Editors

Glenn S. Dardick, Editor-in-Chief
Longwood University
Virginia, USA

Copyright © 2009 ADFSL, the Association of Digital Forensics, Security and Law. Permission to make digital or printed copies of all or any part of this journal is granted without fee for personal or classroom use only and provided that such copies are not made or distributed for profit or commercial use. All copies must be accompanied by this copyright notice and a full citation. Permission from the Editor is required to make digital or printed copies of all or any part of this journal for-profit or commercial use. Permission requests should be sent to Dr. Glenn S. Dardick, Editor, Journal of Digital Forensics, Security and Law, 1642 Horsepen Hills Road, Maidens, Virginia 23102 or emailed to editor@jdfsl.org.

ISSN 1558-7215
Editor’s Note

When I was a younger academic, I attended a conference on accounting behavioral research issues. During the luncheon, one well-known accounting professor stated that “accounting is about information.” At the time, I discounted his statement, but it remained with me. Since then, I have come to agree with those words. Accounting is about information that affects third-party’s perspectives about the future prospects of financial trends. Furthermore such information can come from anywhere. In some cases, we have seen that it has taken the passage of legislation to force practicing accountants to collect and record such information, i.e., 1977’s Foreign Corrupt Practices Act to 2002’s Sarbanes-Oxley Act.

Today is no different. Today there is a financial fraud tsunami occurring, in the face of which accounting practitioners continue to maintain their tradition that they are not responsible for financial fraud as auditors. Such a tradition means the training for fraud detection or prevention must be limited to cover only specific areas of forensic investigation. To truly handle this situation, a new type of financial audit or a supplemental forensic audit needs to be introduced so that tools of digital forensics and accounting can be integrated. For example, accounting majors at our universities have to understand why they cannot continue to only work with paper documents and application programs. Such a change in academia needs to be led by forensically-literate accounting professors who understand digital forensics and its potential in financial fraud detection.

The research found in this Special Edition of the Journal of Digital Forensics, Security and Law (JDFSL) combines digital forensics with accounting. The articles: (1) identify graduate student’s perspectives toward the field of forensic accounting; (2) show how to use the raw data in an electronic audit trail to identify fraudsters; and (3) conceptualize a definition for a forensic audit. The academics writing in this area are rare as they combine research in two areas that have not found a voice in the literature. For that reason alone the editor of the JDFSL, Glenn Dardick, needs to be commended for bringing together this Special Edition.

G. Stevenson Smith
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 3rd issue of the 2009 volume of the Journal of Digital Forensics, Security and Law, manuscripts should be submitted prior to midnight June 30th, 2009.

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 format using the following link: http://www.jdfsl.org/submission.asp.

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

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/copyrighttransfer.pdf.

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

Call for Papers ........................................................................................................ 3
Guide for Submission of Manuscripts ................................................................. 3
Graduate Accounting Students' Perception of IT Forensics: A Multi-Dimensional Analysis .............................................................. 5
Grover S. Kearns
Continuous Fraud Detection in Enterprise Systems through Audit Trail Analysis .......................................................... 39
Peter J Best, Pall Rikhardsson and Mark Toleman
Defining a Forensic Audit .............................................................................. 61
G. Stevenson Smith and D. Larry Crumbley
Subscription Information ........................................................................ 81
Announcements and Upcoming Events .......................................................... 82