Acquiring Forensic Evidence: Imaging

Dr. Philip Craiger
College of Engineering Technology
Daytona State College

Drive Information

- A good way to find out how many drives are installed are
  - Open up the case and LOOK, or
  - From a dormant machine, pop-in your Linux-boot forensic CD.
  - Configure the BIOS so that the CD boots before the hard drive
    - Better, unplug the power cable from the hard drive so that it can't boot
  - Use Linux utilities to do some investigation without affecting the system

HD Information You need

```
[root@whammo root]# /sbin/fdisk -l

Disk /dev/hda: 255 heads, 63 sectors, 9729 cylinders
Units = cylinders of 16065 * 512 bytes

   Device Boot    Start       End    Blocks   Id  System
/dev/hda1   *         1      6374  51199123+   c  Win95 FAT32 (LBA)
/dev/hda3          6375      6384     80325   83  Linux
/dev/hda4          6385      9729  26868712+   f  Win95 Ext'd (LBA)
/dev/hda5          6385      8296  15358108+  83  Linux
/dev/hda6          8297      8394    787153+  82  Linux swap
/dev/hda7          8395      9729  10723356    b  Win95 FAT32

Disk /dev/hdb: 128 heads, 63 sectors, 787 cylinders
Units = cylinders of 8064 * 512 bytes

   Device Boot    Start       End    Blocks   Id  System
/dev/hdb1   *         1       520   2096608+   6  FAT16
```

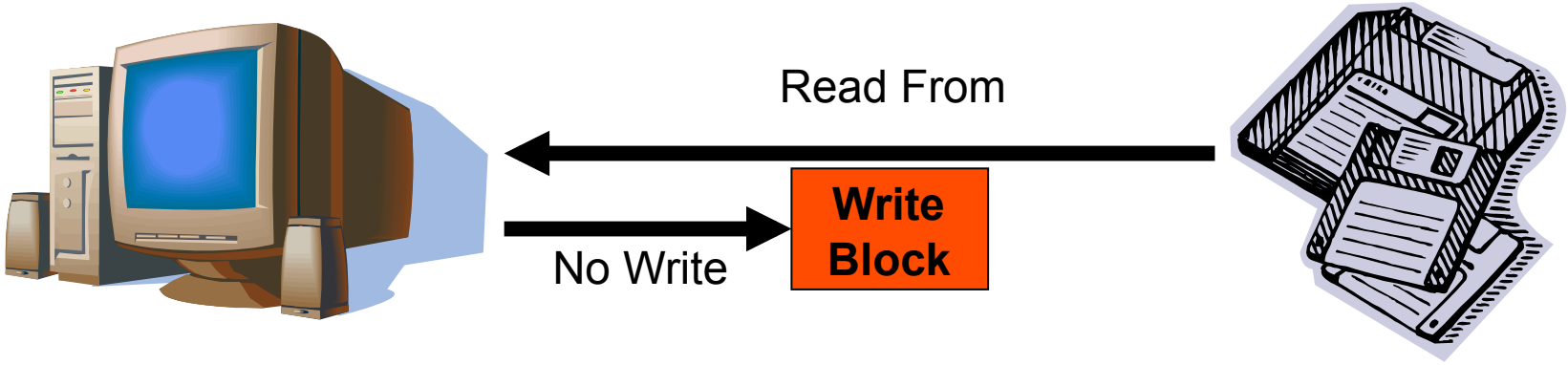
Write this information down! or Save copy to USB or floppy.

Windows or Linux

- You can use either but there are different ramifications
- Remember the #1 rule: **Don't change the evidence**
- You want to be able to image and/or mount the hard drive without affecting its contents
- How do you do that?

Windows or Linux

- If you go the Windows route, you will need a PHYSICAL WRITE-BLOCKER
  - This is typically a physical device that fits between the HD and the computer

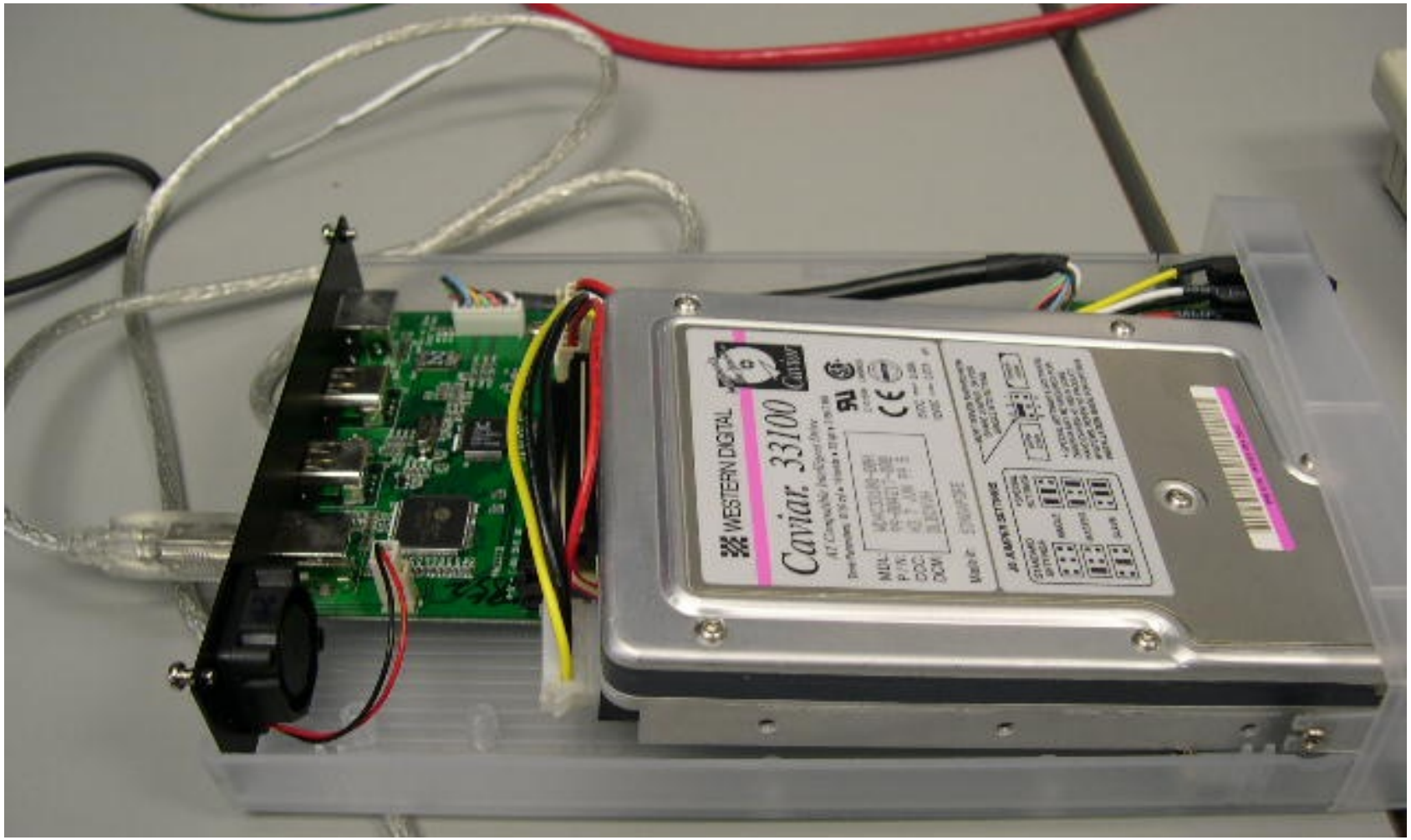


  - Allows read but not write access to HD
  - Essentially stops any signals from Interrupt 13 from being transmitted to the HD.

Windows or Linux

- Linux is more flexible
- However, some bootable Linux distributions automatically mount drives! Be careful…
- Linux allows you to
  - Connect and duplicate the HD without mounting
  - Mount an image Read-Only for logical analysis
- Most forensics books speak of Linux as a required tool (preferred?) for forensics toolbox

External Harddrive Connection



Drive Information

- How is the drive setup?
  - What type of file system?
    - NTFS
    - FAT16
    - FAT32
    - EXT2
    - ReiserFS
  - More than one partition?
  - More than one HD?
  - Which HD boots?

Linux Utilities

- **fdisk** is a menu driven program for creation and manipulation of partition tables.
  - # fdisk <device> provides you information on the parition/volume
- *device* is usually one of the following:
  - /dev/hda or /dev/hdb or /dev/sda or /dev/sdb
    - (/dev/hd[a-h] for IDE disks
    - /dev/sd[a-p] for SCSI disks
    - /dev/ed[a-d] for ESDI disks
    - /dev/xd[ab] for XT disks).

Linux Utilities

- A device name refers to the entire disk.
  - /dev/hda is IDE hard drive A
  - /dev/hdb is IDE hard drive B
  - /dev/sda is SCSI hard drive A
  - /dev/hda1 is the first partition on IDE hard drive A
  - /dev/sdb5 is the fifth partition on SCSI hard drive B
  - /dev/fd0 is the floppy
  - /dev/cdrom is the cdrom
  - /dev/cdrom1 is the second cdrom

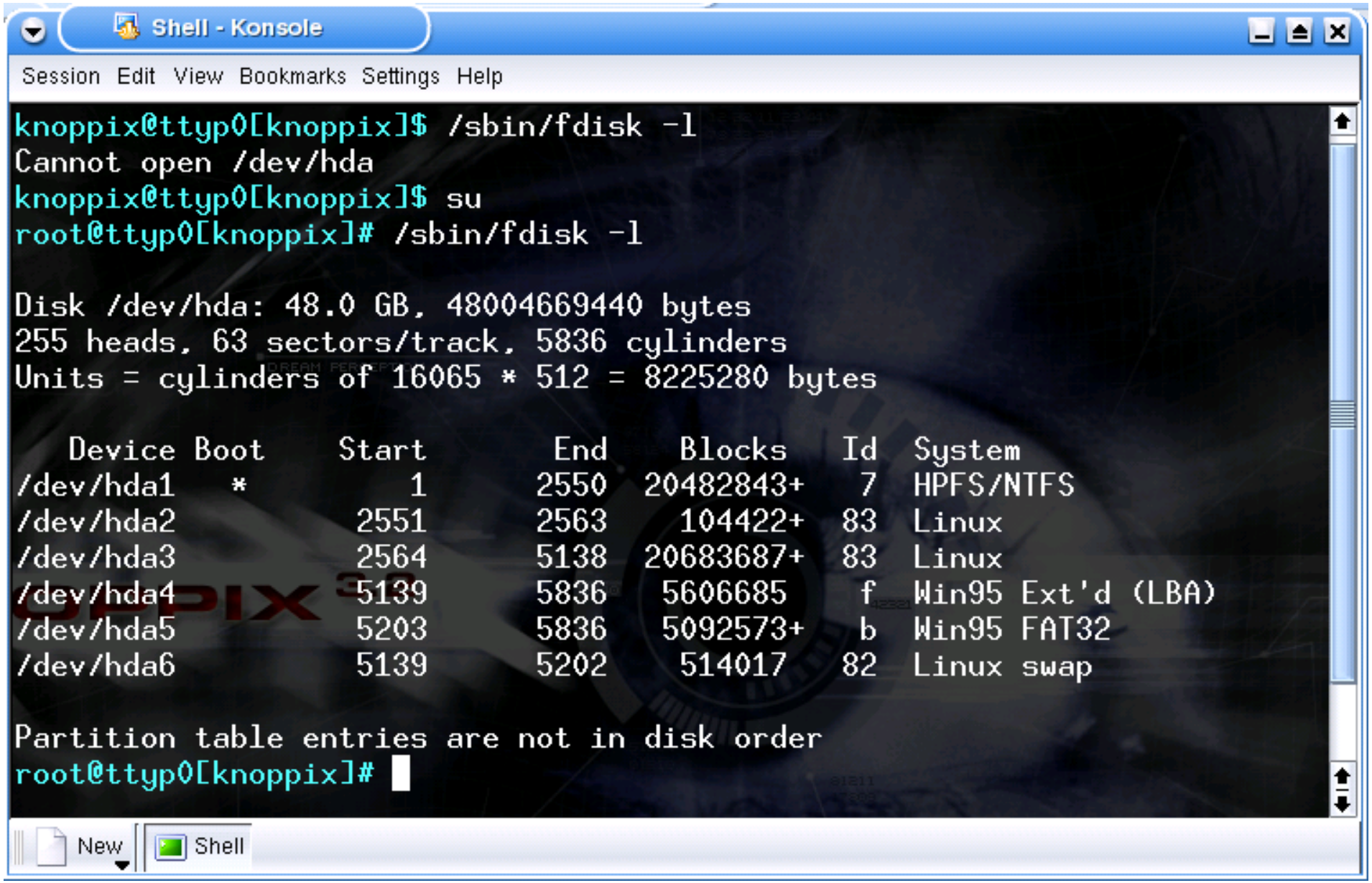
/sbin/fdisk

- **-b** *sectorsize*
  - Specify the sector size of the disk. Valid values are 512, 1024, or 2048. (Recent kernels know the sector size. Use this only on old kernels or to override the kernel's ideas.)
- **-l**
  - List the partition tables for the specified devices and then exit. If no devices are given, those mentioned in */proc/partitions* (if that exists) are used.
- **-u**
  - When listing partition tables, give sizes in sectors instead of cylinders.
- **-s** *partition*
  - The *size* of the partition (in blocks) is printed on the standard output.
- **-v**
  - Print version number of **fdisk** program and exit.

How-to with Linux Bootable

- From dormant machine
  - Take out the suspect HD
    - Why?
  - Insert bootable CD (e.g., Knoppix or FIRE)
  - As machine boots up you need to ensure the order of boot.
    - Do so by getting into the BIOS setup program
  - Knoppix will boot if CD is set to boot before HD
  - Once Knoppix has booted, open a terminal window
  - Run “sudo /sbin/fdisk –l”

Knoppix-STD Bootable Forensic CD



Forensic Image Duplication

- There are numerous ways to perform bit-level duplication
  - Commercial applications
    - Symantec Ghost
    - Safeback
    - EnCase
  - Freeware
    - dd
- The commercial utilities are fast, some use a a proprietary format (e.g., EnCase).
- We will use dd, the UNIX/Linux utility

Standard dd command line options

- # dd if=/dev/hda1 of=/mnt/suspect.dd bs=1M
- Options
  - # if=
    - Input file
  - # of=
    - Output file
  - # bs=
    - Specifies the block size, how much data to transfer in one operation
  - # count=
    - How many blocks to transfer
  - # skip=
    - Specifies the number of blocks to skip at the beginning of the file
  - # conv=
    - Data conversion

At prompt, type ‘man dd’

dd for Windows

- Difference in command line arguments
- Physical drive syntax
  - \\.\PhysicalDrive?
  - Where ? is a drive number: 0, 1, 2, etc.
  - \\. Represents the local machine
- Logical Volume
  - Need logical volume name (see volume_dump later).

Different dd Syntax per OS

	UNIX	Windows
Logical	/dev/hdb1	\\.\f: (or volume name)
Physical	/dev/hdb	\\.\PhysicalDrive0

dd for Windows

- Version by Garner has more options than the standard UNIX/Linux version.
  - dd.exe
    - if=\\.\PhysicalDrive0
    - of=d:\evidence\PhysicalDrive0.img
    - --md5sum
    - --verifymd5
    - --md5out = a:\PhysicalDrive0.img.md5
  - Bit-image drive 0 (hda or sda) to d:\evidence, calculate the md5, verify that they are the same, and write it out the a floppy.

References

- Schulz & Shumway (2002). *Incident response*. New Riders.
- U.S. Secret Service. *Best Practices for Seizing Electronic Evidence, version 3.*
- *All the man files for dd, netcat, etc.*