THE JOURNAL OF
DIGITAL FORENSICS,
SECURITY AND LAW

Journal of Digital Forensics, Security and Law

Volume 9 | Number 3 Article 5

2014

# Book Review: The X-Ways Forensics Practitioner's Guide

Linda Lau
*Longwood University*

## Recommended Citation

Lau, Linda (2014) "Book Review: The X-Ways Forensics Practitioner's Guide," *Journal of Digital Forensics, Security and Law*: Vol. 9 : No. 3 , Article 5.
DOI: https://doi.org/10.15394/jdfsl.2014.1188
Available at: https://commons.erau.edu/jdfsl/vol9/iss3/5

# 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, would like to write a book review for us, or have any comments or 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 book.reviews@jdfsl.org.

### Book Review

Shavers, B., and Zimmerman, E. (2013*). The X-Ways Forensics Practitioner's Guide.* Waltham, MA: Syngress, 242 pages. ISBN: 978-0-12-411605-4. Print: US $50.90. Includes exercises, case studies, references, and index. Reviewed by Linda K. Lau, Longwood University

Brett Shavers is a former law enforcement officer, a digital forensics examiner, an adjunct instructor, and a frequent speaker at many conferences. After writing his first book, titled *Placing the Suspect Behind the Keyboard: Using Digital Forensics and Investigative Techniques to Identify Cybercrime Suspects*, he co-wrote his 2nd book with Eric Zimmerman and Jimmy Weg, who is a knowledgeable technical editor. Both Brett and Eric are experts in cyber forensics, with many years of law enforcement experience at both the state and federal levels.

This book is a primer for all novice as well as expert users of the X-Ways Forensics (XWF) software, and is a good resource for readers who are entry-level digital forensics professionals, law enforcement officers, or government agency investigators. Further, it can also be utilized as a good reference manual supplementing a college cyber forensics course.

Written in a straightforward, easy to read, and compact format, *The X-Ways Forensics Practitioner's Guide* contains 10 chapters and two appendices that fully cover the major topics associated with the XWF tool. Each chapter starts with a short introduction and ends with a short summary. Throughout the chapters, there are many XWF Tips and Tricks that provide additional sidebar to various selected items, and numerous screenshots are displayed to help readers follow through the discussion. If any menu shortcut keys were used, they will then be listed at the end of the chapter. Using detailed explanations, tutorials, and hands-on case demonstration of real-life examples, the authors started with software installation in Chapter 1 and advanced at a reasonable pace through the chapters to advanced topics in Chapter 7.

Chapter 1 Installation and Configuration of X-Ways Forensics (XWF) differentiates the difference between the installation and configuration of XWF from other forensic applications. It describes the different ways to install XWF, the XWF dongle, the XWF user interface, and finally, the initial configuration steps for XWF.

Once XWF is installed on the computer, readers learn how to create and manage cases, add evidences to new cases, organize case data, and manage case files in Chapter 2 Case Management and Imaging. Readers also learn how to create a forensic image of a computer media. Different types of imaging–reverse imaging, skeleton imaging, cleansed imaging, and physical memory imaging–are clearly explained. Other topics described in this chapter include working with RAID arrays and leveraging the power of F-Response.

Chapter 3 Navigating the X-Ways Forensics Interface is the longest chapter, in which the authors thoroughly described all the basic and advanced navigation features of the XWF user interface. Some of these features include working with the Case Data window and its directory tree, reviewing all the options in the Directory Browser, selecting and working with files and directories in the Directory Browser, and understanding the Mode buttons when previewing a certain file or a group of files. Options that were not discussed in previous chapter, such as General Options, Viewer Options, and Security Options, were also covered in this chapter.

Refine Volume Snapshot (RVS)–a very important and distinct feature of XWF–is covered in Chapter 4. Although the concept of VS was introduced in Chapter 2, its capabilities and options are explored in more in-depth here.

Two important, distinct, and easy-to-use features of XWF–the XWF Internal Hash Database and Registry Viewer–are covered in Chapter 5. XWF has only one, but very large, hash database containing thousands of hash sets. The XWF Registry Viewer and Registry Report are used for registry analysis, and they have many functions such as searching, copying, and reporting, that can be used to find and display relevant information in the XWF case report from registry hives.

Chapter 6 Searching in X-Ways Forensics describes the powerful and flexible options available to users to help them search for data and information in the evidence case. For instance, readers can use the Simultaneous Search feature to quickly and easily find search terms using both simple strings and regular expressions. This chapter concluded with a discussion on creating and using an index and the various ways to perform both text and hex searches.

We move into more advanced topics in Chapter 7, titled Advanced Use of X-Ways Forensics. Readers learn how to customize XWF configuration files, maneuver in hex, perform timeline and event analysis, collect ambient data such as free or slack space, and conduct RAM analysis. Timeline analysis can be performed in two ways: Calendar mode and Events view. The last topic discussed in this chapter is the different ways to automate XWF through scripts or the application programming interface (API).

Reader can take a breather from the technical features in Chapter 8 X-Ways Forensics Reporting. Writing forensics investigative reports can be quite simple and straightforward. In this chapter, readers learn how to create report tables (RTs) that can be used as bookmarks, associate items to the RTs, then generate an investigative report that can be viewed online and by anyone using a Web browser.

Chapter 9 X-Ways Forensics and Electronic Discovery narrates all the complete functionality of XWF that can be used for document collection in eDiscovery, ranging from identification to production. Users can review relevant data using X-Ways Investigator, a scaled-down version of XWF.

Chapter 10 X-Ways Forensics and Criminal Investigations is the shortest chapter, covering informative criminal investigations topics such as knock and talks, search warrants, and probationary-type reviews of computers. A knock and talk occurs when the owner of a computer consents to the search by voluntarily waiving his/her rights. A search warrant must be authorized by a judge after a probable cause was established by the law enforcement officer.

Materials included in the two appendices can be quite helpful to XWF users too. Appendix A XWF Additional Information provides a list of online resources and keyboard shortcuts of popular menu commands. Appendix B XWF How to's addresses FAQs and more XWF tips that could be handy and helpful to any users.

This is indeed a good reference manual for anyone who wants to learn more about the XWF software. It is also highly recommended for expert forensics specialists who want to utilize the fullest potential of the XWF software tools.