Seventh Annual IFIP WG 11.9 International Conference on Digital Forensics
National Center for Forensic Science
University of Central Florida
Orlando, Florida
January 30 – February 2, 2011

January 30, 2011 (Sunday)

06:30pm - 08:30pm: Dinner (High Tide Harry's, 4645 S. Semoran Boulevard; Tel: (407) 273-4422)
Meet in Hotel Lobby @ 05:30pm for Car Pooling

January 31, 2011 (Monday)

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

08:20am - 08:30am: Welcoming Remarks and Logistics

08:30am - 09:30am: Keynote Lecture
U.S. Secret Service Efforts in Cell Phone and Embedded Device Forensics
Special Agent James Darnell, U.S. Secret Service, Washington, DC

09:30am - 10:30am: Session 1: Themes and Issues
Chair: Mark Pollitt, Daytona State College, Daytona, Florida

The State of the Science of Digital Evidence Examination
F. Cohen, J. Lowrie and C. Preston
California Sciences Institute, Livermore, California

Cloud Forensics
K. Ruan, J. Carthy, T. Kechadi and M. Crosbie
University College Dublin, Dublin, Ireland
IBM, Dublin Ireland

10:30am - 10:45am: Break

10:45am - 11:45am: Session 2: Business Applications
Chair: Hein Venter, University of Pretoria, Pretoria, South Africa

Leak Detection Analysis of Business Processes
R. Accorsi and C. Wonnemann
University of Freiburg, Freiburg, Germany

Detecting Collusion in ERP Systems
A. Islam, M. Corney, G. Mohay, A. Clark, S. Bracher, T. Raub and U. Flegel
Queensland University of Technology, Brisbane, Australia
SAP Research Center, Brisbane, Australia

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

01:30pm - 03:00pm: Session 3: Investigative Frameworks
Chair: Jill Slay, University of South Australia, Mawson Lakes, Australia

A Framework for Investigative Questioning in Incident Analysis and Response
C. Blackwell
Oxford Brookes University, Oxford, United Kingdom

A Case-Based Reasoning Framework for Live Forensics
B. Hoelz, C. Ralha and F. Mesquita
National Institute of Criminalistics, Brazilian Federal Police, Brasilia, Brazil
University of Brasilia, Brasilia, Brazil

January 31, 2011 (Monday) (continued)

Sensitivity Analysis of Digital Forensic Reasoning Using Bayesian Networks
M. Kwan, K.-P. Chow, H. Tse, F. Law and P. Lai
University of Hong Kong, Hong Kong, China

03:00pm - 03:30pm: Break

03:30pm - 04:30pm: Session 4: Network Forensics I

Chair: Rafael Accorsi, University of Freiburg, Freiburg, Germany

Deterministic Router and Interface Marking for Network Forensics
E. Pilli, R. Joshi and R. Niyogi
Indian Institute of Technology – Roorkee, Roorkee, India

Extracting Digital Evidence from VoIP Applications
D. Irwin and J. Slay
University of South Australia, Mawson Lakes, Australia

06:30pm - 08:00pm: Dinner (Smoky Bones, 303 N. Alafaya Trail; Tel: (407) 249-2009)

Meet in Hotel Lobby @ 06:15pm for Car Pooling

February 1, 2011 (Tuesday)

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

08:30am - 09:30am: Keynote Lecture
Gathering Evidence of Large-Scale Internet Frauds
Tyler Moore, Center for Research on Computation and Society, Harvard University, Cambridge, Massachusetts

09:30am - 10:30am: Session 5: Phishing and Malware Analysis
Chair: Kam-Pui Chow, University of Hong Kong, Hong Kong, China

What's So Smart about Mr. Brain?
H. McCalley, B. Wardman and G. Warner
University of Alabama at Birmingham, Birmingham, Alabama

Cross Evidence Malware Identification Using deLink
A. Flaglien, K. Franke and A. Arnes
Gjovik University College, Gjovik, Norway

10:30am - 10:45am: Break

10:45am - 11:45am: Session 6: Network Forensics II
Chair: Martin Olivier, University of Pretoria, Pretoria, South Africa

A Network Forensic Implementation for Detecting Mobile Botnets using Artificial Immune Systems
I. Vural and H. Venter
University of Pretoria, Pretoria, South Africa

An FPGA-Based System for Detecting Malicious DNS Network Traffic
B. Thomas, B. Mullins, G. Peterson and R. Mills
Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio

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

01:30pm - 03:00pm: Session 7: Forensic Techniques and Tools
Chair: Gilbert Peterson, Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio

Fast Content-Based File Type Identification
I. Ahmed, K. Lhee, H. Shin and M. Hong
Queensland University of Technology, Brisbane, Australia
Ajou University, Suwon, South Korea

`lightgrep`*: A Multipattern Regular Expression Search Tool for Digital Forensics*
J. Stewart and J. Uckelman
Lightbox Technologies, Arlington, Virginia
University of Amsterdam, Amsterdam, The Netherlands

Assembling the Metadata for a Database Forensic Examination
H. Beyers and M. Olivier
University of Pretoria, Pretoria, South Africa

03:30pm - 03:30pm: Break

03:30pm - 04:45pm: Panel: Preserving the Authenticity of Digital Evidence
Chair: Barbara Endicott-Popovsky, University of Washington, Seattle, Washington

Panelists
B. Endicott-Popovsky, University of Washington, Seattle, Washington
F. Cohen, California Sciences Institute, Livermore, California
L. Duranti, University of British Columbia, Vancouver, Canada
A. Jansen, University of British Columbia, Vancouver, Canada

February 1, 2011 (Tuesday) (continued)

06:30pm - 08:30pm: Dinner (Miller's Ale House, 641 N. Alafaya Trail; Tel: (407) 736-0333)
Meet in Hotel Lobby @ 06:15pm for Car Pooling

February 2, 2011 (Wednesday)

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

08:30am - 10:00am: Session 8: Novel Techniques

Chair: Philip Craiger, Daytona State College, Daytona, Florida

Stylometric Approaches to Author Obfuscation: An Empirical Study
P. Juola and D. Vescovi
Duquesne University, Pittsburgh, Pennsylvania

SWF Steganography: Techniques for Hiding Data in SWF Files
M.-A. Fouche and M. Olivier
University of Pretoria, Pretoria, South Africa

Resolving Conflicts between Access Control and IT Forensics
C. Winter, M. Schneider and Y. Yannikos
Fraunhofer Institute for Secure Information Technology, Darmstadt, Germany

10:00am - 10:15am: Break

10:15am - 11:15am: Session 9: Forensic Analysis Techniques

Chair: Mason Rice, University of Tulsa, Tulsa, Oklahoma

Investigating Forensic Processes for the Apple iPad
A. Hay, D. Krill, B. Kuhar and G. Peterson
Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio

Forensic Analysis of Plug Computers
S. Conrad, G. Dorn and P. Craiger
National Center for Forensic Science and University of Central Florida, Orlando, Florida
Daytona State College, Daytona, Florida and National Center for Forensic Science, Orlando, Florida

11:15am - 12:30pm: Lunch (Marketplace@UCF Campus – Shuttle Transportation Provided)