Linux Forensics

Dr. Phil Polstra
PhD, CISSP, CEH

@ppolstra
http://philpolstra.com

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

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

Filesystem Analysis: RO Compatible Features

Read-only Compatible Features

- Filesystem may be mounted read-only if these features are not supported
- The fsck utility should not be run against this filesystem

Why do we care about features?

- Affect the structure of block groups
- That in turn affects where data is located
- Affects how data is stored in inodes, etc.
- Some features might supply additional metadata for analysis

Read-only Compatible Features

Bit	Name	Description
0x1	Sparse Super	Sparse superblocks (only in BG 0 or power of 3, 5, or 7)
0x2	Large File	File(s) larger than 2GB exist on the filesystem
0x4	Btree Dir	Btrees are used in directories (not common)
0x8	Huge File	File sizes are represented in logical blocks, not sectors
0x10	Gdt Csum	Group descriptor tables have checksums
0x20	Dir Nlink	Subdirectories are not limited to 32k entries
0x40	Extra Isize	Indicates large inodes are present on the filesystem
0x80	Has Snapshot	Filesystem has a snapshot
0x100	Quota	Disk quotas are being used on the filesystem

RO Compatible Features (cont.)

Bit	Name	Description
0x200	BigAlloc	File extents are tracked in multi-block clusters
0x400	Metadata Csum	Checksums are used on metadata items
0x800	Replica	The filesystem supports replicas
0x1000	ReadOnly	Should only be mounted as read-only

Features that affect layout

- Sparse Super Blocks
  - Backup superblocks only in groups that are powers of 3, 5, and 7
- Extra isize
  - Indirectly affects layout by changing inode size

Getting Compatible Feature Information