Evidence in Internet Paedophilia Cases

Peter Sommer[1]
Information Systems Integrity Group, London School of Economics & Political Science

This is version is an August 2005 updating revision of paper first produced for a NCS/ACPO Conference in July 2002

Without evidence, and in the absence of a confession, prosecutions do not often succeed. Where offences of child abuse are said to have taken place in and around the Internet, much of the evidence will be computer-derived. Typically it will have been obtained from personal computers and data media such as CD-ROMS, floppies and zip discs, from the accused's Internet Service Provider and telephone company, and from the results of surveillance activities by investigators.

Computer-derived evidence has to have all the attributes of conventional evidence – it must be admissible, authentic, accurate and complete. But it also has certain qualities which create difficulties for those who wish to rely on it – it is very volatile, easily unintentionally altered without obvious trace, and it is highly novel, creating problems not only of explanation but also of forensic testing.

Potentially we face a dangerous combination: a set of offences around the sexual abuse of children which cause widespread repugnance and where there is great demand for determined law enforcement action; and uncertainty about the forensic quality of evidence that may be being adduced. Such combinations have been behind some of the great miscarriage of justice cases of the last twenty-five years.

In this article I hope to provide a guide for non computer-specialists of the techniques used to acquire and sustain evidence in these cases and the issues that can arise.

[1] p.m.sommer@lse.ac.uk; peter@pmsommer.com

Characteristics of Computer-derived evidence

When we say that evidence must be *admissible* we mean that it must conform to certain rules before it can be considered by the court for its probative value. The best known of these rules is "hearsay"[2] but for the purposes of this article one of the more important can be described as "fairness in acquisition"; if evidence is obtained in breach of law or a Code of Practice, the defence can ask the judge to use his discretion to exclude it – s 78, Police and Criminal Evidence Act, 1984 (PACE) . Until April 2000 when it was repealed[3] there was also a specific admissibility test which applied to computer evidence – under s 69 PACE, 1984, but its interpretation had become baroque and it was no longer performing its original purpose of protecting a jury from unreliable material.

When we say that evidence should be *authentic* we are looking for something that links it to persons and events - some-one must either "produce" an exhibit – say where it came from, take responsibility for it and be prepared to be cross-examined, or it must be found in circumstances which firmly associate it with an accused – for example by being seized from some-one's home or office, or the linkage must somehow be unambiguously inferred. For example a telephone company may produce records of calls made for a particular telephone line which is installed in a suspect's home.

The *accuracy* of evidence can refer to several things: it could be the accuracy of recollection a witness who is being examined in the box. In relation to computer to evidence it can include the reliability of how a computer or a program or database on it works – no longer an issue of admissibility[4] but still a critical test of the weight of probative value; it can also refer to any procedures used to examine a computer and produce exhibits from it – we'll return to this topic shortly.

An exhibit needs to provide a *complete* account of itself in its own terms; just as a witness to events shouldn't select just those items that favour a particular conclusion, extracts of log files or selections of what was found on a computer may not be enough – the court should be able to see the entire context.

A specific practical problem of handling digital evidence is that it is highly volatile; not only can a document, record or log be changed simply by typing a few keystrokes, often this can be done without leaving a manifest trace. Little skill in "forgery" is required. The basic actions of turning a computer on,

[2] The concept is becoming increasingly complex; see Law Commission Report Law Com No 245; 1997
[3] s 60. Youth Justice and Criminal Evidence Act, 1999
[4] the old s 69 PACE test of "proper working"

viewing but not overtly altering a single file or two, and then closing the computer down, will cause many files on the hard-disk actually to be written to. The apparently simple acts of collecting evidence from a computer, or of carrying out some form of passive surveillance of computer-based activities on the Internet may cause considerable levels of contamination.

Another problem is the novelty of computer evidence, not the fact that it exists, but that it includes a great deal more than such obvious items as documents and pictures. There will be configuration files which might tell us how programs on the computer were set up and used and other normally ignored files from which it will be claimed that the actions of the computer's user can be reconstructed. Even in a simple case involving the Internet, those having to decide on the merits of the case will be called on to understand the operation of the various constituent institutions of the Internet - the world wide web, email, newsgroups, chat, etc – not only at the level of the ordinary user, but at the level of the technician, understanding how each element actually *works*. Very often an investigation may need to attempt to recover data which has been deleted – is the court simply to accept this as "magic"? What happens when the more extreme forms of data recovery are deployed, and where the techniques used are not simple and automated?

Computer forensics is now a reasonably well-established subject-area, but unlike most forms of forensic science many of its individual techniques have not been around long enough to have been properly tested by peer-reviewed publication. Compare, for example, DNA evidence which started off with a 1984 paper suggesting that DNA may be a reliable unique indicator like fingerprinting; DNA testing today is the result of gradual refinements and improvements since then[5]. Fingerprinting too has been around for 120 years and has been widely accepted for a century[6]. But the explicit techniques of computer forensics must constantly undergo rapid and profound revision each time popularly used computer technology changes. Today's most widely used operating systems only date from 1995 at the earliest and many of the very popular programs for utilising the various Internet institutions are even younger. There may be significant variations between successive *versions* of operating systems and programs[7]. Even such apparently trivial matters as the

[5] Steventon, B., *The Ability to Challenge DNA Evidence*, (Royal Commission on Criminal Justice Research Study No 9, HMS0, 1993); Alldridge, P., "Recognising Novel Scientific Techniques: DNA as a test case" [1992] Crim. L.R. 687 at pp 689-691

[6] *Fingerprints*, Colin Beavan, Fourth Estate, London, 2002

[7] Windows 95 as an operating system for home users was replaced in turn by Windows 98, Windows 98 Second Edition, Windows Millennium Edition and Windows XP Home – all within the period 1995 to 2001. MIRC is a very popular "client" program for Internet Relay Chat, the public domain version of chat. It has been widely used by convicted Internet paedophiles as well as many more wholly innocent fans of this form of communication. The program was first issued in February 1995; by February 2002 it was in its sixth extensive revision. File-sharing programs are now in their third generation.

great increase in the capacity of hard-disks installed in personal computers can have a surprisingly complex impact on the procedures computer forensic technicians may have to use.

The result is that "computer forensics" is in a perpetual state of instability. Insist on higher standards of testing of methodology and you run the risk that important investigative techniques are denied the police and courts until such testing is completed. We may not be able to afford that as some Internet paedophiles are also computer hobbyists, eager to use and exploit the latest technology[8]. Allow the current under-tested techniques before a court and you face other risks: that a judge and jury cannot easily assess the reliability of the evidence - or arbitrate between the conflicting views of opposing experts.

Against these rather gloomy problems are some more positive factors. Computers also create evidence: many more personal and commercial activities are now recorded. These can include archives of emails sent and received, indications of websites etc visited and pictures viewed. In the hands of a skilled technician/investigator , the hard-disk of a computer may be able to produce a very detailed time-line of the activities of its owner. More-over the computer is also a powerful investigative aid, able to search rapidly and tirelessly through vast quantities of data for specific items of information, sorts of file, and patterns of behaviour.

The Range of Offences

In order more specifically to understand the problems of investigation and prosecution we must first look at the range of offences available to prosecutors, what sorts of evidence will be needed in each instance and then the forms of investigation available to the police

The main UK legislation is the Protection of Children Act, 1978 (PCA). S 1(1) describes a series of offences in relation to indecent photographs: (a) "taking" and "making", (b) "distributing" or "showing", (c) "possession with a view to distribution", (d) "publishing an advertisement". Children have to appear be under the age of 18[9] and "indecent" implies some sexual element. There is a defence to s 1(1)(b) of "legitimate reason". For a while there was no similar defence to a s 1(1)(a) defence, but s 46 Sexual Offences Act 2003 provides one: a defendant must show "it was necessary for him to make the photograph or pseudo-photograph for the purposes of the prevention, detection

[8] Based on my own experience as an instructed expert.
[9] Until May 2004, when s 45 Sexual Offences Act 2003 came into force, the determining age was 16.

or investigation of crime, or for the purposes of criminal proceedings".[10] . A Memorandum of Understanding between the Crown Prosecution Service and the Association of Chief Police Officers dated 6 October 2004 provides some detailed guidance.[11] As a result of s 84(4), Criminal Justice and Public Order Act, 1994, the photographs do not have to be of actual children but may have been "morphed", that is, made up from several different elements using graphics software – these are referred to as "pseudo-photographs". S 160, Criminal Justice Act , 1988 (CJA) provides an additional offence, that of simple "possession". There is no need to demonstrate, as in the PCA offence, that there was any intent to distribute. The offence is "strict liability", that is, the offence is committed simply by the fact of possession – there are some very limited defences which the accused has to prove "on the balance of probabilities"; these include "legitimate reason" and that the offending material was received without request and expectation.

There is a modest amount of case law - *R v Fellows and Arnold* (1996) [12] establishes that files held in electronic form on disk are "pictures". Three 1999 Appeal Court cases, *Bowden,*[13] *Atkins, Goodland* considered together[14] help define "making" for the purposes of s 1(1)(a) PCA and set a very low threshold: even the simple making of a copy of a picture, or saving a picture to disk is "making". They also say that "possession" in the s 160 CJA offence must involve the knowledge of possession so that if a photograph is found on a disk in circumstances where the disk owner is unlikely to realise that it is there[15], the disk owner is not guilty. In *R v Graham Westgarth Smith; Mike Jayson (2002)*[16] , it was said that voluntarily browsing through indecent images of children from the internet, so that they appeared on a computer screen, for whatever period of time, of itself amounts to making indecent pseudo-photographs of a child. The recipient of an e-mail attachment containing an indecent image of a child would not commit an offence under s.1(1) by opening that attachment if he was unaware that it contained or was likely to contain an indecent image.[17] "Showing" for the purposes of s 1(1)(b) PCA must be to a third party and not just to the person accused – *ET*[18].

[10] This defence tends to be interpreted quite strictly – the actions of self-appointed researchers or of police officers operating beyond the scope of their immediate instructions would probably not be protected.
[11] See http://www.cps.gov.uk/publications/docs/mousexoffences.pdf
[12] (1997) 1 Cr App R 244
[13] (2000) 2 Cr App R (S) 26
[14] [2000] 1WLR 1427
[15] For example in the cache of a web browser and where the accused did not know of the existence of the browser
[16] Court of Appeal, 7/3/2002 – Times Law Report 23 April 2002; [2002] EWCA Crim 683
[17] One consequence of *Westgarth Smith, Jayson* is that, as far as the Internet is concerned, it now seems there are very few circumstances in which some-one can be guilty of simple possession as opposed to "making"
[18] (1999) 163 JP 349

It is also possible to use the law of conspiracy – s 1 Criminal Law Act, 1977, where a group of individuals are involved. Here the test is the formation of a common purpose. Conspiracy was the charge faced by those convicted in the most extensively publicised of the trials emerging from Operation Cathedral / the W0nderland Club[19].

Another possibility is the notion of incitement to commit an offence. If you subscribe to a website knowing that you would thereby receive indecent material, you are inciting the owner of that website to distribute material to you.[20] The advantage to prosecutors is that, for the offence to be made out there is no need for offending material to be found on computers or data storage media associated with the accused – what is required is evidence of the subscription and that at the time of taking out the subscription the accused knew what he would be receiving.

A further weapon available to prosecutors, though a more indirect one, is s 43, Telecommunications Act, 1984 which concerns the sending of offensive and indecent materials over a telecommunications service.

Evidence and Offences

We can set out in tabular form each of these offences as they apply on the Internet and the types of evidence required in typical instances[21]:

"possession" – s 160 CJA	file(s) of indecent pictures on data media which can be uniquely associated with the accused and of which he must have had knowledge of their existence. *Usually a case can be built solely from what is found on an accused's hard-disk*
"making" – s 1(1)(a) PCA	file(s) of indecent pictures on data media which can be uniquely associated with the accused plus some indication that he copied or modified. Copying can include voluntary viewing. *Again, a case can be built solely from what is found on an accused's hard-disk*

[19] The charges covered events between November 1996 and September 1998; although some UK club members were dealt with separately, a group of men were charged with conspiracy and brought to trial early in 2001; all eventually pleaded guilty.
[20] *O'Shea*[2004] EWHC 905 (Admin). This was a "case stated" arising out of Operation Ore.
[21] This is not an exhaustive taxonomy

"distributing", "showing" – s 1(1)(b) PCA	file(s) of indecent pictures on data media which can be uniquely associated with the accused plus some indication that a showing to some-one else or a distribution took place. *While it may be possible to build a case from what is found on an accused's hard-disk, other types of evidence may be needed to demonstrate actual distribution and showing*
"possession with a view to distribution" – s 1(1)(c) PCA	the same as for simple "possession" plus proof of intent to distribute. *Usually a case can be built from what is found on an accused's hard-disk but inferring intent may be difficult. But some applications such as peer-to-peer file sharing are specifically designed to facilitate distribution so that an inference could be drawn if such an application is found fully installed*
"publishing an advertisement" – s 1(1)(d) PCA	self evidently, something approximating to an advertisement visible in a relatively public place is required. *Although collateral evidence may be available on an accused's computer, the primary evidence will tend to be on a world wide web or FTP site, as newsgroup posting, as public activity in a chat room, or an offering via a P2P service.*[22]
conspiracy – s 1 CLA, 1977	here the test is that a group of people formed a common purpose to do something illegal. *In effect evidence will be required from the hard-disks of the alleged co-conspirators and prosecutors, in the absence of confessions, email or chat, will need to show that a commonality of approach and precise technical infrastructure existed*

[22] See below for explanations

incitement to distribute	the test case of *O'Shea* relates to the taking out of a subscription to material which the accused must have known was indecent. *There is no need to find any indecent material on computers and/or data media associated with the accused. But there must be reliable evidence of the taking out of a subscription which may be found on the computers that were offering the material , or some subscription fulfilment service. Further evidence may come from banking records. Separate strands of evidence are also required to demonstrate what was being subscribed to – and these need to be contemporaneous with the date of the subscription. Finally, it is also necessary to demonstrate that an accused knew at the time of subscription that indecent material would be made available to him*

Evidence of Propensity

The 2003 Criminal Justice Act made important changes to the way in which evidence of bad character or general disposition is admitted. The Act abolished the earlier common law rules and replaced them with a regime which gives the judge discretion to admit certain such evidence in particular circumstances[23] .

Among the criteria are that the evidence must be "important explanatory evidence", "the question whether the defendant has a propensity to commit offences of the kind with which he is charged, except where his having such a propensity makes it no more likely that he is guilty of the offence", and "the question whether the defendant has a propensity to be untruthful, except where it is not suggested that the defendant's case is untruthful in any respect".

It is beyond the scope of this paper to provide a full account of these "bad character" provisions, but clearly investigators will also wish to search for material which could be put forward as evidence of proclivity.

These might include:

[23] http://www.opsi.gov.uk/acts/acts2003/30044--l.htm#98

- emails sent from or to a suspect but which do not of themselves directly contain offending material
- photographs which while not themselves strong enough to be offending for the purposes of the Protection of Children Act may nevertheless be regarded as inappropriate or indicative
- evidence of visiting particular web sites, message boards and other internet locations which might show patterns of interest and behaviour

Internet Institutions

In considering substantive direct evidence in practice we need to identify which of the many Internet institutions / protocols are most attractive to would-be offenders, as the evidence that might exist will depend on how the protocols actually work, what might be found on a suspect's hard-disk, and what might be visible or locatable by investigators.

The simplest form of acquisition and distribution is via *email attachment*; almost everyone who uses the Internet uses email and all email client programs (such as Outlook, Outlook Express, Eudora, Firebird) make it very easy to "attach" a file. But email is essentially a one-to-one medium, between people who already know each other.

The *world wide web* is for most normal purposes a very attractive way of distributing information (and it is possible to set up a website so that it is password-protected and can generate revenue by selling services by subscription), every UK ISP would immediately close down any paedophile site as soon as they discovered they were hosting it; and there would be a ready means of identifying who had set up the website. The same applies to many other countries; paedophile websites tend to be domiciled in countries with weak legal systems and where UK enforcement authorities are unlikely to get co-operation. However UK-based paedophiles are very likely to visit these sites in order to build up their own collections. For those who pay a website owner for access to paedophile images, there is the substantial risk that they will be traced via the credit card or other banking details.[24]

Similar considerations apply to those who would publish via a UK-based *FTP* (File Transfer Protocol) server. FTP is the Internet's oldest means of making files available for distribution. As with websites, an FTP server can be set up to admit only those who have paid for access. It is possible to put up a semi-

[24] As in, for example, US Operation Avalanche and UK Operation Ore (1999-2005).

covert FTP server on any computer with a permanent connection to the Internet. However, once discovered, tracing the server's owner is usually trivial.

More attractive to the paedophile are the *newsgroups* (also known as Usenet)[25]. This is a global service, also ancient in terms of its history on the Internet, which consists of several tens of thousands of themed "groups" in which any of a very large number of topics of interest are discussed in an "offline" conference. Participants do not interact in real time but "post" messages of interest to the group and to which others may comment. Participants pop into the service every now and then to see how the discussions are progressing. A system of news-servers and a particular Internet protocol take care of world-wide distribution. It is possible to "attach" a picture file to a posting. A small number of newsgroups are devoted to paedophilia. There is little to stop a "poster" from attempting to disguise who he is. The newsgroups provide an apparent degree of anonymity to paedophiles – and also a place where other paedophiles can be met. This may be important for several reasons: as trust develops, individuals may reveal their email addresses to each other so that the sharing of pictures can be carried out more privately; the newsgroups may also provide a sense of community and normalcy, said by some analysts to be an important component of paedophile behaviour.[26]

Whereas the newsgroups provide off-line discussion, *Internet Relay Chat* (IRC) [27], as the name implies, allows for real-time chat. The chat takes place on a series on themed channels which are very easily set up; the technical infrastructure depends on a series of server computers linked by a special protocol. On "chat" participants have a significant degree of anonymity[28] – they use nicknames and often adopt online personalities different from their real ones. Again for paedophiles an additional attraction of their specialist channels is the sense of community. Exchange of files is normally achieved by "going DCC", that is leaving the IRC server system and setting up a Direct Computer to Computer link - IRC client software usually allows users to do this by means of a simple mouse click. As a further refinement for those who wish to swap larger numbers of files, there is an add-on to one of the most popular IRC "clients", MIRC[29] called Panzer. This automates

[25] Based on RFC1036 – see http://www.ietf.org/

[26] For example, Rachel O'Connor, http://www.uclan.ac.uk/facs/science/psychol/gcrf/crime1.htm

[27] This is the public domain version of chat-rooms, based on RFCs 1459, 2810-2813 ; there are also proprietary forms of chat organised by large ISPs/portals such as AOL and Yahoo. IRC is un-supervised. Chat rooms have also attracted attention as they provide an environment in which paedophiles can masquerade as children and "groom" their victims. See *Chat Wise, Street Wise*, available at http://www.internetcrimeforum.org.uk/chatwise_streetwise.html

[28] But not complete anonymity – it is often possible though not straight-forward to trace participants to their real identities

[29] http://www.mirc.com

the process of trading files so that the user does not have to be present all the time. This is sometimes known as a "Fserver" – short for File Server. [30] Panzer does several things: most file traders want to make sure that they receive new material in exchange for offering their existing files – Panzer and similar facilities allow the trader to "set a ratio" – force each person who wants to take files to give a proportion (measured in file sizes) back. It also sends a regular automated message to the channel or chat room, saying that it is present and what is on offer

A modified form of IRC was used by the W0nderland Club and its variants in 1996-1998; the modifications meant that the W0nderland and other special channels were not available and readily visible to non-club members[31].

Peer-to-Peer – P2P – is another means of sharing large numbers of files. Although one of the main drivers for the development of the technology was the sharing of music (MP3) files, as in Napster, paedophiles have also found the technology convenient. There are a variety of different P2P systems. Newer ones have evolved to avoid legal actions from copyright holders which have resulted in first-generation services being closed down. At the core of first-generation services like Napster is a computer (or in a subsequent versions, a series of computer nodes) to which would-be participants connect. The central computer extracts from each participant a list of the files they have available for sharing from which it generates a master database which all participants can then search. Once a participant has located from this master database a file they wish to acquire, the service then puts them into direct contact with the computer that holds it.[32] The central computer never holds the files itself. As with IRC, participants use pseudonyms and thus acquire a degree of anonymity, though there are techniques to reveal actual identities.

In later versions, such a Gnutella and Kazaa, there is no central node. Even more recent versions such as BitTorrent enable fragments of a file to be collected from a variety of different source computers and then re-assembled. Kazaa-like file sharing programs tend to leave significant forensic traces of what was downloaded and shared ; indeed

[30] Details appear at http:// arnts.tripod.com. Similar facilities can be created using other combinations of software

[31] The author was instructed as expert by defence lawyers

[32] A more general explanation of the technology and its supposed advantages can be found at: http://www.openp2p.com/pub/a/p2p/2000/11/24/shirky1-whatisp2p.html. See also the Gnutella project: http://www.gnutella.co.uk/ and also http://www.infoanarchy.org/ and http://www.slyway.com/, http://en.wikipedia.org/wiki/Peer-to-peer Other popular P2P services include Morpheus, http://www.musiccity.com/ and Kazaa, http://www.kazaa.com/

it is sometimes possible to identify files that were formerly on a computer even if no traces of the substantive files remain.

Also worth mentioning as a means for paedophiles to meet and exchange files is Instant Messaging, of which AOL Instant Messenger (AIM)[33] is an example.

Each of these institutions that may be used by paedophiles create different problems of investigation by law enforcers, and produce different types of evidence. In particular each requires a user to have specific "client" software in order to participate – a "browser" for the World Wide Web such as Internet Explorer, a news-reader for Usenet such as Forte Free Agent, Eudora for regular email, an IRC client such as MIRC, and so on. Each P2P family of services also require client programs which enable the participant to collect and offer up files. But for each of these are many alternative programs[34] which may turn up in an individual case and which will have their own unique characteristics in capturing activity and hence have potential evidential value. Similar considerations apply to the "server"[35] facilities that ISPs have in order to service the needs of their customers.

Police investigatory armoury

It will be seen that there are two main divisions in the sorts of technical evidence that are available to investigators: computer hard-disks and data media associated with the accused, and material somehow garnered from the Internet and communications service providers[36]. In addition, if the computers of a distributing service (which could be based on the world wide web, FTP, IRC or P2P) are seized and preserved, these may contain evidence against a wide variety of suspects.

[33] http://www.aol.co.uk/aim/about.html

[34] For example, Netscape Communicator combines web browsing, email and the newsgroups, Microsoft Outlook and Outlook Express are very popular email clients, Newsgrabber and Ozum are Usenet readers. Visual IRC is one of many rivals to MIRC.

[35] For example, TACACS+ or RADIUS (Remote Authentication Dial in User Service) used to control access to IP routers or network access servers, logs from NNTP (Network News Transfer Protocol), HTTP (HyperText Transfer Protocol)

[36] Other forms of Internet surveillance, not involving ISPs are also possible, but may be expensive or difficult to deploy.

As far as computers hard-disks and media are concerned, they are usually seized under regular PACE powers[37]. The circumstances leading to the application for a warrant may be a tip-off[38] or the result of intelligence activities.

Potential police techniques for scrutiny of Internet activity can be divided as follows:

- passive scrutiny, where the police do no more than act as observers but try to collect evidence of what they see
- active scrutiny, where the police interact, to one degree or another, with suspected Internet paedophiles and while doing so try to collect evidence of what happens
- active interference with the property of the accused by using key stroke monitors or programs[39] which allow remote access of suspected computers, to see what is on the computer and/or to obtain passwords[40]
- interception of communications associated with a suspect
- information about their customers[41] obtained under powers from Internet Service Providers and telecommunication companies

Each of these methods present problems if the evidence is not to be ruled inadmissible or made the subject of a defence abuse of process application. Not the least of the difficulties is that some of the more important powers are very new and derived from the Regulation of Investigatory Powers Act, 2000. [42] This in turn, like all similar

[37] ss 18-20 PACE, 1984 plus associated Code of Practice. But cases can be lost if the correct procedures are not followed, as in the 2001 case of Andrew Aspinall in Scotland where Lothian and Borders Police failed to include their civilian forensic technician in a warrant. . See http://news.bbc.co.uk/hi/english/uk/newsid_1660000/1660618.stm and http://news.bbc.co.uk/hi/english/uk/scotland/newsid_1658000/1658447.stm

[38] As in the 1998 Gary Glitter case where the initial tip-off came from some-one asked to repair a hard-disk and another case from the same year, *Atkins*, an academic reported to the police by his colleagues

[39] For example, Back Orifice, SubSeven, Hak'a'Tak and their many variants. These are sometimes referred to as remote administrations tool and emerge from the "hacker" community. An example of a commercially available tool, apparently aimed at parents concerned about the online activities of their children, is Spectorsoft – www.spectorsoft.com

[40] See the US *Scarfo* case: http://epic.org/crypto/scarfo.html

[41] including, depending on circumstances, certain "retained" communications data – see ATSCA, 2001, Part XI

[42] See also the website of the Office of Surveillance Commissioners. http://www.surveillancecommissioners.gov.uk/

legislation, has to interact with the Human Rights Act, 1998[43] which among other things requires that intrusive forms of surveillance are necessary and proportionate.

A further problem is disclosure: it is an entirely natural reaction of police to wish to avoid publicity for some of the techniques they deploy, but this has to be balanced by the requirement for a fair trial, which means that anything that is evidence as opposed to intelligence has to be available for testing by the defence. In addition, there is a general duty to make available to the defence any material of relevance to a case upon which the prosecution does *not* intend to rely – "unused material". Under the Criminal Procedure and Investigations Act, 1996 (CPIA) and the associated Code of Practice, there is a statutory duty upon the investigating police officer to record and retain information and material gathered or generated during the investigation. Police may be successful in persuading a judge to grant a Public Interest Immunity (PII) certificate in respect of the fact of the use of the use of certain tools, and also in respect of the technical operation of the precise tool deployed. But any evidence (as opposed to intelligence) thereby acquired would probably not be allowed to go before a jury. As if this were not complicated enough CPIA has also to interact with s 17 of RIPA which, in relation to the interception of the *content* of messages, forbids both its introduction as evidence and any questions as to whether such interception has taken place.[44]

There isn't room here to do more than sketch out the main problems:

[43] For a critical analysis, see *BigBrother.gov.uk: State Surveillance in the age of information and rights*. Akdeniz, Taylor, & Walker [2001] Crim L.R. (February) 73-90. See also Justice's analysis: http://www.justice.org.uk/images/pdfs/7regula.PDF; and that of the Foundation for Information Policy Research: http://www.fipr.org/rip/index.html.

[44] http://www.homeoffice.gov.uk/docs4/CoP_Pre_consultation_draft1.pdf

passive scrutiny, where the police do no more than act as observers but try to collect evidence of what they see	*Such activity will probably be "directed surveillance" under s 28, RIPA. Prior authorisation would be required under Part II RIPA and the associated Codes of Conduct*[45]*. Failure to obtain such authorisation or in the granting of authorisation may result in the acquired evidence being excluded or a defence submission of abuse of process. (The same consideration applies to most of what follows here)*
active scrutiny, where the police interact, to one degree or another, with suspected Internet paedophiles and while doing so try to collect evidence of what happens	*This would make the police "covert human sources" under s 26(8) RIPA; authorisation would have to follow the requirements of s 29 RIPA and the detailed Code of Practice*[46] *Police have to act extremely carefully to avoid defence charges of entrapment; they cannot commit any illegal acts themselves, nor appear to be encouraging such an act in those whom they observe; they must avoid appearing to encourage confessions*[47]

[45] http://www.homeoffice.gov.uk/ripa/covsurv.htm; http://www.surveillancecommissioners.gov.uk/

[46] http://www.homeoffice.gov.uk/ripa/covhis.htm. There are also ACPO Codes of Practice; much of the detail relies on experience in narcotics cases.

[47] See the Robert Coleshill case, thought to be the first where UK police officers behaved proactively by posing as a teenager in a chat room: http://news.bbc.co.uk/hi/english/uk/england/newsid_1769000/1769159.stm. On the perils of undercover activity more generally: the 1992 Rachel Nickell case and its fall-out: http://news.bbc.co.uk/hi/english/uk/newsid_111000/111406.stm

active interference with the property of the accused by using key stroke monitors or programs which allow remote access of suspected computer	*An authorisation could be available under the Police Act, 1997, Part III, to "interfere with property", though this was intended primarily for the use of covert radio transmitters - bugs*[48] *. The Act and associated Code of Practice describe the circumstances of issue, range of powers and associated controls. One could also point to powers under RIPA 2000: such an activity might be considered an "interception" within the definition of s 2 and warrants could be issued under Part I Chapter 1. There are two main problems: the use of a keystroke monitor violates the integrity of any evidence on a hard disk*[49]*; there may be considerable problems of disclosure*
interception of communications associated with a suspect. This will nearly always take place with the co-operation of an ISP	*RIPA draws a distinction between "interception of communications" (Part I Chapter I) and "acquisition of communications data". The first includes the contents of transmission and can only be used for intelligence purposes – it is otherwise inadmissible; warrants are issued by the Home Secretary. The second is limited to traffic data (Part I Chapter II) – the technical instructions enabling a transmission to be transmitted and delivered*[50]*; these require authorisations from senior law enforcement officers*[51] *rather than politicians or judges. Communications data is admissible.* [52]

[48] s 92 Police Act 1997

[49] Considered below as an issue of forensics

[50] The detailed definitions are in s 21 RIPA, 2000

[51] s 22 RIPA, 2000. A draft Statutory Instrument issued in June 2002 sought greatly to extend the number of agencies whose middle managers could issue such orders, though this was later withdrawn while the Home Office rethought its position

[52] One important practical problem is that whereas the distinction between "content" and "traffic data" is clear enough in relation to ordinary telephone traffic, it is much more difficult to make for Internet activities. As a result lawyers acting for ISPs may need to ask the courts for

communications data subject to data retention laws. The main value of such powers is to enable law enforcement to track the activities of a suspect at times *before* he came to their attention	*Under the Anti-Terrorism Security and Crime Act, 2001, ISPs and others may retain communications data for longer than would otherwise be the case*[53]*. Again there is the problem of precisely identifying the distinction between "content" and "traffic data" which may make ISP co-operation difficult and lead defence lawyers to claim that data was retained illegally.*
information about their customers obtained under powers from Internet Service Providers and telecommunication companies	*This information can include the owner of a telephone number, an email account, who held a lease on an IP address at a specific time and also billing data. This information can be obtained by persuading an ISP on the basis of a declaration under s 29(3) Data Protection Act 1998*[54] *but also under RIPA Part I Chapter II*

Forensic precautions and procedures

The purpose of a forensic procedure is that any conclusions can not only be demonstrated but tested. The Association of Chief Police Officers produced a first edition of a *Good Practice Guide for Computer Based Evidence* in March 1998; the current edition is the third and has the following Principles[55]:

Principle 1: No action taken by law enforcement agencies or

---

rulings in particular circumstances; more seriously, defence lawyers in criminal proceedings may raise issues of abuse of process, disclosure, human rights and data protection.

[53] Part XI, ATSCA, 2001. EC Telecommunications Data Protection Directive 97/66/EC and the UK's Telecommunications Data Protection and Privacy Regulations 1999, place obligations on CSPs to erase communications data or make it anonymous immediately after the telecommunications service is provided, unless they are necessary for billing or service quality purposes; ATSCA derogates. See also the *Data Retention Inquiry* by the All-Party Parliamentary Internet Group, 2003, http://www.apig.org.uk/

[54] http://www.linx.net/misc/dpa28-3form.html

[55] The current edition can be downloaded from http://www.nhtcu.org/media/documents/publications/ACPO_Guide_for_computer-based_electronic_evidece.pdf.

> their agents should change data held on a computer or storage media which may subsequently 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.

There are two stages: evidence preservation and analysis. What is striking at the moment is the extreme difference in practical standards between disk forensics and network forensics.

Disk Forensics

In disk forensics the *evidence preservation* problem is addressed by a procedure variously known as "imaging"[56], or making a "bit-stream" or "sector-by-sector" copy. As has been mentioned earlier, if you take a computer upon which a modern complex operating system such as one of the Windows®, Apple Mac or Unix families has been installed, even during the process of starting it up, files are being written to the main hard-disk, and almost every activity on the computer, even if it only seems like passive viewing, may result in further writings to disk; still more takes place when the computer is shut down in the normal way. To avoid this, the subject computer may be started up from the floppy drive – in it is a disk containing a minimal operating system such as DOS or pared-down non-graphical version of Linux. An alternative is to place the suspect hard-disk in a special unit which prevents any writing to the disk – "write-protect". There will also be a small program to perform the bit-stream copying on to some other media – which could be another hard-disk or tape[57]. The result will be a very large intermediate file, about the same size as the total

[56] This is an unfortunately confusing term, as a computer "image" can mean both "a full copy of a disk" and a "file containing a displayable picture"

[57] There are other technical approaches – the subject hard-disk may be removed and placed in a specialist forensic work-station with a "clean" environment. Laptop PCs may require special attention – if the internal hard-drive can't be removed, the "image" file may have to extracted via the parallel port or a network card.

capacity of the original hard-disk; as the name implies, the process seeks to capture *every* part of the hard-disk, whether apparently occupied or not.[58]

The specialist small program could be a free one like *dd* which runs under Linux, a low cost utility designed for computer maintenance staff such as *PowerQuest DriveImage*, *Acronis TrueImage* and *Ghost*, or more costly ones designed especially for forensic use[59]. In any event the technician has to make sure he is using the product properly – the more specialised software packages assist in the taking of precautions, create audit records of what they do and have in-built integrity checks[60].

From the resulting image file any number of exact clones of the original can be created by "restoring" the file to a fresh hard-disk of identical or larger capacity at which point it can be examined. Some of the specialist disk forensic tools carry out their analyses, non invasively, directly on the image files, thus saving some time[61].

The usual first step in *evidence analysis* is to recover deleted files. Data, which includes substantive documents, applications programs, operating system files and various temporary files, is stored electro-magnetically on disk in a series of "sectors" or "clusters". The sectors are arranged along a series of concentric tracks which are read and written to by a moveable arm similar to that used on record players, at the tip of which is a "head" which performs the reading and writing. A particular part of the disk known as the File Allocation Table (under the Windows® 95/98 operating system) or the Master File Table (under Windows NT and XP) acts as an index, relating the files to their physical locations on the disk. When a user wishes to locate a file, they usually do so via the "My Computer" or "Windows® Explorer" programs that are integral to the Windows® operating system – what they see on the screen display is information derived from the File Allocation Table[62]. There will also be date and time information stating when a file was "last accessed" – often there is

[58] For convenience the original very large file is often split into smaller chunks of about 650 MB so that they can be archived, at very low cost, to CD-ROM. Some specialist imaging programs are also able to compress the image file so that it takes up less storage space.
[59] For example, EnCase, AccessData FTK, SafeBack
[60] It is also more important to use specialist tools if it is suspected that the owner of a subject computer is technically sophisticated and may have sought to hide parts of the hard-disk from normal scrutiny. See http://www.cftt.nist.gov/;
http://www.scmagazine.com/scmagazine/2001_04/testc/testc.html
[61] One widely-used tool, EnCase, allows investigators to "preview" a hard-disk – look at it non-invasively via another computer connected across the parallel interface and without the need to make a full "image". This can save investigators time; if the disk is found to be of interest, a full image can be subsequently made for evidential purposes.
[62] Similar general principles apply to other operating systems such as Windows NT/XP, Unix/Linux etc, though the extent to which data is recoverable varies considerably

further information relating to the date of file creation but this may not be immediately visible[63].

In normal use data is constantly being written to various sectors on the disk and the File Allocation Table updates itself. Another function of the normal activity of a computer is that many temporary files, not normally visible to the ordinary user, are created and then deleted. These temporary files are used to increase the efficiency and functionality of the computer, or to provide integrity in the event of error.

When a user decides to delete a file, the actual data remains on the sectors of the disk; all that happens initially is an alteration to the File Allocation Table. The relevant sectors are marked as being free for re-use. Eventually the sectors will be re-used but, depending on such circumstances as the size of the disk and its frequency of use, not for some time. Until then it is possible to recover the files. The popular Symantec "Norton Utilities" suite which costs about £40 includes a facility to do this but there are many other similar programs. The extent to which such recovery is possible and the ease with which the process can be deployed depends on circumstances; in general terms, recently deleted files are more easily recovered than older files. However extensive recovery is possible even if a disk has been reformatted; that is to say, where regular operating systems tools have been used apparently to remove everything on the hard-disk, to the point at which everything that was on it – operating system and all applications – all have to be reinstalled. In order to recover the older data, greater technical skill and more powerful recovery tools are needed. These are also available on the open market and include PowerQuest "Lost and Found"[64]; further more expensive tools aimed at technicians specialising on computer forensics are available. The more extreme forms of data recovery involve dealing with fragments, rather than complete files. These fragments may have lost their context and their date/time stamps. The technician is thus in the position of having lots of pieces to lots of jigsaw puzzles.

Once the data recovery has taken place, the investigator will want to look for, among other things:

- substantive files relevant to the inquiry such as documents, databases, spreadsheets, pictures
- copies of emails, newsgroup postings
- particular installed applications, including the configuration files which may define the way in which a program has been set up and log and cache[65] files which might record activity

[63] "MAC" information – First Created, Last Modified, Last Accessed
[64] Also Zero Assumption Recovery, and ACR data recovery, DiData Media Tools and others
[65] caches are often a feature of Internet browsers

- file fragments from old and temporary files, or which point to recent usage of a file

From these, investigators, ideally police working closely with technicians, can try to infer patterns of behaviour, perhaps producing a chronology of events on that particular computer. In turn this evidence may inter-work with other types of evidence such as evidence found on other computers or other items located at a suspect's home or work-place.

Often the precise location of files on a disk and associated day/time-stamps is crucial to the successful framing of charges. To take the most common example: an investigator has located graphics files on the hard-disk which, on inspection appear to contain indecent pictures of minors:

- if extant pictures are found arranged in an orderly fashion in a series of directories apparently specially created in order to store them – the owner of the computer is certainly in possession of them (the strict liability s 160 CJA offence) and on the basis that he did the arranging one can infer copying (the "making" offence in s 1(1)(a) PCA as interpreted in *Bowden, Atkins, Goodland*)
- if the pictures are found in a directory associated with the cache[66] of an Internet browser, that might indicate that a website was visited but no more. In the absence of other evidence, there would no offence of "making" and, if the computer owner did not know about caches, there might be no offence of "possession" either[67]
- where there is a "live" installation of MIRC and Panzer[68] - files located in a disk directory that seem to indicate that they are being offered by the computer's owner are likely to be evidence of a s 1(1)(c) PCA offence. But if offending files are only found in the default directory where they will have been *uploaded* by others, then depending on circumstances the computer owner can say that it was not he that "made" them, and he may also be able successfully to argue a defence under the "possession" offence in s 160 CJA.

---

[66] the purpose of a cache is to speed up performance; during a typical browse of website, most users tend to want to return to certain key pages which contain indexes to the site as a whole; instead of fetching these pages from the remote website on each occasion, it would be helpful if a copy was stored on the user's PC. The cache in fact stores everything a user does on the 'net – for potential re-use. After a while, older material is deleted to make way for newer.

[67] *Atkins v DPP* [2000] 1 WLR 1427; however Simon Brown LJ also said: "So far as the cache material is concerned, it was also common ground before us that (the Defendant) would have no defence to charges of possession had the prosecution case been put simply on the basis of transient downloading of the image onto the screen rather than on the basis of its subsequent inadvertent storage in the cache." This view is also sustained by *Smith, Jayson,* Court of Appeal; [2002] EWCA Crim 683

[68] For the semi-automated exchange of files via Internet Relay Chat

- where some-one is suspected of distributing offending files via a P2P service such as Morpheus, the suspect will require a piece of "client" software on his PC. Typically this will have a "shared files" folder/directory. Anything in this would probably be "possession with a view to distribution" – s 1(1)(c) PCA. In most instances it wouldn't matter whether the computer owner had placed the files there himself or had previously requested a download from a remote source. The computer owner may also be guilty of "making" – s 1(1)(a) PCA – by inference. P2P client programs may also create configuration files which contain substantial records of files that have been on the computer[69].

Investigators may also want to use material found on a hard-disk to show patterns of behaviour. For example, it may be helpful to be able to demonstrate that the owner of a computer had a persistent interest in paedophile images; it might be possible to do this by retrieving from the cache evidence of the use of web-search engines such as Google against the use of "telling" key words such as "pre-teen", "Lolita[70]" etc. Such evidence might be used to counter a claim by a defendant that the arrival on his computer of an offending file was wholly unexpected.

In addition to hard-disks and data media directly associated with an accused via their home or place of work, evidence may also exist on computers owned by others. Thus: emails and chats logs on a third party computer may corroborate what is found on an accused's computer. Where a computer used for large-scale distribution is located there may be significant records of who uploaded, or downloaded, or subscribed, but these are likely to quite specialist in nature and may require significant effort to understand and analyse.[71] But these third party computers need to have been properly seized and preserved if they are to provide admissible and reliable evidence.

It is for all these reasons that a defence lawyer is very likely to want to have his own expert verify the procedures, findings and inferences made by police investigators and technicians.

All manner of interesting discoveries of potential value to investigators are being made about the internal workings of popular operating systems and applications, but not all have been exhaustively tested. There is an important

[69] Geoff Fellows *Peer-to peer networking issue – an overview*, , Digital Investigation, Vol 1 Issue 1

[70] It may be worth reporting that the use of the word "Lolita" does not invariably and immediately mean under-age sex; there are plenty of pictures of "lolitas" on the web who are over the age of 18, but it should certainly prompt further investigation

[71] See below for Landslide Productions and UK NCS Operation Ore.

rule: the greater the novelty element in a forensic procedure the greater the likelihood it may turn out to mislead.

Network Forensics

If for disk forensics the basic techniques of evidence preservation might be regarded as "sorted", the same cannot be said for network forensics. In a typical situation an investigator will be running an application which enables them to observe a range of activity on the 'net; the application should somehow be creating a log file of this activity and it is this log which is usually produced as evidence. Let us take some examples:

- a website is of interest and it is desirable to capture what is on it at a particular time – will it be enough for evidential purposes to use a regular browser such as Microsoft Internet Explorer or Netscape Navigator to a do a series of regular "saves"?[72]
- activities on certain newsgroups are be scrutinised to see if paedophile material is being published and exchanged – will it be enough for investigators to use the same sort of news reader that everyone else uses[73] and to take a small amount of additional care to preserve the collected postings?
- on Internet Relay Chat – nearly all of the regular client programs contain logging facilities – will these alone be enough for court use?

The problem with all of these log files is that they are very easily altered; logs associated with newsgroup and IRC clients are simply ASCII text files, readily edited using the most basic of text editors; stored web-pages can be edited using any of a number of packages designed to create web-sites (and indeed also by some word-processing packages). Given that log files can be lengthy and difficult to follow, and that not all forms of "saving" of web-pages always capture everything that is seen on screen, there is often strong temptation for investigators to "improve" and "clarify" evidence, even though there is no intention in any way to mislead. In fact there are both procedural means of providing more comfort about the integrity and value of log-files and technical

[72] Peter Sommer, *Downloads, Logs and Captures: Evidence from Cyberspace,* Journal of Financial Crime, October, 1997, 5JFC2 138-152; [2002] CTLR 33-42
[73] eg Forte FreeAgent

ways of preserving them. Currently too few witness statements producing such logs as exhibits even identify the program from which the logging has been obtained. Log file exhibits need to be demonstrated for integrity and continuity just as much as exhibits derived from hard-disks. Some programs produce fuller and more detailed logs than others – a time stamp for each line not only provides a check for completeness, but it may be possible to corroborate it against other streams of evidence, produced from an ISP, phone company, or from findings on a suspect's hard-disk. The problems of log and other audit files that are too long and complex to be immediately understandable and require further interpretation can be overcome by producing two or more exhibits – the original "raw" log, and then successive interpretations derived from it. The "raw" log could probably stay in electronic form, as it is only the defence's expert who is likely to want to check it. The preservation of original logs can be addressed by technical means using tools suggested by Schneier & Kelsey[74]; the log is subjected to regular digital fingerprinting which can be checked for non-interference afterwards.

Tracing Individuals

A very common requirement is to identify individuals located via Internet surveillance or whose nicknames and records of activities are found on hard-disk. As we have seen, on many of the Internet institutions where paedophile activity is found, participants do not use their real names, or even their regular email addresses. Indeed on IRC, the newsgroups and on various P2P services, one individual may adopt several simultaneous nicknames and personalities. A very useful document produced by the London Internet Exchange – LINX – explains the techniques of tracing[75]. Sometimes it is necessary for an investigator to connect his machine to that of a suspect in order to derive its IP address.[76] Most ISPs assign an IP address to a customer each time the customer dials into their service – that address is held only for that session. The ISP typically holds a log of which customer had ISP address at what time in what is called a RADIUS log. Thus, an investigator having obtained an IP address of a suspect will first have to identify the ISP who owns it – which can be done via a general Internet resource[77] – and then ask the ISP to identify their customer. Each stage needs to be covered by appropriate witness statements and an expert hired by the defence will want to test the evidence to ensure that no technical

[74] Secure Audit Logs to Support Computer Forensics, Bruce Schneier and John Kelsey, *ACM Transactions on Information and System Security*, v. 1, n. 3, 1999 http://www.counterpane.com/audit-logs.pdf

[75] LINX Best Current Practice – *Traceability*: http://www.linx.net/noncore/bcp/traceability-bcp.html

[76] An IP address is essential for a communication on the Internet. It takes the form of "4dot3" - eg 192.168.123.123.

[77] Whois queries to RIPE, ARIN and APNIC or via a combination look-up tool such as the ones available at www.geektools.com

mistakes were made and that all the actions were carried out under the relevant legal powers.

Encryption

A further set of problems arise where a suspect is using encryption. There can be several situations. In the most common, *parts* of the suspect's stored data are encrypted – most of the PC is "open" but there are sections, files, directories, or "containers" which hold files, which are encrypted. This approach is popular because it is easy to implement and there are relatively large numbers of robust software products available; the computer can be used normally and then specific actions are needed to decrypt the "secret" items. Data in encrypted form can be shared – either via the Internet or on CD-ROM – by passing on the encrypted files *plus* the passphrase needed to decrypt. Another approach is to encrypt the *whole* of a hard-disk This can be done either in software – tricky because *some* of the hard-disk has to remain unencrypted or the computer's operating system won't work – or in hardware (via a token, dongle, or card)

RIPA now gives the authorities the power to issue a notice requiring disclosure in respect of encrypted data[78]; the maximum penalty is two years and there has been concern that this might be regarded as "acceptable" by a paedophile who may otherwise face a maximum punishment of 10 years and be placed on the Sex Offenders' Register.

In practice, it does not always require the assistance of the owner of a computer to be able to decrypt material on it. Some encryption packages are weak, or may be weakly implemented such that clues about passwords or even whole sections of unencrypted files may be recovered forensically. There are also a whole variety of encryption-breaking software and hardware facilities available. In the United Kingdom, the centralised law enforcement resource for this is NTAC, the National Technical Assistance Centre. Even where encrypted files do not yield to attack, it is sometimes possible to find log and configuration files which give the *names* of the files that have been encrypted; if these are suggestive of certain content, that may be enough to meet the needs of some charges.

There is an interesting problem, too complex to go into in this article, of how one obtains proof of correct decryption[79]

[78] Part III, ss 49-55, but at the time of writing in mid-2005 was still awaiting detailed implementation

[79] See Schneier, Bruce, *Applied Cryptography*, pp 235-236 on unicity distance

Evidence and Sentencing

When some-one is convicted of a Protection of Children Act offence, guidelines for sentencing are provided by the case of *R v Oliver*[80]. This in turn relied heavily on a report produced by the Sentencing Advisory Panel (SAP) [81] in 2002.

The advice suggests that the two primary factors determining the seriousness of an offence should be:

- the nature of the indecent material (from images of nudity or erotic posing to those depicting gross assault of children by adults, sadism or bestiality); and
- the extent of the offender's involvement with the material (from possession for the offender's personal use to the original production of images or widescale commercial distribution).

In respect of the first there is a 5-stage classification of the seriousness of child abuse photographs:

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

This can sometimes create a degree of uncertainty as to the precise category into which a specific image should be placed, however these are only guidelines.

In respect of establishing the extent of an offender's involvement, one normally has to conduct an investigation of the available evidence in a manner similar to that required to secure a conviction.

Typical Defences

[80] [2003] Cr. App. R. 28: 463.
[81] http://www.sentencing-guidelines.gov.uk/docs/advice_child_porn.pdf

A number of "standard" defences offered by accuseds has appeared and it is worth examining them briefly – and seeing how investigators and prosecutors can counter them.

Whose Fingers on the Keyboard?

In its simplest form a defendant says: "Yes, you have may found child abuse material on my computer but I was not the only user and I deny that I am responsible for what you say have found." On many personal computers it may turn out to be difficult to determine whose fingers were on the keyboard at any one time. Personal computers usually lack the sophisticated access control systems such as usernames and passwords that are used on larger-scale and corporate computers – for most practical purposes in a home environment such a level of security is unnecessary.

But investigators do have some answers:

- at the point at which a suspect is first interviewed it is useful to ask an early question to establish whether anyone else has the use of the computer, thus thwarting a later change of story
- Operating systems such as Windows XP create special sets of folders (directories) for each user and these can include an individual Internet cache, sets of programs and configuration files. Material found in a unique user folder is more likely to have been acquired by that user
- Alibi or absence of alibi may be established by reference to dates and times at which particular offending material arrived on a computer
- Evidence of proclivity may be found in emails sent by or to a suspect even if there are no offending files attached[82].

Offending material not solicited

The defendant says: "The offending material you have found was not requested or sought by me; it simply arrived." If the defendant is charged under s 160 Criminal Justice Act for "possession", the onus is on the defendant to demonstrate on the balance of probabilities "that the photograph was sent to him without any prior request made by him or on his behalf and that he did not keep it for an unreasonable time."[83]. But if the charges are under s 1 Protection of Children Act 1978 the evidential onus is on the prosecution. In those circumstances prosecutors can point the court to:

- the quantity of material that seems to have been collected
- the time over which the material that seems to have been collected

[82] Now made easier by Criminal Justice Act, 2003, Part II, sections 98-112.
[83] s 160 s 2(c)

- emails, websites visited, discovered documents as evidence of proclivity

Pop-up Windows

This is a variant on the "offending material not solicited" theme but with a specific technical characteristic. A "pop-up" window while web-browsing is one which is subsidiary and additional to the main viewing window. In typical situations they may contain information additional to that on the main window (for example, more detail on a product for sale or explanations of terms and conditions) or they may contain advertising. There are a variety of simple-to-implement programming facilities available to web-designers who wish to create pop-up windows. Some of these facilities allow the pop-ups to be surprisingly persistent, obscuring the main window, being difficult to close down or generating further pop-ups when one pop-up is closed down.

The advertising pop-up in particular is usually unsolicited and visitors to "legal" sites offering sexual content may indeed be subjected to pop-ups offering "illegal" material.

Content from pop-up windows is stored in the Internet cache along with material from the main windows and hence may be located by forensic investigators.

In distinguishing from circumstances where this defence may be legitimate, a prosecutor can consider:

- whether all the offending material is limited to the cache or if it has been "saved" elsewhere to disk (in which case there is evidence of a "making" for the purposes of s 1(1)(a) PCA
- the proportion of offending material against "innocent" – how often can a computer owner be "shocked and horrified" to be receiving indecent material in particular circumstances?
- whether there is any evidence of searching for questionable material, for example by the use of significant search phrases on a search engine
- the time and date stamps of the offending pictures – sometimes the speed of arrival just after the request for a "legitimate" site
- whether there is any code within recovered web-pages which shows the operation of the pop-up[84]

[84] Though more typically it will be defence experts to go searching for such code

Trojans

In the "trojan defence" the defendant claims that his computer had been taken over by a rogue program which enabled a third party to control its activities remotely over the Internet. Such "Trojan horse" programs undoubtedly exist and are relatively easy to acquire and install. However it is also easy to detect whether they have been deployed in any specific situation.

Trojans work because a small "server" program has been installed on the computer that is to be the subject of remote control. The remote controller needs another program – a "client" – which sends the instructions over the Internet to the server. The installation of the server can be carried out covertly, for example by including it an apparently innocent email or when some-one browses on a web-site and "clicks" on an apparently innocent link.

Once installed and depending on the precise variety, Trojans can do anything that a legitimate user of an infected computer can do, they can enable monitoring of key-strokes and they can locate passwords.

But Trojans do leave traces of their activities. Nearly all anti-virus programs scan for Trojans as well[85] and for the ordinary user, regular scanning is the best defence.

Counters to the Trojan Defence include:

- scanning to see if there is a Trojan present, or deleted traces
- considering the quantity of offending material present – the more there is the less plausible it is for a defendant to suggest that he was unaware of the material
- considering the time period over which the offending material arrived on the computer – the longer the period the less plausible it is for a defendant to suggest that he was unaware of the material
- the presence of other files, emails, site visits etc which indicates a proclivity on the part of the defendant for indecent material

Access by the Defence

The position of defence lawyers and those they employ in handling material containing pictures of child sexual abuse is identical to that of police and prosecutors. S 46 Sexual Offences Act 2003 provides a defence to s 1(1)(a) Protection of Children Act, 1978: a defendant must show "it was necessary for

[85] Using forensic software it is sometimes possible to trace deleted Trojans; however a scan using a conventional anti-virus program would only pick up extant Trojans.

him to make the photograph or pseudo-photograph for the purposes of the prevention, detection or investigation of crime, or for the purposes of criminal proceedings". Once some-one is accused, arrested, charged, the s 46 kicks in provided that all activities can be justified. There is no provision in the legislation for the police or Crown Prosecution Service to seek to impose blanket conditions on the provision of what would otherwise be evidence upon which they seek to rely. Normally the *age* and *Oliver Level* of pictures can be established at a simple View at a police station but any detailed examination of an individual's activities as reflected by hard-disk evidence will need to proceed on the basis of the supply of copies of hard-disk and media forensic images to a defence expert. These experts will want to be able to examine the material at their leisure and at a time of their chosing, in exactly the same way as experts retained by the police. Defence reports are privileged until disclosed.

Police and prosecutors can of course seek to withhold evidence or impose terms on its viewing against arguments specific to a particular situation, for example if the disk contains material that can be justified as "sensitive" (perhaps because it refers to other investigations not yet complete) or because there is a real belief that an individual retained by the defence might break the law by using indecent material outside the scope of the specific criminal proceedings.

Defence experts who feel the need to carry out investigations into the contents of websites that might contain offending material would do well to obtain the agreement of those instructing, to keep detailed notes of all activities, and to have techniques for destroying relevant files, including those in internet caches, at the conclusion of the instructions.

Conclusions

The investigatory techniques described here have had to evolve over a very short period of time and in many cases without the traditional controls of forensic science in the form of publication in a peer-reviewed journal. At the moment too little attention is being paid to the third principle in the ACPO Best Practice document: "An audit trail or other record of all processes applied to computer based evidence should be created and preserved. An independent third party should be able to repeat those processes and achieve the same result". The very high standards now used in disk forensics make the practices deployed in network forensics and interception look weak. Too often prosecution witness statements fail to refer explicitly to what forensic tools were deployed, and to address issues of "continuity" so that each step taken can be followed. It is not always clear where an expert witness has moved from a "finding" (something which an expert hired by the defence should be able to replicate) to an "inference" (which would call for an agreement on

interpretation). Police concern that publication of some of its methods may make future similar investigations more difficult sometimes leads to coyness in their witness statements, or attempts to exclude particular aspects on Public Interest grounds.

We have yet to see any significant testing of the operation of RIPA, either in respect of powers to intercept or those sections dealing with encrypted material.[86]

Few of these issues are entirely new; it is the speed of change in the technology that creates many of the problems. Improvements in this area would seem to depend partly on training of investigators and prosecutors but also the development of the sort of Quality Assurance protocols that are used in more established areas of forensic science[87].

Parliament has over the last few years introduced a number of powerful changes to police powers of investigation. But the new regime is extremely complex as the new powers also have to inter-work with legislation on Human Rights and on disclosure. It seems likely that investigating officers will have to think extremely carefully before adopting certain techniques which they may wish to avoid disclosing; for the same reason, prosecutors will have to consider very carefully the precise charges they wish to have tried in court.

Finally, there are still too many poorly researched and worded indictments which lead to unnecessarily prolonged pre-trial activities as well as over-long trials. As this article has sought to show, it is not enough for offending material simply to have been "found" in the course of an examination by a forensic computing technician – but there needs to be precise evidence of an accused's activities and intent.

[86] Part III

[87] eg based on BS5750/ISO9000 series which provide the testing of the value of a process and then introduce a scheme whereby it can be consistently followed.