Conference on
Digital Forensics, Security and Law
Daytona Beach, Florida
May 15-16, 2017

Conference Chairs

Gary Kessler
gary.kessler@erau.edu
Conference Chair
Embry-Riddle Aeronautical University
Florida, USA

Dr. Jigang Liu
jigang.liu@metrostate.edu
Program Chair
Metropolitan State University
Minnesota, USA

Copyright © 2017 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 ADFSL 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 Dr. Glenn S. Dardick, Association of Digital Forensics, Security and Law, 4350 Candlewood Ln., Ponce Inlet, FL 32127 or emailed to office@adfsl.org.

ISSN 1931-7379
Thank You to Our Sponsors

Daytona State College

Oklahoma State University

Embry-Riddle Aeronautical University

ACE Advanced Cyber Forensics Education

Australian Edith Cowan University

Journal of Digital Forensics, Security and Law
Contents

Committee ........................................................................................................... 4
Schedule ............................................................................................................. 5
Keynote Speaker: Anni R. Coden ........................................................................ 5

Kelihos Botnet: A Never-Ending Saga ................................................................ 9
Arsh Arora*, Max Gannon and Gary Warner

An Accidental Discovery of IoT Botnets and a Method for Investigating Them With a
Custom Lua Dissector ..........................................................................................27
Max Gannon*, Gary Warner and Arsh Arora

Detect Kernel-Mode Rootkits via Real Time Logging & Controlling Memory Access .............................................................................................................39
Irvin Homem, Satoshi Tanda and Igor Korkin*

Harnessing Predictive Models for Assisting Network Forensic Investigations of DNS
Tunnels ................................................................................................................ 79
Irvin Homem* and Panagiotis Papapetrou

Source Anonymization of Digital Images: A Counter–Forensic Attack on PRNU based
Source Identification Techniques ...........................................................................95
Prithviraj Sengupta*, Venkata Udaya Sameer, Ruchira Naskar and Ezhil Kalaimannan

Fast Filtering of Known PNG Files Using Early File Features .................................107
Sean McKeown*, Gordon Russell and Petra Leimich

Defining a Cyber Jurisprudence ............................................................................123
Peter R. Stephenson Ph.D.*

Development of A Professional Code of Ethics in Digital Forensics .........................135
Kathryn C. Seigfried-Spellar*, Marcus Rogers and Danielle M. Crimmins

Detecting Deception in Asynchronous Text .............................................................145
Fletcher Glancy *

Understanding Deleted File Decay on Removable Media Using Differential Analysis ..........................................................153
James H. Jones, Jr.*, Anurag Srivastava, Josh Mosier, Connor Anderson and Seth Buenafe

Downstream Competence Challenges and Legal/Ethical Risks in Digital Forensics ..........................................................167
Michael M. Losavio and Antonio Losavio *

Digital Forensics Tool Selection with Multi-Armed Bandit Problem ........................179
Umit Karabiyik* and Tugba Karabiyik

Exploring Digital Evidence with Graph Theory.......................................................197
Imani Palmer*, Roy Campbell and Boris Gelfand

A New Method for Investigating Crimes Against Children ....................................207
Hallstein Asheim Hansen*, Stig Andersen, Stefan Axelsson and Svein Hopland

* Author Presenting
# ADFSL 2017 Conference Committee

The 2017 ADFSL Conference on Digital Forensics, Security and Law is pleased to have the following as chair of the conference and chair of the conference program committee:

<table>
<thead>
<tr>
<th>Name</th>
<th>Institution</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gary Kessler</td>
<td>Embry-Riddle Aeronautical University</td>
<td><a href="mailto:gary.kessler@erau.edu">gary.kessler@erau.edu</a></td>
</tr>
<tr>
<td>Jigang Liu</td>
<td>Metropolitan State University</td>
<td><a href="mailto:jigang.liu@metrostate.edu">jigang.liu@metrostate.edu</a></td>
</tr>
</tbody>
</table>

The 2017 ADFSL Conference on Digital Forensics, Security and Law is pleased to have the following as members of the program committee:

<table>
<thead>
<tr>
<th>Name</th>
<th>Institution</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mamoun Alazab</td>
<td>Macquarie University Australia</td>
<td></td>
</tr>
<tr>
<td>Gaurav Gupta</td>
<td>Ministry of Communications &amp; Information Technology</td>
<td>india</td>
</tr>
<tr>
<td>John W. Bagby</td>
<td>The Pennsylvania State University Pennsylvania, USA</td>
<td><a href="mailto:m.johnstone@ecu.edu.au">m.johnstone@ecu.edu.au</a></td>
</tr>
<tr>
<td>John Sammons</td>
<td>Asst. Professor at Marshall Univ. West Virginia, USA</td>
<td></td>
</tr>
<tr>
<td>Zubair Baig</td>
<td>Edith Cowan University Western Australia</td>
<td></td>
</tr>
<tr>
<td>Andy. Jones</td>
<td>University of Hertfordshire United Kingdom</td>
<td></td>
</tr>
<tr>
<td>Diane Barrett</td>
<td>Bloomsburg University of Pennsylvania</td>
<td></td>
</tr>
<tr>
<td>Ezhil S. Kalaimannan,</td>
<td>University of West Florida Florida, USA</td>
<td></td>
</tr>
<tr>
<td>Bob Bird</td>
<td>Coventry University Coventry, United Kingdom</td>
<td></td>
</tr>
<tr>
<td>Umit Karabiyik</td>
<td>Sam Houston State University Texas, USA</td>
<td></td>
</tr>
<tr>
<td>Raymond Choo</td>
<td>The University of Texas at San Antonio</td>
<td></td>
</tr>
<tr>
<td>Frederick Lane</td>
<td>Mathom Enterprises, LLC. New York, USA</td>
<td></td>
</tr>
<tr>
<td>Fred Cohen</td>
<td>All.Net &amp; Affiliated Companies California, USA</td>
<td>Stephen Larson Pennsylvania, USA</td>
</tr>
<tr>
<td>David Dampier</td>
<td>Mississippi State University Mississippi, USA</td>
<td>Jigang Liu Metropolitan State University Minnesota, USA</td>
</tr>
<tr>
<td>Gareth Davies</td>
<td>University of South Wales Wales, UK</td>
<td>Thomas Anthony Martin Khalifa University of Science, Technology &amp; Res. (KUSTAR) United Arab Emirates</td>
</tr>
<tr>
<td>Sanjay Goel</td>
<td>University at Albany, SUNY USA</td>
<td>John Riley Bloomburg University Pennsylvania, USA</td>
</tr>
</tbody>
</table>
ADFSL 2017 Conference Program Schedule

MONDAY – MAY 15

8:00 AM  Conference Registration
8:00 AM - 8:55 AM

9:00 AM  Welcoming Remarks
Karen F. Gaines, Ph.D.
Professor and Dean, College of Arts and Sciences
Embry-Riddle Aeronautical University
9:00 AM – 9:15 AM

9:15 AM  Introductions
Glenn S. Dardick CCE, CCFP, Ph.D., Associate Professor of Cybersecurity, Embry-Riddle Aeronautical University, Director of the Association of Digital Forensics, Security and Law and Editor-in-Chief of the Journal of Digital Forensics, Security and Law
9:15 AM – 9:30 AM

9:30 AM  Morning Session 1 - Keynote Speaker: Anni R. Coden
Anni R. Coden Ph.D., IBM Systems G Anomaly Detection Solution
9:30 AM - 10:10 AM

10:10 AM  Break
10:10 AM - 10:25 AM

10:25 AM  Morning Session 2 - Botnet Detection and Prevention
Diane Barrett, Session Chair, Bloomsburg University of Pennsylvania
Arsh Arora, University of Alabama, Birmingham - Kelihos Botnet: A Never-Ending Saga
Max Gannon, University of Alabama, Birmingham - An Accidental Discovery of IoT Botnets and a Method for Investigating Them With a Custom Lua Dissector
10:25 AM - 11:55 PM

12:00 PM  Lunch
12:00 PM - 1:00 PM

1:00 PM  Afternoon Session 1 - Rootkit and Network Security and Forensics
Jigang Liu, Session Chair, Metropolitan State University
Igor Korkin, Independent Researchers, Moscow, Russia - Detect Kernel-Mode Rootkits via Real Time Logging & Controlling Memory Access
Irvin Homem, Department of Computer and Systems Sciences, Stockholm University-Harnessing Predictive Models for Assisting Network Forensic Investigations of DNS Tunnels
1:00 PM - 2:30 PM

2:30 PM  Break
2:30 PM – 2:45 PM

2:45 PM  Afternoon Session 2 - Image Forensics
Joseph Schwerha IV, JD, Session Chair, Director, Entrepreneurial Leadership Center, Associate Professor of Business Law & Technology, Department of Business & Economics, California University of Pennsylvania
Sean McKeown, Napier University- Fast Filtering of Known PNG Files Using Early File Features
2:45 PM - 4:15 PM
ADFSL 2017 Conference Program Schedule

TUESDAY – MAY 16 (morning)

8:00 AM  Conference Registration
          8:00 AM - 8:25 AM

8:30 AM  Tuesday Greeting
          Glenn S. Dardick CCE, CCFP, Ph.D., Associate Professor of Cybersecurity, Embry-Riddle Aeronautical University, Director of the Association of Digital Forensics, Security and Law and Editor-in-Chief of the Journal of Digital Forensics, Security and Law
          8:30 AM - 8:35 AM

8:35 AM  Morning Session 1 - Keynote Speaker: Benjamin Goldsmith
          Benjamin Goldsmith, DHS Office of Cybersecurity & Communications Enterprise Performance Management Office
          8:35 AM - 9:15 AM

9:15 AM  Morning Session 2 - Legal Issues in Cybersecurity and Digital Forensics
          Diane Barrett, Session Chair, Bloomsburg University of Pennsylvania
          Peter R. Stephenson Ph.D., Independent Researcher in Cyber Jurisprudence - Defining a Cyber Jurisprudence
          Kathryn C. Seigfried-Spellar, Purdue University - Development of A Professional Code of Ethics in Digital Forensics
          9:15 AM - 10:45 PM

10:45 AM Break
          10:45 AM - 11:00 AM

11:00 AM Morning Session 3 - File System Forensics
          Philip Craiger Ph.D., CISSP, and CCFP, Session Chair
          Fletcher Glancy, Oklahoma State University - Main Campus - Detecting Deception in Asynchronous Text
          James Jones, George Mason University - Understanding Deleted File Decay on Removable Media Using Differential Analysis
          11:00 AM - 12:30 AM

12:30 PM Lunch
          12:30 PM - 1:30 PM
ADFSL 2017 Conference Program Schedule

TUESDAY - MAY 16 (afternoon)

1:30 PM  Afternoon Session 1 - Digital Forensic Challenges and Tool Selection
Ezhil Kalaimannan, Session Chair, University of West Florida
Antonio Losavio, University of Central Florida - Downstream Competence Challenges and Legal/Ethical Risks in Digital Forensics
Umit Karabiyik, Sam Houston State University - Digital Forensics Tool Selection with Multi-Armed Bandit Problem
1:30 PM - 3:00 PM

3:00 PM  Break
3:00 PM - 3:15 PM

3:15 PM  Afternoon Session 2 - Cyber Investigation and Forensics
Glenn S. Dardick CCE, CCFP, Ph.D., Session Chair, Associate Professor of Cybersecurity, Embry-Riddle Aeronautical University, Director of the Association of Digital Forensics, Security and Law and Editor-in-Chief of the Journal of Digital Forensics, Security and Law
Imani Palmer, University of Illinois at Urbana-Champaign - Exploring Digital Evidence with Graph Theory
Hallstein Asheim Hansen, Norwegian Police - A New Method for Investigating Crimes Against Children
3:15 PM - 4:45 PM

4:45 PM  Conference Close
Glenn S. Dardick CCE, CCFP, Ph.D., Associate Professor of Cybersecurity, Embry-Riddle Aeronautical University, Director of the Association of Digital Forensics, Security and Law and Editor-in-Chief of the Journal of Digital Forensics, Security and Law
4:45 PM
ADFSL 2017 Conference Keynote Speaker

Anni R. Coden Ph.D.

Anni R. Coden, Ph.D. is currently the project manager and technical lead of the IBM Systems G Anomaly Detection Solution. Previously she led a project at IBM’s T.J. Watson Research Center on Modeling and Simulation in a Smarter Cities environment, with a focus on Emergency Response Management. Anni also managed the Medical Text and Image Analysis group. The team had a long-term collaboration with the Mayo Clinic, worked with the Memorial Sloan-Kettering Cancer Center and was also involved with academic research.

Anni Coden joined IBM in 1981. Previously, she was a Researcher at the Massachusetts Institute of Technology from where she received her Ph.D. and M.S. in Computer Science. The received her M.S. in electrical engineering and her B.S. in mathematics from the Vienna University of Technology (Austria). Anni Coden has published in many areas such as theoretical computer science, computer vision, and computational linguistics and is the holder of multiple patents.