Broadview
www.broadview.com.cn

安全技术大系

数据恢复技术

经典重现版

戴士剑 涂彦晖 编著
张喜平 审校

数据恢复与电子证据调查必备基础
最好的“恢复”永远是备份、备份、再备份

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

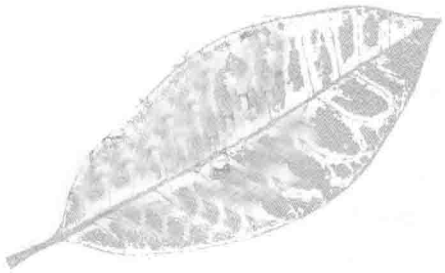
安全技术大系

数据恢复技术

经典重现版

戴士剑 涂彦晖 编著

张喜平 审校



電子工業出版社

Publishing House of Electronics Industry

北京•BEIJING

内 容 简 介

数据恢复技术是一门新兴技术，它通过各种手段把丢失和遭到破坏的数据还原为正常数据。本书通过多种典型实例详细介绍了 Windows 系统下数据恢复技术的原理和方法，内容包括硬盘数据组织、文件系统原理、数据恢复技术、文档修复技术、密码遗失处理技术、数据安全技术和数据备份技术。

本书作者戴士剑是知名数据恢复专家，有多年的数据恢复工作经验。本书是作者工作经验和技术理论的总结，适合 IT 系统客户服务人员、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、计算机取证人员、操作系统开发人员、存储技术相关人员、学生，以及任何对相关技术和工作感兴趣的读者，作为学习材料、参考资料或培训教材使用。

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：经典重现版 / 戴士剑，涂彦晖编著. —北京：电子工业出版社，2014.7
（安全技术大系）
ISBN 978-7-121-23537-5
Ⅰ. ①数… Ⅱ. ①戴… ②涂… Ⅲ. ①电子计算机—数据管理—安全技术 Ⅳ. ①TP309.3

中国版本图书馆 CIP 数据核字（2014）第 127695 号

责任编辑：徐津平
印　　刷：北京中新伟业印刷有限公司
装　　订：河北省三河市路通装订厂
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：43　　字数：1040 千字
版　　次：2003 年 5 月第 1 版
　　2014 年 7 月第 3 版
印　　次：2014 年 7 月第 1 次印刷
印　　数：4000 册
定　　价：99.00 元

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。

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。

服务热线：（010）88258888。

第 2 版序言

世界上没有完美无缺的人，同样也没有永远不出差错的计算机和软件系统。

在信息化时代的今天，无论是个人、公司、企业还是国家机关，都越来越依赖计算机系统。个人档案、文件、电子邮件、公司财务记录、销售合同，甚至国家军事机密等，无一不存储在计算机中。设想一下：如果现在你的计算机系统崩溃，硬盘故障，数据损失，将会出现什么样的情景？

1999 年 4 月 26 日，很多公司和个人就有过这样惨痛的体验。CIH 病毒的大爆发导致许多硬盘出现故障，无法正常启动，杀毒公司门口排起数百人的长队，大家神情焦灼，等候修复硬盘数据。

虽然现在 CIH 病毒不会再如此肆虐，但硬盘和软件系统出现故障导致数据丢失的意外事件并不少见。好在现在刻录光盘十分便捷，价格低廉，数据备份容易多了，所以养成良好的数据备份习惯是十分必要的。但是，意外是无处不在的，即使你做了周全的准备工作，也可能会遇到突然的致命一击。大部分的计算机用户，甚至包括软件技术高手，都不可能做到时刻备份数据资料。因此，一旦遇到突如其来的系统故障和数据损失，如何进行数据恢复，就成了至关重要的问题。然而，对于大部分用户而言，出现数据丢失的情况以后，他们并不知道应该如何处理，往往心急如焚，不知所措。

其实，数据恢复虽然不是件简单的事情，但也不是高不可攀的技术。

只要了解操作系统的文件系统结构的基本原理，掌握一些重要工具的使用，加上细心和耐心，就可以解决绝大部分的数据丢失问题。

大家都知道，Norton 是很有名的工具软件，其实早期 Norton 的成名和数据恢复紧密相关。远在 DOS 时代，还是一个业余计算机爱好者的 Peter Norton 发现，在 MS-DOS 系统中删除文件后，并没有在磁盘上直接删除文件的数据，而只是在文件的目录上做了个“E5”的删除标志，于是就写了个恢复删除文件的工具，受到广大用户的热烈欢迎。后来逐渐发展起来的 Norton Utility，更是傲视群雄，其中的 Disk Doctor 和 DiskEdit 是修复硬盘数据的必备工具。即使到今天，Windows 系统中的硬盘诊断和整理工具的技术还是从 Norton 买过来的。正是从一个小小的数据恢复工具软件开始，Norton 逐渐发展成了著名的工具软件和安全软件品牌。

市面上很少见到讲述数据恢复技术的书籍，而其实它是非常有用的，很多人甚至仅仅依靠这个技术就足以安身立命。例如，早些年，有的用户计算机硬盘出了问题，不能启动，只得花钱找专门的公司去修复。而实际上，大部分所谓的维修，只不过是用 Disk Doctor 扫描一下硬盘，标出坏磁道，就把系统数据恢复了。可见这项技术的实用性。

到了 Windows 2000/XP 时代，文件系统从 FAT16 升级到 FAT32/NTFS，数据恢复技术有了进一步的发展，文件系统结构比以前复杂了，但幸运的是也有了许多更强大的工具，如 ERD

Commander。

同时，我们也有了更充实的技术指导资料。这本《数据恢复技术》，就是当前技术图书市场上非常出色的一本数据恢复技术书籍。

本书全面详尽地讲述了数据恢复的原理和技术，共分 3 篇。

在第 1 篇中，作者详细讲解了 Windows 系统的文件系统原理。作为全书的理论基础，这是十分必要的，特别是当你动手去恢复硬盘文件、诊断故障和修复数据时，有时候要像医生做手术那样小心谨慎。你一定要十分明白你在做什么，否则可能出现灾难性的后果。

第 2 篇是关于数据恢复技术和工具的讲解，内容十分丰富，除了关于硬盘故障修复的详细讲解以外，还介绍了数据文件出错（在网络时代，这种情况经常发生）、密码丢失等状况的处理，对于数据文件的保护和备份也做了全面的介绍。这些方法和工具都是十分实用的，善用这些工具，将大大提高你的数据安全系数。

第 3 篇是实例性的讲解。作者精心挑选了最有代表意义的数据故障，做了分步骤的详细说明。这些都是在计算机使用中发生的案例，很有实际的指导意义。

这是一本非常实用、全面的工具书，保护数据对于每个计算机用户都是十分重要的，无论你是初级用户，还是软件高手，都能从中获益。因此，我乐于为此书作序，希望它能帮助读者保护自己的每一个字节。

CSDN 创始人 蒋涛

此为试读，需要完整PDF请访问：www.ertongbook.com

再版前言

《数据恢复技术》第1版出版于2003年5月，第2版出版于2005年3月，至今已经过去11年和9年，最后一次重印是2008年6月，两版的总销量达4万余册，为社会培养了一大批从事数据恢复、智能仪器设备消费品开发、计算机法庭科学等方面的优秀人才。虽然经过这么多年，等级保护、灾难备份等应用已深入人心，但从来就没有万无一失的系统，包括数据恢复技术本身，也无法解决所有问题，它虽然可以作为“后悔药”来使用，但却不是每次都有效，因此它只是一种补救措施——最好的“恢复”，永远是备份、备份、再备份。

但是，数据恢复技术自有其不可替代的应用领域，除了情报获取、失泄密调查、数据销毁、数据挽救等传统应用外，作为重要的证据调查技术，它更是具有基础性的地位。顺应信息时代的实际需求，我国《刑事诉讼法》和《民事诉讼法》均做了修订，“电子数据”作为证据已经被人们所认识和接纳。

我们无时无刻不处于电磁环境的笼罩之下，信息世界与物理世界一起，共同构成我们所处的真实世界，信息世界本身就是真实世界的一个重要组成部分，在工作过程中会自动记录各种各样的信息，这些信息有着丰富多彩的表现形式，存在于形形色色的网络和设备中，如监控网、通信网、游戏网、即时聊天系统、IC卡、互联网、广播电视网、有线电视电话网、雷达网、全球定位系统、证券交易系统、期货交易系统、各类管理及办公系统等。而随着三网融合与物联网的发展，这些信息网络在我们的日常生活中将发挥着越来越重要的作用，人们在这些网络中的活动都必然留下相应的“痕迹”，这些痕迹，通常不仅表结果，还表过程，其信息量巨大，最容易实现过程重建。因此，我们在勘验犯罪现场时，除了传统模式的勘验物理世界痕迹外，还必须勘验相应的信息世界，从信息世界得到物理世界所得不到的内容，共同重建犯罪现场与犯罪过程。

国内外都有许多利用这种电子数据痕迹破案的经典案例，并且通过这些网络，可以获取大量的背景信息，包括个人社会文化知识背景、兴趣爱好、生活消费习惯、朋友圈等。电子数据在司法实践中起着越来越重要的作用，如利用信息对嫌疑人进行画像，对其性格特征、作案手法、心理活动进行分析，对犯罪过程进行重建等。

从以上应用也可以看出，信息系统在实际案件办理过程中，往往既不是纯粹的线索，也不是纯粹的证据，我个人给它的定位是“沉默的‘现场知情人’”，它自己不会诉说，需要通过相应的技术手段将它们展现出来，这正是计算机法庭科学的研究领域。

计算机法庭科学研究信息技术在司法活动中的应用，包括线索发现、证据调查（《电子证据调查指南》将由中国检察出版社出版）、证据分析与鉴定、法庭示证等方面的问题，而证据分析与鉴定直接与数据管理相关。例如，通常的以单机为对象的电子证据的鉴定范围主要包括如下部分。

（一）电子证据数据内容一致性的认定。

（二）对各类存储介质或设备存储数据内容的认定。

（三）对各类存储介质或设备已删除数据内容的认定。

（四）加密文件数据内容的认定。

（五）计算机程序功能或系统状况的认定。

（六）电子证据的真伪及形成过程的认定。

（七）根据诉讼需要进行的关于电子证据的其他认定。

显然，磁盘数据分析在这个鉴定过程中占据着重要的地位，而磁盘分析，正是建立在操作系统、文件系统、文档格式、计算机编程、加解密等技术基础之上。本书的主要内容，就是文件系统原理，最早设定的书名就是《文件系统原理与数据恢复技术》，后因书名太长而进行了取舍。

本书停止重印后，经常遇到好学之人需要参考该书而无处可得，原计划后续出版《文档格式与碎片处理技术》，却因我工作变动，从军队研究机构，到大学（只做了两三个月老师，为中国人民大学信息学院设置了“计算机取证”方向的研究生，目前仍在招生），再到最高人民检察院，专门从事电子证据调查与分析工作。结合当前司法改革实际，和电子工业出版社聊到该书的重印问题，没想到与郭立女士一拍即合，也讨论了多个方案，最后还是决定重印，原因是多方面的，最主要的原因是给这本书的定位：经典重现——数据恢复与电子证据调查必备基础。其他内容，如 GPT、exFAT、Ext2、Ext3、UFS 等，在学好本书的基础上，都不是什么难题。毕竟现在与我当年分析这些系统时的环境不一样了，有太多的信息渠道可以提高分析效率，但如果不能将数据库碎片恢复技术、文档碎片重组技术写进来就出版第 3 版，我自己都是无法接受的。

这本书非常适合自学，读者在学习时，只要多进行对照分析，就一定能掌握其索引规则，从而达到举一反三的效果。

废话不再说，以下内容是直接保留下来的。

本书特点

本书饱含我多年心血之精华，是我在多年数据恢复工作经验的基础上，进一步完善技术资料，总结恢复经验写成的，主要有以下特点。

- **由浅入深，精简有序**。是什么原因让读者觉得数据恢复技术神秘而深不可测？是什么挡住了读者的探索之路？本书基于多年的数据恢复工作经验和对数据恢复技术的深刻理解，用最贴近读者需求的方式阐述了数据恢复技术需要了解和掌握的关键内容。
- **结构合理，脉络清晰**。本书首先对文件系统原理进行剖析，然后在此基础上剖析数据恢复技术并通过实例精讲数据恢复操作，使没有任何数据恢复基础的读者都能迅速掌握文件系统原理和数据恢复技术。不同技术基础的读者，可以选择从不同的章节切入，以最快的速度掌握所需的技术。
- **操作性强，容易掌握**。由于数据恢复技术是一门理论和实践结合很强的技术，掌握起来有一定难度，单纯从理论上介绍会使人感到乏味，因此，本书结合实例对原理和操作技术进行介绍，使之可操作性强，且易于掌握。

主要内容

本书共分为 3 篇。第 1 篇是文件系统原理篇（包括第 1 章～第 4 章），详细讲解了硬盘数据组织管理和文件系统原理等基础知识；第 2 篇是数据恢复技术篇（包括第 5 章～第 9 章），是本书的中心内容，详细介绍了当前典型的数据恢复技术、坏磁道处理技术、文档修复技术、密码遗失处理技术、数据安全与备份技术，以及光盘、软盘、数码存储设备的数据恢复技术，基本涵盖了数据恢复技术的各个方面；第 3 篇为数据恢复典型实例篇（包括第 10 章），通过实例对各种典型数据丢失情况的处理操作进行了介绍，特别是其中的操作注意事项和心得体会，是多年的经验总结。

读者对象

本书适合 IT 系统客户服务人员、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、学生及任何对此感兴趣的朋友作为参考资料或培训教材使用。

感谢

本书由戴士剑、涂彦晖统筹，由罗松、赵强、李祥芬、郭久武、李毅、贾永军、杨婕、张宇、杨霖、陈永红、戴士礼、柳红梅、代仕林、陈向东、段秀英、刘秀明、陈福寿、刘金玲分工负责完成各章节的编写工作，由张喜平博士审校定稿。

在本书的写作过程中，得到了我的亲人和朋友的大力支持和帮助，特别是得到了数据恢复网所有网友的支持和鼓励，在此表示最真挚的谢意，并祝福所有的亲人和朋友一生平安。

结束语

硬盘有价，数据无价。愿所有的朋友都能从数据丢失和损坏的“噩梦”中走出来，从此不再有数据丢失、损坏的烦恼！

电子证据调查，不怕不承认，不怕删除和破坏，只怕压根儿不使用！

戴士剑

2014 年 3 月

電子工業出版社 PUBLISHING HOUSE OF ELECTRONICS INDUSTRY http://www.phei.com.cn
Broadview WWW.BROADVIEW.COM.CN
博文视点 · IT出版旗舰品牌

十载耕耘奠定专业地位

博文视点诚邀精锐作者加盟

以书为证彰显卓越品质

《C++Primer（中文版）（第5版）》、《淘宝技术这十年》、《代码大全》、《Windows内核情景分析》、《加密与解密》、《编程之美》、《VC++深入详解》、《SEO实战密码》、《PPT演义》……

“圣经”级图书光耀夺目，被无数读者朋友奉为案头手册传世经典。

潘爱民、毛德操、张亚勤、张宏江、咎辉Zac、李刚、曹江华……

“明星”级作者济济一堂，他们的名字熠熠生辉，与IT业的蓬勃发展紧密相连。

十年的开拓、探索和励精图治，成就**博**古通今、**文**圆质方、**视**角独特、**点**石成金之计算机图书的风向标杆：博文视点。

“凤翱翔于千仞兮，非梧不栖”，博文视点欢迎更多才华横溢、锐意创新的作者朋友加盟，与大师并列于IT专业出版之巅。

英雄帖

江湖风云起，代有才人出。
IT界群雄并起，逐鹿中原。
博文视点诚邀天下技术英豪加入，
指点江山，激扬文字
传播信息技术，分享IT心得

• 专业的作者服务 •

博文视点自成立以来一直专注于 IT 专业技术图书的出版，拥有丰富的与技术图书作者合作的经验，并参照 IT 技术图书的特点，打造了一支高效运转、富有服务意识的编辑出版团队。我们始终坚持：

善待作者——我们会把出版流程整理得清晰简明，为作者提供优厚的稿酬服务，解除作者的顾虑，安心写作，展现出最好的作品。

尊重作者——我们尊重每一位作者的技术实力和生活习惯，并会参照作者实际的工作、生活节奏，量身制定写作计划，确保合作顺利进行。

提升作者——我们打造精品图书，更要打造知名作者。博文视点致力于通过图书提升作者的个人品牌和技术影响力，为作者的事业开拓带来更多的机会。

联系我们

博文视点官网：http://www.broadview.com.cn　　CSDN官方博客：http://blog.csdn.net/broadview2006/

投稿电话：010-51260888　88254368　　投稿邮箱：jsj@phei.com.cn

新浪微博 weibo.com　@博文视点Broadview

微信公众账号　博文视点Broadview

反侵权盗版声明

电子工业出版社依法对本作品享有专有出版权。任何未经权利人书面许可，复制、销售或通过信息网络传播本作品的行为；歪曲、篡改、剽窃本作品的行为，均违反《中华人民共和国著作权法》，其行为人应承担相应的民事责任和行政责任，构成犯罪的，将被依法追究刑事责任。

为了维护市场秩序，保护权利人的合法权益，我社将依法查处和打击侵权盗版的单位和个人。欢迎社会各界人士积极举报侵权盗版行为，本社将奖励举报有功人员，并保证举报人的信息不被泄露。

举报电话：（010）88254396；（010）88258888

传　　真：（010）88254397

E－mail：dbqq@phei.com.cn

通信地址：北京市万寿路 173 信箱　电子工业出版社总编办公室

邮　　编：100036

目　　录

第 1 篇　文件系统原理

此为试读，需要完整PDF请访问：www.ertongbook.com

第 2 篇 数据恢复技术详解

第 3 篇 数据恢复典型实例

第 1 篇

文件系统原理

本篇包括 4 章：第 1 章为综述，介绍一些基本知识和基本概念；第 2 章介绍硬盘的物理结构和数据的逻辑结构；第 3 章重点分析 Windows 95/98/Me 操作系统下的文件系统管理技术；第 4 章重点分析 Windows NT/2000/XP/2003 操作系统下的文件系统管理技术。

本篇内容是数据恢复技术的基础知识，是作者在多年数据恢复工作的基础上，进一步充实技术资料而完成的，其中很多资料无法通过一般的途径收集，把它们汇集在一起，既方便查阅和使用，又可以作为资料收藏。特别要指出的是，要想掌握一门技术，“知其然，不知其所以然”是远远不够的，只有掌握数据恢复技术的原理，才能真正成为一名数据恢复技术工程师。如果读者有一定的计算机基础，也可以跳过本篇内容，直接进入下一篇。

第 1 章　综述

本章主要讲述数据存储技术方面的基础知识和数据恢复技术的基本概念、内涵和类别，从而使读者在总体上对数据恢复知识有一个全面的了解。

1.1　数据存储技术总论

信息时代的核心无疑是信息技术，而信息技术的核心则在于信息的处理与存储。随着数据量的剧增，数据存储技术已经面临着巨大的挑战。当我们每天关注 CPU 主频的不断提高、操作系统版本的不断升级和计算机网络技术的日新月异的时候，或许不应该忽略这样的事实——无论信息处理技术多么先进，我们都必须将信息存储于一定的介质之上，信息和信息技术本身都需要依托一定的存储介质而存在。

近年来，计算机在商业和个人方面的应用得到了显著的增长，现在几乎每一间办公室都拥有计算机，许多家庭都已经拥有计算机，大多数的公司都建立了计算机网络来共享应用程序和数据。所有这些变化使数据字节取代了纸张，提高了生产力和生产效率，减小了冗余，并增强了信息的可用性。

由于越来越多的信息变成了电子信息，这就使信息存储技术显得更加重要，特别是计算机网络应用的迅速增长，更大大增加了对信息存储产品的需求量和对信息存储技术的安全性、可靠性的要求。根据 3M 公司对 800 名网络计算机用户的调查发现，每次硬盘的失效将造成 5 个以上的无效工作日。而在一个典型的商业应用中，重建 1 000MB 数据平均要耗时 3.5 个月，费用为 95 000 美元。由此可见，信息存储的安全对最终用户来说是何等的重要。

1.1.1　数据存储介质

凡是仅有两种稳定的物理状态，能方便地检测出属于哪种稳定状态，两种稳定状态又容易相互转换的物质或元器件，都可以用来存储二进制代码“0”和“1”，这样的物质或元器件称为存储介质或记录介质。存储介质不同，存储信息的机理也不同。

信息存储技术在近几年的发展非常迅速，各种新产品、新技术层出不穷，但从总体上看，呈现出一种类似金字塔的结构，其中塔尖为 CPU，距离 CPU 越近则存储速度越快，每兆字节的存储成本越昂贵，容量也越小；反之，存储速度越慢，每兆字节的存储成本越低，容量也越大。

计算机的存储设备从体系结构上看可分为内存储器和外存储器。

内存储器（即内存）直接与计算机的 CPU 相连，处于金字塔的最上层。内存的存取速度要

此为试读，需要完整PDF请访问：www.ertongbook.com