

# 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

<b>5</b>	<b>Analyzing Data and Writing Reports</b>	<b>37</b>
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
 <b>Part II Put it to Practice</b>		
<b>6</b>	<b>Collecting Data</b>	<b>49</b>
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
<b>7</b>	<b>Indexing, Searching, and Cracking</b>	<b>61</b>
7.1	Indexing	61
7.2	Searching	63
7.3	Cracking	64
7.4	Questions and Tasks	69
<b>8</b>	<b>Finding Artifacts</b>	<b>71</b>
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

<b>9</b>	<b>Some Common Questions</b> . . . . .	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
<b>10</b>	<b>FTK Specifics</b> . . . . .	97
10.1	FTK: Create a Case . . . . .	98
10.2	FTK: Preprocessing . . . . .	101
10.3	FTK: Overview . . . . .	104
10.4	Registry Viewer: Overview . . . . .	111
<b>11</b>	<b>Basic Memory Analysis</b> . . . . .	117
11.1	Questions and Tasks . . . . .	122
	References . . . . .	122
 <b>Part III Vocabulary</b>		
<b>12</b>	<b>Vocabulary</b> . . . . .	125
 <b>Part IV Appendices</b>		
<b>13</b>	<b>Appendix A—Solutions</b> . . . . .	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
<b>14</b>	<b>Appendix B—Useful Scripts</b> . . . . .	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

<b>15</b>	<b>Appendix C—Sample Report Template</b>	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
<b>16</b>	<b>Appendix D—List of Time Zones</b>	139
	Reference	141
<b>17</b>	<b>Appendix E—Complete Jitsi Chat Log</b>	143

Guide to Digital Forensics

A Concise and Practical Introduction

Kävrestad, J.

2017, XII, 147 p. 79 illus., Softcover

ISBN: 978-3-319-67449-0