

Linux uses ext4

```
dd if=/dev/zero of=myhd.img bs=1024 count=4096
```

As root:

```
losetup /dev/loop0 /home/crandall/fstomfoolery/myhd.img
```

```
mkfs.ext4 /dev/loop0
```

```
mkdir /mnt/myhd
```

```
mount /dev/loop0 /mnt/myhd/
```

```
df -Th
```

```
debugfs /dev/loop0
```

```
stat hello.txt
```

```
logdump
```

ctime – change time, updated if anything about the file changes (inode or content – because mtime is part of the inode)

atime – access time, updated when the file is accessed

mtime – modification time, updated when the file contents are modified

Check out:

extcarve (<http://www.giis.co.in/giis/>)

Bulk Extractor ([http://www.forensicswiki.org/wiki/Bulk\\_extractor](http://www.forensicswiki.org/wiki/Bulk_extractor))