Introduction to Computer Forensics in the Age of Information Warfare

Terry T. Kidd
University of Texas School of Public Health, USA

Police and prosecutors are fashioning a new weapon in their arsenal against criminals: digital evidence. The sigh of hard drives, Internet files and emails as court room evidence is increasingly common.

Michael Coren, CNN Correspondent

INTRODUCTION

The rapid expansion and dramatic advances in information technology in recent years have without question generated tremendous benefits to business and organizations. At the same time, this expansion has created significant, unprecedented risks to organization operations. Computer security has, in turn, become much more important as organizations utilize information systems and security measures to avoid data tampering, fraud, disruptions in critical operations, and inappropriate disclosure of sensitive information. Such use of computer security is essential in minimizing the risk of malicious attacks from individuals and groups. To be effective in ensuring accountability, management and information technology security personnel must be able to evaluate information systems security and offer recommendations for reducing security risks to an acceptable level. To do so, they must possess the appropriate resources, skills, and knowledge.

With the growing perverseness of information systems and the technologies used to support such tools, the growing need to keep the integrity of both the data and the system used to manage that data, will become a major priority. Therefore, it is important for security personnel and management to keep abreast of the issues and trends in information systems, security and the tools and techniques used to secure systems and data.

In order to determine if information safe and systems secured from outside attacks from computer criminals, information systems security assessments must be conducted on a regular and on going basis to insure system security integrity. If there is suspicion of wrongdoing or of misuse of the computer or system, one may employ techniques of procedures of computer forensics. The aim of this chapter is to introduce to the information technology community, a conceptual overview of information computer forensics and investigations and to discuss some of its problems and concerns.

BACKGROUND

Current literature of computer forensics (Nelson, Phillips, Enfinger, & Steurt, 2004; Noblett, Pollitt & Presely, 2000; Weise & Powell, 2005; Whitman & Mattord, 2003) state that the roots of computer forensics start with the first time a system administrator had to figure out how and what a hacker had done to gain unauthorized access to explore the system. This was mainly a matter of discovering the incursion, stopping the incursion if it was still in progress, hunting down the hacker to chastise the attacker, and fixing the problem allowing the unauthorized access to begin with. In the beginning, the classic hackers breaking into computer systems were more interested in how things work than actually being malicious. So, collecting evidence for a hearing was not a process a system administrator needed to worry about. Just plug the hole, and often get back to personal hacking projects.

As computers evolved out of academia to businesses and government, there was more data and resources at risk. Hacker incursions became an issue handled through legal channels (Ferbrache & Sturt, 1997). Also, as computer technology advanced, it became more affordable. This allowed computers to be put not only on each employee's desk of even small business, but in people's homes. More people looking for uses for the computers lead to the increase in supply of programs. More programs made more types of information collected as possible evidence. Evidence derived from computers has been used in court for almost 30 years. This is consistent with the research conducted by Ra-

num (1997). Initially, judges accepted the evidence as no different from forms of evidence they were already seeing. As computer technology advanced, the accepted similarities to traditional evidential material became ambiguous. In 1976, the U.S. Federal Rules of Evidence was passed to address some of the ambiguities.

A great deal has evolved with computers since 1976. One item of significance is the Internet. This information superhighway has become a major passage of items that fall under legal scrutiny (Nelson et al., 2004). Another item is the amount of data an individual computer can hold. Personal computers of the early 1980's had no internal storage and the removable storage only held 360-kilobytes per diskette. Today, an average personal computer bought for teenager game playing and Internet cruising holds internally 40 billion bytes of data and removable disks hold from 2 million bytes to 2 billion bytes. Large server computers used by academia, government, and business are starting with internal storage averaging 100 billion bytes and have the expandability to use storage devices holding trillions of bytes of data.

This explosion of technology, while providing many times the computing power of the building size computers of the beginning, have made the field of computer forensics exponentially more complicated from the relativity simple tasks of evidence gathering only five years ago.

EXPLORING BRIEF HISTORY OF COMPUTER FORENSICS

Thirty years ago, most people did not image that computers would be an integral part of everyday life. Now computer technical is a common place and a hot bed for criminal activity.

In the 1970s electronic or computer evidence did not hold up in court due to the fact that the fields of computing and computer forensics were new. Yet, computer crimes were being committed by those involved in white collared crimes. According to Nelson (2004), most computers in this era were mainframes, and they were sued by an exclusive realm of highly education and specialized professionals. Professionals who used such computer systems worked in banks, business, and in other markets where the free exchange of many and information was readily available. White-collar fraud began when people in those industries saw a way to make money by manipulating computer data.

One of the most well-known and documented crimes of the mainframe era was the one cent crime. It was common for banks to rack monies in account to the third decimal place or more. Banks used and still use the rounding up method when paying interest. If the interest applied to an account resulted in a fraction of a cent, that fraction would be used in the calculation for the next account until the total resulted in a whole cent. It was assumed that sooner or later every customer would benefit. This method was corrupted on more than one occasion by computer programmers who would open an account for themselves and write program so all the fractional monies went into their accounts. In smaller banks, this could amount to one a few hundred dollars a month. In larger banks with branch offices, the amount reached hundreds of thousands of dollars.

In the 1970s and early 1980s, when computer crimes such as the one half cent crime were being committed, most law enforcement officers did not know enough about computers to ask the right questions or how to preserve electronic or digital evidence for a trial. Many attended the Federal Law Enforcement Training Center programs that were designed to train law enforcement in recovering digital data (Department of Justice, 2002).

As personal computers gained popularity and replaced mainframes as the source of computing, different operating systems emerged. Apple released the Apple 2E in 1982 and then launched the Macintosh in 1984. The disk operating system (DOS) was available in many varieties, including PC DOS, QDOS, DR-DOS, IBM-DOS, and MS-DOS. Forensic tools at the time were simple and most were generated by government agencies such as the Royal Canadian Mounted Police in Ottawa and the Internal Revenue Service. At this time most of the tools were written in C and assembly language and were not available to the general public.

By the mid 1980s, tools such as X Tree Gold appeared. It recognized files types and retrieved lost or deleted files. Norton Disk Edit soon followed and became one of the leading tools in file recovery.

By the early 1990s specialized tools for computer forensic appeared. The International Association of Computer Investigative Specialist (IACIS) introduced training on the software available for forensic investiga-