
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-LrYDTI>.

Happy reading!

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	7
2	Ethics and Integrity	9
2.1	Tracing Online Users	10
2.2	Key Disclosure Law(s)	11
2.3	Police Hacking	12
2.4	Ethical Guidelines	13
2.5	Questions and Tasks	15
	References	16
3	Computer Theory	17
3.1	Secondary Storage Media	17
3.2	The NTFS File Systems	18
3.3	File Structure	19
3.4	Data Representation	20
3.5	User Accounts in Windows 10	21
3.6	Windows Registry	22
3.7	Encryption and Hashing	25
3.8	SQLite Databases	27
3.9	Memory and Paging	28
3.10	Questions and Tasks	28
	References	29
4	Notable Artifacts	31
4.1	Metadata	31
4.2	EXIF Data	32
4.3	Prefetch	33
4.4	Shellbags	34
4.5	.LNK Files	35

4.6	MRU-Stuff	36
4.7	Thumbcache	38
4.8	Windows Event Viewer	39
4.9	Program Log Files	42
4.10	USB Device History	42
4.11	Questions and Tasks	44
	References	45
5	Decryption and Password Enforcing	47
5.1	Password Theory	47
5.2	Decryption Attacks	50
5.3	Password Guessing Attacks	51
5.4	Questions and Tasks	55
	References	55
Part II The Forensic Process		
6	Cybercrime, Cyber Aided Crime, and Digital Evidence	59
6.1	Cybercrime	60
6.2	Cyber Aided Crime	60
6.3	Crimes with Digital Evidence	61
6.4	Questions and Tasks	62
	References	62
7	Incident Response	63
7.1	Why and When?	63
7.2	Establishing Capabilities	64
7.3	Incident Handling	66
7.4	Questions and Tasks	68
	References	68
8	Collecting Evidence	69
8.1	When the Device Is Off	70
8.2	When the Device Is On	71
8.3	Live Investigation: Preparation	72
8.4	Live Investigation: Conducting	74
8.5	Live Investigation: Afterthoughts	77
8.6	Questions and Tasks	77
	References	78
9	Triage	79
9.1	Specific Examinations	79
9.2	White and Blacklisting	81
9.3	Automated Analysis	81

9.4	Field Triage	82
9.5	Questions and Tasks	83
	References	83
10	Analyzing Data and Writing Reports	85
10.1	Setting the Stage	85
10.2	Forensic Analysis	87
10.3	Reporting	90
	10.3.1 Case Data	91
	10.3.2 Purpose of Examination	92
	10.3.3 Findings	94
	10.3.4 Conclusions	95
10.4	Final Remarks	97
10.5	Questions and Tasks	98
 Part III Get Practical		
11	Collecting Data	101
11.1	Imaging	101
11.2	Collecting Memory Dumps	106
11.3	Collecting Registry Data	108
11.4	Collecting Network Data	109
11.5	Collecting Video from Surveillance	110
11.6	Process of a Live Examination	111
11.7	Questions and Tasks	113
	References	113
12	Indexing and Searching	115
12.1	Indexing	115
12.2	Searching	117
	12.2.1 Questions and Tasks	121
13	Cracking	123
13.1	Password Cracking Using PRTK	124
13.2	Password Cracking Using Hashcat	129
13.3	Questions and Tasks	133
14	Finding Artifacts	135
14.1	Install Date	135
14.2	Time Zone Information	136
14.3	Users in the System	136
14.4	Registered Owner	138
14.5	Partition Analysis and Recovery	138
14.6	Deleted Files	141
	14.6.1 Recovering Files Deleted from MFT	141
	14.6.2 File Carving	142

14.7	Analyzing Compound Files	143
14.8	Analyzing File Metadata	143
14.8.1	NTFS Time Stamps	144
14.8.2	EXIF Data	145
14.8.3	Office Metadata	145
14.9	Analyzing Log Files	146
14.10	Analyzing Unorganized Data	148
14.11	Analyzing SQLite Databases	150
14.12	Questions and Tasks	152
	References	153
15	Some Common Questions and Tasks	155
15.1	Was the Computer Remote Controlled?	155
15.1.1	Analysis of Applications	156
15.1.2	Scenario Testing	157
15.2	Who Was Using the Computer?	158
15.3	Was This Device Ever at Site X?	160
15.4	What Device Took the Picture and Where?	160
15.5	Where Were the Documents Created?	162
15.6	Application Analysis: The Windows Firewall	164
15.7	Questions and Tasks	167
16	FTK Specifics	169
16.1	FTK: Create a Case	169
16.2	FTK: Preprocessing	172
16.3	FTK: Overview	176
16.4	Registry Viewer: Overview	182
17	Open-Source or Freeware Tools	189
17.1	Prefetch Parser by Erik Zimmerman	189
17.2	Shellbags Explorer by Erik Zimmerman	189
17.3	.lnk File Parser by Erik Zimmerman	191
17.4	Thumbcache Viewer	191
17.5	USBDevview by NirSoft	191
17.6	Autopsy	193
17.6.1	Get Going	194
17.6.2	Autopsy Overview	197
17.6.3	The Image Gallery	202
17.6.4	Communications	203
17.6.5	Timeline	204
17.7	Registry Explorer	205

Part IV Memory Forensics

18	Memory Analysis	211
18.1	Data Storage	211
18.2	Processes	214
18.3	Forensic Techniques	215
18.4	Questions and Tasks	216
	Reference	216
19	Memory Analysis Tools	217
19.1	Volatility	217
19.1.1	What Is Volatility Made Up from?	218
19.1.2	How to Get Volatility	219
19.1.3	Basic Usage	220
19.1.4	Volshell	221
19.2	Redline	221
19.2.1	Components of Redline	221
19.2.2	Redline Usage	223
	References	224
20	Memory Analysis in Criminal Investigations	225
20.1	Questions and Tasks	230
21	Malware Analysis	231
21.1	Malware Analysis with Volatility	231
21.2	Malware Analysis with Redline	236
21.3	Questions and Tasks	242
	Appendix A: Solutions	243
	Appendix B: Useful Scripts	250
	Appendix C: Sample Report (Template)	255
	Appendix D: List of Time Zones	258
	Appendix E: Complete Jitsi Chat Log	261
	Index	267