2010

Book Review: Digital Forensic Evidence Examination

Gary C. Kessler
Gary Kessler Associates, gck@garykessler.net

BOOK REVIEWS

Gary C. Kessler
Editor
Gary Kessler Associates
Burlington, VT 05401
gck@garykessler.net

BOOK REVIEW

Cohen, F. (2010). *Digital Forensic Evidence Examination* (2nd ed.). Livermore, CA: ASP Press. 452 pages, ISBN: 978-1-878109-45-3, US$79..

Reviewed by Gary C. Kessler, Gary Kessler Associates & Edith Cowan University (gck@garykessler.net)

On the day that I sat down to start to write this review, the following e-mail came across on one of my lists:

> Person A and Person B write back and forth and create an email thread. Person A then forwards the email to Person C, but changes some wording in the email exchange between A & B. What is the easiest way (and is it even possible) to find out when that earlier email message was altered before sent to Person C?

Before you try to answer these questions, read Fred Cohen's *Digital Forensic Evidence Examination*. His book won't actually tell you how to answer these questions but it will help you understand the difficulty in even trying to answer them with any level of certainty.

Cohen's book is not a professional reference text. Don't read this book if you need to know how to image a Mac computer or build a computer forensics lab. Rather, it is an academic text for students pursuing a doctorate in digital forensics (such as the program at the California Sciences Institute where Cohen is president and runs the Ph.D. program). In that regard, this is a book about science -- digital forensic science and information physics.

The book has 10 chapters, each ending with a set of questions meant for the classroom. The first short chapter is an introduction to, and overview of, the rest of the book. Concepts of finite state machines and a mathematical nomenclature for describing an examination of digital forensic evidence are among the concepts introduced here. As stated above, this is no ordinary digital forensics reference.

Cohen provides what he calls "the fundamental theorem of digital forensic evidence examination...: What is inconsistent is not true" (p. 13). As a book on theory, I think that the fundamental theorem is a powerful statement. As a

practitioner, we live with this every day as we try to match digital evidence to patterns of behavior. As a researcher, I know where I would focus my anti-forensics tools; namely, anything that disrupts consistency.

The second chapter is an overview of the digital forensics process. Cohen defines a roadmap for the text to discuss issues ranging from the legal context under which digital forensics examiners work to the digital forensics process to admissibility issues of digital forensic evidence. Evidence, tools, people, and challenges form the heart of the book's content.

The practicalities, implications, and context of digital forensics are the keys to the entire book. Cohen, for example, observes that if Party A offers a fact into evidence and Party B stipulates to that fact, it is legally immaterial if the digital forensic evidence contradicts the fact. As a practice, we have many constraints such as time, money, and personnel. The remainder of the chapter discusses the processes related to digital evidence that form the focus and basis of the rest of the book. Cohen names 13 steps in the computer forensics process and the book focuses on the four that pertain to the examination phase, namely, analysis, interpretation, attribution, and reconstruction. Cohen steps through topics from legal context and evidence to people and tools, nicely laying out the model he uses throughout the book.

Chapter 3 is titled "The physics of digital information." Here is where Cohen really defines what he means by this term. He observes that the laws of physics that govern matter and energy are strict enough that a certain set of stimuli will always cause a given response. The granularity of real world physics is different from that of digital sources. He is not talking here about the physical manifestation of digital evidence such as disk drives and fiber optic cables; here he refers to the abstraction of data itself. This chapter is where he articulates how the physics of cyberbits differ from the physics of real atoms, largely because the cyberworld is a set of finite, discrete elements.

Chapter 4 introduces a formal framework for digital forensics examinations. This chapter discusses previous models such as those offered by Carrier and Gladyshev, and presents a formal description of the modeling process. While I see a value is using mathematical definitions and symbols to add to the precision of a discussion, I also wonder if it adds an unnecessary level of complexity. For some readers, this formal language will clarify concepts and add to understanding; others will be turned off and miss the forest for the trees.

The next four chapters discuss the various phases of the examination step in the computer forensics process. Chapter 5 is titled "Analysis" and describes the criteria for digital forensic evidence and expert opinions. The overriding theme of this chapter is how analysis is aided by redundancies in digital systems that allow examiners to find consistencies with which they can base opinions. Indeed, it is these very redundancies that assist us in finding inconsistencies when an adversary changes something in the digital evidence in a different

manner than the operating system, file system, or application would have allowed.

Chapter 6, "Interpretation," addresses how we apply context to the traces of activity that we find on a computer. Cohen makes the point here -- as he had long held -- that digital forensic examiners should be careful not to assert too many absolutes to our interpretations because we are almost always not in possession of one or two facts that might change our understanding. Thus, "it appears to be" is usually a better phrase than "it is this way" and we need to always be on the lookout for an alternate explanation. We also need to understand the limitations of our tools, our knowledge, the evidence, and our logic.

Chapter 7 is titled "Attribution" and addresses how we attach cause to effect. This chapter discusses how correaltion of two events does not necessarily lead one to properly conclude a cause-effect relationship. This chapter's material will cause the reader to think twice when trying to determine what sequence, or possible set of sequences, of events within the finite state machine caused certain traces to be left behind.

Chapter 8, "Reconstruction," represents the Holy Grail of digital forensics. After all of the analysis and interpretation, we need to somehow show that what we purport to have occurred actually happened -- or, at least, could have happened. Here is where experiment comes into play in the computer forensics process; can we construct an experiment to support or refute our theory of what happened? Of course, if the experiment contradicts the theory, then we know that the theory is wrong; if the experiment supports the theory, however, we only know that we are right insofar as the current set of facts represents the truth.

Chapters 9 and 10 are shorter than the rest and wrap-up the themes of the book. Chapter 9 addresses the limitations of the tools that are used for examination. The theme here, again, is knowing what the tools are telling you, not inadvertantly inferring too much, and being able to replicate the results. Chapter 10 finishes the book by reasserting Cohen's view that digital forensics is a science based on information physics and his belief that digital forensics may eventually be understood that way by future students and practitioners.

I obviously like this book and think it a valuable contribution to the professional literature but I do have some nits to pick. For example, while all authors believe that what they write is correct, I do not think that the author's correctness should be the basis for student problems. In Question 1 of Chapter 3, for example, the student is given the task of offering an argument to support the correctness of several of the author's assertions. In a Ph.D. text, I would think that a higher level of critical thinking might be in order, perhaps requesting a critique of the author's ideas.

And the book contains technical points that I think could be vigorously argued. For example, Cohen takes the statement "An IP address is a unique numeric address" (p. 223) to task by observing that "an IP address is not numeric (it is a set of octets)" (p. 223) and that use of private addresses means that there are duplicate addresses on the Internet. I would counter that IP addresses certainly are numeric; software tends to treat IP version 4 addresses as 32-bit unsigned integers regardless of whether they are expressed by the user in decimal, dotted decimal, or hexadecimal, which is why a lot of browsers will properly interpret *http://3486257654/* and take a user to *http://207.204.17.246/*. As to uniqueness, I would observe that every routable device on the Internet does have, and has to have, a unique address. Indeed, while there are at least four other devices with an IP address of 192.168.1.100 within 100 m. of my computer (which also has that address), each of those devices advertises a different public address and it is the public address -- not the private address -- that is the basis for a search warrant. Of course, with wireless networks so prevalent, we often still get the wrong house.

But are these major flaws? Hardly. What is the point of an advanced academic text if not to get these debates about fact and interpretation going? Indeed, it is this very discussion that leads to deeper understanding. This all said, I do wish that the book had an index rather than a detailed table of contents.

Digital forensics is still a field of practice that has not yet reached the status -- or stature -- of *science*. For that reason, I would argue that any professional in the field would be well served by learning the message of this text. Cohen wrote this book and its predecessor, *Challenges to Digital Forensic Evidence* (reviewed by me in *JDPSL*, Vol. 3, Issue 1), in order to define a science. And trying to do so is a Good Idea since the American Academy of Forensic Sciences (AAFS) accepted digital forensics as a forensics science in 2008 and the National Academy of Sciences (NAS) wrote its scathing report on the state of forensics practice in the U.S. in 2009.