

Contents

Malware and Botnet

FindEvasion: An Effective Environment-Sensitive Malware Detection System for the Cloud.	3
<i>Xiaoqi Jia, Guangzhe Zhou, Qingjia Huang, Weijuan Zhang, and Donghai Tian</i>	
Real-Time Forensics Through Endpoint Visibility	18
<i>Peter Kieseberg, Sebastian Neuner, Sebastian Schrittwieser, Martin Schmiedecker, and Edgar Weippl</i>	
On Locky Ransomware, Al Capone and Brexit.	33
<i>John MacRae and Virginia N. L. Franqueira</i>	

Deanonymization

Finding and Rating Personal Names on Drives for Forensic Needs	49
<i>Neil C. Rowe</i>	
A Web-Based Mouse Dynamics Visualization Tool for User Attribution in Digital Forensic Readiness	64
<i>Dominik Ernsberger, R. Adeyemi Ikuesan, S. Hein Venter, and Alf Zugenmaier</i>	

Digital Forensics Tools I

Open Source Forensics for a Multi-platform Drone System	83
<i>Thomas Edward Allen Barton and M. A. Hannan Bin Azhar</i>	
A Novel File Carving Algorithm for EVTX Logs	97
<i>Ming Xu, Jinkai Sun, Ning Zheng, Tong Qiao, Yiming Wu, Kai Shi, Haidong Ge, and Tao Yang</i>	
Fuzzy System-Based Suspicious Pattern Detection in Mobile Forensic Evidence	106
<i>Konstantia Barmapsalou, Tiago Cruz, Edmundo Monteiro, and Paulo Simoes</i>	

Cyber Crime Investigation and Digital Forensics Triage

Digital Forensic Readiness in Critical Infrastructures: A Case of Substation Automation in the Power Sector	117
<i>Asif Iqbal, Mathias Ekstedt, and Hanan Alobaidli</i>	
A Visualization Scheme for Network Forensics Based on Attribute Oriented Induction Based Frequent Item Mining and Hyper Graph	130
<i>Jianguo Jiang, Jiuming Chen, Kim-Kwang Raymond Choo, Chao Liu, Kunying Liu, and Min Yu</i>	
Expediting MRSH- \forall 2 Approximate Matching with Hierarchical Bloom Filter Trees	144
<i>David Lillis, Frank Breitingner, and Mark Scanlon</i>	
Approxis: A Fast, Robust, Lightweight and Approximate Disassembler Considered in the Field of Memory Forensics	158
<i>Lorenz Liebler and Harald Baier</i>	

Digital Forensics Tools Testing and Validation

Memory Forensics and the Macintosh OS X Operating System.	175
<i>Charles B. Leopard, Neil C. Rowe, and Michael R. McCarrin</i>	
Sketch-Based Modeling and Immersive Display Techniques for Indoor Crime Scene Presentation.	181
<i>Pu Ren, Mingquan Zhou, Jin Liu, Yachun Fan, Wenshuo Zhao, and Wuyang Shui</i>	
An Overview of the Usage of Default Passwords	195
<i>Brandon Knieriem, Xiaolu Zhang, Philip Levine, Frank Breitingner, and Ibrahim Baggili</i>	

Hacking

Automation of MitM Attack on Wi-Fi Networks.	207
<i>Martin Vondráček, Jan Pluskal, and Ondřej Ryšavý</i>	
SeEagle: Semantic-Enhanced Anomaly Detection for Securing Eagle.	221
<i>Wu Xin, Qingni Shen, Yahui Yang, and Zhonghai Wu</i>	
Coriander: A Toolset for Generating Realistic Android Digital Evidence Datasets	228
<i>Irvin Homem</i>	

Author Index	235
-------------------------------	-----

Digital Forensics and Cyber Crime

9th International Conference, ICDF2C 2017, Prague,

Czech Republic, October 9-11, 2017, Proceedings

Matoušek, P.; Schmiedecker, M. (Eds.)

2018, X, 235 p. 83 illus., Softcover

ISBN: 978-3-319-73696-9