

[WP-011]

## Whitepaper: Introduction in IT Forensics Management

A Brief Discussion about IT Forensics Management and How It Will Be Used

**Version 040727**

July 2004

Author: Bob Radvanovsky, [rsradvan@unixworks.com](mailto:rsradvan@unixworks.com)

*(A special thanks goes to those listed for being my “sounding board” on this project.)*

Copyright © 2004 Bob Radvanovsky. All rights reserved.



## Limited Liability Statement

---

In no event shall the author(s) be liable for any found errors contained herein or for any direct, indirect, special, incidental or consequential damages (including lost profit or lost data) whether based on warranty, contract, tort, or any other legal theory in connection with the furnishing, performance, or use of this material.

The information contained within this document may be subject to change without any notice. No trademark, copyright, or patent licenses are expressly or implicitly granted (herein) with this whitepaper.

Documentation pertaining to any security-related technical or proprietary information, its data and all information provided and contained within this document is considered proprietary in nature and subject to copyright protection and is intended solely for use by its owner. Additionally, this documentation is solely for the purpose of discussing a possible, and/or proposed IT security issue, and is not dependent upon any specified infrastructure, architectural condition or its issue(s).

All other product names mentioned herein are trademarks or registered trademarks of their respective owners. NOTE: Any names not outlined or mentioned above are fictional in nature; as such, any relation to any name or trademark (if any) is purely coincidental.

## Introduction

---

Since everything today is going “high tech”, modern-day crimes will require modern-day criminal specialists, especially in problem determination. This opens a completely new realm in a quickly growing industry often referred to as “forensics management”. However, this type of forensics doesn’t deal with dead bodies or spatters of blood. Rather, this type of forensics management deals with 1’s and 0’s. Welcome to the “World of IT Forensics Management”.

What is “forensics management”?

For starters, the word “forensics” is the definition “of the application of science to questions which are of interest to the legal system. For example, forensic pathology is the study of the human body to determine cause and manner of death. Criminalistics is the application of various sciences to answer questions relating to examination and comparison of biological evidence, trace evidence, impression evidence, drugs and firearms. Forensic odontology is the study of the uniqueness of dentition, and forensic toxicology is the study of drugs and poisons, and their effects on the human body”<sup>1</sup>. Similar to studying dead bodies at a crime scene, “IT forensics” however, works with piecing together electronic fingerprints, or traces of tampering or digital trespassing by criminals<sup>2</sup>. All of these clues lead law enforcement into solving possible crimes; as more and more potential criminals turn to computers to perform their activities, similarly, business groups and government agencies will need to become more aware of tools and techniques to catch the digital offenders.



IT forensics deals with many of the aspects of the computer itself, as all evidence is stored, in some form or another, on the target computer. What this translates to is that data, any data, leaves key signature marks and trails behind on the disk drives (hard disk, USB disk, floppy disk), tape drives, or other storage media (such as CD-R, CD-RW or now even DVD-R devices). What can be written can share a wealth of knowledge of what was done, dates, times, and who might have even accessed the data at that time. All are telltale signs of usage, access, and more importantly, if it was tampered with. Everything that is done with any computer that uses any operating system (Microsoft Windows, Mac OS, even Linux), leaves a trail – though it may only be a cookie or a digital signature – with the proper tools and training, an investigator could possibly follow this trail back to its source.

Some of the more common scenarios in which IT forensics evidence may be used include areas such as child pornography, electronic fraud (phishing), corporate fraud, or even terrorism. To make an accusation either an individual or a group of people (many electronic frauds today are conducted with more than one person involved, usually from geographically different locations), recovery of evidential data must be accurate enough to save companies and governments time and perhaps lives.

In many cases, digital offenders often think that deletion of data from a storage medium will remove any evidence of their tampering or trespassing. However, unless the individual has physically tampered or destroyed the storage medium or computer, IT forensics specialists have been successful in retrieving deleted files and directories, much to the surprise of the accused individual(s). And, there are data recovery companies today that are capable of recovering data from damaged to almost completely destroyed storage media devices (and its media) to recover almost the entire section of data in question. So it comes as no surprise that data recovery specialty investigative services will become an even more increasingly popular service for physical tampering or attempted destruction of corporate or government data.



## Phases of IT Forensics Management

---

There are (essentially) three (3) phases for recovering evidence from a computer system or storage medium. Those phases are: (1) ACQUIRE, (2) ANALYZE, and (3) REPORT. Although I have read that the phases may be performed independently of each other, and not in any particular order, observation has concluded contrary to those beliefs in that the correct order and methodology must be used, and in the proper sequence, or the resulting court case may be thrown out for lack of proper evidence or credentials.

In the ACQUIRE phase, this involves the seeking and transferring of data from either the storage medium (floppy disk drives, hard disk drives, USB drives, et. al) to the actual computer system itself. IT forensics specialists must ensure that the original storage medium is not overwritten to by either the investigating computer system, or the tampered computer system. Additionally, investigators must confirm and verify that the data transferred from the storage medium or computer system matches to that of the data stored on a separate system.

In the ANALYZE phase, the IT forensics specialist analyzes the data content for specific information – such as files, electronic messages, electronic mail, cookies, digital signatures, encryption keys, et. al. Once the data is found, and if found encrypted, must be deciphered and documented (if relevant). One caveat about significantly larger hard disk drives of today is the amount of data that must be sifted through with a microscope. In order to quickly process the data, the IT forensics specialist must have a fairly comprehensive knowledge of the computer system architecture, or specifically the type of file, email, or data snippet that is being tracked down.

Once the data has been found, analyzed and categorized, the data must be recorded and reported to legal professionals. In the REPORT phase, a report detailing the findings from all data collect and analyzed, as well as any statements of possible reasons (or perhaps conclusions for probable reasons), and why the data is relevant to the case, is required. Some law enforcement agencies often require a summary report in addition to the actual report itself, since much of the report details so much information, that it may overwhelm legal professionals and investigative staff members.

A reason for necessitating digital evidence is that it is becoming increasingly required by law to have forensics capabilities. Various state and federal laws now may require companies to perform IT forensics investigations prior to pressing criminal charges. A prime example is the Sarbanes-Oxley Act of 2002, which was a product of many corporate scandals arising from the Post-DotCom bailout starting around Year 2000. This included companies such as Worldcom, Enron, Tyco, and more. Scandals such as these amounted in the millions, perhaps billions, of dollars, which cost both investors and governments money – money that may never be recovered. Thus, the government (some states, mostly federal) mandated that U.S. corporations have more structured, more auditing capabilities internally. This might include IT forensics management and investigative capabilities within each corporation.



## Reasons for an Internal Audit

---

Corporate business often have older computer architectures that are sometimes powered off, laying in a storage closet or warehouse someplace – often with a significant amount of corporate confidential information. As with anything else involving human nature, not all people think clearly or logically of ramifications of old computer equipment, and what impact this may have upon their corporate environment(s). In fact, when faced with overworked, and largely ignorant IT staff members of most corporations, many of these staff members simply throw out the old computer equipment, often recovered by data scroungers, computer hobbyists, or corporate espionage specialists, usually with the data intact. Old as it may be, some of this data may still be relevant, esp. if there are legal ramifications involving corporate executives.

This can lead to disastrous conclusions, esp. a corporation's scandal is leaked to news media. Since many corporations are concerned about their public image, any news press or media coverage that involved data or information recovered from old computer equipment, can have a devastating effect upon the public's perception of the corporation, and in the long-term timeframe, can have a financial impact upon it as well.

Another possible risk is the use of leased or rented computer systems, which are becoming more popular with the corporations today. Since computer technology changes so rapidly, many companies feel that leasing computer systems is cheaper than owning. Notwithstanding their decision for leasing versus owning computer systems, leasing/renting computer equipment can be just as risky as improper disposal of owning older computer equipment. Once a lease or rental agreement has expired, and the company has elected not to renew their contract, the computer equipment is returned to back to the leasing company. Similarly with improper disposal of equipment, many IT staff members fail to eradicate corporate data and information from the storage medium used. This too, poses a serious risk for the corporation that leases their computer equipment, and its impact can be almost as significant as the previous reason (owning equipment and information being released to the news media).

Though a corporation may feel that they may save money by leasing their computer equipment, ultimately, the cost of data destruction may remain virtually similar to that of computer equipment owned by a corporation. In both cases, the data must be exhumed from the storage medium and ensure that there is absolutely no trace of any information whatsoever.

So how does this apply to state and federal government agencies and associations?



## Further Issues with IT Forensics Management

---

With the increasing threat towards global terrorism and its use of computer and the Internet-connected capabilities, government agencies need to be able to perform IT forensics management reliably. One challenge faced is involving languages that are not based upon the Roman alphabet – languages such as Chinese, Korean, Japanese, Cyrillic (Russian and many other Slovak languages), Arabic, Indian, et. al. Many IT forensics investigators are faced with this challenge and fall flat on their faces as internationalized computer system configurations cause grief and confusion to English-only speaking professionals.

Ironically, many personal computer systems are donated to schools, churches, flea markets, etc., or to relatives or other charitable organizations. Even if individuals manage to successfully wipe clean all evidence or data, no matter how many times, from their hard disk drives, floppy disks, or USB drives, valuable personal information, such as financial statements, bank account numbers, bank transferring statements, electronic messages, electronic mails, home-related, or even work-related documents – all may be easily retrieved.

Though none of this infers that an individual or organization is stupid or ignorant, merely that proper education needs to be provided to these entities. For the IT forensics specialist, this is treasure trove of information, providing a wealth of spending patterns, personal or corporate histories, contact information, and more. With so many people using computers today (approx. 10% of the world has a computer in their household; approx. 60% [or more] of the United States has a computer in their household), IT forensics management is quickly becoming a sought-after career paradigm. However, it is not without its faults.

## Tools of the Trade

---

What kinds of tools and equipment are needed for IT forensics management? For starters, a good digital camera (preferably one with a significantly high resolution of 3 or more megapixel resolution) is required for use at the scene of the investigation (both inside and outside of the computer system, as well as the area surrounding the computer system). Images of the front and rear of the computer system, what cables are connected, and their functions must be recorded, along with serial numbers, model numbers and any other relevant data that can be used to help identify the computer system.

Other tools required for IT forensics management includes a small to medium computer toolkit. This comprises of different sized screwdrivers, wrenches, canned air (believe it or not, you'd be surprised just how big "dust bunnies" [dirt particles that have clumped together] can get), and various cables [networking patch, networking cross-over, narrow SCSI, IDE, EIDE, floppy disk, keyboard, etc.). For the screwdrivers, all sizes from 0 to 3 are recommended, both flat bladed and "philips" ("+" ). Wrenches are not always necessary, but do come in handy esp. when working with larger computer systems that are enclosed within a rack cabinet enclosure; wrenches include both hex and torx wrenches from T-10 through T-50. For reading of non-SCSI devices, ABCUS, Inc. has a wonderful device called the FASTBLOC<sup>3</sup>. This device prevents the reading computer system from writing ANY data back onto the storage medium (in this case, the IDE or EIDE disk drive). This device tricks the reading computer system into thinking that the writes have been successful. The



device ensures that a bit by bit data transfer of the storage medium image has been taken without tampering with the computer system or storage medium evidence. The IT forensics specialist simply attaches the hard disk drive to the FASTBLOC<sup>3</sup> device, then attaching the FASTBLOC device to the reading computer system via USB or FireWire ports. Having USB and/or FireWire ports makes the device laptop-friendly, thus allowing IT forensics specialists to go to the site or location of the investigation.

To review any data or information extrapolated from the computer system or storage medium, IT forensics software is used to review for any possible clues of data, which was just transferred from the storage medium. There are both Open Source tools available as well as commercial versions. Of the Open Source solutions, Knoppix-STD, Penguin Sleuth Kit, and Local Area Security – all are good in offering a low-cost forensics management capability. For internal audits, using these tools are perfect in saving and conserving licensing costs of the forensics software tools. However, legal professionals are becoming more demanding that standardized software is used during all phases of the forensics process.

## **Conclusion**

---

With cyber crimes on the rise, IT forensics specialists will need be more aware of the tools necessary in keeping up with criminals. As IT forensics management grows, so will the awareness and capabilities of data recovery and analysis.



## Bibliography

---

1. ref: <http://www.wordiq.com/definition/Forensics>.
2. ref: <http://www.crimeinstitute.ac.za/2ndconf/papers/britz.pdf>.
3. ref: <http://www.guidancesoftware.com/products/accessories/FastBloc/fastblocl.shtm>.

