一、MBR分区结构

MBR磁盘分区是一种使用最为广泛的分区结构，它也被称为DOS分区结构，但它并不仅仅应用于Windows系统平台，也应用于Linux，基于X86的UNIX等系统平台。它位于磁盘的0号扇区（一扇区等于512字节），是一个重要的扇区（简称MBR扇区）。

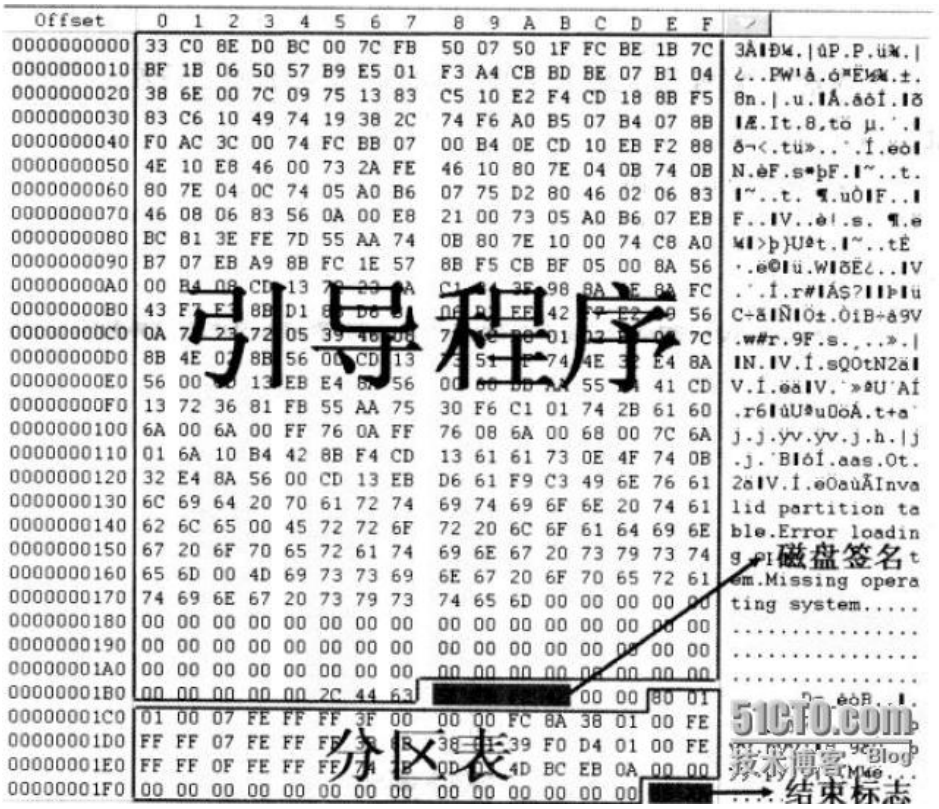
MBR扇区由以下四部分组成：

引导代码：引导代码占MBR分区的前440字节，负责整个系统启动。如果引导代码被破坏，系统将无法启动。

Windows磁盘签名：占引导代码后面的4字节，是Windows初始化磁盘写入的磁盘标签，如果此标签被破坏，则系统会提示“初始化磁盘”。

MBR分区表：占Windows磁盘标签后面的64个字节，是整个硬盘的分区表。

MBR结束标志：占MBR扇区最后2个字节，一直为“55 AA”。



注意：作者分析磁盘使用的工具是Winhex，如果读者需要请自行下载。

下面详细分析分区表结构

磁盘在使用前都要进行分区，也就是将硬盘划分为一个个逻辑的区域。每一个分区都有一个确定的起始结束位置。MBR磁盘的分区形式一般有3种，既主分区，扩展分区和非DOS分区。主分区既主DOS分区，扩展分区既扩展的DOS分区（扩展分区可以分逻辑分区），非DOS分区对于主分区的操作系统来说是一块被划分出去的区域，只能非DOS分区中操作系统可以管理。

如下：是MBR分区表

MBR一共占用64个字节，其中每16个字节为一个分区表项。也就是在MBR扇区中只能记录4个分区信息，可以是4个主分区，或者是3个主分区1个扩展分区。

每个分区项中对应的字节解释如下表：

字节偏移	字段长度	值	字段名和定义
0x01BE	1 字节	0x80	引导标志（Boot Indicator）：指明该分区是否是活动分区
0x01BF	1 字节	0x01	开始磁头（Start Head）
0x01C0	6 位	0x01	起始扇区（Start Sector）：只用了 0～5 位，后面的两位（第 6 位和第 7 位）被开始柱面字段所使用
0x01C1	10 位	0x00	起始柱面（Start Cylinder）：共占用 10 位，最大值为 1023
0x01C2	1 字节	0x07	分区的类型描述（Partition type indicator）：定义了分区的类型，详细定义，请参见表 4-2
0x01C3	1 字节	0xFE	结束磁头（End Head）
0x01C4	6 位	0xFF	结束扇区（End Sector）：只使用了 0～5 位。最后两位（第 6、7 位）被结束柱面字段所使用
0x01C5	10 位	0xFF	结束柱面（End Cylinder）：结束柱面是一个 10 位的数，最大值为 1023
0x01C6	4 字节	0x0000003F	本分区之前使用的扇区数（Sectors preceding partition）：指从该磁盘开始到该分区开始之间的偏移量，以扇区数来表示
0x01CA	4 字节	0x01388AFC	分区的总扇区数（Sectors in partition）：指该分区所包含的扇区总数

表 4-2　常见分区类型

00H	DOS 或 Windows 不允许使用，视为非法	5CH	Priam Edisk
01H	FAT12	61H	Speed Stor
02H	XENIX root	63H	GNU HURD or Sys
03H	XENIX usr	64H	Novell Netware
04H	FAT16 小于 32MB	65H	Novell Netware
05H	Extended	70H	Disk Secure Mult
06H	FAT16 大于 32MB	75H	PC/IX
07H	HPFS/NTFS	80H	Old Minix
08H	AIX	81H	Minix/Old Linux

09H	AIX bootable	82H	Linux swap
0AH	OS/2 Boot Manage	83H	Linux
0BH	Windows 95 FAT32	84H	0S/2 hidden C:
0CH	Windows 95 FAT32	85H	Linux extended
0EH	Windows 95 FAT16	86H	NTFS volume set
0FH	Windows 95 Extended（大于 8GB）	87H	NTFS volume set
10H	OPUS	93H	Amoeba
11H	Hidden FAT12	94H	Amoeba BBT
12H	Compaq diagnost	A0H	IBM Thinkpad hidden
16H	Hidden FAT16	A5H	BSD/386
14H	Hidden FAT16 小于 32MB	A6H	Open BSD
17H	Hidden HPFS/NTFS	A7H	NextSTEP
18H	AST Windows swap	B7H	BSDI fs
1BH	Hidden FAT32	B8H	BSDI swap
1CH	Hidden FAT32 partition（using LBA-mode INT 13 extensions）	BEH	Solaris boot partition
1EH	Hidden LBA VFAT partition	C0H	DR-DOS/Novell DOS secured partition
24H	NEC DOS	C1H	DRDOS/sec
3CH	Partition Magic	C4H	DRDOS/sec
40H	Venix 80286	C6H	DRDOS/sec
41H	PPC PreP Boot	C7H	Syrinx
42H	SFS	DBH	CP/M/CTOS
4DH	QNX4.x	E1H	DOS access
4EH	QNX4.x 2nd part	E3H	DOS R/0
4FH	QNX4.x 3rd part	E4H	SpeedStor
50H	OnTrack DM	EBH	BeOS fs
51H	OnTrack DM6 Aux	F1H	SpeedStor
52H	CP/M	F2H	DOS 3.3+ secondary partition
53H	OnTrack DM6 Aux	F4H	SpeedStor
54H	OnTrack DM6	FEH	LAN step
55H	EZ-Drive	FFH	BBT
56H	Golden Bow		

扩展分区的结构分析

由于MBR仅仅为分区表保留了64字节的存储空间，而每个分区则占用16字节的空间，也就是只能分4个分区，而4个分区在实际情况下往往是不够用的。因此就有了扩展分区，扩展分区中的每个逻辑分区的分区信息都存在一个类似MBR的扩展引导记录(简称EBR)中，扩展引导记录包括分区表和结束标志“55 AA”，没有引导代码部分。

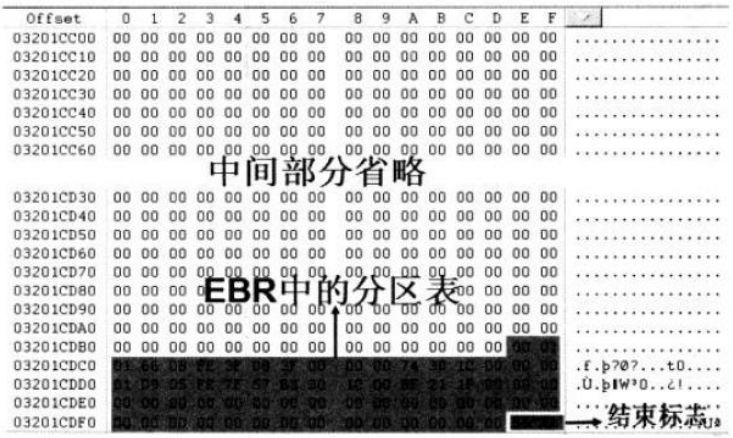


图 4-23　EBR 扇区

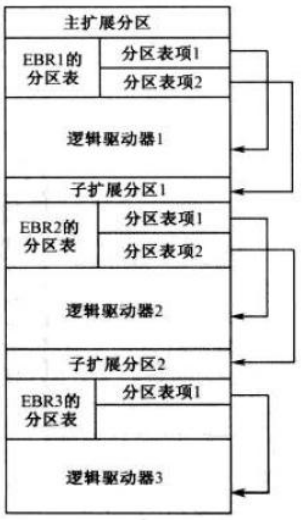


图 4-24　扩展分区结构

如上图：EBR中分区表的第一项描述第一个逻辑分区，第二项指向下一个逻辑分区的EBR。如果下一个逻辑分区不存在，第二项就不需要了。

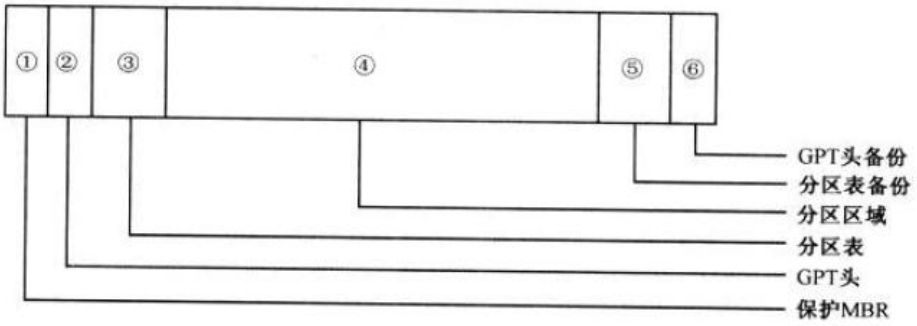
MBR分区的结构大致就介绍到这了。如果硬盘的MBR被破坏，可以复制其他硬盘的MBR到故障盘，然后修复分区表，也可以初始化故障盘然后修复分区表。

二、GPT分区结构

GPT磁盘分区的基本特点

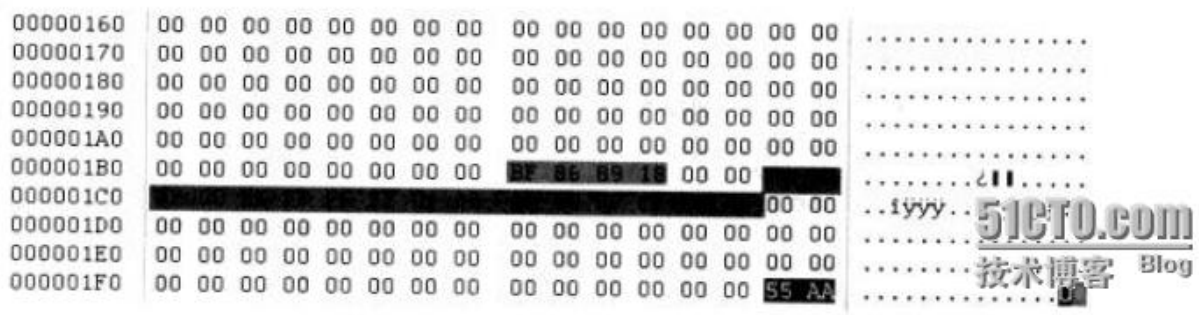
GPT磁盘分区结构解决了MBR只能分4个主分区的的缺点，理论上说，GPT磁盘分区结构对分区的数量好像是没有限制的。但某些操作系统可能会对此有限制。

GPT磁盘分区结构由6部分组成，如下图：

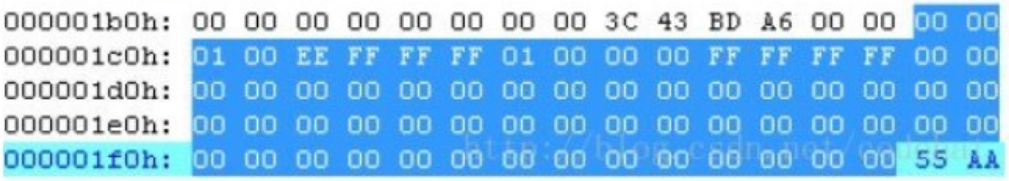


1、保护MBR

保护MBR位于GPT磁盘的第一扇区，也就是0号扇区，有磁盘签名，MBR磁盘分区表和结束标志组成，没有引导代码。而且分区表内只有一个分区表项，这个表项GPT根本不用，只是为了让系统认为这个磁盘是合法的。

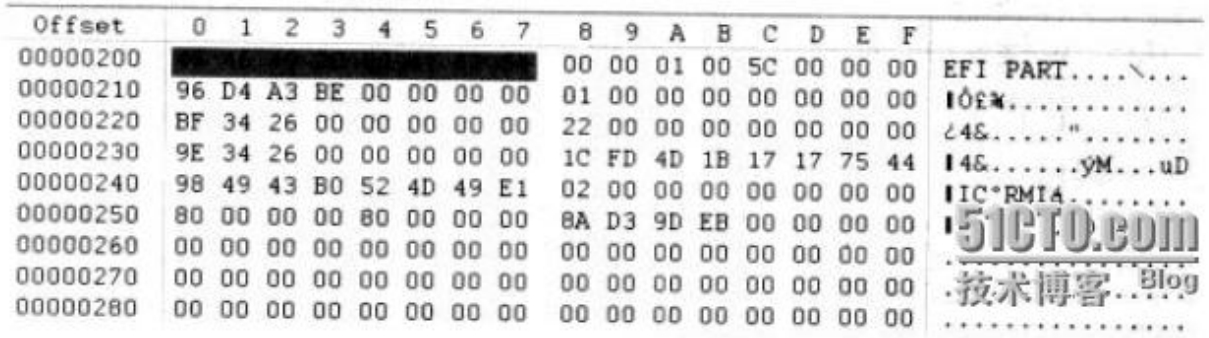


下面看一个GPT分区的第0个扇区，即MBR实例：



2、GPT头

GPT头位于GPT磁盘的第二个磁盘，也就是1号扇区，该扇区是在创建GPT磁盘时生成，GPT头会定义分区表的起始位置，分区表的结束位置、每个分区表项的大小、分区表项的个数及分区表的校验和等信息。



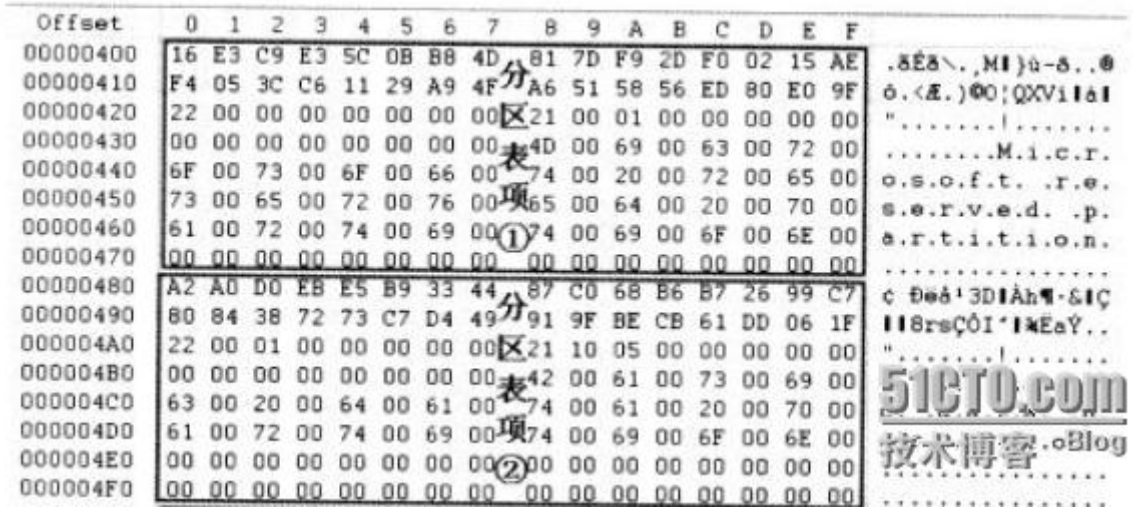
GPT头中参数的含义解释如下表：

字节偏移	字段长度（字节）	字段名和定义	字节偏移	字段长度（字节）	字段名和定义
0x00	8	签名，固定为 ASCII 码“EFI PART”	0x30	8	GPT 分区区域结束扇区号
0x08	4	版本号	0x38	16	磁盘 GUID
0x0C	4	GPT 头字节总数	0x48	8	GPT 分区表起始扇区号
0x10	4	GPT 头 CRC 校验和	0x50	4	分区表项数
0x14	4	保留	0x54	4	每个分区表项的字节数
0x18	8	GPT 头所在扇区号	0x58	4	分区表 CRC 校验和
0x20	8	GPT 头备份所在扇区号	0x5C	420	保留
0x28	8	GPT 分区区域起始扇区号			

3、分区表

分区表位于GPT磁盘的2-33号磁盘，一共占用32个扇区，能够容纳128个分区表项。每个分区表项大小为128字节。因为每个分区表项管理一共分区，所以Windows系统允许GPT磁盘创建128个分区。

每个分区表项中记录着分区的起始，结束地址，分区类型的GUID，分区的名字，分区属性和分区GUID。



分区表项中各参数的含义解释如下表：

字节偏移	字段长度（字节）	字段名和定义	字节偏移	字段长度（字节）	字段名和定义
0x00	16	分区类型 GUID	0x28	8	分区结束地址
0x10	16	分区 GUID	0x30	8	分区属性
0x20	8	分区起始地址	0x38	72	分区名（Unicode 码）

4、分区区域

GPT分区区域就是用户使用的分区，也是用户进行数据存储的区域。分区区域的起始地址和结束地址由GPT头定义。

5、GPT头备份

GPT头有一个备份，放在GPT磁盘的最后一个扇区，但这个GPT头备份并非完全GPT头备份，某些参数有些不一样。复制的时候根据实际情况更改一下即可。

6.分区表备份

分区区域结束后就是分区表备份，其地址在GPT头备份扇区中有描述。分区表备份是对分区表32个扇区的完整备份。如果分区表被破坏，系统会自动读取分区表备份，也能够保证正常识别分区。

GPT的分区结构相对于MBR要简单许多，并且分区表以及GPT头都有备份。

来源： http://dengqi.blog.51cto.com/5685776/1348951