The SleuthKit and Autopsy

Florian Buchholz

October 26th, 2005

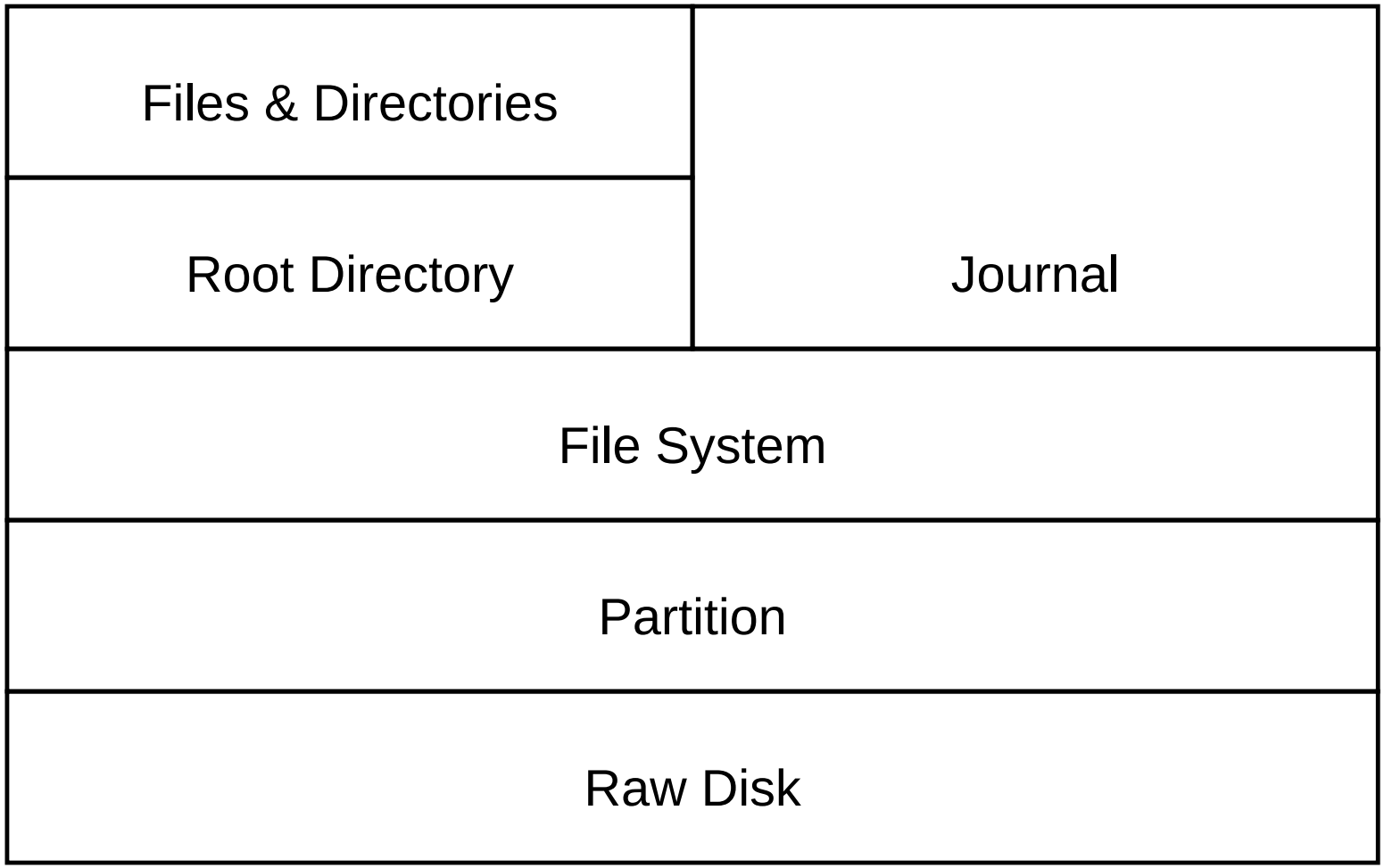
The SleuthKit and Autopsy

- Open source tools for Unix systems
- Developed by Brian Carrier
- Collection of tools to extract data from disks, partitions, and partition images
- http://www.sleuthkit.org
- Extend The Coroner's Toolkit (TCT) written by Dan Farmer and Wietse Venema

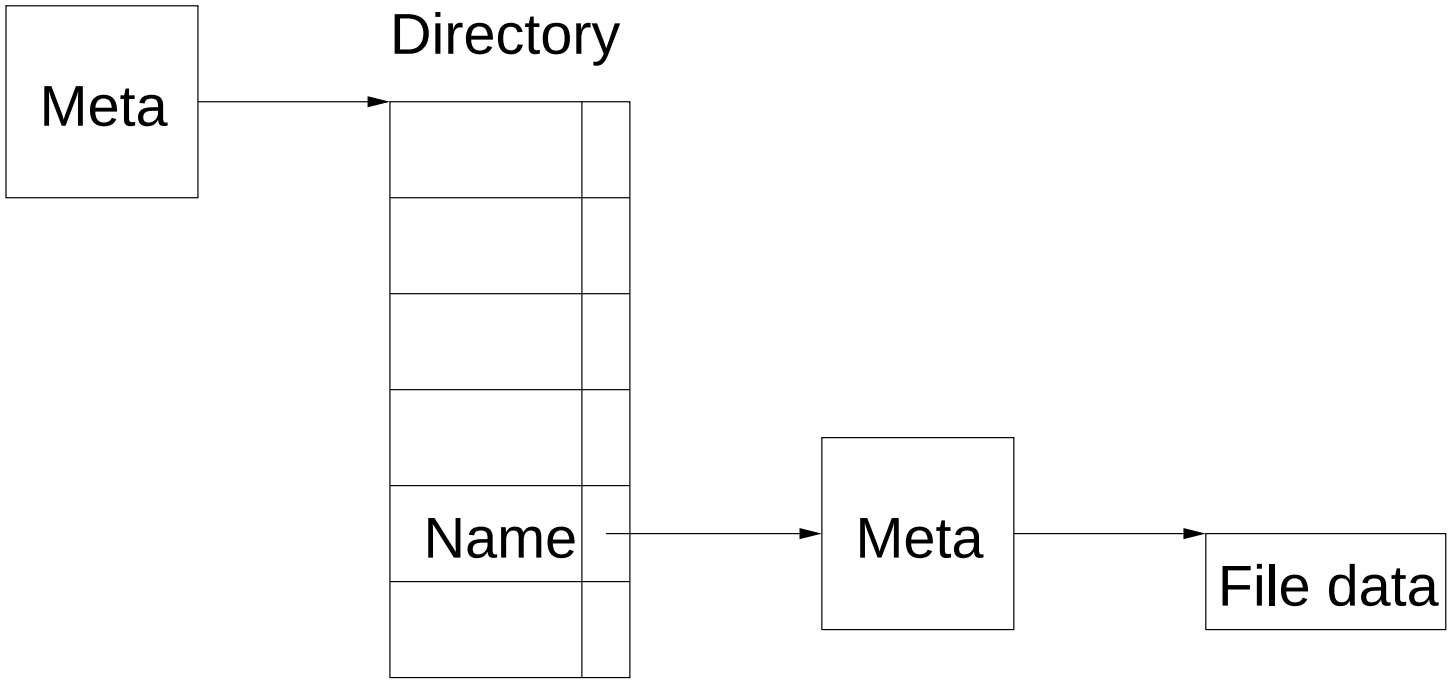
Terms

- **Block/Cluster**: the basic unit a file system can address. For the Unix file systems these are called *blocks*, for FAT and NTFS they are called *clusters*.
- **Fragment/Sector**: the basic unit of space a disk provides. Blocks/clusters are made of a number of fragments/sectors.
- **Inode**: the unit in the file system that contains the meta data for a file. In FAT, an inode equivalent is the combination of data from the FAT entry and data from the directory entry. In NTFS an inode corresponds to an MFT entry.
- **Meta data**: parameters of a file/directory. Includes values such as timestamps, owner, group, permissions, and attributes, but also information on how to assemble the file from the blocks/clusters of the file system.

Data organization



Directories and files



The SleuthKit

- Command-line programs written in C
- Supported file systems: NTFS, FAT, Ext2/3, UFS1/2
- Layers of abstraction:
  - Disk/Image and file system
  - Meta data
  - Directory
  - Data
  - Journal (ext3; no NTFS support yet)

Disk and Image tools

- **disk_stat**: detects host protected area (HPA) and determines actual sector count (works under Linux/ATA only)
- **disk_sreset**: temporarily removes HPA
- **img_stat**: shows details of image format
- **mmls**: displays layout of disk
- **fsstat**: shows the file system details (layout, sizes, labels, …)

Meta data and directory tools

- **ifind**: finds a meta-data structure given a file name or block/cluster
- **ils**: lists inode information
- **istat**: displays detailed meta information for a given inode
- **ffind**: finds the file or directory name that is using a given inode
- **fls**: lists file and directory entries

Data tools

- **dcat**: displays contents of block/cluster chunks
- **icat**: copies the file with the given inode number
- **dls**: copies unallocated data blocks
- **dstat**: displays the allocation status of a given fragment/sector
- **dcalc**: creates block/cluster mapping for dls output

Journal tools

- File system journals:
  - changes to the file system are written into a journal first
  - when a journal entry is “committed”, the actual file system is modified
  - easy recovery after crash: file system is always in a consistent state
- **jls**: lists the contents of a file system journal
- **jcat**: shows the contents of a block/cluster in the file system journal

Other tools

- **hfind**: looks up hash values in a database (supports md5sum output and NSRL)
- **mactime**: creates a timeline of file activity
- **sorter**: sorts files in a partition/image into categories based on file type
- **sigfind**: finds a binary sequence in a given file

Autopsy

- Graphical interface to the command-line tools from the SleuthKit
- Serves as a mini web server and can be accessed with any browser
- Additional features:
  - Case management
  - Event sequencer
  - Notes
  - Report generation
  - Logging of all actions