Fundamentals of Digital Forensics

Joakim Kävrestad

Fundamentals of Digital Forensics

Theory, Methods, and Real-Life Applications

Springer

Joakim Kävrestad
School of Informatics
University of Skövde
Skövde, Sweden

ISBN 978-3-319-96318-1 ISBN 978-3-319-96319-8 (eBook)
https://doi.org/10.1007/978-3-319-96319-8

Library of Congress Control Number: 2018948608

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

Preface

Fundamentals of Digital Forensics presents and discusses the fundamental building blocks of computer forensics in a practical and accessible manner. Building on *Guide to Digital Forensics: A Concise and Practical Introduction*, it presents a theoretical background discussing forensic methods, artifacts, and constraints primarily relating to computer forensic examinations in the context of crime investigations. Further, the book discusses artifacts and methodology in a practical manner that introduces forensic tools that are commonly used in forensic examinations in law enforcement as well as in the corporate sector.

The book was written to fulfill a 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 *Fundamentals of Digital Forensics* has several years of experience as a computer forensic examiner with the Swedish Police and is certified as an AccessData Certified Examiner. He is now working as a university level lecturer and researcher in the domain and as a forensic consultant. To further ensure that the content provided in this book is relevant and accurate in the real world, the book has been developed in close relation with the Skövde Office of the Swedish police in general and Jan-Åke Pettersson in particular. Thank you ever so much for your help!

Fundamentals of Digital Forensics 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 be able as well as motivated to start the journey of becoming a computer forensic expert!

Skövde, Sweden Joakim Kävrestad

Contents

Part I Theory

Part II Put It to Practice

Part III Memory Forensics

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 was:

- 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 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. Since forensic software can be quite expensive, I decided to use two options interchangeably. The first collection of tools are the proprietary AccessData Forensic Toolkit that was chosen for the sole reason that AccessData provides the ability to get certified, free of charge, at the time of writing. Using the predecessor of this book in teaching shows that this book can in fact be used to prepare for the AccessData certification test. Further, this book uses a collection of various open source or otherwise free tools that can accomplish the same as the proprietary AccessData tools.

This book begins with setting the stage for forensics examinations by discussing the theoretical foundation that the author regards as relevant and important for the area. This section will introduce the reader to the area of computer forensics and introduce forensic methodology as well as a discussion on how to find and interpret certain artifacts in a Windows environment. The book will then take a more practical turn 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 and use forensic tools. 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 are 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 the previous version of Windows.

Also, most chapters in the book come with a "Questions and tasks" section. Some are questions with a right or wrong answer, and some are of more exploratory nature. Whatever the case, answers or discussions are found in Appendix A—Solutions. Complementing the book, there are video lectures covering most of the book content available for viewing at YouTube: https://www.youtube.com/playlist?list=PLEjQDf4Fr75pBnu8WArpeZTKC9-LrYDTl.

Happy reading!