



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

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

Volume 10

Article 6

2015

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

(2015) "Front Matter," *Journal of Digital Forensics, Security and Law*: Vol. 10 , Article 6.

DOI: <https://doi.org/10.58940/1558-7223.1355>

Available at: <https://commons.erau.edu/jdfsl/vol10/iss1/6>

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 | **PURDUE**
Aeronautical University | UNIVERSITY

(c)ADFSL



JDFSL

The Journal of
Digital Forensics,
Security and Law



Volume 10, Number 1
2015

JDFSL

The Journal of Digital Forensics, Security and Law

Volume 10, Number 1 (2015)

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 Breitingner
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 © 2015 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
A Survey of Botnet Detection Techniques by Command and Control Infrastructure	7
Thomas S. Hyslip, Sc.D., and Jason M. Pittman, Sc.D.	
Data Loss Prevention and Control: Inside Activity Incident Monitoring, Identification, and Tracking in Healthcare Enterprise Environments	27
Manghui Tu, Kimberly Spoa-Harty, and <u>Liangliang Xiao</u>	
To License or Not to License Reexamined: An Updated Report on State Statutes Regarding Private Investigators and Digital Examiners	45
Thomas Lonardo, Alan Rea, and Doug White	
Litigation Holds: Past, Present and Future Directions	57
Milton Luoma and Vicki M. Luoma	
Subscription Information	69
Announcements and Upcoming Events	71

FROM THE EDITOR-IN-CHIEF

Welcome to JDFSL's first issue for 2015! First, I would like to thank our editorial board, reviewers, and the JDFSL team for bringing this issue to life.

It has been a big year for JDFSL as the journal continues to progress. We are continuing our indexing efforts for the journal and we are getting closer with some of the major databases.

In this issue, we continue our multidisciplinary tradition. The first paper *A survey of botnet detection techniques by command and control infrastructure*, the authors reviewed the history of botnets and botnet detection techniques illustrating that traditional techniques are passive, relying on honeypots, which are not effective at detecting peer-to-peer and decentralized botnets even though recent work has illustrated that hierarchical clustering of data flow and the use of machine learning are effective in detecting botnet peer-to-peer traffic.

In the second paper *Data loss prevention and control: Inside activity incident monitoring, identification, and tracking in healthcare enterprise environments*, the authors discuss the timely issue of healthcare data security in enterprise environments. The authors provide a novel approach to model internal threats, especially insider activities. They then investigated threat vectors and potential data loss paths in healthcare enterprise environments where vectors are enumerated and data loss statistics for some threat vectors were collected. They then disclosed a method to provide guidance for inside activity identification, tracking and reconstruction using evidence trees.

In the third paper *To license or not to license reexamined: An updated report on state statutes regarding private investigators and digital examiners*, the authors provided an update to their work in 2012 where they examined statutes that regulate, license, and enforce investigative functions in each U.S. state. Their results indicated that few state statutes explicitly differentiate between Private Investigators (PI) and Digital Examiners (DE). There seems to also be a growing trend in which some states are changing definitions or moving to exempt DEs from PI licensing requirements.

The fourth paper *Litigation holds: Past, a present and future direction* discusses litigation hold challenges with electronically stored information. The author points out that litigation holds best practices were created to prevent routine destruction of documents and to preserve documents relevant to a litigation hold. The author further explains that for the first seven years of the new e-discovery rules, litigants who failed to preserve data received severe sanctions for spoliation of evidence and that recent cases and proposed new rules have reversed the trend of stringent standards requiring litigation holds. The author argues that this has challenged the state of the law in spite of the fact that accepted best practices do recommend high standards for litigation holds.

Finally, we are extremely proud of the multidisciplinary nature of this issue once more, spanning Digital Forensics, Security and Law. We will continue on this path as we move forward because it is our core belief at JDFSL that our domain is multidisciplinary and that impactful research should tackle cyber issues from different perspectives.

Sincerely,

Dr. Ibrahim Baggili PhD Editor-in-Chief