CIS2390 PRACTICAL

Week 13

Questions

This week you may download an ext3 filesystem image from:

http://helios.hud.ac.uk/scomcjp/ext3-img-kw-1.dd

This image has the MD5 hash:

30e7f792cc853e34e17335b243605d3a.

Use *Winhex* to analyze this image and answer the following questions:

1. This question gets you to examine the key ext3 data structures.
   a. By analyzing the superblock, answer the following questions (verify your answers against the information present in *Winhex's* image details tab):
      i. How many sectors are in a block?
      ii. How many block groups are on this image?
      iii. How many inodes are there in each block group?
      iv. At what sector does block group 0 start?
   b. By analyzing the group descriptor table for block group 0, answer the following questions:
      i. At what sector does the block bitmap start?
      ii. At what sector does the inode bitmap start?
      iii. At what sector does the inode table start?
   c. What blocks and inodes have been allocated in block group 0?
2. The file `/file3` has been deleted, this question gets you to try and undelete this file. In order to aid you in doing this, answer the following questions:
   a. What inode number did this file have?
   b. Assuming free space was available, in what block group are this files contents located?
   c. What can you determine by looking at this inode's entry in the block group's inode table?

d. By examining the contents of inode 2, answer the following questions:

   i. What type of indirect block pointers are used to store the contents of the root directory entries?

   ii. What blocks are the root directory entries located in?

e. By examining the root directory entries, what can you say about the file `/file3`?

f. By assuming that contiguous blocks were originally allocated to this file, and that the file contained the string *third*, what blocks were allocated to this file?

g. You are told that this is a journaling filesystem. By examining the filesystem journal, what else (if anything) can you determine about the blocks that were originally allocated to the file `/file3`?

Ext3 Data Structures

Superblock

Byte Range	Description
0-3	Number of inodes in file system
4-7	Number of blocks in file system
..	..
20-23	Block where block group 0 starts
24-27	Block size (= $1024*2^{(\text{value of this field})}$ bytes)
..	..
32-35	Number of blocks in each block group
..	..
36-39	Number of blocks in each block group
40-43	Number of inodes in each block group
..	..
58-59	File system state
..	..
84-87	First non-reserved inode in file system
88-89	Size of each inode structure
..	..
208-223	Journal ID

Byte Range	Description
224-227	Journal inode
..	..

Flags For File System State (In Superblock)

Flag Value	Description
0x0001	File system is clean
0x0002	File system has errors
0x0004	Orphan inodes are being recovered

Group Descriptor Tables

Byte Range	Description
0-3	Starting block address of block bitmap
4-7	Starting block address of inode bitmap
8-11	Starting block address of inode table
..	..

Inodes

Byte Range	Description
0-1	File mode (type and permissions) - see tables below
..	..
40-87	12 direct block pointers
88-91	1 single indirect block pointer
92-95	1 double indirect block pointer
96-99	1 triple indirect block pointer
..	..

Permission Flags (Bits 0-8 Of Inode File Mode)

Permission Flag	Description
0x001	Other - execute permission
0x002	Other - write permission
0x003	Other - read permission
0x008	Group - execute permission
0x010	Group - write permission
0x020	Group - read permission
0x040	User - execute permission
0x080	User - write permission
0x100	User - read permission

Miscellaneous Flags (Bits 9-11 Of Inode File Mode)

Permission Flag	Description
0x200	Sticky Bit
0x400	Set Group IP
0x800	Set User ID

Type Flags (Bits 12-15 Of Inode File Mode)

Type Value	Description
0x1000	FIFO
0x4000	Directory
0x6000	Block Device
0x8000	Regular File
0xA000	Symbolic Link
0xC000	UNIX Socket

Directory Entry

Byte Range	Description
0-3	Inode Value
4-5	Length of this entry
6-6	Name length
7-7	File type - see table below
8+	Name in ASCII

Value For Directory Entry Type Field

	Description
0	Unknown type
1	Regular file
2	Directory
3	Character device
4	Block device
5	FIFO
6	Unix socket
7	Symbolic link

Journal Data Structures

Superblock

Byte Range	Description
0-3	Signature (0xC03B3998)
4-7	Block Type (see below)
8-11	Sequence number
..	..
24-27	Sequence number of first transaction
28-31	Journal block of first transaction
..-1023	..

Descriptor Block

Byte Range	Description
0-3	Signature (0xC03B3998)
4-7	Block Type (see below)
8-11	Sequence number
12-15	File system block
16-19	Entry Flags
..-35	..

Commit Block

Byte Range	Description
0-3	Signature (0xC03B3998)
4-7	Block Type (see below)
8-11	Sequence number

Type Field (Journal Headers)

Value	Description
1	Descriptor block
2	Commit block
3	..
4	Superblock
5	..