

Contents

Contributing Authors	ix
Preface	xvii
PART I THEMES AND ISSUES	
1	
A History of Digital Forensics	3
<i>Mark Pollitt</i>	
2	
Toward a Science of Digital Forensic Evidence Examination	17
<i>Fred Cohen</i>	
3	
Using a Local Search Warrant to Acquire Evidence Stored Overseas via the Internet	37
<i>Kenny Wang</i>	
4	
An Analysis of the Green Dam Youth Escort Software	49
<i>Frankie Li, Hilton Chan, Kam-Pui Chow and Pierre Lai</i>	
PART II FORENSIC TECHNIQUES	
5	
Forensic Analysis of a PlayStation 3 Console	65
<i>Scott Conrad, Greg Dorn and Philip Craiger</i>	
6	
A Consistency Study of the Windows Registry	77
<i>Yuandong Zhu, Joshua James and Pavel Gladyshev</i>	

7

- Forensic Tracking and Mobility Prediction in Vehicular Networks 91
Saif Al-Kuwari and Stephen Wolthusen

8

- A Forensic Readiness Model for Wireless Networks 107
Sipho Ngobeni, Hein Venter and Ivan Burke

PART III INTERNET CRIME INVESTIGATIONS

9

- Evaluation of Evidence in Internet Auction Fraud Investigations 121
Michael Kwan, Richard Overill, Kam-Pui Chow, Jantje Silomon, Hayson Tse, Frank Law and Pierre Lai

10

- Detecting Ponzi and Pyramid Business Schemes in Choreographed Web Services 133
Murat Gunestas, Murad Mehmet and Duminda Wijesekera

11

- Identifying First Seeders in Foxy Peer-to-Peer Networks 151
Ricci Jeong, Pierre Lai, Kam-Pui Chow, Michael Kwan and Frank Law

PART IV LIVE FORENSICS

12

- Uncertainty in Live Forensics 171
Antonio Savoldi, Paolo Gubian and Isao Echizen

13

- Identifying Volatile Data from Multiple Memory Dumps in Live Forensics 185
Frank Law, Patrick Chan, Siu-Ming Yiu, Benjamin Tang, Pierre Lai, Kam-Pui Chow, Ricci Jeong, Michael Kwan, Wing-Kai Hon and Lucas Hui

14

- A Compiled Memory Analysis Tool 195
James Okolica and Gilbert Peterson

PART V ADVANCED FORENSIC TECHNIQUES

15		
Data Fingerprinting with Similarity Digests		207
<i>Vassil Roussev</i>		
16		
Refining Evidence Containers for Provenance and Accurate Data Representation		227
<i>Bradley Schatz and Michael Cohen</i>		
17		
Virtual Expansion of Rainbow Tables		243
<i>Vrizlynn Thing</i>		
18		
Digital Watermarking of Virtual Machine Images		257
<i>Kumiko Tadano, Masahiro Kawato, Ryo Furukawa, Fumio Machida and Yoshiharu Maeno</i>		
19		
A Visualization System for Analyzing Information Leakage		269
<i>Yuki Nakayama, Seiji Shibaguchi and Kenichi Okada</i>		

PART VI FORENSIC TOOLS

20		
Forensic Analysis of Popular Chinese Internet Applications		285
<i>Ying Yang, Kam-Pui Chow, Lucas Hui, Chunxiao Wang, Lijuan Chen, Zhenya Chen and Jenny Chen</i>		
21		
Data Recovery Function Testing for Digital Forensic Tools		297
<i>Yinghua Guo and Jill Slay</i>		

Advances in Digital Forensics VI

Sixth IFIP WG 11.9 International Conference on Digital
Forensics, Hong Kong, China, January 4-6, 2010,

Revised Selected Papers

Chow, K.-P.; Shenoi, S. (Eds.)

2010, XVIII, 311 p., Hardcover

ISBN: 978-3-642-15505-5