Linux Incident Response - EXT4 superblock basics

Taz Wake | Halkyn Consulting Ltd | Originally published 2024-02-15

Overview

In EXT4 filesystems, the *superblock* is a fundamental component that contains the metadata needed for the filesystem to function.

The metadata includes details such as the filesystem's size, its configuration parameters including block size and the total number of blocks, and inode allocation information.

Essentially, the superblock enables the operating system to efficiently navigate, access, and manage the filesystem, acting as the blueprint from which the entire filesystem's structure is comprehended and interacted with. It is similar to a master index in a vast library system, offering immediate access to the whereabouts and specifics of every file and directory housed within.

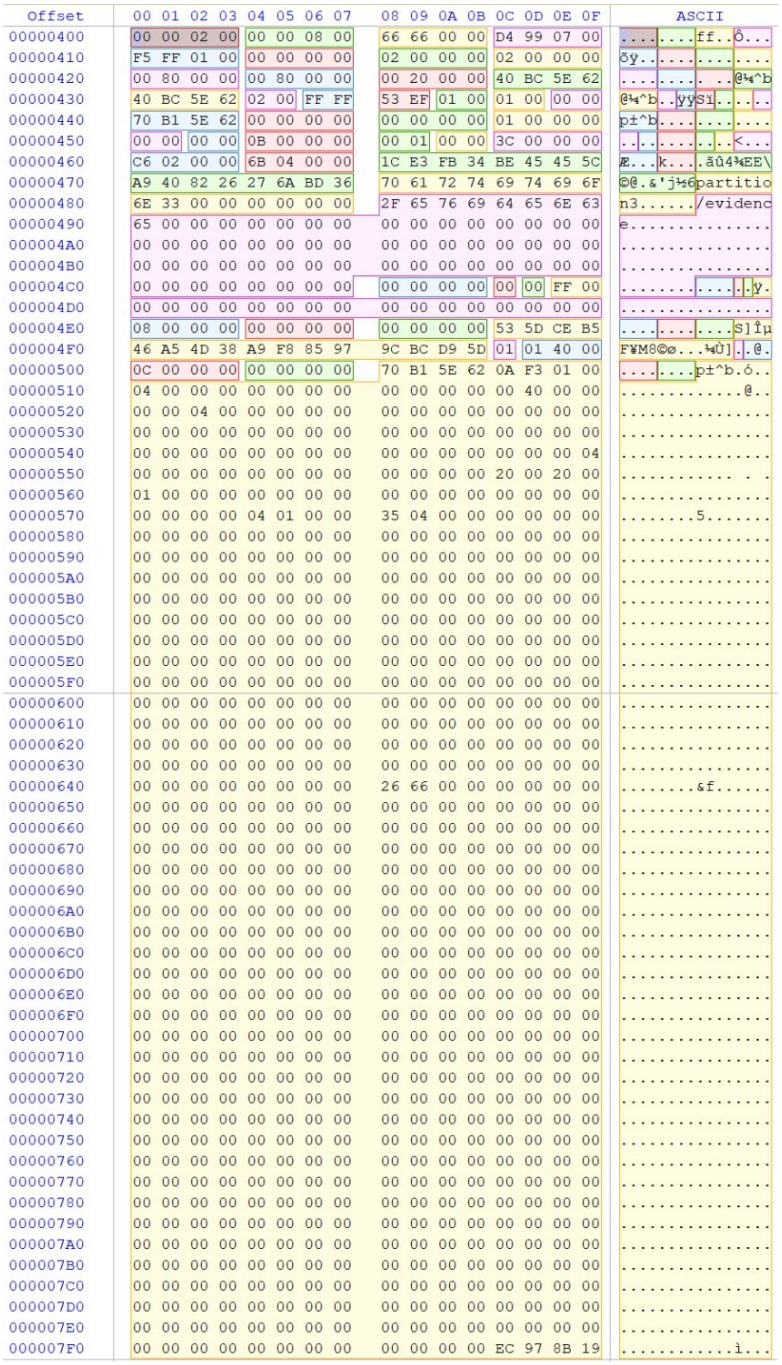
Location

The primary superblock is located at offset 0x400 (1024 bytes) into the filesystem.

In addition, because the superblock is so important to how the filesystem works, there are backup superblocks. In the early days, there was a backup copy in every block group, but this changed a long time ago. In EXT4, it does depend on how the filesystem is created, but the most common is to use the sparse_super parameter which will create backups in block groups 0, 1 and each block group that is a power of 3, 5 and 7.

Layout

The superblock is 1024 bytes long.



Offset	00 01 02 03 04 05 06 07	08 09 0A 0B 0C 0D 0E 0F	ASCII
00000400	00 00 02 00 00 00 08 00	66 66 00 00 D4 99 07 00	....ff..Ô...
00000410	F5 FF 01 00 00 00 00 00	02 00 00 00 02 00 00 00	õÿ..
00000420	00 80 00 00 00 80 00 00	00 20 00 00 40 BC 5E 62	.. @¼^b
00000430	40 BC 5E 62 02 00 FF FF	53 EF 01 00 01 00 00 00	@¼^b..ÿÿSï....
00000440	70 B1 5E 62 00 00 00 00	00 00 00 00 01 00 00 00	p±^b....
00000450	00 00 00 00 0B 00 00 00	00 01 00 00 3C 00 00 00	..<...
00000460	C6 02 00 00 6B 04 00 00	1C E3 FB 34 BE 45 45 5C	Æ...k...ãû4¾EE\
00000470	A9 40 82 26 27 6A BD 36	70 61 72 74 69 74 69 6F	©@.&'j½6partitio
00000480	6E 33 00 00 00 00 00 00	2F 65 76 69 64 65 6E 63	n3....../evidenc
00000490	65 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	e...
000004A0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	...
000004B0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	...
000004C0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 FF 00	....
000004D0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	...
000004E0	08 00 00 00 00 00 00 00	00 00 00 00 53 5D CE B5	....S]Îµ
000004F0	46 A5 4D 38 A9 F8 85 97	9C BC D9 5D 01 01 40 00	F¥M8©ø...¼Ù]..@.
00000500	0C 00 00 00 00 00 00 00	70 B1 5E 62 0A F3 01 00	....p±^b.ó..
00000510	04 00 00 00 00 00 00 00	00 00 00 00 00 40 00 00	.....@..
00000520	00 00 04 00 00 00 00 00	00 00 00 00 00 00 00 00	...
00000530	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	...
00000540	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 04	...
00000550	00 00 00 00 00 00 00 00	00 00 00 00 20 00 20 00	.... . .
00000560	01 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	...
00000570	00 00 00 00 04 01 00 00	35 04 00 00 00 00 00 00	....5...
00000580	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	...
00000590	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	...
000005A0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	...
000005B0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	...
000005C0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	...
000005D0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	...
000005E0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	...
000005F0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	...
00000600	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	...
00000610	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	...
00000620	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	...
00000630	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	...
00000640	00 00 00 00 00 00 00 00	26 66 00 00 00 00 00 00	....&f....
00000650	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	...
00000660	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	...
00000670	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	...
00000680	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	...
00000690	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	...
000006A0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	...
000006B0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	...
000006C0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	...
000006D0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	...
000006E0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	...
000006F0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	...
00000700	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	...
00000710	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	...
00000720	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	...
00000730	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	...
00000740	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	...
00000750	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	...
00000760	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	...
00000770	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	...
00000780	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	...
00000790	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	...
000007A0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	...
000007B0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	...
000007C0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	...
000007D0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	...
000007E0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	...
000007F0	00 00 00 00 00 00 00 00	00 00 00 00 EC 97 8B 19	....ì...

The EXT4 Superblock

Key elements

There are lots of interesting fields in a superblock, but for this article, I will highlight some of the ones we review most often during incident response.

Offset 0x00-0x04, Inodes Count. This is the total number of inodes (index nodes) available in the filesystem. This creates a hard limit to the maximum number of files that can exist.

Offset	00 01 02 03
00000400	00 00 02 00

inode count

In the example Superblock above, the inode count is shown as . This is in little endian, so the number is This converts into using decimal notation.

Offset 0x05-0x08, Blocks Count. This is the total number of blocks available to the filesystem. This gives you an idea of how much space on the physical disk the filesystem occupies. EXT4 typically uses 4kb blocks, but this can be validated at offset 0x18.

04 05 06 07
00 00 08 00

block count

In the example above, the block count is shown as (little endian hex) which is 524288 blocks. This calculation can be confirmed with tools like

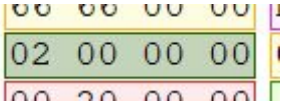
```
File System Type: Ext4
Volume Name: partition3
Volume ID: 36bd6a27268240a95c4545be34fbe31c

Last Written at: 2022-04-19 14:42:24 (BST)
Last Checked at: 2022-04-19 13:56:16 (BST)

Last Mounted at: 2022-04-19 14:42:24 (BST)
Unmounted properly
Last mounted on: /evidence

Source OS: Linux
Dynamic Structure
Compat Features: Journal, Ext Attributes, Resize Inode, Dir Index
InCompat Features: Filetype, Needs Recovery, Extents, 64bit, Flexible Block Groups,
Read Only Compat Features: Sparse Super, Large File, Huge File, Extra Inode Size

Journal ID: 00
Journal Inode: 8

METADATA INFORMATION
----------------------------------------
Inode Range: 1 - 131073
Root Directory: 2
Free Inodes: 131061
Inode Size: 256

CONTENT INFORMATION
----------------------------------------
Block Groups Per Flex Group: 16
Block Range: 0 - 524287
Block Size: 4096
Free Blocks: 498132

BLOCK GROUP INFORMATION
----------------------------------------
Number of Block Groups: 16
Inodes per group: 8192
Blocks per group: 32768
```

fsstat output - 16 block groups with 32768 blocks per group is a total of 524288 blocks

Offset 0x18-0x0B, Block Size. This records the size of the blocks. This isn't in a simple integer (why should anything be simple?), rather it is a value that is used to calculate the block size.

There are a few approaches you can use to determine the blocksize value in bytes:

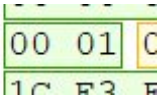
- Block size is *2 ^ (10 + [value])*
- Bitwise "left shift", *1024 << [value]*



Block size

In our example, the block size is (little endian), or , which converts to a block size of 4096 bytes (4kb blocks).

Offset 0x58-0x59, Inode Size. This records the size of the inodes, in bytes. This is a simple translation as it is stored in little endian.

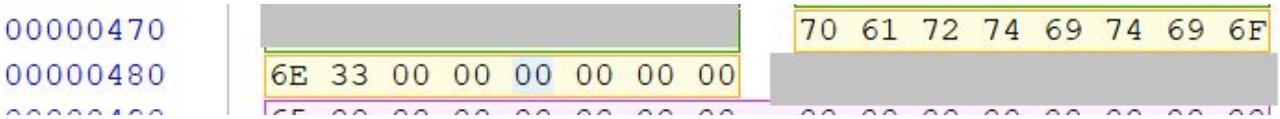


Inode size

In the example image, the inode size is (little endian) or which is 256 in decimal.

Offset 0x78-0x87, Volume Name. This is the volume label assigned to the files system. It is important for things like maintaining chain of custody and validating that you have the correct object.

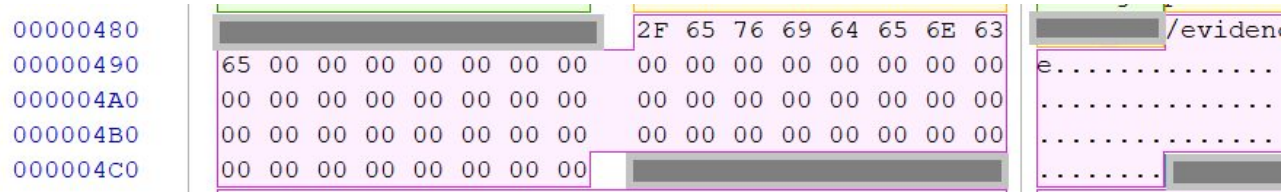
The contents are hex-encoded ASCII characters.



Volume name field

In the example evidence, the volume name is "Partition 3".

Offset 0x88-0xC7, Last Mount Point. The last field we will discuss here is the record of the last location where this filesystem was mounted. Again, this is a useful record of where the filesystem was last used and should be recorded in any evidence logs.



Last mount point

In the example used for this article, the filesystem was last mounted as somewhere.

Wrap up

This is a really quick look at a very few, basic, components of the EXT4 superblock. There is way more stuff than we can cover in this article but these are *some* of the areas we look at *most often* during DFIR.

It is important that any incident responders looking at a modern Linux system have an understanding of this, although it is worth noting that XFS has a very different structure.

Hopefully, you will simply use tools like TSK for most of your analysis but it is also good to be able to drop into the source and validate things. This also helps if you need to work in a constrained environment.

About Halkyn Consulting

Halkyn Consulting Ltd is a UK-based security and risk management consultancy providing 24/7 incident response, digital forensics, threat hunting, virtual security leadership (vCISO) and security compliance support to organisations worldwide. We deliver clear, practical, vendor-independent advice based on real-world threats — no hype, no upsell.

More free security resources are available at www.halkynconsulting.co.uk/security-resources.

Web: www.halkynconsulting.co.uk | **Email:** info@halkynconsulting.co.uk | **Tel:** +44 1244 940858