

BOOK REVIEW

Building a Digital Forensic Laboratory: Establishing and Managing a Successful Facility.

By A. Jones and C. Valli

2008, Burlington, MA: Elsevier. xxvii + 285 pp. ISBN 13: 978-1-85617-510-4. \$69.95.

Like so many things in our just-in-time world, this book was sent to me just as one of my colleagues was looking for a text for a course he was developing in computer forensics laboratory operations and management. The two lead authors—and contributing author P. Swinburne—bring decades of experience in military and law enforcement environments in Australia and the UK to these topics. The book provides valuable insights that are applicable to digital forensics lab managers in both the public and private sector.

Like many aspects of digital forensics, there are several public sector guidelines from around the world for building computer forensics labs. That said, the largest growth in digital forensics staffing and activity is in the private sector, as information security incident response teams, representatives for the defense in criminal investigations, and e-discovery specialists in civil litigation employ a larger number of computer forensics specialists.

This book is composed of 24 chapters divided into four sections covering a broad spectrum of topics. Section I is titled, “Creating a Digital Forensic Laboratory” and comprises the first 9 chapters of the book. These chapters cover a range of topics that set down the framework for determining why one is building such a capability in the first place; knowing *why* you need to build a lab will help immensely in *how* you design the facility, assemble the resources, and recruit the personnel.

The first chapter offers a broad overview of the history and processes of digital forensics, setting the stage at 50,000 ft (or, in deference to the authors, 15,240 m) of what computer forensics is all about. The second

chapter delves into the types of digital forensics investigations, including aspects of criminal and civil litigation, e-discovery, and data recovery. These two chapters are essential because they provide the baseline for everything else that follows.

The next two chapters offer a checklist of issues to consider when establishing a lab and scoping out the requirements. These chapters discuss topics from the role of the lab within the organization/agency, staffing, and quality assurance to managing evidence, purchasing equipment, and prioritizing the cases. These chapters provide the framework for the rest of the book.

The remaining chapters in this section drill deeper into some of the specific topics introduced earlier. Three chapters briefly describe the creation of a business plan for the lab, determining the location for the lab (including issues related to physical site security and environmental factors), and guidelines for selecting staff and defining roles within the lab.

One entire chapter is devoted to training and education of lab personnel. Though this chapter contains excellent information, it focuses more on the development of academic programs and training courses than it does on guidance about the role of continuing education, training, and certification of staff. The chapter is augmented somewhat by an appendix that lists the major industry certification organizations, but there is little discussion about the relative merits of such certifications.

The final chapter in this section addresses laws, regulations, and standards. Though interesting to all professionals audiences, the chapter has a decidedly U.K. slant; the reader from the United States might be disappointed that there is no analysis about how

accreditation from the American Society of Crime Lab Directors (ASCLD) might apply—positively or negatively—to a digital forensics lab facility and, certainly, other countries are similarly unrepresented. (ASCLD and similar accreditation could, in some ways, affect U.S. police departments more than other countries merely because we have thousands of law enforcement agencies at the local, state, and federal levels.)

Section II offers five chapters addressing “Digital Forensics and Crime Investigation Management.” This section is all about the first steps of the digital forensics process, namely, identification, preservation, and acquisition of evidence. The first chapter in this section offers some policy and procedure considerations for the response team in preparation to being called to a scene, such as ways in which to deal with stand-alone versus networked devices, desktop systems versus servers, mobile and wireless devices, etc. The next chapter discusses management issues related to the collection of evidence from a scene, including identification, documentation, and legal issues. This is followed by a chapter dealing with the management and storage of the physical evidence media and examination media, including steps to protect and preserve the integrity of the original (or best) evidence.

This is followed by a very important chapter on quality assurance, covering topics ranging from acquisition methods, lab processes, and evidence presentation to hardware, software, and documentation. The section closes with a chapter summarizing some major high-technology crime cases from around the world that provide case studies highlighting the issues described in this section.

Section III is titled, “Overview of the Digital Forensics Investigations Profession and Unit.” This part of the book comprises seven chapters and, as the name implies, addresses topics related to the management of the facility and people after a computer lab has been set up. The section starts with a chapter describing the role of the lab director in managing finances, personnel, cases, and the facility itself. This is followed by a chapter that discusses how to run the lab like a small business, including the development of strategic and tactical goals and the role of annual plans. The next three chapters address other side issues related to lab management; namely, obtaining, vetting, and classifying information; the use of metrics to measure lab activity; and the role that outsourcing might play with respect to lab personnel and specialized functions.

Section IV is titled, “Future Digital Forensics Investigation Challenges” and comprises the final three chapters of the book. The first two chapters discuss the future role of digital forensics in criminal investigations and the criminal justice system, respectively; it is noteworthy that future implications for civil litigation are not addressed because e-discovery and litigation support are presenting some of today’s thorniest legal questions.

The final chapter addresses challenges facing the digital forensics lab manager; this individual, like any good manager, needs to juggle many issues at once, have many personal talents for dealing with people, and needs to serve many masters. One challenge that was not clearly addressed—and, indeed, what makes writing anything about the “future” so difficult—is the ability to recognize, react, and respond to the changes in technology, law, and process that are sure to (continue to) affect our profession; changes that, in many cases, we cannot even begin to anticipate today. Not everyone wants to be a change agent or can be a change agent, but change is thrust upon all of us who practice digital forensics.

This book has several gaps in its topical coverage, some of which are mentioned above. Some others include: how does one build a secure network interface to a secure storage facility for images, evidence files, and reports? How would one implement secure network access to this storage network for multi-location and/or multi-agency access? What are some of the features and criteria—and examples—of case management tools?

Despite these omissions, I recommend this book for any professional digital forensics professional who aspires—or is assigned—to build a lab and/or manage a unit. It provides one of the only professional references on this topic and makes an excellent starting point. The multidisciplinary approach to the text, employing aspects of management theory and practice, will serve the reader well, particularly if he or she is new to this aspect of the field.

Disclaimer: The authors of this text are colleagues of the author of this review at Edith Cowan University in Perth, Western Australia. This book was submitted to the reviewer by a third party who was unaware of this relationship.

Reviewed by
Gary C. Kessler

Book Review