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: Compatible Features

Compatible Features

- Filesystem may be mounted read/write even 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

Compatible Features

Bit	Name	Description
0x1	Dir Prealloc	Directory preallocation
0x2	Imagic inodes	?
0x4	Has Journal	Has a journal (Ext3 and Ext4)
0x8	Ext Attr	Supports Extended Attributes
0x10	Resize Inode	Has reserved Group Descriptor Table entries for expansion
0x20	Dir Index	Has directory indices
0x40	Lazy BG	Support for uninitialized block groups (not common)
0x80	Exclude Inode	Not common
0x100	Exclude Bitmap	Not common
0x200	Sparse Super2	If set superblock backup_bgs points to 2 BG with SB backup

Features that affect layout

- Resize inode
  - Extra space for future expansion in the Group Descriptor Table in each block group
- Sparse super 2
  - Backup super blocks found in the two block groups listed in the super block and in no other block groups

Getting Compatible Feature Information