The Increasing Importance of Digital Forensics and Investigations in Law Enforcement, Government and Commercial Sectors

Nhien-An Le-Khac and Kim-Kwang Raymond Choo

Abstract Digital forensics and investigations play an increasingly important role in a broad range of scenarios, such as those in pandemics (e.g. COVID-19 contact tracing), criminal cases, civil litigations, and national security cases. In this book, the editors documented their education and research activities with students enrolled in the Master of Science (MSc) in Forensic Computing and Cybercrime Investigation program at University College Dublin, Ireland, who are also from the law enforcement and government community in Canada, Ireland, Germany, The Netherlands, and United Kingdom. Collaboratively, the authors focused on topics ranging from Internet of Things (IoT) malware analysis, IoT testbed setup, malware analysis (e.g. ransomware), CCTV forensics, financial investigations (e.g. PayPal accounts and Bitcoins), cloud forensics, and network and ToR forensics.

Keywords Digital forensics · Digital investigations · Criminal investigations · Civil litigations · National security investigations

1 Introduction

The twenty-first century has seen significant advances in information and communications technologies (ICT) that were, perhaps, considered science fiction a decade or two ago. ICT now pervades many aspects of society today, and the number and range of digital device users are rapidly increasing. For example, if we take a stroll down a street in any city/country, we would likely encounter a broad range of digital devices, such as IP-based closed-circuit televisions (CCTVs), some Internet of Things (IoT) devices (e.g. temperature sensors, and remote terminal units—RTUs), autonomous vehicles, mobile devices (e.g. Android and iOS phones), as well as ICT that are embedded in human bodies such as Internet of Medical Things (IoMT; or

N.-A. Le-Khac (✉)
University College Dublin, Dublin, Ireland
e-mail: an.lekhac@ucd.ie

K.-K. R. Choo
University of Texas at San Antonio, San Antonio, TX, USA

© The Editor(s) (if applicable) and The Author(s), under exclusive license to Springer Nature Switzerland AG 2020
N.-A. Le-Khac and K.-K. R. Choo (eds.), Cyber and Digital Forensic Investigations, Studies in Big Data 74, https://doi.org/10.1007/978-3-030-47131-6_1
known as embedded medical devices). Increasingly, IoT devices are also found in military and battlefield settings (e.g. Internet of Military/Battlefield Things).

There are, however, implications with the increased digitalisation of our society. For example, such devices can be the target of cybercriminals and those with malicious intent. This reinforces the importance of law enforcement investigators, including those that are tasked with physical/conventional crime investigations (e.g. murder, drug trafficking, money laundering and terrorism financing), to keep pace with ICT advances, understand the role of technologies in their investigations, understand the type and range of forensic/evidential artefacts that could be obtained from such devices, and how to go about data acquisition in a forensically sound manner.

Digital forensics (DF) and digital investigations (DI) are not restricted to only law enforcement matters, as the use of ICTs is also prevalent in commercial and national security settings. In other words, DF and DI play a role in civil litigations and national security investigations, such as those involving nation states (e.g. espionage), or cyber warfare like activities (e.g. corrupting supply chains to inject hardware Trojans). They may also play a role in pandemics, such as COVID–19 contact tracing. Hence, there is also a need for ongoing education and research in DF and DI, involving and targeting a broad range of stakeholders.

In this book, both editors of this book documented their education and research activities with one such stakeholder group, namely: law enforcement and government community. The lead authors of the next ten chapters (i.e. Chaps. “Defending IoT Devices from Malware” to “The Bitcoin-Network Protocol from a Forensic Perspective”) are law enforcement and government employees who are also enrolled in the Master of Science (MSc) in Forensic Computing and Cybercrime Investigation program at University College Dublin, Ireland, collaborated with both editors¹ and other researchers on a broad range of topics, described in the next section.

## 2 Organisation of This Book

Chapters “Defending IoT Devices from Malware” and “Digital Forensic Investigation of Internet of Thing Devices: A Proposed Model and Case Studies”, respectively led by William O’Sullivan (Irish Defence Forces, Ireland) and Alexander Hilgenberg (State police in Lower Saxony, Germany), focus on IoT device forensics. In Chap. “Defending IoT Devices from Malware”, the authors examined two popular IoT malware, namely: Mirai and Qbot, and proposed mitigation and detection strategies based on their analysis. In Chap. “Digital Forensic Investigation of Internet of Thing Devices: A Proposed Model and Case Studies”, the authors explained how one can set up an IoT testbed/laboratory for training of future forensic investigators.

Chapter “Forensic Investigation of Ransomware Activities—Part 1”, led by Young (Irish Defense Force, Ireland) and in collaboration with McArdle (Trend Micro Ltd.,

¹Nhien-An Le-Khac is the Director of the MSc in Forensic Computing and Cybercrime Investigation program, and Kim-Kwang Raymond Choo is the external examiner of the program.
Ireland) and both editors, focuses on ransomware analysis. Similarly, Chap. “Forensic Investigation of Ransomware Activities—Part 2” led by Boyton (Irish Defence Forces, Ireland) focuses on ransomware forensics.

CCTVs are found not only in public places (e.g. streets and public transportation venues), but also at private homes and offices. Hence, they are a potential source of evidence (e.g. video recordings). However, the variety of CCTV systems and the significant volume of data that can potentially be extracted from CCTV video can be challenging for forensic examiners. Chapter “CCTV Forensics in the Big Data Era: Challenges and Approaches”, authored by Gomm (Garda Síochana Ombudsman Commission, Ireland), Brooks (Avon and Somerset Constabulary, UK), and Hew (Royal Canadian Mounted Police, Canada) in collaboration with both editors, focuses on CCTV forensics.

In Chap. “Forensic Investigation of PayPal Accounts”, Standare (German Police, Germany) collaborated with Hayes (Pace University, USA) and both editors to study financial fraud investigation, using PayPal as a case study.

Cloud forensics is the focus of Chap. “Digital Forensic Approaches for Cloud Service Models: A Survey” led by Schlepphorst (Federal Office for Information Security, Germany), where we give an overview of digital forensic approaches for different cloud service models.

The forensic investigation of mobile networks is always a challenge for law enforcement due to their ad hoc nature, hence in Chap. “Long Term Evolution Network Security and Real-Time Data Extraction” led by Redmond (Deloitte LLP Ireland, also a former member of Irish National Cyber Security Centre) we describe the security issues of LTE and GSM networks as well as how to extract artefacts from these networks.

Chapter “Towards an Automated Process to Categorise Tor’s Hidden Services”, led by Kinder (National Crime Agency, UK), examines at how ToR hidden services are set up, and presents an approach to successfully identify criminal sites without manual interaction. Finally, Chap. “The Bitcoin-Network Protocol from a Forensic Perspective”, led by Veldhuizen (Team High Tech Crime, Dutch National Police, The Netherlands), forensically examines the Bitcoin-network protocol.

Nhien-An Le-Khac is a lecturer at the School of Computer Science (CS), University College Dublin (UCD), Ireland. He is currently the program director of MSc program in Forensic Computing and Cybercrime Investigation (FCCI)—an international program for the law enforcement officers specializing in cybercrime investigations. He is also the co-founder of UCD-GNECB Postgraduate Certificate in fraud and e-crime investigation. Since 2008, he is a research fellow in Citibank, Ireland (Citi). He obtained his Ph.D. in Computer Science in 2006 at the Institut National Polytechnique de Grenoble (INPG), France. His research interest spans the area of Cybersecurity and Digital Forensics, Data Mining/Distributed Data Mining for Security, and Fraud and Criminal Detection. Since 2013, he has collaborated on many research projects as a principal/co-PI/funded investigator. He has published more than 150 scientific papers in peer-reviewed journal and conferences in related research fields, and his recent edited book has been listed the Best New Digital Forensics Book according to the Book Authority.
Kim-Kwang Raymond Choo received the Ph.D. in Information Security in 2006 from the Queensland University of Technology, Australia. He currently holds the Cloud Technology Endowed Professorship at the University of Texas at San Antonio (UTSA). In 2015, he and his team won the Digital Forensics Research Challenge organized by the Germany’s University of Erlangen-Nuremberg. He is the recipient of the 2019 IEEE Technical Committee on Scalable Computing (TCSC) Award for Excellence in Scalable Computing (Middle Career Researcher), 2018 UTSA College of Business Col. Jean Piccione and Lt. Col. Philip Piccione Endowed Research Award for Tenured Faculty, British Computer Society’s 2019 Wilkes Award Runner-up, 2019 EURASIP Journal on Wireless Communications and Networking (JWCN) Best Paper Award, Korea Information Processing Society’s Journal of Information Processing Systems (JIPS) Survey Paper Award (Gold) 2019, IEEE Blockchain 2019 Outstanding Paper Award, Inscrypt 2019 Best Student Paper Award, IEEE TrustCom 2018 Best Paper Award, ESORICS 2015 Best Research Paper Award, 2014 Highly Commended Award by the Australia New Zealand Policing Advisory Agency, Fulbright Scholarship in 2009, 2008 Australia Day Achievement Medalion, and British Computer Society’s Wilkes Award in 2008. He is also a fellow of the Australian Computer Society, an IEEE senior member, and co-chair of IEEE Multimedia Communications Technical Committee’s Digital Rights Management for Multimedia Interest Group.