

# Using Linux for Today's Data Forensics



Thomas Rude, CISSP  
3 November 2004

# Using Linux for Data Forensics

## **Note:**

I have combined my presentation given on Monday, 3 November, with two that I was called in to assist with on Tuesday, 4 November. This single presentation combines the three CSI presentations into one.

# Using Linux for Data Forensics

## **Agenda**

- Review
- Foren-volution
- Penguin Power
- Hiccups, Tools, & Other Musings

# Using Linux for Data Forensics

## Review

- acquisition, analysis, & reporting
- historically geeking;
  - small hard drives < 1GB
  - DOS-based tools
  - stand alone, post mortem analysis
  - little legal

# Using Linux for Data Forensics

## **Foren-volution**

# Using Linux for Data Forensics

## **Foren-volution**

- elements of change include;
  - cheap technology
  - larger hard drives > 40GB
  - plethora of data storage devices
  - litigious world
  - job market

# Using Linux for Data Forensics

## **Penguin Power**

- 40+ filesystem types supported in kernel 2.4.18+
- non-invasive operating system architecture
- loopback device driver & files
- cost, speed, & efficiency
- source code review
- enterprise scalable and friendly

# Using Linux for Data Forensics

## **Hiccups, Tools, & Other Musings**

# Using Linux for Data Forensics

## Hiccups

- odd sector out on an IDE hard drive

Data is read by the block layer in 1k blocks.

If the last sector is odd (512), it is ignored.  
Goodbye, so long, too bad, no soup for you....

What to do?

- 1) head over to KFC and patch the kernel
- 2) bypass the block layer and use raw devices
- 3) bury your head in the sand and cry for mama

# Using Linux for Data Forensics

## **Tools**

May be divided into system tools and other tools;

- System tools include;

dd, md5sum, grep, strings, stat, file, find,  
etc.

(I.E., those that ship with most distributions)

- Non-system tools = 3<sup>rd</sup> party tools, both free and commercial

# Using Linux for Data Forensics

## Tools

- data forensic tools include, but **not** limited to;

**SMART for Linux**      [www.asrdata.com](http://www.asrdata.com)

**Sleuthkit**      [www.sleuthkit.org](http://www.sleuthkit.org)

**FLAG**      [www.dsd.gov.au/library/software/flag/](http://www.dsd.gov.au/library/software/flag/)

**The Coroner's Toolkit**      [www.porcupine.org](http://www.porcupine.org)

# Using Linux for Data Forensics

## Tools Comparison

	SMART	Sleuthkit	FLAG
Acquire Physical Image	X		
Acquire Logical Volume/Partition	X		
Acquire via Network (LAN or WAN)	X		
Acquire & Clone Simultaneously	X		
Custom Acquisition (specify range)	X		
Authenticate (CRC32, MD5SUM, SHA1)	X	X	X
Search	X	X	X
Bootable CD	X		
Deleted File Recovery	FATx, NTFS, ext2	FATx, ext2	FATx, ext2
Wiping	X	X	
Hash Sets		X	X

# Using Linux for Data Forensics

## More Tools

libpst	<a href="http://www.sourceforge.net/projects/ol2mbox">www.sourceforge.net/projects/ol2mbox</a>
captive-ntfs	<a href="http://www.jankratochvil.net/project/captive">www.jankratochvil.net/project/captive</a>
dcfldd	<a href="http://biatchux.dmzs.com/">http://biatchux.dmzs.com/</a>
fatback	
foremost	<a href="http://foremost.sf.net/">http://foremost.sf.net/</a>
md5deep	<a href="http://md5deep.sf.net/">http://md5deep.sf.net/</a>

# Using Linux for Data Forensics

## Other Musings

- Linux does **not** require the use of a write blocker
- Linux may be used to acquire, browse, authenticate, and search various media such as; compact flash cards, secure digital cards, memory sticks, handhelds/PDAs, hard drives, RAID arrays, tape cartridges, & other storage containers
- Contrary to popular belief, Linux is **not** free, see below;

"Linux is free only if your time is worthless"

# Using Linux for Data Forensics

## Other Musings

- **Yes**, Linux **may** be used in all aspects of your investigation;
  - acquisition
  - analysis
  - reporting
- **Yes**, Linux **is** accepted by courts around the world
- **Yes**, Linux has been validated by independents and agencies alike (such as NIST)

# Using Linux for Data Forensics

Questions?    Comments?    Checks payable to . . .

f a r m e r d u d e @ c r a z y t r a i n . c o m

Note: No part of this document, either in whole or in part, may be reproduced, distributed, or publicly displayed without prior express written consent from the author.