IDEA GROUP PUBLISHING **ITB12242**

701 E. Chocolate Avenue, Suite 200, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com

This paper appears in the publication, Enterprise Information Systems Assurance and Systems Security
edited by Merril Warkentin © 2006, Idea Group Inc.

Chapter XX

Digital Forensics

David A. Dampier, Mississippi State University, USA

A. Chris Bogen, United States Army Corps of Engineers,
Engineering Research & Development Center, USA

Abstract

This chapter introduces the field of digital forensics. It is intended as an overview to permit the reader to understand the concepts and to be able to procure the appropriate assistance should the need for digital forensics expertise arise. Digital forensics is the application of scientific techniques of discovery and exploitation to the problem of finding, verifying, preserving, and exploiting digital evidence for use in a court of law. It involves the use of hardware and software for finding evidence of criminal activity on digital media, either in a computer or in a network device, and attributing that evidence to a suspect for the purposes of conviction. Digital forensics can also be used for non-law enforcement purposes. Data recovery is a form of computer forensics used outside of the legal arena. The authors hope that the reader will understand some of the intricacies of digital forensics and be able to intelligently respond to incidents requiring a digital forensic response.

Introduction

While violent crimes such as armed robbery and murder are decreasing in the US, computer crime[1] is becoming more prevalent worldwide (Anderson, 2000; Householder, Houle, & Dougherty, 2002; Noblett, Pollit, & Presley, 2000; Wolfe, 2003). The growth of the Internet has contributed to an increase in cyber crimes such as child pornography, gambling, money laundering, financial scams, extortion, and sabotage (Bequai, 2002; Kessler & Schirling, 2002; Wolfe, 2003). From teenage network hackers (Gibson, 2002) and corporate executives to child pornographers and terrorists (Gordon, 2002; Quayle & Taylor, 2002), the computer has attracted a potpourri of potential offenders with various skills, motives, experiences, and nationalities.

In addition to using a computer in the commission of a crime, computer criminals share another similarity: the chances of their being caught, prosecuted, reported, and/or detected are relatively small (Householder, Houle, & Dougherty, 2002). In one example, a sheriff's department investigator working exclusively on computer crimes full-time for five years made only five arrests, none of which led to convictions (Thompson, 1999). Though the FBI has attempted to encourage businesses to report computer crimes against their infrastructures, law enforcement often seems to respond apathetically towards relatively small business victims (Gibson, 2002; Schultz, 2002). This may be due to a heavy backlog of computer forensics cases and the need to prioritize efforts to catch the higher profile criminals. Large businesses, on the other hand, are more likely to become victims of computer crime but may be reluctant to report computer crimes for fear that it would result in a lack of confidence among customers or stockholders. Many businesses are more interested in getting their systems running again than in determining who the culprit is or perhaps prosecuting the root cause of the problem (May, 2002).

While computer crime continues to increase, computer forensics analysts and technicians remain scarce (Kessler & Schirling, 2002). A shortage of qualified digital forensics personnel is an obvious cause of backlogs in handling digital forensics cases. However, there are also secondary contributing factors that are important to consider: the constant growth of digital storage media capacity (Alameda County, 2000; Anderson, 2000; Shannon, 2004), and the lack of standard technical methodologies for digital forensics (Carney & Rogers, 2004; Palmer, 2001). When searching for evidence on a 100 GB (or bigger) hard drive, it is going to take a large amount of time to do the analysis. It is no longer sufficient to rely upon ad hoc, best-guess keyword search techniques for finding evidence (Anderson, 2000). More intelligent and efficient ways to structure searches are needed to reduce the time necessary to conduct analyses.

The inexperience of local law enforcement agencies (with respect to digital forensics), lack of standard digital forensics methodologies, constantly increasing digital storage capacity, and the "hidden"[2] nature of computer crimes all contribute to what may be referred to as an emerging e-crime crisis.

Digital forensic science is an emerging scientific discipline defined by the First Annual Digital Forensics Research Workshop as (Palmer, 2001):

> *The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation,*