THE JOURNAL OF DIGITAL FORENSICS, SECURITY AND LAW

Journal of Digital Forensics, Security and Law

Volume 8 | Number 2 Article 6

2013

Front Matter

Recommended Citation

(2013) "Front Matter," *Journal of Digital Forensics, Security and Law*: Vol. 8 : No. 2 , Article 6.
Available at: https://commons.erau.edu/jdfsl/vol8/iss2/6

JDFSL

The Journal of Digital Forensics, Security and Law

Volume 8, Number 2
2013

JDFSL

The Journal of Digital Forensics, Security and Law

Volume 8, Number 2 (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

Call for Papers 2

Guide for Submission of Manuscripts 2

From the Editor-in-Chief..5

Automating Vendor Fraud Detection in Enterprise Systems....................7
Kishore Singh, Peter Best, and Joseph Mula

Information Security Challenge of QR Codes 41
Nik Thompson and Kevin Lee

How often is Employee Anger an Insider Risk II? Detecting and Measuring Negative Sentiment versus Insider Risk in Digital Communications–Comparison between Human Raters and Psycholinguistic Software
(**Part 2 of 2**)..73
Eric Shaw, Maria Payri, Michael Cohn, and Ilene R. Shaw

Technology Corner: **Visualising Forensic Data**: **Evidence Guidelines**
(**Part 2 of 2**)..93
Damian Schofield and Ken Fowle

Book Review: ***Placing the Suspect behind the Keyboard: Using Digital Forensics and Investigative Techniques to Identify Cybercrime Suspects*** (**Brett Shavers**)...115
Thomas Nash

Subscription Information...119

Announcements and Upcoming Events 121

From the Editor-in-Chief

Welcome to the second issue of Volume 8. If you enjoyed the articles in the last issue, you'll be happy to know that the conclusions for the two "part-ones" are in this issue.

Our first article is on *Automating Vendor Fraud Detection in Enterprise Systems*, by Kishore Singh, Peter Best, and Joseph Mula. They present a model for proactively detecting fraudulent activities through pattern analysis of audit trails in enterprise systems. They also present methods of visualizing user activities in the transaction data, which assists in detecting potential fraud.

In *The Digital Forensics and Security Challenge of QR Codes*, Nik Thompson and Kevin Lee argue that the common implementation of QR codes potentially presents security and privacy issues. As with any technology that experiences rapid acceptance, there may not be commensurate adoption of sound security practices. The authors provide ample evidence that such is the case with the use of QR codes.

Next we present part two of Eric Shaw, et al.'s research on the detection of insider threat risk in *How Often is Employee Anger an Insider Risk? Detecting and Measuring Negative Sentiment versus Insider Risk in Digital Communications–Comparison Between Human Raters and Psycholinguistic Software*. In this article, Eric Shaw, Maria Payri, Michael Cohn, and Ilene Shaw explore the effectiveness of techniques that can serve as an initial screen to narrow the search for individuals at-risk for undesirable insider activities.

In part two of *Visualising Forensic Data: Evidence Guidelines*, Damien Schofield and Ken Fowle present a range of examples of where forensic data has been visualized using various techniques, and discuss benefits and potential problems of implementing this technology. It is probably safe to assume that the same technologies used to generate animated movies and computer games are going to be increasingly used to generate advanced visual presentations of evidence in a number of jurisdictions around the world, so this paper provides guidelines on the use of such technologies in the courtroom.

Brett Shavers is a former law enforcement detective and prolific speaker on digital forensics. He wrote his first book, *Placing the Suspect behind the Keyboard: Using Digital Forensics and Investigative Techniques to Identify Cybercrime Suspects*, in which he teaches us how to combine traditional investigative methods with forensic analysis to build a solid criminal or civil case. Read about Detective Corporal Thomas Nash's review on this book.

So far, nobody has taken me up on the invitation to comment through a Letter to the Editor (mailto: editor@jdfsl.org). I had proposed a discussion topic regarding the intended audience of the Journal: the level or kind of audience the *JDFLS* should attempt to reach. Please consider weighing in on that issue, or any other you would care to address.

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