



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

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

Volume 9 | Number 1

Article 7

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. 1 , Article 7.

Available at: <https://commons.erau.edu/jdfsl/vol9/iss1/7>

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.

EMBRY-RIDDLE
Aeronautical University™
SCHOLARLY COMMONS

(c)ADFSL



JDFSL

The Journal of
Digital Forensics,
Security and Law



Volume 9, Number 1
2014



The Journal of Digital Forensics, Security and Law

Volume 9, Number 1 (2014)

Editorial Board

Editor-in-Chief

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

Associate Editor-in-Chief

Linda K. Lau
Longwood University
Virginia, USA

Frank Adelstein
Cayuga Networks
New York, USA

John W. Bagby
The Pennsylvania State University
Pennsylvania, USA

Diane Barrett
Bloomsburg University
USA

David P. Biros
Oklahoma State University
Oklahoma, USA

Raymond Choo
University of South Australia
South Australia, Australia

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

Fred Cohen, Ph.D.
California Sciences Institute
Livermore, CA

Philip Craiger, Ph.D., CISSP, CCFP
Daytona State College
Florida, USA

Glenn S. Dardick, Ph.D., CCE
ADFSL
Virginia, USA

David Dampier, Ph.D.
Mississippi State University
Mississippi, USA

Denis Edgar-Neville, Ph.D.
Canterbury Christ Church University
Canterbury, UK

Barbara Endicott-Popovsky
University of Washington
Washington, USA

Nick V. Flor, Ph.D.
University of New Mexico
New Mexico, USA

Simson Garfinkel, Ph.D.
Naval Postgraduate School
Monterey, CA USA

Pavel Gladyshev
University College Dublin
Ireland

Gregg Gunsch, Ph.D., PE, CCE, CISSP
Defiance College
Ohio, USA

Joshua James
Soonchunhyang University
South Korea

Andy Jones, Ph.D.
University of South Wales
UK

Erin Kenneally, M.F.S., J.D.
Elchemy, Inc.
University of California San Diego
California, USA

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

Jigang Liu
Metropolitan State University
Minnesota, USA

Michael M. Losavio
University of Louisville
Kentucky, USA

Andrew Marrington
Zayed University
UAE

Martin Oliver
University of Pretoria
South Africa

Denise Pheils
Indiana Tech
Indiana, USA

Pedro Luís Próspero Sanchez, Ph.D.
University of Sao Paulo
Sao Paulo, Brazil

John Riley
Bloomsburg University
Pennsylvania, USA

Marcus K. Rogers, Ph.D., CISSP
Purdue University
Indiana, USA

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

Vassil Roussev
University of New Orleans
Louisiana, USA

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

Il-Yeol Song
Drexel University
Pennsylvania, USA

Bernd Carsten Stahl
De Montfort University
Leicester, UK

Craig Valli, DIT
Edith Cowan University
Western Australia, Australia

Eli Weintraub
Afeka Tel Aviv Academic College of
Engineering
Israel

Nigel Wilson
The University of Adelaide
South Australia, Australia

Copy Editor

Alexandra K. Greene
ADFSL

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/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
Idiographic Digital Profiling: Behavioral Analysis Based on Digital Forensics	7
Chad Steel	
Personal Denial of Service (PDOS) Attacks: A Discussion and Exploration of a New Category of Cyber Crime	19
Michael Bartolacci, Larry LeBlanc, and Ashley Podhradsky	
On Cyber Attacks and Signature based Intrusion Detection for MODBUS Based Industrial Control Systems	37
Wei Gao and Thomas H Morris	
Using Internet Artifacts to Profile a Child Pornography Suspect	57
Marcus K. Rogers and Kathryn C. Seigfried-Spellar	
Hot Zone Identification: Analyzing Effects of Data Sampling on Spam Clustering	67
Rasib Khan, Mainul Mizan, Ragib Hasan, and Alan Sprague	
Book Review: The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics (John Sammons)	83
Stephen Larson	
Subscription Information	87
Announcements and Job Postings	89

From the Editor-in-Chief

One cannot deny the importance of what we are doing at *JDFSL*. We are truly bridging various disciplines in one publication venue. This is reflected not only in this Journal's issue, but also in the diverse backgrounds of both our authors and editorial board.

I am honored and excited to have been appointed the new editor-in-chief of *JDFSL*, and I would like to take the opportunity to share with you our goals for the upcoming year:

1. *Work on increasing the indexing and impact factor of the Journal*

This is of critical importance to the Journal and our peers. Our Journal is indexed by ProQuest and EBSCOhost for several years already. Currently, we are working on getting the Journal indexed by other prominent venues as well. We strive to become the strongest indexed, and most impactful journal in our domain.

2. *Establish JDFSL as the premiere multidisciplinary journal in cyber forensics*

JDFSL is currently known as a multidisciplinary journal. We are working hard to ensure that this mission is strongly supported, and focused. Our new slogan is *Where the world discovers multidisciplinary cyber forensics*. The bioethicist Dr. Glenn McGee inspired the idea for this slogan while I was conversing with him on the vision for *JDFSL*. Dr. Glenn McGee is the former editor-in-chief of the *American Journal of Bioethics*.

3. *Identify ways to enable stronger opportunities for open access*

All prior publications up to Volume 7 had been designated as open access. We are in the process of establishing relationships with several high-impact conferences, and we are also working on several special issue ideas that we shall announce in the near future.

4. *Have an impactful editorial board*

We plan to host a virtual editorial board meeting at least once a year to garner the board's feedback on the Journal's activities. We really want the editorial board to play a critical role in this Journal's success and future direction.

I am confident that with the help of Glenn Dardick, Linda Lau, and the editorial board, we will achieve the goals that I outlined for this year.

In this issue

This issue consists of five blind peer-reviewed publications and a book review. Chad Steel wrote the first paper, titled *Idiographic Digital Profiling: Behavioral Analysis based on Digital Forensics*. This paper is of critical importance to the community for both scientists and practitioners alike because it opens the doors to debates, ideas, and studies around the challenges of behavioral analysis when applied to digital forensics.

The second paper, titled *Personal Denial of Service (PDOS) Attacks: A Discussion and Exploration of a New Category of Cyber Crime*, was written by Michael Bartolacci, Larry LeBlanc, and Ashley Podhradsky. This paper presents a strong contribution to our domain by identifying a new type of a denial of service attack that targets both individuals and groups.

The third paper, titled *On Cyber Attacks and Signature Based Intrusion Detection from MODBUS Based Industrial Control Systems*, was written by Wei Gao and Thomas Morris. This paper is important for a multitude of reasons. First, a lot of hype and talk has been discussed with regards to SCADA security, but not much experimental work has been presented on this matter. The work in this paper discussed 28 cyber attacks against industrial control systems and how to detect and respond to these attacks.

The fourth paper, titled *Using Internet Artifacts to Profile a Child Pornography Suspect*, was written by Marcus K Rogers and Kathryn Seigfried-Spellar. This paper is seminal because it is one of the first contributions in our domain to have used behavioral analysis as a form of evidence that was submitted in a court case. They present both a methodology and a real case study in which browser URLs were used to profile the suspect. This is of strong value to our domain, and future work can expand on their proposed methodology.

The last paper, titled *Hot Zone Identification: Analyzing Effects of Sampling on Spam Clustering*, was written by Rasib Khan, Mainul Mizan, Ragib Hasan, and Alan Sprague. They present a sampling technique that reduces the amount of spam data that needs to be analyzed to produce reliable results. This is a very timely topic given the intersection of Big-Data, cyber forensics, and cyber security.

Ibrahim (Abe) Baggili PhD
Chief Editor, *JDFSL*
IBaggili@newhaven.edu