Kelompok gak tau brp

October 2, 2023

EXT4

A linux filesystem.

OUR TOPICS

1. What is EXT4?
2. EXT4 Topology
3. Creating & Deleting FIles
4. Forensic Implications

Kelompok gak tau brp

October 2, 2023

WHAT IS EXT4?

Let's begin.

EXT4

A journaling file system yang digunakan oleh linux.

What exactly is an Ext4?

EXT4 101:

- Singkatan dari Fourth Extended Filesystem
- Sebuah Linux based OS
- Bertujuan untuk mengatur penyimpanan data, hdd maupun ssd.
- Berperan sebagai struktur dalam menyimpan data (incl. Files, Dir, Metadata, dsb)

Kelompok gak tau brp

October 2, 2023

EXT4 VS NTFS

Differences.

EXT4 VS NTFS

What makes them different?

Differences:

- **Designated OS**
- **Fiturnya berbeda (EXT4 ada Unix file permission**
- **Max size EXT4 (16TB)**
- **NTFS Ada build-in file compression EXT4 tidak ada**

Kelompok gak tau brp

October 2, 2023

TOPOLOGY

Of Ext4

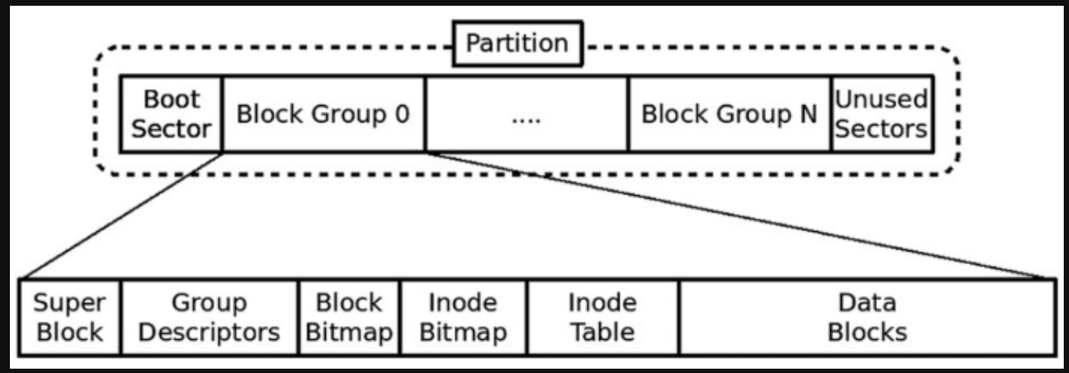
TOPOLOGY

• • •

Topology:

- Block Groups, EXT4 membagi penyimpanan kedalam storage group.
- Super Block, berisii essential information tentang file systemnya.
- Group Descriptors, berisi tentang informasi tambahan, seperti available free block, inodes.
- Block Bitmaps, track data block mana yang sedang digunakan dan yang mana yang free. Begitu juga alocating dan delocating data blocks.
- Inodes Bitmaps, Hampir sama dengan block bitmaps, tapi penggunaannya untuk inodes

Fig. 1. File system layout. Adapted from Bovet and Cesati (2005).



TOPOLOGY

• • •

Inodes:

- Inodes merupakan struktur data yang merepresentasikan file dan juga directory.
- Setiap node memiliki metadata, isinya bisa jadi permission, timestamps, dll
- Di kumpulin jadi inodes table.

Data blocks:

- Available storage space dibagi ke data blocks ini
- Biasanya 1 block store 4kb data
- Yang handle storing data

Fig. 2. Inode data block pointers. Adapted from Carrier (2005).

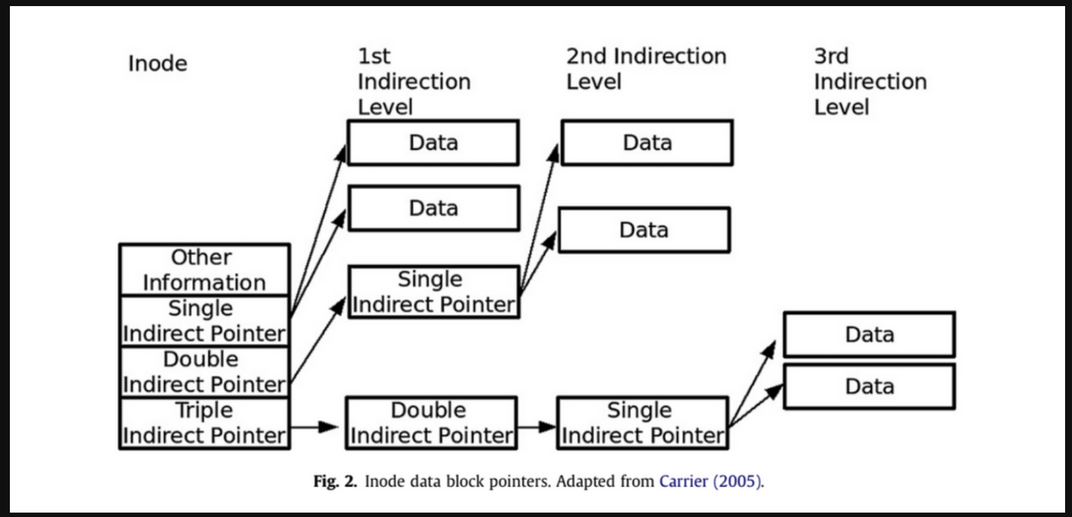


Fig. 2. Inode data block pointers. Adapted from Carrier (2005).

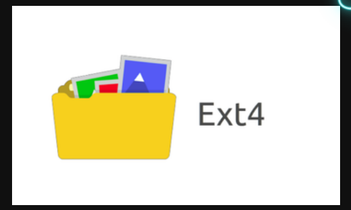
Kelompok gak tau brp

October 2, 2023

CREATING & DELETING FILES

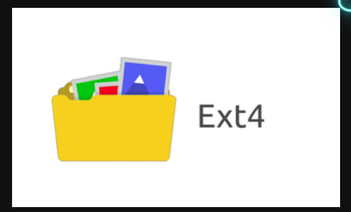
For Ext4

CREATING FILES



- Inode Allocation
- Metadata Initialization
- Data Block Allocation
- File Content Creation
- Updating Directory Entries

DELETING FILES



- Locating the Inode
- Inode Deallocation
- Data Block Deallocation
- Directory Entry Removal
- Journaling (optional)

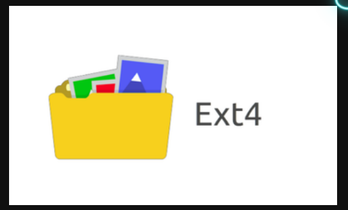
Kelompok gak tau brp

October 2, 2023

FORENSIC IMPLICATIONS

For Ext4

FORENSIC IMPLICATIONS



...

Deleted Files:

- The index node is not zeroed upon file deletion. it is possible to follow the extent tree all of the way to the actual file data

00042273	00	00	00	00	00	00	00	00	00	00	00	00	A4	81	00	00
00042284	00	E8	74	02	06	58	29	4F	27	58	29	4F	27	58	29	4F	00
00042295	00	00	00	00	00	01	00	42	3E	01	00	00	00	08	00	01	00
000422A6	00	00	0A	F3	01	00	04	00	03	00	00	00	00	00	00	00	00
000422B7	00	28	7C	00	00	00	00	00	00	90	1B	00	00	E8	68	00	00
000422C8	00	00	00	00	20	37	00	00	12	D7	00	00	00	00	00	00	B0
000422D9	52	00	00	74	65	01	00	00	00	00	00	85	3A	3A	8A	00	00
000422EA	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000422FB	00	00	00	00	00	A4	81	00	00	00	04	00	00	9E	57	29	4F

Fig. 13. Inode with extent index before deletion.

...

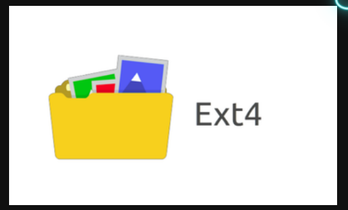
00042273	00	00	00	00	00	00	00	00	00	00	00	00	A4	81	00	00
00042284	00	00	00	00	CB	5A	29	4F	50	E5	3B	4F	50	E5	3B	4F	50
00042295	E5	3B	4F	00	00	00	00	00	00	00	00	00	00	08	00	01	00
000422A6	00	00	0A	F3	00	00	04	00	00	00	00	00	00	00	00	00	00
000422B7	00	28	7C	00	00	00	00	00	00	90	1B	00	00	E8	68	00	00
000422C8	00	00	00	00	20	37	00	00	12	D7	00	00	00	00	00	00	B0
000422D9	52	00	00	74	65	01	00	00	00	00	00	85	3A	3A	8A	00	00
000422EA	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000422FB	00	00	00	00	00	A4	81	00	00	00	04	00	00	9E	57	29	4F

Fig. 14. Inode with extent index after deletion.

01F09FE5	31	2D	36	39	36	37	30	2D	32	32	7C	66	69	6C	65	5F	36	1-69670-22|file_6
01F09FF6	39	36	37	30	2D	31	2D	36	39	36	0A	F3	06	00	54	00	02	9670-1-696....T..
01F0A007	00	00	00	00	00	00	00	00	00	3A	0C	00	00	00	00	00	00	.....:.....
01F0A018	90	1B	00	00	E8	68	00	00	00	00	00	00	20	37	00	00	12	.....h..... 7...
01F0A029	D7	00	00	00	00	00	00	B0	52	00	00	74	65	01	00	00	00	.....R..te.....
01F0A03A	00	00	40	6E	00	00	2A	7C	00	00	00	00	37	37	D0	89	00	..@n..*|....77...
01F0A04B	00	0E	9B	00	00	00	00	33	7C	66	69	6C	65	5F	33	35	37	.....3|file_357
01F0A05C	37	36	2D	30	2D	33	35	37	37	36	2D	34	7C	66	69	6C	65	76-0-35776-4|file
01F0A06D	5F	33	35	37	37	36	2D	30	2D	33	35	37	37	36	2D	35	7C	_35776-0-35776-5|

Fig. 15. Extent index node before deletion.

FORENSIC IMPLICATIONS



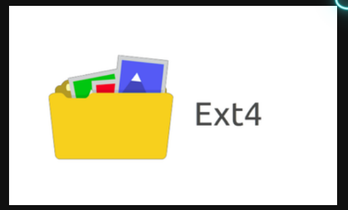
Metadata:

- Inode disimpan dalam tabel seperti pada ExtX
- Metadata tidak hanya disimpan dalam inode tapi dicampur dalam blok data normal
- Dalam proses klasifikasi, extent header bisa digunakan untuk identifikasi blok indeks dan letaknya dalam extent tree hierarchy

Data:

- Data file dan direktori terus disimpan dalam blok data seperti di ExtX
- Node Htree memiliki banyak ruang ekstra dan tidak banyak di dalamnya, seseorang dapat menggunakan ruang tersebut untuk menyembunyikan data tanpa menimbulkan masalah pada sistem komputer.
- Tempat-tempat potensial lain untuk menyembunyikan data termasuk blok pertumbuhan deskriptor grup dan struktur data dalam grup blok yang belum diinisialisasi. Setiap tempat penyembunyian potensial ini akan menampilkan tingkat volatilitas yang berbeda yang perlu diteliti lebih lanjut.

FORENSIC IMPLICATIONS



Journal:

- Journaling bisa membantu untuk memastikan integritas data saat kita sedang melakukan data forensic. Karena builtin system loggingnya.
- Tentu saja hal ini mengarah pada mengurangnya kemungkinan hilangnya data

REFERENCES

Our source of information <3

Reference!

- https://www.kernel.org/doc/html/v4.19/filesystems/ext4/ondisk/index.html#block-and-inode-bitmaps
- https://opensource.com/article/18/4/ext4-filesystem
- https://wiki.archlinux.org/title/ext4#:~:text=Ext4%20is%20the%20evolution%20of,to%20store%20the%20file%20data.
- https://medium.com/teknomuslim/penjelasan-file-system-extended-ext-di-linux-jenis-ext2-ext3-ext4-3181d79bb764
- https://newbinusmaya.binus.ac.id/lms/view-article/973e037c-5100-4d46-9ff7-385e06cf32c3/82887690-3a78-46c6-9297-d6cc7a4b2ebe/915882b8-2d7d-4b8f-8b7c-4dc72982ed07