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)： 信息安全

学 号： 2021302181156

姓 名： 赵伯俣

课程名称： 软件安全实验

任课教师： 赵磊

2023年 10 月 15日

**目 录**

[实验1 磁盘格式与数据恢复(模板) 1](#_Toc35439173)

[1.1实验名称 1](#_Toc35439174)

[1.2实验目的 1](#_Toc35439175)

[1.3实验步骤及内容 1](#_Toc35439176)

[1.4实验关键过程、数据及其分析 3](#_Toc35439177)

[1.4.1 xxxx（章节自拟） 3](#_Toc35439178)

[1.4.2 xxxx 3](#_Toc35439179)

[1.4.3 课后习题思考 3](#_Toc35439180)

[1.5实验体会和拓展思考 3](#_Toc35439181)

# 实验1 磁盘格式与数据恢复

## 1.1实验名称

磁盘格式与数据恢复

## 1.2实验目的

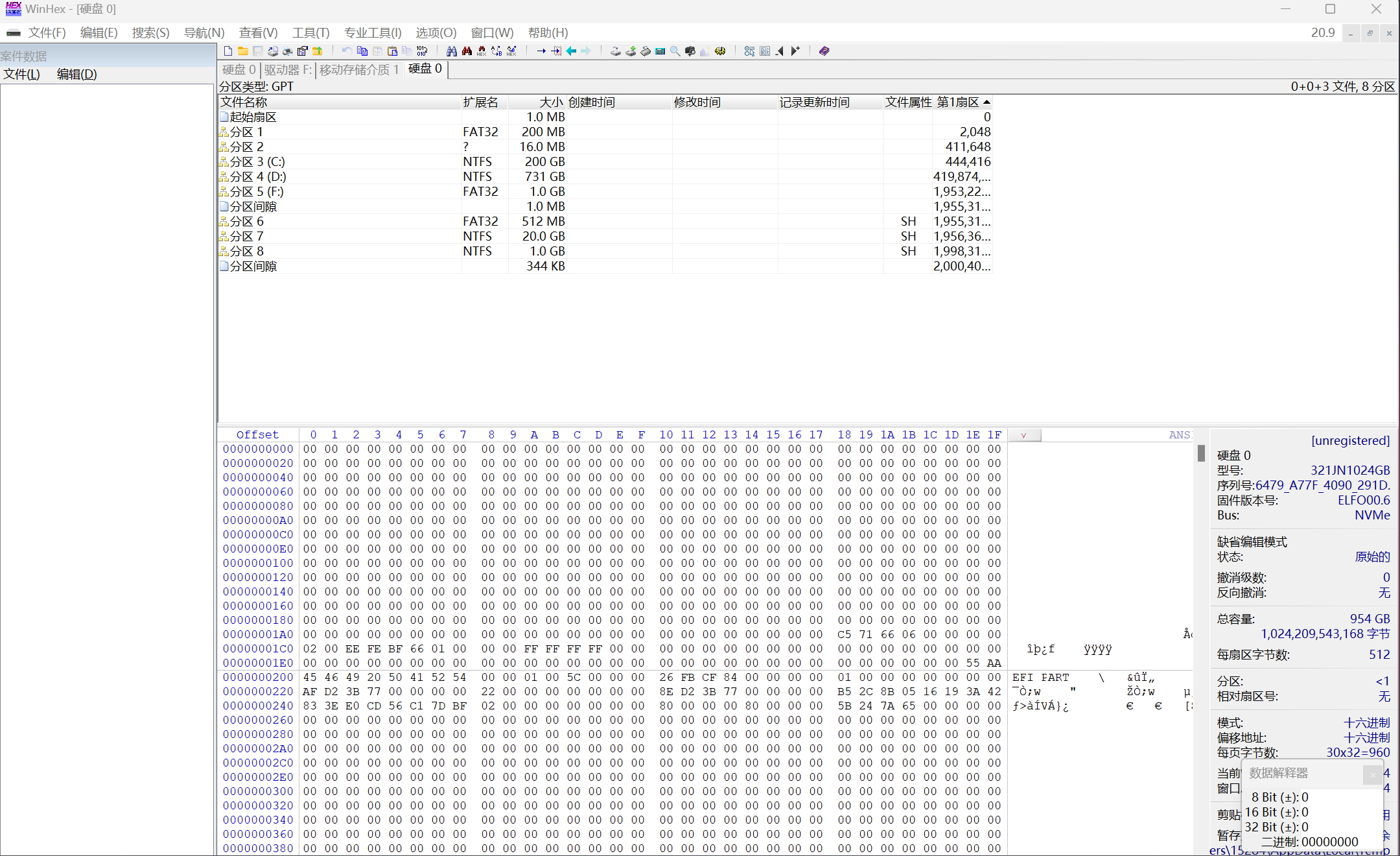
1. 了解磁盘的物理和逻辑结构
2. 熟悉FAT32文件系统
3. 学会使用磁盘编辑软件
4. 了解文件删除、格式化的基本原理
5. 能够利用工具或者手工恢复被删除的文件

## 1.3实验步骤及内容

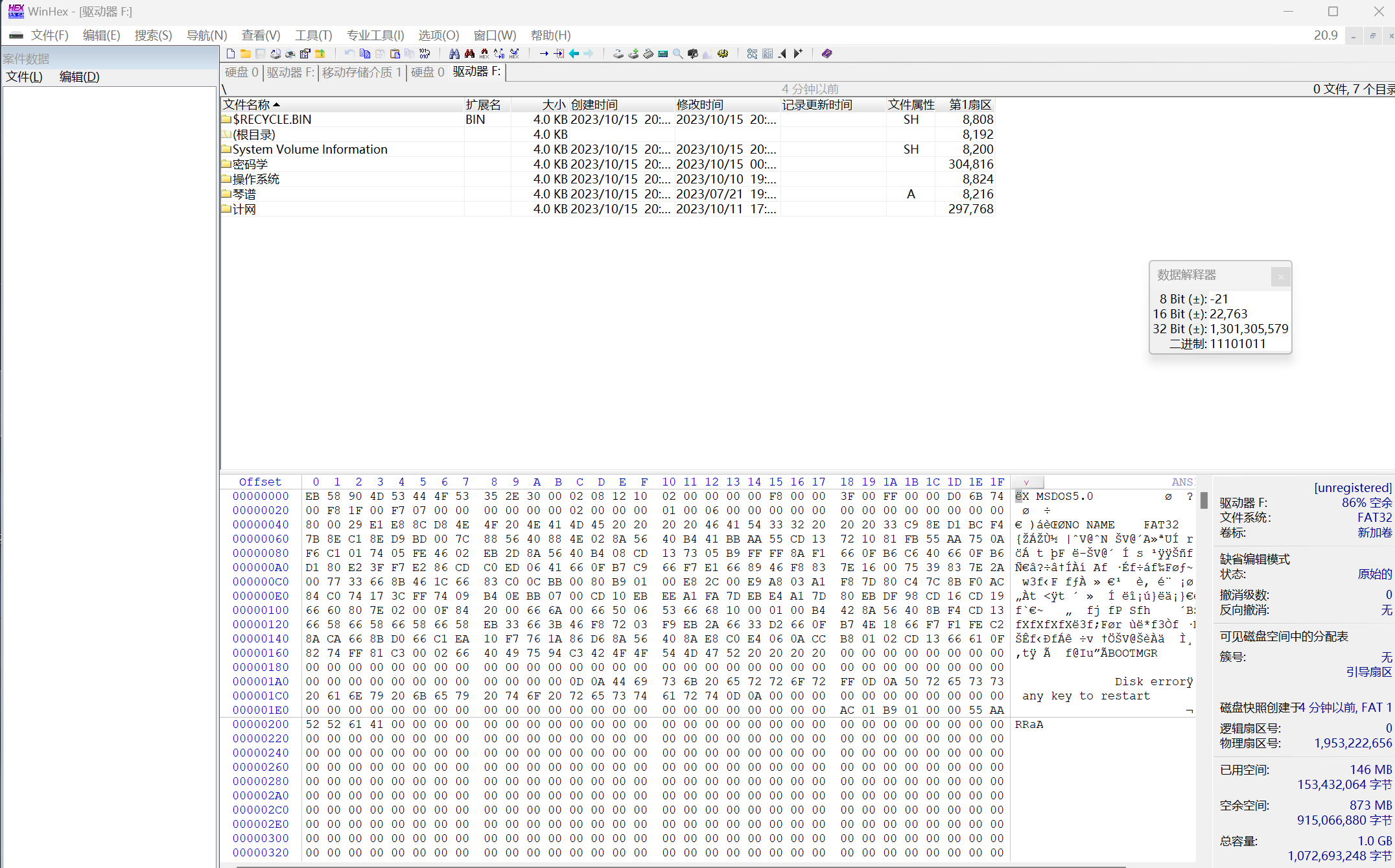
### 第一阶段：

* 熟悉WinHex的使用。
  + 利用WinHex查看物理磁盘和逻辑磁盘。

利用WinHex打开本地的物理盘的情况如下图所示，存在有8个分区和2个分区间隔。



使用WinHex打开本地的逻辑分区后可以看到在逻辑分区中的众多文件目录。



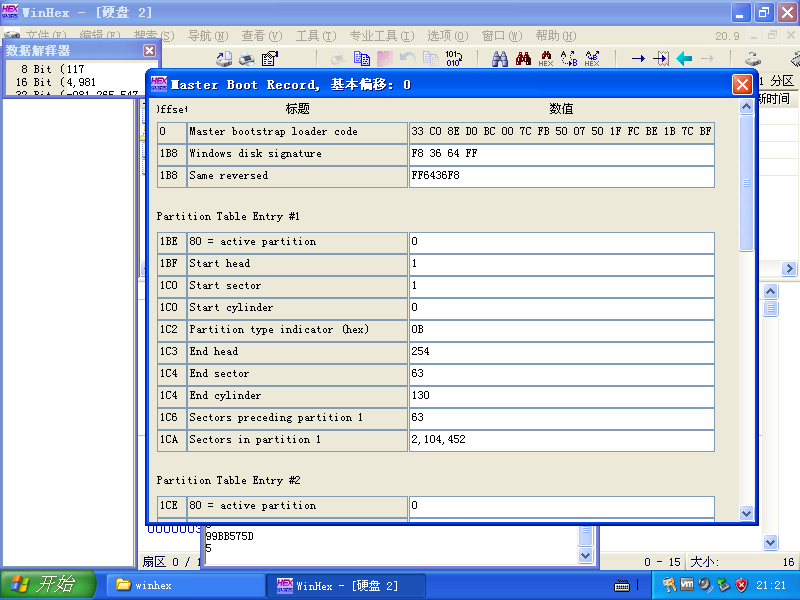
* + 了解WinHex中相关工具的用法。

通过使用导航栏中的跳转至偏移量和跳转至扇区可以成功跳转到对应的位置上。

### 第二阶段：

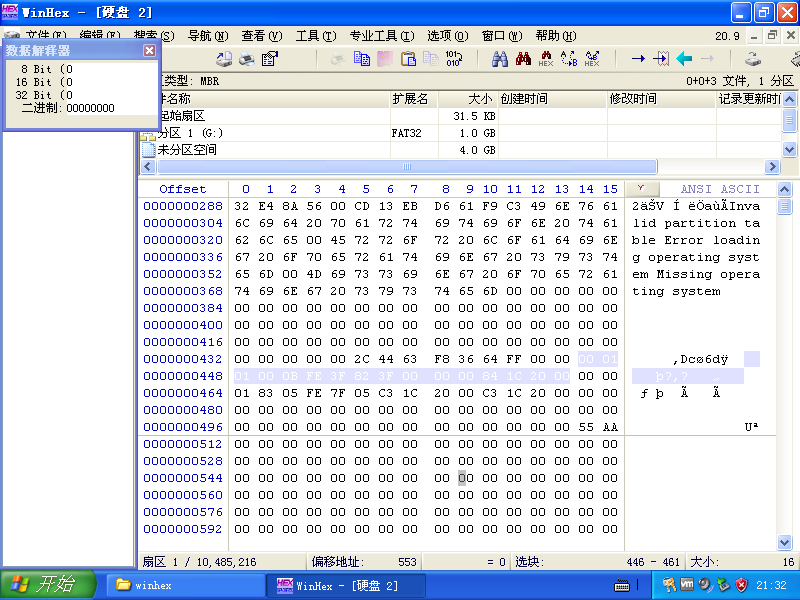
* 分析本地硬盘的主引导扇区
* 利用磁盘编辑工具查看MBR磁盘分区并分析：
  + 主引导扇区由哪些部分组成？

将主引导扇区的分区表打开后如下图所示。其中前1B8H（440）个字节为主引导扇区的引导代码，从第1BEH（446）个字节开始为主引导扇区的分区表，最后以55AA结尾。



* + 四个主分区项的内容各代表什么？

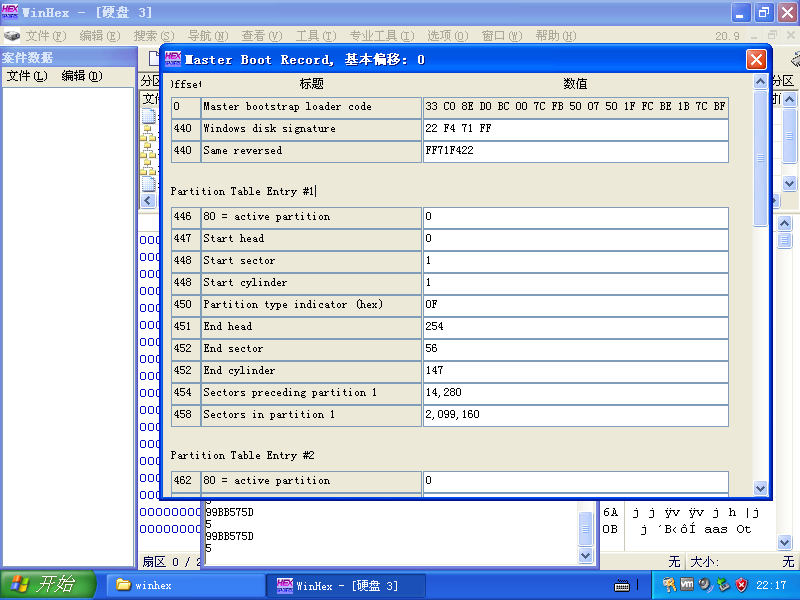
四个主分区项的内容如下图所示，

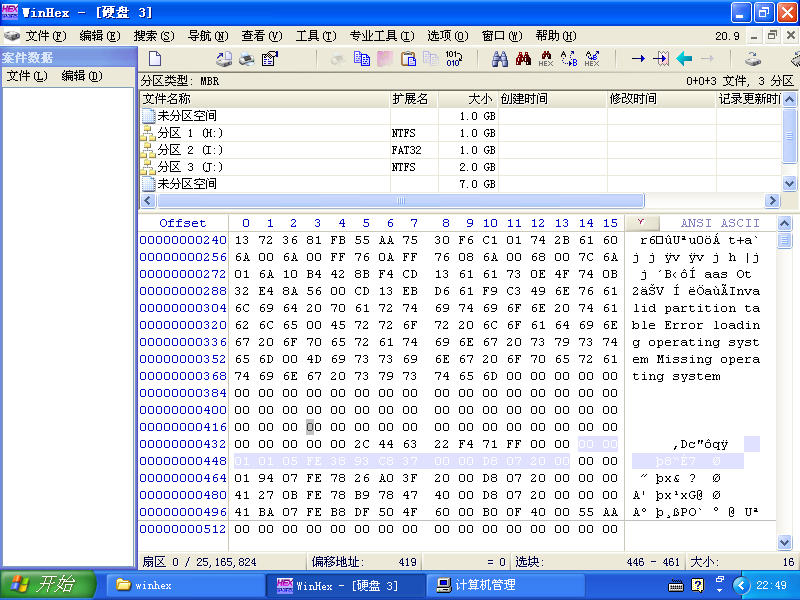


其中，每一个分区表项的大小为16个字节。在一个分区表项中，首先00代表分区的启动盘，010100代表这个分区的起始扇区为（0柱面，1磁头，1扇区），0B代表该分区的文件系统为FAT32，FE3F82代表磁头号为254; 扇区号为63 柱面号为255，3F000000代表该分区前面已有63个扇区，这63个扇区为系统隐藏扇区。84 1C 20 00代表表明该分区有2104452个扇区。

* + 分析主扩展分区表的结构。

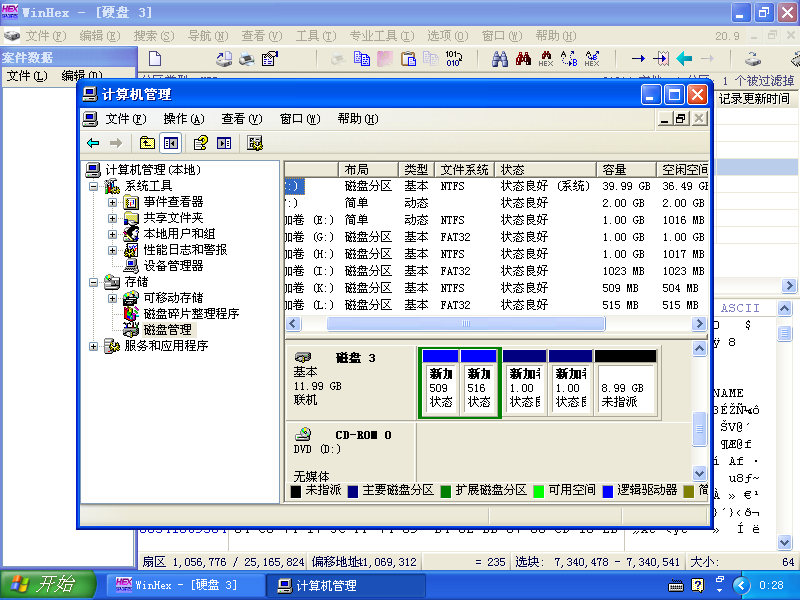
打开一个主拓展分区的分区表如下图所示。





一个拓展分区中可以有多个逻辑驱动器，扩展分区中的每个逻辑驱动器的分区信息都存在一个类似于MBR的扩展引导记录中，如上图所示，扩展引导记录包括分区表和结束标志“55 AA”，没有引导代码部分。

EBR中分区表的第一项描述第一个逻辑驱动器，第二项指向下一个逻辑驱动器的EBR。如果不存在下一个逻辑驱动器，第二项就不需要使用。下图为在磁盘管理器中查看逻辑磁盘状态。绿色框中的部分就是主拓展分区。



* + 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。

对于第一个分区项（00 00 01 01 05 FE 38 93 C8 37 00 00 D8 07 20 00），开始扇区位置为(0磁头，1扇区，1柱面)，总扇区数为2099160,结束扇区位置为(254磁头,56扇区，147柱面)，保留空间为2,099,160扇区，即约为1GB。

对于第二个分区项（00 00 01 94 07 FE 78 26 A0 3F 20 00 D8 07 20 00），开始扇区的位置为（0扇区 ，1磁头，148柱面），总扇区数为2,099,160，

结束扇区位置为（254磁头，56扇区，294柱面），保留空间大小为2,099,160扇区，

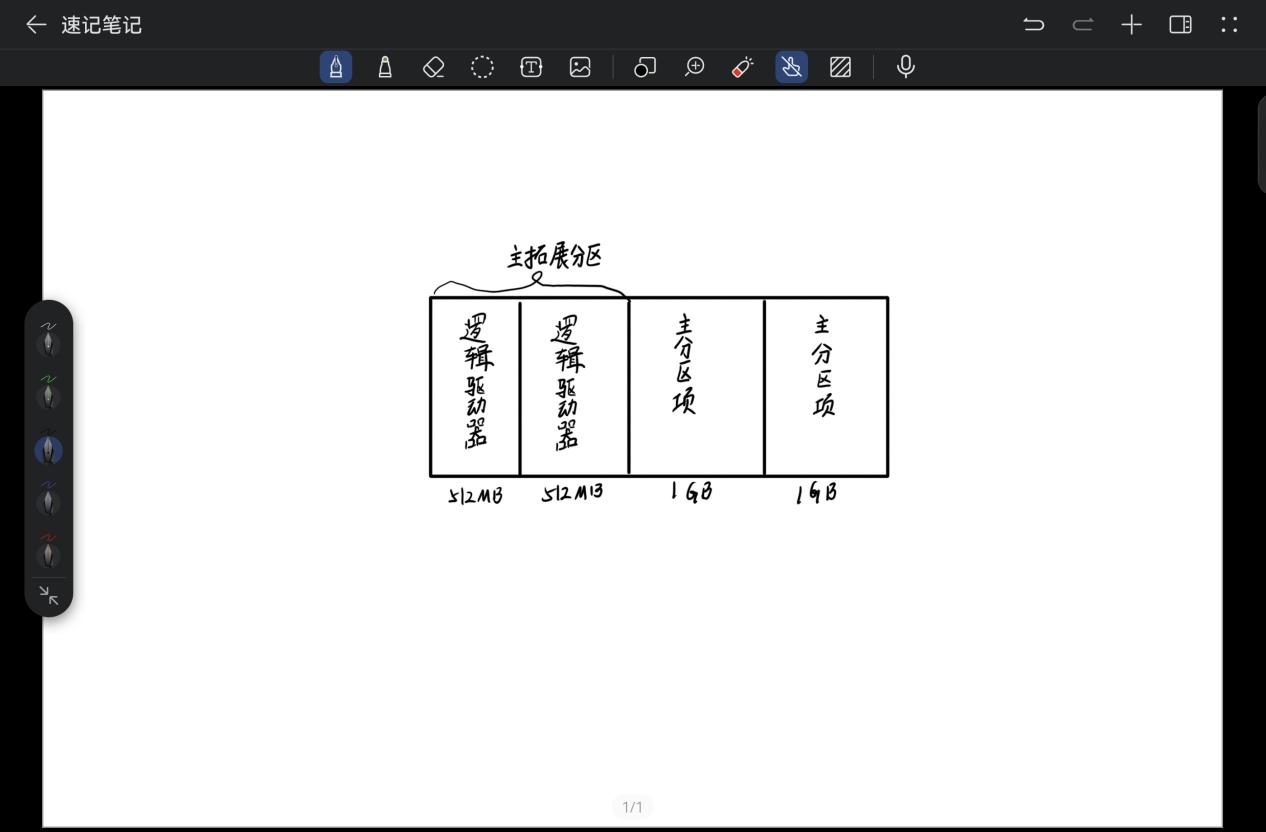
约为1GB。

对于第三个分区项（00 00 41 27 0B FE 78 B9 78 47 40 00 D8 07 20 00），开始扇区的位置为（0扇区 ，1磁头，295柱面），总扇区数为2,099,160，

结束扇区位置为（254磁头，56扇区，441柱面），保留空间大小为2,099,160扇区，

约为1GB。

本地硬盘的逻辑结构如下图所示：



* 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？

1.MBR中分区表的组织将磁盘的可寻址存储空间限制为2TB（232×512字节）。

2.MBR只支持4个主分区，或者3个主分区和1个扩展分区的组合。如果要创建更多分区，则需要将其中一个主分区设为“扩展分区”，然后在扩展分区内创建更多逻辑分区。否则，磁盘将转换为动态磁盘。

3.在MBR中，分区表的大小是固定的；在GPT分区表头中可自定义分区数量的最大值，也就是说GPT分区表的大小不是固定的。

* + 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。

包含主引导扇区代码，bios在执行自己固有的程序以后就会jump到MBR中的第一 条指令。将系统的控制权交由mbr来执行。

**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）。

### 1.4实验关键过程、数据及其分析

#### 1.4.1 xxxx（章节自拟）

#### 1.4.2 xxxx

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。

### 1.5实验体会和拓展思考

**注意：实验报告书写完毕之后请更新目录**