电子科技大学

计算机科学与工程学院

标 准 实 验 报 告

（实验）课程名称 信息对抗综合设计实验 II

电子科技大学教务处制表

电 子 科 技 大 学

实 验 报 告

学生姓名： 刘芷溢 学 号： 2020080907009 指导教师： 李忻洋

一、实验项目名称： FAT12 文件系统分析 DOS 中断向量

二、实验目的：

了解 FAT12 文件系统;熟悉 FAT12 文件系统结构如根目录区、FAT 表；掌握 FAT12 文件删除与恢复原理；掌握系统引导原理并编写引导代码使用自己的软盘进行引导。

三、实验原理：

虚拟机可以创建空白软盘；将已连接勾选掉软盘相当于弹出，虚拟机将修改写入软盘文件；

format a: /u 创建 FAT12 文件系统；dir 查看卷标；

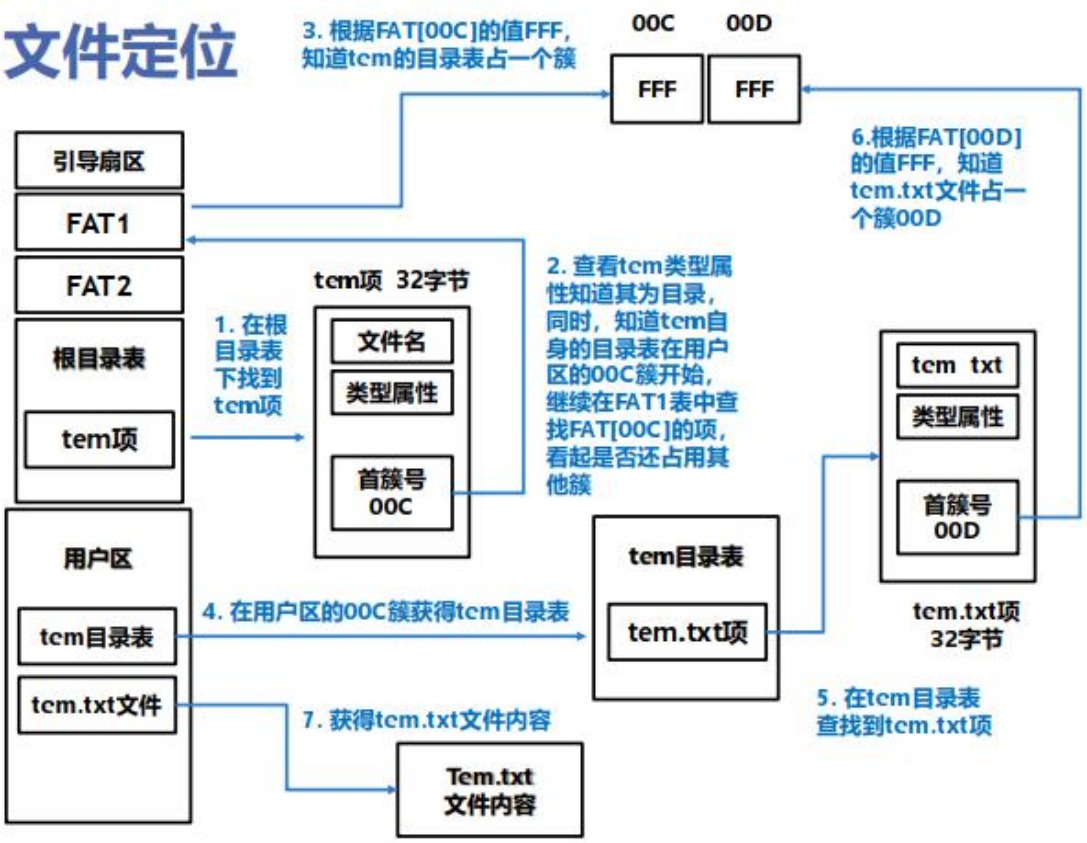
根目录区前有一个保留扇区，两个 FAT 表（每个 FAT 表占 9 个扇区）；在文件系统中，扇区被组成一个更大的单位簇文件，分配的最小单位是簇，簇由几个扇区组成在引导扇区的引导记录中定义（这

里为 512 字节）。

FAT 表：在 FAT12 文件系统中，FAT 表以 3 个半字节（3*0.5 Byte = 1.5 Byte =12 bit）来记录一个簇的相关情况；FAT 表中每 3 个半字节为一个元素， 这个元素就代表一个簇，簇号从 0 开始，这个元素中存放的整数值表示其链接的下一簇的簇号。FAT 表开始的 3 个字节没用于用户文件分配，用户的数据从簇 2 开始分配。

根目录：根目录表包含多条记录，每条记录占 32 字节，实验中我们主要关注文件名（查找需要）和首簇（遍历需要）；每一条记录，从该记录开始偏移 0xB 处有个字节指示出文件的类型；卷标为 28，文件为 20，目录为 10.

文件定位：通过根目录找到目录项，通过 FAT 表找到目录对应的簇；在用户数据区找到目标目录的目录表，在目录表找到目标文件，根据首簇号到 FAT 中查找下一簇号；最后到数据区找到文件内容。



删除与恢复文件：文件删除只是在目录表的该目录项的首字节变为 E5；同时该文件占据的 FAT 变为 00 00

系统引导：BIOS 在自检完成后，会根据用户指定的顺序从磁盘或光盘启动；如果以软盘启动， BIOS 会将第一个扇区（0 头 0 道 1 扇区）加载到内存 7C00H 处，并跳到该处执行，这段代码就是系统引导代码，它会运行操作系统加载器，加载我们的操作系统。

四、实验环境（设备、元器件）：

个人 PC 机；Windows10 系统；DOS 虚拟机 MS-DOS.vmx

五、实验步骤：

实验一：格式化软盘与 FAT12 初识

格式化后查看磁盘下目录（序号后 11 位的子目录）

```
A:\>dir

 Volume in drive A is 20080907009
 Volume Serial Number is 2F4F-10F4
 Directory of A:\

WINA20   386         9,349 05-31-94   6:22a
20080907     <DIR>          03-31-23   9:18a
80907009     <DIR>          03-31-23   9:38a
        3 file(s)          9,349 bytes
                       1,445,888 bytes free
```

根目录

```
00002600  32 30 30 38 30 39 30 37  30 30 39 28 00 00 00 00  20080907009(
00002610  00 00 00 00 00 00 C0 49  7F 56 00 00 00 00 00 00        ÀI V
00002620  57 49 4E 41 32 30 20 20  33 38 36 20 00 00 00 00  WINA20  386
00002630  00 00 00 00 00 00 C0 32  BF 1C 02 00 85 24 00 00        À2¿    …$
00002640  32 30 30 38 30 39 30 37  20 20 20 10 00 00 00 00  20080907
00002650  00 00 00 00 00 00 57 4A  7F 56 15 00 00 00 00 00        WJ V
00002660  38 30 39 30 37 30 30 39  20 20 20 10 00 00 00 00  80907009
00002670  00 00 00 00 00 00 DD 4C  7F 56 17 00 00 00 00 00        ÝL V
```

WINA20.386 文件占据 19 个簇，每簇扇区数 1，共占据 19 个扇区

```
00000200  F0 FF FF 03 40 00 05 60  00 07 80 00 09 A0 00 0B  ðÿÿ @   `   €
00000210  C0 00 0D E0 00 0F 00 01  11 20 01 13 40 01 FF FF  À  à        @ ÿÿ
00000220  FF 00 F0 FF 00 00 00 00  00 00 00 00 00 00 00 00  ÿ ðÿ
00000230  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
```

在子目录 80907009 创建 LIUZHIYI.txt

```
A:\80907009>dir

 Volume in drive A is 20080907009
 Volume Serial Number is 2F4F-10F4
 Directory of A:\80907009

.            <DIR>          03-31-23   9:38a
..           <DIR>          03-31-23   9:38a
LIUZHIYI TXT              24 03-31-23   9:39a
        3 file(s)             24 bytes
                       1,445,888 bytes free
```

定位子目录：

计算子目录：此时的簇号为 0x0017 (23)

用户区地址为：1+18+224*32/512 = 33 (DATA 区前面的扇区数)

33 + (23 - 2) = 54 = 0x36

0x36 * 200 = 0x6C00

```
00006C00  2E 20 20 20 20 20 20 20  20 20 20 10 00 00 00 00  .
00006C10  00 00 00 00 00 00 DD 4C  7F 56 17 00 00 00 00 00        ÝL V
00006C20  2E 2E 20 20 20 20 20 20  20 20 20 10 00 00 00 00  ..
00006C30  00 00 00 00 00 00 DD 4C  7F 56 00 00 00 00 00 00        ÝL V
00006C40  4C 49 55 5A 48 49 59 49  54 58 54 20 00 00 00 00  LIUZHIYITXT
00006C50  00 00 00 00 00 00 F9 4C  7F 56 18 00 18 00 00 00        ùL V
```

定位文件：

子目录下 LIUZHIYI.txt 簇为：0x0018

DATA 区地址：0x37 * 200 = 0x6E00

```
00006E00  32 30 32 30 30 38 30 39  30 37 30 30 39 5F 6C 69  2020080907009_li
00006E10  75 7A 68 69 79 69 0D 0A  0D 01 0E 01 0F 01 10 01  uzhiyi
```

实验二：文件删除与恢复

删除文件：

子目录显示

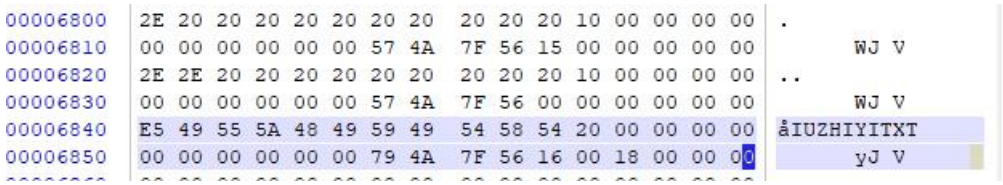
```
A:\80907009>dir

 Volume in drive A is 20080907009
 Volume Serial Number is 2F4F-10F4
 Directory of A:\80907009

.            <DIR>          03-31-23   9:38a
..           <DIR>          03-31-23   9:38a
       2 file(s)              0 bytes
                         1,446,400 bytes free
```

FAT 表，删除文件占据簇号由 FF FF 变为 00 F0

```
00000200  F0 FF FF 03 40 00 05 60  00 07 80 00 09 A0 00 0B  ðÿÿ @  `  €
00000210  C0 00 0D E0 00 0F 00 01  11 20 01 13 40 01 FF FF  À  à        @ ÿÿ
00000220  FF FF FF FF 00 00 00 00  00 00 00 00 00 00 00 00  ÿÿÿÿ
```

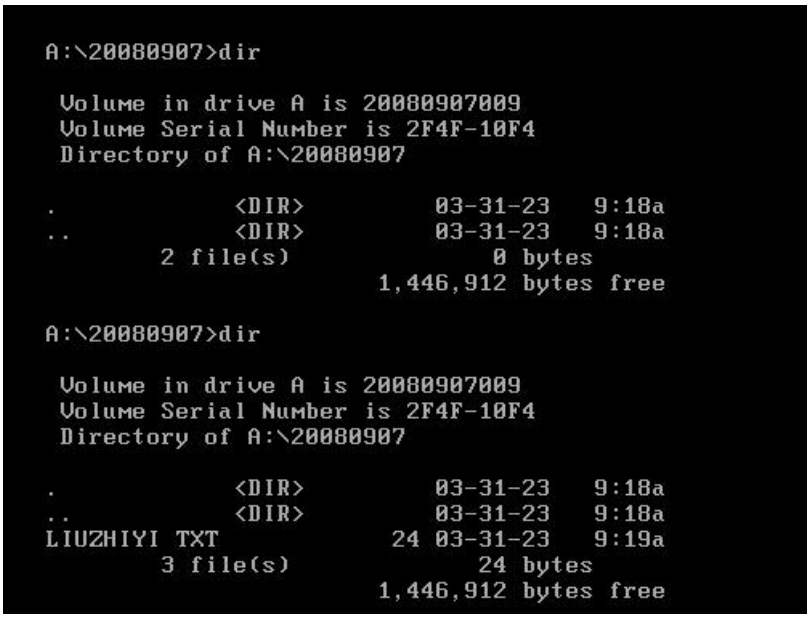
```
00000200  50 FF FF 03 40 00 05 60  00 07 80 00 09 A0 00 0B  ðÿÿ @  `  €
00000210  C0 00 0D E0 00 0F 00 01  11 20 01 13 40 01 FF FF  À  à        @ ÿÿ
00000220  FF 00 F0 FF 00 00 00 00  00 00 00 00 00 00 00 00  ÿ ðÿ
```

根目录区变化，删除文件目录项首字节变为 E5



```
00006800  2E 20 20 20 20 20 20 20  20 20 20 10 00 00 00 00  .
00006810  00 00 00 00 00 00 57 4A  7F 56 15 00 00 00 00 00        WJ V
00006820  2E 2E 20 20 20 20 20 20  20 20 20 10 00 00 00 00  ..
00006830  00 00 00 00 00 00 57 4A  7F 56 00 00 00 00 00 00        WJ V
00006840  E5 49 55 5A 48 49 59 49  54 58 54 20 00 00 00 00  åIUZHIYITXT
00006850  00 00 00 00 00 00 79 4A  7F 56 16 00 18 00 00 00        yJ V
```

恢复文件：文件目录项首字节改回 L 对应的 ASCII 码；FAT 表找到第一个空闲簇（文件大小小于一个簇）改为 FF XF；结果如下图，恢复成功。



```
A:\20080907>dir

 Volume in drive A is 20080907009
 Volume Serial Number is 2F4F-10F4
 Directory of A:\20080907

.            <DIR>          03-31-23   9:18a
..           <DIR>          03-31-23   9:18a
       2 file(s)              0 bytes
                      1,446,912 bytes free

A:\20080907>dir

 Volume in drive A is 20080907009
 Volume Serial Number is 2F4F-10F4
 Directory of A:\20080907

.            <DIR>          03-31-23   9:18a
..           <DIR>          03-31-23   9:18a
LIUZHIYI TXT             24 03-31-23   9:19a
       3 file(s)             24 bytes
                      1,446,912 bytes free
```

实验三：系统引导

设置系统为软盘启动；下载汇编工具 nasm，通过“nasm 汇编文件名 -o 生成文件名”的命令来生成 com 文件，生成所需的 com 文件后，将 com 文件中的机器码拷贝到软盘文件的第一个扇区（0 头 0 道 1 扇区）；引导代码如下

```
org 07c00h          ; 指定起始地址，告诉编译器程序加载到7c00
mov ax, cs
mov ds, ax
mov es, ax          ; ds = es = cs
call    DispStr          ; 调用显示字符串例程
jmp $   ; 无限循环，等待中断响应，$当前位置，即jmp首址
DispStr:
mov ax, BootMessage
mov bp, ax          ; ES:BP = 串地址
mov cx, 13          ; CX = 串长度  “Hello, OS world!”
mov ax, 1301h       ; AH = 13,  AL = 01h
mov bx, 000ch       ; 页号为0(BH = 0) 黑底红字(BL = 0Ch,高亮)
mov dl, 0
int 10h                ; 10h号中断 显示器和屏幕中断
ret
BootMessage: db "2020080907009"    ; 这里改为你的学号
times 510-($-$$) db 0
dw 0xaa55
```

六、实验结论：

FAT12 文件系统查找文件：文件簇号存放在 FAT 表中，寻找文件先找到目录表中的目录项，根据目录项的首簇号查找 FAT 表找到后续簇号，通过得到的簇号可以到用户数据区查找文件内容。

根目录

```
00002600  32 30 30 38 30 39 30 37  30 30 39 28 00 00 00 00  20080907009(
00002610  00 00 00 00 00 00 C0 49  7F 56 00 00 00 00 00 00        ÀI V
00002620  57 49 4E 41 32 30 20 20  33 38 36 20 00 00 00 00  WINA20  386
00002630  00 00 00 00 00 00 C0 32  BF 1C 02 00 85 24 00 00        À2¿   …$
00002640  32 30 30 38 30 39 30 37  20 20 20 10 00 00 00 00  20080907
00002650  00 00 00 00 00 00 57 4A  7F 56 15 00 00 00 00 00        WJ V
00002660  38 30 39 30 37 30 30 39  20 20 20 10 00 00 00 00  80907009
00002670  00 00 00 00 00 00 DD 4C  7F 56 17 00 00 00 00 00        ÝL V
```

WINA20.386 文件占据 19 个簇，每簇扇区数 1，共占据 19 个扇区

```
00000200  F0 FF FF 03 40 00 05 60  00 07 80 00 09 A0 00 0B  ðÿÿ @  `  €
00000210  C0 00 0D E0 00 0F 00 01  11 20 01 13 40 01 FF FF  À  à       @ ÿÿ
00000220  FF 00 F0 FF 00 00 00 00  00 00 00 00 00 00 00 00  ÿ ðÿ
00000230  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
```

定位子目录：

计算子目录：此时的簇号为 0x0017 (23)

用户区地址为：1+18+224*32/512 = 33 (DATA 区前面的扇区数)

33 + (23 - 2) = 54 = 0x36

0x36 * 200 = 0x6C00

```
00006C00  2E 20 20 20 20 20 20 20  20 20 20 10 00 00 00 00  .
00006C10  00 00 00 00 00 00 DD 4C  7F 56 17 00 00 00 00 00        ÝL V
00006C20  2E 2E 20 20 20 20 20 20  20 20 20 10 00 00 00 00  ..
00006C30  00 00 00 00 00 00 DD 4C  7F 56 00 00 00 00 00 00        ÝL V
00006C40  4C 49 55 5A 48 49 59 49  54 58 54 20 00 00 00 00  LIUZHIYITXT
00006C50  00 00 00 00 00 00 F9 4C  7F 56 18 00 18 00 00 00        ùL V
```

定位文件：

子目录下 LIUZHIYI.txt 簇为：0x0018

DATA 区地址：0x37 * 200 = 0x6E00

```
00006E00  32 30 32 30 30 38 30 39  30 37 30 30 39 5F 6C 69  2020080907009_li
00006E10  75 7A 68 69 79 69 0D 0A  0D 01 0E 01 0F 01 10 01  uzhiyi
```

FAT12 文件系统删除和恢复文件：

FAT 表，删除文件占据簇号由 FF FF 变为 00 F0

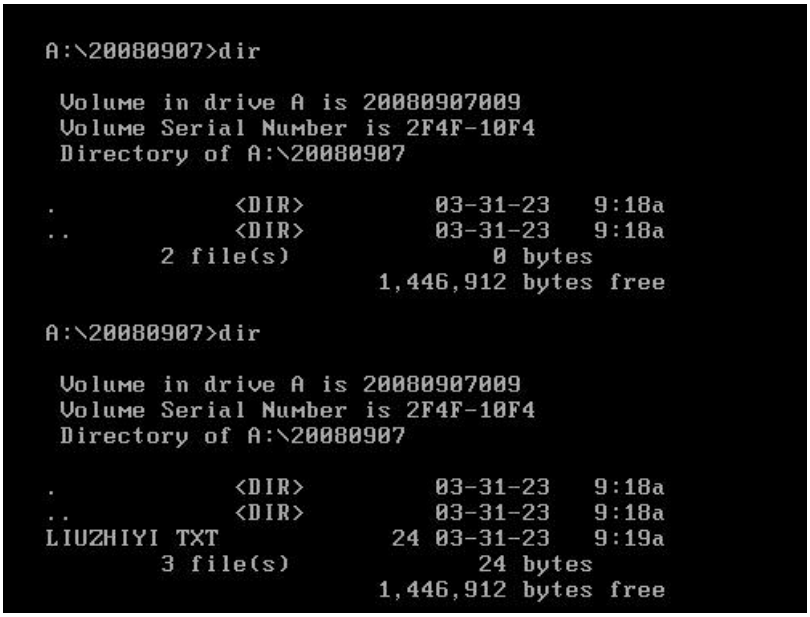
```
00000200  F0 FF FF 03 40 00 05 60  00 07 80 00 09 A0 00 0B  ðÿÿ @  `  €
00000210  C0 00 0D E0 00 0F 00 01  11 20 01 13 40 01 FF FF  À  à       @ ÿÿ
00000220  FF FF FF FF 00 00 00 00  00 00 00 00 00 00 00 00  ÿÿÿÿ
```

```
00000200  F0 FF FF 03 40 00 05 60  00 07 80 00 09 A0 00 0B  ðÿÿ @  `  €
00000210  C0 00 0D E0 00 0F 00 01  11 20 01 13 40 01 FF FF  À  à       @ ÿÿ
00000220  FF 00 F0 FF 00 00 00 00  00 00 00 00 00 00 00 00  ÿ ðÿ
```

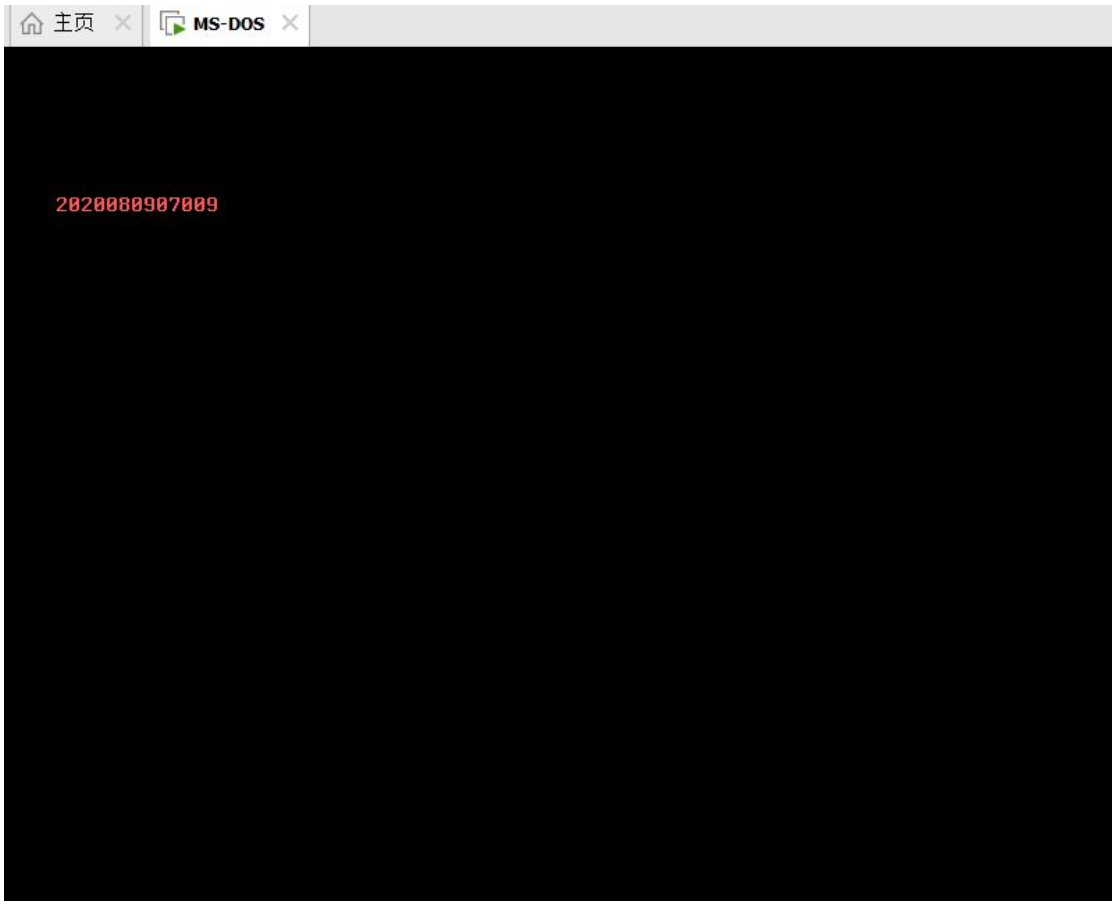
根目录区变化，删除文件目录项首字节变为 E5

```
00006800  2E 20 20 20 20 20 20 20  20 20 20 10 00 00 00 00  .
00006810  00 00 00 00 00 00 57 4A  7F 56 15 00 00 00 00 00        WJ V
00006820  2E 2E 20 20 20 20 20 20  20 20 20 10 00 00 00 00  ..
00006830  00 00 00 00 00 00 57 4A  7F 56 00 00 00 00 00 00        WJ V
00006840  E5 49 55 5A 48 49 59 49  54 58 54 20 00 00 00 00  åIUZHIYITXT
00006850  00 00 00 00 00 00 79 4A  7F 56 16 00 18 00 00 00        yJ V
```

恢复文件：文件目录项首字节改回 L 对应的 ASCII 码；FAT 表找到第一个空闲簇（文件大小小于一个簇）改为 FF XF；结果如下图，恢复成功。



系统引导：如果以软盘启动， BIOS 会将第一个扇区（0 头 0 道 1 扇区）加载到内存 7C00H 处，并跳到该处执行，这段代码就是系统引导代码，它会运行操作系统加载器，加载我们的操作系统。通过运行上面我们编写的引导代码，屏幕中成功打印了学号“2020080907009”。



七、总结及心得体会：

通过这次实验，我对 DOS 下的 FAT12 文件系统有了深刻的认识；了解到 FAT12 文件系统的 FAT 表、根目录表、引导扇区以及用户数据区；掌握了查找文件的方法，理解了文件删除更多的是逻辑删除，其文件内容在没有被覆写之前仍然在磁盘中；掌握了手动文件恢复的方法；同时也学习了软盘启动时系统引导的过程，编写了引导代码，让其执行打印学号的功能，让我对系统有了更深刻的认识和兴趣。

八、对本实验过程及方法、手段的改进建议：

希望可以有高级语言编写的代码，多一些引导代码的讲解和示例。

报告评分：

指导教师签字：