Innovations in Digital Forensics
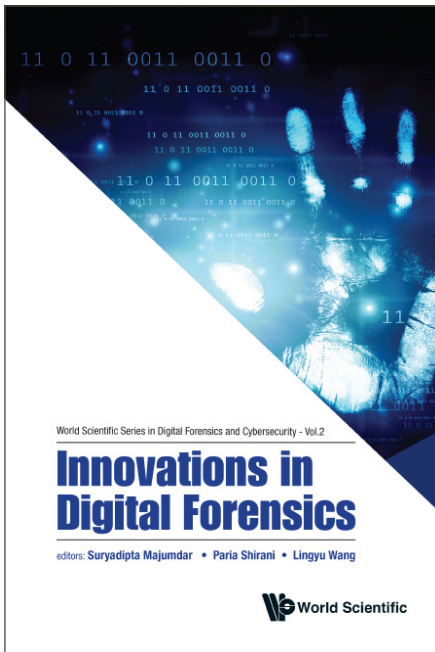
Edited By Suryadipta Majumdar
(*Concordia University, Canada*)

Paria Shirani
(*University of Ottawa, Canada*)

Lingyu Wang
(*Concordia University, Canada*)

ABOUT THE BOOK

Digital forensics deals with the investigation of cybercrimes. With the growing deployment of cloud computing, mobile computing, and digital banking on the internet, the nature of digital forensics has evolved in recent years, and will continue to do so in the near future.

This book presents state-of-the-art techniques to address imminent challenges in digital forensics. In particular, it focuses on cloud forensics, Internet-of-Things (IoT) forensics, and network forensics, elaborating on innovative techniques, including algorithms, implementation details and performance analysis, to demonstrate their practicality and efficacy. The innovations presented in this volume are designed to help various stakeholders with the state-of-the-art digital forensics techniques to understand the real world problems. Lastly, the book will answer the following questions: How do the innovations in digital forensics evolve with the emerging technologies? What are the newest challenges in the field of digital forensics?

READERSHIP

Law enforcement agencies involved with digital forensics, industry practitioners in digital forensics, academic and industry researchers in cybersecurity and forensics, undergraduate and graduate students majoring in digital forensics and cybersecurity.

CONTENTS

- Introduction
- Current Challenges in Digital Forensics
- Digital Evidence Collection in IoT Environment
- Optimizing IoT Device Fingerprinting using Machine Learning
- Evaluating Deleted File Recovery Tools per NIST

- Forensic Data Analytics for Anomaly Detection in Evolving Networks
- On Offloading Network Forensic Analytics to Programmable Data Plane Switches
- An Event-Driven Forensic Auditing Framework for Clouds
- A Multi-Level Proactive Security Auditing Framework for Clouds Through Automated Dependency Building
- Conclusion

ABOUT THE EDITORS

Suryadipta Majumdar is an Assistant Professor at the Concordia Institute for Information Systems Engineering (CIISE), Concordia University, Montreal, Canada. He is involved in the Concordia Information Security Research (CISR) Lab and NSERC/Ericsson IRC in Software Defined Networking (SDN)/Network Functions Virtualization (NFV) Security Program. Previously, Suryadipta was an assistant professor at the Information Security and Digital Forensics department at State University of New York (SUNY), Albany. During his PhD, he was a National Sciences and Engineering Research Council (NSERC) Canada Graduate Scholar at Concordia University. He finished his MASc in Information Systems Security from Concordia University and his BSc in Computer Science and Engineering from Bangladesh University of Engineering and Technology (BUET). His research interests are mainly in different topics of cybersecurity and forensics, such as cloud computing security, Internet-of-Things (IoT) security, network security, and IoT forensics.

Paria Shirani is an assistant professor at the School of Electrical Engineering and Computer Science at University of Ottawa in Canada. Prior to joining the University of Ottawa, she was an assistant professor at the Department of Computer Science at Toronto Metropolitan University. Previously, she was a National Sciences and Engineering Research Council (NSERC) postdoctoral fellow at Carnegie Mellon University (CMU), USA. Paria Shirani earned her PhD degree in information systems engineering at Concordia University, during which she was awarded a *Fonds de recherche du Québec — Nature et technologies* (FRQNT) doctoral scholarship. Her research interests are mainly in the fields of cybersecurity, such as binary code and malware analysis, IoT security, vulnerability detection, and cyberthreat intelligence generation.

Lingyu Wang is a Professor at the Concordia Institute for Information Systems Engineering (CIISE) at Concordia University, Montreal, Canada. He holds the National Sciences and Engineering Research Council (NSERC)/Ericsson Senior Industrial Research Chair in SDN/NFV Security. He received his PhD degree in Information Technology in 2006 from George Mason University. His research interests include cloud computing security, SDN/NFV security, security metrics, software security, and privacy. He has co-authored five books, two patents, and over 120 refereed conference and journal articles at reputable venues including ACM Transactions on Privacy and Security (TOPS), IEEE Transactions on Information Forensics and Security (TIFS), IEEE Transactions on Dependable and Secure Computing (TDSC), Journal of Computer Security, IEEE Transactions on Mobile Computing (TMC), IEEE Symposium on Security and Privacy (S&P), ACM Conference on Computer and Communications Security (CCS), Network and Distributed System Security Symposium (NDSS), European Symposium on Research in Computer Security (ESORICS), International Conference on Database Theory (ICDT), etc.