Linux Forensics

Dr. Phil Polstra
PhD, CISSP, CEH

@ppolstra
http://philpolstra.com

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

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

Inode Extensions & Details

File Mode

15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
Reg/Slink-13/Socket-14	**Directory/Block Bit 13**	**Char Device/Block Bit 14**	**FIFO**	Set UID	Set GID	Sticky Bit	Owner Read	Owner Write	Owner Exec	Group Read	Group Write	Group Exec	Others Read	Others Write	Others Exec

Inode Flags (low word)

15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
File tail not merged	Data written through journal	AFS Magic	Directory has hash indexes	Encrypted Inode	Don't compress file	Compressed clusters	Dirty compressed file	No access time update	No dump	Append only	File is immutable	Synchronous Writes	File is compressed	Preserve for undelete	Secure Deletion

Inode Flags (high word)

31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16
Reserved for Ext4 Library	Unused	Unused	Inode has inline data	Snapshot shrink completed	Snapshot is being deleted	Unused	Inode is snapshot	Unused	Blocks past EOF (depric)	Inode stores large ext attrib	Unused	Inode uses extents	Huge file	Top of directory	Directory entry sync writes

Inode Timestamps

- Change/Modify/Access/Delete timestamps in lower 128 bytes
- Timestamps stored in **Signed** 32-bit seconds since epoch
- Extra timestamp values in upper bytes
  - Lowest 2 bits used to extend timestamp to 34-bit value
  - Upper 30 bits provide nanosecond accuracy of timestamps

Examining Inodes