ASSOCIATION OF
CHIEF POLICE OFFICERS

ACPO Good Practice Guide for Digital Evidence

The Association of Chief Police Officers has agreed to this revised good practice guide being circulated to, and adopted by, Police Forces in England, Wales & Northern Ireland.

It is NOT PROTECTIVELY MARKED under the Government Protective Marking Scheme and it is disclosable under the Freedom of Information Act 2000.

Document information

Protective marking	**NOT PROTECTIVELY MARKED**
Author	**DAC Janet Williams QPM**
Force/Organisation	**Metropolitan Police Service**
ACPO Business Area	**Crime BA**
Contact details	**020 7230 6800**
Review date	**As required**
Version	**5.0**

This good practice guide has been produced by the ACPO Crime Business Area and was originally approved by ACPO Cabinet in December 2007. The purpose of this document is to provide guidance not only to assist law enforcement but for all that assists in investigating cyber security incidents and crime. It will be updated according to legislative and policy changes and re-published as required.

Any queries relating to this document should be directed to either the author detailed above or the ACPO Programme Support Office on 020 7084 8958/8959.

Contents

Section		Page
	Introduction to the Guide	4
	Foreword	5
1	Application of Guide	6
2	The Principles of Digital Evidence	6
3	Plan	7
4	Capture	8
5	Analyse	10
6	Present	11
7	General	13

Appendix A	Network Forensic and Volatile Data Collection
Appendix B	Crimes involving Websites, Forums and Blogs
Appendix C	Crime Scenes
Appendix D	Developing a Digital Investigation Strategy
Appendix E	ACPO Workbook

INTRODUCTION TO THE GUIDE FOR DIGITAL EVIDENCE

It gives me great pleasure to introduce the 5th version of the ACPO Good Practice Guide for Digital Evidence. Much effort has been put in to ensure that the right information is available to practitioners and managers in the fight against cyber crime. I would like to thank all those who contributed to its creation for their efforts in drawing together their expert knowledge in tackling the criminal misuse of current and emerging technologies. The review board drew together people from academia, private and the public sector and has been an excellent example of collaborative working.

Since taking the UK policing lead for e-Crime in April 2008, I have overseen the creation of the Police Central e-Crime Unit. The team has grown from strength to strength through partnership working leading to the formation of a centre of excellence for cyber crime and the successful prosecution of cyber criminals. It is only through bringing together the expertise in policing across the UK, the capability and best practice within industry, support of Government and the Criminal Justice System that we will combat those responsible for cyber crime.

I am pleased that there has been recognition of a need to co-ordinate the UK response to cyber security issues through the establishment of the Office of Cyber Security and the Cyber Security Operations Centre. This approach will combine the various industries, law enforcement and agencies' hard work to corral them into a single effort to gather intelligence, enforcement capability and create the right framework of policy and doctrine to better enable us all to tackle the major issues identified.

This guide has changed from version 4, where it centred on computer based evidence; the new revision reflects digital based evidence and attempts to encompass the diversity of the digital world. As such this guide would not only assist law enforcement but the wider family that assists in investigating cyber security incidents. I commend all to read and make use of the knowledge and learning contained in this guide to provide us with the right tools to carry out our role.

Janet Williams QPM
Deputy Assistant Commissioner
Metropolitan Police Service
ACPO lead for the e-Crime Portfolio.

FOREWORD

It seems that whenever a review of ACPO guidance is carried out we are in the middle of technological changes that have vast impact on the work that is done within digital forensic units. It is a testament to the authors of the original four guiding principles for digital forensics that they still hold today, and one of the key early decisions of the review board was to keep those four principles, with only a slight change of wording to principle four.

We work in an area of constant change. There is a continuing need to re-evaluate and revise our capacities to perform our duties. There is a need to recover and analyse digital data that can now be found within the many devices that are within day to day use, and can supply vital evidence in all our investigations.

Hence a second key early decision was to change the title of the document to ACPO Good Practice Guide for Digital Evidence. This would hopefully encompass all aspects of digital evidence and remove the difficulty about trying to draw the line to what is or isn't a computer and thus falling within the remit of this guide.

It is important that people who work within the arena of digital forensics do not just concentrate on the technology, as essential as that is, but that the processes we use are fit for the purpose, and that skills and capacities within units reflect the demands that are made on them.

A prime example of this is the use of the word 'triage'. It has been a subject of much discussion within the forensic community. It should be noted that it does not mean a single triage tool rather it is a complete process where certain tools will play a part but are not the whole solution.

This guide is not intended to be an A-Z of digital forensics, or a specific "how to do" instruction manual. It should paint an overall picture and provides an underlying structure to what is required within Digital Forensic Units (DFUs). Therefore, the guide has been produced as a high-level document without the specific guidance included in previous versions, as this guidance is now available elsewhere. Where relevant, links to other guidance documents will be given.

In this document Digital Forensic Unit is used to cover any type of group that is actively involved in the processing of digital evidence.

1. SECTION 1 – APPLICATION OF GUIDE

1.1 When reading and applying the principles of this guide, any reference made to the police service also includes the Scottish Crime and Drugs Enforcement Agency (SCDEA) and the Police Service for Northern Ireland (PSNI) unless otherwise indicated.

1.2 This guide is primarily written for the guidance of UK law enforcement personnel who may deal with digital evidence. This will include:

- Persons who are involved in the securing, seizing and transporting of equipment from search scenes with a view to recovering digital evidence, as well as in the identification of the digital information needed to investigate crime;
- Investigators who plan and manage the identification, presentation and storage of digital evidence, and the use of that evidence;
- Persons who recover and reproduce seized digital evidence and are trained to carry out the function and have relevant training to give evidence in court of their actions. **Persons who have not received appropriate training and are unable to comply with the principles should not carry out this category of activity;**
- Persons who are involved in the selection and management of persons who may be required to assist in the recovery, identification and interpretation of digital evidence.

1.3 Since the previous version of the guide was published, the Forensic Science Regulator has published new draft Codes of Conduct and Practice covering forensic science throughout the UK. All practitioners working in the field of digital forensics must abide by these codes.

2. SECTION 2 – THE PRINCIPLES OF DIGITAL EVIDENCE

2.1 PRINCIPLES

2.1.1 **Principle 1:** No action taken by law enforcement agencies, persons employed within those agencies or their agents should change data which may subsequently be relied upon in court.

2.1.2 **Principle 2:** In circumstances where a person finds it necessary to access original data, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.

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

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

2.2 EXPLANATION OF THE PRINCIPLES

2.2.1 All digital evidence is subject to the same rules and laws that apply to documentary evidence.

2.2.2 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 law enforcement.

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

2.2.4 In order to comply with the principles of digital evidence, wherever practicable, proportionate and relevant an image should be made of the device. This will ensure that the original data is preserved, enabling an independent third party to re-examine it and achieve the same result, as required by principle 3.

2.2.5 This may be a physical / logical block image of the entire device, or a logical file image containing partial or selective data (which may be captured as a result of a triage process). Investigators should use their professional judgement to endeavour to capture all relevant evidence if this approach is adopted.

2.2.6 In cases dealing with data which is not stored locally but is stored at a remote, possibly inaccessible location it may not be possible to obtain an image. It may become necessary for the original data to be directly accessed to recover the data. With this in mind, it is essential that a person who is competent to retrieve the data and then able to give evidence to a court of law makes any such access. Due consideration must also be given to applicable legislation if data is retrieved which resides in another jurisdiction.

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

2.2.8 It should be noted that the application of the principles does not preclude a proportionate approach to the examination of digital evidence. Those making decisions about the conduct of a digital investigation must often make judgements about the focus and scope of an investigation, taking into account available intelligence and investigative resources. This will often include a risk assessment based on technical and non-technical factors, for example the potential evidence which may be held by a particular type of device or the previous offending history of the suspect. Where this is done it should be transparent, decisions should be justifiable and the rationale recorded.

2.2.9 Application of the four principles will also be informed by:

- The Forensic Science Regulator's forthcoming Codes of Practice and Conduct;
- The guidance around digital forensic process improvements developed by the National Policing Improvement Agency's Forensic 21 programme and those engaged in the collection, examination or reporting of digital evidence should also refer to that guidance.

3. SECTION 3 – PLAN

3.1 This also refers to the:

- The NPIA Forensic21 HTCU Computer Examination Process, 2011
- The SCDEA HTCU Guidance.

3.2 The proliferation of digital devices and the advances in digital communications mean that digital evidence is now present or potentially present in almost every crime.

3.3 Digital evidence can be found in a number of different locations:

- Locally on an end-user device – typically a user's computer, mobile/smart phone, satellite navigation system, USB thumb drive, or digital camera;
- On a remote resource that is public – for example websites used for social networking, discussion forums, and newsgroups;
- On a remote resource that is private – an internet Service Provider's logs of users' activity, a mobile phone company's records of customers' billing, a user's webmail account, and increasingly common, a user's remote file storage;

- In transit – for example mobile phone text messages, or voice calls, emails, or internet chat.

3.4 It would be quite common for evidence of a crime to be in more than one of the locations mentioned above. However it might be much easier to obtain the evidence from one location rather than another; careful consideration should be given to the resources required to obtain the evidence.

3.5 For example, if evidence is required of contact between two mobile phone numbers, the best method would be to obtain call data from the Communication Service Providers via the force SPOC, rather than to request a forensic examination of the mobile phones. The call data is likely to be more comprehensive than call logs from a mobile phone and the times and dates can be relied upon, which is not necessarily the case with logs from a mobile phone.

3.6 In addition, investigators seeking to capture 'in transit' evidence must be aware of the implications under the Regulation of Investigatory Powers Act (RIPA) and the need to seek appropriate authorities for doing so. Further information is available from force SPOCs.

3.7 With the above in mind, it is important that investigators develop appropriate strategies to identify the existence of digital evidence and to secure and interpret that evidence throughout their investigation.

3.8 Due consideration should always be given by the investigators of the benefits to the overall investigation of conducting any digital forensic work. Proportionality should be assessed when a digital forensic strategy is being considered to ensure that limited resources for digital forensic investigation are directed appropriately.

4. SECTION 4 – CAPTURE

4.1 This also refers to:

- Retrieval of Video Evidence and Production of Working Copies from Digital CCTV Systems v2.0;
- Network forensics and volatile data collection – Appendix A;
- Crimes involving websites, forums and blogs – Appendix B.

4.2 PHYSICAL CRIME SCENES

4.2.1 There are many different types of digital media and end-user devices, which may be encountered during a search of a crime scene, all of which have the potential to hold data which may be of value to the investigation. In order to preserve the data and achieve best evidence, these items must be handled and seized appropriately, and should be treated with as much care as any other item that is to be forensically examined. This section is intended to assist individuals to ensure their actions in relation to seizure are correct.

4.3 PROPORTIONALITY ISSUES RELATING TO SEIZURE

4.3.1 Proportionality issues relating to seizure are:

- Before seizing an item, consider whether the item is likely to hold evidence. For example, is this a family computer or a computer belonging to a suspect?
- Ensure that details of where the item was found are recorded, which could assist in prioritising items for examination at a later stage;
- Consider when the offence was committed; when seizing CCTV, give consideration to narrowing down what is seized, by camera and/or time period. Check whether another system may be better placed to record the evidence;

- Differentiate between mobile phones found on a suspect (likely to be in current use) and phones found in a drawer (may not be in current use), as different levels of examination may be possible for these;
- Also consider that evidence may be stored online, or on an internet service provider's systems and end-user devices may only be needed to obtain the details necessary to request this evidence from the service provider. If so, it is best to seize items in current usage, i.e. computers connected to the internet.

4.3.2 Digital devices and media should not be seized just because they are there. The person in charge of the search must have reasonable grounds to remove property and there must be justifiable reasons for doing so. The search provisions of PACE Legislation Codes of Practice equally apply to digital devices and media in England, Wales and Northern Ireland. In Scotland, officers should ensure they are acting within the terms of the search warrant.

4.3.3 Due regard should also be given to the application of the European Convention of Human Rights.

4.4 BEFORE ATTENDING A SCENE TO CAPTURE DIGITAL EVIDENCE

4.4.1 Persons responsible for the seizure of digital devices, or for on-scene capture of data, should ensure:

- They have the necessary equipment. (Refer to the First Responder's Guide for a detailed breakdown);
- They have considered potential sources of evidence and know what is likely to be relevant, where possible.

4.4.2 Where an investigation is likely to involve the examination of user-created digital images, consideration should be given to the question of seizing of cameras and other devices capable of taking digital photographs. For example, in cases where a suspect is believed to have taken indecent photographs of children, seizure of devices capable of taking digital photos could be useful not only for the data they store, but also to link these devices to previously identified indecent photographs by the examination of digital metadata (EXIF data).

4.4.3 Where necessary, specialist advice from a force's Digital Forensic Unit should be sought in advance. If given sufficient information about the investigation, DFUs will be able to advise on which items are most likely to provide the evidence sought.

4.5 WHEN ATTENDING A SCENE

4.5.1 To comply with principle 3, records must be kept of all actions taken in relation to digital evidence, which could include photographs/diagrams of equipment locations, details of any information provided by persons present, and records of any actions taken at the scene.

4.5.2 Refer to the First Responder's Guide for detailed guidance on seizure for individual items. However, persons attending a scene should be especially aware that **systems which are powered on (running) need to be handled with care**, as there is the potential to make unwanted changes to the evidence if these are not dealt with correctly. Such systems should only be accessed by appropriately trained personnel. In addition, volatile data of evidential value may be lost.

4.6 CAPTURING ONLINE EVIDENCE

4.6.1 In some investigations the capture of digital evidence may be from an online rather than a physical location. Detailed guidance on securing this evidence can be found in 'Crimes involving websites, forums and blogs' and 'Network forensics and volatile data'.

4.6.2 Online evidence can roughly be split into that which is publicly available (e.g. forum postings, where the forum does not require a login to view) and that which is private (e.g. Facebook account information). There may be scope to obtain both (e.g. by capturing the text of a forum posting and then requesting the account details of the user who made the posting from the forum owner).

Investigators should be aware of the potential issues when capturing publicly available data, including the 'footprints' which are left when accessing a site, these can alert a website owner to law enforcement interest.

4.6.3 Records should be kept of all actions taken when capturing online evidence in order to comply with principle 3.

5. SECTION 5 – ANALYSE

5.1 This also refers to:

- The NPIA Forensics21 HTCU Computer Examination Process, 2011;
- Forensic Science Regulator's Codes of Practice and Conduct;
- Digital Imaging Procedure v2.1.

5.2 Devices seized as part of a search will typically be submitted to the force Digital Forensic Unit in accordance with force policy. Due to the volume and complexity of data stored on digital devices, it is not possible or desirable to extract all data held on a device for review by investigators. Instead, a forensic strategy needs to be formulated to enable the examination to be focused on the relevant data.

5.3 The National Policing Improvement Agency is currently formulating suggested processes for digital examinations involving computer and phone devices. Readers should refer to these processes for more specific detail of best practice digital examination processes. Other types of digital examinations should follow the same principles, briefly summarised below.

5.4 The investigator needs to properly consider the nature and purpose of the digital examination. The investigator must be clear on what priorities are placed on the examination as it may well be that key information needs to be found in order to preserve evidence that may exist elsewhere. This is particularly the case where it relates to the existence of additional evidence, offenders and victims.

5.5 When submitting evidence to Digital Forensic Units, investigators must supply specific requirements. It is not practically possible to examine every item of digital data and clear tasking is needed to ensure that the digital forensic practitioner has the best chance of finding any evidence which is relevant to the investigation.

5.6 For more complex or lengthy investigations, an initial triage/review of the digital evidence (whether or not this is done using a specific triage tool) will give investigators and practitioners a better understanding of the nature of the digital evidence held. The forensic strategy should be regularly reviewed to take account of any changes in the direction of the investigation, which may occur as a result of digital forensic examination (for example, finding emails identifying a co-conspirator) or investigations elsewhere (a witness identifying another person as being of interest to the investigation). For this reason it is vital that the investigator and the digital forensic practitioner communicate regularly regarding the progress of the investigation.

5.7 If initial examination results in a large amount of data to be reviewed, consideration must be given to who is best placed to review that data. Often this will be the investigator, due to their greater knowledge of the case. Dependent on the source, this data may include:

- Internet history records;
- E-mails;
- Instant Messaging Logs;
- Media files (images and videos);
- Text documents;
- Spreadsheets;
- CCTV;
- Text Messages.

5.8 Collaboration with the Digital Forensic Unit will ensure that the significance of any reviewed data is not misunderstood. For example, when reviewing keyword hits which exist in deleted files, the significance of a hit's location may need explanation from a digital forensic practitioner.

5.9 For mobile phone examinations, different levels of examination may be appropriate depending on the intelligence relating to the device and the requirements of the investigation. For example, a phone which has been found in a drawer may be examined only to retrieve the necessary information to request billing details and to establish whether it is owned by the suspect (level 1). A phone which is known to be in regular use by a suspect in a high profile investigation may be subject to a much more in-depth examination involving the retrieval of deleted data and potentially the physical removal and examination of memory chips (level 4). These examination levels are outlined in the NPIA mobile phone SOPs.

5.10 INTERPRETATION OF DIGITAL DATA

5.10.1 As with other forensic evidence, interpretation is often required to ensure the evidential weight of recovered digital evidence is clear. Practitioners who undertake the interpretation of digital data must be competent to do so and have had sufficient training to undertake the task assigned to them.

5.10.2 As an example, the presence of indecent images of children on a computer would not in itself be sufficient evidence of possession, as the possessor must be aware of the existence of the images. A digital forensic practitioner may interpret the presence of other digital evidence (such as a list of recently opened files, recent search terms, the name and location of folders/files containing the material, or whether or not the computer is password protected) to establish the likelihood of the user being aware of the existence of these images.

5.10.3 Establishing the provenance of digital evidence is another key task of the forensic practitioner, who must use their knowledge and skills to identify not just that the evidence exists but also how it came to be there. This is common to all forensic disciplines; for example, the presence of a defendant's fingerprint on a bottle at the crime scene may not have any bearing on whether the defendant committed the crime if the bottle may have been carried there by someone else. It is the responsibility of the practitioner to carry out analysis to identify provenance where necessary, to mitigate the risk of their findings being misinterpreted.

5.10.4 Often the role of the digital forensic practitioner will be to make investigators and prosecutors aware of the limitations of the digital evidence as well as its strengths.

5.10.5 It must also be borne in mind that the development of digital technology is dynamic and the practitioners may well face significant challenges to their knowledge. It is not possible to be an expert in all aspects of digital forensic examination, but a practitioner should be aware of the limits of their knowledge and where further research or additional specialist knowledge is required.

6. SECTION 6 – PRESENT

6.1 This also refers to:

- NPIA Forensics21 process maps;
- CPS disclosure manual, annex K.

6.2 Communication of the results of a digital forensic examination may be through a number of means:

- Verbally to an investigator/officer throughout a case;
- By a statement or report on conclusion of the case;
- In court if witness evidence is required.

6.3 In all cases a digital forensic practitioner must be aware of their duty of impartiality and that they must communicate both the extent and the limitations of the digital forensic evidence. This is especially important as, due to the nature of digital forensic evidence, it is not always immediately understandable by the layman.

6.4 VERBAL FEEDBACK

6.4.1 This should be given regularly throughout the progress of an examination. In this way it will enable the investigator to pursue relevant lines of enquiry as these become evident, and will ensure that the practitioner is up-to-date with any information required to better target their investigation.

6.4.2 It is important that this communication be recorded for potential disclosure at a later date. Good practice would be for a verbal conversation to be followed up via email, or to be recorded in contemporaneous notes.

6.5 STATEMENTS OR REPORTS

6.5.1 The statement or report is the ultimate product of the examination. It should outline the examination process and the significant data recovered. Whilst an initial report may be relatively brief, the practitioner should be in a position to produce a full technical report should one later be required.

6.5.2 The report should be written to be understandable to the reader; this may include the use of a glossary, diagrams/screenshots to illustrate points, the use of examples and avoidance of technical jargon.

6.5.3 When particular items are reproduced in a report, care should be taken to ensure that the representation is accurate. For example, pictures should not be reproduced at a larger size without this being made clear in the report. If a report is produced digitally, items should be reproduced where possible in their original file formats, to ensure that those viewing will see the item as close as possible to its original appearance. If this is not appropriate (for example, if a file needs to be converted to a more common format for reviewing) then the fact that it has been converted must be stated in the report. Where it is not possible to reproduce the item as it would have originally been viewed, for example, when a webpage is retrieved some time after the original page was accessed, this must also be clearly stated in the report.

6.5.4 The report should make clear the strength of any conclusions reached and always identify where an opinion is being given, to distinguish this from fact. Where opinion evidence is provided, the practitioner must state the facts on which this is based, and how he or she came to this conclusion.

6.6 WITNESS EVIDENCE

6.6.1 A practitioner may need to testify about not only the conduct of the examination, but also the validity of the procedure and their experience and qualifications to conduct the examination.

6.6.2 Expert witness training should be considered for digital forensic practitioners so they are familiar with the process of giving evidence and aware of their responsibilities as witnesses. A digital forensic practitioner will not always be giving expert evidence and should clearly understand the distinction between expert evidence and evidence of fact.

6.6.3 When giving evidence, practitioners must make clear when they are expressing facts and when they are giving opinions, as above. Practitioners, when giving expert evidence, must take care to do so only where it relates to their own area of expertise and remember that their duty when giving evidence (whether it be in report form or as a witness) is to the court, regardless of which party has instructed them.

6.7 CONTEMPORANEOUS NOTES

6.7.1 It is worth repeating at this point that full records should be made of all actions taken. These must be disclosed to the defence who may subsequently cause a further examination to be conducted. A significant part of such an examination will be to validate the actions and results of the original examination. Such records are also part of the unused material for the case under investigation.

7. SECTION 7 – GENERAL

7.1 TRAINING AND EDUCATION

7.1.1 Also refers to:

- ACPO Good Practice and Advice Guide for Managers of e-Crime Investigations ('Managers' Guide').

7.1.2 The general principle of training in digital investigation significantly differs from usual police training. Owing to the rapidly changing environment of technology, there is a requirement for the continuous but essential retention and updating of skills.

7.1.3 Readers should refer to the section concerning training in the Good Practice and Advice Guide for Managers of e-Crime Investigations**.**

7.1.4 It is also the personal responsibility of any person working within the area of digital forensics to maintain their knowledge of the subject areas they are involved in. Formal training is just one route, but there is also a vast amount of open-source information available for self development and awareness. (Practitioners should be mindful that the veracity of open-source information cannot always be established, and should critically evaluate any information sourced in this way.) Professional development can also be progressed by attending conferences and technical workshops, conducting independent research, participating in online specialist forums or by discussions with subject matter experts in other forces or agencies.

7.1.5 Police personnel should also be aware of POLKA (Police On-Line Knowledge Area), an information sharing resource where there are digital forensic communities that discuss numerous topics and a library of some relevant documentation.

7.2 WELFARE IN THE WORKPLACE

7.2.1 Also refers to:

- ACPO Good Practice and Advice Guide for Managers of e-Crime Investigations.

7.2.2 There are a number of aspects concerning the welfare of staff working within the digital forensic area and the risks associated with that type of work:

- The psychological effect of viewing disturbing material including indecent images of children (IIOC);
- Electrical safety;
- Ergonomics, including working with Display Screen Equipment (DSE);
- Biohazards.

7.2.3 Both staff and managers should be aware of the potential impacts of these and take steps to minimise their effect. For further details, refer to the Managers' Guide.

7.3 DIGITAL FORENSIC CONTRACTORS

7.3.1 Also refers to:

- ACPO Good Practice and Advice Guide for Managers of e-Crime Investigations;
- Forensic Regulator's Codes of Practice and Conduct.

7.3.2 Where the services of commercial forensic service providers are required by law enforcement, it is important to select external consulting witnesses/forensic practitioners carefully. Any external practitioner should be familiar with, and agree to comply with, the principles of digital evidence referred to in this guide.

7.3.3 Selection of external providers, particularly in the more unusual or highly technical areas, can be a problem for the investigator. Digital forensic units may be able to offer more advice on the criteria for selection.

7.3.4 Readers should refer to the ACPO Managers' Guide for further suggestions on the practical aspects of selecting an external forensic service provider (including such aspects as security clearance and physical security requirements or procurement issues). They should also ensure that any forensic service provider engaged on law enforcement work is able to work in accordance with the Forensic Regulator's Codes of Practice and Conduct which requires ISO accreditation (ISO 17025 and ISO 17020). The Regulator will expect compliance for all digital forensic services by 2014, but procurement frameworks and contracts should be looking at compliance for external service providers in advance of this date.

7.3.5 When engaging the services of digital forensic contractors, processes and policies for the retention of case-related data should be considered, both on an ongoing basis and following the termination of the contract. Contractors and those engaging them must comply with the terms of the Data Protection Act, and with any local policies of the engaging organisation.

7.4 DISCLOSURE

7.4.1 Also refers to:

- Attorney General's Guidelines on Disclosure (revised April 2005);
- CPS Disclosure Manual.

7.4.2 The particular issues relating to disclosure of digital evidence are typically those of volume. A digital investigation may involve the examination of a vast amount of data and it is not always straightforward for investigators and prosecutors to discharge their disclosure obligations in respect of this. For example, the average hard disk is now larger than 200 gigabytes and this, if printed out on A4 paper, would be 10,000,000 pages long. In addition, the nature of digital evidence means it is not always possible to create a static representation which preserves the nature of the original evidence (e.g. of a database) and in some cases data can only be disclosed electronically, such as CCTV.

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

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

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

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

7.4.6 Even in relatively straightforward cases, investigators may obtain, and even generate, substantial quantities of material. Some of this material may in due course be used as evidence: for example, physical exhibits recovered from the scene of the crime or linked locations, CCTV material, forensic evidence, statements obtained from witnesses and tape recordings of defendants interviewed under caution before charge. The remaining material is the 'unused material', and it is this material which is the subject of the procedure for disclosure created under the CPIA.

7.4.7 Generally material must be examined in detail by the disclosure officer or the deputy but, exceptionally, the extent and manner of inspecting, viewing or listening will depend on the nature of the material and its form. For example, it might be reasonable to examine digital material by using software search tools. If such material is not examined in detail, it must nonetheless be described on the disclosure schedules accurately and as clearly as possible. The extent and manner of its examination must also be described together with justification [2]for such action.

7.4.8 The CPIA Code of Practice also provides guidance concerning the duty to pursue all reasonable lines of enquiry, in relation to computer material[3]. Examination of material held on a computer may require expert assistance and, in some cases, Digital Evidence Recovery Officers (DEROs) may be commissioned to help extract evidence and assist with unused material. DEROs may be police officers, police staff or external service providers. The use of DEROs and related matters is discussed in detail in Annex H of the Disclosure Manual.

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

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

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

7.4.12 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.

[2] Paragraph 27, Attorney General's Guidelines on Disclosure (2005)
[3] CPIA Code of Practice, paragraph 3.5

7.5 LEGISLATION

7.5.1 Also refers to:

- Legislation.gov.uk;
- ACPO Good Practice and Advice Guide for Managers of e-Crime Investigations.

7.5.2 A wide variety of legislation may apply in examinations of digital evidence. Some of the most relevant is detailed below.

i. Computer Misuse Act 1990 (UK Wide)
(http://www.legislation.gov.uk/ukpga/1990/18/introduction)

S1 Unauthorised Access To Computer Material

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

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

S2 Unauthorised Access with Intent to Commit Other Offence

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

S3 Unauthorised Acts with Intent to Impair Operation

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

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

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

S10 Saving For Certain Law Enforcement Powers

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

S17 Interpretation

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

ii. The Police & Criminal Evidence Act 1984
(http://www.legislation.gov.uk/ukpga/1984/60/contents)

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

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

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

  Or, an order can be made giving a constable access to the material in a visible and legible form within seven days of the order.

S8 Search Warrant

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

S19 General Power of Seizure

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

S20 Extension of Powers of Seizure to Computerised Information

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

S21 Access and Copying

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

S22 Retention

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

S78 Exclusion of Unfair Evidence

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

iii. Criminal Justice & Police Act 2001 (England, Wales & NI.)
(http://www.legislation.gov.uk/ukpga/2001/16/contents)

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.

7.5.3 Factors to be considered prior to removing such property:

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

7.5.4 It should be noted that the use of this act gives additional rights (such as the right to be present during examination) to the owner of the property.

7.5.5 Equivalent powers in Scotland are granted under:

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

7.5.6 SEXUAL OFFENCES ACT 2003 (http://www.legislation.gov.uk/ukpga/2003/42/contents)

46 Criminal proceedings, investigations etc. E+W+N.I.

(1)After section 1A of the Protection of Children Act 1978 (c. 37) insert—
"1B Exception for criminal proceedings, investigations etc.

(1) In proceedings for an offence under section 1(1)(a) of making an indecent photograph or pseudo-photograph of a child, the defendant is not guilty of the offence if he proves that—
(a) it was necessary for him to make the photograph or pseudo-photograph for the purposes of the prevention, detection or investigation of crime, or for the purposes of criminal proceedings, in any part of the world,
(b) at the time of the offence charged he was a member of the Security Service, and it was necessary for him to make the photograph or pseudo-photograph for the exercise of any of the functions of the Service, or
(c) at the time of the offence charged he was a member of GCHQ, and it was necessary for him to make the photograph or pseudo-photograph for the exercise of any of the functions of GCHQ.

(2) In this section "GCHQ" has the same meaning as in the Intelligence Services Act 1994."

7.5.7 CORONERS AND JUSTICE ACT 2009 (Came into force on 06 April 2010)

(http://www.legislation.gov.uk/ukpga/2009/25/contents)

7.5.8 CPS guidance regarding prohibited images of children can be found at: https://www.cps.gov.uk/legal/p_to_r/prohibited_images_of_children/

- Sections 62-68 deal with "possession of prohibited images of children".

7.5.9 The offence targets certain non-photographic images of children, possession of which is not covered by previously existing legislation.

7.5.10 A prohibited image is pornographic and concentrates on genitals or shows a sex act and is grossly offensive, disgusting, or otherwise of an obscene character.

7.5.11 An image is of a child if impression conveyed is that of a child or the predominant impression is that of a child despite some physical characteristics shown are not those of a child.

7.5.12 If the image is in a series then the context of the series can be used to determine if the individual image is prohibited or not.

7.5.13 Classified films are excluded (unless an individual is in possession of a still or clip that has been extracted solely or principally for the purpose of sexual arousal).

7.5.14 There is a defence of having a legitimate reason for possession, or having not seen the image and not knowing, nor having cause to suspect, it was a prohibited image.

7.5.15 The maximum penalty is 3 years' imprisonment.

7.6 OTHER LEGISLATION

7.6.1 For additional guidance or information in relation to legislation not listed, investigators may wish to consult the Police National Legal Database (PNLD) or the UK Legislation website (which replaces the Office of Public Sector Information (OPSI) and Statute Law databases), available online at http://www.legislation.gov.uk.

GLOSSARY OF TERMS/ABBREVIATIONS USED IN THIS GUIDE

ACPO: Association of Chief Police Officers

DFU: Digital Forensic Unit

NPIA: National Police Improvement Agency

IIOC: Indecent Images Of Children

SPOC: Single Point Of Contact

RIPA: Regulation Of Investigatory Powers Act

RIPSA: Regulation Of Investigatory Powers (Scotland) Act

DPA: Data Protection Act

CCTV: Closed Circuit Television

IP Address: Internet Protocol Address - numerical address assigned to device in a computer network that uses the Internet protocol for communications.

PACE: Police & Criminal Evidence Act 1984

SIM: A subscriber identity module or subscriber identification module (SIM) on a removable SIM card securely stores the service-subscriber key (IMSI) used to identify a subscriber on mobile telephony devices (such as mobile phones and computers).

PUK: PIN Unlock Key (PUK)

CSP/ISP: Communications Service Provider/Internet Service Provider

REFERENCES

- ACPO Good Practice and Advice Guide for Managers of e-Crime Investigations ('Managers' Guide')
  http://www.acpo.police.uk/documents/crime/2011/20110301%20CBA%20ACPO%20managers_guide_v10.1.4%20for%20ecrime%20investigations_2011.pdf

- Attorney General's Guidelines on Disclosure (revised April 2005)
  http://www.cps.gov.uk/legal/a_to_c/attorney_generals_guidelines_on_disclosure/

- Crimes involving websites, forums and blogs

- CPS disclosure manual
  http://www.cps.gov.uk/legal/d_to_g/disclosure_manual/

- Digital Imaging Procedure v2.1
  http://tna.europarchive.org/20100413151426/http://scienceandresearch.homeoffice.gov.uk/hosdb/publications/cctv-publications/DIP_2.1_16-Apr-08_v2.3_(Web)47aa.html?view=Standard&pubID=555512

- First Responder's Guide

- Forensic Science Regulator's Codes of Practice and Conduct
  http://www.homeoffice.gov.uk/publications/agencies-public-bodies/fsr/codes-conduct-practice?view=Standard&pubID=868070

- Network forensics and volatile data collection

- NPIA Forensics21 *HTCU Computer Examination Process, 2011*

- NPIA mobile phone SOPs

- Retrieval of Video Evidence and Production of Working Copies from Digital CCTV Systems v2.0
  http://tna.europarchive.org/20100413151426/http://scienceandresearch.homeoffice.gov.uk/hosdb/publications/cctv-publications/66-08_Retrieval_of_Video_Ev13c4f.html?view=Standard&pubID=585513

- SCDEA guidance

ACKNOWLEDGEMENTS

Review Board members
Paul Birch (Serious Fraud Office)
Lisa Burrell (Police Central e-Crime Unit)
Rick Conway (Surrey Police)
Steve Edwards (Police Central e-Crime Unit)
Dennis Edgar-Neville (Canterbury University/British Computer Society)
Danny Faith (NTAC/F3)
Steve Guest (IACIS)
Dan Haagman (7-Safe)
Sonny Hanspal (NPIA)
Keith McDevitt (SCDEA)
Jelle Niemantsverdriet (VerizonBusiness)
Bev Nutter (MPS-DEFS)
Harry Parsonage (Nottingham Police)
Peter Salter (PSNI)
Lindy Shepherd (Cranfield University)
Paul Slater (PWC)
Rob Watson (7-Safe)
Alastair Wilson (SCDEA)
Mark Wilson (MPS-DOI)
Paul Wright (VerizonBusiness)

Other acknowledgments

Esther George (CPS)
Jane Stevenson (Workplace Wellbeing)
Eddie Fisher (MPS-DEFS)

APPENDIX A

NETWORK FORENSICS

Home and corporate network environments

Networks of computers are becoming more common in the domestic environment and are well established in corporate settings. In the home, they are usually based around the broadband Internet connection, which often also offers functionality to set up a small internal (and often wireless) network within the household. In corporate environments, more advanced network setups can be found, for which no generic description can be given.

The use of wireless networks in both the corporate and home environment is also increasing at a considerable rate. To the forensic investigator, this presents a number of challenges and an increased number of potential artefacts to consider. Owing to the potential complexity of 'technical' crime scenes, specialist advice should be sought when planning the digital evidence aspect of the forensic strategy.

Wireless devices

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

- Network devices which connect individual systems or provide network functionality: Switches, hubs, routers, firewalls (or devices which combine all three).
- Devices to connect individual computers to the network, such as network cards (which can also be embedded within the computer)
- Devices to set up a wireless network: Wireless Access Points.
- Printers and digital cameras.
- Bluetooth (small range wireless) devices – PDAs, mobile phones, dongles.
- Hard drives which can be connected to the network.

Wireless networks cannot be controlled in the same way as a traditionally cabled solution and are potentially accessible by anyone within radio range. The implications of this should be carefully considered when planning a search or developing the wider investigative strategy. A device, such as a computer or a hard drive, may not be located on the premises where the search and seizure is conducted.

Home networks and data

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

With the widespread use of broadband type Internet subscriptions such as ADSL and cable, the Internet connection is nowadays likely to be of an 'always on' type connection. This implies that even if no-one is apparently working on a computer or using the Internet, there may be data passing to and from computers or between the network and the Internet.

If a wired network is present, there will usually be a small box (called a 'hub' or a 'switch') also present, connecting the computers together. Hubs, switches and routers look very much the same as one another. The network cables are usually connected at the rear.
The network may also be connected to another device (called a Cable Modem or a ADSL Modem) providing access to the Internet. Sometimes, the hub/switch/router mentioned before are combined with these modems in one device.

One wire from a modem will usually be connected to the telephone or television cable system and another wire will be connected either to one of the computers present or directly to the network hub, or the modem itself may be incorporated within the hub in a modem/router.

Operation planning in networked environments

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

Consider also the possibility of a computer's access to remote online storage, which may physically reside in a foreign jurisdiction. This can include web-based services for email, photo or document storage or other applications offered via the Internet. There will be legal issues in relation to accessing any such material. Legal advice should be sought prior to any access or retrieval and often the provider of the particular service will have to be contacted to ensure that material is preserved while the relevant mutual legal assistance requests are being arranged.

Network detection

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

- Identify and check network devices to see how much network or Internet activity is taking place. Consider using a wireless network detector to determine whether wireless is in operation and to locate wireless devices. Consideration should also be given to mobile Internet devices such as 3G or GPRS dongles or phones, which operate using the mobile phone network;
- As you do so, consider photographing the layout of the network and the location of the machines connected to it, so as to allow a possible future reconstruction;
- Once satisfied that no data will be lost as a result, you may isolate the network from the Internet. This is best done by identifying the connection to the telephone system or wireless communications point and unplugging it from the telephone point. Keep modems and routers running, as they may need to be interrogated to find out what is connected to them. Owing to their nature, it is particularly difficult to ascertain what is connected to a wireless network;
- Trace each wire from the network devices to discover the computer to which it is connected. This may not be possible in premises where cables may be buried in conduits or walls (advice in this case should be sought from the local IT administrator, if available, as to the set up of the system). Make a note of each connection. Note which computer is connected to which number 'port' on the network device (hub / switch / router or multi function device). Label each connection in such a way that the system can be rebuilt exactly as it stands, should there be any future questions as to the layout. It is highly recommended that pictures be taken of the setup;
- Consider making a connection to the access point/router in order to establish the external IP address. Most modern networks use Network Address Translation (NAT) which means that they communicate with an internal IP address and never get assigned and external IP one.

In a wireless environment, remember that no cables are used between a PC and other devices. However, there will still be some physical cabling to each device (which could include a network cable to the wired network, power cables etc.), the configuration of which should be recorded. Please also note that Cable / ADSL modems can have wireless capabilities built in.

- Once satisfied that the evidential impact is acceptable, you may remove each connection in turn from the network device once it has been identified. This will isolate each computer in turn from the network. The same can be done with cabling into wireless devices;
- Seize and bag all network hardware, modems, original boxes and CDs / floppy disks etc. (provided they are easily removable);

- Subsequently treat each device as you would a stand-alone device;
- Remember that the data which is sought may be on any one of the computers on the network. Officers should make a decision based on the reasonable assumption that relevant data may be stored on a device before seizing that device;
- Bear in mind the possibility that the network may be a wireless network as well as a wired one, i.e. certain computers may be connected to the network via conventional network cabling. Others may be connected to that same network via the mains system, and others may be connected via a wireless link;
- Also, bear in mind that any mobile phones and PDAs may be wireless or Bluetooth enabled and connected to a domestic network.

Concerns with remote wireless storage often focus around the inability to locate the device. In this instance, it would be impossible to prove that an offence had been committed. Artefacts on seized computers might provide evidence that a remote storage device has been used, however the analysis of such artefacts will take time and this cannot often be done during the onsite seizure.

Corporate network environments

When dealing with computer systems in a corporate environment, the forensic investigator faces a number of differing challenges. If the system administrator is not part of the investigation then seek their assistance. The most significant is likely to be the inability to shut down server(s) due to company operational constraints. In such cases, it is common practice that a network enabled 'forensic software' agent is installed, which will give the ability to image data across the network 'on-the-fly', or to a network share or a locally connected removable storage medium such as a USB hard drive.

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

By accessing the devices, data may be added, violating Principle 1 but, if the logging mechanism is researched prior to investigation, the forensic footprints added during investigation may be taken into consideration and therefore Principle 2 can be complied with.
In the case of large company networks, consider gaining the advice and assistance of the network administrator/ support team (assuming that they are not suspects).

VOLATILE DATA COLLECTION

In certain circumstances, it may be necessary or advisable for computer forensic investigators to gather evidence from a computer whilst its running or in a 'live' state. This technique has become a common practice as, even though some changes to the original evidence will be made, this method often allows access to evidence which would have been unavailable if the power is removed from a system. In order to capture volatile data on a device the device WILL have to be accessed. Therefore changes WILL be caused by the examiner.

Special consideration should be given to Principle 2 of the guidelines, as conducting live-forensics implies access to the original evidence. Any person doing this needs to be competent and fully aware of the impact their actions have and should be prepared to explain their reasons for taking this route.

Live forensics approach

By profiling the footprint of trusted forensic tools used to gather volatile data, the digital forensic examiner can understand the impact of using such tools and can explain any artefacts left by the tools.

In order to ensure that a consistent approach is used and the chance of errors is minimized, it is recommended to use a scripted approach using a number of basic and trusted tools. Regardless of the tools used, it is advisable to start with capturing the contents of RAM, the volatile memory.

If other tools are used before the contents of the RAM are stored, it is very likely that running the forensic tools will overwrite parts of the RAM.

Other examples of information, which might be available in the dump of the RAM contents, can be retrieved using different tools:

- listings of running processes;
- logged on and registered users;
- network information including listening, open and closing network ports;
- ARP (address resolution protocol) cache;
- Registry information.

The tools used to capture this volatile information are generally run from removable media like a USB stick, DVD or CD-ROM or a floppy disk. A USB stick is generally most convenient, as the output of the tools can be written back to the stick. Writing tool output to the original drive should be avoided whenever possible, as this changes the contents of the hard drive and can destroy potential evidence. Again, principle 2 does allow the investigator to do this, but a conscious decision will have to be made and the process written down.

When inserting USB devices the examiner must ensure that they know the details of the serial numbers of the devices they are connecting so that they can be eliminated when analysing the date captured.

When in doubt as to whether or not to use live forensics, consult with the digital forensic examiner for advice. And, it should be noted that in live forensics it is not always possible to know upfront which approach will yield the best results. Whichever method is chosen, remember to take meticulous notes – as dictated by principle 3.

Summary of steps

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

- Perform a risk assessment of the situation – Is it evidentially required and safe to perform volatile data capture?
- If so, install volatile data capture device to a removable data carrier (such as a USB stick) – preferably, this has already been done prior to starting the operation;
- Plug the data carrier into the machine and start the data collection script;
- Once complete, stop the device (particularly important for USB devices, which if removed before proper shutdown can lose information);
- Remove the device;
- Verify the data output on a separate forensic investigation machine (not the suspect system);
- Immediately follow with standard power-off procedure.

The capture and analysis of volatile data no doubt presents the investigator with technical challenges. However, as cases become more complex and connectivity between devices and public networks proliferate, with an increase in more advanced malware, which cannot always be retrieved using more traditional disk forensics, the above recommendations will need to be considered.

It is vitally important that only someone with the relevant training and is competent to do so should take any of these actions.

APPENDIX B

CRIMES INVOLVING WEBSITES, FORUMS, AND BLOGS

Where a crime involves evidence displayed on a website the most convenient method of recovering the evidence may be by engaging the assistance of suitably trained staff to visit the website and take copies of the evidential content. In order to do this the officer taking report of the matter needs to obtain the address of the website, for example, http://www.acpo.police.uk, or if it is a specific page within the site.

http://www.acpo.police.uk/about_pages/structure.html.

When carrying out any evidence recovery it is essential that an audit trail of all activity carried out by the investigator is recorded in a log. The recommended method for copying a website is to visit the site and record the relevant pages using video capture software so there is a visible representation of how they look when visited at the time. If video capture software is not available then the pages can be saved as screenshots. It is also advisable to follow this by capturing the web pages themselves either by using website copying software or saving the individual pages. Copying the pages themselves, as well as obtaining a visual record, means that the code from the web pages is also secured should that become relevant later.

This work should be conducted from a computer which has been specifically set up to be non-attributable on the Internet. Failure to use an appropriate system may lead to the compromise of other police operations. Anyone visiting a website generally exposes a certain amount of information to the website, for example it is common on police systems to have a web browser which is branded with the forces name. This branding is exposed to a website being visited and so may be recorded in logs on the site along with other information amongst which, will include the pages visited.

If it appears likely that the evidence on the website might be lost by a delay in carrying out the above procedures then the person reporting may be asked to make a copy of the evidence by whatever means they are capable of (either printing, screenshot or saving pages), alternatively this could be done by the person receiving the report. Before taking these steps every effort should be made to secure the services of a competent person to carry out this work as failing to capture the information correctly could have a detrimental impact on the investigation.

Where there is difficulty in capturing the evidence by visiting the site it might be possible to make an official request to the owner of the site by whatever legal procedures are required within the jurisdiction. The CSP/ISP SPOC or Digital Forensic Unit can usually advise on the appropriate procedures.

By making a request to the service provider hosting the site it may be possible to recover evidence of who has created the web page or posting. It is not unusual for details of the user such as name, address, phone number, banking details, email address, and alternative email address to be recorded by a host.

If there is a requirement to identify who has committed some activity on a website, for example where a fraud has been committed by purchasing goods from a website or by posting a message on a website, the likelihood is that the suspect may be traceable from logs on the site. When any user accesses the Internet they are allocated a unique address known as an IP address and their Internet Service Provider (ISP) keeps logs of the times and dates and the identity of the user allocated any IP address.

When a user visits a site and conducts some activity, for example logs on, posts a message, or makes a purchase, it is likely that the user's IP address has been logged by the website. It is often possible to obtain copies of logs from websites if there is a requirement to see who has been active on a website by making a request via the force CSP/ISP SPOC.

If the evidence is no longer available to be retrieved by any of the above means, and where the use of resources can be justified by the seriousness of the case, it may be possible to recover evidence of the site contents from an end user device that has been used to view the site by conducting a forensic examination of the device.

Where investigators wish to carry out open source intelligence research on the Internet they should be trained to do so and conduct the research from a computer which cannot be attributed to the investigator's agency.

Covert Interaction on the Internet

In circumstances where investigators wish to communicate covertly with an online suspect they MUST use the services of a Nationally Accredited and Registered (CII). CIIs have received specialist training which addresses the technical and legal issues relating to undercover operations on the Internet.

Crimes involving email communication

There are generally two methods of sending and receiving email, one by using a web browser and accessing email online for example at the Hotmail, Windows Live, Yahoo or Google websites. In these circumstances the mail is stored on the webmail server and is read through the user's browser. The other method is to access email using a program such as Outlook or Windows Mail to download mail to the user's computer. The program is used to view and store the emails locally.

Where the evidence in a case involves an email sent from a person who the police want to trace the key evidence is usually found in what is known as the email's "Full Internet Header". Each email sent over the Internet contains this header which is normally not visible to the user. It contains details of the route taken across the Internet by the email and includes the IP address of the sender. Even where an email has been sent with a fictitious email address which has been registered with false details, it is often possible to identify the sender from the Full Internet Header.

In order to obtain the Full Internet Header the person taking the incident report needs to ascertain which of the two methods the recipient uses to access their email. Where it is web based identify the webmail host (i.e. Hotmail, Yahoo etc.) or if by a program on the computer ascertain what program and version number of the program. The version number can usually be found in the program's Help on the menu bar under an item called "About".

Each webmail provider and email program treat the Full Internet Header differently and if the officer or user does not know how to display the header the details of the webmail provider or program need to be passed to a specialist in the Digital Forensic Unit or CSP/ISP SPOC who will be able to provide advice.

Once the header has been exposed the relevant email should be printed together with the header, and may also be saved electronically. Depending upon the seriousness of the case and the volume of email evidence, advice may be sought from the digital forensics unit on the most appropriate method of securing and retaining the email evidence.

Once the full header has been obtained the force CSP/ISP SPOC will be able to use this to conduct enquiries to attempt to identify the sender from the originating IP address.

Where an email address of a suspect is known but there is no email available from which a full header can be obtained, it may be possible to identify the user of the email address and their location. Depending upon the email service provider various details of the user may be recorded together with the first registration IP address and a varying period of IP address login history. These details may be obtained by making an appropriate CSP/ISP SPOC request for the email address. In conducting such enquiries it needs to be recognised that it is a trivial exercise to send an email with a false email address in the "From:" field of an email.

On some occasions the investigating agency might access a user's email account with written authority from the user in order to secure evidence. Where this is the case, if third party material is exposed as a consequence of viewing the user's emails, advice should be sought as to whether a Directed Surveillance Authority should be in place in addition to the user's authority. Even if the password and log in details are available. For example as a result of the Forensic examination authority and formal authority is required to access the email account.

Where justified by the investigation, consideration may be given to accessing messages on an email provider's server by obtaining the appropriate RIPA authority.

Crimes Involving Internet Chat

Users can employ a number of different devices to engage in chat on the Internet. There are three main ways to chat - using a website's chat facility, for example Facebook, using an instant messenger program like Windows Live Messenger, or much less commonly, using Internet Relay Chat (IRC).

Where an incident is reported which involves the use of chat the person taking the report needs to ascertain what method of chat was being used, i.e. what is the name of the website hosting the chat and its full Internet address, or what program is being used. The key evidence to be secured is

- any information which may identify the suspect party, and
- the content of any chat.

If the chat is web-based the details of the website, any chat room name and the user name of the suspect should be obtained together with the times and dates of any chat activity. If the chat facility is part of a social networking site the user will most likely have a unique ID number as well as a user name. This is usually visible in the web browser's address bar when viewing a user's profile or when the mouse pointer is moved over the user name. The force CSP/ISP SPOC or Digital Forensic Unit can provide help in finding this ID number. If the chat is by instant messenger program then the user name of the suspect should be obtained together with the associated email address which is usually available from the contact list of the person reporting. Generally a user's contact list can be accessed from any computer connected to the Internet so if it is considered that the user's computer might be retained for a forensic examination then it should not itself be used to access the contact list.

There is usually an option for a user to save chat logs but more often than not the default setting is for logs not to be saved. If the user has saved chat logs that contain evidence, the logs should be saved to removable media for production as evidence, if no removable media is available they should be printed out. Users are able to engage in chat from many types of device in addition to computers. Where the circumstances of the case warrant it, an end-user device could be submitted for forensic examination in order to recover evidence of the suspect's contact details and chat content.
Where a suspect's user details are obtained it may be possible to identify the suspect by making the appropriate CSP/ISP SPOC requests.

In the event that the chat has been conducted using IRC the following details should be obtained - the IRC program used, the name of the IRC server, the channel and any usernames. Further advice should then be sought from the Digital Forensic Unit.

Communications in the course of a transmission

Digital evidence in transit may be any form of communication using the Internet or a telecommunications network such as email, chat, voice calls, text messages, and voice-mail. Where such evidence is sought advice should be obtained from the force Covert Authorities Bureau.

APPENDIX C

CRIME SCENES

There are many different types of digital media and end-user devices, which may be encountered during a search of a crime scene, all of which have the potential to hold data which may be of value to the investigation. In order to preserve the data and achieve best evidence, these items must be handled and seized appropriately, and should be treated with as much care as any other item that is to be forensically examined. This section is intended to assist individuals to ensure their actions in relation to seizure are correct.

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.

Items found during a search will normally fall into the broad categories of computer-based media items, CCTV systems and mobile devices. These are considered separately below.

Proportionality

Before seizing an item, consider whether the item is likely to hold evidence (eg, is this a family computer or a computer belonging to a suspect?) Ensure that details of where the item was found are recorded. Consider when the offence was committed; when seizing CCTV, give consideration to narrowing down what is seized, by camera and/or time period. Check whether another system may be better placed to record the evidence. Differentiate between mobile phones found on a suspect and phones found in a drawer, as different levels of examination may be possible for these. Also consider that evidence may be stored online, or on an internet service provider's systems, and end-user devices may only be needed to obtain the details necessary to request this evidence from the service provider. If so, it is best to seize items in current usage, i.e. computers connected to the internet.

Digital devices and media should not be seized just because it is there. The person in charge of the search must have reasonable grounds to remove property and there must be justifiable reasons for doing so. The search provisions of PACE Legislation Codes of Practice equally apply to digital devices and media in England, Wales and Northern Ireland. In Scotland, officers should ensure they are acting within the terms of the search warrant.

Due regard should also be taken concerning any possible contravention of the European Convention of Human Rights.

What to take to a scene

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 digital systems as well as for their packaging and removal:

- Property register;
- Exhibit labels (tie-on and adhesive);
- Labels and tape to mark and identify component parts of the system, including leads and sockets;
- Tools such as screw drivers (flathead and crosshead), small pliers, and wire cutters for removal of cable ties;
- A range of packaging and evidential bags fit for the purpose of securing and sealing heavy items such as computers and smaller items such as PDAs and mobile phone handsets;
- Cable ties for securing cables;
- Flat pack assembly boxes - consider using original packaging if available;
- Coloured marker pens to code and identify removed items;
- Camera and/or video to photograph scene in situ and any on-screen displays;
- Torch;
- Forensically sterile storage material.

In addition, the following items may be useful when attending scenes to retrieve CCTV:

- Laptop with USB and network connectivity. A selection of proprietary replay software could be installed, to enable the downloaded data to be checked;
- External CD/DVD writer;
- USB hard drives.

Records to be kept

To comply with principle 3, records must be kept of all actions taken in relation to digital evidence, for example:

- Sketch map/photographs of scene and digital equipment;
- Record location and contact details;
- If a business, record opening hours;
- Details of all persons present where digital equipment is located;
- Details of digital items - make, model, serial number;
- Details of connected peripherals;
- Remarks/comments/information offered by user(s) of equipment;
- Actions taken at scene showing exact time;
- Notes/photographs showing state of system when found.

Computer based devices and media

This includes desktop or laptop PCs and Apple Macintosh systems, digital cameras, memory cards, USB sticks, external hard drives and games consoles, amongst other items. Mobile devices which have wireless connectivity/ communications capability (such as tablet computers and satellite navigation systems) fall under the heading of 'mobile devices'.

Systems which are powered on (running) need to be handled with care, as there is the potential to make unwanted changes to the evidence if these are not dealt with correctly. Such systems should only be accessed by appropriately trained officers In addition; volatile data of evidential value may be lost. Be aware of the potential to lose other valuable data, particularly when dealing with business systems, which could give rise to a claim for damages. In these cases expert advice should be sought before seizing a business system which is powered on.

Desktop and laptop computers/games consoles

The scene should be fully documented by written notes and/or a photographic record.
If a device is powered on, it needs to be handled carefully to preserve any volatile data and to avoid unwanted changes to the stored data.

Consider removing the device from any network, as devices can be remotely accessed, causing alteration to the data - but balance this against the possibility of losing data of evidential value, such as the list of currently open connections. If unsure, seek expert advice.

Seizure steps:

1. Secure and take control of the area containing the equipment;
2. Move people away from any computers and power supplies and do not allow any interaction with digital devices by suspect;
3. Photograph or video the scene and all the components including the leads in situ. If no camera is available, draw a sketch plan of the system and label the ports and cables so that system/s may be reconstructed at a later date;
4. Allow any printers to finish printing.

If switched off:

5. Do not, in any circumstance, switch the computer on;
6. Make sure that the computer is switched off, by moving the mouse – 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;
7. Be aware that some laptop computers may power on by opening the lid. Remove the battery from the laptop. Seize any power supply cables for future use.

If switched on:

8. Record what is on the screen by photographing it and by making a written note of the content of the screen;
9. Do not touch the keyboard or click the mouse. If the screen is blank or a screen saver is present, the investigator should be asked to decide if they wish to restore the screen. If so, a short movement of the mouse should restore the screen or reveal that the screen saver is password protected. If the screen restores, photograph or video it and note its content. If password protection is shown, continue as below, without any further touching of the mouse. Record the time and activity of the use of the mouse in these circumstances. (For games consoles, or tablet computers, the equivalent would be moving the controller joystick or touching the touchscreen);
10. If the system may contain valuable evidence in its current state (for example, if it is currently displaying a relevant document or an instant message conversation), seizing officers should seek expert advice from their local digital forensic unit as this may be lost if the power is lost. This is especially important if the suspect is a technically knowledgeable user who may be using encryption, as there may be no way to retrieve evidence stored in encrypted volumes once the power is lost;
11. Consider advice from the owner/user of the computer but make sure this information is treated with caution;
12. Remove the main power source battery from laptop computers. However, prior to doing so, consider if the machine is in standby mode. In such circumstances, battery removal could result in avoidable data loss. This is normally evident by a small LED (light) lit on the casing. In this case, officers should seek advice from their local digital forensic unit;
13. Unplug the power and other devices from sockets on the computer itself (i.e. not the wall socket). When removing the power supply cable, always remove the end connected 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 supply is fitted. If the equipment was switched on, do not close down any programs or shut down the computer, as this will cause changes to the stored data and may trigger wiping software to run, if this is installed;
14. Ensure that all items have signed and completed exhibit labels attached to them. Failure to do so may create difficulties with continuity and cause the equipment to be rejected by the digital forensic unit;
15. Search the area for diaries, notebooks or pieces of paper with passwords on them, often attached or close to the computer;
16. Ask the user about the setup of the system, including any passwords, if circumstances dictate. If these are given, record them accurately;
17. Allow the equipment to cool down before removal;
18. Track any cables that can be seen as they made lead you to other devices in other rooms.

Mobile devices

This includes mobile phones, smartphones, and other devices which may have wireless connectivity/communications capability such as tablet computers, personal digital assistants (PDAs), personal media players and satellite navigation systems.

1. Secure and take control of the area containing the equipment. Do not allow others to interact with the equipment;
2. Photograph the device in situ, or note where it was found, and record the status of the device and any on-screen information;

3. If the device is switched on, power it off. It is important to isolate the device from receiving signals from a network to avoid changes being made to the data it contains. For example, it is possible to wipe certain devices remotely and powering the device off will prevent this.

However, in exceptional circumstances the decision may be made to keep the device on. Timely access to the handset data is critical the decision may be made to leave the device switched on. Consideration may be given to place the handset in a Faraday environment to further prevent signal reception. In such circumstances advice should be sought from the DFU.

4. Seize cables, chargers, packaging, manuals, phone bills etc. as these may assist the enquiry and minimise the delays in any examination;
5. Packaging materials and associated paperwork may be a good source of PIN/PUK details;
6. Be aware that some mobile phone handsets may have automatic housekeeping functions, which clear data after a number of days. For example, some Symbian phones start clearing call/event logs after 30 days, or any other user defined period. Submit items for examination as soon as possible.

Handling and transporting digital evidence

Digital Devices

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

Hard disks

As for all digital devices protect from magnetic fields. Place in anti-static bags, tough paper bags or tamper-evident cardboard packaging or wrap in paper and place in aerated plastic bags.

Removable storage

floppy disks, memory sticks, memory cards, CDs/DVDs) Protect from magnetic fields. Do not fold or bend. Do not place labels directly onto floppy disks or CDs/DVDs. Package in tamper-force approved packaging to avoid interaction with the device whilst it is sealed.

Other items

Protect from magnetic fields. Package correctly and seal in plastic bags. Do not allow items to get wet.

Other Considerations

1. If fingerprints or DNA evidence are likely to be required, always consult with the investigator;
2. 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.

The 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. Dust, smoke, sand, water and oil are also harmful to electronic equipment. Some devices are capable of storing internal data (such as the time and date set on the system) 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 device for long periods before forensic examination and should be addressed in local policy.

APPENDIX D

DEVELOPING A DIGITAL INVESTIGATION STRATEGY

The investigation of crimes and incidents in which digital evidence is involved, particularly the Internet, presents some unique challenges to the investigator. The explosion of the availability and use of technology, the growth of virtual storage, development of 'Cloud Services' (online services) and the convergence of mobile and traditional computer technology has resulted in most investigations having a digital element of some description.

Investigators need to have a greater understanding of the use of digital evidence if interviews of witnesses and suspects are to be effective. This is particularly the case in serious or complex investigations where a failure to identify and secure volatile digital data could have a significant impact on the conduct of the investigation.

It is important that investigators develop appropriate strategies to identify the existence of digital evidence and to secure and interpret that evidence. Irrespective of the size or complexity the investigator should consider five primary stages.

- Data Capture and search and seizure at crime scenes;
- Data Examination;
- Data Interpretation;
- Data Reporting;
- Interview of Witness and Suspects.

Investigators should seek the advice of their force Telecoms/ISP SPOC, Network Investigators and Digital Forensic Units at the earliest opportunity to formulate a written digital forensic strategy.

Due consideration should always be given by the investigators of the benefits to the overall investigation of conducting any digital forensic work

DATA CAPTURE STRATEGY

The investigator should develop a Data Capture Strategy to identify and secure all relevant digital evidence. Other than a requirement to react to immediate events the investigator should be able to plan this strategy in advance.

Where a crime or incident is reported, early consideration should be given to the potential to glean evidence from the Internet or end user devices which have a digital memory capacity and from which evidence / intelligence may be retrieved.

Social Network Sites

Priority – Establish the use of Social Networking, Online Communities, Online Storage and other Cloud Services by witnesses and suspects. Whilst this may be revealed by the examination of seized devices it may be gleaned more quickly if asked during interview.

Many current investigations involve Social Networking Sites. It is imperative that early consideration is made around securing Social Networking Profiles that fall within the investigation. The best evidence is available from the service provider however they are often located outside of the UK and may or may not secure the content on the appropriate request via the force CSP/ISP SPOC. As such the investigator should always secure a copy of what is seen by them as this may be the only opportunity to secure this evidence before it changes.

Open Source Research

The internet is a huge repository of information much of it of value to the investigator. Research by properly **trained** staff, preferably with access to a stand alone computer, will enable the investigator to get the best from the vast amount of information that is now held online. In addition to this the force CSP/ISP SPOCs will be able to give advice on the type of data that can potentially be obtained from ISP's, web mail and web based providers.

Care should be taken when undertaking Internet research from any computer linked to the Police National Network (pnn) as a digital footprint will be left and may reveal the law enforcement interest. This will not be obvious to the general internet user but will most certainly be clear to the hosts or providers of the service and those who are particularly technically aware and monitoring IP addresses.

Registration details are often asked for and whilst in some instances they will inevitably be fictitious, on many occasions they will include the following;

- IP log on;
- Name and Address;
- Landline and Mobile phone Numbers;
- Banking data;
- Emails used;
- Username and passwords;
- Linked accounts.

Whilst law enforcement are used to working with RIPA, RIPSA and the DPA to obtain information this legislation only applies within the UK. Many services are based outside of the UK based organisations.

It is essential that the CSP/ISP SPOC is engaged at the earliest opportunity to these enquiries with the objective of preserving known time critical data.

National Technical Assistance Centre (NTAC)

If encrypted files are located or suspected it is important that the suspect is asked for them, failure to do so may result in an offence under sec 49 of RIPA. Encryption is difficult to break and assistance can be sought via the Digital Forensic Unit from the National Technical Assistance Centre (NTAC) in London.

The National Technical Assistance Centre (NTAC) provides technical support only to public authorities, particularly law enforcement agencies and the intelligence services. It includes a facility for the complex processing of lawfully obtained protected electronic information.

NTAC is the leading national authority for all matters relating to the processing of protected information into an intelligible format and the disclosure of key material.

All public authorities should consult with NTAC at the earliest opportunity when considering exercising the powers in Part III of the Regulation of Investigatory Powers Act (RIPA).

A public authority cannot serve any notice under Section 49 of RIPA or, when the authority considers it necessary, seek to obtain appropriate permission, without the prior written approval of NTAC.

Investigating Crimes where Digital Evidence may be present

The proliferation of digital devices and the advances in digital communications mean that digital evidence is now present or potentially present in almost every crime.

Digital evidence can be found in a number of different locations,

- Locally on an end-user device - typically a users computer, mobile/smart phone, satellite navigation system, USB thumb drive, or digital camera;

- On a remote resource that is public - for example websites used for social networking, discussion forums, and newsgroups;
- On a remote resource that is private – an Internet Service Provider's logs of users' activity, a mobile phone company's records of customers' billing, a user's webmail account, and increasingly common, a user's remote file storage;
- In transit – for example mobile phone text messages, or voice calls, emails, or Internet chat.

Investigating Different Types of Crime and Identifying Sources of Evidence

It would be quite common for evidence of a crime to be in more than one of the locations mentioned above. However it might be much easier to obtain the evidence from one location rather than another; careful consideration should be given to the resources required to obtain the evidence.

For example, if evidence is required of contact between two mobile phone numbers, the best method would be to obtain call data from the Communication Service Providers via the force SPOC, rather than to request a forensic examination of the mobile phones. The call data is likely to be more comprehensive than call logs from a mobile phone and the times and dates can be relied upon, which is not necessarily the case with logs from a mobile phone.

COVERT FORENSIC COMPUTING

Some investigations may require consideration of gathering digital intelligence in a covert manner. It is evidently not appropriate to discuss covert tactics within this document however opportunities exist to capture digital data online and physically from devices in a covert manner where the appropriate authorities are in place.

DATA EXAMINATION STRATEGY

Devices seized as part of a search will be forwarded to the force Digital Forensic Unit in accordance with force policy.

The investigator needs to properly consider the nature and purpose of the digital examination.
The investigator must tailor the needs of the digital examination not only based on the investigation requirements but the ability of the Digital Forensic Unit to deliver it. The better the briefing the better the advice will be.

The Investigator must be clear on what priorities are placed on the examination as it may well be, as previously stated, that key information needs to be found in order to preserve evidence that may exist elsewhere. This is particularly the case where it relates to the existence of additional evidence, offenders and victims. A preview of content may be appropriate albeit the limitations of this approach will require to be properly understood.
Priorities may also be set on the type of data to be extracted and viewed by persons other than the Digital Forensics Unit as this may reduce the burden on the unit and increase the likelihood of the delivery of the data. This will of course depend on the nature of the examination. But could include;

- Internet History;
- Emails;
- Evidence of webmail;
- Instant Messaging Logs;
- Media Files (images & videos);
- Social Networks;
- Forums & Chat Rooms;
- Cloud Services / Virtual Storage;
- File Sharing programs;
- Usernames / Passwords;
- Encrypted Files;
- Word Documents;
- Spreadsheets.

The discussion between the investigator and digital forensic unit should result in an agreed digital extraction / examination plan to achieve an agreed outcome. The plan may need to be reviewed as the evidential picture and priorities change.

DATA INTERPRETATION STRATEGY

Staff tasked by the investigator to undertake the digital data extraction / examination must be competent to do so and have had sufficient training to undertake the task assigned to them. It must be borne in mind that the development of digital technology is dynamic and the examiners may well face significant challenges to their knowledge.

It is the role of the Digital Evidence Examiner to provide the investigator with a report/statement accounting for the examination of the devices as part of the investigation. The report should account in full for the parameters set for the examination, data extracted and data examined. There should also be provision to provide an interpretation of technical aspects of the examination relevant to the provision of evidence in the case.

The investigator should have a full discussion with the examiner ahead of the production of any reports to ensure all the relevant evidence is contained in the report and that the processes used adhered to the ACPO Principles governing handling digital based evidence. These principles are explained in the section headed "The Principles of Digital Evidence" in this guide.

DATA REPORTING

The report is the ultimate product of the examination. It should outline the examination process and the significant data recovered. Whilst an initial report may be relatively brief, the examiner should be in a position to produce a full technical report should one later be required.

Examination notes must be preserved for disclosure or testimony purposes and, if required, the preparation of a full technical report. 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 their experience and qualifications to conduct the examination.
The role of the examiner is to secure from any seized material true copy of any data that they may contain Forensic hardware should be subject to initial and periodic testing. . It is worth repeating at this point that full records should be made of all actions taken. These can be made available to the defence who may subsequently cause a further examination to be conducted. A significant part of such an examination will be to validate the actions and results of the original examination. Such records are also part of the unused material for the case under investigation.

It is important to remember that legislation continues to change to keep up with technological and societal change. It is important, therefore, to consider the legal requirements and restrictions when examining digital evidence. Recent case law and precedents set at higher courts are important considerations when preparing an evidence package for an investigator This applies, in particular, to the use of the Internet and files downloaded from the Internet; or material accessible from foreign jurisdictions i.e. online data stores.

<u>Interview of Witnesses and Suspects</u>

The interview of witnesses/suspects is a crucial opportunity to identify key information about the nature and use of digital data relative to the investigation in hand. As such those involved must be properly briefed and competent to undertake the interview having the necessary understanding of the areas to explore.

Consideration should be given to consulting with a trained Interview Advisor with a view to the compilation of an appropriate interview strategy.

Bear in mind that the digital examination of devices seized will take time and may not necessarily reveal vital information that the witness / suspect may be aware of. Typically this may include;

- Web Mail Addresses / Username & Passwords / shared or sole use;
- Social Network Profiles / Username & Passwords / shared or sole use;
- Use of Forums & Chat Rooms / Username & Passwords;
- Use of Cloud Services / Username & Passwords / shared or sole use;
- Use of Virtual Storage / Username & Passwords / shared or sole use;
- Use of Role Play Gaming Sites / Username & Passwords / shared or sole use;
- Use of Auction sites / Username & Passwords / shared or sole use;
- Use of Online Banking;
- List of User Names;
- Use of Encryption / Encryption Keys;
- User Names of contacts;
- Use of the devices;
- Websites Visited;
- Internet Service Provider.

This list is not exhaustive

WORKBOOK FOR THE CREATION OF ACPO GUIDANCE/PRACTICE ADVICE

This workbook, with all sections completed, must be included in the final document as an Appendix and submitted, through the Head of the Business Area, to the Programme Support Office for quality assurance prior to submission to Cabinet for approval as ACPO Doctrine.

ACPO EQUALITY IMPACT ASSESSMENT TEMPLATE (DIVERSITY AUDIT) AS AGREED WITH THE CRE

1. Identify all aims of the guidance/advice

1.1 Identify the aims and projected outcomes of the guidance/advice:
To provide coherence to police policy and practice in relation to evidence obtained from digital media
1.2 Which individuals and organisations are likely to have an interest in or likely to be affected by the proposal?
Police, CPS, HMRC, SOCA, CEOP, SFO, PCeU, SCDEA

2. Consider the evidence

2.1 What relevant quantitative data has been considered?	
Age	N/A
Disability	N/A
Gender	N/A
Race	N/A
Religion / Belief	N/A
Sexual Orientation	N/A
2.2 What relevant qualitative information has been considered?	
Age	N/A
Disability	N/A
Gender	N/A
Race	N/A
Religion / Belief	N/A
Sexual Orientation	N/A
2.3 What gaps in data/information were identified?	
Age	N/A
Disability	N/A
Gender	N/A
Race	N/A
Religion / Belief	N/A
Sexual Orientation	v
2.4 What consideration has been given to commissioning research?	
Age	N/A
Disability	N/A
Gender	N/A
Race	N/A
Religion / Belief	N/A
Sexual Orientation	N/A

3. Assess likely impact

3.1	**From the analysis of data and information has any potential for differential/adverse impact been identified?**
Age	N/A
Disability	N/A
Gender	N/A
Race	N/A
Religion / Belief	N/A
Sexual Orientation	N/A
3.2	**If yes explain any intentional impact:**
Age	
Disability	
Gender	
Race	
Religion / Belief	
Sexual Orientation	
3.3	**If yes explain what impact was discovered which you feel is justifiable in order to achieve the overall proposal aims. Please provide examples:**
Age	
Disability	
Gender	
Race	
Religion / Belief	
Sexual Orientation	
3.4	**Are there any other factors that might help to explain differential/adverse impact?**
Age	
Disability	
Gender	
Race	
Religion / Belief	
Sexual Orientation	

4. Consider alternatives

4.1	**Summarise what changes have been made to the proposal to remove or reduce the potential for differential/adverse impact:**
N/A	
4.2	**Summarise changes to the proposal to remove or reduce the potential for differential/adverse impact that were considered but not implemented and explain why this was the case:**
N/A	
4.3	**If potential for differential/adverse impact remains explain why implementation is justifiable in order to meet the wider proposal aims:**
N/A	

5. Consult formally

5.1 Has the proposal been subject to consultation? If no, please state why not. If yes, state which individuals and organisations were consulted and what form the consultation took:	
Early drafts of the work have been consulted on with law enforcement and those in the specialist ecrime private sector.	
Age	N/A
Disability	N/A
Gender	N/A
Race	N/A
Religion / Belief	N/A
Sexual Orientation	N/A
5.2 What was the outcome of the consultation?	
Additional revisions based on good practice in this specialist area of investigation. There were no revisions based on the 6 diverse areas.	
Age	N/A
Disability	N/A
Gender	N/A
Race	N/A
Religion / Belief	N/A
Sexual Orientation	N/A
5.3 Has the proposal been reviewed and/or amended in light of the outcomes of consultation?	
5.4 Have the results of the consultation been fed back to the consultees?	

6. Decide whether to adopt the proposal

6.1 Provide a statement outlining the findings of the impact assessment process. If the proposal has been identified as having a possibility to adversely impact upon diverse communities, the statement should include justification for the implementation:
N/A

7. Make Monitoring Arrangements

7.1 What consideration has been given to piloting the proposal?
N/A
7.2 What monitoring will be implemented at a national level by the proposal owning agency and/or other national agency?
N/A
7.3 Is this proposal intended to be implemented by local agencies that have a statutory duty to impact assess policies? If so, what monitoring requirements are you placing on that agency?
N/A

8. Publish Assessment Results

8.1 What form will the publication of the impact assessment take?
N/A