The Journal of Digital Forensics, Security and Law

Volume 9, Number 2 (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
Bloomburg University
Pennsylvania, USA

David P. Biros, PhD
Oklahoma State University
Oklahoma, 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 Craigier, PhD, CISSP, CCIFP
Daytona State College
Florida, USA

Glenn S. Dardick, PhD, CCE, CCIFP
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

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

Joshua James, PhD
Soochunhyang 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, CCIFP, 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, CCIFP
University of Pretoria
South Africa

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

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

John Riley, PhD
Bloomburg University
Pennsylvania, USA

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

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

Vassil Roussev, PhD
University of New Orleans
Louisiana, 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

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

© 2014 ADFSL
# Technical Program Committee

**General Chair - ICDF2C and SADFE**

Ibrahim Baggili  
University of New Haven  
Director of UNHcFREG

**ICDF2C TPC Chairs**

Frank Breitinger  
University of New Haven  
Joshua I. James  
Digital Forensic Investigation Research Laboratory  
Soon Chun Hyang University

**SADFE TPC Chairs**

Ricci Leong  
University of Hong Kong  
Andrew Marrington  
Zayed University

**Grey Eminence**

Eugene Spafford  
CERIAS, Purdue University

**Publicity Chair**

David Baker  
MITRE

## TPC Members

<table>
<thead>
<tr>
<th>Name</th>
<th>Institution</th>
<th>Country</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frank Adelstein</td>
<td>ATC-NY</td>
<td></td>
</tr>
<tr>
<td>Irfan Ahmed</td>
<td>University of New Orleans</td>
<td>Bangladesh</td>
</tr>
<tr>
<td>Ibrahim Baggili</td>
<td>University of New Haven (UNHcFREG)</td>
<td></td>
</tr>
<tr>
<td>Dave Baker</td>
<td>MITRE</td>
<td></td>
</tr>
<tr>
<td>Nicole Beebe</td>
<td>University of Texas at San Antonio</td>
<td></td>
</tr>
<tr>
<td>Harlan Carvey</td>
<td>Dell SecureWorks</td>
<td></td>
</tr>
<tr>
<td>K P Chow</td>
<td>University of Hong Kong</td>
<td></td>
</tr>
<tr>
<td>Fred Cohen</td>
<td>Management Analytics</td>
<td></td>
</tr>
<tr>
<td>Dave Dampier</td>
<td>Mississippi State University</td>
<td></td>
</tr>
<tr>
<td>Glenn Dardick</td>
<td>Longwood University</td>
<td></td>
</tr>
<tr>
<td>Barbara Endicott-Popovský</td>
<td>University of Washington</td>
<td></td>
</tr>
<tr>
<td>Ernest Foo</td>
<td>Queensland University of Technology</td>
<td></td>
</tr>
<tr>
<td>Simson Garfinkel</td>
<td>Naval Postgraduate School</td>
<td></td>
</tr>
<tr>
<td>Pavel Gladyshev</td>
<td>University College Dublin</td>
<td></td>
</tr>
<tr>
<td>Farkhund Iqbal</td>
<td>Zayed University</td>
<td></td>
</tr>
<tr>
<td>Meng-Chow Kang</td>
<td>Cisco Systems, Inc</td>
<td></td>
</tr>
<tr>
<td>Thomas Kemmerich</td>
<td>University of Bremen, IS-Bremen</td>
<td></td>
</tr>
<tr>
<td>Michael Losavio</td>
<td>University of Louisville</td>
<td></td>
</tr>
<tr>
<td>James Lyles</td>
<td>NIST</td>
<td></td>
</tr>
<tr>
<td>Richard Mislav</td>
<td>Rochester Institute of Technology</td>
<td></td>
</tr>
<tr>
<td>Stig Mjolsnes</td>
<td>Norwegian Univ. of Science and Technology NTNU</td>
<td></td>
</tr>
<tr>
<td>David Naccache</td>
<td>Panthéon-Assas University</td>
<td></td>
</tr>
<tr>
<td>Bruce Nikkel</td>
<td>Director of IT and Forensics</td>
<td></td>
</tr>
<tr>
<td>Martin Olivier ICSA</td>
<td>University of Pretoria</td>
<td></td>
</tr>
<tr>
<td>Martin Olivier ICSA</td>
<td>University of Pretoria</td>
<td></td>
</tr>
<tr>
<td>Marcus Rogers</td>
<td>Purdue</td>
<td></td>
</tr>
<tr>
<td>Vassil Roussev</td>
<td>University of New Orleans</td>
<td></td>
</tr>
<tr>
<td>Neil Rowe</td>
<td>U.S. Naval Postgraduate School</td>
<td></td>
</tr>
<tr>
<td>Shahzad Saleem</td>
<td>Stockholm University</td>
<td></td>
</tr>
<tr>
<td>Bradley Schatz</td>
<td>Queensland University of Technology, Australia</td>
<td></td>
</tr>
<tr>
<td>Kathryn Seigfried-Spellar</td>
<td>The University of Alabama</td>
<td></td>
</tr>
<tr>
<td>Hossain Shahriar</td>
<td>Kennesaw State University</td>
<td></td>
</tr>
<tr>
<td>Jill Slay</td>
<td>Australian Centre for Cyber Security</td>
<td></td>
</tr>
<tr>
<td>Timothy Vidas</td>
<td>Carnegie Mellon University</td>
<td></td>
</tr>
<tr>
<td>David Wolinsky</td>
<td>Yale University</td>
<td></td>
</tr>
<tr>
<td>York Yannikos</td>
<td>Fraunhofer SIT</td>
<td></td>
</tr>
</tbody>
</table>
Conference Sponsors
# Contents

<table>
<thead>
<tr>
<th>JDFSL Editorial Board</th>
<th>.......................................................................................................................... 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICDF2C 2014 Technical Program Committee</td>
<td>......................................................................................................................... 3</td>
</tr>
<tr>
<td>From the Editor-in-Chief</td>
<td>....................................................................................................................................... 7</td>
</tr>
<tr>
<td>On Identities in Modern Networks</td>
<td>.............................................................................................................................. 9</td>
</tr>
<tr>
<td>Libor Polčák, Radek Hranický and Tomáš Martinek</td>
<td></td>
</tr>
<tr>
<td>File Detection on Network Traffic using Approximate Matching</td>
<td>................................................................. 23</td>
</tr>
<tr>
<td>Frank Breitinger and Ibrahim Baggili</td>
<td></td>
</tr>
<tr>
<td>Accurate Modeling of the Siemens S7 SCADA Protocol for Intrusion Detection and Digital Forensics</td>
<td>................................................................. 37</td>
</tr>
<tr>
<td>Amit Kleinman and Avishai Wool</td>
<td></td>
</tr>
<tr>
<td>Understanding Computer Forensics Requirements in China via the “Panda Burning Incense” Virus Case</td>
<td>................................................................. 51</td>
</tr>
<tr>
<td>Frank Law, K P Chow and Y H Mai</td>
<td></td>
</tr>
<tr>
<td>Multi-Stakeholder Case Prioritization in Digital Investigations</td>
<td>.......................................................................................................................... 59</td>
</tr>
<tr>
<td>Joshua I. James</td>
<td></td>
</tr>
<tr>
<td>Forensics of Software Copyright Infringement Crimes: The Modern POSAR Test Juxtaposed with the Dated AFC Test</td>
<td>.......................................................................................................................... 73</td>
</tr>
<tr>
<td>P Vinod Bhattachiripad</td>
<td></td>
</tr>
<tr>
<td>Leveraging Decentralisation to Extend the Digital Evidence Acquisition Window: Case Study on BitTorrent Sync</td>
<td>.......................................................................................................................... 85</td>
</tr>
<tr>
<td>Mark Scanlon, Jason Farina, Nhien-An Le-Khac and Tahar Kechadi</td>
<td></td>
</tr>
<tr>
<td>Fast RTP Detection and Codecs Classification in Internet Traffic</td>
<td>.......................................................................................................................... 101</td>
</tr>
<tr>
<td>Petr Matousek, Ondrej Rysavy and Martin Kmet</td>
<td></td>
</tr>
<tr>
<td>Developing A Conceptual Framework for Modeling &quot;Deviant Cyber Flash Mob&quot;: A Socio-Computational Approach Leveraging Hypergraph Constructs</td>
<td>.......................................................................................................................... 113</td>
</tr>
<tr>
<td>Samer Al-Khateeb and Nitin Agarwal</td>
<td></td>
</tr>
<tr>
<td>AUDIT: Automated Disk Investigation Toolkit</td>
<td>.......................................................................................................................... 129</td>
</tr>
<tr>
<td>Umit Karabiyik and Sudhir Aggarwal</td>
<td></td>
</tr>
<tr>
<td>Exploring Forensic Implications of the Fusion Drive</td>
<td>.......................................................................................................................... 145</td>
</tr>
<tr>
<td>Shruti Gupta and Marcus Rogers</td>
<td></td>
</tr>
<tr>
<td>An Efficient Similarity Digests Database Lookup - A Logarithmic Divide and Conquer Approach</td>
<td>.......................................................................................................................... 155</td>
</tr>
<tr>
<td>Frank Breitinger, Christian Rathgeb and Harald Baier</td>
<td></td>
</tr>
<tr>
<td>Erin Smith Crabb</td>
<td></td>
</tr>
<tr>
<td>Relating Admissibility Standards for Digital Evidence to Attack Scenario Construction</td>
<td>.......................................................................................................................... 181</td>
</tr>
<tr>
<td>Changwei Liu, Anoop Singhal and Duminda Wijesekera</td>
<td></td>
</tr>
</tbody>
</table>
Contents (continued)

Evidentiary Power and Propriety of Digital Identifiers and the Impact on Privacy Rights in the United States ................................................................. 197
Michael Losavio and Deborah Keeling

Effects of the Factory Reset on Mobile Devices ...................................................... 205
Riqui Schwamm and Neil Rowe

Testing Framework for Mobile Device Forensics Tools ......................................... 221
Maxwell Anobah, Shahzad Saleem and Oliver Popov

Announcements and Upcoming Events ................................................................. 235
FROM THE EDITOR-IN-CHIEF

We are proud to share with you this special edition issue of the JDFSL. This year, JDFSL partnered with both the 6th International Conference on Digital Forensics and Cyber Crime (ICDF2C) and Systematic Approaches to Digital Forensic Engineering (SADFE)—two prominent conferences in our field that were co-hosted. Fifty-three papers were submitted, and the Technical Program Committee accepted only 17 after a rigorous review process.

A lot has happened since our last issue. We have accomplished a variety of goals. We list some of them below:

1. Our journal is now fully indexed with Open Academic Journal Index (OAJI)
2. All our issues are now indexed by DBLP
3. We still accept submissions in PDF format but can now accept the final accepted manuscript in either LaTeX or Word
4. We now have a new upgraded general Website more integrated with the submission website for access to published manuscripts
5. We were granted access to archive our journal with arxiv.org
6. All our issues are now open access and now made available under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License
7. The JDFSL continues its policy of not requiring authors to pay a fee in order to publish in the regular issues of the JDFSL. The JDFSL is indeed very grateful to our many sponsors who make this possible.
8. We have added many new members to our editorial board increasing our scope and depth

We hope to continue to forge strong relationships with other high-impact conferences so that we can provide research academics and practitioners the possibility of publishing high impact articles in a quality peer-reviewed open access form.

In this special issue, we are especially proud of the quality of the published research presented. It reflects our tradition of remaining a truly multi-disciplinary publication venue.

The seventeen papers in this issue can be categorized into the following themes: (1) Network Forensics; (2) Digital Investigations and Case Studies; (3) Online/Internet Forensics; (4) Digital Investigations–Tools and Approaches; (5) Digital Forensic Analysis Techniques; (6) Laws and Standards; and (6) Small Scale Digital Device Forensics.

Besides the diversity of the topics in this issue, we also note the international nature of our authors. Papers published in this issue, in no particular order, come from authors in the following countries: (1) United States; (2) Czech Republic; (3) Israel; (4) Hong Kong; (5) South Korea; (6) India; and (7) Ireland. However, the conference
received audience from fourteen countries, and eight US states—which we hope increases JDFS\'s international visibility.

At this point, I would like to thank the hard work of our Associate Editor-in-Chief Linda Lau, our publisher Glenn Dardick and our Administrative Assistant Alex Greene for working hard to make sure this issue is released in a timely fashion.

I would also like to thank our new board members and the TPC committee from the ICDF2C and SADFE conferences for helping ensure a quality peer-reviewed process for this edition. I would like to especially thank the TPC Chairs Joshua James, Frank Breitinger, Andrew Marrtington and Ricci Ieong.

We hope that with all these activities, we continue to solidify our goal of making JDFS\ the top venue for the publication of open-access, multidisciplinary cyber forensics and security research.

Sincerely,
Ibrahim (Abe) Baggili PhD
Editor-in-Chief, JDFS\nIBaggili@newhaven.edu