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

Preface .......................................................................................................................................5

Petr Matoušek

Drone Forensic Analysis Using Open Source Tools .................................................................7

M A Hannan Bin Azhar, Thomas Edward Allen Barton and Tasmina Islam

Testing Memory Forensics Tools for the Macintosh OS X Operating System .........................31

Charles B. Leopard, Neil C. Rowe, and Michael R. McCarrin

A Sketch-Based 3D Modeling Method for 3D Crime Scene Presentation .................................43

Pu Ren, Wuyang Shui, Jin Liu, Yachun Fan, Wenshuo Zhao and Mingquan Zhou

Automated Man-in-the-Middle Attack Against Wi-Fi Networks .............................................59

Martin Vondracek, Jan Pluskal and Ondrej Rysavy

Hierarchical Bloom Filter Trees for Approximate Matching ..................................................81

Author David Lillis, Frank Breitinger and Mark Scanlon

Subscription Information ..........................................................................................................97
This special issue of the Journal of Digital Forensics, Security and Law (JDFSL) comprises extended versions of the top research papers that were presented on the 9th EAI International Conference on Digital Forensics & Cyber Crime (ICDF2C) that was held in October 2017 in Prague, Czech Republic.

On behalf of the ICDF2C 2017 organizing committee I would like to express my thanks to JDFSL journal, especially to JDFSL Editor-In-Chief Glenn Dardick, for the opportunity to publish selected papers in the JDFSL journal. Topics of these papers are practically oriented and our aim is to make them available to all potential readers through this renowned open access journal.

The papers cover current issues of digital forensics and investigation like cybercrime scene modelling using virtual reality, drone forensics, memory forensics of OS, exploitation of WiFi protection, or advanced searching methods for the data on a seized device.

I believe that the contents of this issue will be interesting for many readers who are involved in digital forensics, cybercrime investigation, and security.

Enjoy the reading.

Petr Matoušek
General Co-Chair of ICDF2C 2017
Brno University of Technology, Czech Republic