

# Maintaining The Digital Chain of Custody

By John Patzakis

*john.patzakis@guidancesoftware.com*

Employing proper computer forensic processes is the foundation of computer investigations. Even the best corporate policies for incident response and computer data preservation can mistakenly allow the mishandling of potentially key computer evidence. Once compromised, either during the collection or analysis process, the evidentiary integrity of the data is lost.

Computer investigators must follow four basic steps in order to correctly maintain a digital chain of custody. These include:

- Physically control the scene, or if conducting a remote network investigation, log all access and connectivity through an integrated and secure reporting function
- Create a binary, forensic duplication of original data in a non-invasive manner
- Create a digital fingerprint (hash) that continually verifies data authenticity
- Log all investigation details in a thorough report generated by an integrated computer forensics software application

## The Problem of Improper Computer Evidence Handling

Maintaining the integrity of computer evidence during an internal investigation or incident response is important, especially when computer evidence may be presented in court. This is true whether human resource personnel suspect that an employee's violation of company policies may warrant termination, if IT staff are responding to a network intrusion, or outside consultants suspect criminal activity that may need to be reported to authorities. However, the ability to maintain and precisely document digital contents, including its exact location on the subject media should stand as the cornerstone of any computer investigation. By not taking steps to preserve the digital chain of custody, a company is leading itself into an investigation that is compromised from the beginning.

Such a lax investigation also can make it difficult to later map out the exact location of electronic evidence on a drive, or to prove who manipulated or created data, as it is no longer clear if it was the suspect or the investigator who was the last to access it. In fact, this is the reason that worldwide agencies regulating financial institutions have mandated incident response plans.

Recent policies, standards, and court decisions strongly establish a compelling obligation for all types of businesses to preserve electronic data that may be relevant to a legal matter, audit, etc. On the U.S. legislative front, the Sarbanes-Oxley Act, which passed in response to the Enron/Arthur Anderson debacle, imposes severe penalties for the destruction of records, including electronic data. The act expressly prohibits the destroying records in "contemplation" of an investigation or proceeding. Securities Exchange Commission rules require retention for six years of all business-related email and Internet communications sent and received by brokers, dealers and exchange members. Additionally, the data must be preserved and maintained in a manner that verifies its authenticity.<sup>1</sup>

## The Process of Computer Forensics – Duplication of Original Data

Electronic evidence is fragile by nature and can easily be altered or erased without proper handling. Merely booting a subject computer to a Windows® environment

will alter critical date stamps, erase data contained in temporary files and create new files. Specialized computer forensic software employs boot processes or utilizes hardware write-blocking devices that ensure the data on the subject computer is not altered in any way. After initiating these measures, the examiner uses the forensic software to create a complete mirror image copy or “exact snapshot” of the target hard drive and all other external media, such as floppy or zip disks that are subject to the investigation. This evidentiary image must be a complete, but non-invasive sector-by-sector copy of all data contained on the target media in order to recover all active, “deleted” and otherwise unallocated data, including often critical file slack, clipboards, printer spooler information, swap files and data contained or even hidden in bad sectors or clusters. This process allows the examiner to “freeze time” by having a complete snapshot of the subject drive at the time of acquisition. This snapshot can also be stored and kept for reference or future use.

### **Verifying Data Authenticity**

Gathering computer evidence by employing proper forensic tools and techniques is the best means to establish the integrity of the recovered data. Computer forensic examiners rely on software that utilizes a standard algorithm to generate a “hash” value, which calculates a unique numerical value based upon the exact contents contained in the evidentiary “mirror image” copy. If one bit of data on the acquired evidentiary bit-stream image changes, even by adding a single space of text or changing the case of a single character, this value changes. The standard “hashing” process is the MD5, which is based on a publicly available algorithm developed by RSA Security. The MD5 (Message Digest number 5) value for a file is a 128-bit value similar to a checksum. The MD5 hash function allows the examiner to effectively and confidently stand by the integrity of the data in court.

Using digital signatures such as checksums and the MD5 hash concurrent to the acquisition of data, allows the examiner to effectively establish a digital chain of custody. This is because an integrated verification process, which is another important feature of computer forensic software, establishes that the examiner did not corrupt or tamper with the subject evidence at any time in the course of the investigation. This is a particularly important step, as courts will only accept duplicated computer data if the data is demonstrated to be an accurate copy of the “original” computer data. In one recent appellate decision, the court specifically upheld the admission of key computer evidence in court on finding that proper computer forensic software was employed.<sup>2</sup>

After the mirror image copy is created, authenticated and verified, computer forensic software will “mount” the mirror image as a read-only drive, thus allowing the examiner to conduct the examination on the mirror image of the target drive without ever altering the contents of the original. This process is essentially the only practical means to search and analyze computer files without altering date stamps or other information. Often times, a file date stamp is a critical piece of evidence in litigation matters.

An IT administrator should approach every computer investigation, systems audit or incident response with the assumption that the mirror images of the targeted computers will ultimately either be turned over to company lawyers or law enforcement for civil litigation or criminal prosecution purposes. The creation of a mirror image that is verified and authenticated pursuant to proper computer forensic protocol is essential to ensure a smooth transition from the response stage of the investigation to the enforcement or litigation process.

Maintaining a proper digital chain of custody also can turn out to be just as significant even months after the employee has left the organization. Routine image

back-ups are becoming more common, as they help protect individuals and companies from liability and claims of evidence spoliation (did you mean tampering? Spoliation is robbing or plundering). Because imaging is now non-invasive and non-disruptive to the work environment, many companies simply image drives whenever an employee is terminated or leaves voluntarily. This standard imaging also serves as a critical tool to fully investigate cases involving intellectual property theft – a claim that is often difficult to investigate once a terminated employee’s computer is recycled and put back into use. Often times an employer will not learn of possible trouble until long after an employee has left. Since employees engaged in illegal activities or internal misconduct typically delete files to cover their tracks, traditional back up techniques are of little help because they lack the ability to retrieve data and do not adhere to even basic forensic standards.

## **Report of investigation details and findings**

In any type of computer forensic investigation, it is the chain of custody that is used to not only verify but also illustrate the existence and use of data. Investigations and searches on a piece of computer media can find endless amounts of evidence, but it is the chain of custody that maps its placement within the media and its use in relation to criminal or unauthorized actions. For this reason, a report is critical to prove and maintain a chain of custody. Forensic software now can clearly depict where every file on a piece of media is located, while also listing its many properties, including creation date, date last accessed, and date deleted. In fact, without a thorough report, despite the use of proper forensics techniques, it is extremely difficult to illustrate the exact location of evidence. Frequently admitted as key evidence in trials, these hard copy reports are the print out of the electronic crime scene, indicating even at what specific second a file was deleted or manipulated in some way.

Despite the investigator’s level of in-depth forensic experience, following these four basic steps helps ensure that electronic evidence is not altered or manipulated in any way: Require physical control, data duplication, authenticity verification and reporting.

## **Conclusion**

There are six reasons to employ proper forensics protocols when collecting computer evidence:

- Enables simpler referral of computer crimes to law enforcement
- Allows corporations to defend their interests in civil litigation
- Eliminates evidence spoliation (destruction) claims
- Limits corporate liability
- Better controls corporate assets and infrastructure
- Helps comply with worldwide privacy, data, and information integrity standards and regulations

---

*John Patzakis is President of Guidance Software. Recognized as a leading authority on the admissibility and authentication of computer evidence, he is the author of the EnCase Legal Journal, a publication that focuses on legal issues relating to computer forensics and electronic evidence.*

---

<sup>1</sup> 17 C.F.R. § 240.17a-4(f)(1).

<sup>2</sup> *State v. Cook*, 777 N.E.2d 882, 2002 WL 31045293 (Ohio App. 2 Dist.)