# Forensics with Linux 101 or How to do Forensics for Free

## **Chuck Willis**

chuckfwillis@netscape.net

Black Hat USA 2003 31 July 2003

# Agenda

## Introduction

- About using Linux for Forensics
- Preparations
- Pre-imaging
- Imaging
- Preparing the analysis system
- Conducting analysis
- Conclusion

## About me

- I have done a lot of computer forensics using commercial tools
- I have not written any computer forensic tools
- I do not work for any company that sells computer forensic tools
- I am here representing only myself

## About this presentation

- Feel free to ask questions at any time
- I have not done exhaustive testing on any of these tools and they:
  - May not work properly under all circumstances
  - May contain viruses or Trojans
- Use these tools at your own risk
- I will present the features and limitations of tools as I understand them

# More on this presentation

- Doing computer forensics with Linux is not the best solution for everyone
- I assume that everyone here is at least somewhat familiar with Linux and using the command line
- I will speak about imaging and analyzing an IDE hard disk, but most of the techniques can be used to image other media as well
- I will only be discussing dead-disk forensics

# Agenda

- Introduction
- About using Linux for Forensics
- Preparations
- Pre-imaging
- Imaging
- Preparing the analysis system
- Conducting analysis
- Conclusion

# What is good about using Linux for forensics?

- Most tools are free of charge
- Most tools are open source
  - Allows you to know exactly what the tool is doing
  - See "Open Source Digital Forensic Tools: The Legal Argument" by Brian Carrier (author of The Sleuth Kit) at www.atstake.com/research/reports/acrobat/ atstake\_opensource\_forensics.pdf.
- Environment is very flexible
- When tools are used properly, evidence should stand up in court

# What are the limitations of using Linux for forensics?

- Most tools are free you don't get any tech support and may not be able to call the author in to court if necessary
- Most tools are open source, which allows those who oppose you in court to scour the code for bugs and try to call the tool into question
- Environment is very flexible it is often difficult to decide what is the best way to do something and there are no universally accepted standard procedures

## Limitations continued

- Free tools are not as full featured as commercial packages or iLook
- Tools are significantly more complicated to use than commercial packages and most involve using the command line
- In many operations, especially when imaging, you can destroy your work or even your original evidence with a typo

## Linux and Odd Sized Drives

- You will probably never, ever see a drive with an odd number of sectors
- Linux cannot see the last sector on hard drives with an odd number of sectors
- If you come across an odd-sized drive, use a BSD variant to image

# Agenda

- Introduction
- About using Linux for Forensics
- Preparations
- Pre-imaging
- Imaging
- Preparing the analysis system
- Conducting analysis
- Conclusion

# **Computer Systems**

- Forensic Analysis System running Linux
- Imaging System that boots to F.I.R.E. Boot CD – can be the same as one of the other systems
- Evidence Hard Drive running any operating system
- Image Hard Drive which will be formatted ext3

# The F.I.R.E. Boot CD

- Forensic and Incident Response Environment by William Salusky
- Download and burn F.I.R.E. Boot CD from fire.dmzs.com
- Does not mount partitions
- Designed for Forensics and Incident Response
- By default uses bash with "vi" style editing change to emacs style by typing set -o emacs (must be done in each shell opened)

## F.I.R.E. Alternatives

- Knoppix older versions had evidence contamination issues (uses Linux swap partition)
- Penguin Sleuth modified version of Knoppix for forensics
- Others not designed or tested for forensics

# **Preparing for Imaging**

- Using HD label or model information from manufacturer's Web site, note size and total number of sectors for this drive
- Wipe and format a very large drive (Image Drive) using ext3 file system (> 3x evidence size)
  - Wipe drive with dcfldd if=/dev/zero of=/dev/hda bs=8k conv=noerror,sync
  - Create a partition with fdisk /dev/hda
  - Reboot
  - Format with mkfs -t ext3 /dev/hda1
  - Can be done with F.I.R.E. boot CD or normal Linux system

# **Preparing for Imaging**

- Mount evidence drive read-write (mount /dev/hda1 /mnt/hda1)
- Create directory on the evidence drive for this case mkdir /mnt/hda1/case\_no
- Create a subdirectory under that for this piece of evidence mkdir /mnt/hda1/ case\_no/evidence\_no

# Create a text file about the case

- General information about the case:
  - Your name and organization
  - Case number or other identifier
  - Date
  - General information about the case

# Create a separate text file about this piece of media

- Include information about this case and all identifying information about this media:
  - Your name and organization
  - Case number or other identifier for this job
  - Evidence number assigned to this HD
  - Date and time image will be made
  - Make, model, and serial number of computer
  - IP and hostname of computer
  - Make, model, and serial number of HD
  - Where HD came from and why you are looking at it

# Agenda

- Introduction
- About using Linux for Forensics
- Preparations
- Pre-imaging
- Imaging
- Preparing the analysis system
- Conducting analysis
- Conclusion

## Connect evidence

- Connect Evidence Drive and Image Drive to Imaging System
- Ensure that Master/Slave/Cable Select jumper(s) are correct
- Ensure BIOS is set to boot from CD only

# Getting Started with F.I.R.E.

## • Boot to F.I.R.E.

- F.I.R.E. can boot in X-Windows or Console mode
- I prefer console (boot option 1) because there is less going on with the system
- When booting to console mode, a menu is displayed
- Change to another VT (Ctrl-Alt-F2) and type everything on the command line
- Log in as root the root password is "firefire"

# Do not mount evidence partitions

- Known issue in mounting journaling filesystems – updates journal count
  - ext3
  - ReiserFS

# Figure out which hard drive is which

- dmesg | grep hd
- Note which hard drive (/dev/hda, /dev/hdb, /dev/hdc, or /dev/hdd) your evidence hard drive and which is the image hard drive

bash# dmesg | grep hd

ide0: BM-DMA at 0xff00-0xff07, BIOS settings: hda:DMA, hdb:DMA

ide1: BM-DMA at 0xff08-0xff0f, BIOS settings: hdc:DMA, hdd:DMA hda: WDC WD300AB-00BVA0, ATA DISK drive

hdc: IBM-DTTA-371440, ATA DISK drive

hdd: SONY CD-RW CRX175E2, ATAPI CD/DVD-ROM drive

hda: 58633344 sectors (30020 MB) w/2048KiB Cache, CHS=3649/255/63

hdc: 28229040 sectors (14453 MB) w/462KiB Cache, CHS=28005/16/63

hdd: ATAPI 40X CD-ROM CD-R/RW drive, 2048kB Cache

(...)

# Figure out which hard drive is which

- For this example I assume image HD is /dev/hdc and evidence is /dev/hda. IT IS VERY IMPORTANT TO KEEP THESE DEVICE NAMES STRAIGHT!
- Mount the image hard drive read-write mount /dev/hdc1 /mnt/hdc1
- Change to your directory for this piece of evidence cd /mnt/hdc1/case\_no/evidence\_no
- dmesg | tee case\_no\_dmesg.txt

## Use hdparm

- hdparm -giI /dev/hda | tee case\_no\_hdparm.txt
- I have seen drives where the serial numbers in different parts of the output do not match
- Do NOT use "current sector capacity" or "Host Protected Area feature set" as an indication of an HPA, look at "LBA user addressable sectors"
- You can use hdparm to adjust hard disk settings for optimal performance, but I strongly recommend not messing with these settings

## Sample hdparm output

# hdparm -giI /dev/hda | tee hdparm.txt

/dev/hda:

geometry = 3649/255/63, sectors = 58633344, start = 0

Model=WDC WD300AB-00BVA0, FwRev=21.01H21, SerialNo=WD-WMA7H1042700
Config={ HardSect NotMFM HdSw>15uSec SpinMotCtl Fixed DTR>5Mbs
FmtGapReq }

RawCHS=16383/16/63, TrkSize=57600, SectSize=600, ECCbytes=40
BuffType=DualPortCache, BuffSize=2048kB, MaxMultSect=16, MultSect=16
CurCHS=16383/16/63, CurSects=16514064, LBA=yes, LBAsects=58633344
IORDY=on/off, tPIO={min:120,w/IORDY:120}, tDMA={min:120,rec:120}
PIO modes: pio0 pio1 pio2 pio3 pio4
DMA modes: mdma0 mdma1 mdma2 udma0 udma1 udma2 udma3 udma4 \*udma5
AdvancedPM=no WriteCache=enabled

Drive Supports : Reserved : ATA-1 ATA-2 ATA-3 ATA-4 ATA-5

## Sample hdparm output (cont)

non-removable ATA device, with non-removable media

Model Number: WDC WD300AB-00BVA0 Serial Number: WD-WMA7H1042700 Firmware Revision: 21.01H21 Standards: Supported: 1 2 3 4 5 Likely used: 5 Configuration: Logical max current cylinders 16383 16383 heads 16 16 63 63 sectors/track bytes/track:57600 (obsolete) 600 bytes/sector: (obsolete) current sector capacity: 16514064 LBA user addressable sectors = 58633344

## Sample hdparm output (cont)

Capabilities:

LBA, IORDY(can be disabled) Buffer size: 2048.0kB ECC bytes: 40 Queue depth: 1 Standby timer values: spec'd by standard, with device specific minimum r/w multiple sector transfer: Max = 16 Current = 16

DMA: mdma0 mdma1 mdma2 udma0 udma1 udma2 udma3 udma4 \*udma5

Cycle time: min=120ns recommended=120ns

PIO: pio0 pio1 pio2 pio3 pio4

Cycle time: no flow control=120ns IORDY flow control=120ns

Commands/features:

Supported:				
READ BUFFER cmd				
WRITE BUFFER cmd				
Host Protected Area feature set				
look-ahead				

(continues)

## List partitions with sfdisk

bash# sfdisk -luS /dev/hda | tee sfdisk.txt Disk /dev/hda: 3649 cylinders, 255 heads, 63 sectors/track Units = sectors of 512 bytes, counting from 0

Device	Boot	Start	End	#sectors	Id	System
/dev/hda1		63	208844	208782	83	Linux
/dev/hda2		208845	417689	208845	7	HPFS/NTFS
/dev/hda3		417690	626534	208845	b	Win95 FAT32
/dev/hda4		0	-	0	0	Empty

bash#

## Hashing

- hash text files md5sum \*.txt | tee case\_no\_txt\_hashes.txt
- hash drive md5sum /dev/hda | tee serial\_no.original.md5.txt

# Agenda

- Introduction
- About using Linux for Forensics
- Preparations
- Pre-imaging
- Imaging
- Preparing the analysis system
- Conducting analysis
- Conclusion

# Imaging options

- dd the old standby
- rda
  - Built into F.I.R.E.
  - Adds remote acquisition capability

# dcfldd – best option

- Variant of dd by Nicholas Harbour of the U.S.
   Department of Defense Computer Forensics
   Lab
- Online Help dcfldd -- help
- Shows progress while imaging
- dcfldd is included on the F.I.R.E. CD
- Source code to dcfldd available at sourceforge.net/projects/biatchux/

## dcfldd options - conv

- conv=sync,noerror
  - noerror = do not stop on a read error
  - sync = if there is a read error, pad output with
     0x00. Without sync, read errors result in skipping sectors, which messes up file allocation table, etc.

# dcfldd options - bs

- bs means blocksize
- Default bs=512 bytes
- Will get better performance with larger bs (such as bs=8k) based off hdparm results
- If there is a read error, you will lose the entire block (so I leave bs at default)

# dcfldd options

- Can hash while imaging
  - hashwindow=0
  - hashlog=case\_no\_dcflddhash.txt.
- Can split while imaging (use a script or pipe to split)
- Example command with all recommended options: dcfldd if=/dev/hda of=/mnt/hdc1/ case\_no/evidence\_no/serial\_no.dd conv=noerror,sync hashwindow=0 hashlog=serial\_no.md5.txt
  - DO NOT CONFUSE if= AND of= !!!
### When imaging is done

- shutdown with shutdown -h now
- Disconnect and store evidence

### Agenda

- Introduction
- About using Linux for Forensics
- Preparations
- Pre-imaging
- Imaging
- Preparing the analysis system
- Conducting analysis
- Conclusion

# Prepare your Forensic Analysis System

- Install Linux on Forensic Analysis System Red Hat required for NASA drivers, I used Red Hat 8.0
- Because some of the packages we will use are distributed as source, be sure to include all the development packages

# Install NASA Enhanced Loopback Drivers

- This driver by Don Becker, Dan Ridge, Rick Niles, Howard Barnes, and the current maintainer Jason Luttgens allows you to mount a complete disk image as a loopback device instead of only one partition
- Download from ftp://ftp.hq.nasa.gov/pub/ig/ccd/enhanced\_loopback/
- There are different kernels for i386, i686, p4, and athlon architectures
  - Do NOT rely on your hardware to determine what kernel to install
  - The kernel type you need is shown in the /boot/kernel.h file

# Install NASA Enhanced Loopback Drivers

- Run./createdev start
- Install loop-utils rpm rpm --force -ivh loop-utils-0.0.1-1.i386.rpm
- Untar kernel to /
  - cd /
  - tar xvfz vmlinuz-2.4.xx-xfsenhanced\_loop.x.tar.gz
- Edit grub.conf

### Install NASA Drivers

```
[root@localhost /]# cat /boot/grub/grub.conf
  (...)
title Red Hat Linux (2.4.18-14)
       root (hd0,4)
       kernel /boot/vmlinuz-2.4.18-14 ro root=LABEL=/
        initrd /boot/initrd-2.4.18-14.img
[root@localhost /]# gedit /boot/grub/grub.conf
[root@localhost /]# cat /boot/grub/grub.conf
   (...)
title Red Hat Linux (2.4.18-14)
       root (hd0,4)
       kernel /boot/vmlinuz-2.4.18-14 ro root=LABEL=/
        initrd /boot/initrd-2.4.18-14.img
title Red Hat Linux with NASA Loopback (2.4.21-pre4-xfs-enhanced loop)
       root (hd0,4)
       kernel /boot/vmlinuz-2.4.21-pre4-xfs-enhanced loop ro root=LABEL=/
        initrd /boot/initrd-2.4.21-pre4-xfs-enhanced loop.img
[root@localhost /]#
```

# National Software Reference Library

- NSRL is a compilation of hash values of files from operating systems and applications by the U.S.
   National Institute of Standards and Technology
- Includes primarily "known good" files, but does include "Hacker Tools" as well
- Download from ftp://ftp.nist.gov/pub/itl/div897/ nsrl/ver\_2\_0/nsrl\_2\_0.iso
- Unzip NSRL before you install Autopsy

# Install The Sleuth Kit and Autopsy

- Written by Brian Carrier and formerly known as The @stake Sleuth Kit
- Based off some code from The Coroner's Toolkit by Dan Farmer and Wietse Venema
- The Sleuth Kit and Autopsy make up a computer forensic browser
  - The SleuthKit is a collection of command line tools
  - Autopsy is a Web server that you connect to with any browser
- Source code and information available at www.sleuthkit.org

### Install Sleuthkit

- Download sleuthkit and autopsy source files to /usr/local/src.
- **Decompress**:tar zxvf sleuthkit-1.62.tar.gz
- Change Dir: cd sleuthkit-1.62
- Compile: make

### Install Autopsy

- **Decompress**: tar zxvf autopsy-1.73.tar.gz
- Change Dir: cd autopsy-1.73
- Install: make
- Give location of sleuthkit and NSRL
- Give location of "evidence locker" where all case data is kept - this directory should be on a Unix filesystem that supports symlinks

### Install Foremost

- Disk carving utility by Kris Kendall and Jesse Kornblum
- Extracts files from a data file by looking for known headers and footers
- Download from foremost.sourceforge.net
- **Decompress**: tar xzvf foremost-0.64.tar.gz
- Change Dir: cd foremost-0.64
- Compile: make
- Install: make install

### Agenda

- Introduction
- About using Linux for Forensics
- Preparations
- Pre-imaging
- Imaging
- Preparing the analysis system
- Conducting analysis
- Conclusion

### Administrivia

- Make image file read-only chmod a-w serial\_no.dd
- Hash complete image and compare to hash of drive and hash result from dcfldd md5sum serial\_no.dd
- To backup to CDs
  - Compress and Split gzip -c serial\_no.dd | split -b 699m - serial\_no.dd.gz
  - Hash all chunks:md5sum serial\_no.dd\* >>
     serial\_no\_chunks.md5.txt
  - Burn image chunks, text files, and hashes
- Reconstruct with cat serial\_no.dd.gz\* | gunzip - > serial\_no\_out.dd

# Mount image loopback with NASA drivers

- As root, mount loopback device with losetup /dev/loopa serial\_no.dd
- List the partition table from the image sfdisk -luS /dev/loopa
- Leave the loopback device mounted to run Autopsy
- When done unmount with losetup -d /dev/loopa

# Demo of mounting image loopback

[root@localhost wd30gb]# losetup /dev/loopa wd30gb.dd [root@localhost wd30gb]# sfdisk -luS /dev/loopa Disk /dev/loopa: cannot get geometry Disk /dev/loopa: 0 cylinders, 0 heads, 0 sectors/track Warning: The first partition looks like it was made

for C/H/S=\*/255/63 (instead of 0/0/0).
For this listing I'll assume that geometry.
Units = sectors of 512 bytes, counting from 0

Device Boot	Start	End #se	ectors Id	d S	ystem
/dev/loopa1	63	208844	208782	83	Linux
/dev/loopa2	208845	417689	208845	7	HPFS/NTFS
/dev/loopa3	417690	626534	208845	b	Win95 FAT32
/dev/loopa4	0	-	0	0	Empty
[root@localhost	wd30gb1#				

# Mount Filesystems if desired

- The file systems do NOT need to be mounted to run Autopsy
- Will alter journaling filesystems (ext3 and reiser) for the same reasons you do not mount the filesystems before imaging – see next slide
- Allows you to browse the active files on the command line or with you favorite GUI file manager
- For example mount -o ro /dev/loopa2 /mnt/evidence\_a2
- When you are done with the files, you unmount with umount /mnt/evidence\_a2

# Mount Journaling Filesystems

- Journaling filesystems cannot be mounted using NASA drivers without changing the image
- If you need to mount, you have two options:
  - Accept that changes will be made to the mount count (the data files are untouched, but you should still restore from a backup after unmounting)
  - Extract partition image from the disk image and mount using mount -o ro,loop ext3part.dd /mnt/ext3part

### Demo of mounting filesystems

[root@localhost wd30gb]# mkdir /mnt/image2 [root@localhost wd30gb]# mount -o ro /dev/loopa2 /mnt/image2 [root@localhost wd30gb]# ls -la /mnt/image2 total 8 dr-x----1 root 4096 Jun 28 11:27 . root drwxr-xr-x 12 root 4096 Jun 28 13:39 .. root dr-x---- 1 root 4096 Jun 28 11:27 dosutils root dr-x----1 root 0 Jun 28 11:27 RECYCLER root dr-x----1 root root 0 Jun 28 11:10 System Volume Information [root@localhost wd30gb]# mount (...) /dev/loopa2 on /mnt/image2 type ntfs (ro) (...) [root@localhost wd30gb]# umount /mnt/image2 [root@localhost wd30gb]#

### Virus Scanning

- F-prot www.fprot.org
  - f-prot is free for personal use only
  - I understand that it is legal to use if you do not install it on the machine
- Bitdefender www.bitdefender.com
  - "freeware"

### Searching

- Strings and grep can be used to do basic searching
- Helpful for quickly searching for text
- ACSII strings -t d case\_no.dd > case\_no.strings
- UNICODE strings -t d -e l case\_no.dd > case\_no.strings-el
- Use grep to search through output files

### Run Foremost

- Copy foremost.conf from install directory to current directory
- Edit foremost.conf to search for file types you want
- Run Foremost foremost -o serial\_no\_fm -v serial\_no.dd
- This will create the serial\_no\_fm directory if it does not exist
- If serial\_no\_fm directory exists, it MUST be empty

### **Running Foremost**

- Can run on disk image or on loopback devices
   foremost -o loopa3\_fm -v /dev/loopa3
- Can also be run on free space (.dls) extracted by Autopsy

### **Issues with Foremost**

- Problem foremost creates the directory and an audit file immediately
  - Even if you have specified invalid options so foremost cannot run
  - If you fix your mistake and run it again, it will not run because the directory you specified is not empty
- Issue foremost reads through the image without interpreting the filesystem - it will extract logical files as well as deleted ones and ones from free space
- Issue file must be contiguous for foremost to find it

# Run Sleuthkit/Autopsy

- I will not be able to cover all the details of running Autopsy, but this should be enough to get started
- Start Autopsy as root ./autopsy -d /mnt/hdc1/evidlock
- Start Web browser as a non-root user
- Connect to URL Autopsy displays
- Potentially dangerous files (HTML) are viewed in a sanitized environment by default

# **Initial Autopsy Screen**



### Autopsy terminology:

- Case = A case
- Host = A computer (one or more hard drives and partitions)
- Image = A partition

### Problem:

- The Sleuthkit/Autopsy require images of individual partitions
- We have an image of an entire disk
- There are two options:
  - Split the partition images out of the disk image For more information see:
    - sleuthkit.sourceforge.net/informer/sleuthkit-informer-2.html
    - talk.trekweb.com/~jasonb/articles/linux\_loopback.shtml
  - Point Autopsy to the loopback mounted filesystem

### **Initial Steps**

- Create case
- Create host
- Add Image with symlisk option to /dev/loopa1
- Be careful what you name the mount point I usually leave it / for non-unix systems
- For example, if you use C:, the View Directory box will not work.
- Creates directories under Evidence Locker

<u>File Edit View Go Bo</u>	okmarks <u>T</u> ools <u>W</u> indow <u>H</u> elp
	> http://localhost:9999/3656566 Search
	CREATE A NEW CASE
1. Enter	Case Name (directory name): plackhat-0001
2. Enter D	escription (one line, optional): Demo at Blackhat
	3. Enter Investigator Logins (no spaces):
a, Chuck	ъ.
	d
с. ј	
e.	f.
e. g.	f.   h.





✓ Add A New Host To blackhat-0001 - Mozilla							
_ <u>F</u> ile <u>E</u> dit <u>V</u> iew <u>G</u> o <u>B</u> ookmarks <u>T</u> ools <u>W</u> indow <u>H</u> elp							
🔾 🕘 💿 💿 💿 💿 💿 👘							
Case: blackhat-0001							
ADD A NEW HOST							
1. Host Name (directory name): 192.168.1.1							
2. Description (one line, optional): computer	-						
3. Timezone: EST5EDT							
4. Timeskew (in +/- seconds): 0							
5. Path of Alert Hash Database (optional) i.e. known bad files:	-						
6. Path of Ignore Hash Database (optional) i.e. known good files:	-						
ADD HOST CANCEL HELP							



Add Image To blackhat-0001:192.168.1.1 - Mozi	lla 🔤 🗖 🗄					
<u>File Edit View Go Bookmarks Tools W</u> indow	Help					
	st:9999/3656566 🔽 🔍 Search 🖉 🌆					
Case: blackhat-0001 Host: 192.168.1.1						
ADD A NEW MACE						
ADD A NEW IMAGE						
Image Location (starting with /):	/dev/loopa1					
Import Method:	Symlink to Evidence Locker					
	Copy to Evidence Locker					
	Move to Evidence Locker (Warning:					
	image loss could occur during a system failure)					
File System Type:	linux-ext2 🗾					
Mounting point:	V					
Image Integrity Check Options (i.e. MD5)						
Calculate Now:	•					
Ignore:	•					
Add:	•					
MD5:						
	Verify MD5 After Importing?					
ADD IMAGE CANCEL HELP						
m 🖂 🖙 🗊 Transferring data from localhost						

### Looking at files

- Go to File Analysis, which will let you browse file system
- Can only browse and search one partition at a time

▶ blackhat-0001:192.168.1.1:	images/loopa1 - N	lozilla				×	
<u>File Edit View Go Book</u>	(marks <u>T</u> ools <u>W</u> ind	low <u>H</u> elp			-		
🔍 🕞 🌑 🕥 💿 http://localhost:9999/23321725914186395979/autopsy?func=28 💽 🔍 Search							
File Analysis Keywork	D SEARCH FILE		GE DETAILS MET		A UNIT HELP	CLOSE	
<b>_</b>			12:16:18 (EDT)	12:16:17 (EDT)	12:16:18 (EDT)	<b></b>	
View Directory:	r/r	<u>gr8.txt</u>	2003.06.28 12:17:56 (EDT)	2003.06.28 12:17:56 (EDT)	2003.06.28 12:17:56 (EDT)	21	
	r/r	<u>initrd.img</u>	2003.06.28 12:16:18 (EDT)	2003.06.28 12:16:18 (EDT)	2003.06.28 12:16:18 (EDT)	202	
OK	<u>ا</u>						
ALL DELETED FILES	file: Using regu couldn't find an ASC	lar magic file ` y magic files! II ( <u>display</u> - <u>rep</u>	/home/user/sleuthk port) * Strings ( <u>disp</u> File Tyne: AS	it_src/sleuthkit-1.6 <u>lay</u> - <u>report</u> ) * <u>Expo</u> CII text	2/share/magic' file ort * <u>Add Note</u>	9:	
HIDE DIRECTORIES							
<b>_</b>	Contents Of Fil	le: /dosutils/a	autoboot/gr8.txt				
/ + <u>/lost+found</u>	drug money is g	great!					
+/dosutils							
++ <u>/autoboot</u> ++/fips20							
+++/restorrb							
	(0.04					-m- 0	
Document: Doc	ne (U.94 secs)					T-TH-1 E	

ᆚᄂ
## **Deleted Files**

- The listed file will have a Check on the left if they have been deleted
- Deleted files are listed in two shades of red:
  - Bright red indicates that the file data blocks are free (not allocated to another file)
  - Dark red indicates that file data blocks are allocated to another file

✓ blackhat-0001:192.168.1.1:images/loopa3 - Mozilla							
<u>File E</u> dit <u>V</u> iew <u>G</u> o <u>B</u> ookmarks <u>T</u> ools <u>W</u> indow <u>H</u> elp							
Co Search Attp://localhost:9999/2604230612394918610/autopsy?func=2&r							
FILE ANALYSIS KEYWORD SEARCH FILE TYPE IMAGE DETAILS META DATA DATA UNIT HELP CLOSE							
			14.40.16 (ED 1)	00.00.00 (ED I) II			
View Directory:	r/r	<u>/dosutils/autoboot/_mlinuz</u>	2002.04.19 14:45:04 (EDT)	2003.06.28 20 00:00:00 (EDT) 11			
	r/r	<u>/dosutils/autoboot/_oot.img</u>	2003.06.28 11:35:02 (EDT)	2003.06.28 20 00:00:00 (EDT) 11			
	r/r	<u>/dosutils/autoboot/_oot.img</u>	2003.06.28 11:35:02 (EDT)	2003.06.28 20 00:00:00 (EDT) 11			
	d/d 	<u>/images/_s</u> III	2003.06.28	2003.06.28 20▼ ▶			
ALL DELETED FILES	file: Using regular magic file `/home/user/sleuthkit_src/sleuthkit-1.62/share/magic' file: couldn't find any magic files! ASCII ( <u>display</u> - <u>report</u> ) * Strings ( <u>display</u> - <u>report</u> ) * <u>Export</u> * <u>Add Note</u> File Type: ASCII English text, with no line terminators						
EXPAND DIRECTORIES							
	Contents Of File: /dosutils/autoboot/_oot.img						
	The worst	t cocaine can do is kilo you.					
🔟 🖂 🚱 🎦 Document: Done (0.938 secs)							

╞

Chuck_Laptop:Laptop:images/hda5 - Mozilla								
<u>File Edit V</u> iew <u>G</u> o <u>B</u> ookmarks <u>T</u> ools <u>W</u> indow <u>H</u> elp								
Colored Co								
FILE ANALYSIS KEYWORD	SEARC	File Type	IMAGE DETAILS	META DATA	DAT	AUNIT	J.	PELP CLOSE
View Directory		2003.06.20 16:03:05 (EDT)	2003.06.24 21:57:14 (EDT)	2003.06.24 21:57:14 (EDT)	7264	0	0	<u>192904</u> (realloc)
		2003.06.20 16:03:05 (EDT)	2003.06.24 21:57:14 (EDT)	2003.06.24 21:57:14 (EDT)	5916	0	0	<u>192905</u> (realloc)
OK		2003.06.20 09:52:52 (EDT)	2003.06.29 15:04:24 (EDT)	2003.06.20 09:52:52 (EDT)	4096	500	4	<u>130121</u>
· ·	<u>ur. gz</u>	2003.06.20 16:03:04 (EDT)	2003.06.24 21:57:14 (EDT)	2003.06.24 21:57:14 (EDT)	87883	0	0	<u>192463</u> (realloc)
ALL DELETED FILES		2003.06.20 16:03:04 (EDT)	2003.06.24 21:57:14 (EDT)	2003.06.24 21:57:14 (EDT)	110474	0	0	<u>192523</u> (realloc) 🖵
	•				111			•
EXPAND DIRECTORIES								
🔟 🖂 🐏 🚺 Document: Done (3.065 secs)								

# Keyword Search

- As noted in the keyword screen, strings that cross file fragmentation boundaries will not be found
- Can use regular expressions and/or case insensitive options
- Does not have Unicode option

♥ blackhat-0001:192.168.1.1:images/loopa3 - Mozilla	X
<u>F</u> ile <u>E</u> dit <u>V</u> iew <u>G</u> o <u>B</u> ookmarks <u>T</u> ools <u>W</u> indow <u>H</u> elp	
Content of the second secon	Search
FILE ANALYSIS KEYWORD SEARCH FILE TYPE IMAGE DETAILS META DATA DATA	A UNIT HELP CLOSE
Keyword Search on images/loopa3	
Enter String: drug	=
🗖 Case Insensitive 🗖 Regular Expression	
SEARCH	
grep cheat sheet	
(Note that strings that cross <u>non-consecutive</u> Sectors in a file will not be four	nd)
Document: Done (0.228 secs)	

Markhat-0001-102 168 1 1-in	nagos/loona2 - Mozilla
File Edit View Go Bookm	arks Tools Window Help
	N http://localhost:9999/23321725914186395979/autopsy?func=28
FILE ANALYSIS KEYWORD	SEARCH FILE TYPE IMAGE DETAILS META DATA DATA UNIT HELP CLOSE
Q.	? X
New Search	
2 coordination one of the	EXPORT CONTENTS ADD NOTE
were found	ASCII (display - report) * Hey (display - report) * Strings (display - report)
Search Ontions:	file: Using regular magic file `/home/user/sleuthkit_src/sleuthkit_1 62/share/magic' file:
Case Sensitive	couldn't find any magic files! <b>File Type:</b> ASCII English text, with no line terminators
	Sector 89834
	Allocated
	Hide Meta Data Address
Sector 89826 ( <u>Hex</u> -	Pointed to by Dir Entry: <u>1410642</u>
Asc11)	Pointed to by file:
1, 19 (t do drugs)	/RECYCLED/Dz5.txt (DZ5.TXT)
Sector 89830 (Hex -	NOTE Contracts of Contra 20224 (F10 botton) in incare (losse)
Ascii)	ASULL CONCERCS OF SECTOR 89834 (SLZ DYCES) IN IMAGES/100pa3
2:12 (ish, drugs is )	The dense are in the torol
	The drugs are in the trash
Sector 89834 ( <u>Hex</u> -	
$\frac{ASCII}{2:4}$ (mba drugge area)	
3.4 (Ine drugs are)	
🔟 🖂 📴 🗊 🛛 Document: Done	(1.79 secs)

╞

✓ blackhat-0001:192.168.1.1:images/loopa3 - Mozilla								
<u>File E</u> dit <u>V</u> iew <u>G</u> o <u>B</u> ookmarks <u>T</u> ools <u>W</u> indow <u>H</u> elp								
L C http://localhost:9999/2604230612394918610/autopsy?func=2&r C C Search So UUU								
FILE ANALYSIS KEYWORD SEARCH FILE TYPE IMAGE DETAILS META DATA DATA UNIT HELP CLOSE								
						?	X	
				11:16:02 (EDT)	00:00:00 (EDT)	11:16:00 (EDT)		
	1	r/r	MP2.tmp	2003.06.28	2003.06.28	2003.06.28	0	
ALL DELETED FILES				11:41:20 (EDT)	00:00:00 (EDT)	11:41:18 (EDT)	E	
		r/r 🧕	allwords.txt	2003.06.28	2003.06.28	2003.06.28	11	
				11:41:22 (EDT)	00:00:00 (EDT)	11:40:42 (EDT)		
		r/r 🤉	<u>hanges.txt</u>	2001.10.12	2003.06.28	2003.06.28	23 -	
				111				
Ζ =	file: Usin	a requisr	magic file `/b	ome/user/sleuthkit	are/sleuthkit-1.62/	share/magic' file		
+/dosutils	couldn't find any magic files!							
++/rawritewin	ASCII (display - report) * Strings (display - report) * Export * Add Note							
(RAWRIT~1)	File Type: Little-endian UTE-16 Unicode character data, with no line terminators							
++/fips20		o rypo. 2	inne chanaire			11110 001 1111100010		
+++/source								
+++/restorrb	writewin (	writewin (RAWRIT~1)/allwords.txt						
++/fips15c								
+++/source	0.000000000	0~^0~^04	NAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA	~~~~~~~~~~~~~~~~~~		0.000-00-00-00-00-00-00-00-00-00-00-00-0		
+++/restorrb	Junon 01"	00°°00°00.	oe o: o opro	0 0010,10 10010010C	: oa or on oe o, d	o ou or ou og os.	0, 10	
++/autoboot								

8 5

# More Autopsy Features

- File Type will let you sort files by type and extract graphic files.
- Image Details will list details for this Hard disk image (has nothing to do with Graphic Files)
- Meta Data lets you enter an inode by number and see what file it points to and even view the contents of that file
- Data Unit lets you view the data areas on disk directly

# Agenda

- Introduction
- About using Linux for Forensics
- Preparations
- Pre-imaging
- Imaging
- Preparing the analysis system
- Conducting analysis
- Conclusion

# Other Potentially Useful Tools

- MD5deep (md5deep.sourceforge.net) recursive md5s
- Fatback (sourceforge.net/projects/biatchux) File uneraser for FAT file systems
- Stegdetect (www.outguess.org) will detect some kinds of steganography in images
- Galleta (www.openforensics.org) IE Cookie Parser
- Pasco (www.openforensics.org) IE Activity Parser
- Rifiuti (www.openforensics.org) Recycle Bin INFO2 File Parser
- LibPST (sourceforge.net/projects/ol2mbox) converts Outlook and Outlook Express files to Linux mbox format

# Upcoming utilities that show promise

- Odessa Project www.openforensics.org
  - OpenDD (odd) aka Network Evidence Duplicator (ned)
    - Menu driven!
    - Remote imaging
    - Remote analysis with rex
  - Rapid Evidence eXtractor (rex)
    - Remote analysis
    - Cross-platform (Windows, Linux, OSX)
- Penguin Sleuth www.linux-forensics.com
  - Forensics Boot CD based on Knoppix
- Forensic and Log Analysis GUI (FLAG) www.dsd.gov.au/software/flag/

# **Additional Resources**

- Honeynet Project Scans of the Month (www.honeynet.org/scans/) #15, #24, and #26 deal with forensics
- SleuthKit/Autopsy information, mailing list, and download – www.sleuthkit.org
  - Case studies of Honeynet Scans www.sleuthkit.org/case/index.php
  - Great news letter www.sleuthkit.org/informer/index.php
- Linux Forensic User Group groups.yahoo.com/group/linux\_forensics/

# **Additional Resources**

- Information about the National Software Reference Library (NSRL) - www.nsrl.nist.gov
- Tools, forums, mailing lists www.openforensics.org
- Penguin Sleuth CD, forums, and information www.linux-forensics.com
- Tools and information www.opensourceforensics.org
- The Coroner's Toolkit www.porcupine.org/forensics/tct.html

# Any final questions?

## Conclusion

- Thank you all for coming
- I hope that this has been helpful in getting you started in this area
- I am available after this presentation or at any other time during Black Hat to answer any additional questions
- Or, contact my by email at chuckfwillis@netscape.net
- Enjoy the show!