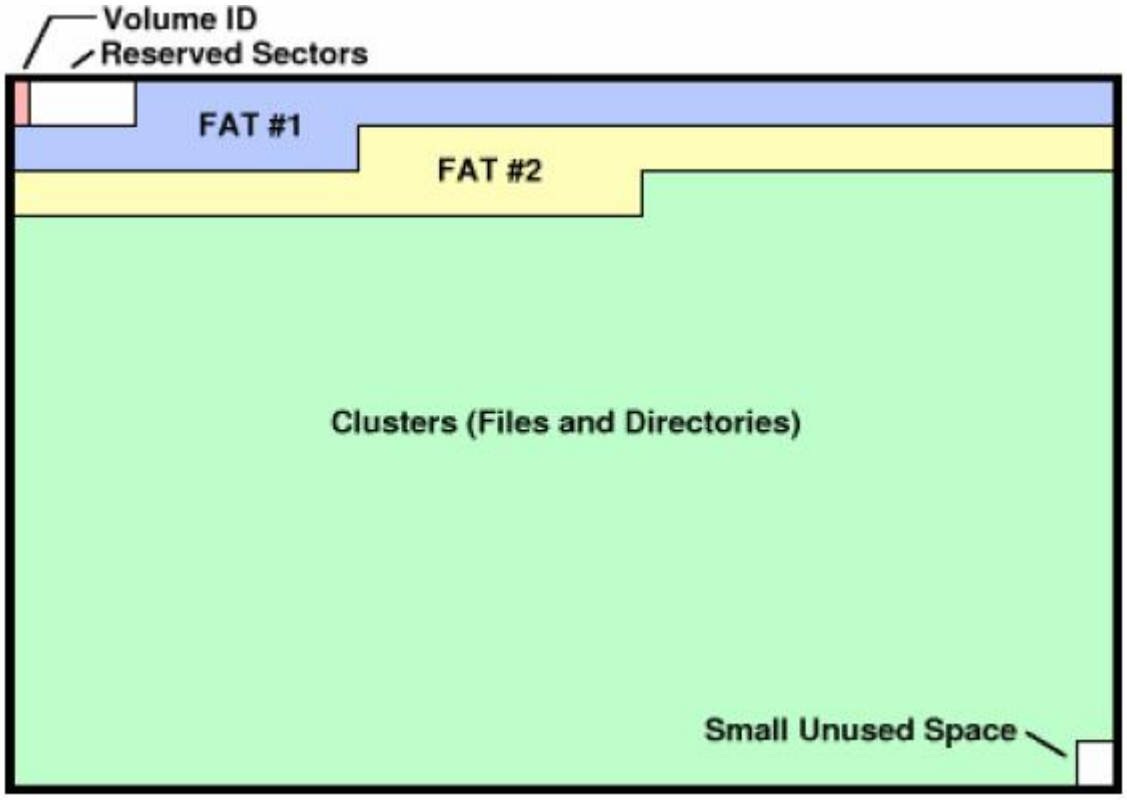
DBR:操作系统引导记录区（包括BPB）

一.一般硬盘数据结构是按下面来建立的



二．首先看看启动区的内容，也就是第一个扇区。使用软件：WinHex

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00000000	EB	58	90	4D	53	44	4F	53	35	2E	30	00	02	08	24	00	隔恚SDOS5.0...$.
00000010	02	00	00	00	00	F8	00	00	3F	00	FF	00	00	00	00	00	.....?.?. .....
00000020	00	1F	0F	00	C6	03	00	00	00	00	00	00	02	00	00	00	....?..........
00000030	01	00	06	00	00	00	00	00	00	00	00	00	00	00	00	00	....
00000040	00	00	29	04	09	C6	5C	4E	4F	20	4E	41	4D	45	20	20	..)..芒NO NAME
00000050	20	20	46	41	54	33	32	20	20	20	33	C9	8E	D1	BC	F4	FAT32 3蔺鸭
00000060	7B	8E	C1	8E	D9	BD	00	7C	88	4E	02	8A	56	40	B4	08	{幜仄?|圩.糞@?
00000070	CD	13	73	05	B9	FF	FF	8A	F1	66	0F	B6	C6	40	66	0F	?s.? 矮f.镀@f.
00000080	B6	D1	80	E2	3F	F7	E2	86	CD	C0	ED	06	41	66	0F	B7	堆e?麾噻理.Af.
00000090	C9	66	F7	E1	66	89	46	F8	83	7E	16	00	75	38	83	7E	霍歷f墩鴃~..u8僧

有用的内容用彩色线标志下

⑴．灰色线内容：EB 59 90 跳转指令

⑵．灰色点线内容：4D 53 44 4F 53 35 2E 30 为厂商标志和os 版本号，这里是MSDOS5.0

⑶．红色部分：00 20（偏移地址0BH,长度2)注意这里数据的布局，高地址放高字节，低地址放低字节（数据为小端格式组织），所以数据应该是0200，就是512。表示的意思是，该磁盘每个扇区有512个字节。有的可能是1024、2048、4096.

⑷．黄色部分：08（偏移地址0DH,长度1)表示的意思是每个簇有8个扇区。这个值不能为0，而且必须是2的整数次方，比如1、2、4、8、16、32、64、128.但是这个值不能使每个簇超过32KB字节。

⑸. 蓝色部分：24 00（偏移地址0EH, 长度2），转换一下，就是00 24，意思是保留区域中的保留扇区数为36个。那么就可以知道下面的FAT1区的开始的地址就是：0x24*200（每个扇区的字节数）=0x4800，

⑹. 粉色部分：02（偏移地址 10H, 长度 1），此卷中的 FAT 结构的份数为 2，另外一个是备份的。

⑺. 黑色部分：C6 03 （偏移地址 24H, 长度 2)转换一下，03C6，每个 FAT 占用的扇区数。那么每个扇区占用的字节数就是 0x03c6*200=78C00。根据启动区、FAT1、FAT2、根目录、数据区的次序，可以依次计算出它们的地址了。

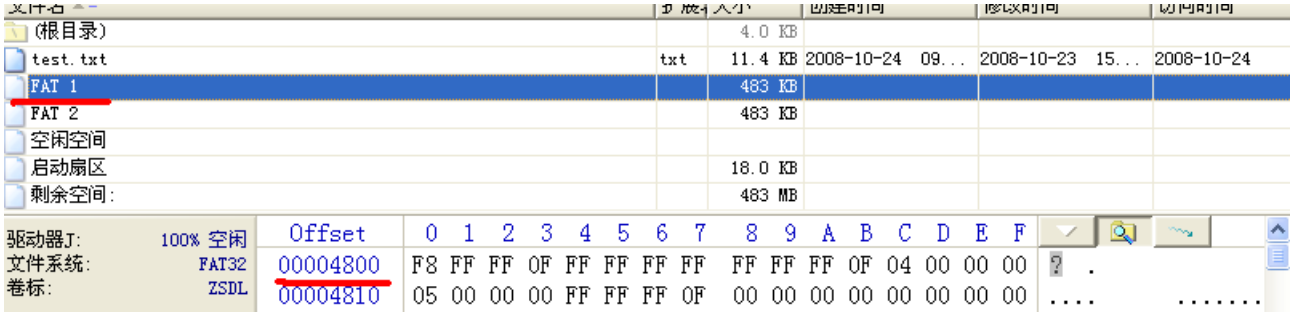
启动区：理所当然是 0x00；

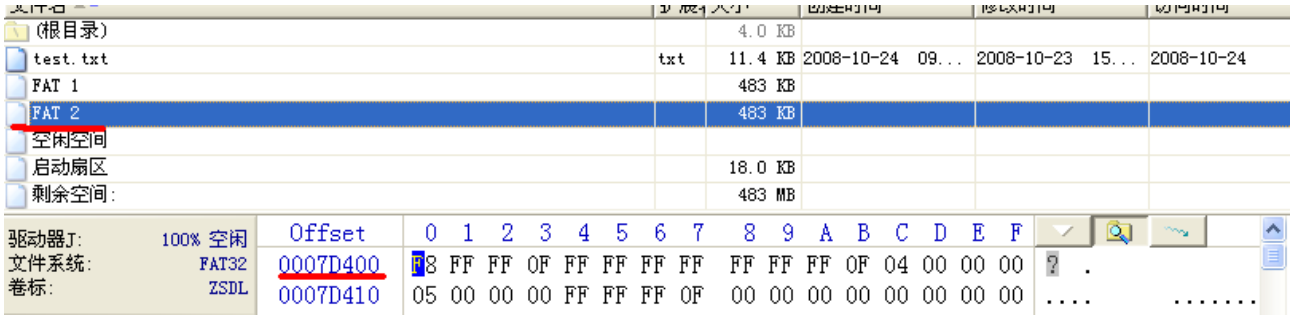
FAT1：0x4800；

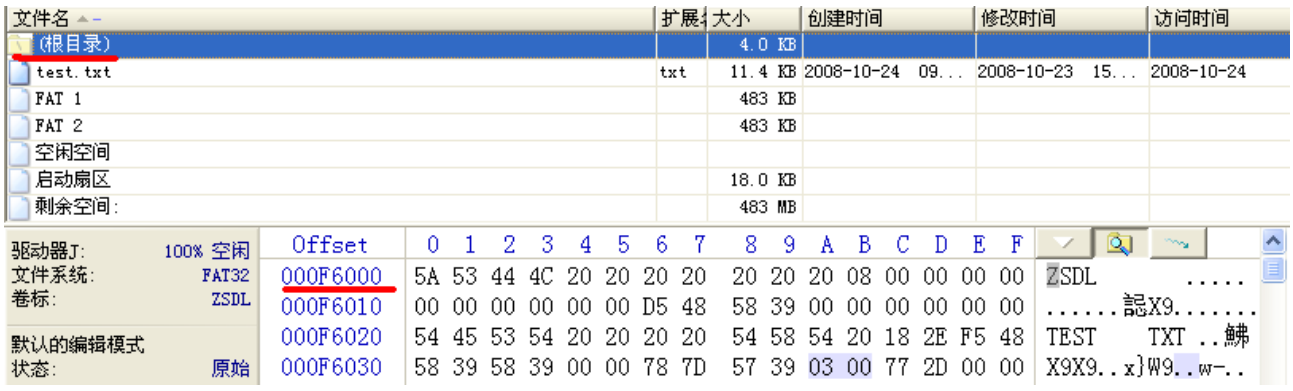
FAT2:0x4800 + 0x78C00 = 7D400；

根目录区：7D400 + 78C00 = F6000；

数据区的地址，等等再计算。这个只是计算，可以看看是不是和实际的一致。







怎么样，是不是和计算的很一致。

为什么要计算 SD 数据的读取要给出地址，而且每次读取都是一个整扇区，512 个字节。找出这些地址后，可以很方便的找到数据。

三．现在分析下根目录区的内容。

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
000F6000	5A	53	44	4C	20	20	20	20	20	20	20	08	00	00	00	00
000F6010	00	00	00	00	00	00	D5	48	58	39	00	00	00	00	00	00
000F6020	54	45	53	54	20	20	20	20	54	58	54	20	18	2E	F5	48
000F6030	58	39	58	39	00	00	78	7D	57	39	03	00	77	2D	00	00
000F6040	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00

这里使用的是FAT32短文件目录项，每32个字节表示一个文件（文件夹也是），32个字节的表示定义分别如下

⑴．黑色部分：驱动器的名称，8个字节，

⑵．红色部分：54 45 53 54 20 20 20 20　(偏移地址20H,长度8)文件名：TEST　　(空缺部分是空格)。

⑶．红色点线：54 58 54 (偏移地址28H,长度3)文件类型，为ASCII字符表示。

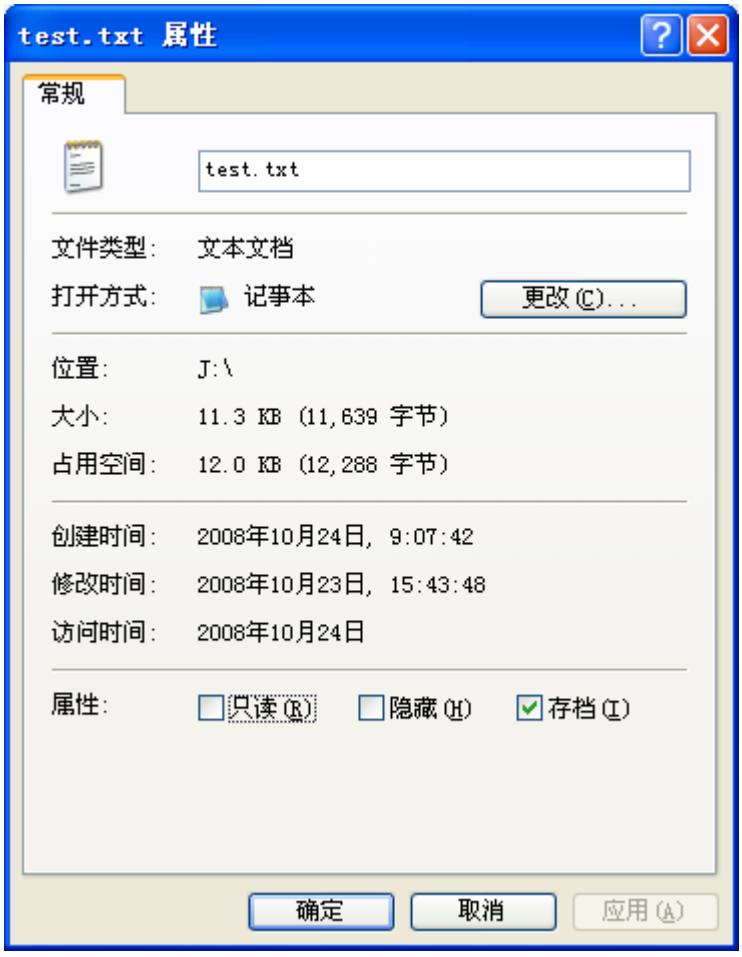
⑷.绿色：20(偏移地址2BH,长度2)文件属性，00000000(读写)；00000001(只读)；00000010(隐藏)；00000100(系统)；00001000(卷标)；00010000(子目录)；00100000(归档)。

⑸．蓝色点线：2E(偏移地址2EH,长度2) 文件创建时间。

⑹．粉色线、点线 依次表示文件创建日期 文件最后访问日期。

⑺．灰色线、点线：依次为该文件开始簇号的高位字节、地位字节，这里也是用了小端格式组织。转换下为00 00 00 03，根据这个就可以找到文件下一个簇号在FAT1中的位置了。4800+03*04（因为四个字节存一个簇号）= 480C。

⑻．黄色线部分：文件长度。转后 00 00 2D 77 就是 11639 字节。



但是它占用的 12KB 的空间，因为文件是按照整簇来存放的，不够一个簇的大小，也要给一个簇的空间。

四．计算出该文件放置空间。

从文件的大小可以计算出，需要占用多少个簇。根据前面的数据，每个簇放 8 个扇区，每个扇区 512 个字节，那么一个簇的空间就是 4096 字节了，4KB。那么 11639 字节需要 3 个簇，这三个簇的开始的地址

就可以计算出来了。

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
00004800	F8	FF	FF	0F	FF	FF	FF	FF	FF	FF	FF	0F	04	00	00	00
00004810	05	00	00	00	FF	FF	FF	0F	00	00	00	00	00	00	00	00
00004820	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00

上面已经知道开始簇开始的地址了：03，那么开始地址为：F6000（根目录区地址）+ （03-2）*08*200=F7000（第一个簇开始地址）；这里 03 减去的 02 的意思是：簇号都是从 2 开始的，

第二个簇 4800+03*04=480C，查查 480C 里面的内容是什么：04 00 00 00，转化后为 04，不是 0x0FFFFFFF（文件最后一簇的标志），那么还有簇号存在（文件还没有放完呢，下一个簇不计算），第二个簇就可以算出来了，地址为 F6000+（04-2）*08*200 = F8000（第二个簇开始地址）；

480C 的内容是 04，指出的下个簇号地址位置，4800+04*04=4810，4810 的数据为 05，也不是 0x0FFFFFFF, 同样可以计算出第三个簇地址：F6000+（05-2）*08*200 = F9000（第三个簇开始地址）；继续看看下一个簇号：4800+05*04=4814，内容为 0x0FFFFFFF, 文件放置结束，没有了。

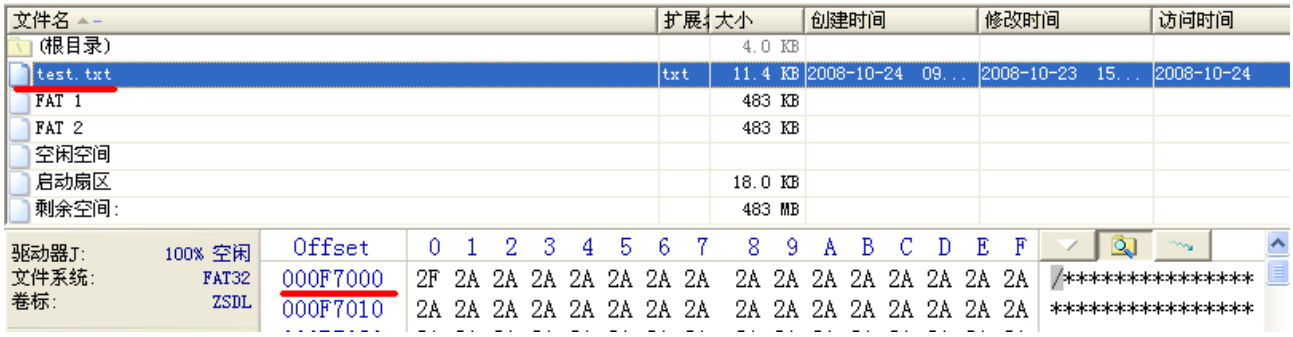
总结下：

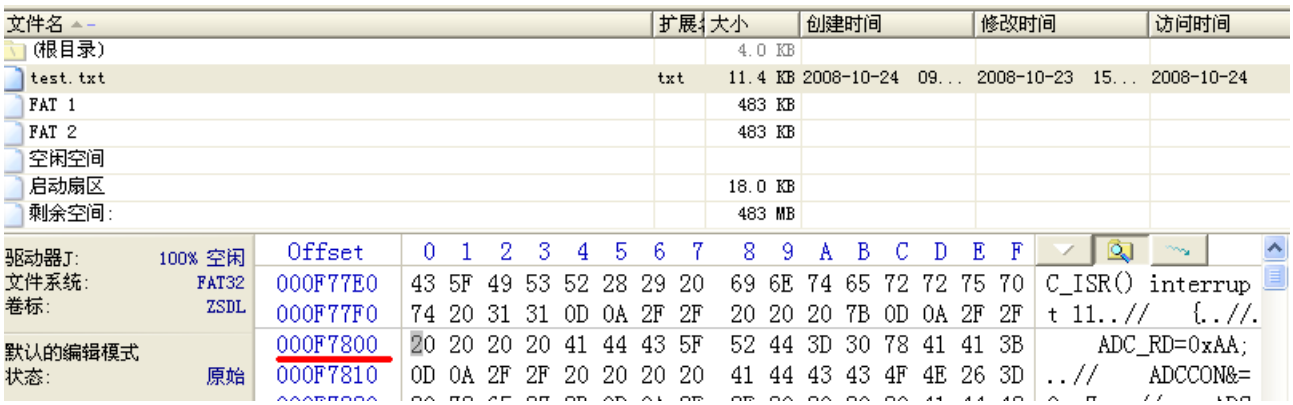
F7000（第一个簇开始地址）

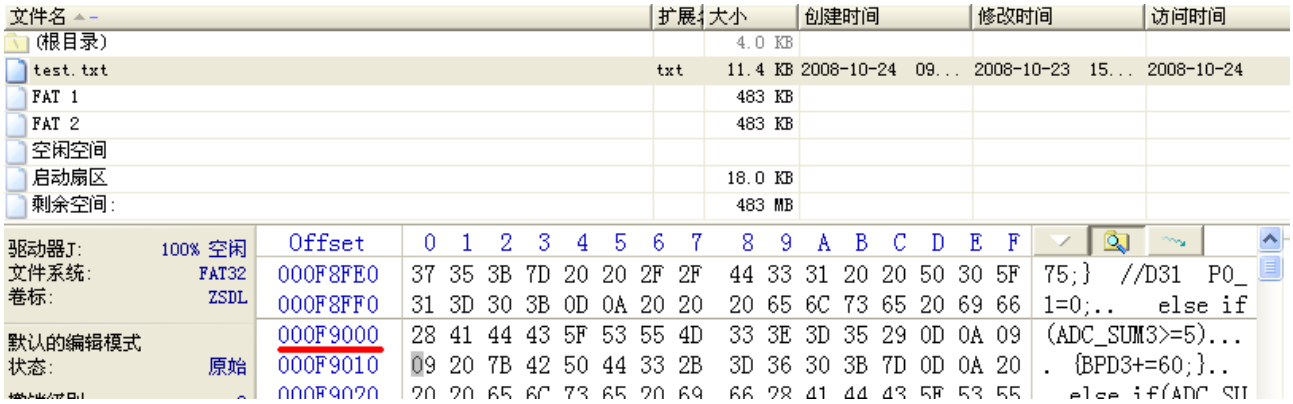
F8000（第二个簇开始地址）

F9000（第三个簇开始地址）

看图检验下。







暂时学习到这里，现在可以读取文件。但是读取长文件名，写文件如何进行，接下来继续学习。
资料的起源来自此，现在也回到这里。。。。