

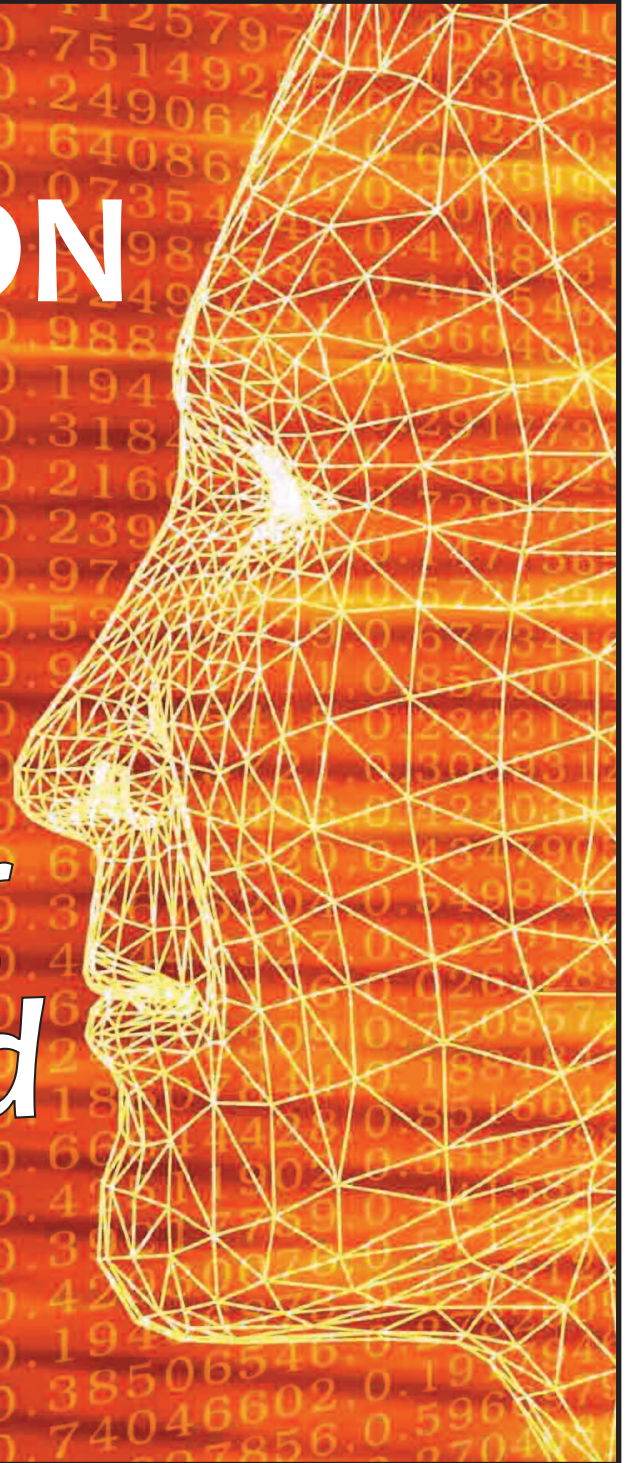
The Investigator

November/December 2009
www.the-investigator.co.uk

ESSENTIAL READING FOR TODAY'S INVESTIGATORS

DIGITAL REVOLUTION

Embracing Mobile and Computer Forensics



Also inside this issue:

Volume Crime Conference Review - Digital Forensics Conference Review
Payphone Sex Offender Case Study - Future Digital Standards

Live news feeds Recruitment Conferences Daily news



www.the-investigator.co.uk

COVER STORY: Chris Simpson, the NPIA's head of e-crime training looks at the growing importance of communications data as evidence in investigations.

6

DIGITAL FORENSICS CONFERENCE: Experts gather to discuss the latest trends in computer and mobile phone forensics.

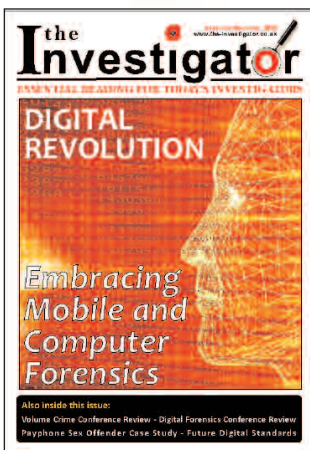
8

VOLUME CRIME CONFERENCE: All the news and headlines from the Investigator's recent conference.

18

CASE STUDY: An Investigation by Humberside Police resulted in the conviction of a man who used public telephone boxes to incite young girls to perform sexual acts.

31



Also in this issue:

16	Digital Standards	46	Technology
35	Linguistics	52	Events
42	Cyber Crime	56	In this week

training

design and delivery

overview

Belmont Training was started by Alan Oliver in 2005 to bring first-rate, practical interviewing skills to all investigators. We work with police, central government departments and private industry to improve their technique. We believe in “design and delivery” and work with our clients to NPIA standards. The trainers are all detectives, experienced interviewers and gifted communicators. We also dip sample after delivery to confirm improvement of both performance and evidential product. We can do the same for you!



courses and training

Investigative Interviewing to the National Standard (formerly Tiers 2 - 5)

TRAINING AVAILABLE:

- Courses are flexible and role specific.
- Achieving Best Evidence and Enhanced Cognitive Interviewing.
- Suspect interviewing for Specialist Interviewers.
- Interview Advisor courses.
- Time line interviewing, and note taking.
- SE3R to analyse and plan.

LEARNING OUTCOMES:

- Focussed planning.
- Structured, detailed interviews.
- High quality, evidentially sound product.
- Ability to deal with Legal Advisors.
- Identification of new “Lines of Enquiry”.
- A structure for “No Comment” interviews.

contact us

Telephone: 07956 327032

Telephone: 01494 714604

E-mail: alan-oliver@tiscali.co.uk



Belmont Training Ltd

EDITORIAL

Editor: Carol Jenkins
Tel: +44 (0) 844 660 8702
 carol@the-investigator.co.uk

ANALYSIS

Sophie Harrison
Tel: 0844 660 8702
 sophie@the-investigator.co.uk

FORENSICS

Daniel Dexter
Tel: 0844 660 8702
 daniel@the-investigator.co.uk

CONSULTANT

Gary Shaw
Tel: 0844 660 8702
 gary@the-investigator.co.uk

COMMERCIAL MANAGER

Dale Hazell
Tel: 0844 660 8707
 sales@the-investigator.co.uk

CONFERENCES

Tel: 0844 660 8707
 info@the-investigator.co.uk

PRODUCTION

Tel: 0844 660 8707
 snoops@the-investigator.co.uk

CIRCULATION

circulation@the-investigator.co.uk
Tel: 0844 660 8707

PUBLISHING

The Investigator
 Kingfisher House
 61 Walton Street
 Aylesbury
 Bucks, HP21 7AY
Tel: +44 (0)844 660 8707
Fax: +44 (0)844 660 8701

info@the-investigator.co.uk
www.the-investigator.co.uk



From the editor

Mobile phones and computers are now such an integral part of our lives it is not surprising that communications data now provides investigators with a wealth of evidential opportunities that could make or break a case.

The main challenge for the service is that digital forensics is still regarded as a developing and fringe specialism that is practiced by a small number of geeks and is not yet considered an integral part of an investigative strategy.

The fact that so many of us are using phones and computers to communicate means that this perception must be challenged.

This is where the NPIA's e-crime training unit will play a central role in disseminating best practice and providing help and advice to forces to give them the tools and techniques needed to gain best evidence out of this critical area.

Chris Simpson and his team are not only providing relevant training to investigators of all levels but they are ensuring that the issues are debated and highlighted by attending events such as The Investigators recent computer and mobile phone forensics conference.

Also attending the conference were well established experts from academia and private companies who are all doing their bit to work with forces and promote this valuable science.

Their efforts are proof that no one agency is the answer to using digital forensics more effectively within investigations and that we must all pool together our individual expertise to ensure that the UK is leading the way in this vital field.

Carol Jenkins



Digital Revolution

Increased use of mobile phone and computers presents new opportunities for investigators to glean vital evidence. Chris Simpson, the head of the NPIA's e-crime training unit talks to Carol Jenkins about this growing area of investigative practice.

The way in which we all communicate has undergone a revolution over the past decade with mobile phones, the internet and other devices such as Satellite Navigations systems and gaming consoles now being routinely used in our daily lives. With this digital revolution comes exciting potential for investigators to secure evidence in both minor and major crime in a way that hasn't existed in the past.

Chris Simpson the head of the NPIA's e-crime training unit, who like many of us confesses to being a gadget addict, has been given the job of providing training and advice to forces on how to maximise the evidential potential of digital devices.

"Despite the fact that we all carry mobile phone and use the internet, the service is still trying to get its teeth into the nature and extent of e-crime," he said.

"If you are investigating a crime whether it is a low level or a series crime – in the vast majority of cases there will be some form of communications data. If the crime involves two or three individuals below

the age of 35 then they will almost certainly have access to a mobile phone or the internet."

With this in mind, Chris is now working to build awareness within forces of the importance of training investigators not just about the vast amount of evidential potential that exists but also the possible pitfalls and other legal issues.

"We are encouraging investigators to consider during the early stages of an investigation the history of communication between a victim and a possible suspect. Look at their internet or phone history. Do they have a social networking presence that could throw us some vital evidence about associates and the history and nature of their communication?"

He uses examples of cases involving a young person who has gone missing or who has been the victim of bullying and urges investigators to look at their MSN or Facebook account for any record of derogatory comments or contact from somebody who might have vitals clues about their disappearance.

"You can not only get a wealth of information from a person's phone history, their texting history and their internet history but also from gadgets such as Satellite Navigation systems which could give you clues as to their geographic location."

Satellite navigation systems can also provide valuable information about a suspect who might have carried out hostile reconnaissance of a scene to plan a crime. This is a common tactic amongst criminals who are planning crimes in and around an airport and aren't familiar with the surroundings. A key part of the planning would be for them to visit the scene and make themselves familiar with its location and layout. This kind of information could prove that the criminal was not only at the scene but that they had attended the scene previously to carry out hostile reconnaissance.

Chris believes there is still a long way to go before forces incorporate digital evidence into their investigative strategies. He wants SIOs to include a communications data/digital strategy within the policy log in the same way that aspects such as an FLO strategy are routinely included.

He also highlighted the importance of SIOs being able to consult an e-crime advisor to provide assistance on the investigative opportunities that might arise from digital evidence.

Police forces also need to be more aware of the growing trend for people of all ages to take part in virtual worlds and of crime that has been committed in a virtual world.

“We've got to be asking the question what if somebody went into their local police station and reported that they had some virtual property stolen. Are we geared up to deal with this? I would say at the moment we are not. It is all too easy to dismiss this as not a priority but what if we ignored the report and it escalated into a serious crime that ended in murder?”

The growing issues of virtual worlds and other trends are incorporated into the training courses that the e-crime unit delivers to forces. Unlike other training that is often only updated on a yearly basis, the e-crime training is updated on an ongoing basis to reflect the changing nature of the threat.

In one recent training session, officers were given information about a new mobile phone mast that can be fitted into a person's home which means

that it would make it difficult to track their activity via cell site analysis.

One other example concerns a software package that is now being used by a number of forces to identify the area that a computer is in when it is used to distribute child abuse images.

As well as highlighting the evidential opportunities that exist from communications data, Chris urges investigators to ensure that all activity complies with the ACPO digital standards guidelines.

“If you are investigating a person's social networking site or similar internet history – you need to handle with care and not make it obvious you are police. It's essential that you consult the experts to ensure you obtain best evidence.”

As the popularity of electronic devices increases, Chris says that the biggest challenge will be for managers in deciding which devices to seize.

“The first instinct is to seize everything in a house but this could have implications on time, resources and on storage and so like every other areas of policing it's important to prioritise and to know which devices are worth seizing.”

Another challenge for forces is the growing international element of e-crime particularly in offences such as large scale fraud which don't respect local force boundaries.

“An offence can be committed in a number of countries throughout the world and never be unearthed because of its complex nature.” Looking to the future, Chris and his unit will continue to highlight both the threat of e-crime and the evidential potential of communications evidence. He is hopeful that more SIOs and frontline officers will begin to appreciate the value of such evidence.

“As more cases are solved with the help of communications data and there is an increasing awareness among forces of its evidential potential then I can see a team when digital evidence will be an integral part of all investigations.”

COMPUTER & MOBILE PHONE

F^{orensics} CONFERENCE

APPLYING CUTTING EDGE TECHNIQUES TO CRIMINAL INVESTIGATIONS

Conference Review

Off the busy high street in Towcester, Northants, in a wood panelled room of a 16th century coaching inn, experts met on September 29 to discuss how best to apply cutting edge technologies to criminal investigations.

The Investigator's computer and mobile phone forensics conference hosted a varied and valuable selection of speakers and delegates giving an insight into a range of issues that included how best to obtain intelligence from suspects, a study of new and emerging threats facing investigators, how to maximise the potential of digital evidence, and the risks associated with an ever increasing technology-dependant society. Daniel Dexter reports.

Open source intelligence can yield vital clues

As technology and the internet continue to become much more an integral part of individuals' personal lives, Detective Chief Inspector Christopher Simpson, head of the National Policing Improvement Agency's (NPIA) e-crime Training Unit, believes products like mobile phones and social networking websites should be utilised much more in order to obtain intelligence.

"Investigators need to be aware of the

opportunities and resources available for generating open-source intelligence in order to exploit investigative practices," he said.

"It is an underused tool because the investigative community has not experienced resources such as covert internet investigators who can increase intelligence gathering opportunities."

In one case involving a gang murder, DCI Simpson said the suspects responsible had posted a rap song on the internet celebrating and detailing the specific details of the crime.

"It was an absolutely tragic case but the reality is that criminals are posting this type of information on the internet which can be accessed by law investigators relatively easily, is not resource intensive and provides fantastic evidence to present to a jury."

In another recent operation, open source intelligence gathering helped uncover a criminal gang responsible for stealing valuable haulage loads after the stolen goods were denitrified on an online auction websites.

DCI Simpson said mobile internet access is the fastest growing area within the telecommunications arena, an important fact to bear in mind when conducting investigations.

“Broadband availability has literally changed the way we live our lives and represents a form of social interaction that can yield investigative opportunities. It can provide officers with details such as lifestyle, associations, geographic locations and an insight into a person’s lifestyle that could otherwise take months of surveillance to realise.”

DCI Simpson said there is a “lack of awareness” about digital evidence and open source intelligence opportunities within the investigative community.



“Investigators must ask suspects the question: ‘have you got a social networking presence’, and if so, examine the online resource available. This applies for victims, witness and suspects,” said DCI Simpson.

He added that in some cases during trial at court, the defence has produced correspondence between a suspect and the complainant, which can undermine the entire investigation.

DCI Simpson said forces should adopt a digital evidence strategy that “clearly articulates” what can be done in terms of open source intelligence gathering: “Without a shadow of a doubt, open source intelligence should be in obtained for all crimes, looking in detail at any interactions conducted online.”

He added that NPIA legal experts are “always on hand” to provide guidance on intelligence issues such as when direct surveillance authority is needed and when a covert internet investigator should be deployed.

Taking threats seriously

DCI Simpson there is a wealth of internet-based applications that can provide open source intelligence opportunities, ranging from mobile

phones to games console networks.

However, websites such as Second Life and World of Warcraft may not be taken seriously by investigators due to their ‘virtual’ existence. DCI Simpson said organised criminals are now targeting these websites, utilising them to launder large amounts of money.

“Second Life is an online 3D virtual world imagined and designed by its users,” said DCI Simpson.

“Users purchase a virtual currency (Linden dollars) that allows them to trade and operate businesses online. It is an unregulated financial institution and one which is being used as a haven by criminals to launder illegal profits due to the unmonitored flow of money.”

DCI Simpson said Second Life is just one of many ‘virtual’ worlds frequented by criminals. Another recent case in China involved an individual reporting to the police that his \$1,500 ‘dragon sword’ had been stolen from his online World of Warcraft account.



The crime was not taken seriously by the police and the individual later murdered the thief after discovering his identity.

“It may sound like a crime not worth investigating and we may have stereotypical opinions about who inhabits such websites, but it underlines the fact that ‘virtual’ worlds are spilling into the real world,” said DCI Simpson.

How a criminal may benefit from the unmonitored flow of money through virtual worlds such as Second Life:

Online obsession leads to murder

In September 2008 a German man stabbed a British student to death after he became obsessed with his girlfriend through an internet gaming site.

Office worker David Heiss, 21, of Limburg, near Frankfurt, stabbed 20-year-old Matthew Pyke 86 times in a savage and sustained attack after becoming infatuated with his girlfriend Joanna Witton. Nottingham Crown Court was told.

The murder took place after Heiss started stalking Miss Witton through a war games website she ran with her boyfriend from their Nottingham flat.

Mr Pyke and 20-year-old Miss Witton met in 2005 through a website called awwarbunker.com. They started a cyber-relationship through the site, talking about their A-levels, before meeting up and beginning a relationship in real life.

In September 2007 they both started at Nottingham Trent University. Mr Pyke was studying a foundation course in physics while his girlfriend was studying for a degree in environmental sciences.

Mr Pyke was to drop out of his course but the couple shared a flat in Nottingham city centre. In November 2007, awwarbunker.com closed down but the couple set up a new website, warcentral.com, a month later.

Mr Smith told jurors that the pair administered the site, which had some 300 users, up to 40 of whom would visit the site regularly.

Mr Pyke used the alias Shade while his girlfriend called herself Jojo. They first came across Heiss in March last year, when he contacted Miss Witton, telling her that he had a crush on her.

Miss Witton was unaware that behind the scenes Heiss had been reading her online journal and looking at photographs of her on social networking site Facebook.

Future trends, future problems

Multi-skilled digital examination teams are needed to combat emerging and future technical challenges such as netcentricism, a leading expert told delegates at The Investigator's computer and mobile phone forensics conference facing investigators of digital forensics.

According to Angus Marshall, senior lecturer in digital forensics at the University of Teesside, common skills are "no longer appropriate" as the world of technology continues to converge and diverge.

"As the number of mobile storage devices increases along with the memory capacity of hard drives the distinction between portable and desktop products is blurring; a convergence is taking place and investigators must be ready to customise skills to cope with this challenge," said Mr Marshall.

"A smartphone, for example, is both a computer and a mobile communication unit and should be treated, from an examination point of view, as both."

At the same time, no single software developer exists and there continues to be multiple operating software and functions; another challenge for digital investigators.

However, perhaps the most daunting of challenges is the possibility of netcentricism, or remote network storage.

"It is possible, in the future, that devices will have much less storage facility, and that local storage will be replaced by a remote function," said Mr Marshall.

It operates very much like the Google document function, which allows a number of remote users to access and edit a document that is saved on a provider's network as opposed to a single device's network.

"This would present challenges for investigators because a number of cheap devices could become part of a much larger network that is situated

offshore, could be distributed in a fragmented way and could be easily replicated,” said Mr Marshall.

The language of murder: forensic linguistics in digital investigations

The role of a forensic linguist can be invaluable to investigators, especially when piecing together non time-stamped mobile phone messages, helping to paint a picture of events and link suspects to a scene of a crime.

Internationally renowned forensic linguist John Olsson told delegates at The Investigator digital forensics conference how an understanding of language structures and patterns of speech can be used to identify anonymous text and email messages for evidence in criminal investigations.

Mr Olsson is the world’s first full time forensic linguist, has been serving as an independent expert since 1994, and has handled more than 300 major cases.

One of those cases was the viscous murder of Stephen Green, 55, who was attacked in an underpass beneath the M1 in Dunstable, Beds, by a gang of four as he cycled home on May 5, 2007.



John Olsson

He was kicked and stamped on by the teenage robbers and died in hospital nine days later from a blood clot as a result of the injuries he suffered.

Darryl Bennett, 17, Richard McNamara, 17, Nicholas Garland, 18, and Shane Liddy, 18, all from Luton, were found guilty of murder following a three-week trial at Luton Crown Court. Mr Olsson’s analysis of seemingly random text messages linked to three mobile phones helped reconstruct a conversation and net the offenders.

At the centre of Mr Olsson’s examination were the messages sent by ringleader Bennett, to his girlfriend, Sam, 16. Sam was also Liddy’s cousin. On

top of this were references to a Sandra, Liddy’s mother and Sam’s aunt. All messages were deleted.

“Many of the messages were not time stamped, but we were able to obtain the message log details from the mobile phone service provider. Although we knew the frequency and content of the messages, we did not know the sequence in which they were sent and received. It was a case of working out who sent which message to whom,” said Mr Olsson.

In order to reconstruct whether a conversation of significance had taken place, Mr Olsson analysed “units of language” that would give clues to the meaning of the conversation that had taken place following the crime.

Evidential value can be obtained from studying, for example, sequences of challenges and denials; topic dismissal; ‘coolness moves’, which can follow accusations; requests for information; and attempts to ‘block’ a conversation.

“These are all ‘moves’ made during discourse and can be of evidential value, often providing clues as to the roles individuals adopted during an incident,” said Mr Olsson.

The messages

In total, Sam’s phone contained 150 text messages. Some of the connected content included:

Nick Sandra cn da blood on ur hands darryle Sandra sed she cn da cut on ur hed u sed u wldnt do robbery agen n u promised u wldnt do nuffin wen shane was der u lied n wt was u guna say u sed 1st fingz 1st n den u stopped wt dt al bowt ring me or tb lv sam x
Wat we didn’t sam

Y u liein shane told me ur an idiot u promised u

wldnt nw I na hu I can n
cnt trust n ur on da cnt
trust list x

Shane chattin shit trust
me

Yh k wt eva I
bored... shane mangled e
bn sick evry wer... I swear I
fink shane guna need his
stomach pumped or summin
swear dwn I shook lol x sam x

“The first of these messages is an opening challenge made by Sam to Bennett, followed by his denial,” said Mr Olsson.

This is followed by a second challenge, a repeated denial before the topic is finally dismissed, what is described as a ‘coolness move’.

That is a very common pattern of discourse, said Mr Olsson. He added that the linguistic question is: did Sam and Bennett engage in a text conversation in which an assault and robbery are mentioned, where was Bennett when this conversation took place, and what kind of linguistic evidence can be adduced to support the above points.

He added: “It is interesting to note Bennett’s use of the plural ‘we’ in his initial denial. Personal participation is being denied, but what is not being denied is that something happened. In the denial, the function of ‘what’ is a speech element, not a written convention and is a discourse move made by Bennett aimed at restricting the receiver’s access to information.”

Linking cell site information to the message content helped prove the guilt of the four teenagers and they were eventually given minimum sentences of between 12 and 19 years.

“You can not write software that is able to evaluate every sentence made via mobile phone text messages due to the many idiosyncratic spellings, terminology and forms of language,” said Mr Olsson.



“The process relies on individuals and forensic linguistics can add value to a digital forensic investigation. It is not the analysis of language, but the analysis of conversation.”

Mr Olsson’s work includes analysis of all kinds of texts including ransom notes, suicide texts, threat texts and a variety of other types of documents. He has analysed the authorship of many cell phone text messages and has assisted in a number of investigations involving electronic media, including email messages. He has also analysed the discourse of codes, including gang codes, for police officers in intelligence operations.

What lies beneath: the emerging threat of steganography

A technique known as steganography that potentially allows organised criminals and terrorists to relay digital messages undetected, is a latest threat facing law enforcement agencies, according to Dr Tim Watson, head of the Department of Computer Technology at De Monfort University.



Speaking to delegates at The Investigator computer and mobile phone forensics conference, Dr Watson said a host of criminals could be communicating through the sending of messages encrypted steganographically in e-mail correspondence. “The word steganography is of Greek origin and means ‘concealed writing’,” said Dr Watson.

He added that while computer files that are encrypted may draw the attention of law enforcement investigators, steganography overcomes that problem by concealing secret messages in seemingly innocuous documents. “Generally, messages will appear to be something else, such as an image, a word document, a music

file or some other text,” said Dr Watson.

“Steganography hides the fact that a message is present at all.”

“The advantage of steganography is that messages do not attract attention to themselves. Plainly visible encrypted messages, no matter how unbreakable, will arouse suspicion and may in themselves be incriminating in countries where encryption is illegal.

“Therefore, steganography can be said to protect both messages and communicating parties.”

Steganography includes the concealment of information within computer files. In digital steganography, electronic communications may include steganographic coding inside of a transport layer, such as a document file, image file or program. Media files are ideal for steganographic transmission because of their large size. As a simple example, a sender might start with a harmless image file and adjust the color of every 100th pixel to correspond to a letter in the alphabet, a change so subtle that someone not specifically looking for it is unlikely to notice the alteration.

Dr Watson said steganography works by altering the series of numbers that translate as the pixels within a digital image, a techniques known as least significant bit steganography.

“It is used to hide messages on the internet and on other communication media, and works by changing the last digit of the number that represents one of the three colour values, red, green and blue, at each pixel.

“The difference between 11111111 and 11111110 in the value for blue intensity, for example, is likely to be undetectable by the human eye. Therefore, the least significant bit can be used, more or less undetectably, for something else other than color information.”



Image of a tree. By removing all but the last two bits of each colour component, an almost completely black image results. Making the resulting image 85 times brighter results in the image below.



Image of a cat extracted from above image

Dr Watson said computer programs as basic as a word processor can easily extract the altered pixel information to reveal the hidden message, which could include, for example, child sex abuse images, maps of geographical locations, or a terrorist cell communication.

“A single dot within a word document, when shrunk, is capable of hiding an image that can be sent and exchanged for example, between members of a child abuse network.”

He added that evidence involving suspected child sex offenders shows that incriminating images often remain in a place that can be conveniently

XRY XACT

The leading systems in mobile forensics



**FIND THE EVIDENCE WITH MOBILE PHONE
FORENSIC SYSTEMS BY MICRO SYSTEMATION**

MICRO SYSTEMATION

Mobile: +44 (0) 7776 466 451 | Office: 0800 234 2450 | Fax: 0800 234 2449
Email: sales@msab.com | Web: www.msab.com

www.msab.com

accessed: “Steganography allows individuals regular and instantaneous access to illegal images; it is convenient for offenders and a problem for investigators.”

Other tools are more sophisticated. Steghide, for example, is a program which hides bits of a data file in some of the least significant bits of another file in such a way that the existence of the data file is not visible and cannot be proven.

Dr Watson said a particular convenient form of digital media that suits steganography is the JPEG file.

“A JPEG file, such as an image, always introduces some error into the decompressed data; it is possible to exploit this for steganographic use,” he said.

It is alleged, added Dr Watson, that Al Qaeda cells

have used steganographic techniques to encode messages into images before sending them via email.

The USA Today, for example, in July 2001, reported that: “Lately, Al-Qaeda operatives have been sending hundreds of encrypted messages that have been hidden in files on digital photographs on the auction site eBay.com.”

However, no actual proof exists which can ground such allegations in truth said Dr Watson. An actual recent case featuring steganography saw compromised credit card details remain on a company’s website, encoded steganographically into images as opposed to being extracted.

“The compromised details never left the company yet were hidden with near instantaneous access by the criminal gang visiting the website,” said Dr Watson.

The Investigator conferences

ESSENTIAL LEARNING FOR TODAY’S INVESTIGATORS

A world of learning

DIARY OF FORTHCOMING CONFERENCES

25 & 26 November 2009 - INVESTIGATING MAJOR CRIME

8 December 2009 - INVESTIGATING ROAD TRAFFIC INCIDENTS

15 December 2009 - PRATICAL MOBILE & COMPUTER DIGITAL FORENSICS

(All of the above conferences are being held at Tally Ho!, West Midlands Police Training & Resource Centre)

For further information contact: 0844 660 8707 or email: info@the-investigator.co.uk

Digital Standards

As digital evidence becomes a more integral part of investigations it is vital that officers are aware of the good practice guidance that exists. Computer forensic expert Angus Marshall looks at the guidance and provides advice on how to implement it.

The next four years will be a time of great change in forensic science. This is being driven by Andrew Rennison, the forensic science regulator. Andrew took up his appointment in April 2008, working through the Home Office, as a result of the infamous “Forensic Science on Trial” report.

In this report, a number of concerns were raised about the quality of forensic science in the UK and the relative ease with which anyone can set themselves up as an expert witness.

Since his appointment Andrew and his team have produced a set of proposed regulations for forensic science providers which will have an impact on every part of the system, from crime scene right through to court.

The key documents are the “Manual of Regulation”, which lays down the rules by which the regulator operates, and the draft “Quality Standards for Forensic Science Providers” which defines how forensic science providers will be assessed by the accrediting body (UKAS). (Both documents are available from <http://police.homeoffice.gov.uk/operational-policing/forensic-science-regulator/reports-publications/>)

The Quality Standards document is fairly lengthy but at the back, it contains a series of appendices covering every discipline which is currently thought to be relevant – and more can be added.

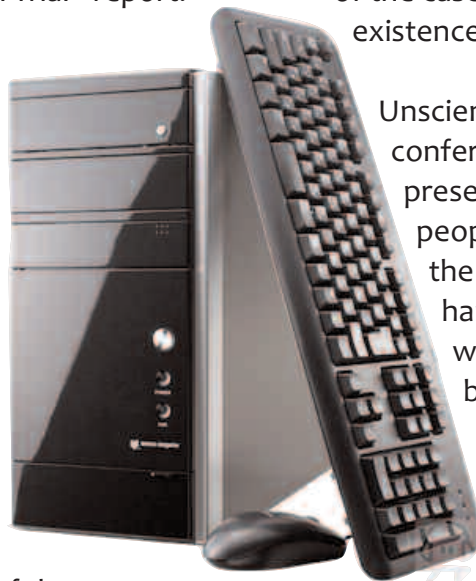
Currently, the only appendix which is nearly ready for publication is that for Digital Evidence – and it worries me.

It worries me, even though I've helped to write it, because I know that very few people outside the world of forensic geekery are aware that we have had some standards to work to for years. Ever since I started to practice, I have been careful to comply with the principles and procedures laid down in the “ACPO Good Practice Guide for Computer Based Electronic Evidence” (version 4 is currently available at http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf), but very few of the case officers I speak to are aware of the existence of this document, let alone the content.

Unscientifically, I carried out a poll of CSIs at a conference last year. Before I gave my presentation I asked a room of over 200 people how many of them had a) heard of the manual and b) read it. Only one or two hands went up – and they were people who'd heard me talk on the subject before.

So – if no-one outside the digital evidence world knows about it, and cases are not collapsing because of that – why do I care about an apparently little-known document so much?

Simple – the ACPO Guidelines describe things like the correct way to shut down a PC during seizure, how to handle mobile phones, what NOT to do as well as what to do. It is the most up to date guide available and, although much of what it says applies to lab. work, a lot of it applies to everyone involved in the investigation of crime. It supercedes all other advice on digital device handling (especially that given in the Major Incident Manual which is just plain wrong now). Mishandling a device at any stage can create a weakness in the



case, I know – I look for those chinks when I am carrying out defence examinations and am duty bound to inform the court of anything that may weaken the prosecution case.

At the moment, there is a way round this issue, of course. Proper contemporaneous notes allow one of the four principles laid down by ACPO to be satisfied and give the digital evidence examiner and opportunity to explain any discrepancies, BUT - in the regulator's world we are proposing a new principle – that the forensic science provider “shall have the ability to demonstrate that all tools, techniques and methods are fit for purpose”.

This means that every process applied to a digital device, from point of seizure through to the end of the examination MUST be demonstrably appropriate and safe. Currently, there really is only one way to do that – by following the ACPO Guidelines.

Let's face it – digital devices are not going to go

away – they're just going to keep getting smaller and more powerful, and more useful to everyone. As sources of evidence and intelligence they are invaluable and crop up in more and more enquiries, but if the processes used can be questioned their value disappears instantly.

About the author

Angus Marshall is an independent forensic computing consultant and trainer, specialising in Internet crime. Most recently he has assisted with the preparation of briefing materials for juries in cases involving Internet communications and is the Forensic Science Society's representative on the Forensic Science Regulator's working group on digital evidence. His book, “Digital Forensics : Digital Evidence in Criminal Investigations” was published by Wiley in November 2008 and provides a clear guide for investigators and lawyers on key issues relating to digital devices.

PNC Training



PNC (Police National Computer) Training is offered to Police Forces and other organisations that have PNC Access.

Training is delivered at the client site although a mobile classroom. All training is carried out by accredited NPIA trainers who have the appropriate security clearance.

Standard Courses:

- 5 Day - Vehicles, Property and Names Enquiry Course • 4 Day - Vehicles and Names Enquiry Course
- 2 Day - Vehicles and Property Course • 3 Day - Names Enquiry Course

For a free consultation on your PNC training contact us on: 07811 982022 or email: pennymayhew@me.com www.pnctraining.co.uk



Conference Sponsor



Frontline police officers from around the country as well as Garda and Jersey State Police attended a conference which looked at best practice in volume crime investigations.

Organised by the Investigator, experts gave presentations in subjects including interviewing, the PNC, giving evidence in court and effective relationships with the CPS.

Conference sponsors SmartWater were also present with CEO Phil Cleary giving a presentation on the successful crime prevention initiatives the company is working on alongside police forces.

Carol Jenkins editor of the Investigator said: "The day was a great success and managed to bring together experts in a variety of disciplines who all gave best practice advice on dealing with volume crime cases. We look forward to holding similar conferences next year."

investigating volume crime conference, Mr Farmer said a range of issues, which must be rectified, are behind the fact that up to 50 per cent of all arrests do not proceed to court.

Ranging from not properly understanding what to disclose pre-interview and not fully utilising the investigative interviewer's tool set, Mr Farmer called for a "reinforcement" of the interviewer's responsibility and a drive to "make officers more confident in their role".

"Evidence suggests that officers are quite unsure about how to use bad character evidence, adverse inference and special warnings. Rather than being afraid of using these powers, officers' objectives seem to change in the presence of a solicitor," said Mr Farmer.

He added that a "perspective is needed" on the role between interviewing officers and solicitors.

A solicitor's only role is to protect and advance the legal rights of his/her client, through gaining information usually through disclosure to assist in this aim.

"Any friction between the interviewer and the solicitor arrives at the point of disclosure," said Mr Farmer.

"Unfortunately, in many cases, solicitors are obtaining all the information they desire;

Knowledge gaps 'must be filled' to improve standard of investigative interviews



The quality of interviewing nationally is poor, with gaps in knowledge and models of good practice not being realised, according to Alan Farmer, an experienced investigative interviewer trainer.

Speaking to delegates at The Investigator's

statements and full disclosure pertaining to incidents. Operationally, that can not be good practice.”

Mr Farmer said investigators are “only required to disclose the facts” to be discussed in the interview which is about to be conducted.

“Although officers are required to disclose the custody record, information contained on the EDL is not required to be disclosed and information relating to police searches and witness details, for example, could be inadvertently disclosed and undermine a disclosure strategy.”

In order to achieve admissions from suspects, Mr Farmer believes “determining what a suspect wishes to reveal before informing the suspect what is known already”, is a model of good practice.

“The dangers of disclosing too much information allows a suspect of a lying persuasion to align an account to the information disclosed,” said Mr Farmer.

He added that every investigation should be regarded on a case-by-case basis; it is very much a thinking man’s game and officers must be aware of what they are doing and why.

When deciding what and what not to disclose, Mr Farmer said the emphasis is on individual officers to decide, taking into account that appropriate disclosure allows a solicitor to advise their client whilst allowing interviewing officers to test the truthfulness of the suspect’s account.

“It is up to investigative/interviewing officers to judge what can be gained and lost from disclosing evidence. It is no value to withhold evidence that is already known to a solicitor and officers must check custody records to gain an understanding of what a solicitor may already have knowledge of, such as terms of arrest and what was stated by an arresting officer.”



Overcoming the ‘no comment’ situations

The importance of pre-interview disclosure decisions may be realised during ‘no comment’ situations, said Mr Farmer.

“It is considered by some as a problem. However, adverse inferences – Section 34 of the Criminal Justice and Public Order Act 1994: ‘fail to mention when questioned something which later rely on in court’ – if the appropriate questions have been asked, allows the investigator to pursue an interview and close off the defence.”

Mr Farmer said the significance of Section 34 “does not lie on a silence during interview, it relies in reliance at trial at something which should have been said in interview”.

He added that the asking question is “not was it reasonable to rely on a solicitor’s advice, but could be the appellant reasonably had been expected to say what he now relies upon at trial”.



“The service needs to professionalise itself in relation to the ‘no comment’ interview by ensuring more time is dedicated to investigative interviews; the average time of an interview is around eight minutes, which is not long enough.”

Mr Farmer also questioned if managers are properly supporting interviewing officers.

“Is it correct to send one officer to conduct an interview? Can a single officer listen to answers, formulate questions and challenges and manage topics without support? Is it good practice to ask an officer to carry out a ‘quick interview’? The simple answer is no.”

Bad character evidence and special warnings: useful tools

Special warnings under Criminal Justice and Public Order Act 1994, sections 36 and 37, are used when a suspect, after arrest, fails or refuses to answer certain questions, or to answer satisfactory after due warning. Mr Farmer believes it is an “under-utilised tool”.

“Officers are unsure of when to use a special warning, and operationally I am aware that officers issue a special warning and then cease interviewing. That is the wrong procedure; questions must follow in relation to the fact a suspect is being asked to account for.”

Mr Farmer also called for greater training to be given in the use of bad character evidence.

Bad character evidence is evidence of, or a disposition towards misconduct; other than evidence which has to do with the alleged facts of the offence with which the defendant is charged or is evidence of misconduct in connection with the investigation or prosecution of that offence.

“It is a fantastic tool and is much more than a list of past convictions,” said Mr Farmer.

“Detailed reports of previous offending history and misconduct, for example, can be a valuable resource. If an investigator knows a suspect’s claim to be of good character can be challenged, then it must be pursued. Major investigating units, for example, incorporate planning time for this type of evidence and I believe it should at least be a post-charge consideration at all levels.”

Section 36 special warning

A Special Warning is given when a suspect is interviewed at a police station after being arrested and fails or refuses to account for any objects, marks, or substances, or marks on such objects found: in or on their person, or footwear, or otherwise in their possession or in any place in which he was at the time of his arrest any object substance or mark, or there is any mark on any such object; and the interviewing officer must inform the suspect:

- (a) what offence he is investigating
- (b) what fact he is asking the suspect to account for
- (c) that he believes the fact may be due to the suspect’s involvement in the offence in question
- (d) that the Court may draw proper inferences from his silence
- (e) that a record is being made of the interview and that it may be given in evidence; then in any proceedings against the person for the offence specified the court, or jury, may draw such inferences that appear fair and proper from the failure or refusal.



Investigative mindset must be encouraged

An end to the mentality of ‘taking a quick statement’ and a better understanding of an officer’s role to investigate crime from the outset will lead to higher detection rates and greater success in the courtroom, an expert told delegates at The Investigator’s investigating volume crime conference.

“Police officers should be encouraged to move away from a role of taking statements and enter into an investigative mindset, which should be viewed as the foundation of investigation strategies,” said Gary Shaw, MBE, the National Policing Improvement Agency’s (NPIA) national investigative interview advisor.

Sharing the NPIA’s 2009 revised seven principles of investigative interviewing with delegates at the event, Mr Shaw delivered a passionate presentation which called for “a better understanding of the role of police investigator from all levels within the police service”.

“We have lost the plot as to what the role of an investigator is, and the seven principles should be viewed as the basic values that must underline investigative practice,” he said.

“Investigation is a core duty of policing. Given that

the interviewing of victims, witnesses and suspects is central to the success of an investigation, the highest standards need to be upheld. In order to do this, forces need to develop and maintain the valuable resource that the skills of their interviewers represent.”

The principles of investigative interviewing

- The aim of investigative interviewing is to obtain accurate and reliable accounts from victims, witnesses or suspects about matters under police investigation.
- Investigators must act fairly when questioning victims, witnesses or suspects. Vulnerable people must be treated with particular consideration at all times.
- Investigative interviewing should be approached with an investigative mindset. Accounts obtained from the person who is being interviewed should always be tested against what the interviewer already knows or what can reasonably be established.
- When conducting an interview, investigators are free to ask a wide range of questions in order to obtain material which may assist an investigation.
- Investigators should recognise the positive impact of an early admission in the context of the criminal justice system.
- Investigators are not bound to accept the first answer given. Questioning is not unfair merely because it is persistent.
- Even when the right of silence is exercised by a suspect, investigators have a responsibility to put questions to them.

Mr Shaw said the gathering of information from a well-prepared victim and witness interview contribute significantly to the investigation.

“An effective interview of a suspect will commit them to an account of events that may include an admission. In the admission, the suspect may detail how the offence was committed and thus the investigation can be more focused. The value of a properly obtained admission can prove the offence, beyond doubt.”

Referring to each of the seven principles in turn, Mr Shaw questioned if all officers and police leaders

understood the significance of them, or are properly encouraged to apply them.

“I believe officers’ analysis of an incident, interviewing skills and confidence in conducting interviews and the presentation of what was obtained through investigative interviews, is lacking,” he said.

“Investigators should be trained to question everything. What does it mean, for example, if an individual states he/she has ‘been robbed’? It is a mindset that will help officers know what information to pursue.”

Mr Shaw said it is a mindset that must be pursued “across the service” and at “all levels”.

He added that although it is important to act fairly, as stated in the principles, officers must remember the importance of being persistent.

“Questioning should pursue throughout an interview, even when a suspect is silent. The well informed officer, with well presented material during an interview, can encourage answers and build a better case.”

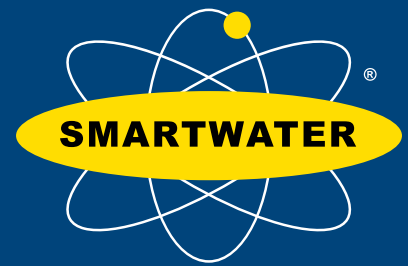
Mr Shaw said the strategic role of taking a statement should never be underestimated.

“The police service is not a confession-based culture and the taking of a statement should not be viewed as a chore. Far from a quick task, it should be considered an integral part of any investigative strategy.

Making better use of PNC can generate greater intelligence

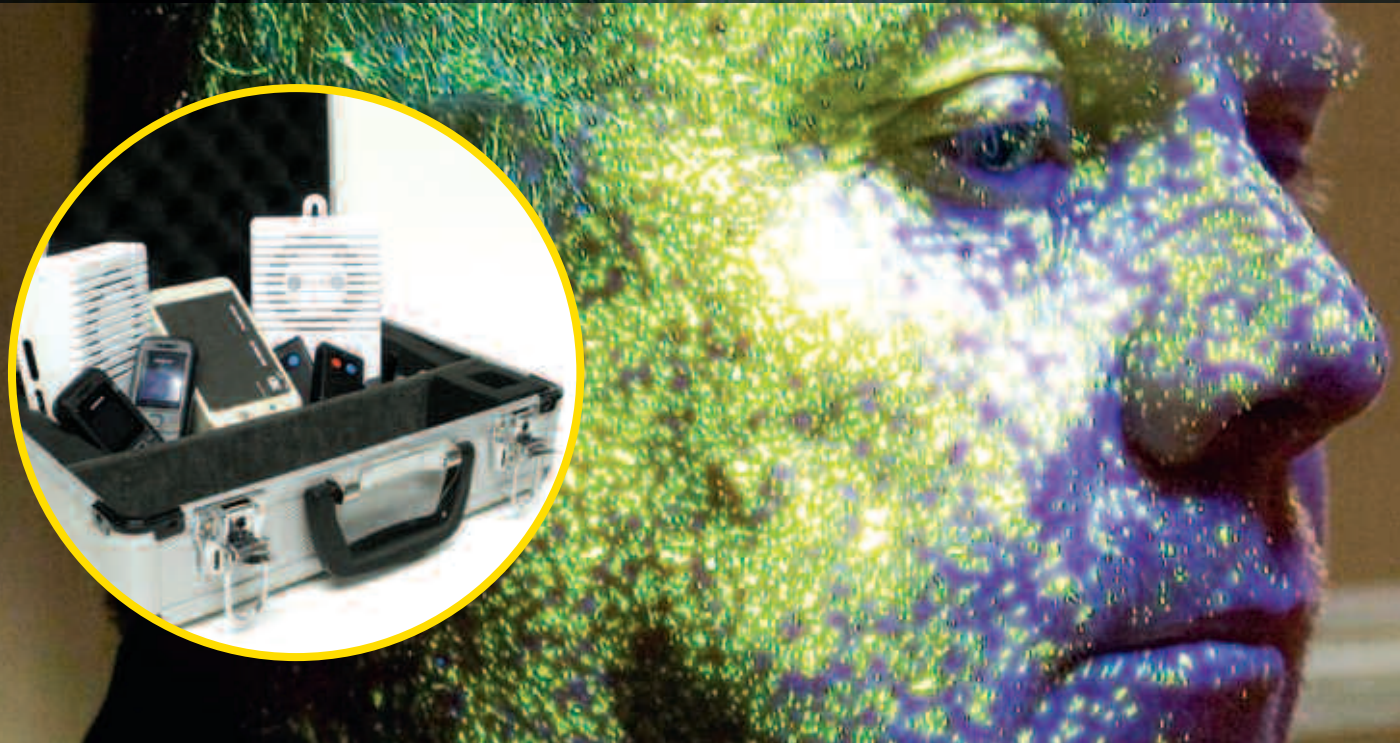
Increased training in how to utilise the Police National Computer (PNC) could provide greater intelligence to investigators and help net more prolific and priority offenders.





TRACEABILITY = ACCOUNTABILITY

Use our KEVIN to Capture and Convict Persistent Offenders



SmartWater's Rapid Deployment Covert System, for exclusive use by Law Enforcement Agencies

KEVIN is SmartWater's innovative, standalone, covert system designed for Police-led covert operations. KEVIN deploys SmartWater's Index Spray System: a robust forensic liquid which marks the skin and clothing of offenders, irrefutably linking them to a specific crime.

- Enhanced forensic and investigative opportunities
- Responsible for hundreds of convictions
- Proven in Courts of Law
- 100% Conviction rate

Offers Enhanced Features:

- Wireless CCTV and audio evidence capture, including time and date stamp
- "Double knock" PIR system with SMS activation alerts to investigating officers
- Battery life of up to 30 days (rechargeable)
- Requires no specialist training or tools to install

Available to rent from just £320 + VAT per month, and includes:

- Installation advice
- Scenes of Crime training
- Forensic Analysis
- Expert Witness Statements (FSS Trained)

For more information contact SmartWater's Crime Support Team on 0800 521 669 or email crimesupport@smartwater.com



0800 521 669

www.smartwater.com

© SmartWater Technology Limited 2009.

Information and training for Police Officers provided by The SmartWater Foundation - a not-for-profit company, limited by guarantee.

Devoting more time to officers' understanding of the Police National Computer (PNC) would help generate more information about suspects as well as alerting officers in neighbouring forces to important details related to individuals, believes Penny Mayhew, a leading PNC trainer and consultant.

Speaking to delegates at The Investigator's investigating volume crime conference, Mrs Mayhew said the PNC is a valuable tool that is capable of generating "detailed profiles" of suspects, vehicles and property.

"As well as detailing individuals known to the police through, for example, arrests, convictions, wanted status and disqualification from driving, the PNC provides search indexes that can yield significant information such as locations frequented, known associates, modus operandi and membership to organisations," said Mrs Mayhew.

Other useful information that can be generated following an informed search of the PNC can inform officers of a suspect's characteristic behaviour.

Investigators can learn, for example, what clothing a suspect was wearing at the time of arrest and access a photograph location; a useful fact if attempting to cross reference a description of an offender, said Mrs Mayhew.

"This type of information can be used to help locate a suspect as well as linking a series of burglaries, for example, to individuals who match a description or the methods used when committing a crime."

Another investigative benefit of the PNC is the ability to carry out a transaction enquiry. It allows officers to determine whether a suspect has been checked against the PNC, when, where, the reason, and who by; another effective way of generating

information about an individual.

Furthermore, added Mrs Mayhew, since the Bichard enquiry, every individual who comes into contact with an officer, regardless of arrest or conviction, is included on the PNC and is subject to a search.

Warning signals can also be added and retrieved from the PNC, alerting an officer of an individual's known reaction to being arrested, for example.

However, Ms Mayhew added that custody staff must continually update the PNC if it is to be properly utilised by investigating officers.

"Anything that may be of interest should be added to the PNC so that it becomes available through an indexed search."



She said this would enable better use of the PNC's ability as a "local cross reference tool".

This refers to a reference held on the PNC, which identifies the existence of further police information about the subject which would not normally be held on the PNC. Generally, this is information held on a local level by a police force's intelligence department and lets other forces know that further intelligence exists.

“It also offers the facility to have an ‘intelligence marker’ placed against the subject – this means that a force/station is actively seeking intelligence about the subject,” said Ms Mayhew.

“For example, if a person is stopped and checked, and the PNC check highlights that there is an intelligence marker held against the subject, the officer asking for a check is then obliged to contact the force which placed the marker, and to tell them about the subject and why they have checked him/her.

“The local cross reference information will show the force/station which placed the report on the PNC, with a reference number to quote should further enquiries be necessary.”

A suspect vehicle?

Mrs Mayhew said the PNC is an effective tool for investigating vehicles and has a number of indexes that can prompt police action. For example, as well as holding information on all vehicles registered by the DVLA, the PNC also contains an index of vehicle unregistered but of police interest.



A multiple vehicle search can also be conducted, used for identifying any link between incidents, vehicles and witness accounts.

“Officers may also wish to conduct a post code enquiry, which produces a list of possible vehicles a suspect may have access to,” said Mrs Mayhew.

She added that the PNC has an ‘action’ report facility that requests officers to make contact should a vehicle of interest be the subject of a PNC check, before completing a ‘react’ report.

“If officers are fully aware of the investigative benefits the PNC can bring, then a much more informed intelligence picture can be generated and obtained,” said Mrs Mayhew.

A new look at criminals



Delegates at The Investigator’s investigating volume crime conference saw first hand the benefits of a unique technology that produces near photo-realistic facial composites based on witnesses recognising individual characteristics as opposed to recalling and describing them.

The software, called the EFIT-V system, is being used by 12 police departments in the UK and by four European countries. In pilot studies, it led to twice as many identifications of suspects as traditional methods.

Typically, facial composites are currently generated by asking witnesses or victims to try to



visualise the face of the person who committed the crime by describing individual facial features and answering questions such as ‘what was the mouth like?’ or ‘what shape was their face?’, sometimes with the help of pictures. The various elements of the face are then ‘pasted’ together to create a facial composite.

But Dr Chris Solomon, head of the project team that has developed the new approach to creating facial composites at the School of Physical Sciences, University of Kent, believes the images produced are often not as accurate or realistic as they could be.

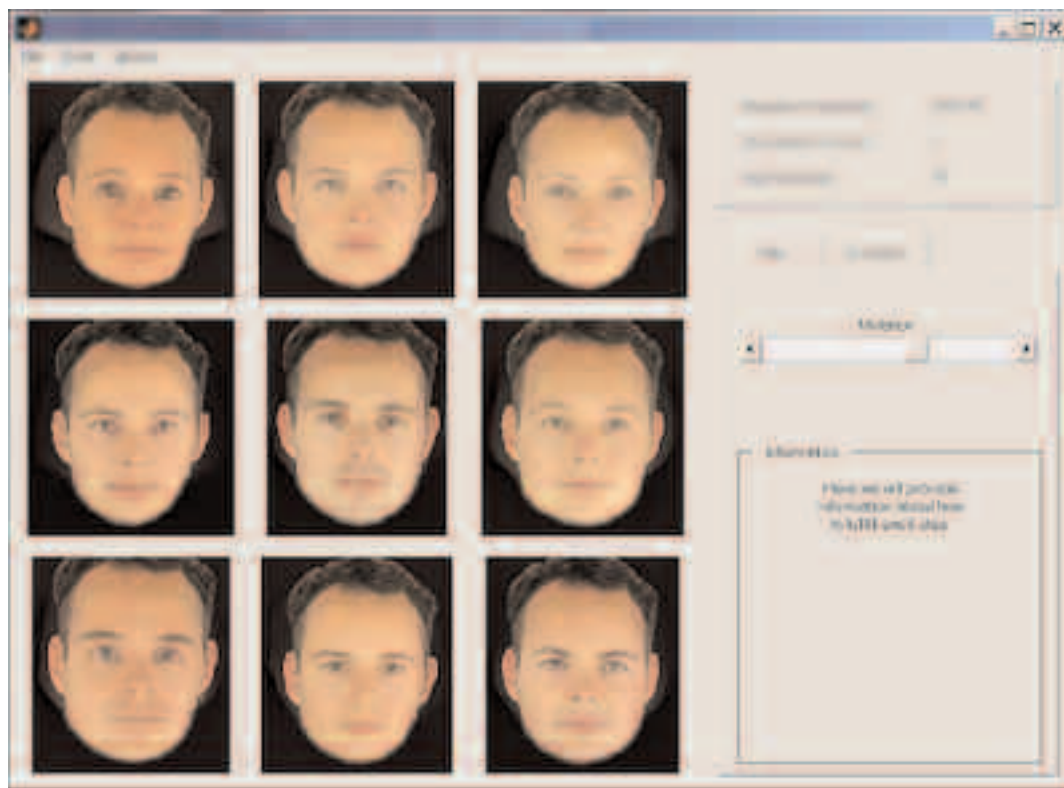
“The problem with this approach is that it doesn't take into account how the memory actually works. A number of psychological studies suggest that we are not so good at recalling and describing a face.”

EFIT-V’s software generates its own faces that progressively evolve to match witness’ memories.

The witness starts with a general description such as, for example, ‘I remember a young white male with dark hair.’ Nine different computer-generated faces that roughly fit the description are generated, and the witness identifies the most matching

features. The software uses the best fit as a template to automatically generate nine new faces with slightly mutated features, based on what it learned from the rejected faces.

Each facial image is represented by an array of principal components. "If we change just one of these parameters it alters the image presented," said Dr Solomon. Once a feature is correct it can be 'locked', and the rest of the face evolved around it. "It is an evolutionary procedure and over a number of generations, the computer can learn what face a witness is seeking to present," said Dr Solomon.



The system also has a host of tools that allow the operator to add significant features such as facial hair, ageing, skin tone and jewellery. Facial composites produced by EFIT-V can also be exported to other programmes such as Photoshop.

The cycle continues until the witness is happy with the likeness. Each generation can be calculated in seconds, making the process far quicker than retrieving facial features from databases and trying them one by one.

He added that one advantage of this technique is its ability to be used on witnesses who can't recall

details about a suspect's appearance, but say that they would remember the face if they saw it again.

"Traditionally methods are unable to help these people but by tapping into recognition instead of recall, the EFIT-V system can be quite effective even when witnesses say they can't describe a person," said Dr Solomon.

A one year pilot study of the software led to a hundred per cent increase in the production of composite images, bringing obvious benefits to any officers investigating volume crime. Furthermore, EFIT-V can produce images in half the time as

traditional methods and can be operated with only a modest amount of training.

"Because of its quick production of composite images, EFIT-V has beneficial implications for providing e-fits in tackling volume crime," said Dr Solomon. "The current procedure for generating an e-fit and disseminating it to the public and other forces is quite time-consuming but EFIT-V is reducing this significantly."

The license cost for EFIT-V is £1,899 per annum and the producers, Visionmetric, run a three-day training course to ensure it meets the needs of individual forces.

VisionMetric Ltd, Canterbury Enterprise Hub,
University of Kent, Canterbury, Kent, CT2 7NJ, UK
Tel: +44 1227 824667
E: enquiries@visionmetric.com
www.visionmetric.com

Conference reporter - Daniel Dexter
daniel@the-investigator.co.uk

Collateral Benefits of Positive Investigations

Volume crimes are a moveable force which continually fluctuate and are ultimately driven by two things; confidence amongst offenders and opportunities for profit.

Persistent criminals will concentrate their efforts on whatever they believe will earn them the most reward for the minimum effort. What's more, they will only stop targeting something when it either stops being profitable or the associated risk becomes too great.

Therefore, it follows that in order to suppress volume crime, it is necessary to capture and convict persistent offenders, preferably those known to be responsible for the significant majority of offences. This also has the knock on effect of sending out a powerful deterrent message to other would-be criminals.

It is this ability to capture and convict persistent and prolific offenders (PPOs) that has established SmartWater as one of the most powerful crime reduction tools in the UK. SmartWater provides



robust forensic evidence to the Police with no charge for forensic analysis or the provision of expert witness statements, should the matter go to court.

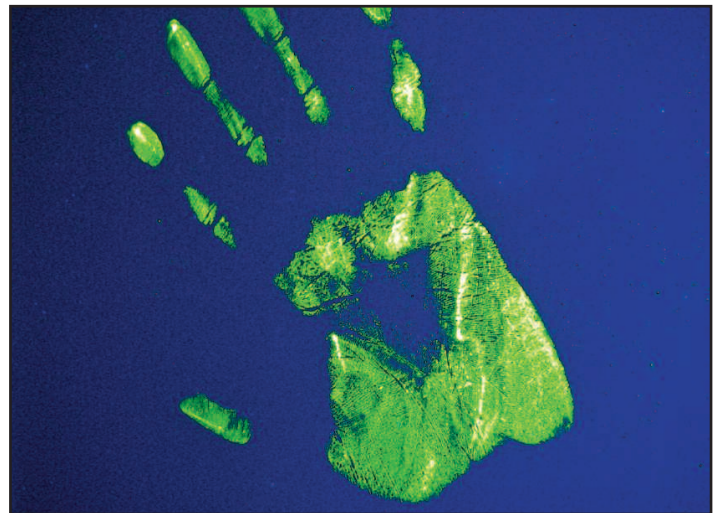
This has helped the Police to secure more than 600 criminal convictions across the UK, whilst maintaining a 100% conviction rate – having never lost a case in court when SmartWater evidence has been used. The majority of these convictions have been achieved as part of Police-led covert operations, specifically targeting persistent offenders.

South Yorkshire Police in Doncaster have had

phenomenal success using this technology within a rat trap vehicle to secure the arrest of over 40 known car thieves. The trap car was baited with a Sat Nav or



other valuable to tempt opportunistic thieves and rigged with SmartWater's Index Spray System as a means of forensically tagging offenders at the point of committing a crime.



The SmartWater liquid stays on skin for many weeks and on clothing for even longer, acting as an undeniable link back to a specific crime scene. In addition, offenders will leave behind significant levels of residual evidence such as foot treads and handprints which can be photographed and catalogued to help build a prosecution case. The trap car was used to directly target the area's most prolific offenders, who despite being well known to the Police, often alluded arrest because there was no way to link them with a specific crime.

Over a two week period the trap car led to the successful arrest and prosecution of three of Doncaster Top 5 PPOs for vehicle crime, with all three activating the SmartWater Spray System.

This included Stephen Barrett, Doncaster's most prolific vehicle crime offender. During the three

months that these offenders were off the streets of Doncaster vehicle crime fell by 75%.

This subsequently led to Doncaster Police placing “Am I the Trap Car?” warning signs across the area, attacking criminals with a form of psychological warfare by playing on their fears of detection.



Stephen Barrett

The use of SmartWater to capture persistent offenders has been successfully implemented by Police Forces, Law Enforcement Agencies and Commercial Organisations across the UK.

SmartWater covert systems have been deployed within a wide range of environments, including trap

cars, rat trap houses, freight vehicles, gaming machines, heritage buildings, utility sites, are more.

These installations have helped the Police to secure prison sentences of up to 17 years amongst PPOs. Word of this has spread quickly amongst the criminal fraternity, and

is continually aided by an ongoing media strategy generating a readership of over 17 million people every month.

SmartWater also employs former Police officers and crime prevention specialists to link in with Police-led operations and carry out high visibility stop and searches to look for traces of SmartWater, putting further pressure on criminals.

All of this activity is having a significant impact on criminal behaviour, with leading criminologist Professor Martin Gill carrying out academic research on over 100 criminals to assess their knowledge and awareness of SmartWater. His



results revealed that 91% of those interviewed could describe what SmartWater was and how it worked. Furthermore, an incredible 74% said that they would abandon their plans to break into a building if they believed SmartWater to be in use.

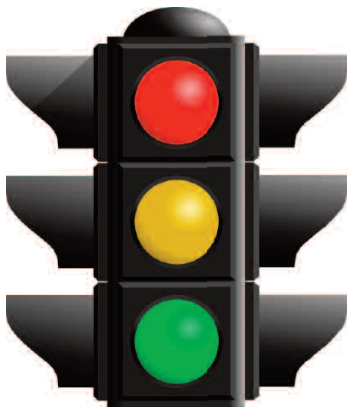
This underlines the power of SmartWater to not only provide robust evidence to assist investigations, but also the additional effect this is having on criminals and crime in general. With Police Force across the UK continuing to check for SmartWater, it is becoming an ever more effective deterrent, attacking the fundamental anxiety that exists within all criminals – the fear of getting caught.



For more information about SmartWater please call us on: 0800 521 669 or email: enquiry@smartwater.com

www.smartwater.com





INVESTIGATING ROAD TRAFFIC INCIDENTS

CONFERENCE



8 December 2009

West Midlands Police Training & Resource Centre - Tally Ho!

APPLY BEST PRACTICE TO TRAFFIC INVESTIGATIONS

The Investigator magazine is holding a one day conference for those involved in the investigation of road traffic incidents.

Experts from industry and police forces will be delivering a series of presentations on current best practice surrounding the investigation of road traffic incidents.

The day will be opened by Inspector Alan Jones, the spokesperson on traffic matters from the Police Federation of England and Wales. Alan will outline the main issues facing traffic officers and look at ways to address these challenges.



£195.00

With 15% early bird discount
£165.00

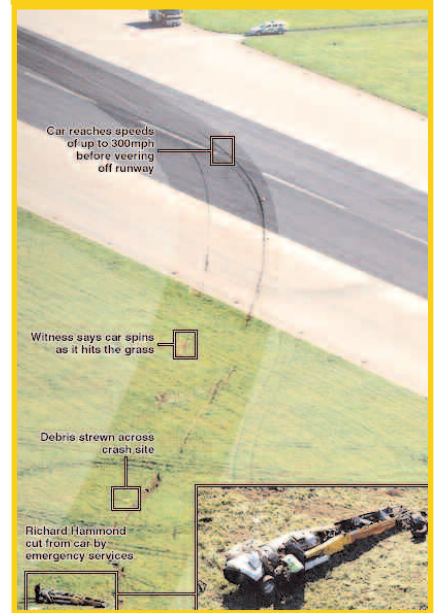
(Book before 23 November)



Speakers and presentations include:

- **David Price** - the expert who gave evidence in the Princess Diana Crash inquiry; the Richard Hammond crash and the Selby Train Crash will be speaking on 'The Forensic Investigation of Vehicle Component Failures'
- **DS David Hindmarsh, Senior Investigating Officer from the Met Police Collision Investigation Unit** – Operation Stride, How the Met used undercover officers for the first time ever to investigate the suspect of a road death in Holloway North London.
- **Inspector Simon Westwood – Central Motorway Police Group** - Contemporary issues surrounding the investigation of fatal road traffic collisions on motorways
- **Det Sgt Ian Orton – Central Motorway Police Group** - Use of Automatic Number Plate Recognition Technology (ANPR) as an investigative tool
- **Derek Hance** – Renowned Accident Investigator - The quality of accident investigation reports
- **Clive E Neal-Sturgess BSc, PhD, CEng, FIMechE, FIMMM, FRSA, FHEA – Emeritus Professor of Mechanical Engineering** - University of Birmingham

Other speakers to be confirmed



**15%
DISCOUNT**

Early bird

Book and pay before 23 November and receive a 15% discount.
You pay just £165 for the full day

To reserve your place simply email the name(s) of the delegates and contact address to: info@the-investigator.co.uk

You can contact the conference organisers on:
Tel: (+44) 0844 660 8707
or email: info@the-investigator.co.uk

The Investigator conferences
ESSENTIAL LEARNING FOR TODAY'S INVESTIGATORS

Courtroom and Associated Legal Training for the Police

Bond Solon
the legal training consultancy



Bond Solon Training is the leading provider of Evidential and Courtroom Training in the UK. Since 1992 Bond Solon has worked with every Police force in the UK providing specific training courses for a range of police departments, disciplines and ranks.

Bond Solon have worked closely with many Police forces to develop a training portfolio to address both specific and generic aspects of gaining confidence and competence in the delivery of evidence, including:

- Excellence in Written Evidence
- Courtroom Skills
- Cross Examination Training
- Law, Evidence, Procedure and Best Practice

Departments/ranks that we regularly work with include;

- Analysts
- CSI/SOCO
- Electronic Crime
- Collision Investigation
- Probationers
- Test Purchasing
- Firearms
- ICIDP
- Fingerprints
- Expert Witnesses
- Financial Crime
- Surveillance Units
- Senior Investigating Officers
- Emergency Planning



For further information please contact [Daniel Cutts](mailto:dcutts@bondsolon.com) on 020 7549 2549 or email dcutts@bondsolon.com

The **Bond Solon Expert Witness Conference 2009** will again return to The Church House Conference Centre, Westminster, London on Friday 6 November 2009.

Please call [Daniel Cutts](mailto:dcutts@bondsolon.com) on 020 7549 2549 or visit our website for further details.

Bond Solon -
the legal training consultancy

Paulton House
8 Shepherdess Walk
London
N1 7LB

Tel: 020 7549 2549
Fax: 020 7549 2505

www.bondsolon.com
info@bondsolon.com

BT55267

The payphone sex offender

The stereotypical image of a child sex offender is of an individual who masks his identity at a computer screen, making contact with vulnerable young people before luring them into deplorable acts of abuse. However, the mould was broken when a Humberside Police investigation team was tasked with netting Derek Hindmarch, who used public telephone boxes to approach, groom and incite young girls to perform sexual acts. Daniel Dexter reports.

In August 2009, Hindmarch, 46, a Humberside man, received a twelve year prison sentence following a joint investigation by Humberside Police and the Child Exploitation and Online Protection (CEOP) Centre.

As part of his pattern of offending, Hindmarch would identify public telephone kiosks in the region, wait in a nearby location watching for young girls to walk by and then attract their attention by calling the phone. Once contact had been made, he would begin grooming them in order to encourage them to create indecent images of themselves.

The joint investigation began in February 2009 following a tip off from a member of the public



which uncovered the modus operandi of an offender who was taking significant steps to evade law enforcement detection. Hindmarch was identified following specialist intelligence development by CEOP officers and arrested by officers from Grimsby CID on May 7.

Hindmarch subsequently pled guilty to 35 charges including 20 counts of causing or inciting a child to engage in sexual activity, two counts of meeting a child following sexual grooming and 13 counts of making indecent photographs of children. Twenty children under 16 were identified and safeguarded during the course of this investigation.

Senior investigating officer Detective Sergeant Stuart Watson said the investigation was initiated after a complaint from one of the potential victim's mother.

"The child was interviewed and supplied a mobile telephone number used by the offender. Checks on this number identified that it had been subject of two previous allegations; one two years previous concerning telephone calls to children requesting photographs and meetings for the purposes of sexual abuse," said DS Watson.

A detailed investigation was necessary to identify

usage by the unregistered phone used by Hindmarch. DC Watson said 'top-up' details for a prepaid mobile telephone take time to obtain and information supplied by the service provider is usually received too late for the recovery of CCTV evidence.

"Prompting single point of contacts and airtime providers to give detailed and up-to-date information was crucial to ensure other lines of enquiry could be made where the phone was topped up in order to identify the suspect," said DS Watson.

The investigation team also made contact with colleagues from CEOP at an early stage of the investigation in order to take full advantage of the centre's specialist knowledge. The partnership helped gain an overview of the potential extent of Hindmarch's offending.

DS Watson said it was crucial to build a rapport with the suspect from the point of arrest: "Both myself and another interviewing officer arrested Hindmarch. The first hour after arrest was critical and our treatment of Hindmarch ensured his commitment early on to admitting the offences."

Where and when to arrest Hindmarch was also chosen carefully to catch him off guard and with the evidence necessary to convict him, said DS Watson.

"The run up to his arrest entailed detailed investigation of him, his lifestyle and behaviour to ensure when he was arrested he would be more likely to believe denial was fruitless."

Overcoming the challenges

DS Watson said gaining the necessary evidence in a timely fashion from the telecommunication industry was the investigation team's "biggest hurdle".

"Being a small force investigating a crime which fell

outside the remit of murder or terrorism was a hindrance in needing urgent material from oversubscribed and busy units. We knew that if we had an up-to-date product we could identify Hindmarch," said DS Watson.

"The greatest challenge was ensuring the investigation continued after charge. The team was not dedicated to this enquiry alone and had two other major investigations running alongside, as well as conducting the daily duties of a CID team."

The arrest and charging of Hindmarch was only the start of the enquiry. The discovery of so many telephone numbers for victims necessitated numerous trips and interviews with victims, the majority of which required to be video taped.

DS Watson said the investigation team had a very short window of time to complete the majority of the enquires needed - the CPS gave a deadline in order that the case was trial ready.

"This window of some ten weeks placed a great strain on the team," he said. "We had to make an enormous commitment, working long hours and at times travelling at very short notice."

He added that too often, senior officers see the charging of a suspect as a conclusion to a case, not the beginning. Some 80 per cent of the work to ensure Hindmarch's conviction and reflective sentence took place after arrest.

Lessons learned?

Early request for assistance from CEOP, with its close liaison with the telecoms industry and expertise in dealing with similar offenders assisted us greatly and was crucial to a successful outcome, said DS Watson.

"Also important is the need to promote your investigation with the single point of contacts and



other agencies; you must encourage them to see your investigation as theirs also.”

He added: “Early advice from the CPS is critical. The lawyer in this investigation received the case from the start and provided evidence on it from the first day. Meetings were open and honest. The lawyer was kept up to speed weekly during the early stages of the enquiry and directed lines of enquiry necessary to reflect Hindmarch’s criminality without unnecessary expenditure of time and resources, which sometimes happens in cases such as these.



“The lawyer’s understanding of the case and the team’s other commitments ensured she didn’t waste the time that the team had to spend on the case.”

DS Watson said another key factor in securing a conviction

was ensuring the investigation team remains dedicated and focused in its approach.

“A small team, in this case four officers, were able to complete this enquiry only due to the support and assistance provided by the other agencies, namely CEOP and the telecommunications industry. The team needed to be flexible in its work ethos. Late nights and few days off were usual. The team understood from the outset the commitment required to complete this enquiry as well as balancing their other commitments.

“It is unlikely that a small force could ever commit a dedicated team to a similar case, however in the ‘perfect world’ then this is what an enquiry such as this would deserve.”

The actual court hearings ran smoothly. Prior to each the team would liaise with the CPS and ensure that a member attended court no matter how trivial the hearing may have appeared

DS Watson said counsel was appointed early by the

CPS and the presence of an experienced barrister assisted the case greatly.

“The case presented allowed little manoeuvre for Hindmarch; His counsel offered pleas in an attempt to minimise their offending but counsel held firm resulting in guilty pleas being offered on the entire 35 counts.”

Key learning points

DS Watson said he would recommend the following points to officers who may face similar investigation:

- The choice of team members is crucial. A small dedicated team is far more effective than a larger team whose individual roles appear far removed from the main enquiry. In this team each of the members completed enquires to trace Hindmarch and either interviewed him or the victims. Each knew the whole picture and contributed to it directly.
- Be honest with the team and ensure that they are honest with you. If, due to other commitments, they cannot fulfil their role in an intense enquiry such as this you need to know. The smaller the team, the more reliant they are on each other. One member’s failure to carry their share of the demands could cause major problems.
- The benefit of using such a small team however is obvious. Each member is directly involved and has intimate knowledge at all stages. They assume ownership of the enquiry and their dedication to ‘their enquiry’ is obvious from the start. The reliance on each forms a working relationship far better than that in larger enquires where some see their role as only minor without ownership.
- Control the urge to attempt to do everything at once. We concentrated on groups of victims, finishing one group completely before moving onto the next.
- Get other agencies on board. CEOP’S assistance was crucial and early advice from CPS was critical to the final outcome.



Master the past

Advance cold cases to a new level of success

With 23% of submitted rape cases remaining unsolved, cold case investigation has never been so important. FSS gives you a wealth of original case information, scientific expertise and technology. So you can bring unsolved crimes out of the cold and gain justice for offenders and victims. The power of intelligence, people, techniques and the police have already helped to secure convictions in 130 cases. Secure yours.

To master the past in your cold case investigations
talk to Gemma Lord on 0121 329 5287.
Or visit www.forensic.gov.uk for more information.



FORENSIC SCIENCE SERVICE

The Forensic Linguistics Institute

What and who is the Institute?

The Forensic Linguistics Institute (the FLI) was set up in 1995 to provide an analysis service for texts and language samples of all types, in the context of criminal and civil investigations.

The institute has written over 300 reports for courts, law enforcement agencies, and lawyers and corporate and private clients. A wide variety of text types and situations have been analysed, including witness statements, suicide notes, ransom demands, harassment texts, anonymous and threatening email transmissions, confessions, audio evidentiary tapes, mobile phone (SMS) messaging, and many other text types implicated in a broad range of investigations.

Forensic Linguistics is an increasingly popular subject of study, both at universities and other higher education institutes and as part of vocational training for in-service legal professionals and police and other law enforcement officers. Other professionals who have taken the Institute's courses include personnel managers and senior administrators as well as US federal government employees.

The Forensic Linguistics Institute has been running courses from their website at www.thetext.co.uk since 2001. In that time hundreds of students have taken our Introduction to Forensic Linguistics Course, or have downloaded the Forensic Linguistics Course Notebook.

They have recently introduced a new course on Forensic Transcription. Our Institute is accredited by ODLQC (the Open and Distance Learning Quality Council) of Great Britain and their introductory course is taught as part of the Masters in Forensic Science at Nebraska Wesleyan University.

Principal profile

John Olsson, the world's first full time forensic

linguist, has been serving as an independent expert since 1994. He has handled more than 300 major cases, making him one of the world's most experienced in this field.



John Olsson

John is frequently commissioned by law enforcement agencies, solicitors, government departments, companies and private clients. These have included large UK insurance companies, a major US publisher and several of the world's most eminent universities and colleges.

He is also on the United Kingdom National Crime Operations Faculty register (Centre for Policing Excellence, NPIA) as an expert. His work has been used in evidence at Crown Court, Magistrates' Court, County Court and Coroner's Court levels, in addition to several industrial tribunals and other internal disciplinary hearings, representing students in plagiarism hearings and university staff in misconduct allegations. He has given evidence at venues as diverse as the Central Criminal Court, (the 'Old Bailey'), a number of Coroners' courts, and the UK Asylum and Immigration Tribunal.

John's forensic analysis has been submitted for evidence before the U.S. Supreme Court and a U.S. District Court. In addition, he has been admitted as an expert in an Australian Federal Court in connection with copyright infringement and has written a number of reports in connection with copyright and trademark infringement.

Every major crime is represented in his practice including murder, suspicious death, terrorism, product contamination, witness intimidation, blackmail, fraud, sexual assault, armed robbery,

money laundering, gang violence and narcotics investigations.

His work includes analysis of all kinds of texts including ransom notes, suicide texts, threat texts and a variety of other types of document. John Olsson has analysed the authorship of many cell phone text messages and has assisted in a number of investigations involving electronic media, including email messages.

He has also analysed the discourse of codes, including gang codes, for police officers in intelligence operations. He has also undertaken many transcriptions and other phonetic analyses of police interviews, phone calls – both malicious and genuine – to the emergency services, surveillance audio tapes, etc. This work also includes voice identification and audio enhancement. In all he has written hundreds of reports for police services and law enforcement agencies, lawyers and private clients.

John Olsson has published in the Forensic Linguistics peer reviewed professional journal, is the author of a well-known university textbook, Forensic Linguistics (subtitled An Introduction to Language, Crime and the Law), now in its second edition. Olsson has also presented at conferences in several countries.

He takes an active interest in matters of scientific interest and is a member of a number of learned and other societies (including the Royal Statistical Society and the British Academy of Forensic Sciences), as well as of the professional association for forensic linguists.

His primary concern in working as a forensic linguist is to serve the justice system honestly, impartially, and professionally. All inquiries are treated in the strictest confidence.

Forensic Linguistics Full Length Courses

Certificate in Forensic Linguistics

A general introduction to forensic linguistics

including text measurement, analysis of suicide notes and statement analysis. Certificate award is by assignments. The course consists of three units. There are a number of assignments to choose from including text measurement, textual comparisons, transcription of an audio file, the study of reversion, and observation of an audio recording.

NEW Detecting authorship of mobile phone texts

With the dramatic increase in e-crime, investigators will find this new course on how to detect authorship of mobile phone texts (SMS texts).

NEW Diploma in Forensic Linguistics

Our most advanced and detailed course, the Diploma in Forensic Linguistics is equivalent to a postgraduate diploma.

This is a detailed course covering all aspects of linguistics from authorship to statement analysis, to phonetic and forensic transcription, police interview strategies and much more.

NEW Forensic Transcription Course

A full length course on transcribing audio and written language material. The course requires completion of a number of assignments and there is a written examination.

Audio and written evidence is important in any investigation or trial. Good transcribers are in demand by law enforcement agencies and governments around the world.

Forensic Linguistics Course Notebook

The Forensic Linguistics Course Notebook summarizes the entire Forensic Linguistics Certificate course, and contains information on all the same cases.

Contact:

Forensic Linguistics Institute

Bryntirion Mawr, Llanfair Caereinion,
SY21 0BL Wales U.K.

Telephone: +44 (0)1938 811192

CELLEBRITE'S UFED

ESCALATES MOBILE PHONE FORENSICS TO THE HIGHEST LEVEL



NEW!

UFED PHYSICAL PRO

- Extends the existing UFED capabilities
- Extracts physical phone memory
- Enables file system dump and reconstruction
- Recovers phone passwords
- Accesses deleted content

 **CelleBrite**
Universal Forensic Products

HARD EVIDENCE FROM MOBILE PHONES MADE SIMPLE



UFED RUGGEDIZED

UNIVERSAL FORENSIC EXTRACTION DEVICE

- Extracts phone data - Phonebook, SMS, Photos, Videos, Audio files, Call history
- Standalone kit - No computer required for data extraction
- Thorough evidence reports generated automatically
- supports over 2,000 handset models
- Portable and easy to use

INVESTIGATING

MAJOR CRIME

CONFERENCE

APPLYING BEST PRACTICE TO SERIOUS AND COMPLEX CRIME

25 & 26 November 2009

Venue: West Midlands Police Learning & Resource Centre Tally Ho!

The Investigator magazine (www.the-investigator.co.uk) has announced two one-day conferences aimed at practitioners of all ranks who are involved in the investigation of major crime. Some of the country's leading experts will gather together over the two days to deliver a mix of best practice and case studies that will provide delegates with some of the vital skills and techniques needed to investigate major crime.

- ✓ Maximising the evidential potential of a crime scene
- ✓ Standalone mobile phone forensic analysis in the field and lab
- ✓ Using Automatic Number Plate Recognition Technology (ANPR) as evidence – advice and pitfalls
- ✓ Maximising the potential of HOLMES
- ✓ Use of pollen forensics and mycology in murder inquiries
- ✓ Making effective use of analysts
- ✓ Cold case reviews – tips and techniques
- ✓ Use of geographical profiling
- ✓ Maximising evidential potential of both cell site analysis and mobile phone evidence
- ✓ Image capture in custody

The Investigator
conferences
ESSENTIAL LEARNING FOR TODAY'S INVESTIGATORS

Day 1 Sponsor

 **CelleBrite**
Universal Forensic Products

www.cellebrite.com

£175
one day


£300
two days



INVESTIGATING

MAJOR CRIME CONFERENCE

Day 1 Sponsor


Universal Forensic Products

www.cellebrite.com

Venue: West Midlands Police Learning & Resource Centre Tally Ho!

Topics covered on November 25


Universal Forensic Products

- Maximising the evidential potential of a crime scene
- How to carry out effective house-to-house inquiries
- Using Automatic Number Plate Recognition Technology (ANPR) as evidence – advice and pitfalls
- Standalone mobile phone forensic analysis, both in the field and in the lab
- Image capture in custody

Topics covered on November 26

- Maximising the potential of HOLMES
- Making effective use of analysts
- Cold case reviews – tips and techniques
- Use of geographical profiling
- Maximising the evidential potential of both cell site analysis and mobile phone evidence
- Use of pollen forensics in murder inquiries
- Using mycology to catch a killer – a case study

Attend one or both days of this conference

One day - £175

Two days - £300 (no accommodation)

Two days - £340 (including over night stay on 25 November)

(Additional accommodation is available on 24 November)

Tel: 0844 660 8707 or email: info@the-investigator.co.uk



INVESTIGATING

MAJOR CRIME CONFERENCE

25 and 26 November

Confirmed speakers

- John Dean, National Policing Improvement Agency (NPIA) lead on ANPR
- Paul Smith, Senior Tutor Institute for Criminal Justice, University of Portsmouth
- A member of the NPIA's HOLMES team – name to be confirmed
- Sue Prior, Higher Analyst, Met Police Operation Trident
- Cathy Turner, National Scientific Lead – Cold Case Reviews, Forensic Science Service
- Pat Wiltshire – Pollen forensic expert who worked on the Soham and Ipswich murder inquiries
- Prof David Hawksworth CBE - International mycologist
- Neil Trainor - Geographic profiler, NPIA
- Det Supt Stuart McKenzie from South Wales Police National lead on house-to-house inquiries training

Further speakers to be confirmed

To reserve your place simply email the name(s) of the delegates and contact address to: info@the-investigator.co.uk

You can contact the conference organisers on:

Tel: (+44) 0844 660 8707 or email: info@the-investigator.co.uk

I the
Investigator
conferences
ESSENTIAL LEARNING FOR TODAY'S INVESTIGATORS

Fighting Cybercrime



Back to the future!

A new initiative established in Newcastle upon Tyne in the North East of England is paving the way for law enforcement and academic researchers to join forces to counter cyber criminals.

Think back 20 years and assess what sorts of threats crimes and dangers faced the citizen and the business community in 1987? Essentially 20 years ago crimes were very much 'in your face' incidents. There was a predominance of offences such as robberies occurring at banks, building societies, post offices and cash in transit.

Think about today's society and how offences are now committed in a virtual world such as, cyber bullying, phishing and Identity theft. Yesterday's bank robbers have now distanced themselves from; 'in your face' crimes and now commit fraud, drugs, extortion, tax evasion and prostitution on their behalf. Yesterday's robbers are now 'property developers' with extensive and expansive property and business portfolios through which they launder their criminal monies.

In March 2003 The North East Fraud Forum was founded at an event held at St James Park,

Newcastle upon Tyne. Four hundred delegates attended the event from the public and private sectors in a unique initiative to combine forces to fight fraud and financial crime.

The initiative soon earned the support of regional, national and international government including, The Attorney General's office, The United States Treasury Department and the United Nations Trade and International Law Commission and United Nations Drugs and Organised Crime agency. The initiative has since spread across the United Kingdom to eight other British regions and continues to grow.

Three strands of work became fundamental to Fraud Forums across the U.K. Fraud, Money Laundering and Cybercrime. What soon became evident was that there was growing dependence on technology as a means of committing these financial crimes. As such pressure grew to try and stay one step ahead of the cyber criminals.

On Thursday 29th November and Friday 30th November 2007 30 leading strategic thinkers from across the United Kingdom, the region and Europe gathered at Close House, Heddon on the Wall,

Northumberland as part of a think tank. Sponsored by the Regional Development Agency One North East, Newcastle University and N.E.F.F.

The event coincided with recent problems in the region, Northern Rock, loss of private data at the Washington Child Benefit Office and the most recent incident of the North East benefactor giving covert political donations to the Labour party, academics, representatives of local and national government, representatives of the local business community and police officers carried out discussions and workshops and to try and set a new agenda for the region.

Those in attendance acknowledged the difficulties business faced with a clear conflict between a pressure to generate profit and a balance against risk. There were clear risk tolerances considered by all businesses but a general apathy of 'I'm alright Jack' mentality existed not just by business but by the public also. There was a general lack of understanding of technology by the citizen.

Greater incentives are required despite the complex, dynamic issues faced. The answer lay in working more closely together for the benefit of the consumer, business and government. Education is a key factor at all ages and levels and Britain must work together in developing a strong anti-fraud culture.

The growth in cyber crime and the exploitation by global organized crime brought both challenges and opportunities, which could be exploited by academic research with positive outputs and outcomes for the practitioner.

There was an acknowledged balance between the freedoms and

rights of the individual and law enforcement and some tools available such as cryptography could be seen as a double edged sword. Clearly these tools are extremely relevant, cost effective but there often is a danger in assessing what we can get quickly and taking a short-term approach to resolving long-term problems.

50 per cent of the world's malicious computer misuse comes from EU member states. **There is a firm commitment from EU government to raise awareness and combat cyber crime in a coordinated harmonized way. The key priorities for Europe are:**

- Network security and what will the Internet look like in 2020?
- Secure service infrastructures
- Critical infrastructure
- Protection and sustainability
- Service enabling technologies

The EU must work towards creating sustainable and resilient Meta layer infrastructures, which are understandable and secure. Two of the most important issues are security and trust building identification management and empowering end users. Obstacles to achieving this could be such things as, complexity, usability, trust, and privacy and software assurance.

The key conclusions were, are the current instruments adequate and flexible to adapt? And will our current strategy and priority choices stand the proof of time?

The project evolved and the following key objectives were set:

- Re build civic confidence and community trust gaining reassurance that the North east is a good place to do business
- There must be a multi disciplined approach with commercial spin offs and applications



- We must recognize the size and shape of current/future problems and what we can achieve in turning problems into leading and competitive advantages

Spurred on by the recent bad press about incidents of data security breaches within public sector governmental departments members of the project felt empowered and determined to take a positive and robust stance to provide some protection for the North East community not only for today but also for the future.

Combining the talent and research of the regions universities with North East business and law enforcement delegates identified clear spin offs. It was decided that any such venture must be a legal entity representing the interest of the citizen and must span the region giving guidance, advice, assistance and protection for all North East citizens.

It was noted that the event was being held within the close vicinity of Hadrian's Wall a world heritage site. It was further recognized that when first constructed it was built on the frontier of the then Roman Empire and is still seen today as a sign of strength and security for the region.

As such there was a real synergy with the aims, objectives and the conclusions of the two day event hence the "HADRIAN" project was born. A pledge made by all representatives from regional, national, European partners, law enforcement business and citizen leaders was made to work together to recognize threats and seek opportunities to rebuild public confidence and trust and build a strong and confident region for the future.

The project has evolved into an embryonic centre for Cybercrime and Computer Security. The centre

will our current strategy and priority choices stand the proof of time?

As such there was a real synergy with the aims, objectives and the conclusions of the two day event hence the "HADRIAN" project was born. A pledge made by all representatives from regional, national, European partners, law enforcement business and citizen leaders was made to work together to recognize threats and seek opportunities to rebuild public confidence and trust and build a strong and confident region for the future.

The project has evolved into an embryonic centre for Cybercrime and Computer Security. The centre has prioritized its activities in line with the regions strategic objective of making the area safer for all to visit, work and reside in. In essence the goals and objectives of the centre are closely aligned to that of community safety and already we are seeing results in the area of safer Internet training for parents and carers.

Hadrian together with Microsoft and the Northern Grid for Learning have developed an accredited training course for, children, teachers, social workers and parents to raise awareness about the dangers of unsupervised use of the Internet and how to promote greater safety.

Responding to the rise in child-targeted cybercrime such as internet grooming and cyber bullying, the university's Centre for Cybercrime and Internet Security has developed a nationwide training programme that will teach parents and carers how to help children use the internet safely. Offering advice on installing family safety settings and monitoring a child's use of the net.

Newcastle University's Phil Butler, a former DCI





with Northumbria Police and head of the North East Fraud Forum is leading the initiative and said:

“What came out of our discussions with parents is that not only are many of them frightened of the Internet and the dangers it poses to their children but they also have a real sense of helplessness.”

“They feel they are unable to protect their children because they weren’t equipped with the technical know-how.

“Our aim is to not only raise awareness of the dangers of unsupervised use but also to empower parents to be able to help their child use the internet safely so they can enjoy all the benefits it has to offer without being put at risk.”

The programme will be delivered under the isafely training organisation created specifically to deliver the training.

Topics covered in the training programme include:

- To highlight the differences in the way adults and young people use the internet
- To address key concerns such as cyber bullying and internet grooming
- To look at what parents can do to make the internet safer for their children

Professor Pete Lee, Head of the Centre for Cybercrime and Internet Security, added: “This is exactly the kind of initiative the Centre was set up to achieve – drawing on the university’s

internationally-renowned expertise in cybercrime to tackle some of the challenges facing today’s society.

“It is our intention that through this programme, parents will be supported and guided to help their children use the Internet safely.”

The team has joined forces with Microsoft and the Northern Grid for Learning to develop training that will be rolled out to all schools, colleges, learning centre’s, companies and public sector organizations across the UK.

Safer Internet Training for Parents is the first of what will be a number of training modules which can also be the start to obtaining a recognized education qualification or as part of a person’s continuous development training.

Members of the Hadrian project are very proud of what they have achieved and feel that they have jointly devised a means to tackling some of the problems of the future by using solutions designed today.

Anyone wishing to find out more about the “Hadrian” project and training should contact www.hadrianproject.com.

Phil Butler
Director of External Relations
Newcastle University
Centre for Cybercrime and Computer Security



CRIMINAL & CIVIL INVESTIGATIONS AND REVIEWS
FRAUD INVESTIGATION
INVESTIGATIVE TRAINING
IDENTITY AND DOCUMENT FRAUD

Investigative Consultancy Services Ltd

PO Box 231
Chester-le-Street
DH3 9DF
Tel: 08444 151 077
info@dstics.co.uk
www.dstics.co.uk

Searching Solutions



The need for police forces to make more effective use of intelligence has led them to implement increasingly sophisticated information management software solutions. Carol Jenkins talks to David Carrick the CEO of Memex about one current project that is running with Surrey Police.

The old adage ‘life happens while you’re busy making plans’ is something that David Carrick the Chief Executive of Memex, the Scottish-based company that delivers information management software solutions to police and other agencies throughout the world, is familiar with.

Joining Memex 20 years ago as a software engineer, a young David Carrick told himself he would work for the company for 18 months before moving onto a new challenge.

“I did intend to move on after about 18 months but over the years, the company has evolved so much that I feel I have worked for four or five different companies,” he explains.

Two decades later and he is pleased to say he is now CEO for a company that has made great strides in breaking into the UK police market.

Surrey Police is one force that announced in the summer that it would implement an enterprise-wide information management system. It will be implemented in phases over the next three years joining all of the key police business under one platform.

The system forms part of the force’s ‘Programme Enterprise’ which will bring together all of Surrey’s

policing functions, systems and sources which have, until now, been handled separately. It will ultimately link all recorded information and intelligence across the force which includes Memex’s core Intelligence, Crime, plus Case and Custody solutions.

This will give all users across the entire force a valuable tool to predict, prevent and respond to crime. It will also help to free police time, reduce reliance on paperwork, and improve the quality of information held in their systems, thus helping the force to meet the challenge of tight budgets in the years ahead.



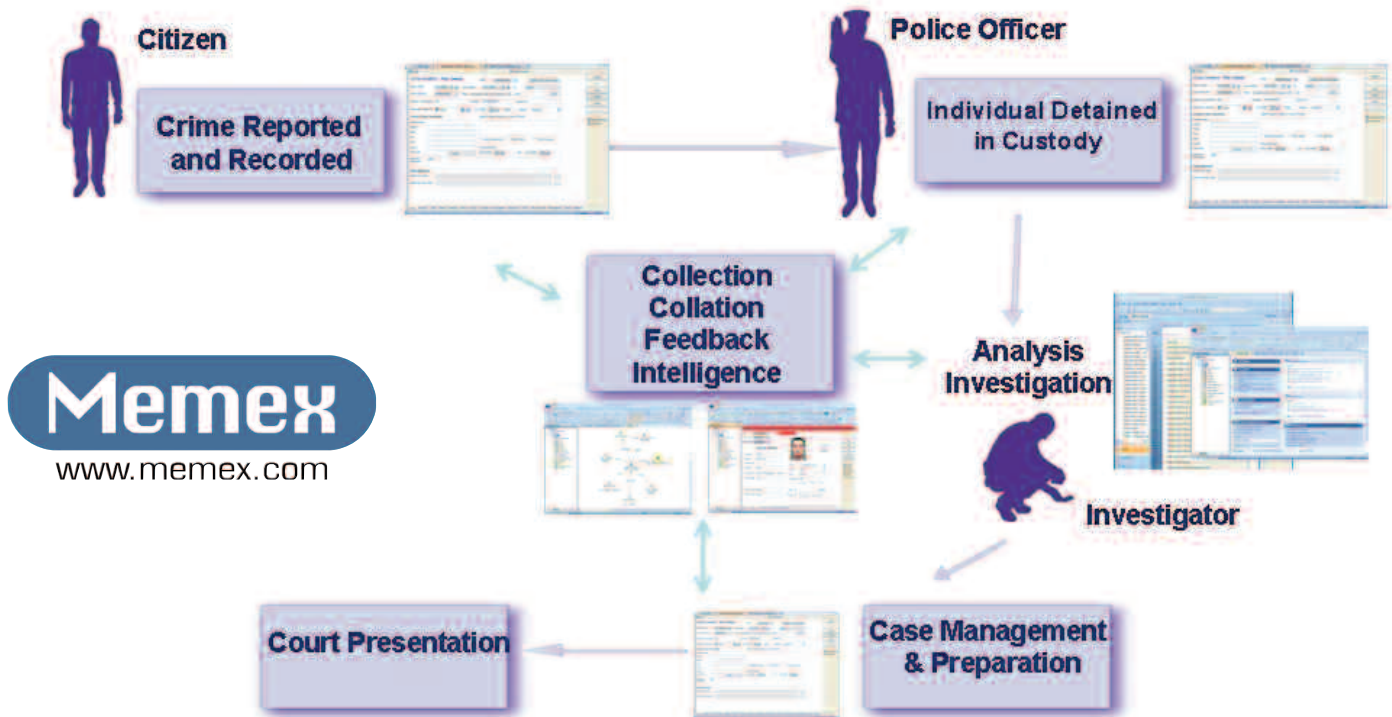
David Carrick

Speaking at the time, David described the project as one of the “biggest IT implementations in the UK law enforcement community.”

He said Memex would be working with the force to deliver its market ready Crime and Intelligence Management Solution, as well as building, in partnership, Case and Custody solutions over the next few years.

The software supports the move by not just Surrey but all of the 43 forces to become more intelligence-led. In a time when police performance

End to End Policing Scenario



is under scrutiny and budgets becoming tighter, forces are facing up to the reality that they must work not just harder but smarter, and becoming more sophisticated in their compilation and use of intelligence is central to this approach.

Surrey Police will go live with the system in 2011, which replaces its existing crime and intelligence systems, which was first introduced in 1993. The new system will be operational before the 2012 Olympics, helping the force respond effectively to the policing challenges it will bring.

For Memex, the project is important in that it highlights the continuing emphasis the company puts on working in partnership with organisations such as police forces rather than being just a technology provider.

“This approach came out of a recognition that while we are the technology experts, it’s the officers who are out there doing the job that know their business and can provide valuable input into everything we do,” said David.

“With the Surrey project, we have worked hand in hand with frontline officers to make sure that what we deliver is what is needed by them.

He explained that the Enterprise Information Management Solution would give all users across the force a valuable tool to predict, prevent and respond to crime.

It will also help free police time, reduce reliance on paperwork and improve the quality of information held in their systems.

As well as the UK, Memex has its sights firmly set on working in other areas of the world such as the US and South Africa providing solutions for organisations including governments, public safety agencies and commercial organisations in sectors such as financial services and telecommunications.

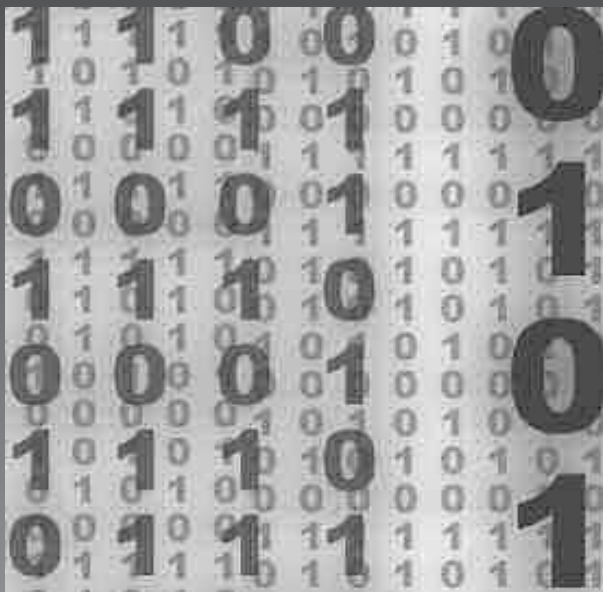
One key challenge that David believes all technology companies face is the view that technology is somehow the panacea to solving police and security problems.

“People watch shows like 24 and CSI and think organisations like the police have a ‘whodunit button’ they can press which will solve all the problems. We are not there yet but what we are doing is providing robust and sophisticated technology to help organisations predict, prevent and respond to threats in real time.”

GRIFFIN FORENSICS



*Digital Investigations &
Data Recovery*



Computer Investigations

Mobile Phone Analysis

Forensic Data Recovery

Sat Nav Analysis

CCTV Analysis

- Initial analysis completed within 5 working days
- Very competitive pricing
- 2 stage, cost effective, investigation
- Experienced prosecution & defence experts
- Non-technical statements & reports provided

Tel: 01280 704433

eMail: info@griffinforensics.com

Web: www.griffinforensics.com



Griffin Forensics
9b Market Place, Brackley,
Northamptonshire NN13 7AB



**PRACTICAL COMPUTER
AND MOBILE PHONE**

F^{orensics} CONFERENCE

APPLYING CUTTING EDGE TECHNIQUES TO CRIMINAL INVESTIGATIONS
15 December, 2009
West Midlands Police Training & Resource Centre - Tally Ho!

Computers and mobile phones often hold the key to solving many of today's criminal investigations and can be used as vital evidence in court.

This one day conference provides anyone involved in the investigation process with all the latest thinking and best practice in digital forensics. Experts from the police service, industry and academia will provide a fascinating insight into current and future trends and provide invaluable advice as to how to maximise use of the techniques available to investigators.

- ✓ How the forthcoming digital forensic standards will impact on investigations.
- ✓ The emerging threat of steganography – where criminals use hidden messages in computer files to conceal vital evidence.
- ✓ How to identify anonymous text and email messages for use as evidence in criminal investigations.
- ✓ Key evidential issues, pitfalls and practical advice on how to maximise the potential of digital evidence.
- ✓ Using computer forensics to catch a killer who murdered his wife and faked her suicide.
- ✓ Emerging future technical challenges facing investigators.
- ✓ Mobile Phone Forensics – what an investigator needs to know.

Early Bird Booking Discount
Book and pay before 30th November and
receive a 25% discount (You pay £150)

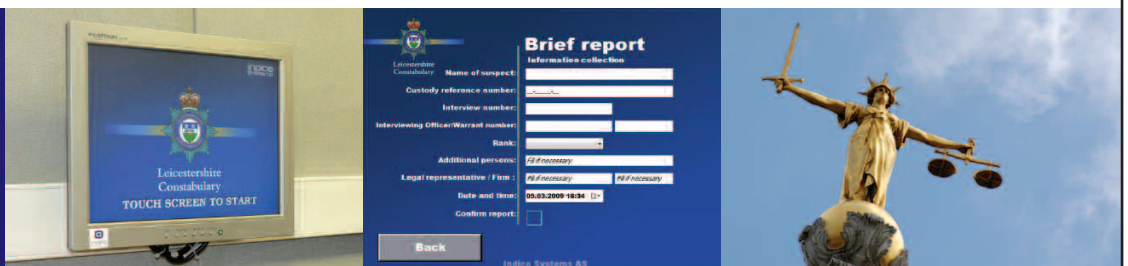
To book contact: 0844 660 8707 or info@the-investigator.co.uk

£200
per
delegate



Indico Systems is changing the way the criminal justice sector approaches the secure recording, transcribing and management of video and audio interviews and related evidence.

Don't get left behind.



Indico in the interview room

- ▣ PACE-compliant, high quality and secure interview recordings on CD or DVD
- ▣ audio-only or video/audio options available at the touch of a button
- ▣ user interface is a 15" touch panel
- ▣ CD and DVD recordings easily transcribed from a standard PC
- ▣ interview summarisers receive high quality digital output

Indico Server

the ultimate in secure data retrieval and management

Installed on a Windows server platform, Indico Server takes the secure retrieval, storage and management of video and/or audio evidence to a new level. Criminal justice personnel can access interviews within seconds for transcription, or monitor the interview across the network.

To find out how Indico Systems can easily demonstrate a suitable solution for your force contact:

Tel: 0044 (0)1483 549059

Simon Jones

Sales Director

Indico Systems UK

simon.jones@indicosys.com

www.indicosys.com

0044 (0)7850 541001



Indico Portable

Established in 2000 and with offices in Norway, Denmark, the UK and Tallinn, Indico Systems develops, installs and maintains a range of secure digital recording solutions for a wide variety of applications, most notably within the police and criminal justice sectors.

Indico Systems is committed to delivering world-leading software solutions for a variety of applications, as well as supporting an increasing network of European customers. Our solutions, services and support are delivered via a dedicated team of developers, technical account managers and sales professionals to ensure that customer expectations are always met and where possible, exceeded.

Our focus is the criminal justice sector, however Indico Systems solutions extend into any area where the investigative process requires that audio and/or video be recorded. Central to our philosophy is the provision of robust solutions that are as easy to use as they are reliable.

Behind these easy to use solutions lie sophisticated programmes capable of delivering a range of applications to our clients.

In 2009, Indico Systems UK has provided solutions to Gloucestershire, Leicestershire and Surrey Police forces, Teesside and Portsmouth University, and Triangle Services in Brighton. Elsewhere in Europe, Indico has had success in the Danish Courts, the German Police Academy and Project KARIN in Sweden, a specialist centre for vulnerable adult and child interviewing. Indico Systems continues to develop the relationship with the Norwegian criminal justice sector and has recently installed a server solution for a leading childcare agency in Oslo.

Why Indico?

Indico is a Latin word which means to proclaim, make publicly known, announce or disclose. The word is a derivation of Indigo, a blue colour pigment which in ancient times was very expensive to produce. Wearing indigo coloured clothes attracted attention, and was associated with

making something publicly known. Indico Systems has therefore chosen to use indigo blue in its logo. One of Indico System's largest clients is the police and in most countries their uniforms are blue, a tradition derived from the United Kingdom.

Established in 1866, the first modern police force was the Metropolitan Police, who used blue uniforms to distinguish them from other enforcement bodies that were using traditional military uniforms.

The expression 'the thin blue line' describes the balance the police must maintain between state enforcement requirements and the acceptance of the general public. Indico products are designed to provide openness and access, which in use will aim to improve the legal security of the public, and contribute to the confidence of society in our various law enforcement agencies.

Indico Systems delivers tailor-made software for the reliable recording of audio and video. Our recording solutions can be adapted to clients' needs without special products being required. Recordings from Indico can be played on all standard PCs, DVD or CD players. Indico supplies special versions for the police, the courts, the armed forces, the health service and the private sector. The software is available in Swedish, Danish, Icelandic, English, German and Polish. You can find out more about areas of usage and solutions under the client groups or products page at www.indicosys.com

Indico Systems' goals are to:

- Understand the needs and work processes of our clients
- Provide advice about cost-effective recording solutions
- Adapt our solutions to the specific needs of a country or region
- Deliver robust, reliable and secure solutions to the criminal justice and private sectors
- Commit to a long-term relationship with each and every client
- Deliver 100% client satisfaction



University of Sunderland

Sunderland Hosts Interviewing Conference

The University of Sunderland will be hosting a national conference in “Contemporary Issues in Investigation” at its campus on Wednesday November 25.

The aim of the conference is to promote debate around the subject of investigative interviewing and specifically around the contemporary issues facing today’s interviewer. Speakers will include NPIA national interview advisor Gary Shaw, MBE.

The conference will also showcase the work that the University has carried out in developing a suite of BA and Masters programmes to assist in the professionalization of the role of the investigator. The programmes were initially developed to focus on the role of the suspect or witness interviewer, and are being delivered to officers in the UK and also in Northern Ireland, they are also being delivered to a cohort of crime investigators in the Humberside force.

They map onto existing internal training and add high level learning and critical thinking skills to extend and develop knowledge in the wider aspects of investigative management.

Through studying research skills, personal development, legal aspects of investigation, behavioural sciences and other relevant topics, the interviewer will not only achieve a transferrable Higher Education qualification, but also develop knowledge and skills in the wider aspects of the role.

The BA Honours programme is currently offered as a direct-entry level 3 programme, therefore taking only one year to complete, for existing Tier 3 interviewers who can provide evidence of their completed portfolio.

In addition to a reflective report, they will study a module that focuses on their own professional competence and development, as well as a contemporary issues module

requiring them to research a specific issue within investigation.

The MA programme is offered to existing Tier 5 interviewers who go on to study the role of behavioural sciences, legal aspects, data collection and research methods and finally a large work-based dissertation.

Pauline Wonders, Head of Centre for Flexible Learning at the University, said: “these programmes reflect the best in employer engagement and work based learning. We have worked hard to align the learning with role of the interviewer and add value to the service through transferrable skills and knowledge.

“We are confident that some of the learning and research that these students complete will inform ACPO strategy.

“The delivery team includes experts in the field so that the learning is contextualised and relevant. We are incredibly proud of these programmes and their potential to help professionalise this highly complex role.”

The intention is to further develop the programmes to be applicable to other aspects of investigation and discussions will take place in the coming months to develop courses for Family Liaison, collision investigation and other areas.

INVESTIGATOR TRAINING-EVENTS-CONFERENCES

CALL FOR PAPERS

Evaluation and effectiveness of investigative interviewing:
A multi-disciplinary approach

iIIRG 
International Investigative
Interviewing Research Group

3rd Annual Conference of the International Investigative
Interviewing Research Group (iIIRG)

22 - 24 June 2010, Norwegian Police University College
Conference Centre in Stavem, Norway



Photos by: NPUC and Kjetil Rolseth

Abstracts of no more than 200 words should be submitted electronically to iiirg@tees.ac.uk. Abstract submission deadline: **Friday 15 January 2010**.

The Organising Committee encourages submission of individual and symposium abstracts in the following general areas:

- Investigative interviewing of suspects, witnesses, or victims
- Expert advice to interviewers
- Interview training and policy
- Interview decision making processes
- False confessions
- Detecting deception
- Forensic linguistics

Confirmed keynotes are:

Professor Laurence Alison, Director of the Centre for Critical Incident Research, University of Liverpool

Professor Ray Bull, Professor of Forensic Psychology, University of Leicester

Chief Constable Mick Creedon, Derbyshire Police, UK

Professor Pär Anders Granhag, Professor of Psychology, Göteborg University, Sweden and Visiting Professor, Scottish Institute for Policing Research

Professor Günter Köhnken, Professor of Psychology, Christian-Albrechts-Universität, Kiel, Germany

Professor Martine Powell, Personal Chair (School of Psychology), Deakin University, Australia

Gary Shaw MBE, National Interview Advisor, National Improvement Agency, UK

For submission and conference details visit: www.tees.ac.uk/iiirg.

Sponsored by



COUNTER TERROR

EXPO 2010

14-15 April 2010 | National Hall, Olympia

Countering the Global Threat



PRE-REGISTRATION
ENTRANCE ONLY,
ATTENDEES WILL NOT
BE PERMITTED
TO REGISTER ON-SITE

- ⊗ Dedicated exhibition for companies of specialist security and counter terrorism technologies and solutions
- ⊗ High level conference featuring multiple streams
- ⊗ Comprehensive programme of free-to-attend technology and practical workshops
- ⊗ Networking Functions

For more information on exhibiting, visiting or attending the conference please contact: Nicola Greenaway
Tel: + 44 (0) 208 542 9090 or
email: ngreenaway@niche-events.com

Headline Sponsor

THALES

Register now at www.counterterrorexpo.com



Where else would you study such professionally orientated programmes?

The School of Social Sciences at City University London is a vibrant place of teaching, learning and research. With an exceptional reputation for graduate employability a postgraduate degree from City University provides an excellent step up to your future career. We combine first class teaching with an exciting programme of postgraduate courses and offer a number of specialist degree programmes. We are now accepting entry on the following programmes:

MA Surveillance Studies

This distinctive Interdisciplinary degree is designed to present cutting edge knowledge of recent developments in surveillance. Taught by leading academics in the field, it provides in-depth analysis and discussion of the key issues characterising the expansion of Surveillance in 21st century society. The programme includes modules on Security and Crime Control, Victimology, Surveillance Theory and Concepts, Human Rights, Globalising Cities and Transnational Policing.

MA Criminology

This postgraduate degree will appeal to those wishing to undertake advanced study in contemporary developments in criminology and criminal justice. The course emphasises the importance of locating key developments in crime and crime control within an interdisciplinary and global context. Students can investigate the latest thinking concerning 21st century crime and evaluate the latest criminological research and policy proposals.

Start the discussion...

For further information, or to receive an application pack, please contact Postgraduate Admissions on **+44 (0)20 7040 8512** or email socscipg@city.ac.uk and quote ref **IV0709** alternatively for open day information, please visit the website www.city.ac.uk/social



www.the-investigator.co.uk



**The Investigator
Media Information**
essential reading for today's investigators

Advertise in The Investigator

Tel: +44 (0)844 660 8707 or email: sales@the-investigator.co.uk

To get your event listed email: info@the-investigator.co.uk

5 November 1604 Gunpowder Plot



Guy Fawkes and the plotters

It's more than 400 years since the Gunpowder Plot was discovered. But did you know that Guy Fawkes wasn't working alone, and that he wasn't the only plotter with links to York?

Everybody knows that Guy Fawkes was behind the Gunpowder Plot. He's the one who was going to blow up the Houses of Parliament, it was his idea and he masterminded the whole thing.... didn't he?

Well, no he didn't.

York's most infamous son, Guy Fawkes, was certainly a key player in the plot and, probably because he was caught red handed preparing to detonate the gunpowder, his has become the name we all remember. But it almost certainly wasn't his idea.

The Plotters

The mastermind behind the plot was Warwickshire born Robert Catesby. The son of a persecuted Roman Catholic, Catesby was a charismatic man described as handsome and well liked.

He married a wealthy protestant and seemed content to attend Church of England services while practising his Roman Catholic faith in private. But after the death of his wife, in 1598, he turned back to his Catholic roots with devotion.

Catesby knew most of his co-conspirators through a network of friendships with various Roman Catholic families. The exception was Guy Fawkes.

Gunpowder Plot Facts

It's believed the plot began at a pub called the Duck and Drake in London in 1604



The plan was to overthrow Protestant rule by killing the King and installing his daughter as a figurehead to Roman Catholic leadership of England

After the plot was revealed many Catholics feared a legislative backlash which, surprisingly, never came.

The Fawkes connection

Fawkes was almost definitely brought up as a protestant. The son of an ecclesiastical lawyer, Guy was born in York and baptised in St Michael le Belfrey Church, next to York Minster (the baptism record exists in the parish register).

However his father died while Guy was quite young and his mother married a Catholic. At some point the young Guy Fawkes converted to Catholicism.



It's fairly well known that Guy Fawkes attended St Peter's school in York, but less well known is that fellow plotters John and Christopher Wright were there at the same time and it's likely that Guy was already mixing in Catholic circles.

In 1591 when Guy was 21 he left England to serve in Spain's Army of Flanders, fighting against Dutch Protestant rebels

in The Netherlands. He served with distinction achieving a rank equivalent to 2nd lieutenant.

It's during this time that Fawkes is believed to have developed an expertise in explosives and the handling and storage of gunpowder. The Plot

The plan was to destroy parliament, killing the King and a good number of his protestant officials. The hope was that this would plunge the country into chaos. At the same

time an uprising in the Midlands would seize Princess Elizabeth to become a figurehead for Roman Catholic rule of England.

Perhaps what's most startling about the Gunpowder Plot is just how close it came to being realized. The government was seen as quite paranoid about potential Catholic plots but the intelligence network seemingly failed to spot anything of concern.

It was an anonymous letter, sent at the last moment to a parliamentary official who was known to have been a Catholic, that prompted a search of the Parliament buildings.

Apparently even this wasn't taken too seriously, but during the search Guy Fawkes was found, along with lots of gunpowder.

The plot had been foiled. Fawkes was arrested and there's little doubt he was tortured to extract information. He apparently held up well, not giving up his co-conspirators for about two days.

But in the meantime the governments intelligence network kicked into action, and it wasn't long before the rest of the plotters were rounded up.



Specialist Books on Analysis and Policing

Get 15% off purchases of books on analysis and policing through *The Investigator* plus free postage.

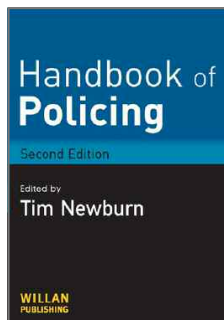
Handbook of Policing (2e)

Edited by **Tim Newburn** (LSE, University of London)

This new edition of the *Handbook of Policing* updates and expands the highly successful first edition, and now includes a completely new chapter on policing and forensics. It provides a comprehensive but highly readable overview of policing in the UK, and is an essential reference point combining the expertise of leading academic experts on policing and policing practitioners themselves.

'A major contribution to the study of policing in the UK ... authoritative, interesting and extremely wide ranging.' - **Sir Ian Blair** (Commissioner, Metropolitan Police)

August 2008 912pp
9781843923237 (Pbk) £34.99 / 9781843925002 (Hbk) £87.50



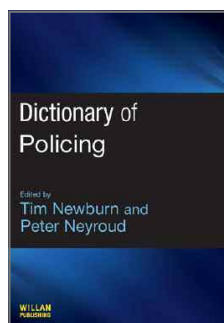
Dictionary of Policing

Edited by **Tim Newburn** (LSE, University of London) and **Peter Neyroud** (Chief Executive, NPIA)

'This is the first time that the body of knowledge about Policing has been brought together in a single volume dictionary accessible to practitioner and member of public alike. It is a really welcome development.' - **Paul Stephenson QPM** (Deputy Commissioner, Metropolitan Police Service)

This dictionary contains approximately 300 entries (of between 500 and 1500 words) on key terms and concepts arranged alphabetically. It is edited by the UK's leading academic expert on policing and the Chief Executive of the National Policing Improvement Agency

April 2008 384pp
9781843922872 (Pbk) £24.99 / 9781843922889 (Hbk) £62.00



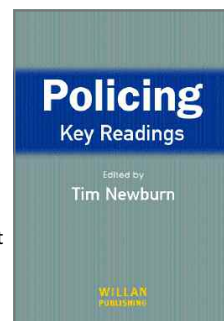
Policing: Key Readings

Edited by **Tim Newburn** (LSE, University of London)

This book aims to bring together the key readings which constitute this core of policing studies, setting them within the necessary theoretical, social and political context, and providing an explanatory commentary. It will provide both students and practitioners with key literature and writing on policing.

'A collection of classic and contentious contributions to the literature on policing that will be an indispensable companion to any course on police and policing' - **Professor P. A. J. Waddington** (University of Wolverhampton)

November 2004 848pp
9781843920915 (Pbk) £33.99 / 9781843920922 (Hbk) £87.50

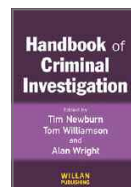


Handbook of Criminal Investigation

Edited by **Tim Newburn** (LSE), **Tom Williamson** (formerly Univ. of Portsmouth) and **Alan Wright** (Keele Univ.)

Handbook of Criminal Investigation is the most comprehensive and authoritative book yet published on the subject of criminal investigation, provides a rigorous and critical approach to not only the process of criminal investigation but also the context in which this takes place, the theory underlying it.

May 2007 728pp
9781843921875 (Pbk) £34.99 / 9781843921882 (Hbk) £85.00



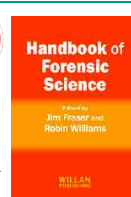
Handbook of Forensic Science

Edited by **Jim Fraser** (Strathclyde University) **Robin Williams** (University of Durham)

This Handbook aims to provide an authoritative map of the landscape of forensic science within the criminal justice system of the UK. It sets out the essential features of the subject, covering the disciplinary, technological, organizational and legislative resources that are brought together to make up contemporary forensic science practice.

July 2009 728pp
9781843923114 (Pbk) £34.99 / 97818439213121 (Hbk) £87.50

NEW Title



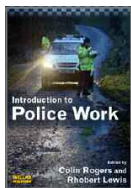
Introduction to Police Work

Edited by **Colin Rogers** (University of Glamorgan) and **Rhobert Lewis** (University of Glamorgan)

This book provides student police officers with a highly readable and up to date introduction to the work of the police, exploring what this currently involved and the directions it may be going in.

'Written by practitioners for practitioners, this book is a comprehensive introduction to the work of policing and will provide a useful insight for anyone, seeking to understand our profession.' - **Peter Neyroud QPM** (Chief Executive, NPIA)

July 2007 312pp 9781843922834 (Pbk) £19.99



Criminal Investigation

Peter Steffox (Head of Investigative Practice, National Policing Improvement Agency [NPIA])

This book provides an authoritative and highly readable introduction to criminal investigation, from somebody ideally placed to write about it, focusing on how police practitioners carry out investigations.

It will be essential reading for both student police officers as well as officers taking higher levels of CPD within the police service.

March 2009 256pp
9781843923374 (Pbk) £18.50 / 9781843923381 (Hbk)

NEW Title



Police Corruption

Exploring police deviance and crime
Maurice Punch (LSE)

Policing and corruption are inseparable. This book argues that corruption is not one thing but covers many deviant and criminal practices in policing.

It provides a fresh, accessible overview of this under-researched topic for students, academics, police and criminal justice officials and members of oversight agencies.

June 2009 256pp
9781843924104 (Pbk) £21.99 / 9781843924111 (Hbk) £55.00

NEW Title



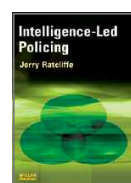
Intelligence-Led Policing

Jerry Ratcliffe (Temple University, Philadelphia)

'Dr Ratcliffe has that rare ability to combine theory and practice using language that practitioners will find both useful and applicable in an operational environment. This is a book for everyone with a stake in understanding crime and the value of intelligence-led approaches as an effective response.'

- **R. Mark Evans** (Director, Analytical Services, Police Service of Northern Ireland)

February 2008 280pp
9781843923398 (Pbk) £22.99 / 9781843923404 (Hbk) £58.00

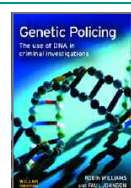


Genetic Policing

The use of DNA in criminal investigations
Robin Williams (University of Durham) and **Paul Johnson** (University of Surrey)

This book is about the increasing significance of DNA profiling for crime investigation in modern society. It focuses on developments in the UK as the world-leader in the development and application of forensic DNA technology and in the construction of DNA databases as an essential element in the successful use of DNA for forensic purposes.

February 2008 240pp
9781843922049 (Pbk) £22.99 / 9781843922056 (Hbk) £55.00



Order via our website www.willanpublishing.co.uk using discount code INV09, or call 44(0)1884 849085 quoting *The Investigator* to receive your discount.

All orders are made through Willan Publishing, Culmcott House, Mill Street, Uffculme, Devon EX15 3AT.