



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

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

---

Volume 7 | Number 4

Article 8

---

2012

## 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

(2012) "Front Matter," *Journal of Digital Forensics, Security and Law*: Vol. 7 : No. 4 , Article 8.

Available at: <https://commons.erau.edu/jdfsl/vol7/iss4/8>

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**  
Aeronautical University™  
SCHOLARLY COMMONS

(c)ADFSL



# JDFSL

The Journal of  
Digital Forensics,  
Security and Law



Volume 7, Number 4  
2012



# JDFSL

## The Journal of Digital Forensics, Security and Law

Volume 7, Number 4 (2012)

### Editorial Board

#### Editor-in-Chief

Gary C. Kessler  
Embry-Riddle Aeronautical  
University  
Florida, USA

#### Associate Editor-in-Chief

Marcus K. Rogers  
Purdue University  
Indiana, USA

#### Section Editors

##### *Digital Forensics*

Gregg Gunsch  
Defiance College  
Ohio, 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

##### *Science of Digital Forensics*

Fred Cohen  
California Sciences Institute  
California, USA

Simson Garfinkel  
Naval Postgraduate School  
California, USA

##### *Book Review*

Jigang Liu  
Metropolitan State University  
Minnesota, 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

#### 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  
Univ. of South Australia  
South Australia, Australia

Il-Yeol Song  
Drexel University  
Pennsylvania, USA

Bernd Carsten Stahl  
De Montfort University  
Leicester, UK

Copyright © 2012 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).

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 Website 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>Column: The Science of Digital Forensics: Recovery of Data from Overwritten Areas of Magnetic Media</b> .....	7
Fred Cohen	
<b>"Preemptive Suppression" – Judges Claim the Right to Find Digital Evidence Inadmissible before It is Even Discovered</b> .....	21
Bob Simpson	
<b>An Australian Perspective on the Challenges for Computer and Network Security for Novice End-Users</b> .....	51
Patryk Szewczyk	
<b>Forensic Evidence Identification and Modeling for Attacks against a Simulated Online Business Information System</b> .....	73
Manghui Tu, Dianxiang Xu, Eugene Butler, & Amanda Schwartz	
<b>Implementing the Automated Phases of the Partially-Automated Digital Triage Process Model</b> .....	99
Gary Cantrell & David A. Dampier	
<b>Book Review: <i>Mastering Windows Network Forensics and Investigation, 2/e</i> (Anson, Bunting, Johnson, &amp; Pearson)</b> .....	117
John C. Ebert	
<b>Technology Corner: A Regular Expression Training App</b> .....	125
Nick V. Flor	
<b>Subscription Information</b> .....	133
<b>Announcements and Upcoming Events</b> .....	135



## **From the Editor-in-Chief**

Welcome to the final issue of Volume 7. We start the issue with the Digital Forensics as Science column, with Fred Cohen taking on the sometimes-controversial issue of recovering overwritten data from magnetic media. In our other standing columns, John C. Ebert provides an in-depth review of a new edition of one of the best-known Windows forensics books written by Anson et al., and Nick Flor presents a Technology Corner article with an app for teaching regular expressions. And, of course, we have four peer-reviewed papers in this issue, covering the trifecta of the Journal – digital forensics, information security, and the law.

The first paper, *'Preemptive Suppression' – Judges Claim the Right to Find Digital Evidence Inadmissible before It is Even Discovered* (Simpson), is a very timely review of a recent Vermont Supreme Court decision. On the heels of the controversial *U.S. v. Comprehensive Drug Testing* ruling that essentially eliminated plain view on digital devices, a trial judge in Vermont started to add strict limitations and conditions on search warrants for digital devices in criminal investigations. Prosecutors sought clarity from the state Supreme Court about the constitutionality of those restrictions, as reported in this paper.

*An Australian Perspective on the Challenges for Computer and Network Security for Novice End-Users* (Szewczyk) discusses research about why following "simple" information security guidelines is often beyond the reach of many novice computer users. The paper further describes methods that may prove beneficial to improving users' security and computer proficiency.

The third paper, *Forensic Evidence Identification and Modeling for Attacks against a Simulated Online Business Information System* (Tu, Xu, Butler, & Schwartz), describes mechanisms that can be used by an organization to maintain *forensic readiness*, i.e., the ability of an organization to be prepared to launch an investigation or perform an audit after an event. The authors describe several scenarios of internal and external attacks, and a honeypot-based simulation model.

Our final paper, *Implementing the Automated Phases of the Partially-Automated Digital Triage Process Model* (Cantrell & Dampier), describes ways of automating the digital triage process. As the number of digital devices with a possible nexus to an arrest or crime increases, as well as the size of the digital media to examine, triage in the field becomes an important way to minimize a huge backlog in the lab that might include non-probative information.



I also wish to note that this is my final issue as Editor-in-Chief. They say that "change is good." Over the last two years, with the support of publisher and founding editor, Glenn Dardick, and the amazing set of professionals listed on the journal's masthead, we have morphed the journal in several subtle and not-so-subtle ways. For starters, we added section editors to assist in the review of papers, which has increased the rate at which we can process submissions. We also added regional editors in an effort to increase international submissions. We added two columns – Digital Forensics as a Science (Fred Cohen and Simson Garfinkel) and Technology Corner (Nick Flor) – to our extant Book Review column (Jigang Liu, who also steps down after this issue). And we have increased the number of peer-reviewed papers from three to four per issue. I thank all of the editors, reviewers, authors, and readers in continuing the journal's success. With this, I hand the EIC reins over to David Biros and trust that he will have the same level of support as I have had. Thank you all.

Gary C. Kessler, Ph.D., CCE, CISSP  
*gary.kessler@erau.edu*