**Assessing the applicability of “Advanced Data Acquisition Model (ADAM) in different environments.**

ABSTRACT

With the rise of technology, electronic evidence has become more prevalent in legal proceedings, replacing paper-based evidence Previous models in digital forensics have only been suitable for specific environments, overlooking the needs of investigators in other areas like commerce, incident response and more.

Some courts require rigorous testing to establish the reliability of digital evidence, however, the technical complexity of digital tools required explanations that are easily understood by the normal people. Courts used to adopt methodologies like Daubert test to evaluate the admissibility of digital evidence, but problems come up due to evolving digital forensic process. There have been some efforts to standardize terminology and models are ongoing but limited. Ongoing research is vital to address the rising challenges by cybercrime and change digital forensic practices.

Existing process models for digital data acquisition are critically evaluated from both theoretical and legal perspectives, revealing a notable absence of a generic process description. Advanced Data Acquisition Model (ADAM) is a breakthrough in the practice of digital forensic, this model helps address the need for an adaptable framework to guide the practitioners in digital investigations. Most models overlook the intricacies of digital forensic work outside of law enforcement settings and ADAM fills that void. It distinguishes itself as a versatile solution capable of meeting demands of investigators in different sectors like incidence response.

ADAM has a three-stage process model which provides a structured framework for digital evidence acquisition. Various professionals can confirm this model’s adaptability and reliability across a diverse investigation context.

INTRODUCTION

This essay goes into the assessment of ADAM’s applicability across different environments, building upon the research conducted by Peffers et al 2006(reference this). The background and literature review section goes into the landscape of digital evidence as well as previous process models, identifying important parts such as the design elements, scientific approaches and model requirements. Based on this, the model requirements are defined, laying the way for the design and the development of ADAM, it undergoes refinement based on the components necessary for generic and forensically sound data process. The demonstration phase identifies discrepancies and make the model better as it elucidates the methods used for evaluating ADAM. The evaluation section goes into the external review process, assessing the theoretical validity and usability. Through this approach, this essay explores the efficacy and adaptability of ADAM across different forensic environments.

BACKGROUND AND LITERATURE REVIEW

The evolution of digital evidence has posed challenges to modern legal principles, such as the Evidence Rule, which previously required the production of original documents in court. Differences between hard and soft copy records have emerged, including differences in accessibility, visibility. Also, viewing digital documents can change the original data, complicating the preservation of evidence. The Uniform Evidence Acts in Australia have expanded the definition of documents to include digital storage devices, allowing electronic copies to have the same status as the originals under specific conditions. These conditions tend to include utilizing proven acquisition tools and techniques, verifying data source and making sure data integrity with methods like hash value recording. Some digital forensics practitioners adhere to “forensically sound tasks”, which includes authenticity, chain of custody, reproducibility and minimization, as identified by scholars like Rogers, McKemmish, and Mocas.

Guidelines and standards are crucial in determining the practices of digital forensic investigators across different environments, including commercial and law enforcement. Noblett et al. proposed a hierarchical model for developing guidelines to digital forensic activities. The International Organisation for Standardization and the British Standards Institute are bodies that have developed guidelines for handling digital evidence. Also, some scholars and practitioners have contributed rules and guidelines. These are essential for providing frameworks for conducting investigations, abiding legal and ethical standards as well as ensuring evidence integrity.

Ill be reviewing some digital forensic models. The models fall into three themes ‘ad hoc’, ‘process flow’ and ‘scientific’ approaches.

The Integrated Digital Investigative Process(IDIP), (1), applies concepts from physical crime scene investigation to digital environments, they liken the computer to a doorway leading to a virtual space.

A diagram of a crime scene

Description automatically generated

Baryamureeba and Tushabe's Enhanced Digital Investigation Process Model (EDIPM)(2),The EDIPM streamlines the process into five key phases: Readiness, Deployment, Trace Back, Dynamite, and Review, integrating Carrier and Spafford's definition of the physical crime scene. Unlike the IDIP(1), however, the EDIPM eliminates the Reconstruction phase, resulting in a more concise model.

A diagram of a process

Description automatically generated

Kohn et al. (2006) propose the Framework for a Digital Forensic Investigation (FDFI)(3), which emphasizes understanding the legal landscape and comprises three stages: preparation, investigation, and presentation The Preparation stage includes elements such as organizational standards, policies, training, legal counsel, and documentation of past incidents. For data acquisition, both Preparation and Investigation stages are pertinent, involving activities like evidence searching, collection, transportation to secure environments, and storage.

A diagram of a diagram

Description automatically generated

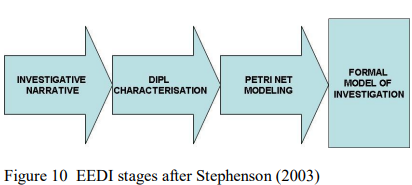
The goal of the Four Step Forensic Process (FSFP)(4),is to make digital forensic investigations more approachable for non-technical staff members in organisations. Four essential processes: Identification, Collection, Examination, and Presentation. The authors advise using this procedure as the basic framework for digital forensic capabilities, even if they acknowledge that legal and regulatory environments differ throughout organisations. For digital data acquisition, the Collection phase—which includes tasks like locating possible data sources, organising the acquisition, carrying it out, and confirming data integrity—is emphasised as being very important. The FSFP, in spite of its simplicity, provides useful advice for businesses looking to improve their digital forensic skills.

A diagram of a process

Description automatically generated

The Extended Model of Cybercrime Investigations was first presented by Ciardhuáin (5) in an effort to fill in apparent gaps in the literature, mainly the absence of a clear identification of information flows. Thirteen tasks make up the model, the first eight of which are devoted to gathering evidence. These tasks, which are all seen as linear but may need repeats, include Awareness, Authorization, Planning, Notification, Search & Identification of Evidence, Collection of Evidence, Transport of Evidence, and Storage of Evidence. Ciardhuáin highlights the significance of a chain of custody and how it helps to preserve the accuracy of digital data. From alerting the investigator to properly storing devices that may contain evidence, the actions related to data collecting cover a range of phases, guaranteeing completeness and accuracy all the way through the inquiry.

Stephenson (6) suggests the End-to-End Digital Investigation (EEDI) paradigm, which is designed for intricate inquiries utilising advanced instruments such as link analysers. The EEDI model consists of general steps, of which only one—called "Collecting Evidence"—relates to data collecting. In order to guarantee the reliability of evidence chains, Stephenson highlights the significance of verifying original evidence and presents the First Rule of End-to-End forensic digital analysis. While DIPL may be useful for assuring comprehensive investigations and providing testimony in court, its actual application and future development are still unknown.



Wang and Yu (7) in their analysis, they suggest adding a Petri net to the digital forensic procedure. Using a Petri net and a narrative, this method entails modelling a portion of the forensic process and focuses on events and circumstances pertinent to the initial onsite phase of gathering digital evidence.

This details above provides an overview of the current understanding of existing models and of acquiring digital data as well as understanding digital forensics. There isn't much agreement on how to define the digital forensic process, but there is increasing agreement that a formal approach is necessary.

METHOD

The evaluation standards for earlier iterations of the digital forensic procedure have two primary elements: conformity to fundamental prerequisites and fulfilment of the Daubert test. According to Carrier and Spafford's paradigm, the fundamental needs are specificity, applicability to all user populations, neutrality of technology, practicality, and a foundation in physical crime scene investigation theory. The degree to which each model satisfies these criteria determines its score. In addition, each model's testability, peer review, error rate, and acceptance within the scientific community are evaluated using the Daubert test, which is frequently used to judge the validity of scientific evidence in legal proceedings. The purpose of this twofold assessment is to shed light on how well-suited the current models are to assist courts in determining the credibility of digital evidence.

There is still no consensus on the number of processes or stages involved in digital forensics, and little agreement on its recognition as a formal scientific discipline.

A white text on a white background

Description automatically generated

When models are compared to the Daubert test, it becomes clear that most of them fall short of the requirements. Only one model passes two of the four tests, while most pass one or none. Peer review is claimed by many models, however there is no testing, no standard for calculating error rates, and no widespread acceptance. This implies that the dependability of digital evidence collecting systems may not be accurately assessed by the Daubert test. The published guidelines for digital forensic practitioners are mostly focused on domains such as law enforcement and incident response, leaving practitioners in other professions with inadequate coverage. To meet the demands of practitioners in many areas, the International Standards Organisation (ISO) is creating guidelines for digital evidence collecting, but at the moment, there is no formal representation or process model for the entire process.

Therefore, identifying essential components is vital for a new model. The models that best represent the fundamental characteristics of a digital forensic process model have been found through study using Carrier and Spafford's criteria. The new model (ADAM) will incorporate elements or a structure from these chosen models. Turnbull's approach also means that ADAM needs to be flexible enough to accommodate new and developing technology. The contributions that were specifically selected to guide the creation of ADAM are described in the following section, and each is incorporated into the model directly.

Some of the key contributions are as mentioned below:

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

Stressing the importance of chain of custody factors   
Taking into account every aspect of digital forensics instead of favouring one group over another   
Encouraging a practical approach that prioritises data collecting and focuses on the crucial areas that other components of the task depend on   
Insisting that a model ought to be independent of both tools and technologies.

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):

Presenting the idea of "information flow"   
Determine the phases of "awareness," "authorization," and "planning." Recognise that there might be involvement from both internal and external authorities.

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

The notion of broadly defined standard stages from earlier forensic procedures Presenting the idea of "digital forensics," which is more comprehensive than "computer forensics."

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

The concept of an ‘umbrella activity’ for documentation.

By combing the key contributions and the reviewed models, the essential elements for data acquisition are summarised and grouped:

- An initial preparation stage that incorporates activities that take place once the practitioner is notified or becomes aware of a potential 124 requirement to undertake some work but prior to them gaining access to the ‘incident scene

- 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)

Based on the three-stage hierarchical model, ADAM needs to:

* Include guiding concepts drawn from the International Standards Organisation, the Association of Chief Police Officers, and other sources.
* Comply with organisational policy and practice, including rules, signing authority, and other specifications.
* Provide methods and approaches that may be adjusted and improved upon when new information becomes available.
* Take into account the important insights from earlier studies.
* The original data should not be changed by the digital forensic practitioner's actions. The impact of the practitioner's activities on the original data should be clearly identified, and the procedure that resulted in any changes should be justified, if the work constraints make this impractical.
* All operations related to the collecting, processing, and storage of the original data, as well as any copies of the original data, must be fully documented. This entails adhering to the relevant evidence regulations, such as keeping a chain of custody record, and verification techniques like hashing.   
    
  The digital forensic specialist is not allowed to engage in any actions that are outside the scope of their training or experience.
* When doing their duties, digital forensic professionals need to consider every facet of personal safety.

The ADAM has three stages for the process of getting digital data. These stages are:

STAGE 1– The initial planning stage

This is where important factors that concern the investigation's paperwork, logistics, and other related matters are decided. Depending on the kind and scope of the investigation being conducted, this can entail a clandestine survey, which is occasionally done by private investigators. This step could be as short as reviewing documentation in some cases, such as when law enforcement officials have already confiscated devices and brought them to digital forensic experts for review.

STAGE 2– The onsite survey

The primary acquisition plan is developed once all the information gaps regarding the location, dimensions, and format of the devices storing the digital data are filled in. In certain cases, such as with previously acquired devices as previously noted, this stage might not matter.

STAGE 3 – The acquisition of digital data

This will include the replication and storage of the acquired data

A diagram of a work flow

Description automatically generated

Reference: Adams, R., Hobbs, V., & Mann, G. (Year). The Advanced Data Acquisition Model (2012): A Process Model for Digital Forensic Practice.

Evaluation:

Three high-level factors are typically the focus of evaluating a process model:

-Is the theoretical model valid?

-Can you use the model?

-Does the model give the user to explain the user the ability to explain?

A process model's efficacy is contingent upon its conformity to the guiding principles that provide structure to the process. When people can organise and sequence their actions using a model in real-world settings, making it easier and more efficient to attain desired results, that model is deemed useable.

Some of the experts who reviewed this case were the following:

1. A law enforcement representative leading a State Police Computer Crime Squad.

2. Another law enforcement representative serving as a Digital Forensics Examiner at a government ministry, holding certifications as a Computer Information Systems Security Professional (CISSP) and Information Systems Auditor (CISA).

3. A commercial practice representative who is a committee member of the High Technology Crime Investigators Association.

4. Another commercial practice representative serving as the National Director of computer forensics for a professional services company, with extensive experience instructing law enforcement agencies globally, including Scotland Yard, Hong Kong Police, and the FBI's Regional Computer Forensics Labs.

5. An incident response representative with 15 years of IT experience, holding certifications as a Computer Information Systems Security Professional (CISSP) and Information Systems Auditor (CISA), and having served as a Technical Trainer at the 2007 Malaysia Forum of Incident Response and Security Teams Technical Colloquia.

The main key messages from them were:

Stage 3 - Include time restrictions on acquisitions

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

Stage 3 - Transportation requirements if devices are to be taken off-site

Stage 3 - Include plans for Client/Team updates or project status

Stage 3 - Needs to be some explicit sense of protecting any legal rights, and of keeping objectivity in the exam.

Ensuring that the ADAM records all action made by practitioners in the three target areas of law enforcement, incident response, and commerce was the usefulness requirement of the external evaluation. None of the ADAM's steps were found to be inconsistent with the procedures used by experts or practitioners in their experiences or surroundings. Feedback was received on multiple occasions, offering suggestions for improvements or additions to the ADAM.

There are some positives to the model such as:

-Reasonably easy to use and adapt

-It would be easy to incorporate for use

-Very straight forward, and fewer cross-over feedback loops, therefore good process management

CONCLUSION

In this essay we looked into how ADAM was used to collect digital data for forensics that can be used in incident response, law enforcement and commercial environment. We assessed previous models for key features and requirements needed for ADAM. We reviewed ADAM, with some of its pros, and cons, and how to better use it in its intended environment.

Therefore, ADAM must satisfy the following, model must be relevant in the fields of commercial, incident response and law enforcement. After a thorough analysis of the most recent research in the field, the characteristics of existing models were synthesised in a generic manner to fulfil the need for the model to be relevant. Proficient practitioners with experience in law enforcement, trade, and incident response have assessed the model's applicability.

However, a limited number of instances were included in the internal assessment of the model, which functioned as a test run for its composition and organisation prior to an outside examination. Despite representing several areas of digital forensic practice, the external reviewers were a small sample size in relation to the entire practitioner population. The model was improved by taking into account reviewers' comments, which included those from the authors of earlier models.

REFERENCES

1) Carrier, M., & Spafford, E. (2003). Integrated Digital Investigative Process (IDIP). Digital Forensic Research Workshop.

2) Baryamureeba, V., & Tushabe, F. (2004). Enhanced Digital Investigation Process Model (EDIPM).

3) Kohn, M., Jayakar, K., & Eloff, J. H. P. (2006). Framework for a Digital Forensic Investigation. In R. Choo (Ed.), Handbook of Information Security (Vol. 3, pp. 203-218). Springer.

4) Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). The Four Step Forensic Process (FSFP). In Proceedings of the Sixth Annual IEEE SMC Information Assurance Workshop (pp. 21-27).

5) Ciardhuáin, M. (2004). Extended Model of Cybercrime Investigations.

6) Stephenson, T. (2003a). End-to-End Digital Investigation (EEDI) process.

7) Wang, H., & Yu, T. (2007). Modeling Computer Forensic Process from a Workflow Perspective. In 2007 IEEE International Conference on Granular Computing (pp. 53-58). IEEE.