Front Matter

Follow this and additional works at: https://commons.erau.edu/jdfs

Part of the Computer Law Commons, and the Information Security Commons

Recommended Citation

DOI: https://doi.org/10.58940/1558-7223.1343
Available at: https://commons.erau.edu/jdfs/vol9/iss2/19

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.
The Journal of Digital Forensics, Security and Law

6th International Conference on
DIGITAL FORENSICS & CYBER CRIME

CO-HOSTED WITH THE
Systematic Approaches to Digital Forensic Engineering (SADFE)

New Haven, CT • September 18–20 2014

ORGANIZED BY:
University of New Haven
Tagliatela College of Engineering

ICDF2C Special Issue
Volume 9 Number 2
2014
# 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**  
Rici 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>Institution</th>
<th>Institution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frank Adelstein</td>
<td>ATC-NY</td>
<td>Glenn Dardick</td>
<td>James Lyles</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Longwood University</td>
<td>NIST</td>
</tr>
<tr>
<td>Irfan Ahmed</td>
<td>University of New Orleans</td>
<td>Barbara Endicott-Popovskij</td>
<td>Richard Mislante</td>
</tr>
<tr>
<td></td>
<td></td>
<td>University of Washington</td>
<td>Rochester Institute of Technology</td>
</tr>
<tr>
<td>Ibrahim Baggili</td>
<td>University of New Haven (UNHcFREG)</td>
<td>Ernest Foo</td>
<td>Stig Mjolsnes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Queensland University of Technology</td>
<td>Norwegian Univ. of Science and Technology NTNU</td>
</tr>
<tr>
<td>Dave Baker</td>
<td>MITRE</td>
<td>Simson Garfinkel</td>
<td>David Naccache</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Naval Postgraduate School</td>
<td>Panthéon-Assas University</td>
</tr>
<tr>
<td>Nicole Beebe</td>
<td>University of Texas at San Antonio</td>
<td>Pavel Gladysehv</td>
<td>Bruce Nikkel</td>
</tr>
<tr>
<td></td>
<td></td>
<td>University College Dublin</td>
<td>Director of IT and Forensics</td>
</tr>
<tr>
<td>Harlan Carvey</td>
<td>Dell SecureWorks</td>
<td>Farkhund Iqbal</td>
<td>Martin Olivier ICSA</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Zayed University</td>
<td>University of Pretoria</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Timothy Vidas</td>
</tr>
<tr>
<td>K P Chow</td>
<td>University of Hong Kong</td>
<td>Meng-Chow Kang</td>
<td>Marcus Rogers</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Cisco Systems, Inc</td>
<td>Purdue</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>David Wolinsky</td>
</tr>
<tr>
<td>Fred Cohen</td>
<td>Management Analytics</td>
<td>Thomas Kemmerich</td>
<td>Vassil Roussev</td>
</tr>
<tr>
<td></td>
<td></td>
<td>University of Bremen, IS-Bremen</td>
<td>University of New Orleans</td>
</tr>
<tr>
<td>Dave Dampier</td>
<td>Mississippi State University</td>
<td>Michael Losavio</td>
<td>Neil Rowe</td>
</tr>
<tr>
<td></td>
<td></td>
<td>University of Louisville</td>
<td>U.S. Naval Postgraduate School</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

© 2014 ADFSL
Conference Sponsors
Contents

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