



THE JOURNAL OF  
**DIGITAL FORENSICS,  
SECURITY AND LAW**

**Journal of Digital Forensics,  
Security and Law**

---

Volume 8

Article 6

---

2013

## Front Matter

Follow this and additional works at: <https://commons.erau.edu/jdfsl>



Part of the [Computer Law Commons](#), and the [Information Security Commons](#)

---

### Recommended Citation

(2013) "Front Matter," *Journal of Digital Forensics, Security and Law*: Vol. 8 , Article 6.

DOI: <https://doi.org/10.58940/1558-7223.1331>

Available at: <https://commons.erau.edu/jdfsl/vol8/iss3/6>

This Front Matter/Back Matter is brought to you for free and open access by the Journals at Scholarly Commons. It has been accepted for inclusion in Journal of Digital Forensics, Security and Law by an authorized administrator of Scholarly Commons. For more information, please contact [commons@erau.edu](mailto:commons@erau.edu).

**EMBRY-RIDDLE | PURDUE**  
Aeronautical University | UNIVERSITY

(c)ADFSL



# 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

#### Editor-in-Chief

Gregg Gunsch  
Defiance College  
Ohio, USA

#### Associate Editor-in-Chief

Jigang Liu  
Metropolitan State University  
Minnesota, USA

#### Section Editors

##### Digital Forensics

John Riley  
Bloomsburg University  
Pennsylvania, USA

Scott Inch  
Bloomsburg University  
Pennsylvania, USA

##### Cyber Law

Erin Kenneally  
Univ. of California San Diego  
California, USA

Nigel Wilson  
The University of Adelaide  
South Australia, Australia

##### Information Security

David Dampier  
Mississippi State University  
Mississippi, USA

Daniel P. Manson  
Cal Poly Pomona  
California, USA

Denise Pheils  
Indiana Tech  
Indiana, USA

##### Science of Digital Forensics

Fred Cohen  
California Sciences Institute  
California, USA

Simson Garfinkel  
Naval Postgraduate School  
California, USA

#### Book Review

Diane Barrett  
University of Advanced Technology  
Arizona, USA

#### Technology Corner

Nick V. Flor  
University of New Mexico  
New Mexico, USA

#### Regional Editors

##### Australia

Craig Valli  
Edith Cowan University  
Western Australia, Australia

##### Europe/UK

Denis Edgar-Neville  
Canterbury Christ Church Univ.  
Canterbury, UK

##### Latin America

Pedro Luís Próspero Sanchez  
University of Sao Paulo  
Sao Paulo, Brazil

##### Mid-East and Africa

Andrew Jones  
Khalifa Univ of Science,  
Technology & Research  
Sharjah, United Arab Emirates

##### Mid-East/Israel

Eli Weintraub  
Afeka Tel Aviv Academic College  
of Engineering  
Tel Aviv, Israel

##### Assistant Copy Editor

Alexandra K. Greene  
Longwood University

#### Editorial Board

John W. Bagby  
The Pennsylvania State Univ.  
Pennsylvania, USA

Ibrahim Baggili  
Zayed University  
Abu Dhabi, United Arab Emirates

David P. Biros  
Oklahoma State University  
Oklahoma, USA

Philip Craiger  
Daytona State College  
Florida, USA

Glenn S. Dardick  
Longwood University  
Virginia, USA

Fred C. Kerr  
Consultant  
California, USA

Linda K. Lau  
Longwood University  
Virginia, USA

Wei Ren  
Chinese Univ. of Geosciences  
Wuhan, China

Jill Slay  
University of South Australia  
South Australia, Australia

Il-Yeol Song  
Drexel University  
Pennsylvania, USA

Bernd Carsten Stahl  
De Montfort University  
Leicester, UK

Copyright © 2013 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 Editor, JDFSL, 1642 Horsepen Hills Road, Maidens, Virginia 23102, or emailed to [editor@jdfsl.org](mailto:editor@jdfsl.org).

## **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**

<b>Call for Papers</b> .....	2
<b>Guide for Submission of Manuscripts</b> .....	2
<b>From the Editor-in-Chief</b> .....	5
<b>Risk Management of Email and Internet Use in the Workplace</b> .....	7
John Ruhnka, and Windham E. Loopesko	
<b>Technology Corner: Trends in Android Malware Detection</b> .....	21
Kaveh Shaerpour, Ali Dehghantanha, and Ramlan Mahmood	
<b>Money Laundering Detection Framework to Link the Disparate and Evolving Schemes</b> .....	41
Murad Mehmet, and Miguel Fuentes Buchholtz	
<b>System-Generated Digital Forensic Evidence in Graphic Design Applications</b> .....	71
Enos Mabuto, and Hein Venter	
<b>Book Review: Professional Penetration Testing: Creating and Learning in a Hacking Lab 2E (Thomas Wilhelm)</b> .....	87
Joshua Bartolomie	
<b>Subscription Information</b> .....	91
<b>Announcements and Job Postings</b> .....	93



## **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, Dehghantaha, and Mahmood, 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](mailto:ggunsch@jdfsl.org)