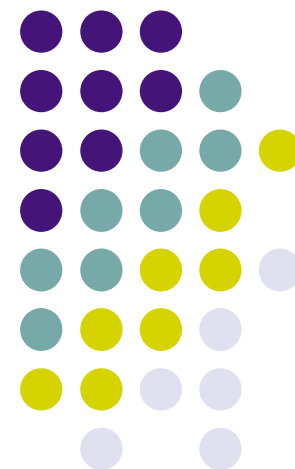


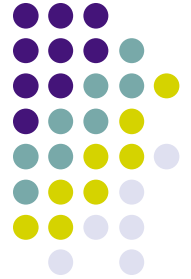
An Introduction to Linux as a Tool for Digital Investigation and Analysis

Chris Marberry / Paul Burke
National Center for Forensic Science

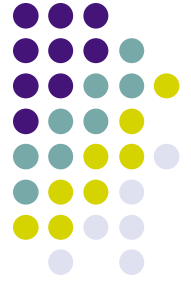
Part 2



What Free Software can do for you!

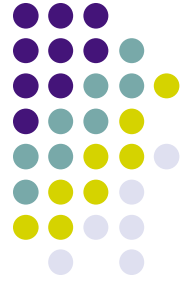


- Accessing hard drives/partitions
- Detect deleted files
- Repair broken partition tables



Accessing a Hard Drive

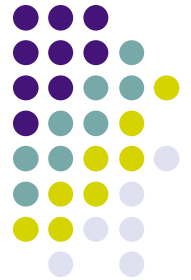
- Mount command
 - Perform as 'root'
- Again, everything in Linux is a file
 - Hard drives are located off of the /dev directory
 - hda is used for an IDE hard drive
 - sda would be used for a SCSI drive.
 - hda1 would be the first partition on the first drive
 - hdb4 would be the fourth partition on the second drive



Accessing a Hard Drive

- How do you tell what drives are accessible?
- Use the fdisk command
 - fdisk -l
 - Lists the accessible drives on the system
 - This includes IDE, SCSI, USB, SAN, and many more types of storage.

fdisk

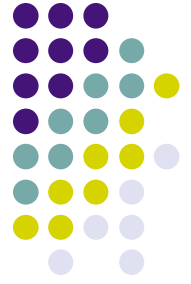


```
root@1[~]# fdisk -l

Disk /dev/hda: 40.0 GB, 40020664320 bytes
255 heads, 63 sectors/track, 4865 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes

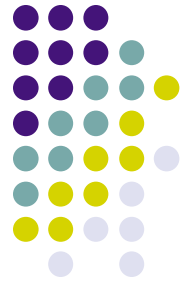
   Device Boot      Start         End      Blocks   Id  System
/dev/hda1    *          1         4864    39070048+   7  HPFS/NTFS

root@1[~]#
```



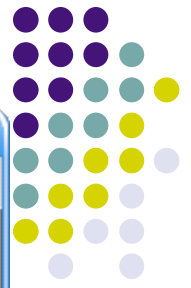
So you have a bad MBR

- What happens when someone overwrites their MBR?
- Typically, you have to reinstall everything to get a usable system right?
- Lets take a look at gpart!



gpart

- This program examines the hard drive to ‘**G**uess the **P**artition layout’
- Run the program to see what it concludes:
 - Ex: `gpart /dev/hda`
- If its results look good add the ‘-W’ flag to write the changes to the hard drive.



```
Shell - Konsole
Session Edit View Bookmarks Settings Help
root@1[knoppix]# gpart /dev/hda

Begin scan...
Possible partition(Windows NT/W2K FS), size(38154mb), offset(0mb)

* Warning: short read near sector(78165171), 64512 bytes instead of 66048. Skip
ping...
End scan.

Checking partitions...
Partition(OS/2 HPFS, NTFS, QNX or Advanced UNIX): primary
Ok.

Guessed primary partition table:
Primary partition(1)
  type: 007(0x07)(OS/2 HPFS, NTFS, QNX or Advanced UNIX)
  size: 38154mb #s(78140097) s(63-78140159)
  chs: (0/1/1)-(1023/15/63)d (0/1/1)-(77519/15/63)r

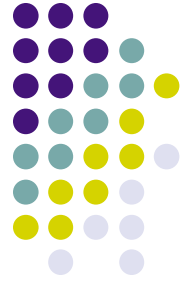
Primary partition(2)
  type: 000(0x00)(unused)
  size: 0mb #s(0) s(0-0)
  chs: (0/0/0)-(0/0/0)d (0/0/0)-(0/0/0)r

Primary partition(3)
  type: 000(0x00)(unused)
  size: 0mb #s(0) s(0-0)
  chs: (0/0/0)-(0/0/0)d (0/0/0)-(0/0/0)r

Primary partition(4)
  type: 000(0x00)(unused)
  size: 0mb #s(0) s(0-0)
  chs: (0/0/0)-(0/0/0)d (0/0/0)-(0/0/0)r
```

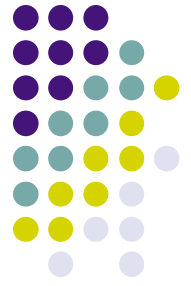
Shell





How to Mount a Hard Drive

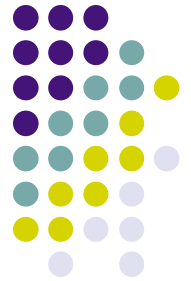
- Example:
 - `mount <item to mount> <mount point>`
 - To mount read-only:
 - `mount -o ro /dev/hda1 /mnt/harddrive`
 - What if you have an image of a drive?
 - `mount -o loop image.dd /mnt/harddrive`



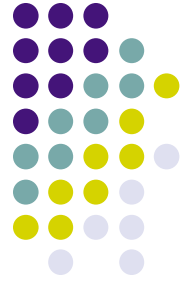
Neat Trick

- You can mount more than one item to the same location
- What does this mean?
- Run the 'mount' command with no parameters to see what is mounted on the system!

Hiding in Plain Sight

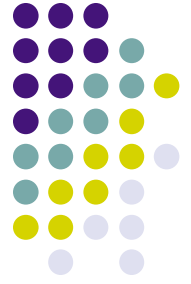


```
Shell - Konsole
Session Edit View Bookmarks Settings Help
root@1[test]# pwd
/root/test
root@1[test]# ls
file.txt
root@1[test]# cd ..
root@1[~]# mount -o loop image.dd test/
root@1[~]# cd test/
root@1[test]# ls
root@1[test]# mount
/dev/root on / type ext2 (rw)
/dev/hdc on /cdrom type iso9660 (ro)
/dev/cloop on /KNOPPIX type iso9660 (ro)
/ramdisk on /ramdisk type tmpfs (rw,size=193648k)
/UNIONFS on /UNIONFS type unionfs (rw,noatime,dirs=/ramdisk=rw:/KNOPPIX=ro)
/dev/pts on /dev/pts type devpts (rw)
/proc/bus/usb on /proc/bus/usb type usbfs (rw,devmode=0666)
automount(pid2236) on /mnt/auto type autofs (rw,fd=4,pgrp=2236,minproto=2,maxproto=4)
/UNIONFS/root/image.dd on /UNIONFS/root/test type vfat (rw,loop=/dev/loop0)
root@1[test]#
```



Acquiring an Image

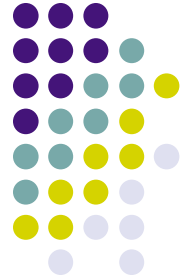
- Most common Unix application for imaging is dd
- dd's only purpose is to read and write bits
- Can image from partition to another; one disk to another; even from one computer to another



DD continued

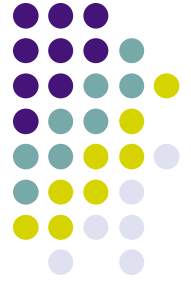
- Usage:
 - `dd if=<target> of=<target> [additional options]`
 - `if` stands for Input File, i.e., What is the source?
 - `of` stands for Output File, i.e., What is the destination?
 - Additional options...

DD Example

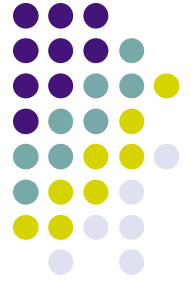
A screenshot of a terminal window titled "Shell - Konsole". The window has a menu bar with "Session", "Edit", "View", "Bookmarks", "Settings", and "Help". The terminal prompt is "knoppix@1[knoppix]\$". The command entered is "dd if=/dev/hda1 of=/mnt/storage/image.dd bs=1M conv=noerror,notrunc". The background of the terminal is a dark image with the text "LINUX IN USE" in a stylized font. The window has standard Linux window controls (minimize, maximize, close) in the top right corner and a taskbar at the bottom with a "Shell" icon.

```
knoppix@1[knoppix]$ dd if=/dev/hda1 of=/mnt/storage/image.dd bs=1M conv=noerror,notrunc
```

The Network Swiss Army Knife

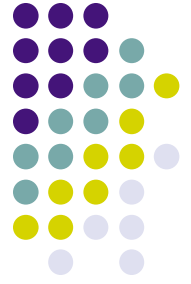


- Netcat is a truly versatile utility
- Functions similarly to dd
- Say you want to acquire a hard drive image but all you have is a network connection
- Simple!



Netcat

- Make their computer a client
`dd if=/dev/hda | nc 10.0.0.1 11 -w 3`
- Make your computer a server
`nc -l -p 11 | dd of=/acquired.image.dd`
- Presto!



Reminder: Hashing

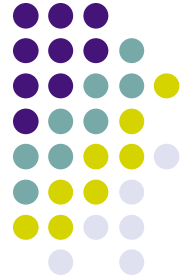
- Don't forget to always hash
 - Make sure to hash the source and destination!
 - md5 is the norm, but sha1 or even sha256 should be used
 - You can even use nc!
`md5sum /dev/hda | nc 10.0.0.1 11 -w 3`



Recovering Deleted files

- Sleuthkit is a tool framework for analyzing and recovering data
- Comprised of many small utilities that each accomplish one task

Sleuthkit



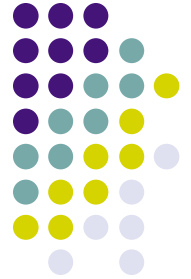
- Some of the programs
 - fsstat
 - fls
 - ils
 - icat
 - etc...

Fsstat



- fsstat is used to analyze an image
 - This tells you the:
 - Filesystem type
 - Filesystem layout
 - Volume ID
 - Volume serial number

fsstat



```
Shell - Konsole <2>
Session Edit View Bookmarks Settings Help
root@2[bin]# ./fsstat -f fat image.dd
FILE SYSTEM INFORMATION
-----
File System Type: FAT12
DEM Name: mkdosfs
Volume ID: 0x42dab76b
Volume Label (Boot Sector):
Volume Label (Root Directory):
File System Type Label: FAT12

Sectors before file system: 0

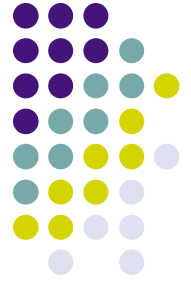
File System Layout (in sectors)
Total Range: 0 - 199
* Reserved: 0 - 0
** Boot Sector: 0
* FAT 0: 1 - 1
* FAT 1: 2 - 2
* Data Area: 3 - 199
** Root Directory: 3 - 34
** Cluster Area: 35 - 198
** Non-clustered: 199 - 199

METADATA INFORMATION
-----
Range: 2 - 2626
Root Directory: 2

CONTENT INFORMATION
-----
Sector Size: 512
Cluster Size: 2048
Total Cluster Range: 2 - 42

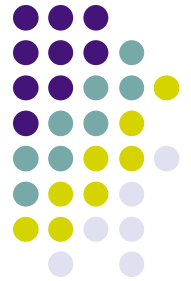
FAT CONTENTS (in sectors)
-----
```

fls

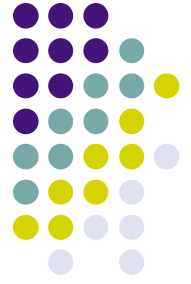


- Analyzes an image to report information about file
 - Allows easy identification of files in unallocated space
 - Use the '-d' flag to show deleted files

fls



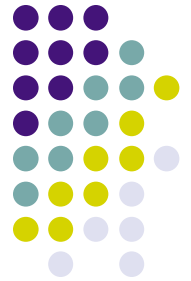
```
Shell - Konsole <2>
Session Edit View Bookmarks Settings Help
root@2[bin]# mount -o loop image.dd /ramdisk/home/knoppix/mount/
root@2[bin]# ls
dcalc      dls      fls      ifind     istat     md5       sigfind
dcat       dstat   fsstat   ils       jcat      mmls     sorter
disk_sreset ffind   hfind   image.dd  jls       mmstat   srch_strings
disk_stat  file    icat    img_stat  mactime   sha1
root@2[bin]# cp md5 /ramdisk/home/knoppix/mount/
root@2[bin]# rm /ramdisk/home/knoppix/mount/md5
rm: remove regular file `/ramdisk/home/knoppix/mount/md5'? y
root@2[bin]# umount /ramdisk/home/knoppix/mount
root@2[bin]# ./fls -f fat -d image.dd
r/r * 4:      _D5
root@2[bin]#
```



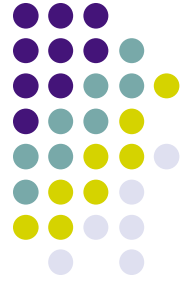
ils

- This tool is used to list inode numbers
- What is an inode?
 - Keeps track of file types
 - Permissions
 - Number of links
 - Owner and group
 - Size of the file
 - When it was last modified

ils example



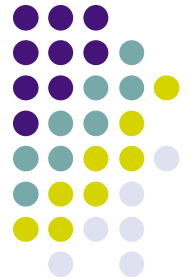
```
root@localhost:~  
File Edit View Terminal Tabs Help  
[root@localhost ~]# ils -f fat image.dd  
class|host|device|start_time  
ils|localhost.localdomain||1121732577  
st_ino|st_alloc|st_uid|st_gid|st_mtime|st_atime|st_ctime|st_mode|st_nlink|st_size|st_block0|st_block1  
4|f|0|0|1121732368|1121659200|1121732368|100777|0|0|0|0  
[root@localhost ~]#
```



icat

- icat copies the specified inode from specified source
- So with the information given from ils you can extract the deleted file

icat example



```
root@localhost:~  
File Edit View Terminal Tabs Help  
[root@localhost ~]# icat -f fat image.dd 4 > recovered,file  
[root@localhost ~]# ls -l recovered,file  
-rw-r--r-- 1 root root 20 Jul 18 20:27 recovered,file  
[root@localhost ~]# file recovered,file  
recovered,file: ASCII text  
[root@localhost ~]# cat recovered,file  
this is a text file  
[root@localhost ~]#
```

Autopsy



- A graphical front end for using the Sleuthkit tools.
- Quite like using FTK or Encase, except where they differ.

Autopsy Forensic Browser - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://localhost:9999/autopsy

Red Hat, Inc. Red Hat Network Support Shop Products Training

WARNING: Your browser currently has Java Script enabled.

You do not need Java Script to use Autopsy and it is recommended that it be turned off for security reasons.

Autopsy Forensic Browser 2.05



<http://www.sleuthkit.org/autopsy/>

OPEN CASE NEW CASE HELP

Done



Create A New Case - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://localhost:9999/autopsy?mod=0&v

Red Hat, Inc. Red Hat Network Support Shop Products Training

CREATE A NEW CASE

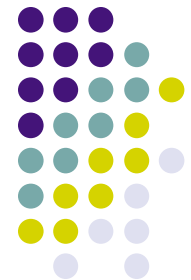
1. **Case Name:** The name of this investigation. It can contain only letters, numbers, and symbols.

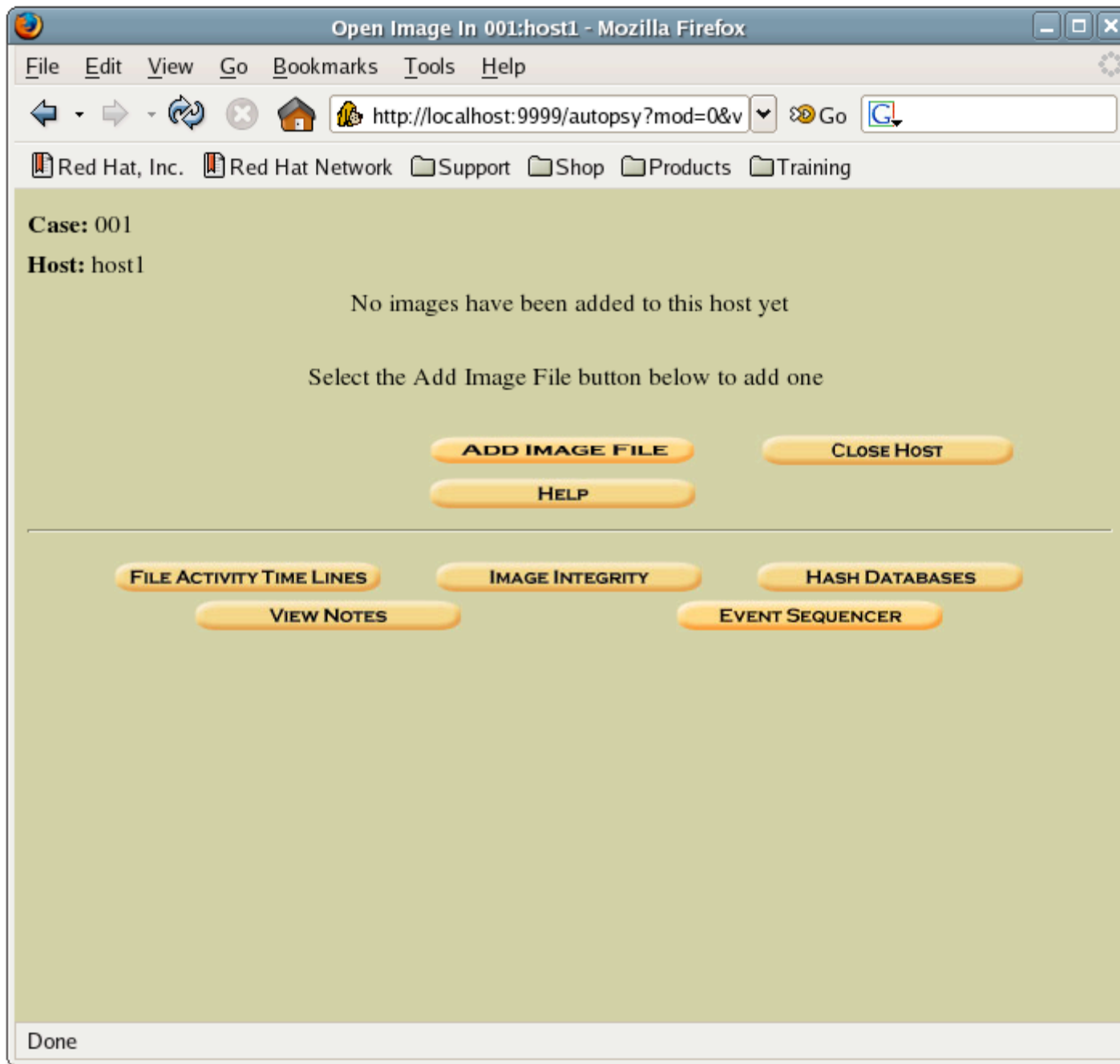
2. **Description:** An optional, one line description of this case.

3. **Investigator Names:** The optional names (with no spaces) of the investigators for this case.

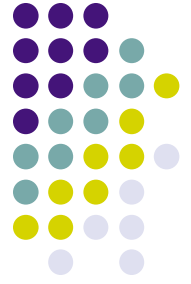
a.	<input type="text" value="Chris Marberry"/>	b.	<input type="text" value="Paul Burke"/>
c.	<input type="text"/>	d.	<input type="text"/>
e.	<input type="text"/>	f.	<input type="text"/>
g.	<input type="text"/>	h.	<input type="text"/>
i.	<input type="text"/>	j.	<input type="text"/>

Done

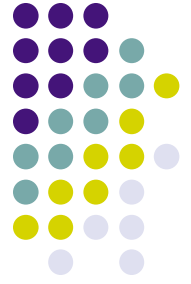




Knoppix

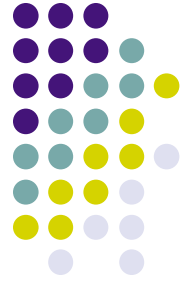


- Linux boot CD
- Very useful for
 - repairing
 - recovery
 - acquisition



Boot Parameters

- What are boot parameters
- Why are they useful
 - Lots of different configurations
 - Customization may be needed



Boot Parameters

- Common parameters for knoppix
 - Boot to cli: “knoppix 2”
 - Enable DMA “knoppix dma”
 - Disable ACPI “knoppix noacpi”
 - Disable DDC detection “knoppix skipddc”

Thank you for your time.

Questions? Comments?

Feel free to ask!

