Global Information Assurance Certification Paper

Computer Forensic Procedures for the Corporate Security Specialist

Stephen McFall
November 22, 2000

Introduction

One of the duties of the corporate security specialist is to discover and preserve evidence of computer crime. This evidence can exist in many forms and reside on many different types of computer storage media. In order to protect corporate interests and assist law enforcement agencies, the corporate security specialist should have a thorough understanding of what constitutes the "best" evidence both in the practical and legal sense. All security specialists and systems administrators should be trained in the procedures used to preserve and document computer evidence and how to properly duplicate this evidence to other types of computer media for further analysis. This paper, which is geared to the security specialist and systems administrator in the corporate environment, will provide a basic understanding of what is the "best" evidence and will discuss this evidence in the context of proving its reliability and being able to authenticate its origins. Practical steps and guidelines to preserve, duplicate and document computer evidence will also be discussed.

What is the "best" evidence?

Although law enforcement agencies think of computer evidence as information or data that can assist in apprehending and, later, convicting a person who has committed a crime, evidence can just as easily be important in a variety of other corporate matters. [1] Civil law matters such as sexual harassment issues and disputes among corporate employees over the origination of new product ideas may also be among the many valid reasons which require the corporate security specialist to preserve and protect computer evidence.

As all good scientists know, objectivity is important when conducting experiments. Likewise, it is highly important to be extremely objective when preserving evidence. The key to this objectivity is to assume nothing and to document the smallest of details concerning the origin and existence of the evidence. The importance of this process cannot be overstated since in today's world of computer networks, it is entirely possible to steal an individual's identity and utilize the account for criminal purposes making the suspicion fall on the account owner instead of the actual subject.[2] Federal law states that "[to] prove the content of a writing, recording, or photograph, the original writing, recording, or photograph is required, except as provided in the rules or by Act of Congress."[3] This part of the law is referred to as the "best" evidence rule since the

original is considered the "best" item of evidence. Other parts of these rules readily relate to computer data saying that "[a] duplicate is admissible to the same extent as an original unless (1) a genuine question is raised as to the authenticity of the original."[4] Further parts of these rules define a duplicate and in general state that whatever the copying technique, it must accurately reproduce the original to be considered a duplicate.[5] Therefore, a corporate security specialist must be concerned with proving that any duplicate made of servers or stand alone computers are accurate reproductions of the original and that human witnesses can testify under oath as to the origins of the evidence and how it was protected.

Authentication and Accuracy

Most computer forensic examiners agree that the analysis of a write-protected copy of computer evidence is preferable to examining the original evidence due to the transitory and obscure nature of computer operations. In other words, data can be easily and unintentionally altered thereby destroying the authenticity of the original evidence. The authenticity of an item can often be proven by what the courts recognize as a "process or system", which in the law enforcement arena is called a "chain of custody" or a hand-to-hand chain of accountability.[6] A crucial part of this system is really just a document that stays with the evidence and includes the name of each person that handles the evidence as well as the date and time the evidence is received by each person in the chain. The document should describe in detail the item of evidence and should include any pertinent serial numbers or other description that would uniquely identify the item. If multiple items such as floppy disks are listed on one chain of custody document, then these items should always be kept together even if passed to another individual. A good way of doing this is to seal the items in a manila folder and staple the chain of custody document to the outside of the folder. For larger items, a box may be used. For actual computer equipment, the document may be placed in a clear plastic sleeve and taped to the outside of the central processing unit or device containing the computer storage media (i.e., a RAID device). The chain of custody document should be initiated upon the receipt of the evidence, or in the case of a duplicate, the time that the duplicate is completed. A chain of custody document should be completed for each duplicate copy made if it is anticipated that these copies will be going to different individuals for long periods of time. An example of this would be a case where different individuals in the company will be performing analysis on the copies.

All items of evidence should be afforded physical security by limiting the access to the items to only the individual in the possession of the evidence. If a system administrator makes a backup copy of a server as evidence, then, after creating a chain of custody document, the item should be stored in a filing cabinet or room to which only the system administrator has a key. If the item is passed to another individual, then that person should place the item in a secure area maintained by only that person. This methodology will ensure that only the current individual on the chain of custody document has access to the evidence item.

The computer, hard drive, or other type of computer storage media gathered as evidence should have the initials of the first individual who took possession of the item and the date the item was obtained written in permanent ink somewhere on the item. This allows the first person in the chain of custody to identify the item with greater specificity.

While the above procedures help prove the authenticity and reliability of the evidence, what about proving that a duplicate of a particular type of computer storage media is the same as the original? [7]

The authenticity and reliability of a duplicate can be shown by proving that no data has been changed from the original media, that a complete copy of the data was made and that the program and process used to copy the data is reliable.[8] The use of commercially available copying software, some of which was specifically designed for law enforcement forensic computer examiners, is usually the best option since commercially available software tools have usually undergone some type of testing and have a documented history of upgrades and modifications. The corporate security specialist should have a clear and thorough understanding of the copying software tools that are being used. A thorough understanding would include a knowledge of all switches used by the program commands and all documentation provided by the software manufacturer should be read so that all limitations of the software are understood. To prove that the data contained in the duplicate is the same as that contained in the original, an MD5 hash or other similar algorithm can be run on both the original and the duplicate and the results documented.

Stand Alone Computers versus Servers

Computer forensic procedures for stand alone computers may vary for the corporate security specialist. While it may be acceptable to take a stand alone computer belonging to an employee out of service for an extended period of time, taking a server or even a stand alone computer crucial to business operations out of service for even a day may be unacceptable. For this reason and because computer storage media are particularly susceptible to apparent and unapparent change, it has become accepted practice to make copies of the original evidence and to analyze the copies instead of the original. These copies are usually what are referred to as mirror image copies or a bit by bit copy of the original evidence. A true mirror image copy will preserve not only the original file structure of the media being copied but will also preserve unallocated clusters, erased files and data remnants that exist on the original media.

In the case of large file servers, it may not be practical or necessary to make an image copy. In these cases, for example a server that was not attacked but contains log files showing computer intrusion activity, copying a complete set of logs to some type of media is acceptable as long as the other procedures outlined in this paper have been

followed. In the case of a computer that has been attacked, the computer should be taken offline and a mirror image copy should be made as soon as possible so that further intrusion activity does not destroy pertinent evidence. This copy can then be compared to the most recent backup of the computer taken before the intrusion activity to discover what alterations and changes have occurred.

Since both civil and criminal matters may take years to come to court, it is also a good idea to photograph the computer system, hard drive or other original evidence from which the copy was made as a way of refreshing an individual's memory of the original evidence if called upon to testify in court over a year later. In addition, the software tool, manufacturer and version number used to copy the original evidence should be documented for each item copied since this information will change over time.

Summary

The importance of understanding the concept of the "best" evidence, how to properly authenticate the original evidence, how to make and work from a copy of that evidence and document the handling of the original evidence and any copies cannot be emphasized enough. Following a sound set of procedures will help maintain the integrity of the evidence obtained and will help in protecting the corporate security specialist and his employer from any liability associated with the improper handling of computer evidence.

References

1. "Federal Guidelines for Searching and Seizing Computers", 1992. URL: http://www.usdoj.gov/criminal/cybercrime/searching.html

2. Icove, David, Seger, Karl, and VonStorch, William. "Computer Crime, A Crimefighter's Handbook". First Edition, August 1995. O'Reilly &Associates, Inc.

3. Federal Rules of Evidence, Section 1002

4. Federal Rules of Evidence, Section 1003

5. Federal Rules of Evidence, Section 1001(4)

6. "Federal Guidelines for Searching and Seizing Computers", 1992. URL: http://www.usdoj.gov/criminal/cybercrime/searching.html

7. "Uniform Electronic Evidence Act", published by the Uniform Law Conference of

Canada, URL: http://www.law.ualberta.ca/alri/ulc/current/eelev.htm

8. Feldman, Joan E. and Kohn, Rodger I. “Collecting Computer-Based Evidence”. New York Law Journal. 26 January 1998. URL: http://www.nylj.com/tech/012698t6.html