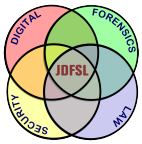

THE JOURNAL OF
DIGITAL FORENSICS, SECURITY AND LAW

Journal of Digital Forensics, Security and Law

Volume 8 | Number 2 Article 5

2013

Book Review: Placing the Suspect behind the Keyboard: Using Digital Forensics and Investigative Techniques to Identify Cybercrime Suspects

Thomas Nash
Internet Crime against Children Task Force

Follow this and additional works at: https://commons.erau.edu/jdfsl

 Part of the Computer Engineering Commons, Computer Law Commons, Electrical and Computer Engineering Commons, Forensic Science and Technology Commons, and the Information Security Commons

Recommended Citation
Nash, Thomas (2013) "Book Review: Placing the Suspect behind the Keyboard: Using Digital Forensics and Investigative Techniques to Identify Cybercrime Suspects," *Journal of Digital Forensics, Security and Law*: Vol. 8 : No. 2 , Article 5.
DOI: https://doi.org/10.15394/jdfsl.2013.1146
Available at: https://commons.erau.edu/jdfsl/vol8/iss2/5

This Article is brought to you for free and open access by the Journals at Scholarly Commons. It has been accepted for inclusion in Journal of Digital Forensics, Security and Law by an authorized administrator of Scholarly Commons. For more information, please contact commons@erau.edu, wolfe309@erau.edu.

EMBRY-RIDDLE Aeronautical University DAYTONA BEACH, FLORIDA | PURDUE UNIVERSITY

(c)ADFSL

BOOK REVIEWS

Diane Barrett
Book Review Editor
University of Advancing Technology
2625 W. Baseline Rd.
Tempe, AZ 85283

If you have any suggestions on books for review, or you would like to write a book review for us, or you have any comments and concerns on the book reviews published in this column, please feel free to send an email to Diane Barrett, the editor for this column, at dm_barrett@msn.com.

BOOK REVIEW

Shavers, B. (2013). *Placing the Suspect behind the Keyboard: Using Digital Forensics and Investigative Techniques to Identify Cybercrime Suspects*. Waltham, MA: Elsevier, 290 pages, ISBN-978-1-59749-985-9, US$51.56. Includes bibliographical references and index.

*Reviewed by **Detective Corporal Thomas Nash** (tnash@bpdvt.org), Burlington Vermont Police Department, Internet Crime against Children Task Force. Adjunct Instructor, Champlain College, Burlington VT.*

In this must read for any aspiring novice cybercrime investigator as well as the seasoned professional computer guru alike, Brett Shaver takes the reader into the ever changing and dynamic world of Cybercrime investigation. Shaver, an experienced criminal investigator, lays out the details and intricacies of a computer related crime investigation in a clear and concise manner in his new easy to read publication, *Placing the Suspect behind the Keyboard. Using Digital Forensics and Investigative techniques to Identify Cybercrime Suspects*. Shaver takes the reader from start to finish through each step of the investigative process in well organized and easy to follow sections, with real case file examples to reach the ultimate goal of any investigation: identifying the suspect and proving their guilt in the crime. Do not be fooled by the title. This excellent, easily accessible reference is beneficial to both criminal as well as civil investigations and should be in every investigator's library regardless of their respective criminal or civil investigative responsibilities.

As any good investigator would attest, a thorough investigation is beneficial to any case investigation. Online computer related cases provide unique challenges not usually associated with the "typical" case load. Shaver, a current adjunct professor of Digital Forensics, is a former law enforcement officer and computer forensic examiner that provides step by step instruction and guidance

from his vast real life experience to reach the ultimate goal of *Placing the Suspect behind the Keyboard*. Shaver has a unique perspective in this ever changing and evolving investigative discipline and his book would be of immeasurable importance in any investigation no matter the size or complexity.

In addition, the book's technical editor, Harlan Carvey, is a well-known and knowledgeable contributor to the digital forensics world. His unique experience and guidance add an unparalleled perspective to this timely and well-researched area of investigation.

In any civil or criminal investigation, the time spent, resources used, effort expended, evidence gathered, and testimony taken means absolutely nothing if you can't *Place the suspect behind the Keyboard*. Shaver provides the experience, guidance, resources, and expertise necessary to do so in his book.

The book is divided into 11 Chapters with a foreword by Troy Larson from Microsoft Network Security and a preface by the author himself. In addition to the eleven subject chapters, the book includes bibliographical references at the conclusion of each chapter and a well-organized, easy to reference index. There is a small overview segment at the beginning of each chapter which is further broken down into individual reference content providing a brief synopsis of each topic covered in the chapter. The first chapter contains the book introduction covering the concepts and standard procedures of computer forensics and use in criminal and civil investigations.

Each chapter contains specific and unique topics starting from Chapter 1, which explains the concepts of digital evidence collection to "live box" versus "dead box" acquisitions along with other preview/triage approaches. Chapter 2 deals with the victim, witness, and suspect interviews. While not a text on interrogation, the chapter does provide questions needed for interrogation that are related to computer-related investigation. Chapters 3 and 4 cover physical and technical investigations necessary to conduct a thorough investigation both in and out of the computer lab. Shaver's focus in Chapter 5 titled *Putting it all together*, aids the investigator in getting into the *investigator mindset* and weeding out irrelevant data to develop a suspect list.

Chapter 6 and 7's *Investigative Case Management* and *Case Presentation* titles speak for themselves. Shaver offers helpful management strategies and tools necessary to maintain large amounts of data and evidence present in digital investigations. He explains how to present relevant evidence and case information in a manner that the audience will understand while filtering out the superfluous.

Chapter 8 *Cheat Sheet and Quickstart Guides* demonstrates, the use of reference materials as constant reminders of staying the course in a case in placing the suspect behind keyboard by providing useful and time tested study

aids, reference guides, and checklists. In Chapter 9, Shavers explains the complexities and pitfalls of the ever changing and evolving technologies which can be both an advantage and hindrance in an investigation.

The vast online world is discussed in Chapter 10 *Online Investigations*. The chapter covers useful information that can be found online to identify a suspect, helpful search engines, and online investigative tools as well as procedures for capturing webpages as evidence. The book's last Chapter titled *Case Studies* provides case specific details along with suggested investigative actions and available resources to assist the investigator.

Shaver, utilizing his experience as a former law enforcement digital investigator and computer forensic examiner, provides a wealth of knowledge that includes links to online resources, applications, and software beneficial in any online or digital investigation. The applications and well-illustrated examples throughout the book are pertinent to the topic discussed. Each resource is clearly marked with an online linked address and information.

While Shaver himself notes that the book is not a text in forensic examination, he does cover the concepts of digital forensics in an easy to understand manner necessary for any investigation utilizing digital storage devices and other electronic equipment. Novice investigators should not shy away from the book. His explanation is clear about the uses and practicalities for the investigator. Conversely the book is also not Computer Forensics 101. This is a book for investigators with all levels of computer investigative experience.

What I like in particular about the book is that it is an enjoyable read from cover to cover. I found myself through the first 50 pages before I realized it, because it was easy to read and Shaver presented a clear writing style. Also of particular interest and effectiveness, is the book's easily referenced content. My copy has found a location on my desk for use as a quick reference as well as a complex problem solver.

In 2012, the IC3 received 289,874 consumer complaints with an adjusted dollar loss of $525,441,110, which is an 8.3 percent increase in reported losses since 2011 (Internet Crime Complaint Center (IC3), 2012). According to Go-gulf (2013), an international online Web application design and development company, cyber crimes are growing. By 2017, the global cyber security market is expected to skyrocket to $120.1 billion. In addition there are an estimated 556,000,000 online crime victims per year, 1,500,000 victims per day, 18 victims per second. Other alarming statistics include an estimated 600,000 Face book accounts are compromised everyday, 1 in 10 social network users said they have fallen victim to a scam or fake link on social network platforms, and 59% of ex-employees admitted to stealing company data when leaving previous jobs.

In light of these reports and estimates, Shaver's book could not come at a more opportune time. Undoubtedly digital and online crime investigators' work loads are only going to get larger requiring more complex and sophisticated investigative techniques and resources for each unique case. Shaver presents the concepts of digital forensics and digital investigative techniques so they are understandable by a wide audience and does so in a unique and expert manner.

I would highly recommend the book to anyone in the field of digital investigation, computer forensics, or who may just have an interest in the fascinating world of cybercrime investigation. This is a must read for any aspiring novice cybercrime investigator and the seasoned professional computer guru as well as a needed addition to any digital investigator's library.

References

Go-gulf (2013, May 17). Cyber Crime Statistics and Trends [Weblog post] Retrieved from http://www.go-gulf.com/blog/cyber-crime/ on May 17, 2013.

Internet Crime Complaint Center (IC3) 2012. Internet Crime Report. Retrieved from http://www.ic3.gov/media/annualreports.aspx.