实验二
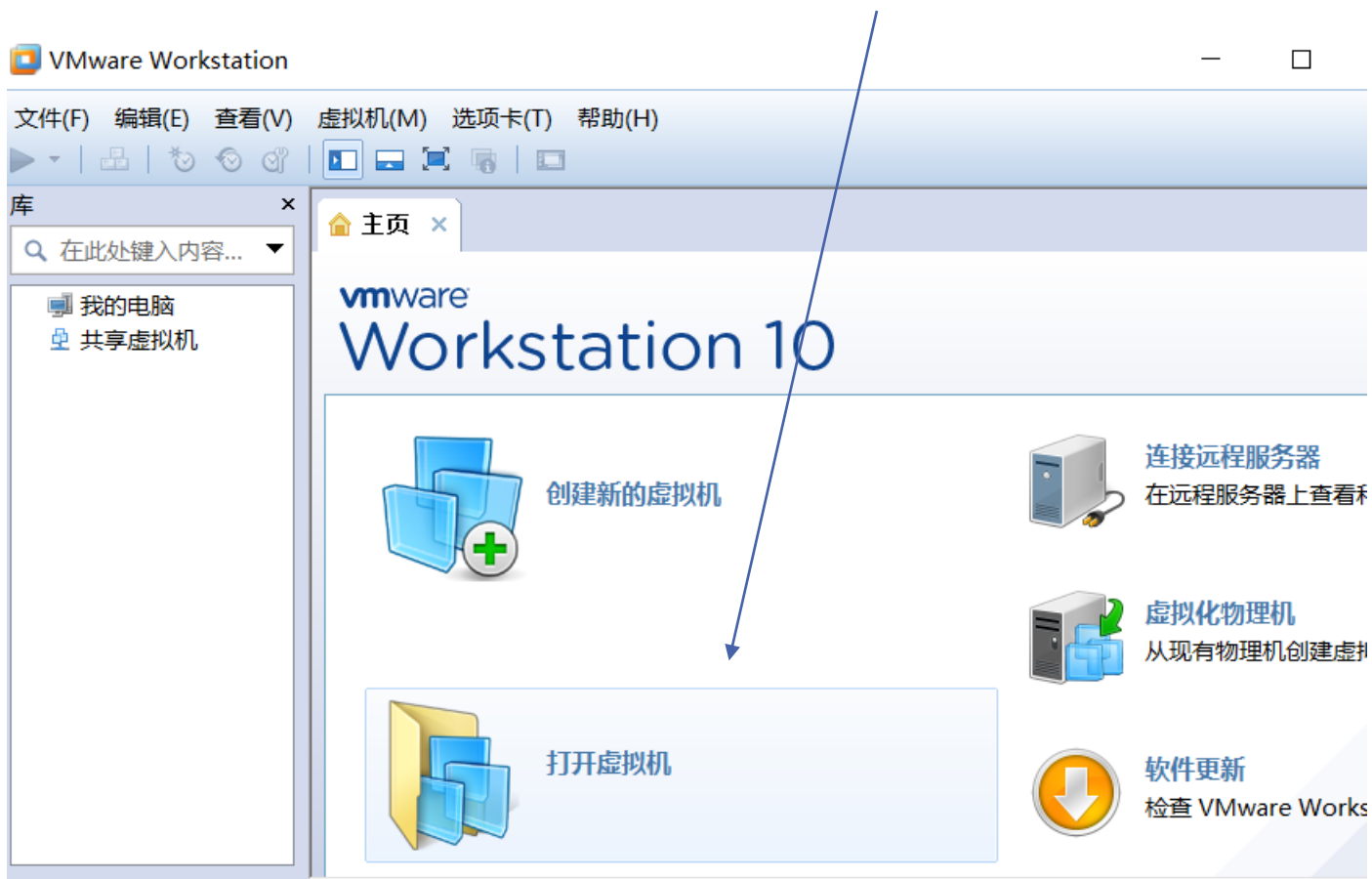# FAT12文件系统分析
DOS中断向量

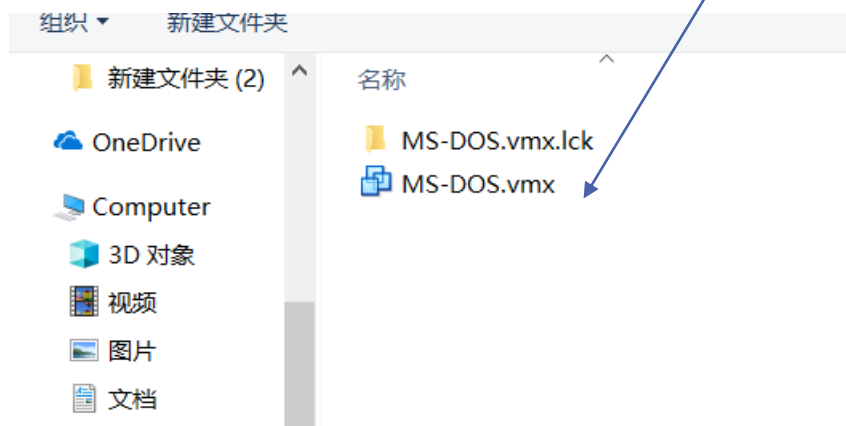# 实验准备：DOS环境

安装DOS虚拟机

解压缩提供的DOS虚拟机压缩包
安装VMWare Workstaion —— 选择打开虚拟机

安装DOS虚拟机

现在解压缩文件目录，打开MS-DOS.vmx

组织▼　　新建文件夹

- 新建文件夹 (2)
- OneDrive
- Computer
- 3D 对象
- 视频
- 图片
- 文档

名称

MS-DOS.vmx.lck

MS-DOS.vmx

选择获取所有权

VMware Workstation　　　　×

⚠ 该虚拟机似乎正在使用中。

如果该虚拟机未在使用，请按"获取所有权(T)"按钮获取它的所有权。否则，请按"取消(C)"按钮以防损坏。

配置文件: C:\Users\qiuxw\Desktop\【实验课】信息综合对抗II 2021\2021-第二次实验课\DOS\MS-DOS.vmx。
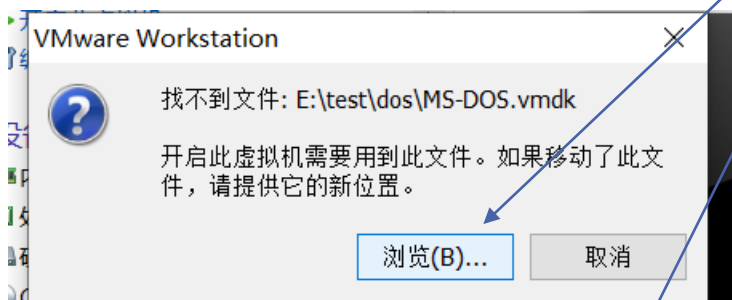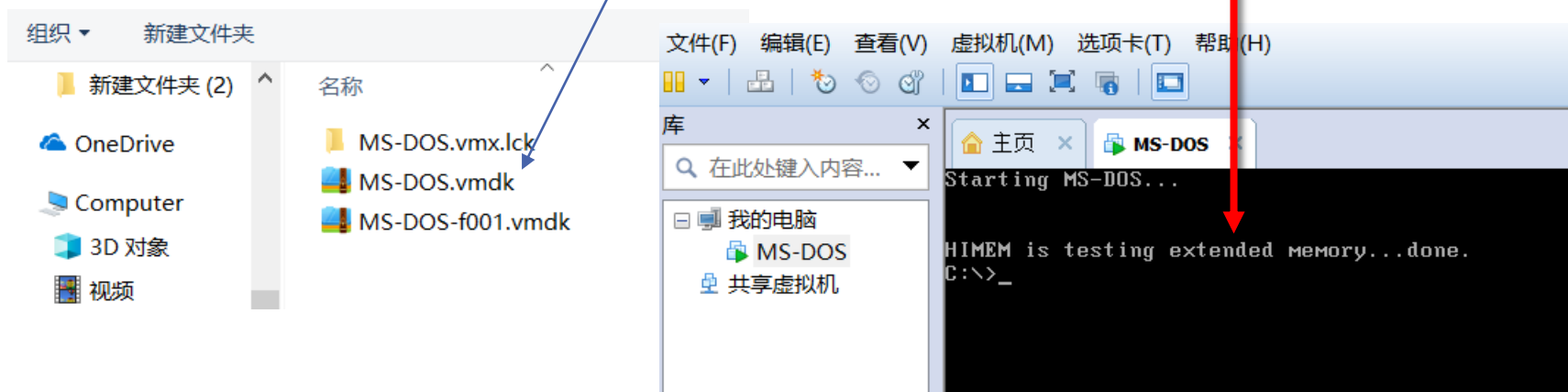
获取所有权(T)　　取消

安装DOS虚拟机

开启虚拟机

安装DOS虚拟机

在解压缩目录下加载虚拟机的MS-DOS.vmdk文件
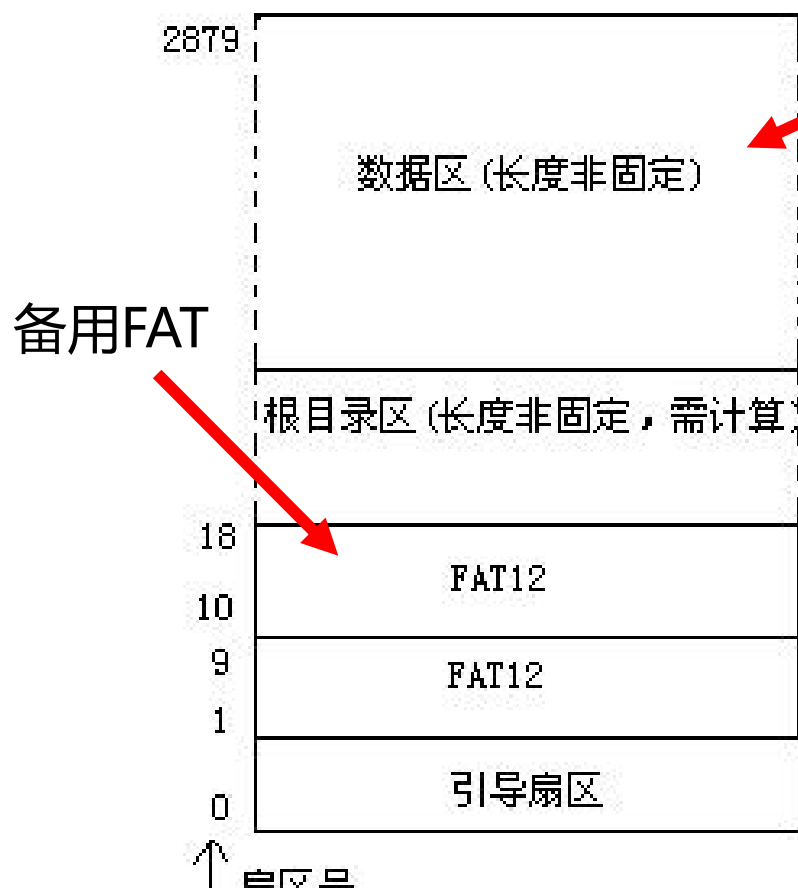
等待DOS系统启动

FAT12文件系统实验

FAT12文件系统介绍

1个FAT9个扇区，引导扇区1个扇区，根目录区有224条记录（一个记录32字节），这些参数都都可以在引导扇区的引导记录中设定

用户数据：（文件和子目录）数据真正存放的区域

文件目录表（DIR）：记录根目录文件项的表，文件项包括文件，目录。通过它可以查找到根目录下的文件和目录信息，比名称，大小，日期等
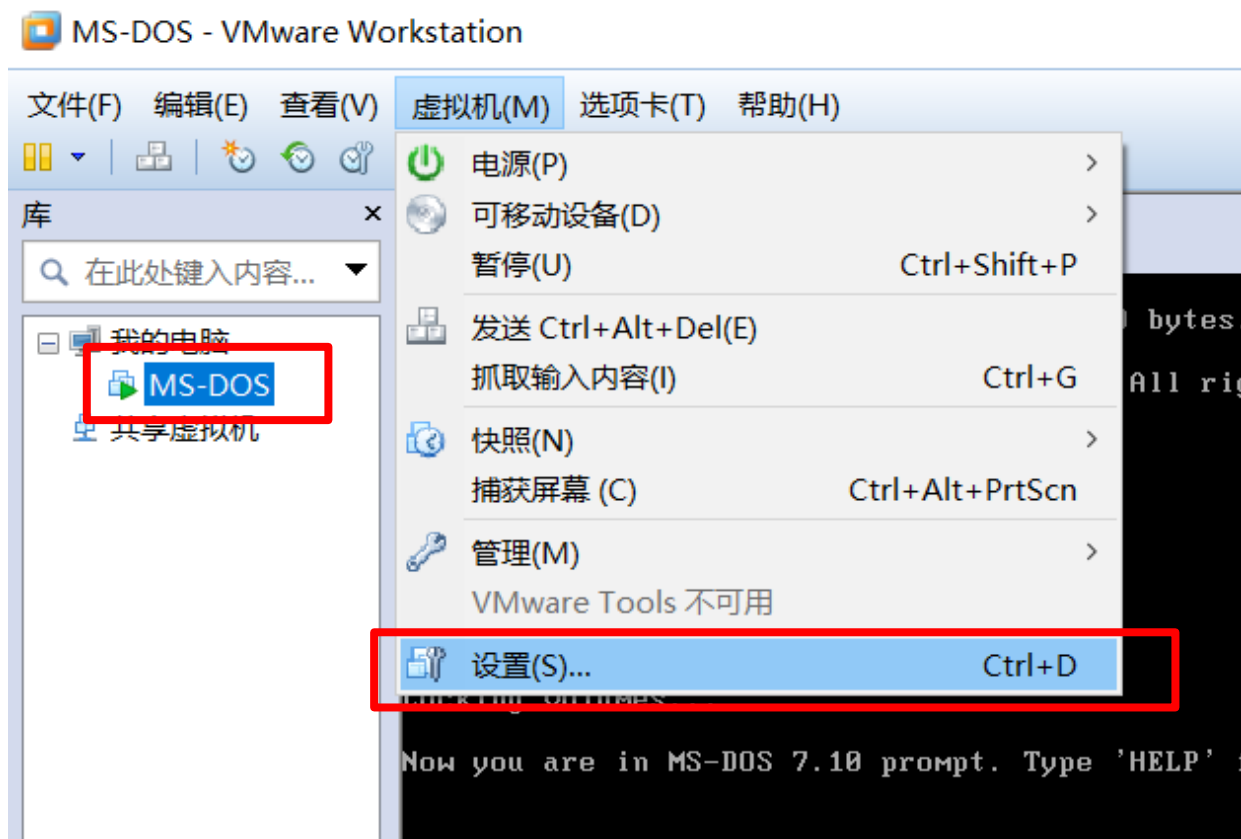
文件分配表（FAT）：记录已分配的扇区和可用扇区，并通过链表依序记录一个文件占用的扇区

引导扇区（DBR）：记录磁盘和文件系统相关的各种参数，比如扇区大小，一簇的扇区数等

1 创建FAT12文件系统

虚拟机生成空白软盘文件

▶ 选择MS-DOS虚拟机，选择虚拟机的设置菜单产生一张空白磁盘

► 1 在硬件中添加软盘

► 2 选择创建软盘映像文件

▶ 输入创建的软盘文件名，选择已连接插入软盘

名称
📁 564d2108-79eb-395b-5edf-b52e7f2..
📁 MS-DOS.vmdk.lck
📁 MS-DOS.vmx.lck

💻 Computer
　⯈ 🧊 3D 对象
　⯈ 🎞 视频
　⯈ 🖼 图片
　⯈ 📄 文档
　⯈ ⬇ 下载
　⯈ 🎵 音乐
　⯈ 🖥 桌面
　⯈ 💾 Windows (C:)
　⯈ 🖧 网络

文件名(N): flp1.flp

保存类型(T): 软盘映像(*.flp)

硬件　　选项

设备	摘要
🖴 内存	16 MB
⬜ 处理器	1
🖴 硬盘(IDE)	20 MB (预先分配)
💿 CD/DVD (IDE)	自动检测
💾 软盘	正在使用文件 E:\mydocs\教学\病...
🖧 网络适配器	NAT
🔊 声卡	自动检测
🖥 显示器	自动检测

设备状态
☑ 已连接(C)
☐ 启动时连接(O)

连接
○ 使用物理驱动器(P):
　　自动检测
● 使用软盘映像文件(M):
　　flp1.flp
　　　　　　创建(T)...　　浏览(B)...
☐ 只读(E)

- ▶ 在虚拟机窗口按Ctrl+Alt可以退回到原系统窗口
- ▶ 用UE打开软盘文件，可见未格式化之前软盘文件全是00
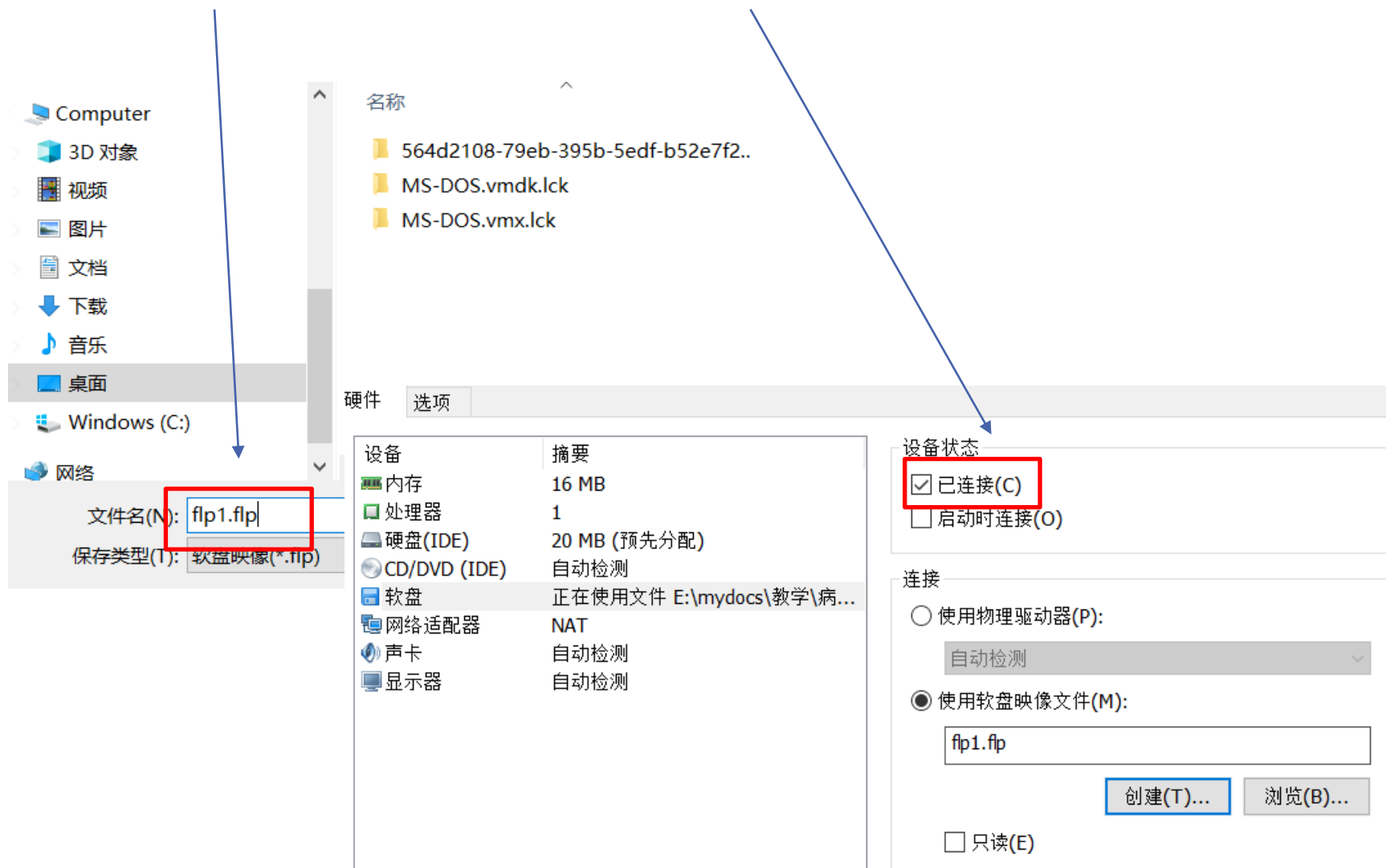
▶ 回到虚拟机的DOS系统，输入format a：/u来创建FAT12
文件系统

其中，/u是强迫DOS做格式化，不做保存恢复之类的操作

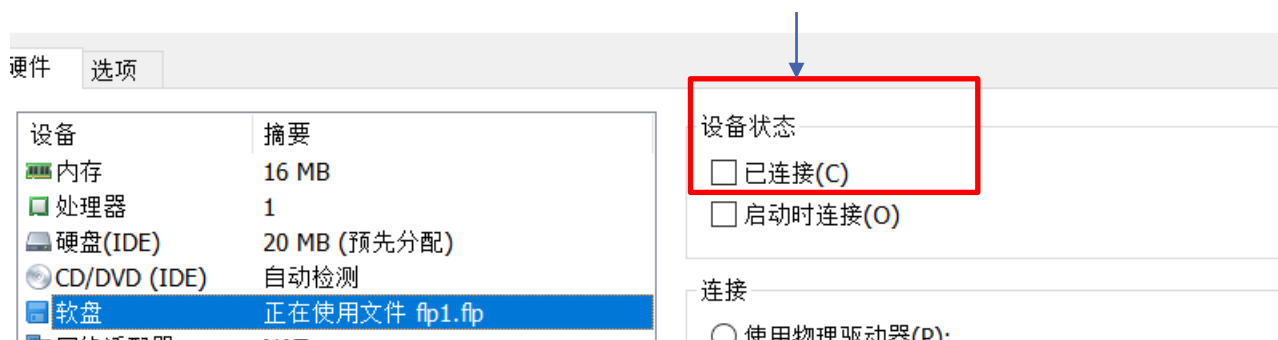格式化，先回车，然后看见让你输入卷标的提示，输入学号后
11位 （最大11个字符）

```
C:\>format a: /u
Insert new diskette for drive A:
and press ENTER when ready...

Formatting 1.44M
Format complete.

Volume label (11 characters, ENTER for none)? 20210326S_
```

▶ 输入自己学号

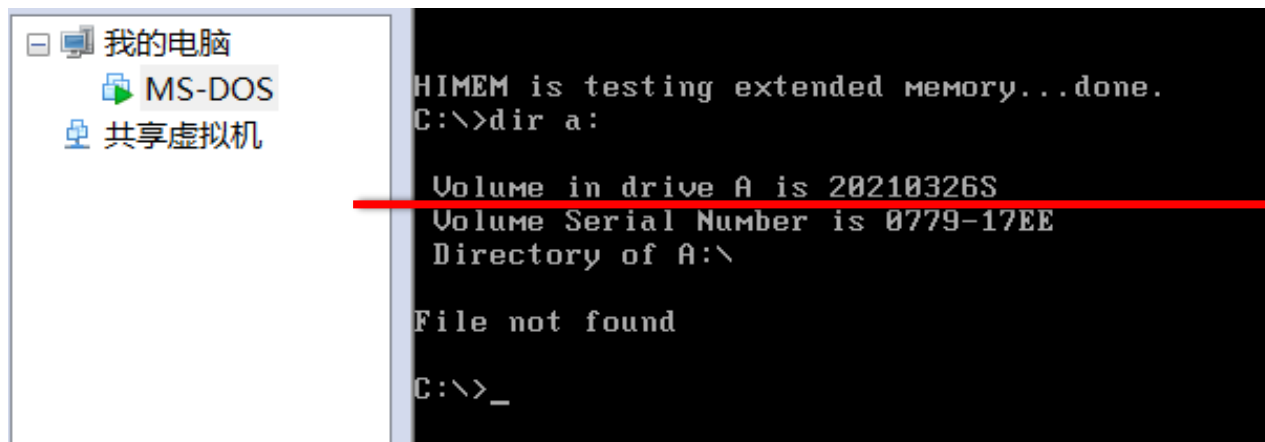▶ 进入虚拟机设置，选择软盘，将 已连接 框勾选掉，并确定，此时，软盘相当于弹出，虚拟机会将修改写入软盘文件

查看格式化后的软盘

▶ 用dir命令可以查看卷标

▶ 找到根目录区，(1+18) * 512 = 9728，用UE在软盘文件跳转过去
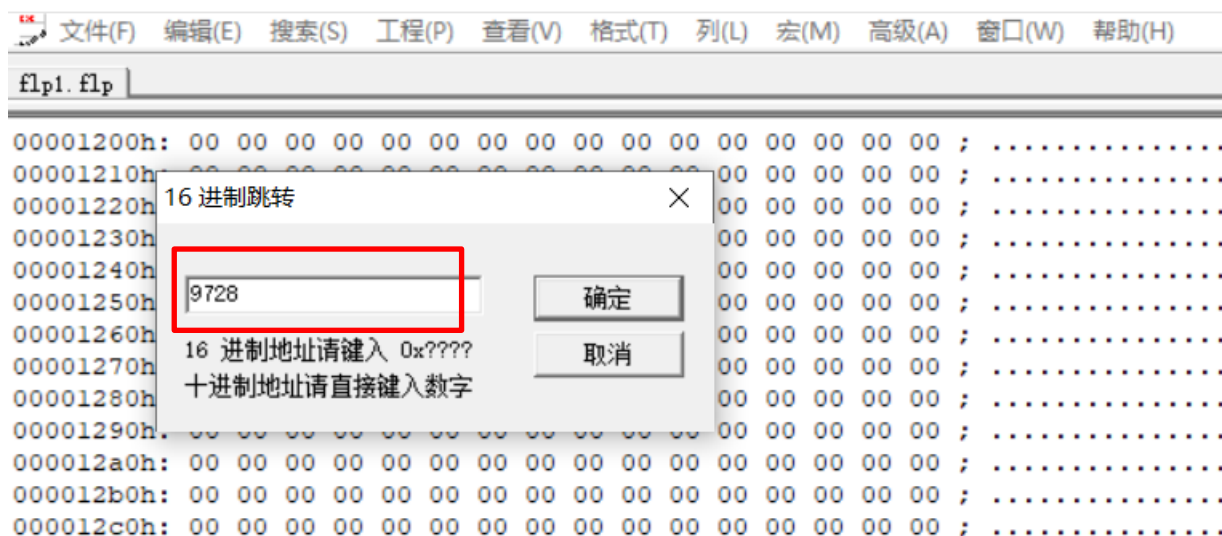
找到根目录下软盘的卷标，修改第一个字符看看是否有效果
保存文件前在DOS虚拟机中弹出a盘

再查看a盘，看看卷标的变化
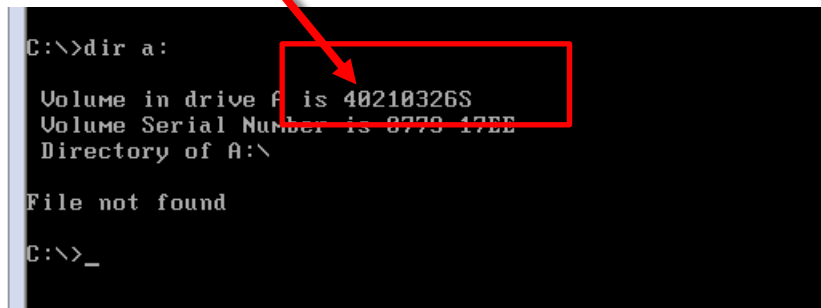
2 FAT表及文件定位

FAT表格式

▶ 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，哪怕只有一个字节也会分配一簇

▶ 簇由几个扇区组成在引导扇区的引导记录中定义

BPB_SecPer Clus	13	1	每簇扇区数	0x01	

此处表明，一簇由一个扇区构成，即512字节

```
00000000h: EB 3C 90 4D 53 44 4F 53 35 2E 30 00 02 01 01 00
```
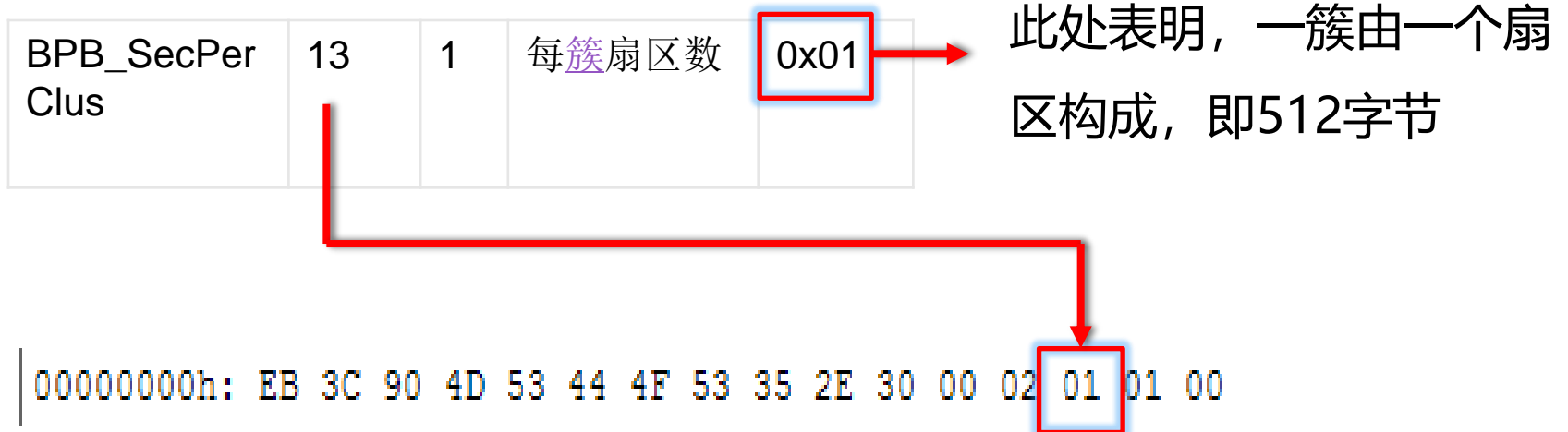
FAT12文件系统的FAT表

▶ FAT表的本质是什么？是磁盘簇分配情况的数据表示

▶ 引导扇区有引导记录说明了磁盘共有多少个扇区

BPB_TotSec16	19	2	扇区总数	0xB40（2880）

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，这也是"FAT12"文件系统中命名12的原因

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表的查找和遍历机制

- FAT表是一个数组，数组中每个元素是1.5字节的整数，为了查找FAT表中簇号为N的元素，只需用N作为索引查找FAT[N]元素

- 如下图，假定一个文件的首簇号是00C

  (1) 查找FAT[00C]中是00F，它代表00F簇是文件的下一簇

  (2) 接着查看FAT[00F]，其值是00E，则说明下一簇是00E

  (3) 找到FAT[00E]，发现其值为FFF，则说明到尾部了，不再遍历
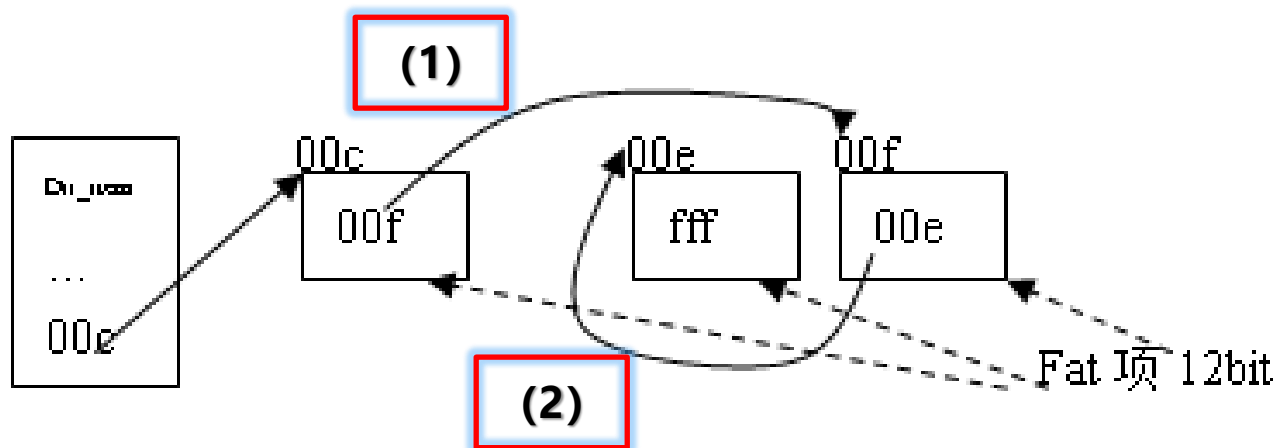
- 最终知道该文件由00C, 00F, 00E簇组成

- 根据FAT12缺省设置，引导区占1扇区，FAT1紧跟其后，所以在偏移512，即200h处开始

簇0 簇1   **簇2 簇3**   簇4 簇5

```
00000200h:  F0  FF  FF  FF  FF  FF  00  00  00  00  00  00  00  00  00  00
```
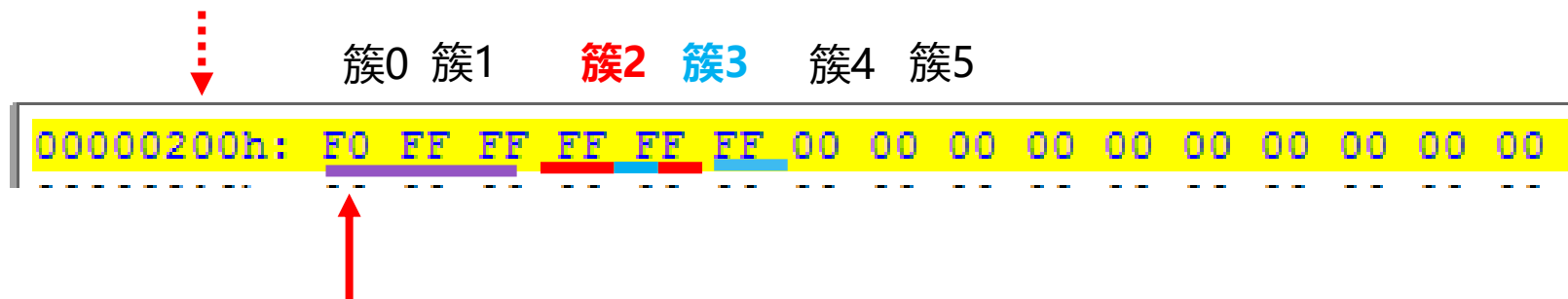
▶ FAT表开始3个字节没用于用户文件分配，3字节有2组12bits所以，占用了0,1两个簇号，用户的数据从簇2开始分配。

- FAT表从头开始按3字节分成一组：

在这3个字节中，用第2字节的低半字节和第1字节形成整数表示一个簇号，用第2字节的高半字节和第3字节形成的整数来表示另一个簇号

请问如图所示的FAT表有几个用户文件，其分别的簇是什么

根目录表中的记录格式

根目录表包含多条记录

其中，每条记录占32字节，其结构如下表所示

目前我们关注**文件名**（查找需要）和**首簇**（遍历需要）

名称	偏移	长度	描述
DIR_Name	0	0xB (11)	文件名8字节，扩展名3字节
DIR_Attr	0xB	1	文件属性
保留	0xC	10	
DIR_WrtTime	0x16	2	最后修改时间
DIR_WrtDate	0x18	2	最后修改日期
DIR_FstClus	0x1A (26)	2	此条目对应的开始簇号
DIR_FileSize	0x1C (28)	4	文件大小

将C盘下的WinA20.386文件拷贝到A盘（copy wina20.386 a：）

```
C:\>dir

 Volume in drive C has no label
 Volume Serial Number is 4650-9772
 Directory of C:\

DOS          <DIR>        02-16-15    6:57p
OLD_DOS  1   <DIR>        02-16-15    6:57p
COMMAND  COM        54,645 05-31-94    6:22a
WINA20   386         9,349 05-31-94    6:22a
CONFIG   SYS           109 02-16-15    6:59p
AUTOEXEC BAT            54 02-16-15    6:59p
        6 file(s)        64,157 bytes
                      5,331,008 bytes free

C:\>copy wina20.386 a:
        1 file(s) copied
```

```
C:\>dir a:

 Volume in drive A is 40210326S
 Volume Serial Number is 0779-17EE
 Directory of A:\

WINA20   386         9,349 05-31-94    6:22a
        1 file(s)         9,349 bytes
                      1,447,936 bytes free
```

再次找到根目录区，看看WinA20.386文件的首簇号
注意，UE需要重新加载软盘文件

flp1.flp

```
00002600h: 34 30 32 31 30 33 32 36 53 20 20 28 00 00 00 00 ; 40210326S  (....
00002610h: 00 00 00 00 00 00 54 81 7A 52 00 00 00 00 00 00 ; ......T剽R......
00002620h: 57 49 4E 41 32 30 20 20 33 38 36 20 00 00 00 00 ; WINA20  386 ....
00002630h: 00 00 00 00 00 00 C0 32 BF 1C 02 00 85 24 00 00 ; ......??...?..
00002640h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
```

Ctrl+G跳到FAT表
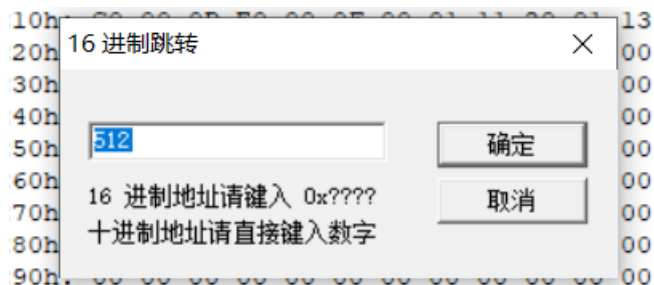
**回答，根据FAT表，该文件占据了哪些簇，共占据了多少个扇区
用文件大小（9349）来验证一下**


```
flp1.flp

00000200h: F0 FF FF 03 40 00 05 60 00 07 80 00 09 A0 00 0B ;
00000210h: C0 00 0D E0 00 0F 00 01 11 20 01 13 40 01 FF 0F ;
00000220h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ;
00000230h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ;
00000240h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ;
```

```
C:\>dir a:

 Volume in drive A is 40210326S
 Volume Serial Number is 0779-17EE
 Directory of A:\

WINA20   386         9,349 05-31-94   6:22a
         1 file(s)            9,349 bytes
                         1,447,936 bytes free
```

在A盘根目录下创建一个和卷标同名（学号后11位）的子目录

```
C:\>a:

A:\>dir

 Volume in drive A is 40210326S
 Volume Serial Number is 0779-17EE
 Directory of A:\

WINA20   386        9,349 05-31-94   6:22a
        1 file(s)          9,349 bytes
                       1,447,936 bytes free

A:\>c:

C:\>a:

A:\>md 40210326S_
```

再以自己的姓名拼音创建一个txt文件
如下图，edit xxxx.txt
在弹出的编译器中任意输入一个字符串，然后Alt+F进行保持退出
用dir查看子目录情况

```
A:\>cd 40210326

A:\40210326>edit QQ.txt
```

```
 File  Edit  Search  Options
                              QQ.TXT
virus
```

```
A:\40210326>dir

 Volume in drive A is 40210326S
 Volume Serial Number is 0779-17EE
 Directory of A:\40210326

.            <DIR>         03-28-21  10:48a
..           <DIR>         03-28-21  10:48a
QQ      TXT        9 03-28-21  10:50a
        3 file(s)          9 bytes
                       1,446,912 bytes free
```

系统如何区分卷标项和文件项

▶ 目录记录中应该有属性表示卷标目录项和正常文件的目录项的区别，否则遍历时，如果有个文件名叫HANHONGT.EST怎么区分？

名称	偏移	长度	描述
DIR_Name	0	0xB　(11)	文件名8字节，扩展名3字节
DIR_Attr	0xB	1	文件属性
保留	0xC	10	
DIR_WrtTime	0x16	2	最后修改时间
DIR_WrtDate	0x18	2	最后修改日期
DIR_FstClus	0x1A　(26)	2	此条目对应的开始簇号
DIR_FileSize	0x1C　(28)	4	文件大小

■ 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

分析目录项的类型属性

▶ 在DOS虚拟机下弹出软盘，有UE重新加载软盘文件

▶ 然后查看软盘文件中根目录区的情况（0x2600开始处）

▶ 查看卷标、文件、目录的类型区别

```
00002600h: 34 30 32 31 30 33 32 36 53 20 20 28 00 00 00 00 ; 40210326S  (....
00002610h: 00 00 00 00 00 00 54 81 7A 52 00 00 00 00 00 00 ; ......T乱R.....
00002620h: 57 49 4E 41 32 30 20 20 33 38 36 20 00 00 00 00 ; WINA20  386 ....
00002630h: 00 00 00 00 00 00 C0 32 BF 1C 02 00 85 24 00 00 ; ......??..?..
00002640h: 34 30 32 31 30 33 32 36 20 20 20 10 00 00 00 00 ; 40210326   ....
00002650h: 00 00 00 00 00 00 1B 56 7C 52 15 00 00 00 00 00 ; ......V|R.....
```
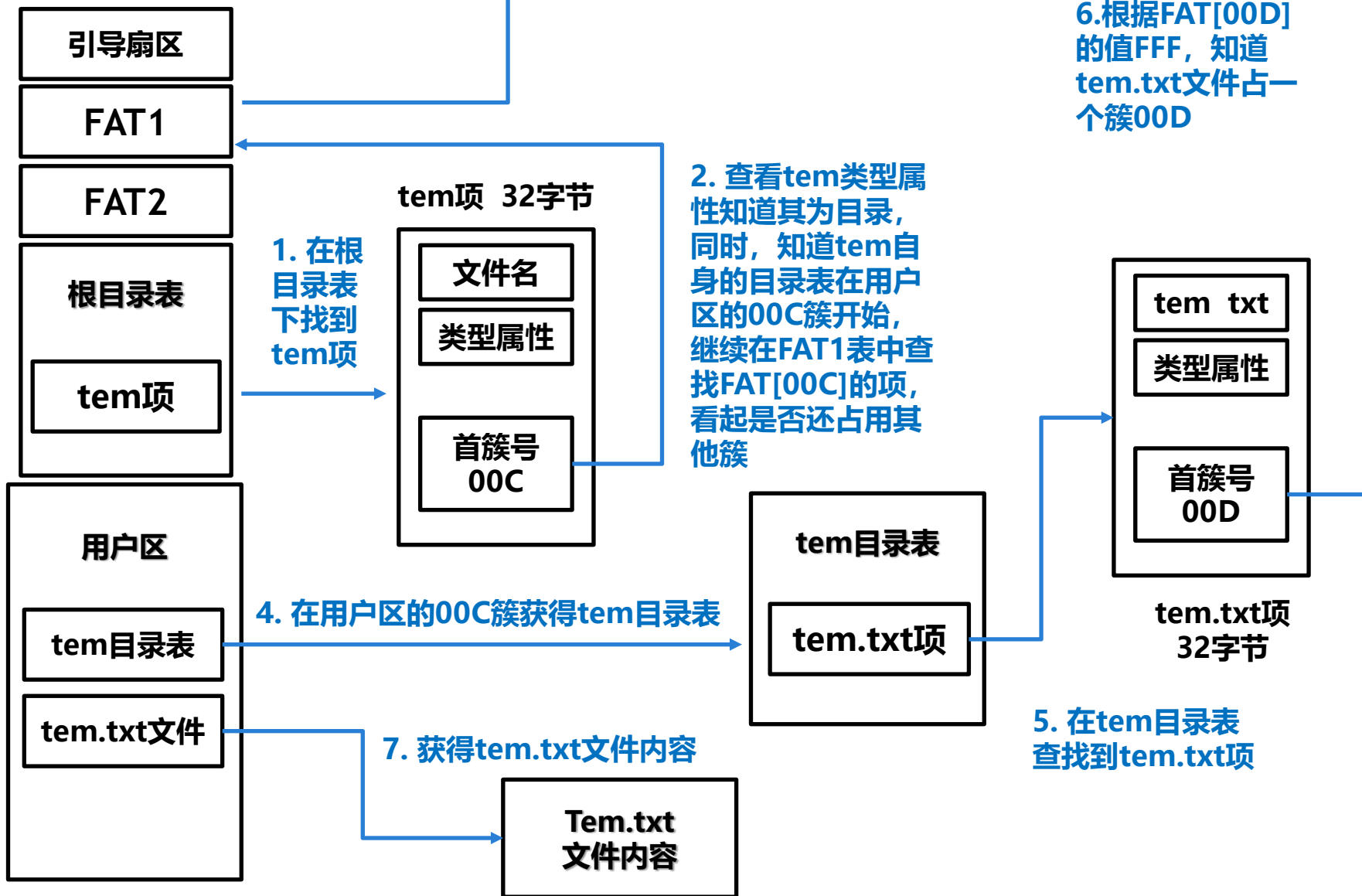
文件定位

3. 根据FAT[00C]的值FFF，知道tem的目录表占一个簇

00C 00D

| FFF | FFF |

| 引导扇区 |

| FAT1 |

| FAT2 |

| 根目录表 |

| tem项 |

1. 在根目录表下找到tem项

tem项 32字节

| 文件名 |
| 类型属性 |
| 首簇号 00C |

2. 查看tem类型属性知道其为目录，同时，知道tem自身的目录表在用户区的00C簇开始，继续在FAT1表中查找FAT[00C]的项，看起是否还占用其他簇

6.根据FAT[00D]的值FFF，知道tem.txt文件占一个簇00D

| tem txt |
| 类型属性 |
| 首簇号 00D |

tem.txt项 32字节

| 用户区 |

| tem目录表 |

| tem.txt文件 |

4. 在用户区的00C簇获得tem目录表

tem目录表

| tem.txt项 |

5. 在tem目录表查找到tem.txt项

7. 获得tem.txt文件内容

Tem.txt 文件内容

实验任务一

▶ 按照上述实验步骤完成实验内容

▶ 并在软盘文件中定位刚才创建的以自己姓名拼音创建的文件

▶ 然后在软盘文件中找到你在文件中输入的字符串

```
00002600h: 34 30 32 31 30 33 32 36 53 20 20 28 00 00 00 00 ; 40210326S  (....
00002610h: 00 00 00 00 00 00 54 81 7A 52 00 00 00 00 00 00 ; ......T乱R......
00002620h: 57 49 4E 41 32 30 20 20 33 38 36 20 00 00 00 00 ; WINA20  386 ....
00002630h: 00 00 00 00 00 00 C0 32 BF 1C 02 00 85 24 00 00 ; ......??...?..
00002640h: 34 30 32 31 30 33 32 36 20 20 20 10 00 00 00 00 ; 40210326   ....
00002650h: 00 00 00 00 00 00 1B 56 7C 52 15 00 00 00 00 00 ; .......V|R......
```

首先，定位子目录，首簇号0x0015，即21

```
00002600h: 34 30 32 31 30 33 32 36 53 20 20 28 00 00 00 00 ; 40210326S  (....
00002610h: 00 00 00 00 00 00 54 81 7A 52 00 00 00 00 00 00 ; ......T罸R......
00002620h: 57 49 4E 41 32 30 20 20 33 38 36 20 00 00 00 00 ; WINA20  386 ....
00002630h: 00 00 00 00 00 00 C0 32 BF 1C 02 00 85 24 00 00 ; ......?2?..?..
00002640h: 34 30 32 31 30 33 32 36 20 20 20 10 00 00 00 00 ; 40210326   .....
00002650h: 00 00 00 00 00 00 1B 56 7C 52 15 00 00 00 00 00 ; .......V|R......
```

子目录，首簇号0x0015，即21

```
00000200h: F0 FF FF 03 40 00 05 60 00 07 80 00 09 A0 00 0B
00000210h: C0 00 0D E0 00 0F 00 01 11 20 01 13 40 01 FF FF
00000220h: FF FF 0F 00 00 00 00 00 00 00 00 00 00 00 00 00
```

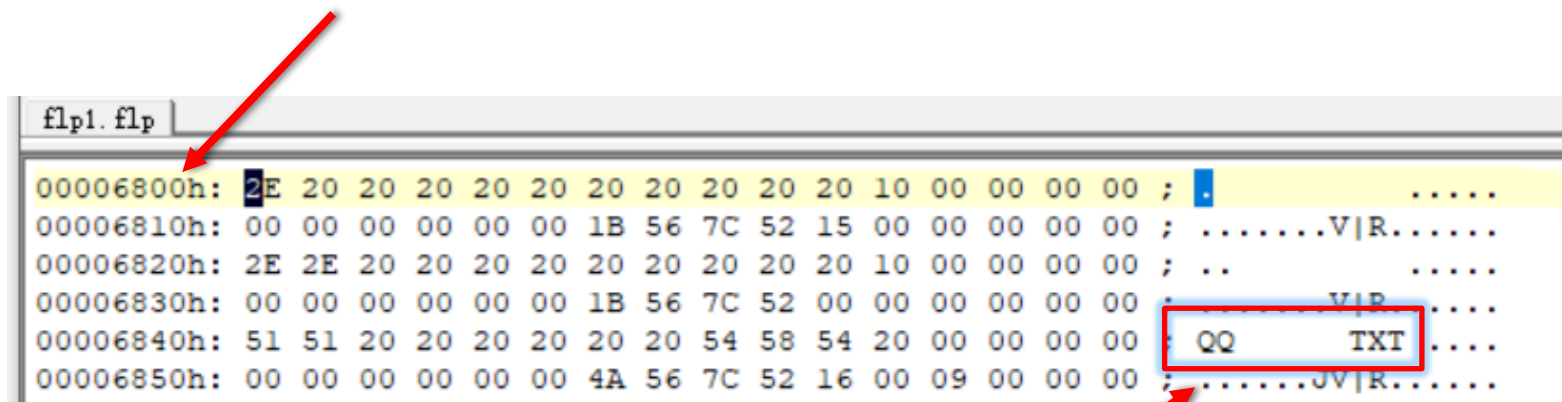子目录，首簇号0x0015，即21，FAT表告诉该子目录只占一个簇

1+18 + 224*32/512 = 19+14 = 33
用户区起始位置对应簇2，那么簇21的位置是
33+（21-2）= 52 = 0x34 （注意换成16进制）
定位
0x34*200=0x6800


```
flp1.flp

00006800h: 2E 20 20 20 20 20 20 20 20 20 20 10 00 00 00 00 ; .          .....
00006810h: 00 00 00 00 00 00 1B 56 7C 52 15 00 00 00 00 00 ; .......V|R......
00006820h: 2E 2E 20 20 20 20 20 20 20 20 20 10 00 00 00 00 ; ..         .....
00006830h: 00 00 00 00 00 00 1B 56 7C 52 00 00 00 00 00 00 ;       V|R...
00006840h: 51 51 20 20 20 20 20 20 54 58 54 20 00 00 00 00 ; QQ      TXT ....
00006850h: 00 00 00 00 00 00 4A 56 7C 52 16 00 09 00 00 00 ; ......JV|R......
```

接下来，定位到文件的工作，请同学们自行完成

3 删除并恢复文件

DOS虚拟机插入软盘，删除文件名为学号的文件，观察目录表和FAT表的变化


```
A:\40210326>del qq.txt

A:\40210326>_
```


目录表

FAT

```
00000200h: F0 FF FF 03 40 00 05 60 00 07 80 00 09 A0 00 0B
00000210h: C0 00 0D E0 00 0F 00 01 11 20 01 13 40 01 FF FF
00000220h: FF FF 0F 00 00 00 00 00 00 00 00 00 00 00 00 00
```

flp1.flp

```
00000200h: F0 FF FF 03 40 00 05 60 00 07 80 00 09 A0 00 0B ;
00000210h: C0 00 0D E0 00 0F 00 01 11 20 01 13 40 01 FF FF ;
00000220h: FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ;
```

同学们自行完成文件恢复，并在DOS系统下展示恢复效果

```
A:\40210326>dir

 Volume in drive A is 40210326S
 Volume Serial Number is 0779-17EE
 Directory of A:\40210326

 .           <DIR>          03-28-21  10:48a
 ..          <DIR>          03-28-21  10:48a
SQ      TXT            9 03-28-21  10:50a
        3 file(s)              9 bytes
                      1,446,912 bytes free
```
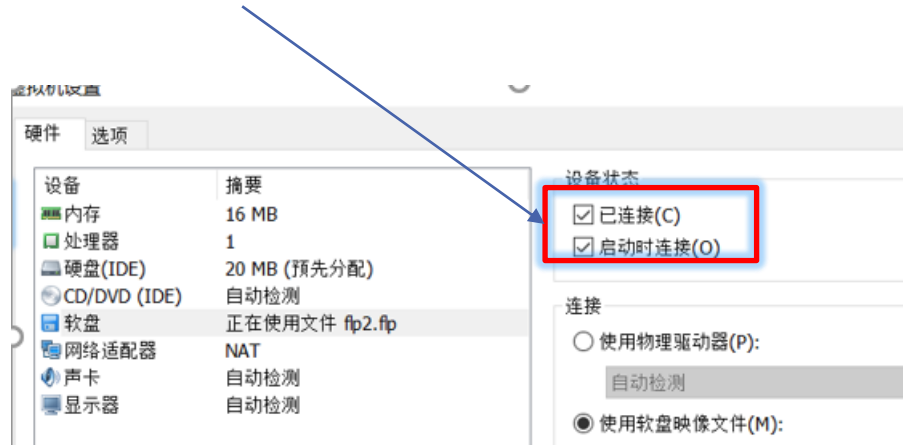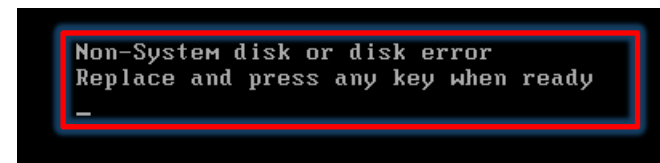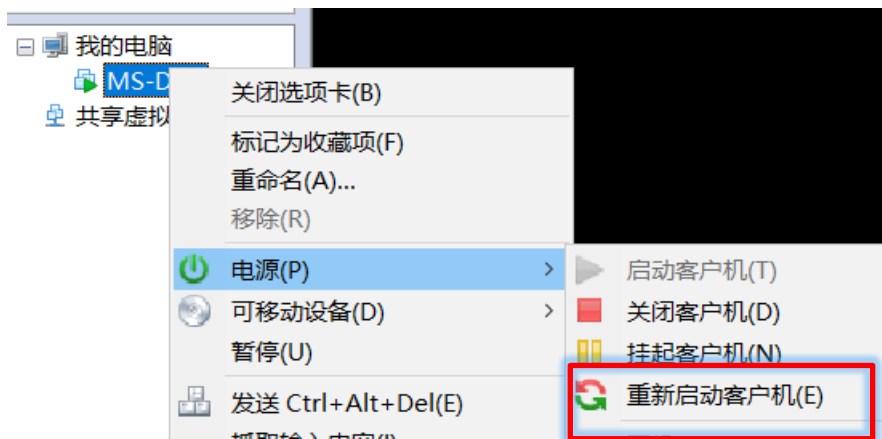
如图，将被删除的文件
恢复为了SQ.txt文件

4 系统引导

设置系统为软盘启动

重启虚拟机，看看默认的FAT12引导程序的作用


```
Non-System disk or disk error
Replace and press any key when ready
_
```

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

▶ 下面我们将引导程序设计为打印字串"Hello!"写到一个软盘文件开始的512字节，此正好对应0头0道1扇区。

▶ 插入该软盘启动虚拟机，这时，运行的是我们设计的引导程序，应该打印相应的字串

实验准备工作

▶ 软盘引导区的内容为机器码，因此，我们需要生成打印程序的机器码，**.com**文件是只包含机器码的文件，没有任何附件格式（如文件头）

▶ 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），可以通过UE工具的操作或者编写C语言程序来实现

▶ 完成拷贝后，我们就在软盘上做成了我们所需要的引导扇区

编写引导代码 此代码来自《自己动手做操作系统》

```
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，$当前位置，即jmp首址
DispStr:
mov ax, BootMessage
mov bp, ax               ; ES:BP = 串地址
mov cx, 6                ; CX = 串长度  "Hello, OS world!"
mov ax, 1301h            ; AH = 13,  AL = 01h
mov bx, 000ch            ; 页号为0(BH = 0) 黑底红字(BL = 0Ch,高亮)
mov dl, 0
int   10h                ; 10h号中断 显示器和屏幕中断
ret
BootMessage: db "Hello!"   ; 这里改为你的学号
times 510-($-$$) db 0
dw 0xaa55
```

生成机器码并拷贝到软盘


```
2021/03/28  11:51    <DIR>              ..
2021/03/28  11:50              933 boot.asm
2021/03/27  10:07    <DIR>          contrib
2014/02/20  08:04            1,521 LICENSE
2014/02/20  08:05          906,752 nasm.exe
2014/02/20  08:04            2,238 nasm.ico
2014/02/20  08:05          773,016 nasmdoc.pdf
2021/03/27  10:07               62 nasmpath.bat
2014/02/20  08:05          501,248 ndisasm.exe
2021/03/27  10:07    <DIR>          rdoff
2021/03/27  10:07           90,389 Uninstall.exe
               8 个文件      2,276,159 字节
               4 个目录 518,369,542,144 可用字节

C:\Users\qiuxw\AppData\Local\nasm>nasm boot.asm -o boot.com
```

用UE拷贝COM文件

用UE粘贴到软盘文件第一个扇区

```
flp1.flp*  boot.com

00000000h: 8C C8 8E D8 8E C0 E8 02 00 EB FE B8 1E 7C 89 C5 ; 屏厅帮?.膛?|瞽
00000010h: B9 06 00 B8 01 13 BB 0C 00 B2 00 CD 10 C3 48 65 ; ?.?.?.??阄e
00000020h: 6C 6C 6F 21 00 00 00 00 00 00 00 00 00 00 00 00 ; llo!............
00000030h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00000040h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00000050h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00000060h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00000070h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00000080h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00000090h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
000000a0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
000000b0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
000000c0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
000000d0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
000000e0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
000000f0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00000100h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00000110h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00000120h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00000130h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00000140h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00000150h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00000160h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00000170h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00000180h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00000190h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
000001a0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
000001b0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
000001c0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
000001d0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
000001e0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
000001f0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 55 AA ; ..............U?
```

重新由软盘启动系统，查看效果