Chapter 6 Investigating digital crime

Robin Bryant with Ian Kennedy

7.1 Introduction

In this chapter we examine how the investigation of digital crime fits within the wider context of criminal investigation, how it is modelled and the place of digital evidence within the criminal justice system. We conclude the chapter with a discussion on digital forensic standards and accreditation.

In this chapter we focus primarily on investigating digital crime in the UK and Europe but much will also be relevance and interest to those involved with, or studying, the policing of digital crime in other jurisdictions.

Since the 1990s there has been a move in many western countries (and particularly those that employ the adversarial form of justice) away from treating criminal investigation as primarily a ‘case building’ exercise against a suspect towards a more principled, but more nebulous, ‘seeking after the truth’.

This more modern approach demands, for example, that a criminal investigator develops lines of enquiry that point towards the innocence of a suspect as well as to those that suggest guilt, and that equal attention should be devoted to this. Indeed, by the mid 1990s statute this “new wave” in criminal investigation was manifested in the UK through section 23(1)(a) the CPIA that required that all “reasonable lines of enquiry” be pursued whether they point towards or away from the suspect.

Much of the legislation was enacted as a reaction to a number of miscarriages of justice where police withheld important information, ignored exonerating facts and simply constructed cases against individuals.

7.2 Intelligence and Intelligence-led policing
The use of intelligence, the collection and use made of evidence, and most pertinently of all, the investigative process itself are all of importance to the policing of digital crime in any jurisdiction. Intelligence, in the investigative context, may be considered a form of information, but with a particular quality—that is, it is information which has taken on meaning. Within a criminal investigation there are likely to be three distinguishable forms of incoming data (Bryant et al, 2012): information, intelligence and evidence (at the time of capture these will not necessarily be distinguishable one from the other). Information is normally from a source with no confidentiality constraints or protection requirements. It is overt information, such as a message posted on Twitter. Intelligence is more difficult to define but is generally considered to be information derived from many sources (some confidential) that has been recorded, graded, and evaluated. In short, intelligence is information with meaning. Whitaker (1999) defines intelligence as ‘the systematic and purposeful acquisition, sorting, retrieval, analysis interpretation and protection of information’. For example, we might have information derived from a social networking site which uses a particular form of criminal argot. If we link this information to a particular group of criminal associates then we begin to derive intelligence from the information. Evidence can be either of the above, but is generally material that can be admitted in a court of law and abides by the ‘rules of evidence’—that is to say, it is both admissible and carries probative weight (see below).

Intelligence is thus not the same as evidence. Some intelligence may become evidence or suggest the a means of obtaining evidence but some will not be used as evidence in any circumstances.

One way of categorising intelligence is to typify it as either ‘open’ (overt) or ‘closed’ (covert). One example of open intelligence that used for policing digital crime is so-called ‘Internet Open Source Intelligence’ (OSINT). The use of social network sites such as Facebook to adduce gang membership would be a tangible example of OSINT. Examples of covert forms of intelligence include police investigator use of ‘keyloggers’ to remotely monitor a suspect’s use of a PC keyboard to capture intelligence on the websites visited, passwords used to access sites and Darkweb and so on (see later). Despite the greater availability of open forms of intelligence, academic research has repeatedly shown that the police tend to underestimate the utility and importance of open forms of intelligence, and
overestimate that of closed (e.g. Dupont 2003). There are probably a number of reasons for this, including the psychologically compelling nature of intelligence that is appears to be ‘secret’ and difficult to come by, and the need to justify the often costly investment in time and people needed to capture covert forms of intelligence.

Intelligence-led policing (ILP) methodologies can be discerned in a number of approaches to investigating digital crime. For example, the use of ‘honey traps’ to collect intelligence on offenders (see below), police officers posing as casual users of social network sites and so on. Urbas (2010) describes the legal context (in Singapore and Australia) that allows police officers to assume a ‘false’ identity to identify individuals intent upon online child grooming for sexual purposes. He notes that for a police investigator “[a]dopting a false or fictitious identity, as is commonplace in covert policing generally, is particularly easy to do online” (p.412), and goes on to claim that the practice is frequently undertaken in many countries (ibid p. 414). However, in some countries the law entrapment issues might well complicate such operations at best, or at worst prohibit them altogether.

On a practical level, in some jurisdictions these intelligence-led covert operations will be mounted by a national law enforcement unit, rather than a regional police force. However, at least according to published sources, overall there would appear to have been only a limited and piecemeal application of ILP approaches to counterin digital crime, and particularly so in terms of targeting high volume online offenders. A further problem is that detection as a tactical operational approach to digital crime tends to be emphasised at the expense of disruption and dissuasion as alternatives. Hence, there would appear to be some scope for adopting a more intelligence-led approach to policing digital crime. For example, in 2010 it was estimated that a single botnet (Rostock) was responsible for almost 40% of all the world’s spam (CNET, 2010).

In the UK there are three levels of criminal intelligence with its ‘National Intelligence Model’:

- Level 1 (local neighbourhood level) in relation to local crime capable of being managed by local resources and antisocial behaviour; examples include ‘traditional’ volume crimes such as illegal drug supply but which have a digital crime component to them (such as the recovery of digitally-based evidence)
- Level 2 (force and regional level) in relation to force, inter-force and regional criminal activity, usually requiring additional resources; examples include ??

- Level 3 (national level) in relation to the most serious and organized crime, with a ‘high impact and high spread’ (Home Office, 2011, p. 15. Examples include organized crime groups operating online fraud. In the UK this is likely to involve the cybercrime unit of the National Crime Agency (the NCA).

However, reporting decisions regarding recorded crime might well influence local approaches to countering digital crime. UK legislation does not formally define digital crime as an offence type although the Home Office has recently introduced new recording classifications that include malware, hacking and DDoS attacks. At the force level a DDoS attack for example is likely to be reported in the UK as extortion demand only.

One approach to gathering intelligence in some countries is the use of ‘honeypots’. The term ‘honeypot’ is used to mean a computing system or resource on a computing system that has attractions for an offender to interact with, but with little attraction to non-offenders. As Spitzner explains, “A honeypot is an information system resource whose value lies in unauthorized or illicit use of that resource” (Spitzner, 2003). Different types of honeypot have different purposes: some are used to waste the time of the purported attacker and hence keep them away from resources of value, while others capture information about cyber-criminals tactics and how to protect against them. Honeypots can also be used to gather information to allow prosecution of intruders, though even after collecting data it is not always a straightforward matter to obtain convictions (Even, 2000). The typical honeypot sits inside an organisation’s firewall. The route for accessing it clearly indicates that it is for authorised users only, although many cyber criminals will not in fact pass through the ‘authorised entrance’ and hence may not see the ‘authorised users only’ message. Once inside the system, the activities of the cyber-criminal are monitored, and fake data is used to maintain the interest of the criminal to further capture information. Although most commentators do not believe that honeypot deployment is unlawful (for example, in terms of the term ‘entrapment’ - see Spitzner, 2010), other legal issues may apply, for example privacy and liability, though as yet it appears that
there has been no case law to clarify these. (By privacy we mean the issue of recording information about the users of the honeypot and whether this can be allowed under law.) One view relating to their use has been put forward by Salgado, senior counsel for the Department of Justice's computer crime unit (Poulsen, 2003). In his argument he does not argue honeypots are illegal, but rather that there are a number of legal issues to consider carefully when deploying them. The second issue of liability is whether any resultant effect on others of the use of the honeypot by a criminal could itself be open to a civil case for damages. For example a honeypot that becomes a resource for criminals to store and run pirated software might leave the owners of the honeypot open to prosecution by the original copyright holders for breach of copyright. These and other issues relating to the use of honeypots are discussed at length by Lakhani (Lakhani, 2003). The Honeynet project (The Honeynet Project, 2012) has developed a number of software projects that enable organisations to develop their own honeypots and have associated tools to enable information capture and analysis about usage.

7.3 Models of criminal investigation

In the UK an influential model of a synthesised general criminal investigation is the ACPO Core Investigative Doctrine first developed in 2003 by the National Centre for Policing Excellence. (This was subsumed within the National Police Improvement Agency, the NPIA, aspects of which are soon to become part of the new National Crime Agency). The doctrine ‘articulates the principles’ (McGory and Treacy, in Haberfeld et al., 2012, p. 124) underpinning criminal investigation in the UK.

The Doctrine covers six main areas, within the two broad themes of Underlying Principles and Knowledge (investigative knowledge, the legal framework and) and the Process of Investigation (the criminal investigation process, investigative decision-making, investigative strategies and management) (ACPO Centrex, 2005). Further, the doctrine proposes conceptualising investigation in terms of Activities, Decisions and Outcomes. An overview of the doctrine is given in the table below:
<table>
<thead>
<tr>
<th>Theme</th>
<th>Area</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Underlying Principles and Knowledge</td>
<td>Investigative knowledge</td>
<td>Characteristics of crime (victims, witnesses and offenders), national and force policies, principles of investigation</td>
<td>Modus operandi of offenders. Understanding the investigative process.</td>
</tr>
<tr>
<td></td>
<td>Legal framework</td>
<td>Evidence, the CJS, key legislation</td>
<td>Admissibility of types of evidence. Understanding the adversarial system of justice. Knowledge of PACE 1984, CPIA 1996 etc.</td>
</tr>
<tr>
<td></td>
<td>The criminal investigation process</td>
<td>The generation of material, the stages of investigation, a standard model for investigation (see 7.4 below)</td>
<td>Material gathered from locations. The ‘Golden Hour’ of forensic opportunity. Gathering intelligence. Reactive and proactive forms of investigation.</td>
</tr>
<tr>
<td></td>
<td>Investigative decision-making</td>
<td>How decisions are made, the ‘investigative mindset’, investigative and evidential evaluation, the evaluation process,</td>
<td>Verification bias and availability error. Planning, preparation, examination, recording and</td>
</tr>
</tbody>
</table>
7.4 Criminal investigation in practice

The notion of a ‘criminal investigation’ superficially suggests a process of police enquiry into a crime. However, an intrinsic part of all criminal investigation is also to establish whether there is a case to be answered. In the UK for example, a criminal investigation is legally and formally defined by section 22 of the Criminal Procedure and Investigations Act 1996) as ‘[a]n investigation conducted by police officers with a view to it being ascertained whether a person should be charged with an offence, or whether a person charged with an offence is guilty of it’.

The CPIA Codes of Practice also explain
that this will include investigations begun in the belief that a crime is about to be committed as well as those reported as already having happened.

Criminal investigation can be either reactive (based for example, on the report of a suspected crime, or attendance by a police officer in uniform at an incident), or proactive, that is consequent to the acquisition of intelligence or following a covert police operation (see intelligence above).

In the UK the model of criminal investigation is currently based on the 2005 Core Investigative Doctrine (see above) which consists of eight possible stages: instigation, initial investigation, investigative evaluation, suspect management, evidence assessment, charge, case management, and finally 'court' (ACPO Centrex, 2005). The typical activities, decisions and outcomes at each stage are illustrated in the table below:

<table>
<thead>
<tr>
<th>Phase</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instigation (activity)</td>
<td>Instigation of an investigation may occur reactively; e.g. reports from the public, re-opening of an old case in the light of more information or proactively; e.g. through an intelligence source</td>
</tr>
</tbody>
</table>
| Initial investigation (activity) | In the case of an emergency call this will include the 'first officer on the scene'.  
The crime scene is managed (if applicable) – e.g. the ‘golden hour’ of forensic opportunity.  
Other ‘fast track’ actions may occur e.g. quickly collecting CCTV footage.  
‘Material’ begins to be collected e.g. from places (including scenes of crime), witnesses, victims, suspects, databases (including intelligence databases), mobile phone records etc.  
Specifically, Initial interviews with witnesses, victims and suspects (if identified) will be conducted. An investigating officer may be appointed, a risk assessment of |
<table>
<thead>
<tr>
<th>the case conducted, information recorded. The investigation may be handed over to a more experienced officer.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Investigative evaluation (decisions) Material is evaluated for evidential relevance, reliability and admissibility. Decisions include further investigation is required or no further investigation warranted (although intelligence might still be collected and disseminated). In the case of further investigation a ‘gap analysis’ is conducted.</td>
</tr>
<tr>
<td>Suspect management (activity) A number of investigative strategies may be employed e.g. to test the veracity of a suspect’s claims</td>
</tr>
<tr>
<td>Evidence evaluation (decisions) Material is further evaluated for evidential relevance, reliability and admissibility. Decisions include ‘charge’ as well as ‘no charge’ or another form of resolving the enquiry short of a court appearance by the suspect. On many occasions will lead to further investigation before a final decision is made.</td>
</tr>
<tr>
<td>Charge (outcome) Is there sufficient admissible evidence to charge the suspect?</td>
</tr>
<tr>
<td>Case management (activity) Any new relevant lines of enquiry to be followed up, file preparation, forensic reports to be checked, exhibits, liaison with the defence (e.g. disclosure process).</td>
</tr>
<tr>
<td>‘Court’ In some cases the final outcome e.g. suspect attends a Magistrates’ Court.</td>
</tr>
</tbody>
</table>

Note that only a proportion of criminal investigations are likely to result in a court appearance by a suspect. In some cases a suspect will accept some kind of process short of prosecution (such as a
formal caution), in others the investigation will be dropped (perhaps because there is no case to answer), in others the prosecuting authorities (such as the CPS in the UK) might decide not to go ahead with a prosecution, perhaps because of insufficient evidence. The sequence of activities in a criminal investigation frequently overlap and are not necessarily distinct.

The details of practice of criminal investigation will also vary, not only from country to country but also between different law enforcement agencies within the same country. Often some form of overarching process will be adopted, sometimes expressed in a way that enables an investigator to focus on the ‘unknowns’ of an investigation, establish hypotheses and test them. For example, in the UK a frequent way of doing this is for the investigator to consider the ‘five W’s and the H’ of the investigation: Who? What? When? Where? Why? and How?

7.5 Models of digital crime investigation

Given the ubiquitous availability of digital devices it is inevitable that more and more criminal investigations, and not just those involving cybercrime, will involve also forms of digital forensic investigation. We discuss in chapter 5 the organisational structures that have been established for digital investigation. Here we examine the models for the process itself. As with criminal investigation generally, there are a number of reasons why it is important to study the models of digital investigation employed by law enforcement agencies and others. However, perhaps the most important reason was given by Ó Ciardhuáin when he argued that “A good model of cybercrime investigations is important, because it provides an abstract reference framework, independent of any particular technology or organisational environment, for the discussion of techniques and technology for supporting the work of investigators” (Ó Ciardhuáin, 2004, P. ?)

At the outset it is worth noting that as Yusoff et al. point out, that the reader might encounter various terms used to describe the process of digital investigation “model, procedure, process, phase, tasks, etc” (Yusoff et al 2011, p.18). It is also unlikely that a universal model of digital criminal
Investigation could be formulated, because the definition of ‘digital crime’, and therefore what qualifies as such, is diverse, and specific technical challenges are likely to arise in different cases. In practice the model adopted for any one case might have to reflect the particular form of digital criminal investigation undertaken and the specific circumstances of the case. Finally, it is worth noting the distinction between models of digital criminal investigation and digital forensic investigation guidelines (such as the ACPO guidelines): the latter are more concerned with the specific requirements around the collection and analysis of digital evidence.

Models of digital crime investigation, although subscribing to the basic principles of the more generalised models of criminal investigations described above, have some unique features and are not simply subsets of criminal investigation (see for example Casey, 2003 and Hutton’s 2009 ‘Cybercrime Investigation Framework’). Etoundi and Moyo (2012) discern three possible categories for models of digital investigation: proactive, active and reactive processes. But they also add that ‘[a]lthough several models exist within the digital forensic industries, they are essentially limited to reactive digital forensics’ (Etoundi and Moyo, 2012, p. 14).

An early model was outlined in 1984 by Pollitt who described a ‘Computer Forensic Investigation Process’ as consisting of acquisition (electronic evidence captured in a legally acceptable manner), identification (human recognition of the meaning of data), evaluation (deciding whether the identified data is relevant to the investigation) and admission (presentation to the criminal justice system) (Pollitt, 1984). In 2001, the first Digital Forensics Research Workshop (Palmer, 2001) agreed a linear process model (known as the ‘DFRWS’ model) with seven stages: ‘identification’ e.g. audit analysis), ‘preservation’ (e.g. chain of custody), ‘collection’ (e.g. recovery of data), ‘examination’ and ‘analysis’ (although described as separate stages these two aspects often converge, examples include the recovery of hidden data), ‘Presentation’ (e.g. documentation) and ‘Decision’. In 2002 Reith, Carr and Gunsch (2002) outlined a model which, although based in part on the DFRWS model, was somewhat more detailed and comprehensive: ‘identification’, ‘preparation’, ‘approach strategy’ (largely a reference to the need to make preparations before a seizure of digital forensic evidence),
In 2004 (but building on earlier work) Eoghan Casey set out a four stage model of digital evidence investigation: recognition, preservation, collection, and documentation, classification, comparison, and individualization and finally, reconstruction. (Casey, 2004).

One of the most theoretically-grounded models was proposed by Ó Ciardhuáin in 2004. His ‘extended model of cybercrime investigations’ was one of the first to move from a largely forensically-based model to one that conceptualised digital crime investigation in its own right. A novel feature was the emphasis on information-flow as an important aspect of digital criminal investigations. There are 13 activities in the model, summarised in the table below:

<table>
<thead>
<tr>
<th>Activity</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Awareness</td>
<td>Recognition that an investigation is needed e.g. validated report of hacking</td>
</tr>
<tr>
<td>Authorisation</td>
<td>For example, through the issuing of a warrant</td>
</tr>
<tr>
<td>Planning</td>
<td>Using information collected by the investigator</td>
</tr>
<tr>
<td>Notification</td>
<td>Informing the subject and other interested parties that an investigation is taking place</td>
</tr>
<tr>
<td>Search for and identify evidence</td>
<td>e.g. locating the PC used by a suspect</td>
</tr>
<tr>
<td>Collection of evidence</td>
<td>Potential evidence is taken possession of …</td>
</tr>
<tr>
<td>Transport of evidence</td>
<td>… and then transported to an appropriate location</td>
</tr>
<tr>
<td>Storage of evidence</td>
<td>Storage methods should reduce the risk of cross-contamination</td>
</tr>
<tr>
<td>Examination of evidence</td>
<td>The use of specialist techniques e.g. recovery of deleted data</td>
</tr>
<tr>
<td>Hypothesis</td>
<td>A tested formulation of what may of occurred</td>
</tr>
<tr>
<td>Presentation of hypothesis</td>
<td>e.g. presented to a jury</td>
</tr>
<tr>
<td>Proof/Defence of hypothesis</td>
<td>Contrary hypotheses will also be considered</td>
</tr>
</tbody>
</table>
Dissemination of information

The information may influence investigations in the future

There are a number of distinct advantages of the Œ Ciardhuáin model, particularly its use of hypothesis testing to formalise the reasoning used in a digital criminal investigation, and that it has been ‘field-tested’ and evaluated in practice.

Further models have since been proposed, for example, the ‘Enhanced Digital Investigation Process Model’ (EDIP) by Carrier & Spafford (2004), the ‘Computer Forensics Field Triage Process Model’ (CFFTPM) (2006) and in 2011 Ademu and Imafidon’s ‘systematic digital forensic investigation model’ (SRDHM). In the same year Yusoff et al proposed a ‘Generic Computer Forensic Investigation Model (GCFIM)’ which was a synthesis of models he established through an inductive examining of all extant and previous models. In many cases the models described above were built upon earlier attempts and therefore became more detailed and involved.

A particularly active researcher of models of digital criminal investigation is Hunton (2009, 2010) who has proposed a ‘Cybercrime Execution Stack’ and latterly set out the ‘Stages of Cybercrime Investigation’ followed by a ‘Cybercrime Investigation Framework’. His Framework is based in part on the ACPO Core Investigative Doctrine (see above) but also incorporates some of his earlier work. It involves Investigation, Initiation, Modelling, Assessment, Impact/Risk Planning, Tools, Actions and Outcome. However, note that Hunton intends this to be a somewhat more cyclic process than a mere list suggests.

7.6 Digital criminal investigation in practice

Note that in the sections that follow references to the law are in the context of a digital criminal investigation: civil matters can be very different and are not covered here.

Despite the advent of intelligence-led policing (see above) most digital criminal investigations in most parts of the world will begin in a traditional reactive manner: that is the report of a crime or suspected crime, involving data as either the target and/or as part of the potential evidence.
As we discussed earlier, a criminal investigation in the UK (and most other parts of the world), when seen through to a prosecution, more or less follows a set of activities in seven phases from instigation to Court. In general terms a digital crime investigation will be part of a more general criminal investigation, running alongside it and according to the nature of the offences being investigated, occupy a greater or larger proportion of the overall investigation. So, for example, a homicide enquiry might involve the recovery of deleted SMS messages from a set of mobile phones and the intelligence gathered could then influence the interview strategy of the underlying criminal investigation.

The digital criminal investigation will be used to test hypotheses both on the level of the digital information itself and also at the level of the criminal investigation that it might feature within. A digital investigation can either support a hypothesis (through inculpatory evidence) or refute it through exculpatory evidence: the terms ‘proof’ and ‘disproof’ are not normally used at this stage.

A digital criminal investigation may instigated reactively through reports from the public or public agencies, as a result of other investigations or proactively, for example based on open or closed investigation. However, in common with most crime, many online crimes will not be reported to the police (and hence not recorded in police data). This is particularly the case with online fraud, which is often reported only to the banks and companies concerned. There is also a problem that in the UK at least, local crime reporting and recording still tends follows geography, with the general ‘rule’ that crime is recorded where it took place – in the case of online auction house fraud this poses obvious dilemmas. In response to these problems, by April 2013 all police forces in England and Wales are expected to use ‘Action Fraud’, for reporting allegations of ‘fraud and cybercrime’ (in this case defined as financially motivated internet crime). This centralised system is run by the National Fraud Authority working in partnership with the National Fraud Intelligence Bureau. Members of the public can also report suspected online crime to Action Fraud.

The procedures at a digital crime scene are described in chapter 7 that follows. In many cases the first response to a serious crime that involves a digital dimension will be a police officer or employee, the
so-called ‘First Officer on the Scene’. In the UK ss 19 and 20 of the PACE Act 1984 provide the legal basis for the seizure of data. There are two issues here: first the need to be aware of where digital evidence might reside. Most police officers or police staff will be aware of the importance of a suspect’s mobile(s) and computing equipment but may not appreciate that digital evidence can also be potentially located in games consoles, digital cameras and indeed any other device that can store data. (The ACPO e-crime strategy has more to say on this issue). Secondly, there is the need to eliminate or at least minimise the risk of digital contamination. For this reason, it is considered important in many jurisdictions for the first officer to keep careful notes of any actions that were taken (e.g. turning off a PC as it appeared to be running a destructive routine). Many countries have detailed guidelines on the processes to be followed: for example, in the UK there are the ACPO Good Practice etc guidelines and in the US the Department of Justice’s ‘Forensic Examination of Digital Evidence: A Guide for Law Enforcement’. If the seizure of a suspect’s PC is planned, a police force Digital Forensics Unit (or Computer Crime Unit or similar) will be contacted by the investigating team in advance for advice and, if needed, attendance at the scene. However, in at least some cases it is likely to be a generalist uniformed police officer who will physically size and package digital devices, whilst probably having some basic initial training, will not be a specialist in digital crime. In the UK a police constable also has the legal power to seize and examine a mobile phone. However, they normally only do so to establish the IMEI of the mobile and check this against the National Mobile Property Register (NMPR) rather than for purposes of digital forensic analysis.

Regardless of who may be seizing digital evidence, there remains the question of what should be seized. For example, when searching a suspect’s home address there are likely to be many sources of digital data, and not only the more obvious mobile phones, digital cameras, laptops and PCs, but also tablet devices, media servers, games consoles and satellite receivers. The temptation must be to seize everything that might possibly contain data, and copy all live data in situ but this has obvious problems not only in terms of practicality but also in terms of proportionality and respect for privacy and human rights. As ACPO argue, ‘Digital devices and media should not be seized just because it is there’ (ACPO, 2012, p. 30). The rule adopted is one of a reasonable expectation that the digital device
The process of selecting which devices to be seized, or live data to be copied, is often known as ‘triage’ (the term is also used when referring to choices made when analysing large amounts of data). The concept of triage originated in medical practice and refers to the process of sorting injured people into groups according to both the need for, a likely benefit from, treatment. It is not simply ‘first come, first served’. In terms of a digital crime scene the considerations for prioritisation are likely to include the devices most likely to contain relevant information and the volatility of the data. However, as Professor Peter Sommer notes, in the UK at least ‘Insufficient thought has been given to how [triage] is executed – and by whom’ (Sommer, 2012, p. 97).

In the UK there are particular issues concerning the ‘disclosure’ of unused digital material that has been gathered during an investigation (that is material that will not be used by the prosecution in court as evidence against the defendant or defendants). In essence the Criminal Procedure and Investigations Act 1996 (CPIA) requires the recording, retention, revelation and disclosure (to the defence) of unused material obtained during a criminal investigation, and this includes electronic (digital) material. The CPIA Code of Practice also makes it the duty of the investigator to pursue all reasonable lines of enquiry. Both of these strictures have particular implications in the context of digital material which is often voluminous by its very nature, and analysed in ways where large amounts of data are ‘unused’ (for example, a 2Tb hard drive might only contain a few Mb of data that are determined to be relevant to the case). In practical terms the responsibility for the digital criminal investigator is to ensure that all unused material is made known to the prosecutor for decisions to be made concerning disclosure.

The forensic analysis of digital evidence is described later in chapter 8. During their basic initial training a police constable in the UK will be given some information on digital forensics, such as the potential evidence that might be recovered from a website, examples of mobile phone traffic data, service use and subscriber information. A generalist criminal investigator in the UK will also be able and permitted to undertake some of the more common digital forensic techniques such as identifying and retrieving an email header, printing off a screen-shot of a PC, checking e-Bay for suspicious
activity, and how to access electronic open sources of intelligence (see above) from social network sites.

However, in many countries that the expertise required to undertake an initial digital crime investigation lies outside of the conventional law enforcement agencies and resides instead in industry, the private sector and the security and intelligence agencies. In the UK for example, the government has responded by creating a new form of ‘Special Constable’ (a volunteer part-time police officer) based with the new National Cyber Crime Unit within the National Crime Agency with specific responsibility to assist in the investigation of digital crime. From time to time there are calls to create a new specialist post of ‘Digital Scene of Crimes Officer’.

Irrespective of the agency or role of the person carrying out the forensic analysis there is normally a requirement to communicate the on-going and final results of any examinations and analysis carried out. This is normally given verbally by the analyst on a regular basis throughout the enquiry although it is often considered good practice for the analysts to back up the verbal report soon after with a written report (perhaps in an email) and to keep their own notes of the verbal report. In the UK this practice is considered particularly important given the requirements of ‘disclosure’. Most jurisdictions require some form of formal written statement from the analysts at the conclusion of the enquiry, which normally includes a discussion of the reliability, validity and confidence in the conclusions, with ‘opinion’ clearly identified as such. A key stage of an enquiry will be the charging of the suspect or a decision not to continue with a prosecution. Where charges are laid specific cybercrime legislation is likely to be cited, such as the UK’s Computer Misuse Act (1990) in the case of allegations of hacking or virus attacks. Note however, that in many jurisdictions a crime committed online is likely to be prosecuted under ‘terrestrial’ legislation (such as fraud or communications legislation) rather than specific digital crime legislation.

In the case of a prosecution a digital forensic analyst may be required to give evidence in court. The analyst is likely to be asked to give details concerning their qualifications and experience of the analyst, and in the UK will be mindful of the important distinction between ‘opinion’ and ‘facts’ when
giving their evidence. However, there are a number of issues surrounding expert witnesses and these are discussed later.

Cooperation with ISPs and ICANN

In the course of a digital criminal investigation there are a number of circumstances when cooperation with an external body such as Internet Service Provider (ISP) might be required. ISPs are normally private companies (such as Comcast in the US and Virgin Media in the UK) which provide individuals and companies with the means to gain access to the internet. So, for example, a person sowing malware will use an ISP to attempt to upload and distribute it. No doubt many such perpetrators will take steps to try to hide their identity, through for example using public wifi or ‘anonymising’ web-services. However, in some cases naive individuals have used their usual ‘home’ ISP to facilitate and enact the crime, and the ISP would be able to provide evidence of this. Indeed, in all digital crime cases an ISP might hold information that could potentially be of great importance to an investigation. A suspect could request information themselves from an ISP to pass to an investigator but this cooperation is unlikely. In the UK authorisation is required (usually in the form of a court order) to require an ISP to hand over data, such as weblogs, to an investigator. Such an authorisation is provided under the Regulation of Investigatory Powers Act 2000 (RIPA). The ISP might also be able to provide evidence or intelligence from emails that a suspect or others may have sent or received, although these types of evidence can also be recovered from PCs and other similar devices. RIPA will also apply for data concerning traffic (eg email recipients and senders and the amount of data transferred) authorisation is provided under Chapter II, but for actual content a warrant signed by the Home Secretary is required. In many other countries there are similar legal requirements, for example in the US the Communications Assistance for Law Enforcement Act (CALEA) provides for the monitoring of broadband traffic through ISPs.

A number of digital crimes (such as the distribution of malware or the provision of illegal online services) will exploit the relative ease of creating and changing domain names (the registrars of domain names generally make little attempt to validate the details of customer registrations). Law
enforcement Agencies in a number of countries have been lobbying ICANN (the Internet Corporation for Assigned Names and Numbers) to improve the validity of domain name information (e.g. the name and address of registrant) which in turn will improve the reliability of WHOIS searches, a valuable technique for digital criminal investigation.

**Use of covert techniques**

A digital crime investigator will sometimes need to employ covert investigatory techniques, for example to identify suspects who are grooming for sexual purposes or participating in online organised criminal activity. An investigator might need to employ a ‘false’ identity for other aspects of an investigation; otherwise simply accessing a website could alert its controller that a police investigation is underway. However, even if the information gained is to be used as intelligence rather than as evidence (see above), the requirements of RIPA and PACE (the Police and Criminal Evidence Act 1984) still need to be met.

The police will also use Social Network Services (SNSs, such as Facebook) as part of an investigation, sometimes by first creating a false profile (e.g. as a child) and then collecting information when contacted by those apparently intent on sexual grooming. However, there may be legal problems associated with a police officer creating a false identity on an SNS in order to gather intelligence or evidence. As O'Floinn and Ormerod note (2011, p. 4): “In conclusion, in all but the most passive activities, such as monitoring public profiles, there is a risk that SNS policing using fake profiles might be criminal”. Their argument is that an SNS is a ‘private telecommunication system’ under section 2(1) of RIPA 2000 and that monitoring of communications by investigating officers on a SNS could be an interception offence under section 1(2) of RIPA 2000.

Covert monitoring of a suspect’s PC via a network or the internet is sometimes carried out by investigators. Indeed, software for this very purpose is available to law enforcement authorities: examples include Encase’s Field Intelligence software which allows remote forensic imaging of a PC’s hard drive, recovery of deleted data and even the capture of volatile data from running processes,
(Encase 2012. However, as with many covert techniques, the investigator needs to be mindful of the legal context in order to avoid falling foul of the law: in this case a warrant under section 26(3) of RIPA 2000 is required (which in turn refers to section 32(3) which sets out the tests of necessity and proportionality). There are potential problems; the covert monitoring being identified by the user of the target machine and hence alerting them (for example, being identified by a virus checker), and the reliability of any evidence gained through these techniques could be challenged because covert entry on a suspect’s PC will give rise to a change in data in the target machine. Software is also available to allow law enforcement authorities to monitor traffic on a suspect’s machine to capture usernames and passwords (this is particularly useful where a suspect is using encryption – see later) but RIPA 2000 also applies to this kind of activity.

Another possible covert tactic for the police digital crime investigator is the use of keyloggers to gather intelligence and evidence. There are two possible forms of keylogger: physically installed hardware on the target machine and software covertly run on a target machine, either directly or remotely via the internet. Using covertly installed hardware keyloggers would appear to fall under Part 3 of the Police Act 1997 but again investigators need to be mindful of the requirements of RIPA 2000 (in this case section 1).

**Dealing with encrypted data**

Investigators may encounter encrypted data as part of an investigation. There could be ‘innocent’ reasons for why the data has been encrypted: for example, it might be company policy. However, some suspects may have taken deliberate and careful steps to encrypt data which would incriminate them, or to inhibit a police investigation. Some countries have a national resource to support investigators in dealing with encrypted data: for example the National Technical Assistance Centre (NTAC) in the UK. It is also worth noting that the legislation relating to investigations where suspects have used encryption often employs a specific language. For example, in the UK, RIPA 2000 uses the terms 'Protected Information', 'Data key' and 'Intelligible form'
An early step in de-crypting a suspect’s encrypted material is to attempt to identify the form of encryption used (e.g. symmetric or asymmetric) and the software employed e.g. Kruptos. As described in chapter 10, encryption is a potentially very difficult problem to solve, and ‘industrial – strength’ encryption is available to anybody via the internet. A password will usually be required to decrypt the data and it might be possible to obtain it by:

1. Asking the suspect for the password.
2. Exploiting inherent weakness in the method of encryption used. This is unlikely but some encryption software do have ‘back door’ entry points.
3. Conducting a physical search for the password e.g. a ‘post it’ note on the reverse of the keyboard, an entry in a mobile phone.
4. Conducting an electronic search of the suspect’s PC and other devices for a plaintext version (or fragment) of the password.
5. A ‘dictionary attack’, in both English and the language of the suspect (for example, Polish in the case of a Polish-speaking suspect), where words from a dictionary (together with numbers and other symbols are checked against the encryption software.
6. A ‘frequency attack’ (but only in the case of some particular forms of encryption), which exploits the fact that letters of the alphabet occur with variable frequencies.

In the UK, section 50(3)(c) of RIPA 2000 provides the authorities with a power ‘to require disclosure of the means to access protected information or the means to put it into intelligible form’ with failure to do so an offence. There have been a number of successful prosecutions under this legislation but some of these are likely to have involved offenders who have weighed up the likelihood of prosecution under RIPA against the potentially more serious repercussions of facilitating access to incriminating material (for example, child sexual abuse imagery).

The CJS and Digital Evidence

In this section we examine how investigation of digital criminal sits within the Criminal Justice System (CJS), and in particular, the issues surrounding digital evidence. Our focus here is mainly on
the criminal law rather than the civil law, and on the UK in particular. However, much of what follows will also apply in other jurisdictions. A digital crime investigation is situated within the framework for criminal investigation in general, and hence a broad understanding of the Criminal Justice System (the CJS), the forms and legal standing of digital evidence would seem appropriate. Digital evidence is certainly of growing importance, as we witness the ‘emergence of digital evidence not only featuring in computer specific criminal cases such as hacking and malware attacks, but becoming a more common element in almost any type of crime’ (Grobler, 2012, p.1).

The CJS encompasses a number of procedures and institutions, for example the law, law enforcement, and dealing with transgressions of the law in a particular country. So for example, the criminal justice system in England and Wales includes the police, the courts of law, the National Offenders Management Service (NOMS), the Youth Justice Board, and the Crown Prosecution Service (CPS).

In order to determine the guilt or otherwise of a defendant a Court will consider the evidence. During many criminal investigations, particularly complex ones, a large amount of material will be generated by the crime itself (some of which will only be known to the offender), a subset of which will be gathered by the police (for example, a witness statement) but only a proportion of this will be admissible as evidence in any prosecution (ACPO/Centrex 2005, p. 45). In the UK evidence is usually regarded as consisting of four kinds: oral (also called verbal or spoken); real (an article, object, or thing with material existence; that is, it can be produced in court); documentary (a document, paper, or record, which can be electronic); or hearsay. As far as we can tell (research is by necessity limited) the Courts (and juries in particular) are most comfortable with oral evidence that is given by a person describing their direct experience of what they saw, heard, felt and so on, and with real evidence such as object, like a knife (used to harm someone). Carrier and Spafford (2006) defined digital evidence as digital data that supports or refutes a hypothesis about digital events or the state of digital data. However, digital data as evidence is unusual because it is virtual, not actual and its meaning has to be inferred. (Whereas the device used to produce the digital evidence is real, such as a physical PC, the data produced is not). Digital evidence has to be represented at some more abstract level than the bits and bytes of its actuality. For example, a prosecutor could simply print out a long list of the 1s and 0s
of the code that related to a particular deleted document on a PC, but this would ‘prove’ nothing.

Hence the decision instead is always to show an interpretation in the form of file structures, images within folders and so on and to present this instead documentary evidence instead of the ‘real’ data.

However, there are few if any, uniform standards in place for the interpretation and presentation of this digital data, but accepted customs and practice have gradually developed since the inception of digital evidence. By and large in the UK the documentary digital evidence realised from the actions of a PC is admissible, under a presumption that it was reliably produced. The person making the interpretation will give a witness statement and also be present in Court to give oral evidence and to be available for cross-examination. The reliability of the record may however be called into question.

We can identity a number of categories of digital evidence, which are summarised in the table below (the categories are neither mutually exclusive nor exhaustive):

<table>
<thead>
<tr>
<th>Type of digital evidence</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content data</td>
<td>Words, sentences, numbers, images etc from PC hard drives, emails, websites, mobile phone memory dumps etc.</td>
</tr>
<tr>
<td>Recovered data</td>
<td>Data which has been (apparently) deleted by the suspect but then recovered by an investigator e.g. recovering deleted instant messaging logs on a mobile phone</td>
</tr>
<tr>
<td>Hidden data</td>
<td>Data which has been deliberately hidden e.g. using steganography to hide a child sexual abuse image</td>
</tr>
<tr>
<td>Event and location data</td>
<td>Data which includes information about events and location e.g. from a satnav device giving details of places, times, duration of stops eg Android location cache files etc.</td>
</tr>
<tr>
<td>Meta-data</td>
<td>Information about data e.g. when an MS Excel spreadsheet file was created, edited eg Android YAFFS2 (moving to Ext4) metadata etc.</td>
</tr>
</tbody>
</table>
Ambient data | The Windows page file, fragments of data
---|---
File and folder data | Windows registry data, time stamps eg Nokia S40 format dates
Back up data | Data backed up e.g. to a Cloud service
Network communication data | E.g. email traffic data collected from an ISP or by covert means (e.g. using a ‘sniffer’); GPRS data from communications service provider

In the UK evidence generally only features within the deliberations of the Court if it satisfies the tests of relevance, admissibility and weight. (It is likely that these considerations will feature throughout many stages of a digital criminal investigation, and not simply at the stages of formal prosecution, when it might be rather too late). Evidence is relevant if it has some bearing on proving or disproving some point in dispute in a prosecution and trial. Admissibility is closely related to relevance and simply refers (in a rather circular fashion) to evidence which can be properly received and heard by the court. Evidence is considered inadmissible if it has been ‘unfairly acquired’, if for example it has been obtained in violation of codes of conduct such as PACE 1984. In many European countries that employ the inquisitorial system of justice (with an examining magistrate) there are no formal rules of admissibility but instead the single test of ‘relevancy’. In the US admissibility is determined by the Federal Rules of Evidence.

If the digital evidence is deemed admissible, it is then considered in terms of what ‘weight’ of fact it might carry – that is its probative value. Digital evidence is likely to have greater weight if it is authentic, accurate and complete. The degree of authenticity depends on how explicitly the evidence is connected to the suspect or others and the circumstances of the alleged crime. For example, the authenticity of a print out of an email would be high if it was shown that the email was sent using the account controlled by the suspect from the IP address of a networked PC under his control and regular use, and the email content related to the alleged offence. Likewise, the simple existence of an indecent image of a child on a person’s PC would not in itself carry sufficient weight to prove possession in a court of law, but the existence of the image together with date stamps showing when the image had
been accessed, the creation of a folder to store the image and so on would significantly add to the weight in terms of authenticity.

The weight of accuracy of the digital evidence also partly depends on the reliability of the methods that have been used to collect, analyse and interpret the data. Hence it includes considerations of the likelihood of the ‘contamination’ of the evidence (e.g. undocumented change to the data), and the scientific standing of the techniques used. For example, digital evidence that has been produced by a person with recognised professional standing, and who has used a suite of recognisable and reliable forensic software according to professional guidelines (such as, in the UK, the ACPO Good Practice guidelines for Digital Evidence, ACPO 2012), is more likely to carry significant weight in terms of its accuracy (but see below). Finally, the more complete the digital evidence is, the more weight it carries. Completeness is a reference to the quality of the ‘narrative’ of the digital evidence: does it hang together as a coherent account confirmed by cross referencing?

There are a number of issues surrounding digital evidence and the CJS. One concern is that legal practitioners are not able to fully appreciate the potential weight of digital evidence (Boddington et al. 2008). The volatility, complexity and at times large quantity of digital evidence be challenging for legal practitioners. There may be doubts about the authenticity and completeness of electronic records because they are much easier to fabricate than physical evidence, and this can impact, they argue, on the admissibility and weight of the evidence.

Moves by the Forensic Regulator (Home Office 2010) to improve the quality of forensic practice in the UK refer to scientific concepts such as ‘reliability’ and ‘validation’. Unlike professional scientists, most forensic investigators do not necessarily have the skills or training needed to carry out authoritative scientific research (Jason Beckett & Jill Slay 2007). Furthermore, the House of Commons Science and Technology Committee have previously expressed concerns over the lack of an established protocol for admitting expert evidence (House of Commons 2005). In the same report, the admissibility systems of Frye and Daubert in the USA are cited as an ‘interesting development’,
suggesting there may be moves in the future towards a similar gate-keeping system for expert evidence in the UK (and not just for digital evidence).

Furthermore, the probative value of at least some digital evidence is subject to a number of possible ‘defences’, particularly within adversarial systems of justice. For example, the separation of user actions from events caused by malicious software is the basis of the so-called ‘malware defence’, often also referred to colloquially as the ‘Trojan defence’. In the UK the cases of R v Caffrey (2003), R v Green (2003), R v Gray (2009), R v Schofield (2003), Amero (Rasch, 2007) and Fiola (Leyden, 2009) all involved a defence citing malware as the cause of all or part of their alleged actions. Typically, the Defence (in an adversarial system) will argue in terms of possibilities (and hence introduce reasonable doubt), while the Prosecution focus on likelihoods (and how low such likelihoods are in their experience). Unfortunately, on the matter of the events that could be caused by malware, neither side usually present anything other than anecdotal evidence to support their stance.

From a sceptic’s perspective, the malware defence is not an issue. Conventional artefacts are sufficient to determine if the identified actions were performed by malware, or intentionally by the user (Carvey 2009). However, anti-forensic measures (which with malware is common practice) are cited as a risk to the practice of using conventional artefacts in this way (Kessler, 2007), (Casey, 2002). Anti-forensic include packers (Desfossez et al. 2009), virtual machine (VM) protectors (M. Sharif et al. 2009) and RAM based malware that does not touch the disk (Miller 2004), (Wallisch 2009) using techniques such as ‘Reflective DLL injection’ (Fewer 2008).

There may be anecdotal arguments of certain behaviours having not been witnessed (McLinden 2002), (Douglas 2007) and this can be convincing, but according to the principles of ‘falsifiability’ proposed by Popper (1968) the arguments are insufficient. Simply because something has not been observed, it cannot be discounted as a possible explanation, and offenders may attempt to exploit this. It may be argued that anecdotal arguments are accepted by Courts and are therefore sufficient, but some see this simply as the result of the Court’s naivety in the area of forensic science (Saks & Faigman 2008).
The use and interpretation of statistical values is yet another area where problems arise, for example five different schools of thought on interpreting probabilities in a legal context have been identified (Schum 1986). The Prosecutor’s Fallacy (House of Commons 2005), (Garrett & Neufeld 2009) and the Ecological Fallacy (Beach 2010) are well-documented examples of inappropriately cited statistics.

**Digital forensic standards and accreditation**

High profile miscarriages of justice in the UK such as R v Cannings 2004, R v Clark 2003 and Patel (BBC 2003a) have been attributed in part to questionable expert evidence (Law Commission 2011). As a result, in the UK there is a move to incorporate a systemised and regulated approach to expert evidence. We have perhaps moved on from Garfinkle’s (2010), ‘Golden Age’ of digital forensics (the period from 1999 to 2007) with the implicit trust in the digital investigator as expert. This change has been mirrored elsewhere in the world, with Beckett and Slay observing (2011, p. 214) that ‘National bodies in the United States and elsewhere are beginning to call into question the validity of science and forensics in general, with a call for reform across all disciplines’. The absence of scientific principles in several forensic disciplines is well documented (Beckett & Slay 2007; Sean Peisert et al., 2008; Saks & Faigman, 2009; and Sommer, 2010). Following the bad press that exposed the weaknesses of expert evidence within the CJS (BBC, 2003a and 2005), a review of science as applied to expert evidence is now underway.

Thus the office of Forensic Regulator was formed in 2008 with a remit to “establish and monitor compliance with quality standards for the provision of forensic science services to the police and wider criminal justice system” (Forensic Science Regulator 2009). The Regulator’s ‘Codes of Practice and Conduct’ (Home Office 2011) are aligned to BS EN ISO/IEC 17025:2005 (ISO 2005). Forensic service providers now therefore face an emerging regulatory requirement to be able to demonstrate that their working practices meet with minimum standards. In anticipation of this trend, in some police forces the contracts for outsourced work are now being awarded partly on the condition that the provider is ISO 17025 accredited.
The draft Codes of Practice produced by the Forensic Regulator for forensic service providers and practitioners seek to provide greater “confidence in the reliability of forensic science evidence” (Home Office, 2010). The standard is designed for the testing and calibration of laboratory equipment. It makes reference to procedures that incorporate concepts such as validation, reproducibility, and objectivity. The standard also makes provision for the use of non-standard methods, such as might be applied to the extraction and interpretation of data from an unfamiliar file format. The requirements are explicitly set out and provide a clear indication of the scientific approach that underpins the standard as a whole. The techniques for non-standard methods are required to include at least one of the following:

- Calibration using reference standards or reference materials
- Comparison of results achieved with other methods
- Inter-laboratory comparisons
- Systematic assessment of the factors influencing the result
- Assessment of the uncertainty of the results based on scientific understanding of the theoretical principles of the method and practical experience.

Given these concepts and requirements, the ISO 17025 standard (and hence the Forensic Regulator’s draft Codes of Practice) demonstrate a significant commitment to scientific principles.

One of the drawbacks of the standard for forensic service providers is that it is a quality based standard. It therefore clearly addresses what a provider should do, but not how it should be done. So although a provider must demonstrate it has a validation procedure for a forensic process, a description of the validation method itself is not required. This creates uncertainty with respect to the efficacy of the validation procedure. Furthermore, addressing scientific questions within the CJS is inherently problematic since the philosophy of science is fundamentally different to that of law, and hence the levels of proof differ (Kritzer, 2009), (House of Commons, 2005). Scientific inquiry values
scepticism, seeks to generalise and recognises the complexity of truth which may be multi-faceted. However, legal inquiry values certainty, considers specific events and seeks to reveal a single truth.

Applying the ISO 17025 standard to malware forensics presents a number of challenges, such as the lack of science, the inherent conflict between scientific and legal requirements, testing methodologies and the skill needs of both forensic and legal practitioners with respect to malware forensics. For example, section 5.4.6 outlines the requirement for an estimation of the uncertainty of measurement. A measurement is a property comprising of both a quantity and the associated units of measurement (Bell 2001), and the International Vocabulary of Metrology from which the ISO 17025 standard takes its definitions also defines a measurement in terms of a quantity and unit of measurement. Many of the artefacts obtained from a computer investigation cannot be quantified in terms of physical units of measurement, eg: registry values, Internet history records, chat-logs and even file sizes in kilobytes. The standard is therefore more readily applicable to physical science than to computer science laboratories. ILAC-G19 and the newly emerging ISO 27041 standard are however now addressing these particular difficulties (Marshall 2011).

Another area where challenges might arise during a prosecution concerns the forensic practitioner’s experience and training in scientific methodologies. Neither the private sector nor police authorities have the experience, personnel, financial resources or culture to undertake scientific research to create an established body of knowledge (Jeffreys 2011). Beckett & Slay (2007) argue that law enforcement practitioners have “a way to go to meet minimum standards for a scientific discipline”. The overarching priority to be profitable and manage high volumes of cases dictates that only tried and trusted techniques are used.

Critics also argue that many claims concerning expert evidence have never been scientifically justified and also use poorly designed test data (S. Peisert et al. 2007). However, the cost and resource implications of applying a scientific approach to the testing every function of a tool under all conditions are untenable (Beckett & Slay, 2007). It has been suggested that rather than invalidating
an entire expensive forensic software package, a more practical approach would be to test its functionality for particular circumstances (Guo et al., 2009 and Guo & Slay, 2010).

The practice of simply relying on the corroboration of two tools to verify results is also subject to flaws as it overlooks the possibility that both tools may be wrong. An example of this is where two tools both rely on querying the same Windows API (Application Programming Interface) (Eric & Liu 2006 and Beckett & Slay 2007). Errors from an API can arise due to vulnerabilities in the design (similar to those utilised by malware) or simply because a given API function was not written with a forensic application in mind.

As to who performs the testing, it is argued that testing by practitioners (normally the investigators and analysts) is problematic due to a combination of inexperience in choosing the required number of observations, ill equipped labs and a heavy workload (Pan & Batten 2009). However, no evidence is offered to uphold this position. They go on to present a testing methodology designed to calculate the minimum number of observations required for testing. The authors maintain that performance testing is measured by "establishing the level of errors", but no attempt to determine the level of error is presented. In a network-monitoring scenario uncertainty might be reported by employing a seven point qualitative scale ranging from ‘Erroneous/Incorrect” to “Certain” (E. Casey 2002). In more general terms, Skeels at al. (2010) identify three primary sources of uncertainty; Measurement precision, Completeness and Inferences. Each of these is susceptible to two further sources of uncertainty: disagreement and credibility.

References

(Some taken from Wiley chapters).


ACPO Centrex.

ACPO (2007) Practice Advice on Resources and the People Assets of the National Intelligence Model [Online] Available at:


Online: http://www.ijde.org/docs/02_full_art2.html [visited 30 June 2004]
Urbas (2010) Protecting Children From Online Predators: The Use of Covert Investigation
Techniques by Law Enforcement Journal of Contemporary Criminal Justice
Vol. 26(4) pp. 410–425

Micheal O’FlOinn David Ormerod (2011) Social networking sites, RIPA and criminal investigations
Criminal Law Review 766
Mark Taylor , John Haggerty , David Greesty , Tom Berry (2011) Digital evidence from peer-to-peer networks computer law & security review 2 7 ( 2 0 1 1 ) 6 4 7 e 6 5 2


ACPO/Centrex (2005) Practice Advice on Core Investigative Doctrine


Interpol (2013) Cybercrime [online] Available at: https://secure.interpol.int/Public/ICPO/FactSheets/FHT02.pdf
