<<NTFS文件系统扇区存储探秘>>

图书基本信息

书名：<<NTFS文件系统扇区存储探秘>>

13位ISBN编号：9787115291233

10位ISBN编号：7115291233

出版时间：2012-10

出版时间：宋群生、 宋亚琼 人民邮电出版社 (2012-10出版)

作者：宋群生，宋亚琼 著

页数：344

<<NTFS文件系统扇区存储探秘>>

内容概要

《NTFS文件系统扇区存储探秘》主要内容包括：介绍NTFS文件系统优越的性能特征；介绍作者为了探索NTFS文件系统的存储特点编写的21个WIN32工具程序；使用作者编写的WIN32工具程序，探秘NTFS文件系统的扇区存储规律。

全书分3篇，共计17章。

第1章至第3章是“基础篇”，重点介绍了NTFS文件系统的性能和存储特点，同时也辅助性地介绍了FAT16和FAT32两种文件系统；第4章至第5章是“工具篇”，介绍了作者编写的工具程序；第6章至第17章是“探秘篇”，使用工具程序对NTFS文件系统的扇区存储规律进行了探索。

《NTFS文件系统扇区存储探秘》附送的光盘里收录了书中使用的全部工具程序，读者可以使用这些工具程序对硬盘扇区数据进行各种读写与分析。

《NTFS文件系统扇区存储探秘》可作为从事数据恢复和硬盘维修的技术人员参考用书，也可供研究文件系统和进行扇区数据分析的爱好者参考使用。

作者简介

宋群生，早在1998年即从事数据恢复研究，是国内计算机数据恢复界最早的开拓者之一，经过十几年的研究，作者成功开发了多套FAT16、FAT32、NTFS文件恢复程序。
2004年，作者率先在国内开创了远程数据恢复，并于当年4月出版了《硬盘扇区读写技术——修复硬盘与恢复文件》一书。

<<NTFS文件系统扇区存储探秘>>

书籍目录

章节摘录

版权页： 插图： 4.6查找硬盘扇区特征程序 在探索文件系统在物理硬盘上的扇区存储规律时，一般不能依赖被操作硬盘上的操作系统与文件系统。
否则的话，就会受到操作系统的权限限制和文件系统的保护限制。
那么不依赖操作系统与文件系统，如何找到硬盘上的文件，或是系统在某些扇区中的字段记录呢？
作者使用了一种逆向分析的方法，该方法的大致过程如下。
先使用工具程序在硬盘上找到具有文件特征的扇区号，然后根据扇区号算出计算扇区地址的方法，进而再去探索系统存储的字段规律和文件数据的存储地址。
这种方法运用的详细情况在《探秘篇》中再作介绍。
在实际操作中要使用这种分析方法，查找扇区特征就是至关重要的一步。
本节介绍的工具程序，能够查找5种类型的扇区特征，如下。
（1）系统引导扇区的特征—BOOT扇区。
（2） MS—DOS使用的8.3格式的文件名—DOS文件名。
（3） NTFS文件系统使用的文件名——长文件名。
（4）文件存储在数据区中的文本内容——扇区字符串。
（5）文件名使用汉字时的一汉字文件名。
4.6.1NTFS文件系统扇区特征介绍 NTFS文件系统使用了“磁盘上的任何事物都为文件”的存储模式，因此要想探索NTFS文件系统的扇区存储规律，就必须对NTFS在存储文件时的扇区特征有所了解。
下面分别讲解本节工具程序所能查找的NTFS文件系统的5种扇区存储特征。
1.BOOT扇区 本节所说的“BOOT扇区”，指的是存储系统引导数据的扇区。
既然是针对物理硬盘进行扇区读写，那为什么还需要查找“BOOT扇区”呢？
原因主要有两个方面。
在NTFS文件系统中，所有在扇区中存储的有关扇区地址的字段记录，都是以簇为单位计算的。
也就是说，NTFS文件系统只用簇来标识磁盘地址，而不用扇区进行标识。
可是在使用物理硬盘扇区读写技术对磁盘进行操作时，是使用线性寻址所定义的扇区编号，作为对硬盘扇区进行寻址的依据。
这就要求操作者必须进行两种数据间的换算，要将NTFS记录在扇区中的簇号标识字段值，换算成线性寻址的扇区号。
要进行这种换算，必须知道每个簇中有多少个扇区。
而记录每簇扇区数的字段，就存储在BOOT扇区中，这是查找BOOT扇区的原因之一。
在将簇号转换成扇区号以后，还必须知道是从哪一个扇区开始计算扇区号的。
因为NTFS文件系统不是管理物理硬盘，而是管理某一个逻辑驱动器。
所以不能用物理硬盘的第1个扇区作为起始扇区进行计算，而应将NTFS管理的逻辑驱动器的第1个扇区作为起始扇区，这第1个扇区就是分区引导记录所在的扇区，这是查找BOOT扇区的原因之二。
下面举一个实例来说明查找BOOT扇区的必要性。
先将实例的内容介绍一下。
假如操作者已经找到了文件系统在扇区中记录的一个字段值，该字段值记录的是文件数据在扇区中的存储地址。
现在需要通过计算，从已得到的字段值中解读出存储地址的扇区号。
下面介绍具体的计算过程。
字段值在扇区中的字节数据是“4C 0302”，因为存储数据时是低字节在前，高字节在后，所以写成十六进制应为“02034cH”，换算成十进制是“131916”。
现在得到的是文件存储数据的逻辑簇号，需要将簇号乘以每簇占用的扇区数，才是文件存储数据的逻辑扇区号。
实际上到这一步，就需要查找BOOT扇区了，因为每簇扇区数就属于系统数据，是记录在BOOT扇区中的。

为了简化叙述的过程，假设已经知道了每簇扇区数是4，则存储文件数据的扇区号是131916×4=527664。

上面计算出的结果不是一个绝对数值，而是一个相对数值，它是相对于逻辑驱动器的第1个扇区的。现在必须查找逻辑驱动器的第1个扇区的地址，也就是分区引导记录所在的扇区号。

媒体关注与评论

这是一本实际工作中非常需要的工具书，保护和抢救数据对于每个人来说都非常重要，我很乐意向读者推荐本书，相信有志的读者朋友一定能够从此书中获得相关的技术知识与操作经验。
——效率源信息安全技术有限责任公司副总经理、技术总监 张彬最难能可贵的是，本书是一本实操性非常强的书，全书都贯穿作者对技术探索的过程，跟随着作者探究的步伐，读者一定能够分享到作者在对NTFS技术不断探索和发现过程中得到的快乐。
——彦安科技总经理 《数据安全与编程技术》、《数据恢复技术（第二版）》作者 涂彦晖本书对NTFS的扇区存储结构分析得比较详细，特别指出NTFS的原始数据以文件形式存于硬盘，而且分析了MFT特有的属性和作用，在知识面上有新的认识。
总体上看，此书在国内同类技术书籍中比较领先，对NTFS文件系统研究比较深入，是针对计算机硬盘数据存储安全工作者的一本重要参考书籍。
——上海嘉岛商贸有限公司计算机管理员 詹胜本书以全新的方式分析了NTFS文件系统的扇区存储规律，对NTFS的很多优越性能，都以扇区存储的特征为视角进行了详细分析和探索。
本书所提供的工具程序，对扇区的操作透明、直观，针对性强，可以为读者在分析扇区存储规律时提供高效实用的方法和技巧，很容易上手。
本书内容丰富，有很高的实用价值，是分析和研究NTFS文件系统不可或缺的工具书。
——济南市技师学院副教授级高工 邢人璋

编辑推荐

彦安科技总经理涂彦晖、效率源公司技术总监张彬联袂推荐揭示微软未公布的NTFS文件系统扇区存储规律附赠作者自己开发的、价值数百元的实用工具程序

名人推荐

本书对NTFS的扇区存储结构分析得比较详细，特别指出NTFS的原始数据以文件形式存于硬盘，而且分析了MFT特有的属性和作用，在知识面上有新的认识。
总体上看，此书在国内同类技术书籍中比较领先，对NTFS文件系统研究比较深入，是写给计算机硬盘数据存储安全工作者的一本重要参考书。
——上海嘉岛商贸有限公司计算机管理员 詹胜 本书以全新的方式分析了NTFS文件系统的扇区存储规律，对NTFS的很多优越性能，都以扇区存储的特征为视角进行了详细分析和探索。
本书所提供的工具程序，对扇区的操作透明、直观，针对性强，可以为读者在分析扇区存储规律时提供高效实用的方法和技巧，很容易上手。
本书内容丰富，有很高的实用价值，是分析和研究NTFS文件系统不可或缺的工具书。
——济南市技师学院副教授级高工 邢人璋

版权说明