硬盘之解读NTFS计算机等级考试 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/644/2021_2022__E7_A1_AC_E7_9B_98_E4_B9_8B_E8_c98_644351.htm 解读NTFS NTFS是一个比FAT复杂的多的文件系统，我们一起努力来把它完整的解读出来 NTFS的引导扇区也是完成引导和定义分区参数，和FAT分区不同，FAT分区的BOOT记录正常，就显示分区没有错误，即使文件不正确，而 NTFS分区 的BOOT不是分区的充分条件，它要求必须MFT中的系统记录如$MFT等正常该分区才能正常访问。其BPB参数如下表所示。 字节偏移 长度 常用值 意义 0x0B 字 0x0002 每扇区字节数 0x0D 字节 0x08 每簇扇区数 0x0E 字 0x0000 保留扇区 0x10 3字节 0x000000 总为0 0x13 字 0x0000 NTFS未使用，为0 0x15 字节 0xF8 介质描述 0x16 字 0x0000 总为0 0x18 字 0x3F00 每磁盘扇区数 0x1A 字 0xFF00 磁头数 0x1C 双字 0x3F000000 隐含扇区 0x20 双字 0x00000000 NTFS未使用，为0 0x28 8字节 0x4AF57F0000000000 扇区总数 0x30 8字节 0x0400000000000000 $MFT的逻辑簇号 0x38 8字节 0x54FF070000000000 $MFTMirr的逻辑簇号 0x40 双字 0xF6000000 每MFT记录簇数 0x44 双字 0x01000000 每索引簇数 0x48 8字节 0x14A51B74C91B741C 卷标 0x50 双字 0x00000000 检验和 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1KB。文件记录在MFT文件记录数组中物理上是连续的，且从0开始编号，所以， NTFS 是预定义文件系统。MFT仅供系统本身组织、架构文件系统使用，这在NTFS中称为元数据（metadata，是存储在卷上支持文件系统格式管理的数据。它不能被应用程序访问，只能为系统提供服务）。

其中最基本的前16个记录是操作系统使用的非常重要的元数据文件。这些元数据文件的名字都以“$”开始，所以是隐藏文件，在Windows 2000/XP中不能使用dir命令（甚至加上/ah参数）像普通文件一样列出。在WINHEX中带有NFI.EXE，用此工具可以显示这些记录与文件的对应关系，下一次再详细解释。 这些元数据文件是系统驱动程序管理卷所必需的，Windows 2000/XP给每个分区赋予一个盘符并不表示该分区包含有Windows 2000/XP可以识别的文件系统格式。如果主文件表损坏，那么该分区在Windows 2000/XP下是无法读取的。为了使该分区能够在Windows 2000/XP下能被识别，就必须首先建立Windows 2000/XP可以识别的文件系统格式即主文件表，这个过程可通过高级格式化该分区来完成。Windows以簇号来定位文件在磁盘上的存储位置，在FAT 格式的文件系统中，有关簇号的指针包含在FAT表中，在NTFS中，有关簇号的指针则包含在$MFT及$MFTMirr文件中。 NTFS使用逻辑簇号（Logical Cluster Number，LCN）和虚拟簇号（Virtual Cluster Number，VCN）来对簇进行定位。LCN是对整个卷中所有的簇从头到尾所进行的简单编号。用卷因子乘以LCN，NTFS就能够得到卷上的物理字节偏移量，从而得到物理磁盘地址。VCN则是对属于特定文件的簇从头到尾进行编号，以便于引用文件中的数据。VCN可以映射成LCN，而不必要求在物理上连续。 在NTFS卷上，跟随在BPB后的数据字段形成一个扩展BPB。这些字段中的数据使得 Ntldr能够在启动过程中找到主文件表MFT（Master File Tabl ）。在NTFS卷上，MFT并不象在FAT 16卷和FAT 32卷上一样，被放在一个预定义的扇区中。由于这个原因，如果在MTF的正常位置中有

坏扇区的话，就可以把MFT移到别的位置。但是，如果该数据被破坏，就找不到MFT的位置，Windows 2000假设该卷没有被格式化。 因此，如果一个ntfs的卷提示未格式化，可能并未破坏MFT,依据BPB的各字段的意思是可以重建BPB的。 NTFS的缺省簇的大小 卷大小 每簇的扇区 缺省的簇大小 小于等于512MB 1 512字节 513MB~1024MB(1GB) 2 1024字节(1KB) 1025MB~2048MB(2GB) 4 2048字节(2KB) 大于等于2049MB 8 4KB 从上面可以看出，也就是说不管驱动器多大 NTFS 簇的大小不会超过 4KB NTFS文档：文档属性定义 每个文档属性都由以下部分组成： 一个由该属性的实际值组成的被称为“流”的重要的字节序列，元数据可访问该流。 文件中的每个文件属性都可能会有一个名字：在这种情况下，在命令行方式下可以通过语法“ 文件名：属性名 ”来访问该流（这也是文件名中不能使用“ ：”的原因）。Windows NT 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com