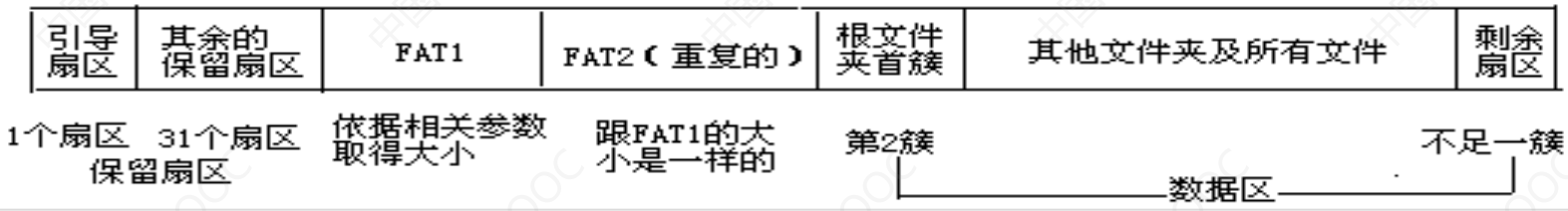
2.5 FAT32文件系统及数据恢复




计算机
网络
回收站
backup
Internet Explorer
2012年讲课比赛
Google Chrome
0.04K/S
22.4K/S
360 U盘小助手
设置
关闭
安全
CRUZER (I:)
剩余空间：7.4GB
U盘查杀
U盘鉴定
误删恢复
中简半

2.5.1 FAT32文件系统结构

引导扇区

FAT（File Allocation Table，文件分配表）

数据存储区
（以簇为单位，每簇包含多个扇区，以簇号进行标示）

描述分区属性：
1.分区大小；
2.簇的大小
3.FAT表个数与大小
4.分区引导程序等

FAT1+FAT2

两个功能：
1.记录数据存储区每一个簇的使用情况（是否被使用，或坏簇）；
2.形成每个文件的簇链表

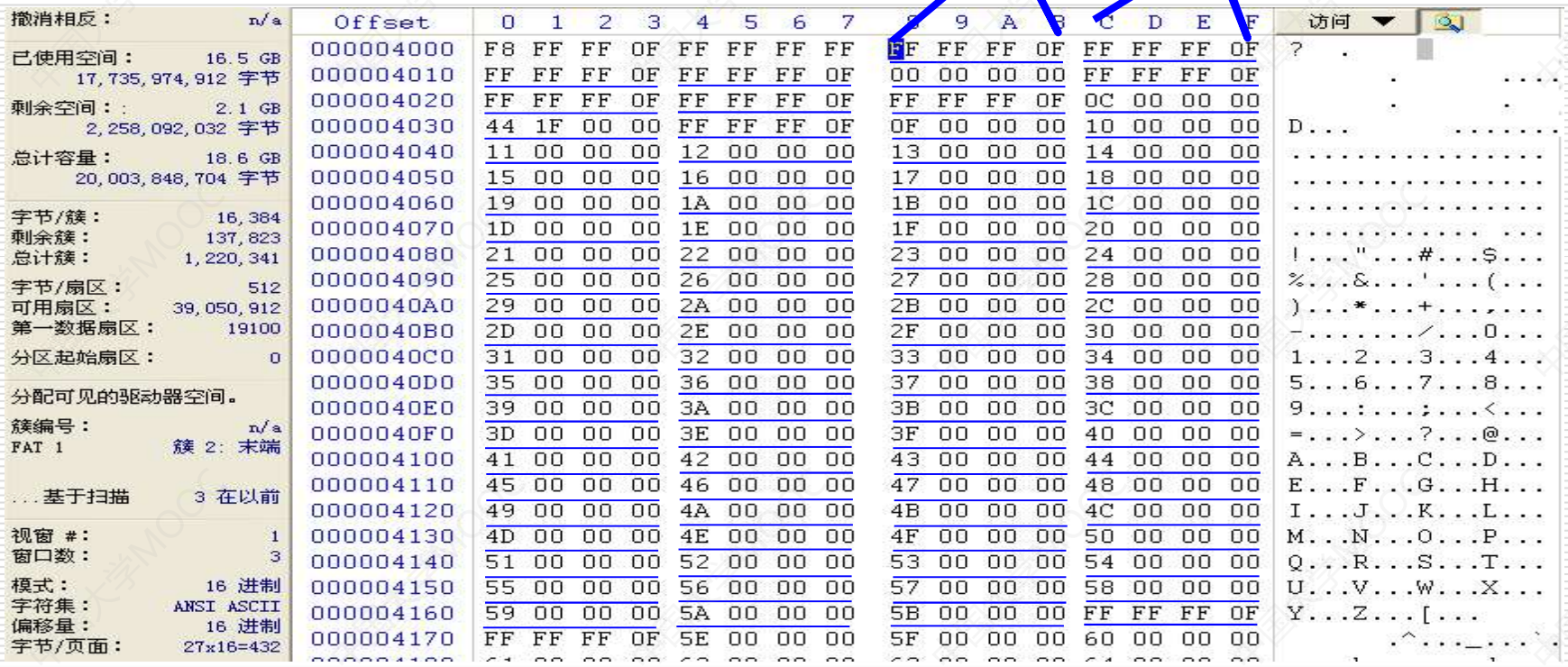
功能：存储两类数据
•目录项（目录和文件的属性信息，如文件名，大小，文件存储首簇号，时间等）-文件档案
•文件数据

概念1：簇

- 文件系统将磁盘空间以一定数目（2^n，n为整数）的扇区为单位进行划分，这样的单位称为簇。
  - 每扇区大小为**512**字节。
    - 簇的大小一般是**512B**、**1KB**、**2KB**、**4KB**、**8KB**、**16KB**、**32KB**、**64KB**等。

簇是进行文件空间分配的最小单位。

概念2： FAT表

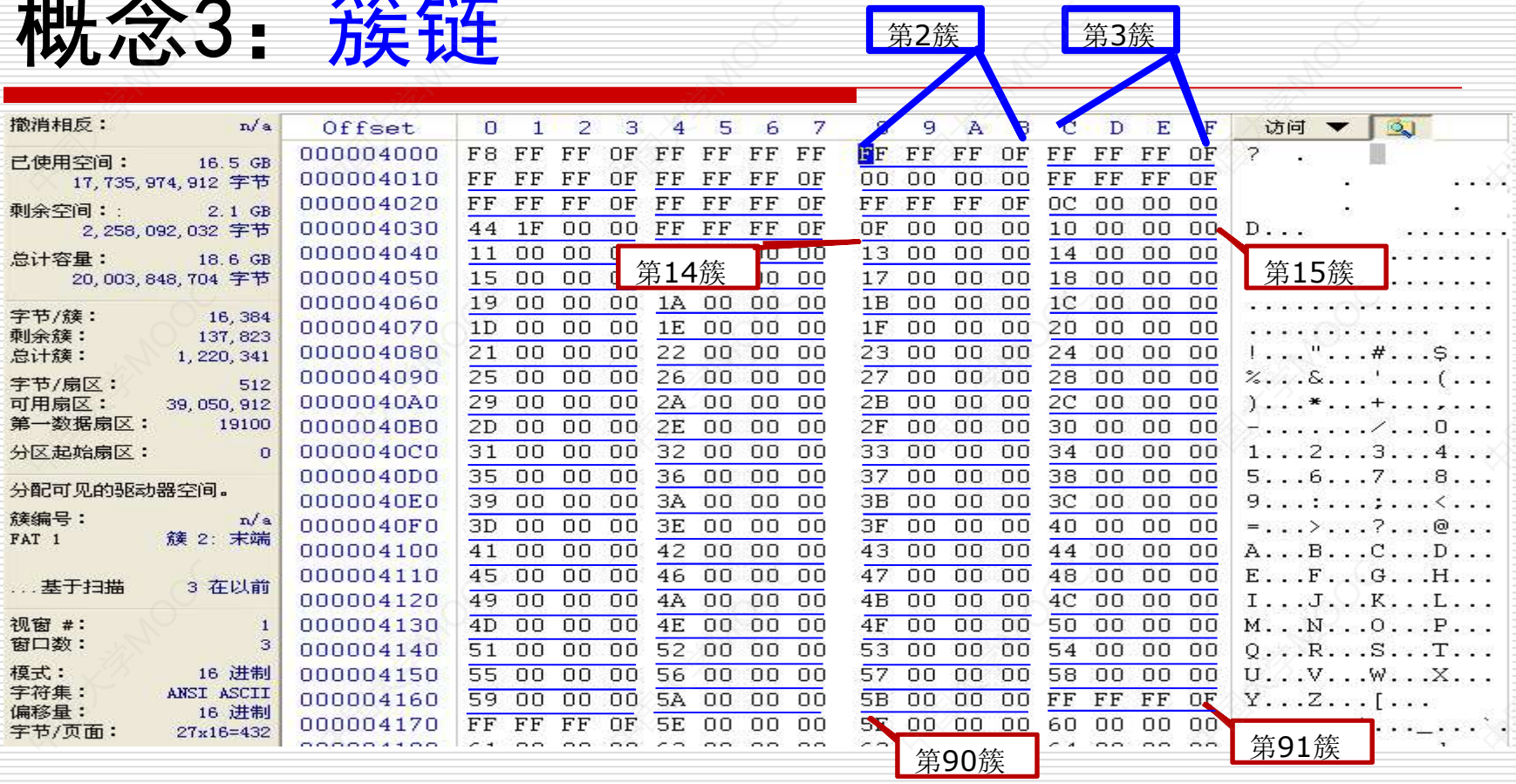

第2簇
第3簇
撤消相反： n/a
已使用空间： 16.5 GB
17,735,974,912 字节
剩余空间： 2.1 GB
2,258,092,032 字节
总计容量： 18.6 GB
20,003,848,704 字节
字节/簇： 16,384
剩余簇： 137,823
总计簇： 1,220,341
字节/扇区： 512
可用扇区： 39,050,912
第一数据扇区： 19100
分区起始扇区： 0
分配可见的驱动器空间。
簇编号： n/a
FAT 1 簇 2: 末端
...基于扫描 3 在以前
视窗 #: 1
窗口数： 3
模式： 16 进制
字符集： ANSI ASCII
偏移量： 16 进制
字节/页面： 27x16=432
Offset 0 1 2 3 4 5 6 7 8 9 A B C D E F
000004000 F8 FF FF 0F FF FF FF FF FF FF FF 0F FF FF FF 0F
000004010 FF FF FF 0F FF FF FF 0F 00 00 00 00 FF FF FF 0F
000004020 FF FF FF 0F FF FF FF 0F FF FF FF 0F 0C 00 00 00
000004030 44 1F 00 00 FF FF FF 0F 0F 00 00 00 10 00 00 00
000004040 11 00 00 00 12 00 00 00 13 00 00 00 14 00 00 00
000004050 15 00 00 00 16 00 00 00 17 00 00 00 18 00 00 00
000004060 19 00 00 00 1A 00 00 00 1B 00 00 00 1C 00 00 00
000004070 1D 00 00 00 1E 00 00 00 1F 00 00 00 20 00 00 00
000004080 21 00 00 00 22 00 00 00 23 00 00 00 24 00 00 00
000004090 25 00 00 00 26 00 00 00 27 00 00 00 28 00 00 00
0000040A0 29 00 00 00 2A 00 00 00 2B 00 00 00 2C 00 00 00
0000040B0 2D 00 00 00 2E 00 00 00 2F 00 00 00 30 00 00 00
0000040C0 31 00 00 00 32 00 00 00 33 00 00 00 34 00 00 00
0000040D0 35 00 00 00 36 00 00 00 37 00 00 00 38 00 00 00
0000040E0 39 00 00 00 3A 00 00 00 3B 00 00 00 3C 00 00 00
0000040F0 3D 00 00 00 3E 00 00 00 3F 00 00 00 40 00 00 00
000004100 41 00 00 00 42 00 00 00 43 00 00 00 44 00 00 00
000004110 45 00 00 00 46 00 00 00 47 00 00 00 48 00 00 00
000004120 49 00 00 00 4A 00 00 00 4B 00 00 00 4C 00 00 00
000004130 4D 00 00 00 4E 00 00 00 4F 00 00 00 50 00 00 00
000004140 51 00 00 00 52 00 00 00 53 00 00 00 54 00 00 00
000004150 55 00 00 00 56 00 00 00 57 00 00 00 58 00 00 00
000004160 59 00 00 00 5A 00 00 00 5B 00 00 00 FF FF FF 0F
000004170 FF FF FF 0F 5E 00 00 00 5F 00 00 00 60 00 00 00
访问

概念3：簇链

- 一个文件所占用簇的序号形成的单向链表。

- 实现方法：
  - 在文件占用簇的对应簇号的FAT项，填写下一个簇的簇号，如果为最后一簇，则输入结束标识“FFFFFF0F”

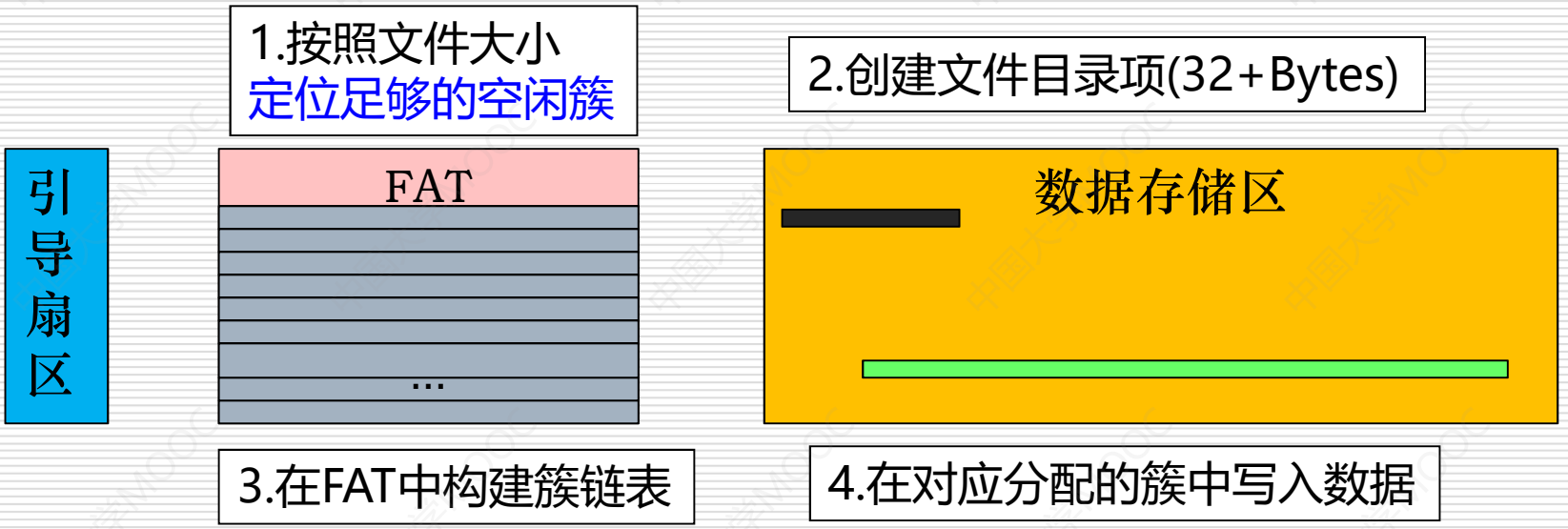
概念3：簇链


第2簇
第3簇
第14簇
第15簇
第90簇
第91簇
撤消相反： n/a
已使用空间： 16.5 GB
17,735,974,912 字节
剩余空间： 2.1 GB
2,258,092,032 字节
总计容量： 18.6 GB
20,003,848,704 字节
字节/簇： 16,384
剩余簇： 137,823
总计簇： 1,220,341
字节/扇区： 512
可用扇区： 39,050,912
第一数据扇区： 19100
分区起始扇区： 0
分配可见的驱动器空间。
簇编号： n/a
FAT 1 簇 2: 末端
...基于扫描 3 在以前
视窗 #： 1
窗口数： 3
模式： 16 进制
字符集： ANSI ASCII
偏移量： 16 进制
字节/页面： 27x16=432
Offset 0 1 2 3 4 5 6 7 8 9 A B C D E F
000004000 F8 FF FF 0F FF FF FF FF FF FF FF 0F FF FF FF 0F
000004010 FF FF FF 0F FF FF FF 0F 00 00 00 00 FF FF FF 0F
000004020 FF FF FF 0F FF FF FF 0F FF FF FF 0F 0C 00 00 00
000004030 44 1F 00 00 FF FF FF 0F 0F 00 00 00 10 00 00 00
000004040 11 00 00 00 00 00 00 00 13 00 00 00 14 00 00 00
000004050 15 00 00 00 00 00 00 00 17 00 00 00 18 00 00 00
000004060 19 00 00 00 1A 00 00 00 1B 00 00 00 1C 00 00 00
000004070 1D 00 00 00 1E 00 00 00 1F 00 00 00 20 00 00 00
000004080 21 00 00 00 22 00 00 00 23 00 00 00 24 00 00 00
000004090 25 00 00 00 26 00 00 00 27 00 00 00 28 00 00 00
0000040A0 29 00 00 00 2A 00 00 00 2B 00 00 00 2C 00 00 00
0000040B0 2D 00 00 00 2E 00 00 00 2F 00 00 00 30 00 00 00
0000040C0 31 00 00 00 32 00 00 00 33 00 00 00 34 00 00 00
0000040D0 35 00 00 00 36 00 00 00 37 00 00 00 38 00 00 00
0000040E0 39 00 00 00 3A 00 00 00 3B 00 00 00 3C 00 00 00
0000040F0 3D 00 00 00 3E 00 00 00 3F 00 00 00 40 00 00 00
000004100 41 00 00 00 42 00 00 00 43 00 00 00 44 00 00 00
000004110 45 00 00 00 46 00 00 00 47 00 00 00 48 00 00 00
000004120 49 00 00 00 4A 00 00 00 4B 00 00 00 4C 00 00 00
000004130 4D 00 00 00 4E 00 00 00 4F 00 00 00 50 00 00 00
000004140 51 00 00 00 52 00 00 00 53 00 00 00 54 00 00 00
000004150 55 00 00 00 56 00 00 00 57 00 00 00 58 00 00 00
000004160 59 00 00 00 5A 00 00 00 5B 00 00 00 FF FF FF 0F
000004170 FF FF FF 0F 5E 00 00 00 5F 00 00 00 60 00 00 00
访问

2.5.2文件的存储与删除

中国大学MOOC

文件的存储


1.按照文件大小
定位足够的空闲簇
2.创建文件目录项(32+Bytes)
引导扇区
FAT
...
数据存储区
3.在FAT中构建簇链表
4.在对应分配的簇中写入数据

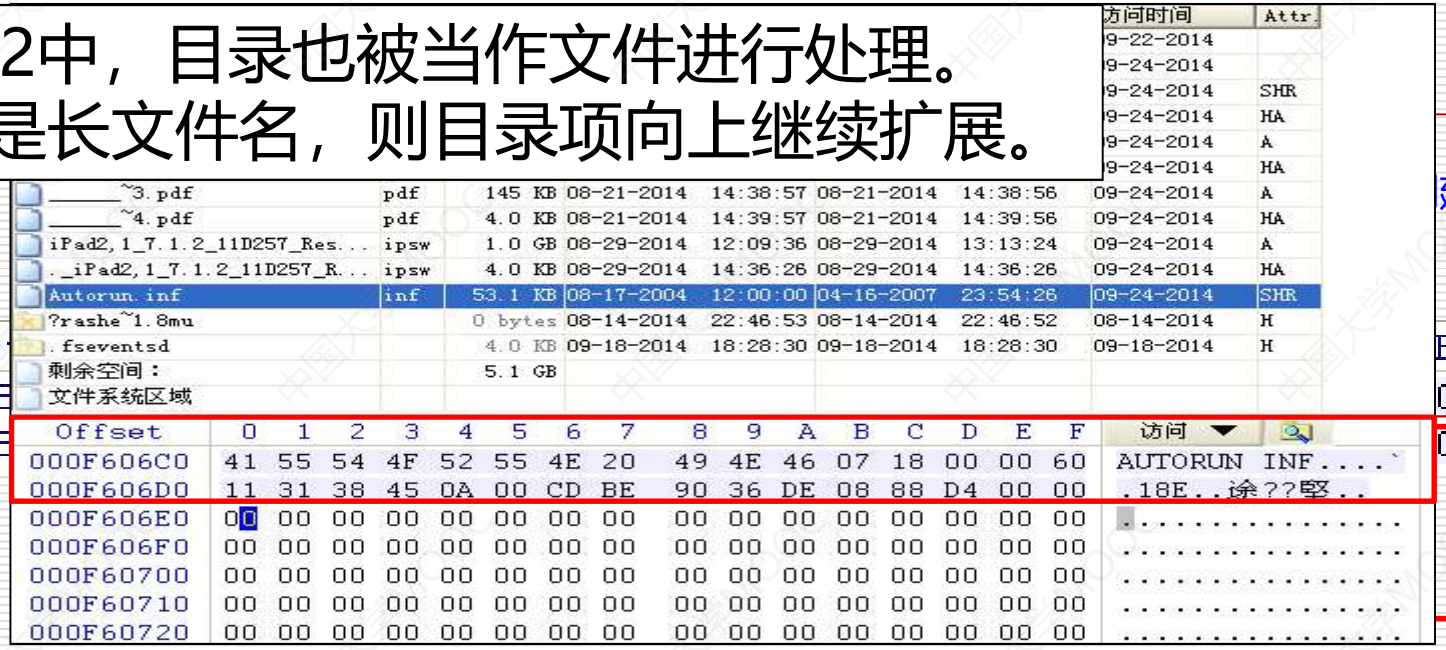
操作示意图

目录项的含义

（Short Directory Entry）

这个是短文件名的大小标志：
FNAME_LOWER_CASE　　0x08——01000
FEXT_NAME_LOWER_CASE　0x10——10000
如果文件名是小写的话0x08，而如果扩展名是小写的话则设置0x10，
而如果文件名和扩展名都是小写的则11000（0x18）

FAT32中，目录也被当作文件进行处理。
如果是长文件名，则目录项向上继续扩展。



名称	类型	大小	修改时间	创建时间	访问时间	Attr
_____~3.pdf	pdf	145 KB	08-21-2014 14:38:57	08-21-2014 14:38:56	09-24-2014	A
_____~4.pdf	pdf	4.0 KB	08-21-2014 14:39:57	08-21-2014 14:39:56	09-24-2014	HA
iPad2,1_7.1.2_11D257_Res...	ipsw	1.0 GB	08-29-2014 12:09:36	08-29-2014 13:13:24	09-24-2014	A
._iPad2,1_7.1.2_11D257_R...	ipsw	4.0 KB	08-29-2014 14:36:26	08-29-2014 14:36:26	09-24-2014	HA
Autorun.inf	inf	53.1 KB	08-17-2004 12:00:00	04-16-2007 23:54:26	09-24-2014	SHR
?rashe~1.8mu		0 bytes	08-14-2014 22:46:53	08-14-2014 22:46:52	08-14-2014	H
.fseventsd		4.0 KB	09-18-2014 18:28:30	09-18-2014 18:28:30	09-18-2014	H
剩余空间：		5.1 GB				
文件系统区域						

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	访问
000F606C0	41	55	54	4F	52	55	4E	20	49	4E	46	07	18	00	00	60	AUTORUN INF....`
000F606D0	11	31	38	45	0A	00	CD	BE	90	36	DE	08	88	D4	00	00	.18E..途??堅..
000F606E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000F606F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000F60700	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000F60710	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000F60720	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....

建时间

Offse E F

000F606 0 60

000F606 0 00

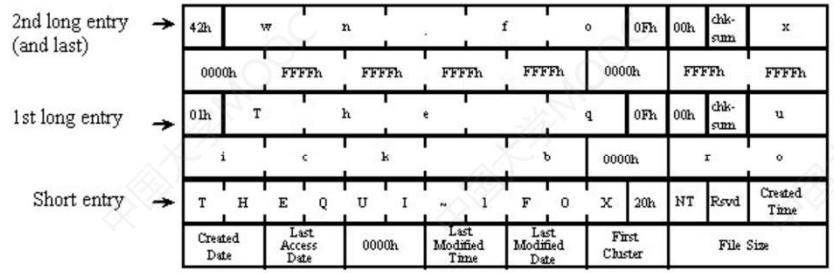
000F606C0	41	55	54	4F	52	55	4E	20	49	4E	46	07	18	00	00	60	AUTORUN INF....`
000F606D0	11	31	38	45	0A	00	CD	BE	90	36	DE	08	88	D4	00	00	.18E..途??堅..

长目录项

（LDE，Long Directory Entry）

名字	偏移(字节)	大小(字节数)	描述
mOrder	0	1	这表示当前DE在LDE序列中的序号 如果这个值是和0x40相与的结果，则表示这是LDE序列中最后一个LDE了
mName1	1	10	LDE中的前1-5个字符，Unicode。
mAttr	11	1	文件属性，只能是ATTR_LONG_NAME（0x0F）
mNameCase	12	1	在这里一直为0
mChksum	13	1	校验和。这个值由于此对应的SDE的前11字节计算而得，具体计算等下再讲。
mName2	14	12	LDE中的前6-11个字符，Unicode。
mFstClusLO	26	2	0
mName3	28	4	LDE中的前12-13个字符，Unicode。

如文件名为“The quick brown.fox”的磁盘结构




```
42 77 00 6E 00 2E 00 66  00 6F 00 0F 00 07 78 00  Bw.n...f.o....x.
00 00 FF FF FF FF FF FF  FF FF 00 00 FF FF FF FF  ................
01 54 00 68 00 65 00 20  00 71 00 0F 00 07 75 00  .T.h.e. .q....u.
69 00 63 00 6B 00 20 00  62 00 00 00 72 00 6F 00  i.c.k. .b...r.o.
54 48 45 51 55 49 7E 31  46 4F 58 20 00 41 94 7D  THEQUI~1FOX .A擁
FC 40 FC 40 00 00 95 7D  FC 40 00 00 00 00 00 00  鋘鋘..昌鋘......
```

文件创建实例

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
000F606C0	41	55	54	4F	52	55	4E	20	49	4E	46	07	18	00	00	60
000F606D0	11	31	38	45	0A	00	CD	BE	90	36	DE	08	88	D4	00	00

首簇高16位

首簇低16位

文件大小

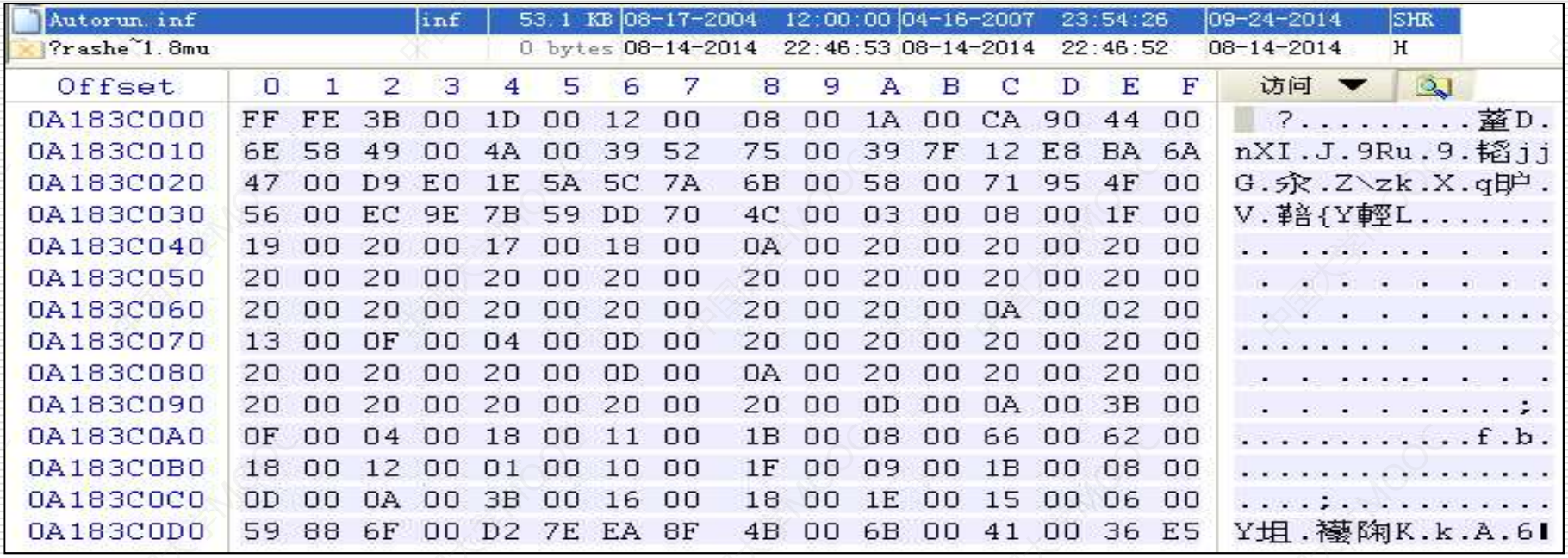
首簇号：000A08DE
（657630）

文件大小：D488
（54408字节，占14簇，每簇4096字节）

000287360	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000287370	00	00	00	00	00	00	00	00	DF	08	0A	00	E0	08	0A	00
000287380	E1	08	0A	00	E2	08	0A	00	E3	08	0A	00	E4	08	0A	00
000287390	E5	08	0A	00	E6	08	0A	00	E7	08	0A	00	E8	08	0A	00
0002873A0	E9	08	0A	00	EA	08	0A	00	EB	08	0A	00	FF	FF	FF	0F
0002873B0	ED	08	0A	00	EE	08	0A	00	EF	08	0A	00	F0	08	0A	00

000F606C0	41	55	54	4F	52	55	4E	20	49	4E	46	07	18	00	00	60	AUTORUN INF....`
000F606D0	11	31	38	45	0A	00	CD	BE	90	36	DE	08	88	D4	00	00	.18E..途??堅..

文件存储位置：0A183C000



Autorun.inf	inf	53.1 KB	08-17-2004 12:00:00	04-16-2007 23:54:26	09-24-2014	SHR
?rashe~1.8mu		0 bytes	08-14-2014 22:46:53	08-14-2014 22:46:52	08-14-2014	H

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	访问
0A183C000	FF	FE	3B	00	1D	00	12	00	08	00	1A	00	CA	90	44	00	?.....蓥D.
0A183C010	6E	58	49	00	4A	00	39	52	75	00	39	7F	12	E8	BA	6A	nXI.J.9Ru.9.铯jj
0A183C020	47	00	D9	E0	1E	5A	5C	7A	6B	00	58	00	71	95	4F	00	G.汆.Z\zk.X.q旷.
0A183C030	56	00	EC	9E	7B	59	DD	70	4C	00	03	00	08	00	1F	00	V.鞨{Y輕L.....
0A183C040	19	00	20	00	17	00	18	00	0A	00	20	00	20	00	20	00	.. ..
0A183C050	20	00	20	00	20	00	20	00	20	00	20	00	20	00	20	00	. . . .
0A183C060	20	00	20	00	20	00	20	00	20	00	20	00	0A	00	02	00	. . . .
0A183C070	13	00	0F	00	04	00	0D	00	20	00	20	00	20	00	20	00	....
0A183C080	20	00	20	00	20	00	0D	00	0A	00	20	00	20	00	20	00	. . ..
0A183C090	20	00	20	00	20	00	20	00	20	00	0D	00	0A	00	3B	00	. . . .;.
0A183C0A0	0F	00	04	00	18	00	11	00	1B	00	08	00	66	00	62	00	.....f.b.
0A183C0B0	18	00	12	00	01	00	10	00	1F	00	09	00	1B	00	08	00	.....
0A183C0C0	0D	00	0A	00	3B	00	16	00	18	00	1E	00	15	00	06	00	....;.....
0A183C0D0	59	88	6F	00	D2	7E	EA	8F	4B	00	6B	00	41	00	36	E5	Y坦.襼陶K.k.A.6▮

文件删除实例（AUTORUN.INF）-目录项的变化

文件被删除后目录项的变化

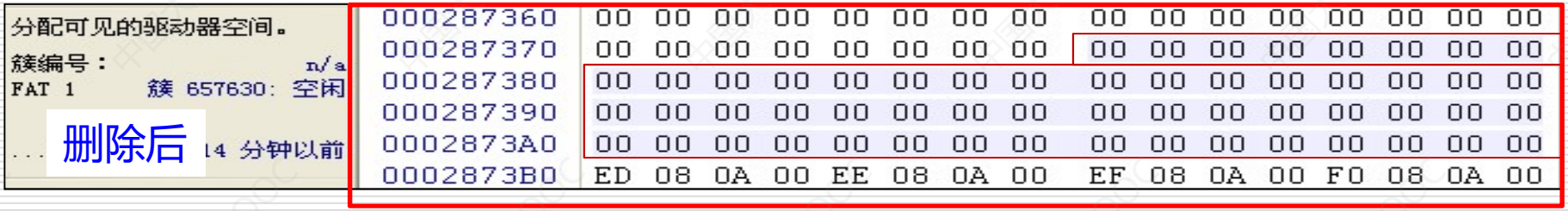
```
000F606C0  E5 55 54 4F 52 55 4E 20  49 4E 46 02 18 00 00 60  鈸TORUN INF....`
000F606D0  11 31 39 45 00 00 CD BE  90 36 DE 08 88 D4 00 00  .19E..途??堅..鬲.
```

2.首簇高位被清零

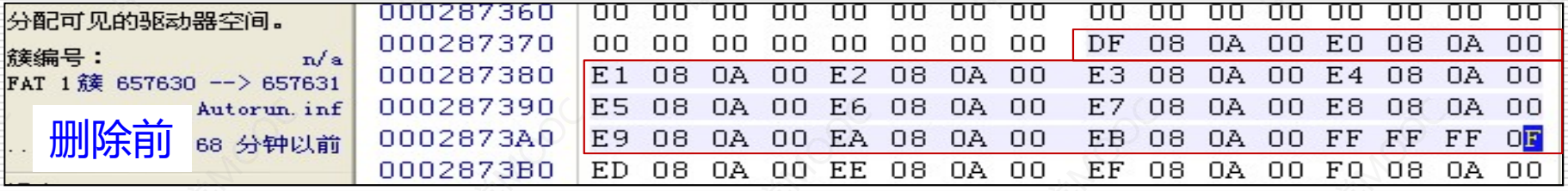
```
000F606C0  41 55 54 4F 52 55 4E 20  49 4E 46 07 18 00 00 60  AUTORUN INF....`
000F606D0  11 31 38 45 0A 00 CD BE  90 36 DE 08 88 D4 00 00  .18E..途??堅..
```

删除前

文件删除实例（AUTORUN.INF）
-簇链表变化



文件被删除后FAT表的变化：簇链表已被清空



文件删除实例（AUTORUN.INF）

-文件内容无变化

Autorun.inf	inf	53.1 KB	08-17-2004	12:00:00	04-16-2007	23:54:26	09-24-2014	SHR
?rashe~1.8mu		0 bytes	08-14-2014	22:46:53	08-14-2014	22:46:52	08-14-2014	H

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	访问
0A183C000	FF	FE	3B	00	1D	00	12	00	08	00	1A	00	CA	90	44	00	?.....蓥D.
0A183C010	6E	58	49	00	4A	00	39	52	75	00	39	7F	12	E8	BA	6A	nXI.J.9Ru.9.韬jj
0A183C020	47	00	D9	E0	1E	5A	5C	7A	6B	00	58	00	71	95	4F	00	G.汆.Z\zk.X.q眇.

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	访问
0A183C000	FF	FE	3B	00	1D	00	12	00	08	00	1A	00	CA	90	44	00	?.....蓥D.
0A183C010	6E	58	49	00	4A	00	39	52	75	00	39	7F	12	E8	BA	6A	nXI.J.9Ru.9.韬jj
0A183C020	47	00	D9	E0	1E	5A	5C	7A	6B	00	58	00	71	95	4F	00	G.汆.Z\zk.X.q眇.
0A183C030	56	00	EC	9E	7B	59	DD	70	4C	00	03	00	08	00	1F	00	V.鞨{Y輕L.....
0A183C040	19	00	20	00	17	00	18	00	0A	00	20	00	20	00	20	00	.. ..
0A183C050	20	00	20	00	20	00	20	00	20	00	20	00	20	00	20	00	. . . .
0A183C060	20	00	20	00	20	00	20	00	20	00	20	00	0A	00	02	00	. . . .
0A183C070	13	00	0F	00	04	00	0D	00	20	00	20	00	20	00	20	00	....
0A183C080	20	00	20	00	20	00	0D	00	0A	00	20	00	20	00	20	00	. . ..
0A183C090	20	00	20	00	20	00	20	00	20	00	0D	00	0A	00	3B	00	. . . . ;.
0A183C0A0	0F	00	04	00	18	00	11	00	1B	00	08	00	66	00	62	00	.....f.b.
0A183C0B0	18	00	12	00	01	00	10	00	1F	00	09	00	1B	00	08	00	.....
0A183C0C0	0D	00	0A	00	3B	00	16	00	18	00	1E	00	15	00	06	00	....;.....
0A183C0D0	59	88	6F	00	D2	7E	EA	8F	4B	00	6B	00	41	00	36	E5	Y坦.襼陱K.k.A.6▮

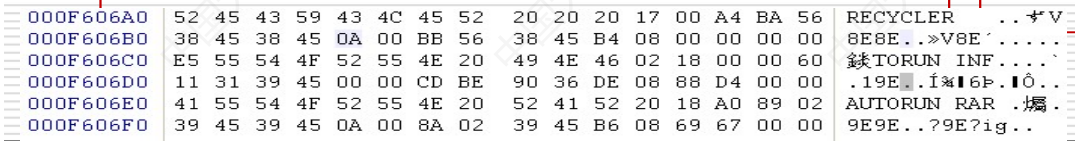
2.5.3被删除文件的恢复机理

差异

- 目录项：
  - 文件名首字节被修改为E5
  - 首簇高位被清零
- FAT表簇链：
  - 被全部清空
- 文件内容：
  - 无变化

可否恢复？

- 目录项
  - 文件名首位是否可还原？
  - 如何确定高位？
- FAT表簇链如何修复？
  - 连续存储（默认）
  - 总簇数（文件大小）



2.5.3被删除文件的恢复机理

- 还原文件名首字节
  - 长文件名：直接逆向定位完整文件名。
- 确定高位并还原
  - 参考相邻目录项的首簇高位
  - 从0往上试探，看首簇指向内容是否为预期文件头部
- 修复FAT表簇链
  - 通过文件大小计算所占簇数
  - 按照连续存储假设，进行簇链修补，其中末簇FAT项用0FFFFFFF结尾。

实例及操作

000F606C0	41	55	54	4F	52	55	4E	20	49	4E	46	07	18	00	00	60	AUTORUN INF....`
000F606D0	11	31	39	45	0A	00	CD	BE	90	36	DE	08	88	D4	00	00	.19E..Í¾▮6Þ.▮Ô..

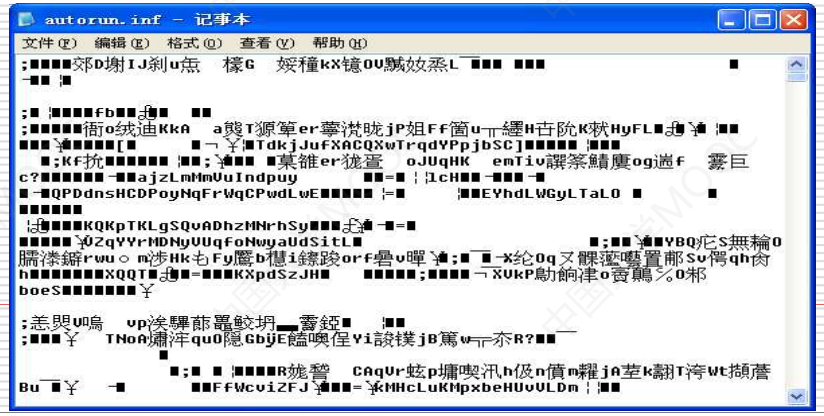
分配可见的驱动器空间。

簇编号： n/a

FAT 1 簇 657643: 末端

...基于扫描 4 分钟以前

000287360	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000287370	00	00	00	00	00	00	00	00	DF	08	0A	00	E0	08	0A	00
000287380	E1	08	0A	00	E2	08	0A	00	E3	08	0A	00	E4	08	0A	00
000287390	E5	08	0A	00	E6	08	0A	00	E7	08	0A	00	E8	08	0A	00
0002873A0	E9	08	0A	00	EA	08	0A	00	EB	08	0A	00	FF	FF	FF	0F
0002873B0	ED	08	0A	00	EE	08	0A	00	EF	08	0A	00	F0	08	0A	00



2.5.4数据恢复的几个注意事项

- 重要文件被删除之后，不得对分区继续进行写操作
- 定期对磁盘进行碎片整理，有利于数据恢复
- 格式文件更容易被恢复
- 大文件通过自动化工具进行完全恢复难度大

- 覆盖之后的恢复问题

中国大学MOOC