Call for Papers

The *Journal of Digital Forensics, Security and Law* has an open call for papers in, or related to, the following subject areas:

1) Digital Forensics Curriculum
2) Cyber Law Curriculum
3) Information Assurance Curriculum
4) Digital Forensics Teaching Methods
5) Cyber Law Teaching Methods
6) Information Assurance Teaching Methods
7) Digital Forensics Case Studies
8) Cyber Law Case Studies
9) Information Assurance Case Studies
10) Digital Forensics and Information Technology
11) Law and Information Technology
12) Information Assurance and Information Technology

Guide for Submission of Manuscripts

Manuscripts should be submitted through the *JDFSL* online system in Word format using the following link: [http://www.jdfsl.org/for-authors](http://www.jdfsl.org/for-authors). If the paper has been presented previously at a conference or other professional meeting, this fact, the date, and the sponsoring organization should be given in a footnote on the first page. Articles published in or under consideration for other journals should not be submitted. Enhanced versions of book chapters can be considered. Authors need to seek permission from the book publishers for such publications. Papers awaiting presentation or already presented at conferences must be significantly revised (ideally, taking advantage of feedback received at the conference) in order to receive any consideration. Funding sources should be acknowledged in the *Acknowledgements* section.

The copyright of all material published in *JDFSL* is held by the Association of Digital Forensics, Security and Law (ADFSL). The author must complete and return the copyright agreement before publication. The copyright agreement may be found at [http://www.jdfsl.org/for-authors](http://www.jdfsl.org/for-authors).

Additional information regarding the format of submissions may be found on the *JDFSL* Web site at [http://www.jdfsl.org/for-authors](http://www.jdfsl.org/for-authors).
Contents

Call for Papers ........................................................................................................................................... 2
Guide for Submission of Manuscripts ........................................................................................................... 2
Multiple Content Adaptive Intelligent Watermarking Schemes for the Protection of Blocks of a Document ........................................................................................................................................ 5
  K. R. Chetan and S. Nirmala
Varying Instructional Approaches to Physical Extraction of Mobile Device Memory ............................ 29
  Joan Runs Through and Gary Cantrell
Digital Forensic Readiness in Organizations: Issues and Challenges ......................................................... 43
  Nickson M. Karie and Simon M. Karume
Broadband Router Security: History, Challenges and Future Implications ............................................. 55
  Patryk Szewczyk and Rose Macdonald
Evidence Verification Complications with Solid-State Drives ................................................................. 75
  Ryne Teague and Michael Black
A Data Hiding Scheme Based on Chaotic Map and Pixel Pairs ............................................................... 87
  Sengul Dogan
Subscription Information ............................................................................................................................... 101
Special Issue on the International Conference of Digital Forensics & Cyber Crime