Good Practice Guide for Computer based Electronic Evidence

(Version 3.0)

Association of Chief Police Officers

Application of this Guide

When reading and applying the principles of this guide, any reference made to NHTCU also includes the National Hi-Tech Crime Unit for Scotland (NHTCUS) and the Police Service for Northern Ireland (PSNI) unless otherwise indicated. This so that the anomalies between the different legal system 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; guidelines are not intended for use when dealing with evidence produced by witnesses from third party computer systems.

The guidelines in this document relate to:

Personnel attending crime scenes or making initial contact with a victim

Also, when 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 the 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.

Suggested procedures for access to certain material by defence

Mobile phone handling procedures

This guide is not intended to be a definitive manual of every operation that may take place during the investigation of a high tech crime or recovery of computer based electronic evidence. It is intended to address the most common circumstances that will be encountered where computer based electronic evidence is involved; principally with electronic evidence obtained from computer based media and from mobile phones. It is recognised that other forms of electronic evidence exist that do not fall within the remit of this guide.

Non-compliance with this guide should not necessarily be considered as grounds to reject evidence.

Contents

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 law enforcement.

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. However, the law enforcement community comprises other organisations that are essential to the rule of law in the United Kingdom. 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 changed, the principles 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 co-operation.

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

Principle 3: An audit trail or other record of all processes applied to computer based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.

Principle 4: The person in charge of the investigation (the case officer) has overall responsibility for ensuring that the law and these principles are adhered to.

Explanation of the principles

Computer based electronic evidence is no different from text contained within a document. For this reason, the 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.

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 show objectively to a court both 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 that have helped law enforcement to progress.

Computers can be used in the commission of crime, 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 are crucial issues.

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 scenes.

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.

Attending 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 carrying out such searches to ensure that their actions in relation to the seizure of such material are correct. The language used in this section is intended to be understood by anyone involved in search activities.

The most common types of storage devices are illustrated in the glossary of terms appended to this document. When encountered, 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.

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 for floppy disks, CDs or other storage devices). Other machines are becoming more widespread, in particular, personal organisers and palmtop computers. These can hold large amounts of data, often in storage areas not immediately obvious to the investigator.

Desktop and Laptop computers

Upon discovery of computer equipment which is switched off:

- ❑ Secure and take control of the area containing the equipment
- ❑ Allow any printers to finish printing
- ❑ Move people away from any computers and power supplies
- ❑ Don't, 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 battery from laptop computers
- ❑ Unplug the power and other devices from sockets: 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 and photograph (or video) all the components *in situ* and if no camera is available, draw a sketch plan of the system
- ❑ Label the ports and cables so that the computer may be reconstructed at a later date
- ❑ Carefully remove the equipment and record unique identifiers - the main unit, screen, keyboard and other equipment will have separate identifiers
- ❑ Ensure that all items have signed and completed exhibit labels attached to them as failure to do so may create difficulties with continuity and cause the equipment to be rejected by the forensic examiners
- ❑ Search area for diaries, notebooks or pieces of paper with passwords on which are often stuck to or close to the computer
- ❑ Consider asking the user if there are any passwords and 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
- Disconnect the modem if attached
- If the computer is believed to be networked, seek advice from the case officer, in-house forensic analyst or external specialist
- Do not take advice from the owner/user of the computer
- Label and photograph or video 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 the computer may be reconstructed at a later date
- Remove all other connection cables leading from the computer to other wall or floor sockets or devices
- Carefully remove the equipment and record the unique identifiers - the main unit, screen, keyboard and other equipment will have different numbers
- Ensure that all items have signed exhibit labels attached to them as 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 stuck to or close to the computer
- Consider asking the user if there are any passwords and if these are given, record them accurately
- Make detailed notes of all actions taken in relation to the computer equipment
- Record what is on the screen by photograph and by making a written note of the content of the screen
- Do not touch the keyboard or click the mouse and 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 will restore the screen or reveal that the screen saver is password protected. If the screen restores, photograph or video 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
- 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
- **N.B. It is accepted that the action of switching off the computer may mean that a small amount of evidence may be unrecoverable if it has not been saved to a storage medium but the integrity of the evidence already present will be retained.**

What should be seized

For the retrieval of evidence:

- 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: small connectors plugged into the back of the machine (see glossary)
- Modems (some contain phone numbers)
- External drives and other external devices
- Wireless network cards (see glossary)
- Digital cameras
- Floppy disks
- Back up tapes

- Jaz/zip cartridges
- CDs
- DVDs
- Hard disks not connected to the computer
- PCMCIA cards (see glossary)
- Memory sticks and memory cards (see glossary).

- N.B. Always label the bags containing these items, not the items themselves.

To assist in the examination of the equipment, seize:

- Manuals of computer and software
- Anything that may contain a password
- Keys.

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 of these tend to use the Palm OS, the Psion EPOC, or the Windows CE operating systems. Use of the Windows CE operating system makes the PDA fully compatible with Windows based PCs.

Application of the principles

With a PC, the essential concern is not to change the evidence on the hard disk and to produce an image which represents its state exactly as it was when seized. With an organiser/PDA, there is 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 does 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 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. Where the organiser (PDA) is fitted with only a single rechargeable battery, the appropriate mains adaptor should be connected to the device with the cable passing through the evidence bag so that it can be kept on charge. 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 using the on/off switch in order to preserve battery life. 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 the case is 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 TV.

If any of these items are to be seized and disconnected from a power supply, their memory may be erased.

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 and windows and police radios).

Monitors

Best transported screen down on the back seat of a car and belted in.

Hard disks

As for 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 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 use of batteries. If the battery is allowed to become flat, internal data will be lost. It is not possible to determine the life expectancy of any one battery. However this is an important consideration when storing a computer and should be covered by a local policy.

Investigating Personnel

Investigating Personnel

Whenever possible and practicable, thought must be given to the possibility of there being computer based electronic evidence on premises prior to a search being conducted. 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 1984, and the 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, then 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. Stand-alone computers, which are those most commonly found, can usually be seized by staff that have received the basic level of training in the subject.

It is appreciated, however, that in the majority of cases, there will be no prior warning to the finding of a computer upon premises being searched. The investigator will have to decide on the best course of action, bearing in mind the nature of the investigation.

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.

- Tools such as screw drivers (flathead and crosshead), small pliers, wire cutters for removal of cable ties
- Property register
- Labels and tape to mark and identify component parts of the system, including leads and sockets

- Exhibit labels (tie-on and adhesive)
- Paper sacks or bags for protection of the equipment being removed - do not use polythene bags to store individual internal components
- 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 this 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 obtain 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.

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 the Police and Criminal Evidence Act and the Codes of Practice equally apply to computers and peripherals in England and Wales. In Scotland, officers should ensure that they are acting within the terms of the search warrant.

Examination considerations

See section on electronic evidence recovery personnel.

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 Police and Criminal Evidence Act 1984 and the 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 Police and Criminal Evidence Act 1984 (this legislation is not applicable in Scotland). The grounds for any such decision should be carefully considered and noted accordingly.

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.

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 liquid crystal display together with memory chips in which all the information is stored. The amount of memory available for storage is often indicated in the name of the organiser, for example: 2KB, 15KB, 32KB and so on. KB stands for Kilobyte and 1KB represents approximately enough storage room for a thousand characters of text information. The memory is kept active by batteries and if these fail all information contained in the organiser (PDA) may be lost. 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. Consider changing them at regular intervals.

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

Evidence Recovery

Evidence Recovery

This section is directed towards staff engaged in the specialised field of computer based electronic evidence recovery, who have the requisite experience and received the appropriate training. 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 special challenges for its admissibility in court. Follow established forensic procedures. 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, then sound and established forensic principles should be adhered to. This means that 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 the 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.

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 and 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 be seized.

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

Welfare and Health and Safety Considerations

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.

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 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 and this list is by no means definitive. A number of these personnel may be employed in-house or contractors from outside the service. All need to be reminded of the sensitivity of such material and adequate precautions 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, the frequency of this will vary 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 ‘confidential’. 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 it 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.

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, released on a written undertaking, if appropriate, or to defer charge and bail pending advice from the Crown Prosecution Service or in Scotland the Procurator Fiscal Service. 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 advice as necessary.

Defence access

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. In no circumstances is access to take place of any such material except at law enforcement premises. (In Scotland, a request to view productions by the defence will be channelled through the relevant Procurator Fiscal).

There is no defence to the making of such an image and therefore no further copy is made specifically for use by the defence should they make such a request, the only exception is by order of the trial judge or magistrate (see below) and such a request would not be accepted in Scotland.

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. Such work sought by the defence in Scotland, would necessitate the defence expert attending at the law enforcement establishment to check on the gathering of such evidence in controlled conditions. No copies would be made.

It is expected that defence and law enforcement respect and understand each other's responsibilities in these circumstances. The defence has 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.

The defence will not always need full access to a forensic computer image. Likewise, it may not always be appropriate for law enforcement to deny access to a forensic computer image.

In cases of difficulty

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 (in Scotland the defence would not be provided with a copy of such an image).

If necessary, the defence technical witness may be given private facilities to examine the image at law enforcement premises (in Scotland the defence would be afforded controlled facilities).

Where no agreement is reached, the case should be referred to the court to hear argument and issue directions (in Scotland the matter would in the first instance be referred back to the appropriate Procurator Fiscal for a decision).

Magistrates court hearing

(not applicable in Scotland)

The first hearing at a magistrates court will normally not involve the production of the disc. 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 disc 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 disc. 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 available a laptop computer and appropriate screen facilities 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 disc 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.

It may be necessary for the examiner to give evidence as to the proof of the CD-ROM or DVD used. 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

External Consulting Witnesses

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.

And, 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 and the National Hi-Tech Crime Unit 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 skillful 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.

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 officer 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 then 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 electronic evidence: how does the prosecution disclose the massive amounts of data that they often analyse? For example, 27 Gigabytes of data if printed on A4 paper would create a stack of paper 920 metres high: bear in mind most computer hard disks are now larger than this.

The Criminal Procedure and Investigations Act 1996 (CPIA) came into force in 1997 and introduced a framework for the disclosure of unused material. In even a straightforward case, investigators can expect to gather a lot of information. A large proportion will be used as evidence. However, the CPIA governs what happens to the information left over, in other words, the unused material.

The rules of disclosure apply to computer based electronic evidence in exactly the same way as any other material obtained during the course of an investigation. However, due to the amount of material that could be stored on electronic media it is likely, in some cases, that not all of the information has been examined.

This raises a problem with the completion of forms which would normally list items shown on the schedule which undermine the prosecution case (primary disclosure) or assist the defence (secondary disclosure) or are required to be supplied under Section 7.3 of the code.

If the data has not been viewed, the disclosure officer will not know if it contains any items as above. It is suggested that an entry be made on the relevant form identifying the unused material that has not been viewed. A comment should be made as to the reasons why this has not been done, and that it is therefore not known if it holds any data which may undermine the case or assist the defence.

After a defence statement has been supplied, defence can make an application to the court for access to the items listed on the schedules. If after consultation with the disclosure officer the prosecutor is of the opinion that items should be disclosed, a copy of the unused data should be supplied to the defence.

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.

Handling Instructions – Mobile Phones

Handling of mobile phones

Any interaction with the handset on a mobile phone could result in loss of evidence and it is important not to interrogate the handset or SIM.

Before handling, decide if any other evidence is required from the phone (such as DNA/fingerprints/drugs/accelerants). If evidence in addition to electronic data is required, follow the general handling procedures for that evidence type laid out in the *Scenes of Crime Handbook* or contact the scenes of crime officer.

General advice is to switch the handset OFF due to the potential for loss of data if the battery fails or new network traffic overwrites call logs or recoverable deleted areas (e.g. SMS); there is also potential for sabotage. However, investigating officers (OIC) may require the phone to remain on for monitoring purposes while live enquiries continue. If this is the case, ensure the unit is kept charged and not tampered with. In all events, power down the unit prior to transport.

Recovery and packaging

Package and secure the phone in a rigid box (e.g. FSS box) with plastic ties. This will prevent accidental operation in transit.

- □ Insert the box into a Tamper proof bag and seal
- □ Fully complete exhibit/production labels
- □ Submit the phone with detailed examination requirements (i.e. DNA/fingerprint/electronic data recovery).

N. B. It should be noted that not all fingerprint enhancement methods will be used due to the potential for damage of the electronic memory.

The phone will then be examined for security measures such as personal identification number (PIN). If a PIN is in place, the OIC will be informed and will need to apply for a PUK (PIN unlock key) from the service provider. To obtain the PUK, the OIC must contact his or her force single point of contract (SPOC), who will require certain information from the phone and from the SIM card.

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 e-mail, including the "reply to" element?
- ❑ Did you save the e-mail in your computer? If so, request a copy on floppy disk or CD – 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:

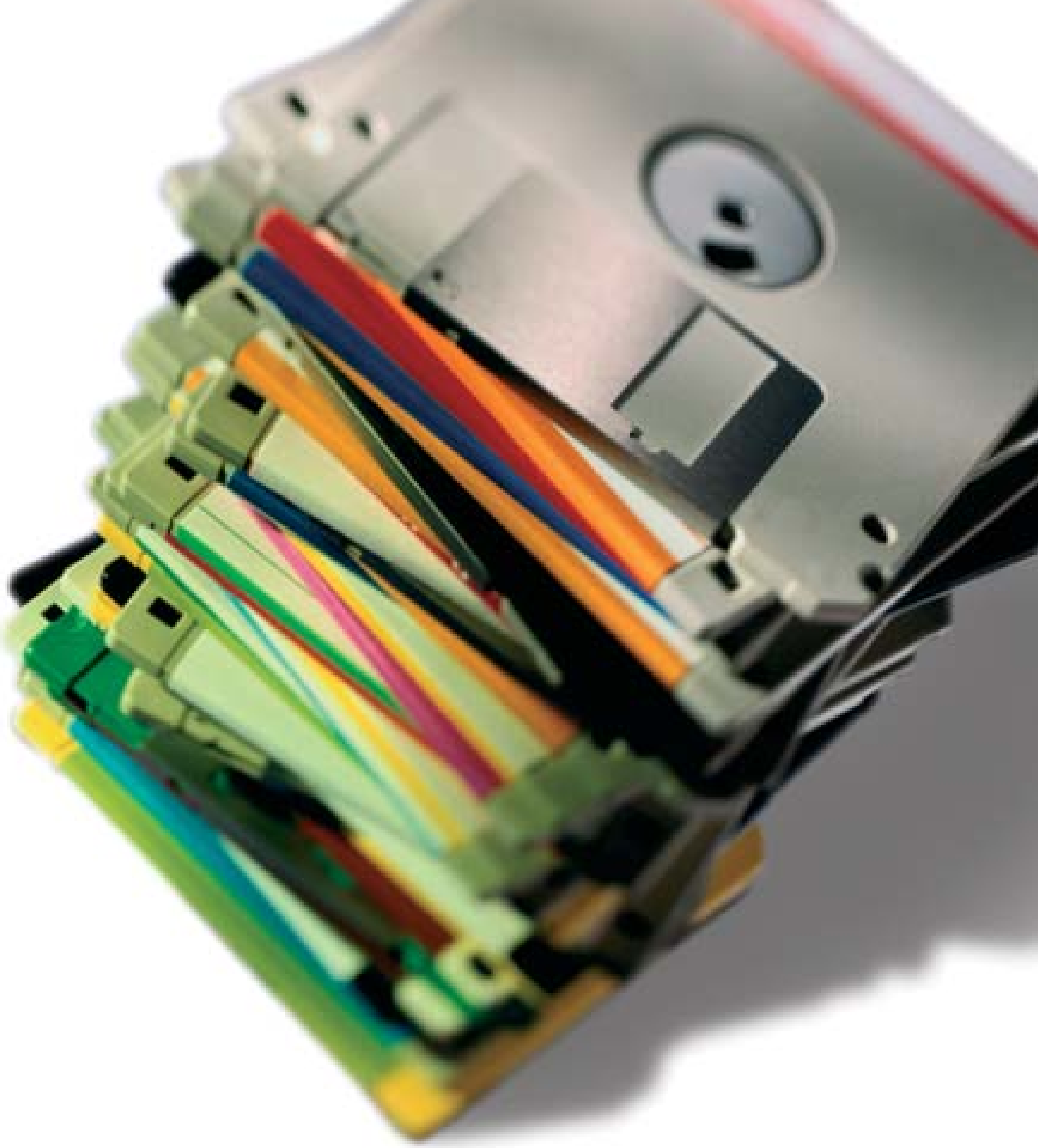
- ❑ Who is your Internet Service Provider (ISP)?
- ❑ What is the chat channel name?
- ❑ Who is the chat channel operator?
- ❑ What is the name of the server?
- ❑ What is the offending party’s nickname and what is your nickname?
- ❑ Did you save a copy of the conversation in your computer? If so, request copy of it on floppy disk or CD
- ❑ 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?

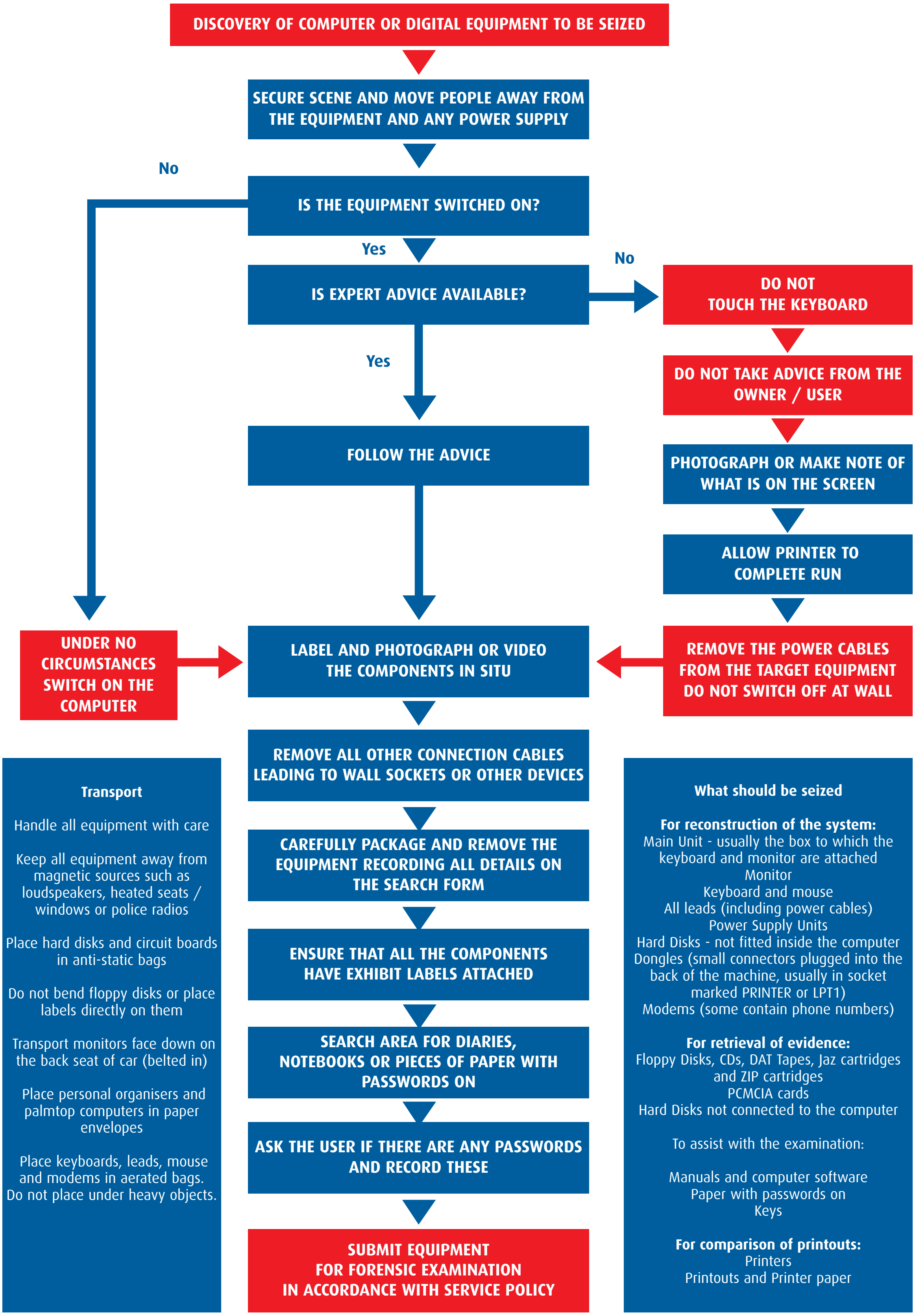
Newsgroup related crimes

- ❑ 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 or CD? 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?



Appendices

Best Practice for the Seizure of Electronic Evidence



DISCOVERY OF COMPUTER OR DIGITAL EQUIPMENT TO BE SEIZED

SECURE SCENE AND MOVE PEOPLE AWAY FROM THE EQUIPMENT AND ANY POWER SUPPLY

IS THE EQUIPMENT SWITCHED ON?

No → UNDER NO CIRCUMSTANCES SWITCH ON THE COMPUTER

Yes → IS EXPERT ADVICE AVAILABLE?

Yes → FOLLOW THE ADVICE

No → DO NOT TOUCH THE KEYBOARD

DO NOT TAKE ADVICE FROM THE OWNER / USER

PHOTOGRAPH OR MAKE NOTE OF WHAT IS ON THE SCREEN

ALLOW PRINTER TO COMPLETE RUN

REMOVE THE POWER CABLES FROM THE TARGET EQUIPMENT DO NOT SWITCH OFF AT WALL

LABEL AND PHOTOGRAPH OR VIDEO THE COMPONENTS IN SITU

REMOVE ALL OTHER CONNECTION CABLES LEADING TO WALL SOCKETS OR OTHER DEVICES

CAREFULLY PACKAGE AND REMOVE THE EQUIPMENT RECORDING ALL DETAILS ON THE SEARCH FORM

ENSURE THAT ALL THE COMPONENTS HAVE EXHIBIT LABELS ATTACHED

SEARCH AREA FOR DIARIES, NOTEBOOKS OR PIECES OF PAPER WITH PASSWORDS ON

ASK THE USER IF THERE ARE ANY PASSWORDS AND RECORD THESE

SUBMIT EQUIPMENT FOR FORENSIC EXAMINATION IN ACCORDANCE WITH SERVICE POLICY

Transport

Handle all equipment with care

Keep all equipment away from magnetic sources such as loudspeakers, heated seats / windows or police radios

Place hard disks and circuit boards in anti-static bags

Do not bend floppy disks or place labels directly on them

Transport monitors face down on the back seat of car (belted in)

Place personal organisers and palmtop computers in paper envelopes

Place keyboards, leads, mouse and modems in aerated bags. Do not place under heavy objects.

What should be seized

For reconstruction of the system:
Main Unit - usually the box to which the keyboard and monitor are attached
Monitor
Keyboard and mouse
All leads (including power cables)
Power Supply Units
Hard Disks - not fitted inside the computer
Dongles (small connectors plugged into the back of the machine, usually in socket marked PRINTER or LPT1)
Modems (some contain phone numbers)

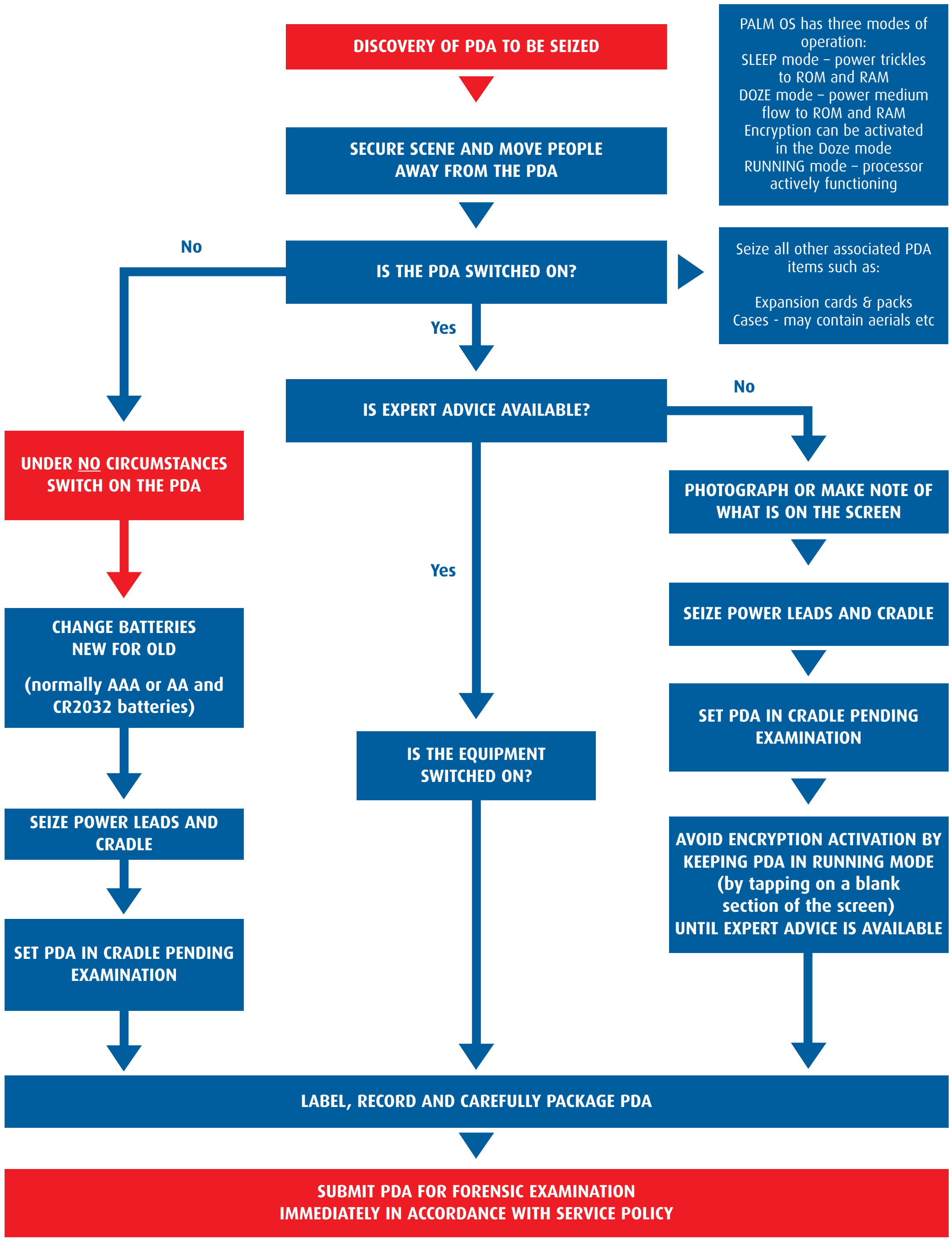
For retrieval of evidence:
Floppy Disks, CDs, DAT Tapes, Jaz cartridges and ZIP cartridges
PCMCIA cards
Hard Disks not connected to the computer

To assist with the examination:

Manuals and computer software
Paper with passwords on
Keys

For comparison of printouts:
Printers
Printouts and Printer paper

Seizure of Personal Digital Assistants



DISCOVERY OF PDA TO BE SEIZED

SECURE SCENE AND MOVE PEOPLE AWAY FROM THE PDA

IS THE PDA SWITCHED ON?

PALM OS has three modes of operation:
SLEEP mode – power trickles to ROM and RAM
DOZE mode – power medium flow to ROM and RAM
Encryption can be activated in the Doze mode
RUNNING mode – processor actively functioning

Seize all other associated PDA items such as:

Expansion cards & packs
Cases - may contain aerials etc

No

UNDER NO CIRCUMSTANCES SWITCH ON THE PDA

CHANGE BATTERIES NEW FOR OLD

(normally AAA or AA and CR2032 batteries)

SEIZE POWER LEADS AND CRADLE

SET PDA IN CRADLE PENDING EXAMINATION

Yes

IS EXPERT ADVICE AVAILABLE?

Yes

IS THE EQUIPMENT SWITCHED ON?

No

PHOTOGRAPH OR MAKE NOTE OF WHAT IS ON THE SCREEN

SEIZE POWER LEADS AND CRADLE

SET PDA IN CRADLE PENDING EXAMINATION

AVOID ENCRYPTION ACTIVATION BY KEEPING PDA IN RUNNING MODE (by tapping on a blank section of the screen) UNTIL EXPERT ADVICE IS AVAILABLE

LABEL, RECORD AND CAREFULLY PACKAGE PDA

SUBMIT PDA FOR FORENSIC EXAMINATION IMMEDIATELY IN ACCORDANCE WITH SERVICE POLICY

Glossary and Explanation of terms

ADDRESS The term address is used in several ways.

- An Internet address or 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 all information held on a computer in case something goes wrong with the original copy.

BIOS Basic input output system. A programme 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 floppy disk that contains the files needed to start an operating system.

BUFFER An area of memory, often referred to as a "cache", 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 generally 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. Web pages you browse to are stored in your browser's cache directory on your hard disk. When you return to a page you've recently browsed to, the browser can get it 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 Webcasting.

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-Conductant. This is a low power version of a chip, 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 that uses his or her skill to break into computer systems with malicious intent or motives (cracking). The term was coined by Hackers to differentiate themselves from those who do damage to systems or steal information.

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 aimed at specific Web sites. The attacker floods the Webserver with messages endlessly repeated. This ties up the system and denies access to legitimate users.

DIGITAL SIGNATURE A code which is used to guarantee that an e-mail was sent by a particular sender.

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 external hardware devices with some memory inside it. Companies that sell expensive software packages use dongles as 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 extended headers – information that is added by e-mail 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 Can contain file clusters that are not currently used by the operating system but nevertheless contain deleted data.

FLOPPY DISk These are disks that hold information magnetically. They come in 2 main types 3- inch and 5- inch. The 5- inch disks are flexible and easily damaged, the 3- 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 access personal information about other people with their expertise, and use it to commit computer crimes. 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.

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.

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 A high capacity removable hard disk system.

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 signatures (i.e. fingerprints) of storage media such as a computer hard drive.

When this algorithm is applied to a hard drive then 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 PC 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 is 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.

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.

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.

PIRATE SOFTWARE Software that has been illegally copied.

PORT The word port has 3 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.
- ❑ On the Internet Port often refers to a number that is part of an URL appearing after a colon (:) right after the domain name.
- ❑ 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 Programs that are 'free'.

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

RAM Random access memory is the PC's short-term memory. It provides working space for the PC to work with data. Information stored in the RAM is lost when the PC is turned off.

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

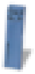
SD Expansion Card

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.

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.

SYSTEM UNIT Usually the largest part of a PC, the system unit is a box that contains the major components. It 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, usually a virus, that is hidden or disguised as another program or an e-mail. The victim downloads or starts what he or she thinks is a safe program and instead finds something actually 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.

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 piece of programming code, which is inserted into other programming for the purpose of causing some unexpected and, for the victim, usually undesirable event. Viruses can be transmitted by downloading programming from other sites or be present on a diskette. Some are harmless (messages on the screen, etc), others are destructive (corruption of information), while some may be fatal.

WINDOWS 95 (or 98) 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, .NET, Office XP, Windows XP and Windows Server are registered trademarks of Microsoft Corporation.

WINDOWS NT Operating system marketed by Microsoft primarily aimed at the business market. Multiple layers of security are available with this system.

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

WORM Like a virus but is capable of moving from computer to computer over a network without being carried by another program.

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 3.5-inch removable disk drive. 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

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.

It is important to remember that this is a summary only offence; proceedings must commence within 6 months from the date the prosecutor feels there is sufficient evidence to prove the offence. (DPP-v-MORGANS 1988). S25 general arrest conditions apply. Max penalty: 6 months imprisonment or Level V fine. (English Decision).

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 arrestable offence the S1 offence is still committed. Max penalty: 5 years imprisonment.

S3 Unauthorised Modification of Computer Material

An offence is committed if any person does an act that causes unauthorised modification of the contents of any computer. The accused must have the intent to cause the modification and be aware the modification has not been authorised. There is no necessity for any unauthorised access to have been obtained during the commission of this offence. This offence is used instead of The Criminal Damage Act 1971, as it is not possible to criminally damage something that is not tangible. (England and Wales only) Max penalty: 5 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 7 days of the order. For information held on 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 7 days of the order.

S8 Search Warrant

A justice of the peace can issue a search warrant if it is believed a serious arrestable 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

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

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

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

S22 Retention

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 for which there is no power to have seized it must be returned as soon as reasonably practicable as would items found of legal privilege, excluded and special procedure material if there is no power to retain it.

Equivalent powers in Scotland are granted under:

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

Local Hi Tech Crime Units are contactable via the following addresses

Local Hi Tech Crime Units: contact addresses

Force	Address	Telephone Number
Avon and Somerset Constabulary	PO Box 37, Portishead, BRISTOL BS20 8QJ	01275 818181
Bedfordshire Police	Woburn Road, Kempston, BEDFORD MK43 9AX	01234 841212
British Transport Police	PO Box 260, 15 Tavistock Place LONDON WC1H 9ST	020 7388 6463
Cambridgeshire Constabulary	Hinchingbrooke Park, HUNTINGDON PE18 8NP	01480 456111
Central Scotland Police	Police Headquarters, Randolphfield, STIRLING FK8 2HD	01786 456000
Cheshire Constabulary	Castle Esplanade, CHESTER CH2 2PP	01244 350000
City of London Police	26 Old Jewry, LONDON EC2R 8DJ	020 7601 2222
Cleveland Constabulary	PO Box 70, Ladgate Lane, MIDDLESBOROUGH, Cleveland TS8 9EH	01642 326326
Cumbria Constabulary	Carleton Hall, PENRITH, Cumbria CA10 2AU	01768 891999
Derbyshire Constabulary	Butterley Hall, RIPLEY, Derbyshire DE5 3RS	01773 570100
Devon & Cornwall Constabulary	Middlemoor, EXETER Devon EX2 7HQ	08705 777444
Dorset Police	Winfrith, DORCHESTER, Dorset DT2 8DZ	01929 462727
Dumfries and Galloway Constabulary	Police Headquarters, Cornwall Mount, DUMFRIES DG1 1PZ	01387 252112
Durham Constabulary	Aykley Heads, DURHAM DH1 5TT	0191 386 4929
Dyfed Powys Police	PO Box 99, Llangunnor, CARMARTHEN SA31 2PF	01267 222020
Essex Police	PO Box 2 Springfield, CHELMSFORD, Essex CM2 6DA	01245 491491
Fife Constabulary	Police Headquarters, Detroit Road, GLENROTHES, Fife KY6 2RJ	01592 418888
Gloucestershire Constabulary	Holland House, Lansdown Road, CHELTENHAM, Glous GL51 6QH	01242 521321
Grampian Police	Force Headquarters, Queen Street, ABERDEEN AB10 1ZA	01224 386000
Greater Manchester Police	PO Box 22 (S West PDO), Chester House, Boyer Street, MANCHESTER M16 0RE	0161 872 5050
Gwent Constabulary	Force Headquarters, Croesyceiliog, Cwmbran, GWENT NP44 2XJ	01633 838111
H M Customs & Excise	Custom House, Lower Thames Street, LONDON EC4	020 72835353
Hampshire Constabulary	Force Headquarters, West Hill, WINCHESTER, Hants SO22 5DB	0845 0454545
Hertfordshire Constabulary	Stanborough Road, Welwyn Garden City, HERTS AL8 6XF	01707 354000
Humberside Police	Police Headquarters, Priory Road, HULL, HU5 5SF	01482 326111
Kent County Constabulary	Force Headquarters, Sutton Road, MAIDSTONE, Kent ME15 9BZ	01622 690690
Lancashire Constabulary	PO Box 77, HUTTON, Nr Preston, Lancashire PR4 5SB	01772 614444
Leicestershire Constabulary	Police Hq St Johns Enderby LEICESTER LE19 2BX	0116 222 2222
Lincolnshire Police	PO Box 999, LINCOLN LN5 7PH	01522 532222
Lothian and Borders Police	Fettes Avenue, EDINBURGH EH4 1RB	0131 311 3131
Merseyside Police	PO Box 59, LIVERPOOL L69 1JD	0151 709 6010
Metropolitan Police Service	New Scotland Yard, LONDON SW1H 0BG	020 7230 1212
Ministry of Defence Police	MDP Wethersfield, BRAINTREE, Essex CM7 4AZ	01371 854000
Norfolk Constabulary	Martineau Lane, NORWICH, Norfolk NR1 2DJ	01953 424242
Northamptonshire Police	Wootton Hall, NORTHAMPTON NN4 0JQ	01604 700700
Northumbria Police	Ponteland, NEWCASTLE-UPON-TYNE NE20 0BL	01661 872555
North Wales Police	Glan-y-Don, COLWYN BAY, Conwy, North Wales LL29 8AW	01492 517171
North Yorkshire Police	Newby Wiske Hall, NORTHALLERTON, North Yorkshire DL7 9HA	01609 783131
Northern Constabulary	Old Perth Road, INVERNESS IV2 3SY	01463 715555
Nottinghamshire Police	Sherwood Lodge, Arnold, NOTTINGHAM NG5 8PP	0115 967 0999
Police Service for Northern Ireland	Brooklyn, Knock Road, BELFAST BT5 6LE	028 9065 0222
South Wales Police	BRIDGEND, Mid Glamorgan CF31 3SU	01656 655555
South Yorkshire Police Service	Snig Hill, SHEFFIELD S3 8LY	0114 220 2020
Staffordshire Police	Cannock Road, STAFFORD ST17 0QG	01785 257717
Strathclyde Police	Police Headquarters, 173 Pitt Street, GLASGOW G2 4JS	0141 532 2000
Suffolk Constabulary	Martlesham Heath, IPSWICH IP5 7QS	01473 613500
Surrey Police	Mount Browne, Sandy Lane, GUILDFORD Surrey GU3 1HG	01483 571212
Sussex Police	Malling House, LEWES, Sussex BN7 2DZ	0845 60 70 999
Tayside Police	PO Box 59, West Bell Street, DUNDEE DD1 9JU	01382 223200
Thames Valley Police	KIDLINGTON, Oxford, OX5 2NX	01865 846000
Warwickshire Police	PO Box 4, Leek Wootton, WARWICK CV35 7QB	01926 415000
West Mercia Constabulary	Hindlip Hall, Hindlip, PO Box 55, WORCESTER WR38SP	01905 723000
West Midlands Police	PO Box 52 Lloyd House Colmore Circus, Queensway, BIRMINGHAM B4 6NQ	0845 113 5000