USERS 两个预定义项下,是项、子项和值的离散体,它位于注册表层的顶部。配置单元是一个文件,可以通过注册表编辑器中"加载配置单元"和"卸载配置单元"选项,从一个系统移动到另一个系统。

注册表配置单元是注册表中的一组项、子项和值,它有一组包含其数据备份的支持文件,如表 3-3 所示。配置单元(HKEY_CURRENT_USER 除外)的支持文件都位于Windows\System32\Config文件夹中,包括SAM、Security、System、Software、Default,称为系统注册表文件,包含Hardware(硬件)、User Settings(用户配置)、Software(软件)、System configuration(系统配置等信息);HKEY_CURRENT_USER 的支持文件位于Windows\Users\用户名文件夹中,包含NTUSER.DAT,称为用户注册表文件,每一个用户都有一个注册内容,能够记录用户活动的相关细节,是取证应该检查的关键内容。

注册表配置单元	相关文件
HKEY_LOCAL_MACHINE\SAM	SAM, SAM. log, SAM. sav
HKEY_LOCAL_MACHINE\Security	SECURITY, Security. log, Security. sav
HKEY_LOCAL_MACHINE\Software	SOFTWARE, Software. log, Software. sav
HKEY_LOCAL_MACHINE\System	SYSTEM, System. alt, System. log, System. sav
HKEY_USERS\DEFAULT	Default, Default. log, Default. sav
HKEY_CURRENT_CONFIG	System, System. alt, System. log, System. sav, Ntuser. dat, Ntuser. dat. log

表 3-3 配置单元文件

2. 注册表取证

注册表给取证人员提供了大量的系统配置信息和用户使用信息。通过分析注册表,可 以提供一份详尽的嫌疑人计算机设备的简要报告,包括硬件配置、系统配置、使用者信息、用 户账号、外置设备等。

常见的注册表取证分析项有:

- ① 用户账户及安全设置(SAM/SECURITY)。
- 用户账号/SID;
- 登录时间、登录次数;
- 最后登录时间等。
- ② 系统及软件信息(SYSTEM/SOFTWARE)。
- 系统信息(OS版本、安装日期、最后关机时间等);
- 时区信息(Time Zone);
- 硬件信息/服务列表;
- 网络配置信息/共享文件夹信息;

- 应用程序运行痕迹记录;
- USB设备使用记录等。

③用户相关信息(NTUSER.DAT)。

最近打开的文件记录(MRU, RecentDocs)。

3.3.2 实验目的与条件

1. 实验目的

通过本实验,让读者在了解注册表基础知识和常见的注册表分析项的基础上,学会使用 常见的注册表分析工具,掌握常用的注册表键值的取证方法。

2. 实验条件

本实验所需要的软硬件清单如表 3-4 所示。

序 号	设备	数量	参数
1	取证工作站	1台	Windows XP 以上
2	U 盘	1 个	无
3	WRR. exe	1个	无

表 3-4 注册表分析取证实验清单

3.3.3 实验过程

读者在做此实验内容前,需要在自己的计算机上进行如下操作,作为实验素材。

① 在 IE 地址栏分别输入任意 2 个网址,并浏览查看。

② 单击"开始"→"运行",分别执行 regedit、msconfig、eventvwr 命令。

③ 依次单击"开始"→"搜索"→"文件或文件夹",并执行 2 次搜索任务(搜索内容自己 定,例如可以搜索 C 盘所有 bmp 图片或者包含有 *** 内容的文件)。

④ 打开并简单查看"**.pdf"。

⑤将U盘插入到自己的主机上。

1. 打开注册表编辑器查看相应注册表项内容

步骤 1: 打开注册表编辑器中如下项,查看通过标准的文件"打开/保存"对话框所操作 文件的历史记录(MRU为 most recently used 缩写),如图 3-24 所示。

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU

步骤 2: 打开注册表编辑器中如下项,查看通过 Windows 资源管理器打开或者运行的 最近的文件,如图 3-25 所示。

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs

步骤 3: 打开注册表编辑器中如下项,查看通过"开始"→"运行"方式执行的命令,如 图 3-26 所示。

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU

步骤 4: 打开注册表编辑器中如下项,查看系统中安装的程序信息,如图 3-27 所示。

HKLM\Software\Microsoft\Windows\CurrentVersion\Uninstall

值得注意的是,运行于 64 位系统下的 32 位应用程序默认操作 32 位注册表项(即被重 定向到 WOW6432Node 下的子项),而 64 位应用程序才是上述操作的直观子项。

÷

BitBucket ·	名称	类型	数据	
BrowseNewProcess	(数认)	REG_SZ	(数值未设置)	
CabinetState	22 0	REG_BINARY	14 00 1f 50 e0 4f d0 20 ea 3a 69 10 a2 d8 08	
CD Burning	35 1	REG BINARY	14 00 1f 50 e0 4f d0 20 ea 3a 69 10 a2 d8 08	
CIDOpen	## MRUListEx	REG BINARY	01 00 00 00 00 00 00 00 ff ff ff ff	
CIDSave	-SQ			
L CLSID				
ComDlg32				
- CIDSizeMRU				
- JirstFolder				
- LastVisitedPidIMRU				
LastVisitedPidIMRULegacy				
OpenSavePidIMRU				
🕼 dll				
- 😹 dsw 🗉				
- de exe				
GHO				
- i txt				
- wmx				
Discardable				
FileExts				
HideDesktopIcons				
LowRegistry				
MenuOrder				
Modules				
B MountDointe?	e			

图 3-24 最近使用文件列表 1

> MyComputer	^ 名称	类型	数据
- NDUP	产(数 3)	REG SZ	(数值未设置)
- OperationStatusManager	22 O	REG BINARY	6c 51 89 5b 80 62 2f 67 66 5b d1 79 33 75 a5 6
- Package Installation	322 1	REG BINARY	63 00 68 00 61 00 70 00 33 00 2d 00 57 00 69 0
> PhotoPrintingWizard	22 10	REG BINARY	31 00 30 00 31 00 8b 73 d7 5f 3a 5f 2e 00 64 00
✓ RecentDocs	22 11	REG BINARY	d5 6c ba 4e c1 8b 66 4e 7f 4f 28 75 a1 5b 79 62
7z	課 12	REG BINARY	63 00 68 00 61 00 70 00 32 00 2d 00 35 75 50 5
caj	题13	REG BINARY	31 00 31 00 2e 00 31 00 32 00 2e 00 64 00 6f 00
dat	322 14	REG BINARY	3a 53 57 57 fe 94 9f 53 06 74 ca 53 73 51 2e 95
Joc	課15	REG BINARY	0a 30 51 7f dc 7e 89 5b 68 51 0e 4e 67 62 d5 6
.docx	歸 16	REG BINARY	2f 65 91 64 50 67 99 65 ee 76 55 5f 31 00 2e 00
at	2217	REG BINARY	2f 65 91 64 50 67 99 65 ee 76 55 5f 32 00 2e 00
- inf	22 18	REG BINARY	31 00 30 00 33 00 20 00 4e 67 73 82 cb 79 2e 0
- iso	課 19	REG BINARY	9e 5b 8c 9a 00 4e 1a ff d6 53 c1 8b fa 57 40 78
- ipg	22	REG BINARY	44 96 f6 4e 32 00 2e 00 5f 6c cf 82 01 77 d8 9a
- KDH	324 3	REG BINARY	3a 53 57 57 fe 94 71 51 c6 8b 97 7b d5 6c 2d 0
.log	## 4	REG BINARY	0a 30 35 75 50 5b 70 65 6e 63 d8 52 e5 67 d6 5
- 🔚 .md5	## 5	REG BINARY	35 75 50 5b 70 65 6e 63 d8 52 e5 67 d6 53 c1 8
- ankv	226	REG BINARY	10 30 03 80 df 5b b9 65 48 68 11 30 35 75 50 5
- 🛄 .mp4	SH 7	REG BINARY	35 75 50 5b 70 65 6e 63 d8 52 e5 67 d6 53 c1 8
.pdf	(1) (1) (1) (1) (1) (1) (1) (1) (1) (1)	REG BINARY	10 30 03 80 df 5b b9 65 48 68 11 30 35 75 50 5
png	22 9	REG BINARY	10 30 03 80 e5 67 b9 65 48 68 11 30 35 75 50 5
- ppt	# MRUListEx	REG BINARY	05 00 00 00 09 00 00 00 08 00 00 04 00 00 0

图 3-25 最近使用文件列表 2

CIDOpen	•	名称	类型	数据
▷ - ↓ CIDSave		ab)(默认)	REG_SZ	(数值未设置)
Þ- 🔐 CLSID		aba	REG_SZ	mstsc\1
D- ComDlg32		abb	REG_SZ	cmd\1
Discardable		abc	REG_SZ	regedit\1
FileExts HideDesktop LowRegistry MenuOrder Modules MoutPoints NewShortcut RecentDocs RunMRU SearchPlatfor	2	MRUList	REG_SZ	cba

图 3-26 cmd 中运行命令的历史记录

> Syncmgr	名称	英型	数据
SysPrepTapi	(USB)	REG SZ	(数值未设置)
SystemProtectedUserData	ab AuthorizedCDFPrefix	REG SZ	
Tablet PC	ab Comments	REG SZ	Caution. Removing this product might prevent some a
Telephony	ab Contact	REG SZ	
ThemeManager	ab DisplayName	REG SZ	Microsoft Visual C++ 2017 x64 Minimum Runtime - 14
Themes	ab DisplayVersion	REG SZ	14.13.26020
TouchKeyboard	75 EstimatedSize	REG DWORD	0x0000086c (2156)
UFH	ab HelpLink	REG EXPAND SZ	http://go.microsoft.com/fwlink/?LinkId=133405
	ab HelpTelephone	REG SZ	
- (1CEAC85D-2590-4760-800F-8DE5E91F37	ab InstallDate	REG SZ	20211012
(21406001-0A/6-4336-8340-F403/C003:	AB InstallLocation	REG SZ	
22100004-4022-533C-8098-374953100	(ab) InstallSource	REG SZ	C:\ProgramData\Package Cache\{221D6DB4-46E2-333
(2E171580-9C56-4A25-A5D5-CBRAA025R	20 Language	REG DWORD	0x00000409 (1033)
- (41D2D254-D869-4CD8-B440-5DF49083C	ab ModifyPath	REG EXPAND SZ	MsiExec.exe /X(221D6DB4-46E2-333C-B09B-5F49351D
(5016990D-7F61-4A20-9451-A915D6616E	77 NoModify	REG DWORD	0x00000001 (1)
- (788371EA-0802-40AD-85D0-218E107E3	ab Publisher	REG SZ	Microsoft Corporation
- (900D0BCD-0B86-4DAA-8639-89BE70445	ab Readme	REG SZ	
- [] (90160000-007E-0000-1000-0000000FF1C	ab Size	REG SZ	
- [] {90160000-008C-0000-1000-0000000FF1C	75 SystemComponent	REG DWORD	0x00000001 (1)
- 90160000-008C-0804-1000-0000000FF1C	ab UninstallString	REG EXPAND SZ	MsiExec.exe /X(221D6DB4-46E2-333C-B09B-5F49351D
- (A0983640-26D2-4CD8-A512-747BF3CF3F	ab URLInfoAbout	REG SZ	
- A0CDAD3D-0329-4E3E-8DC1-30E333D6!	ab URLUpdateInfo	REG SZ	
- 428339C8-E641-4CCE-A316-56F405D1C2	11 Version	REG DWORD	0x0e0d65a4 (235759012)
- [] {B2FE1952-0186-46C3-BAEC-A80AA35AC:	11 Version Major	REG DWORD	0x0000000e (14)
- (B2FE1952-0186-46C3-BAEC-A80AA35AC	10 VersionMinor	REG DWORD	0x0000000d (13)
- (B2FE1952-0186-46C3-BAEC-A80AA35AC:	25 WindowsInstaller	REG DWORD	0x00000001 (1)
- [] {B2FE1952-0186-46C3-BAEC-A80AA35AC			

- 电子数据取证实训

图 3-27 安装的应用程序信息

步骤 5: 打开注册表编辑器中如下项,查看 32 位应用程序(如 WeChat)的相关信息,如 图 3-28 所示。

HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall

is (x86)\Tencent\WeChat\WeChat.exe 9573) .com 5 (x86)\Tencent\WeChat 保公司 es (x86)\Tencent\WeChat\Uninstall.ex



步骤 6: 打开注册表编辑器中如下项,查看自动运行的程序,如图 3-29 所示。 HKLM\Software\Microsoft\Windows\CurrentVersion\Run

> PrecisionTouchPad ^	名称	美型	数据
- PreviewHandlers	(版认)	REG SZ	(数值未设置)
- Privacy	ab Everything	REG SZ	*C:\Program Files\Everything\Everything.exe* -startup
> PropertySystem	ab RtkAudUService	REG SZ	*C:\Windows\System32\DriverStore\FileRepository\realtekservice.inf amd64 2913
> Proximity	ab SecurityHealth	REG EXPAND SZ	%windir%\system32\SecurityHealthSystray.exe
> PushNotifications	ab SunloginClient	REG SZ	*C:\Program Files\Oray\SunLogin\SunloginClient\SunloginClient.exe*cmd=autor
> qua QualityCompat	ab WavesSvc	REG_SZ	*C:\Windows\System32\DriverStore\FileRepository\wavesapo10de.inf_amd64_4dc
> Reliability			
> ReserveManager			
> RetailDemo			
Run			
- RunOnce			
- SecondaryAuthFactor			
> Security and Mainten			



步骤 7: 打开注册表编辑器中如下项,查看浏览器地址栏中键入的 URL 地址和文件路 径,如图 3-30 所示。

HKCU\Software\Microsoft\Internet Explorer\TypedURLs

- Repld	^	名称	类型	数据
> SearchScopes		(武法)	REG_SZ	(数值未设置)
- Security		ab url1	REG SZ	http://go.microsoft.com/fwlink/p/?LinkId=255141
- Services		19705		0.007 D. 10701
- Settings				
- Setup				
- SQM				
- Suggested Sites				
> TabbedBrowsing				
> Toolbar				
TypedURLs	1.00			
URLSearchHooks				
- VersionManager				
Zoom				

图 3-30 浏览器地址栏中键入的 URL 地址和文件路径

步骤 8: 打开注册表编辑器中如下项,查看计算机上曾经使用过的所有 USB 设备,如 图 3-31 所示。

HKLM\SYSTEM\ControlSet001\Enum\USBSTOR



图 3-31 计算机上使用过的所有 USB 设备

步骤 9: 打开注册表编辑器中如下项,查看计算机连接过的无线接入点的 GUID 列表, 如图 3-32 所示。

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles



图 3-32 计算机连接过的无线接入点

步骤 10: 打开注册表编辑器中如下项,查看每个接口的 IP 地址及相关信息,如图 3-33 所示。

HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces

>	SVSVC	名称	運動	数据
>	swenum	ab (2004)	REG SZ	(数值未设置)
	swprv	AddressType	REG DWORD	0x00000000 (0)
1	Synth3dVsc	脚 DhcpConnForceBroadca	REG DWORD	0x00000000 (0)
2	SysMain	ab DhcpDefaultGateway	REG MULTI SZ	172.17.121.254
2	SystemEventsBroker	想 DhcpGatewayHardware	REG BINARY	ac 11 79 fe 06 00 00 00 00 1a a9 17 83 73
2	TabletInputService	#DhcpGatewayHardwareC	REG DWORD	0x00000001 (1)
1 2	TapiSrv	DhcpInterfaceOptions	REG BINARY	fc 00 00 00 00 00 00 00 00 00 00 00 00 00
×.	Терір	ab DhcpIPAddress	REG SZ	172.17.121.29
	Linkage	ab DhcpNameServer	REG SZ	172.17.200.129 172.17.200.127 114.114.114.114
	Parameters	ab DhcpServer	REG SZ	172.17.121.254
	DNSPerinteredAdapterr	ab DhcpSubnetMask	REG SZ	255.255.255.0
		ab DhcpSubnetMaskOpt	REG MULTI SZ	255.255.255.0
	(48b807f5-6720-42b8-b40a-ccc130acbb7e)	ab Domain	REG SZ	
11	(5b01516e-2ac5-11ec-973a-806e6f6e6963)	24 EnableDHCP	REG DWORD	0x00000001 (1)
	- (61d476e1-3ab4-4ce1-a860-f83a3b6b6472)	# IsServerNapAware	REG DWORD	0x00000000 (0)
	(78c72ada-5af9-4e47-8280-c5f34d5d401e)	#Lease	REG DWORD	0x00015180 (86400)
	- (92222dd7-73b7-4201-9d27-8b59422b1d6e)	部 LeaseObtainedTime	REG DWORD	0x62451119 (1648693529)
	- (ab89191f-c8b8-417c-affa-9add55e8d626)	200 LeaseTerminatesTime	REG DWORD	0x62466299 (1648779929)
	{ada4604d-0477-4ac8-b399-2768af0b1d5a}	ab NameServer	REG SZ	
	- NsiObjectSecurity	1840 T1	REG DWORD	0x6245b9d9 (1648736729)
	- PersistentRoutes	188 T2	REG DWORD	0x62463869 (1648769129)
1	> Winsock		0.07000=00010707070	

图 3-33 每个接口的 IP 地址及相关信息

步骤 11: 打开注册表编辑器中如下项, 查看计算机连接的默认打印机信息, 如图 3-34 所示。

- Fonts	^ 名称	美型	数据
> HostActivityManager	()()()()()()()()()()()()()()()()()()()	REG_SZ	(数值未设置)
> III ICM	ab Device	REG SZ	Brother HL-5450DN series Printer, winspool, Ne06:
> MsiCorruptedFileRecovery	# IsMRUEstablished	REG DWORD	0x00000001 (1)
> Network	24 LegacyDefaultPrinterMode	REG DWORD	0x00000000 (0)
- PrinterPorts	ab MenuDropAlignment	REG SZ	0
> TileDataModel	~		
> TokenBroker			
 Windows 			
- InteractiveControl			
> Pen			
Winlogon			
> Windows Script			
> Windows Search			
> Windows Security Health			
> Wisp			

图 3-34 默认打印机

2. 使用 WRR(Windows Registry Recovery)工具查看注册表文件

步骤 1:导出计算机中的注册表文件,包括 SAM、Software、System 等。

步骤 2: 使用 WRR 工具打开注册表文件 SAM,查看计算机中所有用户信息,如图 3-35 所示。

步骤 3: 使用 WRR 工具打开注册表文件 Software, 查看计算机中安装的软件信息, 包括操作系统信息, 如图 3-36、图 3-37 所示。

步骤 4: 使用 WRR 工具打开注册表文件 System,查看系统配置相关信息,如服务及驱动、网络配置、防火墙设置等,如图 3-38、图 3-39、图 3-40 所示。

其他信息操作类似,不再一一列出。





1	Mi <u>F</u> ile	TeC Windows Registry Re e Options Explore W	covery - [software] (indows <u>H</u> elp		 •	×
0	SAM	1 Software	System	default 🕼 SECURITY		
File II		Export to REGEDIT4 form	General Installed	I Software Hot Fixes	 	_
•		File Information	Owner:	Microsoft Windows AP 微软用户		
	è	Security Records	Organization:	微软中国	 	
	0	SAM	Product ID:	76481-640-8834005-23332	 	
	8.	Windows Installation	Product Key:	MRX3F-4789T-24873-KWKMF-RPWBY	 	
)#	Hardware	Product Version: Install Date:	Uniprocessor Free 5.1.2600.xpsp_sp3_gdr.101209-1647 2011/5/9 4:31:40	 	
		User Data	Service Pack:	Service Pack 3	 	Ĩ
Ę		Startup Applications	System Root:	C:\WINDOWS	 	۲,
v plo	63	Services and Drivers				_
"	0	Network Configuration	Last Boot:	<no found="" information=""></no>	 	
	di	Windows Firewall Settings	Last Shutdown:	<no found="" information=""></no>		
		Environment				
	6	Shell Folders				
	3	Outlook Express				
	2	Raw Data				

图 3-36 Software 注册表文件中操作系统信息

86 — 电子数据取证实训 -

0	SAM		🗑 software	system	🗑 defa	ult		SECURITY				
•	I‰ E	Export to REGEDIT4 form		General In	stalled Softw	vare	lot Fixe	s				
	Export Data		Name 局暴风影音 V3.10.07.30		Version		Company 360安全中心	Datetime 20101011	Uninstall "C:\Program Files\St D:\Program Files\360	ormII\unin: D\360safe\	s000.i 🔺	
	響 F ふ S	File Information	tion	局 360杀毒 局 Adobe Flash	Player 10	2.0.0.1	331 31.26	360安全中心 Adobe Systems		d:\Program Files\360 C:\WINDOWS\syste)\360sd\un m32\Macro	inst.e medV
	t s	SAM		局 AutoCAD 2002		15.0.6	.030	Autodesk	20020430	MsiExec.exe /I{5783 C:\Program Files\Au	F2D7-010 toCAD 200	1-080 2\unir
	€ ۷	Windows Ins	stallation	C-Dilla Licence	e Manage	1.0.0.1				C:\C_DILLA\setup\cdunin16.exe		e t.exe
)н н	lardware		Free Launch	Bar T Framew	1.0	777	TrueSoft Microsoft Corp	20110509	"C:\Program Files\Fr	eeLaunchB	lar\Un
	D C	Jser Data	lications	Microsoft .NE	T Framew	2.0.30	727	Microsoft Corp	20110309	C:\WINDOWS\Micros	soft.NET\F	ramev
xplorer	ing s	Services and	d Drivers	Microsoft .NE	Microsoft .NET Framew	1.1.50	/2/	Microsoft Corp	20110509	C:\WINDOWS\Micros	soft.NET\F	ramev
	Q N	Network Cor	nfiguration	Microsoft Ker	nel-Mode			Microsoft Corp	20110509	"C:\WINDOWS\\$NtL	IninstallWd	f0100
	Ø v	Vindows Fir	ewall Settings	Microsoft Off	ice Protes ice Word 2	11.0.8	173.0	Microsoft Corp Microsoft	20110622 20101011	MsiExec.exe /I{901 MsiExec.exe /I{C21	10804-6000 82670-EEF	0-11D 5-4B1
	B) E	Environment	t	Microsoft Rep	port Viewe	9.0.21	022	Microsoft Corp	20110509			
	🖻 s	Shell Folders		Microsoft Rep	port Viewe	5.0.22		Microsoft Corp	2010000	C:\WINDOWS\Micros	soft.NET\F	ramev
	S 0	Outlook Exp	ress	局 Microsoft 报	表查看器 0.01			Microsoft Corp		C:\WINDOWS\Micros RunDll32 advpack.dl	soft.NET\F I,LaunchIN	ramev FSect
	3 R	Raw Data		NVIDIA Drive	rs					C:\WINDOWS\syste	m32\nvuni	nst.ex

图 3-37 Software 注册表文件中安装软件信息

SAM	software	system (🗑 default	SECURITY			
Export	to REGEDIT4 form	Services Drivers	1			E. 2015.0	
	D-1-	Name 🔺	Descri	pton	2.329	Туре	Startup
Export I	Data	NET Runtime Opti	miz Micros	oft .NET Framework NG	EN	OwnProcess	Manu /
R Ele Tofe	rmation	%。360 杀毒全盘扫描	酬… scan			SharedProcess	Manu
S File Information		%。360 杀毒实时防护服务 360 杀毒实时防护服务程序,实时监控病毒…				Node	Autor
Security	Records	Walerter 通知所选用户和计算机有关系统管理级警				SharedProcess	Disab
db		Application Layer (Gat 为Int	ernet 连接共享和 Wind	OwnProcess	Disab	
SAM		% Application Management 提供软件安装服务,诸如		次件安装服务,诸如分	派,发行以及…	SharedProcess	Manu
R Window	s Installation	State Ser	vice Provid	les support for out-of-p	rocess session st	OwnProcess	Manu
		Automatic Updates	\$ 允许	下载并安装 Windows 更	SharedProcess	Disab	
Hardwa	re	Background Intellig	gent 在后线	台传输客户端和服务器	之间的数据。	SharedProcess	Manu
🗐 User Da	ita	ClipBook	启用"	剪贴簿查看器"储存信	息并与远程计算	OwnProcess	Disab
(<u>11</u>) 030 00		COM+Event Syste	em 支持	系统事件通知服务(SEN	lS),此服务为订…	SharedProcess	Manu
Startup	Applications	COM+System App	olica 管理	基于COM+组件的配置	和跟踪。如果	OwnProcess	Manu
Canica	a and Drivere	Computer Browser	维护	网络上计算机的更新列	表,并将列表	SharedProcess	Autor
Service:	s and Drivers	Cryptographic Ser	a Cryptographic Services 提供三种管理服务:编录数据库服务,它确			SharedProcess	Manu
Q Network	k Configuration	DCOM Server Proc	ess 为DC	OM 服务提供加载功能	•	SharedProcess	Autor
All use to		BHCP Client	通过	主册和更改 IP 地址以及	GDNS 名称来管…	SharedProcess	Autor
Window Window	s Firewall Settings	🖏 Distributed Link Tra	acki 在计算	算机内 NTFS 文件之间	保持链接或在网	SharedProcess	Manu
Environ	ment	🖏 Distributed Transa	ctio 协调	跨多个数据库、消息队	列、文件系统	OwnProcess	Manu
		🖏 DNS Client	为此	十算机解析和缓冲域名	系统 (DNS) 名…	SharedProcess	Autor
C Shell Fo	lders	Error Reporting Se	rvice 服务	 	请下运行时允	SharedProcess	Disabi
Cuttook	Express	🖏 Event Log	启用者	生事件查看器查看基于	Windows的程	SharedProcess	Autor
		By Extensible Authent	tica foj Wi	ndows 客户端提供可扩	展身份验证协	SharedProcess	Manu

图 3-38 System 注册表文件中服务及驱动信息

¢

SAM	software	🕼 system 🕼 default 🕼	SECURITY
Export to R	REGEDIT4 form	Components TCP/IP	
Export Dat	a	□ 4 地注按 Adapter	Realtek PCIe FE Family Controller
		UseZeroBroadcast	0
File Information		EnableDeadGWDetect	1
		EnableDHCP	0
Security Re	ecords	IPAddress	192.168.1.20
the case		SubnetMask	255.255.255.0
SAM		DefaultGateway	192.168.1.1
😨 Windows Ir	nstallation	DefaultGatewayMetric	0
		NameServer	202.103.24.68,202.103.44.150
Hardware		RegistrationEnabled	1
Con Lines Date		RegisterAdapterName	0
Er: User Data		TCPAllowedPorts	0
Startup Ap	olications	UDPAllowedPorts	0
	<u></u>	RawIPAllowedProtocols	0
Services and	nd Drivers	DheeSequer	255 255 255 255
A Natwork Co	onfiguration	Lesse	E10
INCOVOR CO	omgurauon	LeaseObtainedTime	4DE2EA75
Windows Fi	irewall Settings	T1	4DE3017D
-		T2	4DE306C3
Servironmer	nt	LeaseTerminatesTime	4DF30885
Can Shell Folder	re	IPAutoconfigurationAddress	0.0.0.0
- SHELT OLDER		IPAutoconfigurationMask	255.255.0.0
Cutlook Ex	press	IPAutoconfigurationSeed	2A944404
-		AddressType	0
Raw Data		IsServerNapAware	0



6	File Options Explore V	Mindows Help				- 5	×			
0	SAM 🕼 software	system	🍘 default	SECURITY						
	Export to REGEDIT4 form	🗆 DomainProfile					^			
	Lig and a construction of the	AuthorizedAp	plications							
Ξ.	Export Data	%windir%	Wetwork Diagnost	tic\xpnetdiag.exe	%windir%Wetwork Diagnostic\xpnetdiag.exe:*:En	abl				
		Sowindir %	system32 sessing	r.exe	%windir%jsystem32jsessmgr.exe: "enabled:@xp:	sp2				
	File Information	C: Program	n Files (Tencent)Q	2000011.2.251.4001	C: Program Files (Tencent) QQVVubi (1.2.251.400) QC	200				
	Sacurity Pacorde	C: Program	n Files (Tencent)()	200011122251.4001	C: Program Files/Tencent/QQWubi/1.2.251.400/Q	2				
	By Security Records	C:\Program	n Files (Tencent)()	2000011.2.251.4001	C: Program Electron Color to Color C: Program Electron Color to C: Victor and C: Victo	2IIII				
	SAM	C:\Program	C. Program Files Tencent (QQWdbi (1.2.251.400 Q	200						
	•		Porte	2000111212011100111	c. Frogram ries (rencent (22 main (1.2.2.51.400 (2	2	1			
	Windows Installation	139:TCP	U.D.		139:TCP:*:Enabled:@xpsp2res.dll -22004		-11			
	June 1 and a second	445:TCP			445:TCP:*:Enabled:@xpsp2res.dll22005		9			
	jan Hardware	137:UDP			137:UDP: *:Enabled: @xpsp2res.dll22001					
	📰 User Data	138:UDP			138:UDP:*:Enabled:@xpsp2res.dll22002					
		StandardProfi	StandardProfile							
5	Startup Applications	AuthorizedApplications								
Por 1	8 Services and Drivers	%windir%	Wetwork Diagnost	tic\xpnetdiag.exe	%windir%Wetwork Diagnostic\xpnetdiag.exe:*:En	abl				
ă	Cos ou fices and prives	%windir%	\system32\sessmg	r.exe	%windir%\system32\sessmgr.exe:*:enabled:@xp	sp2				
	Network Configuration	C:\Program	n Files\Tencent\Q0	QWubi\1.2.251.400\	C:\Program Files\Tencent\QQWubi\1.2.251.400\Q	QW				
		C:\Program	m Files \Tencent \QC	2Wubi\1.2.251.400\	C:\Program Files\Tencent\QQWubi\1.2.251.400\Q0	QW				
	Windows Firewall Settings	C: Program	C:\Program Files\Tencent\QQWubi\1.2.251.400\Q0	QIm						
	D Environment	C:\Program	m Files\Tencent\Q(QWubi\1.2.251.400\	C:\Program Files\Tencent\QQWubi\1.2.251.400\Q	QIm				
	S Environment	C:\Program	n Files\Tencent\Q	2Wubi\1.2.251.400\	C:\Program Files\Tencent\QQWubi\1.2.251.400\Q0	QW				
	P Shell Folders	D: Program	n Files\360\360saf	e LiveUpdate360.exe	D:\Program Files\360\360safe\LiveUpdate360.exe:	*:E				
1	-	D:\Program	n Files\360\360saf	fe\safemon\360tray	D:\Program Files\360\360safe\safemon\360tray.ex	œ:				
	🔄 Outlook Express	C: Program	n Files (Tencent)QC	21/Bin 1/QQ.exe	C: Wrogram Files (Tencent) QQ Bin) QQ.exe: *: Enable	:				
		C: Program	n Files (Tencent QC	2/Bin Vaudt.exe	C: Wrogram Files (Tencent)QQ (Bin \audt.exe:*:Enab	led				
	Raw Data	C: Program	n Files bogouInput	t15.2.0.5374\Pinyin	C: program Files Sogournput (5.2.0.5374 PinyinUp.	ex				

图 3-40 System 注册表文件中防火墙设置信息

3.3.4 实验小结

通过本次实验的学习,读者了解注册表不仅仅是一个用于存储 Windows 系统用户、硬 件和软件的存储配置信息的数据库,更是计算机犯罪取证中的一个宝库。虽然常见的综合

性取证软件大都集成了注册表分析功能,但仍存在很多信息需要取证人员结合案情手工分 析。想要成为一名合格的计算机取证人员,必须要熟练运用和掌握注册表的相关知识。

3.4 Windows 事件日志取证

3.4.1 预备知识: Windows 事件日志

1. Windows 事件日志

从 Microsoft Windows NT 3.5 操作系统起,日志服务就一直存在于微软公司开发的 Windows 操作系统中。但是从 Microsoft Windows NT 6.0 操作系统(Windows Vista 与 Windows Server 2008)开始,微软公司采用了一种全新的日志(EVTX 日志)服务,EVTX 由 Windows 事件查看器创建,包含 Windows 记录的事件列表,以专有的二进制 XML 格式 保存。

Windows 事件日志文件保存在 C:\Windows\System32\winevt\Logs 路径中,如图 3-41 所示。

Image: Second		名称	修改日期	类型	大小
 OneDrive 図 Dell.evtx 2022/4/13 17:57 事件日志 1,028 KE WPS网盘 圖 HardwareEvents.evtx 2021/10/12 3:28 事件日志 68 KE 圖 Internet Explorer.evtx 2021/10/12 3:28 事件日志 68 KE 圖 Microsoft-Client-Licensing-Platform%4Admin.evtx 2022/4/13 17:48 事件日志 68 KE 圖 Microsoft-Client-Licensing-Platform%4Admin.evtx 2022/4/13 17:48 事件日志 68 KE 圖 Microsoft-Windows-AAD%4Operational.evtx 2022/3/1 14:15 事件日志 68 KE 圖 Microsoft-Windows-All-User-Install-Agent%4Admin 2021/10/12 3:28 事件日志 68 KE ○ 文档 圖 Microsoft-Windows-AppHost%4Admin.evtx 2021/10/12 3:28 事件日志 68 KE ○ 文档 I Microsoft-Windows-AppIost%4Admin.evtx 2021/10/12 3:28 事件日志 68 KE ○ 文档 I Microsoft-Windows-AppIost%4Admin.evtx 2021/10/12 3:28 事件日志 68 KE ○ 文档 I Microsoft-Windows-Application Server-Application. 2021/10/12 3:28 事件日志 68 KE □ apin I Microsoft-Windows-Application Server-Application. 2022/3/1 14:28 事件日志 68 KE □ DATA (D:) I Network Wicrosoft-Windows-Application-Experience%4Pro 2021/10/12 3:28 事件日志 68 KE I Microsoft-Windows-Application-Experience%4Pro 2021/10/12 3:28 事件日志 68 KE I Microsoft-Windows-Application-Experience%4Pro 2021/10/12 3:28 事件日志 68 KE I Microsoft-Windows-Application-Exp	A CARANTA	Application.evtx	2022/4/14 15:54	事件日志	6,212 KE
WPS网盘 Image: Figure 2 and the provided of the provid	OneDrive	Dell.evtx	2022/4/13 17:57	事件日志	1,028 KE
Internet Explorer.evtx 2021/10/12 3:28 事件日志 68 KE Image: Display Microsoft-Client-Licensing-Platform%4Admin.evtx 2021/10/12 3:28 事件日志 68 KE Image: Display Microsoft-Client-Licensing-Platform%4Admin.evtx 2022/4/13 17:48 事件日志 68 KE Image: Display Microsoft-Client-Licensing-Platform%4Admin.evtx 2022/3/1 14:15 事件日志 68 KE Image: Display Microsoft-Windows-AAD%4Operational.evtx 2022/3/1 14:15 事件日志 68 KE Image: Display Microsoft-Windows-ADP%4Operational.evtx 2021/10/12 3:28 事件日志 68 KE Image: Display Microsoft-Windows-Applot%4Admin.evtx 2021/10/12 3:28 事件日志 68 KE Image: Display Microsoft-Windows-Applot%4Admin.evtx 2021/10/12 3:28 事件日志 68 KE Image: Display Microsoft-Windows-Applot%4Admin.evtx 2021/10/12 3:28 事件日志 68 KE Image: Display Microsoft-Windows-Application Server-Application. 2021/10/12 3:28 事件日志 68 KE Image: Display Microsoft-Windows-Application Server-Application. 2022/3/1 14:28 事件日志 68 KE Image: Display Microsoft-Windows-Application Server-Application. <t< td=""><td>会 WPS网由</td><td>HardwareEvents.evtx</td><td>2021/10/12 3:28</td><td>事件日志</td><td>68 KE</td></t<>	会 WPS网由	HardwareEvents.evtx	2021/10/12 3:28	事件日志	68 KE
世地館 図 Key Management Service.evtx 2021/10/12 3:28 事件日志 68 KE 3 3D 对象 図 Microsoft-Client-Licensing-Platform%4Admin.evtx 2022/4/13 17:48 事件日志 1,028 KE 2 3D 对象 図 Microsoft-Client-Licensing-Platform%4Admin.evtx 2022/3/1 14:15 事件日志 68 KE 2 2011 図 Microsoft-Windows-AAD%4Operational.evtx 2022/3/1 14:15 事件日志 68 KE 2 2011 図 Microsoft-Windows-ADP/64Operational.evtx 2021/10/12 3:28 事件日志 68 KE 2 文档 図 Microsoft-Windows-ApPlotS%4Admin.evtx 2021/10/12 3:28 事件日志 68 KE 3 optimization Microsoft-Windows-ApplO%4Operational.evtx 2021/10/12 3:28 事件日志 68 KE 3 optimization Microsoft-Windows-ApplO%4Operation.evtx 2021/10/12 3:28 事件日志 68 KE 3 optimization Microsoft-Windows-Application Server-Application. 2021/10/12 3:28 事件日志 68 KE 3 optimization Microsoft-Windows-Application Server-Application. 2022/3/1 14:28 事件日志 68 KE 3 optimization Microsoft-Windows-Application Server-Application. 2022/3/1 14:28 事件日志 68 KE	and the of the	Internet Explorer.evtx	2021/10/12 3:28	事件日志	68 KE
③ 3D 对象 圖 Microsoft-Client-Licensing-Platform%4Admin.evtx 2022/4/13 17:48 事件日志 1,028 KE ■ 視頭 圖 Microsoft-Windows-AAD%4Operational.evtx 2022/3/1 14:15 事件日志 68 KE ■ 関片 圖 Microsoft-Windows-AAD%4Operational.evtx 2021/12/6 14:55 事件日志 68 KE ◎ 文档 圖 Microsoft-Windows-All-User-Install-Agent%4Admin 2021/10/12 3:28 事件日志 68 KE ◎ 文档 圖 Microsoft-Windows-AppHot%4Admin.evtx 2021/10/12 3:28 事件日志 68 KE ◎ 方舌 圖 Microsoft-Windows-AppIO%4Operational.evtx 2021/10/12 3:28 事件日志 68 KE ◎ 点面 I Microsoft-Windows-AppIO%4Operations.evtx 2021/10/12 3:28 事件日志 68 KE ◎ 点面 I Microsoft-Windows-AppICabion Server-Application 2021/10/12 3:28 事件日志 68 KE ◎ 点面 I Microsoft-Windows-Application Server-Applicatio 2022/3/1 14:28 事件日志 68 KE ◎ DATA (D:) I Microsoft-Windows-Application-Experience%4Pro 2021/10/12 3:28 事件日志 68 KE ◎ Network I Microsoft-Windows-Application-Experience%4Pro 2021/10/12 3:28 事件日志 68 KE ◎ Network I Microsoft-Windows-Application-Experience%4Pro <t< td=""><td>🛄 此电脑</td><td>Key Management Service.evtx</td><td>2021/10/12 3:28</td><td>事件日志</td><td>68 KE</td></t<>	🛄 此电脑	Key Management Service.evtx	2021/10/12 3:28	事件日志	68 KE
■ 視频 圖 Microsoft-Windows-AAD%4Operational.evtx 2022/3/1 14:15 事件日志 68 KE ■ 聞片 圖 Microsoft-Windows-AllJoyn%4Operational.evtx 2021/12/6 14:55 事件日志 68 KE ◎ 文档 圖 Microsoft-Windows-All-User-Install-Agent%4Admi 2021/10/12 3:28 事件日志 68 KE ● 下载 圖 Microsoft-Windows-AppHost%4Admin.evtx 2021/10/12 3:28 事件日志 68 KE ● 方音乐 圖 Microsoft-Windows-AppIcational.evtx 2021/10/12 3:28 事件日志 68 KE ■ dicrosoft-Windows-AppIcational.evtx 2021/10/12 3:28 事件日志 68 KE ■ dicrosoft-Windows-Application Server-Application. 2021/10/12 3:28 事件日志 68 KE ■ dicrosoft-Windows-Application Server-Application. 2022/3/1 14:28 事件日志 68 KE ■ DATA (D:) 圖 Microsoft-Windows-Application-Experience%4Pro 2021/10/12 3:28 事件日志 68 KE ■ Network 圖 Microsoft-Windows-Application-Experience%4Pro 2021/10/12 3:28 事件日志 68 KE	🧊 3D 对象	Microsoft-Client-Licensing-Platform%4Admin.evtx	2022/4/13 17:48	事件日志	1,028 KE
図片 図 Microsoft-Windows-AllJoyn%4Operational.evtx 2021/12/6 14:55 事件日志 68 KE 文档 Microsoft-Windows-All-User-Install-Agent%4Admi 2021/10/12 3:28 事件日志 68 KE 下載 Microsoft-Windows-AppHost%4Admin.evtx 2021/10/12 3:28 事件日志 68 KE 声音乐 Microsoft-Windows-AppIcabilityEngine%4Operational.evtx 2021/10/12 3:28 事件日志 68 KE 画面 Microsoft-Windows-AppIcabilityEngine%4Operational.evtx 2021/10/12 3:28 事件日志 68 KE 画面 Microsoft-Windows-ApplicabilityEngine%4Operation 2022/10/12 3:28 事件日志 68 KE 画面 Microsoft-Windows-Applicabion Server-Application. 2022/3/1 14:28 事件日志 68 KE DATA (D:) Microsoft-Windows-Application-Experience%4Pro 2022/3/1 14:28 事件日志 68 KE Network Microsoft-Windows-Application-Experience%4Pro 2022/3/1 14:28 事件日志 68 KE	📓 视频	Microsoft-Windows-AAD%4Operational.evtx	2022/3/1 14:15	事件日志	68 KE
図 文档 圖 Microsoft-Windows-All-User-Install-Agent%4Admi 2021/10/12 3:28 事件日志 68 KE ● 下號 圖 Microsoft-Windows-AppHost%4Admin.evtx 2021/10/12 3:28 事件日志 68 KE ● 下號 圖 Microsoft-Windows-AppHost%4Admin.evtx 2021/10/12 3:28 事件日志 68 KE ● 首乐 圖 Microsoft-Windows-AppIcabilityEngine%4Operati 2021/10/12 3:28 事件日志 68 KE ■ 直面 圖 Microsoft-Windows-ApplicabilityEngine%4Operati 2021/10/12 3:28 事件日志 68 KE ■ DATA (D:) 圖 Microsoft-Windows-Application-Experience%4Pro 2022/1/12 19:12 事件日志 68 KE ■ Network Microsoft-Windows-Application-Experience%4Pro 2022/10/12 3:28 事件日志 68 KE		Microsoft-Windows-AllJoyn%4Operational.evtx	2021/12/6 14:55	事件日志	68 KE
■ Netrosoft-Windows-AppHost%4Admin.evtx 2021/10/12 3:28 事件日志 68 KE ● 下號 ■ Microsoft-Windows-AppI0%4Operational.evtx 2021/10/12 3:28 事件日志 68 KE ● 音乐 ■ Microsoft-Windows-AppICabilityEngine%4Operati 2021/10/12 3:28 事件日志 68 KE ● 直面 ■ Microsoft-Windows-AppIcabilityEngine%4Operati 2021/10/12 3:28 事件日志 68 KE ■ 点面 ■ Microsoft-Windows-ApplicabilityEngine%4Operati 2022/3/11 14:28 事件日志 68 KE ■ OS (C:) ■ Microsoft-Windows-Application Server-Application 2022/3/11 14:28 事件日志 68 KE ■ DATA (D:) ■ Microsoft-Windows-Application-Experience%4Pro 2022/4/12 19:12 事件日志 68 KE ■ Microsoft-Windows-Application-Experience%4Pro 2021/10/12 3:28 事件日志 68 KE ■ Microsoft-Windows-Application-Experience%4Pro 2021/10/12 3:28 事件日志 68 KE ■ Network ■ Microsoft-Windows-Application-Experience%4Pro 2021/10/12 3:28 事件日志 68 KE		Interest Mindows-All-User-Install-Agent%4Admi	2021/10/12 3:28	事件日志	68 KE
 ▶ 客 ● 片気 ■ Microsoft-Windows-ApplD%4Operational.evtx 2021/10/12 3:28 事件日志 68 KE ■ 直面 ■ Microsoft-Windows-ApplicabilityEngine%4Operati 2021/10/12 3:28 事件日志 68 KE ■ DaTA (D:) ■ Microsoft-Windows-Application-Experience%4Pro 2022/3/1 14:28 事件日志 68 KE ■ DATA (D:) ■ Microsoft-Windows-Application-Experience%4Pro 2022/3/1 14:28 事件日志 68 KE ■ Microsoft-Windows-Application-Experience%4Pro 2022/3/1 14:28 事件日志 68 KE ■ Microsoft-Windows-Application-Experience%4Pro 2021/10/12 3:28 事件日志 68 KE ■ Microsoft-Windows-Application-Experience%4Pro 2021/10/12 3:28 事件日志 68 KE ■ Microsoft-Windows-Application-Experience%4Pro 2021/10/12 3:28 ■ 401-00-00-00-00-00-00-00-00-00-00-00-00-0		Microsoft-Windows-AppHost%4Admin.evtx	2021/10/12 3:28	事件日志	68 KE
♪ 音乐 副 Microsoft-Windows-ApplicabilityEngine%4Operati 2021/10/12 3:28 事件日志 68 KE ● 点面 副 Microsoft-Windows-Application Server-Application 2022/3/1 14:28 事件日志 68 KE ● OS (C:) 副 Microsoft-Windows-Application Server-Application 2022/3/1 14:28 事件日志 68 KE ● DATA (D:) 副 Microsoft-Windows-Application-Experience%4Pro 2022/4/12 19:12 事件日志 68 KE ● Network ■ Microsoft-Windows-Application-Experience%4Pro 2021/10/12 3:28 事件日志 68 KE	◆ 下転	Microsoft-Windows-AppID%4Operational.evtx	2021/10/12 3:28	事件日志	68 KE
■ 桌面 Wicrosoft-Windows-Application Server-Application. 2022/3/1 14:28 事件日志 68 KE ■ OS (C:) Microsoft-Windows-Application Server-Application. 2022/3/1 14:28 事件日志 68 KE ■ DATA (D:) Microsoft-Windows-Application-Experience%4Pro 2022/4/12 19:12 事件日志 68 KE ■ Microsoft-Windows-Application-Experience%4Pro 2021/10/12 3:28 事件日志 68 KE ■ Microsoft-Windows-Application-Experience%4Pro 2021/10/12 3:28 事件日志 68 KE	♪ 音乐	Microsoft-Windows-ApplicabilityEngine%4Operati	2021/10/12 3:28	事件日志	68 KE
Loss (C:) I Microsoft-Windows-Application Server-Application 2022/3/1 14:28 事件日志 68 KE DATA (D:) I Microsoft-Windows-Application-Experience%4Pro 2022/4/12 19:12 事件日志 68 KE Microsoft-Windows-Application-Experience%4Pro 2022/4/12 19:12 事件日志 68 KE Microsoft-Windows-Application-Experience%4Pro 2021/10/12 3:28 事件日志 68 KE Network I Microsoft-Windows-Application-Experience%4Pro 2021/10/12 3:28 事件日志 68 KE	回 桌面	Microsoft-Windows-Application Server-Applicatio	2022/3/1 14:28	事件日志	68 KE
■ DATA (D:) I Microsoft-Windows-Application-Experience%4Pro 2022/4/12 19:12 事件日志 68 KE I Microsoft-Windows-Application-Experience%4Pro 2021/10/12 3:28 事件日志 68 KE I Microsoft-Windows-Application-Experience%4Pro 2021/10/12 3:28 事件日志 68 KE I Microsoft-Windows-Application-Experience%4Pro 2021/10/12 3:28 事件日志 68 KE	: OS (C:)	Microsoft-Windows-Application Server-Applicatio	2022/3/1 14:28	事件日志	68 KE
● Network III Microsoft-Windows-Application-Experience%4Pro 2021/10/12 3:28 事件日志 68 KE	DATA (D:)	Microsoft-Windows-Application-Experience%4Pro	2022/4/12 19:12	事件日志	68 KE
Network Determine the function of the second seco		Microsoft-Windows-Application-Experience%4Pro	2021/10/12 3:28	事件日志	68 KE
	Network		2021/10/12 2.20	当注日十	co vo

图 3-41 Windows 事件日志文件

核心的日志文件主要有三个,分别是: System. evtx、Application. evtx 和 Security. evtx,它们分别是系统日志、应用程序日志和安全日志。

(1)系统日志:系统日志记录系统进程和设备的驱动程序的活动。它输出的记录包括 设备驱动程序是否启动失败,硬件是否自检出错,以及系统服务的开启、关闭、暂停。

(2)应用程序日志:记录普通的用户程序和一些商用程序在运行过程中出现的事件, 它会输出自己记录的所有报错和需要用户知晓的信息。

(3)安全日志:记录系统的安全审计日志事件,比如登录事件、对象访问、进程追踪、特权调用、账号管理、策略变更等。安全日志也是取证中最常用到的,是处理入侵事件的重要 武器,分析者需要查看和筛选这些文件中的信息从而发现蛛丝马迹。

三个文件的默认大小均为 20480KB(20MB),当记录事件数据超过 20MB 时,系统将优先覆盖过期的日志记录,从头开始写入新的记录,也就是相当于一个循环记录的缓存文件。

2. Windows 事件日志的查看方式

查看 Windows 事件日志的标准方法是使用 Windows 系统自带的"事件查看器"(可以 通过运行"eventvwr"来启动),如图 3-42 所示。

副事件查看器 (本地)	Windows 日志				操作
 > □● 自定义视图 > □● 自定义视图 ■ 協用程序 ■ 安全 □ Setup ■ Setup ■ Forwarded Events ■ Forwarded Events ■ Dell > □ Intel ■ Intel ■ Internet Explorer > □ Microsoft ■ Microsoft ■ Microsoft ■ Microsoft ■ Microsoft ■ Microsoft ■ Windows PowerShell ■ 密销管理服务 ■ 硬件事件 ● □ 	名称 应用程序 安全 Setup 系统 Forwarded Events	类 管理理作 智 握 管理作的 握 管理作的 一种 化合物	事件数 12,551 25,500 1,928 13,576 0	大小 6.07 MB 20.00 MB 1.00 MB 6.07 MB 0 字节	Windows 日志 打开保存的日 创建自定义视 导入自定义视 查看 刷新 報助 加用程序 打开 服性 報助

图 3-42 事件查看器

在事件查看器中,系统日志被分为 Windows 日志,应用程序和服务日志两大类,其中 Windows 日志包括了应用程序、安全、Setup、系统和 Forwarded Events(转发事件)。

事件查看器可以将日志文件导出为 evt、evtx、xml、txt 和 csv 等格式,并导入其他系统 的事件查看器进行浏览。因为日志文件格式在各个 Windows NT 版本中通用,所以调查人 员也可以利用本地计算机的事件查看器远程连接其他计算机,以管理员权限查看浏览日志 文件。调查人员可以利用事件查看器的"筛选"功能,显示特定时间类型和时间段的相关 内容。

通过对 Windows 系统日志的取证分析,取证人员可以对操作系统、应用程序、服务、设备等操作行为记录通过关键的时间点进行回溯。

3. 常见的 Windows 事件日志分析

(1) 系统日志

系统日志可以捕获由系统自身产生的事件。任何自动执行的操作,或直接利用 OS 功能的用户驱动操作都会记入日志,包括软硬件安装、打印作业和网络层事件等。取证人员关注的系统事件常与案件的性质和被调查者的抗辩有关,常见的有:

① 事件日志启动和停止。事件 ID6005 和 ID6006 代表日志服务的启动和停止,主动关闭日志服务的行为往往值得深入追查。

② 系统关机和重启。事件 ID6008 表示系统的一次意外关闭, ID6009 则和系统重启相

关。当发现 ID6006 后不久紧跟 ID6009 事件,通常可以认为是系统原因。事件 ID1074 显示 引起系统关闭的进程,ID1076 显示系统关闭的原因。

③ 登录失败。事件 ID100 表示一个已知账户的验证失败,调查中发现的这类事件,有可能是特定用户通过猜测密码或使用穷举等破解工具的线索。

④ 机器信息改变。事件 ID6011 表示系统名称改变,如果发现名称与现存信息不匹配, 就要重点查找这个事件 ID。

⑤ 打印。ID10显示的是打印作业和来源,以打印请求者用户名的方式显示。

(2) 应用程序日志

应用程序日志由应用程序使用产生,Windows 允许第三方软件通过 API 记录应用程序 事件,防病毒软件和安装程序通常会使用这样的功能,在调查中经常使用到的有:

① 确认软件安装。使用微软安装程序的情况下,通过事件 ID11707(成功)、事件 ID11708(失败)和事件 ID11724(卸载)来记录软件包的运行,查看这些 ID 可以发现特定软件的安装、试图安装和卸载的时间。

② 确认和排除病毒感染。大多数防病毒软件在检测到病毒时,会产生一个 ID5 事件。 案件调查中,涉案人员有时会辩称系统问题是病毒引起的,通过查看这个事件,可以显示和 排除他声称的时间内是否有病毒发作。

③ 启动和关闭防火墙。记录了用户主动打开或关闭系统防火墙的行为。

④ 检查黑客攻击企图。ID 为 1000~1004 的事件记录有错误的应用程序,可以提供应 用程序漏洞被利用的线索,事件 ID4097 也有可能代表类似活动。

应用程序日志事件常依赖于特定系统中安装的具体应用程序,以及是否独立使用事件 日志服务,或者利用本地私有日志对系统日志进行补充,所以调查人员在检查应用程序日志 之外,通常还必须检查应用程序是否使用了本地私有日志记录。

(3) 安全日志

安全日志是所有日志的基础,登录、注销、尝试连接和改变系统策略等关键事件,都会在 安全日志中反映出来。企业为了支持安全事件调查和溯源,通常会在本地或组策略下的审 核策略中要求计算机系统激活如审核账户登录事件、账户管理、登录、策略改变、特权使用 等。其中,登录和注销对于证实什么人在什么时间执行了什么操作尤为重要,而其他安全事 件则根据案件不同,会对某些特定的调查有帮助。

① 成功登录和注销事件。交互式的登录事件通过事件 ID4624 来描述,是登录类型的 一个子类,调查人员比较关注的登录类型有 ID2(本地)、ID3(网络)、ID7(Ctrl+Alt+Del 或 屏幕解锁)、ID10(远程桌面)、ID11(缓存的用户凭证登录)。

另外,注销事件显示了某用户连接的时间段,以 ID4647 为用户启动注销的开始, ID4634 为结束。

② 登录失败事件。登录失败是判定是否有人进行密码猜测或暴力攻击的有力证据之一,登录失败事件通过 ID4625 来描述。可以输入事件 ID: 4625 进行日志筛选,若用户登录失败次数明显偏多,那么这台服务器管理员账号可能遭遇了暴力猜解。

③ 对象访问。在一个特定对象属性的"安全"选项卡上单击"高级"按钮,可对待定的 NTFS文件和文件夹进行审核。激活对象审核可以记录从试图读取对象到成功删除对象的 任何操作。如果系统开启这个级别的审核,就能显示某个特定实体在何时被访问、被谁访

问、特定文件和目录的改变和删除,或者突出显示对关键对象的非法访问企图。

④ 用户账户相关事件。事件 ID4720、ID4722、ID4723、ID4724、ID4725、ID4726、ID4738、 ID4740,表示当用户账号发生创建、删除、改变密码时的事件记录。

⑤ 日志清除。事件 ID1102 表示安全事件日志被清除。在没有合理原因将旧文件存储 到一个新文件之前,安全日志几乎是不会被清除的,一旦有该事件发生,很有可能表明使用 者或入侵者在故意掩盖痕迹。

综上所述,不同的事件 ID 代表了不同的意义,这些可以在网上很容易查到,需要根据案件的类型和基本情况,有重点地查看。

3.4.2 实验目的与条件

1. 实验目的

通过本实验,读者可以掌握以下内容:

(1) 了解 Windows 事件日志的概念及查看方式;

(2) 掌握 Windows 事件日志的种类及内容;

(3) 掌握常见的 Windows 事件日志的分析。

2. 实验条件

本实验所使用的 Windows 操作系统为 Windows 10(Windows Vista 以上)。

3.4.3 实验过程

步骤 1: 学生两两分组,互相进行远程桌面访问,首先打开将要被远程访问的计算机,在 计算机系统属性中,选择"远程"选项卡,在远程桌面选项中勾选"允许运行任意版本远程桌 面的计算机连接(较不安全)",单击"确定"按钮,如图 3-43 所示。

+算机名 硬件 高级 系約	徐保护 远程
远程协助	
☑ 允许远程协助连接这台计算	机, (B)
有关启用远程协助的信息	
	高级(1)
远程桌面	
单击一个选项,然后指定谁可以	以连接(如果需要)。
◎ 不允许连接到这台计算机 @)
◎ 允许运行任意版本远程桌面	的计算机连接(较不安全)(L)
⑦ 仅允许运行使用网络级别身机连接 (更安全) (20)	份验证的远程桌面的计算
\$106-51-24-4交	选择用户(S)

图 3-43 开启远程桌面功能

步骤 2: 在另一台计算机上打开远程桌面窗口,输入被控制计算机的 IP 地址,单击"连接"按钮,如图 3-44 所示,尝试包括登录成功、断开连接等操作。

电子	·数据取证实训	
-E J	奴加林ய天师	۰.

🖥 远程桌面)	车接		X
	远程桌面 连接		
计算机(C):	172.17.66.19	•	
用户名: 当您连接时	未指定 将向您询问凭据。		
😠 选项 @)	〔连接 01〕 【帮I	助 010

图 3-44 远程桌面访问

步骤 3: 在被远程访问的计算机上,右击"我的电脑",在弹出的快捷菜单中选择"管理" 选项,打开"事件查看器"; 或者按下 Win+R 的组合键,在运行窗口中输入"eventvwr.msc", 如图 3-45 所示,直接打开"事件查看器"。

۰	Windows ¥ 文件夹、文	等根据你所输) 档或 Internet	、的名称, 为你打 资源。	开相应的程序、
打开(0):	eventvwr.r	msc		

图 3-45 打开事件查看器

步骤 4: 攻击者使用 RDP 远程登录受害者计算机,会在事件日志中生成相应事件。在 "Windows 日志"下,选择"安全"(Security. evtx),筛选事件 ID 为 4624,如图 3-46 所示,即 为账户成功登录事件,如图 3-47 所示。其中,"LogonType=10"的为远程桌面访问,可以看 到访问主机的源 IP 地址。

常选当前日志		
筛选器 XML		
记录时间(<u>G</u>):	任何时间 ~	
事件级别:	□ 关键(L) □ 警告(W) □ 详细(B)	
	□ 错误(B) □ 信息(I)	
④ 按日志(Q)	事件日志(E): 安全	
○ 按源(S)	事件来源(\):	
任务类别(]):	<u>4524</u>	
关键字(1):		
用户(U):	<所有用户>	
11997+0 (0)	<所有计算机>	
计异机(巴):		
计算机(P):	清除(A)	1

图 3-46 筛选日志

	1							
·····································	安全 事件数: 1	操	操作					
▲ Windows 日志	 (二) 审核成功 (二) 审核成功 	2022/9/22 9:52 2022/9/22 9:52	2:35 2:35	Microsof Microsof	4672 4624	特殊登录 登录	iii Y	打开保存的日志 创建自定义视图
 ☐ Setup ☑ 系统 □ 转发事件 	 () 审核成功 () 审核成功 () 审核成功 	2022/9/22 9:5 2022/9/22 9:5 2022/9/22 9:5	2:35 3:13 3:42	Microsof Microsof Microsof	4648 4634 4634	登录 注销 注销		导入自定义视图… 清除日志… 筛选当前日志…
○ 四月9月4日度 ○ 四月9月4日度 ○ 10月9月4日度	 電核成功 2022/9/22 9:5 電核成功 2022/9/22 9:5 電核成功 2022/9/22 9:5 	1:54:08 Microsof 1:54:08 Microsof 1:54:08 Microsof	4672 特殊登录 4624 登录 4648 登录	特殊登录 登录 좌录		属性 查找		
	事件 4624 , Mic 常规 详细(rosoft Windows 1息	安全审核。				<u>×</u> H	将所有事件另存为… 将任务附加到此日志… 查看
	● 友好视图(N) ◎ XML 视图(X) TargetLogonId 0x325d97						· 2	刷新 帮助
	LogonType 10 LogonProcessNameUser32 AuthenticationPackageNameNegotiate WorkstationNamePC-1-8						* 0	件 4624 , Microsoft Wi 事件尾性 将任务附加到此事件 保存选择的事件
	TransmittedServices -							复制 刷新
	Key Pro Pro	PackageNar /Length ocessId ocessName	0 0xad0 C:\Win 172 17	dows\Syst	tem32\\	winlogon.exe	E 2	帮助

图 3-47 远程桌面登录成功

步骤 5: 查看同路径下事件 ID 为 4648 的事件,为用户使用明文凭证尝试登录的事件, 其中,"详细信息"记录了用户的 IP 地址,如图 3-48 所示为本机登录,图 3-49 所示为远程主 机登录。

牛查看器 (本地)	安全 事件数: 11		操作				
自定义视图	关键字	日期和时间	来夏	事件 ID	任务类别	-	安全
日の用程序	0、审核成功	2022/9/22 9:54	:10 Microsoft Windows	安 4672	特殊登录	100	◎ 打开保存的日志
	0、审核成功	2022/9/22 9:54	10 Microsoft Windows	安 4624	登录		♥ 创建自定义视图
Setup	@、审核成功	2022/9/22 9:54	:09 Microsoft Windows	安 4634	注明		导入自定义视图
日系统	0、审核成功	2022/9/22 9:54	:08 Microsoft Windows	安 4672	特殊登录		清於日志
目 转发事件	0、审核成功	2022/9/22 9:54	:08 Microsoft Windows	安 4624	登录		
应用程序和服务日志	9、审核成功	2022/9/22 9:54	08 Microsoft Windows	安 4648	登录		1 HADENICS-
订网	④ 审核成功	2022/9/22 9:53	42 Microsoft Windows	安 4634	注钠		
	0、审核成功	2022/9/22 9:53	:13 Microsoft Windows	安 4634	注销	16	墨 查找
	0、审核成功	2022/9/22 9:52	:35 Microsoft Windows	安 4672	特殊登录	1	。将所有事件另存为
	0、审核成功	2022/9/22 9:52	:35 Microsoft Windows	安 4624	受受		将任务附加到此日志
	《审核成功	2022/9/22 9:52	:35 Microsoft Windows	安 4648	登录		查看
	④ 重核成功	2022/9/22 9-52	35 Microsoft Windows	空4624	<u> </u> 중문	*	ର ଅକ
	事件 4648 , Micro	soft Windows §	2全审核。			×	
	常報 详细信	2					La result
	1.1.1.1						事件 4648, Microsoft Windows 安
	② 友好视图(N)	© X	ML 视图(X)			1	画 事件属性
	TargetDomainNamePC-1-8						圆 将任务附加到此事件
	Tarc	etLogonGu	id {0000000-0000-0000	0-0000-00000	00000000}	1	注 复制
	Tar	etServerNa	melocalhost		· · · · · · · · · · · · · · · · · · ·	1	保存选择的事件
	Tar	etInfo	localhost				
	Bro	receid	0v1424				
	Processia UA1424						M MON
	Pro	essivame	C:\windows\System32	(winiogon.e)	xe =		
	IpA	dress	127.0.0.1		1		

图 3-48 本机明文登录事件

又14(F) 望(F(A) 亚祖(V)	400(H)						
					P		
副事件查看器 (本地)	安全 事件数: 11,329	操作					
P III字 日本又死回 A IIII Windows 日本	关键字 日期和时	印 未遊	事件 ID	任务类别	安全		
日 comentation College	④ 审核成功 2022/9/1	2 9:54:10 Microsof	t Windows 安 4672	特殊登录	a 打开保存的日志		
	④ 审核成功 2022/9/	2 9:54:10 Microsof	t Windows 安 4624	登 录	♥ 创建自定义视图		
Setup	④、审核成功 2022/9/2	2 9:54:09 Microsof	t Windows 安 4634	注例	导入自定义视图		
同 系统	《审核成功 2022/9/2	2 9:54:08 Microsoft	t Windows 安 4672	特殊登录	清除日志		
目 转发事件	《审核成功 2022/9/	2 9:54:08 Microsoft	t Windows 安 4624	登录	▼ 装饰当前日本		
III 应用程序和服务日志	④ 审核成功 2022/9/	2 9:54:08 Microsoft	t Windows 安 4648	登录	1 1942-1912-0		
間订阅	④、审核成功 2022/9/2	2 9:53:42 Microsof	t Windows 安 4634	注例	I ALLE		
	《审核成功 2022/9/	2 9:53:13 Microsof	t Windows 安 4634	注明			
	Q 审核成功 2022/9/.	2 9:52:35 Microsof	t Windows 安 4672	特殊登录	日 将所有事件另存为		
	Q 审核成功 2022/9/2	2 9:52:35 Microsof	t Windows 安 4624	登录	将任务附加到此日志		
	《审核成功 2022/9/	2 9:52:35 Microsof	t Windows 安 4648	登录	查看		
	④ 重總成功 2022/9/	2 9:52:35 Microsof	t Windows @ 4624	함 문 *	G BH		
	事件 4648, Microsoft Win	lows 安全审核。		×	E sash		
	安妮 洋田信息						
				1	事件 4648, Microsoft Windows 安		
	● 友好视图(N)	◎ XML 视图(X)			事件屬性		
	TargetDon	nainNamePC-1-8			③ 将任务附加到此事件		
	TargetLog	onGuid (00000000-00	000-0000-0000-0000	(0000000)	Ba 复制		
	TargetServ	TargetServerNamelocalhost					
	TargetInfo	localhost			G Die		
	Processid	0xad0					
	Processia	C:\Windows\S	wtom??\winlogon.ex		M WEIGH		
	Processiva	ne C.\Windows\s	ystem52 (winiogon.e)	e E			
	IpAddress	1/2.17.66.17		1	1		

图 3-49 远程主机明文登录事件

步骤 6:同样地,ID4778事件为重新连接到一台 Windows 主机的会话,ID4779事件为断开到一台 Windows 主机的会话。

步骤 7: 查看远程连接日志,具体路径为:应用程序和服务日志-Microsoft-Windows-TerminalServices-RemoteConnectionManager-Operational。其中,ID1149 事件为用户认证 成功,如图 3-50 所示,可以清晰地看到用户名及源网络地址。

PowerShell	Operational	事件数:12			操	Pi:
 PrimaryNetwork! PrintService ReadyBoost ReadyBoost ReadyBoostDrive 	级别 () 信息 () 信息	日期和时间 朱语 2022/9/22 9:48:41 Ter 2022/9/22 9:52:24 Ter	新年 ID mi 261 mi 261 261	任 5 类 则 无 无	1 OF	perational 打开保存的日 创建自定义视
Accovery Reliability-Analysi The RemoteApp and RemoteAssistanc RemoteAssistanc Resource-Exhaus)48)48)48	2022/9/22 9:50:11 Ter 2022/9/22 9:52:11 Ter 2022/9/22 9:45:26 Ter 2022/9/22 9:45:25 Ter 2022/9/22 9:45:25 Ter 2022/9/22 9:48:41 Ter	mi 261 mi 261 mi 1136 mi 1149 mi 1149	<u></u> 无 无 无 无 无	•	导入自定义视 清除日志 / 筛选当前日志 属性
Besource-Exhaus Besource-Leak-D BestartManager Bescurity-Audit-Cc Security-Identity	事件 1149 , Ter 常规 详细	minalServices-RemoteConnectic	nManager		× 99	禁用口志 查找 將所有事件另 将任务附加到
Gervice Reporting Gervice Reporting Gervice Reporting Gervice Reporting Gervice Reporting	远程桌面服的 用户: admin	計用户身份验证已成功:			0	查看 周新 帮助
	7%: 遵网络地址: 日志名称(M):	172.17.66.17 Microsoft-Windows-Terr	ninalServices-Re	moteConnectionManager/Operational		件 1149 , Term 事件星性 将任务附加到
Admin Operational TZUtil UAC	来源(S): 事件 ID(E): 级别(L):	TerminalServices-Remote 1149 信息	□ 记录时间(D): 任务类别(Y): 关键字(K):	2022/9/22 9:52:35 无		」复制 保存选择的事 刷新
III UAC-FileVirtualizz III User Profile Servi III VDRVROOT III VHDMP	用户(U): 操作代码(O): 更多信息(I):	NETWORK SERVICE 信息 事件日志默机整胎	计算机(R):	PC-1-8	2	帮助

图 3-50 用户认证成功

3.4.4 实验小结

其他常见的 Windows 事件包括:用户登录或注销、远程访问审计、即插即用设备使用、 系统时间修改、无线网络接入等,读者可自行查阅资料,练习、查看。实际应用中,要通过日 志准确分析出恶意行为是需要大量实践经验的,同样也需要了解 Windows 日志中各种事件 ID 组合、状态码所对应的事件。

3.5 回收站取证

3.5.1 预备知识:回收站运行机制

对删除文件的恢复,一直都是电子数据取证的重要部分。在 Windows 操作系统中, 用户选择删除一个文件后,这个文件并没有真正删除,而是进入了一个叫作回收站的地 方,如果删错了或者后悔了都可以在回收站中进行恢复操作。所以,回收站是一个重要的 信息来源,通过分析回收站可以知道被删除文件的信息,包括原始路径、删除时间、文件大 小等。

回收站是 Windows 操作系统中的一个隐藏的系统文件夹,其文件名及存放路径根据 Windows 系统版本的不同而不同,具体如表 3-5 所示。

操作系统版本	分 区 格 式	回收站位置
Windows 95/98/ME	FAT32	\Recycled\INFO2
Windows NT/2K/XP	FAT32	\Recycled\INFO2
	NTFS	\Recycled\< USER SID>\INFO2
Windows 7/10	NTFS	\$ Recycle. Bin\< USER SID>\

表 3-5 回收站文件夹存储位置

对于 Windows XP 来说,在 FAT32 文件系统下,删除的文件在 Recycled 文件夹中的命 名格式为: D[文件原始隶属盘符][索引号][原始扩展名]。同时在文件夹中会存在一个名 为 INFO2 的二进制文件,用来记录所有删除文件的时间及路径信息。

而 Windows 7 及以后的系统,回收站的机制发生了改变,抛弃了 INFO2 文件保存删除 文件信息的做法,而是为每个被删除文件建立一个删除记录。通过分析每个删除记录,可以 了解文件的原始信息。当一个文件被删除时,它被进行两个操作:①将删除的文件重命名 为"\$R"开头的文件,后面跟着随机字符串,后缀与原来文件一致。②创建一个"\$I"开头的 文件,后面与"\$R"开头的文件相同。"\$I"开头的文件为对应的"\$R"开头的文件的回收站 记录文件。这样每个删除文件都有自己的回收站记录文件。

"\$I"开头的回收站记录文件,大小都是 544 字节,主要包括以下删除记录信息(具体结构如表 3-6 所示):

- 被删除文件原始路径;
- 被删除文件大小;
- 被删除文件的删除信息(64 位 Windows 时间)。

数 据 结 构	长度	偏移量
操作系统版本	8	0x00
被删除的文件大小	8	$0 \mathbf{x} 0 8 \sim 0 \mathbf{x} F$
文件删除时间	8	0x10~0x17
被删除的文件名(全路径)	0~520	0x18~0x21F

表 3-6 回收站记录文件结构

目前主流的取证工具,例如 EnCase、FTK 等都支持对回收站文件的解析。但是由于操 作系统的版本不同,导致回收站的结构和运行机制都有所不同。因此还需要在理解回收站 的结构和机制的前提下,利用相应的工具进行取证。

3.5.2 实验目的与条件

1. 实验目的

通过本实验,读者重点掌握以下内容:

- (1) 了解回收站的运行机制;
- (2) 掌握回收站记录文件的解析过程;
- (3) 掌握在注册表中查找文件删除者信息的过程。

2. 实验条件

本实验所需要的软硬件清单如表 3-7 所示。

表 3-7 回收站取证实验清单

序 号	设备	数 量	参数
1	取证工作站	1台	Windows XP 以上
2	EnCase 软件	1 套	EnCase7
3	检材 U 盘 (包含证据文件"Malone's HDD 1A. Ex01")	1个	无

3.5.3 实验过程

步骤 1: 打开 EnCase 软件,新建案例并添加证据文件"Malone's HDD 1A. Ex01"。 步骤 2: 找到分区 C 中的 \$ Recycle. Bin 文件夹,如图 3-51 所示。



图 3-51 回收站文件夹

步骤 3: 查看回收站文件夹中的文件,找到可疑文件(如图 3-52 所示: nuclearexplosion.jpg),查看其短名(如图 3-53 所示: \$RAFR6IT.jpg),即为文件删除后,重命名 为"\$R"开头的文件。

) EnCase Forensic (版本 7.12.01)						
- • 🗋 案例 (mi) • 🔍 祝園 • 🗇 エ具 • 🕆 EnScript • 🖓 添加運動						-
1 年 2 日 年 × 1						
3 〇 ↑ 正在查看(入口)▼ □ 折分模式▼ (語条件▼ 7 过滤器▼ -	□标签 * ◎ 文档检查 * ** 已选择原始搜索 * ◇ 书3	· · · · · · · · · · · · · · · · · · ·	牧相关项目▼ 18-入	a + 538	東京 山 法福	14
이미늄 자미	四利表 行时间转 臣 和家					
▲ Q maione	⑦ Ⅲ + 41 + □ B赴祭 085473					
• 0] = C			and a second second second	. In second		
Dig Stand	看教	自然目前 文件扩展名	逻辑大小 种类	盖名分析	文件类型	Ŧ
C Stecyce bin	1 BitLocker Recovery Key 6C894E50-1384-48	. bd	906 文档			
O S-1-5-21-3774130484-663992614-3010368698-1001	2 desktop.ini	ini	129 Windo.			
> O b b3386d33b6bd2acbbcba57e1	3 3 51784PQ4.jpg	ipg	544 图片			
DO Boot	4 SIAFR6IT.jpg	ipg	544 图片			
-O Documents and Settings	5 Sty05007.bd	txt	544 文档			
D MSOCache	🖸 6 🚄 nuclear-explosion.jpg	ipg	18,218 圓片	正配	JPEG Image	
D D PerfLogs	7 SRV8WJ89.jpg	ipg	17,299 图片	正配	JPEG Image	_
DO Program Files	3 8 SRGWKT8LJPG	JPG	1,643,232 图片	正配	JPEG Image	
Degrambata	9 SRR0U7OAjpg	ipg	16,416 圓片	変配	JPEG Image	
A COLL System Volume Information	10 PHOTO_02 pg	ipg	15,017 圓片	正配	JPEG Image	
b of all Users	11 SRV3OKRQ.jpg	ipg	18,723 圓片	変配	JPEG Image	
- O	12 mg SRMEJSVS.jpg	ipg	16,160 圖片	正配	JPEG Image	

图 3-52 回收站中的可疑文件

G EnCase Forensic (版本 7.12.01)								
■ •] 案例 (ml) • 🥄 视图 • 🔅 工具 • 😚 EnScript • 23 添加证据								
合家 /2证据×								
○ ⑦ ↑ 正在查看(入口) ▼ □ 折分模式 ▼ (語条件 ▼) 可过滤器 ▼	□标签、	⑥ 文档检查	已选择	#原始搜索▼ ▲ 书签▼ 图 转至文	件 ① 查找相	关项目 * 包入	a • (1)	ŧ.
▲ O□ 悟 入口	m	1.5 Option	6 E 88					
- D maione	2	1- 4-	2 2 2 2 2 0 2 5	473				
C SExtend		证据文件	文件标识符	全球唯一称识符(GUID)	Hash Set Names	短名	VFS 名称	Ī
SRecycle.Bin S.1.5.21.3774130484_663992614_3010368698_1000	1	malone	1605.0	acb5a23ba74918e9873ede1115a1		\$RY0500		0
S-1-5-21-3774130484-663992614-3010368698-1001	2	malone	49159.8	9a6cdae481ca8838b473f6e86c5f8				
b-DC b3385d33b5bd2acbbcba57e1	3	maione	49893.2	157d38b4bea1483a4c86cebe92aa				
D D Boot	4	malone	49894 d	7e530ea8465998a92410c128d8f2				
- D Documents and Settings	0 6	malone	49895 8	a8bd0acfd404683bad61b76c9d83				
DO MSOCache	6	maione	500357	03856e1507f3d83b25788a350de6f		SRAFR6IT		c
PerfLogs	07	malone	551185	edb33dfb0577e82ba00104849cb3				T
D-D- Program Files	08	malone	66464 b	6b0a3eadd7ccb8ebcec5195382d7				
P-D I ProgramData	0 9	malone	66465 d	59bea55b5dec58495dd410910c58				
D-D Recovery	3 10	malone	66467 b	016e11d8f446d8f8e3b1a9f4b4f7d2f		SR784PQ4		
DU System Volume Information	11	malone	66468 ft	b08f17daa62138597d130c861e038				Ť
- O Mindows	1	maione	67847.2	cb9ab21fe02348c9fa2302f0152150e				1

图 3-53 可疑文件的短名

步骤 4: 根据该文件的短名找到其对应的以" \$I"开头的回收站记录文件(如图 3-54 所示: \$IAFR6IT.jpg)。

학교 (요건물×)										
○ ○ ? 正在查看(入口) * 二 新分模式 * (三条件 * ? 过速器 *	○标签 *	○ 文稿检查 * ※ 已选择原始搜索 * ◇ 书	× • ● 秋亚)	2件 2 重要	\$相关项目▼	圣入	- (Ja	100×运进程	20 25 -	四打开方式。
이 같 사미	ma	(表 ⊕)时间线 Ⅲ 图库								
• O makene	3	- 2↓- □ 已选择 0/85473								
► O SExtend		68		文件扩展名	逻辑大小	10 	高名分析	文件类型	更保护	保护复杂性
O □ □ SRecycle.Bin O □ □ □ S.1.6.21.3774130454.653992614.3010365698.1000 O □ □ □ S.1.6.21.3774130454.653992614.3010365698.1000 O □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □	01	Bill.ocker Recovery Key 6C894E50-1384-48	-	bd	906	文档			and the second	
OC S-1-6-21-3774130484-663992614-3010368698-1001	2	desktop.ini		ini	125	Windo				
> O() b3385d33b5bd2acbbcba57e1	3	SI784PQ4 jpg		ipg	544	4国片				
D-DC Boot	4	SIAFREIT jpg		ipg	544	(面片				
DC Documents and Settings	. 5	SIYO5007.bd		bd	544	4文積	-			
▷ O(□)) MSOCache	6	nuclear-explosion.jpg		ipg	18,218	國片	読配	JPEG Image		
D D PerLogs	07	SRV8WJ89.jpg		ipg	17,295	國片	正配	JPEG Image		
 D() Program Files 	0 8	SRGWKT8LJPG		JPG	1,643,233	2團片	読配	JPEG Image		1
ProgramData	09	SRR0U7OA.pg		ipg	16,416	調片	調整	JPEG Image		1
O Accovery Sustan Visions Information	10	PHOTO_02.pg		ipg	15,017	7團片	の配	JPEG Image		
COLL lisers	11	SRV3OKRQ.pg		ipg	18,723	画片	正配	JPEG Image		1
A COT III Windows	1 12	SRMEJSVS.pg		ipg.	16,160	國府	調整	JPEG Image		

步骤 5: 通过查看回收站记录文件中的十六进制数据,解析回收站记录文件(操作系统版本、文件大小、删除时间、原始路径等)。

其中,0x00~0x07 按小端顺序解析为1,表示是 windows 7 操作系统,如图 3-55 所示。

- 二 安何 (123) - 6 周辺 - 6 丁目 - 水 EnCertet - 2 後加辺	<u>10</u> .																					
· J 来所(123)· 4 代内· J LA· 5 Enocipt · C Aprille 家 /2 正規×	200 -																					
○ * 正在查看(入口) · □ 振分模式 · □ 条件 · 7 讨波器 ·	08	· 25. *	o ve	5检查		- E3	无托用	2.661	の会 .	• 00 -	书签	- 0	转至	2件	a	查找 相	日关耳	iII •	En .	λ	11.1	- 18
	^	三列	<u>الم</u>	时间	线!	11 11	库		~~~	Ť	1		11.00.0		1						5- 5	
+ 0 □ == C		17 11	- 21 -	01	已选择	¥ 0/8	547	3														
► coll \$Extend		-					名称					B	Re Ec	kat	文件	扩展分	5 13	報大	4	种类	-	5分相
• OLI W SKECYCE.BIN	2	-	3 Dat	oskor	Dec		Koul	80.00	MESO	120	4 40	-		-	M		-		008	1120	-	
o S-1-5-21-3774130484-663992614-3010368698-1001		02) des	kton i	ni	overy	Rey	0005	PE DU	-130	4-40				ini				1201	X.13 Windo		
▶ c□} b3385d33b5bd2acbbcba57e1		03	= \$178	34PO4	tipa										ipa				544	图片		
Boot		04	= SIAI	FRGIT	ipg							1		- 9	ipg				544	图片		
Colling Documents and Settings		15	1 SIYO	3500	/.bd			_	_	_	_	_			bđ	_	_	_	544	又相	_	_
PerfLogs	1	06	a nucl	lear-e:	plosi	ion.jp	g								ipg			18,	218	图片		
▷ c□ I Program Files		07	≅ \$R\	/8WJ1	89.jpg	1.	- 254							_			2.	17,	299	图片		
o □ ↓ ProgramData		8	a SRO	SWKT	8L JF	PG 7	133									1	\sim	,643,	232	割片		
CO Recovery Sector Vehrma Information		9	SRF	20070	JA jp	9	解釈	6选中	的文	木								16,	416	出片		
		0 11		/30KI	20 in	0	~		_								-	18	723	国計		
▷ c□ ↓ Windows		12	a SRA	MEJS	VSip	a	\odot	little	End	an								16	160	图片		
▶ ○□ № 丢失的文件数							OF	Big-E	ndia	n												
• COM D							~		Ē		-					-						
COM SECON EBIN	~	<					01	其他		1												
字母 日報告 日 文本 屈十六法制 益銀码 可文档 日地	*	1 四日	-14	otal 4	7 03-				-	_							- 1					
19 15 P. IDITITY - A system P - A WAR IN PACIFIC PROVIDE	Port 1	A	1000000		COURS	1				A.r.ta		10	10	147	÷.		- 8					
	21		. 70	50	0.0			2	9	相定			40.3	11			- 8	10.1		0.0		
400 73 00 50 00 53 00 61 00 6D 00 2E 00 4	4D	00 6	00	60	0.0	6		1000							200			33 0	0 7	4 0	0 75	5 6
72 00 65 00 73 00 5C 00 6E 00 75 00 63 0	00	6C 00	65	00	61	00	72	00	2D	00	65	00	78	00	70	00	6C (00 6	F (00 7	3 00	0 6
00 6F 00 6E 00 2E 00 6A 00 70 00 67 00 0	00	00 00	00 0	00	00	00	00	00	00	00	00	00	00	00	00	00	00 0	0 0 0	0 0	0 00	0 00	0 1
	00	00 00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00 0	0 0	0 0	0 0	0 00	
00 00 00 00 00 00 00 00 00 00 00 00 00	00	00 00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00 0	00 0	0 0	0 0	0 00	0
00 00 00 00 00 00 00 00 00 00 00 00 00	00	00 00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00 0	0 00	0 0	0 00	0 00	0
	00	00 00	00 00	00	00	00	00	00	00	00	00	00	00 0	00	00	00	00 0	0 0	0 0	0 00	0 00	
	00	00 00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00 0	00 0	0 0	0 00	0 00	0 0
foo oo	00	00 00	00 0	00	00	00	00	00	00	00	00	00	00	00	00	00	00 0	0 0 0	0 0	0 00	0 00	0 (
400 00 00 00 00 00 00 00 00 00 00 00 00	00	00 00	00 00	00	00	00	00	00	00	00	00	00	00	00	00	00	00 00	00 0	0 0	0 00	0 00	
	00	00 01	, 00	00	00	00	00	00	00	00	00	00	00	0.0	00	00	00 0	10 0	0 0	0 0	0 00	

图 3-55 回收站记录文件中操作系统版本解析

0x08~0x0F 按小端顺序解析为 18218,表示被删除的文件逻辑大小是 18218 字节(与 EnCase 解析的 nuclear-explosion.jpg 文件逻辑大小一致),如图 3-56 所示。

le EnCase Forensic (版本 7.12.01)																						
* · □ 案例 (123) · Q 视图 · O 工具 · セ EnScript · 2 添加证据 ·																						
白家 品证据×																						
○○?正在查看(入口)•□拆分模式•□条件• ~过滤器• ○村	标签。	应 文材	制枪者	£+ #	- ES	选择	原始	度蒙	• 5	书签	• 🗃	转至3	2件	9	查找	相关	项目	• 10	入口	• 19	获取	+ 24
・CI含入口 ・CI層 malone	M	表包	时间	线	F 图	库 85.47	73															
> c⊒ ≝ SExtend > c⊒ ≝ SRecycle Bin			-	21(2)	p ove	名称	13				8	Rs Es	686	文件	扩展	名;	逻辑;	大小	种乡	ŧ 3	5名分	析
-o□		BitL des	ktop i	r Reci ni 4 ing	overy	Key	6C89	4E50	-13B	1-48				bd ini				906 129 544	文档 Wind	0		
► OD Boot	04	= SIA	FR6IT	ipg	-						-			ipg				544	图片			
Colle Documents and Settings Colle MSOCache Colle Perfl.ogs		I SIYO	0500 lear-e	7.bt xplos	ion.jp	g								bd ipg				544 18,218	又档			T
 ○○□ Program Files ○○□ Recovery ○○□ Recovery ○○□ Users ○○□ Windows ○○□ Windows 	7 8 9 10 11 12	R SR SR PH SR SR SR SR SR	/8WJ GWKT ROU7(DTO_ /3OK /EJS	89.jpc 8L.JF 0A.jpc 02.jpc RQ.jp VS.jp) 9 9 9 9	转	到 解释: ① Ei	选中的 ttle-E g-En	的文本 ndiar dian	1	_					×	1 34 1 1 1 1	7,299 13,232 16,416 15,017 18,723 16,160	图图图图图图图			
COL SExtend SRECYCLE BIN	<					į.	O JI	他	18	3218					\$					_		
 リ字段 当报告 日文本 四十六进制 業解码 三文档 三抄本 つ透項 3 代码页・A 文本样式・A 査技 3 円目 「圧縮抑限」 00001 00 00 00 00 00 00 2A 47 00 00 00 00 	F 图) 1000	t = 1	空制 f	7 - 20 69	文作 8B			l	602	24	l		収消	i	l		0	73	00 1	35	00 7	72
$ \begin{array}{cccccccccccccccccccccccccccccccccccc$	6C 0 00 0 00 0 00 0 00 0 00 0 00 0	0 00 0 00 0 00 0 00 0 00 0 00 0 00 0 0	6C 00 00 00 00 00 00 00	00 61 00 00 00 00 00 00 00	6F 00 00 00 00 00 00 00	72 00 00 00 00 00 00		2D 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00	65 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	78 (00 (00 (00 (00 (00 (00 (00 (0		70 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	6C 00 00 00 00 00 00 00	03 00 00 00 00 00 00 00	00 6F 00 00 00 00 00 00	74 00 00 00 00 00 00 00 00 00 00	00 73 00 00 00 00 00 00	75 00 00 00 00 00 00 00 00 00 00 00 00 00	

0x10~0x17 字节(如图 3-57 所示)选中后,使用 EnCase 解码功能,按照"Windows 日 期/时间"格式解析即可得到文件的删除时间,如图 3-58 所示。

图 3-56 回收站记录文件中文件大小解析

 ③ と 広格 本 (入口)・二 拆分模式・皿 条件・ ギ 过滤器・ ○ 杯签・ ② 文档检査・* □ 志持版始投索・ ○ 书签・ 圖 特 金 文件 (④ 査技相关項目・ ⑤ 入口・ 匀 获取・ ○ ○ ⑦ た 正在 査 石 (入口)・二 拆分模式・皿 条件・ ギ 过滤器・ ○ 示 签・ ② 文档检査・* □ 志持版始投索・ ○ 书签・ 圖 特 金 文件 (④ 査技相关項目・ ⑤ 入口・ 匀 获取・ ○ ○ ⑦ た 正 査 方 ⑤ ○ ③ 差 Stend ・ ○ □ 第 ■ Stend * ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○
 ○○○ 大 ○○○○ 大 ○○○○ 大 ○○○○ 大 ○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○
- ○ご愛 入口 - ○ご愛 入口 - ○ご愛 入 - ○ご → - ○ご@ 入 - ○ご@ 人 - ○ご@ A - ○ご@ 人
COLUM SEctend COLUM SECTION COLU
COLL RC
Coll a Statesycle Bin Coll a Sta
Coll S-15-21-377413048-683992614-3010368698-1000 coll S-15-21-377413048-683992614-3010368698-1000 coll S-15-21-377413048-683992614-3010368698-1000 coll S-15-21-377413048-683992614-3010368698-1001 coll S-15-21-377413048-68392614-3010368698-1001 coll S-15-21-377413048-68392614-3010368698-1001 coll S-15-21-377413048-68392614-3010368698-1001 coll S-15-21-377413048-68392614-3010368698-1001 coll S-15-21-377413048-68392614-3010368698-100 coll S-15-21-377413048-68392614-3010368698-100 coll S-15-21-377413048-68392614-30108-892 coll S-15-21-377413048-68392614-301036898-100 coll S-15-21-377413048-68392614-30108-892 coll S-15-21-377413048-978 coll S-15-21-377413 coll S-15-21-377413 coll S-15-21-377413 coll S-15-21-377413 coll S-15-21-37741 coll S-15-21-377413 coll S-15-21-37741 coll S-15-21-377413 coll S-15-21-37741 coll S-15-21-37741 coll S-15-21-3774 coll S-15-21 coll S-15-21 coll S-1
C =
COLL b3385d3ab5bd2ab5bd2ab5bd3ab5bd2ab5bd3ab5bd2ab5b
COLL Boot COLL Bot
CO→ Documents and Settings CO→ Documents and Settings CO→ Documents and Settings CO→ Documents and Settings CO→ Define
COL MSUCARDE
17 第KVWU89.pg pg 17.299 图片 17 第KVWU89.pg pg 17.299 图片 18 第KRWTRLIPG JPG 1,643,222 图片 1001 Recovery pg 16,161 图片 101 PHOTO_02.pg pg 15,017 图片 101 PHOTO_02.pg pg 15,017 图片 111 第KVOKRA.pg pg 16,160 图片 112 \$KMEJSVS.pg pg 16,160 图片 0013 \$Extend 0013 \$Extend 0013 \$Extend 0013 \$Extend 0013 \$Extend
COL Program Data C
・ の口』 System Volume Information 10 第 PH FOT 0.02 pg pg 15,017 图片 ・ の口』 Users ・ の口』 Microws 11 第 SRV30KRQ.pg pg 18,723 图片 ・ の口』 String ・ の口」 String pg 18,723 图片 12 第 SRMEJSVS pg pg 16,160 图片 ・ の口』 String ・ の口 新 String ・ の目
COUL Users COULD Users COULD Users COULD EXEMPTION COULD COULD COULD COULD COULD C
COL Windows COL Windows COL State COL
○OLDA 法共的人科教 >OLDA D >OLDA D >OLDA SEcted +OT# SPECYCLE PRH ● 学校 日报告 □文本 周十六进制 単解码 □文档 日抄本 下 图片 □控制合 ∞ 文件区域 □许可 出散列集 足属性
○字段 日报告 日文本 四十六进制 単解码 日文档 日抄本 原图片 日控制台 ※文件区域 3 許可 目散列集 2 属性
· 14X 出版目 GE大学 OF 1716291 塑描程 GE大任 コウ学 ていけ デカゼロ 二人口に成 がりり おはたりた G 時日
□ 透現 * 入代码页 * A 文本样式 * A 查找 4 □ □ □ □ 压缩视图 □ □
00001 00 00 00 00 00 00 00 2A 47 00 00 00 00 00 00 70 F0 69 8B 2E C7 CB 01 43 00 3A 00 5C 00 55 00 73 00 65 00 72
03/00 /3 00 5C 00 53 00 61 00 6D 00 2E 00 4D 00 61 00 6C 00 6F 00 6E 00 65 00 5C 00 50 00 69 00 63 00 /4 00 /2 00 62 00 67 00 72 00 6C 00 6F 00 72 00 6C 00 73 00 6C 00 75
14800 00 00 00 00 00 00 00 00 00 00 00 00
18500 00 00 00 00 00 00 00 00 00 00 00 00
222 00 00 00 00 00 00 00 00 00 00 00 00 00
2290 0 00 00 00 00 00 00 00 00 00 00 00 00
37800 00 00 00 00 00 00 00 00 00 00 00 00
40700 00 00 00 00 00 00 00 00 00 00 00 00
444 00 00 00 00 00 00 00 00 00 00 00 00 00

@ EnCase Forensic (版本 7.12.01)

图 3-57 回收站记录文件中文件删除时间解析



图 3-58 EnCase 解码日期时间

0x18~0x21F 字节解析为"C:\Users\Sam. Malone\Pictures\nuclear-explosion.jpg", 即为被删除文件的原始路径(全路径),如图 3-59 所示。

步骤 6: 单击工具栏中的"许可"按钮,可以看到该回收站记录文件的权限信息,其所有 者为 Sam. Malone,如图 3-60 所示,说明文件的删除者即为 Sam. Malone。 99

圖 EnCase Forensic (版本 7.12.01)				
* · □ 案例 (123) · Q 视图 · O 工具 · 号 EnScript · 四添加证据				
在家 凸证据×				
○ O ? 正在查看 (入口)· 三 拆分模式 · 四 条件 · ィ 过滤器 · ○	标签、应文档检查、= 已选择原始搜索、公书签、	· 回转至文件 [3] 查找相关	項目・多入口・分表取	· 点进程 建设备 · 动打开方式 ·
• oG/b 入口	▲ □ 利志 白时间线 町 開皮			
o □	IN THE PERIOD PROT			
+ c C	オコ・11・□ 已迭择 0/85473			
+ o(1) SExtend	2.8	Ba Ba Ea Ma 文件扩展名	逻辑大小 种类 签名分	析 文件类型 一受保护 保护复
* 0.1 8 SKECYCE.DIN			000 -048	
CUE S.15.21.3774130484.683992814.3010368698.1001	J 1 J BILLOCKER RECOVERY Key 6C894E50-1384-48.	00	900 X 13	
+ or11 b3385d33b5bd2acbbcba57e1	U 2 U deskopin	in	129 Windo	
Boot	U 3 W SI/84PQ4 pg	(Pg	544 图片	
oil a Documents and Settings	J 4 Ja SIA Roll pg	IP9	544 SHF	
+ oci ili MSOCache	J 5 J SIYUSUU/DI	bđ	544 × 13	
i o⊒ ji PerLogs	16 an nuclear-explosion.jpg	IPg	18,218 田斤	
FOCULE Program Files	J 7 J SHV8WJ89.00	IP9	17,299 出斤	
i⊧o⊡ i ProgramData	J 8 ad SRGWK18L3PG	JPG	1,643,232 图片	
I O I II Recovery	J 9 a SHOUTOA pg	IPg	16,416 H F	
> 0.1 Ji System Volume Promation	0 10 as PHOTO_02 pg	PO	15,017 田斤	
LOTE Windows	LI 11 LIS SKVJUKRU (pg		18,723 图开	
10716 无序的文件的	U 12(a) SHOME JSVS (pg	IPG	16,160 23,5	
+ older D				
+ o ⊒ li SExtend				
LOCIE SRECYCLE BN	v c			
1) 字段 目报告 回文本 周十六进制 甾醇码 回文档 目抄本	■ 图片 □ 控制台 ⊷ 文件区域 □ 许可 □ 散列集	1. 公居性		
· 济道· ? 伊思斯· A 文本群式· A 表述 · [第四] 西任總國際	(4)			
	00 00 70 F0 69 88 2E C7 CB 01 43 1	5C 00 50 00 69 00	63 00 74 00 75 0	10 Sam Malone Richt
072172 00 65 00 73 00 5C 00 6F 00 75 00 63 00	6C 00 65 00 61 00 72 00 2D 00 65 0	00 78 00 70 00 6C	00 6F 00 73 00 6	9 resinuclear explosi
11100 GF 00 GE 00 2E 00 GA 00 70 00 G7 00 00	00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00	00 00 00 00 00 00	00 lon ind
14800 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00	00 00 00 00 00 00	00
18500 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00	00 00 00 00 00 0	10
22200 00 00 00 00 00 00 00 00 00 00 00 0	00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00	00 00 00 00 00 00	10
				10
23000 00 00 00 00 00 00 00 00 00 00 00 00			00 00 00 00 00 00	10
37000 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00	00 00 00 00 00 0	50
40700 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00	00 00 00 00 00 0	00
44400 00 00 00 00 00 00 00 00 00 00 00 0	00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00	00 00 00 00 00 00	30
48100 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00	00 00 00 00 00 00	30
121800 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00 00 00 00	00		

图 3-59 回收站记录文件中文件原始路径解析

Case Forensic	(版4 7.12.01)						
■・□ 案例 (123)・4	4、视图・掌工具・	* EnScript • 🕾	添加证据、	e			
◎家 ②证据×							
○ ● ? 正在查看 (入	、口) * 巴 拆分模式	• 四条件 • 7 过	[滤器▼-□林	宗签 •	▶ 文档检查 • * 已选择原始搜索 • ≫ 书签	• • • • • • • • • • • • • • • • • • •	@ 查找相
• 6日告入日			^	[m 20]	志 の財間线 肥 図底		
🔺 o 🗔 💹 malone					to all the second		
• 00 C				NA TH	・2↓・□已选择 0/85473		
► OCI SExtend	Bin				名称	Re Re Ec las	文件扩展名
-00 S-1-5-2	1-3774130484-6639	992614-301036869	8-1000	0.1	Bill ocker Peroven Key 6C804E50 13B4 48	100000000000000000000000000000000000000	byt.
o⊡≣ S-1-5-2	1-3774130484-6639	92614-301036869	8-1001	122	a billocker kecovery key ocos4230-1304-40		ini
> o⊡] b3385d33	3b5bd2acbbcba57e	1		13	SI784PO4 ing		ing
⊳o⊡ iii Boot				4	= \$IAFR6IT ipg		ipa
-o Documen	ts and Settings			5	1 \$IY05007.txt		txt
Not MSOCac	ne			0 6	nuclear-explosion.jpg		ipg
PenLogs	Filos			07	RV8WJ89 ipg		ipg
Program	Data			08	SRGWKT8LJPG		JPG
Pol Recovery				09	a \$RR0U7OA.jpg		ipg
> o System V	olume Information			0 10	R PHOTO 02 jpg		ipg
⊳o⊡ II Users				0 11	SRV30KRQ ipg		ipq
▷ o□ Windows	20120		~	<			
○字段 国报告 □	文本 圖十六进制	篇 解码 国 文相	当]] 抄本	下 图片	□ 控制台 ∞ 文件区域 □ 许可 □ 散列	및 ⊇属性	
山・針・□已选择O	/6 四拆分模式。	↓ 浏览数据					
名称	ID	属性	许?	ŋ			
1 a Low Integrity L	S-1-16-4096	必需	[NW] [Inh A	CEJ			
2 Administrators	S-1-5-32-544	允许	[FC] [M] [R	&X] [R]			
3 System	S-1-5-18	允许	[FC] [M] [R	&X] [R]			
4 A Sam Malone	S-1-5-21-377413	分许	[FC] [M] [R	&X] [R]			
🗆 5 🗟 Sam Malone	S-1-5-21-377413	所有者					
G G None	S-1-5-21-377413	组					

图 3-60 文件删除者信息解析

步骤 7:联系所学注册表取证相关知识,在注册表中查看文件删除者的相关信息。在 C:\Windows\System32\Config 下找到注册表文件"SAM",如图 3-61 所示。

步骤 8: 解析该复合文件"SAM",找到 SAM\Domains\Account\Users 的文件夹,可以 看到 000003E9 文件夹(图 3-62),而十六进制 3E9 的十进制数为 1001,与回收站目录文件夹 SID 中的 UID(如图 3-63 所示: 1001)一致,说明删除文件的用户就是 3E9,即该 000003E9 文件夹为 Sam. Malone 的用户文件夹。

步骤 9: 解析 000003E9 文件夹中的文件,其中 F 文件记录了用户创建时间等信息,V 文件记录了用户名和 SID 等信息,不再具体一一解析,如图 3-64 所示,即为用户名。

由此,不仅得到被删除文件的相关信息,更进一步获知删除者的相关信息。

100_
	100.000 No. 342								
素 写氏版×									
○ + 正在查看 (入口)· 三 拆分模式 · 即 条件 · # 过)	波田・ つる	、 答・ 」 文档检査・ ・ 己進 目前 指数 を ・ 、 书答	· 通转至文件 』 查找相	关项目•复	λD •	1)获取•	心进程 副设	各•司打开	153
+ oC) a sevicing	^	四对方 白时间接 医鼻炎							
⊢o())∦ Setup									
og ji ShelNew		# L • 1: • L C151 0185473							
GOL SoftwareUrstribution		28	Bi Bi Ei Bi 文件扩展名	逻辑大小	102	签名分析	文件表型	委保护	10
of all system		CL 2 L BCD Templete L CC	100	25.000	et-100				1
• oClill System32		C # D CONDONENTS	100	10,660,800	4.50				
- o() 0409		C B COMPONENTS LOC	102	1024	広田				
- o() Advancedinstallers		D 10 D COMPONENTS LOG1	1001	262 144	72/18 7				
ol⊒≣ ar SA		11 11 COMPONENTS/Fcced2ed.6e01.11de.8hed	N	65 536	*				
-oGiji bg-BG		112 COMPONENTS//ccort2od.6e01.11de.8hed	southans.	524 288	Ŧ				
► o(3) Boot		13 DEFAULT	- regrand-	262 144	+10				
Pourge caroot		O M D DEFAULTLOG	106	1.024	中田				
Cale Calenterity		0 15 DEFAULTLOG1	1061	115 712	¥				
⇒ ol⊒i com		CT 10 T SAM		262.144	未知				
+ config		G 17 J SAMLOG	LOG	1.024	应用				
ociji cs-CZ		G 18 G SAMLOG1	LOG1	58,368	£				
o⊖i⊯ da DK		G 19 L SECURITY		262.144	未50				
ola de DE		220 D SECURITYLOG	LOG	1,024	应用				
FOLDE DISM		2 21 LI SECURITYLOG1	LOG1	21,504	£				
> oug anvers		22 D SOFTWARE		33,816,576	未知				
of all eLGR		23 SOFTWARE LOG	LOG	1,024	应用				
oCJL en		24 D SOFTWARE LOG1	LOG1	262,144	£				
> o() iii en-US		25 D SYSTEM		11,534,336	未知				
o() es ES	~	26 SYSTEMLOG	LOG	1.024	应用				

图 3-61 注册表文件"SAM"

⑥ EnCase Forensic (版本 7.12.01)
 • ③ 案例 (123) • ○ 視图 • ◎ 工具 • ○ EnScript • 忌添加证据 •

ODIS SAM		列表 ①时间接 汇 图底	↓ 1 = 0 +(1, 1, 1)	1.136-11361	1.7.911	E.753H
 CMI-CreateHive(899121E8-11D8-44B6-ACEB-301713D5ED8C) COSAM 	#	□• 1 • □已选择 0/144				
OCH Domains OCH Account		名称	Bis Ris Es las	文件扩展名	逻辑大小	种类
▷ c□ Alases	01	D.F.			80	未知
ocal Groups	02	2 D V			472	未知
000001F4	13	UserPasswordHint			27,812	未知

图 3-62 SAM 注册表文件解析



⑥ EnCase Forensic (版本 7.12.01)			
** 3 案例(123)* 4 視用 * 0 工具 * 5 EnScript * 2 添加証拠 *			
な家 四征数×			
○ O ? 正在在看 (SAM) · 巴努分模式 · # 条件 · # 过滤器 · ○标	答· ⑤文档检查· + 已活样原始搜索· ③书签	· iei 转至文件 @ 查找相关项目 · So 入	口·匀获取·点进程 副设备·司打开方式·
・ cc:(* SAM ・ cc:)』 CM CreateHive(899121E8-11D8-4486 ACEB-301713D5ED(・ cc:)』 SAM	四 列表 日时间线 - 原 田岸 タ ヨ・11 - 〇 己追拝 0/144		
colla Domains colla Account	名称	BB BB BB 文件扩展名 逻辑大小 科	类 签名分析 文件类型 受保护 保护
COUL Alases COUL Groups COUL Users	21_1F 22_3 V 23_3 UserTile	00 #3 472 #3 27 812 #3	2 0
Culi 00000175 Culi 00000085 Culi 00000089 >Culi Names >Culi Names >Culi Names >Culi Names	J UserPasswordHint	26.43	
11 字段 日报告 回文本 同十六进制 無解码 回文档 日抄本 新	图片 口控制台 …文件区域 口许可 当数列	集 立属性	
○ 透明、3 代码页・A 文本样式・約 査我 □ □□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□			
$ \begin{array}{cccccccccccccccccccccccccccccccccccc$	$ \begin{array}{cccccccccccccccccccccccccccccccccccc$	$ \begin{array}{cccccccccccccccccccccccccccccccccccc$	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0

图 3-64 注册表文件中用户信息的解析

101

¢

3.5.4 实验小结

回收站文件夹中, \$R 文件记录原始文件内容, \$I 文件记录恢复被删除文件的必要信息(文件大小、被删除时间、原始路径及文件名称)。当恢复被删除文件而原始目录不存在时,利用 \$I 文件的信息可以重建目录。同时,联系回收站文件夹与注册表文件,可获知删除者的重要信息。在计算机调查取证过程中,需时刻记得回收站的重要作用,在回收站中出现的只字片语,很有可能对案件的侦破起决定作用。

3.6 分区恢复

3.6.1 预备知识:磁盘分区原理

在使用计算机进行数据存储与读取的过程中,分区丢失是一种比较常见的故障表现形式。由于意外断电、删除、格式化,或罪犯分子为妨碍案件调查而恶意破坏等原因,分区可能 会被删除或破坏。因此,无论是在取证调查中为了发现证据,还是为了不影响用户正常使 用,恢复被删除的分区都有着重要的意义。

1. 硬盘分区

硬盘分区是在一块物理硬盘上创建多个独立的逻辑单元,这些逻辑单元就是C盘、D盘、 E盘等,又称为逻辑卷。

在实际分区时,通常把硬盘分为主分区和扩展分区,然后根据硬盘大小和使用需要将扩展分区继续划分为几个逻辑分区。建立硬盘分区的步骤是:建立主分区→建立扩展分区→ 将扩展分区分成多个逻辑分区。硬盘划分多个分区后,可以用于存放不同类型的文件,如存 放操作系统、应用程序、数据文件等。

随着科技的发展,硬盘的容量越来越大,市场上1TB或2TB的大容量硬盘已经很常见。大容量硬盘给用户提供更多存储空间的同时,也使得在创建硬盘分区之前,好好地规划 硬盘分区的方案成为必要。合理划分分区可以方便用户更好地管理自己的硬盘。

2. MBR 的数据结构

主引导记录(Master Boot Record, MBR)是采用 MBR 分区表的硬盘的第一个扇区,即 C/H/S 地址的 0 柱面 0 磁头 1 扇区,也叫作 MBR 扇区,共 512 字节。当计算机启动并完成 自检后,首先会读取磁盘的 MBR 扇区。MBR 主要由三部分组成:引导程序、分区信息表、 结束标志。其中引导程序占用 446 字节,主要用于硬盘启动时将系统控制权转移给用户指 定的并在分区表中登记了的某个操作系统区;分区信息表占用 64 字节,主要负责描述磁盘 内的各分区情况;结束标志为 2 字节"55 AA"。MBR 数据结构如图 3-65 所示。



图 3-65 MBR 数据结构

MBR 主要功能如下:

① 首先检查硬盘中分区表是否完好;

② 从分区表查找可引导的"活动"分区;

③ 将活动分区中第一逻辑扇区数据加载到内存中。 在 DOS 分区中,该扇区内容被称为 DOS 引导记录,简称 DBR。

3. 分区表项数据结构

分区表用于记录分区信息,从 MBR 的第 0x1BE 字节开始,共 64 字节,其中共有 4 个分 区表项,每个表项 16 字节,各字节含义如图 3-66 所示。

		16学	<节		
00	00 00 00	00	00 00 00	00 00 00 00	00 00 00 00
Bootable	Starting Sector	Partition Type	Last Sector	Relative	Total Sectors
引导分区	起始扇区	分区类型	结束扇区	相对扇区数	总扇区数

图 3-66 分区表项数据结构

引导标志只有两种可能值,0x80为可引导(即表示该分区为操作系统分区),0x00为不可引导;分区类型标志表明它所描述的分区类型,如NTFS的类型值为0x07、FAT的类型 值为0x0B;起始扇区及结束扇区均以CHS方式表示,CHS区域的值主要用于较老的操作 系统,C、H、S分别代表磁盘的柱面号、扇区号、磁头号;相对扇区数(分区起始逻辑扇区)及 占用总扇区数均以LBA方式表示。分区起始LBA地址是非常重要的参数,如果该区域数 据受到破坏,操作系统将无法找到文件系统分区或扩展分区的起始位置。

如果在没有人为因素改变分区的情况下,因意外而导致的磁盘显示分区丢失、分区显示 未格式化等,应该首先检查主分区表是否损坏,通过查看现有分区表描述的各个分区的前后 关系是否合理、跳转到分区起始扇区查看是否为正常的 DBR 来判断故障原因。

3.6.2 实验目的与条件

1. 实验目的

通过本实验,读者重点掌握以下内容:

(1) 掌握 MBR 引导扇区中分区表的解析过程;

(2) 掌握使用 EnCase 工具进行分区恢复的方法。

2. 实验条件

本实验所需要的软硬件清单如表 3-8 所示。

序号	设备	数 量	参数
1	取证工作站	1台	Windows XP 以上
2	EnCase 软件	1套	EnCase7
3	检材 U 盘 (包含证据文件"Malone's HDD 1A. Ex01")	1个	无

表 3-8 分区恢复实验清单

3.6.3 实验过程

步骤 1: 打开 EnCase 软件,新建案例并添加证据文件"Malone's HDD 1A. Ex01"。

步骤 2: 单击工具栏中的"设备"按钮,选择"磁盘视图"选项,如图 3-67 所示,即可进入 磁盘视图。

步骤 3: 单击磁盘视图下"查看簇"按钮前的复选框,可在扇区和簇视图之间切换,如 图 3-68 所示。 103

- 电子数据取证实训 -

104

Encare roreine (gen riteor)	A CONTRACTOR AND							0 X
**:1 第例(123)*Q 夜田・0 上共・4E たかしのにおよ	nScript • Crap interaction •							
○ ● ↑ 正在在看(入口) · 二 新分稽式 · 件	条件· · · · · · · · · · · · · · · · · · ·	•	· 查找相关项目• %	入口、匀花取、	-5-999	· · · · · · · · · · · · · · · · · · ·		
•03% 入口	四列表 马时间线 军 图库					些 截点视用	1	
cCa≌ materie + polae C + polae D	オヨ・社・コ 出活計 0/85473	オコ・社・ロビ店計 0/85473						
	名称	副副副副	扩展名 逻辑大小	种类 签名分析	文相美	25.9. X11 X	最后访问时间	文件叙述
	010C 0200	□1/wC 4,096文件表 近年… □2/wD 4,096文件表 数利…						07/14/09 10 01/30/11 09
	USB TOTOLAIN		43,120,590	*34		封捕組食活构		

图 3-67 EnCase 磁盘视图



图 3-68 切换扇区和簇视图

步骤 4: 在扇区视图下(即显示的是硬盘上各扇区的状态和数据),单击第一个小方块 (LBR0 号扇区),即为主引导记录 MBR 扇区,单击中间工具栏中的"十六进制"按钮,查看该 扇区中的十六进制数据,如图 3-69 所示。



图 3-69 MBR 扇区

步骤 5:联系所学的 MBR 扇区数据结构可知,结束标志"55 AA"前的 64 字节为分区信息表,如图 3-70 所示。共分为 4 个分区表项,每个分区表项为 16 字节,经分析发现仅有 2 个分区表项有数据,即分区信息表中仅存在 2 个分区信息。

固文/	5 開	1+7	进制	1	解码		控制	台																				□ 镇定
白透り	E *2	代码	页 。	AX	木样	式.	25	生找	4	10																		
00033 027 CB 05400 061 C1 10800 135 B8 1627 52 2167 C 2437 5 2705 3 297 F6 324 F0 351 F8 3780 0 4057 3 4326 5	C0 FB 55 01 00 7D 32 66 AC 24 45 76	8E B9 C6 00 68 02 80 55 B0 31 53 00 32 72 65 00 20 20 20 20 20 20 20 20 20	D0 04 46 74 00 BB 7E AA FF 9 66 7C 00 03 72 6D 00	BC 000 111 03 7C 00 00 75 E6 02 55 00 74 49 6F 00 00	00 BD 05 FE 68 7C 80 6E 64 01 66 00 96 E 72 4D 09 6E 72	7 C BE C6 46 01 8A 0F FF 88 72 68 CD BB 76 20 69 7B	8E 07746 1005684 76752C 00018 07616C 7399A	C0 80 10 66 68 00 8A 00 00 66 00 60 60 60 60 60 67 3 19	8E 7E 000 600 100 8A 000 E88 688 000 B7 64 69 61 69 7 67 67 67 67 67 67 67 67 67 67 67 67 6	D8 00 B4 80 00 76 B2 8D B8 07 00 07 05 64 64 64 64 64 64	BE 000 41 7E B4 01 80 00 00 BB 66 EB CD 20 69 67 45	000 7C BB 100 422 8A EB 75 BB 000 68 08 100 700 620 000	7 C 0 B AA 0 0 8 A 4 E 8 4 17 CD 0 0 0 0 A0 EB 6 1 6 7 6 F 0 0	BF 0F 555 74 56 02 55 FA 16 66 7C 86 F2 72 20 70 80	00 85 CD 26 00 8A 32 B0 66 68 00 07 F4 74 65 20	06 0E 13 66 8B 6E E4 D1 23 00 00 EB EB 69 70 72 21	89 01 5D 68 F4 03 8A E6 C0 02 66 03 FD 74 65 61 00	000 833 72 000 CDD CDD 56 64 75 000 61 A00 2B 699 72 74	02 C5 0F 000 13 13 00 E8 3B 00 68 B5 C9 6F 61 69 FE	FC 10 81 00 9F 66 CD 83 66 66 66 00 07 E4 6E 74 6E FF	F3 E2 FB 00 83 61 13 00 81 68 00 32 64 20 69 67 FF	A4 F1 55 66 C4 73 5D B0 FB 08 07 E4 EB 74 6E 20 00	50 CDAAFF 10 1CEB DF 54 00 CD 05 00 61 67 73 08	68 18 75 9E FE E6 43 00 1A 00 24 62 20 79 00	1C 888 09 88 4E 81 60 50 00 5A 07 02 6C 73 73 00	06 56 F7 68 14 11 3E E8 41 66 32 8B E0 65 79 74 00	$ \begin{array}{llllllllllllllllllllllllllllllllllll$	^
4880.0	00	02	00	00	DO.	00	00	00	00	00	00	00	00	02	00	00	00	00	00	00	00	00	0.01	55	0.0	00	0_ P37 P37 A A	~

图 3-70 分区信息表

步骤 6:选中该 64 字节分区信息表,单击中间工具栏中的"解码"按钮,选择"Windows-分区入口"选项,可得到解析完成后的分区信息,如图 3-71 所示。



图 3-71 分区信息表解析

可以看出,该磁盘共有2个分区,其中第一个分区为活动分区(系统盘)。第一个分区起 始位置逻辑扇区为2048,占用总扇区数为39841792。第二个分区起始位置逻辑扇区为 40663040,占用总扇区数为1275904。

步骤 7: 在扇区视图下,鼠标停留在第一个扇区并右击,在弹出的快捷菜单中选择"转到"选项,跳转到 2048 号扇区(图 3-72),即为分区 1 的起始扇区 DBR,如图 3-73 所示。



图 3-72 跳转到分区 1 起始扇区



图 3-73 分区 1DBR

步骤 8: 同样,在扇区视图下,鼠标停留在第一个扇区并右击,在弹出的快捷菜单中选择 "转到"选项,跳转到 40663040 号扇区,即为分区 2 的起始扇区 DBR,如图 3-74 所示。由此 找到了磁盘上的两个分区,可进一步对分区引导记录 DBR 解析,获取各分区重要参数信息。



图 3-74 分区 2DBR

步骤 9: 分区 1 与分区 2 大小相加为 41117696 扇区,而物理磁盘总大小为 59.8GB (125337600 扇区),如图 3-75 所示。由此可见,已知的两个分区仅占了该磁盘的小部分空

间。存在未使用磁盘空间或删除分区的情况。

The second s	A REAL PROPERTY AND A REAL
□字段 □报告 □文本 翌十	/六进制 論解码 国文档 国抄本 影图片 回控制台 ∞文件区域 副许可 回散列集 歐属性
*放大 = 缩小 @ 100% • 📑 🛽	2 · · · · · · · · · · · · · · · · · · ·
名称	malone
逻辑大小	0
种类	文件夹
项目路径	malone
真实路径	123\malone
描述	物理磁盘, 125,337,600 扇区数 59.8 GB
获取的文件	08/20/00 03:35:04
已初始化的大小	0
物理大小	512
开始范围	050
文件区域	1
物理位置	0
物理扇区	0
证据文件	malone
文件标识符	0
全球唯一标识符(GUID)	4f672608cf5d86ac9bf38b135b795953

图 3-75 磁盘基本信息

步骤 10:由分区 1 的起始扇区与占用扇区可计算得到分区 1 的结束扇区,发现分区 1 的结束扇区与分区 2 的起始扇区之间存在大量松弛区,不符合常理,判断可能存在删除分区。

步骤 11: 跳转到分区 1 结束扇区后的 1 扇区,即 39843840 号扇区,查看该扇区十六进 制数据,猜测可能为 DBR,且分区文件系统为 FAT32。单击工具栏中的"分区"按钮,选择 "添加分区"选项,如图 3-76 所示。在弹出的"添加分区"对话框中,选择卷类型为"FAT32", 单击"确定"按钮,如图 3-77 所示。



图 3-76 分区的添加

步骤 12:关闭并重新打开该证据文件(EnCase 不能自动刷新,必须手动关闭重新进入),发现除了原有的两个分区外,多了一个分区,即完成了删除分区的恢复,如图 3-78 所示。

-	申	子	数	据	取	ìF	实	ill	1
	-		72 X	1/6	ᅭᄉ	- LII	75	พก	

⊈家 ^{malone ×} 己证据 ×		
※分区・□ 查看族 ※自动范围 - 转到 □ 导出 ◇	书签 -	
		^
81813228	添加分区	×
83843218	<u> </u>	
8381338	39843840 () () () () () () () () () () () () () (^
83833728		
	FAT 32 exFat	
83844928	EXT2	
882200	型用 MF12 EXT3 和合称的出现 新 (D=Auto) Reiser	
8週4938	8 CHARTER (CHARTER)	
□ 文本 親十六进制 論解码 □ 控制台	分区中的所有扇区 Solaris UFS CDFS	口領定
000 1 58 90 4D 53 44 4F 53 35 2E 30	819200 C UDF	MSDOS5.0-1-0-?9
02700 00 F8 5F 02 00 80 0C 00 19 03 05400 00 00 00 00 00 00 00 00 00 00 80 09120 45 41 54 33 32 20 20 20 32 50	註释:必须在"证据"选项卡中重新加载这些条目才能看到更改	€)@\$(zNO NAME
10856 40 B4 41 BB AA 55 CD 13 72 10 1358A 56 40 B4 08 CD 13 73 05 B9 FF	确定取消) A>U rúľu oA tpF o- 10
162E2 86 CD C0 ED 06 41 66 0F B7 C9 18900 77 32 66 8B 46 1C 66 83 C0 0C		[Åi A! Éf-ál‰Fə∫u8∫-* 2[κF I∫Å » €' è+ é, ü]
2167D 88 F0 AC 84 C0 74 17 3C FF 74 243F9 7D EB E0 98 CD 16 CD 19 66 60	09 B4 0E BB 07 00 CD 10 EB EE A0 FB 7D EB E5 A0 80 7E 02 00 0F 84 20 00 66 6A 00 66 50 06 53 66)kōn At kyt ' » i el 0jeå 0jea1 i r €, fi IP St
27068 10 00 01 00 B4 42 8A 56 40 8B 297F8 72 03 F9 EB 2A 66 33 D2 66 0F	F4 CD 13 66 58 66 58 66 58 66 58 EB 33 66 3B 46 B7 4E 18 66 F7 F1 FE C2 8A CA 66 8B D0 66 C1 EA	h BSV@k0l1XXXXX23;F or úe130/ N 1-fpÅSErbtÅé
35181 C3 00 02 66 40 49 75 94 C3 42 37800 00 00 00 00 00 00 00 00 00 00 00	4F 4F 54 4D 47 52 20 20 20 20 00 00 00 00 00 00 00 00 00	Ă-1@u/ABOOTMGR
40500 00 00 00 00 00 00 00 00 00 00 00 4326D 6E 76 65 20 64 69 73 6B 73 20	00 00 00 00 00 00 00 00 00 00 00 00 00	Re move disks or other media i
4590D 0A 44 69 73 6B 20 65 72 72 6F 48679 20 74 6F 20 72 65 73 74 61 72	72 FF 0D 0A 50 72 65 73 73 20 61 6E 79 20 6B 65 74 0D 0A 00 00 00 00 00 AC CB D8 00 00 55 AA	Disk errory Press any ke y to restart===EØ -U#



⑥ EnCase Forensic (版本 7.12.01)

■ • □ 案例 (123) •	Q视图·O工具·号EnSci	ipt · 23添加证据 ·					
每家 G证据×							
○○?正在查看(入口)、二拆分模式、66条件	 ▼ 讨波器 • ○ k 	· 签· 应 文档检查· =	已选择原始搜索 ▼ 、	→ 书签・团 抄至文(+ 0 查找相	关项目•
• 0日告入日		the period	四列表 6时间线	图库	- 1	11001000	88.0U.
→ o 🛛 🖉 malone			企用·41·口已洗掉	0/85528			
				Ath	Dr. Dr. Ex. Int	六供給國 名	29240 L.J.
⊧o⊡⇔ E				名称		义件别 胰名	逻辑大小
							4,09
			0200				4.05
			□4 型未使用的磁盘空(ศ			42 701 159
			Card an Argonandan ar	-		1	12,101,100
*放大 = 縮小 @ 從 文件系统	100% • 🗋 🗔 FAT32						
每个簇的扇	×数 8						
每个扇区的	子节 512						
所有加区	819,200 415,006 ex # #	(206 MP)					
点簇数	101 376	(390 MB)					
未分配的	415,203,328 字节数	(396 MB)					
空闲簇	101, 368						
已分配的	32,768 字节数 (32 K	B)					
卷名称	PROJECTS						
老偏移量	39, 843, 840						
驱动器类型	固定						
57 IX.	00						
迷型	已经恢复						
起始扇区	39, 843, 777						
所有扇区	819, 263						

图 3-78 删除分区的信息

108_

•

3.6.4 实验小结

当磁盘中的某个分区被删除后,分区中的数据并未被真正删除。此时,对应的分区表项 会被清零,被删除的分区变为未分配状态且数据不可访问。要恢复被删除的分区,需要找出 分区的起始位置、大小和分区类型等重要信息,然后将其写回被清零的分区表项。通常来 说,在磁盘中创建多个分区,分区会占用所有磁盘空间。此时,通过查看现有的分区信息,找 到被删除分区的位置并不复杂。接着,进一步分析被删除分区的具体数据可以判断出文件 系统类型。

EnCase 具备了分区恢复功能,在分区恢复时,应该首先检查主分区表是否损坏,通过查 看现有分区表描述的各个分区的前后关系是否合理、跳转到分区起始扇区查看是否为正常 的 DBR 等来综合分析、判断并恢复分区。

读者也可利用 WinHex 工具尝试删除分区的恢复操作。

3.7 FAT 文件系统数据恢复

3.7.1 预备知识: FAT 文件系统原理

文件系统是操作系统用于明确磁盘或分区上的文件的保存方法和数据结构,即在磁盘 上组织文件的方法。一个分区或磁盘作为文件系统使用前需要初始化,并将数据结构写到 磁盘上,这个过程就叫建立文件系统。FAT32、exFAT、NTFS 是目前最常见的三种文件 系统。

FAT(file allocation table,文件分配表)文件系统是 Windows 操作系统所使用的一种 文件系统,它的发展过程经历了 FAT12、FAT16、FAT32 三个阶段。FAT 文件系统用"簇" 作为数据单元。一个"簇"由一组连续的扇区组成,簇所含的扇区数必须是 2 的整数次幂。 所有簇从 2 开始进行编号,每个簇都有一个自己的地址编号。用户文件和目录都存储在 簇中。

FAT 文件系统由保留扇区、FAT 区和数据区组成,数据结构如图 3-79 所示。

保留	留扇区	FA	TZ	~~~~	数据区	_
分区引 导记录 DBR	其他保 留扇区	FAT1	FAT2	根目录	用户文件及文件夹	

图 3-79 FAT 文件系统数据结构

1. DBR 区

分区引导记录 DBR,也称为操作系统引导记录,位于相对扇区 0 扇区。DBR 由 5 个部 分组成:

① 0x00~0x02: 跳转指令。FAT32 文件系统跳转指令为"EB 58 90"。在汇编当中 0xEB 是跳转指令,0x58 是跳转的地址,而 0x90 则是空指令。CPU 读取到 EB 58 这个指令 时,便跳转到 0x58 这个地址并继续读取指令来执行,而 0x58 地址之后的内容通常都是载入 操作系统的指令。

② 0x03~0x0A: OEM(original entrusted manufacture,代工厂商)代号。

109

③ 0x0B~0x59: BPB(BIOS parameter block,本分区参数记录表)。BPB 参数块记录 着本分区的起始扇区、结束扇区、文件存储格式、硬盘介质描述符、根目录大小、FAT 个数、 簇的大小等重要参数。具体如表 3-9 所示。

		表 3-9 BPB 参数信息
偏移量	字节数	含义
0x0B	2	每扇区字数
0x0D	1	每簇扇区数
0x0E	2	保留扇区数
0x10	1	FAT 个数
0x11	2	根目录项数,FAT32 以突破该限制,无效
0x13	2	扇区总数,小于 32M 使用
0x15	1	存储介质描述符
0x16	2	每 FAT 表占用扇区数,小于 32M 使用
0x18	2	逻辑每磁道扇区数
0x1A	2	逻辑磁头数
0x1C	4	系统隐含扇区数
0x20	4	扇区总数,大于 32M 使用
0x24	4	每 FAT 表扇区数,大于 32M 使用
0x28	2	标记
0x2A	2	版本 (通常为零)
0x2C	4	根目录起始簇
0x30	2	Boot 占用扇区数
0x32	2	备份引导扇区位置
0x34	14	保留
0x42	1	扩展引导标记
0x43	4	序列号
0x47	10	卷标
0x52	8	文件系统

④ 0x5A~0x1FD: 引导程序。在 Windows 98 之前的系统中,这段代码负责完成 DOS 三个系统文件的装入。在 Windows 2000 之后的系统中,这段代码负责完成将系统文件 NTLDR 装入,对于一个没有安装操作系统的分区来讲,这段程序没有用处。

⑤ 0x1FE~0x1FF: 结束标志。DBR 的结束标志与 MBR、EBR 的结束标志都相同,为 "55 AA"。

2. FAT 🗵

文件分配表 FAT 是用来描述文件系统内存储单元的分配状态及文件内容前后链接关系的表格。它对于 FAT 文件系统来讲是至关重要的一个组成部分,假若丢失 FAT,那么硬盘上的数据就无法定位,也就不能使用了。由于 FAT 对文件管理的重要性,FAT 有一个备份,即在原 FAT1 后再建一个同样的 FAT2。

根据 FAT 文件系统数据结构可知,FAT1 的起始扇区可由 BPB 中记载的保留扇区数 而获知(保留扇区数的信息位于 BPB 模块 0x0E~0x0F 两个字节),FAT2 的起始扇区可由 保留扇区数+FAT1 占用扇区数(BPB 模块 0x24~0x27)计算所得。

FAT 是由一个个表项组成,其中每一个表项的值对应了相应簇的使用情况,如2号表项对应了2号簇的使用情况,3号表项对应了3号簇的使用情况,以此类推(但是第0项和第1项例外)。FAT 第0项和第1项是系统保留,记录分区所在的介质类型和分区状态。

FAT 32 的每个 FAT 项的大小为 32 位,相当于 4 字节,即从 00-00-00~FF-FF-FF, 不同数值具体含义如下:

① 空闲簇(未分配簇): 00-00-00-00;

② 系统保留簇: 00-00-00-01;

③ 被占用的簇,其值指向下一个簇号: 00-00-02~0F-FF-FF-EF;

④ 保留数值: 0F-FF-FF-F0~0F-FF-FF6;

⑤ 坏簇: 0F-FF-FF-F7;

⑥ 文件最后一个簇: 0F-FF-FF-F8~0F-FF-FF-FF.

FAT 表项的填写规则是:如果该簇是文件的最后一簇,填入的值为 0x0F-FF-FF; 如果该簇不是文件的最后一簇,则填入的值为该文件占用的下一簇号。

3. FDT 区

文件目录表(File Directory Table, FDT)也称为根目录,位于数据区头部(第2簇),用 来存放根目录下的文件的目录项。

根据 FAT 文件系统数据结构可知,根目录起始扇区=保留扇区数+FAT 扇区数×2。

FDT 区是由一个个目录项构成,类似于 FAT。每一个目录项占用 32 字节,记录文件 或者文件夹的名称、属性、大小、起始簇号、创建时间、创建日期、最近访问日期、最近修改日 期等内容,具体如表 3-10 所示。

偏移量	字节数	含义
0 x 00	8	文件名
0x08	3	后缀名
0x0B	1	文件属性(00H 读写; 01H 只读; 02H 隐藏; 04H 系统; 08H 卷标; 10H 子目录; 20H 归档)
0x0C	1	系统保留
0x0D	1	创建时间的 10 毫秒位
0x0E	2	文件创建时间
0x10	2	文件创建日期
0x12	2	文件最后访问日期
0x14	2	文件起始簇号高 16 位
0x16	2	文件最近修改时间
0x18	2	文件最近修改日期
0x1A	2	文件起始簇号低 16 位
0x1C	4	文件长度

表 3-10 FDT 信息

值得注意的是: FAT 分区下,文件在被删除之后,文件对应的文件目录项的第一个字 节会被改为 0xE5,表示该文件被删除,而文件目录项的其他字节没有变化,所以被删除的文 件仍旧能够找到其起始簇,从而使得该文件是可恢复的。

3.7.2 实验目的与条件

1. 实验目的

通过本实验,读者重点掌握以下内容:

(1) 了解 FAT32 文件系统存储原理;

(2) 掌握 FAT32 文件系统各数据结构的解析;

(3) 掌握使用 WinHex 进行 FAT32 文件系统数据恢复的过程。

2. 实验条件

本实验所需要的软硬件清单如表 3-11 所示。

表 3-11 FAT32 文件系统数据恢复实验清单

序号	设 备	数 量	参数
1	取证工作站	1台	Windows XP 以上
2	WinHex 工具	1套	无

3.7.3 实验过程

1. 创建虚拟磁盘 VHD

步骤 1: 打开计算机管理中的磁盘管理。单击工具栏中的"操作"按钮,选择"创建 VHD" 选项,如图 3-80 所示。



图 3-80 磁盘管理创建 VHD

步骤 2: 在弹出的对话框中选择路径及虚拟磁盘大小,单击"确定"按钮,如图 3-81 所示。

步骤 3. 此时,在磁盘管理视图下,可以看到多了一个未初始化磁盘。在该磁盘左边部分 右击,在弹出的快捷菜单中选择"初始化磁盘"选项,设置磁盘分区形式为"MBR",如图 3-82 所示。

位置(L):	
C:\Users\nxl\Desktop\nxl.vhd	浏览(B)
虚拟硬盘大小(S):	GB GB
虚拟硬盘格式	
● VHD(<u>V</u>)	
最大可支持 2040 GB 大小的虚持	以磁盘。
○ VHDX(X) 可支持大于 2040 GB 的虚拟磁道 障事件中恢复。该格式在早于 W 的操作系统中不受支持。	主(最大可支持 64 TB),并且可从电源故 indows 8 或 Windows Server 2012
○ VHDX(X) 可支持大于 2040 GB 的虚拟磁 障事件中恢复。该格式在早于 W 的操作系统中不受支持。 虚拟硬盘类型	主(最大可支持 64 TB),并且可从电源故 indows 8 或 Windows Server 2012
 ○ VHDX(<u>X</u>) 可支持大于 2040 GB 的虚拟磁扩 障事件中恢复。该格式在早于 W 的操作系统中不受支持。 虚拟硬盘类型 ⑧ 固定大小(<u>F</u>)(推荐) 	盐(最大可支持 64 TB),并且可从电源故 indows 8 或 Windows Server 2012
 ○ VHDX(X) 可支持大于 2040 GB 的虚拟磁排障事件中恢复。该格式在早于 W的操作系统中不受支持。 虚拟硬盘类型 ④ 固定大小(F)(推荐) 创建虚拟硬盘时,会为虚拟硬盘 	主(最大可支持 64 TB),并且可从电源故 indows 8 或 Windows Server 2012 文件分配最大大小。
 ○ VHDX(X) 可支持大于 2040 GB 的虚拟磁排 障事件中恢复。该格式在早于 W的操作系统中不受支持。 ▲ 监拟硬盘类型 ④ 固定大小(E)(推荐) 创建虚拟硬盘时,会为虚拟硬盘 ○ 动态扩展(D) 	a(最大可支持 64 TB),并且可从电源故 indows 8 或 Windows Server 2012 文件分配最大大小。
 VHDX(X) 可支持大于 2040 GB 的虚拟磁排障事件中恢复。该格式在早于 W的操作系统中不受支持。 虚拟硬盘类型 固定大小(E)(推荐) 创建虚拟硬盘时,会为虚拟硬盘 动态扩展(D) 虚拟硬盘文件会随着数据写入到 	1(最大可支持 64 TB),并且可从电源故 indows 8 或 Windows Server 2012 文件分配最大大小。 查拟硬盘而增长到其最大大小。

图 3-81 创建和附加虚拟磁盘

磁盘必须经过初始化,逻辑磁盘管理	器才能访问。	
选择磁盘(S): ☑ 磁盘 2		
为所选磁盘使用以下磁盘分区形式:		
○ GPT (GUID 分区表)(G) 注意:所有早期版本的 Windows 都7	F识别 GPT 分区形式。	
	18:5	Rocat

图 3-82 初始化磁盘

步骤4:此时,在磁盘管理视图下可以看到该磁盘显示为"联机"状态,在该磁盘右边部 分右击,在弹出的快捷菜单中选择"新建简单卷"选项,如图 3-83 所示。

步骤 5: 在新建简单卷向导下按需要设置逻辑卷属性信息,如卷大小、卷标等。在格式 化分区步骤,选择文件系统类型为"FAT32"文件系统,如图 3-84 所示。

- 电子数据取证实训

114

基本 238.35 GB 联机	200 M 状态良	OS (C:) 219.62 GB NTFS 状态良好 (启动, 页印	990 MB 状态良好	16.18 GB 状态良好 (恢复	1.39 GB 状态良好 (
一 磁盘 1 基本 1862.89 GB 联机	DATA 1862.89 状态良好	(D:) 9 GB NTFS 子 (基本数据分区)			
■ 截盘 2 基本 1023 MB 联机	1023 M 未分配	B		建简单卷(I) 建跨区卷(N) 建帝区卷(T)	
■ 未分配 ■ 主分	×		雇	性(P)	

图 3-83 新建简单卷

建简单卷向导		
格式化分区 要在这个磁盘分区上储存数据,你	必须先将其格式化。	
选择是否要格式化这个卷;如果要	略式化,要使用什么设置。	
〇不要格式化这个卷(D)		
●按下列设置格式化这个卷(0	<u>)</u> :	
文件系统(E):	FAT32	
分配单元大小(A):	FAT FAT32	
卷标(V):	NTFS 新加密	
☑执行快速格式化(P)		
启用文件和文件夹压	缩E)	
		Doct
	< 工一至(B) 下一页(B) >	取消

图 3-84 格式化分区

步骤 6:完成后,发现在此电脑下,多了一个 FAT32 文件系统的分区 E,如图 3-85 所示,至此,完成 VHD 的创建。

2. 连续存储文件的删除恢复

步骤 1:在上述虚拟磁盘 E中,存入一个图片文件 lena.jpg 并删除该文件。

步骤 2:用 WinHex 工具打开该 E 盘,找到该分区的起始扇区,即引导记录 DBR,如 图 3-86 所示。

步骤 3: 分析引导记录 DBR,获得以下信息(小端):

- (1) 0x0D: 每簇扇区数: 08:8;
- (2) 0x24-0x27: FAT 占用扇区数: 00-00-07-F3: 2035;
- (3) 0x0E-0x0F: 保留扇区数: 10-1A: 4122。

ð



图 3-85 虚拟磁盘 E

19.8 x64 _ #						340	WED CHAN	80 R		2) 1	透明()	L(I)	WT.F	D 1	IR	100	=	SON0	-194	(S)	ANF E1] 日 祝	vinntex - [10.2] 2(件(E) 編編(
	4	1 *	85 H	0 _ 0	34	÷ 1		-161 4	-+	6	4.2		4 14	1 4	1017 010	3.9		Da	1	1	ď	- E 2 a
0+1+5=6 文件, 3 个目					以前	3440	1.															a c [
	第1扇区	文件履性		记录更新时间	設时间	伊			10	別建約	大小 言	文件;	-	展名	Ť							5称▲
		SH		25214239F 1	1000	- 20			37 1	820362 1544025	KB 1	4.0		IN	B							ELED
		CH		4回405月1	同時用	400			P 1 97 1	用中的	KRI	4.0								antin	Inform	tem Volume
		A		報出边界 T	出动用	43			来主	8:H3b	KB	155		a	in					auto	morn	NA.ipg
				超出边界 1	出边界	超			界工	部出版	MB	1.0		-	- 11							T 1
				超出边界 1	出边界	相			件1	記出込	MB #	1.0										T 2
				- 輕出边界↑	出边界	報			界工	副出込	MB 1	2.0										9扇区
100% 空		BE:	^ 驱动	UTF-8	11	F	Е	D	С	В	A	9	8	7	6	S	4	3	2	1	0	ffset
FAT		系统:	文件	spos5.000000		10	1A	08	02	00	30	2E	35	53	4F	44	53	4D	90	58	EB	000000
8510			老标	00 00 00	000	00	00	00	80	00	FF	00	3F	00	00	F8	00	00	00	00	02	000010
		edia:r	-	0000000000		00	00	00	02	00	00	00	00	00	00	07	F3	00	1F	E8	00	000020
89 ki			经水			00 (00	00	00	00	00	00	00	00	00	00	00	00	06	00	01	000030
		(1. W)-	-	O O NAME		20	20	45	4D	41	4E	20	4F	4E	E6	74	93	A7	29	00	80	000040
10 T-0		900C 96%-	State State	132 3Y O D	1	: F4	BC	D1	8E	C9	33	20	20	20	32	33	54	41	46	20	20	000050
87.8			and the second		1 .	1 56	8A	02	4E	88	40	56	88	7C	00	BD	D9	8E	C1	8E	7B	000060
	分配表	进盘空间中的	可见	l OrOO u	1_4	OA	75	AA	55	FB	81	10	72	13	CD	55	AA	BB	41	B4	40	000070
			接导	00 -0 00		CD	08	B4	40	56	SA	2D	EB	02	46	FE	05	74	01	Cl	F6	080000
						B6	OF	66	40	C6	B6	OF	66	F1	BA	FF	FF	B9	05	73	13	000090
					а,	C9	87	0F.	66	41	06	ED	CO	CD	86	E2	F/	3F	E2	80	DI	0000A0
1 分钟以		快關創建于	現象	0 0090	1.5	ZA	7E	83	39	75	00	16	7E	83	F8	46	89	66	El	27	66	000080
		884:	25		W.	01	B9	80	00	BB	OC	CO	83	66	10	46	UB	66	33	11	00	0000000
1		庙区号:	物理		- L	AC	FU	SB	70	07	80	70	FS	Al	03	AS	29	00	ZC	E8	00	0000000
100.0		Part 10.				10	10	16	CD	07	DP	UE	84	70	19	PP.	SC En	20	79	20	84	0000020
184 320 32		2046	Dia	00 000	1.04	0.06	50	10	00	50	66	00	20	04	OP	00	02	70	00	60	66	000020
104,000 1		-	-		a.f.	12	CD	E4	en	40	56	93	42	BA	00	01	00	10	60	66	62	000110
1 066 217 472 3		24	2094	FX FXD FD	FX	03	72	FR	46	38	66	33	FR	58	66	5.8	66	58	66	5.8	66	000120
1,000,017,412.9			-	D NDFD		C2	FE	FI	F7	66	18	4F	87	OF	66	D2	33	66	2A	EB	19	000130
1.0 0			10.86	0 CO ~ V		56	8A	DG	86	1A	76	F7	10	EA	C1	66	DO	88	66	CA	8A	000140
1,010,000,000 9				0 / 000 0	1 en	OF	61	66	13	CD	02	01	B8	CC	0A	06	E4	CO	E8	8A	40	000150
4,0		字节数	句族	O QIUD O	0	41	41	42	C3	94	75	49	40	66	02	00	C3	81	FF	74	82	000160
260,3		98: *	空余	00000000	TM	00	00	00	00	00	00	00	00	20	20	20	20	52	47	4D	54	000170
260,3		RDC:	M.C.			00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	000180
5		区字节数:	毎島			00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	000190
2,082,8		順区: 東京 おんしつま	可用	CCCCCCCCC Di		69	44	0A	0D	00	00	00	00	00	00	00	00	00	00	00	00	0001A0
81	5 C		80.98	errorD ress	sk	3 73	73	65	72	50	0A	0D	FF	72	65	72	72	65	20	6B	73	0001B0
		總慶 :	10:12	key to rest	a	3 74	73	65	72	20	6F	74	20	79	65	6B	20	79	6E	61	20	0001C0
origin		时区:	显示	0000000000	art	00	00	00	00	00	00	00	00	00	00	00	0A	0D	74	72	61	0001D0
Ż		0.000	模式			00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	0001E0
十六进		地址:	偏移	0000 0000	000	AA	55	00	00	01	B9	01	AC	00	00	00	00	00	00	00	00	0001F0
37x16=5		于行款	600	000000000000		00 (00	00	00	00	00	00	00	00	00	00	00	41	61	52	52	000200
		會口:	尚前			00 0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	000210
		0.Rt:	金口			00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	000220
						0.00	0.0	0.0	00	00	00	00	00	00	00	00	00	00	00	00	00	000230
								122	2.2	1.2.1	1.00			122.0	-	-		2.21		2.2	1.2.2	

图 3-86 DBR 扇区

步骤 4: 单击工具栏中的"跳转扇区"按钮,根据保留扇区数(图 3-87),跳转到 FAT1 起始扇区,如图 3-88 所示。

👹 WinHex - [認識)器 E:]				10000						1997-1997-1997-1997-1997-1997-1997-1997			
♀ 文件E 编辑	E) 搜	建索(S)	导	斻(<u>N</u>)	查看	F(V)	工具		₽₩.T.₽	L(1) ;	选项(O) 窗口(W) #	要助(H)		
07830	1	1	1 10		1		101-010	2 4	14	HEX T	ઢ ક્ર≰ ∣ → સિંચિ		à 🖬	P 📫 🔬 🗎 🕄
驱动器 E:														
\												3 小时以前		
文件名称▲							ł	广展名	_	文件/	小 创建时间	修改时间		记录更新时间
SRECYCLE.BIN							E	BIN		4.0	KB 超出边界↑	超出边界↑		超出边界 1
(根目录)										4.0	KB 超出边界↑	超出边界↑		超出边界↑
System Volume	Inform	matio	n						4.0		跳至扇区		×	超出边界 1
X ?ena.jpg							ji	pg		155				超出边界 1
FAT 1										1.0	N		-	超出边界↑
FAT 2										1.0	●逻辑U: 扇	⊠: 4122 □		超出边界↑
]]]引导扇区										2.0)後: 🗌 🗆		超出边界↑
Offset	0	1	2	3	4	5	6	7	8	9	1			UTF-8 A
00000000	EB	58	90	4D	53	44	4F	53	35	2E				5.000000
00000010	02	00	00	00	00	F8	00	00	3F	00				
00000020	00	E8	1F	00	F3	07	00	00	00	00				0000000
00000030	01	00	06	00	00	00	00	00	00	00				
00000040	80	00	29	A7	93	74	F6	4F	4F	20	+ 确定(<u>O</u>)	取消(<u>A</u>)		O NAME
00000050	20	20	46	41	54	33	32	20	20	20	33 C9 8E D1	BC F4 FAT	F32	3¥ Ô □

图 3-87 跳至扇区

Offset	0	1	2	3	4	5	6	7	8	9	A	в	C	D	E	F	1			UTF-8	^
00203400	F8	FF	FF	0F	FF	0F	FF	FF	FF	0F											
00203410	FF	FF	FF	0F	06	00	00	00	07	00	00	00	08	00	00	00					
00203420	09	00	00	00	0A	00	00	00	0B	00	00	00	0C	00	00	00					
00203430	0D	00	00	00	0E	00	00	00	OF	00	00	00	10	00	00	00					
00203440	11	00	00	00	12	00	00	00	13	00	00	00	14	00	00	00					
00203450	15	00	00	00	16	00	00	00	17	00	00	00	18	00	00	00					
00203460	19	00	00	00	1A	00	00	00	1B	00	00	00	1C	00	00	00					
00203470	1D	00	00	00	1E	00	00	00	1F	00	00	00	20	00	00	00					
00203480	21	00	00	00	22	00	00	00	23	00	00	00	24	00	00	00	100	0"00		00\$000	
00203490	25	00	00	00	26	00	00	00	27	00	00	00	28	00	00	00	800		0'00		
002034A0	29	00	00	00	2A	00	00	00	2B	00	00	00	FF	FF	FF	OF) [[0+00		
002034B0	FF	FF	FF	0F	FF	FF	FF	0F	FF	FF	FF	0F	00	00	00	00					
002034C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00					
002034D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00					
002034E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00					
002034F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00					
00203500	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00					
00203510	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00					
00203520	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00					
00203530	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00					
00203540	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00					
00203550	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00					
00203560	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00					
00203570	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00					
00203580	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00					

图 3-88 FAT1 起始扇区

步骤 5: 同样,根据保留扇区数+FAT 扇区数×2=4122+2035×2=8192,跳转到数据 区的起始 2 号簇,即 FDT 区,如图 3-89 所示。

步骤 6: 解析 FDT 区的删除图片目录项(图 3-90),获得该文件相关信息:

(1) 文件后缀名: JPG;

(2) 文件起始簇: 0x14-0x15+0x1A-0x1B: 00-00-00-05: 5 号簇;

(3) 文件大小: 0x1C-0x1F: 00-02-6B-F7: 158711 字节。

步骤 7:分析由于 VHD 分区上只存在过该图片文件,因此该文件应为简单连续存储 (查看 FAT 可以验证),既找到了文件的起始簇,又知晓了文件大小,就能找到文件结尾。

Offset	0	1	2	3	4	5	6	7	8	9	A	в	С	D	E	F	1		UTF-8
00400000	DO	C2	BC	D3	BE	ED	20	20	20	20	20	08	00	00	00	00			00000
00400010	00	00	00	00	00	00	DB	59	A6	54	00	00	00	00	00	00		100	000000
00400020	42	20	00	49	00	6E	00	66	00	6F	00	0F	00	72	72	00	B DI	nDfC	loCCrrC
00400030	6D	00	61	00	74	00	69	00	6F	00	00	00	6E	00	00	00	mDaD1	DiD	000n000
00400040	01	53	00	79	00	73	00	74	00	65	00	0F	00	72	6D	00	DSDy	sOt	leCCCrmC
00400050	20	00	56	00	6F	00	6C	00	75	00	00	00	6D	00	65	00		010	ucccmcec
00400060	53	59	53	54	45	4D	7E	31	20	20	20	16	00	42	DB	59	SYSTE	EM~1	
00400070	A6	54	A6	54	00	00	DC	59	A6	54	03	00	00	00	00	00			000000
00400080	E5	45	4E	41	20	20	20	20	4A	50	47	20	18	7C	AE	5A			JPG D D
00400090	A6	54	A6	54	00	00	EA	75	6E	4E	05	00	F7	6B	02	00			
004000A0	24	52	45	43	59	43	4C	45	42	49	4E	16	00	C1	AE	5A	\$REC:	CLER	BINCO
004000B0	A6	54	A6	54	00	00	AF	5A	A6	54	2C	00	00	00	00	00	TO		,00000
004000C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00			
004000D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00			
004000E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00			
004000F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00			
00400100	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00			
00400110	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00			
00400120	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00			
00400130	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00			
00400140	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00			
00400150	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00			
00400160	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00			
00400170	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00			
00400180	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00			

图 3-89 FDT 区

Offset	0	1	2	3	4	5	6	7	8	9	A	в	C	D	E	F	1		UTF-8	^
00400000	DO	C2	BC	D3	BE	ED	20	20	20	20	20	08	00	00	00	00			00000	
00400010	00	00	00	00	00	00	DB	59	A6	54	00	00	00	00	00	00	0000		000000	
00400020	42	20	00	49	00	6E	00	66	00	6F	00	OF	00	72	72	00	B DI	OnOfC	loCCrrC	
00400030	6D	00	61	00	74	00	69	00	6F	00	00	00	6E	00	00	00	mDaD	tDiDo	000n000	
00400040	01	53	00	79	00	73	00	74	00	65	00	0F	00	72	6D	00	DSDy	OsOto	leCCCrmC	
00400050	20	00	56	00	6F	00	6C	00	75	00	00	00	6D	00	65	00		0010u		
00400060	53	59	53	54	45	4D	7E	31	20	20	20	16	00	42	DB	59	SYST	EM~1	DDBD	
00400070	A6	54	A6	54	00	00	DC	59	A6	54	03	00	00	00	00	00			000000	
00400080	E5	45	4E	41	20	20	20	20	4A	50	47	20	18	7C	AE	5A		J	PG DID	
00400090	A6	54	A6	54	00	00	EA	75	6E	4E	05	00	F7	6B	02	00				
004000A0	24	52	45	43	59	43	4C	45	42	49	4E	16	00	C1	AE	5A	\$REC	YCLEE	BINDOD	
004000B0	A6	54	A6	54	00	00	AF	5A	A6	54	2C	00	00	00	00	00	тロ		,00000	
004000C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00				

图 3-90 删除文件的目录项

步骤 8: 跳转到 5 号簇,即为文件的起始簇,选中第一个字节,即为文件首字节,右击该 字节,在弹出的快捷菜单中选择"选块起始位置"选项,如图 3-91 所示。

Offset	0 1 2 3 4 5 6	7 8	9	A B	С	DE	F	UTF-8	^
00403000	FF D8 FF F0 00 10 4A	46 49	46	00 01	02	01 00	48	O COJFIFOCOCOH	
00403010	00 选块起始位置 Alt+1	0A 45	78	69 66	00	00 41	4D	OHODO ExifOOMM	
00403020	0(选块尾部 Alt+2	07 01	12	00 03	00	00 00	01	0*0000000000000	
00403030	00	05 00	00	00 01	00	00 00	62	d0000000000000000000000000000000000000	
00403040	01 \$ 添加节盘	01 00	00	00 6A	01	28 00	03	00000000000j0 (00	
00403050	00 编辑(E)	00 01	31	00 02	00	00 00	1B	00000000100000	
00403060	00 00 00 72 01 32 00	02 00	00	00 14	00	00 00	8D	000r02000000000	
00403070	87 69 00 04 00 00 00	01 00	00	00 A4	00	00 00	D0	0 00000000	
00403080	00 00 00 48 00 00 00	01 00	00	00 48	00	00 00	01	нооссосноссо	
00403090	41 64 6F 62 65 20 50	68 6F	74	6F 73	68	6F 70	20	Adobe Photoshop	
004030A0	43 53 20 57 69 6E 64	6F 77	73	00 32	30	30 37	3A	CS Windows 2007:	
004030B0	30 37 3A 32 39 20 31	32 3A	32	32 3A	33	34 00	00	07:29 12:22:3400	
004030C0	00 00 00 03 A0 01 00	03 00	00	00 01	FF	FF 00	00	00000 00000	
	图	3-91 逐	片文	て件首等	字节				

步骤 9:相对于当前文件首字节位置,根据文件大小 0x26BF7=158711 字节,跳转到文件的尾字节,如图 3-92、图 3-93 所示。

步骤 10: 在文件尾字节"D9"上右击,在弹出的快捷菜单中选择"选块尾部"选项,即文件首尾之间所有字节都被选中(文件所有字节)。在选中的字节上右击,在弹出的快捷菜单中选择"编辑"→"复制选块"→"至新文件"选项,如图 3-94 所示,将选中区域保存成一个文件。

- 电子数据取证实训 -

Offset	0	1	2	3	4	5	6	7	8	9	A	в	С	D	E	F	1		UTI	r-8	^
00403000	FF	D8	FF	E0	00	10	4A	46	49	46	00	01	02	01	00	48		DDJF	IFOOD	ΠUΗ	
00403010	00	48	00	00	FF	E1	1B	0A	45	78	69	66	00	00	4D	4D			ExifO	MM	
00403020	00	2A	00	++ 704		00	- 0.0	07	0.1	10		00	00		00	01					
00403030	00	01	00	*5310	财团									~	00	62				Шb	
00403040	01	1B	00			-	_							- 10	00	03			looojo		
00403050	00	00	00	新	位置(N):	26B	F7		E	Byte <u>s</u>	(+;	六进制	D	00	1B			01000		
00403060	00	00	00	相	Tto		OH	·始(B)						-	00	8D		r0200			
00403070	87	69	00			Г	○ ±	前位	F(C)						00	DO			0000		
00403080	00	00	00				Ŭ.	而应	EDM	后往前	前)				00	01		HOODC	000н00		
00403090	41	64	6F				〇结	尾田	以后往	前)					70	20	Ado	be Ph	notosho	qq	
004030A0	43	53	20	-			-								37	3A	CS	Windo	ws0200	07:	
004030B0	30	37	3A	155	+ 确示	定(Q)		取	消(A)		9	帮助	(H)		00	00	07:	29 12	2:22:34	100	
004030C0	00	00	00	~~		~+		~~	~~		~~	~-			00	00			00000		
004030D0	A0	02	00	04	00	00	00	01	00	00	02	00	AO	03	00	04			00000		
004030E0	00	00	00	01	00	00	02	00	00	00	00	00	00	00	00	06					

图 3-92 转到偏移量

Offset	0	1	2	3	4	5	6	7	8	9	A	в	C	D	E	F	1		U	TF-8	^
00429B20	E5	11	A1	B1	в5	AD	DF	65	01	20	F4	EF	78	8A	21	E1				!0	
00429B30	90	D2	0B	D5	D2	A6	78	40	8E	84	35	44	8A	C3	C4	2A		0			
00429B40	12	41	0C	3C	42	C8	48	47	43	54	92	30	55	94	C0	C1	DAD<	вП	тΠ		
00429B50	0B	07	42	24	58	E4	2C	09	41	4A	77	14	6E	B0	CC	FO	BŞ	хD	Jw□	n🗆	
00429B60	B4	92	55	66	31	19	97	6C	90	C1	11	CF	65	72	D6	91					
00429B70	4F	16	52	07	91	15	A4	49	0A	85	31	2B	83	22	29	57				")W	
00429B80	DC	8D	9C	E9	46	5A	1D	C8	CD	28	48	3A	DD	51	43	D6	• 🗆		:		
00429B90	56	30	79	CD	F2	BC	66	5A	35	F2	88	E4	BA	15	50	01	V0y□	Z	5 🗆	PП	
00429BA0	B2	D7	4A	EA	6D	AD	49	A9	3A	B8	C9	77	47	95	D1	22		m			
00429BB0	31	33	29	4B	6D	34	51	7B	C5	47	16	6B	68	F2	F2	34	3) K	m4Q{		h□	
00429BC0	23	58	06	32	1B	63	92	16	0C	F2	90	09	04	32	в1	06	X□2	□c□			
00429BD0	78	DF	74	B8	FF	00	F9	6E	AD	45	BD	45	23	63	C4	72	tD	n		#c□	
00429BE0	C3	93	16	E8	85	EB	38	62	26	37	23	5A	2F	2E	09	AD		b	&7#Z	/. 🗆	
00429BF0	49	A 0	A1	14	EB	FF	D9	00	00	00	00	00	00	00	00	00				0000	
00429000	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00					
00429C10	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00					
00429C20	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00					

图 3-93 图片文件尾字节

Offset	0	1	2	3	4	5	6	7	8	9	A	в	С	D	E	F	1		τ	JTF-	-8	^
00429AC0	0E	5D	19	D8	B9	0C	CC	2A	A4	D5	4E	94	10	6E	85	92	30[0		N	1		
00429AD0	37	21	23	5A	50	100	05/1 IN			Chil	. 7	B9	65	0C	AB	56	Z		1'	eDD		
00429AE0	14	63	A0	EE	4	384	19(0)			cui	72	A8	F1	A5	AO	A 8		K	כ			
00429AF0	62	B7	92	80	5 %	剪	切(T).			Ctrl	+X	87	DO	D1	A1	15	b□	*□		0		
00429B00	46	91	51	00	8 00	复	制选均	ŧ(C)			>		正常	(O)			Ctrl+	C I	1,0	۵	B	
00429B10	2A	3E	86	BD	10	剪	贴板素	y据(B)		_	>		作为	Unice	ode				101	SvC		
00429B20	E5	11	A1	B1	E	我	l金(R)			1)el		至新	☆ #±(1	ม		Ctrl+8+	N		1	! 🗆	
00429B30	90	D2	0B	D5	1 ^	192	RE-(IV)-				201	_	±	×1+()	•)		CUIT#T		90			
00429B40	12	41	0C	3C	4	粘	貼0 =	字节(P).					十六	进制数	值(H))	Ctrl+#+	-C	TD	0		
00429B50	0B	07	42	24	E.	=	Vitte	h(D)					编辑	諸显示	E(E)		Alt+#+	-c	Jw	InD		
00429B60	В4	92	55	66	1.1	~E	× 1007	e(D)		C 1			-					-		כ		
00429В70	4F	16	52	07	ŝ	Ŧ	四(A)			Ctri	+A		GRE	P Hex						")) W	
00429B80	DC	8D	9C	E9	4	清	除远均	ŧ(E)		E	sc		C 源	码(C)] :	:0		
00429B90	56	30	79	CD	I Re	-	加扇区	ζ(S)		Ctrl	+R		Pasc	al 源	码(P)				Z5 🗆	I	PD	
00429BA0	B2	D7	4A	EA	€ 101-	45	201801	E(M)		Ctrl	+T	77	47	95	D1	22		m				
00429BB0	31	33	29	4B	€ 010	1.12		a(141)		cui		6B	68	F2	F2	34	3) K	m4Q	(□	h□		
00429BC0	23	58	06	32	1	項	九四马	e(L)		Ctri	+L	09	04	32	B1	06	X□2			E		
00429BD0	78	DF	74	B8	FF	00	F9	6E	AD	45	BD	45	23	63	C4	72	tD	l 1	nD	#c[
00429BE0	C3	93	16	E8	85	EB	38	62	26	37	23	5A	2F	2E	09	AD		l k	0&7#2	2/.		
00429BF0	49	AO	A1	14	EB	FF	D9	00	00	00	00	00	00	00	00	00						

图 3-94 复制文件选块

步骤 11:选择保存路径为桌面,文件名为"恢复.jpg"(图 3-95),单击"保存"按钮,即在 桌面上成功恢复该图片文件,如图 3-96 所示。

3. 非连续存储文件的删除恢复

步骤1:在FAT32分区(VHD)中创建一个文本文件 test.txt,写入一些数据后保存。

118____

å



图 3-95 恢复图片的保存路径



图 3-96 桌面上恢复的图片文件

然后在该分区中存入另一文件,再次打开 test. txt 文件对其中内容进行增加(增加内容超过 1 簇),可多次重复该操作,文件会更"碎片"地存储。最后删除 test. txt 文件。

步骤 2:用 WinHex 打开该分区,找到该分区的起始扇区,即引导记录 DBR。通过解析 获知每簇扇区数、FAT 区起始扇区、FDT 区起始扇区。解析过程同上,不再赘述。

步骤 3: 找到该删除文件的目录项,如图 3-97 所示。

ffset	0	1	2	3	4	5	6	7	8	9	A	в	C	D	E	F	/ ANSI ASC	II A
400000	DO	C2	BC	D3	BE	ED	20	20	20	20	20	08	00	00	00	00	ÐÂĦÓĦÍ	
400010	00	00	00	00	00	00	F5	58	3C	55	00	00	00	00	00	00	õX <u< td=""><td></td></u<>	
400020	42	20	00	49	00	6E	00	66	00	6F	00	0F	00	72	72	00	B Infor	r
400030	6D	00	61	00	74	00	69	00	6F	00	00	00	6E	00	00	00	matio n	
400040	01	53	00	79	00	73	00	74	00	65	00	0F	00	72	6D	00	Syste r	m
400050	20	00	56	00	6F	00	6C	00	75	00	00	00	6D	00	65	00	Volu m	e
400060	53	59	53	54	45	4D	7E	31	20	20	20	16	00	96	F4	58	SYSTEM~1 -	ôX
400070	3C	55	3C	55	00	00	F5	58	3C	55	03	00	00	00	00	00	<u<u td="" őx<u<=""><td></td></u<u>	
400080	E5	в0	65	FA	5E	87	65	2C	67	87	65	OF	00	D2	63	68	å°eú^‡e,g‡e ò	ch
400090	2E	00	74	00	78	00	74	00	00	00	00	00	FF	FF	FF	FF	.txt ÿÿ	ΫŸ
4000A0	E5	C2	BD	A8	CE	C4	7E	31	54	58	54	20	00	13	DD	59	åÂ≒"ÎÄ~1TXT	ÝY
4000B0	3C	55	3C	55	00	00	E0	59	3C	55	00	00	00	00	00	00	<u<u td="" ày<u<=""><td></td></u<u>	
4000C0	24	52	45	43	59	43	4C	45	42	49	4E	16	00	27	DD	59	\$RECYCLEBIN '	ÝY
4000D0	3C	55	3C	55	00	00	EO	59	3C	55	05	00	00	00	00	00	<u<u td="" ày<u<=""><td></td></u<u>	
4000E0	E5	45	53	54	20	20	20	20	54	58	54	20	18	13	DD	59	åest txt	ÝY
4000F0	3C	55	3C	55	00	00	14	86	3C	55	07	00	4C	2C	00	00	<u<u +<u="" l,<="" td=""><td></td></u<u>	
400100	41	CE	98	4B	4E	37	8C	2E	00	бA	00	0F	00	7B	70	00	AÎ~KN7Œ.j {	p
400110	67	00	00	00	FF	FF	FF	FF	FF	FF	00	00	FF	FF	FF	FF	g YYYYYY YY	ΫŸ
400120	B7	E7	D6	AE	B9	C8	20	20	4A	50	47	20	00	24	51	5D	·çö@1È JPG \$	Q]
400130	3C	55	3C	55	00	00	2C	в5	17	4F	08	00	39	A2	01	00	<u<u ,µ="" 0="" 9¢<="" td=""><td></td></u<u>	
400140	54	44	20	20	20	20	20	20	4A	50	47	20	18	76	0D	86	TD JPG V	+
400150	3C	55	3C	55	00	00	80	5D	93	4E	26	00	2E	0E	00	00	<u<u .<="" td="" €]"n&=""><td></td></u<u>	

图 3-97 删除文件的目录项

步骤4:分析该文件目录项,获得以下信息:

(1) 文件的起始簇号高 16 位: 0x14~0x15: 00-00;

(2) 文件的起始簇号低 16 位: 0x1A~0x1B: 00-07;

(3) 文件的长度 0x1C~0x1F: 00-00-2C-4C。

可得:

文件的起始簇为:7号簇;

文件大小为:11340字节。

步骤 5: 跳转到 FAT1 位置,查看 FAT 中 7 号表项内容(对应数据区 7 号簇的状态), 7 号表项内容为 00-00-00-25(小端),如图 3-98 所示,说明文件存储的下一簇为 0x25,即 37 号簇。

Offset	0	1	2	3	4	5	6	7	8	9	A	в	C	D	E	F	1	Al	ISI A	ASCII	^
00203400	F8	FF	FF	0F	FF	0F	FF	FF	FF	0F	øÿÿ	YYYY	YYYY	ŸŸŸ							
00203410	FF	FF	FF	0F	FF	FF	FF	OF	FF	FF	FF	0F	25	00	00	00	YYY	YYY	ŸŸŸ	÷	
00203420	09	00	00	00	0A	00	00	00	0B	00	00	00	0C	00	00	00					
00203430	0D	00	00	00	0E	00	00	00	0F	00	00	00	10	00	00	00					
00203440	11	00	00	00	12	00	00	00	13	00	00	00	14	00	00	00					
00203450	15	00	00	00	16	00	00	00	17	00	00	00	18	00	00	00					
00203460	19	00	00	00	1A	00	00	00	1B	00	00	00	1C	00	00	00					
00203470	1D	00	00	00	1E	00	00	00	1F	00	00	00	20	00	00	00					
00203480	21	00	00	00	22	00	00	00	FF	FF	FF	OF	FF	FF	FF	OF	1		ууу	YYY	
00203490	FF	FF	FF	0F	27	00	00	00	FF	FF	FF	0F	FF	FF	FF	OF	ŶŶŶ		ŶŶŶ	YYY	
002034A0	FF	FF	FF	OF	00	00	00	00	00	00	00	00	00	00	00	00	ŸŸŸ				

图 3-98 FAT1 中 7 号表项内容

步骤 6:同样地在 FAT 中查看 37 号簇的状态,FAT 中 37 号表项为 00-00-00-27(39), 如图 3-99 所示,说明 37 号簇的下一簇为 39 号簇。

Offset	0	1	2	3	4	5	6	7	8	9	A	в	C	D	E	F	1	Al	ISI	ASCII	~
00203400	F8	FF	FF	0F	FF	0F	FF	FF	FF	0F	øÿÿ	YYY:	YYYY	ŸŸŸ							
00203410	FF	FF	FF	OF	FF	FF	FF	OF	FF	FF	FF	OF	25	00	00	00	999	ŸŸŸ	ŸŸŸ	8	
00203420	09	00	00	00	0A	00	00	00	0B	00	00	00	0C	00	00	00					
00203430	0D	00	00	00	0E	00	00	00	0F	00	00	00	10	00	00	00					
00203440	11	00	00	00	12	00	00	00	13	00	00	00	14	00	00	00					
00203450	15	00	00	00	16	00	00	00	17	00	00	00	18	00	00	00					
00203460	19	00	00	00	1A	00	00	00	1B	00	00	00	10	00	00	00					
00203470	1D	00	00	00	1E	00	00	00	1F	00	00	00	20	00	00	00					
00203480	21	00	00	00	22	00	00	00	FF	FF	FF	OF	FF	FF	FF	OF	1		<u> </u>	222	
00203490	FF	FF	FF	OF	27	00	00	00	FF	FF	FF	OF	FF	FF	FF	OF	222	1	ŸŸŸ	YYY	
002034A0	FF	FF	FF	OF	00	00	00	00	00	00	00	00	00	00	00	00	YYY				
002034B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00					

图 3-99 FAT1 中 37 号表项内容

步骤 7: 以此类推,可以发现 39 号表项的状态为 0F-FF-FF-FF(结束标识)。

由此可知,文件一共分为3块存储:7号簇、37号簇、39号簇,其中39号簇为文件存储的最后一簇,一般情况下未存满。

步骤 8:选中7号簇(8扇区)所有字节,保存为新文件在桌面上,命名为"1",如图 3-100 所示。同样,选中 37号簇所有字节,保存在桌面上,命名为"2"。

步骤 9: 找到 39 号簇的起始字节,右击,在弹出的快捷菜单中选择"选块起始"选项,找到 39 号簇中最后一个字节,右击,在弹出的快捷菜单中选择"选块结束"选项,如图 3-101 所示,保 存为新文件在桌面上,命名为"3"。此时,文件的 3 个分块都已导出在桌面上,如图 3-102 所示。

步骤 10:打开 cmd 命令行工具,进入 3 个文件分块所在的目录下,利用 cmd 命令行工 具"copy"命令,将文件的 3 个分块组合成 1 个文件,如图 3-103 所示。即在桌面上生成了 txt 文件,完成了碎片文件的恢复,如图 3-104 所示。



图 3-100 导出 7 号簇所有字节数据



图 3-101 导出文件第三块内容



图 3-102 恢复的文件三个分片

- 电子数据取证实训

122



图 3-103 "copy"命令组合文件碎片



图 3-104 拼接完成的 txt 文件

3.7.4 实验小结

磁盘上的文件常常要进行创建、删除、增长、缩短等操作。这样的操作越多,盘上的文件 就被存储得越零散。即同一个文件的数据并不一定完整地存放在磁盘的一个连续的区域 内,而往往会分成若干段,像一条链子一样存放,这种存储方式称为文件的链式存储。而 FAT 是实现文件链式存储的关键。

在取证过程中,恢复被删除或丢失的数据是一项重要的工作。当一个文件被删除时,文件系统中存储的文件内容等数据不会立即消失。已删除的数据在被其他的新数据覆盖之前,一直都完整地存在于原始位置。当在 FAT 文件系统中删除一个文件时,操作系统会更新目录项,将文件目录项的第一个字节设置为一个特殊字符,即十六进制的 0xE5,表示这是一个被删除的目录项。除第一个字节之外,目录项中的其他位置信息都未发生变化。换句话说,目录项中剩余的文件名、扩展名、创建日期和时间、权限、大小、文件起始簇地址等均保持不变。且文件的数据在数据区中保持不变。

基于此,我们找到文件的目录项并解析后,可根据 FAT 进一步获知文件的存储"链"如何构成,而后即可在数据区找到文件的各个分片,拼接出完整的文件内容。

3.8 NTFS 文件系统数据恢复

3.8.1 预备知识: NTFS 文件系统原理

NTFS 的英文全称为"new technology file system",中文意为 NT 文件系统,是 Windows NT 以及之后操作系统的标准文件系统,具有安全性、可恢复性、容错性、文件压缩、硬盘配额等

优势。FAT32 文件系统的出现对于 FAT16 而言,可以说是有了比较明显的改善,但 NTFS 对 FAT32 的改进,就必须得用"卓越"来形容了。

NTFS文件系统同 FAT32 文件系统一样,也是用"簇"为存储单位,一个文件总是占用 一个或多个簇。但与 FAT32 文件系统不同的是,NTFS 文件系统将所有的数据,包括文件 系统管理数据都作为文件进行管理,所以 NTFS 文件系统中所有扇区都被分配以簇号,并 从 0 开始对所有簇进行编号,文件系统的 0 号扇区为 0 号簇的起始位置。

NTFS 文件系统使用逻辑簇号(LCN)和虚拟簇号(VCN)对分区进行管理。

逻辑簇号:即对分区内的第一个簇到最后一个簇进行编号,NTFS使用逻辑簇号对簇进行定位。

虚拟簇号:即将文件所占用的簇从开头到结尾进行编号,虚拟簇号不要求在物理上是 连续的。

一个 NTFS 系统是由分区引导扇区、主文件表(MFT)和数据区组成,另外 MFT 有一部分重要备份在数据区,数据结构如图 3-105 所示。



图 3-105 NTFS 文件系统数据结构

1. 分区引导扇区

分区引导扇区包含了 NTFS 文件系统结构的关键信息。与 FAT 的引导扇区类似, NTFS 的引导扇区描述了文件系统的数据结构,如簇大小、MFT 项(MFT entry,或称 MFT 文件记录项)大小及 MFT 起始簇地址等。

分区引导扇区中的第一个扇区为 DBR,由"跳转指令""OEM 代号""BPB""引导程序" 和"结束标志"组成,这里和 FAT32 文件系统的 DBR 一样,具体如下:

① 0x00~0x02: 跳转指令。NTFS文件系统中跳转指令为"EB 52 90",意为转到 0x52 字节。

② 0x03~0x0A: OEM 代号。固定为"4E-54-46-53-20-20-20-20",表示"NTFS"。

③ 0x0B~0x53: BPB。记录了有关该文件系统的重要信息,共 73 字节,具体见表 3-12。

偏移量	字节数	含 义
0x0B	2	每扇区字数
0x0D	1	每簇扇区数
0x0E	2	保留扇区数
0x10	3	总为 0
0x13	1	不使用
0x14	2	存储介质描述符,硬盘为 F8
0x16	2	总为 0
0x18	2	逻辑每磁道扇区数
0x1A	2	逻辑磁头数
0x1C	4	系统隐含扇区数

表 3-12 BPB 参数信息

- 电子数据取证实训

124

偏移量	字节数	含 义
0x20	4	不使用
0x24	4	不使用,总为 80 00 80 00
0x28	8	扇区总数,即分区大小
0x30	8	\$ MFT 的开始簇号
0 x 38	8	\$ MFTmirr 的开始簇号
0x40	4	每个 MFT 记录的簇数
0x44	4	每索引的簇数
0x48	8	分区的逻辑序列号
0x50	4	校验和,一般都为0

④ 0x54~0x1FD: 引导程序。负责将系统文件 NTLDR 装入,对于没有安装系统的分 区是无效的。

⑤ 0x1FE~0x1FF: 结束标志。为"55 AA"。

2. MFT

MFT(master file table,主文件表)对于 NTFS 文件系统来说尤为重要,在 NTFS 文件 系统中,磁盘上的所有数据都是以文件的形式存储,其中包括元文件。每个文件都有一个或 多个文件记录,每个文件记录占用两个扇区。MFT 的前 16 个文件记录总是元文件的,并且 顺序是固定不变的,如表 3-13 所示。第一个 MFT(MFT 0 或 \$ MFT)用于描述 MFT 本身, 记录了 MFT 的大小和位置。第二个 MFT(MFT 1 或 \$ MFTMirr)是 MFT 中第一个表项 的备份。后续保存的是每一个文件和每一个目录所对应的 MFT 项。

序号	元文件	描述
0	\$ MFT	主文件表
1	\$ MFTMirr	主文件表前几项的备份
2	\$ LogFile	日志文件,记录元数据变化
3	\$ Volume	卷文件,包含卷标及版本信息等
4	\$ AttrDef	属性定义列表,定义每种属性的名字和类型
5	\$ Root	根目录文件
6	\$ Bitmap	位图文件,每一个二进制位对应一个簇的状态,1表示该簇已分配,0表示该簇未分配
7	\$ Boot	引导文件,DBR扇区是引导文件的第一个扇区
8	\$ BadClus	坏簇记录文件,防止文件系统再次分配这些簇
9	\$ Secure	文件的安全属性和访问控制(仅用于 Windows 2000 和 Windows XP)
10	\$ UpCase	大小写字符转换表文件
11	\$ Extend	扩展属性如\$Quota(磁盘配额)、\$ObjId(对象 ID 文件)和\$Reparse (重解析点文件)
12~15	:	其他属性预留

表 3-13 NTFS 文件系统元文件

由于 NTFS 文件系统是通过 MFT 来确定文件在磁盘上的位置以及文件的属性,所以 MFT 是非常重要的,MFT 的起始位置在 DBR 中有描述。

续表

3. 文件记录

偏移量

文件记录由三部分组成,一部分是文件记录头,然后是属性 列表,最后结尾为4字节的"FF",文件记录的结构如图 3-106 所示。

在同一个操作系统中,文件记录头的长度和偏移位置的数据 含义是基本不变的,属性列表会随着数据的不同而不同,不同的属 性有着不同的含义。如图 3-107 所示,偏移量 0x00~0x37 是一个 文件记录头,文件记录头各字节的具体含义如表 3-14 所示。

文件记录头 属性1 属性2 属性3 : 结束标志

125

图 3-106 文件记录结构

	QQ	FILEO	00	00	00	00	00	20	51	51	00	03	00	30	45	4C	49	46	15455000
		8	00	00	04	00	00	00	01	A0	00	01	00	38	00	01	00	01	15455010
			00	00	00	00	00	00	00	07	00	00	00	00	00	00	00	00	15455020
•			00	00	00	60	00	00	00	10	00	00	00	00	00	00	00	02	15455030
	Н		00	00	00	18	00	00	00	48	00	00	00	00	00	18	00	00	15455040

图 3-107 文件记录头 表 3-14 文件记录头各字节含义

字节数 含 义

0x00	4	固定值,总为"FILE"
0x04	2	更新序列号的偏移
0x06	2	更新序列号与更新数组大小(以字为单位)
0x08	8	日志文件序列号(每次记录修改,该序列号加1)
0x10	2	序列号
0x12	2	硬连接数,即有多少目录指向该文件
0x14	2	第一个属性的偏移地址
0x16	2	标志字节,0x00表示删除文件,0x01表示正常文件,0x02表示删除目录,0x03表示正常目录
0x18	4	文件记录实际大小
0x1C	4	文件记录分配大小
0x20	8	基本文件记录的文件索引号
0 x 28	2	下一属性 ID,当增加新的属性时,将该值分配给新属性,然后该值增加,如果 MFT 记录重新使用,则将它置为0,第一个实例总是0
0x2A	2	边界,Windows XP 中使用,本记录使用的两个扇区的最后两个字节的值
0x2C	4	Windows XP 中使用,本文件记录号
0x30	2	更新序列号
0x32	4	更新数组

在 NTFS 文件系统中所有与文件相关的数据结构均被认为是属性,包括文件的内容。 文件记录是一个与文件相对应的文件属性数据库,它记录了文件的所有属性。每个文件记 录中都有多个属性,它们相对独立,有各自的类型和名称。如图 3-108 所示,在 0x38 之后的 4 大块颜色数据是 4 条属性,描述名称、时间、索引等信息,最后以"FF FF FF FF"结束。

每个属性都由两部分组成,即属性头和属性体,如图 3-109 所示。其中,属性头的前 4字节为属性的类型。

另外,属性还有常驻与非常驻之分。当一个文件很小时,其所有属性体都可以存放在文 件记录中,该属性就称为常驻属性。如果某个文件很大,1KB(2个扇区)的文件记录无法记 - 电子数据取证实训 ·

15455000	46	49	4C	45	30	00	03	00	51	51	20	00	00	00	00	00	FI	LE0		QQ		I
15455010	01	00	01	00	38	00	01	00	A0	01	00	00	00	04	00	00		8				
15455020	00	00	00	00	00	00	00	00	07	00	00	00	00	00	00	00						1
15455030	02	00	00	00	00	00	00	00	10	00	00	00	60	00	00	00					•	
15455040	00	00	18	00	00	00	00	00	48	00	00	00	18	00	00	00				Н		
15455050	50	E8	8C	83	F9	7E	D8	01	50	E8	8C	83	F9	7E	D8	01	₽è	Œfù	~Ø	PèŒf	ù~Ø	
15455060	50	E8	8C	83	F9	7E	D8	01	50	E8	8C	83	F9	7E	D8	01	Pè	Œfù	~Ø	PèŒf	ù~Ø	
15455070	06	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00						
15455080	00	00	00	00	00	01	00	00	00	00	00	00	00	00	00	00						
15455090	00	00	00	00	00	00	00	00	30	00	00	00	68	00	00	00				0	h	
154550A0	00	00	18	00	00	00	03	00	4A	00	00	00	18	00	01	00				J		
154550B0	05	00	00	00	00	00	05	00	50	E8	8C	83	F9	7E	D8	01				PèŒf	ù~Ø	
154550C0	50	E8	8C	83	F9	7E	D8	01	50	E8	8C	83	F9	7E	D8	01	Pè	Œfù	~Ø	PèŒf	ù~Ø	
154550D0	50	E8	8C	83	F9	7E	D8	01	00	40	00	00	00	00	00	00	₽è	Œfù	~ø	0		
154550E0	00	40	00	00	00	00	00	00	06	00	00	00	00	00	00	00	0	1				
154550F0	04	03	24	00	4D	00	46	00	54	00	00	00	00	00	00	00		\$ M	F	т		l
15455100	80	00	00	00	48	00	00	00	01	00	40	00	00	00	06	00	€	Н		0		
15455110	00	00	00	00	00	00	00	00	3F	00	00	00	00	00	00	00				?		
15455120	40	00	00	00	00	00	00	00	00	00	04	00	00	00	00	00	0					
15455130	00	00	04	00	00	00	00	00	00	00	04	00	00	00	00	00						
15455140	31	40	55	54	01	00	00	00	в0	00	00	00	50	00	00	00	10	UT		•	P	
15455150	01	00	40	00	00	00	05	00	00	00	00	00	00	00	00	00		0				
15455160	01	00	00	00	00	00	00	00	40	00	00	00	00	00	00	00				0		
15455170	00	20	00	00	00	00	00	00	08	10	00	00	00	00	00	00						
15455180	80	10	00	00	00	00	00	00	31	01	54	54	01	31	01	D1				1 TT	11	Ň
15455190	AB	FE	00	00	00	00	00	00	FF	FF	FF	FF	00	00	00	00	«Ì	5		YYYY		
154551A0	00	00	04	00	00	00	00	00	31	40	55	54	01	00	00	00				1@UT		

图 3-108 文件记录

0000003000	46	49	4C	45	30	00	03	00	DC	B 3	72	C5	02	00	00	00
0000003010	01	00	01	00	38			- P	A8	01	00	00	00	04	00	00
0000003020	00	00	00	00	00	属	生头		.06	00	00	00	00	00	00	00
0000003030	AB	83	00	00	00	00	00	00	10	00	00	00	60	00	00	00
0000003040	00	00	18	00	00	00	00	00	48	00	00	00	18	00	00	00
0000003050	60	OC	4E	B6	D1	78	CF	01	60	OC	4E	B 6	D1	78	CF	01
0000003060	60	OC	4E	B6	D1	78	CF	01	60	OC	4E	B 6	D1	78	CF	01
0000003070	06	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000003080	00	00	00	00	00	01	00	00	00	00	00	00	00	00	00	00
0000003090	00	00	00	00	00	00	00	00 -		122 JA	14-	00	68	00	00	00
00000030A0	00	00	18	00	00	00	03	00		周任	:14	00	18	00	01	00

图 3-109 属性结构

录所有属性时,则文件系统会在 MFT 元文件之外的区域(也称数据流)存放该文件的其他 文件记录属性,这些存放在非 MFT 元文件内的记录就称为非常驻属性。出现非常驻属性 一般是由于 DATA 文件较大,即 80H 属性大。

属性头中包含了该属性的重要信息,如属性类型、属性大小、是否为常驻属性等。而常 驻属性与非常驻属性的属性头结构略有不同。常驻属性的属性头信息如表 3-15 所示。非 常驻属性的属性头信息如表 3-16 所示。

偏移量	字节数	含 义
0 x 0 0	4	属性类型
0x04	4	整个属性的长度
0x08	1	是否为常驻属性,0x00表示常驻
0x09	1	属性名的长度,0x00表示无属性名
0x0A	2	属性名的开始偏移

表 3-15 常驻属性的属性头各字节含义

126___

续表

偏移量	字节数	含义
0 x 0 C	2	标志位(压缩、加密、稀疏)
0x0E	2	属性 ID
0x10	4	属性体的长度
0x14	2	属性体的开始偏移位置
0x16	1	索引标志
0x17	1	填充
0x18		属性体开始

表 3-16 非常驻属性的属性头各字节含义

偏移量	字节数	含 义
0 x 0 0	4	属性类型
0x04	4	整个属性的长度
0x08	1	是否为常驻属性,0x01表示非常驻
0x09	1	属性名的长度,0x00表示无属性名
0x0A	2	属性名的开始偏移
0x0C	2	标志位(压缩、加密、稀疏)
0x0E	2	属性 ID
0x10	8	属性体的起始虚拟簇号 VCN
0x18	8	属性体的结束虚拟簇号 VCN
0x20	2	Data Run 的偏移地址
0x22	2	压缩单位大小,2的N次方
0x24	4	不使用
0x28	8	属性体的分配大小
0x30	8	属性体的实际大小
0x38	8	属性体的初始大小
0x40		Data Run 信息开始

属性的种类很多,因此各属性体的含义也不同。NTFS 文件系统中常见的文件属性如 表 3-17 所示。

表 3-17 NTFS 文件系统常见属性类型

属性类型(属性偏移 0x00~0x03 数据,小端)	属 性 名 称	属 性 含 义
10H	\$ STANDARD_INFORMATION	标准属性,包含文件的基本属性(如只读、系统、存档),时间属性,硬连接数等
20H	\$ ATTRIBUTE_LIST	属性列表,当一个文件需要多个文件记录时, 描述文件的属性列表
30H	\$ FILE_NAME	文件名属性(UNICODE 编码)
40 H	\$ OBJECT_ID	对象 ID 属性,64 字节的标志符,其中最低 16 位对卷来说是唯一的
50H	\$ SECURITY_DESCRIPTOR	安全描述符属性,文件访问控制安全属性
60 H	\$ VOLUME_NAME	卷名属性
70H	\$ VOLUME_INFOMATION	卷信息属性

属性类型(属性偏移 0x00~0x03 数据,小端)	属 性 名 称	属 性 含 义
80 H	\$ DATA	文件的数据属性
90 H	\$ INDEX_ROOT	索引根属性
A0H	\$ INDEX_ALLOCATION	索引分配,90H 属性的拓展版(90H 属性只能在 MFT 内记录文件列表,A0H 属性将文件列表记录到数据区可以记录更多文件)
B0H	\$ BITMAP	位图属性
C0H	\$ REPARSE_POINT	重解析点属性
D0H	\$ EA_INFORMATION	拓展属性信息
E0H	\$ EA	拓展属性
100H	\$ LOGGED_UTILITY_STREAM	EFS加密属性

上表中的两个属性\$STANDARD_INFORMATION 和\$FILE_NAME 包含了文件 系统的所有4个时间戳信息(创建时间、修改时间、更改时间、访问时间)。操作系统在更新 时间戳信息时应该同时更新两个属性,但实际研究表明,不同操作系统的具体表现有所不 同,有些只更新\$STANDARD_INFORMATION,有些只更新\$FILE_NAME,所以在分 析 NTFS 文件系统的时间属性时需要格外注意。

NTFS文件系统里每个文件至少要占用一个 MFT 项, 而 MFT 项的大小只有 1024 字 节, 如果一个文件有太多属性, 那么这些属性就需要占用其他 MFT 项。在 NTFS 文件系统 里, 增加的 MFT 项使用 \$ ATTRIBUTE_LIST 属性进行记录。每种属性的结构不尽相同。 取证中关注的几个重要属性如下:

① 10H 属性被称为标准信息属性,英文标识为 \$ STANDARD_INFORMATION。 10H 属性是所有文件记录所必备的属性,它包含了许多文件或文件夹的基本信息,如:文件 或文件夹的创建时间、文件或文件夹的修改时间、目录硬连接数等。

② 30H 属性被称为文件名属性,英文标识为\$FILE_NAME。30H 属性常紧跟于10H 属性之后,用于描述文件名以及文件或文件夹更详细的信息,如:文件名长度、文件大小、文件名命名空间、文件名 Unicode 码等。

③ 80H 属性被称为数据属性,英文标识为 \$ DATA。该属性容纳着文件的数据内容。 80H 属性是整个文件属性中最重要的部分,可大概分为 3 种类型:一是只有属性头无属性体,这种情况主要存在于小型文本文件中,文件大小为 0 字节,即文件内容为空,因此数据属性为空,无需属性体记录数据。二是常驻属性,这种情况存在于文件内容简短的情况下,为 了节省空间,不额外分配簇进行存储,直接在 80H 属性体内存储文件数据,最后以"FF FF FF FF"为结束标志。三是非常驻属性,这是 80H 属性中最复杂最重要的类型。在此种情况中,文件内容大于 80H 属性体最大长度,因此采用数据运行列表(data run list)的方式存储数据信息,80H 属性体中记录数据运行列表。

④ 90H 属性被称为索引根属性,英文标识为\$INDEX_ROOT。90H 属性主要存在于 \$MFT 的文件夹记录中,一般为常驻属性。该属性是实现 NTFS 文件系统的 B+树索引的 根节点。

⑤ A0H 属性被称为索引根拓展属性,英文标识为 \$ INDEX_ALLOCATION。该属性

续表

包含一个 B 树的子节点,是一个非常驻属性。对于小型目录,此属性不存在,所有信息将保存在 \$ INDEX_ROOT 结构中。这个属性的内容是一个或多个索引记录(index rocord),每个索引节点(这里是 B 树节点)有一个记录。每个索引记录包含一个或多个索引条目(index entry)结构,这些结构与 \$ INDEX_ROOT 相同。

通过以上几个文件重要属性的解析,就能获知在取证中较为关注的文件信息,如文件 名、文件的时间、文件的位置、文件的数据内容等。

3.8.2 实验目的与条件

1. 实验目的

通过本实验,读者重点掌握以下内容:

- (1) 了解 NTFS 文件系统存储原理;
- (2) 掌握 NTFS 文件系统各数据结构的解析;

(3) 掌握使用 WinHex 进行 NTFS 文件系统数据恢复的过程。

2. 实验条件

本实验所需要的软硬件清单如表 3-18 所示。

表 3-18 NTFS 文件系统数据恢复实验清单

序号	设 备	数量	参数
1	取证工作站	1台	Windows XP 以上
2	WinHex 工具	1 套	无

3.8.3 实验过程

1. 常驻文件的删除恢复

步骤 1: 创建虚拟磁盘 VHD,并在该磁盘上建立 NTFS 分区。具体步骤见 3.7.3节。 步骤 2: 在新建的 VHD(E盘)中创建一个 txt 文件,写入较少的内容并保存,如图 3-110 所示。

⇒ * ↑		电脑 → 新加卷 (E:)	õ		族	
▲ 供 2	test.txt	🗐 *testtxt - 记事本			- 0	×
L 1		文件(E) 编辑(E) 格式(Q) 查看(V) 帮助(H)				
デ 王 王 二 2 二 2 二 5 二 4		Hello World!				
Or Or						
■此						~
		第1行,第13列	100	0% Windows (CRLF)	UTF-8	34

图 3-110 虚拟磁盘中新建小文件

步骤 3. 按下"Shift+Delete",将"test.txt"文件删除。 步骤 4. 用 WinHex 工具打开 E 盘,可以看到该磁盘中的各文件情况,如图 3-111 所示。 🎬 WinHex - [驱动器 E:] → 文件(E) 编辑(E) 搜索(S) 导航(N) 查看(V) 工具(T) 专业工具(I) 选项(O) 窗口(W) 帮助(H) 日月日建筑后日一个时间后期第一般的表情发(→用←→「乙基金回入中国第一 安任教坛 编辑(D) 驱动器 E: 文件(山) 扩展名 大小 创建时间 记录更新时间 文件属件 第1扇区 文件名称▲ 修改时间 0.6 KB 2022/07/04 10:... 2022/07/04 10:... 2022/07/04 10:... 697,022 SExtend SH SRECYCLE.BIN BIN 224 B 2022/07/04 10:... 2022/07/04 10:... 2022/07/04 10:... 697,080 SH (相目录) 4.1 KB 2022/07/04 10-2022/07/04 10- 2022/07/04 10-SH 288 160 B 2022/07/04 10:... 2022/07/04 10:... 2022/07/04 10:... 697,072 System Volume Information SH 2.5 KB 2022/07/04 10:... 2022/07/04 10:... 2022/07/04 \$AttrDef 10:... SH 280 SBadClus 0 B 2022/07/04 10 2022/07/04 10 2022/07/04 10 ... SH 697,016 \$Bitmap 31.9 KB 2022/07/04 10:... 2022/07/04 10:... 2022/07/04 10:... SH 696,928 SBoot 8.0 KB 2022/07/04 10:... 2022/07/04 10:... 2022/07/04 10:... SH 0 4.8 MB 2022/07/04 10:... 2022/07/04 10:... 2022/07/04 10:... \$LogFile SH 687,136 \$MFT 256 KB 2022/07/04 10:... 2022/07/04 10:... 2022/07/04 10:... SH 697,000 4.0 KB 2022/07/04 10:... 2022/07/04 10:... 2022/07/04 10:... SH 16 Secure 0 B 2022/07/04 10:... 2022/07/04 10:... 2022/07/04 10:... SH \$UpCase 128 KB 2022/07/04 10:... 2022/07/04 10:... 2022/07/04 10:... SH 24 697 006 \$Volume 0 B 2022/07/04 10:... 2022/07/04 10:... 2022/07/04 10:... SH 12 B 2022/07/04 10:... 2022/07/04 10:... 2022/07/04 10:... test.txt txt IA 697.078 8 9 A B C D E F 20 20 20 00 02 08 00 00 Offset 5 ANSI ASCII 0 1 2 3 4 6 7 00000000 EB 52 90 4E 54 46 53 20 ER NTES 00000010 00 00 00 00 00 F8 00 00 3F 00 FF 00 80 00 00 00 æ 2 9 € 00000020 00 00 00 00 80 00 80 00 FF E7 1F 00 00 00 00 00 € € ÿç 00000030 55 54 01 00 00 00 00 00 02 00 00 00 00 00 00 00 UT 00000040 F6 00 00 00 01 00 00 00 63 57 41 F4 78 41 F4 1A cWAôxAô ð 00000050 00 00 00 00 FA 33 CO 8E D0 BC 00 7C FB 68 C0 07 ú3ÀŽĐ4 |ûhÀ 00000060 1F 1E 68 66 00 CB 88 16 OE 00 66 81 3E 03 00 4E hf Ë* f > N

图 3-111 WinHex 中磁盘情况

步骤 5: 要找到删除文件的内容,按照 NTFS 文件系统原理,必须先找到其文件记录。 在该文件的文件记录中,会记录文件的名称、时间、数据等属性。现已知文件名为"test.txt",由 于 WinHex 以十六进制为核心,因此先将文件名转为十六进制 ASCII 编码(可用网页在线 工具转换),如图 3-112 所示,为"0074006500730074002E007400780074"。

在线ASCII编码解码			3. 全屏 上代码
URL网址 UTF-8 Unicode	ASCII		
文字:		A	SCII:
test.txt		编码 > く 解码	\u0074\u0065\u0073\u0074\u002e\u0074\u0078\ u0074
		□ 不转换字母和 数字	

图 3-112 文件名 ASCII 编码

步骤 6:在\$MFT中,向下搜索十六进制数据"0074006500730074002E007400780074",如 图 3-113 所示,单击"确定"按钮,即跳转到\$MFT中文件"test.txt"所属文件记录,如图 3-114 所示。

步骤 7:按照 3.8.1 节理论知识,分析该文件记录,找到 80H 属性,即为文件的数据属性。在 80H 的属性头中 0x08 位置即为是否为常驻属性的标志位,可以看出该文件的 80H 属性为常驻属性,意味着该文件的数据内容直接记录在了 80H 属性体中。

步骤 8: 在该 80H 属性的属性头中,0x10~0x13 位置为属性体的大小(00 00 00 0C),

0 7 8 4 4 6 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	A 500 m	A #2 26 m →	生	📫 🔬 🖓 👔	1 P. B
区动器 E:		2			
2件名称▲	扩展名	文件大小 创建时间	修改时间	记录更新时间	文件属性
]]\$Extend		0.6 KB 超出边界 1	超出边界 †	超出边界 †	SH
\$RECYCLE.BIN	BIN	224 B 超出边界 1	超出边界 †	超出边界↑	SH
](根目录)		4.1 KB 超出边界 1	超出边界↑	超出边界 †	SH
System Volume Information		280 B 超出边界 🗃	322十六讲创教值	→ 边界↑	SH
\$AttrDef		2.5 KB 超出边界	13G T / VIII WISKIEL	^ 边界↑	SH
\$BadClus		0 B 超出边界		边界 1	SH
\$Bitmap		31.9 KB 超出边界	搜索下列十六进制数值(3) 3	边界 †	SH
\$Boot		8.0 KB 超出边界	0074006500730074002E007400780 -	边界 †	SH
\$LogFile 1		4.8 MB 超出边界	L	边界↑	SH
\$MFT		256 KB 超出边界	☑用作通配符(U): 3F	边界↑	SH
\$MFTMirr		4.0 KB 超出边界	#を(の) 「向下」 >	边界 1	SH
\$Secure		0 B 超出边界		边界 1	SH
\$UpCase		128 KB 超出边界	□条件 同下 512 = 0	边界 ↑	SH
\$Volume		0 B 超出边界		边界 †	SH
]空余空间 (net)		1.0 GB 超出边界	在所有打开窗口中搜索(四)	边界 1	
空闲空间		? 超出边界	◎ 列出搜索结果,最多 10000	边界 †	

图 3-113 在 \$MFT 中搜索十六进制数据

Offset	0	1	2	3	4	5	6	7	8	9	A	В	С	D	E	F	V	AN	ISI AS	CII	^
1545EC00	46	49	4C	45	30	00	03	00	10	7E	20	00	00	00	00	00	FILEO		~		
1545EC10	02	00	01	00	38	00	00	00	60	01	00	00	00	04	00	00	8				
1545EC20	00	00	00	00	00	00	00	00	05	00	00	00	27	00	00	00					
1545EC30	04	00	00	00	00	00	00	00	10	00	00	00	60	00	00	00					
1545EC40	00	00	00	00	00	00	00	00	48	00	00	00	18	00	00	00			H		
1545EC50	16	33	A 8	4A	51	8F	D8	01	7D	9C	22	58	51	8F	D8	01	3"JQ	ø	}œ"XQ	ø	
1545EC60	7D	9C	22	58	51	8F	D8	01	7D	9C	22	58	51	8F	D8	01	}œ"XQ	ø	}œ"XQ	ø	
1545EC70	20	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00					
1545EC80	00	00	00	00	08	01	00	00	00	00	00	00	00	00	00	00					
1545EC90	E8	08	00	00	00	00	00	00	30	00	00	00	70	00	00	00	è		0 p		
1545ECA0	00	00	00	00	00	00	03	00	52	00	00	00	18	00	01	00			R		
1545ECB0	05	00	00	00	00	00	05	00	16	33	A 8	4A	51	8F	D8	01			3"JQ	ø	
1545ECC0	16	33	A 8	4A	51	8F	D8	01	16	33	A 8	4A	51	8F	D8	01	3″JQ	ø	3JÖ	ø	
1545ECD0	16	33	A 8	4A	51	8F	D8	01	00	00	00	00	00	00	00	00	3"JQ	ø			
1545ECE0	00	00	00	00	00	00	00	00	20	00	00	00	00	00	00	00					
1545ECF0	08	00	74	00	65	00	73	00	74	00	2E	00	74	00	78	00	te	3	t.t	x	
1545ED00	74	00	00	00	00	00	00	00	40	00	00	00	28	00	00	00	t		0 (
1545ED10	00	00	00	00	00	00	04	00	10	00	00	00	18	00	00	00					
1545ED20	83	C0	09	24	42	FB	EC	11	97	5A	C8	94	02	E2	28	D8	fÀ \$B	ûì	−ZÈ″	â (Ø	
1545ED30	80	00	00	00	28	00	00	00	00	00	18	00	00	00	01	00	€ (
1545ED40	0C	00	00	00	18	00	00	00	48	65	6C	6C	6F	20	77	6F			Hello	WO	
1545ED50	72	6C	64	21	00	00	00	00	FF	FF	FF	FF	82	79	47	11	rld!		ŶŶŶŶ,	уG	

图 3-114 test. txt 的文件记录

0x18 位置即为常驻属性属性体的开始,即属性体中内容为"48 65 6C 6C 6F 20 77 6F 72 6C 64 21", 如图 3-115 所示。

步骤 9:按照 ASCII 编码规则转换十六进制数据"48 65 6C 6C 6F 20 77 6F 72 6C 64 21"为 "Hello World!",即为删除文件"test.txt"的内容。

至此完成了常驻文件的删除恢复!

2. 非常驻文件的删除恢复

步骤 1: 在新建的 VHD(NTFS 文件系统)中存入图片文件"lena.jpg"。

步骤 2: 按下"Shift+Delete",将"lena.jpg"文件删除,如图 3-116 所示。

步骤 3:用 WinHex 工具打开 E 盘,查看磁盘基本信息。

电子数据取证实训

Offset	0	1	2	3	4	5	6	7	8	9	A	в	С	D	E	F	٧		Ţ	JTF-8	^
1545EC00	46	49	4C	45	30	00	03	00	10	7E	20	00	00	00	00	00	FIL	EODDD	0~ 0	0000	
1545EC10	02	00	01	00	38	00	00	00	60	01	00	00	00	04	00	00		8000	1000	0000	
1545EC20	00	00	00	00	00	00	00	00	05	00	00	00	27	00	00	00				1000	
1545EC30	04	00	00	00	00	00	00	00	10	00	00	00	60	00	00	00				1,000	
1545EC40	00	00	00	00	00	00	00	00	48	00	00	00	18	00	00	00			HOOD	0000	
1545EC50	16	33	A 8	4A	51	8F	D8	01	7D	9C	22	58	51	8F	D8	01			">	CD .	
1545EC60	7D	9C	22	58	51	8F	D8	01	7D	9C	22	58	51	8F	D8	01					
1545EC70	20	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00					
1545EC80	00	00	00	00	08	01	00	00	00	00	00	00	00	00	00	00					
1545EC90	E8	08	00	00	00	00	00	00	30	00	00	00	70	00	00	00		0000	0000	1p000	
1545ECA0	00	00	00	00	00	00	03	00	52	00	00	00	18	00	01	00			RDDD	0000	
1545ECB0	05	00	00	00	00	00	05	00	16	33	A 8	4A	51	8F	D8	01			□3□		
1545ECC0	16	33	A 8	4A	51	8F	D8	01	16	33	A 8	4A	51	8F	D8	01					
1545ECD0	16	33	A 8	4A	51	8F	D8	01	00	00	00	00	00	00	00	00				0000	
1545ECE0	00	00	00	00	00	00	00	00	20	00	00	00	00	00	00	00				0000	
1545ECF0	08	00	74	00	65	00	73	00	74	00	2E	00	74	00	78	00		leOsO	tD.D	ltoxO	
1545ED00	74	00	00	00	00	00	00	00	40	00	00	00	28	00	00	00	tDD		0000	(000	
1545ED10	00	00	00	00	00	00	04	00	10	00	00	00	18	00	00	00					
1545ED20	83	C0	09	24	42	FB	EC	11	97	5A	C8	94	02	E2	28	D8		BD	ZŪ		
1545ED30	80	00	00	00	28	00	00	00	00	00	18	00	00	00	01	00		0 (000		0000	
1545ED40	0C	00	00	00	18	00	00	00	48	65	6C	6C	6F	20	77	6F			Hell	o wo	
1545ED50	72	6C	64	21	00	00	00	00	FF	FF	FF	FF	82	79	47	11	rld	10000			

图 3-115 80H 属性解析

← → •	↑ ~ >	此电脑 > 新加	卷 (E:)	~	U	▶ 在新加卷	(E:) 中搜
lange de la construcción de la c	ve - I ^	名称		^			
🍋 WPS网络	盘	🔳 lena.jpg					
●此电脑	删除文件					×	
 3D 对 视频 图片 文档 ▼ 下载 	×	确实要永久性的	地删除此文件吗? lena.jpg 项目类型: JPG 文件 拍摄日班: 2007/7/29 12:22 分辨率: 512 x 512 大小: 154 KB				
♪ 音乐 ■ 桌面				是(Y)		否(N)	:
个项目	近中「千切	H 154 KD					

图 3-116 删除图片文件"lena.jpg"

步骤 4:使用编码转换工具将所要恢复文件的文件名"lena.jpg"转换为十六进制 ASCII 编码为"006c0065006e0061002e006a00700067"。

步骤 5:单击 \$ MFT,跳转到 \$ MFT 起始扇区,单击工具栏中的"查找十六进制数值" 按钮,在弹出的对话框中,向下搜索十六进制数据"006c0065006e0061002e006a00700067", 具体如图 3-117 所示。

步骤 6: 单击"确定"按钮,成功跳转到 \$ MFT 中"lena. jpg"的文件记录,如图 3-118 所示。

步骤 7:解析该文件记录,找到 80H 属性(数据属性),其中 0x08 位置为"01",即该条属 性为非常驻属性。也即是说,文件的数据属性较大,在文件记录中存储不下,因此,文件的数 据内容存放于簇流之中。此时,80H 属性的属性体中存放的是指向文件簇流的索引(Data Runs)。

步骤 8: 非常驻属性的属性体开始位置为 0x40, 即 80H 属性的属性体中十六进制数据

132___

驱动器 C.															
۱									9分	钟以	前				
文件名称▲							扩	展名	大小 创建时间 修改时间			记录更新时间		文件属性	第1扇区
■\$Extend									0.5 KB 2022/07/04 14: 2022/07/	/04	14:	2022/07/04	14:	SH	697,022
■\$RECYCLE.B	IN						BI	N	224 B 2022/07/04 14: 2022/07/	/04	14:	2022/07/04	14:	SH	697,07
(根目录)									4.1 KB 2022/07/04 14: 2022/07/	/04	14:	2022/07/04	14:	SH	28
■System Volu	ime Ir	forn	natio	n					160 B 2022/07/04 14: 2022/07/	/04	14:	2022/07/04	14:	SH	697,072
■\$AttrDef									2.5 KB 2022/07/04 14: 2022/07/	/04	14:	2022/07/04	14:	SH	28
■\$BadClus									0 R 2022/07/04 14- 2022/07/	104	14:	2022/07/04	14:	SH	697,016
■\$Bitmap									查找十六进制数值 ×	<	14:	2022/07/04	14:	SH	696,928
⊒\$Boot			1								14:	2022/07/04	14:	SH	(
1\$LoaFile							_		搜索下列十六进制数值(s) 2		14:	2022/07/04	14:	SH	687,136
1\$MFT			_						17/# 17/17/1/2000 (EQ)	1 1	14:	2022/07/04	14:	SH	697,000
□\$MFTMirr									006c0065006e0061002e006a00700C ~		14:	2022/07/04	14:	SH	10
⊒\$Secure											14:	2022/07/04	14:	SH	
1\$UpCase									□用作通配符(<u>U</u>): 3F		14:	2022/07/04	14:	SH	24
■\$Volume									相告(4) (内下) 2		14:	2022/07/04	14:	SH	697,006
Iena.jpg							jp	g	按案团 同下 3		14:	2022/03/29	09:	A	11,328
Offset	0	1	2 :	3 4	5	6	7	8	条件:偏移计算 512 = 0	S	CII	^			
15455000	46 4	19 4	C 4	5 30	00	03	00	51	日在港地市搜索	LE					
15455010	01 (0 0	1 00	38	00	01	00	A0	一方在客様日本日本総本()						
15455020	00 (0 0	0 00	00 0	00	00	00	07	在所有打开图口甲摸索(型)	L L					
15455030	02 (0 0	0 00	00 00	00	00	00	10	3列出搜索结果,最多 10000	1					
15455040	00 0	00 1	8 00	00 00	00	00	00	48	Δ						
15455050	D0 0	:8 1	D 7	L 6E	8F	D8	01	DO		k	ø				
		10 1	Ph		0.85	DO	0.1	DO		10	0				

图 3-117 在 \$MFT 中搜索十六进制数据

Offset	0	1	2	3	4	5	6	7	8	9	A	в	С	D	E	F	V	A	NSI	AS	CII	^
1545E800	46	49	4C	45	30	00	03	00	FB	74	20	00	00	00	00	00	FILE)	ût			
1545E810	02	00	01	00	38	00	00	00	58	01	00	00	00	04	00	00	8	3	х			
1545E820	00	00	00	00	00	00	00	00	03	00	00	00	26	00	00	00				&		
1545E830	04	00	00	00	00	00	00	00	10	00	00	00	60	00	00	00				•		
1545E840	00	00	00	00	00	00	00	00	48	00	00	00	18	00	00	00			Н			
1545E850	A7	3A	BA	80	6B	8F	D8	01	00	4C	5C	C5	31	DA	D4	01	§:°€}	ø	L	\Å1	ÓÔ	
1545E860	57	40	64	DA	0B	43	D8	01	9F	61	BA	80	6B	8F	D8	01	W@dÚ	сø	Ÿa	°€k	ø	
1545E870	20	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00						
1545E880	00	00	00	00	08	01	00	00	00	00	00	00	00	00	00	00						
1545E890	00	00	00	00	00	00	00	00	30	00	00	00	70	00	00	00			0	р		
1545E8A0	00	00	00	00	00	00	02	00	52	00	00	00	18	00	01	00			R			
1545E8B0	05	00	00	00	00	00	05	00	A7	3A	BA	80	6B	8F	D8	01			s:	°€k	ø	
1545E8C0	Α7	3A	BA	80	6B	8F	D8	01	A7	3A	BA	80	6B	8F	D8	01	§:°€]	ø	s:	°€k	ø	
1545E8D0	A7	3A	BA	80	6B	8F	D8	01	00	70	02	00	00	00	00	00	§:°€}	ø	р			
1545E8E0	00	00	00	00	00	00	00	00	20	00	00	00	00	00	00	00						
1545E8F0	08	00	бC	00	65	00	6E	00	61	00	2E	00	6A	00	70	00	1 6	n	a	. j	р	
1545E900	67	00	00	00	00	00	00	00	80	00	00	00	48	00	00	00	g		€	Н		
1545E910	01	00	00	00	00	00	01	00	00	00	00	00	00	00	00	00						
1545E920	26	00	00	00	00	00	00	00	40	00	00	00	00	00	00	00	&		0			
1545E930	00	70	02	00	00	00	00	00	F7	6B	02	00	00	00	00	00	р		÷k			
1545E940	F7	6B	02	00	00	00	00	00	21	27	88	05	00	00	00	00	÷k		! '	^		
1545E950	FF	FF	FF	FF	82	79	47	11	00	00	00	00	00	00	00	00	ŸŸŸŸ,	УG				

图 3-118 "lena.jpg"文件记录

为"21 27 88 05 00",按照 Data Runs 的解析规则,该删除文件的数据内容位于从 0x588 开始的 0x27 个簇中。

步骤 9: 单击工具栏中的"跳至扇区"按钮,输入簇号"1416(0x588)",单击"确定"按钮, 如图 3-119 所示。即跳转至删除文件内容起始簇。

步骤 10:在 1416 号簇的首字节处右击,在弹出的快捷菜单中选择"选块起始位置"选项,如图 3-120 所示。

步骤 11:由于该删除文件的数据内容位于从 0x588(1416)开始的 0x27(39)个簇中。因此,文件的最后一簇为 1416+39-1=1454 号簇。同上,跳转到 1454 号簇,如图 3-121 所示。

133

- 电子数据取证实训 -

											_								
30-9768 C.														36.754	LINE AND				
立州夕約。		_	_	_	_	_	_	dr"	104		+4) 61	at a dist		AR2hratia	164399	23-3-6-96-16		文字和十個級統计	位100
XIII Cutond								N.	/PR T	1	VJ 6	N22/07/	4.14	2022/07/0	4 14	2022/07/04	14	CH	607.02
= \$Extend								D		0.	D ND ZU	22/01/0	14	2022/07/0	4 14	2022/07/04	14	SH	697,022
SKECYCLE.	SIN.							B	N	跳至扇区	7				× 1	2022/07/04	14	SH	697,078
三(根目录)										Walks Well	A				4:	2022/07/04	14:	SH	288
■System Vol	ume	Info	rma	tion						_					4:	2022/07/04	14:	SH	697,072
■\$AttrDef										0		-		3	4:	2022/07/04	14:	SH	280
SBadClus										•	27年(L):	扇区:	113	28 2	4:	2022/07/04	14:	SH	697,016
SBitmap												= <u>8</u> .	1416	3	4:	2022/07/04	14:	SH	696,928
SBoot															4:	2022/07/04	14:	SH	(
\$LogFile										1					4:	2022/07/04	14:	SH	687.136
DSMET										1					4:	2022/07/04	14:	SH	697.000
■\$MFTMirr										1					4:	2022/07/04	14:	SH	16
Offset	0	1	2	3	4	5	6	7	8		2				II	^			
1545E800	46	49	4C	45	30	00	03	00	FB		-3								
1545E810	02	00	01	00	38	00	00	00	58		The share of		-						
1545E820	00	00	00	00	00	00	00	00	03	-0	備定(℃)	0	取消(A)					
1545E830	04	00	00	00	0.0	00	00	00	10			_							

图 3-119 跳转至删除文件内容起始簇

Offset	0 1 2 3 4 5	678	9 A B C D E F	V ANSI ASCII 🔨
00588000	FF D8 FF E0 00 10	4A 46 49	46 00 01 02 01 00 48	🖗 Øÿà JFIF H
00588010	0 选块起始位置	Alt+1 15	78 69 66 00 00 4D 4D	H ÿá Exif MM
00588020	0 法协民部	Alt+2 1	12 00 03 00 00 00 01	*
00588030		AIL+2 00	00 00 01 00 00 00 62	b
00588040	0	0	00 00 6A 01 28 00 03	j (
00588050	0)1	31 00 02 00 00 00 1B	1
00588060	0 3闸4目(E)	0	00 00 14 00 00 00 8D	r 2
00588070	87 69 00 04 00 00	00 01 00	00 00 A4 00 00 D0	ti ¤ Đ
00588080	00 00 00 48 00 00	00 01 00	00 00 48 00 00 00 01	н н
00588090	41 64 6F 62 65 20	50 68 6F	74 6F 73 68 6F 70 20	Adobe Photoshop
005880A0	43 53 20 57 69 6E	64 6F 77	73 00 32 30 30 37 3A	CS Windows 2007:
005880B0	30 37 3A 32 39 20	31 32 3A	32 32 3A 33 34 00 00	07:29 12:22:34
005880C0	00 00 00 03 A0 01	00 03 00	00 00 01 FF FF 00 00	ŸŸ
005880D0	A0 02 00 04 00 00	00 01 00	00 02 00 A0 03 00 04	
005880E0	00 00 00 01 00 00	02 00 00	00 00 00 00 00 00 06	
005880F0	01 03 00 03 00 00	00 01 00	06 00 00 01 1A 00 05	
00588100	00 00 00 01 00 00	01 1E 01	1B 00 05 00 00 00 01	
00588110	00 00 01 26 01 28	00 03 00	00 00 01 00 02 00 00	& (
00588120	02 01 00 04 00 00	00 01 00	00 01 2E 02 02 00 04	2.00
00588130	00 00 00 01 00 00	19 D4 00	00 00 00 00 00 00 48	Ô H
00588140	00 00 00 01 00 00	00 48 00	00 00 01 FF D8 FF E0	H ÿØÿà
00588150	00 10 4A 46 49 46	00 01 02	01 00 48 00 48 00 00	JFIF H H
00588160	FF ED 00 0C 41 64	6F 62 65	5F 43 4D 00 03 FF EE	ÿí Adobe_CM ÿî
00588170	00 OE 41 64 6F 62	65 00 64	80 00 00 00 01 FF DB	Adobe d€ ÿÛ
00588180	00 84 00 0C 08 08	08 09 08	OC 09 09 OC 11 OB 0A	<i>"</i> ~

图 3-120 删除文件存储的起始簇

Offset	0	1	2	3	4	5	6	7	8	9	Α	В	C	D	E	F	V ANSI ASCII	^
005AE000	A3	06	00	11	A7	A 8	24	73	29	6C	BF	66	C6	C0	46	9D	£ §"\$s)l;f#ÀF	
005AE010	64	42	F1	49	9C	23	OF	2A	43	24	E5	89	89	03	3D	7C	dBñIœ# *C\$å‱ =	-
005AE020	69	A1	27	BF	5F	B2	7F	50	73	91	EF	FO	5E	EB	C0	60	i;';_ Ps'ið^ëà`	
005AE030	73	7C	5C	12	B2	32	2F	33	C8	FA	DF	19	93	CB	62	81	s \ ² 2/3Èúß "Ëb	
005AE040	27	9A	B6	77	15	21	92	35	A0	AB	44	28	05	6A	1F	8B	'š¶w !'5 «D(j <	
005AE050	E7	B2	48	C2	E3	F9	1C	9E	37	93	BB	1D	F3	22	9F	85	ç² HÂãù ž7"» ó"Ÿ	
005AE060	99	9C	E1	BF	E2	A 8	88	64	31	8C	A3	44	D7	26	D4	8A	™œá;â¨^dlŒ£D×&ÔŠ	
005AE070	09	3E	24	75	EA	BE	E9	EB	F2	EC	73	19	7E	89	C6	4E	>\$uê¾éëòìs ~‰ÆN	
005AE080	B2	E1	BB	5F	CB	AF	04	B1	F1	9C	В3	D6	28	D2	FC	B6	²á≫_Ë ±ñœ³Ö(Òü¶	
005AE090	C5	18	F9	20	5E	4B	45	33	0A	0A	30	13	7A	37	B1	72	Å ù ^KE3 0 z7±r	
005AE0A0	4D	C1	F2	1E	C1	3C	F2	71	3E	CB	3E	43	2C	7C	67	EC	MÁÒ Á<òq>Ë>C, gì	
005AE0B0	9E	13	1E	3C	8E	0B	92	CA	43	22	AE	1B	F3	58	BF	F4	č <Ž 'ŜC'® óS; č>	
005AE0C0	6D	3A	83	71	11	07	34	2C	7A	E7	7D	13	DC	F8	66	6C	m:fq 4,zç} Üøfl	
005AE0D0	CF	5D	E5	32	31	F9	1B	95	DA	20	39	69	A1	C1	E4	23	Ï]å21ù •Ú 9i;Áä#	
005AE0E0	7C	2C	85	2B	2E	36	7E	69	C7	73	80	8E	D9	1C	B 3	68	,+.6~iÇs ŽÙ ³h	
005AE0F0	1B	51	E9	FC	06	26	0E	6F	A4	F2	3E	78	09	C3	BB	4B	Qéü & o≖ò>x Ã≫K	
005AE100	8B	C1	CF	CE	C4	В9	D8	83	27	8F	75	C8	97	86	65	CE	<ÁÏÎÄ'Øf' uÈ-teî	
005AE110	11	38	F2	D8	F2	6B	4A	DE	57	AC	98	24	95	54	CD	00	8òØòkJÞW¬~\$•TÍ	
005AE120	86	53	91	1E	F1	17	E5	C6	AF	26	37	F1	BB	23	44	20	†S`ñ åÆ~&7ñ≫#D	
005AE130	36	BA	DA	F4	B9	6B	46	E8	0C	7C	6F	C9	76	90	C9	13	6°Úô¹kFè oÉv É	

图 3-121 删除文件存储的最后一簇

134___

¢

步骤 12:由分区的 DBR 解析可知,该 E 分区中簇的大小为每簇 8 扇区,在该最后一簇 中向下拉,直至找到文件的最后一字节(位于该簇的第 6 个扇区中),在最后一字节上右击, 在弹出的快捷菜单中选择"选块尾部"选项,如图 3-122 所示。

Offset	0	1	2	3	4	5	6	7	8	9	A	В	С	D	E	F	v ANSI ASCII	^
005AEAE0	14	63	A 0	EE	40	3D	4B	9F	2D	8F	25	A 8	F1	Α5	A 0	A 8	с î@=КŸ- %"ñ¥ "	
005AEAF0	62	в7	92	80	97	2A	AC	A9	A 0	AE	85	87	D0	D1	A1	15	b •' €-*-© ©‡ĐÑ ;	
005AEB00	46	91	51	00	8D	19	07	DA	21	2C	A6	8C	11	CB	7F	42	F`Q Ú!,¦ŒËB	
005AEB10	2A	3E	86	BD	39	53	23	CB	B1	21	40	14	53	76	C2	69	*>†¾9S#˱!@ SvÂi	
005AEB20	E5	11	A1	в1	в5	AD	DF	65	01	20	F4	EF	78	8A	21	E1	å ¡±µ-ße ôïxŠ!á	
005AEB30	90	D2	0B	D5	D2	A6	78	40	8E	84	35	44	8A	С3	C4	2A	ò õò¦x@ž"5DŠÃÄ*	
005AEB40	12	41	0C	3C	42	C8	48	47	43	54	92	30	55	94	C0	C1	A <bèhgct'ou"àá< td=""><td></td></bèhgct'ou"àá<>	
005AEB50	0B	07	42	24	58	E4	2C	09	41	4A	77	14	6E	в0	CC	FO	B\$Xä, AJw n°Ìð	
005AEB60	B4	92	55	66	31	19	97	6C	90	C1	11	CF	65	72	D6	91	′′Ufl -l Á ÏerÖ`	
005AEB70	4F	16	52	07	91	15	A4	49	0A	85	31	2B	83	22	29	57	O R ' ¤I1+f")W	
005AEB80	DC	8D	9C	E9	46	5A	1D	C8	CD	28	48	3A	DD	51	43	D6	Ü œéFZ ÈÍ(H:ÝQCÖ	
005AEB90	56	30	79	CD	F2	BC	66	5A	35	F2	88	E4	BA	15	50	01	V0yÍò≒fZ5ò^ä° P	
005AEBA0	B2	D7	4A	EA	6D	AD	49	A9	3A	B8	C9	77	47	95	D1	22	²×Jêm−IC:,ÉwG•Ñ"	
005AEBB0	31	33	29	4B	6D	34	51	7B	C5	47	16	6B	68	F2	F2	34	13)Km4Q{ÅG khòò4	
005AEBC0	23	58	06	32	1B	63	92	16	0C	F2	90	09	04	32	B1	06	#X 2 c' ò 2±	
005AEBD0	78	DF	74	B8	FF	00	F9	6E	AD	45	BD	45	23	63	C4	72	xßt,ÿ ùn-E≒E#cÄr	
005AEBE0	C3	93	16	E8	85	EB	38	62	26	37	23	5A	2F	2E	09	AD	Ó èë8b&7#Z/	
005AEBF0	49	A 0	A1	14	EB	FF	D9		¥++++	+=+/	12.00		-	1.1	2	00	I; ëÿŬ	
005AEC00	00	00	00	00	00	00	00		远伏	巴始	们又自	1	AI	(+1		00		
005AEC10	00	00	00	00	00	00	00		选块	尾部	5		Al	t+2	P	00		
005AEC20	00	00	00	00	00	00	00		`T.bo	1244		_	_		-	00		
005AEC30	00	00	00	00	00	00	00	φ	添加	也签	·				2	00		
005AEC40	00	00	00	00	00	00	00		编辑	(E)					Þ	00		
005AEC50	00	00	00	00	00	00	00				~~	~~		~ ~)	00		
005AEC60	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		~

图 3-122 删除文件的最后一字节

步骤 13:由此,该删除文件的所有数据字节均被选中,在选中块上右击,在弹出的快捷 菜单中选择"编辑"→"复制选块"→"至新文件"选项,如图 3-123 所示,保存在桌面上,命名 为"huifu.jpg",如图 3-124 所示。

Offset	0	1	2	3	4	5	6	7	8	9	A	В	С	D	E	F	v	AN	SI	ASCII	~
005AEAE0																A8				"ñ¥ "	- 22
005AEAF0	62															15				‡ÐÑ;	
005AEB00	46															42				ŒËВ	
005AEB10	2A				1	-	ALLAN P				~	1.1	1000	76		69	*>†\$			SvÂi	
005AEB20					1 7	łi	议钥(U)			C	rl+Z		$\Xi \mathbf{A}$		E1	á ;±			ĭzš!á	
005AEB30					X	1	剪切(D			Ct	rl+X		03		2A	ÒÖ			dšāā*	
005AEB40					Do	1	夏朱小	たけ中()	\sim				>		正常	t(n)				Ctrl+C	1
005AEB50	()B)				10	1	市田上お		2/D)						TLU	5(0)				curre	
005AEB60						5	3火山位	NEXEX I	古(D)			~	<u></u>		作为	J UT	F-16				
005AEB70	4.57				×	札	5 除(I	R)				De			至亲	乐文化	‡(N)		Ct	rl+t+N	
005AEB80						¥	上 ()	つ字	H(P)					_		12-21	1 (0 4)				-
005AEB90	56					1	1711		50.7.						+7	、进制	制数值(H)	Ct	trl+t+C	
005AEBA0						둤	主义这	赴块(1	D)						伯胡		a示(F)		٨	It+++C	
005AEBB0	31					2	14t	A)			Ct	rl 1 A			-71110-11	1697				attite	
005AEBC0	23					-	E Re(4)			C	II+P	•:		GR	EP H	ex				
005AEBD0						1	青 除炎	选块(I	E)			Esc			C 30	5771	~ \				
005AEBE0	C3				i Da		shoe		-		C	-1.0			て混	灵伯当((-)				
005AEBF0	49					5	呈川山月	回区(:	5)		C	II+R			Pas	cal i	原码(P)	È			
005AEC00	00	00	00	00	(010	作	多改支	双据(M)		Ct	rl+1	1	00	00	00			_		-
005AEC10	00	00	00	00	(tj	直充送	选块(I	L)		C	trl+L		00	00	00					
005AEC20	00	00	00	00	011-1	ш		THI	- 1111			THE		00	00	00					

图 3-123 复制文件数据块至新文件

- 电子数据取证实训

136



图 3-124 恢复删除图片文件至桌面

至此完成非常驻文件的删除恢复!

3.8.4 实验小结

NTFS 文件系统与 FAT 文件系统差别很大,在 NTFS 中所有数据均以文件的形式存在,MFT 文件记录尤为重要,通过 MFT 可以定位每一个文件。

本实验意在让读者掌握 NTFS 文件系统的基本原理,如数据结构、索引存储等,实验环 境较为理想。在实际应用中,不连续存储的文件删除后,对于某些类型的文件,比如视频文 件,如果根据数据结构上下文搜索匹配进行恢复,运算量较大。