# SpringerBriefs in Computer Science

More information about this series at http://www.springer.com/series/10028

Joakim Kävrestad

# Guide to Digital Forensics

## A Concise and Practical Introduction

Springer

Joakim Kävrestad
University of Skövde
Skövde
Sweden

ISSN 2191-5768 ISSN 2191-5776 (electronic)
SpringerBriefs in Computer Science
ISBN 978-3-319-67449-0 ISBN 978-3-319-67450-6 (eBook)
https://doi.org/10.1007/978-3-319-67450-6

Library of Congress Control Number: 2017952933



Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer International Publishing AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

# Preface

This book introduces the reader to the world of digital forensics in a practical and accessible manner. The book was written to fulfill the need for a book that introduces forensic methodology and sound forensic thinking combined with hands-on examples for common tasks in a computer forensic examination. The author of this book has several years of experience as a computer forensic examiner, and is now working as a university-level lecturer. To further ensure that the content provided in this book is relevant and accurate in the real world, Jan-Åke Pettersson from the Swedish Police were asked to provide a feedback on the content. Thank you ever so much for your help!

This book is intended for students that are looking for an introduction to computer forensics and can also be used as a collection of instructions for practitioners. The aim is to describe and explain the steps taken during a forensic examination with the intent of making the reader aware of the constraints and considerations that apply during a forensic examination in law enforcement and in the private sector. Upon reading this book, the reader should have a proper overview of the field of digital forensics and started a journey of becoming a computer forensic expert!

Skövde, Sweden — Joakim Kävrestad

# Contents

# Introduction

This is a book written for the sole reason that when I wanted to hold a course on digital forensics, I could not find a textbook that seemed to fulfill my requirements. What I needed a book to cover were the following:

- Sound forensic thinking and methodology
- A discussion on what Computer Forensics can assist with
- Hands-on examples

My answer to my own needs was, well, to write my own book. It has become obvious to me that writing a book that fulfills those demands is not a very easy task. The main problem lies within making proper hands-on examples. For that reason I decided to put an emphasis on what digital forensics is at its very core and to make this piece of literature relevant worldwide, I have tried to omit everything that only seems relevant in a certain legislation. That being said, this is the book for you if you want to get an introduction to what computer forensics is, what it can do, and of course what it cannot do. It did feel good to use some sort of well-known forensic software for the examples in this book. I decided to go with the AccessData Forensic Toolkit for the sole reason that AccessData provides the ability to get certified, free of charge, at the time of writing.

This book begins with setting the stage for forensics examinations by discussing the theoretical foundation that the author seems as relevant and important for the area. The book will then take a more practical approach and discuss how's and why´s about some key forensic concepts. Finally, the book will provide a section with information on how to find and interpret several artifacts. It should at this point be noticed that the book does not, by far, cover every single case, question, or artifact. The practical examples are rather here to serve as demonstrations of how to implement a forensically sound way of examining digital evidence. Throughout the book you will find real-world examples where I provide examples on when something was used or important in a real-world setting.

Since most computers targeted for a forensic examination is running some version of Windows, the examples and demonstrations in this book are presented in a Windows environment. Being the most recent flavor of Windows, Windows 10 was used. However, the information should to a very large extent be applicable for previous version of Windows.

Also, every chapter in the book comes with a "Questions and tasks" section. The answers to the questions or tasks are located in Appendix A—solutions.

Happy reading!