

Contents

	Introduction	xi
1	Introduction to Software Forensics	1
	Digital Forensic Definitions	2
	Software Forensics	4
	Objectives and Objects of Software Forensics	5
	Identity	6
	Other Objects of Study	11
	Software Forensic Tools	12
	The Process	12
	The Products	14
	Finally, Already, the Tools	16
	Software Forensic Technologies and Practices	18
	Content Analysis	18
	Noncontent Analysis	19
	Legal Considerations	20
	Presentation in Court	21
	Summary	21
2	The Players—Hackers, Crackers, Phreaks, and Other Doodz	23
	Terminology	24
	Types of Blackhats	26
	Motivations and Rationales	29
	General Characteristics	35
	Blackhat Products	37

	Other Products	42
	Summary	43
3	Software Code and Analysis Tools	45
	The Programming Process	47
	The Products	51
	The Resulting Objects	52
	The Analytical Tools	53
	Forensic Tools	63
	Summary	64
4	Advanced Tools	65
	Decompilation	65
	Desquirr	67
	Dcc	68
	Boomerang	68
	Plagiarism	68
	JPlag	69
	YAP	70
	Other Approaches	71
	Summary	76
5	Law and Ethics—Software Forensics in Court	77
	Legal Systems	77
	Differences within Common Law	78
	Jurisdiction	79
	Evidence	80
	Types of Evidence	80
	Rules of Evidence	81
	Providing Expert Testimony	84
	Ethics	87
	Disclosure	88
	Blackhat Motivations as a Defense	89

	Summary	90
6	Computer Virus and Malware Concepts and Background	91
	History of Computer Viruses and Worms	91
	Malware Definition and Structure	95
	Virus Structure	98
	Worm Structure	100
	Trojan Structure	101
	Logic Bomb Structure	103
	Remote Access Trojan (RAT) Structure	103
	Distributed Denial of Service (DDoS) Structure	104
	Detection and Antidetection Techniques	104
	Detection Technologies	106
	Stealth and Antidetection Measures	111
	Summary	112
7	Programming Cultures and Indicators	113
	User Interface	113
	Cultural Features and “Help”	116
	Functions	120
	Programming Style	122
	Program Structure	122
	Programmer Skill and Objectives	124
	Developmental Strictures	126
	Technological Change	127
	Summary	127
8	Stylistic Analysis and Linguistic Forensics	129
	Biblical Criticism	130
	Shakespeare and Other Literature	131
	Individual Identification and Authentication	134
	Content Analysis	137

	Noncontent Analysis	139
	The Content/Noncontent Debate	144
	Noncontent Metrics as Evidence of Authorship	145
	Additional Indicators	146
	Summary	146
9	Authorship Analysis	147
	Problems	147
	Plagiarism Detection versus Authorship Analysis	148
	How Can It Work?	150
	Source Code Indicators	150
	More General Indicators	151
	Is It Reliable?	152
	Summary	153
	References and Resources	155
	Introduction and Background	156
	Blackhats	166
	Tools	174
	Advanced Tools	190
	Law and Ethics	190
	Viruses and Malware	196
	Stylistic Analysis and Linguistic Forensics	201
	Software Authorship Analysis	202
	Index	205