

Contents

Contributing Authors	ix
Preface	xvii
PART I THEMES AND ISSUES	
1	
The State of the Science of Digital Evidence Examination <i>Fred Cohen, Julie Lowrie and Charles Preston</i>	3
2	
An Investigative Framework for Incident Analysis <i>Clive Blackwell</i>	23
3	
Cloud Forensics <i>Keyun Ruan, Joe Carthy, Tahar Kechadi and Mark Crosbie</i>	35
PART II FORENSIC TECHNIQUES	
4	
Searching Massive Data Streams Using Multipattern Regular Expressions <i>Jon Stewart and Joel Uckelman</i>	49
5	
Fast Content-Based File Type Identification <i>Irfan Ahmed, Kyung-Suk Lhee, Hyun-Jung Shin and Man-Pyo Hong</i>	65
6	
Case-Based Reasoning in Live Forensics <i>Bruno Hoelz, Celia Ralha and Frederico Mesquita</i>	77
7	
Assembling Metadata for Database Forensics <i>Hector Beyers, Martin Olivier and Gerhard Hancke</i>	89

8

- Forensic Leak Detection for Business Process Models 101
Rafael Accorsi and Claus Wonnemann

9

- Analyzing Stylometric Approaches to Author Obfuscation 115
Patrick Juola and Darren Vescovi

PART III FRAUD AND MALWARE INVESTIGATIONS

10

- Detecting Fraud Using Modified Benford Analysis 129
Christian Winter, Markus Schneider and York Yannikos

11

- Detecting Collusive Fraud in Enterprise Resource Planning Systems 143
Asadul Islam, Malcolm Corney, George Mohay, Andrew Clark, Shane Bracher, Tobias Raub and Ulrich Flegel

12

- Analysis of Back-Doored Phishing Kits 155
Heather McCalley, Brad Wardman and Gary Warner

13

- Identifying Malware Using Cross-Evidence Correlation 169
Anders Flaglien, Katrin Franke and Andre Arnes

14

- Detecting Mobile Spam Botnets Using Artificial Immune Systems 183
Ickin Vural and Hein Venter

PART IV NETWORK FORENSICS

15

- An FPGA System for Detecting Malicious DNS Network Traffic 195
Brennon Thomas, Barry Mullins, Gilbert Peterson and Robert Mills

16

- Router and Interface Marking for Network Forensics 209
Emmanuel Pilli, Ramesh Joshi and Rajdeep Niyogi

17

- Extracting Evidence Related to VoIP Calls 221
David Irwin and Jill Slay

PART V ADVANCED FORENSIC TECHNIQUES

18	
Sensitivity Analysis of Bayesian Networks Used in Forensic Investigations	231
<i>Michael Kwan, Richard Overill, Kam-Pui Chow, Hayson Tse, Frank Law and Pierre Lai</i>	
19	
Steganographic Techniques for Hiding Data in SWF Files	245
<i>Mark-Anthony Fouche and Martin Olivier</i>	
20	
Evaluating Digital Forensic Options for the Apple iPad	257
<i>Andrew Hay, Dennis Krill, Benjamin Kuhar and Gilbert Peterson</i>	
21	
Forensic Analysis of Plug Computers	275
<i>Scott Conrad, Greg Dorn and Philip Craiger</i>	