
Fundamentals of Digital Forensics

Joakim Kävrestad

Fundamentals of Digital Forensics

Theory, Methods, and Real-Life Applications

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

© Springer International Publishing AG, part of Springer Nature 2018

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.

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

1	What Is Digital Forensics?	3
1.1	A Forensic Examination	4
1.2	How Forensics Has Been Used	6
1.3	Questions and Tasks	7
	References	8
2	Cybercrime, Cyber Aided Crime and Digital Evidence	9
2.1	Cybercrime	10
2.2	Cyber Aided Crime	10
2.3	Crimes with Digital Evidence	11
2.4	Questions and Tasks	12
	References	12
3	Computer Theory	13
3.1	Secondary Storage Media	13
3.2	The NTFS File Systems	14
3.3	File Structure	15
3.4	Data Representation	16
3.5	Windows Registry	17
3.6	Encryption and Hashing	19
3.7	Memory and Paging	21
3.8	Questions and Tasks	22
	References	22
4	Notable Artifacts	23
4.1	Metadata	23
4.2	EXIF Data	24
4.3	Prefetch	25
4.4	Shellbags	26
4.5	.LNK Files	27
4.6	MRU-Stuff	28
4.7	Thumbcache	31

4.8	Windows Event Viewer	32
4.9	Program Log Files	34
4.10	USB Device History	34
4.11	Questions and Tasks	37
	References	37
5	Decryption and Password Enforcing	39
5.1	Decryption Attacks	39
5.2	Password Guessing Attacks	41
5.3	Questions and Tasks	46
	References	46
6	Collecting Evidence	47
6.1	When the Device Is Off	48
6.2	When the Device Is On	49
6.3	Live Investigation: Preparation	49
6.4	Live Investigation: Conducting	51
6.5	Live Investigation: Afterthoughts	55
6.6	Questions and Tasks	55
	References	55
7	Analyzing Data and Writing Reports	57
7.1	Setting the Stage	57
7.2	Forensic Analysis	59
7.3	Reporting	62
	7.3.1 Case Data	63
	7.3.2 Purpose of Examination	64
	7.3.3 Findings	65
	7.3.4 Conclusions	67
7.4	Final Remarks	69
7.5	Questions and Tasks	70
 Part II Put It to Practice		
8	Collecting Data	73
8.1	Imaging	73
8.2	Collecting Memory Dumps	78
8.3	Collecting Registry Data	80
8.4	Collecting Video from Surveillance	80
8.5	Process of a Live Examination	81
8.6	Questions and Tasks	83
	References	83

9	Indexing and Searching	85
9.1	Indexing	85
9.2	Searching	87
9.3	Questions and Tasks	91
10	Cracking	93
10.1	Password Cracking Using PRTK	94
10.2	Password Cracking Using Hashcat	98
10.3	Questions and Tasks	102
11	Finding Artifacts	105
11.1	Install Date	105
11.2	Time Zone Information	106
11.3	Users in the System	106
11.4	Registered Owner	108
11.5	Partition Analysis and Recovery	108
11.6	Deleted Files	111
	11.6.1 Recovering Files Deleted from MFT	111
	11.6.2 File Carving	112
11.7	Analyzing Compound Files	113
11.8	Analyzing File Metadata	113
	11.8.1 NTFS Time Stamps	114
	11.8.2 EXIF Data	115
	11.8.3 Office Metadata	115
11.9	Analyzing Log Files	116
11.10	Analyzing Unorganized Data	118
11.11	Questions and Tasks	121
	References	121
12	Some Common Questions	123
12.1	Was the Computer Remote Controlled?	123
	12.1.1 Analysis of Applications	124
	12.1.2 Scenario Testing	125
12.2	Who Was Using the Computer?	126
12.3	Was This Device Ever at Site X?	128
12.4	What Device Took the Picture and Where?	128
12.5	Where Was the Documents Created?	130
12.6	Questions and Tasks	132
13	FTK Specifics	133
13.1	FTK: Create a Case	133
13.2	FTK: Preprocessing	136
13.3	FTK: Overview	140
13.4	Registry Viewer: Overview	147

14	Open-Source or Freeware Tools	153
14.1	Prefetch Parser by Erik Zimmerman	153
14.2	Shellbags Explorer by Erik Zimmerman	153
14.3	.lnk File Parser by Erik Zimmerman	154
14.4	Thumbcache Viewer	155
14.5	USBDevview by NirSoft	156
14.6	Autopsy	158
14.6.1	Get Going	158
14.6.2	Autopsy Overview	161
14.6.3	The Image Gallery	166
14.6.4	Communications	168
14.6.5	Timeline	169
14.7	Registry Explorer	170
 Part III Memory Forensics		
15	Memory Management	175
15.1	Array, Record and String	177
15.2	Linked Lists	177
15.3	Questions and Tasks	178
	Reference	178
16	Volatility	179
16.1	What Is Volatility Made up from?	179
16.2	How to Get Volatility	180
16.3	Basic Usage	181
16.4	Volshell	182
	References	183
17	Memory Analysis in Criminal Investigations	185
17.1	Questions and Tasks	190
18	Malware Analysis	191
18.1	Questions and Tasks	196
Appendix A: Solutions		197
Appendix B: Useful Scripts		207
Appendix C: Sample Report (Template)		215
Appendix D: List of Time Zones		219
Appendix E: Complete jitsi Chat Log		223
Index		229

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!