Third Annual IFIP WG 11.9 International Conference on Digital Forensics
National Center for Forensic Science
University of Central Florida
Orlando, Florida
January 28 - 31, 2007

January 28, 2007 (Sunday)

06:30pm - 08:30pm: Dinner (High Tide Harry's, 925 N. Semoran Boulevard; Tel: (407) 273-4422)
Meet in Hotel Lobby @ 05:45pm for Car Pooling

January 29, 2007 (Monday)

06:30am - 08:00am: Breakfast (Hotel Radisson University)

08:15am - 08:30am: Welcoming Remarks and Logistics

08:30am - 09:30am: Keynote Lecture
Alternative Routes for Data Acquisition and System Compromise
mudge, BBN Technologies, Boston, Massachusetts (Former CEO and Chief Scientist, LØpht)

09:30am - 10:30am: Session 1: Insider Threats
Chair: Marc Rogers, Purdue University, West Lafayette, Indiana

ICMAP: An Information-Centric Modeling Tool for Insider Threat Analysis
D. Hua, S. Upadhyaya, H. Ngo and S. Mathew
State University of New York at Buffalo, Buffalo, New York

An Insider Threat Detection Digital Forensics System
D. Ray and P. Bradford
University of Alabama, Tuscaloosa, Alabama

10:30am - 10:45am: Break

10:45am - 11:45am: Session 2: File System Forensics
Chair: Philip Craiger, National Center for Forensic Science, University of Central Florida, Orlando, Florida

In-Place File Carving
G. Richard III, V. Roussev and L. Marziale
University of New Orleans, New Orleans, Louisiana

File System Journal Forensics
C. Swenson, R. Phillips and S. Shenoi
University of Tulsa, Tulsa, Oklahoma

11:45am - 01:00pm: Lunch (Marketplace@UCF Campus – Shuttle Transportation Provided)

01:15pm - 02:45pm: Session 3: Legal Issues
Chair: Martin Olivier, University of Pretoria, Pretoria, South Africa

Legal Issues Related to the Collection and Analysis of Telephone Call Records
C. Swenson, C. Adams, W. Whitledge and S. Shenoi
University of Tulsa, Tulsa, Oklahoma

Role of Calibration in Establishing the Foundation for Expert Testimony
B. Endicott-Popovsky, B. Chee and D. Frincke
University of Washington, Seattle, Washington
University of Hawaii Manoa, Honolulu, Hawaii
Pacific Northwest National Laboratory, Moscow, Idaho

January 29, 2007 (Monday) (continued)

Perceptions of Prosecutors' and Judges' Knowledge and Willingness to Deal with Digital Evidence: A Survey
M. Rogers, K. Scarborough, K. Frakes and C. San Martin
Purdue University, West Lafayette, Indiana
Eastern Kentucky University, Richmond, Kentucky

02:45pm - 03:00pm: Break

03:00pm - 04:45pm: Session 4: Network Forensics
Chair: Golden Richard III, University of New Orleans, New Orleans, Louisiana

GooSweep: Mining Search Engines to Acquire Network Forensic Evidence
R. McGrew and R. Vaughn
Mississippi State University, Starkville, Mississippi

Forensic Analysis of Modbus-Based Distributed Control Systems
T. Kilpatrick, J. Gonzalez, R. Chandia, M. Papa and S. Shenoi
University of Tulsa, Tulsa, Oklahoma

Investigating Railroad Accidents Using Digital Forensics
A. Basha, M. Hartong, R. Goel and D. Wijesekera
George Mason University, Fairfax, Virginia
Federal Railroad Administration, Washington, DC
Howard University, Washington, DC

Forensic Logging System Using a Secure OS and Network Processor
T.-K. Park, Y.-H. Im and I. Ra
Hanseo University, Chungnam, Korea
Trusted Systems on the Net, Taejon, Korea
University of Colorado at Denver, Denver, Colorado

06:30pm - 08:00pm: Dinner (Don Pablo's, 11400 University Drive; Tel: (407) 208-1828)
Meet in Hotel Lobby @ 06:15pm for Car Pooling

January 30, 2007 (Tuesday)

06:30am - 07:45am: Breakfast (Hotel Radisson University)

08:00am - 09:00am: Keynote Lecture
A Law Enforcement Challenge to the Digital Forensics Research Community
W. Anthony Whitledge, Director, IRS Criminal Investigation/Electronic Crimes Program (Ret'd.), Washington, DC

09:00am - 10:00am: Session 5: Forensic Techniques I
Chair: Buks Louwrens, University of Johannesburg, Johannesburg, South Africa

Factors Affecting Cryptographic One-Way Hashes of CD-R Media
C. Marberry and P. Craiger
National Center for Forensic Science, University of Central Florida, Orlando, Florida

Disk Drive I/O Commands and Write Blocking
J. Lyle, S. Mead and K. Rider
National Institute of Standards and Technology, Gaithersburg, Maryland

10:00am - 10:15am: Break

10:15am - 11:45am: Session 6: Forensic Techniques II
Chair: Indrajit Ray, Colorado State University, Fort Collins, Colorado

Using Tokens for Redacting Digital Information from Electronic Devices
A. Barclay, L. Watson, D. Greer, J. Hale and G. Manes
University of Tulsa, Tulsa, Oklahoma
Oklahoma Digital Forensics Professionals, Tulsa, Oklahoma

A New Text String Search Process for Digital Forensic Investigations
N. Beebe and G. Dietrich
University of Texas at San Antonio, San Antonio, Texas

Steganography Detection Using Multi-Class Classification
B. Rodriguez and G. Peterson
Air Force Institute of Technology, Wright-Patterson AFB, Ohio

11:45am - 01:15pm: Lunch (Marketplace@UCF Campus – Shuttle Transportation Provided)

01:30pm - 02:30pm: Session 7: Authorship Attribution
Chair: Barbara Endicott-Popovsky, University of Washington, Seattle, Washington

Future Trends in Authorship Attribution
P. Juola
Duquesne University, Pittsburgh, Pennsylvania

The Keyboard Dilemma and Forensic Authorship Identification
C. Chaski
Institute for Linguistic Evidence, Georgetown, Delaware

02:30pm - 03:30pm: Session 8: Evidence Analysis and Management
Chair: Gilbert Peterson, Air Force Institute of Technology, Wright-Patterson AFB, Ohio

Specializing CRISP-DM for Evidence Mining
J. Venter, A de Waal and N. Willers
Council for Scientific and Industrial Research, Pretoria, South Africa

Applying the Biba Integrity Model within a Forensic Evidence Management System
K. Arthur and M. Olivier
University of Pretoria, Pretoria, South Africa

03:30pm - 03:45pm: Break

January 30, 2007 (Tuesday) (continued)

03:45pm - 04:45pm: Session 9: Formal Methods
Chair: Jigang Liu, Metropolitan State University, St. Paul, Minnesota

A Systematic Approach for Forensic Investigations of Computer Attacks Using Attack Trees
N. Poolsapassit and I. Ray
Colorado State University, Fort Collins, Colorado

Attack Patterns: A New Forensic and Design Tool
E. Fernandez, J. Pelaez and M. Larrondo-Petrie
Florida Atlantic University, Boca Raton, Florida

06:30pm - 08:30pm: Dinner (Smoky Bones, 303 N. Alafaya Trail; Tel: (407) 249-2009)
Meet in Hotel Lobby @ 06:15pm for Car Pooling

January 31, 2007 (Wednesday)

06:30am - 07:45am: Breakfast (Hotel Radisson University)

08:00pm - 09:00am: Session 10: Rootkit Detection
Chair: David Dampier, Mississippi State University, Starkville, Mississippi

An Analysis of Forensic Tools in Detecting Rootkits and Hidden Processes
A. Todd, J. Benson, G. Peterson, T. Franz, M. Stevens and R. Raines
Air Force Institute of Technology, Wright-Patterson AFB, Ohio

A Method for Detecting Linux Kernel Module Rootkits
D. Wampler and J. Graham
University of Louisville, Louisville, Kentucky

09:00am - 09:15am: Break

09:15am - 11:15am: Session 11: Portable Electronic Device Forensics
Chair: Mark Pollitt, National Center for Forensic Science, University of Central Florida, Orlando, Florida

Parametrizing Super-Resolution Analysis of Video for Forensic Applications
A. Gehani and J. Reif
SRI International, Menlo Park, California
Duke University, Durham, North Carolina

A Framework for Analyzing Volatile Data Stores
T. Vidas
University of Nebraska at Omaha, Omaha, Nebraska

Forensic Analysis of Xbox Consoles
P. Burke and P. Craiger
National Center for Forensic Science, University of Central Florida, Orlando, Florida

Forensic Analysis of Credit Card Skimmers
M. Davis, A. Guernsey and S. Shenoi
University of Tulsa, Tulsa, Oklahoma

11:15am - 12:15pm: Lunch (Marketplace@UCF Campus – Shuttle Transportation Provided)