

# SpringerBriefs in Computer Science

## Series editors

Stan Zdonik, Brown University, Providence, Rhode Island, USA

Shashi Shekhar, University of Minnesota, Minneapolis, Minnesota, USA

Xindong Wu, University of Vermont, Burlington, Vermont, USA

Lakhmi C. Jain, University of South Australia, Adelaide, South Australia, Australia

David Padua, University of Illinois Urbana-Champaign, Urbana, Illinois, USA

Xuemin (Sherman) Shen, University of Waterloo, Waterloo, Ontario, Canada

Borko Furht, Florida Atlantic University, Boca Raton, Florida, USA

V.S. Subrahmanian, University of Maryland, College Park, Maryland, USA

Martial Hebert, Carnegie Mellon University, Pittsburgh, Pennsylvania, USA

Katsushi Ikeuchi, University of Tokyo, Tokyo, Japan

Bruno Siciliano, Università degli di Napoli Federico II, Napoli, Italy

Sushil Jajodia, George Mason University, Fairfax, Virginia, USA

Newton Lee, Newton Lee Laboratories, LLC, Tujunga, California, USA

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

© The Author(s) 2017

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, express 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.

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

## Part I Theory

<b>1</b>	<b>What Is Digital Forensics?</b> .....	3
1.1	A Forensic Examination .....	4
1.2	Questions and Tasks .....	6
	References .....	7
<b>2</b>	<b>What Is Cybercrime?</b> .....	9
2.1	Questions and Tasks .....	10
	References .....	11
<b>3</b>	<b>Computer Theory</b> .....	13
3.1	Secondary Storage Media .....	14
3.2	The NTFS File Systems .....	14
3.3	File Structure .....	15
3.4	Data Representation .....	16
3.5	Windows Registry .....	18
3.6	Encryption and Hashing .....	20
3.7	Decryption Attack and Password Cracking .....	21
3.8	Memory and Paging .....	24
3.9	Questions and Tasks .....	25
	References .....	25
<b>4</b>	<b>Collecting Evidence</b> .....	27
4.1	When the Device Is off .....	28
4.2	When the Device Is on .....	29
4.3	Live Investigation: Preparation .....	31
4.4	Live Investigation: Conducting .....	32
4.5	Live Investigation: Afterthoughts .....	35
4.6	Questions and Tasks .....	35
	References .....	35

- 5 Analyzing Data and Writing Reports . . . . . 37**
  - 5.1 Setting the Stage . . . . . 38
  - 5.2 Forensic Analysis . . . . . 40
  - 5.3 Reporting . . . . . 43
    - 5.3.1 Case Data. . . . . 43
    - 5.3.2 Purpose of Examination . . . . . 43
    - 5.3.3 Findings . . . . . 44
    - 5.3.4 Conclusions . . . . . 45
  - 5.4 Final Remarks. . . . . 45
  - 5.5 Questions and Tasks . . . . . 46
  
- Part II Put it to Practice**
  
- 6 Collecting Data . . . . . 49**
  - 6.1 Imaging . . . . . 49
  - 6.2 Collecting Memory Dumps . . . . . 53
  - 6.3 Collecting Registry Data . . . . . 57
  - 6.4 Collecting Video from Surveillance . . . . . 58
  - 6.5 Questions and Tasks . . . . . 58
  - References . . . . . 58
  
- 7 Indexing, Searching, and Cracking . . . . . 61**
  - 7.1 Indexing . . . . . 61
  - 7.2 Searching . . . . . 63
  - 7.3 Cracking. . . . . 64
  - 7.4 Questions and Tasks . . . . . 69
  
- 8 Finding Artifacts . . . . . 71**
  - 8.1 Install Date . . . . . 71
  - 8.2 Time Zone Information . . . . . 72
  - 8.3 Users on the System . . . . . 73
  - 8.4 Registered Owner . . . . . 74
  - 8.5 Partition Analysis and Recovery . . . . . 75
  - 8.6 Deleted Files. . . . . 76
    - 8.6.1 Recovering Files Deleted from MFT . . . . . 77
    - 8.6.2 File Carving . . . . . 77
  - 8.7 Analyzing Compound Files . . . . . 78
  - 8.8 Analyzing File Metadata . . . . . 79
    - 8.8.1 NTFS Timestamps . . . . . 80
    - 8.8.2 Exif Data . . . . . 80
    - 8.8.3 Office Metadata . . . . . 81
  - 8.9 Analyzing Log Files . . . . . 82
  - 8.10 Analyzing Unorganized Data . . . . . 84
  - 8.11 Questions and Tasks . . . . . 86
  - References . . . . . 86

- 9 Some Common Questions . . . . .** 89
  - 9.1 Was the Computer Remote Controlled? . . . . . 90
    - 9.1.1 Analysis of Applications . . . . . 90
    - 9.1.2 Scenario Testing . . . . . 91
  - 9.2 Who Was Using the Computer? . . . . . 93
  - 9.3 Was This Device Ever at Site X? . . . . . 94
  - 9.4 Questions and Tasks . . . . . 95
- 10 FTK Specifics . . . . .** 97
  - 10.1 FTK: Create a Case . . . . . 98
  - 10.2 FTK: Preprocessing . . . . . 101
  - 10.3 FTK: Overview . . . . . 104
  - 10.4 Registry Viewer: Overview . . . . . 111
- 11 Basic Memory Analysis . . . . .** 117
  - 11.1 Questions and Tasks . . . . . 122
  - References . . . . . 122

**Part III Vocabulary**

- 12 Vocabulary . . . . .** 125

**Part IV Appendices**

- 13 Appendix A—Solutions . . . . .** 129
  - 13.1 Chapter 1 . . . . . 129
  - 13.2 Chapter 2 . . . . . 129
  - 13.3 Chapter 3 . . . . . 130
  - 13.4 Chapter 4 . . . . . 130
  - 13.5 Chapter 5 . . . . . 130
  - 13.6 Chapter 6 . . . . . 131
  - 13.7 Chapter 7 . . . . . 131
  - 13.8 Chapter 8 . . . . . 132
  - 13.9 Chapter 9 . . . . . 132
  - 13.10 Chapter 11 . . . . . 132
  - Reference . . . . . 132
- 14 Appendix B—Useful Scripts . . . . .** 133
  - 14.1 Capturing Basic Computer Information  
on MAC and Linux . . . . . 133
  - 14.2 Capturing Basic Computer Information on Windows . . . . . 135
  - 14.3 Parse Jitsi Chat Logs . . . . . 136



- 15 Appendix C—Sample Report Template . . . . . 137**
  - 15.1 Examination Data . . . . . 137
    - 15.1.1 Summary . . . . . 137
    - 15.1.2 Findings . . . . . 138
  - 15.2 Conclusions . . . . . 138
    - 15.2.1 Word List. . . . . 138
- 16 Appendix D—List of Time Zones . . . . . 139**
  - Reference . . . . . 141
- 17 Appendix E—Complete Jitsi Chat Log . . . . . 143**

# 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!