IGI PUBLISHING **ITJ 5042**

701 E. Chocolate Avenue, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.igi-global.com

This paper appears in the publication, International Journal of Digital Crime and Forensics, Volume 1, Issue 3
edited by **Chang-Tsun Li © 2009, IGI Global**

Evidentiary Implications of Potential Security Weaknesses in Forensic Software

Chris K. Ridder, Stanford University, USA

ABSTRACT

Computer forensic software is used by lawyers and law enforcement to collect and preserve data in a "forensic image" so that it can be analyzed without changing the original media, and to preserve the chain of custody of the evidence. To the extent there are vulnerabilities in this software, an attacker may be able to hide or alter the data available to a forensic analyst, causing courts to render judgments based on inaccurate or incomplete evidence. There are a number of legal doctrines designed to ensure that evidence presented to courts is authentic, accurate and reliable, but thus far courts have not applied them with the possibility of security weaknesses in forensic software in mind. This article examines how courts may react to such claims, and recommends strategies that attorneys and courts can use to ensure that electronic evidence presented in court is both admissible and fair to litigants. [Article copies are available for purchase from InfoSci-on-Demand.com]

Keywords: *Admissible; Authenticity; "Best Evidence"; Daubert; Evidence; Forensic; Hacking; Reliability; Security; Vulnerability*

INTRODUCTION

Forensic software is frequently used for evidence collection in both civil and criminal matters, because it mitigates risks that can arise with examining media in its native environment, such as alteration of metadata like time and date stamps, or overwriting of deleted files, which can impair attempts to recover lost data. Many forensic tools also provide features such as MD5 hashing and assignment of CRC values to data, to validate that the evidence to be introduced at trial remains in the same state as when it was collected. (Guidance Software, 2006). The legal and law enforcement communities depend heavily on forensic software to analyze and preserve critical evidence.

In addition to being a common practice among attorneys for prudential reasons, courts have suggested, and in some cases required, exact binary duplicates ("image copies") to be made of hard drives, particularly when deleted files are in issue. For example, in Gates Rubber Co. v. Bando Chem. Indus. Ltd. (1996), the court criticized the plaintiff for failing to make an "image backup" of the hard drive and for failing to properly preserve undeleted files, where there was evidence that certain files may have been deleted, and held that a party should "utilize the method which would yield the most complete and accurate results." The court in Simon Prop. Group L.P. v. mySimon, Inc. (2000) cited the Gates Rubber case favorably when it required the plaintiff to make what it called a "mirror image" copy of hard drives, citing the risks associated with overwriting of deleted files. In Playboy Enters., Inc. v. Welles (1999), the court ordered a court-appointed forensic computing expert to make a "mirror image" of the defendant's hard drive where there was evidence that emails had been deleted during litigation. Courts have also noted that forensic images can be a useful tool outside the context of deleted files. In Zubulake v. UBS Warburg LLC (2003) the court suggested that creation of mirror-image copies of computer systems is one way to preserve documents in the state they existed at the time of collection.

There are approximately 150 different automated tools used by law enforcement organizations in the investigation of computer crime, many of which are likely also used in the civil litigation context. (National Institute of Standards and Technology Computer Forensics Tool Testing Program, n.d.). The National Institute of Standards and Technology has a program to test that this software does what it claims, but some have argued that not enough work is being done to identify and correct security vulnerabilities. Newsham, Palmer & Stamos (2007) have argued that there is very little data on two popular forensic packages, EnCase and TSK, in the Common Vulnerabilities and Exposures database, and that vendors do not take advantage of the protections for native code that platforms provide (pp. 2, 11-12). Harris (2006) found that forensic software needs to be hardened against a wide range of potential attack vectors, and that "it would seem that perpetrators are working harder to subvert the system than academia is working to strengthen forensics." (pp. 44-49). The Grugq (n.d.) found that computer forensics are "[a]s vulnerable as other technologies," yet "[l]ess scrutinized than other technologies." (p. 12).

Forensic software marketing materials promise a high degree of accuracy and reliability. EnCase, one of the industry-standard tools, claims that it produces "an exact binary duplicate of the original drive or media." (Guidance Software, 2006). However, some researchers have noted that forensic software in certain situations may be vulnerable to deliberate attempts to hide data from the software, or to cause the software to crash. (Grugq, n.d.; Newsham et al., 2007).[1] To the extent code execution vulnerabilities are present or impersonation attacks are possible, an attacker may be able to change data on the forensic image, or to change the way such data appears to a forensic analyst. (Grugq, n.d.; Newsham et al., 2007).

The possibility that an attacker may seek to hide data from forensics software is a serious concern for those trying to collect evidence, but because hidden data by its nature is not likely to cause significant evidentiary concerns unless it is found, this article focuses on vulnerabilities that