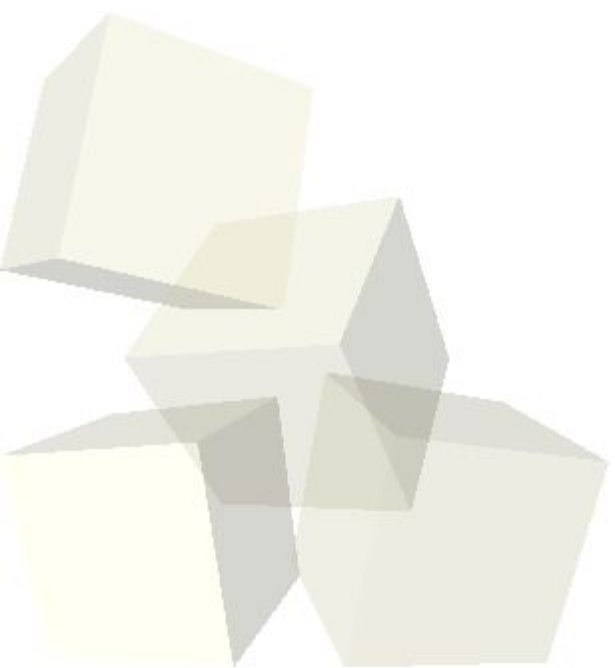




Southeast
Cybercrime Summit
Atlanta, GA

*A digital world
requires digital protectors*

2-5 March 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.



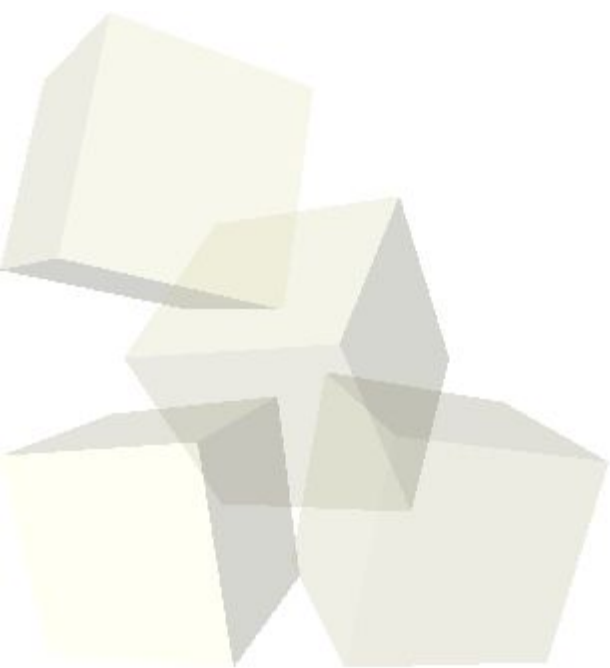


Proactive vs. Reactive Incident Response & Data Forensics

Why Linux (why *not* Microsoft)?

Your Linux Toolbox!

Questions?

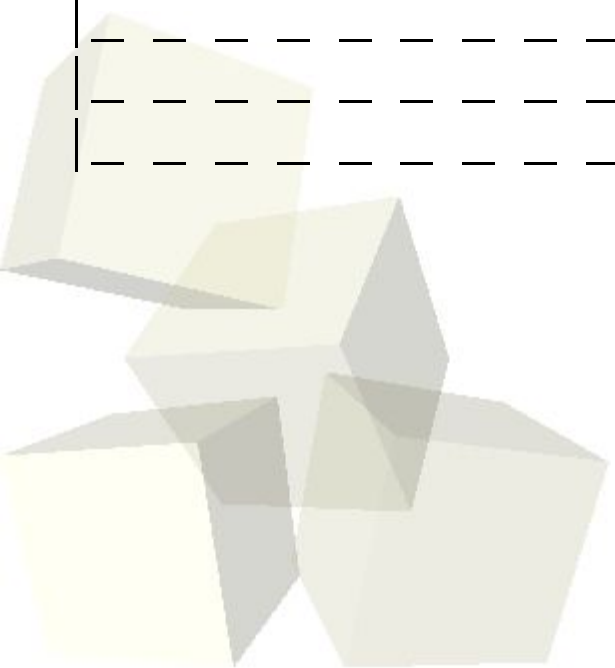




Proactive vs. Reactive Incident Response & Data Forensics

- Reactive Incident Response & Data Forensics

- | _ _ _ current majority and historical norm
- | _ _ _ _ _ stand-alone personal computers
- | _ _ _ _ _ typically Win32 variant
- |
- | _ _ _ _ _ postmortem analysis
- | _ _ _ _ _ no processes
- | _ _ _ _ _ no system state
- | _ _ _ _ _ volatile information?
- | _ _ _ _ _ crypto?





Why Linux (why *not* Microsoft)?

- Power of the Penguin
 - _ _ _ minimally invasive by default
 - _ _ _ _ _ no write blocker required
 - _ _ _ filesystem types support
 - _ _ _ _ _ one system to analyze any number of systems
 - _ _ _ operating system control and granularity
 - _ _ _ _ _ monitor and log actions
 - _ _ _ loopback device
 - _ _ _ _ _ mount filesystem contained within regular file & browse logical structure



Linux is Minimally Invasive!

- Minimally invasive
- by default Linux will **not** stomp (or lightly brush against) on evidentiary media
 - _ _ _ safely attach media
 - _ _ _ _ _ SD, compact flash, memory sticks, hard drives
 - _ _ _ **can** use hardware write blocker
 - _ _ _ _ _ if you feel compelled, if you feel the need
 - _ _ _ '/var/log/messages'
 - _ _ _ _ _ attach device & view system log
 - _ _ _ _ _ '/proc' filesystem to glean more hardware info



One Linux System can Analyze Numerous Other Systems!

- filesystem types support
 - we can use one system (Linux) to analyze numerous systems
 - | _ _ _ mount disk-based filesystems
 - | _ _ _ _ _ VFAT, NTFS, ext2/ext3, ReiserFS, XFS, JFS, HFS+
 - | _ _ _ mount network filesystems
 - | _ _ _ _ _ AFS, Coda, NFS, etc.
 - | _ _ _ browse logical structure
 - | _ _ _ review active content
 - | _ _ _ permissions, credentials, etc.
 - | _ _ _ Virtual Filesystem Layer (VFS)
- (`'/usr/src/kernel_version/Documentation/filesystems/vfs.txt'`)



Linux Gives Control to YOU!

- granular control of the Linux Operating System Environment (LOSE)
- we can monitor and log actions, as well as control behavior
 - |_ _ _ monitor actions
 - |_ _ _ _ _ 'script'
 - |_ _ _ _ _ 'strace'
 - |_ _ _ everything is a file
 - |_ _ _ _ _ security & control



Linux & Loopback - the Perfect Pair!

- loopback device allows us to treat a regular file as a block device
- a filesystem contained within a file may be mounted locally
 - _ _ _ maximum of 255 loop device files ('/dev/loop0', etc.)
 - _ _ _ specified during 'mount' command
 - _ _ _ _ _ 'mount -o ro,loop *file_name* *mount_point*'
 - _ _ _ specify offset of filesystem within physical image
 - _ _ _ _ _ 'mount -o ro,loop,offset=28672 *file_name*
mount_point '
 - _ _ _ once mounted logical structure & content may be viewed



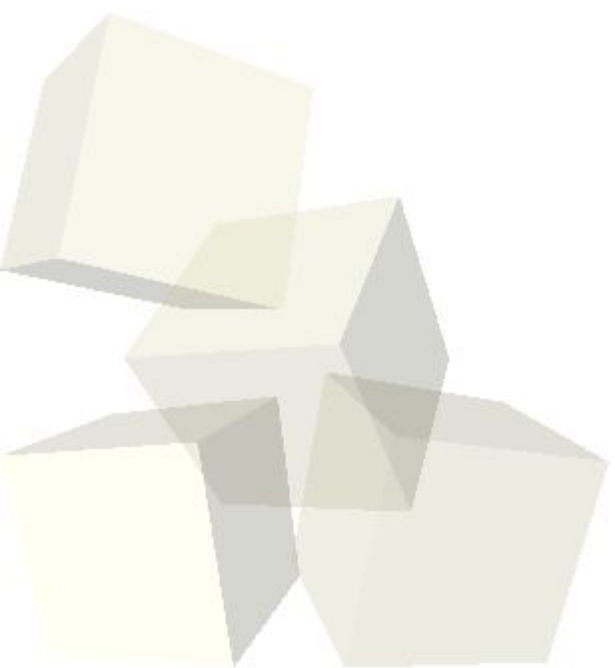
Your Linux Toolbox!

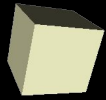
- acquisition utilities
- tools that acquire media in some form
 - | _ _ _ 'dd'
 - | _ _ _ _ _ _ probably the best, for all media
 - | _ _ _ _ _ _ acquire, create files, convert data, & wipe media
 - | _ _ _ 'dcfldd'
 - | _ _ _ _ _ _ mod'd version of 'dd' to include MD5 value of data
 - | _ _ _ 'sdd' (sdd+)
 - | _ _ _ _ _ _ mod'd version of 'dd' to include MD5 value, IBS/OBS enhancements, etc.



Your Linux Toolbox!

- authentication utilities
- tools that authenticate media in some form
 - |_ _ _ 'cksum'
 - |_ _ _ 'md5sum'
 - |_ _ _ 'sha1sum'
 - |_ _ _ 'md5deep'





Your Linux Toolbox!

- analysis utilities
- tools that allow you to analyze media in some manner
 - | _ _ _ 'file'
 - | _ _ _ _ _ _ _ used to determine type of file
 - | _ _ _ 'find'
 - | _ _ _ _ _ _ _ used to find something & pass arguments
 - | _ _ _ 'egrep' 'fgrep' 'grep' 'mailgrep'
 - | _ _ _ _ _ _ _ used to search for something
 - | _ _ _ 'ls'
 - | _ _ _ _ _ _ _ used to list directory contents
 - | _ _ _ 'hdparm'
 - | _ _ _ _ _ _ _ used to get hard drive information (or set it)



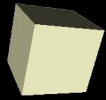
Your Linux Toolbox!

- live analysis utilities
- tools that allow you to analyze live media in some manner
 - |_ _ _ 'script'
 - |_ _ _ _ _ _ _ used to make typescript of terminal session
 - |_ _ _ 'date' 'clock'
 - |_ _ _ _ _ _ _ gather system date & time, & processor time
 - |_ _ _ 'ps' 'pstree' 'lsof' 'top'
 - |_ _ _ _ _ _ _ used to gather process information and open files
 - |_ _ _ 'id' 'whoami' 'who' 'finger'
 - |_ _ _ _ _ _ _ used to gather user information



Your Linux Toolbox!

- data forensic programs
- 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



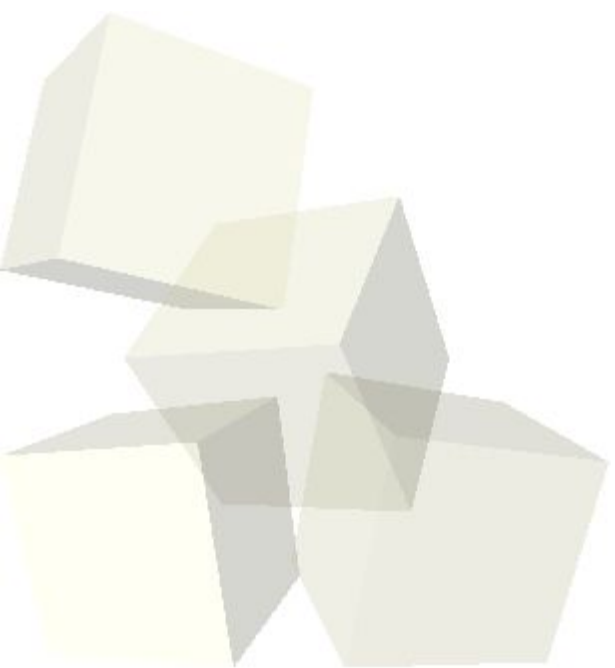
Linux Resources

www.crazytrain.com

www.smartforensics.net

www.opensourceforensics.org

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



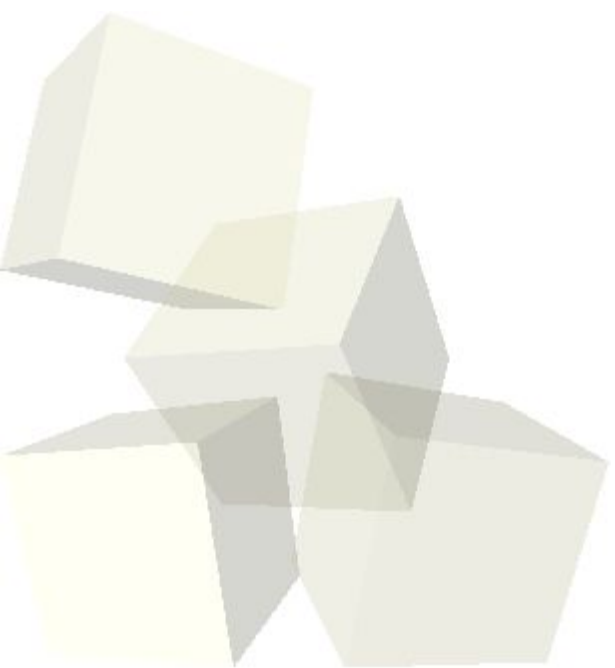
Copyright ©2004 Thomas Rude All Rights Reserved

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.



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.