THE JOURNAL OF
DIGITAL FORENSICS,
SECURITY AND LAW

Journal of Digital Forensics, Security and Law

Volume 8 Article 6

2013

Front Matter

JDFSL

The Journal of Digital Forensics, Security and Law

Volume 8, Number 3
2013

JDFSL

The Journal of Digital Forensics, Security and Law

Volume 8, Number 3 (2013)

Editorial Board

ISSN 1558-7215

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/submission.asp. 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/copyrighttransfer.pdf.

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

Contents

From the Editor-in-Chief

Welcome to the third issue of Volume 8. I hope that during the winter holiday season you'll find time to slow down, relax, and take in a few of these interesting articles.

In the first article, professors Ruhnka and Loopesko describe the types of liabilities that corporations can incur from the electronic communications of its employees. Few effective defenses exist to shield companies from legal liability for employee email misuse or intentional abuse, even when the liability-creating communication was specifically prohibited. In their paper, *Risk Management of Email and Internet Use in the Workplace,* the authors present an alternative approach to risk management, focusing on controlling only those potential risks relevant to an organization's specific activities.

In this issue's Technology Corner, the paper titled *Trends in Android Malware Detection,* written by Shaerpour, Dehghantanha, and Mahmod, describes the current state of malicious software detection on the popular Android operating system for mobile devices. The cat-and-mouse game between malware authors and defenders is gaining traction in the Android, and should sound familiar since trouble-makers generally follow the users and their money.

Money-laundering detection requires unraveling concealed connections among multiple, but seemingly unrelated, human money-laundering networks; ties among actors in sophisticated schemes; and amounts of funds transferred among the participating entities. In the third article, Mehmet and Buchholtz present their approach to detecting money-laundering schemes in *Money Laundering Detection Framework to Link the Disparate and Evolving Schemes*.

In the fourth paper, *System-Generated Digital Forensic Evidence in Graphic Design Applications* by Mabuto and Venter, the authors explore the kinds of digital footprints left by graphic design software, specifically when used for counterfeiting documents. They demonstrate that interesting and useful forensic evidence may be found in the artifacts left by the software during document scanning, editing, and saving of the new counterfeit.

The final article is a very thorough review by Joshua Bartolomie of the book, *Professional Penetration Testing: Creating and Learning in a Hacking Lab 2E,* written by Thomas Wilhelm.

Over the next few months we will be recruiting section editors and article reviewers, and providing online training in those functions. Please consider your role in keeping the journal a fitting resource for our diverse academic and

professional audiences. Self-nominations are welcome. Targeted recruiting may follow if needed.

Gregg Gunsch, Ph.D., PE, CISSP, GCFA, CCE, DFCP

ggunsch@jdfsl.org