# CFET 2010

**4th International Conference on**
**Cybercrime Forensics Education & Training**

# Conference Programme & Abstracts

**Canterbury Christ Church University**
**Faculty of Social & Applied Sciences**
**Department of Computing**
**North Holmes Road Campus**
**Powell Building**
**2nd & 3rd September 2010**

**ISBN 978-1-899253-73-9**

# Contents

# Introduction to the Conference

Cybercrime Forensics one of the fastest areas of growth within the Computing discipline as it mirrors the explosive growth of criminal activity involving computers. The growing complexity and vulnerability of computer systems and the new forms of criminal activities require research and development to continue to ensure the integrity and security for computer users. The demand for people qualified to assist in cybercrime investigations is very large and growing.

This conference invited papers and presentations on the following:

- Development of cybercrime forensics as a new discipline
- Commercial training in cybercrime forensics
- Supporting police investigations
- Defining educational programmes and their objectives
- Ethical, Professional and legal issues
- New software tools for cybercrime forensics
- International cooperation to develop standards
- Career pathways in cybercrime forensics
- Network and mobile communication technologies
- Cooperation of commercial and academic partners
- Case studies in cybercrime forensics
- Risk management and disaster planning
- Future trends in cybercrime forensics

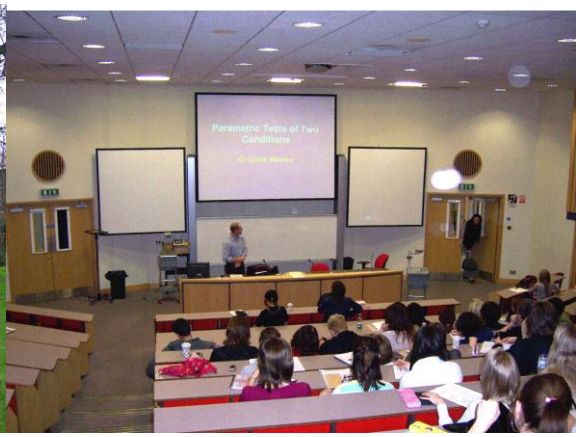
The conference has attracted a range of speakers, sponsors and delegates from eleven countries. These include serving police officers, high tech crime practitioners, independent consultants, police trainers and university teachers and researchers.

The conference is very grateful to the support provided by its sponsors and the advice and help of the CFET International Advisory Panel (detailed later in this booklet).

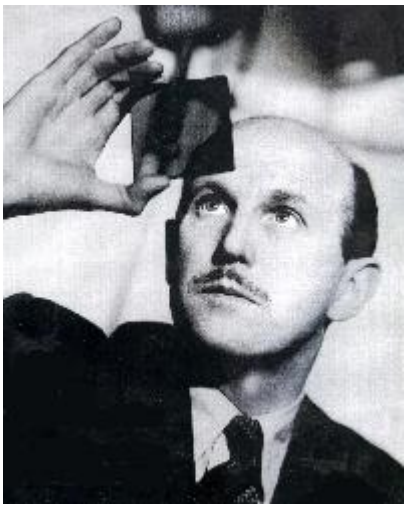
I would like to welcome everyone to Canterbury Christ Church University and the Department of Computing who are playing host to this fourth annual international conference and hope your stay with us is a very enjoyable and informative one.

Denis Edgar-Nevill
Chair, CFET 2010

## Conference Venue




The Powell Building was opened in 1999 and named after film maker Michael Powell. Powell's contribution to British, and indeed, to world cinema cannot be overestimated. His influence can be seen in the works of many of today's leading film makers, including Martin Scorsese and Francis Ford Coppola.



# Conference Organisers

## *Conference Chair*

**Denis Edgar-Nevill** Canterbury Christ Church University

## *Conference Organising Committee*

**Dr Abhaya Induruwa** Canterbury Christ Church University
**Dr Man Qi** Canterbury Christ Church University
**Paul Stephens** Canterbury Christ Church University
**Matthew Tubby** Canterbury Christ Church University

## *International Advisory Panel*

**Susan Ballou** Program Manager, Office of Law Enforcement Standards, NIST, USA

**Dr Robin Bryant** Head of Crime & Policing, Canterbury Christ Church University, UK

**Professor Joe Carthy** University College Dublin, Republic of Ireland

**Professor Peter Cooper** Department Chair Computer Science, Sam Huston State University, Texas, USA

**Dr Philip Craiger** Assistant Director for Digital Evidence, National Center for Forensic Science University of Central Florida, USA

**Bill Crane** Head of Operations, National Digital Crime Investigations Unit, New Zealand

**Dr. Rob D'Ovidio** Drexel University, USA

**Denis Edgar-Nevill** Head of Computing, Canterbury Christ Church University, UK

**Keerthi Goonatillake** School of Computing, University of Colombo, Sri Lanka

**Dr Douglas Harris** CyberSecurity and Emergency Preparedness Institute, Associate Dean, Erik Jonsson School, Engineering and Computer Science, University of Texas at Dallas, USA

**Ron Jewell** Manager, Forensic Science Center, Marshall University, USA

**Professor Nigel Jones** Managing Director, Technology Risk Ltd, UK
Adjunct Professor University College Dublin, Republic of Ireland

**Dr Manolya Kavakli** Department of Computing, Macquarie University, Australia

**Gary C. Kessler** Cybercrime Consultant, Vermont, USA

**Jack McGee** President, Justice Institute of British Columbia, Canada

**Rob Risen** Police Academy of the Netherlands

**Professor Rongsheng Xu** Chief Scientist, National Computer Network Intrusion Protection Center, China

# CFET 2010 Conference Schedule

## *Day 1 –2nd September 2010*

10.00 - 10.30 **Registration & Coffee – foyer Powell Building**

10.30 - 10.45 **Welcome to the Conference – Powell Lecture Theatre**

Dr Robin Baker, Vice Chancellor
Canterbury Christ Church University, UK

Denis Edgar-Nevill, Chair CFET 2010
Head of Department Computing
Canterbury Christ Church University, UK

10.45 - 11.30 **Invited Keynote Presentation – Powell Lecture Theatre**

***"Forensic science quality standards: the past, present and future (focusing on computer forensics)"***

Andrew Rennison
UK Forensic Regulator

11.30 – 13.00 **Parallel Presentation Sessions**

**Powell Lecture Theatre**

11.30 – 12.00 ***"Combating Cyber Crime in the UAE"***
Jassim I Al Mansoorii, Grahame Benmore, Margaret Ross
Southampton Solent University

12.00 – 12.30 ***"Protecting Intellectual Property and Computer Software: Legislation in China"***
Dr Man Qi & Yongquan Wang
Canterbury Christ Church University

12.30 – 13.00 "**HoneyClients for Teaching in Cybercrime and Forensics"**
Peter Komisarczuk
Thames Valley University &
Victoria University of Wellington, New Zealand

**Powell Pg06 Lecture Theatre**

11.30 – 12.00 ***"Digital Meta-Forensics"***
Richard Overill, Kings College London

12.00 – 12.30 ***"An Investigation into Forensic Analysis of Deniably Encrypted Drives"***
Ellen Moar, University of Abertay Dundee

12.30 – 13.00 ***"Assessing Cryptology"***
David Bennett, Canterbury Christ Church University

**Powell Pf07 Lecture Theatre**

11.30 – 12.00 ***"Student Perception of On-line Lectures within a Blended Learning Environment for Security and Digital Forensics"***
Bill Buchanan, Richard MacFarlane, and Robert Ludwiniak
Napier University

12.00 – 12.30 ***"Cybercrime vs Cyber War"***
Denis Edgar-Nevill, Canterbury Christ Church University

12.30 – 13.00 ***"A Low Cost Forensic Tool for Analyzing Huge Data Sets in Digital Investigations"***
Yasantha N Hettiarachchi, T.N.K. De Zoysa, K. S. Goonetillake
University of Colombo, Sri Lanka

**Workshop Computer Laboratory**

12.00-13.00 ***"The exploit, the exploiter, the exploited…"***
Righard J. Zwienenberg, Norman Data Defense Systems

13.00 - 14.00 **Lunch**

14.00 – 15.30 **Parallel Presentation Sessions**

**Powell Lecture Theatre**

14.00 – 14.30 ***"Virtualisation based Forensic Computing Research Tool"***
Chris Hargreaves & Howard Chivers, Cranfield University

14.30 – 15.00 ***"The Advantages and Risks of Live Data Collection"***
Ron Tasker, University of Bradford

15.00 – 15.30 ***"Integrating Digital Forensics in a Crime Scene Investigation Exercise"***
Michael Jones, Bournemouth University

**Powell Pg06 Lecture Theatre**

14.00 – 14.30 ***"Using Biometric Access Control for Forensic Identification: Benefit or Bind?"***
Lynne Norris-Jones, University of Wales Institute

14.30 – 15.00 ***"An Enhanced Eigenfaces-based Biometric Forensic Model"***
Nasser S. Abouzakhar and Praneeth Enjamuri
The University of Hertfordshire

15.00 – 15.30 ***"Towards Scientific Malware Analysis"***
Ian Kennedy, The Open University

**Powell Pf07 Lecture Theatre**

14.00 – 14.30 ***"Antivirus Testing and AMTSO: has anything changed?"***
David Harley, ESET

14.30 – 15.00 ***"Traffic Analysis, Anonymity, Ethics and digital "cat and mouse" in Cyberspace"***
Jon Shahab, Reza Mousoli, Canterbury Christ Church University

15.00 – 15.30 ***"Constantly Evolving Technological Challenges in Cybercrime Forensic Investigation"***
Abhaya Induruwa, Canterbury Christ Church University

**Workshop Computer Laboratory**

14.00 – 15.00 ***Cellbrite*** Miss. Adi Lutchinsky

15.30 - 16.00 **Coffee & Exhibitors - Powel Foyer and Powell Pg05**

16.00 - 17.20 **AGM BCS Cybercrime Forensics Specialist Group** (Open meeting)

16.00-16.15 Review of the last year
16.15-16.20 Committee Elections (BCS members only)
16.20-16.30 Prize – Summer Competition
16.30-17.30 Invited Presentation
***"Think Like a Hacker***
***- An Ethical Hacker's View of Corporate Security"***

Peter Wood, CEO First Base Technologies

17.30 – 18.30 **BCS Cybercrime Forensics SG Committee Meeting** (Closed meeting)

18.30 – 19.00 **Drinks Reception**
Blue Room and the Senior Common Room of the North Holmes Rd Campus of Canterbury Christ Church University.

19.00- 21.00 **Conference Dinner**
Blue Room and the Senior Common Room of the North Holmes Rd Campus of Canterbury Christ Church University.

## *Day 2 – 3rd September 2010*

09.00 – 10.00 **Parallel Presentation Sessions**

**Powell Lecture Theatre**

09.00-09.30 ***"The Relationship between Digital Investigations and Reduction in Cybercrime"***
Alastair Irons, University of Sunderland

09.30-10.00 ***"Detection of Information Compromise Committed by Malicious Insiders"***
Andrew Hawkins and Denis Edgar-Nevill
Metropolitan Police, Canterbury Christ Church University

**Powell Pg06 Lecture Theatre**

09.00-09.30 "***A comparative study of the structure and behaviour of the operating system thumbnail caches used in Kubuntu and Ubuntu (9.10 and 10.04)"***
Sarah Morris, Professor Howard Chivers, Cranfield University

09.30-10.00 ***"Developing a GUI interface to the MS Log Parser"***
Fahad Mir and Dimitris Tsaptsinos, Kingston University

**Powell Pf07 Lecture Theatre**

09.00-09.30 ***"Open Delegates Discussion: Cybercrime, Digital Forensics & the 'Cloud' (ETHICS, PROFESSIONAL & LEGAL ISSUES)"***
Robet Dube, Roehampton University

09.30-10.00 ***"SODDImy and the Trojan Defence"***
David Harley, ESET

10.00 – 10.30 **Coffee & Exhibitors - Powel Foyer and Powell Pg05**

10.30 – 11.15 **Invited Keynote Presentation – Powell Lecture Theatre**
***"ACPO Good Practice Guide for Digital Evidence (Ver 5)"***
Steve Edwards, PCeU

11.15 – 13.00 **Parallel Presentation Sessions**

**Powell Lecture Theatre**

11.15-11.40 ***"Support for Paedophile image viewers"***
Clare Bracey & Denis Edgar-Nevill
Sussex Police & Canterbury Christ Church University

11.40-12.05 ***"Social Networking Sites, Privacy and Digital Security"***
Kate Andrade, Reza Mousoli
GCHQ & Canterbury Christ Church University

12.05-12.30 ***"A Digital Forensics Case Generator"***
Michael Jones, Bournemouth University

12.30-13.00 ***"Using PFSense and Commodity Hardware as a Medium Interaction Honey-net Network"***
Georgios Chlapoutakis, Anastasios Laskos,
Phillip J. Brooke, Mark Truran
University of Sunderland & University of Teesside

**Powell Pg06 Lecture Theatre**

11.15-11.40 ***"A Chi-square testing-based intrusion detection Model"***
Nasser S. Abouzakhar and Abu Bakar Muhammad
The University of Hertfordshire

11.40-12.05 ***"Machine Learning based Spam Filtering: Advantages and Challenges"***
Man Qi, Canterbury Christ Church University

12.05-12.30 ***"A model to support the authentication of mobile transaction"***
Xuan Huang, University of Abertay Dundee

12.30-13.00 ***"Problems with prosecuting Computer crimes"***
Karl Obayi, iTevidence

**Powell Pf07 Lecture Theatre**

11.15-11.40 ***"Criteria for Successful MSc Research Projects in Computer Forensics"***
Paul Douglas & Colin Myers
University of Westminster

11.40-12.05 ***"The Use of Digital Forensic Case Studies for Teaching and Assessment"***
Harjinder Singh Lallie, University of Derby

12.05-12.30 ***"Engaging Students into Digital Forensics and Cybercrime with Challenging, Ever-changing and Stimulating Environments"***
Bill Buchanan, Richard MacFarlane, Robert Ludwiniak, Jamie Graves and Gordon Russell, Napier University

12.30-13.00 ***"Educating Digital Forensic Investigators at Newport"***
Stilianos Vidalis, Eric Llewellyn
University of Wales, Newport

**Workshop Computer Laboratory**

11.30 – 13.00 ***"XRY Workshop"***
Mike Dickinson, MSAB

13.00 - 14.00 **Lunch**

14.00 - 14.45 **Invited Keynote Presentation – Powell Lecture Theatre**

Professor Nigel Jones
University College Dublin, Republic of Ireland

14.45 - 15.30 **Plenary Panel Session - Powell Lecture Theatre**

15.30—16.00 **Coffee & Exhibitors**

1600 **Conference Close**

# Invited Keynote Presentation

# Forensic Science Quality Standards: the Past, Present and Future (Focusing on Computer Forensics)

Andrew Rennison
UK Forensic Regulator

**Abstract**

The UK has different structures across England and Wales, Scotland and Northern Ireland for its delivery of forensic science services.
Regardless of that we have to acknowledge that crime and science recognise no borders or jurisdictional differences, therefore the quality standards we apply to the delivery of forensic science have to apply across the board. This argument holds equally true for the international arena and the ever increases in exchanges of evidence from country to country and the fast growing need for international investigations - a fact certainly not lost on the computer forensics community.

The delivery model in England and Wales is based largely on a commercial market with half the overall spend on forensics being through work outsourced to companies, this is very much the case with computer forensics but with a large proportion retained in-house by the police high tec-crime units. This commercialisation was the catalyst for change leading to the recruitment of an independent forensic science regulator to essentially develop a modern quality standards framework.

In this presentation the Regulator will explain the history and set the context for a modern standards framework. He will outline that framework, focussing on computer forensics. Current economics and public spending restrictions dictate that the context has to reflect the financial world we operate in and the challenges this presents. Finally, the global context has to be addressed. What value is there is designing a standards framework for the UK that fails to meet the broader and ever pressing international pressures?

**Biography**

Andrew Rennison is the first Forensic Science Regulator, with a vision to develop a modern quality standards framework for UK forensic science and to influence the drive for international standards. He came to this role after a 2 years regulating gambling which in turn followed a 30 year career as a police detective.

# Combating Cyber Crime in the UAE

Jassem I Al Mansoori, Graham Benmore, Margaret Ross
Southampton Solent University,
East Park Terrace, Southampton,
Hampshire, UK
Jassem Al Mansoori jhfa123@hotmail.com,
Graham.Benmore@Solent.ac.uk, Margaret.Ross@Solent.ac.uk

**Abstract**

The paper discusses the growth of the use of the Internet in UAE and the usage of the Internet by the population in the UAE compared with the other Arabian states. This growth and the increasing globalisation, has made the UAE, like other countries, vulnerable to cyber crime. The demographics of the Internet users are considered, including changes over a five year period,

The growth in the use of hand-held devices with Internet access, in the UAE, has led to the proposed ban being placed from Autumn 2010 such as on Blackberry for e-mail and SMS, where the services are being hosted outside the UAE, and are encrypted before being sent out of the UAE, as this makes it difficult for the Government to monitor the content of the communications.

The paper discusses the current development of training for the UAE police forces, at both officer and constable level, to combat e-crime. Other initiatives, such as computer training for the judiciary, and a series of international conferences on computer and Internet crime which were organized in the UAE, are discussed.

The most relevant UAE legislation related to e-crime, Federal Law Number (2), 2006, The Prevention of Information Technology Crimes is considered together with the relevant penalties. The significant differences between this and the relevant UK legislation are considered, including the UAE legislation on e-crimes related to the Islamic Sharia law. The additional content of the UAE legislation, compared to that of the UK is discussed, such as specifically applying to the use of computing for accessing medical information, to terrorism and human trafficking.

Case studies of recent e-crimes in the UAE are considered. The paper concludes by discussing the future plans and recommendations concerning the training for the police and further relevant legislation, the need for increased understanding of digital evidence and the detection of e-related crime is needed together with the availability of computer forensic experts and forensic laboratories in order to combat the crimes of the future,

A rehabilitation programme is considered that could be established for perpetrators of cyber crime, to enable many of them in the future to assist in the prevention and detection of future cyber crimes. Future areas of research are also discussed.

# Protecting Intellectual Property and Computer Software: Legislation in China

Man Qi[1], Yongquan Wang[2]
[1]Department of Computing
Canterbury Christ Church University, Canterbury, UK
man.qi@canterbury.ac.uk
[2]School of Information Science and Technology
East China University of Political Science and Law, Shanghai, China
wangyongquan@ecupl.edu.cn

**Abstract**

Since China joined the World Trade Organization (WTO) in 2001, legislation on intellectual property protection has been anticipated to grow substantially. A range of laws and regulations in this area have been adopted to protect intellectual property and computer software.

The main weapon for computer software protection is the Regulations on the Protection of Computer Software [1], which came into force on 1st January 2002. It clearly addresses software copyright.

For copyright disputes over computer networks, Several Issues concerning the Application of Law in the Trial of Cases Involving Copyright Disputes over Computer Networks (II) [2] is amended by the Supreme People's Court on 20th November 2006. It affirms that the digital form of various works shall be protected by the Copyright Law.

The most remarkable regulation is on network information dissemination is the Regulation on the Protection of the Right to Network Dissemination of Information [3] which came into force on 1st July 2006. The promulgation of the Regulation is to cope the serious situation in which unauthorized works, from movies to television dramas, from music to video games, could be easily downloaded from the Internet. It says that any organization or individual who provides the general public with any other person's works, performance or audio-visual products through the information network shall obtain the owner's permission and pay the relevant remunerations, and technical measures are allowed to be adopted to protect the right to network dissemination of information. The Regulation gives the power to Copyright Administration Departments to punish any individual or company or ISPs who violate the Regulation.

Other valid regulations for intellectual property protection include:

- Notice on the Administration of Computer Software Copyright [4] (Issued by the State Copyright Bureau on October 19, 1994).
- Opinion of the State Copyright Bureau on Copyright Protection of Computer Software [5] (No. 26 [2003] of the State Copyright Bureau).
- Notice of the Ministry of Information Industry, the National Copyright Administration and the Ministry of Commerce on the Relevant Issues about the Presale Installation of Official Operating System Software in Computers [6] (No. 199 [2006] of the Ministry of Information Industry).

- Measures for the Registration of Computer Software Copyright [7] (Issued by the National Copyright Administration of the People's Republic of China on February 20, 2002).
- Administrative Measures for Software Products [8] (Issued by the Ministry of Industry and Information Technology of the People's Republic of China on March 1, 2009).

**References**


[1] Regulations on the Protection of Computer Software.
http://www.lawinfochina.com/law/displayModeTwo.asp?ID=2161&DB=1&keyword=.
last accessed 14/06/2010

[2] Several Issues concerning the Application of Law in the Trial of Cases Involving Copyright Disputes over Computer Networks (II)
http://www.lawinfochina.com/law/display.asp?ID=5691&DB=1
last accessed 10/06/2010

[3] Regulation on the Protection of the Right to Network Dissemination of Information
http://www.lawinfochina.com/law/display.asp?ID=5224&DB=1
last accessed 10/06/2010

[4] Notice on the Administration of Computer Software Copyright
http://www.chinabaike.com/law/zy/bw/gwy/bqj/1376164.html
Last accessed 11/06/2010

[5] Opinion of the State Copyright Bureau on Copyright Protection of Computer Software
http://www.lawinfochina.com/law/display.asp?db=1&id=2990
last accessed 12/06/2010

[6] Notice of the Ministry of Information Industry, the National Copyright Administration and the Ministry of Commerce on the Relevant Issues about the Presale Installation of Official Operating System Software in Computers
http://www.lawinfochina.com/law/display.asp?ID=5140&DB=1
last accessed 13/06/2010

[7] Measures for the Registration of Computer Software Copyright
http://www.lawinfochina.com/law/display.asp?ID=2266&DB=1
last accessed 13/06/2010

[8] Administrative Measures for Software Products
http://www.lawinfochina.com/law/display.asp?ID=7348&DB=1
last accessed 13/06/2010

# HoneyClients for Teaching in Cybercrime and Forensics

Peter Komisarczuk
School of Computing and Technology, Thames Valley University,
St Marys Rd, Ealing, London, UK, W5 5RF
peter.komisarczuk@tvu.ac.uk

**Abstract**

This short paper explore the "honeyclient" as a tool for teaching in cybercrime and forensics. The honeyclient is a device which is used to detect and analyse drive-by-downloads, which in 2010 are the most prevalent of attacks on the Internet. The honeyclient provides a means of determining whether the content received from the Internet is malicious in nature and as such allows the investigator to determine the exploit, the malicious server and the exploit servers used to launch the attack on a users system. It provides a means by which researchers can analyse these types of cyber attacks and acts as a case study that can be used to explore various areas in forensics and cybercrime.

# Digital Meta-Forensics: Quantifying the Investigation

Richard E Overill and Jantje A M Silomon
*Department of Computer Science, King's College London, Strand, London WC2R 2LS, UK*
{richard.overill | jantje.a.silomon}(at)kcl.ac.uk

**Abstract**

We review, analyse and evaluate recent developments in two related areas of digital forensics. The first involves quantifying the extent to which the recovered digital evidential traces support the prosecution's contention that a particular digital crime has been committed. The second addresses the issue of quantifying the cost-effectiveness of the digital forensic investigative process, in order to optimise the deployment of valuable and scarce resources for maximum efficacy.

**Keywords:** conditional probability; Bayesian network; likelihood ratio; odds ratio; complexity; cost-effectiveness; return on investment; cost-benefit ratio; forensic triage**.**

# An Investigation into Forensic Analysis of Deniably Encrypted Drives

Ellen Moar[1], Andrew Wakelin[2]
Computing and Engineering Systems, University of Abertay Dundee
Bell St, Dundee, DD1 1HG
[1]e.moar@abertay.ac.uk
[2]a.wakelin@abertay.ac.uk

**Abstract**

Deniable encryption in this context refers to the ability to surrender keys to decoy data, and the forensic examiner being unable to prove the existence of any other encrypted data. Two main types of deniable encryption have been investigated: hidden volumes and hidden operating systems. Hidden volumes are hidden containers inside non-hidden encrypted containers. The user can surrender the key to the outer container with the hope that the hidden container will not be found. Hidden operating systems hide an entire operating system inside a non-hidden container; again key surrender is made in the hope that only the files in the outer container will be discovered.

For the forensic examiner, this creates a problem. How can we determine whether a hidden volume or a hidden operating system is in use? This investigation looks at the ways in which a forensic examiner can potentially determine that a hidden volume or hidden operating system is installed on the system, including looking for clues left behind by the operating system and applications, brute force tactics, and examining network data. Guidelines for avoiding the detection of deniably encrypted drives are also discussed for a user who wishes to foil such a forensic investigation.

# Assessing Cryptology

David Bennett
Canterbury Christ Church University
North Holmes Road
Canterbury, Kent CT1 1QU, UK
david.bennett@canterbury.ac.uk

**Abstract**

The assessment of cryptology can be seen as somewhat different to other areas of Computing. It is often taught as a technical subject – with a focus on how individual algorithms and protocols work. Whereas it is reasonable to expect undergraduate students to write novel computer programs, or even develop novel computer programming languages it is unreasonable to expect them to develop novel ciphers that are worthy of any merit. Such things are beyond the mathematical skills of them.

So what things can we ask students to perform as part of assignment, and what success have we had with them? The main summative assessment tools outside of examinations we have used are: working through a cipher/protocol or by hand, implementing a cipher on computer (DES in Excel Spreadsheets), researching and summarising technical cryptological information to different audiences (newspaper articles/posters), and critical evaluation of non-technical aspects of the area and designed protocols. We found that where we have two assessments per year the second assessment received significantly lower marks than the first ($F=3.632$, $df=4,82$, $p=0.009$). Futher analysis found that cutting the number of assignments to one would appear to put the marks were roughly equidistant between the previous years' first and second assessments. We discuss the differences between the original assignments when there were two and the single assignment used this year.

In the examinations we moved from a situation where we had a compulsory section and a section with options to one where we had only optional questions. By doing this we found there was a significant difference in the marks received by students, with all optional receiving much higher marks ($F=3.480$, $df=2,56$, $p=0.038$). We discuss a number of possible reasons for this.

We conclude by discussing the intended future assessment regimes for the undergraduate programme.

# Student Perception of On-line Lectures within a Blended Learning Environment for Security and Digital Forensics

Prof Bill Buchanan, Richard MacFarlane, and Robert Ludwiniak[1],
[1] School of Computing, Edinburgh Napier University
w.buchanan@napier.ac.uk, r.macfarlane@napier.ac.uk, r.ludwiniak@napier.ac.uk

**Abstract**

Educational institutions are increasingly moving towards enhancing learning through the use of integrated information technology. Blended, or augmented, learning, aims to support the traditional learning environment – where the instructor blends online learning with the traditional face-to-face teaching. This may take the form of centrally Managed Systems (LMS), for example, or Instructor-led content such as online video, quizzes and activities. This paper investigates student preferences within a Computer Security and Digital Forensics module, regarding the integration of lecture using narrative-plus-PowerPoint within a traditional educational infrastructure. It thus assesses student perceptions in the usage of on-line lectures for security and digital forensics material, with a specific focus on whether students actually prefer the on-line version to the traditional lecture situation, and on how they use the on-line lecture material.

# Cybercrime vs Cyber-War

Denis Edgar-Nevill
Canterbury Christ Church University

**Abstract**

The word 'Cyber' has been over used in recent years. In particular the notion of 'Cyber-War' has gained recognition and has become a focus for study and debate. But what is 'Cyber-War'? Are we over using the parallels between attacks on the Internet (which are happening with increasing frequency) and the physical reality of conventional war?

This presentation will consider how Cyber-War is beginning to make itself manifest and just how far the analogy with conventional war can reasonably be stretched. The types of attack which are being launched will be considered in the context of the wider notion of cybercrime. The organisations launching such attacks will be discussed, together with their motivation, resources and visibility and the extent to which this threat will constitute a problem.

The phases of a cyber-war will be discussed. In particular the preparation phase involving industrial espionage in the form of penetration testing, SQL injection and the production of malware. The attack phase itself will be discussed together with the defences put in place. An important consideration is the consequences of sustained cyber-warfare from its present levels to more overt attacks on the infrastructure of the Internet.

Understanding the severity of the problem is not easy for the typical Internet user. During the Beijing Olympics (an obvious potential target for cyber attacks) there were 15 million security threats recorded per day; almost 150 per second. Efforts to monitor the threat in real-time include building networks of security points on major Internet pipes and counting the threats as they pass by (e.g. Internet Barometer http://barometer.interoute.com/barom_main.php).

As individuals, for the most part, we consider such things are out there in cyberspace but not something which will have impact on our lives – other than perhaps causing the occasional inconvenience. The situation, if it is not to have a more dramatic consequence, must be in part owned by everyone. To paraphrase the famous quotation about Israeli citizens – every Internet citizen is a front line soldier in the cyber-war.

# A Low Cost Forensic Tool for Analyzing Huge Data Sets in Digital Investigations

Yasantha N Hettiarachchi[1], Kasun De Zoysa[2], Keerthi Goonatilake[3], George R S Weir[4]
[1]ynh@ucsc.cmb.ac.lk
[2]Kasun@ucsc.cmb.ac.lk
[3]Keerthi@ucsc.cmb.ac.lk
University of Colombo School of Computing, Colombo, Sri Lanka
[4]Department of Computer and Information Sciences, Livingstone Tower,
Glasgow G1 1XH Scotland,UK
George.weir@cis.strath.ac.uk

**Abstract**

Due to the recent advances in hard disk drive technologies, the storage capacity of computers continues to grow exponentially, while the costs of such devices remain to decline. This effect leads digital crime investigators to analyze even Tera-byte sized data sets and spending tremendous time and effort in forensic investigations. When handling with the large volumes of data most of the existing open source and commercial forensic tools available show poor performance. To handle with huge volumes of data it is wise to use a discipline like data mining. In this paper we propose a low cost framework and a set of guidelines which incorporates data mining techniques in criminal and intelligence analysis. It is capable of extracting only the important information from huge data sets, revealing the overall patterns of the data set and assisting direct computer forensic investigators to locate their points of interest. Moreover, it will classify data according to number of attributes found on the storage medium and group data items into classes with similar characteristics. This will speed-up the investigation process and reduces the time taken for a digital investigation. Also it will improve the quality of the information associated with the data analysis and release the investigator from most low level tasks that they currently have to do. Finally and most importantly this framework will reduce the huge monetary cost associated with the digital forensic investigation process.

# The exploit, the exploiter, the exploited…

Righard J. Zwienenberg,
Chief Research Officer,
Norman Data Defense Systems,
righard.zwienenberg@norman.com

**Abstract**

As long as there have been computer systems, vulnerabilities exist and have been exploited. There are people that have made it their business to find vulnerabilities and there are people that have made it their business to 'use' the vulnerabilities. And you have people that do both. And as well, their motives are as diverse. What kind of companies are keeping themselves busy looking for exploits, what kind of people are (mis)using them. What are they looking for, what are they after? The presentation will deal with this going back to the early nineties to very recent events. Will we ever resolve the problem of exploits, being the exploited? Or be the exploiter?

# A Virtualisation Based Forensic Computing Research Tool

Christopher Hargreaves[1] and Howard Chivers[2]
[1]c.j.hargreaves@cranfield.ac.uk
[2]h.chivers@cranfield.ac.uk
Centre for Forensic Computing,
Cranfield University, Shrivenham, UK

**Abstract**

One type of forensic computing research is the investigation of artefacts left by a particular application. This kind of research often involves monitoring test systems and investigating the changes made to them. Existing system monitoring techniques have limitations such as causing their own artefacts to be left on the system under test, being limited to certain operating systems, failing to preserve multiple states of the system for ease of comparison and missing changes made entirely. This paper investigates the extent to which these limitations can be overcome and develops a virtual machine based approach that involves making full duplicates of the disk image of the virtual machine before and after performing experiments. The analysis of this data is achieved using a Python based prototype tool, which can identify files created, deleted and modified between the ‘before’ and ‘after’ disk images. The tool is also extensible, for example it allows a Windows Registry plug-in to explore structural changes to the Registry hives. The main contribution is that the technique, through preserving the ‘before’ and ‘after’ disk images in full, means that not only are file system changes detectable, but the contents of files before and after can be inspected and compared to see *how* they were changed. This offers potential benefit over existing methods to both analysts and those engaged in digital forensics research.

# The Advantages and Risks of Live Data Collection

Ron Tasker
UB: 08013794
School of Computing Informatics and Media
University of Bradford
Bradford, UK
rtasker@bradford.ac.uk

**Abstract**

Live data collection at the scene of an incident has been a controversial subject since the inception of forensic computing as a science. Traditionally, incident response methodologies have favoured the immediate disconnection of power from running systems at the scene of an incident. This approach preserves time stamps. On the other hand, much valuable data, which is volatile in nature, may be lost by removing power from a suspect system immediately. Recently, many police forces have changed policy in favour of live data collection from running machines at the scene of a crime.

This paper will discuss some of the risks and benefits of live data collection at the scene of a crime, by using an example scenario. The example scenario will be used to synthesis the literature with direct application to practice.

**Keywords:** live data collection, acquisition, risks, advantages, practice issues

# Integrating Digital Forensics in a Crime Scene Investigation Exercise

Michael Jones[1], Alexandra Otto[2]
[1]School of Design, Engineering & Computing, Bournemouth University
[2]School of Applied Sciences, Bournemouth University

**Abstract**

Within a higher education environment there are considerable overheads in organising and conducting a Crime Scene Investigation (CSI) exercise. These include: selecting a suitable venue, populating it with appropriate 'evidence', training students, and monitoring student activity.

In a digital forensics investigation the context in which artefacts are gathered may be of less relevance than in other branches of forensics. It follows that there may be few obvious pedagogical benefits from creating and populating a crime scene with digital evidence. There may be other benefits that would help justify the investment of staff time. In order to evaluate this theory, digital artefacts were introduced into a CSI exercise organised for forensic science students. The 'scene' consisted of a number of locations, some of which contain samples of blood, hair, and other forensic evidence, including knives and guns. When the (non-digital) forensics students located a digital artefact in one of the locations, digital forensics students were called in. These students captured and swabbed the data under relevant supervision.

In a survey, all responding digital forensics students stated that they enjoyed their involvement in the exercise, and found that it helped to paint a more rounded picture of digital forensics. It was reported that the forensic science students commented favourably on the joint exercise. Further combined exercises are planned, involving a wider range of digital artefacts and capture techniques.

# Using Biometric Access Control for Forensic Identification: Benefit or Bind?

Lynne Norris-Jones
Senior Lecturer in Law for Information Systems, Department of Information Systems & International Studies
Cardiff School of Management, University of Wales Institute, Cardiff
lnorris@uwic.ac.uk

**Abstract**

The use of biometric data in forensic science dates back to the mid to late Nineteenth Century, applying scientific principles and technical methods to investigate the existence of a crime, determine the identification of the perpetrator and to establish their modus operandi (Dessimoz & Champod, 2008). More recently its impact has stemmed from the events of September 11th 2001, following which biometric access control within public places has been heightened leading to a new form of forensic identification. Despite its increasing necessity within safety critical areas, there is general recognition that social acceptance of biometrics is dependent on society's perception of its value to individuals weighed against perceived risks of intrusion and invasion of privacy.
This paper focuses on measures taken by manufacturers, suppliers and managers of biometric access control systems to implement procedures to address this dichotomy within working environments. The findings provide a practical insight into the major considerations in applying access control techniques in a variety of workplace environments and suggest a number of guidelines for achieving maximum social, legal and ethical acceptance from academic, manufacturing, supply and management perspectives.

**References**

[1] Bromby, M. (2002) To be taken at Face Value? Computerised Identification, Information & Communications Technology Law, Vol. 11 Issue 1

[2] Dessimoz, D. & Champod, C. (2008) Handbook of Biometrics, Springer, US

# An Enhanced Eigenfaces-based Biometric Forensic Model

Nasser S. Abouzakhar and Praneeth Enjamuri
School of Computer Science, The University of Hertfordshire,
College Lane, Hatfield AL 10 9AB, Hertfordshire, UK
{N.Abouzakhar, P.Enjamuri1}@herts.ac.uk

**Abstract**

The recent explosive development of the Internet allowed unwelcomed visitors to gain access to private information and various critical - mission resources such as financial institutions, hospitals, airports ... etc. Internet security has become a hot topic and relies on advanced technology. Now, more than ever, there is an increasing need for stronger identification mechanisms such as biometrics, which are in the process of replacing traditional identification solutions. Also, critical - mission systems and applications require mechanisms to detect when legitimate users try to misuse their privileges. Biometrics enables cybercrime forensics specialists to gather evidence whenever needed.

This paper aims to introduce a biometric forensic model using facial identification approach. This model is based on the Eigenfaces approach for recognition proposed by Turk and Pentland [1]. Here, an unknown input image is compared with a set of images stored in a database to identify the best match. A freely accessible faces database has been used to develop our model which is based on a mathematical approach, called Principle Component Analysis (PCA).

The paper addresses the issue of extracting global features of the images which are stored separately in the database. The features of a test image were compared with a set of images whose features were stored. The distance of the two images was calculated and when was minimum and below a certain threshold, the two images were considered to be the same and belong to a particular person. The calculated distance could be used and / or adjusted by a forensic specialist for deciding whether or not a suspicious user is actually the person who claims to be. The performance of the proposed face identification model was evaluated using standard methods. Distance values were used to express the similarity between any input image and other stored images. The model's performance was evaluated using FAR (False Acceptance Rate), FRR (False Rejection Rate) and EER (Equal Error Rate). In FAR, each user's image was compared with all images present in the database excluding the user's own image. In FRR, each user's image was compared with his own stored in the database. The major findings of the experiments showed promising and interesting results in terms of the model's performance and similarity measures.

# Towards Scientific Malware Analysis

Ian Kennedy
Centre for Research in Computing, The Open University,
Walton Hall, Milton Keynes MK7 6AA
I.M.Kennedy@open.ac.uk

**Abstract**

The emerging techniques in volatile memory acquisition and analysis are ideally suited to malware analysis. However, context based data such as the extraction of unpacked binaries, data allocated to hidden processes, identification of terminated processes are developments in need of quantifiable evaluation. A greater level of science in tool and process evaluation arises out of the move towards higher standards in the delivery of forensic science services.

In this paper, we propose a number of experiments to gather data that will allow derivation of a statistical measure of error for volatile memory acquisition. The design of these experiments takes into account the flux nature of volatile memory not only between acquisitions but also during the imaging process, and there applies piecewise hashing is applied to each of the files containing the RAM acquisitions to derive an error rate. Repeating the experiments for multiple tools and operating systems/patches will produce a more generalised error rate for the procedures alone.

It is intended that the proposed experiments will be offered to postgraduate students following the Open University's Computer Forensics and Investigations course (M889). Therefore, the paper also discusses the risks and challenges associated with teaching malware analysis techniques within a distance-learning setting. Also discussed are the challenges relating to the technical skills required to perform malware analysis. Programming, debugging, assembly language and obfuscation, for example, are tasks often outside the student's skill set.

For the student, the experiments demonstrate a quantifiable data gathering technique to inform decisions made regarding the validation of tools where reference data may be difficult or impossible to produce. Further to this, these experiments are an initial step to develop a methodology to quantifiably evaluate other processes and tools associated with malware analysis.

# Antivirus Testing and AMTSO: has anything changed?

David Harley BA CITP FBCS CISSP
Cyber Threat Analysis Center
ESET LLC, San Diego, CA 92101, US
david.harley@eset.com

**Abstract**

Since it was formally founded in May 2008, the Anti-Malware Testing Standards Organization has been through a number of changes and generated some serious documentation and significant press coverage. AMTSO was actually founded as the result of many years of concern, not to say rage on occasion, on the part of anti-malware vendors and mainstream product testers, at the low level of competence and accuracy demonstrated by so many of the individuals and organizations offering comparative testing and/or product certification.

The organization announced its intention of improving levels of objectivity, quality and relevance of anti-malware testing methodologies. Clearly that wasn't going to happen overnight, but how far along the road to better testing practice have we travelled?
This paper looks at testing as it was, as it is, and as AMTSO would like it to be. Is testing really so difficult? Is it appropriate for the vendors who make the products under test to be so involved in the process of defining good practice? In the process, core issues will be considered such as:

- Comparative testing versus certification
- Detection testing versus performance testing, and why it's rarely a good idea to mix the two
- Detection testing in a time of glut: when a virus lab may process tens or hundreds of thousands of unique binaries on a daily basis, prioritization is not a trivial issue. How big is the margin for error?
- Comparing apples to oranges: can you penalize an orange for not tasting like an apple?
- Default configuration and level playing fields
- Correct classification and selection of samples.
- Validation: is that sample really malicious, and how does a tester check?
- Static analysis and static testing: is there still a place for signatures and WildList testing?
- Is a good static test better than a bad dynamic test?
- The AMTSO fundamental principles of testing: do they help or hinder? Is standardization of testing even a good idea?

# Traffic Analysis, Anonymity, Freedom and Digital "Cat and Mouse" in Cyberspace: A Case Study of China vs Iran

Cameron J. Shahab
King's College London, University of London
London, United Kingdom
Reza Mousoli
Department of Computing, Canterbury Christ Church University
Canterbury, Kent, United Kingdom

**Abstract**

This paper aims to compare Chinese and Iranian cyberspace to highlight the excessive traffic analysis, surveillance, filtering and the resulting effects on anonymity and freedom of expression in the borderless society of the Internet. The paradoxical contrasts between these two different states provide much scope for analysis and discourse, particularly in light of recent media attention. As has been shown by the government crackdowns in the aftermath of the Iranian election of 2009, and China's recent dispute with Google, cyberspace is highly contested by government's seeking to harness digital economic and e-business benefits whilst restricting online dissent and political activism. Interdisciplinary by its very nature, this paper will investigate the ongoing 'cat and mouse' game between the authoritarian governments and how tools such as TOR, Mixminion, Incognito and Anonymizer are helping dissenters to hide their identity and stay anonymous. The multifaceted approach to the research consisted of semi-structured interviews with key actors, interviews with Iranian and Chinese citizens currently in the UK, focus groups and textual analysis of websites and blogs. This paper has shown the increase in traffic analysis and surveillance in both Iran and China. On the other hand, in this digital "cat and mouse" game, protesters persistently get their message out and access forbidden and filtered sites. The various tools used to bypass filters and restrictions have been outlined and briefly assessed, and the role of the new digital media landscape in shaping the political debates has been discussed. The Chinese government has been very successful in creating a society in which the state not only controls cyberspace for high e-commerce growth, but also uses it as a tool for reinforcing social control. From the interviews with Chinese citizens it was clear that although they were aware of the traffic analysis and filtering and surveillance, most were unconcerned, even considering it normal. In contrast, the Iranian citizens interviewed were extremely unhappy with the increasing trend towards surveillance, filtering and the limit on connection speed within Iran. The Iranian government has not been able to subtly enforce its control over cyberspace. Unlike China where there are large e-transaction activities and huge online commercial interests, Iran still rely heavily on traditional commerce (Bazaar) and lacks advanced IT infra structure, expertise and software tools for traffic analysis and filtering; instead they have relied on slowing the entire Internet or bringing the system to a halt completely to deter protesters.

**Keywords:** privacy, traffic analysis, anonymity, freedom, cyberspace, China, Iran, tor, mixminion, incognito, anonymizer, anonymous, surveillance, filtering, ethics, "Open Net Initiative", ONI, bbc Persian, voa, gooyanews, jingjing, chacha, panopticon, censorship, e-business, golden shield, Reporters Sans Frontiers, rsf

# Constantly Evolving Technological Challenges in Cybercrime Forensic Investigation

Abhaya Induruwa
Department of Computing,
Canterbury Christ Church University
Canterbury CT1 1QU, United Kingdom
abhaya.induruwa@canterbury.ac.uk

**Abstract**

Digital consumer electronic market rapidly evolves as consumers demand for more performance and features, and as every manufacturer tries to capture a share of this lucrative market. Digital forensic investigators constantly face challenges as the industry continues to innovate and produce consumer electronic devices that are more and more powerful, contain enhanced features with increased performance and capacities. Among the areas that are expected to throw the greatest challenges are constantly evolving Microsoft Windows operating systems, migration of the Internet to IPv6 protocol, Social engineering and social networking, increasing use of VoIP in IP telephony communication, smart mobile devices operating on a plethora of operating systems including Windows Mobile, Apple iOS, Symbian, etc, virtualisation and cloud computing.

This paper aims to serve as an overview of the state-of-the-art in digital forensic investigation and specifically concentrates on aspects of networks running IPv6, communication using Voice over IP (VoIP), smart mobile phones (BlackBerry, Apple iPhone), GPS navigation systems (TomTom) and games consoles (Xbox 360, Nintendo Wii and Sony PS3). The paper focuses on the recent developments of technologies, services and devices that today's digital forensic investigator should be aware of and provides an overview of products and processes based on contemporary work and material reported in the literature. The discussion on technical details are limited to a level that is essential for the understanding of the processes and tools but the paper provides adequate references to explore for further and more complete information on the topics treated. It is hoped that this should help the investigators to further develop their knowledge and skills.

# Invited Keynote Presentation

# Think Like a Hacker - An Ethical Hacker's View of Corporate Security

Peter Wood **FBCS CITP FIMIS MIEEE CISSP M.Inst.ISP**
CEO, First Base Technologies

**Abstract**

Sometimes it seems like the criminals will always have the upper hand. No matter what we do and how much we spend they still steal our data, our credit cards and even our identities. Why does this happen? It's because criminals know how to 'think outside the box' – to automatically look for the back door or the hidden weaknesses. It's time we learned how to build our defences on the same basis - to use our imagination as well as technology. To examine and test our systems, buildings and people as though we were a criminal, not the developer or the architect. Criminals use technical, physical and human attacks to achieve their goals - unless we understand these attack we will continue to be hacked. This presentation will show you how criminal hackers think and offer you ideas for defending against them effectively.

**Biography**

Peter is a world-renowned security evangelist, speaking at conferences and seminars on ethical hacking techniques and social engineering. He has appeared in documentaries for BBC television, provided commentary on security issues for TV and radio and written many articles on a variety of security topics. He has also been rated the British Computer Society's number one speaker.

Peter serves on the ISACA conference committee for the Information Security Management Conference and Network Security Conference in both the US and Europe, as well as speaking at both events.

Peter has worked in the electronics and computer industries since 1969. He founded First Base Technologies in May 1989 as a services-only consultancy, providing security testing and audit services to commercial and government clients. Peter has hands-on technical involvement in the firm on a daily basis, working in areas as diverse as penetration testing, social engineering and skills transfer.

Peter is a Fellow of the British Computer Society and a Chartered IT Professional. He is a member of the BCS Register of Security Specialists and a CISSP. He is also a member of ACM, IEEE, IISP, IMIS, ISACA, ISSA and Mensa.

## Presentation Abstracts – 3rd September 2010

# The Relationship between Digital Investigations and Reduction in Cybercrime

Alastair Irons
Department of Computing, Engineering and Technology,
University of Sunderland, Sunderland, SR6 0DD
alastair.irons@sunderland.ac.uk

**Abstract**

The purpose of this paper is to examine the relationship between the provision of digital investigations services provided by police forces and the attempt to reduce the amount of cybercrime in society. In the paper a case study exploring the digital investigations provision in the North East of England will be presented. In order to examine the relationship between the impact on society and the way cybercrime is tackled the paper will consider issues including the resolution of cybercrime cases, the priority placed on cybercrime cases (including measurement of crime, police resourcing and police funding), the concept of the "victimless" crime and the way the criminal justice system in England and Wales is used to manage cybercrime cases. In the papre the impact of cybercrime and hi-tech units being part of police forces (using police forces in the North East of England as a case study) is discussed. The paper concludes with suggestions on how society can be made safer through the prevention, identification, resolution and prioritisation of cybercrime in UK police forces and the criminal justice system in England and Wales.

# Detection of Information Compromise Committed by Malicious Insiders

Andrew Hawkins and Denis Edgar-Nevill
Metropolitan Police Service & Canterbury Christ Church University

**Abstract**

The major characteristic of the 'Information Age' is our ability to access information wherever and whenever we need it. This has brought numerous benefits to business, education and individuals, but is has also provided an opportunity for 'malicious insider' to misuse information systems for their own dishonest reasons. Information has become one of the most valuable assets that any organisation needs to protect, and surveys have shown that malicious insiders now pose a more direct threat to information assets that that posed by outsiders. Police corruption involving the misuse of information systems was firsts recognised by Her Majesty's Inspectorate of Constabulary in 1999. Other researchers have highlighted that the misuse of information systems has become the most prolific form of police malfeasance. Public and private organisations should recognise the threat posed to their information systems, and deploy measures to mitigate the harm that malicious insiders can cause. This research is intended to identify the types of misuse of police information systems that are currently taking place, and identify whether technology offers a means of detecting it.

# A comparative study of the structure and behaviour of the operating system thumbnail caches used in Kubuntu and Ubuntu (9.10 and 10.04)

Sarah Morris[1], Howard Chivers[2]
Centre for Forensic Computing,
Cranfield University, Shrivenham, SN6 8LA, UK
[1]S.L.Morris@cranfield.ac.uk
[2]H.Chivers@cranfield.ac.uk

**Abstract**

Browsing directories in thumbnail mode can assist the user in locating relevant documents quickly by providing a graphical representation of each file. Whilst thumbnail images can assist the user, they can be resource intensive to generate; therefore operating systems generally cache these images, along with associated metadata, to prevent unnecessary rendering. Thumbnail caches can provide a variety of information, including file paths and images of documents; however it is necessary to understand the user activity which resulted in the artefacts being created to understand their forensic significance.

This research used baseline versions of Ubuntu and Kubuntu (both versions 9.10 and 10.04) in virtual machines to determine the effects of a variety of user actions on the information stored in the thumbnail caches. A series of experiments were conducted to identify the structures used to store artefacts both in the thumbnail cache and any related file throughout the system, as well as determining the meaning of each artefact. Each experiment was performed on both operating systems and mimicked a variety of typical user behaviours, such as moving a file or accessing a USB stick.

Whilst both thumbnail caches implement the same structure for storing data, the user behaviour which leads to artefacts being stored in the thumbnail caches differs considerably between the two operating systems. Other information about user activity can be deduced from the thumbnail cache itself; for example, Kubuntu uses an RGB format for items cached without the directory being viewed and uses an RGBA format for standard record creation. This paper also identifies the user activity which led to artefacts being recovered and discusses the strengths and weaknesses of the thumbnail caches.

This research shows that similar artefacts from two closely related operating systems may nevertheless suggest different types of user activity, and hence have a different forensic significance.

# Developing a GUI interface to the MS Log Parser

Fahad Mir and Dimitris Tsaptsinos
Faculty of CISM, Kingston University,
Penhryn Road, Kingston Upon Thames, KT1 2EE
d.tsaptsinos@kingston.ac.uk

**Abstract**

Computer Administrators and computer forensic specialists often use different tools to extract data from different log files and based on that information, they create a link between those results. There are number of tools available nowadays but in this contribution we concentrate on the MS Log Parser that contains support for various log file formats including IIS, Windows Event Log, Windows File system, Windows registry. The Microsoft Log parser is a console based application and uses the Structured Query Language as the main language to extract data from log files. Although the Microsoft Log Parser is a powerful tool it still lacks an interactive Graphical User Interface to ease the use of the system by people who might not be experts in designing complex queries. During our background research the Lizard Log parser was identified but the user still must have the ability to write a query The main motive of this project, part of an MSc course, was to create a GUI application for the MS Log Parser with all the powerful features that log parser possesses as a console application but allowing a user without formal training on the query language to employ.

# Open Delegates Discussion: Cybercrime, Digital Forensics & the 'Cloud' (Ethics, Professional and Legal Issues)

Robet Dube
Roehampton University, London

**Abstract**

This Workshop/Discussion Group is aimed at exploring Ethical, Professional and Legal Issues surrounding Cybercrime and Digital Forensics with some reference to the 'Cloud'. Following on from the discussion last year, l am planning to look at the nature of cybercrime and its association with digital forensics and cloud computing.

This will be an Open Discussion driven by the delegates who attend on their understanding of Cybercrime, Digital Forensics and Cloud Computing
.
Delegates will be introduced to 'provisional working definitions' of cybercrime, Ethics, Digital Forensics, Cloud Computing, professional and legal issues related to Cybercrime. Delegates' views, ideas and inputs will be collated so as to inform further debates and research into an area that is going to be a 'hot potato' in the coming years.

The main focus of the Workshop/Discussion will be Cybercrime, Cloud Computing, Privacy, Human Rights, Statutory Rights and Civil Liberties, Religious, Cultural, Customary, Research, Policing, Terror, societal modelling, confidentiality, responsibility, values, democracy, integrity, Ethical Hacker? and any related Conspiracy Theories.

**Keywords:** Cybercrime, Cloud Computing, Ethics, Digital Forensic, computers, investigation, privacy, law, legal, policing, Human Rights, Rights, Culture, custom, terror, terrorism, society, conspiracy, trust, religion.

# SODDImy and the Trojan Defence

David Harley BA CITP FBCS CISSP
Senior Research Fellow, Cyber Threat Analysis Center, ESET, Email:
david.harley@eset.com

**Abstract**

SODDI is a familiar acronym among those working in cybercrime: it stands for Some Other Dude Did It. There's nothing novel about criminals claiming that some offence with which they are charged was someone else's responsibility, of course, whether it's the victim or some third party. In the specific area of child abuse, it can be difficult to untangle layers of denial [1, 2] but in recent years frequent use has been made of the Trojan Defence, [3] which might be tersely if loosely summarized as "it must have been a virus" (leaving aside for now the technical differences in malware classification). This attempt at a "Get Out of Jail Free" card is not confined to one type of crime (indeed, it's as likely to be heard in workplace disciplinary contexts as in courtrooms), but it is currently particularly associated with child-related offences, at least in popular perception. As always where child abuse is concerned, attempts to negotiate these murky legal waters have been hampered by a strong emotional undercurrent: debate has been polarized between those who believe that the SODDI defence is about as convincing as "the Internet ate my homework" [4], and those who fear that natural revulsion at paedophile activity and eagerness to prosecute those who practice it may lead to the conviction of innocent parties. In fact, as a general rule, the assertion that "malware installed itself, performed some illegal act, then removed itself leaving evidence of the activity behind but no trace of itself", while not technically impossible, is not particularly likely. But most modern malware is primarily a constantly changing delivery mechanism for attacks that themselves change ownership, target, and context according to market forces and the need to evade tracking by law-enforcement and other interested parties. [5]

Much has been made of the way in which the Julie Amero case was compromised not only by forensic flaws and inadequate preservation of the chain of evidence, but by the presence ineffective, obsolete security software. [6] Malware and anti-malware have evolved since then, but has forensic understanding of those evolutions increased correspondingly?

This paper will review the 2010 threatscape, considering some cases and scenarios that highlight some of the ways in which malicious software has impacted (or could impact in the future) on investigation, whether by law enforcement agencies or in the workplace. But it will also look at some of the psychosocial issues that may distort our ability to apply our understanding of those technologies appropriately in emotionally charged contexts.

The paper will be available after the conference presentation at http://www.eset.com/documentation/white-papers.

## References

[1] Murphy, W.D. (1990) Assessment and Modification of Cognitive Distortions in Sex Offenders, in "Handbook of Sexual Assault: Issues, Theories and the Treatment of the Offender".

[2] Mezey, G. et al. (1991) A Community Treatment Programme for Convicted Child Sex Offenders: A Preliminary Report. Journal of Forensic Psychiatry 1: 11-25.

[3] Haagman, D., & Ghavalas, B. (2005) Trojan Defence: a Forensic View. Available from: http://220.231.93.23:8000/collect/EN-digital/index/assoc/HASH815b.dir/1c(53).pdf (Accessed: 3rd July 2010).

[4] Liesik, G. (2009) Authorities Scoff at 'Child Porn Virus' Tale. Available from http://www.deseretnews.com/article/705343760/Authorities-scoff-at-child-porn-virus-tale.html (Accessed: 3rd July 2010).

[5] Harley, D. (2009) The Game of the Name: Malware Naming, Shape Shifters and Sympathetic Magic. Available from: http://www.eset.com/resources/white-papers/cfet2009naming.pdf (Accessed: 3rd July 2010)

[6] Phillips, D., Harley, J., & Harley, D. (2007) Education in Education. In "The AVIEN Malware Defense Guide for the Enterprise, ed. Harley (Syngress).

# Invited Keynote Presentation

# ACPO Good Practice Guide for Digital Evidence (Ver 5)

Steve Edwards
Police Central e-Crime Unit
Metropolitan Police Service

**Abstract**

An editorial panel is currently reviewing the ACPO Good Practice Guide for Computer-Based Electronic Evidence. The panel's remit is to update the content to ensure it is current and relevant, and to see if there is any area of digital forensics not included in the guide that would benefit from inclusion.

An online survey was conducted to gather views to inform decisions that the panel would make.

The workshop will explain the make-up of the board, the current situation of the review, and the survey results.

**Biography**

Steve has ten years service within the digital forensic law enforcement area. He worked as computer forensic investigator from 2000 to 2009 within the Digital Forensic Unit at the Serious Fraud Office in London during which time he was involved in the investigations of serious and complex frauds, and at one time was the head of that unit.

He is currently in the middle of a two secondment to the Police Central e-Crime Unit (PCeU) where he is working on a number of digital forensic projects including the Digital Forensic Triage Working Group and leading on the review of the ACPO guidelines for Computer/Digital Evidence. He is also involved in a MPS project to develop a harm scoring matrix for criminal activity.

The PCeU remit is to develop the mainstream cyber-crime capability of the Police Service across England, Wales and Northern Ireland, co-ordinating the law enforcement approach to all types of cyber-crime and providing an investigative capability for the most serious cyber crime incidents.

# Support for Paedophile Image Viewers

Clare Bracey & Denis Edgar-Nevill
Sussex Police & Canterbury Christ Church University

**Abstract**

Counsellors and psychologists have long since recognised that investigators can suffer from vicarious traumatisation or "compassion fatigue". There have been many studies in this area and there are recognisable symptoms.

Sussex Police are at the forefront in recognising the impact of exposure to these disturbing images on HTCU staff. They have introduced a welfare policy to ensure that the mental health of examiners is regularly reviewed. Many other Hi Tech Crime Units have no such policy and have not completed a risk assessment considering this potential problem. There are professionals who do not accept that the risk of harm to staff is high. For example the Thames Valley Police Force Medical Examiner has stated that, in his opinion, their Hi Tech Crime Investigators who view indecent images of children are categorised as low-risk of developing problems.

The Health and Safety Officer for Sussex Police completed a risk assessment for their Hi Tech Crime Examiners; which suggested they are high risk. As a result, in 2006 the Welfare Department devised, with the help of the HTCU supervisor and Detective Inspector, a welfare policy which provides support for Hi Tech Crime Investigators.

This study intends to consider if there is a potential impact on Hi Tech Crime Investigators viewing indecent images of children. Also whether this occurs in just one police force area or whether it is common across the UK. It will also consider how requirement for support may be satisfied.

# Social Networking Sites, Privacy and Personal Digital Security: A Case Study of Facebook and Bebo

Kate Andrade, Reza Mousoli
Computing Department
Canterbury Christ Church University
Canterbury, Kent, United Kingdom

**Abstract**

Facebook social networking site's traffic rating is ranked second in the world after Google with 776,492 sites linking in to its domain name. Bebo, another social networking site, ranked 712 with only 18,928 sites linking in to its site [1]. Privacy and security settings of both sites have been under intense scrutiny by the public as there have been cases of sensitive information such as date of birth, address, colour of hair, eye colour, likes/dislikes which has been compromised or have been utilised by criminals to commit crimes. A 17 year old girl was tragically murdered after she befriended a convicted double rapist posing as a teenage boy on Facebook. This highlights an urgent review of personal security, privacy issues, security education and security settings when using social networking sites like Facebook and Bebo.

This paper investigates users' security awareness and the dangers of posting vast amounts of personal data which is openly accessible to the public on these sites. We would also investigate how educating users could help to protect them from cyber criminals. In this research 150 people who had social networking accounts were surveyed from a wide range of age groups, including a local secondary school and students, to explore their attitudes to personal security and safety, along with their views on how training and education might improve security levels of social networking sites. The majority of the participants surveyed were aware of digital security issues and took good precautions to protect themselves online. However, the research found that a large number of 11 to 18 year olds still add unknown contacts, post sensitive details and would not be willing to read booklets or watch videos on privacy and online security. The research compared technological aspects of security mechanism and procedures built into Facebook and Bebo and how abuse reporting, safe default settings and user friendly interfaces could alert the users of misconduct and manage privacy and digital security effortlessly and effectively.

**Keywords:** Facebook, Bebo, privacy, security settings, computer security, computer forensic, education, protection, digital security, social networking site, abuse reporting

# A Digital Forensics Case Generator

Michael Jones
School of Design, Engineering & Computing, Bournemouth University
Talbot Campus, Fern Barrow, Poole
mwjones@bournemouth.ac.uk

**Abstract**

The creation of a digital artefact (image) for analysis by students is a time-consuming process. Items need to be selected, manipulated and aggregated in such a way that the analysis of the resulting image addresses the relevant learning outcomes and can be conducted in a reasonable (but not trivial) timeframe. The construction of the image also has to be cognisant of the software tools being used in the analysis – the sophistication of these will have a significant impact on the analytical processes and the time involved.

Using a single image in a learning environment presents two further challenges: students might collaborate and effectively subdivide the analysis. Secondly, inter-cohort communication (both within and between institutions) can limit the extent to which an image can be re-used.

A software framework and system has been developed to facilitate the creation of individual images of equivalent complexity. The system is organised in three phases: manipulation, population and rendition. In the manipulation phase, existing or created source documents are selected and than manipulated using one or more techniques. In the second phase a directory structure is created and populated both with the manipulated documents and a selection of others. The rendition process transcribes the populated structure onto the target media and then performs post-rendition processes, including deletion of files and manipulation of timestamps. The system is configurable, both in terms of the processes included, and the manner of their application.

The system has been used in the delivery of a second year unit in an undergraduate programme. Multiple images of varying complexity were created to support workshop exercises and assessment. In the case of all workshops and assessments, each student was supplied with a different image of equivalent complexity. The students informally reported that they found the analysis of these images to be a rewarding experience. The use of individual but overlapping images meant that students could support each other without compromising the sense of competition that naturally occurs within a student group.

The manipulations had to be cognisant of the availability (to students) of a range of software tools, including commercial digital forensics software. Where the commercial software was used, more obtuse manipulations were employed. Sample manipulations included the generation of contact data and triangulated GPS points, insertion of metadata, aggregation of files, encoding of generated data, encryption using passwords of varying robustness, and file renaming.

Consideration is given to further developments and to the use of the tool in future presentations of relevant units/modules.

# Using PFSense and Commodity Hardware as a Medium Interaction Honey-net

Georgios Chlapoutakis[1], Anastasios Laskos[2], Phillip J. Brooke[3], Mark Truran[4]
School of Computing, Teesside University, United Kingdom
[1]g.chlapoutakis@tees.ac.uk
[3]pjb@scm.tees.ac.uk
[4]m.a.truran@tees.ac.uk
School of Computing, University of Sunderland, United Kingdom
[2]bd74yy@student.sunderland.ac.uk

**Abstract**

*Honey-pots* and *honey-nets* are network-accessible decoy resources designed to attract unauthorized users, thereby deflecting their attention from security-critical systems. Combined with a process known as a LaBrea *tar pit*, honey-net and honey-pots can effectively entrap suspicious connection attempts and prevent the proliferation of further attacks via the host network. Use of these 'sticky' honey-pots and honey-nets is quite common within the network security community, and several 'off the shelf' solutions are available to individuals and commercial clients alike.

In this paper we describe a *LaBrea* tar-pit honey-net solution specifically designed for researchers interested in network security. Unlike the various honey net solutions mentioned above, this solution gives the user direct access to *raw, packet-level data*. Our reference implementation is built around a customized firewall distribution which acts as the *honey-net bridge*. This bridge uses an BSD-based firewall distribution known as *PFSense* in combination with a highly customizable network packet capturing facility called *tcpdump*.

The contribution of this work is twofold. Firstly, our reference implementation will enable researchers to quickly deploy a medium interaction honey-net network (with LaBrea Tar-pit functionality) that is more secure, more adaptable and more upgradeable than comparable systems. Secondly, our reference implementation will allow researchers to transparently gather raw, live-traffic data without the additional overhead of performing on-site traffic analysis. It is hoped that this will stimulate higher quality dataset collection throughout the network security field.

# A Chi-square Testing-based Intrusion Detection Model

Nasser S. Abouzakhar and Abu Bakar
School of Computer Science, The University of Hertfordshire,
College Lane, Hatfield AL10 9AB, Hertfordshire, UK
{N.Abouzakhar, A.Bakar}@herts.ac.uk

**Abstract**

The rapid growth of Internet malicious activities has become a major concern to network forensics and security community. With the increasing use of IT technologies for managing information there is a need for stronger intrusion detection mechanisms. Critical - mission systems and applications require mechanisms able to detect any unauthorised activities. An Intrusion Detection System (IDS) acts as a necessary element for monitoring traffic packets on computer networks, performs analysis to suspicious traffic and makes vital decisions. IDSs allow cybercrime forensic specialists to gather useful evidence whenever needed. This paper presents the design and development process of a Network Intrusion Detection System (NIDS) solution, which aims at providing an effective anomaly based detection model using Chi-Square statistics. One of the design objectives in this paper is to minimise the limitations of current statistical network forensics and intrusion detection. Throughout the development process of this statistical detection model several aspects of the process of building an effective detection model are emphasized. These aspects include dataset pre - processing and feature selection, network traffic analysis, statistical testing and detection model development. The calculated / output statistical figures of this model are based on certain threshold values which could be used and / or adjusted by a forensic specialist for deciding whether or not a suspicious event took place.

The modelling and development process of this proposed anomaly detection has been achieved using various software and development tools. In this paper we focus on modelling dynamic anomaly detection using the Chi-square technique. It investigates a network traffic dataset collected by CAIDA in 2008 that contains signs for denial of service (DoS) attacks called backscatter. The normal dataset patterns are analysed to build a profile for the legitimate network traffic. Any deviations from these normal profiles will be considered anomalous. The dataset was pre - processed using Wireshark and T-Shark, the detection model was developed using MATLAB for different variants of denial of services attacks and promising results were achieved.

# Machine Learning based Spam Filtering: Advantages and Challenges

Man Qi
Department of Computing
Canterbury Christ Church University
Canterbury, UK
man.qi@canterbury.ac.uk

**Abstract**

The application of machine learning techniques for spam filtering has become increasingly popular. These approaches do not depend on any pre-defined rule-sets analogous with non-machine learning counterparts. Two principal approaches are used, namely supervised and un-supervised. The former depends on an initial training set to assert classification[1], whilst the latter does not, but rather employs other techniques such as clustering to achieve its objectives.

Identifying features of a message which have the qualities to indicate whether it is spam is a critical task for machine learning approaches. This includes, where applicable, a number of pre-processing tasks such as lexical analysis and dimensionality reduction, in the form of stemming, cleansing and normalization i.e. consideration for specific qualities, removal of common words etc. etc., which are intended to help better identify and amplify the importance of more relevant features[2]. Features can take the form of words, combination of words and phrases etc. etc. Generally speaking, fewer features normally represent greater generalization and better performance, however this mostly at the expense of not being able to obtain the required class separation, i.e. the identification of the optimal separating level between the classes (spam / ham) and thus minimize or remove entropy. Various schemes intended to identify the best features in terms of quality and number. Feature vectors are typically associated with weights that are intended to influence the outcome of the classification. Popular weighting schemes include term frequency (TF), binary representation and TF-IDF – term frequency inverse document Frequency [3].

Beside the definition of the respective feature vectors and subsequent creation of the training set, there is also the actual classification algorithm itself that needs to be considered. There are numerous algorithms in this respect and that are in widespread use in this context. These include Decision Trees [4], Bayesian classifiers[5][6][7][8], k Nearest Neighbor (kNN), Artificial Neural Networks (ANN) and Support Vector Machines (SVM) [9][10].

Even though these approaches use specialized features, there is a simple, yet crucial fact that both spam and ham could share the same features. Using linguistic features for filtering could increase the overall detection rate. A context sensitive warning generation mechanism is also helpful to educate users about the consequences of spam. But a generic and scalable solution is still a challenge. For spam encoded as an image is difficult to extract the necessary textual and structural features. Therefore, other characteristics are needed to be addressed such as the layout and behaviour of the linked-to websites (e.g. in phishing emails). Evaluation of the various machine learning based techniques is also a great challenge for spam filtering.

## References

[1] Lim, T. Loh, W. and Shih, Y. An Empirical Comparison of Decision Trees and Other Classification Methods, (1998).

[2] Sebastiani, F. and Ricerche, D. Machine Learning in Automated Text Categorization, ACM Computing Surveys, vol. 34(2002), pp. 1–47.

[3] Salton, G. and Buckley, C. Term-weighting approaches in automatic text retrieval Information Processing and Management, (1988), pp. 513–523.

[4] Quinlan, J. R..Induction of Decision Trees. Mach. Learn. 1, 1 (Mar. 1986), 81-106. (1986) [Online] Available at http://www.cs.toronto.edu%2F~roweis%2Fcsc2515-2006%2Freadings%2Fquinlan.pdf (Accessed on 7/10/2009)

[5] Chen, C. Tian, Y. and Zhang, C. Spam Filtering with Several Novel Bayesian Classifiers 19TH International Conference on Pattern Recognition, VOLS 1-6, 345 E 47TH ST, NEW YORK, NY 10017 USA: IEEE, (2008), pp. 1897-1900.

[6] Khorsi, A. An Overview of Content-Based Spam Filtering Techniques. Informatica (Slovenia), vol. 31, (2007), pp. 269-277.

[7] Song, Y. Kolcz, A. and Giles, C.L. Better Naive Bayes classification for high-precision spam detection Software-Practice & Experience, vol. 39, Aug. (2009), pp. 1003-1024.

[8] Ye, M. Tao, T. Mai, F. and Cheng, X. An spam discrimination based on mail header feature and SVM 2008 4th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM), Piscataway, NJ, USA: (2008), pp. 1-4

[9] Yang, Z. Nie, X. Xu, W. and Guo, J. An approach to spam detection by naive Bayes ensemble based on decision induction 2006 6th International Conference on Intelligent Systems Design and Applications, Los Alamitos, CA, USA: (2006), pp. 861-866

[10] Blanco, A. Ricket, A.M and M. Combining SVM classifiers for email anti-spam filtering Computational and Ambient Intelligence. Proceedings 9th International Work-Conference on Artificial Neural Networks, IWANN 2007, Berlin, Germany: (2007), pp. 903 - 910.

# A Model to Support the Authentication of Mobile Transaction

Xuan Huang
School of Computing and Engineering Systems
University of Abertay Dundee
The kydd building, Dundee DD1 1HG, UK
X.Huang@abertay.ac.uk

**Abstract**

With the development of mobile communication, user authentication and access control are becoming the most important aspects of mobile security. The mobile personal identification is critical in a wide range of application domains, and the biometrics is inherently more reliable and more capable than traditional methods in differentiating between an authorised person and an impostor. The traditional method to implement identity authentication and access control is achieved through an API (Application Programming Interface) between the identity authentication and access control service provider and an application. The security and practicability of these methods can not satisfy the development of network and its applications. This paper presents an experimental study and proposes a smart, biometric-based user authentication system for mobile devices; the objective of this research is to achieving a composite authentication mechanism and design a biometric-based authentication system which is capable of achieving mobile authentication. The proposed intelligent authentication mechanism defined four different alert levels in the system according to user's requirements, each level corresponding to different authentication methods: direct access, pin, password and biometrics; On the other extreme, in a mobile security application, the facial, voice and typing behaviour recognition are the three preferred techniques to achieve biometric authentication. According to this mechanism, the intelligent authentication system not only improve systematical safety, but also more convenient for the user, mobile passport, mobile identity card and mobile transaction will come true.

# Problems with Prosecuting Computer Crimes

Karl Obayi
Solicitor & Advocate
Digital Forensics Attorney
iTevidence, Mitcham Surrey CR4 3FH
kobayi@itevidence.co.uk
www.itevidence.co.uk

**Abstract**

This paper seeks to examine the myriad of problems associated with prosecuting computer crimes from the perspective of a Defence Attorney. These identified problems will indeed form the pedestal for the attack and opposition to the use of computer evidence in a legal setting.

It starts with the position, that the successful prosecution of computer crime is fraught with – procedural, structural, legal and lack of relevant expertise. The paper will examine the legal environment in which computer evidence is identified, extracted, analysed, reviewed and presented with the aim of identifying the legal pitfalls that awaits the forensic investigator at each stage of the investigation.

On the structural heading, it will examine the extant make up of our evidential rules on the admissibility and probative value that can be attached to digital evidence and the possible strategic use of the procedural rules to diminish the probative value of digital evidence.

It will address the international effort at coordination with respect to the use of computer evidence against the background of the several complications that may arise through the strategic use of conflict of laws to defeat and complicate the use of computer evidence.

The current practices of forensic investigators in the field or in the laboratory will be analysed with a view to highlighting the dangers associated with forensic lab. Practices and the pitfalls associated with tunnel vision investigation tactics.

In conclusion the paper will aim to alert digital forensic practitioners to the fact that digital crime investigation and subsequent prosecution may lead to the discovery of a smoking bomb. However, that smoking bomb may not just be for the benefit of the prosecution it may actually lead to the benefit and acquittal of the defendant if and when a strategic defence is mounted against the life circle of digital evidence in any given case.

# Criteria for Successful MSc Research Projects in Computer Forensics

Paul Douglas (P.Douglas@wmin.ac.uk)
Colin Myers (colin@wmin.ac.uk)
University of Westminster

**Abstract**

This paper discusses factors that make a successful research-orientated project in computer forensics at MSc level. We briefly outline the University of Westminster MSc Computer Forensics programme and the role of the project within that context.

We consider the general nature of projects undertaken by students over the years the course has been running (it is just completing its third full year) and address the specific issue of why projects that are research-orientated tend to be either very successful or very unsuccessful, whereas more traditional (i.e., primarily practical) projects achieve the distribution of marks and levels of success that would normally be expected from a student cohort of this size and diversity.

We divide our discussion into two principal areas.

Firstly, we look at the sort of research skills that we generally find in our students. These come from diverse backgrounds: some are recent graduates; some graduated up to twenty years ago; some have never been to University before. Are there significant differences in the capabilities of each group? Perhaps surprisingly, we have found that there are not, and that all of the groups tend to lack some (possibly many) of the skills needed to successfully undertake research. This brings us to the question of how we teach them.

The University runs many different "Research Methods" courses, varying quite widely in nature and content. We give an overview of some of these, and try to identify which have been more successful and why.

Secondly, we look at the nature of the projects themselves, and address the question of what sort of project is likely to succeed, and to what extent it is the precise nature of the project rather than the preliminary skills of the student that is most influential in determining its ultimate degree of success. We find that one of the major factors is the initial scoping of the project, and that this is something that even those students who start with above average research skills usually find difficult. Many students choose a topic that is simply far too broad, and it can sometimes be difficult to convince them that this is the case. All too often this leads to the student finding a bewildering array of material that makes it impossible to adequately focus their research. This is a far more common problem than choosing a topic that is too narrow.

Finally, we give an overview of the assessment criteria we use for the projects, and a brief survey of some of our more successful research projects in which we consider how closely they conformed to the suggestions we make for success in a research project at this level.

# The Use of Digital Forensic Case Studies for Teaching and Assessment

Harjinder Singh Lallie
School of Computing, University of Derby, Kedleston Road, Derby DE22 1GB
h.s.lallie@derby.ac.uk

**Abstract**

This study analyses the use and development of Digital Forensic case studies for the purpose of teaching and assessing Digital Forensics students and practitioners. Within this study, case studies are categorised and a number of available case studies are explored. The importance of evidentiary and non-evidentiary artefacts within the case study are examined. Mechanisms for integrating case study development and/or investigation with student assessment are proposed, the benefits and the challenges of this approach are examined. Practical and technical issues involved in the development of case studies are examined. The study concludes by proposing guidelines for the development of Digital Forensic case studies.

# Engaging Students into Digital Forensics and Cybercrime with Challenging, Ever-changing and Stimulating Environments

Prof Bill Buchanan, Richard MacFarlane, Robert Ludwiniak, Dr Jamie Graves and Dr Gordon Russell, School of Computing, Edinburgh Napier University

**Abstract**

This paper aims presents a novel and engaging teaching infrastructure using an environment which is built around small snippets of lectures followed by ever-changing challenges, and which has a strong story narrative. The material has been developed over three years in or-der to engage schoolchildren into computing, and covers some key principles within digital forensics and Cybercrime, in order to solve crime. The material is integrated into a fast-paced, one hour session with 11 challenges covering some key principles such as for: ASCII coding; Caesar Codes; Shifted Alphabet codes; Pigpen Coding; Differing Encoding Meth-ods (Base64, Hex and Binary); Hidden Content within Files (using binary reading of the file); Directory Searching Hash Codes; Dictionary Searching Cipertext; and in finding Cov-ert Messages.

The objective of environment given to the students is to solve a series of challenges in order to find: Who did it? Where it was? Why they did it? When did they do it? and so on. Each time it is run the environment creates a new set of the investigation parameters, and all of the challenges are based around these. For example, if the student where to run the envi-ronment, and the crime was done by Fred Smith, the shifted alphabet code might be: UGTS HBXIW (which is a 15 letter shift), and they must then use a shifted alphabet calculator to find the number of shifts required, and thus the message. There is thus randomisation within the solving of a challenge, and which cannot be solved easily by running the challenge over consecutive time intervals, or from the answers from other students.

The environment uses current state-of-the-art graphical presentation methods such as Mi-crosoft .NET Page Flicking technology to generate the material which the student searches for clues. This includes generating a unique page flicking book which contains the codes which are used to contain the code that they are trying to break. For example, with a mes-sage which is presented in Base64 encoding, a page flicking book is automatically generated with a graphic within the book which contains the Base64 code that they are looking for. Thus Edinburgh (for the place) would appear in the book as RWRpbmJ1cmdo. The students then use the Encoding calculator to determine the mapping between Base64 and the plaintext equivalent. The environment also uses Microsoft .NET Deep Zoom tech-nology, so that students can zoom-in and zoom-out of a document in order to find hidden covert messages. This uses the Deep Zoom Composer package to create different levels of abstraction of an image, where students can zoom-in to identify changes in font, in the lay-out of the text, and so on.

The main environment splits into three main presentation areas: investigation parameters (where the student enters the things they have found out about the investigation); the main investigation area (where students zoom-in to find their challenges); and a toolkit (which contains the main computing calculators and tools that they will use to solve the chal-2 lenges). Deep Zoom is also used to allow students to move around and find the challenges, and investigate the material around the investigation.

# Educating Digital Forensic Investigators at Newport

Stilianos Vidalis[1], Eric Llewellyn[2], Olga Angelopoulou[3]
[1, 2] Centre for Information Operations
University of Wales, Newport
stilianos.vidalis@newport.ac.uk
eric.llewellyn@newport.ac.uk
[3]Information Security Research Group
University of Glamorgan
oangelop@glam.ac.uk

**Abstract**

Digital forensics is a multi-disciplinary applied science governed by strict and rigorous rules and regulations. Individuals pursuing a career in this discipline are required to have an interdisciplinary background drawing elements of practical experience from fields as varied as sociology, psychology, forensic science, computing and the law. Despite the above, there is no professional body or QA benchmarks that specifically govern education in this science. The subject area has proved popular and where the profession has traditionally been limited to a select circle of individuals from specific industry sectors, it is now open to all. To meet this demand, many product vendors and Higher Education establishments have developed programmes ranging from short training courses to full undergraduate and postgraduate degree programmes. All these educational offerings promote the fact that individuals will be trained to an appropriate level, however without clear benchmark or regulatory guidance, students face the risk of being ill-equipped for the challenges presented in industry. The challenge faced by educators is to train individuals, many of whom have no prior theoretical or practical experience in the aforementioned fields, to become digital forensic investigators. This paper discusses the approach used at the University of Wales, Newport to overcome this challenge. It demonstrates how industry requirements have influenced and shaped the learning styles adopted by the teaching team in order to produce high calibre graduates that are ready to engage in a career in digital forensics.

## Sponsor - Canterbury Christ Church University

The Department of Computing plays host to the CFET 2010 conference based at the North Holmes Road Campus of Canterbury Christ Church University.

The Department comprises of 12 full-time and 5 part-time staff running undergraduate an postgraduate courses for 300 students. The Department is centred in the Invicta Building of the North Holmes Road Campus which includes four purpose built computer laboratories with over 100 workstations.

The Department developed the MSc Cybercrime Forensics in 2004 which is jointly validated with the NPIA (National Policing Improvement Agency). This award is currently offered to serving police officers, members of High Tech Crime Units in the UK and other Home Office officials. In July 2007 the Department added an undergraduate award the BSc Forensic Computing to its course portfolio offered from September 2007.

In 2008 as a result of CFET 2008 Denis Edgar-Nevill (Head of Department) was invited to propose the creation of the BCS Cybercrime Forensics Specialist Group which held its inaugural meeting at the University in December 2008.

The Department is pleased to welcome The Carphone Warehouse as a new sponsor and its support for work in the area of mobile phone forensics.

## Sponsor – National Policing Improvement Agency

The NPIA (formally CENTREX prior to 2007) provide specialist training and support to the 43 national police forces in the UK. NPIA will support the police service by providing expertise in areas as diverse as information and communications technology, support to information and intelligence sharing, core police processes, managing change and recruiting, developing and deploying people.

Their task is to help the police service take forward their priorities, working closely with the professional leadership of the programmes and services they are responsible for. In close co-ordination with our partners, ACPO, APA and the Home Office their role is to help face the challenging and demanding needs of policing in the 21st century.

# Sponsor – Justice Institute of British Columbia, Canada

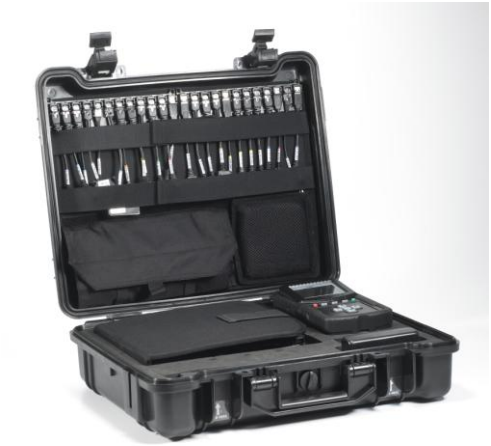
JUSTICE INSTITUTE of BRITISH COLUMBIA

Provincial post-secondary institute, founded under College & Institute Act, for Justice & Public Safety education in 1978, by Dr. Patrick McGeer, Minister of Education. Its mission is to provide Innovative education and training for those who make communities safe. Its vision is to be a world leader in education, training and the development of professional standards of practice in justice, public safety and human services. Offerings include programs ranging from basic training to Bachelor degree programs. When it was founded in 1978 2,000 students were trained. Today, student numbers are over 30,000 annually, with more than 6,000 students in online programs. Instructors are in more than 190 communities in British Columbia delivering programs. In 2005/06, 6,249 organizations chose the Justice Institute of BC for training, education, and research needs in justice & public safety training.

# Sponsor – Cellbrite

**About Cellebrite**

Founded in 1999 by a team of highly experienced telecom and mobile telephony professionals, Cellebrite is a global company known for its technological breakthroughs in the cellular and forensics industries.
The pioneers in mobile phone to phone content transfer, today Cellebrite provides a complete range of solutions for the mobile retail industry, from stand-alone content transfer at the Point of Sale (POS) to Over-the-Air (OTA) mobile applications for subscriber content management.
With proven ability to impact sales of phones, upgrades, and services, Cellebrite customers include the world's largest mobile operators and deployments by more than 140 major carriers.
Building on its expertise in mobile data technology, in 2007, Cellebrite introduced a new line of products targeted to the mobile forensics industry.
Using next-generation extraction methods and analysis techniques, Cellebrite's Universal Forensic Extraction Device (UFED) is able to extract and analyze data from more than 3,000 phones and mobile devices, including smartphones, mass storage devices and GPS systems.
In use by military, law enforcement, governments, and intelligence agencies across the world, Cellebrite's UFED is the tool of choice for thousands of forensic specialists in police, Special Forces, tax fraud, customs, border control, and anti-terrorist investigations in more than 60 countries. From more info: **www.cellebrite.com**

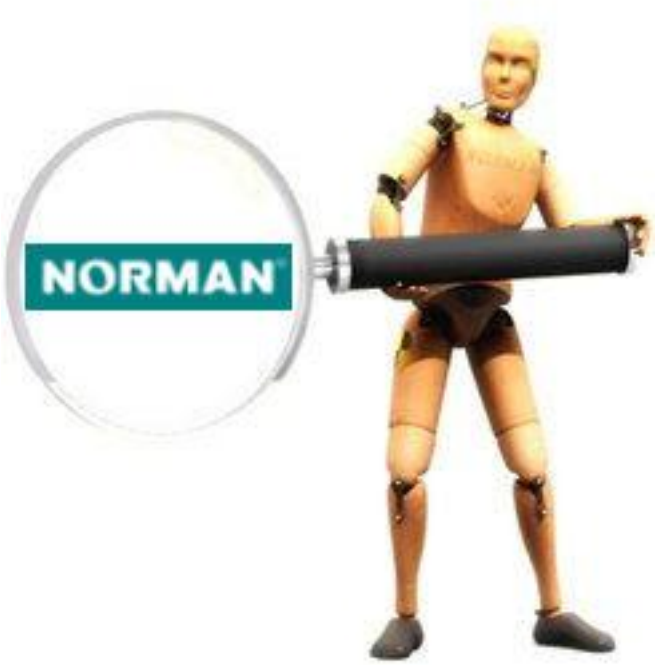



**Ruggedized kit**

## Sponsor – Norman Data Defense Systems

Norman is one of the world's leading companies within the field of data security. With products for antivirus (virus control), personal firewall, anti-spam, and encryption, the company plays an important role in the data industry. Norman's products are focused on secure computing.

Products from Norman are available for both home users who want to surf the Internet and large corporations. And everyone in between.

## Sponsor – RTL

Modern day crime requires modern day policing and the increase of cyber crime means that police forces across the world need to be armed with the latest mobile forensic technology. Radio Tactics and its range of forensic solutions are equipped for this very occurrence.

Interaction with the community and crime deterrents remain hugely important parts of modern day local policing. In an effort to reduce and tackle every day crime, Radio Tactics has created a range of product solutions that offer the police everything from complete forensic analysis kits for the custody suites to truly portable devices ideal for on the street policing.

## Sponsor – MicroSystemation

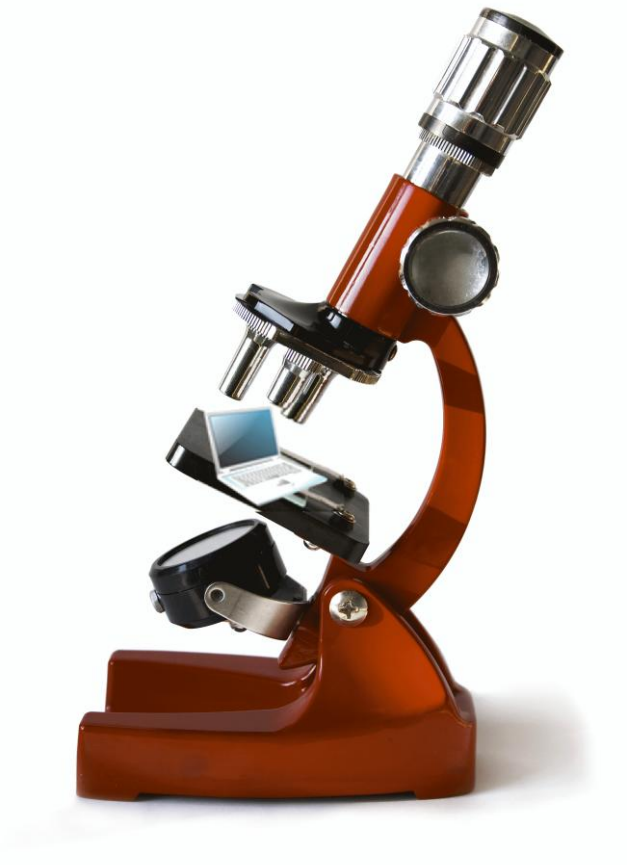

Micro Systemation solely develops mobile forensic products for forensics professionals. We aim to offer you an efficient, easy-to-use, easy to administer, secure cell phone forensic work tool – that sticks in court! We want to develop our mobile forensic systems in close cooperation with our customers – for the most professional input possible. We produce our own hardware and mobile forensic cables to ensure highest possible quality. Finally, we give you a skilled support that is efficient, helpful – and they will not give up until your problem is solved**.**

## Sponsor – British Computer Society
## Cybercrime Forensics Specialist Group

Established in 2008, the SG now has over 1100 members in the UK and beyond.

**Aim**

"Promoting Cybercrime Forensics and the use of Cybercrime Forensics; of relevance to computing professionals, lawyers, law enforcement officers, academics and those interested in the use of Cybercrime Forensics and the need to address cybercrime for the benefit of those groups and of the wider public."



# Delegates List

(as of 15th August 2010)

| Surname | First Name | Organisation | Country |
|---|---|---|---|
| Abouzakhar | Nasser | University of Hertfordshire | UK |
| Addrade | Kate | GCHQ Cheltenham | UK |
| Askwith | Bob | Liverpool John Moores University | UK |
| Baig | Mirza | | UK |
| Bates | Danny | Metropolitan Police Service | UK |
| Bennett | David | Canterbury Christ Church University | UK |
| Biggs | Stephen | University of Wales, Newport | UK |
| Buchanan | Bill | Napier University | UK |
| Campbell | Jacueline | Leeds Metropolitan University | UK |
| Case | Nikki | Norman Data Defense Systems | UK |
| Chlapoutakis | Georgios | University of Teesside | UK |
| Dickinson | Mike | Micro Systemation AB | UK |
| Douglas | Paul | University of Westminster | UK |
| Dube | Robet | Roehampton University | UK |
| Edgar-Nevill | Denis | Canterbury Christ Church University | UK |
| Edgar-Nevill | Val | Canterbury Christ Church University | UK |
| Edwards | Steve | PCeU | UK |
| Elvey | Mary | Canterbury Christ Church University | UK |
| Elvey | Thomas | Canterbury Christ Church University | UK |
| Ferguson | Ian | University of Abertay | UK |
| Goo | Swee Keow | University of Abertay | UK |
| Goonetillake | Keerthi | University of Colombo | Sri Lanka |
| Harley | David | ESET/AMTSO | USA |
| Hargreaves | Christopher | Cranfield University | UK |
| Harris | Douglas | University of Texas at Dallas | USA |
| Hawkins | Andrew | Metropolitan Police Service | UK |
| Huang | Xuan | University of Abertay Dundee | UK |
| Induruwa | Abhaya | Canterbury Christ Church University | UK |
| Irons | Alastair | University of Sunderland | UK |
| Jan | Philippe | Lancaster University | UK |
| Johnson | Joel | UWN | UK |
| Jones | Michael | Bournemouth University | UK |
| Jones | Nigel | University College Dublin | Ireland |
| Kennedy | Ian | The Open University | UK |
| Komisarczuk | Peter | Thames Valley University | NZ |
| Lallie | Harjinder Singh | University of Derby | UK |
| Lazarevski | Sanela | Leeds Metropolitan University | UK |
| Llewellyn | Eric | University of Wales, Newport | UK |
| Lutchinsky | Adi | Cellbrite | Israel |

| | | | |
|---|---|---|---|
| MacFarlane | R | Napier University | UK |
| Mansoorii | Jassim | Southampton Solent University | UK |
| Marsh | Steve | University of Wales Institute | UK |
| Moar | Ellen | University of Abertay | UK |
| Moffat | Callum | Canterbury Christ Church University | UK |
| Morgan-Busher | Melody | BCS CFSG Prize Winner | UK |
| Morris | Sarah | Cranfield University | UK |
| Mousoli | Reza | Canterbury Christ Church University | UK |
| Norris-Jones | Lynne | University of Wales Institute | UK |
| Obayi | Karl | iTevidence | UK |
| Overill | Richard | Kings College London | UK |
| Price | Dan | Lancaster University | uk |
| Qi | Man | Canterbury Christ Church University | UK |
| Quay-Ross | Adam | Canterbury Christ Church University | UK |
| Rennison | Andrew | UK Forensics Regulator | UK |
| Ross | Margaret | Southampton Solent University | UK |
| Shahab | Cameron | Kings College London | UK |
| Stahl | Bernd | Demontfort University | UK |
| Stephens | Paul | Canterbury Christ Church University | UK |
| Sutcliffe | Shaun | Micro Systemation AB | Sweden |
| Tasker | Ron | University of Bradford | UK |
| Thorne | Tim | Metropolitan Police Service | UK |
| Toon | Ian | Metropolitan Police | UK |
| Tubby | Matthew | Canterbury Christ Church University | UK |
| Uhomoibhi | James | University of Ulster | UK |
| Vered | Arie | Cellbrite | Israel |
| Vidalis | Stilianos | University of Wales, Newport | UK |

## Copyright Statement