# Linux Forensics

Dr. Phil Polstra
PhD, CISSP, CEH

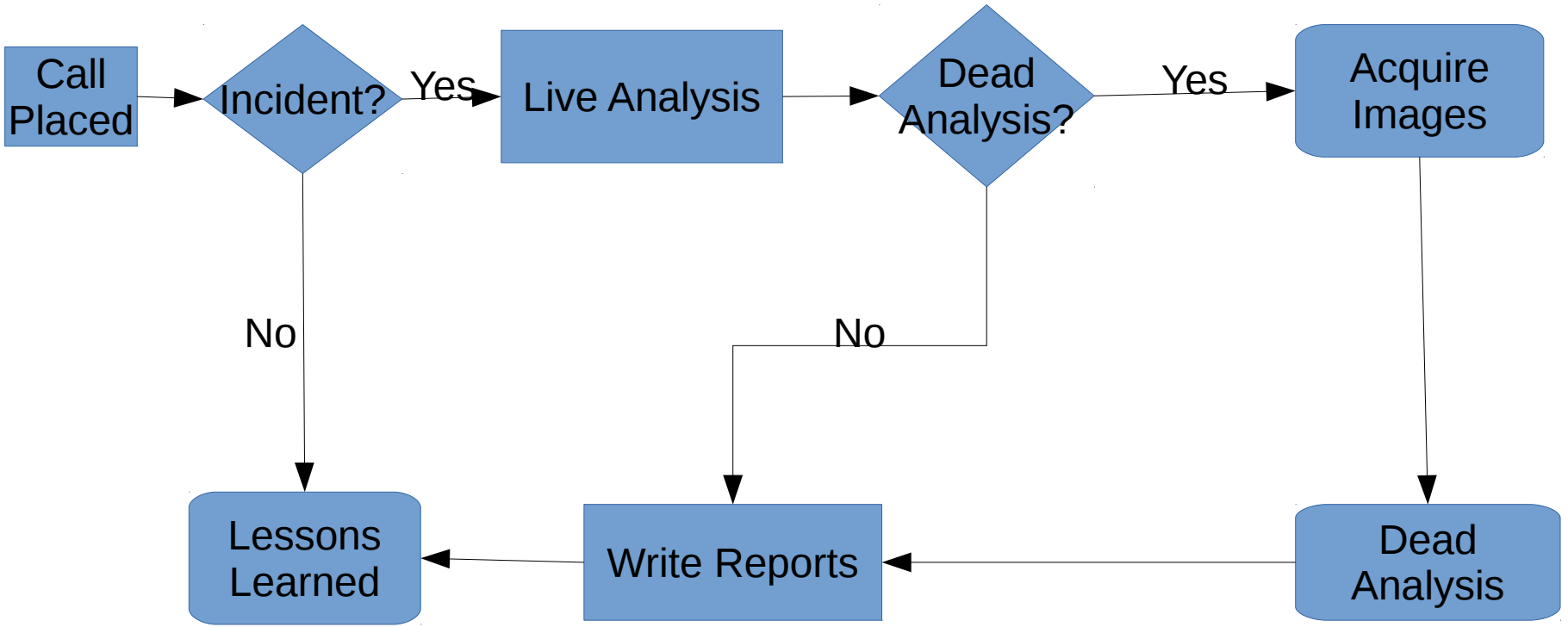
@ppolstra
http://philpolstra.com

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

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

# Filesystem Analysis: Ext2 Basics

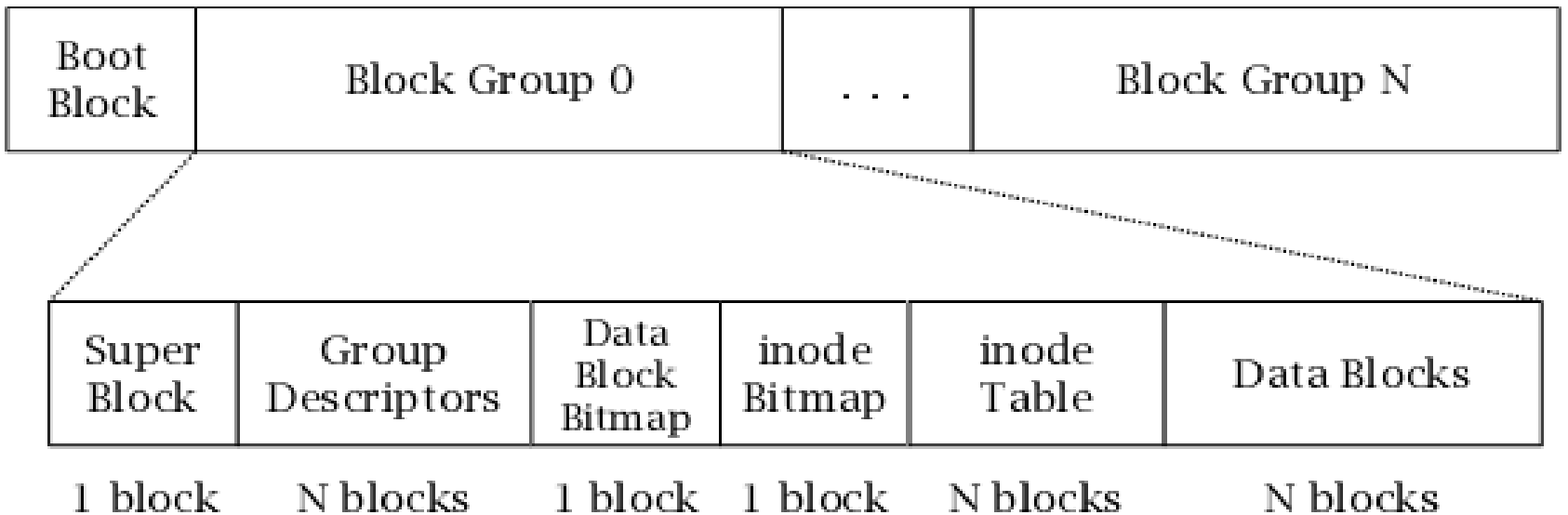
# High Level Process



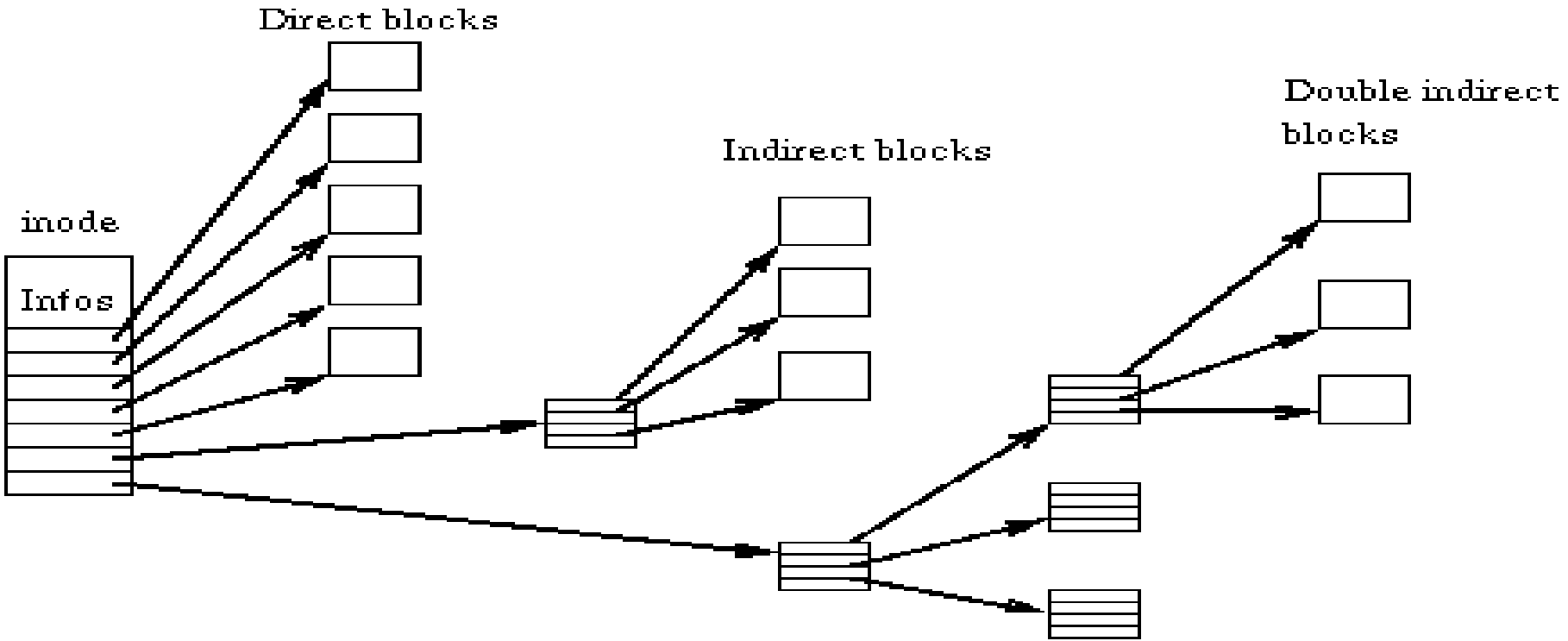
# Extended Filesystem

- Based on the Unix File System (UFS)
- Simpler than UFS
- Meant to be robust with good performance
- Most common filesystem
- Ext2 is common for partitions that don't change much
- Ext3/4 are journaling and used most often

# Ext2 Structure



# Ext2 Inodes



# Ext Optional Features

- Compatible – if OS doesn't support feature it can still safely mount filesystem
- Incompatible – if OS doesn't support feature the filesystem should not be mounted
- Compatible Read Only – if OS doesn't support feature the filesystem can be mounted but not for writing
- Suspected attacker might have non-standard extensions

# The Superblock

- 1024 bytes from start and 1024 bytes long
- Repeated in first block of each group
- The superblock contains
  - Block size
  - Total blocks
  - Blocks per block group
  - Reserved blocks before the first block group
  - Total inodes
  - Inodes per block group
  - Volume name
  - Last write time
  - Last mount time
  - Path where the file system was last mounted
  - Filesystem status (clean?)

# Getting basic Ext2 Information