1st International Conference on
Digital Forensics and Cyber Crime
September 30 – October 2, 2009, Albany, NY

ICDF2C 2009

Tentative Program & Conference Guide

Conference Hosts:

In Cooperation with: **New York State Police**

Organizing Committee

General Chair	Sanjay Goel	University at Albany, SUNY
Conference Co-Chairs	Fabio R. Auffant II	NYS Police Computer Crime Unit
	Ingrid Fisher	University at Albany, SUNY
Steering Committee	Imrich Chlamtac	Create-Net
	Tibor Kovacs	ICST, Hungary
TPC Chair	Miklos A. Vasarhelyi	Rutgers University
Workshop Chair	Deborah Snyder	NYS Office of Temp. & Disability Assistance
Organizational Chair	Damira Pon	University at Albany, SUNY
Asst. to General Chair	Anthony Colon	University at Albany, SUNY
Conf. Coordinator	Barbara Torok	ICST, Hungary
Local Arrangements Chair	Sally Mills	University at Albany, SUNY
Webmaster	Robert Tracey	University at Albany, SUNY

Track and Workshop Chairs and Co-Chairs

Accounting and Fraud	Michael Alles	Rutgers University
Multimedia & Handheld Device Forensics	Marcus Rogers	Purdue University
Cyber Crime Investigations	Angela Orebaugh	George Mason University
Cyber Security & Information Warfare	Michael Smith	Symantec
Standardization & Accreditation	Carrie Whitcomb	UCF
Forensics & Law	Stephen V. Treglia	Nassau County DA's Office
	Susan Axelrod	NY County DA's Office
Open Source Forensic Training	NYS Digital & Multimedia Evidence TWG	

Technical Program Committee

Fabio R. Auffant II	NYS Police, USA
Nicole Beebe	University of Texas at San Antonio, USA
George Berg	University at Albany, SUNY, USA
Roger Debreceny	University of Hawaii, USA
Ingrid Fisher	University at Albany, SUNY, USA
Miroslav Goljan	SUNY Binghamton, USA
Richard Hurley	University of Connecticut, USA
Andrew Jones	British Telecom, UK
Michael Lavine	Johns Hopkins University, USA
Cathryn Levine	NYS Division of Criminal Justice Services, USA
Siwei Lyu	University at Albany, SUNY, USA
Jeimy Jose Cano Martinez	Universidad de Los Andes, CO
William F. Mosher Jr.	N.Y.S. Police Financial Crimes Unit, USA
David Naccache	ENS DI, Equipe de Cryptographie, FR
Damira Pon	University at Albany, SUNY, USA
H. R. Rao	University at Buffalo, SUNY, USA
Indajit Ray	Colorado State University, USA
Golden G. Richard III	University of New Orleans, USA
Marc Rogers	Purdue University, USA
Michael Smith	NYS CSCIC
Gale Spring	RMIT University, AU
Leonard Stokes	Siena College, USA
Miklos A. Vasarhelyi	Rutgers University, USA
Wei Yan	Trend Micro, USA

External Reviewers

Rob Brown, NYS CSCIC, USA
Thomas Hacker, Purdue University, USA
Sydney Liles, Purdue University, USA
Gregg Gunsch, Defiance College, USA
Sam Liles, Purdue University, USA
John Springer, Purdue University, USA

Welcome to ICDF2C 2009!

Message from the Conference General Chair

Sanjay Goel

It gives me great pleasure to welcome you all to the First International Conference on Digital Forensics and Cyber Crime (ICDF2C). The field of digital forensics is growing rapidly with implications for several fields including law enforcement, network security, disaster recovery and accounting. This is a multidisciplinary area that encompasses multiple fields, including: law, computer science, finance, networking, data mining, and criminal justice. This conference brings together practitioners and researchers from diverse fields providing opportunities for business and intellectual engagement among attendees.

The conference features with an excellent program comprised of high quality paper presentations and invited speakers from all around the world as well as training from highly respected members of the field. The conference is run over three days. The first day features accounting fraud, financial crime, and multimedia and handheld forensics related tracks. The second day of the conference features forensics law and cyber crime tracks. The third day of the conference features both basic and advanced tutorials on open source forensics. We also have two outstanding keynotes on the first two days of the conference - the first keynote by Miklos Vasarhelyi is focused on financial crimes and accounting fraud and the second keynote by Nitesh Dhanjani is focused on digital forensics and crime.

The conference is organized by the School of Business at the University at Albany, State University of New York with partnership with New York State Police and collaboration with the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering (ICST) and Create-Net. The conference is also sponsored by the New York State Department of Criminal Justice Services (DCJS).

I would like to thank the conference co-chairs Technical Lt. Fabio Auffant from the Computer Crime Unit of the New York State Police and Ingrid Fisher from the University at Albany for helping to organize the conference. Thanks also to Leonard Stokes from Siena College, Cathryn Levine from DCJS, and Senior Investigator William Mosher from the Financial Crimes Unit of the New York State Police for helping with organization of the conference. Technical Lt. Auffant also was integral in getting the participation of the New York State Digital & Multimedia Evidence Technical Working Group, members of which are offering the basic and advanced forensics tutorials on the last day of the conference.

Many thanks to Stephen Treglia for organizing the forensics and law track and making arrangements for CLE credits, Carrie Whitcomb for organizing the standardization and accreditation track, Michael Alles for the accounting forensics track, and Angela Oerbaugh for the cyber crime investigations track. I am also very grateful to Michael Smith and Marc Rogers (cyber security & information warfare and multimedia & handheld device forensics track chairs respectively) for their help in managing the review process and to the other technical program committee members for their assistance in paper reviews. In addition, I would like to thank Sally Mills for an excellent job in dealing with local arrangements and the ICST staff including Karen Decker, Beatrix Ransburg, Barbara Torok, and Eszter Hajdu for leading us through the process of organizing the conference.

The conference came together through a lot of work by my dedicated assistants Damira Pon, the Organizational Chair, and a UAlbany doctoral student as well as Anthony Colon a UAlbany undergraduate student. They worked tirelessly keeping track of the papers, working on the program details, helping with reviews, and supporting the authors. I would like to express my deep appreciation for their hard work. Thanks to Robert Tracey and Damira Pon for developing and reviewing the conference website.

Sanjay Goel
Conference General Chair, ICDF2C 2009

Table of Contents

Technical Program at a Glance

WEDNESDAY SEPTEMBER 30, 2009	
REGISTRATION – *Upper Mezzanine* 8:00 - 9:00am	
PLENARY SESSION – *Stonehenge D* 9:00 - 10:30am	
MORNING COFFEE AND PASTRY BREAK *Upper Mezzanine* – 10:30-11:00am	
Miklos Vasarhelyi, Rutgers Univ. – *Stonehenge D* 11:00-12:00pm	
LUNCH – *Stonehenge C* 12:00 – 1:00pm	
ICDF2C SESSION 1 1:00 - 3:00PM	
TRACK A- Stonehenge A	*TRACK B- Stonehenge D*
ACCOUNTING & FRAUD TRACK *Chairs: Michael Alles*	*MULTIMEDIA & FORENSICS I TRACK* *Chair: Marcus Rogers & Ibrahim Baggili*
AFTERNOON BEVERAGE AND DESSERT BREAK *Upper Mezzanine* – 3:00 - 3:30pm	
ICDF2C SESSION 2 3:30 - 5:30pm	
TRACK A- Stonehenge A	*TRACK B- Stonehenge D*
FINANCIAL CRIMES TRACK *Chair: William F. Mosher*	*MULTIMEDIA & FORENSICS II TRACK* *Chair: Marc Rogers & Ibrahim Baggili*
GALA DINNER – *Phoenix Ballroom* 7:00-8:30pm	

THURSDAY OCTOCER 1 , 2009	
REGISTRATION – *Upper Mezzanine* 8:00 – 9:00am	
Nitesh Dhanjani, Ernst & Young, LLP – *Stonehenge D* 9:00 – 10:00am	
MORNING COFFEE AND PASTRY BREAK *Upper Mezzanine* – 10:30-11:00am	
ICDF2C SESSION 3 10:30am – 12:00pm	
TRACK A- Stonehenge A	*TRACK B- Stonehenge D*
CYBER CRIME INVESTIGATIONS TRACK *Chair: Angela Orebaugh*	*FORENSICS & LAW I TRACK* *Chair: Stephen V. Treglia*
LUNCH – *Stonehenge C* 12:00 – 1:00pm	
ICDF2C SESSION 4 1:00 - 3:00pm	
TRACK A- Stonehenge A	*TRACK B- Stonehenge D*
CYBER SECURITY & INFORMATION WARFARE TRACK *Chair: Michael Smith*	*FORENSICS & LAW II TRACK* *Chair: Susan Axelrod*
AFTERNOON BEVERAGE AND DESSERT BREAK RAFFLE WINNER ANNOUNCEMENT *Upper Mezzanine* – 3:00 - 3:30pm	
ICDF2C SESSION 5 3:30 - 6:00pm	
TRACK A- Stonehenge A	*TRACK B- Stonehenge D*
FORENSIC STANDARDS & ACCREDITATION *Chair: Carrie Whitcomb*	*FORENSICS & LAW III TRACK* *Chair: Stephen V. Treglia*
SPEAKERS & ORGANIZERS DINNER *(TBA)* 7:00-8:30pm	

FRIDAY OCTOBER 2, 2009
REGISTRATION – *Stonehenge C* 8:00 – 9:00am
ICDF2C SESSION 6 – *Stonehenge C*
BASIC OPEN SOURCE FORENSICS TRAINING 9:00 - 10:30am **Open Source Forensic Tools: Introduction** *NYS Digital & Multimedia Evidence Technical Working Group*
MORNING COFFEE AND PASTRY BREAK *Stonehenge C* – 10:30 – 11:00am
ICDF2C SESSION 7 – *Stonehenge C*
ADVANCED OPEN SOURCE FORENSICS TRAINING 11:00-12:30pm **Open Source Forensic Tools: Live Memory Forensics** *NYS Digital & Multimedia Evidence Technical Working Group*
CONFERENCE WRAP-UP– *Stonehenge C* 12:30-1:00pm

Day 1

Wednesday, September 30, 2009

REGISTRATION – *Upper Mezzanine* **8:00 – 9:00am**

PLENARY SESSION: INVITED SPEAKERS - *Stonehenge D* **9:00 – 10:30am**

George Phillip is the 18th president of the University at Albany, State University of New York. He was appointed to this position by the State University of New York (SUNY) Board of Trustees on June 16, 2009 after serving 18 months as the interim president. Prior to this appointment, Philip served as executive director of the New York State Teachers' Retirement System (NYSTRS), one of the 10 largest public retirement funds in the nation, with more than 400,000 members and managed assets of $105 billion, since 1995 and as chief investment officer for the system since 1992. He has served as the chairman of the University Council from 1996-2007 and is a member of the board of directors of the Research Foundation of SUNY. He served from 1970 – 1976 in the New York Army National Guard attached to the 42nd infantry. He has a B.A. and M.A. in History from the University at Albany and a J.D. from the Western New England College School of Law.

Superintendant Harry J. Corbitt was unanimously confirmed the State Police Superintendent by the New York State Senate in 2008 as the first African-American in the history of the State Police to hold the agency's highest rank. Superintendant Corbitt was a member of the New York State Police for more than 25 years before his retirement in 2004. Prior to his appointment as Superintendent, he was the Director of Safe Schools and Violence Prevention for the City of Albany School District. A life term member of the National Organization of Black Law Enforcement Executives, Colonel Corbitt served as the Region One Vice President from 2003 to 2007. He has also served as a member of the Advisory Board for the Center of American and International Law Institute for Law Enforcement Administration. From 1966 to 1972, Superintendent Corbitt served in the United States Army in the Military Intelligence Division. He was awarded the Bronze Star Medal for Meritorious Achievement in Ground Operations Against Hostile Forces.

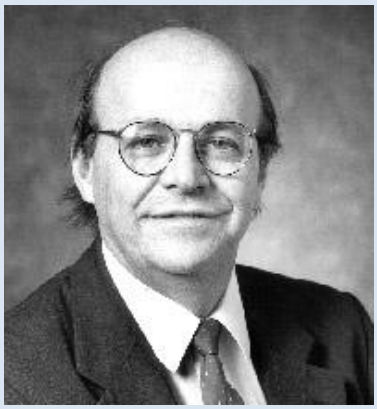
William F. Pelgrin is the Director of the NYS Office of Cyber Security & Critical Infrastructure Coordination (CSCIC) and the Chief Cyber Security Officer for New York State. Mr. Pelgrin is responsible for directing NYS efforts regarding cyber readiness and resilience. CSCIC operates a 7x24 Cyber Security Center to analyze and respond to intrusions and other anomalous cyber activity; deploy intrusion/prevention detection architecture for critical segments of states and local governments' network and computing infrastructure. He is the Multi-State ISAC Chair which collaborates across states to better prevent, detect, respond to and recover from cyber incidents representing the 50 states, the District of Columbia, local governments and U.S. Territories. He was elected Chair of the National Information ISAC Council, whose mission is to advance the physical and cyber security of the critical infrastructures of North America. Also, Mr. Pelgrin was appointed in 2007 to serve as a Commission Member of the Center for Strategic and International Studies (CSIS) Commission on Cyber Security to Brief the President of the United States.

MORNING COFFEE AND PASTRY BREAK **10:30 – 11:00am**

D1 Keynote: Miklos Vasarhelyi, Rutgers University - *Stonehenge D* **11:00 – 12:00pm**

Continuous Monitoring, Continuous Audit and Forensics: What Management Needs to Know
We are in the real time economy. Modern businesses focus on rapid response to satisfy customers and deal with the competitive environment. Technology relies on sensors, ERPs, continuous monitoring, and heavy analytics to understand what clients are doing and to respond to their needs. This talk discusses how forensic analysis, forensic experience and real time technology can be combined to create a major discrepancy deterrence framework for business. The key steps in the process, management considerations, and a profile of risk are discussed. Projections are made for the issues, methods and concerns in the next five years.

Biography: Miklos A. Vasarhelyi [Ph.D in MIS (UCLA) MBA (MIT) and BS in Economics and Electrical Engineering (the State University of Guanabara and Catholic University of Rio de Janeiro)]. Professor Vasarhelyi is currently the KPMG Professor of Accounting Information Systems and Director of the Continuous Auditing and Reporting Laboratory (CARLAB) at Rutgers University. He is also the Technology Consultant at the AT&T Laboratories. He has published more than 200 journal articles and 20 books. He is the editor of the Artificial Intelligence in Accounting and Auditing series and academic journals. Professor Vasarhelyi has taught executive programs on electronic commerce to many large international organizations including GE, J&J, Eli Lilly, Baxter, ADL, Volvo, Siemens, Chase Bank, and AT&T.



LUNCH – *Stonehenge C* **12:00 – 1:00pm**

ICDF2C SESSION 1 **1:00 – 3:00pm**

TRACK A – Stonehenge A	***TRACK B – Stonehenge D***
ACCOUNTING & FRAUD TRACK *Chair: Michael Alles, Rutgers University*	***MULTIMEDIA & HANDHELD DEVICE FORENSICS I TRACK*** *Chair: Marcus Rogers, Purdue University / Ibrahim M Baggili, Zayed University, Abu Dhabi, United Arab Emirates*
Digital Evidence Composition in Fraud Detection Sriram Raghavan, *Information Security Institute, Queensland University of Technology* S.V. Raghavan, *Network Systems Laboratory, Dept. of Computer Science & Engineering, IIT Madras*	File Carving for Forensics Recovery Nasir Memon, *Polytechnic University & Digital-Assembly*
Would Continuous Auditing Have Prevented the Credit Crisis? Michael Alles & Miklos Vasarhelyi, *Rutgers Business School* Roger Debreceny, *University of Hawaii*	iForensics: Forensic Analysis of Instant Messaging on Smart Phones Mohammad Iftekhar Husain & Sridhar Ramalingam, *University of Buffalo*
A Model to Detect Potentially Fraudulent/ Abnormal Wires of an Insurance Company: An Unsupervised Rule-based Approach Yongbum Kim , *Rutgers University*	A Survey of Forensic Localization and Tracking Mechanisms in Short-Range and Cellular Networks Saif M Al-Kuwari, *Information Security Group, Department of Mathematics, Royal Holloway, University of London*
Intelligent Visual Fraud: Supporting Fraud	

Detection Efforts of Exchange Regulators Using Visual Modeling Abbas Bagherian Kasgeri, *IAU University* Hamed Mosavi, *Tehran Stock Exchange* Saeed Roohani, *Bryant University*	Stephen Wolthusen, *Norwegian Information Security Laboratory, Gjøvik University College* SMIRK SMS Management and Information Retrieval Kit Ibrahim M Baggili, *Zayed University, Abu Dhabi, United Arab Emirates* Ashwin Mohan & Marcus Rogers, *Purdue University*
AFTERNOON BEVERAGE AND DESSERT BREAK	**3:00 – 3:30pm**
ICDF2C SESSION 2	**3:30 – 5:30pm**
TRACK A – Stonehenge A	***TRACK B – Stonehenge D***
FINANCIAL CRIMES TRACK *Chair: William F. Mosher, NYS Police* Towards a new Data Mining-based Approach for Anti-Money Laundering in an International Investment Bank Nhien-An Le-Khac, Sammer Markos & Mohand-Tahar Kechadi, *School of Computer Science & Informatics, University College Dublin Belfield* Anti-Corruption Compliance and Remediation Justin Offen & Matt Shelhorse, *PricewaterhouseCoopers LLP, New York Office* Anatomy of a Fraud Investigation – the First 48 Hours and Beyond Vincent Hom & Jared D. Crafton *Fraud Investigation & Dispute Services, Ernst & Young LLP*	***MULTIMEDIA & HANDHELD DEVICE FORENSICS II TRACK*** *Chair: Marcus Rogers, Purdue University / Ibrahim M Baggili, Zayed University, Abu Dhabi, United Arab Emirates* Localization and Detection of Vector Logo Image Plagiarism Jong P. Yoon & Zhixiong Chen, *Dept of Computer Information Science, Mercy College* Analysis of Free Download Manager (FDM) for Forensic Artefacts Muhammad Yasin, Muhammad Arif Wahla & Firdous Kausar, *Information Security Department, College of Signals, National University of Science and Technology* On the Reliability of Cell Phone Camera Fingerprint Recognition Martin Steinebach, Mohamed El Ouariachi & Huajian Liu, *Information Assurance, Fraunhofer SIT* Stefan Katzenbeisser, *CASED, Darmstadt*
GALA DINNER - *Phoenix Ballroom*	**7:00 – 8:30pm**

Day 2

Thursday, October 1, 2009

REGISTRATION - *Stonehenge C* **8:00 – 9:00am**

D2 KEYNOTE: Nitesh Dhanjani, Ernst & Young LLP - *Stonehenge D* 9:00 – 10:00am

Psychotronica: Exposure, Control, and Deceit

This talk will expose how voluntary and public information from new communication paradigms such as social networking applications can enable you to remotely capture private information about targeted individuals. Topics of discussion will include: Hacking the Psyche: Remote behavior analysis that can be used to construct personality profiles to predict current and future psychological states of targeted individuals, including discussions on how emotional and subconscious states can be discovered even before the target is consciously aware. Techniques on how individuals may be remotely influenced by messaging tactics, and how criminal groups and governments may use this capability, including a case study of Twitter and the recent terror attacks in Bombay. Reconnaissance and pillage of private information, including critical data that the victim may not be aware of revealing, and that which may be impossible to protect by definition. The goal of this presentation is to raise consciousness on how the new paradigms of social communication bring with it real risks as well as marketing and economic advantages.

Biography: Nitesh Dhanjani is the author of "Network Security Tools: Writing, Hacking, and Modifying Security Tools" (O'Reilly) and "HackNotes: Linux and Unix Security" (Osborne McGraw-Hill). He is also a contributing author to "Hacking Exposed 4" (Osborne McGraw-Hill) and "HackNotes: Network Security" (Osborne McGraw-Hill). Dhanjani is a frequent speaker at some of the most well known information security events around the world including Hack in the Box, RSA, the Black Hat Briefings and the Microsoft Bluehat Briefings. Currently, Dhanjani is Senior Manager at Ernst & Young LLP where he is responsible for advising some of the largest corporations on how to establish enterprise wide information security programs and solutions. Dhanjani is also responsible for evangelizing brand new technology service lines around emerging technologies and trends such as cloud computing and virtualization. Prior to E&Y, Dhanjani was Senior Director of Application Security and Assessments at Equifax where he spearheaded brand new security efforts into enhancing the enterprise SDLC, created a process for performing source code security reviews & threat modeling, and managed the attack & penetration team. Before Equifax, Dhanjani was Senior Advisor at Foundstone's Professional Services group where, in addition to performing security assessments, he contributed and taught Foundstone's Ultimate Hacking security courses. Dhanjani graduated from Purdue University with both a Bachelor's and Master's degree in Computer Science. In summary, Dhanjani is probably the greatest human being who ever lived.

MORNING COFFEE AND PASTRY BREAK **10:00 – 10:30am**

ICDF2C SESSION 3 10:30am – 12:00pm

TRACK A – Stonehenge A	*TRACK B – Stonehenge D*
CYBER CRIME INVESTIGATIONS TRACK *Chair: Angela Orebaugh, George Mason University* Analysis of Evidence Using Formal Event Reconstruction Joshua James & Pavel Gladyshev, *Centre for Cybercrime Investigation, University College Dublin* Mohd Taufik Abdullah, *Department of Computer Science Faculty of Computer Science and Information Technology, Putra University of Malaysia* Yuandong Zhu, *Centre for Cybercrime Investigation, University College Dublin* Data Mining Instant Messaging Communications to Perform Author Identification for Cybercrime Investigations Angela Orebaugh & Jeremy Allnutt, *George Mason University* Digital Evidence Retrieval and Forensic Analysis on Gambling Machine Pritheega Magalingam, Azizah Abdul Manaf, Rabiah Ahmad & Zuraimi Yahya, *University Technology Malaysia*	***FORENSICS & LAW I TRACK*** *Chair: Steven V. Treglia, Nassau County DA Office* Electronic Communications Privacy Act Susan Axelrod, *New York County DA's Office Appeals Bureau, Senior Appellate Counsel* *Anticipated CLE – 75 min*
LUNCH – *Stonehenge C*	**12:00 – 1:00pm**
ICDF2C SESSION 4	**1:00 – 3:00pm**
TRACK A – Stonehenge A	***TRACK B – Stonehenge D***
CYBER SECURITY & INFORMATION WARFARE TRACK *Chair: Michael Smith, CSCIC* Detecting and Preventing the Electronic Transmission of Illicit Images and its Network Performance Amin Ibrahim & Miguel Vargas Martin, *University of Ontario Institute of Technology* A Discretionary Access Control Method for Preventing Data Exfiltration via Removable Devices Duane Wilson, *Network Security Branch, U.S. Army Research Laboratory* Michael Lavine, *Information Security Institute, John Hopkins University*	***FORENSICS & LAW II TRACK*** *Chair: Steven V. Treglia, Nassau County DA Office* Online Acquisition of Digital Forensic Evidence Mark Scanlon & Mohand-Tahar Kechadi, *UCD Centre for Cybercrime Investigation, School of Computer Science and Informatics, University College Dublin* Criminal Defense Challenges in Computer Forensics Rebecca Mercuri, *Ph.D. Computer Forensics Expert, Notable Software, Inc. and The College of New Jersey* Forensics as a Toolset to Support eDiscovery Mandates in Civil Litigation Michael W. Deyo, Esq., *Director, eDiscovery and Forensics, JANUS Associates* *Anticipated CLE – 50 min*

A Host-based Approach for BotNet Investigation Frank Y.W. Law, K.P. Chow, Pierre K.Y. Lai & Hayson K.S. Tse, *The University of Hong Kong*	
AFTERNOON BEVERAGE AND DESSERT BREAK	**3:00 – 3:30pm**
ICDF2C SESSION 5	**3:30 – 6:00pm**
TRACK A – Stonehenge A	***TRACK B – Stonehenge D***
FORENSIC STANDARDIZATION & ACCREDITATION TRACK *Chair: Carrie Whitcomb, National Center for Forensic Science, University of Central Florida* The Evolution of Digital Evidence as a Forensic Science Discipline Carrie Whitcomb, *National Center for Forensic Science, University of Central Florida* Accreditation for the Digital Forensics Laboratory John K. Neuner, *Program Manager, ASCLD/LAB-International Accreditation Program* Digital Evidence Standards Barbara Guttman, *National Institute for Standards and Technology (NIST)*	***FORENSICS & LAW III TRACK*** *Chair: Stephen V. Treglia, Nassau County DA Office* Admissibility of Computer-Generated Evidence Stephen V. Treglia, *Chief of the Technology Crime Unit of the Nassau County DA's Office (NCDA)* *Anticipated CLE – 75 min* Direct and Cross-Examination of Computer Forensic Examiner Stephen V. Treglia, *Chief of the Technology Crime Unit of the Nassau County DA's Office (NCDA)* Susan Axelrod, *New York County District Attorney's Office Appeals Bureau, Senior Appellate Counsel* *Anticipated CLE – 75 min*
SPEAKERS & ORGANIZERS DINNER – *TBA*	**7:00 – 8:30pm**

Day 3

FRIDAY OCTOBER 2, 2009	
REGISTRATION – *Stonehenge C*	**8:00 – 9:00am**
ICDF2C SESSION 6 – *Stonehenge C*	**9:00 - 10:30am**
BASIC OPEN SOURCE FORENSICS TRAINING Open Source Forensic Tools: Introduction Nikki Brate, John Griffin, Corey Harrell & Michael Gibbs *NYS Digital & Multimedia Evidence Technical Working Group*	
MORNING COFFEE AND PASTRY BREAK – *Stonehenge C*	**10:30 – 11:00am**
ICDF2C SESSION 7 – *Stonehenge C*	**11:00 - 12:30pm**
ADVANCED OPEN SOURCE FORENSICS TRAINING Open Source Forensic Tools: Live Memory Forensics Adnan Baykal & Mark Bilanski *NYS Digital & Multimedia Evidence Technical Working Group*	
CONFERENCE WRAP-UP – *Stonehenge C*	**12:30-1:00pm**

Abstract

DAY 1: WEDNESDAY SEPTEMBER 30, 2009

ICDF2C Session 1 (1:30 – 3:00pm)

ACCOUNTING & FRAUD TRACK
Chair: Michael Alles, Rutgers University

Digital Evidence Composition in Fraud Detection

Sriram Raghavan, *Information Security Institute, Queensland University of Technology*
S.V. Raghavan, *Network Systems Laboratory, Dept. of Computer Science & Engineering, IIT Madras*

In recent times, digital evidence has found its way into several digital devices. The storage capacity in these devices is also growing exponentially. When investigators come across such devices during a digital investigation, it may take several man-hours to completely analyze the contents. To date, there has been little achieved in the zone that attempts to bring together different evidence sources and attempt to correlate the events they record. In this paper, we present an evidence composition model based on the time of occurrence of such events. The time interval between events promises to reveal many key associations across events, especially when on multiple sources. The time interval is then used as a parameter to a correlation function which determines quantitatively the extent of correlation between the events. The approach has been demonstrated on a network capture sequence involving phishing of a bank website. The model is scalable to an arbitrary set of evidence sources and preliminary results indicate that the approach has tremendous potential in determining correlations on vast repositories of case data.

Would Continuous Auditing Have Prevented the Credit Crisis?

Michael Alles, *Rutgers Business School*

This paper examines the question whether the credit and subprime crisis could have been avoided if firms had adopted continuous auditing, which is a system of automated auditing with assurance provided with reduced latency with the transaction date. While we cannot make such a bold claim examining the question raises important questions about the role and efficacy of auditing and the differences in scope and impact of manual versus automated auditing.

A Model to Detect Potentially Fraudulent/ Abnormal Wires of an Insurance Company: An Unsupervised Rule-based Approach

Yongbum Kim , *Rutgers University*

Fraud prevention/detection is an important function of internal control. Prior literature has focused mainly on fraud committed by external parties such as customers. However, according to a 2009 survey by the Association of Certified Fraud Examiners (ACFE), intense financial pressure s of the current economic crisis have led to an increase of fraud and it was noted that employees pose the greatest fraud threat. Fraud detection is difficult because fraudulent transactions look similar to normal transactions and fraudsters are highly adaptive to new fraud prevention and detection techniques. In academic research methodology, classification methods based on prior data are used to discriminate fraudulent from legitimate data. However, this methodology may not be practicable because known fraud examples are rarely documented and disclosed. This study proposes the unsupervised method of profiling fraud. The fraud detection model is based on potential fraud/anomaly indicators in the wire transfer payment process

of a major insurance company in the United States. Each indicator is assigned an arbitrary score based on its severity. Once a particular wire transfer payment is processed through the indicators and scored, an aggregate total will be calculated and those wire transfer payments above a threshold will be suggested for investigation. Anomaly/outlier indicators are popular in practice because they can be translated into actionable items. Our contribution is to report what we have learned and to document our findings using fraud/anomaly indicators to detect potential fraud on real data from a major insurance company.

Intelligent Visual Fraud: Supporting Fraud Detection Efforts of Exchange Regulators Using Visual Modeling

Abbas Bagherian Kasgeri, *IAU University*
Hamed Mosavi, *Tehran Stock Exchange*
Saeed Roohani, *Bryant University*

Stock exchange regulators around the world are interested in fast and effective fraud detection mechanisms that continuously detect and report outliers. The proactive surveillance approach for detection of fraud is more cost effective over reactive. In many places around the world fraudulent attempts at the securities markets are becoming more creative, and techniques are changing rapidly over the time. This paper discusses a visual modeling concept as a prototype for supporting financial fraud detection by stock exchange regulators. The proposed solution is a dynamic fraud modeling and monitoring for regulatory organizations. Further, this paper extends the application of visual modeling for fraud detection to the supply chain. The idea is to design a human surveillance mechanism using fraud detection algorithm from the literature, and delegate some monitoring activities to a tool instead: "Intelligent Visual Fraud". This tool is a new visual application that designs dynamic patterns for detecting financial frauds. It processes XBRL files for calculation of fraud alerts and then compiles and reports fraud pattern detected in financial statements of the filer. XBRL Surveillance and Analysis desktop is also able to apply ratio analysis on companies' annual and quarterly report.

MULTIMEDIA & HANDHELD DEVICE FORENSICS I TRACK

Chair: Marcus Rogers, Purdue University

File Carving for Forensics Recovery

Nasir Memon, *Polytechnic University & Digital-Assembly*

ABSTRACT

iForensics: Forensic Analysis of Instant Messaging on Smart Phones

Mohammad Iftekhar Husain & Sridhar Ramalingam, *University of Buffalo*

Smart phones with Internet capability are growing in popularity, due to many of their useful capabilities. Among other handy features of smart phones, Instant Messaging (IM) is very popular due to the level of convenience it provides in interpersonal communications. As the usage of IM on smart phone is increasing rapidly, it is important to take measures in advance from forensic standpoint forecasting the potential use of it in cyber crimes such as the cyber stalking and cyber bullying. Although, current IM applications for smart phones are in most cases a downsized version of the one used on traditional computers, diverse structure of file systems and storage device on different smart phones pose unique challenges to forensic examiners for recovering digital evidences of a conversation under investigation. In this work, we study and report the forensic analysis of three different IMs: AIM, Yahoo! Messenger and Google Talk, (both client based and web based version) on Apple iPhone. Our results show that the forensic analysis of IMs on smart phones has significant value and needs further attention.

A Survey of Forensic Localization and Tracking Mechanisms in Short-Range and Cellular Networks

Saif M Al-Kuwari, *Information Security Group, Department of Mathematics, Royal Holloway, University of London*
Stephen Wolthusen, *Norwegian Information Security Laboratory, Gjøvik University College*

Localization and tracking are critical tools in criminal and, increasingly, forensic investigations, which we show to be greatly aided by the proliferation of mobile phone and other wireless devices even if such devices are not suitable for communication and hence interception. In this paper we therefore provide a survey and taxonomy of both established and novel techniques for tracking the whereabouts of individuals and devices for different environments and platforms as well as the underlying assumptions and limitations in each case. In particular, we describe cellular, wireless, and personal area networks in infrastructure and ad- hoc environments. As individual localization and tracking methods do not always yield the required precision and accuracy, may require collaboration, or will exhibit gaps in densely built-up or highly active radio frequency environments, we additionally discuss selected approaches de- rived from multisensor data fusion and tracking applications for enhancing performance and assurance. This paper also briefly discusses possible attacks against a localization/tracking process and how trustworthy the measurement estimations are, an aspect that has been evidently less investigated so far.

SMIRK SMS Management and Information Retrieval Kit

Ibrahim M Baggili, *Zayed University, Abu Dhabi, United Arab Emirates*
Ashwin Mohan & Marcus Rogers, *Purdue University*

There has been tremendous growth in the information environment since the advent of the Internet and wireless networks. Just as e-mail has been the mainstay of the web in its use for personal and commercial communication, one can say that text messaging or Short Message Service (SMS) has become synonymous with communication on mobile networks. With the increased use of text messaging over the years, the amount of mobile evidence has increased as well. This has resulted in the growth of mobile forensics. A key function of digital forensics is efficient and comprehensive evidence analysis which includes authorship attribution. Significant work on mobile forensics has focused on data acquisition from devices and little attention has been given to the analysis of SMS. Consequentially, we propose a software application called: SMS Management and Information Retrieval Kit (SMIRK). SMIRK aims to deliver a fast and efficient solution for investigators and researchers to generate reports and graphs on text messaging. It also allows investigators to analyze the authorship of SMS messages.

ICDF2C Session 2 (3:30 – 5:30pm)

FINANCIAL CRIMES TRACK

Chair: William F. Mosher, NYS Police

Towards a new Data Mining-based Approach for Anti-Money Laundering in an International Investment Bank

Nhien-An Le-Khac, Sammer Markos & Mohand-Tahar Kechadi, *School of Computer Science & Informatics, University College Dublin Belfield*

Today, money laundering (ML) poses a serious threat not only to financial institutions but also to the nation. This criminal activity is becoming more and more sophisticated and seems to have moved from the cliché of drug trafficking to financing terrorism and surely not forgetting personal gain. Most international financial institutions have been implementing anti-money laundering solutions (AML) to

fight investment fraud. However, traditional investigative techniques consume numerous man-hours. Recently, data mining approaches have been developed and are considered as well-suited techniques for detecting ML activities. Within the scope of a collaboration project for the purpose of developing a new solution for the AML Units in an international investment bank based in Ireland, we propose a new data mining-based approach for AML. In this paper, we present this approach and some preliminary results associated with this method when applied to transaction datasets.

Anti-Corruption Compliance and Remediation

Justin Offen & Matt Shelhorse, *PriceWaterhouseCoopers LLP, New York Office*

Recent settlements of corruption cases with US and global regulators have shown tangible benefits to companies that have developed robust and effective compliance programs, including reduced sanctions and the ability to continue operations in key territories where problems have occurred. A proactive approach to developing such a program can add value for an organization by strengthening its reputation with key regulators, closely monitoring and managing risks, avoiding potentially harmful transactions or relationships, boosting employee morale, managing revenue leakage/expense creep, working to limit potentially damaging allegations/actions and reducing the management or operational distractions often caused by an investigation. This session will provide an overview of hot topics, trends and techniques in anti-corruption compliance and remediation, including the following:

- The Foreign Corrupt Practices Act (FCPA) - key provisions, terms and defences/exceptions;
- Regulatory and enforcement environment - current trends, recent settlements and global standards;
- International business risks and red flags - framework for analysis, typical areas of risk, third parties
- and intermediaries, travel and entertainment and other areas;
- The role of the forensic accountant - investigations, transaction testing, M&A activity, compliance
- assessments and training programs; and
- Use of technology - managing global projects, tools and methodology, locating and obtaining data,
- typical obstacles, data quality challenges, data privacy and protection and techniques for the analysis of general/subledgers.

The program is intended for anyone with an interest in this area, which has been a hot topic in recent years from both a compliance and investigative perspective. As seen from recent bribery and corruption cases, regulatory scrutiny has remained at high levels across many industries and geographies and indications are that these trends will continue for the foreseeable future.

Anatomy of a Fraud Investigation – the First 48 Hours and Beyond

Vincent Hom & Jared D. Crafton
Fraud Investigation & Dispute Services, Ernst & Young LLP

You have to conduct an investigation into the facts and circumstances behind a financial statement restatement, a scandal related to the credit crisis, or allegations of bribery and corruption. How do you respond? What capabilities do you require? How do you assemble a competent team with the right knowledge, skills and experiences to face the myriad of issues in front of you? What are some of the long term consequences of the early decisions you must make? The first 48 hours of an investigation can set the stage for success or start you on the path to terrific failure. Two experienced Ernst & Young investigators share their experiences and insight into getting through those first critical 48 hours and beyond.

MULTIMEDIA & HANDHELD DEVICE FORENSICS II TRACK

Chair: Marcus Rogers, Purdue University

Localization and Detection of Vector Logo Image Plagiarism

Jong P. Yoon & Zhixiong Chen, *Dept of Computer Information Science, Mercy College*

One of the main research issues in forensic computing is to protect intellectual properties. Logo images, one type of intellectual properties, are posted in the Internet and widely available. Logo image plagiarism and theft are not unusual. Detection and localization of logo image plagiarism are crucial to protect logo intellectual property. In recent years, logo images that are written in Scalable Vector Graphics format are able to be rendered efficiently in the web browser and accessed easily. In this paper, after introducing logo images edited and rendered from scalable vector graphics, we classify all possible types of logo image plagiarism, localize a possible set of logo images being infringed using distance functions, and detect and verify logo plagiarism using reversible transformation. We believe our work is valuable to businesses involving logo creation and development.

Analysis of Free Download Manager (FDM) for Forensic Artefacts

Muhammad Yasin, Muhammad Arif Wahla & Firdous Kausar, *Information Security Department, College of Signals, National University of Science and Technology*

Free Download Manager (FDM) is one of the most popular download managers due to its free availability, high download speed and versatility. It contains a lot of information that is of potential evidentiary value even if a user deletes web browser history, cookies and temporary internet files. This software records download activities across multiple files saved with .SAV extensions in the User Profile. This paper analyzes: 1) the windows registry entries particularly concerned to configuration and user settings, 2) the log files (with .SAV extension) created by FDM to trace download activities, and 3) RAM and swap files from a forensic perspective. This research work describes a number of traces left behind after the use of FDM such as install location, default download path, downloaded files, and menu extensions to name a few, thus enabling digital investigators to search for and interpret download activities. The widespread use of FDM makes this research work an attractive option for forensic investigators, ranging from law enforcement agencies to employers monitoring personnel.

On the Reliability of Cell Phone Camera Fingerprint Recognition

Martin Steinebach, Mohamed El Ouariachi & Huajian Liu, *Information Assurance, Fraunhofer SIT*
Stefan Katzenbeisser, *CASED, Darmstadt*

Multiple multimedia forensic algorithms have been introduced allowing tracing back media copies back to its source by matching artifacts to fingerprint databases. While this offers new possibilities for investigating crimes, important questions arise: How reliable are these algorithms? Can a judge trust their results? How easy are they to manipulate? It has been shown that forensic fingerprints of digital cameras can be copied from one image to the next. Our aim is to develop new concepts for increasing the security of theses algorithms. In this work we describe the state of our research work regarding attacks against forensics and provide an outlook on future approaches to increase their reliability.

DAY 2: THURSDAY OCTOBER 1, 2009

ICDF2C Session 3 (10:30am – 12:00pm)

CYBER CRIME INVESTIGATIONS TRACK
Chair: Angela Orebaugh, George Mason University

Analysis of Evidence Using Formal Event Reconstruction
Joshua James & Pavel Gladyshev, *Centre for Cybercrime Investigation, University College Dublin*
Mohd Taufik Abdullah, *Department of Computer Science Faculty of Computer Science and Information Technology, Putra University of Malaysia*
Yuandong Zhu, *Centre for Cybercrime Investigation, University College Dublin*

This paper expands upon the finite state machine approach for the formal analysis of digital evidence. The proposed method may be used to support the feasibility of a given statement by testing it against a relevant system model. To achieve this, a novel method for modeling the system and evidential statements is given. The method is then examined in a case study example.

Data Mining Instant Messaging Communications to Perform Author Identification for Cybercrime Investigations
Angela Orebaugh & Jeremy Allnutt, *George Mason University*

Instant messaging is a form of computer-mediated communication (CMC) with unique characteristics that reflect a realistic presentation of an author's online stylistic characteristics. Instant messaging communications use virtual identities, which hinder social accountability and facilitate IM-related cybercrimes. Criminals often use virtual identities to hide their true identity and may also supply false information on their virtual identities. This paper presents an IM authorship analysis framework and feature set taxonomy for use in cyber forensics and cybercrime investigations. We explore authorship identification of IM messages to discover the parameters with the highest accuracy for determining the identity of a cyber criminal.

Digital Evidence Retrieval and Forensic Analysis on Gambling Machine
Pritheega Magalingam, Azizah Abdul Manaf, Rabiah Ahmad & Zuraimi Yahya, *University Technology Malaysia*

Hardware forensic analysis involves the process of analyzing digital evidence derived from digital sources. The analysis is done to facilitate and prove either the device is used to commit crime, whether it contains evidence of a crime or is the target of a crime. Gambling machines serve as the main source by which illegal games are conducted. This paper presents a method for retrieving information from a seized gaming machine, along with an analysis of the interpreted information to prove that the gaming machine was used illegally. The proposed procedures for the gambling machine forensic process will be important for forensic investigators (e.g., the police or private investigators), as they will assist these individuals in the digital forensic evidence analysis necessary to produce evidence relevant to illegal gambling.

FORENSICS & LAW I TRACK
Chair: Steven V. Treglia, Nassau County DA Office

Electronic Communications Privacy Act
Susan Axelrod, *New York County DA's Office Appeals Bureau, Senior Appellate Counsel*

The Electronic Communications Privacy Act, 18 U.S.C. 2701-2712, was enacted to address the privacy issues surrounding the growing use of computers, and storage facilities that stored and processed electronic data. The statute was enacted in 1986 and was most recently updated under the Patriot Act. The statute governs the circumstances under which storage providers may release the content of stored data as well as information about the subscribers using their services. In other words, it is the statutory scheme that governs how both private and government investigators may obtain information that is crucial to their investigations. Despite the importance of the statute, it poses a number of problems for lawyers, investigators and judges alike. The statutory scheme is difficult to navigate, rendering it unfriendly to users. It was also drafted prior to the popularity of the internet and the explosion of technology. As such, it is particularly unsuited to address all of the issues that investigators confront today, such as the appropriate method by which to obtain GPS information or other location information in real time. The Patriot Act did little to address most of these issues either.

As with all statutes, the ECPA is subject to interpretation by the courts. This judicial layer poses an additional problem, as many of the judges are not technically savvy and do not understand how information moves across the internet. Thus, the courts have difficulty interpreting the statute and, as a result, the case law in this area, while limited, is confusing and contradictory. In this lecture, I intend to discuss all of these problems. I will be doing so in a manner designed to assist practitioners in how to navigate the statute and to avoid potential pitfalls. First, I will provide an explanation of the ECPA's framework, with a focus on how both private investigators and government officials can obtain certain types of electronic data, such as the content of e-mail and information about the subscribers and users of e-mail accounts. I will also discuss how the statute should be used to obtain other types of electronic information from ISP's, such as, for instance, text messages. I will then go through the efforts that the courts have made to interpret the statutes in light of today's technology, highlighting the significant cases and noting how their analyses overlooks several of the statutes components. As part of this discussion, I will address the recent spate of federal cases dealing with whether and how the ECPA authorizes the collection of real-time information concerning the location of the user of a hand-held device.
Finally, I intend to summarize the statutory penalties for failure to follow the ECPA's provisions. I will discuss the fact that the statute does not mandate suppression as a remedy but looks instead to civil penalties. I will also list the statutory defenses to potential civil lawsuits.

Anticipated CLE – 75 min

ICDF2C Session 4 (1:00 – 3:00pm)

CYBER SECURITY & INFORMATION WARFARE TRACK
Chair: Michael Smith

Detecting and Preventing the Electronic Transmission of Illicit Images and its Network Performance
Amin Ibrahim & Miguel Vargas Martin, *University of Ontario Institute of Technology*

Child exploitation through the use of the Internet as a delivery and exchange tool is a growing method of abuse towards children. It is shown that a Stochastic Learning Weak Estimator learning algorithm and a Maximum Likelihood Estimator learning algorithm can be applied against Linear Classifiers to identify

and filter illicit pornographic images. In this paper, these two learning algorithms were combined with distance algorithms such as the Non-negative Vector Similarity Coefficient-based Distance algorithm, Euclidian Distance, and a Weighted Euclidian Distance algorithm. Experimental results showed that classification accuracies and the network overhead did have a significant effect on routing devices.

A Discretionary Access Control Method for Preventing Data Exfiltration via Removable Devices

Duane Wilson, *Network Security Branch, U.S. Army Research Laboratory*
Michael Lavine, *Information Security Institute, John Hopkins University*

One of the major challenges facing the security community today is how to prevent data exfiltration. Data exfiltration is the unauthorized release of information from a computer system or network of systems. Current methods attempt to address this issue by controlling the information that is released over the Internet. In this paper, we present a host-level discretionary access control method that focuses on exfiltration via removable devices (e.g. thumb drives or external hard drives). Using XML to store extended file attributes, we classify files based on user-defined distribution levels and the community of interest to which they belong. Files are classified with a distribution statement upon creation and re-classified (if necessary) when modified. By monitoring the access to all classified files present on a file system, we allow or prevent release of this information based on predefined policies. With this approach, we show that the unauthorized release of information can be prevented by using a system of accounting that is tied to access control policies. Users are given the authority to transfer files to a removable device according to their current access rights. As a proof of concept, our method demonstrates the value of using accounting as a means of preventing data loss or theft. Our approach can be applied to a variety of data types found on a file system including: executables, archived files, images, and even audio or video files.

A Host-based Approach for BotNet Investigation

Frank Y.W. Law, K.P. Chow, Pierre K.Y. Lai & Hayson K.S. Tse, *The University of Hong Kong*

Robot Networks (BotNets) are one of the most serious threats faced by the online community today. Since their appearance in the late 1990's, much effort has been expended in trying to thwart their unprecedented growth. However, with robust and advanced capabilities, it is very difficult for average users to avoid or prevent infection by BotNet malware. Moreover, whilst BotNets have increased in scale, scope and sophistication, the dearth of standardized and effective investigative procedures poses huge challenges to digital investigators in trying to probe such cases. In this paper we present a practical (and repeatable) host-based investigative methodology to the collection of evidentiary information from a Bot-infected machine. Our approach collects digital traces from both the network and physical memory of the infected local host, and correlates this information to identify the resident BotNet malware involved.

FORENSICS & LAW II TRACK

Chair: Steven V. Treglia, Nassau County DA Office

Online Acquisition of Digital Forensic Evidence

Mark Scanlon & Mohand-Tahar Kechadi, *UCD Centre for Cybercrime Investigation, School of Computer Science and Informatics, University College Dublin*

Providing the ability to any law enforcement officer to remotely transfer an image from any suspect computer directly to a forensic laboratory for analysis, can only help to greatly reduce the time wasted by forensic investigators in conducting on-site collection of computer equipment. RAFT (Remote

Acquisition Forensic Tool) is a system designed to facilitate forensic investigators by remotely gathering digital evidence. This is achieved through the implementation of a secure, verifiable client/server imaging architecture. The RAFT system is designed to be relatively easy to use, requiring minimal technical knowledge on behalf of the user. One of the key focuses of RAFT is to ensure that the evidence it gathers remotely is court admissible. This is achieved by ensuring that the image taken using RAFT is verified to be identical to the original evidence on a suspect computer.

Criminal Defense Challenges in Computer Forensics

Rebecca Mercuri, *Ph.D. Computer Forensics Expert, Notable Software, Inc. and The College of New Jersey*

Computer forensic techniques may be unfairly applied in order to tip the scales of justice in the direction of prosecution. Particular areas that are known to be problematic for defense experts include: erroneous allegations of knowledgeable possession; misuse of time stamps and metadata; control and observation of the discovery process; authentication issues; deficiencies and the lack of verification for proprietary software tools; deliberate omission or obfuscation of exculpatory evidence; and inadvertent risks resulting from the use of legitimate services. Examples in the author's caseload are used to illustrate these inequities in an effort to encourage reform.

Forensics as a Toolset to Support eDiscovery Mandates in Civil Litigation

Michael W. Deyo, Esq., *Director, eDiscovery and Forensics, JANUS Associates*

Discovery of electronically stored information during litigation requires attorneys to lead a multi-faceted approach with responsibility spanning across outside counsel firms, in-house counsel, senior management, Information Technology (IT) and Telecommunications departments, application owners, data custodians, and eDiscovery vendors. Forensic investigators must understand both the legal and practical issues invoked by eDiscovery in order to best support counsel's need to discover and produce electronic evidence during litigation. Moreover, inside counsel, IT, and forensic investigators will need to understand the interplay of eDiscovery and proactive records management in order to craft policies and business processes to control the risks and costs of litigation and eDiscovery. This session will brief recent developments in eDiscovery law and provide a foundation of knowledge that will aid corporations and government agencies in supporting eDiscovery needs and mandates through the use of computer forensics as a set of technical tools.

Anticipated CLE – 50 min

ICDF2C Session 5 (3:30 – 6:00pm)

FORENSIC STANDARDIZATION & ACCREDITATION TRACK

Chair: Carrie Whitcomb, National Center for Forensic Science, University of Central Florida

The Evolution of Digital Evidence as a Forensic Science Discipline

Carrie Whitcomb, *National Center for Forensic Science, University of Central Florida*

Law enforcement began to collect computer related items as evidence in the late 1970's. The FBI accepted a computer and it was taken to their Questioned Document Section in the 1980's. We have come a long way since then. Digital evidence is defined… "Any information of probative value that is stored or transmitted in a binary form"(SWGDE) and includes digitized text, sounds, numerals, images both still and moving. The scientific underpinnings related to digital evidence have been developed by following the Daubert criteria for the admissibility of scientific evidence in to court. The presentation will give you the history from one person's perspective.

Accreditation for the Digital Forensics Laboratory

John K. Neuner, *Program Manager, ASCLD/LAB-International Accreditation Program*

Laboratory accreditation for digital forensics laboratories in the US and internationally is currently based on ISO/IEC 17025:2005 accreditation requirements. Each accrediting body in the world offering accreditation in the digital forensics discipline will also require conformance with specific supplemental requirements. Examples of specific supplemental requirements will be reviewed. The primary focus of this presentation will be a general discussion of the ISO/IEC 17025:2005 accreditation requirements, with an emphasis on how key ISO requirements apply to the digital forensics discipline. The process of preparing for accreditation, undergoing the assessment, and maintaining accreditation will also be reviewed. Special requirements of the ASCLD/LAB-International accreditation program will be highlighted for those participants who have an interest in seeking accreditation with ASCLD/LAB.

Digital Evidence Standards

Barbara Guttman, *National Institute for Standards and Technology (NIST)*

FORENSICS & LAW III TRACK

Chair: Stephen V. Treglia, Nassau County DA Office

Admissibility of Computer-Generated Evidence

Stephen V. Treglia, *Chief of the Technology Crime Unit of the Nassau County DA's Office (NCDA)*

The admissibility of computer-generated evidence is rapidly becoming one of the hot topics of litigation in the 21st Century. With computers routinely being the repository of business records, online communications, as well as evidence of criminal activity and contraband, it is becoming the responsibility of every participant in the legal continuum to understand how to best acquire, preserve and analyze such evidence. This lecture will be a multi-faceted overview of the entire area, mostly from the criminal law point of view, but with many issues that will carryover well even to the civil arena. Specific topics will include search and seizure, acquisition of online evidence, forensics, admissibility of evidence, hearsay objections and solutions.

Anticipated CLE – 75 min

Direct and Cross-Examination of Computer Forensic Examiner

Stephen V. Treglia, *Chief of the Technology Crime Unit of the Nassau County DA's Office (NCDA)*
Susan Axelrod, *New York County District Attorney's Office Appeals Bureau, Senior Appellate Counsel*

The introduction of computer-generated evidence through the use of trained forensic examiner, once a rarity at trial, is becoming a regular occurrence. Likewise, the elements of testimony typically covered by the litigator seeking to have such proof admitted into evidence have begun to take the form of a ritualized series of questions and answers. As can be expected, the cross-examination of such a witness is as completely uncharted territory as the litigant may wish to pursue. This 75-minute session will present the direct and cross-examination of an experienced law enforcement officer who routinely performs computer forensic examinations. The two prosecutors conducting the mock direct and cross have both had prior experience attending the week-long sessions organized by the Federal Bureau of Investigation during which anywhere from 30-50 trainees of the FBI's Computer Analysis Response Team program are taken through similar direct and cross-examinations in a moot-court setting. During these week-long training sessions, each prosecutor conducts five or six direct and cross examinations of these trainees in an attempt to admit or exclude evidence secured as the result of a computer forensic examination.

Anticipated CLE – 75 min

DAY 3: FRIDAY OCTOBER 2, 2009

ICDF2C SESSION 6 (9:00 - 10:30am)

BASIC OPEN SOURCE FORENSICS TRAINING

Open Source Forensic Tools: Introduction

Nikki Brate, John Griffin, Corey Harrell & Michael Gibbs

NYS Digital & Multimedia Evidence Technical Working Group

The analysis of main memory can provide valuable help in incident response and forensic investigations. In this talk, we will be discussing how to perform Incident Response focusing on the importance of the evidence that can be found and extracted from the live memory using Open Source Tools. We will also be discussing other publically available tools and websites that aid analysts in incident response efforts. This will serve as a introductory training session for beginners and will provide a background for the next training session that follows.

ICDF2C SESSION 7 (11:00 - 12:30pm)

ADVANCED OPEN SOURCE FORENSICS TRAINING

Open Source Forensic Tools: Live Memory Forensics

Adnan Baykal & Mark Bilanski

NYS Digital & Multimedia Evidence Technical Working Group

The analysis of main memory can provide valuable help in incident response and forensic investigations. In this talk, we will be discussing how to perform Incident Response focusing on the importance of the evidence that can be found and extracted from the live memory using Open Source Tools. We will also be discussing other publically available tools and websites that aid analysts in incident response efforts. This session covers advanced topics building upon the training delivered in the previous training session.

Sponsors

Guidance™ SOFTWARE

The Maker of EnCase

SpringerLink

Media Sponsors

HELP NET SECURITY
WWW.NET-SECURITY.ORG

GoingToMeet.com
ONLINE CONFERENCE DIRECTORY

BVENTS.com

Biographies

Mohd Taufik Abdullah
Department of Computer Science Faculty of Computer Science and Information Technology, Putra University of Malaysia
Mohd Taufik Abdullah is a PhD student at the Faculty of Computer Science and Information Technology, University Putra Malaysia (UPM). He holds a Master's of Science in Software Engineering from UPM. He is actively involves in the research area of computer forensics and security computing.

Rabiah Ahmad
Centre for Advanced Software Engineering, University Technology Malaysia
Rabiah Ahmad, Ph.D. is a senior lecturer for Information Security at Centre for Advanced Software Engineering, University Technology Malaysia (UTM). She graduated with BSc. Computer Science (UTM) in 1997, MSc. Information Security (Royal Holloway University of London, UK) 1998 and Ph.D. Information Studies (University of Sheffield, UK) 2006. Her current areas of interest and research are Threat Identification Tools for Medical Online System Using Combination Technique Genetic Algorithm and Coz Regression, Virus and Worm Analysis Using Bayesian Network and Regression Model for Healthcare System, Privacy issue in data mining and Security Architecture and Access Control. She is the author of numerous journal publications and article in the field of digital forensics, watermarking, steganography and health information management research. She presented an extensive amount of papers at national and international conferences on her research areas. Rabiah Ahmad has also held management position at the Faculty level such as Program Coordinator Master Computer Science Information Security (2004-2009), Assistant Treasurer for Malaysia Society of Cryptology Research (2009 – Present) and Academic Adviser at German Malaysian Institute (2005 – Present).

Jeremy Allnutt
George Mason University
Jeremy Allnutt earned his B.Sc. and Ph.D. in electrical engineering from the University of Salford, UK, in 1966 and 1970, respectively. From 1970 to 1977 he was at the Appleton Laboratory in Slough, England, where he ran propagation experiments with the US satellite ATS-6 and the European satellites SIRIO and OTS. In 1977 he moved to BNR, now Nortel, in Ottawa, Canada, and worked on satellite and rural communications projects before joining the International Telecommunications Satellite Organization (INTELSAT) in Washington, DC, in 1979. Jeremy Allnutt spent 15 years at INTELSAT in various departments. During this period he ran experimental programs in Europe, Asia, Africa, North and South America, Australia, and New Zealand, finishing as Chief, Communications Research Section. Jeremy Allnutt spent one year as Professor of Telecommunications Systems at the University of York, England, and then joined the Northern Virginia Center of Virginia Tech in 1986, where he later ran the masters program in ECE as well as being on the team that designed and set up the Masters in Information Technology program. In August of 2000 he moved to George Mason University with dual appointments: Director of the new Masters in Telecommunications program (http://telecom.gmu.edu/) and Professor in the ECE department. Jeremy Allnutt has published 100 papers in conferences and journals and written one book, most in his special field: radiowave propagation. He is a Fellow of the UK IEE and a Senior Member of the US IEEE.

Saif M Al-Kuwari
Information Security Group, Department of Mathematics, Royal Holloway, University of London
Saif Al-Kuwari received a Bachelor's of Engineering in Computers and Networks from the University of Essex (with distinction) in 2006. Since 2008, he has been a full-time PhD student in the Informational Security Group (ISG) at the Mathematics Department in the Royal Holloway, University of London. He is interested in computer forensics and cybercrime investigations. In particular, he works on suspects'

clandestine localizations and tracking through MANET (Mobile Ad Hoc Networks) and VANET (Vehicular Ad Hoc Networks). He is also interested in mobility and radio propagation modeling of tracking environments.

Michael Alles

Rutgers University

Michael Alles, Ph.D., specializes in corporate governance, the design of strategic control systems, continuous auditing, and cost-based decision making. He is widely published in all these areas and has presented his work at conferences throughout the world. Currently, Alles serves on the editorial boards of multiple corporate governance and accounting information systems journals. He also was an executive committee member of the management accounting section of the American Accounting Association. He has performed frequent consultancies with companies including the RAND Corporation and Texas Correctional Industries.

Susan Axelrod

New York County DA's Office Appeals Bureau, Senior Appellate Counsel

Susan has been the Senior Appellate Counsel in the Appeals Bureau at the New York County District Attorney's Office since 1995. She prosecutes all levels of criminal appeals in New York state courts and represents New York state authorities in federal habeas proceedings. She also serves as the Director of the Eavesdrop review group and supervises units within the Appeals Bureau responsible for approving narcotics and money laundering related wiretap applications prior to their submission to court. In addition, she advises attorneys conducting investigations regarding telephone and electronic surveillance issues. In the past, she was the Assistant District Attorney for the Special Investigations Bureau, Special Narcotics from 1991-1995 and for the New York County Trial Division from 1985-1991. She also wrote parts of the 2003 ABA International Corporate Privacy Handbook and the 2002 ABA International Guide to Combating Cybercrime. She graduated with a J.D. from Duke University School of Law in 1984 and a B.A. in American History from Wesleyan University in 1981 with honors for both degrees.

Ibrahim M. Baggili

Zayed University, Abu Dhabi, United Arab Emirates

Adnan Baykal

NYS Office of Cyber Security and Critical Infrastructure Coordination
NYS Digital & Multimedia Evidence Technical Working Group

Adnan Baykal is currently working as a member of the Incident Response Team of Multi State ISAC (MS-ISAC) and is the project manager for the NYS Vulnerability Assessment Project. He is also a Ph.D. Student in the Computer Science Department at the State University of New York, University at Albany. He has received a B.S. in Computer Science and Applied Mathematics, and MS in Computer Science from UAlbany. His research interests include Intrusion Detection, High quality Audit Generation, Malware Analysis and Data Mining. Adnan's main expertise is in Incident Response, Computer Forensics and Vulnerability Assessment and holds various certifications in these areas.

Mark Bilanski

NYS Incident Response Team Manager NYS CSCIC
Incident Response Team Manager at MS-ISAC
NYS Digital & Multimedia Evidence Technical Working Group

Mark Bilanski is currently the Incident Response Team Manager at Multi State ISAC (MS-ISAC). He has over 10 years of experience in the IT field. He has worked at Office of Mental Health for over 8 years managing and supporting over 16000 desktops and 200 servers. He is considered an expert in securing and auditing Microsoft Operating Systems. He holds several certifications in Incident Handling, Ethical Hacking and various MS certifications.

Nikki Brate
Manager IT, Technical Services, NYS Insurance Department
NYS Digital & Multimedia Evidence Technical Working Group

Zhixiong Chen
Dept of Computer Information Science, Mercy College
Zhixiong Chen is currently a Professor at Mercy College in the Department of Computer Information Science and has been a part of the faculty since 2003. He serves as the Program Director of Information Assurance and Security at the college. In the past, he has been employed as an engineer in IBM T.J. Watson Research Center from 1997 to 2003. At present, he is involved in the services curriculum, services university, and is working on integrated price modeling to open source applications in services computing. He is also doing work on information assurance and security in services computing. Just for background, has been involved with self-autonomic computing, network monitoring, compiled parallel computing, and neuronal modeling.

K.P. Chow
The University of Hong Kong
Dr. Chow began his academic career in this department upon completion of his doctoral degree in the United States. His first contribution was on establishing HARNET, the first academic and research network for tertiary institutions in Hong Kong (with Raymond Lo and Dr. Ng). His earlier research works were in expert systems development and Chinese computing. In those years, Dr. Chow has used expert systems techniques successfully in implementing a staff roster rostering system for a local airline (with Dr. Lucas Hui), a refuse collection vehicle scheduling system for Regional Services Department (with D. Hung and C.T. Hung), and an air conditioning plant diagnostic system. In the years 1994-1997, Dr. Chow, together with Dr. D. Cheung, Prof. Chin, Dr. T.W. Lam, Dr. W.W. Tsang and a team of software engineers developed the search engine for Hong Kong Telecom's 108 Telephone Directory Enquiry System using state of the art technology in main memory database and distributed computing. In the recent years, Dr. Chow' research interests have migrated to cryptography and software engineering, and has involved in the design and implementation of the Strong Cryptographic Library (SCL). Being the Associate Director of Center for Information Security and Cryptography, Department of Computer Science and Information Systems, the University of Hong Kong, he is the Project Manager of the Strong Cryptographic Infrastructure for Electronic Commerce project. Recently, he has worked with Jasmine Ma and C.T. Hung in the design and implementation of the bilingual software Digital Evidence Search Kit (DESK), which is a computer forensic tool to collect digital evidence in Chinese and English. In addition to forensic tool development, Dr. Chow is also interested in software vulnerability analysis and has performed studies in buffer overflow techniques and prevention. Besides cryptography and computer security, Dr. Chow's research interests also include heuristic scheduling and rescheduling algorithms. Dr. Chow is also the Associate Programme Director for the MSc in E-Commerce and Internet Computing Programme. He is the instructor for the course Java Technology. Most of his Java experiences are gathered during the development of the forensic tool DESK, which is written in Java. Dr. Chow has provided consultancy and training to local organizations including Hong Kong Telecom, Hong Kong Airport Services Limited, Hewlett Packard and MPFA in the areas distributed computing, Internet technology and software quality assurance.

Jared D. Crafton
Manager, Fraud & Dispute Services, Ernst & Young LLP
Jared Crafton is a Manager in Ernst & Young's Fraud Investigation & Dispute Services practice. Jared specializes in text analytics, forensic data mining and electronic discovery services. Jared has extensive experience handling the information management and electronic discovery needs for large scale, complex

litigations, investigations and proactive anti-fraud programs. Jared is experienced with providing clients leading anti-fraud based innovation, research and analytics, including, link analysis, text data mining, metadata analysis, entity extraction, and predictive modeling that seek to identify or predict fraud risk variables, data anomalies or data inefficiencies that can lead to unnecessary costs or enterprise risks. Jared leads teams to help clients discover patterns and anomalies in huge sets of disparate data, with a focus on unstructured, text-based data sources such as email and corporate file share networks.

Roger Debreceny

University of Hawaii

Dr. Debreceny is a Shidler Distinguished Professor of Accounting in the School of Accountancy at the Shidler College of Business, University of Hawai'i, Hawaii. His teaching and research interests are in accounting information systems, information systems audit, electronic commerce and financial reporting on the Internet. He is also the Chair of the CobiT Steering Committee and Associate Editor of the Journal of Information Systems. His interests outside University life are his family, reading, travel, listening to classical music and opera, movies, theater and music, cycling, keelboat sailing and working out in the gym.

Michael W. Deyo, Esq.

Director, eDiscovery and Forensics, JANUS Associates

Mike currently leads the Electronic Discovery practice for JANUS Associates. He has been involved in the computer forensic and information security fields for seven years, working in both technical and project management roles. He regularly leads and conducts digital forensic investigations for law firms, government agencies, and private businesses, and has experience in assisting law firms in drafting electronic discovery motions and pleadings. Mike recently delivered presentations on e-Discovery to the NYC Bar Labor, Employment Law Committee, and did an e-Discovery CLE for our agency. He has served as an instructor and presenter for computer forensic workshops and seminars at national and state information security conferences. Mike holds a Bachelors Degree in Economic Crime Investigation and Computer Forensics from Utica College of Syracuse University, and a Law Degree from Albany Law School. His unique combination of technical skills, practical experience, and legal training enables him to provide unique insights and solutions in the convergence of digital forensics, electronic discovery and the use of electronic evidence.

Mohamed El Ouariachi

Information Assurance, Fraunhofer SIT

Michael Gibbs

NYS Digital & Multimedia Evidence Technical Working Group

Pavel Gladyshev

Centre for Cybercrime Investigation, University College Dublin

Dr. Pavel Gladyshev is a lecturer in the School of Computer Science and Informatics at University College Dublin, Ireland where he manages MSc programme in Forensic Computing and Cybercrime Investigation. Dr. Gladyshev's research interests lie in the area of digital forensics. He is a member of the editorial board of the International Journal of Digital Evidence, and a referee for the Digital Investigation Journal and International Journal of Digital Crime and Forensics. Dr. Gladyshev is also serving as an invited expert to the INTERPOL working party on IT Crime - Europe.

John Griffin

NYS Office of Temporary and Disability Assistance (OTDA)
NYS Digital & Multimedia Evidence Technical Working Group

Barbara Guttman
National Institute for Standards and Technology (NIST)

Corey Harrell
NYS Office of the State Comptroller (OSC)
NYS Digital & Multimedia Evidence Technical Working Group

Vincent Hom
Senior Manager, Fraud Investigation & Dispute Services, Ernst & Young LLP
Vincent Hom is a Senior Manager in Ernst & Young's Fraud Investigation & Dispute Services practice. Vincent has extensive experience leading internal investigations involving various financial statement and U.S. Foreign Corrupt Practices Act issues. He has conducted numerous global investigation and remediation efforts for audit committees and outside counsel. Investigative topics have included accounting fraud, bribery and corruption, and misappropriation of assets. Vincent was a member of the development team for Ernst & Young's Anti-Fraud service. Vincent's experience also includes a two-year assignment with Ernst & Young Singapore's Fraud Investigation & Dispute Services practice, where he managed the performance of fraud and forensic accounting and investigation services for clients within the Asia-Pacific region.

Mohammad Iftekhar Husain
University of Buffalo
Mohammad is currently in the University at Buffalo Computer Science and Engineering doctoral program (Ph.D. expected 2011). He graduated with an MS in Computer Science and Engineering from the same school in 2008 and a BS in Computer Science from Yamagata University in Japan in 2006. His broad research interests are in the field of Wireless Network Security. Other research interests include Soft Security approaches such as Steganography and Covert Communication as well as Economic and Social Network Analysis based Information Security research. His current research projects include: Social Network Analysis methods for transforming network metrics to actionable intelligence, Economic model for routing misbehavior in Wireless Ad hoc Network, Soft Security for Wireless Embedded Systems, and Hybrid Key Management for Wireless Body Area Network. He has received a Microsoft Research Grant in 2008.

Amin Ibrahim
University of Ontario Institute of Technology
Amin received his Bachelor's degree in Computer Engineering at the University of Toronto. He is currently enrolled in his Master's degree program in Computer Engineering at UOIT, where he is undertaking a research to combat child pornography on the Internet. His research interests are image processing and computer security. He has taught in the Faculty of Engineering, and the Faculty of Business and Information Technology. Prior to joining UOIT, Amin had roles in electrical control systems design at Air-o-Mix Systems.

Joshua James
Centre for Cybercrime Investigation, University College Dublin
Mr. Joshua James is a research student in the Centre for Cybercrime Investigation at University College Dublin, Ireland. Coming from a background in Network Security and Administration, his focus is now on automatic digital evidence identification and correlation. He is specifically working in the area of rigorous automated investigation and analysis techniques for digital investigations with emphasis of ease of use. To this end, he has started the open source project titled Rapid Evidence Acquisition Project for Event Reconstruction (http://cybercrimetech.com).

Abbas Bagherian Kasgeri

IAU University

Stefan Katzenbeisser

CASED, Darmstadt

Dr. Stefan Katzenbeisser received his Ph.D. in Computer Science at the Vienna University of Technology, Austria in 2004, and is currently assistant professor at the Computer Science Department and part of the security engineering group at the Technische Universität Darmstadt, Germany. His main research activities are Cryptographic protocols (design, analysis), Cryptographic techniques for noisy and fuzzy data, Privacy Enhancing Technologies, Software Security, Watermarking, Digital Rights Management, Copyright Protection and Malicious Code Detection. In the past, he has served as a senior scientist at Philips Research Europe, in the Information and System Security Group. He has been a chair in several conferences and served as the associate editor for the IEEE Transactions on Dependable and Secure Computing and the EURASIP Journal on Information Security. He has been the Editor-in-Chief of the Springer LNCS Transactions on Data Hiding and Multimedia Security and is a member of the Technical Committee on Information Forensics and Security, IEEE Signal Processing Society

Firdous Kausar

Information Security Department, College of Signals, National University of Science and Technology

Firdous Kausar is a Ph.D. candidate at the College of Signals, National University of Science and Technology, Islamabad, Pakistan. She has authored more than 20 papers including a book chapter and journal papers. She reviewed papers for several journals, conferences and workshops. She is a member of IEEE and IACR (International Association of Cryptologic Research). Her research interests are in network and data security, key management and authentication protocols, computer forensics, sensor networks, mobile and ad hoc networks.

Mohand-Tahar Kechadi

UCD Centre for Cybercrime Investigation, School of Computer Science and Informatics, University College Dublin

Prof. Tahar Kechadi was awarded PhD in Computer Science from the University of Lille 1, France. After working as a post-doctoral researcher under TMR program at UCD, he joined the UCD School of Computer Science and Informatics in 1999. He is director of PCRG laboratory and head of teaching and learning at the School of Computer Science and Informatics. His research interests span the areas of optimisation techniques, Distributed Data mining, forensic computing, Grid computing. He is a member of the communication of the ACM and IEEE computer society.

Yongbum Kim

Rutgers University

Yongbum Kim is currently pursuing his Ph.D. Accounting Information Systems from the School of Business at Rutgers University. He was awarded a prestigious summer scholarship this May given to 10 Rutgers Business School Doctoral students.

Nhien-An Le-Khac

School of Computer Science & Informatics, University College Dublin Belfield

Nhien-An Le-Khac is a Postdoctoral Fellow at the School of Computer Science and Informatics, University College Dublin, Ireland. He obtained his M.Sc. in Computer Science in 2000 at National University of Vietnam (VNU-HCM), and Ph.D. in Computer Science in 2005 at the INP (Institut National Polytechnique) Grenoble, France. His research interest spans the area of Parallel Computing, Grid computing, heterogeneous clusters and Distributed Data Mining. He is a member of the IEEE computer society.

Michael Lavine

Information Security Institute, John Hopkins University
Dr. Michael Lavine is Managing Director of Homeland Security Consultants, Inc. and is an international expert in the field of IT security. He is a highly sought after consultant in the field with over twenty years of experience in the security, audit/assessment and consulting industries. His main areas of expertise are in information assurance, IT auditing, computer security and management consulting and he has conducted projects for a diverse group of international and local clients. He previously worked from PricewaterhouseCoopers, LLP in the Baltimore-Washington area where he provided information technology security reviews, audits and consulting services to a wide variety of clients in the: financial services, manufacturing, high technology, government, healthcare, and middle market sectors. Mike has a Ph.D. in Management from Sir John Cass Business School - City University, London, England in Computer Information Systems. He holds a M.S. in Information and Telecommunication Systems for Business from Johns Hopkins University in Baltimore, Maryland, a MSc. from City University Business School in London and a B.S. from Touro College in New York City. Currently, Mike also serves on the faculty of Johns Hopkins Information Security Institute and Robert H. Smith School of Business – University of Maryland and also is a Visiting/Guest Lecturer and Associate Researcher at City University, Sir John Cass Business School. He also teaches on the Masters of Information Assurance program at Norwich University. He is an active member of several professional organizations including Computer Forensic Educators Working Group, Federal Information Systems Security Educators Association, IEEE Computer Society – Technical Committee on Security and Privacy, Information Assurance Technical Framework Forum, and ISSA.

Pierre K.Y. Lai
The University of Hong Kong
Ms. Pierre K.Y. Lai is a Ph.D. student in the Computer Forensics Research Group, in the Center for Information Security and Cryptography (CISC), Department of Computer Science in the University of Hong Kong.

Frank Y.W. Law
The University of Hong Kong
Mr. Frank Y.W. Law is a Ph.D. student in the Computer Forensics Research Group, in the Center for Information Security and Cryptography (CISC), Department of Computer Science in the University of Hong Kong.

Huajian Liu
Information Assurance, Fraunhofer SIT

Pritheega Magalingam
Centre for Advanced Software Engineering, University Technology Malaysia
Pritheega Magalingam is a MSc.(Information Security) graduate (2009) from University Technology Malaysia. Currently, she is a research and teaching assistant in Centre for Advance Software Engineering, University Technology Malaysia. Her MSc. thesis comprises Digital Evidence Retrieval and Forensic Analysis Guideline for an Illegal Gambling Machine and she has published few papers on how to extract evidence from gambling machine and data analysis using keyword search techniques. Her current research focuses on forensic analysis tool development for evidence retrieved from electronic gaming machine. Applying artificial intelligence techniques through the development of a multi-agent system that acts based on expert's knowledge of the technical domain would be her great interest.

Azizah Abdul Manaf
College Science and Technology, University Technology Malaysia
Azizah Abdul Manaf (PhD) is a Professor of Image Processing and Pattern Recognition from University Technology Malaysia (UTM). She graduated with B. Eng. (Electrical) 1980, MSc. Computer Science

(1985) and PhD (Image Processing) in 1995 from UTM. Her current areas of interest and research are image processing, watermarking, steganography and computer forensics and have postgraduate students at the Masters and PhD level to assist her in these research areas. She has written numerous articles in journals and presented an extensive amount of papers at national and international conferences on her research areas. Prof. Dr. Azizah has also held management positions at the University and Faculty level such as Head of Department, Deputy Dean, Deputy Director and Academic Director pertaining to academic development as well as on training for teaching and learning methodologies at the University.

Sammer Markos
School of Computer Science & Informatics, University College Dublin Belfield
Sammer Markos is a PhD. Student at the School of Computer Science and Informatics, University College Dublin, Ireland. She obtained her M.Sc. in Statistics and Actuarial Science in 2004 at University College Dublin, Ireland. Her research interest are in the area of Financial Data Mining with special interest in Money laundering and Fraud.

Miguel Vargas Martin
University of Ontario Institute of Technology
Dr. Miguel Vargas-Martin is an Assistant Professor of the Faculty of Business and Information Technology, and the Faculty of Engineering and Applied Science. Before joining UOIT, Dr. Vargas Martin worked as a Post-doctoral Researcher on Network Security for Alcatel Canada Inc. and Carleton University, where he got a PhD. in Computer Science (Canada, 2002). He has a Masters degree in Electrical Engineering from Cinvestav del IPN (Mexico, 1998), and a Bachelor in Computer Science from the Universidad Autonoma de Aguascalientes (Mexico, 1996). His main research interests include computer forensics; intrusion prevention, detection, and reaction; denial-of-service (DoS) and distributed DoS attacks; security issues of voice-over-IP, interconnection protocols; Internet connectivity; as well as web modeling and optimization.

Nasir Memon
Polytechnic University & Digital-Assembly
Nasir Memon is a Professor in the Computer Science Department, Polytechnic University, New York and also one of the founders of Digital-Assembly, which has developed Adroit Photo Recovery, a photo / media recovery tool. Professor Memon's research interests include data compression, computer and network security, and multimedia communication, computing, and security. He has published more than 200 articles in journals and conference proceedings. He was a Visiting Faculty at Hewlett-Packard Research Labs during the academic year 1997–1998. He has won several awards including the NSF CAREER Award and the Jacobs Excellence in Education Award. He was an Associate Editor for the IEEE Transactions on Image Processing from 1999 till 2002. He is currently an Associate Editor for the IEEE Transactions on Information Security and Forensics, ACM Multimedia Systems Journal, and the Journal of Electronic Imaging.

Rebecca Mercuri, Ph.D.
Computer Forensics Expert, Notable Software, Inc. and The College of New Jersey
Rebecca Mercuri is the president and lead forensic expert at Notable Software, Inc. <www.notablesoftware.com>, the company she founded in 1981. Her caseload has included matters involving contraband, child endangerment, murder, computer viruses and malware, wrongful work termination, class-action suits, financial fraud, copyright and patent infringement, and election recounts (most notably Bush vs. Gore). Dr. Mercuri has provided formal testimony

and comment to the House Science Committee, the U.S. Commission on Civil Rights, the Election Assistance Commission, the National Institute of Standards and Technologies, the U.K. Cabinet, and numerous state legislatures and municipal bodies. She holds 5 academic degrees, including a Ph.D. from the University of Pennsylvania's School of Engineering and Applied Science, with post-doctoral research at Harvard University's Kennedy School of Government and a fellowship at the Radcliffe Institute. While serving as a contributing editor for the Communications of the Association for Computing Machinery, she authored the Security Watch feature and numerous guest columns of Inside Risks. Rebecca is also an adjunct member of the Computer Engineering faculty at The College of New Jersey, where she teaches a broad range of subjects, including a recent senior engineering lecture/laboratory elective on Digital Forensics.

Ashwin Mohan
Purdue University

Hamed Mosavi
Tehran Stock Exchange

William F. Mosher
Senior Investigator, Financial Crimes Unit, NYS Police

Senior Investigator William Mosher is the member in charge of the New York State Police Financial Crimes Unit. Mr. Mosher has supervised the unit since its inception in February of 2001. The unit is responsible for assisting with the financial aspects of criminal investigations. These investigations include money laundering and asset seizures as well as identity theft and embezzlements. The unit is also responsible for providing the Treasury Department's Financial Crimes Enforcement Network data to all state and local law enforcement in upstate New York. Mr. Mosher has been a member of the New York State Police since 1986. He is an adjunct instructor for the National White Collar Crime Center, a train the trainer for FinCEN's Gateway system, and an instructor for the New York State Department of Criminal Justice Services. He also instructs all new State Police investigators in financial crimes and money laundering investigations at the Bureau of Criminal Investigation Basic School. In 2007, Mr. Mosher was named the Law Enforcement Officer of the Year by the Capital District Bank Security Officer's Association.

John K. Neuner
Program Manager, ASCLD/LAB-International Accreditation Program
Mr. Neuner currently serves as the Program Manager for the ASCLD/LAB-*International* accreditation program. He is a graduate of Campbell University (North Carolina) (Public Administration/Public Policy) and has been an active participant in the forensic science profession for the past thirty-five years. In 2003 John retired as Deputy Assistant Director of the North Carolina State Bureau of Investigation Crime Laboratory System. Since mid-2003, he has coordinated ASCLD/LAB's development and implementation of an ISO compliant accreditation program for crime laboratories. The ASCLD/LAB-*International* accreditation program has now gained full, international recognition. He is an active member of the National Cooperation of Laboratory Accreditation (NACLA) where he currently serves on the Board of Directors. He also serves as one of ASCLD/LAB's representatives to the Inter-American Accreditation Cooperation (IAAC) - a regional cooperation of ISO accrediting bodies serving all of North, Central and South America. Mr. Neuner currently represents the US on an International Laboratory

Accreditation Cooperation (ILAC) Working Group developing internationally accepted practices for the assessment and accreditation of crime scene operations.

Justin Offen

Director, Forensic Technology Solutions, PricewaterhouseCoopers LLP, New York Office
Justin is a Director in PwC's Forensic Technology practice in New York City. Mr. Offen joined the firm in 2001 and has considerable experience assisting clients obtain, manage and analyze data including e-mail, financial data, and "deleted" information from workstations, servers, and other media. He has assisted in developing various proprietary tools which PwC uses for the analysis of G/L and sub-ledger and procurement data. Such tools include TRIA (Transactional Risk Identification and Analysis) which is used to identify unusual and suspicious transactions and has been developed using PwC's knowledge bank of fraud schemes. Over the last several years, he has focused on large and complex investigations where he led teams in identifying relevant data sources, extracting the necessary data and analyzing data to identify red flags and trends. His experience is cross-industry and he has worked with clients in more than thirty countries on five continents including spending extensive time in the field in the EU, AsiaPac, and Africa. His extensive travel has enabled him to gain experience in dealing with various data privacy and protection issues. Mr. Offen is an Oracle Certified Associate (OCA) and a member of the Association of Certified Fraud Examiners.

Angela D. Orebaugh

George Mason University
Angela Orebaugh is a security technologist, scientist, and author. She is the author of the Syngress' Wireshark and Ethereal Network Protocol Analyzer Toolkit and Ethereal Packet Sniffing. She is also known for her work as a researcher, writer, and speaker for the SANS Institute and as faculty for The Institute for Applied Network Security. She is a frequent speaker at a variety of conferences and security events. She currently serves as a technology advisor and consultant for commercial and government clients.[citation needed] She is a contractor supporting the National Institute of Standards and Technology (NIST), where she is the lead contractor for several security initiatives including the authoring of security special publications, the National Vulnerability Database (NVD), Security Content Automation Protocol (SCAP) project, and electronic voting security standards development. Ms. Orebaugh is a Research Fellow and Adjunct Professor for George Mason University where she performs research and development in information security. At GMU she developed and taught the Intrusion Detection curriculum for the Forensics program in the Department of Electrical and Computer Engineering. Her current research interests include peer-reviewed publications in the areas of intrusion detection and prevention, data mining, attacker profiling, user behavior analysis, and network forensics.

Sriram Raghavan

Information Security Institute, Queensland University of Technology
Sriram Raghavan is a PhD research student at the Queensland University of Technology Brisbane. Previously, Sriram received his Masters degree in Computer Science from the IIT Madras and enjoyed a stint in the Industry with Intel and a Business intelligence startup. His research interests include Digital forensics, Ubiquitous networking environments, Multi agent systems, Robotics and Machine Intelligence.

S. V. Raghavan

Computer Science and Engineering, IIT Madras
Prof. Raghavan is a Professor of Computer Science and Engineering at IIT Madras. He is the father of the Education and Research Network (ERNET) in India and has recently championed the design of National Knowledge Network (NKN) which connects over 500 education institutions in India in a hierarchical high-speed network running at several gigabits/sec. Prof. Raghavan has a wide range of specialization and enjoys many publications to his credit in the area of Networking, Multimedia, E-Commerce and Electronic Security.

Sridhar Ramalingam

University of Buffalo

Sridhar Ramalingam received a B.E. (Honors) degree in Electrical and Electronics Engineering from Guindy Engineering College, University of Madras in 1980, MS and PhD in Electrical and Computer Engineering from Washington State University in 1983 and 1987 respectively. Since 1987 he has been with the University at Buffalo, The State University of New York where he is an Associate Professor in the Department of Computer Science and Engineering. His research interests are in Wireless and sensor network security, pervasive and RFID systems, secure architectures, Embedded technologies, deep submicron VLSI systems, Clocking and Synchronization, and memory circuits & architecture. He was an IEEE CAS Distinguished Lecturer. He has served as Program Chair and General Chair of ASIC/SoC Conference and has served in the editorial board of many journals and technical committee of numerous conferences in wireless systems and VLSI.

Marcus Rogers

Purdue University

Marc Rogers, Ph.D., CISSP, CCCI is the director of the Cyber Forensics Program in the Dept. of Computer and Information Technology at Purdue University. He is a Professor, University Faculty Scholar and research faculty member at the Center for Education and Research in Information Assurance and Security (CERIAS). Dr. Rogers is the International Chair of the Law, Compliance and Investigation Domain of the Common Body of Knowledge (CBK) committee, Chair of the Ethics Committee for the Digital and Multimedia Sciences section of the American Academy of Forensic Sciences, and Chair of the Certification and Test Committee – Digital Forensics Certification Board. He is a former Police officer who worked in the area of fraud and computer crime investigations. Dr. Rogers is the Editor-in-Chief of the Journal of Digital Forensic Practice and sits on the editorial board for several other professional journals. He is also a member of other various national and international committees focusing on digital forensic science and digital evidence. Dr. Rogers is the author of books, book chapters, and journal publications in the field of digital forensics and applied psychological analysis. His research interests include applied cyber forensics, psychological digital crime scene analysis, and cyber terrorism.

Saeed Roohani

Bryant University

Saeed Roohani is a Professor and Chair of the Accounting department at Bryant University. He is also a PriceWaterhouseCoopers XBRL Fellow. He graduated with a BA in Accounting from the Institute of Advanced Accounting (In Iran) in 1974, received an M.B.A. from Sol Ross State University in 1978, a M.S. in Accounting from Louisiana State University in 1982 and a D.B.A. in Accounting and Information Systems from Mississippi State University in 1992. He has taught courses in Corporate Governance in the 21st Century, Accounting Information Systems, Financial Accounting and Reporting, and IT Auditing. In addition, he has published over 30 articles, on Editorial Board of three journals, edited a research monograph funded by PricewaterhouseCoopers; research area includes financial reporting supply chain; corporate governance; synergy between IT and accounting and auditing; XBRL and International Financial Reporting Standards, and forensic accounting. Saeed has established and promoted meaningful relations with local, national, and international accounting firms, occasionally consultant to local firms in Rhode Island on accounting issues and Sarbanes Oxley compliance, engaged in initial AACSB accreditation and reaccreditation at Bryant University, and founding Director of PricewaterhouseCoopers Accounting Careers Leadership Institute at Bryant University.

Mark Scanlon

UCD Centre for Cybercrime Investigation, School of Computer Science and Informatics, University College Dublin

Mark Scanlon has recently completed a Master of Science in the Centre for Cybercrime Investigation, School of Computer Science & Informatics at University College Dublin, under the guidance of Prof. Tahar Kechadi. He received his B.A. (Hons.) degree in Computer Science and Linguistics from University College Dublin in 2006, before working as an application developer in IBM Ireland. Mark's research interests include Computer Forensics and Cybercrime Investigation, Networking and Internet protocols.

Matt Shelhorse

Partner, Forensic Services, PricewaterhouseCoopers LLP, New York Office

Matt is a Partner in PricewaterhouseCoopers LLP's ("PwC") Forensic Services Practice in New York. Matt has over seventeen years of forensic accounting, consulting and financial management experience. He provides accounting, financial, operational and investigative expertise to attorneys, corporate clients, individuals and governmental agencies to assist them in a variety of matters across various industry sectors. Matt has experience in leading large complex engagements for multinational organizations involved in situations that involve the assessment of global activities. Matt has conducted work in over sixteen countries across Europe, the Middle East, Asia Pacific, Africa and the Americas and has coordinated work with client and PwC professionals based in various other international locations. Matt has developed and instructed training courses and case studies on fraud and forensic accounting and has lectured groups on such topics at numerous corporations, universities, professional associations and Firm events. One such training program was provided to the Board and management team of a publicly-traded technology company based on an agreement reached with the SEC. Recent programs have focused on bribery and corruption and investigative techniques designed to detect and investigate such activity. Matt is a Member of the AICPA and the NYSSCPA and an Associate Member of the ACFE. Matt is a CPA in the State of New York and is certified in Financial Forensics (CFF) by the AICPA.

Michael Smith

NYS Office of Cyber Security and Critical Infrastructure Coordination

Mr. Smith received his MS in Computer Science with an emphasis in Information Security from James Madison University. He has over 12 years of experience working in the field of Information Security. He has numerous industry certifications, including PMP, CISSP, NSA CNSS NSTISSI No. 4011 (Certification for Information Systems Security Professionals) and NSA CNSS CNSSI No. 4014 (Certification for Information Systems Security Officers). His experience has included the planning, design, implementation, testing and management of enterprise security solutions. He currently is a Sr. Manager at Symantec Corporation where he manages a 24x7 team that provides operational security services.

Martin Steinebach

Information Assurance, Fraunhofer SIT

Dr.-Ing. Martin Steinebach is a researcher at Fraunhofer SIT and director of the CASED application lab. His main research interest is digital audio watermarking. He has developed algorithms for mp2, MIDI and PCM data watermarking, content fragile watermarking and invertible audio watermarking. Dr. Steinebach studied computer science at the Technical University of Darmstadt, where he completed his diploma thesis on copyright protection for digital audio in 1999. In 2003 he received his PhD from the Technical University of Darmstadt for his work on digital audio watermarking.

Steven V. Treglia

Nassau County DA Office

Stephen has been a prosecutor for over 28 years and is currently Chief of the Technology Crime Unit of the Nassau County DA's Office (NCDA). This Unit was created in 1997 and is one of the first of its kind in the country. Stephen has supervised this operation since its inception, and the Unit presently utilizes

several of the resources within the Investigations Division of the NCDA to create a fully in-house investigative and prosecutorial task force of prosecutors, forensic examiners, undercover agents, investigators, accountants and IT personnel. The Unit handles most of the high technology-related cases investigated and prosecuted by the NCDA, and the NCDA is still, to this day, one of the few prosecutor's offices in the country to have a fully self-sufficient computer and Internet crime investigative unit. Stephen routinely lectures to law enforcement and governmental agencies across the country, as well local community groups, on the topics of computer crime, Internet safety and identity theft. He has also authored numerous articles appearing in the New York Law Journal and The Nassau Lawyer, as well as publications issued by the National Association of Attorneys General, the New York Prosecutor's Training Institute and the High Technology Crime Investigation Association to its members. On four occasions over the past four years Stephen has been invited by the FBI to act in the roles of prosecutor and defense attorney during a week-long Moot Court session comprising a combined total of more than 200 computer forensic trainees from the FBI's Computer Analysis Response Team. He has received the FBI's "Exceptional Service Award" for assistance provided in training their new computer forensic examiners. Stephen is also one of the founding members of the Legislative Subcommittee on Computers and Technology of the NYS DA Association and served as Subcommittee Chair from 2002-2005.

Hayson K.S. Tse
The University of Hong Kong

Muhammad Arif Wahla
Information Security Department, College of Signals, National University of Science and Technology
Muhammad Arif was born in Bahawal Nagar, Pakistan, on February 1, 1968. He graduated from National University of Sciences and Technology, Islamabad, Pakistan with B.E. degree in Electrical and Communications Engineering in 1996. He received his M.Sc. Engg. degree in Electronics and Communications Engineering from University of Engineering and Technology Lahore, Pakistan, 2003. He received his Ph.D. degree in Electronics and Communications Engineering from University of Engineering and Technology Lahore, Pakistan, 2008. He is currently HoD of Information Security Department, College of Signals, National University of Science and Technology, Islamabad, Pakistan. His research interests include digital communications, error control coding, information security, digital forensics and wireless communications.

Carrie Whitcomb
Director, National Center for Forensic Science, University of Central Florida
Ms. Whitcomb received a BS in zoology with a minor in chemistry at the University of Kentucky in 1967 and a MS in Forensic Science from George Washington University in 1976. She became the Director of the National Center for Forensic Science (NCFS) at the University of Central Florida (UCF) from 1999 to present; see www.ncfs.org. She was a practicing forensic chemist from 1969 until she joined the management ranks in 1988 when she became the Director of the US Postal Inspection Service’s Headquarters Crime Laboratory in Washington, DC. She was the President of the American Society of Crime Laboratory Directors in 1995. Her goals have been to encourage and develop the scientific underpinnings of digital evidence. She was the first Vice-Chair of the Scientific Working Group on Digital Evidence (SWGDE) in 1998 that defined digital evidence. At UCF, she helped facilitate the development of the Graduate Certificate in Computer Forensics in 2001 and the MS in Digital Forensics in 2008. She has been an American Academy of Forensic Sciences (AAFS) Fellow, starting in the Criminalistics Section in 1989; transferred to the General Section in 2005 and again transferred to the newest AAFS section, the Digital and Multimedia Sciences Section, in February 2008 where she serves as the Section Director. She was elected to the AAFS Executive Committee at the February 2008 and 2009 meetings. The National Institute of Justice awarded the NCFS a grant to develop a professional certification program within the digital forensics community. The Digital Forensic Certification Board (DFCB) launched their Founders Application on March 2, 2009.

Duane Wilson
Network Security Branch, U.S. Army Research Laboratory
Duane Wilson, M. Eng. is a Computer Scientist in the Network Security Branch, Computational Information Sciences Directorate at the U.S. Army Research Laboratory in Aberdeen, MD. His research interests focus on computer and network forensics, data exfiltration prevention techniques, and proactive computer defense.

Stephen Wolthusen
Norwegian Information Security Laboratory, Gjøvik University College
Dr. Stephen D. Wolthusen is a Reader in Mathematics in the Information Security Group. He has held this appointment since 2008 and had previously held a lectureship since 2006. He also is (part-time) Full Professor in Information Security at the Norwegian Information Security Laboratory at Gj_vik University College in Norway since 2007, where he previously held an appointment as Associate Professor since 2005. Since 2008 he also holds a honorary Guest Professorship at the Department of Computer Science of the Harbin Institute of Technology in Harbin, China, and he is adjunct professor at the Advanced Research Institute of Virginia Tech University in Alexandria, Virginia, USA. Before joining the ISG, Dr. Wolthusen was with the Security Technology Department of the Fraunhofer IGD Institute in Darmstadt, Germany, where he is also retained as a senior scientist. He has published more than 70 peer-reviewed papers in these areas, is author and editor of several books as well as past Editor-in-Chief of Computers & Security.

Zuraimi Yahya
University Technology Malaysia

Muhammad Yasin
Information Security Department, College of Signals, National University of Science and Technology
Muhammad Yasin is MS leading to Ph.D. candidate at the College of Signals, National University of Science and Technology, Islamabad, Pakistan. His research interests include information security and computer forensics with particular emphasis on registry analysis to trace the artifacts left by download managers, portable email clients and various applications.

Jong P. Yoon
Assistant Professor, Information Assurance, Dept of Computer Information Science, Mercy College

Yuandong Zhu
Centre for Cybercrime Investigation, University College Dublin
Yuandong Zhu is a PhD student at the School of Computer Science and Informatics at University College Dublin, Ireland. His research interests include user activity analysis and forensic tool development. His current work focuses on the analysis of different states of Window Registry snapshots within Windows Restore Points and he has published several papers about how to extract comprehensive user activity information from a computer running Microsoft Windows by utilizing novel Registry snapshot comparison techniques.