Editorial Board

Ozgur Akan  
*Middle East Technical University, Ankara, Turkey*

Paolo Bellavista  
*University of Bologna, Italy*

Jiannong Cao  
*Hong Kong Polytechnic University, Hong Kong*

Falko Dressler  
*University of Erlangen, Germany*

Domenico Ferrari  
*Università Cattolica Piacenza, Italy*

Mario Gerla  
*UCLA, USA*

Hisashi Kobayashi  
*Princeton University, USA*

Sergio Palazzo  
*University of Catania, Italy*

Sartaj Sahni  
*University of Florida, USA*

Xuemin (Sherman) Shen  
*University of Waterloo, Canada*

Mircea Stan  
*University of Virginia, USA*

Jia Xiaohua  
*City University of Hong Kong, Hong Kong*

Albert Zomaya  
*University of Sydney, Australia*

Geoffrey Coulson  
*Lancaster University, UK*
Preface

As we continue our journey into the twenty-first century, our reliance on technology and cyber infrastructure has increased at an incredible pace. This fact is not lost on those who wish to use technology for criminal activities. If we believe the current statistics that are available, the frequency and prevalence of cybercrime have reached epidemic proportions. The estimated loss as a result of cyber criminal activity is hundreds of millions of dollars annually. Cybercrime is undoubtedly the new transnational criminal activity with no boundaries or borders. As such, it is important that the international community (industry, government, law enforcement, and academia) come together in order to share ideas and possible solutions to help us deal with this global, increasing risk.

This volume contains papers presented at the 4th Annual International ICST Conference on Digital Forensics and Cybercrime (ICDF2C 2012), held October 25–26 2012, in Lafayette, Indiana, USA. ICDF2C is unique in that it brings together the various constituents in the digital forensic field (e.g., academia, government, law enforcement, business). The focus of the conference is on the applied nature of digital forensics and it provides an opportunity for researchers and practitioners to interact and discuss the various challenges and potential solutions.

The 20 papers presented in this volume represent an excellent cross section of the current work in the field of digital forensics. The topics covered range from behavior and law, to mobile devices, malware and new developments. The papers went through a double-blind peer review process. Three reviewers selected from the Technical Program Committee reviewed each paper.

We would like to thank those individuals who volunteered their time to be on the Technical Program Committee, as well as all of the people who volunteered to be Chairs of the various sections. The success of the conference was in large part due to the efforts of the staff at EAI, with a special thank you for the tireless efforts of Erica Polini, who kept us all on track.

Marcus Rogers
Kathryn C. Seigfried-Spellar
Organization

General Chair
Marcus Rogers Purdue University, USA

Technical Program Committee Chairs
Pavel Gladyshev University College Dublin, Ireland
Eugene Spafford Purdue University, USA

Publicity Co-chairs
Ibrahim Baggili Zayed University, United Arab Emirates
Sanjay Goel University at Albany, State University of New York, USA

Industry Track Chair
Fred Kerr USA

Local Chair
Tejashree Datar Purdue University, USA

Conference Manager
Erica Polini EAI, Italy

Workshop Chair
Frank Adelstein ATC-NYC, USA

Publications Chairs
Nasir Memon Polytechnic Institute of New York University, USA
Andrew Marrington Zayed University, United Arab Emirates

Demos and Tutorials Chair
John Sammons Marshall University, USA

Law Enforcement Chair
Lt. Chuck Cohen Indiana State Police, USA
### VIII Organization

#### Legal Chair

Mike Losavio  
University of Louisville, USA

#### Behavioral Sciences Chair

Kate Seigfried-Spellar  
Seattle University, USA

#### Steering Committee

<table>
<thead>
<tr>
<th>Name</th>
<th>University/Institution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pavel Gladyshev</td>
<td>University College, Dublin</td>
</tr>
<tr>
<td>Marcus Rogers</td>
<td>Purdue University, USA</td>
</tr>
<tr>
<td>Ibrahim Baggili</td>
<td>Zayed University, United Arab Emirates</td>
</tr>
<tr>
<td>Sanjay Goel</td>
<td>University at Albany, State University of New York, USA</td>
</tr>
</tbody>
</table>

#### Technical Program Committee

<table>
<thead>
<tr>
<th>Name</th>
<th>University/Institution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ibrahim Baggili</td>
<td>Zayed University, United Arab Emirates</td>
</tr>
<tr>
<td>Felix Balado</td>
<td>University College Dublin, Ireland</td>
</tr>
<tr>
<td>Florian Buchholz</td>
<td>James Madison University, USA</td>
</tr>
<tr>
<td>Glenn Dardick</td>
<td>Longwood University, USA</td>
</tr>
<tr>
<td>Katrin Franke</td>
<td>Gjovik University College, Norway</td>
</tr>
<tr>
<td>Felix Freiling</td>
<td>University of Mannheim, Germany</td>
</tr>
<tr>
<td>Sandra Frings</td>
<td>Fraunhofer IAO, Germany</td>
</tr>
<tr>
<td>Zeno Geradts</td>
<td>Netherlands Forensic Institute, The Netherlands</td>
</tr>
<tr>
<td>Pavel Gladyshev</td>
<td>University College Dublin, Ireland</td>
</tr>
<tr>
<td>Sanjay Goel</td>
<td>University at Albany, State University of New York, USA</td>
</tr>
<tr>
<td>Andrew Harbison</td>
<td>Grant Thornton, Ireland</td>
</tr>
<tr>
<td>Michael Harris</td>
<td>Ernst &amp; Young, Ireland</td>
</tr>
<tr>
<td>Andrew Jones</td>
<td>Khalifa University, United Arab Emirates</td>
</tr>
<tr>
<td>Anthony Keane</td>
<td>Blanchardstown Institute of Technology, Ireland</td>
</tr>
<tr>
<td>Tahar Kechadi</td>
<td>University College Dublin, Ireland</td>
</tr>
<tr>
<td>Chang-Tsun Li</td>
<td>University of Warwick, UK</td>
</tr>
<tr>
<td>Juha Lampinen</td>
<td>National Bureau of Investigation, Finland</td>
</tr>
<tr>
<td>Vivienne Mee</td>
<td>Rits Computer Forensics, Ireland</td>
</tr>
<tr>
<td>Nasir Memon</td>
<td>Polytechnic Institute of New York University, USA</td>
</tr>
<tr>
<td>Stig Mjolsnes</td>
<td>Norwegian University of Science and Technology, Norway</td>
</tr>
<tr>
<td>George Mohay</td>
<td>Queensland University of Technology, Australia</td>
</tr>
<tr>
<td>Bruce Nikkel</td>
<td>UBS, Switzerland</td>
</tr>
<tr>
<td>Slim Rekhis</td>
<td>Institute of Technology in Communications, Tunisia</td>
</tr>
</tbody>
</table>
Marcus Rogers Purdue University, USA
John Sheppard Waterford Institute of Technology, Ireland
Eugene Spafford CERIAS - Purdue University, USA
Bhadran V.K. Resource Centre for Cyber Forensics, India
Vinod Bhattathiripad Farouq Institute of Management Studies, India
Oscar Vermaas Netherlands National Police Force, The Netherlands
Svein Willassen Norwegian University of Science and Technology, Norway
Gregg Gunsch Defiance College, USA
Tim Wedge Defiance College, USA
James Lyle NIST, USA
Nicole Beebe University of Texas San Antonio, USA
# Table of Contents

## Cloud Investigations

Cloud Computing Reference Architecture and Its Forensic Implications: A Preliminary Analysis ........................................... 1  
*Keyun Ruan and Joe Carthy*

Cloud Forensic Maturity Model .................................... 22  
*Keyun Ruan and Joe Carthy*

Identifying Remnants of Evidence in the Cloud ................. 42  
*Jeremy Koppen, Gerald Gent, Kevin Bryan, Lisa DiPippo, Jillian Kramer, Marquita Moreland, and Victor Fay-Wolfe*

## Malware

On Improving Authorship Attribution of Source Code ............. 58  
*Matthew F. Tennyson*

## Behavioral

Towards Automated Malware Behavioral Analysis and Profiling for Digital Forensic Investigation Purposes ....................... 66  
*Ahmed F. Shosha, Joshua I. James, Alan Hannaway, Chen-Ching Liu, and Pavel Gladyshev*

Measuring the Preference of Image Content for Self-reported Consumers of Child Pornography ........................................... 81  
*Kathryn C. Seigfried-Spellar*

## Law

When Should Virtual Cybercrime Be Brought under the Scope of the Criminal Law? .................................................. 109  
*Litska Strikwerda*
New Developments in Digital Forensics

Research Trends in Digital Forensic Science: An Empirical Analysis of Published Research .................................................. 144
   Ibrahim Baggili, Afrah BaAbdallah, Deena Al-Safi, and Andrew Marrington

Face Recognition Based on Wavelet Transform and Adaptive Local Binary Pattern .................................................. 158
   Abdallah Mohamed and Roman V. Yampolskiy

Similarity Preserving Hashing: Eligible Properties and a New Algorithm MRSH-v2 ........................................................ 167
   Frank Breitinger and Harald Baier

Investigating File Encrypted Material Using NTFS $logfile ........................................ 183
   Niall McGrath and Pavel Gladyshev

Finding Data in DNA: Computer Forensic Investigations of Living Organisms ...................................................... 204
   Marc B. Beck, Eric C. Rouchka, and Roman V. Yampolskiy

On the Completeness of Reconstructed Data for Database Forensics .... 220
   Oluwasola Mary Adedayo and Martin S. Olivier

Mobile Device Forensics

BlackBerry PlayBook Backup Forensic Analysis ................................. 239
   Mohamed Al Marzougy, Ibrahim Baggili, and Andrew Marrington

ANTS ROAD: A New Tool for SQLite Data Recovery on Android Devices .......................................................... 253
   Lamine M. Aouad, Tahar M. Kechadi, and Roberto Di Russo

   Shahzad Saleem, Oliver Popov, and Oheneba Kwame Appiah-Kubi

Detection of Masqueraded Wireless Access Using 802.11 MAC Layer Fingerprints .................................................. 283
   Christer Idland, Thomas Jelle, and Stig F. Mjølsnes
Cybercrime Investigations

BREDOLAB: Shopping in the Cybercrime Underworld .................. 302
   Daan de Graaf, Ahmed F. Shosha, and Pavel Gladyshev

A Review and Comparative Study of Digital Forensic Investigation
Models ................................................................. 314
   Kwaku Kyei, Pavol Zavarsky, Dale Lindskog, and Ron Ruhl

Author Index ............................................................. 329