Good Practice Guide for Computer-Based Electronic Evidence

Official release version

7safe information security

The ACPO Good Practice Guide for Computer-Based Electronic Evidence
published by 7Safe. For more information visit www.7safe.com

7safe information security

www.acpo.police.uk

It gives me great pleasure to introduce the fourth version of the Association of Chief Police Officers' (ACPO) Good Practice Guide for Computer-Based Electronic Evidence. I would like to personally thank all of the public and private sector authors for their valuable contributions towards making this latest revision a timely reality. In particular, I would like to thank 7Safe for their assistance in publishing the document itself.

With ever-increasing numbers of digital seizures and constantly developing technology, these guidelines are essential to informing the collection and preservation of this most fragile form of evidence. Previous versions of this document have set vital standards for law enforcement and corporate investigators alike, a position I would like to see continue with this and future revisions of the document. The continuing fast paced evolution of both hardware and software makes it essential to develop best practice in line with the technical challenges which we face when capturing digital evidence, in order to prevent its contamination or loss. This latest revision has been not only timely, but also essential, in order that our practices are fit for purpose when considering recent and upcoming advances in every day technology.

Historically, the impact of e-crime or computer related crime has involved only a small proportion of victims and investigators. However, this position is changing and the impact of digital evidence within 'conventional' investigations is already widespread. Indeed, any investigation within the public or private arena is likely to involve the seizure, preservation and examination of electronic evidence, therefore a digital evidence strategy must form an integral part of the wider investigative process. I commend this guide and recommend the application of its principles to both managers and practitioners alike.

Sue Wilkinson
Commander, Metropolitan Police Service
Chair of the ACPO E-Crime Working Group

www.7safe.com

7Safe has partnered with the ACPO E-Crime Working Group in the publication of this guide. As a contributing author of this document, 7Safe's considerable research in the field of digital forensics has focused not only on traditional approaches to digital evidence, but also the fast-evolving areas of volatile data, live acquisition and network forensics. The future of digital forensics will present many challenges and in order to optimise the credibility of investigators, the progressive and proven practices outlined in this guide should be adhered to.

The traditional "pull-the-plug" approach overlooks the vast amounts of volatile (memory-resident and ephemeral) data that will be lost. Today, investigators are routinely faced with the reality of sophisticated data encryption, as well as hacking tools and malicious software that may exist solely within memory. Capturing and working with volatile data may therefore provide the only route towards finding important evidence. Thankfully, there are valid options in this area and informed decisions can be made that will stand the scrutiny of the court process.

The guide also considers network forensics pertaining to "information in transit" i.e. as it passes across networks and between devices, on a wired and wireless basis. As forensic investigators, we need to take into consideration, where legally permitted, the flow of data across networks. This type of approach can prove critical when analysing and modelling security breaches and malicious software attacks.

7Safe advocates best practice in all dealings with electronic evidence. By publishing this guide in conjunction with ACPO, our aim is to help ensure that procedural problems do not arise during investigations or in the court room and that the very highest of standards are achieved and maintained by those working in the electronic evidence arena.

Dan Haagman
Director of Operations, 7Safe

Contents

Application of this guide	2
Introduction	3
The principles of computer-based electronic evidence	4
Overview of computer-based electronic investigations	5
Crime scenes	7
Home networks & wireless technology	14
Network forensics & volatile data	17
Investigating personnel	20
Evidence recovery	23
Welfare in the workplace	26
Control of paedophile images	28
External consulting witnesses & forensic contractors	32
Disclosure	35
Retrieval of video & CCTV evidence	38
Guide for mobile phone seizure & examination	45
Initial contact with victims: suggested questions	52
Glossary and explanation of terms	54
Legislation	60
Local Hi-Tech Crime Units	63

Application of this guide

When reading and applying the principles of this guide, any reference made to the police service also includes the Scottish Crime and Drugs Enforcement Agency e-crime Unit and the Police Service for Northern Ireland (PSNI) unless otherwise indicated. This is so that the anomalies between the different legal systems and legislation within Scotland and the differences in procedures between England and Wales, Scotland and Northern Ireland are included. It also makes this guide a national United Kingdom document. Details in this guide are designed to ensure good practice when collecting computer-based electronic evidence

The guidelines in this document relate to:

Personnel attending crime scenes or making initial contact with a victim/witness/suspect

Securing, seizing and transporting equipment from search scenes with a view to recovering computer-based electronic evidence, as well as in the identification of the information needed to investigate a high-tech crime.

Investigators

Planning and management by investigators of the identification, presentation and storage of computer-based electronic evidence.

Evidence recovery staff

Recovery and reproduction of seized computer-based electronic evidence by personnel who are trained to carry out the function and have relevant training to give evidence in court of their actions. Persons who have not received the appropriate training and are unable to comply with the principles, must not carry out this category of activity.

External consulting witnesses

The selection and management of persons who may be required to assist in the recovery, identification and interpretation of computer-based electronic evidence.

Introduction

Since the initial publication of this guide, the electronic world and the manner in which it is investigated has changed considerably. This guide has been revised in the light of those developments.

Information Technology is ever developing and each new development finds a greater role in our lives. The recovery of evidence from electronic devices is now firmly part of investigative activity in both public and private sector domains.

Electronic evidence is valuable evidence and it should be treated in the same manner as traditional forensic evidence - with respect and care. The methods of recovering electronic evidence, whilst maintaining evidential continuity and integrity may seem complex and costly, but experience has shown that, if dealt with correctly, it will produce evidence that is both compelling and cost effective.

This guide is an Association of Chief Police Officers' (ACPO) publication written in association with the Association of Chief Police Officers Scotland and is aimed principally at police officers, police staff, and private sector investigators working in conjunction with law enforcement. However, this document will be of relevance to other agencies and corporate entities involved in the investigation and prosecution of incidents or offences which require the collection and examination of digital evidence. It is appreciated that they may make use of this guide. Recognising this, the generic terms "investigator" and "law enforcement" have been used wherever possible.

Although the electronic world has evolved, the principles of evidential preservation recommended in previous versions of this document are still highly relevant and have remained broadly the same, with only a few minor changes to terminology. They are consistent with the principles adopted by the G8 Lyon group as a basis for international standards.

It cannot be overemphasised that the rules of evidence apply equally to computer-based electronic evidence as much as they do to material obtained from other sources. It is always the responsibility of the case officer to ensure compliance with legislation and, in particular, to be sure that the procedures adopted in the seizure of any property are performed in accordance with statute and current case law.

This good practice guide is intended for use in the recovery of computer-based electronic evidence; it is not a comprehensive guide to the examination of that evidence.

The advice given here has been formulated to assist staff in dealing with allegations of crime which involve a high-tech element and to ensure they collect all relevant evidence in a timely and appropriate manner.

The principles of computer-based electronic evidence

Four principles are involved:

Principle 1:

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

Principle 2:

In circumstances where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to give evidence explaining the relevance and 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.

Explanation of the principles

Computer-based electronic evidence is subject to the same rules and laws that apply to documentary evidence.

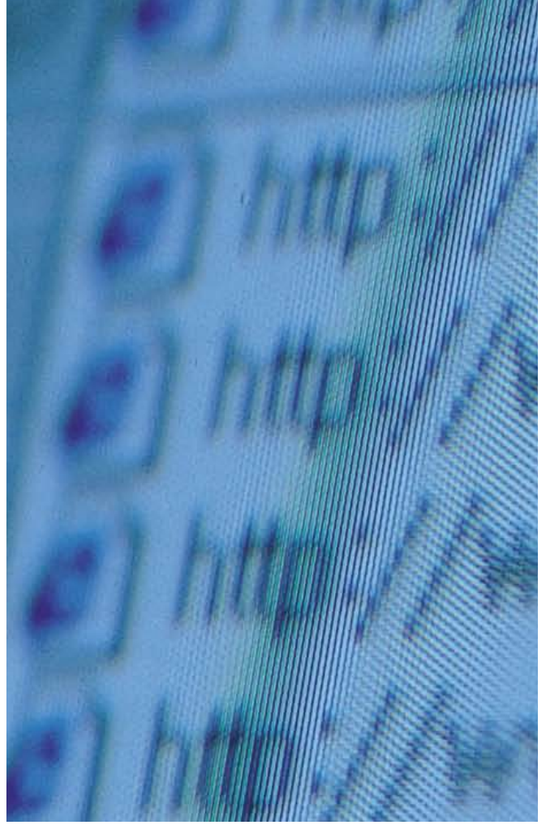
The doctrine of documentary evidence may be explained thus: the onus is on the prosecution to show to the court that the evidence produced is no more and no less now than when it was first taken into the possession of police.

Operating systems and other programs frequently alter and add to the contents of electronic storage. This may happen automatically without the user necessarily being aware that the data has been changed.

In order to comply with the principles of computer-based electronic evidence, wherever practicable, an image should be made of the entire target device. Partial or selective file copying may be considered as an alternative in certain circumstances e.g. when the amount of data to be imaged makes this impracticable. However, investigators should be careful to ensure that all relevant evidence is captured if this approach is adopted.

In a minority of cases, it may not be possible to obtain an image using a recognised imaging device. In these circumstances, it may become necessary for the original machine to be accessed to recover the evidence. With this in mind, it is essential that a witness, who is competent to give evidence to a court of law makes any such access.

It is essential to display objectivity in a court, as well as the continuity and integrity of evidence. It is also necessary to demonstrate how evidence has been recovered, showing each process through which the evidence was obtained. Evidence should be preserved to such an extent that a third party is able to repeat the same process and arrive at the same result as that presented to a court.



Overview of computer-based electronic investigations

Overview of computer-based electronic investigations

Technology is present in every aspect of modern life. At one time, a single computer filled an entire room. Today, a computer can fit in the palm of your hand. Criminals are exploiting the same technological advances which are driving forward the evolution of society.

Computers can be used in the commission of crime, they can contain evidence of crime and can even be targets of crime. Understanding the role and nature of electronic evidence that might be found, how to process a crime scene containing potential electronic evidence and how an agency might respond to such situations is crucial.

This guide represents the collective experience of the law enforcement community, academia and the private sector in the recognition, collection and preservation of computer-based electronic evidence in a variety of crime scenarios.

Each responder must understand the fragile nature of computer-based electronic evidence and the principles and procedures associated with its collection and preservation.

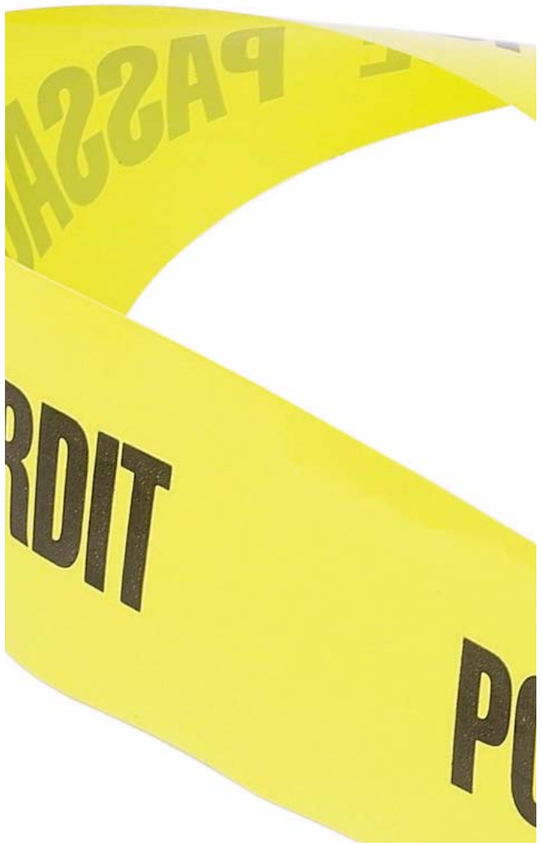
The Nature of Computer-Based Electronic Evidence

Computer-based electronic evidence is information and data of investigative value that is stored on or transmitted by a computer. As such, this evidence is latent evidence in the same sense that fingerprints or DNA (deoxyribonucleic acid) evidence is latent.

In its natural state, we cannot see what is contained in the physical object that holds our evidence. Equipment and software are required to make the evidence available. Testimony may be required to explain the examination and any process limitations.

Computer-based electronic evidence is, by its very nature, fragile. It can be altered, damaged, or destroyed by improper handling or improper examination. For this reason, special precautions should be taken to document, collect, preserve and examine this type of evidence. Failure to do so may render it unusable or lead to an inaccurate conclusion.

This guide suggests methods that will help preserve the integrity of such evidence. Whilst this document focuses mainly on the retrieval of evidence from standalone or networked computer systems and its subsequent detailed examination, consideration is also given to retrieving evidence from the wider Internet e.g. web sites.



Crime scenes

Crime scenes

There are many data storage devices/media that may be encountered whilst searches are being conducted during criminal investigations. These are often valuable sources of evidence which, if dealt with in an evidentially acceptable manner, may enhance the investigation. This section is intended to assist individuals who have received no specialist training in this area, to carry out such searches and ensure that their actions in relation to the seizure of such material are correct.

The most common types of storage devices are illustrated in the glossary of terms appended to this document. These devices should be treated with as much care as any other item that is to be forensically examined.

The following guidance deals with the majority of scenarios that may be encountered. The general principles, if adhered to, will ensure the best chance of evidence being recovered in an uncontaminated and, therefore, acceptable manner.

It is accepted that, depending on the particular circumstances found during a search, there may be more appropriate options available than those that follow. However, these alternative options will not be addressed in this guide, as such courses of action should only be invoked by individuals who have received appropriate training in this specialised area of work.

The majority of computers found during searches are desktop or laptop PCs. These machines usually consist of a screen, keyboard and main unit (with slots in the front or sides for floppy disks, CDs or other storage devices). Other machines are becoming more widespread, in particular, personal organisers, palmtop computers, next generation games consoles, portable media players and mobile phones incorporating: software, removable storage ans significant processing power. These can hold large amounts of data, often in storage areas not immediately obvious to the investigator.

If in any doubt as to the correct action to be taken, seek specialist advice.

Desktop and Laptop Computers

Upon discovery of computer equipment which appears to be switched off:

- Secure and take control of the area containing the equipment.
- Move people away from any computers and power supplies.
- Photograph or video the scene and all the components including the leads in situ. If no camera is available, draw a sketch plan of the system and label the ports and cables so that system/s may be reconstructed at a later date.
- Allow any printers to finish printing.
- Do not, in any circumstances, switch the computer on.
- Make sure that the computer is switched off – some screen savers may give the appearance that the computer is switched off, but hard drive and monitor activity lights may indicate that the machine is switched on.
- Be aware that some laptop computers may power on by opening the lid.
- Remove the main power source battery from laptop computers. However, prior to doing so, consider if the machine is in standby mode. In such circumstances, battery removal could result in avoidable data loss.
- Unplug the power and other devices from sockets on the computer itself (i.e. not the wall socket). A computer that is apparently switched off may be in sleep mode and may be accessed remotely, allowing the alteration or deletion of files.
- Label the ports and cables so that the computer may be reconstructed at a later date.
- Ensure that all items have signed and completed exhibit labels attached to them. Failure to do so may create difficulties with continuity and cause the equipment to be rejected by the forensic examiners.
- Search the area for diaries, notebooks or pieces of paper with passwords on which are often attached or close to the computer.
- Consider asking the user about the setup of the system, including any passwords, if circumstances dictate. If these are given, record them accurately.
- Make detailed notes of all actions taken in relation to the computer equipment.

Upon discovery of computer equipment which is switched on:

- Secure the area containing the equipment.
- Move people away from computer and power supply.
- Photograph or video the scene and all the components including the leads in situ. If no camera is available, draw a sketch plan of the system and label the ports and cables so that system/s may be reconstructed at a later date.
- Consider asking the user about the setup of the system, including any passwords, if circumstances dictate. If these are given, record them accurately.
- Record what is on the screen by photographing and by making a written note of the content of the screen.
- Do not touch the keyboard or click the mouse. If the screen is blank or a screen saver is present, the case officer should be asked to decide if they wish to restore the screen. If so, a short movement of the mouse should restore the screen or reveal that the screen saver is password protected. If the screen restores, photograph or video it and note its content. If password protection is shown, continue as below, without any further touching of the mouse. Record the time and activity of the use of the mouse in these circumstances.
- Where possible, collect data that would otherwise be lost by removing the power supply e.g. running processes and information about the state of network ports at that time. Ensure that for actions performed, changes made to the system are understood and recorded. See section on Network forensics and volatile data.
- Consider advice from the owner/user of the computer but make sure this information is treated with caution.
- Allow any printers to finish printing.
- If no specialist advice is available, remove the power supply from the back of the computer without closing down any programs. When removing the power supply cable, always remove the end attached to the computer and not that attached to the socket. This will avoid any data being written to the hard drive if an uninterruptible power protection device is fitted.
- Remove all other connection cables leading from the computer to other wall or floor sockets or devices.
- Ensure that all items have signed exhibit labels attached to them. Failure to do so may create difficulties with continuity and cause the equipment to be rejected by the forensic examiners.
- Allow the equipment to cool down before removal.
- Search area for diaries, notebooks or pieces of paper with passwords on which are often attached or close to the computer.
- Ensure that detailed notes of all actions are taken in relation to the computer equipment.

What should be seized

For the retrieval of evidence (Examples):

- Main unit: usually the box to which the monitor and keyboard are attached.
- Monitor, keyboard and mouse (only necessary in certain cases. If in doubt, seek expert advice).
- Leads (again only necessary in certain cases. If in doubt, seek expert advice).
- Power supply units.
- Hard disks not fitted inside the computer.
- Dongles (see Glossary).
- Modems (some contain phone numbers).
- External drives and other external devices.
- Wireless network cards (see Glossary).
- Modems.
- Routers.
- Digital cameras.
- Floppy disks.
- Back up tapes.
- Jaz/Zip cartridges.
- CDs.
- DVDs.
- PCMCIA cards (see glossary).
- Memory sticks, memory cards and all USB/firewire connected devices.
- N.B. Always label the bags containing these items, not the items themselves.

If the power is removed from a running system, any evidence stored in encrypted volumes will be lost, unless the relevant key is obtained. Also, note that potentially valuable live data could be lost, leading to damage claims, e.g. corporate data.

To assist in the examination of the equipment, seize:

- Manuals of computer and software.
- Anything that may contain a password.
- Encryption keys.
- Security keys – required to physically open computer equipment and media storage boxes.

For comparisons of printouts, seize:

- Printers, printouts and printer paper for forensic examination, if required.

Treatment of electronic organisers and personal digital assistants

Introduction

Electronic organisers and Personal Digital Assistants (PDAs) range from very small, very cheap devices that hold a few telephone entries to expensive devices that are as powerful as some desktop PCs and can hold large amounts of text, sound, graphics and other files. The most powerful tend to use Palm OS, Symbian OS or Windows CE.

Personal Organisers (PDAs)

Although each may perform differently in detail, all organisers (PDAs) follow a similar basic design. They contain a small microcomputer with a miniature keyboard and a display screen, together with memory chips in which all the information is stored. The memory is kept active by batteries and, if these fail, all information contained in the organiser (PDA) may be lost. However, data may be recovered from flash memory. Often, there are two sets of batteries: a main set which is designed to run the display and keyboard when the organiser is switched on and a backup battery which maintains information in the memory, if and when the main batteries fail. Some organisers (PDAs) have a single rechargeable battery, which is normally kept topped up by keeping the organiser (PDA) in its cradle connected to a PC.

This battery tends to fail very quickly when not kept charged. Standard batteries will also fail at some time. When seizing PDAs, seek specialist advice at an early stage in relation to charging and/or battery charging, in order to prevent loss of evidence.

Remember to seize all power cables, leads and cradles associated with the PDA.

Application of the principles

With a PC, the essential concerns are to leave the evidence on the hard disk unchanged, and to produce an image which represents its state exactly as it was when seized. With an organiser/PDA, there tends to be no hard disk and the concern has to be to change the evidence in the main memory as little as possible and then only in the certain knowledge of what is happening internally. The possibility of producing an image may exist with the use of specialist software.

This results in two major differences between PCs and organisers (PDAs). To access the device, it will almost certainly have to be switched on (an action which should be avoided at crime scenes), which effectively means that Principle 1 cannot be complied with. It is therefore necessary to ensure that Principle 2 is adhered to. This makes the competence of the analyst and Principle 3, the generation of a detailed audit trail, even more important.

Procedures

On seizure, the organiser/PDA should not be switched on. It should be placed in a sealed envelope before being put into an evidence bag. This procedure prevents the organiser from being opened and accessed whilst still sealed in the evidence bag, a situation that can easily arise with smaller organisers. Many mobile phones now incorporate PDA functionality. If a device suspected of having WiFi or Bluetooth or mobile phone capability is recovered at the crime scene, investigators should consider placing the device in a shielded box, as per the principles for the seizure of mobile phones (see page 45). A search should also be conducted for associated memory devices, such as IC Cards, Solid State Disks, CF Cards, SmartMedia Cards and Memory Sticks, as well as any leads or cradles used for connecting the organiser to a PC.

If switched on when found, consideration should be given to switching the organiser/PDA off, in order to preserve battery life. However, if it is likely that the device is password protected, it should be kept active and immediate forensic examination sought. It should undergo the same consideration as a computer that is switched on. A note of the time and date of the process should be made. Then, package as above.

Any power leads, cables or cradles relating to the organiser/PDA should also be seized.

The organiser/PDA should never be returned to the accused at the scene or prior to the evidence recovery procedures being completed. Remember, pressing the RESET button or the removal of all batteries can result in the complete loss of all information held in the device.

A competent person should examine the organiser (PDA) at an early stage and batteries replaced or kept recharged as necessary to prevent any loss of evidence. Batteries must be checked at regular intervals to preserve the evidence until all examinations are complete. A competent person who understands the specific implications of the particular model should access the organiser. As recommended in the explanation of the principles, it is essential that a witness who is competent to give evidence in a court of law makes this access.

Because of the wide variety of different organiser models, no attempt has been made here to outline the procedures that should be adopted by persons in accessing organisers/PDAs. The procedure will vary greatly from model to model, particularly in respect of the kind of operating system used and in obtaining access to password-protected areas.

It is of paramount importance that anyone handling electronic organisers/PDAs prior to their examination, treat them in such a manner that will give the best opportunity for any recovered data to be admissible in evidence in any later proceedings.

Other storage media

It should be borne in mind that a number of electronic devices encountered at searches might contain evidence relevant to your criminal investigation. These include:

- Mobile telephones.
- Pagers.
- Land line telephones.
- Answering machines.
- Facsimile machines.
- Dictating machines.
- Digital cameras.
- Telephone e-mailers.
- Internet-capable digital TVs.
- Media PC.
- Satellite receivers.
- HD recorders.
- Next generation games consoles.

If any of these items are to be seized and disconnected from a power supply, their memory may be erased. Seek expert advice before taking any action.

Transport

Main computer unit

Handle with care. If placing in a car, place upright where it will not receive serious physical shocks. Keep away from magnetic sources (loudspeakers, heated seats & windows and police radios).

Monitors

These are best transported screen down on the back seat of a car and belted in.

Hard disks

As for the main unit, protect from magnetic fields. Place in anti-static bags or in tough paper bags or wrap in paper and place in aerated plastic bags.

Floppy Disks, Jaz & Zip cartridges, Memory Sticks and PCMCIA cards

As for the main unit, protect from magnetic fields. Do not fold or bend. Do not place labels directly onto floppy disks.

Personal Digital Organisers, Electronic Organisers and Palmtop computers

Protect from magnetic fields.

Keyboards, leads, mouse and modems

Place in plastic bag. Do not place under heavy objects.

Other Considerations

- Preservation of equipment for DNA or fingerprint examination.
- If fingerprints or DNA are likely to be an issue, always consult with the case officer.
- Using aluminium powder on electronic devices can be dangerous and result in the loss of evidence. Before any examination using this substance, consider all options carefully.
- Store equipment in conditions of normal humidity and temperature. Do not store in conditions of excessive heat, cold, dampness or humidity.

Batteries

Most computers are capable of storing internal data, including CMOS (see Glossary) settings, by using batteries. Batteries must be checked at regular intervals to preserve the evidence, until all examinations are complete and the data secured. It is not possible to determine the life expectancy of any one battery. However, this is an important consideration when storing a computer for long periods before forensic examination and should be addressed in local policy.

Storage after seizure

The computer equipment should be stored at normal room temperature, without being subject to any extremes of humidity and free from magnetic influence such as radio receivers. Some computers are capable of storing internal data by use of batteries. If the battery is allowed to become flat, internal data will be lost.

Dust, smoke, sand, water and oil are harmful to computers. Aluminium fingerprint powder is especially harmful and dangerous.

Crime scenes on the Internet

The Internet is a medium through which material can be stored, relayed or shared. Despite its size and complexity, it is nothing more than a large computer network. Ultimately, any information on the Internet physically resides on one or more computer systems and, therefore, it could be retrieved through a forensic examination of those physical devices. However, some of this information may be volatile, e.g. instant messaging content; or it could be altered or deleted prior to the location and examination of those devices, e.g. website content. In such cases, it may be necessary to capture evidence directly from the Internet, possibly during 'live' interaction with a suspect or by capturing live website content.

E-mail

E-mail is increasingly seen as the communications medium of choice, amongst a technically aware population. E-mail can be forensically retrieved from physical machines, although in certain circumstances it may be that only a small number of e-mails require retrieval and examination. Investigators may wish to obtain these from a victim's computer system, without having to address possible delays in obtaining a forensic examination or causing significant inconvenience to the victim. In such circumstances, printed copies of the e-mails themselves, including header information, would be sufficient to evidence the sending / receipt and content of the e-mail. Header information is not normally visible to the reader of the e-mail, but it can be viewed through the user's e-mail client program. The header contains detailed information about the sender, receiver, content and date of the message. Investigators should consult staff within their force Computer Crime Units or Telecommunications Single Point of Contact if they are under any doubt as to how to retrieve or interpret header information. Clearly any such evidential retrievals need to be exhibited in the conventional manner i.e. signed, dated and a continuity chain established.

Crime scenes (cont.)

E-mail / Webmail / Internet Protocol Address account information

Investigators seeking subscriber information relating to e-mail, webmail or Internet connections should consult their force Telecommunications Single Points of Contact who are able to advise on the potential availability and nature of user or subscriber information. Any request for Telecommunications Data is subject to the provisions of the Regulation of Investigatory Powers Act (RIPA) 2000.

Websites / Forum Postings / Blogs

Evidence relating to a crime committed in the United Kingdom may reside on a website, a forum posting or a web blog. Capturing this evidence may pose some major challenges, as the target machine(s) may be cited outside of the United Kingdom jurisdiction or evidence itself could be easily changed or deleted. In such cases, retrieval of the available evidence has a time critical element and investigators may resort to time and dated screen captures of the relevant material or 'ripping' the entire content of particular Internet sites. When viewing material on the Internet, with a view to evidential preservation, investigators should take care to use anonymous systems. Advice on the purchase and use of such systems should be obtained from the force Computer Crime or Open Source Intelligence Unit. Failure to utilise appropriate systems could lead to the compromise of current or future operations. Investigators should consult their force Computer Crime Unit if they wish to 'rip' and preserve website content.

Open Source Investigation

There is a public expectation that the Internet will be subject to routine 'patrol' by law enforcement agencies. As a result, many bodies actively engage in proactive attempts to monitor the Internet and to detect illegal activities. In some cases, this monitoring may evolve into 'surveillance', as defined under RIPA 2000. In such circumstances, investigators should seek an authority for directed surveillance, otherwise any evidence gathered may be subsequently ruled inadmissible. Once again, when conducting such activities, investigators should utilise anonymous systems which are not likely to reveal the fact that law enforcement is investigating that particular section of the Internet.

Covert Interaction on the Internet

In circumstances where investigators wish to covertly communicate with an online suspect, they MUST utilise the skills of a trained, authorised Covert Internet Investigator (CII). CIIs have received specialist training which addresses the technical and legal issues relating to undercover operations on the Internet. The interaction with the suspect(s) may be in the form of e-mail messaging, instant messaging or through another online chat medium. When deploying CIIs, a directed surveillance authority must be in place, as well as a separate CII authority. Prior to deploying CIIs, investigators should discuss investigative options and evidential opportunities with the force department responsible for the co-ordination of undercover operations. The deployment of CIIs is governed by the National Standards in Covert Investigations, which are detailed in the Manual of Standards for the Deployment of Covert Internet Investigators.

Home networks & wireless technology

Home networks & wireless technology

Networks of computers are becoming more common in the domestic environment and are well established in corporate settings. In the home, they are usually based upon what is called a 'Workgroup', or "MSHOME" network, where the user of one networked computer is able to access others over the network without any particular computer being 'in charge' of the others.

The use of wireless networks in both the corporate and home environment is also increasing at a considerable rate. Being able to move around a room whilst retaining network / Internet access has obvious advantages, hence its increasingly popularity. To the forensic investigator, this presents a number of challenges and an increased number of potential artefacts to consider. Due to the potential complexity of 'technical' crime scenes, specialist advice should be sought when planning the digital evidence aspect of the forensic strategy.

A whole range of wired and wireless devices may be encountered:

- Switches, hubs, routers, firewalls (or devices which combine all three).
- Embedded network cards (e.g. Intel Centrino).
- Access Points.
- Printers and digital cameras.
- Bluetooth devices – PDAs, mobile phones, dongles etc.
- Hard drives both wired and wireless*.
- Wireless networks cannot be controlled in the same way as a traditionally cabled solution and are potentially accessible by anyone within radio range. The implications of this should be carefully considered when planning a search or developing the wider investigative strategy.

* Storage devices may not be located on the premises where the search and seizure is conducted.

If computers are networked, it may not be immediately obvious where the computer files and data which are being sought are kept. Data could be on any one of them. Networks, both wired and wireless, also enable the users of the computers to share resources such as printers, scanners and connections to the Internet. It may well be that the fact that one of the computers is connected to the Internet means that some or all of the others are also connected to the Internet as well.

The Internet connection may be an 'always on' type connection, such that, even if no-one is apparently working on a computer or using the Internet, there may be data passing to and fro between computers or between the network and the Internet nevertheless.

If a wired network is present, there will usually be a small box (called a 'hub' or a 'switch') also present, connecting all the computers and the Internet together. Hubs and switches look very much the same as one another. The network cables are usually connected at the rear.

There is usually a row of small lights somewhere on the box in clear view. Each light relates to one of the networked connections, computers, printers, scanners etc. These indicate whether or not the network is busy. If any of the lights are flashing rapidly, this is an indicator that there is a lot of data passing over the network. If a network is quiet, some of the lights may flash from time to time, but with fairly long gaps between the flashes.

The network may also be connected to another device (called a Cable Modem or a DSL Modem) providing access to the Internet. This may be mounted on the wall, or on the floor, or on the surface of a desk. It may not be immediately obvious that it is there. One wire from this device will usually be connected to the telephone system and another wire will be connected either to one of the computers present or directly to the network hub, or the modem itself may be incorporated within the hub in a modem/router.

When planning an operation involving a network, consider carefully the possibility of remote access, i.e. person(s) accessing a network with or without permissions from outside the target premises. Investigators should consider the possibility of nefarious activity being carried out through the insecure network of an innocent party. The implications of such a scenario are that search warrants could be obtained on the basis of a resolved Internet Protocol address, which actually relates to an innocent party. The implications are potentially unlawful searches and legal action taken against the relevant investigative agency.

Consider also the possibility of a computer's access to remote online storage, which may physically reside in a foreign jurisdiction. There will be legal issues in relation to accessing any such material. Legal advice should be sought prior to any access or retrieval.

Network detecting and monitoring is a specialist area and should not be considered without expert advice. Recommendations for dealing with networks and wireless implementations involve the following steps:

- Identify and check network devices to see how much network or Internet activity is taking place. Consider using a wireless network detector to determine whether wireless is in operation and to locate wireless devices.
- Once satisfied that no data will be lost as a result, you may isolate the network from the Internet. This is best done by identifying the connection to the telephone system or wireless communications point and unplugging it from the telephone point. Keep modems and routers running, as they may need to be interrogated to find out what is connected to them. Due to their nature, it is particularly difficult to ascertain what is connected to a wireless network.
- Trace each wire from the network devices to discover the computer to which it is connected. This may not be possible in business premises where cables may be buried in conduits or walls (advice in this case should be sought from the local IT administrator as to the set up of the system). Make a note of each connection. The connections on the network device will be numbered 1 to 4, or perhaps 1 to 8. Note which computer is connected to which number 'port' on the device (hub / switch / router or multi-function device). Label each connection in such a way that the system can be rebuilt exactly as it stands, should there be any future questions as to the layout. In a wireless environment, remember that no cables are used between a PC and its base station. However, there will still be some physical cabling to each device (which could include a network cable to the wired network, power cables etc.), the configuration of which should be recorded. Please note too that Cable / DSL modems can also have wireless capabilities built in.
- Once satisfied that you will lose no potential evidence as a result, you may remove each connection in turn from the network device once it has been identified. This will isolate each computer in turn from the network. The same can be done with cabling into wireless devices.
- As you do so, consider photographing the layout of the network and the location of the machines connected to it, so as to allow a possible future reconstruction.
- Seize and bag all network hardware, modems, original boxes and CDs / floppy disks etc. (provided they are easily removable).
- Subsequently treat each computer as you would a stand-alone computer.
- Remember that the data which is sought may be on any one of the computers on the network, so do not be tempted to leave behind a computer in a child's bedroom, for instance. Incriminating material may be stored on it without the child's knowledge.
- Bear in mind the possibility that the network may be a wireless network as well as a wired one, i.e. certain computers may be connected to the network via conventional network cabling. Others may be connected to that same network via the mains system, and others may be connected via a wireless link.
- Also, bear in mind that any mobile phones and PDAs may be WiFi or Bluetooth enabled and connected to a domestic network.

Concerns with remote wireless storage often focus around the inability to locate the device. In this instance, it would be impossible to prove that an offence had been committed. However, when considering remote wireless storage, the investigator is encouraged to consider the artefacts on the seized machines in question according to existing practice. Artefacts such as cached images, typed URLs etc. are still to be found, together with evidence that a remote storage device has been used.

An important note to consider during a forensic investigation is the use of clones, whereby a suspect's hard drive is cloned and placed into (usually) the original chassis. In the event the clone was taken from an environment using wireless technology and, when powered up, it is possible that the data stored on the cloned drive may be accessible to anyone in the vicinity. This would cause evidential issues and may result in serious ethical consequences.

To reduce this problem, the following steps could be taken:

- Disable the wireless card by removing it from the chassis.
- Install a "dummy load" antenna on the wireless card (if an external antenna connection is present).
- Conduct the investigation in a Faraday cage / tent / bag.
- Install network protection software (researching the evidential consequences first).

Network forensics & volatile data

Network forensics & volatile data

Computer forensic investigators may be able to, in certain circumstances, glean further evidence from a machine whilst it is still in its running, or 'live', state. Information available includes network connectivity details and volatile (non-persistent) memory-resident data. Caution must be taken to avoid unnecessary changes to evidence – please refer to Principle 2 of the guidelines.

The types of information that may be retrieved are artefacts such as running processes, network connections (e.g. open network ports & those in a closing state) and data stored in memory. Memory also often contains useful information such as decrypted applications (useful if a machine has encryption software installed) or passwords and any code that has not been saved to disk etc.

If the power to the device is removed, such artefacts will be lost. If captured before removing the power, an investigator may have a wealth of information from the machine's volatile state, in conjunction with the evidence on the hard disk. By profiling the forensic footprint of trusted volatile data forensic tools, an investigator will be in a position to understand the impact of using such tools and will therefore consider this during the investigation and when presenting evidence.

A risk assessment must be undertaken at the point of seizure, as per normal guidelines. to assess whether it is safe and proportional to capture live data which could significantly influence an investigation.

Considering a potential Trojan defence, investigators should consider collecting volatile evidence. Very often, this volatile data can be used to help an investigator support or refute the presence of an active backdoor.

The recommended approach towards seizing a machine whilst preserving network and other volatile data is to use a sound and predetermined methodology for data collection.

It may be worthwhile considering the selected manual closure of various applications, although this is discouraged unless specific expert knowledge is held about the evidential consequences of doing so. For example, closing Microsoft Internet Explorer will flush data to the hard drive, thus benefiting the investigation and avoiding data loss. However, doing this with certain other software, such as KaZaA, could result in the loss of data.

Individual tools could be run, but often the results require interpretation and this approach also results in inconsistency and allows for potential error to occur. It is therefore recommended that a scripted approach be adopted using a number of basic trusted tools to obtain discrete information, such as:

- process listings.
- service listings.
- system information.
- logged on & registered users.
- network information including listening ports, open ports, closing ports.
- ARP (address resolution protocol) cache.
- auto-start information.
- registry information.
- a binary dump of memory.

All of the above may be run from a forensically sound, bootable, floppy disk, DVD / CD-ROM or USB Flash Drive. The latter is recommended (with the exception of systems running Windows 9x), as it can be quickly installed, run and the resultant output written back to the device. Considering the potential size of a memory dump, the amount of data could be substantial, thus a sizeable USB Flash Drive is recommended. Once the device is stopped, it should be safely removed and then standard power-off forensic procedures followed.

Network forensics & volatile data (cont.)

A summary of the steps to be taken is shown below. Documentation of all actions, together with reasoning, should also apply when following such steps:

- Perform a risk assessment of the situation – Is it evidentially required and safe to perform volatile data capture?
- If so, install volatile data capture device (e.g. USB Flash Drive, USB hard drive etc.)
- Run the volatile data collection script.
- Once complete, stop the device (particularly important for USB devices which if removed before proper shutdown can lose information).
- Remove the device.
- Verify the data output on a separate forensic investigation machine (not the suspect system).
- Immediately follow with standard power-off procedure.

When dealing with computer systems in a corporate environment, the forensic investigator faces a number of differing challenges. The most significant is likely to be the inability to shut down server(s) due to company operational constraints. In such cases, it is common practice that a network enabled 'forensic software' agent is installed, which will give the ability to image data across the network on-the-fly. However, other forensic software is available which does not entail installation of an agent.

Other devices could be encountered which may assist the investigation. For example, routers and firewalls can give an insight into network configuration through Access Control Lists (ACLs) or security rule sets. This may be achieved by viewing the configuration screens as an administrator of the device. This will require the user names and passwords obtained at the time of seizure or from the suspect during interview.

By accessing the devices, data may be added, violating Principle 1 but, if the logging mechanism is researched prior to investigation, the forensic footprints added during investigation may be taken into consideration and therefore Principle 2 can be complied with.

In the case of large company networks, consider gaining the advice and assistance of the network administrator/ support team (assuming that they are not suspects).

Network forensics and volatile data no doubt presents the investigator with technical challenges. However, as cases become more complex and connectivity between devices and public networks proliferates together with the number of Trojan defence claims, the above recommendations will need to be considered.

Investigating personnel

Investigating personnel

Whenever possible and practicable, thought must be given to the potential availability and nature of computer-based electronic evidence on premises, prior to a search being conducted. Investigators may wish to consider the use of covert entry and property interference in more serious cases, particularly if encrypted material is likely to be encountered. The appropriate RIPA consent must, of course, be obtained prior to any such activity. Consideration must also be given to the kind of information within and whether its seizure requires any of the special provisions catered for in the Police and Criminal Evidence Act (PACE) 1984 and the associated Codes of Practice. In Scotland, when seeking a search warrant through the relevant Procurator Fiscal to the Sheriff, the warrant application should clearly indicate what electronic evidence is anticipated and which persons are required to expedite the recovery and seizure of that material. Where there is concern that special procedure material is to be part of the electronic evidence, that should also be disclosed to the Procurator Fiscal.

Pre-search

When a search is to be conducted and where computer-based electronic evidence may be encountered, preliminary planning is essential. As much information as possible should be obtained beforehand about the type, location and connection of any computer systems. If medium or large network systems are involved and are considered a vital part of the operation, then relevant expert advice should be sought before proceeding. Single computers with an internet connection are those most commonly found and can usually be seized by staff that have received the basic level of training in digital evidence recovery. The IT literacy of the suspect and the known intelligence should be considered in any risk assessment/policy decision, in relation to calling in specialist assistance or seeking specialist advice pre-search.

Briefing

It is essential that all personnel attending at the search scene be adequately briefed, not only in respect of the intelligence, information and logistics of the search and enquiry, but also in respect of the specific matter of computers.

Personnel should be encouraged to safeguard computer-based electronic evidence in the same way as any other material evidence. Briefings should make specific mention, where available, of any specialist support that exists and how it may be summoned. Strict warnings should be given to discourage tampering with equipment by untrained personnel.

Consider using visual aides to demonstrate to searchers the range of hardware and media that may be encountered.

Preparation for the search

Investigators should consider the following advice when planning and preparing to conduct searches where computer equipment is known or believed to be present. Depending upon availability, persons trained and experienced in the seizure of computer equipment may be in a position to advise investigators.

What to take

The following is a suggested list of equipment that might be of value during planned searches. This basic tool-kit should be considered for use in the proper dismantling of computer systems as well as for their packaging and removal:

- Property register.
- Exhibit labels (tie-on and adhesive).
- Labels and tape to mark and identify component parts of the system, including leads and sockets.
- Tools such as screw drivers (flathead and crosshead), small pliers, wire cutters for removal of cable ties.
- A range of packaging and evidential bags fit for the purpose of securing and sealing heavy items such as computers and smaller items such as PDAs and mobile phone handsets.
- Cable ties for securing cables.
- Flat pack assembly boxes - consider using original packaging if available.
- Coloured marker pens to code and identify removed items.
- Camera and/or video to photograph scene in situ and any on-screen displays.
- Torch.
- Mobile telephone for obtaining advice, but do not use in the proximity of computer equipment.

Who to take

If dealing with a planned operation and it is known that there will be computers present at the subject premises, consideration should be given to obtaining the services of personnel who have had formal training and are competent to deal with the seizure and handling of computer-based evidence. In some circumstances, the case officer may feel it necessary to secure the services of an independent consulting witness to attend the scene of a search and indeed subsequent examination. This is particularly relevant if some of the material seized is likely to constitute special procedure material, as defined under section 14 of PACE 1984 (England & Wales only).

Records to be kept

In order to record all steps taken at the scene of a search, consider designing a pro-forma, which can be completed contemporaneously. This would allow for recordings under headings such as:

- Sketch map of scene.
- Details of all persons present where computers are located.
- Details of computers - make, model, serial number.
- Display details and connected peripherals.
- Remarks/comments/information offered by user(s) of computer(s).
- Actions taken at scene showing exact time.

Remember, a computer or associated media should not be seized just because it is there. The person in charge of the search must make a conscious decision to remove property and there must be justifiable reasons for doing so. The search provisions of PACE 1984 and the associated Codes of Practice equally apply to computers and peripherals in England and Wales. In Scotland, officers should ensure they are acting within the terms of the search warrant.

Interviews

Investigators may want to consider inviting trained personnel or independent specialists to be present during an interview with a person detained in connection with offences relating to computer-based electronic evidence. There is currently no known legal objection to such specialists being present during an interview and it would not breach the principles referred to in this guide. However, consideration must be given to the responsibilities of an investigating officer imposed by the PACE 1984 and the associated Codes of Practice.

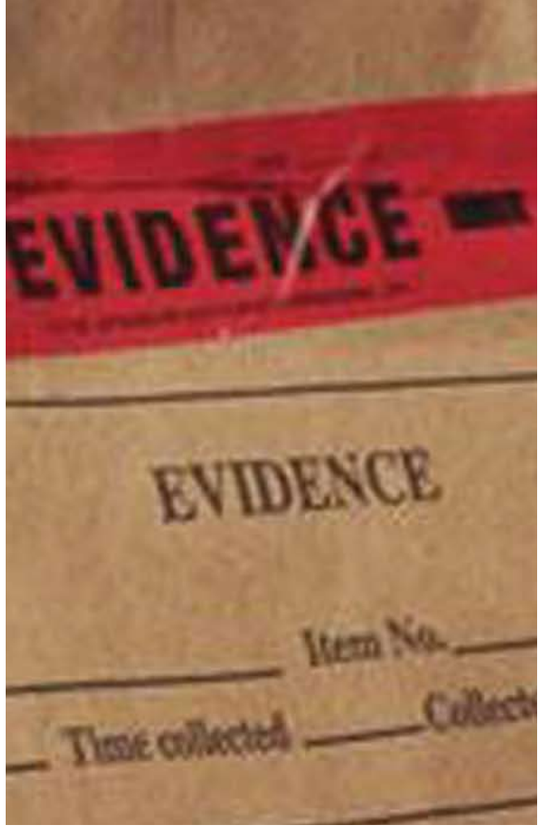
Remember that any such participation by a specialist may affect his/her position as an independent witness.

The use of technical equipment during interviews may be considered, in order to present evidence to a suspect. There is no known legal objection to evidence being shown to a suspect in such a fashion. Hard copy exhibits, referred to as 'productions' in Scotland, shown to a suspect should be identified according to local instructions, ensuring there will be no future doubt as to what exhibit the suspect was shown. Suspects are not specifically required to sign production labels in Scotland. This process will not be possible with data exhibited through a computer. Care should therefore be taken that a court will be satisfied that the data referred to during an interview is clearly identified.

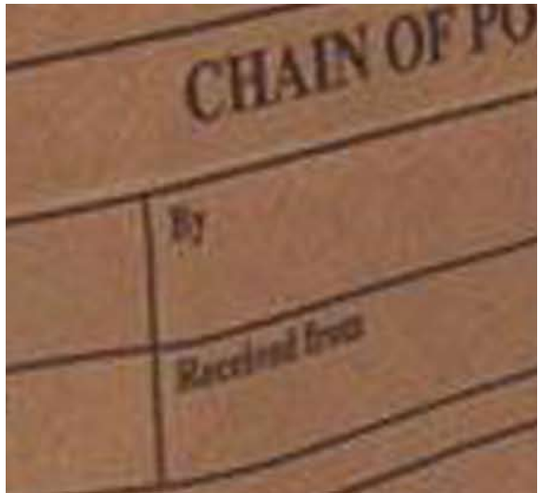
The advice in relation to interviews is to be read in conjunction with National Guidelines on interview techniques.

Retention

Consider retaining the original exhibit as primary evidence notwithstanding any obligation under S22 PACE 1984 (this legislation is not applicable in Scotland). The grounds for any such decision should be carefully considered and noted accordingly.



Evidence recovery



Evidence recovery

This section is directed towards staff engaged in the field of computer-based electronic evidence recovery, who have received the appropriate training and who have the requisite experience. These persons will normally have specialised equipment to assist in their role and this, together with the aforementioned training and experience, will enable them to comply with the principles set out above and any local directives. This section is not intended for use by any other personnel, as this may lead to the erosion of the integrity and continuity of the evidence.

The recovery process

The nature of computer-based electronic evidence is such that it poses unique challenges to ensure its admissibility in court. It is imperative that established forensic procedures are followed. These procedures include, but are not limited to, four phases: collection, examination, analysis, and reporting.

Although this guide concentrates on the collection phase, the nature of the other three phases and what happens in each are also important to understand.

The collection phase

Involves the search for, recognition of, collection of and documentation of computer-based electronic evidence. The collection phase can involve real-time and stored information that may be lost unless precautions are taken at the scene.

The examination process

This process helps to make the evidence visible and explain its origin and significance and it should accomplish several things. First, it should document the content and state of the evidence in its totality. Such documentation allows all parties to discover what is contained in the evidence. Included in this process is the search for information that may be hidden or obscured.

Once all the information is visible, the process of data reduction can begin, thereby separating the “wheat” from the “chaff.” Given the tremendous amount of information that can be stored on electronic media, this part of the examination is critical.

The analysis phase

This phase differs from examination in that it looks at the product of the examination for its significance and probative value to the case. Examination is a technical review that is the province of the forensic practitioner, while analysis may be conducted by a range of people. In some agencies, the same person or group will perform both these roles.

The report or statement

This outlines the examination process and the pertinent data recovered and completes an examination. Examination notes must be preserved for disclosure or testimony purposes. In Scotland, they will be preserved as productions to be used as evidence in court. An examiner may need to testify about, not only the conduct of the examination, but also the validity of the procedure and his or her qualifications to conduct the examination.

The role of the examiner is to secure from any seized material, be it hard disks, floppy disks, tape or any other storage media, a true copy of the data contained therein. This should be obtained without compromising the original data. In order to ensure this, care should be taken in the selection of software or hardware utilised in any procedure that is undertaken.

As the process that is being conducted is a forensic examination, sound and established forensic principles should be adhered to. This means full records should be made of all actions taken. These can be made available to the defence who may subsequently conduct a further examination to validate the actions taken. Such records are also part of the unused material for the case under investigation.

It is important to remember that legislation continues to change to keep up with requirements of the society. Therefore, it is important to consider the legal requirements when examining computer-based electronic data for evidential purposes.

Recent case studies and precedents set at higher courts are important considerations when preparing an evidence package for a case officer. This specifically applies to the use of the Internet and files downloaded from the Internet, or material accessible from foreign jurisdictions i.e. online data stores.

Evidence recovery (cont.)

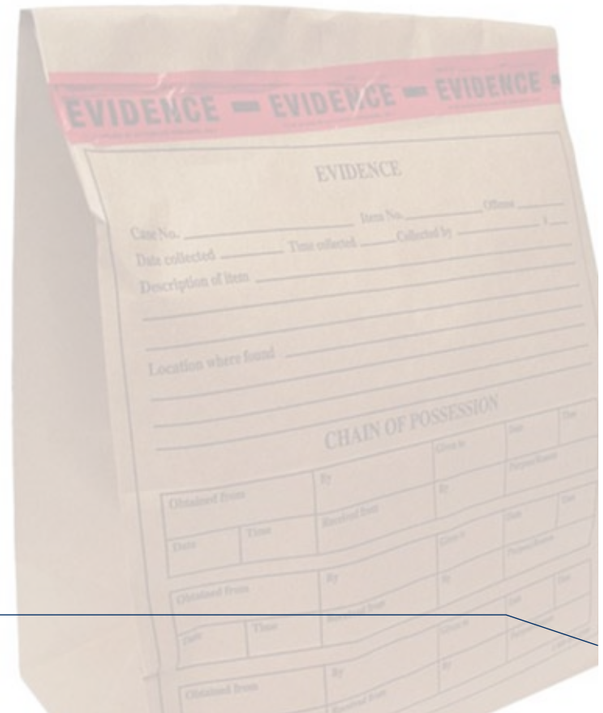
Examining electronic organisers (PDAs)

A number of schemes are employed which permit the user to protect some or all of the information in an electronic organiser/personal digital assistant (PDA), by means of a password. This is called password protection. One scheme is where the organiser requires the entry of a password as soon as it is switched on, preventing access to any information until the correct password has been given. Another scheme provides for two separate compartments in the organiser: a secret compartment and an open compartment. To obtain access to information in the secret compartment, the correct password must be given to open it. Yet another scheme provides for the encryption of any file that is password protected. The file is held in memory in an encrypted form and cannot be opened until the correct password is given for that file. One or more of these schemes are available in almost all organisers/PDAs.

Implications of switching the organiser/PDA on

The significance of switching on the organiser varies across the entire range. It is important to appreciate that pressing the ON button will always change the internal memory and hence the evidence in some respect or another. Keystrokes made on the keyboard are themselves stored in the internal memory, so the act of pressing the ON button itself changes the value held in the current key memory location. This change itself is unlikely to affect any stored data but, what happens thereafter depends on the operating system of the organiser and what other keystrokes are made. If it is a Windows CE operating system, changes to a number of files will take place as the operating system becomes active, in a manner similar to that when running a Windows based system on a PC. Some other operating systems, which maintain date and time stamping of files will change file settings when files are opened and closed. Again, this results in evidence being changed. All power cables, leads and cradles relating to the PDA should have been seized.

Remember, the integrity and continuity of evidence is of paramount importance.



Welfare in the workplace

Welfare in the workplace

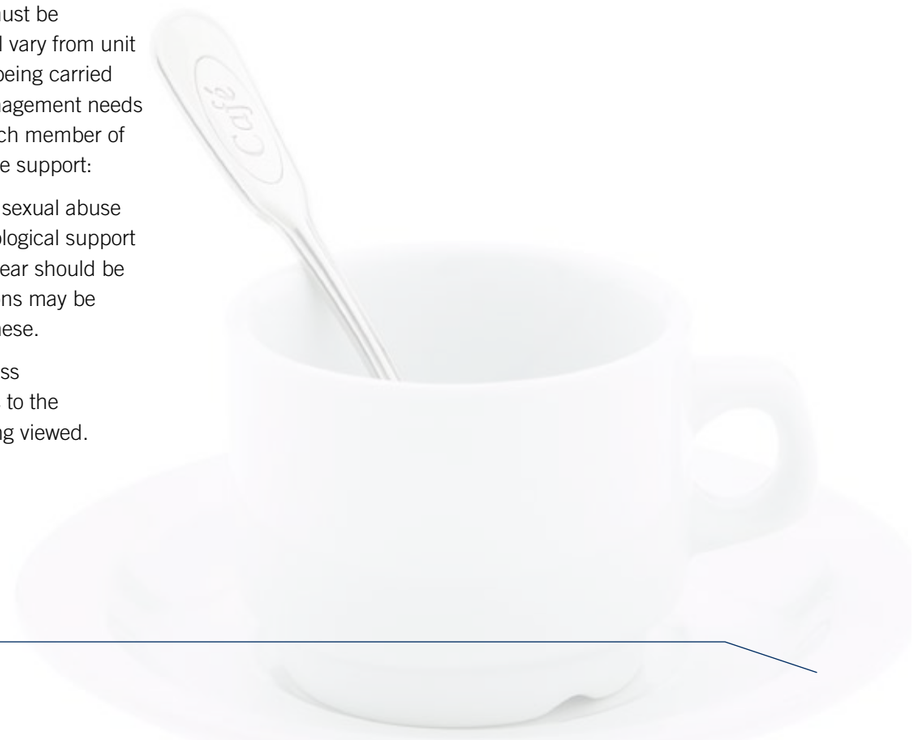
The examination of any medium that contains images of sexually abused children is an important role in investigations. The evidence contained within these images, be it video cassette or one of many other types of electronic data, is a permanent record of sexual abuse. The viewing and examination of this type of material is demanding and stressful. Anecdotal evidence suggests that such images may be encountered during the examination of digital evidence retrieved in operations not specifically targeting paedophile activity.

It must be borne in mind that it is not only examiners who come into contact with this type of material. We must not forget those staff who image/copy material, produce transcripts, statements, taped interviews, reports or interviews. Following examination, these images are often shown to the Crown Prosecution Service, district judges, magistrates, defence experts, prosecution counsel, crown court judges and the equivalent personnel in Scotland, jury members and the probation service. This list is by no means definitive. A number of these personnel may be employed in-house or may be contractors from outside the service. All need to be reminded of the sensitivity of such material and adequate precautions need to be taken to ensure support. In fact, any person or organisation that comes into contact with this type of material may need support.

Support comes in various forms. No definitive list can be produced but the following is a suggested guide. Each case should be dealt with according to its own circumstances and each individual risk must be assessed. Conditions and experiences will vary from unit to unit depending upon the type of work being carried out. Because of this, the response of management needs to meet the individual requirements of each member of staff. The following individuals may require support:

Individuals who are exposed to images of sexual abuse on a regular basis should attend a psychological support scheme. A minimum of one session per year should be considered and group or individual sessions may be appropriate or a combination of both of these.

Consider, too, a protocol for 24-hour access to occupational health and restrict access to the environment where these images are being viewed.



Control of paedophile images

Control of paedophile images

It is essential that all material relating to this type of offence be subject to the appropriate protective marking scheme. The minimum level of classification should be 'restricted'. Possession of this material is in itself an offence and each enquiry will also contain personal information and, in some cases, identities of victims.

As with any prosecution, it is essential that evidence is preserved, retrieved and stored in a correct and systematic manner to ensure continuity, integrity and security of the evidence. This will ensure that the best possible evidence remains intact and avoids criticism at any future court proceeding.

Retrieval of evidence

Evidence will usually be recovered from a computer hard disk, floppy disks, CD-ROM, DVD, memory sticks, CF cards or organisers/PDAs. These items will have been seized at the scene and recorded in accordance with existing procedures. It is essential that the security of the media is evidentially sound between seizure and production to the examiner. Continuity of handling will also need to be proved. Furthermore, the security of exhibits at the office of the examiner is equally important.

Formation of evidence

During the examination, a suggested method is that the images and any technical report produced should be exhibited on an encrypted disk or disks and be password controlled. The disk(s) can then be made available to legal representatives and the court for viewing. The CD-ROM or DVD must be kept in secure storage when not being used and a system set in place for it to be signed in and out when it is removed from the storage facility.

It is recommended that printed copies of paedophile images be made in only the most exceptional circumstances and certainly not as a matter of routine. Any printed copies that are made should be controlled with the same level of security as the original media.

As some courts do not yet have the facility to view images from a DVD or a CD-ROM, it may be necessary for the purpose of court proceedings to have the evidential material transferred from the disk onto a video. Alternatively, arrangements could be made to install temporary computer facilities to view images via monitors.

These and any court computer systems used should be cleared of any paedophilic material after use.

Interview

The disk is available against signature to the case officer or any other person conducting an interview of the suspect. The contents of the disk can then be shown and referred to in the interview room by use of a laptop. When referring to the images during the interview, the investigator will use the identifying reference in the same way as on the target computer or storage medium.

Prior to interview, the defence solicitor will be allowed to view the images. This consultation will take place at law enforcement premises under controlled conditions.

Advice/charge

After interview, a decision will be made whether to charge and bail or, in Scotland, release on a written undertaking, if appropriate. Other alternatives would be to defer the charge and bail pending advice from the Crown Prosecution Service (CPS) or, in Scotland the Procurator Fiscal Service (PFS). Arrangements will be made for the CPS or PFS in Scotland to view the disk at a mutually agreeable location. At all times, the disk must remain in the possession of the case officer (in Scotland the Forensic Computer Units). The CPS (PFS) will issue confirmation of charges or advise as necessary.

Defence access

CPS and ACPO Memorandum of Understanding

Section 1(1)(a) of the Protection of Children Act 1978 prohibits the "taking or making" of an indecent photograph or pseudo-photograph of a child. 'Making' includes the situation where a person downloads an image from the internet, or otherwise creates an electronic copy of a file containing such a photograph or pseudo-photograph. To fall within the definition of an offence, such "making" must be a deliberate and intentional act, with knowledge that the image made was, or was likely to be, an indecent photograph or pseudo-photograph of a child (R v Smith and Jayson, 7th March 2002).

Section 46 of the Sexual Offences Act 2003 amends the Protection of Children Act 1978, and provides a defence to a charge of "making". The defence is available where a person "making" an indecent photograph or pseudo-photograph can prove that it was necessary to do so for the purposes of the prevention, detection or investigation of crime, or for the purposes of criminal proceedings.

This reverse burden defence is intended to allow people instructed to act for defence or prosecution who need to be able to identify and act on the receipt of an indecent photograph or pseudo-photograph, to deal with such images. It also creates an obstacle to would be abusers and those who use technology to gain access to paedophilic material for unlawful (or personal) reasons.

The Memorandum of Understanding between the CPS and ACPO is the result of the enactment of section 46 of the Sexual Offences Act 2003. The Memorandum of Understanding is intended to provide guidance to those who have a legitimate need to handle indecent photographs of children by setting out how the defence provided in section 46 of the Sexual Offences Act 2003 may be applied. The Memorandum provides guidance to the Police Service, CPS and others involved in the internet industry, in order to create the right balance between protecting children and effective investigation and prosecution of offences.

After charge, defence solicitor / counsel will always be permitted access to view the images at reasonable hours at either the office of the case officer or the examiner. The accused will only be permitted access whilst he/she is in the company of their legal representative.

It is important to understand that the defence may request access to either the original hard disk or a copy of the image taken by law enforcement. The request is likely to be for them to be able to check the integrity of the evidence or to examine patterns of activity against the allegations. It is expected that defence and law enforcement respect and understand each other's responsibilities in these circumstances. The defence have a duty to defend their client and law enforcement has a duty to ensure that they do not unnecessarily create more paedophile images or compromise sensitive confidential material.

It will not always be the case that the defence need full access to a forensic computer image. Likewise it may not be always appropriate for law enforcement to deny access to a forensic computer image.

In cases of difficulty

In cases of difficulty, in order to decide whether or not to release such illegal material, the following approach can be adopted:

a) A meeting should take place between defence and prosecution technical witnesses in order to establish whether it is necessary to copy and supply a complete forensic image to defence technical witness.

b) If it is necessary the defence technical witness may be given private (or controlled) facilities to examine the image at law enforcement premises at reasonable hours.

c) If the person in charge of the investigation considers it necessary, then the work may take place other than at police premises if the defence technical witness signs a memorandum of undertaking.

d) Where no agreement is reached, the case can be referred to the court to hear argument and issue directions.

e) If the court directs that a copy of the illegal material should be given to the defence technical witness, that person must sign a memorandum of undertaking.

Once the memorandum of undertaking is signed, the person in charge of the investigation may supply a copy of the relevant forensic images to a technical witness. The undertaking aims to ensure that the images are kept in a secure environment and not copied outside of the

terms of the undertaking. All persons having contact with the images will be expected to sign the undertaking. Breach of the undertaking may leave the signatory open to prosecution.

Magistrates court hearing
(not applicable in Scotland)

The first hearing at a magistrates court will normally not involve the production of the disk. However, this will be dictated by local practice. Advocates must be very alert to the need for the preparation of a full file, prior to the determination of mode of trial. It will usually be impossible for magistrates to decide the seriousness of the case without viewing the disk, which will not be available at the first hearing.

When the subsequent hearing in the magistrates court is due, either for mode of trial, committal for sentence or, exceptionally, for sentence in that court, the case officer or forensic examiners will provide the disk at the hearing. The parties in the case will view the images. At all times when dealing with the court, the case officer or examiner will retain control of the disk. Following the hearing, the disk will be returned to the appropriate storage facility and signed back in as before.

Committal
(not applicable in Scotland)

At committal proceedings at the lower court, it will rarely be necessary to show the disk. It may be necessary if the defence wishes to submit there is no case to answer but, usually, the viewing of images will only be of evidence in jury points, such as the age of the victims or whether the images are indecent. Arguments surrounding the act of 'making' or 'taking' can normally be determined without having to view the images. If it becomes necessary for them to be viewed at the hearing, the case officer or examiner will be warned to attend court. Following the hearing, the disk will be returned and signed back in as before.

Plea and directions hearing (PDH)
(not applicable in Scotland)

At the PDH, the case officer or forensic examiner will be warned to attend. The attendance of the examiner may be preferable because of the possible arguments surrounding the technical aspects of the case. Their advice at this stage may be critical to the case. The disk will be available at court for the judge, defence counsel, and for the prosecution. The case officer or examiner will retain control of the disk, but may release it to the defence subject to the usual undertakings as set out above. Following the hearing, the disk will be returned and signed back in as before.

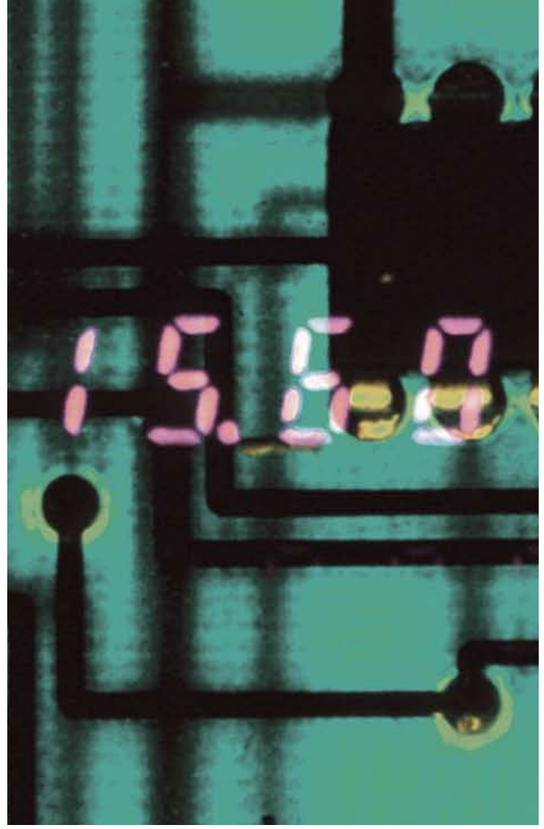
Crown court/magistrates court trial
(High court/sheriff court in Scotland)

At the trial, the best evidence will be direct evidence of an image from the CD-ROM or DVD. The case officer or forensic examiner will attend court and will have a laptop computer and appropriate screen facilities available for display, dependent on local practices. The images can be presented in a number of ways including the use of a PowerPoint or similar presentation on the disk. It is suggested that a warning about the content of the disk is included on the physical disk and also at the beginning of any presentation involving illegal material. By using these methods of presentation, a consistent approach should develop enabling all within the criminal justice system to become used to evidence being presented in this manner.

By adopting a common approach, the issue of security and integrity of the evidence is enhanced. Relevant information about each presented image can be placed on a preceding slide to assist any subsequent process. For example: identifying references, file names, location on disk etc. could be included.

If a point is taken as to the authenticity of the prime images, or of the CD-ROM or DVD, then a defence examiner may be allowed to examine the imaged copy. This will take place in the environment of law enforcement premises or otherwise under the supervision of the forensic examiner at some other premises.

There must be an auditable system in place to track the movement of the CD-ROM or DVD. Each time it is removed and returned, it must be signed in or out. The same applies to any printed material.



External consulting witnesses & forensic contractors

External consulting witnesses and forensic contractors

It is recommended that, wherever practicable, all investigations involving paedophilia and sensitive material should be conducted by law enforcement personnel. However, it is recognised that this is not always possible. Additionally, some investigations involving computer-based electronic evidence may require specialist advice and guidance. Before contracting out any work, it is important to select any external consulting witnesses carefully. Any external witness should be familiar with, and agree to comply with, the principles of computer-based electronic evidence referred to in this guide.

Where agencies ask external specialists to accompany personnel during the search of premises, the name of any such person should be included within the wording of any warrant.

Selection of external consulting witnesses, particularly in the more unusual or highly technical areas, can be a problem for the investigator. The process of selection should not be haphazard, but active and structured from the start. Computer Crime Units may be able to offer more advice on the criteria for selection.

The following guidance should be included when making a selection and the following areas are considered to be the foundation of independent consulting witness skills.

Specialist expertise

- This is the skill or competence to do a particular job.
- What are the individual's relevant qualifications?
- How skilful is the person at this particular job?
- What specific skills does he or she have?
- Is the skill based on technical qualifications or length of experience?

Specialist experience

- What experience of this type of work does the individual have?
- How many cases has he or she been involved with?
- What type of cases are these?
- How long has the individual been working in this area?
- What proof is there of this experience?

Investigative knowledge

Understanding the nature of investigations in terms of PACE, in England and Wales, confidentiality, relevance and the distinction between:

- Information.
- Intelligence.
- Evidence.

Contextual knowledge

Understanding the different approaches, language, philosophies, practices and roles of:

- Police.
- Law.
- Science.

Fundamental to this is the understanding of probability in its broadest sense and differences between scientific proof and legal proof.

Legal knowledge

Understanding of relevant aspects of law such as legal concepts and procedures in relation to:

- Statements.
- Continuity.
- Court procedures.
- A clear understanding of the roles and responsibilities of expert witnesses is essential.

Communication skills

The ability to express and explain in layman's terms, both verbally and in writing:

- Nature of specialism.
- Techniques and equipment used.
- Methods of interpretation.
- Strengths and weaknesses of evidence.
- Alternative explanations.

General

- Cleared to appropriate security level to handle the evidential material.
- Made aware of the paedophilic material guidelines in this guide.
- Made aware of the impact on staff of such material and risk assess appropriately.

Legal considerations

A letter of contract should be made out between any such witness and the police thereby giving them the same protection as is offered to the police under Section 10 of the Computer Misuse Act 1990.

This contract should include advice which outlines their acceptance of the Principles 1 - 4 and clear advice that they should make their own notes of specific actions taken by them during any part of the investigation.

Emphasise clearly that:

- A suitably qualified third party should be able to duplicate their actions by reference to these notes.
- The rules of evidence apply to the notes as if they were made by a Police employee in England and Wales. Consideration must be given as to how the images are to be produced at court.
- All material must be returned to law enforcement at the conclusion of the investigation.

Other considerations

If it is likely that a consulting witness will uncover paedophile images or sensitive information during an investigation, it is suggested that certain preliminary checks should be made before any contractual obligations are undertaken.

These checks could include:

- A search of the Police indices against all staff likely to have contact with the case.
- Confirmation of the address at which the examination will take place.
- Confirmation that material be kept in adequate secure storage (such as a safe) when not in use.
- That the premises where the material is kept are alarmed to national standards.
- That the computer on which this material is to be viewed has adequate security.

Disclosure

Disclosure

This section is designed to address one specific aspect of disclosure in relation to computer-based evidence: how do investigators and prosecutors discharge their disclosure obligations in respect of the massive amounts of data they often have to analyse? For example, 27 Gigabytes of data, if printed out on A4 paper, would create a stack of paper 920 metres high and most computer hard disks are now considerably larger than that.

The Criminal Procedure and Investigations Act 1996 (CPIA) came into force on 1 April 1997[1]. The Act, together with its Code of Practice, introduced a statutory framework for the recording, retention, revelation and disclosure of unused material obtained during criminal investigations commenced on or after that date.

Additional guidance for investigators and prosecutors to assist them in complying with their statutory duties is set out in the Attorney General's Guidelines on Disclosure (revised April 2005). ACPO and the CPS have also agreed detailed joint operational instructions for handling unused material, currently set out in the Disclosure Manual.

What follows should be regarded as a very brief summary of some of the relevant guidance in the Disclosure Manual. It is not intended as a replacement for the detailed guidance provided in the Manual itself.

Even in relatively straightforward cases, investigators may obtain, and even generate, substantial quantities of material. Some of this material may in due course be used as evidence: for example, physical exhibits recovered from the scene of the crime or linked locations, CCTV material, forensic evidence, statements obtained from witnesses and tape recordings of defendants interviewed under caution before charge.

The remaining material is the 'unused material', and it is this material which is the subject of the procedure for disclosure created under the CPIA.

This statutory procedure applies to material held on computers in exactly the same way as it does to material which exists in any other form. In fact, if an investigator comes across relevant information which is not already recorded in any durable or retrievable form, the officer in charge of the investigation may decide to record it on computer disk[2]. Other items may be captured digitally and held on a computer if:

- The original is perishable;
- The original was supplied to the investigator rather than generated by him and is to be returned to its owner; or
- The retention of a copy rather than the original is reasonable in all the circumstances[3].

There may therefore be substantial quantities of computer material obtained or generated by investigators during the course of an investigation, depending on the nature and scale of the investigation.

Where an investigation involves use of the Holmes 2 computer database, the detailed Guidance in Chapter 31 of the Disclosure Manual should be consulted.

Disclosure officers (or deputy disclosure officers) are appointed in the course of criminal investigations, in accordance with paragraphs 3.2 and 3.3 of the CPIA Code of Practice. They have the important duty (amongst others) of examining the material obtained or generated during the investigation and, in due course, describing it on the schedules of unused material, which is a key part of the disclosure process.

Clearly, where there is a large quantity of computer-held material, inspection and description of it may present difficulties. Due to this, the Attorney General has provided some helpful guidance, as shown on the following page:

[1] It has recently been amended in key respects following the implementation of some of the provisions of Part V of the Criminal Justice Act 2003, as of 4 April 2005.

[2] CPIA Code of Practice, paragraph 4.1

[3] CPIA Code of Practice, paragraph 5.1

Disclosure (cont.)

Generally material must be examined in detail by the disclosure officer or the deputy but, exceptionally, the extent and manner of inspecting, viewing or listening will depend on the nature of the material and its form. For example, it might be reasonable to examine digital material by using software search tools. If such material is not examined in detail, it must nonetheless be described on the disclosure schedules accurately and as clearly as possible. The extent and manner of its examination must also be described together with justification[4] for such action.

The CPIA Code of Practice also provides guidance concerning the duty to pursue all reasonable lines of enquiry, in relation to computer material[5].

Examination of material held on a computer may require expert assistance and, in some cases, Digital Evidence Recovery Officers (DEROs) may be commissioned to help extract evidence and assist with unused material. DEROs may be police officers, police staff or external service providers. The use of DEROs and related matters is discussed in detail in Annex H of the Disclosure Manual.

It is important that the material is inspected and described on the unused material schedule, in accordance with the above guidance, as it is the schedules (non-sensitive and sensitive) which are, in due course, revealed to the prosecutor, in order that the latter can comply with the duty under section 3 CPIA to provide primary disclosure to the accused (or initial disclosure, where the criminal investigation in question has commenced on or after 4 April 2005).

After a defence statement has been served by or on behalf of the accused, the prosecutor has a duty to review disclosure. This may trigger further reasonable lines of enquiry, which may lead to the gathering or generation of additional unused material. Some or all of this material may fall to be disclosed to the accused in accordance with the statutory procedures.

The accused may also seek specific disclosure of undisclosed unused prosecution material, by making an application to the court under section 8 of the CPIA, using the procedure set out in rule 25.6 of the Criminal Procedure Rules 2005. In response to such an application, the prosecutor may, after consultation with the disclosure officer, agree to disclosure of some or all of the material sought.

In any case, whether the material is disclosed under section 3 of the CPIA, following service of a defence statement, or after an application for specific disclosure under section 8 of the Act, disclosure may be in the form of providing a copy or copies of the material in question to the defence. It may also be by permitting the defence (or a suitable expert, instructed by the defence) access to the actual material. Guidance concerning this is set out in the Disclosure Manual, 30.8 – 30.13.

It is important to note that where the computer material consists of sensitive images falling within section 1(1)(a) of the Protection of Children Act 1978, the guidance set out in the Memorandum of Understanding Between CPS and ACPO concerning Section 46 Sexual Offences Act 2003 (signed on 4th October 2004) should be followed.

In Scotland, the question of disclosure is fundamentally different from that in England and Wales and is one specifically for the Procurator Fiscal. The question of disclosure was judicially considered in the case of McLeod Petitioner, 1988, SLT233. There is no obligation upon the Crown to produce every document in their possession that has any connection with the case. It is the duty of the Procurator Fiscal to disclose anything that is relevant to establish the guilt or innocence of the accused. The court will not lightly interfere with the view of the Procurator Fiscal.

4 Paragraph 27, Attorney General's Guidelines on Disclosure (2005)

5 CPIA Code of Practice, paragraph 3.5

Retrieval of video & CCTV evidence

Retrieval of video & CCTV evidence

Digital CCTV installations vary greatly in terms of the recording methods used and export functionality provided. The systems often do not allow quick and easy access to data in a suitable form by police investigators. This procedure is designed to enable police technical staff to select the most appropriate method for retrieving video from digital CCTV systems.

The guidance is aimed at video content investigators, rather than computer systems investigators, who are advised to refer to the relevant Digital Evidence Group guidelines. The key difference in approach is that this procedure is intended for those whose priority is to extract video sequences from PCs and Digital Video Recorders (DVRs), rather than to forensically examine the entire system.

The procedure is based around a flow chart which poses four fundamental questions in sequence:

- Is the request reasonable?
- Is the method possible?
- Is the method practical?
- Does the method lead to the creation of an evidential master copy?

On being confronted with an unfamiliar CCTV system, the first step is to determine which options for download are available. Then, it is important to select the method that is best suited to the volume of data required. The final stage is to produce a master copy of the video sequence.

The priority should be to extract data in its native file format and the flow chart only includes those techniques that enable this to be achieved. Options such as recording to tape via an analogue output or scan conversion of the VGA signal, are not included as they do not result in bit-for-bit copies of the original, as required in the Digital Imaging Procedure[6]. However, in circumstances where it is not possible or practical to extract the data in its native format, alternative methods may be justifiable. These other techniques will be covered in more detail in the second part of this guidance, which covers the production of working copies, where, in certain applications, a bit-for-bit copy is not essential or would prevent necessary processing from being undertaken.

Most of the techniques described are relatively straightforward and could be undertaken by a competent and experienced user of computers and DVRs.

The part of the procedure that deals with removal and replacement of hard drives, however, requires a higher level of competence and familiarisation with health and safety issues.

Download Checklist

There are certain procedures that should be followed whatever method is ultimately selected for downloading the data.

1. Contemporaneous notes should be kept, detailing the course of action taken, to provide an audit trail.
2. Note the make and model of the CCTV system and the number of cameras. Take photographs of the system if possible, particularly if the recorder is unfamiliar or the manufacturer uncertain.
3. Note the basic system settings (e.g. current record settings and display settings), so that, if changes have to be made to facilitate the download, it is then possible to return the system to its original state.
4. Time check – compare the time given by the speaking clock with that displayed by the CCTV system. Any error between the system time and real time should be noted and compensated for when carrying out the download. This will ensure that the correct section of data is copied.
5. Determine time period required in conjunction with Senior Investigating Officer (SIO), if this has not already been specified in the request.
6. Determine which cameras are required and whether they can be downloaded separately. Depending on the nature of the incident, there might, for example, be a requirement to archive all cameras with external views. Some systems enable video from individual cameras to be downloaded, but some do not, in which case data from all cameras will need to be taken. The decision taken, and the reasons for it, should be documented in the audit trail.
7. Check storage / overwrite time – to determine how long the relevant data will be retained on the system. This is particularly important if the download cannot be carried out immediately, or needs to be prioritised against other tasks.
8. The recording should not be stopped during the archiving process unless (a) this is an unavoidable feature of the system or (b) there is an immediate risk that important data will be overwritten, before it can be archived.
9. Protect data. Some systems offer the option of write-protecting a selected video sequence to prevent it from being overwritten before it can be archived. However, it should not be assumed that this facility will be present.
10. Confirm that the data can be archived in its native file format. It is preferable to extract the CCTV sequence in its native format in order to maintain image quality and provide best evidence, even where this file format is proprietary to the CCTV manufacturer. Some systems may provide an option to write the sequence to AVI file, which may seem to be an advantage, in that the video will be replayable using standard software. However, the generation of the AVI file often requires the video to be recompressed, resulting in a loss of quality, so this method should be avoided. Time and date information may also be lost, along with any stored bookmarks.
11. Replay software. Is the data format proprietary? If so, it is necessary to download a copy of the replay software alongside the data. Some CCTV systems provide this facility, but others do not and the software has to be obtained separately, e.g. from the manufacturer's website. It should be established that the facility exists to replay the data before leaving the scene and allowing the system recording to be overwritten.
12. Confirm success of download. The downloaded data should be checked before leaving the scene (or immediately on returning to the lab) to confirm that (a) the archiving process was successful and (b) that any associated replay software functions correctly. This check should be done on a machine other than the original recorder.
13. Restart the CCTV system (if necessary) and confirm in the presence of the owner/operator that it is operating as it was originally.
14. Complete evidence sheet. The following information should be included with the evidence to assist the investigator with subsequent replay and analysis:
    - Make and model (important when trying to identify suitable replay software, or hardware).
    - Error in display time and date.
    - Time period covered by download.
    - Include replay software if available.

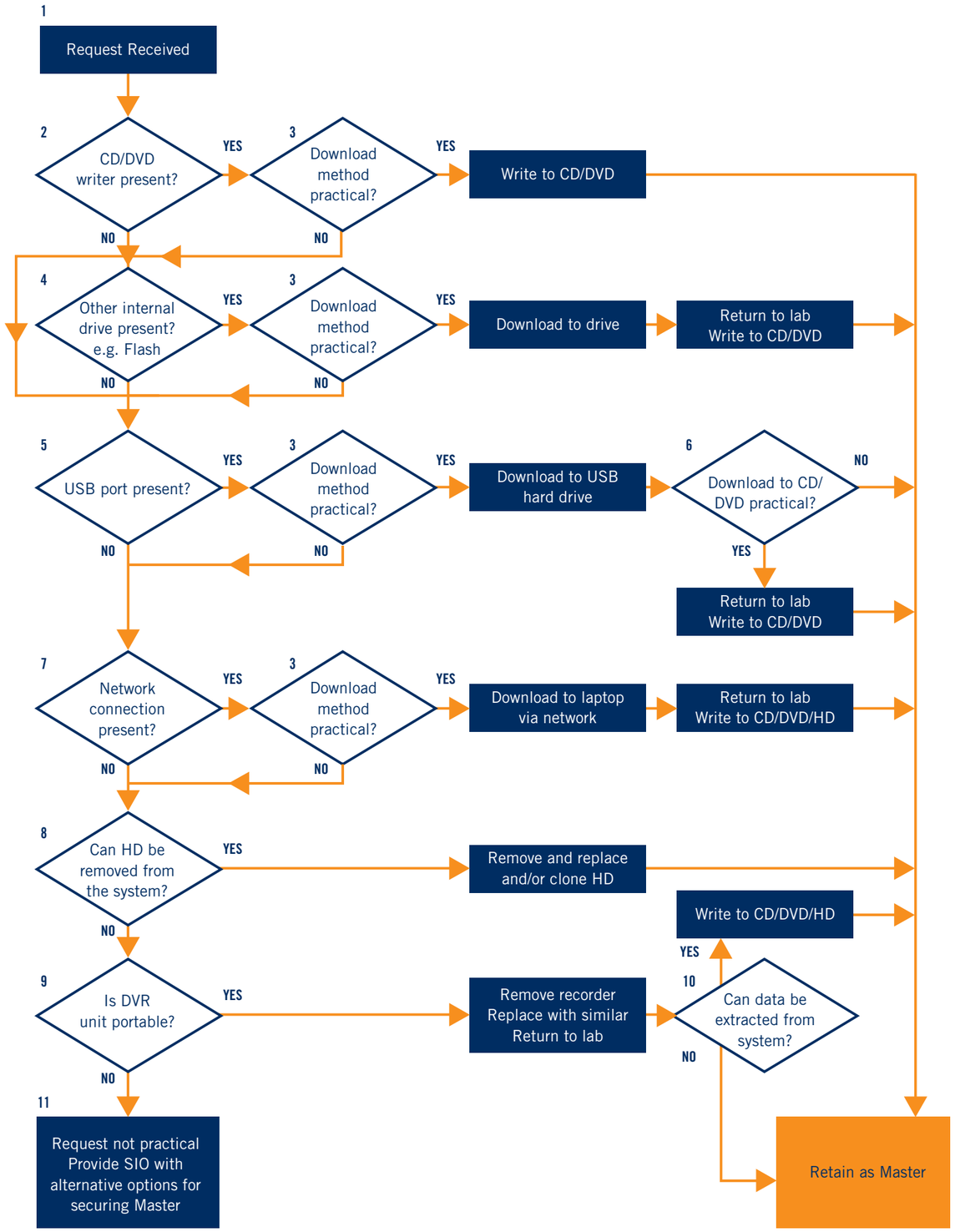
Equipment

Suggested field kit list for operational retrieval from digital CCTV systems:

- Laptop, with USB and network connectivity. A selection of proprietary replay software could be installed, to enable the downloaded data to be checked.
- External CD/DVD writer.
- USB hard drives (capacity 200GB+).
- Replacement hard disks (range of sizes 80-400GB).
- Network cables (crossover and patch).
- Replacement (loan) DVR units.
- Blank media, e.g. CD-R, DVD-R, DVD+R, DVD-RAM.
- Extension cables (e.g. 4-way power distribution cables).
- Analogue/digital video monitor.
- Digital camera – to record cabling and connections before disconnecting system.
- Tool kit (plus torch, mirror, pens and labels for cable marking).
- Appropriate forms for documenting the audit trail.

[6] Digital Imaging Procedure, PSDB Ref: 2 2006; J Aldridge

Download chart for digital CCTV



Retrieval of video & CCTV evidence (cont.)

Explanatory Notes for Chart

1. Request received

An initial assessment should be made to determine whether the request seems reasonable, i.e. whether the volume of data asked for is appropriate to the nature of the incident being investigated. If a general request has been submitted for all available video from a site, then an attempt should be made, in conjunction with the SIO, to narrow down the period of interest before starting the download.

It should also be confirmed that alternative routes for obtaining the data have already been explored before requesting technical support, i.e. has the owner been asked to undertake the download, or is help available from the installer or manufacturer of the CCTV system?

2. CD/DVD writer present

Many digital CCTV systems have a built-in CD/DVD writer for archiving data, in which case there should be an option within the CCTV software to facilitate the back-up of the selected video sequences (in the native file format). There may also be the option to include the replay software on the disk along with the data. Write-once disks should be used.

3. Assess practicality of download

The practicality of a particular export method is determined by the resource (e.g. staff hours), cost (e.g. media/hardware), time (e.g. data transfer time), and quality (e.g. WORM vs HD) implications for the volume of data to be retrieved. Before an export method is chosen, it should be assessed against each of the criteria to determine whether it is appropriate.

For example:

- Long sequences of video from multiple cameras may require an impractically large number of CDs for storage. The download process may also take several hours to complete. Archiving to a USB hard drive or via a network connection may be a more practical option than the use of a CD writer, as no regular changing of disks is required during the download process.
- It may be more time-efficient to replace the hard drives or remove the DVR and undertake the download in the laboratory, although this may be more expensive in replacement hardware/media cost.
- To assess whether archiving to CD is time-efficient for large downloads, the time taken to create one CD should be checked, and the percentage of the required video that fits on this disk noted. From this information, the total number of disks required and the total archiving time can be calculated.
- For other archiving methods such as via USB hard drive and network, the file transfer rate should be monitored and the total transfer time estimated.

4. Other internal drives present

If the facility exists to back-up data to memory cards/ sticks such as compact flash, this may be utilised for extracting short video sequences. The storage capacity for compact flash is approximately the same as a CD (albeit increasing with time) and therefore similar problems may be encountered if archiving large volumes of data.

Memory cards are not the ideal medium for storing master copies, as cards are more expensive than CDs and drives are less common so are likely to provide difficulties in accessing data for playback. Thus, if a memory card is used to extract data from a CCTV recorder, it is recommended that this is used as a transport medium only and the data files are then copied to the master medium e.g. CD/DVD.

5. USB (or other external) hard drive

Archiving to USB hard drive may be the preferred option in several scenarios, for example:

- For downloading smaller quantities of data where there is no other easy option (e.g. CD writer). The USB drive in this case is just a transport medium and the data may then be copied to DVD/CD later, at the lab, to make the master copy.
- For downloading large quantities of data, where it is quicker or more practical than writing to several CDs. When copying large quantities of data, it may be more efficient to exit the CCTV system software (which may be possible on a PC Windows-based system) and copy the required files directly using Windows Explorer. This may also be necessary if the CCTV software does not recognise the addition of the USB device and consequently offers no suitable menu option.

6. Data Transfer

Where a USB hard drive has been used to archive the data at the premises, either for convenience or out of necessity, it is suggested that a master copy is then made from this on a write-once medium such as CD-R/DVD-R. This is also more cost-effective than retaining the USB drive permanently as evidence. The USB drive can then be wiped and reused.

If very large volumes of data have been extracted (several tens of GB), it may be deemed impractical to archive to CD/DVD, in which case a decision could be made to retain the USB drive as the master.

7. Network connection

Where CCTV software provides for network connectivity, a laptop could be linked to the system and IP address specified to allow transfer of data to a back-up medium.

With a PC-based CCTV system, it may be possible to exit from the CCTV software and create a connection to a laptop via Windows. Video data can be downloaded to the hard disk on the laptop or to a USB hard drive connected to it and a master copy then created from this on an appropriate medium.

Some systems may provide a remote network connection for off-site monitoring or download. Before using this facility, the network speed should be checked and it should be confirmed that the transmitted video is of the same quality as that which is stored locally.

8. Replace Hard Drives

This can be a quick method for extracting large volumes of data from a system. The recorder may be equipped with a removable hard drive in a caddy, or the casing of the unit may need to be opened and the storage drives extracted and replaced. Depending on the system, the disk could be replaced with a blank (the quickest option) or a clone could be taken and the original disk replaced.

There are several risks with this approach, however, and it should only be attempted with caution, by an experienced engineer.

- It should first be clearly established that it will be possible to replay the data from this hard drive in the laboratory. A DVR may have a fully removable hard drive for storing data, but this drive may not be compatible with anything other than the original recorder.
- Where the casing of the DVR needs to be removed to access the drive, care must be taken to follow appropriate health and safety procedures, particularly with regard to potential exposure to electricity. The possibility of invalidating the manufacturer's warranty or damaging the storage media by undertaking this procedure also needs to be considered.
- A hard disk removed from a stand alone DVR may not be in Windows compatible format and therefore the data files will not be accessible via connection to a PC. It may be possible to replay the data from the hard disk by fitting the disk to another similar CCTV recorder (e.g. if there is a unit in stock from a previous job) but, in the worst case scenario, the hard drive will be locked to a specific CCTV recorder and will only play on that one machine.
- The data drive may appear to be in a removable caddy and thus easy to extract. However, there may be a second data drive within the DVR, which is only accessible by removing the case.
- The DVR may not recognise any replacement drive fitted, even a clone of the original. If this is the case, there may be no option but to take the whole CCTV recording unit.

9. Remove whole recording unit

In circumstances where all other download options have been rejected as impractical or impossible, the decision may be made to remove the recorder, assuming that it is physically possible to do so and that the severity of the incident justifies this course of action. However, the implications (legal, insurance etc.) of removal should be considered and a decision taken as to whether a replacement recorder should be provided, or other arrangements made in order to maintain security at the premises.

Where the volume of data required is very large, it may be time-efficient to remove the recorder, rather than wait at the site for a download to complete. Alternatively, for some poorly designed systems, there may no straightforward method for extracting the required video (e.g. no CD writer or data output ports and a hard disk that cannot be replayed in another machine). In this scenario, it may be necessary to take the recorder and retain the unit as evidence.

10. Extracting data from portable recorders

If a DVR unit has been removed from the premises because it was more time efficient to do so than to wait while the video was downloaded, then the data should be archived to CD/DVD on returning to the lab. For those systems where it is impossible to extract the data in a replayable format, the DVR unit itself may need to be retained as evidence.

11. Refer back to SIO

Where it is impractical or not economically viable to download the required data and the CCTV recorder is too large or complex to be removed, the request should be referred back to the SIO for a policy decision.

The SIO should be presented with alternative options to enable data to be retrieved. For example:

- It may be possible to reduce the volume of data required by reconsidering the time period of interest or the number of cameras needed. By reducing the volume of data, it may then be possible to use some of the methods that had previously been rejected.
- It may at this stage be necessary to consider using other techniques such as recording of the system analogue output or scan conversion, which does not provide a bit-for-bit copy of the original data, but which may be the only practical way of recovering video evidence from the system.

Guide for mobile phone seizure & examination

Guide for mobile phone seizure & examination

This document is intended to describe how generic digital evidence principles apply in the field of mobile phone forensics. The four ACPO Principles of Digital Evidence are presented and discussed in turn, both in terms of the implication on the personnel involved in seizing mobile devices and also the implications for those examining such devices.

To recap, the four ACPO Principles are as follows:

Principle 1:

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

Principle 2:

In circumstances where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to give evidence explaining the relevance and 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.

Principle 1

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

Seizure / Preservation of Evidence

Principle 1 has the following implications for personnel involved in the seizure of mobile phones.

Isolate device from network - this may be achieved by one of the following techniques:

Turn device off at the point of seizure

Authentication codes (e.g. SIM PIN and/or handset security codes) may be required to regain access to the device and data. This may delay examination. In circumstances where delay is unacceptable, such as life at risk, specialist advice should be sought. In the case of some overseas service providers PUKs may never be available.

If the device is left on, changes MAY occur to content which would be undesirable (scheduled scripts etc.)

Place device in shielded container/bag

Battery life will be reduced due to power increase as handset tries to connect to network. Therefore, immediate delivery to examination unit is required.

For devices that have volatile memory, consideration should be given to charging the device at appropriate intervals to ensure that data is not lost.

Examination

Principle 1 has the following implications for personnel involved in the examination of mobile phones.

Isolate device from network - this may be achieved by one of the following techniques:

- **Use a jamming device - NOT RECOMMENDED**

  Such devices are illegal in many countries. Use of such a device may also interfere with network coverage outside of the examination area.

- **Use a shielded room - RECOMMENDED**

  For a fixed room, cost is relatively high and examinations tied to specific location (i.e. reduced mobility).

  "Faraday tents" are a cheaper and portable solution but are likely to be less secure than a fixed room (and cables cannot be fed into the tent as they will act as antennae).

  Battery life will be reduced due to power increase as handset tries to connect to network - device should be fully charged prior to examination.

- Use a shielded container/box

  This may allow examinations to be conducted safely at different geographic locations.

  Battery life will be reduced due to power increase, as handset tries to connect to network.

As such, the device should be fully charged prior to examination or a portable power source attached to the device within the enclosure.

Cables into the box must be fully shielded to prevent intrusion by network signals.

- Use an "access card" type SIM that will mimic the identity of the original SIM card and will not allow network access

  This does allow examinations to be conducted safely at different geographic locations.

  Such cards need to be configured with the exact subscriber/card identity to "fool" the handset into thinking that the original SIM is present. Although the user data is preserved, there is a possibility that other data on the handset may be lost or changed as a result of such a card being inserted.

- Request that service provider disable the subscriber account

  This would require intervention by the service provider who may not be willing to co-operate.

  Such an approach has not been thoroughly tested and the effects on the handset and SIM are not fully understood at the time of writing. Therefore, this is not a recommended approach at this time, however, if the subscriber account is disabled, any voicemail held on the system for that account may be lost.

Use software which is designed for forensic use wherever possible

Most tools acquire data via requests to the operating system therefore 2-way data transfer is inevitable.

The Device may not be supported by a forensic tool only by a handset manager type product.

If using non-forensic tools:

- they should be tested in safe environment with same make/model of device prior to use on actual exhibit so that their operation / effects are understood.
- they should be used as late as possible in the examination process.

Use a secure reliable connection interface which minimises data change on the device

Check cable is secure, generally reliable and has least impact on handset. Infra red is less secure, less reliable and will normally require interaction on the exhibit to activate.

Bluetooth is currently the least secure of the choices of interface and data will typically be written to the handset during the activation / authentication process.

When using Bluetooth be aware that there is a risk of infection of the examining computer equipment by a software virus which may compromise current and subsequent examinations.

Cable is the preferred interface, followed by infra-red then Bluetooth then WiFi.

WiFi interfaces may be available in the near future and will require evaluation at that time to assess their suitability.

Examiners should accept that the process of reading some data types will affect their state

For example, retrieving un-read SMS messages via the handset may result in their status changing to "Read". This may be unavoidable but should be logged. Subsequent examinations may therefore produce different results.

Plan the examination process to avoid the loss of data which is very important to the case

Sequence of Examination (i.e. handset vs.SIM) will depend upon a number of factors and the decision may lead to data loss. The decision on sequence will depend to some extent upon case specifics (e.g. importance of date and times), as well as the examination environment and tools available.

Removing the SIM typically requires battery removal which MAY lead to loss of time and date information.

Allowing the battery to become completely discharged may also result in the loss of date and time information. Therefore, provision should be made for early (and maybe repeated) charging to minimise this risk.

Turning the handset on with the original SIM card present may lead to changes of data on the SIM card (e.g. Location Area Information).

The sequence of examination should also take into account the consequences if any forensic tools that introduce agents are used. These violate Principle 1 and the examiner must assess the impact it may have on the integrity of any evidential data and record the decision to use such software.

Inserting a different SIM into a handset will, in most cases, result in the deletion or hiding of user data (e.g. call registers). As such, this practice should be avoided.

If the handset is on, the authentication codes may be active (e.g. PIN lock on SIM and/or handset security codes) and hence handset-first examination may be preferable (otherwise entire examination is delayed).

All examinations should include some degree of manual examination (i.e. navigating through the menu structure of the phone and capturing the contents of the screen display)

The device may not be supported by tools hence manual examination may be the only option for data acquisition.

Even if the device is supported by tools, manual examination should be conducted to verify results and ensure completeness of download.

Examiners should familiarise themselves with the operation of a device prior to examination (e.g. download of user manual, practice with same make/model).

Specifically, the examiner should identify buttons which may result in changes to user data (e.g. the green "Send" button) and which button(s) will cancel an operation and return to the main menu (e.g. the red "End" button).

Exercise care when dealing with access PINs/passwords to avoid permanent damage to the device

The first step for SIM cards should be to check the number of remaining attempts for PIN & PUK using a forensic tool.

It may be appropriate to "try" the PIN based on service provider defaults etc. in order to avoid the delay in receiving the PUK from the service provider.

Three attempts can be made to enter the correct PIN. However, one PIN attempt should always be left in case the PIN is provided by owner or some other means.

The PUK should NEVER be guessed as ten incorrect entries will result in the contents of the SIM card being forever irretrievable.

Principle 2

In circumstances where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.

Seizure / Preservation of Evidence

Principle 2 has the following implications for personnel involved in the seizure of mobile phones.

Ensure that seizing personnel are trained to deal with mobile devices and are equipped with appropriate packaging materials.

Seizing personnel should be aware that mobile devices may have the ability to wipe data and hence any manual interaction with the device should be minimised. Although this is not currently common, it is likely that destructive tools/scripts will appear in the way as they have with PCs.

Examination

Principle 2 has the following implications for personnel involved in the examination of mobile phones:

Ensure that examiners have received relevant and current training in the tools and procedures that they will use.

Before undertaking real case work, an examiner should have prior and recent experience of examining a device of similar functionality with the tool(s)/process to be used.

This is particularly relevant if using non-forensic tools which may synchronise the device and PC and possibly cause changes to the evidence stored on the device.

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.

Seizure / Preservation of Evidence

Principle 3 has the following implications for personnel involved in the seizure of mobile phones.

Make appropriate use of photography and/or video to record the status of the exhibit.

Consideration should be given to photographing the scene at which the device was seized.

The status of the exhibit at the point of seizure should be recorded. Any on-screen information should be noted and/or photographed.

Examination

Principle 3 has the following implications for personnel involved in the examination of mobile phones.

Ensure that a log of actions taken with the exhibit is maintained

Any changes to the data which occur during the examination should be noted (e.g. accidental changes during manual examination, arrival of incoming messages etc.)

Consideration should be given to recording results of the examination (e.g. photography or video) for inclusion within final reports. This is particularly relevant for manual examinations.

Even for automated downloads, photographs can be used to indicate the condition of the exhibit and to provide a record of certain key information (e.g. numbers of contacts in the phonebook, numbers of SMS messages etc.), such that the results of forensic tools can be validated.

The details of tools and products used (including version numbers) should be recorded.

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.

Seizure / Preservation of Evidence

Principle 4 has the following implications for personnel involved in the seizure of mobile phones.

The investigating officer should ensure that personnel involved in seizing mobile devices are appropriately trained.

Examination

Establish effective communication between the examiner(s) and the investigating officer.

Only the investigating officer can fully understand the importance or relevance of specific data held on the device.

In some situations, the most suitable examination process may result in the loss of specific data (e.g. date and time from battery removal). The examiner cannot fully appreciate the importance or relevance of such information without guidance from the investigating officer.

Clear and open dialogue between the examiner and investigating officer is required to ensure that data which is critical to the case is not lost.

The examiner should recommend an examination strategy which is appropriate to the nature of the case and explain the implications of this to the investigating officer

At the basic level, standard forensic tools should retrieve active handset and SIM data (i.e. what can be viewed via the handset by the user). In addition, deleted SMS messages can be retrieved from the SIM.

At an intermediate level, the use of flash dump techniques may be able to recover deleted and other useful handset data, but requires specialist hardware and expertise.

At the most advanced level, physical removal of memory chips is possible, but requires very specialist hardware and expertise. Such techniques may be able to recover deleted handset data (possibly over and above that from flash dumps).

Other considerations

The following issues should also be considered when dealing with mobile phone exhibits.

The examination should take into consideration any requirements to preserve other forensic evidence (DNA, fingerprints, firearms, narcotics)

The sequence of examination is critical (e.g. fingerprint retrieval techniques may result in the handset being unusable).

Examining a handset, without taking appropriate precautions, might destroy vital fingerprint or DNA evidence.

Seizing personnel should aim to take any other material and equipment related to the device

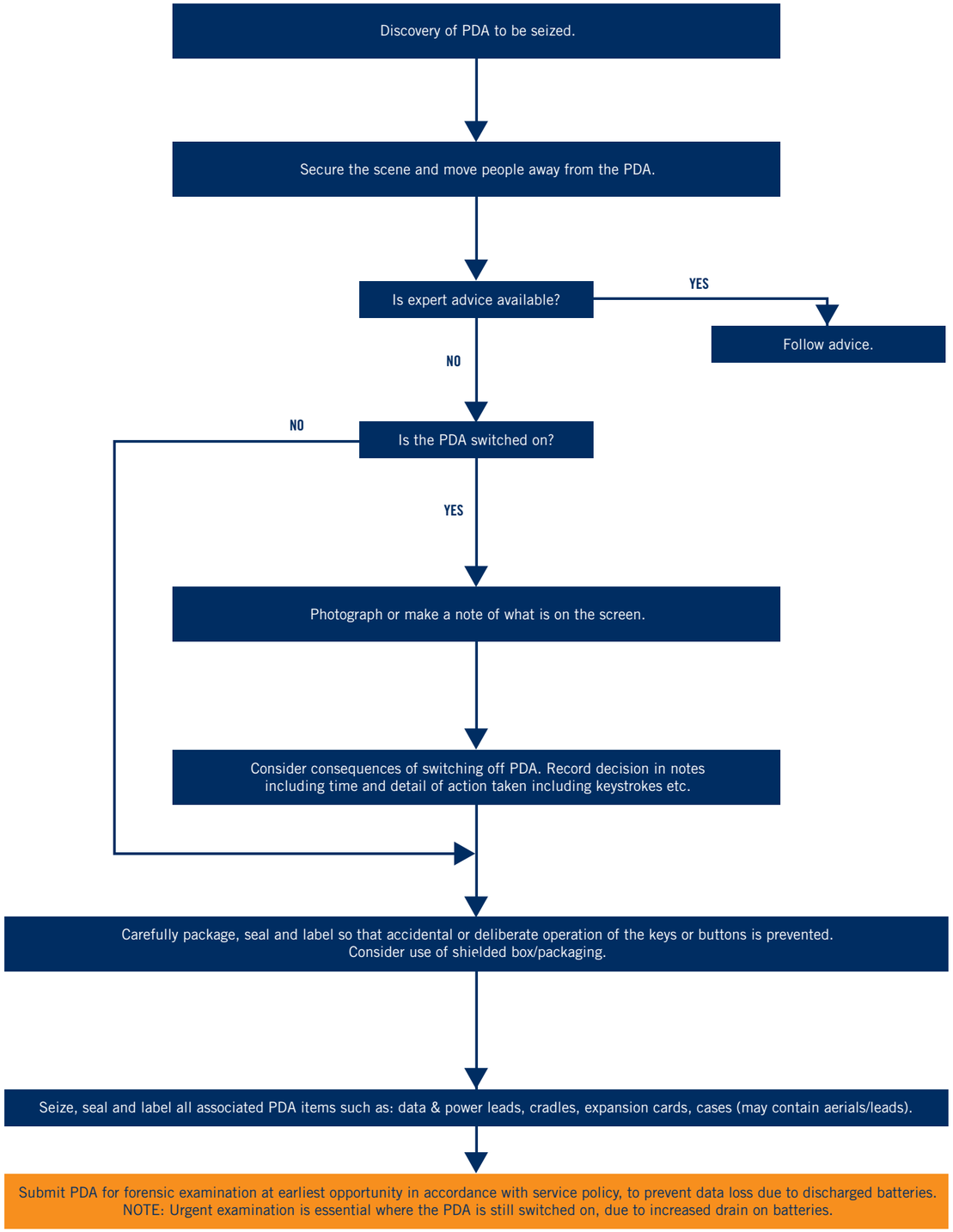
Cables, chargers, packaging, removable media cards, manuals, phone bills etc. may assist the enquiry and minimise the delays in any examination.

Packaging materials and associated paperwork may be a good source of PIN / PUK details.

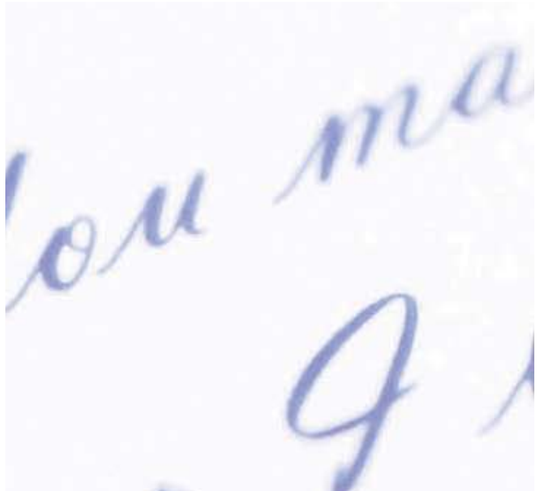
Consideration should be given to seizing PC equipment that may have been used to synchronise or otherwise connect to the handset.

Finally, be aware that some handsets may have automatic housekeeping functions, which clear data after a number of days. For example, some Symbian phones start clearing call/event logs after 30 days, or any other user defined period.

Seizure of personal digital assistants



Initial contact with victims: suggested questions



Initial contact with victims: suggested questions

Internet related evidence is volatile and action needs to be taken to preserve it as soon as possible. Any delay will result in loss of evidence. Always ask for any passwords that you consider may be relevant.

E-mail related crimes

Ask the victim/complainant:

- Do you have the e-mail address of the person who sent the email, including the "reply to" element?
- Did you save the e-mail in your computer? If so, request a copy on floppy disk, CD or USB Flash Disk – including the extended headers (at the top or bottom of the message - see Glossary). Or, if not, do you have a printed copy of the e-mail?
- Is your e-mail software or web based?

Website related crimes

Ask the victim/complainant:

- What exactly happened?
- What is the website(s) address?
- Who is your Internet Service Provider?
- Do you have a copy of the web page you visited?
- What was the date and time you visited the website? (note the time zone)

Chat room (IRC) related crime

Ask the victim/complainant:

- Who is your Internet Service Provider (ISP)?
- What is the chat channel name?
- Who is the chat channel operator?
- What is the name of the server?
- What is the offending party's nickname and what is your nickname?
- Did you save a copy of the conversation in your computer? If so, request copy of it on floppy disk, CD or USB Flash Disk.
- If not, did you save a printed version of it?

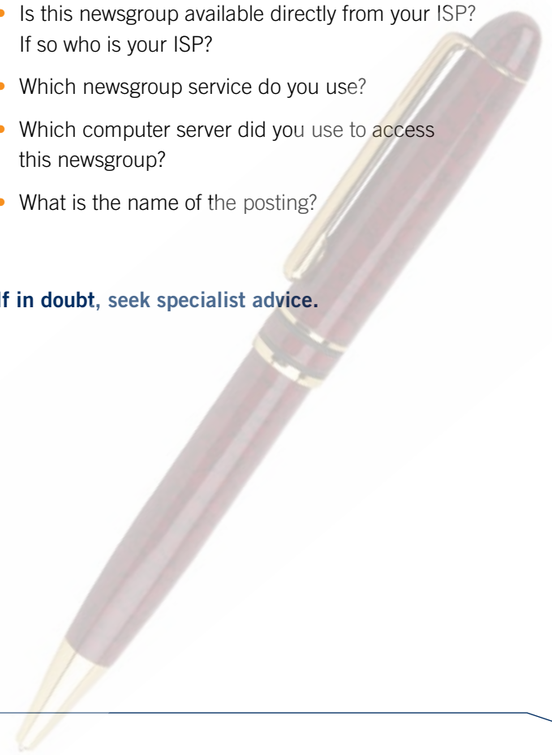
Internet service provider (ISP) chat related crimes

- Who is your Internet Service Provider?
- What is the chat room's name?
- What is the offending party's nickname?
- Did the chat room have an operator or moderator? If so what name did they use?
- Did you save a copy of the conversation in your computer? If so, request a digital copy of it.
- If not, did you save a printed version of it?

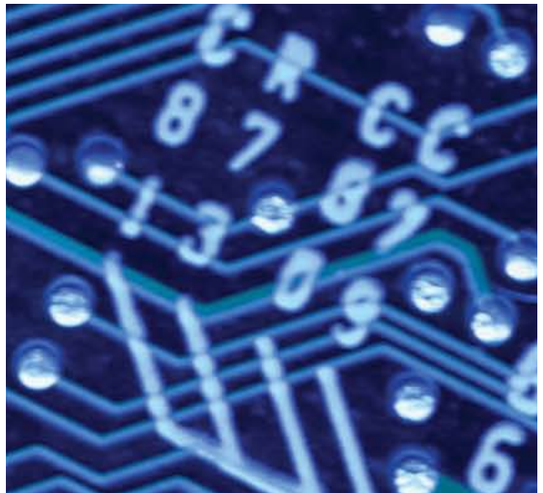
Newsgroup related crimes

- What is the name of the newsgroup?
- Do you access newsgroups via software or through a website?
- Did you save the posting in your computer? If so, can I have a copy of it on floppy disk, CD or USB Flash Disk? If not, have you got a printed copy of the posting?
- Is this newsgroup available directly from your ISP? If so who is your ISP?
- Which newsgroup service do you use?
- Which computer server did you use to access this newsgroup?
- What is the name of the posting?

If in doubt, seek specialist advice.



Glossary & explanation of terms



Glossary & explanation of terms

ADDRESS
The term address is used in several ways.

- An Internet address or Internet Protocol (IP) address is a unique computer (host) location on the Internet.
- A Web page address is expressed as the defining directory path to the file on a particular server.
- A Web page address is also called a Uniform Resource Locator, or URL.
- An e-mail address is the location of an e-mail user (expressed by the user's e-mail name followed by an "at" sign (@) followed by the user's server domain name).

ARCHIVE FILE
A file that contains other files (usually compressed files). It is used to store files that are not used often or files that may be downloaded from a file library by Internet users.

BACKUP
A copy taken of information held on a computer in case something goes wrong with the original copy.

BIOS
Basic Input Output System. A program stored on the motherboard that controls interaction between the various components of the computer.

BOOT
To start a computer, more frequently used as "re-boot".

BOOT DISK
Refers to a disk that contains the files needed to start an operating system.

BROADBAND
A high bandwith internet connection e.g. ADSL or cable.

BUFFER
An area of memory used to speed up access to devices. It is used for temporary storage of the data read from or waiting to be sent to a device such as a hard disk, CD-ROM, printer or tape drive.

BULLETIN BOARD SERVICE (BBS)
A BBS is like an electronic corkboard. It is a computer system equipped for network access that serves as an information and message-passing centre for remote users. BBSs are generally focused on special interests, such as science fiction, movies, Windows software, or Macintosh systems. Some are free, some are fee-based access and some are a combination.

BYTE
In most computer systems, a byte is a unit of data consisting of 8 bits. A byte can represent a single character, such as a letter, a digit, or a punctuation mark.

CACHE
A cache (pronounced CASH) is a place to store something more or less temporarily. Pages you browse to are stored in your web browser's cache directory on your hard disk. When you return to a page you have recently browsed to, the browser can retrieve the page from the cache rather than the original server, saving you time and the network the burden of some additional traffic. Two common types of cache are cache memory and a disk cache.

CDF
Channel Data Format: a system used to prepare information for Web-casting.

CD-R
Compact Disk – Recordable. A disk to which data can be written but not erased.

CD-ROM
Compact Disk – Read Only Memory or Media. In computers, CD-ROM technology is a format and system for recording, storing, and retrieving electronic information on a compact disk that is read using laser optics rather than magnetic means.

CD-RW
Compact Disk – ReWritable. A disk to which data can be written and erased.

CMOS
Complementary Metal-Oxide Semi-Conductor. It commonly holds the BIOS preference of the computer through power off with the aid of a battery.

CPU
Central Processing Unit. The most powerful chip in the computer. Located inside a computer, it is the "brain" that performs all arithmetic, logic and control functions.

CRACKER
A computer expert who uses his or her skill to break into computer systems by circumventing security measures (cracking). The term was coined to provide an alternative to using the word 'hacker' to mean this, although the common usage remains more popular.

CRC
Cyclic Redundancy Check. A common technique for detecting data transmission errors.

CRYPTOGRAPHY
The process of securing private information that is sent through public networks, by encrypting it in a way that makes it unreadable to anyone except the person or persons holding the mathematical key/knowledge to decrypt the information.

DATABASE
Structured collection of data that can be accessed in many ways. Common database programs are: Dbase, Paradox, Access. Uses: various including – address links, invoicing information, etc.

DELETED FILES
If a subject knows there are incriminating files on the computer, he or she may delete them in an effort to eliminate evidence. Many computer users think that this actually eliminates the information. However, depending on how the files are deleted, in many instances a forensic examiner is able to recover all or part of the original data.

DENIAL OF SERVICE ATTACKS (DOS)
Denial of Service Attacks are attempts to make a computer resource unavailable to its intended users. e.g. a web site is flooded with requests, which ties up the system and denies access to legitimate users.

DIGITAL SIGNATURE
Use of cryptography to provide authentication of the associated input, or message.

DISK CACHE
A portion of memory set aside for temporarily holding information read from a disk.

DISK SPACE
Disk storage. The space on the web hosting a company's server/computers that a website's content is allowed to utilise.

DONGLE
A term for a small external hardware device that connects to a computer to authenticate a piece of software; e.g. proof that a computer actually has a licence for the software being used.

DVD
Digital Versatile Disk. Similar in appearance to a compact disk, but can store larger amounts of data.

ENCRYPTION
The process of scrambling, or encoding, information in an effort to guarantee that only the intended recipient can read the information.

E-MAIL HEADER
E-mails come in two parts – the body and the header. Normal header information gives the recipient details of time, date, sender and subject. All e-mails also come with (usually hidden) extended headers – information that is added by email programs and transmitting devices – which shows more information about the sender that is in many circumstances traceable to an individual computer on the Internet.

FREE SPACE
File clusters that are not currently used for the storage of 'live' files, but which may contain data which has been 'deleted' by the operating system. In such cases, whole or part files may be recoverable unless the user has used specialist disk cleaning software.

FLOPPY DISK
These are disks that hold information magnetically. They come in two main types 3.5 inch and 5.25 inch. The 5.25 inch disks are flexible and easily damaged, the 3.5 inch disks are in a stiff case. Both are square and flat. Older machines may use larger or smaller sizes of disk.

GIGABYTE (GB)
1 Gigabyte = 1024 Megabytes. A gigabyte is a measure of memory capacity and is roughly one thousand megabytes or a billion bytes. It is pronounced Gig-a-bite (with hard Gs).

HACKER
Persons who are experts with computer systems and software and enjoy pushing the limits of software or hardware. To the public and the media, they can be good or bad. Some hackers come up with good ideas this way and share their ideas with others to make computing more efficient. However, some hackers intentionally use their expertise for malicious purposes, (e.g. to circumvent security and commit computer crimes) and are known as 'black hat' hackers. Also see Cracker.

HARD DISK
The hard disk is usually inside the PC. It stores information in the same way as floppy disks but can hold far more of it.

HARDWARE
The physical parts of a computer. If it can be picked up it is hardware as opposed to software.

HOST MACHINE
For the purpose of this document, a host machine is one which is used to accept a target hard drive for the purpose of forensically processing.

HUB
A central connection for all the computers in a network, which is usually Ethernet-based. Information sent to the hub can flow to any other computer on the network.

IMAGING
Imaging is the process used to obtain all of the data present on a storage media (e.g. hard disk), whether it is active data or data in free space, in such a way as to allow it to be examined as if it were the original data.

IMEI
International Mobile Equipment Identifier.

A unique 15-digit number that serves as the serial number of a GSM handset.

IMSI
International Mobile Subscriber Identity.

A globally unique code number that identifies a Global System for Mobiles (GSM) handset subscriber to the network.

Glossary & explanation of terms (cont.)

INTERNET RELAY CHAT
A virtual meeting place where people from all over the world can meet and talk about a diversity of human interests, ideas and issues. Participants are able to take part in group discussions on one of the many thousands of IRC channels, or just talk in private to family or friends, wherever they are in the world.

ISP
Internet Service Provider. A company that sells access to the Internet via telephone or cable line to your home or office. This will normally be free - where the user pays for the telephone charge of a local call - or by subscription - where a set monthly fee is paid and the calls are either free or at a minimal cost.

JAZ DISK
A high capacity proprietary removable hard disk system from a company named Iomega.

KILOBYTE (KB)
1 Kilobyte = 1024 bytes.

LINUX
An operating system popular with enthusiasts and used by some businesses.

MACRO VIRUS
A virus attached to instructions (called macros) which are executed automatically when a document is opened.

MAGNETIC MEDIA
A disk, tape, cartridge, diskette or cassette that is used to store data magnetically.

MD5 HASH
An algorithm created in 1991 by Professor Ronald Rivest that is used to create digital fingerprints of storage media, such as a computer hard drive. When this algorithm is applied to a hard drive, it creates a unique value. Changing the data on the disk in any way will change the MD5 value.

MEGABYTE (MB)
1 Megabyte = 1024 Kilobytes.

MEMORY
Often used as a shorter synonym for random access memory (RAM). Memory is the electronic holding place for instructions and data that a computer's microprocessor can reach quickly. RAM is located on one or more microchips installed in a computer.

MODEM
Modulator / Demodulator. A device that connects a computer to a data transmission line (typically a telephone line). Most people use modems that transfer data at speeds ranging from 1200 bits per second (bps) to 56 Kbps. There are also modems providing higher speeds and supporting other media. These are used for special purposes - for example to connect a large local network to its network provider over a leased line.

MONITOR
A device on which the computer displays information.

MOUSE
Device that, when moved, relays speed and direction to the computer, usually moving a desktop pointer on the screen.

MS-DOS
Microsoft Disk Operating System. Operating system marketed by Microsoft. This was once the most common operating system in use on desktop PCs, which automatically loads into the computer memory in the act of switching the computer on. Often only referred to as DOS.

OPERATING SYSTEM
This software is usually loaded into the computer memory upon switching the machine on and is a prerequisite for the operation of any other software. Examples include the Microsoft Windows family of operating systems (including 3.x, NT, 2000, XP and Vista) and UNIX operating systems and their variants like Linux, HP-UX, Solaris and Apple's Mac OSX and BSD.

ORB
A high capacity removable hard disk system. ORB drives use magnetoresistive (MR) read/write head technology.

PASSWORD
A word, phrase or combination of keystrokes used as a security measure to limit access to computers or software.

PCMCIA CARDS
Similar in size to credit cards, but thicker. These cards are inserted into slots in a Laptop or Palmtop computer and provide many functions not normally available to the machine (modems, adapters, hard disks, etc.)

PERSONAL COMPUTER (PC)
A term commonly used to describe IBM & compatible computers. The term can describe any computer useable by one person at a time.

PERSONAL ORGANISER or Personal Digital Assistant
(PDA) These are pocket-sized machines usually holding phone and address lists and diaries. They often also contain other information. Modern PDAs take many forms and may best be described as a convergent device capable of carrying out the functions of a multitude of devices.

PIRATE SOFTWARE
Software that has been illegally copied.

PORT
The word port has three meanings:

- Where information goes into or out of a computer, e.g. the serial port on a personal computer is where a modem would be connected.
- In the TCP and UDP protocols used in computer networking, a port is a number present in the header of a data packet. Ports are typically used to map data to a particular process running on a computer. For example, port 25 is commonly associated with SMTP, port 80 with HTTP and port 443 with HTTPS.
- It also refers to translating a piece of software to bring it from one type of computer system to another, e.g. to translate a window programme so that it will run on a Macintosh.

PUBLIC DOMAIN SOFTWARE
Any programme that is not copyrighted.

PUK
Personal Unblock Key. PUK is the code to unlock a GSM SIM card that has disabled itself after an incorrect PIN was entered three times in a row.

QUERY
To search or ask. In particular, to request information in a search engine, index directory or database.

RAM
Random Access Memory is a computer's short-term memory. It provides working space for the PC to work with data at high speeds. Information stored in the RAM is lost when the PC is turned off ('volatile data').

REMOVABLE MEDIA
Items e.g. floppy disks, CDs, DVDs, cartridges, tapes that store data and can be easily removed.

REMOVABLE MEDIA CARDS
Small-sized data storage media which are more commonly found in other digital devices such as cameras, PDAs (Personal Digital Assistants) and music players. They can also be used for the storage of normal data files, which can be accessed and written to by computers.

There are a number of these including –

Smartmedia Card	SD Expansion Card
Ultra Compact Flash	Compact Flash
Multimedia Card	Memory Stick

The cards are non-volatile – they retain their data when power to their device is stopped – and they can be exchanged between devices.

SHAREWARE
Software that is distributed free on a trial basis with the understanding that, if it is used beyond the trial period, the user will pay. Some shareware versions are programmed with a built-in expiration date.

SIM
Subscriber Identity Module. A Smart Card which is inserted into a cellular phone, identifying the user account to the network and providing storage for data.

SLACK SPACE
The unused space in a disk cluster. The DOS and Windows file systems use fixed-size clusters. Even if the actual data being stored requires less storage than the cluster size, an entire cluster is reserved for the file. The unused space is called the slack space.

SMARTCARD
Plastic cards, typically with an electronic chip embedded, that contain electronic value tokens. Such value is disposable at both physical retail outlets and on-line shopping locations.

SOFTWARE
The pre-written programs designed to assist in the performance of a specific task, such as network management, web development, file management, word processing, accounting or inventory management.

SWITCH
A typically a small, flat box with 4 to 8 Ethernet ports. These ports can connect to computers, cable or DSL modems, and other switches. A switch directs network communications between specific systems on the network as opposed to broadcasting information to all networked connections.

SYSTEM UNIT
Usually the largest part of a PC, the system unit is a box that contains the major components. It usually has the drives at the front and the ports for connecting the keyboard, mouse, printer and other devices at the back.

TAPE
A long strip of magnetic coated plastic. Usually held in cartridges (looking similar to video, audio or camcorder tapes), but can also be held on spools (like reel to reel audio tape). Used to record computer data, usually a backup of the information on the computer.

TROJAN HORSE
A computer program that hides or disguises another program. The victim starts what he or she thinks is a safe program and instead willingly accepts something also designed to do harm to the system on which it runs.

UNIX
A very popular operating system. Used mainly on larger, multi-user systems.

USB STORAGE DEVICES
Small storage devices accessed using a computer's USB ports, that allow the storage of large volumes of data files and which can be easily removed, transported – and concealed. They are

about the size of a car key or highlighter pen, and can even be worn around the neck on a lanyard. They now come in many forms and may look like something entirely different such as a watch or a Swiss Army knife.

USIM
An enhancement of the Subscriber Identity Module (SIM) card designed to be used in Third Generation (3G) networks.

VIDEO BACKER
A program that allows computer data to be backed up to standard video. When viewed, the data is presented as a series of dots and dashes.

VIRUS
A computer virus is a computer program that can copy itself and infect a computer without permission (and often without knowledge) of the user. A virus can only spread from one computer to another when its host is taken to the uninfected computer, for instance by a user sending it over a network or carrying it on a removable medium such as a floppy disk, CD, or USB drive. Additionally, viruses can spread to other computers by infecting files on a network file system or a file system that is accessed by another computer. Some are harmless (messages on the screen etc.), whilst others are destructive (e.g. Loss or corruption of information).

VIRTUAL STORAGE
A 'third party' storage facility on the internet, enabling data to be stored and retrieved from any browser. Examples include Xdrive and Freeway.com.

WINDOWS
Operating system marketed by Microsoft. In use on desktop PCs, the system automatically loads into the computer's memory in the act of switching the computer on. MS-DOS, Windows, Windows 3.0, Windows 95, Windows 98, Office XP, Windows XP, Windows NT, Windows Vista and Windows Server are registered trademarks of Microsoft Corporation.

WORD PROCESSOR
Used for typing letters, reports and documents. Common Word Processing programs: Wordstar, Wordperfect and MS-Word.

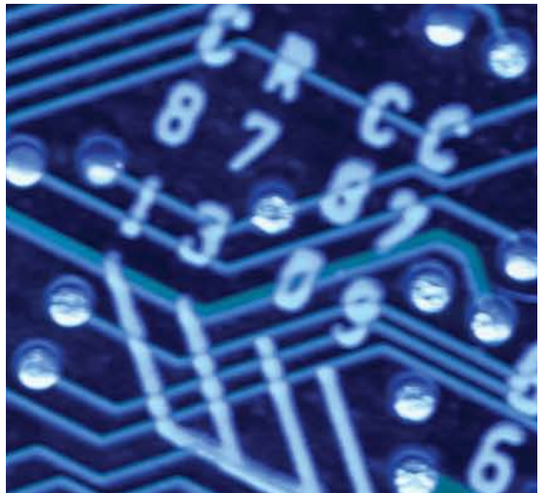
WORM
Like a virus but is capable of moving from computer to computer over a network without being carried by another program and without the need for any human interaction to do so.

WIRELESS NETWORK CARD
An expansion card present in a computer that allows cordless connection between that computer and other devices on a computer network. This replaces the traditional network cables. The card communicates by radio signals to other devices present on the network.

ZIP DRIVE/DISK
A proprietary 3.5-inch removable disk drive produced by Iomega. The drive is bundled with software that can catalogue disks and lock files for security.

ZIP
A popular data compression format. Files that have been compressed with the ZIP format are called ZIP files and usually end with a .ZIP extension.

Legislation



Legislation

Computer Misuse Act 1990 (UK Wide)

S1 Unauthorised Access To Computer Material

It is an offence to cause a computer to perform any function with intent to gain unauthorised access to any program or data held in any computer. It will be necessary to prove the access secured is unauthorised and the suspect knows this is the case. This is commonly referred to as 'hacking'.

The Police and Justice Bill 2006 amended the maximum penalty for Section 1 offences. The offence is now triable either way, i.e. in the Magistrates Court or the Crown Court. The maximum custodial sentence has been increased from six months to two years.

S2 Unauthorised Access With Intent to Commit Other Offence

An offence is committed as per S1 but the S1 offence is committed with the intention of committing an offence or facilitating the commission of an offence. The offence to be committed must carry a sentence fixed by law or carry a sentence of imprisonment of 5 years or more. Even if it is not possible to prove the intent to commit the further offence, the S1 offence is still committed.
Max penalty: 5 years imprisonment.

S3 Unauthorised Acts with Intent to Impair Operation

An offence is committed if any person does an unauthorised act with the intention of impairing the operation of any computer. This 'impairment' may be such that access to data is prevented or hindered or that the operation or reliability of any program is affected. This offence carries a maximum penalty of ten years imprisonment. This offence is used instead of the Criminal Damage Act 1971, since it is not possible to criminally damage something that is not tangible. The Police and Justice Bill 2006 amended the original Section 3 Computer Misuse Act offence, unauthorised modification, and increased the maximum penalty to ten years imprisonment.

S3A Making, Supplying or Obtaining Article for Use in S1 or S3 offences

The Police and Justice Bill 2006 created a new S3A offence of making, supplying (including offers to supply) or obtaining articles for use in S1 or S3 computer misuse offences. The maximum penalty for this offence is two years imprisonment.

S10 Saving For Certain Law Enforcement Powers

This section explains that S1 of the Act has effect without prejudice to the operation in England, Wales or Scotland of any enactment relating to powers of inspection, search and seizure.

S14 Search Warrants

This section details the power by which a constable may apply for a search warrant if an offence under S1 has been or is about to be committed in any premises and there is evidence of that offence in those premises. It also gives the power to seize any items found in those premises that are evidence of the offence. Only a Circuit Judge can grant a warrant under this section.

S17 Interpretation

This section assists by explaining the meaning of some of the words and phrases used within the Act.

The Police & Criminal Evidence Act 1984

This legislation does not apply in Scotland unless officers from England, Wales and Northern Ireland are using their cross-border policing powers and procedures.

Schedule 1 details the procedure by which special procedure material and excluded material can be obtained.

A circuit judge can order that such material be produced to a constable for him to take away or that such material be made available for the constable to access within seven days of the order. For information held on a computer, an order can be made that the material is produced in a visible and legible form in which it can be taken away.
Or, an order can be made giving a constable access to the material in a visible and legible form within seven days of the order.

S8 Search Warrant

A justice of the peace can issue a search warrant, if it is believed an indictable offence has been committed and evidence of that offence is on the premises.
This warrant may, as per S16 of PACE, also authorise persons who can accompany the officers conducting the search – for example a computer expert.

S19 General Power of Seizure

This details the power by which an officer can seize items and the circumstances in which they can be seized.

S20 Extension of Powers of Seizure to Computerised Information

This details the power for requiring information held on a computer to be produced in a form in which it can be taken away and in which it is visible and legible.

S21 Access and Copying

This details the power in relation to having items seized accessed and copied to other relevant parties.

S22 Retention

This details the circumstances in which seized property can be retained.

S78 Exclusion of Unfair Evidence

The court can exclude evidence where, with regard to all the circumstances, it would have an adverse effect on the fairness of the proceedings.

Criminal Justice & Police Act 2001 (England, Wales & NI.)

(NB – when enacted)

S50 (re search and seizure – bulk items)

Describes the power by which an item can be seized, if it is believed it may be something or it may contain an item or items for which there is a lawful authorisation to search.

S50 (1)

Where a person is lawfully on premises carrying out a search and it is not practicable to determine at the time if an item found is something that he is entitled to seize, or if the contents of an item are things that he is entitled to seize, the item can be taken away for this to be determined. There must be reasonable grounds for believing the item may be something for which there was authorisation to search.

S50 (2)

Where a person is lawfully on premises and an item for which there is a power to seize is found, but it is contained within an item for which there would ordinarily be no power to seize and it is not practicable to separate them at the time, both items can be seized.

Factors to be considered prior to removing such property:

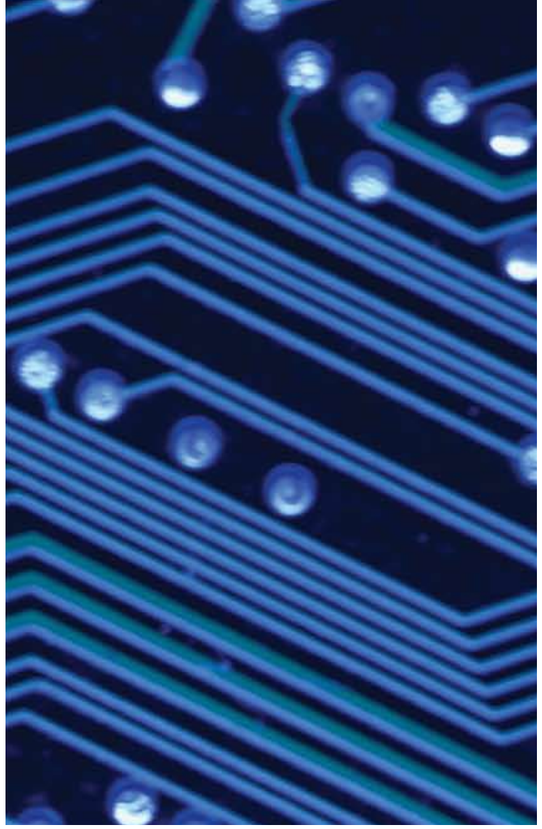
- How long would it take to determine what the item is or to separate the items?
- How many people would it take to do this within a reasonable time period?
- Would the action required cause damage to property?
- If the items were separated, would it prejudice the use of the item that is then seized?
- Once seized, the items must be separated or identified as soon as practicable. Any item found, which was seized with no power to do so, must be returned as soon as reasonably practicable. Items of legal privilege, excluded material and special procedure material, should also be returned as soon as practicable, if there is no power to retain them.
- It should be noted that the use of this act gives additional rights (such as the right to be present during examination) to the owner of the property.

Equivalent powers in Scotland are granted under:

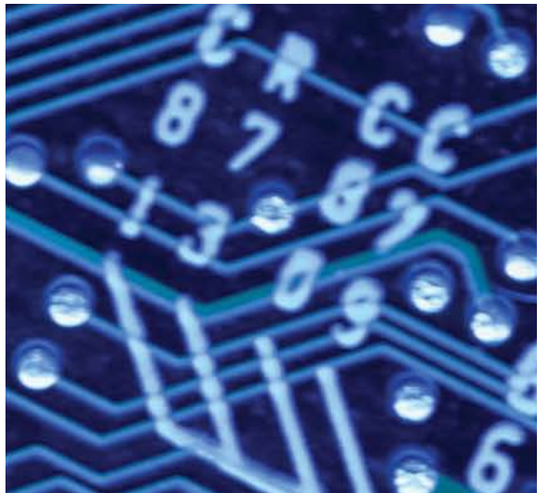
- Civic Government Scotland Act 1982.
- Criminal Procedure Scotland Act 1995.
- Common Law.

Other legislation

For additional guidance or information in relation to legislation not listed, investigators may wish to consult the Police National Legal Database (PNLD) or the Office of Public Sector Information (OPSI), available online at http://www.opsi.gov.uk



Local Hi-Tech Crime Units



Local Hi-Tech Crime Units

Avon and Somerset Constabulary 01275 818181
PO Box 37, Portishead,
BRISTOL BS20 8QJ

Bedfordshire Police 01234 841212
Woburn Road, Kempston,
BEDFORD MK43 9AX

British Transport Police 020 7388 6463
PO Box 260, 15 Tavistock Place
LONDON WC1H 9ST

Cambridgeshire Constabulary 01480 456111
Hinchingbrooke Park,
HUNTINGDON PE18 8NP

Central Scotland Police 01786 456000
Police Headquarters, Randolphfield,
STIRLING FK8 2HD

Cheshire Constabulary 01244 350000
Castle Esplanade,
CHESTER CH2 2PP

City of London Police 020 7601 2222
26 Old Jewry,
LONDON EC2R 8DJ

Cleveland Constabulary 01642 326326
PO Box 70, Ladgate Lane,
MIDDLESBOROUGH, Cleveland TS8 9EH

Cumbria Constabulary 01768 891999
Carleton Hall,
PENRITH, Cumbria CA10 2AU

Derbyshire Constabulary 01773 570100
Butterley Hall,
RIPLEY, Derbyshire DE5 3RS

Devon & Cornwall Constabulary 08705 777444
Middlemoor,
EXETER Devon EX2 7HQ

Dorset Police 01929 462727
Winfrith,
DORCHESTER, Dorset DT2 8DZ

Dumfries and Galloway Constabulary 01387 252112
Police Headquarters, Cornwall Mount,
DUMFRIES DG1 1PZ

Durham Constabulary 0191 386 4929
Aykley Heads,
DURHAM DH1 5TT

Dyfed Powys Police 01267 222020
PO Box 99, Llangunnor,
CARMARTHEN SA31 2PF

Essex Police 01245 491491
PO Box 2 Springfield,
CHELMSFORD, Essex CM2 6DA

Fife Constabulary Police Headquarters 01592 418888
Detroit Road,
GLENROTHES, Fife KY6 2RJ

Gloucestershire Constabulary 01242 521321
Holland House, Lansdown Road,
CHELTENHAM, Glous GL51 6QH

Grampian Police 01224 386000
Force Headquarters, Queen Street,
ABERDEEN AB10 1ZA

Greater Manchester Police 0161 872 5050
PO Box 22 (S West PDO), Chester House, Boyer Street,
MANCHESTER M16 0RE

Gwent Constabulary 01633 838111
Force Headquarters, Croesyceiliog, Cwmbran,
GWENT NP44 2XJ

H M Customs & Excise 020 72835353
Custom House, Lower Thames Street,
LONDON EC4

Local hi-tech crime units

Hampshire Constabulary 0845 0454545
Force Headquarters, West Hill,
WINCHESTER, Hants SO22 5DB

Hertfordshire Constabulary 01707 354000
Stanborough Road, Welwyn Garden City,
HERTS AL8 6XF

Humberside Police 01482 326111
Police Headquarters, Priory Road,
HULL, HU5 5SF

Kent County Constabulary 01622 690690
Force Headquarters, Sutton Road,
MAIDSTONE, Kent ME15 9BZ

Lancashire Constabulary 01772 614444
PO Box 77,
HUTTON, Nr Preston, Lancashire PR4 5SB

Leicestershire Constabulary 0116 222 2222
Police Hq St Johns Enderby
LEICESTER LE19 2BX

Lincolnshire Police 01522 532222
PO Box 999,
LINCOLN LN5 7PH

Lothian and Borders Police 0131 311 3131
Fettes Avenue,
EDINBURGH EH4 1RB

Merseyside Police 0151 709 6010
PO Box 59,
LIVERPOOL L69 1JD

Metropolitan Police Service 020 7230 1212
New Scotland Yard,
LONDON SW1H 0BG

Ministry of Defence Police 01371 854000
MDP Wethersfield,
BRAINTREE, Essex CM7 4AZ

Norfolk Constabulary 01953 424242
Martineau Lane,
NORWICH, Norfolk NR1 2DJ

Northamptonshire Police 01604 700700
Wootton Hall,
NORTHAMPTON NN4 0JQ

Northumbria Police 01661 872555
Ponteland,
NEWCASTLE-UPON-TYNE NE20 0BL

North Wales Police 01492 517171
Glan-y-Don,
COLWYN BAY, Conwy, North Wales LL29 8AW

North Yorkshire Police 01609 783131
Newby Wiske Hall,
NORTHALLERTON, North Yorkshire DL7 9HA

Northern Constabulary 01463 715555
Old Perth Road,
INVERNESS IV2 3SY

Nottinghamshire Police 0115 967 0999
Sherwood Lodge, Arnold,
NOTTINGHAM NG5 8PP

Police Service for Northern Ireland 0845 600 8000
Knocknagoney House, 29 Knocknagoney Road
BELFAST BT4 2PP

Scottish Crime and Drugs Enforcement Agency 0141 3021099
Osprey House, Inchinnan Road
PAISLEY PA3 2RE

Serious Organised Crime Agency
PO Box 8000, London SE11 5EN

South Wales Police 01656 655555
BRIDGEND, Mid Glamorgan CF31 3SU

South Yorkshire Police Service 0114 220 2020
Snig Hill,
SHEFFIELD S3 8LY

Staffordshire Police 01785 257717
Cannock Road,
STAFFORD ST17 0QG

Strathclyde Police 0141 532 2000
Police Headquarters, 173 Pitt Street,
GLASGOW G2 4JS

Suffolk Constabulary 01473 613500
Martlesham Heath,
IPSWICH IP5 7QS

Surrey Police 01483 571212
Mount Browne, Sandy Lane,
GUILDFORD Surrey GU3 1HG

Sussex Police 0845 60 70 999
Malling House,
LEWES, Sussex BN7 2DZ

Tayside Police 01382 223200
PO Box 59, West Bell Street,
DUNDEE DD1 9JU

Thames Valley Police 01865 846000
KIDLINGTON, Oxford, OX5 2NX

Warwickshire Police 01926 415000
PO Box 4, Leek Wootton,
WARWICK CV35 7QB

West Mercia Constabulary 01905 723000
Hindlip Hall, Hindlip, PO Box 55,
WORCESTER WR38SP

West Midlands Police 0845 113 5000
PO Box 52 Lloyd House Colmore Circus, Queensway,
BIRMINGHAM B4 6NQ

West Yorkshire Police 01924 375222
PO Box 9,
WAKEFIELD, West Yorkshire WF1 3QP

Wiltshire Constabulary 01380 722 341
London Road,
DEVIZES, Wiltshire SN10 2DN

Acknowledgements

Serious Organised Crime Agency

Chris Simpson
Metropolitan Police Service

Alan Phillips
7Safe Information Security

Dan Haagman
7Safe Information Security

Jim Kent
7Safe Information Security

Dominic Cahalin
7Safe Information Security

Geoff Fellows
LG Training Partnership

Mark Wilson
Metropolitan Police OES

Esther George
Crown Prosecution Service

Jim Stark
NCPE

Nigel Jones
NCPE

ACPO E-Crime Working Group

Home Office Scientific Development Branch

Interpol European Working Party on IT Crime – Mobile Phone Forensic Tools Sub-Group

The document may be downloaded in electronic format from www.7safe.com/electronic_evidence