

Contents

Contributing Authors	ix
Preface	xvii
PART I THEMES AND ISSUES	
1	
Establishing Findings in Digital Forensic Examinations: A Case Study Method	3
<i>Oluwasayo Oyelami and Martin Olivier</i>	
2	
A Model for Digital Evidence Admissibility Assessment	23
<i>Albert Antwi-Boasiako and Hein Venter</i>	
PART II MOBILE AND EMBEDDED DEVICE FORENSICS	
3	
Evaluating the Authenticity of Smartphone Evidence	41
<i>Heloise Pieterse, Martin Olivier and Renier van Heerden</i>	
4	
Forensic Evaluation of an Amazon Fire TV Stick	63
<i>Logan Morrison, Huw Read, Konstantinos Xynos and Iain Sutherland</i>	
5	
Detecting Anomalous Programmable Logic Controller Events Using Machine Learning	81
<i>Ken Yau and Kam-Pui Chow</i>	
PART III NETWORK AND CLOUD FORENSICS	
6	
A Forensic Methodology for Software-Defined Network Switches	97
<i>Tommy Chin and Kaiqi Xiong</i>	

7

- Identifying Evidence for Cloud Forensic Analysis 111
Changwei Liu, Anoop Singhal and Duminda Wijesekera

PART IV THREAT DETECTION AND MITIGATION

8

- Digital Forensic Implications of Collusion Attacks on the Lightning Network 133
Dmytro Piatkivskyi, Stefan Axelsson and Mariusz Nowostawski

9

- Insider Threat Detection Using Time-Series-Based Raw Disk Forensic Analysis 149
Nicole Beebe, Lishu Liu and Zi Ye

10

- Anti-Forensic Threat Modeling 169
Bruno Hoelz and Marcelo Maues

PART V MALWARE FORENSICS

11

- A Behavior-Based Approach for Malware Detection 187
Rayan Mosli, Rui Li, Bo Yuan and Yin Pan

12

- Categorizing Mobile Device Malware Based on System Side-Effects 203
Zachary Grimmer, Jason Staggs and Sujeet Shenoi

PART VI IMAGE FORENSICS

13

- Semantic Video Carving Using Perceptual Hashing and Optical Flow 223
Junbin Fang, Sijin Li, Guikai Xi, Zoe Jiang, Siu-Ming Yiu, Liyang Yu, Xuan Wang, Qi Han and Qiong Li

14

- Detecting Fraudulent Bank Checks 245
Saheb Chhabra, Garima Gupta, Monika Gupta and Gaurav Gupta

PART VII FORENSIC TECHNIQUES

15

Automated Collection and Correlation of File Provenance Information 269
Ryan Good and Gilbert Peterson

16

Using Personal Information in Targeted Grammar-Based Probabilistic Password Attacks 285
Shiva Houshmand and Sudhir Aggarwal

Advances in Digital Forensics XIII
13th IFIP WG 11.9 International Conference, Orlando,
FL, USA, January 30 - February 1, 2017, Revised
Selected Papers
Peterson, G.L.; Shenoi, S. (Eds.)
2017, XVIII, 303 p. 98 illus., Hardcover
ISBN: 978-3-319-67207-6