



011000101 **e-Forensics 2009**
 1100100111
 0010100110



University of
South Australia



Draft Program

International Conference on Forensic Applications and Techniques in
Telecommunications, Information and Multimedia

National Wine Centre

Adelaide, Australia, January 19-21, 2009

<http://www.e-Forensics.eu>

| Session | Monday January 19 | Tuesday January 20 | Wednesday January 21 |
|-------------|---|---|---|
| 9am-10:30 | 9.00 Official Opening 9:30 Keynote Presentation , Dr Andy Jones, BT Security Research | Plenary Session <i>Digital Forensics Practice</i> | Plenary Session <i>The Interaction Between Technology and Law</i> |
| 10:30-11.00 | Morning Tea | | |
| 11:00-12:30 | Technical Session 1 <i>Voice and Telephony</i> | Technical Session 2 <i>Investigative Practice</i> | Technical Session 5 <i>Legal Considerations</i> |
| 12:30-1:30 | Lunch | | |
| 1:30-3:00 | International Workshop on e-Forensics Law <i>Plenary Session</i> | Technical Session 3 <i>Image Source Identification</i> | Technical Session 6 <i>Security and Applications</i> |
| 3:00-3:30 | Afternoon Tea | | |
| 3:30-5:00 | International Workshop on e-Forensics Law <i>Academic Papers Session</i> <i>Panel Discussion</i> | Technical Session 4 <i>Image Authentication</i> | Plenary Session <i>Strategic priorities in Digital Forensics Research</i> Close |
| Evening | Conference Banquet | <i>Dinner: own arrangements</i> | |

REGISTRATION NOW OPEN AT www.e-forensics.eu

This draft program released January 6, 2009. Please visit www.e-forensics.eu for updated program details

e-Forensics 2009: International Conference on Forensic Applications and Techniques in Telecommunications, Information and Multimedia

Keynote Speaker

Dr Andy Jones, BT Security Research, UK

Future Forensic Issues

This presentation will look at some of the issues that the advances in technology and the changing environment will create for the forensic practitioner. It will look at some of the new technologies that are coming into use, the way that they are being utilised and take a high level view of existing computer crime legislation and forensic tools and techniques and the potential gaps that can be foreseen.

Dr. Andy Jones MBE MBCS CITP M Inst ISP

During a full military career Andy Jones directed both Intelligence and Security operations and briefed the results at the highest level, and was awarded the MBE for his service in Northern Ireland. After 25 years service with the British Army's Intelligence Corps he became a business manager and a researcher and analyst in the area of Information Warfare and computer crime at a defence research establishment.

In September 2002, on completion of a paper on a method for the metrication of the threats to information systems, he left the defence environment to take up a post as a principal lecturer at the University of Glamorgan in the subjects of Network Security and Computer Crime and as a researcher on the Threats to Information Systems and Computer Forensics. At the University he developed and managed a well equipped Computer Forensics Laboratory and took the lead on a large number of computer investigations and data recovery tasks.

In January 2005, he joined the Security Research Centre at British Telecommunications where he is currently the head of information security research.

He is the author of five books on the topics of Information warfare, information security and digital forensics, and holds a Ph.D. in the area of threats to information systems.

Plenary Session – Digital Forensics Practice

Implementation of Paperless Case Files in the Queensland Police Department
Troy O'Malley, Queensland Police

Activities in the Speech, Image and Signal Processing Department, IRCGN
Joseph Razik, CNRS-LTCI Telecom ParisTech, France

Plenary Session – The Interaction Between Technology and Law

The Increasing Sophistication of Technology Users: The Case for Counter Anti-Forensics Training
Glenn Dardick, Longwood University

Spoilation and tampering with evidence are certainly not new phenomena, but the current level of sophistication and potential for such actions going undiscovered are cause for concern. Applications and systems are increasingly becoming more sensitive to the privacy needs of individuals. Such new applications and systems upgrades are not necessarily deleting evidence; indeed, they may no longer be creating it in the first place. Applications with the specific purpose of deleting evidence that have been available for some time have now become off-the-shelf software. If the Digital Forensics Expert is a “finder-of-fact”, as is often said, then that expert may be finding those facts more difficult to discover. In truth, the role of the Digital Forensics Expert is, and has been, much more than only a “finder-of-fact”. It is increasingly important that the Digital Forensics Expert develop further investigative critical thinking skills relevant to Counter Anti-Forensics. Additionally, IT security personnel will need to focus more on implementing Counter Anti-Forensics measures.

Glenn S. Dardick is an Assistant Professor of Information Systems at Longwood University, USA, and is an Adjunct Associate Professor at Edith Cowan University, Australia. He is responsible for the Digital Forensics, Security and Law program at Longwood University and lectures at the undergraduate and postgraduate levels. Glenn S. Dardick also serves as the Editor-in-Chief of the Journal of Digital Forensics, Security and Law and has over 34 years experience in the IT Industry serving in technical, managerial and academic positions in both public organizations and private enterprises. He began working with microcomputers and microcomputer storage media over 30 years ago and was an original member of the IBM PC development team.

What Lawyers Want

Nigel Carson, Ferrier Hodgson

Nigel began his computer forensics career within the Computer Based Evidence section of the NSW Police Service where he helped establish an effective support base for major criminal investigations assisting with State and Federal investigations, working alongside other investigative agencies such as ASIO and the Crime Commission. Since leaving the service, Nigel has worked within forensics for KPMG and as the computer security manager for Australasia with Coca Cola Amatil.

Nigel has personally examined thousands of computers, electronic devices and other digital media. He has provided expert reports and presented expert testimony in computer forensics and electronic evidence for numerous civil and criminal proceedings at all levels of the judicial process. He has also presented computer evidence in numerous criminal matters including fraud, drug supply, child protection matters, copyright matters, homicide investigations and cyber crimes. In particular, Nigel has recently provided expert evidence in the Kazaa music piracy matter.

The Admissibility of Forensic Evidence

Anna Davey, Forensic Foundations Pty Ltd

Principles outlining the admissibility of all evidence are found both in the common law and in statute. The admissibility of expert evidence has additional and more stringent requirements than does evidence of fact or of a ‘lay’ witness.

This presentation will discuss the admissibility of evidence generally, and expert evidence including electronic evidence more specifically. This will include an examination of the processes used before and during the examination (including chain of custody & documentation) and the training/qualifications/experience of the witnesses. This presentation will also highlight a number of significant cases both in Australia and overseas.

From 2000 - 2004, Anna was Executive Officer of the National Institute of Forensic Science and in 2004, she was appointed Deputy Director. Anna acted as Director of the Institute for seven months in 2003/4 and twelve months in 2007/8. She has a particular interest in the interface between science and the law and has conducted Provision of Expert Evidence workshops over the last eight years.

Anna operates in all areas of the forensic sciences focusing on quality management, the interface between science and the legal system and forensic science based R&D. Anna brings an unequalled depth of knowledge and experience to these. Of special interest is her ability to help prepare inexperienced practitioners for appearances in court or when required to provide expert advice.

Technical Program

confirmed papers, subject to minor scheduling changes

Technical Session 1: Voice and Telephony

- 9795 Forensics for detecting P2P network originated MP3 files on the user device
- 9774 Developing Speaker Recognition System: from Prototype to Practical Application
- 10396 Vocal forgery in forensic sciences

Technical Session 2: Investigative Practice

- 9879 A Preliminary Approach to the Forensic Analysis of an Ultraportable ASUS Eee PC
- 9785 Investigating Encrypted Material
- 9779 Robust Correctness Testing for Digital Forensic Tools
- 9835 The Development of a Generic Framework for the Forensic Analysis of SCADA and Process Control Systems.

Technical Session 3: Image Source Identification

- 10518 Detection of Block Artifacts for Digital Forensic Analysis
- 9831 Distinguishing between camera and scanned images by means of frequency analysis
- 10447 Analysis of Sensor Photo Response Non-Uniformity in RAW images
- 10627 Decomposed Photo Response Non-Uniformity for Digital Forensic Analysis

Technical Session 4: Image Authentication

- 9816 Authenticating Medical Images through Repetitive Index Modulation Based Watermarking
- 9843 Medical Image Authentication using DPT Watermarking: A Preliminary Attempt
- 10443 Audit Log for Forensic Photography

Technical Session 5: Legal Considerations

- Invited Paper* Grey Areas? The Legal Dimensions of Cloud Computing
- 9844 Cyber forensics Ontology for the cyber criminal investigation
- 9870 Legal and Technical Implications of Collecting Wireless Data as an Evidence Source
- 9800 FIA: An Open Forensic Integration Architecture for Composing Digital Evidence

Technical Session 6: Security and Applications

- 9833 A Provable Security Scheme of ID-based Threshold Decryption
- 9770 Image Encryption Using Chaotic and Max-Heap Tree
- 10480 Surveillance Applications of Biologically-Inspired Smart Cameras
- 9841 A Novel Handwritten Letter Recognizer Using Enhanced Evolutionary Neural Network

International Workshop on e-Forensics Law

Note: Registration for the e-Forensics Conference includes automatic registration for e-Forensics Law. Registration for the workshop is available separately.

Plenary Session

Opening Remarks,

The Hon John Ronald Mansfield, Judge, Federal Court of Australia

The Cybercrime Convention: a roadmap across jurisdictional nightmares?

Professor Joseph A. Cannataci Spes. Rettsinfo. (Oslo) LLD FBCS CTP

ICANN and the World Summits on the Information Society in Geneva or Tunis may have their importance but the Cybercrime Convention is the only binding international treaty governing the Internet. What is it all about and is it going places?

Is Everything Sacred? The Increasing Effect of Privacy and Privilege on eDiscovery and the Changing Role of the Digital Forensics Expert

Dr Glenn S. Dardick

In an adversarial legal system, the potential for abuse in the discovery process has long been recognized. The potential for abuse exists with those seeking discovery and the rights of those from whom discovery is sought must be protected. In the past discovery could be restricted only with convincing arguments that the information from such discovery might be found unresponsive and consequently certain rights might be abridged. However, it is now with increasing frequency that the claims of Privacy and Privilege are being used to effectively hinder discovery and, in particular, eDiscovery. This has resulted in the substitution of "sparse" data discovery for the full digital forensic images of media. It is under these new circumstances that the role and necessary expertise of digital forensics experts is changing.

Suspect sciences? Evidentiary problems with emerging technologies

Associate Professor Gary Edmond

Many different types of expertise are used in security, surveillance, investigations and the prosecution of crime. In recent years the proliferation of networked computers, mobile phones, and CCTV cameras has fostered new types of evidence and new types of expertise, facilitating the identification of persons from voice recordings, security images, and even the linguistic analysis of SMS and email messages. As things stand, Australian police, investigative and security agencies, prosecutors, along with federal and state courts, have not developed principled approaches to the use and admissibility of emerging technologies, their products and the different forms of expertise (and opinion) based upon them. The paper suggests that these developments are unfortunate because relatively few of the new techniques have been tested or independently reviewed. Using the identification of offenders from security and surveillance images as an example, the paper endeavours to explain some of the problems with pervasive technologies and new forms of expert opinion evidence. In response, it suggests that judges: should show more interest in the reliability (really validity and reliability) of incriminating expert opinion evidence; should abandon recourse to inclusive admissibility criteria (such as the exception to opinion evidence based on *ad hoc expertise*); should be more willing to apply exclusionary rules and discretions; and should adopt a more credible approach to the practical limitations of adversarial trials and the risks posed by incriminating expert opinion evidence. In closing, it will be suggested that that courts, particularly Australian and British courts, will impose more demanding admissibility standards over the next decade and that those involved in e-forensics, biometrics and identification should begin to respond to anticipated interest in the validity and reliability of their systems and opinions.

Academic Papers Session

9791 Digital Identity - The legal Person?

9852 Surveillance and Datenschutz in Virtual Environments

10380 Complying Across Continents: At the Intersection of Litigation Rights and Privacy Rights

This draft program released January 6, 2009. Please visit www.e-forensics.eu for updated program details

e-Forensics Law Workshop: Academic Papers Session

9791 Digital Identity - The legal Person?

Clare Sullivan, University of Adelaide, Australia

This paper examines the concept of digital identity which the author asserts is now clearly evident in the United Kingdom as a consequence of the Identity Cards Act (UK) 2006 and the National Identity Scheme it establishes. The nature and functions of the concept, particularly the set of information which constitutes an individual's transactional identity, are examined. The paper then considers the central question of who, or what, is the legal person in a transaction i.e. who or what enters into legal relations. The analysis presents some intriguing results which were almost certainly not envisaged by the legislature. The implications extend beyond the United Kingdom to similar schemes in other jurisdictions, and to countries, like Australia, which may implement such a scheme.

9852 Surveillance and Datenschutz in Virtual Environments

Sabine Cikic, Fritz Lehmann-Grube, and Jan Sablatnig, Technische Universität Berlin, Germany

Virtual environments are becoming more and more accepted, and part of the everyday online experience for many users. This offers new potential for both surveillance and data mining. Some of the techniques used are discussed in this paper. However, such activities may in many countries conflict with the legal framework in place, for example with the German Federal Data Protection Act (Datenschutzgesetz). This point is illustrated by means of comparisons with real-world collection of personal data scenarios such as telephone tapping or video surveillance.

10380 Complying Across Continents: At the Intersection of Litigation Rights and Privacy Rights

Milton H. Luoma, Jr., Metropolitan State University, Minnesota. Vicki M. Luoma, Minnesota State University, USA

Complying with legal restrictions on litigation rights and privacy rights in different international jurisdictions has proven to be one of the most difficult challenges facing multinational corporations. At the heart of this challenge are the different priorities that different nations place upon an individual's right to litigate disputes and an individual's right to privacy. This paper addresses the issues and challenges facing multinational corporations when they become involved in litigation that crosses international borders.

Technical Session 1: Voice and Telephony

9795 Forensics for detecting P2P network originated MP3 files on the user device

Heikki Kokkinen and Janne Nöyränen, Nokia Research Center, Finland

This paper presents how to detect MP3 files that have been downloaded from peer-to-peer networks to a user hard disk. The technology can be used for forensics of copyright infringements related to peer-to-peer file sharing, and for copyright payment services. We selected 23 indicators, which show peer-to-peer history for a MP3 file. We developed software to record the indicator values. A group of selected examinees ran the software on their hard disks. We analyzed the experimental results, and evaluated the indicators. We found out that the performance of the indicators varies from user to user. We were able to find a few good indicators, for example related to the number of MP3 files in one directory.

9774 Developing Speaker Recognition System: from Prototype to Practical Application

P. Fränti, J. Saastamoinen, I. Kärkkäinen, T. Kinnunen, V. Hautamäki, I. Sidoroff, University of Joensuu, Finland

In this paper, we summarize the main achievements made in the 4-year PUMS project during 2003-2007. The emphasis is on the practical implementations, how we have moved from Matlab and Praat scripting to C/C++ implemented applications in Windows, UNIX, Linux and Symbian environments, with the motivation to enhance technology transfer. We summarize how the baseline methods have been implemented in practice, how the results are utilized in forensic applications, and compare recognition results to the state-of-art and existing commercial products such as ASIS, FreeSpeech and VoiceNet.

10396 Vocal forgery in forensic sciences

Patrick Perrot, Mathieu Morel, Joseph Razik, Gérard Chollet

Institut de Recherche Criminelle de la Gendarmerie Nationale and CNRS-LTCI-Telecom-ParisTech, France

This article describes different techniques of vocal forgery able to affect automatic speaker recognition system in a forensic context. Vocal forgery covers two main aspects: voice transformation and voice conversion. Concerning voice transformation, this article proposes an automatic analysis of four specific disguised voices in order to detect the forgery and, for voice conversion, different ways to automatically imitate a target voice. Vocal forgery appears as a real and relevant question in the area of forensic speaker recognition. In most cases, criminals who make a terrorist claim or a miscellaneous call, disguise their voices in order to hide their identity or to take the identity of another person. Disguise is considered in this paper as a deliberate action of the speaker who wants to conceal or falsify his identity. Channel distortion or environment noise for instance, are not considered as a way of disguise. Different techniques exist to transform one's own voice. Some are sophisticated as software manipulation, some others are simpler as using an handkerchief over the mouth. In the field of voice transformation, the presented work is dedicated to the study of disguise used in the most common cases. In the field of voice conversion, different techniques will be presented, compared, and applied on an original example of the French President's voice.

Technical Session 2: Investigative Practice

9879 A Preliminary Approach to the Forensic Analysis of an Ultraportable ASUS Eee PC

Trupti Shiralkar, Michael Lavine, Johns Hopkins University, USA; Benjamin Turnbull, University of South Australia

Subnotebooks, or Netbooks, are a relatively new consumer market but one that continues to grow significantly worldwide. The aim of this paper is to analyse one of the leading subnotebooks, the ASUS Eee PC from a forensics perspective. Specifically, the work investigates current image creation methods for making image of Eee PCs Solid State Drive and it analyses forensically important artefacts.

9785 Investigating Encrypted Material

Niall McGrath, Pavel Gladyshev, Tahar Kechadi and Joe Carthy, University College Dublin, Dublin, Ireland

When encrypted material is discovered during a digital investigation and the investigator cannot decrypt the material then s/he is faced with the problem of how to determine the evidential value of the material. This research is proposing a methodology of extracting probative value from the encrypted file of a hybrid cryptosystem. The methodology also incorporates a technique for locating the original plaintext file. Since child pornography (KP) images and terrorist related information (TI) are transmitted in encrypted format the digital investigator must ask the question Cui Bono? - who benefits or who is the recipient? By doing this the scope of the digital investigation can be extended to reveal the intended recipient.

9779 Robust Correctness Testing for Digital Forensic Tools

Lei Pan and Lynn M. Batten, Deakin University, Australia

In previous work, the authors presented a theoretical lower bound on the required number of testing runs for performance testing of digital forensic tools. We also demonstrated a practical method of testing showing how to tolerate both measurement and random errors in order to achieve results close to this bound. In this paper, we extend the previous work to the situation of correctness testing. The contribution of this methodology enables the tester to achieve correctness testing results of high quality from a manageable number of observations and in a dynamic but controllable way. This is of particular interest to forensic testers who do not have access to sophisticated equipment and who can allocate only a small amount of time to testing.

9835 The Development of a Generic Framework for the Forensic Analysis of SCADA and Process Control Systems

Jill Slay, University of South Australia

There is continuing interest in researching generic security architectures and strategies for managing SCADA and process control systems. Documentation from various countries on IT security does now begin to recommendations for security controls for (federal) information systems which include connected process control systems. Little or no work exists in the public domain which takes a big picture approach to the issue of developing a generic or generalisable approach to SCADA and process control system forensics. The discussion raised in this paper is that before one can develop solutions to the problem of SCADA forensics, a good understanding of the forensic computing process, and the range of technical and procedural issues subsumed with in this process, need to be understood, and also agreed, by governments, industry and academia. This then provides the holistic framework into which potential technical solutions can be fitted in a jigsaw-like fashion.

Technical Session 3: Image Source Identification

10518 Detection of Block Artifacts for Digital Forensic Analysis

Chang-Tsun Li, University of Warwick, UK

Although the metadata, such as the header, of a piece of media carries useful information, the metadata may be tampered with for various purposes. It is therefore desirable in the context of forensic analysis that investigators are able to infer properties and information about a piece of media directly from its content without any reference to the metadata. The block size of the block operations that a piece of media has undergone can provide useful clue about the trustworthiness of the metadata and in turn reveals the integrity of the media. In this work, we proposed a novel block artifact detection method for inferring the block size of block-wise operations, such as JPEG compression, that has been applied to the media under investigation. Based on the assumption that block operation create disparities across block boundaries and those boundaries form straight lines, our method exploits the fact that intra-block variance tend to be less than inter-block variance and if most of the pixels along the same vertical line or horizontal line exhibit this relationship then the straight line is believed to be the block boundary.

9831 Distinguishing between camera and scanned images by means of frequency analysis

Roberto Caldelli, Irene Amerini, and Francesco Picchioni, University of Florence, Italy,

Distinguishing the kind of sensor which has acquired a digital image could be crucial in many scenarios where digital forensic techniques are called to give answers. In this paper a new methodology which permits to determine if a digital photo has been taken by a camera or has been scanned by a scanner is proposed. Such a technique exploits the specific geometrical features of the sensor pattern noise introduced by the sensor in both cases and by resorting to a frequency analysis can infer if a periodicity is present and consequently which is the origin of the digital content. Experimental results are presented to support the theoretical framework.

10447 Analysis of Sensor Photo Response Non-Uniformity in RAW images

Simon Knight, Simon Moschou, and Matthew Sorell, The University of Adelaide, Australia

The focus of this paper is a review of a digital camera identification technique proposed by Lukas et al, and a modification of the denoising filter, allowing it to be used for raw sensor data. The approach of using raw sensor data allows analysis of the noise pattern separate from any artefacts introduced by on-board camera processing. We use this extension for investigating the reliability of the technique when using different lenses between the same camera and between cameras of the same manufacturer.

10627 Decomposed Photo Response Non-Uniformity for Digital Forensic Analysis

Yue Li and Chang-Tsun Li, University of Warwick, UK

The last few years have seen the applications of Photo Response Non-Uniformity noise (PRNU) - a unique stochastic fingerprint of image sensors, to various types of digital forensic investigations such as source device identification and integrity verification. In this work we proposed a new way of extracting PRNU noise pattern, called Decomposed PRNU (DPRNU), by exploiting the difference between the physical and artificial color components of the photos taken by digital cameras that use a Color Filter Array for interpolating artificial components from physical ones. Experimental results presented in this work have shown the superiority of the proposed DPRNU to the commonly used version. We also proposed a new performance metrics, Corrected Positive Rate (CPR) to evaluate the performance of the common PRNU and the proposed DPRNU.

Technical Session 4: Image Authentication

9816 Authenticating Medical Images through Repetitive Index Modulation Based Watermarking

Chang-Tsun Li and Yue Li, University of Warwick, UK

In this work we propose a Repetitive Index Modulation (RIM) based digital watermarking scheme for authentication and integrity verification of medical images. Exploiting the fact that many types of medical images have significant background areas and medically meaningful Regions Of Interest (ROI), which represent the actual contents of the images, the scheme uses the contents of the ROI to create a content-dependent watermark and embeds the watermark in the background areas. Therefore when any pixel of the ROI is attacked, the watermark embedded in the background areas will be different from the watermark calculated according to the attacked contents, making the authentication unsuccessful. Because the creation of the watermark is content-dependent and the watermark is only embedded in the background areas, the proposed scheme can actually protect the content without distorting it.

9843 Medical Image Authentication using DPT Watermarking: A Preliminary Attempt

*M. L. Dennis Wong, Antionette Goh and Hong Siang Chua,
Swinburne University of Technology, Sarawak Campus, Malaysia.*

Secure authentication of digital medical image content provide great value to the e-Health community and medical insurance industries. Fragile Watermarking has been proposed to provide the mechanism to authenticate digital medical image securely. Transform Domain based Watermarking are typical slower than spatial domain watermarking owing to the overhead in calculation of coefficients. In this paper, we propose a new discrete Pascal transform based watermarking technique. Preliminary experiment result shows authentication capability. Possible improvements on the proposed scheme are also presented before conclusions.

10443 Audit Log for Forensic Photography

Timothy Neville, Matthew Sorell, University of Adelaide, Australia

We propose an architecture for an audit log system for forensic photography, which ensures that the chain of evidence of a photograph taken by a photographer at a crime scene is maintained from the point of image capture to its end application at trial. The requirements for such a system are specified and the results of experiments are presented which demonstrate the feasibility of the proposed approach.

Technical Session 5: Legal Considerations

Invited Paper: Grey Areas? The Legal Dimensions of Cloud Computing

Michael Davis and Alice Sedsman, Delta Legal, Adelaide

Cloud computing has been heralded as a new era in the evolution of information and communications technologies. Corporate giants IBM, Google, Amazon and Microsoft have invested millions of dollars in developing new technologies which allow end users to access web-based applications without the need to invest in software applications. Cloud computing hosts store data uploaded by end users in huge server facilities designed specifically for this purpose. Businesses using cloud computing services will benefit from reduced operating costs as they cut back on IT infrastructure and personnel. Individuals will no longer need to install ad pay for software application licences.

For everyday users, the ability to access their data from any internet device from anywhere in the world is a tempting prospect. However, for every benefit associated with cloud computing, there is an inherent legal risk. The global nature of cloud computing raises many questions about privacy, security, confidentiality and access to data. Current terms of use do not adequately address the multitude of legal issues that are unique to cloud computing and legal systems around the world continue to play catch-up. In the face of this legal uncertainty, end users should be educated about the risks involved in entering the cloud.

9844 Cyber forensics Ontology for the cyber criminal investigation

Heum Park, Hyuk-Chul Kwon, Pusan National University, Busan, Korea

We developed Cyber Forensics Ontology for the criminal investigation in cyber space. Cyber crime is classified into cyber terror and general cyber crime, and those two classes are connected with each other. The investigation of cyber terror requires high technology, system environment and experts, and general cyber crime is connected with general crime by evidence from digital data and cyber space. Accordingly, it is difficult to determine relational crime types and collect evidence. Therefore, we considered the classifications of cyber crime, the collection of evidence in cyber space, and the application of laws to cyber crime. In order to efficiently investigate cyber crime, it is necessary to integrate those concepts for each cyber crime-case. Thus, we constructed a cyber forensics domain ontology for criminal investigation in cyber space, according to the categories of cyber crime, laws, evidence and information of criminals. This ontology can be used in the process of investigating of cyber crime-cases, and for data mining of cyber crime; classification, clustering, association and detection of crime types and criminals.

9870 Legal and Technical Implications of Collecting Wireless Data as an Evidence Source

Benjamin Turnbull, Grant Osborne and Matthew Simon, University of South Australia

The collection of digital devices for forensic analysis is an area that requires constant revision. New technologies and connectivity options change what devices are able to hold electronic evidence and also the methods needed to secure it. This work focuses on the development of an 802.11-based wireless networking (Wi-Fi) forensic analysis tool that can aid in the identification and collection of evidence by identifying the presence of wireless networks and the devices to which they are attached. Specifically, this paper seeks to discuss the potential legal and technical challenges faced in the development of a wireless forensic tool.

9800 FIA: An Open Forensic Integration Architecture for Composing Digital Evidence

Sriram Raghavan, Andrew Clark and George Mohay, Queensland University of Technology, Australia

The analysis and value of digital evidence in an investigation has been the domain of discourse in the digital forensic community for several years. While many works have considered different approaches to model digital evidence, a comprehensive understanding of the process of merging different evidence items recovered during a forensic analysis is still a distant dream. With the advent of modern technologies, pro-active measures are integral to keeping abreast of all forms of cyber crimes and attacks. This paper motivates the need to formalize the process of analyzing digital evidence from multiple sources simultaneously. In this paper, we present the forensic integration architecture (FIA) which provides a framework for abstracting the evidence source and storage format information from digital evidence and explores the concept of integrating evidence information from multiple sources. The FIA architecture identifies evidence information from multiple sources that enables an investigator to build theories to reconstruct the past. FIA is hierarchically composed of multiple layers and adopts a technology independent approach. FIA is also open and extensible making it simple to adapt to technological changes. We present a case study using a hypothetical car theft case to demonstrate the concepts and illustrate the value it brings into the field. **KEYWORDS:** FIA, technology-independent, digital evidence, evidence unit, evidence correlation, evidence composition

Technical Session 6: Security and Applications

9833 A Provable Security Scheme of ID-based Threshold Decryption

WANG Xue-Guang, East China University of Politics and Law, China;

Chai Zhen-Chuan, Samsung Electronics R&D Centre

This paper presents an ID-based threshold decryption scheme and proves that it is selective chosen ciphertext secure without random oracles based on solving decisional problem assumption.

9770 Image Encryption Using Chaotic and Max-Heap Tree

F.Mahmoudi,R. Enayatifar, Azad Ghazvin University, Ghazvin, Iran

In this paper, a new method is proposed for image encryption using chaotic signals and Max-Heap tree. In this method, Max-Heap tree is utilized for further complexity of the encryption algorithm, higher security and changing the amount of gray scale of each pixel of the original image. Studying the obtained results of the performed experiments, high resistance of the proposed method against brute-force and statistical invasions is obviously illustrated. Also, the obtained entropy of the method which is about 7.9931 is very close to the ideal amount of 8.

10480 Surveillance Applications of Biologically-Inspired Smart Cameras

Kosta Haltis, Lee Andersson, Matthew Sorell, Russell Brinkworth, University of Adelaide, Australia

Biological vision systems are capable of discerning detail and detecting motion in a wide range of highly variable lighting conditions. We describe the real-time implementation of a biological vision model using a high dynamic range video camera and a General Purpose Graphics Processing Unit (GPGPU) and demonstrate the effectiveness of the implementation in two surveillance applications: dynamic equalization of contrast for improved recognition of scene detail; and the use of biologically-inspired motion processing for the detection of small or distant moving objects in a complex scene.

9841 A Novel Handwritten Letter Recognizer Using Enhanced Evolutionary Neural Network

Mohsen Mirzashaeri, Ehsan Shahamatnia and Fariborz Mahmoudi, IslamicAzad University of Qazvin, Iran

This paper introduces a novel design for handwritten letter recognition by employing a hybrid back-propagation neural network with an enhanced evolutionary algorithm. Feeding the neural network consists of a new approach which is invariant to translation, rotation, and scaling of input letters. Evolutionary algorithm is used for the global search of the search space and the back-propagation algorithm is used for the local search. The results have been computed by implementing this approach for recognizing 26 English capital letters in the handwritings of different people. The computational results show that the neural network reaches very satisfying results with relatively scarce input data and a promising performance improvement in convergence of the hybrid evolutionary back-propagation algorithms is exhibited.