Fourteenth Annual IFIP WG 11.9 International Conference on Digital Forensics
The Lalit, Barakhamba Avenue, Connaught Place, New Delhi, India
January 3-5, 2018

January 2, 2018 (Tuesday)

07:15pm - 09:00pm: Dinner (Farzi Café, E-38/39, First Floor, Connaught Place, New Delhi; paid participants only)
Meet in the Hotel Lobby @ 06:45pm for transportation to the restaurant

January 3, 2018 (Wednesday)

07:30am - 08:45am: Breakfast (The Lalit, Barakhamba Avenue, Connaught Place; hotel guests only)

09:00am - 09:10am: Welcoming Remarks and Logistics

09:10am - 09:40am: Keynote Lecture
Cyber Security – The Indian Perspective
Gulshan Rai, National Cyber Security Coordinator (NSCS)
National Security Council Secretariat, New Delhi, India

09:40am - 10:30am: Keynote Lecture
Digitized Document Fraud: New Directions and Opportunities
Gaurav Gupta, Joint Director and Scientist D
Ministry of Electronics and Information Technology, New Delhi, India

10:30am - 11:30am: Session 1: Themes and Issues
Chair: Somitra Sanadhya, Indian Institute of Technology Ropar, Rupnagar, India

Case Studies and Challenges in Internet of Things Forensics
Saad Alabdulsalam, Kevin Schaefer, Arie Kouwen and Nhien An Le Khac
University College Dublin, Dublin, Ireland
German Federal Police, Stuttgart, Germany
Dutch Police, Amsterdam, The Netherlands

Measuring the Probative Value of Evidence in Digital Forensic Triage
Richard Overill and Kam-Pui Chow
King’s College London, London, United Kingdom
University of Hong Kong, Hong Kong, China

11:30am - 11:45am: Break

11:45am - 01:15pm: Session 2: Network Forensics I
Chair: Duminda Wijesekera, George Mason University, Fairfax, Virginia, USA

A Real-Time Collaborative Network Forensic Scheme for Evidence Analysis
Nour Moustafa and Jill Slay
University of New South Wales, Canberra, Australia

Entropy-Based Prediction of Network Protocols in the Forensic Analysis of DNS Tunnels
Irvin Homem, Panagiotis Papapetrou and Spyridon Dosis
Stockholm University, Stockholm, Sweden
KTH Royal Institute of Technology, Stockholm, Sweden
January 3, 2018 (Wednesday) (continued)

Traffic Classification and Application Identification in Network Forensics
Jan Pluskal, Ondrej Lichtner and Ondřej Ryšavý
Brno University of Technology, Brno, Czech Republic

01:15pm - 02:00pm: Lunch (The Lalit, Barakhamba Avenue, Connaught Place)

02:00pm - 02:30pm: Invited Lecture
Legal Challenges to Digital Forensics in India
Suhaan Mukerji, Partner, PLR Chambers, New Delhi, India
Founding Member of the Governing Board, Cloud Computing Innovation Council of India, New Delhi, India

02:30pm - 04:00pm: Session 3: Forensic Techniques I
Chair: Emmanuel Pilli, Malaviya National Institute of Technology, Jaipur, India
Challenges, Opportunities and a Framework for Web Environment Forensics
Mike Mabey, Adam Doupé, Ziming Zhao and Gail-Joon Ahn
Arizona State University, Tempe, Arizona, USA
Google Drive Client Artifacts in a macOS Sierra
Swasti Bhushan Deb
IBM India, Bangalore, India
Anti-Forensic Capacity and Detection Rating of Hidden Data in the ext4 Filesystem
Thomas Göbel and Harald Baier
Darmstadt University of Applied Sciences, Darmstadt, Germany

04:00pm - 04:45pm: Break and Poster Session
Chair: Mahesh Govil, Malaviya National Institute of Technology, Jaipur, India
A Dynamic Taint Analysis Tool for Android App Forensics
Yong Guan, Zhen Xu, Chen Shi and Zhenqiang Gong
Iowa State University, Ames, Iowa, USA
Forensic Analysis of a DVR Hard Disk
Chunduru Prasad
Central Forensic Science Laboratory, Hyderabad, India
Solid State Drive Forensics
Santosh Khadsare
Cyber Security and Digital Forensics Practice, New Delhi, India
Forensics-as-a-Service
Raksha Khandelwal and Reeti Rastogi
Mody University, Laxmangarh, India
Multimodal and Continuous Smartphone User Authentication: Applications in Forensics and e-Governance
Himanshu Gangwar and Sachin Vashistha
Kurukshetra University, Kurukshetra, India
Quick Response Codes for Scalable and Secure Forensic Solutions
Yansi Keim, Shweta Singh, and Vibha Masiwal
Indira Gandhi Delhi Technical University for Women, New Delhi, India
Maharshi Dayanand University, Rohtak, India
Rukmini Devi Institute of Advanced Studies, New Delhi, India.

04:45pm - 05:15pm: Business Meeting

07:15pm - 09:00pm: Dinner (Chew – Pan Asian Café, M-16, 1st Floor, Outer Circle, Connaught Place, New Delhi; paid participants only)
Meet in the Hotel Lobby @ 06:45pm for transportation to the restaurant
January 4, 2018 (Thursday)

07:30am - 08:45am: Breakfast (The Lalit, Barakhamba Avenue, Connaught Place; hotel guests only)

09:00am - 10:00am: Session 4: Cloud Forensics
Chair: Jill Slay, University of New South Wales, Canberra, Australia
A Layered Graphical Model for Cloud Forensics and Mission Attack Impact Analysis
Changwei Liu, Anoop Singhal and Duminda Wijesekera
George Mason University, Fairfax, Virginia, USA
National Institute of Standards and Technology, Gaithersburg, Maryland, USA
A Taxonomy of Cloud Endpoint Forensic Tools
Anand Mishra, Emmanuel Pilli and Mahesh Govil
Malaviya National Institute of Technology, Jaipur, India

10:00am - 11:00am: Session 5: Industrial Control System Forensics
Chair: Anoop Singhal, National Institute of Standards and Technology, Gaithersburg, Maryland, USA
Enhancing the Forensic and Anomaly Detection Capabilities of Programmable Logic Controllers
Chun-Fai Chan, Kam-Pui Chow, Siu-Ming Yiu and Kwai-Keung Yau
University of Hong Kong, Hong Kong, China
Effective Logging System for Digital Forensic Readiness of Siemens Programmable Logic Controllers
Kwai-Keung Yau, Kam-Pui Chow and Siu-Ming Yiu
University of Hong Kong, Hong Kong, China

11:00am - 11:20am: Break

11:20am - 11:40am: Sponsor Presentation (Cellebrite)

11:40am - 01:10pm: Session 6: Network Forensics II
Chair: Yong Guan, Iowa State University, Ames, Iowa, USA
Enabling the Non-Expert Analysis of Large Volumes of Intercepted Network Traffic
Erwin Van Wiel, Mark Scanlon and Nhien An Le Khac
Dutch Police, Amsterdam, The Netherlands
University College Dublin, Dublin, Ireland
Network Forensics with Snort – Collecting Evidence Using Constrained Approximate Search
Ambika Shrestha Chitrakar and Slobodan Petrovic
Norwegian University of Science and Technology, Gjovik, Norway
Hashing Unordered and Incomplete Network Streams on the Fly
Chao Zheng, Xiang Li, Qingyun Liu, Yong Sun and Binxing Fang
Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China
University of Electronics Science and Technology of China, Guangdong, China

01:10pm - 02:10pm: Lunch (The Lalit, Barakhamba Avenue, Connaught Place)

02:10pm - 02:30pm: Sponsor Presentation (Magnet Forensics)

02:30pm - 04:00pm: Session 7: Forensic Techniques II
Chair: Kam-Pui Chow, University of Hong Kong, Hong Kong, China
Obtaining Valuable Precision-Recall Trade-Offs During Fuzzy Searches of Large E-Mail Corpora
Kyle Porter and Slobodan Petrovic
Norwegian University of Science and Technology, Gjovik, Norway
Recovery of Forensic Artifacts from Deleted Jump Lists
Pankaj Sharma, Rajender Nath, Bhupendra Singh and Azad Singh
Chitkara University, Rajpura, India
Kurukshetra University, Kurukshetra, India
Defence Institute of Advanced Technology, Pune, India
National Institute of Technology, Hamirpur, India
Detecting the Leakage Source of Hard Copy Documents
Jijnasa Nayak, Shweta Singh, Saheb Chhabra, Gaurav Gupta, Monika Gupta and Garima Gupta
National Institute of Technology, Rourkela, India
Maharshi Dayanand University, Rohtak, India
Indraprastha Institute of Information Technology Delhi, New Delhi, India
Ministry of Electronics and Information Technology, New Delhi, India

04:00pm - 04:20pm: Break

04:20pm - 04:40pm: Sponsor Presentation (Lab Systems)

04:40pm - 05:40pm: Session 8: Cell Phone and Embedded Device Forensics
Chair: Richard Overill, King's College London, London, United Kingdom
Forensic Analysis of Steganography Apps in Android Devices
Wenhao Chen, Yangxiao Wang, Yong Guan, Jennifer Newman, Li Lin and Stephanie Reinders
Iowa State University, Ames, Iowa, USA
Automated Vulnerability Detection in Embedded Systems
Danjun Liu, Yong Tang and Baosheng Wang
National University of Defense and Technology, Changsha, China

07:15pm - 09:00pm: Dinner (Ardor 2.1, N 55-56 & 88/89, Outer Circle, Connaught Place, New Delhi; paid participants only)
Meet in the Hotel Lobby @ 06:45pm for transportation to the restaurant
January 5, 2018 (Friday)

07:30am - 08:45am: Breakfast (The Lalit, Barakhamba Avenue, Connaught Place; hotel guests only)

09:00am – 10:30am: Keynote Lecture
*Case Studies in Invasive Embedded Device Forensics: Evidence Extraction and Firmware Verification*
Sujeet Shenoi, F.P. Walter Professor of Computer Science and Professor of Chemical Engineering
University of Tulsa, Tulsa, Oklahoma, USA

10:30am - 11:00am: Break

11:00am - 12:30pm: Keynote Lecture
*Digitized Document Fraud: New Directions and Opportunities - Part II*
Gaurav Gupta, Joint Director and Scientist D
Ministry of Electronics and Information Technology, New Delhi, India

12:30pm - 01:15pm: Lunch (The Lalit, Barakhamba Avenue, Connaught Place)

01:15pm - 05:30pm: Guided Tour of New Delhi
Meet in the Hotel Lobby @ 01:15pm to catch the tour bus

01:15pm - 02:15pm: Invited Lecture for Law Enforcement
*Why are Critical Infrastructure Assets so Easy to Attack?*
Sujeet Shenoi, F.P. Walter Professor of Computer Science and Professor of Chemical Engineering
University of Tulsa, Tulsa, Oklahoma, USA

02:15pm - 02:45pm: Invited Lecture for Law Enforcement
*Biometrics and Forensics*
Mayank Vatsa, Associate Professor of Computer Science and Engineering
Indraprastha Institute of Information Technology Delhi, New Delhi, India

2:45pm - 03:00pm: Break

03:00pm - 03:40pm: Invited Lecture for Law Enforcement
*Digital Forensic Investigations of Fraud in Online Shopping Companies*
Varun Nair, Information Security Manager
Fareportal India, Gurgaon, India

03:40pm - 04:20pm: Invited Lecture for Law Enforcement
*Admissibility of Electronic Evidence: Emerging Challenges in Court*
Neeraj Aarora, Cyber Lawyer and Arbitrator
Supreme Court of India, New Delhi, India

04:20pm - 05:00pm: Invited Lecture for Law Enforcement
*Cloud Forensic Investigations in India*
Emmanuel Pilli, Assistant Professor of Computer Science and Engineering
Malaviya National Institute of Technology, Jaipur, India