

# LET'S TALK

THE MAGAZINE OF FORENSIC COMPUTING

Issue 4

Spring 2008

## PRESERVING EVIDENCE

Your essential guide

A DAY IN THE LIFE  
...of a managing director

NEWS AND VIEWS  
Analysis of latest cyber-crime

## COMMENT

Forensics expert  
**ANDREW SHELDON**  
gives his personal  
opinion on the latest  
developments in the  
world of cyber-crime



## Step AWAY from that computer...until you've read this vital guide to dealing with a digital 'incident' at your organisation

IMAGINE the scene...

Someone's been up to no good on their office computer and has been sent home.

The gossip around the water cooler is deafening. You've been summoned by the boss to investigate.

Naturally, you boot up the computer straight away and go hunting for incriminating 'evidence'.

Now consider a different scenario...

There's a corpse at the desk and lots of blood. What do you do? Prod the body with your shoe, then have a quick shuffty in all the drawers looking for a 'murder' weapon?

Of course not. You call the police and cordon off the area until the SOCOs arrive.

What's the difference between these two situations? None. They are both potential crime scenes, and the last thing any innocent bystander would want to be accused of is tampering with the evidence.

So let's start from the beginning with the computer 'incident'. You arrive at the desk. You observe. You think before you act.

Get a notepad and a pen and write down what you see. What's on the screen? What printers, scanners or other peripheral devices are connected to the computer? Are there any other digital devices on the desk?

Pick up a camera (NOT the one on the desk!) and start taking pictures; the screen, the devices, the cables connecting the devices, the CD racks.

And take notes. Copious amounts. Including times and the date.

OK, OK, it all sounds a bit amateur Columbo, but there's a serious point here.

If a conviction is to be secured in a court of law there has to be a 'continuity of evidence'.

This means the facts are so well documented even the smartest of barristers can't find a 'hole' in them.

As a hugely-experienced former policeman-turned forensic computing analyst, Dick Peake is better placed than most to know the critical importance of preserving and documenting that 'chain of custody'.

"We can have the most compelling evidence possible to obtain a conviction, but if we can't prove that the offending material was bagged, tagged and preserved in accordance with criminal justice procedures, we leave ourselves open to fierce cross-examination from some of the keenest minds in the legal business," says Dick.

"We can have the bad guy bang to rights, but if we make one mistake along the way our evidence can be ruled inadmissible."

So what are Dick's top tips?

"Once you have photographed and taken notes about the offending PC, you need to preserve the contents of the hard disk. Whatever you do, don't do a shutdown. That will spark off a chain of events

FOR years I have been banging on about the dangers of revealing too much personal information about yourself on the internet.

And now, it seems, a government watchdog agrees.

The obvious risk is identity fraud, caused by giving out dates of birth and home addresses.

But you can also damage your reputation by revealing personal character traits which a future employer – or romantic partner – might find objectionable.

Comments and pictures posted on the web after a raucous night on the town might seem hilarious at the time, but what will people think in the sober light of day?

The golden rule is simple: Don't post anything on the net that you wouldn't be happy for someone to find lying in the street.

WHAT a howler...

When Her Majesty's Revenue and Customs 'lost' two CDs containing incredibly confidential personal information about 25 million people, they knew what a furore it would cause.

But it beggars belief why they would even think of delivering information in this manner in the first place.

The obvious way to send the data was electronically via an uncrackable Virtual Private Network (VPN).

At least then there would have been an audit trail, in the extraordinary event the information was accessed or copied.

THE end of the internet is nigh according to the latest research.

The network will grind to a halt in 2010 unless billions are spent on increasing bandwidth, according to Nemertes Research.

An exponential increase in the number of people downloading memory-hungry videos and films will clog the web's arteries, they warn.

But don't be too alarmed.

I'm not a gambling man, but I've a gut instinct the cavalry of technological invention will ride to the rescue of our beloved internet.

# Could you PRESERVE the evidence?

which could irrevocably change vital evidence. Computers like to be orderly and clean up after themselves, updating files and changing access dates and times. You could pull the plug—and remove the battery in a laptop—which would leave you with an electronic 'snapshot in time' that can be recreated at a later date, but — depending on circumstances — this might NOT be the best move. If in any doubt, contact a forensics expert for advice before taking any action."

Everything should then be placed in evidence bags which can be sealed and tagged.

Now is the time to contact forensic computing

experts, such as the one Dick works for — Evidence Talks. They will 'image' the computer's hard drive and then analyse it — after deploying a 'bit-blocker', which write-protects the device and makes sure no information gets altered from the moment it is seized.

Once analysis is complete the evidence is locked away in a secure exhibit store, and finally, after any legal proceedings are over, it should be archived or destroyed, depending on the prevailing retention policy.

Despite these vital evidence-handling procedures, most cases, whether criminal, tribunal or civil, are resolved before they come to court.

## Rules of our most senior policemen...



THE Association of Chief Police Officers (ACPO) sets out four clear principles for the handling of digital evidence if it is to be deemed admissible in court:

- No action taken by law enforcement agencies, or their agents, should change data held on a computer or storage media which may subsequently be relied upon in court
- In circumstances where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to give evidence explaining the relevance and implications of their actions
- An audit trail or other record of processes applied to computer-based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result
- The person in charge of the investigation (the case officer) has overall responsibility for ensuring that the law and these principles are adhered to

## Web users put careers at risk

THREE-QUARTERS of young people who use social networking websites fear information they post about themselves could damage their future careers.

A survey by watchdog the Information Commissioner's Office (ICO) revealed that 71 per cent of 14 to 21-year-olds who use sites such as Facebook, MySpace and Bebo would not want a college or employer to run a web search on them.

But despite their fears, more than half of young users still openly publish information about things such as drinking habits and the type of people they associate with.

The ICO urged people to be more aware of their 'electronic footprint' and keep personal identifying information private.

## ID card plan hit by data blunder

THE lost data blunder which nearly cost chancellor Alistair Darling his job could prove the final nail in the coffin for the government's controversial ID card scheme.

Campaigners say the disappearance of two CDs containing the bank account details of 25 million parents and their children prove the government is not fit to handle the population's personal information.

It could also have implications for advanced plans to put everyone's health records on line, where they could be accessed at any time by up to 300,000 interested parties.

A spokesman for the anti-ID card group NO2ID said: "Sadly, it takes a catastrophe like this to sharpen people's focus on the issue."

## Net 'gridlocked' in three years

THE internet will grind to a halt by 2010 unless drastic action is taken.

That's the verdict of analyst firm Nemertes Research, which thinks the web will be unable to cope with the amount of data being carried.

It claims the next Google or YouTube could fail to get off the ground as users resort to dial-up to get a connection.

Nemertes claims £66 billion needs to be spent on upgrades.

"We like the bad guys to roll over with their legs in the air," says Dick. "Our evidence should be so compelling that they are ill-advised to challenge it.

"But the vital part of that evidence is the chain of custody. We have to be able to show where the evidence was at every stage of the investigation, and who had access to it. And, as in any police investigation, we take contemporaneous notes of everything we see and do.

"Not only does this protect the evidence, but it also protects us as a business. Reputation is everything in our line of work, and if we were to mess that up we would be shot to bits."

## Mobiles are the new fingerprints in war on crime

MOBILE phones have become the new 'fingerprints' in the battle against crime in the 21st century.

The ubiquitous handsets, which now outnumber people in the UK, are increasingly being used to obtain convictions in cases such as murder, fraud and conspiracy.

But it's not just call logs and incriminating texts that can get the phone's owner into trouble.

As long as it is switched on, a mobile is broadcasting its almost exact location to the network operator. And that information can be stored – and easily retrieved – for many years.

In fact, the conviction of Soham killer Ian Huntley was partially based on crucial mobile phone evidence.

Andrew Sheldon, who has years of experience of forensic digital analysis, says: "The on-board memory of a mobile phone works pretty much like any other. Data, such as incoming and outgoing telephone numbers and text messages, are not overwritten when they are deleted. The phone merely tags that space as available for use.

"Using specialist equipment it is often possible to retrieve information many years after it was deleted.

"Text messages that have been received but have never been saved can also be retrieved."

Password protection and PIN numbers may slow down the analysis of phone data, but some technologies exist that can help bypass them.

Adds Andrew: "While evidence retrieved from mobile phones is rarely enough to secure a conviction on its own, it forms a vital part of the jigsaw, particularly in conspiracy cases where it can prove links with associates.

"And the company mobile phone should never be overlooked when businesses are investigating allegations such as intellectual property theft against current and former employees."

For more information on mobile phone forensics, contact Andrew on 0845 125 4400.

## A DAY IN THE LIFE...

Managing Director

### What's your name?

Andrew David Sheldon.

### Your age?

0x110011 (work it out).

### Job title?

Managing director and principal consultant.

### Describe a typical day at Evidence Talks?

Interesting, challenging, fun and exciting. We're always doing new stuff.

### What are you working on at the moment?

Relaxing by trying to be more efficient, achieving my goals for the business and extending my knowledge.

### Why is that so important?

If you keep doing what you've always done, you'll keep going where you've always been!

### What's the best thing about your job?

We play with some cool stuff and we help to solve problems that have a genuine impact on people.

### And the worst?

Keeping up with progress. There is so much happening and so much to learn that it can be frustrating just trying to keep up.

### What's the most unusual project you have worked on at ET?

Working out how a major peer-to-peer application was disabled by a competitor.

### What's the strangest thing you have achieved in your career?

Managing to break some very strong encryption by getting frustrated and swearing at the screen.

### Before Evidence Talks?

I ran a company that developed desktop audit technology for asset management.

### Any other careers?

Industrial radiographer in the oil business back in the days before health and safety!

### Ambition?

To write a book about the things I've seen during my career in forensics.

### How do you relax?

Relax, what's that?

### Favourite meal?

Fried egg on toast with tomato sauce. Unbeatable.

### Favourite drink?

Gin and Harpic – drives you clean round the bend!

### Best night out?

At my age they all merge together, but recently I took my wife Elizabeth to see George Michael.

### Favourite sport?

Anything with an engine.

### Favourite sporting moment?

Watching the New England Patriots American football team win their 16th consecutive game in a hotel in New England over Christmas. Fantastic atmosphere but I still don't understand the game.