Contents

Contributing Authors ix
Preface xvii

PART I THEMES AND ISSUES

1 Establishing Findings in Digital Forensic Examinations: A Case Study Method 3
   Oluwasayo Oyelami and Martin Olivier

2 A Model for Digital Evidence Admissibility Assessment 23
   Albert Antwi-Boasiako and Hein Venter

PART II MOBILE AND EMBEDDED DEVICE FORENSICS

3 Evaluating the Authenticity of Smartphone Evidence 41
   Heloise Pieterse, Martin Olivier and Renier van Heerden

4 Forensic Evaluation of an Amazon Fire TV Stick 63
   Logan Morrison, Huw Read, Konstantinos Xynos and Iain Sutherland

5 Detecting Anomalous Programmable Logic Controller Events Using Machine Learning 81
   Ken Yau and Kam-Pui Chow

PART III NETWORK AND CLOUD FORENSICS

6 A Forensic Methodology for Software-Defined Network Switches 97
   Tommy Chin and Kaiqi Xiong
Identifying Evidence for Cloud Forensic Analysis

Changwei Liu, Anoop Singhal and Duminda Wijesekera

PART IV  THREAT DETECTION AND MITIGATION

Digital Forensic Implications of Collusion Attacks on the Lightning Network

Dmytro Piatkivskyi, Stefan Axelsson and Mariusz Nowostawski

Insider Threat Detection Using Time-Series-Based Raw Disk Forensic Analysis

Nicole Beebe, Lishu Liu and Zi Ye

Anti-Forensic Threat Modeling

Bruno Hoelz and Marcelo Maues

PART V  MALWARE FORENSICS

A Behavior-Based Approach for Malware Detection

Rayan Mosli, Rui Li, Bo Yuan and Yin Pan

Categorizing Mobile Device Malware Based on System Side-Effects

Zachary Grimmett, Jason Staggs and Sujeet Shenoi

PART VI  IMAGE FORENSICS

Semantic Video Carving Using Perceptual Hashing and Optical Flow

Junbin Fang, Sijin Li, Guikai Xi, Zoe Jiang, Siu-Ming Yiu, Liyang Yu, Xuan Wang, Qi Han and Qiong Li

Detecting Fraudulent Bank Checks

Saheb Chhabra, Garima Gupta, Monika Gupta and Gaurav Gupta
## Contents

**PART VII FORENSIC TECHNIQUES**

15
Automated Collection and Correlation of File Provenance Information
*Ryan Good and Gilbert Peterson*

16
Using Personal Information in Targeted Grammar-Based Probabilistic Password Attacks
*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.; Shenoi, S. (Eds.)
2017, XVIII, 303 p. 98 illus., Hardcover
ISBN: 978-3-319-67207-6