CFET 2012

6th 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
6th & 7th September 2012

ISBN 978-1-899253-94-4

Contents

Introduction to the Conference

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

This conference invited papers and presentations on the following:

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

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

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

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

Denis Edgar-Nevill
Chair, CFET 2012

Copyright Statement

Conference Organisers

Conference Chair

Denis Edgar-Nevill Canterbury Christ Church University

Conference Organising Committee

Dr Man Qi Canterbury Christ Church University

Dr Abhaya Induruwa Canterbury Christ Church University

Matthew Tubby Canterbury Christ Church University

International Advisory Panel

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

Professor. Joe Carthy University College Dublin, Republic of Ireland

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

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

Bill Crane Adjunct Professor, Champlain College, Vermont, USA

Dr. Rob D'Ovidio Drexel University, USA

Denis Edgar-Nevill Head of Department (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 Technology Risk Ltd/Visiting Professor, Canterbury Christ Church University, UK

Dr Manolya Kavakli Department of Computing, Macquarie University, Australia

Dr Gary C. Kessler Gary Kessler Associates, USA

Jack McGee President, Justice Institute of British Columbia, Canada

Theo Derksen Police Academy of the Netherlands, Netherlands

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

Edward Gibson Director, Colead Cybercrime Practice, Forensic Services, PwC, USA

Jens Kirschner Director—Jens Training Ltd, UK

Professor Bill Buchanan School of Computing, Edinburgh Napier University, Director Centre for Distributed Computing, UK

Dr Richard Overill Kings College London, UK

Conference Programme

Day 1 – 6th September 2012

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

10.30 - 10.45 **Welcome to the University and Conference – Ramsey Lecture Theatre**

Dr Janet Haddock-Fraser
Dean, Faculty of Social & Applied Sciences
Canterbury Christ Church University, UK

Denis Edgar-Nevill, Chair CFET 2012
Head of Department Computing
Canterbury Christ Church University, UK

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

"Training at the Dutch Police Academy and Digital Forensic Training Programme New Developments and Involvement in ISEC and ECTEG"
Theo Derksen and Alwin Hilbrink
Police Academy of the Netherlands

11.30 – 13.00 **Parallel Presentation Sessions**

Ramsey Rg31 (Chair – Dr Man Qi)

11.30 – 12.15 ***"Cross-Drive Analysis Using Automated Digital Forensic Timelines"***
Chris Hargreaves
Cranfield University

12.15 – 13.00 ***"Do state-of-the-art forensic image processing techniques address the problem of policing photographic data in the current file sharing culture?"***
Susan Welford and Dr Stuart Gibson
University of Kent

Ramsey Rg36 (Chair – Dr Abhaya Induruwa)

11.30 – 12.15 ***"FUD and Blunder: Tracking PC Support Scams"***
David Harley, Martijn Grooten, Steve Burn, Craig Johnston
ESET, Virus Bulletin, MalwareBytes, Sophos

12.15 – 13.00 ***"BYOD:(B)rought (Y)our (O)wn (D)estruction?"***
Righard J. Zwienenberg
ESET

13.00 - 14.00 **Lunch**

14.00 – 14.45 **Invited Keynote Presentation – Ramsey Lecture Theatre**

"The European Cybercrime Centre (EC3)"

Mikael Lindstrom
EUROPOL

14.45- 16.00 **Parallel Presentation Sessions**

Ramsey Rg31 (Chair – Dr Man Qi)

14.45 – 15.30 ***"Textual Analysis as a Digital Forensic Tool"***
George R S Weir
University of Strathclyde

Ramsey Rg36 (Chair – Dr Abhaya Induruwa)

14.45 – 15.30 ***"On the Digital Forensic Analysis of the Firefox Browser Via Recovery of SQLite Artifacts from Unallocated Space"***
R.I. Ferguson, P. Leimich and R. Bagley
University of Abertay

15.30 - 16.00 **Coffee - foyer Ramsey Building**

16.00 - 17.30 **AGM BCS Cybercrime Forensics Specialist Group** (Open meeting)
Ramsey Lecture Theatre

16.00-16.15 Review of the last year
16.15-16.25 Committee Elections (BCS members only)
16.30-17.30 **"*ECENTRE—England's Cybercrime Centre of Excellence Network for Training, Research and Education"***

Denis Edgar-Nevill
Canterbury Christ Church University
Chair, BCS Cybercrime Forensics SG

17.30 – 18.30 **BCS Cybercrime Forensics SG Committee Meeting** (Closed meeting)
Ramsey Rg31

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

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

Day 2 – 7th September 2012

09.00 – 10.00 **Parallel Presentation Sessions**

Ramsey Rg31 (Chair – Dr Man Qi)

09.00-09.30	***"A Targeted Malicious Email (TME) Attack tool"*** Tuan Phan Vuong, Diane Gan University of Greenwich
09.30-10.00	***"An Analysis of Hotmail Artefacts in Firefox 9"*** Anne David Cranfield University

Ramsey Rg36 (Chair – Dr Abhaya Induruwa)

09.00-09.30	***"Virtual Crime: Forensic Artefacts from Second Life"*** Sarah Morris Cranfield University
09.30-10.00	"***A Forensics Approach to Digital Fingerprinting on Windows Servers"*** Christie Oso and Diane Gan University of Greenwich

10.00 – 10.30 **Coffee - foyer Ramsey Building**

10.30 – 11.15 **Invited Keynote Presentation – Ramsey Lecture Theatre**

"Mobile Phone Forensics at PSNI"

Peter Salter
Police Service Northern Ireland

11.15- 13.00 **Parallel Presentation Sessions**

Ramsey Lecture Theatre (Chair – Denis Edgar-Nevill)

11.15-11.50	***"Intensive Teaching of Cyber Security For Mid-Career Physical Security Professionals With Limited Academic Background"*** Chadwick D, Loukas G, Gan D, Frangiskatos D University of Greenwich
11.50-12.25	*"**A Simple Enterprise Security Architecture (SESA): Towards a Pedagogic Architecture for Teaching Cyber Security"*** Harjinder Singh Lallie University of Warwick
12.25-13.00	***"A Forensic Image Description Language for Generating Test Images"*** Dr Gordon Russell & Robert Ludwiniak Napier University

Ramsey Rg31 (Chair – Dr Abhaya Induruwa)

11.15-11.50 ***"From Criminal to Digital Criminal Profiling: Advances in Criminal Profiling in the Digital Age"***
Georgios Chlapoutakis
Expert Witness in Digital Forensics

11.50-12.25 ***"The Utilisation of the Unified Modelling Language in Digital Forensic Science"***
Peter Forster
Cranfield University

12.25-13.00 ***"VoIP Forensics"***
Abhaya Induruwa & Nathan Attoe
Canterbury Christ Church University

Ramsey Rg36 (Chair –Dr Man Qi)

11.15-11.50 ***"Towards a Science of Digital Forensics"***
Clive Blackwell
Oxford Brookes University

11.50-12.25 ***"A Comprehensive Methodology for Profiling Cyber Criminals"***
Hemamali Tennakoon
Kingston University

12.25-13.00 ***"Social Media in Law Enforcement: the Role and Issues"***
Dr Man Qi
Canterbury Christ Church University

13.00 - 14.00 **Lunch**

14.00 – 14.45 **Invited Keynote Presentation – Ramsey Lecture Theatre**
"Update of 2Centre Network of Centres of Excellence"

Professor Nigel Jones
Technology Risk Ltd/Canterbury Christ Church University

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

15.30—16.00 **Coffee - foyer Ramsey Building**

1600 **Conference Close**

Presentation Abstracts – 6th September 2012

Invited Keynote Presentation

Training at the Dutch Police Academy and Digital Forensic Training Programme New Developments and Involvement in ISEC and ECTEG

Theo Derksen and Alwin Hilbrink
Police Academy of the Netherlands

POLITIE

• Politieacademie

The Police Academy of the Netherlands is a School of Professional Education that offers fully accredited bachelor and master degree programs in Policing and Criminal Investigation techniques. The Police Academy is the official training centre for the Dutch Police. Most programs can be studied in part-time, full time or in blended learning formats.

The Police Academy of the Netherlands is the centre of excellence in Policing issues in the Netherlands. It is a dynamic organisation that offers education and knowledge at a high level, anticipates social trends and can translate these into tailor-made training. The Academy cooperates with the police forces and many partner organisations in the field of safety & security, education, knowledge and research.

Policing is of course an international affair. With the progressive internationalization of society this will even be more so in the future. Police forces across Europe form partnerships in order to fight and prevent crime. For police officers from abroad, there are opportunities to take part in courses offered by the Police Academy of the Netherlands. These courses are taught in English

Cross-Drive Analysis Using Automated Digital Forensic Timelines

Chris Hargreaves
Cranfield University

Abstract

Cross-Drive Analysis (CDA) is a technique designed to allow an investigator to "simultaneously consider information from across a corpus of many data sources" (Garfinkel 2006). Existing approaches include correlation of data obtained on multiple drives through text searching, e.g. email addresses, message IDs, credit card numbers or social security numbers. Such techniques have the potential to identify drives of interest from a large set, provide additional information about events that occurred on a single disk, and potentially determine social network membership.

Another analysis technique that has significantly advanced in recent years is the use of timelines. Tools currently exist that can extract dates and times from the file system metadata (i.e. MACE times) and also examine the content of certain file types and extract metadata from within those (Guðjónsson 2010; Carbone & Bean 2011; Olsson & Boldt 2009). This approach provides a great deal of data that can assist with an investigation, but also compounds the problem of having too much data to examine.

A recent paper adds an additional timeline analysis capability, by automatically producing a high-level summary of the activity on a computer system, by combining sets of low-level events, into high-level events, for example reducing a setupapi event and several events from the Windows Registry to a single event of 'a USB stick was connected'.

This paper provides an investigation into the extent to which events in such a high-level timeline have the properties suitable to assist with Cross Drive Analysis. The paper provides several examples that use timelines generated from multiple disk images, including a USB stick connected to multiple systems, Skype calls, and email exchanges.

References

Carbone, R. & Bean, C., 2011. Generating Computer Forensic Super Timelines Under Linux. pp.1– 136.

Garfinkel, S.L., 2006. Forensic feature extraction and cross-drive analysis. Digital Investigation, 3(Supplement 1), pp.71–81.

Guðjónsson, K., 2010. Mastering the Super Timeline with log2timeline. pp.1–84.

Olsson, J. & Boldt, M., 2009. Computer forensic timeline visualization tool. Digital Investigation, 6 (Supplement 1), pp.S78–S87.

Do State-of-the-Art Forensic Image Processing Techniques Address the Problem of Policing Photographic Data in the Current File Sharing Culture?

Susan Welford and Dr Stuart Gibson
Forensic Imaging Group, University of Kent
Canterbury, Kent, CT2 7NZ

Abstract

With continuing progress and improvements in the field of digital photography and the vast array of, and widely available photo-editing software, verification techniques play a significantly important position in terms of identification and security. This paper presents an evaluation of the current camera verification techniques and looks at some future possibilities in the field. Verification is the process by which the truth, accuracy or validity of something is established. Camera verification is therefore the act of providing as proof or evidence for, and confirming the validity of the particular camera in question as being the device from which an image originated.

In this paper, we examine the five categories of verification techniques: sensor pattern noise; analysis of DCT coefficients; DQT; EXIF headers or watermarks; and lens aberrations. The *sensor pattern noise* technique measures the correlation between the relative fingerprint of the camera's image sensor and the comparative fingerprint embedded within the evidential image. Analysis of *DCT coefficients* is a measure of lossless JPEG compression within a camera upon the output image. The resultant histograms of DCT coefficients used can aid in the identification of the camera used to produce the image. Detection of double JPEG lossless compression using *Discrete Quantisation Tables (DQT)* can help to identify both the primary compression and secondary compression and therefore the camera that originally captured the image. *Exchangeable Image File Format (EXIF)* is a header that details information relating to the image such as digital camera make, model, exposure data, GPS location, and date and time of capture. In high-end cameras, watermarks are embedded into images containing information similar to EXIF headers with the addition of biometric data relating to the photographer. Finally, *lens aberration* is in reference to the camera's optical system and its inability to flawlessly focus light of different wavelengths leading to imperfections. Measuring these imperfections can give support to the identification of individual camera lens systems.

Individual results for these techniques show them to be feasible procedures in source camera verification with varying degrees of success. The credibility of any digital image used as evidence within a court of law rests on the ability of the professionals to be able to prove and verify the image. Successful collaboration of some, if not all, of the above techniques would be a useful tool within image forensics to add extra weight to, and be able to validate an image and gain the advantage over the manipulators. However, further investigation is required to ascertain the robustness of these techniques in the ability to verify images that have been shared, i.e. over mobile networks or via social networking websites.

FUD and Blunder: Tracking PC SupportScams

David Harley, ESET North America, Martijn Grooten, Virus Bulletin
Steve Burn, MalwareBytes, Craig Johnston, Sophos Pty Ltd

Abstract

Fake security products are not just an attack on the victim's credit card: while the main driver of nearly all malware authoring nowadays is profit, fake security is also an attack on the credibility and effectiveness of the real security industry. The attack is not restricted to scareware and other utilities without utility and constantly morphing malicious binaries, either: it's carried out on many levels, though not necessarily by the same gangs:

- Threatened or actual legal action from cease-and-desist letters to court action in order to hamper the effectiveness and credibility of the security community;
- PR-oriented activities such as forum, email and blog spamming, blogs and articles proclaiming the legitimacy of a dubious product;
- Quasi-legitimate marketing, online support structures, and pricing models that mimic - or parody - the models used by the security industry;
- The semi-fraudulent selling-on of legitimate but free products and services;
- The increasingly sophisticated use and misuse of social media bolstering traditional Black Hat Search Engine Optimization.

Fake security products, supported by variations on Black Hat SEO and social media spam constitute a longstanding and well-documented area of cybercriminal activity. By comparison, lo-tech Windows support scams receive less attention, perhaps because they're seen as primarily social engineering not really susceptible to a technical "anti-scammer" solution. Yet they've been a consistent source of fraudulent income for some time, and have quietly increased in sophistication. But in recent years the battlefield has been broadening far beyond the highly adaptive technical attacks that characterize malware-based attacks: increased volumes, sophistication and infrastructural complexity of cold-call support scams prove that social engineering with a minimum of programmatic content can be as profitable as unequivocally malware-based attacks: lo-tech attacks with hi-tech profits. Here, we consider the evolution of the FUD and Blunder approach to cold-calling support scams, from "Microsoft told us you have a virus" to technically sophisticated hooks such as deliberate misrepresentation and misinterpretation of output from system utilities such as Event Viewer, Assoc, Prefetch and Inf. Next, we look at the developing PR-orientated infrastructure behind the phone calls:

- deceptive company web sites;
- flaky Facebook pages;
- scraped informational content and fake testimonials.

We discuss some of the interaction we've had with scammers, scammer and scam-victim demographics, and scammer techniques, tools and psychology, as gleaned from conversational exchanges and a step-through remote cleaning and optimization session with a particular scammer. We go on to the resemblances between the support scam industry, other telephone scams, and the security fakery associated with mainstream malware. And finally we ask where the scammers might go next, what are the legal implications, and how can the industry best help the user distinguish between "good" and "bad" products and services? In the absence of a technical attack susceptible to a technical defence, are education and reverse victimology the only answer?

BYOD:(B)rought (Y)our (O)wn (D)estruction?

Righard J. Zwienenberg
Senior Research Fellow
ESET, spol. s r.o.
mailto://righard.zwienenberg@eset.com

Abstract

Nowadays most employees bring their own internet-aware devices to work. Employers and institutions such as schools think they can save a lot of money having their employees or students use their own kit. But is that true, or are they over-influenced by financial considerations? There are so many pros and cons to the BYOD trend. The sheer range of different devices that might need to be supported can cause problems, not all of them obvious. The paper will list pros and cons, including those for internet-aware devices that people do not think of as dangerous or even potentially dangerous. These devices are often 'powered' by applications downloaded from some kind of App-Store/Market. The applications there are assumed to be safe, but should they be? What kind of risks do they pose for personal or corporate data? Furthermore, the paper will describe different vectors of attack towards corporate networks and the risk of intractable data leakage problems: for example, encryption of company data on portable devices is by no means common practice. Finally, we offer advice on how to handle BYOD policies in your own environment and if it is really worth it. Maybe "Windows To Go", a feature of Windows 8 that boots a PC from a Live USB stick which contains Win8, applications plus Group Policies applied by the admin, is a suitable base model for converting BYOD into a Managed By IT Device. Remember: BYOD isn't coming to us, it is here already here and it is (B)ig, (Y)et (O)utside (D)efense perimeters!

Biography:

Zwienenberg started dealing with computer viruses in 1988 after encountering the first virus problems at the *Technical University of Delft*. His interest thus kindled, Zwienenberg has studied virus behaviour and presented solutions and detection schemes ever since. Initially he started as an independent consultant, in 1991 he co-founded *CSE Ltd.* where he was the Research and Development Manager. In October 1995, Zwienenberg left *CSE* and one month later he started at the Research and Development department of *ESaSS BV* – developers of ThunderBYTE. In 1998, *Norman Data Defense Systems* acquired *ESaSS* and Zwienenberg joined the Norman Development team to work on the scanner engine. In 2005 Zwienenberg took the role of Chief Research Officer at Norman. After AMTSO was formed, Zwienenberg was chosen as its president. He is serving as a Vice-President of AVAR and on the Technical Overview Board of the WildList. Zwienenberg left Norman in 2011 looking for new opportunities and started as a Senior Research Fellow at ESET, spol. s r.o. Zwienenberg has been a member of CARO since late 1991. He is also vice-president of AVAR. He is a frequent speaker at conferences – among these Virus Bulletin, EICAR, AVAR, RSA, InfoSec, SANS, CFET, Government Symposia, SCADA seminars, etc - and seminars. His interests are not limited to viruses but have broadened to include general security issues and encryption technologies over the past years.

Invited Keynote Presentation

The European Cybercrime Centre (EC3)

Mikael Lindstrom
EUROPOL

Abstract

The European Cybercrime Centre (EC3) will open its doors on 1st January 2013. Building on Europol's existing work to combat online fraud, cyber-attacks and child sexual exploitation, it will strengthen law enforcement's information position, provide greater levels of operational support, build capacity and serve as the collective voice of cybercrime investigators. Ultimately, the aim is to make Europe smarter, faster and stronger in the fight against cybercrime. This presentation will briefly describe how we intend to do this, how you can help and - most importantly - how you should benefit from EC3.

Textual Analysis as a Digital Forensic Tool

George R S Weir
University of Strathclyde

Abstract

Software tools are the stock and trade of the digital forensic analyst. Most software is used in detection or analysis of digital information. But such information is often low level and requires interpretation on the part of the analyst in order to comprehend its relevance to the 'bigger picture'. This is no less true when dealing with text-based information rather than checksums, timelines, file types or browser histories. This lesson is important as increasingly, cybercrime investigators must explore collections of textual evidence. Sets of email messages, stored correspondence or company documents may contain significant information that indicates the commission of a criminal offence or points to an individual as agent of an offence. In common with other contexts of digital investigation, the quantity of information often demands automated processing and analysis in order to be practicable.

Students of digital forensics may assume that modern textual analysis tools afford insights on texts and text collections that simplify such investigations. Applied Linguistics is a relevant field of study that has a wide relevance to language-based investigations. Obvious applications range from spam detection, document forensics and authorship analysis.

In fact, the reality with such software tools is analogous to the general situation with forensic data analysis software. A common characteristic is generation of much low level data with little or no support for gaining broader perspectives on the contexts represented by the data or the data analysis.

This paper describes the use of the Posit Textual Analysis Tools as a teaching aid in the context of email and document analysis. Posit (developed by the present author) is a set of software tools that support the quantitative analysis of individual texts. A significant component in this analysis is the integration of a part-of-speech tagger. This allows the textual analysis to consider part-of-speech patterns within (or between) texts. In addition, Posit supports vocabulary analysis in terms of multi-word units, ranging from 1 to 5-word units. Applying Posit to any substantial text generates a series of data analyses that have the prospect of shedding light on document characteristics.

In applying Posit to the context of digital forensic teaching, The learning objective is twofold. Firstly, to identify settings in which such analyses should prove insightful. Secondly, to establish realistic expectations of what textual analysis tools can achieve and compare their application to the broader context of forensic enquiry.

On the Digital Forensic Analysis of the Firefox Browser Via Recovery of SQLite Artefacts from Unallocated Space

R.I. Ferguson, P. Leimich and R. Bagley
University of Abertay, School of Computing and Engineering Systems, Dundee, UK
<ian.ferguson,p.leimich,r.bagley>@abertay.ac.uk

Abstract

A technique and supporting tool for the recovery of browsing activity (both stored and deleted) from current and recent versions of the Firefox web-browser is presented. The generality of the technique is discussed: It is applicable to any software that uses the popular SQLite embedded database engine such as the Apple Safari web-browser and many Android apps.

The reconstruction of browsing activity is a well-recognised problem in digital forensics. Both commercial and open-source solutions for IE, Firefox and other browsers have been available for sometime. Why then, is this a problem worth revisiting? The developers of the Firefox browser have recently moved to a “rapid release” schedule which sees new versions of the software emerge every six weeks; a schedule with which the tool vendors struggle to keep pace. As part of this evolution, Firefox now uses a series of SQLite database tables to store details of browsing history, cookies, favourites etc. One approach employed by examiners has been to export the SQLite files used by Firefox and examine them with open-source SQLite tools. Whilst this technique will extract the current contents of the various database tables in which Firefox records its activity, it makes no attempt to recover deleted records. Recovery of browsing activity even after its deletion from the database is possible due to the journalling approach to handling database updates employed by recent versions (>=4) of SQLite (WAL files).

The technique presented here involves the analysis of unallocated disk space to recover fragments of the SQLite journalling files and hence the records associated with Firefox activity.

The approach, which has been evaluated both as a manual procedure and embedded in a software tool, comprises three stages:

1) Identification Stage: Potential records are located by performing a search for a sequence of bytes that consist of two constant values that appear in all moz_places records, followed by a URL protocol that appears at the beginning of the records' URL field;

2) Verification Stage: To filter out any false positives that were identified, further bytes that exist within the potential moz_places record are examined. Predetermined values and ranges are compared to these bytes to ensure only genuine records are recovered;

3) Reading Stage: Finally, with an authentic moz_places record located, its contents were read and extracted to a text file. An additional program was developed to organise the recovery result into a XML table and a summary document.

To evaluate the approach, a copy of Mozilla Firefox 10.0.2 was used over a period of two days to browse the Internet and local files. Subsequently the browsing history was deleted. A routine forensic disk imaging procedure was followed and the resulting

On the digital forensic analysis of the Firefox browser via recovery of SQLite artefacts from unallocated space image examined using our technique. A total of 455 records from an original 469 records were recovered from unallocated space which was a recovery success rate of 97%. Although it was initially designed to recover deleted browsing history from Firefox version 10.0.2, the developed tool is capable of functioning on version 4.0 and above.

The conclusion of this project was that it is possible to recover individual deleted records of the Firefox browsing history in an accurate and forensically sound manner.

Future work will examine the broader applicability of the technique to other SQLite based systems including Apple's Safari browser and Android apps.

BCS AGM Presentation

ECENTRE—England's Cybercrime Centre of Excellence Network for Training, Research and Education

Denis Edgar-Nevill
Canterbury Christ Church University
Chair, BCS Cybercrime Forensics SG

Abstract

The fight against cybercrime is a high priority for the European Union to protect commerce and individual citizens from Internet crime. Central to any successful strategy is building the capacity in law enforcement agencies to deal with cybercrime through education programmes informed by research and development keeping pace with this fast moving field.

Denis Edgar-Nevill, Head of the Department of Computing at Canterbury Christ Church University, has made a successful bid on behalf of a consortium of 17 organisations (police, universities and companies in the UK) to the European Commission to establish ECENTRE - England's Cybercrime Centre of Excellence Network for Training, Research and Education.

On Thursday 5th July 2012 the European Commission confirmed its grant of up to €899,481.73 (£716,437) to support the work which, together with contributions from partners, brings the project total budget to just over €1.08 million (£803,000) funding for the initial 16 months phase. The grant is awarded under the *Programme Prevention of and Fight against Internet Crime Targeted Call – ISEC 2011 Action Grants – Project Number HOME/2011/ISEC/AG/INT/4000002226.*

Denis spent the last three years forming the ECENTRE consortium based upon 10 years collaboration with the NPIA (National Policing Improvement Agency); responsible for specialist training for the UK's police forces. Without their involvement and support this bid would not have been possible. The development of the partnerships was further assisted by the national British Computer Society Cybercrime Forensics Specialist Group. The ECENTRE partners are also indebted to Debbie Wells and her colleagues in RED (Research and Enterprise Development) Centre at Canterbury Christ Church University supporting the final preparation and submission of this bid to the European Commission.

OVERVIEW OF THE WORK OF THE CENTRE

ECENTRE comprises a network of five regional clusters bringing together law enforcement, universities and companies to share research and training and educational materials and cybercrime forensics educational resources. The group will develop software tools, case studies, lectures, training materials and share collective expertise enhancing and developing practitioner training in this field.

ECENTRE joins a growing European network of national Centres of Excellence in Ireland, France, Estonia, Spain, Romania and Greece; sharing expertise, educational materials, research and best practice in the fight against cybercrime.

Many other universities and companies have indicated support for ECENTRE and will become members as the project develops. Expressions of support internationally, to peer review work, have already been received from the Police Academy of the Netherlands, the Justice Institute of British Columbia, Canada and NIST (National Institute of Standards and Technology), USA.

ECENTRE will use the series of international CFET (Cybercrime Forensics Education and Training) conferences hosted by the Department of Computing at Canterbury Christ Church as one of the many avenues used to publish results and the work of the Centre of Excellence.

ECENTRE PROJECT CONSORTIUM

Project Manager – Denis Edgar-Nevill, Canterbury Christ Church University

Law Enforcement Agencies

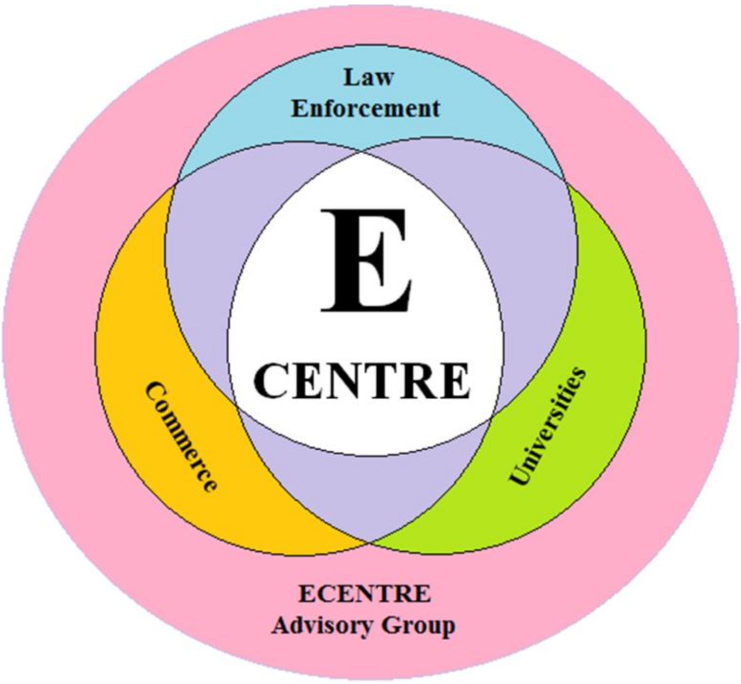
NPIA (National Policing Improvement Agency)
ACPO eCrime Training PCeU (Police Central e-Crime Unit) (Advisors to Project)
Cheshire Constabulary

Universities

Canterbury Christ Church University
Anglia Ruskin University
Kings College London
University of Bedfordshire
University of Greenwich
Liverpool John Moores University
University of Plymouth
DeMontFort University
University of Coventry
University of Staffordshire

Companies

Evidence Talks Ltd
Technology Risk Ltd
First Cyber Security
n-Gate Ltd
ManageMyProject



A Targeted Malicious Email (TME) Attack Tool

Tuan Phan Vuong, Diane Gan
School of Computing and Mathematical Sciences,
University of Greenwich, UK
D.Gan@gre.ac.uk

Abstract

Spam email is a big problem on the Internet, with 89% of all email consisting of spam. The aim of this work was to develop an automated tool that would perform the three steps of email harvesting, applying social engineering content and sending out the spam emails. It clearly demonstrated how emails could still be harvested to produce spam emails, even when the Web Administrator had attempted to obfuscated them.

Two common techniques to protect email addresses included replacing the text of address with an image or using JavaScript to safeguard email address in the code. Both of these techniques are aimed at discouraging harvesting activities. In order to bypass the anti-spam system, spammers need to harvest large numbers of valid email addresses and this process needed to be automated. Having identified how the email addresses were stored, these then needed to be extracted for use in the tool. This was done using regular expressions. Having obtained a large number of valid emails, the next step was to design an email that the “victim” would open using social engineering techniques. This was known as a targeted malicious email (TME).

It was important to understand the motivation behind TME because this affected the success of the attack. TME needed to pay more attention to the list of recipients and the content of the emails, as well as the process of delivery. TME distribution was also limited to specific groups of users. This meant that the email contents were crafted to match the interests of the target group and then the content template was applied to the sending email. In order to deliver the email, the tool had to be able to interact with the SMTP server to send out the email. Open relay server was selected for managing this process. The tool was able to harvest email addresses, send deceptive messages based on social engineering and perform targeted email attacks using the CMS School at the University of Greenwich as the target.

Keywords
Spam email, social engineering, regular expressions, targeted malicious email (TME)

An Analysis of Hotmail Artefacts in Firefox 9

Anne David
Cranfield University

Abstract

Webmail is a convenient way of accessing emails via a web browser on any computer connected to the Internet and it has gained popularity amongst Internet users. Many webmail service providers offer a free email service where users can set up an email account (or accounts) online by supplying their personal details and choosing a preferred username.

Email artefacts such as usernames, aliases, message subject and body may be useful in a digital investigation and thus require recovery and analysis. Unlike client based email software where a user's messages are stored locally on the hard disk, webmail messages are stored remotely on the webmail provider's servers, potentially making it difficult for digital investigators to obtain relevant artefacts. However, due to webmail being accessed through a browser it may be possible to recover the artefacts that will be useful in investigations.

This paper shows and discusses certain artefacts that can be left on a user's hard disk as a result of using Hotmail. For instance, artefacts that could be used to infer when an email account was created by a user and the details supplied at set up; details of exchanged emails such as who a user sent an email to, when the email was sent and whether it was replied to; full or partial contents of the email; details of contacts that had been added, edited, deleted or restored by the account user.

The research experiments are carried out on Hotmail using Firefox 9 and involve the analysis of the various file formats used by Firefox as well as their evidential value. The research also involves a multi-tool analysis technique which is necessary due to the differences in the format of artefacts recovered and to ensure the accurate interpretation of data.

Virtual Crime: Forensic Artefacts from Second Life

Sarah Morris
Centre for Forensic Computing, Cranfield University,
Shrivenham, SN6 8LA
S.L.Morris@Cranfield.ac.uk

Abstract

Second Life is an online virtual environment which is populated by users from all over the world. The virtual environment is split into a variety of public and private areas; these provide avatars with a chance to explore a wide range of environments and interact with other users. There is also an opportunity for users to create personalised environments; organisations such as the BCS have created customised environments to assist with education and training. Over the past few years the media has highlighted various legal cases involving virtual worlds; these cases cover both civil and criminal activities such as adultery, stalking and simulated child molestation. An analyst may potentially have an investigation where they need to understand the activity which goes on in a virtual environment and how to recover potential evidence. Digital Forensic Analysts may require training as they may not be familiar with how virtual worlds work and the types of digital artefacts left by their use. Previous research into Digital Forensics on Virtual Environments has primarily focused on their use to provide scenario based education. Little research has yet been published on methodologies for identifying artefacts relating to activities in virtual environments.

This paper highlights the requirement to provide focused training on both the criminal activity and digital artefacts relating to the use of virtual environments. The paper also describes a series of experiments that were conducted to ascertain the artefacts left after using Second Life. The experiments were conducted in virtual machines and aimed to replicate typical interaction between a user's avatar and the Second Life environment. This paper provides useful reference material for an analyst during an investigation, as it describes the artefacts identified as a result of this research. Finally this paper uses the results of this research to provide a basis for a discussion on the educational requirements for investigating crime in virtual environments.

A Forensics Approach to Digital Fingerprinting on Windows Servers

Christie Oso and Diane Gan
School of Computing and Mathematical Sciences,
University of Greenwich, UK
Christiext@gmail.com; D.Gan@gre.ac.uk

Abstract

The internet has placed a major part in the increase of cybercrime on computers and network by making attack tools available to everyone. With the number of cyber attacks on the increase this has resulted in the security of networks being severely diminished. The use of digital fingerprinting technologies have facilitated the collection of evidence to use in the prosecution of cyber criminals who have left behind vital evidence when compromising servers. Research has shown that cyber attacks are often carried by an employee within an organisation. This research demonstrates how the computers within a network can be used to breach a server within the same network.

The work was carried out in a virtual environment using a Window 2003 Small Business Server and two computers running Windows XP operating systems. A variety of attack tools were used to simulate an insider attack on the server. The attack phase consisted on the following steps:- scanning, enumeration and vulnerability assessment. The experiment demonstrated how the administrator password was easily compromised by an unauthorised user, using the Cain and Able tool. The consequence of this was a network breach that created a number of new user accounts in the admin and user groups, exposed vulnerable ports, the attacker could copy, insert and delete files and logs at will. The attacker was able to remotely log in to the server. Other exploits included the creation a backdoor to communicate with a remote server. Compromised computers within the network also became part of a botnet. The attack tools used, e.g. Nmap, were successful in penetrating the server, but this could just as easily have been carried out by an external attacker, and the vulnerability assessment clearly collaborated this. Further, security policies, especially for passwords, were also disabled therefore this permitted users to set up weak passwords which included the Administrator account.

This research has demonstrated that the greatest threat to any network comes from the insider, as a workstation on the network was able to breach the target server. This type attack would cause the most damage, which was particularly true if the attack was carried out by a trusted employee who had access to a number of key network resources within the organization.

Keywords
Extracting information, admin, passwords, vulnerability, digital fingerprinting, security, attack tools, forensics.

Invited Keynote Presentation

Making Digital Forensics Work within the Modern Policing Environment

Peter Salter
Police Service Northern Ireland

Abstract

Within its relatively short lifespan the technological environment within which digital forensics operates has changed dramatically. At the outset it had certainty and predictability, easily controlled and managed addressing a niche requirement within investigations generally concerned with low volumes of exhibits and data. The situation has changed dramatically driven by factors including virtualisation, technological convergence and low cost barriers together with social and economic change. Still immature it now presents few certainties and little predictability. It exists within a dynamic environment where digital sources of evidence and intelligence are prodigious in nature and ubiquitous in number and data volumes unconstrained. Everything exists within a 'connected' world where data connectivity is the expected norm and social and commercial interaction within this environment is second nature.

The impact of all this to policing is momentous placing huge demand on finite and centralised digital forensic assets in the form of backlogs of work and large data sets unscrutinised. The varied and vast numbers of digital devices presenting investigative opportunities mean digital forensics is no longer a niche requirement but a mainstream one increasingly focused around mobile communication and computing. There is a fundamental requirement within policing to understand and address the need to maximise evidential and intelligence opportunities within an overall strategical approach and in a manner that allows investigators to make operational decisions based on quality assured information with the minimum of delay.

This presentation looks at choices made within one UK policing jurisdiction in mainstreaming such capability and at the same time seeking to exploit the vast quantities of data obtained within investigations in the interests of public safety within an overall strategical approach. This is particularly relevant to mobile handset related forensics. Equally it details hard choices taken in challenging traditional 'gold standard' computer forensic approaches that the speaker would contend are unavoidable, but ultimately in the interests of victims, within the context of finite policing resources.

Intensive Teaching of Cyber Security for Mid-Career Physical Security Professionals with Limited Academic Backgrounds

Chadwick D, Loukas G, Gan D, Frangiskatos D
C-SAFE Team
University of Greenwich, UK

Abstract

This paper addresses the approach taken by the C-SAFE (Cyber - Security, Auditing, Forensics, Education) team at the University of Greenwich when asked to produce a one week course for physical security experts who wished to know more about cyber security technologies. This paper discusses the expectations of both teachers and learners and their resultant feelings after the course had been delivered.

Mature adults, returning to education for a short course, are liable to face various problems. They are not conversant with the academic approach and have been absent from formal learning for many years. They are required to learn a great deal in a short time when they have been learning ad-hoc on-the-job as they progressed through their careers. The academic detail of 'how and why' things happen contrasts with the accumulated practical on-the-job experience of simply making things happen.

The academic team itself also faced various problems. They lacked the practical everyday experiences of the students they were teaching, they were concerned about how to maintain the pace of learning with relatively 'novice' students, and how best to involve the students in the academic material especially as the students had varying background knowledge in cyber security technologies. Also, we discuss the problem of how to assess the students – what sort of assessment to give them, how to mark it, what kind of feedback to give etc.

A questionnaire was given to the students after the course delivery in order to explore their professional role, their expectations of the course and their suggestions for improvement. The students were given a graded assessment and asked about their feelings on their resultant marks – whether they did as well as they were expecting or otherwise. This has resulted in a set of useful guidelines for teaching short courses in cyber security to mature learners involved in lifelong learning to enhance their career progression and knowledge diversity.

Keywords
Lifelong learning, cyber, security, short course, teaching

From Criminal to Digital Criminal Profiling: Advances in Criminal Profiling in the Digital Age

Georgios Chlapoutakis
SecurityBible Networks, 27 Agathovoulou Street, Giannitsa, 58100, Greece,
george.chlapoutakis@secbible.com

Abstract

Criminal profiling has seen a rise in both publicity and use in the last few years. Coined to the process of inferring the physical, mental and behavioural traits of individuals who have committed a crime through the analysis of various aspects of the crime scene, the crime itself and the victim's statement, the term, and the associated discipline has been extensively used in a number of real-world scenarios in the past to inform and aid the authorities in apprehending individuals who have committed one or more crimes.

While many theoretical and practical approaches have been introduces in policing, however, the pervasiveness the Internet nowadays enjoys in individuals' personal, social and professional lives has slowly changed the nature of crime to incorporate an increasing digital element. To this effect, there has been relatively much research interest in the transposition of classic criminal and offender profiling theories to Internet-oriented criminal acts.

In this paper, we define criminal profiling, discuss its modern inception and use in the US and follow its progress across the Atlantic to the UK and the rest of the world. We then introduce the application of criminal profiling on the Internet and, in particular, its application to digital crime and digital forensic investigations and policing.

Finally, we are going to attempt to properly define the term *"digital forensic profile"* in the form of an explanation of some of the theories and models proposed to define it sociologically and mathematically.

The contribution of this work is twofold. Firstly, our discussion will enable researchers to consider the progress of criminal profiling from its original intended field of application to the new era of the Internet, and will further stimulate academic interest in this field. Secondly, we hope that our discussion and the theoretical model produced by the mapping of classical criminal profiling theory to digital crime will allow the evolution of a properly defined mathematical or statistical model that will allow researchers to properly profile a digital criminal act and its perpetrator.

The Utilisation of the Unified Modelling Language in Digital Forensic Science

Peter Forster
Cranfield University

Abstract

This paper discusses the utilisation of the Unified Modelling Language 8 (UML) in the field of digital forensic science. Digital forensics usually requires a detailed examination of objects and events on a variety of systems. The results of these examinations are regularly discussed and presented to fellow practitioners, other professionals and members of the public, such as members of a jury. These presentations can include a variety of different diagrams and other methods for describing and modelling the results.

The UML is a flexible language with the ability to extend itself when used in a specialist problem domain. This flexibility appears to lend itself to being a candidate for the development of a visual modelling language for use in digital forensic science. Areas of digital forensics that would benefit from this include casework, information exchange, reporting, teaching and research. A review of the existing literature concerning modelling in digital forensics concludes that this is a subject in which there has been very little research and no standardisation. A research project is therefore introduced to address this and research objectives are described.

As an initial step in this research the use of core UML in a digital forensic case study is evaluated. This involves an examination of Microsoft Internet Explorer index.dat file organisation and internal structure. Existing methods of describing and exchanging this information are compared with UML models. The results show that this is a useful method for displaying digital forensic information in a concise visual format. However they identify some limitations within the core UML for use in this field.

In conclusion the strengths and weakness of this approach are discussed and future research highlighted. This will involve the use of additional case studies, including an examination of file date/time attribution as a result of file movement as a system process, to explore further the use of UML, and its extensibility, with the intention to develop a UML profile for use in digital forensic science.

VoIP Forensics

Abhaya Induruwa & Nathan Attoe
Department of Computing,
Canterbury Christ Church University
North Holmes Road, Canterbury, CT1 1QU, United Kingdom
abhaya.induruwa@canterbury.ac.uk

Abstract

VoIP is gradually becoming a popular technology and a protocol for person to person communication of both voice and multimedia services. Telecommunication industry uses it to provide services over the telecommunication backbone. Smartphones and other Internet devices allow their users to send voice or SMS messages using VoIP over 3G or Wireless networks. Skype, the most popular person to person communication service on the Internet, has a reported user base of 663 million. Over 25 million of them use Skype at any given moment. Microsoft which acquired Skype recently intends to integrate Skype into their products range including Xbox and Kinect, Xbox Live, the Windows Phone, Lync and Outlook. Microsoft has also pledged support to developing Skype clients on non-Microsoft platforms. Skype is more popular as a free service than a paying service. This along with the technology that is used to implement it are two reasons why cybercrime forensic investigators have become interested in VoIP, specifically Skype. There is a high probability that criminals may find these features attractive in their attempts to hide any traces of their presence at a crime scene or any connection with the crime they have committed.

Forensic Examiners ultimately want to be able to extract information about the call and caller location if possible. However the challenges faced by cybercrime forensic investigators are twofold. In terms of technology VoIP offers a major challenge when it comes to intercepting a VoIP call. Since the voice in a VoIP call is digitised and then packetised, and these packets are routed via multiple routes on the Internet, the interception is only meaningful if carried out at the sender’s or recipient’s site. This is unlike the case of ordinary telephone calls which can be easily 'tapped' at an intermediate telephone exchange. Skype as a VoIP service throws a major challenge because of the way the communication payload is encrypted using a key pair specific to the sender and the recipient. Even if the entire Skype session is captured the decryption of it is a major technical feat.

However, there is much information about the VoIP communication that can be extracted by examining the sender's or recipient's computer. This paper discusses how the Windows registry keys can be used to extract information about the installation of a VoIP client such as Skype, the last user to login and also how live data from a running VoIP session and data that is stored within the computer is extracted and presented using specialised forensic tools such as FTK and WinHex as well as common tools such as Wireshark. Particular to Skype are tools such as Skypelog viewer and Skype analyser that can be used to analyse the Skype client logs which are saved either as .dbb files or in a SQLite database. More recently a number of Skype analyser tools have appeared [1], [2], [3] and vulnerabilities have been exposed [4]. The paper concludes by drawing attention to the need for more research to understand the depth of available data and how they can be interpreted.

References

1. Skype Extractor (no date)
   Available at: http://www.simplecarver.com/tool.php?toolname=Skype%20Extractor (accessed on 4 August 2012)

2. Belkasoft Skype Analyzer (2012)
   Available at: http://home.belkasoft.com/en/bsa/en/Skype_Analyzer.asp (accessed on 4 August 2012)

3. SkypeAlyzer (2012)
   Available at: http://sandersonforensics.com/forum/content.php?116-SkypeAlyzer (accessed on 4 August 2012)

4. Furneaux, N. (2012) "Skype IP addresses in the clear"
   Available at: http://nickfurneaux.blogspot.com/2012/04/skype-ip-addresses-in-clear.html (accessed on 4 August 2012)

Towards a Science of Digital Forensics

Clive Blackwell
Computer and Communication Technologies
Faculty of Technology, Design and Environment
Oxford Brookes University
OXFORD OX33 1HX. UK
CBlackwell@brookes.ac.uk

Abstract

The scientific basis of forensic science has been widely evaluated and criticised, and these issues also apply to digital forensics. We elucidate some of the challenges with the creation of a science of digital forensics.

Digital forensics is a young discipline developed according to the convictions and exigencies of investigators, rather than using well-defined criteria based on scientific principles that establish its validity. The classic report [1] questioning the scientific basis of the more established physical forensic sciences demonstrates the limitations and highlights the challenges for all forensic disciplines. These include techniques commonly believed to be valid, such as fingerprint evidence as there have been several miscarriages of justice. One high profile example was the case of US lawyer Brandon Mayfield held for the Madrid train bombing on account of a supposed fingerprint match for which he was awarded $2 million in compensation [2]. Many fingerprint practitioners have claimed a zero error rate that raises questions regarding its scientific practices and possibly its theoretical validity [3].

Similarly, the Scientific Working Group on Digital Evidence (SWGDE) in its response to the report [4] downplayed the problems with errors with these sentences. ‘It should be noted that most processes regarding digital evidence are discrete in nature and not subject to statistical error. Systematic error is generally identified during validation and accounted for in the standard operating procedures regarding that tool or technique.’ This ignores several issues including that digital evidence is ultimately represented physically, and copying and analytical techniques may not be correctly applied. In addition, the in-distinguish ability of a copy from the original is an additional concern not usually present in physical evidence, as digital evidence can be easily fabricated without detection.

Firstly, we need to determine the extent to which digital forensics can be founded on a reliable scientific basis. We ask firstly: ‘How do we establish a science of digital forensics by more scientific rigour to the discipline?’. This is similar to many other forensics sciences where fundamental research is lacking [5].

Having answered how we establish a science of digital forensics, we ask ‘How do we apply scientific rigour to digital forensics practice?’. It is impossible to construct a scientific discipline without agreement about the engineering processes and procedures to achieve accurate, reliable and valid results. Where are the materials, methods, procedures, results and conclusions characteristic of scientific experimentation? As the old management adage says: ‘You cannot manage what you cannot measure’. We must consider the practices that help to adequately analyse systems, report results, make decisions, take effective from previous experience. In addition, the profession will be held in low standing if computer evidence that is relied upon is later shown to be incorrect.

We also need effective processes to validate new tools extending the tool checking carried out by NIST with its worthy Computer Forensics Tool Testing (CFTT) Project [6]. We need to move beyond validating basic techniques such as imaging and write blocking to file carving, analysing novel devices, cloud forensics and so forth, to keep up with the rapid technological changes.

Finally, we elucidate some fundamental principles on which a sound basis of digital forensics can be based, inspired by the five Daubert guidelines for expert testimony laid down by the US Supreme court in the case Daubert v Merrill Lynch [7] in 1993.

Some objectives that may help to establish digital forensics with a sound underlying scientific and engineering basis include:

a) Establishing fundamental scientific and engineering principles;
b) Clarifying achievable forensic objectives and forming realistic plans for their achievement;
c) Encouraging a holistic view of investigations, taking account of their real world contexts rather than focusing purely on computer evidence;
d) Establishing suitable education and training for practitioners with appropriate enforceable standards;
e) Adequate recognition and management of the issues by interested stakeholders in the legal system and forensic laboratories;
f) Establishing processes for improvement by learning from previous incorrect or suboptimal choices and activities;
g) Informing the public about the true nature of forensics, challenging the perception given by its colourful TV counterparts like CSI.

Developing a science of digital forensics is a very hard challenge, which will take many years to bring to fruition, but it is necessary to attempt because of the importance and current state of digital forensics, as computers are used more and more in criminal activities as tools, targets and evidence repositories. Training should move beyond apprentice-like transmittal of practices to education based on scientifically valid principles. We must move from a craft of learned performance from prior experience and pragmatic beliefs, to scientifically validated processes and procedures. We have proposed some questions that must be answered before digital forensics can be truly called a science, but this is only a small step on a long path.

References

[1] National Research Council, Strengthening Forensic Science in the United States: A Path Forward, The National Academies Press (2009), at https://www.ncjrs.gov/pdffiles1/nij/grants/228091.pdf.

[2] Associated Press, FBI apologizes to lawyer held in Madrid bombings, MSNBC, 25 May 2004, at www.msnbc.msn.com/id/5053007/ns/us_news-security/t/fbi-apologizes-lawyer-held-madrid-bombings.

[3] SA Cole, More than zero: Accounting for error in latent fingerprint identification, Journal of Criminal Law and Criminology, vol 95, pp 985-1078, University of Chicago Press (2005).

[4] Scientific Working Group on Digital Evidence, Position on the National Research Council Report to Congress Strengthening Forensic Science in the United States: A Path Forward, SWGDE (2010).

[5] JL Mnookin, SA Cole, IE Dror, BA J Fisher, MM Houck, K Inman, DH Kaye, JJ Koehler, G Langenburg, DM Risinger, N Rudin, J Siegel, and DA Stoney, The Need For A Research Culture in the Forensic Sciences, UCLA Law Review, volume 58, issue 3, pp. 725-779, UCLA School of Law (2011), at http://uclalawreview.org/pdf/58-3-3.pdf

[6] NIST, Computer Forensics Tool Testing Project Handbook, NIST (2012), at www.cftt.nist.gov/CFTT-Booklet-Revised-02012012.pdf.

[7] DE Bernstein and JD Jackson, The Daubert Trilogy in the States, Journal of Jurimetrics, vol 44, pp 351–366, American Bar Association (2004), at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=498786.

A Simple Enterprise Security Architecture (SESA): Towards a Pedagogic Architecture for Teaching Cyber Security

Harjinder Singh Lallie
E-Security Group, WMG, University of Warwick, Coventry, CV4 7AL, UK,
h.s.lallie@warwick.ac.uk

Abstract

Enterprise Security is a highly complex issue which is complicated further by conflicting views of the different elements of cyber security which are often represented as a while in terms of an architecture or model. In this paper we consider a number of approaches to defining architectures in the computer science domain and determine a number of architectural guiding principles from these. We consider a number of approaches to defining cyber security architectures and propose a Simple Enterprise Security Architecture (SESA) which encompasses security from the strategic through to the protocol level in three simple layers.

Keywords
Enterprise security; Security architecture; Security models

A Comprehensive Methodology for Profiling Cyber-Criminals

Hemamali Tennakoon
Kingston University

Abstract

In dealing with crimes in the physical world, forensic psychologist are able to identify common characteristics of criminals, understand their mind-set, personality traits, nature of their victims etc. and profile them so that either the motives behind their crimes can be understood or predict where they are likely to strike next. So far, this seems possible in the physical world. However, in the cyber-space, the situation is far more challenging. Often, many cyber-crimes go unreported or unnoticed and the ability to commit crimes anonymously on the Internet makes it even more difficult to trace them back to a criminal. Thus, lack or absence of evidence results in crimes that go unpunished. Attempts at developing methods for profiling cyber-criminals have met with little success. In profiling cyber-criminals, knowledge about psychology, criminology, law and Information Technology re essential, which might be one of the reasons why an operational model of cyber-criminal profiling is still to emerge. It is evident that an interdisciplinary approach is required in dealing with such an issue. Hence, this paper is an attempt to develop a comprehensive methodology for profiling cyber-criminals based on the inductive and deductive profiling techniques used in crime analysis in the physical world. The paper first looks into challenges in profiling cyber-criminals. Then, the discussion moves to the application of existing tools that can be used for profiling cyber criminals leading to a proposed model. The paper ends with a brief discussion on the future of cyber-criminal profiling.

Key words
Cyber-space, criminals, profiling, operational model

A Forensic Image Description Language for Generating Test Images

Dr Gordon Russell & Robert Ludwiniak
Napier University
Edinburgh Napier University
School of Computing, Merchiston Campus
10 Colinton Road, Edinburgh, UK
g.russell@napier.ac.uk, r.ludwiniak@napier.ac.uk

Abstract

When teaching digital forensics it is often useful to have a range of suitable disk images for students to work on. However these images are time consuming to build by hand. Additionally, if near-identical images could quickly be produced containing variations on a theme, students could be allowed to explore many variations of particular issues in a controlled manner. For instance, when exploring cylinder alignment issues, the ability to produce on demand different alignment variations of the same data could greatly improve concept understanding.

There are some forensic description languages in use today, such as the DFXML used in fiwalk [1] or the output of log2timeline [2]. However these focus on describing the output of a forensic analysis in complete detail, rather than offering an easily editable summary suitable for image creation and variation. This paper proposes an XML style specification language for disk image creation which allows summarisation of the details, allowing disk images to be rapidly created on demand.

The XML description language proposed here must support the definition of realistic images suitable for students learning about key forensic issues. This includes system files, user files, deleted files, hidden files, and application usage such as URLs visited in Internet Explorer, cookies set in Firefox, cache files generated in Chrome, and program execution history in file explorer. However the assumption should be that unspecified XML information should result in the selection of automated sensible values to match other specified criteria, thus maintaining realism of the image while avoiding extensive definitions appearing in the XML. It should however always possible to override automatic defaults where a particular setting is needed.

This paper also discusses an image creation application, which reads the XML specification and produces images rapidly on demand. This allows scenarios with variations to be created as needed. This enables challenges to be quickly setup and varied, such as “find a file with a secret slackspace message in partition 2” [3], which greatly increases the student engagement when learning forensics.

A particular issue in our approach is the management of windows registry hives. The registry files have no public documentation, so setting forensically important registry values (such as the last accessed URL) is challenging. A number of techniques are considered in the paper.

Our digital forensic teaching uses cloud-based virtual machines coupled with an integrated tutorial environment, which is offers a safe, reliable, and flexible learning approach to digital forensics [4] [5]. Analysing large images takes time even on fast machines, and fast cloud machines can be expensive for large class sizes. Additionally

large image files can take long periods to distribute around a cloud system. Therefore the image creation application tried to greatly reduce image sizes through various techniques, while maintaining a realistic partition structure and thus avoiding forensic tools highlighting any shortcuts as anomalies. Techniques considered include truncated system files, sparse files, NTFS junctions, and zeroed file contents.

Finally, an analysis of the use of the new XML description language and image creation application is presented. This considers a number of factors, including realism, efficiency, creation time, flexibility, and its impact on student engagement. Various analysis tools are considered in this evaluation, including the Caine environment and Encase.

References

[1] S. Garfinkel, "Digital forensics XML and the DFXML toolset," *Digital Investigation*, vol. Volume 8, no. 3-4, pp. 161-174, February 2012.

[2] K. Guðjónsson, "Mastering the super timeline with log2timeline," SANS Institute, 2010.

[3] E. Huebner, D. Bern and C. Kai Wee, "Data hiding in the NTFS file system," *Digital Investigation*, vol. 3, no. 4, pp. 211-226, December 2006.

[4] G. Russell and R. Macfarlane, "Security Issues of a Publicly Accessible Cloud Computing Infrastructure," in *Proceedings of the 11th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom-2012),* Liverpool, 2012.

[5] G. Russell and A. Cumming, "Student Behaviour in a Flexible Learning Course Framework," in *Proceedings of the IADIS International Conference on e-Learning,* Rome, 2011.

Social Media in Law Enforcement: the Role and Issues

Dr Man Qi
Canterbury Christ Church University

Abstract

The law enforcement field has used social media and experience successes in recent years. Social media has been used for crime investigations and community communications and become a powerful crime-fighting tool for law enforcement.

With more and more users of social media showing their actions and thoughts openly, there are always people flaunting their crimes online. Social media makes it possible to search friends and friends of friends of the suspects. There have been many criminals whose social networking footprints led to their eventual arrests.

Social media is facilitating closer and more collaborative relationships between law enforcement and the community. It can be used to notify the public of crime problems or emergency situations, improve community outreach and citizen engagement and promote crime prevention activities. Citizens can also use social media to report crime and other public safety incidents timely.

Social media is a double-edged sword for law enforcement. It not only brings technical challenges but also changes in organisation structure and management practices. In community communications, law enforcement officers should be very cautious posting any content to avoid affecting normal procedure. On the other hand, it is also important to avoid public voices on social media affecting the course of justice. In crime investigations, enforcement agencies are actively seeking and using information from online social media thus there are intense debates on privacy in handling social media contents. Current laws show the limits in how police can legally retrieve personal data.

References

[1]Roger Yu, Social media role in police cases growing, USA TODAY, Available from http://www.usatoday.com/tech/news/story/2012-03-18/social-media-law-enforcement/53614910/1, 18 March 2012.
[2] Social Media the Internet and Law Enforcement: Using Social Media to Improve Law Enforcement and Engage Citizens. Available from http://thesmileconference.com/, 9-12 Sept 2012
[3] David J. Roberts (2011) "Technology's Impact on Law Enforcement—:Community Interaction," Technology Talk, The Police Chief 78 : 78-82.
[4] Social Networking for Law Enforcement Officers, http://www.reputation.com/reputationwatch/articles/savvy-social-networking-law-enforcement-officersm, last visited 6 Aug 2012.
[5] Doug Wyllie, Social media for investigators: Why departments should invest in training, Available from http://www.policeone.com/investigations/articles/5885816-Social-media-for-investigators-Why-departments-should-invest-in-training/, 31 July 2012
[6] Crump, Jeremy (2011) "What Are the Police Doing on Twitter? Social Media, the Police and the Public," *Policy & Internet*: Vol. 3: Iss. 4, Article 7.

Invited Keynote Presentation

Professor Nigel Jones MBE FBCS
Canterbury Christ Church University

Biography

Nigel Jones is currently a director of Technology Risk Limited, a company specialising in technology risk solutions and training and for 1st September 2011 he has been appointed as a Visiting Professor at Canterbury Christ Church University. He was most recently European Practice Leader and Managing Director of the Financial and Litigation Consulting Services Practice of a major insurance broker. Prior to this he was responsible for the creation of the National High Tech Crime Training Centre at the National Centre for Policing Excellence at Wyboston in the UK and was responsible for the creation of the design and delivery of a core curriculum and modular high tech crime training programme for the UK police service. In addition to wide ranging experience in major commercial fraud and computer crime investigation, he was the Secretary of the Association of Chief Police Officers Computer Crime Working Group and the UK Internet Crime Forum as well as being the UK Police representative on the G8 sub group on high tech crime and UK coordinator of a series of G8 Industry conferences. During his time as a fraud investigator he designed and delivered an academically accredited fraud training programme.

Nigel formed the Kent Police Computer Crime Unit in 1993 and is co-author of the ACPO “Computer Based Evidence - Good Practice Guide” and member of the Technical Working Group on the Investigation of Electronic Evidence (TWGIEE) in the USA. In 2002 he was appointed by the UK as a member of the Interpol European Working Party on IT Crime.

In May 2009, he was invited to Interpol as an expert to provide advice on an international IT forensics investigation. He also chaired the cybercrime panel at the 2009 Interpol General Assembly. He is currently a member of the Home Office Forensic Regulators digital forensics specialist group which is assisting in identifying requirements for new or improved quality standards, applying to the provision of digital forensics services to the police service and the wider Criminal Justice System. Nigel is currently the training manager for a €2.7m European Commission funded programme to further harmonise cybercrime training across international borders. He is also the law enforcement coordinator for the creation of the international network of centres of cybercrime training, research and education (2CENTRE), funded by the European Commission.

Sponsor - Canterbury Christ Church University

Canterbury Christ Church University

The Department of Computing plays host to the CFET 2012 conference based at the North Holmes Road Campus of Canterbury Christ Church University.

.

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

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

Sponsor – National Policing Improvement Agency

NPIA

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

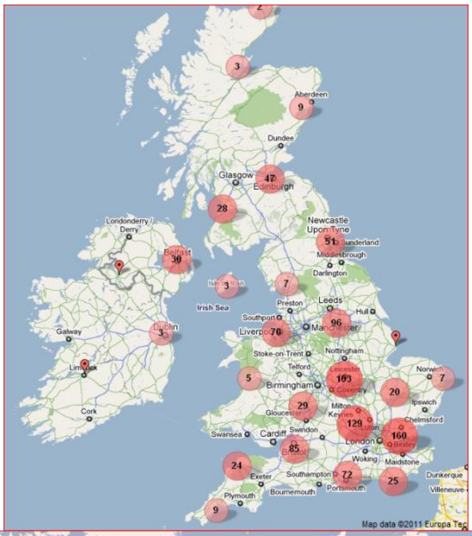
Provincial post-secondary institute, founded under College & Institute Act, for Justice & Public Safety education in 1978, by Dr. Patrick McGeer, Minister of Education. Its mission is to provide Innovative education and training for those who make communities safe. Its vision is to be a world leader 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 2011/12 over 6,000 organizations chose the Justice Institute of BC for training, education, and research needs in justice & public safety training.

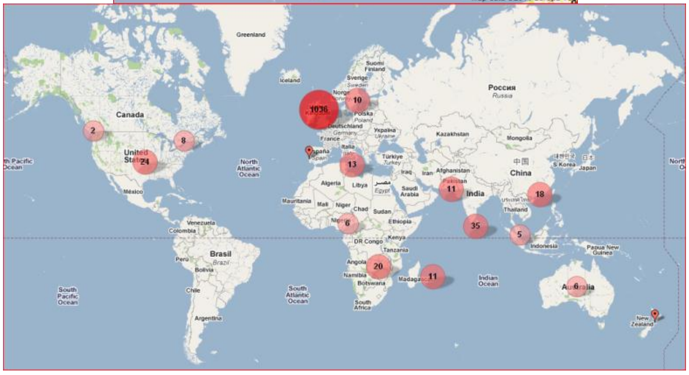
Sponsor – British Computer Society
Cybercrime Forensics Specialist Group

bcs The Chartered Institute for IT

Cybercrime Forensics Specialist Group

Established in 2008, the SG now has over 1550 members in 47 countries:





Aim

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