NTFS文件系统实例详解

NTFS WENJIAN XITONG SHILI XIANGJIE

陈培德 吴建平 王丽清 著

随书附光盘一张

国防工业出版社
National Defense Industry Press

云南省高校数字媒体技术重点实验室2014年度开放课题

NTFS文件系统实例详解

陈培德　吴建平　王丽清　著

国防工业出版社
·北京·

内 容 简 介

本书结合实例（实例素材附光盘）以 WinHex 磁盘编辑软件为工具，系统地论述了 NTFS 文件系统的基本原理、总体布局、元文件$MFT 记录的结构、NTFS 的其他元文件、索引目录结构；文件基本操作对元文件$MFT、索引目录、位图表等的影响；高级格式化对 NTFS 文件系统的影响；NTFS 文件系统下的数据恢复等。每章后有大量的思考题及参考答案（附光盘），读者通过每章的学习并完成思考题后，加深对每一章知识的理解和掌握。

本书用大量的实例论证了 NTFS 文件系统对索引目录的管理是采用 B-树结构。为读者进一步深入研究 NTFS 文件系统、恢复 NTFS 文件系统的数据等方面提供强有力的理论依据。

本书内容丰富、案例详实，论述由浅入深、循序渐进、重点突出，内容与案例紧密结合；在编排上系统全面、新颖实用、可读性强。

本书适用于从事 NTFS 文件系统研究与教学工作的人员，也适合于从事有关 NTFS 文件系统下的数据恢复、电子取证以及其他有关人员自学、参考。

图书在版编目（CIP）数据

NTFS 文件系统实例详解/陈培德，吴建平，王丽清著. —北京：国防工业出版社，2015.3

ISBN 978-7-118-09926-3

Ⅰ. ①N… Ⅱ. ①陈… ②吴… ③王… Ⅲ. ①文件系统－数据存贮—研究 Ⅳ. ①TP311.13 ②TP333

中国版本图书馆 CIP 数据核字（2015）第 023214 号

※

国防工业出版社出版发行

（北京市海淀区紫竹院南路 23 号 邮政编码 100048）

北京奥鑫印刷厂印刷

新华书店经售

*

开本 787×1092 1/16 **印张** 21¾ **字数** 536 千字

2015 年 3 月第 1 版第 1 次印刷 **印数** 1—2500 册 **定价** 69.00 元（含光盘）

（本书如有印装错误，我社负责调换）

国防书店：（010）88540777 发行邮购：（010）88540776

发行传真：（010）88540755 发行业务：（010）88540717

对《NTFS 文件系统实例详解》书著的推荐

NTFS 文件系统是微软公司自 Windows NT 操作系统核心问世以来最引以为豪的一类磁盘数据存储及检索的基本系统，NTFS 文件系统结构在存储数据安全性、稳定性、容错性及拓展性方面都体现出良好的性能及效率。不过，NTFS 文件系统也因为结构复杂、关联技术多、运行开销较大，使用者熟悉和掌握这个系统有较大难度，甚至使人望而生畏。

随着个人计算机、互联网络和信息技术的进一步普及（包括客户端和服务端），Windows 操作系统已经成为个人用户常规信息平台之一。而且，在系统和信息安全、电子证据取证、计算机及网络司法鉴定等领域，涉及 Windows 操作系统的案例大量增加，针对 NTFS 文件系统及其数据处理（搜索、追踪、恢复、取证、统计等）也迅速提升。因此，需要我们从技术上、教学上、案例上提供相应的支撑。本书的撰写对 NTFS 文件系统领域的教学与研究又增加了一项有力的工具和参照。

本书是一本较详细的阐述 NTFS 文件系统的底层结构、数据关联结构、物理存储记录和读写操作流程的实用技术书籍。作者系统地讲述了 NTFS 文件系统的基本原理、总体布局、元文件记录结构、索引目录结构等。同时，以丰富的操作案例给读者展示了对 NTFS 文件系统的基本操作（如文件读写、搜索、删改、移动、复制等流程）和核心操作（如物理磁盘结构、数据记录结构、索引追溯链接、数据恢复技术等）。同时，本书各章节后也都配置了大量的思考题，帮助读者加深对章节内容的理解和实践操作。

本书所讨论的 NTFS 文件系统及其案例，主要以 Windows 7 系统为基础，也向前兼容 Windows XP；磁盘分析与管理软件采用著名的 WinHex，并指导读者借助软件工具对 NTFS 文件系统有更深入的理解，尤其是对数据的物理存储、文件布局、索引结构、链接方式、参数设置等进行直观的展现和操作。这些案例和操作过程，对读者建立系统性的知识具有有效的帮助，从而建立对 Windows 系统、文件、数据、记录结构、存储装置和存储介质的系统理解。这种理解将有助于信息安全、数据恢复、电子证据取证等领域的实践应用的技术提升。

本书内容与实际案例（实例素材）等紧密结合，既可作为高等院校和技术培训机构的教材使用，也可作为从事 NTFS 文件系统研究与教学工作的技术参考，也适合于从事有关 NTFS 文件系统下的数据恢复、电子证据取证以及其他有关人员自学和参考。

本书具有很好的实用价值，特推荐出版。

电子科技大学计算机科学与工程学院
计算机与网络取证与鉴定实验室主任
刘乃琦教授
2014 年 10 日

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，集中体现在高效和安全两大特性上。NTFS 文件系统早年在服务器领域得到了广泛应用。自微软公司推出 Windows 2000 和 Windows XP 以来，NTFS 文件系统在 PC 上得到了迅速普及。

NTFS 文件系统将会在相当长的一段时间内仍然是 Windows 系列操作系统的主要文件系统。然而在 NTFS 文件系统的设计者发表的官方资料中，很少涉及有关 NTFS 文件系统内核的资料或文章。在国外有关 NTFS 文件系统的书籍中，一般只介绍 NTFS 文件系统的基本特点；而在国内的一些有关 NTFS 文件系统的书籍中，也只是对 NTFS 文件系统进行了一些简单的介绍，没有发现比较系统、全面地介绍 NTFS 文件系统的资料或文章。这给基于 NTFS 文件系统下的电子取证、数据恢复、故障排除、系统维护或有关 NTFS 文件系统下的服务器磁盘阵列重组带来一定的困难。

因此，有必要对 NTFS 文件系统的基本原理、总体布局、元文件$MFT 记录等进行深入的探索研究，揭示 NTFS 文件系统的基本原理、总体布局以及基本操作对 NTFS 文件系统的影响等，为基于 NTFS 文件系统下，故障及时排除、系统维护、电子取证、数据恢复、有关 NTFS 文件系统下的服务器磁盘阵列重组提供科学的理论依据。

作者经过长时间的思考，认为有必要撰写一本有关 NTFS 文件系统的专著，以满足社会对 NTFS 文件系统学习研究者的需要。如何撰写才能让读者接受？根据长期教学经验，只有理论与实践相结合的书籍才会受到读者的喜爱。因此，本书在撰写过程中始终坚持 NTFS 文件系统的基本理论与案例（案例素材附光盘）相结合的原则，本书中所列举的案例在所附光盘中都能够找到相应的素材，从而形成了理论与实践的相互统一，为读者在较短的时间内学习掌握 NTFS 文件系统的基本原理、故障排除、数据恢复等提供一本不可多得的参考书目。

如果你使用的计算机操作系统是 Windows 7，可以将本专著所提供的素材复制到计算机的硬盘上，使用 Windows 7 操作系统计算机管理中的硬盘管理将素材文件附加成为虚拟硬盘，即可按本书的章节进行研究学习。

如果你使用的计算机操作系统是 Windows XP，可以下载并安装虚拟磁盘管理软件（如 InsPro Disk v2.0），将本专著所提供的素材复制到计算机的硬盘上，并将素材文件的扩展名“.vhd”改为“.hdd”，使用虚拟磁盘管理软件加载素材文件成为虚拟硬盘，同样也可以按本书的章节进行研究学习。

值得一提的是，在本书所附光盘中，有两个“.xls”文件，文件名分别为“数据运行列表定位算法.xls”和“元文件$MFT 的 B0H 属性记录号定位.xls”。读者通过“数据运行列表定位算法.xls”文件可以非常方便的将文件记录的数据运行列表转换成文件的开始簇号和结束簇号以及开始簇号和结束簇号在位图文件$Bitmap 中的位图位置。通过“元文件$MFT 的 B0H 属性

记录号定位.xls”文件可以非常方便地将元文件$MFT 的记录号在元文件$MFT 的 B0H 属性中定位，也可将元文件$MFT 的 B0H 属性的任意一位计算出所表示的记录号。

本书共分为 6 章，第 2 章～第 6 章、本书所附光盘上的素材及每章思考题参考答案由陈培德老师完成，每章后的思考题（注：附光盘）由吴建平老师完成，第 1 章由王丽清老师完成。本书的部分排版及校对由云南大学图书馆殷莉芬老师完成，全书由陈培德老师最后完成审稿及校对工作。

本书在策划与撰写过程中，得到了电子科技大学计算机科学与工程学院计算机与网络取证与鉴定实验室主任刘乃琦教授，云南大学省电子计算中心杨建国、代红兵、艾昌文、孙权以及 77200 部队自动化站郭昆等专家学者的大力支持并提出了许多建设性的意见和建议，在此表示由衷感谢。同时也感谢云南省高校数字媒体技术重点实验室以及国防工业出版社的支持与帮助，使得本书得以顺利出版。

学习的道路是没有尽头的，作者非常愿意与广大读者进行交流、共同进步、共同提高，同时也非常愿意为广大读者提供帮助和技术支持。

由于作者水平有限，书中难免存在某些疏漏和不足，恳请读者批评指正。

如果读者在使用本书时有什么意见或建议，请与我们联系，谢谢。

联系方式：1814433586@qq.com。

作　者

云南大学省电子计算中心

2014 年 10 月

目　录

第 1 章　NTFS 文件系统概述 …… 1

1.1　文件系统简介 …… 1
1.2　NTFS 文件系统 …… 2
1.2.1　NTFS 文件系统简介 …… 2
1.2.2　NTFS 文件系统的发展历史 …… 2
1.2.3　NTFS 文件系统的主要特性 …… 3
1.2.4　与 NTFS 文件系统有关的概念 …… 6
1.2.5　NTFS 文件系统的元文件和总体布局 …… 7
1.2.6　NTFS 文件系统引导扇区 …… 10
1.2.7　有关 NTFS 文件系统容量计算的公式 …… 15

第 2 章　元文件$MFT 文件记录结构 …… 16

2.1　元文件$MFT 概述 …… 16
2.1.1　元文件$MFT 的总体结构 …… 16
2.1.2　文件记录结构 …… 16
2.1.3　文件记录头结构 …… 18
2.1.4　记录属性及其分类 …… 20
2.2　文件和文件夹常用属性介绍 …… 25
2.2.1　10H 属性 …… 26
2.2.2　30H 属性 …… 28
2.2.3　80H 属性 …… 32
2.2.4　90H 属性 …… 38
2.2.5　A0H 属性 …… 52
2.2.6　B0H 属性 …… 53
2.3　文件和文件夹不常用属性介绍 …… 56
2.3.1　20H 属性 …… 56
2.3.2　40H 属性 …… 62
2.3.3　50H 属性 …… 63
2.3.4　60H 属性 …… 67
2.3.5　70H 属性 …… 68

2.3.6 C0H 属性 70
2.3.7 D0H 属性 71
2.3.8 E0H 属性 71
2.3.9 100H 属性 71

第 3 章 NTFS 文件系统的元文件 72

3.1 元文件$MFT 72
3.2 元文件$MFTMirr 84
3.3 元文件$LogFile 88
3.4 元文件$Volume 92
3.5 元文件$AttrDef 97
3.6 元文件“.” 103
3.7 元文件$Bitmap 106
3.8 元文件$Boot 111
3.9 元文件$BadClus 113
3.10 元文件$Secure 114
3.11 元文件$UpCase 117
3.12 元文件$Extend 118
3.13 元文件$Quota 119
3.14 元文件$ObjId 120
3.15 元文件$Reparse 122
3.16 元文件$RmMetadata 123
3.17 元文件$Repair 125

第 4 章 NTFS 索引节点结构、根目录与回收站 126

4.1 索引节点结构 126
4.2 B-树和 B+树的差异 130
4.3 小目录的 B-树结构 131
4.4 中目录的 B-树结构 135
4.5 大目录的 B-树结构 144
4.6 长文件名的 B-树结构 150
4.7 根目录的结构 155
4.8 回收站的结构 161
4.8.1 Windows XP 回收站的结构 161
4.8.2 Windows 7 回收站的结构 163

第 5 章 文件基本操作对 NTFS 元文件的影响 166

5.1 建立文件对$MFT 和索引目录等的影响 166

5.2 复制文件对$MFT 和索引目录等的影响 ····· 174
5.2.1 复制短文件名的小文件对$MFT 和索引目录等的影响 ····· 174
5.2.2 复制短文件名的大文件对$MFT 和索引目录等的影响 ····· 178
5.2.3 复制长文件名的小文件对$MFT 和索引目录等的影响 ····· 181
5.2.4 复制长文件名的大文件对$MFT 和索引目录等的影响 ····· 184
5.3 文件重命名对元文件$MFT 和索引目录的影响 ····· 189
5.3.1 短文件名重命名为短文件对$MFT 和索引目录的影响 ····· 189
5.3.2 短文件名重命名为长文件对$MFT 和索引目录的影响 ····· 194
5.3.3 长文件名重命名为短文件对$MFT 和索引目录的影响 ····· 196
5.3.4 长文件名重命名为长文件对$MFT 和索引目录的影响 ····· 200
5.4 删除文件对$MFT 和索引目录等的影响 ····· 202
5.4.1 删除短文件名的小文件对$MFT 和索引目录等的影响 ····· 202
5.4.2 删除短文件名的大文件对$MFT 和索引目录等的影响 ····· 222
5.4.3 删除长文件名的小文件对$MFT 和索引目录等的影响 ····· 228
5.4.4 删除长文件名的大文件对$MFT 和索引目录等的影响 ····· 230
5.4.5 删除多个短文件名的小文件对索引目录结构的影响 ····· 234
5.5 移动文件对索引目录的影响 ····· 239
5.5.1 移动短文件名的小文件对索引目录的影响 ····· 240
5.5.2 移动短文件名的大文件对索引目录的影响 ····· 242
5.5.3 移动长文件名的小文件对索引目录的影响 ····· 243
5.5.4 移动长文件名的大文件对索引目录的影响 ····· 244
5.6 同名文件被覆盖对 NTFS 元文件的影响 ····· 245
5.6.1 覆盖短文件名的小文件对 NTFS 元文件的影响 ····· 245
5.6.2 覆盖短文件名的大文件对 NTFS 元文件的影响 ····· 247
5.7 更改文件属性对$MFT 和索引目录的影响 ····· 254
5.8 编辑文件对$MFT、索引目录和位图文件的影响 ····· 256
5.9 通过位图文件计算磁盘已用空间和自由空间的基本方法 ····· 262
5.9.1 通过位图文件计算磁盘已用空间的基本方法 ····· 263
5.9.2 通过位图文件计算磁盘自由空间的基本方法 ····· 265
5.10 压缩卷对分区表及 NTFS 文件系统的影响 ····· 265
5.11 扩展卷对分区表及 NTFS 文件系统的影响 ····· 272

第 6 章 NTFS 文件系统下的数据恢复 ····· 274

6.1 文件被删除后的手工恢复 ····· 274
6.2 NTFS 的 DBR 被破坏的现象与手工恢复 ····· 276
6.3 NTFS 分区表被破坏的现象与手工恢复 ····· 284
6.4 分区表及 DBR 被破坏的现象与手工恢复 ····· 289

6.5 Windows 7 下快速格式化后的数据恢复 ····· 297
6.5.1 Windows 7 下 NTFS 被快速格式化成 FAT32 的恢复 ····· 297
6.5.2 Windows 7 下 FAT32 被快速格式化成 NTFS 的恢复 ····· 301
6.5.3 Windows 7 下 NTFS 被快速格式化成 NTFS 的恢复 ····· 302
6.6 Windows 7 下格式化后的数据情况 ····· 302
6.7 Windows XP 下快速格式化后的数据恢复 ····· 302
6.7.1 Windows XP 下 FAT32 被快速格式化成 NTFS 的恢复 ····· 302
6.7.2 Windows XP 下 NTFS 被快速格式化成 FAT32 的恢复 ····· 307
6.7.3 Windows XP 下 NTFS 被快速格式化成 NTFS 的恢复 ····· 308
6.8 Windows XP 下格式化后的数据恢复 ····· 309
6.8.1 Windows XP 下 FAT32 被格式化成 NTFS 的恢复 ····· 309
6.8.2 Windows XP 下 NTFS 被格式化成 FAT32 的恢复 ····· 310
6.8.3 Windows XP 下 NTFS 被格式化成 NTFS 的恢复 ····· 312
6.9 有关 NTFS 文件系统数据恢复案例 ····· 312

参考文献 ····· 335

第 1 章　NTFS 文件系统概述

1.1　文件系统简介

操作系统中负责管理和存储文件信息的软件称为文件管理系统，简称文件系统。它是操作系统的重要组成部分。文件系统由三部分组成：与文件管理有关的软件、被管理文件以及实施文件管理所需数据结构。从系统角度来看，文件系统是对文件存储器空间进行组织和分配，负责文件存储并对存入的文件进行保护和检索的系统。具体地说，它负责为用户建立文件、删除文件、读出文件、存入文件、控制文件的存取等。

常见的文件系统主要有 FAT（包括 FAT12、FAT16、FAT32 和 ExFAT）、NTFS、EXT、UFS、HPFS、HFS、CDFS、GFS 等，它们存在于不同的操作系统中，完成对数据的组织与管理，下面分别对这些文件系统作简单介绍。

1．FAT

FAT 是微软公司用于在 PC 中对数据和文件进行管理的文件系统，至今已发展包括了 FAT12、FAT16、FAT32、ExFAT，它们是以 FAT 表的表项长度来命名的。例如：表项长度为 12 位，则为 FAT12。

FAT12 是微软 DOS 操作系统中支持的一个文件系统，主要用于软磁盘等小容量设备的文件管理。

FAT16 管理分区存储容量可达到 2GB，不支持长文件名。一般情况下，如果没有作特别说明，FAT 指的就是 FAT16。

FAT32 文件系统随 Windows 95 操作系统发布，FAT32 与 FAT16 相比较，大大增强了对磁盘的管理能力，存储效率比 FAT16 提高了 15%，可管理的分区容量也达到了 32GB，但目前已被性能更优越的 NTFS 文件系统所取代。

ExFAT（Extended File Allocation Table）也叫 FAT64，是微软公司在 Windows Embedded CE6.0 中引入的一种适合于闪存的文件系统，后又用到 Windows Vista SP1 中，主要用于 U 盘闪存、嵌入式系统等场合。

2．NTFS

NTFS 是 Windows NT 引入的新型文件系统，它具有许多优秀的新特性，也是本书重点讨论的内容，详见 1.2 节。

3．UFS

UFS 文件系统是 UNIX 文件系统的简称，是 Solaris 的默认文件系统，具有日志记录功能。在 UFS 中，重要数据结构的复制贯穿于整个文件系统，并且数据做到了局部化，因此在读取文件的时候，磁头的运动量大大降低。UFS 使用“柱面组”对数据进行分段组织，每个柱面组的大小与磁盘的几何特性关联。

4．EXT

EXT 是 Linux 操作系统中采用的文件系统。基于 UFS，是一种快速、稳定的文件系统。

目前已推出了 EXT2、EXT3、EXT4 版本。其中：EXT2 文件系统是非日志式文件系统，EXT3 文件系统是 EXT2 的升级版，增加了日志功能。而 EXT4 在 EXT3 的基础上对数据结构进行了改进，提高了可靠性，可支持无限数量的子目录，文件大小可支持到 16TB，而 EXT3 仅支持到 2TB 的文件。

5. HPFS

HPFS（High Performance File System）是 OS/2 操作系统所支持的文件系统。HPFS 保留了 FAT 的目录组织，增加了基于文件名的自动目录排序功能。HPFS 允许由“数据”和特殊属性组成文件，从而在支持其他命名规则和安全性方面增加了灵活性。

6. HFS

HFS 是由苹果公司开发，并使用在 Mac OS 上的文件系统。1985 年诞生在 Macintosh 计算机。此后又在此基础上开发了 HFS+文件系统。HFS+也被称为 Mac OS Extended，是一个 HFS 的改进版本，支持更大的文件，并用 Unicode 码来命名文件或文件夹名，代替了 Mac OS Roman 或其他一些字符集。

7. CDFS

CDFS（Compact Disc File System）是一种适合光存储的文件系统。CDFS 管理 CD 格式文件，即音轨文件。部分 U 盘也可通过量化软件进行 CDFS 系统化，如银行的网银 U 盾 HDZB_USBKEY 就使用这样的方法。

8. GFS

由于 Google 的迅速增长带来的巨大数据处理要求，Google 设计并实现了 GFS（Google File System）。GFS 是一个可扩展的分布式文件系统，用于大型、分布式、对大量数据的访问和管理，具有容错功能。

9. RAW

RAW 文件系统是一个没有被 Windows 操作系统识别的磁盘分区格式。

1.2 NTFS 文件系统

1.2.1 NTFS 文件系统简介

NTFS（New Technology File System）是运行于 Windows NT 操作系统环境和 Windows NT 高级服务器网络操作系统环境的文件系统，随着 Windows NT 操作系统的诞生而产生。特别针对网络、磁盘配额、文件加密等管理安全特性进行设计，其结构比 FAT32 文件系统要复杂得多，支持文件系统故障恢复，尤其是大容量存储媒体、长文件名。

NTFS 文件系统的设计目标就是用来在大容量硬盘上支持快速、安全、高效的读/写和检索操作，由于其优秀的结构设计，使它具有安全性高、稳定性好、不易产生文件碎片的优点，并且在充分理解了 NTFS 文件系统的管理机制和原理后，能快速借助其容错结构日志等实现 NTFS 上的数据恢复，这也是本书所以花费大量篇幅以实例方式详细介绍 NTFS 文件系统管理机制的原因。

1.2.2 NTFS 文件系统的发展历史

20 世纪 90 年代早期，微软公司和 IBM 公司共同组建了一个联合计划，其目标是创建一个下一代的操作系统，并由此诞生了 OS/2 操作系统。但由于微软公司和 IBM 公司在很多重要

问题上不能达成共识，OS/2 操作系统最终归属 IBM 公司。OS/2 操作系统使用了 HPFS 文件系统，微软公司从 HPFS 文件系统中汲取有关文件系统方面的特性和经验开发了 NTFS 文件系统。也许正因为如此，HPFS 文件系统和 NTFS 文件系统共享了相同的 MBR 分区标识代码（即 0X07），因此，在用于区分文件系统的算法时，当遇到代码 0X07 的时候需要进行额外的检查，才能区分出文件系统是 NTFS 还是 HPFS。

到目前为止，微软公司发布了如下 NTFS 文件系统的正式版本。

NTFS V1.0，1993 年 7 月份随 Windows NT3.1 一起发布；

NTFS V1.1，1994 年秋季随 Windows NT3.5 一起发布（注：NTFS V1.0 和 NTFS V1.1 与以后所有的版本都不兼容）；

NTFS V1.2（也称为“NTFS 4.0”），1995—1996 年随 Windows NT3.51 和 Windows NT4.0 一起发布，NTFS V1.2 支持压缩文件、命名流、基于 ACL（访问控制列表）的安全性等功能；

NTFS V3.0（也称为“NTFS 5.0”），用于 Windows 2000，NTFS V3.0 支持磁盘限额、加密、稀疏文件、重解析点，更新串行数（USN）日志、$Extend 文件夹以及其中的文件，并改进了安全描述符，以便于使用相同安全设置的多个文件共享一个安全描述符；

NTFS V3.1（也称为“NTFS 5.1”），于 2001 年秋季用于 Windows XP，并于 2003 年春季在 Windows Server 2003 发布了“NTFS 5.2”，2005 年中旬在 Windows Vista 发布了“NTFS 6.0”，2008 年初在 Windows Server 2008、Windows Server 2008 R2 以及 Windows 7 上发布了“NTFS 6.1”。

1.2.3 NTFS 文件系统的主要特性

NTFS 文件系统具备以下主要特性。

1．安全性

数据安全性对于处理私人或敏感信息的客户（如银行、医院以及国防安全机构等）至关重要。NTFS 的安全性很高，它提供了许多安全性能方面的选项，可以在本机也可以通过远程的方法保护文件和目录。同时，它还支持加密文件系统（EFS）、可以阻止没有授权的用户访问文件。

2．可恢复性

NTFS 文件系统数据存储的可靠性强，比较适合用于服务器，因为其提供了基于原子事务概念的文件系统可恢复性。原子事务是数据中处理数据更新的一项技术，可保证即使系统失败也不影响数据库的正确和完整。

NTFS 文件系统中设计了极强的恢复能力，无需用户在 NTFS 卷中运行磁盘修复程序即可恢复数据。在系统崩溃事件中，NTFS 文件系统使用日志文件和更新点信息，自动恢复文件系统的一致性。

3．数据冗余容错性

除了文件系统数据的可恢复性外，在断电或灾难发生时，如何最大限度避免灾难性的系统失败所带来的数据危害。NTFS 的恢复功能确保了卷中的文件系统的可访问性，为避免文件数据损失风险，采用数据冗余提供额外的保护。

4．大容量磁盘和文件管理能力

随着计算机应用的发展，经常要存储和处理大容量的数据和信息。NTFS 实现了对大容量磁盘和大数据文件的支持。NTFS 也使用簇对磁盘进行分配，并使用 64 位代码对簇进行编号，这样就可以产生 2^{64} 个簇号，每个文件可以长达 2^{64} 字节，满足了大容量数据存储的需求。

5．文件压缩特性

NTFS 文件系统具有文件压缩功能，可压缩单个文件或整个文件夹。对那些不经常使用的数据或较大的文件可以使用 NTFS 的压缩功能对其进行压缩以便节约磁盘空间。NTFS 系统的压缩机制可让用户直接读/写压缩文件，而不需要使用解压软件将这些文件解压。

6．支持稀疏文件

稀疏文件是应用程序生成的一种特殊文件，文件尺寸非常大，但实际上只需要很少的磁盘空间，NTFS 为稀疏文件实际写入的数据分配磁盘存储空间。

7．保留的文件名

NTFS 文件系统支持最长 32767 个 Unicode 字符的路径，但是包括目录或文件名的每个路径组成部分最多只允许包含 255 个字符，同时某些特定的名称需要用于保存 NTFS 元文件，元文件都存放在卷的根目录下，这些特定名称被禁止用于普通文件名或目录名，被 NTFS 保留的文件名有：$MFT、$MFTMirr、$LogFile、$Volume、$AttrDef、“.”（即根目录）、$Bitmap、$Boot、$BadClus、$Secure、$Upcase、$Extend 等。在这些名称中，“.”（即根目录）和$Extend 是目录类型，其他名称均为文件类型。

8．最大卷尺寸

NTFS 理论上最大支持的卷尺寸为 $2^{64}-1$ 个簇。但目前在 Windows XP 中实现 NTFS 卷的最大尺寸是 $2^{32}-1$ 个簇。例如：如果簇大小为 64KB，则 NTFS 卷的最大尺寸是 256TB 减去 64KB；如果簇的尺寸是用默认大小（4KB），则 NTFS 卷的最大尺寸是 16TB 减去 4KB。另外，由于主引导记录（MBR）上的分区表支持的单个分区容量最大为 2TB，因此如果 NTFS 卷的尺寸超过 2TB，则必须创建为动态卷或者 GPT 卷。

9．支持活动目录和域

此特性使得用户能够方便灵活地查看和控制网络资源。

10．机会锁

机会锁允许网络客户端改变对文件或数据流的缓存策略，以便于增强性能或降低网络占用。机会锁应用到文件某个打开的流上，不影响同一个文件的其他流。机会锁可以用于在后台透明访问文件。如果没有其他进程访问服务器文件，网络客户端可以避免向文件写入数据；而如果没有其他进程正在写入数据，客户端可以缓存即将读取的数据。

11．磁盘配额

磁盘配额是管理员为用户所能使用的磁盘空间进行的配额限制。每一用户只能使用最大配额范围内的磁盘空间。设置磁盘配额后，可以对每一用户的磁盘使用情况进行跟踪和控制，通过监测可以标识超过配额报警阈值和配额限制的用户，从而采取相应的措施。磁盘配额管理能力的提供，使管理员可以方便合理地为用户分配存储空间，避免由于磁盘空间使用的失控造成系统崩溃，提高了系统的安全性。

12．对文件目录采用 B-树进行管理

NTFS 对文件目录采用 B-树进行管理，这种技术比在 FAT 文件系统中使用链表技术来管理优越得多。NTFS 文件夹的 B-树结构使得用户在访问较大文件夹中的文件时，速度甚至比访问卷中较小的文件夹中的文件还要快。在 NTFS 中文件名是按顺序存放的，因而查找速度更快，当文件目录不断增加时，B-树会在宽度上增加，而不会在深度上增长。

13．多数据流

在 NTFS 中，每个与文件有关的信息单元，包括文件名、文件所有者、文件的时间标记、

文件的内容等，都作为文件属性（对象属性）来执行。每个属性由单个的“流”组成，即简单的字节队列。这种普通的实现方式可容易地为每个文件添加更多的属性。因为文件的数据仅仅是文件的“另一个属性”，并且因为可以添加新的属性，NTFS 文件（或文件目录）可以包含多个数据流。

14．基于 Unicode 命名文件

Unicode 是 16 位字符编码方案，允许世界上的每种主要语言中的每个字符被唯一地表示。NTFS 完全使用 Unicode 字符来存储文件名、目录和卷。

15．可靠性

在 NTFS 文件系统中，逻辑 0 扇区也就是引导扇区（即 DBR），保存着该分区的 BPB 参数和分区引导代码。并将该文件系统中最重要的文件也就是主文件（Master File Table，$MFT）存储在分区的某一位置，从而使得该文件不易被破坏，从而大大提高了 NTFS 文件系统的稳定性和安全性。但这种将$MFT 放在分区中某一位置的做法也存在瑕疵，如果 DBR 中的 BPB 参数指向$MFT 的开始簇号不正确，那么 NTFS 文件系统不知道去哪里寻找$MFT，从而会报告“文件或目录损坏且无法读取”的错误提示信息。为了确保 DBR 的安全，在 NTFS 分区的最后一个扇区保存了 DBR 的一个备份（注：该扇区不属于 NTFS 文件系统），一旦逻辑 0 扇区（即 DBR）被破坏，用户可以将该扇区（即 DBR 备份）复制到逻辑 0 扇区，即可恢复逻辑 0 扇区（即 DBR），使得 NTFS 文件系统恢复正常。

16．高效性

对于 FAT 文件系统中文件的属性有只读、隐藏、系统、归档四种。而在 NTFS 文件系统中，在这些属性基础上极大扩展了属性的概念。在 NTFS 文件系统中，一切都是一种属性，包括文件内容。这些属性的列表不是固定的，可以随时增加，这也就是为什么你会在 NTFS 分区上看到文件有更多属性的原因。

NTFS 文件系统中的文件属性分成两种：常驻属性和非常驻属性。常驻属性直接保存在$MFT 中，像文件名和相关时间信息（如创建时间、修改时间等）属于常驻属性，非常驻属性则保存在$MFT 之外，但会使用数据运行列表来指明文件存储的位置，一般情况下，文件或文件夹小于 1500 字节，那么它们的所有属性，包括内容都会常驻在$MFT 的记录中，而$MFT 是 Windows 一启动就会载入到内存中，这样当你查看这些文件或文件夹时，其实它们的内容早已在缓冲区中，从而大大地提高了文件和文件夹的访问速度。

17．磁盘自我修复功能

NTFS 是一种“自我疗伤”的系统，可以对硬盘上的逻辑错误和物理错误进行自动侦测和修复。每次读/写时，都会检查扇区的正确性。一旦发现读取错误，NTFS 会报告这个错误；当向磁盘写文件时发现错误，NTFS 将会自动换一个完好扇区存储数据。在这两种情况下，NTFS 都会在坏扇区所对应的簇号上作标记，以防止今后被使用。这种工作模式可以使磁盘错误较早地被发现，避免了数据丢失事故的发生。

18．事件日志功能

在 NTFS 文件系统中，任何操作都可以被看成是一个“事件”。比如将一个文件从 C 盘复制到 D 盘，整个复制过程就是一个事件。事件日志一直监督并记录着整个操作，当它在目标盘 D 盘发现了文件完整后，就会记录下一个“已完成”的标记。假如复制中途断电，事件日志中就不会记录“已完成”，NTFS 可以在来电后重新完成刚才的事件。事件日志的作用不在于它能挽回损失，而在于它监督所有事件，从而让系统知道完成了哪些任务，哪些任务还没

有完成，保证系统不会因为断电等突发事件发生紊乱，最大程度降低了破坏性。

19. 数据加密

NTFS 支持磁盘数据加密，加密文件系统（Encrpyted File System，EFS）是 NTFS 支持的一个重要特性，可以对用户赋予单个文件和文件夹权限。

20. 文件系统的转换

可以将 FAT 文件系统转换成 NTFS 文件，但其性能会有折扣，如果分区是从 FAT32 转换为 NTFS 文件系统（使用命令为“CONVERT 驱动器盘符/FS:NTFS”），不仅$MFT 会很容易出现磁盘碎片，更糟糕的是，磁盘碎片整理工具往往不能整理这个分区中的$MFT，因而严重影响到系统性能。因此，建议将分区直接格式化为 NTFS 文件系统，以保证系统获得较高的性能。

21. 附加功能

NTFS 提供了为不同用户设置不同访问控制、隐私和安全管理的功能。

1.2.4 与 NTFS 文件系统有关的概念

在学习研究 NTFS 文件系统时，经常会遇到一些与 NTFS 文件系统有关的概念，下面对这些概念分别进行解释说明。

（1）分区：分区是磁盘的基本组成部分，被划分的磁盘的一部分，是一个能够被格式化和单独使用的逻辑区域。

（2）卷：NTFS 是以卷为基础，卷建立在磁盘分区之上，当以 NTFS 格式来格式化磁盘分区时就创建了 NTFS 卷，一个磁盘可以有多个卷，一个卷也可以由多个磁盘组成。

（3）簇：NTFS 与 FAT32 一样，使用簇作为磁盘空间分配和回收的基本单位，即一个文件占用若干个整簇，而最后一簇的剩余空间不再使用。在内部，NTFS 仅引用簇，而不知道磁盘扇区的大小。这样使 NTFS 保持了与物理扇区大小的独立性，能够为不同大小的磁盘选择合适的簇。卷上簇的大小（称为簇因子）是用户使用 Format 命令或其他格式化程序格式化卷时确定的，它随着卷的大小而不同，但都为物理扇区的整数倍。簇的定位可使用逻辑簇号（LCN）和虚拟簇号（VCN）。

（4）逻辑簇号（LCN）：LCN 对卷中所有的簇号从头到尾进行简单顺序编号。

（5）虚拟簇号（VCN）：VCN 对属于特定文件的簇号从 0 到 m 编号（注：文件的总簇数为 m+1），以便引用文件中的数据，VCN 不要求在物理上连续，可以映射到卷上任何的 LCN。

（6）主文件表（$MFT）：在 NTFS 中，卷中存放的所有数据，包括用于定位和恢复文件的数据结构、引导程序数据和记录整个卷的分配状态的位图，都包含在一个称为主文件表（$MFT）的文件中，$MFT 是 NTFS 卷结构的核心，是 NTFS 最重要的系统文件。$MFT 由文件记录组成，每个文件记录的大小为 1KB，卷上每个文件（包括$MFT 本身）或者文件夹都在元文件$MFT 中都有一条记录，有个别的文件或文件夹有 2 条甚至 3 条记录。

（7）文件引用号：NTFS 卷中的文件是通过称为“文件引用号”的 64 位值来标识的。文件引用号由文件记录号（低 48 位）和文件顺序号（高 16 位）组成。文件记录号对应文件在$MFT 中的位置，顺序号随文件记录的使用而增加，从而使得 NTFS 能完成内部的一致性检查。

（8）文件记录：NTFS 不是将文件仅仅视为一个文本库或二进制数据，而是将文件作为许多属性和属性值的集合来处理，除数据属性外，其他文件属性包括文件名、文件时间标记、文件拥有者等，每个文件或文件夹在元文件$MFT 均有一个文件记录号。

（9）文件名：NTFS 中的每个文件名或者目录名长度可达 255 字节，可以包含 Unicode 字

符、多个句点和空格。MS-DOS 不能正确识别 Win32 的文件名，因此，NTFS 自动生成 8 个字符（加 3 个字符的扩展名）以内的 MS-DOS 文件名。POSIX 子系统需要 Windows NT 支持的所有应用程序环境中最大的名字空间，因此，NTFS 的名字空间等于 POSIX 的名字空间。POSIX 子系统可以创建在 Win32 和 MS-DOS 中不可见的名称。

（10）常驻属性：若文件的属性值能直接存储在$MFT 记录中时，该属性称为常驻属性。一般情况下，小文件或小目录的所有属性均直接存储在$MFT 记录中。如果属性值直接存放在$MFT 中，则 NTFS 只需访问磁盘一次即可获得数据。

（11）非常驻属性：若文件的内容（文件体）比较大，不能直接存储在$MFT 记录中，需要在$MFT 之外为其分配足够的空间进行存储，该属性称为非常驻属性。一般情况下，大文件或大目录的记录属性为非常驻属性；而小文件或小目录的记录属性为常驻属性；但是有的小文件或小目录的记录属性也可能是非常驻属性，这些小文件或小目录往往是由大文件或大目录通过删除文件内容或目录中的文件改变而来。

（12）文件名索引：在 NTFS 中，文件目录仅仅是文件名的一个索引，即为了便于快速访问而用一种特殊的方式组织起来的文件名的集合。要创建一个目录，NTFS 应对目录中文件的文件名属性进行索引。

（13）数据压缩：NTFS 压缩功能可以对单个文件、整个目录或卷上的整个目录树进行压缩，NTFS 压缩只能在用户数据上执行，而不能在文件系统元数据上执行。数据压缩可减少磁盘使用空间，但每次解压缩需要大量数据运算，如果要复制一个压缩文件，过程是解压缩、复制、重新压缩复制的文件。

1.2.5 NTFS 文件系统的元文件和总体布局

从整体结构上讲，NTFS 文件系统由元文件、用户文件以及数据组成。NTFS 系统在创建时，会将一些重要的系统信息以文件的形式进行存储，存储这些重要信息所对应的文件就是元文件，它是 NTFS 系统最重要的部分。

在 NTFS 元文件中最重要的元文件就是$MFT。$MFT 决定了 NTFS 文件系统中所有文件或者文件夹在卷上的位置。$MFT 是一个数据库，由一系列文件记录组成。卷中每一个文件都有一个文件记录号，文件记录编号从 0 开始，其中 0 号文件记录称作基本文件记录，也就是$MFT 本身。$MFT 中的文件记录大小一般是固定的，不管簇的大小是多少，均为 1024 字节（1KB），（在 DBR 中有描述）。其中：记录号从 0～11 的前 12 号记录是 NTFS 文件系统中最基本、也是最重要的元文件。除根目录外，元文件的文件名均以“$”符号开头，元文件是隐藏的系统文件，用户不能直接对元文件进行访问，在资源管理器中也看不到 NTFS 文件系统的元文件。

NTFS 文件系统的总体布局如图 1.1 所示。

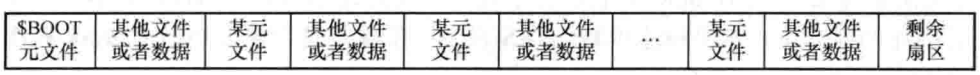

图 1.1 NTFS 文件系统的总体布局

从图 1.1 可知，NTFS 的元文件是分散地存储在逻辑盘（或者卷）中。整个 NTFS 文件系统中是以簇为单位来分配磁盘空间的。而在分区时，总扇区数不一定是簇的倍数，因此有可能会出现剩余扇区，剩余扇区一般大于或等于 1 个扇区而小于 1 个簇（即最后不能够成一个