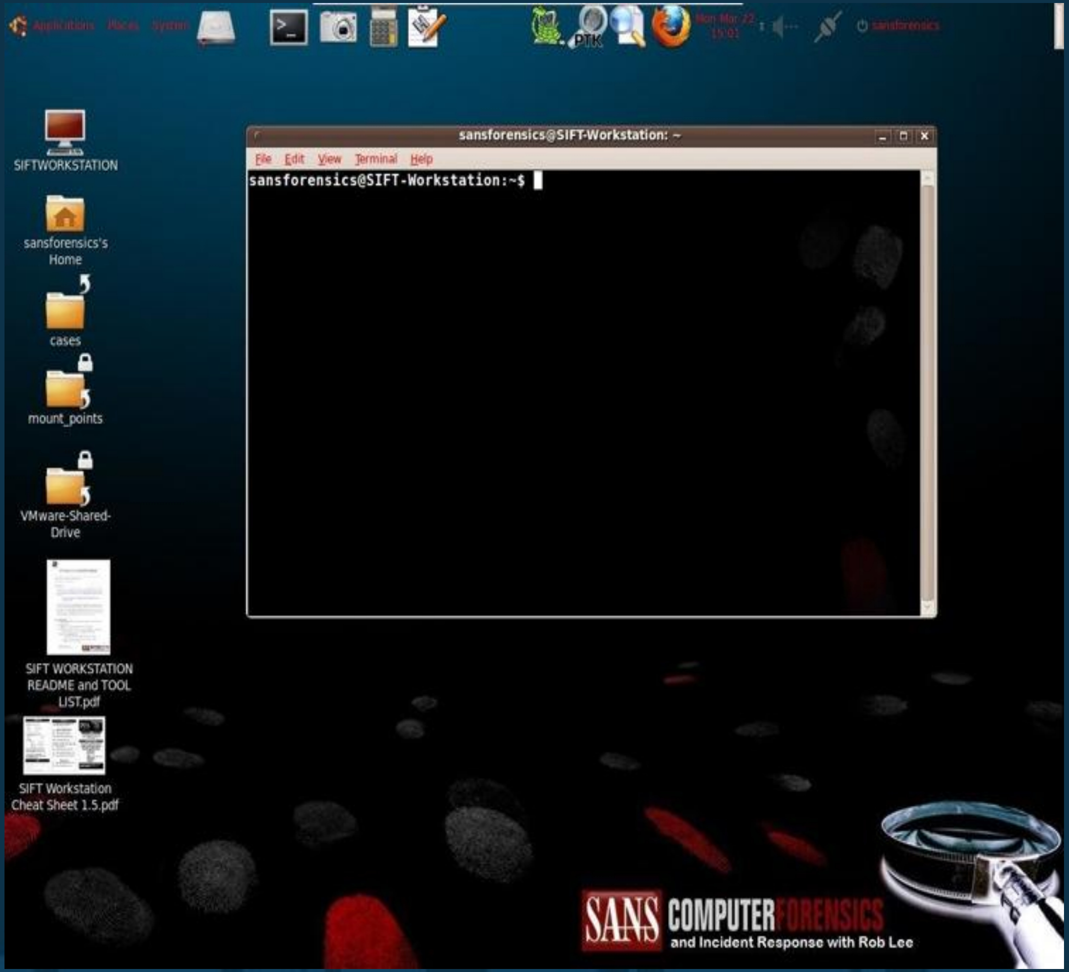
DD IS GANGSTA

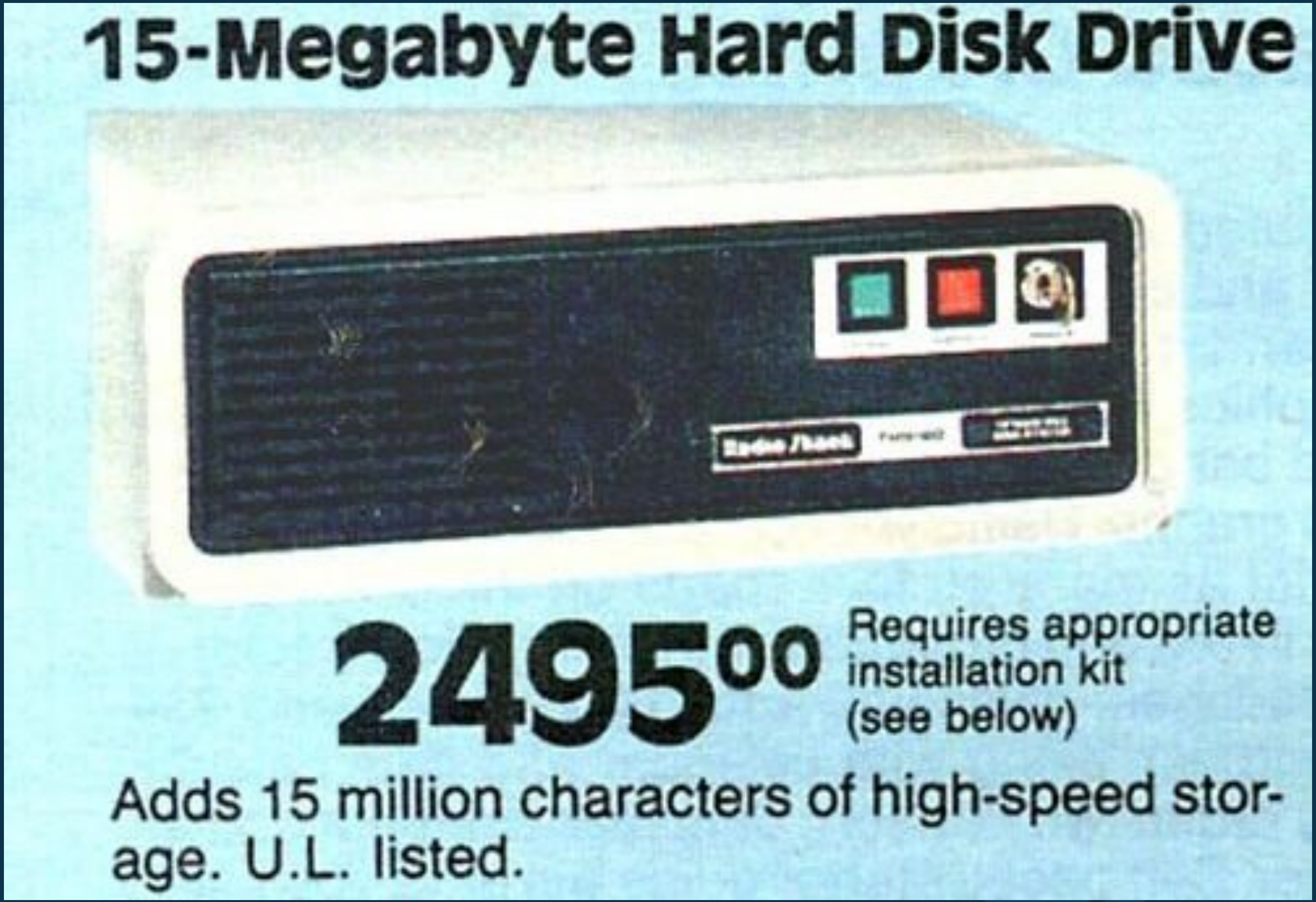
"If you don't know, now you know"

SANS SIFT Kit 2.1

http://computer-forensics.sans.org/community/downloads


Applications Places System
SIFTWORKSTATION
sansforensics's Home
cases
mount_points
VMware-Shared-Drive
SIFT WORKSTATION README and TOOL LIST.pdf
SIFT Workstation Cheat Sheet 1.5.pdf
PTK
sansforensics@SIFT-Workstation: ~
File Edit View Terminal Help
SANS COMPUTER FORENSICS and Incident Response with Rob Lee

```
sansforensics@SIFT-Workstation:~$
```

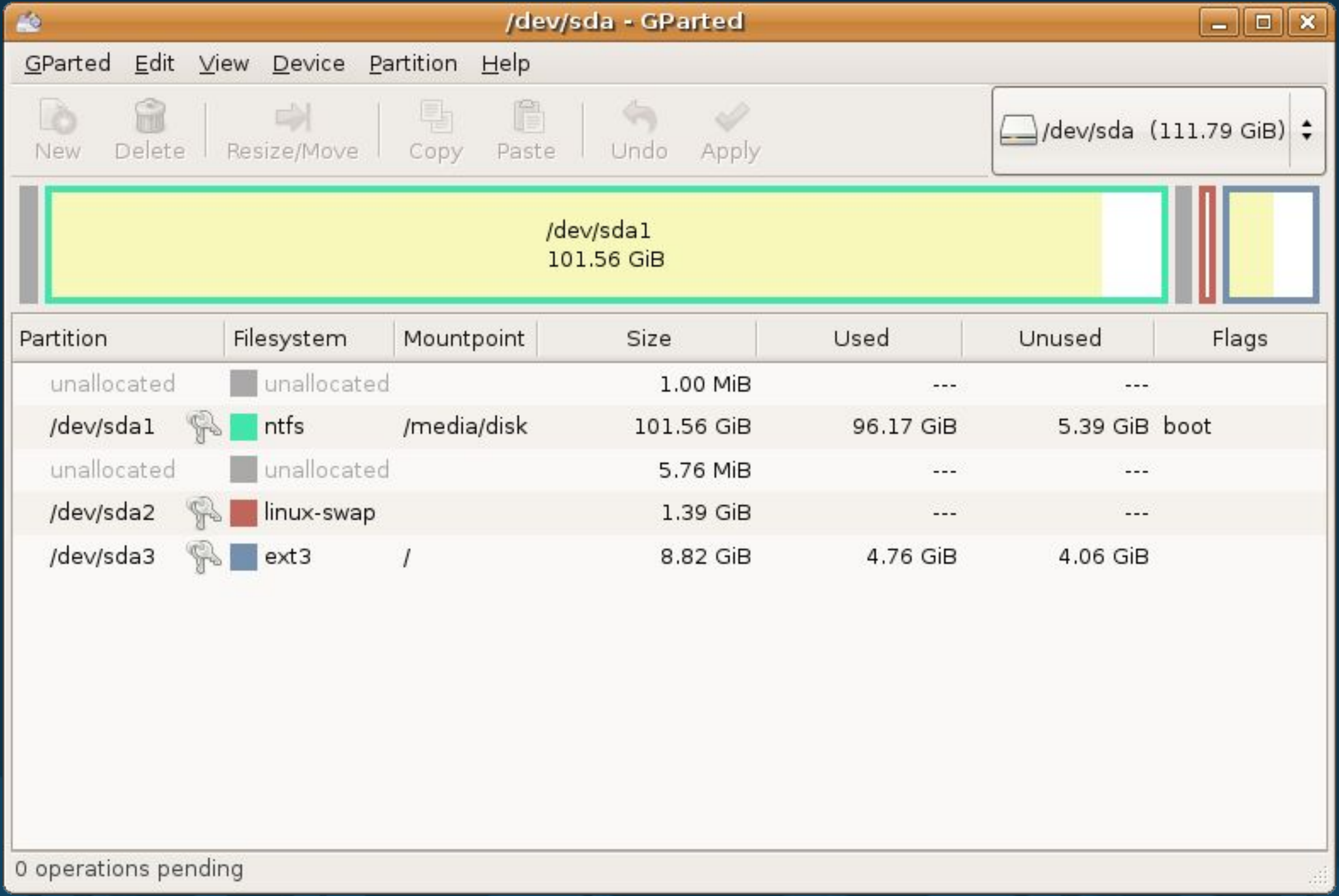


15-Megabyte Hard Disk Drive

2495^{00} Requires appropriate installation kit (see below)

Adds 15 million characters of high-speed storage. U.L. listed.

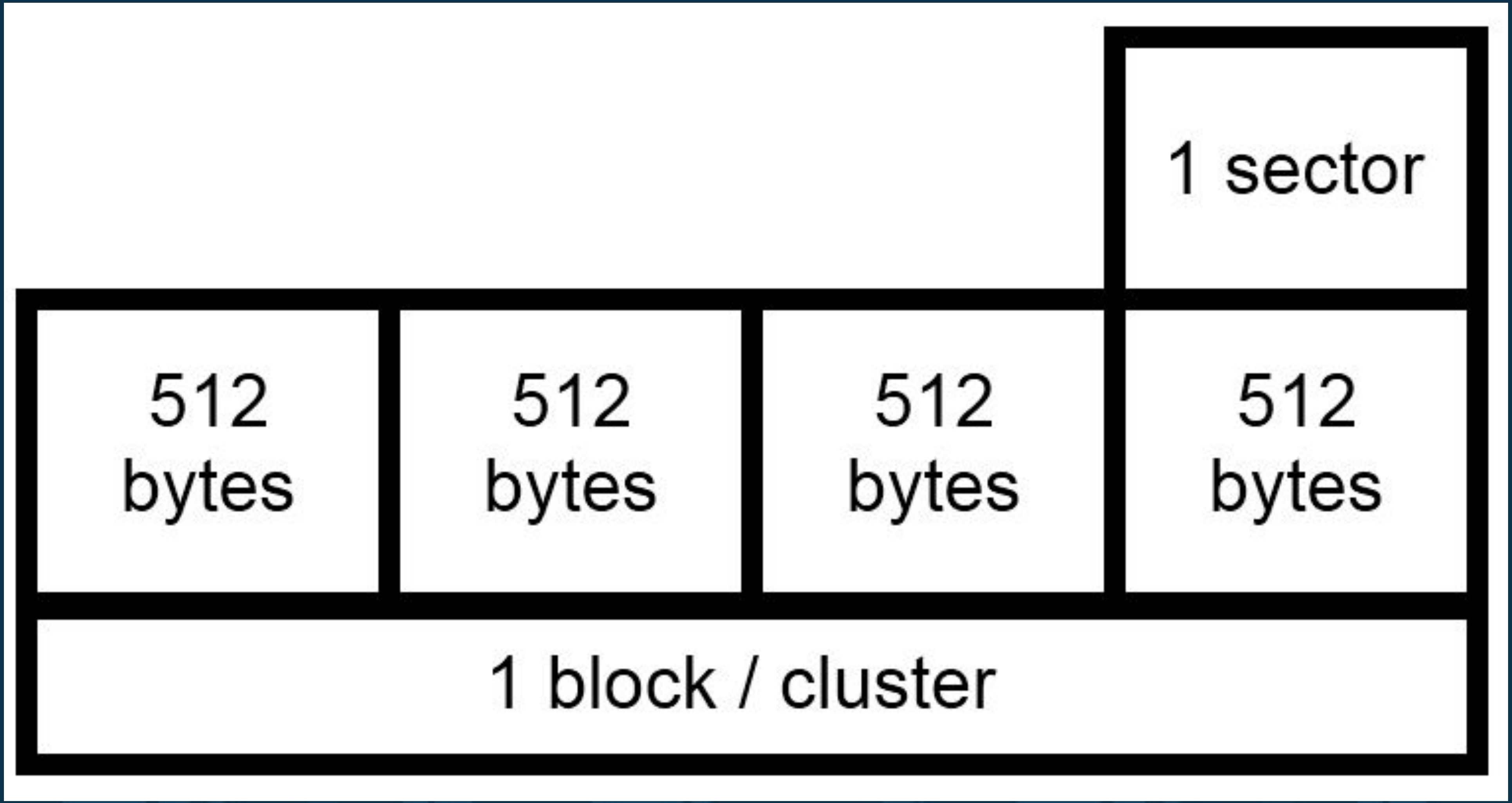
Layer 1 - Physical



Partition	Filesystem	Mountpoint	Size	Used	Unused	Flags
unallocated	▨ unallocated		1.00 MiB	---	---	
/dev/sda1	🟩 ntfs	/media/disk	101.56 GiB	96.17 GiB	5.39 GiB	boot
unallocated	▨ unallocated		5.76 MiB	---	---	
/dev/sda2	🟥 linux-swap		1.39 GiB	---	---	
/dev/sda3	🟦 ext3	/	8.82 GiB	4.76 GiB	4.06 GiB	

0 operations pending

Layer 2 - Filesystem / Partition



1 sector

512 bytes

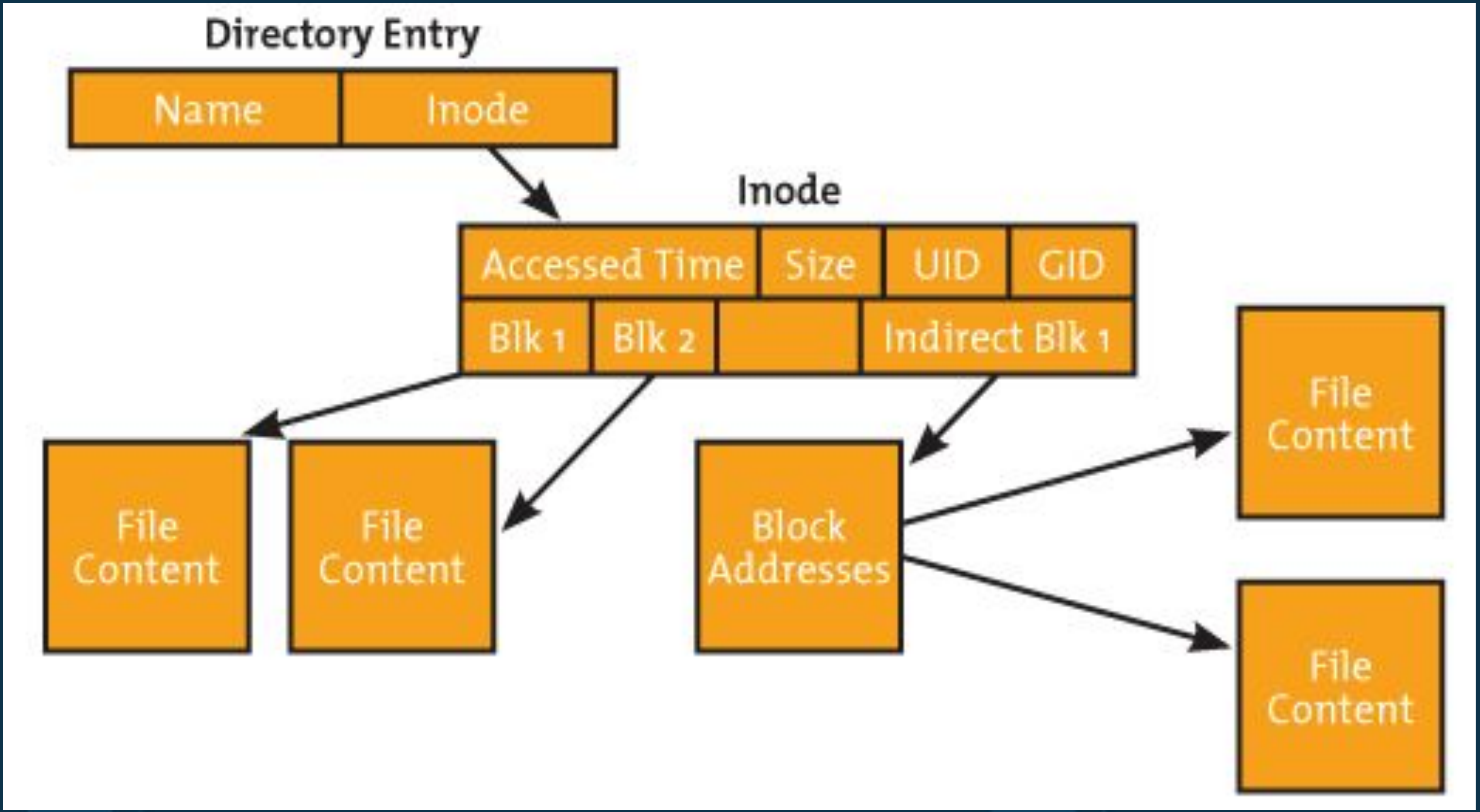
512 bytes

512 bytes

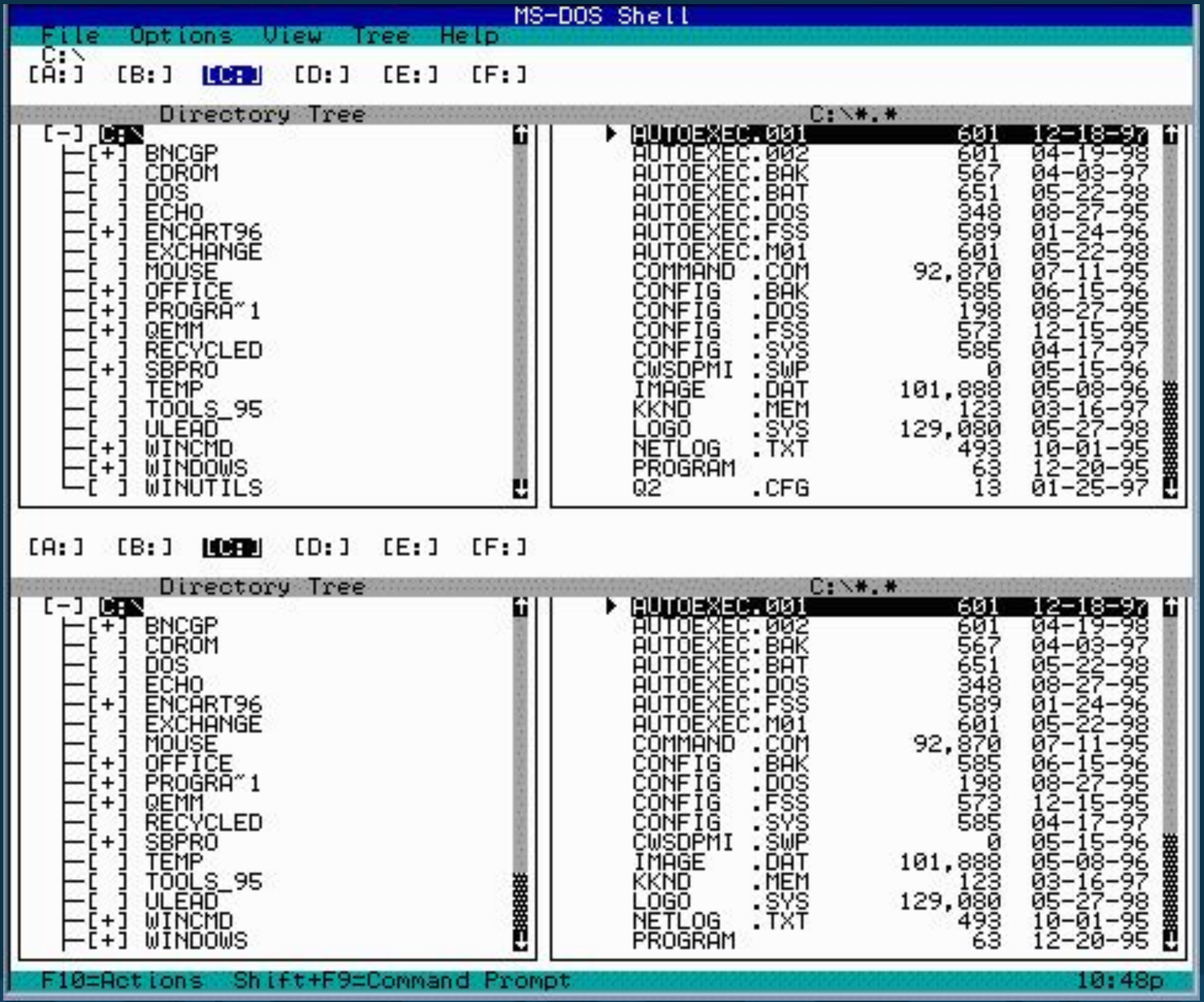
512 bytes

1 block / cluster

Layer 3 - Data



Layer 4 - Metadata



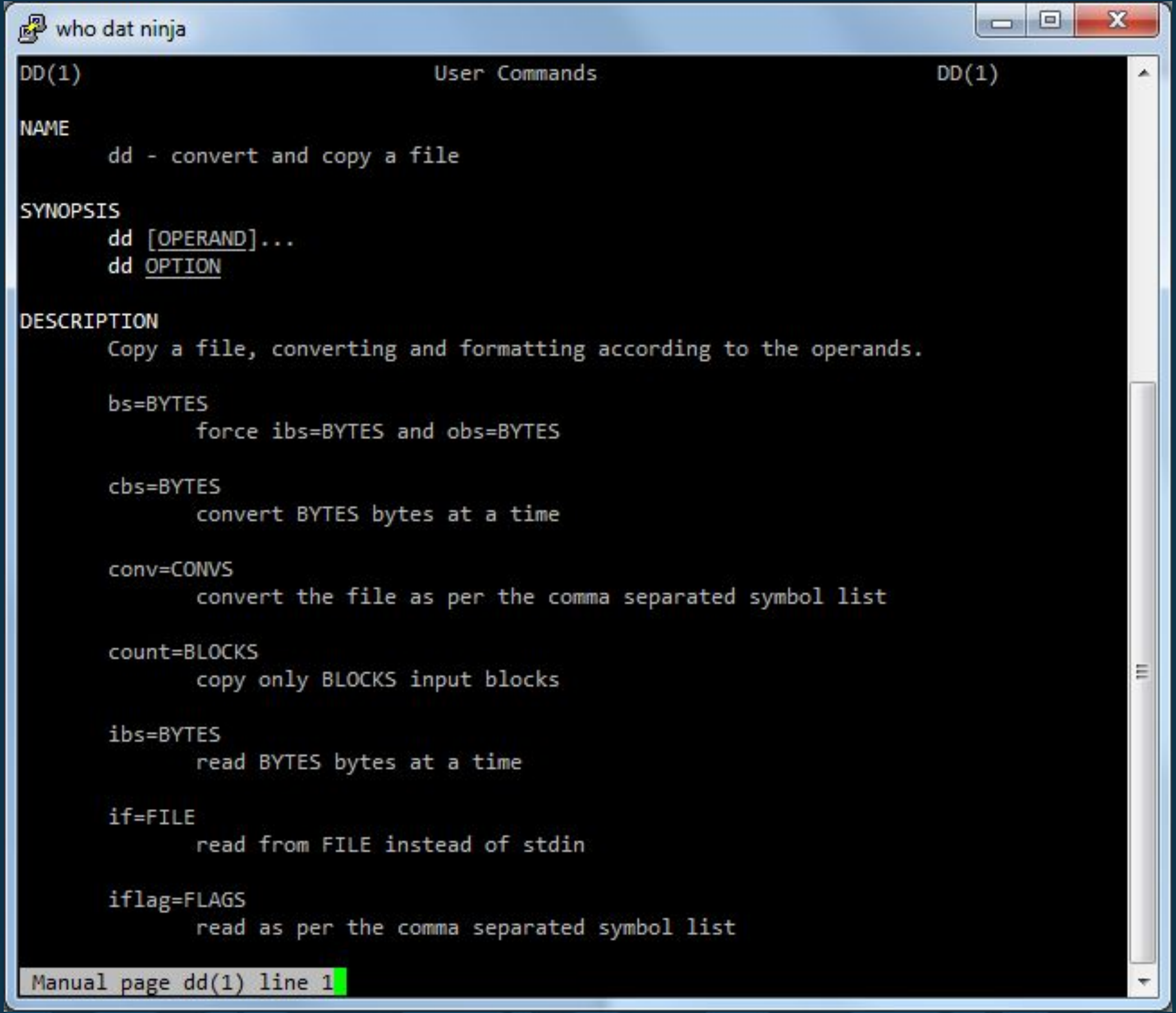
```
                              MS-DOS Shell
  File  Options  View  Tree  Help
  C:\
 [A:]  [B:]  [C:]  [D:]  [E:]  [F:]
          Directory Tree                           C:\*.*
  [-] C:\                              ▶ AUTOEXEC.001       601  12-18-97
    ├─[+] BNCGP                          AUTOEXEC.002       601  04-19-98
    ├─[ ] CDROM                          AUTOEXEC.BAK       567  04-03-97
    ├─[ ] DOS                            AUTOEXEC.BAT       651  05-22-98
    ├─[ ] ECHO                           AUTOEXEC.DOS       348  08-27-95
    ├─[+] ENCART96                       AUTOEXEC.FSS       589  01-24-96
    ├─[ ] EXCHANGE                       AUTOEXEC.M01       601  05-22-98
    ├─[ ] MOUSE                          COMMAND .COM    92,870  07-11-95
    ├─[+] OFFICE                         CONFIG  .BAK       585  06-15-96
    ├─[+] PROGRA~1                       CONFIG  .DOS       198  08-27-95
    ├─[+] QEMM                           CONFIG  .FSS       573  12-15-95
    ├─[ ] RECYCLED                       CONFIG  .SYS       585  04-17-97
    ├─[+] SBPRO                          CWSDPMI .SWP         0  05-15-96
    ├─[ ] TEMP                           IMAGE   .DAT   101,888  05-08-96
    ├─[ ] TOOLS_95                       KKND    .MEM       123  03-16-97
    ├─[ ] ULEAD                          LOGO    .SYS   129,080  05-27-98
    ├─[+] WINCMD                         NETLOG  .TXT       493  10-01-95
    ├─[+] WINDOWS                        PROGRAM             63  12-20-95
    └─[ ] WINUTILS                       Q2      .CFG        13  01-25-97

 [A:]  [B:]  [C:]  [D:]  [E:]  [F:]
          Directory Tree                           C:\*.*
  [-] C:\                              ▶ AUTOEXEC.001       601  12-18-97
    ├─[+] BNCGP                          AUTOEXEC.002       601  04-19-98
    ├─[ ] CDROM                          AUTOEXEC.BAK       567  04-03-97
    ├─[ ] DOS                            AUTOEXEC.BAT       651  05-22-98
    ├─[ ] ECHO                           AUTOEXEC.DOS       348  08-27-95
    ├─[+] ENCART96                       AUTOEXEC.FSS       589  01-24-96
    ├─[ ] EXCHANGE                       AUTOEXEC.M01       601  05-22-98
    ├─[ ] MOUSE                          COMMAND .COM    92,870  07-11-95
    ├─[+] OFFICE                         CONFIG  .BAK       585  06-15-96
    ├─[+] PROGRA~1                       CONFIG  .DOS       198  08-27-95
    ├─[+] QEMM                           CONFIG  .FSS       573  12-15-95
    ├─[ ] RECYCLED                       CONFIG  .SYS       585  04-17-97
    ├─[+] SBPRO                          CWSDPMI .SWP         0  05-15-96
    ├─[ ] TEMP                           IMAGE   .DAT   101,888  05-08-96
    ├─[ ] TOOLS_95                       KKND    .MEM       123  03-16-97
    ├─[ ] ULEAD                          LOGO    .SYS   129,080  05-27-98
    ├─[+] WINCMD                         NETLOG  .TXT       493  10-01-95
    ├─[+] WINDOWS                        PROGRAM             63  12-20-95
  F10=Actions  Shift+F9=Command Prompt                                10:48p
```

Layer 5 - File Name

dd: /dee-dee/ [from IBM {JCL}] vt. Equivalent to {cat} or {BLT}. A UNIX copy command with special options suitable for block-oriented devices. Often used in heavy-handed system abuse, as in "Let's dd the root partition onto a tape, then use the boot PROM to load it back on to a new disk". The UNIX `dd(1)' was designed with a weird, distinctly non-UNIXy keyword option syntax reminiscent of IBM System/360 JCL (which had a similar DD command); though the command filled a need, the design choice looks like somebody's idea of a joke. The slang usage is now very rare outside UNIX sites and now nearly obsolete even there, as `dd(1)' has been {deprecated} for a long time (though it has no replacement). Replaced by {BLT} or simple English `copy'.

Dat s$!# cray!

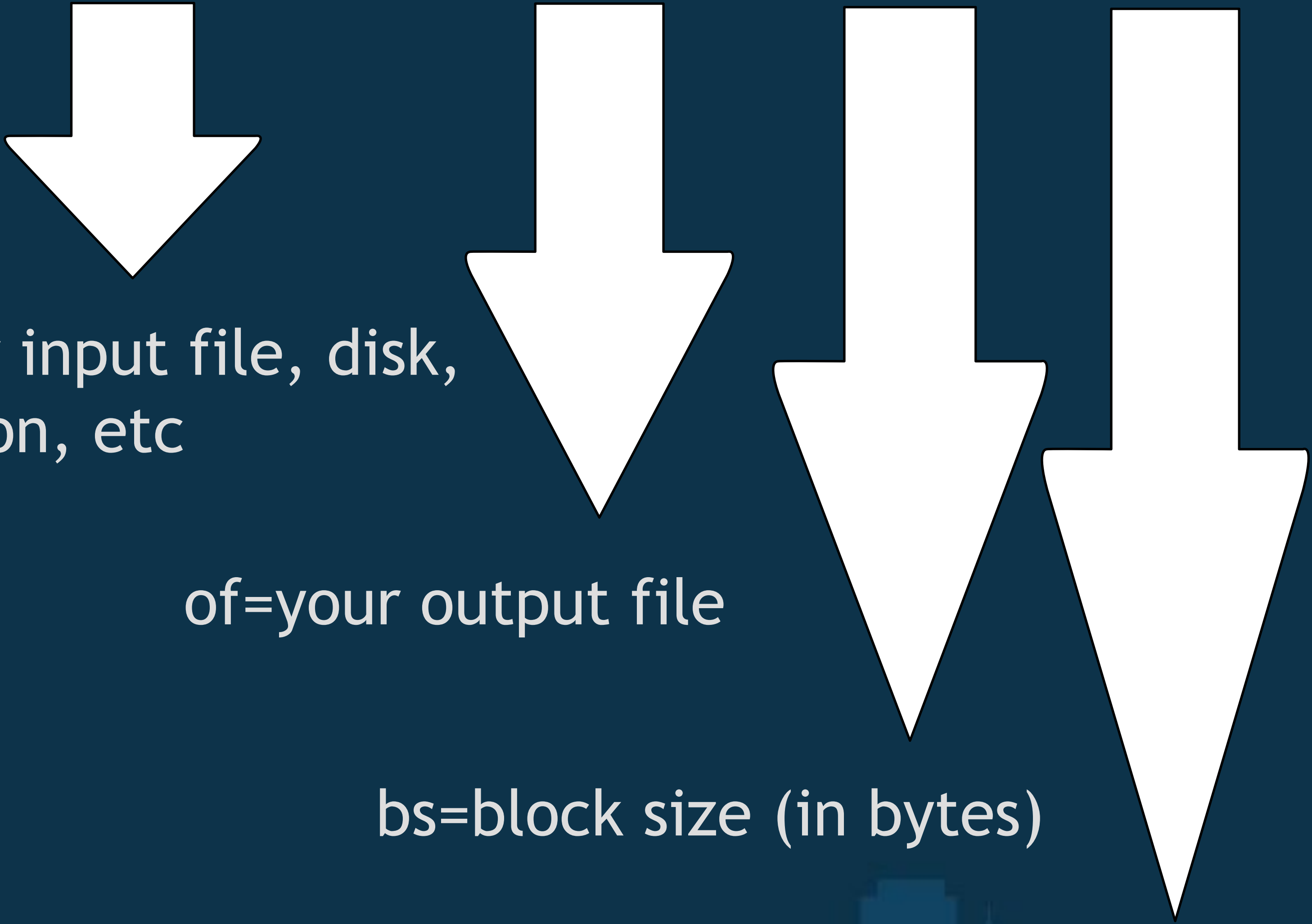
From the Jargon File...



```
DD(1)                         User Commands                        DD(1)

NAME
       dd - convert and copy a file

SYNOPSIS
       dd [OPERAND]...
       dd OPTION

DESCRIPTION
       Copy a file, converting and formatting according to the operands.

       bs=BYTES
              force ibs=BYTES and obs=BYTES

       cbs=BYTES
              convert BYTES bytes at a time

       conv=CONVS
              convert the file as per the comma separated symbol list

       count=BLOCKS
              copy only BLOCKS input blocks

       ibs=BYTES
              read BYTES bytes at a time

       if=FILE
              read from FILE instead of stdin

       iflag=FLAGS
              read as per the comma separated symbol list

 Manual page dd(1) line 1
```

MAN says...

```
$ dd if=/dev/sda of=mbr.img bs=512 count=1
```



if=your input file, disk, partition, etc

of=your output file

bs=block size (in bytes)

count=how many blocks to copy

Input/output files in UNIX/Linux/BSD

Can be a path...

```
$ dd if=/home/jwhall/file.img
```

Or a partition...

```
$ dd if=/dev/sdb2
```

Or a disk...

```
$ dd if=/dev/sdb
```

Or, STDIN / STDOUT

```
$ dd if=/dev/sdb | xxd
```

Input/output files in Windows

Can be a path...

```
C:\>dd.exe if=C:\autoexec.bat
```

Or a partition...

```
C:\>dd.exe if=\Device\Harddisk0\Partition1
```

Or a disk...

```
C:\>dd.exe if=\\.\PhysicalDrive0
```

Or, STDIN / STDOUT

```
C:\>dd.exe if=\\.\PhysicalDrive0 | <hex editor>
```

The CONV flag

```
$ dd if=/dev/sda of=./sda.img bs=4096 conv=noerror,sync
```

CONV options:

noerror: don't quit if you encounter an error on the disk

sync: pad blocks so that the output size matches the input

ucase/lcase: change lowercase to uppercase (& vice versa)

notrunc: if the output file already exists, and what you're dumping is smaller, leave the remainder alone

DD across a network

*nix

```
jw@host-a:~$ nc -l -p 7777 > ./disk.img

jw@host-b:~$ dd if=/dev/sda bs=4096 | nc -w 3 host-a 7777
```

Windows

```
C:\> dd.exe if=\Device\Harddisk0\Partition1 of=\\host-a\c$\disk.img
```

Other common uses...

Write zeroes or random data to a drive:

```
$ dd if=/dev/zero of=/dev/sdc bs=1M
$ dd if=/dev/urandom of=/dev/sdc bs=1M
```

Make a copy of an optical disc:

```
$ dd if=/dev/cdrom of=./windows-7-ultimate.iso
```

Fix a file with errors:

```
$ dd if=old_busted.avi of=new_hotness.avi conv=noerror
```

Other DD's

Win32dd / Win64dd can dump Windows' memory to a file
http://www.moonsols.com/windows-memory-toolkit/

dc3dd can create hashes and log its activity
http://sourceforge.net/projects/dc3dd/

don't leave your disk around
me
true playa for real,
i run dd

Questions?

Stupid DD tricks!