

MFTMirr UFS1 UFS2
Winhex LBA DOS Windows Linux Unix Apple FreeBSD
OpenBSD MBR DBR EBR 55AA MHDD FinalData GPT
FAT12 FAT16 FAT32 NTFS HFS HFS+ MFT

数据重现

马林 编著

与数据恢复最佳实践
文件系统原理精解

Winhex LBA DOS Windows Linux Unix Apple FreeBSD OpenBSD MBR DBR EBR 55AA
MHDD FinalData GPT FAT12 FAT16 FAT32 NTFS HFS HFS+ MFT MFTMirr UFS1 UFS2
Ext2 Ext3 lnode Sun Solaris NetApp HP RAID JBOD SCSI SAS ATA SATA

- 数据恢复行业机密冒险公开
- 全面解密PC机、服务器分区体系
- 全面解密Windows、Linux、Apple、Sun、BSD文件系统
- 国内首次全面披露泛Unix类文件系统技术细节
- 从原理入手以“渔”代“鱼”
- 涉及众多底层细节，中文资料独家提供
- 大量阵列模型/阵列恢复实战

超值赠送
2DVD

- 分区、格式化模型
- 提供近30个阵列完整全真模拟环境
- 涵盖RAID0、RAID5、RAID 1E、HP双循环
- 块大小从3KB至256KB，盘数从3盘到13盘
- 包含左、右循环，同步、异步各种类型



清华大学出版社

分区卷柱面磁道扇区主引导记录数据恢复簇链
文件目录删除文件格式化
阵列跨区卷阵列循环方向布局左循环右循环同步
异步校验块双循环阵列红描述

本书详细讲解文件系统原理、目录长文件名、短文件名、分配策略、超级块、组、inode、文件目录、文件删除、文件删除文件、格式化、阵列、跨区卷、阵列恢复

数 据 重 现

——文件系统原理精解与数据恢复最佳实践

马 林 编著

清华大学出版社

北 京

内 容 简 介

本书是国内第一本全面介绍 Windows 及非 Windows 文件系统的数据恢复技术书籍, 不仅涵盖面广, 内容也达到了足够的深度。

本书不仅对常见的 DOS 分区体系及 Windows 的 FAT 文件系统、NTFS 文件系统进行了详细的介绍, 更涵盖了苹果机分区、BSD 分区、SPRC 平台的 Sun Solaris 分区、GPT 分区等分区方式, 以及 Linux 的 Ext2/Ext3、Unix 的 UFS1/UFS2、MAC 的 HFS+ 等文件系统布局及详细数据结构的讲解, 多数资料的详细程度是目前绝无仅有的。同时对常见 RAID 类型及包括 HP 内外双循环、RAID 1E、RAID 6 及 RAID DP 在内的异种或新型 RAID 类型进行了详细的分析和介绍。

另外, 本书还充分考虑到初学者刚接触数据恢复实际工作时无从下手的感觉, 从数据恢复前的准备到实际恢复工作的进行, 从理论分析到数据恢复软件的使用, 一步步带领读者踏入数据恢复的殿堂。

更为重要的是, 为了使读者有接近实战的机会练习 RAID 分析与恢复技术, 配书光盘(双 DVD)中附送了近 30 个精心制作的 RAID 模型, 包含了 RAID 0、RAID 5、RAID 1E、HP 内外双循环阵列等。

本书适合文件系统研究人员、数据恢复从业人员、数据恢复教学人员、数据恢复编程人员、电子取证工作者、数据安全研究人员、系统管理员及数据安全存储与灾难恢复爱好者阅读和使用。

本书封面贴有清华大学出版社防伪标签, 无标签者不得销售。

版权所有, 侵权必究。侵权举报电话: 010-62782989 13701121933

图书在版编目(CIP)数据

数据重现——文件系统原理精解与数据恢复最佳实践/马林编著. —北京: 清华大学出版社, 2009.4

ISBN 978-7-302-19893-2

I. 数… II. 马… III. 数据管理—安全技术 IV. TP309.3

中国版本图书馆 CIP 数据核字(2009)第 044473 号

责任编辑: 栾大成 宋延清

封面设计: 杨玉兰

版式设计: 北京东方人华科技有限公司

责任印制: 王秀菊

出版发行: 清华大学出版社

地 址: 北京清华大学学研大厦 A 座

<http://www.tup.com.cn>

邮 编: 100084

社 总 机: 010-62770175

邮 购: 010-62786544

投稿与读者服务: 010-62776969, c-service@tup.tsinghua.edu.cn

质 量 反 馈: 010-62772015, zhiliang@tup.tsinghua.edu.cn

印 刷 者: 清华大学印刷厂

装 订 者: 北京鑫海金澳胶印有限公司

经 销: 全国新华书店

开 本: 188×260 印 张: 35.5 字 数: 859 千字

附 DVD 光盘 2 张

版 次: 2009 年 4 月第 1 版

印 次: 2009 年 4 月第 1 次印刷

印 数: 1~5000

定 价: 69.00 元

本书如存在文字不清、漏印、缺页、倒页、脱页等印装质量问题, 请与清华大学出版社出版部联系调换。联系电话: (010)62770177 转 3103 产品编号: 032826-01

推 荐 序



在信息时代中，数据的重要性不言而喻。但由于各种原因(计算机病毒、物理损伤、误操作等)，导致数据丢失问题不断发生。例如 1998 年 4 月 26 日，全世界爆发了 CIH 计算机病毒，一夜之间，上千万台计算机的数据被病毒破坏，这就要求我们必须在数据意外丢失后能够尽最大可能地挽回数据，将损失降到最低。数据恢复便成了保障数据安全的一道防线。

数据恢复在安全系统中是最为精细的工作，稍不注意就会造成不可挽回的损失、彻底断送客户最后的希望。因此，数据恢复这个行业需要受过专业教育的从业人员和经过资质认证的企业。然而，用于数据恢复这方面教育和培训的书籍目前非常匮乏，很少有特别实用的数据恢复核心资料进入市面。

另外，恢复数据的工作要求必须对数据存储及管理方式有足够的了解，但这方面的相关资料也比较匮乏。在已有的部分数据恢复书籍中，内容一般都只集中于 Windows 方面，非 Windows 方面的内容一直缺乏足够的深度。《数据重现——文件系统原理精解与数据恢复最佳实践》一书，恰恰弥补了这个不足。

在分区体系方面，该书不仅介绍了使用较为广泛的 MBR 分区体系，还详细介绍了 Apple、GPT 等分区体系；在文件系统方面，不仅对 Windows 类的 FAT、NTFS 文件系统进行了详细的介绍，而且对 Linux、FreeBSD、OpenBSD、Sun Solaris、Mac 等操作系统所使用的文件系统格式进行了详细的讲解。不仅包含基本磁盘的数据恢复，还包含了磁盘跨区、RAID 等多磁盘卷的介绍。涵盖范围之广，内容之详细程度，是绝无仅有的。

最难能可贵的是，该书不仅为有志于数据恢复技术研究的人士提供了难得的技术资料，更兼顾了初学数据恢复者不知从何学起、不知如何下手恢复数据的状

况。作者结合实际工作经验，从如何检测磁盘、如何克隆磁盘、如何恢复数据、数据恢复软件恢复结果分析等一步步进行介绍，为有志于学习数据恢复的人士提供了很好的书籍，也是相关大学及专业进修学校的有力教材和参考书。

我在上世纪(1992年)就开始研究数据恢复技术，在民用和企业级防病毒安全产品上就提供了基本的数据恢复功能，深知这个领域的艰辛与重要性。

我衷心希望这本书的出版，能为数据恢复这个行业培育出更多的人才，让数据恢复产业更加蓬勃发展。

本书的作者马林，首次将数据恢复行业的一些核心技术内容放到书中，很有勇气！希望该书的出版能为中国的数据恢复行业做出应有的贡献！

江民科技创始人

2008 北京奥林匹克运动会特聘信息安全专家
北京市网络行业协会信息安全应急响应与处置中心主任



前 言

随着信息化技术的飞速发展和无纸化办公时代的到来，计算机正在我们的工作和生活中扮演着日益重要的角色。越来越多的企业、商家、政府机关和个人通过计算机来获取和处理信息，同时将自己最重要的信息以数据文件的形式保存在计算机硬盘或其他各种存储介质中。这些重要数据一旦因种种原因而丢失，将会给个人或企业造成重大的损失。因此，在数据遭遇丢失后，能否很好地保护数据现场并找回丢失的数据就显得尤为重要。于是，数据恢复，这一在国外已发展二十余年、在国内却鲜为人知的名词和技术开始被国人接触和涉足。但数据恢复技术却一直给人一种神秘莫测的感觉，数据恢复人员的具体工作方式仍然很少被了解。

数据恢复，就是将由于硬件损坏、误分区、误格式化、误删除、病毒破坏或其他原因导致的丢失或不可正常访问的数据恢复至正常状态的过程。

数据恢复可以分为“硬恢复”和“软恢复”两种。“硬恢复”是指由于存储介质物理上出现问题而导致的数据无法读取的恢复。“软恢复”则是指因逻辑故障导致的数据丢失的恢复，存储介质不存在物理的故障。硬恢复需要对存储介质的结构及工作原理相当了解，软恢复则需要对数据在存储介质内的管理方式——分区及文件系统有足够的认知。

曾有业内人士将数据恢复(单指“软恢复”)分为如下 3 个层次。

(1) 软件使用层

没有存储方面的理论基础，只是利用已有的恢复软件进行恢复操作，恢复效果只能由软件来决定。

(2) 理论知识与软件结合层

具有深厚的理论功底，对所要进行恢复的文件系统环境及文件结构有相当的了解，熟悉恢复软件各种参数设置的理论含义，可以针对不同的数据丢失情况进行详细分析并制定切实有效的恢复方案。在纯软件操作无法很好地完成恢复工作时，能够手工修改部分参数，为软件创造一个良好的恢复环境，从而最大限度地挽救数据。

(3) 数据恢复的“自由王国”

具备第 2 层次的基础，同时具有良好的编程能力，在现有的数据恢复软件无法胜任恢复要求的情况下，随时可以自行编写实用的程序，以弥补现有软件的不足，最大程度、最为快速地恢复数据。

进入第 1 个层次很容易，这也是最危险的层次。因为数据恢复的成功率既取决于数据丢失灾难的严重程度，又取决于灾难现场的保护程度。我们在实际工作中发现，很多数据无法



恢复的原因是由于数据丢失现场没有得到很好的保护，甚至是由于一些恢复人员不懂得数据存储原理，产生错误操作导致现场被二次破坏造成的。

一个好的数据恢复人员必须进入第 2 个层次，因为挽救丢失的数据需要在保护好现场的前提下从底层恢复数据，这就要求恢复人员必须对分区结构、文件系统结构、文件系统对数据的管理方式及数据存储时的分配策略有足够的了解。但文件系统结构及工作方式往往是核心技术而不被公开，导致相关的资料比较匮乏。尤其是对于在服务器领域应用较为广泛的非 Windows 类文件系统来说，其技术内幕更是难得知晓。同时，数据恢复又是一门理论与实践相结合的技术，尤其 RAID 的分析与重组，更需要对磁盘布局及文件系统结构有足够的了解并能够对其进行灵活运用，但技术资料的匮乏却使得很多数据恢复技术人员无法获得足够的理论知识。

本书将为读者揭开众多数据恢复技术底层知识的神秘面纱。通过对本书的学习，读者不但可以直接进入第 2 个层次，而且，如果您具有编程基础，还可从中获得很多的数据恢复编程思路。

读者对象

本书适合文件系统研究人员、数据恢复从业人员、数据恢复教学人员、数据恢复编程人员、电子取证工作者、数据安全研究人员、系统管理员及一切数据安全存储与灾难恢复爱好者阅读和使用。

本书特点

本书是国内第一本全面介绍 Windows 及非 Windows 文件系统的书籍，不仅涵盖面广，内容也达到了足够的深度。

本书不仅对常见的 DOS 分区体系及 Windows 的 FAT 文件系统系列、NTFS 文件系统进行了详细的介绍，更涵盖了**苹果机分区、BSD 分区、Sparc 平台的 Sun Solaris 分区、GPT 分区等分区方式**，以及**Linux 的 Ext2/Ext3、Unix 的 UFS1/UFS2、MAC 的 HFS+**等文件系统布局及详细数据结构的讲解，多数资料的详细程度是目前绝无仅有的。同时对常见 RAID 类型及包括**HP 内外双循环、RAID 1E、RAID6 及 RAID DP**在内的异种或新型 RAID 类型进行了详细的分析和介绍。

而且，本书在进行文字讲解的同时配以详细的图示，将枯燥抽象的理论与实际内容相结合，便于读者通过实际图示进行阅读和理解。同时，在理论讲解的基础上，将工作中的典型实际案例进行总结并浓缩成实验，对数据灾难发生时的破坏程度、系统的分配策略及数据的可恢复性进行分析，使读者能够在实际分析的过程中加深对理论的理解，将理论知识与实际数据恢复操作联系起来，从中获取数据恢复思路并将其拓展。

另外，本书不仅注重内容的深度及含金量，还兼顾了初学者刚接触数据恢复实际工作时感觉无从下手的情况，从数据恢复前的准备到实际恢复工作的进行，从理论分析到数据恢复

软件的使用，一步步带领读者踏入数据恢复的殿堂。

最后，本书通过对 RAID 的介绍与实例分析，使读者在分析 RAID 的过程中将文件系统知识与 RAID 知识相结合，不仅可以进一步熟悉文件系统，而且可以达到能够利用文件系统进行 RAID 分析与数据重组的技术水平。同时，还在配书光盘中准备了大量的 RAID 实例，使读者可以通过大量的实际练习加深理解，从而提高技术水平。

主要内容

本书共分为 11 章。

第 1 章介绍学习数据恢复需要掌握的一些基础知识，并对学习过程中需要用到的几个工具软件进行简要的介绍。

第 2 章详细地讲解 DOS 分区、Apple 分区、BSD 分区、Sun Solaris 分区及 GPT 分区。

第 3~7 章详细讲解 FAT、NTFS、Ext2/3、UFS1/2、HFS+ 等文件系统。

第 8 章讲解多磁盘卷，包括 RAID 和跨区卷。

第 9~11 章为数据恢复实际分析与讲解。其中——

第 9 章介绍恢复前应该进行的准备工作，对分区、格式化等操作给数据造成的破坏进行详细的分析。

第 10 章对误分区、误格式化、误删除等的可恢复性进行详细的分析，并对手工恢复及软件恢复做出详细的讲解。

第 11 章详细地讲解 RAID 的分析思路及恢复方法。

光盘说明

为了便于读者理解和消化理论，本书打破了以往同类书籍单纯书面介绍分区及文件系统的方法，将讲解过程中使用的磁盘模型附在配书光盘中，使读者不仅可以直观地观察到书中所讲到的实际操作结果，还可以将模型复制到本地磁盘中，跟随书中的讲解进行实际操作。

更为重要的是，为了使读者有更多机会练习 RAID 分析与恢复技术，配书光盘中附送了近 30 个精心制作的 RAID 模型，不仅包含了 RAID0、RAID5、RAID 1E，更包含了 HP 内外双循环阵列；块大小从 8 个扇区至 512 个扇区，盘数最多的阵列模型达到 13 块磁盘。各种阵列模型为广大读者创造了丰富的实际练习环境。

致谢

感谢江民科技创始人王江民先生在本书创作过程中给予的指点和肯定。

感谢北京信息科技大学数据恢复研究所刘伟老师、《大话存储》作者张冬、中国矿业大学博士江传力对本书的支持。



同时，在该专区中设立专门的“数据重现”交流区，便于读者就书中存在的问题、希望深入了解的知识内容等提出建议，也便于读者就书中不太理解的知识提出问题，与其他读者及作者本人进行讨论与交流。在该专区中，读者不仅可以深入学习和理解书中的知识内容，更有机会将书中的知识进行延展！

致谢

感谢江民科技总裁王江民先生在本书创作过程中给予的指点和肯定。

感谢北京信息科技大学数据恢复研究所刘伟老师、《大话存储》作者张冬、中国矿业大学博士江传力对本书的支持。

感谢天亚数据恢复研究中心(www.tysjhf.com)全体同仁为本书的创作提供的支持与帮助。

感谢青岛四通数据恢复王鹏、数据恢复资深爱好者王建华对本书的帮助。

特别感谢中国硬盘基地(bbs.intohard.com)站长田茂帅及工作人员对本书的发行所做的贡献。

感谢黄国伟为本书提供编程函数附录。

结束语

本书旨在抛砖引玉，作者愿与广大读者共同探讨有关的技术问题，欢迎读者光临网站 www.tysjhf.com 或致信 sjhfm1@163.com 进行沟通和交流。

目 录

PART 1 理论篇

第 1 章 数据恢复相关基础	3	2.1.3 扇区地址	37
1.1 硬盘探秘	4	2.1.4 根据合理性判断分区信息的 正确性	38
1.1.1 硬盘结构	4	2.1.5 数据恢复及电子取证	40
1.1.2 硬盘接口	7	2.2 DOS 分区	41
1.1.3 磁道、扇区与柱面	10	2.2.1 概述	41
1.1.4 硬盘的启动过程	12	2.2.2 主引导记录扇区 MBR	42
1.1.5 硬盘的性能指标	12	2.2.3 扩展引导记录扇区 EBR	50
1.1.6 寻址方式	13	2.2.4 数据恢复及电子取证	54
1.2 计算机运行流程	14	2.3 Apple 分区	56
1.2.1 基本概念	14	2.3.1 概述	56
1.2.2 计算机的启动过程	15	2.3.2 Apple 磁盘布局	56
1.3 “数”之体验	17	2.3.3 分区表项数据结构	58
1.3.1 数制	17	2.3.4 数据恢复与电子取证	61
1.3.2 数制间的转换	18	2.4 BSD 分区	61
1.3.3 取整与取余运算	19	2.4.1 BSD 分区概述	61
1.3.4 数的存储格式	19	2.4.2 Free BSD 分区	63
1.4 工具软件	20	2.4.3 NetBSD 与 OpenBSD 分区	64
1.4.1 虚拟磁盘软件 InsPro Disk	20	2.4.4 磁盘标签数据结构	65
1.4.2 十六进制编辑软件 Winhex	22	2.4.5 磁盘标签实例分析	67
1.4.3 硬盘检测软件 MHDD	29	2.4.6 总结	72
第 2 章 分区	33	2.5 Sun Solaris 分区	72
2.1 概述	34	2.5.1 概述	73
2.1.1 分区与卷	34		
2.1.2 Unix 下卷的使用	36		



2.5.2 Sparc 平台下的 Sun Solaris 分区.....	74	3.7.4 根目录与目录项.....	133
2.5.3 i386 平台下的 Sun Solaris 分区.....	78	3.8 分配策略.....	133
2.5.4 总结.....	82	3.8.1 簇的分配策略.....	133
2.6 GPT 分区.....	82	3.8.2 目录项的分配策略.....	134
2.6.1 概述.....	82	3.9 文件的建立与删除.....	136
2.6.2 GPT 磁盘总体布局.....	84	3.10 总结.....	137
2.6.3 数据结构.....	85	3.10.1 数据恢复分析.....	137
2.6.4 总结.....	90	3.10.2 取证分析.....	140
2.7 移动介质分区.....	90	第 4 章 NTFS 文件系统.....	145
第 3 章 FAT 文件系统.....	93	4.1 NTFS 概述.....	146
3.1 文件系统总论.....	94	4.1.1 概述.....	146
3.2 FAT 文件系统概述.....	99	4.1.2 基本概念.....	147
3.3 FAT 文件系统整体布局.....	100	4.2 NTFS 文件系统总体布局.....	149
3.4 FAT32 的保留区.....	100	4.3 引导扇区.....	149
3.4.1 引导扇区.....	101	4.4 主文件表 MFT.....	152
3.4.2 引导代码.....	106	4.4.1 基本概念.....	152
3.4.3 FSINFO 信息扇区.....	106	4.4.2 Windows 2000 的 MFT 项.....	153
3.5 FAT32 的 FAT 表.....	108	4.4.3 Windows XP 的 MFT 项.....	156
3.5.1 FAT 表概述.....	108	4.5 MFT 属性.....	160
3.5.2 FAT 表的特性.....	108	4.5.1 属性的结构.....	160
3.5.3 FAT 表的使用.....	109	4.5.2 常规属性类型.....	165
3.5.4 其他.....	111	4.5.3 其他属性.....	188
3.6 FAT32 的数据区.....	112	4.6 文件系统元文件.....	190
3.6.1 根目录.....	112	4.6.1 \$MFT 文件.....	190
3.6.2 子目录.....	115	4.6.2 \$MFTMirr 文件.....	191
3.6.3 目录项.....	116	4.6.3 \$LogFile 文件.....	192
3.7 FAT12/16 文件系统.....	128	4.6.4 \$Volume 文件.....	193
3.7.1 FAT12/16 文件系统概述.....	128	4.6.5 \$AttrDef 文件.....	193
3.7.2 引导扇区.....	128	4.6.6 \$Root 文件.....	195
3.7.3 FAT 表.....	131	4.6.7 \$Bitmap 文件.....	195
		4.6.8 \$Boot 文件.....	196
		4.6.9 \$Secure 文件.....	197

4.6.10 \$UsnJrnl 文件.....	198	5.7.3 i-节点的属性.....	239
4.6.11 \$Quota 文件.....	200	5.7.4 i-节点中时间值的更新	240
4.6.12 \$ObjId 文件.....	202	5.8 扩展属性	242
4.7 分配策略	203	5.8.1 扩展属性的结构.....	242
4.7.1 簇空间分配策略.....	203	5.8.2 扩展属性实例分析	245
4.7.2 MFT 项分配策略	203	5.9 目录项.....	246
4.7.3 属性分配策略	204	5.9.1 目录项数据结构.....	247
4.8 时间值的更新.....	204	5.9.2 目录项的特性.....	248
4.9 文件的建立与删除	205	5.9.3 目录项实例分析	250
4.9.1 建立文件.....	205	5.10 链接和挂载点.....	251
4.9.2 删除文件.....	206	5.10.1 链接	251
4.10 总结	207	5.10.2 挂载点.....	251
4.10.1 分析注意事项	207	5.11 Hash 树	252
4.10.2 数据恢复与取证分析	208	5.11.1 Hash 树数据结构	253
第 5 章 ExtX 文件系统.....	211	5.11.2 Hash 树实例分析	254
5.1 ExtX 文件系统概述.....	212	5.12 文件系统日志.....	255
5.2 ExtX 文件系统整体布局	213	5.12.1 数据结构.....	256
5.3 超级块.....	216	5.12.2 日志实例分析	258
5.3.1 超级块数据结构	216	5.13 分配策略	260
5.3.2 超级块实例分析	221	5.13.1 块的分配策略.....	260
5.4 块组描述符表和块组描述符	224	5.13.2 i-节点分配策略	261
5.4.1 块组描述符数据结构.....	224	5.13.3 文件名空间分配策略.....	262
5.4.2 块组描述符实例分析.....	225	5.14 文件的建立与删除	262
5.5 块位图	227	5.14.1 建立文件.....	262
5.5.1 块位图的工作方式	227	5.14.2 删除文件.....	264
5.5.2 块位图实例分析	228	5.15 总结	265
5.6 i-节点位图	229	5.15.1 分析注意事项	265
5.6.1 i-节点位图实例	229	5.15.2 数据恢复与电子取证.....	268
5.6.2 定位一个 i-节点的位图	230	第 6 章 UFS 文件系统.....	273
5.7 i-节点表与 i-节点.....	230	6.1 概述.....	274
5.7.1 i-节点数据结构	231	6.2 UFS 文件系统整体布局	276
5.7.2 i-节点实例分析	237		



6.3	超级块	276	7.2.3	主要数据结构类型	322
6.3.1	概述	276	7.2.4	HFS+特性	324
6.3.2	数据结构	277	7.3	HFS+文件系统整体布局	325
6.4	柱面组摘要	288	7.4	卷头	326
6.5	柱面组描述符	289	7.4.1	数据结构	326
6.5.1	概述	289	7.4.2	实例分析	331
6.5.2	数据结构	291	7.5	节点	333
6.5.3	位图	295	7.5.1	节点的种类	333
6.6	引导代码	297	7.5.2	节点的基本结构	333
6.7	i-节点	298	7.5.3	头节点	337
6.7.1	UFS1 的 i-节点	299	7.5.4	图节点	343
6.7.2	UFS2 的 i-节点	301	7.5.5	索引节点	344
6.8	目录项	305	7.5.6	叶节点	346
6.8.1	数据结构	306	7.5.7	节点的使用	346
6.8.2	实例分析	306	7.5.8	HFS+节点与 HFS 节点的 区别	347
6.9	分配策略	307	7.6	目录文件	348
6.9.1	存储空间分配策略	308	7.6.1	目录文件中档案项的 key 部分	349
6.9.2	i-节点分配策略	309	7.6.2	目录文件中档案项的 数据部分	350
6.9.3	目录项分配策略	309	7.7	域溢出文件	358
6.10	文件的建立与删除	310	7.7.1	域溢出文件中档案项的 key 部分	359
6.10.1	建立文件	310	7.7.2	域溢出文件中档案项的 数据部分	359
6.10.2	删除文件	312	7.7.3	域溢出文件节点实例分析	360
6.11	总结	313	7.7.4	域溢出文件的使用	361
6.11.1	分析注意事项	313	7.8	坏块文件	363
6.11.2	数据恢复与取证分析	315	7.9	分配文件	363
第 7 章	HFS+文件系统	317	7.10	属性文件	364
7.1	HFS 封装	318	7.10.1	叉数据属性	365
7.1.1	HFS 卷主目录块结构	318	7.10.2	域属性	366
7.1.2	HFS 卷主目录块实例分析	319			
7.2	概述	320			
7.2.1	HFS+的改进	320			
7.2.2	基本概念	321			

第 8 章 多磁盘卷	367
8.1 RAID	368
8.1.1 RAID 级别简介	368
8.1.2 RAID 中的基本概念	375
8.1.3 RAID0 阵列原理	376
8.1.4 RAID1 阵列原理	377
8.1.5 RAID4 阵列原理	377
8.1.6 RAID5 阵列原理	378
8.1.7 RAID6 阵列原理	382
8.1.8 RAID 1E 阵列原理	384

8.1.9 RAID DP 阵列原理	386
8.1.10 RAID 的实现	388
8.1.11 数据恢复及取证注意事项	389
8.2 磁盘跨区	391
8.2.1 概述	391
8.2.2 Linux MD	392
8.2.3 Linux LVM	394
8.2.4 Microsoft Windows LDM	395
8.2.5 总结	402

PART 2 实践篇

第 9 章 数据恢复前的准备	405
9.1 写在数据恢复之前的话	406
9.2 检测磁盘	408
9.2.1 用 MHDD 检测磁盘	408
9.2.2 用 MHDD 清除主引导扇区 “55AA” 标志	411
9.2.3 用 PC-3000 检测磁盘	412
9.3 坏道处理	415
9.4 镜像磁盘	417
9.4.1 什么是“镜像磁盘”	417
9.4.2 什么情况下需要对磁盘 进行镜像	418
9.4.3 用 Media Tools 镜像磁盘	419
9.4.4 用 HDClone 镜像磁盘	424
9.4.5 用 Winhex 镜像磁盘	427
9.5 分区及格式化对磁盘的写入	431
9.5.1 Winhex “比较” 功能的 使用	431
9.5.2 分区过程对磁盘的写入	434
9.5.3 格式化过程对磁盘的写入	440

第 10 章 基本数据恢复	447
10.1 分区恢复	448
10.1.1 主分区表损坏恢复	448
10.1.2 重新分区未格式化	459
10.1.3 分区布局改变并进行了 格式化	461
10.1.4 使用 FinalData 快速 寻找分区	462
10.2 DBR 损坏后的恢复	465
10.2.1 FAT 文件系统 DBR 损坏后 的恢复	465
10.2.2 NTFS 文件系统 DBR 损坏后 的恢复	473
10.3 格式化恢复	477
10.3.1 原 FAT32 格式化成 FAT32	477
10.3.2 原 FAT32 格式化成 NTFS ...	479
10.3.3 原 NTFS 格式化成 NTFS	480
10.3.4 原 NTFS 格式化成 FAT32 ...	480
10.4 删除恢复	481



10.4.1	FAT16 文件系统下的删除	481	11.4	RAID0 阵列恢复	513
10.4.2	FAT32 文件系统下的删除	483	11.4.1	参数分析	514
10.4.3	NTFS 文件系统下的删除	484	11.4.2	使用 Winhex 重组数据	515
10.5	数据恢复软件的使用	486	11.4.3	使用 R-Studio 恢复数据	518
10.5.1	使用 R-Studio 恢复数据	486	11.5	RAID5 阵列恢复	523
10.5.2	使用 Recover My Files 恢复数据	500	11.5.1	循环方向的判断	524
第 11 章	RAID 数据恢复	503	11.5.2	同步与异步的判断	525
11.1	概述	504	11.5.3	计算各个成员盘第一个校验块的位置	526
11.2	FAT 表在阵列恢复中的作用	504	11.5.4	利用 FAT 恢复演示	528
11.2.1	利用 FAT 表计算块大小	505	11.5.5	利用 MFT 恢复演示	532
11.2.2	利用 FAT 表判断数据块顺序	506	11.6	HP 内外双循环阵列恢复	537
11.2.3	利用 FAT 表寻找校验块	507	11.7	RAID 1E 阵列恢复	538
11.3	MFT 在阵列恢复中的作用	508	11.7.1	参数判断	539
11.3.1	利用 MFT 记录编号判断块大小及数据块顺序	508	11.7.2	数据恢复	539
11.3.2	利用 MFT 寻找校验块	510	附录 A	Win32 环境下磁盘操作五大函数	541
			附录 B	文件后缀名速查表	545

PART 1

理 论 篇

俗话说，“知己知彼，百战不殆”。同样，要恢复数据，就必须对操作对象有足够的了解。要恢复对于文件系统而言已经不存在的数据，就必须了解数据在某种文件系统下的管理方式，这样才能够根据它的工作原理进行分析并反向恢复已经丢失的数据。要解决因分区信息损坏导致的数据丢失问题，就必须熟知分区体系。而要恢复多磁盘卷上的数据，就必须了解多磁盘共同工作的原理及组合方式。而所有的这一切，都要求我们首先要具备最基本的条件：拥有计算机及存储介质基础知识。

本部分我们将首先介绍数据恢复所涉及的一些基础知识，然后详细介绍分区体系、文件系统及多磁盘卷。

- 基础知识
- 分区
- FAT 文件系统
- NTFS 文件系统
- ExtX 文件系统
- UFS 文件系统
- HFS+ 文件系统
- 多磁盘卷

