Linux Forensics

Dr. Phil Polstra
PhD, CISSP, CEH

@ppolstra
http://philpolstra.com

Certifications:
http://www.securitytube-training.com

Pentester Academy: http://www.PentesterAcademy.com

Inodes

Inode Size

- Standard is 128 bytes for Ext2 and Ext3
- Ext4 currently uses 156 bytes
- Ext4 allocates 256 bytes on disk to allow for future expansion

Finding Inodes

- Block group =

  (Inode number -1) / (Inodes per group)

- Index within group =

  (Inode number -1) modulus (Inodes/group)

- Offset into inode table =

  index * (Inode size)

Inode Structure

Offset	Size	Name	DescriptionF
0x0	2	File Mode	File mode and type
0x2	2	UID	Lower 16 bits of owner ID
0x4	4	Size lo	Lower 32 bits of file size
0x8	4	Atime	Access time in seconds since epoch
0xC	4	Ctime	Change time in seconds since epoch
0x10	4	Mtime	Modify time in seconds since epoch
0x14	4	Dtime	Delete time in seconds since epoch
0x18	2	GID	Lower 16 bits of group ID
0x1A	2	Hlink count	Hard link count
0x1C	4	Blocks lo	Lower 32 bits of block count
0x20	4	Flags	Flags
0x24	4	Union osd1	Linux : l version

Inode Structure (cont)

Offset	Size	Name	Description
0x28	60	Block[15]	15 pointers to data blocks
0x64	4	Version	File version for NFS
0x68	4	File ACL low	Lower 32 bits of extended attributes (ACL, etc)
0x6C	4	File size hi	Upper 32 bits of file size (ext4 only)
0x70	4	Obsolete fragment	An obsoleted fragment address
0x74	**12**	**Osd 2**	**Second operating system dependent union**
0x74	2	Blocks hi	Upper 16 bits of block count
0x76	2	File ACL hi	Upper 16 bits of extended attributes (ACL, etc.)
0x78	2	UID hi	Upper 16 bits of owner ID
0x7A	2	GID hi	Upper 16 bits of group ID
0x7C	2	Checksum lo	Lower 16 bits of inode checksum

Inode Structure Extended (Ext4)

Offset	Size	Name	Description
0x80	2	Extra size	How many bytes beyond standard 128 are used
0x82	2	Checksum hi	Upper 16 bits of inode checksum
0x84	4	Ctime extra	Change time extra bits
0x88	4	Mtime extra	Modify time extra bits
0x8C	4	Atime extra	Access time extra bits
0x90	4	Crtime	File create time (seconds since epoch)
0x94	4	Crtime extra	File create time extra bits
0x98	4	Version hi	Upper 32 bits of version
0x9C		Unused	Reserved space for future expansions

Special Inodes

Inode	Special Purpose
0	No such inode, numberings starts at 1
1	Defective block list
2	Root directory
3	User quotas
4	Group quotas
5	Boot loader
6	Undelete directory
7	Reserved group descriptors (for resizing filesystem)
8	Journal
9	Exclude inode (for snapshots)
10	Replica inode
11	First non-reserved inode (often lost + found)

Examining Inodes