Contents

Malware and Botnet

FindEvasion: An Effective Environment-Sensitive Malware Detection System for the Cloud. ......................................................... 3
   Xiaoqi Jia, Guangzhe Zhou, Qingjia Huang, Weijuan Zhang,
   and Donghai Tian

Real-Time Forensics Through Endpoint Visibility ........................... 18
   Peter Kieseberg, Sebastian Neuner, Sebastian Schrittwieser,
   Martin Schmiedecker, and Edgar Weippl

On Locky Ransomware, Al Capone and Brexit ............................. 33
   John MacRae and Virginia N. L. Franqueira

Deanonymization

Finding and Rating Personal Names on Drives for Forensic Needs ....... 49
   Neil C. Rowe

A Web-Based Mouse Dynamics Visualization Tool for User Attribution
in Digital Forensic Readiness ..................................................... 64
   Dominik Ernsberger, R. Adeyemi Ikuesan, S. Hein Venter,
   and Alf Zugenmaier

Digital Forensics Tools I

Open Source Forensics for a Multi-platform Drone System ............... 83
   Thomas Edward Allen Barton and M. A. Hannan Bin Azhar

A Novel File Carving Algorithm for EVTX Logs ............................ 97
   Ming Xu, Jinkai Sun, Ning Zheng, Tong Qiao, Yiming Wu,
   Kai Shi, Haidong Ge, and Tao Yang

Fuzzy System-Based Suspicious Pattern Detection in Mobile
Forensic Evidence ......................................................................... 106
   Konstantia Barmpatsalou, Tiago Cruz, Edmundo Monteiro,
   and Paulo Simoes
Cyber Crime Investigation and Digital Forensics Triage

Digital Forensic Readiness in Critical Infrastructures: A Case of Substation Automation in the Power Sector ........................................ 117
Asif Iqbal, Mathias Ekstedt, and Hanan Alobaidli

A Visualization Scheme for Network Forensics Based on Attribute Oriented Induction Based Frequent Item Mining and Hyper Graph ....... 130
Jianguo Jiang, Jiuming Chen, Kim-Kwang Raymond Choo, Chao Liu, Kunying Liu, and Min Yu

Expediting MRSH-v2 Approximate Matching with Hierarchical Bloom Filter Trees ......................................................... 144
David Lillis, Frank Breitinger, and Mark Scanlon

Approxi: A Fast, Robust, Lightweight and Approximate Disassembler Considered in the Field of Memory Forensics ............... 158
Lorenz Liebler and Harald Baier

Digital Forensics Tools Testing and Validation

Memory Forensics and the Macintosh OS X Operating System ............. 175
Charles B. Leopard, Neil C. Rowe, and Michael R. McCarrin

Sketch-Based Modeling and Immersive Display Techniques for Indoor Crime Scene Presentation ........................................ 181
Pu Ren, Mingquan Zhou, Jin Liu, Yachun Fan, Wenshuo Zhao, and Wuyang Shui

An Overview of the Usage of Default Passwords ............................ 195
Brandon Knieriem, Xiaolu Zhang, Philip Levine, Frank Breitinger, and Ibrahim Baggili

Hacking

Automation of MitM Attack on Wi-Fi Networks ............................ 207
Martin Vondráček, Jan Pluskal, and Ondřej Ryšavý

SeEagle: Semantic-Enhanced Anomaly Detection for Securing Eagle .... 221
Wu Xin, Qingni Shen, Yahui Yang, and Zhonghai Wu

Coriander: A Toolset for Generating Realistic Android Digital Evidence Datasets .......................................................... 228
Irvin Homem

Author Index ........................................................................ 235