Do-It-Yourself Guide to Storage Forensics

Richard Austin, CISSP
Knowledge Transfer
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.
Abstract

DIY Guide to Storage Forensics
As more and more enterprise information is consolidated into storage area networks, the likelihood of storage administrators finding themselves challenged to identify, collect and preserve electronic evidence relevant to an intrusion, crime, policy violation or e-discovery request is steadily increasing. This presentation presents a whirlwind tour of the processes for collecting and preserving digital evidence and the challenges traditional forensics practitioners face in a world where servers may have no directly attached disks.
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, Knowledge Transfer nor SNIA assume any responsibility or liability for damages arising out of any reliance on or use of this information.
I’ve seen CSI but what is this “forensics” thing?
A Primer on Evidence
Policy – the first step
The Forensics Process
Collecting Evidence
  ♦ Data on Disk
  ♦ Log Records
Why does it matter?

- Regulatory and other legal obligations
  - New Federal Rules of Civil Practice (FRCP) specifically recognize the importance of Electronically Stored Information (ESI)
  - Support a dismissal decision and defend against a wrongful termination action
  - Support or defend against other legal actions
    - Theft of intellectual property
    - Tampering, willful-destruction, etc

- Criminal Investigation
  - Fraud, terrorism, etc
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)
Evidence

- An item does not officially become a piece of evidence until a court admits it as such
  - Opposing counsel can challenge this admission
- The word “evidence” is used here as a shortcut for “item of potential evidentiary value”
- Forensics practice is concerned with identifying, collecting and analyzing these items without compromising their potential to be admitted as evidence in a court of law
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
This is a private system

Management reserves the right to examine all data stored in or transmitted by these systems.
... without prior notice, management reserves the right to examine archived electronic mail, private file directories, hard disk drive files, and other information stored on company information systems.
...workers must have no expectation of privacy associated with the information they store in or send through these systems.

I have read and understood

Policies communicated and agreed to in writing
Forensics Process

1. Policy Violation or Crime Suspected
2. Seek Authorization to Investigate
3. Investigation Authorized?
   - Yes: Collect Evidence
   - No: Archive
4. E-discovery Request
5. Incident Response
6. Collect Evidence
7. Archive
8. Produce Report and Submit for Disposition
9. Analyze Evidence
Sources of Evidence

- Data on Disk
- Log Records from IDS
- Archived Log Records
- Live Logs on Switches
- Server Logs

DIY Guide to Storage Forensics
© 2007 Storage Networking Industry Association. All Rights Reserved.
Data on Disk

- Most common subject of forensic investigation
  - Also common in e-discovery for preserving information sources for later culling to identify relevant information
- Sound, repeatable process is critical
- Very common to create a bit stream image for later analysis
A normal file copy would only copy File 1 and File 3

Un-deleting files before copying would retrieve file 4 but would modify the disk contents

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
Authenticating Evidence

- Digital information is highly volatile, easily changed or destroyed
- How can a specific piece of digital evidence be authenticated 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 changing the case of two letters generated wildly different hash values
- Cryptographic hashes are used to produce a sort of “digital fingerprint” to demonstrate authenticity and integrity
- Commonly MD5 or SHA are used
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

- Become very familiar with the tool you use and make sure it is accepted in legal circles
Why A Linux CD?

- 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
Imaging Walkthrough

- http://www.e-fense.com/Helix (free)
  - Downloadable ISO image
  - Both live response and bootable
  - Current version is 1.9

- 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

For SAN storage, a small server replaces the laptop
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
  \[
  \text{dd if=} \text{input\_file of=} \text{output\_file options}
  \]
- Common options
  - `bs=block_size`
  - `conv=noerror,notrunc,sync`
- Example: Copy the contents of first IDE drive to the second IDE drive
  
  \[
  \text{dd if}=/\text{dev/hda of}=/\text{dev/hdb bs}=4096 \text{ conv}=\text{noerror,notrunc,sync}
  \]
- Note that target does not have to be the same size or technology -- 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

Task is to image the SUSPECT drive /dev/hda to a file on the forensic TARGET /dev/hdb.

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

Suspect Drive

Target Drive

Mount a filesystem on the TARGET so we can write files to it.
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`
Documentation helps assure both authenticity and integrity

Create a permanent record of your actions

- 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 supplements the electronic copies
Package and Secure

- Forms help you collect the 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
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.
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
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 Sources of Evidence

Most devices common in the SAN environment are intelligent and generate event log records

- 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
Correlating Logs

- Multiple sources of logs are a harsh reality in our environment
- Prepare in advance for being able to correlate log records
  - 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

<table>
<thead>
<tr>
<th>Time Stamp</th>
<th>Message</th>
</tr>
</thead>
</table>

Time Stamp from Device

<table>
<thead>
<tr>
<th>Time Stamp</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>2006/07/22-19:32:44</td>
<td></td>
</tr>
</tbody>
</table>

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)
Good Practices

- 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)
Live Logs

- The intruder may have cleared them (but this 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
Centralized Logs

 опасные газы

“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
For More Information

www.e-evidence.info

www.tritechusa.com – forensic supplies

http://www.staticbags.com/
Q&A / Feedback

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

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

SNIA Education Committee

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

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