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)：

学 号：

姓 名：

课程名称：

任课教师： 彭国军

2020年 xx 月 xx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(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 xxxx（章节自拟）

#### 1.4.2 xxxx

#### 1.4.3 课后习题思考

### 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**