

GPT 磁盘克隆成 MBR 磁盘后数据恢复的研究

陈培德, 吴建平, 王一景, 邓 剑, 朱辰龙

(云南大学 信息学院, 云南 昆明 650223)

摘 要: 用户在使用 Ghost 工具软件安装操作系统或者克隆磁盘时, 有时会将“选择镜像文件到分区”误操作为“选择镜像文件到磁盘”; 克隆结束后, 导致整个 GPT 磁盘成为一个大 C 盘, GPT 磁盘中各逻辑盘丢失的现象。针对这种情况, 以 Windows7 为平台, Ghost8.0 为实验软件, WinHex15.08 为数据分析与恢复软件, 在虚拟 GPT 磁盘中建立 5 个卷, 5 个卷的文件系统都是 NTFS。再制作一个镜像文件, 在镜像文件中建立一个 MBR 分区, 对应文件系统也是 NTFS。将镜像文件克隆到 GPT 磁盘中, 造成 GPT 磁盘中原来 5 个卷对应分区丢失。对克隆后的 GPT 磁盘结构进行分析, 提出了恢复 GPT 磁盘各卷的基本思路、方法与步骤, 即恢复克隆前的 GPT 头和 GPT 头备份。实验结果表明: 除第 1 个分区中的部分数据被覆盖无法恢复外, GPT 磁盘中剩余 4 个卷的数据均可完整恢复。

关键词: GPT 分区; MBR 分区; NTFS 文件系统; NTFS_DBR 中 BPB 参数; 元文件 \$ MFT

中图分类号: TP393

文献标识码: A

文章编号: 1673-629X(2020)05-0094-05

doi: 10.3969/j.issn.1673-629X.2020.05.018

Research on Data Recovery after GPT Disk Cloned into MBR Disk

CHEN Pei-de, WU Jian-ping, WANG Yi-jing, DENG Jian, ZHU Chen-long

(School of Information Science and Engineering, Yunnan University, Kunming 650223, China)

Abstract: When users install operating systems or clone disks using Ghost tool software, sometimes “Select Mirror File to Partition” is misrepresented as “Select Mirror File to Disk”, leading to the entire GPT disk to become a large C disk and loss of logic disks on GPT disks after the cloning. In this case, with Windows 7 as the platform, Ghost 8.0 as the experimental software, WinHex15.08 as the data analysis and recovery software, 5 volumes are created on virtual GPT disks. Five volumes of the file system are NTFS. Make another mirror file where a MBR partition is established. The corresponding file system is also NTFS. Clone a mirror file into a GPT disk, which causes loss of the original 5 volumes corresponding partition in GPT disk. Analysis of the cloned GPT disk structure, the basic ideas, methods and steps of restoring the volumes of GPT disk are presented, that is, restoring the GPT head and GPT head backup before cloning. The experiment shows that unless part of the data in the first partition is overwritten and cannot be restored, the data of the remaining 4 volumes in the GPT disk can be fully restored.

Key words: GPT partition; MBR partition; NTFS file system; BPB parameter of NTFS_DBR; \$ MFT meta file

0 引言

Ghost 是目前使用得比较多的快速地在硬盘上安装操作系统、备份和恢复数据的一款工具软件^[1], 实现了多种硬盘分区格式的分区及硬盘数据的备份和还原功能^[2]。

在微软视窗操作系统广为流传的基础上, 为避开视窗操作系统原始完整安装的费时和重装系统后驱动应用程序再装的麻烦, 许多软件安装人员把自己做好的干净系统用 Ghost 来备份和还原^[3]。为易于操作, 其流程被一键 Ghost、一键还原精灵等进一步简化, 它

的易用很快得到了软件安装人员的喜爱^[4]。将视窗操作系统 Windows XP、Windows VISTA、Windows 7 等软件与系统引导文件、硬盘分区工具等集成为一体, 进一步进行配套, 这样用户在需要重装系统时有效且简便地完成系统快速重装。

GPT 是 Globally Unique Identifier Partition Table 的缩写, 其含义是“全局唯一标识磁盘分区表”^[5]。GPT 的出现是为了替代旧式的 MBR (master boot record)^[6], 主要解决了 MBR 分区表不支持容量大于 2 TB 的分区问题^[7]。

收稿日期: 2019-06-27

修回日期: 2019-10-30

网络出版时间: 2020-01-10

基金项目: 国家自然科学基金面上项目(41571010); 云南大学项目(C176240501007)

作者简介: 陈培德(1966-), 男, 实验师, 研究方向为文件系统与数据恢复技术。

网络出版地址: <http://kns.cnki.net/kcms/detail/61.1450.TP.20200110.1121.040.html>

如果用户的硬盘为 GPT 分区,即 GPT 磁盘,用户在使用 Ghost 软件安装系统时,由于操作不慎,会误将选择分区操作为选择整个硬盘^[8];以至于安装系统后,只有一个分区,其分区的大小为整个硬盘的大小^[8]。导致 GPT 磁盘中的各分区丢失,出现 GPT 磁盘中数据无法正常读取的现象。

针对这一情况,对 Ghost 后,GPT 磁盘中的数据恢复进行了大量的实验,发现 Ghost 后大部分数据可以完整恢复。

1 实验环境与制作实验素材

1.1 实验环境

- 操作系统:Windows 7;
- 硬盘:虚拟硬盘;
- 工具软件:Ghost32 8.0;
- 数据分析及恢复工具:WinHex 15.08。

1.2 制作目标盘实验素材

步骤 1:在 Windows 7 操作系统下,使用 Windows 7 的虚拟磁盘管理功能在 D 盘的根目录上建立一个名为 abcd1.vhd 的文件,文件大小为 5 GB。

步骤 2:将 abcd1.vhd 文件附加为虚拟磁盘 1,转换成 GPT 磁盘;在磁盘 1 上依次建立 5 个分区,并分别对 5 个分区进行(快速)格式化操作,文件系统选择 NTFS,磁盘 1 中 5 个分区依次对应 5 个逻辑盘情况如下:

- (1)H 盘,文件系统:NTFS,容量:800 MB;
- (2)I 盘,文件系统:NTFS,容量:1 000 MB;
- (3)J 盘,文件系统:NTFS,容量:1 200 MB;
- (4)K 盘,文件系统:NTFS,容量:1 000 MB;
- (5)L 盘,文件系统:NTFS,容量:1 085 MB。

步骤 3:分别复制一定数量的文件夹和文件到这 5 个逻辑盘中。

至此,目标盘实验素材已制作完成。

1.3 制作源盘实验素材

步骤 1:在 Windows 7 操作系统下,使用 Windows 7 的虚拟磁盘管理功能在 D 盘的根目录上建立一个名为 abcd2.vhd 的文件,文件大小为 300 MB。

步骤 2:将 abcd2.vhd 文件附加为虚拟磁盘 2,转换成 MBR 磁盘;在磁盘 2 上依次建立 1 个分区,并对该分区进行(快速)格式化操作,文件系统选择 NTFS,对应的盘符为 M 盘。

步骤 3:复制一定数量的文件夹和文件到 M 个逻辑盘中。

步骤 4:使用 Ghost 软件中的镜像功能将磁盘 2 镜像成为一个文件,文件名为 abcd2.GHO,存储在 D 盘的根目录下。

至此,源盘实验素材已制作完成。

2 Ghost 前磁盘 1 布局图

Ghost 前,磁盘 1 的布局如图 1 所示,说明如下:

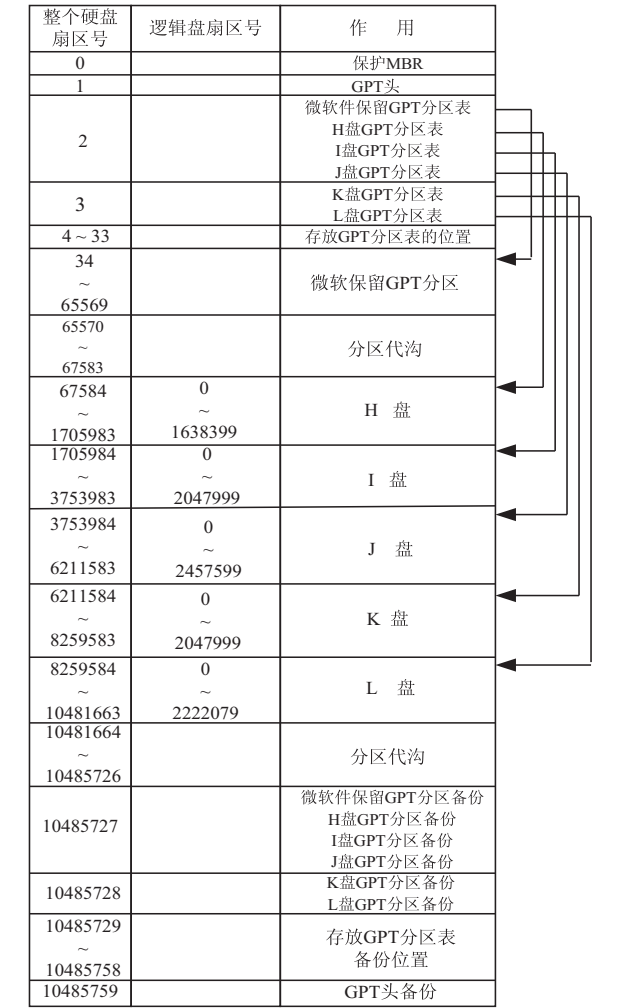


图 1 Ghost 前,磁盘 1 布局图

(1)磁盘 1 为 GPT 磁盘;而 0 号扇区存储的 MBR 分区表为“00 00 02 00 EE FF FF FF 01 00 00 00 FF FF FF FF”^[9],从分区表可知,相对扇区为 01(注:存储形式为 01 00 00 00)^[10],总扇区数为 4 294 967 295(注:存储形式为 FF FF FF FF)^[10],分区标志为“EE”^[11],即该分区是保护 MBR^[10]。

(2)1 号扇区存储的是 GPT 头^[12];2 号扇区存储了 4 个 GPT 分区表,即微软保留、H 盘、I 盘、J 盘;而 3 号扇区存储了 2 个 GPT 分区表,即 K 盘和 L 盘 GPT 分区表。

(3)通过 2 号扇区和 3 号存储的分区表可以定位微软保留 GPT 分区、H 盘、I 盘、J 盘、K 盘和 L 盘在 GPT 磁盘中的具体位置。

(4)10485727 号扇区和 10485728 号扇区分别存储的是 2 号扇区和 3 号扇区的备份,10485729 号扇区存储的是 GPT 头备份。

3 对磁盘 1 进行 Ghost 操作

步骤 1:附加 D 盘根目录下的 abcd1. vhd 文件成为磁盘 1,所产生的 5 个逻辑盘符分别为 H 盘、I 盘、J 盘、K 和 L 盘。

步骤 2:运行 Ghost32 8. 0,选择“Local→Disk→From →Image”,在弹出的窗口中选择 D 盘根目录下的 abcd2. GH0 文件,即源文件选择“abcd2. GH0”。

步骤 3:在“Select local destination drive by clicking on the drive number”窗口中选择 Drive2,即选择第 2 个物理硬盘,也就是 abcd1. vhd 文件附加后的虚拟磁盘 1,单击“OK”按钮。

步骤 4:大约 6 秒后,磁盘 1 中的 5 个逻辑盘被 1 个逻辑盘所取代,即磁盘 1 中只有 1 个逻辑盘,盘符为 H:,大小为 4. 99 GB。

至此,实验素材已制作完成。

4 Ghost 后磁盘 1 布局图

Ghost 后,磁盘 1 的布局如图 2 所示,说明如下:

整个硬盘扇区号	作 用	
0	Ghost后,新H盘MBR分区表	
1		
2	Ghost前, 微软保留、H、I、J盘GPT分区表	
3	Ghost前, K和L盘GPT分区表	
4 ~ 62		
63 ~ 67583		被覆盖的区域
67584 ~ 614462	Ghost前, H盘所在位置	
614463 ~ 614464		
614464 ~ 1705983		
1705984 ~ 3753983	Ghost后, 新H盘所占区域	
3753984 ~ 6211583		Ghost前, I盘所在位置
6211584 ~ 8259583	Ghost前, J盘所在位置	
8259584 ~ 10474378	Ghost前, K盘所在位置	
10474379 ~ 10474380		
10474380 ~ 10485726		
10485727		
10485728	Ghost前, 微软保留、H、I、J盘GPT分区表备份	
10485729	Ghost前, K盘和L盘GPT分区表备份	
10485730 ~ 10485758		
10485759		

图 2 Ghost 后,磁盘 1 布局图

(1)磁盘 1 已经由 GPT 磁盘自动转换为 MBR 磁

盘;而 0 号扇区存储的 MBR 分区表为“00 01 01 00 07 FE BF 8B 3F 00 00 00 4D D3 9F 00”;从分区表可知,相对扇区为 63(注:存储形式为 3F 00 00 00),总扇区数为 10 474 317(注:存储形式为 4D D3 9F 00);分区标志为“07”^[13],即该分区对应的文件系统是 NTFS^[14]。

(2)1 号扇区存储的 GPT 头已被 00 填充,即 GPT 头已被破坏;2 号扇区存储的 4 个 GPT 分区表和 3 号扇区存储的 2 个 GPT 分区表均完好无损地保存着。

(3)10 485 727 号扇区存储的 4 个 GPT 分区表备份和 10 485 728 号扇区存储的 2 个 GPT 分区表备份均完好无损地保存着;而 10 485 759 号扇区存储的 GPT 头备份已被 00 填充,即 GPT 头备份已被破坏。

(4)由于 0 号扇区存储的保护 MBR,1 号扇区存储的 GPT 头,10 485 759 号扇区存储的 GPT 头备份已经被破坏;所以,2 号扇区和 3 号扇区存储的 GPT 分区表;10 485 727 号扇区和 10 485 728 号扇区存储的 GPT 分区表备份已经不再起作用。

(5)Ghost 后,从 0 号扇区的 MBR 分区表可知,新 H 盘的开始扇区号为 63,而结束扇区为 10 474 379,即被覆盖的区域为 63 号扇区~614 463 号扇区;也就是说 Ghost 前,只有微软保留分区和 H 盘的部分扇区被覆盖,因为 abcd2. GH0 的实际大小为 300 MB,占 614 400 个扇区。所以,I 盘、J 盘、K 盘和 L 盘中存储的数据均未被覆盖;为成功恢复 I 盘、J 盘、K 盘和 L 盘中全部数据以及 H 盘中的部分数据带来了希望。

5 重建 GPT 分区的基本思路与方法

从图 2 可知,Ghost 后,从 614 464 号扇区到 10 485 759 号扇区,除 10 474 379 号扇区被新 H 盘 NTFS_DBR 备份所覆盖,10 485 759 号扇区被填充为 00 外,其余扇区的内容一般都完好无损地保留。

作者经过大量的实验,发现重建 GPT 分区的基本思路与方法如下:

(1)将 2 号扇区和 3 号扇区以文件的形式备份。

(2)在磁盘管理中删除 MBR 分区。

(3)将 MBR 磁盘转换为 GPT 磁盘。

(4)通过备份的 2 号扇区和 3 号扇区恢复 GPT 分区表和 GPT 分区表备份。

(5)重新计算 GPT 头中对应 GPT 分区表的 CRC 校验和 GPT 头的 CRC 校验。

(6)重新计算 GPT 头备份中对应 GPT 分区表的 CRC 校验和 GPT 头的 CRC 校验。

6 重建 GPT 分区操作步骤

步骤 1:使用 WinHex 软件打开 D 盘根目录下的

abcd1.vhd 文件,并映像为磁盘。

步骤 2:将光标移动到 2 号扇区的开始位置,定义块首;将光标移动到 3 号扇区的结束位置,定义块尾;单击“复制”按钮。

步骤 3:通过 WinHex 的文件菜单,新建一个 VHD 文件,文件大小为 1 024 字节,并将光标移动到新建文件的开始位置,单击“粘贴”按钮,将该文件存盘,文件为“2~3.vhd”。

步骤 4:从 2 号扇区和 3 号扇区可以得到 6 个分区的开始扇区号和结束扇区号;将 6 个分区的开始扇区号和结束扇区号分别填入表 1 中。

步骤 5:退出 WinHex。

步骤 6:使用计算机管理中的磁盘管理附加 abcd1.vhd 后成为磁盘 1。

表 1 Ghost 后 6 个分区表的开始扇区号和结束扇区号

分区	开始扇区号	结束扇区号	存储内容
分区 1	34	65 569	微软保留分区
分区 2	67 584	1 705 983	H 盘分区
分区 3	1 705 984	3 753 983	I 盘分区
分区 4	3 753 984	6 211 583	J 盘分区
分区 5	6 211 584	8 259 583	K 盘分区
分区 6	8 259 584	10 481 663	L 盘分区

步骤 7:删除磁盘 1 中 H 盘分区;将 MBR 磁盘转换为 GPT 磁盘。

至此,磁盘 1 中 0 号扇区已经变成保护的 MBR,1 号扇区的 GPT 头已建立;而 2 号扇区和 3 号扇区存储的 6 个 GPT 分区表已经被删除 5 个,只保留 1 个,即微软保留分区表;10 485 727 号扇区和 10 485 728 号扇区存储的 GPT 分区表备份只保留 1 个,即微软保留分区表;而 10 485 759 号扇区存储的 GPT 头备份已建立。

步骤 8:分离磁盘 1,使用 WinHex 软件打开 D 盘根目录下的 abcd1.vhd 文件,并映像为磁盘。

步骤 9:使用 WinHex 软件打开 2~3.vhd 文件,全选,单击“复制”按钮;将光标移动至 abcd1.vhd 文件的 2 号扇区开始位置,单击“粘贴”按钮;将光标移动至 abcd1.vhd 文件的 10 485 727 号扇区开始位置,单击“粘贴”按钮,最后单击“保存”按钮,即通过 2~3.vhd 文件来恢复 abcd1.vhd 中的 GPT 分区表和 GPT 分区表备份,关闭 2~3.vhd 文件。

步骤 10:将光标移动 1 号扇区,即 GPT 头所在扇区号,可以查看到扇区偏移 0X58~0X5B 处的 GPT 分区表 CRC32 校验和为“4378B542”,注:存储形式为“42 B5 78 43”;如图 3 所示。

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	/
000000200	45	46	49	20	50	41	52	54	00	00	01	00	5C	00	00	00	EFI PART...\...
000000210	FF	5B	75	12	00	00	00	00	01	00	00	00	00	00	00	00	+{u.....
000000220	FF	FF	9F	00	00	00	00	00	22	00	00	00	00	00	00	00	yyI....."
000000230	DE	FF	9F	00	00	00	00	00	A7	88	41	D1	08	20	47	43	ÿI.....\$IÄÑ. GC
000000240	BE	06	88	23	97	9C	DB	F3	02	00	00	00	00	00	00	00	%.#I!Üö.....
000000250	80	00	00	00	80	00	00	00	42	B5	78	43	00	00	00	00	I...I...BjuxC...
Sector 1 of 10485761	Offset							29F	=0 Block: 13FFFE00-13FFFFFFF Size:								

图 3 1 号扇区的 GPT 头

步骤 11:将光标移动 2 号扇区开始位置,定义块首;将光标移动到 33 号扇区的末尾定义块尾,“工具”→“比较 Hash 值(M)...”→“CRC32(32Bit)”,可以计算出 6 个分区表的 CRC32 校验值为“78BBC529”;注:存储形式为“29 C5 BB 78”。

步骤 12:将 1 号扇区偏移 0X58~0X5B 处的 GPT 分区表 CRC32 校验和“4378B542”修改为“78BBC529”,注:存储形式为“29 C5 BB 78”。

步骤 13:将 1 号扇区偏移 0X10~0X13 处的 GPT 头 CRC32 校验和“12755BF7”修改为“00000000”。

步骤 14:将光标移动 1 号扇区开始位置,定义块首;将光标移动到 1 号扇区偏移 0X5B 处定义块尾,“工具”→“比较 Hash 值(M)...”→“CRC32(32Bit)”,可以计算出这 92 个字节的 CRC32 校验值为“FB7F2E0C”;注:存储形式为“0C 2E 7F FB”,然后存盘。

至此,1 号扇区的 GPT 头已成功恢复。

步骤 15:将光标移动到 10 485 759 号扇区,如图 4 所示,将偏移 0X58~0X5B 处的 GPT 分区表 CRC32 校验和“4378B542”修改为“78BBC529”,注:存储形式为“29 C5 BB 78”。

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	/
13FFFE00	45	46	49	20	50	41	52	54	00	00	01	00	5C	00	00	00	EFI PART...\...
13FFFE10	EB	8C	C4	68	00	00	00	00	FF	FF	9F	00	00	00	00	00	äIÄh...ÿyI....
13FFFE20	01	00	00	00	00	00	00	00	22	00	00	00	00	00	00	00"
13FFFE30	DE	FF	9F	00	00	00	00	00	A7	88	41	D1	08	20	47	43	ÿI.....\$IÄÑ. GC
13FFFE40	BE	06	88	23	97	9C	DB	F3	DF	FF	9F	00	00	00	00	00	%.#I!ÜöÿI....
13FFFE50	80	00	00	00	80	00	00	00	42	B5	78	43	00	00	00	00	I...I...BjuxC...
Sector 10485759 of 10485761	Offset							13FFFE6F	=0 Block: 200-25B Size:								

图 4 10 485 759 号扇区的 GPT 头备份

步骤 16:将 10 485 759 号扇区偏移 0X10~0X13 处的 GPT 头 CRC32 校验和“68C48CEB”修改为“00000000”。

步骤 17:将光标移动 10 485 759 号扇区开始位置,定义块首;将光标移动到 10 485 759 号扇区偏移 0X5B 处定义块尾,“工具”→“比较 Hash 值(M)...”→“CRC32(32Bit)”,可以计算出这 92 个字节的 CRC32 校验值为“81CEF910”,注:存储形式为“10 F9 CE 81”,然后存盘。

至此,10 485 759 号扇区的 GPT 头备份已成功恢复。

综上所述,Ghost 前的 GPT 分区表、GPT 分区表备份、GPT 头和 GPT 头备份已成功恢复。

步骤 18:使用 WinHex 软件重新打开 abcd1. vhd 文件并映像为磁盘,Partition2 ~ Partition5、Partition1 的开始扇区号,如图 5 所示。

Partitioning style: GPT					
Name ^	Ext.	Size	Created	Attr.	1st sector
Partition 2	?	0.8 GB			67584
Partition 3	NTFS	1.0 GB			1705984
Partition 4	NTFS	1.2 GB			3753984
Partition 5	NTFS	1.0 GB			6211584
Partition 6	NTFS	1.1 GB			8259584
Partition 1 (MS Reserved)		32.0 MB			34
Partition gap		1.0 MB			65570
Start sectors		17.0 KB			0
Unpartitioned space		2.0 MB			10481664
Sector 67584 of 10485761		Offset:	2100000	= 150 Block	

图 5 磁盘 1 中各 GPT 分区情况

从图 5 可知,Partition2 的开始扇区号为 67 584,而结束扇区号为 1 705 983,将 67 584 号扇区以文件的形式保存,将 1 705 983 号扇区复制到 67 584 号扇区,即通过 H 盘的 NTFS_DBR 备份恢复 NTFS_DBR,然后存盘并退出 WinHex。

步骤 19:通过计算机管理中的磁盘管理附加 abcd1. vhd 文件为磁盘 1,到资源管理器中可以看到 I 盘、J 盘、K 盘和 L 盘中的全部文件和文件夹,但是由于 H 盘前面的数据被覆盖,无法正常读取,H 盘的文件系统为 RAW^[15],单击盘符时,出现“磁盘未格式化”提示^[16]。

步骤 20:在 DOS 下,使用“CHKDSK H:/F/I”^[17]自动修复被破坏的 NTFS_文件系统,大约 3 分钟后,H 盘的文件系统已成功修复完成。

至此,H 盘中的大部分文件已成功恢复,但是被覆盖的文件无法恢复。

7 结束语

针对 GPT 磁盘被 Ghost 后,提出了恢复 GPT 分区的基本思路、方法与步骤;该方法的难点在于计算 GPT 头前 92 字节 CRC 校验和 GPT 分区表的 CRC 校验;未覆盖的逻辑盘中的数据可以成功恢复^[18],但被覆盖的数据无法恢复。如果硬盘总容量小于 2 TB 且分区数量小于或者等于 4 个时,也可以通过在硬盘 0 号扇区建立 MBR^[19]分区表的形式来恢复。

参考文献:

[1] 陈培德,吴建平,王丽清. Ghost 后数据恢复的研究与实现[J]. 计算机技术与发展,2017,27(1):112-116.

[2] 贺惠萍,荣彦,张兰,等. Windows 7 万能 Ghost 启动盘仿真软件的设计与实现[J]. 实验技术与管理,2014,31(5):127-130.

[3] 丁一钧. 利用 GHOST 重装操作系统疑难问题解析[J]. 电脑编程技巧与维护,2013(14):122-123.

[4] 杨海瑞. 试谈机房使用 Ghost 恢复系统的方法[J]. 电脑编程技巧与维护,2013(20):111-112.

[5] RUSSINOVICH M E, SOLOMON D A, LONESCU A. 深入解析 Windows 操作系统(英文版)[M]. 第 5 版. 北京:人民邮电出版社,2009.

[6] 陈培德. 大话数据恢复[M]. 北京:清华大学出版社,2019:71.

[7] 陈培德,吴建平,钱文华,等. 重建 GPT 分区的研究与实现[J]. 计算机技术与发展,2019,29(2):96-100.

[8] 刘伟. 数据恢复技术深度揭秘[M]. 北京:电子工业出版社,2010:185.

[9] 马林. 数据重现—文件系统原理精解与数据恢复最佳实践[M]. 北京:清华大学出版社,2009:84.

[10] 汪中夏,张京生,刘伟. RAID 数据恢复技术揭秘[M]. 北京:清华大学出版社,2010:157.

[11] 杨倩. 数据备份与恢复实训教程[M]. 北京:电子工业出版社,2016:74.

[12] NIKKEL B J. Forensic analysis of GPT disks and GUID partition tables[M]. Switzerland: Digital Investigation, 2009:39-47.

[13] SEONGBUK D, LEE S. Forensic signature for tracking storage devices: analysis of UEFI firmware image, disk signature and windows artifacts[J]. Digital Investigation, 2019, 29:21-27.

[14] CARRIER B. File system forensic analysis[M]. U. S. : Addison Wesley Professional, 2005.

[15] 陈培德,吴建平,王丽清. NTFS 文件系统实例详解[M]. 北京:国防工业出版社,2015.

[16] 陈培德,吴建平,王丽清. 重建 NTFS 的 DBR 及分区表的研究与实现[J]. 实验科学与技术,2016,14(6):56-59.

[17] 陈培德,王丽清,吴建平. NTFS 被快速格式化后数据恢复的研究[J]. 计算机技术与发展,2018,28(8):191-195.

[18] CHO G. A computer forensic method for detecting timestamp forgery in NTFS[J]. Computer & Security, 2013, 34:34-46.

[19] 封富君,姚俊萍,李晓军. 基于 NTFS 的数据恢复系统设计与实现[J]. 计算机科学与应用,2017,7(12):1245-1253.