

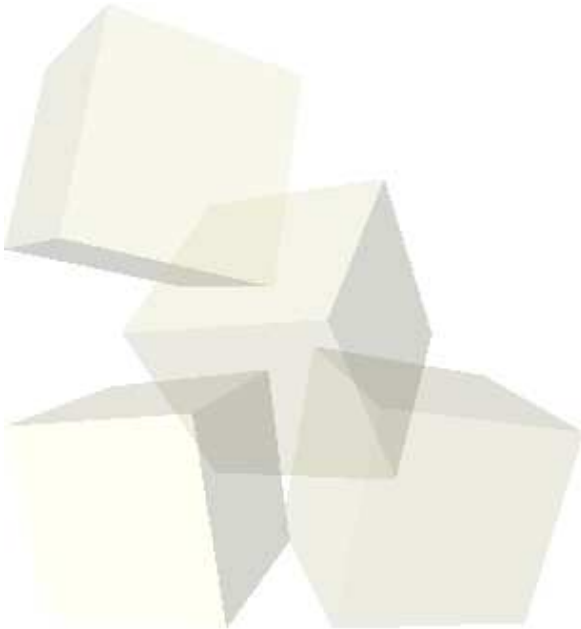


Incident Response & Data Forensics Using Linux

Building Your Linux Toolbox

NetSec2004

14-16 June 2004



Thomas Rude, CISSP

www.crazytrain.com

Copyright ©2004 Thomas Rude All Rights Reserved

This document is protected by applicable copyright laws. You may not show, adapt, or distribute this document or any part thereof without prior express written consent of copyright holder.





Incident Response & Data Forensics Using Linux

Building Your Linux Toolbox

An agenda

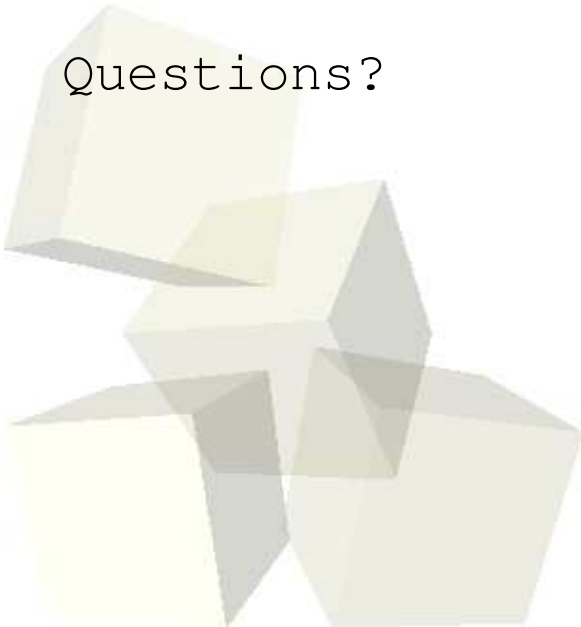
Introduction?

Why are we here?

Why Linux?

Your Linux Toolbox!

Questions?



Copyright ©2004 Thomas Rude All Rights Reserved

This document is protected by applicable copyright laws. You may not show, adapt, or distribute this document or any part thereof without prior express written consent of copyright holder.

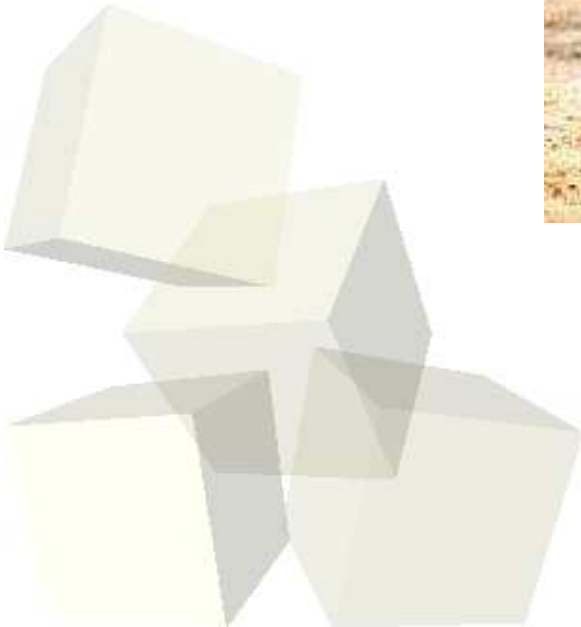


Incident Response & Data Forensics Using Linux

Building Your Linux Toolbox

Introduction?

.... I did have a prior job



Copyright ©2004 Thomas Rude All Rights Reserved

This document is protected by applicable copyright laws. You may not show, adapt, or distribute this document or any part thereof without prior express written consent of copyright holder.

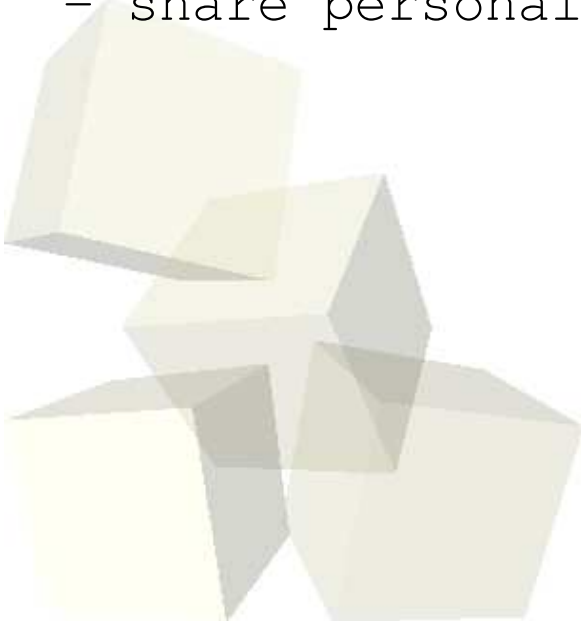


Incident Response & Data Forensics Using Linux

Building Your Linux Toolbox

Why are we here....really?

- understand why Linux is so powerful for data forensics
- understand factors that may affect selecting a tool
- learn what tools are out there and their strengths and weaknesses
- share personal experiences to help all of us



Copyright ©2004 Thomas Rude All Rights Reserved

This document is protected by applicable copyright laws. You may not show, adapt, or distribute this document or any part thereof without prior express written consent of copyright holder.

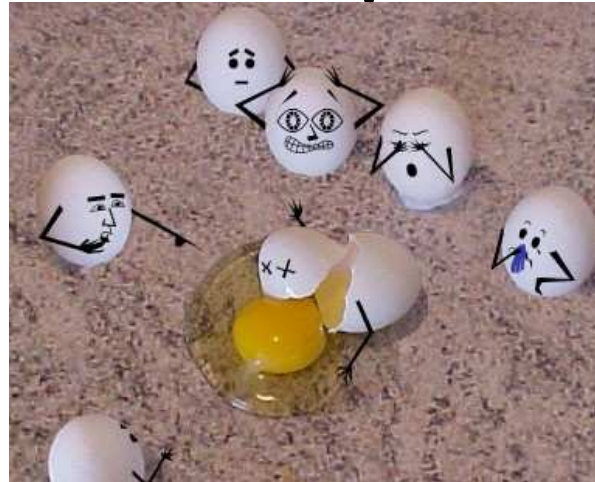


Incident Response & Data Forensics Using Linux

Building Your Linux Toolbox

Why Linux?

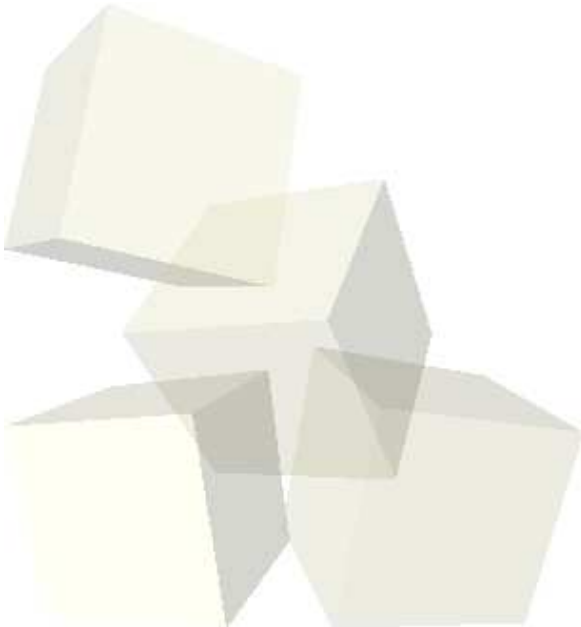
YIKES! Marv has committed suicide . . . I told him he'd have to pay extra to mount an image file in Windows!



Heh heh heh . . . he forgot his write blocker! What a shame....

Oh the humanity! 'Marv, the penguin was here to help you!'

He should have known better . . . crippled boot disk . . . I told him 'Linux, Marv, Linux'!



Copyright ©2004 Thomas Rude All Rights Reserved

This document is protected by applicable copyright laws. You may not show, adapt, or distribute this document or any part thereof without prior express written consent of copyright holder.

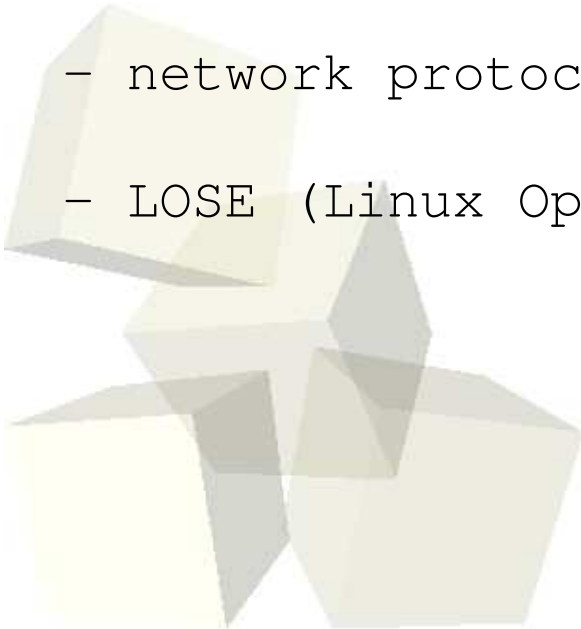


Incident Response & Data Forensics Using Linux

Building Your Linux Toolbox

Why Linux Penguin Power

- minimally invasive by default
- filesystem types support & disk layout support
- control
- loopback device
- network protocols
- LOSE (Linux Operating System Environment)



Copyright ©2004 Thomas Rude All Rights Reserved

This document is protected by applicable copyright laws. You may not show, adapt, or distribute this document or any part thereof without prior express written consent of copyright holder.

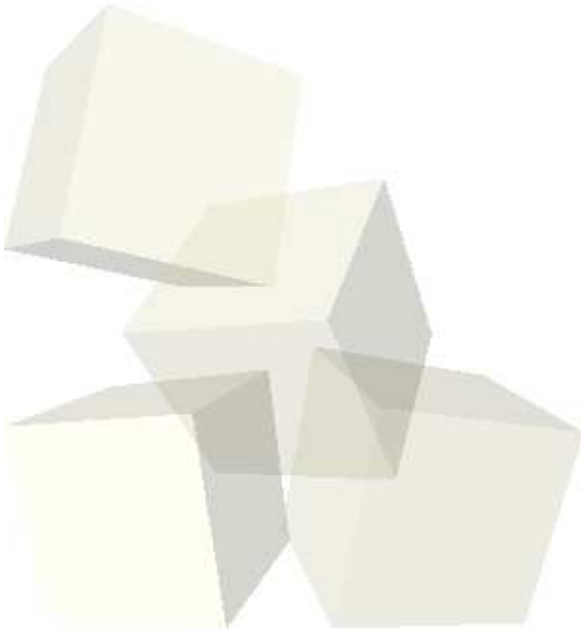


Incident Response & Data Forensics Using Linux

Building Your Linux Toolbox

Linux Power Minimally Invasive

- no hardware write blocker required
- you can safely attach media without worry of writes
 - thumbdrives, zip drives, compact flash, SD, etc.
- **BUT** if you like both a belt *and* suspenders you can use a hardware write blocker with Linux



Copyright ©2004 Thomas Rude All Rights Reserved

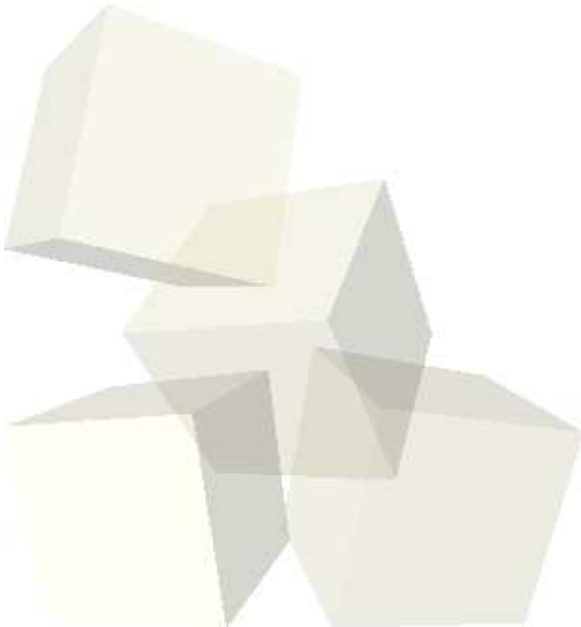
This document is protected by applicable copyright laws. You may not show, adapt, or distribute this document or any part thereof without prior express written consent of copyright holder.



Incident Response & Data Forensics Using Linux

Building Your Linux Toolbox

Linux Power Minimally Invasive



Copyright ©2004 Thomas Rude All Rights Reserved

This document is protected by applicable copyright laws. You may not show, adapt, or distribute this document or any part thereof without prior express written consent of copyright holder.



Incident Response & Data Forensics Using Linux

Building Your Linux Toolbox

Linux Power Filesystem Types & Disk Layout Support

- support for many FS TYPES, including;
 - disk-based
 - network
 - special
- support for many disk layouts, including;
 - DOS style partitions
 - disklabels
 - slices
- what does all of this really mean to you?

One platform to analyze any number of platforms!

Copyright ©2004 Thomas Rude All Rights Reserved

This document is protected by applicable copyright laws. You may not show, adapt, or distribute this document or any part thereof without prior express written consent of copyright holder.

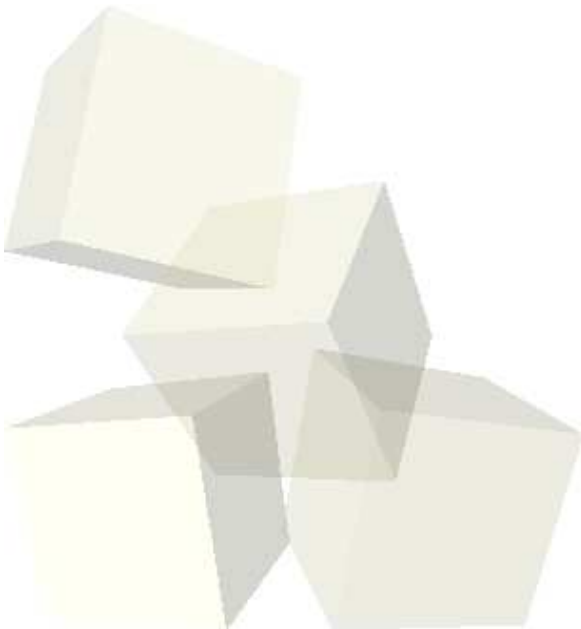


Incident Response & Data Forensics Using Linux

Building Your Linux Toolbox

Linux Power Operating System Control

- **you** control the operating system
- log actions taken
- decide how the operating system should handle devices
- customize code for personal needs



Copyright ©2004 Thomas Rude All Rights Reserved

This document is protected by applicable copyright laws. You may not show, adapt, or distribute this document or any part thereof without prior express written consent of copyright holder.

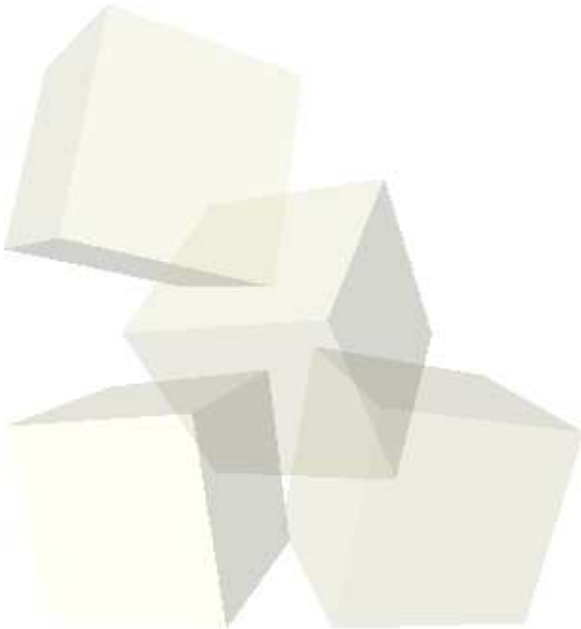


Incident Response & Data Forensics Using Linux

Building Your Linux Toolbox

Linux Power Operating System Control

- do you get this control in a Win32 environment?



Copyright ©2004 Thomas Rude All Rights Reserved

This document is protected by applicable copyright laws. You may not show, adapt, or distribute this document or any part thereof without prior express written consent of copyright holder.

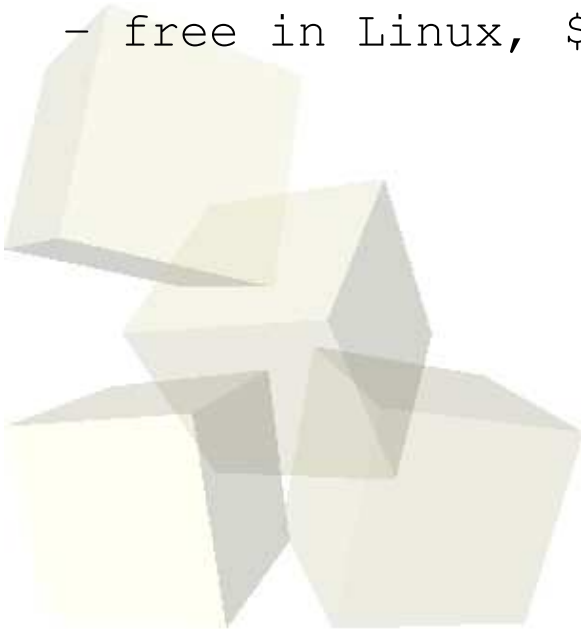


Incident Response & Data Forensics Using Linux

Building Your Linux Toolbox

Linux Power Loopback Device

- treat regular file as block device
- mount filesystem read only
- view logical structure
- view active data
- free in Linux, \$\$\$ in Win32



Copyright ©2004 Thomas Rude All Rights Reserved

This document is protected by applicable copyright laws. You may not show, adapt, or distribute this document or any part thereof without prior express written consent of copyright holder.

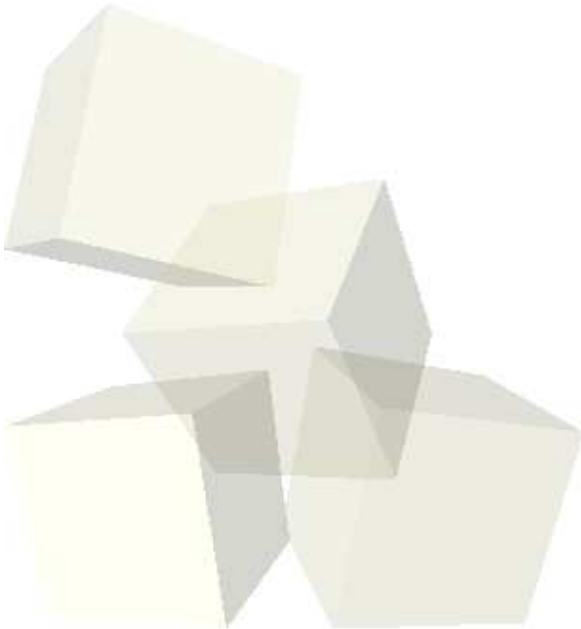


Incident Response & Data Forensics Using Linux

Building Your Linux Toolbox

Linux Power Network Protocols

- Appletalk
- IPX
- IP
- drop attack box in any network and grab packets



Copyright ©2004 Thomas Rude All Rights Reserved

This document is protected by applicable copyright laws. You may not show, adapt, or distribute this document or any part thereof without prior express written consent of copyright holder.

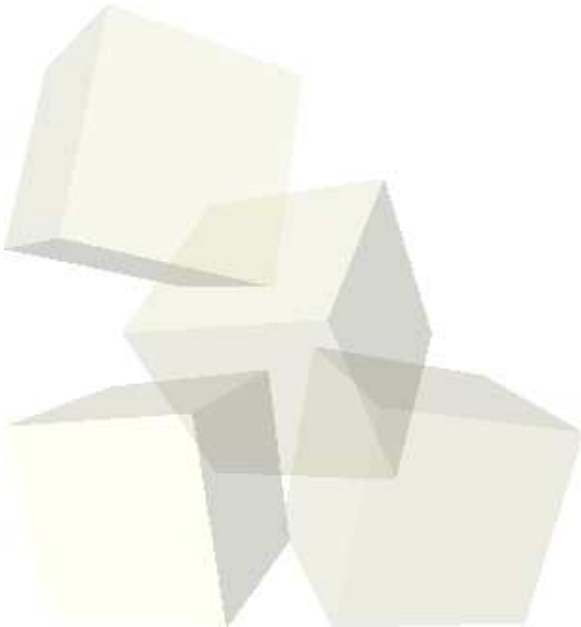


Incident Response & Data Forensics Using Linux

Building Your Linux Toolbox

Linux Power Linux Operating System Environment (LOSE)

- I/O scheduler
 - requests to disc, CD-ROM, etc.
- memory management
 - much more flexible memory *and* paging models than Win32
- pervasively multi-tasking and multi-threading



Copyright ©2004 Thomas Rude All Rights Reserved

This document is protected by applicable copyright laws. You may not show, adapt, or distribute this document or any part thereof without prior express written consent of copyright holder.



Incident Response & Data Forensics Using Linux

Building Your Linux Toolbox

Linux Power .

Linux
Operating
System
Environment
(LOSE)

Fly
High
with
Linux



Copyright ©2004 Thomas Rude All Rights Reserved

This document is protected by applicable copyright laws. You may not show, adapt, or distribute this document or any part thereof without prior express written consent of copyright holder.



Incident Response & Data Forensics Using Linux

Building Your Linux Toolbox

Okay, 'Linux' but 2.4 or 2.6 kernel?

+ 2.6

- scalable processing (16CPU vs. 8CPU for 2.4)
- support > 8GB RAM
- I/O Scheduler choice (deadline, anticipatory)
- improved threading (NPTL)
- LVM now 'device mapper' and improved
- security improvements
- user mode Linux (uml)
 - virtual machine

Copyright ©2004 Thomas Rude All Rights Reserved

This document is protected by applicable copyright laws. You may not show, adapt, or distribute this document or any part thereof without prior express written consent of copyright holder.



Incident Response & Data Forensics Using Linux

Building Your Linux Toolbox

Okay, 'Linux' but 2.4 or 2.6 kernel?

- 2.6
- removed filesystem types support
- removed hardware support
- horrible firewire support

So, which?

- 2.4 for acquire and analysis **except** for odd sector drives, then 2.6
- but sometimes

Copyright ©2004 Thomas Rude All Rights Reserved

This document is protected by applicable copyright laws. You may not show, adapt, or distribute this document or any part thereof without prior express written consent of copyright holder.

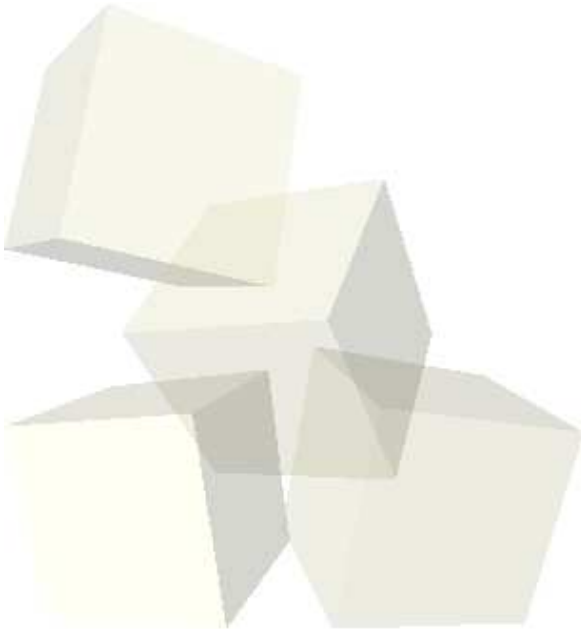


Incident Response & Data Forensics Using Linux

Building Your Linux Toolbox

Okay, 'Linux' but which distro?

- are there differences?
- are there differences that directly affect data forensics and incident response?



Copyright ©2004 Thomas Rude All Rights Reserved

This document is protected by applicable copyright laws. You may not show, adapt, or distribute this document or any part thereof without prior express written consent of copyright holder.



Incident Response & Data Forensics Using Linux

Building Your Linux Toolbox

Okay, 'Linux' but which distro?

- up to YOU! ! ! !
- there **are** differences, beyond the graphical obvious ones
 - kernel nuances
 - drivers
 - included tools/programs/packages
- do your homework;
 - define your objectives
 - perform research
 - narrow selection
 - test/validate/verify
- that being said; Red Hat Linux 9 updated, Fedora Core 1

Copyright ©2004 Thomas Rude All Rights Reserved

This document is protected by applicable copyright laws. You may not show, adapt, or distribute this document or any part thereof without prior express written consent of copyright holder.



Incident Response & Data Forensics Using Linux

Building Your Linux Toolbox

Okay, 'Linux' but which distro?

- if you don't do your homework, you'll get a visit from this guy



Copyright ©2004 Thomas Rude All Rights Reserved

This document is protected by applicable copyright laws. You may not show, adapt, or distribute this document or any part thereof without prior express written consent of copyright holder.



Incident Response & Data Forensics Using Linux

Building Your Linux Toolbox

Factors that influence tool selection;

- accuracy
- validity (verify/validate)
- user friendliness (personal, subjective)
- installation & configuration
- support
- documentation



Copyright ©2004 Thomas Rude All Rights Reserved

This document is protected by applicable copyright laws. You may not show, adapt, or distribute this document or any part thereof without prior express written consent of copyright holder.



Incident Response & Data Forensics Using Linux

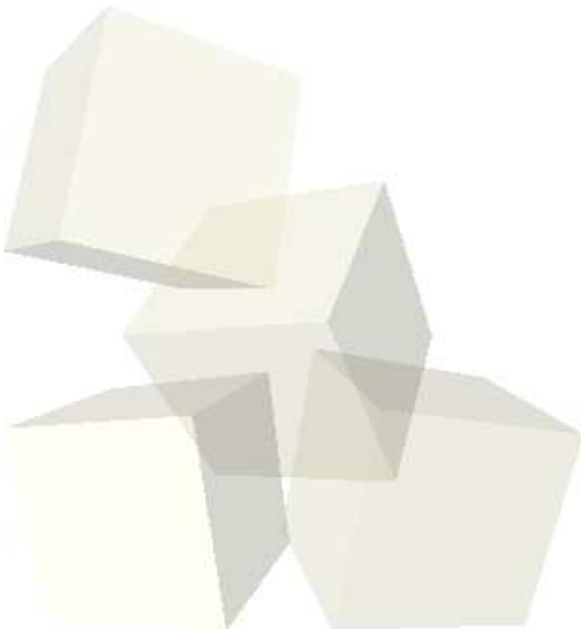
Building Your Linux Toolbox

Tool Types;

- two types, really;

1) single purpose

2) multi-purpose



Copyright ©2004 Thomas Rude All Rights Reserved

This document is protected by applicable copyright laws. You may not show, adapt, or distribute this document or any part thereof without prior express written consent of copyright holder.

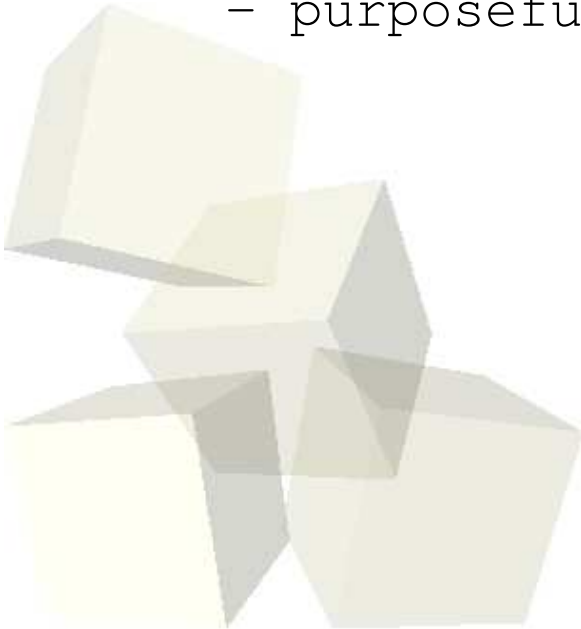


Incident Response & Data Forensics Using Linux

Building Your Linux Toolbox

Building your Linux toolbox

- large number of programs exist!
- what's discussed here is a sampling of what's available
- attempt to focus on the 'best';
 - user friendly
 - sound functionality / accurate
 - purposeful / features



Copyright ©2004 Thomas Rude All Rights Reserved

This document is protected by applicable copyright laws. You may not show, adapt, or distribute this document or any part thereof without prior express written consent of copyright holder.



Incident Response & Data Forensics Using Linux

Building Your Linux Toolbox

Building your Linux toolbox



Linux Toolbox

Windows Toolbox



Which do you prefer?

Copyright ©2004 Thomas Rude All Rights Reserved

This document is protected by applicable copyright laws. You may not show, adapt, or distribute this document or any part thereof without prior express written consent of copyright holder.



Acquisition Utilities

- tools to acquire media

--- 'dd'

----- part of 'coreutils' package from www.gnu.org

----- flexible, options, customizable

--- 'dd_rhelp'

----- useful for bad media (sectors)

----- www.kalysto.ath.cx/utilities/dd_rhelp/index.en.html

--- 'sdd'

----- modified version of 'dd' to include MD5 value, IBS/OBS enhancements, etc.

--- 'SMART for Linux'

----- ability to acquire and clone simultaneously

----- www.asrdata.com

Copyright ©2004 Thomas Rude All Rights Reserved

This document is protected by applicable copyright laws. You may not show, adapt, or distribute this document or any part thereof without prior express written consent of copyright holder.



Incident Response & Data Forensics Using Linux

Building Your Linux Toolbox

Authentication Utilities

- tools that authenticate media in some form

--- 'md5sum'

----- part of 'coreutils' package

--- 'md5deep'

----- recursive MD5, time estimation

----- md5deep.sourceforge.net

--- 'shasum'

----- part of 'coreutils' package

--- 'SMART for Linux'

----- CRC32, MD5, and/or SHA1

----- authenticate against device

Copyright ©2004 Thomas Rude All Rights Reserved

This document is protected by applicable copyright laws. You may not show, adapt, or distribute this document or any part thereof without prior express written consent of copyright holder.



Analysis Utilities

- tools that allow you to analyze media in some manner

--- 'e2retrieve'

----- recover deleted files from ext2 filesystem

--- 'fatback'

----- recover deleted files from FAT filesystem

--- 'file'

----- useful for determination of file type

--- 'find'

----- used to find something & pass arguments

--- 'foremost'

----- carve for deleted files via headers and footers

Copyright ©2004 Thomas Rude All Rights Reserved

This document is protected by applicable copyright laws. You may not show, adapt, or distribute this document or any part thereof without prior express written consent of copyright holder.



Incident Response & Data Forensics Using Linux

Building Your Linux Toolbox

Analysis Utilities

- tools that allow you to analyze media in some manner
 - 'gpart'
 - rebuild damaged partition table(s)
 - 'lde'
 - Linux disk editor, recover deleted files
 - 'memdump'
 - dump contents of memory on *nix systems
 - 'memget' and 'procget'
 - dump memory and /proc information
 - 'recoverdm'
 - recover data from bad sectors, including CD/DVD

Copyright ©2004 Thomas Rude All Rights Reserved

This document is protected by applicable copyright laws. You may not show, adapt, or distribute this document or any part thereof without prior express written consent of copyright holder.

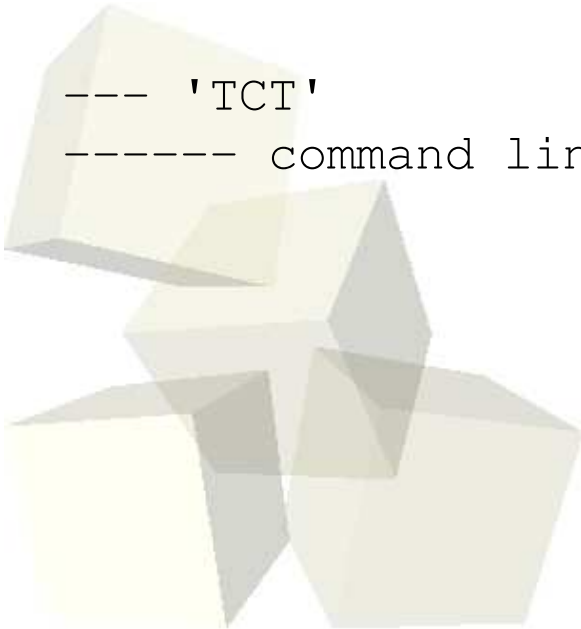


Incident Response & Data Forensics Using Linux

Building Your Linux Toolbox

Analysis Utilities

- tools that allow you to analyze media in some manner
 - 'Sleuthkit'
 - modified TCTutils, uses AUTOPSY web browser GUI
 - 'SMART for Linux'
 - commercial Linux data forensic program
 - functionality and feature rich
 - 'TCT'
 - command line based tools for data forensics



Copyright ©2004 Thomas Rude All Rights Reserved

This document is protected by applicable copyright laws. You may not show, adapt, or distribute this document or any part thereof without prior express written consent of copyright holder.



Incident Response & Data Forensics Using Linux

Building Your Linux Toolbox

Completing Your Linux Toolbox

- tools that were designed to perform data forensic processes

|_ _ _ 'SMART for Linux' www.asrdata.com

|_ _ _ _ _ feature-rich, point and click GUI program

|_ _ _ _ _ sector matching acquisition component

|_ _ _ _ _ robust authentication capabilities

|_ _ _ _ _ on-the-fly compression for images

|_ _ _ _ _ filesystem study feature

|_ _ _ _ _ LAN/WAN acquisition friendly

|_ _ _ 'Sleuthkit' www.sleuthkit.org

|_ _ _ _ _ collection of command utilities

|_ _ _ _ _ uses web browser interface

|_ _ _ _ _ view timeline activity

|_ _ _ _ _ sort files by category

|_ _ _ _ _ image thumbnail viewer

Copyright ©2004 Thomas Rude All Rights Reserved

This document is protected by applicable copyright laws. You may not show, adapt, or distribute this document or any part thereof without prior express written consent of copyright holder.



Incident Response & Data Forensics Using Linux

Building Your Linux Toolbox

Sleuthkit

- collection of command line tools
- 'Autopsy' front end, web browser GUI
- support disk layouts for;
 - DOS partitions
 - BSD disklabels
 - Macintosh partitions
 - Sun slices
- support FS TYPES;
 - FAT
 - NTFS
 - ext2/ext3
 - FFS

Copyright ©2004 Thomas Rude All Rights Reserved

This document is protected by applicable copyright laws. You may not show, adapt, or distribute this document or any part thereof without prior express written consent of copyright holder.

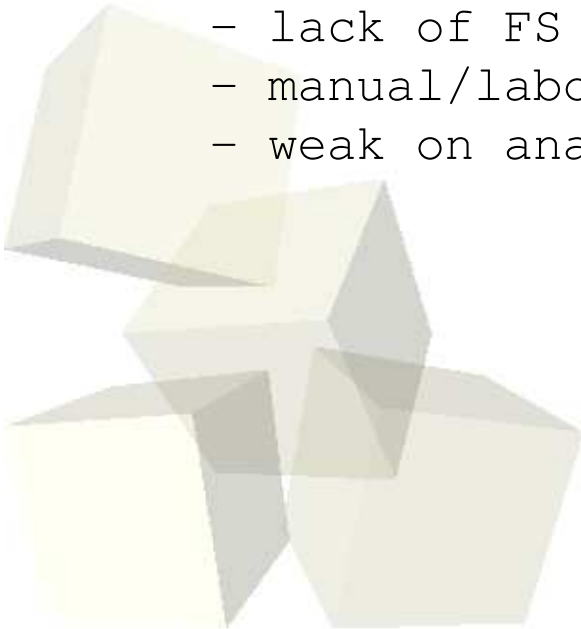


Incident Response & Data Forensics Using Linux

Building Your Linux Toolbox

Sleuthkit

- Strengths
 - financially free
 - thumbnail generator & viewer
 - hashset importer
 - file signature analysis
- Weaknesses
 - cannot acquire
 - lack of FS TYPES support
 - manual/laborious setup and case management
 - weak on analysis features



Copyright ©2004 Thomas Rude All Rights Reserved

This document is protected by applicable copyright laws. You may not show, adapt, or distribute this document or any part thereof without prior express written consent of copyright holder.



Incident Response & Data Forensics Using Linux

Building Your Linux Toolbox

SMART for Linux

- full graphical point and click program
- plugin architecture
- right-click happy
- support disk layouts for;
 - all supported by Linux
- support FS TYPES;
 - all supported by Linux
 - SMART FS plugins (FAT12/16/32, NTFS, ext2/ext3)

Copyright ©2004 Thomas Rude All Rights Reserved

This document is protected by applicable copyright laws. You may not show, adapt, or distribute this document or any part thereof without prior express written consent of copyright holder.



Incident Response & Data Forensics Using Linux

Building Your Linux Toolbox

SMART for Linux

- Strengths
 - acquire and clone simultaneously
 - customization for acquisition, analysis, & authentication
 - Filesystem Study feature
 - Stackable filtering
 - Logging/reporting
 - network capable
 - well documented user manual
 - hash set creator and importer
 - boot CD-ROM
- Weaknesses
 - not financially free
 - SMP issues

Copyright ©2004 Thomas Rude All Rights Reserved

This document is protected by applicable copyright laws. You may not show, adapt, or distribute this document or any part thereof without prior express written consent of copyright holder.



Incident Response & Data Forensics Using Linux

Building Your Linux Toolbox

Your Linux Toolbox!

	SMART	Sleuthkit	FLAG
Acquire Physical Image	X		
Acquire Logical Image	X		
Acquire via Network (LAN or WAN)	X		
Acquire & Clone Simultaneously	X		
Custom Acquisition (sectors, etc.)	X		
Authenticate (CRC32, MD5SUM, SHA1)	X	X	X
Search	X	X	X
Bootable CD	X		
Deleted File Recovery ext2	FATx, NTFS, ext2	FATx, ext2	FATx,

Wiping Feature

Copyright ©2004 Thomas Rude All Rights Reserved

This document is protected by applicable copyright laws. You may not show, adapt, or distribute this document or any part thereof without prior express written consent of copyright holder.

X



Incident Response & Data Forensics Using Linux

Building Your Linux Toolbox

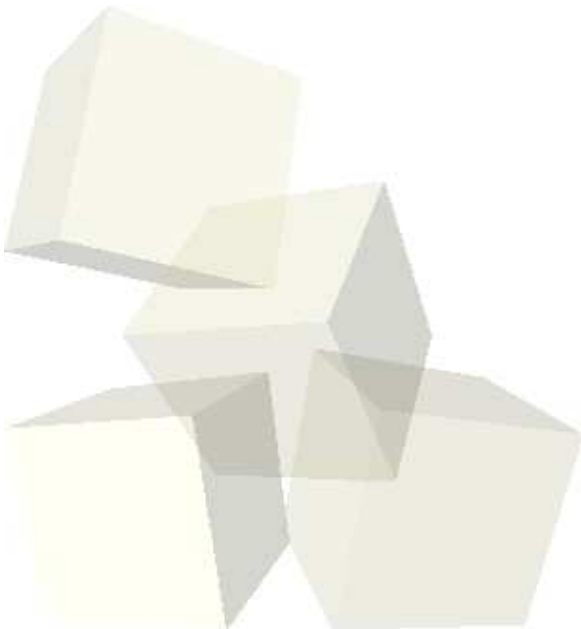
Linux Resources

www.crazytrain.com

www.smartforensics.net

www.opensourceforensics.org

http://groups.yahoo.com/group/linux_forensics/



Copyright ©2004 Thomas Rude All Rights Reserved

This document is protected by applicable copyright laws. You may not show, adapt, or distribute this document or any part thereof without prior express written consent of copyright holder.

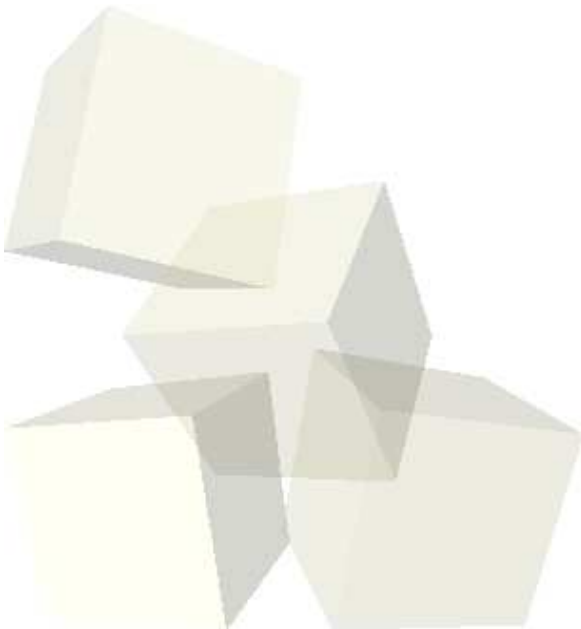


Incident Response & Data Forensics Using Linux

Building Your Linux Toolbox

Questions?

`farmerdude@crazytrain.com`



Copyright ©2004 Thomas Rude All Rights Reserved

This document is protected by applicable copyright laws. You may not show, adapt, or distribute this document or any part thereof without prior express written consent of copyright holder.