Editor’s Note

The Association of Digital Forensics, Security and Law recently held its first annual conference, the Conference on Digital Forensics, Security and Law, on April 20-21, 2006 in Las Vegas, Nevada, USA. The conference featured papers and discussions from professionals in both the public and private sector. The conference was attended by academics, students, and practitioners. This issue of the Journal of Digital Forensics, Security and Law is a special issue containing only those papers from the conference that were chosen as best papers.

Call for Papers

The Journal of Digital Forensics, Security and Law is now calling for papers in, or related to, the following 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

To be considered for inclusion in the third issue of the Journal of Digital Forensics, Security and Law, manuscripts should be submitted prior to midnight July 31st, 2006.
Guide for Submission of Manuscripts

All manuscripts should be word-processed (letter or correspondence-quality font). 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. Funding sources should be acknowledged in the "Acknowledgements" section. 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.

Manuscripts should be submitted through the JDFSL online system in Word or PDF format using the following link: http://www.jdfsl.org/submission.asp.

Manuscripts may also be submitted to the editor in Word, Word Perfect, RTF, or PDF format. The editor of the JDFSL, Dr. Glenn S. Dardick, may be reached via email at editor@jdfsl.org.

In special circumstances, papers will be accepted in paper format, but this may considerably delay the review of the paper. Authors are advised to contact the Editor before submitting hard copy.

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.jdfsll.org/copyrighttransfer.pdf.

Additional information regarding the format of submissions may be found on the JDFSL website at http://www.jdfsll.org/authorinstructions.htm.
Contents

Call for Papers.................................................................2
Guide for Submission of Manuscripts...............................3
Development of a National Repository of Digital Forensic
Intelligence .................................................................5
Mark Weiser, David P. Biros and Greg Mosier

Computer Forensics Field Triage Process Model ................19
Marcus K. Rogers, James Goldman, Rick Mislan, Timothy Wedge
and Steve Debrota

Development and Delivery of Coursework:
Legal/Regulatory/Policy Environment of Cyber-Forensics ....39
John W. Bagby and John C. Ruhnka

Forensic Tools for Mobile Phone Subscriber Identity Modules ....75
Wayne Jansen and Rick Ayers

Subscription Information ..............................................95