XFS_DB FTW!

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@infosec.exchange

https://archive.org/details/HalLinuxForensics

ABOUT XFS

High-performance file system, originally created by SGI

Common in NAS appliances

Default file system for Red Hat distributions

Forensic tool support?

- X-Ways?
- Sleuthkit branch?

KEY FEATURES

Journaling file system

64-bit addressing

Inodes allocated as needed

Extent-based file allocation

MACB timestamps with nanosecond resolution

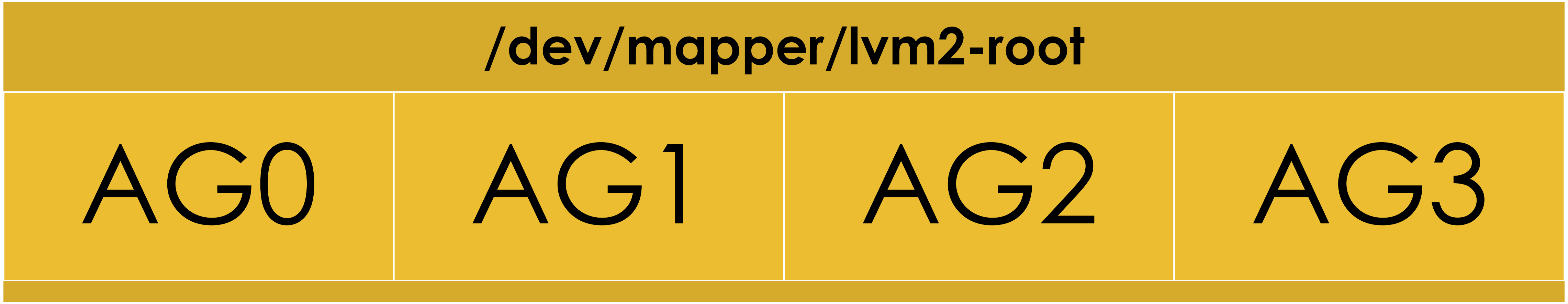
All file system data structures are big-endian

WHAT'S DIFFERENT ABOUT XFS?

Each file system made up of several *Allocation Groups (AGs)*

Each AG can be written independently

Allows parallel writes for faster throughput



/dev/mapper/lvm2-root

AG0

AG1

AG2

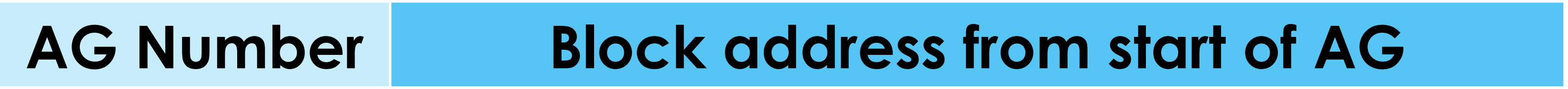
AG3

BLOCK AND INODE ADDRESSING

Addresses are packed structures

- Upper bits hold the AG number
- Lower bits are the AG relative block offset

Field lengths are *variable*, based on AG size in file system



LOOKING FOR TREASURE

Learn about XFS tools and addressing with a case study

Located a string of interest in a file system image

What file is this string found in?

Start by converting byte offset into sector offset

```
[lab@LAB ~]$ cd /images/All-Images/CentOS-XFS/
[lab@LAB CentOS-XFS]$ strings -a -t d centos-root.raw | gzip >strings.asc.gz
[lab@LAB CentOS-XFS]$ zgrep -Fi treasure strings.asc.gz
[… snip …]
9010062352                    Unit 1/2/3, 20/F, New Treasure Center
[… snip …]
[lab@LAB CentOS-XFS]$ expr 9010062352 / 512
17597778
```

XFS_DB CONVERTS ADDRESSES

```
[lab@LAB CentOS-XFS]$ xfs_db -r centos-root.raw
xfs_db> convert daddr 17597778 fsblock
0x3390aa (3379370)
xfs_db> convert fsblock 3379370 agno
0x3 (3)
xfs_db> convert fsblock 3379370 agblock
0x390aa (233642)
```

daddr	Sector offset
fsblock	Packed AG+block num
agno	AG number only
agblock	AG relative block num

XFS_DB CONTENT PREVIEW

```
xfs_db> daddr 17597778
xfs_db> type text
xfs_db> print
000:  6c 65 63 74 72 6f 6e 69 63 73 20 4c 74 64 2e 0a  lectronics.Ltd..
010:  09 09 09 09 55 6e 69 74 20 31 2f 32 2f 33 2c 20  ....Unit.1.2.3..
020:  32 30 2f 46 2c 20 4e 65 77 20 54 72 65 61 73 75  20.F..New.Treasu
030:  72 65 20 43 65 6e 74 65 72 0a 0a 09 09 09 09 48  re.Center......H
040:  4b 0a 0a 30 30 2d 31 41 2d 35 39 20 20 20 28 68  K..00.1A.59....h
[… snip …]
```

BLOCKGET/BLOCKUSE FTW!

```
xfs_db> blockget -n -s
xfs_db> fsblock 3379370
xfs_db> blockuse -n
block 3379370 (3/233642) type data inode 25629955 usr/share/hwdata/oui.txt
```

```
[root@LAB CentOS-XFS]# mkdir -p /mnt/xfs
[root@LAB CentOS-XFS]# mount -o ro,noexec,loop centos-root.raw /mnt/xfs
[root@LAB CentOS-XFS]# grep -F -C2 'New Treasure' /mnt/xfs/usr/share/hwdata/oui.txt
00-1A-54   (hex)                Hip Shing Electronics Ltd.
001A54     (base 16)            Hip Shing Electronics Ltd.
                                Unit 1/2/3, 20/F, New Treasure Center

                                HK
```

WHAT ABOUT DELETION?

Directory

- Entry marked as free space
- Inode field partially overwritten but still readable

Inode

- ctime updated to deletion time
- File size, num extents zeroed
- Extent data *not* overwritten

THANK YOU!

Any final questions?

Thanks for listening!

hrpomeranz@gmail.com

@hal_pomeranz@infosec.exchange

https://archive.org/details/HalLinuxForensics

Linux Forensics Live Online!
September 12-15

Linux Command Line
at WWHF Deadwood