

Understanding Computer Evidence



**EVIDENCE
MATTERS**

www.evidence-matters.com

Presented by Paul Vella

Tel: 0845 644 3652

© Evidence Matters Ltd

Contents

Our Services	3
Evidence Matters Promise	4
Contents of CD	5
Computer-based Evidence	6
ACPO Good Practice Guide	7
Examinations.....	8
Data Recovery	8
Document Authentication	8
The Internet	9
Websites	10
Email.....	11
File sharing	12
Trojans & Hackers	13
Indecent Images of Children	14
Mobile Telephones	19
Cell Site Analysis.....	20
SatNav Forensics	20

Evidence Matters Ltd.
DX 16940
TOWCESTER

Tel. 0845 644 3652
Fax. 0845 644 3653
Email office@evidence-matters.com

Our Services

- ▶ Computer forensics
- ▶ Mobile phone forensics
- ▶ Cell site analysis
- ▶ Insolvency & liquidation services
- ▶ Intellectual property investigation
- ▶ Remote activity/keystroke monitoring
- ▶ In-car SatNav forensics



- ▶ Data preservation & recovery
- ▶ Internet tracking
- ▶ Website capture
- ▶ Chatroom logging
- ▶ IT investigation

Evidence Matters Promise

- ▶ YOUR questions answered in **PLAIN English**
- ▶ Easy to understand, professional report
- ▶ Jargon free
- ▶ Impartial evidence from a recognised Expert
- ▶ **24 Hour Nationwide Service**
- ▶ No charge for travel for computer examinations within England & Wales
- ▶ Deadlines & Budget met
- ▶ Confidentiality & Discretion

What you **don't** get....

- ▶ Industry jargon
- ▶ Techno-babble
- ▶ Incomprehensible reports

Call **0845 644 3652** for an
informal discussion of your needs

Contents of CD

With this pack, you will have a CD which contains a number of documents in 'pdf' format. If you do not have a 'pdf' reader such as Adobe Acrobat Reader, you will need to download and install one. We recommend the free reader from www.foxitsoftware.com. The application is called 'Foxit Reader for Windows'.

The CD contains the following documents, many of which have been referred to in today's session, and will be mentioned in this booklet.

- ACPO Good Practice Guide
- CENTREX – Investigating Indecent Images of Children on the Internet
- Data Protection Act Letter Template
- Data Protection Act Data Controller Addresses
- Memorandum of Understanding between CPS and Police
- Mobile Telephone Providers Addresses
- Sentencing Guidelines – Sexual Offences Act 2003
- SAP Advice – Child Pornography
- R v BOWDEN
- R v OLIVER
- R v PORTER
- R v SMITH
- ATKINS v DPP

Computer-based Evidence

Forensic Computing

“Forensic Computing is the collection, preservation, analysis and presentation of computer-based evidence using methodology whereby any evidence discovered is acceptable in a court of law”.

Where is it?

Electronic evidence can be found in a growing number of devices and media including

- ▶ Computer hard drives (internal)
- ▶ External hard drives
- ▶ Laptop computers
- ▶ Mobile telephones
- ▶ Personal digital assistants (PDAs)
- ▶ GPS devices
- ▶ Blackberrys
- ▶ SatNav systems
- ▶ Home entertainment such as Sky+, Tivo, X-Box, Playstation, Wii
- ▶ Ipods and other MP3 players
- ▶ Compact discs/DVDs
- ▶ Floppy/ZIP disks
- ▶ Digital cameras & digital video cameras
- ▶ Digital photo frames
- ▶ Data cards
- ▶ USB thumb drives
- ▶ Dictaphones

This is not an exhaustive list.

ACPO Good Practice Guide

- ▶ Data is no different to information in a paper document
- ▶ The prosecution must show that the evidence produced is no more and no less now than when it was first taken into police hands
- ▶ All steps taken by during prosecution examination must be repeatable

ACPO Principles

Principle 1

No action taken by Law Enforcement agencies or their agents should change data held on a computer or storage media, which may be relied upon in court.

Principle 2

In exceptional 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 the implications of their actions.

Principle 3

An audit trail or other record of all 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.

Principle 4

The person in charge of the investigation (the case officer) has overall responsibility for ensuring that the law and these principles are adhered to.

Examinations

All forensic examinations of computers and related equipment should be conducted in a manner which can be reproduced, at a later date, from the information contained in the Examiner's statement and contemporaneous notes.

Due to financial limitations, examinations conducted on behalf of the prosecution, or the plaintiff, often tend to look only at 'what' is there. The question of 'how' or 'why' it is there is left for the Examiner working on behalf of the defence.

Forensic evaluation will put the evidence into context and can reveal elements of the case that had previously been unconsidered – which in turn can create significant defence/prosecution case opportunities.

Data Recovery

Physical faults excepted, it is nearly always possible to recover *some* information from a hard drive. There are tools available to the general user which can totally erase data, however their effectiveness is limited depending on how often/recently they have been run by the user.

Specialist forensic tools can also recover deleted data which is not accessible to the average person.

Document Authentication

It is often possible to establish whether or not a document has been created or accessed on a particular computer, and often more importantly, the creation and access dates.

We have seen a number of cases now where the user has attempted to alter the computer's internal clock to 'forge' the creation date of a document. This will usually leave a trail which can be identified by any good examiner.

The Internet

The 'Web' is not the Internet, but just one function of the Internet. The Internet has been in existence in one form or another for several decades, whereas the 'World Wide Web' was developed in the late 1980s and early 1990s, and was made available to the general public in the mid 1990s.

We access the World Wide Web by connecting our computer to an Internet Service Provider, usually via a telephone cable, and the Internet Service Provider then allows us access to the various protocols and functions of the Internet, such as:

- ▶ Email
- ▶ File Transfer Protocol (FTP)
- ▶ Usenet (Newsgroups)
- ▶ Telnet
- ▶ World Wide Web

Due to the nature of the Internet, it is not controlled or governed by any one organisation or country, and as such, is extremely difficult to police, since someone sitting in their home in the United Kingdom can easily access information on a website based in Indonesia.

Websites

- ▶ Identity of websites can sometimes be established

Websites have to be 'hosted' somewhere, usually on a commercial web server somewhere in the world, but as a result, it is often possible to establish who the owner is, or at least where it is. Having said that, with modern technology, it is now possible to host a website on portable devices, and it is likely that in future, this will become a common trend amongst those wishing to evade the law.

- ▶ Website address embedded in photo or....
- ▶ Through Web Browser history

When it comes to indecent images of children on websites (or found downloaded to a computer), it is sometimes possible to identify which website the images came from.

- ▶ CENTREX guidelines

If the ownership or management of a website can be established, then the CENTREX document on the CD provides a basis for how the Police should approach and investigate the matter. This includes attempting to identify and protect the victims of abuse – something that the Police very rarely do in our experience.

Email

Email is one of the oldest functions of the Internet, and technically, has changed little in nearly forty years. These days we access our email using one of two basic methods. Email (client) applications, or Web Based services.

Web-Based Mail is a system that allows the user to access their email account from the World Wide Web. The user can send and receive email messages from almost any computer that is connected to the Internet. When this type of email (Hotmail, Gmail etc.) is encountered, The email account and password may be required to access the data for forensic examination purposes, although email received from such an account can still be traced back to the internet service provider. Fragments of these emails can often still be recovered from the computer because they have been displayed within a web page.

Email Applications such as Outlook are less flexible in that the emails are retrieved from the mail server by the application and downloaded to the local computer. In these cases, the email is usually easily retrievable during forensic examination.

Emails contain hidden information known as 'headers', which can allow us to trace the origin of an email.

File sharing

File sharing is a method of connecting two or more computers together via the Internet, and allowing them to share files. Where file sharing avoids the use of a central server to store data, they are referred to as 'Peer to Peer' or P2P networks.

Peer to Peer file sharing is often used to distribute genuine legal content on systems such as Sky Anytime and the BBC iPlayer, but is also used with systems such as Kazaa, Limewire, eDonkey, eMule etc. to search for and download pirated movies, music, computer software and child pornography.

Where an application such as eMule, Kazaa, Limewire etc is used, it is not unusual to recover comprehensive logs of what has been downloaded and when. In some cases it is possible to identify what the user's search parameters were, and whether files have been accidentally download as part of a 'bulk' download.

Trojans & Hackers

Trojans and Malicious Code is a huge subject, one that cannot be covered here in any great detail, but in short, a Trojan is a device to deliver a payload of malicious software. This malicious software is often referred to as a 'Trojan' in itself.

The implications of this is that a Trojan can be programmed to do any number of things from delivering adverts to stealing credit card numbers and allowing hackers the ability to control your computer remotely.

One of the most common traits of a Trojan is to hijack the web browser and force it to visit websites that the user doesn't want to go to. They can present 'pop-ups', although this is becoming less common, and they can add websites to the favourites or bookmarks of a web browser.

The concept of Trojans is often raised in cases involving indecent images of children.

The 'Trojan defence' was applied successfully in the matter of R v Aaron Caffrey, who was charged with breaking into computer systems owned by the American port authority in Houston. It has been known for criminals to purposefully infect their computers with viruses and malicious code, laying the foundations for just such a defence should the need ever arise.

Indecent Images of Children

Relevant Legislation

Protection of Children Act 1978 Section 1 creates the offences of 'taking, making, possessing, distributing or possessing with a view to distributing' indecent images of children.

This was amended to include 'pseudo-photographs' by the Criminal Justice and Public Order Act 1994.

The Protection of Children Act 1978 was further amended by the Sexual Offences Act 2003 which creates defences for the creation/possession of such images as part of a criminal investigation (defence examination). The Act also increases the age of a 'child' from 16 to 18.

Influential Cases

The Protection of Children Act of 1978 defines what is considered 'Indecent' and illegal by the British courts.

There are a number of significant cases which have defined the way child pornography cases are dealt with by the courts and they include:-

Atkins v Director Of Public Prosecutions

The Court Held: knowledge is an essential element in the offence of possession under section 160 Criminal Justice Act 1988 so that an accused cannot be convicted where, as here, he cannot be shown to be aware of the existence of a cache of photographs in the first place.

R v Bowden (1999)

The Court of Appeal held that downloading data representing indecent photographs of children from the Internet amounts to an offence within the meaning of section 1(1)(a) of the Protection of Children Act 1978.

R v Oliver (2002)

This case saw the adoption of the COPINE scale into English law in 2002. To distinguish between child pornographic content, authorities rank material on a sliding scale of severity from one to five. This system is based upon the COPINE Typology and ranges from semi-nude/nude photographs (level one) through to penetrative sexual assault (level four) and sadism or bestiality (level five).

R v Ross Warwick Porter (2006) considered offences that related to the making of indecent photographs of a child under section 1(1)(a) Protection of Children Act 1978 and of possessing indecent photographs of children contrary to section 160(1) Criminal Justice Act 1988. However, the images in question had been deleted by the Defendant before his arrest and were retrieved by the authorities only with the support of specialist forensic technologies. The question of possession was raised. The Court Held:

"It will, therefore, be a matter for the jury to decide whether images on a hard disk drive are within the control of the defendant, and to do so having regard to all the circumstances of the case. Such is the speed at which computer technology is developing that what a jury may consider not to be within a defendant's control today may be considered by a jury to be within a defendant's control in the near future. Further, in the course of time more and more people will become skilled in the use of computers. This too will be a relevant factor for the jury to take into account".

Are they really children?

In R v LAND (1997) , the Court of Appeal held that a jury is as well placed as an expert (e.g. a paediatrician) to assess any argument addressed to the question whether the prosecution had established that the person depicted in a photograph was a child.....

U.S.C. Title 18, Section §2257 Disclaimers

Often we find that images, classified as ‘indecent images of children’ by the prosecution’s Expert, have in fact come from websites that display ‘Title 18’ disclaimers.

In the highly publicised case of the Liverpool choirmaster, Keith Knowles, our contact with the webmasters from some of these sites, and the subsequent production of model I.D.s and passports, led to the successful appeal against conviction.

Below is a typical Title 18 Disclaimer providing contact details for the ‘Custodian of Records’.

COMPLIANCE
18 U.S.C. 2257
In compliance with the United States Federal Labelling and Record-Keeping Law (also known as 18 U.S.C. 2257), all models located within this domain and associated domains were 18 years of age or older during the time of photography. All model’s proof of age is held by the custodian of records, which is listed below, organized by model name and producer. All content and images are in full compliance with the requirements of 18 U.S.C. 2257 and associated regulations.

Custodian of Records: The General Manager
Name: Amsterdam Entertainment
E-mail address: support@adam-media.com

Adamsboys is an Amsterdam Entertainment website. Amsterdam Entertainment is a venture of Cobra Photo B.V., Amsterdam, The Netherlands.

- Custodian of Records: **The General Manager**
- Name: **Cobra Photo B.V.**
- Address: **Wenckebachweg 49d**
- City: **Amsterdam, The Netherlands**
- Zip: **1096AK**
- Telephone number: **+31 20 468 2335**

It is fair to say that many pornographic websites are hosted outside the USA, and do not therefore have to confirm to this legislation, in which case there are only two reasons for why they might appear to comply with USA Title 18 Section 2257:

- A) The website is geared toward USA customers, and the webmasters have therefore complied voluntarily with the legislation and all models are 18 years old or over, or
- B) The website is deliberately misleading their potential customers into thinking that the models are 18 years or over, and do not comply with the USA legislation.

Pop-Ups

There are a number of ways images can be stored without a deliberate action on the part of the user – the most common being the result of ‘pop-up’ adverts, and even entire web pages that can pop-up uninvited. Computers running Microsoft’s Internet Explorer have always been susceptible to annoying ‘pop-up’ adverts.

The problem arises as the user does not know what the content of the windows underneath these pop-ups is. More worryingly though is the fact that the images on all these windows has already been stored by the computer in the Temporary Internet Files, even though they may never have seen them.

Most ‘pop-ups’ are quite harmless, although users browsing seedier subjects *may* attract pop-ups which contain indecent images of children. Eventually, when the cache is emptied, these images will almost certainly find their way into the ‘Unallocated Clusters’ of their hard drive and subsequently, whilst not normally accessible to the user, they will be recoverable during any forensic examination.

It is fair to say that in recent years, Microsoft and Mozilla have improved their web browsers, and so instances of unsolicited pop-ups are becoming far less frequent.

Sentencing Advisory Panel / COPINE Scale

The case of R v Oliver in the Court of Appeal (2002/04477/Z3, 2002/04164/X2 & 2002/02052/X1) established a scale by which indecent images of children could be 'graded'.

This scale was defined as follows:

Level	Description
1	Images depicting erotic posing with no sexual activity
2	Sexual activity between children, or solo masturbation by a child
3	Non-penetrative sexual activity between adults and children
4	Penetrative sexual activity between children and adult
5	Sadism or bestiality

The scale was based on COPINE topology and are often incorrectly referred to as 'COPINE Scale'. The COPINE Scale had ten levels. The SAP document makes a comparison between the new SAP scale and the COPINE scale, and states that the COPINE scale was not designed for use by the court.

Of particular interest, is that the SAP document states that the comparison does not include "COPINE category 1 (Indicative (non-erotic / non sexualised pictures)) because images of this nature would not be classed as indecent"

The SAP document goes on to state that COPINE categories 2 & 3 might be the subject of a dispute as to whether or not they were indecent (2 = Nudist (naked or semi-naked in legitimate settings/sources) (3 = Erotica (surreptitious photographs showing underwear/nakedness)).

In The August 2002 document, the Sentencing Advisory Panel defined the levels as follows:

Level	Description
1	Images depicting nudity or erotic posing with no sexual activity
2	Sexual activity between children, or solo masturbation by a child
3	Non-penetrative sexual activity between adult(s) and child(ren)
4	Penetrative sexual activity between child(ren) and adult(s)
5	Sadism or bestiality

More recently, it was decided that 'penetrative sexual activity between children' should be treated as a level 4 image and not level 2.

Mobile Telephones

Examinations

Mobile telephones can store electronic data in three separate places

- ▶ On the handset
- ▶ On the SIM card
- ▶ On the media card (where utilised)

The information held *may* include call logs (incoming/outgoing/missed and duration), text and multimedia messages (sent, received and deleted, including their content), photograph and video files created or received, email and web browsing history. The information recoverable will depend on the make and model of phone, with some of the SMART phones having the potential for up to 8Gb of data!

This evidence can stand alone or be used in conjunction with call data obtained from the telephone service providers.

Mobile Phone Service Providers

Many providers will retain call data in excess of 12 months. Often only the most recent call data is easily retrieved by the Service Providers and archived data can run into months to retrieve, something which should be borne in mind when scheduling PCMHs.

If the phone in question is owned by the client, and is a contract phone, then such data should be readily released under a Data Protection Act 'Subject Access Request' to the Service Provider for the payment of the nominal fee.

Where the phone is a 'Pay as you go' and ownership cannot be proved then a court order will be required to obtain the release of the call data.

The call data will usually include all incoming, outgoing and missed calls, their duration, and which calls have gone to voicemail as opposed to being answered by the handset user. It will also include time and date information for text and multimedia messages but will NOT include the content detail of the message.

It should also be noted that whilst Service Providers will guarantee to capture 100% all incoming calls received from their network they will not guarantee to capture all incoming calls from other networks – this may lead to a discrepancy with your client's proof/statement, and it may be necessary to obtain call data from the 'other' phone's service provider to obtain the full picture.

Cell Site Analysis

Often, the physical reality of cell coverage differs to the theoretical area suggested by the cell operator.

Utilising specialist cell capture and mapping tools we can retrospectively ascertain where an individual mobile telephone has been, or more importantly, *hasn't* been using cell ID data from the Service Providers.

We conduct a 'drive survey', where we navigate the public roads in a given area with specialist equipment in the vehicle linked to a GPS (Global Positioning System) receiver. Together, they can plot hundreds of points on a map of where the coverage from an individual cell reaches.

Once this data has been overlaid on a map of the area involved, it is easy to see which areas the mobile phone in question has been, and what his or her likely movements were over a period of time.

SatNav Forensics

Typically, satellite navigation devices such as TomTom and Garmin store data on media cards or internal hard drives, which can be interrogated. The data that can be retrieved depends on the make and model, but typically, we can retrieve information about the recent destinations, mobile phones connected to the device, favourite locations etc.