

# Preface

With approximately 40 % of the world's population now connected to the Internet, many people have unprecedented access to education, commerce, and cultural exchange. As new technologies allow more people to connect, these opportunities will continue to grow well into the future. However, the same opportunities that allow legitimate businesses to reach new customers online also allow opportunities for cyber criminals to perpetrate large-scale fraud, intrusions, and data theft.

Beyond what could be considered traditional cybercrime, the actors, and their motivations, are changing. Perpetrators of cybercrime are increasingly organized and global. Governments are investing heavily in military-grade cyber-offensive and defensive capabilities. Unfortunately, average businesses and Internet users are still largely unaware of the potential dangers of cyber crime and how to protect themselves. Governments are still largely uncooperative and ineffectual during the majority of international cyber crime investigation requests, and some countries still lack legislation on cyber crime.

While progress is being made in national investigation capacities, cyber criminals are taking advantage of the weak cooperation between countries. Unsecured infrastructure and poor policies allow civilian and government infrastructure to become part of criminal organizations' or foreign military assets.

Indeed, improved information security and cyber crime investigation education is needed, as well as a better understanding of such crimes, refined investigation techniques, and an increase in global cooperation from all stakeholders.

In an attempt to raise awareness and improve cultural understanding and international cooperation in cyber crime investigations, the 7th International ICST Conference on Digital Forensics and Cyber Crime (ICDF2C 2015) was held in Seoul, Republic of Korea; the first time ICDF2C was hosted in Asia.

This volume contains papers presented at ICDF2C 2015, held October 6–8, 2015 in Seoul, Republic of Korea. Unlike other conferences in the field of digital forensics, ICDF2C focuses on the applications of digital forensic research, providing a forum where practitioners can learn how the latest research results can be used in everyday investigations of cyber crimes and corporate misconduct.

The 14 papers and three abstracts contained in this volume cover a variety of topics ranging from tactics of cyber crime investigations to digital forensic education, network forensics, and international cooperation in digital investigations. Each paper was reviewed in a double-blind peer review process. We sincerely thank the Technical Program Committee for their hard work in reviewing the submissions. We thank the Organizing Committee, Sang-Jin Lee, Pavel Gladyshev, Frank Breitinger, Yunsik “Jake” Jang, Taeshik Shon, Kisik Chang, YooJin Kwon, Young-jin Son, Songmin Lee, Jae Hyeok Bang, and Boyoung Lim, as well as ASCO, the Korean National Police, the Korean Digital Forensics Society, and the Seoul Tech Society for their tireless efforts in

managing all of the arrangements required for a successful conference. We would also like to thank JETCO and DUZON for sponsoring the event. Finally, we offer special thanks to all the staff at EAI who made this conference possible.

August 2015

Joshua I. James  
Frank Breiting

Digital Forensics and Cyber Crime

7th International Conference, ICDF2C 2015, Seoul,  
South Korea, October 6-8, 2015. Revised Selected  
Papers

James, J.I.; Breitinger, F. (Eds.)

2015, X, 217 p. 57 illus. in color., Softcover

ISBN: 978-3-319-25511-8