Cybercrime and Cloud Forensics:

Applications for Investigation Processes

Keyun Ruan
University College Dublin, Ireland

Information Science
REFERENCE

Managing Director: Lindsay Johnston
Editorial Director: Joel Gamon
Book Production Manager: Jennifer Yoder
Publishing Systems Analyst: Adrienne Freeland
Development Editor: Austin DeMarco
Assistant Acquisitions Editor: Kayla Wolfe
Typesetter: Christy Fic
Cover Design: Jason Mull

Published in the United States of America by
Information Science Reference (an imprint of IGI Global)
701 E. Chocolate Avenue
Hershey PA 17033
Tel: 717-533-8845
Fax: 717-533-8661
E-mail: cust@igi-global.com
Web site: http://www.igi-global.com

Library of Congress Cataloging-in-Publication Data

Cybercrime and cloud forensics: applications for investigation processes / Keyun Ruan, editor.
p. cm.
Includes bibliographical references and index.
Summary: “This book presents a collection of research and case studies of applications for investigation processes in cloud computing environments, offering perspectives of cloud customers, security architects as well as law enforcement agencies on the new area of cloud forensics”-- Provided by publisher.
ISBN 978-1-4666-2662-1 (hardcover) -- ISBN 978-1-4666-2693-5 (ebook) -- ISBN 978-1-4666-2724-6 (print & perpetual access) 1. Computer crimes--Investigation. 2. Forensic sciences--Data processing. 3. Cloud computing. 4. Computer crimes--Investigation--Case studies. 5. Cloud computing--Case studies. I. Ruan, Keyun, 1986-
HV8079.C65C95 2013
363.25’968--dc23

2012033552

British Cataloguing in Publication Data
A Cataloguing in Publication record for this book is available from the British Library.

Chapter 4
The Emergence of Cloud Storage and the Need for a New Digital Forensic Process Model

Richard Adams
Murdoch University, Australia

ABSTRACT

Cloud computing is just one of many recent technologies that have highlighted shortcomings in the development of formal digital forensic processes, which up until now have been focused on a particular group of practitioners, such as law enforcement, and have been too high-level to be of significant practical use, or have been too detailed and specific to accommodate new technology as it emerges. Because the tools and procedures employed by digital forensic practitioners are generally outside the knowledge and understanding of the courts, they need to be described in such a way that they can be understood by the layperson. In addition, they should also conform to some standards of practice and be recognised by other practitioners working in the field (Armstrong, 2003; Kessler, 2010). Unfortunately, as Cohen (2011) points out, the whole field of digital forensics lacks consensus in fundamental aspects of its activities in terms of methodology and procedures. There has been a lot of activity around different aspects of cloud computing, and in Australia this has centered on the protection of personal data (Solomon, 2010). On an international scale, there have been several articles written by lawyers (Gillespie, 2012; Hutz, 2012; Kunick, 2012) discussing other legal considerations of accessing data in the cloud; however, this chapter looks at the issues surrounding digital evidence acquisition and introduces a new high-level process model that can assist digital forensic practitioners when it comes to presenting evidence in court that originated in the cloud.

DOI: 10.4018/978-1-4666-2662-1.ch004

BACKGROUND

Given the pervasive nature of information technology the nature of evidence presented in court is less likely to be paper-based and in most instances will be in electronic form (Stanfield, 2009). However, evidence relating to computer crime, regardless of definition, is significantly different from that associated with the more 'traditional' crimes for which there are well-established standards and procedures (Smith, Grabosky, & Gregor Urbas, 2004; Stanfield, 2009).

In Australian courts, the admissibility of evidence is governed by both statute and common law. Each state and territory have their own Evidence Act, with some combined to echo the Federal (Commonwealth) Evidence Act. The general principle adopted by these courts for copies of documents presented as evidence is that a copy of a document is recognised as equivalent to the original and that this applies to computer records. As with other types of evidence, the courts make no presumption that such evidence is reliable without some evidence of empirical testing in relation to the theories and techniques associated with the production of the copy (Mason, 2007). Edmond states that *"…reliability assessments should focus on the technique and its accuracy (as well as the proficiency of the operator/analyst)"* (Edmond, 2010, p. 94). This issue of reliability means that courts pay close attention to the manner in which electronic evidence has been obtained and in particular the process in which the data is captured and stored (Cohen, 2011; Grant v Marshall FCA 1161, 2003; Hargreaves, 2009; Kessler, 2010; Mason, 2007).

Because the tools and procedures employed by digital forensic practitioners are generally outside the knowledge and understanding of the courts and juries they need to be described in such a way that they can be understood by the layperson. In addition, they should also conform to some standards of practice and be recognised by other practitioners working in the field (Armstrong, 2003; Kessler, 2010). Courts may apply methods used for testing scientific evidence to digital evidence presented before them and this is commonly based on American practice (Abdullah, Mahmod, Ghani, Abdullah, & Sultan, 2008; Beebe & Clark, 2004; Palmer, 2001; Peisert, Bishop, & Marzullo, 2008; Stanfield, 2009; Moles, 2007; Stephenson, 2003). In this regard it is the practice of American Courts, when seeking to determine the reliability of scientific evidence, to apply the Daubert Test, named after the Daubert v Merrell Dow Pharmaceuticals case (Supreme Court of the United States, 1993). In this case the US Supreme Court determined that it was the duty of a trial judge to scrutinise evidence, particularly if it is of an 'innovative or unusual scientific' nature to ensure that it meets with the requirements of the Federal Rule of Evidence 702. This has been identified as the judge taking on the role of 'gatekeeper' (Kessler, 2010).

Based on the Federal Rule of Evidence 702 the process for determining the admissibility of evidence requires that any expert testimony must be derived from "scientific knowledge." However, "scientific knowledge" itself requires that "sound scientific methodology" has been applied based on the "scientific method" and this led to the court in the Daubert v Merrell Dow Pharmaceuticals case establishing what has become known as the Daubert Test. In practice the Daubert Test is often summarised as four components that provide clarity around determination of 'sufficient facts or data' and 'reliable principles and methods' (Gosh, 2004a; Stephenson, 2003):

1. Whether the theory or technique in question can be and has been tested.
2. Whether it has been subjected to peer review and publication.
3. Its known potential rate of error along with the existence and maintenance of standards controlling the technique's operation.
4. The degree of acceptance within the relevant scientific community

Another American case, that of Kumho Tyre Co. v Carmichael (1999), expanded the Daubert Test to allow for 'non-scientists' to give expert evidence, such as engineers and other technical witnesses, as noted by Gianelli (2007), Calhoun (2008), and Rogers (2006). Despite the fact that the Daubert case was heard in 1993 its influence is still strong in relation to digital evidence as demonstrated by the consultation paper issued by the Law Commission for England and Wales which effectively mimics the Daubert Test used in the United States (Edmond, 2010, p. 93). However, when applying the Daubert Test to cases involving digital forensic tools and techniques it appears that regarding digital forensics as a science causes some issues, in particular the lack of generally accepted standards and procedures (Carrier, 2002; Meyers & Rogers, 2004). Peisert et al. (2008) suggest a reason for this is that the discipline has been developed without the typical initial research that would have provided the sound scientific basis necessary for admitting digital forensic evidence. Contrary to the contention of Buskirk and Liu (2006) who suggest that digital evidence is 'automatically' presumed to be reliable we have a situation in which, in the absence of anything better, courts are often using methods that apply to 'classical' science to determine the reliability of objects from digital forensics (Calhoun, 2008; Cheng, 2007; Kenneally, 2005; Kessler, 2010; Limongelli, 2008; Meyers & Rogers, 2004).

ACQUIRING DATA FROM THE CLOUD

At first sight, it would seem that the issue of acquiring evidence from the cloud is really just an extension of current activities that are employed to acquire data from a network on the basis that the data is stored on a device other than the one being used to access the data. The similarities and fundamental differences between the two situations can be described under the headings of 'logical access,' 'physical access,' 'flexibility of methods,' 'segregation of data/evidence,' and (of particular relevance) 'legal implications.' These headings are now considered:

Logical Access

Network

In the case of a network acquisition, the Digital Forensic Practitioner (DFP) will be provided with access through a device that is attached to the client's network and also provided with authentication details. Although possible, it is less likely that external connections, i.e. using resources not owned by the client, will be used to access the device to be imaged and therefore the path that the data takes from the source storage device to the target storage device is fixed and known.

Cloud

Access to cloud resources will typically be provided through the normal process by which the cloud consumer connects to the hosted resources. The access from resources not owned by the cloud consumer is possible as the intermediate connection between source and target storage devices is provided by the Internet in most cases. However, it is not a simple matter to identify the path that the data takes from source storage device to the target storage device and this path may not remain fixed.

Physical Access

Network

In some situations, it may be necessary to acquire physical images of server storage devices rather than the logical data provided by the operating system. An organization's ability to make the physical device available for acquiring the data makes this a feasible activity, notwithstanding the practical implications such as ensuring that the impact on the organization's normal activities is minimized.

Cloud

As the cloud consumer that owns the data does not have physical control of the hardware on which the data resides the process of obtaining a physical image of the storage device is complex. From a practical perspective, the host server may be located in one or more locations around the world requiring the DFP to travel overseas with all the associated issues of time and cost—always assuming that they will be granted access to the host server in the first place.

From a technical perspective, the server running on the host resource is likely to be an instance of a virtual machine, which is also likely to be one of many on the same physical device. The options for acquiring the 'physical machine data,' i.e. all storage locations including file slack and unallocated space, require a copy of the virtual machine (and snapshots) which will, by necessity, have to be supplied by someone with access to the host server. However, this access is unlikely to be provided to the DFP working for the hosted client. A person with access to the host server may not be a DFP in their own right nor be aware of the actions to be taken in order to ensure that the evidence is admissible.

Flexibility of Methods

Network

The DFP will have a variety of methods available that will depend on the use to which the device to be imaged is being put (i.e. options will be more restricted if the device is the main company fileserver or email server). With a device on the company network that is to be acquired 'live' a common practice is to run a local 'agent' on the source device which then transmits the acquired data to another node on the network. Alternatively, the device may be powered down and the appropriate method selected from a variety of acquisition options such as removal of hard disk and attachment (via write blocker) to an acquisition device or booting the source device from a Linux or Windows-based forensic boot disk or USB.

Cloud

The options for acquiring the data remotely are more restricted in a cloud environment and will depend on the type of service being provided. For Platform as a Service (PaaS) the cloud consumer (and therefore the DFP) will not have any access to the hardware or operating system that is provided on the host. In this instance the DFP will have to rely on the Cloud Provider (CP) having the resources and the incentive to be able to acquire cloud consumer data in a forensically sound manner—complicated more if the data is physically stored on a device hosted by a subcontracted third-party.

For Software as a Service (SaaS) the DFP has even less visibility of the hardware on which the data to be acquired resides and to make matters more complicated not only may there be more than one cloud consumer being served by a particular host computer but the servicing of cloud consumer tasks may be distributed over multiple host computers. Again, the DFP will be reliant on the CP being willing and able to acquire the data in a forensically sound manner.

For Infrastructure as a Service (IaaS) the cloud consumer, and hence the DFP, will typically be provided with a virtual machine on which they can install their own operating system and applications. Despite the cloud consumer's virtual machine typically residing with numerous other virtual machines on the same hardware the DFP is able to take advantage of the fact that then operating system is accessible and can deploy the same tools as for a normal network acquisition.

Segregation of Data/Evidence

Network

Within a single organization there is usually no issue with having to identify and segregate different data for logical acquisitions as this will be accomplished during the normal course of identifying data of relevance as extraneous data will be wasteful of resources, especially the time to acquire, process, and review. The logical acquisition of data for a particular matter that is part of an investigation, such as for e-Discovery or compliance with a court order or notice (such as a notice served by the Australian Securities and Investment Commission under Section 30 ASIC Act) are situations whereby not all the data acquired will be involved in the proceedings due to issues of relevance, confidentiality, and privilege. This can often be the case when acquiring email server data, which will include all correspondence including that between an organization and their lawyers; however normally there is an agreed protocol to remove material that is not the subject of the warrant, notice etc. after it has been acquired.

Where there is more of a problem is when a physical acquisition is obtained from a device that has been used to store information from more than one legal entity. For an organization that may have several businesses sharing resources this issue can be relatively easily managed, as typically there are only a few parties involved and agreement can be reached on a protocol for segregating the data collected. There is more of a problem when the data that is to be acquired belongs to many other parties, such as data stored on the server of a law firm or firm of accountants. Although the number of entities involved may be quite large, it is ultimately possible to identify all of them and address the legal complications.

Cloud

None of the options provided by a CP enable physical access to the host computers and therefore this is unlikely to be an option available to the DFP. The fact that the data to be acquired may reside on one or more physical devices which themselves are being used by multiple cloud consumers and that the configuration of the devices may not be static makes it unlikely that the CP will be able to offer any form of physical acquisition.

The logical acquisition process for IaaS will follow similar line to that for a networked resource. But for cloud consumers that have purchased the PaaS and SaaS options the DFP will require the assistance of the CP.

Legal Implications

Network

When working on a network the legal aspects are relatively easy to identify and address. If the network is owned by the cloud consumer and their 'computer use' police clearly states that all data contained on their systems is, in effect, deemed to be their property then in many situations the work of the DFP is straight forward. The exceptions arise when, as mentioned earlier, the client or organization that owns the network may be storing information relating to third parties as in the case of lawyers, financial advisers and accountants. If the DFP is operating under a court order or warrant then they need to ensure that the details of the document are in order in that they authorize the intended activities of the DFP although it is often the case that the DFP may not be granted immediate access due to a legal challenge but these are, in many cases, resolved by the lawyers involved relatively quickly.

Cloud

There are several factors that have the potential to make the acquisition of data from the cloud far more complicated. Firstly, data may be distributed across hardware owned and operated by different entities. Secondly, these entities may be in more than one legal jurisdiction, and finally data may be co-mingled with data from other organizations who themselves may come under different legal jurisdictions. However, these issues should really only become a problem if physical acquisitions are required. For logical acquisitions, the location and nationality of the CP should not be an issue, as the DFP will be using the credentials of the cloud consumer to access the data as it is presented to them under their agreement.

For cases in which access to the physical storage devices are required the DFP will be reliant on their legal advisers to confirm that they have the authority to undertake the work on the basis of information supplied by the CP in relation to the physical location of the data—which may not be a simple or straightforward task. Furthermore, the DFP will also be reliant on one or more third parties to collect the data in a forensically sound manner, particularly if it resides overseas.

This section has highlighted some of the practical difficulties being faced by DFPs when they are considering acquiring data from the cloud. In essence, for logical acquisitions the process is only slightly more complicated than for a network acquisition and little different from that encountered when an organization has their datacenter hosted by a third party through a private network rather than across the Internet. The main issue arises when having to consider the physical locations of data when a 'live' or 'logical' acquisition is not an option.

A NEW DIGITAL ACQUISITION PROCESS MODEL

The amount of storage capacity being encountered by DFPs is making the process of undertaking a 'dead' acquisition impractical. Whilst storage capacity for the acquired data is relatively cheap, the speed with which the data can be collected is not keeping up with the increase in data volume with even entry-level laptops having 1TB of storage. If we look at what the DFP is trying to do, we can summarize this as collecting data in such a way that a court can make a determination of the reliability of any evidence that may be presented before it that formed part of that data. The technical aspects of the acquisition are not expected to be understood by the court but the process adopted by the DFP should be capable of being explained as well as all the aspects of the work that were taken into consideration.

In the early days of digital forensics, a lot of emphasis was placed on the ability to ensure that data had not been altered on the source device through the use of write-blocking devices and this was a relatively simple concept to explain in court. However, it soon became apparent that there were likely to be more and more situations in which it was not possible to shut down the computer storing the data and so the concept of 'least intrusion' evolved whereby the DFP identifies the likely changes that may occur to the data as a result of their activities together with their implications for any evidence contained within that data. We have rapidly seen an expansion in the volume of data being encountered and the impact of taking file servers or email servers offline recognized as being unacceptable in many instances.

We are therefore moving away from the utopia in which everything can be isolated as well as the concept that data can be located on a single physical device and this requires DFP to adopt alternative techniques. The courts want to see a clear process description for the activities undertaken by a DFP so that they can assess whether the DFP considered

all the appropriate factors, such as authority to do the work, in undertaking their activities. With the advent of the cloud, the non-technical aspects of the DFP's work are assuming an ever-greater proportion of the data acquisition process. This is not to say that the courts will not want to query certain technical aspects of the DFP's work (usually by calling upon other experts) but they want to be able to place these in context with the other non-technical factors which could render the technical discussions irrelevant. In this regard, there is an urgent need for a process model that describes the activities undertaken by a DFP working in a commercial or a law-enforcement environment.

The multi-jurisdictional, multi-environmental nature of cases result in different applications of digital forensic principles being seen by courts in different ways, therefore the methodology employed by digital forensic practitioners will always come under scrutiny (Kessler, 2010; Rogers, 2006). This issue is not confined to the law enforcement environment as it applies equally to the activities of many commercial practitioners working in the field of digital forensics and incident response who may also be involved in legal proceedings (Kohn, Eloff, & Olivier, 2006; Meyers & Rogers, 2004; Peisert, et al., 2008; Turnbull, 2008).

Ciardhuáin has stated that "A comprehensive model of cybercrime investigations is important for standardising terminology, defining requirements, and supporting the development of new techniques and tools for investigators" (Ciardhuain, 2004, p. 1). Ciardhuáin goes on to suggest that a comprehensive model would have general benefits for IT managers, auditors and others not necessarily involved in the legal process due to the increasing incidence of 'crimes' involving computers. Going further still, Trcek et al. push the notion of an agreed "template legislation" that would harmonize the practice of digital forensics on an international basis (Trcek, Abie, Skomedal, & Starc, 2010). Yet, as Selamat et al. (2008) observe *"…there is no single framework can be used as a general guideline for investigating all incidents cases. Therefore, further research is needed to design a general framework to overcome this issue."* It is to address this issue that the model introduced in this chapter has been developed.

Given the rigorous standards that apply to material used in court there is an urgent need to establish a framework for digital forensics that assists courts in their determination of the admissibility of digital evidence (Ami-Narh & Williams, 2008; Brown, 2006; Rogers, 2004). The problem, according to many researchers (Carrier & Spafford, 2004; Meyers & Rogers, 2004; Peisert, et al., 2008; Sun, Yoon, & Yoo, 2008; Turnbull, 2008) is that there are several obstacles that must be overcome in order to develop such a framework, namely:

- There is no standard for the collection of digital evidence, although there are published guidelines in various countries.
- There is no standard of training/knowledge required of someone undertaking the collection of digital evidence.
- The environment in which digital evidence exists is not heterogeneous and is constantly changing requiring flexibility in the application of techniques and processes.
- The existing knowledge resides within a relatively small number of experienced practitioners and given the nature of the work there is little opportunity for passing this knowledge on in a timely manner to trainees.
- Often inexperienced investigators or IT personnel are required to collect electronic evidence.

There has been little progress in refining and defining a generic digital forensic process since an initial meeting of experts in 2001 concluded that this was necessary (Council of Europe, 2001; Nance, Armstrong, & Armstrong, 2010; Pollitt, 2009; US-CERT, 2008). Many researchers writing

in this field have adopted their own terminology for describing process models which rather than being generic are aimed at particular environments, such as law enforcement (Rogers, 2006), and incident response (Cummins & Lowry, 2003; Mandia & Prosise, 2001; Stephenson, 2003b). Some researchers have tried to utilize existing formal languages and methods rather than invent their own terminology but they still have focused on a particular environment (Pollitt, 2007).

Standards and Guidelines

When considering 'standards' against which the DFP activities can be assessed by courts in Australia there is an aspect of definition that has to be addressed. The international body for 'standards,' the International Standards Organisation (ISO), defines a 'standard' as a "document, established by consensus and approved by a recognized body, that provides, for common and repeated use, rules, guidelines or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context." However, Australian Standards, the national body in Australia, considers that "Standards are published documents setting out specifications and procedures designed to ensure products, services and systems are safe, reliable and consistently perform the way they were intended to. They establish a common language which defines quality and safety criteria." Notwithstanding this issue, the relevant references are now considered individually.

ISO is the main international body that is relevant to standards within the field of digital forensics and is a non-government organisation that is composed of representatives from 157 national standards organisations, one of which is Standards Australia. ISO is based in Geneva, Switzerland and although it has no government-enforced powers ISO standards are often adopted by its member countries. In addition to the standards that it sets, ISO also publishes technical reports, guides and other technical literature, normally based on the output from special committees that are established for a particular purpose. One of these committees, JTC1 (the only joint committee of ISO), is the specialist standards-setting organisation for electrical, electronic and related technologies the IEC. At a meeting held in Kyoto in April 2008 a sub-committee of JTC1 (JTC1/SC 27 – IT Security Techniques) proposed a Study in the area of Evidence Acquisition Procedure for Digital Forensics. The ongoing contribution of the Australian Standards Working Group is currently being coordinated by Ajoy Gosh who has authored previous standards and guidelines in this area (Gosh, 2004a, 2004b) with input from practitioners working within law enforcement, education and commerce.

The BSI has produced a standard, BS 10008, whose title, 'Evidential Weight and Legal Admissibility of Electronic Information: Specification,' suggests that it may be related to the acquisition of electronic evidence. However, the standard relates to the production of electronic documents that may be required as evidence of business transactions and provides guidelines for practices and procedures involving information management systems.

The UK National Hi-Tech Crime Unit produces (on behalf of the Association of Chief Police Officers) the Good Practice Guide for Computer Based Electronic Evidence (Association of Chief Police Officers, 2003) which contains definitions of the four Principles of Computer Based Electronic Evidence (developed prior to the advent of cloud computing) which are as follows:

Principle 1: No action taken by law enforcement agencies or their agents should change data held on a computer or storage media, which may subsequently be relied upon in court.

Comment: This Principle will be difficult to follow in most, if not all, cloud environments without placing reliance on third parties (potentially other law enforcement personnel in the hosting country)

and thus adding a further tier of complexity to task, notwithstanding the timing issues this raises.

Principle 2: In exceptional circumstances, where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.

Comment: For cloud computing this 'exception' is likely to become the rule.

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

Comment: The audit trail and logging of activities from the cloud consumer access point should be straight forward; however the records from a third-party, such as a technician from the CP, may not potentially be of a suitable standard.

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

Comment: The inability to directly supervise the work undertaken by third-parties, such as the CP's technicians replicating a virtual machine, introduces considerable risks for the investigating officer.

Fundamental to the concept of work undertaken in a forensic environment is the ability to use material and information discovered in a court of law. As quoted above, Principles 1 and 2 require that, if possible, the original electronic data is not altered by any activities of the investigator or, if data has been altered, the person responsible is able to explain what was altered and the implications of this on the evidence being presented.

In general terms the ACPO rules are mirrored by the International Organization on Computer Evidence (IOCE) in its draft guidelines (IOCE, 2002) which themselves are based on the ISO 17025 Standard[1]. The IOCEs purpose is stated as being *"…to provide an international forum for law enforcement agencies to exchange information concerning computer investigation and computer forensic issues."*

The IOCE's guidelines can be summarised as:

- The general rules of evidence should be applied to all digital evidence.
- Upon seizing digital evidence, actions taken should not change that evidence.
- When it is necessary for a person to access original digital evidence that person should be suitably trained for the purpose.
- All activity relating to the seizure, access, storage or transfer of digital evidence must be fully documented, preserved, and available for review.
- An individual is responsible for all actions taken with respect to digital evidence whilst the digital evidence is in their possession.

The risks and issues identified in the ACPO rules are also present in the IOCE guidelines.

McKemmish (1999) introduces four Rules which he states must be followed by digital forensic practitioners during the course of their work. These Rules provide the framework under which the digital forensic practitioner should be working but they do not provide detailed guidance, although McKemmish does provide justification and examples of their application in context.

- **First Rule:** This involves the handling of evidence and requires that the original source of the data should be handled as little as possible and only to the extent needed in order to obtain an authenticated copy.

- **Second Rule:** Accommodating situations in which the practitioner has no choice but to undertake some activity that alters the data, such as entering a password to access a computer, the second rule requires the practitioner to account for changes they may make to any of the data, which comes under their control. Identifying and recording these changes will require the practitioner to have a deep technical knowledge of the environment such that they are aware of the implications of their actions.
- **Third Rule:** This states the need to comply with the rules of evidence such that the admissibility of the evidence cannot be brought into question. This involves adhering to the other Rules as well as maintaining a chain of custody and other documentation in order that any challenges relating to admissibility may be defended.
- **Fourth Rule:** This states that the digital forensic practitioner should not proceed with activities in a situation where they have exceeded their knowledge of the environment or situation. Given the ever-changing environment, this requires practitioners to keep their training program updated.

The McKemmish Rules follow the guidelines of ACPO and the IOCE but with particular emphasis on ensuring admissibility and working from a position of knowledge of the environment. This final point will be particularly challenging as, even if the CFP is knowledgeable with regard to the generic cloud environment, they are unlikely to be familiar with each particular cloud implementation that they may be called to deal with and thus require time to gather the necessary knowledge before they can proceed and this may not always be practical, particularly for law enforcement.

The document 'Guidelines for the Management of IT Records' (Gosh, 2004b) is intended to assist organisations manage the data stored on their systems in such a way that it may be readily accessed and provided in an admissible form in the event that it may be relevant in some form of litigation. Although digital forensic methods are referenced, the focus of this document is with Electronic Discovery rather than third party investigations and does not take into account the wider needs of digital forensic practitioners. In a similar vein the document 'Guidelines for Evidence Collection and Archiving' (Brezinski & Killalea, 2002) is a Network Working Group memo that is focused on incident response although it does provide advice on a range of digital forensic activities in the form of actions to be carried out under various headings, including 'chain of custody' considerations. However, despite this and the other references mentioned earlier, there has been little real progress since 2001 in refining the process for the acquisition of digital data to the point where there is a formal definition, generally accepted guidelines and reference to a standard that encompasses the activities of law enforcement, commercial, and incident response practitioners. Fundamentally, there even appears to be little agreement on the number of processes/stages involved. In January 2012, the US-CERT organisation included in its online 'reading room' a paper which suggests that we are also no further forward with regard to digital forensics becoming a 'mainstream' scientific discipline than we were at the time of the 2001 DFRWS and the paper includes the comment *"Because computer forensics is a new discipline, there is little standardization and consistency across the courts and industry. As a result, it is not yet recognized as a formal "scientific" discipline"* (US-CERT, 2008, p. 1).

The Daubert Test

The Daubert Test forms the basis on which many courts assess a particular 'scientific' process model (Gosh, 2004a; Stephenson, 2003) however, whilst the authors of many of the existing models can claim that they have been peer reviewed only a small number have undergone any form

of testing and none of them are complying with any particular standard. This situation suggests that the Daubert Test is currently ineffective as a standard for determining the reliability of the process employed for acquiring digital evidence. Whilst there are several guidelines available for digital forensic practitioners these are focused on either law enforcement, electronic discovery or incident response and do not cover all the specific requirements of practitioners working in other areas. ISO is currently working on a standard for digital evidence collection with contributions from the Australian Committee IT-012-04, but this has not yet been published and this ISO document is also likely to be a 'Guideline' rather than a 'Standard' although it is intended to cater for the needs of digital forensic practitioners working in a number of different areas, including law enforcement and commercial practice. However, whilst the document itself contains 'baseline steps' for certain activities involving the collection and acquisition of electronic data there is no overall process model.

Previous Models

Agarwal et al. (2011) comment that there have been many initiatives to satisfy the need for a standard methodology that can be applied to the different environments in which digital forensics is practiced but that so far these models are mainly ad-hoc and further work is needed in this area. We are currently progressing towards having a separate process model for each new technology as it comes along. Therefore, rather than having a further ad hoc process model specifically for the cloud environment, we need a process model that can assist the DFP (and the courts) in relation to determining the reliability of electronic evidence by describing the acquisition process in a way that can be applied in different environments (such as law enforcement and commercial practice), is described formally, relates to recognized industry standards and accommodates new environments such as the cloud. Previous researchers have provided pointers to some of the key elements that could be included in a new generic model as detailed in the following paragraphs:

Rogers: The Digital Crime Scene Analysis Model (DCSA) (2004)

1. Supporting the adoption of a common approach by considering the similarities between physical and digital evidence.
2. Emphasizing chain of custody considerations.
3. Considering all areas of digital forensics rather than bias the model towards a particular group.
4. Acknowledging that in a fast-moving technological environment, the practitioners cannot be expert and experienced in all areas.
5. Promoting a pragmatic approach concentrating on the important areas on which other aspects of the work are dependant with an emphasis on data acquisition.
6. Emphasizing that a model should be tool and technology independent.
7. Recognizing that the high-level phases are dependent on the type of investigation.

Carrier and Spafford: The Integrated Digital Investigative Process (IDIP) (2003)

8. The concept of treating the computer as a digital crime scene
9. Identifying the important attributes for a model of the digital forensic process

Ciardhuain: An Extended Model of Cybercrime Investigations (EMCI) (2004)

10. Introducing the concept of 'information flow'
11. Covering all aspects of the investigation process

12. Identifying 'awareness,' 'authorization' and 'planning' stages
13. Incorporating the concept of iterations between stages (with Beebe and Clark)
14. Identifying that there may be both internal and external authorities involved

Reith et al.: The Abstract Digital Forensic Model (ADFM) (2002)

15. The concept of abstractly defined common steps from previous generic forensic protocols
16. Introducing the concept of 'digital forensics' as more encompassing than 'computer forensics'

THE ADVANCED DATA ACQUISITION MODEL (ADAM)

By combining the key contributions and considering previous models collectively the essential elements for a data acquisition activity can be summarized as comprising of three stages:

1. An initial preparation stage that incorporates activities that take place once the practitioner is notified or becomes aware of a potential requirement to undertake some work but prior to them gaining access to the 'incident scene[2]' (the detail of training, lab preparation and other activities prior to the notification/ awareness point should not be the subject of a new model).
2. Actions that the practitioner undertakes to prepare for the acquisition of digital data once they have access to the 'incident scene' including, but not limited to, safety considerations, documentation, securing the scene and identifying potential locations for relevant digital data.
3. The actual process of acquiring digital data that may be of evidentiary value and its subsequent handling.

Carrier and Spafford (2003) state that digital forensic practitioners find the flexibility of objectives-based steps makes them more useful than a task-based 'tick-list' given that each 'crime scene' is unique and this is particularly relevant when we look at the possible permutations that can exist in a cloud environment. In addition, the principals under which the practitioner should be working are clearly stated (Association of Chief Police Officers, 2003) and these form the framework under which all the activities in the various stages are undertaken (Beebe & Clark, 2004). Shortcomings of previous models have been that:

1. Some tried to encompass all aspects of digital forensic activity in one model which became too wieldy and complicated.
2. Some confused the different activities of incident response and digital forensics leading to inappropriate activities (such as network-biased requirements) with a heavy emphasis towards an environment that does not represent a generic workspace for digital forensic practitioners.
3. Some are either very high-level descriptions providing no useful guidance or too low-level in which case they become too complicated to employ in practice.

The new model should therefore:

1. Have a narrow focus on the stages leading up to and including the acquisition of potential digital evidence.
2. Adopt terminology that is generic.
3. Be structured in such a way that digital forensic practitioners from different environments (law enforcement, commercial, etc.) will be able to easily adopt the model as a description of their processes whilst having the ability

to incorporate requirements specific to their own environment.

4. Introduce the concept of descriptors/prefixes for tasks, namely 'MUST' and 'SHOULD' to differentiate between activities that must always be carried out and those activities that may or may not apply in a given situation respectively. This will be done by using those keywords as defined in the document 'Keywords for use in RFCs to indicate Requirement Levels' [RFC2119] (Brezinski & Killalea, 2002).
5. Provide varying degrees of detail sufficient to assist the forensic practitioner at all levels whilst allowing for the simple, structured addition of new information to address the issues associated with advancing technology and tools.
6. Provide a well-defined process diagram (and associated narrative) for each stage such that it may be presented in court to help explain the work undertaken.
7. Be consistent with the ACPO Guidelines and draft ISO/IEC document CD27037 'Guidelines for identification, collection, acquisition, and preservation of digital evidence' as at July 2011, further adding to the credibility of the process described.

The new model, referred to as ADAM (Advanced Data Acquisition Model), addresses the 'Principles of Examination' stage of Noblett et al.'s (2000) Hierarchical Classification whilst allowing for the more detailed (lower level) organisational and situational aspects to be dealt with as necessary by the digital forensic practitioner.

In relation to the three-stage hierarchical model, ADAM:

1. Incorporates the principles of examination based on the guidelines from ACPO, ISO, and elsewhere.
2. Incorporates organizational policy and practice including guidelines, signing authorities, and other requirements.
3. Incorporates procedures and techniques that can be modified and expanded upon to accommodate new technological challenges (such as the cloud).

The ADAM itself consists of three stages associated specifically with the acquisition of electronic data. These stages were identified following the literature review (summarised in paragraph 3.4.3 Essential elements for the ADAM) and are described as:

Stage 1: The initial planning stage.

This is where high-level considerations are determined that relate to the documentation associated with the investigation, the investigation logistics, etc. This may involve a covert survey (sometimes carried out by private detectives) depending on the type and nature of the investigation being undertaken. In some instances, such as where law enforcement officers have already seized devices and present them for examination to the digital forensic practitioners, this stage may be very brief and simply consist of checking paperwork. In relation to cloud computing this may involve the CFP ensuring that they have the necessary knowledge within the team in relation to the particular environment and configuration that they are likely to encounter.

Stage 2: The onsite survey.

This is where all the gaps in knowledge relating to the location, size, and format of the devices holding the electronic data are filled in and the main acquisition plan is created. There may be instances in which this stage may be irrelevant as in the case for previously obtained devices mentioned above. However, in the case of cloud computing this information is likely to come from

a third-party source, i.e. the CP who will be in a position to describe the particular environment configuration of relevance.

Stage 3: The acquisition of electronic data.

This will include both replication and storage of the acquired data.

The common factor associated with all the stages is documentation. Documentation is vital to ensure that a record is kept of all activity associated with the acquisition of the electronic data and subsequent transportation and storage as there is the potential for the whole process to come under close scrutiny in court (Brown, 2006; Casey, 2004; Jones, et al., 2006; Kruse & Heiser, 2002).

In order to avoid the complication of including a large amount of low-level detail the new model incorporates several key assumptions (in accordance with the current draft ISO/IEC document (ISO/IEC, 2011):

1. The digital forensic practitioner is authorised, trained and qualified with specialized knowledge, skills and abilities for performing digital evidence acquisition, handling, and collection tasks.
2. The digital forensic practitioner ensures that they and any members of their team comply with local jurisdictional laws and regulations—particularly relevant for the cloud environment where multiple jurisdictions may be involved.
3. The digital forensic practitioner observes the requirements that their actions should be auditable (through maintenance of appropriate documentation), repeatable where possible (in that using the same tools on the same item under the same conditions would produce the same results), reproducible where possible (in that using different tools on the same item would produce substantially similar results) and justified.

Having identified the three stages and the assumptions for the new model the next sections draw upon the contributions of previous researchers to develop the elements that go to make up each stage.

ADAM Stage 1: Initial Planning

McKemmish emphasises the importance of the initial planning stage in a document written for the Australian Institute of Criminology in which he says that the forensic process begins with the identification of digital evidence (McKemmish, 1999). McKemmish goes on to say that until the location and storage format of potential digital evidence are identified it is not possible to determine the most appropriate process for its acquisition (McKemmish, 1999). Casey (2004) identifies three topics related to the acquisition of electronic data, the first of which he describes as Authorisation and Preparation. Under this topic, Casey describes the processes that should be undertaken in preparing for a warrant and although he doesn't give a name to a plan he states that: "*Planning is especially important in cases that involve computers*" (Casey, 2004).

In the ideal world it would be possible to obtain perfect knowledge of the environment containing the electronic data to be acquired thus enabling a detailed plan to be created that would simply have to be followed on site, indeed Sammes and Jenkinson (2007) state in a book section titled 'Pre-Search Intelligence' that: "*It is vital that the number of computers, their types, operating systems and connections are all known before entry*." However in practice the digital forensic examiner often has insufficient detail about the computer systems, quantity, and location of data, types of hard disk or the operating system involved to enable anything beyond a rough outline of a plan to be produced. Whilst agreeing with the earlier sentiments of Sammes and Jenkinson (2007), Brown (2006) adopts a more pragmatic approach than theirs and introduces the concept

of 'boilerplates' which he describes as being guides that are: "*…general enough to be useful in a wide array of situations but detailed enough to be helpful."*

Due to the fact that initial information relating to the specific onsite environment may be scarce, incomplete or simply inaccurate, the planning stage should concentrate on preparing for as many likely scenarios as possible, allowing for the fact that:

…each computer forensics collection operation can vary so greatly, investigators need to have a playbook from which to operate, similar to what a sports team coach would use to contain all the plays he intends to use (Brown, 2006)

Even if information can be obtained that provides some guidance on what to expect onsite., allowance always has to be made for errors or inaccuracies in this information. The planning stage is fundamental to the process of acquiring digital evidence and in one form or another is common across the different environments in which digital forensic personnel are employed. The ADAM provides more guidance than previous models in this regard, as it uniquely incorporates consideration of a number of constraints during the planning stage. These constraints are in relation to:

- Authorisation
- Physical
- Timing
- Data

The concepts behind each of these constraints will be covered in more detail in the following sub-sections, the results of which in practice would lead to the concluding activity for this first stage of the new model, i.e., the formulation of the Outline Plan.

Authorization Constraints

The primary consideration, before any of the process detail is considered, must be ensuring that you have the authority to undertake the work. This authority can be made up of several discrete aspects including authority from the organisation providing the services (internal authorisation), authority in law and authority from the owner of the resources containing the material to be acquired such as a CP (external authorisation).

The extent to which the authorization aspect of the Planning stage is covered in literature varies greatly. For instance, in their book 'Real Digital Forensics' (Jones, Bejtlich, & Rose, 2006) the authors do not mention the issue of planning and ignore preliminary background tasks by starting with instructions for acquiring data from a 'live' Microsoft Windows computer. This approach is also true for the authors of Forensic Discovery (Farmer & Venema, 2005) who again begin with the practical aspects of locating certain types of potentially relevant information on computer systems. Kruse and Heiser (2002) make a passing reference to authority under a paragraph entitled 'Legal Access' but only from the perspective of an in-house practitioner when they advise that the digital forensic practitioner must check that their company policies allow them access to the resources that are the focus of their investigation before commencing work. In contrast to the single paragraph, Casey (2004) devotes several pages to the issue.

Further support for the importance of this issue of authorization comes from Marcella and Menedez (2008) who provide a list of the basic steps for a 'cyber investigation' that begins with '1. Obtain proper authorization.' They then cover this issue in some detail beginning with:

Obtaining authorization to begin an investigation is critical, especially if the investigation involves an internal company employee and organizational management initiates the investigation. If

the investigation is initiated by law enforcement, they too must follow established procedures for obtaining authorisation (Marcella & Menendez, 2008, p. 283).

For those working in a cloud environment the process of identifying what authorization is required and from whom may be a lengthy process.

Internal Authorisation

For a small specialist provider of digital forensic services the process of internal authorisation is relatively straight-forward and should consist of a signed agreement detailing the services to be delivered.

For a firm that provides digital forensic services as part of a larger service offering, for instance a global accounting firm, the procedure may be far more complicated in that various conflict checks and risk assessments will need to be undertaken (it would be a serious issue to turn up at an office to acquire a forensic image as part of some investigation only to find out that the premises belong to an audit client of the firm carrying out the investigation).

The conflict checks and risk assessments seek to mitigate potential conflicts of interest and form part of the due diligence procedures for many large organisations. The conflicts of interest may be focused on legislative rules and guidelines or commercial considerations, such as working on a matter for which an existing client is an opposing party.

The existing literature relating to corporate digital forensic investigations is primarily based on the digital forensic practitioner being employed within the organisation that owns the resources to be investigated and assumes that internal authorisation has been granted, although this process is not referenced in the text (Steel, 2006; Wiles, 2007). Digital forensic services being provided by a third party have not been covered in literature relating to process models.

Authority in Law

For commercial practitioners, in cases such as assisting with the serving of Anton Pillar orders or matters where government bodies have 'search and seize' powers, the investigator needs to ensure that they have the authority to provide the services in the manner in which they have been requested. This may involve being named on court orders or other documents.

Law enforcement practitioners will need to confirm the details of the appropriate warrant and any limitations imposed.

Court orders permitting access to a third party's property should be closely scrutinized, as the investigator may become the subject of litigation if they perform any actions not permitted by law. Where data is physically stored in one or more 'outside' jurisdictions, there may be a requirement to obtain multiple court orders.

Consideration should be given to the possibility of processing material that is covered by criminal law, for instance where there was a suspicion that child pornography may have been contained on one or more of the computer systems to be analysed.

Mere knowledgeable possession of child pornography, as well as certain other material, is a criminal offence in Australia and elsewhere and if there is a strong chance that this type of material could exist then the investigator needs to review the situation with the client in relation to discussing the matter and obtaining legal advice.

External Authority

When engaged to undertake work for an organisation that requires "their" systems to be accessed (such as in the case of a CP) the investigator needs to confirm that the entity giving the instructions has a right of access to the resources involved. For instance, there may be occasions in which data from more than one legal entity has been stored on a single computer system—this is often the case if the resources are held at a third-party IT provider, e.g. a provider of disaster recovery services hold-

ing a 'live' copy of several organisations' data or if the computers are used by an accountant or lawyer to store information from many clients. In addition, cloud solutions may involve resources from other sub-contracted entities who supply, for instance, storage resources.

Physical Constraints

Physical access to the systems containing electronic data is generally not considered in any great depth by other models and is often approached from the perspective of a commercial digital forensic practitioner simply needing to determine if data may be located at more than one site (Brown, 2006; Jones, et al., 2006; Marcella & Menendez, 2008; Steel, 2006; Wiles, 2007). The only other aspect of physical constraints that tend to be considered is in relation to dealing with external 'attacks' on systems involving the Internet which leads to a discussion of its technical characteristics. With regard to physical constraints, the new model involves two considerations that need to be addressed prior to undertaking the data acquisition.

Access

For non-cloud environments the first aspect of physical constraints to consider is that physical access to the resources containing the data to be acquired is needed in the majority of cases, obvious exceptions being data that can be accessed via the Internet or Internal/external networks, although in the later case there would need to be a good reason for obtaining the data remotely rather than using someone onsite. Commercial premises may be located on a site that is security controlled and require the appropriate authorisation to enter or there may be door access codes. Commercial premises may also be shared with other legal entities that may restrict access. Private premises may have limited access or restricted parking, such as private premises that have security gates thus requiring the lawyers to negotiate entry with the occupants in order to serve orders and begin the data acquisition process.

For cloud environments there is unlikely to be the option for the CFP to physically access the data storage devices and therefore reliance will be made on third parties; either resources from the CP or recognised CFPs that are local to the data.

Layout

The second aspect of physical constraints to consider is whether the data is held on resources at more than one location, either on separate sites or scattered between different offices or floors within the same building. This aspect may determine how many team members are required and how many sets of equipment are needed. Steel spends some time considering the physical aspects of accessing the data under a heading of 'Identifying the scene' (Steel, 2006). CPs may have a complex mixture of resources and on initial contact may not even know where particular data are stored.

Timing Constraints

An important aspect of the planning stage is determining constraints based on time. Several authors refer to choosing appropriate techniques or methods based on 'practical' considerations but do not include timing as part of their initial preparation (Casey, 2004; Wiles, 2007). Some authors, especially those basing their discussions on in-house digital forensic practitioners, don't consider the timing aspects at all (Marcella & Menendez, 2008; Steel, 2006). If data is known to be stored in the cloud then additional time should be allowed in order to understand the particular environment, obtain the necessary authorisations and make arrangements for third-parties. The ADAM requires consideration of three aspects of timing constraints, which are now considered individually.

Court Orders and Warrants

It is often the case with court orders that there are strict time limits placed on when the acquisition activities can take place and at what point they must be terminated regardless of whether the processing has been completed or not. Similar restrictions may also be contained within warrants. With the likely involvement of multiple jurisdictions for matters involving the cloud the identification of all relevant courts and completing the process of obtaining the necessary orders may have a significant bearing on how practical the proposed acquisition may be.

Private Premises

Engagements involving data located on private premises may require getting to the premises before the subject of the court order leaves for work (or some other activity) but preferably after partners and /or children have left the building. Of particular concern is the situation when data is stored in locations within different time zones in which case it may not be possible to synchronise activities to ensure that those under investigation have no opportunity to interfere with potential evidence after becoming aware of the activities of the DFP.

Commercial Premises

Engagements involving commercial premises often require a key holder to arrive and provide access to the offices following their review of the court order. Often there is a requirement to gain access to commercial premises after normal working hours and have the acquisition completed prior to employees turning up the following day. This may be to avoid business disruption or to ensure that employees suspected of some activity are not alerted to the investigation nor do they have the potential to destroy or remove data. The business disruption aspect is considered by Sammes and Jenkinson who also suggest a 'search briefing' that not only covers the allocation of tasks and the key objectives but identifies the provisions of the warrant or court order (Sammes & Jenkinson, 2007). If the data is held at multiple sites a suitable time frame needs to be allowed such that all forensic teams are able to co-ordinate their arrival to ensure that no one is alerted to the investigation before a team arrives. Although CPs will have support for their systems on a 24/7 basis the involvement of particular personnel to provide the required authority, access and/or technical assistance will restrict when certain activities in relation to acquiring the data can take place. In addition, for resources running multiple virtual servers such as used by CPs, there is unlikely to be a 'window of opportunity' when the resources can be taken offline without impacting on cloud consumers unrelated to the investigation.

Data Constraints

The data is the electronic information that is the target of the acquisition process and can take many forms. As for other aspects of the planning stage, it is not always clear at the outset whether there is in fact any data that is relevant to the investigation or where this data might be located.

It is common practice for authors of digital forensic books to list 'types' of electronic data and suggest possible locations for this data (Hutt, 1995; Brown, 2006; Casey, 2004; Farmer & Venema, 2005; Jones, et al., 2006; Marcella & Menendez, 2008). In addition, the ADAM also requires consideration of the potential quantity of data that may be acquired and therefore there are three aspects of data constraints that are covered in the following paragraphs.

Identification of Data

The type of data to be acquired can vary greatly. For example, it could be in simple text files, images, design drawings, accounting packages or even fragments of deleted material. If data needs to be previewed prior to acquisition then the means

of identifying any relevant data needs to be addressed, for instance if relevant data is likely to be in the form of graphics images, i.e. pictures, then a keyword search will not be appropriate. There may be the need to have specialist software installed on a forensic workstation (such as a CAD application) if this is being used to preview the data in native format 'offline.' The processes undertaken in relation to identifying the relevant data may have a significant impact on the time required to carry out the work. A CP may be hosting an entire server or just application data that may exist on more than one physical machine. An entire virtual machine can be reproduced, through an appropriate technique and with the necessary audit trail, enabling examination of deleted material, registry information and other system files. However, if data is being stored within a hosted or shared application then a process of extraction will need to be undertaken which may only be possible through the CP.

Amount of Data

The amount of data to be acquired will have a direct impact on the amount of storage space required for the acquisition disks and also the amount of time that will be involved in the acquisition process itself. If a 'live' acquisition is being performed and there is likely to be an effect on network performance this needs to be communicated to the client/lawyers so that the impact on the business holding the data can be considered which may lead to negotiations on when and how the operation takes place. If data is being extracted remotely from a CP this may have a significant impact on their resources and interfere with other businesses and may therefore require some negotiations to be entered into in order to minimise this impact.

Location of Data

If the data to be reviewed and acquired is stored on backup tapes, e.g. the time period of interest is such that the data is not likely to be currently residing on any 'live' systems, access to a means of restoring the relevant backup tapes will need to be considered or a plan put in place to remove and duplicate the tapes offsite. It is becoming increasingly common for data to be held by a third party as part of a 'cloud' solution that is accessed via the Internet. This presents many potential difficulties, particularly in relation to authorization, but from a location perspective, it may not be possible to physically access the place in which the data is stored. There may not even be such a thing as a single location for the 'data' due to its nature and/or the fact that it is distributed across different physical devices that may be in different jurisdictions. This could make the drafting of the necessary court orders or authorisations very difficult.

The Outline Plan

Based on the outcome of the previous considerations the logistics of the acquisition exercise can be considered. Without a survey of the site(s), which is normally not practical due to the urgency of the work, only a reasonable estimate can be made at this stage with certain contingency measures put in place, e.g. somebody placed on 'standby' to collect and deliver additional storage media or other resources. A key part of the Outline Plan implementation is a briefing. Although Sammes and Jenkinson (2007) are writing from a law enforcement perspective when describing their 'Search Briefing,' this activity is no less relevant in the commercial field as it ensures that all those involved are aware of the information available at the time including any constraints imposed by court orders or other authorities. The following is based on the recommendations of Sammes and Jenkinson:

Answers to the following questions need to be addressed:

1. How many trained personnel are required?

2. How many teams are required, where do they need to be and at what date/time (this may be influenced by how many lawyers are available)?
3. How many sets of equipment are required and what should be in those kits?
4. Are any particular specialist skills required, if so how are they to be made available (e.g. someone with mainframe server knowledge may need to be at a specific location)?
5. How much storage media is required at each location and how can this be supplemented if necessary?
6. Will the services of another employee/ contractor be required (e.g. a system IT administrator to assist with shutting down servers or locating backup tapes or a resource at a CP to acquire the data locally)?

The output of the Initial Planning stage should be the Outline Plan detailing:

1. Personnel required (with site allocations if applicable) and team composition.
2. Equipment required at each site (including software, dongles, write-blockers and image storage media).
3. Start time at each site.
4. Estimate of duration of acquisition stage.
5. Details of other personnel involved.
6. Contact numbers of team leaders/lawyers/ client liaison distributed (if applicable).
7. Acquisition plan detailing target storage locations, protocol and key words (if applicable).
8. Applicable constraints—authorisation, physical, timing, and data.

Some authors delve into great detail in relation to the equipment that should be taken on site such as Sammes and Jenkinson (2007) whilst other authors such as Brown (2006) and Jones et al. (2006) include write-blockers of various types at the top of their recommendations for an 'onsite kit' (that are not included in Sammes and Jenkonson's list) as well as various software tools for acquiring digital data. The ACPO Guidelines make no recommendations at all for the equipment to be taken on site on the basis that the guidelines are for law enforcement personnel who would not normally deal with computers but whose role may cause them to come across computer equipment and their task is to seize that equipment. There is no consensus or standard set of guidelines for what equipment should be considered for inclusion in the onsite kit. The ADAM is not intended to provide this level of detail as the composition of the kit contents should be determined by the appropriate digital forensic professional.

ADAM Stage 2: The Onsite Plan

Having gained access to the site(s) in which relevant electronic data is thought to be stored, steps must be taken to ensure that the risk of potential evidentiary data being destroyed or removed is reduced as much as possible. Many writers of digital forensic guides, particularly those with a bias towards the work of law enforcement agencies, suggest that the whole 'crime scene' is immediately 'locked down' with the intention to obtain what Casey calls a "pristine environment" (Casey, 2004; Craiger, 2005; Sammes & Jenkinson, 2007). Whilst this may often be achievable for law enforcement investigations this is seldom practical in the commercial environment, a view supported by Kruse and Heiser (2002):

The ideal way to examine a system and maintain the most defensible evidence is to freeze it and examine a copy of the original data. However, this method is not always practical and may be politically unacceptable.

Brown (2006) suggests that one of the first actions upon arrival on site is to ensure the safety of the digital forensic practitioner(s) whilst some authors incorporate safety and security as one process (Sammes & Jenkinson, 2007). The ACPO

Guide (Association of Chief Police Officers, 2003) incorporates a section on safety and welfare but this is in relation to the potential for disturbing material being accessed during the course of the investigation. Guidelines for those involved in digital forensics within an organisation, normally involving incident response, tend to ignore the safety aspects. This may be because they have a more intimate knowledge of the environment, and tend to start with processing the electronic data. This approach has also been adopted in other circumstances such as the broader commercial environment (Casey, 2004; Farmer & Venema, 2005; Jones, et al., 2006). In order to provide a consistent and generic approach the ADAM contains basic procedures to be followed when attending the site as a pre-cursor to reviewing the Outline Plan. Rather than being too prescriptive and reducing the necessary flexibility required of a digital forensic practitioner the basic procedures are relatively 'high-level.'

Updating the Outline Plan

Once the digital forensic practitioner (or their proxy in the case of resources at a CP) is on site the Outline Plan needs to be reviewed and updated now that its various assumptions can be tested. There will often be areas of the plan that could not be completed at all prior to attending the site(s) containing the electronic data. If more than one site is involved there will be the need to have separate Onsite Plans to take account of the specific local circumstances. The overall goals will likely remain the same but the steps to be taken in order to achieve them may have to be altered. This is where the knowledge and experience of the digital forensic practitioner responsible for the particular site is critical. Few authors on forensic practice spare much time, if any, in describing a process for producing an onsite plan. Instead many simply state that the equipment likely to contain potential evidence should be identified (Baryamureeba & Tushabe, 2004; Casey, 2004; Pollitt, 2009). A more thorough approach is supported by Newman who suggests taking photographs of the scene, in line with most authors, but then goes on to list various activities that should be included in his 'Preliminary Survey':

1. Determine all the locations that might need to be searched.
2. Look for any specifics that must be addressed relating to hardware and software.
3. Identify possible personnel and equipment needs for the investigation.
4. Determine which devices can be physically removed from the site.
5. Identify all individuals who had access to the computer or electronic resources (Newman, 2007).

ADAM Stage 3: Data Acquisition

Some authors infer that the acquisition process is always undertaken in some 'ideal' environment where storage devices can be write-blocked (Jones, et al., 2006). McKemmish (1999) adopts a more practical view where he states that in certain circumstances "*changes to data are unavoidable*" (McKemmish, 1999, p. 1). His solution is to clearly identify and record the consequences of any actions undertaken. With a trend towards 'live' acquisition and given the technical nature of the devices (such as mobile phones and solid state drives), the environment (such as computer data stored in volatile memory) (Sutherland, Evans, Tryfonas, & Blyth, 2008), full disk encryption (Casey & Stellatos, 2008), and time/storage constraints (individual hard disk drives exceeding 2TB) (Gosh, 2004a) the concept of the 'ideal' environment is becoming even further removed from practice (Adelstein, 2006; Carrier, 2006; Leong & Leung, 2007). Given the many different potential scenarios, it would not be practical or appropriate to develop detailed guidelines that could be generally applied. Each organisation undertaking the acquisition of digital evidence

should have developed their own procedures to supplement those of the ACPO and ISO Guidelines, but inevitably, it is down to the practitioner to decide how these guidelines are to be applied in a particular set of circumstances.

It is the role of the digital forensic practitioner to determine the most appropriate technique to be employed and maintain documentation of all activities associate with data acquisition. This will include starting the 'chain of evidence' and other documentation such that they will be able to describe their actions and reasons to a court. In situations in which a third-party resource is used and not directly supervised they must be issued with very clear instructions including the requirement to document all their activities.

MODEL VALIDATION

As part of the DSRP methodology, the ADAM was initially tested by undertaking a 'demonstration' activity in which the processes undertaken in three previous investigations were compared to those that form the ADAM. Differences were highlighted, considered and appropriate changes were made to the ADAM. Two experienced digital forensic practitioners were then approached (one from commerce and one from law enforcement) to provide feedback on the practical aspects of the ADAM from their respective environments prior to the ADAM being sent for review by a panel of experts that included notable researchers in the field of digital forensics. After the feedback from the panel of experts had been considered and implemented, a panel of practitioners was then asked to assess the model and provide feedback and this too was considered and implemented.

The final version of the ADAM consists of a set of Guidance Notes, a three-stage Operation Presentation in the form of a narrative, which includes ADAM Principles, and a set of UML Activity diagrams (one for each stage of the ADAM). Specific organization-based operating procedures can be integrated into the ADAM as well as 'best practice' guidelines to ensure relevance of the process model for its use in a particular environment as well as accommodating future advances in technology.

FUTURE WORK

Having created a model for the process of acquiring digital data that accommodates new and emerging technology whilst also allowing for the needs of groups of practitioners operating in different environments, the next stage for research is to consider following the same process used to develop the ADAM in order to model other aspects of the DFP work, i.e. analysis and presentation.

CONCLUSION

The issues surrounding the acquisition of digital evidence from the cloud may finally force the 'traditional' approaches that have been struggling to be relevant in networked environments to be superseded by a 'new generation' of process models, such as the ADAM, that both prescribe (as an aid to DFPs) and describe (as an aid to the courts) the activities of those whose task it is to acquire, analyze, and present digital evidence. Courts in Australia and New Zealand have already seen flowcharts introduced to assist the jury in understanding 'scientific' evidence in much the same way as the UML Activity Diagrams of the ADAM are intended with some of these flowcharts having been produced by judges themselves (Ogloff, Clough, & Goodman-Delahunty, 2006). This indicates that the proposed new model has a good chance of gaining acceptance as a useful tool in the legal environment and so what is now needed is the adoption by digital forensic practitioners of the ADAM or similar process model based on the same concepts to enable the field of digital

forensics to justify its scientific credentials and accommodate new technologies as they arise.

REFERENCES

Adelstein, F. (2006). Live forensics: Diagnosing your system without killing it first. *Communications of the ACM*, *49*(2), 63–66. doi:10.1145/1113034.1113070

Agarwal, A., Gupta, M., Gupta, S., & Gupta, S. C. (2011). Systematic digital forensic investigation model. *International Journal of Computer Science and Security*, *5*(1), 118–130.

Armstrong, C. (2003). Mastering computer forensics. In Irvine, C., & Armstrong, H. (Eds.), *Security Education and Critical Infrastructures*. Dordrecht, The Netherlands: Kluwer Academic Publishers.

Association of Chief Police Officers. (2003). *Good practice guide for computer based evidence*. Retrieved from http://www.acpo.police.uk/asp/policies/Data/gpg_computer_based_evidence_v3.pdf

Baryamureeba, V., & Tushabe, F. (2004). *The enhanced digital investigation process model*. Paper presented at the Digital Forensic Research Workshop. New York, NY.

Beebe, N., & Clark, J. (2004). *A hierarchical, objectives-based framework for the digital investigations process*. Paper presented at the Digital Forensics Research Workshop 2004. New York, NY.

Brezinski, D., & Killalea, T. (2002). *Guidelines for evidence collection and archiving*. Retrieved from http://www.ietf/org/rfc/rfc3227.txt

Brown, C. (2006). *Computer evidence: Collection & preservation*. New York, NY: Charles River Media.

Buskirk, E. V., & Liu, V. T. (2006). Digital evidence: Challenging the presumption of reliability. *Journal of Digital Forensic Practice*, *1*(1), 19–26. doi:10.1080/15567280500541421

Calhoun, M. C. (2008). Scientific evidence in court: Daubert or Frye, 15 years later. *Legal Backgrounder, 23*(37).

Carrier, B. (2002). *Open source digital forensic tools: The legal argument*. Retrieved from http://www.digital-evidence.org/papers/opensrc_legal.pdf

Carrier, B. (2006). Risks of live digital forensics. *Communications of the ACM*, *49*(2), 56–61. doi:10.1145/1113034.1113069

Carrier, B., & Spafford, E. H. (2003). Getting physical with the digital investigation process. *International Journal of Digital Evidence*, *2*(2).

Casey, E. (2004). *Digital evidence and computer crime*. London, UK: Elsevier Academic Press.

Casey, E., & Stellatos, G. J. (2008). The impact of full disk encryption on digital forensics. *SIGOPS Operating Systems Review*, *42*(3), 93–98. doi:10.1145/1368506.1368519

Cheng, E. (2007). Independent judicial research in the Daubert age. *Duke Law Journal*, *56*, 1263–1318.

Ciardhuain, S. O. (2004). An extended model of cybercrime investigations. *International Journal of Digital Evidence*, *3*(1).

Cohen, F. (2011). Putting the science in digital forensics. *Journal of Digital Forensics. Security and Law*, *6*(1), 7–14.

Craiger, J. P. (2005). *Computer forensic procedures and methods*. Retrieved from http://ncfs.org/craiger.forensics.methods.procedures.final.pdf

Daubert v Merrell Dow Pharmaceuticals Inc 509 US at 579, 113 S.Ct. 2786, 125 L.Ed.2d 469 (1993).

Edmond, G. (2010). Impartiality, efficiency or reliability? A critical response to expert evidence law and procedure in Australia. *The Australian Journal of Forensic Sciences*, *42*, 83–99. doi:10.1080/00450610903258128

Farmer, D., & Venema, W. (2005). *Forensic discovery*. Reading, MA: Addison-Wesley.

Giannelli, P. C. (2007). *Scientific evidence* (4th ed.). Newark, NJ: Lexis Law.

Gillespie, A. A. (2012). Jurisdictional issues concerning online child pornography. *International Journal of Law and Information Technology*, *20*(3). doi:10.1093/ijlit/eas007

Gosh, A. (2004a). *Guidelines for the management of IT evidence*. Paper presented at the APEC Telecommunications and Information Working Group. New York, NY.

Gosh, A. (2004b). *HB 231:2004 information security risk management guidelines*. Sydney, Australia: Standards Australia.

Grant v Marshall FCA 1161 (2003).

Hargreaves, C. J. (2009). *Assessing the reliability of digital evidence from live investigations*. Cranfield, UK: Cranfield University.

Hutz, R. E. (2012, May 22). E-discovery: The relationship between cloud computing, e-discovery and privilege. *InsideCounsel*.

IOCE. (2002). *Guidelines for best practice in the forensic examination of digital technology*. Retrieved from http://www.ioce.org/fileadmin/user_upload/2002/Guidelines%20for%20Best%20Practices%20in%20Examination%20of%20Digital%20Evid.pdf

ISO/IEC. (2011). *Draft - Guidelines for identification, collection, acquisition, and preservation of digital evidence, CD 27037: ISO/IEC*. Retrieved from http://www.iso.org

Jones, K. J., Bejtlich, R., & Rose, C. W. (2006). *Real digital forensics*. Reading, MA: Addison-Wesley.

Kenneally, E. E. (2005). Confluence of digital evidence and the law: On the forensic soundness of live-remote digital evidence collection. *UCLA Journal of Law and Technology, 5*.

Kessler, G. C. (2010). *Judges' awareness, understanding, and application of digital evidence*. Davie, FL: Nova Southeastern University.

Kruse, W. G., & Heiser, J. G. (2002). *Computer forensics: Incident response essentials*. Reading, MA: Addison Wesley.

Kumho Tire Company v. Carmichael 526 U.S. 137; 1999 (1999).

Kunick, J. (2012, June 15). Technology: The promises and perils of the cloud. *InsideCounsel*.

Leong, R., & Leung, H. (2007). Deriving cse-specific live forensics investigation procedures from FORZA. In *Proceedings of the 2007 ACM Symposium on Applied Computing*. ACM Press.

Limongelli, V. (2008). Digital evidence: Findings of reliability, not presumptions. *Journal of Digital Forensic Practice*, *2*(1), 13–16. doi:10.1080/15567280701721913

Marcella, A. J., & Menendez, D. (2008). *Cyber forensics: A field manual for collecting, examining and preserving evidence of computer crimes* (2nd ed.). New York, NY: Auerbach Publications.

Mason, S. (2007). *Electronic evidence: Disclosure, discovery & admissibility*. London, UK: Butterworths.

McKemmish, R. (1999). *What is forensic computing?* Retrieved from http://www.aic.gov.au/publications/tandi/ti118.pdf

Meyers, M., & Rogers, M. (2004). Computer forensics: The need for standardization and certification. *International Journal of Digital Evidence*, *3*(2).

Moles, R. N. (2007). *The role and function of the expert witness*. Retrieved from http://netk.net.au/Reports/ExpertWitness.asp

Newman, R. C. (2007). *Computer forensics: Evidence collection and management*. London, UK: Auerbach Publications.

Ogloff, J., Clough, J., & Goodman-Delahunty, J. (2006). *The jury project: Stage 1 - A survey of Australian and New Zealand judges*. Melbourne, Australia: Australian Institute of Judicial Administration.

Peisert, S., Bishop, M., & Marzullo, K. (2008). *Computer forensics in forensis.* Paper presented at the Third International Workshop on Systematic Approaches to Digital Forensic Engineering. Oakland, CA.

Pollitt, M. (2009). The good, the bad and the unaddressed. *Journal of Digital Forensic Practice*, *2*, 172–174. doi:10.1080/15567280902882852

Reith, M., Carr, C., & Gunsch, G. (2002). An examination of digital forensic models. *International Journal of Digital Evidence*, *1*(3).

Rogers, M. K. (Ed.). (2004). *DCSA: A practical approach to digital crime scene analysis* (5th ed., *Vol. 3*). New York, NY: Taylor and Francis.

Rogers, M. K. (2006). DCSA: Applied digital crime scene analysis. In Tipton & Krause (Eds.), *Information Security Management Handbook* (5th ed.). New York, NY: Auerbach.

Sammes, T., & Jenkinson, B. (2007). *Forensic computing: A practitioner's guide* (2nd ed.). Berlin, Germany: Springer.

Smith, R. G., Grabosky, P. N., & Urbas, G. (2004). *Cyber criminals on trial*. Cambridge, UK: Cambridge University Press. doi:10.1017/CBO9780511481604

Solomon, A. (2010). *Privacy and the cloud*. Paper presented at the Cloud Computing Conference and Expo. New York, NY.

Stanfield, A. (2009). *Computer forensics, electronic discovery & electronic evidence*. London, UK: Reed International Books.

Steel, C. (2006). *Windows forensics: The field guide for conducting corporate computer investigations*. New York, NY: Wiley Publishing.

Stephenson, P. (2003). A comprehensive approach to digital incident investigation. *Information Security Technical Report*, *8*(2), 42–54. doi:10.1016/S1363-4127(03)00206-1

Sutherland, I., Evans, J., Tryfonas, T., & Blyth, A. (2008). Acquiring volatile operating system data tools and techniques. *SIGOPS Operating Systems Review*, *42*(3), 65–73. doi:10.1145/1368506.1368516

US-CERT. (2008). *Computer forensics*. Retrieved December 2008 from http://www.us-cert.gov/reading_room/forensics.pdf

Wiles, J. (Ed.). (2007). *The best damn cybercrime and digital investigations book period*. New York, NY: Syngress Publishing.

ADDITIONAL READING

Carrier, B., & Spafford, E. H. (2003). Getting physical with the digital investigation process. *International Journal of Digital Evidence*, *2*(2).

Carrier, B. D. (2006). Risks of live digital forensics. *Communications of the ACM*, *49*(2), 56–61. doi:10.1145/1113034.1113069

Cohen, F. (2011). Putting the science in digital forensics. *Journal of Digital Forensics. Security and Law*, *6*(1), 7–14.

Daubert v Merrell Dow Pharmaceuticals Inc 509 US at 579, 113 S.Ct. 2786, 125 L.Ed.2d 469 (1993).

Edmond, G. (2010). Impartiality, efficiency or reliability? A critical response to expert evidence law and procedure in Australia. *The Australian Journal of Forensic Sciences*, *42*, 83–99. doi:10.1080/00450610903258128

Kumho Tire Company v. Carmichael 526 U.S. 137 (1999).

Mason, S. (2007). *Electronic evidence: Disclosure, discovery & admissibility*. London, UK: Butterworths.

ENDNOTES

1 This is the main standard used by testing and calibration laboratories and was first published in 2001. This is a general purpose document concerned with management and quality procedures that do not specifically relate to computer forensic labs.

2 The environment in which the evidence is thought to reside.