IDEA GROUP PUBLISHING **ITB13036**

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, *Digital Crim and Forensic Science in Cyberspace*
edited by Panagiotis Kanellis, Evangelos Kiountouzis, Nicholas Kolokotronis, and Drakoulis Martakos

Chapter III

Computer and Network Forensics

Sriranjani Sitaraman, University of Texas, USA

Subbarayan Venkatesan, University of Texas, USA

Abstract

This chapter introduces computer and network forensics. The world of forensics is well understood in the non-digital world, whereas this is a nascent field in the digital cyberworld. Digital evidence is being increasingly used in the legal system such as e-mails, disk drives containing damaging evidence, and so on. Computer forensics deals with preserving and collecting digital evidence on a single machine while network forensics deals with the same operations in a connected digital world. Several related issues and available tools are discussed in this chapter.

Introduction

The widespread use of personal computers by domestic users and corporations in the past few years has resulted in an enormous amount of information being stored electronically. An increasing number of criminals use pagers, cellular phones, laptop computers and network servers in the course of committing their crimes (US DOJ, 2001). Computers are used in electronic crime in different ways. In some cases, computers provide the means of committing crime. For example, the Internet can be used to launch hacker attacks against a vulnerable computer network, or to transmit inappropriate

images. In other cases, computers merely serve as convenient storage devices for evidence of crime. Such persistent electronic material may, in certain cases, constitute critical evidence of criminal activity.

Prosecutors and law enforcement agents need to know how to obtain electronic evidence stored in computers. Digital evidence may be found in magnetic storage media such as hard disks, floppy disks, flash drives, random access memory (RAM), and so forth. Electronic records such as computer network logs, e-mails, word processing files, and picture files increasingly provide the government with important (and sometimes essential) evidence in criminal cases. Even free space on the disk may contain important evidence. Manual review of such data is impossible. Proper collection and automated analysis procedures are essential to preserve computer data and present it as evidence in a court of law. *Computer forensics* deals with the "preservation, identification, extraction, documentation, and interpretation of computer media for evidentiary and/or root cause analysis" (Kruse, 2001).

The need for well-defined procedures for acquiring and analyzing evidence without damaging it and providing a chain-of-custody that will hold up in court was discussed in the First Digital Forensics Research Workshop (Palmer, 2001). A framework for digital forensic science was proposed. The framework outlined a linear process of investigation involving the following steps: identification, preservation, collection, examination, analysis, presentation, and decision. Based on this investigation framework, structured approaches such as End-to-End Digital Investigation (EEDI), and others, have been developed to facilitate complex investigations (Stevenson, 2003).

Network forensics involves determining how unauthorized access to a distant computer was achieved. Network forensics yields information about computer intrusions. Log files in the computer (the victim of the intrusion), routers, and internet service providers (ISPs) are used to track the offender.

A number of sophisticated tools have been developed for forensic analysis of computers and networks. Mohay, Anderson, Collie, McKemmish, et al. (2003) identify three main categories of forensic functionality: imaging, analysis, and visualization. Imaging is the first step where a copy of the evidence is made for subsequent analysis in order to prevent tampering of the original. Some tools widely used for imaging purposes are Norton Ghost, Safeback, Encase, Linux *dd*, and so on. A complete forensic analysis of the image is required to find information related to a specific case. Digital information is not always readily available. Some files may be deleted, corrupted, or otherwise hidden. Forensic analysis allows the recovery of deleted, hidden, password-protected, and encrypted files. Sleuthkit and WinInterrogate are some commonly used analysis tools. Visualization involves timelining of computer activity using information found in the various log files, and so forth.

Network forensics can be accomplished using tools such as Snort, TcpDump, and BlackIce. Intrusion detection systems use system logs and audit trails in the computer and/or information collected at routers/switches. A number of approaches have been proposed to detect intrusions and trace the origin (Sekar, Xie, Maltz, Reiter, & Zhang, 2004; Thurimella, Burt, Sitaraman, & Venkatesan, 2005).

Most computer forensics vendors offer a variety of tools and some of them offer complete suites. The Computer Forensic Investigative Toolkit (CFIT) developed by Defence