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

Available at: https://commons.erau.edu/jdfsl/vol7/iss3/7

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, wolfe.309@erau.edu.
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 .................................................. 4
The Science of Digital Forensics: Analysis of Digital Traces .... 5
Fred Cohen

On the Development of a Digital Forensics Curriculum .......... 13
Manghui Tu, Dianxiang Xu, Samsuddin Wira, Cristian Balan, & Kyle Cronin

Automatic Crash Recovery: Internet Explorer's Black Box ...... 33
John Moran & Douglas Orr

Extraction of Electronic Evidence From VoIP: Identification & Analysis of Digital Speech ........................................... 55
David Irwin, Arek Dadej, & Jill Slay

To License or Not to License Updated: An Examination of State Statutes Regarding Private Investigators and Digital Examiners.... 83
Thomas Lonardo, Doug White, & Alan Rea

Book Review: *Dispute Resolution and e-Discovery* (Garrie & Griver) ................................................................. 111
Milton Luoma

Subscription Information.................................................. 115

Announcements and Upcoming Events ............................... 117
From the Editor-in-Chief

Welcome to the third issue of Volume 7. We continue with our regular columns. The Digital Forensics as Science column contains a new installment by Fred Cohen about information physics. Milton Luoma provides a review of a book about e-discovery and conflict resolution. While slightly off the topic of computer forensics, the book touches on these two related -- but different -- legal problems. Finally, Nick Flor has part 2 of his Technology Corner article on automated data extraction using Facebook. And, of course, we have four peer-reviewed papers in this issue.

The first paper, "On the Development of a Digital Forensics Curriculum" (Tu, Xu, Wira, Balan, & Cronin), is a broad overview of the development of digital forensics curricula over the last ten years. The paper also reports on a survey about what tools are being used by practitioners and in the classroom.

"Automatic Crash Recovery: Internet Explorer's Black Box" (Moran & Orr) provides a detailed examination of IE's Web history contents. This paper pays particular attention to IE's Automatic Crash Recovery feature, a source of a great deal of information that is generally unknown to most users (meaning that they don't attempt to delete its contents) and to many computer forensic examiners (meaning that they don't look there for evidence).

The third paper, "Extraction of Electronic Evidence From VoIP: Identification & Analysis of Digital Speech" (Irwin, Dadej, & Slay), describes software intellectual property and methods with which one can determine whether a particular Android application is using code pirated from another app. The Android's Java virtual machine architecture enables rapid app development but also allows straightforward ways to analyze -- and reverse engineer -- those apps.

Our final paper, "To License or Not to License Updated: An Examination of State Statutes Regarding Private Investigators and Digital Examiners" (Lonardo, White, & Rea), is an up-to-date glimpse of the status of state statutes requiring digital forensic examiners to be licensed as private investigators in order to practice. This issue is perhaps one of the most pressing for practitioners in our field.

We continue to actively solicit academic and practitioner papers and, in particular, look for papers with an international perspective. As always, we welcome feedback and comments about the Journal.

Gary C. Kessler, Ph.D., CCE, CISSP

teditor@jdfsl.org