

# 数据恢复技术

# R 深度揭秘

# Recovery

( 第二版 )

Recovery

The Deep Secret on Data Recovery Vehicle

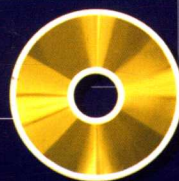
The Deep Secret

刘 伟 编著

Data Recovery

Vehicle

本书附赠光盘中含有作者讲授的案例分析教学视频，将多年经验无保留地分享给读者；  
作者编写的50个WinHex全中文模板，让WinHex应用变得直观、高效。



DVD-ROM



中国工信出版集团



电子工业出版社  
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY  
<http://www.phei.com.cn>

# 数据恢复技术深度揭秘

## (第二版)

刘 伟 编 著

電子工業出版社·

Publishing House of Electronics Industry

北京·BEIJING

## 内 容 简 介

《数据恢复技术深度揭秘》第二版是在第一版的基础之上增加和充实了服务器磁盘阵列(RAID)的恢复技术,新增了大量实战案例的分析和讲解,并精选书中的部分案例由作者制作成视频教学资料(DVD 光盘)随书附赠。

本书从逻辑类恢复和物理类恢复两个层面全面讲解当前最实用的数据恢复技术。

在逻辑类数据恢复方面,内容包括 MBR 磁盘分区、动态磁盘分区、GPT 磁盘分区、Solaris 分区、APM 分区、BSD 分区的恢复技术;Windows 平台的 FAT32、FAT16 文件系统、NTFS 文件系统、ExFAT 文件系统的恢复技术;UNIX 平台的 UFS1、UFS2 文件系统恢复技术;Apple 平台的 HFS+文件系统恢复技术;Linux 平台的 EXT3、EXT4 文件系统恢复技术;还包括 Windows、UNIX、Apple、Linux 平台的 RAID-0、RAID-1、RAID-1E、RAID-5、RAID-5EE、RAID-6、HP 双循环等磁盘阵列恢复技术。

在物理类数据恢复方面,内容包括各大品牌硬盘出现电路故障、磁头故障、电机故障、扇区读取故障、固件故障后数据恢复的方法,还包括优盘无法识别的恢复方法。

如果你是数据恢复技术的初学者,本书可以由浅入深,一步步将你引入数据恢复技术的神秘殿堂;如果你已经是数据恢复技术的高手,本书同样可以为你带来令你惊喜的经验 and 技巧。

未经许可,不得以任何方式复制或抄袭本书之部分或全部内容。

版权所有,侵权必究。

### 图书在版编目(CIP)数据

数据恢复技术深度揭秘 / 刘伟编著. —2 版. —北京:电子工业出版社,2016.10

ISBN 978-7-121-29927-8

I. ①数… II. ①刘… III. ①数据管理 IV. ①TP274

中国版本图书馆 CIP 数据核字(2016)第 222443 号

责任编辑:刘海艳

印 刷:北京京科印刷有限公司

装 订:三河市良远印务有限公司

出版发行:电子工业出版社

北京市海淀区万寿路 173 信箱 邮编 100036

开 本:787×1092 1/16 印张:64 字数:1679.4 千字

版 次:2016 年 10 月第 2 版

2010 年 5 月第 1 版

印 次:2016 年 10 月第 1 次印刷

印 数:3 000 册 定价:198.00 元(含 DVD 光盘 1 张)

凡所购买电子工业出版社图书有缺损问题,请向购买书店调换。若书店售缺,请与本社发行部联系,联系及邮购电话:(010) 88254888, 88258888。

质量投诉请发邮件至 zlts@phei.com.cn, 盗版侵权举报请发邮件至 dbqq@phei.com.cn。

本书咨询联系方式: lhy@phei.com.cn。

# 前言

## 写在再版之前

《数据恢复技术深度揭秘》是笔者在数据恢复领域从业及教学近十年经验积累基础之上的呕心之作，书籍出版后深受读者喜爱，是数据恢复技术的爱好者及从业者案头的必备参考书籍，从出版至今已经连续加印五次，好评如潮。

近几年笔者也收到了大量热心读者的来信，读者在表达读书感言和收获的同时，也希望能读到更多的实战案例，尤其是服务器磁盘阵列（RAID）方面的恢复案例，因为大多读者很难有机会实际接触到服务器磁盘阵列（RAID）的恢复。鉴于此，《数据恢复技术深度揭秘》借第二版改版的机会，在第一版的基础之上增加和充实了服务器磁盘阵列（RAID）的恢复技术及大量实战案例的分析和讲解，并精选书中的部分案例制作成视频教学资料（DVD 光盘）随书附赠，读者可以借助观看视频教学及阅读文字从多个角度全方位学习，更加有利于对数据恢复技术的掌握。

为了让读者通过一本书就能够比较系统、全面地了解数据恢复技术，笔者对本书的内容进行了最大限度的充实，但技术和知识是永无止境的，限于篇幅原因必须做出取舍，所以对于数据恢复的一些外延技术，如 Office 文档修复、数据库文档修复、磁盘录像机文件恢复、手机文件恢复等相关知识，本书虽未能涉及，只要读者通过对本书的认真学习，掌握了各种文件系统结构及数据结构的分析能力，对其他相关技能也就手到擒来了，因为学会了“渔”，还怕没有“鱼”吗？

## 噩梦般的经历，你是否有过

你是否有过这样的经历，多年积累和收藏的数据因为突然爆发的病毒而遭到破坏，文件丢失、打不开或者成为乱码？

你是否有过这样的经历，一不小心删除了重要文件，让你后悔莫及，损失惨重？

你是否有过这样的经历，因为一次重装操作系统，结果导致所有的数据分区从你眼前消失，整个硬盘中只剩下一个操作系统分区？

你是否有过这样的经历，昨天还在正常使用的计算机，今天早晨开机时突然检测不到硬盘，硬盘内所有的数据就这样无情地拒绝你的访问？

你是否有过这样的经历，想使用优盘中的文件，但优盘莫名其妙地打不开了，任你怎么着急，它自岿然不“开”。

你是否有过这样的经历，单位的服务器突然崩溃，核心数据全部丢失，导致工厂不能开工、企业无法正常运营，甚至面临倒闭的危险？

如果你有过以上这些噩梦般的经历，并想通过自己的努力找回丢失的数据；或者你还没有遇到以上问题，但对如何解决这些问题很有兴趣，那么，这本书是你最佳的选择，她将一步一步引领你实现自己成为数据恢复技术高手的心愿。

## 本书特点

本书从逻辑类恢复和物理类恢复两个层面对数据恢复技术进行全面讲解，讲解过程概念

清楚，逻辑性强，图文并茂，内容新颖，不仅涵盖面广，内容也达到了足够的深度。

本书力求用通俗易懂的语言、一目了然的图示演绎深奥的数据恢复技术理论，并用大量真实的案例帮助读者巩固和消化枯燥的理论，有利于读者理解和学习。

本书讲解的案例全部来自于笔者在北京信息科技大学数据恢复研究所工作期间的实际业务，绝不是通过程序模拟出来的，所以每一个案例都有血有肉，对数据恢复技术的爱好者来讲应该是弥足珍贵的。

### 主要内容

本书分为四篇进行讲解。

第一篇：数据恢复入门与进阶知识储备，包括第 1 章到第 3 章。这一篇讲述学习数据恢复技术必备的基础知识，主要包括计算机中数据的表示方法、字节序的含义、数据恢复技术中常用的逻辑运算和数据结构、硬盘的结构揭秘、常用数据恢复工具等。

第二篇：逻辑类数据恢复技术揭秘，包括第 4 章到第 7 章。这一篇主要讲解逻辑类数据恢复的方法，内容涵盖 Windows 系统、UNIX 系统、Linux 系统和 Apple 系统下的分区结构及文件系统结构。

第三篇：物理类数据恢复技术揭秘，包括第 8 章到第 14 章。这一篇主要讲解物理类数据恢复的方法，内容涵盖各大品牌硬盘出现电路故障、磁头故障、电机故障、扇区读取故障、固件故障后数据恢复的方法，还包括优盘无法识别的恢复方法。

第四篇：服务器数据恢复技术揭秘，包括第 15 章到第 20 章。这一篇主要讲解服务器磁盘阵列（RAID）数据恢复的方法，内容涵盖 Windows、UNIX、Apple、Linux 平台的 RAID-0、RAID-1、RAID-1E、RAID-5、RAID-5EE、RAID-6、HP 双循环等磁盘阵列恢复技术。

### 读者对象

如果你是数据恢复技术的初学者，本书可以由浅入深，一步步将你引入数据恢复技术的神秘殿堂；如果你已经是数据恢复技术的高手，本书同样可以为你带来令人惊喜的经验和技巧。

本书理论详细而充实，案例丰富而实用，是数据恢复技术从业者及爱好者、IT 系统服务人员、技术支持工程师、技术培训人员、数据恢复技术工程师、信息安全工作人员、系统管理人员、安全保密部门人员、电子证据调查分析人员、操作系统开发人员、存储技术相关人员的必备工具书，同时也可作为计算机相关专业在校大学生的课外补充教材。

### 致谢

感谢汪中夏、张宇、宋杨、戴森、赵建平、张悦等老师和朋友对本书的大力支持。

感谢我的父母、我的爱人，你们对我的爱和关怀是本书得以完成的保障。

参加本书编写的还有童勤强、李兰、陶军、颜廷芳、刘岩、陈洁、武月明、赵前勇、李海慧、袁亦书、张赛、朱宇鹏、王奇童、陈焕芹、胡杨、吴晓强、王现芳、李红艳、顾越等。

# 目 录

## 第一篇 数据恢复入门与进阶知识储备

|                               |    |
|-------------------------------|----|
| 第 1 章 计算机中数据的记录方法 .....       | 2  |
| 1.1 数据的表示方法 .....             | 2  |
| 1.1.1 计算机中数据的含义 .....         | 2  |
| 1.1.2 数值数据在计算机中的表示方法 .....    | 6  |
| 1.1.3 字符数据在计算机中的表示方法 .....    | 11 |
| 1.1.4 图形数据在计算机中的表示方法 .....    | 14 |
| 1.2 数据存储的字节序与位序 .....         | 14 |
| 1.2.1 Endian 的含义 .....        | 14 |
| 1.2.2 Little-endian 的含义 ..... | 15 |
| 1.2.3 Big-endian 的含义 .....    | 15 |
| 1.2.4 字节序与 CPU 架构的关系 .....    | 15 |
| 1.2.5 位序的含义 .....             | 17 |
| 1.3 数据的逻辑运算 .....             | 17 |
| 1.3.1 逻辑或 .....               | 17 |
| 1.3.2 逻辑与 .....               | 18 |
| 1.3.3 逻辑非 .....               | 18 |
| 1.3.4 逻辑异或 .....              | 18 |
| 1.4 数据恢复中常用的数据结构 .....        | 19 |
| 1.4.1 数据结构简介 .....            | 19 |
| 1.4.2 树 .....                 | 21 |
| 1.4.3 二叉树 .....               | 23 |
| 1.4.4 B 树、B-树、B+树和 B*树 .....  | 24 |
| 1.4.5 树的遍历 .....              | 27 |
| 第 2 章 现代硬盘结构揭秘 .....          | 29 |
| 2.1 机械硬盘的物理结构揭秘 .....         | 29 |
| 2.1.1 硬盘的外壳及盘标信息 .....        | 29 |
| 2.1.2 硬盘的电路结构 .....           | 32 |
| 2.1.3 硬盘的磁头定位驱动系统 .....       | 36 |
| 2.1.4 硬盘的主轴系统 .....           | 37 |
| 2.1.5 硬盘的数据控制系统 .....         | 37 |
| 2.1.6 硬盘的盘片 .....             | 38 |
| 2.1.7 硬盘的区段及物理 C/H/S .....    | 39 |
| 2.1.8 硬盘的接口技术 .....           | 40 |

|       |                               |    |
|-------|-------------------------------|----|
| 2.1.9 | 硬盘的主要性能指标                     | 47 |
| 2.2   | 机械硬盘的逻辑结构揭秘                   | 49 |
| 2.2.1 | 硬盘的逻辑磁道                       | 49 |
| 2.2.2 | 硬盘的逻辑扇区                       | 50 |
| 2.2.3 | 硬盘的逻辑柱面                       | 50 |
| 2.2.4 | 硬盘的逻辑磁头                       | 51 |
| 2.2.5 | 硬盘的逻辑 C/H/S                   | 51 |
| 2.2.6 | 硬盘的 28 位 LBA 及 48 位 LBA       | 51 |
| 2.3   | 固态硬盘结构揭秘                      | 52 |
| 2.3.1 | 固态硬盘的结构                       | 52 |
| 2.3.2 | 固态硬盘的优点                       | 54 |
| 2.3.3 | 固态硬盘的缺点                       | 55 |
| 第 3 章 | 数据恢复基本工具揭秘                    | 56 |
| 3.1   | 磁盘编辑器类工具                      | 56 |
| 3.1.1 | WinHex 使用方法详解                 | 56 |
| 3.1.2 | DiskExplorer for Fat 使用方法详解   | 72 |
| 3.1.3 | DiskExplorer for NTFS 使用方法详解  | 78 |
| 3.1.4 | DiskExplorer for Linux 使用方法详解 | 81 |
| 3.2   | 虚拟工具                          | 83 |
| 3.2.1 | 虚拟硬盘工具使用方法详解                  | 83 |
| 3.2.2 | 虚拟机使用方法详解                     | 86 |

## 第二篇 逻辑类数据恢复技术揭秘

|       |                      |     |
|-------|----------------------|-----|
| 第 4 章 | Windows 系统数据恢复技术     | 90  |
| 4.1   | Windows 系统的 MBR 磁盘分区 | 90  |
| 4.1.1 | 主引导记录 MBR 的结构和作用     | 90  |
| 4.1.2 | 主磁盘分区结构分析            | 95  |
| 4.1.3 | 扩展分区结构分析             | 100 |
| 4.1.4 | MBR 及 EBR 被破坏的分区恢复实例 | 106 |
| 4.1.5 | 分区误删除的恢复实例           | 117 |
| 4.1.6 | 系统误 Ghost 后的分区恢复实例   | 125 |
| 4.2   | Windows 系统的动态磁盘卷     | 129 |
| 4.2.1 | 动态磁盘概述               | 129 |
| 4.2.2 | 动态磁盘卷的种类及创建方法        | 130 |
| 4.2.3 | 动态磁盘 LDM 结构原理详解      | 132 |
| 4.2.4 | MBR 磁盘误转换为动态磁盘的恢复实例  | 155 |
| 4.2.5 | 动态磁盘扩展卷丢失的恢复实例       | 159 |
| 4.3   | Windows 系统的 GPT 磁盘分区 | 171 |
| 4.3.1 | GPT 磁盘分区基本介绍         | 171 |
| 4.3.2 | GPT 磁盘分区的创建方法        | 173 |

|        |                               |     |
|--------|-------------------------------|-----|
| 4.3.3  | GPT 磁盘分区结构原理                  | 177 |
| 4.3.4  | GPT 磁盘分区丢失的恢复实例               | 184 |
| 4.4    | FAT16 文件系统详解                  | 189 |
| 4.4.1  | FAT16 文件系统结构总览                | 189 |
| 4.4.2  | FAT16 文件系统的 DBR 分析            | 190 |
| 4.4.3  | FAT16 文件系统的 FAT 表分析           | 194 |
| 4.4.4  | FAT16 文件系统的 FDT 分析            | 197 |
| 4.4.5  | FAT16 文件系统目录项分析               | 198 |
| 4.4.6  | FAT16 文件系统根目录与子目录的管理          | 207 |
| 4.4.7  | FAT16 文件系统删除文件的分析             | 209 |
| 4.4.8  | FAT16 文件系统误格式化的分析             | 213 |
| 4.4.9  | FAT16 文件系统 DBR 手工重建的实例        | 215 |
| 4.5    | FAT32 文件系统详解                  | 218 |
| 4.5.1  | FAT32 文件系统结构总览                | 218 |
| 4.5.2  | FAT32 文件系统的 DBR 分析            | 219 |
| 4.5.3  | FAT32 文件系统的 FAT 表分析           | 223 |
| 4.5.4  | FAT32 文件系统的数据区分析              | 225 |
| 4.5.5  | FAT32 文件系统目录项分析               | 226 |
| 4.5.6  | FAT32 文件系统根目录与子目录的管理          | 230 |
| 4.5.7  | FAT32 文件系统删除文件的分析             | 235 |
| 4.5.8  | FAT32 文件系统删除文件后目录项起始簇号高位清零的分析 | 239 |
| 4.5.9  | FAT32 文件系统误格式化的分析             | 244 |
| 4.5.10 | FAT32 文件系统 DBR 破坏的恢复实例        | 247 |
| 4.5.11 | FAT32 分区文件乱码的手工恢复实例           | 248 |
| 4.5.12 | FAT32 分区被苹果电脑误格式化后的完美恢复实例     | 253 |
| 4.6    | NTFS 文件系统详解                   | 263 |
| 4.6.1  | NTFS 文件系统基本介绍                 | 263 |
| 4.6.2  | NTFS 文件系统结构总览                 | 264 |
| 4.6.3  | NTFS 文件系统引导扇区分析               | 266 |
| 4.6.4  | 元文件 \$MFT 分析                  | 270 |
| 4.6.5  | 文件记录分析                        | 272 |
| 4.6.6  | 10H 属性分析                      | 281 |
| 4.6.7  | 20H 属性分析                      | 282 |
| 4.6.8  | 30H 属性分析                      | 284 |
| 4.6.9  | 40H 属性分析                      | 287 |
| 4.6.10 | 50H 属性分析                      | 287 |
| 4.6.11 | 60H 属性分析                      | 292 |
| 4.6.12 | 70H 属性分析                      | 292 |
| 4.6.13 | 80H 属性分析                      | 294 |
| 4.6.14 | 90H 属性分析                      | 297 |
| 4.6.15 | A0H 属性分析                      | 299 |

|        |                        |     |
|--------|------------------------|-----|
| 4.6.16 | B0H 属性分析               | 299 |
| 4.6.17 | C0H 属性分析               | 300 |
| 4.6.18 | D0H 属性分析               | 301 |
| 4.6.19 | E0H 属性分析               | 302 |
| 4.6.20 | 100H 属性分析              | 302 |
| 4.6.21 | 元文件\$MFTMirr 分析        | 302 |
| 4.6.22 | 元文件\$LogFile 分析        | 304 |
| 4.6.23 | 元文件\$Volume 分析         | 313 |
| 4.6.24 | 元文件\$AttrDef 分析        | 315 |
| 4.6.25 | 元文件\$Root 分析           | 318 |
| 4.6.26 | 元文件\$Bitmap 分析         | 319 |
| 4.6.27 | 元文件\$Boot 分析           | 320 |
| 4.6.28 | 元文件\$BadClus 分析        | 321 |
| 4.6.29 | 元文件\$Secure 分析         | 322 |
| 4.6.30 | 元文件\$UpCase 分析         | 324 |
| 4.6.31 | 元文件\$Extend 分析         | 325 |
| 4.6.32 | 元文件\$ObjId 分析          | 326 |
| 4.6.33 | 元文件\$Quota 分析          | 327 |
| 4.6.34 | 元文件\$Reparse 分析        | 329 |
| 4.6.35 | 元文件\$UsnJrnl 分析        | 330 |
| 4.6.36 | NTFS 的索引结构分析           | 331 |
| 4.6.37 | 手工遍历 NTFS 的 B+树        | 335 |
| 4.6.38 | NTFS 的 EFS 加密分析        | 339 |
| 4.6.39 | NTFS 文件系统删除文件的分析       | 341 |
| 4.6.40 | NTFS 文件系统格式化的分析        | 347 |
| 4.6.41 | NTFS 文件系统 DBR 手工重建的实例  | 350 |
| 4.7    | ExFAT 文件系统详解           | 354 |
| 4.7.1  | ExFAT 文件系统基本介绍         | 354 |
| 4.7.2  | ExFAT 文件系统结构总览         | 356 |
| 4.7.3  | ExFAT 文件系统的 DBR 分析     | 357 |
| 4.7.4  | ExFAT 文件系统的 FAT 表分析    | 360 |
| 4.7.5  | ExFAT 文件系统的簇位图文件分析     | 361 |
| 4.7.6  | ExFAT 文件系统的大写字符文件分析    | 362 |
| 4.7.7  | ExFAT 文件系统的目录项分析       | 363 |
| 4.7.8  | ExFAT 文件系统根目录与子目录的管理   | 371 |
| 4.7.9  | ExFAT 文件系统删除文件的分析      | 376 |
| 4.7.10 | ExFAT 文件系统误格式化的分析      | 377 |
| 4.7.11 | ExFAT 文件系统 DBR 手工重建的实例 | 380 |
| 4.7.12 | 能够支持 ExFAT 文件系统的恢复工具   | 385 |
| 第 5 章  | UNIX 系统数据恢复技术          | 386 |
| 5.1    | UNIX 家族介绍              | 386 |

|        |                      |     |
|--------|----------------------|-----|
| 5.1.1  | UNIX 的起源及分裂          | 386 |
| 5.1.2  | UNIX 分类及特点           | 387 |
| 5.2    | UNIX 的分区详解           | 389 |
| 5.2.1  | Solaris 分区基本介绍       | 389 |
| 5.2.2  | Sparc Solaris 分区结构分析 | 391 |
| 5.2.3  | Sparc Solaris 分区恢复实例 | 396 |
| 5.2.4  | x86 Solaris 分区结构分析   | 399 |
| 5.2.5  | x86 Solaris 分区恢复实例   | 404 |
| 5.2.6  | Free BSD 分区结构分析      | 405 |
| 5.2.7  | Free BSD 分区恢复实例      | 410 |
| 5.2.8  | Open BSD 分区结构分析      | 413 |
| 5.3    | UFS1 及 UFS2 文件系统详解   | 417 |
| 5.3.1  | UFS 文件系统基本介绍         | 417 |
| 5.3.2  | UFS 文件系统结构总览         | 418 |
| 5.3.3  | UFS 文件系统的引导块分析       | 419 |
| 5.3.4  | UFS 文件系统的超级块分析       | 420 |
| 5.3.5  | UFS 文件系统的柱面组概要分析     | 435 |
| 5.3.6  | UFS 文件系统的柱面组描述符分析    | 437 |
| 5.3.7  | UFS 文件系统的位图分析        | 441 |
| 5.3.8  | UFS 文件系统的 i-节点分析     | 443 |
| 5.3.9  | UFS 文件系统的目录项分析       | 450 |
| 5.3.10 | UFS 文件删除与恢复的分析       | 454 |
| 5.3.11 | UFS 文件系统超级块的恢复实例     | 462 |
| 5.3.12 | UNIX 系统数据恢复专业工具详解    | 463 |
| 第 6 章  | Apple 系统数据恢复技术       | 466 |
| 6.1    | Apple 电脑介绍           | 466 |
| 6.1.1  | Apple 电脑的起源与发展       | 466 |
| 6.1.2  | Mac 操作系统的发展          | 467 |
| 6.2    | Apple 电脑的分区结构详解      | 468 |
| 6.2.1  | APM 分区结构分析           | 468 |
| 6.2.2  | APM 分区恢复实例           | 477 |
| 6.2.3  | GPT 分区结构分析           | 480 |
| 6.3    | HFS+文件系统详解           | 482 |
| 6.3.1  | HFS+文件系统基本介绍         | 482 |
| 6.3.2  | HFS+文件系统结构总览         | 484 |
| 6.3.3  | HFS+文件系统的卷头分析        | 485 |
| 6.3.4  | HFS+文件系统的头节点分析       | 491 |
| 6.3.5  | HFS+文件系统的位图节点分析      | 497 |
| 6.3.6  | HFS+文件系统的索引节点分析      | 498 |
| 6.3.7  | HFS+文件系统的叶节点分析       | 499 |
| 6.3.8  | HFS+文件系统节点的综合应用      | 500 |

|        |                           |     |
|--------|---------------------------|-----|
| 6.3.9  | HFS+文件系统的编录文件分析 .....     | 501 |
| 6.3.10 | HFS+文件系统的盘区溢出文件分析 .....   | 510 |
| 6.3.11 | HFS+文件系统的分配文件分析 .....     | 513 |
| 6.3.12 | HFS+文件系统的属性文件分析 .....     | 513 |
| 6.3.13 | HFS+文件系统的坏块文件分析 .....     | 515 |
| 6.3.14 | 手工遍历 HFS+的 B-树 .....      | 515 |
| 6.3.15 | HFS+文件删除与恢复的分析 .....      | 518 |
| 6.3.16 | HFS+文件系统卷头的恢复实例 .....     | 520 |
| 6.3.17 | Apple 系统数据恢复专业工具详解 .....  | 521 |
| 第 7 章  | Linux 系统数据恢复技术 .....      | 525 |
| 7.1    | Linux 系统介绍 .....          | 525 |
| 7.1.1  | Linux 系统的起源与发展 .....      | 525 |
| 7.1.2  | Linux 系统的分类及特点 .....      | 526 |
| 7.2    | Linux 系统的分区结构详解 .....     | 528 |
| 7.2.1  | MBR 磁盘分区结构分析 .....        | 528 |
| 7.2.2  | MBR 磁盘分区恢复实例 .....        | 531 |
| 7.2.3  | GPT 分区结构分析 .....          | 534 |
| 7.3    | Ext3 文件系统结构详解 .....       | 537 |
| 7.3.1  | Ext3 文件系统基本介绍 .....       | 537 |
| 7.3.2  | Ext3 文件系统结构总览 .....       | 538 |
| 7.3.3  | Ext3 文件系统的超级块分析 .....     | 539 |
| 7.3.4  | Ext3 文件系统的块组描述符分析 .....   | 545 |
| 7.3.5  | Ext3 文件系统的块位图分析 .....     | 547 |
| 7.3.6  | Ext3 文件系统的 i-节点位图分析 ..... | 548 |
| 7.3.7  | Ext3 文件系统的 i-节点分析 .....   | 550 |
| 7.3.8  | Ext3 文件系统的目录项分析 .....     | 556 |
| 7.3.9  | Ext3 文件删除与恢复的分析 .....     | 559 |
| 7.3.10 | Ext3 文件系统超级块的恢复实例 .....   | 570 |
| 7.3.11 | Linux 系统数据恢复专业工具详解 .....  | 572 |
| 7.4    | Ext4 文件系统分析 .....         | 575 |
| 7.4.1  | Ext4 文件系统介绍 .....         | 575 |
| 7.4.2  | Ext4 文件系统的特点 .....        | 576 |
| 7.4.3  | Ext4 文件系统的结构 .....        | 577 |
| 7.4.4  | Ext4 文件系统的向前与向后兼容 .....   | 579 |

第三篇 物理类数据恢复技术揭秘

|       |                        |     |
|-------|------------------------|-----|
| 第 8 章 | 硬盘物理故障的种类及判定 .....     | 582 |
| 8.1   | 硬盘外部物理故障的种类和判定方法 ..... | 582 |
| 8.1.1 | 电路板供电故障 .....          | 582 |
| 8.1.2 | 电路板接口故障 .....          | 584 |

|        |                                  |     |
|--------|----------------------------------|-----|
| 8.1.3  | 电路板缓存故障 .....                    | 584 |
| 8.1.4  | 电路板 BIOS 故障 .....                | 585 |
| 8.1.5  | 电路板电机驱动芯片故障 .....                | 585 |
| 8.2    | 硬盘内部物理故障的种类和判定方法 .....           | 586 |
| 8.2.1  | 磁头组件故障 .....                     | 586 |
| 8.2.2  | 主轴电机故障 .....                     | 587 |
| 8.2.3  | 盘片故障 .....                       | 588 |
| 8.2.4  | 固件故障 .....                       | 589 |
| 第 9 章  | 硬盘电路板故障数据恢复方法 .....              | 590 |
| 9.1    | 维修法 .....                        | 590 |
| 9.1.1  | 电路板常见故障及维修方法 .....               | 590 |
| 9.1.2  | 希捷硬盘电路板的故障及检测方法 .....            | 591 |
| 9.1.3  | 西部数据硬盘电路板的故障及检测方法 .....          | 592 |
| 9.2    | 替换法 .....                        | 592 |
| 9.2.1  | 替换法介绍 .....                      | 592 |
| 9.2.2  | 希捷 3.5 英寸硬盘电路板兼容性判定及替换方法 .....   | 593 |
| 9.2.3  | 希捷 2.5 英寸硬盘电路板兼容性判定及替换方法 .....   | 595 |
| 9.2.4  | 西部数据 3.5 英寸硬盘电路板兼容性判定及替换方法 ..... | 595 |
| 9.2.5  | 西部数据 2.5 英寸硬盘电路板兼容性判定及替换方法 ..... | 597 |
| 9.2.6  | 迈拓 3.5 英寸硬盘电路板兼容性判定及替换方法 .....   | 598 |
| 9.2.7  | 富士通 2.5 英寸硬盘电路板兼容性判定及替换方法 .....  | 599 |
| 9.2.8  | 三星 3.5 英寸硬盘电路板兼容性判定及替换方法 .....   | 600 |
| 9.2.9  | 三星 2.5 英寸硬盘电路板兼容性判定及替换方法 .....   | 601 |
| 9.2.10 | 日立 3.5 英寸硬盘电路板兼容性判定及替换方法 .....   | 602 |
| 9.2.11 | 日立 2.5 英寸硬盘电路板兼容性判定及替换方法 .....   | 602 |
| 9.2.12 | 日立 1.8 英寸硬盘电路板兼容性判定及替换方法 .....   | 604 |
| 9.2.13 | 东芝 2.5 英寸硬盘电路板兼容性判定及替换方法 .....   | 605 |
| 第 10 章 | 硬盘磁头组件故障数据恢复方法 .....             | 608 |
| 10.1   | 硬盘磁头组件故障的恢复思路 .....              | 608 |
| 10.1.1 | 开盘换磁头所需环境及工具 .....               | 608 |
| 10.1.2 | 开盘换磁头的操作步骤 .....                 | 610 |
| 10.2   | 希捷硬盘磁头兼容性判定及开盘方法 .....           | 611 |
| 10.2.1 | 3.5 英寸硬盘开盘实例 .....               | 611 |
| 10.2.2 | 2.5 英寸硬盘开盘实例 .....               | 615 |
| 10.3   | 西部数据硬盘磁头兼容性判定及开盘方法 .....         | 618 |
| 10.3.1 | 3.5 英寸硬盘开盘实例 .....               | 618 |
| 10.3.2 | 2.5 英寸硬盘开盘实例 .....               | 621 |
| 10.4   | 迈拓硬盘磁头兼容性判定及开盘方法 .....           | 623 |
| 10.5   | 富士通硬盘磁头兼容性判定及开盘方法 .....          | 625 |
| 10.6   | 三星硬盘磁头兼容性判定及开盘方法 .....           | 626 |
| 10.6.1 | 3.5 英寸硬盘开盘实例 .....               | 626 |

|        |                                        |     |
|--------|----------------------------------------|-----|
| 10.6.2 | 2.5 英寸硬盘开盘实例 .....                     | 627 |
| 10.7   | 日立硬盘磁头兼容性判定及开盘方法 .....                 | 629 |
| 10.7.1 | 3.5 英寸硬盘开盘实例 .....                     | 629 |
| 10.7.2 | 2.5 英寸硬盘开盘实例 .....                     | 631 |
| 10.8   | 东芝硬盘磁头兼容性判定及开盘方法 .....                 | 632 |
| 10.9   | 开盘成功后如何获得数据 .....                      | 634 |
| 10.9.1 | 物理镜像法 .....                            | 634 |
| 10.9.2 | 数据提取法 .....                            | 634 |
| 第 11 章 | 硬盘主轴电机故障数据恢复方法 .....                   | 635 |
| 11.1   | 主轴电机故障的恢复思路 .....                      | 635 |
| 11.1.1 | 处理主轴电机故障所需环境及工具 .....                  | 635 |
| 11.1.2 | 处理主轴电机故障的操作步骤 .....                    | 636 |
| 11.2   | 希捷 3.5 英寸硬盘主轴电机故障处理方法 .....            | 636 |
| 11.2.1 | 主轴电机兼容性判定 .....                        | 636 |
| 11.2.2 | 实例演示 .....                             | 637 |
| 11.3   | 迈拓 3.5 英寸硬盘主轴电机故障处理方法 .....            | 640 |
| 11.3.1 | 主轴电机兼容性判定 .....                        | 640 |
| 11.3.2 | 实例演示 .....                             | 641 |
| 11.4   | 东芝 2.5 英寸硬盘主轴电机故障处理方法 .....            | 643 |
| 11.4.1 | 主轴电机兼容性判定 .....                        | 643 |
| 11.4.2 | 实例演示 .....                             | 643 |
| 第 12 章 | 硬盘盘片故障数据恢复方法 .....                     | 646 |
| 12.1   | 盘片扇区故障的检测方法 .....                      | 646 |
| 12.2   | 盘片扇区故障的修复方法 .....                      | 649 |
| 12.2.1 | 重写校验法 .....                            | 649 |
| 12.2.2 | G-List 替换法 .....                       | 650 |
| 12.2.3 | P-List 隐藏法 .....                       | 650 |
| 12.3   | 盘片扇区故障的数据恢复方法 .....                    | 650 |
| 12.3.1 | 物理镜像法与数据提取法的区别与联系 .....                | 650 |
| 12.3.2 | 用 Media Tools Professional 做物理镜像 ..... | 651 |
| 12.3.3 | 用 HD Duplicator 做物理镜像 .....            | 655 |
| 12.3.4 | 用 PC-3000 UDMA DE 做物理镜像 .....          | 659 |
| 12.3.5 | 用 PC-3000 For SCSI 做物理镜像 .....         | 663 |
| 12.3.6 | 用 PC-3000 UDMA DE 提取数据 .....           | 667 |
| 12.3.7 | 用 PC-3000 UDMA DE 分磁头做物理镜像 .....       | 668 |
| 第 13 章 | 硬盘固件故障数据恢复方法 .....                     | 673 |
| 13.1   | 现代硬盘的固件结构 .....                        | 673 |
| 13.1.1 | 什么是硬盘的固件 .....                         | 673 |
| 13.1.2 | 硬盘固件的组成及作用 .....                       | 673 |
| 13.1.3 | 硬盘的生产流程 .....                          | 675 |
| 13.1.4 | 硬盘固件故障的表现 .....                        | 675 |

|        |                             |     |
|--------|-----------------------------|-----|
| 13.2   | 硬盘固件修复工具介绍                  | 676 |
| 13.2.1 | PC-3000 for DOS             | 676 |
| 13.2.2 | PC-3000 for Windows         | 677 |
| 13.2.3 | PC-3000 UDMA                | 678 |
| 13.2.4 | PC-3000 UDMA for SCSI       | 678 |
| 13.3   | 用 PC-3000 UDMA 修复迈拓硬盘的固件    | 679 |
| 13.3.1 | 识别迈拓硬盘的型号                   | 679 |
| 13.3.2 | 迈拓硬盘的固件结构                   | 681 |
| 13.3.3 | 迈拓硬盘 A 区、B 区和 C 区固件         | 684 |
| 13.3.4 | 备份固件                        | 685 |
| 13.3.5 | 检测固件                        | 687 |
| 13.3.6 | 修复固件                        | 689 |
| 13.4   | 用 PC-3000 UDMA 修复希捷硬盘的固件    | 689 |
| 13.4.1 | 识别希捷硬盘的型号                   | 689 |
| 13.4.2 | 希捷硬盘与 PC-3000 UDMA 的连接方法    | 691 |
| 13.4.3 | 希捷硬盘的固件结构                   | 692 |
| 13.4.4 | 希捷硬盘指令详解                    | 693 |
| 13.4.5 | 酷鱼 7200.11 “固件门”解决方案        | 694 |
| 13.4.6 | 酷鱼企业级硬盘 ES.2 “固件门”解决方案      | 699 |
| 第 14 章 | 优盘物理故障数据恢复方法                | 700 |
| 14.1   | 优盘物理故障的表现及分类                | 700 |
| 14.1.1 | 优盘物理故障的表现                   | 700 |
| 14.1.2 | 优盘物理故障的分类                   | 701 |
| 14.2   | 优盘物理故障的修复                   | 703 |
| 14.2.1 | 补焊                          | 703 |
| 14.2.2 | 替换晶振                        | 703 |
| 14.2.3 | 替换主控芯片                      | 703 |
| 14.2.4 | 替换闪存芯片                      | 704 |
| 14.3   | 用 PC-3000 Flash 直接提取闪存芯片的数据 | 705 |
| 14.3.1 | PC-3000 Flash 的工作原理         | 705 |
| 14.3.2 | 提取闪存芯片的数据                   | 706 |

## 第四篇 服务器数据恢复技术揭秘

|        |                |     |
|--------|----------------|-----|
| 第 15 章 | 服务器的 RAID 技术揭秘 | 711 |
| 15.1   | 什么是 RAID       | 711 |
| 15.1.1 | RAID 基础知识      | 711 |
| 15.1.2 | RAID 能解决什么问题   | 711 |
| 15.1.3 | RAID 级别简介      | 712 |
| 15.1.4 | 如何实现 RAID      | 712 |
| 15.1.5 | RAID 专业术语详解    | 718 |

|         |                           |     |
|---------|---------------------------|-----|
| 15.2    | RAID-0 技术详解               | 720 |
| 15.2.1  | RAID-0 数据组织原理             | 720 |
| 15.2.2  | RAID-0 故障原因分析             | 720 |
| 15.2.3  | RAID-0 数据恢复思路             | 721 |
| 15.3    | RAID-1 技术详解               | 722 |
| 15.3.1  | RAID-1 数据组织原理             | 722 |
| 15.3.2  | RAID-1 故障原因分析             | 723 |
| 15.3.3  | RAID-1 数据恢复思路             | 723 |
| 15.4    | RAID-10 技术详解              | 724 |
| 15.4.1  | RAID-10 数据组织原理            | 724 |
| 15.4.2  | RAID-10 故障原因分析            | 725 |
| 15.4.3  | RAID-10 数据恢复思路            | 725 |
| 15.5    | RAID-1E 技术详解              | 726 |
| 15.5.1  | RAID-1E 数据组织原理            | 726 |
| 15.5.2  | RAID-1E 故障原因分析            | 727 |
| 15.5.3  | RAID-1E 数据恢复思路            | 728 |
| 15.6    | RAID-2、RAID-3、RAID-4 技术详解 | 729 |
| 15.6.1  | RAID-2 数据组织原理             | 729 |
| 15.6.2  | RAID-3 数据组织原理             | 729 |
| 15.6.3  | RAID-4 数据组织原理             | 730 |
| 15.7    | RAID-5 技术详解               | 731 |
| 15.7.1  | RAID-5 数据组织原理             | 731 |
| 15.7.2  | RAID-5 的常规左异步结构           | 732 |
| 15.7.3  | RAID-5 的非常规左异步结构          | 733 |
| 15.7.4  | RAID-5 的常规左同步结构           | 733 |
| 15.7.5  | RAID-5 的非常规左同步结构          | 734 |
| 15.7.6  | RAID-5 的常规右异步结构           | 735 |
| 15.7.7  | RAID-5 的非常规右异步结构          | 735 |
| 15.7.8  | RAID-5 的常规右同步结构           | 736 |
| 15.7.9  | RAID-5 的非常规右同步结构          | 736 |
| 15.7.10 | RAID-5 故障原因分析             | 737 |
| 15.7.11 | RAID-5 数据恢复思路             | 738 |
| 15.8    | RAID-5E、RAID-5EE 技术详解     | 739 |
| 15.8.1  | RAID-5E 数据组织原理            | 739 |
| 15.8.2  | RAID-5EE 数据组织原理           | 740 |
| 15.8.3  | RAID-5EE 故障原因分析           | 740 |
| 15.8.4  | RAID-5EE 数据恢复思路           | 741 |
| 15.9    | HP 双循环技术详解                | 742 |
| 15.9.1  | HP 双循环数据组织原理              | 742 |
| 15.9.2  | HP 双循环故障原因分析              | 743 |
| 15.9.3  | HP 双循环数据恢复思路              | 744 |

|         |                          |     |
|---------|--------------------------|-----|
| 15.10   | RAID-6 技术详解              | 744 |
| 15.10.1 | P+Q 双校验 RAID-6 数据组织原理    | 744 |
| 15.10.2 | NetApp 双异或 RAID-6 数据组织原理 | 746 |
| 15.10.3 | X-Code 编码 RAID-6 数据组织原理  | 750 |
| 15.10.4 | ZZS 编码 RAID-6 数据组织原理     | 751 |
| 15.10.5 | Park 编码 RAID-6 数据组织原理    | 751 |
| 15.10.6 | RAID-6 故障原因分析            | 752 |
| 15.10.7 | RAID-6 数据恢复思路            | 753 |
| 15.11   | JBOD 技术详解                | 754 |
| 15.11.1 | JBOD 数据组织原理              | 754 |
| 15.11.2 | JBOD 故障原因分析              | 754 |
| 15.11.3 | JBOD 数据恢复思路              | 755 |
| 第 16 章  | 服务器数据恢复前的准备工作            | 757 |
| 16.1    | 服务器硬盘与数据恢复工作机的连接         | 757 |
| 16.1.1  | 将 RAID 中的成员盘去 RAID 化     | 757 |
| 16.1.2  | 服务器专用硬盘介绍                | 759 |
| 16.1.3  | 多块服务器硬盘与工作机的连接方法         | 759 |
| 16.2    | RAID 成员盘的物理故障检测          | 762 |
| 16.2.1  | 电路板故障                    | 762 |
| 16.2.2  | 磁头组件故障                   | 762 |
| 16.2.3  | 盘片划伤及缺陷扇区                | 762 |
| 16.2.4  | 固件出错                     | 762 |
| 16.3    | RAID 成员盘的镜像方法            | 762 |
| 16.3.1  | RAID 成员盘镜像的必要性           | 763 |
| 16.3.2  | RAID 成员盘没有坏扇区的镜像方法       | 763 |
| 16.3.3  | RAID 成员盘有坏扇区的镜像方法        | 766 |
| 16.4    | 判断 RAID 数据的新鲜度           | 766 |
| 16.4.1  | 判断 RAID 数据新鲜度的必要性及方法     | 766 |
| 16.4.2  | 挑出不新鲜的 RAID 成员盘          | 768 |
| 16.5    | RAID 数据恢复软件介绍            | 769 |
| 16.5.1  | WinHex                   | 769 |
| 16.5.2  | Raid Reconstructor       | 772 |
| 16.5.3  | R-studio                 | 775 |
| 16.5.4  | FileScav                 | 777 |
| 16.5.5  | UFS Explorer             | 779 |
| 16.5.6  | Getway Raid Recovery     | 781 |
| 第 17 章  | Windows 系统服务器数据恢复揭秘      | 783 |
| 17.1    | Windows 系统分区及文件系统知识的应用   | 783 |
| 17.1.1  | 分区结构在 RAID 分析中的作用        | 783 |
| 17.1.2  | \$BOOT 文件在 RAID 分析中的作用   | 787 |
| 17.1.3  | \$MFT 文件在 RAID 分析中的作用    | 790 |

|        |                                    |     |
|--------|------------------------------------|-----|
| 17.1.4 | 0x10 属性在 RAID 分析中的作用               | 791 |
| 17.1.5 | 0x30 属性在 RAID 分析中的作用               | 792 |
| 17.1.6 | 0x80 属性在 RAID 分析中的作用               | 793 |
| 17.2   | 基于 Windows 系统的 RAID 结构判断方法         | 793 |
| 17.2.1 | RAID 条带大小的判断                       | 793 |
| 17.2.2 | RAID 成员盘的盘序判断                      | 795 |
| 17.2.3 | RAID 校验方向的判断                       | 796 |
| 17.2.4 | RAID 数据同步与异步的判断                    | 798 |
| 17.3   | Windows 系统下各种 RAID 数据恢复实例分析        | 799 |
| 17.3.1 | 实例一: RAID-0 的实例分析                  | 800 |
| 17.3.2 | 实例二: RAID-1E 实例分析                  | 810 |
| 17.3.3 | 实例三: 左同步 RAID-5 实例分析               | 814 |
| 17.3.4 | 实例四: 右同步 RAID-5 实例分析 (每扇区 2048 字节) | 822 |
| 17.3.5 | 实例五: 成员盘前部有 RAID 信息的 RAID-5 实例分析   | 844 |
| 17.3.6 | 实例六: 成员盘中部有 RAID 信息的 RAID-5 实例分析   | 860 |
| 17.3.7 | 实例七: HP 双循环实例分析                    | 874 |
| 17.3.8 | 实例八: HP ADG RAID-6 实例分析            | 878 |
| 第 18 章 | Linux 系统服务器数据恢复揭秘                  | 885 |
| 18.1   | Linux 系统分区及文件系统知识的应用               | 885 |
| 18.1.1 | 分区结构在 RAID 分析中的作用                  | 885 |
| 18.1.2 | 超级块在 RAID 分析中的作用                   | 887 |
| 18.1.3 | 块组描述符在 RAID 分析中的作用                 | 889 |
| 18.1.4 | 位图在 RAID 分析中的作用                    | 890 |
| 18.1.5 | i-节点在 RAID 分析中的作用                  | 893 |
| 18.1.6 | 目录项在 RAID 分析中的作用                   | 895 |
| 18.2   | 基于 Linux 系统的 RAID 结构判断方法           | 895 |
| 18.2.1 | RAID 条带大小的判断                       | 896 |
| 18.2.2 | RAID 成员盘的盘序判断                      | 896 |
| 18.2.3 | RAID 校验方向的判断                       | 896 |
| 18.2.4 | RAID 数据同步与异步的判断                    | 897 |
| 18.3   | Linux 系统下 RAID 数据恢复实例分析            | 897 |
| 18.3.1 | 实例一: 有热备盘的 RAID-5 实例分析             | 897 |
| 18.3.2 | 实例二: 右异步 RAID-5 实例分析               | 912 |
| 第 19 章 | UNIX 系统服务器数据恢复揭秘                   | 926 |
| 19.1   | UNIX 系统分区及文件系统知识的应用                | 926 |
| 19.1.1 | 分区结构在 RAID 分析中的作用                  | 926 |
| 19.1.2 | 超级块在 RAID 分析中的作用                   | 927 |
| 19.1.3 | 柱面组描述符在 RAID 分析中的作用                | 928 |
| 19.1.4 | 位图在 RAID 分析中的作用                    | 929 |
| 19.1.5 | i-节点在 RAID 分析中的作用                  | 931 |
| 19.1.6 | 目录项在 RAID 分析中的作用                   | 933 |