Linux Forensics

Dr. Phil Polstra
PhD, CISSP, CEH

@ppolstra
http://philpolstra.com

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

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

From Inodes to Files

What's in an inode block?

- Regular files & directories = direct & indirect blocks (sometimes)
- Symbolic links will be stored in inode block if target is less than 60 bytes long
- If in-line data flag is set the first 60 bytes of a file can be stored here
- Extent tree (ext4 only) listing data runs (contiguous blocks)

Direct and Indirect Blocks

- First 12 blocks point to data blocks (first 48k)
- Thirteenth block points to indirect block that contains pointers to blocks (1k * 4k = 4MB)
- Fourteenth block points to a double-indirect block that points to block containing block pointers (1k * 1k * 4k = 4GB)
- Fifteenth block points to a triple-indirect block that points to blocks containing double-indirect blocks (1k * 1k * 1k * 4k = 4TB)

Extents (ext4 only)

- Tree structure is used
- Three types of entries
  - Header
  - Index (middle node)
  - Extent (leaf node)

Extent Header (ext4 only)

Offset	Size	Name	Description
0x0	2	Magic	Magic number 0xF30A
0x2	2	Entries	Entries that follow the header
0x4	2	Max Entries	Maximum number of entries that might follow header
0x6	2	Depth	0=this node points to data blocks 1-5=this node points to other other extents
0x8	4	Generation	Generation of the tree

Extent Index (ext4 only)

Offset	Size	Name	Description
0x0	4	Block	This node covers block x and following
0x4	4	Leaf lo	Lower 32 bits of block containing the node (leaf or another index) one level lower in tree
0x8	2	Leaf hi	Upper 16 bits of the block described above
0xA	2	Unused	Padding to 12 byte size

Extent Node (ext4 only)

Offset	Size	Name	Description
0x0	4	Block	First block covered by this extent
0x4	2	Len	If <= 32768 initialized blocks in extent If > 32768 extents is (len-32768) uninit blocks
0x6	2	Start hi	Upper 16 bits of the starting block
0x8	4	Start lo	Lower 32 bits of the starting block

Examining Inodes