Editor-in-Chief: Eoghan Casey

Forensic Science International: Digital Investigation

1182,35 €
1105,00 € (zzgl. MwSt.)
Institutionen

Lieferfrist: bis zu 10 Tage

Artikelnummer: 9772666282007
Medium: Zeitschrift
ISBN: 977-266628200-7
Verlag: Elsevier
Erscheinungsweise: vierteljährlich
Sprache(n): Englisch
Produktform: Other printed item

FSI Digital Investigation covers a broad array of subjects related to crime and security throughout the computerized world. The primary pillar of this publication is digital evidence and multimedia, with the core qualities of provenance, integrity and authenticity. This publication promotes advances in investigating cybercrimes, cyberattacks and traditional crimes involving digital evidence, using scientific practices in digital investigations, and reducing the use of technology for criminal purposes. This widely referenced publication promotes innovations and advances in utilizing digital evidence and multimedia for legal purposes, including criminal justice, incident response, cybercrime analysis, cyber-risk management, civil and regulatory matters, and privacy protection. Relevant research areas include forensic science, computer science, data science, artificial intelligence, and smart technology. This journal is used by investigative agencies and forensic laboratories, computer security teams, practitioners, researchers, developers, and lawyers from industry, law enforcement, government, academia, and the military to share their knowledge and experiences, including current challenges and lessons learned in the following areas: Research and development: Novel research and development in forensic science, computer science, data science, and artificial intelligence applied to digital evidence and multimedia. New methods to deal with challenges in digital investigations, including applied research into analysing digital evidence and multimedia, exploiting specific technologies, and into preparing for and responding to computer security incidents. Cyber-criminal investigation: develop new methods of online investigation and analysis of financially motivated cyber-crime such as banking Trojans, phishing, ransomware and other forms of cyber-fraud. In addition, researching future criminal activity involving peer-to-peer payments and crypto currencies. Hardware Forensics: develop new methods of extracting and analyzing evidence from electronic hardware. This includes analyzing IoT devices, embedded systems, industrial control systems, automobiles, and other systems requiring hardware component access to extract data (e.g., chip-off, debugging interfaces like JTAG, fault injection). Cyber-risk management: Improved ways of using digital evidence to address security breaches involving information systems, methods to find zero day attacks and to perform cyber threat intelligence. The techniques and findings of digital investigations are essential in drawing post-incident conclusions, which are vital feedback components of the security policy development process, and managing risk appetite. Case Notes: Brief investigative case studies with practical examples of how digital evidence is being used in digital investigations, forensic analysis, and incident response. Case Notes can also describe current challenges that practitioners are facing in cybercrime and computer security, highlighting areas that require further research, development or legislation. The format for Case Notes is simple and short: case background, any technical or legal challenges, the digital evidence and multimedia involved, processes and/or tools used, and outcomes (e.g., solutions, barriers, need for R&D). Please check the following example for preferred Case Note format: https://www.sciencedirect.com/science/article/pii/S1742287618301713. Scientific practices: Novel approaches to strengthening the scientific foundation and rigor of digital investigations, and to increasing the reliability of and confidence in processes, analysis methods, results, and conclusions involving digital evidence and multimedia. Effective practices: Studies that assess new practices in digital investigations and propose effective approaches to handling and processing digital evidence. Survey papers: Discussion of current methods and future needs relevant to digital investigations, including analysing digital evidence and multimedia from computers, smart technology, mobile phones, memory, malware, network traffic, as well as systems that support enterprises, telecommunications, and satellites. In addition, advanced approaches to analysing digital evidence and multimedia, including novel applications of artificial intelligence and data analytics.Application analysis: Novel approaches to analysing applications on mobile devices and computers from a digital forensic perspective. Analysis may include configuration and log data, network telemetry and cloud storage,

Kundenservice Verlag Dr. Otto Schmidt KG
Neumannstraße 10, 40235 Düsseldorf | kundenservice@otto-schmidt.de | 0221-93738-997 (Inland)