Fundamentals of Digital Forensics

Joakim Kävrestad

Fundamentals of Digital Forensics

Theory, Methods, and Real-Life Applications

Second Edition

Springer

Joakim Kävrestad
School of Informatics
University of Skövde
Skövde, Sweden

ISBN 978-3-030-38953-6 ISBN 978-3-030-38954-3 (eBook)
https://doi.org/10.1007/978-3-030-38954-3

© Springer Nature Switzerland AG 2018, 2020
This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.
The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.
The publisher, the authors, and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

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

Preface

Overview and Audience

Fundamentals of Digital Forensics: Theory, Methods, and Real-Life Applications 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. Furthermore, it discusses artifacts and methodologies, in a practical manner, that introduce forensic tools commonly used in forensic examinations in law enforcement as well as in the corporate sector.

This 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 examiner. He currently works 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 with Jan-Åke Pettersson in particular, for which the author is extremely thankful. *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!

Following the first edition of this book, this second edition has been updated with more material covering incident response practices and tasks. It has also been partly

rewritten following student feedback, and on that note, a special thanks to Marcus Birath for the much appreciated proofreading!

Motivation and Features

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 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 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 and what it can and 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, which was chosen for the sole reason that AccessData provided 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 areas of computer forensics and forensic methodology as well as will discuss on how to find and interpret certain artifacts in a Windows environment. The book will then take a more practical turn and discuss hows and whys 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. 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 applicable 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 version of Windows, Windows

10 was used. However, the information should to a very large extent be applicable for the previous version of Windows.

In this second volume, more content describing digital forensics in the corporate secure has been added, introducing incident response work in a reasonable manner. Furthermore, the chapters on memory analysis have been greatly rewritten to include more practices and tools.

Also, most chapters in this 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 in YouTube: https://www.youtube.com/playlist?list=PLEjQDf4Fr75pBnu8WArpeZTKC9-LrYDTl.

Happy reading!

Skövde, Sweden Joakim Kävrestad

Contents

Part IV Memory Forensics