文章编号：2095-2163(2019)04-0304-04 中图分类号：TP316 文献标志码：A

Linux 下 Ext3 文件系统结构研究

苏神保，刘 丹
（湖南商务职业技术学院，长沙 410205）

摘 要：在 Linux 操作系统中，磁盘的分区结构与 Windows 系统一样，都采用 MBR 或者 GPT 磁盘分区，但在文件系统的结构上却有很大的差别，Windows 系统常见的文件系统有 FAT32、NTFS、exFAT 等，而 Linux 系统的则为 Ext2/3/4。本文以 Linux 操作系统中常见文件系统 Ext3 为例，详细介绍该文件系统的结构并举例说明其手工提取文件的方法。

关键词：Winhex；Ext3；Block；i-节点

Research on Ext3 file system structure under Linux

SU Shenbao, LIU Dan
(Hunan Vocational College of Commerce, Changsha 410205, China)

【Abstract】 In Linux operating system, disk partitioning structure is the same as that of Windows system which uses MBR or GPT disk partitioning. But there are great differences in the structure of file system. The common file systems in Windows system are FAT32, NTFS, exFAT, while in Linux system, they are Ext2/3/4.Taking Ext3 which is a common file system in Linux operating system as an example, this paper introduces the structure of the file system in detail and illustrates the method of extracting files manually.

【Key words】 Winhex; Ext3; Block; i-node

1 Ext3 文件系统基本介绍

Ext3 文件系统所在区域先是被划分为一个个的块(Block)，每个块的大小都是一样的，但是对于不同的 Ext3 文件系统，块的大小也可能存在差别。典型的块大小有 1 024 字节、2 048 字节或者 4 096 字节，在 Winhex 中分别为 2 扇区、4 扇区或者 8 扇区。该数值将在创建文件系统时被决定，可以由文件系统的创建程序根据硬盘分区的大小来自动选择一个较为合理的值。

块是文件系统中数据的分配单元，每个块均有唯一的编号，第一个块的编号为 0，此后依序排列，0 号块起始于文件系统的开始扇区。

Ext3 文件系统的全部空间被划分为若干个块组，每个块组内的结构都大致相同，Ext3 文件系统的整体结构及第一个块组的单元结构如图 1 所示。

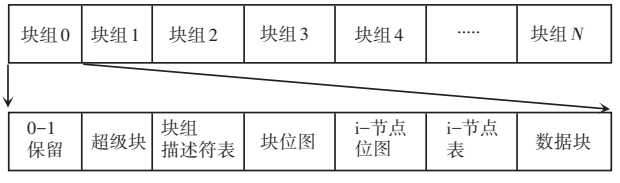

图 1 Ext3 文件系统的结构(部分截取)

Fig. 1 Structure of Ext3 file system(partial interception)

由图 1 可以看出，Ext3 文件系统的第一个块组的结构功能分析可阐释如下。

(1)Ext3 文件系统的前两个扇区用来存放引导程序，称为引导扇区。如果没有引导程序则保留不用，一般为空扇区，没有任何数据。

(2)Ext3 文件系统的第 3 个扇区、也就是 2 号扇区是超级块，超级块占用 2 个扇区，用于存储文件系统的配置参数(如块大小、总块数和 i-节点数)和动态信息(如当前空闲块数和 i-节点数)。

(3)块组描述符表用于存储块组描述符，占用一个或者多个块，设计时取决于文件系统的大小。每个块组描述符主要描述块位图、i-节点位图和 i-节点表的地址等信息。

为了系统的健壮性，Linux 最初在每个块组内部对超级块和块组描述符表做了备份，但是当文件系统很大时，这将耗费很多空间，尤其是块组描述符表占用的块较多时。为此后来采用了一种稀疏的方式来存储这些备份，也就是只有在块组号是 3、5、7 的幂的块组(如 0、1、3、5、7、9、25、27、49 等)内才对超级块和块组描述符进行备份。

(4)i-节点用于描述文件的元数据，每个 i-节点对应文件系统中唯一的节点号。

作者简介：苏神保(1982-)，男，硕士，讲师，主要研究方向：电子与通信。

收稿日期：2019-05-17

2　Ext3 文件系统的超级块分析

一般地，当块大小为 8 个扇区时，超级块起始于 0 号块，其位于 0 号块的 2~3 号扇区，0~1 号扇区是引导程序或者保留扇区，4~7 号扇区则是空闲的。另外，在块组号是 3、5、7 的幂的块组中，超级块也有相应的备份，通过在 Winhex 中向下搜索超级块标志 53EF 可以跳转至有超级块备份的相应块组中去。Ext3 文件系统的超级块是一个至关重要的扇区，其中记录的参数非常多。这里给出了某一 Ext3 文件系统的 0 号块组的超级块如图 2 所示。而该超级块中主要参数及含义详见表 1。

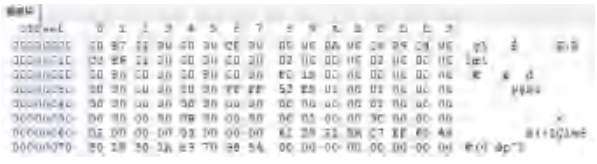

图 2　Ext3 文件系统 0 号块组的超级块(部分截取)

Fig. 2　Super block of block group 0 for Ext3 file system (partial interception)

表 1　Ext3 文件系统的超级块主要参数表

Tab. 1　Main parameters of super block for Ext3 file system

字节偏移	字段长度	字段名和定义	典型值(字节)	大小
0X00~0X03	4	i-节点总数	00E73100	3 270 400
0X04~0X07	4	总块数	00000C8	13 107 200
0X18~0X1B	4	块大小描述值	02000000	2^2×1 024
0X20~0X23	4	每块组包含的块数	00800000	32 768
0X28~0X2B	4	每块组包含的 i-节点数	F01F0000	8 176
0X58~0X59	2	i-节点大小	0001	256
0X5A~0X5B	2	当前超级块所在的块组	0000	0

在上述 Ext3 文件系统中，超级块的参数描述了文件系统的总块数是 13 107 200，每块组包含的块数是 32 768，块大小、即每块包含的扇区数为 2^2×1 024=4 096B=8S，而每块组包含的扇区数为 32 768×8=262 144 S，总块组数为 13 107 200/32 768=400，分别编号为 0~399。

3　Ext3 文件系统的块组描述符分析

Ext3 文件系统的每个块组描述符占用 32 字节，有超级块备份的块组都包含有块组描述符备份，这是用来描述该块组中的块位图的起始块号、i-节点位图的起始块号以及 i-节点表的起始块号等信息，一个 Ext3 文件系统有多少个块组，都需要在块组描述符中体现出来。而本文中研发得到的某一 Ext3 文件系统 0 号块组的块组描述符实例则如图 3 所示。此处以 0 号块组描述符为例，其 hex 数值代表的含义详见表 2。

图 3　Ext3 块组描述符实例(部分截取)

Fig. 3　Ext3 block group descriptor example (partial interception)

表 2　块组描述符的结构

Tab. 2　The composition of Ext3 block group descriptor

字节偏移	字段长度	字段名和定义	典型值(字节)	大小
0X00~0X03	4	该块组块位图起始块号	01040000	1 025
0X04~0X07	4	该块组的 i-节点位图起始块号	02040000	1 026
0X08~0X0B	4	该块组的 i-节点表起始块号	03040000	1 027
0X0C~0X0D	2	该块组的空闲块数	FC79	31 228
0X0E~0X0F	2	该块组的空闲 i-节点数	BC1F	8 124
0X10~0X11	2	该块组的目录总数	0300	3

由表 2 可知，在该块组中，块位图开始于 1 025 号块，i-节点表位图开始于 1 026 号块，i-节点表开始于 1 027 号块，块组中已用块数 32 768-31 228=1 540，已用 i-节点数为 8 176-8 124=52 个。块位图描述该块组中块的使用情况，i-节点位图描述该块组中 i-节点的使用情况。因篇幅有限，文中不再一一赘述。

4　Ext3 文件系统的 i-节点分析

Ext3 文件系统的 i-节点用来存储与文件相关的除文件名以外的所有信息，每个块组中都有一个自己的 i-节点表，i-节点表由很多的 i-节点组成，每个文件或者目录使用一个 i-节点。i-节点表起始于 i-节点位图所在块的下一个块，超级块中记录着文件系统的 i-节点总数和每块组包含的 i-节点数，i-节点的大小在超级块中指定，一般为 128 字节或者 256 字节。每个 i-节点都有一个编号，第 1 个 i-节点的编号为 1，1~10 号 i-节点被系统保留，所以在超级块中会描述第一个非保留的 i-节点，这个值一般为 11，前 10 个保留的 i-节点在 i-节点位图中被表示为已分配，其中 1 号 i-节点一般用于描述坏块，2 号 i-节点被分配给根目录使用，8 号 i-节点通常用于描述日志，如果已知一个 i-节点号，就可以计算出该 i-节点所在的块组，计算方法为：(i-节点号-1) DIV 每块组 i-节点数

在此基础上,还将计算得出在该块组中的 i-节点号,计算公式为:(i-节点号-1) MOD 每块组 i-节点数+1

至此,可得一文件的 i-节点表如图 4 所示。

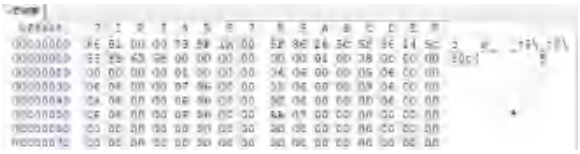

图 4 Ext3 文件系统的 i-节点表(部分截取)

Fig. 4 i-node table of Ext3 file system(partial interception)

由图 4 中的偏移地址 0X28 可知,在 i-节点中用块指针描述文件内容的存放地址。每个 i-节点中有 15 个块指针,包含 12 个直接块指针,1 个间接块指针,1 个二级间接块指针和 1 个三级间接块指针。12 个直接块指针指向文件内容的前 12 个数据块地址,如果文件大于 12 个块,则第 13 个块指针是一个间接块指针,由其指向的块存放的是直接块指针而不是文件内容,以此类推。当文件较小时一般只需用到直接块指针,当文件较大时才会用到间接块指针。由上述实例可知,该文件从 0X28 至 0X57 已经使用了 12 个直接指针块,0X58 为间接块指针。如需手工提取文件,需要从 i-节点 0X04 位置读取文件大小后换算提取。

5 Ext3 文件系统目录项分析

目录项用来存放文件及目录的 i-节点号、目录项的长度、文件名等信息,并实际存储在分配给目录的块中。研究得到的一 Ext3 文件系统的根目录如图 5 所示。

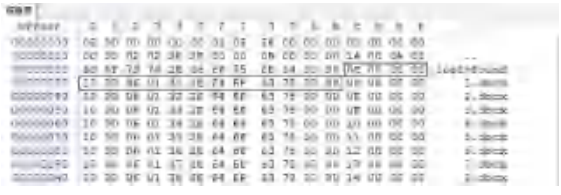

图 5 Ext3 文件系统的根目录(部分截图)

Fig. 5 Root directory of Ext3 file system(partial interception)

Ext3 文件系统的目录项结构见表 3。

表 3 Ext3 文件系统的目录项结构

Tab. 3 Directory item structure of Ext3 file system

字节偏移	字段长度(字节)	字段名和定义
0X00~0X03	4	i-节点号
0X04~0X05	2	目录项长度
0X06~0X06	1	名字长度
0X07~0X07	1	文件类型
0X08~		名字

在图 5 中标注出了文件 1.docx 的目录项,由表 3 可知,该文件的 i-节点号为 0C000000 即为 12,目录项的长度为 1 000、即为 16,文件名的长度占用 6 个字节,文件类型为文件,文件名为 1.docx。同理可知,2.docx 的 i-节点号为 0D000000、即为 13,目录项的长度也是 1 000、即为 16,文件名的长度占用 6 个字节,文件类型为文件,文件名为 2.docx。

6 Ext3 文件系统的手工提取文件实例分析

某 Ext3 文件系统因计算机突然断电导致无法读取文件,现需恢复该文件系统的 18.docx 号文件,这一过程中将会涉及的操作步骤可做完整表述如下。

由 2 号扇区超级块信息可知,块大小为 4 096 字节、即 8 个扇区,i-节点大小为 256 字节,每块组包含的块数为 32 768。跳转至 8 号扇区、即块组描述符,找到 0 号块组描述符的 i-节点表的起始块号,跳转过去就可到达 0 号块组的 i-节点表位置。因 1 号 i-节点一般用于描述坏块,2 号 i-节点用于描述根目录的起始块号,读取 2 号 i-节点的直接块指针为 1538 号块、即 12304 号扇区就可跳转至根目录,依据根目录结构可知 18.docx 文件的 i-节点号为 1D000000、即为 29,因每块组包含的 i-节点数为 8 176,故 29 号 i-节点位于 0 号块组,由块组描述符再次跳转至 0 号块组的 i-节点表,从上至下数至 29 号i-节点、即为 18.docx 文件的 i-节点。具体如图 6 所示。

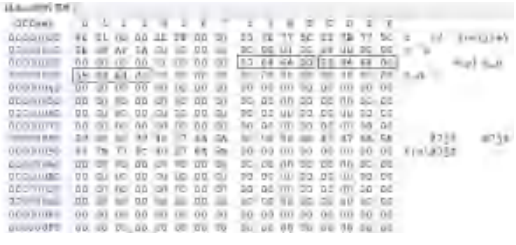

图 6 18.docx 文件的 i-节点

Fig. 6 i-node of 18.docx file

由 i-节点定义可知,该文件的 i-节点包含有 3 个直接块指针(在图 6 中用方框标出),分别为 6 587 479、6 587 480、6 587 481 号块,文件大小为 12 077 字节,跳转至 6 587 479 号块,手工提取文件即可。

7 结束语

全文借助 Winhex 底层十六进制数据编辑恢复软件,以 Linux 下 Ext3 文件系统为例,详细分析了该

(下转第 312 页)