Investigating Computer Forensics

Steve Brown
Capella University, USA

INTRODUCTION

Forensics is the application of sciences that help to seek out, examine, and answer questions about certain characteristics. For example, forensic toxicology helps us understand certain drug interactions, whereas forensics evidence helps us understand evidence that is uncovered at a crime scene. Since computers are now often used in criminal activity, a forensic branch of science has been created termed computer forensics. Unfortunately, unlike other forensics sciences, the complexity, legality, and even the nature of computer forensics may make it more vulnerable to errors.

Computer forensics is defined by Nelson, Phillips, Enfinger, and Steuart (2006) as a process that involves "obtaining and analyzing digital information for the use as evidence in civil, criminal, or administrative cases" (p. 2). It is also defined by Noblett, Pollitt, and Presley (2000) as "the science of acquiring, preserving, retrieving, and presenting data that been processed electronically and stored on computer media", but rather than simply examining a computer system, computer forensics investigations need to produce "direct information and data that may have significance in a case" (p. 1).

Computer forensics as now grown into a sub-field of learning within information technology (IT), and according to Berghel (2003):

> *"while not a profession, computer forensics satisfies the definition of a discipline. It is a well-defined field of study and practice. Like IT itself, it satisfies both the durability condition and the body of principles. It also has a codified body of practices that have evolved over the years through courtroom experience, and standards for competence, ethics and practice (p. 15)."*

These definitions of computer forensics imply that this science is more than uncovering data; it is the uncovering of data that will have some potential usefulness, such as the applicability in a court of law. The reverse is also true; the complexity introduces the very real danger of the opposite, that is, bad investigations, faulty record keeping, maintaining the integrity and custody of data, and that if an investigator is not careful, the data he or she collects will not be admissible in a court of law.

Computer forensics investigations also differ from other forensics sciences, like DNA forensics evidence testing where a conclusion is reached. Forensic science "makes no interpretive statement as to the accuracy, reliability, or discriminating power of the actual data or information" (Noblett et al., 2000, p. 1). Since computer forensics science investigations do not reach a conclusion, to withstand court challenges, the methodology used must be rigid, detailed, and logically conducted in steps that adhere to widely-accepted practices and procedures.

BACKGROUND

Born out of necessity, computer forensics was created to combat the increase in computer crimes. The discipline was modeled after basic law enforcement principles, and followed with well-defined processes and procedures (Berghel, 2003). It was created by the blending of two unique needs: first, the increasing dependence of law enforcement on computing; and second, the ubiquity of computer systems in our everyday life. Because of this ubiquitous nature, the general public still does not understand how a computer could be used for a crime, and often fails to understand even after a crime has occurred (Armstrong & Jayaratna, 2004).

Brungs and Jamieson (2005) report that computer crime continues to grow, and according to a financial fraud survey, 80% of respondent companies admitted to some type of financial fraud with losses averaging $1.4 million. Busing, Null, and Forcht (2005) reported that in 2004, 384 companies reported losses of $377 million due to computer crime. According to Icove, Seger, and VonStorch (1995), they report:

"Criminals are using computers to store records regarding drug deals, money laundering, embezzlement, mail fraud, telemarketing fraud, prostitution, pornography, gambling matters, extortion, and a myriad of other criminal activities (p. 1)."

Computer crimes are basically electronic crimes that are facilitated with the use of a computer, and the terms "computer crime, high-tech crime, digital crime, e-crime, and cyber crime" are considered interchangeable (Brungs & Jamieson, 2005, p. 59). Computer forensics is used to investigate these computer crimes, and a host of other possible criminal activities. Mercuri (2005) illustrates some of these examples as:

- Investigation of a law firm's accounting information by a state Office of Attorney Ethics to determine whether escrowed funds had been misused;
- Reconstruction of thousands of deleted text and image files in a murder case, in order to gather information about the activities of the victim and various suspects;
- Examination of source code used in the construction of an MPEG decoder chip set, to see if patents had been violated;
- Evaluation of the contents of a database to determine the cost of its production, as mitigating evidence in a large financial disagreement between business partners;
- Consideration of possible foul play by a former company employee, in the damage of computer records;
- Mathematical analysis of photographs to see if they have been digitally altered; and
- Preparation of explanations for an abnormally high missed vote rate exhibited by certain self-auditing electronic election equipment (p. 18).

Just this small set of different criminal activities where computer forensics investigations can be used to examine questionable activity, show the potential reach of the discipline—and its complexity. Even while forensics investigation has been used to identify criminal activity for the last 30 years, electronic evidence continues to be challenged on authentication and admissibility grounds (Giordano, 2004).

Legality of Computer Forensics

There are differences in the way forensics investigations are conducted between the private enterprise and law enforcement agencies. Private organizations usually have their own internal staff of legal and security experts that have to deal with a myriad of issues such as embezzlement, stealing trade secrets, and also human resource issues, like sexual harassment. Corporations will also have to tackle the problem of preservation of data. Unfortunately, most organizations are ill-equipped to deal with forensics investigations, and must work quickly to collect and preserve data in a sound and secure manner so that the evidence is complete and the authenticity can be accurately determined for future use (Casey, 2006). Corporations normally do not want to prosecute an individual, just stop the actions from occurring (Brungs & Jamieson, 2005). This may have to do with the potential of bad publicity if the situation becomes known in the media.

The use of computer forensics evidence in a court of law had not normally been accepted, and has not achieved the level of status as other forensics investigations, for example, fingerprinting and DNA evidence. One reason is that this field is still somewhat new and courts are hesitant to apply existing laws to a new area. Giordano (2004) has noted that in order for computer forensics to be accepted like other forensics's fields, computer evidence has to be built around core legal requirements of evidence handling, which include:

- **Admissible:** It must conform to certain rules before it can be put before a jury.
- **Authentic:** It must be possible to positively tie evidentiary material to the incident.
- **Complete:** It must tell the whole story and not just a particular perspective.
- **Reliable:** There must be nothing about how the evidence was collected and subsequently handled which causes doubt about is authenticity and veracity.
- **Believable:** It must be readily believable and understandable to members of a jury (p. 162).

In order to reduce inaccuracies when presenting evidence, the Federal Rules of Evidence requires the application of the best evidence rule. This is usually