说明：

MBR ：Master Boot Record ( 主引导记录)

DBR ：DOS Boot Record ( 引导扇区)

FAT ：File Allocation Table ( 文件分配表)

硬件：本文SD卡为Kingston 4GB，FAT32格式，簇大小4KB，每扇区512字节。

**第一章 硬盘结构与SD卡结构**

**1.1 硬盘介绍**

**1.1硬盘结构**

如果你熟悉硬盘结构跳过本节。下图是硬盘的结构，如果你只是为了学习SD卡FAT32文件系统的话，这里你只需要注意硬盘排序结构：主引导记录（MBR）—引导扇区—数据—引导扇区—数据。

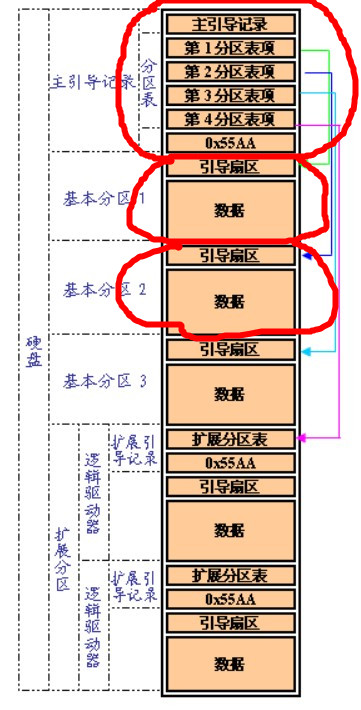


图1

**1.2 MBR分析**

MBR（Main Boot Record 主引导记录区）放置在硬盘物理地址0的地方。总共512字节的主引导扇区中，MBR只占用了其中的446个字节，另外64个字节交给了 DPT（Disk Partition Table硬盘分区表），最后两个字节“55，AA”是分区的结束标志。DPT由4个分区表组成，每个16字节。下图中以以硬盘的MBR图，粉红色为硬盘分区表。

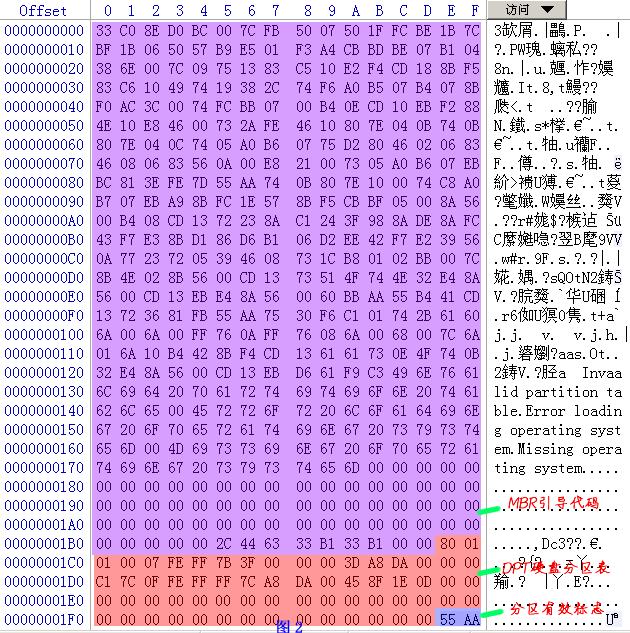


图2

对于我们来说，更关注硬盘分区表表中红色区域：下图为硬盘分区表详细说明 。如果要对SD卡、U盘等分多个区，DPT的内容就表示各个区的偏移地址和大小。

|  |  |  |
| --- | --- | --- |
| 起始地址 | 字节数 | 描述 |
| 0x1BE | 1 | 可引导标志，0x00不可引导，0x80可引导 |
| 0x1BF~0x1C1 | 3 | 分区起始CHS地址(CHS＝磁头、柱面、扇区)，起始地址 |
| 0x1C2 | 1 | 分区类型 |
| 0x1C3~0x1C5 | 3 | 分区结束CHS地址 |
| 0x1C6 | 4 | 从磁盘开始到该分区开始的偏移量（分区起始LBA地址Little-endian顺序） |
| 0x1CA | 4 | 总扇区数（Little-endian顺序） |



图3

**SD结构**

SD卡没有分区，默认就是一个分区。首先用WinHex文件打开SD所在的盘符，显示如下图：



图4

①　非分区空间（红线所示）: 起始扇区0，我认为这个分区就是硬盘上的MBR所在区域，

打开后如下图所示,也可以称为SD卡的MBR区域。

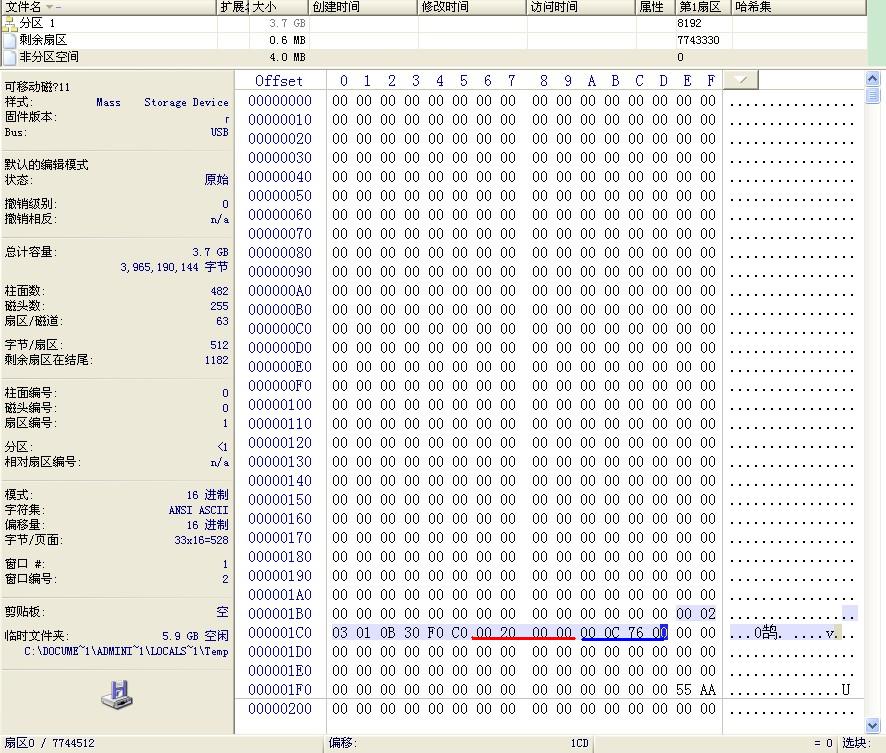


图5

根据表1知道：

红线区域（00002000）为下个分区的扇区地址，即第8192扇区，见图3分区1的起始扇区。

蓝线区域（00760C00）为SD卡总的扇区个数，我们可以计算一下：

     0x760C00 \*512（每扇区字节）= 3960995840 （字节），与实际大小基本一样。

②　分区1（蓝线所示）：起始扇区8192.

③　剩余扇区    : 才疏学浅，我不知道干嘛的，呵呵

**1.3 SD卡存储结构**

由此可知SD卡文件系统并不是处在整个SD卡最开始的地方，它处在MBR所处的保留区之后，于是我们可以对使用FAT32文件系统的SD卡整体布局给出如下图示。



图6

**第二章****FAT32文件系统介绍**

**2.1 FAT文件系统简介**

FAT（File Allocation Table，文件分配表）文件系统是windows操作系统所使用的一种文件系统，它的发展过程经历了FAT12、FAT16、FAT32三个阶段。FAT文件系统用“簇”作为数据单元。一个“簇”由一组连续的扇区组成，簇所含的扇区数必须是2的整数次幂。簇的最大值为64个扇区，即32KB。所有簇从2开始进行编号，每个簇都有一个自己的地址编号。用户文件和目录都存储在簇中。 本文每簇4KB大小。

FAT文件系统的数据结构中有两个重要的结构：文件分配表和目录项：

文件分配表：文件和文件夹内容储存在簇中，如果一个文件或文件夹需要多余一个簇的空间，则用FAT表来描述，如何找到另外的簇。FAT结构用于指出文件的下一个簇，同时也说明了簇的分配状态。FAT12、FAT16、FAT32这三种文件系统之间的主要区别在与FAT项的大小不同。

目录项：FAT文件系统的每一个文件和文件夹都被分配到一个目录项，目录项中记录着文件名、大小、文件内容起始地址以及其他一些元数据。

在FAT文件系统中，文件系统的数据记录在“引导扇区中（DBR）”中。引导扇区位于整个文件系统的0号扇区，是文件系统隐藏区域（也称为保留区）的一部分，我们称其为DBR（DOS Boot Recorder——DOS引导记录）扇区，DBR中记录着文件系统的起始位置、大小、FAT表个数及大小等相关信息。在FAT文件系统中，同时使用“扇区地址”和“簇地址”两种地址管理方式。这是因为只有存储用户

数据的数据区使用簇进行管理（FAT12和FAT16的根目录除外），所有簇都位于数据区。其他文件系统管理数据区域是不以簇进行管理的，这部分区域使用扇区地址进行管理。文件系统的起始扇区为0号扇区。

**2.2 FAT32文件系统结构**

FAT文件系统整体分布如上图 存储器文件结构图 所示，有：

【1深绿色】保留区含有一个重要的数据结构——系统引导扇区（DBR）。FAT12、FAT16的保留区通常只有一个扇区，而FAT32的保留扇区要多一些，除0号扇区外，还有其他一些扇区，其中包括了DBR的备份扇区。

【2黄色】  FAT区由来年各个大小相等的FAT表组成——FAT1、FAT2，FAT2紧跟在FAT1之后。

【3灰色】  FAT12、FAT16的根目录虽然也属于数据区，但是他们并不由簇进行管理。也就是说FAT12、FAT16的根目录是没有簇号的，他们的2号簇从根目录之后开始。而FAT32的根目录通常位于2号簇。

**2.2.1 保留区（深绿色区域）**

FAT32文件系统的开始部分有一个由若干个扇区组成的保留区，保留区的大小会记录在DBR扇区中，比较常见的为32、34或38个扇区。如上图：由DBR中）0x0e和0x0f两个地址的数值决定，记得是小端模式，即N的值。

**2.2.1.1 引导扇区（DBR）**

【大小】：512字节；

对读写FAT文件系统来说常用的就图中红色划线部分，48个字节。其他的均为一些标注信息。想了解具体的定义请看附录表。

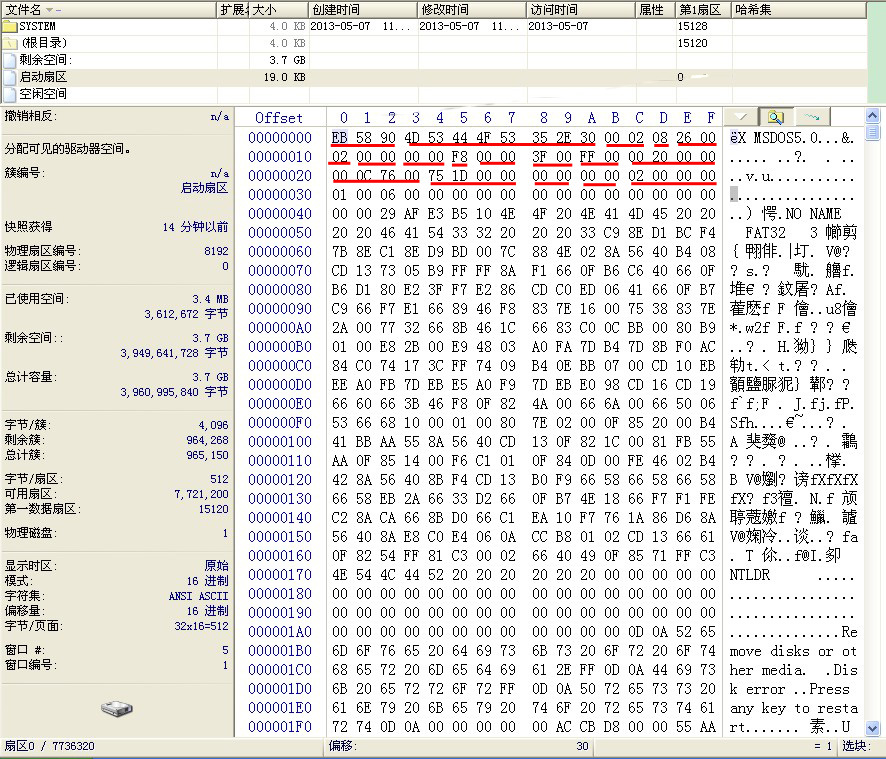


图7

【1】0x00~0x02：3字节，跳转指令。

【2】0x03~0x0A：8字节，文件系统标志和版本号，这里为MSDOC5.0。

【3】0x0B~0x0C：2字节，每扇区字节数，512（0X02 00）。

【4】0x0D~0x0D：1字节，每簇扇区数，8（0x08）。

【5】0x0E~0x0F：2字节，保留扇区数，38（0x00 26），符合FAT1起始地址为38扇区。

【6】0x10~0x10：1字节，FAT表个数，2。

【7】0x11~0x12：2字节，FAT32必须等于0，FAT12/FAT16为根目录中目录的个数；

【8】0x13~0x14：2字节，FAT32必须等于0，FAT12/FAT16为扇区总数。

【9】0x15~0x15：1字节，哪种存储介质，0xF8标准值，可移动存储介质，常用的 0xF0。

【10】0x16~0x17:2字节，FAT32必须为0，FAT12/FAT16为一个FAT 表所占的扇区数。

【11】0x18~0x19：2字节，每磁道扇区数，只对于有“特殊形状”（由磁头和柱面每 分割为若干磁道）的存储介质有效，63（0x00 3F）。

【12】0x1A~0x1B：2字节，磁头数，只对特殊的介质才有效，255（0x00 FF）。

【13】0x1C~0x1F：4字节，EBR分区之前所隐藏的扇区数，8192（0x00 00 20 00），与MBR中地址0x1C6开始的4个字节数值相等。

【14】0x20~0x23：4字节，文件系统总扇区数，7736320（0x 00 76 0C 00），7736320 \*  512 = 3960995840  ≈ 3.67GB。

【15】0x24~0x27：4字节，每个FAT表占用扇区数，7541（0x 00 00 1D 75）。

【16】0x28~0x29：2字节，标记，此域FAT32 特有。

【17】0x2A~0x2B：2字节，FAT32版本号0.0，FAT32特有。

【18】0x2C~0x2F：4字节，根目录所在第一个簇的簇号，2。（虽然在FAT32文件系统 下，根目录可以存放在数据区的任何位置，但是通常情况下还是起始于2号簇）

【19】0x30~0x31：2字节，FSINFO（文件系统信息扇区）扇区号1，该扇区为操作 系统提供关于空簇总数及下一可用簇的信息。

【20】0x32~0x33：2字节，备份引导扇区的位置。备份引导扇区总是位于文件系统 的6号扇区。

【21】0x34~0x3F：12字节，用于以后FAT 扩展使用。

【22】0x40~0x40：1字节，与FAT12/16 的定义相同，只不过两者位于启动扇区不

同的位置而已。

  【23】0x41~0x41：1字节，与FAT12/16 的定义相同，只不过两者位于启动扇区不

同的位置而已 。

【24】0x42~0x42：1字节，扩展引导标志，0x29。与FAT12/16 的定义相同，只不过 两者位于启动扇区不同的位置而已

【25】0x43~0x46：4字节，卷序列号。通常为一个随机值。

【26】0x47~0x51：11字节，卷标（ASCII码），如果建立文件系统的时候指定了卷 标，会保存在此。

【27】0x52~0x59：8字节，文件系统格式的ASCII码，FAT32。

★【28】0x5A~0x1FD：90~509共410字节，未使用。该部分没有明确的用途。

【29】0x1FE~0x1FF：签名标志“55 AA”。

★说明：引导代码

FAT文件系统将引导代码与文件形同数据结构融合在一起，FAT32文件系统引导扇区的512字节中，90~509字节为引导代码，而FAT12/16则是62~509字节为引导代码。同时，FAT32还可以利用引导扇区后的扇区空间存放附加的引导代码。一个FAT卷即使不是可引导文件文件系统，也会存在引导代码。

**2.2.1.2 FSInfo信息分区**

FAT32在保留区中增加了一个FSINFO扇区，用以记录文件系统中空闲簇的数量以及下一可用簇的簇号等信息，以供操作系统作为参考。FSINFO信息扇区一般位于文件系统的1号扇区，结构非常简单。FSINFO信息扇区结构。

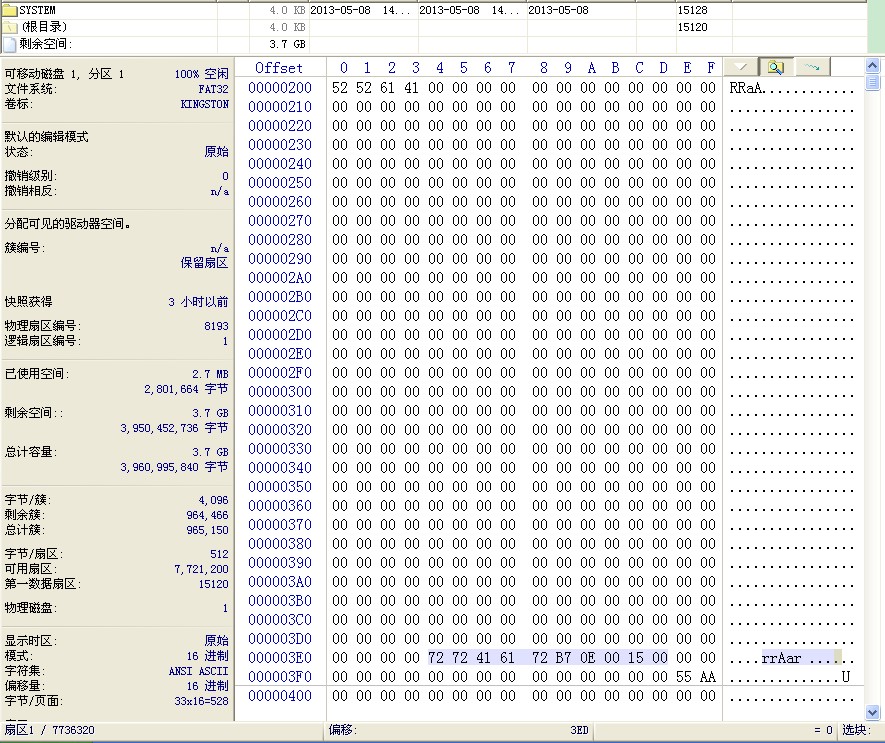


图8

【1】0x00~0x03: 4个字节，扩展引导标志“0x52526141”。

【2】0x04~0x1E3：480个字节，未使用，全部置0。

【3】0x1E4~0x1E7： 4个字节，FSINFO签名“0x72724161”。

【4】0x1E8~0x1EB： 4个字节，文件系统的空簇数，964466（0x00 0E B7 72）。

【5】0x1EC~0x1EF： 4个字节，下一可用簇号（0x 00 00 00 15）。

【6】0x1F0~0x1FD： 14个字节，未使用。

【7】0x1FE~0x1FF： 2个字节，“55 AA”标志。

温馨提示：通常情况下，文件系统的2号扇区结尾也会被设置“55 AA”标志。6号扇区也会有一个引导扇区的备份，相应的，7号扇区应该是一个备份FSINFO信息扇区，8号扇区可以看做是2号扇区的备份。

**2.2.2 文件分区FAT表（黄色区域）**

紧跟在保留分区后面的是FAT区，其由两个完全相同的FAT（File Allocation Table， 文件分配表）表单组成，FAT文件系统的名字也是因此而来。FAT 表（File Alloacation Table）是一组与数据簇号对应的列表。FAT2紧跟在FAT1之后，它的位置可以通过FAT1的位置加上FAT表的大小扇区数计算出来。

**2.2.2.1 文件系统概述**

文件系统分配磁盘空间按簇来分配。因此，文件占有磁盘空间时，基本单位不是字节而是簇，即使某个文件只有一个字节，操作系统也会给它分配一个最小单元：即一个簇。对于大文件，需要分配多个簇。同一个文件的数据并不一定完整地存放在磁盘中一个连续地区域内，而往往会分若干段，像链子一样存放。这种存储方式称为文件的链式存储。为了实现文件的链式存储，文件系统必须准确地记录哪些簇已经被文件占用，还必须为每个已经占用的簇指明存储后继的下一个簇的簇号，对于文件的最后一簇，则要指明本簇无后继簇。这些都是由FAT表来保存的，FAT 表对应表项中记录着它所代表的簇的有关信息：诸如是空，是不是坏簇，是否是已经是某个文件的尾簇等。

v 对于文件系统来说，FAT表有两个重要作用：描述簇的分配状态以及标明文件或目录的下一簇的簇号。

v 通常情况下，一个FAT把文件系统会有两个FAT表，但有时也允许只有一个FAT表，FAT表的具体个数记录在引导扇区的偏移0x10字节处。

v 由于FAT区紧跟在文件系统保留区后，所以FAT1在文件系统中的位置可以通过引导记录中偏移0x0E~0x0F字节处的“保留扇区数”得到，如存储器结构体图中M值。

**2.2.2.2 FAT表分析说明**

FAT32中每个簇的簇地址是有32bit（4个字节），FAT表中的所有字节位置以4字节为单位进行划分，并对所有划分后的位置由0进行地址编号。0号地址与1号地址被系统保留并存储特殊标志内容。从2号地址开始，每个地址对应于数据区的簇号，FAT表中的地址编号与数据区中的簇号相同。我们称FAT表中的这些地址为FAT表项，FAT表项中记录的值称为FAT表项值。

当文件系统被创建，也就是进行格式化操作时，分配给FAT区域的空间将会被清空，在FAT1与FAT2的0号表项与1号表项写入特定值。由于创建文件系统的同时也会创建根目录，也就是为根目录分配了一个簇空间，通常为2号簇，与之对应的2号FAT表项记录为2号簇，被写入一个结束标记。

几点说明：

Ø 由于簇号起始于2号，所以FAT表项的0号表项与1号表项不与任何簇对应。FAT32的0号表项值总是“F8FFFF0F”。

Ø 1号表项可能被用于记录脏标志，以说明文件系统没有被正常卸载或者磁盘表面存在错误。不过这个值并不重要。正常情况下1号表项的值为“FFFFFFFF”或“FFFFFF0F”。

Ø 如果某个簇未被分配使用，它对应的FAT表项内容为0；

Ø 当某个簇已被分配使用，则它对应的FAT表项内的FAT表项值也就是该文件的下一个存储位置的簇号。如果该文件结束于该簇，则在它的FAT表项中记录的是一个文件结束标记，对于FAT32而言，代表文件结束的FAT表项值为0x0FFFFFFF。

Ø 如果某个簇存在坏扇区，则整个簇会用0xFFFFFF7标记为坏簇，这个坏簇标记就记录在它所对应的FAT表项中。

Ø 在文件系统中新建文件时，如果新建的文件只占用一个簇，为其分配的簇对应的FAT表项将会写入结束标记。如果新建的文件不只占用一个簇，则在其所占用的每个簇对应的FAT表项中写入为其分配的下一簇的簇号，在最后一个簇对应的FAT表象中写入结束标记。

Ø 新建目录时，只为其分配一个簇的空间，对应的FAT表项中写入结束标记。当目录增大超出一个簇的大小时，将会在空闲空间中继续为其分配一个簇，并在FAT表中为其建立FAT表链以描述它所占用的簇情况。

**2.2.2.3 FAT表示例**

【0号表项】：0x0FFFFFF8;FAT表起始固定标识

【1号表项】：0xFFFFFFFF;不是用，默认值

【2号表项】：0x0FFFFFFF;根目录所在簇，

紫色的为3号表项，绿色的为4号表项，以此类推。注意：0和1号表项均不与实际的物理地址对应，2号表项开始才与物理地址对应。2号表项物理地址为FAT2表后紧跟着的那个簇！3号在2号表项紧跟着的一个簇。

计算：FAT所占扇区数 7541（0x1D75）；FAT2起始扇区为38+7541=7579；根目录起始扇区在7579 + 7541 = 15120。记得本文8个扇区为一个簇，即4K（0x1000），簇是系统分配内存的最小单元。

如图表中的起始地址对比，发现根目录起始地址刚好在15120，所以FAT表中0和1号表项没有对应物理地址！



图9

我将SD格式化，新建了一个test.txt的文本文件，大小为8.2kB。如下图：



图10

我们来分析上图：

在图中可以看出，test.txt文件起始簇为15128，这个地址是我们根目录（2号簇）后的一个簇，所以test.txt文件起始簇是3号簇，也就是3号表项（FAT表中表项值与簇号对应）。

【1】：2号表项为根目录，即2号簇。

【2】：3号表项为-0x00 00 00 04，test文件的下一簇号在4号表项，查看4号表项。

【3】：4号表项为-0x00 00 00 05，test文件下一簇号在5号表项，查看5号表项。

【4】：5号表项为-0x0F FF FF FF，结束符号。说明文件在5号簇时就存储完毕。

**2.2.3 数据区（灰色区域）**

数据区时真正用于存放用户数据的区域。数据区紧跟在FAT2之后，被划分成一个个的簇。所有的簇从2开始进行编号，也就是说，2号簇的起始位置就是数据区的起始位置。

**2.2.3.1 根目录**

FAT表示例中，根目录截图：



图11

虽然原则上FAT32允许根目录位于数据区的任何位置，但通常情况下它都位于数据区起始扇区，2号簇，可以在DBR偏移地址0x2C~0x2F查看。在FAT文件系统中，先要寻找数据区的第一簇（即2号簇）的位置，它不是位于文件系统开始处，而是位于数据区。从前面的学习知道，在数据区前面是保留区域和FAT区域，在前面还有MBR区域，这些区域都不使用FAT表进行管理。因此，数据区以前的区域只能使用扇区地址，而无法使用簇地址。

其实在2.2.2.3节，FAT表示例中我们就已经计算过其实地址（15128），注意这个地址不是物理地址哦，只是在FAT文件区域中一个相对地址！因为在之前还有MBR保留区域！

【保留区域大小（绿色部分）】：DBR偏移地址0x0E~0x0F，38（0x26），

【FAT表个数】：DBR偏移地址0x10开始2字节，2个，

【每个FAT表扇区数】：DBR偏移地址0x24~0x27，7541（0x 00 00 1D 75），

说明：以上值均参见2.2.1.1节。

【计算公式】：

     数据区起始扇区号 = 保留扇区数 + 每个FAT表大小扇区数 × FAT表个数

【示例】： 数据区起始扇区号 = 38 + 7541\*2 = 15120

为了避免根目录被更改，也可以用下面的计算公式计算出根目录扇区：

    根目录起始扇区=保留扇区数+FAT×2+(根目录起始簇-2)x每簇的扇区数。

说明：1、如果要得到物理地址，需要加上MBR保留区域大小。

**2.2.3.2 根目录的短文件目录项定义**

目录所在的扇区，都是以32 Bytes划分为一个单位，每个单位称为一个目录项（Directory

Entry ），即每个目录项的长度都是32 Bytes 。根目录由若干个目录项组成，一个目录项占用32个字节，可以是长文件名目录项、文件目录项、子目录项等。32字节的具体定义如下图：



图12

示例：

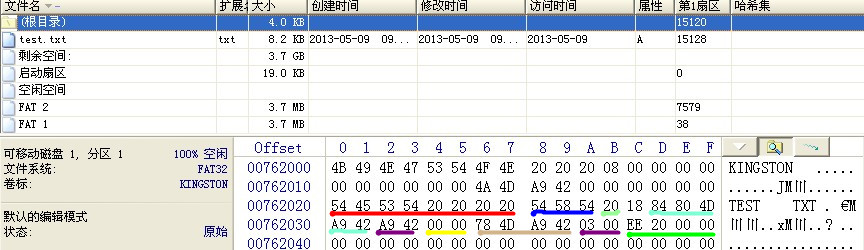


图13

特别关注的参数说明：

【1】：文件或者文件夹存储的起始簇号，上图中紫色区域，偏移地址：0x14-0x15（高16为）和0x1A-0x1B（低16位），0x 00 00 00 03 ，表示这个文件存储在3号簇的位置，在FAT表中为3号表项。

【2】：文件大小：偏移地址0x1C-0x1F，0x 00 00 20 EE（8430字节）；

【3】文件属性：偏移地址0x0B-0x0B，0x20 ，归档。

其他说明：

【0】子目录存储在数据区

【1】文件名的第一个字节，为0xE5，表示该项已被删除。

【2】名字为0x2E(“.”)，表示当前目录。



图14

【3】名字为0x2E 0x2E(“. .”)，表示上一级目录。

**2.2.3.3 长文件目录定义**



图15

点击链接下载本文的pdf版：http://download.csdn.net/detail/mjx91282041/5348397