**《恶意代码分析》实验报告**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **年级、专业、班级** | | **20级信息安全专业01班** | | | **姓名** | **蔡欣彤** |
| **实验题目** | **编程实现FAT32表文件寻找过程** | | | | | |
| **实验时间** | **2023.4.16** | | **实验地点** | **DS3305** | | |
| **实验成绩** |  | | **实验性质** | **□验证性 □设计性 □综合性** | | |
| 教师评价：  □算法/实验过程正确； □源程序/实验内容提交 □程序结构/实验步骤合理；  □实验结果正确； □语法、语义正确； □报告规范；  其他：  评价教师签名： | | | | | | |
| 一、实验目的  1. 认识FAT32文件系统FAT表  2. 认识FAT32文件系统目录表  3. 认识FAT32文件系统簇号链结构 | | | | | | |
| 二、实验项目内容   1. 基本要求：利用Winhex软件，打开FAT32文件系统，通过DBR里提供的信息，手工计算FAT1的大小和位置，计算FDT表的位置，列举根目录下的文件和文件夹，利用FDT中某个文件的信息，列举该文件的簇号链，并根据簇号链，转入到该文件的data区。 2. 编程实现上述过程。 | | | | | | |
| 三、实验过程或算法（源程序）  1.  （1）DBR       |  |  | | --- | --- | | DBR信息 |  | | 每扇区字节数 | 0x200： 512 | | 每簇扇区数 | 0x8： 8 | | 保留扇区数 | 0x1006： 4102 | | 每FAT扇区数 | 0x7FD： 2045 | | 根目录起始簇 | 0x2： 2 |   （2）定位FAT1  在FAT文件系统中FAT表是在保留扇区之后，故而，FAT1表的位置需要从DBR跳转4102个sector。    （3）定位FAT2  在FAT文件系统中FAT2表是在FAT1表之后，故而，FAT2表的位置需要从DBR跳转4102+2045个sector。    （4）定位根目录FDT  FAT2表过后就是rootdir的内容，也就是需要跳转的sector=4102+2045\*2。    （5）解析文件信息     |  |  | | --- | --- | | IMG\_20211117\_142204.jpg |  | | 文件名 | IMG\_20211117\_142204 | | 扩展名 | jpg | | 属性 | 0x20(归档) | | 起始簇号 | 6 | | 文件长度 | 0x3682CB byte |   由起始簇号6，查找FAT表。    簇号链为：0x6一直到0x36E。  根据起始簇号，进入存储该图片的data区，跳转6个簇    Over     |  |  | | --- | --- | | 123(文件夹名) |  | | 文件名 | 123 | | 扩展名 | 0x202020 | | 属性 | 0x10 | | 起始簇号 | 0x36F | | 文件长度 | 0x0 byte |   只有一个簇号，进入0x36F簇号的data区：       |  |  | | --- | --- | | 456(文件夹名) |  | | 文件名 | 456 | | 扩展名 | 0x202020 | | 属性 | 0x10 | | 起始簇号 | 0x370 | | 文件长度 | 0x0 byte |   只有一个簇号，进入0x370簇号的data区：     |  |  | | --- | --- | | 789(文件夹名) |  | | 文件名 | 789 | | 扩展名 | 0x202020 | | 属性 | 0x10 | | 起始簇号 | 0x371 | | 文件长度 | 0x0 byte |   只有一个簇号，进入0x371簇号的data区：     |  |  | | --- | --- | | IMG\_20211210\_123430.jpg |  | | 文件名 | IMG\_20211210\_123430 | | 扩展名 | jpg | | 属性 | 0x20(归档) | | 起始簇号 | 0x372 | | 文件长度 | 0x1066DE byte |   簇号链为：0x372一直到0x478    进入data区 | | | | | | |
| 四、实验结果及分析和（或）源程序调试过程 | | | | | | |