

Contents

Contributing Authors	ix
Preface	xvii

PART I THEMES AND ISSUES

1	
On the Creation of Reliable Digital Evidence	3
<i>Nicolai Kuntze, Carsten Rudolph, Aaron Alva, Barbara Endicott-Popovsky, John Christiansen and Thomas Kemmerich</i>	
2	
Managing Terabyte-Scale Investigations with Similarity Digests	19
<i>Vassil Roussev</i>	
3	
Visualizing Information in Digital Forensics	35
<i>Grant Osborne, Hannah Thinyane and Jill Slay</i>	

PART II FORENSIC TECHNIQUES

4	
XML Conversion of the Windows Registry for Forensic Processing and Distribution	51
<i>Alex Nelson</i>	
5	
Context-Based File Block Classification	67
<i>Luigi Sportiello and Stefano Zanero</i>	
6	
A New Approach for Creating Forensic Hashsets	83
<i>Marcelo Ruback, Bruno Hoelz and Celia Ralha</i>	

7

- Reasoning about Evidence Using Bayesian Networks 99
Hayson Tse, Kam-Pui Chow and Michael Kwan

8

- Data Visualization for Social Network Forensics 115
Martin Mulazzani, Markus Huber and Edgar Weippl

PART III MOBILE PHONE FORENSICS

9

- Forensic Analysis of Pirated Chinese Shanzhai Mobile Phones 129
Junbin Fang, Zoe Jiang, Kam-Pui Chow, Siu-Ming Yiu, Lucas Hui, Gang Zhou, Mengfei He and Yanbin Tang

10

- Comparing Sources of Location Data from Android Smartphones 143
Michael Spreitzenbarth, Sven Schmitt and Felix Freiling

11

- An Open Framework for Smartphone Evidence Acquisition 159
Lamine Aouad, Tahar Kechadi, Justin Trentesaux and Nhien-An Le-Khac

PART IV CLOUD FORENSICS

12

- Finding File Fragments in the Cloud 169
Dirk Ras and Martin Olivier

13

- Isolating Instances in Cloud Forensics 187
Waldo Delport and Martin Olivier

14

- Key Terms for Service Level Agreements to Support Cloud Forensics 201
Keyun Ruan, Joshua James, Joe Carthy and Tahar Kechadi

PART V NETWORK FORENSICS

15

- Evidence Collection in Peer-to-Peer Network Investigations 215
Teja Myneedu and Yong Guan

16		
Validation of Rules Used in Foxy Peer-to-Peer Network Investigations	231	
<i>Ricci Jeong, Kam-Pui Chow and Pierre Lai</i>		
17		
A Log File Digital Forensic Model	247	
<i>Himal Lalla, Stephen Flowerday, Tendai Sanyamahwe and Paul Tarwireyi</i>		
18		
Implementing Forensic Readiness Using Performance Monitoring Tools	261	
<i>Franscois van Staden and Hein Venter</i>		
PART VI ADVANCED FORENSIC TECHNIQUES		
19		
Reconstruction in Database Forensics	273	
<i>Oluwasola Mary Fasan and Martin Olivier</i>		
20		
Data Hiding Techniques for Database Environments	289	
<i>Heloise Pieterse and Martin Olivier</i>		
21		
Forensic Tracking and Mobility Prediction in Vehicular Networks	303	
<i>Saif Al-Kuwari and Stephen Wolthusen</i>		
22		
Using Internal Depth to Aid Stereoscopic Image Splicing Detection	319	
<i>Mark-Anthony Fouche and Martin Olivier</i>		