The Advanced Data Acquisition Model (ADAM): A Process Model for Digital Forensic Practice

---

This thesis is presented for the degree of

Doctor of Philosophy of Murdoch University

By

Richard Brian Adams

2012

Declaration

I declare that this thesis is my own account of my research and contains as its main content work which has not previously been submitted for a degree at any tertiary education institution.

Signature:

Date: 5 March 2013

Acknowledgments

I would like to express my sincere gratitude to my supervisors, Dr Val Hobbs and Dr Graham Mann, for their unfailing support and encouragement – I could not have completed this thesis without them.

Special thanks are due to Phill Russo, Tim Thomas and Dr Colin Armstrong for their help and willingness to provide constructive feedback on my ideas and to all those who took part in the evaluation process.

Finally, I would like to acknowledge the love and support of my wife, Jane, and our children James, Matthew and Charlotte to whom I dedicate this work.

Abstract

Given the pervasive nature of information technology, the nature of evidence presented in court is now less likely to be paper-based and in most instances will be in electronic form . However, evidence relating to computer crime is significantly different from that associated with the more 'traditional' crimes for which, in contrast to digital forensics, there are well-established standards, procedures and models to which law courts can refer.

The key problem is that, unlike some other areas of forensic practice, digital forensic practitioners work in a number of different environments and existing process models have tended to focus on one particular area, such as law enforcement, and fail to take into account the different needs of those working in other areas such as incident response or 'commerce'.

This thesis makes an original contribution to knowledge in the field of digital forensics by developing a new process model for digital data acquisition that addresses both the practical needs of practitioners working in different areas of the field and the expectation of law courts for a formal description of the process undertaken to acquire digital evidence.

The methodology adopted for this research is design science on the basis that it is particularly suited to the task of creating a new process model and an 'ideal approach' in the problem domain of digital forensic evidence. The process model employed is the Design Science Research Process (DSRP) (Peffers, Tuunanen, Gengler, Rossi, Hui, Virtanen and Bragge, 2006) that has been widely utilised within information systems research.

A review of current process models involving the acquisition of digital data is followed by an assessment of each of the models from a theoretical

perspective, by drawing on the work of Carrier and Spafford (2003)[1], and from a legal perspective by reference to the Daubert test[2]. The result of the model assessment is that none provide a description of a generic process for the acquisition of digital data, although a few models contain elements that could be considered for adaptation as part of a new model.

Following the identification of key elements for a new model (based on the literature review and model assessment) the outcome of the design stage is a three-stage process model called the Advance Data Acquisition Model (ADAM) that comprises of three UML[3] Activity diagrams, overriding Principles and an Operation Guide for each stage. Initial testing of the ADAM (the Demonstration stage from the DSRP) involves a 'desk check' using both in-house documentation relating to three digital forensic investigations and four narrative scenarios. The results of this exercise are fed back into the model design stage and alterations made as appropriate.

The main testing of the model (the DSRP Evaluation stage) involves independent verification and validation of the ADAM utilising two groups of 'knowledgeable people'. The first group, the Expert Panel, consists of international 'subject matter experts' from the domain of digital forensics. The second group, the Practitioner Panel, consists of peers from around Australia that are digital forensic practitioners and includes a representative from each of the areas of relevance for this research, namely: law enforcement, commerce and

[1] Who provide a list of the essential requirements for a digital forensic process model
[2] This is a test originating from the United States that has been used by courts to assess 'scientific' evidence in various jurisdictions (for instance it is mimicked in a discussion paper by the Law Commission for England and Wales (Edmond, 2010)).
[3] Unified Modeling Language

incident response. Feedback from the two panels is considered and modifications applied to the ADAM as appropriate.

This thesis builds on the work of previous researchers and demonstrates how the UML can be practically applied to produce a generic model of one of the fundamental digital forensic processes, paving the way for future work in this area that could include the creation of models for other activities undertaken by digital forensic practitioners. It also includes the most comprehensive review and critique of process models incorporating the acquisition of digital forensics yet undertaken.

Table of contents

Figures

Chapter 1: Introduction to the research

This thesis addresses the fundamental issue that there is no comprehensive description for the process of acquiring digital evidence that can be applied by Australian practitioners operating in the different digital forensic areas of law enforcement, incident response (who tend to work mainly within their own organisation) and third-party providers of digital forensic services (who undertake their work on behalf of external clients, often lawyers). This is not an isolated weakness within the subfield of acquisition of digital evidence because, as Cohen (2011) points out, the whole field of digital forensics still lacks consensus in fundamental areas. By providing a formal model for a significant aspect of the digital forensic process this research will not only be of immediate value to digital forensic practitioners but it will establish a starting point from which other researchers can continue to develop the field's scientific credentials.

1.1 Background

Given the pervasive nature of information technology the nature of evidence presented in court is less likely to be paper-based as has previously been the case 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). This has required the courts in Australia and elsewhere to consider how to deal with this type of evidence.

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 Evidence Act 1995 (Cth) (Mason, 2007). 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 (2010) states that "…reliability assessments should focus on the technique and its accuracy as well as the proficiency of the operator/analyst" (p. 94). This issue of reliability means that courts pay close attention to the manner in which digital evidence has been obtained and in particular the process in which the data is captured and stored (Cohen, 2011; 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).

Australian Courts may apply methods used for testing scientific evidence to digital evidence presented before them and this is commonly based on American practice (Kessler, 2010; Moles, 2007) which is to apply the Daubert test, named after *Daubert v Merrell Dow Pharmaceuticals (U.S.) (1993)*. In this case the US Supreme Court determined that it is 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 Rules of Evidence rule 702 (Committee on the Judiciary, 2010)[4]. According to these rules the process for determining the admissibility of evidence requires that expert testimony must be derived from 'specialised knowledge' requiring that reliable principles and methods have been applied. This led to the court in *Daubert v Merrell Dow Pharmaceuticals (U.S.) (1993)* establishing what has become known as the Daubert test. In practice the Daubert test is often summarised as four[5] components that provide clarity around determination of 'sufficient facts or data' and 'reliable principles and methods' (Gosh, 2004a; Stephenson, 2003a):

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

Another American case, *Kumho Tire Company v. Carmichael (U.S.) (1999)*, expanded the Daubert test to allow for non-scientists to give expert

[4] This has often been identified as the judge taking on the role of 'gatekeeper' (Kessler, 2010)
[5] This thesis uses the list from the original court transcript although some references list a five-component test in which 'error rate' and 'standards' are separated.

evidence, such as engineers and other technical witnesses, as noted more recently by Gianelli (2007), Calhoun (2008) and Rogers (2006). This shows that despite the fact that the Daubert case was heard in 1993 its influence is still strong in relation to digital evidence, further demonstrated by the more recent consultation paper issued by the Law Commission for England and Wales which effectively mimics the Daubert test (Edmond, 2010). 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. This view has also been strongly expressed by Meyers and Rogers (2004), who warned of digital forensics being labelled as 'junk science' due to the lack of certifications, standards or peer-reviewed methods. This view is understandable given that the practice of digital forensics was initially undertaken by practitioners who were not scientists but law enforcement officers and only more recently has it become a role for IT professionals.

The United States Computer Emergency Readiness Team (US-CERT, 2012) also identify the immaturity of digital forensics as a significant issue and 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 recognised as a formal 'scientific' discipline (p. 1).

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). In relation to this question of evidence reliability, two of Palmer's (2001) six phases of digital forensics relate directly to the acquisition of digital evidence; Preservation and Collection. These two acquisition phases are open to challenges in relation to breaks in the chain of evidence, the integrity of the evidence, the completeness of the evidence or questioning the policies, procedures and resources used to gather the evidence. As Rogers (2004) points out "If doubt is cast on the initial collection and management of evidence, output from the other phases is moot" (p. 12).

The multi-jurisdictional, multi-environmental nature of cases results 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 (2004) suggests 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. Ciardhuáin goes on to state:

> A comprehensive model of cybercrime investigations is important for standardising terminology, defining requirements, and supporting the development of new techniques and tools for investigators (2004, p. 1).

Going further still, Trcek, Abie, Skomedal and Starc (2010) suggest the notion of an widely agreed-upon 'template legislation' that would harmonize the practice of digital forensics on an international basis.

Many researchers writing in this field have adopted their own terminology for describing their digital forensic process model. However, rather than being generic these models have often been aimed at particular environments, such as law enforcement (Rogers, 2006) and incident response (Cummins & Lowry, 2003; Mandia & Prosise, 2001; Stephenson, 2003b). Although some researchers have tried to utilise existing formal languages and methods rather than invent their own terminology they too have tended to focus on a particular environment (M. M. Pollitt, 2007). There has therefore been little progress in refining and defining a generic digital forensic process since the initial meeting of the Digital Forensic Workshop in 2001 (Cohen, 2011; ISO/IEC, 2011; Nance, et al., 2010; Scholtz & Narayanan, 2010; Trcek, et al., 2010; US-CERT, 2012). Furthermore, Agarwal et al (2011) note that recent process models have been mainly ad hoc and they recommend that more research should be carried out in this area.

1.2 Research problem

These considerations lead us to the research problem which is that:

> *There is no formal generic process model for the acquisition of digital data that encompasses the activities of practitioners working in the different environments of law enforcement, commerce and incident response such that it can assist courts of law in determining the reliability of the acquisition process employed to collect potential digital evidence.*

1.3 Research objective and questions

1.3.1 Research objective

The research objective is to develop a formal model of the process for the forensic acquisition of digital data that is generic in that it can be employed by digital forensic practitioners in the fields of commerce, law enforcement and incident response. The objective therefore consists of two goals:

- There must be a formal representation of the model
- The model must be relevant to the fields of commerce, law enforcement and incident response.

1.3.2 Research questions

In order to achieve the research objective the following three research questions need to be answered:

1. What are the essential components necessary in a model that describes a generic and forensically sound digital data acquisition process?
2. How can the identified components for a generic and forensically sound digital data acquisition process be combined into a working model?
3. What is a suitable way for describing, presenting and using model for acquiring digital data?

In obtaining answers to these research questions this research will enable the development of a new model for the forensic acquisition of digital data that can be used by practitioners working within the fields of law enforcement, incident response and third-party services.

1.4 Research Scope

1.4.1 Limitation of process scope

McKemmish (1999) defines the process of forensic computing as "…the process of identifying, preserving, analysing and presenting digital evidence in a manner that is legally acceptable" (p. 1). McKemmish also describes four key elements associated with this process:

- The identification of digital evidence
- The preservation of digital evidence
- The analysis of digital evidence
- The presentation of digital evidence.

Although many attempts have been made to develop a model that covers all aspects of this definition of digital forensics the process scope of this research will be limited to the context of digital evidence acquisition which only covers the *first two elements* of McKemmish's (1999) definition. This limitation has been introduced on the basis that a review of the literature suggested that the task of incorporating the other key elements, particularly the analysis stage, would be beyond the limits of a single research thesis, particularly in the light of criticism of many other models which is that they have tried to take on too big a task making them unwieldy and complex (Rogers, 2004; Schatz, 2007).

1.4.2 Limitation of environment scope

Although digital forensic tools and processes are employed across a number of environments the environment scope for this research has been restricted to the three areas of 'commerce', 'incident response' and 'law enforcement' digital forensic activity within Australia. The military environment has been excluded on the basis that for anyone outside of this area of the armed forces it is extremely difficult to obtain data on their processes and procedures and it has therefore been considered practical to only identify essential key elements across the three stated environments.

The geographical restriction to Australia is imposed because of the complexity of evaluating the model against the needs of a large number of jurisdictions where digital evidence may be presented, although this could be an element of future research. However, this restriction will not prevent the new model from having relevance in other environments that have a similar legal basis for assessing digital evidence.

1.4.3 Limitation of model detail scope

The field in which computer forensic practitioners work is constantly evolving through advances in technology and tools (Garfinkel, 2010, p. 66; Mercuri, 2005; Schatz, 2007). Given this rapidly-changing environment, from a practical perspective, it would be highly unlikely that every situation could be anticipated and the necessary detail instructions provided as part of the new process model (Garfinkel, 2010, p. 66; McDermott & Fox, 1999). Furthermore, from a risk-mitigation perspective, a low-level prescriptive list of actions could involve practitioners in complicated legal challenges as they may have to explain why they didn't follow every single item on the list where many will be irrelevant in the particular circumstances (Garfinkel, 2010, p. 67). Limiting the level of detail of the new model, and thereby making it more practical and therefore more likely to be adopted, addresses the issue raised with respect to some other process models that have been criticised for their large amount of detail which is claimed to have made them cumbersome and too specific or complex to use (McDermott & Fox, 1999; Reith, et al., 2002; Schatz, 2007; Selamat, et al., 2008). Schatz (2007) refers to this issue as the 'complexity problem' which relates to the ever-changing technical environment in which digital forensic practitioners work that quickly makes lists that are too prescriptive become obsolete very quickly.

In terms of the 'target audience', unlike some earlier process models where the practitioner is expected to have very little (if any) computer forensic experience the new model is aimed at those operating in the area of computer forensics who are professionals and who already have the necessary skills and experience for undertaking data acquisition together with existing processes and

procedures (Brown, 2006; Bunting & Wei, 2006; Calhoun, 2008; B. D. Carrier, 2006; Jones, et al., 2006; Kent, et al., 2006). The new model is intended to help structure their existing processes in a formal way that can be readily described to the court instead of completely replacing them. In addition, existing procedures and practices.

The need for practitioners to have specific guidance in new areas of technology is already addressed in the form of academic papers and other publications (many of which are available online) that are constantly being updated and that can assist practitioners with new or unfamiliar technology and best practices (Kim, Hong, & Chung, 2008; Sammes & Jenkinson, 2007; Savoldi & Gubian, 2008; Sutherland, Evans, Tryfonas, & Blyth, 2008).

1.4.4 Excluded from scope

The field of digital forensics is continually changing as new technology is developed both as the focus of a digital forensic practitioner's activities and in relation to the tools available to undertake those activities. This has led to the difficulties being faced by the U.S. National Institute of Standards and Technology (NIST) who have been unable to keep pace with new digital forensic software being released or even updates to existing software. For instance, the NIST handbook revised on 1 February 2012 (Lyle, 2012) refers to the testing results of EnCase version 6.5, but by 23 February 2012 the production version of EnCase was v7.03. This problem comes about because the tools themselves are victims of the fast-moving environment of digital forensics and the need for those "… tools designed solely for forensic purposes to keep abreast of the broad range of technology" (Slay & Beckett, 2007, p. 4). Therefore this research does not attempt to address the issue of the reliability of the vast array of tools or

computer systems that a digital forensic practitioner may choose to utilise in the course of their work.

1.5 Research contribution

This thesis adds to the body of knowledge by building upon existing digital forensic research in relation to process models and synthesises key elements to produce the first formal generic model for the acquisition of potential digital evidence, the ADAM. In addition, it contains the most comprehensive review to date of existing process models relating to the field of digital forensics. Finally, by demonstrating the instantiation of the theoretical requirements of a digital forensic acquisition process model through the adoption of the Unified Modelling Language (UML)[6] this thesis paves the way for using UML to describe the other aspects of the digital forensic environment that could lead to a complete formal description encompassing all digital forensic activities.

1.6 Methodology

1.6.1 Selection of methodology

This section presents the methodology used in this research. The methods and processes used in this research are discussed in relation to how they address the research objectives.

Design science (A. Hevner & Chatterjee, 2010; AR Hevner, March, Park, & Ram, 2004; A. R. Hevner, 2007; Kuechler & Vaishnavi, 2008; Lee, 2000;

[6] Controlled by the Object Management Group at http://www.uml.org/

McKay & Marshall, 2007; Peffers, et al., 2006; Storey, 2008; Venable, 2006) has been selected as the methodology used for this research. The selection of Design Science rather than alternatives such as Requirements Engineering (Nuseibeh & Easterbrook, 2000) was made on the basis that it is particularly suited to the task of creating a new process model (an artefact). Armstrong & Armstrong (2010) point out that with design sciences' focus on designing solutions it is an 'ideal approach' in the problem domain of digital forensic evidence.

The design science paradigm is concerned with the creation, and subsequent evaluation, of IT artefacts within an organisational context to solve specific problems (A. Hevner & Chatterjee, 2010; AR Hevner, March, Park, & Ram, 2004).These artefacts include constructs, models, methods and instantiations (real-life products such as prototype systems) (AR Hevner, et al., 2004). Design science has as its goals the creation of effective artefacts and utility (Applegate, 1999; AR Hevner, et al., 2004; Simon, 1996).

Hevner et al (2004) make the distinction between routine design and design science research by stating that routine design applies existing knowledge, such as current best practices, to organisational problems whereas design science research addresses either unsolved problems in new ways or solved problems more efficiently or more effectively.

Design science researchers come to understand the problem that is addressed by the artefact and its appropriateness for providing a solution through the artefact's construction and use in the field (Nunamaker, Chen, & Purdin, 1990). In so doing they are not seeking 'truth' but attempting to improve an existing situation through the application of the artefact having considered the environment in which it is to be deployed and the intended users of the artefact

(McKay & Marshall, 2005). McKay and Marshall argue that because Information Systems usage is within an environment in which some part of human activity is aided by computer technology the context and use of such systems should be considered when carrying out research in this area. In addition, Applegate (1999) has called for 'industry-relevant' research as opposed to adopting the more traditional functionalist paradigm that is usually associated with the IS discipline.

The artefact associated with this research is a new model that describes the forensic acquisition of digital data, the Advanced Data Acquisition Model (ADAM). The organisational context is that of a generic digital forensic practitioner, i.e. they may be working in law enforcement (in its broadest meaning), commercial practice or incident response. This research addresses an unsolved problem: that there is no formal generic model for the acquisition of digital data that encompasses the activities of practitioners working in the different environments of law enforcement, commerce and incident response.

1.6.2 Process model for the research

A paper produced by Hevner et al. (2004) on the topic of design science was intended to present design science as an alternative paradigm for IS research and as such it does not provide detail on the actual process for undertaking that research (A. Hevner & Chatterjee, 2010; Venable, 2006). Nunamaker et al (1990) place the building of the artefact as the central activity but Venable (2006) argues that research papers in design science have neglected to emphasise the importance of theory building as a key aspect of design science research and therefore proposes an alternative framework which has theory as the central role.

While both the Venable and Nunamaker et al frameworks are useful as high-level guides for this research they lack sufficient detail in their application.

The process model selected for this research is the Design Science Research Process (DSRP) model developed by Peffers, Tuunanen, Gengler, Rossi, Hui, Virtanen and Bragge (2006) that has been frequently used within information systems research[7]. The DSRP is intended to meet three objectives: (1) to be consistent with prior literature; (2) to provide a nominal process model for doing DS research and (3) to provide a mental model for presenting and appreciating DS research in IS. From the synthesis of the common design process elements Peffers et al developed the DSRP that consists of six activities as shown in Figure 1.

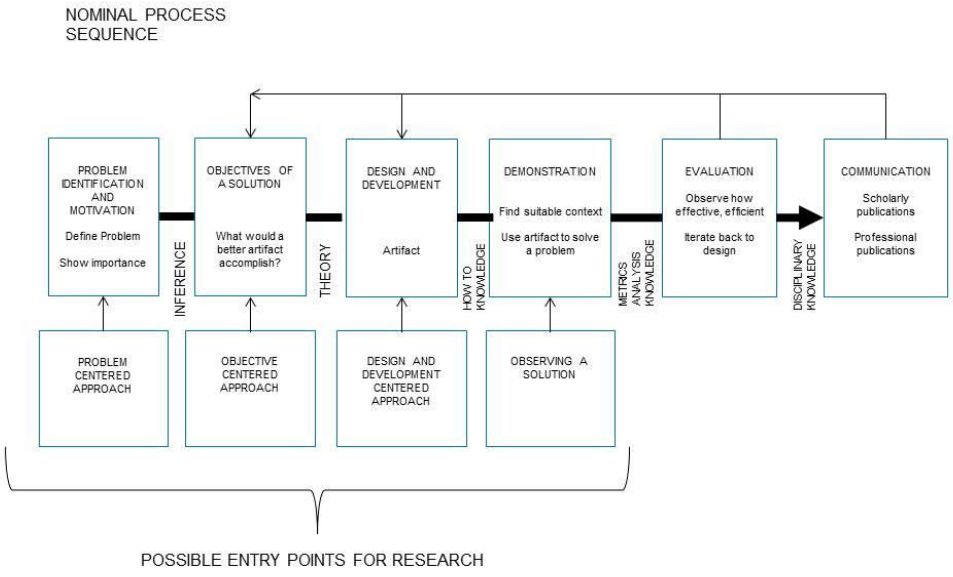

Figure 1 Design Science Research Process (DSRP) model after Peffers et al (2006)

[7] The model has been cited over 60 times in the ACM Digital Library http://dl.acm.org/citation.cfm?id=1481768

Brief descriptions of the activities in the DSRP are outlined below:

- **Activity 1**

  The first of the activities, 'Problem Identification and Motivation', involves establishing the problem to be addressed and justifying the research based on the perceived benefits of the resulting artefact.

- **Activity 2**

  This involves creation of the 'Objectives of a Solution' and requires the researcher to define the objectives which will be based on the problem to be solved.

- **Activity 3**

  The activity 'Design and Development' involves the creation of the artefact.

- **Activity 4**

  For the 'Demonstration' activity the artefact is used in some appropriate environment to solve the stated problem.

- **Activity 5**

  In the 'Evaluation' activity the performance of the artefact is reviewed with reference to the stated objective(s) from activity 2. It may be the case that at this stage the researcher considers that the artefact requires further design and development and therefore resorts to activity 3 as part of an iterative process.

- **Activity 6**

  The final activity is 'Communication' in which the researcher puts forward their research to add to the body of knowledge in their field. Peffers et al (2006) identify the need for communication, initially

proposed by both Archer (1984) and Hevner et al (2004), in order to publicise the problem, its significance and the resulting artefact. This communication should be addressed to practicing professionals, academics and other relevant parties.

Peffers et al (2006) identify several points in relation to the activities that comprise the DSRP at which a researcher may start their research process (Figure 1). The entry point for this research is now discussed.

1.6.3 Applying the methodology to the research problem

This research has as its focus the problem that there is currently no generic process model for the digital forensic acquisition process. The research is therefore based on a 'problem centred approach' and as such the entry point in the DSRP is at the first activity.

The following sections describe how the chosen methodology will be followed in the course of this research. In addition, as the DSRP does not include the low-level detail of how to carry out the activities within the individual stages; this section will also describe the process that will be followed with reference to the appropriate methodologies.

DSRP Activity 1 - Problem Identification and Motivation

The problem that this thesis addresses is:

> *There is no formal generic model for the acquisition of digital data that encompasses the activities of practitioners working in the different environments of law enforcement, commerce and incident response.*

Checkland and Poulter (2006) consider a real-world problematic situation that requires some form of intervention in order to improve it. This intervention requires the identification and analysis of a given problem situation by a researcher to develop a deep understanding of the problem area in order that an appropriate solution can be identified (Rhalibi, England, & Hanneghan, 2005). A deep knowledge of the problem area for this research will be satisfied through an extensive review of the associated literature with respect to relevant process models added to the thesis author's own practitioner experience in the domain of computer forensics.

DSRP Activity 2 - Objectives of a Solution

The objective of this research is to develop a formal model of the process for the forensic acquisition of digital data that is generic in that it can be employed by digital forensic practitioners in the fields of commerce, law enforcement and incident response.

DSRP Activity 3 - Design and Development

The contributions from previous researchers in the literature review, personal experience and interactions with other digital forensic practitioners will be used to create the new model. For the design and development stage the top-level approach taken will be to:

1. **Identify criteria against which existing models will be assessed**

   A review of the comments from other researchers on existing models that are relevant to this research will be used to formulate criteria for the overall assessment of the models or to identify existing criteria that may be employed in this way. These will constitute the Assessment Criteria.

In addition to the identified assessment criteria the models will also be considered in the light of the Daubert tests (Supreme Court of the United States, 1993) as described on page 2. The two methods of assessment will be considered for relevance following on from the argument presented in 1.1 above in which the appropriateness of the Daubert test was brought into question with regard to assisting a court of law to assess the scientific merit of the process of digital data acquisition.

2. Evaluate existing models against criteria

Each existing model will be reviewed to determine which, if any, of the identified assessment criteria have been met by that model. For each model the results of the comparison will be stated and then the overall results summarised.

3. Identify common requirements across different environments

The environments for this research are commerce, incident response and law enforcement. Those models most closely meeting the assessment criteria will be considered for their possible contribution to the ADAM. A set of model attributes will be constructed to obtain both the *core* elements that are common across the three areas of digital forensic practice that form the focus of this research as well as any innovative suggestions made by individual researchers that might enhance the ADAM.

4. Propose a new model incorporating the requirements of the different environments

The contributions of previous researchers through their process models will be used as the basis for the new model whilst paying particular

attention to ‘domain-specific’ attributes (i.e. those associated specifically with either the commerce, incident response or law enforcement environments) to ensure that they are accommodated. Attention will also be paid to criticisms of previous models to gain insight into potential design or implementation pitfalls whilst ensuring that the model remains ‘forensically sound’.

DSRP Activity 4 - Demonstration

The purpose of the model is to describe the data acquisition activities of digital forensic practitioners and therefore the ‘appropriate environment’ for the demonstration activity required by the DSRP will be addressed by applying the ADAM within a commercial computer forensic service provider. The aim of the Demonstration activity (covered in Chapter 5) will be to determine how well the model compares with a sample of previous cases based on documentation produced contemporaneously. Given the confidential nature of the type of documentation being examined and its restricted access the thesis author will take advantage of his position within a service provider of digital forensic services by undertaking the Demonstration activity in-house. This also has the advantage that any obvious shortcomings in the ADAM can be addressed without impinging on the time of external reviewers. As this activity only constitutes a pilot trial the fact that it is to be performed within the thesis author’s own environment will not affect the independent evaluation of the ADAM that occurs in the following activity.

DSRP Activity 5 – Evaluation

Cleven et al (2009) state that, in order to realise utility when developing an artefact based on design science research, attention should be given to two

fundamental requirements which are ‘relevance’ and ‘rigour’. Relevance requires that the artefact addresses a real business need whilst rigour requires the researcher to appropriately apply the existing body of knowledge.

The evaluation activity will be conducted by two independent panels of external reviewers who between them will be able to address the relevance aspect of the development of the ADAM. With regard to the Cleven et al ‘rigour’ requirement the issue of enhancing the credibility of this research through triangulation of data (Creswell, 2005) has been balanced with the practical aspects of obtaining quality feedback through in-depth reviews by authoritative reviewers. Bruce (2007) points out that the trustworthiness of the reporting is a more significant factor for credibility than the number of ‘data events’ and so, despite the relatively small number of reviewers planned to assist with this research, they are all authorities within the field of digital forensics whose feedback should be both insightful and reliable.

DSRP Activity 6 – Communication

As the research is presented in the form of a thesis, the Communication activity cannot be completed by the time of its submission. However, a submission detailing the potential for ADAM to be deployed in a ‘cloud’ environment has been accepted for publication and will appear in a refereed book chapter to be published in December 2012 [8]. The communication aspect of the DSRP will also be covered with respect to academic knowledge through direct communications with academic leaders in this field (also as part of the

[8] IGI Global (Cybercrime and Cloud forensics: Applications for Investigative Processes, Chapter 5- The Emergence of Cloud Storage and a New Digital Forensic Process Model

Evaluation process) and publications in refereed journals together with the publication of this thesis within the Murdoch University Research Repository[9].

With respect to communicating with practitioners, this will be accomplished through the involvement of the High Technology Crime Investigators Association and by introducing the ADAM as part of a postgraduate course in the Centre for Forensic Science at the University of Western Australia (course ref. FNSC8617 – Forensics and Information Technology).

1.7 Outline of the thesis

Chapter 1 (Introduction to the research) provides a brief summary of the digital forensic environment and highlights the importance of digital evidence acquisition. The challenges faced when presenting digital evidence in court are reviewed and the contribution this thesis intends to make to the field stated, including the methodology that will be employed and the limitations of this research.

Chapter 2 (Literature review) will provide a general review of the field of digital evidence followed by detailed review of previous process models involving the forensic acquisition of digital data.

Chapter 3 (Requirements) will introduce the Assessment Criteria and cover the process for identifying the requirements for the new model by evaluating each of the models from the literature review against the Assessment Criteria. The essential components of the new model will be identified.

---

[9] http://researchrepository murdoch.edu.au/view/types/thesis.html

Chapter 4 (Design and development) will describe the design activity for the ADAM together with the rationale behind the requirements for each of the model's stages.

Chapter 5 (Demonstration) will cover an appraisal of the ADAM through the Demonstration activity that involves reviewing the contemporaneous documentation from three previous in-house investigations and comparing the activities against the ADAM. This chapter will also include a walkthrough of the model using four scenarios. Based on the results of the Demonstration process, amendments to the ADAM will be identified in preparation for its submission to the external reviewers consisting of a Panel of Experts and a Panel of Practitioners.

Chapter 6 (Evaluation) will describe the composition of the Expert and Practitioner Panels, the tasks they were set and the results of their feedback including detailed changes to the ADAM.

Chapter 7 (Conclusion) will discuss the limitations of this research together with the potential future research opportunities. The research will be summarised in relation to the research objective and its contribution to the field of digital forensics stated. Finally, the forums in which this research has been, or will be, communicated will be identified.

1.8 Summary

In this chapter the justification for this research has been set out and background information in relation to the research problem and the generic environment for digital forensics has been provided. The research problem has been defined and the research questions stated. The selection of the Design

Science research methodology has been covered and the process of applying the selected methodology to the research question based on the Design Science Research Process of Peffers, Tuunanen, Gengler, Rossi, Hui, Virtanen and Bragge (2006) is described together with the thesis structure and outline.

Chapter 2: Literature review

2.1 Introduction

In relation to the DSRP used for this research this chapter will cover the 'knowledge of the state of the problem' and the 'current solutions'. This chapter first presents a literature review on the field of digital evidence. This provides the necessary background for the review of previous process models involving the forensic acquisition of digital data.

The review of previous models was undertaken using online data resources accessed via the Murdoch University library such as ScienceDirect and the ACM Digital Library. Online search engines were also used to identify conference papers, personal websites and university repositories. The following free-text search terms were used in various combinations and forms: *digital, computer, forensics, process, models, cyber, acquisition, imaging, activities, capture, standards, guidelines, incident response, crime and evidence*.

Several papers provided summaries of relevant process models and these were cross-checked to identify any missing models or references. The review suggested three central themes which provide the framework for this chapter. These themes are:

- The use of 'ad hoc' design elements
- Adopting a 'process flow' approach
- Employing some form of 'scientific' approach.

2.2 Digital evidence

Prior to the existence of digital data storage devices the Best Evidence Rule (in use since the 18th century) meant that the original writing, recording or photograph needed to be produced in court unless these had been destroyed or were unavailable in which case a certified copy or duplicate was admissible (Steel, 2006). This Common Law rule of 'best evidence' had been applied in many jurisdictions, including Australia, but over the years there have been various challenges, particularly with respect to differences between hard copy (paper-based) and soft copy (digital data based) records (Argy, 2006). Some examples of these differences are:

- There may be differences between hard copy and soft copy versions of a document such that some information associated with the document may only be visible during the examination of the digital version, e.g. comments and alterations
- Hard copy documents need no special tools and can be viewed and read by the naked eye, whereas soft copy documents require the appropriate hardware and software
- Soft copy documents can easily be altered
- Soft copy documents can be easily copied and disseminated.

In addition, unlike a paper document, the act of viewing a digital document or record by using a computer and a software application or other facility can cause changes to be made to the original data contained on the digital storage device, i.e. the original evidence is no longer in the form it was in when it was obtained. The requirement to produce original documents was abandoned in some states through the introduction in Australia of the *Evidence Act 1995 (Cth) (Austl.)* that applies to the Federal Court, New South Wales, Australian Capital Territory and Tasmanian proceedings and is in the process of being adopted by other Australian jurisdictions as the Uniform Evidence Acts. Section 51 of the Uniform Evidence Acts now allows for the copy of a document to have the same evidentiary status as the original.

The Uniform Evidence Acts defines a document as any record of information and includes:

1. Anything on which there is writing;
2. Anything on which there are marks, figures, symbols or perforations having a meaning for persons qualified to interpret them;
3. Anything from which sounds, images or writings can be reproduced with or without the aid of anything else; or
4. A map, plan, drawing or photograph.

The wording of the Uniform Evidence Acts also means that a digital storage device is itself a document and in relation to computer records the Evidence Acts in Victoria, Queensland and South Australia specifically state that

evidence derived from computer records will be admissible (although subject to certain conditions of reliability). Whilst the remaining jurisdictions do not provide specific provisions, each of them recognise a copy of a computer record (Argy, 2006).

The "conditions of reliability" are generally the same for most jurisdictions and Steel (2006, p.26) states that electronic copies of data are admissible provided that:

1. They were from the indicated source
2. They were acquired using proven tools and techniques
3. They have not been altered since the time of acquisition.

The use of "proven tools and techniques" is consistent with the Daubert test mentioned in 1.1. In relation to Steel's "conditions of reliability" a process methodology that ensures that comprehensive notes are maintained from the start of the acquisition process will aid in addressing condition (1) by confirming the source of the data; it will aid in addressing the need to show the use of "proven tools and technique" required in condition (2) by recording which tools and techniques were adopted (assuming the digital forensic practitioner has made appropriate choices in this regard), and it will also assist in meeting condition (3) by showing that the data has not been altered since it was acquired through the recording of hash values (Schwarz, Newby, & Carroll, 2009; Steel, 2006).

A further aspect of reliability in relation to the activities of digital forensic practitioners who are handling digital evidence is the concept of "forensically sound tasks" as identified by Rogers (2006) who states that they are derived from properties of digital forensics and comprise of Authenticity, Chain of Custody, Integrity, Minimization and Reproducibility. Rogers cites McKemmish (1999) and Mocas (2004) as sources for these properties.

2.3 Standards and Guidelines in data acquisition

There are significant differences between the activities associated with law enforcement agencies and those practicing digital forensics in another environment. Where there does seem to be a large degree of consistency is in acceptance of the basic principles associated with the handling of digital devices, although there are still many issues surrounding the precise implementation of these principles in the different environments. Noblett et al (2000) suggest a 'Three-Level Hierarchical Model for Developing Guidelines for Computer Forensic Evidence' on the basis that despite short-term changes within the environment in which digital forensic practitioners work there should be a consistent long-term standardised approach to their activities. In order to achieve this, the three stages of the Noblett et al model include a limited number of overarching principles which are then reflected in policies/practices which then lead to specific procedures and techniques. This hierarchy moves from industry best practice principles through to organisational polices for ensuring quality and efficiency and culminates in those activities that are likely to be introduced or modified to cater for changes in technology such as the introduction of a new

software tool or the release of a different type of storage device. Common areas for identifying the details of best practice are published standards and guidelines.

Standards Australia is the Australian non-government body given responsibility by the Commonwealth Government to meet Australia's need for "contemporary, internationally aligned Standards and related services" (Standards Australia, 2012a). Standards Australia provides the following wide-ranging definition for a Standard:

> 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 (Standards Australia, 2012b).

The following sections summarise the various references and guides that are associated with digital data and legal processes. The first two references are described as Standards with the remainder being 'guides' or 'guidelines'.

2.3.1 International Organization for Standardization (ISO)

The main international body that is relevant to standards within the field of digital forensics is the International Organization for Standardization[10] which is a non-government organisation and is an international standard-setting body that is composed of representatives from 164 countries[11], one of which is

[10] http://www.iso.org/iso/home htm
[11] As at September 2012

Standards Australia[12]. ISO is based in Geneva, Switzerland and although it has no government-enforced powers the standards that it creates are often adopted as law 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. 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[13]. The ongoing contribution of the Australian Standards Working Group, of which the author of this thesis is a member, is currently being coordinated by Ajoy Gosh who has authored previous standards and guidelines in this area (Gosh, 2004a, 2004b) with input from law enforcement, education and commerce.

2.3.2 British Standards Institute (BSI)

The British Standards Institute 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 digital evidence. However, the standard relates to the production of electronic documents that may be required as evidence of business transactions and provides advice for practices and procedures involving information management systems.

---

[12] http://www.standards.org.au/

[13] The author is a member of the Australian Standards working group for this document and is therefore aware of its contents and structure.

In contrast to the limited number of Standards associated with the field of digital forensics there are several guidelines with each having a particular focus area such as law enforcement, electronic discovery, commercial digital forensics and incident response. The main references encountered during the literature review are now covered in more detail.

2.3.3 Association of Chief Police Officers (ACPO) Guide

The UK National Hi-Tech Crime Unit produces (on behalf of the Association of Chief Police Officers) its Good Practice Guide for Computer Based Electronic Evidence (Association of Chief Police Officers, 2003) which contains definitions of the four Principles:

> *Principle 1*: No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be relied upon in court.
>
> *Principle 2*: In exceptional circumstances, where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.
>
> *Principle 3*: An audit trail or other record of all processes applied to computer based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.
>
> *Principle 4*: The person in charge of the investigation (the case officer) has overall responsibility for ensuring that the law and these principles are adhered to.

Fundamental to the concept of work undertaken in a forensic environment is the ability to use any material or information discovered in a court of law. As quoted above, Principles 1 and 2 require that, if possible, the original digital 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.

2.3.4 International Organization on Computer Evidence (IOCE)

In general terms the ACPO rules are mirrored by the International Organization on Computer Evidence in its draft guidelines (I.O.C.E, 2002) which themselves are based on the ISO 17025 Standard[14]. The IOCEs purpose is stated as being a forum with an international focus in which law enforcement agencies can exchange information in relation to 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

[14] 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.

- An individual is responsible for all actions taken with respect to digital evidence whilst the digital evidence is in their possession.

2.3.5 McKemmish's rules

McKemmish (1999) introduces four rules that must be followed by digital forensic practitioners during the course of their work but although they provide the framework under which the digital forensic practitioner should be working they do not provide detailed guidance (although McKemmish does provide justification and examples of their application in context). McKemmish's rules are:

- **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**: While 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.

2.3.6 Gosh's guidelines

The focus of the document 'Guidelines for the Management of IT Records' (Gosh, 2004b) is to assist organisations to 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.

2.3.7 Brezinski & Killalea's guidelines

The document 'Guidelines for Evidence Collection and Archiving'(Brezinski & Killalea, 2002) is a Network Working Group memo that is focussed on incident response. It does however 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.

2.4 The First Digital Forensic Research Workshop

The First Digital Forensic Research Workshop (DFRWS) took place in 2001 and included a session titled "A Framework for Digital Forensic Science" whose stated purpose was to "Build a taxonomy to guide and direct research" and "Identify the areas or categories that define the 'universe' of Digital Forensic Science" (Palmer, 2001, p. 21). Palmer suggested that digital forensic practitioners, whose activities are investigative in nature, would benefit from a properly categorized process.

The first attempt at the 'properly categorized process' appeared in the DFRWS's final paper (Palmer, 2001) and consisted of elements that had been included on the basis that they were derived from processes used in digital forensic analysis, although with the recognition that not all of them may come under the heading of 'forensic'. Getting agreement on exactly what constitutes the 'forensic process' seems to have been problematic with the final summary being produced that describes the included tasks as being "…subject to the least confusion" amongst practitioners (Palmer, 2001, p. 23).

The DFRWS produced a summary of the 'major categories' for the forensic process and 'candidate techniques or methods' based on what "…appears to be used in digital forensic analysis" (Palmer, 2001, p. 17), although the term 'preservation' appears four times under different categories. The DFRWS name is now used to describe the US non-profit organisation that supports research in the field of digital forensics.

2.5 Review of digital forensic process models

The models identified through the online search fall into three themes of ‘ad hoc’ models, ‘process flow’ and ‘scientific’ approaches. The key features of these models are now covered in the following sections.

2.5.1 Ad hoc digital forensic process models

In this part of the literature review the models have been grouped on the basis that they do not conform to a recognised methodological approach. Each of the authors has presented their model in their own unique way except for a few instances where they have built upon a previous ad hoc model. The models are presented in chronological order.

2.5.1.1 The Abstract Digital forensics Model (ADFM)

Reith et al (2002) built upon the initial framework of the DFRWS and claimed to have abstractly defined common steps from previous forensic protocols. They comment that the steps reflect the traditional forensics approach applied to a digital context. The ADFM is based on 9 components in relation to evidence: Identification, Preparation, Approach strategy, Preservation, Collection, Examination, Analysis, Presentation and Returning. These components are seen as being a complete representation of the process undertaken by a digital forensic practitioner.

Reith et al introduced the concept of ‘digital forensics’ in order to include all forms of digital storage rather than what they suggest is the more narrow definition of ‘computer forensics’.

In relation to digital evidence acquisition the first 5 steps of the Reith et al model (Identification, Preparation, Approach Strategy, Preservation and Collection) would seem to be relevant although, based on its description, the first step seems to be associated with some form of network/infrastructure attack rather than a generic forensic process. In practice Steps 2 and 3 (Preparation & Approach Strategy) could perhaps not be separated but grouped together under 'Planning'. This concept is supported by Baryamureeba & Tushabe (2004) who point out that upon receiving notification of an event the techniques to be used in the investigation will be part of the response, although they go on to say that in general terms the Reith et al model is a good representation of the forensic process.

2.5.1.2 Integrated Digital Investigation Process (IDIP)

The Integrated Digital Investigative Process (IDIP) developed by Carrier and Spafford (2003) adopts physical crime scene processes for their digital crime scene with the computer being treated as a 'door to another room'. In order to clarify the differences (and similarities) between a physical and digital crime scene Carrier and Spafford provide the following definitions (together with their emphasis):

- **Physical Crime Scene:** The physical environment where physical evidence of a crime or incident exists. The environment where the first criminal act occurred is the primary physical crime scene and subsequent scenes are secondary physical crime scenes.
  (Carrier & Spafford, 2003, p. 6)

- **Digital Crime Scene:** The virtual environment created by software and hardware where digital evidence of a crime or incident exists. The environment where the first criminal act occurred is the **primary digital crime scene** and subsequent scenes are called **secondary digital crime scenes.**

  (Carrier & Spafford, 2003, p. 6)

Carrier and Spafford (2004) produced another paper at the 2004 Digital Forensics Research Workshop with modifications to their original model. This later model was still based on treating the digital crime scene in the same way as a physical crime scene and incorporating both as part of a digital forensic process, with the digital investigation phase diagram as shown in Figure 2.

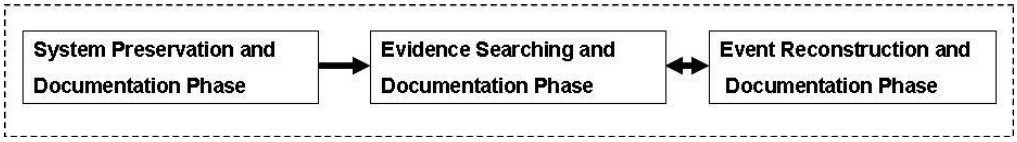

Figure 2 Digital Crime Scene Investigation Phases after Carrier and Spafford (2004)

To place the Digital Crime Scene phases in perspective, Carrier and Spafford's (2004) overall model is shown in Figure 3.

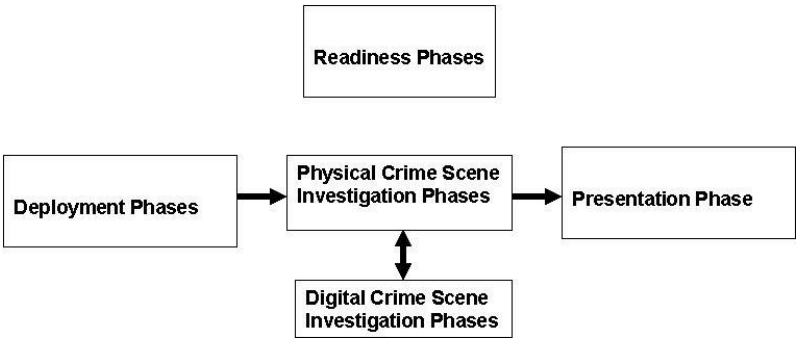

Figure 3 The IDIP after Carrier and Spafford (2004)

2.5.1.3 Enhanced Digital Investigation Process Model (EDIPM)

The Enhanced Digital Investigation Process Model (EDIPM) developed by Baryamureeba & Tushabe (2004) follows the same basic format and takes the same fundamental stance as Carrier and Spafford's (2003) original version of the IDIP in that the digital evidence is treated in the same way as physical evidence, i.e. the computer becomes a digital crime scene in its own right. In the EDIPM the authors establish five 'major phases' (Readiness, Deployment, Trace Back, Dynamite and Review). The EDIPM phases are shown in Figure 4.

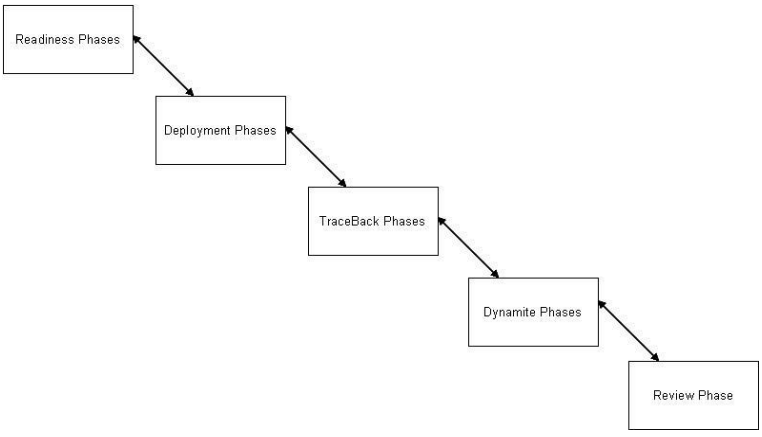

Figure 4 The EDIPM after Baryamureeba and Tushabe (2004)

The Carrier and Spafford IDIP (2003) definition of the physical crime scene is incorporated in the EDIPM which now has 5 phases instead of the 6

phases of Carrier and Spafford caused by dropping the IDIP's Reconstruction phase (which involves developing a theory for the incident based on data analysis - although the IDIP is unclear when this analysis takes place). In relation to acquiring the digital evidence the Preservation phase of the EDIPM, a sub-phase of both the physical and digital crime scene investigation phases (which are themselves sub-phases of the Deployment phase), is described by Baryamureeba & Tushabe (2004) as the process:

> …which preserves the digital crime scene so that evidence can be later synchronized and analysed for further evidence. Duplication of evidence (creation of bit-by-bit copies of the seized data) should be performed for use in multiple analyses (p. 4).

2.5.1.4 Digital Crime Scene Analysis model (DCSA)

The idea of building on the similarities between digital and physical investigations at a conceptual level was progressed by Rogers (2006) in his Digital Crime Scene Analysis model (DCSA), despite the fact that this introduces new challenges, as this enables a common approach to be defined with the benefit of bringing digital forensics into the recognised field of forensic science as first proposed by Carrier and Spafford (2003) and further supported by Baryamureeba & Tushabe (2004).

Rogers (2004) recognises the contributions of digital forensic process models proposed by Carrier and Spafford (2003), in addition to other researchers such as Baryamureeba, Tushabe (2004), Beebe & Clark (2004) and Mocas (2004). However, Rogers contends that "…what is still lacking is an applied/practical approach to dealing with digital crime scenes and the digital

evidence contained therein" (2004, p. 1). Whilst adopting the definition of digital evidence used by Carrier and Spafford (2003), Rogers modifies the definition of a digital crime scene to be "…the electronic environment where digital evidence can potentially exist" (2004, p. 7).

Rogers (2004) takes issue with previous models that have been biased towards incident response on the basis that vital elements of law enforcement activity are missing, such as 'chain of custody' and 'standard of proof' considerations as well as the need to comply with the appropriate rules. In this respect, although Reith et al (2002) point out that even though their model does not include a chain of custody element this is in fact implied as being part of the forensic process, the chain of custody is vitally important on any matter that may appear in court (Ashcroft, 2001; Cummins & Lowry, 2003; Gosh, 2004a; Mercuri, 2005) and therefore Rogers makes a valid point as this process should be explicit within any process model.

Further criticism is made by Rogers (2004) of previous models in relation to the lack of 'stratification' on the basis that non-digital forensic investigations would involve specialists in particular areas of evidence gathering, e.g. fingerprinting, DNA material, but the digital models envisage one person being responsible for the data collection from all digital sources whether they be from a network, router or hard disk drive. This point made by Rogers has some merit as the technological environment is ever-changing and extensive thus precluding an individual from having skills in all areas and ultimately "The mere fact that the scene is digital does not alter the reality that no one can live up to this unrealistic expectation of multiple domain expertise" (Rogers, 2004, p. 12).

Previous models are also identified by Rogers as having a limitation due to their broad approach which Rogers states is understandable on the basis that they try and model the whole investigative process which he says is not possible (given that this cannot even be undertaken for a physical crime scene). Instead Rogers suggests that a more pragmatic approach would be to deal with the most important aspects of the investigation on which further work is reliant, the data acquisition, and in this respect he points out that "If doubt is cast on the initial collection and management of evidence, output from the other phases is moot." (2004, p. 12)

However, with regard to developing a practical generic approach for the high-level phases of a digital investigation Rogers identifies a problem in that the phases are dependent on the type of investigation, which Rogers calls the 'context' and 'content' of the investigation. Rogers defines context to be the type of crime that has been 'committed or assumed' and gives examples of 'hacking incident', 'internal fraud' and 'child porn'. Content is associated with the operating system(s) and file system(s) on which the data resides and also the volume of potential evidence (Rogers, 2004).

On the basis that he believes that the high-level phases are impractical to model Rogers focuses on 'lower level' activities. Referring to Carrier and Spafford's (2003) earlier model consisting of five phases, Rogers introduces in the DCSA an additional hierarchy comprised of the 'lab' and 'corpus delicti' layers. Of relevance to data acquisition, the corpus delicti layer comprises the three phases of Evidence Identification, Evidence Collection and Transportation.

2.5.1.5 A Hierarchical, Objectives-Based Framework for the Digital Investigations Process (HOFDIP)

An alternative to the abstract approach for producing a digital forensic model is proposed by Beebe and Clark (2004) on the basis that the focus on the abstract is at the expense of the fundamental investigative principles. They go on to suggest that although previous models are useful in explaining overarching concepts they lack the detail required to be of practical use. Beebe and Clark propose a framework that they suggest complies with the requirements of a scientific discipline and they adopt the definition of Digital Forensic Science from Palmer's work with the Digital Forensics Research Workshop:

> Digital Forensic Science – The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation of digital evidence derived from digital sources for the purpose of facilitation or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations.
>
> (Palmer, 2001, p. 22)

A problem with this definition is that it specifies *criminal* activity, which is not necessarily the case for all digital forensic investigations, whilst for the theoretical aspect it focuses on predicting events which lends itself more specifically to network intrusions rather than to the other types of digital forensic activity such as law enforcement (Association of Chief Police Officers, 2003;

Craiger, 2005). Beebe and Clark's (2004) proposed framework comprises the following key aspects:

- **Phases and sub-phases** - sequential, time-based, distinct, discrete steps in the process
- **Principles** - high-level procedures, guidelines and/or approaches that apply to one or more phases
- **Objectives** – the intended outcomes.

2.5.1.6 Framework for a Digital Forensic Investigation (FDFI)

Kohn et al (2006) conclude that the important factors in a digital forensic model are knowledge of the legal environment and that the model should contain three stages, namely preparation, investigation and presentation. These stages are based partly on the work of other authors such as the Extended Model of Cybercrime Investigations (Ciardhuáin, 2004) (discussed later), Computer Forensics: Incident Response Essentials (Kruse & Heiser, 2002) and the Reith et al Examination of Digital Forensic Models (2002). Instead of the detail provided in the Carrier and Spafford (2003) model the FDFI is very simple, as shown in a diagram provided to illustrate the order in which the stages need to be carried out (Figure 5).

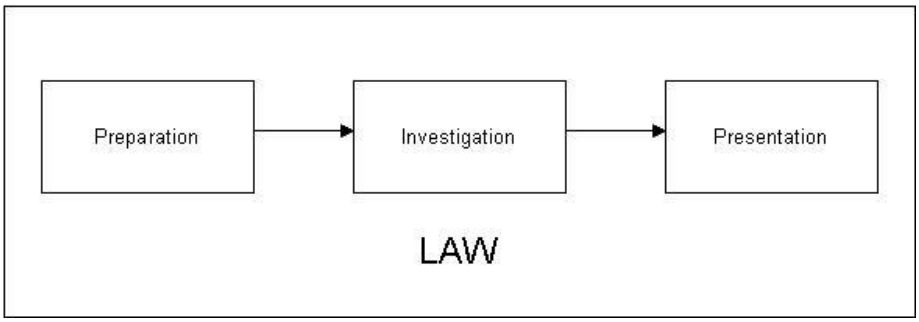

Figure 5 The Three Stage Process after Kohn et al (2006)

In relation to data acquisition both the Preparation stage and the Investigation stages are relevant. Kohn et al (2006) suggest the Preparation stage should incorporate the following elements:

- Standards used in the organization
- Policies and procedures in place to assist in the investigation
- Training
- Legal advice
- Notification to the correct authorities
- Documentation of previous incidents
- Planning, also known as an 'approach strategy'.

The inclusion of activities that would happen after an investigation is under way, 'Notification to the correct authorities' and 'Planning', suggest that the title 'Preparation' covers both preparing for a potential investigation that is yet to happen and preparing to undertake activities during the early stages of an existing investigation. The elements to be included in the investigation stage that are relevant to acquiring digital data are identified as:

- Searching for and identifying evidence on a computer;
- Collection of the evidence from the computer (original is duplicated);
- Transportation of the evidence to a secure environment;
- Storage of evidence collected at the scene.

2.5.1.7 The Four Step Forensic Process (FSFP)

Venter (2006) suggests that there are expectations within many organisations that digital forensics can be carried out by non-technical personnel. Consistent with this idea, Kent, Chevalier, Grance and Dang (2006) developed a guide whose aim is to provide information that would allow an organisation to develop their own digital forensic capability, using IT professionals, for security incident response (although they suggest that the information could also be used in other environments). Kent et al recognise that different organisations may be subject to different laws and regulations and provide a disclaimer to the effect that the guide should only be considered as a starting point for developing policies and procedures and that advice should be sought from specialists working in this area. Kent et al identify several basic stages in other models with the main differentiator being the degree of granularity adopted in describing the detail for each stage of the process. While suggesting that an organisation should adopt the most appropriate model for their own circumstances Kent et al recommend that the four step process as detailed in Figure 6 is followed in all cases. At first sight this suggestion seems impractical but as the process itself is described at a high level it is unlikely to impose unnecessary restrictions in practice.

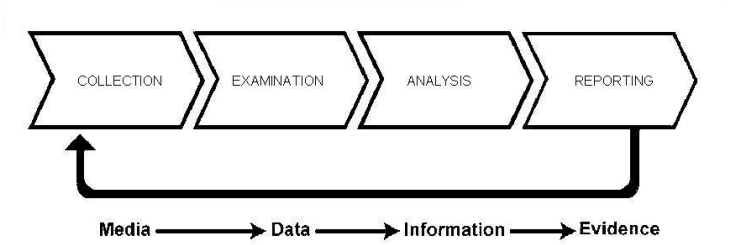

Figure 6 The Four Step Forensic Process (FSFP) after Kent et al (2006)

The FSFP proposed by Kent et al (2006) appears relatively simple when compared to other models such as the Enhanced Digital Investigation Process Model (Baryamureeba & Tushabe, 2004), the Abstract Digital Forensics Model (Reith, et al., 2002) and the Extended Model of Cybercrime Investigations (Ciardhuáin, 2004)(discussed later) but the authors go into some detail as they describe various activities associated with each of the four phases. However, with regard to digital data acquisition only the Collection phase is relevant which is defined as "identifying, labelling, recording, and acquiring data from the possible sources of relevant data, while following procedures that preserve the integrity of the data" (Kent, et al., 2006, p. 26). This definition is consistent with other models (Baryamureeba & Tushabe, 2004; Carrier & Spafford, 2003; Reith, et al., 2002).

The Collection step of the FSFP consists of two activities which are: (1) Identifying Possible Sources of Data and (2) Acquiring the Data. For the first step Kent et al (2006) offer advice to assist in recognising potential data storage devices such as computers, DVDs, thumb drives, memory cards etc., whilst introducing the idea that the 'analysts'[15] should be capable of undertaking an

[15] The term used by the authors to describe the person undertaking the computer forensic activities

onsite survey to identify such data sources. For the second step there are three activities: (1) Develop a plan to acquire the data, (2) Acquire the data and (3) Verify the integrity of the data.

2.5.1.8 The Common Process Model for Incident Response and Computer Forensics (CPMIRCF)

Supporting the views expressed by Cummins and Lowry (2003), Freiling and Schwittay (2007) clearly identify the distinction between incident response and digital forensics. They describe the area of incident response as focusing on the activities of organisations who suffer security breaches on the networks with the prime aims of "…quick detection, containment and recovery" (Freiling & Schwittay, 2007, p. 2). Digital forensics is described as being a "…forensic science that deals with obtaining, analysing and presenting digital evidence…" (Freiling & Schwittay, 2007, p. 6) by adopting proven techniques and principles.

Despite identifying the differences between incident response and digital forensics, Freiling and Schwittay (2007) question whether they should be treated separately on the basis that there are many common elements between the two types of activity. With this in mind they propose a common process model that can be applied in both environments, the Common Process Model for Incident Response and Computer Forensics (CPMIRCF). The CPMIRCF consists of three main phases: (1) Pre-Analysis, (2) Analysis and (3) Post-Analysis. In relation to the data acquisition aspect of the model the relevant phases are the Pre-Analysis phase and the Analysis phase. The Pre-Analysis phase is a 'catch-all' classification and comprises all the processes that take place prior to analysis of the data that has been collected and includes ongoing Incident preparation (that

could be regarded in a generic sense as developing policies, procedures and capability to undertake a forensic data acquisition task). Freiling and Schwittay's Pre-Analysis phase contains three steps:

1. Incident Detection

Despite the stated intention of Freiling and Schwittay to produce a generic model applicable to both incident response and digital forensic processes the description of this step provided by Freiling and Schwittay is all about intrusion detection and other aspects of incident response.

2. Initial Response

Freiling and Schwittay (2007) state that the goal for this step is to confirm the incident has occurred and determine its impact on the organisation. The description is again based on an incident response situation and many of the tasks listed do not have a generic equivalent, e.g. network monitoring, removing compromised hosts and initialising packet filtering.

3. Formulation of Response Strategy

The emphasis on incident response is again evident in that a decision will be made to determine if a 'full forensic' analysis will take place where for a generic model of the digital forensic process this question is moot (Palmer, 2001; Rogers, 2004). Unlike many other authors who use the term 'analysis' to describe the process of analysing the data after it has been collected (Casey, 2004, 2010; Palmer, 2001; Reith, et al., 2002) Freiling and Schwittay regard this stage as being everything between the initial incident and the preparation of a report or presentation.

There are two activities related to data acquisition in Freiling and Schwittay's Analysis stage of the CPMIRCF; Live Response and Forensic Duplication:

Live Response - Notwithstanding the incident response terminology this step would normally be considered as part of the data acquisition stage as it is one of many techniques that may be adopted dependant on the requirements of the investigation.

Forensic Duplication - this step involves copying the contents of storage media whilst ensuring that the original data is unaltered. However, as McKemmish (1999) points out, this is a desirable state but not always possible or practical.

The 'chain of custody' is mentioned in the CPMIRCF as is the requirement to keep the original media, i.e. the source of the data, safe together with the forensic copies. This may not always be practical, especially in the case of a server or other critical system, and would not usually apply to cases involving digital forensic practitioners when providing services to third-parties. Freiling and Schwittay (2007) state their intention is to integrate the Incident Response and Computer Forensic environments to produce a common model and suggest that digital forensic investigations would benefit from the 'proper management' imposed by incident response procedures.

2.5.1.9 Two-Dimensional Evidence Reliability Amplification Process Model (TDERAPM)

Agreeing that there are limitations with previous abstract models and following the concept of the iteration of phases within an investigation Khatir, Hejazi and Sneiders (2008) adopt a 'management' approach to the digital forensic process in their Two-Dimensional Evidence Reliability Amplification Process Model (TDERAPM). They suggest that existing models have shortcomings such as:

- Lack of flexibility between phases
- Lack of tools usage/automation
- Ignoring of management aspects
- Ignoring organisational structure
- Ignoring the distribution of responsibilities.

Having identified these problems, Khatir et al (2008) conclude that the issue of the reliability of evidence has still not been addressed and thus present the TDERAPM which consists of five major phases (of which only the first two are relevant to data acquisition) sixteen sub-phases (of which only the first five are relevant) and four 'umbrella activities' which apply to all phases.

The two major phases of the TDERAPM relevant to data acquisition are Initialization and Evidence Collection whilst the five relevant 'sub-phases' are: Confirmation, Case Assessment, Authorization, Physical Evidence Collection and Digital Evidence Collection. The umbrella activities are: Documentation,

Preservation and Authenticity, Case Management and Team Setup and Computer Tools Utilization. The TDERAPM is reproduced in Figure 7.

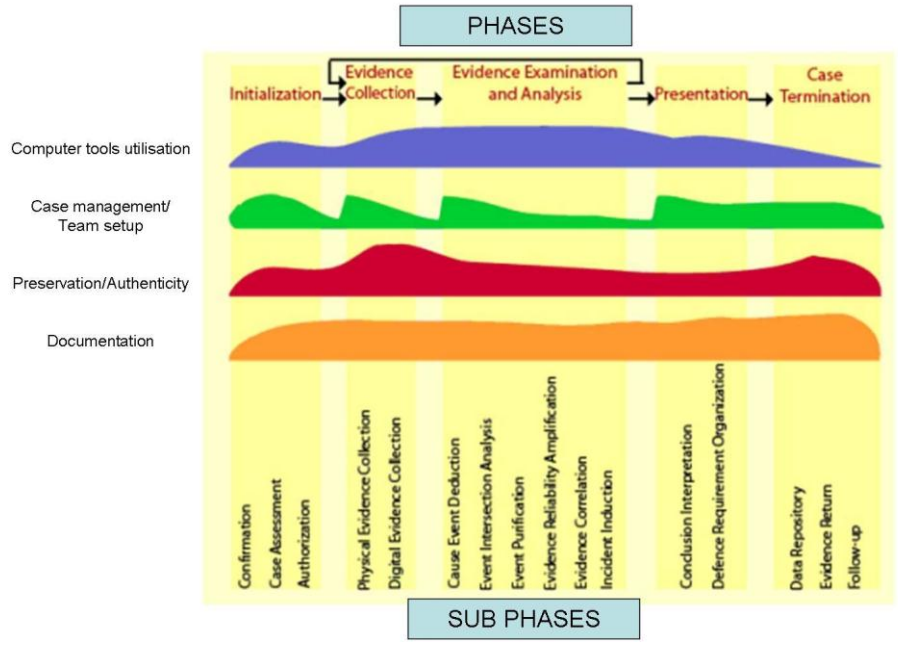

Figure 7 TDERAPM Phases after Khatir et al (2008)

It would appear from the text that the horizontal areas represent the amount of 'effort' involved in a particular umbrella activity but there is no information provided on how this has been assessed or even the units being measured. These umbrella activities are described as being activities that "…should always be practiced during phases of the process" (Khatir, et al., 2008, p. 28) and they are intended to contain guidelines. The narrative for the Documentation umbrella activity says that it is important to maintain documentation but does not indicate how.

The Preservation/Authenticity activity requires the forensic team to follow "…disciplined and fully documented steps" (p. 28) although what this means and how this is to be achieved is not covered. The narrative includes aspects of integrity relating to the acquired data as well as the physical return of

collected items but does not provide any detail, although reference is made again to a table that has been omitted. Case Management and Team Setup is an activity that Khatir et al (2008) have identified through their research. An overview is provided in regard to the requirements of the management role but this high-level narrative is a statement of a few processes that would normally already be in place and that may in certain circumstances be undertaken by the investigator who could fulfil both roles. The final umbrella activity is Computer Tools Utilisation. The narrative does not provide any detail but states that computer tools are useful and can be applied to all aspects of the investigation process. This would seem to be inappropriate as a separate activity when compared to, for instance, the requirement to keep comprehensive documentation.

2.5.1.10 Mapping Process of Digital Forensic Investigation Framework

Selamat, Yusof and Sahib (2008) consider that some previous models have redundancies in terms of their key steps, such as Kohn's Framework for Digital Forensic Investigation (Kohn, et al., 2006) and the Reith et al Abstract Digital Forensics Model (Reith, et al., 2002) , whilst no model provides a single framework for investigating all cases. Selamat et al (2008) identify common phases in previous models and relate them to a more concise framework to produce a map of the Digital Forensic Investigations Framework (DFIF). Their review of thirteen published papers on previous models identified five phases to which the reviewed models could be mapped. Of these phases only Phase 1 (Preparation) and Phase 2 (Collection and Preservation) are relevant to data acquisition.

Selamat et al (2008) note that their review showed that whilst all the models contain Phases 2, 3 and 4 (Collection and Preservation, Examination and Analysis, Presentation and Reporting) only a few contain Phases 1 (Preparation) and 5 (Disseminating the Case) which they consider to be important. From a data acquisition viewpoint the case for some form of preparation prior to arriving on site seems to be well supported. Despite the framework being an amalgamation of previous models, it is missing details such as the Pre-incident Preparation requirements from the Common Process Model (Freiling & Schwittay, 2007).

2.5.1.11 Systematic Digital Forensic Investigation Model

Agarwal, Gupta, M., Gupta, S., and Gupta S.C. (2011) propose the Systematic Digital Forensic Investigation Model (SDFIM) to assist forensic practitioners and organisations to establish their policies and procedures. The SDFIM has eleven phases covering all aspects of a forensic practitioner's work but in contrast to many previous models the analysis phase is not the main focus of the activities described. Only those phases relevant to digital data acquisition are now covered in more detail:

- Phase 1 (Preparation), covers the various constraints and authorisations as well as collecting together the necessary resources to undertake the investigation
- Phase 2 (Securing the Scene) involves identifying the extent of the 'crime scene' in order to set up a perimeter to prevent unauthorised access to potential evidence

- Phase 3 (Survey and Recognition) can be summarised as an onsite survey
- Phase 4 (Documenting the Scene) requires that all equipment and connections must be photographed and this includes any data that is visible on screens. Other documentation involves a log of all those at the scene broken down into various categories such as ‘victim’ and ‘suspect’
- Phase 5 (Communication Shielding) involves preventing communications to any devices involved in the incident
- Phase 6 is where the evidence collection takes place and this is sub-divided into volatile and non-volatile collection
- Phase 7 (Preservation) involves packaging, transportation and subsequent storage prior to analysis
- Phase 11 (Result & Review) is a follow-up assessment of the activities undertaken during the case with a view to process improvement.

2.5.1.12 Ad hoc models reviewed

This section of the literature review has reviewed the following models under the theme ‘ad hoc digital forensic process models’:

- The Abstract Digital Forensic Model (Reith, et al., 2002)
- The Integrated Digital Investigative Process (Carrier & Spafford, 2003)

- The Enhanced Digital Investigation Process Model (Baryamureeba & Tushabe, 2004)
- The Digital Crime Scene Analysis Model (Rogers, 2004)
- A Hierarchical, Objectives-Based Framework for the Digital Investigations
- Process (Beebe & Clark, 2004)
- Framework for a Digital Investigation (Kohn, et al., 2006)
- The Four Step Forensic Process (Kent, et al., 2006)
- The Common Process Model (Freiling & Schwittay, 2007)
- The Two-Dimensional Evidence Reliability Amplification Process Model (Khatir, et al., 2008)
- The Digital Forensic Investigations Framework (Selamat, et al., 2008)
- The Systematic Digital Forensic Investigation Model (SRDFIM) (Agarwal, et al., 2011).

These process models have displayed a range of approaches from those that include a few fundamental stages to those that involve many stages and sub-divisions. In addition, whereas some authors have attempted to develop a generic approach others have focused on a particular environment, such as law enforcement or incident response.

2.5.2 Process flow approaches for digital forensic models

A different approach to that used in the 'ad hoc' models reviewed in 2.5.1 has been adopted by some researchers such as Ieong (2006), Ciardhuáin (2004)

and Venter (2006) who have moved away from the low-level detail of the investigative process and look instead at the issue from a workflow perspective. Whilst this approach may be of limited practical use for an investigator the concept is worthy of consideration as part of an overall formal description as it may capture aspects of the process that have not been included in the ad hoc models covered previously.

2.5.2.1 Extended Model of Cybercrime Investigations

Ciardhuáin (2004) paved the way for the 'information flow' approach when he proposed his 'comprehensive' model for conducting cybercrime investigations. His motivation for proposing the model is founded on the belief that other models did not cover all aspects of the investigation process and the "single largest gap in the existing models is that they do not explicitly identify the information flows in investigations" (p. 4). A further criticism of previous models is that they concentrated on the 'middle' of the investigations process, suggested by Ciardhuáin (2004) as being the Collection and Examination stages. In order to model the entire information flow associated with a digital forensic investigation Ciardhuáin identifies thirteen activities of which only the first eight are relevant to evidence acquisition: (1) Awareness, (2) Authorisation, (3) Planning, (4) Notification, (5) Search & Identification of Evidence, (6) Collection of Evidence, (7) Transport of Evidence and (8) Storage of Evidence. These activities are seen as being addressed in a linear fashion although it is anticipated that 'backtracking' will be necessary with several iterations required, particularly on some of the later activities which is a concept introduced by Beebe and Clarke (2004).

Ciardhuáin (2004) identifies the lack of explicit mention of a chain of custody in the Reith et al model (2002) as a 'major flaw', even for those working in jurisdictions that don't require a chain of custody, because due to its nature digital evidence can often be subject to claims of tampering. Ciardhuáin uses the chain of custody as an example of information flow stating that "...the chain of custody is formed by the list of those who have handled a piece of evidence and must pass from one stage to the next with names added at each step" (Ciardhuáin, 2004, p. 5). Descriptions for the eight activities relevant to data acquisition are:

- **Awareness -** associated with the investigator being made aware that the investigation is needed and notification may come from external or internal sources. The inclusion of this activity addresses a perceived weakness in earlier models in that the source of the notification would have a bearing on the direction the investigation would take and the process methodologies adopted
- **Authorisation** - potentially complex depending on the environment in which the digital forensic practitioner is working, ranging from a simple verbal approval to a formal legal document such as a court order or warrant
- **Planning** - involves resources both inside and outside of the digital forensic practitioners' organisation and may involve regulations and legislation considerations
- **Notification** - involves informing all parties involved in the investigation although this is recognised as not being applicable in all

cases, e.g. when the subject of the investigation must be unaware that it is to take place

- **Search and Identification of Evidence** - ranges from confirming the suspect's computer to tracing network packets
- **Collection** - the activity in which the digital image is acquired
- **Transport** - involves transferring either the original evidence devices, such as seized computers, or forensic images to a suitable location whilst ensuring that the integrity of the potential evidence is not affected
- **Storage** - allows for the fact that the devices containing potential evidence will need to be properly safeguarded whilst not being analysed.

2.5.2.2 FORensics ZAchman framework (FORZA)

Ieong (2006) adopted a different focus for his information flow model, (FORZA), by seeking to accommodate the involvement of legal practitioners in the process of a digital forensic investigation by assigning them specific roles within the framework and using high-level business model descriptions for the various stages rather than technical terms. The FORZA model is based on the Zachman Framework (Zachman, 1987) for producing a high-level way of viewing an enterprise, hence the name given to the model: FORensics ZAchman Framework. The essential idea behind the Zachman framework is that any (usually complex) object, entity or process can be described in different ways for different audiences. The framework allows for six varying levels of detail and six viewpoints or perspectives.

Following on from work by Losavio, Adams and Rogers (2006) (who identify a gap in understanding between the technical digital forensic practitioners and their legal colleagues/clients) Ieong (2006) states that in the IT security environment there are a simple, fundamental set of principles on which all aspects of this field rely, namely Integrity, Confidentiality and Availability. The concept of the linked fundamental principles of the IT Security field is applied by Ieong to digital forensics and he goes on to suggest that a digital forensics investigation has an equivalent three-part set of principles that are Reconnaissance, Reliability and Relevancy (as shown in Figure 8).

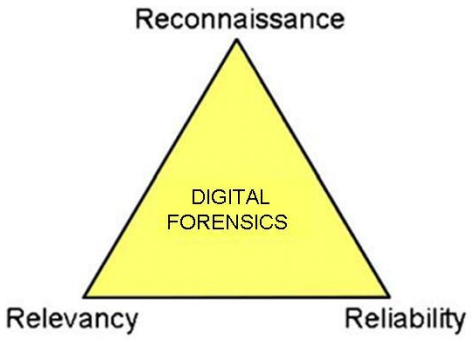

Figure 8 Digital Forensic Principles after Ieong (2006)

Ieong (2006) places the digital investigation process in perspective with an emphasis on the 'forensic aspect' by stating that it is a "… process to determine and relate extracted information and digital evidence to establish factual information for judicial review" (p. 2). Ieong defines Reconnaissance as collecting, recovering and analysing the digital data. The term Reliability is considered to be the process of maintaining chain of custody and the term Relevancy is used to describe where the legal practitioner may be involved in determining what is collected.

Ieong uses a Zachman-like framework in which he identifies eight roles for a 'typical' forensic investigation (although they could be carried out by the same person). These roles are: (1) Case leader, (2) System/business owner, (3) Legal advisor, (4) Security/system architect/auditor, (5) Digital forensics specialist, (6) Digital forensics investigator/system administrator/operator, (7) Digital forensics analyst and (8) Legal prosecutor. A process flow between the various roles is briefly described and produced in a diagram shown as Figure 9.

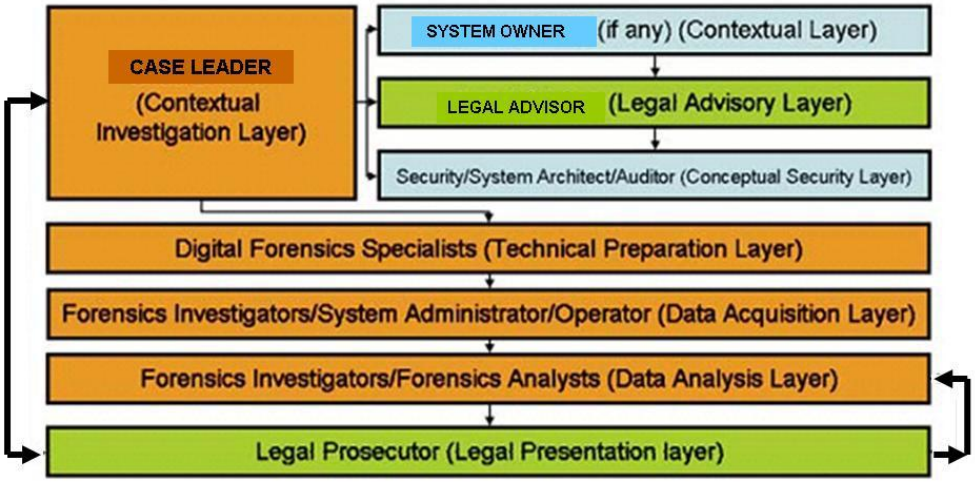

Figure 9 Process Flow Between Roles in a Forensic Investigation after Ieong (2006)

From Figure 9 the data acquisition aspect is identified in the 'Data Acquisition Layer' associated with the 'Forensics Investigator/System Administrator/Operator'. No information is provided in relation to the skills that are required for this activity but in a case example provided by Ieong (2006) the relevant person would need to consider six categories of questions, namely:

- What (the data attributes)
- Why (the motivation)

- How (the procedures)
- Who (the people)
- Where (the location)
- When (the time).

Ieong attributes these questions to the Systems and Business Security Architecture (SABSA) framework but they are also a fundamental aspect of police investigative training and recognised as the 5WH approach (National Centre for Policing Excellence, 2005, p. 68) .

2.5.2.3 Process Flows for Cyber Forensics Training and Operations

Venter (2006) uses the process flow approach to describe a series of activities with the primarily aim being to assist with the training of people with limited technical background knowledge in the role of Cyber First Responder. This is in contrast to Ciardhuáin (2004) who used the same approach but targeted at digital forensic practitioners. The concept of non-technical personnel undertaking what can be a complex and technically demanding task such that the output of their efforts (potential digital evidence) may be admitted by a court seems to be at odds with digital forensic practice. It is unlikely that courts will lower their standards for admissibility on the basis that there was no other person available to collect the evidence in a manner that would have been undertaken by a digital forensic professional. Furthermore, if such evidence were to be admitted then the opposing side would potentially have grounds for contesting that evidence. However, as well as providing training for non-IT personnel, Venter

suggests that by adopting the process flow model described in his paper experienced investigators would be able to speed up their investigations.

Unlike the guide produced for non-IT personnel by the National Institute of Justice (Ashcroft, 2001) that identifies high-level principles and then provides detail around the possible location of potential digital evidence, the Venter (2006) process description includes detailed instructions in a step-by-step approach. Whilst being attractive to the principal audience of non-technical personnel, criticism of this step-by-step approach comes from Beebe and Clark (2004) and Carrier and Spafford (2003) who suggest that practitioners are better able to deal in practice with 'objectives-based steps' given the varied nature of the environment (although Beebe and Clark themselves provide an example of a detailed list of activities as an example in their own model). Venter (2006) counters that this 'unstructured' approach proposed by the other authors is flawed as they require a practitioner to possess "…a certain amount of understanding of the technical field…" (Venter, 2006, p. 3). Several authors have argued that anyone working in the field of digital forensics would require a good technical understanding (C. Brown, 2006; Bunting & Wei, 2006; Calhoun, 2008; B. D. Carrier, 2006; Jones, et al., 2006; Kent, et al., 2006) and if the necessary skills are not available in-house then they can be brought in (even at short notice) from an external provider, of which there are many (such as the 'Big Four' professional services firms and numerous specialist companies).

Suggesting that the benefit of the process flow approach is that it will potentially reduce errors whilst enhancing the standard of documentation, Venter (2006) describes four design principles for the development of a process flow model:

- Ease of use for non-IT professionals
- Applicable in most cases
- Assist with expert testimony or at least not interfere with it
- Can be utilised during operations and not only during training.

In addition to his Design Principles, Venter (2006) incorporates several 'layout characteristics' into his process flow model that can be summarised as:

- Each process flow must fit on a single A4 sheet of paper
- Important information is recorded during the process steps
- Standard naming conventions are adopted.

An overall Process Flow that governs the behaviour common to all situations is presented by Venter starting with Inspect and Prepare Scene, followed by Collect Evidence & Evidence Information and ends with Debrief Scene & Record Seized Information. This generic process flow is complemented by process flows that are specific to a particular type of device:

- Desktop computer hard disks
- PDAs and Cell phones
- CD/DVD/STIFFY/FLASH/OTHER

2.5.2.4 Process flow models reviewed

The models reviewed in this section of the literature review under the theme of Process Flow are:

- An Extended Model of Cybercrime Investigations (Ciardhuáin, 2004)
- FORZA - Digital forensics investigation framework (Ieong, 2006)
- Process Flows for Cyber Forensics Training and Operations (Venter, 2006).

The three Process Flow models provide a different perspective than the earlier Ad Hoc models in that they associate the activities of the digital forensic practitioner with the information they generate and place this in context with the purpose of the investigation.

2.5.3 Scientific approaches for digital forensic models

The authors of the modelling approaches described earlier created their own terminology and definitions to describe their models. Whilst this may have made it easier to create the narrative around ideas and concepts this has meant that these models have not been described or defined in such a way as to make them readily part of a scientific discipline through the lack of an established formal specification. An alternative approach is to adopt a formal method for describing the model. A formal specification is an abstract expression of the properties of a system that are expressed in a formal language (Lamsweerde, 2000) which contains three components:

1. Rules for determining the grammatical well-formedness of sentences (the syntax)
2. Rules for interpreting sentences in a precise, meaningful way within the domain considered (the semantics);
3. Rules for inferring useful information from the specification (the proof theory).

   (Lamsweerde, 2000, p. 2)

Several 'scientific' approaches are now described in chronological order in accordance with their appearance in the literature.

2.5.3.1 End-to-End Digital Investigation (EEDI) process

Stephenson (2003a) introduces the Digital Investigation Process Language (DIPL) as a formal process language, loosely based on LISP[16], "…that allows the characterization of an investigation in formal terms" (p. 12). Although his initial paper does not provide much detail on DIPL Stephenson (2003b) made available a PowerPoint presentation on the Eastern Michigan University website that gives a more in-depth coverage. The PowerPoint presentation summarises the key attributes of Stephenson's DIPL as being:

- Involves a process language like LISP
- Follows the End-to-End Digital Investigation (EEDI) process and the DFRWS framework

[16] LISP is derived from "LISt Processing" and refers to one of the oldest high-level languages. LISP source code is itself made up of lists.

- Gives a detailed and explicit description of the investigation and its findings
- May be used to translate the investigation into a formal model.

(Stephenson, 2003b, p. 2)

Further information is provided in relation to the ways in which the DIPL could be used which are (1) as a structured framework for an investigation, (2) as an analysis of completeness of a completed investigation and (3) as the basis for a formal model of an investigation and event. As well as the proposal for a new language Stephenson also proposed the End to End Digital Investigation (EEDI) model, although he states that the model is not suitable for 'simple digital forensic investigations' but does not expand on this further and no definition of 'complex investigations' is provided beyond the statement that it would typically employ "…sophisticated tools such as link analysers…" (Stephenson, 2003a, p. 2). The reference to 'link analysers' and an example of a digital forensic task involving the investigation of 'worm' attacks suggests that in this instance Stephenson's focus is on the specific area of Incident Response involving the internet or large corporate networks rather than a generic area of digital forensics activity.

Stephenson (Stephenson, 2003a) builds upon the Digital Forensics Research Workshop model (DFRWS) to provide definitions for eight concepts that are used in the EEDI model, only three of which are relevant to acquisition of digital data:

1. Primary evidence - evidence that is corroborated and may in turn corroborate other primary evidence. The corroboration may come from other primary evidence or a significant amount of secondary evidence.
2. Secondary evidence - evidence that in itself is not corroborated but that can assist in corroborating another piece of evidence.
3. Forensic digital evidence collection - the use of tools by trained digital forensic practitioners that have been accepted by the digital forensic discipline in order to obtain digital evidence.

Based on the definitions of primary and secondary evidence Stephenson introduces his First Rule of End-to-End forensic digital analysis:

> Primary evidence should be corroborated by at least one other piece of relevant primary evidence to be considered a valid part of the evidence chain. Evidence that does not fit this description, but does serve to corroborate some other piece of evidence without itself being corroborated, is considered to be secondary evidence.
>
> (2003a, p. 8)

This rule does not have an equivalent in other process models involved with acquiring digital evidence.

The EEDI process itself is characterised by a set of general steps that must be taken by an investigator in order to preserve, collect, examine and analyse digital evidence that follow the framework set by the DFRWS (which is

considered to contain the 'critical elements' of a digital investigation). Of the nine general steps used in the EEDI process only one is relevant to the acquisition of digital data and that is called Collecting Evidence. The overall concept of using DIPL is provided in Figure 10:

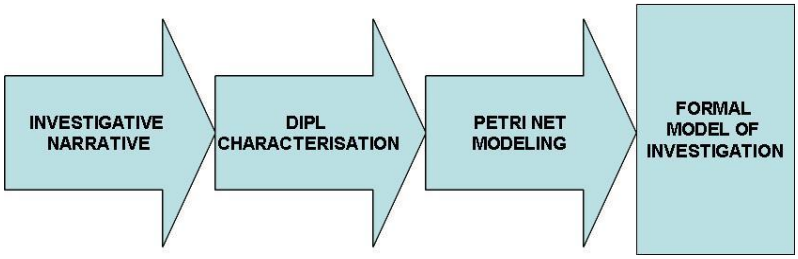

Figure 10 EEDI stages after Stephenson (2003)

Figure 10 shows that the process must first be described in narrative form by, presumably, a skilled investigator who is able to clearly identify all the necessary steps. This is then followed by someone with a degree of software-writing skills understanding the narrative and transforming it into the syntax of DIPL. The inclusion of the Petri Net stage in the EEDI is not explained.

Stephenson (2003a) expands on the potential benefits of adopting a formal language by suggesting that it could be used:

- To discredit an opposing investigator's testimony by showing that their investigative process was flawed
- To persuade the finder of fact that the investigation had been conducted "properly and completely" by showing a DIPL listing in court.

How these additional benefits are to be achieved in practice remains unclear and there seems to have been little further work undertaken on the DIPL.

2.5.3.2 Cyber Tools On-line Search for Evidence (CTOSE)

A European Union project called the Cyber Tools On-line Search for Evidence (CTOSE) went a stage further than Stephenson (2003b) in that rather than just creating a framework and language it implemented a new methodology in a web-based tool. The intention was to "…provide a consistent approach for identifying, preserving, analysing and presenting digital evidence" (Hannan, Frings, Broucek, & Turner, 2003, p. 5). The motivation behind the project was a recognition that in most companies the IT security function was largely focussed on finding technical solutions to the problem of intruders with little, if any, regard to the requirements of the legal system should offenders be identified or evidence located that might help to identify them. To address this and other issues, such as concern for disruption caused to the organisation during an investigation, the CTOSE project developed a model to provide a framework that would enable digital evidence to be collected in such a way that it would be admissible in court. Because of the complexity of the model the CTOSE project team decided to produce the CTOSE Demonstrator which is a software simulation application whose purpose was to demonstrate how the model could be used in practice (Hannan, et al., 2003).

The user interface of the full prototype application, Cyber Crime Advisory Tool (C*CAT), is web-based (written in Java) and it connects via an Apache Web Server to an SQL database which contains the data for the process model (Hannan, et al., 2003). As well as the C*CAT utility that assists the 'management' aspect of the investigation another 'expert system' has been designed that covers the legal aspects (Mann, 2004).

The C*CAT process model itself contains five phases; Preparation, Running, Assessment, Investigation and Learning. These phases are now covered in more detail:

- **Preparation** – This involves the organization ensuring that it has the resources, infrastructure and security aspects in place prior to the need to investigate a security incident, described as 'forensic readiness'
- **Running** – This phase is where the system is running 'normally', i.e. there is no indication of an incident at this point
- **Assessment** – This is the point at which there is some suspicion that a security incident has taken place which may or may not involve the organisation's systems running normally. A decision is made on what actions to take that may involve undertaking an investigation or implementing specific monitoring processes
- **Investigation** – If an investigation is determined to be the appropriate course of action a senior management decision will be made on whether this is to be performed in-house using the organisation's own staff or whether to engage the services of a third-party provider. The outcome of the investigation is to determine the details of the incident and establish how a similar incident can be prevented in the future
- **Learning** – This is where the knowledge gained from the investigation is translated into plans and procedures to mitigate the effect of further incidents of the same type.

The digital forensic practitioner is required to define the situation by selecting from options presented by the process model, which then provides the flow of actions and decisions that have to be considered or executed. Information in the form of advice or hints is stored within the system and this is available at all times (Mann, 2004). Finally, the practitioner is required to enter feedback as part of a knowledge-building process to assist with any future incidents (Mann, 2004).

2.5.3.3 The Unified Modeling Language (UML)

Several authors of digital forensic models have introduced the idea of adopting a formal modelling language used by software developers (Bogan & Dampier, 2005; Kohn, Eloff, & Olivier, 2008; Ruan & Huebner, 2009; Wang & Yu, 2007). This forms a framework for formally describing the digital forensic process without having to 're-invent the wheel' and where there is a large body of knowledge that can be applied to the task (Bell, 2003). Bogan and Dampier (2005) suggest that the lack of formalism in other models is due to the fact that many of those working in the field of digital forensics have come from non-IT specialist roles, such as law enforcement, and therefore they have not followed the structured approach that software engineers would have adopted in relation to developing their plans, procedures and tools. Bogen and Dampier (2005) propose the use of case domain modelling as it affords a structured approach for analysing and documenting the investigation, which addresses the lack of planning and analysis tools that often hinders the digital forensic investigator when it comes to investigating large or complex cases.

Bogan and Dampier (2005) also suggest that the field of digital forensics research will follow the advances in formalism and modelling in methodologies that has been seen in the field of software development. Justification for this view is based on commonalities the authors have identified between software development and digital forensics such as "…quality focus, application of repeatable processes, the use scientific methods, and the support of software tools" (2005, p. 1). Bogan and Dampier propose employing domain analysis as a tool for identifying relevant information within an investigation, and their aim is to develop a methodology that combines both UML notation and that of previous models in order to provide support for:

- Planning the collection and examination activities of a digital investigative process
- Building digital forensics expertise
- Reusing digital forensics knowledge
- Documenting forensics tasks.

The acquisition of digital data would seem to come under Bogan and Dampier's description "…general investigative processes that may be applied to several cases" (2005, p. 2) as well as the "…sequence of activities that occur in an investigation" (2005, p. 2). The issue of acquiring the potential evidence is not described, suggesting that the proposed unification of forensic model approaches does not cover all activities undertaken during a forensic investigation and is only applicable to the analysis stage.

Kohn, Eloff and Olivier (2008) also argue that the field of computer forensics would benefit from formal modelling approaches, such as UML, and comment that most of the process models they have reviewed have adopted an informal or 'intuitive' approach. They model what are described as two existing Digital Forensic Process Models[17] by utilising Use Case and Activity diagrams from UML in order to compare them. However, the 'model' that Kohn et al attribute to Kruse and Heiser (2002) is simply the headings for three steps for investigating a computer incident provided by Kruse and Heiser contained within their book[18]. The resulting Activity diagram is very simple, as shown in Figure 11.

Figure 11 Kruse & Heiser Activity diagram after Kohn et al (2008)

The resulting Use Case diagram for the Kruse and Heiser model does not come directly for the narrative but seems to be an interpretation by Kohn et al based on the environment of Incident Response as shown in Figure 12.

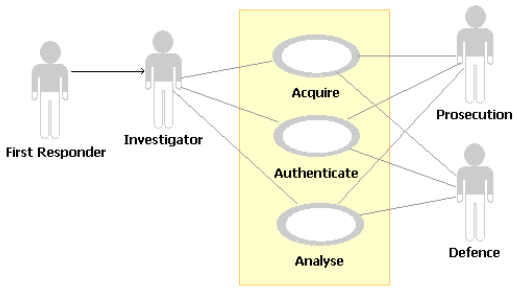

Figure 12 Kruse & Heiser Use Case diagram after Kohn et al (2008)

[17] (Kruse & Heiser, 2002) and (Ashcroft, 2001)
[18] Described by Kruse and Heiser as the "three A's"

In relation to the second ‘model’, that of the United States Department of Justice (US DoJ) (Ashcroft, 2001), the narrative contained in the US DoJ guideline is used as the basis for the Activity diagram (although the original guideline actually concentrates on the Collection phase). The resulting high-level Activity diagram is shown in Figure 13.

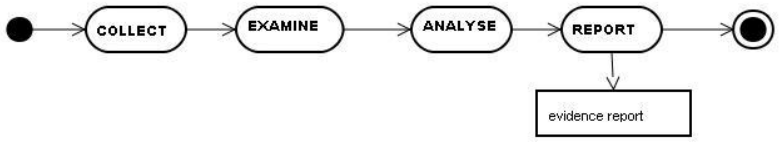

Figure 13 US DoJ Activity diagram after Kohn et al (2008)

The corresponding Use Case diagram is similar to that for the Kruse and Heiser model with the addition of an extra phase as shown in Figure 14.

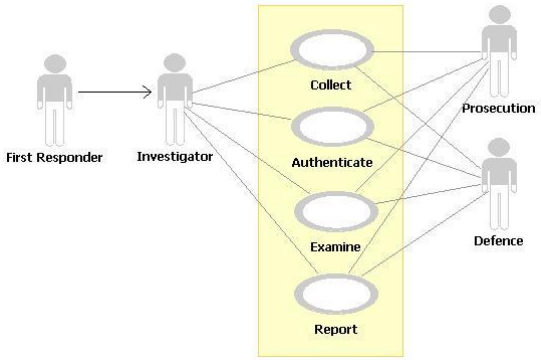

Figure 14 US DoJ Use Case diagram after Kohn et al (2008)

Ruan and Huebner (2009) use UML diagrams to describe the ‘well-accepted’ components of a computer forensic investigation but seem to disagree with Kohn et al (2008) in relation to the involvement of the legal ‘actors’ in different stages of the investigation as shown in the UML Use Case diagram of Figure 15.

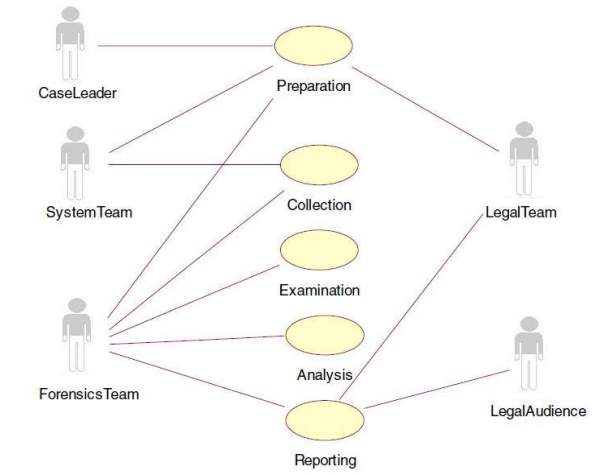

Figure 15 Forensic Process Use Case after Ruan and Huebner (2009)

Ruan and Huebner provide an Activity diagram for each of the processes shown in Figure 15. Shown in Figure 16 is the Activity diagram for the Collection process.

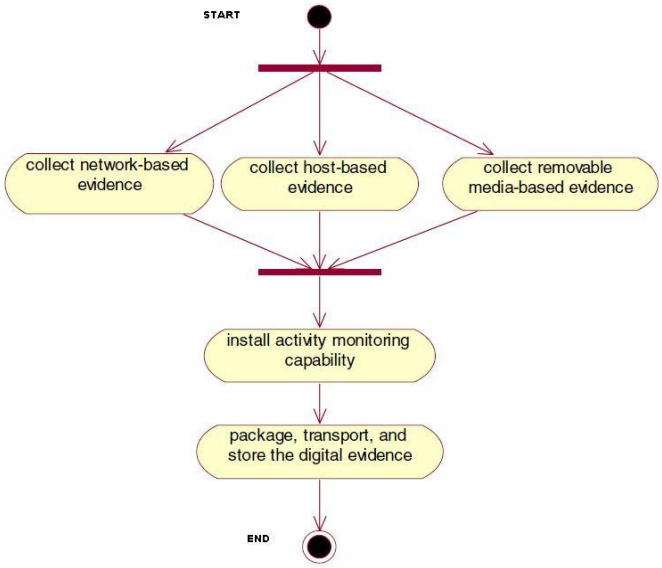

Figure 16 Forensic Process Activity Diagram after Ruan and Huebner (2009)

2.5.3.4 Modeling Computer Forensic Process from a Workflow Perspective

Wang & Yu (2007) identify similarities between the software development process and the digital forensic process. However, whilst acknowledging similarities they also point out that a notable key differentiator between the two is that whilst the particular order of the steps in the software development process is not critical (and some may be skipped entirely) this is not the case in the digital forensic process where certain steps are mandatory and need to be performed in the appropriate order.

Wang and Yu see the benefits of a formal methodology as being of practical use to the forensic practitioner rather than simply adding credibility to the forensic process and describe previous models as being "…very abstract and cursory" (2007, p. 55). They propose enhancing the digital forensic process described by Bogen and Dampier (2005) through the use of a Petri net[19]. Wang and Yu (2007) demonstrate their approach to modelling part of the forensic process using a Petri net together with a narrative that provides a useful summary of some of the actions that would be recognised from other models as a preliminary 'onsite' stage or 'site review' in relation to acquiring digital evidence (Baryamureeba & Tushabe, 2004; Carrier & Spafford, 2004). For their model Wang and Yu introduce the term 'action' (which they project to T-elements[20]) and the term 'condition' (which they project to P-elements[21]).

[19] A Petri net is a mathematical tool that can be used for describing the dynamic activities of a system (Trickovic, 2000)
[20] 'T' elements are active entities of the real world such as events, transitions and actions.
[21] 'P' elements are passive entities of the real world such as conditions, places and resources.

Wang and Yu (2007) provide two lists identifying the particular elements that they state are relevant in describing the sub-process 'Protect Locale and Perambulation':

'Actions' used for the Petri Net

*t*1: The investigator sends ready sign;

*t*2: The investigator starts perambulate;

*t*3: The supervisor gives start sign;

*t*4: The investigator sends finish sign;

*t*5: The supervisor sends finish sign.

'Conditions' used for the Petri Net

*p*1: The investigator prepares for starting;

*p*2: The investigator waits for starting;

*p*3: Ready sign of the investigator;

*p*4: The supervisor starts sign given;

*p*5: The supervisor waits for ready sign;

*p*6: The investigator perambulates;

*p*7: The supervisor supervises the procedure;

*p*8: Finish sign of the investigator;

*p*9: The end of perambulation procedure.

Wang and Yu provide a diagram, as shown in Figure 17, based on the actions and conditions contained in the previous lists:

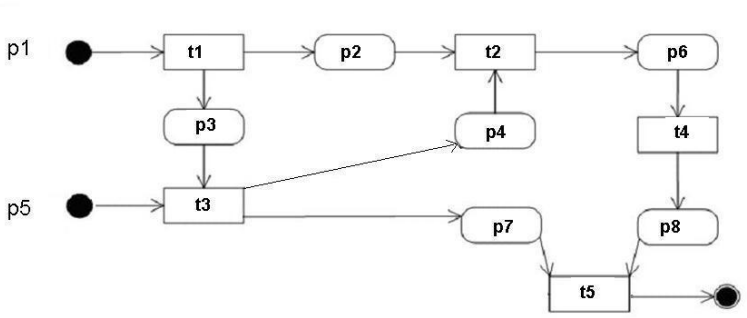

Figure 17 The Perambulation Procedure after Wang and Yu (2007)

The detail shown in Figure 17 can be summarised as:

> *An investigator tells his supervisor that he is ready; the supervisor gives authority to start a process, the investigator undertakes the process and informs the supervisor that it is complete and then the supervisor confirms the process is complete.*

2.5.3.5 Scientific approaches reviewed

This section of the literature review focussed more on the modelling approaches rather than the models themselves and comprised of the contributions from the following researchers:

- Stephenson (2003b)
- Hannan, Frings, Broucek and Turner (2003)
- Bogen and Dampier (2005)
- Kohn, Eloff and Olivier (2008)
- Ruan and Heibner (2009)
- Wang and Yu (2007).

Although Stephenson (2003b), Wang and Yu (2007) support the introduction of a formal language to describe digital forensic process models their particular approaches have not been as popular as that of utilising Activity and other diagrams from UML.

2.6 Summary

This chapter has reviewed the existing body of knowledge in relation to the environment of digital forensics and the existing process models for the acquisition of digital data. Although there has been little agreement on a definition of the digital forensic process, more recently there has been a call to adopt a formal methodology, with UML seeming to have the most support.

Chapter 3 now builds upon the information obtained in the literature review of Chapter 2 and includes an assessment of the models and approaches that were discussed therein.

Chapter 3: Model Requirements

3.1 Introduction

In their description of the DSRP (the design science model adopted for this research) Peffers et al (2006) state that the resources required to define the objectives of a solution include a "…knowledge of the state of the problems and current solutions and their efficacy, if any" (p. 90). The 'knowledge of the state of the problem' and the 'current solutions' for this research have been covered in Chapter 1 and the literature review of Chapter 2. This chapter now describes the process for assessing the current models and approaches discussed in Chapter 2 in order to identify the essential components of the new model that will form the basis of the new model's design and development stage that will be covered in Chapter 4.

3.2 Assessment criteria for previous models

Following on from the Research Objective the overarching requirements of a process model for the acquisition of digital evidence are that:

- There must be a formal representation of the model
- The model must be relevant to the fields of commerce, law enforcement and incident response.

In addition to considering the Research Objective when reviewing each model, in order to determine if there are any attributes of existing models that

could aid in the development of a new model a framework based on the work of Carrier and Spafford (2003) has been utilised which provides a list of the essential requirements for a digital forensic process model[22]. The Carrier and Spafford requirements form a common yardstick for helping to determine which of the reviewed models contains attributes suitable for inclusion in the ADAM. The five requirements of a digital forensic process model as proposed by Carrier and Spafford (2003) are:

1. It must have a basis in existing physical crime scene investigation theory;
2. It must be practical—matching steps taken in actual investigations;
3. It must be technology neutral to ensure the process isn't constrained by current products and procedures;
4. It must have specificity in relation to the classifications or categories used in order to facilitate technology requirement development; and
5. It must be applicable to all possible user communities.

Each model will be given a score out of five based on how many of the Carrier and Spafford requirements have been met. In addition to this, a score based on the Daubert test (Supreme Court of the United States, 1993) will also be applied on the basis that it is a commonly-referenced process used to assess the reliability of scientific evidence by many courts. The Daubert test seeks to determine:

[22] These requirements have also been used by Beebe and Clark (2004) as the basis for the assessment of their own process model.

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

Although the original court transcript includes the 'error rate' and 'standards' as a single factor it is not uncommon to find the test quoted as consisting of five criteria with 'error rate' and 'standards' separated (Pace & Sheehan, 2002; Richards, 2009). Other interpretations are that sometimes 'standards' within the four tests isn't mentioned (Kenneally, 2005) while Marsico groups 'standards' with 'general acceptance' rather than with 'error rates' (2005). For this research the approach adopted is that in order to establish an error rate there have to be standards associated with the particular process or methodology such that they form a single factor (Cheng, 2007). This consideration of 'standards' is separate and independent of the various guidelines and standards covered in 2.3. Each model will be assessed and given a score out of four based on how many of the individual Daubert tests are met.

The application of the Daubert test to existing models may provide an indication of how appropriate, or otherwise, the Daubert test criteria are for aiding the courts in the assessment of the reliability of digital evidence produced using acquisition process models (Cheng, 2007). Although ultimately it is a matter for a court to come to its own conclusion with respect to how a particular

model ‘scores’ under the Daubert test the fact that the criteria are known allows a prima facie examination to be undertaken. Given that there is little or no information relating to the outcome of any court assessments in relation to many of the models this prima facie examination will be the first time that this information will have been produced, albeit based on a single researcher’s interpretation.

3.3 Assessment of previous models

There are no comprehensive studies from which to draw assessment data for earlier process models and this section of the chapter describes how this research has assessed these models. The assessment process is not presented as a definitive assessment but rather the scores assigned to the various models are later used to provide a rough indication of how many of the attributes stated in the selection criteria have been met by a particular model.

The earlier process models included in the literature review will be assessed individually and scored based on the Carrier and Spafford criteria and the Daubert test (except where the models are examples of the application of a particular approach).

3.3.1 The Abstract Digital Forensics Model (ADFM)

There are shortcomings in this model that have been identified to some extent by the authors themselves as they note several disadvantages of applying their own framework, namely:

1. The current high-level approach to categories may be too general to be applied in practice
2. There does not seem to be a way of testing the model
3. As the model is developed to increase its detail it becomes more complex and more cumbersome to use. (Reith, et al., 2002, pp. 8-9)

Another shortcoming of the Abstract Digital Forensics Model in relation to the 'essential components' of the research question is that despite being an 'important facet', the chain of custody is assumed to be automatically incorporated without explicit reference to it in the model. This important aspect of forensic work should be specifically covered in a digital forensics model (Boddington, Hobbs, & Mann, 2008; Peisert, et al., 2008; Selamat, Yusof, & Sahib, 2008). Whilst suggesting that the Abstract Digital Forensics Model meets the requirement of a general framework the authors of a later paper (Carrier & Spafford, 2003) comment that in reality some of the phases would be in a different order and the names of some of the phases have the potential to cause confusion.

Based on the Carrier and Spafford criteria the ADFM meets the first requirement in that it is based on 'the traditional approach' and is also specific enough to allow for technology to be developed to assist the investigator whilst not being restrictive to a particular product, procedure or environment (Requirements 1, 3, 4 & 5). However, it has significant shortcomings in terms of practicality and its ability to accommodate changes without becoming overly complex (Requirement 2). The Carrier and Spafford score for the ADFM is 4/5 as it meets four out of the five criteria stated in section 3.2.

In relation to the selected Daubert test the authors admit that there does not seem to be a way to test the model and although it has been published and peer reviewed comments from the authors and Beebe & Clark suggest the model is incomplete and not practical (Beebe & Clark, 2004, p. 1). There do not appear to be any standards referenced by the ADFM and there seems to have been little or none of the necessary development since the model was proposed. Although there has been some support for the approach, there is also significant criticism as well and it has not achieved general acceptance. The Daubert test score for the ADFM is 1/4 as it meets only one out of the four test conditions - this process will be used for all the following models where a score can be assessed.

3.3.2 Integrated Digital Investigation Process (IDIP)

Baryamureeba & Tushabe (2004) identified various weaknesses (centred around a lack of practicality) in the IDIP developed by Carrier and Spafford (2003) and offered a modified version, the Enhanced Digital Investigation Process Model (EDIPM), that sought to address these shortcomings and is covered later in section 0. Further criticism of the IDIP comes from Shin (2008) who suggests that Carrier and Spafford have missed out important categories such as: ‘classification of the cybercrime’, ‘deciding investigation priority’ and ‘psychological profiling’, although these views do not seem to be shared by other researchers and these categories seem to add unnecessary complications to the process.

Rogers et al (2006) point out that while the IDIP may be suitable for investigations in which the whole process is likely to be followed the time constraints of certain investigations, such as those involving child abduction, make the model impractical. This criticism seems a little harsh in that the IDIP

does not tie the practitioner to a particular time scale and many of the stages may be 'ticked off' relatively quickly in practice. Furthermore, the requirement that the court needs to be able to see a structured process which it can assess for reliability means that the concept of a 'fast track' approach implied by Rogers et al is in itself a risk that data obtained in such a fashion may be challenged in court.

Whilst Carrier and Spafford's (2003) approach is open to criticism, for instance Baryamureeba & Tushabe (2004) are critical of a lack of specificity in relation to the physical location of particular crime scenes, other authors such as Sommer (1998), Reith (2002) and Mercuri (2005) agree that the approach for obtaining digital evidence is not fundamentally any different from that adopted in relation to obtaining 'conventional' evidence. Other researchers, such as Saferstein (2010) and Boddington, Hobbs & Mann (2008) go further in support of Carrier and Spafford's approach by identifying a fundamental similarity between the physical and digital crime scene domains. Despite criticism of the IDIP many of the ideas that it introduced were adopted by other researchers, particularly the concept of a digital crime scene (Baryamureeba & Tushabe, 2004; Beebe & Clark, 2004; Kohn, Eloff, & Olivier, 2006).

Based on their own criteria the IDIP meets the requirements that it needs to be based on the existing theory for physical investigations, is not technology-specific but allows for technology to be used to assist the investigator and can be applied generally amongst practitioners working in different areas of digital forensics. Where the IDIP is weaker is in the area of practicality and it has been criticised in this respect by several researchers in this area (Beebe & Clark, 2004; Rogers, 2004). The IDIP is given a Carrier and Spafford score of 4/5.

In relation to the Daubert tests, although Carrier and Spafford provide two case studies in which they map activities to the IDIP there does not seem to have been any independent testing of the model. With respect to peer review of the IDIP, the feedback has not always been positive (Baryamureeba & Tushabe, 2004; Peisert, et al., 2008; Rogers, et al., 2006), although other researchers have used some of the concepts of a 'digital crime scene' as an element in their own models (Beebe & Clark, 2004; Kohn, et al., 2006). A further weakness of the IDIP from the perspective of the Daubert tests is that there do not appear to be any standards associated with the model so the Daubert Score for the model is 1/4.

Although Carrier and Spafford contribute many useful elements for the digital forensic process, particularly the idea of the 'Digital Crime Scene', the key failing of their model is an overall lack of practicality.

3.3.3 Enhanced Digital Investigation Process Model (EDIPM)

The most significant contribution of the EDIPM is the idea that the phases are iterative rather than linear, however Baryamureeba and Tushabe's (2004) descriptions of phases lean heavily towards incident response, unlike Carrier and Spafford's IDIP (2003) whose phase descriptions can be read in generic terms. An example of this focus is in the scenario used to describe how the model could be used with the introduction of 'primary' and 'secondary' crime scenes and the 'Traceback' phase that involve a computer system (the secondary crime scene) being accessed from another location (the primary crime scene) necessitating the employment of various Internet-related tools to 'Traceback' the origin of the 'attack'.

The descriptive narrative is sometimes unclear, such as the use of the terms ‘multiple analysis’ and ‘synchronized’ that are not explained and that do not have an obvious meaning in the context of analysis. Perumal (2009) criticises the EDIPM for missing essential elements such as the ‘chain of custody’ while Wang and Yu (2007) criticise the practicality of this model (and the earlier IDIP) on the basis that they are both “abstract and cursory” (p. 1).

In relation to the Carrier and Spafford criteria, the EDIPM does meet the requirement to reflect a physical crime scene process and is not dependent on any particular technology. However, the description and structure of the model indicates a heavy focus on incident response thereby reducing its practicality in other areas. Furthermore, a lack of guidance in the EDIPM’s application, such as how the iterative steps feature in the process flow, and unclear narrative make it difficult to apply even within the incident response field. This would hinder the design of technological tools to assist the practitioner. The EDIPM is given a Carrier and Spafford score of 2/5.

In relation to the Daubert tests there does not seem to have been any testing of the EIDIP but it has been published and peer reviewed, although as per the Carrier and Spafford model it has been criticized for lack of practicality (Kohn, et al., 2006). Whilst other researchers acknowledge the EDIPM there are no other models based on it, there are no standards associated with the model and there is no evidence that the EDIPM has been generally accepted. The Daubert score for this model is given as 1/4.

3.3.4 Digital Crime Scene Analysis model (DCSA)

Rogers (2004) states that the 'overriding principal' for the DCSA model is that it should be independent of tools as per Carrier and Spafford (2003) and McKemmish (1999) whilst adhering to the "…criminalistic principles of being methodical, accurate, ensuring authenticity and reproducibility of evidence, maintaining the chain of custody and minimizing the contamination of the original scene…" (p. 14). Rogers also identifies the need, when applying the DCSA model, to keep within the limits of the practitioner's skills and knowledge together with the need to maintain 'proper documentation'.

A further useful contribution from Rogers is the concept of 'forensically sound tasks'. These tasks are derived from 'properties' of digital forensics and comprise of Authenticity, Chain of Custody, Integrity, Minimization and Reproducibility. Rogers cites McKemmish (1999) and Mocas (2004) as inspiration for these properties. However, on reviewing the tasks in detail it appears that Rogers has created separate tasks for what could realistically be one task in practice. This is evident in the tasks 'control the scene', 'survey the scene' and 'document the scene'. In practice these could all be covered by the requirement to 'process the scene as per local guidelines' as one is unlikely to carry out any of these tasks in isolation (Baryamureeba & Tushabe, 2004; I.O.C.E, 2002). Similarly, the tasks 'Identify potential evidence and containers of evidence' and 'Determine the evidence modality' could be undertaken at the same time or as part of the same task 'Identify the source and nature of potential evidence' (Baryamureeba & Tushabe, 2004; Ciardhuáin, 2004). The task 'package for transport' which is identified as being important as it is "…the second most crucial event in crime scene analysis" (Rogers, 2004, p. 24) due to

the potential for evidence to be lost or destroyed, could include the following task ‘turn over to lab or appropriate offsite facility’ which seems to be the final outcome of the previous task. Rogers identifies the risk of transporting evidence which comes about because the evidence leaves the controlled environment of the crime scene and enters a ‘no man’s land’ before reaching the ‘lab’. However the task ‘package and deliver to secure facility’ would be a more reasonable description for the final task involved in acquiring digital evidence.

In relation to the Carrier and Spafford (2003) criteria, Rogers’ DCSA model meets all five requirements being; 1) based on existing crime scene investigations, 2) following the steps of an actual investigation (notwithstanding earlier comments in relation to additional steps), 3) unconstrained to a particular tool or technology, 4) detailed enough to allow for the development of technical aids and 5) capable of being applied in a variety of environments. The DCSA model is given a Carrier and Spafford score of 5/5.

However, in relation to the Daubert test, there is no evidence of any testing having been carried out on the DCSA model and there do not appear to be any standards associated with the model. There seems to have been little adverse comment since the DCSA model was proposed and it has appeared in a handbook (Tipton & Krause, 2006) but there is no indication of its general acceptance or widespread adoption. The Daubert score for the DCSA model is given as 1/4. This is an interesting example of the disparity between what experts in the field, such as Carrier and Spafford, consider makes a good process model for acquiring digital evidence and how the courts might assess the process described by that model.

Despite some of the issues highlighted in relation to a few of the concepts introduced in the DCSA model the overall approach is a valuable contribution to the field of digital forensics, especially the emphasis on the data acquisition element which seems to be lacking in other models . The DCSA model is let down by a lack of testing or associated standards and does not appear to have been widely adopted. In addition, the stance taken by Rogers (2004) that the type of investigation should determine the high-level process can be criticised as the type of investigation can potentially change, e.g. if child pornography is located during a fraud investigation, and this approach has not been adopted elsewhere.

3.3.5 A Hierarchical, Objectives-Based Framework for the Digital Investigations Process (HOFDIP)

The description provided by Beebe and Clark (2004) of the Preparation phase of the HOFDIP suggests it is based on the perspective of a digital forensic practitioner working within their own organization, i.e. incident response. This emphasis is apparent through the author's reference to an organization's decision regarding its 'forensic readiness' (an incident response concept) as well as further references to 'deterrence' and 'computer security incidents' (Beebe & Clark, 2004). The inclusion of an 'incident response' phase is also further evidence of the HOFDIP's focus although a useful aspect of the model is the introduction of 'principles' that are then applied throughout the investigations process, these being 'evidence preservation' and 'documentation'.

In relation to 'evidence preservation' two goals are stated which are firstly to maximize evidence availability and quality and secondly to maintain the integrity of the evidence during the digital investigation process. The goal of

‘documentation’ is to record all information relevant to (or generated by) the investigation. Both of these principles are reflected in other models (Brown, 2006; Ciardhuáin, 2004; Rogers, et al., 2006). Despite Beebe and Clark’s (2004) stated intention to create a model that incorporates the activities of all the previous models they have defined their own principles rather than adopt those defined by the Association of Chief Police Officers (2003) or the IOCE (2002). This seems counter-productive and it would be better to add (if necessary) to existing definitions which are already widely recognised and relatively well-established.

Notwithstanding the introduction of their own principles Beebe and Clarke’s main argument for adopting their model centres around the fact that it is ‘multi-tiered’ (in contrast to the ‘single tier’ approach they identify in other models) which they contend is more appropriate for the complex digital investigation process. Where detail has been provided for the ‘second-tier’ activities (as part of the Data Analysis phase) the prescriptive nature of the tasks for particular objectives would be more appropriate as an appendix that lists possible activities rather than being part of the model to address Schatz’s (2007) ‘complexity problem’.

In relation to the Carrier and Spafford criteria, the HOFDIP meets the requirements to be based on existing physical crime scene theory and to be ‘technology independent’. However, the model in its current state is not practical and is missing the detail in some of the stages necessary to provide a design for technological aids. In addition, it is focused towards the area of incident response rather than being generic. The HOFDIP is given a Carrier and Spafford score of 2/5.

Beebe and Clark (2004) themselves give their framework a high rating based on the Carrier and Spafford criteria suggesting it can be applied generally (despite its incident response phase and focus) and when further developed they believe it will provide sufficient detail to meet the requirements of specificity and practicality. However, Beebe and Clarke admit that as the framework stands in its current form it is "incomplete" (2004, p. 15).

In relation to the Daubert tests there is no evidence that any testing has been undertaken on the HOFDIP as described by Beebe and Clark and there do not appear to be any standards associated with the framework nor is there evidence of the necessary development undertaken since the HOFDIP was proposed. Although the HOFDIP has been published and peer reviewed, the comments from Beebe and Clark suggesting that the framework is incomplete and not yet practical (Beebe & Clark, 2004, pp. 15-16) reduce its usefulness. The Daubert score for the HOFDIP is given as 1/4.

Beebe and Clark's key contribution is the concept of a 'multi-tiered' as opposed to the 'single tier' approach adopted in other models; however several of the key phases and principals are not structured in such a way that they are relevant in their current form to all digital forensic practitioners due to their bias towards incident response. Although their proposed framework is claimed to be another summary of 'best practice', references by Beebe and Clark, such as the installation of 'activity monitoring' devices, have been introduced by the authors as this does not feature in other 'generic' digital forensic models and would be relevant mainly to network intrusion investigations.

3.3.6 Framework for a Digital Forensic Investigation (FDFI)

Kohn et al (2006) combine phases in the FDFI that they have identified in earlier models and highlight legal knowledge of the environment and the 'documentation of all steps taken' as being key elements of any digital forensic model. These are key contributions as identified by Selamat et al (2008), although they propose expanding the process model to five phases (see section 3.3.8).

In relation to the Carrier and Spafford criteria the FDFI meets the requirements to be based on existing physical crime scene theory in as much as the high-level description could be applied in this context and is practical in the sense that its high-level approach does not introduce any hindrance to the practitioner nor does it make it 'technology dependent'. However the lack of detail prevents the adoption of technology to assist with the framework's implementation and the leaning towards the area of incident response means that it is not generic enough to be applied across all areas of the digital forensic environment. The FDFI is given a Carrier and Spafford score of 3/5.

In relation to the Daubert tests there is no evidence provided by Kohn et al (2006) that any testing has been undertaken on the FDFI, there do not appear to be any standards associated or referenced by the framework and there seems to have been no development since the framework was proposed. The FDFI has been published and peer reviewed but does not seem to have been developed further. The Daubert score for the FDFI is given as 1/4.

3.3.7 Two-Dimensional Evidence Reliability Amplification Process Model (TDERAPM)

Within the TDERAPM the step for Initialisation covers two roles, Inspector and Manager with the Inspector being the technical 'hands on' person. Khatir, Hejazi and Sneiders (2008) suggest that at the outset of the investigation the manager should refer to similar previous cases (also suggested by Beebe and Clark (2004)) in order to estimate costs/time/resources and obtain an idea of the likely outcome. Whilst this may seem worthwhile in theory it does not seem to be very practical. The first issue is that the process assumes all previous cases have been adequately recorded and classified although no system for this is suggested in the paper which only refers to some form of purpose-built database. Secondly, the details of a case are likely to differ from one case to the next and to suggest that the costs or the potential conviction rate can be estimated based on previous cases is unrealistic, certainly without a large body of research to draw upon and there is currently no evidence that this exists.

Other aspects of the initialization phase such as determining legal issues, developing a plan, receiving authorisation and setting up a team would be recognisable from the contributions of other authors such as Brown (2006) in his book 'Computer Evidence: Collection and Preservation', Freiling & Schwittay (2007) with their 'Common Process Model for Incident Response' and Stephenson (2003a) with his 'Comprehensive Approach to Digital Incident Investigation'. However, the Khatir et al (2008) focus on 'incident response' as opposed to a generic digital forensic investigation are apparent in their comment "Besides hardening the security of the compromised organization, the ultimate goal of a digital forensic investigation is to support the prosecution"(Khatir, et

al., 2008, p. 3). Notwithstanding the previous comment, with its incident response focus, the reference "to support the prosecution" does not take into account the fact that there may not be a prosecution element to the matter nor does it consider circumstances in which the digital forensic practitioner is working for the defence.

In relation to the Carrier and Spafford criteria the TDERAPM meets the test for being based on the existing theory for physical crime scenes and not being 'technology dependent'. However, although the key factors of an investigation are identified in a unique format the high-level approach is not of great benefit to the investigator as a lot of detail is missing thus limiting the practical aspect of this model as well as the ability to design technology to assist the practitioner. The high-level abstract model (discussed in section 2.5.1.9) would seem to be generic as there are no environment-specific aspects. However, some of the narrative used to describe particular aspects of the model is not generic, for example the reference to "supporting the prosecution". There are also suggestions of an incident response focus to the TDERAPM through comments such as "…hardening the security of the compromised organization" (Khatir, et al., 2008, p. 3). These aspects will require modification in order to remove this bias from the TDERAPM. The model has been given a Carrier and Spafford score of 2/5.

In relation to the Daubert tests there is no evidence that any testing has been undertaken, there do not appear to be any standards referenced or associated with the TDERAPM model and there seems to have been no development since it was proposed. The model has been published and peer

reviewed but does not seem to have been developed further. The Daubert score for the TDERAPM is given as 1/4.

Where many authors adopt over-riding principles (Beebe & Clark, 2004; Selamat, et al., 2008; Wang & Yu, 2007) Khatir et al have used the term 'umbrella activities' and the main contribution provided by this paper is the consideration of management issues rather than purely practical/technical process issues. However, the TDERAPM would be difficult to apply in practice given the lack of information regarding its implementation.

3.3.8 Mapping Process of Digital Forensic Investigation Framework

At a high level the classification system used by Selamat, Yusof and Sahib (2008) provides a useful summary of the phases that make up the digital forensic process. However, the detail provided in relation to each phase is less clear. For instance, the meaning of "provide a mechanism for the incident to be detected and confirmed" (Selamat, et al., 2008, p. 167) in Phase 1 is vague and does not appear to be generic but rather leaning towards incident response. Similarly vague is an activity in Phase 2 "translated [sic] the media into data" (Selamat, et al., 2008, p. 167). Although proposing a guide based on previous work, the Selamat et al paper is almost entirely a summary of earlier models and as it provides only brief Results and Conclusion sections it has not been assessed against either the Carrier and Spafford or Daubert criteria.

3.3.9 Four Step Forensic Process model

A significant criticism of the Four Step Forensic Process model is that it seems to begin with the Collection stage without the necessary preliminary activities such as confirming that you are authorised to carry out the activity and undertaking an initial planning stage, followed by an onsite survey (Brown, 2006; Casey, 2004; Sammes & Jenkinson, 2007). Unlike other researchers who incorporate a planning stage (Brown, 2006; Casey, 2004; Sammes & Jenkinson, 2007) Kent, Chevalier, Grance and Dang (2006) limit the requirements of the plan for acquiring the data to prioritizing the data based on three factors, namely; 'likely value', 'volatility' and 'amount of effort required'. These factors reflect the model's focus on incident response. Whilst Kent et al (2006) provide a lot of background detail to assist an organisation to develop a general capability in terms of training, procedures and resources, the lack of a separate planning stage prior to the physical collection of data is a serious shortcoming, particularly for other environments such as law enforcement and commercial practice (Bogen & Dampier, 2005; Ciardhuáin, 2004; Kohn, et al., 2006). In several places throughout the model's description Kent et al (2006) refer to 'policies and procedures', 'decisions', 'concerns' and 'considerations' prior to the collection of data which indicates an awareness of the need for processes to occur prior to the physical collection of data but this awareness is not translated into a separate planning aspect of the model. Overall, the process described by Kent et al (2006) covers the standard forensic procedures and provides some detail that would assist an organization in preparing its 'incident response' capabilities. The lack of clear structure and emphasis of important activities detracts from the model's general usefulness in other environments.

Although Kent et al (2006) include within their guide a high-level and simplistic model of the forensic process (with the whole data acquisition process combined under the 'collection' stage) many of the detailed elements described in the narrative need to be selected or adjusted for an organisations' particular purpose and given the intended incident response focus the Kent et al model has not been evaluated against the Carrier and Spafford or Daubert criteria.

3.3.10 Common Process Model for Incident Response and Computer Forensics (CPMIRCF)

Although the title of their model suggests that Freiling and Schwittay (2007) have prepared a significant amount of the groundwork for a generic model, in reality their aim was to incorporate some techniques and practices from the field they see as 'computer forensics' into the 'incident response' field. In addition, they do see that the 'good management' of incident response practice could be a benefit in 'pure' computer forensic cases. In relation to the Carrier and Spafford criteria, the CPMIRFC is not based on a physical crime scene scenario and with its heavy focus on incident response it is not applicable as a generic model and misses many steps that would be part of an actual investigation. It is however not 'technology dependent' and a level of specificity has been achieved in relation to classifications and categories. The Carrier and Spafford score is given as 2/5.

With regard to the Daubert test, there is no evidence of any testing or peer-review, and there are no standards associated with it. There is also no evidence of acceptance within the communities for which it was designed. The Daubert score is given as 0/4.

3.3.11 Systematic Digital Forensic Investigation Model (SDFIM)

The activities associated with the various phases of the SDFIM are valid but the criteria for the classification of an activity (or collection of activities) as a phase does not appear to have been applied consistently. For instance, the whole of the preparation activities are covered in one phase whereas the initial onsite activities are spread across six phases. Many phases could be incorporated into a single phase such as Phase 2 (Secure the Scene), Phase 3 (Survey and Recognition) and Phase 5 (Communication Shielding) which would be consistent with the approach taken by many other researchers such as Beebe and Clark (2004), Rogers (2006), Selamat (2008) and Carrier and Spafford (2003).

Another issue with the model is that there are no overriding activities, with 'documentation of the scene' being a specific phase in its own right. Most importantly, the creation and maintenance of a chain of custody is mentioned but not associated with items of potential evidence and it is unclear how it is to be applied in the model.

Agarwal, Gupta, M., Gupta, S. and Gupta, S. C. (Agarwal, et al., 2011) make the statement that the "Majority of the evidence involving mobile devices will be of a volatile nature, being present in ROM" (p. 126). There are technical errors with this statement:

- The majority of evidence contained in mobile devices is non-volatile as most of the data is stored in flash memory and is not lost when power is removed

- The volatile data in a mobile device mostly relates to current communications which Phase 5 of the SDFIM eliminates through the requirement to isolate the device from its carrier
- Data cannot be lost (or altered) from ROM (Read Only Memory) through user activity and mobile devices typically don't use this type of memory.

Based on the Carrier and Spafford criteria the SDFIM is based on physical crime scene theory and is technology neutral as well as being applicable to all environments. There are however significant weaknesses in terms of practicality, as key steps such as chain of evidence are not well documented, and specificity due to inconsistencies in the data flow. The Carrier and Spafford score is given as 3/5.

In relation to the Daubert test there is no evidence of testing having been carried out although the SDFIM has been published in a peer-reviewed journal. There are no standards associated with the model and there is no indication of acceptance within the relevant community. The Daubert score is given as 1/4.

3.3.12 Extended Model of Cybercrime Investigations (EMCI)

The EMCI was produced based in the belief that other models did not cover all aspects of the investigation process. Ciardhuáin's (2004) inclusion of an 'authorisation' activity is something normally lacking in other models which may describe the need to obtain warrants etc. but only as part of a 'preparation' or 'readiness' phase. For instance Reith et al (2002) recognise an 'identification component' whilst Carrier and Spafford (2003) have a 'Confirmation and

Authorization Phase' as one of their Deployment phases. Ciardhuáin suggests that there may be both internal and external authorities involved. This concept is one that has been selected as a useful contribution to a new generic model. With regard to the 'Planning' activity Ciardhuáin identifies several specific sources of influence such as regulations, legislation, internal strategies and internal policies whilst recognising that there is a potential need to re-address the issue of authorisation should the investigation scope be found to be greater than that anticipated in the authorisation activity. The inclusion of a planning stage of an investigation is supported by the initial work of McKemmish (1999) and is in keeping with other contemporary models (Baryamureeba & Tushabe, 2004; Carrier & Spafford, 2003; Reith, et al., 2002). More recently researchers and practitioners give a high weighting to this type of activity (Brown, 2006; Casey, 2004; Sammes & Jenkinson, 2007)

Ciardhuáin's (2004) 'notification' activity involves, where appropriate, notifying the subject or relevant person/authority that the investigation has commenced. It could be argued that whilst this could be identified as an instance of information flow it could just as easily be incorporated into a more detailed planning stage rather than stand alone as a specific activity. Ciardhuáin (2004) describes his 'search and identification of evidence' activity as dealing with locating and identifying the evidence for the next activity and goes on to give an example that this could be considered to be "...finding the computer used by a suspect and confirming that it is the one of interest to the investigators" (p. 6). In this respect Ciardhuáin's statement is too simplistic as finding the computer used by a suspect is not in itself locating evidence but is locating a potential source of evidence as the physical computer is unlikely to be an item of evidence in its

own right but merely ‘seized property’ (Hutton & Johnston, 2000, p. 151). It is also quite possible for the computer to contain nothing of evidentiary value and therefore no evidence will have been seized at all. Steel (2006) provides a better description of this process “Identify the scene - Determine the location or locations where digital evidence of the crime may be resident” (p. 12).

The remaining activities in the EMCI relating to digital evidence acquisition (Collection, Transport and Storage) are roughly similar to those of other models but of particular interest, especially in relation to the Daubert test, is the fact that Ciardhuáin (2004) attempted to test his model. However, unlike Venter (2006) (who later used training sessions for his testing) Ciardhuáin (2004) adopted a ‘focus group’ format for questioning a group of police computer crime investigators[23] and also questioned an ‘experienced investigator’. The results of the focus group where that the EMCI was seen as a good generic description of a police investigation (not just a computer crime investigation) and the ‘backtracking’ was seen as an important feature (Ciardhuáin, 2004). However, although there were no major elements omitted from the EMCI the respondents felt there were activities included that were not normally seen as being separate from other investigative processes and some of these were regarded as irrelevant for their work, namely: Awareness, Transport, Storage and Dissemination (Ciardhuáin, 2004). From a law enforcement perspective the respondents felt that there needed to be tighter controls on the flow of information and were concerned with information ‘leakage’ because of the requirements for confidentiality imposed on them by “external policies,

[23] Size of group not stated

regulation and legislation" (p. 13). There is no comment attributed to the 'experienced investigator' and under the section 'future work' Ciardhuáin suggests that the EMCI should be tested in other environments and identifies those areas of interest as being auditing, civil litigation, investigations by system administrators and judicial inquiries.

In relation to the Carrier and Spafford criteria the EMCI is based on physical crime scene investigations; from the feedback of the focus group the model follows the main steps of an investigation it seems to be practical to implement whilst being generic and not tied to a particular technology. The only test it fails is that of providing sufficient detail to develop technological aids to the investigator. The EMCI is given a Carrier and Spafford score of 4/5.

In relation to the selected Daubert tests, testing has been undertaken (although this was through a focus group session rather than field-based trials and Ciardhuáin identifies the need for testing in fields other than law enforcement). The EMCI has been published and peer reviewed but it does not seem to have been developed further to gain general acceptance and there do not appear to be any standards associated with the model. The overall Daubert score for the EMCI is given as 2/4.

The EMCI introduced a new approach to describing the activities undertaken in a digital forensic investigation by focussing on the flow of information although accepting that " Some additional emphasis needs to be placed on the control of the information flows in the law enforcement environment" (Ciardhuáin, 2004, p. 14).

3.3.13 FORensics ZAchman framework (FORZA)

There are aspects of the FORZA model that are unclear, such as the lack of identification of a 'terminating process', missing data flow between the 'legal advisor' and the 'legal prosecutor' plus the discrepancies between the narrative and diagram in relation to data flow direction. Although the concept of modelling the process flows is a key contribution to the research environment there are various questions raised around how the process would work in the field and many aspects of the narrative appear to be theoretical rather than based on practice.

In relation to the Carrier and Spafford criteria the FORZA model is based on an internal incident response scenario rather than existing theory for a physical crime investigation (although reference to the 5WH approach is generic). From the information supplied it is also not clear that the framework is practical and follows the steps of an actual investigation as the worked example is too theoretical to confirm practical applicability. Examination of the example of process flows raises several questions. For instance, the process flow for most tasks is only one way from the Case Leader whilst the narrative suggests a two-way interaction. Furthermore, there is no 'flow' from the 'Conceptual Security Layer' even though this is not identified as the terminating process in the narrative and in practice there is likely to be some process flow between the 'legal advisor' and the 'legal prosecutor' (assuming they are not the same person). Whilst the model is not dependent on a particular technology the overall lack of detail would prevent the development of general technology requirements. In addition the model is focused towards incident response and

therefore would need development to become a candidate for a generic model. Because of these issues the Carrier and Spafford score is 1/5.

In relation to the Daubert tests, although the model description has been published there is no evidence that any testing has been undertaken, there do not appear to be any standards associated with the model and there is no evidence of general acceptance. The overall Daubert Score is 1/4.

3.3.14 Process Flow Model

While the basic concept of providing flowcharts to assist with the collection of potential evidence, albeit restricted to physical devices, seems to be sound, the intended target audience and the implementation of the concept has been strongly criticised. Fundamentally, the aim to provide adequate training for those with limited technical background seems ambitious given the nature of the digital forensic field (Calhoun, 2008; Carrier & Spafford, 2003; Steel, 2006). Even when the American National Institute of Justice (NIJ) produced a guideline for 'first responders' they stated that the assumption was that these were personnel tasked with collecting digital evidence who were already technically trained (Ashcroft, 2001, p. 17).

Venter (2006) accepts that the process flow approach could come under criticism as being a type of checklist and is critical of the 'lists based approach' based on observations made during training sessions using the US Department of Justices' Guide for First Responders (Ashcroft, 2001) in which the candidates where described as being anxious and making mistakes with the conclusion that the "... lists based approach did therefore not provide sufficient support to the candidates" (Venter, 2006, p. 3). The distinction being made between the term 'list' and 'checklist' is not clear although the process flow approach "…adds

sequence to actions in a manner that is easier to understand than the list approach" (Venter, 2006, p. 6). Venter suggests that his process flow model provides a "…rigorous approach that will deal adequately with most situations" (p. 6) as required by the intended audience and indicates support for his approach from Brezinski (2002) on the basis that the "…amount of decision making needed to be made during the collection process must be minimized" (p. 6).

Whilst it would seem that the process flow approach suggested by Venter is relatively easy to use, given the technical nature of digital forensic investigations the first design principle's target audience would seem to conflict with the nature of forensic work that requires a technical expert to provide evidence, i.e. a person a judge determines is an expert in the relevant field by virtue of their experience and/or training (Mason, 2007, p. 124). The second design principle, that of making the process applicable in 'most cases', would also seem to be ambitious given the author's own recognition of Beebe and Clark's argument against a 'checklist' approach on the basis that each situation can be different (Beebe & Clark, 2004, p. 2). Situations can be identified that are not covered by the 'process flows', such as encountering a file server or laptop, as well as inadequate instructions, e.g. not stating that the hard disk must be placed in an electrostatic bag for protection (Ashcroft, 2001, p. 42; SWGDE, 2006, p. 4).

There is some merit in the third principle that has the concept of assisting with expert testimony through reference to a 'standard' procedure of some form that is easy to follow. However, on the basis that the model is for people with limited technical background they would not qualify as 'expert witnesses' in their own right nor would they be able to express opinions (a key feature of

expert witness testimony; (Mason, 2007, p. 124). It is therefore unclear how this principle would apply in practice. The final principle seems sensible on the basis that for the model to be of any practical use it should be able applicable in the 'real' world rather than be confined to a training environment.

The restriction on the size of the document containing a particular process flow may seem like a reasonable proposition but this may be restrictive in practice, especially when trying to cater for all eventualities (for example, as the forms stand you are limited to recording only three hard disks per computer when it is relatively common to have 5-disk RAID arrays in business situations). The benefit of having a standard A4-sized form is also likely to be negated by having to compress information into this format. Furthermore, with the move towards documentation being presented in court in electronic format and police forces producing their reports in electronic format (such as the Western Australian Police Force Computer Crime Unit) the dimensions of documents when printed is less relevant than the information they contain. Even with regard to the output of Internet access log files and databases, neither of these lends itself to a convenient printed format However, Venter (2006) justifies the use of an A4 format by suggesting that this will enable all the documentation to be kept together, for instance in relation to a particular computer although he doesn't discuss why this is better than having one sheet per item of evidence to create a bundle of documents in the case of a computer with multiple hard disk drives. Another point is that other documentation, such as photos, scene sketches and notes associated with a particular item of potential evidence will be stored separately so there will be multiple forms/documents for each computer in any case (Quality Assurance Institute, 2007).

Examining the detail of how the process flow model should be applied through reference to a specific example (Process to follow at an Electronic Evidence Scene) has as the first task 'verifying the search warrant' which is relevant to law enforcement activities, but a better label would perhaps have been 'verify authority to undertake evidence collection' thus enabling the form to be used by all digital forensic practitioners. This would also identify whether in fact the various hard disk drives or other devices could be removed in their entirety and whether initial analysis was required prior to removing a device (i.e. requirements beyond the ability of the 'Cyber First Responder'). The next step is to answer the question 'suspects around?' which is very specific and could perhaps have been covered by an instruction to 'secure and document the scene' that would also encompass the next step 'Photograph general scene and details'. The process flow then moves to the stage where iterations of the collection process relating to each of the three identified device types begin before finishing with evidence processing tasks and leaving the scene. The evidence collection stage only considers physical evidence so the creation of forensic images or copies of relevant data are not considered and the actual process of how you would go about identifying which items may contain relevant information is not described in the text.

Although the intention seems to be to provide as much detailed advice as possible for the less-experienced responder there are fundamental problems with some of the detailed advice contained within the process flow. For instance, with regard to shutting down the computer or 'pulling the plug' Venter (2006) argues:

> In the absence of support, the power plug is removed from the machine. It is argued that preserving the integrity of the potential evidence on the hard disk is much more important than any evidence that may be lost due to an immediate shutdown (p. 13).

However, the advice to remove the power plug from a running machine if no technically competent person is available has the potential to cause major disruption to the computer's file system and "…can result in loss of evidence and potential severe civil liability" (Ashcroft, 2001, p. 35). Even in a law enforcement situation the Scientific Working Group on Digital Evidence warns "…pulling the plug could severely damage the system; disrupt legitimate business; and/or create officer and department liability" (SWGDE, 2006, p. 4). Of particular concern regarding the preceding advice is the fact that court orders will often require commercial digital forensic practitioners to provide an undertaking to ensure the items that they deal with are unharmed. This is an example of the type of problem that arises when non-IT personnel undertake this type of exercise.

A further issue in the detail is that despite allowing for the processing of laptops (and assuming the concept of pulling the plug on a running machine is acceptable) a laptop "...requires removal of the battery in addition to stand-alone power-down procedure" (Ashcroft, 2001, p. 43). No provision is made within the process flow for this situation. Removing a disk from a laptop that is still running (although if the lid is closed this may not be apparent) could potentially damage both the disk and laptop itself.

Although there are areas in which the Process Flow Model is open to criticism, in contrast to many other models Venter (2006) attempted to test his process flow by staging a trial that consisted of four courses involving law enforcement personnel with Venter setting the test and undertaking the assessment. However, Venter (2006) admits that based on the pass rates for the course "… it cannot conclusively be deduced that the process flows had a significant impact." (p. 17)

In relation to the Carrier and Spafford criteria the Venter Process Flow Model does not appear to be based on existing theory for a physical crime investigation and questions are raised with regard to the practicability of this framework given the restrictive nature of the forms and some contentious guidelines. However, the model is not dependent on a particular technology and there is sufficient detail to enable the development of technology requirements. In addition, despite the fact that in its present form it is more suited to incident response the process flow model is mostly generic. The Carrier and Spafford score is given as 3/5.

In relation to the selected Daubert tests, there is evidence of testing undertaken by Venter and the process flow model has been published and peer reviewed but does not seem to have been adopted or developed further, nor do there do not appear to be any standards associated with the model. The Daubert score is given as 1/4.

3.3.15 End-to-End Digital Investigation (EEDI)

In relation to the Carrier and Spafford criteria the EEDI model by Stephenson (2003b) is based on the DFRWS process for an investigation and follows the same practical steps. Although it is not dependent on a particular

technology its implementation in DIPL is reliant on an understanding of LISP-like language. While the high-level abstract framework would seem to allow for the EEDI's use across different aspects of digital forensics the model's emphasis on a limited sub-set of investigations, despite being based on the DFRWS, makes it unsuited for general use. The Carrier and Spafford score is given as 3/5.

In relation to the selected Daubert tests, the model has been published and peer reviewed but does not seem to have been generally accepted or developed further. There is also no evidence that any testing has been undertaken and there do not appear to be any standards associated with the model. The Daubert score is given as 1/4.

Despite the use of a formal language the fact that this language is minimally defined and is not widely used reduces its usefulness for helping to enhance the scientific standing of digital forensics through a formal definition of the acquisition process.

3.3.16 Cyber Tools On-line Search for Evidence (CTOSE)

A review of an example of the CTOSE model in practice contains decisions/actions that could be criticised. Firstly, the starting point is formally deciding which legal forum is appropriate. This is a flawed initial requirement as such a decision cannot always be determined at the outset of an investigation, especially if you don't know who was involved and therefore cannot determine the jurisdiction. Furthermore, there may be evidence that comes to light during the investigation that constitutes a more serious offence than that being investigated and therefore requires the case to be referred to a higher court.

A further criticism is that, although the intention of the model is to collect evidence in a way admissible to court, an example of its usage shows that a

decision on whether or not to prosecute is made even before the facts of the case are known. Not only does this seem be inappropriate given the intentions of the process model but in practice this decision is often made much later, especially as the person or persons involved have to be identified before a prosecution can even be considered and this doesn't always happen in an investigation.

Criticism can also be made of the decision for the appropriate standard of proof coming at the start of the investigation – again the placement of this process is not logical. If a 'low standard of proof' is selected and the investigation uncovers a serious criminal act it is probably too late to go back and re-acquire the evidence to a higher standard.

Given that the model works by presenting options based on the answers to earlier questions it can be seen that an error in the logic at the start of the process can direct the user down a path that may not be appropriate or that fails to present information that would be useful and relevant for a particular situation.

In relation to the Carrier and Spafford criteria the CTOSE model is designed for an internal incident response environment and does not incorporate the standard physical crime scene theory. Although the key factors of an investigation are identified the need to run the tool in a particular environment with an SQL database limits its practicality and ties it to this technology. The model does not seem to come with the complete decision tree data and the authors refer to the process model's complexity requiring implementation in the form of a computer application. Although some level of detail is provided for certain aspects of the model the overall lack of detail would prevent the development of further general technology requirements and as the model is

designed for incident response it is not suitable as a candidate for a generic model. The overall Carrier and Spafford score is given as 0/5

In relation to the selected Daubert tests, the model has been published and peer reviewed but does not seem to have been generally accepted or developed further. There is no evidence that any testing has been undertaken and there do not appear to be any standards associated with the model. The overall Daubert score is given as 1/4.

The concept of having a framework for acquiring digital data as part of a forensic process that has an associated database of advice/recommendations/information and which can be accessed through a relatively simple front-end application has merit, as digital forensic practitioners are constantly having to deal with new environments and situations as individuals and so a repository of lessons learnt/information found would be an invaluable asset. Unfortunately, the CTOSE project and the C*CAT application do not appear to have been developed further and an Internet search reveals a relatively small number of links – mostly references to the project from contemporary papers from the same field. This suggests that despite the backing of the European Union there was little support from practitioners in the field of digital forensics.

3.3.17 UML Domain Modelling

Bogen and Dampier (2005) recommend that domain modelling using the domain and ontology modelling language UML is appropriate for modelling digital forensic investigations but suggest that the syntax used for the model is less important than the knowledge gained by building the model. This last statement would appear to be at odds with the concept behind the UML in that

the intention with this language is to create a description (model) of a particular system in such a way that all those involved in its design, implementation and use are able to understand the information contained therein, normally in the context of software projects (Bell, 2003). Normally this requires the language used in the model to be precise and that suggests that the syntax must be important. However, in the context of using the language to simply model the digital forensic process (rather than being the specification for a software application) this requirement can be ignored.

As Bogen and Dampier (2005) develop their model it becomes apparent that whilst there are several references to digital storage devices and their relationships to other objects (such as people and workstations) there is no aspect of the model that shows how the information that is to be analysed gets into the 'system', although there is a stated need for 'preparation' and 'identifying items for analysis'.

The issue of acquiring the potential evidence is not described in Bogan and Dampier's 'case domain' model suggesting that the proposed unification of forensic model approaches does not cover all activities undertaken during a forensic investigation and is only applicable to the analysis stage. As the acquisition stage is not described the Bogan & Dampier model has not been assessed against the Carrier and Spafford criteria or Daubert tests but is included in this review because of its use of a formal modelling language to describe aspects of the digital forensic process.

3.3.18 Modelling Computer Forensic Process from Workflow Perspective

Although Wang and Yu's (2007) argument for using a Petri net to model the digital forensic process would seem to have merit there are aspects of the narrative where the authors provide comments that conflict with other practitioners. An example is the practice of creating an image on site and undertaking analysis on a *copy* of the data (thus preserving the 'original' as a backup) which Wang and Yu contend is not practical. Whilst it is true that creating the forensic image on site is not always ideal, Wang and Yu's comment is in contrast to the views of many practitioners working in this field (Arthur E. Hutt, 1995; Ashcroft, 2001; Association of Chief Police Officers, 2003; Baryamureeba & Tushabe, 2004; Beebe & Clark, 2004; Brezinski & Killalea, 2002; Brown, 2006; Carrier & Spafford, 2003; Casey, 2004; Craiger, 2005; Gosh, 2004; McKemmish, 1999).

Wang & Yu's paper is included because it describes a modelling approach (rather than the digital acquisition process), it has therefore not been assessed against the Carrier and Spafford criteria or Daubert tests.

3.4 Summary of model analysis

The review of relevant literature shows that since the First Digital Forensic Research Workshop was held in 2001 there has been little real progress in refining the process for the acquisition of digital data to the point where there is a formal definition 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 or stages involved. As

of January 2012 the US-CERT organisation still included in its online 'reading room' a paper (US-CERT, 2012) which suggests that we are no further forward with regard to digital forensics becoming a 'mainstream' scientific discipline than we were at the time of the 2001 DFRWS:

> 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, 2012, p. 1)

A summary of comments from the literature review indicate the lack of consensus amongst practitioners and researchers:

- Other models are too specific (Reith, et al., 2002)
- Other models are too abstract (Beebe & Clark, 2004)
- Other models are too narrow (Ciardhuáin, 2004)
- Other models are too broad (Rogers, 2004)
- Other models are too complex (Selamat, et al., 2008)
- Other models do not provide sufficient detail (Rogers, 2004)
- Other models are not practical (Baryamureeba & Tushabe, 2004)
- Other models lack flexibility (Khatir, et al., 2008)
- Other models are too technical (Venter, 2006).

Comparing the models that have been developed using ad hoc methodologies against the Carrier and Spafford criteria shows that there are four models meeting at least four of the five criteria whose elements could be incorporated into a generic model, the DCSA, ADFM, EMCI and IDIP. Four

other models meet three out of the five criteria and the remaining models meet only two or less. The result of the assessment of previous models is summarised in **Table 1**.

Table 1 Summary of model scores

	Scores	
Model/Approach	**Carrier and Spafford**	**Daubert**
Ad Hoc		
The Abstract Digital Forensic Model (Reith, et al., 2002)	4	1
The Integrated Digital Investigative Process (Carrier & Spafford, 2003)	4	1
The Enhanced Digital Investigation Process Model (Baryamureeba & Tushabe, 2004)	2	1
The Digital Crime Scene Analysis Model (Rogers, 2004)	5	1
A Hierarchical, Objectives-Based Framework for the Digital Investigations Process (Beebe & Clark, 2004)	2	1
Framework for a Digital Investigation (Kohn, et al., 2006)	3	1
The Two-Dimensional Evidence Reliability Amplification Process Model (Khatir, et al., 2008)	2	1
The Digital Forensic Investigations Framework (Selamat, et al., 2008)	n/a	n/a
The Four Step Forensic Process (Kent, et al., 2006)	n/a	n/a
The Common Process Model (Freiling & Schwittay, 2007)	2	0
The Systematic Digital Forensic Investigation Model (SRDFIM) (Agarwal, et al., 2011b)	3	1
Process flows		
An Extended Model of Cybercrime Investigations (Ciardhuáin, 2004)	4	2
FORZA - Digital forensics investigation framework (Ieong, 2006)	1	1
Process Flows for Cyber Forensics Training and Operations (Venter, 2006)	3	1
Scientific Approaches		
Stephenson (2003b)	3	1
Hannan, Frings, Broucek, & Turner (2003)	0	1
Bogen and Dampier (2005)	n/a	n/a
Wang & Yu (2007)	n/a	n/a

In relation to the Daubert test only one model (the EMCI) met two out of the four tests with the majority of the remaining models only meeting one of the requirements (and one model meeting none of the requirements). The authors of many of the models can claim that they have been peer reviewed whilst only a small number have undergone any form of testing and none of them include

standards against which an error rate can be calculated or have been ‘generally accepted’. This situation suggests that the Daubert test may be ineffective as a standard for determining the reliability of the process employed for acquiring digital evidence.

In relation to guidelines available for digital forensic practitioners, these are focused on law enforcement, electronic discovery or incident response and do not cover all the specific requirements of practitioners working in other areas. The International Standards Organisation (ISO) is currently working on a guideline for digital evidence collection with contributions from the Australian Committee IT-012-04 (of which the author of this thesis is a member). This ISO document 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, while the document itself contains ‘baseline steps’ for certain low-level activities involving the collection and acquisition of digital data, there is no overall process model nor is there a formal representation.

3.5 Summarising the requirements for a new model

3.5.1 Identifying the essential components of the new model

Reviewing the results of the Carrier and Spafford criteria applied to each of the models has identified those which incorporate many of the attributes Carrier and Spafford suggest are essential for a model of the digital forensic process. These models have been selected to provide some of the elements or structure for the new model (ADAM). In addition, and in accordance with the

comments of Turnball (2008), there is the need to ensure that the ADAM will be able to accommodate new and emerging technology.

The following section presents the specific contributions that have been selected to influence the development of ADAM and each of them will be directly addressed within the model.

3.5.2 Key contributions

The key contributions that relate to the acquisition of digital evidence have been identified for each of the models selected via the Carrier and Spafford criteria and these are summarised below:

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

- Emphasising chain of custody considerations
- Considering all areas of digital forensics rather than bias the model towards a particular group
- Promoting a pragmatic approach concentrating on the important areas on which other aspects of the work depend with an emphasis on data acquisition
- Emphasising that a model should be tool and technology independent.

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

- Identifying the important attributes for a model of the digital forensic process

Ciardhuáin (2004) - An Extended Model of Cybercrime Investigations (EMCI)

- Introducing the concept of 'information flow'
- Identifying 'awareness', 'authorisation' and 'planning' stages
- Identifying that there may be both internal and external authorities involved.

Reith, Carr and Gunsch (2002) - The Abstract Digital Forensic Model (ADFM)

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

Khatir, Hejazi and Sneiders (2008) - The Two-Dimensional Evidence Reliability Amplification Process Model

- The concept of an 'umbrella activity' for documentation.

3.5.3 Essential elements identified for the ADAM

By combining the key contributions and considering the reviewed models collectively the essential elements for data acquisition are now summarised and grouped into three stages:

- 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[24]' (the detail of training, lab preparation and other activities prior to the notification/awareness point is not the subject of this model)

- 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
- The actual process of acquiring digital data that may be of evidentiary value and its subsequent handling
- The ADAM will be described through a formal definition using the UML as first proposed by Bogan and Dampier (2005) and supported by Kohn et al (2008) and Ruan and Huebner (2009).

3.6 Summary

This chapter has described how the process for identifying the requirements for the new model was undertaken. This involved evaluating each of the models from the literature review against assessment criteria based on the work of Carrier and Spafford and the Daubert test. The evaluation process is the most comprehensive evaluation so far undertaken of digital forensic process models and is also the first to assess each model against specific criteria.

[24] The environment in which the evidence is thought to reside

Chapter 4: Design and development

4.1 Introduction

This chapter covers the Design and Development stage of the Peffers et al DSRP method that has been adopted for this research. The chapter continues from the review of models in Chapter 2 and their assessment in Chapter 3 that were undertaken to obtain information that would help to address the three research questions:

- "*What are the essential components necessary in a model that describes a generic and forensically sound digital data acquisition process?"*
- "*What is a suitable way for describing, presenting and using model for acquiring digital data?"*
- "*How can the identified components for a generic and forensically sound digital data acquisition process be combined into an effective working model?"*

4.2 Model design elements

4.2.1 Overview of the model

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. In addition, the principles 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). From the literature review of Chapter 2 several shortcomings of previous models were identified:

1. Some models tried to encompass all aspects of digital forensic activity in one model which became too unwieldy and complicated
2. Some models 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 models 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.

These shortcomings will be addressed in the ADAM as well as the failing of previous models to accommodate new and emerging technology. (Turnbull, 2008)

4.2.2 Fundamentals of the Advanced Data Acquisition Model (ADAM)

In accordance with the concepts of the three-stage hierarchical model of Noblett et al (2000) introduced in section 2.3, while making allowance for the

fact that the ADAM is to be a generic model and therefore cannot be prescriptive in relation to organisational guidelines, ADAM needs to:

1. Incorporate overriding principles based on the guidelines from Association of Chief Police Officers, the International Standards Organisation and elsewhere
2. Accommodate organizational policy and practice such as guidelines, signing authorities and other requirements
3. Accommodate procedures and techniques that can be modified and expanded upon as new data becomes available
4. Incorporate the key contributions from previous researchers.

4.2.2.1 ADAM Principles

In relation to the requirement for overriding principles listed as (1) above, these are defined for the ADAM as being

1. The activities of the digital forensic practitioner should not alter the original data. If the requirements of the work mean that this is not possible then the effect of the practitioner's actions on the original data should be clearly identified and the process that caused any changes justified
2. A complete record of all activities associated with the acquisition and handling of the original data and any copies of the original data must be maintained. This includes compliance with the appropriate rules of evidence, such as maintaining a chain of custody record, and verification processes such as hashing

3. The digital forensic practitioner must not undertake any activities which are beyond their ability or knowledge
4. The digital forensic practitioner must take into consideration all aspects of personal safety whilst undertaking their work.

4.2.2.2 ADAM Stages

The ADAM itself consists of three stages associated specifically with the acquisition of digital data. These stages were identified following the literature review and are described as:

STAGE 1 - The initial planning stage

This is where high-level considerations that relate to the documentation associated with the investigation, the investigation logistics etc. are determined. 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, so this stage may be very brief and simply consist of checking paperwork.

STAGE 2 - The onsite survey

All the gaps in knowledge relating to the location, size and format of the devices holding the digital 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.

STAGE 3 - The acquisition of digital 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 digital 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). A practitioner following the ADAM is required to ensure that appropriate documentation be maintained at all times.

The end result of using the ADAM will be that a clear process description is available that can be explained in court together with associated documentation that will support the description of the activities undertaken by a digital forensic practitioner who has acquired digital data. As the ADAM allows for the use of existing forms and processes (where relevant) these can be incorporated into the supporting documentation.

4.2.3 Assumptions

The new model incorporates two 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 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 section draws upon the contributions of previous researchers to develop the elements that go to make up each stage.

4.3 Stage 1: Initial Planning

McKemmish (1999) 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 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. Casey (2004) identifies three topics related to the acquisition of digital 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 says 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 digital 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 that: “It is vital that the number of computers, their types, operating systems and connections are all known before entry” (p. 177). 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 them to produce anything beyond a rough outline of a plan.

Brown (2006) argues that 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, p. 187).

Even if information is obtained that relates to the computer systems that are likely to be encountered, allowance always has to be made for errors or inaccuracies in this information. The thesis author has experienced several occasions in which intelligence gathered by a third party (often a private investigator) has proved to be wildly inaccurate in terms of the number and type of computers involved. 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 is designed to provide more guidance than previous models in this regard as it uniquely incorporates consideration of a number of constraints during the planning stage, which are; authorisation constraints, physical constraints, timing constraints and data constraints. The concepts behind each of these constraints is covered in more detail in the following sections and will lead to the concluding activity for this first stage of the new model, the formulation of the Outline Plan.

4.3.1 Authorisation constraints

The primary consideration, before addressing the process detail, must be one of ensuring that the digital forensic practitioner has the authority to undertake the work. This authority can be made up of several discrete elements: 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 (external authorisation).

Marcella and Menedez (2008) provide a list of the basic steps for a 'cyber investigation' that begins with 'Obtain proper authorization' which they cover in some detail on the basis that this is a 'critical' step.

4.3.1.1 Internal authorization

Internal authorisation will take different forms depending on the particular organisation involved. For a small specialist provider of digital forensic services, the process of internal authorisation is relatively straightforward 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. These 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 focussed on legislative rules and guidelines or commercial considerations, such as working on a matter for which an existing client is an opposing party.

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). The case of digital forensic services being provided by a third party has not been covered in literature relating to process models.

4.3.1.2 Authority in law

For commercial practitioners, in cases such as assisting with the serving of Anton Piller[25] orders or matters where government bodies have 'search and seize' powers, the investigator needs to ensure that they have the legal authority to provide the services in the manner in which they have been requested and 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 but generally any court orders permitting access to a third-

[25] Ex-parte court injunction that requires a defendant to allow the plaintiff to (1) enter defendant's premises, (2) search for and take away any material evidence and, (3) force the defendant to answer some questions. Employed usually in cases of possible copyright violation, its primary objective is to prevent destruction or removal of evidence. This order is not a search warrant, but the defendant is in contempt of court if he or she refuses to comply. Named after the 1976 UK case of 'Anton Piller KG v. Manufacturing Processes.' More recently referred to as a 'search order'.

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.

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. Being aware that you are in possession of child pornography, as well as certain other material, is commonly a criminal offence 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 advice from the relevant law enforcement contact.

4.3.1.3 External authority

When engaged to undertake work for an organisation that requires 'their' systems to be accessed 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 holding a 'live' copy of several organisations' data, a cloud service provider or if the computers are used by an accountant or lawyer to store information from many clients.

4.3.2 Physical constraints

Physical access to the systems containing digital 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 tends to be considered is dealing with external 'attacks' on systems involving the Internet which leads to a discussion of the attack's technical characteristics. With regard to physical constraints the new model involves two considerations that need to be addressed prior to undertaking the data acquisition.

4.3.2.1 Access

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, the obvious exceptions being cases where data can be accessed via the internet or internal/external networks (although in the latter 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 keys or cards 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.

4.3.2.2 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. In some cases the physical ‘scene’ may not exist given the advent of wireless technology and roaming devices.

4.3.3 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). The ADAM requires consideration of three aspects of timing constraints which are now considered individually.

4.3.3.1 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.

4.3.3.2 Private premises

Engagements involving 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.

4.3.3.3 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 have the potential to destroy or remove data. The business disruption aspect is considered by Sammes and Jenkinson (2007) 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. 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.

4.3.4 Data constraints

The data is the digital 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 digital data (such as text files, images, etc.) and to suggest possible locations for this data (Arthur E. Hutt, 1995; Brown, 2006; Casey, 2004; Farmer & Venema, 2005; Jones, et al., 2006; Marcella & Menendez, 2008). The ADAM will not incorporate this level of detail but requires consideration of the potential *quantity* of data that may be acquired. Therefore there are three new constraints covered in the following paragraphs.

4.3.4.1 Identification of data

The type of data to be acquired can vary greatly. For example, it could be 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 must 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' via a write-blocking device. The processes undertaken in relation to this constraint may have a significant impact on the time required to carry out the work.

4.3.4.2 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. Today, disk storage capacity is relatively cheap (for both the owner of the data and the digital forensic practitioner) but there can be problems in relation to physically handling a large number of disks and the form in which they are combined, such as portable storage devices, e.g. Network Attached Storage or Direct Attached Storage technologies. 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.

4.3.4.3 Location of data

If the data to be reviewed and acquired is stored on backup tapes, i.e. 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[26] that is accessed via the internet. This presents many potential difficulties, particularly in relation to authorisation, but from a location perspective it may not be possible to physically access the place in which the data is stored.

4.3.5 The Outline Plan

The output of the Initial Planning stage should be the Outline Plan. Based on the outcome of the previous considerations the logistics of the acquisition exercise can now 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, application software 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

[26] There is an example of applying the ADAM in a cloud environment in Chapter 5 as part of Scenario 4.

that all those involved are aware of the information available at the time including any constraints imposed by court orders or other authorities. Sammes and Jenkinson (2007) state that 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).

The Outline Plan must therefore detail:

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 provide great detail in relation to the equipment that should be taken on site (e.g. Sammes and Jenkinson, 2007) whilst others (e.g. Brown , 2006; Jones et al, 2006) include specific write-blockers of various types at the top of their recommendations for an 'onsite kit' as well as software tools for acquiring digital data. The ACPO Guide (2003) makes no recommendations for the equipment to be taken on site.

There is no consensus or standard set of guidelines for what equipment should be considered for inclusion in the onsite kit and as the composition of the kit contents should be determined by the appropriate digital forensic professional the ADAM is not intended to provide this level of detail.

4.4 Stage 2: The Onsite plan

Having gained access to the site(s) in which relevant digital 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 it is seldom practical in the commercial environment, a view supported by Kruse and Heiser (2002) who state:

> 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 (p. 6).

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 (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 digital 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 general in nature which ensures that they can be applied in different environments.

4.4.1 Updating the Outline Plan

Once the digital forensic practitioner 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 digital 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; M. Pollitt, 2009). A more thorough approach is supported by Newman (2007) 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’:

- Determine all the locations that might need to be searched
- Look for any specifics that must be addressed relating to hardware and software
- Identify possible personnel and equipment needs for the investigation
- Determine which devices can be physically removed from the site
- Identify all individuals who had access to the computer or digital resources.

The ADAM Operation Guide for Stage 2 covers these requirements.

4.5 Stage 3: Acquisition of Digital Data

Some authors imply that the acquisition process is always undertaken in some 'ideal' environment where storage devices can be write-blocked (Jones, Bejtlich, & Rose, 2006). McKemmish adopts a more practical view where he states that in certain circumstances changes to data are unavoidable. 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), important computer data being stored in volatile memory (Sutherland, Evans, Tryfonas, & Blyth, 2008), full disk encryption (Casey & Stellatos, 2008) and time/storage constraints for large drive capacities (Gosh, 2004a) the concept of the 'ideal' environment is becoming even further removed from practice (Adelstein, 2006; Carrier, 2006;

Casey & Stellatos, 2008; 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.

The ADAM is based on the belief that it is the role of the digital forensic practitioner to determine the most appropriate technique to be employed and maintain documentation of all activities associated 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.

4.6 Model creation

So far this chapter has described and justified the elements that make up the Advanced Data Acquisition Model building on the work of previous researchers reviewed in Chapters 2 and 3. The remainder of the chapter shows how these elements have been incorporated in the ADAM, using both a formal representation and an Operational (or field) format.

4.6.1 The ADAM representation

Kohn et al (2008) suggest that because existing digital forensic process models are presented in an informal way they would benefit from the introduction of a formal modelling approach and so too would the whole area of digital forensic investigation. The formal approach proposed by Kohn et al

employs the Unified Modelling Language (UML)[27]. The use of the UML is supported by Bogan and Dampier (2005) as well as Ruan and Huebner (2009) who conclude that the UML is appropriate to describe the high-level processes involved in digital forensics on the basis that the UML is a de facto standard modelling language. As discussed in the literature review (section 3.4.1.17) the use of the UML for modelling digital forensic processes has so far been restricted to high-level activities without providing much detail.

This research will develop the use of UML in digital forensics by employing UML Activity Diagrams within the ADAM to define process flows. The UML Use Case diagrams will not be adopted based on earlier examples of their use (Kohn, et al., 2008; Ruan & Huebner, 2009) as they seem to add little value to the description of the process model and would have to be tailored for each environment (as the 'players' would not be the same across all environments) thereby making the overall model less generic.

Notwithstanding the benefit of adopting a formal approach from a technical perspective, the use of UML Activity Diagrams, being a form of flowchart, is supported in a court environment (Dattu, 1998; Kelly, 2010) and in some instances flowcharts have been prepared by judges in Australian and New Zealand to assist jurors (Ogloff, Clough, & Goodman-Delahunty, 2006). As Ruan and Huebner (2009) point out, "A graph based model has the advantage of visualizing the process requirements, thus making the model more understandable to various parties involved" (p. 185).

[27] Defined and maintained by the Object Management Group. Further information available at http://www.uml.org/

In addition to the formal notation, an ‘Operational’ format is also required that provides the necessary level of detail for applying the model in practice. This is covered in section 4.6.1.2.

4.6.1.1 The ADAM Formal representation

The UML Activity diagrams produced for each of the three stages are shown in Figures 18, 19 and 20. These diagrams represent the first instance of the formal representation of the ADAM prior to the Initial Assessment (described in Section 4.6.2) which will be followed by the in-house demonstration activity as described in Chapter 5.

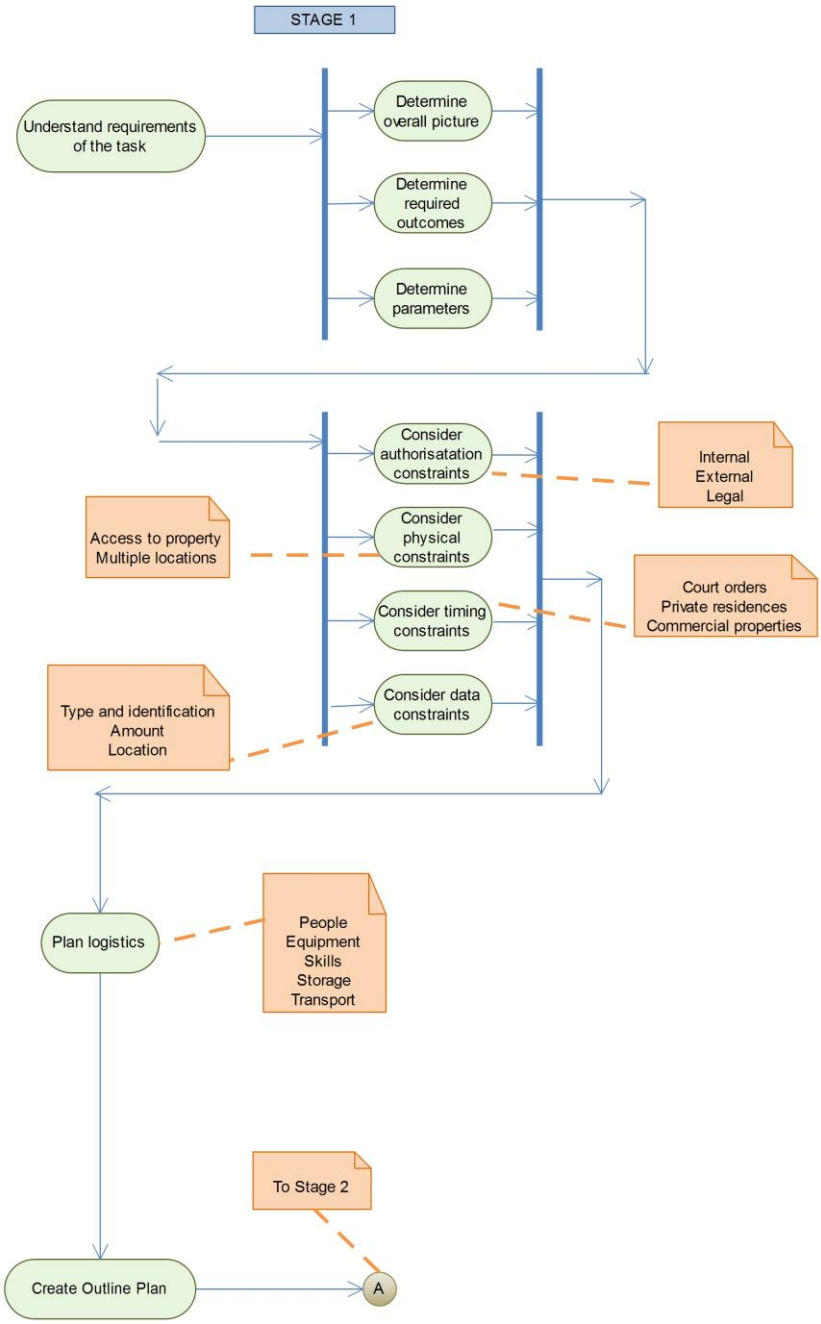

Figure 18 The ADAM Stage 1 – Initial Planning (version 1)

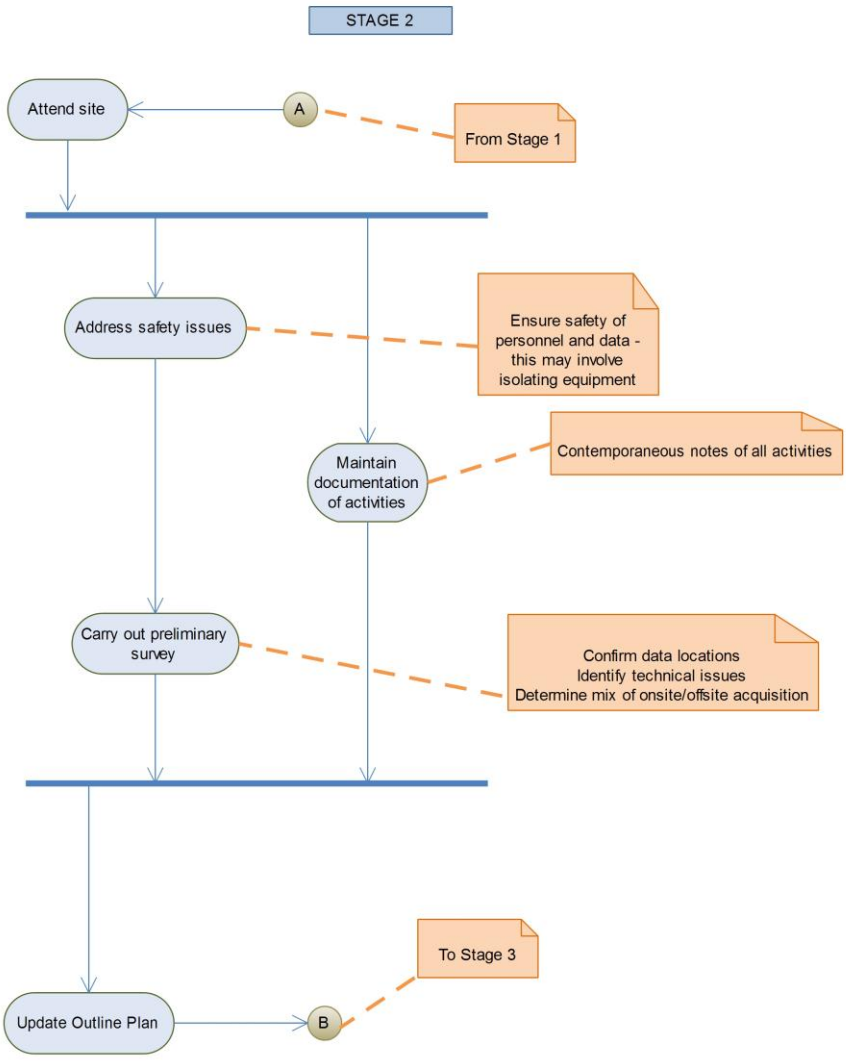

Figure 19 The ADAM Stage 2 – The Onsite Plan (version 1)

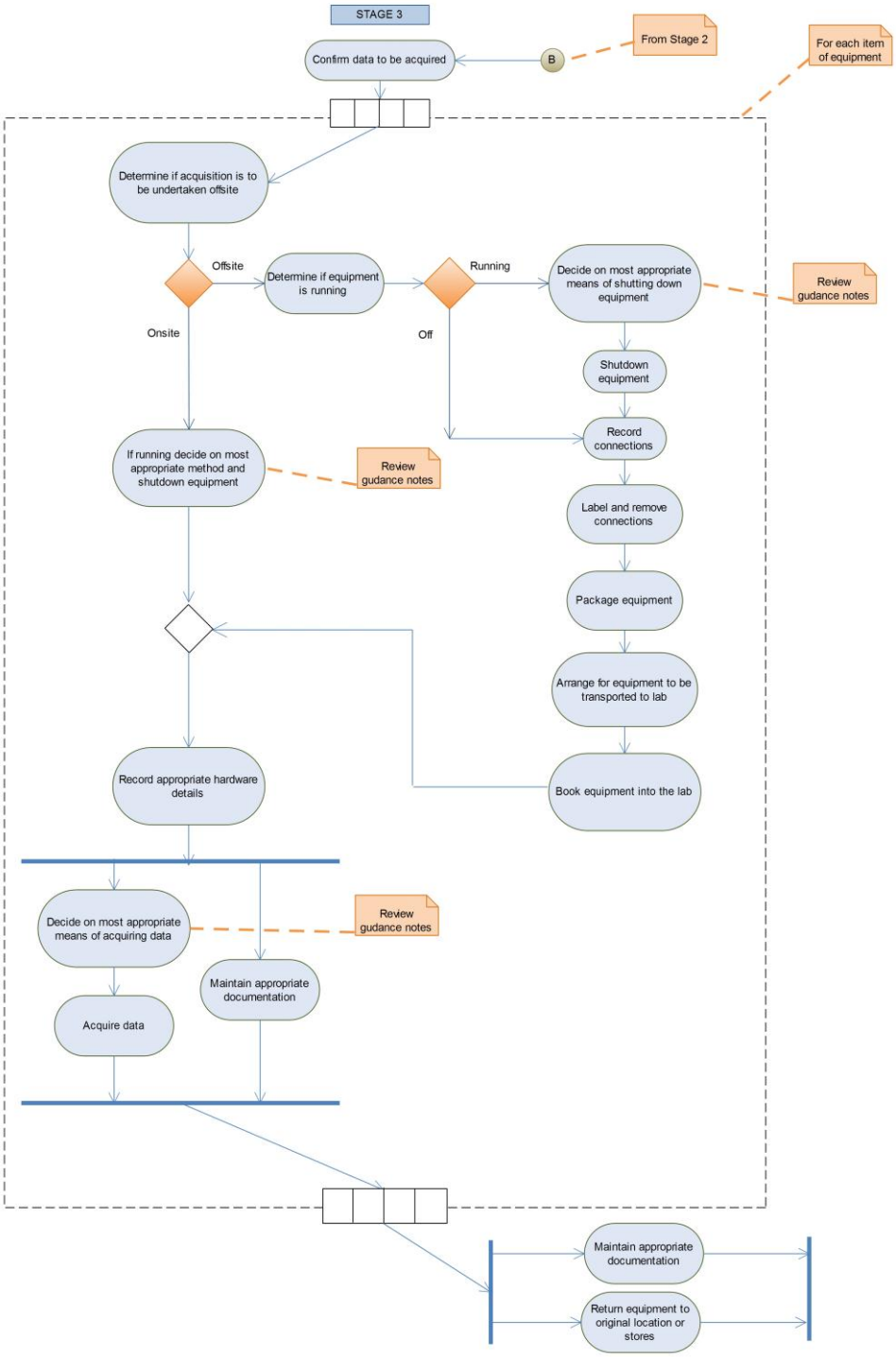

Figure 20 The ADAM Stage 3 – Acquisition of Digital Data (version 1)

4.6.1.2 The ADAM operational representation

To complement the formal notation of the ADAM (described using UML Activity diagrams) a series of guides (one for each stage of the ADAM) as well as a statement of the ADAM Principles (that apply across all activities relating to the use of the ADAM) complete the model. In the later part of this chapter the key words "REQUIRED", "MUST", "MUST NOT", "SHOULD", "SHOULD NOT", and "MAY" are used in the Operational Guides and defined as described in the document "Key words for use in RFCs to Indicate Requirement Levels" [RFC2119] (Brezinski & Killalea, 2002).

This section presents the ADAM in the form in which it will be used and referenced by digital forensic practitioners. Firstly the overarching Principles underlying the model (introduced in section 4.2.2.1) are stated and this is followed by the process model narrative in the form of specific tasks to be undertaken by the forensic practitioner for each of the model's three stages. The version of the Operational representation (the text of the ADAM Principles and Guides for each of the three Stages) shown in this section is prior to it being passed to external reviewers for feedback discussed in Chapter 6.

ADAM PRINCIPLES

The following overriding principles must be followed by the digital forensic practitioner:

1. The activities of the digital forensic practitioner should not alter the original data. If the requirements of the work mean that this is not possible then the effect of the practitioner's actions on the original data should be clearly identified and the process that caused any changes justified
2. A complete record of all activities associated with the acquisition and handling of the original data and any copies of the original data must be maintained. This includes compliance with the appropriate rules of evidence, such as maintaining a chain of custody record, and verification processes such as hashing
3. The digital forensic practitioner must not undertake any activities which are beyond their ability or knowledge
4. The digital forensic practitioner must take into consideration all aspects of personal and equipment safety whilst undertaking their work
5. At all times the legal rights of anyone affected by your actions should be considered
6. The practitioner must be aware of all organisational policies and procedures relating to their activities
7. Communication must be maintained as appropriate with the client, legal practitioners, supervisors and other team members.

ADAM OPERATION GUIDE

Stage 1 – Initial Planning

The digital forensic practitioner:

- MUST understand the requirements of the task, document the work to be performed and have this confirmed by the client or person providing the instructions to undertake the acquisition task

- MUST consider if the work can be undertaken by confirming that you have the appropriate:
    1. internal authorisation and/or
    2. external authorisation and/or
    3. authority in law

- MUST consider
    1. time constraints – is the task achievable within the time allowed?
    2. physical constraints – access to the data and physical/logical locations
    3. data constraints – how will the potential evidence be identified, how much is there likely to be?

- MUST consider safety issues

- SHOULD create the Outline Plan (an exception being in-house acquisition from devices already obtained, e.g. at law enforcement computer crime laboratories).

ADAM OPERATION GUIDE

Stage 2 – Creating the Onsite Plan

The digital forensic practitioner:

- **MUST** identify and address any security or safety issues
- **MUST** secure access to all potential sources of evidence, either directly or remotely
- **MUST** undertake a preliminary survey and document changes to the Outline Plan
- **MUST** consider
    1. all the locations that might need to be searched
    2. any issues that must be addressed relating to hardware and software
    3. personnel and equipment needs for the investigation
    4. whether onsite acquisition, offsite acquisition or a mixture of both is appropriate and possible.

ADAM OPERATION GUIDE

Stage 3 - Acquisition of Digital Data (per device)

The digital forensic practitioner MUST identify the most appropriate way of acquiring potential evidence given the constraints of time, resources, potential evidentiary value and technical limitations.

In order to do this the digital forensic practitioner:

- **MUST** consider
    1. The most appropriate method of shutting down system(s) if applicable
    2. Write-protection method including interface, e.g. via USB/FireWire/eSATA
    3. Addressing encryption issues
    4. The appropriateness of undertaking live acquisition
    5. Acquisition software to be used
    6. Source device interface(s) – e.g. boot device on host, storage device removed and attached to acquisition system, network acquisition, operating system (live acquisition)
    7. Potential volume of data
    8. Target storage capacity
    9. Target interface (speed-related)
    10. Prioritising acquisition if more than one source
- **MUST** maintain comprehensive notes
- **SHOULD** consider photographing and/or sketching the equipment and storage device locations
- **MUST** consider the requirements or benefits of an initial review of potential evidence devices and decide if it is appropriate for this to be carried out 'live' or write-blocked
- **SHOULD** create a 'working copy' of acquired data as quickly as possible and concurrent with the creation of the master copy if possible
- **MUST** keep all copies of acquired data secure
- **MUST** be able to verify the integrity of acquired data.

4.6.2 Initial assessment

As part of the development stage of the Design Science Research Process the head of a Police Computer Crime Unit, the National Director of Digital Forensics from another commercial provider and a forensic practitioner with an 'incident response' background were asked to answer a single question which was:

> *"How accurately do the activities described in the ADAM Activity diagrams relate to your environment"?*

The assessment was carried out through a series of informal discussions with each person with reference to the UML Activity diagrams on which they made various annotations and the author is grateful for their critical feedback.

Several comments and suggestions were made by the initial assessors to help finalise the first iteration of the development stage. These comments are summarised as follows:

1. There is a need to expand on the text relating to the activities in order to provide clarity around the activity
2. The UML Stage 3 diagram does not allow for the device to have already been seized / provided
3. The process flow for 'onsite' and 'onsite or lab' is unclear.

A note was made of these comments for consideration with the results of the Demonstration activity which together would produce the requirements for

the version of the ADAM that would subsequently be provided to the external reviewers as the DSRP Evaluation activity in Chapter 6.

4.7 Summary

This chapter has covered the Design and Development stage for the new model and has provided the rationale behind the requirements for each of the three stages. The ADAM has also been presented in both its ‘formal’ and ‘operational’ forms. An initial assessment has been carried out prior to moving on to the formal Demonstration and Evaluation stages discussed in the following chapter to ensure that there are no major shortcomings from the first iteration of the development stage.

Chapter 5: Demonstration

5.1 Introduction

This chapter discusses the methods used for evaluating the ADAM, firstly by in-house demonstration and subsequently by expert evaluation. The makeup of the review panels and the feedback and comments received are presented, and how the ADAM was amended following a review of the feedback.

The DSRP followed in this research requires that the Demonstration activity involves the artefact to be used in some appropriate environment to solve the stated problem. In order to assess how the ADAM addressed the stated research problem a 'desk check' approach was adopted in which the activities from three previous in-house investigations were mapped to the activities in the ADAM and any discrepancies recorded. In addition, four scenarios were created in order to perform a 'walkthrough' of the ADAM. The approach is identified as being appropriate for evaluating 'simulations and models' (Balci, 2003; Brykczynski, 1999; Hayardeny, Fienblit, & Farchi, 2007).

The Demonstration activity was undertaken in order to identify any obvious errors/omissions prior to submitting the ADAM for independent subjective review by researchers and practitioners working in the field of digital forensics (the Evaluation activity). The Demonstration activity was undertaken in two parts. The first part identified those activities in the ADAM which were not evident in the data acquisition documentation for the selected investigations. Being a convenience sample rather than a statistically representative sample of

previous investigations (and thus not considered as being ideal) there was no expectation that this activity would identify all potential discrepancies. Rather, it would highlight at an early stage aspects of the ADAM that seemed to be unrepresentative of plausibly real activities. As expected, there were discrepancies between activities in the ADAM and those recorded in the acquisition documentation from the selection of historical investigations. The second part of the Demonstration activity was undertaken to identify any activities that were recorded in the acquisition documentation for the selected investigations but were missing from the ADAM. The identified discrepancies from both parts of the Demonstration activity were summarised and their significance considered with a view to determining if changes needed to be made to the ADAM. Once the necessary changes had been made, the involvement of external reviewers was sought.

5.2 Case documentation comparison

The contemporaneous documentation from three existing historical investigations within the thesis author's organisation that took place between 2009 and 2011 were examined and the recorded activities compared against the three stages of the ADAM. The investigations chosen for this demonstration activity were selected such that they involved a range of different circumstances for the data acquisition process as follows:

- Investigation 1

  Assisting with a government agency in obtaining forensic images of data stored on the hard drives of computers

owned by a large corporation as part of an investigation. The investigation took place under the authority of a warrant and approximately twenty computers were identified as being 'of interest'. Over the course of two days the hard drives from these computers were imaged on site by a team of three digital forensic practitioners.

- Investigation 2

  Acquiring forensic images of several laptop hard drives as part of an internal investigation for a large company. The laptops were used by employees of the company who were on suspension on suspicion of being involved in a serious breach of company policy. The laptop computers were handed over to the digital forensic practitioners by an officer of the company to have their hard disks imaged off site. There was a tight deadline for completing the imaging process and subsequent investigation due to the disciplinary policy of the client.

- Investigation 3

  Assisting a client with the execution of an Anton Pillar[28] order whereby forensic images of several computers' hard drives were obtained. An individual digital forensic

[28] Discussed in 4.3.1.2

practitioner accompanied an independent lawyer appointed by the court to a residential address in order to identify and take a copy of computer data that could potentially contain evidence relating to a commercial litigation matter.

These investigations are not intended to be a representative cross-section of work undertaken by digital forensic practitioners because they only relate to the services of a commercial service provider associated with a single organisation (given the sensitivity of this type of information it was not possible to access similar documentation from other organisations). However, this exercise does provide a practical starting point.

5.2.1 Results of the case documentation comparison

The results of the comparison between previous investigations, based on contemporaneous notes, and the ADAM process are summarised in three tables, one for each stage of the ADAM (**Appendix 1**). Any discrepancies between the activities undertaken and the ADAM are highlighted.

Two aspects of the comparison between ADAM and the documentation were considered; firstly where activities that have been included in the ADAM are not reflected within the contemporaneous documentation for each of the investigations being reviewed and secondly where activities had taken place in the sample investigations that are not catered for in the ADAM.

5.2.1.1 Aspect 1 - ADAM activities not recorded in the example case documentation

The comparison between the ADAM activities and those recorded in the case documentation for the three example investigations revealed that there were several instances in which the case documentation did not record a particular activity that was present in the ADAM. This may have been due to the activities not being recorded, not being seen as an activity in their own right or not having been undertaken at all. None of the activity narrative missing from the case documentation (with reference to the ADAM) are considered to be trivial based on relevant guidelines (Association of Chief Police Officers, 2003; ISO/IEC, 2011; Kent, et al., 2006). Had the ADAM been used as a guideline the activities would have been undertaken and documented whereas the situation is currently unverified. In this instance reference to the ADAM has highlighted shortcomings in the organisation's case documentation leading to a review of internal procedures.

The following summarises the comparison between ADAM's overriding principles and the case documentation from previous investigations with comments from the author:

1. The activities of the digital forensic practitioner should not alter the original data. If the requirements of the work mean that this is not possible then the effect of the practitioner's actions on the original data should be clearly identified and the process that caused any changes justified.

Comment: In the documentation associated with all three of the investigations the use and type of a write-blocking tool was recorded and there were no instances in which any action was identified that would have caused the original data to have been altered.

2. A complete record of all activities associated with the acquisition and handling of the original data and any copies of the original data must be maintained. This includes compliance with the appropriate rules of evidence, such as maintaining a chain of custody record, and verification processes such as hashing.

Comment: In all cases:

- The details of the source devices and forensic copies were recorded
- MD5 hash values were recorded and verified
- A complete chain of custody was maintained.

3. The digital forensic practitioner must not undertake any activities which are beyond their ability or knowledge.

Comment: In none of the investigations was there any indication that the practitioners had undertaken activities beyond their ability or knowledge but this is not explicit in the documentation. Whilst it is unlikely that this type of information would be recorded by a practitioner had they acted in an unprofessional way, the expectation is that practitioners will always act in a professional manner and should they be put in a position where

circumstances dictate that they have to acquire additional knowledge from, for instance, a third-party specialist, then this will be documented.

4. The digital forensic practitioner must take into consideration all aspects of personal safety whilst undertaking their work.

Comment: In none of the investigations was there any record of this consideration having been made.

Of the four principles contained within the ADAM both the confirmation that the practitioner was competent to undertake the tasks (Principle 3) and consideration of the safety issues (Principle 4) were lacking in all cases. Concerning the shortcomings with respect to Principle 3, a practitioner could make a 'statement of competence' to confirm that their skills and knowledge are not exceeded. Such a statement would take just a moment to record and should not be an onerous task to implement in standard procedures, regardless of whether the practitioner is operating within the field of law enforcement, commercial practice or incident response. Concerning the shortcomings with respect to Principle 4 with regard to the safety issues, the fact that the Demonstration activity took place within a commercial environment and not law enforcement may explain why safety was not considered automatically and recorded. Again it would be a simple matter for commercial and incident response practitioners to include a comment that safety issues had been considered and record the outcome and, if relevant, how issues had been addressed.

It can be concluded from the above that the discrepancies between the activities contained in the three stages of the ADAM and the activities recorded in the case documentation are due to failings in the case documentation and do not require modifications to the ADAM at this point.

5.2.1.2 Aspect 2 - Activities recorded in the example case documentation but not catered for in the ADAM.

The results of this aspect of the Demonstration activity highlighted shortcomings in the process flow and activities associated with the ADAM's Stage 3 which covers the acquisition process itself. The shortcomings were:

1. The ADAM Stage 3 activity diagram does not account for situations in which some activities may be undertaken on site that would normally be carried out in the forensic lab if the target equipment was removed to there, such as duplicating the acquired image files to create a working copy
2. The ADAM Stage 3 activity diagram does not have an activity for returning any equipment that had been seized
3. The ADAM Stage 3 activity diagram does not show the need to document the process explicitly for each activity.

All three shortcomings were considered and the UML activity diagram for the ADAM Stage 3 was amended to produce the version shown in Figure 21.

Figure 21 The ADAM Stage 3 – Acquisition of Digital Data (version 2)

5.3 Scenario ‘walkthroughs’

For this part of the Demonstration activity, four scenarios have been created and considered from the perspective of deployment of the ADAM. Each of the scenarios demonstrates how the ADAM could be related to specific aspects of an investigation being undertaken in differing circumstances covered by the environment scope of this research. For Scenario 1 the Digital Forensic Investigator (DFP) is working for a professional service provider; Scenario 2 describes a law enforcement computer crime unit where the DFP is not involved in the seizure of the hardware; Scenario 3 describes an incident response situation in which the DFP is working ‘in-house’ and Scenario 4 describes an investigation in which the DFP is working for a government regulator with ‘search and seize’ powers.

All the scenarios are based on actual situations in which the thesis author has either been directly involved or has observed first-hand. They are intended to demonstrate the potential deployment of the ADAM but are not offered as evidence that the ADAM can be successfully deployed into the environments being described.

SCENARIO 1

A client, Company X, contacts their legal advisor, Lawyer Y, to say that they may have an issue with an ex-employee who they believe has removed confidential company material such as customer and price lists prior to their departure and has now set up their own company in direct competition. The legal advisor contacts the digital forensic investigation team at BIG4.

Throughout the following activities Investigator Z and Investigator A maintain contemporaneous notes of all their activities and complete the appropriate documentation as required by the procedures of BIG4.

ADAM Stage 1 – Initial Planning

- The head of the digital forensic investigation team at BIG4, Investigator Z, sets up a meeting with Lawyer Y and Company X. During this meeting Investigator Z develops an understanding of the work required, which is to analyse a desktop computer running the Microsoft Windows Vista operating system that was last used by the ex-employee as well as Company X network data associated with that ex-employee. The outcome of the work is to determine if there is any evidence indicating that the ex-employee accessed and copied company confidential information prior to departure. The legal implications of the work are discussed with Lawyer Y.
- Back at BIG4, Investigator Z follows the in-house procedure for obtaining internal authorisation to do the work, which includes making sure that there are no conflicts issues[29], undertaking a risk assessment and confirming the availability of resources. Investigator Z also confirms that there are no other legal or external authorisations to consider.

[29] Such as the potential client also being an existing audit client of the firm with restrictions on what further work can be undertaken by the firm.

- Investigator Z creates an Outline Plan having considered the time, physical and data constraints as well as any safety issues (such as having to work out of normal office hours at a remote location).
- BIG4 issues a letter of engagement to Company X setting out the terms and conditions under which they will undertake the work as well as defining the scope of the work required.
- Investigator Z confirms that all aspects of the ADAM Stage 1 have been followed by reference to the ADAM Operation Guide for ADAM Stage 1 or BIG4 procedures if these incorporate ADAM Stage 1 activities.
- As a record that all Stage 1 ADAM activities have been completed Investigator Z dates and signs a hard copy of the Stage 1 Activity Diagram as a file note.

ADAM Stage 2 – The Onsite Plan

- Investigator Z and Investigator A attend the offices of Company X with the equipment selected as part of the Preliminary Plan and individual notebooks. They address any safety and/or security issues that may become apparent before starting work.
- Through discussions with the IT Manager from Company X, Investigator Z determines where all sources of potential evidence are located and isolates them with the co-operation of the IT Manager.
- Investigator Z tasks Investigator A to undertake a preliminary survey of the sources of potential evidence and the Outline Plan is updated to create the Onsite Plan now that all the required information is

available. The Onsite Plan includes 'live' acquisition of profile data stored on Company X's fileserver for the ex-employee and onsite acquisition of the data on the ex-employee's desktop computer which at this time is running and showing the login prompt.

- Investigator Z tasks Investigator A with acquiring the data from the ex-employee's computer.
- Investigator Z confirms that all aspects of the ADAM Stage 2 have been followed by reference to the Operation Guide and UML Activity diagram for ADAM Stage 2 or BIG4 procedures if these incorporate ADAM Stage 2 activities.
- As a record that all Stage 2 ADAM activities have been completed Investigator Z dates and signs a hard copy of the Stage 2 Activity Diagram as a file note

ADAM Stage 3 – Acquisition of Digital Data

Network acquisition

- Investigator Z refers to the Operation Guide and UML Activity diagram for ADAM Stage 3 (or BIG4 procedures if these incorporate ADAM Stage 3 activities).
- Investigator Z confirms that the acquisition will be taken onsite.
- Investigator Z decides that a 'live' acquisition of the data is the most appropriate method in the circumstances and attaches a blank external disk drive (the 'master' disk for this forensic acquisition) to a computer on Company X's network that has been provided for the

purpose by the IT Manager. The blank hard disk has been checked for integrity and labelled based on the forensic procedures of BIG4.

- Using a forensic imaging utility in accordance with BIG4's procedures for obtaining 'live' network data, Investigator Z collects the profile data for the ex-employee from Company X's fileserver which is automatically placed in a forensic 'container'[30] on the 'master' disk.
- A hash verification value for the container is calculated and recorded on the Evidence Acquisition Form inn accordance with BIG4 procedures.

Desktop PC acquisition

- Investigator A refers to the Operation Guide and UML Activity diagram for ADAM Stage 3 (or BIG4 procedures if these incorporate ADAM Stage 3 activities), photographs the computer used by the ex-employee and records its model, serial number and other details on a BIG4 Evidence Acquisition Form.
- Investigator A confirms that the acquisition will be undertaken onsite.
- Following the BIG4 Company's digital forensic procedures for shutting down a PC running Microsoft Windows Vista Investigator A turns off the ex-employee's computer and follows BIG4 Company's digital forensic procedures for obtaining a forensic image of the hard disk contained within (making notes of the serial/model details).

[30] Such as AccessData's AD1 format

- Investigator A creates the image on a blank hard disk (the ‘master’ disk for this forensic acquisition) that has been checked for integrity and labelled based on the forensic procedures of BIG4.
- A hash verification value for the acquired data is calculated and recorded on the Evidence Acquisition Form produced by BIG4 in accordance with BIG4 procedures.
- Investigator A re-assembles the computer and returns it to the IT Manager who re-connects it to the Company X network and checks that it is operational.

Transport

- Investigator confirms that all documentation is correct and completes a Chain of Custody form for the two drives containing the acquired data.
- The two drives containing the acquired data are booked into the secure storage facilities at BIG4.
- Investigator Z tasks Investigator B with collecting the two drives from storage and creating ‘working’ copies for analysis based on the operating procedures of BIG4.
- As a record that all Stage 3 ADAM activities have been completed Investigator Z dates and signs a hard copy of the Stage 3 Activity Diagram as a file note.

SCENARIO 2

A police officer seizes a computer system during the execution of a search warrant at private premises. The seized computer placed in an evidence bag and is removed to the police secure storage facility and booked in. The State Computer Crime Unit (CCU) is requested to analyse to contents of the hard disk drive contained in the computer for evidence of a criminal offence. The Unit has its own Standard Operating Procedures (SOPs).

Throughout the following activities contemporaneous notes are maintained and the appropriate documentation is completed as required by internal procedures.

ADAM Stage 1 – Initial Planning

- Officer 1 checks that the documentation supporting the request to analyse the computer is in order as well as chain of custody records.
- Officer 1 considers the nature of the material that may be on the computer's hard disk and makes a risk assessment.
- Officer 1 allocates the work to Officer 2.
- Officer1 confirms that all aspects of the ADAM Stage 1 have been followed by reference to the ADAM Operation Guide for ADAM Stage 1 and CCU SOPs (or just CCU SOPs if these incorporate ADAM Stage 1 activities).
- As a record that all Stage 1 ADAM activities have been completed Officer 1 dates and signs a hard copy of the Stage 1 Activity Diagram as a file note.

ADAM Stage 2 – The Onsite Plan

- Officer 1 simply checks that the activities of ADAM Stage 2 have been documented by the officers seizing the computer.
- As a record that all Stage 2 ADAM activities have been completed Officer 1 dates and signs a hard copy of the Stage 2 Activity Diagram as a file note.

ADAM Stage 3 - Acquisition of Digital Data

- Officer 2 takes custody of the computer from the secure storage facility.
- Officer 2 refers to the ADAM Operation Guide for ADAM Stage 3 and CCU SOPs (or just CCU SOPs if these incorporate the ADAM Stage 3 activities).
- Based on the CCU Standard Operating Procedures (SOPs) Officer 2 determines the most appropriate method for acquiring the data.
- Officer 2 completes the initial sections of the CCU Digital Evidence Acquisition form recording the model/serial numbers of the PC and hard disk drive.
- The acquired master copy of the data is created on the CCU storage system.
- A hash verification value for the acquired data is created and recorded on the CCU Digital Evidence Acquisition form.
- A 'working' copy of the acquired data is created.
- Officer 2 reassembles the computer and returns it to the secure storage facility.

- Officer2 confirms that all aspects of the ADAM Stage 3 have been followed by reference to the ADAM Operation Guide for ADAM Stage 3 and CCU SOPs (or just CCU SOPs if these incorporate the ADAM Stage 3 activities).
- As a record that all Stage 3 ADAM activities have been completed, Officer 2 dates and signs a hard copy of the Stage 3 Activity Diagram as a file note.

At Trial

- The case goes to trial and questions are raised regarding the reliability of the evidence being presented, since the accused denies that certain material ever existed on their computer system.
- The officer that seized the computer is called to give evidence and refers to their contemporaneous notes to the point that the seized computer is placed into secure storage.
- Officer 2 is called to give evidence.
- Officer 2 produces the dated and signed ADAM Stage 3 Activity Diagram, the ADAM Stage 3 Operational Guide, the CCU Digital Evidence Acquisition form and his contemporaneous notes.
- Officer 2 uses the ADAM Stage 3 Activity Diagram to take the court through the process he followed to acquire a forensic image of the seized computer. When asked why a particular software application was used to acquire the forensic image Officer 2 refers to his contemporaneous notes, the ADAM Stage 3 Operational Guide and the relevant Standard Operating Procedures.

SCENARIO 3

The managing director of Company W is notified by a director of Company M that they have been sent confidential material that seems to have originated from Company W. The MD of Company W tasks his IT Director to look into the likelihood of someone compromising the security of Company W's network. The IT Director contacts the manager of his Incident Response Team (IRT) to investigate.

Throughout the following activities contemporaneous notes are maintained and the appropriate documentation is completed as required by internal procedures.

ADAM Stage 1 – Initial Planning

- The IRT Manager meets with the IT director to understand the requirements of the task and obtain background information relating to the material involved.
- The IRT Manager considers the nature of the task and the constraints.
- The IRT Manager decides that they will undertake the investigation and creates an Outline Plan.
- As a record that all Stage 1 ADAM activities have been completed the IRT Manager dates and signs a hard copy of the Stage 1 Activity Diagram as a file note.

ADAM Stage 2 – The Onsite Plan

- The IRT Manager connects to the network and carries out a preliminary survey that involves checking firewall and router logs,

anti-virus messages and other network data that is available to him and that could provide details of the suspected security breach.

- Based on the information obtained from the Preliminary Survey the IRT Manager suspects that a laptop belonging to a director of Company W has been compromised and updates the Outline Plan to create the Onsite Plan.
- The IRT Manager tasks IRT Member1 with acquiring a forensic image of the disk on the suspected laptop.
- The IRT Manager refers to the ADAM Stage 2 Operation Guide and relevant Company W procedures to ensure all the necessary activities have been undertaken.
- As a record that all Stage 1 ADAM activities have been completed the IRT Manager dates and signs a hard copy of the Stage 1 Activity Diagram as a file note

ADAM Stage 3 - Acquisition of Digital Data

Network acquisition

- The IRT manager acquires the appropriate log files from the Company W network and stores them in a forensic container on a blank hard disk using appropriate software.
- The IRT manager creates a hash of the contents of the forensic container and also creates a working copy for later analysis. The appropriate Evidence Acquisition form is completed during this work.

Laptop acquisition

- IRT Member1 arranges to collect the laptop suspected of having been compromised. IRT Member1 refers to the Operation Guide and UML Activity diagram for ADAM Stage 3 (or Company W procedures if these incorporate ADAM Stage 3 activities) and photographs the laptop computer and records its model, serial number and other details on a Company W Evidence Acquisition Form.
- IRT Member1 confirms that the acquisition will be undertaken onsite.
- IRT Member1 follows Company W's digital forensic procedures for shutting down a laptop computer and follows Company W's digital forensic procedures for obtaining a forensic image of the hard disk contained within (making notes of the serial/model details).
- IRT Member1 creates the image on a blank hard disk (the 'master' disk for this forensic acquisition) that has been checked for integrity and labelled based on the forensic procedures of Company W.
- A hash verification value for the acquired data is calculated and recorded on the Evidence Acquisition Form produced by Company W in accordance with Company W procedures.
- IRT Member1 re-assembles the laptop computer and checks that it is operational before returning it to the user.
- IRT Member 1 creates a working copy of the acquired laptop data to be used for later analysis in a forensic sandbox to determine the nature and processes associated with any malware that may be present.

- As a record that all Stage 3 ADAM activities have been completed the IRT Manager records the date and signs a hard copy of the Stage 3 Activity Diagram as a file note.

SCENARIO 4

A government regulator (BigReG) with powers to carry out investigations, including the use of computer forensics, is notified of a possible breach of the Business Trading Act by Company A. Following enquiries Senior Investigator B decides to undertake a seizure of all company documents relating to the activities of Company A including data held on their fileserver.

Throughout the following activities contemporaneous notes are maintained and the appropriate documentation is completed as required by internal procedures.

ADAM Stage 1 – Initial Planning

- Senior Investigator B confirms that all the appropriate authorisations have been obtained and creates an Outline Plan based on the information already obtained through initial enquiries. This plan includes the names of the team members to take part in a raid on the premises of Company A.
- As a record that all Stage 1 ADAM activities have been completed Senior Investigator B dates and signs a hard copy of the Stage 1 Activity Diagram as a file note.

ADAM Stage 2 – The Onsite Plan

- Senior Investigator B and his team arrive unannounced at the premises of Company A. Senior Investigator B shows the court order to a director of Company A and requests that all personnel except the IT Manager leave the premises having turned over their mobile phones and external storage devices to Team Member 2 who will provide a receipt. Senior Investigator B supervises the IT Manager who ensures that all external connections to the network are blocked. Senior Investigator B tasks his team members to undertake a preliminary survey of the locations of potential evidence having considered security and safety issues.
- Team Member 1 reports back that Company A outsources its main IT infrastructure, such as its fileserver, to CloudsRUS, an internet provider of Infrastructure as a Service (IaaS).
- Team Member 2 reports back that all senior executives have company-provided iPhones.
- Team Member 1 obtains the appropriate login credentials for the network
- Team Member 3 reports back that all the laptops for the three senior executives run full disk encryption.
- Senior Investigator B updates the Preliminary Plan to create the Onsite Plan taking into consideration the new circumstances identified by Team Members 1,2 and 3.

- As a record that all Stage 2 ADAM activities have been completed Senior Investigator B dates and signs a hard copy of the Stage 2 Activity Diagram as a file note.

ADAM Stage 3 - Acquisition of Digital Data

Acquiring cloud data

- Senior Investigator B determines that the fileserver on the host machine of CloudsRUS will be imaged remotely using the appropriate tools as set out in the Standard Procedures of BigReG. A record of this decision is made by Senior Investigator B in his notes.
- Senior Investigator B tasks Team Member 1 to undertake the acquisition as she has the necessary skills.
- Team Member 1 uses the appropriate login credentials for the network and follows BigReG Standard Procedures to run a remote process on the Company A fileserver located on the cloud platform. Team Member 1 creates a forensic copy of the fileserver data onto a blank hard disk (the 'master' disk for this forensic acquisition) that has been checked for integrity and labelled based on the forensic procedures of BigReG.
- A hash verification value for the acquired data is calculated and recorded on the Evidence Acquisition Form produced by BigReG in accordance with BigReG procedures.
- All other details of the acquisition process are recorded on the Evidence Acquisition Form.

Mobile phone devices

- Senior Investigator 1 determines that the senior executive iPhones will be seized and transported back to the forensic lab of BigReG for processing by their specialist forensic investigator.
- Senior Investigator 1 tasks Team Member 2 with collecting all the iPhones, securing them in evidence bags and completing the appropriate chain of custody records before transporting them back to the forensic lab for imaging.
- Team Member 2 transports the seized equipment to the forensic lab and hands them over to Mobile Device Investigator A who signs the chain of custody form.
- Mobile Device Investigator A processes each of the iPhones using the appropriate software and techniques as set out in BigReG procedures for acquiring iPhone data and records his activities on an Evidence Acquisition Form for each device. The acquired iPhone data is stored within the relevant directory on the BigReG Forensic Network Attached Storage (NAS) device and hash values are taken and recorded.
- After all the iPhone data has been acquired Team Member 2 takes possession of them, completes the chain of custody record and returns to Company A where the iPhones are returned to the IT Manager who signs for them by completing the chain of custody record.

Encrypted laptop drives

- Senior Investigator B obtains a copy of the encryption recovery software and appropriate recovery data for each laptop.

- Senior Investigator B determines that the task of acquiring the forensic images and then decrypting them onsite is not practical and therefore tasks Team Member 3 with seizing the three laptop computers for processing back at the forensic lab.
- Team Member 3 provides a receipt for the three laptop computers and completes the Chain of Custody record before placing them in separate evidence bags.
- Team Member 3 transports the three laptop computers to the forensic lab where he reviews the BigReG Operating Procedures for dealing with the encryption being used.
- Team Member 3 follows the BigReG Operating Procedures and stores the decrypted drive images on the Forensic NAS in the relevant directory. The process used and the resulting hash values of the decrypted drives are stored on the Evidence Acquisition Form used by BigReG.
- Senior Investigator B remains supervising onsite until the acquisition of the fileserver data is completed and the iPhones have been returned. He then checks the Evidence Acquisition Forms and then dates and signs the ADAM Stage 3 Activity diagram for the fileserver and each of the iPhones as a record that all of the activities have been carried out. Once the laptop drives have been decrypted and the laptops have been returned Investigator B checks the Chain of Custody records and the Evidence Acquisition Forms for the laptop images.

Working copies of all the acquired images and logical containers are created in accordance with the ADAM and as per BigReG Policies and Procedures. Senior Investigator B dates and signs the ADAM Stage 3 Activity Diagram for each of the laptops as a record that all of the activities have been completed.

5.3.1 Results of the scenario walkthroughs

Although there were different types of device and environment encountered by the investigators in the four scenarios they were able to apply a consistent process using the ADAM that could be described in court. The model also provided a useful framework for ensuring that all the activities were carried out and recorded.

5.4 Summary

This chapter has discussed the Demonstration activity stage of the DSRP followed in this thesis. The Demonstration activity involved reviewing the contemporaneous documentation from three previous in-house investigations and comparing the activities described therein against the ADAM, following which some amendments were made to the ADAM. A ‘walkthrough’ using four scenarios was also undertaken that successfully mapped the three stages of the ADAM to representative activities undertaken by a DFP working in different environments covered by the environment scope of this research.

Having completed the Demonstration activity the next step in the DSRP is the evaluation activity which is undertaken by a number of external researchers and practitioners and is described in the following chapter.

Chapter 6: Evaluation

6.1 Introduction

Evaluating a process model can be summarised as normally focusing on three high-level aspects (Barlas, 1996; Groesser & Schwaninger, 2012; Kleijnen, 1995):

1. Is the model theoretical valid? (the model should be logical and consistent with some theory of the topic)
2. Is the model usable? (the model can be applied in a real life environment)
3. Does the model provide explanatory or prescriptive power for the user?

For a process model, the *validity* comes from the degree to which it adheres to guiding principles around which the process is organised. The model is *usable* if people can use it in real scenarios to arrange and sequence their activities to move through the process and generate the required outcomes easily and efficiently. The model has *prescriptive* power if it steers the process, recommends some courses of action and cautions against others. Chapter 4 has described the theoretical basis for the model development and Chapter 5 started the process of determining if the model is useful through in-house assessment and scenario walk-throughs. The prescriptive power of the model comes from the UML Activity diagrams for the three stages of the ADAM and the associated

Operation Guides that are intended to guide the practitioner through the process of acquiring digital evidence. However, the model needs to undergo an independent evaluation of this prescriptive power that also builds on the activities of Chapter 5 to determine if the model is usable. The independent evaluation is the topic for this chapter and continues the Peffers et al (2006) Design Science Research Process that requires the artefact to be used to address one or more instances of the research problem. The chapter begins by discussing the external review process involving two panels of reviewers and then covers the makeup of the review panels followed by details of the feedback and comments received. The chapter concludes with details of how the ADAM was amended following a review of this feedback.

6.2 Use of expert and peer reviewers

Pace and Sheehan (2002) note that a primary validation technique for models and simulations incorporates some form of review by experts and peers. This approach has been supported by other researchers in different environments but the common theme is to draw upon knowledge that cannot be obtained through reference to other data sources and applying this knowledge to the evaluation of an artefact such as a model (Balci, 2003; Hayardeny, et al., 2007; Macal, 2005).

6.3 The Expert Panel

In order to address the first research goal (*the development of a formal model*) a group of internationally renowned practitioners and academics, hereafter referred to as the Expert Panel, were asked if they would provide

feedback on a new formal digital forensic process model for the acquisition of digital data. The Panel recruitment process was deemed to be complete once a diverse group had agreed to take part that would bring different perspectives to bear on the evaluation (Cornelissen, Berg, Koops, & Kaymak, 2002). Considerations for the selection of potential panel members were:

- The person's period of learning and experience in the domain of digital forensics was greater than 10 years; and
- The conditions in which the experience had been gained, e.g. in theoretical or practical circumstances, to ensure a mix of theorists and current practitioners.

The Expert Panel comprises of the following members:

- A Professor of Computer Science
- An Associate Professor of Computer Science and Engineering
- The Director of a commercial computer forensic company and an internationally recognised authority in the field of computer forensics who also holds a Ph.D. in Computer Forensics
- A licensed attorney who advises, researches, publishes, and speaks on prevailing and forthcoming issues at the crossroads of information technology law who holds Juris Doctorate and Master of Forensic Sciences degrees
- The author of a book on collecting and preserving computer evidence with over 20 years' experience of computer security.

The Guidance Notes, ADAM Principles and the UML Activity diagrams were provided to the Expert Panel for them to evaluate the new model of the digital forensic acquisition process and provide comment or feedback on any aspect of the model from the documents that had been supplied. The Expert Panel were not required to structure their feedback in a particular way, thus leaving them free to express their views in whatever manner they felt was most appropriate.

6.4 The Practitioner Panel

The second goal of the research objective is (*the development of a generic model relevant to the fields of commerce, law enforcement and incident response)*. In relation to this objective Ford and Sterman (1998) suggest that an effective way of eliciting information in relation to this type of knowledge-intensive process is to employ expert knowledge from those that are routinely involved in the process. In order to utilise expert knowledge for a practical evaluation of the ADAM, a group of peers (working in different areas of the research environment scope) were recruited to form the Practitioner Panel. These practitioners were asked to assist in this research either directly, via email or via a request from the High Technology Crime Investigators Association (Asia/Pacific region). The practitioners were identified as being representative of their particular areas of activity based on their roles, experience and involvement with relevant national and international associations. The recruitment process for the Practitioner Panel was deemed to be complete once at least one practitioner had agreed to assist from each of the three fields covered by the research scope (i.e. law enforcement, commerce and incident response).

To ensure relevance to the three fields, two attributes, utility and usability, were considered. Utility might also be expressed as 'usefulness', 'functionality' and 'fitness for purpose' (Blandford, Green, Furniss, & Makri, 2008; Gill & Hevner, 2011; ISO, 2001; Vaishnavi & Kuechler, 2009). Assessing this involves the ADAM being evaluated by the Practitioner Panel with respect to how suitable it is for describing the forensic data acquisition process in each of their particular fields (A. Hevner & Chatterjee, 2010; March & Smith, 1995).

The usability[31] testing employs the Practitioner Panel as 'representative users' (Folmer & Bosch, 2004; Heo, Ham, Park, Song, & Yoon, 2009; Karat, 1997) who are asked to review typical tasks associated with acquiring digital data in their own environments through using the ADAM and to then to provide a subjective rating based on how easy it would be to adopt and use the model. This subjective rating will be taken into consideration for improvements to the model. The Practitioner Panel comprised the following members:

- A representative of commercial practice who is the National Director of computer forensics for a professional services company and who has instructed a number of law enforcement agencies including Scotland Yard, Hong Kong Police, ICE Immigration Customs Enforcement, the Australian Federal Police, the FBI's Regional Computer Forensics Labs and the Australia High Tech Crime Centre
- A representative of incident response with 15 years of Information Technology experience who is a certified Computer Information

[31] Defined in the ISO Quality Model 9126-1 (ISO, 2001) as *"A set of attributes that bear on the effort needed for use, and on the individual assessment of such use, by a stated or implied set of users"*

Systems Security Professional (CISSP) and a Certified Information Systems Auditor (CISA) and who was a Technical Trainer at the 2007 Malaysia Forum of Incident Response and Security Teams Technical Colloquia

- A representative of law enforcement who heads a State Police Computer Crime Squad
- A representative of law enforcement who is a Digital Forensics Examiner at a government ministry who is a certified Computer Information Systems Security Professional (CISSP) and a certified Information Systems Auditor (CISA)
- A representative of commercial practice who is a committee member of the High Technology Crime Investigators Association
- Both the descriptive narrative and the UML activity diagrams were provided to the Practitioner Panel. Panel members were asked to provide answers to the following questions (with the evaluation attribute shown in brackets):
- In reviewing this model please identify any aspects that would NOT be representative of the process as carried out in your environment ('utility')
- In reviewing this model please identify any aspects of your data acquisition process that are NOT covered ('utility')
- Please identify any aspects of the model that you feel could be improved ('utility')

- Please rate this model in terms of the usability of the model from 1 to 10 with ‘1’ being very difficult to use and adopt and ‘10’ being very easy to use and adopt (‘usability’).

In relation to Question 4 above, the determination of usability based on a perception scale and does not provide an objective measure but simply an indication of whether there were any inherent problems in using the model in a particular environment.

6.5 Feedback from Panels

6.5.1 Feedback from the Expert Panel

The feedback from the Expert Panel is presented in the form of extracts from correspondence together with specific comments from the researcher in response to detailed feedback. Where the researcher has implemented a modification in response to feedback this is indicated by a reference in the following format: ‘ref MOD #n’ (where n is the number of an implemented modification).

All general comments from the Expert Panel

- *I read through the materials you provided and found helpful value-add in the synthesizing of the state of affairs with respect to the evolution, or lack thereof, of models in this space. Your approach does a nice job of providing a substantive and longitudinal overview of same. Trying to draw common threads throughout the "leading" models is a necessary step to move the ball forward.*

- *I have completed a "Quick Review" of your model and overall I do believe that your work provides some great promise. Noting that finding a level of detail and specificity in a project like this that satisfies all is a daunting task. While I do believe that you are close, I feel that there is room for more in the supporting documentation.*
- *I have looked over your model - I think it generally looks good.*

All detailed feedback from Experts (and thesis author comments)

Feedback E-1: *The one area that I saw that could use some more 'direction' is the topic of Identification which appears in stage 1 and 2. More specifically in 2.3 you identify that a preliminary survey should be conducted to identify data locations. While section 2.3 does cover some detail, I find this to be an area that is rarely accomplished early enough, or thoroughly enough. For instance surveys of this type should be accomplished far before the collection itself if at all possible. Granted, it's not always possible*.

- **Comment**: This issue is important but the detail included in the ADAM is considered sufficient as the feedback is more relevant to the practice of eDiscovery rather than digital forensic investigations in which the subjects of the investigation do not generally disclose the location of potential evidence.

Feedback E-2: *Essentially I feel that the early interview process and review of past audits and policies is of great value here. For instance, an investigator may think they are doing a great job by reviewing a set of IT Management guidelines that state certain types of data will be stored in XXXX, so they include the collection of XXXX in the process. In that same situation the investigator might have found that that data was actually kept somewhere else entirely by 90 % of users if an interview was conducted, or maybe the results of a recent audit. I have found over time that most organizations don't really know where their data is and in some cases what their knowledge workers true workflow process is. It is for this reason that I stress the importance of this step.*

- **Comment**: This is a useful 'operational' point but is considered too specific for inclusion as a step in the generic model process and would be better as part of an organisational procedure document or 'practice guide'.

Feedback E-3: *During stage 3 there needs to be some explicit sense of protecting all equipment and personnel — especially lab equipment.*

- **Comment**: An addition will be made to the ADAM Principles to add 'equipment safety' in addition to personal safety. (REF: MOD #1)

Feedback E-4: *During stage 3 there needs to be some explicit sense of protecting any legal rights, and of keeping objectivity in the exam.*

- **Comment**: A new Principle will be added to consider legal rights. The explicit requirement to maintain objectivity is not considered to be appropriate for the Stage 3 process as this should form part of a practitioners approach. (REF: MOD #2)

Feedback E-5: *In stage 1 there should be some input of study and familiarization with the milieu.*

- **Comment**: This is considered to be too generic to probably warrant a specific task within the preparation of the Outline Plan which already requires consideration of constraints.

Feedback E-6: *In stage 3, there should be some branch if unexpected contraband or material is discovered.*

- **Comment**: This will be explicitly added to the ADAM as a Principle relating to organisational policies and procedures and a branch in Stage 2 where the data may have been reviewed as part of the

'preliminary survey'. An amendment for Stage 3 will cover both this situation and Feedback E-7 (covered in the next paragraph). For law enforcement the presence of illegal material may have been anticipated. (REF: MOD #3)

Feedback E-7: *In stage 3, seized equipment is not always returned, especially if it contains items such as child porn or classified information.*

- **Comment**: The ADAM will be amended to take this into account. (REF: MOD #4)

Feedback E-8: *Stage 2 might be the right place to seek and obtain additional resources and personnel to handle the confiscation and examination of the material (or that may go in multiple places?) Not every organization has everything they need in-house.*

- **Comment**: Stage 2 explicitly requires consideration of personnel needs and it is left to the practitioner to determine how this is to be addressed.

Feedback E-9: *From experience, there is often on-going communications between the examiner and both prosecutors and other investigators. I don't see that represented.*

- **Comment:** This will be added to the ADAM. (REF: MOD #5)

Feedback E-10: *Every case should have a "lessons learned" post-mortem that feeds back into the system.*

- **Comment**: Although this is a good idea in practice it should form part of the organisation's overall procedures and outside the intended scope of the process model, which finishes at the point that the data has been acquired, duplicated and stored.

6.5.2 Feedback from the Practitioner Panel

The feedback from the Practitioner Panel is now presented in the form of quotes from correspondence together with comments from the thesis author in response to the detailed feedback.

All general comments from the Practitioner Panel

- *Other than network forensics, our internal procedure for IR team to perform site raid and investigations is close to your workflow*
- *This model that consists of 3 stages is representative of the process as carried out in our environment*
- *For all the basic and important steps within a 'forensically sound environment', I think your model has these covered.*

All detailed feedback from Practitioners (and thesis author comments)

Feedback P-1: *Stage 1 - Include references to engagement as 'Independent Expert' or as 'Consulting Expert'; this will prepared you for LPP situations as well as how your role might be restricted*

- **Comment**: As it stands this is a valid point but the comment is derived from a commercial perspective where the practitioner is engaged by a third party to undertake work involving digital forensics. In this instance it is common practice, especially within the large professional service companies, to create an engagement letter which clearly states the role in which the practitioner is to be engaged. This reference has therefore not been considered relevant for the ADAM as it forms part of the organisation's administrative procedures for this type of work and does not impact the activities undertaken by the practitioner in acquiring the digital data using a generic process model.

Feedback P-2: *Stage 2 – Include references to company as well as contracting company's OH&S; this often dictates a minimal resource per site / work cover requirements.*

- **Comment**: For large service providers the minimal resources per site may be relevant but for smaller teams (sometimes consisting of only one practitioner) the constraint on the number of practitioners would

not be applicable. With regard to Occupational Health & Safety the organisation's policies should ensure that practitioners are not working alone in circumstances in which they may encounter a hazard, for instance by always having at least one other person with them who may or may not be a digital forensic practitioner. The ADAM Principles will be modified to incorporate relevant policies including the safety requirements (ADAM Principles items 4 and 6).

Feedback P-3: *Stage 3 - Include reference to IT Evidence Management HB 171-2003.*

- **Comment**: The 'IT Evidence Management HB 171-2003' guidelines relate to the organisation that 'owns' the data and are intended to prepare them for litigation/investigations on their systems by adopting proper management of the data, and these guidelines are therefore not considered to be relevant within the ADAM.

Feedback P-4: *Stage 3 - Include time restrictions on acquisitions.*

- **Comment**: This is already considered to be appropriately covered in Stage 1 (the practitioner MUST consider time constraints – is the task achievable within the time allowed?) and Stage 3 (The digital forensic practitioner MUST identify the most appropriate way of acquiring potential evidence given the constraints of time, resources, potential evidentiary value and technical limitations).

Feedback P-5: *Stage 3 - Include authorisation for devices to be taken off-site*

- **Comment**: This will be added to the ADAM. (REF: MOD #6)

Feedback P-6: *Stage 3 - Transportation requirements if devices are to be taken off-site*

- **Comment**: Equipment safety is now added to the ADAM Principles following previous feedback. (REF: MOD #7)

Feedback P-7: *Stage 3 - Check criteria/conditions if LPP claim is made*

- **Comment**: Legal rights consideration is now added to the ADAM Principles following previous feedback. (REF: MOD #8)

Feedback P-8: *Stage 3 - Check OH&S - food/drink requirements*

- **Comment**: As per item 2 of this list of detailed improvements, this is considered to be covered by the requirement in the ADAM Principles to consider all aspects of personal safety (*The digital forensic practitioner must take into consideration all aspects of personal and equipment safety whilst undertaking their work).*

Feedback P-9: *Stage 3 - Include plans for Client/Team updates or project status*

- **Comment**: This is now added to the ADAM as part of a '*maintain appropriate communications with legal team/client/other practitioners'* requirement following previous feedback. (REF: MOD #9)

Feedback P-10: *"Stage 3 - Team/Project debrief on project completion - to check off Task list and lessons learnt"*

- **Comment**: Whilst being a vital aspect of this type of work it is considered to be part of the overall case management process. From the perspective of using the model to describe the process in court this activity would not be relevant.

Feedback P-11: *In relation to 'Cloud storage' - there is insufficient details on how the cloud providers service any search warrant from Court/LE, or any subpoena for litigation data evidence*

- **Comment**: An amendment has been made to the ADAM in the Stage 3 Activity diagram for the digital forensic practitioner (REF: Mod #10). The specific practices and techniques for this particular process are covered by guidelines and other material which is outside the

scope of the ADAM. In terms of obtaining the appropriate authorisation, this is now covered by an earlier change made to the Stage 3 Activity diagram based on MOD #6.

Feedback P-12: *Network forensic process needed to be extended*

- **Comment**: As for previous comment regarding cloud computing, an amendment has been made to the ADAM in the Stage 3 Activity diagram (REF: Mod #10). The specific practices and techniques for this particular process are covered by guidelines and other material which is outside the scope of the ADAM.

6.5.3 Discussion of Evaluation

6.5.3.1 Utility

Design science aims to "…produce and apply knowledge of tasks or situations in order to create effective artefacts" (Simon, 1996, p. 253) including 'utility' (Applegate, 1999; AR Hevner, et al., 2004). The utility requirement of the external review was to ensure that the ADAM captures all of the activities undertaken by practitioners in the three target areas of commerce, incident response and law enforcement. There were no steps within the ADAM that were identified as being unrepresentative of the process carried out in the experts or practitioners' environment or in their experience. There were several instances of feedback with suggestions for some additions or amendments that could be incorporated into the ADAM. Each instance of feedback, consisting of 23 detailed improvements, was considered and ten changes have been made to the

ADAM, some of which incorporate more than one instance of suggested improvement.

The ADAM has now been through a process of review, feedback and modification in order to address the issue of utility.

6.5.3.2 Usability

All the Practitioners provided simple perception scores of between 8 and 10 in response to the request:

> "*Please rate this model in terms of the usability of the model from 1 to 10 with '1' being very difficult to use and adopt and '10' being very easy to use and adopt"*.

The mean score was 9 and the following comments were also provided:

- *It would be very easy to incorporate or formalise for our use if need be*
- *Very straight forward, and there are very few cross-over feedback loops. This is good from a business process management point of view*
- *Reasonably easy to use and adopt*

There were no negative comments.

6.5.4 Changes made to the ADAM in response to external evaluation

6.5.4.1 Changes to the ADAM Principles.

Modifications were made to the ADAM Principles following the feedback as described in section 6.5. These are shown highlighted in the following version of the ADAM Principles.

ADAM PRINCIPLES

The following overriding principles must be followed by the digital forensic practitioner:

1. The activities of the digital forensic practitioner should not alter the original data. If the requirements of the work mean that this is not possible then the effect of the practitioner's actions on the original data should be clearly identified and the process that caused any changes justified
2. A complete record of all activities associated with the acquisition and handling of the original data and any copies of the original data must be maintained. This includes compliance with the appropriate rules of evidence, such as maintaining a chain of custody record, and verification processes such as hashing
3. The digital forensic practitioner must not undertake any activities which are beyond their ability or knowledge
4. The digital forensic practitioner must take into consideration all aspects of personal and equipment safety whilst undertaking their work
5. At all times the legal rights of anyone affected by your actions should be considered
6. The practitioner must be aware of all organisational policies and procedures relating to their activities
7. Communication must be maintained as appropriate with the client, legal practitioners, supervisors and other team members.

6.5.4.2 Changes to the activity diagrams.

The next few pages show the changes made to the UML activity diagrams in response to the evaluation feedback.

Amendments to ADAM Stage 2 Activity diagram for MOD #3 (shaded) - To cater for equipment not being returned

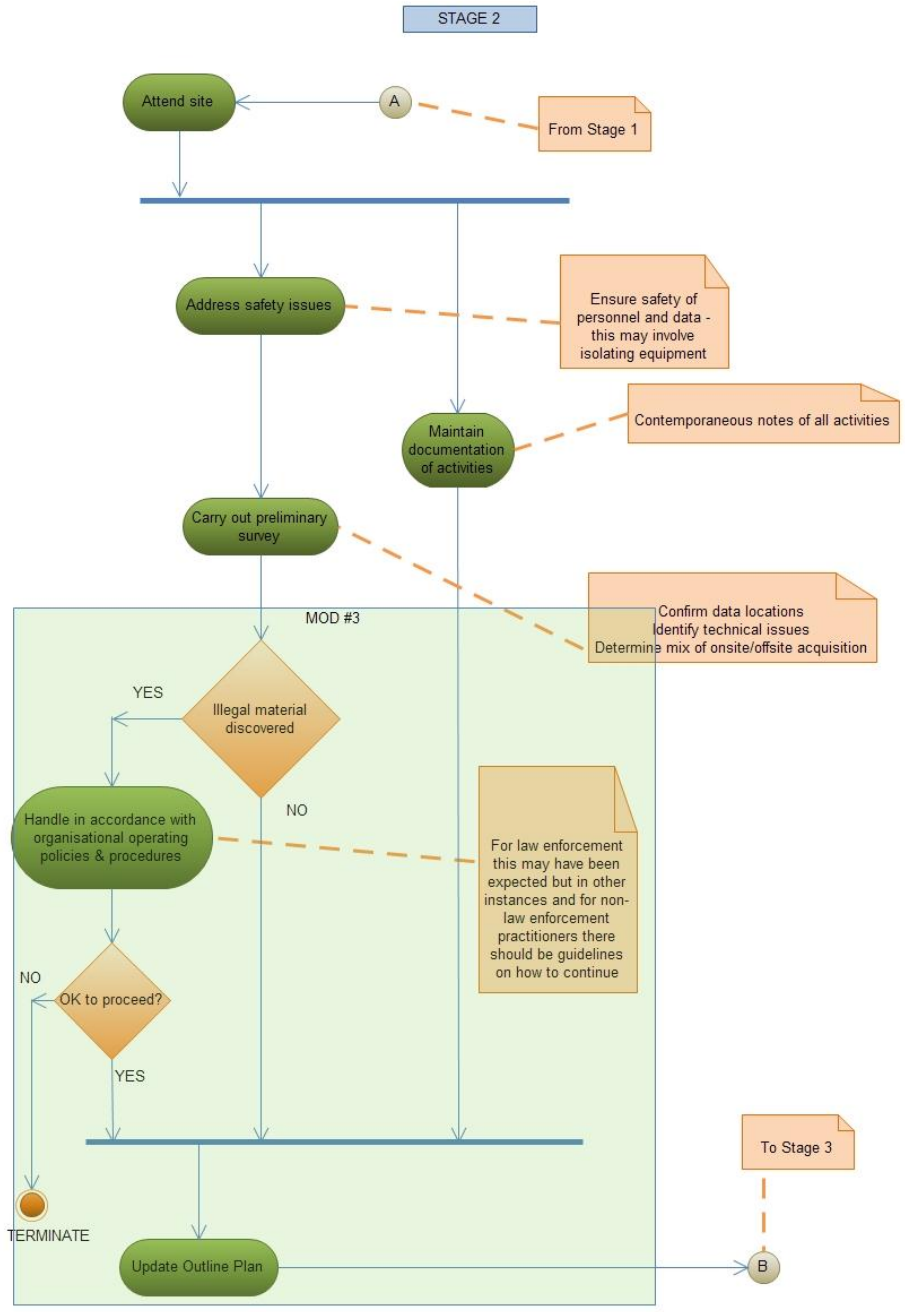

Figure 22 The ADAM Stage 2 amended (within shaded area) for MOD #3

Amendment to ADAM Stage 3 Activity diagram for MODs # 3 & # 4 (shaded) – to cater for equipment not being returned

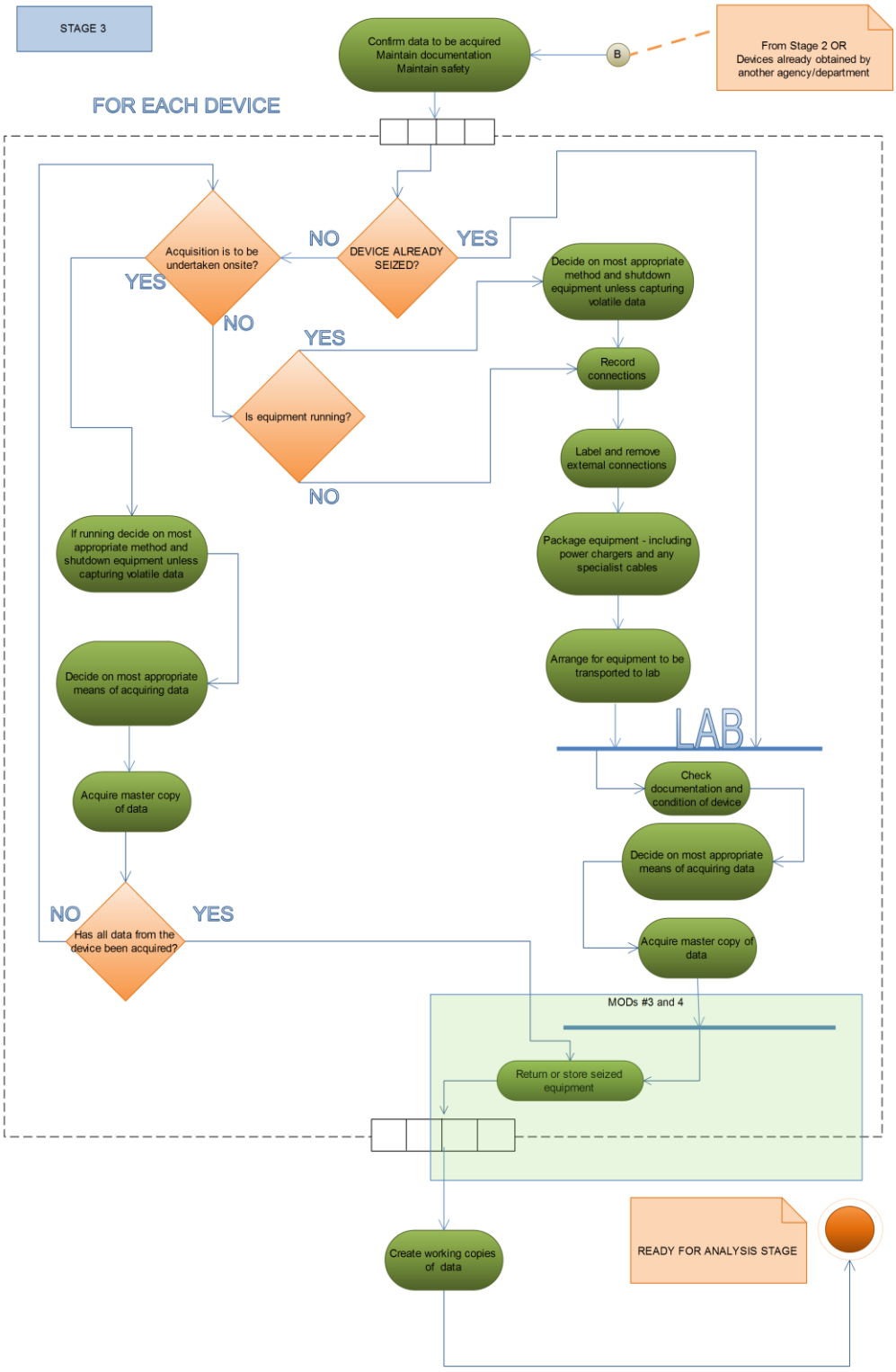

Figure 23 The ADAM Stage 3 amended (within shaded area) for MODs #3 and #4

Amendment to ADAM Stage 3 Activity diagram for MOD #6 (shaded) – to cater for obtaining appropriate authorisations for equipment to be taken offsite

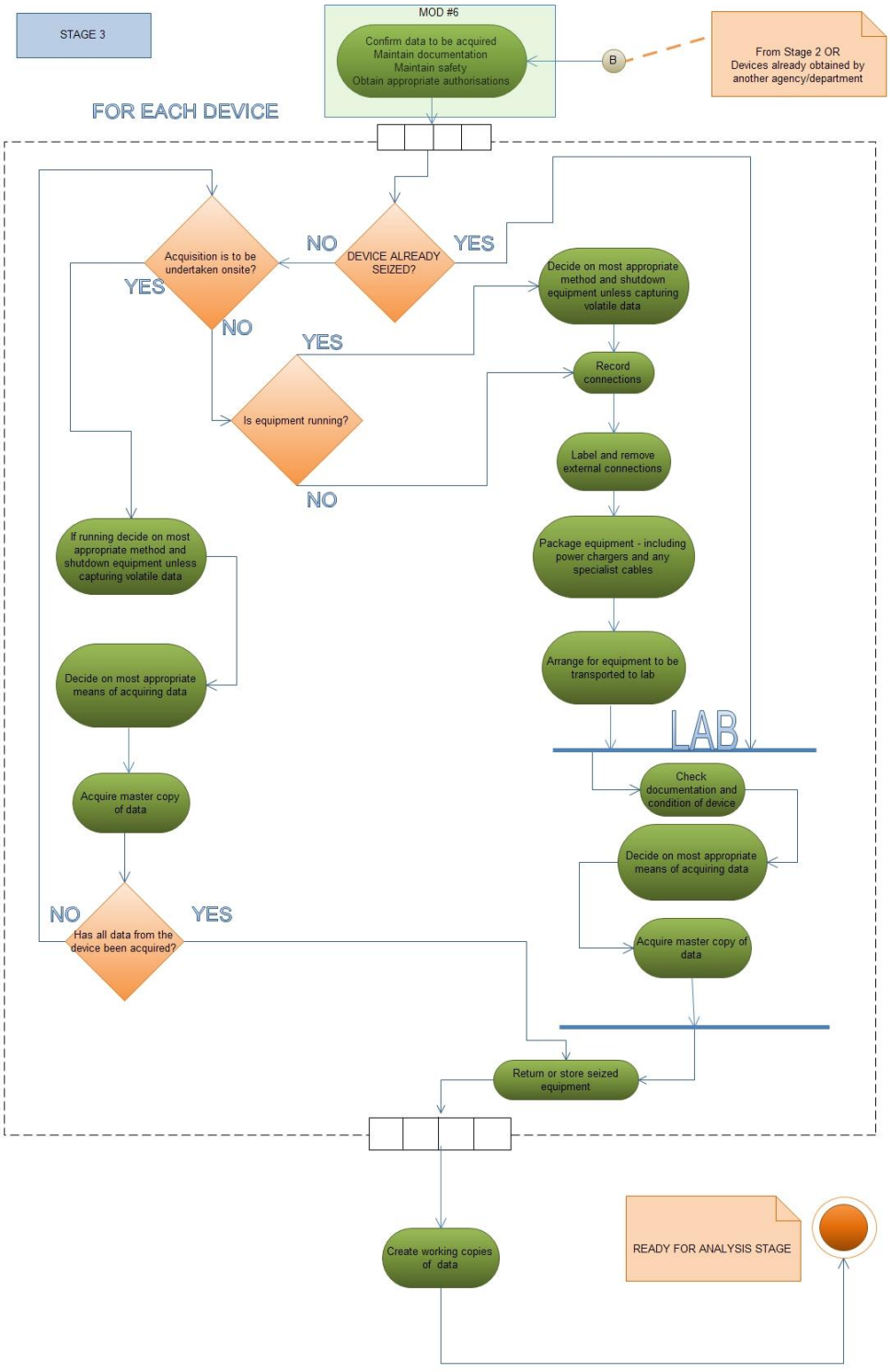

Figure 24 The ADAM Stage 3 amended (within shaded area) for MOD #6

Amendment to ADAM Stage 3 Activity diagram catering for MOD #10 (shaded) – to cater for capturing network/cloud/live data (incorporating previous change for MOD #6 in relation to obtaining appropriate authorisation)

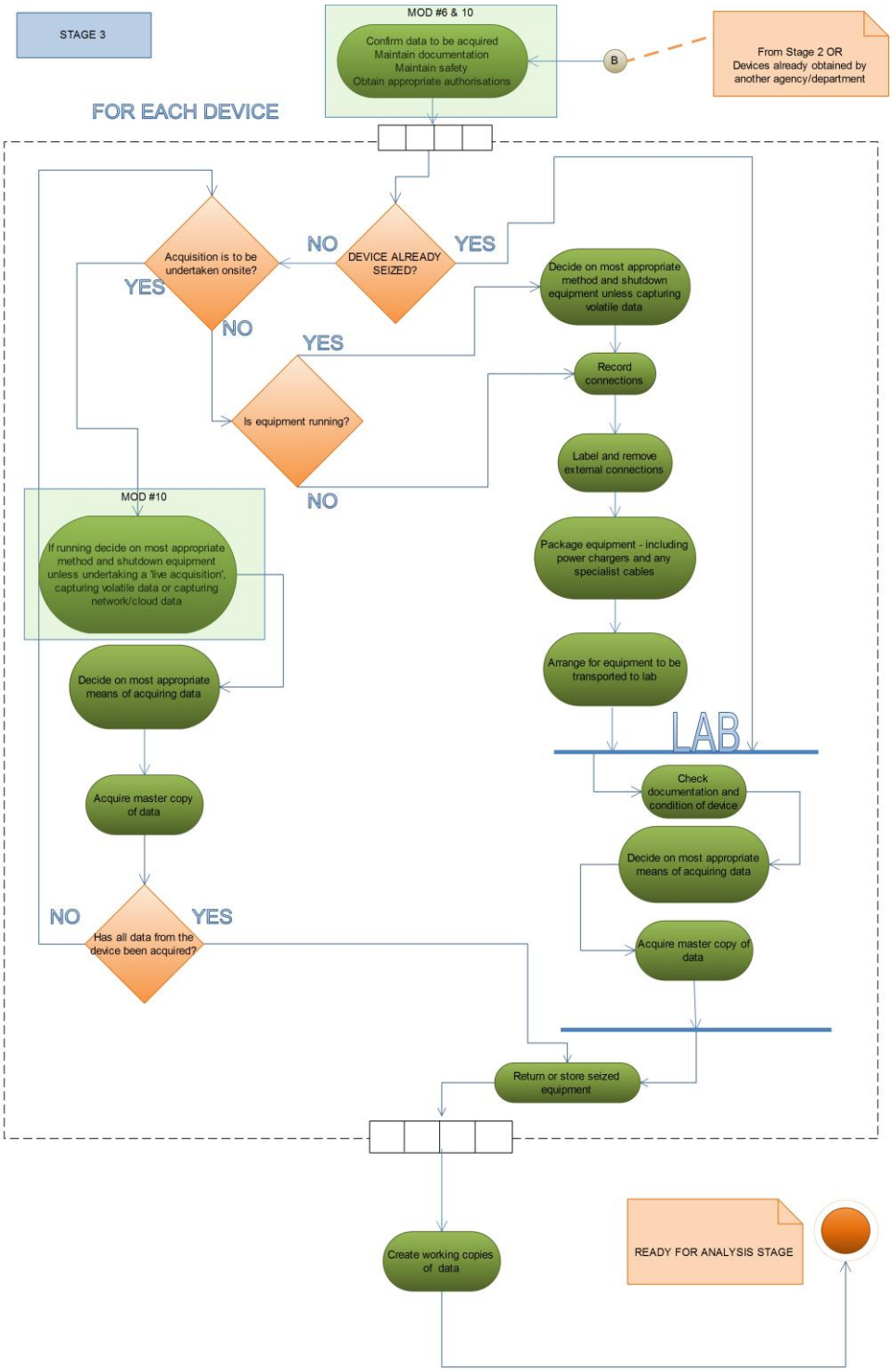

Figure 25 The ADAM Stage 3 amendments catering for network/cloud/live acquisition

6.6 Completed ADAM

The final version of the ADAM is provided at **Appendix 2**. This comprises of the following:

- The formal model representation in the form of three UML Activity diagrams, one for each stage of the model
- The Operation representation in the form of a statement of the ADAM Principles and the Adam Operation guide.

Appendix 3 contains the Background Information for the three stage model that will assist organisations with implementing the ADAM and integrating their own policies and procedures.

6.7 Summary

This chapter has described the evaluation stage of the DSRP model as interpreted in this thesis. The feedback received from both the Expert Panel and the Practitioner Panel regarding the ADAM was generally positive. There were, however, several improvements suggested (23 from both the Expert panel and the Practitioner Panel) and whilst some are considered outside the scope of the ADAM, ten changes were made to either the UML diagrams or the Operational presentation.

Chapter 7: Conclusion

7.1 Introduction

This chapter includes discussion of the final stage of the DSRP (Communication) that has been followed in this research, summarises how this thesis has brought about the development of the ADAM and discusses how it might be used in its intended environment. The ADAM and its development are also placed in context with future research in the field of digital forensics.

7.2 Communication

The final stage of the Peffers et al DSRP is communication of the results. This began with the background and rational for the model being presented to 27 attendees in December 2010 at the HTCIA Asia Pacific Training Conference held in Hong Kong.

Following on from the process of seeking feedback from practitioners for the ADAM a National Director and experienced trainer for two of the leading computer forensic products has indicated that they will be adopting the ADAM as part of their own in-house procedures. In addition:

- The ADAM is introduced in a peer-reviewed book chapter to be published in December 2012 by IGI Global: Chapter 5 – "The Emergence of Cloud Storage Highlights the Need for a New Digital Forensic Process Model" (Adams, 2012a)

- Extracts from this thesis and the ADAM have been published as an article in the Australian Security Magazine (Adams, 2012b) as the first in a series of articles that will cover all aspects of the model
- The ADAM is incorporated into a University postgraduate unit on Forensics and Information Technology (Adams, 2012c)
- The ADAM is to be presented in its final form to members of the High Technology Crime Investigators Association through the vice-president of the Asia-Pacific chapter.

7.3 Research summary

This research was initiated to address the problem that there is no formal generic process model for the acquisition of digital data that encompasses the activities of practitioners working in the different environments of law enforcement, commerce and incident response and which can assist courts of law in determining the reliability of the acquisition process employed to collect potential digital evidence**.**

- **Chapter 1** introduced the research objective which was:

  To develop a formal model of the process for the forensic acquisition of digital data that is generic in that it can be employed by digital forensic practitioners in the fields of commerce, law enforcement and incident response.

From the research objective three research questions were raised:

1. *What are the essential components necessary in a model that describes a generic and forensically sound digital data acquisition process?*
2. *How can the identified components for a generic and forensically sound digital data acquisition process be organised into an operational model?*
3. *What is a suitable way for describing, presenting and using model for acquiring digital data?*

In order to answer the research questions a suitable methodology, the Peffers et al Design Science Research Process (2006), was identified, justified and used to guide the activities of this research. The first of those activities involved 'problem identification and motivation' for which an extensive review of relevant literature was undertaken.

- **Chapter 2** contained a review of the field of digital evidence followed by extensive review of relevant literature involving previous process models associated with the forensic acquisition of digital data. The review of previous models suggested three central themes which provide the framework for the review. These themes are:
    - The use of ad hoc design elements
    - Adopting a process flow approach
    - Employing some 'scientific' approach

The literature review identified a set of criteria for assessing previous process models that involved the acquisition of digital data and from the subsequent model assessment the key features and requirements of a new model were identified. Peffers states that the resources required to define the objectives of a solution include a "…knowledge of the state of the problems and current solutions and their efficacy, if any" (Peffers, et al., 2006, p. 90). The 'knowledge of the state of the problem' and the 'current solutions' for this research has been covered by the literature review of Chapter 2.

- **Chapter 3** embodied the DSRP 'define objectives' activity and sets out the new model's elements and scope, the assessment criteria for the evaluation of previous models and then the analysis of those models against the criteria with a summary of the results leading to a statement of the essential elements for the Advanced Data Acquisition Model.

- **Chapter 4** covered the DSRP 'design and development' activity starting with addressing the research questions and then detailing the model design elements together with the development assumptions. The ADAM was also presented in both its formal and 'operational' forms prior to the evaluation activity.

- **Chapter 5** discussed the methods used for evaluating the ADAM, the makeup of the review panels and the feedback and comments received.

Also discussed is the how the ADAM was amended following a review of the feedback.

- **Chapter 6** discussed how the ADAM will be used in its intended environment and places it in context with future research in the field of digital forensics.

7.4 Research questions revisited

The three research questions are:

1. *What are the essential components necessary in a model that describes a generic and forensically sound digital data acquisition process?*
2. *How can the identified components for a generic and forensically sound digital data acquisition process be organised into an operational model?*
3. *What is a suitable way for describing, presenting and using model for acquiring digital data?*

The first question has been addressed by reviewing the results of the Carrier and Spafford criteria applied to each of the models covered in the literature review of Chapter 2. This identified several researchers whose particular contributions influenced the creation of the ADAM by helping identify the essential components necessary for modelling a generic and forensically sound digital data acquisition process.

The second question was addressed by the Design and Development stage (Chapter 4) in which the information gathered through the literature review was used as the basis for the three-stage ADAM.

The third question was addressed in Chapter 5 in which an evaluation process involving external panels of experts and practitioners was undertaken to determine the suitability of the ADAM for the environment in which it is intended to be used based on the attributes of 'utility' and 'usability'.

7.5 Research objective achieved

The overall research objective is:

> *To develop a formal model of the process for the forensic acquisition of digital data that is generic in that it can be employed by digital forensic practitioners in the fields of commerce, law enforcement and incident response.*

As stated in Chapter 1, in order to achieve the research objective the three research questions needed to be answered and this has been covered in 6.1.2. In addition, also stated in Chapter 1, the ADAM must satisfy the following criteria:

- There must be a formal representation of the model
- The model must be relevant to the fields of commerce, law enforcement and incident response.

The formal representation requirement has been addressed through the adoption of activity diagrams from the UML which have been reviewed and evaluated by a panel of experts and practitioners.

The requirement for the model to be relevant has been addressed by synthesising the aspects of existing models in a generic fashion after a substantial review of current literature in the field. The resulting model has been evaluated for relevance by expert practitioners with backgrounds in law enforcement, commerce and incident response.

7.6 Research contribution

This work provides a generic model of the digital forensic acquisition process where none previously existed thereby creating a common framework that can be adopted by practitioners working in three key areas of digital forensics. The new model can also be used as the basis for further research relating to the other aspects of digital forensic activities; 'analysis' and 'presentation'.

This work also suggests that the use of the Daubert test for determining the reliability of digital evidence is not appropriate for the acquisition stage of the digital forensic process. This assertion is supported through the literature review in which the Daubert test is applied to previous models and found to be currently incompatible with digital forensic process models in two of its key aspects, namely the existence of a 'known potential rate of error' and the 'degree of acceptance within the relevant scientific community', neither of which can be determined through a recognised measure. Finally, in defining the Advanced Data Acquisition Model, this research has shown how the digital forensic

acquisition process can be described using a proven formal notation, the Unified Modelling Language, which will add to the 'scientific' credentials of digital forensics and from a practical perspective aid the courts in relation to the presentation of digital evidence through a better understanding of the process.

7.7 Limitations and future work

7.7.1 Limitations

For the in-house evaluation only a small number of cases were selected and these are not claimed to be representative of all the activities undertaken by the organisation. This activity provides only a preliminary 'proof-of-concept' to determine if there were any serious issues with the model structure and contents prior to the more substantive evaluation carried out by external reviewers.

Although each of the three areas - commercial practice, incident response and law enforcement - were represented by at least one external reviewer, this cannot be considered as being a significant sample of the population of digital forensic practitioners working in Australia as, for example, the Linked-In group 'Digital Forensics Association' has around 90 practitioners registered. However, the external reviewers that participated were made up of both 'Experts' and 'Practitioners' who have extensive skills, interest and experience in the area of digital forensics. In terms of feedback that is directly relevant in this research, several of the reviewers are the authors of previous process models.

The members of the Practitioners Panel all work within the digital forensic environment in Australia. Whilst the work of digital forensics has many common features on an international level, the fact that other practitioners are

operating in different jurisdictions under different laws means that for this research it was deemed inappropriate to attempt to cater for many different environments requiring a much larger sample of practitioner reviewers. This decision was partly based on experience of being a member of a working group on digital evidence that is trying to take into account the activities of practitioners from many different countries. However, despite the focus on Australia, this research could be used as the basis of a process model that is applicable in other jurisdictions with only minor alterations.

An assumption has been made that the courts will not be required to conform to a new international standard to determine the reliability of digital evidence that is incompatible with the new model developed in this research. As a member and contributor of the Australian Standards Working Group for the international guideline being developed in relation to the collection of digital evidence (ISO/IEC DIS 27037) the thesis author has endeavoured to ensure that there are no aspects of the model that would be incompatible with those guidelines. Although the author is not aware of any other international guidelines being developed, potentially from a legal rather than a technical perspective, the processes described in the ADAM can be readily adapted to accommodate additional requirements.

7.7.2 Future work

As the ADAM has yet to be independently evaluated in the field, future work could include a more comprehensive trial by practitioners as part of a wider study. The current focus on Australia could also be extended to other jurisdictions by seeking input and feedback from overseas practitioners,

potentially through one of the international organisations such as the High Technology Crime Investigators Association.

Having established a formal process model for the initial stages of digital forensics, future research could be undertaken that would build on the UML Activity diagrams and textual representations of the ADAM to incorporate other aspects of the UML (such as Sequence diagrams) to provide a more comprehensive model. Ultimately the other activities of digital forensic practitioners (such as analysis and presentation) could be incorporated in the same format in order to provide a complete formal model of digital forensics.

One of the risks associated with developing a process model in a fast-changing environment such as digital forensics is that it may quickly become obsolete as new technology is adopted. By identifying the key high-level processes and leaving implementation of detailed policies and low-level procedures to the digital forensic practitioners the ADAM has addressed this weakness and its adaptability is indicated by its inclusion in a peer-reviewed book chapter where it is applied to the 'cloud' environment (Adams, 2012a).

7.8 Summary

The model has been discussed in its operational context and its key benefits to practitioners have been highlighted. The limitations of this research have been identified as have the potential future research opportunities that can stem from the approach adopted in developing the ADAM. The forums in which this research has been, or will be, communicated have been identified.

Appendix 1 – Demonstration results

(Discrepancies highlighted in red italics)

ADAM Demonstration STAGE ONE

ADAM Activity	Investigation 1	Investigation 2	Investigation 3
Understand requirements of the task	Meeting held with client and notes taken. Official request for services received with scope. Scope confirmed with engagement letter to client.	Meeting held with client and engagement letter created with detailed scope.	Meeting held with client and engagement letter created with detailed scope. Assistance provided with the wording of the application for the Anton Pillar order.
Determine overall picture	Covered in client briefing	Covered in client briefing	Covered in client briefing
Determine required outcomes	Covered in client briefing	Covered in client briefing	Covered in client briefing
Determine parameters	Copy of court order obtained detailing limitations.	Covered in client briefing	Copy of court order obtained detailing limitations.
Consider Constraints			
Authorisation	Internal - All internal engagement acceptance documents completed. External - Confirmed names of personnel involved in the acquisition are included on the court order.	Signed engagement letter taken as authorisation to undertake the work. In addition, the client provided the laptops involved.	Internal - All internal engagement acceptance documents completed. External - Confirmed names of personnel involved in the acquisition are included on the court order.
Physical	Confirmed single location. No pre-site inspection undertaken. Public access available to reception and then reliant on court order to permit access to computers. *Out of hour's access not arranged at this stage.*	Not applicable – client handed over the laptops to be imaged in the forensic lab offsite.	Confirmed single location. No pre-site inspection undertaken. Reliant on court order to permit access to premises and any computers/data storage devices.
Timing	Start time confirmed. No end time set as the court order was flexible.	Engagement letter included details of the time constraints in relation to after-hours and weekend working.	Start and end times noted from court order.

Data	No site inspection possible so type, amount and location of data unknown.	Specifications of the laptops were provided.	Due to the nature of the task no site inspection is possible so type, amount and location of data unknown.
Plan logistics	Logistics planning limited to an estimate of the number of computers involved and allocating three personnel for the data acquisition. An initial quantity of hard disk drives for image storage was allocated with a plan to purchase more if required. Held as file notes not as a separate document.	No record of logistics planning.	Logistics planning limited to an estimate of the likely number of computers. An initial quantity of hard disk drives for image storage was allocated. Details held as file notes not as a separate document.
Create Outline Plan	*Outline plan created as a file note' and not as a formal document.*	Outline plan created but this was based around the time constraints and the delivery of interim and final reports.	*Outline plan created as a file note' and not as a formal document. Additional information recorded on acquisition documentation*

ADAM Demonstration STAGE TWO

ADAM Activity	Investigation 1	Investigation 2	Investigation 3
Attend site	Completed – contemporaneous notes	Completed – contemporaneous notes	Completed – contemporaneous notes
Address safety issues	*Not documented*	*Not documented*	*Not documented*
Carry out preliminary survey	Undertaken with client and a list of rooms and computers formed the basis of our work plan. *Not labelled as Onsite survey*.	Undertaken with client, sources of potential evidence identified as laptops belonging to five employees held in an IT room with restricted access.	Undertaken with the Independent Solicitor and property owner. A list of rooms and computers formed the basis of the work plan. *Not labelled as Onsite survey*.
Maintain documentation of activities	Each person kept a record of their activities either in the form of contemporaneous notes in a workbook or using an acquisition form template. Continuity of evidence was maintained by the client who received the disks containing the image files whilst onsite, recorded the disk details and contents then passed them back to us.	Contemporaneous notes maintained in a workbook. Individual notes of acquisition details kept. Custody record maintained.	Contemporaneous notes maintained in a workbook. Individual notes of acquisition details kept. Custody record maintained.
Update Outline Plan	*Not done as the Outline Plan was a file note maintained on our server in the office.*	*Not required – initial scope accurately reflected the situation which was to take custody of five laptop computers for imaging prior to further analysis.*	*Not done as the Outline Plan was a file note maintained on our server in the office.*

ADAM Demonstration STAGE THREE

ADAM Activity	Investigation 1	Investigation 2	Investigation 3
Confirm data to be acquired	Confirmed with client using Onsite survey notes	Confirmed with client and documented in scope.	Confirmed with Independent Solicitor and documented in contemporaneous notes.
For Offsite Acquisition			
Decision: Device already seized?	Not applicable	Yes	No
Decision: Live acquisition appropriate?	*Consideration not stated in notes*	No	No
Decision: Onsite or offsite acquisition?	*Consideration not stated in notes*	Through documented discussion with client the decision was taken to image the laptop computer hard disks offsite.	Documented discussion with Independent Solicitor regarding decision to acquire data onsite.
Determine if equipment is running	Record made in acquisition template for all devices	Record made in acquisition template for all devices	Record made in acquisition template for all devices
Decide on most appropriate method of shutdown	*Action recorded but not decision process.*	*Action recorded but not decision process.*	Action and decision process documented in contemporaneous notes.
Shutdown equipment	Date and time recorded in acquisition template for all relevant devices.	Date and time recorded in acquisition template for all relevant devices.	Date and time recorded in acquisition template for all relevant devices.
Record connections	Data recorded in acquisition template for all devices.	Details recorded in acquisition template for all devices.	Details recorded in acquisition template for all relevant devices.
Label and remove connections	Data recorded in acquisition template for all devices.	Data recorded in acquisition template for all devices.	Data recorded in acquisition template for all devices.
Package equipment	*No details of packaging recorded*	*No details of packaging recorded*	N/A
Arrange for transportation	*No transportation details recorded separately – recorded as part of continuity documentation.*	*No transportation details recorded separately – recorded as part of continuity documentation.*	N/A

(if device already seized check documentation and state of device)	Not applicable	Documentation provided by IT practitioner.	N/A
For onsite acquisition			
Determine if equipment is running	Recorded on acquisition template for all devices	N/A	Recorded on acquisition template for all devices
Decide on most appropriate shutdown method (if applicable, i.e. if not performing a 'live' acquisition)	*Decision not documented*	N/A	Decision documented in contemporaneous notes.
For onsite or Lab acquisition			
Decision: Most appropriate means of acquiring data	*Decision not documented but outcome is recorded on acquisition template*	*Decision not documented but outcome is recorded on acquisition template*	*Decision not documented but outcome is recorded on acquisition template*
Acquire data	Details recorded on acquisition template together with hash value and verification result.	Details recorded on acquisition template together with hash value and verification result.	Details recorded on acquisition template together with hash value and verification result.
Maintain appropriate documentation	Details recorded on acquisition template and in contemporaneous notes.	Details recorded on acquisition template and in contemporaneous notes.	Details recorded on acquisition template and in contemporaneous notes.
Create working copy and maintain appropriate notes	Details recorded in contemporaneous notes.	Details recorded in contemporaneous notes.	Working copy not created onsite but later on return to forensic lab as first action – documented in contemporaneous notes.
In all cases			
Place working papers in storage	Engagement folder with working papers stored in document management system	Engagement folder with working papers stored in document management system	Engagement folder with working papers stored in document management system
Return any seized equipment	Details recorded on Custody form	Details recorded on Custody form and in contemporaneous notes.	N/A
Maintain documentation for above	Covered above with exceptions highlighted	Covered above with exceptions highlighted	Covered above with exceptions highlighted

Appendix 2 - The ADAM

Formal presentation

The two aspects of the ADAM are now presented in their final form. Firstly the UML Activity diagrams for each of the three stages are shown in Figures 26, 27 and 28.

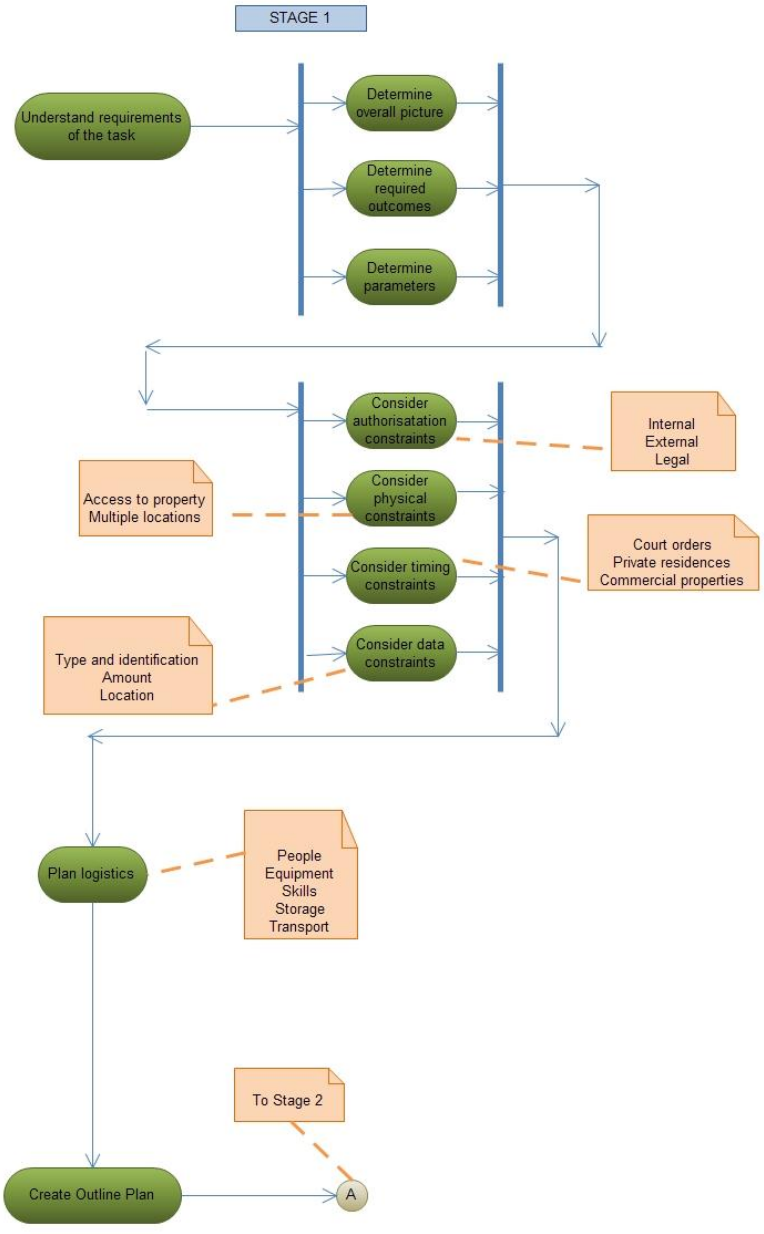

Figure 26 The ADAM STAGE 1 (Initial Planning)

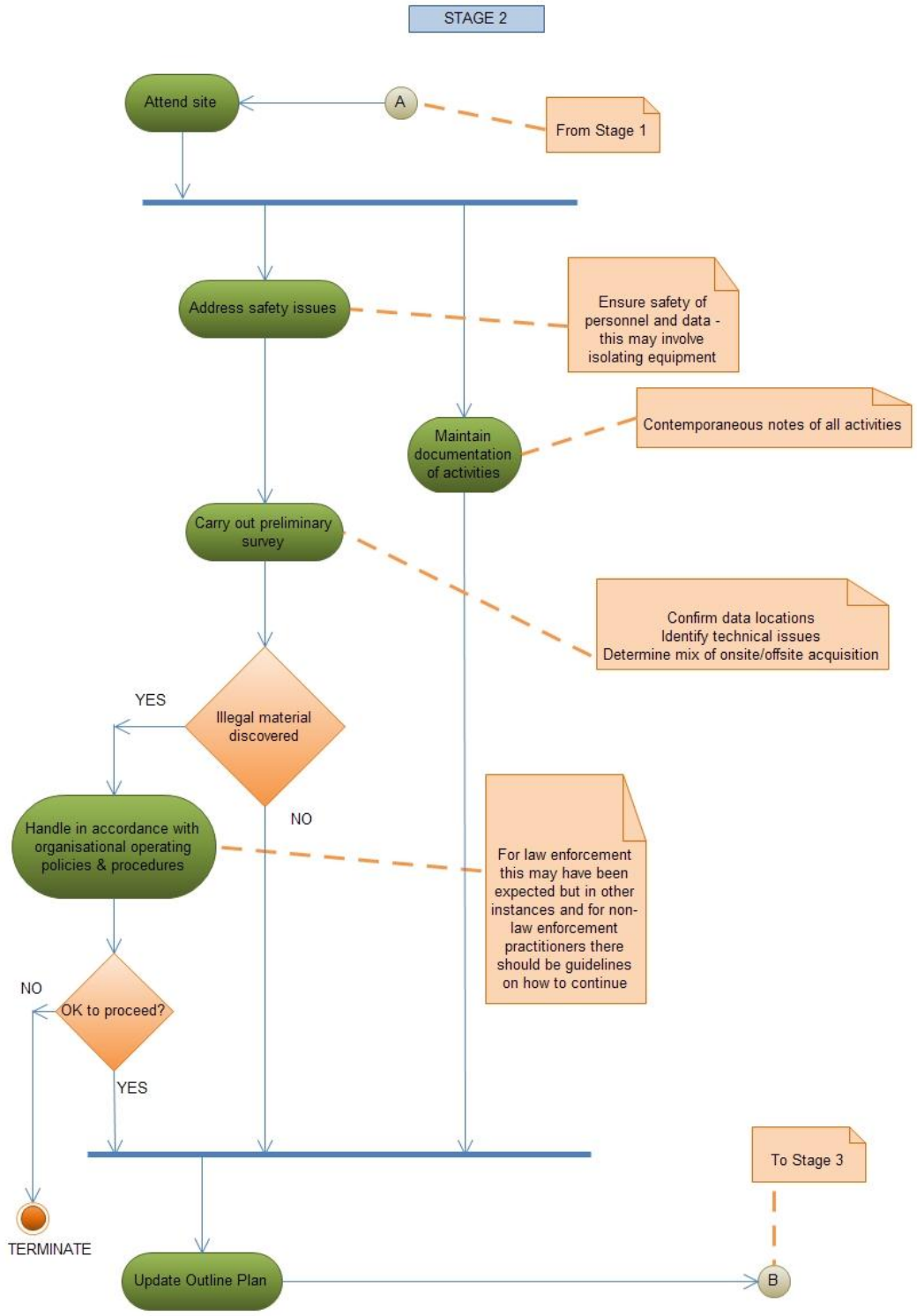

Figure 27 The ADAM STAGE 2 (Creating the Onsite Plan)

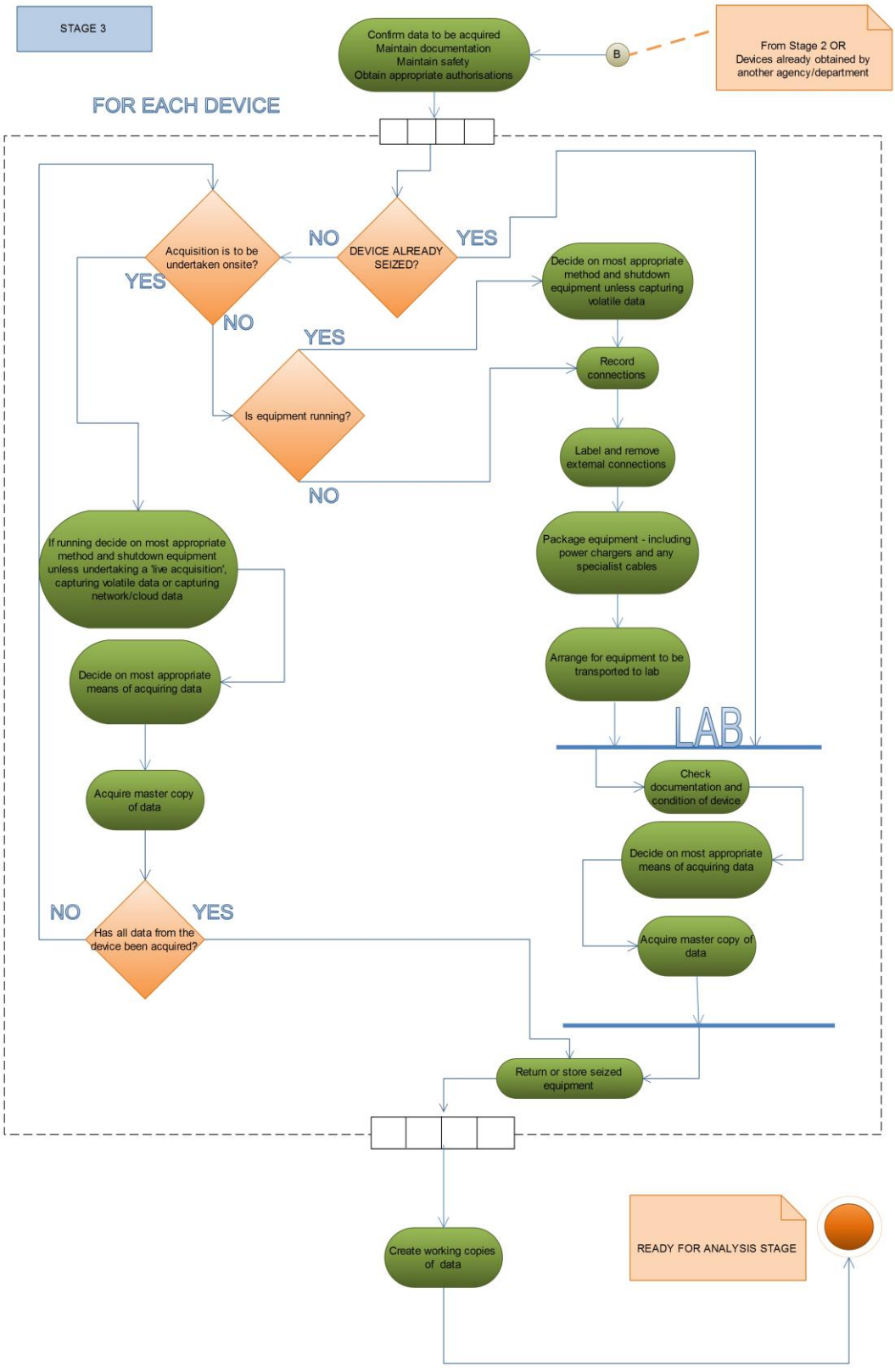

Figure 28 The ADAM STAGE 3 (Acquiring Digital Data)

Operational presentation

The Operational presentation consists of a statement of the overriding ADAM Principles and ADAM Operation Guides enabling them to follow the ADAM process model:

ADAM PRINCIPLES

The following overriding principles must be followed by the digital forensic practitioner:

1. The activities of the digital forensic practitioner should not alter the original data. If the requirements of the work mean that this is not possible then the effect of the practitioner's actions on the original data should be clearly identified and the process that caused any changes justified
2. A complete record of all activities associated with the acquisition and handling of the original data and any copies of the original data must be maintained. This includes compliance with the appropriate rules of evidence, such as maintaining a chain of custody record, and verification processes such as hashing
3. The digital forensic practitioner must not undertake any activities which are beyond their ability or knowledge
4. The digital forensic practitioner must take into consideration all aspects of personal and equipment safety whilst undertaking their work
5. At all times the legal rights of anyone affected by your actions should be considered
6. The practitioner must be aware of all organisational policies and procedures relating to their activities
7. Communication must be maintained as appropriate with the client, legal practitioners, supervisors and other team members.

ADAM OPERATION GUIDE

Stage 1 – Initial Planning

The digital forensic practitioner:

- MUST understand the requirements of the task, document the work to be performed and have this confirmed by the client or person providing the instructions to undertake the acquisition task

- MUST consider if the work can be undertaken by confirming that you have the appropriate:

    1. internal authorisation and/or
    2. external authorisation and/or
    3. authority in law

- MUST consider

    1. time constraints – is the task achievable within the time allowed?
    2. physical constraints – access to the data and physical/logical locations
    3. data constraints – how will the potential evidence be identified, how much is there likely to be?

- MUST consider safety issues

- SHOULD create the Outline Plan (an exception being in-house acquisition from devices already obtained, e.g. at law enforcement computer crime laboratories).

ADAM OPERATION GUIDE

Stage 2 - Creating the Onsite Plan

The digital forensic practitioner:

- **MUST** identify and address any security or safety issues
- **MUST** secure access to all potential sources of evidence, either directly or remotely
- **MUST** undertake a preliminary survey and document changes to the Outline Plan
- **MUST** consider
    1. all the locations that might need to be searched
    2. any issues that must be addressed relating to hardware and software
    3. personnel and equipment needs for the investigation
    4. whether onsite acquisition, offsite acquisition or a mixture of both is appropriate and possible.

ADAM OPERATION GUIDE

Stage 3 - Acquisition of Digital Data (per device)

The digital forensic practitioner MUST identify the most appropriate way of acquiring potential evidence given the constraints of time, resources, potential evidentiary value and technical limitations.

In order to do this the digital forensic practitioner:

- **MUST** consider
    1. The most appropriate method of shutting down system(s) if applicable
    2. Write-protection method including interface, e.g. via USB/FireWire/eSATA
    3. Addressing encryption issues
    4. The appropriateness of undertaking live acquisition
    5. Acquisition software to be used
    6. Source device interface(s) – e.g. boot device on host, storage device removed and attached to acquisition system, network acquisition, operating system (live acquisition)
    7. Potential volume of data
    8. Target storage capacity
    9. Target interface (speed-related)
    10. Prioritising acquisition if more than one source
- **MUST** maintain comprehensive notes
- **SHOULD** consider photographing and/or sketching the equipment and storage device locations
- **MUST** consider the requirements or benefits of an initial review of potential evidence devices and decide if it is appropriate for this to be carried out 'live' or write-blocked
- **SHOULD** create a 'working copy' of acquired data as quickly as possible and concurrent with the creation of the master copy if possible
- **MUST** keep all copies of acquired data secure
- **MUST** be able to verify the integrity of acquired data.

Appendix 3 Background Information

The ADAM Principles, UML activity diagrams for each of the three ADAM Stages together with the ADAM Operation Guide for each stage are designed to be a simple high-level description of the activities to be undertaken by experienced digital forensic practitioners. Practitioners may also want to date and sign hard copies of the appropriate ADAM Stage as a file note confirming that all the activities have been carried out.

The following sections are intended to provide background information relating to the activities for each stage but the detail is deliberately left for the digital forensic practitioner to apply as appropriate based on their own policies and procedures.

Stage 1 - Initial Planning

a. Authorisation 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; 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 (external authorisation).

Internal authorisation

This can range from simply a verbal instruction from a superior to the completion of a comprehensive series of documents requiring numerous checks and signatures.

External authorisation

There may be instances, particularly in commercial practice, whereby access to equipment holding potential evidence may be owned or under the control of someone other than the person or entity providing the instructions such as a provider of IT services storing the data to be acquired on one of their own systems. This may be particularly relevant in the case of cloud computing.

Authorisation in law

The computer forensic practitioner must ensure that all work must be carried out in accordance with the relevant laws. For example, commercial practitioners in cases such as the serving of Anton Pillar orders or helping with matters where government bodies have ‘search and seize’ powers need to ensure that they have the legal 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.

b. Timing constraints

An important aspect of the planning stage is determining constraints based on time, of which there are three aspects. In addition, for relevant data that 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. The three aspects to be considered under timing constraints are in relation to Court Orders/Warrants, Private Premises and Commercial Premises.

Court orders and warrants

Court orders often place strict time limits 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.

Private premises

If private premises are involved this may require getting to the premises before the subject of the court order leaves for work (or some other activity) but preferably after their partners and /or children have left the building.

Commercial premises

If commercial premises are involved this may require a key holder to arrive and provide access. There may be the 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.

c. Physical constraints

There are two physical constraints to consider: access and location. These constraints may also have an impact on other constraints:

Access

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.

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 and private premises may have limited access or restricted parking.

Layout

Data may be 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.

e. Data constraints

The data are the digital information that is the target of the acquisition process and can take many forms. There are three constraints to be considered in this activity:

Identification

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 graphical 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’ via a write-blocking device. The processes undertaken in relation to this constraint may have a significant impact on the time required to carry out the work.

Amount

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. Consideration of the impact on other resources also needs to take place such as the effect on a business network if large volumes of data are being transferred for an extended period during normal work hours.

Location

If the data to be reviewed and acquired are stored on backup tapes, e.g. the time period of interest is such that the data are 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. In the case of 'cloud computing' the data may reside on equipment that is not owned or controlled by the owner of the data.

f. Creating 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.

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 external personnel involved
6. Contact numbers of team leaders/lawyers/client liaison distributed (if applicable)
7. Details of known target storage locations, protocols and key words (if applicable)
8. Applicable constraints – authorisation, physical, timing and data.

The composition of the acquisition equipment to be used should to be determined by the computer forensic professional based on their knowledge, experience and resources.

Stage 2 - the Onsite plan

Once on site there are two activities that need to be undertaken immediately and then the Preliminary Survey should be completed to address any shortcomings in the Outline Plan now that it is possible to obtain more detail of the actual environment.

a. Address safety issues

The first action upon arrival on site is to ensure the safety of the computer forensic practitioner(s).

b. Secure the scene

Having gained access to the site(s) in which relevant digital 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.

c. Carry out a preliminary survey

If possible and appropriate take photographs and/or sketches of the scene. The preliminary survey should be undertaken in order to complete the planning process started with the creation of the Outline Plan. This survey should include the following activities:

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 acquisition process*
4. *Determine which devices can be physically removed from the site*
5. *Identify all individuals who had access to the equipment containing potential evidence.*

d. Updating the Outline Plan

Once the computer forensic practitioner is on site the Outline Plan needs to be reviewed and updated. 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.

Stage 3 - Acquisition of Digital Data

Confirm the details of the data to be acquired and any procedures to be followed or constraints. Each device whose data is to be acquired should be considered separately and it is vitally important to ensure that comprehensive documentation is maintained.

The ADAM Stage 3 Activity Diagram should be used as the framework for acquiring digital data but specific guidance should be sought from the organisations' own standard operating procedures (or similar document), ACPO Guidelines and the ISO/IEC 27037.

Key decision elements of ADAM Stage 3

a. Device already seized?

The model allows for the fact that this stage may not necessarily follow on from Stage 2 in situations where another agency or department has already obtained the equipment containing the data storage device(s). This could occur, for instance, where a law enforcement officer has seized the equipment during a

non-computer forensic operation prior to approaching the computer forensic division for assistance or where the client of a commercial practitioner hands over a device used by a previous employee. If this is the case the process starts at the computer forensic laboratory.

b. Acquisition to be undertaken onsite?

If the device has NOT already been seized a decision is required as to whether it is appropriate to acquire the data onsite or offsite.

c. Is equipment running?

The running status of a device needs to be determined and may involve some activity that could potentially alter data, reference appropriate guidelines.

d. Has all the data from the device been acquired?

The acquisition of volatile data from a particular item of equipment may require that the device has to be accessed on more than one occasion, first whilst still running and then after it has been shut down. The model allows for this particular situation so that the process for acquiring the non-volatile data may be completed following on from the acquisition of the volatile data. If only non-volatile data is required then the loop is not required and the equipment is returned.

The first forensic image acquired from a device is described in the model as the ‘master copy’. In some situations two copies of the acquired data may be created simultaneously in which case one should be identified as the ‘master copy’ and the other identified as the ‘working copy’. Where it is not

possible/practical to create the working copies of acquired data onsite then this process should be carried out as soon as is practical to mitigate the risk of hardware failure of the master copy storage device.

Bibliography

Adams, R. (2012a). The Emergence of Cloud Storage Highlights the Need for a New Digital Forensic Process Model *Cybercrime and Cloud Forensics: Applications for Investigative Processes*: IGI Global.

Adams, R. (2012b). Evidence and Digital Forensics. *Australian Security Magazine* August 2012. from http://www.australiansecuritymagazine.com.au/

Adams, R. (2012c). FNSC8617 Forensics and Information Technology [PG], 2012, from http://units.handbooks.uwa.edu.au/units/fnsc/fnsc8617

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.

Applegate, L. M. (1999). Rigor and Relevance in MIS Research-Introduction. *MIS Quarterly, 23*(1), 1-2.

Archer, L. B. (1984). *Systematic Method for Designers*. London: John Wiley.

Argy, P. (2006). Electronic Evidence, Document Retention and Privacy Retrieved from http://www.mallesons.com/publications/2006/Mar/8367966w.htm

Armstrong, C. (2003). Mastering Computer Forensics. In C. Irvine & H. Armstrong (Eds.), *Security Education and Critical Infrastructures*: Kluwer Academic Publishers.

Armstrong, C., & Armstrong, H. (2010). *Modeling Forensic Evidence Systems Using Design Science.* Paper presented at the IFIP WG 8.2/8.6 International Working Conference, Perth, Western Australia.

Ashcroft, J. (2001). *Electronic Crime Scene Investigation: a guide for first responders*. from http://www.ncjrs.gov/pdffiles1/nij/187736.pdf.

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

Barlas, Y. (1996). Formal aspects of model validity and validation in system dynamics. *System Dynamics Review, 12*(3).

Baryamureeba, V., & Tushabe, F. (2004). *The Enhanced Digital Investigation Process Model*. Paper presented at the Digital Forensic Research Workshop.

Beebe, N., & Clark, J. (2004). *A Hierarchical, Objectives-Based Framework for the Digital Investigations Process*. Paper presented at the Digital Forensics Research Workshop 2004.

Bell, D. (2003). UML basics: An introduction to the Unified Modeling Language. Retrieved from http://www.ibm.com/developerworks/rational/library/769.html

Boddington, R., Hobbs, V., & Mann, G. (2008). *Validating digital evidence for legal argument.* Paper presented at the 6th Australian Digital Forensics Conference, Perth, Western Australia.

Bogan, A. C., & Dampier, D. A. (2005). *Unifying Computer Forensic Modeling Approaches: A Software Engineering Approach*. Paper presented at the Proceedings of the First International Workshop on Systematic Approaches to Digital Forensic Engineering.

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* (First ed.): Charles River Media.

Bruce, C. (2007). Questions Arising about Emergence, Data Collection, and Its Interaction with Analysis in a Grounded Theory Study *International Journal of Qualitative Methods, 6*(1), 51-68.

Buskirk, E. v., & Liu, V. T. (2006). Digital evidence: Challenging the Presumption of Reliability. *Journal of Digital Forensic Practice, 1*(1), 19 - 26.

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.

Carrier, B. (2003). Defining Digital Forensic Examination and Analysis Tools Using Abstraction Layers. *International Journal of Digital Evidence, 1*(4).

Carrier, B., & Spafford, E. H. (2003). Getting Physical with the Digital Investigation Process. *International Journal of Digital Evidence, 2*(2).

Carrier, B., & Spafford, E. H. (2004). *An Event-Based Digital Forensic Investigation Framework*. Paper presented at the Digital Forensics Research Workshop 2004.

Casey, E. (2004). *Digital Evidence and Computer Crime*: Elsevier Academic Press.

Casey, E., & Stellatos, G. J. (2008). The impact of full disk encryption on digital forensics. *SIGOPS Oper. Syst. Rev., 42*(3), 93-98.

Checkland, P., & Poulter, J. (2006). *Learning for Action: A Short Definitive Account of Soft Systems Methodology and its Use for Practitioners, Teachers and Students*. Chichester: John Wiley.

Cheng, E. (2007). Independent Judicial Research in the Daubert Age. *Duke Law Journal, 56*, 1263 - 1318.

Ciardhuáin, S. O. (2004). An Extended Model of Cybercrime Investigations. *International Journal of Digital Evidence, 3*(1).

Cleven, A., Gubler, P., & Huner, K. M. (2009). *Design Alternatives for the Evaluation of Design Science Research Artifacts*. Paper presented at the 4th International Conference on Design Science Research in Information Systems and Technology.

Cohen, F. (2011). Putting the Science in Digital Forensics. *Journal of Digital Forensics, Security and Law, 6*(1), 7-14.

Federel Rules of Evidence (2010).

Cornelissen, A. M. G., Berg, J. v. d., Koops, W. J., & Kaymak, U. (2002). *Eliciting Expert Knowledge for Fuzzy Evaluation of Agricultural Production Systems*. Rotterdam: Erasmus Research Institute of Management.

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

Creswell, J. (2005). *Educational research: Planning, conducting, and evaluating qualitative research* Upper Saddle River, NJ: Merrill Prentice Hall Pearson Education.

Cummins, R., & Lowry, J. (2003). Computer Forensics 101 & Incident Response. Retrieved from httpisacala.orgdoc2003oct1_workshop_pres.pdf

Dattu, F. (1998). Illustrated Jury Instructions: A Proposal. *Law and Psychology Review, 22*, 67-102.

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

Ford, D., & Sterman, J. (1998). Expert knowledge elicitation to improve formal and mental models. *System Dynamics Review, 14*(4), 309 -339.

Freiling, F. C., & Schwittay, B. (2007). *A Common Process Model for Incident Response and Computer Forensics*. Paper presented at the Conference on IT Incident Management and IT Forensics, Germany.

Garfinkel, S. L. (2010). *Digital forensics research: The next 10 years*. Paper presented at the Digital Forensics Research Workshop 2010.

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

Gosh, A. (2004a). *Guidelines for the Management of IT Evidence*. Paper presented at the APEC Telecommunications and Information Working Group.

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

Groesser, S. N., & Schwaninger, M. (2012). Contributions to model validation: hierarchy, process, and cessation. *System Dynamics Review, 28*(2), 157-181.

Hannan, M., Frings, S., Broucek, V., & Turner, P. (2003). *Forensic Computing Theory and Practice: Towards developing a methodology for a standardised approach to computer misuse*. Paper presented at the 1st Australian Computer, Network & Information Forensics Conference 2003.

Hevner, A., & Chatterjee, S. (2010). *Design Research in Information Systems*. New York: Springer.

Hevner, A., March, S., Park, J., & Ram, S. (2004). Design science in information systems research. *Management information systems quarterly, 28*(1), 75-106.

Hutton, G., & Johnston, D. (2000). *Evidence and Procedure* (2nd ed.): Blackstone Press Limited.

I.O.C.E (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

Ieong, R. S. C. (2006). FORZA - Digital forensics investigation framework that incorporate legal issues. *Digital Invetigation, 3*, 29-36.

ISO (2001). ISO/IEC 9126-1:2001, *Software engineering -- Product quality -- Part 1: Quality model*. www.iso.org: International Organization for Standardization.

ISO/IEC (2011). DRAFT - Guidelines for identification, collection, acquisition, and preservation of digital evidence, *CD 27037*: ISO/IEC.

Jones, K. J., Bejtlich, R., & Rose, C. W. (2006). *Real Digital Forensics* (First ed.): Addison-Wesley.

Kelly, E. L. (2010). *Provided Notes as an Alternative to Juror Notetaking: The Effects of Deliberation & Trial Complexity*. University of Tasmania, Hobart.

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*.

Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). Guide to Integrating Forensic Techniques into Incident Response. In National Institute of Standards and Technology (Ed.) (Vol. 800-86): U.S. Department of Commerce.

Kessler, G. C. (2010). *Judges' Awareness, Understanding, and Application of Digital Evidence*. Nova Southeastern University.

Khatir, M., Hejazi, S. M., & Sneiders, E. (2008). *Two-Dimensional Evidence Reliability Amplification Process Model for Digital Forensics*. Paper presented at the Third International Annual Workshop on Digital Forensics and Incident Analysis, Malaga.

Kleijnen, J. (1995). Verification and validation of simulation models. *European Journal of Operational Research, 82*.

Kohn, M., Eloff, J., & Olivier, M. (2006, 5-7 July 2006). *Framework for a Digital Forensic Investigation*. Paper presented at the Information Security South Africa Conference 2006 from Insight to Foresight, Sandton, South Africa.

Kohn, M., Eloff, J. H. P., & Olivier, M. (2008, 7-9 July 2008). *UML Modelling of Digital Forensic Process Models (DFPMs)*. Paper presented at the ISSA Innovative Minds Conference, Johannesburg, South Africa.

Kruse, W. G., & Heiser, J. g. (2002). *Computer forensics: Incident Response Essentials*: Addison Wesley.

Lamsweerde, A. v. (2000). *Formal specification: a roadmap*. Paper presented at the Proceedings of the Conference on The Future of Software Engineering.

Losavio, M., Adams, J., & Rogers, M. (2006). Gap analysis: Judicial Experience and Perception of Electronic Evidence. *Digital Forensic Practice, 1*(1), 13 - 17.

Lyle, J. (2012). Computer Forensics Tool Testing Handbook. Retrieved from http://www.cftt.nist.gov/CFTT-Booklet-Revised-02012012.pdf

Mandia, K., & Prosise, C. (2001). *Incident response : investigating computer crime*: Osborne/McGraw-Hill.

Mann, P. (2004). Cybersecurity: the CTOSE project. *Computer Law & Security Review, 20*(2), 125-126.

Marcella, A. J., & Menendez, D. (2008). *Cyber Forensics: A Field Manual for Collecting, Examining and Preserving Evidence of Computer Crimes* (Second ed.): Auerbach Publications.

March, S. T., & Smith, G. F. (1995). Design and Natural Science Research on Information Technology. *Decision Support Systems, 15*(4), 251-266.

Marsico, C. (2005). *Computer Evidence v. Daubert: The Coming Conflict*: Centre for Education and Research in Information Assurance and Security, Purdue University.

Mason, S. (2007). *Electronic Evidence: Disclosure, Discovery & Admissibility*: LexisNexis Butterworths.

McDermott, J., & Fox, C. (1999). *Using abuse case models for security requirements analysis*. Paper presented at the 15th annual Computer Security Applications Conference (ACSAC '99).

McKay, J., & Marshall, P. (2005, 30Nov - 2 Dec). *A Review of Design Science in Information Systems.* Paper presented at the 16th Australian Conference on Information Systems, Sydney.

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

Mercuri, R. (2005). Challenges in forensic computing. *Commun. ACM, 48*(12), 17-21.

Meyers, M., & Rogers, M. (2004). Computer forensics: The Need for Standardization and Certification *International Journal of Digital Evidence, 3*(2).

Mocas, S. (2004). Building Theoretical Underpinnings for Digital Forensics Research. *Digital Invetigation, 1*(1), 61-68.

Moles, R. N. (2007). The Role and Function of the Expert Witness. Retrieved from http://netk.net.au/Reports/ExpertWitness.asp

National Centre for Policing Excellence (2005). Practice Advice on Core Investigative Doctrine. Retrieved from http://www.ssiacymru.org.uk/media/pdf/6/c/Core_Investigation_Doctrine_Interactive_1_.pdf

Noblett, M. G., Pollitt, M. M., & Presley, L. A. (2000). Recovering and Examining Computer Forensic Evidence. *Forensic Science Communications, 2*(4). Retrieved from http://www.fbi.gov/hq/lab/fsc/backissu/oct2000/cmptrf1.htm

Nunamaker, J. F., Chen, M., & Purdin, T. D. M. (1990). Systems development in information systems research. *Journal of Management Information Systems, 7*(3), 89-106.

Nuseibeh, B., & Easterbrook, S. (2000). *Requirements Engineering: A Roadmap*. Paper presented at the ICSE-2000 International Conference on Software Engineering.

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.

Pace, D. K., & Sheehan, J. (2002). *Subject Matter Expert (SME)/Peer Use in M&S V&V*. Paper presented at the Foundations for the V&V in the 21st Century workshop (Foundations '02).

Palmer, G. (2001). A Road Map for Digital Forensic Research. Retrieved from http://www.dfrws.org/2001/dfrws-rm-final.pdf

Peffers, K., Tuunanen, T., Gengler, C., Rossi, M., Hui, W., Virtanen, V., et al. (2006). *The Design Science research process: a model for producing and presenting information systems research.* Paper presented at the First International Conference on Design Science Research in Information Systems and Technology (DESRIST 2006), Claremont, CA.

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, California, USA.

Perumal, S. (2009). Digital Forensic Model Based On Malaysian Investigation Process *International Journal of Computer Science and Network Security, 9*(8), 38-44.

Pollitt, M. (2009). The Good, the Bad and the Unaddressed. *Journal of Digital Forensic Practice, 2*, 172-174.

Pollitt, M. M. (2007). *An Ad Hoc Review of Digital Forensic Models"*. Paper presented at the Second International Workshop on Systematic Approaches to Digital Forensic Engineering.

Quality Assurance Institute (2007). Performing the Forensic Process. Http://qaiworldwide.org/pdf_files/mar07_pw.pdf.

Reith, M., Carr, C., & Gunsch, G. (2002). An Examination of Digital Forensic Models. *International Journal of Digital Evidence, 1*(3).

Rhalibi, A. E., England, D., & Hanneghan, M. (2005). *Extending Soft Models to Game Design: Flow, Challenges and Conflicts.* Paper presented at the DiGRA 2005 Conference: Changing Views – Worlds in Play, Vancouver, Canada.

Richards, E. (2009). The Daubert Test. *LSU Law Center*, from http:// biotech.law.lsu.edu/map/TheDaubertTest.html

Rogers, M. K. (2006). DCSA: Applied Digital Crime Scene Analysis. In Tipton & Krause (Eds.), *Information Security Management Handbook* (Fifth ed.). New York: Auerbach.

Rogers, M. K. (Ed.). (2004). *DCSA: A Practical Approach to Digital Crime Scene Analysis* (Fifth ed. Vol. 3).

Rogers, M. K., Goldman, J., Mislan, R., Wedge, T., & Debrota, S. (2006). *Computer Forensics Field Triage Process Model.* Paper presented at the Conference on Digital Forensics, Security and Law, 2006.

Ruan, C., & Huebner, E. (2009). *Formalizing Computer Forensics Process with UML*. Paper presented at the UNISCON 2009.

Saferstein, R. (2010). *Criminalistics: An Introduction to Forensic Science* (10 ed.): Prentice Hall.

Sammes, T., & Jenkinson, B. (2007). *Forensic Computing: A Practitioner's Guide* (2nd ed.): Springer.

Schatz, B. (2007). *Digital Evidence: Representation and Assurance.* Queensland University of Technology.

Schwarz, J. M., Newby, T., & Carroll, O. L. (2009). *Rethinking the Storage of Computer Evidence.* Paper presented at the UNAFEI 140th International Training Course: The Criminal Justice Response to Cybercrime, Tokyo.

Selamat, S. R., Yusof, R., & Sahib, S. (2008). Mapping Process of Digital Forensic Investigation Framework. *International Journal of Computer Science and Network Security, 8*(10).

Shin, Y.-D. (2008). *New Digital Forensics Investigation Procedure Model*. Paper presented at the Fourth International Conference on Networked Computing and Advanced Information Management.

Simon, H. A. (1996). *The Sciences of the Artificial*: The MIT Press.

Slay, J., & Beckett, J. (2007). *Digital Forensics: Validation and Verification in a Dynamic Work Environment.* Paper presented at the Proceedings of the 40th Hawaii International Conference on System Sciences - 2007.

Smith, R. G., Grabosky, P. N., & Gregor Urbas (2004). *Cyber Criminals on Trial*: Cambridge University Press.

Sommer, P. (1998). Digital Footprints: Assessing Computer Evidence. *Criminal Law Review (Special Edition)*, 61-78.

Standards Australia (2012a). About Standards Australia, from http: //www.standards.org.au/OurOrganisation/AboutUs/Pages/default.aspx

Standards Australia (2012b). What is a Standard?, from http://www.standards.org.au/ StandardsDevelopment/What_is_a_Standard/ Pages/default.aspx

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

Steel, C. (2006). *Windows Forensics: The Field Guide for Conducting Corporate Computer Investigations*: Wiley Publishing.

Stephenson, P. (2003a). A Comprehensive Approach to digital Incident Investigation. *Information Security Technical Report, 8*(2), 42-54.

Stephenson, P. (2003b). DIPL: The Digital Investigation Process Language. Retrieved from http://people.emich.edu/pstephen/my_presentations/DIPL.ppt

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

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.

SWGDE (2006). *Best Practices for Computer Forensics*. from http://www.swgde.org/ documents/swgde2006/Best_Practices_for_Computer_Forensics%20July06.pdf.

Tipton, H. F., & Krause, M. (Eds.). (2006). *Information Security Handbook*: Taylor and Francis.

Trcek, D., Abie, H., Skomedal, A., & Starc, I. (2010). Advanced Framework for Digital Forensic Technologies and Procedures. *Journal of Forensic Sciences, 55*(6), 1471-1479.

Trickovic, I. (2000). Formalizing Activity Diagram of UML by Petri Nets. *Novi Sad Journal of Mathematics, 30*(3), 161-171.

Turnbull, B. (2008). *The adaptability of electronic evidence acquisition guides for new technologies*. Paper presented at the Proceedings of the 1st international conference on forensic applications and techniques in telecommunications, information and multimedia and workshop.

US-CERT (2012). Computer Forensics, from http://www.us-cert.gov/reading_room/ forensics.pdf

Venable, J. R. (2006). *The Role of Theory and Theorising in Design Science Research.* Paper presented at the First International Conference on Design Science Research in Information Systems and Technology (DESRIST 2006), Claremont, CA.

Venter, J. P. (2006). Process Flows for Cyber Forensics Training and Operations. Retrieved from http:"researchspace.csir.co.za/dspace/bitstream/10204/1073/ 1/Venter_2006.pdf

Wang, Z., & Yu, M. (2007). Modeling Computer Forensic Process from Workflow Perspective. *Journal of Communication and Computer, 4*(1).

Wiles, J. (Ed.). (2007). *The Best Damn Cybercrime and Digital Investigations Book Period*: Syngress Publishing.

Zachman, J. A. (1987). A framework for information systems architecture. *IBM Systems Journal, 26*(3), 276-292.