BOOK REVIEWS

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

INTRODUCTION

This issue presents the fifth 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 S. Dardick (gdardick@dardick.net).

BOOK REVIEW

Cohen, F. (2008). *Challenges to Digital Forensic Evidence*. Livermore, CA: Fred Cohen & Associates. 129 pages, ISBN: 1-878109-41-3, US$39.

Reviewed by Gary C. Kessler (gary.kessler@champlain.edu)

This book is about evidence gleaned as the result of the digital forensics process and providing expert testimony about that evidence. I am always suspicious when someone self-proclaims themselves as an "expert" although all authors are doing just that, at least by inference. Readers who are familiar with the author, Fred Cohen, or his large body of published works will know that he neither proclaims his expertise quietly nor inaccurately. Indeed, Cohen is an ideal person to weigh in on the topic of suitability and malleability of information acquired from computers and about providing testimony about that information and the process with which it was found.

Cohen's relatively short, self-published monograph is a very personal text that clearly draws on his years of experience. Written in the first person and largely devoid of external references (except for the occasional legal citation), you can practically hear Cohen speaking to you as you read the book; while reading it, I felt like I was back in a classroom. The book has six chapters, each of which ends with a set of questions, most of which I found to be interesting, pertinent, and thought-provoking, further adding to the feeling of being back in a seminar course.

Chapter 1 is an introduction to the rest of the book. Cohen here sets the stage to who he is, why you should read the book, and why he wrote the book. The

personal nature of the writing becomes evident on page 1.

Chapter 2 is titled "Overview" and is the second longest chapter of the book. This chapter reviews the basics of digital evidence and starts to outline where the process of digital evidence collection can go wrong -- i.e., the faults that can occur in the process, ranging from identifying and collecting evidence to imaging and analysis. This chapter concludes with a too-brief (in my opinion) discussion of the scientific method and application of Daubert principles.

Chapter 3, "Mechanics of Writing Expert Rebuttals," starts with an outline of a digital forensics report. Cohen spends time here discussing why he prefers use of the first-person personal voice when writing a computer forensics reports rather than the common academic/scientific practice of using the third-person impersonal. It is a departure from some of the common wisdom but flows well into a chapter that discusses why we -- as experts -- need to disclose our errors, experiment to prove to ourselves even those things that we know to be true, and be very careful with version control of reports.

Chapter 4 -- the longest chapter, occupying just more than a third of the book -- is a presentation of case studies. This chapter is where Cohen's experience as both an engineer and expert witness really shows and the stories here provide some interesting insights that readers will generally not find in standard academic texts. One of the case studies worth mentioning was about the use of Message Digest 5 (MD5) hashing. Too many practitioners rely too heavily on hashes, so much so that they sometimes forget whet the role of the hash it. Cohen observes that an MD5 checksum does not prove that the forensics copy of media matches the original but does validate the work we performed based upon our knowledge, experience, and training. This may sound like it is splitting hairs, but there is a precision in our language and word choices, and we must be careful about how we express ourselves, particularly in the legal and scientific settings.

Chapter 5 is another too-short section of the book, this one describing testimony. Although I would like Cohen to have written more, what he does have provides excellent advice to the expert witness: be prepared, tell the truth and only what you know, don't say too much, learn to say "I don't know," and -- my personal favorite -- think before you talk.

The final chapter, "How to Avoid Being Challenged," is a mere three pages (including end-of-chapter questions). The message, simply, is that computer forensics examiners need to be thorough and professional. Digital evidence is what it is and most successful challenges occur when the expert has made procedural errors or assertions that cannot be supported by the evidence. If we do our jobs well, we are told, challenges should be a minor issue. While this is all undoubtedly true, it does seem a bit glib to so state and leave it there; I wish

that this chapter was longer.

In fact, I wish that the whole book was longer. Two chapters (2 and 4) occupy one -third of the book and I think that most of the remaining chapters could use deeper treatment. But this is largely because I liked the book and think that it adds a lot to the professional bookshelf and the classroom. It's not perfect, by any means, and Cohen does not pretend that this is the last word on any of these topics; few other books, however, pay this much attention to guiding computer forensics professionals though this aspect of their job.

I do have some minor quibbles with the book. First, as alluded to above, I wish that the book had more references, although I recognize the difficulty in a personal book such as this. Second, I found the organization of the chapters to be a little challenging because I could not clearly distinguish between headings and subheadings. And, finally, the book is ostensibly about forensics evidence. While I fully understand how we use that term in our profession, I recall what an attorney told me some years ago: "It ain't evidence until the Court says it's evidence."

But, no matter. Cohen's book is well-suited as both a text in a senior level undergraduate or graduate course in a digital forensics program or as a professional reference. Although it is certainly not the only text to read about these issues, Cohen is a well-qualified author and has written a book that is both an easy read yet quite meaty. Whether you follow or reject Cohen's advice, reading the book will stimulate discussion and positively affect how you do your job.