Journal of Digital Forensics, Security & Law

Article · January 2014

CITATIONS
0

READS
416

3 authors, including:

Richard Adams
Curtin University
6 PUBLICATIONS **24** CITATIONS
SEE PROFILE

Graham A. Mann
Murdoch University
35 PUBLICATIONS **106** CITATIONS
SEE PROFILE

THE ADVANCED DATA ACQUISITION MODEL (ADAM): A PROCESS MODEL FOR DIGITAL FORENSIC PRACTICE

Richard Adams
Murdoch University
richard.adams@uwa.edu.au

Val Hobbs
Murdoch University
v.hobbs@murdoch.edu.au

Graham Mann
Murdoch University
g.mann@murdoch.edu.au

ABSTRACT

As with other types of evidence, the courts make no presumption that digital evidence is reliable without some evidence of empirical testing in relation to the theories and techniques associated with its production. The issue of reliability means that courts pay close attention to the manner in which electronic evidence has been obtained and in particular the process in which the data is captured and stored. Previous process models have tended to focus on one particular area of digital forensic practice, such as law enforcement, and have not incorporated a formal description. We contend that this approach has prevented the establishment of generally-accepted standards and processes that are urgently needed in the domain of digital forensics. This paper presents a generic process model as a step towards developing such a generally-accepted standard for a fundamental digital forensic activity–the acquisition of digital evidence.

Keywords: digital forensics, computer forensics, evidence acquisition, forensic process model, ADAM

1. INTRODUCTION

The general principle adopted by Australian courts for documents presented as evidence is that a copy of a document is recognized as equivalent to the original and that this applies to computer copies. This issue of reliability means that courts pay close attention to the manner in which electronic evidence has been obtained and in particular the process in which the data is captured and stored. Unfortunately, the domain of digital forensics is lacking generally-

accepted processes and procedures to which they and the courts can refer. The Advanced Data Acquisition Model (ADAM) presented in this paper and in Adams (2013) was developed to go some way towards addressing this issue.

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. 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 (2006) 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.

Ciardhuáin (2004) suggests that a comprehensive approach to modeling digital forensic processes would have general benefits for IT managers, auditors and others not necessarily involved in the legal process due to the increasing incidence of crimes involving computers. Going further still, Trcek, Abie, Skomedal and Starc (2010) suggest the notion of a widely agreed-upon 'template legislation' that would harmonize the practice of digital forensics on an international basis.

A review of existing digital forensics models was presented in Adams (2013). This review showed that none of the currently available models meet the needs of practitioners and researchers, being criticized variously for being too specific (Reith, Carr, & Gunsch, 2002), too broad (Rogers, 2006), too complex (Selamat, Yusof, & Sahib, 2008), and too technical (Venter, 2006). We contend that this has prevented the establishment of generally-accepted standards and processes that are urgently needed in the domain of digital forensics.

The ADAM model proposed here is designed to address those shortcomings and to present a formal generic approach to acquiring digital evidence that can

be adopted and applied by practitioners operating in the environments of commerce, law enforcement and incident response.

2. DEVELOPING THE NEW MODEL

The design and development of the ADAM followed the design science research process (DSRP) developed by Peffers, Tuunanen, Gengler, Rossi, Hui, Virtanen, and Bragge (2006). The DSRP consists of six activities:

- Problem Identification and Motivation
- Objectives of a Solution
- Design and Development
- Demonstration
- Evaluation
- Communication

The DSRP is iterative, with feedback from the evaluation stage returning to the design and development stage. The process followed to develop the model is summarized next and is described in full in Adams (2013).

2.1 Model Design and Development

For the DSRP the problem identified was the lack of a generic process model for the digital forensic acquisition process and the objective was to create such a model with a formal description that could be adopted by practitioners working in different areas of the discipline.

The scope of the model is 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.

Contributions from previous researchers as found in the literature, personal experience of the primary author, and interactions with other digital forensic practitioners were used to identify the requirements for the new model. For the design and development stage the top-level approach was to:

1. Identify criteria against which existing models will be assessed.
2. Evaluate existing models against criteria.
3. Identify common requirements across different environments.
4. Propose a new model incorporating the requirements of the different environments.
5. Demonstrate that the new model is adequate to fulfilling the requirements, and revise where necessary.

6. Test the new model with a panel of external evaluators, and revise the model where necessary.

These stages are described next.

A review of the comments from other researchers on existing models that are relevant to the research was used to formulate criteria for the overall assessment of the models or to identify existing criteria that may be employed in this way. The adopted criteria are based on those proposed by Carrier and Spafford (2003):

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

In addition to the identified assessment criteria, the models were considered in the light of the Daubert tests (Daubert,1993).

In total, 18 models were evaluated against the criteria identified (Agarwal, Gupta, Gupta, & Gupta, 2011; Baryamureeba & Tushabe, 2004; Beebe & Clark, 2004; Bogan & Dampier, 2005; Carrier & Spafford, 2003; Ciardhuain, 2004; Freiling & Schwittay, 2007; Ieong, 2006; Kent, Chevalier, Grance, & Dang, 2006; Khatir, Hejazi, & Sneiders, 2008; Kohn, Eloff, & Olivier, 2006; Mann, 2004; Reith et al., 2002; Rogers, 2006; Selamat et al., 2008; Stephenson, 2003; Venter, 2006; Wang & Yu, 2007). Each existing model was reviewed to determine which, if any, of the identified assessment criteria had been met by that model. The overall results were summarized.

Although digital forensic tools and processes are employed across a number of environments the environment scope for this process model has been restricted to the three areas of 'commerce', 'incident response' and 'law enforcement' digital forensic activity. The military environment has been excluded on the basis that for anyone outside 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. Those models most closely meeting the assessment criteria were considered for their possible contribution to the new model. A set of model attributes were 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 new model.

The contributions of previous researchers through their process models was 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 were accommodated. Particular attention was paid to criticisms of previous models to gain insight into potential design or implementation pitfalls whilst ensuring that the model remained 'forensically sound'.

2.2 Summary of Model Requirements

Three stages were identified by combining the key contributions and considering the reviewed models collectively: an initial planning stage (Stage 1), an onsite survey stage (Stage 2), and the acquisition stage itself (Stage 3). Each of these stages is logically separate in that it is undertaken at a particular point in time and the three stages are followed sequentially. The activities associated with each stage are summarized as:

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

2.3 Model Representation

The complete representation of the ADAM consists of three related documents: the formal representation in UML, the Principles, and set of Operation Guides.

UML Activity Diagrams are incorporated within the ADAM to define process flows. 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.

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

(2008) employs the Unified Modelling Language (UML)[2]. 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.

This research will develop the use of UML in digital forensics by employing UML Activity Diagrams within the ADAM to define process flows. Other UML representations, such as Case Diagrams, were not be adopted based on earlier examples of their use (Kohn, et al., 2008; Ruan & Huebner, 2009) as they appeared to add little value to the description of the process model and, in addition, 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.

In order to assist the practitioner to apply the concepts and processes that form the ADAM, an Operation Guide was developed for each of the three stages. The Operation Guides state what the practitioner MUST and SHOULD do in each stage, but at a level of detail that permits customization within each case.

2.4 Evaluation and Testing

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. This was followed by external evaluation of the model by experts. 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.

3. THE ADVANCED DATA ACQUISITION MODEL (ADAM)

The complete ADAM is now described, under the headings of the three stages identified in the requirements. Each stage is described and then represented formally in UML, and its Operation Guide presented.

A common factor associated with all three stages is *documentation*. Documentation is vital to ensure that a record is kept of all activity associated

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

with the acquisition of the electronic data and subsequent transportation and storage as there is the potential for the whole process to come under close scrutiny in court. A practitioner following the ADAM is required to ensure that appropriate documentation be maintained at all times.

The ADAM incorporates two key assumptions [in accordance with the relevant ISO/IEC document (ISO/IEC, 2012)[3]]:

- The digital forensic practitioner is authorized, trained and qualified with specialized knowledge, skills and abilities for performing digital evidence acquisition, handling and collection tasks.
- 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.

3.1 ADAM Principles

Overriding principles that must be followed by the digital forensic practitioner were developed following the literature review of previous models, standards and other texts. These principles are defined within the ADAM as:

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.
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.

[3] This document provides guidelines for specific activities in the handling of digital evidence.

6. The practitioner must be aware of all organizational policies and procedures relating to their activities.
7. Communication must be maintained as appropriate with the client, legal practitioners, supervisors and other team members.

3.2 Stage 1 Initial Planning

The first stage, Initial Planning, 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, this stage may be very brief and simply consist of checking paperwork.

In the ideal world it would be possible to obtain perfect knowledge of the environment containing the electronic data to be acquired thus enabling a detailed plan to be created that would simply have to be followed on site. However in practice the digital forensic examiner often has insufficient detail about the computer systems, quantity and location of data, types of hard disk or the operating system involved to enable anything beyond a rough outline of a plan to be produced.

Several sets of constraints must be considered in this stage: authorization constraints, physical constraints, timing constraints and data constraints.

- Authorization 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: (1) authority from the organization providing the services (internal authorization); (2) authority in law; and (3) authority from the owner of the resources containing the material to be acquired (external authorization).

- Physical constraints – Physical access to the systems containing electronic data is generally not considered in any great depth by other models and is often approached from the perspective of a commercial digital forensic practitioner simply needing to determine if data may be located at more than one site. 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; physical access to the resources containing the data to be acquired and 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.

- 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. Some authors, especially those basing their discussions on in-house digital forensic practitioners, don't consider the timing aspects at all. The ADAM requires consideration of three aspects of timing constraints; (1) the terms of court orders and warrants; (2) getting to the premises before the subject of the court order leaves for work (or some other activity); and (3) for commercial premises ensuring the key holder is available to provide access to the offices.
- Data constraints – The data is the electronic information that is the target of the acquisition process and can take many forms. As for other aspects of the planning stage it is not always clear at the outset whether there is in fact any data that is relevant to the investigation or where this data might be located.

The ADAM requires consideration of the potential *quantity* of data that may be acquired. Therefore there are three data constraints considered:

- Identification of data – The type of data to be acquired can vary greatly. The processes undertaken in relation to this constraint may have a significant impact on the time required to carry out the work.
- 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.
- 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.

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. Answers to the following questions need to be addressed:

- How many trained personnel are required?
- 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)
- How many sets of equipment are required and what should be in those kits?
- 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)
- How much storage media is required at each location and how can this be supplemented if necessary?
- 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).

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.

The activities in the ADAM Stage 1 are summarized in the formal UML representation in Figure 1. To complement the UML diagrams an Operational Guide is provided for each of the three stages.

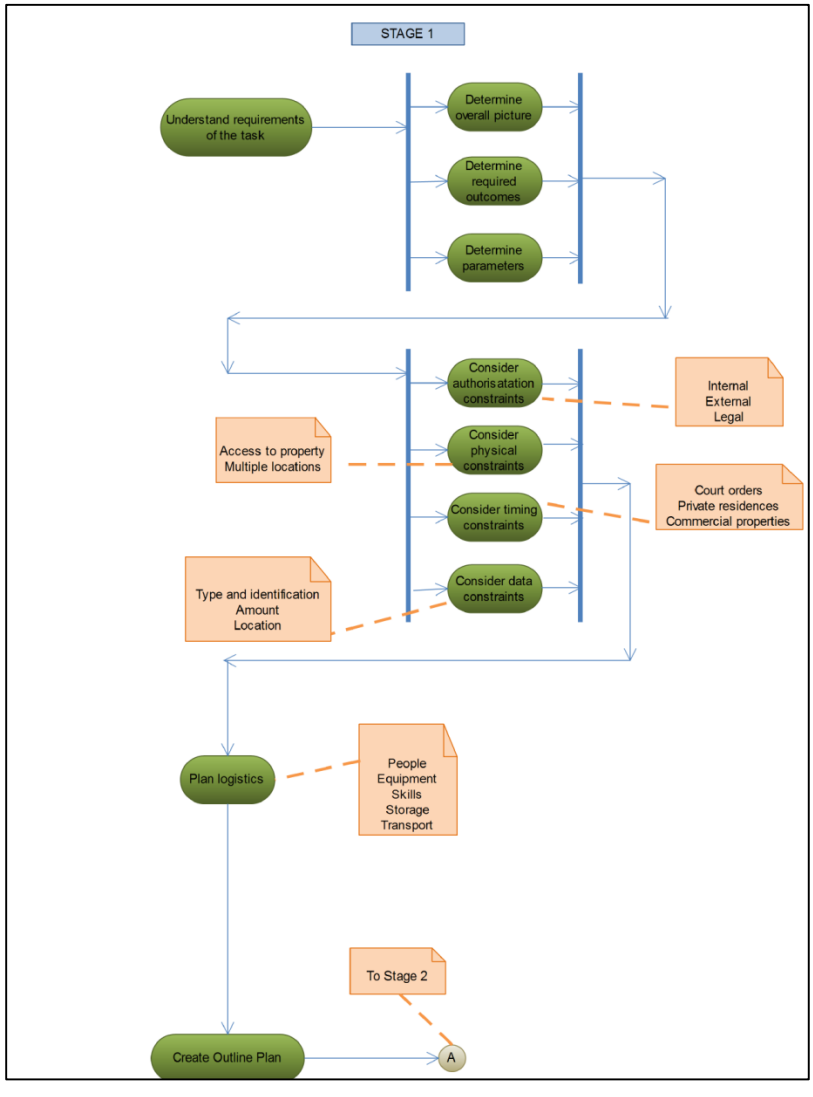

Figure 1 ADAM Stage 1 Initial Planning

3.2.1 Operation Guide for 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:

- internal authorization and/or

- external authorization and/or
- authority in law

MUST consider

- time constraints – is the task achievable within the time allowed?
- physical constraints – access to the data and physical/logical locations
- 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)

3.3 Stage 2 The Onsite Plan

In Stage 2, all the gaps in knowledge relating to the location, size and format of the devices holding the electronic data are filled in and the main acquisition plan is created. There may be instances in which this stage may be irrelevant as in the case for previously obtained devices mentioned above.

Having gained access to the site(s) in which relevant electronic data is thought to be stored, steps must be taken to ensure that the risk of potential evidentiary data being destroyed or removed is reduced as much as possible.

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.

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 electronic data. If more than one site is involved there will be the need to have separate Onsite Plans to take account of the specific local circumstances. The overall goals will likely remain the same but the steps to be taken in order to achieve them may have to be altered. This is where the knowledge and experience of the digital forensic practitioner responsible for the particular site is critical. The activities in the ADAM Stage 2 are summarized in the formal UML representation in Figure 2.

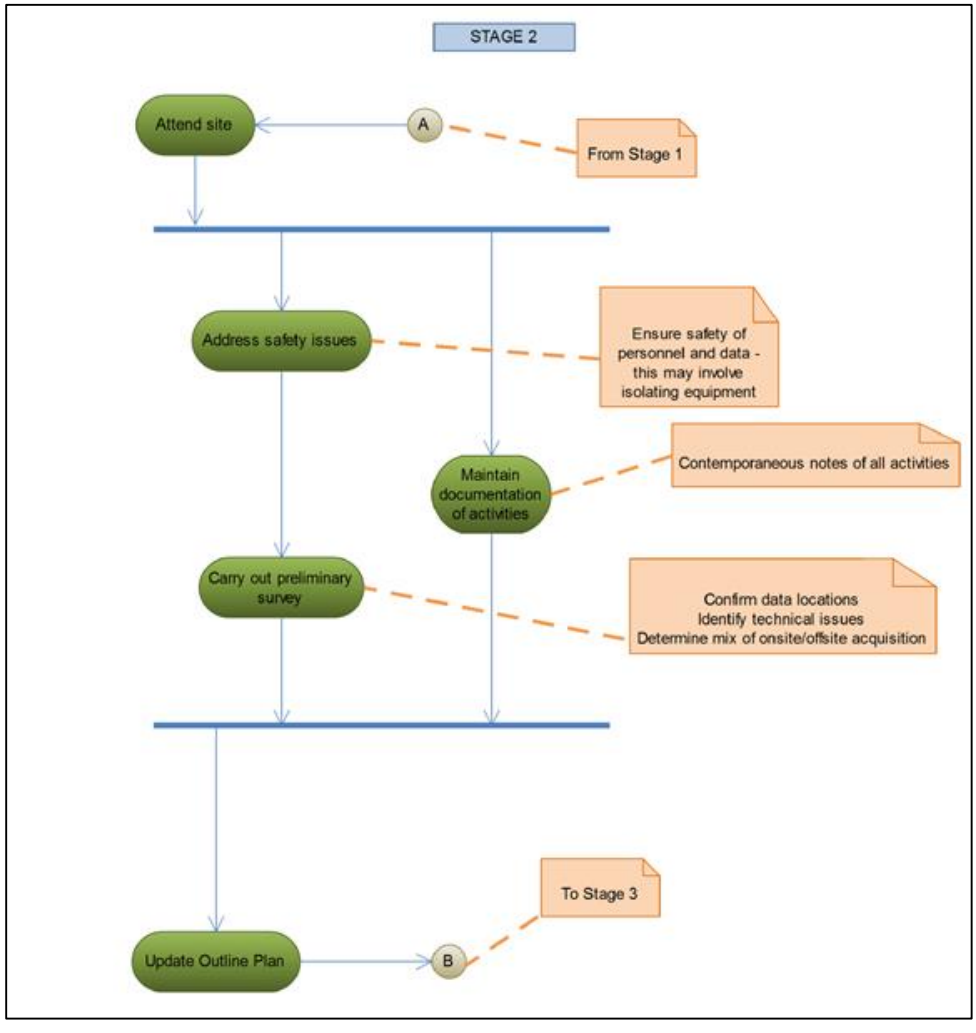

Figure 2 ADAM Stage 2 The Onsite Plan

3.3.1 Operation Guide for 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

- all the locations that might need to be searched

- any issues that must be addressed relating to hardware and software
- personnel and equipment needs for the investigation
- whether onsite acquisition, offsite acquisition or a mixture of both is appropriate and possible

3.4 Stage 3 Acquisition

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 UK Association of Chief Police Officers' (Williams, 2012) and International Standards Organization Guidelines (ISO/IEC, 2012) 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. The activities in the ADAM Stage 3 are summarized in the formal UML representation in Figure 3.

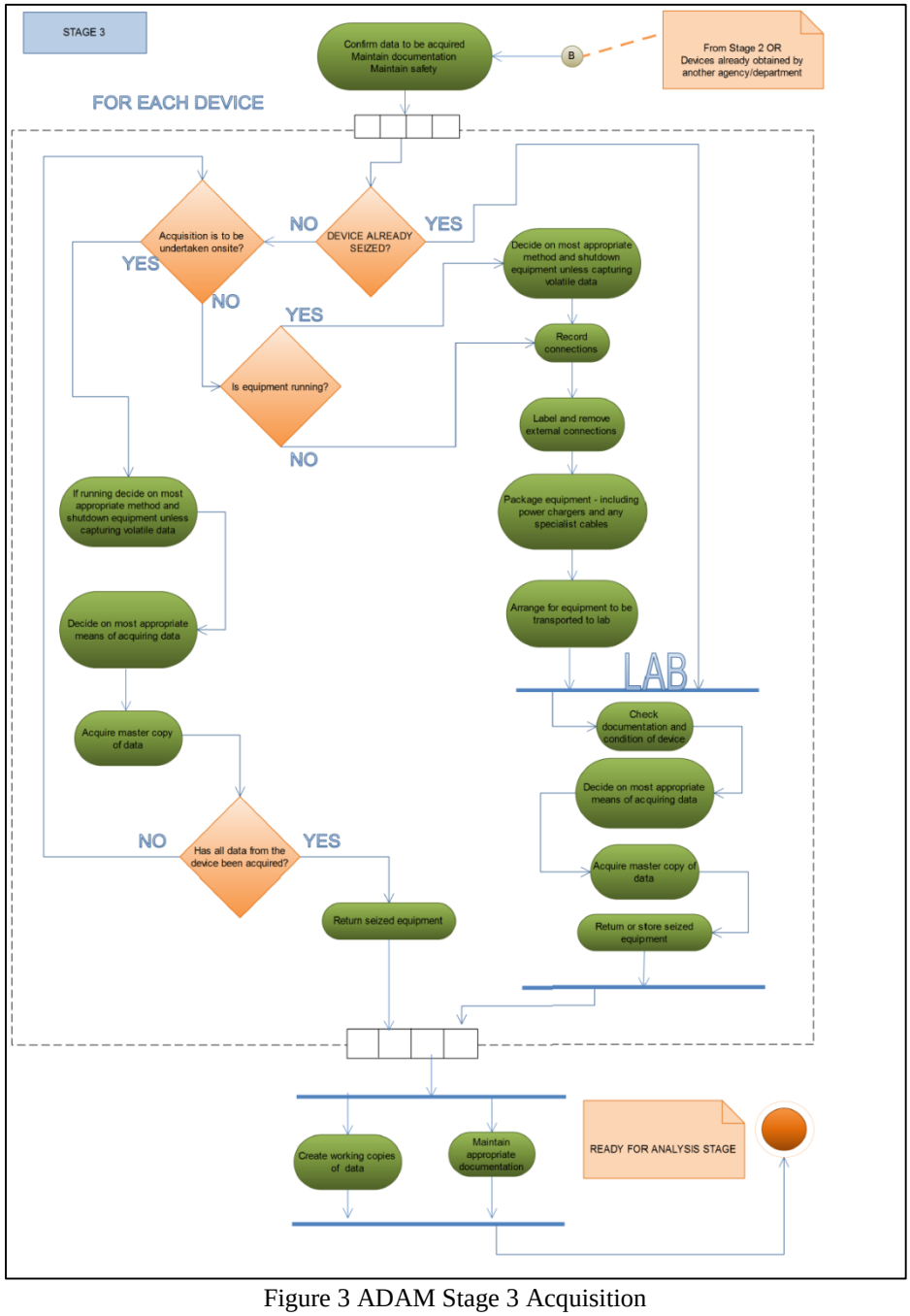

Figure 3 ADAM Stage 3 Acquisition

3.4.1 Operation Guide for 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

- The most appropriate method of shutting down system(s) if applicable
- Write-protection method including interface, e.g., via USB/FireWire/eSATA
- Addressing encryption issues
- The appropriateness of undertaking live acquisition
- Acquisition software to be used
- Source device interface(s) – e.g., boot device on host, storage device removed and attached to acquisition system, network acquisition, operating system (live acquisition)
- Potential volume of data
- Target storage capacity
- Target interface (speed-related)
- Prioritizing 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. EXAMPLE OF USING THE ADAM

Scenario – 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.

4.1 ADAM Stage 1 Initial Planning

Senior Investigator B confirms that all the appropriate authorizations 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.

4.2 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.

4.3 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.

Acquiring 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.

Acquiring 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. DISCUSSION

The expert evaluation and walkthrough scenarios demonstrate that the ADAM has the potential to formally describe the activities followed by digital forensic practitioners working in the areas of commerce, law enforcement and incident response.

For a process model, the *validity* comes from the degree to which it adheres to guiding principles around which the process is organized. 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. 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. The model also underwent an independent evaluation of this prescriptive power to determine if the model is usable. The testing process involved two independent panels of reviewers whose feedback was considered and the necessary changes made to the model.

However, some limitations of the work remain. 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 organization. This activity provided 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. However, the processes described in the ADAM can be readily adapted to accommodate additional requirements. The ADAM is also in accordance with recommended best practice as detailed in the ISO/IEC document (2012).

The ADAM has yet to be independently evaluated in the field. Future work should 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 organizations such as the High Technology Crime Investigators Association.

6. CONCLUSIONS

We have introduced the Advanced Digital Acquisition Mode (ADAM), a generic model of the digital forensic acquisition process that can be adopted by practitioners working in three key areas of digital forensics: commercial practice, incident response and law enforcement. By deliberately identifying the key high-level processes and leaving implementation of detailed policies and low-level procedures to the digital forensic practitioners the ADAM addresses the potential risk that in a fast-changing environment such as digital forensics a model may quickly become obsolete as new technology is adopted. The ADAM is described using a proven formal notation, the Unified Modeling Language, which from a practical perspective will aid the courts in relation to the presentation of digital evidence through a better understanding of the process.

The end result of using the ADAM is a clear process description 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.

Having established a formal process model for the initial stages of digital forensics, future research can build on the UML Activity diagrams and textual representations of the ADAM to incorporate other activities of digital forensic practitioners (such as analysis and presentation) in the same format in order to provide a complete formal model of digital forensics.

REFERENCES

Adams, R. (2013). Doctoral Thesis. The Advanced Data Acquisition Model (ADAM): A process model fordigital forensic practice. Murdoch University. Retrieved from http://researchrepository.murdoch.edu.au/14422/2/02Whole.pdf

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.

Baryamureeba, V., & Tushabe, F. (2004). The enhanced digital investigation process model. Paper presented at the Digital Forensic Research Workshop, Baltimore, Maryland, United States.

Beebe, N., & Clark, J. (2004). A hierarchical, objectives-based framework for the digital investigations process. Paper presented at the Digital Forensics Research Workshop 2004, Baltimore, Maryland, United States.

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, Taipei, Taiwan.

Buskirk, E. V., & Liu, V. T. (2006). Digital evidence: Challenging the presumption of reliability. *Journal of Digital Forensic Practice, 1*(1), 19-26. doi: 1080/15567280500541421

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

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

Daubert v Merrell Dow Pharmaceuticals Inc. (1993). 509 US 579

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.

Ieong, R. S. C. (2006). FORZA: Digital forensics investigation framework that incorporate legal issues. *Digital Invetigation, 3*, 29-36.

ISO/IEC. (2012). Guidelines for identification, collection, acquisition, and preservation of digital evidence *CD 27037*: ISO/IEC.

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.), (NIST SP 800-86): U.S. Department of Commerce.

Kessler, G. C. (2010). Doctoral Thesis. 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.

Kohn, M., Eloff, J., & Olivier, M. (2006). Framework for a digital forensic investigation. Paper presented at the Information Security South Africa Conference 2006 from Insight to Foresight, Sandton, South Africa. Presented on 5-7 July.

Kohn, M., Eloff, J. H. P., & Olivier, M. (2008). UML Modelling of Digital Forensic Process Models (DFPMs). Paper presented at the ISSA Innovative Minds Conference, Johannesburg, South Africa. Presented on 7-9 July.

Mann, P. (2004). Cybersecurity: the CTOSE project. *Computer Law & Security Review, 20*(2), 125-126.

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 2002), John Hopkins University.

Palmer, G. (2001). *A Road Map for Digital Forensic Research*. Digital Forensics Research Workshop, Utica, New York.

Peffers, K., Tuunanen, T., Gengler, C., Rossi, M., Hui, W., Virtanen, V., & Bragge, J. (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.

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

Rogers, M. K. (2006). DCSA: Applied Digital Crime Scene Analysis. In Tipton & Krause (Eds.), *Information Security Management Handbook*, 5th ed. New York, NY: Auerbach.

Ruan, C., & Huebner, E. (2009). Formalizing computer forensics process with UML. Paper presented at the UNISCON 2009, Sydney.

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).

Stephenson, P. (2003). A comprehensive approach to digital incident investigation. *Information Security Technical Report, 8*(2), 42-54.

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.

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), 55-59.

Williams, J. (2012). Good practice guide for computer based evidence: Association of chief police officers of England, Wales & Northern Ireland.