Sponsorship Acceptance Statement

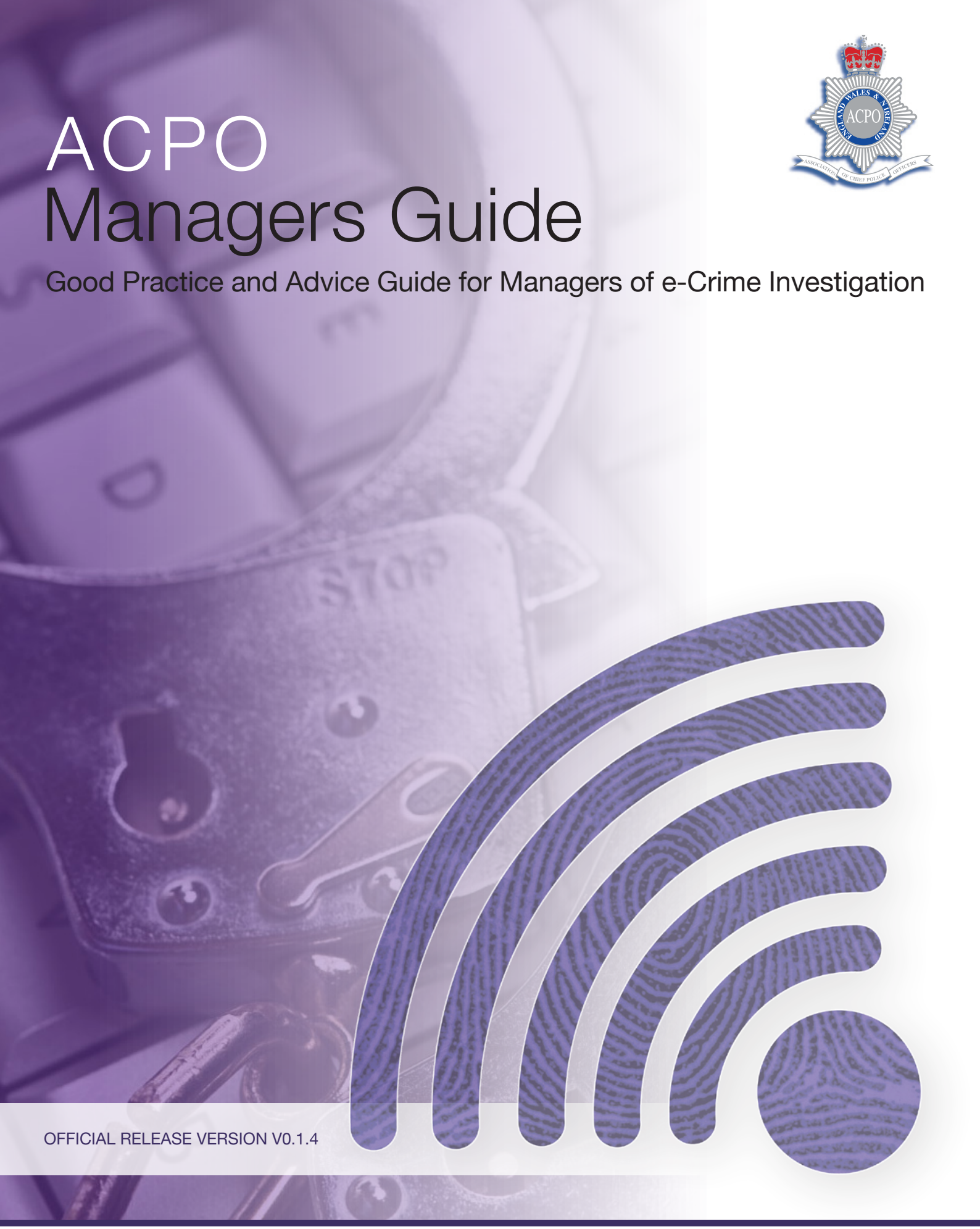
This document has been generously sponsored by 7Safe – content input and the provision of design & publication resources.

The sponsorship has been accepted by the Metropolitan Police Authority, on behalf of ACPO, pursuant to Section 93 of the Police Act 1996.

The ACPO Good Practice Guide for Managers of e-Crime investigation published by 7Safe. For more information visit www.7safe.com

ACPO Managers Guide

Good Practice and Advice Guide for Managers of e-Crime Investigation



OFFICIAL RELEASE VERSION V0.1.4

Supported by 7safe information security

www.acpo.police.uk

It gives me great pleasure to introduce this updated version of the ACPO Good Practice and Advice Guide for Managers of e-Crime Investigation. I would like to congratulate all those who participated in the compilation of this useful guidance document.

I have held the ACPO Lead for e-Crime since 11 April 2008. The creation of this portfolio has been in direct response to the Government and cross-party concern around the dramatic rise in e-Crime offences. Recent figures from the British Chamber of Commerce show a 74% increase on the previous years figures and is the biggest increase since research in this area began. It is estimated that only one in eight e-crimes is reported and that this equates to one fifth of all reported crime at a cost of £12.6 billion.

Criminal behaviour has shifted to take advantage of electronic mediums and serious and organised criminal networks have become increasingly sophisticated. Corporations, Government departments and businesses now need to invest considerable sums in order to protect their assets and data. Lloyds of London have stated that they are defending up to sixty attacks a day on their corporate infrastructure.

Policing needs to equip itself with the necessary skills and knowledge to meet this new challenge.

I recommend this guidance and the application of its principles to both practitioners and managers in the on going battle against e-Crime.

Janet Williams QPM
Deputy Assistant Commissioner
Metropolitan Police Service

ACPO Lead for e-Crime

www.7safe.com

I am delighted that 7Safe is able to provide support this ACPO publication, following similar sponsorship of the Good Practice Guide for Computer-Based Electronic Evidence.

From our company's involvement in data security breach investigations, it is abundantly clear that electronic crime is rising in volume as well as becoming increasingly more complex. It is therefore no surprise that this guidance document has been updated.

Compared to traditional crime, the so called 'cyber criminal' has several advantages, including:

- Potential anonymity
- Remote and cross-border opportunities
- Speed of attack
- Automation and amplification

With the appeal of such factors it is understandable that this genre of crime has grown so rapidly. The challenge is to maintain a thorough understanding and working knowledge of e-Crime, which is a challenge that I believe the Police service will continue to overcome.

Alan Phillips
Chief Executive Officer
7Safe

Contents

Introduction

The Internet, computer networks and automated data systems present wide ranging opportunities for criminals, including organised criminal networks, to partake in an extensive variety of offences; this presents a significant challenge to law enforcement globally.

One of the principal difficulties facing the law enforcement community is how best to tackle the complex and dynamic developments associated with the Internet, Digital Information and evolutions in communications technology. This creates difficulties in the consistency of approach and enforcement nationally; there is a clear need to harmonise practices and procedures throughout the UK. At the same time it should be possible to learn how best to develop and share the experience and skills within British Policing has.

As technology plays and increasingly important part of our lives it is essential to understand the challenges faced by investigators and digital forensic practitioners when dealing with digital evidence, virtual crime scenes and complex communications data. Managers and senior managers need to maintain an awareness of the ever increasing demands for digital forensic services and technological support to mainstream investigations, so that in house specialist providers are adequately supported.

The following issues are fundamental to the support of specialist service practitioners:

- A recognition that digital evidence and communications data are integral to an ever increasing number of mainstream criminal investigations.
- Management commitment to provide sufficient capacity to recover, process and analyse digital evidence.
- A commitment to specialist training for digital evidence recovery staff, network investigators and covert Internet investigators, which also allows for regular refresher updates
- A programme of continual professional development
- A commitment to adequate funding
- A commitment to quality
- An acknowledgement of the importance of digital forensics, open source intelligence gathering and network investigation
- An understanding of the issues and difficulties faced by specialist investigators
- Understanding the necessity of regular upgrading and renewal of equipment
- Making allowances for the challenges in projecting budget spend in the normal five year predictive cycle
- Attending a High Tech Crime Managers' course designed to de-mystify the challenges arising from the recovery and analysis of digital evidence, use of the Internet as an investigative tool and the managerial issues associated with these activities.

In return the force will benefit from:

- Effective specialist capabilities to support criminal investigations of all types
- A very valuable resource for investigators
- A relatively cheap way of gathering intelligence and / or evidence that would otherwise have not been possible or far more costly
- The maintenance of an up-to-date operational capability

The rate of technological change in our society has been and continues to be dramatic, the pace of change is likely to accelerate rather than slow down. New computer operating systems promise seamless encryption to protect data and messaging whilst solid-state technology will produce new forensic challenges. These technological advances provide many new opportunities for criminals to exploit.

Consequently law enforcement agencies must invest in the skills and resources necessary to police the ever changing digital environment.

If the law enforcement community is to continue to prevent and reduce crime, improve the quality if investigations as well as the administration of justice it is absolutely vital that Senior Management understand and address the challenges associated with the Internet and digital evidence, in all its forms.

The issue of commonality and overlap is a real one. Without doubt there are issues, particularly in respect of the Internet, which impact on all other areas of criminality. Terrorism, Child Protection, Vice, Paedophilia and Fraud are examples where this particularly applies. It is important to understand the message that computers and the Internet provide opportunities not only for the commission of new offences, but also for the commission of **traditional crime.**

Conclusion

The collection and analysis of digital evidence is a dynamic and rapidly developing area of law enforcement work and it will continue to be so for the foreseeable future. It will require much careful thought if we are not to miss opportunities or neglect to plan and put in place capability for future demands.

There is a significant operational need to provide an effective capability that can meet the demands of a rapidly changing digital world. Law enforcement must constantly evaluate the current and future threats in order to equip and train our staff to meet that threat.

While local initiatives are vitally important it is also essential for the Law Enforcement community as a whole to be able to benefit from such efforts. An international, well communicated and co-ordinated approach is needed.

With digital systems providing boundless opportunities to industry, the public and criminals alike, there has been a significant increase in the number of private sector investigators. It is therefore necessary to understand that Law Enforcement will often need to liaise closely with these private sector bodies and to provide a consistent and coordinated approach.

It is important that the disciplines of Network Investigation and Forensic Analysis are not confused with network administration expertise. As one would not expect a General Practitioner to be an expert in forensic pathology, one cannot expect an IT network specialist to be knowledgeable in the forensic field. These disciplines are still developing and it is too easy to assume that computer knowledge is forensic knowledge.

This Guide should be read in conjunction with the ACPO Good Practice Guide for Computer Based Electronic Evidence, the ACPO e-Crime Strategy, the Strategic Stakeholders Group Protocol and the ACPO Manual of Standards for Covert Internet Investigations.

In preparing this document a 'Template for Discussion' was formulated which practitioners have said is a very useful 'Health Check'. It is therefore included as an Appendix.

This is a dynamic document which will be required to be regularly updated as technology, the law and practices evolve.

"We never know what we do not know" – Anon

Initial set–up

Initial set–up

Since the first ACPO Guide for Managers of High Tech / Computer Crime Units was published the technological landscape has transformed beyond recognition with the following factors being instrumental in its continuing development:

- Affordability
- Technology convergence
- Social change
- Economic change
- Virtualisation

All these factors have a net result of increasing the type and volume of equipment that we can consider as potential evidence, either in the personal possession of a suspect or present at a crime scene. Similarly technological advances have increased the many different ways criminals have of perpetrating, recording or supporting their criminal activity. This manifests itself in very tangible terms within digital forensic units by way of ever increased workload. Only a few years ago the digital forensic investigator would have had to examine one solitary computer, usually all that would be recovered during the execution of a domestic search warrant. Typically such a computer would have a 20 Gigabytes (GB) hard drive but now investigators are seizing two, three or more computers and a host of other digital devices during the routine execution of search warrants, often amounting to Terabyte's of data. It is not just the volume of digital evidence seizures that has increased but importantly, the volume of data requiring to be examined has risen to levels that would have been unimaginable only a few years previously. Even though the tools and equipment to carry out digital forensic examinations have improved considerably, they on their own are unable to keep pace with the volumes of data being submitted for investigation.

Putting the size of this data into some context may be helpful. The average hard drive selling today in desktop computers is typically between 500 GB and 750GB. 1 MB of data has the ability to produce a pile of A4 paper containing printed text measuring 2.5cm in height. 3.6GB of data has the ability to produce the same A4 paper to a height equivalent to the Statue of Liberty.

The following chapter provides information on the factors involved in the initial setup of a digital forensics, high tech, computer or e-crime unit and will touch on areas that are described in greater detail within this guide.

Role Definition

It should be considered that while technology presents opportunities to criminals it also presents significant opportunities for law enforcement and these can be exploited by properly trained and resourced: intelligence units, online proactive units and digital forensics units. The proliferation of technology within criminal investigations prompted ACPO to redefine its definition of e-Crime which it identified as "The use of networked computers or internet technology to commit or facilitate the commission of crime."

This interpretation of e-Crime has accelerated its mainstreaming within the police service. Today's reality is that virtually every criminal investigation involves some form of digital evidence or communications data, requiring investigators to seek the assistance or advice of in house specialist staff. As a result the role of staff within e-Crime Units continues to broaden and develop in respect of their role and the skill base which they require. There are two general spheres of activity within e-crime unit's namely forensic analysis of digital evidence and network investigations.

Forensic: : "To secure and retrieve evidential material from digital media, mainly computers, to produce such evidence in a form which is admissible in Court, to provide technical advice and support to officers encountering such media during investigations into computer crime or where a computer or digital media have been used in the commission of and such crime".

Network: "To conduct investigations and operations into network based criminal activity to detect Hi-Tech crime, to gather and disseminate relevant and quality intelligence, to provide technical advice and assistance to officers engaged in the investigation of Hi-Tech crime and to produce evidence in a form which is admissible in Court."

Forensic

The above definitions are drawn from the first version of this guide, published by the National High Tech Crime Unit (NHTCU), which now forms part of the Serious Organised Crime Agency. There is heavy emphasis on the term computer within both definitions, however with advances in mobile phone technology the line between computer and mobile phone has blurred and in many cases one device has the functionality of both. Consequently potential sources of digital evidence are much more prevalent. The examination of mobile

phones is now a major component within the work many digital forensic units, since they offer a highly significant evidential source. Additionally personal navigation devices, gaming consoles, digital music players, digital cameras and memory sticks represent only a few of the many sources of digital evidence that could hold vital evidence. The forensic recovery of digital evidence is no longer solely laboratory based and the ability to recover digital evidence from a wide variety of sources "in the field" should be a major consideration for managers in establishing an effective operational capability. This increasingly necessitates the ability to conduct the forensic recovery of digital evidence from live networks, both wired and wireless, as well as stand alone live computer devices.

Network

The role of the network investigator has similarly developed since this definition was first developed. A network investigator cannot undertake the investigation of every allegation of crime which involves technology in some form, such is its volume and any expectation to the contrary is unrealistic. The broad remit of this role is a is to conduct investigations across computer networks, including the Internet, particular techniques include "open source" research as well as Covert online activities, against a range of criminality. Open source research can potentially provide investigators with a great deal of background material, which traditionally may only have been obtainable with the deployment of physical surveillance assets. The material may be used for intelligence or evidence as dictated by circumstances. To thoroughly and properly produce this material to an evidential standard requires equipment and appropriately trained officers. To maintain continuity it would be best if these were dedicated officers, operating within intelligence or other specialist units.

Consideration should be given to the removal of low level taskings from specially trained Network Investigators, such as requests for Internet research, to staff who are equally equipped to deal with such matters. This could include intelligence professionals who have attended the NPIA 'Researching, Identifying and Tracing the Electronic Suspect' (RITES) course. Staff conducting such research can escalate this at any time to a higher qualified professional based within a specialist unit or seek assistance from a specialist unit as required. Network investigators may be best placed to deal with serious or sensitive enquiries. Such a member of staff would have at their disposal accounts for enquiries within most of the social networking sites. They would also have knowledge of which websites to prioritise and methods for finding and retrieving the data.

For proactive, interactive research with online suspects CII can be consulted for advice and guidance, via a deployment officer, as to the best approach or the options available including application for CII deployment and a directed surveillance authority under RIPA 2000.

The management procedures for CII deployments need to include the protocols for the management of intelligence produced by such deployments and the management of a robust firewall between intelligence and potential or actual evidence. Managers must note that CII work requires privacy and seclusion during operations so as not to distract or interrupt the flow of a live operation.

The role of a modern technical specialist investigative unit, commonly referred to as High Tech Crime / Computer Crime or E-Crime units, is both wide and varied and can extend far beyond their core functions. This should be considered by line management in determining the resources required. These wider roles can include:

- To be the centre of excellence within the respective police service for all matters relating to the seizure and retrieval of digital evidence, including the preservation of Internet content
- Advice/Assistance re Judicial Orders
- Obtaining Judicial Orders
- Advice and guidance re submissions to the Communications Data Single Point of Contact (SPOC)
- Attendance at Case Conferences to deal with technical matters
- Assistance with interviews where technical matters are likely to arise, particularly where suspect(s) are believed to have a high level of technical expertise
- Dealing with defence requests to view digital evidence
- Preparation of statements or reports detailing evidence/ material found
- Presentation of evidence at Courts, Judiciary or the Crown Prosecution Service (CPS)
- Advice to Senior Investigating Officers (SIO's)
- Advice and guidance on e-crime prevention to local business groups i.e. Rotary, Chamber of Commerce etc

- Advice and guidance to education facilities within the respective police service area
- Delivery of training across the respective police service including Student Officers, Trainee Investigators, SIO courses, First Responder Training and Search Teams
- Promulgation of best practice and policy in respect of specialist crime prevention and evidence handling across the organisation

Training Issues

The training of the wider law enforcement community outside any specialist investigative unit should be viewed as essential in raising the standard of service that is delivered to the community. This is particularly relevant in respect of crime scene preservation and the seizure of digital evidence, including the handling of mobile phones. This training may be of a bespoke nature to address a particular need or delivered in partnership with bodies such as the National Police Improvement Agency (NPIA) at a local level as well as centrally by the NPIA itself. It is often the case that personnel within specialist investigative units are best placed to deliver this training "in service" due to their technical knowledge, local procedures and in order to promote organisational learning. Managers should be aware that such a training function however can rapidly become a large abstraction on a specialist unit's resources. Due to widely reported issues in respect of underreporting, Units around the country have identified a large appetite within the business community to engage with law enforcement regarding the threats and risks relating to online crime. Units may benefit from developing strong links with the local business community as well as local government. This could assist in identifying the true picture of e-Crime and establishing a robust response to it as well as developing a greater confidence in police capabilities. Again this may require the input of trained personnel, with a strong technical knowledge, in order to fully identify and address relevant issues and provide the necessary support and advice where required.

Strong consideration should be given to the establishment of an Operational Level Agreement (OLA) between any specialist investigative unit and the wider law enforcement agency in order to clearly identify the areas in which the unit will have responsibility, performance indicators, case acceptance criteria, tasking protocol, etc..

Inwardly within the unit there should be a clear identification of roles and responsibilities of the personnel assigned with a regular review in the face of continuing technological development. Where applicable within units it is essential that steps are taken to prevent any contamination between evidential and intelligence matters in accordance with national policy in this area.

Budget

Previously there existed additional central Government funding for e-Crime Units as part of the National High Tech Crime (2000) strategy, this was developed to attain a minimum benchmark standard of capability across police services. This funding is no longer available and units must now rely on funding exclusively from their respective organisations in the face of competing organisational demands.

The costs associated with running a specialist investigative unit within a law enforcement agency in terms of personnel, equipment and training is a significant drain of resources but the overall value for money represented by such an asset can often be overlooked. It is widely accepted that the cost of developing and maintaining this essential modern day policing investigative service is far cheaper than outsourcing large numbers of computer and mobile phone examinations, although in certain operational circumstances this may be the preferred option. There is also a much greater opportunity to quality control services provided internally, as opposed to those contracted in. The benefits to law enforcement are not only financial but importantly the wider quality of service benefits, such as much easier communication with the case officer, provided by an in house investigative asset.

It is recommended that law enforcement agencies develop their specialist investigative assets in a manner that allows them to provide a comprehensive service in keeping with that required by a modern police service or investigatory agency. Adequate resourcing will allow law enforcement agencies to take full advantage of technology in the fight against crime and to mitigate the significant corporate risk represented by forensic backlogs and a lack of overall capability. Line management in charge of units should identify and fully exploit additional revenue sources such as local government funding where available, appropriate partnerships with the business community and the Proceeds of Crime Act (POCA).

Initial set–up (cont.)

Personnel

The selection of the right personnel to perform the various functions within any specialist investigative unit is absolutely vital. It is therefore important to have in place a selection procedure for personnel which identifies those best suited for a role within that department. It is recommended that this includes some level of intermediate written test for applicants in order to fully ascertain their levels of knowledge pertinent to the role they are seeking. Consideration should also be given to the need for additional vetting of applicants and / or security clearance relevant to their prospective role. Managers should be aware that ALL units whose role involves the forensic examination of digital media will invariably come across Indecent Images of Children (IIOC) and it may involve material concerned with National Security and other highly sensitive information. These issues have implications in respect of the health and safety of staff as well as the security and handling of seized / copied material, these should be addressed in the Standing Operating Procedures (SOPs) of the unit.

The retrieval and examination of digital evidence is no different to any other aspect of a criminal investigation. The digital evidence investigator must be aware of: the law; rules of evidence; exhibit handling; the continuity of evidence; the need to remain impartial and disclosure. This is particularly important within the Network Investigator role where detailed knowledge of relevant legislation and full police powers are essential in often sensitive areas of work. Most specialist investigative units now comprise of a mixture of police officers and police staff and managers must accept that there is a requirement for additional training in relevant law, exhibit handling and continuity as well as the presentation of reports and statements, for those members of staff who perhaps lack a policing background. Whilst some staff development will undoubtedly occur through peer to peer interaction managers will need to develop individual development programmes to ensure every member of staff is suitably knowledgeable and experienced to give evidence at court.

Skill Profiles

The core roles of Forensic Digital Recovery and Network Investigator should be viewed as two separate specialist roles within their own right but with important overlapping skills and knowledge. It must be highlighted that an individual's development to the role of Digital Forensic Recovery or Network Investigator requires significant investment in training by an organisation and considerable application by the individual concerned over a number of years. Much hard work will be required to master various complicated techniques, training and the accumulation of knowledge will be an on-going requirement.

It will take at least three years in a specific role before an individual can be considered to have reached a high level of capability. In identifying personnel suitable for training in these roles the following general attributes should be considered as a minimum standard:

- Intermediate understanding of computer architecture
- Intermediate understanding regarding the application and methodology of computer related devices
- Intermediate understanding regarding the application and methodology of software with particular reference to internet and email clients, file sharing, database applications and word processing
- Intermediate understanding of relevant legislation
- Good communication skills
- Ability to manage workload and prioritise tasks
- Ability to work effectively as part of a team

Training establishments have identified that the ideal candidate for a forensic analyst post is that of a keen and knowledgeable amateur in computers with a thirst for the field and previous investigative experience. It should be remembered that some of the most gifted and brilliant practitioners in this field today embarked on this role with little or no relevant qualifications however a balance should also be struck in identifying persons with specialist qualifications in particular areas which will have a positive impact on increasing the broad capability of units. The fact a particular person can demonstrate a detailed and technical knowledge of computers should however not be an overriding factor in identifying successful applicants and persons should be assessed in the round with due regard to all of the above qualities.

Outside of the core roles within specialist investigative units it is often advisable to identify and train particular individuals with an additional skill set in specialised areas in order to make best use of the financial resources available rather than duplicating training to all within a unit. For example, network forensic recovery or Apple Macintosh forensics may be considered suitable for identifying particular individuals within a unit to undertake these roles in addition to their core business. These specialist areas of capability can then be deployed as and when required to address particular need.

It has to be acknowledged that continuing levels of expertise are based on experience, continued training and personal research. Any law enforcement agency still operating a tenure policy for these posts must balance the loss of experienced operatives and the large financial investment made in them against the perceived benefits of replacing them. In the present climate it is highly unlikely that the recruitment of trained personnel directly from outside the police service will be possible considering the levels of remuneration available in the commercial sector. Law enforcement lead in this area and there are few people available 'in the market' and staff will generally have to be developed from the bottom up.

In addition to the core roles Forensic Digital Recovery and Network Investigator the following roles should be considered within any specialist investigative unit, depending on the resources available to it and the scope of service it is intended to provide;

1. Administration / Reception Officer: Duties to involve reception of items for examination, logging receipt, ensuring correct storage and continuity of those exhibits and controlling access to premises.
2. Triage Officer: An officer appointed at local level to filter cases and ensure that the appropriate procedures and documentation have been put in place before a tasking request is accepted. It may be appropriate that this task is undertaken by a member of the units Line Management.
3. Physical examiner/imager: Duties to involve the physical examination of the exhibit, identification of media for imaging/examination, actual imaging, backing-up of images, identification of, and supervision of, items out-sourced for imaging/examination.
4. Previewing Examiner: Duties to involve the examination of material using automated processes and bespoke software to determine the presence of evidential material requiring full examination. For example, the presence of IIOC in computer related media.
5. Advanced Examiner: Specialist examination or experimentation to prove particular outcomes.
6. Quality Assurance Officer: This should be a significant consideration in every unit in order to ensure the production of a high quality evidential product.

   Duties should involve the checking of individuals work and quality assurance of the processes employed. While it is understood that the full retesting of all or indeed most work is impractical consideration should be given to dip sampling of cases also. It may be appropriate that this task is undertaken by line management.
7. Training Officer: Duties to involve the development, coordination and delivery of peer training within any unit ensuring standards are adhered to and applied evenly across the board and to provide for the development of junior colleagues as well as the dissemination of latest techniques to experienced personnel. It may be appropriate that this task is undertaken by a member of the units Line Management or a senior member of the team.

Line Managers within specialist investigation Units

The line management of any specialist investigation unit should be at least at Sergeant Level, or Police Staff equivalent, with overview by an officer of Inspector rank, or Police Staff equivalent as a minimum. It is recommended the frontline line manager is a current or past practitioner and is trained in, as a very minimum, the NPIA Core Skills Data Recovery and Analysis Course or the Core Skills Network Investigator Course. It should be considered prudent however for the frontline line manager to have the same training and skills as the majority of the personnel for which they have responsibility in order to allow for the informed and rigorous supervision of the unit. Arguably a manager without sufficient knowledge of the subject matter concerned cannot adequately supervise investigations for which he/she has responsibility or adequately report to senior management. Managers of specialist investigation units have a unique role within law enforcement agencies requiring an in depth knowledge of legislation and technical matters relevant to their role in order to ensure rigorous supervision as well as often having the responsibility of advising on organisational strategy and future direction.

Initial set–up (cont.)

NPIA has the ACPO mandate to provide training solutions for the police service in e-Crime related issues and it works closely with relevant national groupings in this field to ensure that the information it provides is as up to-date as is possible and reflects best practice. NPIA offer an awareness course for managers namely the High Tech Crime Managers Course. It is designed to allow managers to gain a better understanding of the challenges they face, as well as providing solutions for them. This should be attended by all officers who have line management responsibility for digital forensic investigators, network investigators and CIIs, especially middle and senior management who have decision making responsibility for such staff / units, with the view that such awareness training will assist in the decision making process and clarify fully the present and future needs of their respective units.

Additionally the Centre for Forensic Computing, Cranfield University at the Royal Military College of Science, Shrivenham (CFFC) offer a free 'VIP' day in which awareness issues are highlighted with some problem solving, both technical and financial, and suggested solutions. CFFC also have an open-door policy for all law-enforcement to visit for advice and guidance at mutually convenient times and management, at all levels, should consider taking advantage of this.

Staffing Levels:

The level of staff required within any specialist investigative unit will be, in part, dictated by any SLA in existence with the wider organisation. When considering the adequacy of personnel resources available to staff the unit the existence of forensic backlogs involving both phones and computer related equipment should be taken into account. It is a simple proposition that if the demand for services, particularly the digital forensic examination of computers / mobile phones / electronic devices, exceeds the available capability then a backlog will exist and this is indicative of insufficient resources. Backlogs of work are a common feature of digital forensic units in particular around the country and they create considerable corporate risk for any police service. There are significant potential risks associated with a failure to meet obligations under the European Convention on Human Rights (ECHR). For example, it may not be possible to charge a murder or paedophile suspect whose computer equipment is awaiting digital forensic examination, due to a lack of other available evidence. Consequently the individual may remain at liberty and potentially re-offend. If this occurs the Service could be deemed to liable for breaches under Article 2 ECHR and the right to life. Similar concerns can also be raised in respect to Articles 6 and 8 ECHR issues. Even setting aside obligations under the ECHR there is considerable opportunity through adverse publicity, unfavourable comment by the judiciary, the Independent Police Complaints Commission (IPCC) or scrutiny by any relevant police authority to create significant risk to the organisation. A fundamental question will be why the digital forensic examination was not dealt with in a more expedient manner. Managers should also note that the existence of backlogs caused by a shortage of personnel coupled with the accompanying increased demands on existing personnel to address outstanding work can subject them to considerable stress and strain which can become a corporate risk in itself.

In determining how to make best use of available resources and determining the adequacy of existing personnel resources the following factors may be considered:

- Costs associated with any outsourcing of work when compared to the cost of recruiting and developing new personnel to increase in house capability. It is widely accepted that the costs of providing such services internally are significantly more cost effective than outsourcing.
- Risk assessment of cases in any backlog queue where all cases should be subjected to a rigorous assessment of risk based on the information disclosed by the OIC and a priority attached to them as part of any wider fully audited and documented triage process. Agencies may wish to develop some form of scoring matrix to decide on the prioritisation of examinations
- Possible loss of evidence due to storage inadequacies
- Possible civil action against the force due to loss of opportunity in not completing work within a reasonable time
- Potential claims of abuse of process in not completing digital forensic examinations within a reasonable time
- Is best use being made of technology or other available resources to make the unit more efficient?
- Opportunities for collaboration and co-operation with neighbouring law enforcement agencies, in order to make best use of available resources and obtain economies of scale

It may be considered as part of any worthwhile strategical planning process that the demands on specialist investigative units, particularly digital forensic providers, continues to grow year on year in terms of the diversity of requests, the volume of actual taskings and volumes of data to be examined. This demand for specialist investigative resources is expected to continue to grow at an equivalent or greater rate for the foreseeable future with the ever increasing proliferation of technology and it is highly advisable that this be addressed in any planning process. Significant consideration should also be given to the concept of "succession planning" where staff vacancies or retirements are anticipated. It should be considered prudent to identify upcoming vacancies in advance, where possible, of their actual occurrence and steps be taken to identify staff replacements, who can then commence training / handover in order to minimise any loss of capacity.

Disciplinary Issues within e-Crime Units

Whilst it is always unfortunate to have to discipline a member of staff, it is important to consider the following points;

- A record of all passwords used by all personnel should be securely retained by a line manager for the personnel concerned in order to facilitate access to official equipment if required.
- A need for a well documented procedure in the event that you have a member of staff that you have to dismiss or suspend and the strict adherence to service policy in this area.
- In the event of any significant disciplinary action or criminal proceedings consideration should be given to the individual being removed from the premises without delay, under supervision, and not be allowed to interact with any equipment in any way.
- Consideration should be given to the removal, from personnel subject to significant disciplinary or criminal allegations, of all passes and official equipment and any access they have to IT systems suspended.
- Although no work related material should be outside any secure office except for official business this should be checked with the member concerned as well as others and steps taken to retrieve anything in their personal possession outside the confines of the office environment.
- Steps should be taken to secure any available evidence of disciplinary or criminal behaviour and consideration given to the forensic imaging of any relevant material at the earliest opportunity to minimise any subsequent allegations of wrongdoing against unit personnel.

Location and accommodation

Careful consideration should be given to the geographical location of any unit, where possible, so as to provide the best overall level of access to the organisation.

Due to the nature of work undertaken by most digital forensic units, which can include sensitive material such as national security issues or IIOC, great attention should be given to the physical security of any unit premises with assessment by any internal department with organisational responsibility for security recommended. Security should also extend to general asset protection and the secure storage of documents, electronic data and physical exhibits. This asset protection should extend to all relevant data held on premises and it is strongly recommended that any data held within the unit of a critical nature, such as evidence files, is backed up off site to provide resilience and security. Due to the dangers posed by electronic data in respect to ease of duplication and dissemination a "culture of absolute security" should be encouraged by all within the unit.

Only persons with authorised access should have access to premises directly relevant to their official business and only for as long as is absolutely necessary, whether a member of the law enforcement service or not. Clear procedures should be in place for the securing of premises at the end of duty that are understood by all within the unit and strictly adhered to.

There should be a physical demarcation between working areas and those available to the public in any lay out of premises with the public limited to the reception areas or any viewing room designed for the purpose and even then subject to supervision. It should be noted that few, if any, units are accessible to the general public and in practice this should refer only to defence counsel or experts as well as "independent" barristers for dealing with matters subject to legal privilege for example.

The existence of a secure "reception" area is best suited to control access to and from offices as well as to oversee the management of exhibit submissions and collections. Exhibits should be held within a secure store designed for that purpose with sufficient asset protection afforded to it and access to and from this store should be audited along with the movement of exhibits.

Initial set–up (cont.)

The existence of a separate "working area" adjacent to any store to facilitate the inspection of equipment or imaging is recommended as best practice and which is separate from any examination area.

The actual digital forensic examination area should be separate again with an area set aside for the in depth analysis of digital evidence. Personal working areas should be clearly set out in such a way as to minimise the collateral impact of one person's examination on a neighbouring workstation as well as to provide sufficient desk space for each individual. The needs for individual workspace are far in excess of the average administration worker, with sufficient room required for multiple pieces of hardware as well as to allow for the writing of reports and statements. It is likely the forensic analyst, to operate more efficiently, may well be running more than one job at a time. Physical separation of individual tasks, an examination log as well as individual examination machines will assist in the security and integrity of each particular forensic examination. Thus, analysts' work areas should not just be a simple desk but a full workstation with areas for machines, paperwork, exhibits and so on.

Consideration should be given to the use of desk dividers and issue of headphones to minimise the collateral impact of examinations on other personnel in close proximity. This can refer to both mobile phones and computer related devices and ideally provision should be made for specialist needs in each area, such as a "Faraday Cage" for the examination of mobile phones.

The wider forensic roles of computer related equipment and mobile phones are suitable for sharing a general working area due to their increasing areas of overlap in respect to device capability and examination expertise. It is recommended however that each enjoys clear lines of demarcation within the general working area if applicable. It is also recommended that there is a clear separation of working area between the role of Network Investigator and digital forensic recovery specialist. If the Network Investigator role extends to intelligence related taskings or Covert Internet Investigator (CII) deployments there should be a clear physical and procedural firewall in place to separate any intelligence related work from evidential material and prevent any wider contamination in keeping with national policy in this area.

Attention is drawn to the recently completed premises of Police Service of Northern Ireland (PSNI) e-Crime Unit as a model for the design and lay out of unit premises at a regional police service level where network investigation, covert internet investigation, mobile phone examination and digital evidence recovery are all undertaken in the same premises, with regards to all the issues outlined above. The PSNI particularly welcome any inquiries in this respect from law enforcement colleagues in the interests of raising standards nationally.

General points for consideration:

Authorised Use Policy (AUP): The existence of such a policy in respect to all unit equipment is highly recommended in order to clearly identify to personnel what is permissible and what is not

Internet Auditing: The AUP should extend to the use of Internet access within a specialist unit which is an essential unit facility. It is suggested that the use of any Internet service is subject to auditing through, for example, the use of a "proxy server," in order to minimise corporate risk and to protect individual personnel.

Accreditation: The obtaining of accreditation for units is to be encouraged by line management. Several units throughout the United Kingdom have recently undertaken accreditation for the ISO 9001 standard which culminates in an external examination of procedures and processes at a unit level and adds significantly to the overall credibility of evidential product produced. Consideration is presently underway at a national level to make accreditation with the United Kingdom Accreditation Service (UKAS) applicable to all forensic service providers including digital forensic units and developments in this area should be monitored by line management to ensure compliance with the latest standards. Standards within the forensic arena are currently being developed by the National Forensic Regulator, these will impact upon any unit which performs a digital forensic function, both private and public sector service providers. Initial indications are that units will be encouraged to work towards ISO 9001 in the medium term, with a view to achieving accreditation to ISO 17025 in the longer term. Currently there is no national system for the accreditation of individual members of staff, however some units have chosen to accredit digital forensic examiners through the International Association of Computer Investigation Specialists (IACIS), this is an International non profit making organisation run by current and former law enforcement staff.

Prioritisation: The existence of backlogs in forensic areas of work should necessitate a transparent, standardised and fully documented approach to the prioritisation of submissions to any units. This prioritisation should take into account perceived risk. The criteria for assessment can be incorporated into any application process for services and assessed on the basis of the information disclosed by the IO.

Health and Welfare: Anecdotal evidence indicates that between 60-80% of digital forensic examinations are likely to relate to paedophile related investigations. The prolonged exposure to IIOC related material can have a detrimental effect on personnel and consideration should be given to prevent personnel being subjected to casework involving this material for sustained periods of time. Physical measures, such as screened windows, locked doors, etc should be considered to prevent wider collateral impact. It is suggested that the formulation of teams within a forensic unit are of benefit with each team only having responsibility for IIOC for a set time before they are rotated to work of a non paedophile related nature. In addition to this steps should be taken by line management to ensure an effective system to address the health and welfare of personnel exposed to IIOC is in place, in conjunction with the Occupational Health Department. This does not preclude the responsibilities of individuals to bring to the attention of line management or through "self referral" to Occupational Health and Welfare any concerns they have.

Wider consideration should be given to the Health and Safety of personnel in an environment where there are large amounts of electrical equipment and high temperatures due to its operation.

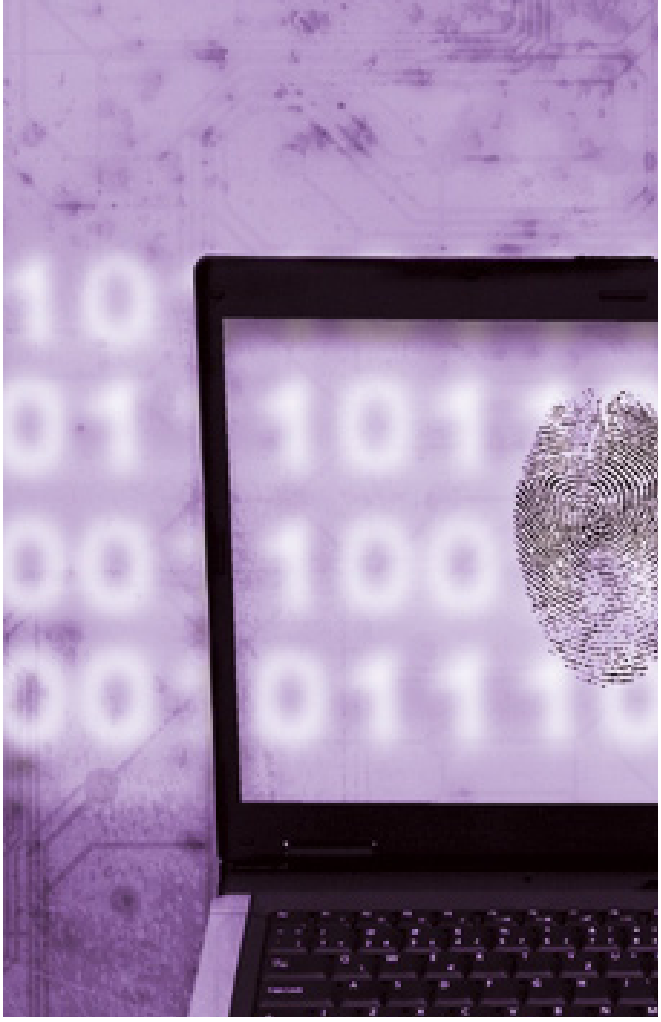
All identified risks should be reported to line management and steps taken to eradicate or mitigate risk where possible in conjunction with service policy. Steps should be taken to ensure an acceptable working climate for all with the mitigation of extreme temperatures through the use of effective temperature control equipment.

Security of data

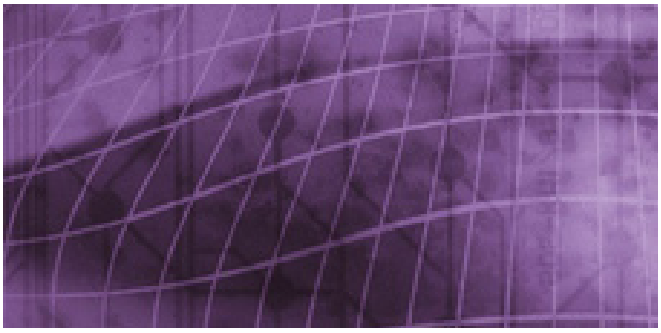
The security of data contained should be of the utmost importance when it is necessity to remove it from unit premises for any one of many entirely legitimate reasons to facilitate official business. The use of more restrictive corporate hardware encryption approaches may restrict any computer to a level where it is not serviceable for use within a specialist investigative unit. Irrespective of this it is strongly recommended that a strong encryption policy in respect to the movement of data by personnel be implemented using alternative encryption techniques where necessary and no work related data, on whatever form of device, should leave the confines of police premises without this being in place. Details of all passwords used held securely and centrally by line management and any policy implemented should have the agreement of senior management and be consistent with service policy.

Management Information

Consideration should be given to the development of statistical management within any unit and preferably through some form of database application. The recording and availability of this information over a range of relevant statistics will have significant benefits in completing periodic returns and compiling business cases for additional resources through the clear demonstration of need and statistical facts.



Management Matters



Management Matters

The following matters are those which it is suggested must be considered by Unit Managers:

Security Issues

As already mentioned, the premises occupied by the Unit must be secure internally.

External security is a matter of Risk Assessment, at the very least the Unit should be protected by an electronic alarm system (with signalling) to protect it against unauthorised intruders and fire whilst out-of-hours.

Property/exhibits

An auditable, and secure, system must be adopted for the continuity of exhibits.

Resilience

Backup copies of all workstations and software in addition to all evidential copies to allow for any failure or corruption of the hard drives and should be kept off site. Due to the increasing importance of work carried out by units it is recommended that a business continuity plan and disaster recovery plans should be designed for implementation should a more serious systems failure occur, enabling continuation of crucial operations. Hardware can be easily replaced within a few days, working files, evidence and research cannot.

Internal Network

If used, should not be connected to any network outside the Unit, a machine should be available for on-line research and downloading of software/drivers and the like. This should be independent of the organisation's network and it should be non attributable so it can be used for investigative purposes without risk of leaving 'digital footprints' leading back to the police service. The Internet is a major resource for low cost or free software and knowledge, its use for these purposes should be encouraged.

Policy

A policy should be adopted for the control of unlawful material. The production of copies of unlawful material from original exhibits should be avoided if at all possible. In circumstances where such production is required the material itself should be closely supervised by a named member of staff who should ensure it does not leave their possession until it is returned to the unit and destroyed. Consideration should be given to encrypting any indecent material that comes into the possession of the unit. Additionally, Managers must ensure that when any indecent images are discovered that the investigation unit responsible for Child Protection matters is informed in order that they can establish if there are any child protection considerations.

With regard to the release of material to the defence, reference should be made to page 30 of the ACPO Good Practice Guide for Computer Based Evidence. It must be stressed the content is advice only and it should be read in its totality. Section 46 of The Sexual Offences Act 2003 addresses the issue of the 'making' images and creates a defence to a charge of "making" an image providing the person can prove that it was necessary to do so for the purposes of the prevention, detection, or investigation of crime, or for the purposes of criminal proceedings.

On 6th October 2004, the CPS and ACPO signed a Memorandum of Understanding relating to S46 Sexual Offences Act 2003. This MoU describes the circumstances in which it is permissible to "make" an image and the expectations in terms of prompt reporting for those who discover such images, it also deals with release of material to defence experts.

Where the "making" was genuinely carried out and reported in a timely manner by the person acting in their legitimate professional capacity, with the right intentions, the exception under section 46 of the Sexual Offences Act 2003 will apply and there will therefore be insufficient evidence to prosecute. If in exceptional circumstances the section 46 defence did not apply to someone who was nevertheless operating in a legitimate professional capacity, it may still not be in the public interest to prosecute. The section 46 defence would not apply where there was other evidence that the person was abusing their position with the intention of "making".

Note

The MoU relating to S46 Sexual Offences Act 2003 may be viewed at:

www.cps.gov.uk/publications/agencies/index.html

Management Matters (cont.)

Equipment and Storage

It is not possible to predict the operating environment of all units; however it is suggested that high specification work stations be purchased for computer forensic analysts. The need for replacement of forensic workstations needs to reviewed regularly, older equipment can be recycled into lower-priority tasks within the unit. Items such as laptops leaving the unit for any reason must be equipped with Government approved full disk encryption.

As well as the purchase of hardware equipment, consideration must be given to the cost and licensing of core software, this should be reviewed annually. Ad hoc software should also be purchased and licensed as required.

Consider

- Dual-tool verification explained in detail in Section 5)
- Replacement of forensic workstations at 12 to 18 months and preferably be more than 3 years
- UPS back-up facility
- Independent access to Broadband
- Business case in place for continuance of hardware, software and licensing needs

For reasons of efficiency the analyst should have immediate access to at least two high-specification machines. Whilst carrying out lengthy searches or scripted operations on one he / she can carry out routine operations on another. A laptop machine is also useful for note taking and report writing, it can also double as an on-site imaging machine if required. An individual laser printer for output and a supply of storage disks will also be required unless network storage is available. Consideration should also be given to the availability of a contingency fund or corporate credit card accessible by the unit. This will enable hire or purchase of immediate use special equipment when unusual media is encountered.

The following checklist is available for use to assist in establishing if minimum equipment requirements are being met:

Minimum Equipment Requirements		
Equipment	**Forensic Examiner**	**Network Investigator**
2 Forensic Workstations		**N/A**
Workstation	**N/A**	
Dual Screens (minimum size 21")		
Broadband access to the internet independent to the police network		
Individual access to the Police Network		
Linked in to a commercial quality printer		
Individually assigned forensic tool software e.g.: Dongles, write blockers.		**N/A**
A Supply of hard drives or access to network storage		
A supply of removable media e.g.: CD's DVD's, thumbdrives		

In addition, a mobile acquisition kit needs to be available for use by both forensic investigators and network investigators.

Laptops need not be so high in their specification as the forensic workstation but they should have the capability of all popular methods of external connection (USB2, Firewire etc.) so they can be transformed externally, if required, to deal with external storage devices and, in particular small digital media. They can be used as portable imagers with the correct connections and external equipment.

Note

No storage media (e.g. CD's, DVD's, HDD's, USB Memory Sick's) used within the unit, should leave it in a usable state

Storage

The increase in sizes of digital media and the need to retain data for long periods puts additional pressure upon digital forensic units. Storage media are required for both evidential material and working files for both short term and long term retention.

There are a number of alternative solutions; the choices made will be dependant upon volume, cost and retention period. However, whichever option is chosen, the media used must be of good quality, there is a vast amount of 'cheap' media available but these may prove unreliable.

In general terms there are three main storage options:

Tape: The most popular and probably cheapest option per Gb. Drawbacks are the slow speed of data transfer to and from tape. Relatively reliable, the technology is well known. The tape may be liable to corruption from magnetic sources.

DVD/CD: Ideal for small amounts of data, particularly working files and evidential extracts. They must be stored properly to avoid physical damage.

Hard Disk/Network Storage: These are considered a real alternative due to the fall in price of hard disks over the last few years. They are reliable, provided they are stored correctly.

It is good practice to backup all evidential material immediately it is obtained. Backup copies of images and working files should be kept separated both physically and digitally from the working copies and ideally be kept off site.

The specification of hardware and the necessary balance between cost and value-for-money is a hard task for the professional analyst let alone those who have little or no knowledge of the requirements.

All media, (HDD's etc) should be removed and physically destroyed before obsolete equipment is disposed of.

Advice on specifications and perceived need is always available from the NPIA, The Centre for Forensic Computing (CFFC) or other academic institutions.

Digital Cameras

The use of digital cameras, both at seizure scenes and in the examination room, is a major advantage. Digital photographs can provide a ready and accurate reference to component location, attachments, machine capability and internal layout as well as identifying the exhibit itself.

For further information on the use of digital cameras to record crime scenes please refer to Practice Advice On Police Use of Digital Images, published by NPIA in 2007. Available for download from the Genesis web site.

Acceptance of Jobs and Prioritisation

One of the important aspects of job acceptance, is clearly understanding the concept of size. Briefly to illustrate this point:

1Gb hard disc will hold 218,000 pages of text and if it was printed out would stand 81 feet high.

Hard disc capacity is increasing all the time. At the time of writing hard discs are available to personal consumers with a capacity of 1TB of data, to put this into context it is roughly equivalent to 50,000 trees made into paper and printed.

Not forgetting also the increase in capacity of other types of data storage, as examples, the Apple iPhone released (Nov '07) with a capacity of 8GB data storage; USB Watches with up to 2GB data storage are also widely available.

The following table may assist when explaining to others the concept of size. The number of pages within a GB varies depending on the type of file. The following common types of file often result in an average number of pages per GB as illustrated below:

DOCUMENT TYPE	AVERAGE PAGES per GB
Microsoft Word Files	64,782
Email files	100,099
Microsoft Excel Files	165,791
Microsoft PowerPoint Files	17,552
Image Files	15,477

Additionally, the increasing complexity of such evidence coupled with the sheer volume of the data, automatically places greater burdens on the resources required to undertake an examination and an investigation.

Before starting work on any case, an assessment of the information available should be made, together with the items provided for examination. Such an assessment may take the following format:

- Is there information or intelligence which indicates there is likely to be evidence of a criminal offence or any material which may assist the defence or undermine the prosecution case?
- Has the submission of the exhibit(s) been authorised by a Senior Officer from the area/branch/department?
- Is the evidence in support of the charges for which the subject(s) have been arrested?
- Will the evidence be pivotal in the likely success of the prosecution or will the evidence have a significant effect on the likely sentence if convicted?
- Has sufficient information pertaining to the case been provided to enable keyword searches?
- Have all available witness statements been provided?
- Has the machine been accessed or switched on since seizure? If so by whom and when?
- What is the continuity chain since seizure?

The assessment may also involve determining:

- the urgency and priority of the need for information
- the other types of forensic examination which may have to be carried out on the same items

It is also important to bear in mind whether recovered data could be present due to other circumstances.

Note

Consider whether to devise an Operational Level Agreement (OLA) for use within the organisation or a Service Level Agreement (SLA) for use outside the organisation.

Existing OLA's and SLA's need to be reviewed regularly to take into account the changing size of storage capacity.

Productivity

It is not the intention of this Guide to prescribe exactly how to increase productivity, as there are clearly a number of factors which can and do affect any method of trying to do so.

However, substantial backlogs of work waiting to be investigated, has been a regular feature of units around the country. It therefore follows Managers should be examining safe ways of reducing these backlogs.

A number of different solutions have been successfully implemented in various units. Such solutions include:

Dorset Police create digital evidence packs which are encrypted by the High Tech Crime Unit using PGP virtual discs. Unique passwords are created for each case and supplied to the officer in the case. The PGP virtual discs are copied to CD, DVD or hard drive and handed to the officer in the case. Each division has paid for a medium spec lap top which has been set up and secured by the High Tech Crime Unit. The sole purpose of these laptops is to be able to unencrypt and view material supplied by the High Tech Crime Unit.

Another innovative solution is one implemented by Avon & Somerset Constabulary. They have created a protocol with CPS locally whereby a full examination of the machine(s) is not undertaken until such time as a 'Not guilty' plea is received. All that is done in the first instance is establishing the presence of sufficient evidence to charge. This has proven to be a successful process within Avon & Somerset and discussions are currently being undertaken to implement this Protocol regionally. Further information can be obtained from Avon & Somerset High Tech Crime Unit.

The West Midlands force area has a Central Hi-Tech Team that delivers digital forensics to an evidential standard. Each of there 21 OCU's has at least one dedicated full time Hi-tech Representative, who delivers a local digital forensic service. The Reps assist local staff with scene management from a digital perspective. The Reps also provide a full forensic service on mobile phones from analysis to court. With computers and other media, they image all the material and complete basic forensic searches and bookmarking of the cases. The case is then submitted into the central team for completion and evidencing. All processes are documented in the usual manner. The Reps and the Senior Management Teams from the OCUs work to an agreed service level agreement with the central team.

The Reps are trained to a development plan, which includes external product specific courses. Each rep has a mentor on the central team, through whom they submit their work. The Hi-tech business is delivered from twenty five sites across the force area. These sites are all connected via an encrypted link to the central team database, thus creating a virtual office on one network. It has meant data can be easily transferred across the network. Staff in the centre can remotely log into the Rep's computers and advise and explore cases, when required, thus making the process much more efficient. This structure has allowed the force to deal with large numbers of cases and can provide a recruiting pool for new members of the central unit.

Whatever the agency structure for delivering digital forensics services the amount of referrals will inevitably rise and with a satellite approach there are likely to be issues involving the crossover of responsibilities. Clearly, these solutions also have their 'downside' and managers need to be aware of these before deciding to follow a similar path or not.

Other solutions involve the purchase of equipment to enable several examination processes to be automated and be 'running' at the same time.

Consider

- Should guidelines be set on time frames for completing examinations for Investigating Officers and the Court?
- Have I 'stream-lined' my processes to make best use of time?
- Should I adopt a matrix or assessment criteria.

Management Information and Performance Measurement

Traditional thinking appears to dictate performance indicators are based simply on numbers and not content. Perhaps given the amount of data that can be stored now this traditional thinking should change and the 'headline' performance indicator should take account of it. This would mean not simply recording the number of requests for work to be completed, but adding a little more details in terms of the amount of work required for each request,. Items that can be specifically measured:

- The total number of Gigabytes imaged per year
- The total number of submissions per year
- The number of child abuse image cases completed each year.
- The number of qualified analysts/network investigations employed on the unit
- The total number of persons employed in the unit

Some suggested performance indicators:

- Request for investigation and examination
- Assisting Major and Serious Crime Detection
- Assisting Volume crime detection
- Crime Reduction initiatives
- Making the best use of available resources
- Education and Awareness training for the force
- 'Turnaround' time
- Number of referrals per force area
- Intelligence logs disseminated
- Number of machines submitted for examination
- Volume of material in gigabytes
- Number of PDAs and mobile telephones submitted
- Number of arrests made by Unit (if applicable)

Communication Generally – Remember

- PCeU – 'Police Central e-crime Unit', new national unit formed to coordinate the reporting of e-crime
- Sharing information – particularly good practice and the lessons learned from the bad
- Line Managers and Strategic Head of Unit to attend Regional meetings
- The Chair of the Regional Meetings must be Superintendent level
- Think about and consult the ACPO Hi-Tech Crime Training Sub-Group
- SOCA e-Crime
- CEOP – a source of advice and assistance
- NPIA – a valuable source of advice especially on training
- CFFC are available for advice to all Law Enforcement
- Digital Evidence Group (DEG) – are there for help and guidance
- F3 – there for help and assistance on forensic computing matters
- A neighbouring force unit – a simple way of getting information
- IWF – Can provide valuable information to help
- Genesis

Record Keeping

Good record keeping is an important part of the investigative process, particularly so given the lawful requirements of 'Disclosure'.

Remember: Record, Retain, Reveal and Review

Good record keeping helps to focus work, particularly in relation to investigative policy and strategy, and is essential to working effectively in an environment where accountability is key to everything that is done. Good records also help with investigative continuity and provide an essential tool for managers to monitor work, advise and challenge where appropriate.

Such records, if they are to serve a useful purpose, should use clear, straightforward language, should be concise and should be accurate not only in relation to facts, but in differentiating between opinion, judgments and hypothesis.

Records should be clear, accessible and comprehensive, with judgments made and actions and decisions made or taken being carefully recorded. Where such decisions have been made involving others outside the police service, or endorsed by line command, this should be made clear.

To comply with such a regime, immediately guarantees that information can be brought together from a number of different sources, thus enabling careful professional judgments to be made.

Outsourcing of Work

Any outsourcing of digital forensic examinations must comply with EU and UK procurement legislation, using a commercially binding well written SLA. Given most forces have units capable of carrying out forensic examinations; there are two main types of work that are outsourced:

1 Work which would normally be carried out by the unit, but due to time constraints or a desire to reduce backlogs, such work is outsourced. In this case there are a number of matters to consider:

- Which individual jobs are to be outsourced – these should be carefully selected to fit in with the profile of what follows.**It is recommended that, wherever practicable, all investigations involving paedophile and sensitive material should be conducted by law enforcement personnel.**
- Who are they to be outsourced to – the forensic contractor to whom the job is to be given must be able to demonstrate their capability to complete the task successfully, competently, to the level required and to comply with requirements on security etc. Liaison with other forces for recommendation of companies who have previously completed this type of work to a good standard with value for money is recommended. The ACPO advice on external consulting witnesses and forensic contractors, as detailed in the ACPO Good Practice Guide on Computer Based Electronic Evidence (Page 33) should be referred to for further guidance on this matter.
- What is the likely cost – generally this question will be answered by 'how long is a piece of string?' It is fair to say it is not possible to specifically quote a figure before the job is partially completed. However, companies experienced in this field should be able to give an outline figure based on experience and the size of media involved. A 'pick-list' of operations is useful to identify like-for-like quotes. Quotes should contain some detail of the operations to be carried out on the suspect media [see forensic

matter below]. Sample reports and costs of previous jobs completed could also give an indication of the professionalism of the company and its likely charges. It is important the OIC or outsourcing officer keeps control of the job, once it is out of the hands of the force control must still be retained.

2 Work which is examined by the unit, but requires specialist advice or guidance, or, as a result of a defence expert report the unit and/or CPS (Crown Prosecution Service) feel the support of an acknowledged expert would be required to carry the case to conviction. Matters for consideration in this case are:

- How to select an expert – the unit's knowledge of the field should help here, the expert should be qualified, accepted regularly as an expert witness in Court and be experienced in the field. The particular expert should be able to indicate if they have knowledge in the specific area around which the case revolves, intimate knowledge of the operation of a piece of software, for instance.
- How long will the job take – there are relatively few experts in the forensic field and they are usually very busy. Most operate a priority system where they will push work back for urgent and important cases such as those with life at risk. It is therefore the case that any lower level, but just as complex, work will take some time to complete. Referral to experts should be reported to the Court relatively quickly to ensure no undue pressure is placed upon the expert. They will have Court experience so will understand the need for speed but cannot be expected to complete work at the expense of quality.
- How much will it cost –such jobs will be expensive, one way of keeping control is to agree a base figure from which the expert will contact the instructing officer with a progress report and an estimate as to how long the job will take to complete and at what likely cost. They will also be able to offer opinions as to what work is likely to reap the greatest rewards in order to focus the examination and keep costs down where possible.

When appointing a forensic expert it is important that they are known in the forensic field, as it has already been pointed out it is a different technological and philosophical area to normal or specific computer knowledge.

Finally, it is also important to read the ACPO Good Practice Guide on Computer Based Electronic Evidence, page 30 and the CPS/ACPO MoU dated 6th October 2004 relating to S46 Sexual Offences Act 2003.

Consider

- Procurement compliance
- Like for like quotes
- Vetting of Premises, Security & Personnel including on site visit
- Selection criteria for outsourcing
- Identification and use of experts
- Liaison with OIC
- Contract terms to ensure no sub-contracting
- Disposal of material following examination
- Disposal/Cleaning of hard drives, servers and tapes
- Time spans for 'running' of cases
- Grading of Jobs for choice of examiner

Business Continuity

The important point to understand in relation to this is to manage the organisations ability to recover within acceptable time scales from those events and environmental surroundings which could adversely affect the Unit and its facilities. These can be reduced by effective risk analysis and risk management. **Matters to consider must include both personnel and data.**

Personnel:

Proper succession planning is critical to the successful running of a unit. Consideration should be given at an early stage in respect of the unit's needs when taking account of pending retirement, sickness absence (long term), turnover of staff, difficult to recruit posts and on-going vacancies. It is suggested that a staff impact analysis of critical employees and roles be carried out identifying how their unavailability would affect the unit and time needed to cross train staff to perform different roles or the time to develop either new or existing staff to replace them.

As can be seen from the Training Section of this guidance it can take between 2-3 years for a new member of staff to become fully competent in their role.

Data:

Managers should anticipate the damage that events such as floods, fire etc can cause and the controls needed to prevent or minimise the effects of potential loss. They should develop and implement procedures for responding to and stabilising the situation following an incident or event, particularly in relation to the recovery of critical data.

See also Equipment and Storage

The importance of back up and off site storage for the force Hi-Tech / Computer Crime Unit / Digital Forensics Provider cannot be overestimated. Off site storage of backup material is essential for an effective business continuity solution. The imaging and back-up regime for the vast majority of units is carried out by one of two methods:

1. Image to HDD – examination on that HDD and evidential material to CD-Rom or DVD.
2. Image to HDD and that image copied to server and tape (back-up) evidential material to CD-Rom or DVD

In both cases, the original HDD is returned to the target machine and then returned to secure storage.

The consequences of failing to have a business continuity plan will be the loss of a case at court, with potentially catastrophic consequences.

It is **recommended** that all digital forensic units are provided with on-site fire-resistant safes and off-site storage facilities are made available to safeguard backup material. All units should develop and test a disaster recovery procedure relevant to their work. Hardware can easily be replaced within a few days; working files, evidence and research cannot.

Health and Safety

Health and Safety considerations are extremely important in all of the work undertaken at all stages of the forensic and investigation process. Personnel engaged in the examination of various forms of digital technology (including mobile phones) should operate in accordance with Force policy and the regulations of the pertinent government, environmental and safety authorities in respect of both emotional and physical well-being.

It is important to identify all risks, including those involved with working with large quantities of offensive and/or sensitive material. Safe systems of work should be communicated to all personnel likely to be exposed to such risks and the availability and attendance at regular counselling should be mandatory. It is good practice for managers of units who are dealing with material which can give rise to emotional reaction, such as paedophile or other disturbing material, to consider the implementation of fixed-period compulsory counselling sessions for all operatives exposed to it. This avoids the 'bravado' refusal and ensures all staff have the opportunity to benefit from sessions if they wish to do so. It may also avoid the possibility of criticism of management for not making it available or not recognising the symptoms of stress caused.

To reduce the risk of emotional/psychological injury, processes must be in place to ensure that all staff requested to view material, as detailed above, are fully aware of what to expect prior to exposure. The difficulties of ensuring that the correct safeguards are in place should soon be made easier. ACPO Combating Child Abuse on the Internet (CCAI) is currently undertaking a project amongst police staff who regularly view images, with the intention of producing some 'guidance' for force managers so that they are aware of their responsibilities and to ensure that adequate safeguards are put in place. Until this is published Managers will have to ensure that they have carefully considered policy in respect of these issues.

Sussex Police have created a policy in respect of the above, of which a summarised version has been provided for inclusion in this guidance document as an example of the types of considerations managers need to be aware of:

Sussex Risk Assessment

A. Consider the environment and work stations in the HTCU

B. The physical and mental well being of the staff, who have been graded as ''High Risk'. The recommendations are that an additional service be employed to ensure their wellbeing and maintain a healthy team. Occupational Health provide a framework and quoted for the following:

1. Initial baseline psychological assessment of all High Tech Crime Unit staff who undertake the viewing of child abuse image material. Agreed testing requirements, which include a clinical interview and completion of various established questionnaires. The initial baseline testing time per individual is between 2 - 3 hours under usual circumstances.
2. Thereafter, whilst they are still employed in this role they receive six monthly follow-up individual psychological assessments. Each 6 monthly follow-up interview and write up is anticipated to take 1 hour.
3. On leaving the Unit, or the force to undertake alternative work, a final individual assessment is carried out.
4. All new staff joining the unit has a baseline assessment before undertaking the work and thereafter follow-ups as described above.
5. Confidential reports indicating outcomes of all individual assessments are sent to the Health, Safety and Welfare Unit's Occupational Health service for retention on staff medical files and any necessary action arising from these.

Key Points

- Need for regular compulsory counselling sessions (at least annually)
- Supervisors to take responsibility and refer at early signs of distress or unusual behaviour amongst staff.
- Regular breaks from viewing screens
- Prevent unnecessary exposure to disturbing images

Safety manuals should be available to all personnel and these should contain details of how to conduct a risk assessment and how to develop safe systems of work, both at the scene of an incident or in the examination room.

Portable Appliance Testing (PAT) should be carried out both on receipt and disposal of computer systems in order to safeguard personnel and prevent frivolous complaints. On reception, such testing should be carried out AFTER any portable media has been removed and the hard discs imaged.

The working environment must be assessed and appropriate remedies in place to protect staff from injury. Common complaints of those working with Display Screen Equipment (DSE) over prolonged periods of time include upper limb pains and discomfort, back pain, eye and eyesight effects, fatigue and stress, epilepsy and facial dermatitis.

Guidance on reducing the risks associated with DSE is available from the Health and Safety Executive at www.hse.gov.uk/pubns/indg36.pdf

Key Points

- Provision of circuit breaker switches to immediately remove power from all workbenches in the event of accident.
- Anti-static flooring and wristbands
- Rubber matting under workbenches to prevent earthing
- Work Station Assessments

Disclosure

The Criminal Procedure and Investigations Act 1996, as amended by the Criminal Justice Act 2003, requires a single objective test for the disclosure of prosecution material to the defence. This test requires the prosecutor to disclose "… any prosecution material which has not previously been disclosed to the accused and which might reasonably be considered capable of undermining the case for the prosecution against the accused, or of assisting the case for the accused." Disclosure affects not only material seized by Law Enforcement, but may extend to other relevant material held by third parties.

Where there is a large volume of computer-held material, inspection and description of it may present difficulties. Due to this the Attorney General has provided some helpful guidance:

"*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, or to establish the contents of large volumes of material by dip sampling. 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 for such action*"

Para 27, Attorney General's Guidelines on Disclosure 2005

Available at www.attorneygeneral.gov.uk/attachments/disclosure.doc

The CPIA Code of Practice also provides guidance concerning the duty to pursue all reasonable lines of enquiry in relation to computer material. CPIA Code of Practice, para 3.5

In cases where the seized material comprises a large volume, which it is not felt a reasonable or proportionate use of police resource to examine all or part of it and the data is retained, a statement, disclosed as part of the disclosure schedule, should be prepared by the Disclosure Officer detailing, in general terms, the material and justification for not examining it.

In the case where inextricably linked material or various categories exists on the same media and due to the large volume or fragmentary nature of the data viewing all may be impossible, or require a disproportionate use of resources, the defence should be advised in statement form, included in the disclosure schedule, of the existence and extent of the material, categories and examination made upon it including lists of keyword searches.

There may be instances where automatic disclosure cannot be permitted, for example:

1. Malicious code, the return of which to a suspect could result in further criminal acts.
2. In cross-disclosure cases of multiple defendants, legally privileged material or personal data relating to persons not under suspicion or who may become at risk if disclosure is made to other suspects.
3. Commercially sensitive data contained within the material.
4. CCTV images, where the collection of data is indiscriminate, consideration must be given to possible collateral intrusion into privacy.

In the above cases agreement should be sought with the defence to manage access, for example the listing of file structure or directories or inviting the provision of additional keyword searches.

In cases where the defence is not permitted full access to the seized material it is the responsibility of the Senior Investigating Officer and the Disclosure Officer to ensure full account is taken of this. Where appropriate a partial disclosure of a file set or subset could be made of files that do not fall within the areas outlined above. Such disclosure will considerably reduce the need for extensive examination of that area of data by the Disclosure Officer. The following is procedure is suggested:

1. Inspection of all undisclosed documents retrieved in keyword searches by the SIO or Disclosure Officer.
2. Reviewing keyword searches and parameters used in the investigation to ensure all reasonable lines of enquiry are covered.
3. Making additional keyword searches, using judgement and knowledge of the case to decide how much work is appropriate. It is important for the SIO to appoint a Disclosure Officer with the appropriate skills and experience to undertake this task.
4. Where the Forensic Examiner has made an examination of a computer program, a folder or files sorted by class e.g. images and film clips, accountancy packages, spreadsheets, document folders, emails, recovered deleted material, as an alternative to or in addition to, keyword searches the Disclosure Officer's inspection should follow the same course.
5. Disclosure Officer to inspect the directory structure and review the examination strategy used by the Forensic Examiner to ensure that this properly covers all reasonable lines of enquiry. It is important the Disclosure Officer has the appropriate skills and experience for this task.
6. Making additional direct examination of programs, folders or classes of files if necessary, using judgement and knowledge of the circumstances of the case to decide how much additional work is proportionate.

7. Identifying, in the disclosure schedule, each item containing stored data. Detailing for each item. :

A Lists of keywords used;

B A printout of the directory structure, or file listing where this is applicable

C Forensic unit's documentation of any applications audit, where this is applicable.

D The details of steps 1 – 7 above that have been carried out.

Presentation of Evidence

Forensic Computing and Investigation requires a very high standard of documentation and exhibit handling. Each examiner is involved in a specialised and responsible field of endeavour which requires considerable knowledge, skill and impartiality.

General advice

- Get a full understanding of the facts of the case and the chain of custody in relation to the storage media to be investigated
- Know the crimes that are suspected or charged and the elements to prove in order to convict
- Having found the key evidence focus on the challenges the Defence expert could raise in relation to it
- When testifying be prepared and consider any question carefully before answering
- Draw on all the experience available to you

- Get a full understanding of the facts of the case and the chain of custody in relation to the storage media to be investigated
- Know the crimes that are suspected or charged and the elements to prove in order to convict
- Having found the key evidence focus on the challenges the Defence expert could raise in relation to it
- When testifying be prepared and consider any question carefully before answering
- Draw on all the experience available to you

How the examiner/investigator presents the evidence for consideration by CPS and then by the Court is an issue which is subject to considerable debate. What is clear is that evidential points must be properly put and supported by factual detail.

The following points have been elicited from a QC who is used to prosecuting and defending when digital/electronic evidence forms part of the case. Although these points may be considered 'basic', it could be argued that sometimes the 'basic' is forgotten.

Advice from a QC

The main body of the evidence should be contained in the witness statement

- All witness statements/reports should list the relevant qualifications of the 'expert'
- Do not put diagrams in the body of the statement
- Append a glossary of the technical terms you have used in the statement
- Simply because you call something an exhibit doesn't mean that it is!
- Placing a commentary on an exhibit may provide the Defence with a legitimate objection to it going before the jury
- If a commentary is required in order to make an exhibit more jury friendly, the commentary should be as brief and uncontentious as possible
- Accurate diagrams may be attached as an exhibit
- Always put what exhibits/documents you have been provided with and what you have used to draw your opinions on
- Where in the course of examining an exhibit, that exhibit is altered/destroyed photographs should be taken at each stage. These may then form part of the record of work or be exhibited themselves
- Where pictures/diagrams etc. are being used as exhibits they should be as jury friendly as possible, for example:
  - Exhibits should be of a size easy to read
  - Use of specialised terms should be kept to a minimum
  - Where there are a series of exhibits if at all possible make all icons and colours consistent with the exhibit throughout

Note

See also Appendix C and Quality of Processes, Peer Review and Record Keeping.

Archiving, Weeding and Disposal

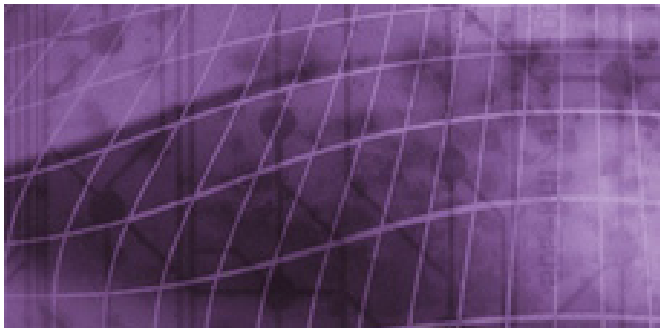
Digital technology poses new risks and threats as well as new opportunities. Its functionality comes with complexity. Reading and understanding digital information requires equipment and software, which is changing constantly and may not be available within a decade of its introduction.

Therefore, in order to comply with existing legislative requirements for the retention of data and information, questions that should be asked and answered in relation to:

Consider	
• Constantly review backup and storage policies. • Make sure fire safes are available and used. • Make sure off site storage is available and policies in place for its use.	• Review weeding policies and ensure compliance. • Make plans for long term retention in the changing technical environment. • Degradation of digital material

NB: Refer to individual force policy on archiving, weeding, disposal. Be aware that retention periods may differ depending on the type of offence being investigated, legislation in respect of civil law, data protection, freedom of information etc..

Investigation Matters



Investigation Matters

It is important that any investigation involving Information and Communication Technology (ICT) is conducted with an acceptable balance between intrusion and privacy. Consideration must be given especially to Articles 6 and 8 of the Human Rights Act 1998 and the Regulation of Investigatory Powers Act (RIPA) 2000.

Many police officers and police staff have a restricted knowledge of ICT. However, ICT is forming an ever increasing element within the overwhelming majority of criminal investigations. Specialist technical investigators can help overcome the obvious difficulties this can cause when conducting an investigation involving ICT by assisting with the development of search and comms data strategies as well as Interview plans or guides.

Consider

- Basic information about the computer and its use
- Data Storage
- Peripherals
- Encryption
- Internet Use
- E-mail
- Online Chat
- Browsing the Internet/ Surfing the Web
- Downloading Files
- Newsgroups
- Computer Security
- Standard Excuses

The Scale and nature of computer-assisted crime

For a comprehensive list of computer-assisted crime supported with practical examples please look at Superhighway Robbery: Preventing e-commerce crime by Graeme R. Newman and Ronald V. Clarke (www.willanpublishing.co.uk) and Introduction To Computer Law by David Bainbridge (www.pearsoned.co.uk) .

Computer assisted crimes

- Theft of telephone services
- Software piracy
- Vandalism
- Terrorism
- Hacking
- Cross-border crime
- Cloning of cellular phones
- Accounting fraud
- Harassment
- Investment fraud
- Sale of illegal/stolen goods
- Gambling Tax evasion
- Criminal conspiracy
- Video piracy
- Copyright
- Spying, industrial espionage
- Electronic funds transfer fraud
- Denial of Service
- Extortion and blackmail
- Credit card fraud
- Stalking
- Money laundering
- Telemarketing fraud
- Identity theft
- Tax evasion
- Aiding and abetting crime

It should be noted that these offences, whilst not exhaustive, appear in most of the nominated Government and ACPO principal objectives.

Intelligence Acquisition and Dissemination

The National Intelligence Model (NIM) drives the work of UK Policing's intelligence community. A key aspect of any soundly based investigative system is the ability to extract information and convert it into usable intelligence.

In a wide variety of crimes involving ICT systems there are new opportunities for intelligence gathering and investigation which exploit information in digital form, even where a computer is neither the target of attack nor the primary tool to commit the crime. Social networking sites in particular have been found to be an extremely useful tool within the intelligence gathering process, such sites can reveal information which would normally only be available through the deployment of surveillance assets. When attempting to access open source intelligence staff should utilise non attributable computer systems and they should consider whether covert authorities are required for the particular activity being undertaken.

It is also worth considering the use of existing software to remotely examine computers, either overtly or covertly providing any such usage complies with the requirements of current legislation.

Risk Assessment

This is an important part of the process which should be automatically considered and completed. The following may assist staff in determining the method of approach to a series of different cases waiting for allocation:

- Physical Vulnerability of victim, suspect and third parties
- Emotional Vulnerability of victim, suspect and third parties
- Professional Vulnerability – suspect's career or vocation damaged
- Economic Impact – suspect's and/or victims business closed down, loss of business reputation
- Time restrictions – evidence may be overwritten
- Impact on Interagency Casework – case is affected by or affects cases in other
- forces and/or agencies or jurisdictions
- Case older than 3 months/ 6 months/8 months/12 months
- National Impact – Denial of Service attacks, Virus distribution etc
- Criminal Justice issues – suspect charged, remanded in custody, on bail or coroners court proceedings
- National Security – imminent threat
- Internal investigation
- Other Factors – Significant Public Interest

Strategies and Tactics

One of the key factors for any manager to understand is the concept of the three quite separate and distinct phases of any investigation involving an ICT or Data Communications Data element:

Consider
• Data Capture • Data Examination • Data Interpretation

There are many different types of media upon which digital material can be stored. Hi-Tech/Computer Crime Units will usually deal only with the most common and will have the equipment to accomplish the tasks of data capture/imaging and digital examination of the material. Their expertise will assist in the interpretation of any relevant digital evidence found.

The first priority on reception of an exhibit containing digital media is securing the data present on that media in such a way the original material is not damaged or changed. This requires specialist equipment and software. In general, this task is called imaging. The imaging process makes a copy of all the data on the media; it secures this by creating a copy of the original on another media. The original can then be re-sealed and all work, further copying (including backups) and examination is done on the image or copies of it.

The examination of the image and identification of relevant data usually takes place on an examination computer set up with specialist software for the purpose. This data can be viewed, extracted and printed as required. The relevant data may also need to be interpreted, either by eye and expertise or by applying software to it to produce tables and reports.

The analyst, having completed their examination of the data, will then if necessary produce a statement or report putting forward the evidence they have found on the media.

For more detail of the process please see forensic matters later in this document.

Quality of Processes

Clearly there is no substitute for quality especially in the area of computer forensics. Units may therefore like to consider adopting the standards provided by various relevant ISO's and which are intended to provide reassurance of ability and quality. Ideal for consideration are:

ISO 9001 – The International Standard for Quality Management. It applies to the processes that create and control the products and services an organisation supplies. It prescribes systematic control of activities to ensure that the needs and expectations of customers are met. It is designed and intended to apply to virtually any product or service, made by any process anywhere in the world.

ISO 17025 - General requirements for the competence of testing and calibration laboratories, the standard covers the operation and effectiveness of the quality management system within the laboratory as well as technical requirements which address the competence of staff, methodology and testing/calibration of equipment. This standard incorporates ISO 9001.

ISO 27001 - a Code of Practice for Information Security Management. It establishes guidelines and general principles for initiating, implementing, maintaining and improving information security management in an organization.

ISO 20000 - a specification and Code of Practice specifically dedicated to IT service management, for the benefit of any enterprise offering IT services. Essentially it details an integrated approach for good service management – a 'good practice' set of principles.

These internationally recognised standards can be used to effect within a computer examination unit to create a quality management system. In practical terms this means that a Hi-Tech/Computer Crime Unit will need to spend some considerable time putting together the various documents required, which in the main will provide Standard Operating Procedures for the unit. These procedures will need to be constantly reviewed because of procedural and process changes due to advances in technology. However, this approach will provide new employees with a quality manual they can look at to understand procedures and practices that take place within the unit at a level of detail that would provide them with path to follow in order to achieve a quality product.

Within a court environment it allows the investigator providing evidence to state, if asked, the fact that the unit works to a qualified international standard for its planning, processes and procedures.

Achieving and maintaining accredited status needs to be managed through the United Kingdom Accreditation Service (UKAS), there are significant costs associated with this, an issue which managers will need to research prior to committing to the accreditation process. Accreditation takes the form of an assessor going through the unit's documentation and looking at its accuracy and quality. The assessor would also review specific digital forensic examinations on arrival, during processing and post completion, then apply the standards from the quality manual to those jobs to assure that practice and procedures are being adhered to. If a unit is planning to embark on implementing these standards they will need to think about appointing a qualified quality manager and document controller. To try and do this without expert advice will be particularly difficult and will inevitably lead to failing the audits and expending additional costs. Applying for, obtaining and retaining these certifications, however worthwhile, is a major, continuous and costly undertaking

What to achieve

- Documented statements of quality policy and quality objectives
- A quality manual
- Documented procedures required by international standard
- Documents needed by the organization to ensure planning, operation and control of its processes and records required by international standard

The Unit should only use properly evaluated techniques and procedures for the forensic examination of digital technology and the interpretation of their evidential significance in the context of the case. In certain cases the use of open source tools may need to be validated through limited in house testing.

Dealing with the Defence

It is now accepted in an increasing range of offences, law enforcement agencies and prosecutors will wish to produce evidence derived from computers and they may use a variety of experts to assist with this. Defence solicitors and counsel will often want to consult their own experts and these too may wish to introduce exhibits of their own The general rules for the serving of evidence, disclosure and arrangements for viewing apply, but computer-derived evidence can generate particular issues.

Experts – The word "expert" can have a number of distinct but overlapping meanings. As far as the courts are concerned, those who are allowed to give expert evidence may, in addition to reporting on what they have seen or done, also offer opinion within their expertise. The competence of an expert witness is governed by the common law. It is open to the prosecution to raise objections about the claimed expertise of a person instructed by the defence and for the defence to challenge the expertise of a prosecution witness. In the final analysis it is for a judge to decide whether, and to what extent, some-one may give evidence of their opinion. The Auld Report on the Criminal Justice System recommended the courts should restrict expert evidence to that which is reasonably required to resolve any issue of importance in the proceedings.

The Auld Report observes:

"There is an increasing tendency, particularly in the criminal courts, for parties to seek to call opinion evidence masquerading as expert evidence on or very close to the factual decision that it is for the court to make. It is for the judges or magistrates to determine whether an issue truly is susceptible to and justifies the calling of expert evidence; in particular whether a proffered expert is likely to be any more expert than anyone else in forming an opinion on separately established facts. In the Crown Court the judge normally directs or indicates at the pre-trial stage whether any particular issue justifies the calling of expert evidence and, if so, of what nature."

As a matter of good practice, an expert report should identify and justify the areas where an opinion is being tendered and make explicit distinctions between a claimed finding of fact and the tendering of an opinion.

An expert's overriding duty in giving evidence is to the court and not to those who are instructing him or her. This applies equally to both prosecution and defence experts. The Auld Report recommended the Criminal Procedure Rules should contain a rule in the same or similar terms to that in Part 35.3 of the Civil Procedure Rules which state that an expert witness's overriding duty is to the court; and that any witness statement or report prepared by an expert witness for the assistance of the court should contain at its head a signed declaration to that effect.

Outside the scope of a trial an expert may also be someone possessed of a specialist skill or area of knowledge. In the context of digital evidence, this expertise may, for example, relate to recovering deleted data, collecting or intercepting data in transmission or the operation of specialist computers. Thus a useful distinction can be made between a forensic technician or practitioner and an "expert" in the sense of having the right to offer an opinion. A forensic technician may not necessarily be competent to give an expert opinion in evidence. Someone may give expert opinion evidence on such matters as social norms of behaviour on parts of the Internet but may lack any associated technical expertise.

Reasons for the instruction of defence experts

Defence solicitors usually instruct a defence expert at a relatively late stage in proceedings and after counsel has been instructed. The range of specific instructions may include:

- To check the integrity and continuity of computer-derived exhibits
- To test any forensic procedures upon which the prosecution are relying
- To explain the nature of the exhibits and their role in the charges which their client face
- To test inferences made by the prosecution and which arise from computer-derived exhibits
- To explain the technical, commercial or cultural environment in which events are alleged to have taken place
- To see how far explanations offered by a defendant can be corroborated from exhibits
- To identify further exhibits which ought to be disclosed
- To provide witness statements which can be served on the prosecution
- To provide testimony in court
- To assist defence counsel in court during cross-examination of prosecution witnesses

Defence expert requirements versus "Court" requirements

In the production of exhibits, law enforcement investigators and prosecutors usually think exclusively of what will be produced in Court. Among other things, this tends to favour the production of exhibits in print-out form. A defence expert, particularly while testing the findings of prosecution experts, is likely to want to examine the material in electronic form, so that computer-based analytic tools can be deployed. Exhibits available to the prosecution in computer-readable form should be made available to the defence in that form. Experts employed by the prosecution should give early consideration to the specific means by which electronic exhibits may be served on the defence. An early task of the defence expert, once instructed, should be to advise those instructing him/her about convenient formats for delivery. Often it may be useful for prosecution and defence experts to contact each other on this matter at an early stage. Such contact would normally be mediated via the CPS and instructing solicitors.

Prosecution witness statements and the use of proprietary analytic tools

There is a large selection of tools and integrated packages available for the analysis of hard-disk and other stored data. Many forensic investigators may use several different tools during an investigation. It is unreasonable to expect a defence expert will have licenses for all such tools that may be deployed. Certain proprietary tools are only made available by their publishers to law

enforcement. In these circumstances prosecution experts have to take particular care to anticipate a defence expert may wish to test their findings, and to consider how they are to be in a position to do so. The following suggestions may be helpful:

- In general terms it is unlikely to be satisfactory simply to say that a specific proprietary package has "found" a file, or produced a chronology of events. The prosecution witness statement must make it clear how the evidence was obtained in sufficient detail for this to be tested by a defence expert.
- In relation to the more extreme forms of data recovery, some generalised explanation such as the technique of recovering entries for directories or the search for strings across a hard-disk may be appropriate. It may also be appropriate to explain that a file was found as an attachment to an email or within an application program email database
- Where a script or grep expression has been used to carry out recurring analytic activities, investigators may need to anticipate a defence expert may wish to test the script performs in the way that is claimed

There have been many occasions when persons appointed by the defence to act as an expert in digital evidence cases have arrived at police premises to examine data and have been unprepared to conduct the work.

This normally takes the form of the person not having any forensic tools with which to conduct an examination of the evidence.

The following points should be remembered:

- Proper facilities for examination should be provided.
- It should be apparent from the prosecution statements, which tools and methodology have been used by the police.
- It is not the responsibility of the police to provide forensic tools for use by defence experts.
- Provision of such tools may be in breach of product licensing conditions.
- Where it is considered that the person appointed by the defence may not be able to conduct the required analysis because of a lack of relevant knowledge or tools, the police should make a report to the CPS. All defendants are entitled to proper representation and the CPS may wish to draw such matters to the attention of the defence solicitors.

"Restricted" Material

Some computer-derived exhibits contain material which is, for one reason or another, deemed restricted in that possession without lawful reason may be illegal, or covered under the Official Secrets Acts and similar legislation, or because of issues of confidentiality and privilege. Some law enforcement agencies and specific police forces follow the practice of permitting defence experts only supervised access to such exhibits. Others release such material at their discretion and against appropriate undertakings.

A particular practical problem is hard-disk "images" which contain sensitive material but which a defence expert will wish to test for overall integrity or to examine inferences drawn from the totality of the data on the disk.

Prosecutors and law enforcement officers should consider the options of releasing sensitive material to defence experts but asking for appropriate formal undertakings to cover such matters as:

- Acknowledgement that the material is restricted and that the sole purpose for which it is being delivered is specific criminal proceedings.
- Handling and copying of the material, including arrangements for physical and logical security controls e.g. the building to be alarmed, the room where analysis takes place to be lockable, items to be stored in a secure area (such as a safe), an exhibit racking system to be in place and encryption to be used where appropriate.
- Agreement not to release any of the material to the custody of the defendant.
- Agreement formally to destroy all copies at the end of instructions.
- Premises of defence "experts" should be examined for suitability.

Forces may also like to consider the security vetting of defence experts and site visits to their premises should be considered if not previously made.

In some circumstances it may be appropriate the undertakings are made to the court and, in the case of commercially sensitive material, to interested third parties. It is always open to defence lawyers to seek a Court Order for release of such information to their expert.

Meetings between Experts

The English Criminal Justice system is based on adversarial principles, although the Auld Report has suggested some areas of amelioration. There is no mechanism, as under the Civil Procedure Rules, for the scope of a dispute to be reduced by mutual agreement, nor is there any formal basis upon which prosecution and defence experts can meet. Nevertheless such meetings may be beneficial, for example:

- To agree areas of technical explanation about which there is no dispute and where it would help the conduct of the trial if the court could be told that the explanation is accepted by the defence
- To allow prosecution experts to demonstrate and defence experts to test, some novel or new forensic procedure
- To agree arrangements where the Prosecution wish to demonstrate some technology in Court; the Defence may also wish to use the demonstration to present alternative explanations

Auld also recommends such meetings take place at the earliest opportunity and before the commencement of trial. Auld goes on to suggest that in certain circumstances the Court may order such meetings to take place.

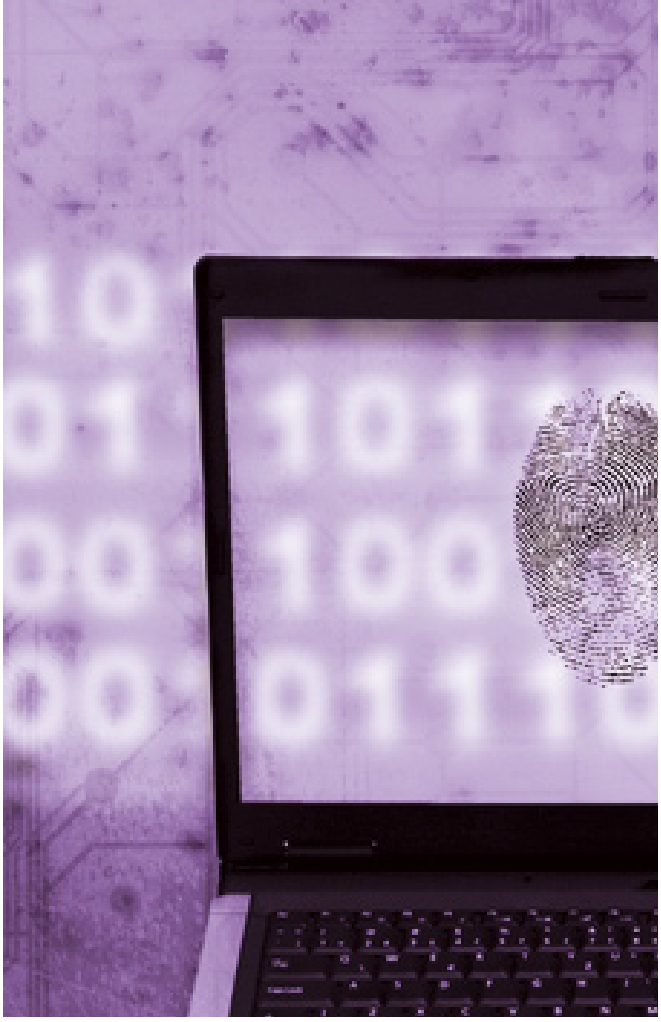
Under normal circumstances such meetings should be under the supervision of the respective instructing lawyers and they may in turn wish to consult the Court. Lawyers need not attend such meetings but where they do not, they may wish to consider providing a note indicating the scope and agenda of such a meeting. However the detail of such arrangements should be a matter for individual instructing lawyers and their sense of the level of experience of such matters of their experts. At the end of such meetings a note should be prepared by the experts to describe what happened and any agreements that were reached; the note can also refer to any issues upon which agreement was sought but not obtained. It is recommended this note, or

Minutes of the meeting, should be signed by all parties and agreement reached on the meaning of the terminology used.

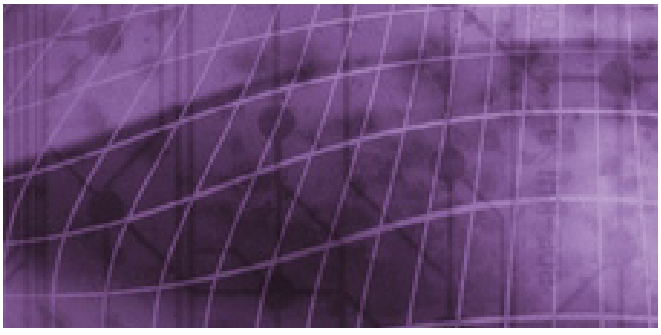
Note

Lord Justice Auld suggested in the Criminal Courts Review the following organisations should co-operate in helping Courts with sources of information about competent experts:

- NPIA Specialist Operations Centre
- The Academy of Experts
- The Expert Witness Institute
- Society of Expert Witnesses
- Forensic Science Society



General Issues



General Issues

There are other matters which need mature reflection and attention to detail in respect of the efficient management of a High-Tech/Computer Crime Unit. This Section attempts to outline some of these.

Searches

It is not within the remit of this document to specify and define methods of searching at premises where digital evidence may be found. Managers of Units should liaise closely with Search Team Co-coordinators and trainers to ensure that all search teams are aware of items which may contain digital evidence relevant to any particular case. Such liaison should keep up to date with the latest in media technology, as there is an increasing move to solid-state storage rather than hard disks. For instance, a secure digital card which is the same size as a normal postage stamp and only 2mm thick can be secreted almost anywhere, in a book, blu-tacked behind a picture or underneath a desktop. Such a card is capable of storing tens of thousands of pages of text and thousands of picture image files. It is **recommended** members of Units should regularly update search team members with current storage media examples and give advice at all search briefings where digital media is likely to be found..

Important Note:

Accepted practice during search and seizure of digital media excludes the seizure of certain items of equipment, for example monitors and keyboards as they are not seen as a source of evidence, nor is their seizure critical to the evidential recovery of digital media from the computer system.

This practice however precludes the obtaining of DNA profiling, particularly from the keyboard, should there be a need to forensically link an individual to use of the computer system. Officers must consider this and other “traditional” forensic options during the pre search planning and risk assessment process.

If DNA swabbing for samples is to be done, it should be carried out at the scene **BEFORE** any members of the search team have touched the article. The method of swabbing should be carefully selected to avoid any internal contamination with liquid of any kind. The item should be marked as being swabbed before bagging, so the unit operative later handling the item is aware and can take precautions to ensure any potential threat to the item is removed prior to examination.

Generally, the fingerprinting of digital exhibits should not take place before the item has been examined and the data on it secured.

Many of the compounds included within common fingerprint dusting powder are electrically conductive. A minute amount of this material on external contacts or internal circuit boards on any digital exhibit is highly likely to render it useless when power is applied. The granules of these compounds are so small as to make it virtually impossible to remove them all without specialist equipment and suitable facilities.

In some cases a value judgement will have to be made balancing the importance of potential fingerprints against loss of digital evidence. If non-conductive powder applied with a previously unused brush is not available, it is recommended the item is examined by the Hi-Tech/ Computer Crime Unit and data secured on separate media before fingerprinting takes place **BUT** only after consultation with the SIO and the force scientific support department.

Think Forensic!

Crown Prosecution Service

It is important to acknowledge the importance of the early involvement of CPS. The CPS as a matter of good practice prefers to be involved at an early stage for a number of very good reasons:

- Identifying avenues to investigate;
- Identifying the kind of evidence which needs to be obtained to enhance the case;
- Minimising the risk of evidence being ruled inadmissible by not being obtained properly, especially in cases involving allegedly corrupt police officers, the use of resident informants and intrusive police techniques etc;
- Identifying potential ECHR issues;
- Advising on the nature of the charge;
- Advising on the charging of minor players in cases involving large numbers of potential defendants;
- Advising on the most efficient groupings of defendants and the knock on effect, to early consideration of indictment;
- Advising on the presentation of evidence;

- Gaining an insight into the size and likely complexity of the case;
- Enabling early CPS planning of resources including allocation of lawyer/caseworker(s);
- Early consideration and selection of the prosecution counsel team;
- Early liaison with the court after charge.

However, from an investigative point of view when operating in this media, it is critical that any liaison with the CPS should involve both the forensic examiner and the investigator. This is so, simply because the examiner is probably best placed to indicate those areas of the evidence which are the best evidence.

The CPS can offer excellent advice on existing Case Law and the impact this will have on an investigation and an examination. Good examples of this can be readily found.

Legal guidance can be obtained from the CPS website – http://www.cps.gov.uk/

Additionally, the CPS is in the process of producing a comprehensive Glossary of universal standard terms. A Glossary of Terms used throughout this document appears at Appendix H and a general glossary of Common Technical Terms appears at Appendix J.

Recent & Intended Changes in Legislation and its impact

> Note
> A current list of some relevant case law is attached at **Appendix F**.

COMPUTER MISUSE ACT 1990 – Amendments

On the 1st October 2007 the Serious Crime Act 2007 was enacted by Parliament. This came into law in October 2008 and it provides revisions to the CMA. Changes to the CMA brought about through the legislation are highlighted in italics.

S.1 - Unauthorised Access to Computer Material

S.1(1) A person is guilty of an offence if:

(a) he causes a computer to perform any function with intent to secure access to any program or data held in any computer, or to enable any such access to be secured;

(b) the access he intends to secure, or to enable to be secured, is unauthorised; and

(c) he knows at the time when he causes the computer to perform the function that this is the case.

S.35 of the Police and Justice Act increases the penalty for this offence on summary conviction to a term of imprisonment not exceeding 12 months, or to a fine or both; on conviction on indictment for a term not exceeding 2 years or to a fine or to both.

There has been much discussion and disagreement between academics and lawyers as to whether or not Denial of Service (DOS) attacks fell within the existing section 3. One court decision (Wimbledon Magistrates Court, Nov 05 – case of RvLENNON) originally upheld the view that this would not be an offence under S.3, however the general belief was that Distributed Denial of Service (DDOS) attacks may be covered although this would depend on the circumstances of the case. This decision was overturned on appeal and LENNON was subsequently convicted in respect of his sending 5 million e-mails to his ex-employer causing the email server to fail. Prior to the decision being reached on appeal the CMA was reworded within Police and Justice Bill.

S.36 of the Police & Justice Act will substitute the existing S3 of the CMA with the following:S.3 Unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer, etc.

S.3 Unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer, etc.

(1) A person is guilty of an offence if –

a. he does any unauthorised act in relation to a computer;
b. at the time when he does the act he knows that it is unauthorised; and
c. either subsection (2) or subsection (3) below applies.

(2) This subsection applies if the person intends by doing the act -

a. to impair the operation of any computer,
b. to prevent or hinder access to any program or data held in any computer,
c. to impair the operation of any such program or the reliability of any such data, or

(3) (3) This subsection applies if the person is reckless

as to whether the act will do any of the things mentioned in paragraphs (a) to (d) of subsection (2) above.

(4) The intention referred to in subsection (2) above, or the recklessness referred to in subsection (3) above, need not relate to -

a. any particular computer;

b. any particular program or data; or

c. a program or data of any particular kind.

(5) In this section –

a. a reference to doing an act includes a reference to causing an act to be done;

b. "act" includes a series of acts;

c. A reference to impairing, preventing or hindering something includes a reference to doing so temporarily.

d. The penalty for this offence is on summary conviction to imprisonment for a term not exceeding 12 months or to a fine not exceeding the statutory maximum or to both. On conviction on indictment, to imprisonment for a term not exceeding ten years, or to a fine or to both.

S.37 of the Act will also create a new offence by inserting after S.3 of the CMA:

S.3A Making, supplying or obtaining articles for use in offence under section 1 or 3

(1) A person is guilty of an offence if he makes, adapts, supplies or offers to supply any article intending it to be used to commit, or to assist in the commission of, an offence under section 1 or 3.

(2) A person is guilty of an offence if he supplies or offers to supply any article believing that it is likely to be used to commit, or to assist in the commission of, an offence under section 1 or 3.

(3) A person is guilty of an offence if he obtains any article with a view to its being supplied for use to commit, or to assist in the commission of, an offence under section 1 or 3.

(4) In this section "article" includes any program or data held in electronic form.

The maximum penalty for this offence on summary conviction is a term of imprisonment not exceeding 12 months or a fine not exceeding the statutory maximum, or both. Upon conviction by indictment, the maximum penalty is a term of imprisonment not exceeding two years, or a fine or both.

Offences will not be committed under the above changes unless they were committed after the date the Act comes into force. An offence is not committed under S.3A unless every act or other event proof of which is required for conviction of that offence takes place after S.37 comes into force.

Fraud Act 2006

The Fraud Act 2006 came into force on the 15th January 2007 and creates a new general offence of fraud with a maximum sentence of ten years; replacing all previous deception offences. It did however NOT abolish the common law offence of conspiracy to defraud.

Section 1: Fraud

Section 1 creates a new general offence of fraud and introduces three possible ways of committing it. The 3 ways are set out in section 2, 3 and 4.

Section 2: Fraud by false representation

Section 2 makes it an offence to commit fraud by false representation. The representation must be made dishonestly, with the intention of making a gain or causing a loss or risk of loss to another. The gain or loss does not have to take place. The representation may be express or implied. It can be stated in words or communicated by conduct. There is no limitation on the way in which the representation must be expressed so it could be written or spoken or posted to a web site. It could also be by way of conduct for example where a person dishonestly misuses a credit card to pay for items. The offence would also be committed by someone who engages in "phishing". Subsection 5 of this section provides that a representation be regarded as made if submitted in any form to any system or device designed to receive communications etc with or without human intervention.

Section 3: Fraud by failing to disclose information

Section 3 makes it an offence to commit fraud by failing to disclose information to another person where there is a legal duty to disclose the information.

Section 4: Fraud by abuse of position

Section 4 makes it an offence to commit a fraud by dishonestly abusing one's position. It applies in situations where the defendant has been put in privileged position, and by virtue of this position is expected to safeguard another's financial interests or not act against those interests.

PART III RIPA 2000– Investigation of Electronic Data Protected by Encryption, Powers To Require Disclosure - came into effect on the 1st October 2007.

Where you lawfully come into possession of material which has been protected by encryption and you have reasonable grounds to believe that the key to the protected information is in the possession of any person you can, if the relevant requirements as laid down in Part III are met, require that person to disclose the key. Failing to comply with this requirement is an either way offence and on conviction carries a maximum penalty of an appropriate maximum term, or a fine or both. The maximum penalty for this offence, as per amendment by S.15 or the Terrorism Act 2006, is 5 years for cases of national security and in any other case two years.

A Code of Practice "Investigation of Protected Electronic Information" relates to the powers and duties conferred or imposed under Part III, RIPA. It provides guidance to be followed when exercising powers under Part III. The National Technical Assistance Centre (NTAC) is the lead national authority for all matters relating to the processing of protected information into intelligible form, all public authorities should consult with NTAC at the earliest opportunity when considering the exercise of the powers in Part III. No public authority may serve any notice under section 49 of the Act, or when the authority considers it necessary, seek to obtain appropriate permission without the prior written approval of NTAC to do so. The Code of Practice is available from the following source:

http://security.homeoffice.gov.uk/ripa/publication-search/ripa-cop/electronic-information

NTAC can be contacted through force control rooms, in force digital forensic providers or via:

ripaiii@ntac.gsi.gov.uk

Proposed amendments to the Obscene Publications Act 1959

At present the Obscene Publications Act does not make an offence of straight forward possession. Therefore, it would not cover someone downloading material from the internet purely for their own use. In respect of this issue the Home Office published a consultation document in respect of making it an offence to possess extreme pornography. This consultation resulted in an announcement on the 30th August 2006 that possession of violent and extreme pornographic material will become a criminal offence punishable by up to 3 years imprisonment. The type of material to be covered would be of the same nature that the Obscene Publications Act 1959 makes it an offence to publish or distribute. The new law is intended to ensure possession of violent and extreme pornography is illegal both on and offline and has been included within the Criminal Justice and Immigration Bill. At the time of writing this document S113 of the Bill relates to the offence and S116 of the Bill looks to increase the penalty for publication of obscene articles from 3 years to 5 years.

There are also **proposals to extend the definition of a photograph** within the Criminal Justice and Immigration Bill. Having passed through the House of Commons this Bill received its' first reading in the House of Lords on the 9th January 2008. Section 118 of the Bill intends to include "a tracing or other image, whether made by electronic or other means which is not itself a photograph or pseudo-photograph but which is derived from the whole or part of a photograph or pseudo photograph. It will also include data stored on a computer disc or by other electronic means which is capable of conversion into an image."

Liaison with Force/Other Agencies

It is easy to become cocooned in an environment which is totally technology based and to forget the assets available to you outside that environment. One such asset is the force call centre. Ask yourself the questions:

'What have I done to brief the staff in the call centre/ crime desk on the aims and objectives of the unit?'

'What have I done to brief the staff in the call centre/ crime desk on how they can provide a better service to the public in relation to ICT issues and at the same time prevent unnecessary telephone calls to the Unit?'

Consider

- Identifying frequent complaints
- Outlining what the criminal does in relation to each
- Recommend what the victim/complainant should do
- Provide general advice in relation to each

In relation to the second question:

What sort of information are you going to ask your colleagues in your own force and those in surrounding forces to provide you with?

Suggestion

- Information that shows the nature and scale of the problem
- Information that contributes to intelligence gathering on the threats, vulnerabilities and adversary capabilities.
- Information that identifies incidents and supports their investigation

Note

Dorset has prepared a Guide for Call Centre operators. This guide along with two hours of training for all call center staff as to what an e-Crime is and what the HTCU was responsible for had a dramatic effect on the reduction of incorrectly directed telephone calls to the unit.

Other Matters

Ask yourself the questions:

- What broad investigative templates have we to cope with the many and different crimes? For example, tackling an auction fraud committed via E-bay or ensuring all machines are examined first for Trojans or other malicious software.
- What proactive interventions have we prepared?
- How am I keeping my ACPO managers briefed and up to-date on the issues?
- Should I consider briefing the Police Authority?
- How do I keep myself up to-date?

Sources of Advice and Points of Reference

There are plenty of technical sources of information for Managers of Hi-Tech/Computer Crime Units. In fact there are so many it is difficult to know which to choose or subscribe to. By way of illustration only attention is drawn to a Digital Evidence Publication available from Science Direct – Digital Investigations. It provides a facility to download in PDF format a number of technical and other 'papers'.

The SOCA e-Crime, ACPO Hi-Tech Crime Sub-Group, NPIA, Digital Evidence Group, The Centre for Forensic Computing and F3 all offer sources of information and assistance.

National Policing Improvement Agency (NPIA)

The NPIA, E-Crime Training Unit is in the business of developing high quality training solutions for criminal investigations involving a technical element e.g. network investigation, covert internet investigation, communications data SPOC and digital evidence recovery.

The National E-crime training strategy and modular training programme is being developed to meet the needs of the police service and NPIA partners in support of the National E-Crime Strategy, which increased the capacity of law enforcement to combat the criminal use of technology.

See Appendix G for other Sources of Information

The Head of E-Crime Training leads the training team that is drawn from a variety of backgrounds, with knowledge and skills in e-crime, training and regulatory arena's.

The assistance of training requirement user groups is a key part of the development of a dynamic programme that is dealing with daily changes in technology and its abuse by the criminal. One key deliverable is the awareness programme for new recruits and this will be the foundation upon which the future of the programme will expand and develop to include all levels within the service.

Academic and professional accreditation for the training programme has been a key objective to enhance credibility within the law enforcement, business and judicial communities. The team has worked with relevant organisations and authorities to achieve this aim and is a contributor to an EU Commission programme examining similar issues on a Europe wide basis. See Appendix C for details.

NPIA is positioned to provide information and advice on training matters and has existing partnerships with training organisations in the UK and abroad that enhance its capability to support High-Tech crime training for the UK police service.

The High-Tech crime training team may be contacted by telephone on 01480 401986 or by email on enquiries_ecrimetraining@npia.pnn.police.uk

NPIA Specialist Operations Centre

The Specialist Operations Centre offers its service as the gateway to NPIA's Specialist Operational Support providing information and specialist law enforcement advice on:

- Doctrine and its implementation
- The lawful and effective use of covert techniques
- The investigation of murder, no-body murder, suspicious missing persons, rape, abduction and serious sexual offences
- Public order and operational planning
- Disaster Management and the policing of major incidents
- The police use of firearms
- Access to the deployable resources of their Crime and Uniform Operational Support departments.

The Specialist Operations Centre is open Monday-Thursday 9am-5pm and Friday 9am-3pm and can be contacted by telephone 0870 241 5641 or by e-mail on soc@npia.pnn.police.uk

Further information can be obtained via www.npia.police.uk

National Technical Assistance Centre (NTAC)

NTAC is a twenty-four hour centre run directly through the Home Office. It is operated on behalf of all the law enforcement, security and intelligence agencies. It provides a central facility for the complex processing needed to derive intelligible material from lawfully intercepted computer to computer communications and from lawfully seized computer data that are increasingly encrypted. The service is completely free to law enforcement. NTAC is the lead national authority for all matters relating to the processing of protected information into intelligible form, all public authorities should consult with NTAC at the earliest opportunity when considering the exercise of the powers in Part III RIPA 2000. No public authority may serve any notice under section 49 of the Act, or when the authority considers it necessary, seek to obtain appropriate permission without the prior written approval of NTAC to do so.

Centre for the Protection of National Infrastructure (CPNI)

CPNI is an interdepartmental organisation formed as a result of the merger of the National Infrastructure Security Co-Ordination Centre (NISCC), part of MI5 and the National Security Advice Centre. NISCC provided advice and information on computer network defences and other information assurance issues. NSAC provided advice on physical security and personnel security issues.

CPNI provides integrated (combining information, personnel and physical) security advice to the businesses and organisations which make up the national infrastructure (communication, emergency services, energy, finance, food, government, health, transport, water.)

Further information can be obtained from www.cpni.gov.uk

The Digital Evidence Group (DEG)

The principal purpose of this Group is to contribute to the development and delivery of high quality forensic recovery and examination of digital evidence throughout the various UK Law Enforcement, Government Departments and associated agencies.

It has a number of specified Goals, which are as follows:

- To provide a channel by which UK Law Enforcement, Government Departments and associated agencies can co-ordinate strategic activities relating to the forensic recovery and examination of digital evidence.
- To seek opportunities for co-operation and to minimize duplication of effort and waste of resources.
- To act as the UK focus for the acquisition, consideration and dissemination of national and international information concerning good practice in the recovery of digital evidence from the increasing variety of technologies encountered in criminal investigations.
- To provide expert opinion to Government, participating and associated agencies.

Its membership includes the following organisations:

ACPO
BT
CFFC
CPS
FSS
HM Revenue & Customs
Metropolitan Police DO17 (3)
NPIA
NTAC
PSNI
SFO
SOCA

If you have issues or concerns that have an impact upon the field of digital evidence acquisition, processing handling and presentation that you would want the Digital Evidence Group to address or have any queries, please contact the Secretary of the Group – Lindy Sheppard at l.c.sheppard@cranfield.ac.uk

The Centre for Forensic Computing (CFFC)

The Centre for Forensic Computing of Cranfield University at the Royal Military College of Science, Shrivenham has been formed as a Centre of Excellence in the Forensic Field. It is a non-profit making unit which has a very close relationship with the Digital Evidence Group.

Details of some of the Courses available at CFFC appear in Appendix C.

Contact:
Further information can be obtained at www.cranfield.ac.uk or telephone The Centre for Forensic Computing (01793 785810)

F3 – First Forensic Forum

F3 is a non-profit making organisation open to all Forensic Computer Practitioners in the U.K. and Europe. It takes no note of which 'side' the practitioner tends to represent. It exists for the benefit of its members in terms of the exchange of knowledge, information and best practice. Importantly, it provides 'Training Days' at little cost, with experts in the field giving of their time for no financial benefit. Run by a small committee of volunteers, F3 also holds an annual conference where current topics in Forensic Computing are openly and freely discussed. Networking and the exchange of information between practitioners is at the core of F3's raison d'etre, members are encouraged to make use of the information and discussion forums on their web-site.

Membership of F3 is regarded as a 'must' for those seeking high-quality, and cheap, training on specific issues and topics. Contact: lindysheppard@f3.org.uk

Internet Watch Foundation

The IWF, launched in the Autumn of 1996, is the only recognised organisation in the UK operating an internet 'Hotline' for the public and IT professionals to report their inadvertent exposure to potentially illegal content online. Their aim is to minimise the availability of potentially illegal internet content, specifically:

- child sexual abuse images hosted anywhere in the world
- criminally obscene content hosted in the UK
- incitement to racial hatred content hosted in the UK

They work in partnership with UK Government departments such as the Home Office, the Ministry of Justice and the Department for Business, Enterprise and Regulatory Reform to influence initiatives and programmes developed to combat online abuse. This dialogue goes beyond the UK and Europe, to ensure greater awareness of global issues and responsibilities.

They are a self-regulatory body, funded by the EU and the wider online industry. This includes internet service providers (ISPs), mobile operators and manufacturers, content service providers, telecommunications and filtering companies, search providers and the financial sector as well as blue-chip and other organisations who support them for corporate social responsibility reasons.

Through the 'Hotline' reporting system, they help ISPs to combat abuse of their services through a 'notice and take-down' service by alerting them to any potentially illegal content within their remit on their systems and simultaneously inviting the police to investigate the publisher.

As a result, less than 1% of potentially illegal content has apparently been hosted in the UK since 2003, down from 18% in 1997.

The IWF is a key component in the UK's Industry/Police/Government partnership for tackling illegal content online. This partnership has proved extremely successful over the years in facilitating the swift removal of potentially illegal content from UK servers and vastly reducing the overall volume of child abuse images found to be hosted in the UK.

Police Officers provide input into the image assessment element of the training for new hotline Internet Content Analysts, ongoing training of analysts and the IWF provide technical Internet training for new police staff on occasions.

The IWF has positive links to most British Police Forces, however their main operational contacts are:

- Child Exploitation and Online Protection Centre (CEOP)
- Virtual Global Taskforce
- Serious Organised Crime Agency (SOCA)
- The Metropolitan Police Paedophile Unit
- West Midlands Police Hi Tech Crime team
- Greater Manchester Police Abusive Images Unit
- The National Hi-Tech Crime Unit Scotland (NHTCUS)

The IWF is also a member of the INHOPE (Internet Hotline Providers in Europe) Forum, which facilitates co-operation and exchange of information between similar initiatives in Europe. Details of INHOPE can be found at: https://www.inhope.org/

Any UK resident can contact the IWF 24 hours a day to let them know about material they have seen on the Internet which they consider to be potentially illegal. More information about the IWF, what to report and how to contact the IWF can be found at their Web site at www.iwf.org.uk telephone 01223 237 700 or e-mail information@iwf.org.uk

Serious Organised Crime Agency (SOCA) E-Crime

SOCA e-crime was formed from the former National High Tech Crime Unit (NHTCU) and is now part of SOCA.

Child Exploitation and Online Protection (CEOP) Centre

The Child Exploitation and Online Protection Centre (CEOP) is a police-led UK national centre dedicated to tackling the sexual abuse and exploitation of children and young people, including where technology may be a factor in that abuse or exploitation. CEOP takes a multi-agency and holistic approach to tackling this complex issue and its remit includes intelligence gathering and dissemination, supporting the work of public protection units through its offender management team, operational support to police forces by way of Behavioural Analysis, Financial investigation, Victim Identification and Covert Internet Investigation, producing strategic advice and guidance on tackling issues such as child trafficking, through to harm reduction measures such as education programmes for children and young people and training for frontline professionals. It acts as a single point of contact for reports of sexual abuse and exploitation from the public (through its online reporting mechanism), the internet and mobile companies, children's charities and law enforcement, both in the UK and abroad. It is first and foremost a child protection agency, which many of its partnerships with both the public and private sectors have been predicated upon.

CEOP has built partnerships with children's charities, industry partners, education establishments, government departments and law enforcement agencies at home and abroad to bring a holistic approach to tackling child sex abuse. CEOP also represents the UK in the Virtual Global Taskforce - an international alliance of law enforcement agencies set up to provide a global response to child sexual exploitation. It works alongside specialists, educators and investigators by adding value, expert knowledge and skills to the good work already taking place at the front line of child protection.

The Chief Executive of CEOP holds ACPO portfolios in the following areas:

- Child Abuse Investigation
- Combating child abuse on the internet
- Travelling Sex Offenders
- Child Trafficking
- Extreme pornography
- Data Communications.

Annually, CEOP produces a Strategic Overview document in an unclassified and restricted format which highlights current developments and areas of concern regarding this crime area.

Specialist Operational Support Faculty

The former Operations Faculty has been renamed the Specialist Operational Support Faculty. This change in title reflects the relationship it has developed in supporting the range of child protection services. The Faculty provides support particularly to police forces, international law enforcement agencies and non governmental organisations, and disseminates intelligence (largely to an evidential standard) leading to safeguarding and intervention activity which protects children, whilst holding offenders to account.

The Faculty provides the following distinct functions:

- The Covert Operations Team which infiltrates networks of paedophiles with a strong emphasis in the online environment.
- The Financial Investigation Team which investigates the commercial distribution of abuse images. This work involves working with partners and other stakeholders to develop an enhanced understanding of the offending environment to inform and influence industry involvement, whilst undertaking target investigations. The team also produces tactical lifestyle analysis and enhances offender management risk assessment.
- The Image Analysis and Victim Identification Team works predominantly with the police service, investigating contemporary child abuse captured in still and video images. This role is delivered through crime investigation, safeguarding children strategies, maintenance of ChildBase and national \ international coordination.
- The Faculty has a small computer forensic data recovery service. This resource can strengthen existing force capability, with access to industry through partner relationships.
- There are NSPCC Child Protection Officers embedded within the faculty. These trained social workers give guidance on safeguarding children strategies and advice on complex case work. Where appropriate, they will provide assistance in developing victim interview plans.
- Best evidence interviews
- Advice and guidance for Senior Investigating Officers
- Advice on interview strategies and risk management (via the Behavioural Analysis Unit)

Whilst providing these key support services, the Faculty also performs roles that include Tactical Advisor (including Senior Child Protection Advisors) and Field Intelligence Officers.

As the Faculty continually addresses new child protection policing challenges, it is designed to flex to demand, drawing in external specialists as appropriate.

CEOP Specialist Operational Support Faculty coordinates all covert internet investigations relating to child sexual abuse conducted by UK law enforcement and where necessary, in liaison with foreign counterparts. CEOP can, on a case by case basis, provide access to and / or signpost specialist resources either through industry relationships (e.g. encryption / data communications resolution), access to UK intelligence agencies where appropriate or to solve particular challenges within the operational environment.

The Image Analysis and Victim Identification Team (VIT) receive submissions of indecent images of children from a large number and wide range of UK Police Forces and other organisations for the purposes of identifying victims of child abuse. The VIT work closely with the international law enforcement partners (such as Europol and Interpol) that are involved in this specialist area of work. CEOP's VIT liaise with such partners to facilitate the identification of victims as well as to ensure there is a coordinated approach to identify children. The team utilises various types of software as part of their work and this includes the maintenance of database of child abuse images (Childbase) to assist in carrying out single or joint investigations in the UK and abroad to locate, identify and safeguard victims.

The Financial Intelligence team is staffed by accredited financial investigators who support CEOP and UK and International law enforcement in the investigation of suspects who have benefited from criminal activity connected to the production and distribution of indecent images of children. In addition, they assist in the identification and location of suspects for wider CEOP and Police investigations. The Financial Intelligence Team work closely with US and European partners to develop intelligence and operational activity against websites and the organisers that profit from the distribution of child abuse images.

Intelligence Faculty

The main function of the Intelligence Function is to provide intelligence to UK law enforcement about child sexual abuse and offenders. CEOP receives information from a range of sources including members of the public, the online and communications industry, children's charities and law enforcement. It will disseminate tactical intelligence to UK law enforcement and children's services to ensure children are safeguarded and offenders are identified. Additionally CEOP will provide strategic intelligence and knowledge based products to UK law enforcement, including the annual strategic overview.

CEOP uses a network of SPOCs in forces to disseminate all intelligence products to, as well as providing a quarterly update.

CEOP also engages and supports UK police forces in offender management issues. The UK Tracker team

works to locate missing high and very high risk registered Child Sexual Offenders and provides a range of services to support forces in this task, including the Most Wanted website. The Overseas Tracker team works to disrupt UK nationals who travel abroad to abuse children. This team focuses on those individuals who are not RSOs and seeks to disrupt their activities and bring such individuals back to the UK to be managed appropriately.

Harm Reduction Faculty

Harm Reduction initiatives are designed to prevent and deter the sexual abuse of children, learning from the work of the intelligence and operational faculties, as well as what is happening elsewhere in the world, so that we can have a better informed response to deal with the problem of child sexual exploitation.

CEOP's public awareness and education programmes, which has reached 4.5 million children and young people across the UK since it was launched in September 2006, are delivered by the Education Team. CEOP is also the UK-node for the EU's Safer Internet Plus programme which focuses on education and public awareness on internet safety and security issues for children and young people. This is supported by CEOP's Youth Advisory Panel (YAP) made up of children and young people from across the UK who help to advise and inform the development of CEOP's programme of work, with a particular focus on education and public awareness.

Accredited training is also delivered by CEOP to professionals who work to protect children and is designed to up skill those tasked with investigating offences, dealing with victims and offenders with necessary knowledge about child sex offending in both the on and offline worlds. CEOP also works closely with the online and mobile environments to look to making those services safer by design. These programmes are informed by the knowledge developed by the intelligence teams and the work of its Behavioural Analysis Unit (BAU).

CEOP has established the BAU which is designed to learn more about the nature of sexual abuse involving children from both the offender and the victim's perspective. This will lead to a better informed response to abuse involving children and young people. As part of their work they conduct debriefs with offenders to examine and understand their motivation and tactics. In addition they provide specialist support to senior and investigating officers on interview strategies and approaches with child sexual offenders, as well as undertaking risk assessments.

Child Trafficking Unit aims to provide a child protection perspective to overall efforts to tackle Trafficking in Human Beings. The CTU works closely with, and supports the work of, the Home Office, Department for Children, Schools and Families (DCSF), the UK Human Trafficking Centre (UKHTC) and SOCA in this respect. The creation on the unit fulfils CEOP's desire to ensure that it focuses on offline child exploitation, not just the online element - and utilises new and existing skills within the Centre to help tackle this aspect of crimes against children.

Lastly, by no means least is the work that Harm Reduction does to build relations with key stakeholders in government, the charitable sector and industry both nationally and internationally to inform them about our work and influence their agendas to provide better protection for children and young people everywhere, as well as conducting or facilitating research to support this. Led by the International and Relations Desk, this work has been supported by secondments from DCSF, Department of Health (DH) and the Australian Federal Police (AFP). The International and Relations Desk also provides the secretariat function for the Virtual Global Taskforce (VGT); an international collaboration of law enforcement agencies committed to working together to tackle child exploitation, and comprising of Australia, Canada, Interpol, Italy, UK and the US.

General enquiries	
CEOP general enquiries:	0870 000 3344
CEOP media enquiries:	0870 000 3434
Further information:	www.ceop.gov.uk
	www.thinkuknow.co.uk
	www.virtualglobaltaskforce.com

Specific enquiries	
Intelligence:	intelligence@ceop.gsi.gov.uk
Operations:	CEOPtasking@ceop.gsi.gov.uk
Behavioural Analysis Unit:	bau@ceop.gsi.gov.uk
Education:	education@ceop.gsi.gov.uk
Training:	training@ceop.gsi.gov.uk

ChildBase & Hash Sets

Approximately 900,000 unique images are held on a database known as ChildBase. Searches on newly seized material can be undertaken against the database using the unique MD5 Hash assigned to individual images or by integrated facial recognition software.

Updated Hash Sets of the stored ChildBase images are regularly made available to force High Tech/Computer Crime Units. The main purpose of distributing these Hash Sets is to easily identify images which are NOT already contained within ChildBase and thereby lessen the volumes of images which need to be submitted to the centre for uploading into ChildBase and further analysis by the Victim Identification Team.

The Hash Sets are for Law Enforcement Use Only and should NOT be distributed outside the Force they are issued to. They can only be used by Commercial Forensic Computing Organisations if that organisation is working on behalf of a Law Enforcement Agency and then only if a Memorandum of Understanding is drawn up stipulating they may only be used for the duration of the examination for which they have been issued.

The following is a definition of the categories currently allocated:

NB: The Categories given are those issued by the Sentencing Advisory Panel PRIOR to 1st May 2007.

0 = Non-Indecent Images of children. These are images which may form part of a series of images which depict child abuse but which on their own would not constitute an indecent image

1 = Images depicting nudity or erotic posing, with no sexual activity.

2 = Sexual activity between children, or solo masturbation by a child

3 = Non-penetrative sexual activity between adult(s) & child(ren)

4 = Penetrative sexual activity between child(ren) and adult(s)

5 = Sadism or bestiality

A = Adult pornographic images

B = Non pornographic or indecent images (banners, software gifs etc)

NC = Not Yet Categorised

VID = Videos held by CEOP

Victim Identification Investigations

If you become aware of images which you suspect may be of unidentified child victims or known victims (as yet unreported to ChildBase) you must contact the CEOP Victim Identification Team prior to commencing an investigation or circulating the images. Apart from the need to avoid duplication of effort we all have a responsibility not to re-victimise children through the unnecessary circulation of their abusive situation.

If you wish to submit images for comparison, have queries with loading the Hash Sets or the categories or require any information regarding victim identification issues please contact the Victim Identification Team on mail to: victimid@ceop.gsi.gov.uk

Single Points of Contact (SPOCs)

The following information is provided in respect of the role of the SPOC in obtaining communications data during a criminal investigation. Relevant to this role is RIPA 2000 Part I Chapter II

- **Communications Data**

The term ‘communications data’ embraces the ‘who’, ‘when’ and ‘where’ of a communication but not the content, not what was said or written. It includes the manner in which, and by what method, a person or machine communicates with another person or machine. It excludes what they say or what data they pass on within a communication including text, audio and video (with the exception of traffic data to establish another communication such as that created from the use of calling cards, redirection services, or in the commission of ‘dial through’ fraud and other crimes where data is passed on to activate communications equipment in order to obtain communications services fraudulently).

Communications data is generated, held or obtained in the provision, delivery and maintenance of communications services, those being postal services or telecommunications services.

Communications service providers may therefore include those persons who provide services where customers, guests or members of the public are provided with access to communications services that are ancillary to the provision of another service, for example in hotels, restaurants, libraries and airport lounges.

• Traffic Data

This is data that is or has been comprised in or attached to a communication for the purpose of transmitting the communication and which 'in relation to any communication':

identifies, or appears to identify, any person, equipment or location to or from which a communication is or may be transmitted;

> identifies or selects, or appears to identify or select, transmission equipment;

> comprises signals that activate equipment used, wholly or partially, for the transmission of any communication (such as data generated in the use of carrier pre-select or redirect communication services or data generated in the commission of, what is known as, 'dial through' fraud);

> identifies data as data comprised in or attached to a communication. This includes data which is found at the beginning of each packet in a packet switched network that indicates which communications data attaches to which communication.

• Service Use Information

Data relating to the use made by any person of a postal or telecommunications service, or any part of it, is widely known as 'service use information' and falls within section 21(4)(b) of the Act.

Service use information is, or can be, routinely made available by a CSP to the person who uses or subscribes to the service to show the use of a service or services and to account for service charges over a given period of time. Examples of data within the definition at section 21(4)(b) include:

> itemised telephone call records (numbers called);

> itemised records of connections to internet services;

> itemised timing and duration of service usage (calls and/or connections);

• Subscriber Information

The third type of communication data, widely known as 'subscriber information', is set out in section 21(4)(c) of the Act. This relates to information held or obtained by a CSP about persons to whom the CSP provides or has provided a communications service. Those persons will include people who are subscribers to a communications service without necessarily using that service and persons who use a communications service without necessarily subscribing to it.

The Roles Outlined

Acquisition of communications data under the Act involves four roles within a relevant public authority:

- the applicant
- the designated person
- the single point of contact
- the senior responsible officer

The Applicant

The applicant is a person involved in conducting an investigation or operation for a relevant public authority who makes an application in writing or electronically for the acquisition of communications data. The applicant completes an application form, setting out for consideration by the designated person, the necessity and proportionality of a specific requirement for acquiring communications data.

The Designated Person

The designated person is a person holding a prescribed office in a relevant public authority who considers the application and records his considerations at the time (or as soon as is reasonably practicable) in writing or electronically. If the designated person believes it is necessary and proportionate in the specific circumstances, an authorisation is granted or a notice is given.

The Single Point of Contact

The single point of contact (SPoC) is either an accredited individual or a group of accredited individuals trained to facilitate lawful acquisition of communications data and effective co-operation between a public authority and CSPs. To become accredited an individual must complete a course of training appropriate for the role of a SPoC and have been issued a SPoC Personal Identification Number (PIN). Details of all accredited individuals are available to CSPs for authentication purposes.

An accredited SPoC promotes efficiency and good practice in ensuring only practical and lawful requirements for

communications data are undertaken. This encourages the public authority to regulate itself. The SPoC provides objective judgement and advice to both the applicant and the designated person. In this way the SPoC provides a "guardian and gatekeeper" function ensuring that public authorities act in an informed and lawful manner.

The SPoC should be in a position to:

- engage proactively with applicants to develop strategies to obtain communications data and use it effectively in support of operations or investigations;
- assess whether the acquisition of specific communications data from a CSP is reasonably practical or whether the specific data required is inextricably linked to other data;
- advise applicants on the most appropriate methodology for acquisition of data where the data sought engages a number of CSPs;
- advise applicants and designated persons on the interpretation of the Act, particularly whether an authorisation or notice is appropriate;
- provide assurance to designated persons that authorisations and notices are lawful under the Act and free from errors;
- provide assurance to CSPs that authorisations and notices are authentic and lawful;
- assess whether communications data disclosed by a CSP in response to a notice fulfils the requirement of the notice;
- assess whether communications data obtained by means of an authorisation fulfils the requirement of the authorisation;
- assess any cost and resource implications to both the public authority and the CSP of data requirements.

The Senior Responsible Officer

Within every relevant public authority a senior responsible officer must be responsible for:

- the integrity of the process in place within the public authority to acquire communications data;
- compliance with Chapter II of Part I of the Act and with this code;
- oversight of the reporting of errors to IOCCO and the identification of both the cause(s) of errors and the implementation of processes to minimise repetition of errors;
- engagement with the IOCCO inspectors when they conduct their inspections, and
- where necessary, oversee the implementation of post-inspection action plans approved by the Commissioner.

Data Held Overseas

Applications for communications data held outside the United Kingdom:

Advice on obtaining communications data from countries outside the UK can be obtained from the SPOC.

Mutual Legal Assistance Treaty (MLAT)

Working relations with the United Kingdom's counterparts in other countries are often formalised under a Mutual Legal Assistance Treaty. This means that authorities in different countries can call on each other's resources and powers to conduct investigations in their own jurisdictions.

The G8 Process

Investigations involving electronic evidence that require urgent assistance from foreign law enforcement make it imperative for technically literate investigators to move at unprecedented speeds to preserve data and locate suspects. Therefore, to enhance and supplement (but not replace) traditional methods of obtaining assistance, the G8 has created a mechanism to expedite contacts between countries and there are now 24-hour points of contact for cases involving electronic evidence. To use this network, law enforcement agents seeking assistance from a foreign state may contact the 24-hour point of contact in their own state, and this individual or entity will, if appropriate, contact his or her counterpart in the foreign state.

SOCA e-Crime are the point of contact for G8 requests made from UK Law Enforcement Agencies for the preservation of data held overseas and also for requests received from Foreign Law Enforcement Agencies asking for data residing within the United Kingdom to be subjected to a preservation order.

Officers should be aware that some other countries have different rules on disclosure, with subjects of requests for communications data subsequently being formally notified of the enquiry.

Issues Specific to the SPOC in e-Crime Investigation

No current Authorisation / Service Level Agreements are in existence for the retrieval of Internet related data from ISPs. All RIPA enquiries to access Internet related data are performed via a Notice sent manually to an ISP. In the near future it is likely that a European Directive will mandate all ISPs to hold records of their data for a period of 12 months e.g. traffic data, financial and subscriber information.

In addition to RIPA enquiries it should be noted that organisations such as EBay and Website Hosting companies are not classified as ISPs. Best Practice dictates the enquiries for access to communications data held by these types of organisations should be carried out by the Comms Data SPOC via Data Protection Legislation. The role of the SPOC in the arena of Internet based crime incorporates the handling of a wide range of complex and time specific logging data held on a range of Computer Hosts, for example, Internet Protocol (IP) address communications logged against RADIUS, Web or Mail Servers denoting access to personal account data.

On accessing Server logging data against a subject account, the preparation of subsequent RIPA notices to ISPs in possession of a given IP communication will form the basis of SPOC applications for IP address to subscriber details. This procedure necessitates the SPOC to satisfy the following with each identified ISP to minimise the impact of collateral intrusion in the identification of a subscriber to IP address;

- A Computer Server retaining log data has been synchronised to an Atomic clock
- The correct date, timestamp and time zone have been logged against the IP address
- The type and status of the Internet Protocol (IP) address communication

Forfeiture – Use of Seized Equipment

Section 143(1) Powers of Criminal Courts (Sentencing) Act 2000 says where a person is convicted of an offence and the Court by or before which he is convicted is satisfied that any property which has been lawfully seized form him, or which was in his possession or under his control at the time he was apprehended for the offence or when a summons in respect of it was issued:

a) Has been used for the purpose of committing or facilitating the commission of any offence, OR

b) Was intended by him to be used for that purpose

The Court may (subject to Section 5) make an order under this section in respect of that property. There is a case in respect of forfeiture the details of which are as follows:

"Regina v Jonathan Aslett, Manchester Crown Court, 25 September 2002, Neutral Citation No: T2001/0383.

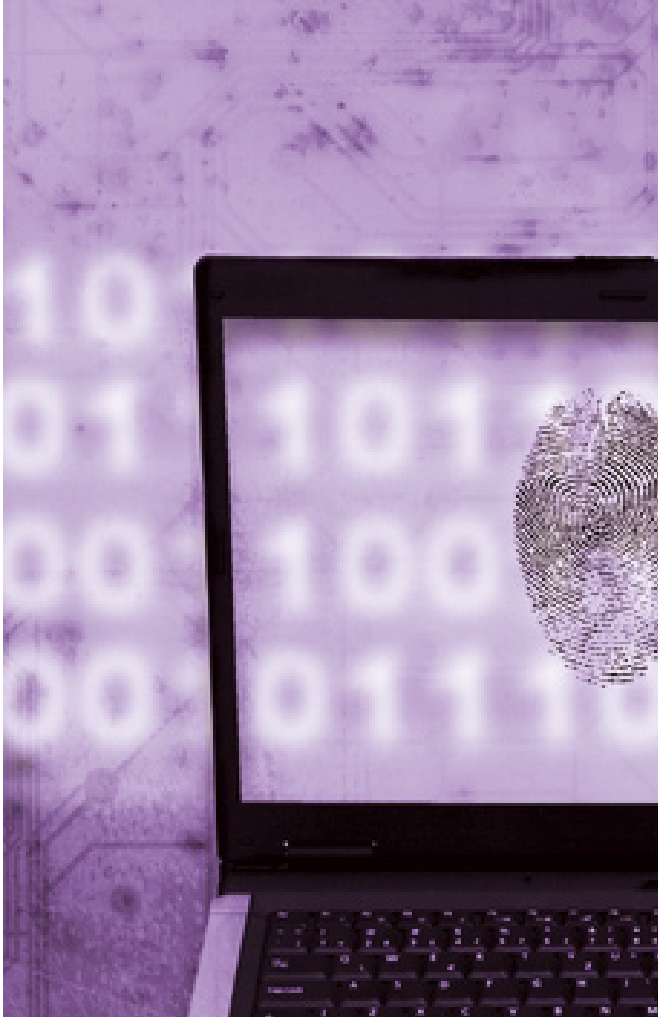
The defendant pleaded guilty to possession and making pornographic photographs of children from the Internet. He was fined and ordered to pay costs. The application for forfeiture for the hard disks upon which those images were stored was adjourned and heard on the 25 September 2002. The prosecution maintained that it was not possible to wipe the hard disks drives and return them to the defendant, because the material may still be stored on those disks, because the software available cannot guarantee that the indecent images will not still be on the disks. The court was satisfied that it is impossible to be one hundred percent sure that all indecent material has been deleted, even if one directs the computer to make deletions of such material. There is no obligation on the police, who have lawful possession of these disks, to carry out deletions of images; the defendant should be deprived of his rights in that property."

Forfeiture of Indecent Photographs of Children

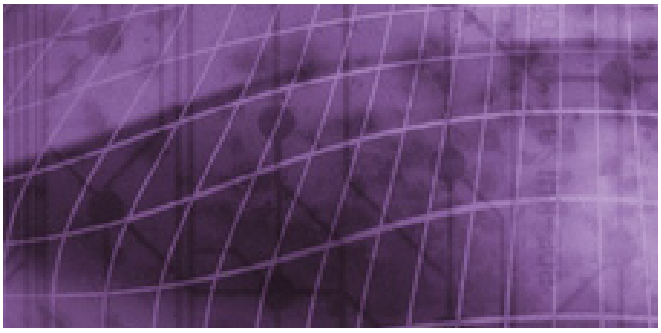
Section 39 & 40 and Schedule 11 & 12 of the Police and Justice Act 2006 give powers to the police without recourse to the court to give notice of forfeiture of -

(a) any indecent photograph or pseudo-photograph of a child;

(b) any property which it is not reasonably practicable to separate from any property within paragraph (a).



Forensic Matters



Forensic Matters

The reader should also refer to the appendix attached to this Guide – 'The Process'

See Appendix G

Whilst it is not possible to write a simple and complete forensic manual within these pages it is incumbent upon the working party to highlight good practice. The items mentioned below are regarded as good practice but it is clear they have not, for a variety of reasons including pressure of work and budgetary matters, been implemented in a number of forces across the country.

Peer Review

There have been a number of cases where the processes followed during a forensic investigation have been questioned successfully by defence. It is therefore important the quality of forensic examinations is kept at a high level despite the pressure of work that units operate under. It is unfortunate some personnel feel under pressure to produce quick results, sometimes at the expense of reliability and accuracy, even, it has been alleged, impartiality.

In order to identify processes that are questionable, or, for whatever reason the unreliability of evidence produced from a unit; it is strongly recommended each unit subject itself periodically to a peer review. This can be carried out at one level locally and continuously by analysts checking their colleagues' work on a regular basis. The main recommendation in this area from the working party is that independent reviews be carried out. This can be achieved either internal or external review.

Internal review can be completed by forces combining with a reciprocal arrangement to review each others' work. External review is more difficult, due to the material examined, but could be carried out by other law enforcement organisations or trusted partners involved in the field.

See also section on Quality of Process

Dual Tool Verification

It is accepted that many cases involve large amounts of evidence pointing to the guilt of the defendant. However, in some cases, the actual evidence recovered may be just a few files, a single file or a few bytes of data. In these cases it is **highly recommended** that the examination is repeated with a totally different software process and tool. All software has 'bugs' (minor programming anomalies) which can cause the erroneous reports of what appears to be fact, a date and time for instance. The repeat of the examination should conclude in the report of the same result, thus giving the one 'nugget of gold' more reliability and credibility.

Horizon Scanning/Internet Research

Computer and Digital Storage technology changes very quickly. In an effort to keep up to date as well as prepare for future developments it is **highly recommended** two steps can be taken at little cost:

A subscription to a monthly computer magazine such as PC PRO will bring with it a number of advantages. Changes in technology go to press early so the arrival of those changes can be planned for, this could also have the effect on the updating of hardware in particular, and good planning can save sizeable amounts of money by the avoidance of purchasing 'old' technology. Discussions in the press about the use of particular pieces of software, and the most popular software for particular tasks provide useful reference when that software in encountered on suspect machines. The Internet is also a useful source of information.

- The identification of hardware availability and its competitive price can assist in negotiations with retailers wishing to sell on at 'list' prices when purchasing upgrades or new kit.

The Internet is a vital tool for any computer crime unit. Used for software upgrades, answers to technical questions, software downloads, open source research, resolution of Internet Protocol addresses and research into paedophile material, it offers a vast resource at little or no cost. Time should be built in to Unit task lists to carry out such research. Broadband connections are the minimum acceptable connection for this type of work.

If the staff of the unit find it difficult to put aside time to conduct research an approach could be made to the Computer Science Faculty of a local university to see if a student was willing to conduct research on behalf of the unit for a small payment.

Asset and Job Database

If not already implemented, Units should equip themselves with an asset and job database. The asset part of which should record equipment kept within the unit. The job part should contain details of each job, all exhibits and continuity trails for all items. A fully functional relational database system can be built from software already provided within Microsoft Office.

Preview of Machines and Triage

Forensic software often provides a preview function which permits a 'safe' (with proviso) look at a disk.

Previous practice might have been to avoid previewing computers and mobile devices as a preview might miss some evidence that would otherwise be found on a full examination and risk the return of a computer in that state to a suspect.

However it is not uncommon now to witness seizures of multiple computers and mobile devices in domestic settings where there might be 10 or more digital devices recovered. With many units suffering large backlogs of forensic examinations, especially given that there is a consistent high proportion of work related to Paedophilia, a Triage solution would thus provide numerous benefits, especially when considering investigation priorities and resources. Where there are insufficient resources to cope with the volume of digital devices being presented for examination, a Triage tool in combination with assessment of the intelligence available in the case could be used to reduce the number of digital devices being given a full examination.

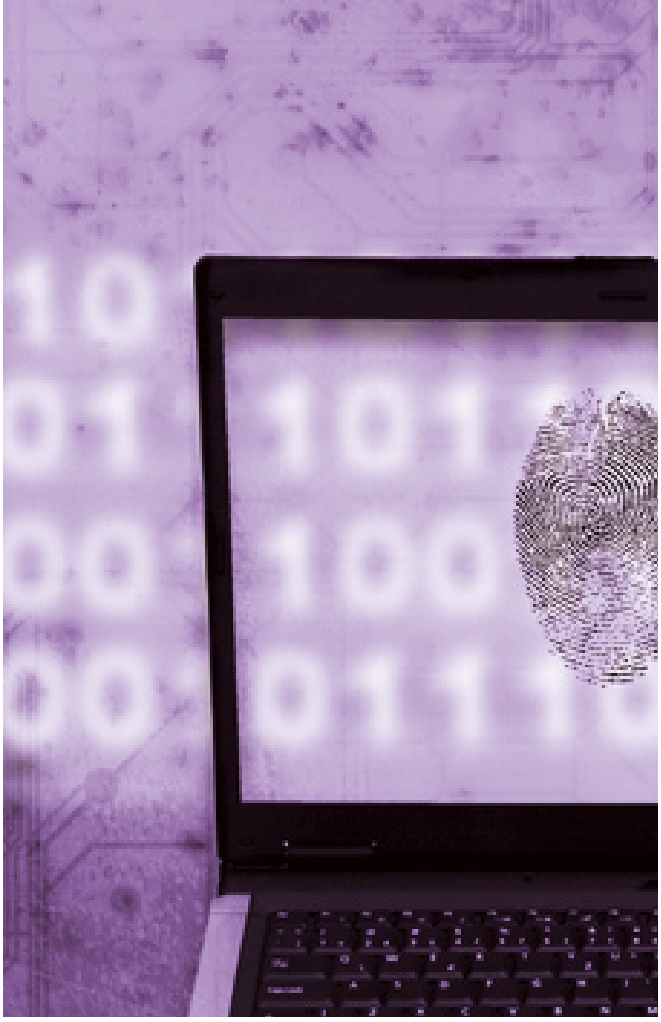
Triage could especially help to identify:

- Media likely to contain evidence
- Those investigations that require a more detailed and technical examination
- The investigations that could be subject of limited examination by qualified practitioners
- Material requiring urgent investigation
- Examinations suitable for out sourcing
- The extent of the assistance the unit will need to provide to an investigation

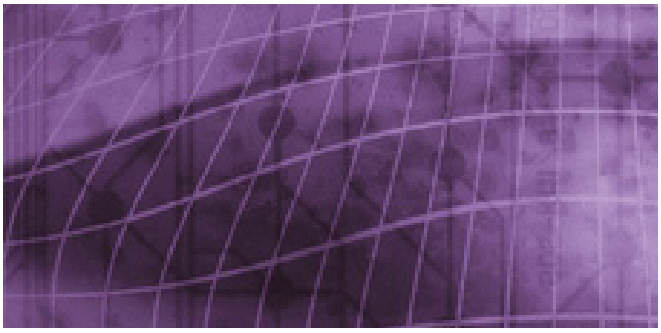
The use of Triage is currently under review by the National e-Crime Programme and they will be producing recommendations around the use of Triage as a process. Until then it is recommended that a Risk Assessment should be performed before a partial examination or preview is considered.

Note

There are various specialist forensic triage software solutions available including those provided by ADF Solutions, whose products are used by the FBI. Further details available at http://www.adfsolutions.com



Training



Training

The general principle of training in Hi-Tech investigation is somewhat dissimilar from usual police training. Due to the rapidly changing environment of technology there is a requirement for constant retaining and updating of skills. This training is often expensive and highly technical and as such raises a number of issues for authorising line managers.

Because of this and the highly technical nature of the topic, managers' often find themselves feeling uncertain about the veracity of the requests they are being asked to authorise. Due to a lack of understanding of the content of the training and it's true worth in the work place, the high expense seems excessive. This is particularly noticeable when those requests include aspects not usually seen in traditional training, such as travel overseas.

The aim of this section is to assist managers in making informed decisions about such requests and to offer a suggested model for core skills training and beyond.

National Occupational Standards (NOS) describe competent performance in terms of outcomes. Together with a defined assessment strategy, developed in parallel with the standards, they allow a clear assessment of competence against nationally agreed standards of performance, across a range of workplace circumstances for all roles. In this way, defining what has to be achieved, rather than what has to be done. They provide the necessary flexibility to meet the needs of the individual forces. Today, national occupational standards are viewed by modern managers as an indispensable tool for managing a highly skilled workforce.

ACPO has signed up to National Occupational Standards (developed by Skills for Justice) and in December 2006 the NOS for Countering e-Crime was introduced. The following 8 units refer to those standards that specifically relate to e-Crime investigation

Units for Countering e-Crime

CO1 Identify and secure electronic evidence sources
CO2 Seize and record electronic evidence sources
CO3 Capture and preserve electronic evidence
CO4 Investigate electronic evidence
CO5 Evaluate and report electronic evidence
CO6 Conduct internet investigations
CO7 Conduct network investigations
CO8 Conduct covert internal investigations

Full details of these units and other additional existing units that have been identified as relevant to e-Crime are available at www.skillsforjustice.com

The NPIA, E-Crime Training Unit has been mandated to take primary responsibility to provide an accredited modular E-Crime training programme for the police service. It was created to ensure police staff are equipped with the knowledge and skills to enable them to meet the challenges set by criminals who use technology in their criminal endeavours.

It is important that any training provided to the police service is progressive and NPIA has created a specific module for all new recruits to ensure they receive a level of training that will allow them to support the overall aim of the programme. Other modules are being created to ensure that the progression is sustainable throughout the service.

NPIA recognises the need to work in collaboration with other organisations to succeed in its objectives. There are many training organisations that provide valuable skills to the police service in its aim to combat E-crime at all levels. A number of the NPIA E-Crime Training courses are now available to those employed in similar roles within Industry. More information may be obtained from NPIA E-Crime Training Team on 01480 401986 or by e-mail on enquiries_ecrimetraining@npia.pnn.police.uk

www.npia.police.uk/hightechcrime

A number of training providers in the private and non profit making sector have training products that will enhance the skills of police staff. Some examples of these are:

- The NPIA, E-Crime Training Unit
- The Centre for Forensic Computing of Cranfield University at the Royal Military College of Science, Shrivenham (CFFC).
- First Forensic Forum (F3)
- Qinetiq
- Guidance Software
- AccessData
- Paraben
- 7Safe
- CISSP
- IRM Plc

Training (cont.)

Programme training means

- All staff will achieve the level of competency required for the designated post.
- A programme of continued and refreshed courses should be maintained for all staff.
- A research and development programme of new technology should be maintained and each staff member should be expected to familiarise themselves with it.

Training in this area cannot be achieved 'on the cheap', managers must ensure that they are fully aware of the aims and content of each course and the skills gained. Previous attendees can be a very useful source of information in the effort to identify the 'correct' course or courses for individuals.

Training can also take place 'on-the-job' with experienced members of staff mentoring and developing new recruits; this should only be of a type for non-technical tasks. Research into new methods, new software tools and updated hardware should be encouraged across the unit as this has been shown to be beneficial to the efficiency of Units. Time should be 'built-in' to allow for this to occur. Tasks which would yesterday take hours could be reduced to a few minutes today with a new piece of software, which may well be available on-line at little cost.

The following proposed training matrix is a guide based on a staff member with investigation experience, and knowledge of rules of evidence and disclosure. These are considered as prerequisites for this type of post, although where a high volume of cases are handled some functions such as basic imaging (forensically copying) can be undertaken by an individual with little or no investigative background, provided of course they understand the basic requirements of evidence handling and processing.

Where to do training

Some specialist training courses, such as those run by Guidance software, may only be available in the United States and there is no alternative but to travel. In addition it is sometimes cheaper to attend training in the USA as overall costs maybe cheaper, dependent upon the exchange rate at the time. Careful scrutiny should be made of each training request, particularly where travel overseas is required.

In most cases, similar specialist training is now available in the UK at comparable cost, so it is worth exploring alternative options. In cases of doubt managers should seek the advice of E-Crime Training Unit at NPIA, Wyboston. They have a wide range of knowledge in the training field and can advise on the availability of current courses, and accept requests for development of new training in this field.

What Courses and When

The first question faced by managers is 'what courses do I need to send my staff on to make them basically operational?'

For a member of staff fresh into this arena it is essential that they rapidly gain an understanding of the work area and the technology that supports it. This business imperative must however be balanced against the member of staff's ability to assimilate highly technical knowledge. The timing and sequence of training is therefore vitally important so that staff can gain the best value and understanding from the information being delivered. It is also vital so that when called to give evidence of their findings staff can support them based on a sound basic understanding of the technology.

Managers of units must plan ahead to ensure new staff learn the appropriate skills at the correct level to carry out their particular role. It is accepted this may cause a new recruit to a specialist unit receiving back-to-back training on a small number of courses prior to being capable of operating in the office. On-the-job training, encouragement and advice from peers, and personal research also form part of this 'basic' introduction to the field. All training should be focused on individual needs coupled with the needs of the unit. It may well be a new recruit with little or no experience in the field should attend the Core Skills Data Recovery and Analysis Course, so ensuring they have the requisite understanding required prior to attending more specialised or product training. It may also be only one analyst need attend a 'specialist' software course if that software is not to be widely used within the Unit. Planning of training courses should be made years in advance and places booked sooner, rather than later. It is important also the needs of the Unit as a whole, with a spread of skills, are recognised as a strategy for year-on-year development of the Unit and its staff, particularly when loss of staff to other duties or retirement is pre-warned.

Often it is tempting to send candidates to product-specific training such as Encase analysis training before a Core Skills Course so the staff member becomes rapidly usable within the office. However, without basic understanding of the hardware that Encase and other forensic tools look at, it is of little use as any evidence found cannot be supported by the knowledge of how it got there.

The following matrix is intended to assist managers in establishing a training path for their staff. It is not exhaustive but is indicative of the training that is needed.

It is **strongly recommended** Forces should consider providing a path to an academic or professional qualification in Forensic Computing or Information Security/Computer Crime for staff within their specialist investigative units. Performance development objectives must be set to take account of individual career progression plans. Such qualifications can be expensive, but very worthwhile and the provision of appropriate funding should be built into the process.

Note

It is vital to have a programme of continuing professional development for staff. This will include attendance at conferences, workshops and other relevant events as well as training courses.

TRAINING MATRIX

Digital Evidence Recovery Personnel			
1-6 months	**6-12 months**	**12-24 months**	**24-36 months**
Portable Appliance Testing		GNU/Linux Forensics	
Core Skills Data Recovery and Analysis	Introductory product training on departments SECONDARY* tool		Intermediate Linux Forensics
*Introductory product training on departments PRIMARY forensic tool	Applied NT Forensics		*Advanced product training on PRIMARY forensic Tool
		*Intermediate product training on departments PRIMARY forensic tool	*Training on task specific product tool
		Consideration **should** be given at this stage re Commencing a relevant MSc Programme	Intermediate product training on departments Secondary forensic tool
Regular attendance at conferences, workshops and other relevant events			

Network Investigators			
1-6 months	**6-12 months**	**12-24 months**	**24-36 months**
	Linux Hands On	Advanced Network Investigation	Covert Internet Investigation
Researching Identifying and Tracing the Electronic Suspect (RITES)	Consider introductory or intermediate product training on departments PRIMARY forensic tool for cross trained staff	Consider specific product training such as MCSE or CCNA to enhance investigators skills	Consider further specific product training such as MCSE or CCNA to enhance investigator skills
Open Source Intelligence Research	Core Skills Network Investigations	Network intrusion course such as those offered by private sector companies	
		Consideration **should** be given at this stage re Commencing a relevant MSc Programme	
Regular attendance at conferences, workshops and other relevant events			

Mobile Phone Examiners		
1-6 months	**6-12 months**	**12-24 months**
Core Skills in mobile phone forensics	Training in force SECONDARY* Specific hardware	
Product Training in force PRIMARY telephone examination tool		
Core Skills in Data Recovery Analysis.		Advanced Training in the PRIMARY examination tool
Regular attendance at conferences, workshops and other relevant events		

* It is important that no unit relies on a single forensic tool and the rationale behind dual tool verification is dealt with elsewhere in this document. The matrix details the time at which product specific training should be considered and is dependent on the needs of the unit. Forensic tools are not all expensive and some are not chargeable as products. It is therefore necessary for units to consider the training requirements in line with their forensic tool strategy. Training in these products should be considered when appropriate.

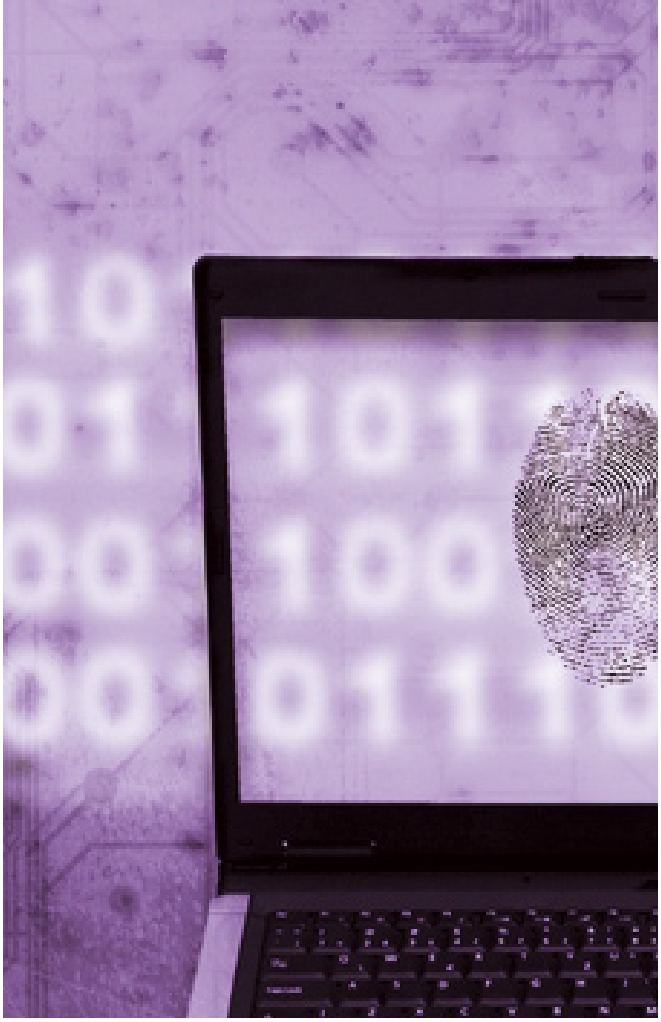
Each of the courses attended should provide details of the aims, objectives and learning outcomes. The above matrix relates to an individual and it should be possible to identify from the training received, details of skills acquired once courses are completed. A scan of all the matrices for a unit will identify the skills available across the available operatives. The timings are suggestions, but due to extraneous circumstances such as previous technical knowledge or requirements of the unit, could be flexible.

It is important the training courses selected are tailored to progress the staff member to the standard required (local levels should be set) as quickly as possible. Courses should be selected for that individual alone and focused upon the duties (s)he is to carry out. However, sight should also not be lost on developing a comprehensive skill set for the Unit as a whole. Further training can be undertaken to expand his/her role as necessary or to prepare him/her to take on additional functions.

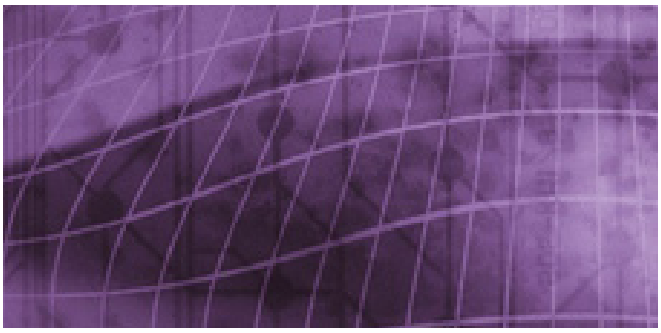
Digital forensics and open source intelligence pervades all types of criminality and technical training is available for other specialists in policing, such as child protection and economic crime investigators. By making them aware of this training it may be possible to reduce the burden placed on Hi-Tech / Computer crime units who deal with the vast majority of these issues. For example a properly trained child protection officer will be better able to interview suspects and interact with the CPS and Counsel as well as recognising potential sources of evidence.

Short details of some of the available courses are provided at **Appendix C**. It is essential that managers ensure that the aims and objectives of training courses meet the identified needs of staff.

At 36 + months it is strongly recommended Officers should be supported for a MSc or PG Certificate in either Cybercrime Investigation, Forensic Computing or Information Security/Computer Crime. Ideally, such a qualification should be sought from the outset, which in the 'long run' could save money. Managers should be aware that a failure to invest in staff has frequently been cited by staff as the main reason for leaving the Service or transferring away from this specialist arena.



APPENDIX A



APPENDIX A

The National e-Crime Strategy

The full strategy is available at the following link:

http://www.acpo.police.uk/policies.asp

The Internet has rapidly become the hub of personal and business activity and is significant in the majority of financial and intellectual transactions. Chatham House recently reported that, "with capacity to transmit several hundred billion dollars via the Internet infrastructure and other IT systems everyday, the cyber world has become a tempting and lucrative target for the modern criminal enterprise". The UK National e-Crime Strategy is designed to assist law enforcement in building a response to this very real challenge. Government support and robust, proactive partnerships with industry are the keys to success and that success will create its own momentum.

This Strategy is the first stage in developing a more consistent approach to e-Crime across UK police forces, increasing the skills and capacity for law enforcement officers to tackle such criminality and to mainstream e-Crime into everyday policing and law enforcement activities. By so doing we will enhance both industry and public confidence.

The Internet and networked computer systems are now fundamental to the way we live our lives. Few activities in the modern world are not touched by technology – from booking a concert ticket to withdrawing money from the bank. However the very convenience and accessibility of this technology has created many new opportunities for criminals.

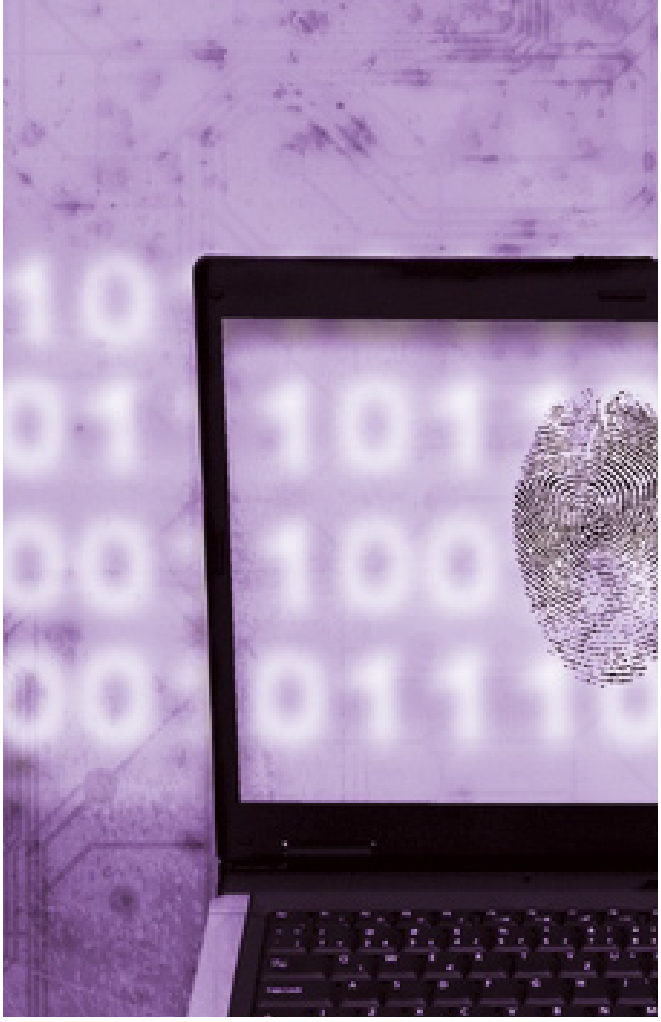
The first significant national police response to e-Crime in England, Wales and Northern Ireland was the creation of the National Hi-Tech Crime Unit (NHTCU) in 2001, along with 43 local Hi-Tech Crime Units at force level. The absorption of NHTCU into the Serious Organised Crime Agency (SOCA) in 2006 however created a gap at national level within the Police Service. This gap led to a reduced focus on mainstream e-Crime prevention issues, a lack of clear co-ordination of police e-Crime resources, and a reduced capability to investigate large-scale e-Crime that did not fall within the remit of SOCA.

In April 2008 the growing prominence of e-Crime led ACPO to create the ACPO e-Crime Portfolio under the leadership of T/Assistant Commissioner Janet Williams of the Metropolitan Police Service (MPS).

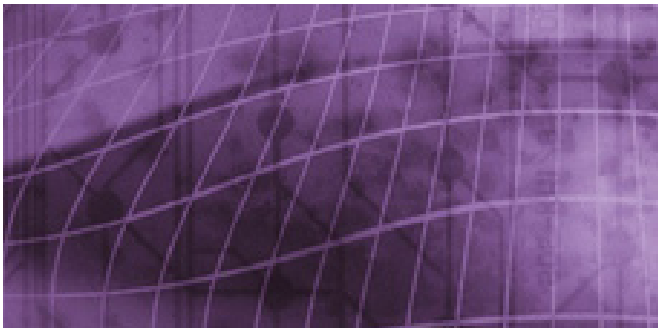
In September 2008 the Home Office announced it would provide £3.5m of funding over 3 years to establish a Police Central e-Crime Unit (PCeU), to be hosted by the MPS as Lead Force for e-Crime. The MPS merged its existing Computer Crime Unit into the PCeU, providing an additional £3.9m of funding over 3 years. The PCeU will work closely with the National Fraud Reporting Centre (NFRC) currently being established by the City of London Police, which it is proposed will also act as national reporting centre for e-Crime.

In January 2009 the National e-Crime Programme was created to co-ordinate the growing number of e-Crime initiatives being identified and implemented under the ACPO e-Crime Portfolio.

The National e-Crime Strategy sets out the strategic approach that the Police Service will take to e-Crime over the next 18 months; it has been produced in consultation with a broad range of stakeholders. The document replaces the *ACPO Strategy for the Investigation of Computer-Enabled Criminality and Digital Evidence* that was published under the aegis of the NHTCU in January 2005. It describes our strategic aims, the National e-Crime Programme that will put these into practice, the challenges that will be faced in implementing this strategy and the action the Police Service will take to achieve it in partnership with government, industry and academia. The Strategy will need to be revisited and updated regularly to reflect how the Internet is being used to facilitate crime and to encompass other strategies that are being produced by partner agencies. This will enable the Service to provide the best possible support for the victims of e-crime and present long term effective solutions.



APPENDIX B



APPENDIX B

Health Check for Units

A Initial Set-Up

Assessment of role required (Manager/supervisor)

- Job Description
- Pre-requisite knowledge/training
- Dual Role considerations

Clarity in relation to Terms of Reference

- Unit objectives
- Acceptance Criteria
- Priority setting

Clarity in relation to Budget

- Control & availability
- External resources
- Online purchasing

Staff levels (and role specification i.e. police / police staff)

- Job Descriptions
- Combination of roles
- Combination of jobs
- Workload
- Qualifications & Experience
- Policy re: Civilian/Police mix
  - Retention
  - Tenure
  - Flexibility
  - Discipline
  - Supervisor
  - Organisational Location (Fraud Squad, Scientific Support etc)
  - Recruitment/Selection
  - Availability of selection board 'expert'
  - Succession planning

Staff competencies: (A need to identify and list)

- National Occupational Standards compliance
- Testing of applicants
- Non technical training (particularly for civilian staff i.e. witness and interview training)
- Training Path for both forensics and investigations
  - Core and optional courses
  - How do managers assess training needs?
  - What courses are suitable for what tasks?
- Security vetting of staff
- Qualification route for staff
  - Training Pathways group
  - Product Specific Training
  - Vocational Training

Academic Recognition

- Minimum Standards – levels of operation
- National performance/management indicators?

Location

- Geography of unit
- Required areas/offices/labs
  - Reception area
  - Viewing/Interview rooms
  - Imaging & Examination Labs
  - Office resources
  - Exhibit storage

Security (physical and virtual)

- Physical on Lab
- Property system
- Continuity
- Resilience
- Network
- Audit of procedures

Equipment and storage (in particular lab standards and establishing minimum standards for equipment and to cover both analysts and investigators)

- Network
- Digital Storage
- Specification of Examination/Imaging/Viewing kit
- Digital Cameras
- Peripherals
- Contract Lease

- Refresh rates
- On-line purchasing
- Access to suppliers who can deliver at very short notice
- Processes for non-contamination
- The need for a sterile research machine
- Back-up equipment

B Management Arrangements.

Investigation set up – Forensic and Network (It may be worth checking out the CTOSE model for some ideas

Line management (and awareness training for those people)

- NPIA High Tech Crime Managers Workshop
- Open Door Shrivenham
- VIP days Shrivenham

Systems employed to manage high volume of requests and to prioritise (including triage and establishing local capability)

- Imaging as preventative tool
- On Site
- Intelligence only previews
- Prioritisation
- Acceptance Criteria

Collection and dissemination of management information

- Measure in GBs, Jobs and time
- Convictions as direct result?
- Result notification (also impacts on retention)

Communication

- Sharing of information between forces and agencies
- Regional/national online discussions
- ACPO Crime e-Crime/Computer Crime Unit

Outsourcing work – guidelines and costs

- Like-for-like quotes
- Grading of jobs for choice of examiner
- Fixed price jobs
- Selection criteria for outsourcing companies
- Identification & Use of experts
- Time spans for running cases – notify Court
- Return to job after defence expert report or statement
- Pick List for specification
- Liaison with OIC

Disaster recovery (business continuity)

- Backups
- On/off site storage
- Storage systems & preventative measures

Health and Safety (staff welfare for example continual viewing of child porn images)

- Mandatory counselling with feedback
- Internet controls on paedophile material
- Quality of screens
- Eyesight testing
- Work space
- Office furniture
- Tools
- Physical Examination training
- Physical handling of machines

Intelligence acquisition and dissemination

- Criteria
- On-site kit
- Later use as evidence?

Disclosure generally

- Release of images to defence experts
- 'Unlawful' material (CPS agreement)
- Arrangements for defence viewing

Presentation of evidence (in particular control and release of exhibits)

- Report/Statement content (factual only?)

Increasing Productivity – Reducing Costs (adopting best value principles and practice)

- Production Line forensics – pick list
- Additional/better equipment
- Multi-tasking of examiners

APPENDIX B (cont.)

Reviews of cases (including peer and supervisor review of evidence and statements)

- Identification of peer review resources
- Setting of percentage
- Selection of cases for review

Weeding and disposal policy

- Complying with Rehabilitation of Offenders Act,
- Criminal Evidence and Procedure Act, Data Protection Act.
- Methods of disposal of equipment and destruction of digital material
- Retention of images and 'paperwork' relating to those images
- Should this be linked to Crime Reports and Intelligence acquisition?

C Investigation.

Terms of Reference

- Liaison with SIO
- Briefing

Parameters (international issues and policies)

- Initial risk Assessment
- Impact for and against
- Acceptance criteria
- Costs
- Potential pitfalls
- Impact on victim
- Impact on suspect or suspect business

Strategies and Tactics

- Uneven flow of potential jobs
- Acceptance criteria
- Prioritisation
- Flexibility of workforce size (Op.Ore)
- Outsourcing to reduce backlogs
- RIPA issues
- Broad investigative templates or standard operating procedures (for example all paedophile cases must be examined for Trojans)

Quality of processes

- Quality assurance
- Supervision
- Pick-lists
- Policy on job acceptance and priority

Exhibit Handling

- Training
- Security
- Continuity within unit

D General Issues.

Case conferences/ meetings – processes

- Policy book/minutes of meetings
- Sharing information and progress reports

Sources of advice/ reference

- Resources
- Magazines/Journals
- Access to academics/experts

Constraints and considerations

- Budgets
- Expertise

Use of seized equipment

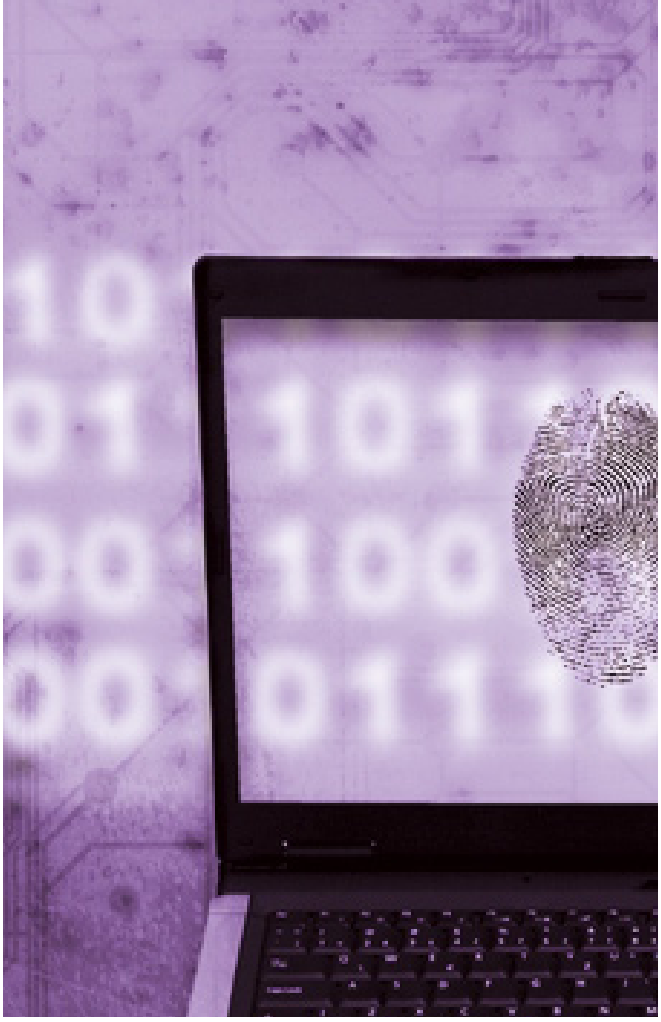
- Use for low-level jobs in unit
- Wording of forfeiture applications
- Wording of forfeiture orders

Liaison with other Agencies

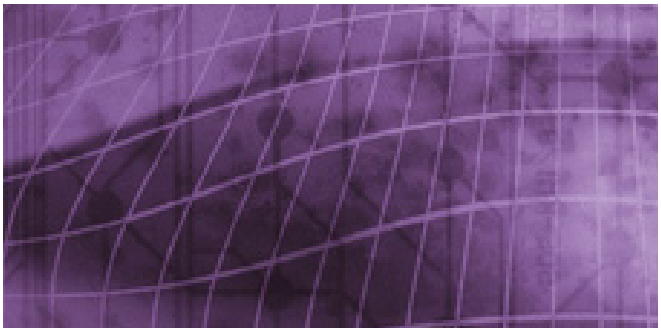
- Exchange of information/expertise/specialist equipment

SOCA e-Crime Unit and what it can offer

SPOCs – their role and level of knowledge



APPENDIX C



APPENDIX C

Details of Training Courses

This is a list of some of the courses that are available and may be considered by managers for their staff and themselves. The list is not exhaustive and is provided to assist managers.

> **Note**
>
> The training courses offered by NPIA are mapped to the National Occupational Standards for Countering e-Crime as signed up to by ACPO in December 2006.

Forensic Examination

Portable Appliance Testing – Various local authorised providers

This is required to satisfy basic Health and Safety Regulations. The course lasting typically for 1 day teaches operative how to test small electronic equipment powered by mains electricity, to ensure its electrical safety. As units regularly receive such appliances in the form of personal computers it is essential that officers are able to accurately establish the safety of such items prior to connection to a mains power supply.

Core Skills in Data Recovery and Analysis – NPIA Wyboston

This is a Law Enforcement tailored course designed to provide candidates with an understanding of PC architecture and operating systems, along with the skills to identify, examine and present evidence found on commonly encountered computers. This course provides the skills and understanding required before embarking on product based training.

Applied NT Forensics – NPIA Wyboston

With the release of Microsoft VISTA and the predominance of NT-based computers running NTFS file systems this course provides the knowledge and skills required for forensic examiners to recover evidence more effectively and provide a much better understanding of what automated forensic tools are doing.

GNU/Linux Forensics – NPIA Wyboston

Provides forensic IT Examiners with the knowledge and core skills necessary to use tools based on the GNU/Linux operating system to undertake forensic analysis of digital evidence.

Forensic Computing Foundation Course – CFFC Shrivenham

The course covers the fundamentals of evidence recovery from mainly PC based computers and the successful presentation of that evidence before a Court of Law. Written and delivered by practitioners for practitioners, this course provides at postgraduate level where appropriate, and with particular reference to, the special problems encountered in a Law Enforcement environment. The course covers sound understanding of the component parts of a computer, start up procedures, detailed knowledge of Disk Geometry, detailed instruction in Data Recovery including Original Integrity, Preparation of Evidence for Court and importantly the need to identify the point at which an approach to a recognised expert in a particular computer field should be made.

Forensic Computing Internet Course – CFFC Shrivenham

The aim of the course is to equip Law Enforcement Officers with sufficient knowledge to enable them to examine computers, which have been used to access the Internet, in a forensically sound manner. It also provides an overview of the most commonly used software available to ordinary Internet users, and to investigators. Practical demonstrations and workshops also show how to identify data left behind by such applications, its recovery and analysis for evidential purposes.

Forensic Computing Network Course – CFFC Shrivenham

The aim of the course is to equip Law Enforcement Officers with the knowledge, understanding and skills for the recovery of evidence from computers, connected to a formal network. The course also covers the issues involved in running site-world networks, building Local Area Networks, Client Server Architecture and an outline of the legal issues involved in seizing networks and isolating evidence.

Forensic Computing - Advanced Forensics – CFFC Shrivenham

The aim of this course is to develop knowledge and understanding of Advanced Forensic Computing techniques and to acquire the skills to apply these successfully. Examining, in a practical setting, a number of areas of current relevance, this course covers amongst other topics, Structure and Analysis of Optical Media Disk Formats, the Use and Implementation of Virtual Machines and the Analysis of Web Site Hosting.

Forensic Computing – Legal Issues & Courtroom Skills – CFFC Shrivenham

The aim of this course is to produce a sound understanding of the practical legal aspects involved in providing evidence in court. Along with the Computer Misuse, Data Protection and the Theft Acts this course also covers EU Directives. One full day is under professional legal instruction on the preparation and giving of evidence.

Forensic Computing Using Linux – CFFC Shrivenham

The aim of this course is to develop a practical working knowledge and understanding of Linux and Open-source tools as a platform for performing computer forensic examinations. The content amongst other issues are an overview of Linux and UNIX Platforms, Managing Forensic Data, Open Source Analysis Tools and Their Use and Building a Forensically Sound Workflow.

Forensic Computing – Corporate Security – CFFC Shrivenham

The aim of this course is to equip the student with the skills to establish and maintain the security of corporate information systems. It covers the principle elements of corporate information and infrastructures, the roles of technical solutions and elements of cryptography and security.

Document Examination Course – CFFC Shrivenham

During this course students will be led through the process of identifying the internal file structures of a Microsoft Word document file, the breaking down of those structures into their component parts and the reconstruction of those specific parts into a meaningful stream of data. Identification of the various items lodged within the streams including a number of dates and times not available from any other method, text-editing history, machine on which created, user identification for creation and edits, last user, template used and the like.

Forensic Investigation – 7Safe

A practical computer forensics training course, gain an understanding of static computer forensics analysis by learning about forensic principles, evidence continuity and methodology to employ when conducting a forensic investigation.

Forensic Artefacts – 7Safe

Extends the knowledge beyond conventional static computer forensics analysis by learning about and applying the forensic investigation methodology, from the principles surrounding the collection of evidence and preliminary case considerations to investigating the evidence left behind by malicious activity and the collection of volatile data

Product Based Training

Forensic units will be required to use tools developed by providers and undertake training on these products. It is important for managers to ask questions about the training element when considering the purchase of software, which of course can be very expensive. The following questions may be of assistance:

- If I buy this product, will my staff be able to obtain training at a reasonable cost?
- If I buy this product how long is the software license valid for?
- How many courses will they have to attend to be a proficient user of the software?
- Is this training available in the UK and targeted for a UK audience?
- Are students assessed so that I know that I know my staff can use the software effectively?
- Will I be told if my member of staff passed or failed a course?

Some examples of product based training are:

Encase Basic/Intermediate/Advanced – Guidance Software

Encase is a forensic tool used by many police forces in the UK. The company behind the product, Guidance Software has a training facility in Slough to cater for the UK audience. These courses are also held in the USA, where Guidance Software is based.

AccessData Forensic Toolkit – AccessData Corporation

AccessData FTK is another tool used by many UK police forces. AccessData provide training for their product and do not have a UK based training facility. AccessData arrange mixed Law enforcement/private sector training in the UK at various times during the year. These courses are also held in the USA, where AccessData is based.

X Ways Forensics

This is another main forensic tool and the company provide training in the use of the software. They do not have a dedicated training facility in the UK but run courses several times a year at UK venues. Courses are also run at venues around Europe and the rest of the world.

APPENDIX C (cont.)

Paraben PDA Forensics – Paraben Corporation

This course provides basic skills to conduct forensic examinations of personal digital assistants (PDA). This course is also held in the USA, where the Paraben Corporation is based.

Some of the forensic software companies have been offering training passports which allow unlimited training for one year which provides good value for money.

Network Investigation

Researching Identifying and Tracing the Electronic Suspect (RITES) – NPIA Wyboston

This course provides the knowledge and skills necessary to access and interpret open source information on the internet as well as how to protect their integrity and the legal implications of their actions. This course does not cater for online undercover investigations.

Core Skills Network Investigation – NPIA Wyboston

This course is designed to provide students with an introduction to computers, computer operating systems, computer crimes and computer investigative resources, together with an insight into Internet services, criminal use of the Internet and investigative techniques.

Covert Internet Investigation – NPIA Wyboston

This course is designed to provide students with the knowledge and skills necessary to conduct covert online investigations, ensuring legal and procedural compliance.

Linux Hands On – Qinetiq Malvern

A Law Enforcement course teaching from basic through to intermediate usage of Linux operating systems. The use of this course is often misunderstood; however as approximately 50% of the network infrastructure of the Internet operates on UNIX based systems a basic understanding is essential to Network Investigators and desirable for Data Recovery Investigators.

Open Source Intelligence Research – Focus Training

Specifically designed open source course developed to provide advice on advanced information collection via the Internet.

Advanced Network Investigation – Qinetiq Malvern

A Law Enforcement course focused on advanced Network Intrusion techniques ranging from Wireless hacking through to Web Site access. Prerequisite for this course are Linux and Core Skills Network Investigation training as the content is very technical.

Ethical Hacking Training – 7Safe

Delivered as two separate courses, the first investigates the hacking mindset, examining and practically applying the tools and techniques that hackers use. The second involves using the frameworks & tools used by professional penetration testers to audit & compromise system security, assess weaknesses in web applications and hijack sessions to steal users' online identities.

Wireless Security Training – 7Safe

This wireless security training course gives delegates a practical understanding of, setting up different types of 802.11i networks, how hackers bypass wireless security and implementing wireless security measures.

Mobile Phone Examinations

Core Skills in Mobile Phone Forensics – NPIA Wyboston

This course is intended for new or existing mobile phone examiners providing exposure to and guidance on the use of appropriate forensic tools ensuring evidence is acquired in a forensically sound manner. It will also equip them with an understanding of how GSM/3G networks operate and relevant legislation in this area

Intermediate Mobile Phone Forensics

This course provides experienced examiners with exposure to and guidance on, enhanced data recovery skills from mobile phones and an awareness of upcoming technologies, relevant legislation and best working practice.

Some examples of product based training are:

PhoneBase – Trew MTE offer a range of continuous professional development certificate and accredited courses.

.XRY – Control-F is MicroSystemation's authorised training provider in the UK and Ireland, the product training is held at the Wyboston site of NPIA. It is intended to teach new or existing mobile phone examiners how to use the full potential of the .XRY system.

Paraben – offer three levels of hand held training packages that include software and hardware to handle evidence from cell phones, PDA's, hybrids, and GPS devices.

What next?

Following a relevant profile of some of the above courses could take up to two years, therefore the tenure of officers must be carefully considered before appointment, to achieve best value for the considerable outlay involved.

In addition to those courses listed it is desirable to cross train against other forms of analysis tools. The need for this is best highlighted within the Forensic field, where it can be readily demonstrated the Law Enforcement tool of choice, Encase, can produce different results to that provided by similar products such as Access Data's Forensic Toolkit. Dual Tool verification, particularly of important pieces of evidence, is good practice. In many cases, for single pieces of evidence, a low/no-cost method is available. Such tools are used as a matter of course on some courses covering more general examination methods.

As a member of staff develops specialist skills and experience, cross training becomes more important as it allows them to properly evaluate and challenge their own results. This is of substantial benefit to a unit as it reinforces the staff members' independence from mainstream investigation by demonstrating their willingness to verify their own results. Peer review and practitioner networking also plays an important part in the process of evaluation and validation as well as adding to the individuals' knowledge by using experience gained by others. The field of Forensic Computing is a very close one with an ethos of helping others.

In addition it is important to consider within an individual's training plan what roles in addition to their core function, staff members will be required to undertake. If it is envisaged that undercover type work will be conducted via the Internet, such as test purchases or interaction via online chat services further specialist training in that field will be required to meet ACPO required standards for Covert Internet Investigation.

Advanced Training and Beyond

Advanced training usually falls within two choices and should be considered on a case-by-case basis. Many members of staff wish to advance themselves by taking an external Masters degree in Forensic Computing or Information Security. This will cause them a great deal of additional work in their own time, but there are benefits to the organisation and wider Law Enforcement as a whole.

Such courses offer a formal academic qualification, which will add and develop knowledge as well as enhancing the staff members' credibility in Court. There is also merit in specialist training in specific areas. Both methods benefit wider Law Enforcement by providing specialists in specific fields who can also pass on knowledge to others.

What about the Manager?

We have looked in some detail at the training of practitioners in these areas of work but what about training for managers, well there is something for you as well.

Line Managers Workshop – NPIA Wyboston

This is a 3 day workshop designed specifically for line managers of Hi-Tech/Computer Crime Units and deals with issues such as resource implications, staff welfare, equipment and training.

Hacking Insight for Managers - 7Safe

An introduction to the hacking mindset, examining the tools and techniques that hackers use. The course illustrates different ways that hackers operate, how they infiltrate organisations and the subsequent damage that can follow.

Training for other police staff

Examples of this type of training are:

Hi-Tech Crime Search and Seizure – NPIA Wyboston

This short course is designed to provide an officer with the knowledge and skills to conduct effective searches at crime scenes where electronic evidence may be present. These include a domestic environment, a small business with RAID servers and a wireless network situation.

More information on courses offered by NPIA at Wyboston may be found at:

www.npia.police.uk/hightechcrime

When Does Training Stop

Due to the ever-changing pace of technology development continuous professional development is required throughout a Hi-Tech/Computer Crime practitioner's career. Whilst the fundamental basics underlying technology remain the same the hardware and software change on a daily basis. Potentially every new piece of software requires update training to enable effective examination and the gathering of evidence. In reality the large portion of this updating is done 'on the job' as technical issues and developments occur. However major revisions often do require more formal training.

APPENDIX C (cont.)

Further Advice

Further advice on training issues for the police is available via NPIA National E-Crime Training, Wyboston (01480 401986)

enquiries_hightechcrime@npia.pnn.police.uk

www.npia.police.uk/hightechcrime

Note

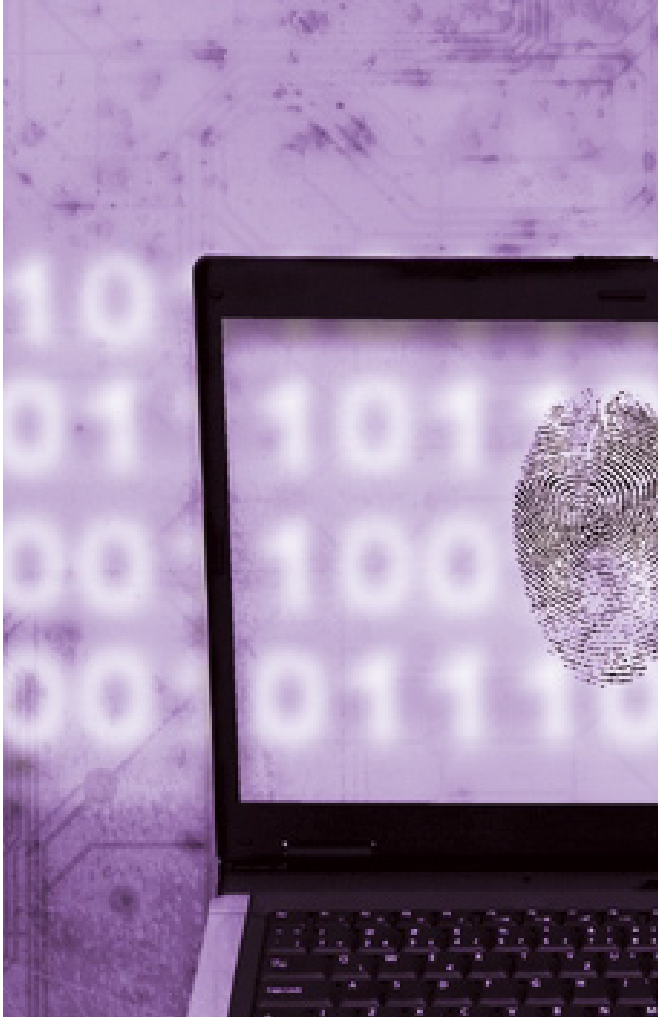
Canterbury Christchurch University in collaboration with NPIA offers an MSc in Cybercrime Forensics. The specialist training courses delivered at NPIA, Wyboston count towards the credit modules of the MSc. This Masters' programme aims to equip students with the skill sets to assist in the investigation of crime which involves the use of IT equipment and acquaint them with the legal, ethical and professional considerations which must be take into account. A first degree is not a pre-requisite for this course.

Note

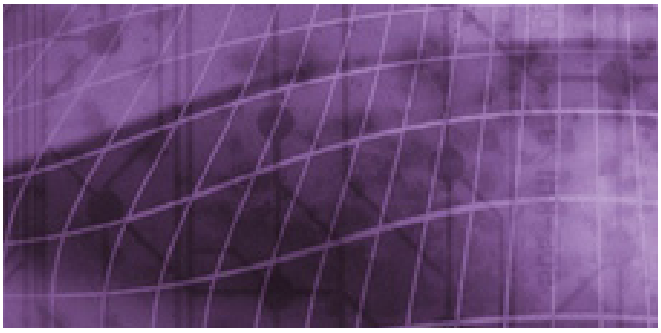
The Centre for Forensic Computing of Cranfield University at the Royal Military College of Science, Shrivenham (CFFC) offers an MSc Course made up of three one year part-time modules of PG Cert, PG Dip, and MSc in Forensic Computing. This is designed primarily for Law Enforcement Officers and does not necessarily require a previous degree for entry.

Note

University College Dublin, in collaboration with the Europol working group on the Harmonisation of Cybercrime Training, provides a Masters degree in Forensic Computing and Cybercrime Investigation. Entry requirements are a first degree or a significant amount of experience within this arena.



APPENDIX D



APPENDIX D

Presentation of Evidence

Documents and Exhibits in Forensic Computing

1. Introduction

Forensic Computing requires a high standard of documentation and exhibit handling. The examiner is involved in a specialised and responsible field which requires considerable knowledge and impartiality. The following guidelines discuss the writing of notes, statements and reports together with the production of exhibits in forensic computing cases. They are incomplete but are part of a larger attempt at producing a national standard.

2. Notes

2.1 Audience and purpose

Notes are made for different reasons and for different people to read. The following are examples

2.1.1 Notes are made for the examiner themselves

Notes are made to record the examiner's own actions in such a way that they can review and recall them. This may be useful when writing statements or reports, for refreshing memory when giving evidence and when talking to other interested parties about the technical details of the case

2.1.2 Notes are made for colleagues

Notes are made to record the examiner's actions so that colleagues can review them. They might do this to establish details of an examination they did not undertake when answering questions from other experts or lawyers. Managers may be required to examine notes in a supervisory capacity. Another examiner may be required to continue an examination in the absence of the original examiner.

2.1.3 Notes are made for independent experts

Notes are made to record the examiner's actions so that a defence expert can review them. Reasons for doing this include: the recreation of steps in the examination in accordance with ACPO guideline; to understand why the examiner reached certain conclusions; to identify errors that they may have made and to establish what they did or omitted to do during the examination or to assist in supporting their evidence.

2.2 Structure of notes

Notes should be kept on an individual case or examination basis. Each case or examination should have its own set of notes. Notes relating to a particular case should not be spread over a number of different notebooks containing notes relating to other cases.

Each page should contain the case name and reference number and the name of the person making the notes together with the dated signature of the person making them.

Each note should include the date and time that it was made.

Notes may be kept electronically. There are significant advantages to this in terms of readability and the ease at which diagrams, tables and pictures can be pasted into the notes. Electronic notes should be printed and signed after each logical break.

2.3 Dos and Don'ts for making notes

Do …

- refer to the existence of notes in any associated witness statement or report.
- disclose the existence of the notes as unused material rather than produce them as an exhibit.
- make notes at the time or immediately after any examination or part of an examination.
- include reasons for any conclusions reached, exhibits produced, damage noted, examiners intentions and reasons for actions.
- include relevant photographs (e.g. of examined equipment).
- make notes sufficiently legible for all likely parties to read and understand.
- include a high level of technical and procedural detail.
- include tables, diagrams screenshots and appendixes.

Don't …

- use acronyms or abbreviations that others will not understand.

3. Witness Statements

3.1 Audience and purpose

Witness Statements are made for different reasons and for different people to read. The following are examples

3.1.1 Statements are made for the court

A witness statement provides the basis for the original evidence that an examiner may give to a court. Under certain circumstances all or part of the statement may be read to the court in the absence of the examiner themselves.

3.1.2 Statements are made for lawyers, barristers and advocates.

A witness statement provides sufficient information for prosecution (for example CPS Prosecutors) and defence lawyers to understand the nature and context of an examiner's findings in order to establish how they will assist with case strategy and the legal points to prove. The statement must therefore be readable for a non-technical person. It allows advocates on both sides to formulate a strategy for arguing the case and for the examiner's examination or cross examination.

3.1.3 Statements are made for the investigating officers

A witness statement provides sufficient information about an examiner's findings to assist with the investigation. It may be used to determine case strategy or tactics and may be extensively referred to during case conferences, meetings and interviews with suspects or witnesses.

3.1.4 Statements are made for independent experts

A witness statement provides independent experts working for the prosecution or defence with a summary of the examiner's technical findings.

3.1.5 Statements are made for the examiner themselves and their colleagues

A witness statement provides the examiner with a summery of their evidence for fast future recall and for colleagues to answer simple questions in the absence of the examiner.

3.2 Structure of witness statements

Witness statements for forensic examiners should be written with a consistent layout. The following headings as subheadings are suggested.

Introduction

Examiner

The examiner should introduce themselves, their rank and position.

They should include a personal profile or personal portfolio of their qualifications/skills/experience and include this either within the statement or as an appendix at the author's preference

Instructions

When and who submitted the examination request and what work was requested
E.g. On xx PC xx submitted a request for examination …

Continuity

The continuity of property on arrival should be dealt with.
E.g. On xx the following items were delivered by PC xx to …
If necessary statements from other people may be required to prove this.

Compliance

A statement of compliance with ACPO guidelines.
indicate if mistakes have been made together with reasons and implications.
reference to existence of examiner's notes.

Item 1

Method

A short summary of what was done with what tools. e.g. "imaged using …"

Results

What items were found Include tables, diagrams etc

Technical Explanations

Technical Details of matters raised by results
E.g. explanation of newsgroups. refer to glossary if appropriate

Context and discussion

The context of the findings and technical points in relation to what was being asked of the examiner.

A discussion of any points which may have multiple explanations

Item 2

Method etc

As above continuing for each item or group of items submitted

Try and use logical groups. Examples might be to group all hard disks in one computer in a section or to group a box of floppy disks in one section.

Summary

A summary of the findings. Many readers will jump straight to this point in a long statement.

Conclusions

Not always required but in some cases the examiner may need to make conclusions. These should always be strongly reinforced by factual argument in the main body of the statement and may cause the court to attribute expert status on the examiner

Appendixes

Personal Profile/Portfolio if not in main body of statement

Include experience and qualifications

List of exhibits

Include the ID reference, description, reference of exhibit they originated from

Selected Glossary

References

3.3 Dos and Don'ts for making statements

Do …

- use appropriate headings and sub-headings.
- number each heading and sub heading using a decimal system
- keep technical explanations simple
- include appendixes where appropriate. These should be included in the statement page count.
- include a personal profile/portfolio.
- include a glossary of specified terms that you understand.
- provide a summary of findings and any conclusions at the end of the statement.
- include references to the sources of any external information used (e.g. manuals, online technical fact sheets).
- give clear explanations where and why evidence or data has been extracted or altered for presentation purposes (e.g. pictures reduced to thumbnails).

Don't …

- include anything in the statement or glossary that is not understood sufficiently to explain under cross examination.
- use abbreviations or initials without using the term in full on their first occurrence. For example, "… I found in RAM (Random Access Memory) the following …".
- refer to pictures as 'images' as this causes confusion with forensic images. Use 'pictures' or 'photographs' instead.

4. Expert Reports

4.1 Audience and purpose

In general terms an expert report is likely to contain a higher level of detail than a witness statement. It should be considered as a response to another expert's report dealing with technical matters raised by that expert. Courts usually expect to see reports from expert witnesses.

Reports therefore share similar audiences to statements but are less likely to be as easily understood. Similarly, in most cases, reports share the same purposes as statements but reports made for other experts have a slightly different focus.

4.1.1 Reports are made for independent experts

Reports are written for independent experts to read and understand the technical details of an examination. They may be written because the technical detail is so central to an examination that it needs to be explained in a highly complex fashion. They may be written in response to a technical report by an independent expert either agreeing with or opposing the views in that report.

4.2 Structure of reports

In general reports should follow the same structure as witness statements. Reports in civil cases must conform to the Civil Procedure Rules 1988.

4.3 Dos and Don'ts for making reports

Do …

- attach a report to a short witness statement as an appendix or even an exhibit.
- put a sufficient level of technical detail in the report to argue or establish any facts that are in dispute.
- agree with other experts where appropriate.

Don't …

- produce reports unnecessarily. In many cases a witness statement will suffice.
- assume that just because a report is produced as an exhibit the jury will see it. They won't.

5. Exhibits

5.1 Audience and purpose

Exhibits are real evidence. This is different to original evidence which comes from the testimony of witnesses. Examples of real evidence in computer cases are the computers themselves, printouts of files present on computer media, tables of file attributes – file names, dates and times. Exhibits should be produced and referenced in a statement or report. The primary reason for producing exhibits is for the court but they additionally serve a useful purpose for other parties.

5.1.1 Exhibits are produced for the court

An exhibit is the real evidence that will be considered by the court. For example in a crown court the jury may be allowed to examine printed file listings. Exhibits such as diagrams made by the examiner, which by their nature reflect the work of the examiner, may be shown to the court if it is considered that they act as useful tools for the jury. It is however vital to understand that the real evidence is just that alone and cannot contain comments or additions representing the explanations by or opinion of the examiner or anyone else. These explanations will have to come from oral evidence. Items containing such amendments should not be shown to a jury.

5.1.2 Exhibits are useful for lawyers, barristers and advocates.

Exhibits are useful both to assist lawyers in understanding the evidence and to assist advocates in understanding and explaining facts to the court.

5.1.3 Exhibits are useful for the investigating officers

Exhibits may assist the investigating officers both to understand important technical points and to assist them during an interview.

5.2 Exhibit references

Exhibit references serve the purpose of uniquely referencing an item (exhibit) referred to in a statement.

There are numerous local methods of referencing exhibits. In general complex systems should be avoided in preference to simply understood references together with a table of exhibits added as an appendix to a statement or report (see 3.2 above). In this way an interested party can quickly see what an exhibit is, and where it came from.

5.3 Dos and Don'ts for exhibits

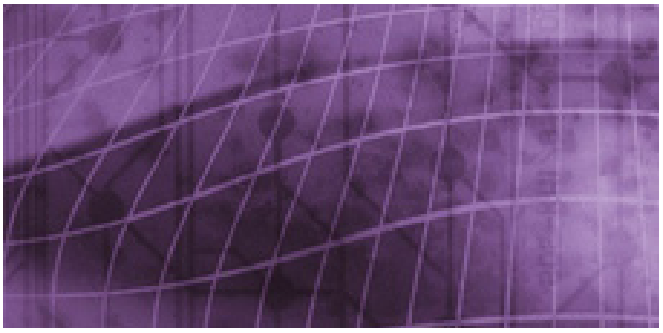
Do …

- reference the exhibit in brackets after it is mentioned in a statement or report. For example "I made an image (ABC/1) of the first hard drive present in the computer…".
- remember what is being exhibited. Is it data or hardware.
- produce tables of file attributes for all computer files referred to or produced as an exhibit.

Don't …

- use over complex exhibit references.
- add comments or explanations to exhibits.
- make unnecessary copies of unlawful images.

APPENDIX E



APPENDIX E

Details of some relevant Case Law

The following is a list of cases relevant to investigations of computer crime and a brief explanation as to the issues they cover. Full details of each of these cases can be found on the Lawtel web-site or National Police Legal Database accessed via the Intranet.

Human Rights:

PERRY v The UK (2003)

Although this case related to covert videoing techniques (where no authorities had been obtained) it deals with the issue of interference with private life in a public place. This case is one to be considered when dealing with cases involving the Internet as at present there is no clear guidance as to which areas of the Internet are public and which are to be considered as private.

R v PERRIN 2002

A conviction under S 2(1) Obscene Publications Act 1959 does not violate the defendant's right to freedom of expression. Apart from the general right to freedom of expression there was no public interest to be served permitting a business for profit to supply material that most people would regard as pornographic or obscene. (Article 10)

R v KHAN (Sultan) 2000

Right to respect for private life – authorities must act within the legislation (Article 8)

R v SMETHURST 2001

Prosecutions under S1 Protection of Children Act 1978 are in place to protect the morals and in particular, for the protection of children being exploited. Such offences do not contravene Article 8 or Article 10 of the convention. (Article 8 and 10)

Computer/Internet Investigations:

R –v- Neil John HARRISON (2007)

This case relates to "pop up" illegal images being automatically stored on the suspect's hard drive as a result of accessing a legal pornographic website. In this case as it was proved the suspect had been aware that by visiting legal sites it was likely "pop ups" of illegal images would occur and they would be stored to his hard drive he was found guilty of possessing illegal images.

R-v-M & 4 ORS (2007)

Compact discs or computer hard drives holding electronic data were capable of being articles within the meaning of the Terrorism Act 2000 S57.

R-v- Ian Anthony JONES (2007)

The police were not guilty of entrapment with regards to an attempt to commit offences under the Sexual Offences Act 2003 s8 where they posed as a 12 year old girl to gather evidence against the offender, as the police had not incited or instigated the crime.

R – Robert Michael BARWELL (2007)

A sentence of imprisonment for public protection was inappropriate where there was evidence to suggest that a defendant's repressed paedophilic tendencies could be controlled and minimised with effective treatment.

Microsoft -v- Paul FOX 2006 (reported on out-law.com 12/09/2006)

Rather than pursue a case under limited British law (Privacy and Electronic Communications Regulations 2003) Microsoft filed a complaint that Fox had breached the terms of its hotmail service. Its conditions state "You may not use any (Microsoft) service to send Spam, You may also not deliver Spam or cause Spam to be delivered to any Microsoft services or customers." Microsoft's case claimed that Fox was running a business via his spamming. The beneficiary of the campaign was a pornographic video download site. The victim would receive an e-mail with a mobile phone number that they would text to receive access to the site which is how FOX was able to make money. Fox was ordered to pay £45,000 in damages.

R – Ross Warwick PORTER (2006)

Porter appealed against conviction for possession of indecent photographs of children contrary to Criminal Justice Act 1988 S160(1). Some of the items he was convicted of had been deleted and could no longer be viewed prior to the date contained on the indictment. In the case of a deleted computer image if a person could not gain access to an image then he no longer had custody or control of it. It was for the jury to decide whether images were beyond the control of a defendant having regard to all circumstances if the case, including his knowledge.

R – v – LENNON, Wimbledon Magistrates Court (Nov 2005)

Lennon, a teenager, was cleared of launching denial of service attacks against his former employer. Sitting at Wimbledon Magistrates Court, Judge Kenneth Grant ruled that the youth had not broken the CMA, under which he was accused of sending five million e-mails to his ex-employer causing the firm's server to crash. In a written ruling Judge Grant said "In this case the individual e-mails caused to be sent each caused a modification which was in each case an "authorised" modification. Although they were sent in bulk resulting in the overwhelming of the server, the effect on the server is not a modification addressed by section 3(of the CMA)." This decision was overturned on appeal and LENNON was subsequently convicted in respect of his sending 5 million e-mails to his ex-employer causing the email server to fail. Prior to the decision being reached on appeal the CMA was reworded within Police and Justice Bill.

R – v – STRASZKIEWICZ 2005

On the 17th August 2005 STRASZKEIWICZ was found guilty at Isleworth Crown Court of dishonestly obtaining an electronic communications service and possessing equipment for fraudulent use of a communications service. He was prosecuted under sections 125 and 126 of the Communications Act 2003, having been caught standing outside a residential area holding a wireless enabled lap top. The CPS confirmed Straszkiewicz was "piggybacking" the wireless network that householders were using.

R – DOOLEY 2005

A person who possessed an indecent photograph or pseudo-photograph of a child, did so "with a view to" its being distributed or shown by him or others, contrary to s 1(1)(c) of the Protection of Children Act 1978, if one of his reasons, but not necessarily the primary reason, for possessing it, was that it would be distributed or shown. HOOPER LJ, giving the judgment of the court, said that thousands of indecent images of children were found on the defendant's computer. Most had been downloaded via a file sharing system whereby members installed software allowing their files, held in their shared folder, to be accessed and downloaded directly into shared folders of other members, whilst connected to the internet. Only six of all the files downloaded were found in his shared folder. He contended that he did not intend to distribute or show them to others. Once downloaded, he usually moved them into folders not accessible to other members. The six files had not yet moved due to the way he downloaded and moved images in bulk. Pre-trial, the judge ruled that if the defendant had knowledge that photographs he downloaded were likely to be seen by others having access to the shared folder, he possessed them "with a view to" their being distributed or shown for the purposes of s 1(1)(c) of the 1978 Act. As a result, the defendant pleaded guilty.

His Lordship said that the defendant allowed the files to remain in the shared folder "with a view to" their being shown or distributed, if one of his reasons, but not necessarily the primary reason, for doing so, was to enable others to see it or download it. Although his state of mind or knowledge regarding whether they were likely to be seen might be very important if not decisive in deciding whether he had "a view to" their being distributed or shown, he could only commit the offence if one of the reasons at least for leaving the file in the shared folder was that it would be distributed or shown to others. Accordingly, the judge erred in ruling as he did, and as the guilty pleas were entered on the basis that the defendant had no defence if he knew the files were likely to be accessed, the convictions were unsafe and would be quashed. No retrial was sought by the prosecution and none would be ordered.

R (O) –v- Coventry Magistrates' Court 2004

This case addressed the argument that by entering information onto a computer you could not be guilty of incitement as you were not inciting a human mind. It was held in this case that it did not matter if the whole process was automated by computer. The computer was used to facilitate the business, it was irrelevant to say that only the computer was encouraged to incite; some-one was lying behind the computer.

R-v- Thompson 2004

This case detailed the practice to be followed when drafting indictments for offences relating to abusive images of children..

R -v- Gary Geoffrey THOMAS 2004

Having been convicted of 5 charges of possession of indecent images of children obtained from the internet and 3 counts of USI, THOMAS was convicted and as part of his sentence the Judge at Mold Crown Court imposed a 5 year restraining order preventing THOMAS from using the internet or mobile phones. (Awaits appeal decision in respect of undue effect of this order on his human rights.)

R –v- Barry HOLLOREN 2004

Again, in this case, having been convicted of 13 counts of making indecent images of children an indefinite restraining order preventing HOLLOREN from owning or using a computer equipment or having access to the internet save in relation to employment was made - this restraining order was successfully appealed against on the basis that there was nothing to indicate that it was necessary to make the order to protect the public or particular member of the public from "serious harm".

LAPPIN -v- HM Customs and Excise (2004)

Although this case does not relate to computer/internet investigations it may be of assistance in respect of cases whereby the defence request an adjournment as they have failed to instruct an expert witness in adequate time. The circumstances in this case were that the appellant had had four months to instruct an expert witness but had failed to do so. A refusal of an application for an adjournment was held not to compromise a breach of the appellant's rights under Article 6 of the European Convention of Human Rights (right to a fair trial.)

Vogon International Limited v The Serious Fraud Office (2004)

This case highlights the importance, when outsourcing work, of ensuring that the company carrying out the work and the person making the request are both clear on what they mean when discussing the work to be completed. In this case there was a dispute over the meaning of the word "database" resulting in Vogon invoicing for a total of £314,375 for work done, the SFO had anticipated the work to only result in a cost of £22,500. It this case it was held in favour of the SFO's and the amount to be paid to Vogon was the anticipated £22,500.

R v Graeme John PARDUE (2003)

This case highlights the importance of following correct procedure re TIC's. It was held that the court could only sentence on the offences to which the defendant had pleaded guilty to at court (17 charges of making indecent images of children) and not the possession of a further 1000 indecent images of children – as although admitted in interview they were never fully admitted as TIC's before the court. Therefore the defendant's initial sentence of 15 months imprisonment was reduced to 10 months.

R v David John RUSSELL 2003 (Ct of Appeal 09/04/2003)

This case followed the sentencing guidelines as per R-v-Oliver above in that a sentence of 18 months imprisonment was reduced to 12 months for the offence of making indecent photographs or pseudo-photographs of children.

NTL Group Limited v Ipswich Crown Court 2002

NTL disputed that they should comply with a request from the Chief Constable of Suffolk Constabulary for access to special material i.e. e-mail content, on two counts (i) NTL held the material in confidence, (ii) to comply with the request would involve committing an offence under S1 RIPA 2000. It was held NTL were to disclose the material and they would not be committing an offence under RIPA, as NTL would be acting under a lawful authority.

R v OLIVER, HARTREY & BALDWIN 2002 (reported 6/12/02 in The Times)

The court in this case adopted the advice of the Sentencing Advisory Panel (published in August 2002) except in one or two respects for the purpose of sentencing those convicted of offences involving indecent photographs or pseudo-photographs of children.

R v THAMES MAGISTRATES COURT (2) C&E COMMISSIONERS, Ex Parte (1) Paul Da Costa (A firm) (2) Stewart Collins (2002)

During the search of two offices a number of documents were seized and retained by the Customs & Excise. An image was taken of two of each of the two hard discs on the firm's computers server and possession was also taken of some computers themselves. Amongst the arguments by defence was that by imaging the hard drive a large number of documents relating to the firms clients were "seized". Lord Justice Kennedy agreed with the argument put forward by Customs & Excise that "a computer hard disk is a single storage entity and fell within the definition of a document because it is something "in which information of any kind is recorded". Thus a hard disk may be seized and removed provided that it contains material which the searching officer at the time of the search has reasonable cause to believe might be required as evidence in relation to a suspected offence or offences. The officer is not required to extract from

the hard disk just the information he believes may be required, nor is it practicable for him to do so".

R v COMMISSIONERS OF INLAND REVENUE, Ex Parte H (2002)

It was held that when the Inland Revenue officer entered a premises under the authority of a warrant and found a computer, and if he had reasonable cause to believe that the data on that computer's hard disc might be required as evidence for the purpose of relevant proceedings, he was entitled to seize and remove the computer even though it might contain irrelevant, non-incriminating material. This case clearly distinguished itself from Bramley, Justice Burton stated "These facts show that the comparison of a hard disc with a filing cabinet is inexact and may be misleading. For some purposes no doubt the files on a hard disc may be regarded as separate documents. But a hard disc cannot be regarded as simply a container of the files visible to the computer's operating system. It is a single object: a single thing. I see no basis, therefore for a computer not being considered a "thing". If there is incriminating (in the normal sense of the word) material on the hard disc, and if it is assumed that the hard disc is not copied, the computer itself may be used, and may be required, as evidence in order to prove the existence of the incriminating material on the defendant's computer. The fact that there is also on the hard disk material that is irrelevant, and not evidence of anything, does not make the computer any less of a thing that may be required as evidence for the purposes of criminal proceedings."

R v (1) CHESTERFIELD JUSTICES (2) CHIEF CONSTABLE OF DERBYSHIRE, ex Parte Bramley (2000).

This case centred on the seizure of a large volume of documents, some of which were known to possibly contain legally privileged material. It was held that police had acted beyond the powers of the search warrant as at this time there is no power to seize items and sift through them at a later date unless you have reasonable grounds to believe they are of evidential value. In this case there were no such grounds and it would have been reasonable to believe some of the documents held legally privileged material.

R v BOW STREET MAGISTRATES' COURT (2) ADENYI MOMODU ALLISON, EX PARTE THE GOVERNMENT OF THE USA 1999

A successful appeal by the Government of the USA to the House of Lords, there had been a conspiracy to commit offences falling within S2 Computer Misuse Act 1990 as alleged, and that computer crime was an offence and extraditable under UK law.

R v (1)Graham Westgarth SMITH (2) Mike JAYSON 2002

SMITH: No offence of "making" or "being in possession of an indecent pseudo-photograph was committed by opening an e-mail attachment, when the recipient was unaware that it contained or was likely to contain an indecent image.

JAYSON: The act of voluntarily downloading an indecent image from the internet to a computer screen was an act of making a photograph or pseudo-photograph because the computer's operator, in so downloading, was causing the image to exist on the screen.

R v GOLDMAN 2001

Ordering porn videos showing young people, from a mail order company is incitement. In this case the accused wrote to a porn company in Holland requesting a specific compilation tape of girls aged 7-13 years. The company did not send anything and accused wrote again insisting his order be filled. In this case he was doing more than merely responding to an advertisement.

ATKINS v DPP 2000

No offence of possession under S160 Criminal Justice Act 1988 unless the accused knew he had possession of the photographs. It needs to be shown the accused is aware of photographs held in the cache.

GOODLAND v DPP 2000

A photographic montage does not fall within the scope of the Protection of Children Act 1978.

R v WADDON 2000

Publishing an article under S1(3)(b) of the Obscene Publications act 1959 included data stored electronically and transmitted. To transmit meant simply to send on from one place or person to another.

R v MOULD 2000

Exhibits showing the interest of an accused in paedophile material are relevant.

MORGANS v DPP 2000

Meaning of communication. Disclosure of telephone type intercepts not required.

R v BOWDEN 1999

The downloading and/or printing out of computer data of indecent images of children from the Internet is capable of amounting to an offence under S1(1)(a) Protection of Children Act 1978

R v LAND 1997

There is no requirement for expert evidence to be produced re the age of a child depicted in indecent images. Such an assessment is within a jury's field of experience.

R v FELLOWS:ARNOLD 1997

Data stored on a computer disc or by other electronic means is capable of being a photograph. Data stored in the disc is also capable of being "shown or projected" in relation to the wording of the Obscene Publications Act 1959.

DPP v BIGNELL 1997

A prosecution brought under the Computer Misuse Act 1990 was to criminalise hacking; improper use of data held on a computer must be prosecuted under the Data Protection Act 1984.

Data Protection:

There have been challenges under the Data Protection Act, the following cases relate to transfer of data between different agencies.

R-v-ROONEY 2006

A police employee was found guilty of using police systems in breach of the Data Protection Act. The judgement appears to clash with the recent verdict in Durant, where a much narrow definition of the meaning of personal data.

Michael John DURANT v Financial Services Authority (2003)

The mere mention of a data subject in a document did not amount to "personal data" within the meaning of the Data Protection Act 1998. The purpose behind the Data Protection Act 1998 was to provide the same standard of accessibility to manual as to computerised records.

R v (1)C (2) D, Ex Parte A 2000

There is no basis for challenging either the transfer of non-conviction information relating to the applicant from one police force to another or the disclosure of that information by the recipient force to a local education authority which had both a legitimate interest and a pressing need to receive it.

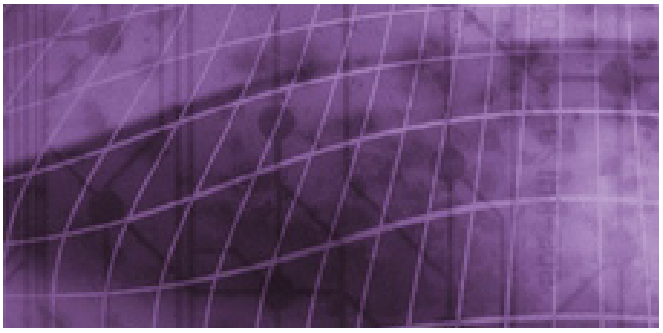
R v (1) A Police Authority in the Midlands (2) A County Council in the Midlands Ex Parte L M 1999

Where allegations of sexual abuse of children had been made against an individual, disclosure of those allegations, whether to the general public or to any other individual(s) had to satisfy the "pressing need" test and in balancing the need to protect children against the right of an individual to a private life, the body making the disclosure had to consider: (I) its belief in the truth of the allegations; (ii) the interest of the third party in obtaining the information; and (iii) the degree of risk posed by the individual if disclosure was not made.

R v Chief Constable for the North Wales Police, Ex Parte Thorpe 1998

An appeal was made in relation to the decision of North Wales Police to disclose details of sex offenders. Each case should be judged on its own facts and disclosure should only be made where there is a pressing need for that disclosure. Any decisions must be judged against Article 8 European Convention on Human Rights.

APPENDIX F



APPENDIX F

Forensic Matters

For the information of managers seeking to understand the operations of the Forensic Analyst, outlined below is a skeleton process which will mimic most operations. Included within the steps are short explanations of the meaning and purpose.

Reception of exhibits into the unit

- Tasks:
- Check that items are sealed and bagged
- Continuity labels should be completed
- Book into Unit Property System
- Issue Job number
- Start Job Log
- Set priority level
- Check content of submission forms, particularly the brief and job requirements
- Take Digital Photographs of exhibits in bags
- Place items requiring onto charger (usually PDAs)
- Charging/Batteries for portable items (ongoing)
- Logging
- Place items into Secure Store

Physical Examination

- Collect item(s) from Secure Store – Continuity
- Remove from bags – record & retain old seal
- Identify items requiring imaging/examination – issue sub exhibit numbers if required
- Identification of examination method for the exhibit/media
- Take Digital Photographs of items
- Disassembly as required
- Internal Photographs
- Safety issues
  - PAT – portable appliance testing (Local Health & Safety requirements)
  - Check item appears safe to apply power
  - Record Foreign items in case & photo as required
- Note internal components, particularly those relevant
- Establish machine capabilities from hardware identification
- Reassembly
  - Computers – Carry out safe boot with any Disks unconnected
  - BIOS Recording of System Time/Date & any other relevant settings
  - Log all operations
  - Return to Secure Store – Continuity

Securing the data

- Secure store – Continuity
- Prepare work area and equipment for operations
- Check & test Imaging equipment & software
  - Retain all versions of software used
  - Record machine used
- Set Exhibit numbers for image files
- Ensure Audit trail
- Carry out imaging operation – obtain complete copy of data from media

Store Forensic images

- Backup of images
- Verify images and copies
- Use of 'Copy'
- Logging
- Secure Store – Continuity

Data Examination

- Secure store – Continuity of image exhibits
- Check brief for parameters of examination
- Check copies of interview/briefing notes/Liaise with OIC
- Carry out Virus Scan if in policy
- Set up for type of Examination required
- Set Level of examination
- Establish expertise of examiner for levels
- First Stage examination
  - Automated processes
  - Use of scripts
  - Pick Lists to identify processes in this stage
  - Production of printed & media exhibits + exhibit numbers
  - Logging of operations
- Second Stage examination
- Detailed examination
- Searches and recovery
- Examination of and recovery from unallocated space
- Expert examination
- Identification and use of Expert
- Use of evidence of opinion
- Experimentation to prove particular outcomes
  - Analysis of evidence found

- Logging

Re-examine & re-visit as required

Security and backup of working files

- Secure Store – Continuity

Report/Statement

- Log of all operations
- Liaison with OIC and CPS re: charges

Disposal

- Of exhibits
- Of seized items
- Of items for destruction
- Destruction or secure wipe?
- Forfeiture – content of order

Use of seized equipment

Retention

- Policy

Comply with ACPO Guide for Management of Police Information

Criminal Procedure and Investigations Act

Other Matters for consideration

Replies to/liaison with defence expert

- Comply with local policy on release of data
- Equality of arms for viewing by defence

Disaster Recovery/Backup

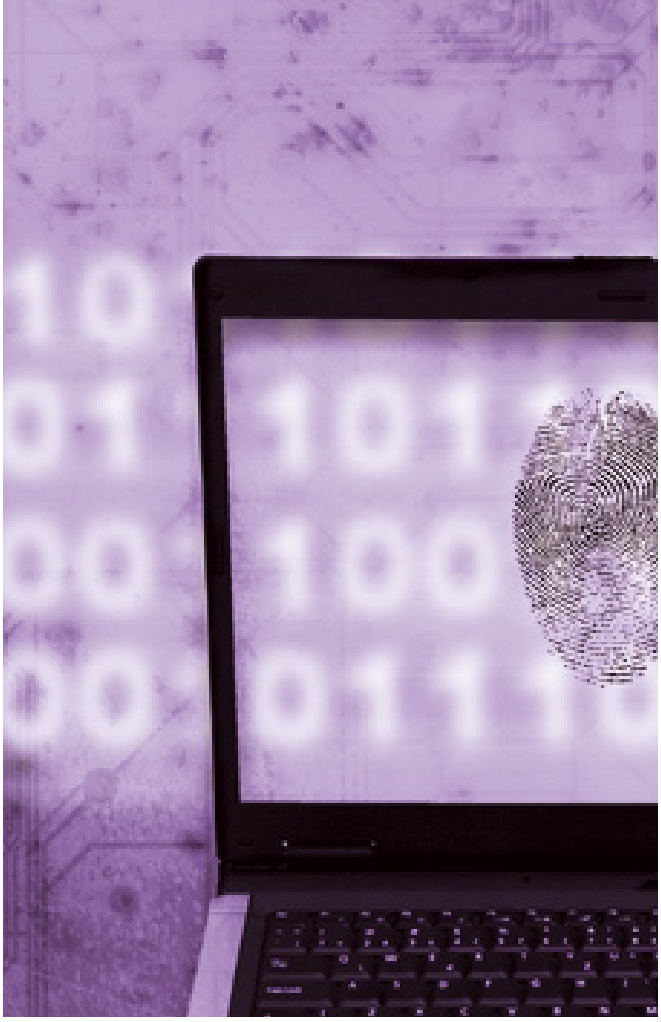
- Image Files
- Working Case Files
- Reports/Statements
- Tools Disks
- Tools Software

Expert evidence

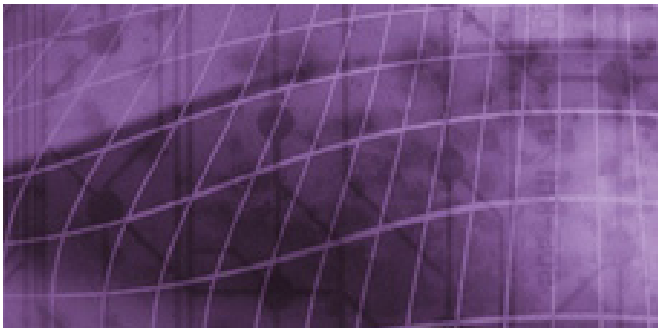
- Recognition of level of local expertise
- Selection and use of external expert

Disclosure

- Image & Working Case Files
- Paper Exhibits
- Unlawful' material
- Viewing of material by defence



APPENDIX G



APPENDIX G

Sources of Advice and Points of Reference

ACPO Good Practice Guide for Computer Based Electronic Evidence, Issue 4, 2006

Interpol Computer Crime Manual – 1992-2004

ACPO eCrime Strategy - A Strategic Approach To National eCrime 2009

Home Office Acquisition and Disclosure of Communications Data Code of Practice, pursuant to Section 71 RIPA 2007

Internet Points of Reference:

Internet Crime Forum
www.internetcrimeforum.org.uk

For ISO Standards, including more details regarding 17799, 20000 & 9001
http://www.iso.org/iso/home.htm

Health and Safety Executive
www.hse.gov.uk

Crown Prosecution Service
www.cps.gov.uk

Cyberangels about Cyberstalking
www.cyberangels.org

Internet Watch Foundation
www.iwf.org.uk

Law Commission
www.lawcom.gov.uk

Legislation
http://www.opsi.gov.uk/legislation/about_legislation.htm

National Infrastructure Security Co-ordination Centre
www.niscc.gov.uk

National Policing Improvement Agency
www.npia.police.uk/hightechcrime

National White Collar Crime Centre (NW3C)
http://www.training.nw3c.org/ocr/courses_desc.cfm

Police Reform Information h
ttp://police.homeoffice.gov.uk/police-reform/

Royal Military College Shrivenham
www.rmcs.cranfield.ac.uk

The Stationary Office
www.tso.co.uk

Keeping up to date:

F3 Forum
http://www.f3.org.uk/

www.digital-detective.co.uk

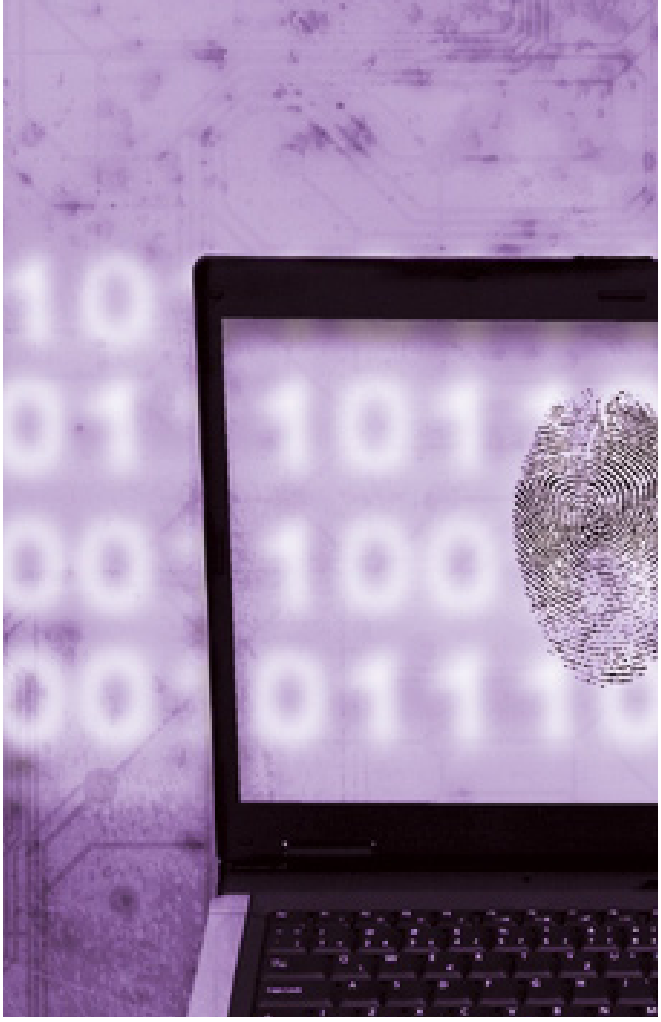
www.cybercrime.gov.

IACIS www.cops.org

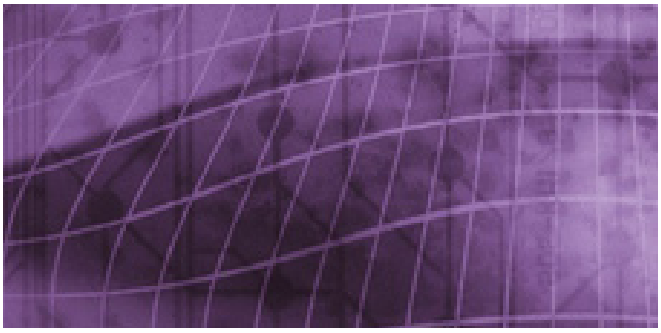
http://www.training.nw3c.org/research/recent_initiatives.cfm

http://www.ojp.usdoj.gov/nij/pubs-sum/187736.htm

www.forensicfocus.com



APPENDIX H



APPENDIX H

Glossary of Acronyms for this Guide

ACPO – Association of Chief Police Officers

BSA – British Software Alliance

CCU – Computer Crime Unit

CEOP – Child Exploitation and On Line Protection Centre

CFFC – Centre for Forensic Computing, Cranfield University, Royal Military College of Science, Shrivenham

CMA – Computer Misuse Act 1990

CMOS – Complimentary metal Oxide conductor, stores system time/date and other machine settings

CPIA – Criminal Procedures Investigations Act 1996

CPNI – Centre for the Protection of National Infrastructure

CPS – Crown Prosecution Service

CSP – Communications Service Provider

CTOSE – Cyber Tools On-Line Search for Evidence

DCI – Detective Chief Inspector

DEG – Digital Evidence Group

DOS – Denial of service Attack

DDOS – Distributed Denial of Service Attack

DP – Designated Person

ECHR – European Commission on Human Rights

F3 – First Forensic Forum

FSA – Financial Services Authority

FSS – Forensic Science Service

Gb – Gigabyte 1,000,000,000 bytes of data

HTCU – Hi-Tech Crime Unit

IACIS – International Association of Computer Investigative Specialists

ICF – Internet Crime Forum

ICT – Information and Communication Technology

ISO – International Standards Organisation

IWF – Internet Watch Foundation

JANET – Joint Academic Network

LEA – Law Enforcement Agency

MLAT – Mutual Legal Assistance Treaty

MLE – Managed Learning Environment

MOU – Memorandum of Understanding

NCALT – National Centre for Applied Learning Technologies

NIM – National Intelligence Model

NISCC – National Infrastructure Security Co-ordination Centre

NPIA – National Policing Improvement Agency

SOCA – Serious Organised Crime Agency

NTAC – National Technical Assistance Centre

OIC – Officer-in-Case

PAT – Portable Appliance Testing

PDA – Personal Digital Assistant/Digital Organiser

PG Cert – Post Graduate Certificate

PSNI – Police Service of Northern Ireland

QC – Queens Counsel

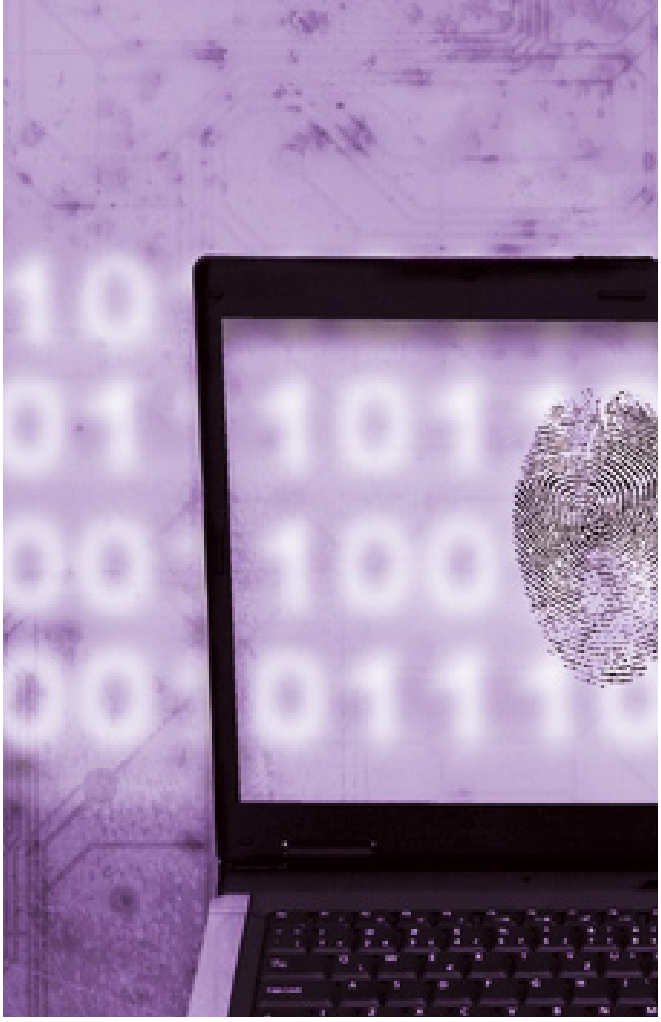
RIPA – Regulation of Investigatory Powers Act 2000

SFO – Serious Fraud Office

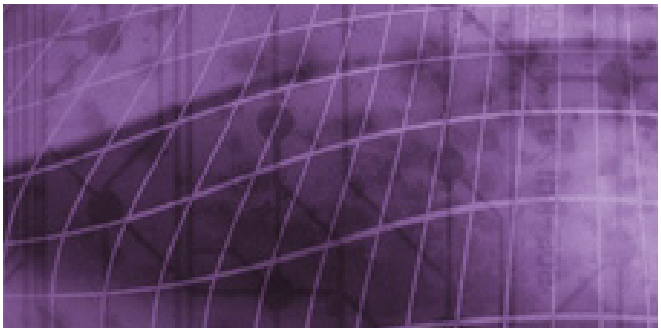
SIO – Senior Investigating Officer

SLA – Service Level Agreement

SPOC – Single Point of Contact



APPENDIX I



APPENDIX I

Explanation of some Common Terms

These terms designed for managers provide a brief description of some of the more common terms that are used. Should more information be required the further research will be necessary.

A

ADDRESS

The term address is used in several ways.

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

AOL (AMERICA ONLINE)

An online information service based in the USA that provides e-mail, news, educational and entertainment services, and computer support by means of a graphical user interface. America Online is one of the largest American Internet access providers.

ARCHIVE FILE

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

ATTACHMENT

A file carried with an e-mail.

B

BACKUP

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

BIOS

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

BOOT

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

BOOT DISK

A disk that contains the files needed to start an operating system.

BROADBAND

A high bandwidth internet connection e.g. ADSL or cable.

BROWSER

A browser is a program that provides a way to look at, read, and even hear all the information on the World Wide Web. Common examples are Firefox, Netscape and Internet Explorer.

BUFFER

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

BULLETIN BOARD SERVICE (BBS)

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

BYTE

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

C

CACHE

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

CDF

Channel Data Format. A system used to prepare information for Webcasting.

CDR

Compact disk – recordable. A disk to which data can be written but not erased. CDROM (compact disc read only memory or media) in computers, CDROM technology is a format and system for recording, storing, and retrieving electronic information on a compact disk that is read using laser optics rather than magnetic means.

CDROM

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

CDRW

Compact disk – rewritable. A disk to which data can be written and erased.

CHAT ROOM

A virtual room on the Internet where chatting takes place. Generally, chat rooms have topics or themes.

CHATTING

On the Internet, chatting is talking to other people who are using the Internet at the same time you are. This "talking" is the exchange of typed in messages by a group of users who take part from anywhere on the Internet. In some cases, a private chat can be arranged between two parties who meet initially in a group chat. Chats can be ongoing or scheduled for a particular time and duration. Most chats are focused on a particular topic of interest. Some involve special guests such as celebrities, athletes and politicians who "talk" to anyone joining the chat.

CMOS

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

COOKIE

A piece of information or message sent by a web site server to a web browser, where it is stored on the local computer. Each time someone on that computer goes back to the particular web page, the message is sent back to the server. Depending on the type of Cookie used, and the browser's settings, the browser may or may not accept the Cookie, and may save the Cookie for either a short time or a long time. Cookies might contain information such as login or registration information, online "shopping cart" information, user preferences, etc.

COMPACT FLASH CARD

A form of storage media, commonly used in digital personal organisers and cameras but can be used in other electronic devices including computers.

CPU

Central processing unit – the computational and control unit of a computer. Located inside a computer, it is the "brain" that performs all arithmetic, logic and control functions in the computer.

CRACKER

A computer expert that uses his or her skill to break into computer systems with malicious intent or motives. The term was coined by Hackers to differentiate themselves from those who do damage systems or steal information.

CRC

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

CRYPTOGRAPHY

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

CYBERSPACE

The area in which computer users travel when navigating a network or the Internet.

D

DATABASE

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

DATA ENCRYPTION KEY

Used for the encryption of message text and for the computation of message integrity checks (signatures).

DECODE

The converting of encoded data to its original form.

DECRYPTION

The reverse of encryption, a method of unscrambling encrypted information so that it becomes legible again.

DELETED FILES

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

DENIAL OF SERVICE ATTACKS & DISTRIBUTED DENIAL OF SERVICE ATTACKS (DOS AND DDOS)

Denial of Service Attacks are aimed at specific Web sites. The attacker floods the Webserver with messages endlessly repeated. This ties up the system and denies access to legitimate users. Denial of Service attacks which are carried out by someone attacking from multiple computers are known as Distributed Denial of Service attacks.

DICTIONARY ATTACKS

The attacker uses a program that continuously tries different common words to see if one matches a password to the system or programs.

DIGITAL BOMB

A program that lies dormant, waiting to be activated by a certain date or action.

DIGITAL EVIDENCE

Information stored or transmitted in binary form that may be relied upon in court.

DIGITAL PIRACY

The unauthorised copying and resale of digital goods (e.g.software, musicfiles).

DIGITAL SIGNATURE

A code which is used to guarantee that an email was sent by a particular sender.

DISCUSSION GROUP

An online forum in which people communicate about subjects of common interest. Forums for discussion groups include electronic mailing lists, Internet newsgroups and IRC channels.

DISK CACHE

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

DOS

The Domain Name Service is one of the core Internet protocols and mechanisms. DNS is what translates human readable names (e.g. “www.microsoft.com”) into the binary IP addresses that are actually used to move data packets around on the Internet.

DOCKING STATION

A device to which a laptop or notebook computer can be attached for use as a desktop computer, usually having a connector for externally connected devices such as hard drives, scanners, keyboards, monitors and printers.

DOMAIN NAME

A domain name locates an organisation or other entity on the Internet; it allows you to reference Internet sites without knowing the true numerical address

DONGLE

A term for a small external hardware device that connects to a Computer, often via a USP Port, to authenticate a piece of software; e.g. proof that a computer actually has a licence for the software being used.

DOWNLOAD

To transfer data from a remote server to your local system.

DVD

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

E

EBAY

A proprietary name for an internet auction web site

ECASH

Money that is used in transactions entirely electronically.

ECOMMERCE

A term used to describe the buying or selling of goods or services over the Internet. Usually, payment is made by using a credit or debit card.

EMAIL BOMBS

To flood an email account or server with mail.

EMAIL HEADER

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

ENCRYPTION

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

EXTENDED HEADERS

Information that is added by email programs and transmitting devices – which shows more information about the sender that is in many circumstances traceable to an individual computer on the Internet.

EXTRANET

An intranet that is accessible to computers that are not actually part of a companies own private network, but that is not accessible to the general public.

F

FAQ (USED IN EMAIL AND NEWSGROUPS)

An acronym that generally refers to a list of frequently asked questions and their answers, or a question from the list. Many USENET newsgroups and some non-USENET mailing lists maintain FAQ lists (FAQs) so that participants don't spend a lot of time answering the same questions. It's a good idea to look at a FAQ file for a newsgroup or mailing list before participating in it.

FILE TRANSFER

The copying of a file from one computer to another over a computer network.

FIREWALL

Software typically run on a dedicated server that blocks transmission of certain classes of traffic to secure internal LANs from the outside world.

FLOPPY DISK

These are disks that hold information magnetically. They come in 2 main types 3½ inch and 5½ inch. The 5½ inch disks which are now rarely seen, are flexible and easily damaged, the 3½ disks are in a stiff case. Both are square and flat. Older machines may use larger or smaller sizes of disks.

FREE SPACE

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

FTP (FILE TRANSFER PROTOCOL)

File Transfer Protocol is used to send whole documents or collections of documents stored in one computer to another through the Internet.

G

GATEWAY

A computer system that transfers data between normally incompatible applications or networks. It reformats the data so that it is acceptable for the new network (or application) before passing it on.

GIGABYTE

(Gb) 1 Gigabyte = 1024 Megabytes. A gigabyte is a measure of memory capacity and is roughly one thousand megabytes or a billion bytes. It is pronounced GIGabite with hard G's.

GOOGLE

Google search is a Web search engine and is the most used search engine on the Web. Google receives several hundred million queries each day through its various services.

H

HACKER

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

HARD DISK

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

HARDWARE

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

HISTORY LIST

A list of Web documents that were seen during a session.

HOME PAGE

The first page presented to a user when he or she selects a site or presence on the World Wide Web. It serves as a starting point for browsing the web site.

HOST

On the Internet, a host is any computer that has full two way access to other computers on the Internet. A host has a specific local or host number that, together with the network number, forms its unique Internet Protocol address. If you use Point to Point Protocols (PPP) to get access to your Internet Service Provider (ISP), you have a unique IP address for the duration of any connection you make to the Internet and your computer is a host for that period. In this context, a host is a node in a network.

HOST MACHINE

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

HOTLINE

Hotlines on the web are usually similar to a telephone hotline. Instead of dialling, you go to the hotline Web site, type the details you wish to report and a message is transmitted to the hotline organisation over the Net.

HTML

Hypertext Mark up Language is the evolving standard for creating hypertext documents published on the World Wide Web. It not only formats documents, but also links text and images to documents residing on other web servers.

HTTP

Hypertext Transfer Protocol Documents formatted with hypertext links are sent and received using HyperText Transmission Protocol. In order for hypertext documents to be sent and displayed properly, and to have active hypertext links, software on both the sending and receiving end must use HTTP.

HUB

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

HYPERTEXT LINK

Any text or graphic that contains links to other documents. Clicking on a link automatically displays the second document.

I

IAP

Internet access provider, also known as an Internet Service Provider.

ICQ ("I SEEK YOU")

A program that alerts users in real time when friends and colleagues sign on. Users can create a Contact List containing only people they want to have there, chat with them, send messages and files, play games or use it as a business tool to find and contact associates in real time through the Internet.

IMAGE

The taking of an exact copy of the data from a digital device for examination

IMAGING

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

IMAP

Internet Message Access Protocol. IMAP is gradually replacing POP as the main protocols by email clients in communicating with email servers. Using IMAP on email client programme can not only retrieve email but can also manipulate messages stored on the server, without having to actually retrieve the messages. So messages can be deleted, have their status changed, multiple mail.

IMEI

International Mobile Equipment Identifier. A unique 15 digit number that serves as the serial number of a GSM handset.

IMSI

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

INSTANT MESSAGING

Technology similar to that of a chat room, it notifies a user when a friend is online allowing them to exchange messages.

INTERNET RELAY CHAT (IRC)

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

INTERNIC (INTERNET NETWORK INFORMATION CENTRE)

InterNIC is the organisation responsible for registering and maintaining the com, edu, gov, net and org domain names on the World Wide Web. If you are creating or already have a web site, you must register the domain name with InterNIC.

INTRANET

An intranet is a network of networks designed for information processing within a company or organisation. Intranets are used for such services as document distribution, software distribution, access to databases and training.

IP

Internet Protocol.

IP SPOOFING

A technique used to gain unauthorised access to computers.

IP ADDRESS

Each computer connected to the Internet is addressed using a unique 32bit number called an IP Address. These addresses are usually written in Dotted Quad notation, as a series of four 8bit numbers, written in decimal and separated by periods. For example: 151.196.75.10. Each number in the IP address falls between 0 and 255. So if you ever see something that looks like an IP address with numbers outside those ranges it's not a real address. For example, a computer running virtual websites will have an IP address for each website it hosts. In addition, a pool of IP addresses may be shared between a number of computers. For example, on a dynamic-IP dialup connection your computer will be allocated a different IP address each time you connect.

ISDO

Integrated Services Digital Network is a standard for transmitting voice, video, and data over digital lines.

ISP

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

J

JAZ DISK

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

JPEG (PRONOUNCED "JAYPEG")

An acronym for the Joint Photographic Experts Group, and refers to a standards committee, a method of file compression and a graphics file format. The committee originated from within the International Standards Organisation (ISO) to research and develop standards for the transmission of image data over networks. The results were a highly successful method of data compression and several closely associated file formats to store the data. JPEG files typically contain photographs, video stills or other complex images.

K

KEYRING

A pair of keys that consists of both a public key and its corresponding private key. Keyrings are used in public key encryption systems such as Pretty Good Privacy (PGP). Data encrypted with someone's public key can only be decrypted with the corresponding private key, and vice versa. See also Encryption, Pretty Good Privacy (PGP).

KILOBYTE

(KB) 1 Kilobyte = 1024 bytes.

Keyword

A word you might use to search for a web site.

L

LAN

Local Area Network, a computer network that covers only a small area (often a single office or building).

LATENT

Present, although not visible, but capable of becoming visible.

LINK

Any text or graphic coded and formatted so that clicking on it automatically displays a second document or image.

LINUX

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

LOGIN

Noun: the account name used to gain access to a computer system. Not a secret (contrast with password)
Verb: the act of connecting to a computer system by giving your credentials (usually your username and password)

LURKING

To receive and read articles or messages in a newsgroup or other online conference without contributing anything to the ongoing exchange.

M

MACRO VIRUS

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

MAGNETIC MEDIA

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

MAILBOX

Directory on a host computer where your email message are stored with some systems you can elect to keep saved messages either on the server or your local computer as you prefer.

MAPS

Mail Abuse Prevention System. An organisation and system set up to defend the internet's email system from abuse by spammers through their RBL (Realtime Blackhouse List)

MD5 HASH

An algorithm that is used to create digital fingerprints of storage media such as a computer hard drive, but is also commonly used to check the integrity of computer files. When this algorithm is applied to a file, it creates a unique value, typically expressed as a 32 digit hexadecimal number. Changing the data on the disk in any way will change the MD5 value.

MEDIA CARDS

Small sized data storage media that are more commonly found in other digital devices such as cameras, PDA's (Personal Digital Assistants) and music players. They can also be used for the storage of normal data files, which can be accessed and written to by computers. There are a number of different formats including –
Smartmedia card
SD Expansion Card
Ultra Compact Flash
Compact Flash
Multimedia Card
Memory Stick
The cards are non-volatile – they retain their data when power to their device is stopped – and they can be exchanged between devices.

MEGABYTE

(Mb) 1 Megabyte = 1024 Kilobytes.

MEMORY

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

MEMORY STICK

A USB storage medium. See USB Storage Devices

MESSAGE ID

A unique number assigned to a message.

MHZ (MEGAHERTZ)

MHz is a unit of alternating current (AC) or electromagnetic (EM) wave frequency equal to one million hertz (1,000,000 Hz). It is commonly used to express microprocessor clock speed.

MODEM

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

MSDOS

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

MULTIMEDIA

Documents that include different kinds of formats for information or data. For example, text, audio, and video, may be included in one document.

N

NETSCAPE

An application used to browse the World Wide Web.

NETWORK

A group of computers and associated devices that are interconnected by communication paths. A network can involve permanent connections, such as cables, or temporary connections made through telephone or other communication links. A network can be as small as a few computers, printers, and other devices, or it can consist of many small and large computers distributed over a vast geographic area.

NEWSGROUP

An electronic discussion surrounding a particular subject. It consists of messages posted a central Internet site and redistributed through Usenet, a worldwide network of news discussion groups.

NODE

Any single computer connected to a network. The processing location within a network. The processing location, node, can be a computer, printer, scanner or other type of device within a network.

O

OFF LINE

Not connected

ON LINE

Having access to the Internet

OPERATING SYSTEM

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

ORB

A high Capacity removable hard disk system. ORB drives use magneto resistive (MR) read/write head technology.

P

PPP (POINT TO POINT PROTOCOL)

PPP is a protocol for communication between two computers using a serial interface, typically a personal computer connected by phone line to a server.

PACKET

A packet is a bundle of data that is routed between an origin and a destination on the Internet. When information such as files, email messages, HTML documents, web pages, etc. are sent from one place to another on the Internet, TCP/IP divides the information into chunks of an efficient size for routing. Each of these packets includes the Internet address of the destination. The individual packets for the information being routed may travel different routes through the Internet. When they have all arrived, they are reassembled into the original file by TCP/IP.

PALMTOPS

A portable personal computer that fits into the palm of your hand. See Personal Organiser or Personal Digital Assistant (PDA)

PASSWORD

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

PCMCIA CARDS

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

PEER TO PEER (P2P)

On the internet, Peer to Peer (often referred to as P2P) is a type of transient internet network or protocol that allows a group of computer users with the same networking program, to connect with each other and directly access files from one another's hard disk drives. There are a wide variety of these networks, including Kazaa, Bit Torrent, eDonkey and Gnutella. Typically the most commonly shared files include pictures, movies, music and software programs.

PICK LIST

A list of relevant items/processes for choice

PENDRIVE

A small USB storage medium. See USB Storage Devices

PERIPHERALS

Devices external to a computer e.g. printer, monitor, external disk

PERSONAL ORGANISER OR PERSONAL DIGITAL ASSISTANT (PDA)

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

PHISHING AND PHARMING

Phishing attacks use 'spoofed' emails and fraudulent websites designed to fool recipients into divulging personal data such as credit card numbers, account user names and passwords, social security numbers, etc. Pharming uses the same malware/spyware to redirect users from real websites to the fraudulent sites (typically DNS hijacking). By hijacking the trusted brands of well known banks, online retailers and credit card companies, phishers are able to convince recipients to respond to them.

PHREAKING

Telephone hacking, usually to obtain free calls, by generating illicit administrative commands to the network computer.

PIRATE SOFTWARE

Software that has been illegally copied.

PORT

The word part has three meanings:

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

PROGRAM

A prewritten sequence of computer commands that is designed to perform a specific task, such as word processing, accounting, inventory management, or accessing the Internet and World Wide Web.

PROXY SERVER

In an enterprise that uses the Internet, this is a server that acts as an intermediary between a workstation user and the Internet so that the enterprise can ensure security, administrative control, and caching service. A proxy server can improve performance by supplying frequently requested data, such as a popular web page, and can filter and discard requests that the owner does not consider appropriate, such as requests for unauthorised access to proprietary files.

PUBLIC DOMAIN SOFTWARE

Any programme that is not copyrighted.

PUK

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

Q

QUICKTIME

A multimedia development, storage, and playback technology developed by Apple Computers, Inc. Quicktime files combine audio, video, text and animation into a single file played with a Quicktime Player that either comes with a web browser or that can be downloaded from Apple. Quicktime files have one of the following extensions: qt, mov, and moov.

QUERY

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

R

RAM

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

RAS

Remote Access Service

REALAUDIO

A continuous streaming audio technology developed by Progressive Networks. Real Audio files are played with a RealAudio Player that either comes with a Web browser or can be downloaded from Apple. Real Audio files have one of the following extensions:ra,ram.

REMOVABLE MEDIA

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

REMOVABLE MEDIA CARDS

Small sized data storage media which are more commonly found in other digital devices such as cameras, PDAs (Personal Digital Assistants) and music players. They can also be used for the storage of normal data files, which can be accessed and written to by computers. There are a number of these including – Smartmedia Card, SD Expansion Card, Ultra Compact Flash, Compact Flash, Multimedia Card, Memory Stick. The cards are nonvolatile – they retain their data when power to their device is stopped – and they can be exchanged between devices.

ROUTER

A system that transfers data between two networks that use the same protocols. Search Engine A program used on the Internet that performs searches for keywords in files and documents found on the World Wide Web, newsgroups, Gopher menus, and FTP archives. Some search engines search only within a single Internet site. Others search across many sites, using such agents as spiders to gather lists of available files and documents and store these lists in databases that users can search by keyword. Examples include Alta Vista, Metacrawler, Yahoo, Dogpile, Lycos and Excite.

S

SAFE BOOT

Start a computer in a controlled manner so as not to change any stored data.

SCRIPT

Small program to automate simple repetitive tasks.

SECURE WIPE

Overwriting all material on a disk so as to destroy, as far as possible, all data stored upon it.

SECURITY FIREWALL

A system that isolates an organisation's computers from external access, as through the Internet. The firewall is intended to protect other machines at the site from potential tampering from the Net.

SERVER

Specific to the Web, a web server is the computer program running on a computer that serves requested HTML pages or files. A web client is the requesting program associated with the user. A web browser is a client that requests HTML files from web servers.

SERVICE PROVIDER (ISP)

A person, organisation or company that provides access to the Internet. In addition to Internet access, many

ISPs provide other services such as web hosting, Domain Name Service and other proprietary services.

SHAREWARE

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

SIM

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

SIGNATURE

A personal tag automatically appended to an email message.

SLACKSPACE

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

SMARTCARD

Plastic cards, typically with an electronic chip embedded, that contains electronic value tokens. Such value is disposable at both physical retail outlets and online shopping locations.

SNIFFER

A sniffer is a program that displays the contents of all packets passing through a particular network. Originally developed to test the performance of Internet connections by reading all of the information passing through a network. They can be used to trace private information such as credit card numbers and passwords.

SOCIAL ENGINEERING

Attacks basically by wit, guile or outright lies, aimed at conning a user to divulge passwords or other confidential information.

SOFTWARE

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

SOFTWARE CRACKING

The removal of copyright protection routines from software.

SOFTWARE PIRACY

The unauthorised copying and resale of software programs.

SPAM (OR SPAMMING)

The same article (or essentially the same article) posted an unacceptably high number of times to one or more newsgroups. Spam is also uninvited email sent to many people or unsolicited email advertising and can also be referred to as junk mail.

STEGANOGRAPHY

The art and science of communicating in a way that hides the existence of the communication.It is used to hide a file in side another. For example, child pornography image can be hidden inside another graphic, image file, audio file, or other file format.

STREAMING AUDIO/VIDEO

Listening or viewing media files from the 'Net in real time as opposed to saving the file and playing it later. See RealAudio

SURF OR SURFING

Exploring the Internet by moving from one Web site to another as the whim of the user dictates. Switch A typically a small, flat box with 4 to 8 Ethernet ports. These ports can connect to computers, cable or DSL modems, and other switches. A switch directs network communications between specific systems on the network as opposed to broadcasting information to all networked connections.

SYSTEM UNIT

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

T

TAPE

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

TCP/IP

Transmission Control Protocol/Internet Protocol is the basic communication language or protocol of the Internet.

TEMPORARY OR SWAP FILES

Many computers use operating systems and applications that store data temporarily on the hard drive. These files, which are generally hidden and inaccessible, may contain information that the investigator finds useful.

TELNET

A verb that means to log onto a distant computer and use it as a local user. The software utility allows persons to access and use a remote computer. In effect, the user's machine becomes a terminal for the other computer. Unlike FTP, Telnet does not allow users to transfer and save files to their own computers.

TERMINAL

A device that allows you to send commands to a computer somewhere else. At a minimum, this usually means a keyboard and a display screen and some simple circuitry.

TLD

Top Level Domain, name such as .com; .org; .net, etc.

TOOLS DISK

Hard disk upon which is stored software programs used for data examination and analysis

TROJAN HORSE

Often just referred to as a 'Trojan', this is a computer program that hides or disguises another program. The victim starts what they think is a safe program and instead willingly accepts something also designed to do harm to the system on which it runs.

U

UNALLOCATED SPACE

Area of the disk available for use, contains deleted files and other unused data

UNIX

A very popular operating system. Used mainly on larger multiuse systems.

UPLOAD

To transfer a copy of a file from a local computer to a remote computer.

UPS

Uninterruptable power–supply a power supply that can continue to provide a regulated supply to equipment even after a mains power failure.

URI

Uniform Resource Identifier, is an address for a resource available on the Internet. The first part of the URI is called the "Scheme", the most well known scheme is the http, but there are many others.

URL

A Uniform Resource Locator is the address of a file accessible on the Internet. An example of a URL is: http://www.usatoday.com/sports/sfront.htm, which describes a Web page to be accessed with an HTTP (Web browser) application that is located on a computer named www.usatoday.com. The specific file is in the directory named /sports and is named sfront.htm.

USB STORAGE DEVICES

Small storage devices accessed using a computer's USB ports, that allow the storage of large volumes of data files and which can be easily removed, transported – and concealed. They are about the size of a car key or highlighter pen, and can even be worn around the neck on a lanyard. They now come in many forms and may look like something entirely different such as a watch or a Swiss Army knife.

USENET

This is like a collection of bulletin boards that is separate from but parallel to the Internet that carries Newsgroups. There are an estimated 90,000 newsgroups on Usenet and each focuses on a single topic ranging from the bizarre to the mundane.

USER NAME (USER ID)

This is the name that identifies you and that you use to "sign on" with an Internet Service Provider. In addition to your registered "user name" you will also use a password.

USIM

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

V

VIDEO BACKER

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

VIRTUAL STORAGE

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

VIRUS

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

VPN

Virtual Private Network. This usually refers to a network in which some of the parts are connected using the public Internet, but the data sent across the Internet is encrypted, so the entire network is "virtually" private.

W

WAN

Wide Area Network. A network, usually constructed with serial lines, which covers a large geographical area.

WEB SERVER

A computer on the Internet or intranet that serves as a storage area for a Web page. When asked by a Web browser, the server sends the page to the browser.

WEBSITE

A related collection of HTML files that includes a beginning file called a home page.

WEBSITE SPOOF

Counterfeit site, which mimics an established one. When users submit information such as passwords and user names, the counterfeit site collects it.

WINDOWS

Operating system marketed by Microsoft. In use on desktop PCs, the system automatically loads into the computer's memory in the act of switching the computer on. MSDOS, Windows, Windows 2.0, Windows 95, Windows 98, Office XP, Windows XP, Windows NT, Windows Vista and Windows Server are registered trademarks of Microsoft Corporation.

WINDOWS 0T

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

WINZIP

The Windows version of a shareware program that lets you archive and compress files so that you can store or distribute them more efficiently.

WIRELESS NETWORK CARD

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

WORD PROCESSOR

Used for typing letters, reports and documents. Common Word Processing programs: Wordstar, Wordperfect and MSword.

WORKING FILES

Files created during examination for further examination or reference

WORM

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

Y

YAHOO! (WWW.YAHOO.COM)

A popular searchable database of information about and links to sites on the World Wide Web

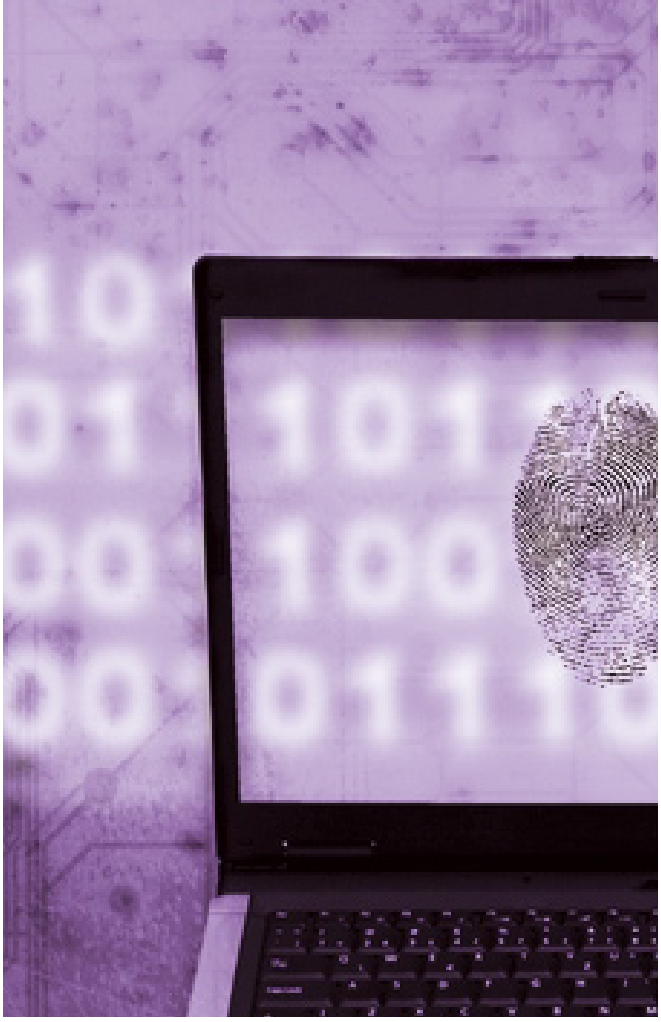
Z

ZIP DRIVE/DISK

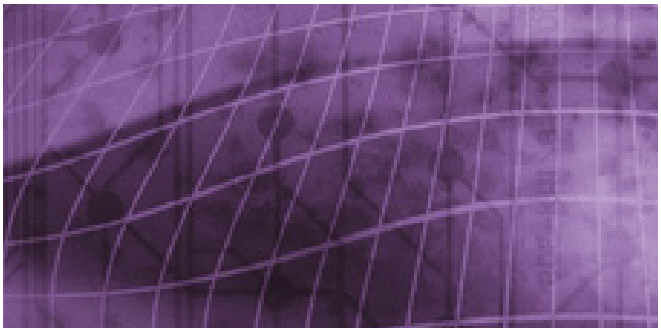
A 3.5 inch removable disk drive. The drive is bundled with software that can catalogue disks and lock files for security.

ZIP

A popular data compression format. Files that have been compressed with the ZIP format are called ZIP files and usually end with a .ZIP extension. There are other formats which form a similar function, including Rar, ALZip, Tar and Stuffit for the Mac OS.



APPENDIX J



APPENDIX J

Interview Guide For Suspects Involved In Computer Related Crime

BASIC INFORMATION ABOUT THE COMPUTER AND ITS USE

What sort of computer do you own?
(make, model, specification – what processor, size of hard drive, how much memory)

How long have you had it? Have you had it from new?

When did you buy it, where from, how much did you pay?

What operating system is on it?
(Ask what version e.g. Windows 95, 98, ME, 2000, XP (Home or Pro), Vista (Home Basic, Home Premium, Business, Ultimate), Linux (many versions), MacOs (system 1-7, OS 8,9,X)

What software is on it?

What software do you use regularly?

Who installed that software?

Where did you get the software from?
(purchased at shop, borrowed from friend, copied at work, downloaded and purchased online, downloaded and cracked)

Who has access to the computer?
(co-occupants and visitors to the address)
If anyone, plenty of detail. Names, times , dates, purpose, etc

Do these people have different user accounts?

How are these accounts accessed, usernames, passwords, who set this up?

If usernames - do the users stick to their own usernames or do they log on using others' details.

(If the suspect has more than one computer) - are your computers connected together in any way?
(direct cable, networked)

Who set up the connectivity?

Do you use a Wireless Router?

If so, who set it up?

How is the security configured?
(WEP, WPA)

What is the login name and password for the Router setup?

Have you configured the Router in any particular way?
(site blocking, firewall rules, special ports, DMZ, remote access)

DATA STORAGE

If you save some files or data on your computer where do you store it? (hard drive of the computer (may be more than one), what folders - My Documents, My Pictures, My Downloads, how do you organise what you save in folders, what folder names)

Do you use a USB drive (aka thumb drive, flash drive, memory stick)?
(If yes, is it password protected –details, do you run any programs from the USB drive – details and why)

Do you use any other external media?
(floppy disks, CD, zip disks, jazz drive, external hard drive, compact flash, smartmedia, USB drive, microdrive)

If stored on CD - what software do you use to copy files on to CD's? (a process often known as burning CD's)

Do you store any files remotely on the Internet or some other remote computer.

OTHER DEVICES CONNECTED TO YOUR COMPUTERS

Do you have any hardware attached to or used with the computer? (printer, scanner, webcam, digital camera, video editing equipment)

Who set up each item?

What do you use each item for and frequency?

Where do you normally store data recorded by any of this equipment? (CD, floppy, hard drive, remotely)

(If stored on the hard drive) - in what directories or folders do you store the files and what file names do you use.

CONNECTING TO THE INTERNET

Do you have Internet Access?

What do you use the Internet for?

How often do you use it?

How do you get connected to the Internet?
(dial-up access via modem, cable/broadband, TV access, satellite, mobile, access at work or via work, direct dial up)

Who is the provider? (AOL, BT Internet, Tiscali, Virgin, etc, may use more than one)

Do you pay for this and if so how? (Free, direct debit, credit card, one off payment)

What are you user names for logging on to the internet?

What are your passwords?
(Consider asking for written consent for HTCU to examine any online email accounts by logging on and using the user name and password)

EMAIL

Do you have e-mail accounts, if so what addresses?
(in the format somesortofname@company.domain, e.g. billysmith@hotmail.com, john@roman.co.uk, i_ate_your_cat@msn.com)

What software do you use to read your email?
(if web based email a web browser likely to be used – Internet Explorer or Firefox, otherwise Outlook, Outlook Express, Windows Mail, Eudora, Pegasus, Forte Agent, AOL, etc)

Does anyone else use the computer for email?
(If yes full details of person(s) and answers to above questions)

ONLINE CHAT

Do you use the Internet for chat or instant messaging?

What software do you use? (may be web based so again using a browser, or specific software or instant messenger client - MSN Messenger, ICQ, MIRC, etc)

What chat rooms do you use? (you will need to know who provides the service and the name of the chat room, MSN might be the service provider and the chat room might be "teen pop idols", or they might use a particular chat server like DALnet –irc.dal.net and join a channel like #fragglerock)

Do you engage in private chat, if so how do you arrange this? (may be using contacts or buddy list and they will be notified when the contact is online, or may meet in public group and then go private or create their own group)

What is your Passport or username and password for your instant messaging? (not uncommon for people to have several Passports)

If using an instant messenger, what is your display name and personal message (Do you change these, how often, why, what changes have you made)

What nicknames do you use in chat?

Have you ever used a webcam whilst chatting?
(If yes, explain details)

Have you exchanged files with other people whilst chatting? (Explain how this works, what happens when someone sends a file, do you get the option to reject the file, where do you store the files.)

BROWSING THE INTERNET/ SURFING THE WEB

What software do you use to web browse?
(Microsoft Internet Explorer and Mozilla Firefox are the main two but there are many others)

What sites do you visit regularly?

How do you find or choose sites to look at?
(search engines, junk mail ads, recommendations from chat, computer magazines, newspapers, porn mags)

Which search engines do you use? (lots ! – Google, Yahoo, MSN, AOL, Ask)

Do you save favourites? (links to sites that can be revisited at a later date)

If so how are these organised? (some people do not organise and have one long list others will break them down into numerous sub categories)

Do you save copies of you favourites or have a copy accessible online?

Do you use any toolbar add-ins or search tool assistants with your browser? (A lot of search engines have toolbars e.g. Google, MSN, Yahoo)

Does your browser have a popup blocker, or have you installed a popup blocker?

Have you created any web sites? (where is it hosted, what is the url, is it paid or free, what is the content, how long has it been up, what software was used to create the site, what software was used to upload the site to the web server)

Passwords and usernames? (for any sites that require user log on, or for any web sites that will require username and password to upload files to a web site)

APPENDIX J (cont.)

DOWNLOADING FILES

Do you save or download files or images from web sites?

Explain how do you do this ? (step by step and where are the files stored)

Have you accessed any password protected web sites for downloading files, - details?

Do you use newsgroups?

What for and which ones? (there are tens of thousands with all manner of interests, the names can be explicit like alt.binaries.underage.sex or more subtle like alt.fan. prettyboy, they can be used for discussion of topics of interest or for sharing images and other files, a major source of indecent images)

How do you access the newsgroups? (can be by using a web browser, if so what site is used (free or paid for?). Altenatively using which software – Outlook Express, Forte Free Agent, NewBinPro)

Do you use file sharing programs, if so which ones? (Morpheus, Kazaa, Bearshare, Grokster, Mirc File Server, these enable people to search for and share all manner of files, a major source for indecent images)

Passwords and usernames?

What files have you downloaded using such file sharing software?

What files have you made available on your computer for others to share? (what folders are shared)

Have you used any remote control or remote access software to enable you to control and access your computer from another location. (Using Windows Terminal Services, Remote Assistance or Remote Desktop, or software like Laplink or PC Anywhere, VNC, or web based service like GoToMyPc or LogMeIn)

COMPUTER SECURITY

(Be aware that previously it was common to have standalone software applications to deal separately with various aspects of computer security – Anti-Virus, Firewall, SpyWare checker, but now they often come in a"security centre" package.)

Is there an anti-virus program installed on the computer? (If yes, when was it installed? What program is it?)

Is it always active, does it do scheduled scans, on-access scans, and mail scans?

Do you keep the virus identity files updated, if so how often? (New viruses are created every day so the anti-virus software must have its files updated frequently to ensure that it can identify new viruses, most software will do this automatically)

Have you had a virus on your computer?

Details, when, what was it, how dealt with? Do you have any firewalls installed, either hardware or software? (Intended to prevent hacking into your computer from the Internet and stop malicious software on your computer providing open access to others via the Internet)

Details, hardware make & model, software name and version, when installed? (Zonealarm, McAfee, Norton, XP has built in firewall if switched on by user)

Do you have a Malware or Spyware checker? (Windows Defender, SpyBot, Ad-Aware)

Do you use any software to wipe delete files or shred files? (BCWipe, PGP and others can delete files and then write over the space they occupied so that the deleted files are unrecoverable)

Why do you use this software?

Do you defrag you hard drive?

(If yes) **What is the purpose of doing this?** (another method of limiting the likelihood of recovering deleted files)

Do you use any form of encryption?

(If yes) **What software do you use?** (BestCrypt, TrueCrypt, PGP, Private Folders, etc)

Why do you use encryption?

What passwords, are they stored somewhere? (may be written on paper or stored on a floppy or other media)

Do you use any software or methods to cover your tracks when using the Internet? (Lots on the market – Evidence Eliminator, Window Washer, System Cleaner, Winnow Cleaner)

If so explain what they are and why you do it.

STANDARD EXCUSES

• The images were sent to me unsolicited –

Who sent them

When were they sent

How often has this happened

What did you do about it

Did you complain to the person who sent them, the ISP, the police, anyone else.

What did you do to get rid of the images.

• It is part of a research project

How long have you been undertaking the project

What is the purpose of the project

Is it funded and if so by whom

Who else knows about it

What have you written up about it so far

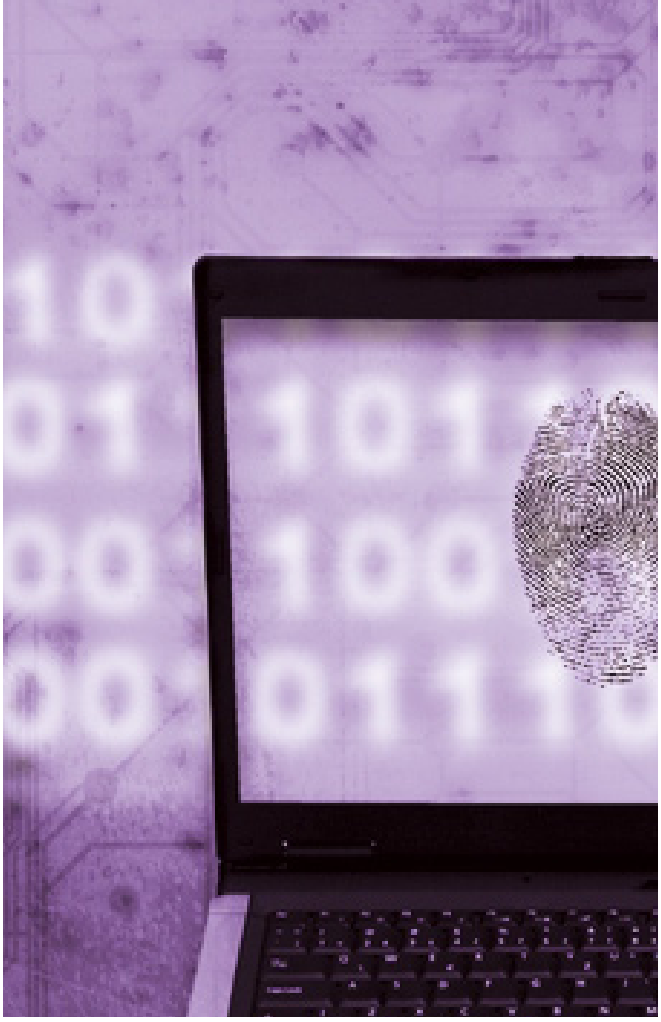
• I was gathering information to report to the police

Why

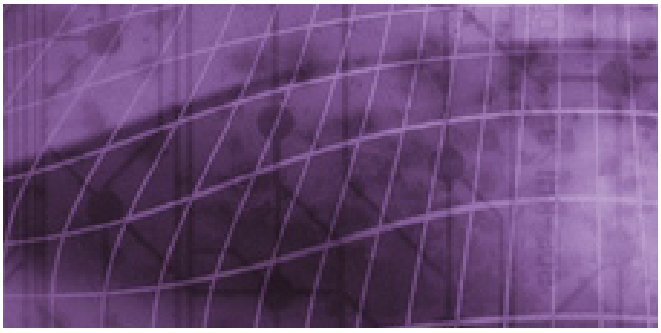
How long have you been gathering the information

Who have you told about it

Have you reported any of this to the police or other agency



APPENDIX K



APPENDIX K

Template for general advice regarding computer related incidents

The following is a copy of a Guide for Call Centre operators prepared by Dorset Police. This guide along with two hours of training for all call centre staff as to what an e-Crime is and what the HTCU was responsible for had a dramatic effect on the reduction of incorrectly directed telephone calls to the unit.

Some of the advice given here is pertinent to Dorset Police local policy and if used as a template would have to be amended to reflect that force's own policy on those issues.

General Advice	Always use good antivirus software and a software firewall. There are many good free software downloads on the Internet. A good site is www.getnetwise.org/tools NEVER save any Indecent Images of children on computers even to assist police to investigate.	
Chat Rooms	Be very wary of chat rooms and be extremely cautious about giving any personal details about name, address telephone number etc. Certain chat rooms are targeted by paedophiles who will pretend to be teenage girls or boys to gain confidence. Their user names, descriptions and language they use will often give the appearance of being teenagers. Never rely on screen details as they are rarely checked Good advice can be obtained at www.iwf.org.uk or http://uk.docs.yahoo.com/parents_guide	From an investigation point of view, chat rooms are extremely difficult to police and it is invariably impossible to trace offending users. Information can be forwarded to Sex Offender Investigation unit or HTCU

APPENDIX K (cont.)

Complaint	What they do	What to do	General Advice
I have found a website advertising pornography	The Internet hosting many thousands of website around the world, many containing images of pornography. Adult porn sites are mostly not illegal. Sites containing indecent images of children (appear under 16yrs) are illegal	The first issue is where the website is actually located in world. Many are outside UK and EU jurisdiction and there is little we can do to stop the site. The vast majority of pornographic websites that advertise child pornography are based in Russia or Eastern Europe. In these circumstances the web site address should be submitted to the Internet Watch Foundation www.iwf.org.uk Any emails received should be deleted immediately and the senders email can be blocked. (See also 'I've received junk email)	Under UK law, offences can be committed by deliberately visiting websites containing indecent images of children. Images MUST NOT under any circumstances be saved to a computer in the UK, even for police to investigate. Doing so is an offence. The website address only should be forward to the IWF
My computer has been hacked	Under certain circumstances and by competent person, it is possible to access files and data on someone's computer. This is however a rare occurrence and home users are rarely targeted.	Contact HTCU for further advice who can then contact victim	Always use a good software firewall and antivirus software and keep them updated preferably daily.
My telephone bill shows a number of premium rate numbers dialed from my computer which I know nothing about.	Many pornographic web sites produce 'dialers' which are small programs which run on a computer and dial premium rate numbers to access services. Many dialers work discretely without the user being aware, but DO NOT work when a user only has a broadband internet.	Record crime as Other Fraud and obtain all supporting documentation. Members of public can record complaint with Independent Committee for the Supervision for the Telephone Information Services website, at www.icstis.org.uk Website has a lot of information on current premium rate numbers under investigation.	Dialers can be downloaded to a computer in a number of ways. The most common is clicking on a link on a pornographic website. Others can arrive by clicking on link perhaps on software crack websites or occasionally virus install dialers. The best protection is antivirus and firewall software which will stop unauthorised outgoing calls.
I have received a email advertising a website containing indecent images of children	Email received inviting recipient to visit website containing child porn.	Nearly all website that send emails advertising child porn do not contain child porn. Most have either images of children which are not indecent (remember naked is not necessarily indecent) or adult (over 16yrs) dressed to look younger. If website is known to contain indecent images of children, then a member of public can report the site and follow instructions on www.iwf.org.uk. Such sites only need to be forwarded to the E-Crime Crime Unit in exception circumstances. i.e. site appears to be located in the UK	Delete emails and do not reply. Do not click on the website link as the site may then know your email is being read and continue to send more email. Set up filters on email software (eg Outlook Express) to filter content and key words. Block email addresses of persistent senders
I have my car advertised on the internet £2500. Someone wants to buy it, but send me a cheque for more than I am asking?	Another extremely common scam. The prospective buyer, normally from abroad is owed money by another. They want to send the cheque directly to you to save time. They send an international cheque for £6000 and ask you to return the balance minus £300 for you trouble, by Western Union to an agent somewhere. Their UK shipping agent will arrange to collect vehicle. You pay cheque into your account and after 5 days it clears and you send balance via Western Union. However, 2 weeks later your bank says cheque is fraudulent / stolen, and you loose the lot.	Record crime details as deception and obtain copies of all emails with full headers. Use the word 'internet' in the description for crime for ease of searching in future. Crime allocated to divisional offices to make enquiries.	Another example of something being too good to be true.Victims are often in financial problems and are responsive to a quick fix. If you want convincing that this is a scam look at the website www.419eater.com

Complaint	What they do	What to do	General Advice
I've paid for goods on ebay auctions but nothing has been sent to me. Also applies to QXL and other online auctions and retailers.	Fraudsters will advertise high value desirable goods such as latest mobile phone or flat screen TVs. They will normally start bidding at £1 to get many people interested and have perhaps 10 for sale. They may ask for payment by Western Union Money or Moneygram transfer anywhere in the world. (very difficult if not impossible to trace) They often use all sorts of social engineering tactics to deceive the buyer into a false sense of security, often over helpful in email responses. They may create websites or emails which appear to be linked to well known reputable companies such as newspapers, but in actual fact are untraceable by authorities.	Contact Auction company in first instance and try to make more enquiries about seller.Does telephone number or address exist? Save all correspondence and emails In auctions for multiple items (normal for fraudulent auctions), are there other persons who have not received goods. If fraud is alleged crime details to be recorded. Copy of all paperwork and correspondence required. Check eBay site at http://pages.bay.co.uk/help/community/index.html	Be very cautious about sending money to an 'unknown' person. Is there a realistic way of tracking the seller if things go wrong? Always use safe pay systems such as PAYPAL on auction sites where possible and be wary if they are not accepted by seller. Look at seller's feedback but do not rely on just a few entries. Don't loose sight of common sense for a bargain. If it seems too good to be true, it probably is.
My credit card has been unlawfully used on websites.	Credit card details have been used by an unauthorized person on the internet to obtain goods or services	Contact the credit card company and get as many details as possible. Record crime and obtain all supporting documentation.	Be wary about sending credit card details over the internet. Never enter credit card details into a website that does not use encrypted transmissions. Look for the Yellow Padlock or HTTPS in the address. Never email credit card numbers.
I have received a threatening email	Emails of threatening nature sent.	Are you sure the email is specifically directed at you? Keep all copies of emails and print out hard copies. Do not automatically assume that it is coming from where it appears to come from. May need to be investigated as a threatening letter the same as any other letter. Divisional OIC to be allocated who can liase with HTCU directly.	Offences are relating to harassment, email is only the method by which it is done. Sec 127 of Communications Act 2003 makes an offence for sending grossly offensive, obscene or persistently annoying email.
I have been sent a computer virus	Email has arrived from known or unknown person with virus attached. N.B There are many virus warnings that circulate by email. Many advise to delete certain programs or forward on to everyone. Virtually every one is a HOAX and should just be deleted. Check www.symantec.com/avcentre/hoax.html for latest list of hoaxes	This is most likely to be the work of a worm as opposed to a deliberate act by the sender.Many common virus spread themselves. Having infected the victim computer, they then try to spawn by automatically sending emails to everyone in the address book on the computer, or attach themselves to genuine emails. The person sending the virus probably does not know they have sent it.	Be very cautious of any files attached to emails and do not open unless you know the source. Install good antivirus software and keep definitions up to date. Advise sender by telephone if possible of virus.
I have received a email from Africa asking for bank details to transfer money. Often called '419 scam'	Lengthy email describing some problem in Nigeria and difficulties of transferring millions of dollars of legitimate currency out of the country. Require UK person with bank account to transfer money too for a percentage of the millions. Very common scam whereby further problems will occur, such as freight costs and customs officers need bribing. They will require a small amount of money (thousands) to actually post trunk full of cash. Needless to say, money never arrives	Never respond to emails and do not send any money. These emails arrive in UK email accounts in their millions each week. No offences are committed just for sending email. Receiver can printout full email with headers and send to FIB at HQ who collate and forward to NCIS. If victim has sent money, contact West African Organised Crime Unit on 020 7238 8012, but divisional officer needs to take statement.	Another example of something being too good to be true.Victims are often in financial problems and are responsive to a quick fix. If you want convincing that this is a scam look at the website www.419eater.com

APPENDIX K (cont.)

Complaint	What they do	What to do	General Advice
I have found a website advertising pornography	The Internet hosting many thousands of website around the world, many containing images of pornography. Adult porn sites are mostly not illegal. Sites containing indecent images of children (appear under 16yrs) are illegal	The first issue is where the website is actually located in world. Many are outside UK and EU jurisdiction and there is little we can do to stop the site. The vast majority of pornographic websites that advertise child pornography are based in Russia or Eastern Europe. In these circumstances the web site address should be submitted to the Internet Watch Foundation www.iwf.org.uk Any emails received should be deleted immediately and the senders email can be blocked. (See also 'I've received junk email)	Under UK law, offences can be committed by deliberately visiting websites containing indecent images of children. Images MUST NOT under any circumstances be saved to a computer in the UK, even for police to investigate. Doing so is an offence. The website address only should be forward to the IWF
My computer has been hacked	Under certain circumstances and by competent person, it is possible to access files and data on someone's computer. This is however a rare occurrence and home users are rarely targeted.	Contact HTCU for further advice who can then contact victim	Always use a good software firewall and antivirus software and keep them updated preferably daily.
My telephone bill shows a number of premium rate numbers dialed from my computer which I know nothing about.	Many pornographic web sites produce 'dialers' which are small programs which run on a computer and dial premium rate numbers to access services. Many dialers work discretely without the user being aware, but DO NOT work when a user only has a broadband internet.	Record crime as Other Fraud and obtain all supporting documentation. Members of public can record complaint with Independent Committee for the Supervision for the Telephone Information Services website, at www.icstis.org.uk Website has a lot of information on current premium rate numbers under investigation.	Dialers can be downloaded to a computer in a number of ways. The most common is clicking on a link on a pornographic website. Others can arrive by clicking on link perhaps on software crack websites or occasionally virus install dialers. The best protection is antivirus and firewall software which will stop unauthorised outgoing calls.
I have received a email advertising a website containing indecent images of children	Email received inviting recipient to visit website containing child porn.	Nearly all website that send emails advertising child porn do not contain child porn. Most have either images of children which are not indecent (remember naked is not necessarily indecent) or adult (over 16yrs) dressed to look younger. If website is known to contain indecent images of children, then a member of public can report the site and follow instructions on www.iwf.org.uk. Such sites only need to be forwarded to the E-Crime Crime Unit in exception circumstances. i.e. site appears to be located in the UK	Delete emails and do not reply. Do not click on the website link as the site may then know your email is being read and continue to send more email. Set up filters on email software (eg Outlook Express) to filter content and key words. Block email addresses of persistent senders
I have my car advertised on the internet £2500. Someone wants to buy it, but send me a cheque for more than I am asking?	Another extremely common scam. The prospective buyer, normally from abroad is owed money by another. They want to send the cheque directly to you to save time. They send an international cheque for £6000 and ask you to return the balance minus £300 for you trouble, by Western Union to an agent somewhere. Their UK shipping agent will arrange to collect vehicle. You pay cheque into your account and after 5 days it clears and you send balance via Western Union. However, 2 weeks later your bank says cheque is fraudulent / stolen, and you loose the lot.	Record crime details as deception and obtain copies of all emails with full headers. Use the word 'internet' in the description for crime for ease of searching in future. Crime allocated to divisional offices to make enquiries.	Problem caused by an anomaly with bank clearing system. A cleared cheque is not allows a guarantee you have the money. As with 419 scams, tracing the offender is extremely difficult if not impossible. All communications are likely to have been done through anonymous email account, and fake ID used to collect money from Western Union. Offender likely to be abroad.

Complaint	What they do	What to do	General Advice
I keep receiving emails advertising mortgages / credit / sex enhancers	This is commonly known as SPAM or Unsolicited Bulk Emails. Sending emails is an extremely inexpensive and efficient way to advertise, and only a tiny percentage or people need to respond and buy goods to cover costs. Therefore SPAM emails are sent out in millions everyday.	Do not respond to these emails and never click on the 'click here to unsubscribe' link. The site may unsubscribe you from their list but your email address then becomes more valuable as it is known to be read and they will sell lists of current email addresses. For further advice visit www.iwf.org.uk	Be careful who you give your email address to on line. Click the box requesting your email is not passed to other companies. Free web based email addresses are regularly hit with SPAM emails. Have two email accounts. One for family and friends which is rarely given out. The other can be used on websites and for surfing and that's where all the spam will end up.
I have indecent pictures of children on my computer.	Occasionally public call and state they have indecent images of children of their computers or computers under their control.	It is an offence to possess, produce or distribute indecent images of children. The HTCU ultimately examine computers for such images and can normally determine if possession was a deliberate or intended act.	All enquiries regarding Indecent images if children should be directed to (Local appropriate unit)
How do I find email headers	When an email is sent an audit trail is attached to the message which the user cannot normally see. This audit trail is useful in trying to trace the sender of an email.	The view email headers in Outlook Express, highlight the message in the inbox and right click on the mouse. Click on the view source option. The list displayed is the computers that the email has passed through from sender to recipient (under normal circumstances)	
What are IP addresses?	Every computer whilst connected to the internet must have a unique address (slightly difference if connected to an internal network such as the Dorset Police system). When a home user dials up to the internet, their computer is allocated a IP number in the form 102.54.123.10. With most dial up accounts, this number is kept on for that dialup session. When many financial transactions take place on the internet, the seller's computer may record the IP address of the user.	Under most circumstances, we can find out which internet provider owns a certain IP address and an enquiry can be made with the internet provider to establish who the user was. This is good in most circumstances but there are certain problems. Some ISP's do not check details of users (they may have lied) and Internet Cafes and Libraries rarely check or record users details.	
I've got a wireless network and someone has hacked me/ there's something wrong with the connection.	People 'war drive'/'war walk' searching for unsecured wireless access points. They are generally searching for free Internet access. This affects the victim because if their Internet access is metered they may end up paying extra in ISP costs. Also if the suspect is committing other criminal acts then IP traces will come back to the victim!	This is an offence under section 125, Communications Act 2003- dishonestly obtaining an electronic communications service.	If a suspect is identified all electronic computer equipment should be seized and HTCU contacted at the earliest opportunity. The victims' wireless router may also need to be examined to prove the offence. If there is no suspect then the victim should be advised to secure their wireless router. They can obtain advice from the manufacturer's website.

Acknowledgements

ACPO
E-Crime Working Group

Stephen Clarke
Metropolitan Police Service

Richard Conway
Surrey Police

Esther George
Crown Prosecution Service

Alan Phillips
7Safe Information Security

Sonny Hanspal
NPIA

Ray Massie
Hampshire Police

Harry Parsonage,
Nottinghamshire Police

Peter Salter
PSNI

Chris Simpson
NPIA

Tracey Stevens
Metropolitan Police Service

The contributors of the previous guide whose content formed a large part of this guide

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