



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

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

Volume 8 | Number 1

Article 5

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 : No. 1 , Article 5.

Available at: <https://commons.erau.edu/jdfsl/vol8/iss1/5>

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.



(c)ADFSL



JDFSL

The Journal of
Digital Forensics,
Security and Law



Volume 8, Number 1
2013

JDFSL

The Journal of Digital Forensics, Security and Law

Volume 8, Number 1 (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 | <i>Technology Corner</i> | Ibrahim Baggili Zayed University Abu Dhabi, United Arab Emirates |
| <i>Digital Forensics</i> Gregg Gunsch Defiance College Ohio, USA | Nick V. Flor University of New Mexico New Mexico, USA | David P. Biros Oklahoma State University Oklahoma, USA |
| Scott Inch Bloomsburg University Pennsylvania, USA | Regional Editors | Philip Craigie Daytona State College Florida, USA |
| <i>Cyber Law</i> Erin Kenneally Univ. of California San Diego California, USA | <i>Australia</i> Craig Valli Edith Cowan University Western Australia, Australia | Glenn S. Dardick Longwood University Virginia, USA |
| Nigel Wilson The University of Adelaide South Australia, Australia | <i>Europe/UK</i> Denis Edgar-Neville Canterbury Christ Church Univ. Canterbury, UK | Fred C. Kerr Consultant California, USA |
| <i>Information Security</i> David Dampier Mississippi State University Mississippi, USA | <i>Latin America</i> Pedro Luís Próspero Sanchez University of Sao Paulo Sao Paulo, Brazil | Linda K. Lau Longwood University Virginia, USA |
| Daniel P. Manson Cal Poly Pomona California, USA | <i>Mid-East and Africa</i> Andrew Jones Khalifa Univ of Science, Technology & Research Sharjah, United Arab Emirates | Wei Ren Chinese Univ. of Geosciences Wuhan, China |
| <i>Science of Digital Forensics</i> Fred Cohen California Sciences Institute California, USA | <i>Mid-East/Israel</i> Eli Weintraub Afeka Tel Aviv Academic College of Engineering Tel Aviv, Israel | Jill Slay Univ. of South Australia South Australia, Australia |
| Simson Garfinkel Naval Postgraduate School California, USA | Editorial Board | Il-Yeol Song Drexel University Pennsylvania, USA |
| <i>Book Review</i> Diane Barrett University of Advanced Technology Arizona, USA | John W. Bagby The Pennsylvania State Univ. 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.

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

| | |
|--|----|
| Call for Papers | 2 |
| Guide for Submission of Manuscripts | 2 |
| From the Editor-in-Chief | 5 |
| Science Column: Measuring Inconsistency Methods for Evidentiary Value | 7 |
| Fred Cohen | |
| A Simple Experiment with Microsoft Office 2010 and Windows 7 Utilizing Digital Forensic Methodology | 17 |
| Gregory H. Carlton | |
| How often is Employee Anger an Insider Risk I? Detecting and Measuring Negative Sentiment versus Insider Risk in Digital Communications (Part 1 of 2) | 39 |
| Eric Shaw, Maria Payri, Michael Cohn, and Ilene R. Shaw | |
| Technology Corner: Visualising Forensic Data: Evidence (Part 1 of 2) | 73 |
| Damian Schofield and Ken Fowle | |
| Subscription Information | 91 |

From the Editor-in-Chief

Welcome to the first issue of Volume 8. It is an honor to assume this responsibility as my first foray into the role of Editor-in-Chief, and I thank Gary Kessler, Glenn Dardick, and the rest of the Journal's leadership for their faith. I will strive to maintain the high level of quality the Journal has achieved, and continue to improve it as fitting to meet the needs of you, the readers.

Towards that end I would like to invite your inputs through Letters to the Editor (mailto: editor@jdfsl.org). Those of interest to the wider audience will be considered for publication. One topic worth discussing is the intended audience of the Journal. I was recently asked, "What level or kind of audience is *JDFSL* trying to hit? Practitioner? Advanced researcher? Novice?" I've asked those questions myself, repeatedly. The answer I gave was "Yes." I see the Journal as a mixed bag. We want to keep the standards high, so that it stands as an archival academic journal; this is why we perform double-blinded peer reviews of the major articles. At the same time, we want it to be a valuable resource for practitioners. And for people new to the field, I hope that it helps open their eyes to the breadth of our disciplines and sparks their interest. Your inputs are welcome.

In this issue we have three papers that share a fortunate confluence of theme: an awareness of the role of bias. This isn't bias in a negative, malicious sense, but rather the natural tendency to de-clutter the world by focusing on only those things that support our current line of reasoning (confirmation bias). The caution is that in our zeal, we need to remember to consider alternative explanations and not lose sight of the fact that when evidence is consistent with a hypothesis, this does not mean that the evidence has proven that hypothesis or refuted any others.

Dr. Fred Cohen's science article, *Measuring Inconsistency Methods for Evidentiary Value*, addresses the situation where two or more pieces of evidence appear to be inconsistent with each other, leading to a potential accusation that evidence has been altered. On the surface that is a reasonable conclusion; however, deeper analysis of their originating mechanisms may reconcile the apparent inconsistencies. The underlying truth is discovered through experimentation, reconstruction, and the conscious effort to avoid succumbing to confirmation bias.

Dr. Gregory Carlton's article, *A Simple Experiment with Microsoft Office 2010 and Windows 7 Utilizing Digital Forensic Methodology*, is aimed at practitioners. It provides a real-world example of a set of experiments to ferret out and understand system artifacts. It reminds us to avoid assumptions and biases, and to be methodical—to have a structured, reasoned and scientific

framework for testing out theories of system operations and interactions. It concludes by asking the question, “To what extent do digital forensic examiners perform such experiments?” while encouraging the research community to investigate whether such experimentation is, in fact, necessary.

In the article titled *Visualising Forensic Data: Evidence Guidelines*, Dr. Damian Schofield provides an introduction to the use of visualization techniques for presenting digital data in the courtroom. Such reconstructions can be extremely beneficial for both prosecution and defense to communicate complex information effectively to the jurors and judge. The caution is that such reconstructions, by their very nature, are potentially prone to promote the biases of their creators.

In the fourth paper, *How often is Employee Anger an Insider Risk? Detecting and Measuring Negative Sentiment versus Insider Risk in Digital Communications*, Dr. Eric Shaw explores the question evident in the title. Security managers should be especially interested, since it is the insiders who typically can do the most damage while evading detection.

Thus launches the first issue of the Journal under this new editor. Your patience and feedback will be greatly appreciated.

Gregg Gunsch, Ph.D., PE, CISSP, GCFA, CCE, DFCP
ggunsch@jdfsl.org