



File System Analysis

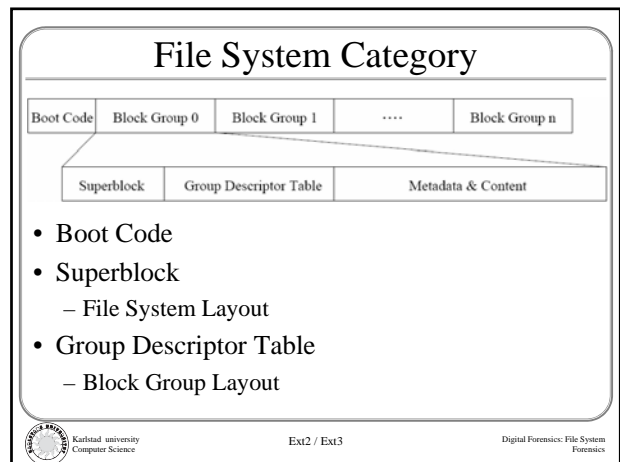
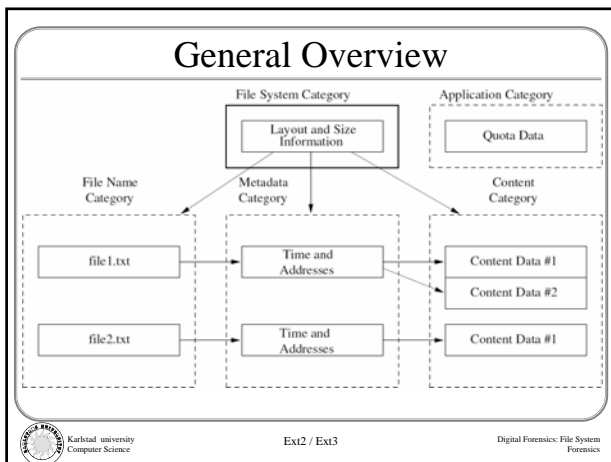
Ext2 and Ext3


Karlstad university
Computer Science
Digital Forensics: File System Forensics

Agenda


- General Overview
- The Categories
 - File system
 - Content
 - Metadata
 - File name
 - Application

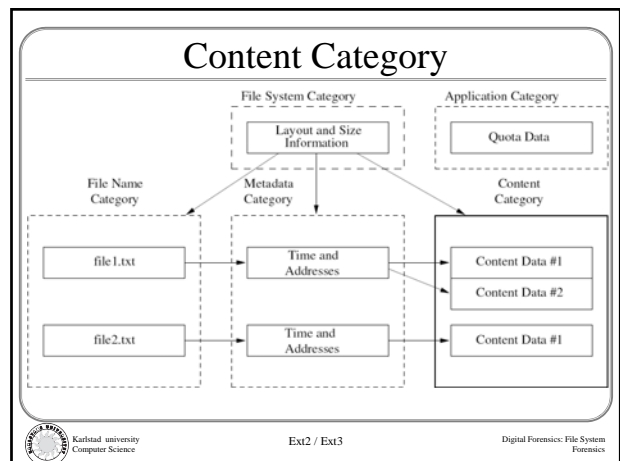

Karlstad university
Computer Science
Ext2 / Ext3
Digital Forensics: File System Forensics



Analysis

- Boot Code
 - 1,024 bytes
 - Is not needed for many file systems
- Superblock
 - 1,024 bytes, most not used
- Group Descriptor Table
 - May be unused space at the end of the table


Karlstad university
Computer Science
Ext2 / Ext3
Digital Forensics: File System Forensics



Content Category

The diagram shows a hierarchy of components. At the top is 'Boot Code'. Below it are 'Block Group 0', 'Block Group 1', and 'Block Group n'. A line connects these groups to a detailed view of a 'Content Category'. This view includes a 'Superblock', a 'Group Descriptor Table', a 'Block Bitmap', 'Meta-data', 'Block 1', and 'Block n'. Arrows indicate that the 'Block Bitmap' and 'Meta-data' are associated with the 'Content Category'.

- Blocks
- Block Bitmap
 - Block Allocation Status

Karlsruhe university Computer Science Ext2 / Ext3 Digital Forensics: File System Forensics

Analysis

- Blocks
 - 1,024; 2048; or 4,096 bytes
 - Easy to locate a given block
 - In same group as its metadata
 - Wiped when allocated
- Block Bitmap
 - The allocation status for all blocks in the group
 - Each bit corresponds to a block
 - Can be used when extracting unallocated blocks

Karlsruhe university Computer Science Ext2 / Ext3 Digital Forensics: File System Forensics

Metadata Category

The diagram illustrates the 'Metadata Category' structure. It is divided into 'File System Category' and 'Application Category'. 'File System Category' includes 'Layout and Size Information'. 'Application Category' includes 'Quota Data'. 'File Name Category' contains 'file1.txt' and 'file2.txt'. 'Metadata Category' contains 'Time and Addresses'. 'Content Category' contains 'Content Data #1' and 'Content Data #2'. Arrows show the relationships between these categories.

Karlsruhe university Computer Science Ext2 / Ext3 Digital Forensics: File System Forensics

Metadata Category

Superblock	Group Descriptor Table	Block Bitmap	Inode Bitmap	Inode Table	Blocks
------------	------------------------	--------------	--------------	-------------	--------

- Inode Table
 - Contains Inodes
- Inode Bitmap
 - Inode Allocation Status
- Extended Attributes
 - For example, ACL

Karlsruhe university Computer Science Ext2 / Ext3 Digital Forensics: File System Forensics

Metadata Category

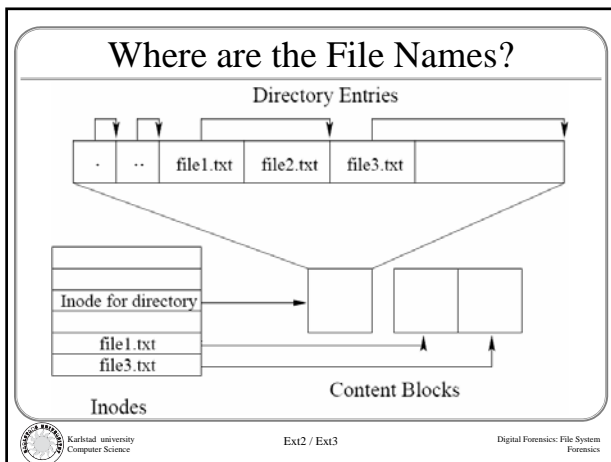
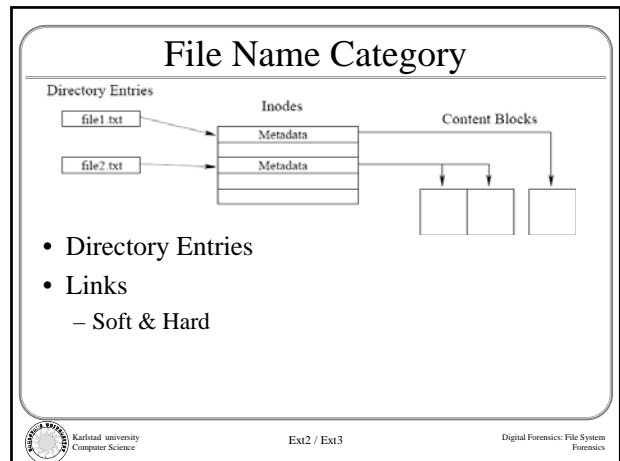
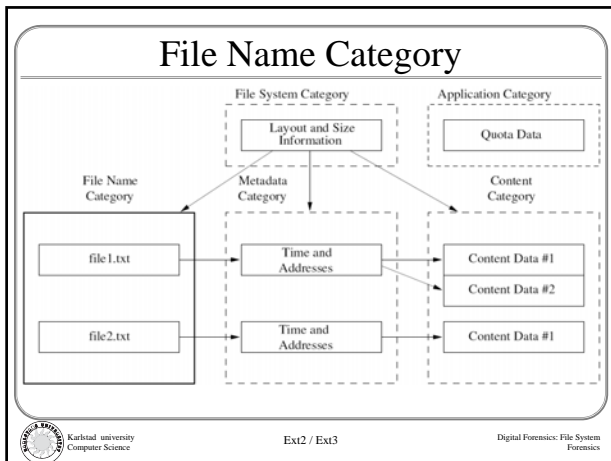
The diagram shows the structure of an 'Inode'. It includes fields for 'File Type & Permissions', 'File Size', and 'Times (MAC)'. It also shows 'Direct Block Pointers' and 'Indirect Block Pointers' that point to a sequence of blocks: 'Block 1', 'Block 12', 'Block 13', 'Block 14', and 'Block 15'. An 'Extended Attribute Block' is also shown pointing to the inodes.

Karlsruhe university Computer Science Ext2 / Ext3 Digital Forensics: File System Forensics

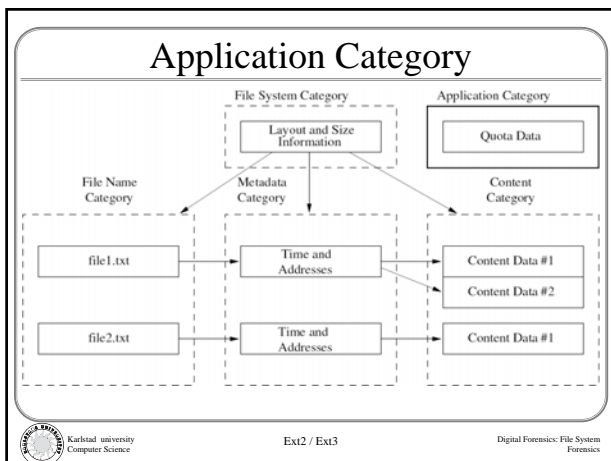
Analysis

- Inodes
 - Easy to locate a given inode
 - Wiped when allocated
 - If file deleted, block pointers cleared in Ext3
 - If file deleted, file name still points to Inode
- Inode Bitmap
- Extended Attributes
 - Collection of key and value pairs

Karlsruhe university Computer Science Ext2 / Ext3 Digital Forensics: File System Forensics



- ### Analysis
- Directory Entries
 - Not removed when files are
 - Short file names will stay longer
 - Inode address not removed in Ext3
 - Inode may be reallocated though
 - Data could be hidden after last entry
- Ext2 / Ext3
- Digital Forensics: File System Forensics



- ### Application Category
- File System Journaling
 - Used to speed up recovery after a system crash
 - Usually contains recent metadata changes
 - Can be used to find deleted file contents
- | | | | | | | | | |
|---------------------|--------------------------|-------------------|-------------------|-------------------|----------------------|--------------------------|-------------------|-----|
| Journal Super Block | Descriptor Sequence #156 | FS Metadata Block | FS Metadata Block | FS Metadata Block | Commit Sequence #156 | Descriptor Sequence #157 | FS Metadata Block | ... |
|---------------------|--------------------------|-------------------|-------------------|-------------------|----------------------|--------------------------|-------------------|-----|
- Ext2 / Ext3
- Digital Forensics: File System Forensics

Analysis

- **Journal**
 - Usefulness depends on degree of system activity
 - Restarted every time file system is mounted
 - Only metadata is logged
 - Metadata is enough for file recovery sometimes!

