## Panoramic perspective of Digital Investigation

Casey, E.; Geradts, Z.; Nikkel, B.

**DOI**
10.1016/j.diin.2019.100886
**Publication date**
2019
**Document Version**
Final published version
**Published in**
Digital Investigation
**License**
Article 25fa Dutch Copyright Act (https://www.openaccess.nl/en/in-the-netherlands/you-share-we-take-care)
Link to publication

**Citation for published version (APA):**
Casey, E., Geradts, Z., & Nikkel, B. (2019). Panoramic perspective of Digital Investigation. *Digital Investigation*, *30*, 173. https://doi.org/10.1016/j.diin.2019.100886

Digital Investigation 30 (2019) 173

Contents lists available at ScienceDirect

Digital Investigation

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

Editorial

# Panoramic perspective of Digital Investigation

It is important to affirm the unique identity of this journal as we prepare to transition to *FSI Digital Investigation* (see Editorial in Volume 29).

From the beginning, this journal has had a unique combination of theory, practice, technology and law, delivering dynamic content that is directly applicable to emerging challenges. Many papers published here have influenced process models and effective practices, providing a firm foundation for digital forensics and incident response. These unique qualities of Digital Investigation will be enhanced by forensic science through closer alignment with Forensic Science International (FSI).

Over time, the number and variety of technical papers in Digital Investigation have increased along with spreading specializations, including forensic analysis of file systems, smartphones, IoT devices, networks, databases, memory, and malware. Digital Investigation has focused on preparation, survey, preservation, examination, analysis and interpretation of digital evidence, and shied away from detection (intrusion detection, forgery detection, malware detection, etc.). There have been recently more papers on forensic analysis of multimedia evidence, as well as broader crime concerns and legal issues. This broadening scope is a natural progression of Digital Investigation becoming more relevant in various legal contexts. Alignment with FSI will nurture this natural progression by extending Digital Investigation to a larger, more diverse, global community.

The techniques and tools in Digital Investigation have largely grown out of computer science. Increased integration with forensic science will augment the existing foundation in computer science. As stated in OSAC Technical Publication 002, "*digital/multimedia evidence, and other forensic disciplines, would be in a much stronger position to demonstrate their scientific basis if they were considered as belonging to a harmonized forensic science rather than as mere disciplines at the intersection of forensic specialties and other sciences.*"

Digital Investigation requires more rigorous scientific support in order to be accepted in court on an equal footing with other forensic disciplines. Less obviously, other forensic disciplines need to adopt a more investigative focus. Many forensic science capabilities, including Digital Investigation, are used in non-judicial contexts such as international disputes, border controls, counter-terrorism operations, and accident reconstructions. Exploring together how to treat these, and other contexts, will enable more cohesive coordinated solutions. As a general example, Digital Investigation is applying big data analysis to improve investigative and forensic processes, and can help other forensic disciplines learn how to harness the power of big data to solve problems collaboratively.

Incident response, and cyber-risk management generally, will continue to be a core component of Digital Investigation. Our hope is that increasing the integration of Digital Investigation with forensic science will reinforce incident response methods and tools. Integrating forensic science processes into existing practices and methods will lead to more reliable results, broadly benefiting practitioners in cyber investigation and cybersecurity. Mature theory and practices of forensic intelligence will bolster cyber threat intelligence.

Work published in FSI Digital Investigation will reach a larger audience, significantly increasing its impact. This impact will not be immediately apparent due to the way that publishing metrics are treated in the first few years of a transition of this kind. Independent of such metrics, increasing collaboration among communities with common interests promises to be both stimulating and productive.

Digital forensics has spent several decades on the outskirts of the traditional forensic science community as a misfitting group of computer scientists and engineers. This move into the FSI family marks a pivotal change in the perception and acceptance of digital forensics. In the larger historical context of forensic science, Digital Investigation is being welcomed into the field as a core pillar of research and practice alongside longstanding disciplines.

Eoghan Casey, Zeno Geradts, Bruce Nikkel

Available online 12 September 2019

https://doi.org/10.1016/j.diin.2019.100886
1742-2876