

Call for Papers

Digital Investigation: The International Journal of Digital Forensics & Incident Response

The **Journal of Digital Investigation** covers cutting edge developments in digital forensics and incident response from around the globe. This widely referenced publication helps digital investigators remain current on new technologies, useful tools, relevant research, investigative techniques, and methods for handling security breaches.

Practitioners in corporate, criminal and military settings use this journal to share their knowledge and experiences, including current challenges and lessons learned. Publication in this journal helps develop an individual's credentials as an active member of their field.

Research papers, survey articles, practitioner reports, case studies, tools reviews, and legal analysis relevant to incident response and digital forensics are welcomed. The first issue of the journal each year is available for free in digital form. Papers from recent issues include:

- An introduction to investigating IPv6 networks (Nikkel, B.J.)
- Pinpointing TomTom location records: a forensic analysis (Nutter, B.)
- Case Study: Recovering Erased Digital Evidence from CD-RW Discs in a Child Exploitation Investigation (Wardwell, J.; Smith, G.S.)
- Contagious errors: Understanding and avoiding issues with imaging drives containing faulty sectors (Byers, D., Nahid Shahmehri, N.)
- Case study: Network intrusion investigation - lessons in forensic preparation (Casey, E.)
- Forensic artefacts left by Windows Live Messenger 8.0 (van Dongen, W.S.)
- Case Study: Forensic analysis of a Samsung Digital Video Recorder (van Dongen, W.S.)
- Forensic discovery auditing of digital evidence containers (Richard, G.G.; Roussev, V.; Marziale, L.)
- Tackling the U3 trend with computer forensics (Spruill, A.; Pavan, C.)
- Using every part of the buffalo in Windows memory analysis (Kornblum, J.)
- The Windows Registry as a forensic artefact: Illustrating evidence collection for Internet usage (Mee, V.; Tryfonas, T.; Sutherland, I.)

- User data persistence in physical memory (Solomon, J.; Huebner, E.; Bem, D.; Szezynska, M.)
- An examination into MSN Messenger 7.5 contact identification by Mike Dickson

Of particular interest are new submissions addressing the intersection of information security and digital forensics, including:

- Incident handling
- Managing rapid emergency response
- Intrusion investigation
- Case management issues with large data quantities
- Volatile data analysis
- Malware analysis
- Vista artifacts
- Network traffic and log analysis
- Certification, qualifications and education of practitioners
- Digital investigators relating to lawyers and regular investigators
- The role of law enforcement

Please visit the journal homepage at <http://www.digitalinvestigation.net> for instructions on submission.

Submissions for all types of manuscripts to Digital Investigation proceeds totally online via the Elsevier Editorial System - <http://ees.elsevier.com/diin>

All papers are peer reviewed by members of the Board of Referees prior to acceptance for publication in the journal.