BOOK REVIEWS

Gary C. Kessler
Editor
Champlain College
Burlington, VT 05401
gary.kessler@champlain.edu

INTRODUCTION

This issue presents the fourth Book Review column for the JDFSL. It is an experiment to broaden the services that the journal provides to readers, so we are anxious to get your reaction. Is the column useful and interesting? Should we include more than one review per issue? Should we also review products? Do you have suggested books/products for review and/or do you want to write a review? All of this type of feedback -- and more -- is appreciated. Please feel free to send comments to Gary Kessler (gary.kessler@champlain.edu) or Glenn Dardick (gdardick@dardick.net).

BOOK REVIEW

Linda Volonino, Reynaldo Anzaldua, and Jana Godwin (2007). *Computer Forensics: Principles and Practices*. Pearson/Prentice Hall. 534 pages, ISBN: 0-13-154727-5 (paper), US$85.33

Reviewed by Jigang Liu (Jigang.Liu@metrostate.edu), Department of Information and Computer Sciences, College of Arts and Sciences, Metropolitan State University, St. Paul, MN 55106

“Computer Forensics: Principles and Practices” by Linda Volonino, Reynaldo Anzaldua, and Jana Godwin, published by Pearson/Prentice Hall in 2007 is one of the newest computer forensics textbooks on the market. The goal of the book, as the authors put it, is to teach “students who want to learn about electronic evidence – including what types exist and where it may be found – and the computer forensics methods to investigate it” so that they will be prepared “in a career in information security, criminal justice, accounting, law enforcement, and federal investigations – as well as computer forensics.”

Linda, Reynaldo, and Jana are not only experienced college professors, but also industry bounded professionals. All of them have substantial working experience with law firms or law enforcement in dealing with both civil and criminal cases. They are all certified information system security professionals (CISSP). Their teaching experience at the college level and their working experience on real cases make this book a must-read book for a college professor.

The book has thirteen chapters and is subdivided into five parts. The first part is “admissibility of electronic evidence.” This part introduces the basic concept of computer forensics and what is related to it. The questions the authors try to answer in this part are “what is computer forensics,” “why is it needed,” and “how is it conducted?”

The second part covers the topics in electronic data and evidence collection, which answers the questions “what tools are available and should be used in electronic evidence collection,” “what are the procedures and policies in evidence collection,” and “how to perform an electronic evidence collection on a desk top or laptop, PDA, or cell phone?”

After a general discussion of computer forensics and its procedures and policies, the authors, in part three, discuss the fundamental concepts and implementation in computer and data communications, such as operating systems, file systems, digital devices, and email and web-mail systems. In part four, computer forensics related fields, such as network forensics, intrusion detection, virus, DoS, Cyber terrorism, and cyberspace warfare, are discussed. In addition, identity theft, fraud and forensic accounting are also presented.

The last part is dedicated to topics in federal rules, criminal codes, and ethical and professional responsibility in testimony. Examples include amendments to the Federal Rules of civil Procedure on E-Discovery, the USA Patriot Act, and the trial process and expert testimony, respectively.

Four appendixes provide readers rich resources in “Online Resources,” “Government and Legal References,” “Sample Legal Forms, Letters, and Motions,” and “Summaries of Court Cases.”

This book is very informative and easy to read. Although the book is neither about Guidance Software’s EnCase nor about AccessData’s FTK, it provides the fundamentals of computer forensics along with a discussion of the usages of the well-known tools, which include EnCase and FTK. Not only is it an excellent overview of the field, the resources provided in the book also gives support to readers for their further research and study.

As a college professor, I was very impressed by the authors’ well-constructed exercises. “Multiple questions” look simple and time-saving but one must read the related chapters before they can accurately select the correct answer. It is an excellent way to encourage reading of the chapter as well as promoting interest; “Homework questions” are constructed in a way in which students need to use the knowledge they learn from the reading to analyze or discuss some issues or problems, or to devise and perform some hands-on exercises; “Projects” are used to help students study a large topic with more emphasis on searching, reading, analyzing, and writing; “Case studies” show students how the principles and rules introduced in the book were applied in real cases. In addition, they provide students with the opportunities to learn how to relate what they learned to reality in the field. This multi-level exercise provides instructors more flexibility in organizing their courses.

Overall, this book is an excellent textbook for an MIS or IS course. With a well thought out set of supplemental materials, this book also suits to the need of a CS, CIS, or IT course. To better understand the content of the book, students are recommended to have had at least two semesters of computer science related courses or an equivalent knowledge of operating systems and computer organization.

There are a few suggestions that I would like to recommend to the authors. One such recommendation includes archiving all the links (with their respective pages) referenced in the book on the book's website. The authors could also supply more details in the case studies, such as having at least two to three court scripts of real cases available on the book's website. In addition, it may be helpful to have a CD enclosed with the book so that most of the chapters' and appendices' materials can be accessed locally. Finally, future editions of this book can be made more attractive to CS students by equipping it with both in-depth discussions on some of the technical issues and hands-on laboratory assignments.