Imaging Systems

```
# dd if=input file of=output file options
```

Example Input Files (if = *input file*)

LINUX

`/dev/hda`	(First IDE Physical Drive)
`/dev/hda2`	(Second Logical Partition)
`/dev/sda`	(First SCSI Physical Drive)

WINDOWS

`\\.\PhysicalDrive0`	(First Physical Drive)
`\\.\D:`	(Logical Drive D:)
`\\.\PhysicalMemory`	(Physical Memory)

Example Output Files (of = *output file*)

`\\hostname\share\imagefile.img`	(Windows Share)
`imagefile.img`	(Bit Image File)
`/dev/usb/`	(USB Drive)
`/dev/hdb`	(2nd IDE Drive)

Useful Options

`bs= block size`	(sets the block size)
`count=N`	(copy only N blocks FILE)
`skip=N`	(skip ahead N blocks FILE)
`conv=noerror`	(do not stop on errors)

DCFLDD for creating integrity checks and status

```
# dcfldd if=(input file) of=(output file)
hashwindow=0 hashlog=input_file.md5.txt
```

MMLS to split out partitions from physical image

 # mmls -t dos imagefile (-t is the type of drive)

Slot	Start (skip)	End	Length (count)	Description
02: 00:00	0000000063	0001028159	0001028097	Win95 FAT32 (0x0B)

Use dd to pull the logical image from physical image

 # dd if=imagefile bs=512 skip=63 count=1028097 of=imagefile.partition1.img

Netcat

Netcat is used to transfer output from one system to another.

```
Listener:       # nc -l -p port
Client:         # nc hostname port -w 3
```

Sleuthkit Tools

File System Layer Tools

fsstat -Displays details about the file system

```
# fsstat -f fs-type imagefile.img
```

Data Layer Tools

dcat -Displays the contents of a disk block

```
# dcat -f fs-type imagefile.img fragment_num
```

dls -Lists contents of deleted disk blocks

```
# dls -f fs-type imagefile.img > imagefile.dls
```

dcalc -Maps between dd images and dls results

```
# dcalc -f fs-type imagefile.img -u
fragment_num_dls
```

dstat -Lists statistics associated with specific disk blocks

```
# dstat -f fs-type imagefile.img fragment_num
```

Meta Data Layer Tools

ils -Displays inode details

```
# ils -f fs-type imagefile.img
```

istat -Displays information about a specific inode

```
# istat -f fs-type imagefile.img inode_num
```

icat -Displays contents of disk blocks allocated to an inode

```
# icat -f fs-type imagefile.img inode_num
```

ifind -Determine which inode has allocated a block in an image

```
# ifind -f fs-type dev_hde8.img -d block_num
```

Filename Layer Tools

fls -Displays deleted file entries in a directory inode

```
# fls -rpd -f fs-type imagefile.img
```

ffind -Determine which file has allocated an inode in an image

```
# ffind -f fs-type imagefile.img 26466
```

SANS INSTITUTE

Forensic Analysis

Cheat Sheet v1.3

Forensics

POCKET REFERENCE GUIDE

SANS Institute
incidents@sans.org
+1 317.580.9756
http://www.sans.org
http://www.incidents.org

Purpose

Forensic Analysts are on the front lines of computer investigations. This guide aims to support Forensic Analysts in their quest to uncover the truth.

How To Use This Sheet

When performing an investigation it is helpful to be reminded of the powerful options available to the investigator. This document is aimed to be a reference to the tools that could be used. Each of these commands runs locally on a system.

This sheet is split into these sections:

- Mounting Images
- Imaging Systems
- Integrity Checking
- Netcat
- Automated Forensic Data Collection
- Recovering Data
- Creating Timelines
- String Searches
- The Sleuthkit

The key to successful forensics is minimizing your data loss, accurate reporting, and a thorough investigation.

Mounting Images

mount -t fstype [options] ***image mountpoint***

device can be a disk partition or image file

Useful Options (`-o`)

`ro`	mount as read only
`loop`	mount on a loop device
`noexec`	do not execute files
`noatime`	do not adjust last access times
`uid=` ***user_id***	mount as a specific user
`gid=` ***group_id***	mount as a group

`umask=` ***set permissions***

`show_sys_files=true` (For NTFS file system only)

Example: Mount an image file at mount_location

```
# mount -t fs_type -o loop,
ro,umask=0222,uid=forensic,gid=users
imagefile.img /mnt/hack/mount_location
```

Integrity Checking

Perform integrity checks on a file or an imagefile to ensure the data has not changed use md5sum.

Example: Calculate a hash for partition 1 of disk hda

```
# md5sum /dev/hda1
```

Tool designed to recursively go through a file system to calculate md5 hashes

`-r` recursive mode

```
# md5deep -r /
```

Creating Timelines

Create the body file of all filename data using fls

```
# fls -f fs-type -m mountpoint -r imagefile.img >
imagefile.fls
```

mountpoint = location of mount (`/` or `C:`)

Create the body file of all deleted inode structures

```
# ils -f fs-type -m imagefile.img >
imagefile.ils
```

Entries from 'ils' will have names such as:
`<dev_hde8.img-dead-992>`

Create the overall body file

```
# cat imagefile.?ls > imagefile.mac
```

Create the timeline

```
# mactime -b imagefile.mac > timeline.all
```

String Searches

Perform a string search in an image and list the offset

```
# strings --radix=d imagefile.img
```

Unicode strings can be searched for using (`sstrings`)

Search for a specific string in an image using grep

GREP Useful Options

`-i`	ignore case
`-A Num`	print Num lines AFTER
`-B Num`	print Num lines BEFORE
`-f dirty_word_list`	

```
# strings --radix=d imagefile.img |
grep -i password -A 8
```

Perform a Dirty Word Search on an image

```
# cat imagefile.img | strings
--radix=d | grep -f dirty_word_list
```

Automated Forensic Data Collection

WINDOWS (Windows Forensic Toolchest)

Use WFT to automate the gathering of information on your windows system. You can execute this from a CDROM D: and set your output file (-dst) to a network share

```
D:\wft_directory\wft.exe -cfg wft_config.cfg
-dst \\server\share\
```

Edit your wft_config.cfg file to gather exactly what is needed.

Recovering Data

Create Unallocated Image Using dls

```
# dls -f fs-type imagefile.img >
unallocated_imagefile.dls
```

Create Slack Image Using dls (for FAT and NTFS)

```
# dls -f fs-type -s imagefile.img >
imagefile.slack
```

Use foremost and lazarus on raw data, slack space, memory, and unallocated space

Lazarus - Attempts to identify disk blocks

```
# lazarus -h unallocated_imagefile.dls
```

Foremost - Carves out files based on headers and footers

```
# foremost -o outputdir -c
/path/to/foremost.conf  data_images
```