

<<数据重现>>

图书基本信息

书名：<<数据重现>>

13位ISBN编号：9787302198932

10位ISBN编号：7302198934

出版时间：2009-4

出版时间：清华大学出版社

作者：马林

页数：562

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

<<数据重现>>

前言

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，这就要求我们必须能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最后一道防线。

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

<<数据重现>>

内容概要

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

为畅销书《大话存储》姊妹篇。

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、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。

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RAID0、RAID5、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。

<<数据重现>>

作者简介

马林，天津市电子技术研究所专业数据存储安全与数据灾难拯救研究员，首席数据恢复专家，天亚数据恢复技术总监。

多年来致力于数据存储与文件系统的研究，时刻跟踪数据恢复技术的发展方向。受天津市国家保密局指定，为党政机关、科研院所等机构提供专业涉密数据恢复保障。同时，还将研究成果应用于民用数据恢复领域，并在实际工作中积累和总结了大量的实践经验。

现就职公司为天津市保密局唯一指定官方涉密数据恢复单位。

<<数据重现>>

书籍目录

PART 1 理论篇	第1章 数据恢复相关基础	1.1 硬盘探秘	1.1.1 硬盘结构	1.1.2 硬盘接口
	1.1.3 磁道、扇区与柱面寻址方式	1.1.4 硬盘的启动过程	1.1.5 硬盘的性能指标	1.1.6 硬盘的启动过程
	1.2 计算机运行流程	1.2.1 基本概念	1.2.2 计算机的启动过程	1.3 “数
	1.3.1 数制	1.3.2 数制间的转换	1.3.3 取整与取余运算	1.3.4 数的存储
	1.4 工具软件	1.4.1 虚拟磁盘软件InsPro Disk	1.4.2 十六进制编辑软件Winhex	
	1.4.3 硬盘检测软件MHDD	第2章 分区	2.1 概述	2.1.1 分区与卷
	2.1.3 扇区地址	2.1.4 根据合理性判断分区信息的正确性	2.1.5 数据恢复及电	2.2.3 扩展引导记录
	2.2 DOS分区	2.2.1 概述	2.2.2 主引导记录扇区MBR	2.3 Apple分区
	2.2.4 数据恢复及电子取证	2.3 Apple分区	2.3.1 概述	2.3.2 Apple磁盘
	2.3.3 分区表项数据结构	2.3.4 数据恢复与电子取证	2.4 BSD分区	2.4.1 BSD
	2.4.2 Free BSD分区	2.4.3 NetBSD与OpenBSD	分区	2.4.4 磁盘标签数据结
	2.4.5 磁盘标签实例分析	2.4.6 总结	2.5 Sun Solaris分区	2.5.1 概述
	Sparc平台下的Sun Solaris分区	2.5.3 i386平台下的Sun Solaris分区	2.5.4 总结	2.6 GPT分区
	2.6.1 概述	2.6.2 GPT磁盘总体布局	2.6.3 数据结构	2.6.4 总结
	2.6.5 移动介	第3章 FAT文件系统	3.1 文件系统总论	3.2 FAT文件系统概述
	3.1 文件系统总论	3.2 FAT文件系统概述	3.3 FAT文件系	3.4 FAT32的保留区
	3.4 FAT32的保留区	3.4.1 引导扇区	3.4.2 引导代码	3.4.3 FSINFO信息
	3.5 FAT32的FAT表	3.5.1 FAT表概述	3.5.2 FAT表的特性	3.5.3 FAT表的使
	3.5.4 其他	3.6 FAT32的数据区	3.6.1 根目录	3.6.2 子目录
	3.7 FAT12/16文件系统	3.7.1 FAT12/16文件系统概述	3.7.2 引导扇区	3.7.3 FAT表
	3.7.4 根目录与目录项	3.8 分配策略	3.8.1 簇的分配策略	3.8.2 目录项的分配策略
	3.9 文件的建立与删除	3.10 总结	3.10.1 数据恢复分析	3.10.2 取证分析
	NTFS文件系统	4.1 NTFS概述	4.1.1 概述	4.1.2 基本概念
	4.3 引导扇区	4.4 主文件表MFT	4.4.1 基本概念	4.4.2 Windows 2000的MFT项
	4.4.3 Windows XP的MFT项	4.5 MFT属性	4.5.1 属性的结构	4.5.2 常规属性类型
	4.5.3 其他属性	4.6 文件系统元文件	4.6.1 \$MFT文件	4.6.2 \$MFTMirr文件
	4.6.3 \$LogFile文件	4.6.4 \$Volume文件	4.6.5 \$AttrDef文件	4.6.6 \$Root文件
	4.6.7 \$Bitmap文件	4.6.8 \$Boot文件	4.6.9 \$Secure文件	4.6.10 \$UsnJrnl文件
	4.6.11 \$Quota文件	4.6.12 \$ObjId文件	4.7 分配策略	4.7.1 簇空间分配策略
	MFT项分配策略	4.7.3 属性分配策略	4.8 时间值的更新	4.9 文件的建立与删除
	4.9.2 删除文件	4.10 总结	4.10.1 分析注意事项	4.10.2 数据恢复与取
	分析	第5章 ExtX文件系统	5.1 ExtX文件系统概述	5.2 ExtX文件系统整体布局
	5.3.1 超级块数据结构	5.3.2 超级块实例分析	5.4 块组描述符表和块组描述符	5.3 超级块
	5.4.1 块组描述符数据结构	5.4.2 块组描述符实例分析	5.5 块位图	5.5.1 块位图的工作
	5.5.2 块位图实例分析	5.6 i-节点位图	5.6.1 i-节点位图实例	5.6.2 定位一个
	5.7 i-节点表与i-节点	5.7.1 i-节点数据结构	5.7.2 i-节点实例分析	
	5.7.3 i-节点的属性	5.7.4 i-节点中时间值的更新	5.8 扩展属性	5.8.1 扩展属性的结构
	5.8.2 扩展属性实例分析	5.9 目录项	5.9.1 目录项数据结构	5.9.2 目录项的特性
	5.9.3 目录项实例分析	5.10 链接和挂载点	5.10.1 链接	5.10.2 挂载点
	5.11.1 Hash树数据结构	5.11.2 Hash树实例分析	5.12 文件系统日志	5.12.1 数
	5.12.2 日志实例分析	5.13 分配策略	5.13.1 块的分配策略	5.13.2 i-节点分
	5.13.3 文件名空间分配策略	5.14 文件的建立与删除	5.14.1 建立文件	5.14
	删除文件	5.15 总结	5.15.1 分析注意事项	5.15.2 数据恢复与电子取证
	文件系统	6.1 概述	6.2 UFS文件系统整体布局	6.3 超级块
	结构	6.4 柱面组摘要	6.5 柱面组描述符	6.5.1 概述
	6.6 引导代码	6.7 i-节点	6.7.1 UFS1的i-节点	6.7.2 UFS2的i-节点
				6.8 目录项

<<数据重现>>

6.8.1 数据结构	6.8.2 实例分析	6.9 分配策略	6.9.1 存储空间分配策略	6.9.2
节点分配策略	6.9.3 目录项分配策略	6.10 文件的建立与删除	6.10.1 建立文件	第7章
6.10.2 删除文件	6.11 总结	6.11.1 分析注意事项	6.11.2 数据恢复与取证分析	第7章
HFS+文件系统	7.1 HFS封装	7.1.1 HFS卷主目录块结构	7.1.2 HFS卷主目录块实例分析	7.2
7.2 概述	7.2.1 HFS+的改进	7.2.2 基本概念	7.2.3 主要数据结构类型	7.2
HFS+特性	7.3 HFS+文件系统整体布局	7.4 卷头	7.4.1 数据结构	7.4.2 实例分析
7.5 节点	7.5.1 节点的种类	7.5.2 节点的基本结构	7.5.3 头节点	7.5.4 图节点
7.5.5 索引节点	7.5.6 叶节点	7.5.7 节点的使用	7.5.8 HFS+节点与HFS节点的区	7.5.9
7.6 目录文件	7.6.1 目录文件中档案项的key部分	7.6.2 目录文件中档案项的数据部	7.7 域溢出文件	7.7.1 域溢出文件中档案项的key部分
7.7 域溢出文件	7.7.1 域溢出文件中档案项的key部分	7.7.2 域溢出文件中档案项	7.7.3 域溢出文件节点实例分析	7.7.4 域溢出文件的使用
的数据部分	7.7.3 域溢出文件节点实例分析	7.8 坏块文件	7.9 分配文件	7.10 属性文件
7.9 分配文件	7.10 属性文件	7.10.1 叉数据属性	7.10.2 域属性	第8章 多磁盘卷
8.1 RAID	8.1.1 RAID级别简介	8.1.2 RAID中的基本概念	8.1.3 RAID0阵列原理	8.1.4 RAID1阵列原理
8.1.4 RAID1阵列原理	8.1.5 RAID4阵列原理	8.1.6 RAID5阵列原理	8.1.7 RAID6阵	8.1.8 RAID 1E阵列原理
列原理	8.1.8 RAID 1E阵列原理	8.1.9 RAID DP阵列原理	8.1.10 RAID的实现	8.1.11 数据恢复及取证注意事项
8.1.11 数据恢复及取证注意事项	8.2 磁盘跨区	8.2.1 概述	8.2.2 Linux MD	8.2.3
Linux LVM	8.2.4 Microsoft Windows LDM	8.2.5 总结	PART 2 实践篇	第9章 数据恢复前的
准备	9.1 写在数据恢复之前的话	9.2 检测磁盘	9.2.1 用MHDD检测磁盘	9.2.2
用MHDD清除主引导扇区“55AA”标志	9.2 检测磁盘	9.2.3 用PC-3000检测磁盘	9.3 坏道处理	9.4 镜像
磁盘	9.4.1 什么是“镜像磁盘”	9.4.2 什么情况下需要对磁盘进行镜像	9.4.3 用Media	9.4.4 用HDClone镜像磁盘
Tools镜像磁盘	9.4.4 用HDClone镜像磁盘	9.4.5 用Winhex镜像磁盘	9.5 分区及格式化对	9.5.1 Winhex“比较”功能的使用
磁盘的写入	9.5.1 Winhex“比较”功能的使用	9.5.2 分区过程对磁盘的写入	9.5.3 格	9.5.4
格式化过程对磁盘的写入	第10章 基本数据恢复	10.1 分区恢复	10.1.1 主分区表损坏恢复	10.1.2 重新分区未格式化
10.1.2 重新分区未格式化	10.1.3 分区布局改变并进行了格式化	10.1.4 使用FinalData快速	10.2 DBR损坏后的恢复	10.2.1 FAT文件系统DBR损坏后的恢复
寻找分区	10.2 DBR损坏后的恢复	10.2.1 FAT文件系统DBR损坏后的恢复	10.2.2 NTFS	10.2.3
文件系统DBR损坏后的恢复	10.3 格式化恢复	10.3.1 原FAT32格式化成FAT32	10.3.2	10.3.3
原FAT32格式化成NTFS	10.3.3 原NTFS格式化成NTFS	10.3.4 原NTFS格式化成FAT32	10.4 删除恢复	10.4.1 FAT16文件系统下的删除
10.4 删除恢复	10.4.1 FAT16文件系统下的删除	10.4.2 FAT32文件系统下的删除	10.4.3 NTFS文件系统下的删除	10.5 数据恢复软件的使用
10.4.3 NTFS文件系统下的删除	10.5 数据恢复软件的使用	10.5.1 使用R-Studio恢复数据	10.5.2 使用Recover My Files恢复数据	第11章 RAID数据恢复
10.5.2 使用Recover My Files恢复数据	第11章 RAID数据恢复	11.1 概述	11.2 FAT表在阵列	11.2.1 利用FAT表计算块大小
恢复中的作用	11.2.1 利用FAT表计算块大小	11.2.2 利用FAT表判断数据块顺序	11.2.3	11.3 MFT在阵列恢复中的作用
利用FAT表寻找校验块	11.3 MFT在阵列恢复中的作用	11.3.1 利用MFT记录编号判断块大小	11.3.2 利用MFT寻找校验块	11.4 RAID0阵列恢复
及数据块顺序	11.3.2 利用MFT寻找校验块	11.4 RAID0阵列恢复	11.4.1 参数分析	11.4.2 使用Winhex重组数据
11.4.2 使用Winhex重组数据	11.4.3 使用R-Studio恢复数据	11.5 RAID5阵列恢复	11.5.1	11.5.2 同步与异步的判断
循环方向的判断	11.5.2 同步与异步的判断	11.5.3 计算各个成员盘第一个校验块的位置	11.5.4 利用FAT恢复演示	11.5.5 利用MFT恢复演示
11.5.4 利用FAT恢复演示	11.5.5 利用MFT恢复演示	11.6 HP内外双循环阵列恢复	11.7.1 参数判断	11.7.2 数据恢复
RAID 1E阵列恢复	11.7.1 参数判断	11.7.2 数据恢复	附录A Win32环境下磁盘操作五大函数	附录B 文件后缀名速查表

PART 1 理论篇 第1章 数据恢复相关基础 1.1 硬盘探秘 1.1.1 硬盘结构 2.盘体

盘体由盘腔、上盖、盘片电机、盘片、磁头、音圈电机和其他的辅助组件组成。

为保证硬盘正常工作，盘体内的洁净度很高。

为防止灰尘进入，盘体处于相对密封的状态。

由于硬盘工作的过程中发热，为了保证盘腔的空气压力与外界平衡，在盘体上有呼吸孔，呼吸孔的内侧安装有一个小的空气过滤器，硬盘的设计不同，呼吸孔的位置和结构也有所差别。

同时由于盘体在装配完成后，要写入伺服信息，所以盘体上有伺服信息的写入口，在工厂无尘车间里将专用的写入设备从这个孔伸入盘体内写入伺服信息，写入完成后，会用铝箔将其封闭。

(1) 盘腔 盘腔一般由铝合金铸造后机加工而成，盘体的其他组件都直接或间接安装在盘腔上面，盘腔上还有将硬盘安装到其他设备上的螺丝孔。

(2) 上盖 上盖一般由铝合金或软磁金属材料加工而成，有的是单层的，有的是由多层材料粘合而成。

它的主要作用是与盘腔一起构成一个相对密封的整体，基本上都是用螺钉与盘腔连接，为了保证密封，上盖与盘腔的结合面一般都有密封垫圈。

(3) 盘片电机 盘片电机的主要作用就是带动盘片旋转，在控制电路板上的盘片电机驱动芯片的控制下，盘片电机带动盘片以设定的速度转动，盘片电机的转速由原来低于4000转/分，发展到现在的10000转/分，甚至15000转/分，盘片转速的提高决定着硬盘的寻道时间。

当然，在提高转速的同时，硬盘的发热量、振动、噪声等也会对硬盘的稳定工作产生影响。

所以一些新的技术也不断地应用到盘片电机上，由最初的滚珠轴承电机发展到现在的液态轴承电机。

盘片的电机一般为转速恒定的直流无刷电机，为三相直流供电。

线圈的绕法分为三角形连接、星形无中线和星形有中线三种，这种电机可以比较精确地控制转速，让盘片稳定地旋转。

(4) 盘片 盘片是硬盘的核心组件之一，不同的硬盘可能有不同的盘片数量。

所有的数据都是存储在盘片上的，盘片是在铝合金或玻璃基底上涂敷很薄的磁性材料、保护材料和润滑材料等多种不同功能的材料层加工而成，其中磁性材料的物理性能和磁层结构直接影响着数据的存储密度和所存储数据的稳定性。

为了提高存储密度，防止超顺磁效应的发生，各相关机构进行了大量的研究工作，不断改进磁层的物理性能和磁层结构。

磁记录层的记录方式也由以前的纵向磁记录发展到现在的垂直磁记录。

(5) 磁头 磁头也是硬盘的核心组件，磁头的性能对硬盘的数据存储密度和内部传输率有很大的影响。

磁头最早应用的是铁磁物质，1979年发明了薄膜磁头，使硬盘进一步减小体积、增大容量、提高读写速度成为了可能。

20世纪80年代末期IBM研发了MR磁阻磁头，后来又研发了GMR巨磁阻磁头。

现在的硬盘都是采用GMR磁头，它利用特殊材料的电阻值随磁场变化的原理来读取盘片上的数据。

磁头在工作的过程中并不与盘片接触，而是在盘片高速旋转带动的空气动力的作用下以很低的高度在盘片上面飞行。

为了提高磁头的灵敏度，磁头的飞行高度在不断降低。

磁头一般跟金属磁头臂、音圈电机线圈和预放电路等组成一个组件，磁头在音圈电机的带动下根据读写数据的需要做往复运动来定位数据所在的磁道。

<<数据重现>>

媒体关注与评论

文件系统将其下层的存储空间虚拟成文件的方式向其上层呈现，是整个数据系统中最关键的一环，是影响IO性能的一个瓶颈点，文件系统如果出了问题，轻则数据丢失，重则数据全毁。

本书全面介绍了各种文件系统原理，而且讲述了主流数据恢复原理和操作，是一本不可多得的好书！

——《大话存储》作者：张冬 网名：冬瓜头 从9.11事件到四川大地震，从CIH到熊猫烧香，您是否想过，在信息引领一切的时代，这些灾难过后，银行能不能正常工作，企业是否能正常运营？这一切都取决于数据是否遭受威胁，遭受威胁的数据又是否能够重现！

本书为你铺就了一条从入门到精通的数据恢复学习之路。

而且，数据恢复程序设计需要透彻了解文件系统的结构及工作方式，本书是目前公开技术资料最多的一本相关书籍，是难得的学习及参考书！

——中国矿业大学博士、哈市海云数据恢复总工、黑龙江科技学院软件讲师 江传力 本书有内容，有深度，是数据恢复不可多得的好书。

回想1996年开始研究数据恢复技术的时候，要想找到这种相关的资料是非常困难的。

为了提高国内数据恢复技术，精心创办了技术交流的平台中国硬盘基地（www.intohard.com），一举成为国内最专业的硬盘维修与数据恢复技术论坛。

时至今日，本书的出版也一定会成为数据恢复技术人员的一大福音！

——中国十大存储论坛之一“中国硬盘基地”网站创始人：田茂帅（八喜） 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。

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！

——08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 王江民

<<数据重现>>

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>