Editorial

Nikkel, B.; Geradts, Z.

DOI
10.1016/j.fsidi.2022.301487
Publication date
2022
Document Version
Final published version
Published in
Forensic Science International: Digital Investigation

Forensic Science International: Digital Investigation 42-43 (2022) 301487

Contents lists available at ScienceDirect

Forensic Science International: Digital Investigation

journal homepage: www.elsevier.com/locate/fsidi

Editorial

Editorial

Dear Readers,

This issue of Digital Investigation is a combined issue containing both volumes 42 and 43. Two dominant themes are present in this issue: IoT forensics and Crypto currency forensics. Both of these topics have attracted researchers in recent years, and the increase in submitted papers is expanding the body of knowledge in the digital forensic sciences. Emerging areas of scientific research often brings challenges with the peer review process, where fewer subject matter experts are available to provide reviews of papers. We have seen this shortage of peer reviewers with IoT and Crypto currency paper submissions in recent years. However, as the number of submissions increases, so does the number of authors available as potential peer reviewers. Authors and reviewers are encouraged to update their areas of expertise ("Personal Classifications") in Elsevier's Editorial Manager. Having accurate personal classifications makes it easier to identify relevant experts for the peer review process.

Forensic analysis related to crypto currencies is becoming an important research topic with Digital Investigation journal. Criminal services bought and sold in the underground economy are typically using crypto currencies to make payments or exchange value. In this issue, one paper augments traditional "follow the money" investigations with improved methods for tracking Bitcoin. Another paper addresses the forensic acquisition process, and presents a preservation methodology for crypto wallets.

Digital forensics related to the "Internet of Things" brings together multiple techniques to enable successful investigations. Hardware techniques such as chip-off support the extraction of data from IoT devices. The contents of local memory and persistent storage requires analysis and interpretation techniques. Network forensic techniques can be leveraged to analyze content and telemetry data transmitted to remote cloud servers. Multiple papers in this issue describe various aspects of IoT forensics, including hardware analysis, blockchain models, and an investigation framework.

Two papers in this issue highlight the use of artificial intelligence and neural networks for the purpose of detection in a forensic investigation context. One paper focuses on techniques for detecting and ranking pornographic material to assist in categorizing video content based on severity. Another paper describes a method for identifying deepfakes by exploiting inconsistencies in texture information.

The remaining papers provide improvements to methods and techniques of traditional digital forensic topics. One paper identifies file system forensic analysis tools and inconsistencies in the interpretation of timestamps. Another paper offers improvements to source detection of multimedia content through analysis of defects in optical sensors.

We hope the articles in this issue will be useful to digital forensic researchers and practitioners.

Bruce Nikkel, Zeno Geradts

https://doi.org/10.1016/j.fsidi.2022.301487