



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

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

Volume 9

Article 21

2014

Back 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) "Back Matter," *Journal of Digital Forensics, Security and Law*: Vol. 9 , Article 21.

DOI: <https://doi.org/10.58940/1558-7223.1344>

Available at: <https://commons.erau.edu/jdfsl/vol9/iss2/21>

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



Announcements and Upcoming Events

The 10th ADFSL Conference on Digital Forensics, Security and Law

Daytona Beach, Florida USA
Embry-Riddle Aeronautical University
May 19-21, 2015



<http://www.digitalforensics-conference.org>

The **ADFSL Conference on Digital Forensics, Security and Law** is the official annual conference of the ADFSL, the Association of Digital Forensics Security and Law. The Conference is a unique and innovative event organized and managed by the Association of Digital Forensics, Security and Law (ADFSL).

The first annual conference of the ADFSL Conference on Digital Forensics, Security and Law was held in Las Vegas, Nevada, USA on April 20-21, 2006. The conference was created on the premise that digital forensics goes beyond digital evidence. The mission of the conference is to significantly expand the domain of digital forensics research to a wide and eclectic audience of academics, consultants and executives who are involved in the curriculum, research and use of digital forensics.

The conference provides an avenue for the presentation and discussion of original research and curriculum about digital forensics and its relationship to security and law. Contributions are particularly welcome which analyze the results of interdisciplinary research and relate to the intersection of theory, method and empirical findings. Of interest will be manuscripts, which present the theoretical concepts of the development, organization, and dissemination of digital forensics concepts. Further, conference proceedings will be made available to include the results of research and case studies that advance the practice and understanding of digital forensics methods and techniques to support efficient and effective investigations.

Conference submissions are double blind refereed and provide a forum for high quality research, communication and debate on the subject of digital forensics and directly related fields.

Journal of Digital Forensics, Security and Law

Volume 9, Number 2

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 Breitingner 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	
Mutli-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 Construct	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 Breitingner, Christian Rathgeb and Harald Baier	
“Time for Some Traffic Problems”: Enhancing E-Discovery and Big Data Processing Tools with Linguistic Methods for Deception Detection	167
Erin Smith Crabb	
Relating Admissibility Standards for Digital Evidence to Attack Scenario Construction	181
Changwei Liu, Anoop Singhal and Duminda Wijesekera	
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