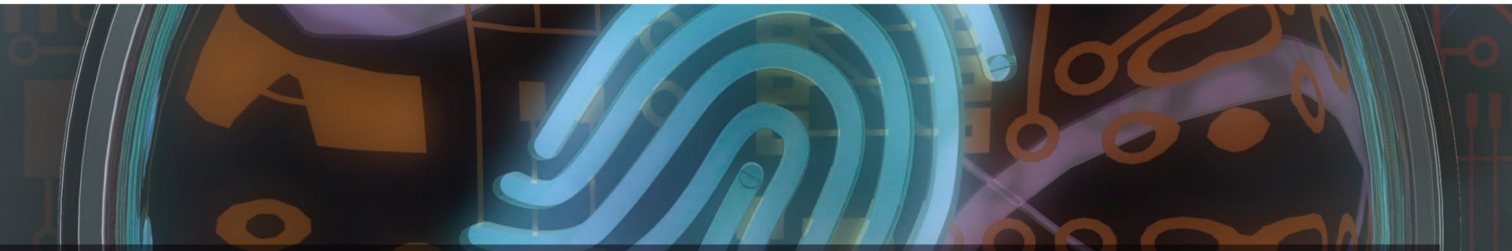

Recent Advancements in Digital Forensics, Part 2

Wojciech Mazurczyk | Warsaw University of Technology
Luca Caviglione | National Research Council of Italy
Steffen Wendzel | Worms University of Applied Sciences

Today, digital forensics experts must operate in a multidisciplinary environment that requires mastery of many disciplines, including law, computer science, finance, networking, data mining, and criminal justice. Meanwhile, cybercriminal activities often compel law-enforcement agencies to investigate across international borders, which means dealing with different jurisdictions and legal systems. Also, computing and networking infrastructures are increasingly intricate, further complicating investigations and activities related to digital forensics. For instance, clues pointing to illegal digital activities are often buried in large volumes of data, making criminal activity that much more difficult to detect and document with suitable evidence.

Thus, the field of digital forensics faces many diverse challenges and issues in the effort to streamline digital evidence processing and related forensic procedures. A paradigm shift is needed for law-enforcement agencies, and forensics professionals must be fully prepared to deal with different technologies, such as those related to the Internet of Things, cloud and fog computing, mobile devices, blockchain, and cryptocurrencies as well as smart buildings and even smart cities. To sum up: forensics experts, tools, and methodologies must all keep pace with new technologies.

This second part of a two-part special issue series of *IEEE Security & Privacy* covers the latest challenges that digital forensics experts face. We are impressed by the enthusiasm of our community in exploring these topics, and we are grateful that so many experts among us were willing to contribute to this issue. We received 42 submissions, of which 11 outstanding articles were accepted for publication (an acceptance rate of 26%). This second part presents six articles covering different emerging and important domains, such as cloud storage, PDF-based malware, and other challenges for digital investigation.

This issue starts with an article by Hui Tian et al., who address the problem of trusting cloud-service providers. The authors present an architecture for public data auditing to tackle this challenge. In the article by Apostolos Axenopoulos et al., the authors support digital forensics departments by providing a framework to assist investigators in their everyday tasks. Joseph Ricci et al., in their article discuss the problem from a forensics perspective of blockchain-based data storage that allows data to be placed in multiple geographic locations.

Digital Object Identifier 10.1109/MSEC.2019.2896857
Date of publication: 20 March 2019

In another article, Rodrigo Carvalho et al. explain and evaluate the hypothesis that semantic technologies could help us better understand malware campaigns. Meanwhile, Sherenaz Al-Haj Baddar et al. discuss, in the context of user privacy, a statistical detector for identifying behavioral anomalies among network nodes. Finally, Davide Maiorca and Battista Biggio summarize the current techniques used to convey PDF malware and discuss state-of-the-art tools for PDF malware analysis.

We thank all authors and reviewers for their contributions to this special issue. We hope you will enjoy this issue as well as its companion "Digital Forensics, Part 1," which was published in *IEEE Security & Privacy*'s November/December 2017 issue. ■

Wojciech Mazurczyk is an associate professor of cybersecurity at Warsaw University of Technology. Contact him at w.mazurczyk@tele.pw.edu.pl.

Luca Caviglione is a research scientist in information security and computer networks at the National Research Council of Italy, Institute for Applied Mathematics and Information Technologies. Contact him at luca.caviglione@cnr.it.

Steffen Wendzel is a professor of information security and computer networks at Worms University of Applied Sciences. Contact him at wendzel@hs-worms.de.

Digital Object Identifier 10.1109/MSEC.2019.2900869