第5章 Windows取证

Windows是由微软公司开发的闭源图形化操作系统，其众多版本广泛应用于各类设备。主要版本如Windows XP、Windows 7、Windows 8、Windows 8.1、Windows 10、Windows 11，以及Windows Server 2003、Windows Server 2008、Windows Server 2012、Windows Server 2016、Windows Server 2019和Windows Server 2022。随着Windows版本的迭代更新，Windows 10和Windows 11已逐渐成为市场份额的主要占据者。本章将主要基于这两大版本展开实验，包括Windows系统的重要痕迹、Windows注册表、事件日志，以及Windows内存取证。

实验5.1 卷影复制

1. 预备知识

卷影复制，又称卷影副本、卷影拷贝（Volume Shadow Copy，VSC），是微软公司提供的一项自动或手动备份服务，旨在实现对卷内文件的有效快照。

系统还原点是指在特定时刻Windows操作系统所创建的系统快照，其目的在于协助操作系统恢复至某一特定时刻的正常运行状态，从而解决计算机运行速度缓慢或出现故障的问题。当Windows操作系统遭遇损坏时，系统可能会建议用户通过还原点进行恢复。用户可以手动创建还原点，或在重大系统事件（如系统更新、安装程序）发生前，由系统自动创建。默认情况下，还原点功能已启用，并每日自动生成一次快照。

卷影复制服务是自Windows 7操作系统起，各项操作系统所具备的一项功能。该服务通过为还原点创建数据快照，实现对操作系统的保护。换言之，该服务为还原点提供源数据，这些源数据即为卷影副本，且每个还原点均对应一个卷影副本。值得注意的是，卷影复制服务仅支持NTFS格式的分区或卷。

在数字取证过程中，调查人员能够通过分析卷影副本获取诸多有益的证据信息。这是因为卷影副本中可能保存了已删除文件的原件，例如已删除的BitLocker密钥，或已经删除的文件等。然而，卷影副本并不包含未分配簇、松弛扇区以及休眠文件等数据。为解析卷影副本，调查人员可运用X-Ways Forensics、自动化分析或ShadowExplorer等工具。

2. 实验目的

通过本实验的学习，了解卷影副本的基本概念，掌握卷影副本分析方法。

3. 实验环境

- 浏览器：推荐使用谷歌浏览器。
- 镜像挂载工具、ShadowExplorer。
- 5-A02-SU.E01。

4. 实验内容

步骤 1：利用镜像挂载工具，挂载 5-A02-SU.E01 镜像，查看盘符，发现本实验中盘符为 J。查看 J 盘的属性，单击“以前的版本”，如图 5-1 所示，可看到存在 2018 年 3 月 23 日的两个卷影副本信息，如图 5-1 所示。

图 5-1　存在两个还原点

步骤 2：运行 ShadowExplorer 软件，可读取出对应盘符中的卷影副本。比较两次还原点中的数据变化，可以参考如图 5-2 和图 5-3 所示的信息。

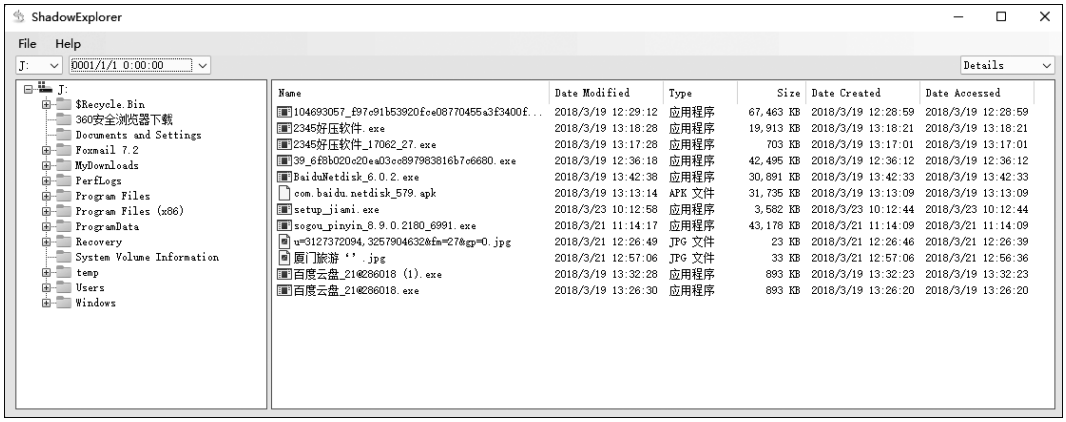


图 5-2　包含 2018 年 3 月 23 日 setup_jiami.exe 文件

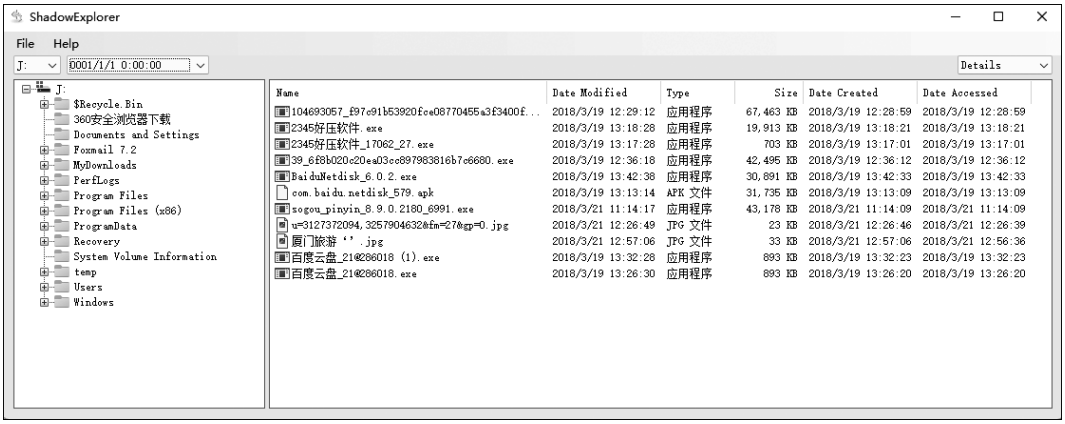


图 5-3　未包含 2018 年 3 月 23 日 setup_jiami.exe 文件

实验5.2　回收站

1. 预备知识

回收站作为 Windows 操作系统中的一项功能，主要用于存储用户已删除的文件，同时具备系统及隐含属性。在用户删除一份文件后，该文件会被默认存放至回收站，并持续保存。用户可选择“还原”操作将回收站内的文件恢复至原始位置，或选择“清空回收站”以彻底删除数据。在涉及企业内部调查的案件中，离职员工窃取并故意删除公司数据的情况屡见不鲜。那么，是否有办法追溯一个人在何时删除了哪些数据呢？通过深入分析回收站，调查人员有望揭示被删除数据及其删除时间。

在 Windows 操作系统中，当文件被删除时，若未清空回收站，实则该文件仍存储于磁盘，仅将之移至“回收站”。待用户执行“清空回收站”操作后，数据才被真正消除。若删除文件时按 SHIFT 键，文件将直接被彻底删除，不予进入回收站。回收站内的文件具有隐含及系统属性，且会被重新命名。在需要时，用户可将回收站中的文件恢复至原始位置。因此，文件原始信息实际上均被回收站保存。需要注意的是，不同版本的 Windows 在保存和处理这些信息方面存在差异。

(1) Windows XP 回收站格式分析

在 Windows XP 操作系统中，回收站的路径为 X:\RECYCLER，其中，X 代表驱动器的盘符。在该路径下，存在多个以 SID 命名的子文件夹，这些子文件夹分别存储着不同用户删除的内容。当文件被移入回收站后，其文件名会被修改为“DC＃＃＃.XXX”，其中，“DC”为固定不变的字符，“＃”为被删除文件自动设定的编号，“XXX”为被删除文件的原始扩展名。

在 RECYCLER 文件夹内，有一个名为 INFO2 的文件，该文件详细记录了已删除文件的原始路径、删除时间以及文件大小等信息。利用 WinHex 工具，可以直接解析 INFO2 文件，并通过预览模式查阅其内容。

不同 Windows 版本的回收站名称见表 5-1。

表 5-1　不同 Windows 版本的回收站名称

操作系统	文件系统	位置和名称
Windows 95/98/ME	FAT32	:\Recylced\INFO2
Windows NT/2000/XP	NTFS	:\Recycler\<ID>\INFO2
Windows Vista/7	NTFS	:\$Recycles.Bin\<USER ID>

（2）Windows 7 及后续版本回收站格式分析

自 Windows 7 至 Windows 11，回收站的路径固定为 X:\$Recycle.Bin，其中，X 代表相应驱动器的盘符。同时，$Recycle.Bin 文件夹内包含多个以 SID 命名的子文件夹，这些子文件夹存储了不同用户删除的各种数据。值得注意的是，与 Windows XP 回收站的命名规则不同，每个单独删除的文件在 $Recycle.Bin 文件夹中均对应两个文件。

在 Windows 系统删除文件的过程中，首先会生成一个文件，该文件用于记录被删除文件的原始名称、大小、路径和删除时间。该文件名的生成规则为“$I＋6 位字母和数字组合的随机数＋原始文件扩展名”。接着，回收站中原始文件的名称会被更改，命名规则为“$R＋相同的 6 位随机数＋原始扩展名”。因此，$I 文件保存了被删除文件的原始信息，而 $R 文件则为被删除的原始文件。两者后 6 位随机数相同。若要对 $I 文件进行解析，须借助专业工具，如 WinHex、RBCmd 和 $I_Parse 等。

需要注意的是，随着 Windows 系统的不断升级，不同版本回收站中的 $I 文件格式存在一定差异。图 5-4 和图 5-5 分别是 Windows 8 和 Windows 11 系统中 $I 文件的格式。

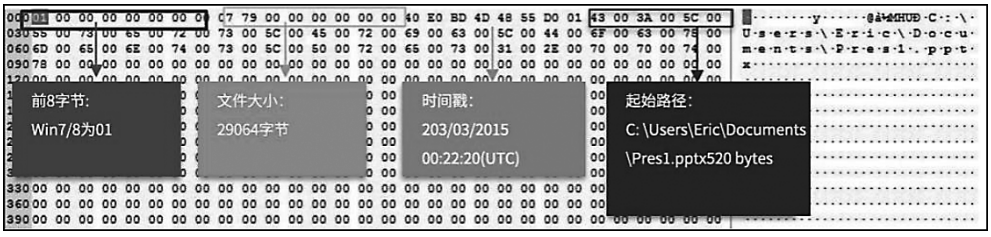


图 5-4　Windows 8 系统中 $I 文件的格式

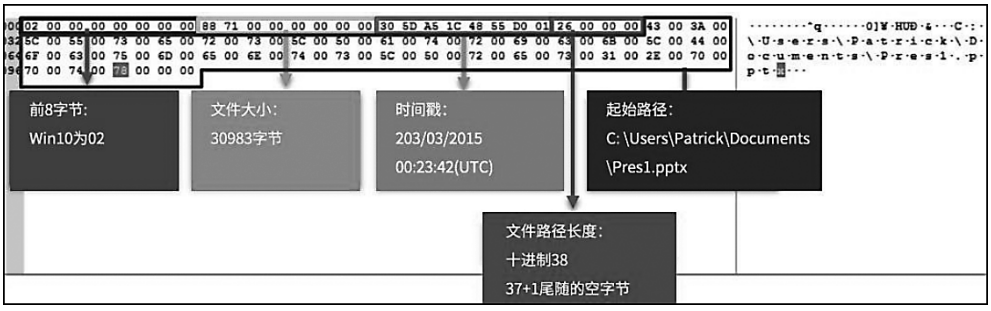


图 5-5　Windows 11 系统中 $I 文件的格式

2. 实验目的

通过本实验的学习，了解不同版本的操作系统中回收站的文件格式。

3. 实验环境

- 浏览器：推荐使用谷歌浏览器。
- WinHex 取证分析软件。
- 2.1-CCFC.E01、5-L04-PIC-FAT32.e01。

4. 实验内容

子实验 1　Windows XP 回收站日志分析

步骤 1：在案件中加载 2.1-CCFC.E01 镜像，通过文件名称过滤查找“INFO2”文件。在目录管理器窗口中，可以看到“分区 1”包含两个 INFO2 文件。通过路径中存在的两个不同的 SID，说明是两个不同的用户所属的回收站，如图 5-6 所示。

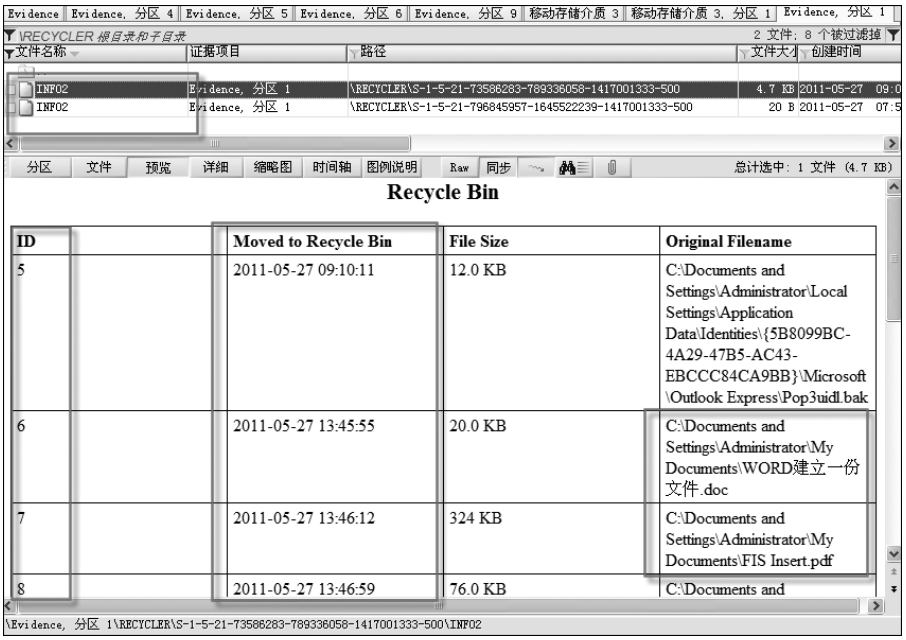


图 5-6　INFO2 预览

步骤 2：图 5-6 中 ID 栏目中的数字与图 5-7 文件名 DC 后面的数字相对应。分析可知删除文件的原始名称、原始路径和转移到回收站的时间。

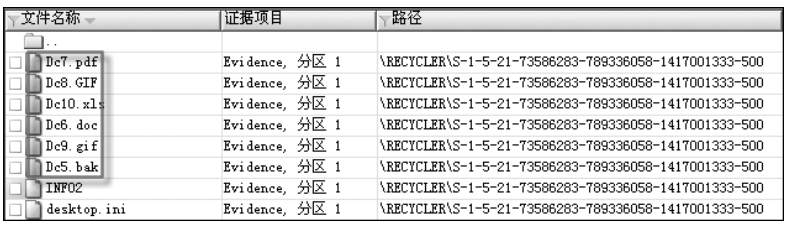
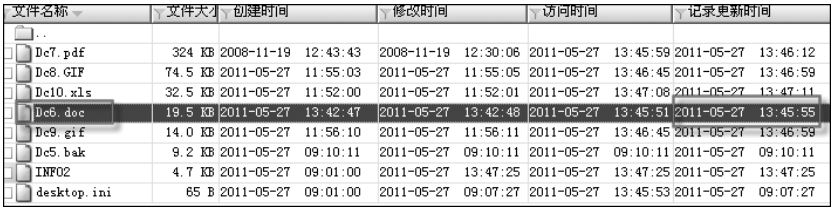


图 5-7　查看回收站文件信息

步骤 3：参考 INFO2 和文件名可知，ID 6 对应的文件是 Dc6.doc，大小为 20KB。文件被删除的时间为 2011-05-27 13:45:55，与 Dc6.doc 的记录更新时间相同，参考图 5-8。被删除文件的原始路径和文件名为：C:\Documents and Settings\Administrator\My Documents\WORD 建立一份文件.doc。



文件名称	文件大小	创建时间	修改时间	访问时间	记录更新时间
..					
Dc7.pdf	324 KB	2008-11-19 12:43:43	2008-11-19 12:30:06	2011-05-27 13:45:59	2011-05-27 13:46:12
Dc8.GIF	74.5 KB	2011-05-27 11:55:03	2011-05-27 11:55:05	2011-05-27 13:46:45	2011-05-27 13:46:59
Dc10.xls	32.5 KB	2011-05-27 11:52:00	2011-05-27 11:52:01	2011-05-27 13:47:08	2011-05-27 13:47:11
Dc6.doc	19.5 KB	2011-05-27 13:42:47	2011-05-27 13:42:48	2011-05-27 13:45:51	2011-05-27 13:45:55
Dc9.gif	14.0 KB	2011-05-27 11:56:10	2011-05-27 11:56:11	2011-05-27 13:46:45	2011-05-27 13:46:59
Dc5.bak	9.2 KB	2011-05-27 09:10:11	2011-05-27 09:10:11	2011-05-27 09:10:11	2011-05-27 09:10:11
INFO2	4.7 KB	2011-05-27 09:01:00	2011-05-27 13:47:25	2011-05-27 13:47:25	2011-05-27 13:47:25
desktop.ini	65 B	2011-05-27 09:01:00	2011-05-27 09:07:27	2011-05-27 13:45:53	2011-05-27 09:07:27

图 5-8　查看时间属性

子实验 2　Windows 10 中被删除的文件夹

步骤 1：在案件中加入 5-L04-PIC-FAT32.e01 镜像文件，浏览镜像中 $Recycle.Bin 文件夹，依据用户 SID 定位对应用户回收站目录，如图 5-9 所示。被删除的文件夹已被重命名为以 $R 为前缀（目录具有 $R 前缀但无扩展名），同时生成一个以 $I 为前缀的描述且后续字符完全相同的文件。原文件保存位置和删除时间可在预览模式下，在 $I 文件中查询。

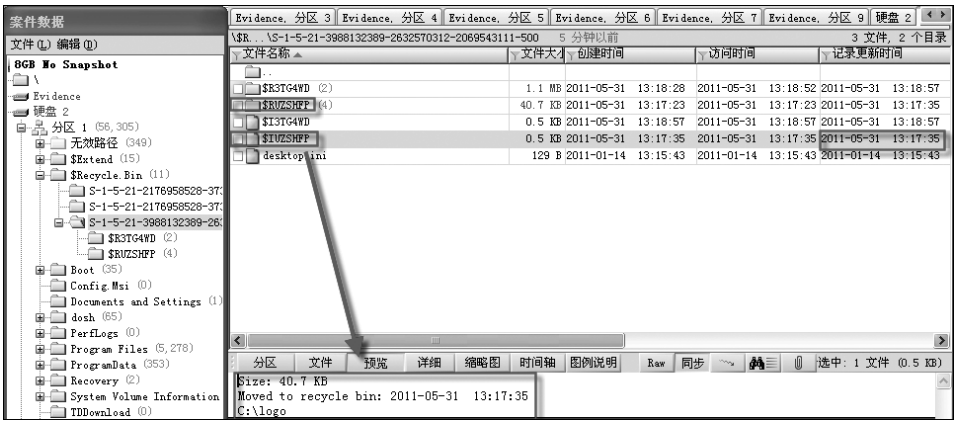


图 5-9　$R 与 $I 文件一一对应

步骤 2：进入 $R 目录下，可以看到被删除的文件原始文件名、扩展名不变，如图 5-10 所示。

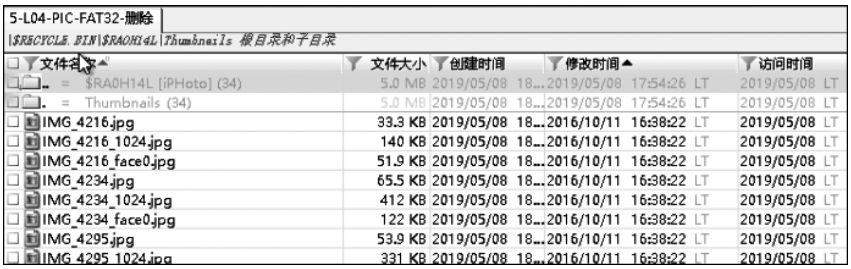


图 5-10　5-L04-PIC-FAT32.e01 案例中被删除的文件

实验5.3 缩略图

1. 预备知识

计算机硬盘中保存着大量的图片，包括正常存在的图片、被删除的图片、复合文件中嵌入的图片、压缩文件中的图片以及缩略图。正常图片文件来源多样，如 Windows 自带的、从互联网暂存的、个人照片以及程序编制的。删除的图片是经过删除或格式化后仍残留的。复合文件中的图片主要来源于 Word、PPT、PDF 以及邮件等。压缩文件中的图片包括压缩文件本身及其中嵌入的图片。缩略图则包括 Thumbs.db 和 JPG 图片中的嵌入信息。

许多取证工具都提供了缩略图查看方式，以便快速浏览众多的图片，如图 5-11 所示。在缩略图查看模式下，当前目录下的所有文件将以图形方式展示。非图片文件显示为文件图标，图片文件则展示其缩略图。若无法预览，则可能出现文件损坏。

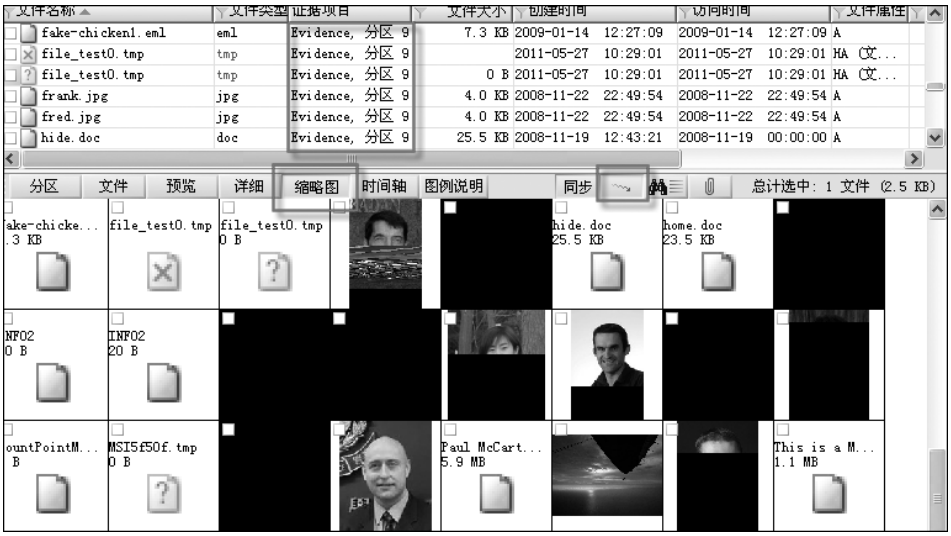


图 5-11 缩略图方式预览

(1) 不同版本 Windows 操作系统中的缩略图存储方式

为了便于用户快速浏览 jpg、png、avi 等多媒体文件内容，自 Windows XP 起，操作系统配备了缩略图功能。在 Windows XP 中，缩略图被固定存储在各个文件夹的 thumbs.db 文件中。而在 Windows 7 中，该功能得以改进，取消了 thumbs.db 方式，将缩略图文件移至“C:\Users\<UserName>\AppData\Local\Microsoft\Windows\Explorer”文件夹下的 thumbcache_*.db 文件。其中，* 代表缩略图的尺寸，包括 32、96、256、1024 等不同等级，以满足用户在文件资源管理器中浏览文件时选择大图标、小图标等不同查看模式的需求。自 Windows 10 版本起，缩略图存储规则保持不变，但增加了 16、48、768、1280、1920 等更多尺寸选项，进一步提升了用户体验。

(2) 缩略图文件内容

Thumbs.db 是 Windows XP/2003 操作系统中用于提升文件夹在缩略图查看模式下响应速度的缓存文件，通常也被称为缩略图文件。当以缩略图形式查看包含图片或视频文件的目录时，系统中会生成一个 thumbs.db 文件。该文件中以 JPEG 格式保存了目录下每个图片的缩略图信息。

Thumbs.db 文件能缓存包括 jpeg、bmp、gif、tif、pdf 和 htm 在内的图像文件格式，其属性为“系统文件＋隐藏文件”，在常规情况下不会显示。随着文件夹中图片数量的增加，该文件体积会相应增大。在 Windows XP Media Center Edition 版本中，生成的缩略图名称为 ehthumbs.db，并能保存视频文件预览。然而，部分旧版本的 thumbs.db 格式缩略图无法正常提取，此类文件会被纳入报告表，并标注为“不支持的 thumbs.db”。此时，可借助 GreenSpot Technologies Ltd 公司发布的免费 DM Thumbs 程序进行查看。

(3) 缩略图文件查看方式

在不同版本的操作系统中，thumbcache_ *.db 文件的签名存在一定差异。如图 5-12 展示的那样，在 Windows 10 系统中，缩略图文件头部特征字节的值为 0x20；而在 Windows 8.1 系统中，该值则为 0x1F；在 Windows 7 系统中，该值为 0x15。

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
00000000	43	4D	4D	4D	20	00	00	00	06	00	00	00	00	00	00	00	CMMM
00000010	18	00	00	00	9C	C6	9D	01	43	4D	4D	4D	6A	62	01	00	œÆ CMMMjb
00000020	0F	07	36	EC	C8	67	C3	EE	20	00	00	00	00	00	00	00	6ìÈgÃî

图 5-12　Windows 10 中缩略图文件的文件头

Thumbcache_x.db 文件需要借助专业的取证工具才能查看，调查人员可以使用 X-Ways Forensics 或 Thumbcache Viewer 等工具来分析缩略图文件。

2. 实验目的

通过本实验的学习，了解缩略图的基础概念，更好地理解在 Windows 系统中缩略图的生成原理和鉴证价值；掌握使用 Windows File Analyzer 分析缩略图的方法。

3. 实验环境

- 浏览器：推荐使用谷歌浏览器。
- WinHex 取证分析软件、Windows File Analyzer。
- 2.1-CCFC.e01、5-C03-缩略图 2.VHD。

4. 实验内容

子实验 1　查询图片中的缩略图

在正常的 JPEG 图像中皆内嵌一副 JPG 格式的小型图像，此图像可手动或自动提取。工具软件提取出的缩略图呈现为一个虚拟文件，其文件名与原图像名称一致，并标记有“Thumbnail”字符。缩略图文件大小通常仅有几 KB 至十几 KB，且不包含创建时间。

步骤 1：在案件中加载 2.1-CCFC.e01 镜像，查找 Thumbs.db 文件。

步骤 2：使用 WinHex 软件解析 Thumbs.db 文件，找到分区 9 的“照片\Camara”目录，以缩略图模式查看目录，可以看到存在 17 幅图片，如图 5-13 所示。

图 5-13　缩略图方式查看图片

步骤 3：按 Ctrl＋A 快捷键，选择所有文件，右击选择“标记”。

步骤 4：选择磁盘快照，经过“查找嵌入在文件内的 JPEG 和 PNG 图片”选项之后，通过对 17 个文件进行分析可看到，新增加了 24 个文件。

步骤 5：从分析结果可以发现，该目录文件都被显示为包含子数据。单击“浏览”，可以看到每个图片中都有一个名称为“缩略图.JPG”的文件，这就是该文件的缩略图。

子实验 2　用 WFA 解析 Windows 缩略图

步骤 1：挂载“5-C03-缩略图 2.VHD”后，可以看到如图 5-14 所示的目录结构。Windows File Analyzer 软件保存在 WFA.zip 压缩文件中。解压缩该文件，运行 Windows File Analyzer。

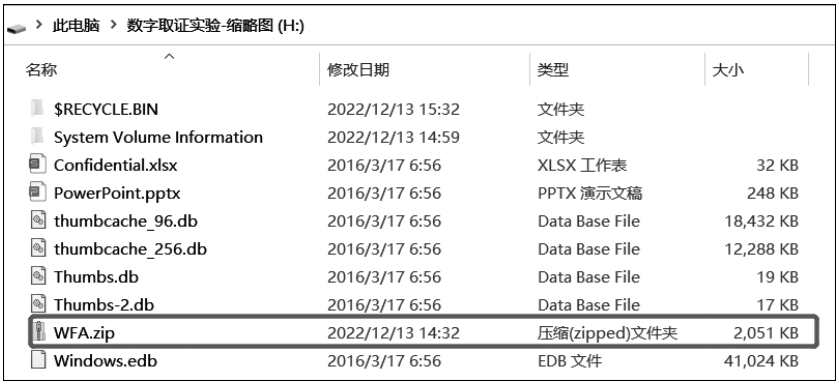


图 5-14　镜像中包含 WFA.zip 压缩包

步骤 2：从主菜单中选择 File，然后选择“Analyze Thumbnail Database”，再选择“Windows XP”，选择解压缩的 Thumbs.db 文件，Windows File Analyzer 将解析数据库并显示信息，如图 5-15 所示。

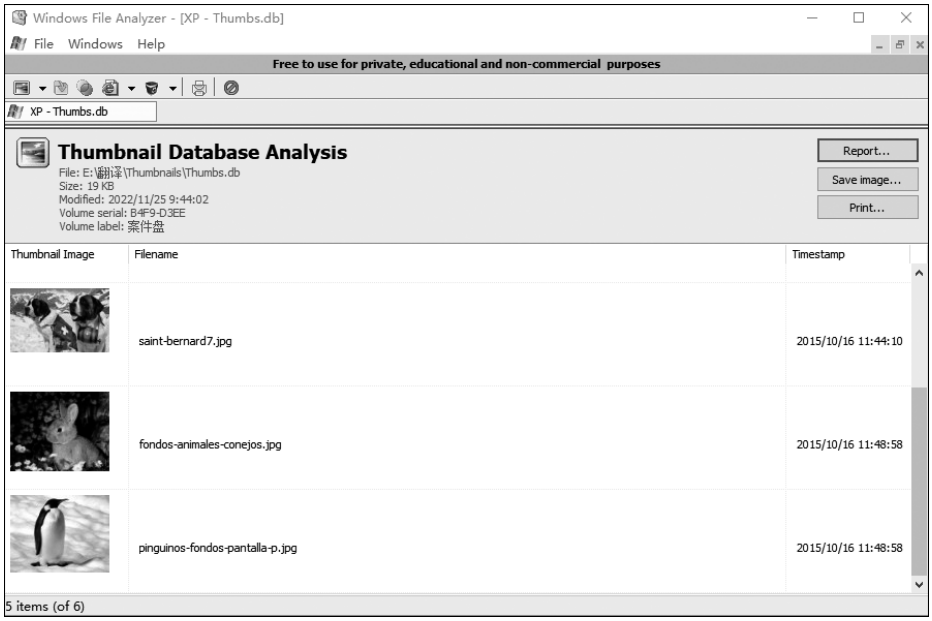


图 5-15　镜像中的数据结构

步骤 3：通过分析可知该卷的序列号为 DC6F-A898，如图 5-16 所示。进一步分析发现，Windows File Analyzer 程序查询了本地硬盘。

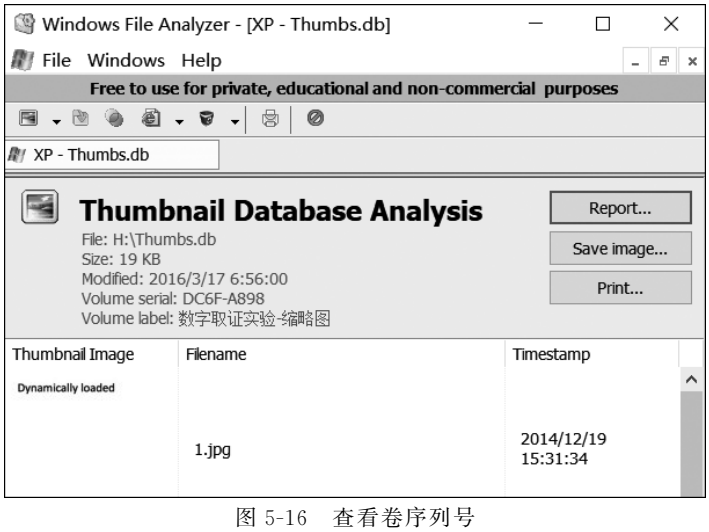


图 5-16　查看卷序列号

步骤 4：过滤出“saint-bernard7.jpg”文件，查询该文件的时间戳，结果如图 5-17 所示，文件的时间戳为 2015 年 10 月 16 日上午 11:44:10(UTC)。