Front Matter
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

European Alliance for Innovation

ICDF2C Special Issue
Volume 9 Number 2
2014
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. Brooks, 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, CCDF
Daytona State College
Florida, USA
Glenn S. Dardick, PhD, CCE, CCDF
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 Gansch, PhD, PE, CISSP
Defiance College
Ohio, USA
Joshua James, PhD
Soonchunhyang University
South Korea
Andy Jones, PhD
University of South Wales
UK
Eri 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, CCDF
University of Pretoria
South Africa

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

Frank Adelstein
ATC-NY

Glenn Dardick
Longwood University

James Lyles
NIST

Shahzad Saleem
Stockholm University

Irfan Ahmed
University of New Orleans

Barbara Endicott-Popovsky
University of Washington

Richard Mislav
Rochester Institute of Technology

Bradley Schatz
Queensland University of Technology, Australia

Ibrahim Baggili
University of New Haven (UNHcFREG)

Ernest Foo
Queensland University of Technology

Stig Mjolsnes
Norwegian Univ. of Science and Technology NTNU

Kathryn Seigfried-Spellar
The University of Alabama

Dave Baker
MITRE

Simson Garfinkel
Naval Postgraduate School

David Naccache
Panthéon-Assas University

Hossain Shahriar
Kennesaw State University

Nicole Beebe
University of Texas at San Antonio

Pavel Gladyshev
University College Dublin

Bruce Nikkel
Director of IT and Forensics

Jill Slay
Australian Centre for Cyber Security

Harlan Carvey
Dell SecureWorks

Farkhund Iqbal
Zayed University

Martin Olivier ICSA
University of Pretoria

Timothy Vidas
Carnegie Mellon University

K P Chow
University of Hong Kong

Meng-Chow Kang
Cisco Systems, Inc

Marcus Rogers
Purdue

David Wolinsky
Yale University

Fred Cohen
Management Analytics

Thomas Kemmerich
University of Bremen, IS-Bremen

Vassil Roussev
University of New Orleans

York Yannikos
Fraunhofer SIT

Dave Dampier
Mississippi State University

Michael Losavio
University of Louisville

Neil Rowe
U.S. Naval Postgraduate School

© 2014 ADFSL
Conference Sponsors

MICROSYSTEMATION

cellebrite
delivering mobile expertise

University of New Haven
TAGLIATELA COLLEGE OF ENGINEERING

TAKE A BYTE OUT OF CRIME
www.UNHcFREG.com

JONES & BARTLETT LEARNING
An AscendLearning Company

HTCIA
HIGH TECHNOLOGY CRIME INVESTIGATION ASSOCIATION
CONNECTICUT CHAPTER

CREATE-NET

EAI European Alliance for Innovation

JDFSL The Journal of Digital Forensics, Security and Law

© 2014 ADFSL
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 Martinek

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, Nhien-An Le-Khac and Tahar Kechadi

Fast RTP Detection and Codecs Classification in Internet Traffic ..................................................... 101
Petr Matousek, Ondrej 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 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 JDFSL’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 Marrington and Ricci Ieong.

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

Sincerely,
Ibrahim (Abe) Baggili PhD
Editor-in-Chief, JDFSL
IBaggili@newhaven.edu