Review and Assessment of the Existing Digital Forensic Investigation Process Models

Reza Montasari
University of Derby
Kedleston Road, Derby
DE22 1GB, U.K.

ABSTRACT

This review paper assesses the existing body of knowledge associated with digital forensic investigation process models. To this end, eleven of the existing models are critically reviewed and evaluated against an assessment criteria, namely the Daubert Test, to determine which models have taken the most scientific approach. This review and assessment reveal that the authors of these models have developed their models based on their own personal experience and on an ad-hoc basis. The critical review and assessment also reveal that there does not exist a comprehensive model encompassing the entire digital investigative process that is formal in that it synthesizes, harmonizes and extends the previous models, and that is generic in that it can be applied in the different fields of law enforcement, commerce and incident response.

Keywords

Digital investigation, Process Models, Daubert Test, Digital Forensics

1. INTRODUCTION

Digital forensics has grown in importance in situations where digital devices are used in the commission of a crime [1]. The original focus of digital forensic investigations was on crimes committed through computers [2]. However, over the past few years, the field has extended to include various other digital devices in which digitally stored information can be processed and used for different types of crimes [3]. A digital forensic investigation, hereafter referred to as DFI, is the process of linking extracted information and digital evidence in order to establish factual information for review by the judiciary [2], [4]. Cohen [5] highlights the need to establish factual information as the outcome of such an investigation. A DFI is carried out as an investigation after the occurrence of an incident [6, 7]. It is therefore a distinct type of investigation "where the scientific procedures and techniques used will allow the results, in other words digital evidence, to be admissible in a court of law [8]. Due to the fact that digital evidence is contained in a digital device and cannot be observed by the naked eye, forensic tools such as Encase and FTK are used to extract and examine data representing potential digital evidence. The extent of the value of digital evidence is based not only on the extent to which a tool is trusted [9, 10], but also on the competence and experience of the investigator carrying out the digital investigation [11, 12]. There are four basic principles of DFIs which must be considered. These are auditability, repeatability, reproducibility and justifiability. Auditability refers to the need for an independent investigator to be able to evaluate the activities performed by other investigators to determine whether or not a suitable scientific method was followed [13]. Repeatability requires one investigator to be able to arrive at the same conclusion as another under similar conditions [14, 15]. Reproducibility is established when the same test results are produced using the same method, but with different instruments and under different conditions, and can be reproduced at any time after the original test [11]. Justifiability refers to an investigator being able to justify all the actions and methods they used during the course of a digital investigation [11].

A DFI is often initiated in order to ascertain certain facts after an incident has occurred. It must be conducted in such a methodical manner that it can withstand scrutiny by the court and defence team [2]. There exist various types of DFIs, including live forensics, static forensics, proactive forensics and cloud forensics [16, 17]. The fundamental point of any DFI is to answer 'what', 'why', 'how', 'who', 'where' and 'when' type questions in relation to the data analysis and evidence in order to confirm or refute allegations of suspicious activity [4], [18]. 'What' refers to the data attributes or metadata, 'why,' the motivation [19], 'how,' the manner in which the incident was initiated or the way in which the necessary evidence was isolated [17], 'who,' the people involved [20], 'where,' the location of the potential digital evidence [2] and 'when' the time of occurrence [21]. This review paper focuses only on the question of "how". Kohn et al. [22] state that the "how" question is addressed by the steps of the investigative process undertaken which have to be defined. Several authors have defined these steps in a digital forensic investigation process model, hereafter referred to as DFPM, which is the main subject of this paper. Due to the fact that there exist a large number of process models, it would be impossible to provide a detailed review of all these models in one single paper. Therefore, only 11 models will be selected and reviewed. The remainder of the paper is structured as follows: Section 2 discusses the methodology. Section 3 presents a detailed review and assessment of the existing DFIPMs, while Section 4 presents the analysis of the models' assessments. The paper is finally concluded in Section 5.

2. METHODOLOGY

In order to determine which existing DFIPMs have taken the most scientific approach, the five-point requirement set by the Daubert Test has been used in this paper as a framework against which the existing models are judged. The idea of assessing the existing DFIPMs against the Daubert Test was originally devised by Adams [23]. To assess the existing DFIPMs in this paper, this test has been selected based on the fact that it is commonly-referenced criteria to judge the reliability of scientific evidence by many courts [2], [14] and [24]. The Daubert Test is currently utilised in the federal courts and some states courts in the United States. It replaced the Frye standard in the federal courts. In the United States, the admission in a federal court of scientific evidence (including digital evidence) is governed by the Federal Rules of Evidence (FRE) [25, 26]. Across the U.S. federal courts, judges employ the Daubert Test [27] in order to determine the admissibility of digital evidence as well as any other types of scientific and technical evidence [23], [28, 29, 30]. Courts make an initial assessment of whether an expert's scientific testimony is based on reasoning or methodology which is scientifically valid and can properly be applied to the facts [31]. A trial judge is required to act as a gatekeeper, determining, prior to its admission, whether the evidence is scientifically valid and relevant to the case [28]. Using the Daubert Test, a judge can objectively determine the reliability of any digital evidence presented in the courts. Using this test, the criteria that must be taken into consideration in establishing whether the methodology is valid include the following "5" requirements:

1. whether the theory or technique in question can be and has been tested;
2. whether it has been subjected to peer review and publication;
3. its known or potential error rate;
4. the existence and maintenance of standards controlling its operation; and
5. whether it has attracted widespread acceptance within the relevant scientific community.

Therefore, to assess each existing model against the Daubert Test five-point requirement, each model will be given a score out of "5" on the basis of how many of the five requirements have been achieved. The idea of score-based assessment was originally created by Adams [23]. Applying the Daubert Test to the existing DFIPMs can indicate how appropriate, or otherwise, the Daubert Test criteria are for assisting courts in judging the reliability of digital investigative process followed using a DFIPM. It will ultimately depend on a court making its own conclusion in relation to how a specific model scores under the Daubert Test. The score-based approach used in this paper to assess the DFIPMs is adopted on the basis that there are no other studies from which assessment data for previous models could be extracted [23]. However, as [23] states, such an approach should not be considered as a conclusive assessment. Instead, the score-based assessment employed is used to score the previous models in order to determine (as closely as possible) how many of the requirements of the criteria have been fulfilled by a given model.

3. ASSESSMENT OF MODELS

3.1 Reith et al's ADFM

Reith et al. [32] identified the common components from the previous models and incorporated those common components into their abstract process model, ADFM. Reith et al's model is mainly based upon the initial model of Palmer [33]; however, it adds a description for each phase. This model is based on nine components as follows: Identification, Preparation, Approach Strategy, Preservation, Collection, Examination, Analysis, Presentation and Return Evidence. Although the ADFM provides a general framework that can be applied to a range of incidents, it has various shortcomings, some of which are identified by the authors themselves. Referring to Reith et al's [32] paper, Adams [23] outlines three disadvantages of applying the ADFM as follows:

- Its high-level approach to categorization may be too general to be applied in practice.
- There is no easy or obvious method to test the model.
- Each sub-category added to the model will make it more cumbersome to use. In other words, as the model is expanded to increase its granularity, it becomes more complex and more cumbersome to use [23].

This model has also been criticized by Carrier and Spafford [20], who argue that the names of the Examination and Analysis Phases included in this model can be confusing because their meaning is only slightly different, and it is common to have two investigators who are referring to the same tasks when they say that they are "analyzing a system" or "examining a system". This criticism seems to be invalid as the Examination and Analysis have different aims and therefore should be assigned two separate phases. Examination Phase should involve activities regarding the extraction of potential digital evidence from the acquired data [22], [34, 35], whereas the Analysis Phase should involve activities related to the methodical analysis of the digital evidence as well as the construction of the incident [2], [34, 35]. Other drawbacks of the model include missing steps in the process or the lack of a graphical representation. For example, the model could include a Forensic Readiness phase as emphasized by the authors in [7], [14], [36] before the Identification Phase to ensure that both infrastructure readiness and operational readiness are in place prior to a possible incident or security breach. Ciardhuáin [10] criticizes the Reith et al's [32] model for its lack of the explicit mentioning of the "Chain of Custody" stating, "… Reith et al. (2002) themselves have noted the absence of any explicit mention of the chain of custody in their model. This is a major flaw when one considers the different laws, practices, languages, and so on which must be correctly dealt with in real investigations."

Other authors such as those in [37, 38, 39] as cited by Adams [23] adopt the same criticism of the AFPM for its lack of the explicit inclusion of the "Chain of Custody". In their model, Reith et al. [32] have taken the view that this Principle is to be applied automatically stating, "this model assumes that a strong chain of custody will be maintained throughout the duration of the investigation." However, in accordance with the ACPO Good Practice Guide for Digital Evidence [12], ISO/IEC 27043 [13] and other researchers including those in [14], [23], [35, 36], this important investigative Principle must be explicitly covered in a DFIPM. According to the Daubert Test, the ADFM meets only Requirement 2 as the model has been subjected to peer review and publication. However, as Reith et al. themselves admit, the ADFM has not been tested (Requirement 1); therefore, its potential error rate is unknown (Requirement 3). There is also no evidence suggesting that the model is based on a standard (Requirement 4), nor does there exist evidence of the model having been widely accepted within the digital forensic community (Requirement 5). The Daubert Test score given to the AFPM is 1/5.

3.2 Carrier and Spafford's IDIP

The Integrated Digital Investigative Process (IDIP) developed by Carrier and Spafford [20] has seventeen phases organized into five groups as illustrated in Figure 1. This model applies physical crime scene processes into the digital crime scene with the computer being treated as a "door to another room". In order to describe the differences and similarities between a physical and digital crime scene, Carrier and Spafford define the physical crime scene as "an 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. The digital crime scene is also defined as "the virtual environment created by software and hardware where digital evidence of a crime or incident exists". The IDIP represents the "Deployment" Phase as being independent of the physical and digital investigation. In practice, it appears impossible to confirm a digital crime unless some initial physical and digital investigation is conducted. The IDIP has come under certain criticisms by some authors. Baryamureeba and Tushabe [40] have criticized the IDIP for not offering "sufficient specificity", stating that the model has not made a clear distinction between investigations at the victim's scene (secondary crime) and those at the suspect's scene (primary crime). However, this criticism is also invalid as the approach for acquiring digital evidence is essentially the same as that employed in terms of acquiring traditional evidence [32] [41].

Baryamureeba and Tushabe [40] ultimately question the practicality of the model by drawing an analogy to illustrate the problem associated with this model. According to the analogy, the primary crime scene is where the crime is initiated; the target of the malicious activity is the victim's location which is the secondary crime investigation. The physical and digital investigation processes of Carrier and Spafford's model do not include the secondary crime scene. The fact that the malicious activity is not included in the physical or digital investigation can have a negative effect on the possible reconstruction of a sequence of events. Therefore, according to Kohn et al. [22], this can lead to incomplete findings in the report presented to the relevant audience.

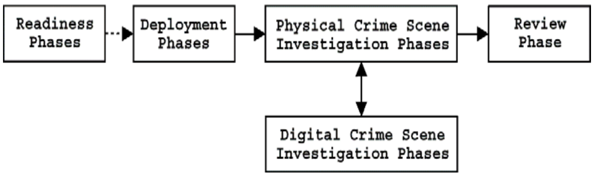
Readiness Phases
Deployment Phases
Physical Crime Scene Investigation Phases
Review Phase
Digital Crime Scene Investigation Phases

Figure 1: The IDIP after Carrier and Spafford (2003)

Rogers et al. [16] have also criticized the IDIP stating that despite the fact that this model might be appropriate for investigations where the entire investigative process needs to be followed, the time limitations of certain investigations such as child abduction makes the model infeasible. However, this criticism appears to be invalid as courts require investigators to conduct digital investigations using a methodical process in order that courts can assess the reliability of digital evidence presented to them. Therefore, the notion of swift data examination and analysis suggested by Rogers et al. [16] in itself is very likely to attract serious challenges by courts, a point raised by Adams [23]. Although some criticisms have been levied upon the IDIP, many researchers [2] [14] [22, 23] [42] have adopted many of the ideas introduced by the model, especially the concept of "digital crime scene". The major and novel contribution of the IDIP is the introduction of the concept of interaction with "physical investigation". Another main benefit of the model is that it has demonstrated well the investigative process, such as Data Collection, Interrogation, Analysis and Reporting. For example, the authors in [37] [43] as cited by Adams [23] approve of Carrier and Spafford's approach by drawing a fundamental similarity between the physical and digital crime scene domains. Furthermore, despite the fact that the IDIP might have some flaws, its inclusion of the physical crime scene is a notable contribution. Making a distinction between a physical and digital crime scene might appear to be trivial; however, dividing physical and digital crime scenes are essential for the practical execution of an investigation.

In relation to the Daubert Test, the IDIP has met Requirements 2 and 5. Although the model has been applied to case studies, it has not been tested by its intended user community (Requirement 1); therefore, its potential error rate is not known (Requirement 3). There is also no evidence of any standard associated with this model (Requirement 4). However, the model has been peer-reviewed and published (Requirement 2), and widely accepted and referenced in the digital forensic community (Requirement 5). The Daubert Test score given to the IDIP is 2/5.

3.3 Ciardhuáin's EMCI

An Extended Model of Cybercrime Investigation (EMCI) proposed by Ciardhuáin [10] is the most comprehensive DFIPM presented to date. Ciardhuáin [10] merges the previously proposed models and extends them by addressing certain activities not incorporated into the previous models. Ciardhuáin's proposed model includes thirteen activities, as shown in Figure 2 in order to model the whole "Information Flow" pertaining to a digital forensic investigation. flow pertaining to a digital forensic investigation.

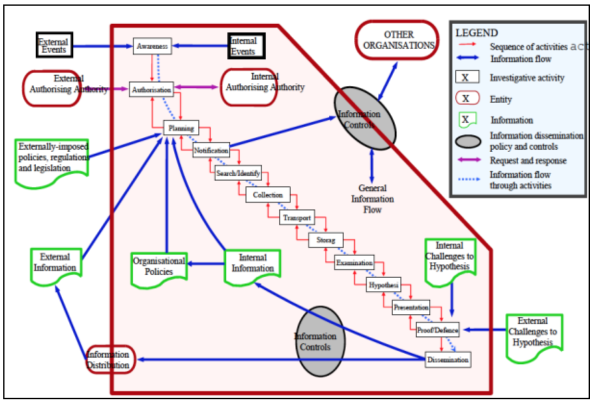

Figure 2: The EMCI after Ciardhuáin (2004)

The EMCI has a linear representation, where the Processes follow the waterfall model allowing the investigators to backtrack to certain Processes if needed. Ciardhuáin takes issue with certain previous models, such as Reith et al's [32] model, and their lack of explicit mentioning of "Chain of Custody". He considers the Chain of Custody as an instance of Information Flow and argues that the Chain of Custody should be created by those who have handled a piece of evidence and must pass it from one stage to the next, with names added at each step. The main contribution of the EMCI is the fact that the model explicitly captures the "Information Flows" in an investigation (from the moment incident is detected until the investigation is concluded.) as opposed to only the processing of evidence. One of the weaknesses of this model is the fact that it has excluded certain important steps such as the return or destruction of digital evidence at the end of investigation. Another shortcoming of this model lies in the fact that the terminology used to describe each activity is not clearly defined [2]. For instance, it is ambiguous whether Ciardhuáin (2004) discounts the "Preservation" step since it is not regarded necessary, or because it is considered as part of the "Acquisition" Process. Casey (2011) has also criticised this model for not defining goals (an important requirement) within each step in an investigation. Thus, various users of the model might take different approaches at each stage of a digital investigation, possibly infringing on important forensic principles.

Concerning the Daubert Test, the EMCI meets the first three requirements. The model has been tested by DFIs operating within the law enforcement. However, as the author himself identifies the need, the EMCI will also need to be tested in other environments that the model has claimed to cover such as auditing, civil litigation, investigations by system administrators and judicial inquiries. The EMCI has been subjected to peer-review and publication (Requirement 2) and its potential error rate appears to be known due to the model having been tested by experts (Requirement 3). The EMCI does not, however, appear to have been widely accepted within the digital forensic field as it has not been further developed since its creation (Requirement 4). There does not also appear to be any evidence suggesting that the model has adhered to a particular standard (Requirement 5). The Daubert Test given to the EMCI is 3/5.

3.4 Beebe and Clark HOBFDIP

Beebe and Clark [17] state that previous models lack the detail required to be of practical use; hence they proposed their model to focus on the lower-level activities of a digital investigation as opposed to abstract concepts. This model consists of six Phases as illustrated in Figure 3.

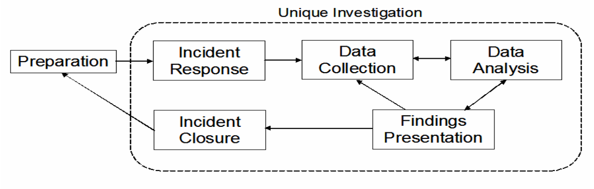

Figure 3: The HOBFDIP after Beebe and Clark (2005)

At a first glance, it appears that this model has not built upon the previous models due to its common Phases. However, upon a closer inspection of Beebe and Clark's paper, it becomes clear that Beebe and Clark have provided lower-level details for the Analysis Phase even though the details are not incorporated into the graphical representation of the model. Beebe and Clark's model consists of Phases, Principles and Objectives. Phases are sequential, time-based and distinct in the process, whereas Principles are high-level procedures that apply to more than one Phase while Objectives are the intended outcomes. There are various shortcomings associated with Beebe and Clark's [17] "Hierarchical, Objectives Based Framework for the Digital Investigation Process" as identified by the authors themselves. These include:

- Its proposed set of Objectives is incomplete.
- The model needs to be expanded upon so that it can also be applied across various layers of abstraction as well as to various types of digital devices.

Other shortcomings of the HOBFDIP include the fact that its lower-level details are only restricted to an initial Sub-Phase structure for the Data Analysis Process. No additional layers of detail have been provided for other Processes in the model. Also, the model is not generic as it is biased towards 'network forensics'. It has incorporated Phases that are often used in the context of incident response such as 'network monitoring'. Moreover, although the model has been applied to two different case studies as part of its evaluation, no independent testing of the model has been carried out by its intended user community. The notable contribution of this model is the concept of a "multi-tiered" approach, as opposed to the "single-layer" approach identified in the previous models. Another contribution of this model is the introduction of "Principles" that should be applied throughout the investigative process such as "Information Flow", "Documentation" and "Evidence Preservation" even though these Principles had been previously covered in [10], [20, 21], [32, 33], [44].

In terms of the Daubert Test, the HOBFDIP does not meet Requirement 1 as there is no evidence suggesting that it has been tested by its intended user community, nor is the model's potential error rate known as it has not been tested independently. Also, there is no evidence of the model being associated with any standard or recognised guidelines. However, the HOBFDIP appears to have been accepted within the digital forensic community as it is widely referenced. The Daubert Test score for the HOBFDIP is 2/5 as it has partially met Requirements 1 and 4.

3.5 Kent et al's FSFP

Kent et al. [45] created a guideline, the aim of which is to enable the organisations to develop their own digital forensic capability through IT professionals for security incident response. Although the authors state that each organisation should employ the most suitable model based on their own requirements, they go on to propose a high-level model, namely "Four Step Forensic Process", consisting of four stages including: Collection, Examination, Analysis and Reporting. Kent et al. [45] consider the four steps as common stages of investigative process that have been derived from the previous models stating that the only difference is the level of details provided for each stage. Figure 4 is the graphical representation of this model.

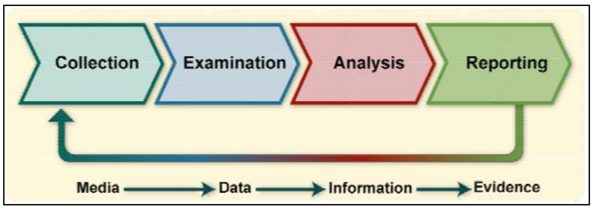

Figure 4: The FSFP after Kent et al. (2006)

Although the FSFP is simple compared to other models, it has provided a large amount of background details to enable the organisations to build a general ability in relation to training, procedures and resources. The model also provides some useful details in terms of the standard forensic procedures that could help the organisations to develop their incident response abilities. However, the FSFP is also missing important phases including Interpretation, Event Reconstruction, Presentation and Investigation Closure, which are required as part of a complete investigative process. Also, the activities specified for each stage are not explicitly represented in the graphical representation of the model but discussed in the text. This significantly reduces the practicality of the model as DFIs would have no visual sighting of the activities that are not presented in the model if they were to adopt it. Moreover, this is in opposition to the complex process simplification requirement proposed by Beebe and Clark [17] which requires the model to be detailed to assist the investigators when undertaking investigations. The absence of a clear structure as well as the lack of important activities in relation to both 'pre-data' and 'post-data' acquisition significantly reduce the practicality of the model.

In terms of the Daubert Test, the FSFP has not met any of the requirements as the model has not been tested by experts in the field, nor has it been subjected to scientific peer- review or publication. Its potential error rate is also unknown as no testing has been carried out on the model, and there is no evidence suggesting that the model has been influenced by any standard. The model has not also been widely accepted in the digital forensic community. The Daubert Test score given to this model is 0/5.

3.6 Rogers et al's CFFTPM

Computer Forensics Field Triage Process Model (CFFTPM) proposed by Rogers et al. [16] includes six phases including: Planning, Triage, User Usage Profiles, Chronology Timeline, Internet and Case Specific. The CFFTPM's focus is to enable investigators to carry out 'onsite triage' to examine and analyse digital devices within hours as opposed to weeks or months. Rogers et al. [16] state that the model's procedures used onsite are forensically sound and maintain the chain of custody. However, there is no explicit graphical representation of this important principle, nor is there any description of how the chain of custody should be maintained by investigators. This model is only appropriate for circumstances where a swift examination would need to be conducted at the crime scene. It should only be used where appropriate and only after carefully weighing the legal and technical considerations associated with digital investigations. The novel contribution of the CFFTPM is that it has moved away from the traditional digital forensic approach of seizing a digital device, transporting it to the lab, making a forensic image, and then searching the entire system for potential evidence.

With regards to the Daubert Test, the CFFTPM meets all the criteria with the exception of requirement 5. The model has been tested by various State and Local Law Enforcement Officers from Southern Indiana, U.S. (Requirement 1). The model has also been subjected to peer review and publication (Requirement 2). Moreover, the CFFTPM's error rates appear to have been identified (Requirement 3) since the model has been used in some real-world cases, and the evidence acquired from these cases has not been challenged in the court proceedings where it has been introduced. The CFFTPM has also been associated with some standards as it has complied with the U.S. Federal and State rules for the admissibility of evidence (Requirement 4). However, there is no evidence that this model has been widely accepted by the digital forensic community; thus, it does not meet Requirement 5. The Daubert Test Score given to the CFTTPM is 4/5.

3.7 Freiling and Schwittay's CPMIRCF

Freiling and Schwittay [6] proposed "A Common Process Model for Incident Response and Computer Forensics (CPMIRCF)", as shown in Figure 5, in which the authors make a distinction between digital forensics and incident response, consistent with the view expressed by Mandia et al. [21]. Freiling and Schwittay argue that incident response should focus on the activities of organisations who have been subjected to security breaches with the main aim of quick detection, containment and recovery. In contrast, digital forensics should be utilised to deal with acquiring, analysing and presenting digital evidence by using proven techniques and principles. The CPMIRCF consists of three main phases including: Pre-Analysis, Analysis and Post-Analysis. This model has introduced a new component, Live Response, which is not explicitly mentioned in many of the previous process models. The Live Response element is concerned with collecting information about an incident on hosts that are still running i.e. live.

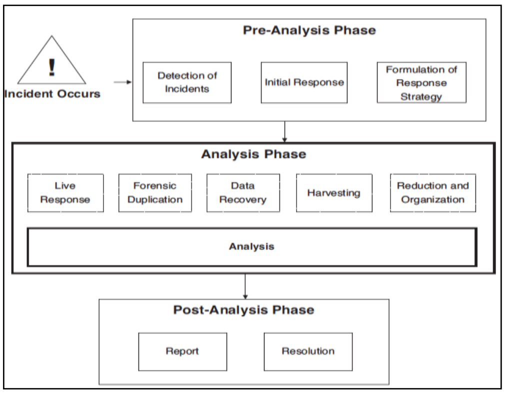

Figure 5: The CPMIRCF after Freiling and Schwittay (2007)

The main drawback of this model pertains to the terminology, and the descriptions of the model's components which are in contrast with other previous models. For instance, the term Analysis is often used by the authors of DFPMs to describe the process of analysing digital evidence after it has been acquired and examined [2] [32, 33]. For instance, referring to authors in [33, 34], Adams [23] state that the term Analysis is often used by these authors to describe the process of analysing digital evidence after it has been acquired and examined. However, Freiling and Schwittay consider this stage to cover all the activities between the initial incident and the preparation of a report Adams [23]. Adams. [23] has criticised this model for the fact that the descriptions of its Sub-Phases do not correspond with the stated intention of Freiling and Schwittay to produce a generic model applicable to both incident response and digital forensic Processes. For example, Adams [23] takes issue with the Incident Detection of this model by stating that the description of this Sub-Phase "... is all about intrusion detection and other aspects of incident response". They further argue that many of the tasks listed within the Initial Response Sub-Phase of the model do not have a generic equivalent, e.g. Network Monitoring, Removing Compromised Hosts and Initialising Packet Filtering. In relation to the Daubert Test, the model has only met Requirement 2 as it has been peer-reviewed and published. However, the model has not been tested; thus, its potential error rate is not known. There is also no evidence of any standard associated with the model or no evidence suggesting that the model is widely accepted in the digital forensic community. The Dauber Test score given to the CPMIRCF is 1/5.

3.8 Khatir et al's TDERAPM

Claiming that their model would present a detailed approach, Khatir et al. [46] proposed an iterative process model, namely the Two-Dimensional Evidence Reliability Amplification Process Model (TDERAPM), consisting of sixteen Sub-Phases grouped into five Phases. The TDERAPM also has four tasks that are "Umbrella Activities" relevant across all the Phases of the model. Figure 5 below graphically represents Khatir et al's [46] TDERAPM. From the graphical representation of this model, it appears that the coloured horizontal lines represent the importance and value of each Umbrella Activity within a particular phase [23]. However, Khatir et al. [46] have not provided any information concerning how they have evaluated these measurements or how the units have been assessed, a point originally raised by Adams [23]. The authors have not also provided information on how their four Umbrella Activities should be maintained [23]. For example, according to the authors, the

Preservation/Authenticity Umbrella Activity is intended to enable the forensic team to follow "...disciplined and fully documented steps". However, no information has been provided concerning what this means and how this is to be achieved in practice, an issue also stated by Adams [23].

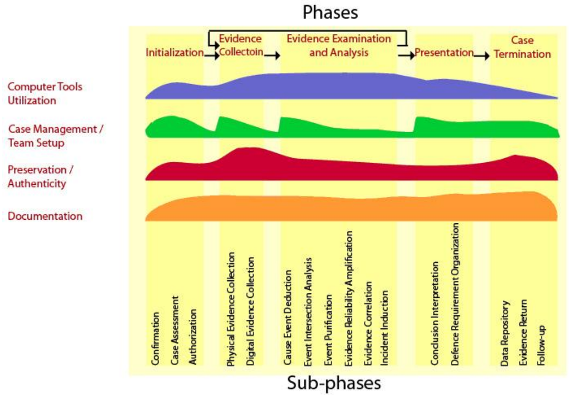
Phases
Initialization
Evidence Collectoin
Evidence Examination and Analysis
Presentation
Case Termination
Computer Tools Utilization
Case Management / Team Setup
Preservation / Authenticity
Documentation
Confirmation
Case Assessment
Authorization
Physical Evidence Collection
Digital Evidence Collection
Cause Event Deduction
Event Intersection Analysis
Event Purification
Evidence Reliability Amplification
Evidence Correlation
Incident Induction
Conclusion Interpretation
Defence Requirement Organization
Data Repository
Evidence Return
Follow-up
Sub-phases

Figure 6: The TDERAPM after Khatir et al. (2008)

The main contribution of this paper is the theoretical concept of 'management issues' introduced as an "umbrella activity" and 'Case Management/Team Setup', as opposed to practical process issues. Using the Daubert Test, the TDERAPM meets only Requirement 2 as it has been peer reviewed and published. The model has not been tested (Requirement 1); therefore, its potential error rate is unknown (Requirement 3). Furthermore, there are no standards referenced by or associated with the TDERAPM (Requirement 4), nor is there any evidence suggesting that the model has been widely accepted by the digital forensic community (Requirement 5). The Daubert Test given to this model is 1/5.

3.9 Selamat et al's MPDFIF

Selamat et al. [39] claimed that they had identified common Phases in the previous models and had mapped them to a "more concise model" to produce a map of digital forensic investigations framework. Five Phases are identified in this model, Mapping Process of Digital Forensic Investigation Framework, including: Preparation, Collection and Preservation, Examination and Analysis, Presentation and Reporting and Disseminating the Case. Selamat et al. [39] claim that their model can be used as a "general digital forensic investigation model for investigating all incident cases without tampering the evidence and protecting the chain of custody". However, the model does not appear to be applicable to the different fields of digital forensics. For instance, it does not include a Forensic Readiness stage as required by ISO/IEC 27043 [13] to ensure that both infrastructure readiness and operational readiness are in place prior to a possible incident or security breach [7], [14], [34]. Also, important Phases relevant to the Incident Response such as pre-incident preparation requirements from the "A Common Process Model for Incident Response and Computer Forensics" of Freiling and Schwittay [6] are missing even though Selamat et al. [39] claim that their model is based on the integration of the previous models. The MPDFIF also lacks a graphical representation to assist the investigators in conducting digital investigations. Using the Daubert Test, the MPDFIF only meets Requirement 1 as it has been peer-reviewed and published. The model has not been tested (Requirement 1); therefore, its potential error rate is not known (Requirement 3). There is also no standard referenced by this model (Requirement 4), nor is there any evidence showing that the model has been widely accepted in the digital forensic community (Requirement 5). The Daubert Test score given to the MPDFIF is 1/5.

3.10 Agarwal et al's SDFIM

Agarwal et al. [8] proposed their Systematic Digital Forensic Investigation Model (SDFIM) claiming that this model addresses some of the shortcomings of the previous methodologies. The SDFIM is based on the model developed by Palmer [33] and consists of eleven Phases as shown in the graphical representation of this model in Figure 7 below.

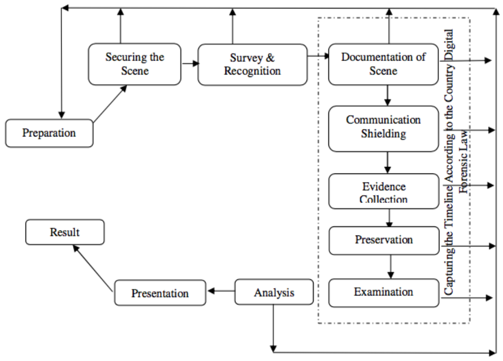

Figure 7: The SDFIM after Agarwal et al. (2011)

Adams [23] criticises Aggarwal et al.'s [8] model for not being consistent in terms of their criteria for the categorisation of the model's Phases. Many of the SDFIM's Phases could have been grouped into one single Phase [23]. Furthermore, vital stages of the investigative process have not been included in the model including: Incident Detection, First Response, Intelligence Gathering, Planning, Interpretation, Event Reconstruction and Reporting. Also, missing in the model is the 'Investigation Closure' stage, where activities associated with the management of evidence are performed such as its return to the rightful owner, its storage, destruction, or cleansing and reuse, where the dissemination of the investigation is communicated to the relevant stakeholders, and where the results are recorded for the future reference. Based on the Daubert Test, the SDFIM only meets Requirement 2 as it has been subjected to peer review and publication. However, the model has not been tested by its intended user community (Requirement 1); therefore, its potential error rate is unknown (Requirement 3). Also, there is no standard pertaining to this model. Although Aggarwal et al. [8] have made a brief reference to the guidelines outlined in the National Institute of Justice, they have not drawn upon any of those guidelines (Requirement 4). Also, there is no evidence suggesting that the SDFIM has been widely accepted in the digital forensic community (Requirement 5). The Daubert Test score given to this model is 1/5.

3.11 Kohn et al's IDFPM

Kohn et al. [22] proposed a Process Flow Diagram consisting of thirty six Sub- Processes grouped into five Processes, namely Preparation, Incident, Incident Response, Digital Forensic Investigation and Presentation. The components of this model have been extracted from the previous models, hence the name Integrated Digital Forensic Process Model (IDFPM). The IDFPM lacks lower-level components as suggested by Beebe and Clark [17]. Although Kohn et al. [22] have made an attempt to model the whole investigative process, the model still has high-order processes without sufficient level of details. However, unlike the authors of many of the previous models, Kohn et al. [22] have distinguished between an investigative Principle and a

Process. For instance, the authors have incorporated Documentation as a Principle, which needs to be maintained throughout the other processes in the IDFPM. Although this is a commendable approach, at the same time other important investigative Principles have not been introduced into the model. These include: Preservation of Evidences, Maintaining Chain of Custody, Maintaining Information Flow, Addressing Safety Issues and Maintaining an Accurate Case Management. The field of forensics in which this model can be applied is not also clear. From the descriptions provided in their paper, it appears that the IDFPM's focus is on the field of incident response. If the model's intended usage were aimed at the law enforcement environment, then it would need additional Processes such as Securing and Evaluating the Crime Scene based on the ACPO [12] and the approach taken by the authors in [47]. However, as it stands, the IDFPM does not provide details for such a Process. In terms of the Daubert Test, the IDFPM only meets Requirement 2 as the model has been peer reviewed and published. However, it has not been tested by the experts in the field (Requirement 1); therefore, its potential error rate is unknown (Requirement 3). There is also no standard associated with the IDFPM (Requirement 4). Also, there is no evidence suggesting that the IDFPM has been widely accepted in the field of digital forensic community (Requirement 5). The Daubert Test score given to this model is 1/5.

4. ANALYSIS OF THE ASSESSMENT

As shown in Table 1, assessing the existing models against the Daubert Test criteria reveals that there are two models that meet four and three out of the five criteria respectively, while there are two models that fulfil two criteria. There are also six models that meet only one criteria, and there is one model that has not achieved any of the criteria.

Table 1. Scores obtained by the previous models based on the three assessment criteria

Models	Daubert Test Score
Reith et al's ADFM	1
Carrier and Spafford's IDIP	2
Ciardhuáin's EMCI	3
Beebe and Clark's HOBFDIP	2
Kent et al's FSFP	0
Rogers et al's CFFTPM	4
Freiling and Schwittay's CPMIRCF	1
Khatir et al's TDERAPM	1
Selamat et al's MPDFIF	1
Agarwal et al's SDFIM	1
Kohn et al's IDFPM	1

From this assessment, it can be deduced that only two authors, namely Ciardhuáin [10] and Rogers et al. [16] have taken the most scientific approach to develop their models. This assessment reveals a lack of scientific consensus in relation to these models which do not conform to a recognized methodological approach [23]. The authors of the existing DFIPMs have presented their models in their own unique way except for a few instances where they have built upon a previous ad-hoc model [23]. In addition, with the exceptions of a few models, the majority of the existing models have not been evaluated in real life environments (i.e. on cases involving law enforcement agencies) to see whether they are usable or not. The followings provide a summary of the results of the analysis of the model assessments:

Existing models are not comprehensive as they do not capture the full scope of an investigation. Instead, they focus only on the middle part of a digital investigation.

- No model could be regarded formal as they all had differing focus and approaches. The authors of these models have adopted their own investigative methods based on their own personal experience.
- Despite the fact that the previous models have been peer-reviewed and published, none has been subjected to any form of testing with the exception of EMCI and CFFTPM.
- Existing DFIPMs do not have a pragmatic and practical approach and have not established a clear, step-by-step guide to what steps should be followed in a forensic process.
- No model included or referenced any standards against which an error rate could be calculated, nor was any model identified that has been widely accepted [23].

Irrespective of the claims of some authors that their models are "generic", none of the reviewed models can be regarded as generic. In order for a model to be considered generic, investigators should be able to apply the model in different fields of digital forensics i.e. law enforcement, commerce and incident response [17], [20]. Furthermore, the existing DFIPMs are single-tier, higher order process models that focus on abstract rather than concrete investigative principles. This limits the applicability of these models in real practice as they do not provide sufficient details to guide the steps of investigators when performing forensic investigations.

5. CONCLUSION

This paper critically reviewed and assessed the existing body of knowledge in relation to digital forensic investigation process models. Reviewing and assessing the existing DFIPMs against the Daubert Test in this paper has been conducted for the second time, Adams [23] being the first to evaluate the previous models against the same test. However, Adams [23] states, "… the Daubert test may be ineffective as a standard for determining the reliability of the process employed for acquiring digital evidence." This critical review and assessment presented in this paper reveal a lack of scientific consensus associated with the existing DFIPMs. The authors of these models have taken different approaches in terms of the number of phases as well as the terminology used in their models. Although many researchers have increasingly called for scientific approaches and formal methods, very little progress, if any, has been made. This critical review and assessment also reveal that there is no comprehensive model encompassing the entire digital investigative process that is formal in that it synthesizes, harmonises and extends the previous models, and that is generic in that it can be applied in the different fields of law enforcement, commerce and incident response. It is contended that this review and assessment of the existing DFIPMs is the most comprehensive evaluation that has been conducted so far.

6. REFERENCES

[1] Garfinkel, S. (2010). 'Digital forensics research: The next 10 years', *Digital Investigation*, 7, pp. 64–73.

[2] Casey, E. (2011). Digital Evidence and Computer Crime: Forensic Science, Computers *and the Internet.* 3rd edn. New York: Elsevier Academic Press.

[3] Nance, K., Hay, B. and Bishop, M. (2009). 'Digital Forensics: Defining a Research Agenda', *42nd Hawaii International Conference on System Sciences*, pp.1–6.

[4] Ieong, R. (2006). 'FORZA - Digital forensics investigation framework that incorporate legal issues', *Digital Investigation*, 3, pp. 29–36.

[5] Cohen, F. (2010). 'Towards a Science of Digital Forensic Evidence Examination', *6th* IFIP WG 11.9 International Conference on Digital Forensics, pp. 17-35.

[6] Freiling, C. and Schwittay, B. (2007). 'A Common Process Model for Incident Response and Computer Forensics', *3rd International Conference on IT-Incident Management & IT-Forensics*, pp. 19–40.

[7] Rowlingson, R. (2004). 'A Ten Step Process for Forensic Readiness', *International Journal of Digital Evidence*, 2(3), pp. 1-28.

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

[9] Wojcik, M., Venter, H., Eloff, J. and Olivier, M. (2006). 'Applying Machine Trust Models to Forensic Investigations', *IFIP international Conference on Advances in Digital Forensics*, pp. 55-65.

[10] Ciardhuáin, O. (2004). 'An Extended Model of Cybercrime Investigations', *International Journal of Digital Evidence*, 3(1), pp. 1-22.

[11] International Organisation for Standardization. (2012). ISO/IEC 27037:2012. *Information technology -- Security techniques -- Guidelines for identification, collection, acquisition and preservation of digital evidence.* Geneva, Switzerland: International Organization for Standardization.

[12] ACPO. (2012). *ACPO Good Practice Guide for Digital Evidence*. U.K. Association of Chief Police Officers. Available at: http://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf (Accessed: 10 June 2016).

[13] International Organisation for Standardization. (2015). ISO/IEC 27043:2015. *Information technology -- Security techniques -- Incident investigation principles and processes.* Geneva, Switzerland: International Organization for Standardization.

[14] Valjarevic, A. and Venter, H. (2015). 'A Comprehensive and Harmonized Digital Forensic Investigation Process Model', *Journal of Forensic Sciences*, 60(6), pp. 1467-1483.

[15] von Solms, S., Louwrens, C., Reekie, C. and Grobler, T. (2006). 'A Control Framework for Digital Forensics', *IFIP International Conference on Advances in Digital Forensics*, pp. 343-355.

[16] Rogers, M., Goldman, J., Mislan, R., Wedge, T. and Debrota, S. (2006). 'Computer Forensics Field Triage Process Model', *Conference on Digital Forensics, Security and Law*, pp. 27-40.

[17] Beebe, N. and Clark, J. (2005). 'A Hierarchical, Objectives-Based Framework for the Digital Investigations Process', *Digital Investigation*, 2(2), pp.147–167.

[18] Kruse, W. and Heiser, J. (2001). *Computer Forensics: Incident Response Essentials*. Boston: Addison-Wesley.

[19] Grobler, C.P., Louwrens, C.P. and Solms, S.H. (2010). 'A Multi-Component View of Digital Forensics', *ARES '10 International Conference on Availability, Reliability and Security*, pp. 647-652.

[20] Carrier, B. and Spafford, E. (2003). 'Getting Physical with the Digital Investigation Process', *International Journal of Digital Evidence*, 2(2), pp.1–20.

[21] Mandia, K., Prosise, C. and Pepe, M. (2003). *Incident Response and Computer Forensics. 2nd edn.* Emeryville: McGraw-Hill/Osborne.

[22] Kohn, M., Eloff, M. and Eloff, J. (2013). 'Integrated digital forensic process model', *Computers & Security*, 38, pp. 103–115.

[23] Adams, R. (2012). *The Advanced Data Acquisition Model (ADAM): A Process Model for Digital Forensic Practice.* PhD thesis. Murdoch University.

[24] Adams, R., Hobbs, V. and Mann, G. (2014). 'The advanced data acquisition model (ADAM): a process model for digital forensic practice', *Journal of Digital Forensics, Security and Law*, 8(4), pp.25–48.

[25] U.S. Courts. (2015). *Federal Rules of Evidence*. Administrative Office of the U.S. Courts. Available at: http://federalevidence.com/rules-of-evidence (Accessed: 21 June 2016).

[26] Sommer, P. (2008). *Directors' and Corporate Advisors' Guide to Digital Investigations and Evidence*. U.K. Information Assurance Advisory Council. Available at: https://www.ucisa.ac.uk/~/media/Files/members/activities/ist/DigitalInvestigationsGuide.ashx (Accessed: 17 June 2016).

[27] Farrell, M. (1993). Daubert v. Merrell Dow Pharmaceuticals, Inc.: Epistemilogy and Legal Process. *Cardozo L. Rev., 15*, p. 2183.

[28] Kessler, C. (2010). Judges' Awareness, Understanding, and Application of Digital *Evidence.* PhD thesis, Nova Southeastern University.

[29] Rothstein, B., Hedges, R. and Wiggins, E. (2007). Managing Discovery of Electronic Information: A Pocket Guide for Judges. Available at: https://bulk.resource.org/courts.gov/fjc/eldscpkt.pdf (Accessed: 21 June 2016).

[30] Meyers, M. and Rogers, M. (2006). 'Digital Forensics: Meeting the Challenges of Scientific Evidence', *IFIP International Conference on Advances in Digital Forensics*, pp. 43-50.

[31] Noblett, M., Pollitt, M. and Presley, L. (2000). 'Recovering and Examining Computer Forensic

Evidence', *Forensic Science Communication*, 2(4), pp. 1-13.

[32] Reith, M., Carr, C. and Gunsch, G. (2002). 'An Examination of Digital Forensic Models', *International Journal of Digital Evidence*, 1(3), pp. 1-12.

[33] Palmer, G. (2001). 'A Road Map for Digital Forensic Research', *1st Digital Forensic Research Workshop (DFRWS*), pp.27–30.

[34] Montasari, R (2016, a). 'An Ad Hoc Detailed Review of Digital Forensic Investigation Process Models', *International Journal of Electronic Security and Digital Forensics (IJESDF)*, 8 (3), pp. 205-223.

[35] Montasari, R. (2016, b). 'A Comprehensive Digital Forensic Investigation Process Model', *International Journal of Electronic Security and Digital Forensics (IJESDF)*, 8 (4), pp. 285-301.

[36] Montasari, R., Peltola, P. and Evans, D. (2015). 'Integrated Computer Forensics Investigation Process Model (ICFIPM) for Computer Crime Investigations', *Proceedings of 10th International Conference on Global Security, Safety and Sustainability: Tomorrow's Challenges of Cyber Security*, pp. 83-95.

[37] Boddington, R., Hobbs, V. and Mann, G. (2008). 'Validating digital evidence for legal argument', *6th Australian Digital Forensics Conference*, pp. 1-16.

[38] Peisert, S., Bishop, M. and Marzullo, M. (2008). 'Computer Forensics in Forensics', *Third International Workshop on Systematic Approaches to Digital Forensic Engineering*, pp. 102-122.

[39] Selamat, S., Yusof, R. and Sahib, S. (2008). 'Mapping Process of Digital Forensic Investigation Framework', *International Journal of Computer Science and Network Security*, 8(10), pp. 163-169.

[40] Baryamureeba, V. and Tushabe, F. (2004). 'The Enhanced Digital Investigation Process Model', *4th Digital Forensic Research Workshop*, pp. 1-9.

[41] Mercuri, R. (2005). 'Challenges in forensic computing', *Communications of the ACM*, 48(12), pp. 17-21.

[42] Montasari, R. and Peltola, P. (2015). 'Computer Forensic Analysis of Private Browsing Modes', *Proceedings of 10th International Conference on Global Security, Safety and Sustainability: Tomorrow's Challenges of Cyber Security*, pp. 96-109.

[43] Saferstein, R. (2010). *Criminalistics: An Introduction to Forensic Science*. 10th edn. Prentice Hall.

[44] Ashcroft, J. (2001). *Electronic Crime Scene Investigation: A Guide for First Responders*. U.S. Department of Justice. Available at: https://www.ncjrs.gov/pdffiles1/nij/187736.pdf (Accessed: 10 June 2016).

[45] Kent, K., Chevalier, S., Grance, T. and Dang, H. (2006). *Guide to Integrating Forensic Techniques into Incident Response*. U.S. Department of Commerce. Available at: http://cybersd.com/sec2/800-86Summary.pdf (Accessed: 16 June 2016).

[46] Khatir, M., Hejazi, M. and Sneiders, E. (2008). 'Two-dimensional evidence reliability amplification process model for digital forensics', *Third International Annual Workshop on Digital Forensics and Incident Analysis*, pp.21–29.

[47] Montasari, R (2016, c). 'A Formal Two Stage Triage Process Model (FTSTPM) for Digital Forensics Practice', *International Journal of Computer Science and Security (IJCSS*), 10 (2), pp. 69-87.