

EXT File System Recovery

Hal Pomeranz, Deer Run Associates

Two Scenarios

“Cheese it! The cops!”

```
rm -rf /*
```

“Oh @&*%!”

```
dd if=/dev/zero of=/dev/sda
```

What Ain't You Got? Metadata!

Inodes overwritten or zeroed

Journal inode lost or journal overrun

Block & inode allocation maps clobbered

What's Left? Directory Contents!

/home/hal

127151	d	.
18350	d	..
127153	d	Downloads
127154	d	Desktop
127157	-	.profile
127160	d	.ssh
...		

/home

18530	d	.
2	d	..
...		
...		
127151	d	hal
...		
...		

What's Left? Directory Contents!

/home/hal

127151	d	.
18350	d	..
127153	d	Downloads
127154	d	Desktop
127157	-	.profile
127160	d	.ssh
...		

/home

18530	d	.
2	d	..
...		
...		
127151	d	hal
...		
...		

Wait a Minute!

Metadata is gone!

How do I locate directory files?

Directories have a signature ...

Directory File Signature

Directories always start with “.” and “..” entries

Directory entry:

- Inode number (4 bytes)
- Entry length (2 bytes, length is 4 byte aligned)
- File name length (1 byte)
- File type (1 byte)
- File name

Inode	E len	N len	Type	Filename
????????	0C00	01	02	2E000000
????????	????	02	02	2E2E0000...
...				

Complications

Large directories tend to fragment

Deleted entries

Multiple copies of directory data

Inode “churn”

Deleted Directory Entries

“rm -rf” happens...

$$4096 - 12 = 4084$$

04000A05	0C00	01	02	2E000000
01007604	0C00	02	02	2E2E0000
05000A05	0C00	04	01	44464952
06000A05	1000	06	01	53756D6D69740000
07000A05	0C00	03	01	666F7200
08000A05	0C00	03	01	74686500
08000A05	B40F	03	01	77696e00...

04000A05	0C00	01	02	2E000000
01007604	F40F	02	02	2E2E0000
05000A05	0C00	04	01	44464952
06000A05	2800	06	01	53756D6D69740000
07000A05	1800	03	01	666F7200
08000A05	0C00	03	01	74686500
08000A05	B40F	03	01	77696e00...

$$4096 - 76 = 4020$$

Block size Prev entries len

Inode “Churn”

12 blocks say that inode 390936 is `/tmp/systemd...NJU28X`

10 blocks say that inode 390936 is `/tmp/systemd...qYKD2F`

Which is the actual file name in the original file system?

HAHAHA! WRONG! The inode is unallocated!

More Info and Tools

<https://digital-forensics.sans.org/blog/tags/ext4>

<https://github.com/halpomeranz/analyzeEXT>

Hal Pomeranz

hal@sans.org

@hal_pomeranz