编号：

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 实验 | 一 | 二 | 三 | 四 | 五 | 六 | 七 | 八 | 总评 | 教师签名 |
| 成绩 |  |  |  |  |  |  |  |  |  |  |

武汉大学国家网络安全学院

课程实验(设计)报告

题 目： 软件安全实验

专业(班)： 信安5班

学 号： 2022302181161

姓 名： 王亚鹏

课程名称： 软件安全实验

任课教师： 赵磊

2024年 11 月 20日

**目 录**

[**实验1 磁盘格式与数据恢复(模板) 1**](#_Toc180505843)

[**1.1实验名称 1**](#_Toc180505844)

[**1.2实验目的 1**](#_Toc180505845)

[**1.3实验步骤及内容 1**](#_Toc180505846)

[**1.4实验关键过程、数据及其分析 3**](#_Toc180505847)

[**1.4.1 磁盘编辑工具基本用法 3**](#_Toc180505848)

[**1.4.2 分析本地硬盘的主引导扇区 4**](#_Toc180505849)

[**1.4.3 熟悉FAT32文件格式 7**](#_Toc180505850)

[**1.4.4手工恢复被删除的文件 9**](#_Toc180505851)

[**1.5 课后习题思考 10**](#_Toc180505852)

[**1.6实验体会和拓展思考 11**](#_Toc180505853)

## 实验1 磁盘格式与数据恢复(模板)

### 1.1实验名称

磁盘格式与数据恢复

### 1.2实验目的

1. 了解磁盘的物理和逻辑结构
2. 熟悉FAT32文件系统
3. 学会使用磁盘编辑软件
4. 了解文件删除、格式化的基本原理
5. 能够利用工具或者手工恢复被删除的文件

### 1.3实验步骤及内容

**第一阶段：**

* 熟悉WinHex的使用。
  + 熟悉磁盘工具的使用。
  + 利用WinHex查看物理磁盘和逻辑磁盘。
  + 了解WinHex中相关工具的用法。

**第二阶段：**

* 分析本地硬盘的主引导扇区
* 利用磁盘编辑工具查看MBR磁盘分区并分析：
  + 主引导扇区由哪些部分组成？
  + 四个主分区项的内容各代表什么？
  + 分析主扩展分区表的结构。
  + 通过分区项来确定每个本地逻辑盘的位置以及大小，并画出本地硬盘的逻辑结构。
    - 每个本地盘的开始扇区位置，总扇区数，结束扇区位置，各扩展分区表扇区位置，保留空间数量。
* 利用磁盘编辑工具查看GPT磁盘分区并分析
  + GPT分区结构与MBR的具体差异有哪些？
  + 主分区头所在扇区包括哪些重要内容，验证这些重要内容的有效性。
  + 通过分区节点分析自己硬盘的各分区信息。

**第三阶段：**

* 熟悉FAT32文件格式。
  + 用WinHex打开某个FAT32分区格式的逻辑盘。
  + 查看该逻辑盘的起始扇区，分析起始扇区中的相关字段（BPB:BIOS Parameter Block）。
  + 查看FAT1和FAT2的内容和大小。
  + 查看该逻辑盘的根目录区。
  + 查看某个文件的目录项结构和FAT链以及具体存储位置。
    - 在根目录下建立文本文件：test-学号后3位.txt，其中填充60K左右的文本字符保存（注意：先行存储其他数据使得该文件的首簇高位不为0）。
    - 查看该文件的目录项，对其进行分析，并得到该文件所在位置以及大小。
    - 查看首簇位置，并得到簇链表。通过簇链表查看该文件内容。
    - 记录首簇位置（14H-15H,1AH-1BH）和文件大小（1CH-1FH）。

**第四阶段：**

* 手工恢复被删除的文件
  + 删除前面所建立的文件。(del&shift+del)
  + 利用WinHex在该文件所在盘符查找该.txt文件的目录项。
  + 查看目录项的变化。
  + 利用该残余目录项来计算被删除的文件所在的位置。
  + 手工恢复该文件（文件名、首簇高位、簇链表修复）。

**课后习题思考：**

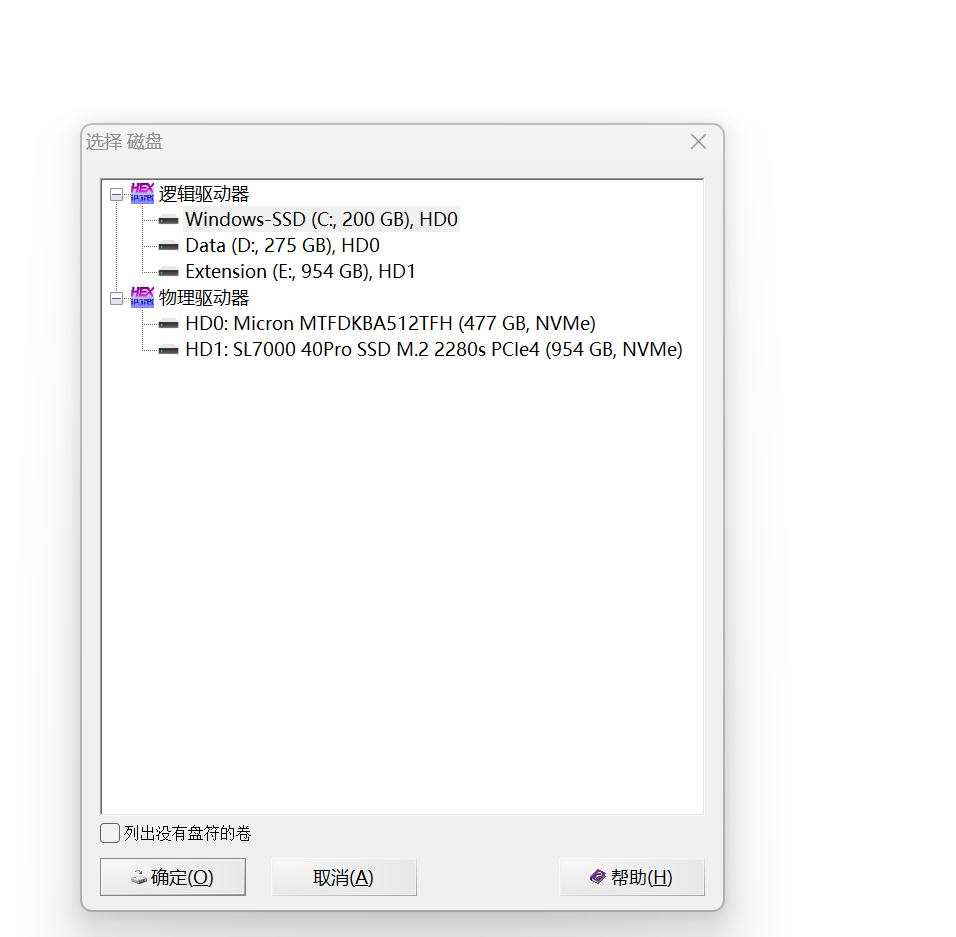
* 在磁盘分区过程中，用户提供了哪些信息？分析分区工具的工作原理。
* 高级格式化与低级格式化的具体原理和区别是什么？
* 查找资料，对NTFS分区的总体结构进行分析，尝试对NTFS下删除的文件进行手工恢复。
* 用数据粉碎工具（如金山、360、Strongdisk等）粉碎指定文件，分析其数据粉碎原理。
* 通过分区表看到的分区字节数为何与资源管理器中看到的分区字节数有差异？
* 如果删除的文件是长文件名，如何恢复所有文件名。

### 1.4实验关键过程、数据及其分析

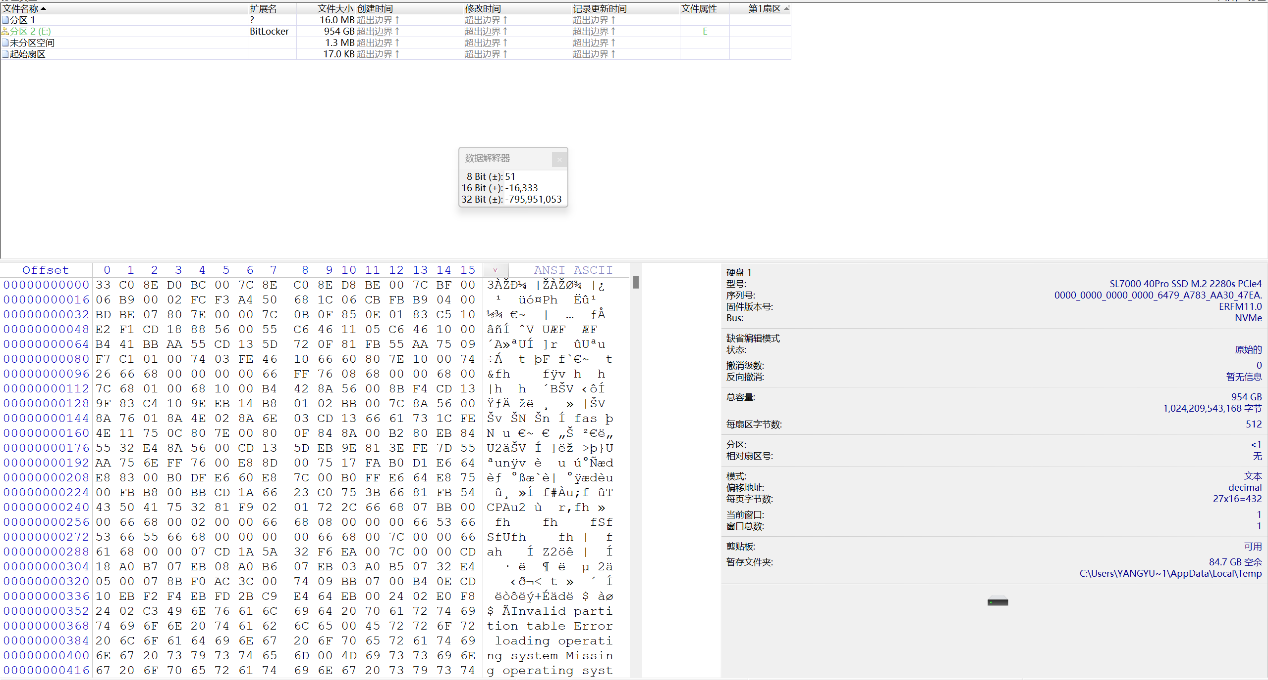
#### 1.4.1 磁盘编辑工具基本用法

（1）**利用WinHex查看物理磁盘和逻辑磁盘及了解WinHex中相关工具的用法**

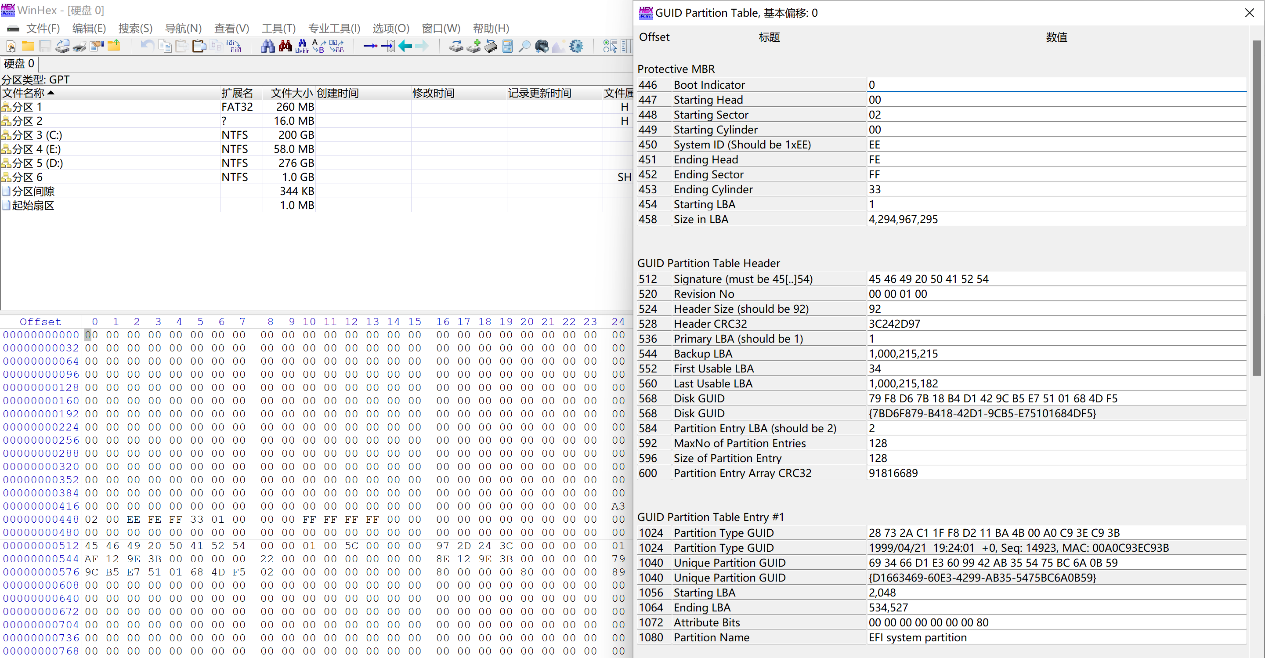
如图所示利用winhex查看本电脑的磁盘分区



打开目标物理驱动器HD0的界面如图所示：可以看到磁盘的容量、可用容量、分区等信息



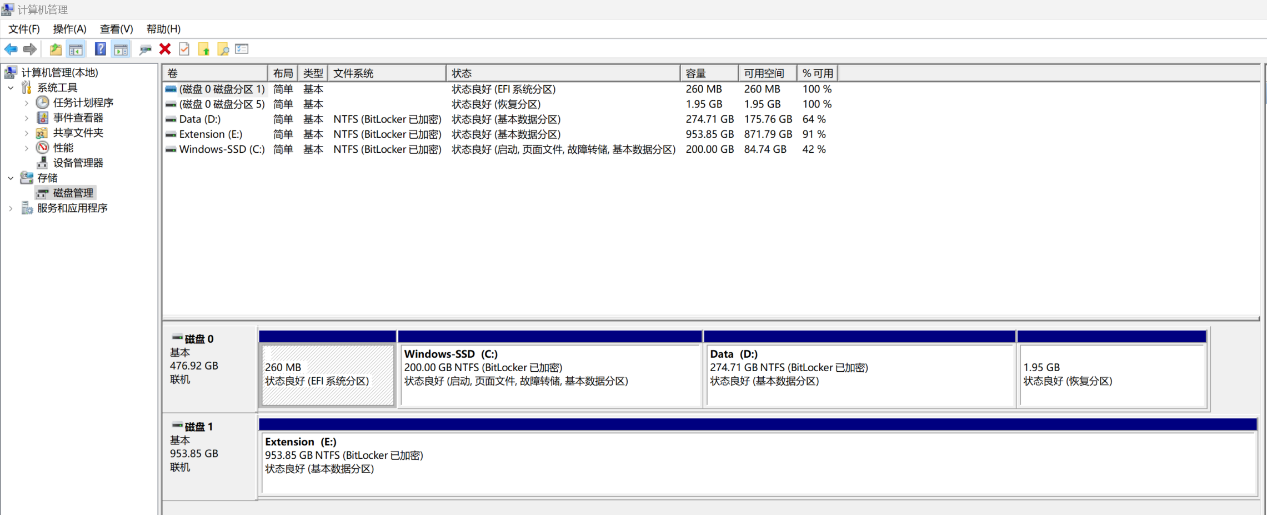
打开另一块区域，也可以使用模板查看分区信息：



查找资料分析图示信息：Protective MBR，是一种保护性的主引导记录，用于保护GUID Partition Table磁盘上的分区信息。包括Boot Indicator（引导标志）、Starting Head（起始磁头）、Starting Sector（起始扇区）、Starting Cylinder（起始柱面）、System ID (Should be 1xEE)（系统标识）、Ending Head（终止磁头）、Ending Sector（终止扇区）、Ending Cylinder（终止柱面）、Starting LBA（逻辑块地址起始位置）、Size in LBA（分区大小，以LBA表示）项

#### 1.4.2 分析本地硬盘的主引导扇区

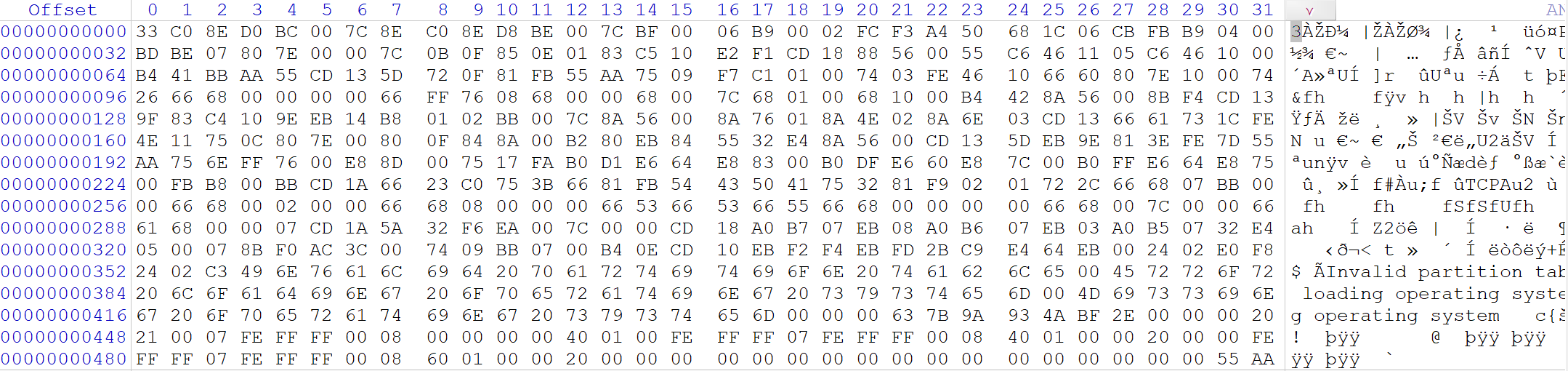
**（1）可以使用Windows自带工具查看磁盘的扇区。打开计算机管理-磁盘管理**



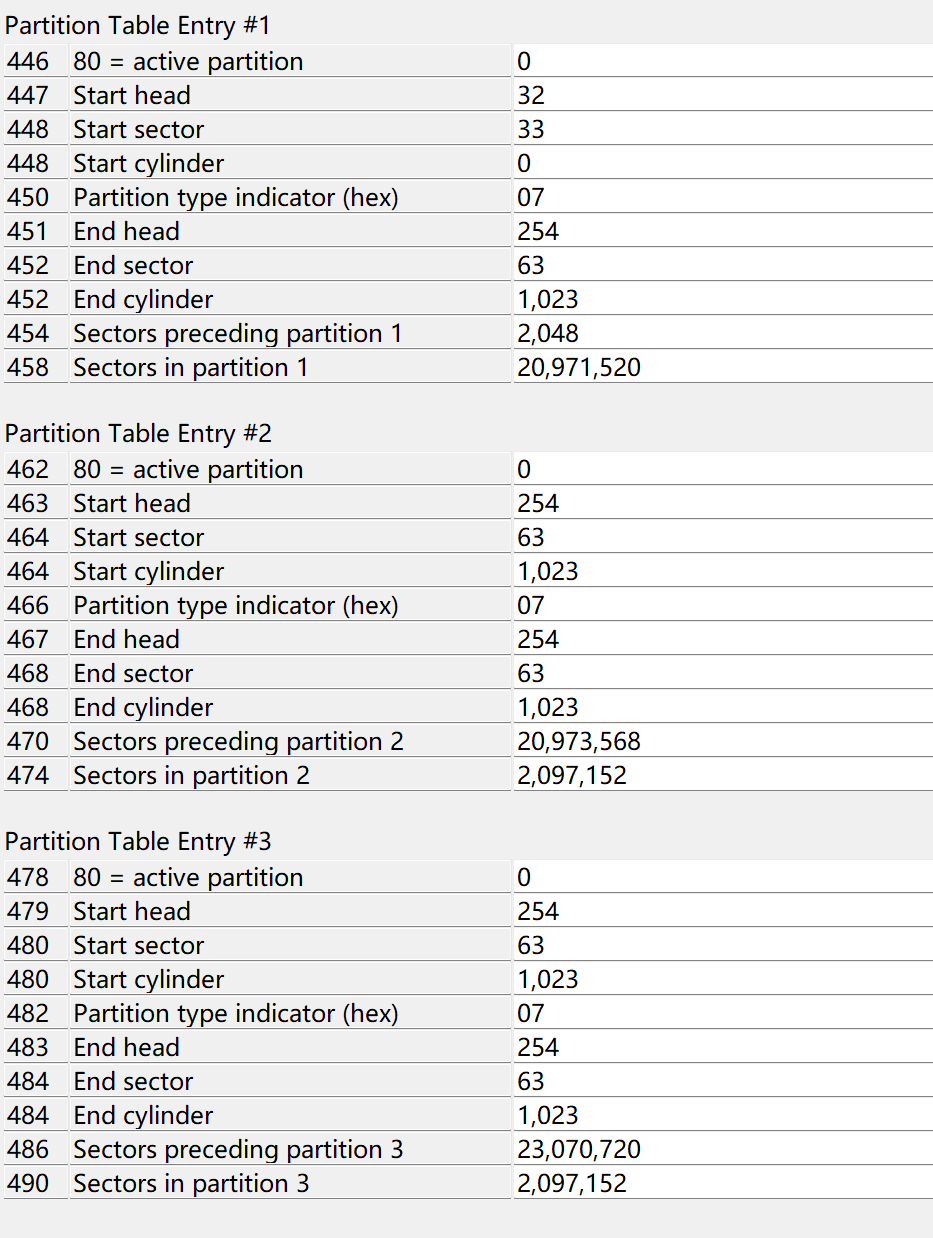
可以看到磁盘0被分成了C盘和D盘，磁盘0未进行分区

也可以看到这些磁盘都是使用了NTFS文件系统管理

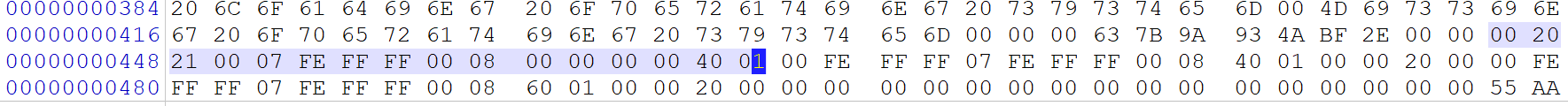
如果使用winhex打开磁盘，从0开始的512字节是主引导扇区



接着查看查看其分区表模板，前440个字节为它的引导代码



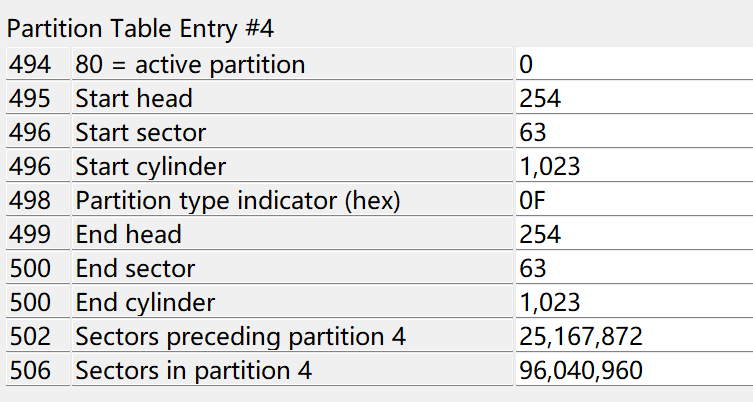
随后是几个分区表，每个分区表项长度为16个字节



最后以55AA结尾

据资料：主分区表在磁盘中最多只能有4个分区，当需要更多分区时，可以利用扩展分区表。要使用扩展分区，首先需要在主分区表中设置一个基本扩展分区项，用于指示所有扩展分区的整体信息。所有的扩展逻辑分区都会建立在这个基本扩展分区项所指示的主扩展分区中。这种机制允许在主分区数目有限的情况下，实现更多的分区需求

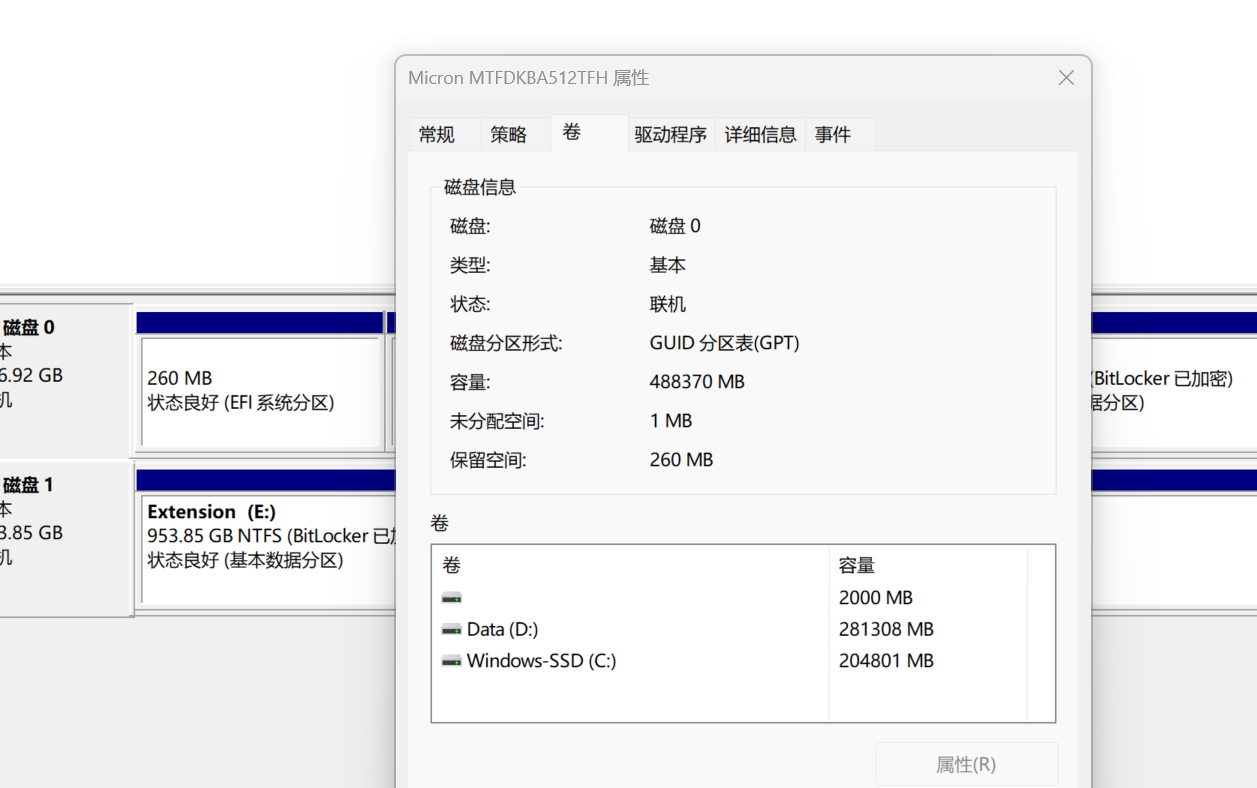
**（2）查看扩展分区的模板**



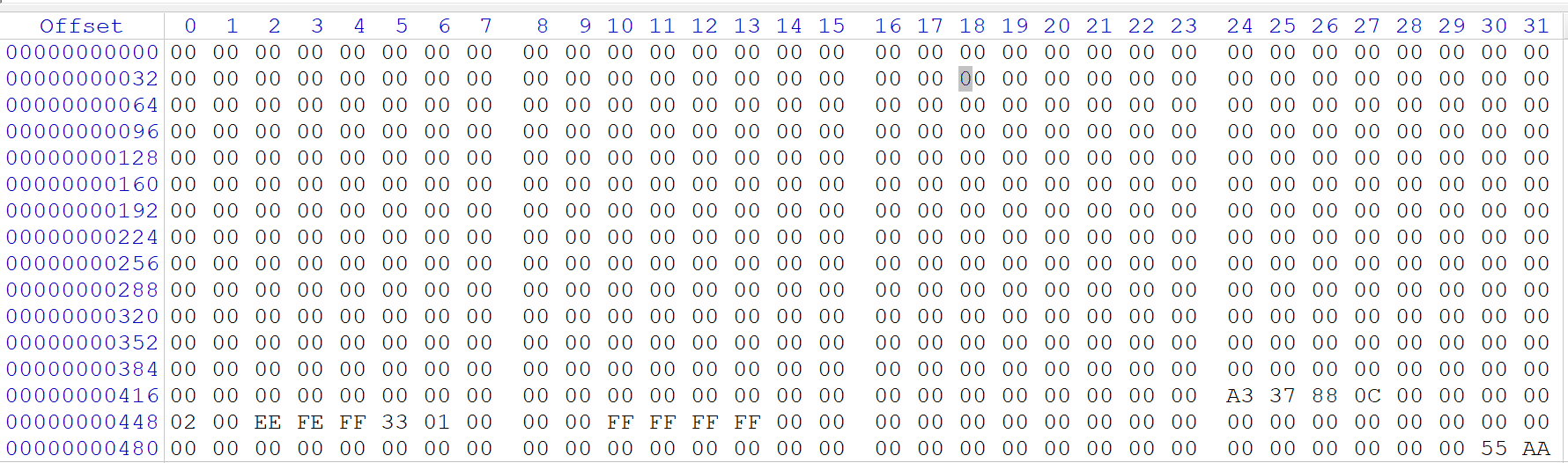
**active partition表示分区表活跃状态，80为活跃状态，0代表未工作状态**

**（3）GPT分区**

首先可以在磁盘管理的磁盘属性中验证磁盘使用了GPT分区管理

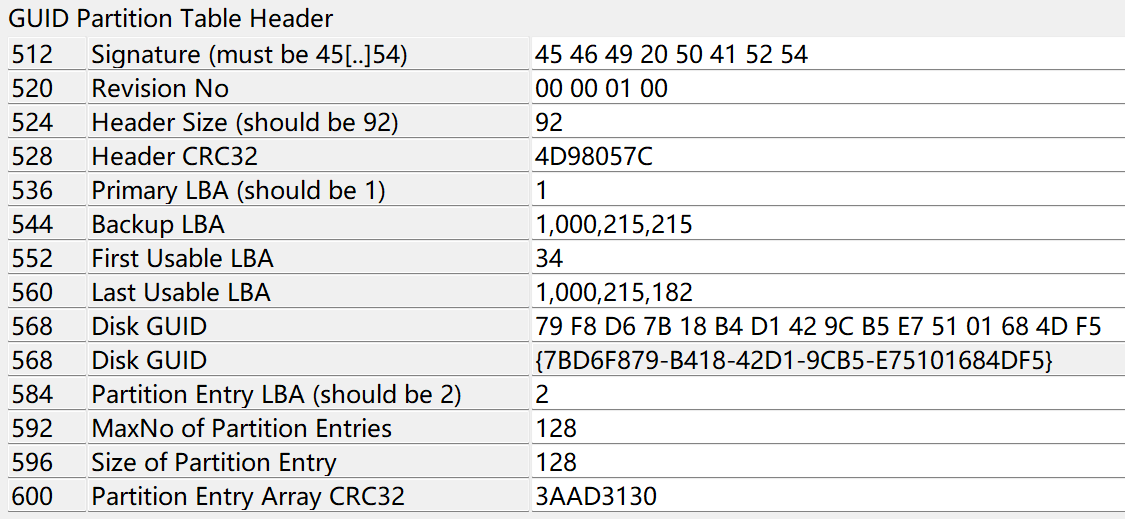
****

使用winhex查看磁盘



GPT前512个字节与MBR类似，都以AA55结尾，这里是一个保护性的MBR，用于与其他系统兼容

使用模板来查看GPT的分区信息如下图所示：



GUID Partition Table Header后每128个字节就是一个分区表项，用来存储分区的起始和终止LBA（逻辑块地址）等信息。每个LBA的大小为512字节。根据这些信息，我们可以计算出每个分区的大小

MBR与GPT的区别如下：

 **支持的磁盘容量**：

* **MBR**：支持最大2TB的磁盘。超过这个容量，MBR无法有效管理。
* **GPT**：可以支持更大的磁盘，理论上可管理多达18EB（Exabyte）的容量，远超现代硬盘的容量。

 **分区数量**：

* **MBR**：最多支持4个主分区。如果需要更多分区，需要将一个主分区设置为扩展分区，再在其中创建多个逻辑分区。
* **GPT**：理论上支持无限多的分区，通常操作系统默认允许创建128个主分区。

 **兼容性**：

* **MBR**：兼容性较好，适用于较老的BIOS引导系统，广泛应用于旧版本的Windows和其他系统。
* **GPT**：需要与UEFI（统一可扩展固件接口）配合使用，支持新版本的操作系统，如Windows 10、Linux、MacOS等。

 **安全性与冗余**：

* **MBR**：分区表只有一个副本，如果分区表损坏，数据恢复比较困难。
* **GPT**：在磁盘的开头和末尾都有分区表的副本，增加了数据安全性，并且包含CRC校验，能自动检测并修复分区表的损坏。

 **引导模式**：

* **MBR**：使用传统的BIOS引导方式。
* **GPT**：与UEFI引导方式兼容，允许更快的启动时间和更灵活的硬件支持。

 **数据结构**：

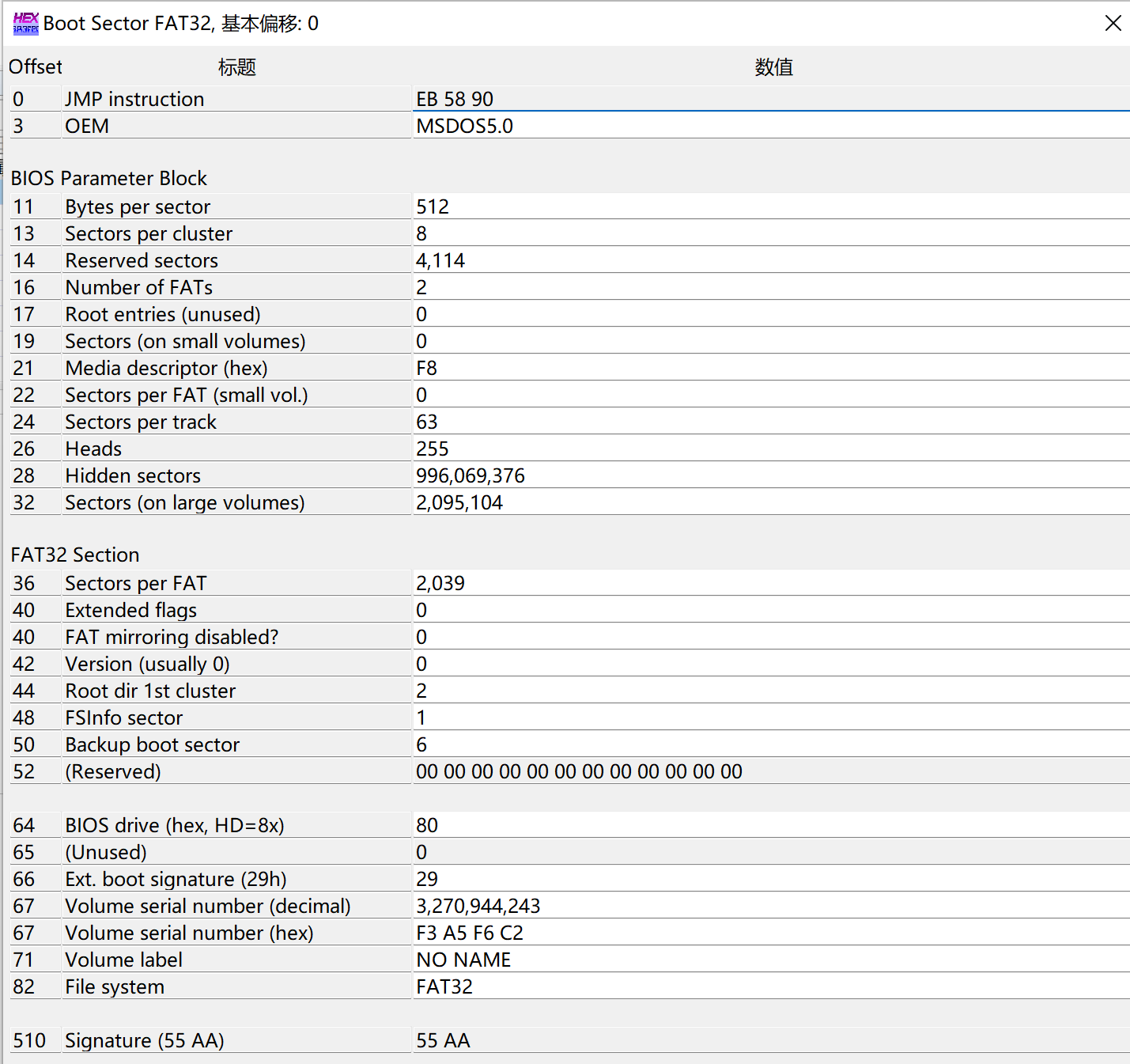
* **MBR**：使用传统的分区结构，较为简单，记录在硬盘的第一个扇区。
* **GPT**：使用更复杂的GUID（全局唯一标识符）来标记分区，支持更多的分区类型和灵活的分区操作

#### 1.4.3 熟悉FAT32文件格式

FAT32文件格式需要自定义创建，完成创建后打开对应的硬盘

查看其磁盘引导扇区

**（1）BPB**



各个项目的信息如下：

1. Bytes per sector：每个扇区的字节数，512字节

2. Sectors per cluster：每个簇包含的扇区数为8，它决定了簇的大小

3. Reserved sectors：为文件系统保留的扇区数，其中包括引导扇区和保留区域

4. Number of FATs：文件分配表的数量，通常是2

5.Media descriptor (hex)：介质描述符的十六进制值，用于指示存储介质的类型

6. Sectors per track：每个磁道上的扇区数

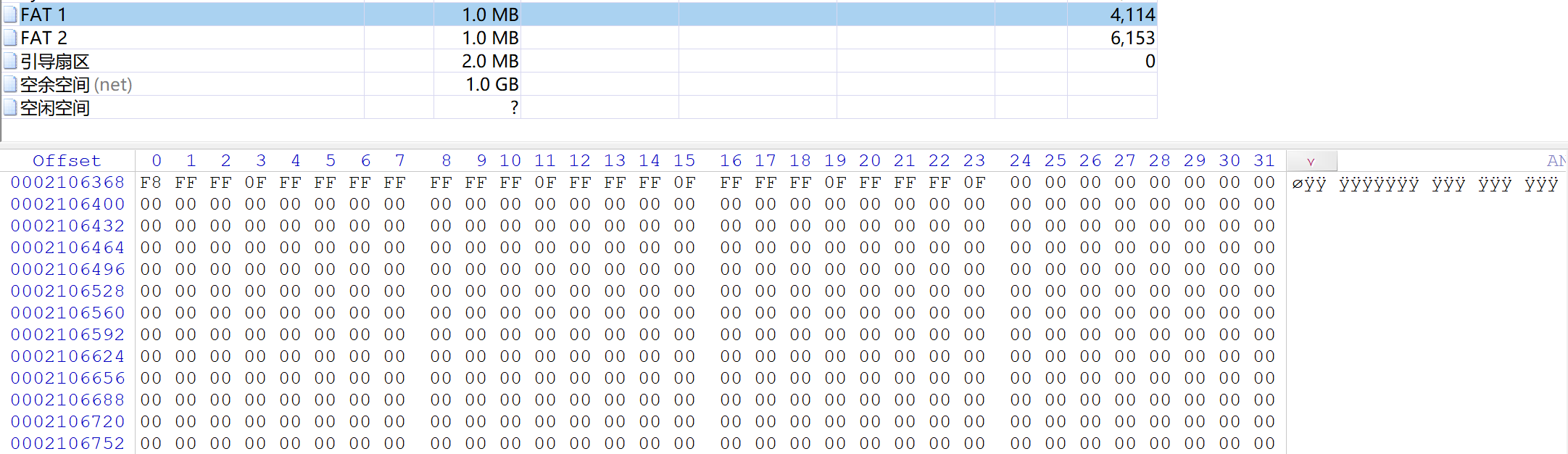
7. Heads：磁头数，也称为表面数

8. Hidden sectors：隐藏扇区的数量，通常指引导区之前的扇区数

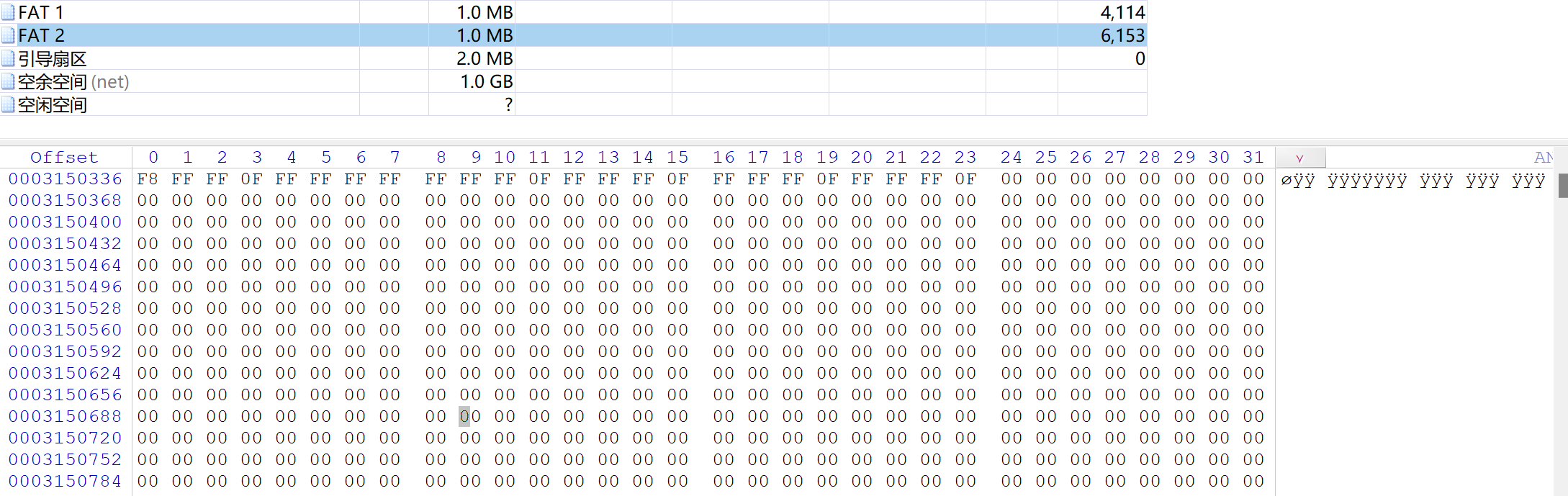
9. Sectors (on large volumes)：大卷上的扇区数，用于描述整个卷的大小

**（2）FAT1和FAT2**

查看FAT1：

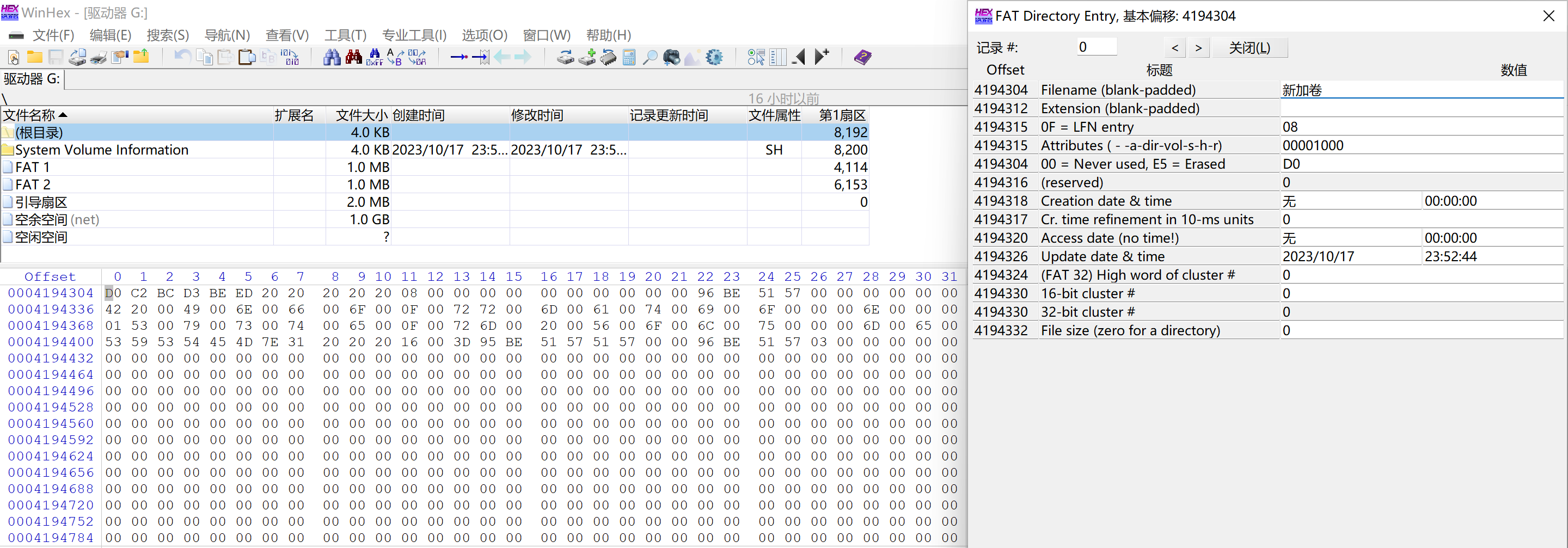


查看FAT2:



两者内容一致，FAT2是FAT1的一个副本，记录了存储在磁盘上的每个文件所占用的簇的信息。这样的设计可以提供冗余性，以防止因FAT损坏而导致数据丢失

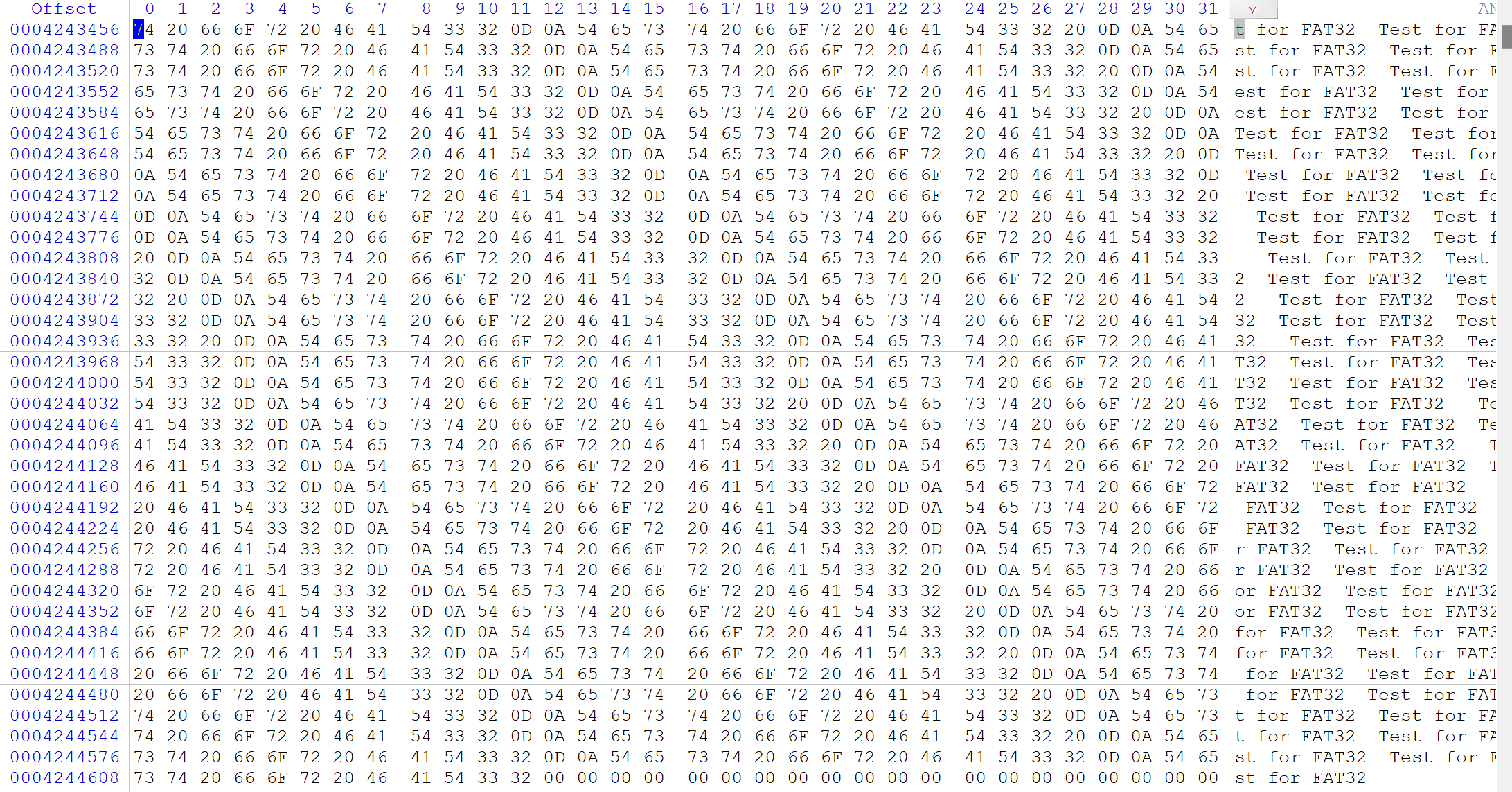
**（3）查看根目录区**

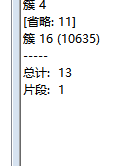


FAT32文件系统将根目录区划分为32字节大小的条目，每个条目用来存储一个文件的信息。这些存储的信息包括文件名、扩展名、创建时间、文件大小以及文件的起始簇编号等。

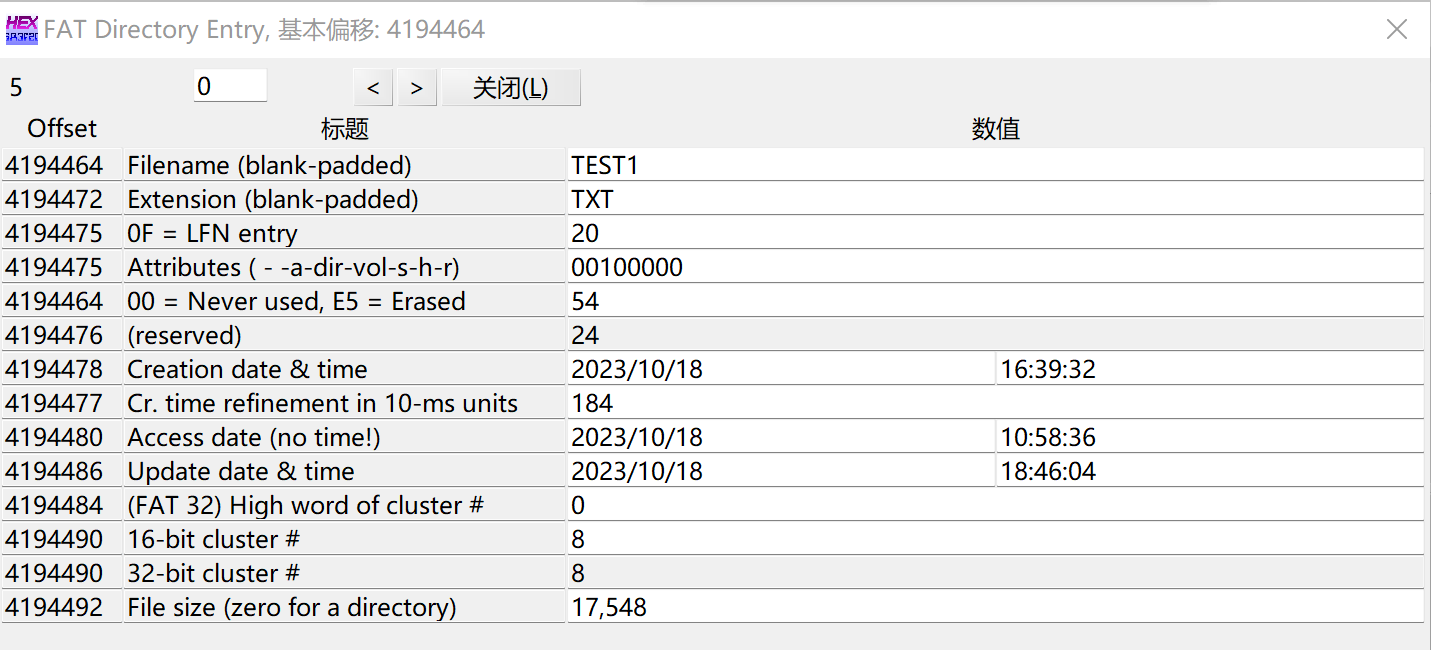
**（4）创建test.txt并开展分析**

创建后利用winhex打开，可以看到填充内容，一堆16进制数字，可以打开边栏或者通过ASCII码值来读取内容





簇信息



在根目录模板中找到

#### 1.4.4手工恢复被删除的文件

删除并恢复上述实验中的test1.txt文件，我们先在winhex下查看要删除的文件的簇号，记录相应的簇信息

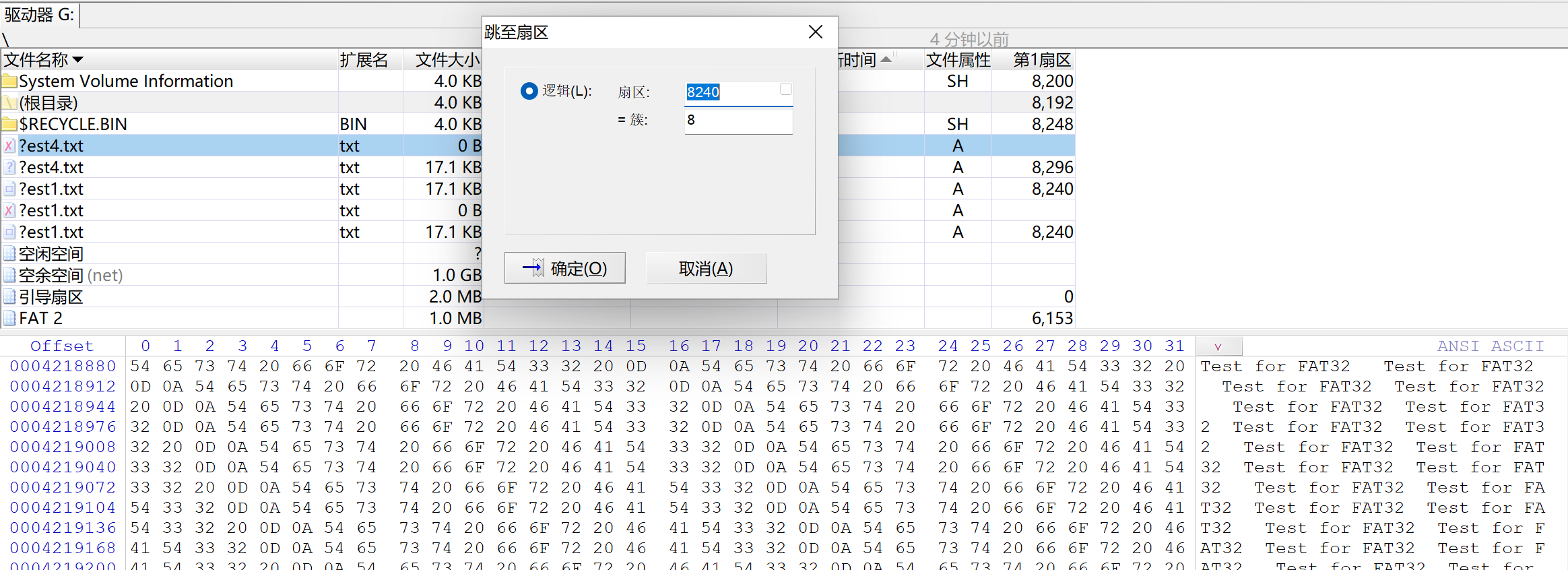
010editor中也可以看到这些信息，可以进一步验证

删除后的恢复需要用到这些信息，要先记录下来

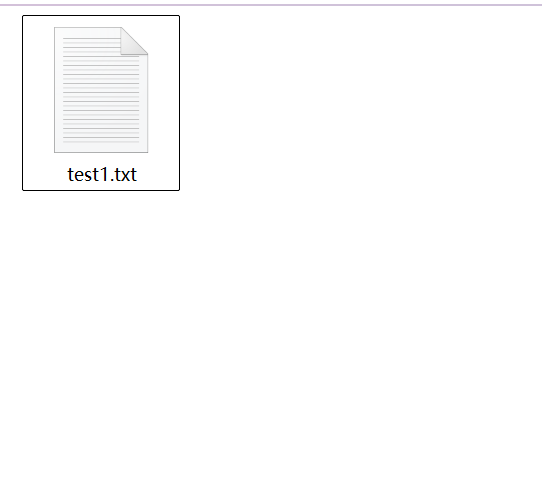
删除后**首项都变为了E5，是文件删除的标志**，其余部分没有变化，可以利用其他部计算文件数据的位置和簇链位置



查看文件内容



由此，我们只需要将E5标志去掉，再观察对应的文本信息，就可以恢复原文件



### 1.5 课后习题思考

* 在磁盘分区过程中，用户提供了哪些信息？分析分区工具的工作原理。

用户通常需要提供分区大小、文件系统类型（如NTFS、FAT32等）、分区标识符以及是否设为活动分区等信息。分区工具会根据这些信息，调整磁盘的分区表，并为新的分区分配空间

* 高级格式化与低级格式化的具体原理和区别是什么？

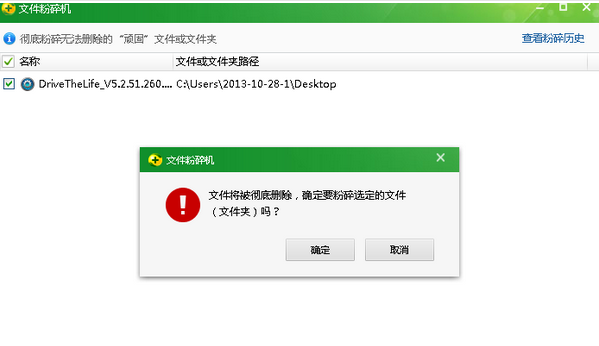
1.低级格式化（物理格式化）：这是制造商在硬盘生产过程中完成的，负责划分扇区和轨道，标记坏道，并在磁盘表面创建物理结构

2.高级格式化（逻辑格式化）：这一步是在操作系统中执行的，它为存储设备创建文件系统，并为数据写入做好准备

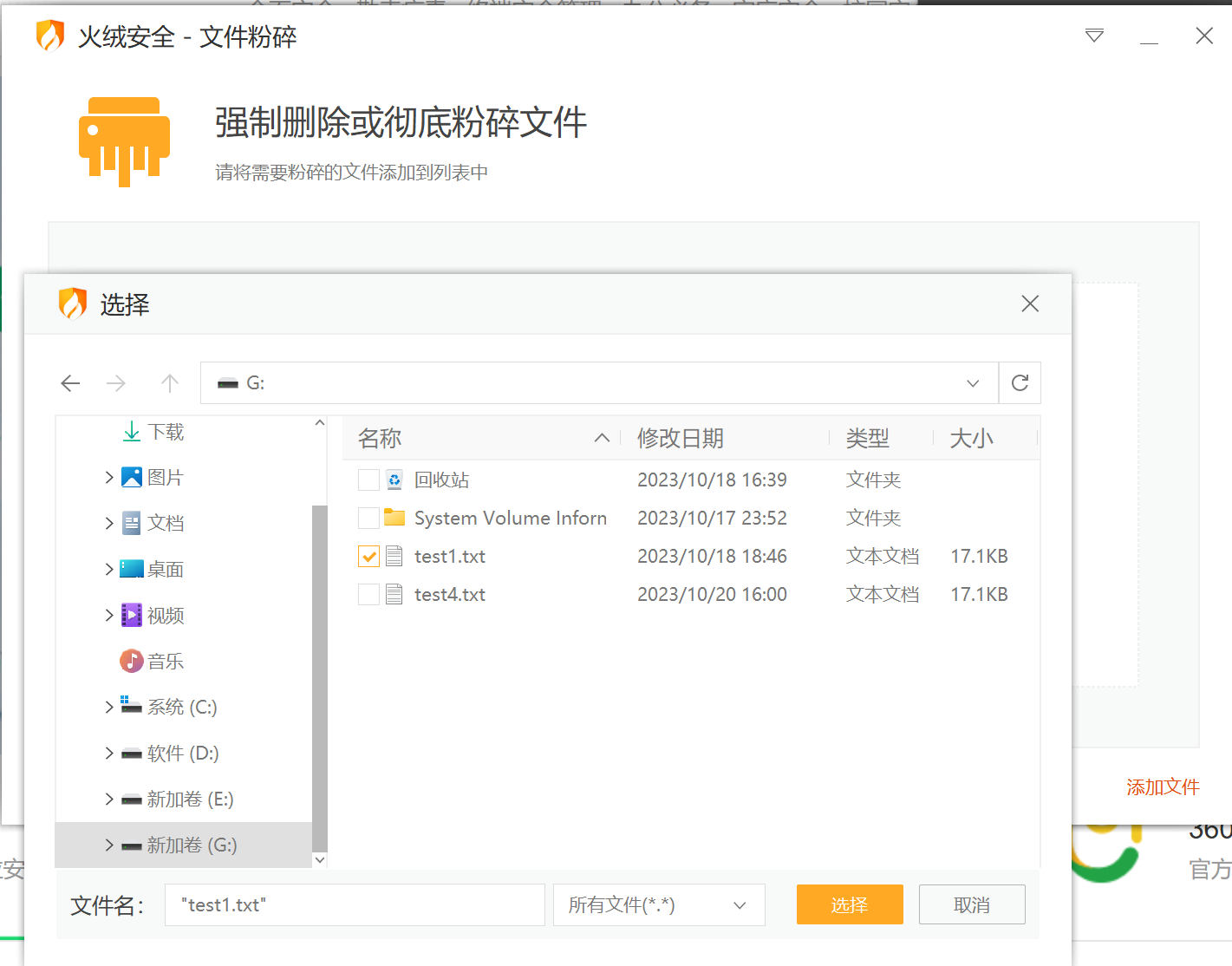
* 查找资料，对NTFS分区的总体结构进行分析，尝试对NTFS下删除的文件进行手工恢复

NTFS使用主文件表（MFT）管理文件。当文件被删除时，其文件记录仍保留在MFT中，文件恢复工具可以通过读取MFT中未被覆盖的文件记录尝试恢复文件。如果文件被覆盖或文件名很长，恢复会更复杂，具体见实验步骤

* 用数据粉碎工具（如金山、360、Strongdisk等）粉碎指定文件，分析其数据粉碎原理



网上找到的360文件粉碎使用图



火绒强制删除工具

数据粉碎原理：数据粉碎工具通过多次覆盖文件数据（使用随机数、特定数据模式等）来确保文件无法被恢复。这种多次写入可以防止简单的文件恢复工具从硬盘中提取已删除的数据

* 通过分区表看到的分区字节数为何与资源管理器中看到的分区字节数有差异？

如果删除的文件是长文件名，如何恢复所有文件名

（1）字节数的差异：分区表显示的分区大小通常是实际的物理大小，而资源管理器显示的是可用大小，扣除了系统保留空间、文件系统开销和对齐损失等

（2）恢复长文件名：长文件名的恢复取决于文件系统的设计和MFT（对于NTFS）的结构。NTFS会将长文件名分割并存储在多个记录中。恢复时需要读取这些分割的部分并重组它们，以恢复完整的文件名。可以通过winhex搜索功能查找文件头来确定文件的位置，一旦找到已删除文件的位置，你可以在 WinHex 中恢复文件名和内容。WinHex 提供了一个数据恢复向导，可以帮助你恢复已删除文件的内容

### 1.6实验体会和拓展思考

通过本次实验，我深入学习了WinHex和其他磁盘工具的使用，全面理解了磁盘的结构以及数据恢复的原理。实验中，我学会了如何查看和分析主引导记录（MBR）和GUID分区表（GPT）的分区结构，并进一步理解了NTFS和FAT32等文件系统的工作机制。在操作中，我尤其关注了GPT与MBR分区的差异，了解了它们在分区表存储、分区数量和容量支持等方面的显著不同。此外，我通过实验详细研究了FAT32文件系统，包括FAT表（FAT1和FAT2）的结构、簇链的管理，以及如何通过簇链来定位文件数据的存储位置。

实验中遇到的挑战包括，理解并分析GPT与MBR的分区结构需要较深入的理论知识；在FAT32文件系统中，分析文件的存储位置、首簇和簇链表也要求准确理解相关字段；在手动恢复被删除的文件时，需要耐心地分析残留目录项，计算出文件存储的位置，并修复相应的簇链。在处理这些问题时，我学习了如何准确定位分区表中的数据以及如何从簇链表中恢复被删除的文件。

总体而言，本次实验让我更加清楚地了解了磁盘结构和文件存储的工作原理，并提高了对数据恢复的理解。同时，我也意识到数据存储和文件删除过程中可能存在的安全隐患，强化了对数据安全和隐私保护的认知。