Look Ma, no disks! When CSI Comes to Your Data Center

Richard Austin, CISSP
Hewlett Packard
SNIA Notice

- The material contained in this tutorial is copyrighted by the SNIA.
- Member companies and individuals may use this material in presentations and literature under the following conditions:
  - Any slide or slides used must be reproduced without modification
  - The SNIA must be acknowledged as source of any material used in the body of any document containing material from these presentations.
- This presentation is a project of the SNIA Education Committee.
Why you should care

• A detective in a child pornography case has a search warrant to seize an employee’s files that reside on your 130TB storage array
• The web server backup has been running twice as long as normal and you find that the web server has mounted the LUNs belonging to the finance department
• Three senior storage administrators are terminated in a downsizing effort. Later that day, the LUNs belonging to the engineering department disappear from the storage array
Why you do care

• Most of current forensics knowledge and practice applies to server attached storage
• This makes the storage admin **the expert** when the forensic technician looks at the server and exclaims “Look ma! No Disks!”
• Would you know the proper steps to take?
Abstract

- With more and more corporate information being centralized in large storage networks, the likelihood of storage administrators being involved in collecting and preserving evidence for use in legal proceedings as a result of intrusion, policy violation, litigation or some form of criminal activity has increased dramatically.
- This presentation will provide a brief, *whirlwind* tour of the world of digital forensics in the context of enterprise storage networks by reviewing the overall place of forensics in the incident response process, required security policy support, sources and types of digital evidence, the legal requirements and controls required for its collection and preservation as well as some commonly used tools.
- Digital forensic technology also poses threats to confidentiality when equipment is discarded or recycled and a brief mention of the growing field of anti-forensics will be made.
- This presentation will focus mainly on fibre channel SANs but the general principles also apply to NAS and iSCSI SANs.
DISCLAIMER

• Forensics is an area where legal issues and technology overlap. **ALWAYS** seek competent legal counsel in this area.

• The author is not an attorney and nothing in this presentation is intended to be nor should be construed as legal advice or opinion.

• The information presented herein represents the author’s personal opinion and current understanding of the issues involved. Neither the author, Hewlett Packard nor SNIA assume any responsibility or liability for damages arising out of any reliance on or use of this information.
What is “forensics”?  

• Webster – from L forensis fr forum. Belonging to, used in or suitable to courts of judicature or to public discussion and debate
• Saferstein – Forensic science in its broadest definition is the application of science to law
• Computer forensics – using accepted methods and procedures to properly seize, safeguard and analyze data. (Kroll Ontrack)
Why it’s important

• Regulatory and other legal obligations
  – New Federal Rules of Civil Practice (FRCP) emphasize importance of Electronically Stored Information (ESI)

• Support a dismissal decision and defend against a wrongful termination action

• Support or defend against a legal action
  • Theft of intellectual property
  • Tampering, willful-destruction, etc

• Criminal Investigation
  – Fraud, terrorism, etc
Evidence

• An item does not officially become a piece of evidence until a court admits it as such
  – Opposing counsel can challenge this admission

• When we use the word “evidence” we’re using it as a shortcut for “item of potential evidentiary value”

• Much of forensics practice concerns how to collect and analyze these items without compromising their potential to be admitted as evidence in a court of law
A Serious Business

- Evidence may save or cost an enterprise millions of dollars
- Evidence may deprive a person of their liberty in a criminal matter (which now includes corporate governance)
- Evidence may deprive a person of their livelihood if it leads to termination of employment

Because of the serious nature of these consequences, the legal system imposes stringent requirements for information to be used as evidence in their proceedings.
Requirements

• Relevant
  – Has an important role in deciding a question of fact

• Authentic
  – The “real” thing

• Integrity Preserved
  – From collection through analysis to presentation
  – Unbroken chain of custody
DIY attempts to gather evidence will almost certainly fail. It’s best to call the experts as soon as you can.

Simon Janes
Former Head of Computer Crime Unit, New Scotland Yard
SC Magazine, September, 2004
Organizational Policy

Incident response is **NOT** the time to be either developing policy **OR** learning how to identify and collect evidence in a forensically sound manner.

Policy must:

- deal with expectation of privacy and the practice of continuous monitoring
- define roles, processes and notifications for incident detection and response
- Be reviewed with legal counsel at least annually
Overall Process Flow

Policy Violation or Crime Detected → Prepare Affidavit Seeking Authorization to Investigate → Investigation Authorized?

- Yes → Collect Evidence → Security Incident Triggers Incident Response Process
- No → Archive

Either externally or internally

Archive → Produce Report and Submit for Disposition → Analyze Evidence
Sources of Evidence

Data on Disk

Live Logs on Switches

Server Logs

Log Records from IDS

Archived Log Records

syslogd server
Data on Disk

- The “meat and potatoes” of traditional digital forensics
- Usual procedure is to image the disk for later analysis
- Imperative to use sound processes and procedures
- Challenges do exist for SAN disks
Forensic Imaging vs File Copy

Two files would be picked up by a normal file copy (File 1 and File 3)

Un-deleting files before copying would additionally pick up file 4 (but at the cost of modifying the disk)

A bit-stream copy that copied each block of the disk would retrieve the two files, the remnants of file 2 (slack space), the deleted file, the free space and the directory
Disk Imaging

• Must meet the evidentiary requirements
  – Authentic
    • Document when, where, how and who collected the image in a signed and witnessed statement
    • Cryptographic hash to establish a baseline integrity reference
    • Imaging cannot modify the source disk in any way
  – Integrity Preserved
    • Document the “chain of custody”
      – Where the item was from collection to analysis to presentation
      – Who accessed it, when and why
Authenticating Evidence

• Digital information is highly volatile, easily changed or destroyed

• How can a specific piece of digital evidence be identified and its integrity verified?
  – By means of a “digital fingerprint” such as a cryptographic hash
Digital Fingerprint

@echo hello there>test.txt
@md5sum test.txt
d03d3fe9afff7a635879916173c1b383 *test.txt

@echo Hello There>test.txt
@md5sum test.txt
4e6a9dbf7699455525018b368c85d123 *test.txt

- Simply capitalizing two letters generated wildly different hash values
- Cryptographic hashes are used as a sort of “digital fingerprint” to demonstrate integrity
- Commonly MD5 or SHA are used

But wait, isn’t MD5 broken?
Imaging Tools

• Wide variety to choose from:
  – Specialized Hardware tools
    • $$$
  – Software tools provided by forensic tool vendors
    • $$
  – Standard Linux utilities such as dd
    • Enhanced versions such as dcfldd and sdd
    • FREE

• Make **sure** you understand how to use your tool of choice
Why Linux CD’s?

- Linux is highly customizable and can be easily specialized for forensic use
- When dealing with a potentially compromised system, you cannot trust anything running on it
  - CD’s are read-only
  - Are built with known versions of trusted tools
Black Bag Kit
Imaging Walkthrough

  - Downloadable ISO image
  - Both live response and bootable
- Introductory Guide
- Optimized for forensic use
  - Specialized tools
  - Does not mount any disk filesystems
    - Mounts a RAM-disk on /dev/ramdisk for temporary storage
- Other Options:
  - Knoppix STD
  - F.I.R.E.
  - Penguin Sleuth Kit
Field Imaging Setup

Suitable for PCs and small servers but probably not a SAN disk array
Imaging Process

- Make sure the target disk is “sterile”
  - Put the soap away, that means it contains no traces of previous contents
- Calculate and record a baseline hash for the suspect disk
- Image the suspect disk
- Calculate and record the hash of the image
  - It should (and had better) match the one for the source
- Package image for transportation
dd command

- Used to generate a bit stream image
- Syntax
  ```
  dd if=input_file of=output_file options
  ```
- Common options
  - `bs=block_size`
  - `conv=noerror,notrunc,sync`
- Example: Copy the contents of first IDE drive to the second IDE drive
  ```
  dd if=/dev/hda of=/dev/hdb bs=4096 conv=noerror,notrunc,sync
  ```
- Note that target does not have to be the same size or technology (e.g., target could be SCSI). Target just has to be bigger than the source.
- `sdd` is an enhanced version with better performance
Sterile Targets

- Eliminate any traces of previous contents
- Prevents allegations of contamination
- Easily done by writing zeroes or random data to the target drive

Writing Zeroes
dd if=/dev/zero of=/dev/hdb bs=1024k

Writing Random Characters
dd if=/dev/urandom of=/dev/hdb bs=1024k
Imaging a Disk

Identify which disks are which

Target Drive

Mount a filesystem on the TARGET so we can write files to it

Task is to image the SUSPECT drive /dev/hda to a file on the forensic TARGET /dev/hdb1
Imaging a Disk

- Calculate the baseline hash and store it as b4HashItem01.MD5
  - `md5sum /dev/hda>/mnt/target/b4HashItem01.MD5`

- Image the suspect disk to a file on the target as Item01.IMG
  - `dd if=/dev/hda of=/mnt/target/Item01.img bs=4096`

- Calculate the hash of the target and store it as afHashItem01.MD5
  - `md5sum /mnt/target/Item01.IMG>afHashItem01.MD5`

- Compare the hashes to verify they match
  - `cat *.MD5`
    ```
    e70fb5d596d6544ad9a87e54f5928751  /dev/hda
    e70fb5d596d6544ad9a87e54f5928751  /mnt/target/Item01.IMG
    ```
Document

• Documentation helps assure both authenticity and integrity
• Create a permanent record of what you’re doing
  – In a permanently **BOUND** record book
  – Sufficient detail that a similarly experienced person could follow the same procedure and expect similar results
  – Sufficient detail to support your testimony even years after the actual event
  – Sign, date and have it witnessed
• Document in **WRITING** the hash values!
  – A signed, witnessed statement of these values supports your claim of authenticity and integrity
  – And yes, I know an electronic copy is on the target drive
Package and Secure

- Forms help you collect all relevant information
- Use tamper evident packaging
  - Seals “self destruct” when opened
- Pay attention to ESD and other precautions appropriate to magnetic media
- Store in a controlled-access location
  - A locked desk drawer will do if that’s all you have
Package and Secure
Package and Secure

- Sign across all seals
  - Prevents someone else from opening the package and replacing the seal without detection
- Document the item both on a label attached to it and on the external envelope
- Maintain *personal* custody and control of the item until it is locked away
### CHAIN of CUSTODY LOG

<table>
<thead>
<tr>
<th>Case Number</th>
<th>Item Number</th>
<th>Relinquished By</th>
<th>Date / Time</th>
<th>Received By</th>
<th>Date / Time</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>PRINTED</td>
<td></td>
<td>PRINTED</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>SIGNATURE</td>
<td></td>
<td>SIGNATURE</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>PRINTED</td>
<td></td>
<td>PRINTED</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>SIGNATURE</td>
<td></td>
<td>SIGNATURE</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>PRINTED</td>
<td></td>
<td>PRINTED</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>SIGNATURE</td>
<td></td>
<td>SIGNATURE</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>PRINTED</td>
<td></td>
<td>PRINTED</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>SIGNATURE</td>
<td></td>
<td>SIGNATURE</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>PRINTED</td>
<td></td>
<td>PRINTED</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>SIGNATURE</td>
<td></td>
<td>SIGNATURE</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**WARNING**

Receiver’s signature warrants that evidence seal was intact with no visible sign of tampering except as noted under Notes at time of receipt.

The Chain of Custody form documents each and every access to the item.

Note the statement on the integrity of the seal as each person receives it.
Process and Procedure

• Process and procedure are boring yet **critical**!
• Most cases are lost here
  – Very seldom is the actual evidence itself challenged
    (e.g., hard to deny that it IS a picture of a nude
    prepubescent child in a sexual situation)
  – Can challenge based on authenticity
  – Can challenge based on “broken” chain of custody
  – Can challenge on how it came to be there (SODDI)
• Attorneys receive training on how to challenge
  forensic evidence
Challenges in SANs

• Size of our arrays typically preclude imaging the “whole thing”

• Very few (see also: none that I’m aware of) imaging tools can “speak” fibre channel”
  – Being added to Helix in a future release

• Write-blocked HBA’s still not widely available

• Does that mean we can’t do forensic data collection and preservation?

Of course not!
Imaging in the SAN Environment

• Image the relevant LUN
  – A SAN LUN is really just a disk (as Roger Cummings once opined “just a bunch of sectors”)

• Use an imaging platform that supports fibre channel and allows you to mount the LUN as read-only
  – Linux-based tools work really well in this environment
    • Make sure the distro supports your HBAs

• Once you have access to the LUN, image it just like it was a any other disk
Analysis

- Forensic analysis typically handled by specially trained people or consultants using specialized tools
- These tools excel at dealing with deleted files, file fragments, operating system and browser artifacts
Other Information Sources

• Most devices common in the SAN environment are intelligent and can collect and generate log records of activities occurring on them
  – A simple example is the authentication-failed messages a switch might generate during a brute force password attack

• These log records can be a valuable tool in establishing what happened and its progress over time
Preparing for Collecting Logs

• Store logs off the device
  – Any “hacker” worthy of the name will attempt to destroy any record of their activities
  – For example, an intruder that modifies a zoning configuration to grant unauthorized access to LUNs will likely clear the switch log

• syslogd servers provide a centralized repository for log records in real time
  – See SNIA whitepaper “Audit Logging for Storage”
  – Protect them appropriately (intruders know about syslogd too)
Correlating Logs

- Multiple sources of logs are a harsh reality in our environment
- Prepare in advance for being able to correlate log records across sources
  - Accurate, standard time source such as a NTP server
  - Set switch timezone to “0” to use ZULU time
    - While many switch vendors do support time zones, few automatically switch from “daylight savings” or “summer time” to standard time
    - Avoid the whole problem with using accurate UT across the fabric
Example: Failed Logon

Time Stamp at syslogd server


Message

Note the 4hr difference between the server time stamp and the device time stamp (hint: this device is located in the US Eastern Time Zone)
Collecting Logs

• “Freeze” the logs
  – Establishes a definite point in time
  – Can be done by simply copying the log file (or more radically by pulling the network cable)

• Document what you do
  – Bound notebook
  – Witnessed record

• Use a cryptographic hash of the acquired log file to establish a baseline integrity reference

• Treat the copy of the log file just like it was a disk image
  – Package and secure
  – Maintain a documented chain of custody
Live Logs

- The intruder may have cleared them (but that is an important fact as well)
- Will require live access to the device
  - Be prepared to testify to **EXACTLY** everything you did and its **consequences** to the information you collected
  - For example, logging on to dump the logs will likely create a LOGON record
  - Do the **absolute minimum** necessary to collect the logs
    - Resist any temptation to poke about to find out what the intruder may have done
- Download the log, immediately calculate a baseline hash and document it
- Treat the downloaded copy similarly to a disk image
  - Package and secure
  - Maintain a documented chain of custody
Anti-Forensics

• Forensic tools have a darker side where they can be used to recover information that you thought was “deleted”

• See Simson Garfinkel’s excellent presentation from Black Hat Federal 2006 on how much information is “leaked” through discarded and recycled disks:
  
Anti Forensics

• When data is destroyed, it must be destroyed in a forensically sound fashion
  – Deleting a file is a joke to a forensic tool
  – Most system formats of media simple re-initialize the O/S disk data structures and leave the data intact (it’s not called a “quick format” for nothing)

• Data destruction typically requires overwriting each sector of the disk at least once to render the original information “unrecoverable”
Sanitizing Media Example

The `shred` command on Linux can be used to shred a file or an entire device

```
shred -n 2 -v -z /dev/hdb
```

- `-n 2` specifies two overwrite passes with random data (default is 25 passes)
- `-v` specifies verbose output (e.g., show progress)
- `-z` specifies that the device is to be overwritten with 0’s as the last step

Choosing A Utility

- See the guidance in NIST Draft publication SP800-88 “Guidelines for Media Sanitization”
- Assure that the utility can handle fibre channel LUNs
- Be aware that data destruction is being mandated in many environments:
  - Payment Card Industry (PCI DSS)
  - DoD5015.2
  - Sedona Principles
  - NIST800-14
  - NIST800-53
  - ISO17799 (9.2.6, 10.7.1 and 10.7.2)
  - ISO27001 (for the overall Management system)
For More Information

www.e-evidence.info

www.tritechusa.com – forensic supplies

http://www.staticbags.com/
Appendix: The Black Bag Kit

- Write Blocker Kit
- Lockable evidence transport container
- Forensic Target Disk in Enclosure
- The Black Bag
- ESD Field Workstation
- Helix CD
- Tie-On Tags
- Power strip
- ESD Warning Labels
- Static Bags

- Evidence Bags
- Evidence Seals
- Powered USB Hub
- USB 3.5” Drive
- Evidence Labels
- Integrity Seals
- Box of assorted nuts, screws, etc
- USB Memory Card Reader
- Tool Kit
Q&A / Feedback

Please send any questions or comments on this presentation to SNIA at tracksecurity@snia.org

Many thanks to the following individuals for their contributions to this tutorial.

Richard Austin, CISSP
David Black
LeRoy Budnik, CISA
Roger Cummings
Eric Hibbard, CISSP, CISA

Larry Hofer, CISSP
Phil Huml
Mike Whitman, CISSP
SW Worth