



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

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


Volume 9 | Number 3

Article 6

2014

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

(2014) "Front Matter," *Journal of Digital Forensics, Security and Law*: Vol. 9 : No. 3 , Article 6.

Available at: <https://commons.erau.edu/jdfsl/vol9/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.

EMBRY-RIDDLE
Aeronautical University,[™]
SCHOLARLY COMMONS

(c)ADFSL



JDFSL

The Journal of
Digital Forensics,
Security and Law



Volume 9, Number 3
2014

JDFSL

The Journal of Digital Forensics, Security and Law

Volume 9, Number 3 (2014)

Editorial Board

Editor-in-Chief

Ibrahim (Abe) Baggili, PhD
University of New Haven
Connecticut, USA

Associate Editor-in-Chief

Linda K. Lau, PhD
Longwood University
Virginia, USA

Frank Adelstein, PhD
Cayuga Networks
New York, USA

John W. Bagby, JD
The Pennsylvania State University
Pennsylvania, USA

Diane Barrett, PhD, CISSP
Bloomsburg University
Pennsylvania, USA

David P. Biros, PhD
Oklahoma State University
Oklahoma, USA

Frank Breitingger
University of New Haven
Connecticut, USA

Raymond Choo, PhD
University of South Australia
South Australia, Australia

Kam Pui (KP) Chow, PhD
University of Hong Kong
Hong Kong, China

Fred Cohen, PhD, CEO
Management Analytics
California, USA

Philip Craiger, PhD, CISSP, CCFP
Daytona State College
Florida, USA

Glenn S. Dardick, PhD, CCE, CCFP
ADFSL
Virginia, USA

David Dampier, PhD
Mississippi State University
Mississippi, USA

Denis Edgar-Neville, PhD
Canterbury Christ Church University
Canterbury, UK

Barbara Endicott-Popovsky, PhD
University of Washington
Washington, USA

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

Simson Garfinkel, PhD
Naval Postgraduate School
California, USA

Pavel Gladyshev, PhD
University College Dublin
Ireland

Sanjay Goel
University at Albany
State University of New York
New York, USA

Gregg Gunsch, PhD, PE, CISSP
Defiance College
Ohio, USA

Joshua James, PhD
Soonchunhyang University
South Korea

Andy Jones, PhD
University of South Wales
UK

Erin Kenneally, MFS, JD
Elchemy, Inc.
University of California San Diego
California, USA

Gary C. Kessler, PhD, CCE, CCFP, CISSP
Embry-Riddle Aeronautical University
Florida, USA

Jigang Liu, PhD
Metropolitan State University
Minnesota, USA

Michael M. Losavio, JD
University of Louisville
Kentucky, USA

Andrew Marrington, PhD
Zayed University
UAE

Martin Oliver, PhD, CCFP
University of Pretoria
South Africa

Denise Pheils, PhD, CISSP, PMP
Texas A&M
Texas, USA

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

John Riley, PhD
Bloomsburg University
Pennsylvania, USA

Marcus K. Rogers, PhD, CISSP
Purdue University
Indiana, USA

Vassil Roussev, PhD
University of New Orleans
Louisiana, USA

Neil Rowe, PhD
U.S. Naval Postgraduate School
California, USA

Kathryn C. Seigfried-Spellar, PhD
The University of Alabama
Alabama, USA

Il-Yeol Song, PhD
ACM Distinguished Scientist
Drexel University
Pennsylvania, USA

Bernd Carsten Stahl, PhD
De Montfort University
Leicester, UK

Craig Valli, DIT
Edith Cowan University
Western Australia, Australia

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

Nigel Wilson
The University of Adelaide
South Australia, Australia

Copyright © 2014 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/for-authors>. 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/for-authors>.

Additional information regarding the format of submissions may be found on the *JDFSL* Web site at <http://www.jdfsl.org/for-authors>.

Contents

Call for Papers 2

Guide for Submission of Manuscripts 2

From the Editor-in-Chief 5

The Cost of Privacy: *Riley V. California's* Impact on Cell Phone Searches 7
Jennifer L. Moore, Jonathan Langton, and Joseph Pochron

**Quantifying Relevance of Mobile Digital Evidence as They Relate to Case Types:
A Survey and a Guide for Best Practice** 19
Shahzad Saleem, Ibrahim Baggili, and Oliver Popov

A Study of Forensic Imaging in the Absence of Write-Blockers..... 51
Gary C. Kessler and Gregory H. Carlton

**Book Review: *The X-Ways Forensics Practitioner's Guide* (Brett Shavers and
Eric Zimmerman)**..... 59
Linda Lau

Subscription Information 63

Announcements and Job Postings 65

FROM THE EDITOR

Welcome to JDFSL's third issue for 2014!

In this issue we have three papers that have made the cut. The first paper titled "The Cost of Privacy: Riley v. California's Impact on Cell Phone Searches" is timely. In 2014 there was a unanimous decision that requires a warrant for all cell phone searches. This has some strong implications on the forensic analysis of mobile phones, and to that end, this article discusses and summarizes this legal precedent with its practical implications.

The second paper titled "Quantifying the Relevance of Mobile Digital Evidence as They Relate to Case Types: A Survey and a Guide for Best Practices" is also a timely article. In this paper the researchers surveyed experts in the field, and using statistical analysis they rated the top type of evidence as they relate to case types. For example, the results showed that in drug cases, Short Message Service (SMS) is the most important type of evidence on average that an investigator should look for on a phone. The results from this work can be integrated in a mobile forensic triage tool.

The third paper is titled "A Study of Forensic Imaging in the Absence of Write-Blockers". This is both an interesting and timely topic – because one assumes that evidence may not be submitted to the court because change was made to it. The study concludes that no changes were made to the user files when a write-blocker was not used – which begs to question on whether or not evidence acquired without a write-blocker could be admitted in court.

Overall, the papers in this issue are multidisciplinary and timely. We hope that our readers enjoy them.

Sincerely,

Dr. Ibrahim Baggili PhD

Editor-in-Chief