Modern digital forensics must work in complex and fast-moving scenarios. The availability of cloud computing, smartphones and wearable devices, ubiquitous Internet access, and novel digital wallet services often lead to investigations spanning international borders. Moreover, the diffusion of Internet of Things (IoT) paradigms, especially in the Industry 4.0 fields, accounts for a new wave of crimes ranging from industrial espionage to attacks endangering individuals’ physical security. To make matters worse, malware and cyberthreats are increasingly equipped with sophisticated antiforensics techniques. Consequently, digital forensics experts are required to move across different jurisdictions and legal systems, and to search for digital activities or artifacts often buried in large volumes of data.

Digital forensics is expected to face new challenges in the near future. Needless to say, law enforcement agencies, academics, and security experts must be fully prepared to gather effective digital evidence and utilize digital forensics to combat the growing number of cybercrimes. Modern digital forensics is a multidisciplinary effort that embraces several fields, including law, computer science, finance, networking, data mining, and criminal justice. Professionals will increasingly face a mixed set of challenges and issues regarding the efficiency of digital evidence processing and related forensic procedures.

This special issue of *IEEE Security & Privacy* is an attempt to collect the most interesting ideas from the community of researchers and professionals working on digital forensics. We are very grateful to this community, especially for its vivacity and vast participation. In fact, we received 42 submissions, of which 11 outstanding articles were accepted for publication (an acceptance rate of 26 percent) and divided in two issues.
This first issue starts with our introductory article, “The Future of Digital Forensics: Challenges and the Road Ahead,” which provides an outlook on current and upcoming trends in the domain.

Programmable logic controllers (PLCs) are a core component of industrial control systems and have been a target of attacks in recent years. In the article “Programmable Logic Controller Forensics,” Irfan Ahmed and his colleagues show how forensics for PLCs can be achieved.

In “Botnet Fingerprinting: Anomaly Detection in SMTP Conversations,” Piotr Bazydlo and his colleagues propose a method for fingerprinting botnets and spam, applying anomaly detection based on the popular Simple Mail-Transfer Protocol (SMTP).

The work of Amarnath Gupta, Subhasis Dasgupta, and Aditya Bagchi, entitled “PROFORMA: Proactive Forensics with Message Analytics,” presents a system that applies forensics techniques for proactive prevention and that inspects the trustworthiness and risk of social communications.

Finally, Maxim Chernyshev and his colleagues summarize current developments and trends in mobile forensics in “Mobile Forensics: Advances, Challenges, and Research Opportunities.”

We hope you enjoy this issue as well as the forthcoming Digital Forensics, Part 2, which is scheduled for publication in January/February 2019.

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 National Research Council of Italy, Institute of Intelligent Systems for Automation. 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.