XENIX 下误删文件的恢复方法

唐兆海　（江苏省洪泽县工商银行）

在 XENIX 系统中，常发生因使用 rm 命令而不慎将文件误删的情况，但只要此时再没人使用系统建立新文件，删除的文件是可以恢复的。因为 rm 命令只是把文件在文件系统中的 i 节点(inode)信息清除，而文件的正文信息与数据信息占据的磁盘块还未被清除，此时只要找到这些磁盘块，重建文件的 i 节点，便可拯救误删文件。

XENIX 文件系统有如下结构：(见图 1)

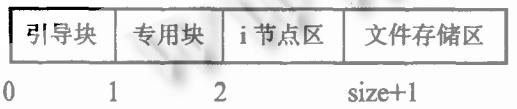

图　1

当文件被删除时，其占据的磁盘块被依次压栈到空闲块索引表(free block list)的顶部，索引表位于文件系统超级专用块(super block)的首端。我们只要从索引表里找出这些块号，填入 i 节点区内，重构文件的 i 节点，便使删除的文件得以恢复。

下面以 sco xenix V release 2,3,2 的根文件系统(/dev/root)为例，步骤如下：

1.首先利用 sync 命令，以内存专用块更新外存专用块。

2.在 2 号专用块上找刚压栈的磁盘块。

hd −wx −s 0x400 /dev/root　more

```
0400   0a8e  a32f  0002  0024  8d66  0001  8d65  0001
0410   8d64  0001  8d63  0001  8d62  0001  8d61  0001
0420   8d60  0001  8d5f  0001  8d5e  0001  8d5d  0001
0430   8d5c  0001  8d5h  0001  8d5a  0001  8d59  0001
0440   8d58  0001  8d57  0001  8d56  0001  8d55  0001
0450   8d54  0001  8d53  0001  8d52  0001  8d51  0001
0460   8d50  0001  8d4f  0001  8d4e  0001  8d4d  0001
0470   8d4c  0001  8d4h  0001  8d4a  0001  8d49  0001
0480   8d48  0001  8d47  0001  8d46  0001  8d45  0001
0490   8d44  0001  8d43  0001  8d42  0001  zae7  0000
04a0   0982  0002  097e  0002  0984  0002  8d3d  0001
04d0   cffa  0001  cff9  0001  cff8  0001  c392  0001
04c0   c391  0001  c390  0001  c38f  0001  c38e  0001
04d0   c38d  0001  c38c  0001  c38b  0001  c38a  0001
04e0   c389  0001  c388  0001  c387  0001  c386  0001
04f0   c385  0001  c384  0001  c383  0001  c382  0001
0500   c381  0001  c380  0001  c37f  0001  c37e  0001
0510   8d24  0001  8d23  0001  8d22  0001  8d21  0001
0520   8d20  0001  8d1f  0001  8d1e  0001  8d1d  0001
0530   8d1c  0001  8d1h  0001  8d1a  0001  8d19  0001
0540   8d18  0001  8d17  0001  8d16  0001  8d15  0001
0550   8d14  0001  8d13  0001  8d12  0001  8d11  0001
0560   8d10  0001  8d0f  0001  8d0e  0001  8d0d  0001
0570   8d0c  0001  8d0h  0001  8d0a  0001  8d09  0001
0580   8d08  0001  8d07  0001  8d06  0001  8d05  0001
0590   8d04  0001  8d03  0001  0063  000f  09f3  09f2
05a0   09f1  09f0  09ef  09ee  09ed  09ec  09eb  09ea
05b0   09e9  09e8  09e7  09e6  09e5  09e4  09e3  09e2
05c0   09e1  09e0  09df  09de  09dd  09dc  09db  09da
05d0   09d9  09d8  09d7  09d6  09d5  09d4  09d3  09d2
05e0   09d1  09d0  09cf  09ce  09cd  09cc  09cb  09ca
05f0   09c9  09c8  09c7  09c6  09c5  09c4  09c3  09c2
0600   09c1  09c0  09bf  09he  09hd  09bc  09hb  09ba
0610   09b9  09b8  09b7  09b6  09b5  09b4  09b3  09b2
0620   09b1  09h0  09af  09ae  09ad  09ac  09ab  09aa
0630   09a9  09a8  09a7  09a6  09a5  09a4  09a3  09a2
0640   09a1  09a0  099f  099e  099d  099c  099b  099a
0650   0999  0998  0997  0996  0995  0994  0993  0798
0660   02e4  0000  0000  5778  2d7d  cff3  0000  91e5
0670   0001  01f4  0000  0000  0000  0000  0000  0000
0680   0000  0000  0000  0000  0000  0000  0000  0000
*
07f0   0000  0000  0000  0000  5544  002h  0002  0000
0800   8000  0000  0000  0000  0000  0000  0000  0000
0810   0000  0000  0000  0000  0000  0000  0000  0000
```

图　2

从地址 0x400e 开始，第七、八两字节 0024 是表示文件系统直接管理的空闲块个数为 36；接着为一百个空闲块号索引表，刚压入的块在索引表最底部，地址 0x598 处。恢复文件时，要充分估计文件的长度，因为估计长了

可在恢复后删掉，而短了所丢失的数据再也无法恢复。现假设文件长度为 4096 字节(8x512)，即占用 8 个磁盘块；若文件长度超过索引表给出的空闲块数，则剩余块号就得从索引表最上端，即 0001 8d66 块号找出。块号 0001 8d66 先转化为二进制数 0001 1000 1101 0110 0110，接着将其左移十位，即于其后添加十个零，则可得十六进制数 6359800h，此为剩余块号首地址，用 hd-wx -s 0x6359800 / dev / root more 读此块内容，若第一字段为 0050 说明其后有 80 个空闲块，将不足的补齐。

3.从图 2 上由后向前取 8 个块号：

00018d03 00018d04 00018d05 00018d06 00018d07 00018d08 00018d09 00018d0a

以上每个块号占 4 字节，因为在 i 节点中每个块号只占 3 字节，所以应将每个块号的最高字节 00 删除，使每 3 字节表示一个空块号。如下所示：

018d03 018d04 018d05 018d06 018d07 018d08 018d09 018d0a

为便于 adb 命令将块号写入 i 节点中，再把块号改为 2 字节一段，并作如下变换：

8d03 0401 018d 8d05 0601 018d 8d07 0801 018d 8d09 0a01 018d

4.在图 2 中，地址 0x599h 信息 0063 表示系统直接管理的 i 节点号个数，其后为一百个空闲 i 节点号索引表。从中任取一个，算出该 i 节点号的首地址，若取 09f3 节点，则 09f3-1 化为二进制 0000 1001 1111 0011，加上二进制数 100000 后，再左移 6 位得到该节点号十六进制数首地址 0x2840h。

5.作超级用户登录，把文件块号及有关信息填入 i 节点区内，重构文件 i 节点。

```
# adb -w / dev / root
* 305c0? w81a4 0001 0000 0000 1000 0000 8d03 0401 018d 8d05 0601 018d8d07 0801 018d 8d09 0a01 018d
```

其中 81a4 是文件 mode 字 100644 表示属性为 -rw-r--r--，0001 为链接数，0000 表示文件属主是 root，下一 0000 表示文件与 root 有同一组号，1000 0000 表示文件长度是 4096 字节(8x512 bytes)，后接文件占用块号。

6.用 fsck 命令检查文件系统(/ dev / root)，遇到询问一律打"Y"通过。

```
# fsck / dev / root
* * Phase 1——Check Block and Sizes
* * Phase 2——Check Pathnames
* * Phase 3——Check Connectivity
* * Phase 4——Check Reference counts
UNREF FILEI = 3069OWNER = rootMODE = 100644
SIZE = 4096 MTIME = AUG 31 08:12 1993 ———— REMOVED
Reconnect? < Y >
FREE INODE COUNT WRONG IN SUPERBLK
Fix? < Y >
* * Phase 5 —— Check Freelist
8 BLK(S) MISSING
BAD FREELIST
SALVAGE? < Y >
* * Phase 6 —— Salvage Free List
5700files 109172 Blocks 198096 Free
* * * * * FILESYSTEM WAS MODIFIED * * * * *
* * * * * REMOUNTING THE ROOT FILESYSTEM * * * * *
```

7.维护完文件系统后，恢复的文件以节点号命名存在目录文件 lost+found 内，检查此文件，将文件尾多余的信息删除，更名后移到适当目录下。

注意：在恢复文件的系统内，必须有一个名为 lost+found 目录，不然恢复的文件没有确定的存放地点而不得恢复。

参考文献：

[1]孙玉方主编《实用 UNIX 系统使用与管理》

[2]孙玉方主编《UNIX 系统工具与使用》

[3]董承章编著《Xenix 培训教程》

[4]《Greatwall Xenix V 系统命令用户手册》