Fourth Annual IFIP WG 11.9 International Conference on Digital Forensics
Centennial Hall, Kyoto University
Yoshida-Honmachi, Sakyo-ku
Kyoto, Japan
January 27 - 30, 2008

January 27, 2008 (Sunday)

07:00pm - 09:00pm: Dinner
Kyoto Royal Hotel and Spa (Sanjo-Agaru, Kawaramachi, Nakagyo-ku, Kyoto)

January 28, 2008 (Monday)

07:00am - 08:30am: Breakfast (Kyoto Royal Hotel and Spa)

09:00am - 09:15am: Welcoming Remarks (Centennial Hall, Kyoto University)

09:15am - 10:00am: Keynote Lecture
Dealing with Emerging Risks in Critical Information Infrastructures
Suguru Yamaguchi, Professor of Information Science, Nara Institute of Science and Technology, Ikoma, Nara, Japan; Information Security Advisor, Cabinet Secretariat, Tokyo, Japan

10:00am - 11:00am: Session 1: Themes and Issues
Chair: Shambhu Upadhyaya, State University of New York at Buffalo, Buffalo, New York, USA

When is Computer Evidence Forensically Sound?
Rodney McKemmish
University of South Australia, Mawson Lakes, Australia

Application of Traditional Forensic Taxonomy to Digital Forensics
Mark Pollitt
National Center for Forensic Science, University of Central Florida, Orlando, Florida, USA

11:00am - 11:15am: Break

11:15am - 12:15pm: Session 2: Portable Electronic Device Forensics I
Chair: Mark Pollitt, National Center for Forensic Science, University of Central Florida, Orlando, Florida, USA

Using Sensor Dirt for Toolmark Analysis of Digital Photographs
Martin Olivier
University of Pretoria, Pretoria, South Africa

Source Camera Identification Based on Image Bi-Coherence and Wavelet Features
Fanjie Meng, Xiangwe Kong and Xingang You
Dalian University, Dalian, China
Beijing Institute of Electronic Technology and Applications, Beijing, China

12:30pm - 01:30pm: Lunch (Centennial Hall, Kyoto University)

01:45pm - 03:15pm: Session 3: Forensic Techniques
Chair: Martin Olivier, University of Pretoria, Pretoria, South Africa

Forensic Analysis of Volatile Instant Messages
Matthew Kiley, Shira Dankner and Marcus Rogers
Purdue University, West Lafayette, Indiana, USA

Timely Rootkit Detection During Live Response
Daniel Molina, Matthew Zimmermann, Gregory Roberts, Marnita Eaddie and Gilbert Peterson
Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio, USA

January 28, 2008 (Monday) (continued)

Identifying Malicious Web Services Using Client Honeypots
Christian Seifert, Radu Muschevici, Ian Welch, Peter Komisarczuk and Barbara Endicott-Popovsky
Victoria University, Wellington, New Zealand
University of Washington, Seattle, Washington, USA

03:15pm - 03:30pm: Break

03:30pm - 05:30pm: Session 4: Evidence Collection
Chair: Vassil Roussev, University of New Orleans, New Orleans, Louisiana, USA

Recovering Data from Failing Floppy Disk Drives
Frederick Cohen and Charles Preston
Frederick Cohen and Associates, Livermore, California, USA

Using Shredder Programs to Remove Sensitive Data in the Registry
Harry Velupillai and Pontjho Mokhonoana
Council for Scientific and Industrial Research, Pretoria, South Africa

Forensic Web Services
Murat Gunestas, Duminda Wijesekera and Anoop Singhal
George Mason University, Fairfax, Virginia, USA
National Institute of Standards and Technology, Gaithersburg, Maryland, USA

Evidence Collection Using Google Desktop Search
Benjamin Turnbull, Jill Slay and Timothy Pavlic
University of South Australia, Mawson Lakes, Australia

07:00pm - 09:30pm: Dinner (The Garden Oriental Kyoto, 484-6 Higashi-Ikesu-Cho, Nakagyo-ku, Kyoto)

January 29, 2008 (Tuesday)

07:00am - 08:30am: Breakfast (Kyoto Royal Hotel and Spa)

09:00am - 10:00am: Keynote Lecture
Emerging Cyber Threats
Shawn Henry, Deputy Assistant Director, Federal Bureau of Investigation, Washington, DC, USA

10:00am - 11:00am: Session 5: Evidence Analysis and Management Techniques
Chair: Ryoichi Sasaki, Tokyo Denki University, Tokyo, Japan

Hash-Based Classification of Data
Vassil Roussev, Golden Richard III and Lodovico Marciale
University of New Orleans, New Orleans, Louisiana, USA

Applying Topic Modeling on Forensic Data
Alta de Waal, Jacobus Venter and Etienne Barnard
Council for Scientific and Industrial Research, Pretoria, South Africa

11:00am - 11:15am: Break

11:15am - 12:15pm: Session 6: Application of Bayesian Techniques
Chair: Jacobus Venter, Council for Scientific and Industrial Research, Pretoria, South Africa

Fusion of Multi-Class Steganalysis Systems Using Bayesian Model Averaging
Benjamin Rodriguez, Gilbert Peterson and Kenneth Bauer
Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio, USA

Digital Forensics Using a Bayesian Network
Michael Kwan, K.P. Chow, Frank Law and Pierre Lai
University of Hong Kong, Hong Kong, China

12:30pm - 01:30pm: Lunch (Centennial Hall, Kyoto University)

01:45pm - 02:45pm: Session 7: Portable Electronic Device Forensics II
Chair: Gilbert Peterson, Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio, USA

Data Hiding and Recovery in Windows CE Based Handheld Devices
Antonio Savoldi and Paolo Gubian
University of Brescia, Brescia, Italy

Legal Issues Regarding the Collection and Analysis of Cell Phone Information
Charles Adams, Anthony Whitledge and Sujeet Shenoi
University of Tulsa, Tulsa, Oklahoma, USA

02:45pm - 03:45pm: Session 8: Event Data Recorder Forensics
Chair: Philip Craiger, National Center for Forensic Science, University of Central Florida, Orlando, Florida, USA

Cryptographic Protection and Recovery of Railroad Event Recorder Data
Mark Hartong, Rajni Goel and Duminda Wijesekera
Federal Railroad Administration, Washington, DC, USA
Howard University, Washington, DC, USA
George Mason University, Fairfax, Virginia, USA

Automobile Event Data Recorder Forensics
Jeremy Daily, Nathan Singleton and Gavin Manes
University of Tulsa, Tulsa, Oklahoma, USA
Oklahoma Digital Forensics Professionals, Inc., Tulsa, Oklahoma, USA

03:45pm - 04:00pm: Break

January 29, 2008 (Tuesday) (continued)

04:00pm - 05:30pm: Session 9: Advanced Investigative Techniques
Chair: Indrajit Ray, Colorado State University, Fort Collins, Colorado, USA

Inferring the Sources of Information Leaks in Document Management Systems
Madhusudhanan Chandrasekaran, Vidyaraman Sankaranarayanan and Shambhu Upadhyaya
State University of New York at Buffalo, Buffalo, New York, USA

Using Data Mining to Detect Remote Exploits
Mohammad Masud, Latifur Khan, Bhavani Thuraisingham, Xinran Wang, Peng Liu and Sencun Zhu
University of Texas at Dallas, Richardson, Texas, USA
Pennsylvania State University, University Park, Pennsylvania, USA

Digital Image Background Matching for Identifying Suspects
Paul Fogg, Gilbert Peterson and Michael Veth
Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio, USA

07:00pm - 09:30pm: Dinner (Ganko Takasegawa Nijo-en, 484-6 Higashi-Ikesu-Cho, Nakagyo-ku, Kyoto)

January 30, 2008 (Wednesday)

07:00am - 08:30am: Breakfast (Kyoto Royal Hotel and Spa)

09:00am - 10:30am: Session 10: Security and Integrity Techniques
Chair: Charles Adams, University of Tulsa, Tulsa, Oklahoma, USA

Using Boot Control to Guard Against Unauthorized Program Execution
Keisuke Fujita, Yuki Ashino, Tetsutaro Uehara and Ryoichi Sasaki
Tokyo Denki University, Tokyo, Japan
Kyoto University, Kyoto, Japan

Hypothesis-Based Investigation of Digital Timestamps
Svein Willassen
Norwegian University of Science and Technology, Trondheim, Norway

Analysis of k-Dimension Hashing to Improve Disk Sector Integrity
Zoe Jiang, Lucas Hui and Siu-Ming Yiu
University of Hong Kong, Hong Kong, China

10:30am - 10:45am: Break

10:45am - 12:15pm: Session 11: Forensic Tools
Chair: Jigang Liu, Metropolitan State University, St. Paul, Minnesota, USA

A Live-System Forensic Evidence Acquisition Tool
Renico Koen and Martin Olivier
University of Pretoria, Pretoria, South Africa

A Time-Analysis Comparison of Hard Drive Imaging Tools
Jack Riley, David Dampier and Rayford Vaughn
Mississippi State University, Starkville, Mississippi, USA

A Virtual Digital Forensics Laboratory
Philip Craiger, Paul Burke, Chris Marberry and Mark Pollitt
National Center for Forensic Science, University of Central Florida, Orlando, Florida, USA

12:30pm - 01:30pm: Lunch (Centennial Hall, Kyoto University)

01:40pm - 03:20pm: Short Paper Session I
Chair: Tetsutaro Uehara, Kyoto University, Kyoto, Japan

A Novel Log-Inflation-Based Criterion for Preserving Fraudulent Audit Logs
Yasuo Hatano, Kunihiko Miyazaki, Mitsuru Iwamura, Tsutomu Matsumoto, Ryoichi Sasaki, Hiroshi Yoshiura, Yoshinori Honda and Satoru Tezuka
Hitachi Ltd., Yokohama, Japan
Waseda University, Tokyo, Japan
Yokohama National University, Yokohama, Japan
Tokyo Denki University, Tokyo, Japan
University of Electro-Communications, Tokyo, Japan

Virtual WORM Function for Preserving the Authenticity of Logs on Client Personal Computers
Satoshi Kai, Masato Arai, Akira Morita and Satoru Tezuka
Hitachi Ltd., Yokohama, Japan

A Privileged Data-Aware Live Forensics Scheme
Ricci Ieong
eWalker Consulting, Hong Kong, China

An XML-Based Framework for Efficiently Acquiring Digital Evidence from Live Windows Systems
Kyungsoo Lim, Jonghyuk Park, Seokhee Lee, Sangjin Lee and Jongin Lim
Korea University, Seoul, Korea
Kyungnam University, Kyungnam, Korea

January 30, 2008 (Wednesday) (continued)

03:20pm - 03:40pm: Break

03:40pm - 05:10pm: Short Paper Session II
Chair: David Dampier, Mississippi State University, Starkville, Mississippi, USA

Legal Issues Related to Digital Forensics and the Response to Privacy Breaches in Japan
Ikuo Takahashi
Utsonomiya University, Fukushima, Japan

Visualization of Worm Path Identification
Taro Inaba, Shinya Tahara, Nobutaka Kawaguchi, Seiji Shibaguchi, Hidekazu Shiozawa and Kenichi Okada
Keio University, Yokohama, Japan
Tamagawa University, Tokyo, Japan

Real Time Detection of Criminal Activities by Monitoring Suspicious Employee Behavior
Masakatsu Nishigaki, Anjan Kumar Das, Hirokazu Maruoka and Toshifumi Sugiura
Shizuoka University, Hamamatsu, Naka, Japan

Certification of Secure Encounter History for Low Power Mobile Sensors
Takurou Sakai, Akira Uchiyama, Yoshitaka Nakamura and Teruo Higashino
Osaka University, Osaka, Japan
Nara Institute of Science and Technology, Ikoma, Nara, Japan

07:00pm - 09:30pm: Farewell Dinner (Kyoto Royal Hotel and Spa)