Proceedings

SADFE 2008

Third International Workshop on Systematic Approaches to Digital Forensic Engineering

22 May 2008
Berkeley, California, USA

Supported by
IEEE Technical Committee on Security and Privacy

Los Alamitos, California
Washington • Tokyo

IEEE COMPUTER SOCIETY
IEEE

Conference Publishing Services
Table of Contents

Message from the Program Chair ........................................................................................................ vii
Organizing Committee ........................................................................................................................ viii
Program Committee ............................................................................................................................. ix
Steering Committee ............................................................................................................................. x

Paper Session I
Finding Evidence for Digital Forensics I

Session Chair: Antonio Savoldi

A Novel Skin Tone Detection Algorithm for Contraband Image Analysis ........................................... 3
Abhishek Choudhury, Marcus Rogers, Blair Gillam, and Keith Watson

Combining Physical and Digital Evidence in Vehicle Environments...................................................... 10
Dennis K. Nilsson and Ulf E. Larson

Towards the Virtual Memory Space Reconstruction for Windows Live Forensic Purposes.................... 15
Antonio Savoldi and Paolo Gubian

Paper Session II
Digital Forensics Theory

Session Chair: Deborah Frincke

Cognitive-Maps Based Investigation of Digital Security Incidents.......................................................... 25
Slim Rekhis, Jihene Krichene, and Noureddine Boudriga

SÁDI – Statistical Analysis for Data Type Identification......................................................................... 41
Sarah J. Moody and Robert F. Erbacher
Paper Session III
Finding Evidence for Digital Forensics II
Workstation Logs and Residual Data

Session Chair: Rob Erbacher

Exemplifying Attack Identification and Analysis in a Novel Forensically Viable Syslog Model

Steena Dominica Steven Monteiro and Robert F. Erbacher

Finding the Evidence in Tamper-Evident Logs

Daniel Sandler, Kyle Derr, Scott Crosby, and Dan S. Wallach

Paper Session IV
A Legal View of Digital Forensics

Implications of Attorney Experiences with Digital Forensics and Electronic Evidence in the United States

Michael Losavio, Deborah W. Keeling, Adel Elmaghraby, George Higgins, and John Shutt

Protecting Digital Legal Professional Privilege (LPP) Data


Computer Forensics in Forensis

Sean Peisert, Matt Bishop, and Keith Marzullo

Legal Issues Pertaining to the Development of Digital Forensic Tools

Charles W. Adams

Works in Progress

Node-Based Probing and Monitoring to Investigate Use of Peer-to-Peer Technologies for Distribution of Contraband Material

Olfa Nasraoui, Deborah W. Keeling, Adel Elmaghraby, George Higgins, and Michael Losavio

A Research Configuration for a Digital Network Forensic Lab

Jeffrey S. Marean, Mike Losavio, and Ibrahim Imam

Network Forensics: Network Data and State Seizures in the United States

Michael Losavio, Deborah W. Keeling, Adel Elmaghraby, George Higgins, and John Shutt

Multidimensional Correlation of Software Source Code

Robert Zeidman

Author Index