
CONTENTS

Introduction	xi
Acknowledgments	xvii
1 A Definition of Computer Forensics	1
Introduction	1
Forensic Science	2
History of Computer Forensics	2
World Wide Web	5
Hacker Community	6
Conclusion	10
Notes	11
Suggested Reading	12
2 Basics of Computer Forensic Concepts	13
Introduction	13
Understanding Digital Evidence	14
Input	15
Storage	15
Processing	16
What Computer Data Is	17
Output	23
Conclusion	24
Notes	24
Suggested Reading	24
3 Preservation and Collection of Digital Evidence	25
Introduction	25
Rules of Evidence	26
Preservation	27
Collection	30
Conclusion	36
Note	37
Suggested Reading	37

4	Analysis of Digital Evidence	38
	Introduction	38
	Forensic Analysis	39
	Conclusion	50
	Notes	50
	Suggested Reading	51
5	Reporting and Rendering the Opinion	52
	Introduction	52
	Preparing the Report	53
	Presentation	57
	Trial Process	57
	Conclusion	64
	Suggested Reading	65
6	Computer Attacks	66
	Hackers and Phreakz Oh My	66
	Hackers: Unauthorized Use and Trespassing	66
	Wireless Hacking	71
	Malware	75
	Attacks from the Inside	79
	Conclusion	85
	Notes	86
	Suggested Reading	87
7	Computers as Tools for Evil	88
	Introduction	88
	Computers and Crime	88
	Identity Theft	89
	Concealment	96
	Auction Fraud and Retail Cons	97
	Counterfeiting and Forgery	100
	Prostitution	100
	Securities Fraud	101
	Conclusion	105
	Notes	105

8	Computer Tools and the Forensic Examination	108
	Introduction	108
	Assuming Control of the Case	109
	Understanding the Case	109
	Evaluating the Evidence	110
	Examining the “Live” System	110
	Collecting Data from a Dead System	116
	Imaging the Drive	118
	Data Extraction	120
	Data Analysis	122
	Conclusion	125
	Notes	126
9	Presenting Digital Evidence in Court	127
	Introduction	127
	Evidence	128
	Types of Evidence	129
	Expert Witnesses	131
	Legal Requirements of Evidence	132
	Search and Seizure	137
	Conclusion	142
	Notes	143
	Index	145

<http://www.pbookshop.com>