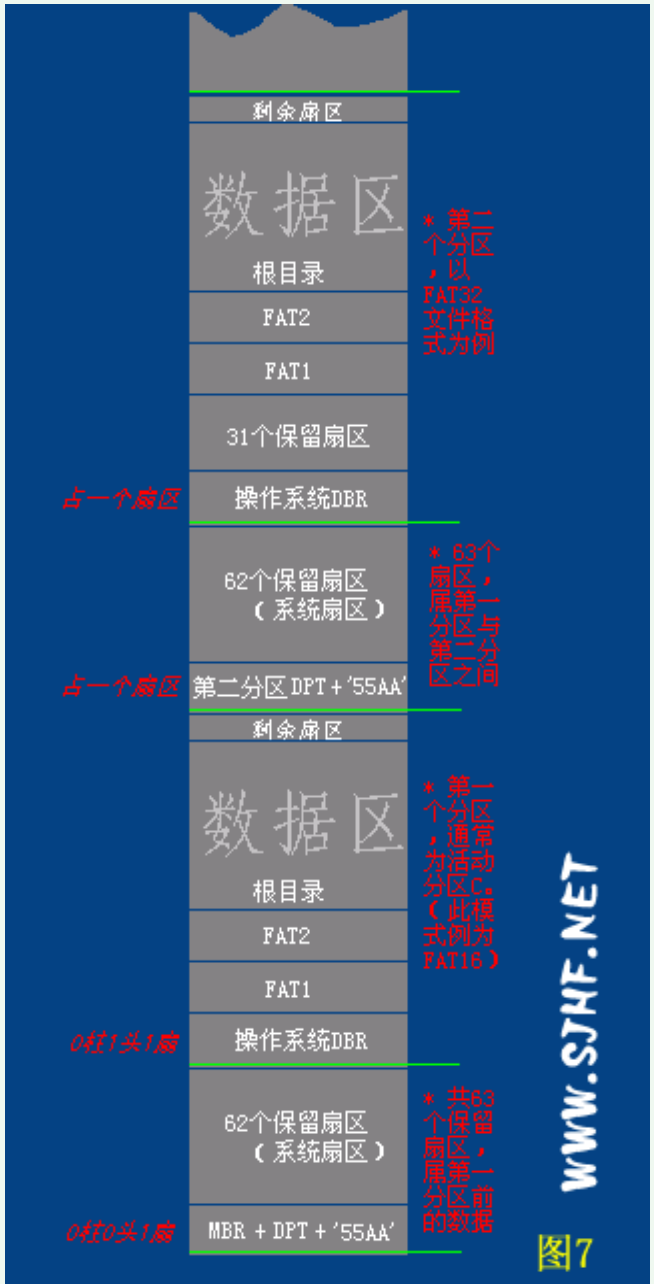
FAT文件系统原理(二)

FAT文件系统原理(二)

更新时间:2004-4-20 【字体：小 大】

四、FAT分区原理。

先来一幅结构图：

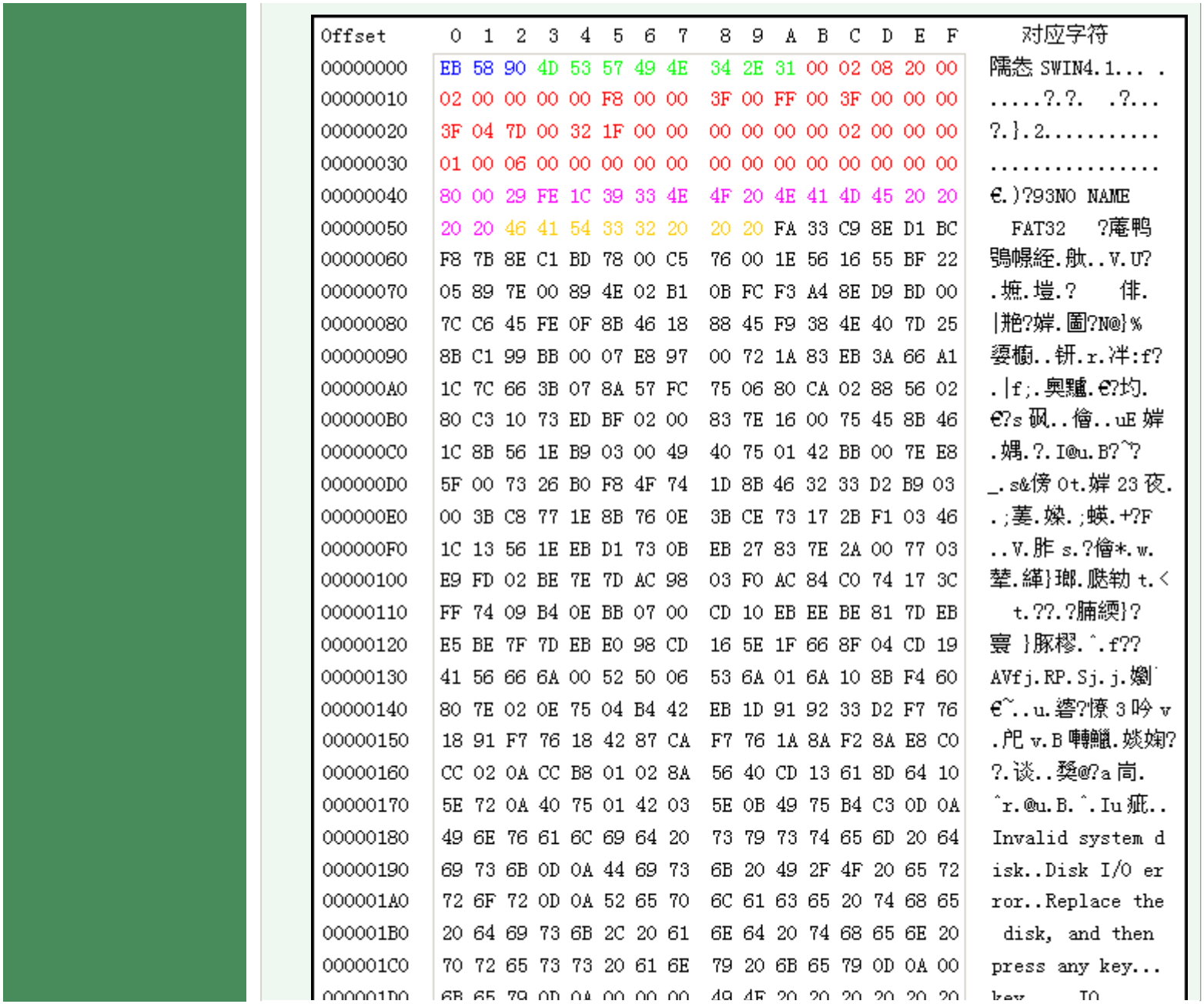

剩余扇区
数据区
根目录
FAT2
FAT1
31个保留扇区
操作系统DBR
62个保留扇区
（系统扇区）
第二分区DPT+'55AA'
剩余扇区
数据区
根目录
FAT2
FAT1
操作系统DBR
62个保留扇区
（系统扇区）
MBR + DPT + '55AA'
占一个扇区
占一个扇区
0柱1头1扇
0柱0头1扇
* 第二个分区，以FAT32文件格式为例
* 63个扇区，一与第二分区之间
* 第一个分区通常为活动分区C.（此模式例为FAT16）
* 共63个保留扇区，一分区前的数据
WWW.SJHF.NET
图7

现在我们着重研究FAT格式分区内数据是如何存储的。FAT分区格式是MICROSOFT最早支持的分区格式，依据FAT表中每个簇链的所占位数(有关概念，后面会讲到)分为fat12、fat16、fat32三种格式"变种"，但其基本存储方式是相似的。

仔细研究图7中的fat16和fat32分区的组成结构。下面依次解释DBR、FAT1、FAT2、根目录、数据区、剩余扇区的概念。提到的地址如无特别提示均为分区内部偏移。

4.1 关于DBR.

DBR区(DOS BOOT RECORD)即操作系统引导记录区的意思，通常占用分区的第0扇区共512个字节(特殊情况也要占用其它保留扇区，我们先说第0扇)。在这512个字节中，其实又是由跳转指令，厂商标志和操作系统版本号，BPB(BIOS Parameter Block)，扩展BPB，os引导程序，结束标志几部分组成。 以用的最多的FAT32为例说明分区DBR各字节的含义。见图8。



Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	对应字符
00000000	EB	58	90	4D	53	57	49	4E	34	2E	31	00	02	08	20	00	隔恚 SWIN4.1... .
00000010	02	00	00	00	00	F8	00	00	3F	00	FF	00	3F	00	00	00	.....?.?. .?...
00000020	3F	04	7D	00	32	1F	00	00	00	00	00	00	02	00	00	00	?.}.2..........
00000030	01	00	06	00	00	00	00	00	00	00	00	00	00	00	00	00	....
00000040	80	00	29	FE	1C	39	33	4E	4F	20	4E	41	4D	45	20	20	€.)?93NO NAME
00000050	20	20	46	41	54	33	32	20	20	20	FA	33	C9	8E	D1	BC	FAT32 ?庵鸭
00000060	F8	7B	8E	C1	BD	78	00	C5	76	00	1E	56	16	55	BF	22	鸮幜絰.舨..V.U?
00000070	05	89	7E	00	89	4E	02	B1	0B	FC	F3	A4	8E	D9	BD	00	.塼.塭.? 俳.
00000080	7C	C6	45	FE	0F	8B	46	18	88	45	F9	38	4E	40	7D	25	|羓?婩.圖?N@}%
00000090	8B	C1	99	BB	00	07	E8	97	00	72	1A	83	EB	3A	66	A1	婆橱..钑.r.冼:f?
000000A0	1C	7C	66	3B	07	8A	57	FC	75	06	80	CA	02	88	56	02	.|f;.奧黷.€?均.
000000B0	80	C3	10	73	ED	BF	02	00	83	7E	16	00	75	45	8B	46	€?s 砜..愔..uE 婩
000000C0	1C	8B	56	1E	B9	03	00	49	40	75	01	42	BB	00	7E	E8	.媧.?.I@u.B?~?
000000D0	5F	00	73	26	B0	F8	4F	74	1D	8B	46	32	33	D2	B9	03	_.s&傍 Ot.婩 23 夜.
000000E0	00	3B	C8	77	1E	8B	76	0E	3B	CE	73	17	2B	F1	03	46	.;萋.嫩.;蛱.+?F
000000F0	1C	13	56	1E	EB	D1	73	0B	EB	27	83	7E	2A	00	77	03	..V.胙 s.?愔*.w.
00000100	E9	FD	02	BE	7E	7D	AC	98	03	F0	AC	84	C0	74	17	3C	荤.緙}瑯.胰钕 t.<
00000110	FF	74	09	B4	0E	BB	07	00	CD	10	EB	EE	BE	81	7D	EB	t.??.?腩缏}?
00000120	E5	BE	7F	7D	EB	E0	98	CD	16	5E	1F	66	8F	04	CD	19	寰 }豚樛.^.f??
00000130	41	56	66	6A	00	52	50	06	53	6A	01	6A	10	8B	F4	60	AVfj.RP.Sj.j.嬲`
00000140	80	7E	02	0E	75	04	B4	42	EB	1D	91	92	33	D2	F7	76	€~..u.谮?憭 3 吟 v
00000150	18	91	F7	76	18	42	87	CA	F7	76	1A	8A	F2	8A	E8	C0	.阣 v.B 囀鼬.嫉婀?
00000160	CC	02	0A	CC	B8	01	02	8A	56	40	CD	13	61	8D	64	10	?.谈..婪@?a 肓.
00000170	5E	72	0A	40	75	01	42	03	5E	0B	49	75	B4	C3	0D	0A	^r.@u.B.^.Iu 疵..
00000180	49	6E	76	61	6C	69	64	20	73	79	73	74	65	6D	20	64	Invalid system d
00000190	69	73	6B	0D	0A	44	69	73	6B	20	49	2F	4F	20	65	72	isk..Disk I/O er
000001A0	72	6F	72	0D	0A	52	65	70	6C	61	63	65	20	74	68	65	ror..Replace the
000001B0	20	64	69	73	6B	2C	20	61	6E	64	20	74	68	65	6E	20	disk, and then
000001C0	70	72	65	73	73	20	61	6E	79	20	6B	65	79	0D	0A	00	press any key...
000001D0	6B	65	79	0D	0A	00	00	00	49	4F	20	20	20	20	20	20	key IO

图8的对应解释见表3

单击此处查看PDF版全文

表3 FAT32分区上DBR中各部分的位置划分

字节位移	字段长度	字段名	对应图8颜色
0x00	3个字节	跳转指令	
0x03	8个字节	厂商标志和os版本号	
0x0B	53个字节	BPB	
0x40	26个字节	扩展BPB	
0x5A	420个字节	引导程序代码	
0x01FE	2个字节	有效结束标志	

图9给出了winhex对图8 DBR的相关参数解释：

Boot Sector FAT32, 基础偏移量：0

Offset	标题	数值
0	JMP instruction	EB 58 90
3	OEM	MSWIN4.1
	BIOS Parameter Block	
B	Bytes per sector	512
D	Sectors per cluster	8
E	Reserved sectors	32
10	Number of FATs	2
11	Root entries (unused)	0
13	Sectors (on small volumes)	0
15	Media descriptor (hex)	F8
16	Sectors per FAT (small vol.)	0
18	Sectors per track	63
1A	Heads	255
1C	Hidden sectors	63
20	Sectors (on large volumes)	8193087
	FAT32 Section	
24	Sectors per FAT	7986
28	Flags	0
2A	Version	0
2C	Root dir 1st cluster	2
30	FSInfo sector	1
32	Backup boot sector	6
34	(Reserved)	00 00 00 00 00 00 00 00 00 00 00 00
40	BIOS drive (hex, HD=8x)	80
41	(Unused)	0
42	Ext. boot signature (29h)	29
43	Volume serial number (decimal)	859380990
43	Volume serial number (hex)	FE 1C 39 33

根据上边图例，我们来讨论DBR各字节的参数意义。

MBR将CPU执行转移给引导扇区，因此，引导扇区的前三个字节必须是合法的可执行的基于x86的CPU指令。这通常是一条跳转指令，该指令负责跳过接下来的几个不可执行的字节(BPB和扩展BPB)，跳到操作系统引导代码部分。

跳转指令之后是8字节长的OEM ID，它是一个字符串， OEM ID标识了格式化该分区的操作系统的名称和版本号。为了保留与MS-DOS的兼容性，通常Windows 2000格式化该盘是在FAT16和FAT32磁盘上的该字段中记录了“MSDOS 5.0”，在NTFS磁盘上(关于ntfs，另述)，Windows 2000记录的是“NTFS”。通常在被Windows 95格式化的磁盘上OEM ID字段出现“MSWIN4.0”，在被Windows 95 OSR2和Windows 98格式化的磁盘上OEM ID字段出现“MSWIN4.1”。

接下来的从偏移0x0B开始的是一段描述能够使可执行引导代码找到相关参数的信息。通常称之为BPB(BIOS Parameter Block)，BPB一般开始于相同的位移量，因此，标准的参数都处于一个已知的位置。磁盘容量和几何结构变量都被封在BPB之中。由于引导扇区的第一部分是一个x86跳转指令。因此，将来通过在BPB末端附加新的信息，可以对BPB进行扩展。只需要对该跳转指令作一个小的调整就可以适应BPB的变化。图9已经列出了项目的名称和取值，为了系统的研究，针对图8，将FAT32分区格式的BPB含义和扩展BPB含义释义为表格，见表4和表5。

表4　FAT32分区的BPB字段

字节位移	字段长度(字节)	图8对应取值	名称和定义
0x0B	2	0x0200	扇区字节数(Bytes Per Sector)硬件扇区的大小。本字段合法的十进制值有512、1024、2048和4096。对大多数磁盘来说，本字段的值为512
0x0D	1	0x08	每簇扇区数(Sectors Per Cluster),一簇中的扇区数。由于FAT32文件系统只能跟踪有限个簇(最多为4 294 967 296个)，因此，通过增加每簇扇区数，可以使FAT32文件系统支持最大分区数。一个分区缺省的簇大小取决于该分区的大小。本字段的合法十进制值有1、2、4、8、16、32、64和128。Windows 2000的FAT32实现只能创建最大为32GB的分区。但是，Windows 2000能够访问由其他操作系统(Windows 95、OSR2及其以后的版本)所创建的更大的分区

0x0e	2	0x0020	保留扇区数(Reserved Sector) 第一个FAT开始之前的扇区数，包括引导扇区。本字段的十进制值一般为32
0x10	1	0x02	FAT数(Number of FAT) 该分区上FAT的副本数。本字段的值一般为2
0x11	2	0x0000	根目录项数(Root Entries)只有FAT12/FAT16使用此字段。对FAT32分区而言,本字段必须设置为 0
0x13	2	0x0000	小扇区数(Small Sector)(只有FAT12/FAT16使用此字段)对FAT32分区而言，本字段必须设置为0
0x15	1	0xF8	媒体描述符(Media Descriptor)提供有关媒体被使用的信息。值0xF8表示硬盘，0xF0表示高密度的3.5寸软盘。媒体描述符要用于MS-DOS FAT16磁盘，在Windows 2000中未被使用
0x16	2	0x0000	每FAT扇区数(Sectors Per FAT)只被FAT12/FAT16所使用,对FAT32分区而言，本字段必须设置为0
0x18	2	0x003F	每道扇区数(Sectors Per Track) 包含使用INT13h的磁盘的“每道扇区数”几何结构值。该分区被多个磁头的柱面分成了多个磁道
0x1A	2	0x00FF	磁头数(Number of Head) 本字段包含使用INT 13h的磁盘的“磁头数”几何结构值。例如，在一张1.44MB 3.5英寸的软盘上，本字段的值为 2
0x1C	4	0x00000 03F	隐藏扇区数(Hidden Sector) 该分区上引导扇区之前的扇区数。在引导序列计算到根目录的数据区的绝对位移的过程中使用了该值。本字段一般只对那些在中断

			13h上可见的媒体有意义。在没有分区的媒体上它必须总是为0
0x20	4	0x007D043F	总扇区数(Large Sector) 本字段包含FAT32分区中总的扇区数
0x24	4	0x00001F32	每FAT扇区数(Sectors Per FAT)(只被FAT32使用)该分区每个FAT所占的扇区数。计算机利用这个数和 FAT数以及隐藏扇区数(本表中所描述的)来决定根目录从哪里开始。该计算机还可以从目录中的项数决定该分区的用户数据区从哪里开始
0x28	2	0x00	扩展标志(Extended Flag)(只被FAT32使用)该两个字节结构中各位的值为: 位0-3：活动 FAT数(从0开始计数，而不是1). 只有在不使用镜像时才有效 位4-6：保留 位7：0值意味着在运行时FAT被映射到所有的FAT 1值表示只有一个FAT是活动的 位8-15：保留
0x2A	2	0x0000	文件系统版本(File ystem Version)只供FAT32使用,高字节是主要的修订号，而低字节是次要的修订号。本字段支持将来对该FAT32媒体类型进行扩展。如果本字段非零，以前的Windows版本将不支持这样的分区
0x2C	4	0x00000002	根目录簇号(Root Cluster Number)(只供FAT32使用) 根目录第一簇的簇号。本字段的值一般为2，但不总是如此
			文件系统信息扇区号(File System Information SectorNumber)

0x30	2	0x0001	(只供FAT32使用) FAT32分区的保留区中的文件系统信息(File System Information, FSINFO)结构的扇区号。其值一般为1。在备份引导扇区(Backup Boot Sector)中保留了该FSINFO结构的一个副本，但是这个副本不保持更新
0x34	2	0x0006	备份引导扇区(只供FAT32使用)为一个非零值，这个非零值表示该分区保存引导扇区的副本的保留区中的扇区号。本字段的值一般为6，建议不要使用其他值
0x36	12	12个字节均为0x00	保留(只供FAT32使用)供以后扩充使用的保留空间。本字段的值总为0

表5 FAT32分区的扩展BPB字段

字节位移	字段长度(字节)	图8对应取值	字段名称和定义
0x40	1	0x80	物理驱动器号(Physical Drive Number) 与BIOS物理驱动器号有关。软盘驱动器被标识为0x00，物理硬盘被标识为0x80，而与物理磁盘驱动器无关。一般地，在发出一个INT13h BIOS调用之前设置该值，具体指定所访问的设备。只有当该设备是一个引导设备时，这个值才有意义
0x41	1	0x00	保留(Reserved) FAT32分区总是将本字段的值设置为0
0x42	1	0x29	扩展引导标签(Extended Boot Signature) 本字段必须要有能被Windows 2000所识别的值0x2

			8或0x29
0x43	4	0x33391CFE	分区序号(Volume Serial Number) 在格式化磁盘时所产生的一个随机序号，它有助于区分磁盘
0x47	11	"NO NAME"	卷标(Volume Label) 本字段只能使用一次，它被用来保存卷标号。现在，卷标被作为一个特殊文件保存在根目录中
0x52	8	"FAT32"	系统ID(System ID) FAT32文件系统中一般取为"FAT32"

DBR的偏移0x5A开始的数据为操作系统引导代码。这是由偏移0x00开始的跳转指令所指向的。在图8所列出的偏移0x00~0x02的跳转指令"EB 58 90"清楚地指明了OS引导代码的偏移位置。jump 58H加上跳转指令所需的位移量，即开始于0x5A。此段指令在不同的操作系统上和不同的引导方式上，其内容也是不同的。大多数的资料上都说win98,构建于fat基本分区上的win2000,winxp所使用的DBR只占用基本分区的第0扇区。他们提到，对于fat32，一般的32个基本分区保留扇区只有第0扇区是有用的。实际上，以FAT32构建的操作系统如果是win98,系统会使用基本分区的第0扇区和第2扇区存储os引导代码；以FAT32构建的操作系统如果是win2000或winxp,系统会使用基本分区的第0扇区和第0xC扇区(win2000或winxp,其第0xC的位置由第0扇区的0xAB偏移指出)存储os引导代码。所以，在fat32分区格式上，如果DBR一扇区的内容正确而缺少第2扇区(win98系统)或第0xC扇区(win2000或winxp系统)，系统也是无法启动的。如果自己手动设置NTLDR双系统，必须知道这一点。

DBR扇区的最后两个字节一般存储值为0x55AA的DBR有效标志，对于其他的取值，系统将不会执行DBR相关指令。上面提到的其他几个参与os引导的扇区也需以0x55AA为合法结束标志。

FAT16 DBR:

FAT32中DBR的含义大致如此，对于FAT12和FAT16其基本意义类似，只是相关偏移量和参数意义有小的差异，FAT格式的区别和来因，以后会说到，此处不在多说FAT12与FAT16。我将FAT16的扇区参数意义列表。感兴趣的朋友自己研究一下，和FAT32大同小异的。

表6 一个FAT16分区上的引导扇区段

字节位移	字段长度(字节)	字段名称
0x00	3	跳转指令(Jump Instruction)
0x03	8	OEM ID

0x0B	25	BPB
0x24	26	扩展BPB
0x3E	448	引导程序代码(Bootstrap Code)
0x01FE	4	扇区结束标识符(0x55AA)

表7 FAT16分区的BPB字段

字节位移	字段长度(字节)	例值	名称和定义
0x0B	2	0x0200	扇区字节数(Bytes Per Sector) 硬件扇区的大小。本字段合法的十进制值有512、1024、2048和4096。对大多数磁盘来说，本字段的值为512
0x0D	1	0x40	每簇扇区数(Sectors Per Cluster) 一个簇中的扇区数。由于FAT16文件系统只能跟踪有限个簇(最多为65536个)。因此，通过增加每簇的扇区数可以支持最大分区数。分区的缺省的簇的大小取决于该 分区的大小。本字段合法的十进制值有 1、2、4、8、16、32、64和128。导致簇大于32KB(每扇区字节数*每簇扇区数)的值会引起磁盘错误和软件错误
0x0e	2	0x0001	保留扇区数(Reserved Sector) 第一个FAT开始之前的扇区数，包括引导扇区。本字段的十进制值一般为1
0x10	1	0x02	FAT数(Number of FAT)该分区上FAT的副本数。本字段的值一

			般为2
0x11	2	0x0200	根目录项数(Root Entries) 能够保存在该分区的根目录文件夹中的32个字节长的文件和文件夹名称项的总数。在一个典型的硬盘上，本字段的值为512。其中一个项常常被用作卷标号(Volume Label)，长名称的文件和文件夹每个文件使用多个项。文件和文件夹项的最大数一般为511，但是如果使用的长文件名，往往都达不到这个数
0x13	2	0x0000	小扇区数(Small Sector) 该分区上的扇区数，表示为16位(<65536)。对大于65536个扇区的分区来说，本字段的值为0，而使用大扇区数来取代它
0x15	1	0xF8	媒体描述符(Media Descriptor)提供有关媒体被使用的信息。值0xF8表示硬盘，0xF0表示高密度的3.5寸软盘。媒体描述符要用于MS-DOS FAT16磁盘，在Windows 2000中未被使用
0x16	2	0x00FC	每FAT扇区数(Sectors Per FAT) 该分区上每个FAT所占用的扇区数。计算机利用这个数和FAT数以及隐藏扇区数来决定根目录在哪里开始。计算机还可以根据根目录中的项数(512)决定该 分区的用户数据区从哪里开始
0x18	2	0x003F	每道扇区数(Sectors Per Trark)
0x1A	2	0x0040	磁头数(Number of head)
			隐藏扇区数(Hidden Sector) 该分区上引导扇区之前的扇区

0x1C	4	0x00000 03F	数。在引导序列计算到根目录和数据区的绝对位移的过程中使用了该值
0x20	4	0x003EF 001	大扇区数(Large Sector) 如果小扇区数字段的值为0，本字段就包含该FAT16分区中的总扇区数。如果小扇区数字段的值不为0，那么本字段的值为0

表8 FAT16分区的扩展BPB字段

字节位移	字段长度(字节)	图8对应取值	字段名称和定义
0x24	1	0x80	物理驱动器号(Physical Drive Number) 与BIOS物理驱动器号有关。软盘驱动器被标识为0x00，物理硬盘被标识为0x80，而与物理磁盘驱动器无关。一般地，在发出一个INT13h BIOS调用之前设置该值，具体指定所访问的设备。只有当该设备是一个引导设备时，这个值才有意义
0x25	1	0x00	保留(Reserved) FAT16分区一般将本字段的值设置为0
0x26	1	0x29	扩展引导标签(Extended Boot Signature) 本字段必须要有能被Windows 2000所识别的值0x28或0x29
0x27	2	0x52368 BA8	卷序号(Volume Serial Number) 在格式化磁盘时所产生的一个随机序号，它有助于区分磁盘
			卷标(Volume Label) 本字段

0x2B	11	"NO NAME"	只能使用一次，它被用来保存卷标号。现在，卷标被作为一个特殊文件保存在根目录中
0x36	8	"FAT16"	文件系统类型(File System Type) 根据该磁盘格式，该字段的值可以为FAT、FAT12或FAT16

4.2 关于保留扇区

在上述FAT文件系统DBR的偏移0x0E处，用2个字节存储保留扇区的数目。所谓保留扇区(有时候会叫系统扇区，隐藏扇区)，是指从分区DBR扇区开始的仅为系统所有的扇区，包括DBR扇区。在FAT16文件系统中，保留扇区的数据通常设置为1，即仅仅DBR扇区。而在FAT32中，保留扇区的数据通常取为32，有时候用Partition Magic分过的FAT32分区会设置36个保留扇区，有的工具可能会设置63个保留扇区。

FAT32中的保留扇区除了磁盘总第0扇区用作DBR，总第2扇区(win98系统)或总第0xC扇区(win2000,winxp)用作OS引导代码扩展部分外，其余扇区都不参与操作系统管理与磁盘数据管理，通常情况下是没作用的。操作系统之所以在FAT32中设置保留扇区，是为了对DBR作备份或留待以后升级时用。FAT32中，DBR偏移0x34占2字节的数据指明了DBR备份扇区所在，一般为0x06，即第6扇区。当FAT32分区DBR扇区被破坏导致分区无法访问时。可以用第6扇区的原备份替换第0扇区来找回数据。

单击此处查看PDF版全文

- 上一篇文章： FAT文件系统原理(一)
- 下一篇文章： FAT文件系统原理(三)

【关闭窗口】

站内文章搜索 文章标题 所有栏目 关键字 搜索

首页 联系我们 加入收藏 版权申明 文章地图 下载地图 RSS生成 XML生成 友情链接

北亚数据恢复中心
全国统一客服电话：4006-505-808
北京部：北京市海淀区中关村大街11号E世界A座832B
京ICP备09039053号