

# XFS: Bit-by-Bit

Hal Pomeranz

# Who the heck uses XFS?

- NAS Appliances
- Every new Red Hat Linux system

# XFS Forensic Tools

- X-Ways?
- ...

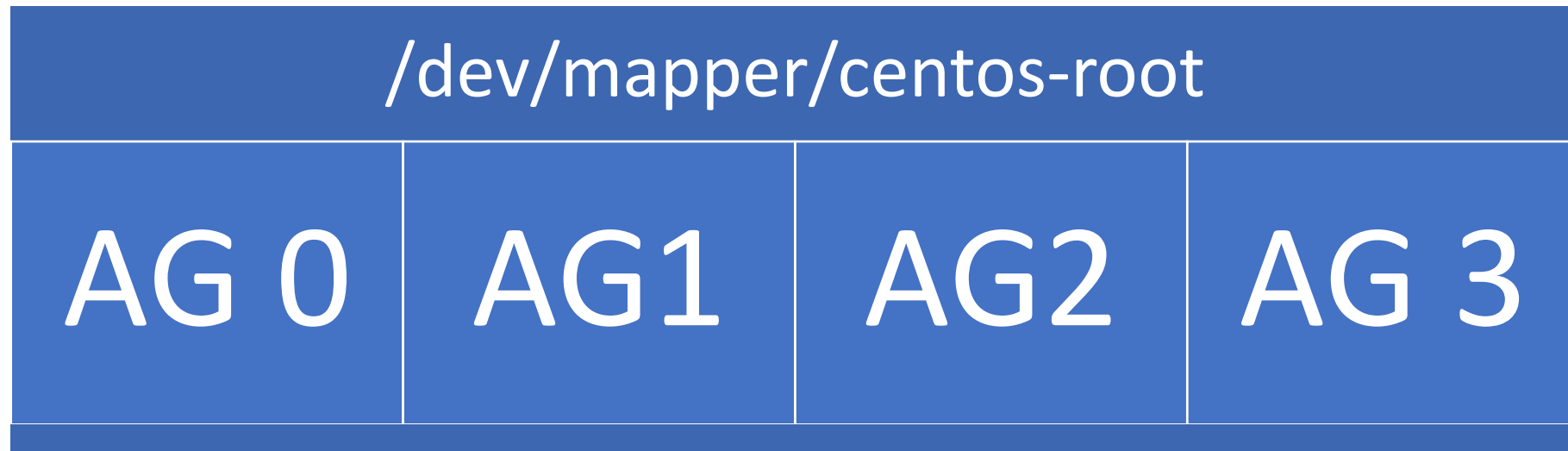
# Quick Overview of XFS

- 64-bit, journaled file system
- File extents, B+Tree directories
- MACB timestamps, Unix epoch format w/ nsec field
- Arbitrary extended attributes
- All metadata structures:
  - Start with unique magic numbers
  - Store file system UUID, inode data
  - Have CRC32 checksums
  - Use big-endian data throughout



# What's Different About XFS?

- Each file system is several *Allocation Groups (AGs)*
- Each AG can be written independently
- Allows parallel writes for higher throughput



# Block and Inode Addressing

- Addresses are packed structures:
  - AG number in the upper bits
  - AG relative offset in the lower bits
- Field lengths are *variable*, based on AG size

AG Num

AG Relative Address

$\text{ceil}(\log_2(\text{blocks per AG}))$

# Block Addressing

40GB file system / 4 AGs / 2,427,136 blocks per AG

$\log_2(2427136) = 21.21$  round up to 22 bits

Block 8388612  
(0x800004)

10 00 0000 0000 0000 0000 0100

AG 2, Block 4

$$\text{Physical Offset} = \underset{2}{(\text{AG number})} * \underset{2427136}{(\text{blocks per AG})} + \underset{4}{(\text{relative block})} = 4854276$$

# Inode Addressing

You can put eight 512 byte inodes in a 4K block

We need an extra three bits for relative inode addresses (25 bits total)

Inode 67761631  
(0x409F5DF)

010 0 0000 1001 1111 0101 1101 1111

AG 2, Inode 0x9F5DF (652767)

Block location = (relative inode#) div (inodes per block) = 652767 div 8 = 81595

Offset in block = (relative inode#) mod (inodes per block) = 652767 mod 8 = 7

xfs\_db to the rescue!

(typical file)

# Data Fork

## Extended Attributes

|       |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |                    |
|-------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|--------------------|
| 0x00) | 49 | 4E | 81 | A4 | 03 | 02 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | IN.α.....          |
| 0x01) | 00 | 00 | 00 | 01 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | .....              |
| 0x02) | 5A | FD | D6 | CD | 24 | 67 | 33 | 0E | 5A | FD | D6 | CD | 24 | 76 | 75 | 68 | zýöí\$g3.zýöí\$vuh |
| 0x03) | 5A | FD | D6 | CD | 24 | 76 | 75 | 68 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 15 | zýöí\$vuh.....     |
| 0x04) | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 01 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 01 | .....              |
| 0x05) | 00 | 00 | 23 | 01 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | A3 | FD | 42 | CD | ...#.....fýBí      |
| 0x06) | FF | FF | FF | FF | B4 | 3F | 0D | 10 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 01 | ýýýý´? .....       |
| 0x07) | 00 | 00 | 00 | 21 | 00 | 00 | 61 | 85 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | ...!..a.....       |
| 0x08) | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | .....              |
| 0x09) | 5A | FD | D6 | CD | 24 | 67 | 33 | 0E | 00 | 00 | 00 | 00 | 06 | 02 | 14 | E7 | zýöí\$g3.....ç     |
| 0x0A) | F5 | 6C | 3B | 41 | CA | 03 | 4B | 41 | B1 | 5C | DD | 60 | 9C | B7 | DA | 71 | ãl;AÊ.KA±\Ý`..Úq   |
| 0x0B) | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 01 | .....              |
| 0x0C) | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | .....              |
| 0x0D) | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | .....              |
| 0x0E) | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | .....              |
| 0x0F) | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | .....              |
| 0x10) | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | .....              |
| 0x11) | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | .....              |
| 0x12) | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | .....              |
| 0x13) | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | .....              |
| 0x14) | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | .....              |
| 0x15) | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | .....              |
| 0x16) | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | .....              |
| 0x17) | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | .....              |
| 0x18) | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | .....              |
| 0x19) | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | .....              |
| 0x1A) | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | .....              |
| 0x1B) | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | .....              |
| 0x1C) | 00 | 3C | 01 | 00 | 07 | 2E | 04 | 73 | 00 | 34 | 01 | 00 | 07 | 2E | 04 | 73 | .<.....s.4...&.s   |
| 0x1D) | 65 | 6C | 69 | 6E | 75 | 78 | 75 | 6E | 63 | 6F | 6E | 66 | 69 | 6E | 65 | 64 | elinuxunconfined   |
| 0x1E) | 5F | 75 | 3A | 6F | 62 | 6A | 65 | 63 | 74 | 5F | 72 | 3A | 61 | 64 | 6D | 69 | _u:object_r:admi   |
| 0x1F) | 6E | 5F | 68 | 6F | 6D | 65 | 5F | 74 | 3A | 73 | 30 | 00 | 3A | 73 | 30 | 00 | n_home_t:s0.:s0.   |

# XFS Extents – Not Byte Aligned (sigh)

0x0B0 00 00 00 00 00 00 00 00 00 00 18 08 0F 20 00 01

00000b0: 00000000 00000000 00000000 00000000 ....  
00000b4: 00000000 00000000 00000000 00000000 ....  
00000b8: 00000000 00000000 00011000 00001000 ....  
00000bc: 00001111 00100000 00000000 00000001 . ..

**Flag bit (1 bit):** 0

**Logical offset (54 bits):** 0

**Absolute start block (52 bits):**

0 00000000 00000000 00000000 00011000 00001000 00001111 001  
0000 0000 0000 0000 0000 0000 0000 1100 0000 0100 0000 0111 1001  
0 0 0 0 0 0 0 C 0 4 0 7 9

block 0xC04079 aka relative block 0x4079 (16505) in AG 3

**block count (21 bits):** 1

(small directory)

|       |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
|-------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| 0x000 | 49 | 4E | 41 | ED | 03 | 01 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| 0x010 | 00 | 00 | 00 | 02 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| 0x020 | 5A | EF | 84 | 6C | 11 | 16 | 6A | BB | 5A | EF | 84 | 67 | 03 | 38 | E8 | 90 |
| 0x030 | 5A | EF | 84 | 67 | 03 | 38 | E8 | 90 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 66 |
| 0x040 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| 0x050 | 00 | 00 | 23 | 01 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 5A | 52 | 79 | A1 |
| 0x060 | FF | FF | FF | FF | 27 | FA | 73 | 4A | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 01 |
| 0x070 | 00 | 00 | 00 | 20 | 00 | 00 | 7F | FC | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| 0x080 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| 0x090 | 5A | EF | 84 | 47 | 13 | FF | 46 | D3 | 00 | 00 | 00 | 00 | 04 | 08 | E5 | 96 |
| 0x0A0 | 55 | 6C | 3B | 41 | CA | 03 | 4B | 41 | B1 | 5C | DB | 60 | 9C | B7 | DA | 71 |
| 0x0B0 | 05 | 00 | 04 | 15 | 9F | A1 | 0C | 00 | 60 | 30 | 31 | 5F | 73 | 6D | 61 | 6C |
| 0x0C0 | 6C | 66 | 69 | 6C | 65 | 01 | 04 | 17 | 97 | 9D | 0A | 00 | 78 | 30 | 32 | 5F |
| 0x0D0 | 62 | 69 | 67 | 66 | 69 | 6C | 65 | 01 | 04 | 17 | 97 | 9E | 0C | 00 | 90 | 30 |
| 0x0E0 | 33 | 5F | 73 | 6D | 61 | 6C | 6C | 66 | 69 | 6C | 65 | 01 | 04 | 17 | 97 | 9F |
| 0x0F0 | 0A | 00 | A8 | 30 | 34 | 5F | 62 | 69 | 67 | 66 | 69 | 6C | 65 | 01 | 04 | 17 |
| 0x100 | A1 | 54 | 0C | 00 | C0 | 30 | 35 | 5F | 73 | 6D | 61 | 6C | 6C | 66 | 69 | 6C |
| 0x110 | 65 | 01 | 04 | 17 | A1 | 55 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| 0x120 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| 0x130 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| 0x140 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| 0x150 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| 0x160 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| 0x170 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| 0x180 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| 0x190 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| 0x1A0 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| 0x1B0 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| 0x1C0 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 34 | 01 | 00 | 07 | 26 | 04 | 73 |
| 0x1D0 | 65 | 6C | 69 | 6E | 75 | 78 | 75 | 6E | 63 | 6F | 6E | 66 | 69 | 6E | 65 | 64 |
| 0x1E0 | 5F | 75 | 3A | 6F | 62 | 6A | 65 | 63 | 74 | 5F | 72 | 3A | 61 | 64 | 6D | 69 |
| 0x1F0 | 6E | 5F | 68 | 6F | 6D | 65 | 5F | 74 | 3A | 73 | 30 | 00 | 00 | 73 | 30 | 00 |



# Block Directories

- More typically directories are stored as block extents
- Directory blocks contain:
  - Header
  - Directory entries
  - Hash lookup table by filename

# Block Directory

Header and Entries

Magic Number

Free Space Array

File System UUID

Directory Entries

Index

|        |                         |                         |                         |
|--------|-------------------------|-------------------------|-------------------------|
| 0x0000 | 58 44 42 33             | AF 6A 41 6D             | 00 00 00 00 02 59 57 38 |
| 0x0010 | 00 00 00 20 00 00 61 FE | E5 6C 3B 41 CA 03 4B 41 |                         |
| 0x0020 | B1 5C DD 60 9C B7 DA 71 | 00 00 00 00 04 08 E6 6D |                         |
| 0x0030 | 00 00 00 00 00 00 00 00 | 00 00 00 00 00 00 00 00 |                         |
| 0x0040 | 00 00 00 00 04 15 9F A1 | 02 2E 2E 02 00 00 00 40 |                         |
| 0x0050 | 00 00 00 00 04 15 9F A1 | 02 2E 2E 02 00 00 00 50 |                         |
| 0x0060 | 00 00 00 00 04 17 97 6B | 0C 30 31 5F 73 6D 61 6C |                         |
| 0x0070 | 6C 66 69 6C 65 01 00 60 | 00 00 00 00 04 17 97 6C |                         |
| 0x0080 | 0A 30 32 5F 62 69 67 66 | 69 6C 65 01 00 00 00 78 |                         |
| 0x0090 | 00 00 00 00 04 17 97 6D | 0C 30 33 5F 73 6D 61 6C |                         |
| 0x00A0 | 6C 66 69 6C 65 01 00 90 | 00 00 00 00 04 17 97 6E |                         |
| 0x00B0 | 0A 30 34 5F 62 69 67 66 | 69 6C 65 01 00 00 00 A8 |                         |
| 0x00C0 | 00 00 00 00 04 17 97 6F | 0C 30 35 5F 73 6D 61 6C |                         |
| 0x00D0 | 6C 66 69 6C 65 01 00 C0 | 00 00 00 00 04 17 97 70 |                         |
| 0x00E0 | 0A 30 36 5F 62 69 67 66 | 69 6C 65 01 00 00 00 D8 |                         |
| 0x00F0 | 00 00 00 00 04 17 97 71 | 0C 30 37 5F 73 6D 61 6C |                         |
| 0x0100 | 6C 66 69 6C 65 01 00 F0 | 00 00 00 00 04 17 97 72 |                         |
| 0x0110 | 0A 30 38 5F 62 69 67 66 | 69 6C 65 01 00 00 01 08 |                         |
| 0x0120 | 00 00 00 00 04 17 97 73 | 0C 30 39 5F 73 6D 61 6C |                         |
| 0x0130 | 6C 66 69 6C 65 01 01 20 | 00 00 00 00 04 17 97 74 |                         |
| 0x0140 | 0A 31 30 5F 62 69 67 66 | 69 6C 65 01 00 00 01 38 |                         |
| 0x0150 | 00 00 00 00 04 17 97 75 | 0C 31 31 5F 73 6D 61 6C |                         |
| 0x0160 | 6C 66 69 6C 65 01 01 50 | 00 00 00 00 04 17 97 76 |                         |
| 0x0170 | 0A 31 32 5F 62 69 67 66 | 69 6C 65 01 00 00 01 68 |                         |
| 0x0180 | 00 00 00 00 04 17 97 77 | 0C 31 33 5F 73 6D 61 6C |                         |
| 0x0190 | 6C 66 69 6C 65 01 01 80 | 00 00 00 00 04 17 97 78 |                         |
| 0x01A0 | 0A 31 34 5F 62 69 67 66 | 69 6C 65 01 00 00 01 98 |                         |

XDB3-jAm....YW8  
... ..apål;AÊ.KA  
±\Y`..Úq.....æm  
.. H.....  
.....æm....@  
.....j.....P  
.....k 01\_small  
lfile..`.....l  
02\_bigfile....x  
.....m 03\_small  
lfile.....n  
04\_bigfile....  
.....o 05\_small  
lfile..À.....p  
06\_bigfile....ø  
.....q 07\_small  
lfile..ð.....r  
08\_bigfile.....  
.....s 09\_small  
lfile.. ..t  
10\_bigfile....8  
.....u 11\_small  
lfile..P.....v  
12\_bigfile....h  
.....w 13\_small  
lfile.....x  
14\_bigfile.....

# Block Directory

Tail Record/Hash Lookup Table

|        |                         |                         |                     |
|--------|-------------------------|-------------------------|---------------------|
| 0x0E50 | 00 00 00 00 00 00 05 10 | 00 00 00 2E 00 00 00 08 | .....               |
| 0x0E60 | 00 00 17 2E 00 00 00 0A | 3F 07 7C 6C 00 00 00 90 | ..... ?. 1....      |
| 0x0E70 | 3F 07 7C EC 00 00 00 96 | 3F 07 7D 6C 00 00 00 84 | ?. ì....?.}1....    |
| 0x0E80 | 3F 07 7D EC 00 00 00 8A | 3F 07 7F 6C 00 00 00 9C | ?. ì....?.}1....    |
| 0x0E90 | 3F 07 9C 6C 00 00 00 72 | 3F 07 9C EC 00 00 00 78 | ?..l....r?...ì...x  |
| 0x0EA0 | 3F 07 9D 6C 00 00 00 66 | 3F 07 9D EC 00 00 00 6C | ?..l....f?...ì...l  |
| 0x0EB0 | 3F 07 9F 6C 00 00 00 7E | 3F 07 BC 6C 00 00 00 54 | ?..l....~?..¼l...T  |
| 0x0EC0 | 3F 07 BC EC 00 00 00 5A | 3F 07 BD 6C 00 00 00 48 | ?..¼ì....Z?..½l...H |
| 0x0ED0 | 3F 07 BD EC 00 00 00 4E | 3F 07 BF 6C 00 00 00 60 | ?..½ì....N?..¿l...` |
| 0x0EE0 | 3F 07 DC 6C 00 00 00 36 | 3F 07 DC EC 00 00 00 3C | ?..Ül...6?..Üì...<  |
| 0x0EF0 | 3F 07 DD 6C 00 00 00 2A | 3F 07 DD EC 00 00 00 30 | ?..Ýl...*?..Ýì...0  |
| 0x0F00 | 3F 07 DF 6C 00 00 00 42 | 3F 07 FC 6C 00 00 00 18 | ?..ßl...B?..üì....  |
| 0x0F10 | 3F 07 FC EC 00 00 00 1E | 3F 07 FD 6C 00 00 00 0C | ?..üì.... ?..ýl...  |
| 0x0F20 | 3F 07 FD EC 00 00 00 12 | 3F 07 FF 6C 00 00 00 24 | ?..ýì....?..ÿl...\$ |
| 0x0F30 | 44 65 FD 31 00 00 00 99 | 44 65 FD 32 00 00 00 5D | Deý1....Deý2...]    |
| 0x0F40 | 44 65 FD 33 00 00 00 21 | 48 65 FD 31 00 00 00 8D | Deý3....!Heý1....   |
| 0x0F50 | 48 65 FD 32 00 00 00 51 | 48 65 FD 33 00 00 00 15 | Heý2....QHeý3....   |
| 0x0F60 | 4A 65 FD 31 00 00 00 93 | 4A 65 FD 32 00 00 00 57 | Jeý1....Jeý2...W    |
| 0x0F70 | 4A 65 FD 33 00 00 00 1B | 4C 65 FD 31 00 00 00 81 | Jeý3....Leý1....    |
| 0x0F80 | 4C 65 FD 32 00 00 00 45 | 4E 65 FD 31 00 00 00 87 | Leý2....ENeý1....   |
| 0x0F90 | 4E 65 FD 32 00 00 00 4B | 4E 65 FD 33 00 00 00 0F | Neý2....KNeý3....   |
| 0x0FA0 | C4 65 FD 32 00 00 00 7B | C4 65 FD 33 00 00 00 3F | Äeý2....{Äeý3...?   |
| 0x0FB0 | C8 65 FD 32 00 00 00 6F | C8 65 FD 33 00 00 00 33 | Èeý2....oÈeý3...3   |
| 0x0FC0 | CA 65 FD 32 00 00 00 75 | CA 65 FD 33 00 00 00 39 | Êeý2....uÊeý3...9   |
| 0x0FD0 | CC 65 FD 31 00 00 00 9F | CC 65 FD 32 00 00 00 63 | Ïeý1....Ïeý2...c    |
| 0x0FE0 | CC 65 FD 33 00 00 00 27 | CE 65 FD 32 00 00 00 69 | Ïeý3... 'Ïeý2...i   |
| 0x0FF0 | CE 65 FD 33 00 00 00 2D | 00 00 00 34 00 00 00 00 | ïeý3...-...4....    |

# What Remains After Deletion?

- Directory
  - Entry becomes free space
  - Inode data partially overwritten, but still readable
- Inode
  - mtime and ctime update
  - File size, num links, num extents, file type/perms zeroed
  - Extent data and extended attributes preserved



# Block Directory

One File Deleted (Tail)

Offset zeroed

Now one free entry

|        |                         |                         |                     |
|--------|-------------------------|-------------------------|---------------------|
| 0x0E50 | 00 00 00 00 00 00 05 10 | 00 00 00 2E 00 00 00 08 | .....               |
| 0x0E60 | 00 00 17 2E 00 00 00 0A | 3F 07 7C 6C 00 00 00 90 | ..... ?. 1....      |
| 0x0E70 | 3F 07 7C EC 00 00 00 96 | 3F 07 7D 6C 00 00 00 84 | ?. i....?.}1....    |
| 0x0E80 | 3F 07 7D EC 00 00 00 8A | 3F 07 7F 6C 00 00 00 9C | ?. i....?..1....    |
| 0x0E90 | 3F 07 9C 6C 00 00 00 72 | 3F 07 9C EC 00 00 00 78 | ?..1....r?..i...x   |
| 0x0EA0 | 3F 07 9D 6C 00 00 00 66 | 3F 07 9D EC 00 00 00 6C | ?..1....f?..i...l   |
| 0x0EB0 | 3F 07 9F 6C 00 00 00 7E | 3F 07 BC 6C 00 00 00 54 | ?..1....~?.%1...T   |
| 0x0EC0 | 3F 07 BC EC 00 00 00 5A | 3F 07 BD 6C 00 00 00 48 | ?.%i...Z?.%1...H    |
| 0x0ED0 | 3F 07 BD EC 00 00 00 4E | 3F 07 BF 6C 00 00 00 60 | ?.%i...N?.%1...`    |
| 0x0EE0 | 3F 07 DC 6C 00 00 00 36 | 3F 07 DC EC 00 00 00 3C | ?..1....6?..i...<   |
| 0x0EF0 | 3F 07 DD 6C 00 00 00 2A | 3F 07 DD EC 00 00 00 30 | ?..1....*?..i...0   |
| 0x0F00 | 3F 07 DF 6C 00 00 00 42 | 3F 07 FC 6C 00 00 00 18 | ?..1....B?..i....   |
| 0x0F10 | 3F 07 EC EC 00 00 00 1E | 3F 07 FD 6C 00 00 00 0C | ?..i... ?..y1...    |
| 0x0F20 | 3F 07 FD EC 00 00 00 00 | 3F 07 FF 6C 00 00 00 24 | ?..y1....?..y1...\$ |
| 0x0F30 | 44 65 FD 31 00 00 00 99 | 44 65 FD 32 00 00 00 5D | Deý1....Deý2...]    |
| 0x0F40 | 44 65 FD 33 00 00 00 21 | 48 65 FD 31 00 00 00 8D | Deý3....!Heý1....   |
| 0x0F50 | 48 65 FD 32 00 00 00 51 | 48 65 FD 33 00 00 00 15 | Heý2....QHeý3....   |
| 0x0F60 | 4A 65 FD 31 00 00 00 93 | 4A 65 FD 32 00 00 00 57 | Jeý1....Jeý2...w    |
| 0x0F70 | 4A 65 FD 33 00 00 00 1B | 4C 65 FD 31 00 00 00 81 | Jeý3....Leý1....    |
| 0x0F80 | 4C 65 FD 32 00 00 00 45 | 4E 65 FD 31 00 00 00 87 | Leý2...ENeý1....    |
| 0x0F90 | 4E 65 FD 32 00 00 00 4B | 4E 65 FD 33 00 00 00 0F | Neý2...KNeý3....    |
| 0x0FA0 | C4 65 FD 32 00 00 00 7B | C4 65 FD 33 00 00 00 3F | Äeý2...{Äeý3...?    |
| 0x0FB0 | C8 65 FD 32 00 00 00 6F | C8 65 FD 33 00 00 00 33 | Èeý2...oÈeý3...3    |
| 0x0FC0 | CA 65 FD 32 00 00 00 75 | CA 65 FD 33 00 00 00 39 | Êeý2...uÊeý3...9    |
| 0x0FD0 | CC 65 FD 31 00 00 00 9F | CC 65 FD 32 00 00 00 63 | Ïeý1....Ïeý2...c    |
| 0x0FE0 | CC 65 FD 33 00 00 00 27 | CE 65 FD 32 00 00 00 69 | Ïeý3... 'Ïeý2...i   |
| 0x0FF0 | CE 65 FD 33 00 00 00 25 | 00 00 00 34 00 00 00 01 | Ïeý3...-...4....    |

# Block Directory

One File Deleted (Header)

Second entry added to  
free space array

|        |                         |                         |                  |
|--------|-------------------------|-------------------------|------------------|
| 0x0000 | 58 44 42 33 DA 98 6C F3 | 00 00 00 00 02 59 57 38 | XDB3Ú.1ó.....YW8 |
| 0x0010 | 00 00 00 20 00 00 78 5F | E5 6C 3B 41 CA 03 4B 41 | ... ..x_ăl;AÊ.KA |
| 0x0020 | B1 5C DD 60 9C B7 DA 71 | 00 00 00 00 04 08 E6 6D | ±\Ý`..Úq.....æm  |
| 0x0030 | 05 10 09 48 00 90 00 18 | 00 00 00 00 00 00 00 00 | .. H.....        |
| 0x0040 | 00 00 00 00 04 08 E6 6D | 01 2E 02 00 00 00 00 40 | .....æm.....@    |
| 0x0050 | 00 00 00 00 04 15 9F A1 | 02 2E 2E 02 00 00 00 50 | .....j.....P     |
| 0x0060 | 00 00 00 00 04 17 97 6B | 0C 30 31 5F 73 6D 61 6C | .....k 01_sma1   |
| 0x0070 | 6C 66 69 6C 65 01 00 60 | 00 00 00 00 04 17 97 6C | 1file..`.....1   |
| 0x0080 | 0A 30 32 5F 62 69 67 66 | 69 6C 65 01 00 00 00 78 | 02_bigfile....x  |
| 0x0090 | FF FF 00 18 04 17 97 6D | 0C 30 33 5F 73 6D 61 6C | ÿÿ.....m 03_sma1 |
| 0x00A0 | 6C 66 69 6C 65 01 00 90 | 00 00 00 00 04 17 97 6E | 1file.....n      |
| 0x00B0 | 0A 30 34 5F 62 69 67 66 | 69 6C 65 01 00 00 00 A8 | 04_bigfile....   |

Inode addr overwritten with 0xFFFF and entry length

There's Lots More!

<https://righteousit.wordpress.com/tag/xf/>

Hal Pomeranz

[hal@sans.org](mailto:hal@sans.org)

[@hal\\_pomeranz](#)

<http://deer-run.com/~hal/>