Chapter XV

Digital Evidence and Computer Crime

Introduction

Throughout Section II of the book, we presented a variety of security mechanisms, technologies, tools, and best practices being used in order to harden up and secure computer networks and the information communication infrastructure. In this chapter and the next, we are shifting from discussing moral and ethical education in order to form an ethical framework in decision making and from implementation of security technologies, tools, and best practices to focus on the legal and law enforcement approaches. We believe, despite the fact that the technology has outpaced the legal system and the technology criminals use is sometimes years ahead of that of law enforcement, the legal system can play a very positive and effective role in the security of networks and the communication infrastructure.
Definitions

Evidence can be in either oral or documentary form and must follow the rules of evidence that govern the method of evidence collection, presentation, and admissibility in a court hearing or deposition. Digital evidence is evidence stored or transmitted in a digital form. Like any other evidence, digital evidence must be collected, processed, analyzed, stored, and then presented in a court of law. In many cases digital evidence is no more than any other criminal case’s evidence; however, special case must be given to digital evidence, because the smallest evidence change (a bit) may provoke the largest error in its interpretation. According to Bruschi and Monga (2005), this is because digital evidence can:

- Be easily and voluntarily erased
- Be easily and voluntarily forged (i.e., False evidence might be created)
- Be altered accidentally by daily activities (i.e., The everyday use of a system might damage evidence)
- Have different abstraction layers with different meanings and properties (e.g., An html document may be considered formatted text, a sequence of ASCII characters, or a set of blocks in the file system structure)

Nature of Digital Evidence

Those of you who followed the Enron case perhaps remember the effort that was put into the destruction of evidence. There were shredding parties to destroy the evidence. While efforts like these are sometimes fruitful in the brick-and-mortar world, in the digital world, it is not so clear. There are both positive and negative aspects of digital evidence so much so that there does not seem to be any gains or losses in dealing with digital evidence. This is the case because of the following aspects of digital evidence (Lundblad, 2005).
18 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the product’s webpage:
www.igi-global.com/chapter/digital-evidence-computer-crime/28509?camid=4v1

www.igi-global.com/e-resources/library-recommendation/?id=1

Related Content

Safe Distances: Online and RL Hyper-Personal Relationships as Potential Attack Surfaces
www.igi-global.com/chapter/safe-distances/206779?camid=4v1a

Information Systems Security: Cases of Network Administrator Threats
www.igi-global.com/article/information-systems-security/2464?camid=4v1a

Data Privacy and Security: HIPAA and Small Business Compliance
www.igi-global.com/article/data-privacy-security/34057?camid=4v1a

Hiding Message in Map Along Pre-Hamiltonian Path
www.igi-global.com/article/hiding-message-map-along-pre/50495?camid=4v1a