CFET 2009 Index

CFET 2009

3rd 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
1st & 2nd September 2009

ISBN 978-1-899253-44-9

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).

In December 2008 the BCS Cybercrime Forensics Specialist Group was formed. We are very pleased to welcome the BCS and the SG as new sponsors of the CFET conferences.

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

Denis Edgar-Nevill
Chair, CFET 2009

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

Brian Brighouse Canterbury Christ Church University
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

Dr. Joe Carthy University College Dublin, Republic of Ireland

Professor Peter Cooper Dept 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

Dr Manolya Kavakli Department of Computing, Macquarie University, Australia

Gary C. Kessler Director Center for Digital Investigation Info.Security, Champlain College, USA

Jack McGee President, Justice Institute of British Columbia, Canada

Rob Risen Police Academy of the Netherlands

Professor Sujeet Shonoi University of Tulsa, USA

Professor Rongsheng Xu Chief Scientist, Nat. Comp. Network Intrusion Protection Center, China

Dr Craig Valli Head, School of Computer & Info. Science, Edith Cowan Univ., Australia

CFET 2009 Conference Schedule

Day 1 –1st September 2009

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

10.30 - 10.45 **Welcome to the Conference – Powell Lecture Theatre**
Denis Edgar-Nevill, Chair CFET 2009
Canterbury Christ Church University, UK

10.45 - 11.30 **Invited Keynote Presentation – Powell Lecture Theatre**
Marc Goodman
Director
Centre for Policy & International Cooperation International Multilateral
Partnership Against Cyber-Terrorism ('IMPACT').

11.30 – 13.00 **Parallel Presentation Sessions**

Powell Lecture Theatre

11.30 – 12.00
"Psychology of Cybercrime"
Alastair Irons & David Sanders
University of Sunderland, UK

12.00 – 12.30
"Weaknesses and Possibilities to Improve the Copine Scale"
James Nichol & Denis Edgar-Nevill
Canterbury Christ Church University, UK

12.30 – 13.00
"Social Networking and Cybercrime"
Margaret Ross, Geoff Staples, Mark Udall
Southampton Solent University, UK

Powell Pg06 Lecture Theatre

11.30 – 12.00
"The Game of the Name - Malware Naming and Sympathetic Magic"
David Harley
Director of Malware Intelligence, ESET, UK

12.00 – 12.30
"Cybercrime Forensics: Two views from opposite sides of the pond"
Gary Kessler & Denis Edgar-Nevill
Champlain College & Canterbury Christ Church University, USA & UK

12.30 – 13.00
"Tracking the evolution of the IP thief"
Phil Beckett
Navigant Consulting, UK

Powell Pf07 Lecture Theatre

11.30 – 12.00
"System Management problems: An Advantage to Malware Developers"
C. Chibelushi and T. Proctor
University of Wolverhampton, UK

12.00 – 12.30
"How Ethical are Computer Forensics?"
Robet Dube
Roehampton University, UK

12.30 – 13.00
"The Ethics of Computer Forensics"
Sheona Anne Hoolachan
University of Glasgow, UK

Workshop Computer Laboratory
11.30-13.00
"Analyzing malicious code looking for interesting behavior using a simulated environment"
Righard J. Zwienenberg
Norman, UK

13.00 - 14.00 **Lunch**

14.00 – 15.00 **Parallel Presentation Sessions**

Powell Lecture Theatre

14.00-14.30
"A Mock Trial for Computer Forensics students"
Maurice Calvert
Leeds Metropolitan University, UK

14.30-15.00
"Development of a facility to aid the teaching of Computer Security and Digital Forensics at the University of Bedfordshire
Geraint Williams & Carsten Maple
University of Bedfordshire, UK

Powell Pg06 Lecture Theatre

14.00-14.30
"Is Finger Vein Authentication a Preferred Alternative to Fingerprint Scanning?"
Steve Marsh & Lynne Norris-Jones
University of Wales Institute, Cardiff, UK

14.30-15.00
"A Fingerprint Matching Model using Unsupervised Learning Approach "
Nasser S. Abouzakhar and Muhammed Bello Abdulazeez
University of Hertfordshire, UK

Powell Pf07 Lecture Theatre

14.00-14.30
"Experiences of using Honeypots as a final year project"
Lawrence Munro & Dr. Dimitris Tsaptsinos
Kingston University, UK

14.30-15.00
"Phishing and E-Trust"
Man Qi, Reza Mousoli
Canterbury Christ Church University, UK

15.00 – 15.30 **Coffee & Exhibitors - Powel Foyer and Powell Pg05**

15.30 – 16.00 **Parallel Presentation Sessions**

Powell Lecture Theatre

15.30-16.00
"Analysis of the Methodology used in Digital Forensic Examinations - Mobile Devices Vs Computer Hard Disk"
Paul Owen and Paula Thomas
University of Glamorgan, UK

Powell Pg06 Lecture Theatre

15.30-16.00
"Simulation in digital forensic education"
Jonathan Crellin, Sevasti Karatzouni,
University of Portsmouth, UK

Powell Pf07 Lecture Theatre

15.30-16.00
"Lessons Learned from Beijing for the London 2012 Olympics"
Man Qi, Denis Edgar-Nevill
Canterbury Christ Church University, UK

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

16.00-16.10	Welcome
16.10-16-20	Committee Elections (BCS members only)
16.20-17.20	Invited Presentation

"eBay: Working to Reduce Online Auction Crime."
Steve Edwards MBE
Head of Law Enforcement Relations eBay (UK) Ltd

17.20 – 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.

Menu

Starters

Prawn and avocado salad with lardoons of bacon

Creamy mixed mushrooms en croute (V)

Main courses

Grilled salmon with béarnaise sauce
With seasonal vegetables and potatoes

Ratatouille stuffed beef tomatoes with tomato sauce (V)

Desserts

Passion fruit bavarois

~~~

Cheese & Biscuits

Coffee and Teas
~~~

Day 2 – 2nd September 2009

09.00 – 10.00 **Parallel Presentation Sessions**

Powell Lecture Theatre

09.00-09.30
“Establishing Context When Investigating a Suspect’s Internet Usage”
Christopher Hargreaves
Cranfield University, UK

09.30-10.00
“FIT4D: A Forensic Investigation Toolkit for a Developing Country”
Yasantha N Hettiarachchi, T.N.K. De Zoysa, Keerthi Goonethilake
University of Colombo, Sri Lanka

Powell Pg06 Lecture Theatre

09.00-09.30
“Teaching European Law Enforcement Forensic Scripting Using Bash”
Paul Stephens
Canterbury Christ Church University, UK

09.30-10.00
“Masterkey Linux for Cybercrime Forensics Education and Training”
Qin Zhou and Nigel Poole
Coventry University, UK

Powell Pf07 Lecture Theatre

09.00-09.30
“Grid Computing for fighting Cybercrime”
Abhaya Induruwa & Sarah Induruwa Fernando
Canterbury Christ Church University & University of Oxford, UK

09.30-10.00
“A fast copy detection tool for forensic analysis of suspect documents”
Austen Rainer, Peter Lane, James Malcolm
University of Hertfordshire, UK

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

10.30 – 11.30 **Invited Keynote Presentation – Powell Lecture Theatre**

James Brokenshire MP
Shadow Home Affairs Minister

11.30 – 12.30 **Parallel Presentation Sessions**

Powell Lecture Theatre

11.30-12.00
"A Novel Investigative Methodology for Cybercrime: An Eastern European Case Study"
Stephen McCombie, Paul Watters
Macquarie University, Australia

12.00-12.30
"Closing the Gap for Open Source Image Handling: Acquisition, Verification and Loop-Mount of e01-type images on Linux systems; converting e01 or dd images into bootable virtual machines"
Jens Kirschner
7Safe, UK

Powell Pg06 Lecture Theatre

11.30-12.00
"Qualcomm v. Broadcom: Illustrating the Need for a Computer Forensic Expert"
Milton & Vicki Luoma
Metropolitan State University & Minnesota State University, USA

12.00-12.30
"Cyber Fraud in Ghana"
Kweku Koranteng
University of Ghana, Ghana

Workshop Computer Laboratory
11.30-13.00
"Analyzing malicious code looking for interesting behavior using a simulated environment"
Righard J. Zwienenberg
Norman, UK

12.30 – 13.00 **Exhibitors - Powel Foyer and Powell Pg05**

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**

Presentation Abstracts – 1st September 2009

Psychology of Cybercrime

Alastair Irons & David Sanders
University of Sunderland

Abstract

Cybercrime is escalating at an exponential rate. There is progress in attempts to combat cybercrime at legislative, procedural and technical levels, but a large gap exists in utilising psychology and profiling with respect to cybercrime. There has been very little written about the psychology of cybercrime. If we as a community are to develop effective tools and techniques, and processes and procedures to tackle cybercrime then we need to understand and appreciate the psychology of cybercrime and the emotional and behavioural issues associated with the cyber criminal. This paper outlines a proposed framework for research into the personality traits (including a range of variables such as gender, age, education, intelligence and employment status) of the cybercriminal and the need to compare and contrast the characteristics of cybercriminals and “traditional” criminals. It is widely documented that cyber criminals have exploited the weaknesses and vulnerabilities of computer systems. Cybercriminals also exploit the human psychology of the computer user to manifest a broad range of malware and threats such as spyware, phishing, botnets, spam and rootkits. The nature of cybercrime makes it different in many respects to “traditional” crime, both in terms of carrying out the crime and detecting the crime. One of the major issues is to determine the methodology for the research into the behavioural characteristics of the cybercriminal and to get access to sources for the purposes of data gathering. The purpose of this submission is to share a position paper on the analysis of the evidence indicating distinguishing characteristics of cybercriminals. It is recognised that cybercrime can take place at a number of levels, including national, organised crime and corporate levels – however the framework proposed in this paper focuses on the individual looking at cyber crimes internal to organisation, individual hacking crimes and cybercrimes associated with paedophile activities. The framework seeks to identify traits associated with the different types of cybercrime and also to identify whether there are overarching traits which are common across a set of cybercrime types. Understanding the personality traits and motivations of the cybercriminal will help the computer forensics community in the battle against cybercrime. Accurate profiles of cybercriminals will potentially help in the identification of the cybercriminal in advance of a cybercrime taking place and also in the computer forensics processes and procedures after a cybercrime has been committed.

Weaknesses and Possibilities to Improve the Copine Scale

James Nicholl & Denis Edgar-Nevill
Canterbury Christ Church University

Abstract

The Copine Scale was adopted during a court of appeal hearing in November 2002, in the case of Oliver and Others [2002] EWCA Crim 2766 2002 WL 31599711. The judgement and directions of this appeal case continues to influence all investigations and court processes relating to indecent photographs of children, mainly due to the acceptance and implementation of the Copine Scale. In the early stages of the Copine Scales implementation the immediate impact was the additional work it created for law enforcement computer crime units. Practitioners found themselves categorising hundreds and thousands of images in addition to the work they already undertook. This task was further exacerbated because of ambiguities identified within the five categories formed within the Copine Scale, which caused confusion for practitioners undertaking these tasks. Despite efforts to reduce the ambiguities in the Copine Scale, which saw the release of a second edition, the ambiguities have continued. In addition to the ambiguities it appears that the original guidelines issued by the SAP are not rigidly adhered to and it appears to be regular and common practice for Judges and Magistrates to decline to view the images and work solely on image descriptions and submitted categorisations. Fundamentally, during the period of the Copine Scales development and implementation there has not been direct consultation with the practitioners, who are required to use the scale. In addition the views of practitioners have never been sought to ascertain their impression of the formulation of the scale or how its implementation impacted on them. This oversight could be viewed as a significant missed opportunity to gain valuable feedback from the very people who have to use the scale on a daily basis and on whom the Copine Scale has had the greatest impact. The other area which appears to have been overlooked concerns risk, specifically offender risk. The scale appears to have been created to provide a sliding tariff of punishment based on quantities, type and use of indecent photographs of children. This, it appears, bears no relationship to the risk an offender may pose to the community or in fact have any concern for the harm that has come to the children abused in the resultant photographs.

Social Networking and Cybercrime

Margaret Ross, Geoff Staples, Mark Udall
Southampton Solent University, Faculty of Technology,
East Park Terrace, Southampton, SO14 0RD
E-mail: Margaret.Ross@Solent.ac.uk

Abstract

The paper discusses the use made of social networking for such diverse aspects of the use of social networks as those related to recruitment into the government/security police departments and also the use made of these sites by organized crime. The paper is a research in progress, based on acquiring responses from students from a variety of interests in different countries, who are currently undertaking undergraduate or postgraduate courses on computer forensics, security and computing. The survey is being conducted with the students to obtain their views on the risks that they perceive, the ways to minimize these risks, associated with the use of social networks, including Second Life and similar sites. It is planned to undertake this research as a longitudinal study, to identify the changing views of students and the effect of changes in university syllabus, relating to the social networks and the growth of students using virtual worlds. A pilot study to for this has already been conducted at Southampton Solent University with students on a variety of computing and networking courses , leading to publication in last year's CFET conference. It is planned to obtain participants for this research from a variety of countries, leading to publication in appropriate conferences and journals.

The Game of the Name: Malware Naming and Sympathetic Magic

David Harley BA CISSP FBCS CITP
ESET LLC, 610 West Ash Street, Suite 1900, San Diego, CA 92101
8 Clay Hill House, Wey Hill, Haslemere, Surrey GU27 1DA; +1 619 204 6461

Abstract

Once upon a time, one infection by specific malware looked much like another infection, to an antivirus scanner if not to the naked eye. Even back then, virus naming wasn't very consistent between vendors, but at least virus encyclopaedias and third-party resources like vgrep made it generally straightforward to map one vendor's name for a virus to another vendor's name for the same malware. In 2009, though, the threat landscape looks very different. Viruses and other replicative malware, while far from extinct, pose a comparatively manageable problem compared to other threats with the single common characteristic of malicious intent. Proof-of-Concept code with sophisticated self-replicating mechanisms is of less interest to today's malware authors than shape-shifting Trojans that change their appearance frequently to evade detection and are intended to make money for criminals rather than getting adolescent admiration and bragging rights.
Sheer sample glut makes it impossible to categorize and standardize on naming for each and every unique sample out of tens of thousands processed each day. Detection techniques such as generic signatures, heuristics and sandboxing have also changed the ways in which malware is detected and therefore how it is classified, confounding the old assumptions of a simple one-to-one relationship between a detection label and a malicious program. This presentation will explain how one-to-many, many-to-one, or many-to-many models are at least as likely as the old one-detection-per-variant model, why "Do you detect Win32/UnpleasantVirus.EG?" is such a difficult question to answer, and explain why exact indication is not a pre-requisite for detection and remediation of malware, and actually militates against the most effective use of analysis and development time and resources. But what is the information that the end-user or end-site really needs to know about an incoming threat?

Cybercrime Forensics: Two Views from Either Side of the Pond

Gary Kessler & Denis Edgar-Nevill
Champlain College & Canterbury Christ Church University

Abstract

To cite the quotation “Britain and America are two nations divided by a common language” (which is variously attributed to several famous people including Winston Churchill, George Bernard Shaw and Oscar Wilde), the focus of interest/emphasis in computer forensics is slightly different on either side of ‘the pond’ (the Atlantic Ocean). This paper’s intention is to provide some insight into these differences by considering the contributions to two international conferences with broadly the same remit chaired by each of the authors; CFET 2008 The 2nd International Conference on Cybercrime Forensics Education and Training held in the UK in September 2008 (CFET 2008) (Denis Edgar-Nevill), and ADFSL 2009 Conference on Digital Forensics, Security and Law held in the USA May 2009 (Gary Kessler) (ADFSL 2009). A review of CFET 2008 can be found in the special edition of an international journal containing selected papers from the conference (ESDF 2009). At first glance the programmes for the two conferences do not seem markedly dissimilar; given the titles of the papers they include. Each conference has a mix of law-enforcement, academic and private sector contributors and participants with contributions from a number of countries. The contrast becomes more apparent with a more detailed examination of their content and the nature of the examples being cited. What would be very noticeable to anyone attending both events would be the changes in emphasis. One has to strongly resist the temptation to reduce the quality of the argument to “well you just had to be there to appreciate this”. It was clear that the arguments/examples used and discussions arising from the presentations that in the USA the focus of computer forensics is much broader (taking in more company disputes or private litigation) than the preoccupation with fighting computer crime and supporting police in the UK. The glorification of the technicalities of ‘bit-twiddling’ was evident in both camps; as one would expect from a computing community. The differences were what types of circumstance these tools were used to detect and analyse. The greatest hurdle is the lack of mutual understanding we share. The differences in our legal systems and structures, and in our politics were also very clear. In Europe we tend to think of the USA a far more of a simple law enforcement structure that it is in reality. In the USA there is a very limited understanding of the nature of the European Union and how it works in practice; the EU are already viewed as federal “United States of Europe” in some quarters. The cry of “Vivre la Différence!“ should be tempered by an understanding that these differences could put up barriers, have profound influences on, how the computer forensics develops globally where we are moving into a phase where international standards are being developed.

References

(ADFSL 2009) Proceedings of the 2009 ADFSL Conference on Digital Forensics, Security and Law, Gar Kessler (Ed), Champlain College, Burlington, Vermont, USA May 20-22, 2009

(CFET 2008) Proceedings of the 2nd International Conference on Cybercrime Forensics Education and Training, Denis Edgar-Nevill (Ed), Canterbury Christ Church University, UK, 1st/2nd September 2008, ISBN 1899253-19x

(ESDF 2009) International Journal of Electronic Security and Digital Forensics, Special edition: Cybercrime Forensics Education and Training, Edgar-Nevill D. (guest Editor), Vol.2 No.2, Inderscience Enterprises Ltd, UK, May 2009, ISSN 1751-911X (Print) ISSN 1751-9128 (Online)

Tracking the evolution of the IP thief

Phil Beckett
Director, Navigant Consulting

Abstract

IP theft is a growing business as highlighted in the recent study by KPMG and Mishcon de Reya that stated that IP theft had grown by 100% between 2006 and 2008 and was set to rise by a further 10% in 2009. Based on the cases they studied, "...the most common data stolen was customer or client-related information...or customer lists...[and] The most common method for employees to transfer stolen data was via email."[1] The evolution of the IP thief. Information is of critical importance to many organisations as it forms a competitive advantage, and because of this it is also attractive to an IP thief who is looking to get a 'head start' in a new job or start their own business. How has this thief evolved over time? Their evolution has been closely linked to the development of technology dating back to when the printing press was first invented by the German goldsmith Johannes Gutenberg in around 1440. Other notable technological advances that have aided the IP thief include the computer (1837 or 1936 depending on whether you are a Babbage or Turing fan), the photocopier (1937), e-mail (1973), the Internet (1978) and USB flash drives (2000). Where do they go? So what artefacts are left behind on a machine to provide evidence of what the IP thief has been accessing? Putting aside log files, which if configured can track every movement a user takes on a system, there are a number of key artefacts to review, including:

- Internet History files (which can also track internal system browsing)
- Link files (to see what files have been opened recently)
- Files left behind when e-mail systems don't clear up correctly (especially Microsoft Outlook)

Identifying the exit route

Looking at confidential data is one thing, but the IP thief needs to be able to extract this to maximise its value to them. Unfortunately gone are the days when we could recover and review print file artefacts showing what files were printed and when (including their content) – a 'hole' that Microsoft eventually fixed. But there are plenty of other artefacts to review to give the investigator an insight into what has occurred. These include:

- Internet History and Cache files (specifically those related to web-based e-mail accounts)
- USBSTOR – what USB devices have been connected to the system
- Link Files again – it is amazing how often people look at the data they are stealing to make sure the transfer has been successful
- Client Sided Cache – if the user has used the "make available off-line" functionality
- StreamMRU – allowing the investigator to identify folders opened, including those opened from CDs, USB devices and network shares
- Bags – allowing the investigator to identify files where the user has altered the default window size
- Restore Points – the Windows time machine, allowing you to step back in time

[1] http://www.mishcon.com/assets/managed/docs/downloads/doc_2373/fighting%20fit%20-%20report%20final.pdf

- Windows.edb – identifying what files have been indexed using the Windows indexing engine – even when they have been subsequently deleted
- CD/DVD log files – which can identify what and when files have been burnt to disk

Bringing it all together

On many investigations the fabled "smoking gun" does not exist, however, in virtually every case it is possible to identify evidence that once put together can give a clear picture of what has occurred on a system, or at the very least provide enough ammunition for action to be taken. This is illustrated in four brief case studies:

1. The liar who didn't know when to stop – when USBSTOR entries and time and date stamps provided damning evidence
2. The global business theft – when web-based e-mail, Sykpe chat logs and USBSTOR entries illustrated a global conspiracy to steal confidential data and poach key staff
3. The snooper – when a departing local manager obtained confidential data was undone by the failings of Outlook
4. Confidential data goes walkies...but the Registry provides a complete catalogue of what happened to it

System Management problems: An Advantage to Malware Developers

C. Chibelushi and T. Proctor
University of Wolverhampton

Abstract

Using the internet for on-line banking, shopping and other forms of e-commerce involves the transfer of sensitive information such as credit card information and other personal or company data. In order to support this type of networked transaction, a variety of security techniques have been developed. Often combined together, they aim to provide a high level of confidentiality, integrity and authenticity in order to secure electronic transactions. However, the number and sophistication of malevolent programs is increasingly threatening network security. In many cases these are no longer developed as a result of intellectual challenge or as a nuisance, but for professionals with an aim to commit fraud. This paper discusses vulnerabilities and the types of attacks that may exploit them. It also looks at other occurrences that can lead to incidents. It identifies research in anti-malware techniques and suggests that although security techniques may be limited, the greatest vulnerability is related to system management problems. It describes the differences between incidents resulting from external and internal actions. Identification is made not only the advantages from being “on the inside” but also that an incident may occur without intended malice. It describes some of the methods frequently used to compromise systems and these include sniffing, password attacks, malicious code, social engineering and denial of service. The difficulty in managing systems for security is further illustrated using the results of data generated by the West Midlands WARP. Managed and operated by the University of Wolverhampton, WARP is a Warning, Advice and Reporting Point for Information Security It is a service to provide warnings and advice and a point to which incidents can be reported. Members receive and share up-to-date advice on the latest information security threats, incidents and solutions. This paper includes an analysis of warnings issued by West Midlands WARP which provides some interesting results.

How Ethical are Computer Forensics?

Robet Dube
Roehampton University, London
80 Roehampton Lane
London SW15 5SL
r.dube@roehampton.ac.uk

Abstract

Delegates will be introduced to ‘provisional working definitions’ of Ethics, Computer Forensics and other related topics. 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. At the end an online discussion forum with regular updates and linked to other similar conferences will be created and Delegates will be asked to join the forum for delegates to continue their discussions. The main focus of the Workshop will be 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: Ethics, Forensic, computers, investigation, privacy, law, legal, policing, Human Rights, Rights, Culture, custom, terror, terrorism, society, conspiracy, trust, religion.

The Ethics of Computer Forensics

Sheona Anne Hoolachan
University of Glasgow,
University Avenue, Glasgow G12 8QQ
sheona.hoolachan@bcs.org

Abstract

Professions that deal with criminal activities and individual's rights arguably have more consequential considerations, repercussions and subsequently more pertinent ethical considerations. Richard O. Mason, in his article Four Ethical Issues of the Information Age, considers the unique aspects of the information age and the subsequent ethical issues presented by digital material. He outlines four main issues: Privacy; Accuracy; Property; and Accessibility. By applying these to the field of digital forensics, in this paper, it is clear that forensic experts will be required not only to comply with legislation, but also with both company specific policies and their own ethical understanding of each individual situation. By contextualising the ethical dilemmas using previous cases, approaching the subject matter in a 'learn from their mistakes' manner, the ambiguity of Mason's concepts is clarified. One could argue that this is the only realistic method by which ethical issues can be addressed as it will be necessary in each situation to consider the merits of the circumstances at hand. Standardised policies, such as the ACPO guidelines assist in highlighting potential pitfalls within law enforcement situations, however they can only act as guiding principles as ethics must be weighted against the type and the severity of the crime. Using examples, such as the "Spycatcher Case" and the multiple losses of data devices by the Ministry of Defence, this paper highlights the interplay between ethical considerations and legal requirements.

A Mock Trial for Computer Forensics students

Maurice Calvert
Leeds Metropolitan University

Abstract

Delivery of a new degree course in Computer Forensics began in the Faculty of Information and Technology at Leeds Metropolitan University in September 2007 with an initial intake of 34 students. The course, like many others in this subject area, is essentially a Computing course with specialist modules allowing students to learn about the forensic analysis of data stored in computer memory. From the outset it was recognised that an important element of the course should be links to practitioners from business and the provision of a thorough understanding of the legal and ethical aspects of the professional's work. A major part of this provision occurs in the Level 2 Group Project. The Group Project is a four module (60 credit point) block of study undertaken by all Level 2 students of the Faculty but with careful contextualisation for each study area. The Group Project for BSc Computer Forensics students culminated in a Mock Trial held in the mock court room of Leeds Law School (part of the university). With the involvement of staff from West Yorkshire Police Hi-Tech Crime Unit and Leeds Law School, it is believed that this project provided a high quality and innovative introduction to many aspects of the professional requirements of computer forensics practitioners. The initial part of the Group Project included lectures delivered by a qualified barrister who has significant previous experience in training of expert witnesses. The lectures covered such issues as the court process and the role and responsibilities of an expert witness. In parallel, students, working in groups, were required to create forensic images of some digital memory. The images were to contain evidence of a supposed kidnapping including instant messages, e-mails and other documentation prepared by and sent between "gang members". After image creation, lecturers selected suitable images to distribute to other groups of students for analysis. The analysis phase involved students (still in groups) searching the images to find evidence of the alleged crime and preparing a detailed expert report such as might be required as evidence in a court case. The final stage in the project involved one or two members of each group defending their evidence under cross-examination in the mock court room. This paper discusses the various stages of this successful project taking opinions from internal and external staff and student participants. It addresses issues which arose and lessons to be learnt for the future delivery of such an experience to the students. Amongst key findings are the value employers, police and students alike place on such an experience, the need for careful advanced planning and the close cooperation required between participants.

Development of a facility to aid the teaching of Computer Security and Digital Forensics at the University of Bedfordshire

Geraint Williams & Carsten Maple
Institute for Research in Applicable Computing
University of Bedfordshire
Park Square, Luton, LU1 3JU, Bedfordshire

Abstract

The UK is suffering a skills shortage in the field of digital forensic investigators at all levels. This has been highlighted in a number of reports including the third phase EURIM e-crime study presented to the House of Commons in May 2004. The report stated that "Law Enforcement agencies require a bigger pool of skilled investigators and digital Forensic experts…the throughput of the high level courses is seriously inadequate". A recent report for the Metropolitan Police Authority regarding the progress of Metropolitan Police Service e-crime strategy indicated that with "the increasing utilisation of digital technology, the demand for associated forensics services are likely to increase by 30-40% over 2006/7". There is a need for investigators with a broad range of skills and a depth of technical knowledge in some of these. The higher education sector is ideally positioned to provide the analytical and higher level skills development that is required. With subjects such as Computer Security and Digital Forensics it is difficult to provide graduates with the necessary skills that industry requires unless it works closely with the industry and interested parties such as the government in developing the curriculum and facilities to support the requirements of the industry. This paper examines the requirements of the digital forensic industry and the transfer of these into the requirements of a higher education course. The paper offers a baseline of our initial curriculum design and supporting infrastructure and outlines the approach of the University in working with industrial partners to develop the curriculum and infrastructure to better provide skilled graduates. The paper further demonstrates the need for academic and industrial interaction to ensure graduates are equipped with the necessary cognitive and applicable skills and experience in the all areas that are vital to ensure the demand for skill digital forensic technicians, investigators and expert witnesses is meet with well rounded graduates. The paper examines the challenges of providing skilled graduates to work in a field that is developing with new technological challenges being faced by the industry continually. The industry has grown in a short period of examining computer hard drives to having to examining live systems that can not be turned off to what is now everyday items such as mobile phones, PDA's and GPS devices to provide evidence of not just directly related cybercrime but evidence for all types of criminal activity.

Is Finger Vein Authentication a Preferred Alternative to Fingerprint Scanning?

Steve Marsh & Lynne Norris-Jones
University of Wales Institute, Cardiff
Cardiff School of Management
Department of Information Systems

Abstract

Fingerprint scanning is a relatively mature biometric technology which has been successfully deployed in security applications including airports, law enforcement agencies and government buildings. This technology does have one major drawback in that it is perceived to be associated with criminal activity hence its established use in forensic science. Such perception may prevent its adoption in certain areas of society and there are often legal and ethical challenges and general concerns over the adoption of centralised databases of fingerprint templates by the government and police forces. One notable example was the European Court of Justice's decision regarding Michael Marper in December 2008, which ruled that the centralised storage of DNA / fingerprint information violated the human right to privacy within Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms. One way of addressing these concerns would be to adopt the policy of storing biometric information on smart cards which are retained by the owner of the fingerprint and presented at the time of enrolment/identification. This integrates well into the practice of two-factor technology which has been used to improve the accuracy and integrity of biometric authentication. This paper considers the use and associated risks of finger vein authentication as an alternative to fingerprint scanning since it has no established association with currently held criminal records and it should therefore be more readily accepted by society. This study will initially involve an investigation into the general perception of fingerprint biometrics for security and law enforcement. It will assess any concerns regarding storage, either via a centralised database or on smart cards, based on participant responses and will be compared with the more recent technology of finger vein authentication. A biometrics solution matrix (Nanavati, 2002) will be developed for both technologies and will consider other factors/ drivers such as the urgency, effectiveness, exclusivity and scope along with the receptiveness to determine whether finger vein authentication is a preferred alternative for deployment.

A Fingerprint Matching Model using Unsupervised Learning Approach

Nasser S. Abouzakhar and Muhammed Bello Abdulazeez
School of Computer Science, The University of Hertfordshire,
College Lane, Hatfield AL 10 9AB, Hertfordshire, UK
{N.Abouzakhar, M.B.Abdulazeez}@herts.ac.uk

Abstract

The growing dependence of modern society on information and communication technologies has become inevitable. Due to the recent explosive boom in the field of communications and transportation, intelligent systems provide access control to various resources such as information, financial data/institutions, hospitals, airports, countries and so on. Because of the nature of those resources and their reliance on computer systems to achieve effective security there is an increased need for stronger authentication mechanisms. Biometric security has taken over many of user authentication and identification technologies as biometrics will definitely change the way access control systems operate. With the increasing use of IT technologies in our daily lives, there is a need for stronger authentication mechanisms. Providing appropriate authentication and identification mechanisms such as biometrics not only ensures that the right users have access to resources and giving legitimate users the right privileges but enables cybercrime forensics specialists to gather useful evidence whenever needed. Also, these resources need mechanisms to detect when invalid users try to misuse their privileges. Certainly biometrics helps to provide such services. This paper investigates the field of biometrics as one of the best mechanisms for user authentication and evidence gathering despite its limitations. A novel biometric model is proposed taking into account the strengths and weakness of biometrics. The model proposes a statistical-based unsupervised learning approach for fingerprint matching. The proposed matching algorithm is based on three various similarity measures, Cosine similarity measure, Manhattan distance measure and Chebyshev distance measure. In this paper we introduce a novel model which uses those similarity measures to compute a fingerprint's matching factor. The calculated matching factor is based on a certain threshold value which could be used by a cybercrime forensics specialist for deciding whether a suspicious user is actually the person who claims to be or not. A freely available fingerprint biometric SDK has been used to implement the suggested algorithm. The major findings of the experiments showed promising and interesting results in terms of the performance of all the proposed similarity measures.

Experiences of using Honeypots as a final year project

Lawrence Munro & Dr. Dimitris Tsaptsinos
Faculty of CISM, Kingston University

Abstract

The purpose of this paper is to outline first-hand experiences of using Honeypots, from the perspective of a final year student with no prior experience of Honeypot technology. The Nepenthes platform was used as both as a tool to collect malware for statistical analysis, and also as a gateway to understanding the white-hat community on the whole. The results from the Nepenthes implementation were expressed using quantitative and qualitative methodologies. Behaviour analysis was applied in conjunction with other recent studies of malware to gain an insight into the way that malware behaves on the Internet. An in-depth behavioural analysis of the conficker worm illustrates how a large amount of detail can be gathered and interpreted by undergraduate level students. The paper additionally demonstrates how through end of year projects, a large area of work can be covered within a very specific are of study. This is demonstrated by the section pertaining to achievements and further study in terms of self-actualisation and interest generated in the subject area.

Phishing and E-Trust

Man Qi, Reza Mousoli
Department of Computing
Canterbury Christ Church University
Canterbury, Kent CT1 1QU, UK

Abstract

Phishing generally refers to e-mail messages that look authentic from trusted companies, but attempt to send fake websites. Recipients of the emails are asked to give out sensitive personal information which could be used to commit identity fraud. Phishing is a serious and rapidly growing problem for service providers, enterprises and consumers. Since August 2008, the Computing Services at Canterbury Christ Church University has frequently posted online notices on phishing attacks that the University has encountered (see Staff Notices: 'Phishing attack', 11/08/2008; 'Phishing email', 06/10/2008; 'Increasing in Phishing emails', 19/11/2008; 'Beware phishing email', 19/01/2009). According to Anti-Phishing Working Group (APWG), phishing reports recorded as high as 173,498 cases only in the second half of 2008. The reports suggest that 7 out of 10 people who go online have received phishing e-mails, while 5% have actually given out sensitive personal information to spoofed websites. Why Phishing works? How is it trusted? Although more and more efforts have been put on anti-phishing from technical, educational or legal aspects, phishers are becoming more sophisticated and the problem is getting more prominent. Phishers do not take advantage of technical vulnerabilities, which is difficult to employ technical countermeasures. Phishers generally use trend-better spelling, sub-domains or cousin domains. Users are deceived by phishing emails mainly because of the lack of Web fraud knowledge. Some users are not aware that phishing is possible, some users simply do not question website legitimacy. Erroneous security knowledge is another reason. Some users have misconceptions about which website security features. Understanding how users build up their own e-trust to evaluate websites is crucial to prevent phishing. Empirical studies show that users generally judge emails by their relevance before authenticity. They often decide whether a website was legitimate or not based on the content. Some typical 'trust indicators' exist, for example, logos and icons etc. Personalization could increase the trustworthiness in email or Web pages. The more personal information is present, the more likely the user finds that the email is authentic.

References

1. Loftesness, S. Responding to "Phishing" Attacks. Glenbrook Partners (2004).
2. Fogg, B. J. et al. How Do Users Evaluate the Credibility of Web Sites? : A Study with Over 2,500 Participants. Proc. DUX (2003).
3. Fogg, B. J. et al. What Makes Web Sites Credible?: A Report on a Large Quantitative Study. Proc. CHI (2001), 61-68.
4. Dhamija, R., Tygar J. D. , H. Marti, Why Phishing Works, Proceedings of the SIGCHI conference on Human Factors in computing systems, 2006
5. Wu, M., R. Miller, & S. Garfinkel. Do Security Toolbars Actually Prevent Phishing Attacks? Proc. CHI (2006).
6. Julie S. Downs, Mandy B. Holbrook, and Lorrie Faith Cranor. Decision strategies and susceptibility to phishing. In SOUPS '06: Proceedings of the second symposium on Usable privacy and security, pages 79-90, New York, NY, USA, 2006. ACM Press.

Analysis of the Methodology used in Digital Forensic Examinations - Mobile Devices Vs Computer Hard Disk

Paul Owen & Paula Thomas
Information Security Research Group
Faculty of Advanced Technology, University of Glamorgan
{pdowen, pthomas} @glam.ac.uk

Abstract

Digital evidence today is proving increasingly pivotal in criminal investigations whether it is an arrest for a minor offence or potential terrorist activity [1]. As people rely on mobile devices and their many other functions, the digital trail of evidence continues to grow. The forensic examination of mobile devices is a relatively new discipline. Research activity into the forensic analysis of these types of devices, and the information they may contain, is limited when compared to the exponential increase in ownership of these devices [2]. The amount of ubiquitous information stored on these mobile devices will continue to grow as they become increasingly powerful and incorporate more functionality. In the United Kingdom, ACPO (Association of Chief Police Officers) have published guidelines for the forensic analysis of mobile devices and computer hard disks. The guidelines and procedures for the forensic examination of computer hard disks are well established, whereas those for mobile devices are very limited. The aim of this paper is to compare and contrast the current methodologies involved in the forensic examination of both types of digital media and to identify those areas of mobile device examination where the current ACPO guidelines are insubstantial.

Keywords: Mobile Forensics, Computer Forensics, Information Security.

Simulation in digital forensic education

Jonathan Crellin, Sevasti Karatzouni,
School of Computing
University of Portsmouth

Abstract

The paper starts by describing the role of simulation and role play in education and training. A variety of examples, such as flight simulation, medical simulation (ExPERT Centre), military personnel and stress (US Military), role play in systems analysis and design (BCS). The core definition of simulation is that it allows students to explore a problem area in a safe and controlled environment. We contrast different approaches, such as high versus low fidelity simulation. Virtual worlds represent one strand of simulation, and have been used in education to teach a variety of subjects (e.g. Chandler, Crellin, Duke-Williams, 2008; Crellin, Chandler, 2008). Simulation is already used in many areas of the forensic subject area, for example by giving students suspect disks to analyse, asking them to seize a computer system in different scenarios, or delivering evidence in a simulated court. Forensic simulation both teaches cognitive practical skills, and acts to reduce the anxiety related to working as a digital forensics practitioner. We are evaluating the use of virtual worlds to extend the range of convenience of forensic simulation and to allow a larger range of scenarios to be used. A comparison of 'role playing' and automated simulation will be compared. We anticipate that for a given development cost a larger variety of scenarios can be used with students, and that more autonomous and learning from a distance can be used. During the academic year 2009-2010 we intend to build a series of forensic simulations, using two different virtual world systems, Second Life (Linden Labs) (a widely used Internet virtual world 'built by the denizens of second life') and Wonderland (Sun Microsystems) (a closed local virtual world, which allows a virtual environment to be run locally behind a firewall). Conventional role playing simulations will also be used. The evaluation will compare development effort for each environment. Development cost, deployment cost, student engagement, student skill acquisition, and student enjoyment will be compared.

References

ExPERT Centre (http://www.expert.port.ac.uk/)
Bonk, C. J. & Dennen, V., (2005) Massive Multiplayer Online Gaming: A Research Framework for Military Training and Education. IN DIRECTORATE, R. A. T. (Ed.), Under Secretary of Defense.
Chandler, J., Crellin, J. and Duke-Williams, E, (2008) Current Topics in T&L : Second Life – Does having a second life make learning more effective? (Keynote) , National Teaching Fellow Symposium, London School of Economics 6th - 7th April 2008.
Crellin, J., Chandler, J. (2008) Using 3D Virtual worlds in ftf and distance learning, Higher Education Academy Annual Conference, Harrogate 1st - 3rd July 2008.
Linden Lab (2003) Second Life. (http://secondlife.com/)
Sun Microsystems (2008) Project Wonderland. (https://lg3d-wonderland.dev.java.net/)

Lessons Learned from Beijing for the London 2012 Olympics

Man Qi, & Denis Edgar-Nevill
Canterbury Christ Church University

Abstract

Computer networks were first used at the Barcelona Olympic Games in 1992. Since then, information and computer network technologies have been playing an increasing role in modern Olympics. However, network and information security issues are gaining severely prominent. We can imagine that, when Olympic Games are ongoing, suddenly the official website is defaced and the important data is lost; the exciting 100 meters competition is to start, but the metering systems are crashed. These disappointing scenes may happen in the Olympics. One case happened in Atlanta Olympics in 1996 as a system failure led to the score of a game could not be sent out in time. The 2008 Beijing Olympic Games attracted not only the best sport talents, but also technically powerful criminals around the world. This is not just an alarm. In fact, during the Beijing Olympics more than 17,000 systems including servers, network switches, routers and application software need to be managed and the information network bears mass data processing such as schedule management, press releases, event services and business operations. Its security was directly related to the normal operation of the whole Olympic Games. How to best prevent attacks and effectively protect information security arouses widespread concern and faces great challenges. Major events tend to be good opportunities to spread computer viruses. The Olympics is a mega event being held once in four years and catches the world's attention. It is more likely to be targeted by hackers and be their stage to be 'famous'. Beijing Olympics information system was the largest and most complex in the history of the Olympic Games with unprecedented data-processing capacity. The system supported 28 games, more than 300 matches, and 15,000 journalists, forming a network with tens of thousands of end-user access points. In addition, the system also covered Beijing, Hong Kong and other cities in seven games and more than 60 non-competition venues. During the Olympic Games in Beijing, there were tens of thousands of athletes, politicians, celebrities and millions of business visitors around the world gathered in the Olympic event cities. This means a huge number of digital cameras, PDAs, USB memories, mobile phones and other mobile devices connected to the network terminals. Viruses could be easily brought in and the infected machines may affect the entire network. The main information network at the Beijing Olympics had five systems: the Olympics Organizing Committee network, the Games network, the Olympic official website, the Olympic ticketing website and the Olympic venues network. Measures have been taken in accordance with five different network security needs. As such a huge system, no one can promise absolute security for the Olympic Games, but most efforts should be given. The authors hope their work could help with the preparation of 2012 London Olympic Games.

References

1. Hui Jin, "Inside" and "outside" of Olympic networks and info. security, www.ccidnet.com, 2008
2. Olympics tests information security in China IT Industry, Comm.and Information News, 2008
3. Shu Li, Beijing Olympic Games set up crisis centre to prevent hacking, Outlook Newsweek, 2008
4. Honghong Gu, China's information security technology has stood the test of the Olympic information security, www.xinhuanet.com, 11th Nov 2008
5. Denis Edgar-Nevill, Problems in Cybercrime Forensics and the London 2012 Olympics, BCS Cybercrime Forensics SG Workshop, London, 4th March 2009
6. Denis Edgar-Nevill, Protect Yourself from Cybercrime at the London 2012 Olympics, BCS Cybercrime Forensics SG Workshop, Southampton, 28th April 2009

FIT4D: A Forensic Investigation Toolkit for a Developing Country

Yasantha N Hettiarachchi[1], T.N.K. De Zoysa[2], Keerthi Goonethilake[3],
University of Colombo School of Computing
No 35, Reid Avenue, Colombo 07. Sri Lanka.
kasun@ucsc.cmb.ac.lk

Abstract

Globalization has caused a tremendous increase in the IT sector, resulting in the increase of cyber crimes in each and every corner of the world including third world countries like Sri Lanka. Therefore efforts have been made in those countries to control the incidence of cyber crimes by using a proper forensic investigation methodology. Although there are over hundreds of digital forensic investigation processes developed all over the world, each organization/ country tend to use their own procedure which is suitable for their legislation and their specific needs. Similarly, previous researches carried out in Sri Lanka revealed that the steps taken in the most of the existing forensic frameworks/ Toolkits are impractical in the context of a country like Sri Lanka. Most of the existing Tools are not well-suited for the current legislation of the country and they are not viable with the limited resources that the developing countries have. Therefore it is need to build a new forensic methodology and Toolkit and which supports the current legislation of Sri Lanka. This paper proposes a new digital forensic framework, FIT4D which includes a software Toolkit and a clear set of guidelines which is appropriate for solving any type of computer related cyber crimes in developing country like Sri Lanka. Our previous studies[1] identified that the DRFWS model proposed by Mark Reith, Client Carr and Gregg Gunsch[2] as the most compatible model to the procedure followed by the forensic experts in Sri Lanka. Activities done under each phase is chosen to match the current legislation of Sri Lanka while utilizing the available limited resources. As many of the common digital forensic analysis tools such as encase [4] ,FTK[5] are developed with commercial interests, it is unlikely that a it is match with the specific legal requirements of a country like Sri Lanka and more importantly the cost of the software can be afford by a developing country like sriLanka. In addition there are open source software like pyflag[6].Unfortunately, PyFlag is not widely used because of its complexity and difficulty of deployment. After doing a survey on available commercial and open source software and their functionalities, we decided to develop a new forensic investigation toolkit based on Carrier's SleuthKit Library[7]. Although there are general purpose graphical user interfaces for the command line interface of Sleuthkit such as PTK[3] and Autopsy browser[8], most of the features we identified in our previous studies that should include in a suitable model/framework for a developing country are missing in these tools .For example features like compressing disk images to save storage space in FIT4D is not available in PTK, which will save the available limited resources in developing countries. Likewise in each and every activity under each phase we will consider the how the activity can be achieved by utilizing the resources. FIT4D will best fit to the current investigation procedure carried out by the forensic experts in Sri Lanka and it will utilize existing resources. Furthermore it will be enriched with a user friendly interface which will help police officers/any user with poor computer literacy to identify evidence in earlier stages of the investigation process before going to a forensic expert. Furthermore

the proposed framework can be easily expanded to include any number of additional phases required in the future.

References

1 “Developing a Digital Forensic Framework for a Third World Country”, , Kasun De Zoysa, Keerthi Goonathillake, Ravith Botejue,University of Colombo, Sri Lanka

2 Mark R. Clint C. & Greg G., An Examination of Digital Forensic Models

3 PTK site, accessed 01/06/2009, http://ptk.dflabs.com/

4 Guidance Software, Inc. EnCase Forensic, 2007. http://www.guidancesoftware.com/products/ef_index.asp.

5 Access Data. Forensic toolkit—overview, 2005. http://www.accessdata.com/Product04_Overview.htm?ProductNum=04

6 M.I. Cohen.PyFlag: An advanced network forensic framework. In Proceedings of the 2008 Digital Forensics Research Workshop. DFRWS, August 2008. http://www.pyflag.net. [Online; accessed 06 March 2009

7 Brian Carrier. The Sleuth Kit & Autopsy: Forensics tools for Linux and other Unixes, 2005. http://www.sleuthkit.org/. [Online; accessed 06 March 2009

8 Sleuthkit web site, accessed 02/06/2009, http://www.sleuthkit.org/autopsy/

Teaching European Law Enforcement Forensic Scripting Using Bash

Paul Stephens
Christ Church University
Email: paul.stephens@canterbury.ac.uk, Telephone: +44 (0)1227 767700

Abstract

Following the success of the Agis “Cybercrime Investigation – developing an international training programme for the future” projects [1] which were recommended by the Falcone “Training: Cybercrime Investigation – Building a Platform for the Future” [2], where seven digital forensics training courses were developed with academic accreditation, this paper examines one aspect of the current incarnation of this project group’s work. The project group comprising of academics, computing industry professionals, and law enforcement officials and funded by the European Commission’s ISEC project [3] and several of the partner institutions, aims to run all courses created so far as a pilot MSc programme. For this to happen three new courses must be added to the existing seven. This paper looks at the development of one of these courses tentatively titled “Advanced Scripting” (although perhaps a better name would be “Forensic Scripting Using Bash”). The aim of this course is to take law enforcement students with no programming experience, and bring them all to a common level of knowledge and understanding of scripting for forensic computing applications in a Linux environment. This paper examines the design and development of this course which is due to run in pilot form between the 7th and 11th September 2009 at the Cybex [4] offices in Madrid, Spain. This will include: an explanation of how and why this development grew out of the Agis “Linux as a Forensic Tool” course; a critical evaluation of the design and development process; an examination of why we think teaching police officers to program is a good idea; and a preview of the course content and suggested evaluation process.

References

[1] European Commission (2006) AGIS was a framework programme to help police, the judiciary and professionals from the EU Member States and candidate countries co-operate in criminal matters and in the fight against crime [online]. Available at: http://ec.europa.eu/justice_home/funding/2004_2007/agis/funding_agis_en.htm [Last accessed 30 June 2009].

[2] European Commission (2002) Falcone - helping people and organisations fight against organised crime at EU level [online]. Available at: http://ec.europa.eu/justice_home/funding/expired/falcone/wai/funding_falcone_en.htm [Last accessed 30 June 2009].

[3] European Commission (2008) Prevention of and Fight against Crime [online]. Available at: http://ec.europa.eu/justice_home/funding/isec/funding_isec_en.htm [Last accessed 30 June 2009].

[4] Cybex (2009) Fraud Prevention, Detection and Investigation in virtual environments [online]. Available at: http://www.cybex.es/defaulten.aspx [Last accessed 30 June 2009].

Masterkey Linux for Cybercrime Forensics Education and Training

Qin Zhou and Nigel Poole
Faculty of Engineering and Computing
Coventry University
Priory Street, Coventry CV1 5FB, United Kingdom
Email: q.zhou@coventry.ac.uk and n.poole@coventry.ac.uk

Abstract

This paper introduces the Masterkey Linux forensics system (www.masterkeylinux.com), its features and usage, to the wide community of cybercrime forensics professionals. A case study is presented to demonstrate how Masterkey may be used in education and training. While access to commercial computer forensics tools is important for future careers, students should also have a collection of open source forensics software tools that they may deploy at leisure on their own computers to learn the methodology of cybercrime forensics, really get enthusiastic about their subject and fully master it. The majority of open source tools have been developed for Linux/Unix platforms. Previous experience tells us that students can be easily discouraged by the potential complications of Linux and package installation on their own equipment. Masterkey Linux (www.masterkeylinux.com) is a live Linux system under development at Coventry University since 2007 and focused on incident response and computer forensics. It comes with a collection of software tools for imaging, data carving, forensic analysis and network analysis as well as other standard Linux applications as shown in Figure 1. With no installation required, the forensic system is started directly from a CD/DVD-ROM or USB drive of a computer and is fully accessible within minutes. Its open source nature and release under the GNU General Public License (GPL) allows its users to download, use and re-distribute it free of charge. With the help of virtual environment tools such as VMWare or VirtualBox, Masterkey Linux can run on a Windows, Mac OS X, or other Linux/Unix platform as a virtual machine, as illustrated in Figure 2. The unique feature of being able to use and switch between different operating systems on a computer without the need of rebooting the physical machine makes the process of teaching and learning cybercrime forensics convenient, time-saving and more enjoyable. Masterkey has been deployed as one of the tools in the teaching and learning of an undergraduate digital forensics module, 109SE Digital Forensics Fundamentals, at Coventry University since the 2008/9 academic year. Since both the University and the students in the class use the Microsoft Windows operating systems as the main working platform, a Masterkey virtual machine has also been prepared and distributed to the students in addition to a live CD/USB pen distribution of Masterkey. The Masterkey virtual machine appears as if it is a Windows application, making it very accessible and easy to use for the students. A mock cybercrime case was given to the students for their investigation and the approach of activity-led learning (ALL) was adopted. The feedback from the students has been very positive. Though the Masterkey Linux forensic system was originally developed for educational purposes, it can also be used by computer forensics professionals, system administrators, incident response individuals for computer-related incident response and investigation.

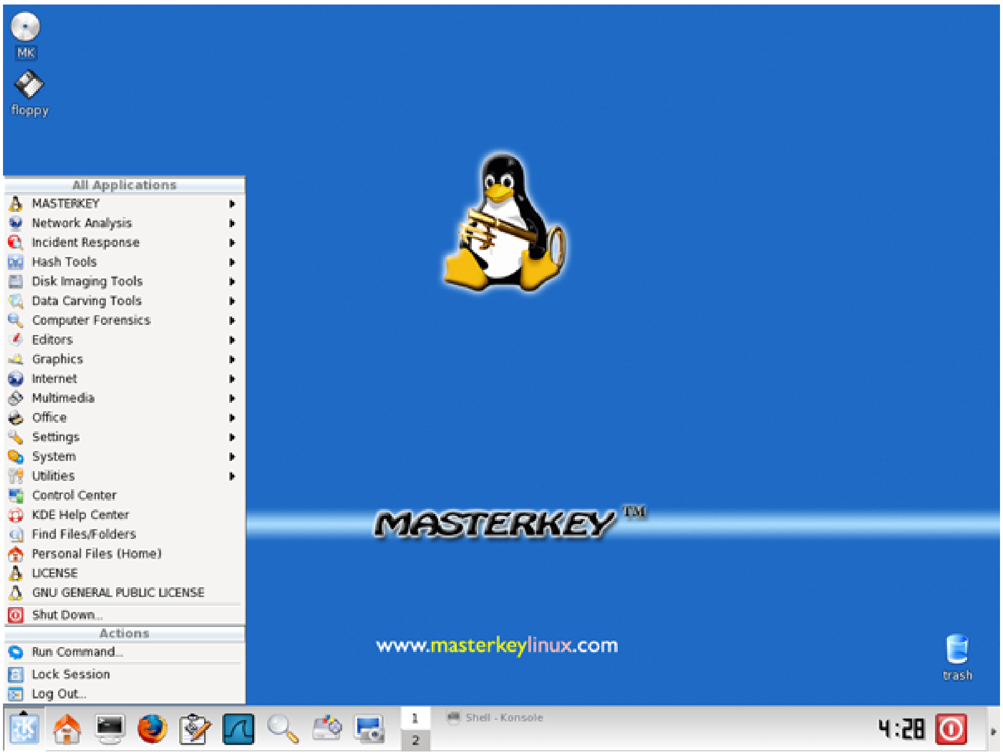


Figure 1 Masterkey Linux Live CD in Action

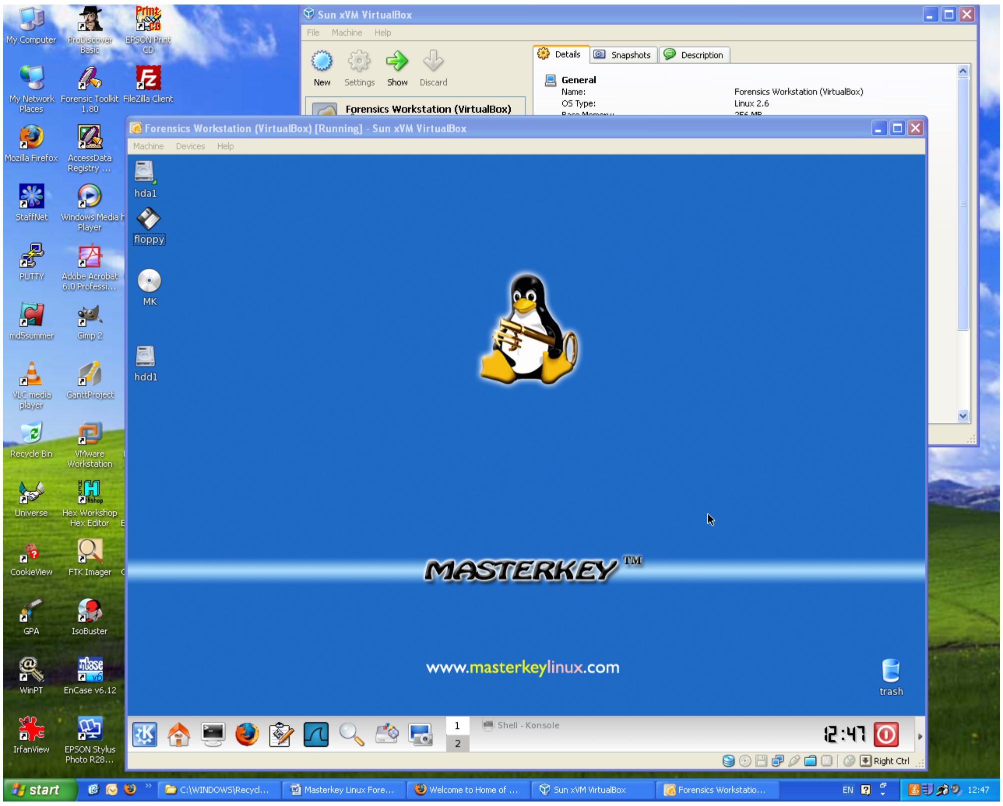


Figure 2 A Masterkey Virtual Machine Running on a Windows XP PC

Grid Computing for fighting Cybercrime

Abhaya Induruwa[1], Sarah Induruwa Fernando[2]
[1]Department of Computing
Canterbury Christ Church University
abhaya.induruwa@canterbury.ac.uk
[2]Computing Laboratory
University of Oxford
dak_62@hotmail.com

Abstract

Cybercrimes are committed around the globe in a large scale. It has become a billion pound illegal business. Cybercriminals have immense manpower resources, use advanced technologies and operate independent of socio-political and geographic borders. It is estimated that the loss in the US alone due to Unsolicited Bulk Email (UBE), also known as spam, is over USD 50 billion. The global impact is estimated to be well over USD 100 billion. Countering cybercrime requires significant technological and manpower resources. Among the available technologies Grid Computing has the potential to aid the criminal investigators by providing a distributed high throughput computing resource that could be utilised to tackle time consuming computational tasks such as data mining, pattern matching and examining the contents of large capacity disk drives with capacities in excess of terabytes, to name a few. This paper looks at the recent developments in the use of Grid Computing for fighting cybercrime.

A fast copy detection tool for forensic analysis of suspect documents

Authors: Austen Rainer, Peter Lane, James Malcolm
School of Computer Science, University of Hertfordshire, UK

Abstract

Over the last 8 years, researchers in the School of Computer Science at the University of Hertfordshire have developed a copy detection tool that very quickly identifies similar texts. For example, the diff tool requires O(n2 log n) time to process one pair of files, where n is the length of the input; by contrast, our copy detection tool requires an estimated O(n) time. The tool is language independent so, for example, the texts to be compared may be in human language (e.g. English or Arabic) or programming language (e.g. Java, C++). The tool works by computing a similarity metric between two documents specifying the degree to which the two documents are similar. The tool also highlights the portions of the texts that are similar. We believe that there are several potential applications of our copy detection tool to forensics. In this paper we explore two of those applications:

- Suspect documents (e.g. a hacking manual) which are written in a foreign language first need to be translated before they can be examined. Once a document has been translated and archived, our copy detection technology would be capable of quickly identifying similar documents (or fragments of documents) in the original language from a pool of documents (e.g. a hard disk). (The concept could also be applied to source code.)
- The copy detection technology constructs an index of each document being compared. The index cannot be used to 'reengineer' the original document. Therefore, the index can be used to efficiently and securely share information between cybercrime agencies about potential similar documents without having to share the source documents themselves. This would help agencies to collaborate on forensic investigations without revealing potentially confidential information that in so doing may, for example, contravene statutory law.

The proposed paper will explore these applications in more detail.

Survey of Eastern European Organised Cybercrime

Stephen McCombie[1], Paul Watters[2]
[1]Cybercrime Research Lab, Macquarie University,
North Ryde Australia
mccombie@science.mq.edu.au
[2] Internet Commerce Security Laboratory, University of Ballarat,
Mt Helen Australia
p.watters@ballarat.edu.au

Abstract

Phishing and related cybercrime is responsible for billions of dollars in losses annually. Gartner reported more than 5 million U.S. consumers lost money to phishing attacks in the 12 months ending in September 2008. This paper examines the part individuals and groups based out of Eastern Europe play in this problem. The Russian “Mafiya” in particular has been popularised by the media and entertainment industries to the point where it can be hard to separate fact from fiction. A well respected and leading security researcher Eugene Kaspersky, a Russian himself, charged that the view of the Russian Mafiya and Russians more generally being behind cybercrime was a “myth”. While the authors agree there is a degree of mythology around the issue there is some strong data pointing to the significant role Eastern Europeans’ play in the cybercrime world. This paper consists of a survey of some of the information available on this area. We take a particular focus on cybercrime from an Australian perspective as Australia was one of the first places where Phishing attacks against Internet banks were seen. In that case it is quite likely these attacks came from Ukrainian spammers. The survey is built from case studies both where individuals from Eastern Europe have been charged with related crimes or unsolved cases where there is some nexus to Eastern Europe. It also uses some earlier work done by the authors looking at those early Phishing attacks, archival analysis of Phishing attacks in July 2006 and new work looking at correlation between the Corruption Index, Internet penetration and educational levels in those countries which the authors believe supports this thesis. This is not meant as a xenophobic exercise but rather to inform and educate those charged with responding to cybercrime where at least part of the problem originates and try to understand why.

Closing the Gap for Open Source Image Handling: Acquisition, Verification and Loop-Mount of e01-type images on Linux systems; converting e01 or dd images into bootable virtual machines.

Jens Kirschner
Jens.Kirschner@7safe.com

Abstract

Computer Forensics as a profession is relying heavily on specialist tools; commonly proprietary and expensive even by closed-source software standards, they are often unaffordable for training purposes. Moreover, as they are closed-source, they may not even be useful in particular in academic environments where understanding of the underlying processes and methodologies is seen as more important than learning to use specific tools. For those reasons, academia tends to favour open source tools, free both in the financial as well as the intellectual property sense. Linux environments have thus long been used in academic environments to teach computer forensics; they have also found their way into professional use as alternative tools for dual-tool verification or in cases where commercial tools fail. Common Linux commands like dd, grep or md5sum have been cited as proof that Linux systems are natural candidates for computer forensics. Yet there is also quite commonly a belittling effect: The dd command creates raw disk images without compression, without additional header information, without integrated error detection or validation. Piping the dd output through bzip or gzip for compression is possible, of course, but results in files that will have to be decompressed before they can be imported into common forensic tools. This presentation will demonstrate several options available for Linux that are quite commonly overlooked when considering Linux for forensic acquisition, image verification or further processing. Based on the open source library libewf, which is available for Linux, BSD and Mac OS X environments, this presentation will demonstrate the acquisition and verification of so-called "EnCase images" employing both compression and built-in error detection. The presentation will then demonstrate how such e01-images can be mounted (similar to mounting an image as a drive in Windows) to access their contents in Linux without the need for commercial software.Finally, the open source virtualisation package QEMU offers a conversion command which will be employed to turn the image of a normal Windows XP system into a bootable VMware disk which can then be imported into VMware and booted virtually to see the system from the user's perspective. Using the free (though closed-source) virtualisation environment VMware Server, this will be an interesting option whether one's interest in computer forensics is professional or academic.

Qualcomm v. Broadcom: Illustrating the Need for a Computer Forensic Expert

Milton Luoma & Vicki Luoma
Assistant Professor Metropolitan State University Milt.Luoma@metrostate.edu
Associate Professor Minnesota State University Vicki.Luoma@mnsu.edu

Abstract

Laurie Miller MBA Student Indiana Wesleyan University In the Qualcomm v. Broadcom case attorneys attempted to comply with legal discovery requests by doing their own keyword searches on the documents subject to discovery. At the end of the trial it was revealed that Qualcomm failed to present approximately 200,000 pages of emails, memoranda, and other documents to Broadcom in the discovery process. The existence of these documents was revealed through the testimony of one of Qualcomm's last witnesses at trial, and most of the missing documents were not available until four months after trial. As a result of the failure of Qualcomm's lawyers to provide adequate discovery, the presiding federal judge in the United States District Court for the Southern District of California ordered that Qualcomm patents should be rendered invalid as to the world and fined the lawyers. With over 90% of all documents existing in electronic formats, should Broadcom have shouldered some of the blame for failure to make more appropriate and precise discovery requests that would have allowed their forensic experts to uncover these documents? The United States Federal Rules of Civil Procedure require the parties to "meet and confer" and the litigants to identify and list all electronic data sources. This case underscores the importance of litigants' understanding of the nature of electronically stored information, how it is stored and retrieved, and most importantly, when a computer forensic expert is necessary in the electronic discovery process. This paper addresses these issues and offers recommendations.

Cyber Fraud in Ghana locally known in the Hausa language as "SAKAWA"
An ethnographic Study of a Popular Slum community in Ghana-Nima

Koranteng, Kweku Oduro
Information Communication Technology Directorate,
University of Ghana, Legon. P.O. Box LG25, Legon
kkoranteng@ug.edu.gh, kweku.koranteng@gmail.com

Abstract

Cyber crime as an area of study has received little or no attention in developing countries round the world where significant proportions of these Internet crimes take place. One of the major issues battling the advancement of Information and Communication Technology in developing countries in general has been the non-existing regulatory framework to control and monitor the advancement ICT in respective countries. In Ghana, like many other developing countries, enforcement and regulation of laws in this area has been a daunting task. Even though Ghana is among the very few African countries with a draft policy on ICT, the issue with regulation has been viewed with lots of skepticism in many quarters. Notwithstanding these setbacks, Governments of Ghana is still poised to ensure equity in the implementation of its ICT programs and policies to facilitate the development of its economy. Government over the years have come to the realization that before their economies can reap total benefit of global economic business exchange in this 21st century, they will have to bring their segmented economies onto a global platform through ICT. Nonetheless, the indispensable nature of ICT in Ghana's economic development has triggered series of policy formulation in other sectors of the economy. National ICT policies formulated in 2005 did set in motion a good basis for the development of ICT in all sectors; education, health care delivery, governance etc. Despite the great strides made by national governments to ensure equitable access to ICT infrastructure, much attention is not paid to the threat these technologies pose to national security and state sovereignty. African Cyber crime Enterprises, for that matter West African Cyber crime syndicates are among one of the most active and vibrant crime syndicates in the world. Significant among these are the Nigerian Cyber crime Enterprises. Ghana, the first black sub-Saharan to gain independence from Britain in 1957, one of the emerging economies in Africa today, and referred to in many economic quarters as the gateway to West Africa, is rather and gradually becoming a safe haven for the perpetuation of all forms of crimes; illegal migration, drug-traffic and cyber related crimes. The research takes an ethnographic view of cyber fraud carried out in Ghana, specifically within a slum community in Ghana-Nima, which is noted as one of the most notorious hideout for most West African migrant. 'Nima' as the slum is called, geographically, lays in the heart of the Accra the capital of Ghana and about 15 minutes drive from the Kotoka International Airport. The total population size of this community is estimated to be about 50,000 inhabitants. Nima extends into neighbouring communities such as Kokomlemle, Malata, Kanda, New Town, Pigfarm, Kotobabi and Mamobi

Sponsor - Canterbury Christ Church University

The Department of Computing plays host to the CFET 2009 conference based at the North Holmes Road Campus of Canterbury Christ Church University.

The Department comprises of 10 full-time and 7 part-time staff running undergraduate and 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 January 2007 the Department secured HEFCE funding for a two year project to promote the development of Cybercrime research in the awards both within the staff and students studying the subject. Part of this development included hosting the 1st International Conference of Cybercrime Forensics Education and Training CFET 2007.

In 2008 after hosting CFET 2008 Denis Edgar-Nevill was invited to put forward a proposal to the BCS to form the BCS Cybercrime Forensics Specialist Group. This was approved and the Department hosted the Inaugural Meeting in December 2008. Selected papers from CFET 2008 appeared in May 2009 as a special edition of the International Journal of Digital 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

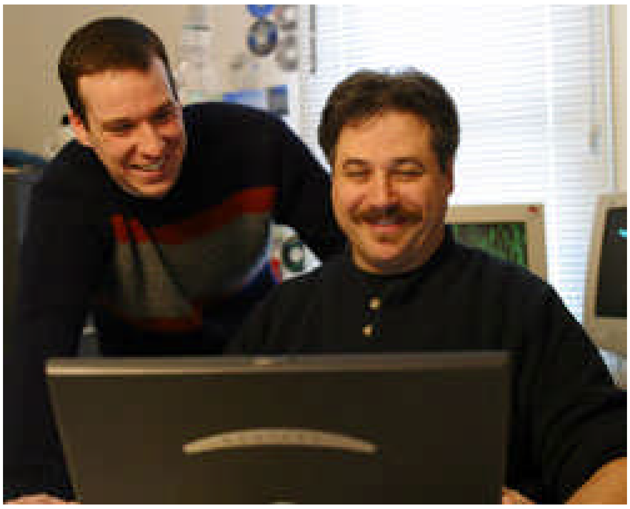
Provincial post-secondary institute, founded under College & Institute Act, for Justice & Public Safety education in 1978, by Dr. Patrick McGeer, Minister of Education. Its mission is to provide Innovative education and training for those who make communities safe. Its vision is to be a world leader 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 – Champlain College, USA

Founded in 1878, Champlain College is a private, baccalaureate institution that offers professionally focused programs balanced by a strong core curriculum. The College is a national leader in educating students to become skilled practitioners, effective professionals and global citizens.

Created in 2006, the Champlain College Centre for Digital Investigation (C3DI) has a charter to assist law enforcement agencies in Vermont and throughout the nation, particularly in areas related to computer forensics and other digital investigations. This goal is being achieved through a number of initiatives and partnerships between academia, the public sector, and the private sector.

The C3DI has been made possible by funding from the U.S. Department of Justice Bureau of Justice Assistance (BJA) and Champlain College, as well as material support from the Burlington Police Department and the Vermont Internet Crimes Task Force (ICTF).



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 – Micro Systemation

MICRO SYSTEMATION

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

.XRY

www.msab.com

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 – British Computer Society Cybercrime Forensics Specialist Group

“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

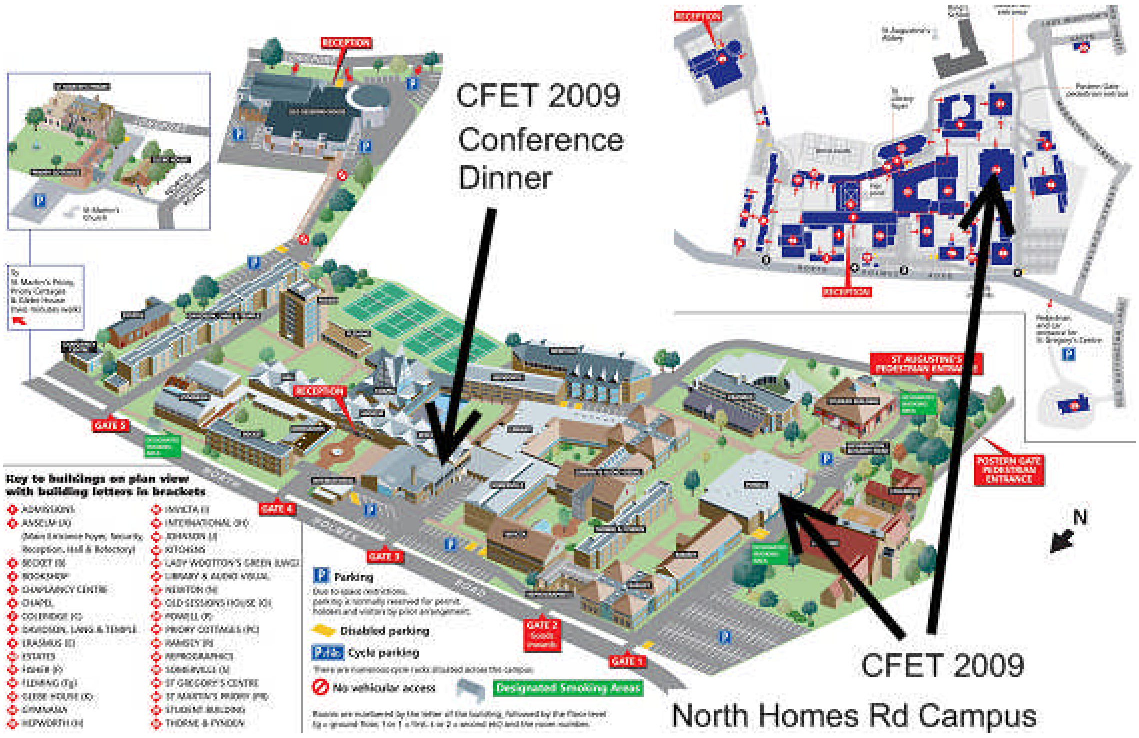
(as of 12th August 2009)

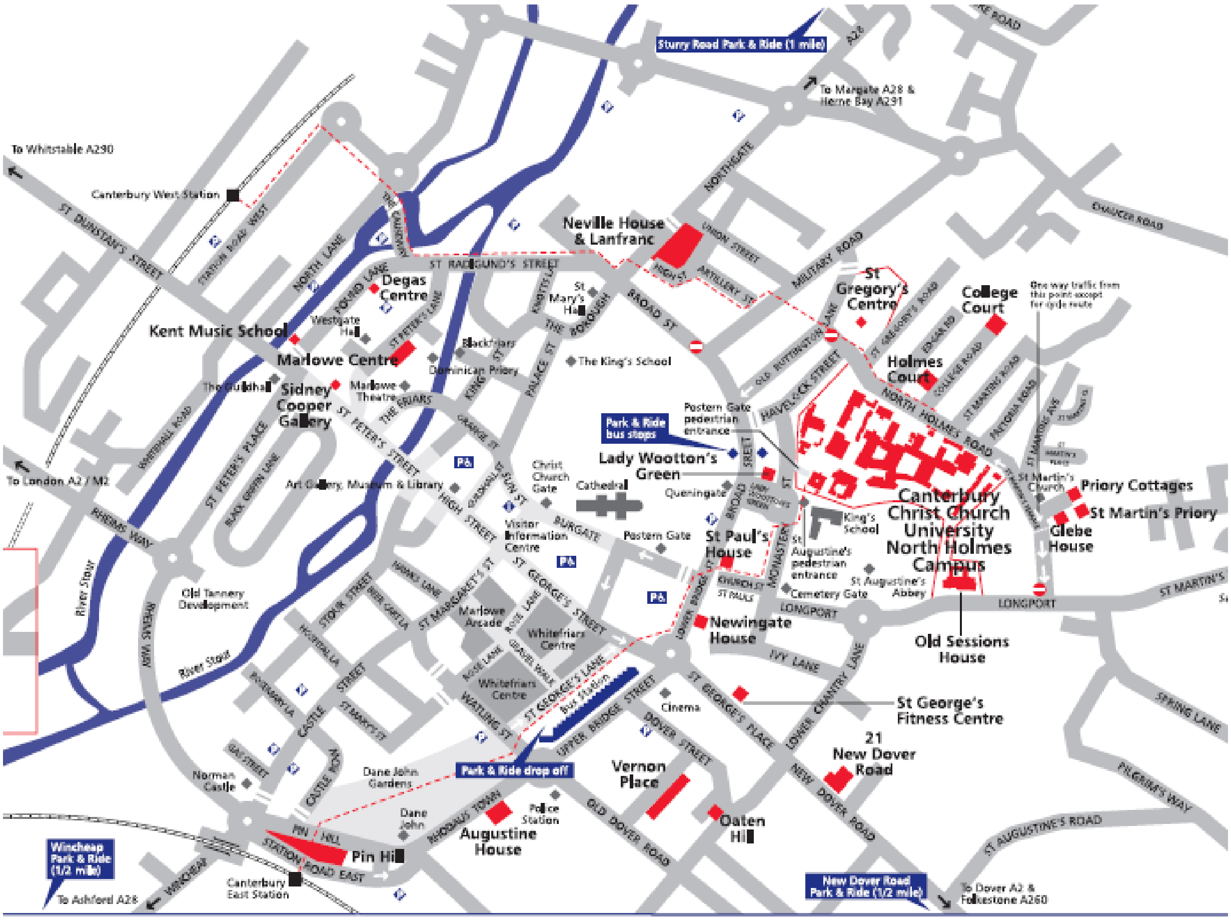
SURNAME	FIRST NAME	ORGANISATION	COUNTRY
Abouzakhar	Nasser	University of Hertfordshire	UK
Baigent	Jon	Baigent's IT Solutions & Data Recovery	UK
Bates	Danny	Police/MSc Cybercrime Forensics	UK
Beckett	Phil	Navigant Consulting (Europe) Limited	UK
Bowden	Lucy	Canterbury Christ Church University	UK
Brighouse	Brian	Canterbury Christ Church University	UK
Brokenshire	James	MP Hornchurch	UK
Bryant	Robin	Canterbury Christ Church University	UK
Callaghan	Anthony	Canterbury Christ Church University	UK
Calvert	Maurice	Leeds Metropolitan University	UK
Case	Nicola	Norman Data Defense Systems	UK
Cassell	Michael	Canterbury Christ Church University	UK
Chibelushi	Caroline	University of Wolverhampton	UK
Childs	David	Police/MSc Cybercrime Forensics	UK
Crellin	Jonathan	University of Portsmouth	UK
Daley	Michael	Cardiff University	UK
De Zoysa	Tirimadura	University of Colombo	Sri Lanka
Dickinson	Muike	MSAB	UK
Dipple	Chris	Motte Technology	UK
Drew	Simon	Canterbury Christ Church University	UK
Dube	Robet	Roehampton University London	UK
Edgar-Nevill	Denis	Canterbury Christ Church University	UK
Edgar-Nevill	Val	Canterbury Christ Church University	UK
Edwards	Steve	eBay	UK
Freeman	Christopher	Canterbury Christ Church University	UK
Gay	James	PhD Student	UK
Gibson	Ed	Microsoft	UK
Goodman	Marc	Impact	UK
Goonatillake	Keerthi	University of Colombo	Sri Lanka
Grave	Lucy	RTL	UK
Gregory	Prezhneve	Mobitel (Pvt) Ltd	Sri Lanka
Hargreaves	Christopher	Cranfield University	UK
Harley	David	Malware Intelligence	UK
Harris	Doug	University of Texas	USA
Hawkins	Andrew	MSc Cybercrime Forensics	UK
Hoolachan	Sheona	University of Glasgow	UK
Induruwa	Abhaya	Canterbury Christ Church University	UK
Jones	Nigel	University College Dublin	Ireland
Kirschner	Jens	7safe	UK
Konstadopoulou	Anastasia	University of Bradford	UK

Koranteng	Kweku	University of Ghana	Ghana
Luoma	Milton	Metropolitan State University	USA
Luoma	Vicki	Minnesota State University	USA
Malcolm	James	University of Hertfordshire	UK
Marsh	Steve	University of Wales Institute, Cardiff	UK
McCoy	Hannal	Canterbury Christ Church University	UK
Mills	Marc	University of Huddersfield	UK
Mousoli	Reza	Canterbury Christ Church University	UK
Munro	Lawrence	Kingston University	UK
Nichol	James	Essex Police/MSc Cybercrime Forensics	UK
Norris-Jones	Lynne	University of Wales Institute, Cardiff	UK
Obluk	Karel	AVG Technologies	Czech Rep
Overill	Richard	Kings College London	UK
Pavlidis	Nikolaos	University of Bedfordshire	UK
Putman	Richard	Sector Forensics	UK
Qi	Man	Canterbury Christ Church University	UK
Rainer	Austen	University of Hertfordshire	UK
Ross	Margaret	Southampton Solent University	UK
Sage	Matthew	Canterbury Christ Church University	UK
Simpson	Chris	NPIA	UK
Staples	Geoff	Southampton Solent University	UK
Stephens	Paul	Canterbury Christ Church University	UK
Stock	Gerald	Canterbury Christ Church University	UK
Thorne	Tim	Police/MSc Cybercrime Forensics	UK
Tubby	Matthew	Canterbury Christ Church University	UK
Turville	Kylie	University of Ballarat	Australia
Uhomoibhi	James	University of Ulster	UK
Valli	Craig	Edith Cowan University	Australia
Watters	Paul	University of Ballarat	Australia
Williams	Geraint	University of Bedfordshire	UK
Zhou	Qin	Coventry University	UK
Zwienenberg	Richard	Norman Data Defense Systems	UK

Copyright Statement

Maps of the Venue


CFET 2009
Conference
Dinner
CFET 2009
North Homes Rd Campus
RECEPTION
GATE 5
GATE 4
GATE 3
GATE 2
Goods inwards
GATE 1
ST AUGUSTINE'S PEDESTRIAN ENTRANCE
POSTERN GATE PEDESTRIAN ENTRANCE
N
Key to buildings on plan view
with building letters in brackets
ADMISSIONS
ANSELM (A)
(Main Entrance Foyer, Security, Reception, Hall & Refectory)
BECKET (B)
BOOKSHOP
CHAPLAINCY CENTRE
CHAPEL
COLERIDGE (C)
DAVIDSON, LANG & TEMPLE
ERASMUS (E)
ESTATES
FISHER (F)
FLEMING (Fg)
GLEBE HOUSE (G)
GYMNASIA
HEPWORTH (H)
INVICTA (I)
INTERNATIONAL (IH)
JOHNSON (J)
KITCHENS
LADY WOOTTON'S GREEN (LWG)
LIBRARY & AUDIO VISUAL
NEWTON (N)
OLD SESSIONS HOUSE (O)
POWELL (P)
PRIORY COTTAGES (PC)
RAMSEY (R)
REPROGRAPHICS
SOMERVILLE (S)
ST GREGORY'S CENTRE
ST MARTIN'S PRIORY (PR)
STUDENT BUILDING
THORNE & FYNDON
Parking
Disabled parking
Cycle parking
No vehicular access
Designated Smoking Areas


Sturry Road Park & Ride (1 mile)
To Margate A28 & Herne Bay A291
To Whitstable A290
Canterbury West Station
Neville House & Lanfranc
St Gregory's Centre
College Court
One way traffic from this point except for cycle route
Degas Centre
Kent Music School
Westgate Hall
Marlowe Centre
Blackfriars
Dominican Priory
The King's School
Holmes Court
The Guildhall
Sidney Cooper Gallery
Marlowe Theatre
Postern Gate pedestrian entrance
Park & Ride bus stops
Lady Wootton's Green
Art Gallery, Museum & Library
Christ Church Gate
Cathedral
Queningate
Canterbury Christ Church University North Holmes Campus
Priory Cottages
St Martin's Priory
Glebe House
To London A2 / M2
Visitor Information Centre
Postern Gate
St Paul's House
King's School
St Augustine's pedestrian entrance
St Augustine's Abbey
Cemetery Gate
Old Tannery Development
Newingate House
Old Sessions House
Marlowe Arcade
Whitefriars Centre
Bus Station
Cinema
St George's Fitness Centre
21 New Dover Road
Norman Castle
Dane John Gardens
Park & Ride drop off
Vernon Place
Police Station
Oaten Hill
Augustine House
Pin Hill
Wincheap Park & Ride (1/2 mile)
To Ashford A28
Canterbury East Station
New Dover Road Park & Ride (1/2 mile)
To Dover A2 & Folkestone A260
River Stour
ST DUNSTAN'S STREET
NORTH LANE
ST RADIGUND'S STREET
NORTHGATE
UNION STREET
MILITARY ROAD
CHAUCER ROAD
BROAD ST
NORTH HOLMES ROAD
HIGH STREET
ST PETER'S STREET
BURGATE
ST GEORGE'S STREET
LONGPORT
ST MARTIN'S
IVY LANE
LOWER CHANTRY LANE
NEW DOVER ROAD
OLD DOVER ROAD
ST AUGUSTINE'S ROAD
SPRING LANE
PILGRIM'S WAY
RHEIMS WAY
WINCHEAP
STATION ROAD EAST
CASTLE ST
WATLING ST
UPPER BRIDGE STREET
DOVER STREET
ST GEORGE'S PLACE