ALBERT-LUDWIGS-
UNIVERSITÄT FREIBURG

Amir Alsbih and Christian Schindelhauer

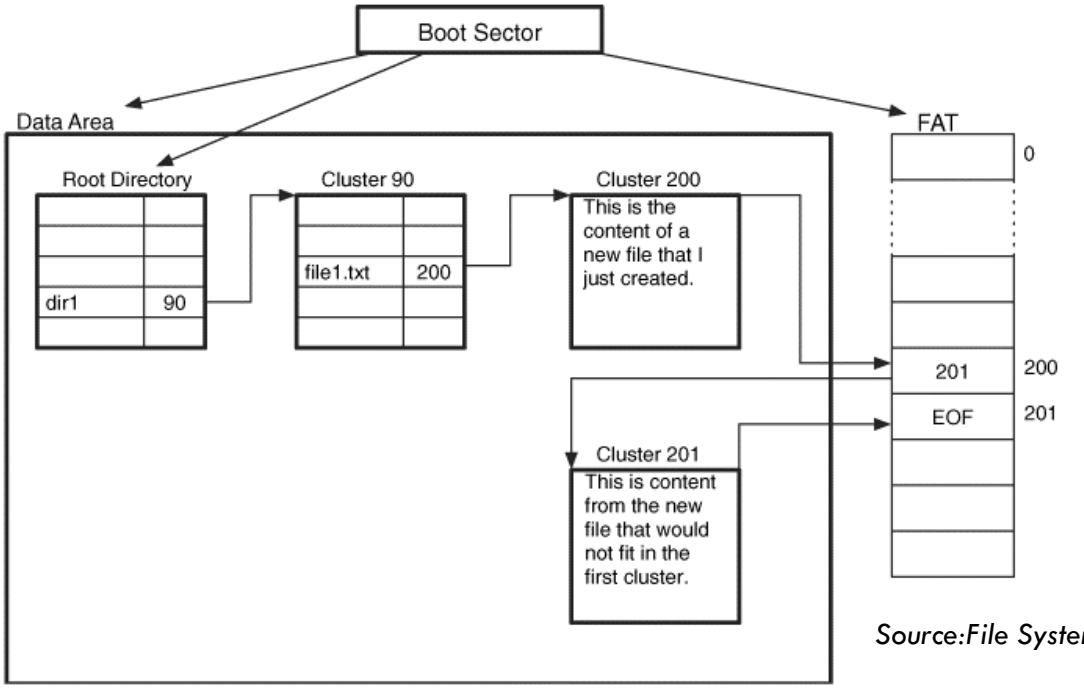
Distributed Storage and

Computer Forensic

2

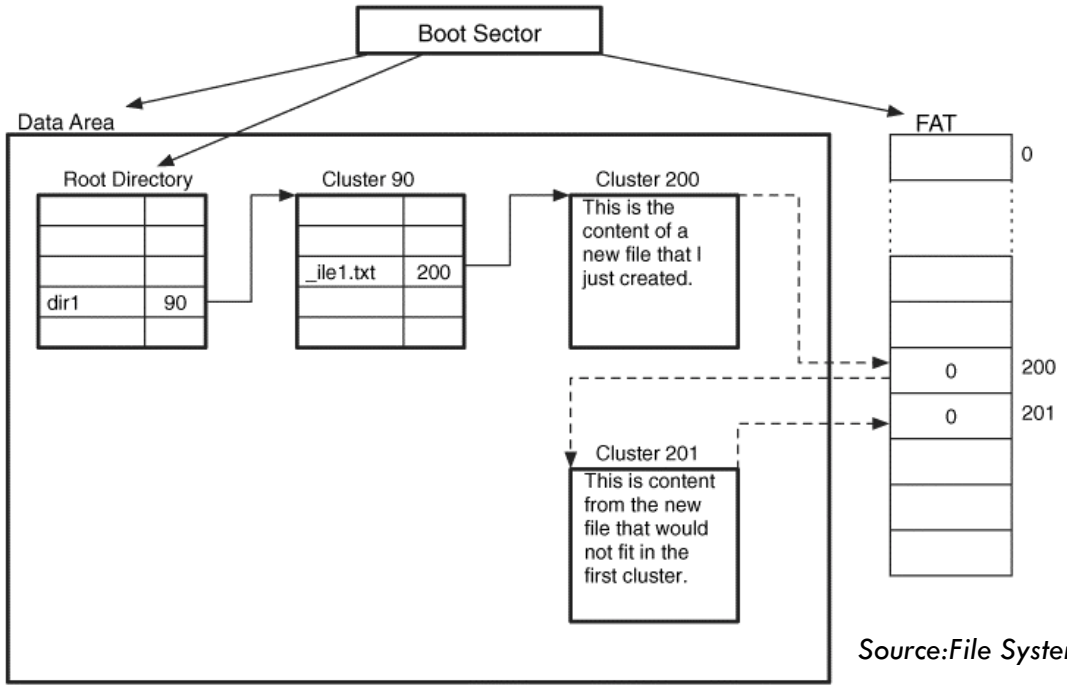
Follow Up

File Allocation Example



Source:File System Forensic Analysis

After File Deletion



Source:File System Forensic Analysis

5 New Technologies File System

Boot Sector

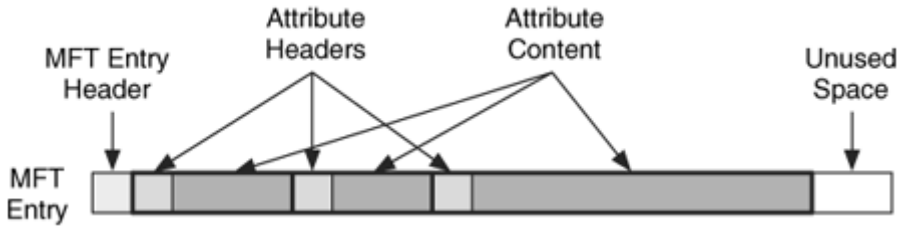
- OEM name: eight-character string (Byte 3-10)
  - NTFS
- Bytes per sector (Byte 11-12)
- Sectors per cluster (Byte 13)
- Total Sectors (Byte 40-47)
- Logical Cluster Number of $MFT (Byte 48-55)
- Logical Cluster Number of $MFT Mirror (Byte 56-63)

NTFS – MFT (Metadata Layer)

ALBERT-LUDWIGS-
UNIVERSITÄT FREIBURG

- In NTFS everything is a file
- The Maste-File-Table (MFT) is a large file that contains the metadata to describe files and directories
- Every file and directory has an entry in the MFT
- Every MFT Entry is 1KB in size, but only the first 42 bytes have a defined purpose

MFT Entry



Source:File System Forensic Analysis

MFT Entry Addresses

ALBERT-LUDWIGS-
UNIVERSITÄT FREIBURG

- MFT entries are sequentially addressed by a 48-bit value.
- The first entry has an address of 0.
- Every MFT entry also has a 16-bit sequence number that is incremented when the entry is allocated.
- The MFT entry and sequence number are combined, with the sequence number in the upper 16-bits, to form a 64-bit file reference address

Source:File System Forensic Analysis

File System Metadata Files

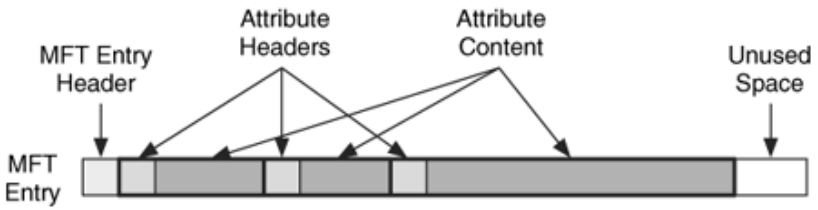
ALBERT-LUDWIGS-
UNIVERSITÄT FREIBURG

Entry	File Name	Description
0	$MFT	The entry for the MFT itself.
1	$MFTMirr	Contains a backup of the first entries in the MFT
4	$AttrDef	Contains the attribute information, such as the identifier values, name, and sizes
5	.	Contains the root directory of the file system
6	$Bitmap	Contains the allocation status of each cluster in the file system
7	$Boot	Volume boot record. Located at the first clusters on the volume. It contains bootstrap code, ... cluster numbers of $MFT and $MFTMirr.

MFT Entry Attribute Concepts

ALBERT-LUDWIGS-
UNIVERSITÄT FREIBURG

- all attributes have two parts: the header and the content
- The attribute header identifies the type of attribute, its size, and its name.
- The attribute header identifies the type of attribute, its size, and its name.
- The content of the attribute can have any format and any size. For example, one of the attributes is used to store the content for a file.
- Remember MFT entry has only 1,024 bytes.

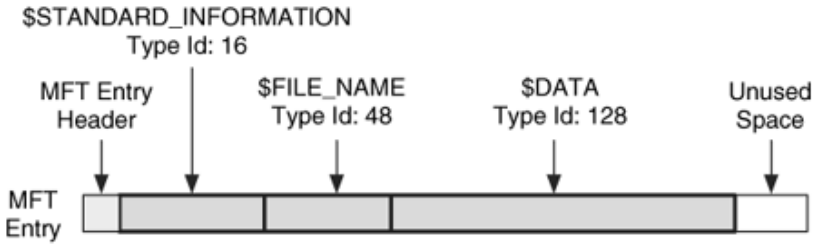


Source:File System Forensic Analysis

Standard Attribute Types

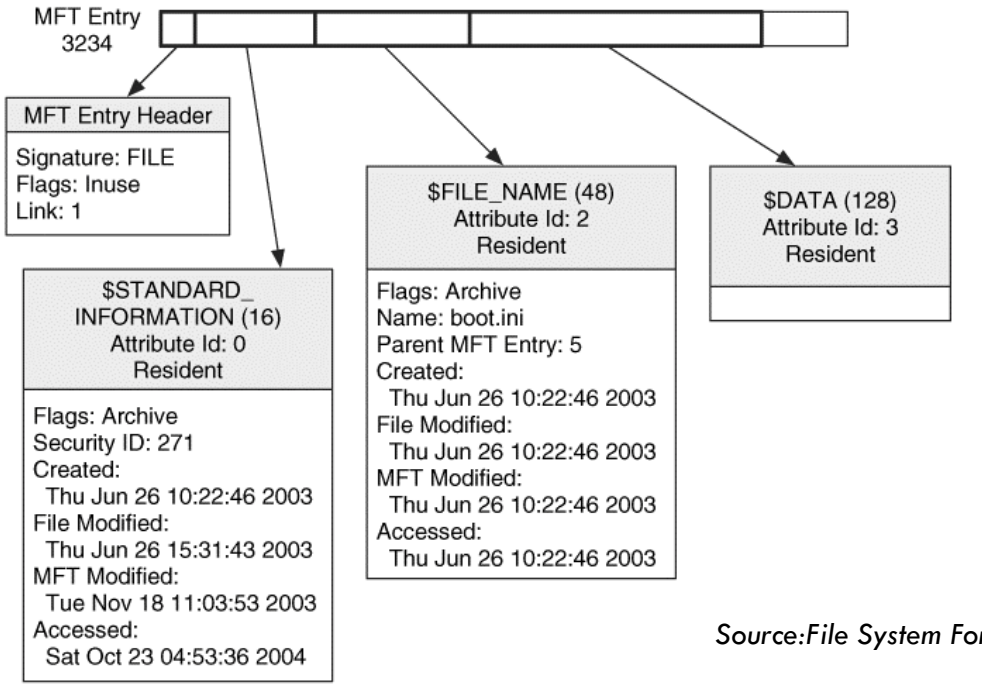
ALBERT-LUDWIGS-
UNIVERSITÄT FREIBURG

- Nearly every MFT entry has a $FILE_NAME and a $STANDARD_INFORMATION .
- The $FILE_NAME attribute contains the file name, size, and temporal information.
- The $STANDARD_INFORMATION attribute contains temporal, ownership, and security information.
- Every file has a $DATA attribute, which contains the file content. If the content is over roughly 700 bytes in size, it becomes non-resident and is saved in external clusters.
- Every directory has an $INDEX_ROOT attribute that contains information about the files and subdirectories that are located in it.



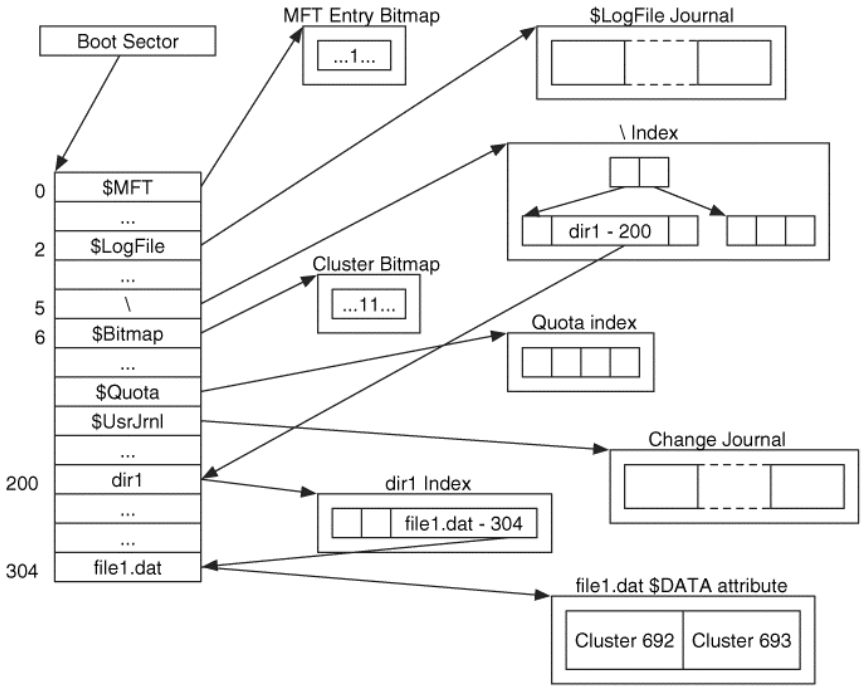
Source:File System Forensic Analysis

MFT Entry for a normal File



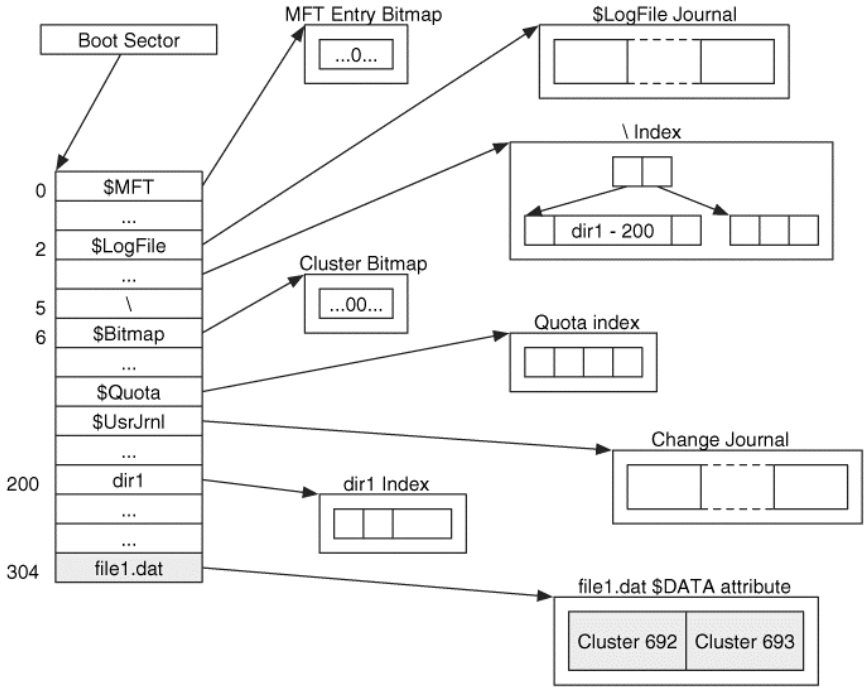
Source:File System Forensic Analysis

File Allocation Example



Source:File System Forensic Analysis

File Deletion Example



Source:File System Forensic Analysis

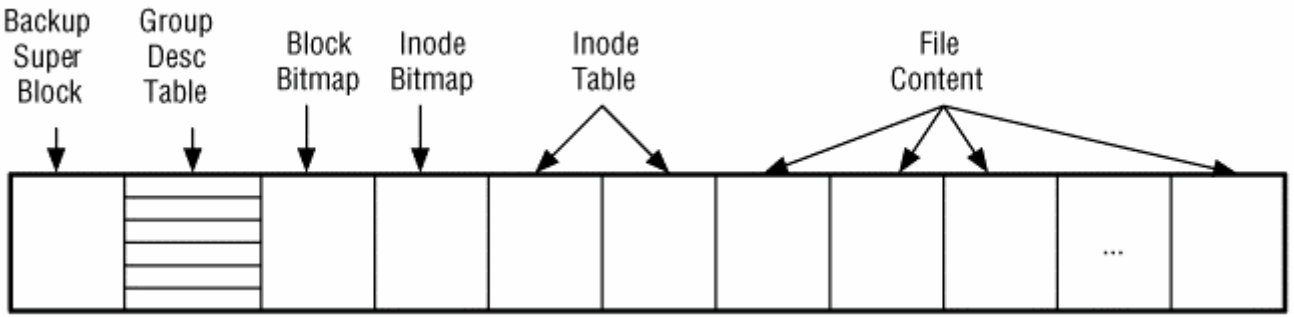
16

EXT2 / EXT3

Superblock

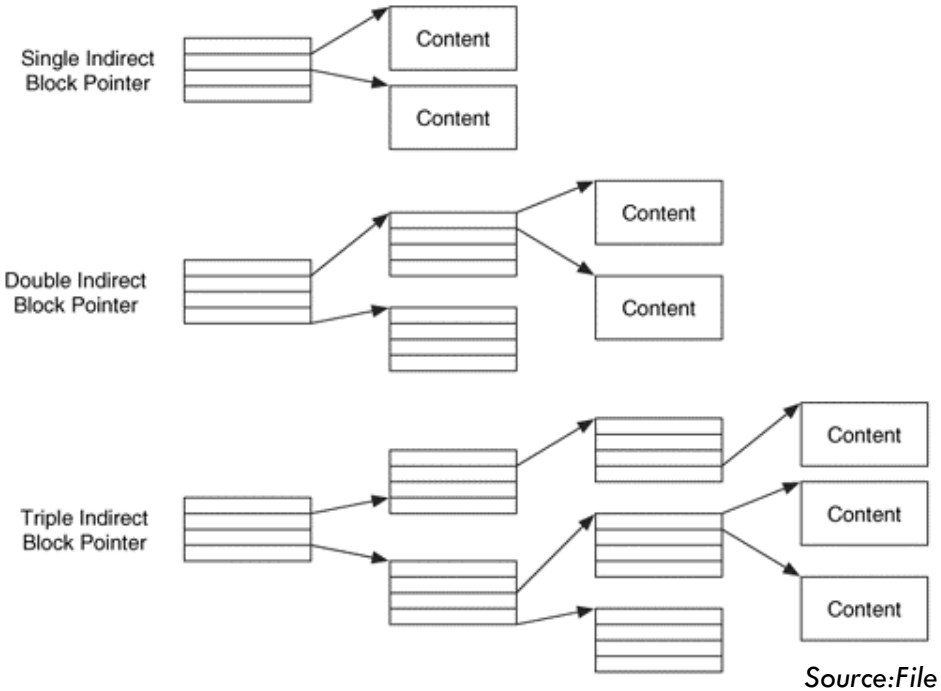
- The ExtX superblock is located at byte 1,024 from the start of the file system.
- Size of the superblock is 1,024 bytes
- contains basic information:
  - the block size,
  - the total number of blocks,
  - the number of blocks per block group,
  - the number of reserved blocks before the first block group.
  - the total number of inodes
  - the number of inodes per block group.

Block Group Descriptor Tables



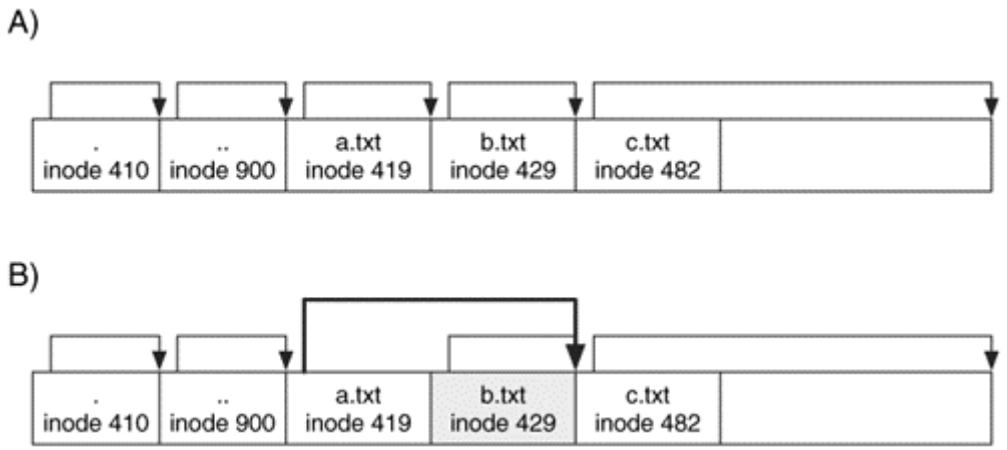
Source:File System Forensic Analysis

Block Pointers



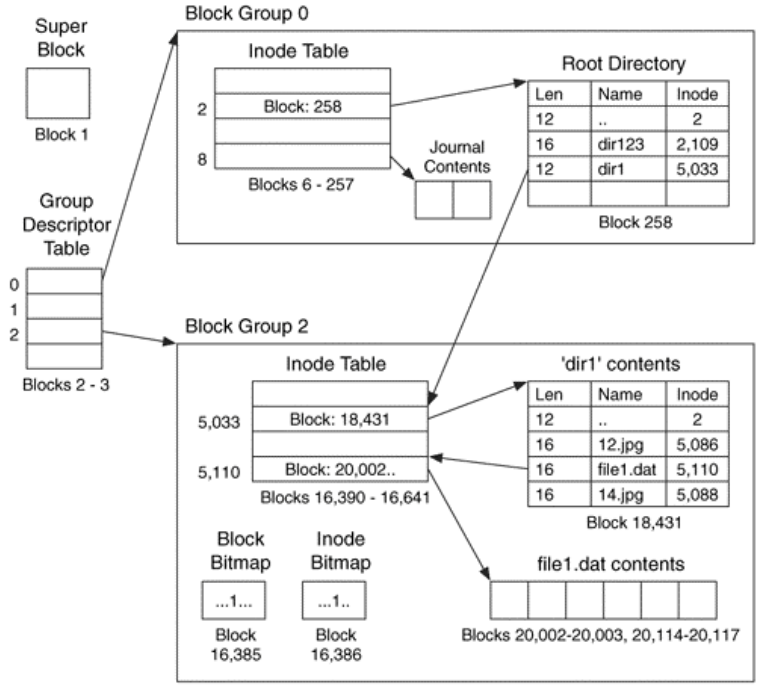
Source:File System Forensic Analysis

File Name Layer



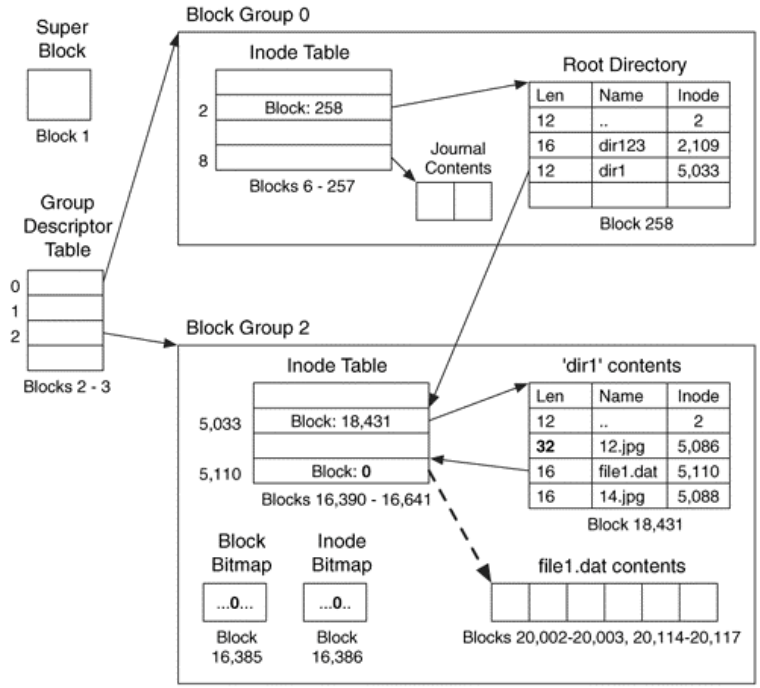
Source:File System Forensic Analysis

File Allocation



Source:File System Forensic Analysis

File Deletion Example



Source:File System Forensic Analysis

Volatile Data Collection

System Memory

- Network Connection
- Processes
- Open Files
- Configuration Parameters
- Encryption Keys
- Passwords
- …

A set of tools

ALBERT-LUDWIGS-
UNIVERSITÄT FREIBURG

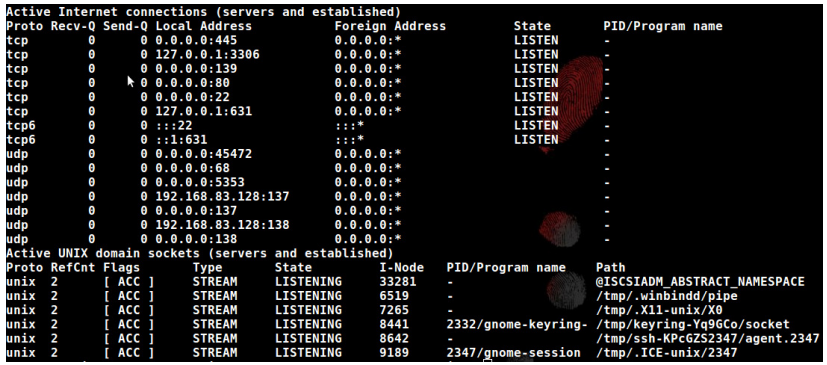
- Volatility Framework
- Win32dd
- memdump
- pd: Process Dumper is able to make a dump of a running process
- pdgmail: gather gmail artifacts
- pdfbook: gather facebook artifacts
- Skypeex: gather skype chat artifacts

Network connections

ALBERT-LUDWIGS-
UNIVERSITÄT FREIBURG

 # netstat –anp

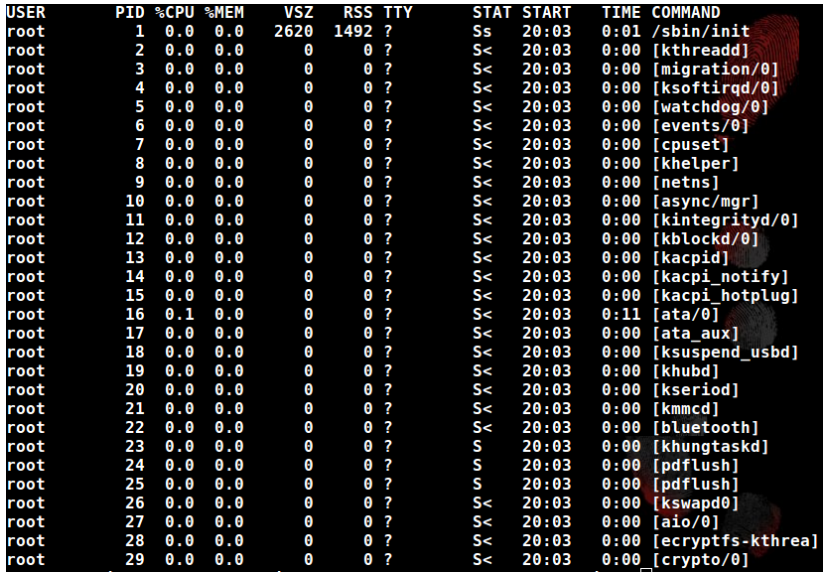
- -a: all sockets
- -n: do not resolve host names
- -p display PID/Programm name for sockets



```
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:445             0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:139             0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -
tcp6       0      0 ::1:631                 :::*                    LISTEN      -
udp        0      0 0.0.0.0:45472           0.0.0.0:*                           -
udp        0      0 0.0.0.0:68              0.0.0.0:*                           -
udp        0      0 0.0.0.0:5353            0.0.0.0:*                           -
udp        0      0 192.168.83.128:137      0.0.0.0:*                           -
udp        0      0 0.0.0.0:137             0.0.0.0:*                           -
udp        0      0 192.168.83.128:138      0.0.0.0:*                           -
udp        0      0 0.0.0.0:138             0.0.0.0:*                           -
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type       State         I-Node   PID/Program name     Path
unix  2      [ ACC ]     STREAM     LISTENING     33281    -                    @ISCSIADM_ABSTRACT_NAMESPACE
unix  2      [ ACC ]     STREAM     LISTENING     6519     -                    /tmp/.winbindd/pipe
unix  2      [ ACC ]     STREAM     LISTENING     7265     -                    /tmp/.X11-unix/X0
unix  2      [ ACC ]     STREAM     LISTENING     8441     2332/gnome-keyring-  /tmp/keyring-Yq9GCo/socket
unix  2      [ ACC ]     STREAM     LISTENING     8642     -                    /tmp/ssh-KPcGZS2347/agent.2347
unix  2      [ ACC ]     STREAM     LISTENING     9189     2347/gnome-session   /tmp/.ICE-unix/2347
```

List processes

- # *ps –aux*
- -a: all
- -u: use effective user ID
- -x: processes without tty



```
USER       PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1  0.0  0.0   2620  1492 ?        Ss   20:03   0:01 /sbin/init
root         2  0.0  0.0      0     0 ?        S<   20:03   0:00 [kthreadd]
root         3  0.0  0.0      0     0 ?        S<   20:03   0:00 [migration/0]
root         4  0.0  0.0      0     0 ?        S<   20:03   0:00 [ksoftirqd/0]
root         5  0.0  0.0      0     0 ?        S<   20:03   0:00 [watchdog/0]
root         6  0.0  0.0      0     0 ?        S<   20:03   0:00 [events/0]
root         7  0.0  0.0      0     0 ?        S<   20:03   0:00 [cpuset]
root         8  0.0  0.0      0     0 ?        S<   20:03   0:00 [khelper]
root         9  0.0  0.0      0     0 ?        S<   20:03   0:00 [netns]
root        10  0.0  0.0      0     0 ?        S<   20:03   0:00 [async/mgr]
root        11  0.0  0.0      0     0 ?        S<   20:03   0:00 [kintegrityd/0]
root        12  0.0  0.0      0     0 ?        S<   20:03   0:00 [kblockd/0]
root        13  0.0  0.0      0     0 ?        S<   20:03   0:00 [kacpid]
root        14  0.0  0.0      0     0 ?        S<   20:03   0:00 [kacpi_notify]
root        15  0.0  0.0      0     0 ?        S<   20:03   0:00 [kacpi_hotplug]
root        16  0.1  0.0      0     0 ?        S<   20:03   0:11 [ata/0]
root        17  0.0  0.0      0     0 ?        S<   20:03   0:00 [ata_aux]
root        18  0.0  0.0      0     0 ?        S<   20:03   0:00 [ksuspend_usbd]
root        19  0.0  0.0      0     0 ?        S<   20:03   0:00 [khubd]
root        20  0.0  0.0      0     0 ?        S<   20:03   0:00 [kseriod]
root        21  0.0  0.0      0     0 ?        S<   20:03   0:00 [kmmcd]
root        22  0.0  0.0      0     0 ?        S<   20:03   0:00 [bluetooth]
root        23  0.0  0.0      0     0 ?        S    20:03   0:00 [khungtaskd]
root        24  0.0  0.0      0     0 ?        S    20:03   0:00 [pdflush]
root        25  0.0  0.0      0     0 ?        S    20:03   0:00 [pdflush]
root        26  0.0  0.0      0     0 ?        S<   20:03   0:00 [kswapd0]
root        27  0.0  0.0      0     0 ?        S<   20:03   0:00 [aio/0]
root        28  0.0  0.0      0     0 ?        S<   20:03   0:00 [ecryptfs-kthrea]
root        29  0.0  0.0      0     0 ?        S<   20:03   0:00 [crypto/0]
```

List open files

ALBERT-LUDWIGS-
UNIVERSITÄT FREIBURG

- # lsof –n
- -n: no host names

```
COMMAND     PID          USER   FD      TYPE     DEVICE SIZE/OFF       NODE NAME
init          1          root  cwd   unknown                             /proc/1/cwd (readlink: Permission denied)
init          1          root  rtd   unknown                             /proc/1/root (readlink: Permission denied)
init          1          root  txt   unknown                             /proc/1/exe (readlink: Permission denied)
init          1          root NOFD                                       /proc/1/fd (opendir: Permission denied)
kthreadd      2          root  cwd   unknown                             /proc/2/cwd (readlink: Permission denied)
kthreadd      2          root  rtd   unknown                             /proc/2/root (readlink: Permission denied)
kthreadd      2          root  txt   unknown                             /proc/2/exe (readlink: Permission denied)
kthreadd      2          root NOFD                                       /proc/2/fd (opendir: Permission denied)
migration     3          root  cwd   unknown                             /proc/3/cwd (readlink: Permission denied)
```

Other things

ALBERT-LUDWIGS-
UNIVERSITÄT FREIBURG

- Current date/time:
  # date
- Partition map
  # fdisk -l
- Mount points
  # mount
- System uptime
  # uptime
- OS type
  # uname -a

```
/dev/sda3 on / type ext3 (rw,errors=remount-ro)
proc on /proc type proc (rw)
none on /sys type sysfs (rw,noexec,nosuid,nodev)
none on /sys/fs/fuse/connections type fusectl (rw)
none on /sys/kernel/debug type debugfs (rw)
none on /sys/kernel/security type securityfs (rw)
udev on /dev type tmpfs (rw,mode=0755)
none on /dev/pts type devpts (rw,noexec,nosuid,gid=5,mode=0620)
none on /dev/shm type tmpfs (rw,nosuid,nodev)
none on /var/run type tmpfs (rw,nosuid,mode=0755)
none on /var/lock type tmpfs (rw,noexec,nosuid,nodev)
none on /lib/init/rw type tmpfs (rw,nosuid,mode=0755)
/dev/sdb1 on /cases type ext3 (rw)
/dev/sda1 on /boot type ext3 (rw)
```

Sample output of mount

On Windows WFT

- WINDOWS FORENSIC TOOLCHEST (WFT):
  - Memory Image
  - Network Information
  - Process Information
  - Filesystem and Registry
  - Files with hashes
  - System Information
  - …

Source: foolmoon.net

One transfer possiblity

ALBERT-LUDWIGS-
UNIVERSITÄT FREIBURG

Unencrypted way

- Forensic Workstation:

  #nc –l –p port > file_dump

- Network Maschine:

  #input | nc IP port

Encrypted way (twofish)

- Forensic Workstation:

  #cryptcat –l –p port –k passwort > file_dump

- Network Maschine:

  #input | cryptcat –k passwort IP port

Evidence

Evidence integrity

ALBERT-LUDWIGS-
UNIVERSITÄT FREIBURG

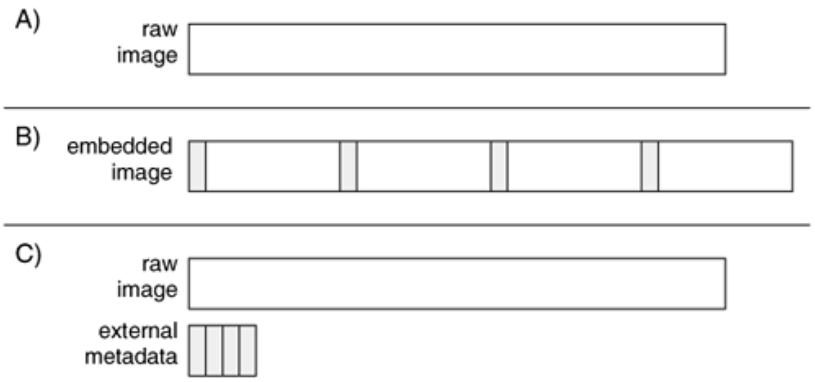
- Hash everything
- Saves you from tampering claims

- MD5:
  - Generate:
    # md5sum file > file.md5
  - Check:
    # md5sum file –c file.md5
- SHA(224|256|384|512):
  - Generate:
    # shaXsum file > file.shaX
  - Check:
    #shaXsum file –c file.shaX

Image Formats

ALBERT-LUDWIGS-
UNIVERSITÄT FREIBURG

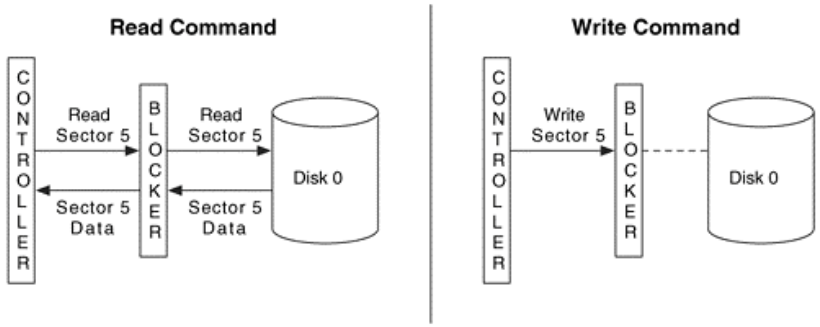
- RAW (.dd|.img):
  - Original true bit copy
  - Same size as orginal drive
  - No compression
  - No metadata
- Expert Witness Format (.E01):
  - Contains metatata (Hash, Dates, …)
  - Can be compressed
  - Proprietary Format
- Advanced Forensic Format (.AFF):
  - Stores metatadata (Hash, Dates, …)
  - Can be compressed
  - AFF: Single lage file with metadata
  - AFD: Multiple small files with metadata
  - AFM: Drive Image is in RAW Format and a secound file contains the metadata



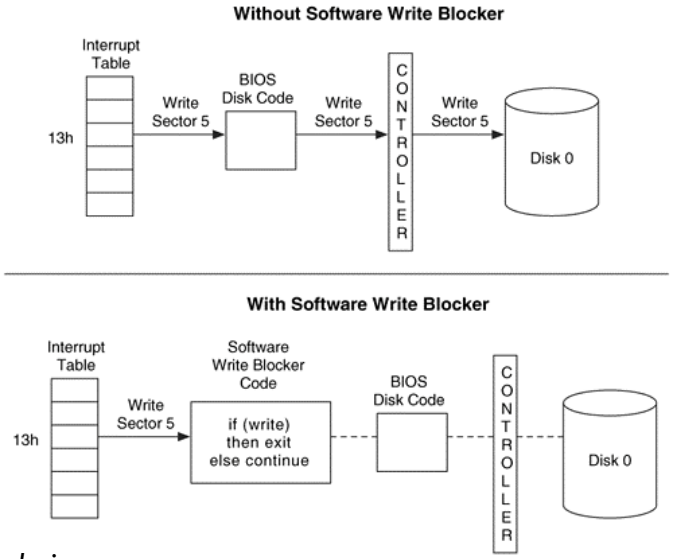
Source:File System Forensic Analysis

Evidence collection

Hardware write blocker



Software write blocker



Source:File System Forensic Analysis

DD

 # dd if=INPUT of=OUTPUT [options]

- bs=value: set block size to value
- count=value: copy only value **blocks**
- skip=value: skip value blocks in input
- **conv=noerror,sync**: skip unreadable sections

On Windows also:

- --cryptsum HASHTYPE [md5,sha, sha1, sha256]
- --log file
- --cryptout file
- --verify

DC3DD

ALBERT-LUDWIGS-
UNIVERSITÄT FREIBURG

 # dc3dd if=INPUT of=OUTPUT [options]

- bs=value: set block size to value
- count=value: copy only value **sectors**
- skip=value: skip value blocks in input
- seek=value: skip value blocks in output
- **conv=noerror,sync**: skip unreadable sections
- progress=on: Display a progress meter
- Hash=ALG: computes hash of the input [md5,sha1,sha256,sha512]
- hashlog=FILE
- log=file