Preface

That life-changing moment looked like a pure coincidence. It was an ordinary evening in Dublin in 2009, and I was flipping through *Newsweek* and came across an article on cloud computing. After reading all the controversies and debates over the emergence of cloud adoption, I suddenly realized that I discovered a perfect research topic for my PhD. All of the sudden, I was so excited by that gigantic question mark over my head—how to investigate cyber crime and past incidents in the Cloud?—that I immediately started writing down all the interesting questions I could think of regarding digital investigation in the Cloud. Back in 2009, nobody seemed to have ever thought about these questions and their significant implications at all, and when I wrote down the term "Cloud Forensics" in the center of the question sheet, I was totally intrigued by a fascinating space of unknown. From that moment, I embarked on the bittersweet journey of trying to answer these questions.

This book is a collective brainchild from this process. With rapid global cloud adoption, cloud-computing environment is inevitably becoming a new battlefield for the evolving threat landscape as well as cyber crime. Cloud forensics, i.e., digital investigation in cloud computing environments, is a relatively green area that is rapidly emerging. This book is the world's first scholarly volume explicitly on the topic of cloud forensics. It is intended to collect different perspectives from both industry and academia on various challenges and possible solutions for carrying out cloud investigations, and I hope it will serve as a good reference book for digital forensic and cloud security researchers, practitioners, and professionals, who wish to carry out research and developments in the emerging area of cloud forensics.

This book opens with an introductory chapter on the background of cloud computing and digital investigation by my colleagues, Joshua James, Ahmed Shosha, and Dr. Pavel Gladyshev, at the Center for Cybersecurity and Cybercrime Investigation, University College Dublin. This chapter provides a comprehensive overview and literature review on the history and state-of-the-art of cloud computing and digital investigation in order to give readers adequate background knowledge on the subject matter.

In chapter 2, Mark Crosbie, security architect and head of the ethical hacking team at IBM Ireland and the CIO Office, introduces the evolving attack surface of cloud environments, where to look for potential evidence, and how digital investigators should think like a hacker.

The inventor of the first computer virus, Dr. Fred Cohen, gives an in-depth analysis of the challenges to digital forensic evidence throughout the evidence life cycle in the Cloud in chapter 3.

In chapter 4, Richard Adams, based on his vast experience from real-world investigations as the Principle in the Forensic Division of a Big4 professional services organization, argues why cloud-based storage demands a new digital forensic process model.

The next part of the book addresses various specific issues relevant to the investigation process in cloud computing environments, from forensic readiness in chapter 5 by Ferguson-Boucher and Endicott-

Popovsky, virtual forensics in chapter 6 by Prof. Diane Barrett, search and seizure in chapter 7 by Josiah Dykstra, to a foundational piece of comprehensive analysis on legal process and requirements for cloud investigations by Ivan Orton, Aaron Alva, and Endicott-Popovsky in chapter 8, followed by chapter 9 on eDisovery in the Cloud written by Dean Gonsowski, eDiscovery council at Symantec, and chapter 10 on data recovery strategies by Theodoros Spyridopoulos and Prof. Vasilios Katos.

Cloud computing poses significant challenges to digital investigation; however, it also brings a unique opportunity for groundbreaking novel approaches to address these challenges. The next part of the book is dedicated to Forensics as a Service. In chapters 11, 12, and 13, Jon Rav Gagan Shende, Dener, and Prof. Ruy J. G. B. de Queiroz from Brazil, Fabio, Dr. Simone Tacconi, and Prof. Giuseppe F. Italiano from Italy present three different models for delivering Forensics as a Service via cloud computing.

To leave the readers with a bit of optimism into the future, despite all the pressing cloud forensic challenges presented, this book concludes with my chapter on designing a forensic-enabling cloud ecosystem. Cloud computing is a major paradigm shift in the history of computing, and it is here to stay. The full impact of cloud computing is estimated to be about three years away (Forbes, 2012), and we are at a unique time to integrate forensic requirements, controls, and implementations into the cloud ecosystem in order to enable post-incident investigations and enhance the overall robustness of our cyber infrastructure.

Today, I am still on the journey of answering those questions I wrote down on that 2009 evening in Dublin, and I am happy that you are now joining this journey. I hope you will enjoy reading this book.

Keyun Ruan
University College Dublin, Ireland October 2012

REFERENCES

BBC. (2011, June 13). New Zealand quake: Christchurch hit by aftershocks. *BBC News*. Retrieved from http://www.bbc.co.uk/news/world-asia-pacific-13745359

Forbes. (2012, October 3). Cloud's full impact is still about three years away. *Forbes*. Retrieved from http://www.forbes.com/sites/joemckendrick/2012/10/03/clouds-full-impact-is-still-about-three-years-away-survey-predicts/

New York Times. (2012). Egypt news – Revolution and aftermath. *New York Times*. Retrieved from http://topics.nytimes.com/top/news/international/countriesandterritories/egypt/index.html

Slate. (2012, July 4). Power outages dampen July 4 parties. *Slate*. Retrieved from http://slatest.slate.com/posts/2012/06/30/washington_d_c_maryland_virginia_derecho_storm_leaves_2_mil_without_power_kills_4_.html