LINUX FORENSICS – MAGICAL MYSTERY TOUR

Hal Pomeranz

WHO IS HAL POMERANZ?

Started as a Unix Sys Admin in the 1980s

Independent consultant since 1997

Digital forensics, incident response, expert witness

Have done some interesting Linux/Unix investigations

hrpomeranz@gmail.com

@hal_pomeranz

LET'S TALK ABOUT EXT

Ext4 is the modern incarnation of a very old file system

Much of what you will see is inherited from 4.2 BSD's FFS

When the old and new worlds mix is when things get fun!

HAVING ATIME

Strict atime updates–

- Useful for DFIR
- Inefficient for file systems

Many file systems no longer update atime

Linux is weird…

RELATIVE ATIMES

Update atime on read if:

1. atime is more than 24 hours old ***OR***
2. atime is earlier than mtime or ctime

Result: atime now tends to indicate first use rather than last

DIRECTORIES

Ext4 directories are unsorted lists of records:

Inode number (4 bytes)
4-byte aligned entry length (2 bytes)
File name length (1 byte)
File type (1 byte)
File name

DELETING A FILE

Directory entry for deleted file *unchanged*

Previous directory entry "grows" to consume space

Result: See the file name and inode of deleted files!

THE BAD NEWS

Extent data is zeroed when files are deleted in Ext4

Knowing the inode of the deleted file doesn't help!

Or does it..?

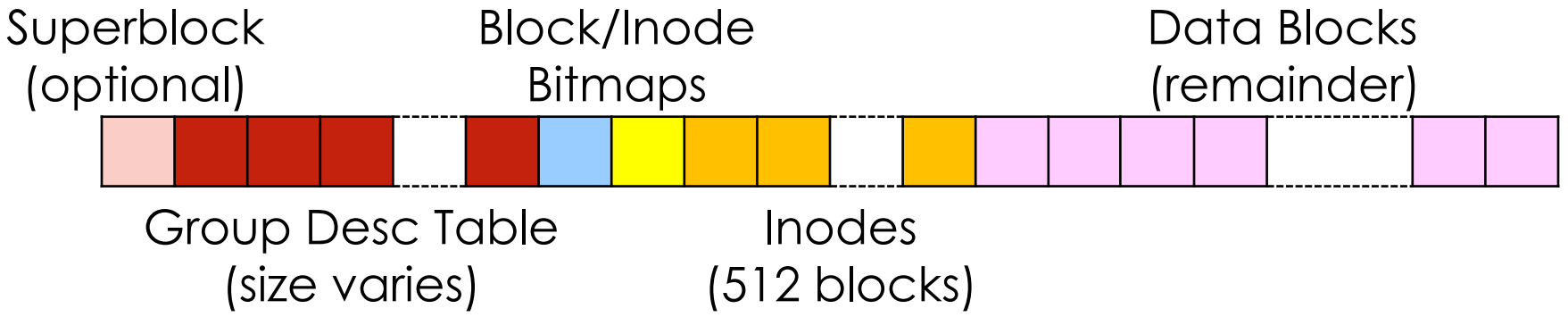
BLOCK GROUPS

Blocks are organized into *Block Groups* of 32K blocks

Each block group contains inodes and data blocks

Block and inode allocation bitmaps each occupy 1 block

May also contain backup superblock, etc



ALLOCATION STRATEGY

New directories are created in the least used block group

New files are added to same block group as directory

DELETED DATA

1. Use directory entry to determine inode of deleted file
2. Determine block group number from inode number
3. Search block group unallocated for deleted data
4. Profit?

THANK YOU!

Any final questions?
Thanks for listening!

hrpomeranz@gmail.com
@hal_pomeranz