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
- 可供从事数据恢复和硬盘维修的技术人员以及研究文件系统和进行扇区数据分析的爱好者参考。

NTFS文件系统扇区存储探秘

宋群生 宋亚琼 编著

CD-ROM光盘

人民邮电出版社
POSTS & TELECOM PRESS

NTFS

文件系统扇区存储探秘

宋群生 宋亚琼 编著

人民邮电出版社
北京

图书在版编目（CIP）数据

NTFS文件系统扇区存储探秘 / 宋群生，宋亚琼编著
— 北京 : 人民邮电出版社，2012.10
ISBN 978-7-115-29123-3

Ⅰ. ①N… Ⅱ. ①宋… ②宋… Ⅲ. ①文件系统－数据存贮－研究 Ⅳ. ①TP311.13

中国版本图书馆CIP数据核字(2012)第177891号

内 容 提 要

本书主要内容包括：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。

本书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。

本书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。

NTFS文件系统扇区存储探秘

◆ 编　　著　宋群生　宋亚琼
责任编辑　王峰松

◆ 人民邮电出版社出版发行　　北京市崇文区夕照寺街14号
邮编　100061　　电子邮件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
北京鑫正大印刷有限公司印刷

◆ 开本：787×1092　1/16
印张：22
字数：537千字　　2012年10月第1版
印数：1－3 500册　　2012年10月北京第1次印刷

ISBN 978-7-115-29123-3

定价：59.00元（附光盘）

读者服务热线：(010)67132692　印装质量热线：(010)67129223
反盗版热线：(010) 67171154

推荐序

随着信息化的飞速发展，人们对硬盘、U 盘等各种存储介质越来越熟悉，而数据信息也由纸质保存演变到如今的电子存储，数据信息的重要性日益凸显，数据已经成为一项最重要的资产。

如今，数据的重要性已远远超越了硬盘等存储介质本身，一旦珍贵的数据遭到损坏或丢失，数据恢复就显得尤为重要。正因为在构筑数据安全保护底线方面所处的特殊地位，数据恢复技术的重要性正在被各行各业广泛关注。

《NTFS 文件系统扇区存储探秘》一书重点揭示了微软公司没有公布的 NTFS 文件系统的扇区存储规律，全书对 NTFS 的基本存储原理由浅入深，并结合大量演示实例的操作与分析进行讲解，是其他的书籍中找不到的，特别是作者介绍的隐藏文件的方法、恢复 EFS 加密文件数据的方法、恢复 NTFS 压缩文件数据的方法，都是现有书籍中尚未涉及的领域。

应当说，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

NTFS 全称是 New Technology File System，即新技术文件系统。20 世纪 90 年代初，微软和 IBM 共同开发了 OS/2，因为对重大问题的分歧，最终双方并没有继续合作，IBM 继续开发 OS/2，而微软则开始研发 Windows NT，随着 Windows NT 第一个版本的诞生，NTFS 文件系统也于 1993 年诞生。

NTFS 从诞生至今已经有 19 年，前后共发布了 5 个版本，直至今天 NTFS 依然是 Windows 操作系统中最主流的文件系统，随着微软官方宣布，其下一代文件系统存储技术 WinFS 项目的停止，NTFS 可能在今后若干年，仍然会是微软操作系统中最主流的文件系统。

本书较全面地介绍了 FAT、FAT32、NTFS 文件系统各类型的数据结构及其工作原理，并重点介绍了 NTFS 文件系统的磁盘管理功能、编码、NTFS 文件常驻与非常驻属性、元数据等知识点，能够使读者对 NTFS 有一个较为深入的了解。

最难能可贵的是，本书是一本实际操作性非常强的书，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

前言

在众多的磁盘文件系统中，NTFS 文件系统是各项性能都比较优越的文件系统，集中体现了高效和安全两大特性。NTFS 文件系统早年在服务器领域得到了广泛应用。微软公司推出 WINDOWS 2000 和 WINDOWS XP 以来，NTFS 文件系统在 PC 机上也得到了迅速普及。

据作者了解，现有的涉及 NTFS 文件系统的书籍，一般只介绍了 NTFS 文件系统的优越性能，并没有揭示其在磁盘上的扇区存储规律。在有关 NTFS 文件系统的扇区存储方面，也没有发现比较系统全面的介绍资料。在 NTFS 文件系统的设计者发表的官方资料中，也很少涉及 NTFS 文件系统的扇区存储规律。

设计者为什么不公开其扇区存储规律呢？这主要是从安全方面考虑的。因为公开了这些扇区存储规律，文件系统的许多保护机制就都能用修改硬盘物理扇区数据的方法进行修改，文件系统的安全保护功能就被削弱了。

不过这是一把双刃剑，如果能够了解 NTFS 文件系统的扇区存储规律，操作者就能在系统维护、数据恢复、开拓应用范围等方面获得很多不可替代的方法和技巧。

为了探索 NTFS 文件系统的扇区存储规律，作者编写了 21 个 WIN32 工具程序，都收录在随书附送的光盘中。使用这些 WIN32 工具程序，可以对硬盘物理扇区进行各种操作，可以监测、分析扇区中的数据变化，从而发现 NTFS 文件系统的优越性能是如何通过扇区数据存储体现的。

虽然这些工具程序在本书中是为了探索 NTFS 文件系统的扇区存储规律而编写的，但是它们在磁盘扇区的读写与分析领域是具有通用性的，因为这些工具程序是对物理硬盘进行操作的，是不受操作系统和文件系统限制的。在探索其他文件系统的扇区存储规律方面，在修复系统参数方面和恢复硬盘、U 盘、存储卡数据方面，可以开拓更多的应用空间。

本书用具体的演示实例，对 21 个 WIN32 工具程序的使用，对 NTFS 文件系统的基本特性、扇区分配、EFS 加密、数据压缩、数据属性，对修改位图数据隐藏用户的机密文件，对 NTFS 逻辑盘的数据恢复等进行了详细的分析和介绍。

作者对 NTFS 文件系统的扇区存储规律所进行的探索，可以为读者继续进行此项工作起到启示和借鉴的作用。NTFS 文件系统具有众多的优越性能，完全揭示其扇区存储规律，还有待于更多技术分析人员的不懈努力。

在对演示实例的操作与分析中，有很多内容在目前是没有资料可查的。特别是笔者介绍的隐藏文件的方法、恢复 EFS 加密文件数据的方法、恢复 NTFS 压缩文件数据的方法，都是其他书籍中没有涉及的领域。

由于作者水平有限，书中难免出现某些疏漏，敬请读者批评指正。

目　录

基　础　篇

工　具　篇

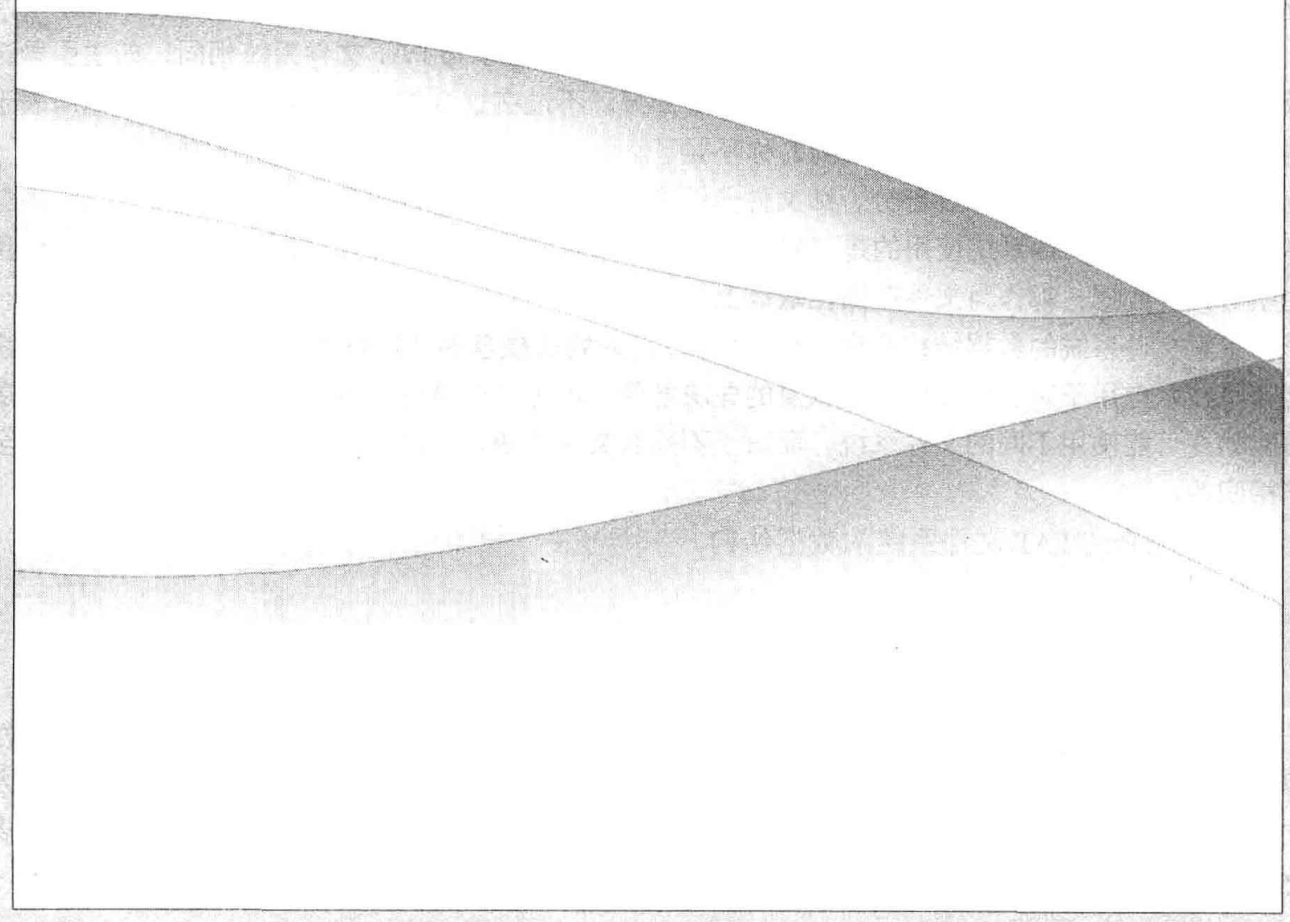
探 秘 篇

基础篇

本篇主要介绍 NTFS 文件系统的基本特性和扇区存储特征。同时，为了能与其他主流文件系统进行比较，以加深对 NTFS 文件系统的认识，本篇还介绍了 FAT16 和 FAT32 两种文件系统的基本特性，以及它们在硬盘扇区中的存储规律。

NTFS 文件系统虽然与两种 FAT 文件系统不同，但它们在扇区存储规律上，还是有某些共通或相似的地方的。

本书讲述的两大主题，第一是使用作者编写的 WIN32 工具程序，对硬盘扇区进行各种操作；第二是使用读写物理硬盘扇区的方法，去探索 NTFS 文件系统的扇区存储规律。掌握了 NTFS 文件系统的扇区存储规律，就能使操作者不受操作系统和文件系统的限制，实现一些用其他方法无法完成的操作目的。譬如从系统已被破坏的硬盘上恢复文件；排除一些常见的由于系统数据受损，而出现的硬盘逻辑故障；通过修改位图文件的扇区数据，来达到隐藏机密文件的目的；移植被 EFS 加密的文件数据；移植被压缩的文件数据；通过直接修改扇区的字节数据，取得原先没有的操作权限，等等。



第 1 章 FAT 文件系统的数据结构

硬盘在分区以后，其每一个逻辑驱动器都必须建立起完整的数据结构，才能正常使用。FAT 文件系统和 NTFS 文件系统的数据结构大部分都不相同，只在存储系统分区数据的扇区上，有某些相同或相似的地方。

FAT 文件系统的数据结构由 6 部分组成，分别是主引导记录、主分区表或分区链表、分区引导记录、文件分配表、文件目录表和数据区。这里需要说明的是，主引导记录和主分区表都只有一个，共同存储在一个扇区中。如果使用 CHS（柱面数、磁头数、扇区数）寻址方式，这个扇区是 0 柱面 0 磁头 1 扇区；如果使用线性寻址方式，这个扇区是 0 号扇区。从硬盘分区后的区域结构上划分的话，该扇区可以认为是属于第 1 个逻辑驱动器，也就是通常所说的 C 盘。而其他的逻辑驱动器就没有主引导记录和主分区表了，在这些逻辑驱动器所属的第 1 个系统隐藏扇区上，只有分区链表。

NTFS 文件系统的数据结构中，用于系统引导的部分基本与 FAT 文件系统相同，如主引导记录、主分区表或分区链表、分区引导记录这 3 部分。不过在这 3 部分中，很多字段的数据所表示的内容是完全不同的，只是都有相同的称呼罢了。

FAT 文件系统的另外 3 部分，即文件分配表、文件目录表和数据区，在 NTFS 文件系统中则不存在。NTFS 文件系统使用的是“磁盘上的任何事物都为文件”的存储模式，甚至连系统使用的引导文件数据，都作为文件存储在磁盘上。

了解文件系统的数据结构和扇区存储规律，是对物理硬盘扇区进行读写操作的基础,也是将扇区读写技术应用于系统修复和文件恢复的先决条件。因为一个硬盘上有很多逻辑驱动器，这些逻辑驱动器可能使用不同的文件系统，而对于不同的文件系统，读写与分析扇区数据的方法是完全不相同的。

本章先介绍 FAT 文件系统的数据结构。

1.1 主引导记录

硬盘的主引导记录也称 MBR，存储在 0 柱面 0 磁头 1 扇区。如果读写扇区时采用线性寻址方式，则该扇区的编号为“0”。在本书后面的章节里，扇区地址全部使用线性寻址方式来表示。该扇区的 512 字节有 3 部分内容，除了主引导记录外，还有分区表和结束标志 55 AA。

主引导记录的作用非常重要，它是硬盘启动时最先加载的扇区数据。下面通过分析硬盘的启动过程，来说明它的重要性。

（1）计算机系统接通电源以后，主板 BIOS 加电进行自检。自检的内容很多，是一个很复杂的过程，这里只介绍与硬盘有关的部分。

（2）将硬盘第 1 个扇区，也就是 0 柱面 0 磁头 1 扇区（线性寻址时是 0 号扇区）的内容读入内存。

（3）检查结束标志，也就是扇区最后两个字节的值是否等于“aa55H”（存储顺序是低字节在前，高字节在后）。若不等则打印屏幕提示，然后死机。

（4）执行主引导记录中的程序，将控制权转交给主引导程序。

（5）主引导程序首先将自己读入内存，然后查找在分区表中是否有活动分区。找到活动分区以后，将分区引导记录读入内存。

（6）检查结束标志是否等于“aa55H”，然后执行分区引导记录中的启动程序，将控制权交给操作系统。

（7）操作系统加载系统文件，计算机启动。

通过对以上过程的分析可以看出，如果主引导记录不正常，后面所有的启动过程都不可能正常执行。

有一种特殊情况，使计算机启动过程的前两步与上面介绍的不一样。如果硬盘上安装了多系统引导软件，如 Partition Magician 分区软件，则该软件将主引导记录替换成自己的一段程序。这段程序将 BIOS 引向软件设置的专用分区，然后根据操作者的选择激活某一个分区，再进入正常的启动过程。类似 Partition Magician 这样的分区软件还有很多，它们各有自己的特点，这些第三方软件都不在本书的讨论范围之内。通常情况下，一块硬盘上只有一个主引导记录。

现在用“读硬盘扇区数据.EXE”程序将一块硬盘的主引导记录读出，程序运行界面如图 1-1 所示。“读硬盘扇区数据.EXE”程序将在《工具篇》中介绍，现在先使用该程序的运行结果。

图 1-1 所示的左图是程序运行的主窗口。在主窗口的编辑框中显示了数值“10084”，这是主引导记录所在扇区中，全部字节的累加算术和。为什么要取这个数值的原因将在《工具篇》中详细说明。

图 1-1 所示的右图是程序运行后弹出的对话框。该对话框中显示了 512 字节的十六进制值，每行显示 16 字节，共显示 32 行。

在图 1-1 中，位移从 00H 到 1bdH 就是主引导记录。如果用扇区内的字节编号来表示某一字节，设起始号为 1，就是从第 1 到第 446 字节。为什么要使用位移和扇区内编号这两种计算方式呢？因为在今后分析扇区数据时，或者是手工编制扇区中的字节数据时，某些场合用编号计算是比较方便的。

譬如在《工具篇》中介绍的“修改扇区文件数据.EXE”程序，可以将每个扇区的 512 字节，按照每行 16 字节，一共 32 行的格式显示在屏幕上。如果从 1 开始编号，则感觉很有对称性，容易查找某一字节。如果用位移值计算，就感觉不太方便。

字节位移是从 0 开始计数，而字节编号是从 1 开始编号，所以对同一字节来说，字节编号的值要比字节位移的值大 1。

位移从 1beH 到 1fdH 是分区表，字节编号为 447 到 510。有关分区表的内容在下一节

讨论。

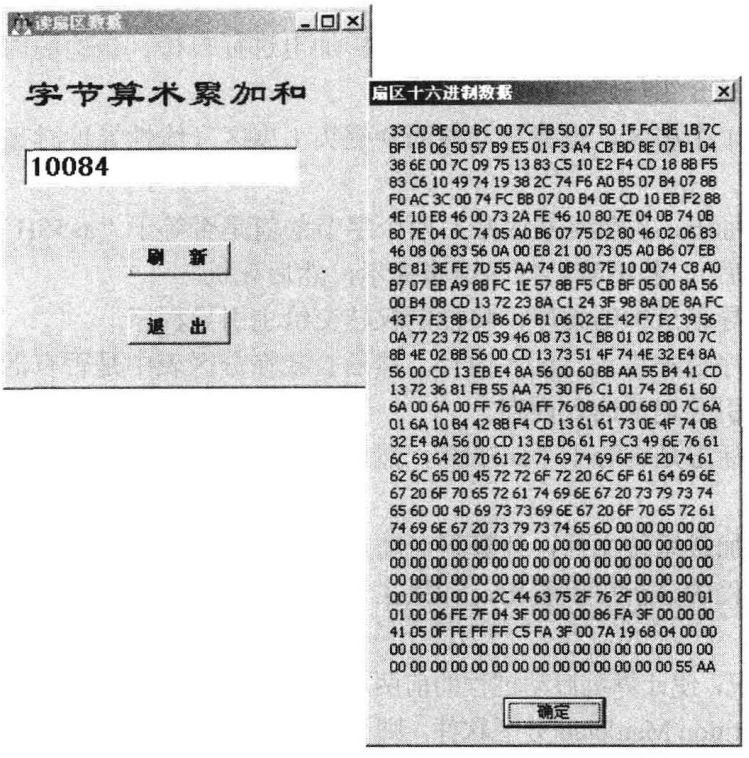


图 1-1

最后两字节是结束标志“55 AA”。因为两字节组成一个字，写入磁盘的顺序是低字节在前，高字节在后，所以“55 AA”写成十六进制应为“aa55H”。

结束标志“55 AA”是查找系统数据扇区的标志，据此对扇区进行搜索，可用于寻找主引导记录、主分区表或分区链表所在的扇区地址，也可以具此查找分区引导记录的扇区地址。

主引导记录扇区所在的磁道，通常称为 0 磁道，它属于隐藏磁道，这个磁道的 63 个扇区属于隐藏扇区。操作系统的所有命令，除了 FDISK 以外都不能访问它们。就连格式化程序 FORMAT，对这些隐藏扇区也无能为力。

主引导记录和主分区表的数据，只占用了 0 磁道的第 1 个扇区，系统对其他的 62 个扇区弃之不用。正因为如此，0 磁道的剩余 62 个扇区就成了一些病毒程序代码、操作系统的引导代码、应用软件用于自我保护的识别标记、BIOS 功能扩展程序代码的栖息之地。

经常监测并分析 0 磁道的扇区数据变化，就能发现很多不为人知的秘密，作者举一例来说明这个问题。

美国的 MACROMEDIA 公司堪称网页制作软件的鼻祖，该公司的三大软件颇具影响力。这三款软件是：网页制作软件 DREAMWEAVER MX、图象处理软件 FIREWORKS MX 和动画制作软件 FLASH MX。

这三款软件有试用版，从操作者安装使用开始，时间限制为 30 天。超过试用期后，软件就不能运行了。即使重新安装操作系统和这三款软件，甚至将硬盘格式化或重新分区，也无济于事。

那么这三款软件采用了什么保护机制呢？作者通过对0磁道扇区数据的监测，发现了这三款软件的一个秘密。

这三款软件中的每一款软件安装以后，都会向0磁道的第32扇区写入一部分识别代码。当操作者对逻辑盘进行格式化，或是对整个硬盘重新分区时，所运行的程序都不会访问第32扇区，所以软件的时间限制仍然有效。

作者用扇区清零程序将32扇区的数据清掉，然后再安装这三款软件的试用版，则可以继续使用了。

采取这种保护方式的软件还有很多，只要经常监测0磁道并用心去分析，就能发现许多不为人知的秘密。

下面用作者使用的两块硬盘运行“监视0磁道变化.EXE”程序，将两块硬盘的0磁道63个扇区的数据分别读出，然后进行比较。所使用的工具程序在《工具篇》中再详细介绍。

先看一块新硬盘的显示数据，如图1-2所示。

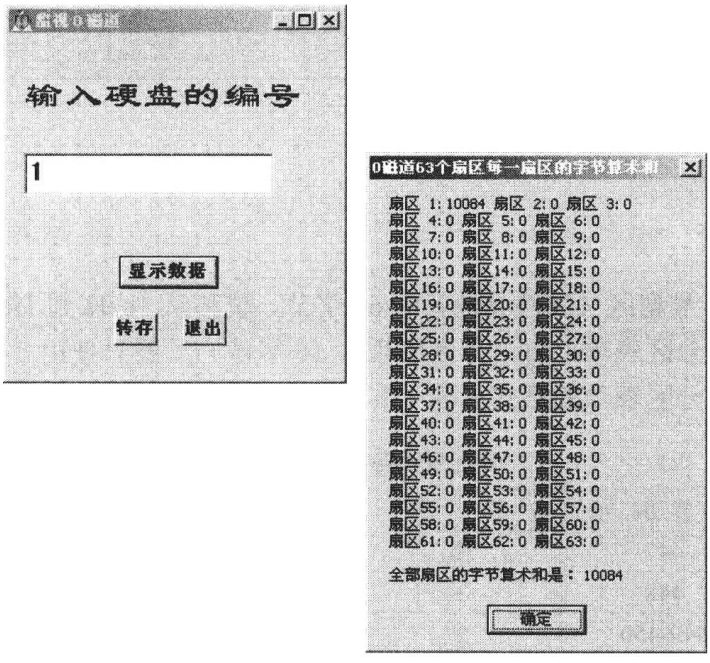


图1-2

图1-2所示的扇区编号没有使用线性寻址的表示方法，而是使用了1～63的编号方式，这是为了强调在硬盘的结构中，每磁道有63个扇区的虚拟物理概念。

从图1-2所示的扇区字节算术和可以看出，只有第1扇区写有数据，其他62个扇区全部为0。这是因为该硬盘使用不久，还没有写入其他程序的垃圾代码。

再看一块老硬盘的显示数据，如图1-3所示。

如图1-3所示，除了第1扇区写有系统引导数据以外，还有很多扇区也写有数据。与第1扇区字节算术和相同的，如第6扇区，是作者备份的系统数据，目的是日后出现引导故障时修复硬盘。与第1扇区字节算术和不相同的扇区，就是硬盘使用三年多来，各种应用软件写入的垃圾代码。

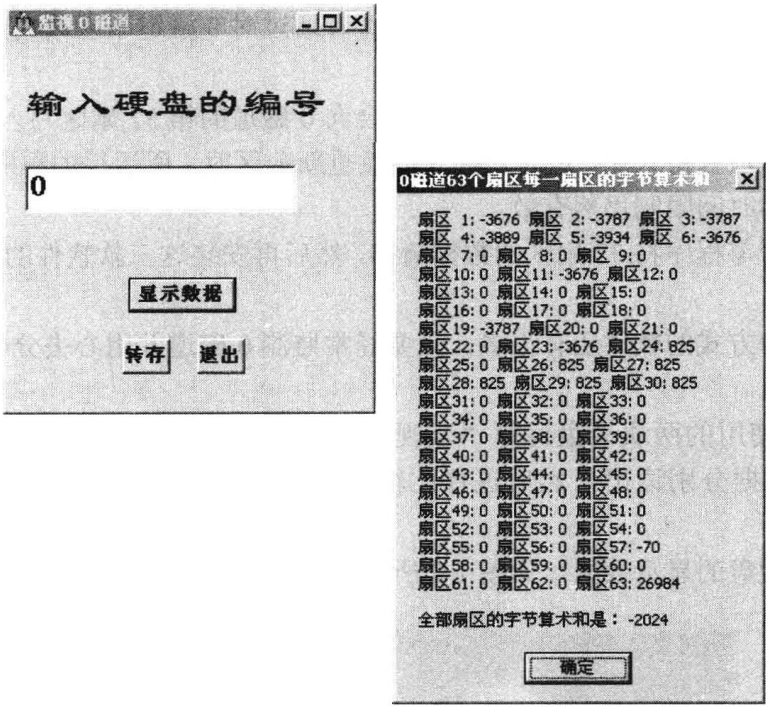


图 1-3

1.2 主分区表

主分区表占用 0 号扇区（线性寻址）的 64 字节，位移从 1beH 到 1fdH，字节编号为 447 到 510。它共有 4 个分区表项，每个分区表项占 16 字节。一般只使用 2 个分区表项，另外 2 个分区表项全为 0。分区表项的格式见表 1-1。

表 1-1　　分区表项各字段值的内容

偏　移　量	字 节 编 号	字　　节	内 容 说 明
1beH	447	1	BOOT ID: 80H 表示可启动分区，否则为 00H
1bfH	448	1	分区起始磁头号
1c0H	449-450	2	分区起始扇区值和柱面值
1c2H	451	1	操作系统和文件系统的 ID 值，常用的字节标志有： 05H 或 0fH　　表示扩展 MS-DOS 分区 06H 或 0eH　　表示 FAT16 0bH 或 0cH　　表示 FAT32 07H 或 17H　　表示 NTFS
1c3H	452	1	分区结束磁头号
1c4H	453-454	2	分区结束扇区值和柱面值
1c6H	455-458	4	分区前扇区总数
1caH	459-462	4	分区内扇区总数

注：偏移量和字节编号是第 1 个分区表项的值，后面的分区表项按照相同的规律递增。

通常说的分区表指的是主分区表，另外在扩展分区的每一个逻辑驱动器中，都有一个分区链表，对它们的解读方法基本是相同的。

下面将图 1-1 所示的两个分区表项单独列出来进行分析。

分区表项一。（位移 1beH 至 1cdH，编号 447 到 462）

1	2	3	4	5	6	7	8
80	01	01 00	06	fe	7f 04	3f 00 00 00	86 fa 3f 00

第 1 个分区表项记录的是本分区的有关参数。

将 16 字节按表 1-1 的格式分为 8 段，分别进行说明。

第 1、2、4、5 段与表中的内容一样，不必重复。

第 3 段是 2 字节，表示扇区值和柱面值，因为本书介绍的工具程序使用线性寻址方式，所以对本字段的内容就没有必要详细解读了。

第 6 段是 2 字节，也表示扇区值和柱面值。

第 7 段是一个双字，存储顺序低字节在前，高字节在后，写成十六进制是“0000003fH”，十进制是“63”。

第 8 段是一个双字，它的值是十六进制为“003ffa86H”，十进制为“4192902”。

分区表项二。（位移 1ceH 至 1ddH，编号 463 到 478）

1	2	3	4	5	6	7	8
00	00	41 05	0f	fe	ff ff	c5 fa 3f 00	7a 19 68 04

第 2 个分区表项记录的是下一分区的有关参数。

将 16 字节按表 1-1 的格式分为 8 段，各字段的解读方法与第 1 个分区表项相同，就不重复说明了。

分区链表的字段组成与解读方法与主分区表基本相同，读者可自行分析研究。需要说明的是，最后一个逻辑驱动器的分区链表中，只使用了 1 个分区表项，其他 3 个分区表项的字节数据全为 0。

1.3 分区引导记录

硬盘的主引导记录只有一个，存储在硬盘的线性 0 号扇区上。而硬盘的分区引导记录不止一个，每一个逻辑驱动器都有一个分区引导记录。如果将一个硬盘分为 C、D、E、F、G 5 个逻辑驱动器，就应该有 5 个分区引导记录，分别存储在各个逻辑驱动器的第 1 个逻辑扇区中。

分区引导记录主要由 4 部分组成。

（1）BIOS 参数记录块 BPB（BIOS Parameter Block）。

（2）磁盘标志记录表。

（3）分区引导记录代码区。

（4）结束标志“55 AA”。

与本书内容相关的是第 1 和第 4 部分，对第 2 和第 3 部分不进行讨论。

BIOS 参数记录块 BPB（简称 BPB 表）所记录的有关参数，能帮助操作者确定分区的容量大小、文件分配表 FAT 的位置和大小、文件目录表 FDT 的位置。BPB 表的结构与使用的文件系统有关，本节讨论 FAT16 和 FAT32 两种文件系统的 BPB 表结构。

结束标志“55 AA”是系统识别引导扇区的标识，也是使用工具程序对硬盘扇区进行搜

索，用于寻找分区引导记录所在扇区地址的依据。

1.3.1 FAT16 文件系统的 BPB 表

FAT16 文件系统 BPB 表从扇区字节位移 0bH 开始，用字节编号计算，就是第 12 字节，BPB 表共占用 25 字节。

FAT16 文件系统 BPB 表的结构见表 1-2。

表 1-2　　FAT16 文件系统 BPB 表的结构

偏　移　量	字 节 编 号	字　　节	内 容 说 明
0bH	12-13	2	每扇区字节数
0dH	14	1	每簇扇区数
0eH	15-16	2	保留扇区数
10H	17	1	FAT 表的数目
11H	18-19	2	根目录登记项数
13H	20-21	2	总扇区数
15H	22	1	磁盘介质描述符
16H	23-24	2	每个 FAT 的扇区数
18H	25-26	2	每个磁道的扇区数
1aH	27-28	2	磁头数
1cH	29-32	4	隐藏扇区数
20H	33-36	4	逻辑驱动器总扇区数

下面用“读硬盘扇区数据.EXE”程序将一个逻辑驱动器的引导记录读出来，然后结合表 1-2 进行分析，程序运行界面如图 1-4 所示。

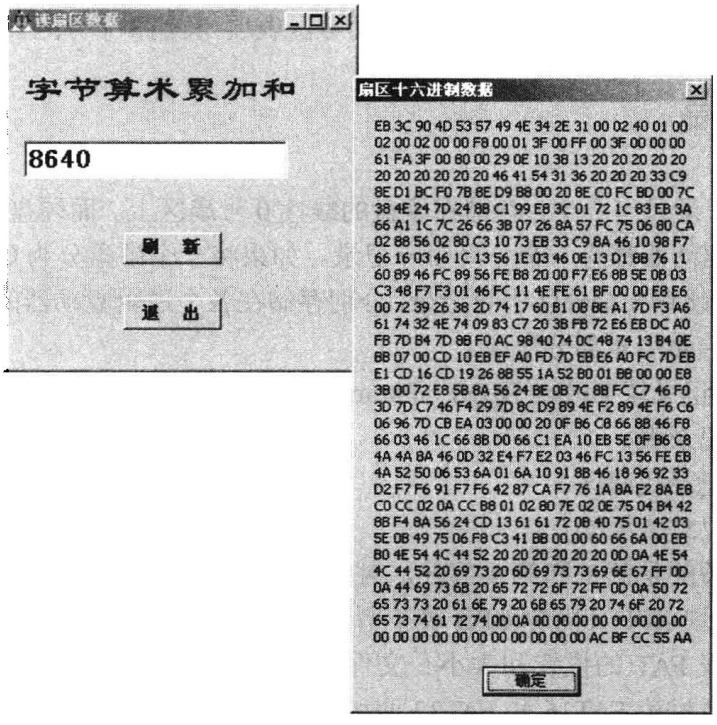


图 1-4

BPB表占用的字节数较多，各个字段值所表示的内容也较为复杂。为了便于分析，下面将BPB表的内容单独列出来。

1	2	3	4	5	6	7	8	9	10
00 02	40	01 00	02	00 02	00 00	f8	00 01	3f 00	ff 00

11	12
3f 00 00 00	61 fa 3f 00

从第12字节开始，将25字节按表1-2的格式分为12段，分别进行说明。

第1段是1个字，它的值为200H，等于512，说明每个扇区有512字节。

第2段是1字节，值为64，说明每个簇包含64个扇区，则每个簇的字节数是：64×512=32768。关于簇的概念，在后面有关章节中再作介绍。

第3段是1个字，值为1，说明有1个保留扇区。

第4段是1字节，值为2，说明有2个FAT表。

第5段是1个字，值为512，说明有512个根目录登记项数。因为每个根目录登记项固定占用32字节，据此可算出FDT表总共占用32个扇区。

第6段是1字，在硬盘中设为0。

第7段是1字节，固定为f8H。

第8段是1个字，值为256，说明每个FAT表占用256个扇区。

第9段是1个字，值为63，说明每个磁道划分成63个扇区。

第10段是1个字，值为255，说明磁头数最大是255，这个数值的含义需要进一步解释。这个参数并不是硬盘的物理磁头数，它是BIOS磁盘服务程序为了管理大容量硬盘，采用位移变换后形成的值。在CHS扇区寻址方式中，柱面用10位二进制数表示，其最大值为1024。硬盘的柱面数一般都超过了1024，因此BIOS磁盘服务程序采用了减少柱面数，增加磁头数的移位算法。

举例说明一下，假如一个硬盘有8192个柱面和16个磁头。很明显在CHS寻址方式中，无法表示全部柱面数。这时由BIOS磁盘服务程序将柱面数换算成8192÷8=1024，将磁头数换算成16×8=128。这样既保证硬盘的容量不变，又能使操作系统或应用程序访问到所有的硬盘扇区。

第11段是1个双字，值为63，说明有63个隐藏扇区。

第12段是1个双字，值为4 192 865，这是逻辑驱动器的总扇区数，但它不包含第11段中的隐藏扇区数。

1.3.2 FAT32文件系统的BPB表

FAT32文件系统BPB表也从扇区字节位移0bH开始，占用53字节。因为FAT16文件系统中的有些磁盘参数在FAT32文件系统中已不适用，必须进行扩充。具体做法是将FAT16文件系统中使用的25字节仍然保留，适用的数据项继续使用，需要扩充的数据项移到后面的28字节里去。目前这28字节只使用了很少一部分，剩下的字节全为0，供系统继续扩充时使用。

FAT32文件系统BPB表的结构见表1-3。